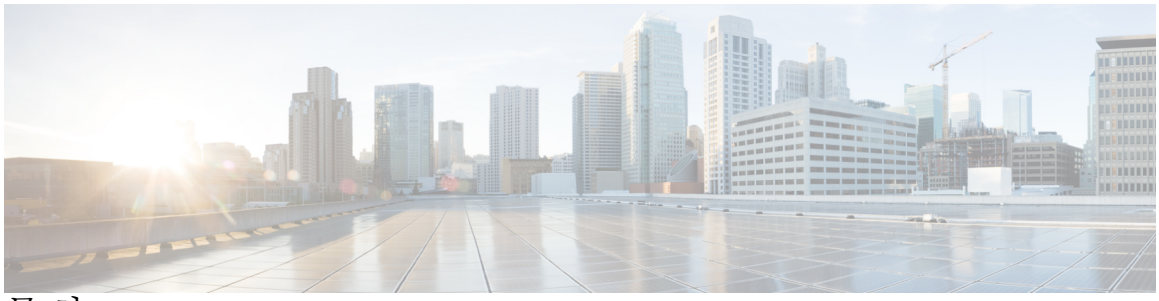
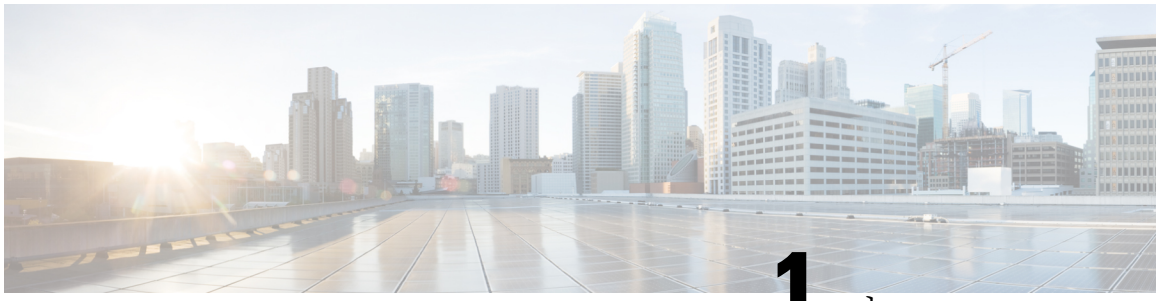
AsyncOS 12.0 for Cisco Email Security Appliances 사용자 가이드 - GD(일반 구축)

초판: 2019년 1월 31일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

Cisco Email Security Appliance 시작하기

이 장에는 다음 섹션이 포함되어 있습니다.

Async OS 12.0의 새로운 기능

표 *1: Async OS 12.0*의 새로운 기능

기능	설명
외부 위협 피드 사용 기능	이제 TAXII 프로토콜을 통해 전달되는 STIX 형식의 외부 위협 정보를 사용하도록 Cisco Email Security Appliance를 구성할 수 있습니다. Cisco Email Security Appliance에서 외부 위협 정보를 사용하는 기능을 통해 조직에서는 다음을 수행할 수 있습니다. • 악성코드, 랜섬웨어, 피싱 공격 및 표적 공격과 같은 사이버 위협에 능동적으로 대응할 수 있습니다. • TAXII 프로토콜을 통해 전달되는 STIX 형식의 외부 위협 피드를 가져올 수 있는 조직의 네트워크에서 외부 위협 피드 또는 기타 디바이스를 구독하고 어플라이언스에서 위협 정보를 사용할 수 있습니다. • 어플라이언스에서 동적 정보(예: URL의 동적 목록)를 가져와 이를 기반으로 메일 정책을 구성하거나 메시지 작업을 정의할 수 있습니다. • Cisco Email Security Appliance의 효율성을 개선할 수 있습니다. Classic Licensing 모드를 사용 중이고 외부 위협 피드 기능 키가 없는 경우 다음과 같이 Cisco GLO(Global Licensing Operations) 팀에 문의하여 기능 키를 얻어야 합니다. **1.** "Request for External Threat Feeds Feature Key"라는 메시지 제목으로 GLO 팀(licensing@cisco.com)에 이메일을 보내 PAK(Product Authorization Key) 파일 및 PO(구매 주문서) 정보를 제공합니다. **2.** GLO 팀은 기능 키를 수동으로 프로비저닝하여 어플라이언스에 설치할 라이선스 키가 포함된 이메일을 전송합니다. 참고 어플라이언스에서 Smart Licensing 모드로 전환하면 외부 위협 피드 기능 키가 자동으로 제공됩니다. 자세한 내용은 외부 피드 위협을 사용하도록 Cisco Email Security 게이트웨이 구성, 307 페이지 및 *AsyncOS for Cisco Email Security Appliance CLI* 참조 가이드를 참고하십시오.

기능	설명
발신자의 도메인 평판을 사용하여 메시지 필터링	Cisco SDR(발신자 도메인 평판)은 발신자의 도메인 및 기타 속성을 기반으로 이메일 메시지에 대한 평판 판정을 제공하는 클라우드 서비스입니다. 도메인 기반 평판 분석은 공유 IP 주소, 호스팅 또는 인프라 제공자의 평판을 확인하여 더 높은 탐지율을 지원하며, SMTP 대화 및 메시지 헤더에서 FQDN(Fully Qualified Domain Name) 및 기타 발신자 정보와 관련된 특성을 바탕으로 판정을 도출합니다. SDR에 대한 자세한 내용은 https://www.talosintelligence.com에서 Cisco Talos Security Intelligence and Research Group(Talos)에 문의하십시오. 자세한 내용은 발신자 도메인 평판 필터링, 323 페이지 및 *AsyncOS for Cisco Email Security Appliance CLI* 참조 가이드를 참고하십시오.
How-Tos 위젯을 사용하여 사용자 경험 개선	How-Tos는 어플라이언스에서 복잡한 작업을 수행할 수 있도록 사용자에게 워크스루 형태로 애플리케이션 내 지원을 제공하는 상황별 위젯입니다. 다음은 이 릴리스에 지원되는 워크스루입니다. • DMARC를 사용하여 수신 메시지 확인. • SPF/SIDF를 사용하여 수신 메시지 확인. • DKIM을 사용하여 수신 메시지 확인. • Email Security 게이트웨이에서 그레이메일 엔진 활성화 및 구성. • Email Security 게이트웨이에서 보안 침해 필터 활성화 및 구성. • 메시지에서 매크로 사용 첨부 파일 탐지. 참고 워크스루 목록은 클라우드에서 업데이트할 수 있습니다. 업데이트된 버전의 How-Tos 위젯 및 팝업 창을 보려면 브라우저 캐시를 지워야 합니다. 자세한 내용은 어플라이언스에 액세스, 11 페이지 및 *AsyncOS for Cisco Email Security Appliance CLI* 참조 가이드를 참고하십시오.

기능	설명
파일 분석을 위한 Cisco AMP Threat Grid 클러스터링 지원	이제 다음과 같은 방법으로 파일 분석을 위해 독립형 또는 클러스터링된 Cisco AMP Threat Grid 어플라이언스를 추가할 수 있습니다. • 웹 인터페이스의 **Security Services** > **File Reputation and Analysis(**파일 평판 및 분석**)** 페이지. File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석), 461 페이지를 참조하십시오. • CLI의 `ampconfig` 명령. *AsyncOS for Cisco Email Security Appliances CLI* 참조 가이드를 참고하십시오.
파일 분석에 대한 임계값 설정 구성	이제 허용되는 파일 분석 점수에 대한 임계값 상한을 설정할 수 있습니다. 임계값 설정에 따라 차단된 파일은 Advanced Malware Protection 보고서의 **Incoming Malware Threat Files(**수신 악성코드 위협 파일**)** 섹션에 **Custom Threshold(**맞춤형 임계값**)**로 표시됩니다. 자세한 내용은 File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석), 461 페이지의 내용을 참고하십시오.
위협 이름을 기준으로 악성 메시지 보기	이제 AMP 엔진에서 악성으로 탐지된 수신 또는 발신 메시지를 메시지 추적에서 위협 이름을 기준으로 검색할 수 있습니다. 자세한 내용은 메시지 추적, 837 페이지의 내용을 참고하십시오.
발신 TLS 연결에 대한 DANE(명명된 엔티티의 DNS 기반 인증) 지원	이제 어플라이언스에서 발신 TLS 연결에 대해 DANE(명명된 엔티티의 DNS 기반 인증)를 활성화하여 유효한 수신자 도메인으로 메시지를 안전하게 전송할 수 있습니다. 유효한 수신자 도메인으로 메시지를 안전하게 전송하는 기능은 대상 도메인이 DANE를 지원하는 경우 조직에서 비즈니스에 중요한 정보 및 기밀 정보를 의도된 수신자에게 전달하도록 도와줍니다. 자세한 내용은 다른 MTA와의 통신 암호화, 645 페이지을 참고하십시오.

기능	설명
Smart Software Licensing 지원	Smart Software Licensing을 사용하면 Cisco Email Security Appliance 라이선스를 원활하게 관리하고 모니터링할 수 있습니다. Smart Software Licensing을 활성화하려면 구매하고 사용하는 모든 Cisco 제품에 대한 라이선싱 세부 정보를 유지하는 중앙 집중식 데이터베이스인 CSSM(Cisco Smart Software Manager)에 어플라이언스를 등록해야 합니다. 다음은 어플라이언스에서 라이선싱 모드를 Classic Licensing 모드에서 Smart Licensing 모드로 전환할 경우의 이점입니다. • 물리적 어플라이언스와 가상 어플라이언스 사이에서 PAK(Product Authorization Key) 라이선스를 쉽게 처리할 수 있습니다. Classic Licensing 모드에서는 처리가 어려웠습니다. • 조직에서 디바이스 또는 가상 어카운트 간에 소프트웨어 라이선스를 쉽게 마이그레이션할 수 있습니다. • 어플라이언스에서 PAK 파일을 관리하거나 복사본을 유지할 필요가 없습니다. • Smart Licensing 어카운트에서 사용자 액세스를 제한할 수 있습니다. 주의 어플라이언스에서 Smart Licensing 기능을 활성화한 후에는 Smart Licensing 모드에서 Classic Licensing 모드로 롤백할 수 없게 됩니다. 자세한 내용은 시스템 관리, 923 페이지 및 *AsyncOS for Cisco Email Security Appliance CLI* 참조 가이드를 참고하십시오.

추가 정보 확인 위치

Cisco에서 제공하는 다음 리소스를 통해 어플라이언스에 대해 자세히 알아볼 수 있습니다.

• Cisco에 의견 보내기, 8 페이지
• Cisco 계정 등록 , 8 페이지

설명서

어플라이언스 GUI의 오른쪽 상단에 있는 Help and Support(도움말 및 지원)를 클릭하여 사용 설명서의 온라인 도움말 버전에 직접 액세스할 수 있습니다.

Cisco Email Security Appliance용 문서 집합에는 다음이 포함됩니다.

- 릴리스 정보
- Cisco Email Security Appliance 모델에 대한 빠른 시작 가이드
- 모델 또는 시리즈에 대한 하드웨어 설치 또는 하드웨어 설치 및 유지 보수 가이드
- *Cisco Content Security Virtual Appliance Installation Guide*
- *AsyncOS for Cisco Email Security Appliance* 사용자 가이드(본 문서)
- *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*
- AsyncOS API for Cisco Email Security Appliances - Getting Started Guide

모든 Cisco Content Security 제품에 대한 문서는 다음에서 이용할 수 있습니다.

Cisco Content Security 제품 설명서	위치
하드웨어 및 가상 어플라이언스	이 표에 있는 해당 제품을 참조해 주십시오.
Cisco Email Security	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd- products-support-series-home.html
Cisco Web Security	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products- support-series-home.html
Cisco Content Security Management	http://www.cisco.com/c/en/us/support/security/content-security-management- appliance/tsd-products-support-series-home.html
Cisco Content Security Appliance의 CLI 참조 가이드	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort Encryption	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html

교육

교육에 대한 추가 정보는 다음에서 이용할 수 있습니다.

- http://www.cisco.com/c/en/us/training-events/training-certifications/supplemental-training/email-and-web-security.html
- http://www.cisco.com/c/en/us/training-events/training-certifications/overview.html

Cisco 알림 서비스

보안 자문, 현장 통지, 판매 중단 및 지원 종료 안내문, 소프트웨어 업데이트 및 알려진 문제에 대한 정보 등 Cisco Content Security Appliance와 관련된 알림을 수신하려면 신청하십시오.

알림 빈도, 수신할 정보 유형 등의 옵션을 지정할 수 있습니다. 사용하는 각 제품에 대한 알림을 받으려면 개별적으로 신청해야 합니다.

신청하려면http://www.cisco.com/cisco/support/notifications.html을 방문해 주십시오.

Cisco.com 계정이 필요합니다. 계정이 없으면 Cisco 계정 등록 , 8 페이지 섹션을 참조해 주십시오.

기술 자료

단계 **1** 기본 제품 페이지(http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html)로 이동합니다.

단계 **2** **TechNotes**라는 이름의 링크를 찾습니다.

Cisco Support Community

Cisco 지원 커뮤니티는 Cisco 고객, 파트너 및 직원을 위한 온라인 포럼입니다. 이 커뮤니티에서는 일반적인 이메일 및 웹 보안 문제뿐만 아니라 특정한 Cisco 제품에 대한 기술 정보에 대해서도 논의할 수 있습니다. 포럼에 주제를 게시하여 궁금한 점을 질문하고 다른 Cisco 사용자와 정보를 공유할 수 있습니다.

다음 URL을 통해 지원 커뮤니티 및 고객 지원 포털에 액세스할 수 있습니다.

- 이메일 보안 및 관련 관리:

  https://supportforums.cisco.com/community/5756/email-security

- 웹 보안 및 관련 관리:

  https://supportforums.cisco.com/community/5786/web-security

Cisco 고객 지원

Cisco TAC: http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

레거시 IronPort에 대한 지원 사이트: http://www.cisco.com/c/en/us/services/acquisitions/ironport.html

심각하지 않은 문제의 경우, 어플라이언스에서 고객 지원에 액세스할 수도 있습니다. 관련 지침은 사용 설명서 또는 온라인 도움말을 참조하십시오.

서드파티 지원업체

사용 중인 릴리스에 대한 오픈 소스 라이선싱 정보는 http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-release-notes-list.html 페이지를 참고하십시오.

Cisco AsyncOS에 포함된 일부 소프트웨어는 FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc. 및 기타 서드파티 기여자의 소프트웨어 라이선스 계약의 약관과 통지에 따라 배포되며, 모든 해당 약관은 Cisco 라이센스 계약에 통합되어 있습니다.

이러한 계약의 전문은 다음에서 찾아볼 수 있습니다.

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html.

Cisco AsyncOS에 포함된 소프트웨어의 일부는 Tobi Oetiker가 명시적으로 서면 동의한 RRDtool을 기반으로 합니다.

이 문서의 일부는 Dell Computer Corporation의 허가로 다시 작성되었습니다. 이 문서의 일부는 McAfee, Inc.의 허가로 다시 작성되었습니다. 이 문서의 일부는 Sophos Plc.의 허가로 다시 작성되었습니다.

Cisco에 의견 보내기

Cisco Technical Publications 팀은 더 우수한 제품 설명서를 제공하기 위해 최선을 다하고 있습니다. 소중한 의견과 제안을 언제라도 보내주십시오. 다음 이메일 주소로 의견을 보내실 수 있습니다.

contentsecuritydocs@cisco.com

제품 이름, 릴리스 번호, 문서 발행일을 메시지 제목에 포함해주십시오.

Cisco 계정 등록

Cisco.com의 많은 리소스에 액세스하려면 Cisco 계정이 필요합니다.

Cisco.com 사용자 ID가 없는 경우 다음에서 등록할 수 있습니다.
https://tools.cisco.com/RPF/register/register.do%20

관련 주제

- Cisco 알림 서비스 , 7 페이지
- 기술 자료, 7 페이지

Cisco Email Security Appliance 개요

AsyncOS™ 운영 체제에는 다음과 같은 기능이 포함되어 있습니다.

- **Anti-Spam(**안티 스팸**)**. SenderBase 평판 필터와 Cisco Anti-Spam이 통합된 고유한 다중 레이어 접근 방식을 통해 게이트웨이에서 제공됩니다.
- **Anti-Virus(**안티바이러스**)**. Sophos 및 McAfee Anti-Virus 검사 엔진과 함께 게이트웨이에서 제공됩니다.

- **Outbreak Filters(**보안 침해 필터**)™**. 신종 바이러스, 스캠 및 피싱 보안 침해에 대처하는 Cisco의 고유한 보호 기능으로, 새 업데이트가 적용될 때까지 위험한 메시지를 격리함으로써 새 메시지 위협에 대한 취약성 기간을 단축합니다.
- **Policy(**정책**), Virus(**바이러스**)** 및 **Outbreak(**보안 침해**)** 격리. 관리자가 평가할 수 있도록 의심스런 메시지를 저장하기 위한 안전한 장소를 제공합니다.
- **Spam Quarantine(**스팸 격리**)**. 격리된 스팸 및 의심스런 스팸에 대한 최종 사용자 액세스를 제공합니다(온박스 또는 오프박스).
- **Email Authentication(**이메일 인증**)**. Cisco AsyncOS는 SPF(Sender Policy Framework), SIDF(Sender ID Framework) 및 DKIM(DomainKeys Identified Mail) 수신 메일 확인, 그리고 DomainKeys 및 DKIM 발신 메일 서명 등 다양한 형식의 이메일 인증을 지원합니다.
- Cisco 이메일 암호화. HIPAA, GLBA 및 유사한 규제 의무를 준수하도록 발신 메일을 암호화할 수 있습니다. 이렇게 하려면 Email Security Appliance에서 암호화 정책을 구성하고, 로컬 키 서버 또는 호스팅된 키 서비스를 사용하여 메시지를 암호화합니다.
- **Email Security Manager(**이메일 보안 관리자**)**. 어플라이언스에서 모든 이메일 보안 서비스 및 애플리케이션을 관리하기 위한 포괄적인 단일 대시보드입니다. Email Security Manager(이메일 보안 관리자)에서는 사용자 그룹을 기반으로 이메일 보안을 시행할 수 있습니다. 따라서 별도의 인바운드 및 아웃바운드 정책을 통해 Cisco 평판 필터, 보안 침해 필터, 안티 스팸, 안티 바이러스 및 이메일 콘텐츠 정책을 관리할 수 있습니다.
- 온박스**(On-box)** 메시지 추적 - AsyncOS for Email에는 Email Security 어플라이언스가 처리하는 메시지의 상태를 쉽게 확인할 수 있도록 온박스(On-box) 메시지 추적 기능이 있습니다.
- 메일 흐름 모니터링 - 모든 인바운드 및 아웃바운드 이메일을 모니터링 하여 기업의 모든 이메일 트래픽에 대하여 완벽한 가시성을 제공합니다.
- 액세스 제어. 발신자의 IP 주소, IP 주소 범위 또는 도메인을 기반으로 인바운드 발신자의 액세스를 제어합니다.
- 메시지 및 콘텐츠 필터링. 광범위한 메시지 및 콘텐츠 필터링 기술을 활용하여 회사 정책을 적용하고 회사 인프라에 메시지가 들어오거나 나갈 때 특정 메시지에 작업을 수행할 수 있습니다. 필터 규칙은 메시지나 첨부 파일 내용, 네트워크에 대한 정보, 메시지 봉투, 메시지 헤더, 메시지 본문 등을 기반으로 메시지를 식별합니다. 필터 작업을 통해 메시지를 삭제, 반송, 보관, 숨은 참조 또는 변경하거나 알림을 생성할 수 있습니다.
- **Transport Layer Security**의 보안 **SMTP**를 통해 메시지 암호화. 회사 인프라 및 기타 신뢰할 수 있는 호스트 간에 이동하는 메시지의 암호화를 보장합니다.
- **Virtual Gateway(**가상 게이트웨이**)™**. 가상 게이트웨이 기술을 통해 Email Security Appliance가 단일 서버 내에서 여러 이메일 게이트웨이 기능을 수행할 수 있습니다. 따라서 이메일을 다른 소스 또는 캠페인과 분리하여 별도의 IP 주소를 통해 전송할 수 있습니다. 이러한 분리 덕분에 한 IP 주소에 영향을 미치는 전달 가능성 문제가 다른 주소에는 영향을 미치지 않습니다.
- 여러 서비스에서 제공하는 이메일 메시지의 악성 첨부 파일과 링크를 보호할 수 있습니다.
- 데이터 손실 방지를 사용하여 조직에서 나가는 정보를 제어하고 모니터링할 수 있습니다.

AsyncOS는 메시지 수락 및 전달을 위한 RFC 2821 준수 SMTP(Simple Mail Transfer Protocol)를 지원합니다.

HTTP 또는 HTTPS를 통해 웹 기반 GUI에서 대부분의 보고, 모니터링 및 구성 명령을 사용할 수 있습니다. 또한 SSH(Secure Shell) 또는 직접 직렬 연결을 통해 액세스할 수 있는 대화형 CLI(Command Line Interface)도 제공됩니다.

또한 Security Management Appliance를 설치하여 여러 Email Security Appliance에 대한 보고, 추적 및 격리 관리를 통합할 수 있습니다.

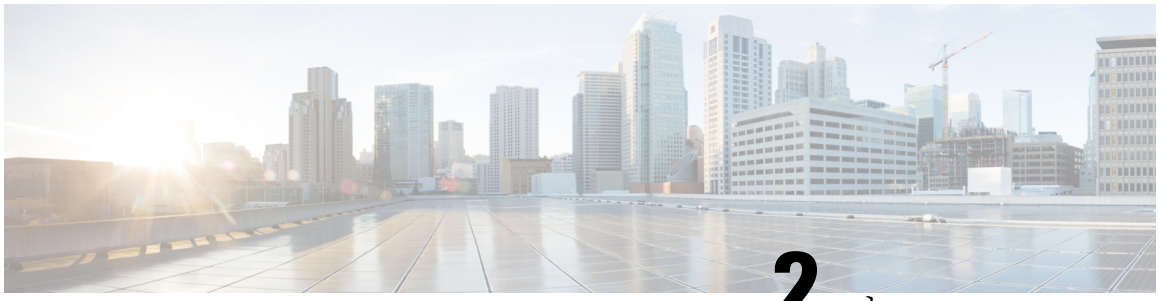
관련 주제

• 지원되는 언어, 10 페이지

지원되는 언어

AsyncOS는 GUI 및 CLI를 다음 언어로 표시할 수 있습니다.

- 영어
- 프랑스어
- 스페인어
- 독일어
- 이탈리아어
- 한국어
- 일본어
- 포르투갈어(브라질)
- 중국어(번체 및 간체)
- 러시아어



2 장

어플라이언스에 액세스

이 장에는 다음 섹션이 포함되어 있습니다.

웹 기반 그래픽 사용자 인터페이스(GUI)

GUI(웹 기반 그래픽 사용자 인터페이스)와 CLI(Command Line Interface)를 모두 사용하여 어플라이언스를 관리할 수 있습니다. GUI에는 시스템 구성과 모니터링에 필요한 기능 대부분이 포함되어 있습니다. 그러나 일부 CLI 명령은 GUI에서 사용할 수 없으며 일부 기능은 *CLI*에서만 사용할 수 있습니다.

브라우저 요구 사항

웹 기반 UI에 액세스하려면 브라우저가 JavaScript 및 쿠키를 지원하고 이를 허용해야 합니다. 또한, CSS(Cascading Style Sheet)가 포함된 HTML 페이지를 렌더링할 수 있어야 합니다.

브라우저	운영 체제
Internet Explorer 11.0	Microsoft Windows 7
Safari 7.0 이상	Mac OS X
Firefox 39.0 이상	Microsoft Windows 7, Mac OS X
Chrome 44.0 이상	Microsoft Windows 7, Mac OS X

어플라이언스를 변경하기 위해 여러 브라우저 윈도우나 탭을 동시에 사용하지 마십시오. GUI와 CLI 세션을 동시에 사용하면 안 됩니다. 그러한 사용 방식은 지원되지 않으며 예기치 않은 동작의 원인이 될 수 있습니다.

인터페이스의 일부 버튼이나 링크를 클릭하면 추가 창이 열리므로 웹 인터페이스를 사용하려면 브라우저의 팝업 차단 설정을 구성해야 할 수 있습니다.

GUI 액세스

새 시스템에서 GUI에 액세스하려면 다음 URL을 확인합니다.

http://192.168.42.42/

로그인 페이지가 표시되면 기본 사용자 이름과 암호를 사용하여 시스템에 로그인합니다.

관련 주제

- 공장 기본 사용자 이름 및 암호, 12 페이지
- 중앙 집중식 관리, 13 페이지

공장 기본 사용자 이름 및 암호

- 사용자 이름: **admin**
- 암호: **ironport**

새로운(이전 AsyncOS 릴리스에서 업그레이드되지 않음) 시스템에서는 시스템 설치 마법사로 자동 리디렉션됩니다.

초기 시스템 설정에서 인터페이스의 IP 주소와 해당 인터페이스에 HTTP 및/또는 HTTPS 서비스를 실행할지 여부를 선택합니다. 인터페이스의 HTTP 및/또는 HTTPS 서비스를 활성화한 경우 지원 브라우저를 사용하여 브라우저의 위치 필드("주소 표시줄")에 IP 인터페이스의 IP 주소 또는 호스트 이름을 URL로 입력하여 GUI를 확인할 수 있습니다.

예를 들면 다음과 같습니다.

`http://192.168.1.1` 또는

`https://192.168.1.1` 또는

`http://mail3.example.com` 또는

`https://mail3.example.com`

참고 인터페이스에 대해 HTTPS가 활성화된 경우(그리고 HTTP 요청이 보안 서비스로 리디렉션되지 않는 경우), "`http`**s**://" 접두사를 사용하여 GUI에 액세스하십시오.

관련 주제

- 사용자 추가 , 897 페이지

중앙 집중식 관리

클러스터를 생성한 경우 클러스터에서 머신을 찾거나 GUI에서 클러스터, 그룹 및 머신에 대한 설정을 생성/삭제하고, 설정을 복사/이동할 수 있습니다(`clustermode` 및 `clusterset` 명령에 해당하는 작업 수행).

자세한 내용은 GUI에서 클러스터 관리, 1132 페이지를 참고하십시오.

How-Tos 위젯을 사용하여 사용자 경험 개선

How-Tos는 어플라이언스에서 복잡한 작업을 수행할 수 있도록 사용자에게 워크스루 형태로 애플리케이션 내 지원을 제공하는 상황별 위젯입니다. 이 릴리스에서 지원되는 워크스루 목록을 보려면 *AsyncOS 12.0 for Cisco Email Security Appliances* 릴리스 *Cisco Email Security Appliance*의 *AsyncOS 12.0*에 대한 릴리스 노트를 참고하십시오.

어플라이언스의 웹 인터페이스에서 How-Tos 위젯을 클릭하여 워크스루에 액세스할 수 있습니다. 기본적으로 How-Tos 위젯은 어플라이언스에서 활성화되어 있습니다. How-Tos 위젯의 내용은 클라우드 업데이트에서 업데이트할 수 있습니다.

각 워크스루에는 다음과 같이 분류된 특정 구성 가능한 값에 대한 권장 설정이 있습니다.

- Conservative Settings(보수적인 설정) - 주의, 과도한 제한이 없는 구성
- Moderate Settings(중간 설정) - 평균, 적절한 제한이 있는 구성
- Aggressive Settings(적극적인 설정) - 강제, 엄격한 제한이 있는 구성

참고

- 현재 워크스루 집합은 admin, cloud-admin 및 operator 사용자로 제한됩니다.
- Internet Explorer 버전 11을 사용하여 어플라이언스의 웹 인터페이스에 액세스하는 경우 How-Tos 위젯이 표시되지 않을 수도 있습니다. How-Tos 위젯을 보려면 웹 인터페이스에서 **System Administration(시스템 관리) > General Settings(일반 설정)** 페이지로 이동하여 Override IE Compatibility Mode(IE 호환성 모드 재정의) 옵션을 활성화하십시오.

어플라이언스에서 How-Tos 위젯 비활성화

어플라이언스에서 How-Tos 위젯을 비활성화하려면 CLI에서 `adminaccessconfig > how-tos` 명령을 사용합니다.

예: 어플라이언스에서 **How-Tos** 위젯 비활성화

```
mail.example.com> adminaccessconfig

Choose the operation you want to perform:

- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator
login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
```

```
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- XSS - Configure Cross-Site Scripting Attack protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
- MAXHTTPHEADERFIELDSIZE - Configure maximum HTTP header Field size.
- HOW-TOS - Configure How-Tos feature.

[]> how-tos
How-Tos consists of a list of generic walkthroughs to assist the users in completing
a particular task (for example, "enabling and configuring a service engine on the appliance").

Would you like to enable How-Tos? [Y]> no
```

구성 설정 변경

구성 변경

이메일 운영이 정상적으로 진행되는 동안에는 구성을 변경할 수 있습니다.

변경사항 커밋 또는 취소

대부분의 구성 변경사항을 저장해야 합니다.

변경 사항이 커밋 대기 중이면 Commit Changes(변경 커밋) 버튼이 주황색으로 바뀝니다.

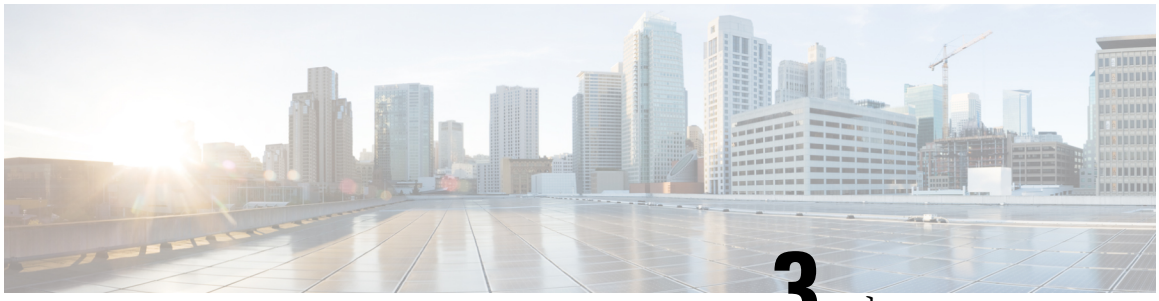
이러한 변경 사항을 지우거나 커밋하려면 **Commit Changes(**변경 커밋**)**를 클릭합니다.

명령줄 인터페이스(CLI)

명령행 인터페이스는 이러한 서비스가 활성화된 상태로 구성된 IP 인터페이스의 SSH를 통해 또는 병렬 포트의 터미널 에뮬레이션 소프트웨어를 통해 액세스할 수 있습니다. 기본적으로 SSH는 관리 포트에서 구성됩니다. `interfaceconfig` 명령를 사용하여 이러한 서비스를 비활성화할 수 있습니다.

CLI 명령 및 규칙에 대한 자세한 내용은 AsyncOS for Cisco Email Security Appliance CLI 참조 가이드를 참고하십시오.

참고 CLI 액세스를 위한 공장 기본 사용자 이름과 암호는 웹 인터페이스와 동일합니다. 공장 기본 사용자 이름 및 암호, 12 페이지를 참조하십시오.



3 장

설정 및 설치

이 장에는 다음 섹션이 포함되어 있습니다.

설치 계획

계획 결정에 영향을 미치는 정보 검토

- 가상 Email Security Appliance를 구성 중인 경우 이 장을 진행하기 전에 *Cisco Content Security Virtual Appliance Installation Guide*를 참조해 주십시오.
- M-Series Cisco Content Security Management Appliance를 구성 중인 경우 Cisco Content(M-Series) Security Management Appliance에서 서비스 중앙 집중화, 1187 페이지를 참고하십시오.
- 설치 전에 이메일 파이프라인 이해, 57 페이지를 검토할 것을 권장합니다. 일부 기능이 인프라 내에서 어플라이언스의 배치에 영향을 줄 수 있기 때문입니다.

네트워크 경계에 **Email Security Appliance**를 배치하기 위한 계획

Email Security Appliance는 MX(mail exchange)라고도 하는 SMTP 게이트웨이 역할을 하도록 설계되었습니다. 최고의 결과를 얻으려면, 일부 기능에서는 어플라이언스가 이메일을 주고받기 위해 인터넷에 직접 액세스할 수 있는 IP 주소가 있는 첫 번째 시스템이어야 합니다.

수신자당 평판 필터링, 안티스팸, 안티바이러스 및 바이러스 Outbreak Filter 기능(SenderBase 네트워크 참여, 1029 페이지, IronPort Anti-Spam 필터링, 358 페이지, Sophos 안티 바이러스 필터링, 336 페이지 및 신종 바이러스 필터(Outbreak Filter), 399 페이지 참조)은 인터넷 및 인터넷 네트워크에서 메시지의 직접 플로우와 작동하도록 설계됩니다. 엔터프라이즈를 드나드는 모든 이메일에 대해 정책을 시행하도록(연결을 허용할 호스트 정의 개요, 93 페이지) 어플라이언스를 구성할 수 있습니다.

Email Security Appliance는 공용 인터넷을 통해 액세스 가능해야 하며, 이메일 인프라의 "첫 번째 홉"이어야 합니다. 또 다른 MTA를 네트워크 경계에 두고 모든 외부 연결을 처리하도록 설정하면 Email Security Appliance에서 발신자의 IP 주소를 확인할 수 없게 됩니다. 발신자의 IP 주소는 메일 플로우 모니터에서 발신자를 식별 및 구별하고, SenderBase Reputation Service에 SBRS(SenderBase Reputation Score)를 쿼리하고, 안티스팸 및 Outbreak Filter 기능의 효율성을 개선하는 데 필요합니다.

참고 인터넷에서 이메일을 수신하는 첫 번째 시스템으로서 어플라이언스를 구성할 수 없는 경우에도 어플라이언스에서 사용할 수 있는 몇 가지 보안 서비스를 실행할 수 있습니다. 자세한 내용은 수신 릴레이 사용 배포 환경에서 발신자 IP 주소 확인 , 374 페이지를 참고하십시오.

Email Security Appliance를 SMTP 게이트웨이로 사용하는 경우

- 메일 플로우 모니터 기능(이메일 보안 모니터 사용, 793 페이지 참조)은 내부 및 외부 발신자 모두에서 오는 모든 이메일 트래픽에 대한 완전한 가시성을 엔터프라이즈에 제공합니다.
- 라우팅, 별칭 및 가장에 대한 LDAP 쿼리(LDAP 쿼리, 735 페이지 참조)는 디렉터리 인프라를 통합하고 좀 더 간단한 업데이트를 제공할 수 있습니다.
- 별칭 테이블(별칭 테이블 만들기, 671 페이지 참조), 도메인 기반 라우팅(도메인 맵 기능, 688 페이지) 및 가장(가장 구성, 678 페이지)과 같은 친숙한 툴을 사용하면 오픈 소스 MTA에서 더 쉽게 전환할 수 있습니다.

DNS에서 Email Security Appliance 등록

악의적인 이메일 발신자는 새로운 희생자를 찾기 위해 공개 DNS 기록을 적극적으로 검색합니다. 안티바이러스, Outbreak Filter, McAfee Antivirus 및 Sophos Anti-Virus의 기능을 최대한 활용하려면 Email Security Appliance가 DNS에 등록되어 있어야 합니다.

DNS에 어플라이언스를 등록하려면 어플라이언스의 호스트 이름을 IP 주소에 매핑하는 A 기록과 공개 도메인을 어플라이언스의 호스트 이름에 매핑하는 MX 기록을 만듭니다. Email Security Appliance를 도메인의 기본 또는 백업 MTA로 알리려면 MX 기록의 우선 순위를 지정해야 합니다.

다음 예에서는 MX 기록에 더 큰 우선 순위 값(20)이 있으므로 Email Security Appliance(ironport.example.com)는 도메인 example.com의 백업 MTA입니다. 다시 말하면, 숫자 값이 더 클수록 MTA 우선 순위는 더 낮습니다.

```
$ host -t mx example.com
```

```
example.com mail is handled (pri=10) by mail.example.com
```

```
example.com mail is handled (pri=20) by ironport.example.com
```

Email Security Appliance를 DNS에 등록하면 MX 기록 우선 순위를 설정한 방식과 상관없이 스팸 공격 대상이 됩니다. 그러나 바이러스 공격이 백업 MTA를 대상으로 하는 경우는 매우 드뭅니다. 이를 염두에 두고, 안티바이러스 엔진의 잠재력을 최대한 평가하려면 MX 기록 우선 순위를 MTA의 나머지와 같거나 더 높게 설정하도록 Email Security Appliance를 구성해 주십시오.

설치 시나리오

기존의 네트워크 인프라에 Email Security Appliance를 여러 가지 방법으로 설치할 수 있습니다.

대부분의 고객 네트워크 구성은 다음 시나리오와 같습니다. 네트워크 구성이 크게 다르고 설치 계획에 도움이 필요한 경우 Cisco 고객 지원에 문의하십시오(Cisco 고객 지원, 7 페이지 참고).

구성 개요

다음 그림은 엔터프라이즈 네트워크 환경에서 Email Security Appliance의 일반적인 배치를 보여줍니다.

일부 시나리오에서 Email Security Appliance는 네트워크 "DMZ"에 상주하는데, 이 경우 Email Security Appliance와 그룹웨어 서버 사이에 추가 방화벽이 놓여 있습니다.

다음과 같은 네트워크 시나리오가 가능합니다.

- 방화벽 뒤: 2개의 리스너 구성(그림 - 방화벽 뒤 시나리오/2개의 리스너 구성)

각자의 인프라에 가장 적합한 구성을 선택하고, 다음 섹션인 시스템 설정 준비, 22 페이지로 진행해 주십시오.

Incoming

- 수신 메일은 지정된 로컬 도메인에 대해 수락됩니다.
- 다른 모든 도메인은 거부됩니다.
- 외부 시스템은 Email Security Appliance에 직접 연결하여 로컬 도메인에 대한 이메일을 전송하고, Email Security Appliance는 SMTP 경로를 통해 메일을 적절한 그룹웨어 서버(예: Exchange™, Groupwise™, Domino™)로 릴레이합니다. (로컬 도메인용 이메일 라우팅, 665 페이지참조.)

Outgoing

- 내부 사용자가 전송한 발신 메일은 그룹웨어 서버에 의해 Email Security Appliance로 라우팅됩니다.
- Email Security Appliance는 프라이빗 리스너에 대한 Host Access Table의 설정을 기반으로 아웃바운드 이메일을 수락합니다. (자세한 내용은 리스너 작업, 70 페이지를 참조하십시오.)

이더넷 인터페이스

이러한 구성에는 Email Security Appliance에서 사용 가능한 이더넷 인터페이스 중 하나만 필요합니다. 그러나 이더넷 인터페이스 2개를 구성하고 내부 네트워크를 외부 인터넷 네트워크 연결과 분리할 수 있습니다.

사용 가능한 인터페이스에 여러 IP 주소를 할당하는 방법에 대한 자세한 내용은 호스팅된 모든 도메인에 대한 메일 게이트웨이 구성에 Virtual Gateway™ 기술 사용, 718 페이지 및 네트워크 및 IP 주소 할당, 1205 페이지을 참조해 주십시오.

하드웨어 포트

하드웨어 어플라이언스에 있는 포트의 수와 유형은 모델에 따라 다릅니다.

포트	유형	C170	C370	C670	X1070	C380	C680	C190	C390	C690
Management	이더넷	0	1	1	1	1	1	0	1	1
데이터	이더넷	2*	3	3	3	3	3	2*	5	5
콘솔	일련 번호	9핀	9핀	9핀	9핀	RJ-45	RJ-45	RJ-45	RJ-45	RJ-45
RPC(Remote Power Management)	이더넷	아니요	아니요	아니요	아니요	예	예	예	예	예

* 전용 관리 포트가 없는 어플라이언스의 경우 관리 목적으로 Data1 포트를 사용해 주십시오.

포트에 대한 자세한 내용은 어플라이언스 모델의 *Hardware Installation Guide(*하드웨어 설치 가이드*)*를 참조해 주십시오.

관련 주제

- 네트워크 인터페이스 구성, 34 페이지
- 시리얼 연결을 통해 이메일 보안 어플라이언스 액세스, 1203 페이지
- 원격 전원 제어 활성화 , 958 페이지

고급 구성

방화벽 뒤 시나리오/2개의 리스너 구성 그림 및 1개의 리스너 구성 그림에 표시된 구성 외에도 다음을 구성할 수 있습니다.

- 중앙 집중식 관리 기능을 사용하는 여러 Email Security Appliance. 클러스터를 사용한 중앙 집중식 관리, 1117 페이지를 참고하십시오.
- NIC 페어링 기능을 사용하여 Email Security Appliance에서 이더넷 인터페이스 2개의 "티밍(teaming)"으로 네트워크 인터페이스 카드 레벨에서 이중화. 고급 네트워크 컨피그레이션, 1039 페이지를 참조하십시오.

방화벽 설정(NAT, 포트)

SMTP 및 DNS 서비스는 인터넷에 액세스해야 합니다. 다른 서비스에서도 열린 방화벽 포트를 요구할 수 있습니다. 자세한 내용은 방화벽 정보, 1227 페이지를 참조하십시오.

Email Security Appliance를 네트워크에 물리적으로 연결

구성 시나리오

Email Security Appliance의 일반적인 구성 시나리오는 다음과 같습니다.

- 인터페이스 - 대부분의 네트워크 환경에는 Email Security Appliance에서 사용 가능한 3개의 이더넷 인터페이스 중 하나만 필요합니다. 그러나 이더넷 인터페이스 2개를 구성하고 내부 네트워크를 외부 인터넷 네트워크 연결과 분리할 수 있습니다.
- 퍼블릭 리스너(수신 이메일) - 퍼블릭 리스너는 많은 외부 호스트에서 연결을 수신하고 메시지를 제한된 수의 내부 그룹웨어 서버로 전달합니다.
  - HAT(Host Access Table)의 설정을 기반으로 외부 메일 호스트에서의 연결을 수락합니다. 기본적으로 HAT는 모든 외부 메일 호스트에서의 연결을 수락(ACCEPT)하도록 구성됩니다.
  - RAT(Recipient Access Table)에 지정된 로컬 도메인에 대해 주소가 지정된 경우에만 수신 메일을 수락합니다. 다른 모든 도메인은 거부됩니다.
  - SMTP 경로에 정의된 대로 적절한 내부 그룹웨어 서버로 메일을 릴레이합니다.
- 프라이빗 리스너(발신 이메일) - 프라이빗 리스너는 제한된 수의 내부 그룹웨어 서버로부터 연결을 수신하고 다수의 외부 메일 호스트로 메시지를 전달합니다.
  - 내부 그룹웨어 서버는 발신 메일을 Cisco C-Series 또는 X-Series 어플라이언스로 라우팅하도록 구성됩니다.
  - Email Security Appliance는 HAT의 설정을 기반으로 내부 그룹웨어 서버로부터의 연결을 수락합니다. 기본적으로 HAT는 모든 내부 메일 호스트로부터의 연결을 릴레이(RELAY)하도록 구성됩니다.

관련 주제

- 수신 및 발신 메일 분리, 20 페이지

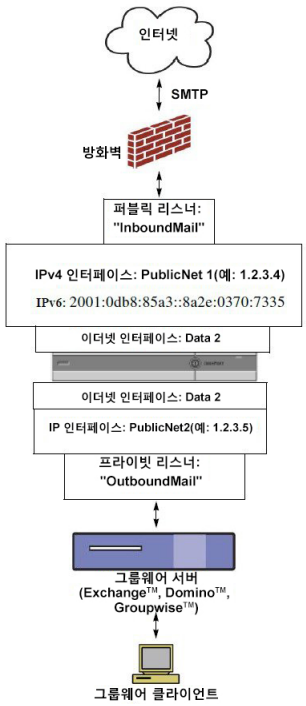
수신 및 발신 메일 분리

별도의 리스너 및 별도의 IP 주소를 통해 수신 및 발신 이메일 트래픽을 분리할 수 있습니다. IPv4(Internet Protocol version 4) 및 IPv6(version 6) 주소를 사용할 수 있습니다. 그러나 어플라이언스의 시스템 설정 마법사는 다음의 초기 구성을 지원합니다.

- 별도의 물리적 인터페이스에 구성된 2개의 논리적 IPv4 및 2개의 IPv6 주소의 개별 리스너 2개
  - 수신 및 발신 트래픽 분리
  - 각 리스너에 IPv4 및 IPv6 주소를 각각 하나씩 할당 가능
- 하나의 물리적 인터페이스에 구성된 1개의 논리적 IPv4 주소의 리스너 1개
  - 수신 및 발신 트래픽을 모두 결합
  - 리스너에 IPv4 및 IPv6 주소를 모두 할당 가능

1개 리스너 및 2개 리스너 구성 모두에 대한 구성 워크시트가 아래에 포함되어 있습니다(설정 정보 수집, 25 페이지 참조). 대부분의 구성 시나리오는 다음 세 가지 그림 중 하나로 표현됩니다.

그림 ***1:*** 방화벽 뒤 시나리오***/2***개 리스너 구성



참고:

- 리스너 2개
- IPv4 주소 2개
- IPv6 주소 2개
- 이더넷 인터페이스 1개 또는 2개(1개만 표시)

- 구성된 SMTP 경로

인바운드 리스너**: "InboundMail"(**퍼블릭**)**

- IPv4 주소: 1.2.3.4
- IPv6 주소: 2001:0db8:85a3::8a2e:0370:7334
- Data2 인터페이스의 리스너는 포트 25에서 수신 대기
- HAT(모두 수락)
- RAT(로컬 도메인에 대한 메일 수락, 모두 거부)

아웃바운드 리스너**: "OutboundMail"(**프라이빗**)**

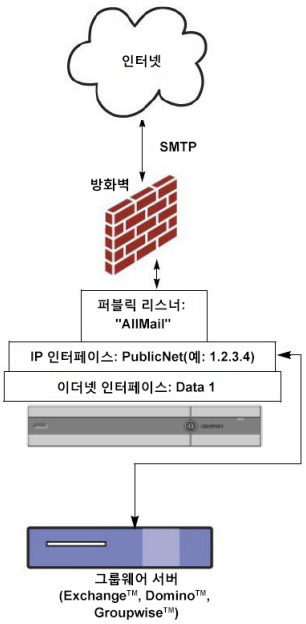
- IP 주소: 1.2.3.5
- IPv6 주소: 2001:0db8:85a3::8a2e:0370:7335
- Data2 인터페이스의 리스너는 포트 25에서 수신 대기
- HAT(로컬 도메인에 대한 릴레이, 모두 거부)

인터넷 루트 서버 또는 내부 DNS 서버를 사용하도록 DNS 구성 가능

SMTP 경로가 메일을 적절한 그룹웨어 서버로 전달

Email Security Appliance로 드나드는 해당 서비스에 대해 열리는 방화벽 포트

그림 ***2:*** 리스너 ***1***개 구성



참고**:**

- 리스너 1개
- IP 주소 1개
- 이더넷 인터페이스 1개
- 구성된 SMTP 경로

인바운드 리스너**: "InboundMail"(**퍼블릭**)**

- IP 주소: 1.2.3.4
- Data2 인터페이스의 리스너는 포트 25에서 수신 대기
- HAT(모두 수락)에 RELAYLIST에 있는 그룹웨어 서버에 대한 항목 포함
- RAT(로컬 도메인에 대한 메일 수락, 모두 거부)

인터넷 루트 서버 또는 내부 DNS 서버를 사용하도록 DNS 구성 가능

SMTP 경로가 메일을 적절한 그룹웨어 서버로 전달

어플라이언스로 드나드는 해당 서비스에 대해 열리는 방화벽 포트

시스템 설정 준비

프로시저

	명령 또는 동작	목적
단계 **1**	어플라이언스에 연결할 방법을 확인합니다.	어플라이언스에 연결하기 위한 방법 확인, 23 페이지를 참조하십시오.
단계 **2**	네트워크 및 IP 주소 할당을 확인합니다. • 어플라이언스를 이미 네트워크에 연결한 경우 Email Security Appliance의 기본 IP 주소가 네트워크의 다른 IP 주소와 충돌하지 않는지 확인합니다.	확인 어플라이언스에 연결하기 위한 방법 확인, 23 페이지 및 네트워크 및 IP 주소 지정 확인, 24 페이지
단계 **3**	시스템 설정에 대한 정보를 수집합니다.	설정 정보 수집, 25 페이지를 참조하십시오.
단계 **4**	어플라이언스에 대한 최신 제품 릴리스 정보를 검토합니다.	릴리스 정보는 설명서 , 6 페이지의 링크에서 사용할 수 있습니다.
단계 **5**	어플라이언스의 포장을 풀고 랙에 물리적으로 설치한 후 전원을 켭니다.	사용 중인 어플라이언스에 대한 빠른 시작 가이드를 참고하십시오. 이 가이드는 설명서 , 6 페이지의 링크에서 사용할 수 있습니다.

	명령 또는 동작	목적
단계 **6**	CLI(명령줄 인터페이스)를 사용하여 설정 마법사를 실행하려는 경우 CLI에 액세스합니다.	CLI(Command Line Interface) 시스템 설정 마법사 실행, 41 페이지 참조
단계 **7**	웹 인터페이스를 사용하여 설정 마법사를 실행하려는 경우 다음을 수행합니다.	**1.** (가상 어플라이언스에만 해당) 명령줄 인터페이스에 액세스한 후 `interfaceconfig` 명령을 사용하여 HTTP 및/또는 HTTPS를 활성화합니다. **2.** 웹 브라우저를 실행하고 어플라이언스의 IP 주소를 입력합니다.
단계 **8**	가상 Email Security Appliance를 설정하는 경우 가상 어플라이언스 라이선스를 로드합니다.	`loadlicense` 명령을 사용합니다. 자세한 내용은 설명서 , 6 페이지의 링크에서 사용할 수 있는 *Cisco Content Security Virtual Appliance Installation Guide*를 참조해 주십시오.
단계 **9**	시스템에 대한 기본 설정을 구성합니다.	시스템 설정 마법사 사용 , 28 페이지를 참조하십시오.

어플라이언스에 연결하기 위한 방법 확인

현재 환경에서 Email Security Appliance를 성공적으로 설정하려면 Email Security Appliance를 네트워크에 연결하고자 하는 방법에 대한 중요한 네트워크 정보를 네트워크 관리자로부터 수집해야 합니다.

관련 주제

- 어플라이언스에 연결, 23 페이지

어플라이언스에 연결

초기 설정 중에 다음 두 가지 방법 중 하나로 어플라이언스에 연결할 수 있습니다.

표 ***2:*** 어플라이언스에 연결하기 위한 옵션

이더넷	PC와 네트워크 간 그리고 네트워크와 Management 포트 간 이더넷 연결. 출고 시 관리 포트에 할당된 IPv4 주소는 192.168.42.42입니다. 네트워크 구성에서 작동하는 경우 이것이 가장 쉬운 연결 방법입니다.

일련 번호	PC 및 Serial Console 포트 간 시리얼 통신 연결. 이더넷 방법을 사용할 수 없는 경우, 관리 포트에 대체 네트워크 설정을 적용할 수 있을 때까지 컴퓨터와 어플라이언스 간의 직접 시리얼-시리얼 연결이 작동합니다. 핀아웃 정보는 시리얼 연결을 통해 이메일 보안 어플라이언스 액세스, 1203 페이지 항목을 참고하십시오. 시리얼 포트에 대한 통신 설정은 다음과 같습니다. 초당 비트 수: 9600 데이터 비트: 8 패리티: None 정지 비트: 1 플로우 제어: 하드웨어

참고 초기 연결 방법이 최종이 아니라는 점에 유의해 주십시오. 이 프로세스는 초기 구성에만 적용됩니다. 다른 연결 방법을 허용하려면 나중에 네트워크 설정을 변경할 수 있습니다. (자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지를 참조해 주십시오.) 어플라이언스에 대한 액세스 권한이 서로 다른 여러 사용자 계정을 만들 수도 있습니다. (자세한 내용은 사용자 추가 , 897 페이지를 참조하십시오.)

네트워크 및 IP 주소 지정 확인

IPv4 및 IPv6 주소를 모두 사용할 수 있습니다.

Management 및 Data 포트의 기본 IP 주소

관리 포트(C170 및 C190 어플라이언스의 데이터 1 포트)에 사전 구성된 IP 주소는 192.168.42.42입니다.

이메일 수신 및 전달을 위한 네트워크 연결 선택

대부분의 사용자는 Email Security Appliance로부터 두 네트워크에 연결함으로써 어플라이언스에서 두 개의 Data 이더넷 포트를 활용합니다.

- 사설 네트워크는 내부 시스템으로 향하는 메시지를 수락 및 전달합니다.
- 공용 네트워크는 인터넷으로 향하는 메시지를 수락 및 전달합니다.

다른 사용자들은 두 기능을 모두 제공하는 하나의 Data 포트만 사용할 수 있습니다. Management 이더넷 포트는 어떤 기능이든 지원할 수 있지만, 그래픽 사용자 인터페이스 및 커맨드 라인 인터페이스에 액세스하도록 사전 설정되어 있습니다.

논리적 IP 주소를 물리적 이더넷 포트에 바인딩

별도의 리스너 및 별도의 IP 주소를 통해 수신 및 발신 이메일 트래픽을 분리할 수 있습니다. IPv4(Internet Protocol version 4) 및 IPv6(version 6) 주소를 사용할 수 있습니다. 그러나 어플라이언스의 시스템 설정 마법사는 다음의 초기 구성을 지원합니다.

- 별도의 물리적 인터페이스에 구성된 2개의 논리적 IPv4 및 2개의 IPv6 주소의 개별 리스너 2개
  - 수신 및 발신 트래픽 분리
  - 각 리스너에 IPv4 및 IPv6 주소를 각각 하나씩 할당 가능
- 하나의 물리적 인터페이스에 구성된 1개의 논리적 IPv4 주소의 리스너 1개
  - 수신 및 발신 트래픽을 모두 결합
  - 리스너에 IPv4 및 IPv6 주소를 모두 할당 가능

Email Security Appliance는 단일 리스너에서 IPv4 및 IPv6 주소를 모두 지원할 수 있습니다. 리스너는 두 주소의 메일을 모두 수락합니다. 리스너의 모든 설정은 IPv4 및 IPv6 주소에 모두 적용됩니다.

연결을 위한 네트워크 설정 선택

사용하기 위해 선택하는 각 이더넷 포트에 대한 다음 네트워크 정보가 필요합니다.

- IP 주소(IPv4 또는 IPv6 또는 모두)
- CIDR 형식의 IPv4 주소용 넷마스크
- CIDR 형식의 IPv6 주소용 접두사

또한 전체 네트워크에 대한 다음 정보가 필요합니다.

- 네트워크 기본 라우터(게이트웨이)의 IP 주소
- DNS 서버의 IP 주소 및 호스트 이름(인터넷 루트 서버를 사용하려는 경우 필요하지 않음)
- NTP 서버의 호스트 이름 또는 IP 주소(Cisco의 시간 서버를 사용하려는 경우에는 필요 없음)

자세한 내용은 네트워크 및 IP 주소 할당, 1205 페이지를 참조하십시오.

참고 인터넷과 Email Security Appliance 사이에서 네트워크의 방화벽을 실행하려는 경우 어플라이언스가 제대로 작동하도록 하려면 특정 포트를 열어야 할 수 있습니다. 자세한 내용은 방화벽 정보, 1227 페이지를 참조하십시오.

설정 정보 수집

이제 시스템 설정 마법사에서 필요한 옵션을 선택할 때의 요구 사항과 전략을 이해했으니, 다음 표를 사용하여 이 섹션을 읽는 동안 시스템 설정에 대한 정보를 수집해 주십시오.

네트워크 및 IP 주소에 대한 자세한 내용은 네트워크 및 IP 주소 할당, 1205 페이지을 참조해 주십시오. Cisco Content Security Management Appliance를 구성 중인 경우 Cisco Content(M-Series) Security Management Appliance에서 서비스 중앙 집중화, 1187 페이지 항목을 참고하십시오.

표 *3:* 시스템 설정 워크시트*:* 이메일 트래픽 분리를 위한 리스너 *2*개

시스템 설치		
기본 시스템 호스트 이름:		
다음 사용자에게 이메일로 시스템 경고문 보내기:		
예약 보고서 배달 대상:		
표준 시간대 정보:		
NTP 서버:		
관리자 암호:		
SenderBase 네트워크 참여:	활성/비활성	
자동지원:	활성/비활성	
네트워크 통합		
게이트웨이:		
DNS(인터넷 또는 직접 지정):		
인터페이스		
Data 1 포트		
IPv4 주소/넷마스크:		
IPv6 주소/접두사:		
전체(Fully Qualified) 호스트 이름:		
수신 메일 수락:	도메인	대상
발송 메일 중계:	시스템	
Data 2 포트		
IPv4 주소/넷마스크:		
IPv6 주소/접두사:		
전체(Fully Qualified) 호스트 이름:		
수신 메일 수락:	도메인	대상

시스템 설치		
발송 메일 중계:	시스템	
관리 포트		
IP 주소:		
네트워크 마스크:		
IPv6 주소:		
접두사:		
전체(Fully Qualified) 호스트 이름:		
수신 메일 수락:	도메인	대상
발송 메일 중계:	시스템	
메시지 보안		
SenderBase Reputation 필터:	활성/비활성	
안티 스팸 스캔 엔진	없음/IronPort	
McAfee 안티 바이러스 스캔 엔진	활성/비활성	
Sophos 안티 바이러스 스캔 엔진	활성/비활성	
Outbreak Filter	활성/비활성	

표 ***4:*** 시스템 설정 워크시트***:*** 모든 이메일 트래픽을 위한 리스너 ***1***개

시스템 설치		
기본 시스템 호스트 이름:		
다음 사용자에게 이메일로 시스템 경고문 보내기:		
예약 보고서 배달 대상:		
표준 시간대:		
NTP 서버:		
관리자 암호:		
SenderBase 네트워크 참여:	활성/비활성	

시스템 설치		
자동지원:	활성/비활성	
네트워크 통합		
게이트웨이:		
DNS(인터넷 또는 직접 지정):		
인터페이스		
Data2 포트		
IPv4 주소/넷마스크:		
IPv6 주소/접두사:		
전체(Fully Qualified) 호스트 이름:		
수신 메일 수락:	도메인	대상
발송 메일 중계:	시스템	
Data1 포트		
IPv4 주소/넷마스크:		
IPv6 주소/접두사:		
전체(Fully Qualified) 호스트 이름:		
메시지 보안		
SenderBase Reputation 필터:	활성/비활성	
안티 스팸 스캔 엔진	없음/IronPort	
McAfee 안티 바이러스 스캔 엔진	활성/비활성	
Sophos 안티 바이러스 스캔 엔진	활성/비활성	
Outbreak Filter	활성/비활성	

시스템 설정 마법사 사용

• 웹 기반 GUI(그래픽 유저 인터페이스) 액세스, 29 페이지

- 웹 기반 시스템 설정 마법사를 사용하여 기본 구성 정의 , 30 페이지
- Active Directory에 대한 연결 설정, 38 페이지
- 다음 단계로 진행, 39 페이지
- CLI(Command Line Interface)에 액세스, 39 페이지
- CLI(Command Line Interface) 시스템 설정 마법사 실행, 41 페이지
- 시스템을 엔터프라이즈 게이트웨이로 구성 , 55 페이지

완전한 구성을 보장하기 위해 초기 설정에 대해 시스템 설정 마법사를 사용해야 합니다. 나중에 시스템 설정 마법사에서 사용할 수 없는 맞춤형 옵션을 구성할 수 있습니다.

브라우저 또는 CLI(command line interface)를 사용하여 시스템 설정 마법사를 실행할 수 있습니다. 자세한 내용은 웹 기반 GUI(그래픽 유저 인터페이스) 액세스, 29 페이지 또는 CLI(Command Line Interface) 시스템 설정 마법사 실행, 41 페이지 섹션을 참조해 주십시오.

시작하기 전에 시스템 설정 준비, 22 페이지에 나와 있는 전제 조건을 완료해 주십시오.

주의 가상 Email Security Appliance를 설정하는 경우 시스템 설정 마법사를 실행하기 전에 loadlicense 명령을 사용하여 가상 어플라이언스 라이선스를 로드해야 합니다. 자세한 내용은 *Cisco Content Security Virtual Appliance Installation Guide*를 참조해 주십시오.

주의 시스템 설정 마법사는 시스템을 완전히 재구성합니다. 어플라이언스를 처음 설치할 때 또는 기존 구성을 완전히 덮어쓰고자 할 때에만 시스템 설정 마법사를 사용해야 합니다.

주의 Email Security Appliance는 모든 하드웨어의 Management 포트에서 기본 IP 주소가 192.168.42.42인 상태로 제공됩니다. 단, C170 및 C190 어플라이언스에서는 Data 1 포트가 대신 사용됩니다. 어플라이언스를 네트워크에 연결하기 전에 이 공장 기본 설정과 충돌하는 다른 장비의 IP 주소가 없는지 확인해 주십시오. Cisco Content Security Management Appliance를 구성 중인 경우 Cisco Content(M-Series) Security Management Appliance에서 서비스 중앙 집중화, 1187 페이지 항목을 참고하십시오.

네트워크에 여러 개의 공장 구성 Content Security Appliance를 연결 중인 경우, 한 번에 하나씩 각 어플라이언스의 기본 IP 주소를 재구성해 주십시오.

웹 기반 GUI(그래픽 유저 인터페이스) 액세스

웹 기반 GUI(Graphical User Interface)에 액세스하려면 웹 브라우저를 열고 192.168.42.42를 가리킵니다.

관련 주제

- 공장 기본 사용자 이름 및 암호, 30 페이지

공장 기본 사용자 이름 및 암호

새 가상 또는 하드웨어 어플라이언스를 설치하는 경우 어플라이언스 설정에 대한 모든 권한을 얻으려면 기본 암호를 변경해야 합니다. 처음으로 어플라이언스에 로그인하면 웹 인터페이스에서 기본 암호를 변경하라는 메시지를 표시하며, 기본 암호를 변경할 때까지 CLI는 다음 명령에 대한 액세스를 제한합니다.

- 커밋
- Interfaceconfig
- passphrase
- Loadconfig
- Systemsetup
- loadlicense(가상 어플라이언스용)
- 기능 키
- Ping
- Telnet
- netstat

- 사용자 이름: **admin**
- 암호: **ironport**

예를 들면 다음과 같습니다.

```
login: admin
passphrase: ironport
```

참고 세션이 시간 초과되면 사용자 이름과 암호를 다시 입력하라는 메시지가 표시됩니다. 시스템 설정 마법사를 실행하는 동안 세션이 시간 초과되면 처음부터 다시 시작해야 합니다.

웹 기반 시스템 설정 마법사를 사용하여 기본 구성 정의

단계 **1** 시스템 설정 마법사 구동

- 웹 기반 GUI(그래픽 유저 인터페이스) 액세스, 29 페이지에 설명한 대로 GUI에 로그인합니다.
- 이전 AsyncOS 릴리스에서 업데이트하지 않은 새로운 시스템의 경우 브라우저에 시스템 설정 마법사가 자동으로 표시됩니다.
- 그렇지 않은 경우 System Administration(시스템 관리) 탭의 왼쪽 링크 리스트에서 System Setup Wizard(시스템 설정 마법사)를 클릭합니다.

단계 **2** 시작. 1단계: 시작, 31 페이지을 참조하십시오.

- 라이선스 계약을 읽고 그 내용에 동의합니다.

단계 **3** 시스템. 2단계: 시스템, 31 페이지을 참조하십시오.

- 어플라이언스의 호스트 이름 설정
- 경고문 설정, 보고서 전달 설정 및 AutoSupport 구성
- 시스템 시간 설정과 NTP 서버 설정
- 관리자 암호 재설정
- SenderBase 네트워크 참여 활성화

단계 **4** 네트워크. 3단계: 네트워크, 33 페이지를 참조하십시오.

- 기본 라우터 및 DNS 설정 정의
- 네트워크 인터페이스 활성화 및 구성: 수신 메일 구성(인바운드 리스너), SMTP 경로 정의(선택 사항), 발신 메일 구성(아웃바운드 리스너) 및 어플라이언스를 통해 메일을 릴레이할 수 있는 시스템 정의(선택 사항) 포함

단계 **5** 보안. 4단계: 보안, 37 페이지을 참조해 주십시오.

- SenderBase Reputation Filtering 활성화
- 안티스팸 서비스 활성화
- 스팸 격리 활성화
- 안티바이러스 서비스 활성화
- Advanced Malware Protection 활성화(파일 평판 및 분석 서비스)
- Outbreak Filter 서비스 활성화

단계 **6** 검토. 5단계: 검토, 38 페이지를 참조하십시오.

- 설정 검토 및 구성 설치
- 프로세스 끝에 변경 사항을 커밋하라는

단계 **7** 프롬프트가 표시됩니다.

커밋할 때까지는 변경 사항이 적용되지 않습니다.

1단계: 시작

라이선스 계약을 읽는 것으로 시작합니다. 라이선스 계약을 읽고 내용에 동의하면 동의를 나타내는 확인란을 선택하고 **Begin Setup(**설정 시작**)**을 클릭하여 계속 진행합니다.

계약서 내용은 https://support.ironport.com/license/eula.html에서 확인할 수 있습니다.

2단계: 시스템

- 호스트 이름 설정, 32 페이지
- 시스템 경고문 구성, 32 페이지
- 보고서 전달 구성, 32 페이지

호스트 이름 설정

Email Security Appliance에 대한 인증된 호스트 이름을 정의합니다. 네트워크 관리자가 이 이름을 할당해야 합니다.

시스템 경고문 구성

사용자 개입이 필요한 시스템 오류가 발생하면 Cisco AsyncOS는 이메일을 통해 경고문 메시지를 전송합니다. 그러한 경고문을 전송하기 위한 이메일 주소를 입력합니다.

시스템 경고문을 수신할 이메일 주소를 하나 이상 추가해야 합니다. 단일 이메일 주소를 입력하거나, 여러 주소를 쉼표로 구분하여 입력합니다. 이메일 수신자는 DHAP(Directory Harvest Attack Prevention) 경고문을 제외하고, 처음에 모든 레벨에서 모든 유형의 경고문을 수신합니다. 나중에 경고문 구성을 더 세부적으로 조정할 수 있습니다. 자세한 내용은 알림, 962 페이지를 참고하십시오.

보고서 전달 구성

기본 예약된 보고서를 전송하기 위한 주소를 입력합니다. 이 값을 비워두는 경우 예약된 보고서는 여전히 실행되지만, 전달되는 대신 어플라이언스에 보관됩니다.

시간 설정

메시지 헤더와 로그 파일의 타임스탬프가 정확하도록 Email Security Appliance의 표준 시간대를 설정합니다. 드롭다운 메뉴를 사용하여 표준 시간대를 찾거나 GMT 오프셋을 통해 표준 시간대를 정의합니다(자세한 내용은 GMT 차감 시간 선택, 991 페이지 참조).

나중에 시스템 시계 시간을 수동으로 설정하거나, NTP(Network Time Protocol)를 사용하여 네트워크의 다른 서버 또는 인터넷과 시간을 동기화합니다. 기본적으로 어플라이언스의 시간을 동기화하기 위한 Cisco Systems 시간 서버의 한 항목(**`time.ironport.com`**)은 이미 구성되어 있습니다.

암호 설정

관리자 계정의 암호를 설정합니다. 이는 필수 단계입니다. Cisco AsyncOS 관리자 계정의 암호를 변경하는 경우 새 암호는 6자 이상이어야 합니다. 암호는 안전한 장소에 보관해야 합니다.

SenderBase 네트워크에 참여

SenderBase는 이메일 관리자가 발신자를 조사하고 이메일의 합법적인 소스를 식별하고 스패머를 차단하도록 지원하기 위해 설계된 이메일 평가 서비스입니다.

SenderBase 네트워크 참여에 동의할 경우 Cisco는 조직에 대한 집계된 이메일 트래픽 통계를 수집합니다. 여기에는 Email Security Appliance에서의 서로 다른 유형의 메시지 처리 방식에 대한 정보 및 메시지 특성에 대한 요약 데이터만 포함됩니다. 예를 들어 Cisco는 메시지 본문이나 메시지 제목은 수집하지 않습니다. 개인 식별이 가능한 정보 및 조직을 식별하는 정보는 기밀이 유지됩니다. 수집되는 데이터를 포함하여 SenderBase에 대해 자세히 알아보려면 **Click here for more information about what**

data is being shared(공유되는 데이터에 대해 자세히 알아보려면 여기 클릭)… 링크를 참조해 주십시오(FAQ(자주 묻는 질문), 1030 페이지 참조).

SenderBase 네트워크에 참여하려면 "Allow IronPort to gather anonymous statistics on email and report them to SenderBase in order to identify and stop email-based threats(IronPort에서 이메일에 대한 익명의 통계를 수집하고 이메일 기반 위협의 식별 및 중단을 위해 SenderBase에 보고하도록 허용)" 옆에 있는 확인란을 선택하고 **Accept**(수락)를 클릭합니다.

자세한 내용은 SenderBase 네트워크 참여, 1029 페이지를 참조하십시오.

AutoSupport 활성화

AutoSupport 기능(기본적으로 활성화됨)은 사용자를 더 잘 지원할 수 있도록 어플라이언스의 문제를 Cisco 고객 지원팀에 지속적으로 알려줍니다. (자세한 내용은 AutoSupport, 963 페이지를 참조하십시오.)

Next(다음)를 클릭하여 계속합니다.

3단계: 네트워크

3단계에서는 기본 라우터(게이트웨이)를 정의하고 DNS 설정을 구성한 다음, Data 1, Data 2 및 Management 인터페이스를 구성하여 이메일을 수신 및/또는 릴레이하도록 어플라이언스를 설정합니다.

- DNS 및 기본 게이트웨이 구성, 33 페이지
- 네트워크 인터페이스 구성, 34 페이지
- 메일 수락, 34 페이지
- 메일 릴레이(선택 사항), 35 페이지
- C170 및 C190 설치, 36 페이지

DNS 및 기본 게이트웨이 구성

네트워크에서 기본 라우터(게이트웨이)의 IP 주소를 입력합니다. IPv4 주소, IPv6 주소 또는 둘 다를 사용할 수 있습니다.

그런 다음, DNS(Domain Name Service) 설정을 구성합니다. AsyncOS는 인터넷의 루트 서버에 직접 쿼리할 수 있는 고성능 내부 DNS 확인자/캐시를 포함합니다. 또는 시스템에서 사용자가 지정한 DNS 서버를 사용할 수 있습니다. 자신의 서버를 사용하도록 선택하는 경우 각 DNS 서버의 IP 주소와 호스트 이름을 제공해야 합니다. 시스템 설정 마법사를 통해 최대 4개의 DNS 서버를 입력할 수 있습니다. 직접 입력하는 DNS 서버의 초기 우선 순위는 0입니다. 자세한 내용은 DNS(Domain Name System) 설정 구성, 986 페이지를 참고해 주십시오.

참고 어플라이언스는 수신 연결에 대한 DNS 조회를 수행하기 위해 작동 중인 DNS 서버에 액세스해야 합니다. 어플라이언스 설정 중에 어플라이언스에서 도달할 수 있는 작동 중인 DNS 서버를 지정할 수 없는 경우 해결책은 "Use Internet Root DNS Servers(인터넷 루트 DNS 서버 사용)"를 선택하거나, 시스템 설정 마법사를 완료할 수 있도록 일시적으로 Management 인터페이스의 IP 주소를 지정하는 것입니다.

네트워크 인터페이스 구성

Email Security Appliance에는 시스템의 물리적 이더넷 포트와 연결된 네트워크 인터페이스가 있습니다.

인터페이스를 사용하려면 "Enable(활성화)" 확인란을 선택한 다음 IP 주소, 네트워크 마스크 및 인증된 호스트 이름을 지정합니다. 입력하는 IP 주소는 DNS 기록에 반영된 인바운드 메일에 대한 주소여야 합니다. 일반적으로 이 주소는 MX 기록이 DNS와 연결되어 있습니다. IPv4 주소, IPv6 주소 또는 둘 다를 사용할 수 있습니다. 둘 다 사용하는 경우 인터페이스에서 두 가지 연결 유형을 모두 수락합니다.

이메일을 수락(수신)하거나, 릴레이(발신)하거나, 어플라이언스를 관리하도록 각 인터페이스를 구성할 수 있습니다. 설정 중에는 각각 하나로 제한됩니다. 대부분의 어플라이언스에서는 인터페이스를 수신, 발신 및 어플라이언스 관리에 각각 하나씩 사용합니다. C170 및 C190 어플라이언스에서는 인터페이스를 수신 및 발신 메일에 하나 그리고 관리에 다른 하나를 사용합니다.

이메일 수신을 위한 인터페이스를 반드시 구성해야 합니다.

어플라이언스에서 물리적 이더넷 인터페이스 중 하나에 논리적 IP 주소를 할당하여 구성합니다. Data 1 이더넷 포트 및 Data 2 이더넷 포트를 모두 사용하려는 경우 두 가지 연결을 위해 이 정보가 필요합니다.

C370, C670, X1070, C380, C680, C390 및 **C690** 어플라이언스의 경우: 물리적 이더넷 포트 중 하나는 퍼블릭 리스너를 통해 인바운드 이메일을 수신하기 위해 인터넷에 직접 연결하는 데 사용하고, 또 다른 물리적 이더넷 포트는 프라이빗 리스너를 통해 아웃바운드 이메일을 릴레이하기 위해 내부 네트워크에 직접 연결하는 데 사용하는 것이 좋습니다.

C170 및 **C190** 어플라이언스의 경우: 일반적으로 시스템 설정 마법사는 1개의 리스너를 통해 인바운드 이메일을 수신하고 아웃바운드 이메일을 전달하는 물리적 이더넷 포트를 1개만 구성합니다.

논리적 IP 주소를 물리적 이더넷 포트에 바인딩, 25 페이지를 참조하십시오.

다음 정보가 필요합니다.

- 네트워크 관리자가 할당한 **IP** 주소. IPv4 주소, IPv6 주소 또는 둘 다일 수 있습니다.
- IPv4 주소의 경우: 인터페이스의 넷마스크. AsyncOS에서는 CIDR 형식의 넷마스크만 사용할 수 있습니다. 예: `255.255.255.0` 서브넷에 대해 `/24`.

  IPv6 주소의 경우: CIDR 형식의 접두사. 예: 64비트 접두사에 대해 `/64`.
- (선택 사항) IP 주소에 대한 인증된 호스트 이름.

참고 동일한 서브넷 내의 IP 주소는 별도의 물리적 이더넷 인터페이스에서 구성할 수 없습니다. 네트워크 및 IP 주소 컨피그레이션에 대한 자세한 내용은 네트워크 및 IP 주소 할당, 1205 페이지을 참조해 주십시오.

메일 수락

메일 수락을 위한 인터페이스를 구성할 때 다음을 정의합니다.

- 메일을 수락할 도메인

- 각 도메인의 대상(SMTP 경로)(선택 사항)

메일을 수락하기 위한 인터페이스를 구성하려면 Accept Incoming Mail(수신 메일 수락) 확인란을 선택합니다. 메일을 수신할 도메인의 이름을 입력합니다.

Destination(대상)을 입력합니다. 이것은 SMTP 경로 또는 지정한 도메인에 대한 이메일을 라우팅할 시스템의 이름입니다.

이것은 첫 번째 SMTP 경로 항목입니다. SMTP 경로 테이블에서는 각 도메인(RAT(Recipient Access Table) 항목으로도 알려짐)에 대한 모든 이메일을 지정된 MX(mail exchange) 호스트로 리디렉션할 수 있습니다. 일반적인 설치에서 SMTP 경로 테이블은 특정 그룹웨어(예: Microsoft Exchange) 서버 또는 인프라의 이메일 전달에서 "다음 홉"을 정의합니다.

예를 들어, 도메인 `example.com`과 `.example.com`의 모든 하위 도메인에 대해 허용되는 메일이 그룹웨어 서버 `exchange.example.com`으로 라우팅되도록 지정하는 경로를 정의할 수 있습니다.

여러 도메인 또는 대상을 입력할 수 있습니다. 또 다른 도메인을 추가하려면 **Add Row(**행 추가**)**를 클릭합니다. 행을 제거하려면 휴지통 아이콘을 클릭합니다.

참고 이 단계에서 SMTP 경로를 구성하는 것은 선택 사항입니다. SMTP 경로가 정의되어 있지 않으면 시스템은 리스너에서 수신하는 메일의 전달 호스트를 조회 및 확인하기 위해 DNS를 사용합니다. (로컬 도메인용 이메일 라우팅, 665 페이지 참조)

Recipient Access Table에 하나 이상의 도메인을 추가해야 합니다. 도메인을 입력합니다(예: `example.com`). `example.net`의 하위 도메인으로 전송될 메일이 Recipient Access Table에서 일치하도록 보장하려면 도메인 이름과 함께 `.example.net`을 입력합니다. 자세한 내용은 수신자 주소 정의, 132 페이지를 참고하십시오.

메일 릴레이(선택 사항)

메일을 릴레이하기 위해 인터페이스를 구성할 때 어플라이언스를 통해 이메일을 릴레이할 수 있는 시스템을 정의합니다.

이러한 시스템은 리스너에 대한 Host Access Table의 RELAYLIST에 있는 항목입니다. 자세한 내용은 발신자 그룹 구문, 96 페이지를 참조해 주십시오.

메일을 릴레이할 인터페이스를 구성하려면 Relay Outgoing Mail(발신 메일 릴레이) 확인란을 선택합니다. 어플라이언스를 통해 메일을 릴레이할 수 있는 호스트를 입력합니다.

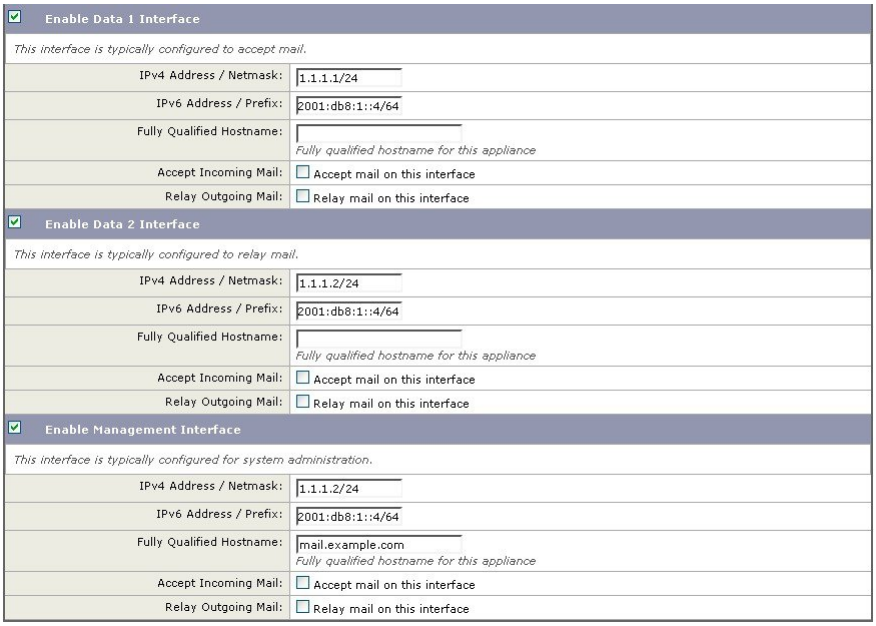
아웃바운드 메일을 릴레이할 인터페이스를 구성할 때, 인터페이스를 사용할 퍼블릭 리스너가 구성되어 있지 않으면 시스템 설정 마법사는 인터페이스에 대한 SSH를 켭니다.

다음 예에서는 IPv4 주소의 두 인터페이스가 생성됩니다.

- 192.168.42.42는 Management 인터페이스에서 구성된 상태로 유지됩니다.
- 192.168.1.1은 Data 1 이더넷 인터페이스에서 활성화됩니다. 이 주소는 .example.com으로 끝나는 도메인에 대한 메일을 수락하도록 구성되며, SMTP 경로가 exchange.example.com에 대해 정의됩니다.
- 192.168.2.1은 Data 1 이더넷 인터페이스에서 활성화됩니다. 이 주소는 exchange.example.com에서 오는 메일을 릴레이하도록 구성됩니다.

C370, C670, X1070, C380, C680, C390 및 C690 설치

그림 *3:* 네트워크 인터페이스*: Management* 외에 *2*개의 인터페이스*(*분리된 트래픽*)*

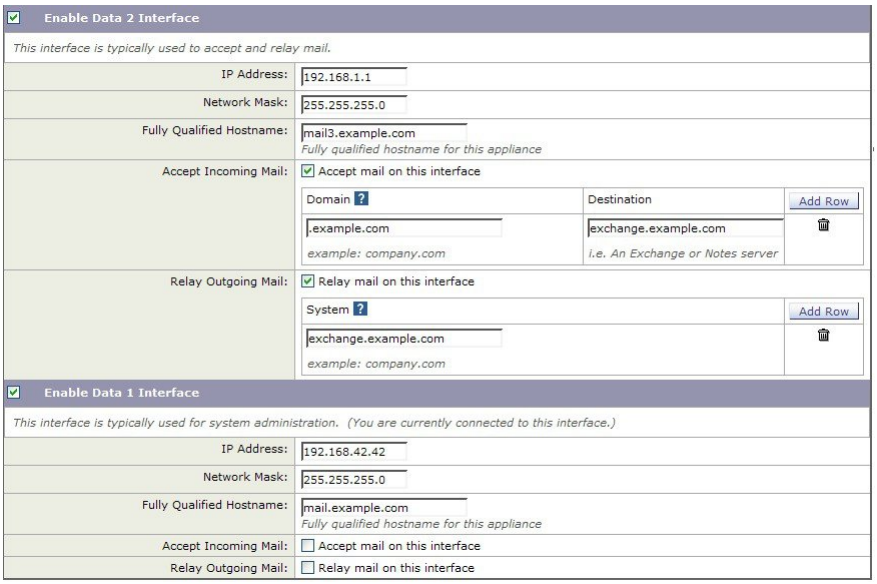


C170 및 C190 설치

C170 및 C190 어플라이언스의 경우, Data 1 인터페이스는 어플라이언스 관리에 사용되는 반면 Data 2 인터페이스는 일반적으로 수신 및 발신 메일 모두에 대해 구성됩니다.

모든 이메일 트래픽에 대해 단일 IP 주소를 구성하는 경우(분리되지 않은 트래픽), 시스템 설정 마법사의 3단계는 다음과 같습니다.

그림 *4:* 네트워크 인터페이스*:*수신 및 발신*(*분리되지 않음*)* 트래픽용 *IP* 주소 *1*개



Next(다음**)**를 클릭하여 계속합니다.

4단계: 보안

4단계에서는 안티 스팸 및 안티바이러스 설정을 구성합니다. 안티 스팸 옵션에는 SenderBase Reputation Filtering 및 안티 스팸 검사 엔진 선택이 포함됩니다. 안티바이러스의 경우 Outbreak Filter나 Sophos 또는 McAfee 안티바이러스 검사를 활성화할 수 있습니다.

- SenderBase Reputation Filtering 활성화, 37 페이지
- 안티 스팸 검사 활성화, 37 페이지
- 안티바이러스 검사 활성화, 37 페이지
- Advanced Malware Protection 활성화(파일 평판 및 분석 서비스) , 38 페이지
- Outbreak Filter 활성화, 38 페이지

SenderBase Reputation Filtering 활성화

SenderBase Reputation Service는 독립적인 안티스팸 솔루션으로 사용할 수도 있지만, Anti-Spam과 같은 콘텐츠 기반 안티스팸 시스템의 효과를 높이는 것이 기본 설계 목표입니다.

SenderBase Reputation Service(http://www.senderbase.org)는 원격 호스트의 연결 IP 주소를 기반으로 의심스런 스팸을 거부 또는 조절(throttle)하기 위한 정확하고 유연한 방법을 사용자에게 제공합니다. SenderBase Reputation Service는 특정 소스에서 온 메시지가 스팸일 가능성을 기반으로 점수를 반환합니다. SenderBase Reputation Service는 이메일 메시지 볼륨의 전역 보기를 제공하고, 관련된 이메일 소스를 쉽게 식별 및 그룹화하는 방식으로 데이터를 구성한다는 점에서 고유합니다. Cisco는 SenderBase Reputation Filtering을 활성화할 것을 적극 제안합니다.

활성화되면 SenderBase Reputation Filtering은 수신(수락) 리스너에서 적용됩니다.

안티 스팸 검사 활성화

어플라이언스는 안티 스팸 소프트웨어에 대한 30일 평가 키와 함께 제공될 수 있습니다. 시스템 설정 마법사의 이 부분 중에 어플라이언스에서 Anti-Spam을 전역적으로 활성화하도록 선택할 수 있습니다. 이 서비스를 활성화하지 않을 수도 있습니다.

안티스팸 서비스를 활성화하기로 선택한 경우, 스팸 및 의심스런 스팸 메시지를 로컬 스팸 격리로 전송하도록 AsyncOS를 구성할 수 있습니다. 스팸 격리는 어플라이언스에 대한 최종 사용자 격리 역할을 합니다. 최종 사용자 액세스가 구성될 때까지는 관리자만 격리에 액세스할 수 있습니다.

어플라이언스에서 사용 가능한 모든 안티스팸 구성 옵션은 Anti-Spam, 355 페이지을 참조해 주십시오. 정책, 바이러스, 보안 침해 격리, 847 페이지를 참조하십시오.

안티바이러스 검사 활성화

어플라이언스는 Sophos Anti-Virus 또는 McAfee Anti-Virus 검사 엔진에 대한 30일 평가 키와 함께 제공될 수 있습니다. 시스템 설정 마법사의 이 부분 중에 어플라이언스에서 안티바이러스 검사 엔진을 전역적으로 활성화하도록 선택할 수 있습니다.

안티바이러스 검사 엔진을 활성화하기로 선택하는 경우 기본 수신 및 기본 발신 메일 정책 모두에 대해 활성화됩니다. 어플라이언스는 메일에서 바이러스를 검사하지만 감염된 첨부 파일을 복구하지는 않습니다. 어플라이언스는 감염된 메시지를 삭제합니다.

어플라이언스에서 사용 가능한 모든 안티바이러스 구성 옵션은 Anti-Virus, 335 페이지를 참조해 주십시오.

Advanced Malware Protection 활성화(파일 평판 및 분석 서비스)

Advanced Malware Protection은 클라우드 기반 서비스로부터 첨부 파일에 대한 평판 정보를 가져옵니다.

자세한 내용은 File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석), 461 페이지을 참조해 주십시오.

Outbreak Filter 활성화

어플라이언스는 Outbreak Filter에 대한 30일 평가 키와 함께 제공될 수 있습니다. Outbreak Filter는 기존의 안티바이러스 보안 서비스를 신종 서명 파일로 업데이트할 수 있을 때까지 의심스런 메시지를 격리하여 신종 바이러스 전파 확산에 대한 "제1 방어선"을 제공합니다.

자세한 내용은 신종 바이러스 필터(Outbreak Filter), 399 페이지를 참조해 주십시오.

Next(다음)를 클릭하여 계속합니다.

5단계: 검토

컨피그레이션 정보의 요약이 표시됩니다. **Previous(이전)** 버튼을 클릭하거나 각 섹션 우측 상단에 있는 해당 **Edit(수정)** 링크를 클릭하여 System Settings(시스템 설정), Network Integration(네트워크 통합) 및 Message Security(메시지 보안) 정보를 수정할 수 있습니다. 변경을 위해 특정 단계로 돌아가는 경우, 검토 페이지에 다시 도달할 때까지 나머지 단계를 다시 진행해야 합니다. 이전에 입력한 모든 설정이 기억됩니다.

표시된 정보에 만족하면 **Install This Configuration(이 컨피그레이션 설치)**을 클릭합니다.

확인 대화 상자가 표시됩니다. **Install(설치)**을 클릭하여 새 컨피그레이션을 설치합니다.

이제 어플라이언스에서 이메일을 전송할 준비가 되었습니다.

참고 어플라이언스에 연결하는 데 사용하던 인터페이스(C370, C670, X1070, C380, C680, C390 및 C690 어플라이언스의 Management 인터페이스, 또는 C170 및 C190 어플라이언스의 Data 1 인터페이스)의 IP 주소를 기본값에서 변경한 경우 **Install(설치)**을 클릭하면 현재 URL(http://192.168.42.42)에 대한 연결이 손실됩니다. 그러나 브라우저는 새 IP 주소로 리디렉션됩니다.

시스템 설정이 완료되면 몇 가지 경고문 메시지가 전송됩니다. 자세한 내용은 즉각 경고문, 54 페이지를 참조하십시오.

Active Directory에 대한 연결 설정

시스템 설정 마법사가 Email Security Appliance에 컨피그레이션을 제대로 설치하면 Active Directory 마법사가 나타납니다. 네트워크에서 Active Directory 서버를 실행하는 경우, Active Directory 마법사를 사용하여 Active Directory 서버용 LDAP 서버 프로필을 구성하고 수신자 확인용 리스너를 할당합

니다. Active Directory를 사용하고 있지 않거나 나중에 구성하려는 경우 Skip this Step(이 단계 건너뛰기)을 클릭합니다. **System Administration(**시스템 관리**) > Active Directory Wizard(Active Directory** 마법사**)** 페이지에서 Active Directory 마법사를 실행할 수 있습니다. **System Administration(**시스템 관리**) > LDAP** 페이지에서 Active Directory 및 기타 LDAP 프로필을 구성할 수도 있습니다.

Active Directory 마법사는 LDAP 서버 프로필을 만드는 데 필요한 시스템 정보(예: 인증 방법, 포트, 기본 DN, SSL 지원 여부)를 검색합니다. Active Directory 마법사는 또한 LDAP 서버 프로필에 대한 LDAP 수락 및 그룹 쿼리를 만듭니다.

Active Directory 마법사가 LDAP 서버 프로파일을 생성한 후 **System Administration(**시스템 관리**) > LDAP** 페이지를 사용하여 새 프로파일을 보고 추가 변경을 수행할 수 있습니다

단계 **1** Active Directory 마법사 페이지에서 **Run Active Directory Wizard(Active Directory** 마법사 실행**)**를 클릭합니다.

단계 **2** Active Directory 서버의 호스트 이름을 입력합니다.

단계 **3** 인증 요청을 위한 사용자 이름 및 암호를 입력합니다.

단계 **4** **Next(**다음**)**를 클릭하여 작업을 계속합니다.

Active Directory 마법사는 Active Directory 서버에 대한 연결을 테스트합니다. 성공적이면 Test Directory Settings(디렉터리 설정 테스트) 페이지가 표시됩니다.

단계 **5** Active Directory에 있는 알고 있는 이메일 주소를 입력하고 **Test(**테스트**)**를 클릭하여 디렉터리 설정을 테스트합니다. 연결 상태 필드에 결과가 나타납니다.

단계 **6** **Done(**완료**)**을 클릭합니다.

다음 단계로 진행

Active Directory 마법사와 작동하도록 어플라이언스를 성공적으로 구성하거나 이 프로세스를 건너뛰면 System Setup Next Steps(시스템 설정 다음 단계) 페이지가 나타납니다.

어플라이언스의 컨피그레이션을 계속 진행하려면 System Setup Next Steps(시스템 설정 다음 단계) 페이지에서 링크를 클릭합니다.

CLI(Command Line Interface)에 액세스

CLI에 대한 액세스는 어플라이언스에 연결, 23 페이지에서 선택한 관리 연결 방법에 따라 달라집니다. 공장 기본 사용자 이름 및 암호가 다음에 나열됩니다. 처음에는 관리자 사용자 계정만 CLI에 액세스할 수 있습니다. 관리자 계정을 통해 커맨드 라인 인터페이스에 처음 액세스한 후에는 서로 다른 권한 레벨의 사용자를 추가할 수 있습니다. (사용자 추가에 대한 자세한 내용은 사용자 추가 , 897 페이지 섹션을 참조해 주십시오.) 시스템 설정 마법사에서 관리자 어카운트의 암호를 변경하라는 메시지를 표시합니다. 관리자 어카운트의 암호는 `passphrase` 명령을 사용하여 언제든지 직접 재설정할 수도 있습니다.

이더넷을 통해 연결: 공장 기본 IP 주소인 192.168.42.42로 SSH 세션을 시작합니다. SSH는 포트 22를 사용하도록 구성되어 있습니다. 아래의 사용자 이름 및 암호를 입력합니다.

시리얼 연결을 통해 연결: 시리얼 케이블이 연결된 PC의 통신 포트로 터미널 세션을 시작합니다. 어플라이언스에 연결, 23 페이지에 소개된 시리얼 포트의 설정을 사용합니다. 아래의 사용자 이름 및 암호를 입력합니다.

사용자 이름 및 암호를 입력하여 어플라이언스에 로그인합니다.

관련 주제

- 공장 기본 사용자 이름 및 암호, 30 페이지

공장 기본 사용자 이름 및 암호

새 가상 또는 하드웨어 어플라이언스를 설치하는 경우 어플라이언스 설정에 대한 모든 권한을 얻으려면 기본 암호를 변경해야 합니다. 처음으로 어플라이언스에 로그인하면 웹 인터페이스에서 기본 암호를 변경하라는 메시지를 표시하며, 기본 암호를 변경할 때까지 CLI는 다음 명령에 대한 액세스를 제한합니다.

- 커밋
- Interfaceconfig
- passphrase
- Loadconfig
- Systemsetup
- loadlicense(가상 어플라이언스용)
- 기능 키
- Ping
- Telnet
- netstat

- 사용자 이름: **admin**
- 암호: **ironport**

예를 들면 다음과 같습니다.

```
login: admin
passphrase: ironport
```

참고 세션이 시간 초과되면 사용자 이름과 암호를 다시 입력하라는 메시지가 표시됩니다. 시스템 설정 마법사를 실행하는 동안 세션이 시간 초과되면 처음부터 다시 시작해야 합니다.

CLI(Command Line Interface) 시스템 설정 마법사 실행

시스템 설정 마법사의 CLI 버전은 몇 가지 사소한 점을 제외하면 GUI 버전 단계와 유사합니다.

- CLI 버전에는 웹 인터페이스 활성화를 위한 프롬프트가 포함됩니다.
- CLI 버전에서는 사용자가 만드는 각 리스너에 대해 기본 메일 플로우 정책을 수정할 수 있습니다.
- CLI 버전에는 전역 안티바이러스 및 Outbreak Filter 보안 설정 구성을 위한 프롬프트가 포함되어 있습니다.
- CLI 버전은 시스템 설정이 완료된 후 LDAP 프로필을 만들기 위한 프롬프트를 표시하지 않습니다. LDAP 프로필을 만들려면 `ldapconfig` 명령을 사용해 주십시오.

시스템 설정 마법사를 실행하려면 명령 프롬프트에서 `systemsetup`을 입력합니다.

```
IronPort> systemsetup
```

시스템 설정 마법사는 시스템이 재구성된다는 경고를 표시합니다. 어플라이언스를 처음 설치하는 경우 또는 기존 컨피그레이션을 완전히 덮어쓰려는 경우 질문에 "Yes"(예)로 답하십시오.

```
WARNING: The system setup wizard will completely delete any existing

'listeners' and all associated settings including the 'Host Access Table' -
mail operations may be interrupted.


Are you sure you wish to continue? [Y]> Y
```

참고 시스템 설정 단계 나머지는 아래에서 설명합니다. 웹 기반 시스템 설정 마법사를 사용하여 기본 구성 정의 , 30 페이지에 설명되어 있는 GUI 시스템 설정 마법사와 다른 섹션에 대해서만 CLI 시스템 설정 마법사 대화 상자의 예가 포함됩니다.

관련 주제

- 관리자 암호 변경, 42 페이지
- 라이선스 계약 동의, 42 페이지
- 호스트 이름 설정 , 42 페이지
- 논리 IP 인터페이스 지정 및 구성, 42 페이지
- 기본 게이트웨이 지정, 43 페이지
- 웹 인터페이스 활성화, 43 페이지
- DNS 설정 구성, 43 페이지
- 리스너 만들기, 44 페이지
- Anti-Spam 활성화, 51 페이지
- 기본 안티 스팸 스캐닝 엔진 선택, 52 페이지
- 스팸 격리 활성화, 52 페이지

관리자 암호 변경

먼저 AsyncOS 관리자 어카운트의 암호를 변경합니다. 계속하려면 이전 암호를 입력해야 합니다. 새 암호는 6자 이상이어야 합니다. 암호는 안전한 장소에 보관해야 합니다. 암호 변경 사항은 시스템 설정 프로세스가 완료된 후 적용됩니다.

라이선스 계약 동의

표시되는 소프트웨어 라이선스 계약을 읽고 그 내용에 동의합니다.

호스트 이름 설정

이제 Email Security Appliance에 대한 인증된 호스트 이름을 정의합니다. 네트워크 관리자가 이 이름을 할당해야 합니다.

논리 IP 인터페이스 지정 및 구성

이번에는 Management(C370, C670, X1070, C380, C680, C390 및 C690 어플라이언스) 또는 Data 1(C170 및 C190 어플라이언스)이라는 이름의 물리적 이더넷 인터페이스에서 논리적 IP 인터페이스를 할당 및 구성합니다. 그러면 어플라이언스에서 사용 가능한 다른 물리적 이더넷 인터페이스에서 논리적 IP 인터페이스를 구성하라는 프롬프트가 표시됩니다.

각 이더넷 인터페이스에는 여러 IP 인터페이스를 할당할 수 있습니다. IP 인터페이스는 IP 주소와 호스트 이름을 물리적 이더넷 인터페이스와 연결하는 논리적 구조입니다. Data 1 및 Data 2 이더넷 포트를 모두 사용하기로 한 경우 두 연결을 위한 IP 주소 및 호스트 이름이 필요합니다.

C370, C670, X1070, C380, C680, C390 및 **C690** 어플라이언스의 경우: 물리적 이더넷 포트 중 하나는 퍼블릭 리스너를 통해 인바운드 이메일을 수신하기 위해 인터넷에 직접 연결하는 데 사용하고, 또 다른 물리적 이더넷 포트는 프라이빗 리스너를 통해 아웃바운드 이메일을 릴레이하기 위해 내부 네트워크에 직접 연결하는 데 사용하는 것이 좋습니다.

C170 및 **C190** 어플라이언스의 경우: 기본적으로 `systemsetup` 명령은 1개의 리스너를 통해 인바운드 이메일을 수신하고 아웃바운드 이메일을 전달하는 물리적 이더넷 포트를 1개만 구성합니다.

참고 아웃바운드 메일을 릴레이할 인터페이스를 구성할 때, 인터페이스를 사용할 퍼블릭 리스너가 구성되어 있지 않으면 시스템은 인터페이스에 대한 SSH를 켭니다.

다음 정보가 필요합니다.

- 나중에 IP 인터페이스를 가리키기 위해 만드는 이름(별칭). 예를 들어 사설 네트워크에 이더넷 포트 하나를 사용하고 공용 네트워크에 다른 하나를 사용하려는 경우 이름을 각각 PrivateNet과 PublicNet으로 지정할 수 있습니다.

참고 인터페이스에 대해 정의하는 이름은 대/소문자를 구분합니다. AsyncOS에서는 두 개의 동일한 인터페이스 이름이 허용되지 않습니다. 예를 들어 **Privatenet** 및 **PrivateNet** 이름은 두 개의 서로 다른(고유한) 이름으로 간주됩니다.

- 네트워크 관리자가 할당한 **IP** 주소. IPv4 또는 IPv6 주소일 수 있으며, 단일 IP 인터페이스에 두 가지 IP 주소 유형을 할당할 수 있습니다.
- 인터페이스의 넷마스크. 넷마스크는 CIDR 형식이어야 합니다. 예를 들어, `255.255.255.0` 서브넷에는 `/24`를 사용합니다.

참고 동일한 서브넷 내의 IP 주소는 별도의 물리적 이더넷 인터페이스에서 구성할 수 없습니다. 네트워크 및 IP 주소 컨피그레이션에 대한 자세한 내용은 네트워크 및 IP 주소 할당, 1205 페이지을 참조해 주십시오.

C170 및 C190 어플라이언스의 경우 Data 2 인터페이스가 먼저 구성됩니다.

기본 게이트웨이 지정

`systemsetup` 명령의 다음 부분에서는 네트워크에 있는 기본 라우터(게이트웨이)의 IP 주소를 입력합니다.

웹 인터페이스 활성화

`systemsetup` 명령의 다음 부분에서는 어플라이언스(관리 이더넷 인터페이스)의 웹 인터페이스를 활성화합니다. 보안 HTTP(https)를 통해 웹 인터페이스를 실행하도록 선택할 수도 있습니다. 사용자가 HTTPS 사용을 선택하면, 시스템에서는 사용자 자신의 인증서를 업로드할 때까지 데모 인증서를 사용합니다.

DNS 설정 구성

이번에는 DNS(Domain Name Service) 설정을 구성합니다. AsyncOS는 인터넷의 루트 서버에 직접 쿼리할 수 있는 고성능 내부 DNS 확인자/캐시를 포함합니다. 또는 시스템에서 사용자 고유의 DNS 서버를 사용할 수 있습니다. 자신의 서버를 사용하도록 선택하는 경우 각 DNS 서버의 IP 주소와 호스트 이름을 제공해야 합니다. DNS 서버를 필요한 만큼 입력할 수 있습니다(각 서버의 우선 순위는 0). 기본적으로, `systemsetup`에서는 사용자 고유의 DNS 서버를 입력하도록 요구합니다.

리스너 만들기

"리스너"는 특정 IP 인터페이스에 구성될 인바운드 이메일 처리 서비스를 관리합니다. 리스너는 내부 시스템 또는 인터넷에서 Email Security Appliance로 들어가는 이메일에만 적용됩니다. Cisco AsyncOS는 리스너를 사용하여 메시지가 수락되고 수신자 호스트로 전달되기 위해 충족해야 하는 기준을 지정합니다. 리스너를 위에서 지정한 IP 주소에 대해 실행되는 이메일 리스너(또는 "SMTP 데몬")라고 생각할 수 있습니다.

C370, C670, X1070, C380, C680, C390 및 **C690** 어플라이언스의 경우: 기본적으로 `systemsetup` 명령은 2개의 리스너(퍼블릭 및 프라이빗)를 구성합니다. (사용 가능한 리스너 유형에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지 섹션을 참조해 주십시오.)

C170 및 **C190** 어플라이언스의 경우: 기본적으로 `systemsetup` 명령은 인터넷에서 메일을 수신하고 내부 네트워크에서 이메일을 전달하는 퍼블릭 리스너 1개를 구성합니다. C170 및 C190 어플라이언스에 대한 리스너 예 , 48 페이지를 참조하십시오.

리스너를 정의할 때 다음 특성을 지정해야 합니다.

- 나중에 리스너를 가리키기 위해 만드는 이름(별칭). 예를 들어 내부 시스템에서 인터넷으로 전달되는 이메일을 수락하는 리스너의 이름은 OutboundMail이라고 지정할 수 있습니다.
- 이메일을 수신할 IP 인터페이스 중 1개(`systemsetup` 명령의 초기 단계에서 생성한 인터페이스)
- 이메일을 라우팅할 시스템의 이름(퍼블릭 리스너 전용). (이것이 첫 번째 `smtproutes` 항목입니다. 로컬 도메인용 이메일 라우팅, 665 페이지 섹션을 참조해 주십시오.)
- 퍼블릭 리스너에 대한 SBRS(SenderBase Reputation Score)를 기반으로 필터링을 활성화할지 여부. 활성화한 경우 Conservative(신중), Moderate(중간) 또는 Aggressive(적극적) 설정 중에 선택할 수 있는 프롬프트가 표시됩니다.
- 호스트 단위 속도 제한: 원격 호스트에서 수신할 시간당 최대 수신자 수(퍼블릭 리스너 전용).
- 이메일을 수락할 수신자 도메인이나 특정 주소(퍼블릭 리스너) 또는 어플라이언스를 통해 이메일을 릴레이할 시스템(프라이빗 리스너). (이들이 리스너에 대한 첫 번째 Recipient Access Table 및 Host Access Table 항목입니다. 자세한 내용은 발신자 그룹 구문, 96 페이지 및 메시지를 수락할 도메인 및 사용자 추가, 131 페이지 섹션을 참조해 주십시오.)

관련 주제

- 퍼블릭 리스너, 44 페이지
- 프라이빗 리스너, 47 페이지
- C170 및 C190 어플라이언스에 대한 리스너 예 , 48 페이지

퍼블릭 리스너

참고 퍼블릭 및 프라이빗 리스너를 만드는 다음 예는 C370, C670, X1070, C380, C680, C390 및 C690 어플라이언스에만 적용됩니다. C170 및 C190 어플라이언스의 경우 C170 및 C190 어플라이언스에 대한 리스너 예 , 48 페이지 섹션으로 건너뛰십시오.

`systemsetup` 명령의 이 예 부분에서는 InboundMail이라는 퍼블릭 리스너가 PublicNet IP 주소에서 실행되도록 구성됩니다. 그런 다음 `example.com` 도메인의 모든 이메일을 수락하도록 구성됩니다. MX

에 대한 초기 SMTP 경로 `exchange.example.com`이 구성됩니다. 속도 제한이 활성화되고, 단일 호스트로부터 수신할 시간당 최대 수신자 수의 값 4500이 퍼블릭 리스너에 대해 지정됩니다.

참고 원격 호스트에서 수신할 시간당 최대 수신자 수에 대해 입력하는 값은 완전히 임의의 값이며, 일반적으로 이메일을 관리하는 엔터프라이즈의 크기와 관련이 있습니다. 예를 들어, 시간당 200개 메시지를 보내는 발신자는 "스패머"(원치 않는 대량 이메일 발신자)라고 간주될 수 있지만, 10,000명 규모 회사의 모든 이메일을 처리하도록 Email Security Appliance를 구성하는 경우 하나의 원격 호스트에서 오는 시간당 메시지 200개는 적절한 값일 수도 있습니다. 반대로 50명 규모의 회사에서 시간당 200개 메시지를 보내는 사람은 명백히 스패머일 수 있습니다. 엔터프라이즈의 퍼블릭 리스너(throttle) 인바운드 이메일에서 속도 제한을 활성화하는 경우 적절한 값을 선택해야 합니다. Default Host Access(기본 호스트 액세스) 정책에 대한 자세한 내용은 발신자 그룹 구문, 96 페이지 섹션을 참조하십시오.

이제 리스너에 대한 기본 호스트 액세스 정책이 수락됩니다.

```
You are now going to configure how the appliance accepts mail by

creating a "Listener".

Please create a name for this listener (Ex: "InboundMail"):

[]> InboundMail


Please choose an IP interface for this Listener.

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 3


Enter the domains or specific addresses you want to accept mail for.


Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

Usernames such as "postmaster@" are allowed.

Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.
```

```
Separate multiple addresses with commas.

[]> example.com


Would you like to configure SMTP routes for example.com?  [Y]> y


Enter the destination mail server which you want mail for example.com to be delivered.
Separate multiple entries with commas.

[]> exchange.example.com


Do you want to enable rate limiting for this listener? (Rate limiting defines the maximum
number
of recipients per hour you are willing to receive from a remote domain.) [Y]> y


Enter the maximum number of recipients per hour to accept from a remote domain.

[]> 4500


Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 1,000

Maximum Number Of Messages Per Connection: 1,000

Maximum Number Of Recipients Per Message: 1,000

Maximum Number Of Recipients Per Hour: 4,500

Maximum Recipients Per Hour SMTP Response:

    452 Too many recipients received this hour

Use SenderBase for Flow Control:  Yes

Virus Detection Enabled:  Yes

Allow TLS Connections: No
```

```
Would you like to change the default host access policy?  [N]> n


Listener InboundMail created.

Defaults have been set for a Public listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```

프라이빗 리스너

systemsetup 명령의 이 예 부분에서는 OutboundMail이라는 이름의 프라이빗 리스너가 PrivateNet IP 주소에서 실행되도록 구성됩니다. 그런 다음 `example.com` 도메인 내 모든 호스트에 대한 이메일을 릴레이하도록 구성됩니다. 항목의 시작 부분에 있는 점에 유의하십시오(`.example.com`).

이제 속도 제한에 대한 기본값(활성화되지 않음) 및 이 리스너에 대한 기본 호스트 액세스 정책이 수락됩니다.

프라이빗 리스너에 대한 기본값은 앞서 만든 퍼블릭 리스너와 다릅니다. 자세한 내용은 리스너 작업, 70 페이지를 참고하십시오.

```
Do you want to configure the appliance to relay mail for internal hosts?  [Y]> y


Please create a name for this listener (Ex: "OutboundMail"):

[]> OutboundMail


Please choose an IP interface for this Listener.

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 2


Please specify the systems allowed to relay email through the appliance.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.
```

```
IP addresses, IP address ranges, and partial IP addressed are allowed.

Separate multiple entries with commas.

[]> .example.com


Do you want to enable rate limiting for this listener?
(Rate limiting defines the maximum number of recipients per hour you are willing
to receive from a remote domain.)  [N]> n


Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control:  No

Virus Detection Enabled:  Yes

Allow TLS Connections: No

Would you like to change the default host access policy?  [N]> n


Listener OutboundMAil created.

Defaults have been set for a Private listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```

C170 및 C190 어플라이언스에 대한 리스너 예

참고 리스너를 만드는 다음 예는 C170 및 C190 어플라이언스에만 적용됩니다.

systemsetup 명령의 이 예 부분에서는 MailInterface라는 이름의 리스너가 MailNet IP 주소에서 실행되도록 구성됩니다. 그런 다음 example.com 도메인의 모든 이메일을 수락하도록 구성됩니다. MX에 대한 초기 SMTP 경로 exchange.example.com이 구성됩니다. 그런 다음 동일한 리스너가 example.com 도메인 내 모든 호스트에 대한 이메일을 릴레이하도록 구성됩니다. 항목의 시작 부분에 있는 점에 유의하십시오(.example.com).

속도 제한이 활성화되고, 단일 호스트로부터 수신할 시간당 최대 수신자 수의 값 450이 퍼블릭 리스너에 대해 지정됩니다.

참고 원격 호스트에서 수신할 시간당 최대 수신자 수에 대해 입력하는 값은 완전히 임의의 값이며, 일반적으로 이메일을 관리하는 엔터프라이즈의 크기와 관련이 있습니다. 예를 들어, 시간당 200개 메시지를 보내는 발신자는 "스패머"(원치 않는 대량 이메일 발신자)라고 간주될 수 있지만, 10,000명 규모 회사의 모든 이메일을 처리하도록 어플라이언스를 구성하는 경우 하나의 원격 호스트에서 오는 시간당 메시지 200개는 적절한 값일 수도 있습니다. 반대로 50명 규모의 회사에서 시간당 200개 메시지를 보내는 사람은 명백히 스패머일 수 있습니다. 엔터프라이즈의 퍼블릭 리스너(throttle) 인바운드 이메일에서 속도 제한을 활성화하는 경우 적절한 값을 선택해야 합니다. Default Host Access(기본 호스트 액세스) 정책에 대한 자세한 내용은 발신자 그룹 구문, 96 페이지 섹션을 참조하십시오.

이제 리스너에 대한 기본 호스트 액세스 정책이 수락됩니다.

```
You are now going to configure how the appliance accepts mail by creating a "Listener".

Please create a name for this listener (Ex: "MailInterface"):

[]> MailInterface


Please choose an IP interface for this Listener.

1. MailNet (10.1.1.1/24: mail3.example.com)

2. Management (192.168.42.42/24: mail3.example.com)

[1]> 1


Enter the domain names or specific email addresses you want to accept mail for.


Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

Usernames such as "postmaster@" are allowed.

Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.
```

```
Separate multiple addresses with commas.

[]> example.com


Would you like to configure SMTP routes for example.com?  [Y]> y


Enter the destination mail server where you want mail for example.com to be delivered.
Separate multiple entries with commas.

[]> exchange.example.com


Please specify the systems allowed to relay email through the appliance.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addresses are allowed.

Separate multiple entries with commas.

[]> .example.com


Do you want to enable rate limiting for this listener?
(Rate limiting defines the maximum number of recipients per hour you are willing
to receive from a remote domain.)  [Y]> y


Enter the maximum number of recipients per hour to accept from a remote domain.

[]> 450


Default Policy Parameters

==========================

Maximum Message Size: 10M

Maximum Number Of Connections From A Single IP: 50

Maximum Number Of Messages Per Connection: 100
```

```
Maximum Number Of Recipients Per Message: 100

Maximum Number Of Recipients Per Hour: 450

Maximum Recipients Per Hour SMTP Response:

    452 Too many recipients received this hour

Use SenderBase for Flow Control:  Yes

Spam Detection Enabled:  Yes

Virus Detection Enabled:  Yes

Allow TLS Connections: No

Would you like to change the default host access policy?  [N]>


Listener MailInterface created.

Defaults have been set for a Public listener.

Use the listenerconfig->EDIT command to customize the listener.

*****
```

참고 `systemsetup` 명령은 C170 및 C190 어플라이언스에 대한 인바운드와 아웃바운드 메일 모두에 대해 하나의 리스너만 구성하므로 모든 발신 메일은 메일 플로우 모니터 기능(일반적으로 인바운드 메시지에 사용됨)에서 계산됩니다. 이메일 보안 모니터 사용, 793 페이지를 참조하십시오.

Anti-Spam 활성화

어플라이언스는 안티 스팸 소프트웨어에 대한 30일 평가 키와 함께 제공됩니다. **systemsetup** 명령의 이 부분 중에, 라이선스 계약에 동의하고 어플라이언스에서 Anti-Spam을 전역적으로 활성화하도록 선택할 수 있습니다.

그러면 안티스팸 검사는 수신 메일 정책에서 활성화됩니다.

참고 라이선스 계약에 동의하지 않으면 안티 스팸이 어플라이언스에서 활성화되지 않습니다.

어플라이언스에서 사용 가능한 모든 안티스팸 구성 옵션은 Anti-Spam, 355 페이지을 참조해 주십시오.

기본 안티 스팸 스캐닝 엔진 선택

둘 이상의 안티 스팸 스캔 엔진을 활성화한 경우 어떤 것을 기본 수신 메일 정책에 사용하도록 활성화할지 묻는 프롬프트가 표시됩니다.

스팸 격리 활성화

안티스팸 서비스를 활성화하기로 선택한 경우, 스팸 및 의심스런 스팸 메시지를 로컬 스팸 격리로 전송하도록 수신 메일 정책을 활성화할 수 있습니다. 스팸 격리를 활성화하면 어플라이언스의 최종 사용자 격리도 활성화됩니다. 최종 사용자 액세스가 구성될 때까지는 관리자만 최종 사용자 격리에 액세스할 수 있습니다.

로컬 스팸 격리 설정, 868 페이지를 참조하십시오.

안티바이러스 검사 활성화

어플라이언스는 바이러스 검사 엔진에 대한 30일 평가 키와 함께 제공됩니다. `systemsetup` 명령의 이 부분 중에, 하나 이상의 라이선스 계약에 동의하고 어플라이언스에서 안티바이러스 검사를 활성화하도록 선택할 수 있습니다. 어플라이언스에서 활성화할 각 안티바이러스 검사 엔진에 대한 라이선스 계약에 동의해야 합니다.

계약에 동의하면, 선택한 안티 바이러스 스캔 엔진이 수신 메일 정책에서 활성화됩니다. Email Security Appliance는 수신 메일에서 바이러스를 검사하지만 감염된 첨부 파일을 복구하지는 않습니다. 어플라이언스는 감염된 메시지를 삭제합니다.

어플라이언스에서 사용 가능한 안티바이러스 컨피그레이션 옵션은 Anti-Virus, 335 페이지를 참조해 주십시오.

Outbreak Filter 및 SenderBase Email Traffic Monitoring Network 활성화

이번 단계에서는 SenderBase 참여 및 Outbreak Filter 모두의 활성화에 대한 프롬프트가 표시됩니다. 어플라이언스는 Outbreak Filter에 대한 30일 평가 키와 함께 제공됩니다.

관련 주제

- 신종 바이러스 필터(Outbreak Filter), 52 페이지
- SenderBase 참여, 53 페이지

신종 바이러스 필터(Outbreak Filter)

Outbreak Filter는 기존의 안티바이러스 보안 서비스를 신종 서명 파일로 업데이트할 수 있을 때까지 의심스런 메시지를 격리하여 신종 바이러스 전파 확산에 대한 "제1 방어선"을 제공합니다. Outbreak Filter는 활성화될 경우 기본 수신 메일 정책에서 활성화됩니다.

Outbreak Filter를 활성화하도록 선택하는 경우 임계값을 입력하고 Outbreak Filter 경고문 수신 여부를 선택합니다. Outbreak Filter 및 임계값에 대한 자세한 내용은 신종 바이러스 필터(Outbreak Filter), 399 페이지 섹션을 참조해 주십시오.

SenderBase 참여

SenderBase는 이메일 관리자가 발신자를 조사하고 이메일의 합법적인 소스를 식별하고 스패머를 차단하도록 지원하기 위해 설계된 이메일 평가 서비스입니다.

SenderBase Email Traffic Monitoring Network 참여에 동의할 경우 Cisco는 조직으로 전송되는 이메일에 대한 집계된 통계를 수집합니다. 여기에는 Email Security Appliance에서의 서로 다른 유형의 메시지 처리 방식에 대한 정보 및 메시지 특성에 대한 요약 데이터가 포함됩니다.

자세한 내용은 *Cisco Email Security Appliance* 가이드의 *SenderBase* 네트워크 참여 장을 참고하십시오.

알림 설정 및 **AutoSupport** 구성

사용자 개입이 필요한 시스템 오류가 발생하면 Cisco AsyncOS는 이메일을 통해 사용자에게 알림 메시지를 전송합니다. 시스템 경고문을 수신할 이메일 주소를 하나 이상 추가해 주십시오. 주소가 여러 개인 경우 쉼표로 구분해 주십시오. 입력한 이메일 주소에서는 DHAP(Directory Harvest Attack Prevention) 경고문을 제외하고, 처음에 모든 레벨에서 모든 유형의 경고문을 수신합니다. CLI의 `alertconfig` 명령 또는 **GUI**의 **System Administration(**시스템 관리**) > Alerts(**알림**)** 페이지를 사용하여 알림 구성을 더욱 세부적으로 조정할 수 있습니다. 자세한 내용은 *Cisco Email Security Appliance* 가이드에서 관리 작업 배포 장의 알림 섹션을 참고하십시오.

AutoSupport 기능은 업계 최고의 지원을 제공할 수 있도록 어플라이언스의 문제를 Cisco 고객 지원 팀에 지속적으로 알려 줍니다. Cisco 지원에 경고문 및 주간 상태 업데이트를 전송하려면 "Yes"(예)로 답하십시오. 자세한 내용은 *Cisco Email Security Appliance* 가이드에서 관리 작업 배포 장의 *AutoSupport* 섹션을 참고하십시오.

예약된 보고 구성

기본 예약된 보고서를 전송하기 위한 주소를 입력합니다. 이 값을 비워둘 수 있으며 이 경우 보고서는 이메일을 통해 전송되는 대신 어플라이언스에 보관됩니다.

시간 설정 구성

Cisco AsyncOS에서는 NTP(Network Time Protocol)를 사용하여 네트워크의 다른 서버 또는 인터넷과 시간을 동기화하거나, 시스템 시계를 수동으로 설정할 수 있습니다. 메시지 헤더와 로그 파일의 타임스탬프가 정확하도록 어플라이언스의 표준 시간대를 설정해야 합니다. 또한 Cisco Systems 시간 서버를 사용하여 어플라이언스에서 시간을 동기화할 수 있습니다.

Continent(대륙), Country(국가) 및 Timezone(표준 시간대)을 선택하고 사용할 NTP 서버의 이름을 포함하여 NTP를 사용할지 여부를 선택합니다.

변경 사항 커밋

마지막으로, 시스템 설정 마법사는 전체 절차에서 수행한 컨피그레이션 변경 사항을 커밋(`commit`)하도록 요구합니다. 변경 사항을 커밋하려면 "Yes"(예)로 답합니다.

시스템 설정 마법사를 성공적으로 완료하면 다음 메시지가 나타나며 명령 프롬프트가 표시됩니다.

```
Congratulations! System setup is complete. For advanced configuration, please refer to the
 User Guide.
```

```
mail3.example.com>
```

이제 어플라이언스에서 이메일을 전송할 준비가 되었습니다.

컨피그레이션 테스트

CiscoAsyncOS 구성을 테스트하려면 mailconfig 명령을 사용하여 `systemsetup`명령으로 방금 만든 시스템 구성 데이터가 포함된 테스트 이메일을 즉시 전송할 수 있습니다.

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send

the configuration file. Separate multiple addresses with commas.

[]> user@example.com


The configuration file has been sent to user@example.com.

mail3.example.com>
```

시스템이 네트워크에서 메일을 보낼 수 있음을 확인하기 위해 액세스 권한이 있는 사서함에 컨피그레이션을 보냅니다.

즉각 경고문

Email Security Appliance는 기능 키를 사용하여 기능을 활성화합니다. 처음 `systemsetup` 명령으로 리스너를 만들거나, 안티스팸을 활성화하거나, Sophos 또는 McAfee Anti-Virus를 활성화하거나, Outbreak Filter를 활성화하면 알림이 생성되어 2단계: 시스템, 31 페이지에서 지정한 주소로 전송됩니다.

이 알림에서 키의 남은 시간을 주기적으로 알려줍니다. 예를 들면 다음과 같습니다.

```
Your "Receiving" key will expire in under 30 day(s).
Please contact IronPort Customer Support.


Your "Sophos" key will expire in under 30 day(s).
Please contact IronPort Customer Support.


Your "Outbreak Filters" key will expire in under 30 day(s).
Please contact IronPort Customer Support.
```

30일 평가 기간 이후에 기능을 활성화하는 방법에 대한 자세한 내용은 Cisco 영업 담당자에게 문의하십시오. **System Administration(**시스템 관리**) > Feature Keys(**기능 키**)** 페이지 또는 `featurekey` 명령을 통해 남은 키의 남은 평가 기간을 확인할 수 있습니다. (자세한 내용은 기능 키, 926 페이지를 참조하십시오.)

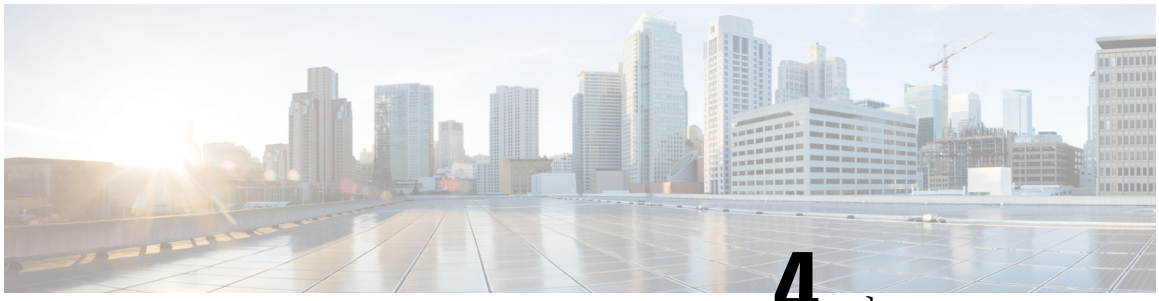
시스템을 엔터프라이즈 게이트웨이로 구성

시스템을 엔터프라이즈 게이트웨이(인터넷에서 이메일 수락)로 구성하려면 먼저 이 장을 완료하고, 이메일을 수신하도록 게이트웨이 구성, 69 페이지에서 추가 정보를 참고하십시오.

컨피그레이션 확인 및 다음 단계

이제 시스템 설정이 완료되었으므로 Email Security Appliance에서 메일을 전송 및 수신할 수 있습니다. 안티바이러스, 안티스팸 및 바이러스 Outbreak Filter 보안 기능을 활성화한 경우 시스템은 또한 수신 및 발신 메일에서 스팸과 바이러스를 검사할 수 있습니다.

다음 단계에서는 어플라이언스의 구성을 맞춤 설정하는 방법을 살펴봅니다. 이메일 파이프라인 이해, 57 페이지에서는 시스템을 통해 이메일이 라우팅되는 방법에 대한 자세한 개요를 제공합니다. 각 기능은 순서대로(위에서 아래로) 처리되며, 이 가이드의 나머지 장에서 각 기능에 대해 설명합니다.



4 장

이메일 파이프라인 이해

이 장에는 다음 섹션이 포함되어 있습니다.

이메일 파이프라인 개요

이메일 파이프라인은 어플라이언스에 의해 처리되는 이메일의 플로우로서 다음과 같은 세 단계로 구성됩니다.

- Receipt(수신) - 어플라이언스는 수신 이메일을 받기 위해 원격 호스트에 연결할 때 구성된 제한 및 기타 수신 정책을 준수합니다. 예를 들면 호스트가 사용자에게 메일을 전송할 수 있는지 확인하고, 수신 연결 및 메시지 제한을 시행하고, 메시지의 수신자를 검증합니다.
- Work Queue(작업 대기열) - 어플라이언스는 수신 및 발신 메일을 처리하면서 필터링, 허용 목록/차단 목록 검사, 안티스팸/안티바이러스 검사, 보안 침해 필터, 격리와 같은 작업을 수행합니다.
- Delivery(전달) - 어플라이언스는 발신 이메일을 전송하기 위해 연결할 때 구성된 전달 제한 및 정책을 준수합니다. 예를 들면 아웃바운드 연결 제한을 시행하고 전달할 수 없는 메시지를 지정된 대로 처리합니다.

이메일 파이프라인 플로우

다음 그림에서는 수신에서 라우팅, 전달까지 시스템을 통해 이메일이 처리되는 방법에 대한 개요를 제공합니다. 각 기능은 순서대로(위에서 아래로) 처리됩니다. trace 명령을 사용하여 이 파이프라인에 있는 기능의 컨피그레이션을 대부분 테스트할 수 있습니다.

그림 ***5:*** 이메일 파이프라인 **-** 이메일 연결 수신

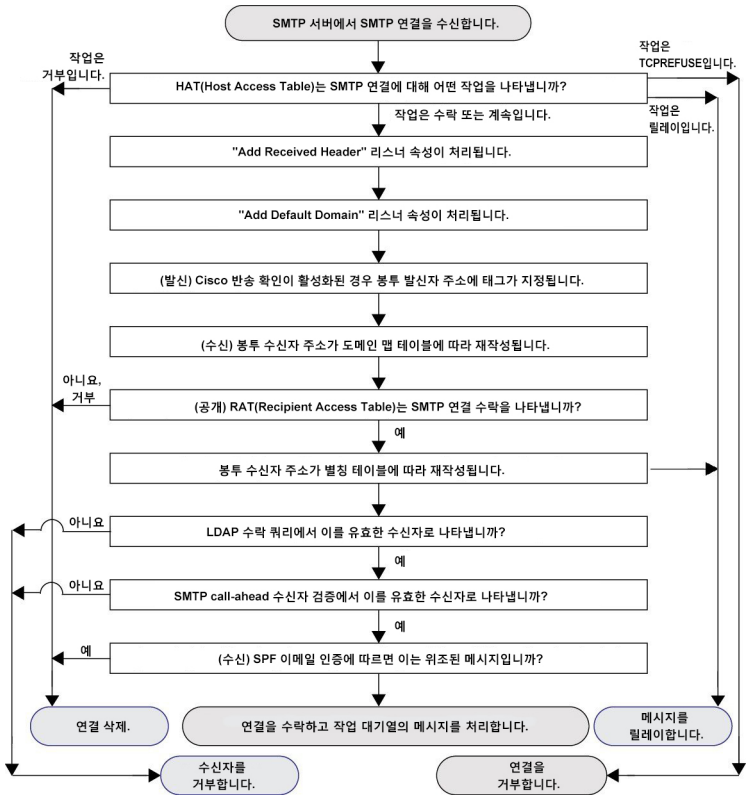


그림 *6:* 이메일 파이프라인 - 작업 대기열

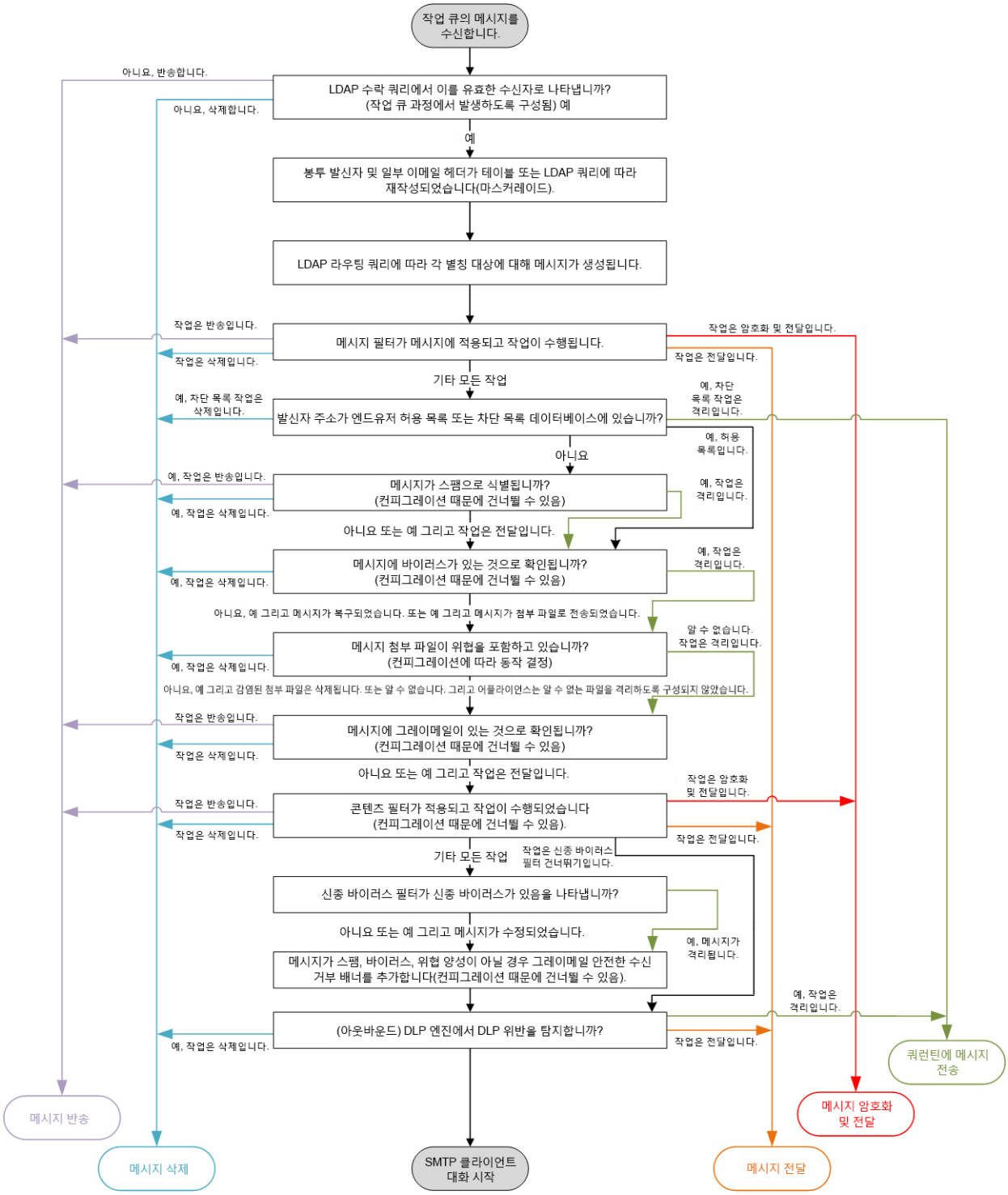
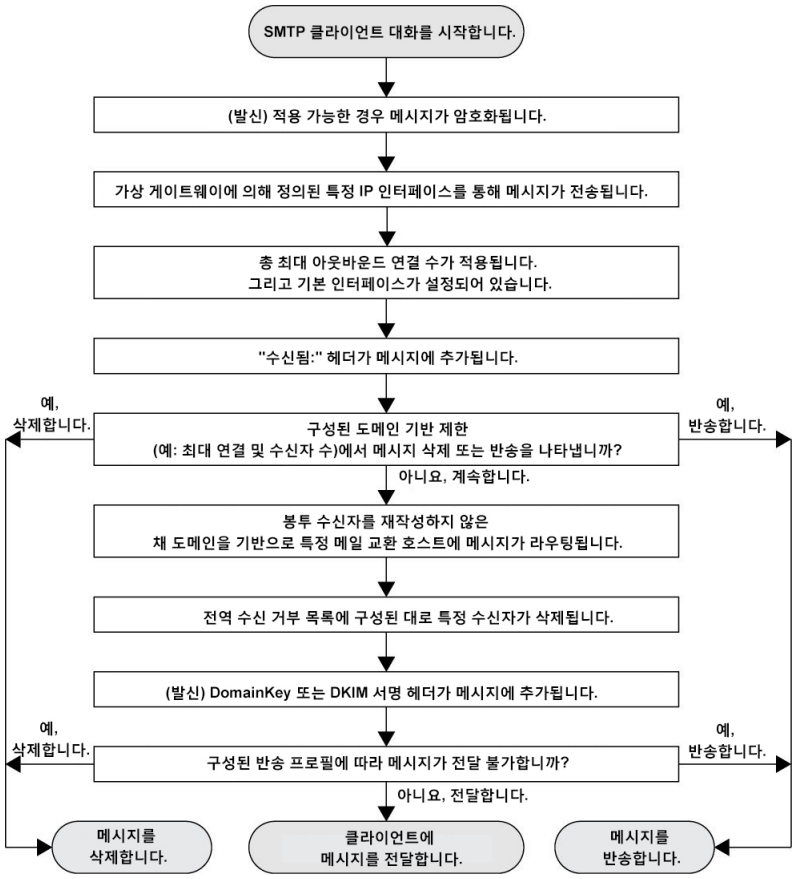


그림 *7:* 이메일 파이프라인 - 이메일 전달



수신/발신

이메일 파이프라인의 수신 단계에는 발신자 호스트로부터의 초기 연결이 포함됩니다. 각 메시지의 도메인을 설정할 수 있고, 수신자를 확인하며, 메시지를 작업 대기열로 전달합니다.

관련 주제

- HAT(Host Access Table), 발신자 그룹 및 메일 플로우 정책, 61 페이지
- 수신됨: 헤더, 61 페이지
- 기본 도메인, 61 페이지
- 반송 확인, 61 페이지
- 도메인 맵, 62 페이지
- RAT(Recipient Access Table), 62 페이지
- 별칭 테이블, 62 페이지
- LDAP 수신자 수락, 62 페이지
- SMTP Call-Ahead 수신자 검증, 62 페이지

HAT(Host Access Table), 발신자 그룹 및 메일 플로우 정책

HAT를 사용하면 리스너에 연결할 수 있는 호스트를 지정할 수 있습니다(즉, 어떤 호스트가 이메일을 전송할 수 있는지를 지정).

발신자 그룹은 하나 이상의 발신자를 그룹에 연결하는 데 사용되며, 그렇게 되면 메시지 필터 및 기타 메일 플로우 정책을 적용할 수 있습니다. 메일 플로우 정책은 HAT 매개변수(액세스 규칙 뒤에 속도 제한 매개변수 및 사용자 지정 SMTP 코드와 응답) 그룹을 표현하는 방법입니다.

발신자 그룹 및 메일 플로우 정책은 리스너의 HAT에 정의되어 있습니다.

발신자 그룹에 대한 호스트 DNS 확인 설정을 사용하면 SMTP 대화 전에 미확인 발신자를 분류하고 여러 유형의 미확인 발신자를 다양한 발신자 그룹에 포함할 수 있습니다.

연결 호스트는 발신자 그룹에서 호스트 DNS 확인을 받았지만(SMTP 대화 전에), 봉투 발신자의 도메인 부분은 메일 플로우 정책에서 DNS 확인을 받으며 확인은 SMTP 대화 중에 발생합니다. 형식이 잘못된 봉투 발신자의 메시지는 무시될 수 있습니다. 봉투 발신자 DNS 확인 설정과 상관없이 메일을 수락 또는 거절하는 도메인 및 이메일 주소 목록인 Sender Verification Exception(발신자 확인 예외) 테이블에 항목을 추가할 수 있습니다.

발신자 평판 필터링을 사용하면 이메일 발신자를 분류하고, Cisco SenderBase Reputation Service에서 결정한 발신자의 신뢰도를 기반으로 이메일 인프라에 대한 액세스를 제한할 수 있습니다.

자세한 내용은 사전 정의된 발신자 그룹 및 메일 플로우 정책 이해, 103 페이지를 참고하십시오.

수신됨: 헤더

`listenerconfig` 명령을 사용하면, 수신하는 모든 메시지에 대해 기본적으로 Received: 헤더를 포함하지 않도록 리스너를 구성할 수 있습니다.

자세한 내용은 리스너 작업, 70 페이지를 참고하십시오.

기본 도메인

인증된 도메인 이름이 포함되지 않은 발신자 주소에 기본 도메인을 자동으로 추가하도록 리스너를 구성할 수 있습니다. 이러한 주소를 "bare(베어)" 주소라고도 합니다(예: "joe" 대 "joe@example.com").

자세한 내용은 리스너 작업, 70 페이지를 참고하십시오.

반송 확인

발송 메일에는 특수 키가 태그로 지정됩니다. 해당 메일이 반송되는 경우 태그가 인식되고 메일이 전달됩니다. 자세한 내용은 반송 확인, 703 페이지를 참고하십시오.

도메인 맵

구성하는 각 리스너에 대해 도메인 맵 테이블을 작성할 수 있습니다. 그러면 도메인 맵 테이블의 도메인과 일치하는 메시지에서 각 수신자에 대한 봉투 수신자가 재작성됩니다. 예: joe@old.com -> joe@new.com

자세한 내용은 도메인 맵 기능, 688 페이지를 참고하십시오.

RAT(Recipient Access Table)

인바운드 이메일의 경우에만, RAT를 통해 어플라이언스가 메일을 수락할 모든 로컬 도메인의 목록을 지정할 수 있습니다.

자세한 내용은 수신자 주소를 기반으로 연결 수락 또는 거부 개요, 129 페이지를 참고하십시오.

별칭 테이블

별칭 테이블은 메시지를 하나 이상의 수신자에게 리디렉션하는 메커니즘을 제공합니다. 별칭은 매핑 테이블에 저장됩니다. 이메일의 Envelope Recipient(봉투 수신자)(Envelope To 또는 RCPT TO라고도 함)가 별칭 테이블에 정의된 별칭과 일치하면 봉투 수신자의 이메일 주소가 재작성됩니다.

별칭 테이블에 대한 자세한 내용은 별칭 테이블 만들기, 671 페이지 섹션을 참조하십시오.

LDAP 수신자 수락

기존의 LDAP 인프라를 사용하여, SMTP 대화 중에 또는 작업 대기열 내에서 수신 메시지의 수신자 이메일 주소(퍼블릭 리스너에서)를 처리하는 방법을 정의할 수 있습니다. 자세한 내용은 리스너 작업, 70 페이지 섹션을 참조하십시오. 이렇게 하면 어플라이언스가 디렉터리 수집 공격(DHAP)을 고유한 방식으로 차단할 수 있습니다. 시스템은 메시지를 수락하고 SMTP 대화 또는 작업 대기열 내에서 LDAP 수락 검증을 수행합니다. LDAP 디렉터리에서 수신자가 발견되지 않으면 지연된 반송을 수행하거나 메시지를 완전히 삭제하도록 시스템을 구성할 수 있습니다.

자세한 내용은 LDAP 쿼리 작업, 745 페이지를 참고하십시오.

SMTP Call-Ahead 수신자 검증

SMTP call-ahead 수신자 검증을 구성할 경우 Email Security Appliance는 전송 MTA와의 SMTP 대화를 일시 중단하고 수신자 확인을 위해 SMTP 서버에 "미리 연락(call ahead)"합니다. 어플라이언스가 SMTP 서버에 쿼리하면, SMTP 서버 응답이 Email Security Appliance로 반환됩니다. Email Security Appliance는 SMTP 대화를 다시 시작하고 전송 MTA에 응답을 전송하여, SMTP 서버 응답(그리고 SMTP Call-Ahead 프로필에 구성한 설정)을 기반으로 대화를 계속 진행하도록 허용하거나 연결을 삭제합니다.

자세한 내용은 SMTP 서버를 사용하여 수신자 검증, 637 페이지을 참조해 주십시오.

작업 대기열/라우팅

작업 대기열은 전달 단계로 이동하기 전 수신된 메시지가 처리되는 곳입니다. 처리에는 가장, 라우팅, 필터링, 허용 목록/차단 목록 검사, 안티스팸/안티바이러스 검사, 파일 평판 검사 및 분석, 보안 침해 필터, 격리 등이 포함됩니다.

참고 DLP(Data Loss Prevention) 검사는 발신 메시지에만 사용할 수 있습니다. DLP 메시지 검사가 작업 대기열의 어디에서 발생하는지에 대한 자세한 내용은 메시지 분리, 274 페이지 섹션을 참조하십시오.

관련 주제

- 이메일 파이프라인 및 보안 서비스, 63 페이지
- LDAP 수신자 수락, 62 페이지
- 마스커레이드 또는 LDAP 마스커레이드, 64 페이지
- LDAP 라우팅, 64 페이지
- 메시지 필터, 64 페이지
- 이메일 보안 관리자(수신자 단위 검사), 64 페이지
- 쿼런틴, 66 페이지

이메일 파이프라인 및 보안 서비스

일반적으로 보안 서비스(안티스팸 검사, 안티바이러스 검사 및 보안 침해 필터)를 변경하는 경우 이미 작업 대기열에 있는 메시지는 영향을 받지 않습니다. 예를 들면 다음과 같습니다.

메시지가 처음 파이프라인에 들어갈 때 다음과 같은 이유 때문에 안티바이러스 검사를 우회할 경우

- 안티바이러스 검사가 어플라이언스에 대해 전역적으로 활성화되지 않음
- HAT 정책이 안티바이러스 검사를 건너뛰도록 지정됨
- 메시지 필터에서 메시지가 안티바이러스 검사를 우회하도록 지정함

안티바이러스 검사가 다시 활성화되었는지 여부와 관계없이 메시지가 격리에서 릴리스될 때 안티바이러스 검사를 거치지 않습니다. 그러나 메시지가 격리에 있는 동안 메일 정책의 설정이 변경될 수 있으므로, 메일 정책 때문에 안티바이러스 검사를 우회하는 메시지는 격리에서 릴리스될 때 안티바이러스 검사를 받을 수 있습니다. 예를 들어 메시지가 메일 정책 때문에 안티바이러스 검사를 우회하고 격리되었고, 격리에서 릴리스되기 전 메일 정책이 안티바이러스 검사를 포함하도록 업데이트된 경우, 해당 메시지는 격리에서 릴리스될 때 안티바이러스 검사를 받습니다.

마찬가지로, 실수로 안티스팸 검사를 전역적으로 비활성화했고 메일이 작업 대기열이 있을 때 이를 알았다고 가정해보겠습니다. 이 시점에 안티스팸을 활성화하면 작업 대기열에 있는 메시지에 대해 안티스팸 검사가 수행되지 않습니다.

LDAP 수신자 수락

기존의 LDAP 인프라를 사용하여, SMTP 대화 중에 또는 작업 대기열 내에서 수신 메시지의 수신자 이메일 주소(퍼블릭 리스너에서)를 처리하는 방법을 정의할 수 있습니다. 자세한 내용은 리스너 작업, 70 페이지 섹션을 참조하십시오. 이렇게 하면 어플라이언스가 디렉터리 수집 공격(DHAP)을 고유한 방식으로 차단할 수 있습니다. 시스템은 메시지를 수락하고 SMTP 대화 또는 작업 대기열 내에서 LDAP 수락 검증을 수행합니다. LDAP 디렉터리에서 수신자가 발견되지 않으면 지연된 반송을 수행하거나 메시지를 완전히 삭제하도록 시스템을 구성할 수 있습니다.

자세한 내용은 LDAP 쿼리 작업, 745 페이지를 참고하십시오.

마스커레이드 또는 LDAP 마스커레이드

Masquerading(가장)은 작성한 테이블에 따라 프라이빗 또는 퍼블릭 리스너에서 처리되는 이메일에서 Envelope Sender(봉투 발신자)(발신자 또는 MAIL FROM이라고도 함)와 To:, From:, 및/또는 CC: 헤더를 재작성합니다. 만든 각 리스너에 대해 두 가지 방법(만든 매핑의 고정 테이블을 통해 또는 LDAP 쿼리를 통해) 중 하나를 사용하여 서로 다른 가장 매개변수를 지정할 수 있습니다.

고정 매핑 테이블을 통한 가장에 대해 자세히 알아보려면 가장 구성, 678 페이지 섹션을 참조하십시오.

LDAP 쿼리를 통한 가장에 대해 자세히 알아보려면 LDAP 쿼리 작업, 745 페이지 항목을 참고하십시오.

LDAP 라우팅

네트워크의 LDAP 디렉터리에서 사용 가능한 정보를 기반으로 적절한 주소 및/또는 메일 호스트로 메시지를 라우팅하도록 어플라이언스를 구성할 수 있습니다.

자세한 내용은 LDAP 쿼리 작업, 745 페이지를 참고하십시오.

메시지 필터

메시지 필터를 사용하면 메시지 및 첨부 파일을 수신할 때 어떻게 처리할지를 설명하는 특수 규칙을 만들 수 있습니다. 필터 규칙은 메시지나 첨부 파일 내용, 네트워크에 대한 정보, 메시지 봉투, 메시지 헤더, 메시지 본문 등을 기반으로 메시지를 식별합니다. 필터 작업의 결과 메시지가 삭제, 반송, 보관, 격리, 숨은 참조 또는 변경될 수 있습니다.

자세한 내용은 메시지 필터를 사용하여 이메일 정책 적용, 137 페이지를 참고하십시오.

다중 수신자 메시지는 이 단계 이후 이메일 보안 관리자 이전에 "분리"됩니다. 메시지 분리란 이메일 보안 관리자를 통해 처리하기 위해 수신자별로 이메일의 분리 복사본을 만드는 것을 말합니다.

이메일 보안 관리자(수신자 단위 검사)

- 허용 목록/차단 목록 검사, 65 페이지
- Anti-Spam, 65 페이지

- Anti-Virus, 65 페이지
- 그레이메일 탐지 및 안전한 수신 거부, 66 페이지
- 파일 평판 검사 및 파일 분석 , 66 페이지
- 콘텐츠 필터, 66 페이지
- 신종 바이러스 필터(Outbreak Filter), 66 페이지

허용 목록/차단 목록 검사

최종 사용자 허용 목록 및 차단 목록은 최종 사용자별로 생성되며 안티스팸 검사 전에 확인되는 데이터베이스에 저장됩니다. 각 최종 사용자는 항상 스팸으로 처리하거나 스팸으로 처리하지 않을 도메인, 하위 도메인 또는 이메일 주소를 식별할 수 있습니다. 발신자 주소가 최종 사용자 허용 목록의 일부이고 안티스팸 검사가 생략되는 경우, 그리고 발신자 주소가 차단 목록에 포함되어 있는 경우, 관리자 설정에 따라 해당 메시지는 격리되거나 삭제될 수 있습니다. 허용 목록 및 차단 목록 구성에 대한 자세한 내용은 스팸 격리, 867 페이지를 참조하십시오.

Anti-Spam

안티스팸 검사는 인터넷 전체의 완전한 서버 측 안티스팸 보호를 제공합니다. 안티스팸 검사는 사용자에게 불편을 주고 네트워크를 마비 또는 손상시키기 전에 스팸 공격을 적극적으로 식별 및 차단합니다. 따라서 사용자 개인정보를 침해하지 않은 채 사용자의 받은 편지함에 도달하기 전에 원치 않는 메일을 제거할 수 있습니다.

스팸 격리에 메일을 전달하도록 안티스팸 검사를 구성할 수 있습니다(온박스 또는 오프박스). 스팸 격리에서 릴리스된 메시지는 대상 대기열로 직접 이동하며, 이메일 파이프라인에서 추가 작업 대기열 처리를 건너뜁니다.

자세한 내용은 Anti-Spam, 355 페이지 장을 참조해 주십시오.

Anti-Virus

어플라이언스에는 통합 바이러스 검사 엔진이 포함됩니다. "메일 정책" 기반으로 메시지와 첨부 파일에서 바이러스를 검사하도록 어플라이언스를 구성할 수 있습니다. 바이러스가 발견될 때 다음과 같은 작업을 수행하도록 어플라이언스를 구성할 수 있습니다.

- 첨부 파일을 복구하려고 시도
- 첨부 파일 삭제
- 제목 헤더 수정
- X-header 추가
- 메시지를 다른 주소 또는 메일호스트로 전송
- 메시지 보관
- 메시지 삭제

격리에서 해제된 메시지(쿼런틴, 66 페이지 참조)에 대해 바이러스가 검사됩니다. 안티바이러스 검사에 대한 자세한 내용은 Anti-Virus, 335 페이지를 참조하십시오.

그레이메일 탐지 및 안전한 수신 거부

그레이메일 메시지를 탐지하고 최종 사용자 대신 안전한 수신 거부를 수행하도록 어플라이언스를 구성할 수 있습니다. 사용 가능한 작업은 안티바이러스 검사의 경우와 비슷합니다.

자세한 내용은 그레이메일 관리, 387 페이지를 참고하십시오.

파일 평판 검사 및 파일 분석

메시지 첨부 파일에서 새로운 위협 및 대상 지정 위협을 검사하도록 어플라이언스를 구성할 수 있습니다. 사용 가능한 작업은 안티바이러스 검사의 경우와 비슷합니다.

자세한 내용은 File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석), 461 페이지을 참조해 주십시오.

콘텐츠 필터

발신자 또는 수신자 기반으로 메시지에 적용할 콘텐츠 필터를 만들 수 있습니다. 콘텐츠 필터는 이메일 파이프라인에서 더 뒤에(한 메시지가 일치하는 각 이메일 보안 관리자 정책에 대해 여러 메시지로 "분리"된 후) 적용된다는 점을 제외하면 메시지 필터와 유사합니다. 콘텐츠 필터의 기능은 메시지에 대해 메시지 필터 처리와 안티스팸 및 안티바이러스 검사가 수행된 후 적용됩니다.

콘텐츠 필터에 대한 자세한 내용은 콘텐츠 필터, 283 페이지 섹션을 참조하십시오.

신종 바이러스 필터(Outbreak Filter)

Cisco의 Outbreak Filters(보안 침해 필터) 기능에는 새로운 보안 침해에 대해 첫 번째 주요 방어막을 제공하도록 선제적으로 작동하는 특수 필터가 있습니다. Cisco에서 게시한 보안 침해 규칙을 기반으로, 특정 파일 형식의 첨부 파일이 있는 메시지를 Outbreak(보안 침해)란 이름의 격리로 전송할 수 있습니다.

Outbreak(보안 침해) 격리로 전송된 메시지는 격리의 다른 메시지처럼 처리됩니다. 격리 및 작업 대기열에 대한 자세한 내용은 쿼런틴, 66 페이지 섹션을 참조하십시오.

자세한 내용은 신종 바이러스 필터(Outbreak Filter), 399 페이지를 참조하십시오.

쿼런틴

수신 또는 발신 메시지를 필터링하고 격리에 배치할 수 있습니다. 격리는 메시지를 유지 및 처리하는 데 사용되는 특수 대기열 또는 저장소입니다. 격리의 구성 방식에 따라 격리에 있는 메시지를 전달하거나 삭제할 수 있습니다.

다음의 작업 대기열 기능은 메시지를 격리로 전송할 수 있습니다.

- 스팸 필터
- 메시지 필터
- Anti-Virus
- 보안 침해 필터
- 콘텐츠 필터

- 파일 분석(Advanced Malware Protection)

격리에서 전달된 메시지에 대해 위협이 재검사됩니다.

관련 주제

- 정책, 바이러스, 보안 침해 격리, 847 페이지
- 스팸 격리, 867 페이지

전달

이메일 파이프라인의 전달 단계는 연결, 반송 및 수신자 제한을 포함하여 이메일 처리의 최종 단계에 집중합니다.

관련 주제

- 가상 게이트웨이, 67 페이지
- 전달 제한, 67 페이지
- 도메인 기반 제한, 67 페이지
- 도메인 기반 라우팅, 68 페이지
- 전역 수신 거부, 68 페이지
- 반송 제한, 68 페이지

가상 게이트웨이

가상 게이트웨이 기술을 통해 사용자는 하나의 어플라이언스를 이메일을 보내고 받을 수 있는 여러 가상 게이트웨이 주소로 분리할 수 있습니다. 각 가상 게이트웨이 주소에는 고유한 IP 주소, 호스트 이름과 도메인 및 이메일 전달 대기열이 제공됩니다.

자세한 내용은 호스팅된 모든 도메인에 대한 메일 게이트웨이 구성에 Virtual Gateway™ 기술 사용, 718 페이지를 참고하십시오.

전달 제한

전달 시 사용할 IP 인터페이스를 기반으로 전달에 대한 제한을 설정하고, 어플라이언스가 아웃바운드 메시지 전달에 대해 지정할 수 있는 최대 동시 연결 수를 설정하려면 `deliveryconfig` 명령을 사용합니다.

자세한 내용은 이메일 전달 매개변수 설정, 715 페이지를 참고하십시오.

도메인 기반 제한

각 도메인에 대해 지정된 시간 동안 시스템에서 초과할 수 없는 최대 연결 및 수신자 수를 할당할 수 있습니다. 이 "good neighbor" 테이블은 Mail Policies(메일 정책) > Destination Controls(대상 제어) 페이지(또는 `destconfig` 명령)를 통해 정의됩니다.

자세한 내용은 대상 제어를 사용하여 이메일 전달 제어, 703 페이지를 참고하십시오.

도메인 기반 라우팅

봉투 수신자를 재작성하지 않은 채 특정 도메인에 대한 모든 이메일을 특정 MX(mail exchange) 호스트로 리디렉션하려면 Network(네트워크) > SMTP Routes(SMTP 경로) 페이지(또는 `smtproutes` 명령)를 사용합니다.

자세한 내용은 로컬 도메인용 이메일 라우팅, 665 페이지를 참고하십시오.

전역 수신 거부

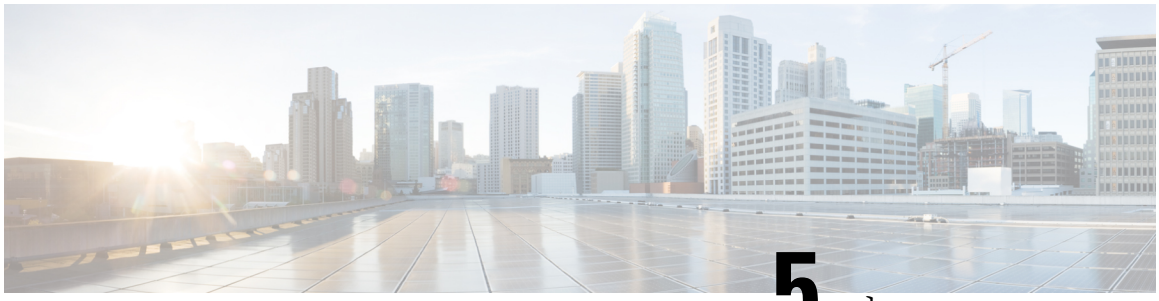
특정 수신자, 수신자 도메인 또는 IP 주소에서 어플라이언스의 메시지를 수신하지 않도록 하려면 Global Unsubscribe(전역 수신 거부)를 사용합니다. Global Unsubscribe(전역 수신 거부)를 활성화하면 시스템은 "전역적으로 수신 거부된" 사용자, 도메인, 이메일 주소 및 IP 주소의 목록을 기준으로 모든 수신자 주소를 점검합니다. 일치하는 이메일은 전송되지 않습니다.

자세한 내용은 전역 수신 거부 사용, 727 페이지를 참고하십시오.

반송 제한

사용자가 만드는 각 리스너에 대해 AsyncOS가 하드 및 소프트 대화형 반송을 처리하는 방법을 구성하려면 Network(네트워크) > Bounce Profiles(반송 프로필) 페이지(또는 `bounceconfig` 명령)를 사용합니다. 반송 프로필을 만든 다음 Network(네트워크) > Listeners(리스너) 페이지(또는 `listenerconfig` 명령)를 사용하여 각 리스너에 프로필을 적용합니다. 메시지 필터를 사용하여 반송 프로필을 특정 메시지에 할당할 수도 있습니다.

반송 프로필에 대한 자세한 내용은 반송된 이메일 전달, 694 페이지 섹션을 참조하십시오.



5 장

이메일을 수신하도록 게이트웨이 구성

이 장에는 다음 섹션이 포함되어 있습니다.

이메일을 수신하도록 게이트웨이 컨피그레이션 개요

어플라이언스는 조직의 이메일 게이트웨이 역할을 하면서 이메일 연결 서비스를 제공하고, 메시지를 수락하고, 적절한 시스템으로 릴레이합니다. 어플라이언스는 인터넷에서 네트워크 내 수신자 호스트로, 그리고 네트워크 내 시스템에서 인터넷으로 이메일 연결 서비스를 제공할 수 있습니다. 일반적으로 이메일 연결 요청은 SMTP(Simple Mail Transfer Protocol)를 사용합니다. 어플라이언스는 기본적으로 SMTP 연결 서비스를 제공하며, 네트워크에 MX(Mail Exchanger)로도 알려진 SMTP 게이트웨이 역할을 합니다.

어플라이언스는 리스너를 사용하여 수신 SMTP 연결 요청의 서비스를 제공합니다. 리스너는 특정 IP 인터페이스에 구성된 이메일 처리 서비스를 설명합니다. 리스너는 인터넷에서 어플라이언스로 들어가거나, 인터넷에 도달하기 위해 네트워크 내 시스템에서 어플라이언스로 들어가는 이메일에 적용됩니다. 리스너를 사용하면 메시지와 연결이 수락되도록 하기 위해, 그리고 메시지를 수신자 호스트로 릴레이하기 위해 충족해야 할 기준을 지정할 수 있습니다. 리스너를 지정된 각 IP 주소에 대한 특정 포트에서 실행되는 "SMTP 데몬"이라고 생각할 수 있습니다. 또한 리스너는 어플라이언스가 어플라이언스에 이메일을 전송하기 위해 시도하는 시스템과 통신하는 방법을 정의합니다.

다음과 같은 유형의 리스너를 만들 수 있습니다.

- 퍼블릭. 인터넷에서 들어오는 이메일 메시지를 수신 대기 및 수락합니다. 퍼블릭 리스너는 다수의 호스트로부터 연결을 수신하고 제한된 수의 수신자에게 메시지를 전달합니다.
- 프라이빗. 네트워크 외부의 인터넷 수신자에게 보내기 위해 네트워크 내 시스템, 특히 내부 그룹웨어 및 이메일 서버(POP/IMAP)에서 오는 이메일 메시지를 수신 대기 및 수락합니다. 프라이빗

리스너는 제한된(알려진) 수의 호스트로부터 연결을 수신하고 다수의 수신자에게 메시지를 전달합니다.

리스너를 만들 때 다음 정보를 지정해야 합니다.

- 리스너 속성**.** 모든 리스너에 적용되는 전역 속성 및 각 리스너에 해당되는 속성을 정의합니다. 예를 들면 특정 리스너에 사용할 IP 인터페이스와 포트를 지정할 수 있으며, 리스너를 퍼블릭 또는 프라이빗으로 지정할 수 있습니다. 이 방법에 대한 자세한 내용은 리스너 작업, 70 페이지 섹션을 참조해 주십시오.
- 리스너에 연결하도록 허용할 호스트**.** 원격 호스트에서의 수신 연결을 제어하는 규칙 집합을 정의합니다. 예를 들면 원격 호스트를 정의하고, 원격 호스트가 리스너에 연결할 수 있는지 여부를 정의할 수 있습니다. 이 방법에 대한 자세한 내용은 Host Access Table을 사용하여 연결할 수 있는 호스트 정의 , 93 페이지 섹션을 참조해 주십시오.
- **(**퍼블릭 리스너 전용**)** 리스너가 메시지를 수락하는 로컬 도메인**.** 퍼블릭 리스너에서 수락할 수신자를 정의합니다. 예를 들어 현재 조직에서 `currentcompany.com` 도메인을 사용 중이고 전에는 `oldcompany.com`을 사용했다면 currentcompany.com과 `oldcompany.com` 모두의 메시지를 수락할 수 있습니다. 이 방법에 대한 자세한 내용은 도메인 이름 또는 수신자 주소를 기반으로 연결 수락 또는 거부, 129 페이지 섹션을 참조해 주십시오.

HAT(Host Access Table) 및 RAT(Recipient Access Table)를 비롯한 리스너에 구성된 설정은 SMTP 대화 중 리스너가 SMTP 서버와 통신하는 방법에 영향을 미칩니다. 이를 통해 어플라이언스는 연결이 닫히기 전에 스패밍 호스트를 차단할 수 있습니다.

그림 ***8:*** 리스너, ***IP*** 인터페이스 및 물리적 이더넷 인터페이스 간 관계

리스너 작업

GUI의 Network(네트워크) > Listeners(리스너) 페이지에서 또는 CLI의 listenerconfig 명령을 사용하여 리스너를 구성합니다.

모든 리스너에 적용되는 전역 설정을 정의할 수 있습니다. 자세한 내용은 리스너에 대한 전역 설정 구성, 72 페이지 섹션을 참고해 주십시오.

어플라이언스에서 리스너로 작업하고 리스너를 구성할 때 다음 규칙과 지침을 고려해 주십시오.

- 구성된 IP 인터페이스당 여러 리스너를 정의할 수 있지만, 각 리스너는 서로 다른 포트를 사용해야 합니다.
- 기본적으로 리스너는 이메일 연결 서비스를 위한 메일 프로토콜로 SMTP를 사용합니다. 그러나 QMQP(Quick Mail Queuing Protocol)를 사용하여 이메일 연결 서비스를 제공하도록 어플라이언스를 구성할 수도 있습니다. 이렇게 하려면 `listenerconfig` CLI 명령을 사용합니다.

- 리스너는 IPv4(Internet Protocol version 4) 및 IPv6(version 6) 주소를 모두 지원합니다. 단일 리스너에서 두 프로토콜 버전 중 하나 또는 모두를 사용할 수 있습니다. 리스너는 메일 전달에 연결하는 호스트와 동일한 프로토콜 버전을 사용합니다. 예를 들어 리스너가 IPv4 및 IPv6 모두에 대해 구성되어 있고 IPv6을 사용하는 호스트에 연결된 경우 리스너는 IPv6을 사용합니다. 그러나 리스너가 IPv6 주소만 사용하도록 구성된 경우 IPv4 주소만 사용하는 호스트에 연결할 수 없습니다.
- 시스템 설정 마법사를 실행하면 어플라이언스에 적어도 하나의 리스너가 기본값으로 구성됩니다. 그러나 리스너를 수동으로 만들면 AsyncOS에서는 SBRS 기본값을 사용하지 않습니다.
- **C170** 및 **C190** 어플라이언스: 기본적으로 시스템 설정 마법사는 인터넷으로부터의 메일 수신 및 내부 네트워크로부터의 이메일 릴레이를 위한 하나의 퍼블릭 리스너를 구성하도록 안내합니다. 즉, 하나의 리스너가 두 가지 기능을 수행할 수 있습니다.
- 어플라이언스의 테스트와 트러블슈팅에 도움이 되도록, 퍼블릭 또는 프라이빗 리스너 대신 "블랙홀" 유형의 리스너를 만들 수 있습니다. 블랙홀 리스너를 만들 때, 메시지를 삭제 전에 디스크에 기록할지 여부를 선택할 수 있습니다. (자세한 내용은 "테스트 및 트러블슈팅" 장을 참조해 주십시오.) 메시지를 삭제 전에 디스크에 기록하면 수신 속도 및 대기열의 속도를 측정하는 데 도움이 될 수 있습니다. 메시지를 디스크에 기록하지 않는 리스너에서는 메시지 생성 시스템에서 수신하는 순수한 속도를 측정할 수 있습니다. 리스너 유형은 CLI의 `listenerconfig` 명령을 통해서만 사용 가능합니다.

그림 - 이더넷 인터페이스가 셋 이상인 어플라이언스 모델의 퍼블릭 및 프라이빗 리스너에서는 이더넷 인터페이스가 셋 이상인 어플라이언스 모델에서 시스템 설정 마법사로 만든 일반적인 이메일 게이트웨이 구성을 보여 줍니다. 첫 번째 인터페이스에서 인바운드 연결을 지원할 퍼블릭 리스너와 두 번째 IP 인터페이스에서 아웃바운드 연결을 지원할 프라이빗 리스너, 이렇게 두 개의 리스너가 생성됩니다.

그림 - 이더넷 인터페이스가 둘뿐인 어플라이언스 모델의 퍼블릭 리스너에서는 이더넷 인터페이스가 둘뿐인 어플라이언스 모델에서 시스템 설정 마법사로 만든 일반적인 이메일 게이트웨이 구성을 보여줍니다. 단일 IP 인터페이스의 한 퍼블릭 리스너는 인바운드 연결과 아웃바운드 연결을 모두 지원하도록 생성됩니다.

그림 ***9:*** 이더넷 인터페이스가 셋 이상인 어플라이언스 모델의 퍼블릭 및 프라이빗 리스너

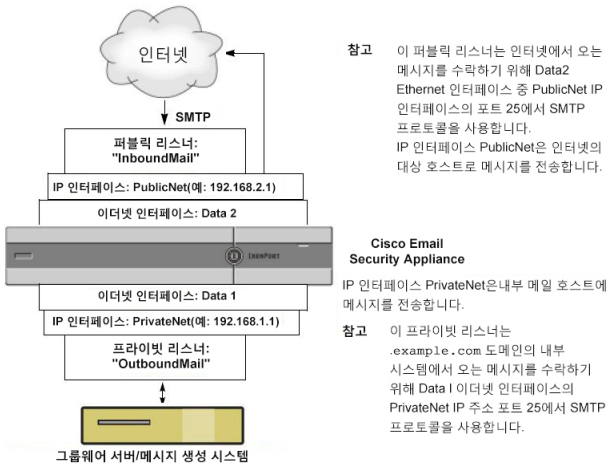
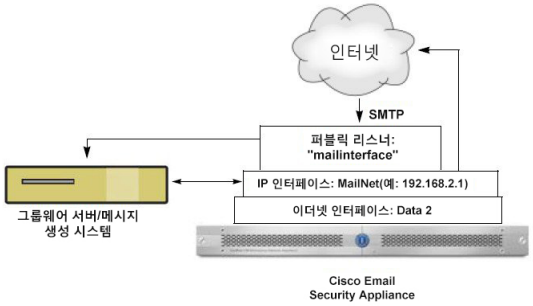


그림 *10:* 이더넷 인터페이스가 둘뿐인 어플라이언스 모델의 퍼블릭 리스너



참고 이 퍼블릭 리스너는 인터넷에서 오는 메시지를 수락하고 `.example.com` 도메인의 내부 시스템에서 오는 메시지를 릴레이하기 위해 Data2 이더넷 인터페이스의 PublicNet IP 주소 포트 25에서 SMTP 프로토콜을 사용합니다. IP 인터페이스 MailNet은 인터넷의 대상 호스트 및 내부 메일 호스트에 메시지를 전송합니다.

리스너에 대한 전역 설정 구성

리스너에 대한 전역 설정은 어플라이언스에 구성된 모든 리스너에 영향을 미칩니다. 리스너가 IPv4(Internet Protocol 버전 4) 및 IPv6(버전 6) 주소가 모두 있는 인터페이스를 사용하는 경우 리스너 설정은 IPv4 및 IPv6 트래픽에 모두 적용됩니다.

단계 **1** **Network(**네트워크**) > Listeners(**리스너**)**를 선택합니다.

단계 **2** **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **3** 다음 표에 정의된 설정을 변경합니다.

표 *5:* 리스너 전역 설정

전역 설정	설명
최대 동시 연결 수	리스너에 대한 최대 동시 연결 수를 설정합니다. C3x0 및 C6x0 모델의 기본값은 300이고, C1x0 모델의 기본값은 50입니다. 리스너에서 IPv4 및 IPv6 연결을 모두 수락하는 경우 연결 수는 둘 사이에서 나누어집니다. 예를 들어 최대 동시 연결 수가 300이면 IPv4 및 IPv6 연결의 합은 300을 넘을 수 없습니다.
Maximum Concurrent TLS Connections(최대 동시 TLS 연결 수)	결합된 모든 리스너 간 최대 동시 TLS 연결 수를 설정합니다. 기본값은 100입니다. 리스너에서 IPv4 및 IPv6 TLS 연결을 모두 수락하는 경우 연결 수는 둘 사이에서 나누어집니다. 예를 들어 최대 동시 연결 수가 100이면 IPv4 및 IPv6 연결의 합은 100을 넘을 수 없습니다.

전역 설정	설명
수신 카운터 리셋 기간:	주입 제어 카운터가 재설정되는 시기를 조정할 수 있습니다. 상당히 많은 수의 서로 다른 IP 주소에 대한 카운터를 유지 관리하는 매우 분주한 시스템의 경우 좀 더 자주 재설정되도록 카운터를 구성하면(예: 60분이 아니라 15분마다), 데이터가 관리할 수 없는 크기로 커져 시스템 성능에 영향을 주는 상황을 피할 수 있습니다. 현재 기본값은 1시간입니다. 1분(60초)에서 4시간(14,400초)까지 기간을 지정할 수 있습니다. 주입 제어 주기 , 119 페이지를 참조하십시오.
Timeout Period for Unsuccessful Inbound Connections(인바운드 연결 실패 시간 초과 기간)	AsyncOS가 실패한 인바운드 연결을 닫기 전에 그대로 유지할 기간을 설정합니다. 실패한 연결은 성공적인 메시지 주입 발생 없이 SMTP 또는 ESMTP 명령을 계속 실행할 수 있는 SMTP 대화일 수 있습니다. 지정된 시간 초과에 도달하면 오류가 전송되고 연결이 끊어집니다. “421 Timed out waiting for successful message injection, disconnecting.(421 성공 메시지 주입 대기 시간 초과, 연결 끊는 중.)” 메시지를 성공적으로 주입하기 전에는 연결이 실패로 간주됩니다. 퍼블릭 리스너의 SMTP 연결에만 사용 가능. 기본값은 5분입니다.
Total Time Limit for All Inbound Connections(모든 인바운드 연결에 대한 총 시간 제한)	AsyncOS가 인바운드 연결을 닫기 전에 그대로 유지할 기간을 설정합니다. 이 설정의 목적은 허용되는 최대 연결 시간을 적용하여 시스템 리소스를 유지하려는 것입니다. 이 최대 연결 시간의 약 80%에 도달하면 다음 메시지가 표시됩니다. “421 Exceeded allowable connection time, disconnecting.(421 허용되는 연결 시간 초과, 연결 끊는 중.)” 최대 연결 시간의 80%를 초과하면 메시지 중간에 연결이 끊기는 것을 막기 위해 어플라이언스는 연결 끊기를 시도합니다. 인바운드 연결이 최대 연결 시간의 80%에 도달할 정도로 오래 열려 있는 경우 문제가 발생할 수 있습니다. 시간 제한을 지정할 때는 이 임계값에 유념하시기 바랍니다. 퍼블릭 리스너의 SMTP 연결에만 사용 가능. 기본값은 15분입니다.
Maximum size of subject(제목 최대 크기)	지정된 제한을 벗어나지 않는 메시지는 수락되고 다른 메시지는 거부됩니다. 이 값을 0으로 설정하면 제한이 적용되지 않습니다.

전역 설정	설명
HAT 지연 거부	메시지 수신자 레벨에서 HAT 거부를 수행할지 여부를 구성합니다. 기본적으로 HAT 거부 연결은 SMTP 대화가 시작될 때 배너 메시지와 함께 닫힙니다. HAT "Reject(거부)" 설정 때문에 이메일이 거부되는 경우 AsyncOS는 SMTP 대화가 시작될 때보다는 메시지 수신자 레벨(RCPT TO)에서 거부를 수행할 수 있습니다. 이렇게 메시지를 거부하면 메시지 거부가 지연되고 메시지가 반송되어, AsyncOS는 거부된 메시지에 대해 좀 더 자세한 정보를 보유하게 됩니다. 예를 들어 메시지가 차단된 주소 및 각 수신자 주소에서 온 메일을 볼 수 있습니다. HAT 거부를 지연하면 MTA 전송이 여러 재시도를 수행할 가능성이 줄어듭니다. HAT 지연 거부를 활성화하면 다음 동작이 발생합니다. MAIL FROM 명령이 수락되면 메시지 개체가 생성되지 않습니다. 이메일 전송 액세스 권한이 거부됨을 설명하는 텍스트와 함께 모든 RCPT TO 명령이 거부됩니다. 전송 MTA가 SMTP AUTH로 인증되는 경우 RELAY 정책이 부여되고 정상적인 메일 전달이 허용됩니다. CLI의 `listenerconfig --> setup` 명령을 통해서만 구성할 수 있습니다.

단계 **4** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- 여러 인코딩이 포함된 메시지에 대한 설정, 74 페이지

여러 인코딩이 포함된 메시지에 대한 설정

다음 매개변수에 대한 메시지 인코딩을 수정하는 한편 어플라이언스의 동작을 정의할 수 있습니다.

- 헤더
- 태그 없는 비 ASCII 헤더
- 일치하지 않는 바닥글 또는 머리글 인코딩

이 동작을 구성하려면 CLI의 localeconfig 명령을 사용합니다.

참고 이 동작은 웹 인터페이스를 사용하여 구성할 수 없습니다.

샘플 CLI 트랜스크립트는 면책조항 스탬프 및 다중 인코딩, 628 페이지 섹션을 참조해 주십시오.

웹 인터페이스를 사용하여 리스너를 만들어 연결 요청 수신 대기

단계 **1** `Network(네트워크) > Listener(리스너)`를 선택합니다.

단계 **2** **Add Listener(**리스너 추가**)**를 클릭합니다.

단계 **3** 다음 표에 정의된 설정을 구성합니다.

표 ***6:*** 리스너 설정

이름	향후 참조를 위해 리스너에 제공하는 고유한 별칭. 리스너에 대해 정의하는 이름은 대/소문자를 구분합니다. AsyncOS에서는 두 개의 동일한 리스너 이름을 만들 수 없습니다.
리스너 유형	다음 리스너 유형 중 하나를 선택합니다. • 퍼블릭. 퍼블릭 리스너는 인터넷에서 이메일을 수신하기 위한 기본 특성을 포함합니다. • 프라이빗. 프라이빗 리스너는 프라이빗(내부) 네트워크에만 사용됩니다.
인터페이스	리스너를 만들도록 구성된 어플라이언스 IP 인터페이스 및 TCP 포트를 선택합니다. 인터페이스에서 사용하는 IP 주소의 버전에 따라 리스너는 IPv4 주소, IPv6 주소 또는 두 버전의 연결을 수락합니다. 기본적으로 SMTP는 포트 25를 사용하고 QMQP는 포트 628을 사용합니다.
반송 프로필	반송 프로필을 선택합니다(CLI의 `bounceconfig` 명령을 통해 생성되는 반송 프로필은 목록에서 사용 가능합니다. 새 반송 프로필 만들기, 701 페이지 섹션을 참조해 주십시오).
면책조항 위	이메일의 위 또는 아래에 어태치할 면책조항을 선택합니다. (Mail Policies(메일 정책) > Text Resources(텍스트 리소스) 페이지 또는 CLI의 `textconfig` 명령을 통해 생성되는 면책조항은 목록에서 사용 가능합니다. "텍스트 리소스" 장을 참조해 주십시오.)
면책조항 아래	이메일의 위 또는 아래에 어태치할 면책조항을 선택합니다. (Mail Policies(메일 정책) > Text Resources(텍스트 리소스) 페이지 또는 CLI의 `textconfig` 명령을 통해 생성되는 면책조항은 목록에서 사용 가능합니다. "텍스트 리소스" 장을 참조해 주십시오.)
SMTP 인증 프로필	SMTP 인증 프로필을 지정합니다.
인증서	리스너에 대한 TLS 연결을 위한 인증서를 지정합니다 (Network(네트워크) > Certificates(인증서) 페이지를 통해 또는 CLI의 `certconfig` 명령을 추가되는 인증서는 목록에서 사용 가능합니다. 다른 MTA와의 통신 암호화 개요, 645 페이지 섹션을 참조해 주십시오).

단계 **4** (선택 사항) 다음 표에 정의된 것처럼 SMTP "`MAIL FROM`" 및 "`RCPT TO`" 명령에서 구문 분석을 제어하기 위한 설정을 구성합니다.

설정	설명
주소 파서 유형	어플라이언스가 다음 파서 유형 중 하나를 사용하여 RFC2821 표준을 얼마나 엄격하게 준수할지를 선택합니다. 엄격 모드**:** • 엄격 모드는 RFC 2821을 준수하려고 시도합니다. 엄격 모드에서 주소 파서는 다음과 같은 예외/개선 사항으로 RFC 2821 규칙을 준수합니다. • "MAIL FROM: <joe@example.com>"과 같이 콜론 뒤에 공백을 추가할 수 있습니다. • 도메인 이름에는 밑줄이 허용됩니다. • "MAIL FROM" 및 RCPT TO" 명령은 대/소문자를 구분합니다. • 마침표는 특별하게 취급되지 않습니다(예: RFC 2821에서는 사용자 이름 "J.D."를 허용하지 않음). 기술적으로 RFC 2821을 위반하는 다음의 몇몇 추가 옵션이 활성화될 수 있습니다. 느슨한 모드**:** 느슨한 파서는 기본적으로 AsyncOS의 이전 버전에서 오는 기존 동작입니다. 느슨한 파서는 최선을 다해 이메일 주소를 "검색"하고 다음을 수행합니다. • 코멘트를 무시합니다. 중첩된 코멘트(괄호에 있는 모든 명령)를 지원하고 무시합니다. • "RCPT TO" 및 "MAIL FROM" 명령으로 제공되는 이메일 주소 주변의 꺾쇠괄호를 요구하지 않습니다. • 여러 중첩된 꺾쇠괄호를 허용합니다(가장 깊은 중첩 레벨에서 이메일 주소 검색).
8비트 사용자 이름 허용	활성화하면, 주소의 사용자 이름 부분에 이스케이프 없이 8비트 문자가 허용됩니다.
8비트 도메인 이름 허용	활성화하면 주소의 도메인 부분에서 8비트 문자가 허용됩니다.

설정	설명
A부분 도메인 허용	활성화하면 부분 도메인이 허용됩니다. 부분 도메인은 도메인이 아니거나 점이 없는 도메인일 수 있습니다. 부분 도메인의 예는 다음과 같습니다. • foo • foo@ • foo@bar Default Domain(기본 도메인) 기능이 제대로 작동하려면 이 옵션을 반드시 활성화해야 합니다. **Add Default Domain(**기본 도메인 추가**):** 인증된 도메인 이름이 없는 이메일 주소에 사용할 기본 도메인. SMTP Address Parsing(SMTP 주소 구문 분석) 옵션에서 Allow Partial Domains(부분 도메인 허용)가 활성화되어 있지 않으면 이 옵션은 비활성화됩니다. 이는 인증된 도메인 이름이 포함되지 않은 발신자 및 수신자 주소에 "기본 발신자 도메인"을 추가하여, 리스너가 릴레이하는 이메일을 수정하는 방법에 영향을 미칩니다. (다시 말하면 리스너가 "bare(베어)" 주소를 처리하는 방법을 맞춤화할 수 있습니다). 발신자 주소에 회사 도메인을 추가(첨부)하지 않고 이메일을 보내는 레거시 시스템이 있는 경우 이 기능을 사용하여 기본 발신자 도메인을 추가합니다. 예를 들어, 레거시 시스템에서 이메일 발신자로 "`joe`" 문자열만 입력하는 이메일을 자동으로 만들 수 있습니다. 기본 발신자 도메인을 변경하면 "joe"에 "`@yourdomain.com`"이 첨부되어 `joe@yourdomain.com`이라는 인증된 발신자 이름이 만들어집니다.
소스 라우팅	"MAIL FROM" 및 "RCPT TO" 주소에서 소스 라우팅이 탐지되는 경우 동작을 결정합니다. 소스 라우팅은 라우팅을 지정하기 위해 여러 '@' 문자를 사용하는 이메일 주소의 특별한 양식입니다(예: @one.dom@two.dom:joe@three.dom). "reject"로 설정된 경우 주소가 거부됩니다. "strip"인 경우 주소의 소스 라우팅 부분이 삭제되고 메시지가 정상적으로 주입됩니다.
알 수 없는 주소 리터럴	시스템에서 다룰 수 없는 주소 리터럴이 수신되는 경우의 동작을 결정합니다. 현재 이것은 IPv4를 제외한 모든 것입니다. 따라서 예를 들어 IPv6 주소 리터럴의 경우 프로토콜 수준에서 거부할 수도 있고, 수락 후 즉시 하드 반송(hard bounce)할 수도 있습니다. 리터럴이 포함된 수신자 주소는 즉각적인 하드 반송을 일으킵니다. 발신자 주소가 전달될 수 있습니다. 메시지를 전달할 수 없는 경우 하드 반송이 하드 반송됩니다(이중 하드 반송). 거부되는 경우 발신자 주소와 수신자 주소 모두 프로토콜 레벨에서 즉시 거부됩니다.
사용자 이름에 다음 문자 사용 금지	여기에 입력된 문자(예: % 또는 !)를 포함하는 사용자 이름은 거부됩니다.

단계 **5** (선택 사항) 다음 표에 정의된 대로 리스너의 동작을 맞춤화하기 위한 고급 설정을 구성합니다.

설정	설명
최대 동시 연결 수	허용되는 최대 연결 수.

설정	설명
TCP 수신 대기열 큐 크기	SMTP 서버가 수락하기 전에 AsyncOS가 관리하게 될 연결의 백로그.
CR 및 LF 처리	Bare CR(Carriage Return) 및 LF(Line Feed) 문자를 포함하는 메시지의 처리 방법을 선택합니다. • **Clean(**삭제**).** 메시지를 허용하지만, Bare CR 및 LF 문자를 CRLF 문자로 변환합니다. • **Reject(**거부**).** 메시지를 거부합니다. • **Allow(**허용**).** 메시지를 허용합니다.
수신 헤더 추가	수신된 헤더를 모든 수신된 이메일에 추가 리스너는 또한 각 메시지에서 Received(수신됨): 헤더를 추가함으로써, 릴레이하는 이메일을 수정합니다. Received(수신됨): 헤더를 포함하지 않으려면 이 옵션을 사용하여 비활성화할 수 있습니다. 참고 Received(수신됨): 헤더는 작업 대기열 프로세싱 내에서 메시지에 추가되지 않습니다. 오히려 전달을 위해 메시지가 대기열이 추가되었을 때 추가됩니다. 수신된 헤더를 비활성화하는 것은 인프라 외부를 이동하는 메시지에서 내부 서버의 IP 주소나 호스트 이름을 드러냄으로써 네트워크 토폴로지가 노출되지 않도록 하는 방법입니다. 수신된 헤더를 비활성화할 때에는 주의를 기울여 주십시오.
SenderBase IP 프로파일링 사용	SenderBase IP Profiling의 비활성화 여부를 선택하고 다음 설정을 구성합니다. • **Timeout for Queries(**쿼리 시간 초과**).** 어플라이언스가 SenderBase Reputation Service에서 쿼리된 정보를 캐시하는 기간을 정의합니다. • **SenderBase Timeout per Connection(**연결당 **Senderbase** 시간 초과**).** 어플라이언스가 SMTP 연결당 SenderBase 정보를 캐시하는 기간을 정의합니다.

단계 **6** (선택 사항) 다음 표에 정의된 대로 이 리스너와 연결된 LDAP 쿼리를 제어하기 위한 설정을 구성합니다.

리스너에서 LDAP 쿼리를 활성화하려면 이러한 설정을 사용합니다. 이 옵션을 사용하기 전에 먼저 LDAP 쿼리를 만들어야 합니다. 각 쿼리 유형에는 구성해야 할 별도의 하위 섹션이 있습니다. 하위 섹션을 확장하기 위한 쿼리의 유형을 클릭합니다.

LDAP 쿼리 만들기에 대한 자세한 내용은 LDAP 쿼리, 735 페이지 섹션을 참조해 주십시오.

쿼리 유형	설명
수락 쿼리	수락 쿼리의 경우 목록에서 사용할 쿼리를 선택합니다. 작업 대기열 프로세싱 중에 또는 SMTP 대화 중에 LDAP 수락 발생 여부를 지정할 수 있습니다. 작업 대기열 프로세싱 중 LDAP 수락의 경우, 일치하지 않는 수신자에 대한 동작을 지정합니다(반송 또는 삭제). SMTP 대화 중 LDAP 수락의 경우, LDAP 서버에 도달할 수 없을 때 메일을 처리하는 방법을 지정합니다. 코드 및 맞춤화 응답으로 메시지를 허용하거나 연결을 삭제하도록 선택할 수 있습니다. 마지막으로, SMTP 대화 중 DHAP(Directory Harvest Attack Prevention) 임계값에 도달할 때 연결을 삭제할지 여부를 선택합니다. SMTP 대화에서 수신자 검증을 수행하면 잠재적으로 여러 LDAP 쿼리 간 레이턴시를 줄일 수 있습니다. 따라서 대화형 LDAP 수락을 활성화하면 디렉터리 서버에서 로드가 증가할 수 있습니다. 자세한 내용은 LDAP 쿼리의 개요, 735 페이지를 참조하십시오.
라우팅 쿼리	라우팅 쿼리의 경우 목록에서 쿼리를 선택합니다. 자세한 내용은 LDAP 쿼리의 개요, 735 페이지 섹션을 참조해 주십시오.
Masquerade(가장) 쿼리	가장 쿼리의 경우 목록에서 쿼리를 선택하고, 마스커레이드할 주소를 선택합니다(예: From 또는 CC 헤더 주소). 자세한 내용은 LDAP 쿼리의 개요, 735 페이지 섹션을 참조해 주십시오.
그룹 쿼리	그룹 쿼리의 경우 목록에서 쿼리를 선택합니다. 자세한 내용은 LDAP 쿼리의 개요, 735 페이지 섹션을 참조해 주십시오.

단계 **7** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

부분 도메인, 기본 도메인 및 형식이 잘못된 MAIL FROM, 79 페이지

부분 도메인, 기본 도메인 및 형식이 잘못된 **MAIL FROM**

봉투 발신자(envelope sender) 확인을 활성화하거나 SMTP Address Parsing(SMTP 주소 구문 분석) 옵션에서 리스너에 대해 부분 도메인 허용을 비활성화하는 경우, 해당 리스너에 대한 기본 도메인 설정이 더 이상 사용되지 않습니다.

이러한 기능은 상호 배타적입니다.

CLI로 리스너를 만들어 연결 요청 수신 대기

다음 표에는 리스너 만들기 및 수정과 관련된 작업에 사용되는 몇 가지 listenerconfig 하위 명령이 나열되어 있습니다.

표 *7:* 리스너 생성 작업

리스너 생성 작업	명령 및 하위 명령
새 리스너 만들기	`listenerconfig -> new`
리스너의 전역 설정 편집	`listenerconfig -> setup`
리스너에 대한 반송 프로필 지정	`bounceconfig, listenerconfig-> edit -> bounceconfig`
면책조항을 리스너와 연결	`textconfig, listenerconfig -> edit -> setup -> footer`
SMTP 인증 구성	`smtpauthconfig, listenerconfig -> smtpauth`
SMTP 주소 구문 분석 구성	`textconfig, listenerconfig -> edit -> setup -> address`
리스너의 기본 도메인 구성	`listenerconfig -> edit -> setup -> defaultdomain`
이메일에 Received 헤더 추가	`listenerconfig -> edit -> setup -> received`
Bare CR 및 LF 문자를 CRLF로 변경	`listenerconfig -> edit -> setup -> cleansmtp`
Host Access Table 수정	`listenerconfig -> edit -> hostaccess`
로컬 도메인 또는 특정 사용자(RAT)에 대한 이메일 수락(퍼블릭 리스너 전용)	`listenerconfig -> edit -> rcptaccess`
리스너에서 대화 암호화(TLS)	`certconfig, listenerconfig -> edit`
인증서 선택(TLS)	`listenerconfig -> edit -> certificate`

listenerconfig 명령에 대한 자세한 내용은 AsyncOS for Cisco Email Security Appliance용 CLI 참조 설명서를 참조하십시오.

이메일 라우팅 및 전달 구성에 대한 자세한 내용은 라우팅 및 전달 기능 구성, 665 페이지 섹션을 참조해 주십시오.

관련 주제

고급 HAT 매개변수, 81 페이지

고급 HAT 매개변수

다음 표에서는 고급 HAT 매개변수의 구문을 정의합니다. 아래의 숫자 값에 대해, 킬로바이트를 나타내는 **k** 또는 메가바이트를 나타내는 **M**을 뒤에 추가할 수 있습니다. 문자가 없는 값은 바이트로 간주됩니다. 다음 표에 별표로 표시된 매개변수는 에 나와 있는 변수 구문을 지원합니다.

표 ***8:*** 고급 ***HAT*** 매개변수 구문

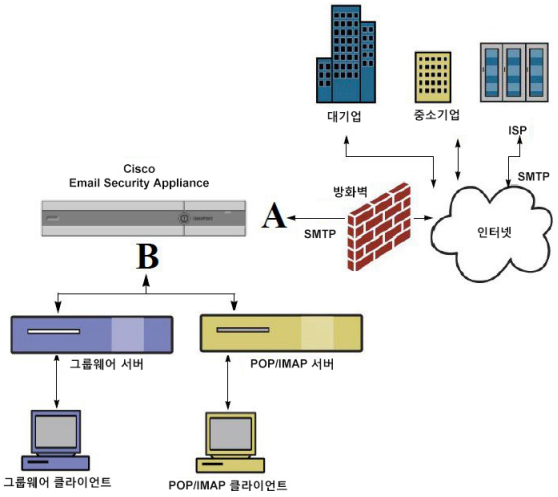
매개변수	구문	값	값 예
연결당 최대 메시지 수	`max_msgs_per_session`	번호	`1000`
Maximum recipients per message(메시지당 최대 수신자 수)	`max_rcpts_per_msg`	번호	`10000` `1k`
최대 메시지 크기	`max_message_size`	번호	`1048576` `20M`
이 리스너에 대해 허용되는 최대 동시 연결 수	`max_concurrency`	번호	`1000`
SMTP 배너 코드	`smtp_banner_code`	번호	`220`
SMTP 배너 텍스트 (*)	`smtp_banner_text`	문자열	`Accepted`
SMTP 거부 배너 코드	`smtp_banner_code`	번호	`550`
MTP 거부 배너 텍스트 (*)	`smtp_banner_text`	문자열	`Rejected`
SMTP 배너 호스트 이름 덮어쓰기	`use_override_hostname`	on | off | default	`default`
	`override_hostname`	문자열	`newhostname`
Use TLS(TLS 사용)	`tls`	on | off | required	`on`
Use anti-spam scanning(안티스팸 검사 사용)	`spam_check`	on | off	`off`
바이러스 검사 사용	`virus_check`	on | off	`off`
시간당 최대 수신자 수	`max_rcpts_per_hour`	번호	`5k`

매개변수	구문	값	값 예
시간당 최대 수신자 수 오류 코드	`max_rcpts_per_hour_code`	번호	`452`
시간당 최대 수신자 수 텍스트 (*)	`max_rcpts_per_hour_text`	문자열	`Too manyrecipients`
SenderBase 사용	`use_sb`	on | off	`on`
SenderBase Reputation 점수 정의	`sbrs[value1:value2]`	-10.0- 10.0	`sbrs[-10:-7.5]`
DHAP(Directory Harvest Attack Prevention): 시간당 최대 잘못된 수신자 수	`dhap_limit`	번호	`150`

Enterprise Gateway Configuration

이 컨피그레이션에서 Enterprise Gateway 컨피그레이션은 인터넷에서 온 이메일을 수락하고 이메일을 그룹웨어 서버, POP/IMAP 서버 또는 기타 MTA로 릴레이합니다. 동시에 엔터프라이즈 게이트웨이는 인터넷의 수신자에게 릴레이하기 위해 그룹웨어 서버 및 기타 이메일 서버에서 온 SMTP 메시지를 수락합니다.

그림 ***11: Enterprise Gateway***용 퍼블릭 및 프라이빗 리스너

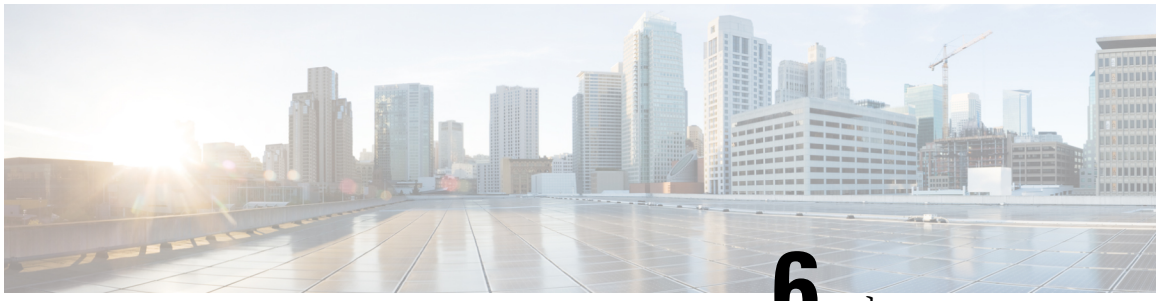


이 컨피그레이션에는 최소 두 개의 리스너가 필요합니다.

- 한 리스너는 인터넷에서 오는 메일을 수락하도록 특별히 구성되었습니다.
- 한 리스너는 내부 그룹웨어 및 이메일 서버(POP/IMAP)에서 오는 메일을 수락하도록 특별히 구성되었습니다.

서로 다른 공용 및 사설 네트워크에 대한 퍼블릭 및 프라이빗 리스너를 만들면 보안, 정책 시행, 보고 및 관리용 이메일을 구분할 수 있습니다. 예를 들어 퍼블릭 리스너에서 수신된 이메일은 구성된 안티스팸 엔진 및 안티바이러스 검사 엔진에 의해 기본적으로 검사되는 반면, 프라이빗 리스너에서 수신된 이메일은 검사되지 않습니다.

엔터프라이즈 게이트웨이용 퍼블릭 및 프라이빗 리스너에서는 이 엔터프라이즈 게이트웨이 구성의 어플라이언스에서 구성된 하나의 퍼블릭 리스너(A) 및 하나의 프라이빗 리스너(B)를 보여 줍니다.



6 장

발신자 평판 필터링

이 장에는 다음 섹션이 포함되어 있습니다.

발신자 평판 필터링 개요

발신자 평판 필터링은 스팸 방지의 첫 번째 레이어로서, 사용자는 Cisco SenderBase™ Reputation Service에 의해 결정된 발신자의 신뢰를 기반으로 이메일 게이트웨이를 통과하는 메시지를 제어할 수 있습니다.

어플라이언스에서는 잘 알려졌거나 평판이 좋은 발신자(예: 고객 및 파트너)가 보낸 메시지를 수락하고 내용 검사 없이 최종 사용자에게 직접 전달할 수 있습니다. 알려지지 않았거나 평판이 좋지 않은 발신자가 보낸 메시지는 안티스팸 및 안티바이러스 검사 등 내용 검사를 받을 수 있으며, 각 발신자로부터 수락할 메시지 수를 조절할 수도 있습니다. 평판이 최악인 이메일 발신자의 경우 연결이 거부되거나 기본 설정을 기반으로 메시지가 반송될 수 있습니다.

참고 파일 평판 필터링은 별도의 서비스입니다. 자세한 내용은 File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석), 461 페이지 섹션을 참조해 주십시오.

SenderBase Reputation Service

Cisco SenderBase Reputation Service는 SenderBase Affiliate 네트워크의 전역 데이터를 사용하여 불만 점수, 메시지 볼륨 통계, 그리고 공개 블랙리스트 및 오픈 프록시 리스트의 데이터를 기반으로 이메일 발신자에게 SenderBase Reputation Score를 할당합니다. SenderBase Reputation Score는 합법적인 발신자를 스팸 소스와 구별하는 데 도움이 됩니다. 평판 점수가 낮은 발신자의 메시지를 차단하기 위한 임계값을 설정할 수 있습니다.

SenderBase Security Network 웹사이트(www.senderbase.org)에서는 최신 이메일 및 웹 기반 위협의 전체적인 개요를 제공합니다. 여기에서는 또한 IP 주소, URI, 도메인 등을 기반으로 평판 점수를 조회할 수 있습니다.

관련 주제

- SBRS(SenderBase Reputation Score) , 86 페이지
- SenderBase 평판 필터 작동 방식 , 87 페이지
- 서로 다른 발신자 평판 필터링 접근 방식에 대한 권장 설정 , 87 페이지
- 신종 바이러스 필터(Outbreak Filter), 399 페이지
- 이메일 보안 모니터 사용, 793 페이지

SBRS(SenderBase Reputation Score)

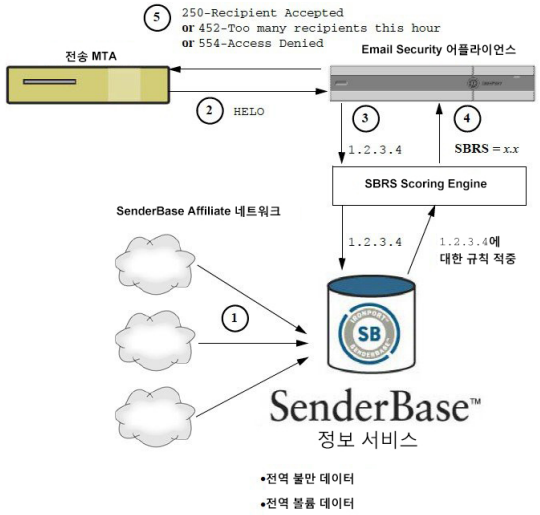
SBRS(SenderBase Reputation Score)는 SenderBase Reputation Service의 정보를 기반으로 IP 주소에 할당된 숫자 값입니다. SenderBase Reputation Service는 25개가 넘는 공개 블랙리스트 및 오픈 프록시 리스트에서 데이터를 수집하고 이를 SenderBase의 전역 데이터와 결합하여 -10.0에서 +10.0의 점수를 할당합니다.

점수	의미
-10.0	스팸 소스일 가능성이 매우 높음
0	중립, 또는 추천할 만한 충분한 정보 없음
+10.0	신뢰할 수 있는 발신자일 가능성이 매우 높음

점수가 낮을수록(음수) 메시지가 스팸일 가능성이 높습니다. 점수가 -10.0이면 메시지는 스팸으로 "인증"되는 반면, 점수가 10.0이면 합법적인 것으로 "인증"됩니다.

SBRS를 사용하면 신뢰도를 기반으로 발신자에게 메일 플로우 정책을 적용하도록 어플라이언스를 구성할 수 있습니다. (시스템에서 처리하는 메시지에 추가 작업을 수행하도록 SenderBase Reputation Score에 대한 "임계값"을 지정하는 메시지 필터를 만들 수도 있습니다. 자세한 내용은 "SenderBase Reputation 규칙, 176 페이지" 및 "안티스팸 시스템 우회 작업, 223 페이지" 섹션을 참조하십시오.)

그림 *12: SenderBase Reputation Service*



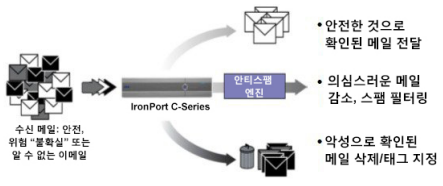
1. SenderBase Affiliate 네트워크에서 실시간 전역 데이터 전송
2. 전송 MTA에서 어플라이언스에 연결
3. 어플라이언스에서 IP 주소 연결을 위해 전역 데이터 검사
4. SenderBase Reputation Service에서 이 메시지가 스팸일 가능성을 계산하고 SenderBase Reputations Score 할당
5. Cisco에서 SenderBase Reputation Score를 기반으로 응답 반환

SenderBase 평판 필터 작동 방식

발신자 평판 필터 기술의 목표는 어플라이언스에서 사용 가능한 나머지 보안 서비스 프로세싱을 가능한 한 많은 메일이 피해갈 수 있도록 하는 것입니다. (이메일 파이프라인 이해, 57 페이지 참조)

발신자 평판 필터링이 활성화되면 알려진 불량 발신자의 메일은 단순히 거부됩니다. 글로벌 2000 기업의 알려진 양호한 메일은 자동으로 스팸 필터를 우회하여 오탐의 가능성을 줄입니다. 알 수 없는 이메일 또는 "그레이" 이메일은 안티 스팸 검사 엔진으로 라우팅됩니다. 이 접근 방식을 사용하여 발신자 평판 필터는 콘텐츠 필터의 부하를 최대 50% 줄일 수 있습니다.

그림 *13:* 발신자 평판 필터링 예



서로 다른 발신자 평판 필터링 접근 방식에 대한 권장 설정

엔터프라이즈의 목표에 따라 보수적, 중도적 또는 적극적 접근 방식을 구현할 수 있습니다.

접근 방식	특징	**Whitelist**(화이트리스트)	**Blacklist**(블랙리스트)	**Suspectlist**(의심 리스트)	**Unknownlist**(알려지지 않은 리스트)
		SenderBase Reputation Score 범위**:**			
보수적	영(0)에 가까운 오탐, 더 나은 성능	7 ~ 10	-10 ~ -4	-4 ~ -2	-2 ~ 7
사회 (설치 기본값)	오탐 거의 없음, 고성능	SenderBase Reputation Score가 사용되지 않습니다.	-10 ~ -3	-3 ~ -1	-1 ~ +10
적극적	약간의 오탐, 최대 성능. 이 옵션을 선택하면 대부분의 메일이 안티스팸 프로세싱을 피하게 됩니다.	4 ~ 10	-10 ~ -2	-2 ~ -1	-1 ~ 4
모든 접근 방식		메일 플로우 정책**:**			
		신뢰성	차단됨	조절됨	허용됨

리스너에 대한 발신자 평판 필터링 점수 임계값 수정

기본 SBRS(SenderBase Reputation Service) 점수 임계값을 변경하거나 평판 필터링을 위한 발신자 그룹을 추가하려면 다음 절차를 사용해 주십시오.

참고 SBRS 점수 임계값과 관련된 기타 설정 및 메일 플로우 정책 설정은 Host Access Table을 사용하여 연결할 수 있는 호스트 정의 , 93 페이지에서 설명합니다.

시작하기 전에

- 어플라이언스가 로컬 MX/MTA에서 메일을 수신하도록 설정된 경우 발신자 IP 주소를 마스크 처리할 수 있는 업스트림 호스트를 식별합니다. 자세한 내용은 수신 릴레이 사용 배포 환경에서 발신자 IP 주소 확인 , 374 페이지를 참조하십시오.
- SenderBase Reputation Score를 이해합니다. SenderBase Reputation 점수별로 발신자 그룹 정의, 99 페이지를 참조하십시오.
- 조직에 대한 필터링 접근 방식을 선택하고 해당 접근 방식의 권장 설정을 메모합니다. 서로 다른 발신자 평판 필터링 접근 방식에 대한 권장 설정 , 87 페이지를 참조하십시오.

단계 **1** **Mail Policies(**메일 정책**)** > **HAT Overview(HAT** 개요**)**를 선택합니다.

단계 **2** **Sender Groups (Listener)(**발신자 그룹**(**리스너**))** 메뉴에서 퍼블릭 리스너를 선택합니다.

단계 **3** 발신자 그룹에 대한 링크를 클릭합니다.

예를 들면 "SUSPECTLIST" 링크를 클릭합니다.

단계 **4** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **5** 발신자 그룹에 대한 SenderBase Reputation Score의 범위를 입력합니다.

예를 들어 "WHITELIST"에 7.0~10 범위를 입력합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

단계 **7** 이 리스너의 각 발신자 그룹에 대해 필요한 만큼 반복합니다.

단계 **8** 변경 사항을 커밋합니다.

다음에 수행할 작업

관련 주제

- SBRS를 사용하여 발신자 평판 필터링 테스트, 89 페이지
- SenderBase Reputation Service의 상태 모니터링 , 91 페이지
- Host Access Table을 사용하여 연결할 수 있는 호스트 정의 , 93 페이지
- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 356 페이지

SBRS를 사용하여 발신자 평판 필터링 테스트

대규모 스팸을 정기적으로 수신하거나 조직에서 스팸을 수신하도록 특별히 "더미(dummy)" 계정을 설정하지 않는 한, 구현한 SBRS 정책을 즉시 테스트하기가 어려울 수 있습니다. 그러나 다음 표에 나와 있는 것처럼 SenderBase Reputation Score와 함께 평판 필터링에 대한 항목을 리스너의 HAT에 추가하면 수신 메일의 더 적은 비율이 "미분류"로 처리되는 것을 알 수 있습니다.

임의의 SBRS와 함께 `trace` 명령을 사용하여 정책을 테스트합니다. 테스트 메시지를 사용하여 메일 플로우 디버깅: 추적, 1149 페이지를 참조하십시오. GUI는 물론 CLI에서도 `trace` 명령을 사용할 수 있습니다.

표 ***9:*** 구현을 위한 메일 플로우 정책 제안

정책 이름	기본 동작(액세스 규칙)	매개변수	값
`$BLOCKED`	`REJECT`	`None`	

정책 이름	기본 동작(액세스 규칙)	매개변수	값
$THROTTLED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Maximum recipients / hour: Use SenderBase:	10 20 1MB 10 ON OFF **20***(권장)* 켜기
$ACCEPTED (퍼블릭 리스너)	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Use SenderBase:	1,000 1,000 100 MB 1,000 ON OFF ON
$TRUSTED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: Use Spam Detection: Use TLS: Maximum recipients / hour: Use SenderBase:	1,000 1,000 100 MB 1,000 OFF OFF -1 *(비활성)* OFF

참고 $THROTTLED 정책에서 원격 호스트에서의 시간당 최대 수신자 수는 기본적으로 시간당 20명으로 설정됩니다. 이 설정은 가능한 최대 조절 범위를 제어합니다. 이 매개변수가 너무 적극적이면 시간당 수신 가능한 수신자 수를 늘릴 수 있습니다. Default Host Access(기본 호스트 액세스) 정책에 대한 자세한 내용은 사전 정의된 발신자 그룹 및 메일 플로우 정책 이해, 103 페이지 섹션을 참조해 주십시오.

SenderBase Reputation Service의 상태 모니터링

SenderBase Reputation Score Service는 어플라이언스에 SRBS 점수를 전송합니다. SenderBase Network Server는 사용자에게 메일을 보내는 IP 주소, 도메인 및 조직에 대한 정보를 어플라이언스에 전송합니다. AsyncOS는 보고 및 이메일 모니터링 기능에 이 데이터를 사용합니다.

이러한 서비스에 대한 연결 상태를 보려면 **Security Services(**보안 서비스**) > SenderBase**를 선택합니다.

Security Services(보안 서비스) 메뉴의 SenderBase 페이지에는 어플라이언스에서 SenderBase Network Status Server 및 SenderBase Reputation Score Service로 보내는 최신 쿼리의 연결 상태 및 타임스탬프가 표시됩니다.

CLI에서 `sbstatus` 명령을 사용해도 동일한 정보가 표시됩니다.

메시지 제목에 낮은 **SBRS** 점수 입력

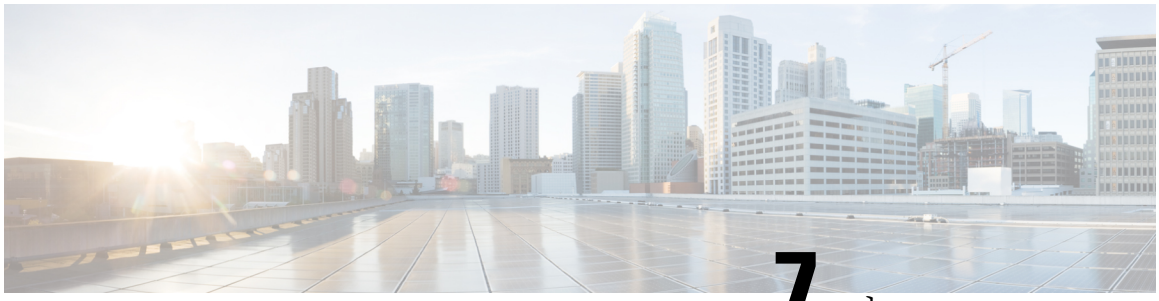
Cisco에서는 조절을 권장하지만, SenderBase Reputation Service를 사용하는 또 다른 방법은 의심스런 스팸 메시지의 제목 줄을 수정하는 것입니다. 이렇게 하려면 다음 표에 나와 있는 메시지 필터를 사용합니다. 이 필터는 reputation 필터 규칙과 strip-header 및 insert-header 필터 작업을 사용하여, SenderBase Reputation Score가 -2.0 미만인 메시지의 제목 줄을 {**{Spam** *SBRS***}**}로 표시되는 실제 SenderBase Reputation Score가 포함된 제목 줄로 교체합니다. 이 예의 *listener_name*을 퍼블릭 리스너의 이름으로 교체해 주십시오. (filters 명령의 명령행 인터페이스에 직접 이 텍스트를 오려서 붙일 수 있도록 별도의 줄에 마침표가 포함되었습니다.)

표**: SBRS**로 제목 헤더를 수정하기 위한 메시지 필터**:** 예 **1**

```
sbrs_filter:

if ((recv-inj == "listener_name
" AND subject != "\\{Spam -?[0-9.]+\\}"))

{

        insert-header("X-SBRS", "$REPUTATION");

        if (reputation <= -2.0)

{

        strip-header("Subject");

        insert-header("Subject", "$Subject \\{Spam $REPUTATION\\}");

      }

 }

.
```

관련 항목

- 메시지 필터를 사용하여 이메일 정책 적용, 137 페이지



7 장

Host Access Table을 사용하여 연결할 수 있는 호스트 정의

이 장에는 다음 섹션이 포함되어 있습니다.

연결을 허용할 호스트 정의 개요

모든 구성된 리스너에 대해 원격 호스트에서 수신 연결을 제어하는 규칙 집합을 정의해야 합니다. 예를 들면 원격 호스트를 정의하고, 원격 호스트가 리스너에 연결할 수 있는지 여부를 정의할 수 있습니다. AsyncOS를 통해 어떤 호스트가 HAT(Host Access Table)를 사용하여 리스너에 연결될 수 있는지 정의할 수 있습니다.

HAT는 리스너에 대한 원격 호스트에서의 수신 연결을 제어하는 규칙 집합을 유지 관리합니다. 구성된 각 리스너는 고유한 HAT를 보유합니다. 퍼블릭 리스너 및 프라이빗 리스너 모두에 대해 HAT를 구성합니다.

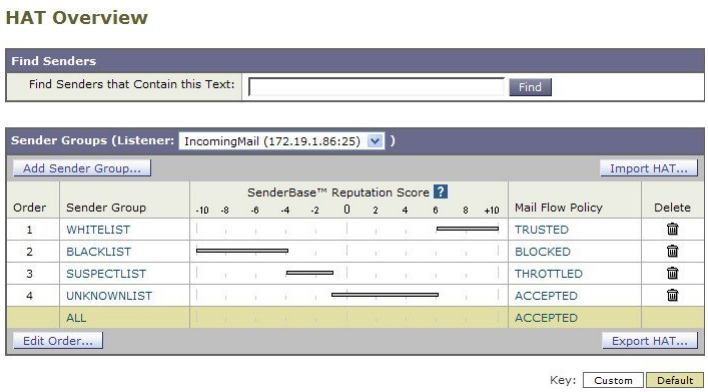
원격 호스트에서 수신되는 연결을 제어하려면, 다음 정보를 정의합니다.

- 원격 호스트. 원격 호스트가 리스너에 연결을 시도하는 방식을 정의합니다. 원격 호스트 정의를 발신자 그룹으로 그룹화합니다. 예를 들어, IP 주소 및 부분 호스트 이름을 기준으로 발신자 그룹에서 여러 원격 호스트를 정의할 수 있습니다. 또한 SenderBase Reputation 점수를 기준으로 원격 호스트를 정의할 수 있습니다. 자세한 내용은 발신자 그룹에 대해 원격 호스트 정의, 95 페이지를 참고하십시오.

- 액세스 규칙. 발신자 그룹의 정의된 원격 호스트가 리스너에 연결 가능한지 여부 및 연결 조건을 정의할 수 있습니다. 메일 플로우 정책을 사용하여 액세스 규칙을 정의합니다. 예를 들어, 특정 한 발신자 그룹이 리스너에 연결될 수 있지만 연결당 최대 메시지 수만 허용하도록 정의할 수 있습니다. 자세한 내용은 메일 플로우 정책을 사용하여 이메일 발신자에 대한 액세스 규칙 정의, 101 페이지 항목을 참조하십시오.

Mail Policies(메일 정책) > HAT Overview(HAT 개요) 페이지에서 어떤 호스트가 리스너에 연결될 수 있는지 정의합니다. 다음 그림은 특정 리스너에 대해 기본적으로 정의된 메일 플로우 정책 및 발신자 그룹이 있는 HAT Overview(HAT 개요)를 보여 줍니다.

그림 ***14: Mail Policies(메일 정책) > HAT Overview(HAT 개요)*** 페이지 - 퍼블릭 리스너



리스너에서 TCP 연결을 수신하는 경우, 리스너는 구성된 발신자 그룹과 소스 IP 주소를 비교합니다. 또한 HAT Overview(HAT 개요) 페이지에 나열된 순서대로 발신자 그룹을 평가합니다. 일치하는 항목이 발견되면 구성된 메일 플로우 정책을 연결에 적용합니다. 발신자 그룹 내에 여러 조건을 구성한 경우 이 조건 중 하나라도 일치하면 해당 발신자 그룹은 일치합니다.

사용자가 리스너를 만들면 AsyncOS는 리스너에 대한 사전 정의된 발신자 그룹 및 메일 플로우 정책을 만듭니다. 사전 정의된 발신자 그룹 및 메일 플로우 정책을 수정할 수 있으며, 새로운 발신자 그룹 및 메일 플로우 정책을 만들 수 있습니다. 자세한 내용은 사전 정의된 발신자 그룹 및 메일 플로우 정책 이해, 103 페이지를 참고하십시오.

Host Access Table에 저장된 모든 정보를 파일로 내보내고 파일에 저장된 Host Access Table 정보를 리스너의 어플라이언스로 가져와 모든 구성된 Host Access Table 정보를 재정의할 수 있습니다. 자세한 내용은 HAT(Host Access Table) 컨피그레이션 작업, 115 페이지를 참고하십시오.

관련 주제

- 기본 HAT 항목, 94 페이지

기본 HAT 항목

기본적으로, HAT는 다음과 같이 리스너 유형에 따라 다양한 작업을 수행하도록 정의됩니다.

- 퍼블릭 리스너. HAT가 이메일 모든 호스트의 이메일을 수락하도록 설정됩니다.
- 프라이빗 리스너. 지정한 호스트의 이메일을 릴레이하고 모든 기타 호스트는 거부하도록 HAT가 설정됩니다.

HAT 개요에서 기본 항목의 이름은 "ALL"입니다. Mail Policies(메일 정책) > HAT Overview(HAT 개요) 페이지에서 ALL 발신자 그룹에 대한 메일 플로우 정책을 클릭하여 기본 항목을 수정할 수 있습니다.

참고 지정한 호스트 외에 모든 호스트를 거부하는 방법을 통해 `listenerconfig` 및 `systemsetup` 명령을 사용하여 의도치 않게 시스템을 "오픈 릴레이"로 구성하는 것을 방지합니다. 오픈 릴레이(종종 "안전하지 않은 릴레이" 또는 "타사" 릴레이라고도 함)는 이메일 메시지의 타사 릴레이를 허용하는 SMTP 이메일 서버입니다. 로컬 사용자에게 보내지 않은 이메일 또는 로컬 사용자가 보내지 않은 이메일을 처리함으로써 오픈 릴레이는 악의적인 발신자가 게이트웨이를 통해 대량의 스팸을 라우팅하도록 할 수 있습니다.

발신자 그룹에 대해 원격 호스트 정의

원격 호스트가 리스너에 연결을 시도하는 방식을 정의할 수 있습니다. 원격 호스트 정의를 발신자 그룹으로 그룹화합니다. 발신자 그룹은 해당 발신자의 이메일을 동일한 방식으로 처리하기 위해 정의한 원격 호스트의 목록입니다.

발신자 그룹은 다음을 통해 식별되는 발신자 목록입니다.

- IP 주소(IPv4 또는 IPv6)
- IP 범위
- 특정 호스트 또는 도메인 이름
- SenderBase Reputation Service "조직" 분류
- SenderBase Reputation 점수(SBRS) 범위(또는 점수 부족)
- DNS 목록 쿼리 응답

발신자 그룹에서 허용 가능한 주소 목록에 대한 자세한 내용은 발신자 그룹 구문, 96 페이지 항목을 참조하십시오.

SMTP 서버가 어플라이언스와 SMTP 연결을 시도하는 경우, 리스너는 발신자 그룹을 순서대로 평가한 다음 발신자 그룹의 임의의 기준(예: SenderBase 평판 점수, 도메인 또는 IP 주소)과 일치하면 발신자 그룹에 연결을 할당합니다.

참고 이중 DNS 조회를 통해 원격 호스트의 IP 주소를 확보하고 그 유효성을 확인합니다. 이는 연결하는 호스트의 IP 주소에 대한 역방향 DNS(PTR) 조회 및 그 뒤에 오는 PTR 조회의 결과에 대한 정방향 DNS(A) 조회로 구성됩니다. 그런 다음 시스템은 A 조회의 결과가 PTR 조회의 결과와 일치하는지를 확인합니다. 결과가 일치하지 않거나 A 레코드가 없는 경우, 시스템은 HAT에 있는 항목과 일치하도록 IP 주소만 사용합니다.

Mail Policies(메일 정책) > HAT Overview(HAT 개요) 페이지에서 발신자 그룹을 정의합니다.

관련 주제

- 발신자 그룹 구문, 96 페이지
- 네트워크 소유자, 도메인 및 IP 주소별로 정의되는 발신자 그룹, 97 페이지
- SenderBase Reputation 점수별로 발신자 그룹 정의, 99 페이지
- DNS 리스트 쿼리에 의해 정의되는 발신자 그룹, 100 페이지

발신자 그룹 구문

표 ***10: HAT:*** 발신자 그룹 구문에서 원격 호스트 정의

Syntax	의미
`n:n:n:n:n:n:n:n`	IPv6 주소에는 선행 0을 포함할 필요가 없습니다.
`n:n:n:n:n:n:n:n-n:n:n:n:n:n:n:n` `n:n:n-n:n:n:n:n:n`	IPv6 주소 범위에는 선행 0을 포함할 필요가 없습니다.
`n.n.n.n`	전체(완전한) IPv4 주소

`n.n.n.`
`n.n.n.`
`n.n.`
`n.n.`
`n.`
	부분 IPv4 주소

`n.n.n.n-n.`
`n.n.n.n-n.`
`n.n.n-n.`
`n.n-n.`
`n.n-n`
`n-n.`
`n-n`
	IPv4 주소 범위

`yourhost.example.com`	인증된 도메인 이름
`.partialhost`	partialhost 도메인 내의 모든 항목

`n/c`
`n.n/c`
`n.n.n/c`
`n.n.n.n/c`
	IPv4 CIDR 주소 블록

`n:n:n:n:n:n:n:n/c`	IPv6 CIDR 주소 블록에는 선행 0을 포함할 필요가 없습니다.
`SBRS[n:n]SBRS[none]`	SenderBase Reputation Score. 자세한 내용은 SenderBase Reputation 점수별로 발신자 그룹 정의, 99 페이지를 참고하십시오.

Syntax	의미
SBO:n	SenderBase Network Owner 식별 번호. 자세한 내용은 SenderBase Reputation 점수별로 발신자 그룹 정의, 99 페이지을 참고하십시오.
dnslist[dnsserver.domain]	DNS 목록 쿼리. 자세한 내용은 DNS 리스트 쿼리에 의해 정의되는 발신자 그룹, 100 페이지를 참고해 주십시오.
ALL	모든 주소와 일치하는 특수 키워드입니다. 이 구문은 모든 발신자 그룹에만 적용되며 항상 포함됩니다(단, 나열되지 않음).

네트워크 소유자, 도메인 및 IP 주소별로 정의되는 발신자 그룹

SMTP 프로토콜에는 이메일 발신자를 인증하기 위한 내장된 방법이 없으므로 원치 않는 대량 이메일 발신자가 자신의 ID를 숨기기 위한 다양한 전략을 구사할 수 있었습니다. 예를 들면 위조된 HELO 주소를 사용하여 메시지에서 봉투 발신자 주소를 스푸핑하거나, 단순히 여러 도메인 이름 간에 회전하는 방법이 있습니다. 이 경우 다수의 메일 관리자는 "이 모든 이메일을 보내는 사람이 누구인가?"라는 기본적인 질문을 하게 됩니다. 이 질문에 답하기 위해 SenderBase Reputation Service는 연결하는 호스트의 IP 주소(발신자가 메시지에서 위조하기가 거의 불가능)를 기반으로 ID 기반 정보를 집계하기 위한 고유한 계층 구조를 개발했습니다.

IP 주소는 전송 메일 호스트의 IP 주소로 정의됩니다. Email Security Appliance는 IPv4(Internet Protocol version 4) 및 IPv6(version 6) 주소를 모두 지원합니다.

도메인은 지정된 두 번째 레벨 도메인 이름(예: yahoo.com)과 함께 호스트 이름을 사용하는 엔티티로 정의되며, IP 주소에 대한 역방향(PTR) 조회에서 확인됩니다.

네트워크 소유자**(Network Owner)**는 IP 주소 블록을 제어하는 엔티티(일반적으로 회사)로 정의되며, ARIN(American Registry for Internet Numbers)과 같은 글로벌 등록 기관 및 기타 소스에서 오는 IP 주소 공간 할당을 기반으로 확인됩니다.

조직은 네트워크 소유자의 IP 블록 내에서 특별한 메일 게이트웨이 그룹을 가장 가깝게 제어하는 엔티티로 정의되며, SenderBase에 의해 확인됩니다. 조직은 네트워크 소유자, 네트워크 소유자 내 부서 또는 네트워크 소유자의 고객과 같을 수 있습니다.

관련 주제

- HAT를 기반으로 정책 설정, 97 페이지

HAT를 기반으로 정책 설정

다음 표에는 네트워크 소유자 및 조직의 몇 가지 예가 나열되어 있습니다.

표 *11:* 네트워크 소유자 및 조직의 예

유형 예	네트워크 소유자	조직
네트워크 서비스 공급자	Level 3 Communications	Macromedia Inc. AllOutDeals.com GreatOffers.com
이메일 서비스 공급자	GE	GE Appliances GE Capital GE Mortgage
상용 발신자	The Motley Fool	The Motley Fool

네트워크 소유자는 크기의 범위가 극적으로 다양할 수 있으므로 메일 플로우 정책의 기반이 될 적절한 엔티티는 조직입니다. SenderBase Reputation Service는 이메일의 소스를 조직 레벨까지 고유한 방식으로 이해하며, 어플라이언스는 이를 활용해 조직을 기반으로 정책을 자동으로 적용합니다. 위의 예에서, 사용자가 HAT(Host Access Table)에서 "Level 3 Communications"를 발신자 그룹으로 지정하는 경우 SenderBase는 해당 네트워크 소유자가 제어하는 개별 조직을 기반으로 정책을 적용합니다.

예를 들어 위의 표에서 사용자가 Level 3에 대해 시간당 수신자를 10명으로 제한하면, 어플라이언스는 Macromedia Inc., Alloutdeals.com 및 Greatoffers.com에 대해 시간당 수신자를 최대 10명까지 허용합니다(Level 3 네트워크 소유자에 대해 시간당 수신자 총 30명). 이 접근 방식의 장점은, 이러한 조직 중 하나에서 스패밍을 시작할 경우 Level 3에 의해 제어되는 나머지 조직이 영향을 받지 않는다는 점입니다. 이는 "The Motley Fool" 네트워크 소유자의 예와 대비됩니다. 사용자가 속도 제한을 시간당 수신자 10명으로 제한하면 The Motley Fool 네트워크 소유자는 시간당 총 10명의 수신자를 수신합니다.

메일 플로우 모니터 기능은 발신자를 정의하고 발신자에 대한 메일 플로우 정책 결정을 내리는 모니터링 도구를 제공하기 위한 방법입니다. 특정 발신자에 대한 메일 플로우 정책을 결정하려면 다음을 질문합니다.

- 어떤 **IP** 주소가 이 발신자에 의해 제어됩니까**?**

  메일 플로우 모니터 기능이 인바운드 이메일 처리를 제어하기 위해 사용하는 첫 번째 정보는 이 질문에 대한 대답입니다. 대답은 SenderBase Reputation Service에 쿼리하여 얻을 수 있습니다. SenderBase Reputation Service는 발신자(SenderBase 네트워크 소유자 또는 SenderBase 조직)의 상대적인 크기에 대한 정보를 제공합니다. 이 질문에 대한 답은 다음을 가정합니다.

  - 조직이 클수록 더 많은 IP 주소를 제어하고 더 많은 합법적인 이메일을 전송하는 경향이 있습니다.

- 크기를 기반으로**,** 이 발신자에 대해 전체적인 연결 수를 어떻게 할당해야 합니까**?**

  - 조직이 클수록 더 많은 IP 주소를 제어하고 더 많은 합법적인 이메일을 전송하는 경향이 있습니다. 따라서 어플라이언스에 할당되는 연결 수가 더 많습니다.
  - 대량 이메일의 소스는 종종 ISP, NSP, 아웃소싱 이메일 전달을 관리하는 회사 또는 원치 않는 대량 이메일을 보내는 곳입니다. ISP, NSP 및 아웃소싱 이메일 전달을 관리하는 회사는 많은 IP 주소를 제어하는 조직의 예이며, 어플라이언스에 할당되는 연결 수가 더 많습니다. 원치 않는 대량 이메일의 발신자는 일반적으로 많은 IP 주소를 제어하지 않습니다. 오히려

소수의 IP 주소를 통해 대량의 메일을 전송합니다. 따라서 어플라이언스에 할당되는 연결 수가 더 적습니다.

Mail Flow Monitor 기능은 SenderBase 네트워크 소유자와 SenderBase 조직의 차이점을 사용하여 SenderBase의 논리를 기반으로 발신자당 연결 할당 방법을 결정합니다. Mail Flow Monitor 기능 사용에 대한 자세한 내용은 "이메일 보안 모니터 사용" 장을 참조해 주십시오.

SenderBase Reputation 점수별로 발신자 그룹 정의

어플라이언스는 SenderBase Reputation Service에 쿼리하여 발신자의 평판 점수(SBRS)를 확인할 수 있습니다. SBRS는 SenderBase Reputation Service의 정보를 기반으로 IP 주소, 도메인 또는 조직에 할당된 숫자 값입니다. 점수 범위는 다음 표에 설명된 대로 -10.0~+10.0입니다.

표 ***12: SenderBase Reputation*** 점수 정의

점수	의미
-10.0	스팸 소스일 가능성이 매우 높음
0	중립, 또는 추천할 만한 충분한 정보 없음
+10.0	신뢰할 수 있는 발신자일 가능성이 매우 높음
none	이 발신자에 대해 사용할 수 있는 데이터 없음(일반적으로 스팸 소스)

SBRS를 사용하면 신뢰도를 기반으로 발신자에게 메일 플로우 정책을 적용하도록 어플라이언스를 구성할 수 있습니다. 예를 들어 점수가 -7.5 이하인 발신자를 모두 거부할 수 있습니다. 이는 GUI를 통해 가장 쉽게 설정할 수 있습니다. 메시지 처리를 위한 발신자 그룹 만들기 , 106 페이지 섹션을 참조해 주십시오. 그러나 텍스트 파일로 내보낸 HAT를 수정하는 경우 SenderBase Reputation 점수를 포함하는 구문에 대한 설명은 다음 표에 나와 있습니다.

표 ***13: SenderBase Reputation*** 점수의 구문

`SBRS[ n n`	SenderBase Reputation Score. 발신자는 SenderBase Reputation Service에 쿼리하여 식별되며, 점수는 범위 사이에 정의됩니다.
SBRS[none]	SBRS를 지정하지 않습니다(최신 도메인은 SenderBase Reputation 점수가 아직 없을 수 있습니다).

참고 GUI를 통해 HAT에 추가된 네트워크 소유자는 `SBO:n` 구문을 사용합니다. 여기서 *n*은 SenderBase Reputation Service에서 네트워크 소유자의 고유한 식별 번호입니다.

리스너가 SenderBase Reputation Service에 쿼리하도록 하려면 **Network(네트워크) > Listeners(리스너)** 페이지 또는 CLI의 `listenerconfig -> setup` 명령을 사용합니다. 또한 SenderBase Reputation Service에 쿼리할 때 어플라이언스가 대기해야 할 시간 초과 값을 정의할 수 있습니다. 그런 다음 GUI의 Mail

Policies(메일 정책) 페이지 또는 CLI의 `listenerconfig -> edit -> hostaccess` 명령에서 값을 사용하여 SenderBase Reputation Service에 대한 조회를 사용할 서로 다른 정책을 구성할 수 있습니다.

참고 시스템에서 처리하는 메시지에 추가 작업을 수행하도록 SenderBase Reputation Score에 대한 "임계값"을 지정하는 메시지 필터를 만들 수도 있습니다. 자세한 내용은 안티스팸 및 안티바이러스 장의 "SenderBase Reputation 규칙", "안티스팸 시스템 작업 우회(Bypass Anti-Spam System Action)" 및 "안티바이러스 시스템 작업 우회(Bypass Anti-Virus System Action)"를 참조해 주십시오.

DNS 리스트 쿼리에 의해 정의되는 발신자 그룹

리스너의 HAT에는 특정 DNS 리스트 서버에 대한 쿼리를 확인하여 발신자 그룹을 정의하는 기능도 있습니다. 쿼리는 원격 클라이언트 연결 시 DNS를 통해 수행됩니다. 원격 리스트를 쿼리하는 기능은 현재 메시지 필터 규칙으로서도 존재하지만("메시지 필터를 사용하여 이메일 정책 시행" 장의 "DNS List(DNS 리스트) 규칙" 참조), 메시지 내용 전체를 수신한 후에야 가능합니다.

이 메커니즘 덕분에 DNS List(DNS 리스트)를 쿼리하는 그룹 내에 발신자를 구성하고 그에 따라 메일 플로우 정책을 적절히 조정할 수 있습니다. 예를 들면 연결을 거부하거나 도메인 연결 동작을 제한할 수 있습니다.

참고 일부 DNS 리스트는 쿼리 중인 IP 주소에 대한 여러 가지 사실을 표시하기 위해 변수 응답(예: "127.0.0.1" 대 "127.0.0.2" 대 "127.0.0.3")을 사용합니다. 메시지 필터 DNS 리스트 규칙을 사용하는 경우("메시지 필터를 사용하여 이메일 정책 시행" 장의 "DNS List(DNS 리스트) 규칙" 참조), 여러 값을 기준으로 쿼리 결과를 비교할 수 있습니다. 그러나 쿼리할 DNS 리스트 서버를 HAT에 지정하는 기능은 단순성을 위해 부울 연산만 지원합니다(즉, IP 주소가 리스트에 나타나는지 여부).

참고 CLI의 쿼리에는 반드시 대괄호를 포함해야 합니다. GUI에서 DNS 리스트 쿼리를 지정할 때에는 대괄호가 필요하지 않습니다. 쿼리를 테스트하거나, DNL 쿼리에 대한 일반 설정을 구성하거나, 현재 DNS 리스트 캐시를 플러시하려면 CLI의 dnslistconfig 명령을 사용해 주십시오.

"좋은" 연결은 물론 "나쁜" 연결을 식별하는 데에도 이 메커니즘을 사용할 수 있습니다. 예를 들면 query.bondedsender.org에 대한 쿼리는 이메일 캠페인의 무결성을 보장하기 위해 Cisco Systems의 Bonded Sender™ 프로그램으로 금융 채권을 게시한 호스트 연결에서 확인됩니다. Bonded Sender 프로그램의 DNS 서버(채권을 게시한 합법적인 이메일 발신자 나열)에 쿼리하고 메일 플로우 정책을 적절히 조정하도록 기본 WHITELIST 발신자 그룹을 수정할 수 있습니다.

메일 플로우 정책을 사용하여 이메일 발신자에 대한 액세스 규칙 정의

메일 플로우 정책을 사용하면 SMTP 대화 중에 발신자로부터 리스너로의 이메일 메시지 플로우를 제어 또는 제한할 수 있습니다. 메일 플로우 정책에서 다음과 같은 매개변수 유형을 정의하여 SMTP 대화를 제어합니다.

- 연결 매개변수(예: 연결당 최대 메시지 수)
- 속도 제한 매개변수(예: 시간당 최대 수신자 수)
- SMTP 대화 중 주고받은 맞춤화 SMTP 코드 및 응답 수정
- 스팸 탐지 활성화
- 바이러스 탐지 활성화
- 암호화(예: TLS를 사용하여 SMTP 연결 암호화)
- 인증 매개변수(예: DKIM을 사용하여 수신 이메일 확인)

궁극적으로 메일 플로우 정책은 원격 호스트에서 연결할 때 다음 작업 중 하나를 수행합니다.

- **ACCEPT.** 연결이 수락되며, 이메일 어플라이언스는 Recipient Access Table(퍼블릭 리스너용)을 비롯한 리스너 설정을 통해 추가로 제한됩니다.
- **REJECT.** 연결이 초기에는 수락되지만, 연결을 시도하는 클라이언트가 4XX 또는 5XX SMTP 상태 코드를 받습니다. 이메일이 수락되지 않습니다.

참고 SMTP 대화가 시작될 때보다는 메시지 수신자 레벨(RCPT TO)에서 이 거부를 수행하도록 AsyncOS를 구성할 수도 있습니다. 이렇게 메시지를 거부하면 메시지 거부가 지연되고 메시지가 반송되어, AsyncOS는 거부된 메시지에 대해 좀 더 자세한 정보를 보유하게 됩니다. 이 설정은 CLI `listenerconfig > setup` 명령으로 구성됩니다. 자세한 내용은 CLI로 리스너를 만들어 연결 요청 수신 대기, 80 페이지를 참고하십시오.

- **TCPREFUSE.** TCP 레벨에서 연결이 거부됩니다.
- **RELAY.** 연결이 수락됩니다. 수신자에 대한 수신이 허용되며 Recipient Access Table에 의해 제약을 받지 않습니다.
- **CONTINUE.** HAT의 매핑이 무시되고 HAT의 처리가 계속됩니다. 수신 연결이 CONTINUE가 아닌 이후의 항목과 일치하면 해당 항목이 대신 사용됩니다. CONTINUE 규칙은 GUI에서 HAT를 수정하는 데 사용됩니다. 자세한 내용은 메시지 처리를 위한 발신자 그룹 만들기 , 106 페이지를 참고하십시오.

관련 주제

- HAT 변수 구문, 102 페이지

HAT 변수 구문

다음 표에서는 메일 플로우 정책에 대해 정의된 Rate Limiting 배너 및 맞춤화 SMTP와 함께 사용할 수 있는 변수의 집합을 보여줍니다. 변수 이름은 대/소문자를 구분하지 않습니다. 즉, $group은 $Group과 같습니다.

표 *14: HAT* 변수 구문

변수	정의
$Group	HAT에서 일치된 발신자 그룹의 이름으로 교체됩니다. 발신자 그룹에 이름이 없으면 "None"이 표시됩니다.
$Hostname	어플라이언스에 의해 검증된 경우에만 원격 호스트 이름에 의해 교체됩니다. IP 주소의 역방향 DNS 조회가 성공했지만 호스트 이름이 반환되지 않은 경우 "None"이 표시됩니다. 역방향 DNS 조회가 실패하면(예: DNS 서버에 도달할 수 없거나 구성된 DNS 서버가 없는 경우) "Unknown"이 표시됩니다.
$OrgID	SenderBase Organization ID(정수 값)로 교체됩니다. 어플라이언스가 SenderBase Organization ID를 얻지 못하거나 SenderBase Reputation Service가 값을 반환하지 않으면 "None"이 표시됩니다.
$RemoteIP	원격 클라이언트의 IP 주소로 교체됩니다.
$HATEntry	원격 클라이언트와 일치한 HAT의 항목으로 교체됩니다.

관련 주제

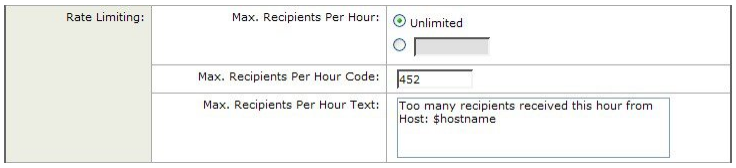
- HAT 변수 사용, 102 페이지
- HAT 변수 테스트, 103 페이지

HAT 변수 사용

참고 이러한 변수는 "이메일을 수신하도록 게이트웨이 구성" 장에서 설명한 `smtp_banner_text` 및 `max_rcpts_per_hour_text` 고급 HAT 매개변수와 함께 사용할 수 있습니다.

이러한 변수를 사용하면 GUI에서 $TRUSTED 정책의 수락된 연결에 대한 맞춤화 SMTP 배너 응답 텍스트를 수정할 수 있습니다.

그림 *15: HAT* 변수 사용



또는 같은 내용이 CLI에서는 다음과 같습니다.

```
Would you like to specify a custom SMTP response?  [Y]> y


Enter the SMTP code to use in the response. 220 is the standard code.

[220]> 200


Enter your custom SMTP response.  Press Enter on a blank line to finish.

You've connected from the hostname: $Hostname, IP address of: $RemoteIP, matched the group:
 $Group,
$HATEntry and the SenderBase Organization: $OrgID.
```

HAT 변수 테스트

이러한 변수를 테스트하려면 신뢰할 수 있는 알려진 시스템의 IP 주소를 어플라이언스에 있는 리스너의 $WHITELIST 발신자 그룹에 추가합니다. 그런 다음 텔넷을 통해 해당 시스템에서 연결합니다. SMTP 응답에서 변수가 교체된 것을 확인할 수 있습니다. 예를 들면 다음과 같습니다.

```
# telnet
IP_address_of_Email_Security_Appliance port


220 hostname
 ESMTP


200 You've connected from the hostname: hostname
, IP address of: IP-address_of_connecting_machine
, matched the group: WHITELIST, 10.1.1.1 the SenderBase Organization: OrgID
.
```

사전 정의된 발신자 그룹 및 메일 플로우 정책 이해

다음 표에는 퍼블릭 리스너를 만들 때 구성하는 사전 정의된 발신자 그룹 및 메일 플로우 정책이 나와 있습니다.

표 *15:* 퍼블릭 리스너용 사전 정의된 발신자 그룹 및 메일 플로우 정책

사전 정의된 발신자 그룹	설명	메일 플로우 정책 기본 구성
WHITELIST	신뢰하는 발신자를 Whitelist 발신자 그룹에 추가합니다. 신뢰하는 발신자의 이메일에 대해 속도 제한이 설정되지 않도록 $TRUSTED 메일 플로우 정책이 구성되며, 이러한 발신자의 콘텐츠는 안티스팸 또는 안티바이러스 소프트웨어에서 검사되지 않습니다.	$TRUSTED
BLACKLIST	Blacklist 발신자 그룹의 발신자는 거부됩니다($BLOCKED 메일 플로우 정책에 설정된 매개변수에 의해). 이 그룹에 발신자를 추가하면 SMTP HELO 명령에서 5XX SMTP 응답이 반환되며 해당 호스트에서의 연결이 거부됩니다.	$BLOCKED
SUSPECTLIST	Suspectlist 발신자 그룹에는 수신 메일의 속도를 조절(throttle)하거나 저하시키는 메일 플로우 정책이 포함됩니다. 발신자가 의심스러우면 Suspectlist 발신자 그룹에 추가할 수 있습니다. 여기서 메일 플로우 정책은 다음을 지시합니다. • 속도 제한은 세션당 최대 메시지 수, 메시지당 최대 수신자 수, 최대 메시지 크기 및 원격 호스트에서 수락할 최대 동시 연결 수를 제한합니다. • 원격 호스트에서 오는 시간당 최대 수신자 수는 시간당 20명으로 설정됩니다. 이 설정이 조절 가능한 최대값입니다. 이 매개변수가 너무 적극적이면 시간당 수신 가능한 수신자 수를 늘릴 수 있습니다. • 안티스팸 검사 엔진 및 안티바이러스 검사 엔진에서 메시지의 내용을 검사합니다(시스템에 대해 이러한 기능을 활성화한 경우). • 발신자에 대한 추가 정보는 SenderBase Reputation Service에 쿼리됩니다.	$THROTTLED

사전 정의된 발신자 그룹	설명	메일 플로우 정책 기본 구성
UNKNOWNLIST	특정 발신자에 대해 사용할 메일 플로우 정책을 결정하지 못한 경우 Unknownlist 발신자 그룹이 유용할 수 있습니다. 이 그룹에 대한 메일 플로우 정책은 이 그룹의 발신자에 대해 메일을 수락하되 안티스팸 소프트웨어(시스템에 대해 활성화된 경우), 안티바이러스 검사 엔진 및 SenderBase Reputation Service를 모두 사용하여 발신자 및 메시지 내용에 대한 추가 정보를 수집하도록 지시합니다. 또한 이 그룹의 발신자에 대한 속도 제한이 기본값으로 활성화됩니다. 바이러스 검사 엔진에 대한 자세한 내용은 바이러스 검사, 337 페이지 섹션을 참조해 주십시오. SenderBase Reputation Service에 대한 자세한 내용은 SenderBase Reputation Service, 85 페이지 섹션을 참조해 주십시오.	$ACCEPTED
ALL	다른 모든 발신자에 대해 적용되는 기본 발신자 그룹. 자세한 내용은 기본 HAT 항목, 94 페이지를 참고해 주십시오.	$ACCEPTED

다음 표에는 프라이빗 리스너를 만들 때 구성하는 사전 정의된 발신자 그룹 및 메일 플로우 정책이 나와 있습니다.

표 ***16:*** 프라이빗 리스너용 사전 정의된 발신자 그룹 및 메일 플로우 정책

사전 정의된 발신자 그룹	설명	메일 플로우 정책 기본 구성
RELAYLIST	알고 있는 발신자 중 릴레이를 허용해야 하는 발신자를 Relaylist 발신자 그룹에 추가합니다. 릴레이를 허용하는 발신자의 이메일에 속도 제한이 없도록 $RELAYED 메일 플로우 정책이 구성되며, 이러한 발신자의 콘텐츠는 안티스팸 검사 엔진 또는 안티바이러스 소프트웨어에서 검사되지 않습니다. 참고 RELAYLIST 발신자 그룹에는 시스템 설정 마법사가 실행될 때 이메일을 릴레이하도록 허용된 시스템이 포함됩니다.	$RELAYED
ALL	다른 모든 발신자에 대해 적용되는 기본 발신자 그룹. 자세한 내용은 기본 HAT 항목, 94 페이지를 참고해 주십시오.	$BLOCKED

참고 이더넷 포트가 두 개뿐인 어플라이언스 모델에서 시스템 설정 마법사를 실행할 경우 하나의 리스너만 생성하라는 프롬프트가 표시됩니다. 내부 시스템을 위해 메일을 릴레이하는 데 사용되는 $RELAYED 메일 플로우 정책도 포함하는 퍼블릭 리스너가 생성됩니다. 이더넷 포트가 셋 이상인 어플라이언스 모델의 경우 RELAYLIST 발신자 그룹 및 $RELAYED 메일 플로우 정책만 프라이빗 리스너에 나타납니다.

발신자 그룹의 메시지를 동일한 방식으로 처리

리스너가 발신자의 메시지를 처리하는 방법을 구성하려면 Mail Policies(메일 정책) > HAT Overview(HAT 개요) 및 Mail Flow Policy(메일 플로우 정책) 페이지를 사용합니다. 여기에서 발신자 그룹 및 메일 플로우 정책을 만들고 수정하고 삭제할 수 있습니다.

관련 주제

- 메시지 처리를 위한 발신자 그룹 만들기 , 106 페이지
- 기존 발신자 그룹에 발신자 추가, 107 페이지
- 수신 연결을 위해 수행할 규칙의 순서 다시 조정, 108 페이지
- 발신자 검색, 108 페이지
- 메일 플로우 정책을 사용하여 이메일 발신자에 대한 액세스 규칙 정의, 101 페이지
- 메일 플로우 정책에 대한 기본값 정의, 114 페이지

메시지 처리를 위한 발신자 그룹 만들기

단계 **1** **Mail Policies(메일 정책) > HAT Overview(HAT 개요)** 페이지로 이동합니다.

단계 **2** 수정할 리스너를 Listener(리스너) 필드에서 선택합니다.

단계 **3** **Add Sender Group(발신자 그룹 추가)**을 클릭합니다.

단계 **4** 발신자 그룹의 이름을 입력합니다.

단계 **5** 발신자 그룹 리스트에 배치할 순서를 선택합니다.

단계 **6** (선택 사항) 코멘트를 입력합니다(예: 이 발신자 그룹 및 설정에 대한 정보).

단계 **7** 이 발신자 그룹에 적용할 메일 플로우 정책을 선택합니다.

참고 이 그룹에 적용할 메일 플로우 정책을 모르는 경우(또는 메일 플로우 정책이 아직 없는 경우) 기본 "CONTINUE (no policy)" 메일 플로우 정책을 사용합니다.

단계 **8** (선택 사항) DNS 리스트를 선택합니다.

단계 **9** (선택 사항) SBRS에 정보가 없는 발신자를 포함합니다. 이를 "none"이라고 하며 일반적으로 의심스런 사용자를 나타냅니다.

단계 **10** (선택 사항) DNS 리스트를 입력합니다.

단계 **11** (선택 사항) 호스트 DNS 확인 설정을 구성합니다.

자세한 내용은 미확인 발신자에 대해 좀 더 엄격한 조절 설정 구현, 124 페이지 장을 참조해 주십시오.

단계 **12** 발신자 그룹을 만들려면 **Submit**(제출)를 클릭합니다.

단계 **13** 새로 생성된 발신자 그룹을 클릭합니다.

단계 **14** 발신자 그룹에 발신자를 추가하려면 **Add Sender**(발신자 추가)를 클릭합니다.

- 발신자 **IP** 주소를 추가합니다. **IP Addresses**(**IP** 주소)를 선택하고 IPv4 주소, IPv6 주소 또는 호스트 이름을 추가한 후 변경 사항을 제출합니다.

  발신자는 IP 주소의 범위 및 부분 호스트 이름을 포함할 수 있습니다.

- 발신자의 발신지 국가를 추가합니다. **Geolocation**(지리위치)를 선택하고 국가를 선택하여 변경 사항을 제출합니다.

단계 **15** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- 리스너에 대한 발신자 평판 필터링 점수 임계값 수정 , 88 페이지

기존 발신자 그룹에 발신자 추가

단계 **1** 도메인, IP 또는 네트워크 소유자 프로필 페이지에서 Add to Sender Group(발신자 그룹에 추가) 링크를 클릭합니다.

단계 **2** 각 리스너에 대해 정의된 리스트에서 발신자 그룹을 선택합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

참고 발신자 그룹에 도메인을 추가하면 GUI에 두 가지 실제 도메인이 나열됩니다. 예를 들어 Add to Sender Group(발신자 그룹에 추가) 페이지에서 `example.net` 도메인을 추가하면 `example.net` 및 `.example.net`이 모두 추가됩니다. 두 번째 항목은 `example.net` 하위 도메인의 모든 호스트가 발신자 그룹에 추가되도록 보장합니다. 자세한 내용은 발신자 그룹 구문, 96 페이지 항목을 참조하십시오.

발신자 그룹에 추가하는 하나 이상의 발신자가 이미 해당 발신자 그룹에 있는 중복된 항목인 경우, 중복된 발신자는 추가되지 않고 확인 메시지가 표시됩니다.

단계 **4** 발신자를 추가하고 Incoming Mail Overview(수신 메일 개요) 페이지로 돌아가려면 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

관련 주제

- 스팸 필터로부터 어플라이언스에서 생성된 메시지 보호, 369 페이지
- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 356 페이지

수신 연결을 위해 수행할 규칙의 순서 다시 조정

리스너에 발신자 그룹을 추가한 경우 발신자 그룹 순서를 수정해야 할 수 있습니다.

리스너에 연결하려고 시도하는 각 호스트에 대해 위에서 아래로 HAT를 읽습니다. 규칙이 연결하는 호스트와 일치하면 해당 연결에 대해 즉시 작업이 수행됩니다.

단계 **1** **Mail Policies(**메일 정책**) > HAT Overview(HAT** 개요**)** 페이지로 이동합니다.

단계 **2** 수정할 리스너를 Listener(리스너) 필드에서 선택합니다.

단계 **3** **Edit Order(**순서 수정**)**를 클릭합니다.

단계 **4** HAT에서 발신자 그룹의 기존 행에 대해 새 순서를 입력합니다.

RELAYLIST(특정 하드웨어 모델 전용)와 그 뒤에 WHITELIST, BLACKLIST, SUSPECTLIST 및 UNKNOWNLIST가 오는 기본 순서는 유지하는 것이 좋습니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

발신자 검색

HAT Overview(HAT 개요) 페이지 위쪽에 있는 Find Senders(발신자 찾기) 필드에 텍스트를 입력하여 발신자를 찾을 수 있습니다. 검색할 텍스트를 입력하고 Find(찾기)를 클릭합니다.

메일 플로우 정책을 사용하여 수신 메시지에 대한 규칙 정의

메일 플로우 정책을 만들기 전에 다음과 같은 규칙 및 지침을 고려해 주십시오.

- "Use Default(기본값 사용)" 라디오 버튼이 선택되어 있으며 정책에 대한 기본값은 "회색으로 표시"됩니다. 기본값을 덮어쓰려면 "On" 라디오 버튼을 선택하고 액세스 가능한 새 값으로 변경하여 기능 또는 설정을 활성화합니다. 기본값 정의 방법은 메일 플로우 정책에 대한 기본값 정의, 114 페이지 섹션을 참조해 주십시오.
- 일부 매개변수는 특정 사전 구성에 따라 달라집니다. (예를 들어 DHAP(Directory Harvest Attack Prevention) 설정을 사용하려면 LDAP 수락 쿼리가 구성되어 있어야 합니다.)

단계 **1** **Mail Policies(**메일 정책**) > Mail Flow Policies(**메일 플로우 정책**)** 페이지로 이동합니다.

단계 **2** **Add Policy(**정책 추가**)**를 클릭합니다.

단계 **3** 다음 표에 설명된 정보를 입력합니다.

표 ***17:*** 메일 플로우 정책 매개변수

파라미터	설명
Connections	

파라미터	설명
최대 메시지 크기	이 리스너에서 수락할 메시지의 최대 크기. 최대 메시지 크기로 사용할 수 있는 최소 크기는 1킬로바이트입니다.
Maximum concurrent connections from a single IP(단일 IP에서의 최대 동시 연결 수)	단일 IP 주소에서 이 리스너로 연결할 수 있는 최대 동시 연결 수
Maximum messages per connection(연결당 최대 메시지 수)	원격 호스트에서 연결당 이 리스너를 통해 전송할 수 있는 최대 메시지 수
Maximum recipients per message(메시지당 최대 수신자 수)	이 호스트에서 수락할 메시지당 최대 수신자 수
SMTP 배너	
Custom SMTP Banner Code(맞춤화 SMTP 배너 코드)	이 리스너와의 연결이 설정될 때 반환되는 SMTP 코드
Custom SMTP Banner Text(맞춤화 SMTP 배너 텍스트)	이 리스너와의 연결이 설정될 때 반환되는 SMTP 배너 텍스트 참고 이 필드에 몇 가지 변수를 사용할 수 있습니다. 자세한 내용은 HAT 변수 구문, 102 페이지를 참고해 주십시오.
Custom SMTP Reject Banner Code(맞춤화 SMTP 거부 배너 코드)	이 리스너에 의해 연결이 거부될 때 반환되는 SMTP 코드
Custom SMTP Reject Banner Text(맞춤화 SMTP 거부 배너 텍스트)	이 리스너에 의해 연결이 거부될 때 반환되는 SMTP 배너 텍스트
Override SMTP Banner Host Name(SMTP 배너 호스트 이름 재정의)	기본적으로 어플라이언스는 원격 호스트에 SMTP 배너를 표시할 때 리스너의 인터페이스와 연결된 호스트 이름을 포함합니다(예: 220-호스트 이름 ESMTP). 여기에 다른 호스트 이름을 입력하여 이 배너를 재정의할 수 있습니다. 또한 배너에 호스트 이름을 표시하지 않도록 선택하여 호스트 이름 필드를 비워둘 수도 있습니다.
호스트에 대한 속도 제한	

파라미터	설명
Max. Recipients per Hour(시간당 최대 수신자 수)	이 리스너가 원격 호스트에서 수신할 시간당 최대 수신자 수. 발신자 IP 주소당 수신자 수는 전역적으로 추적됩니다. 각 리스너는 자체 속도 제한 임계값을 추적합니다. 그러나 모든 리스너가 단일 카운터를 기준으로 검증되므로, 동일한 IP 주소(발신자)가 여러 리스너에 연결된 경우 속도 제한이 초과될 가능성이 높습니다. 참고 이 필드에 몇 가지 변수를 사용할 수 있습니다. 자세한 내용은 HAT 변수 구문, 102 페이지를 참고해 주십시오.
Max. Recipients per Hour Code(시간당 최대 수신자 수 코드)	호스트가 이 리스너에 대해 정의된 시간당 최대 수신자 수를 초과할 경우 반환되는 SMTP 코드
Max. Recipients Per Hour Exceeded Text(시간당 최대 수신자 수 초과 텍스트)	호스트가 이 리스너에 대해 정의된 시간당 최대 수신자 수를 초과할 경우 반환되는 SMTP 배너 텍스트
발신자에 대한 속도 제한	
Max. Recipients per Time Interval(시간 간격당 최대 수신자 수)	메일 형식 주소를 기반으로, 고유한 봉투 발신자로부터 이 리스너가 받는 지정된 기간 동안의 최대 수신자 수. 수신자의 수는 전역에서 추적되지 않습니다. 각 리스너는 자체 속도 제한 임계값을 추적합니다. 그러나 모든 리스너가 단일 카운터를 기준으로 검증되므로, 여러 리스너가 동일한 메일 형식 주소의 메시지를 수신하는 경우 속도 제한이 초과될 가능성이 높습니다. 최대 수신자 기본값을 사용할지, 무제한 수신자를 수락할지, 또 다른 최대 수신자 수를 지정할지를 선택합니다. 기본적으로 다른 메일 플로우 정책에서 사용할 시간 간격 및 최대 수신자 수를 지정하려면 Default Mail Flow Policy(기본 메일 플로우 정책) 설정을 사용합니다. 시간 간격은 Default Mail Flow Policy(기본 메일 플로우 정책)를 사용해서만 지정할 수 있습니다.
Sender Rate Limit Exceeded Error Code(발신자 속도 제한 초과 오류 코드)	봉투(envelope)가 이 리스너에 대해 정의된 시간 간격 중 최대 수신자 수를 초과할 경우 반환되는 SMTP 코드
Sender Rate Limit Exceeded Error Text(발신자 속도 제한 초과 오류 텍스트)	봉투(envelope)가 이 리스너에 대해 정의된 시간 간격 중 최대 수신자 수를 초과할 경우 반환되는 SMTP 배너 텍스트
예외	정의된 속도 제한에서 특정 봉투 발신자를 제외하려면 봉투 발신자를 포함하는 주소 리스트를 선택합니다. 자세한 내용은 수신 연결 규칙에 발신자 주소 리스트 사용, 116 페이지를 참조하십시오.
플로우 제어**Flow Control**(플로우 제어)	

파라미터	설명
Use SenderBase for Flow Control(플로우 제어에 SenderBase 사용)	이 리스너에 대해 SenderBase Reputation Service에 대한 "조회"를 허용합니다.
Group by Similarity of IP Addresses: (significant bits 0-32)(IP 주소의 유사성을 기준으로 그룹화(중요 비트 0-32))	큰 CIDR 블록에서 리스너 HAT(Host Access Table)의 항목을 관리하는 한편 IP 주소 단위로 수신 메일을 추적하고 속도를 제한하는 데 사용됩니다. 속도 제한을 목적으로 유사한 IP 주소를 그룹화할 중요 비트의 범위(0-32)를 정의하는 한편, 각 IP 주소에 대한 개별 카운터를 해당 범위 내에 유지합니다. "Use SenderBase(SenderBase 사용)"를 비활성화해야 합니다. HAT 중요 비트에 대한 자세한 내용은 라우팅 및 전달 기능 구성, 665 페이지 섹션을 참조해 주십시오.
DHAP(Directory Harvest Attack Prevention)	
DHAP(Directory Harvest Attack Prevention): 시간당 최대 잘못된 수신자 수	이 리스너가 원격 호스트에서 수신할 시간당 최대 잘못된 수신자 수. 이 임계값은 RAT 거부 및 SMTP call-ahead 서버 거부의 총계를 SMTP 대화에서 삭제되거나 작업 대기열에서 반송된(관련 리스너의 LDAP 수락 설정에서 구성) 잘못된 LDAP 수신자에 대한 총 메시지 수와 결합하여 표시합니다. LDAP 수락 쿼리를 위해 DHAP를 구성하는 방법에 대한 자세한 내용은 LDAP 쿼리 작업, 745 페이지 섹션을 참조해 주십시오.
Directory Harvest Attack Prevention: Drop Connection if DHAP threshold is Reached within an SMTP Conversation(DHAP(Directory Harvest Attack Prevention): SMTP 대화 내에 DHAP 임계값에 도달하면 연결 삭제)	잘못된 수신자의 임계값에 도달하면 어플라이언스가 연결을 삭제합니다.
시간당 올바르지 않은 최대 수신자 코드:	연결 삭제 시 사용할 코드를 지정합니다. 기본 코드는 550입니다.
시간당 올바르지 않은 최대 수신인 텍스트:	삭제된 연결에 사용할 텍스트를 지정합니다. 기본 텍스트는 "Too many invalid recipients(잘못된 수신자가 너무 많음)"입니다.
Drop Connection if DHAP threshold is reached within an SMTP Conversation(SMTP 대화 내에 DHAP 임계값에 도달하면 연결 삭제)	SMTP 대화 내에 DHAP 임계값에 도달하면 연결을 삭제하도록 설정합니다.
Max. Invalid Recipients Per Hour Code(시간당 최대 잘못된 수신자 수 코드)	SMTP 대화 내에서 DHAP로 인한 연결 삭제 시 사용할 코드를 지정합니다. 기본 코드는 550입니다.

파라미터	설명
시간당 올바르지 않은 최대 수신인 텍스트:	SMTP 대화 내에서 DHAP로 인한 연결 삭제 시 사용할 텍스트를 지정합니다.
스팸 탐지	
Anti-spam scanning(안티 스팸 검사)	이 리스너에서 안티 스팸 검사를 활성화합니다.
바이러스 탐지	
Anti-virus scanning(안티 바이러스 검사)	이 리스너에서 안티바이러스 검사를 활성화합니다.
암호화 및 인증	
TLS	이 리스너에 대한 SMTP 대화에서 TLS(Transport Layer Security)를 Deny(거부), Prefer(기본 설정) 또는 Require(필수)로 설정합니다. Preferred(기본 설정)를 선택하는 경우, 도메인 및 이메일 주소를 지정하는 Address List(주소 리스트)를 선택하여 특정 도메인에서 오는 봉투 발신자 또는 특정 이메일 주소의 봉투 발신자에 대해 TLS를 필수로 지정할 수 있습니다. 이 리스트의 주소 또는 도메인과 일치하는 봉투 발신자가 TLS를 사용하지 않는 연결을 통해 메시지를 전송하려고 시도하면 어플라이언스는 연결을 거부하며 발신자는 TLS를 사용하여 다시 시도해야 합니다. Verify Client Certificate(클라이언트 인증서 확인) 옵션은 클라이언트 인증서가 유효한 경우 사용자 메일 애플리케이션에 대한 TLS 연결을 설정하도록 Email Security Appliance에 지시합니다. TLS Preferred(TLS 기본 설정) 설정에 이 옵션을 선택한 경우, 사용자에게 인증서가 없으면 어플라이언스는 비 TLS 연결을 허용하지만 사용자가 잘못된 인증서를 가지고 있으면 연결을 거부합니다. TLS Required(TLS 필수) 설정에 이 옵션을 선택하는 경우, 어플라이언스에서 연결을 허용하려면 사용자에게 유효한 인증서가 있어야 합니다. 주소 리스트 만들기에 대한 자세한 내용은 수신 연결 규칙에 발신자 주소 리스트 사용, 116 페이지 섹션을 참조해 주십시오. TLS 연결에 클라이언트 인증서를 사용하는 방법에 대한 자세한 내용은 어플라이언스에서 TLS 연결 설정, 787 페이지 섹션을 참조해 주십시오.
SMTP 인증	리스너에 연결하는 원격 호스트의 SMTP 인증을 허용하거나 허용하지 않거나 요구합니다. SMTP 인증에 대한 자세한 내용은 "LDAP 쿼리" 장을 참조해 주십시오.
TLS와 SMTP 인증이 모두 사용 가능한 경우:	TLS에 SMTP 인증을 제공하도록 요구합니다.
Domain Key/ DKIM Signing(Domain Key/DKIM 서명)	이 리스너에 대해 Domain Keys 또는 DKIM 서명을 활성화합니다(ACCEPT 및 RELAY만).
DKIM 확인	DKIM 확인을 활성화합니다.

파라미터	설명
S/MIME 해독 및 확인	
S/MIME Decryption/Verification(S/MIME 해독/확인)	• S/MIME 해독 또는 확인을 활성화합니다. • S/MIME 확인 후 메시지에서 디지털 서명을 유지할지 제거할지를 선택합니다. 삼중 래핑(triple wrapped) 메시지의 경우 내부 서명만 유지 또는 제거됩니다.
S/MIME 공개 키 수집	
S/MIME 공개 키 수집(S/MIME 공개 키 수집)	S/MIME 공개 키 수집을 활성화합니다.
Harvest Certificates on Verification Failure(확인 실패 시 인증서 수집)	서명된 수신 메시지의 확인에 실패할 경우 공개 키를 수집할지 여부를 선택합니다.
Store Updated Certificate(업데이트된 인증서 저장)	업데이트된 공개 키를 수집할지 여부를 선택합니다.
SPF/SIDF 확인	
Enable SPF/SIDF Verification(SPF/SIDF 확인 활성화)	이 리스너에서 SPF/SIDF 서명을 활성화합니다. 자세한 내용은 이메일 인증, 571 페이지를 참고해 주십시오.
Conformance Level(적합성 레벨)	SPF/SIDF 적합성 레벨을 설정합니다. SPF, SIDF 또는 SIDF Compatible 중에서 선택합니다. 자세한 내용은 이메일 인증, 571 페이지 섹션을 참조해 주십시오.
Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used:('Resent-Sender:' 또는 'Resent-From:'이 사용된 경우 PRA 확인 결과 다운그레이드:)	SIDF Compatible(SIDF 호환)의 적합성 레벨을 선택할 때, 메시지에 Resent-Sender: 또는 Resent-From: 헤더가 있을 경우 PRA Identity 확인의 Pass 결과를 None으로 다운그레이드할지 여부를 구성합니다. 보안을 위해 이 옵션을 선택할 수 있습니다.
HELO Test(HELO 테스트)	HELO ID를 기준으로 테스트를 수행할지 여부를 구성합니다(SPF 및 SIDF Compatible 적합성 레벨에 사용).
DMARC 확인	
Enable DMARC Verification(DMARC 확인 활성화)	이 리스너에서 DMARC 확인을 활성화합니다. 자세한 내용은 DMARC 확인, 602 페이지를 참고해 주십시오.

파라미터	설명
Use DMARC Verification Profile(DMARC 확인 프로필 사용)	이 리스너에서 사용할 DMARC 확인 프로필을 선택합니다.
DMARC Feedback Reports(DMARC 피드백 보고서)	DMARC 집계 피드백 보고서의 전송을 활성화합니다. DMARC 집계 피드백 보고서에 대한 자세한 내용은 DMARC 집계 보고서, 609 페이지 섹션을 참조해 주십시오. 참고 DMARC 사양에서는 피드백 보고서 메시지가 DMARC를 준수할 것을 요구합니다. 이러한 메시지에 DKIM 서명이 있는지 또는 적절한 SPF 기록을 게시했는지 확인해 주십시오.
태그 없는 반송	
Consider Untagged Bounces to be Valid(태그 없는 반송을 유효한 것으로 간주)	반송 확인 태그("라우팅 및 전달 기능 구성" 장에서 설명)가 활성화된 경우에만 적용됩니다. 기본적으로 어플라이언스는 태그 없는 반송을 잘못된 것으로 간주하여, Bounce Verification(반송 확인) 설정에 따라 반송을 거부하거나 맞춤화 헤더를 추가합니다. 태그 없는 반송을 잘못된 것으로 간주하도록 선택한 경우 어플라이언스는 반송 메시지를 수락합니다.
봉투 발신자 **DNS** 확인	
	발신자 확인, 119 페이지를 참조하십시오.
예외 테이블	
Use Exception Table(예외 테이블 사용)	발신자 확인 도메인 예외 테이블을 사용합니다. 예외 테이블은 하나만 사용할 수 있지만, 메일 플로우 정책 단위로 활성화할 수 있습니다. 자세한 내용은 발신자 확인 예외 테이블, 122 페이지를 참조해 주십시오.

참고 HAT에서 안티 스팸 또는 안티바이러스 검사가 전역적으로 활성화된 경우, 어플라이언스에서 메시지를 수락할 때 메시지에 안티 스팸 또는 안티바이러스 검사에 대한 플래그가 지정됩니다. 메시지가 수락된 후 안티 스팸 또는 안티바이러스 검사가 비활성화된 경우, 작업 대기열을 떠날 때 여전히 메시지에 대한 검사가 수행될 수 있습니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

메일 플로우 정책에 대한 기본값 정의

단계 **1** **Mail Policies(**메일 정책**) > Mail Flow Policies(**메일 플로우 정책**)**를 클릭합니다.

단계 **2** 수정할 리스너를 Listener(리스너) 필드에서 선택합니다.

단계 **3** 구성된 메일 플로우 정책 아래에 있는 **Default Policy Parameters(**기본 정책 매개변수**)** 링크를 클릭합니다.

단계 **4** 이 리스너에 대한 모든 메일 플로우 정책에서 사용할 기본값을 정의합니다.

속성에 대한 자세한 내용은 메일 플로우 정책을 사용하여 수신 메시지에 대한 규칙 정의, 108 페이지 섹션을 참조해 주십시오.

단계 **5** 변경 사항을 제출 및 커밋합니다.

HAT(Host Access Table) 컨피그레이션 작업

HAT(Host Access Table)에 저장된 모든 정보를 파일로 내보낼 수 있으며, 파일에 저장된 HAT 정보를 리스너에 대한 어플라이언스로 가져와서 모든 기존의 HAT 정보를 덮어쓸 수 있습니다.

관련 주제

- HAT(Host Access Table) 컨피그레이션을 외부 파일로 내보내기, 115 페이지
- 외부 파일에서 HAT(Host Access Table) 컨피그레이션 가져오기, 115 페이지

HAT(Host Access Table) 컨피그레이션을 외부 파일로 내보내기

단계 **1** Mail Policies(메일 정책) > HAT Overview(HAT 개요) 페이지로 이동합니다.

단계 **2** Listener(리스너) 메뉴에서 수정할 리스너를 선택합니다.

단계 **3** **Export HAT(HAT** 내보내기**)**를 클릭합니다.

단계 **4** 내보낸 HAT에 대한 파일 이름을 입력합니다. 이것은 어플라이언스의 configuration 디렉터리에 생성될 파일의 이름입니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

외부 파일에서 HAT(Host Access Table) 컨피그레이션 가져오기

HAT를 가져오면 현재 HAT에서 기존의 모든 HAT 항목이 제거됩니다.

단계 **1** Mail Policies(메일 정책) > HAT Overview(HAT 개요) 페이지로 이동합니다.

단계 **2** Listener(리스너) 메뉴에서 수정할 리스너를 선택합니다.

단계 **3** **Import HAT(HAT** 가져오기**)**를 클릭합니다.

단계 **4** 리스트에서 파일을 선택합니다.

참고 가져올 파일은 어플라이언스의 configuration 디렉토리에 있어야 합니다.

단계 **5** **Submit(**제출**)**를 클릭합니다. 기존의 모든 HAT 항목을 제거할 것인지 묻는 경고 메시지가 표시됩니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.

단계 **7** 변경 사항을 커밋합니다.

파일에 "코멘트"를 추가할 수 있습니다. '#' 문자로 시작되는 줄은 코멘트로 간주되어 AsyncOS에서 무시됩니다. 예를 들면 다음과 같습니다.

```
# File exported by the GUI at 20060530T215438
$BLOCKED
    REJECT {}
[ ... ]
```

수신 연결 규칙에 발신자 주소 리스트 사용

메일 플로우 정책에서는 봉투 발신자 그룹에 적용되는 특정 설정(예: 속도 제한 면제 및 필수 TLS 연결)에 주소 리스트를 사용하도록 허용합니다. 주소 리스트는 이메일 주소, 도메인, 부분 도메인 및 IP 주소로 구성됩니다. GUI의 **Mail Policies(**메일 정책**) > Address Lists(**주소 리스트**)** 페이지 또는 CLI의 `addresslistconfig` 명령을 사용하여 주소 리스트를 만들 수 있습니다. Address Lists(주소 리스트) 페이지에는 주소 리스트를 사용하는 메일 플로우 정책과 함께 어플라이언스에 있는 모든 주소 리스트가 표시됩니다.

단계 **1** **Mail Policies(**메일 정책**) > Address Lists(**주소 리스트**)**를 선택합니다.

단계 **2** **Add Address List(**주소 리스트 추가**)**를 클릭합니다.

단계 **3** 주소 리스트에 대한 이름을 입력합니다.

단계 **4** 주소 리스트의 설명을 입력합니다.

단계 **5** (선택 사항) 주소 리스트에서 전체 이메일 주소 사용을 시행하려면 **Full Email Addresses only(**전체 이메일 주소만**)**를 선택합니다.

단계 **6** 주소 리스트를 생성하려면 다음 옵션 중 하나를 선택합니다.

- 주소 리스트에서 전체 이메일 주소 사용을 시행하려면 **Full Email Addresses only(**전체 이메일 주소만**)**를 선택합니다.
- 주소 리스트에 있는 도메인을 사용하여 적용하려는 경우 **Domains only(**도메인만**)**을 선택합니다.
- 주소 리스트에서 전체 이메일 주소 사용을 시행하려면 **IP Addresses only(IP** 주소만**)**를 선택합니다.

단계 **7** 포함할 주소를 입력합니다. 다음 형식을 사용할 수 있습니다.

- 전체 이메일 주소: `user@example.com`
- 부분 이메일 주소: `user@`

  참고 **Allow only full Email Addresses(**전체 이메일 주소만 허용**)**를 선택한 경우 부분 이메일 주소를 사용할 수 없습니다.

- 이메일 주소의 IP 주소: `@[1.2.3.4]`
- 도메인의 모든 사용자: `@example.com`
- 부분 도메인의 모든 사용자: `@.example.com`

도메인과 IP 주소는 @ 문자로 시작해야 합니다.

이메일 주소는 쉼표로 구분합니다. 새 줄로 이메일 주소를 구분하는 경우 AsyncOS는 항목을 쉼표로 구분된 리스트로 자동 변환합니다.

단계 **8** 변경 사항을 제출 및 커밋합니다.

SenderBase 설정 및 메일 플로우 정책

어플라이언스에 대한 연결을 분류하고 메일 플로우 정책(속도 제한을 포함하거나 포함하지 않음)을 적용하기 위해 리스너에서는 다음 방법론을 사용합니다.

Classification(분류) -> Sender Group(발신자 그룹) -> Mail Flow Policy(메일 플로우 정책) -> Rate Limiting(속도 제한)

자세한 내용은 네트워크 소유자, 도메인 및 IP 주소별로 정의되는 발신자 그룹, 97 페이지 항목을 참조하십시오.

"분류" 단계는 전송 호스트의 IP 주소를 사용하여 인바운드 SMTP 세션(퍼블릭 리스너에서 수신)을 발신자 그룹으로 분류합니다. 이 발신자 그룹과 연결된 메일 플로우 정책에서는 속도 제한에 대한 매개변수가 활성화되어 있을 수 있습니다. (속도 제한은 세션당 최대 메시지 수, 메시지당 최대 수신자 수, 최대 메시지 크기 및/또는 원격 호스트에서 수락할 최대 동시 연결 수를 제한합니다.)

일반적으로 이 과정에서 수신자는 명명된 해당 발신자 그룹의 각 발신자에 대해 계산됩니다. 동일한 시간에 여러 발신자로부터 메일이 수신되는 경우, 모든 수신자에 대한 총 수신자 수가 제한 값과 비교됩니다.

이 계산 방법론에 몇 가지 예외가 있습니다.

- 네트워크 소유자에 의해 분류가 수행되는 경우 SenderBase Reputation Service는 대규모 주소 블록을 더 작은 블록으로 자동 분할합니다.

수신자 계산 및 수신자 속도 제한은 이런 더 작은 블록 각각에 대해 별도로 수행됩니다(일반적으로 /24 CIDR 블록과 같지만 항상 그렇지는 않음).

- HAT Significant Bits(HAT 중요 비트) 기능이 사용되는 경우. 이 경우 정책과 관련된 중요 비트 매개변수를 적용하여 더 큰 주소 블록을 더 작은 블록으로 분할할 수 있습니다.

이 매개변수는 **Mail Flow Policy(메일 플로우 정책) -> Rate Limiting(속도 제한)** 단계와 관련이 있습니다. 또한 발신자 그룹에서 IP 주소 분류에 사용될 수 있는"network/bits" CIDR 표기법의 "bits" 필드와 동일하지 않습니다.

기본적으로 SenderBase Reputation Service 및 IP Profiling 지원은 퍼블릭 리스너에 대해서는 활성화되고 프라이빗 리스너에 대해서는 비활성화됩니다.

관련 주제

- SenderBase 쿼리 시간 초과, 118 페이지
- HAT 중요 비트 기능, 118 페이지

SenderBase 쿼리 시간 초과

리스너를 구성할 때 어플라이언스가 SenderBase Reputation Service에서 쿼리된 정보를 캐시할 시간을 결정할 수 있습니다. 그런 다음 메일 플로우 정책을 구성할 때 SenderBase가 리스너로의 메일 플로우를 제어하도록 지정할 수 있습니다.

GUI에서 메일 플로우 정책을 구성할 때 "Use SenderBase for Flow Control(플로우 제어에 SenderBase 사용)" 설정을 사용하거나 CLI의 `listenerconfig > hostaccess > edit` 명령을 사용하여 메일 플로우 정책에서 SenderBase를 활성화합니다.

HAT 중요 비트 기능

AsyncOS의 3.8.3 릴리스부터, 큰 CIDR 블록에서 리스너 HAT(Host Access Table)의 항목을 관리하는 한편 IP 주소 단위로 수신 메일을 추적하고 속도를 제한할 수 있습니다. 예를 들어 수신 연결이 "10.1.1.0/24" 호스트와 일치하는 경우, 모든 트래픽을 하나의 큰 카운터로 집계하는 대신 해당 범위의 각 주소에 대해 카운터를 생성할 수 있습니다.

참고 중요 비트 HAT 정책 옵션을 적용하려면 HAT에 대한 Flow Control(플로우 제어) 옵션에서 "User SenderBase(사용자 SenderBase)"를 활성화해서는 안 됩니다(또는 CLI에서 `listenerconfig -> setup` 명령을 실행할 경우 SenderBase Information Service를 활성화할지 묻는 질문, "Would you like to enable SenderBase Reputation Filters and IP Profiling support?(SenderBase Reputation Filters 및 IP Profiling 지원을 활성화하시겠습니까?)"에 대해 **no(**아니요**)**로 답해야 합니다). 즉, HAT 중요 비트 기능과 SenderBase IP Profiling 지원 활성화는 상호 배타적입니다.

대부분의 경우 발신자 그룹을 폭넓게("10.1.1.0/24" 또는 "10.1.0.0/16"과 같은 대규모 IP 주소 그룹) 정의하는 데 이 기능을 사용할 수 있습니다. 반면, 메일 플로우 속도 제한은 좀 더 작은 IP 주소 그룹에 좁게 적용합니다.

HAT 중요 비트 기능은 다음과 같은 시스템 구성 요소에 해당합니다.

- HAT 컨피그레이션 , 118 페이지
- 중요 비트 HAT 정책 옵션 , 119 페이지
- 주입 제어 주기 , 119 페이지

HAT 컨피그레이션

HAT 컨피그레이션에는 발신자 그룹과 메일 플로우 정책이라는 두 부분이 있습니다. 발신자 그룹 컨피그레이션은 발신자의 IP 주소를 "분류"하는(발신자 그룹에 넣는) 방법을 정의합니다. 메일 플로우 정책 컨피그레이션은 해당 IP 주소에서 SMTP 세션을 제어하는 방법을 정의합니다. 이 기능을 사용하면 IP 주소는 "CIDR 블록"(예: 10.1.1.0/24) 발신자 그룹으로 분류되는 한편 개별 호스트(/32)로서 제어될 수 있습니다. 이는 "signficant_bits" 정책 컨피그레이션 설정을 통해 수행됩니다.

중요 비트 HAT 정책 옵션

HAT 구문에서는 signficant_bits 컨피그레이션 옵션이 허용됩니다. 이 기능은 GUI의 Mail Policies(메일 정책) > Mail Flow Policies(메일 플로우 정책) 페이지에 나타납니다.

플로우 제어에 SenderBase를 사용하는 옵션이 "OFF"이거나 Directory Harvest Attack Prevention이 활성화된 경우, "significant bits" 값이 연결 발신자의 IP 주소에 적용되며, HAT 내에서 정의된 발신자 그룹을 확인하기 위한 토큰으로 결과 CIDR 표기법이 사용됩니다. CIDR 블록에 포함되는 가장 오른쪽 비트는 문자열을 만들 때 "제로 아웃(zeroed out)"됩니다. 따라서 IP 주소 1.2.3.4에서의 연결이 이루어지고 significant_bits 옵션이 24로 설정된 정책과 일치하면 결과 CIDR 블록은 1.2.3.0/24가 됩니다. 따라서 이 기능을 사용함으로써, HAT 발신자 그룹 항목(이 경우 10.1.1.0/24)은 해당 그룹에 할당된 정책의 중요 비트 항목(이 경우 32)과 다른 네트워크 중요 비트 숫자(24)를 가질 수 있습니다.

`listenerconfig` 명령에 대한 자세한 내용은 AsyncOS for Cisco Email Security Appliance CLI 참조 가이드를 참고하십시오.

주입 제어 주기

주입 제어 카운터가 재설정되는 시기를 조정할 수 있는 전역 컨피그레이션 옵션이 있습니다. 상당히 많은 수의 서로 다른 IP 주소에 대한 카운터를 유지 관리하는 매우 분주한 시스템의 경우 좀 더 자주 재설정되도록 카운터를 구성하면(예: 60분이 아니라 15분마다), 데이터가 관리할 수 없는 크기로 커져 시스템 성능에 영향을 주는 상황을 피할 수 있습니다.

현재 기본값은 3,600초(1시간)입니다. 1분(60초)에서 4시간(14,400초)까지 기간을 지정할 수 있습니다.

GUI를 통해 전역 설정을 사용하여 이 기간을 조정할 수 있습니다(자세한 내용은 리스너에 대한 전역 설정 구성, 72 페이지 참조).

CLI의 `listenerconfig -> setup` 명령으로도 이 기간을 조정할 수 있습니다. `listenerconfig` 명령에 대한 자세한 내용은 AsyncOS for Cisco Email Security Appliance CLI 참조 가이드를 참고하십시오.

발신자 확인

도메인 또는 IP 주소를 DNS로 확인할 수 없는 발신자에 의해 스팸 및 원치 않는 메일이 자주 전송됩니다. DNS 확인 기능을 사용하면 발신자에 대한 신뢰할 수 있는 정보를 얻고 그에 따라 메일을 처리할 수 있습니다. SMTP 대화 전에 발신자를 확인하면(발신자 IP 주소의 DNS 조회를 기반으로 연결 필터링) 어플라이언스에서 메일 파이프라인을 통해 처리되는 정크 이메일의 양을 줄이는 데에도 도움이 됩니다.

미확인 발신자의 메일은 자동으로 삭제되지 않습니다. 대신 AsyncOS는 어플라이언스에서 미확인 발신자의 메일을 처리하는 방법을 지정할 수 있는 발신자 확인 설정을 제공합니다. 예를 들면 SMTP 대화 전에 미확인 발신자의 메일을 모두 자동 차단하거나 미확인 발신자를 조절(throttle)하도록 어플라이언스를 구성할 수 있습니다.

발신자 확인 기능은 다음으로 구성됩니다.

- 연결하는 호스트의 확인. 이는 SMTP 대화 전에 발생합니다. 자세한 내용은 발신자 확인: 호스트, 120 페이지를 참고해 주십시오.

- 봉투 발신자의 도메인 부분 확인. 이는 SMTP 대화 중에 발생합니다. 자세한 내용은 발신자 확인: 봉투 발신자, 121 페이지를 참고하십시오.

관련 주제

- 발신자 확인: 호스트, 120 페이지
- 발신자 확인: 봉투 발신자, 121 페이지
- 발신자 확인 구현 - 설정 예, 123 페이지
- 미확인 발신자의 메시지에 대한 설정 테스트, 125 페이지
- 발신자 확인 및 로깅, 127 페이지

발신자 확인: 호스트

여러 이유로 발신자가 확인되지 않을 수 있습니다. 예를 들면 DNS 서버가 "다운"되었거나 응답하지 않거나 도메인이 존재하지 않을 수 있습니다. 발신자 그룹에 대한 호스트 DNS 확인 설정을 사용하면 SMTP 대화 전에 미확인 발신자를 분류하고 여러 유형의 미확인 발신자를 다양한 발신자 그룹에 포함할 수 있습니다.

어플라이언스는 수신 메일에 대해 DNS를 통해 연결하는 호스트의 전송 도메인을 확인하려고 시도합니다. 이 확인은 SMTP 대화 전에 수행됩니다. 시스템은 이중 *DNS* 조회를 수행하여 원격 호스트 IP 주소(즉, 도메인)의 유효성을 획득하고 확인합니다. 이중 DNS 조회는 연결하는 호스트의 IP 주소에 대한 역방향 DNS(PTR) 조회 및 그 뒤에 오는 PTR 조회의 결과에 대한 정방향 DNS(A) 조회로 정의됩니다. 그런 다음 어플라이언스는 A 조회의 결과가 PTR 조회의 결과와 일치하는지를 확인합니다. PTR 또는 A 조회가 실패하거나 결과가 일치하지 않으면, 시스템은 HAT에 있는 항목의 확인을 위해 IP 주소만 사용하며 발신자는 확인되지 않은 것으로 간주됩니다.

미확인 발신자는 다음 범주로 분류됩니다.

- 연결하는 호스트 PTR 기록이 DNS에 존재하지 않습니다.
- 연결 호스트의 PTR 레코드 찾기가 일시적인 DNS 장애로 실패했습니다.
- 연결하는 호스트 역방향 DNS 조회(PTR)가 정방향 DNS 조회(A)와 일치하지 않습니다.

발신자 그룹 "Connecting Host DNS Verification(연결하는 호스트 DNS 확인)" 설정을 사용하여 미확인 발신자의 동작을 지정할 수 있습니다(SUSPECTLIST 발신자 그룹을 확인하여 미확인 발신자의 메시지 조절, 124 페이지 참조).

발신자 그룹에 대해 발신자 그룹 설정에서 호스트 DNS 확인을 활성화할 수 있습니다. 그러나 발신자 그룹에 호스트 DNS 확인 설정을 추가하면 해당 그룹에 미확인 발신자가 포함됩니다. 즉, 스팸 및 기타 원치 않는 메일이 포함되는 것입니다. 따라서 이 설정은 발신자를 거부하거나 조절(throttle)하는 데 사용되는 발신자 그룹에서만 활성화해야 합니다. 예를 들어 WHITELIST 발신자 그룹에서 호스트 DNS 확인을 활성화하면 미확인 발신자의 메일이 WHITELIST에 있는 신뢰할 수 있는 발신자의 메일과 동일하게 취급됩니다(메일 플로우 정책이 구성된 방법에 따라 안티 스팸/안티바이러스 확인 우회, 속도 제한 등).

발신자 확인: 봉투 발신자

봉투 발신자 확인에서 봉투 발신자의 도메인 부분은 DNS로 확인됩니다. (봉투 발신자 도메인이 확인됩니까? 봉투 발신자 도메인에 대한 DNS에 A 또는 MX 기록이 있습니까?) DNS에서 조회하려고 시도하는 동안 시간 초과 또는 DNS 서버 장애 등 일시적인 오류 조건이 발생하면 도메인이 확인되지 않습니다. 반면, 조회를 시도할 때 "domain does not exist(도메인이 존재하지 않음)"라는 확실한 상태가 반환되면 도메인이 존재하지 않는 것입니다. 이 확인은 SMTP 대화 중에 발생하는 반면, 호스트 DNS 확인은 대화가 시작되기 전에 발생하며 연결하는 SMTP 서버의 IP 주소에 적용됩니다.

자세히 말하면, AsyncOS는 발신자 주소의 도메인에 대한 MX 기록 쿼리를 수행합니다. 그런 다음 MX 기록 조회의 결과를 기반으로 A 기록 조회를 수행합니다. DNS 서버가 "NXDOMAIN"을 반환하면(이 도메인에 대한 기록 없음), AsyncOS는 해당 도메인을 존재하지 않는 것으로 취급합니다. 이는 "Envelope Senders whose domain does not exist(도메인이 존재하지 않는 봉투 발신자)" 범주에 해당합니다. NXDOMAIN은 루트 이름 서버가 이 도메인에 대해 신뢰할 수 있는 이름 서버를 제공하지 않음을 의미할 수 있습니다.

그러나 DNS 서버가 "SERVFAIL"을 반환하면 이는 "Envelope Senders whose domain does not resolve(도메인이 확인되지 않는 봉투 발신자)"로 분류됩니다. SERVFAIL은 도메인이 존재하지 않지만 DNS에 기록 조회와 관련된 일시적인 문제가 있음을 의미합니다.

스패머 또는 불법 메일 발신자의 일반적인 수법은 수락된 미확인 발신자의 메일이 처리될 수 있도록 MAIL FROM 정보를 위조(봉투 발신자에서)하는 것입니다. 이 경우 MAIL FROM 주소로 전송된 반송 메시지를 전송할 수 없으므로 문제가 될 수 있습니다. 봉투 발신자 확인을 사용하면 형식이 잘못된(그러나 비어 있지 않은) MAIL FROM의 메일을 거부하도록 어플라이언스를 구성할 수 있습니다.

각 메일 플로우 정책에 대해 다음을 수행할 수 있습니다.

- 봉투 발신자 DNS 확인을 활성화합니다.
- 형식이 잘못된 봉투 발신자에 대해 맞춤화 SMTP 코드 및 응답을 제공합니다. 봉투 발신자 DNS 확인을 활성화한 경우 형식이 잘못된 봉투 발신자가 차단됩니다.
- 확인되지 않는 봉투 발신자 도메인에 대한 맞춤화 응답을 제공합니다.
- DNS에 존재하지 않는 봉투 발신자 도메인에 대한 맞춤화 응답을 제공합니다.

발신자 확인 예외 테이블을 사용하여 메일을 자동으로 허용하거나 거부할 도메인 또는 주소의 리스트를 저장할 수 있습니다(발신자 확인 예외 테이블, 122 페이지 참조). 발신자 확인 예외 테이블은 봉투 발신자 확인과 별도로 활성화할 수 있습니다. 따라서 예를 들면 봉투 발신자 확인을 활성화하지 않고도 예외 테이블에 지정된 특수 주소나 도메인을 여전히 거부할 수 있습니다. 또한 내부 또는 테스트 도메인의 메일은 달리 확인하지 않더라도 항상 허용할 수 있습니다.

대부분의 스팸은 미확인 발신자로부터 오지만, 미확인 발신자의 메일을 수락해야 할 이유도 있습니다. 예를 들면, DNS 조회를 통해 모든 합법적인 이메일을 확인할 수 있는 것은 아닙니다. DNS 서버에 일시적인 문제가 발생하면 발신자 확인이 중단될 수 있습니다.

미확인 발신자의 메일이 시도되면 발신자 확인 예외 테이블 및 메일 플로우 정책 봉투 발신자 DNS 확인 설정이 SMTP 대화 중에 봉투 발신자를 분류하는 데 사용됩니다. 예를 들면 DNS에 존재하지 않기 때문에 확인되지 않은 도메인에서 전송하는 메일을 수락 및 조절(throttle)할 수 있습니다. 해당 메일이 수락되면, 형식이 잘못된 MAIL FROM의 메시지는 맞춤화가 가능한 SMTP 코드 및 응답으로 거부됩니다. 이는 SMTP 대화 중에 발생합니다.

메일 플로우 정책에 대해 GUI 또는 CLI(`listenerconfig -> edit -> hostaccess -> < policy >`)를 통해 메일 플로우 정책 설정에서 봉투 발신자 DNS 확인(도메인 예외 테이블 포함)을 활성화할 수 있습니다.

관련 주제

- 부분 도메인, 기본 도메인 및 형식이 잘못된 MAIL FROM, 122 페이지
- 맞춤화 SMTP 코드 및 응답, 122 페이지
- 발신자 확인: 봉투 발신자, 121 페이지

부분 도메인, 기본 도메인 및 형식이 잘못된 MAIL FROM

봉투 발신자(envelope sender) 확인을 활성화하거나 SMTP Address Parsing(SMTP 주소 구문 분석) 옵션에서 리스너에 대해 부분 도메인 허용을 비활성화하는 경우("이메일을 수신하도록 게이트웨이 구성" 장의 SMTP 주소 구문 분석 옵션 섹션 참조), 해당 리스너에 대한 기본 도메인 설정이 더 이상 사용되지 않습니다.

이러한 기능은 상호 배타적입니다.

맞춤화 SMTP 코드 및 응답

형식이 잘못된 봉투 발신자의 메시지, DNS에 존재하지 않는 봉투 발신자, DNS 쿼리를 통해 확인되지 않는 봉투 발신자(예: DNS 서버가 다운됨) 등에 대해 SMTP 코드 및 응답 메시지를 지정할 수 있습니다.

SMTP 응답에 `$EnvelopeSender` 변수를 포함할 수 있습니다. 이 변수는 맞춤화 응답이 전송될 때 봉투 발신자의 값으로 확장됩니다.

일반적으로 "Domain does not exist(도메인이 존재하지 않음)" 결과는 영구적이지만 경우에 따라 일시적인 조건일 수도 있습니다. 그러한 경우를 처리하기 위해 "보수적인" 사용자는 오류 코드를 기본값 5XX에서 4XX 코드로 변경할 수 있습니다.

발신자 확인 예외 테이블

발신자 확인 예외 테이블은 SMTP 대화 중 자동으로 허용하거나 거부할 도메인 또는 이메일 주소의 리스트입니다. 또한 선택적인 SMTP 코드를 지정하고 거부된 도메인에 대한 응답을 거부할 수 있습니다. 발신자 확인 예외 테이블은 어플라이언스당 하나만 가능하며 메일 플로우 정책 단위로 활성화됩니다.

발신자 확인 예외 테이블을 사용하면 명백히 가짜지만 형식이 올바른 도메인 또는 이메일 주소를 나열할 수 있으며, 그러한 곳에서 오는 메일을 거부할 수 있습니다. 예를 들면 형식이 올바른 MAIL FROM: `pres@whitehouse.gov`를 발신자 확인 예외 테이블에 나열하고 자동으로 거부되도록 설정할 수 있습니다. 내부 또는 테스트 도메인 등 자동으로 허용할 도메인을 나열할 수도 있습니다. 이는 RAT(Recipient Access Table)에서 발생하는 봉투 수신자(SMTP RCPT TO 명령) 처리와 유사합니다.

발신자 확인 예외 테이블은 GUI의 Mail Policies(메일 정책) > Exception Table(예외 테이블) 페이지에서(또는 CLI의 `exceptionconfig` 명령을 통해) 정의할 수 있으며, GUI(ACCEPTED 메일 플로우 정책을 사용하여 미확인 발신자에게 전송할 메시지 정의, 124 페이지 참조) 또는 CLI(*AsyncOS for Cisco Email Security Appliance*용 *CLI* 참조 설명서 참조)를 통해 정책 단위로 활성화할 수 있습니다.

발신자 확인 예외 테이블에 있는 항목의 구문은 다음과 같습니다.

예외 테이블 수정에 대한 자세한 내용은 발신자의 이메일 주소를 기반으로 발신자 확인 규칙에서 미확인 발신자 제외, 125 페이지 섹션을 참조해 주십시오.

발신자 확인 구현 - 설정 예

이 섹션에서는 호스트 및 봉투 발신자 확인을 보수적으로 구현하는 일반적인 경우의 예를 제공합니다.

이 예의 경우 호스트 발신자 확인을 구현할 때, 역방향 DNS 조회가 일치하지 않는 연결하는 호스트에서 오는 메일은 기존의 SUSPECTLIST 발신자 그룹 및 THROTTLED 메일 플로우 정책을 통해 조절(throttle)됩니다.

새 발신자 그룹(UNVERIFIED) 및 새 메일 플로우 정책 (THROTTLEMORE)이 생성됩니다. 확인되지 않은 연결하는 호스트에서 오는 메일은 SMTP 대화 전에 조절(throttle)됩니다(UNVERIFIED 발신자 그룹 및 좀 더 적극적인 THROTTLEMORE 메일 플로우 정책을 사용하여).

봉투 발신자 확인은 ACCEPTED 메일 플로우 정책에 대해 활성화됩니다.

다음 표에서는 발신자 확인 구현을 위한 설정 제안을 보여줍니다.

표 ***18:*** 발신자 확인*:* 설정 제안

발신자 그룹	정책	포함
UNVERIFIED SUSPECTLIST	THROTTLEMORE THROTTLED	SMTP 대화 전: 연결하는 호스트 PTR 기록이 DNS에 존재하지 않습니다. 연결하는 호스트 역방향 DNS 조회(PTR)가 정방향 DNS 조회(A)와 일치하지 않습니다.
	ACCEPTED	SMTP 대화 중 봉투 발신자 확인: - 형식이 잘못된 MAIL FROM: - 봉투 발신자가 DNS에 존재하지 않음. - 봉투 발신자 DNS가 확인되지 않음.

관련 주제

- SUSPECTLIST 발신자 그룹을 확인하여 미확인 발신자의 메시지 조절, 124 페이지
- 미확인 발신자에 대해 좀 더 엄격한 조절 설정 구현, 124 페이지
- ACCEPTED 메일 플로우 정책을 사용하여 미확인 발신자에게 전송할 메시지 정의, 124 페이지
- 발신자의 이메일 주소를 기반으로 발신자 확인 규칙에서 미확인 발신자 제외, 125 페이지
- 발신자 확인 예외 테이블 내에서 주소 검색, 125 페이지

SUSPECTLIST 발신자 그룹을 확인하여 미확인 발신자의 메시지 조절

단계 1 **Mail Policies(**메일 정책**) > HAT Overview(HAT** 개요**)**를 선택합니다.

단계 2 발신자 그룹의 리스트에서 **SUSPECTLIST**를 클릭합니다.

단계 3 **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 4 리스트에서 THROTTLED 정책을 선택합니다.

단계 5 Connecting Host DNS Verification(연결하는 호스트 DNS 확인) 아래에서 "Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)(연결하는 호스트 역방향 DNS 조회(PTR)가 정방향 DNS 조회(A)와 일치하지 않음)" 확인란을 선택합니다.

단계 6 변경 사항을 제출 및 커밋합니다.

이제 역방향 DNS 조회에 실패한 발신자는 SUSPECTLIST 발신자 그룹과 일치하게 되며, THROTTLED 메일 플로우 정책에서 기본 작업을 수신합니다.

미확인 발신자에 대해 좀 더 엄격한 조절 설정 구현

단계 1 새 메일 플로우 정책을 만들고(이 경우 이름을 THROTTLEMORE로 지정) 좀 더 엄격한 조절(throttling) 설정으로 구성합니다.

a) Mail Flow Policies(메일 플로우 정책) 페이지에서 **Add Policy(**정책 추가**)**를 클릭합니다.

b) 메일 플로우 정책의 이름을 입력하고 Connection Behavior(연결 동작)로 Accept(수락)를 선택합니다.

c) 메일을 조절할 정책을 구성합니다.

d) 변경 사항을 제출 및 커밋합니다.

단계 2 새 발신자 그룹을 만들고(이 경우 이름을 UNVERIFIED로 지정) THROTTLEMORE 정책을 사용하도록 구성합니다.

a) HAT Overview(HAT 개요) 페이지에서 **Add Sender Group(**발신자 그룹 추가**)**을 클릭합니다.

b) 리스트에서 THROTTLEMORE 정책을 선택합니다.

c) Connecting Host DNS Verification(연결하는 호스트 DNS 확인) 아래에서 "Connecting host PTR record does not exist in DNS(연결하는 호스트 PTR 기록이 DNS에 존재하지 않음)" 확인란을 선택합니다.

d) 변경 사항을 제출 및 커밋합니다.

ACCEPTED 메일 플로우 정책을 사용하여 미확인 발신자에게 전송할 메시지 정의

단계 1 **Mail Policies(**메일 정책**) > Mail Flow Policies(**메일 플로우 정책**)**를 선택합니다.

단계 2 Mail Flow Policies(메일 플로우 정책) 페이지에서 ACCEPTED 메일 플로우 정책을 클릭합니다.

단계 3 **Sender Verification(**발신자 확인**)** 섹션으로 스크롤합니다.

단계 4 **Envelope Sender DNS Verification(**봉투 발신자 **DNS** 확인**)** 섹션에서 다음을 수행합니다.

- 이 메일 플로우 정책에 대해 봉투 발신자 DNS 확인을 활성화하려면 **On**을 선택합니다.

- 맞춤화 SMTP 코드 및 응답을 정의할 수도 있습니다.

단계 **5** **Use Domain Exception Table(**도메인 예외 테이블 사용**)**에서 **On**을 선택하여 도메인 예외 테이블을 활성화합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

발신자의 이메일 주소를 기반으로 발신자 확인 규칙에서 미확인 발신자 제외

단계 **1** **Mail Policies(**메일 정책**) > Exception Table(**예외 테이블**)**을 선택합니다.

참고 예외 테이블은 "Use Exception Table(예외 테이블 사용)"이 활성화된 모든 메일 플로우 정책에 전역적으로 적용됩니다.

단계 **2** Mail Policies(메일 정책) > Exception Table(예외 테이블) 페이지에서 **Add Domain Exception(**도메인 예외 추가**)**을 클릭합니다.

단계 **3** 이메일 주소를 입력합니다. 특정 주소(pres@whitehouse.gov), 이름(user@), 도메인(@example.com or @.example.com) 또는 대괄호에 IP 주소가 있는 주소(user@[192.168.23.1])를 입력할 수 있습니다.

단계 **4** 주소에서 오는 메시지를 허용할지 또는 거부할지를 지정합니다. 메일을 거부하는 경우 SMTP 코드 및 맞춤화 응답을 지정할 수도 있습니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

발신자 확인 예외 테이블 내에서 주소 검색

단계 **1** Exception Table(예외 테이블) 페이지의 Find Domain Exception(도메인 예외 찾기) 섹션에 이메일 주소를 입력합니다.

단계 **2** **Find(**찾기**)**를 클릭합니다.

주소가 테이블에 있는 항목과 일치하면 첫 번째 일치 항목이 표시됩니다.

미확인 발신자의 메시지에 대한 설정 테스트

발신자 확인 설정을 구성했으므로 이제 어플라이언스의 동작을 확인할 수 있습니다.

DNS 관련 설정을 테스트하는 것은 이 문서의 범위를 벗어납니다.

관련 주제

- 형식이 잘못된 MAIL FROM 발신자 주소의 테스트 메시지 전송, 126 페이지
- 발신자 확인 규칙에서 제외된 주소의 메시지 전송, 126 페이지

형식이 잘못된 **MAIL FROM** 발신자 주소의 테스트 메시지 전송

THROTTLED 정책에 대한 각종 DNS 관련 설정을 테스트하는 것은 어려울 수 있지만, 형식이 잘못된 MAIL FROM 설정은 다음과 같이 테스트할 수 있습니다.

단계 **1** 어플라이언스에 대한 텔넷(Telnet) 세션을 엽니다.

단계 **2** SMTP 명령을 사용하여 형식이 잘못된 MAIL FROM(예: 도메인 없는 "admin")의 테스트 메시지를 전송합니다.

참고 이메일을 전송하거나 수신할 때 기본 도메인을 사용하거나 부분 도메인을 명확하게 허용하도록 어플라이언스를 구성한 경우 또는 주소 구문 분석을 활성화한 경우("이메일을 수신하도록 게이트웨이 구성" 장 참조), 도메인의 형식이 잘못되거나 누락된 이메일의 생성, 전송 및 수신이 불가능할 수 있습니다.

단계 **3** 메시지가 거부되는지 확인합니다.

```
# telnet IP_address_of_Email_Security_Appliance port
220 hostname ESMTP
helo example.com
250 hostname
mail from: admin
553 #5.5.4 Domain required for sender address
```

SMTP 코드 및 응답은 THROTTLED 메일 플로우 정책의 봉투 발신자 확인 설정에 대해 구성한 것입니다.

발신자 확인 규칙에서 제외된 주소의 메시지 전송

발신자 확인 예외 테이블에 나열된 이메일 주소의 메일이 봉투 발신자 확인의 영향을 받지 않는지 확인하려면

단계 **1** admin@zzzaaazzz.com 주소를 "Allow(허용)" 동작과 함께 예외 테이블에 추가합니다.

단계 **2** 변경 사항을 커밋합니다.

단계 **3** 어플라이언스에 대한 텔넷 세션을 엽니다.

단계 **4** SMTP 명령을 사용하여 발신자 확인 예외 테이블에 입력한 이메일 주소(admin@zzzaaazzz.com)의 테스트 메시지를 전송합니다.

단계 **5** 메시지가 수락되는지 확인합니다.

```
# telnet IP_address_of_Email_Security_Appliance port
220 hostname ESMTP
helo example.com
250 hostname
mail from: admin@zzzaaazzz.com
250 sender <admin@zzzaaazzz.com> ok
```

발신자 확인 예외 테이블에서 해당 이메일 주소를 제거하면, 봉투 발신자의 도메인 부분이 DNS로 확인되지 않으므로 해당 발신자의 메일이 거부됩니다.

발신자 확인 및 로깅

다음 로그 항목은 발신자 확인 판정의 예를 제공합니다.

관련 주제

• 봉투 발신자 확인, 127 페이지

봉투 발신자 확인

잘못된 형식의 봉투 발신자:

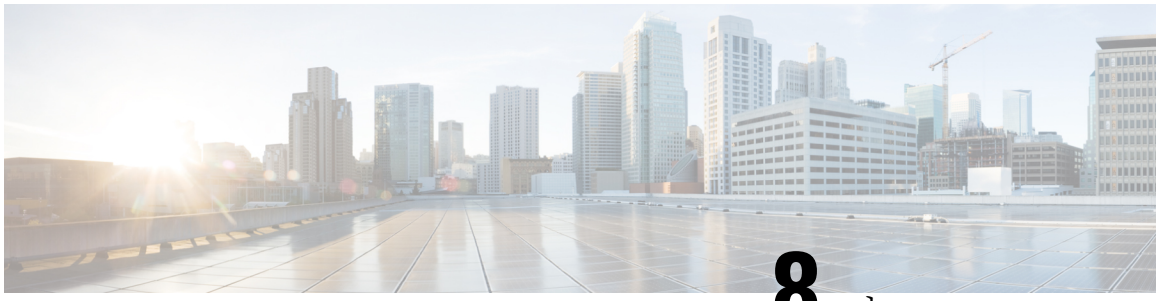
```
Thu Aug 10 10:14:10 2006 Info: ICID 3248 Address: <user> sender rejected, envelope sender
 domain missing
```

도메인이 존재하지 않음(NXDOMAIN):

```
Wed Aug  9 15:39:47 2006 Info: ICID 1424 Address: <user@domain.com> sender rejected, envelope
 sender domain does not exist
```

도메인이 확인되지 않음(SERVFAIL):

```
Wed Aug  9 15:44:27 2006 Info: ICID 1425 Address: <user@domain.com> sender rejected, envelope
 sender domain could not be resolved
```



8 장

도메인 이름 또는 수신자 주소를 기반으로 연결 수락 또는 거부

이 장에는 다음 섹션이 포함되어 있습니다.

수신자 주소를 기반으로 연결 수락 또는 거부 개요

AsyncOS는 각 퍼블릭 리스너에 대해 RAT(Recipient Access Table)를 사용하여 수신자 주소에 대한 작업의 수락 또는 거부를 관리합니다. 수신자 주소에는 다음이 포함됩니다.

- 도메인
- 이메일 주소
- 이메일 주소 그룹

관리자는 시스템 설정 마법사를 통해 어플라이언스에서 하나 이상의 퍼블릭 리스너를 기본값으로 구성할 수 있습니다. 설정 중 퍼블릭 리스너를 구성하는 경우 메일을 수락할 기본 로컬 도메인 또는 특정 주소를 지정할 수 있습니다. 이러한 로컬 도메인 또는 특정 주소는 해당 퍼블릭 리스너용 RAT의 첫 번째 항목입니다.

각 퍼블릭 리스너에서 기본 항목인 "All Other Recipients(다른 모든 수신자)"는 모든 수신자의 이메일을 거부합니다. 관리자는 어플라이언스가 메시지를 수락할 모든 로컬 도메인을 정의합니다. 선택적으로, 어플라이언스에서 메시지를 수락하거나 거부할 특정 사용자를 정의할 수도 있습니다. AsyncOS에서는 RAT(Recipient Access Table)를 사용하여 수락할 로컬 도메인 및 특정 사용자를 정의할 수 있습니다.

여러 도메인에 대한 메시지를 수락하도록 리스너를 구성해야 할 수 있습니다. 예를 들어 현재 조직에서 `currentcompanyname.com` 도메인을 사용 중이고 전에는 `oldcompanyname.com`을 사용했다면

currentcompanyname.com과 oldcompanyname.com 모두의 메시지를 수락할 수 있습니다. 이 경우 퍼블릭 리스너에 대한 RAT에 두 로컬 도메인을 모두 포함합니다.

(참고: 도메인 맵 기능은 한 도메인의 메시지를 다른 도메인으로 매핑합니다. "라우팅 및 전달 기능 구성" 장의 도메인 맵(Domain Map) 기능 섹션을 참조해 주십시오.)

RAT(Recipient Access Table) 개요

Recipient Access Table은 퍼블릭 리스너에서 수락할 수신자를 정의합니다. 이 테이블에서는 최소한 주소 및 주소를 수락할지 또는 거부할지를 지정합니다.

RAT(Recipient Access Table) 페이지에는 RAT에 있는 항목의 목록과 함께 순서, 기본 작업, 그리고 LDAP 수락 쿼리를 우회하도록 항목이 구성되었는지 여부 등이 표시됩니다.

GUI를 사용하여 RAT에 액세스

GUI

Mail Policies(메일 정책**)** > **Recipient Access Table(RAT)**로 이동합니다.

CLI를 사용하여 RAT에 액세스

CLI

listenerconfig 명령을 edit > rcptaccess > new 하위 명령과 함께 사용합니다.

기본 RAT 항목 수정

시작하기 전에

- 퍼블릭 리스너를 설정합니다.
- 인터넷에 오픈 릴레이가 생성되지 않도록 신중하게 수정을 계획합니다. 오픈 릴레이("안전하지 않은 릴레이" 또는 "서드파티 릴레이"라고도 함)는 이메일 메시지의 서드파티 릴레이를 허용하는 SMTP 이메일 서버입니다. 오픈 릴레이는 로컬 사용자에 대한 메일도 아니고 로컬 사용자에게서 온 메일도 아닌 메일을 처리하여 악의적인 발신자가 게이트웨이를 통해 대량의 스팸을 라우팅할 수 있게 합니다. 기본적으로 RAT는 오픈 릴레이 생성을 막기 위해 모든 수신자를 거부합니다.
- RAT의 기본 항목은 삭제할 수 없습니다.

단계 **1** **Mail Policies(**메일 정책**) > Recipient Access Table(RAT)**로 이동합니다.
단계 **2** **All Other Recipients(**다른 모든 수신자**)**를 클릭합니다.

도메인 및 사용자

RAT를 사용하여 메시지를 수락할 도메인 수정

Mail Policies(메일 정책) > Recipient Access Table (RAT) 페이지를 사용하여, 어플라이언스가 메시지를 수락할 로컬 도메인 및 특정 사용자를 구성합니다. 이 페이지에서 다음 작업을 수행할 수 있습니다.

- RAT의 항목을 추가, 삭제 및 수정.
- 항목의 순서 변경.
- RAT 항목을 텍스트 파일로 내보내기.
- RAT 항목을 텍스트 파일에서 가져오기. 텍스트 파일에서 가져오면 기존 항목을 덮어씀

관련 주제

- 메시지를 수락할 도메인 및 사용자 추가, 131 페이지
- Recipient Access Table에서 도메인 및 사용자의 순서 다시 조정, 134 페이지
- Recipient Access Table을 외부 파일로 내보내기, 134 페이지
- 외부 파일에서 Recipient Access Table 가져오기, 134 페이지

메시지를 수락할 도메인 및 사용자 추가

단계 **1** **Mail Policies(**메일 정책**) > Recipient Access Table (RAT)** 페이지로 이동합니다.
단계 **2** Overview for Listener(리스너 개요) 필드에서 수정할 리스너를 선택합니다.
단계 **3** **Add Recipient(**수신자 추가**)**를 클릭합니다.
단계 **4** 항목의 순서를 선택합니다.
단계 **5** 수신자 주소를 입력합니다.
단계 **6** 수신자를 수락할지 또는 거부할지를 선택합니다.
단계 **7** (선택 사항) 수신자에 대해 LDAP 수락 쿼리를 우회하도록 선택합니다.
단계 **8** (선택 사항) 이 항목에 대한 사용자 지정 SMTP 응답을 사용합니다.
a) Custom SMTP Response(사용자 지정 SMTP 응답)에 대해 Yes(예)를 선택합니다.
b) SMTP 응답 코드 및 텍스트를 입력합니다. 수신자에 대한 RCPT TO 명령에 SMTP 응답을 포함합니다.
단계 **9** (선택 사항) Bypass Receiving Control(수신 제어 우회)에 대해 Yes(예)를 선택하여 조절을 우회하도록 선택합니다.
단계 **10** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- 수신자 주소 정의, 132 페이지
- 특정 수신자에 대해 LDAP 수락 우회, 132 페이지
- 특별한 수신인에 대한 수신 제한 Bypass, 133 페이지

수신자 주소 정의

RAT에서는 수신자 또는 수신자 그룹을 정의할 수 있습니다. 수신자는 전체 이메일 주소, 도메인, 부분 도메인, 사용자 이름 또는 IP 주소로 정의할 수 있습니다.

[IPv4 address]	호스트의 특정 IPv4(Internet Protocol version 4) 주소. IP 주소는 "[]" 문자 사이에 있어야 합니다.
[IPv6 address]	호스트의 특정 IPv6(Internet Protocol version 6) 주소. IP 주소는 "[]" 문자 사이에 있어야 합니다.
`division.example.com`	인증된 도메인 이름
`.partialhost`	"partialhost" 도메인 내 모든 것
`user@domain`	완전한 이메일 주소
`user@`	지정된 사용자 이름과 관련된 것
user@[*IP_address*]	특정 IPv4 또는 IPv6 주소의 사용자 이름. IP 주소는 "[]" 문자 사이에 있어야 합니다. "`user@`*IP_address*"(대괄호 문자 없음)는 유효한 주소가 아닙니다. 시스템은 메시지를 수신하면 유효한 주소를 만들기 위해 대괄호를 첨부하는데, 이는 수신자가 RAT에서 일치하는지 여부에 영향을 줄 수 있습니다.

참고 GUI의 시스템 설정 마법사 4단계에서 Recipient Access Table에 도메인을 추가할 때(3단계: 네트워크, 33 페이지 참조) 두 번째 항목을 추가하여 하위 도메인을 지정하는 것을 고려해볼 수 있습니다. 예를 들어 도메인 `example.net`을 입력하는 경우 `.example.net`도 입력할 수 있습니다. 두 번째 항목은 `example.net`의 하위 도메인으로 전송될 메일이 Recipient Access Table에서 일치하도록 보장해줍니다. RAT에서 `.example.com`만 지정하면 `.example.com`의 모든 하위 도메인은 수락되지만, 하위 도메인이 없는 전체 이메일 주소 수신자(예: joe@example.com)의 메일은 수락되지 않습니다.

특정 수신자에 대해 **LDAP** 수락 우회

LDAP 수락 쿼리를 구성하는 경우 특정 수신자에 대한 수락 쿼리를 우회할 수 있습니다. 이 기능은 LDAP 쿼리 중 지연시키거나 대기열에 추가하지 않을 이메일을 수신하는 수신자에게 유용할 수 있습니다(예: `customercare@example.com`).

LDAP 수락 쿼리 전에 작업 대기열에 재작성되도록 수신자 주소를 구성하는 경우(예: 별칭 사용 또는 도메인 맵 사용), 재작성된 주소는 LDAP 수락 쿼리를 우회하지 않습니다. 예를 들면 `customercare@example.com`을 `bob@example.com` 및 `sue@example.com`에 매핑하는 별칭 테이블을 사용하는 경우입니다. `customercare@example.com`에 대한 LDAP 수락을 우회하도록 구성하는 경우, 별칭 사용이 발생한 후 LDAP 수락 쿼리가 여전히 `bob@example.com` 및 `sue@example.com` 모두에 대해 실행됩니다.

GUI를 통해 LDAP 수락을 우회하도록 구성하려면 RAT 항목을 추가 또는 수정할 때 **Bypass LDAP Accept Queries for this Recipient(**이 수신자에 대해 **LDAP** 수락 쿼리 우회**)**를 선택합니다.

CLI를 통해 LDAP 수락을 우회하도록 구성하려면 `listenerconfig -> edit -> rcptaccess` 명령을 사용하여 수신자를 입력할 때 다음 질문에 대해 yes(예)로 대답합니다.

```
Would you like to bypass LDAP ACCEPT for this entry? [Y]> y
```

LDAP 수락을 우회하도록 RAT 항목을 구성할 때에는 RAT 항목의 순서가 수신자 주소의 일치 방법에 영향을 미친다는 점에 유의해야 합니다. RAT에서는 수신자 주소를 자격이 있는 첫 번째 RAT 항목과 비교합니다. 예를 들어 RAT 항목 postmaster@ironport.com 및 ironport.com이 있다고 가정해보겠습니다. postmaster@ironport.com에 대한 항목이 LDAP 수락 쿼리를 우회하도록 구성하고, ironport.com에 대한 항목을 ACCEPT로 구성합니다. postmaster@ironport.com에 대한 메일을 수신하면 postmaster@ironport.com에 대한 항목이 ironport.com에 대한 항목 앞에 있는 경우에만 LDAP 수락 우회가 발생합니다. ironport.com에 대한 항목이 postmaster@ironport.com 항목 앞에 있으면 RAT는 수신자 주소를 이 항목과 맞춰보고 ACCEPT 작업을 적용합니다.

특별한 수신인에 대한 수신 제한 **Bypass**

수신자 항목에 대해, 수신자가 리스너에서 활성화된 조절 제어 메커니즘을 우회하도록 지정할 수 있습니다.

이 기능은 메시지를 제한하지 않으려는 특정 수신인이 있는 경우 유용합니다. 예를 들면 메일 플로우 정책에 정의된 수신 제어를 기반으로 전송 도메인이 조절되고 있는 경우에도, 많은 사용자가 리스너에서 "`postmaster@domain`" 주소에 대한 메일을 수신하고자 합니다. 리스너의 RAT에서 수신 제어를 우회하도록 이 수신자를 지정하면, 리스너는 동일한 도메인의 다른 수신자에 대해서는 메일 플로우 정책을 유지한 채 수신자 "`postmaster@domain`"에 대한 메시지는 무제한 수신할 수 있습니다. 전송 도메인이 제한되어 있는 경우 시스템에서 유지 관리하는 시간당 수신자 카운터에 대해 수신자가 계산되지 않습니다.

GUI를 통해 특정 수신자가 수신 제어를 우회하도록 지정하려면 RAT 항목을 추가 또는 수정할 때 "Bypass Receiving Control(수신 제어 우회)" 설정에 대해 Yes(예)를 선택합니다.

CLI를 통해 특정 수신자가 수신 제어를 우회하도록 지정하려면 `listenerconfig > edit > rcptaccess` 명령을 사용하여 수신자를 입력할 때 다음 질문에 대해 yes로 대답합니다.

```
Would you like to bypass receiving control for this entry?  [N]> y
```

Recipient Access Table에서 도메인 및 사용자의 순서 다시 조정

단계 **1** **Mail Policies(**메일 정책**) > Recipient Access Table (RAT)** 페이지로 이동합니다.
단계 **2** **Overview for Listener(**리스너 개요**)** 필드에서 수정할 리스너를 선택합니다.
단계 **3** **Edit Order(**순서 수정**)**를 클릭합니다.
단계 **4** **Order(**순서**)** 열의 값을 조정하여 순서를 변경합니다.
단계 **5** 변경 사항을 제출 및 커밋합니다.

Recipient Access Table을 외부 파일로 내보내기

단계 **1** **Mail Policies(**메일 정책**) > Recipient Access Table (RAT)** 페이지로 이동합니다.
단계 **2** **Overview for Listener(**리스너 개요**)** 필드에서 수정할 리스너를 선택합니다.
단계 **3** **Export RAT(RAT** 내보내기**)**를 클릭합니다.
단계 **4** 내보낸 항목에 대한 파일 이름을 입력합니다.

이것은 어플라이언스의 컨피그레이션 디렉터리에 생성될 파일의 이름입니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

외부 파일에서 **Recipient Access Table** 가져오기

텍스트 파일에서 Recipient Access Table 항목을 가져오면 기존의 모든 항목이 Recipient Access Table에서 제거됩니다.

단계 **1** **Mail Policies(**메일 정책**) > Recipient Access Table (RAT)** 페이지로 이동합니다.
단계 **2** **Overview for Listener(**리스너 개요**)** 필드에서 수정할 리스너를 선택합니다.
단계 **3** **Import RAT(RAT** 가져오기**)**를 클릭합니다.
단계 **4** 목록에서 파일을 선택합니다.

AsyncOS가 어플라이언스의 컨피그레이션 디렉토리에 모든 텍스트 파일을 나열합니다.

단계 **5** **Submit(**제출**)**를 클릭합니다.

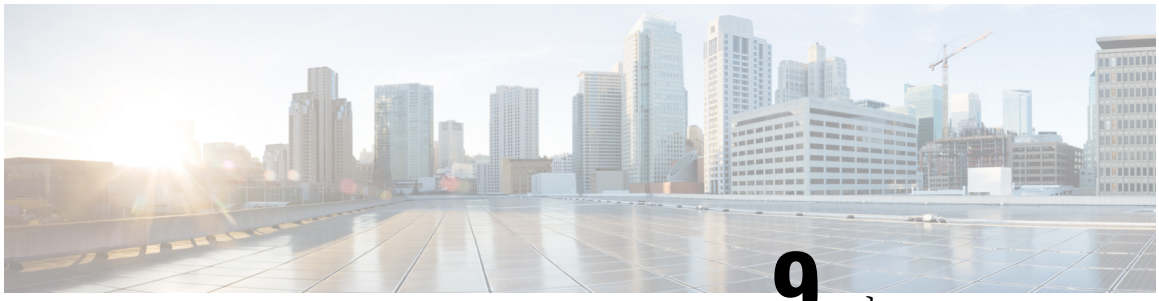
기존의 모든 Recipient Access Table 항목을 제거할 것인지를 묻는 경고 메시지가 표시됩니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.
단계 **7** 변경 사항을 커밋합니다.

파일에 "코멘트"를 추가할 수 있습니다. '#' 문자로 시작되는 줄은 코멘트로 간주되어 AsyncOS에서 무시됩니다. 예를 들면 다음과 같습니다.

예제:

```
# File exported by the GUI at 20060530T220526
.example.com  ACCEPT
ALL  REJECT
```



9 장

메시지 필터를 사용하여 이메일 정책 적용

Cisco 어플라이언스는 회사 정책을 적용하고 회사 네트워크에 특정 메시지가 들어오거나 나갈 때 이 메시지를 대상으로 작업을 수행할 수 있도록 콘텐츠 검사 및 메시지 필터링 기술을 폭넓게 제공합니다.

이 장에는 콘텐츠 검사 엔진, 메시지 필터, 첨부 파일 필터 및 콘텐츠 사전 등 정책 적용을 위해 함께 사용 가능한 강력한 기능에 대한 정보에 관해 설명합니다.

이 장에는 다음 섹션이 포함되어 있습니다.

개요

메시지 필터를 통해 Cisco 어플라이언스에서 메시지를 수신할 때 메시지를 처리하는 방법이 포함된 특수한 규칙을 생성할 수 있습니다. 메시지 필터는 특정 유형의 메시지가 처리되는 방식을 지정합니다. Cisco 메시지 필터를 사용하면 지정하는 단어를 대상으로 메시지 콘텐츠를 검사하여 회사 이메일 정책을 적용할 수 있습니다. 이 장에는 다음 섹션이 포함되어 있습니다.

- 메시지 필터의 구성 요소. 메시지 필터를 통해 메시지를 수신할 때 메시지를 처리하는 방법이 포함된 특수한 규칙을 생성할 수 있습니다. 필터 규칙은 메시지나 첨부 파일 내용, 네트워크에 대한 정보, 메시지 봉투, 메시지 헤더, 메시지 본문 등을 기반으로 메시지를 식별합니다. 필터 작업을 통해 알림을 생성하거나 메시지를 삭제, 바운스, 아카이브, BCC(숨은 참조) 또는 변경할 수 있습니다. 자세한 내용은 메시지 필터의 구성 요소, 138 페이지를 참고하십시오.

- 메시지 필터 처리. AsyncOS에서 메시지 필터를 처리하는 경우 AsyncOS가 검사하는 콘텐츠, 처리 순서 및 수행하는 작업은 메시지 필터 순서, 메시지 콘텐츠를 변경한 이전 처리, 메시지의 MIME 구조, 콘텐츠 일치를 위해 구성된 임계값 점수 및 쿼리 구조 등 여러 가지 요소를 기반으로 수행됩니다. 자세한 내용은 메시지 필터 처리, 140 페이지를 참고하십시오.
- 메시지 필터 규칙. 각 필터에는 필터가 동작하는 대상인 메시지 모음을 정의하는 규칙이 있습니다. 이러한 규칙은 메시지 필터를 생성할 때 정의합니다. 자세한 내용은 메시지 필터 규칙, 138 페이지를 참고하십시오.
- 메시지 필터 작업. 각 필터에는 규칙이 true로 평가된 경우 메시지에 수행하는 작업이 있습니다. 수행할 수 있는 작업에는 2가지 유형이 있습니다. 첫 번째는 최종 작업(예: 메시지 전달, 삭제 또는 바운스)이며 두 번째는 메시지를 더 처리할 수 있도록 허용하는 최종 작업 이외의 작업(예: 헤더 제거 또는 삽입)입니다. 자세한 내용은 메시지 필터 작업, 138 페이지를 참고하십시오.
- 첨부 파일 검사의 메시지 필터. 첨부 파일 검사의 메시지 필터를 통해 메시지에서 회사 정책과 일치하지 않는 첨부 파일은 제거하면서 원본 메시지를 전달할 수 있습니다. 해당하는 특정 파일 유형, 지문 또는 콘텐츠에 따라 첨부 파일을 필터링할 수 있습니다. 또한 이미지 분석기를 사용하여 이미지 첨부 파일을 검사할 수 있습니다. 이미지 분석기는 그래픽에 부적절한 콘텐츠가 포함될 확률을 판단하기 위해 스킨 색상, 본문 크기 및 곡률을 측정하는 알고리즘을 생성합니다. 자세한 내용은 Attachment Scanning(첨부 파일 검사), 229 페이지를 참고하십시오.
- **CLI**를 사용하여 메시지 필터 관리. CLI는 메시지 필터 작업을 위해 명령을 수락합니다. 예를 들어, 메시지 필터 목록의 표시, 재정렬, 가져오기 또는 내보내기를 수행할 수 있습니다. 자세한 내용은 CLI를 사용하여 메시지 필터 관리, 240 페이지를 참고하십시오.
- 메시지 필터 예. 이 섹션에는 각 필터에 대한 간단한 설명과 함께 필터의 몇 가지 실제 예가 포함되어 있습니다. 자세한 내용은 메시지 필터 예, 255 페이지를 참고하십시오.

메시지 필터의 구성 요소

메시지 필터를 통해 메시지를 수신할 때 메시지를 처리하는 방법이 포함된 특수한 규칙을 생성할 수 있습니다. 메시지 필터는 메시지 필터 규칙과 메시지 필터 작업으로 구성됩니다.

관련 주제

- 메시지 필터 규칙, 138 페이지
- 메시지 필터 작업, 138 페이지
- 메시지 필터 예제 구문, 139 페이지

메시지 필터 규칙

메시지 필터 규칙은 필터를 적용할 메시지를 결정합니다. 규칙은 논리 커넥터인 AND, OR 및 NOT을 사용하여 더 복잡한 테스트를 생성할 수 있습니다. 규칙 표현식은 괄호를 통해 그룹화될 수 있습니다.

메시지 필터 작업

메시지 필터의 목적은 선택한 메시지에 작업을 수행하는 것입니다.

작업에는 다음의 2가지 유형이 있습니다.

- 최종 작업(전달, 삭제 및 바운스)은 메시지 처리를 종료하고 다음 필터를 통한 추가 처리를 허용하지 않습니다.
- 최종 작업 이외의 작업은 메시지가 추가 처리되도록 허용합니다.

참고 최종 작업 이외의 메시지 필터 작업은 누적됩니다. 필터마다 다른 작업을 지정하는 여러 필터와 메시지가 일치하는 경우 모든 작업이 누적되어 적용됩니다. 그러나 동일한 작업을 지정하는 여러 필터와 메시지가 일치하는 경우, 이전 작업이 재정의되고 최종 필터 작업이 적용됩니다.

관련 주제

- 필터 작업 요약 표, 196 페이지
- 작업 변수, 206 페이지
- 일치 콘텐츠 가시성, 208 페이지
- 메시지 필터 작업의 설명 및 예, 209 페이지

메시지 필터 예제 구문

필터의 직관적인 의미는 다음과 같습니다.

만약 메시지가 규칙과 일치하면 작업을 순차적으로 적용합니다. else 절이 있는 경우 else 절에 포함된 작업은 메시지가 규칙과 일치하지 않는 경우 실행됩니다.

필터 이름을 지정하면 필터를 활성화, 비활성화 또는 삭제할 때 필터를 쉽게 관리할 수 있습니다.

메시지 필터는 다음 구문을 사용합니다.

예제 구문	목적
expedite:	필터 이름
if (recv-listener == 'InboundMail' or recv-int == 'notmain')	규칙 사양
`{ alt-src-host('outbound1'); skip-filters(); }`	작업 사양
`else { alt-src-host('outbound2'); }`	선택적 대체 작업 사양

대체 작업은 모두 생략할 수 있습니다.

예제 구문	목적
expedite2:	필터 이름

예제 구문	목적
`if ((not (recv-listener == 'InboundMail')) and` (not (recv-int == 'notmain')))	규칙 사양

`{`
`alt-src-host('outbound2');`
`skip-filters();`
}
	작업 사양

단일 텍스트 파일에 나와 있는 순서대로 하나 다음에 하나씩 여러 필터를 결합할 수 있습니다.

작은따옴표 또는 큰따옴표 중 하나로 필터의 값을 묶어야 합니다. 작은따옴표 또는 큰따옴표는 값의 양쪽에 동일하게 짝을 지어야 합니다. 예를 들어, `notify('customercare@example.com')` 및 `notify("customercare@example.com")`은 모두 올바르지만 표현식 `notify("customercare@example.com')`은 구문 오류를 발생시킵니다.

'#' 문자로 시작되는 행은 주석으로 간주되어 무시되지만 `filters -> detail`을 통해 필터를 확인하여 검증할 수 있기 때문에 AsyncOS에서 유지되지 않습니다.

메시지 필터 처리

AsyncOS에서 메시지 필터를 처리하는 경우 AsyncOS가 검사하는 콘텐츠, 처리 순서 및 수행하는 작업은 다음의 여러 요소를 기반으로 수행됩니다.

- 메시지 필터 순서**.** 메시지 필터는 순서가 지정된 목록으로 유지 관리됩니다. 메시지가 처리될 때, AsyncOS는 메시지가 목록에 나타나는 순서대로 각 메시지 필터를 적용합니다. 최종 작업이 발생하는 경우, 메시지에 추가 작업이 수행되지 않습니다. 자세한 내용은 메시지 필터 순서, 141 페이지를 참고하십시오.
- 이전 처리. AsyncOS 메시지에서 수행했던 작업에서 메시지 필터를 평가하기 전에 헤더를 추가하거나 제거할 수 있습니다. AsyncOS는 처리 시 메시지에 있는 헤더에서 메시지 필터 프로세스를 처리합니다. 자세한 내용은 메시지 헤더 규칙 및 평가, 141 페이지를 참고하십시오.
- 메시지의 **MIME** 구조. 메시지의 MIME 구조에 따라 메시지의 어떤 부분을 "본문" 또는 "첨부 파일"로 처리할지 결정됩니다. 메시지 본문에만 또는 메시지의 첨부 파일에만 작업을 수행하도록 여러 메시지 필터가 구성됩니다. 자세한 내용은 메시지 본문과 메시지 첨부 파일 비교, 141 페이지를 참고하십시오.
- 정규식을 위해 구성된 임계값 점수. 정규식과 일치하는 경우 필터 작업을 수행하기 전에 반드시 일치해야 하는 횟수를 계산하는 "점수"를 구성합니다. 점수를 사용하면 다른 용어에 대한 응답에 "가중치"를 사용할 수 있습니다. 자세한 내용은 콘텐츠 검사 시 일치를 위한 임계값, 142 페이지 장을 참조해 주십시오.
- 쿼리 구조. 메시지 필터 내에서 AND 또는 OR 테스트를 평가할 때 AsyncOS는 불필요한 테스트는 평가하지 않습니다. 또한 시스템은 왼쪽에서 오른쪽으로 테스트를 평가하지 않습니다. 대신, AND 또는 OR 테스트를 평가할 때 가장 비용이 적게 드는 테스트가 먼저 평가됩니다. 자세한 내용은 메시지 필터에서 AND 테스트 및 OR 테스트, 145 페이지를 참고하십시오.

관련 주제

- 메시지 필터 순서, 141 페이지
- 메시지 헤더 규칙 및 평가, 141 페이지
- 메시지 본문과 메시지 첨부 파일 비교, 141 페이지
- 콘텐츠 검사 시 일치를 위한 임계값, 142 페이지
- 메시지 필터에서 AND 테스트 및 OR 테스트, 145 페이지

메시지 필터 순서

메시지 필터는 순서가 지정된 목록으로 유지되고 목록에서의 위치에 따라 번호가 매겨집니다. 메시지가 처리될 때 메시지 필터는 연결된 숫자의 순서대로 적용됩니다. 따라서 필터 9번이 이미 메시지에서 마지막 작업을 실행한 경우(예: 바운스됨) 필터 30번은 메시지의 소스 호스트를 변경할 수 없습니다. 목록의 필터 위치는 시스템 사용자 인터페이스를 통해 변경할 수 있습니다. 파일을 통해 가져온 필터는 가져온 파일의 상대적인 순서를 기준으로 정렬됩니다.

최종 작업 이후에는 메시지에 추가 작업이 수행되지 않습니다.

메시지가 필터 규칙과 일치하는 경우에도 필터는 다음 이유로 인해 해당 메시지에 적용되지 않을 수 있습니다.

- 필터가 비활성화된 상태입니다.
- 필터가 유효하지 않습니다.
- 필터가 메시지에 최종 작업을 수행한 이전 필터로 대체되었습니다.

메시지 헤더 규칙 및 평가

필터는 헤더 규칙을 적용할 때 원본 메시지 헤더 대신 "처리된" 헤더를 평가합니다. 그 결과는 다음과 같습니다.

- 헤더가 이전 처리 작업을 통해 추가된 경우, 헤더가 현재 모든 후속 헤더 규칙과 일치할 수 있습니다.
- 헤더가 이전 처리 작업을 통해 제거된 경우, 헤더가 더이상 모든 후속 헤더 규칙과 일치하지 않을 수 있습니다.
- 헤더가 이전 처리 작업을 통해 수정된 경우, 모든 후속 헤더 규칙은 수정된 헤더는 평가하지만 원본 메시지 헤더는 평가하지 않습니다.

이러한 동작은 메시지 필터와 콘텐츠 필터에서 일반적입니다.

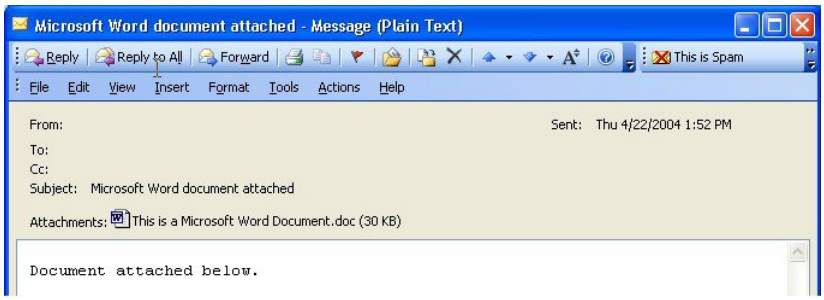
메시지 본문과 메시지 첨부 파일 비교

이메일 메시지는 여러 부분으로 구성됩니다. RFC에서는 메시지 헤더 이후에 오는 모든 요소를 여러 부분으로 구성된 "메시지 본문"으로 정의하지만, 많은 사용자는 메시지의 "본문"과 "첨부 파일"을 다르게 개념화합니다. Cisco 메시지 필터(*body*-`variable` 또는 *attachment*-variable 필터)를 사용하는 경우, Cisco 어플라이언스는 대부분의 사용자가 "본문" 및 "첨부 파일"로 간주하는 부분을 대부분의 MUA가 이와는 다르게 렌더링하는 것과 동일한 방식으로 구분하려고 시도합니다.

body-variable 또는 `attachment`-*variable* 메시지 필터 규칙을 작성하기 위해 메시지 헤더 이후에 오는 모든 요소는 메시지 본문으로 간주되며 이 본문의 콘텐츠는 본문 내에 포함된 MIME 부분의 첫 번째 텍스트로 간주됩니다. 콘텐츠 다음의 모든 요소(즉, 모든 추가 MIME 부분)는 첨부 파일로 간주됩니다. AsyncOS는 메시지의 다양한 MIME 부분을 평가하고 첨부 파일로 처리되는 파일 부분을 식별합니다.

예를 들어, 다음 그림은 "`Document attached below.`"라는 문장이 일반 텍스트 메시지의 본문이고 "`This is a Microsoft Word document.doc`"이라는 문서가 첨부 파일인 Microsoft Outlook MUA를 보여 줍니다. 많은 사용자가 멀티파트 메시지의 첫 번째 부분은 일반 텍스트이고 두 번째 부분은 이진 파일이라는 개념보다는 이런 방식의 이메일 개념을 가지고 있으므로, 비록 RFCS 1521 및 1522에 사용되는 개념에서는 메시지의 본문이 모두 MIME 부분으로 구성되어 있지만, Cisco에서는 메시지 필터에 "첨부 파일"이란 용어를 사용하여, 메시지의 "본문"(첫 번째 일반 텍스트 부분)과 달리 .doc 파일 부분(본질적으로 두 번째 MIME 부분)을 차별화하고 처리할 규칙을 생성합니다.

그림 ***16: "첨부 파일"이 있는 메시지***



Cisco 어플라이언스가 여러 부분으로 구성되는 메시지에서 본문과 첨부 파일을 구분하기 때문에 예상되는 동작을 수행하기 위해 body-*variable* 또는 `attachment`-*variable* 메시지 필터 규칙을 사용할 때 다음과 같은 여러 가지 사례에 대해 알고 있어야 합니다.

- 단일 텍스트가 있는 메시지 즉, "Content-Type: text/plain" 또는 "Content-Type: text/html" 헤더를 포함하는 메시지가 있는 경우 Cisco 어플라이언스는 전체 메시지를 본문으로 간주합니다. 콘텐츠 유형이 다른 경우 Cisco 어플라이언스는 이것을 단일 첨부 파일로 간주합니다.
- 일부 인코딩된 파일(예: UU 인코딩 파일)은 이메일 메시지의 본문에 포함되어 있습니다. 이 경우, 인코딩된 파일은 첨부 파일로 간주되어 추출 및 검사되고 나머지 텍스트는 텍스트의 본문으로 간주됩니다.
- 텍스트가 아닌 단일 파일은 항상 첨부 파일로 간주됩니다. 예를 들어, .zip 파일로만 구성된 메시지는 첨부 파일로 간주됩니다.

콘텐츠 검사 시 일치를 위한 임계값

메시지 본문 또는 첨부 파일에서 패턴을 검색하는 필터 규칙을 추가하는 경우 패턴 발견 횟수에 대한 최소 임계값을 지정할 수 있습니다. AsyncOS는 메시지를 검사할 때 메시지 및 첨부 파일에서 찾은 일치 횟수의 "점수"를 합산합니다. 최소 임계값이 충족되지 않으면 정규식이 true로 평가되지 않습니다. 다음 필터 규칙에 대해 이 임계값을 지정할 수 있습니다.

- body-contains
- only-body-contains

- attachment-contains
- every-attachment-contains
- dictionary-match
- attachment-dictionary-match

또한 `drop-attachments-where-contains` 작업에 대해 임계값을 지정할 수 있습니다.

참고 헤더 또는 봉투 수신자 및 발신자를 검사하는 필터 규칙에 대해서는 임계값을 지정할 수 없습니다.

관련 주제

- 임계값 구문, 143 페이지
- 메시지 본문 및 첨부 파일에 대한 임계값 점수, 143 페이지
- 여러 부분으로 구성된 MIME/대체 MIME에 대한 임계값 점수, 144 페이지
- 콘텐츠 사전에 대한 임계값 점수, 144 페이지

임계값 구문

최소 발견 횟수에 대한 임계값을 지정하려면 true로 평가되는 데 필요한 패턴과 최소 일치 횟수를 다음과 같이 지정합니다.

```
if(<filter rule>('<pattern>',<minimum threshold>)){
```

예를 들어, body-contains 필터 규칙에서 "Company Confidential" 값을 최소 2번 이상 찾도록 지정하려면 다음 구문을 사용합니다.

```
if(body-contains('Company Confidential',2)){
```

기본적으로, AsyncOS는 콘텐츠 검사 필터를 저장할 때, 값을 지정되지 않은 경우 필터를 컴파일하고 임계값을 1로 지정합니다.

또한 콘텐츠 사전의 값에 대해 최소 패턴 일치 횟수를 지정할 수 있습니다. 콘텐츠 사전에 대한 자세한 정보는 "텍스트 리소스" 장을 참조하십시오.

메시지 본문 및 첨부 파일에 대한 임계값 점수

이메일 메시지는 여러 부분으로 구성될 수 있습니다. 메시지 본문 또는 첨부 파일에서 패턴을 검색하는 필터 규칙에 임계값을 지정할 때 AsyncOS는 임계값 "점수"를 확인하기 위해 메시지 부분 및 첨부 파일에서의 일치 횟수를 계산합니다. 메시지 필터에 특정 MIME 부분(예: `attachment-contains` 필터 규칙)이 지정되지 않는 경우 AsyncOS는 메시지의 모든 부분에서 찾은 일치 항목의 총계를 계산하여 일치 항목 개수가 임계값을 만족하는지 확인합니다. 예를 들어, 임계값이 2인 `body-contains` 메시지 필터가 있는 경우, 본문과 첨부 파일에 일치 항목이 각각 1개씩 포함된 메시지를 수신합니다. AsyncOS는 이 메시지의 점수를 매길 때, 일치 항목이 총 2개이며 임계 점수를 만족하는지 확인합니다.

이와 마찬가지로 첨부 파일이 여러 개 있는 경우 AsyncOS는 일치 항목의 점수를 확인하기 위해 각 첨부 파일에 대한 총 점수를 계산합니다. 예를 들어, 임계값이 3인 `attachment-contains` 필터 규칙이 있

는 경우, 각 첨부 파일에 일치 항목 2개가 포함된 첨부 파일 2개가 있는 메시지를 수신합니다. AsyncOS는 일치 항목 4개가 있는 메시지의 점수를 매기고 임계 점수를 만족하는지 확인합니다.

여러 부분으로 구성된 **MIME/**대체 **MIME**에 대한 임계값 점수

동일한 콘텐츠에 2가지 표현이 있는 경우(일반 텍스트 및 HTML) 중복 계산을 방지하기 위해 AsyncOS는 중복 부분에서는 일치 횟수를 계산하지 않습니다. 대신, 각 부분에 있는 일치 항목을 비교하고 가장 높은 값을 선택합니다. 그런 다음 AsyncOS는 총 점수를 생성하기 위해 이 값을 여러 부분으로 구성된 메시지의 다른 부분에서 가져온 점수에 추가합니다.

예를 들어, `body-contains` 필터 규칙을 구성하고 임계값을 4로 구성합니다. 그리고 일반 텍스트와 HTML, 첨부 파일 2개가 있는 메시지를 수신합니다. 메시지는 다음 구조를 사용합니다.

```
multipart/mixed

        multipart/alternative

                text/plain

                text/html

        application/octet-stream

        application/octet-stream
```

`body-contains` 필터 규칙은 먼저 메시지의 text/plain 및 text/html 부분의 점수를 매겨 이 메시지의 점수를 결정합니다. 그런 다음 이 점수의 결과를 비교하고 결과에서 가장 높은 점수를 선택합니다. 다음으로, 이 결과를 각 첨부 파일의 점수에 추가하여 최종 점수를 결정합니다. 메시지에 다음의 일치가 발생하는 경우,

```
multipart/mixed

        multipart/alternative

                text/plain (2 matches)

                text/html (2 matches)

        application/octet-stream (1 match)

        application/octet-stream
```

AsyncOS는 text/plain 및 text/html 부분의 일치 항목을 비교하기 때문에 3점을 반환하며 이는 필터 규칙이 트리거되기 위한 최소 임계값을 만족하지 않습니다.

콘텐츠 사전에 대한 임계값 점수

콘텐츠 사전을 사용할 때 특정 용어가 필터 작업을 보다 쉽게 트리거하도록 용어에 "가중치"를 적용할 수 있습니다. 예를 들어, "은행"이라는 용어에 대해 메시지 필터를 트리거하지 않을 수 있습니다.

그러나 이 "은행"이라는 용어가 "계정"이라는 용어와 결합되고 ABA 은행 식별 번호와 사용되는 경우 필터 작업을 트리거할 수 있습니다. 작업을 완료하기 위해 가중치가 적용된 사전을 사용하여 특정 용어 또는 결합된 용어의 중요도를 높일 수 있습니다. 콘텐츠 사전을 사용하는 메시지 필터는 필터 규칙에 대한 일치 항목의 점수를 매길 때 이러한 가중치를 사용하여 최종 점수를 결정합니다. 예를 들어 다음 콘텐츠 및 가중치가 있는 콘텐츠 사전을 생성하는 경우,

표 ***19:*** 샘플 콘텐츠 사전

용어/스마트 식별자	가중치
ABA 은행 식별 번호	3
계정	2
은행	1

이 콘텐츠 사전을 `dictionary-match` 또는 `attachment-dictionary-match` 메시지 필터 규칙과 연결할 때 AsyncOS는 해당 용어의 가중치를 메시지에서 찾은 일치 용어에 대한 각 인스턴스의 총 "점수"에 추가합니다. 예를 들어 메시지에 메시지 본문의 "계정"이라는 용어의 인스턴스 3개가 포함된 경우, AsyncOS는 총 점수에 6점을 추가합니다. 메시지 필터의 임계값을 6으로 설정하면 AsyncOS는 임계 점수를 만족하는지 여부를 확인합니다. 또는 메시지에 각 용어의 인스턴스 1개가 포함된 경우, 총계가 6이 되며 이로써 필터 작업이 트리거됩니다.

메시지 필터에서 **AND** 테스트 및 **OR** 테스트

메시지 필터 내에서 AND 또는 OR 테스트를 평가할 때 AsyncOS는 불필요한 테스트는 평가하지 않습니다. 따라서 예를 들어 AND 테스트의 한 부분이 false이면 시스템은 다른 부분을 평가하지 않습니다. 시스템은 왼쪽에서 오른쪽으로 테스트를 평가하지 않습니다. 대신, AND 또는 OR 테스트를 평가할 때 가장 비용이 적게 드는 테스트가 먼저 평가됩니다. 예를 들어, 다음 필터에서 `remote-ip` 테스트는 `rcpt-to-group` 테스트보다 비용이 적게 들기 때문에 항상 먼저 처리됩니다(일반적으로 LDAP 테스트는 더 많은 비용 소요).

```
andTestFilter:

if (remote-ip == "192.168.100.100" AND rcpt-to-group == "GROUP")

  { ... }
```

가장 비용이 낮은 테스트가 먼저 수행되므로 테스트에서 항목의 순서를 변경해도 소용이 없습니다. 테스트가 순서대로 수행되도록 보장하려면 중첩된 if 문을 사용합니다. 이는 또한 비용이 높은 테스트를 가능한 한 피하기 위한 최적의 방법입니다.

```
expensiveAvoid:

if (<simple tests>)

  { if (<expensive test>)
```

```
    { <action> }

  }
```

다소 복잡한 예에서는 다음을 고려합니다.

```
if (test1 AND test2 AND test3) { ... }
```

시스템에서는 식을 왼쪽에서 오른쪽으로 그룹화하므로 다음과 같이 됩니다.

```
if ((test1 AND test2) AND test3) { ... }
```

즉, 시스템은 우선 (`test1` AND `test2`)의 비용을 `test3`의 비용과 비교하여 두 번째 AND를 먼저 평가하게 됩니다. 세 가지 테스트의 비용이 모두 동일하다면 (`test1` AND `test2`)의 비용이 두 배이므로 `test3`이 먼저 수행됩니다.

메시지 필터 규칙

각 메시지 필터에는 필터가 작동할 수 있는 메시지 컬렉션을 정의하는 규칙이 포함되어 있습니다. 필터 규칙을 정의한 다음 true를 반환하는 메시지에 대한 필터 작업을 정의합니다.

관련 주제

- 필터 규칙 요약 표, 146 페이지
- 규칙의 정규식, 158 페이지
- 스마트 식별자, 162 페이지
- 메시지 필터 작업의 설명 및 예, 209 페이지

필터 규칙 요약 표

다음 표에는 메시지 필터에 사용할 수 있는 규칙이 요약되어 있습니다.

표 ***20:*** 메시지 필터 규칙

규칙	**Syntax**	설명
Subject Header(제목 헤더)	`subject`	제목 헤더가 특정 패턴과 일치합니까? Subject(제목) 규칙, 165 페이지를 참조하십시오.
Body Size(본문 크기)	`body-size`	본문 크기가 일정한 범위 내에 있습니까? Body Size(본문 크기) 규칙, 168 페이지를 참조하십시오.

규칙	**Syntax**	설명
Envelope Sender(봉투 발신자)	`mail-from`	Envelope Sender(봉투 발신자)(즉, Envelope From, <MAIL FROM>)가 지정된 패턴과 일치합니까? Envelope Sender(봉투 발신자) 규칙, 167 페이지의 내용을 참조하십시오.
Envelope Sender in Group(그룹의 봉투 발신자)	`mail-from-group`	Envelope Sender(봉투 발신자)(즉, Envelope From, <MAIL FROM>)가 지정된 LDAP 그룹에 있습니까? Envelope Sender in Group(그룹의 봉투 발신자) 규칙, 167 페이지의 내용을 참조하십시오.
발신자 그룹	`sendergroup`	리스너의 HAT(Host Access Table)에서 어떤 발신자 그룹이 일치했습니까? Sender Group(발신자 그룹) 규칙, 168 페이지를 참조하십시오.
Envelope Recipient(봉투 수신인)	`rcpt-to`	Envelope Recipient(봉투 수신자)(즉, Envelope To, <RCPT TO>)가 지정된 패턴과 일치합니까? Envelope Recipient(봉투 수신자) 규칙, 166 페이지의 내용을 참조하십시오. 참고 `rcpt-to` 규칙은 메시지 기반입니다. 메시지 수신자가 여러 명인 경우, 메시지가 모든 수신자에게 영향을 미치려면 한 수신자만 지정된 작업에 대한 규칙과 일치해야 합니다.

규칙	**Syntax**	설명
그룹의 봉투 수신자	`rcpt-to-group`	Envelope Recipient(봉투 수신자)(즉, Envelope To, <RCPT TO>)가 지정된 LDAP 그룹에 있습니까? Envelope Recipient in Group(그룹의 봉투 수신자) 규칙, 166 페이지의 내용을 참조하십시오. 참고 `rcpt-to-group` 규칙은 메시지 기반입니다. 메시지 수신자가 여러 명인 경우, 모든 수신자에 대한 메시지에 영향을 미치려면 지정된 작업에 대한 그룹에서 한 수신자만 발견되어야 합니다.
Remote IP(원격 IP)	`remote-ip`	메시지가 지정된 IP 주소나 IP 블록과 일치하는 원격 호스트에서 전송되었습니까? Remote IP(원격 IP) 규칙, 169 페이지를 참조하십시오.
Receiving Interface(수신 인터페이스)	`recv-int`	메시지가 명명된 수신 인터페이스를 통해 도착했습니까? 를 참조하십시오.Receiving IP Interface(수신 IP 인터페이스) 규칙, 170 페이지
Receiving Listener(수신 리스너)	`recv-listener`	메시지가 명명된 리스너를 통해 도착했습니까? Receiving Listener(수신 리스너) 규칙, 169 페이지를 참조하십시오.
Date(날짜)	`date`	현재 시간이 지정된 시간 및 날짜의 이전입니까, 아니면 이후입니까? Date(날짜) 규칙, 170 페이지를 참조하십시오.
Header(헤더)	`header(<string>)`	메시지에 특정 헤더가 포함되어 있습니까? 그 헤더의 값이 특정 패턴과 일치합니까? Header(헤더) 규칙, 170 페이지를 참조하십시오.

규칙	**Syntax**	설명
Random(난수)	`random(<integer>)`	난수가 일정한 범위에 있습니까? Random(난수) 규칙, 171 페이지를 참조하십시오.
Recipient Count(수신자 수)	`rcpt-count`	이 이메일이 몇 명의 수신자에게 전송됩니까? Recipient Count(수신자 수) 규칙, 172 페이지를 참조하십시오.
Address Count(주소 수)	`addr-count()`	수신자의 누적 수는 얼마입니까? 이 필터는 봉투 수신자가 아니라 메시지 본문 헤더에 대해 작동된다는 점에서 rcpt-count 필터 규칙과 다릅니다. Address Count(주소 수) 규칙, 172 페이지를 참조하십시오.
SPF Status(SPF 상태)	`spf-status`	SPF 확인 상태는 무엇이었습니까? 이 필터 규칙을 사용하면 서로 다른 SPF 확인 결과를 쿼리할 수 있습니다. 각각의 유효한 SPF/SIDF 반환 값에 대해 서로 다른 작업을 입력할 수 있습니다. SPF-Status 규칙, 178 페이지를 참조하십시오.
SPF Passed(SPF 통과)	`spf-passed`	SPF/SIDF 확인을 통과했습니까? 이 필터 규칙은 SPF/SIDF 결과를 부울 값으로 생성합니다. SPF-Passed 규칙, 180 페이지를 참조하십시오.
S/MIME 게이트웨이 메시지	`smime-gateway`	메시지가 S/MIME 서명되거나, 인증되거나, 서명 및 인증되었습니까? S/MIME Gateway Message(S/MIME 게이트웨이 메시지) 규칙, 180 페이지 항목을 참조하십시오.

규칙	**Syntax**	설명
S/MIME 게이트웨이 확인됨	`smime-gateway-verified`	메시지가 성공적으로 확인되거나, 해독되거나, 해독 및 확인되었습니까? S/MIME Gateway Verified(S/MIME 게이트웨이 확인됨) 규칙, 181 페이지의 내용을 참조하십시오.
Image verdict(이미지 판정)	`image-verdict`	이미지 검사 판정이 무엇이었습니까? 이 필터 규칙을 사용하면 서로 다른 이미지 분석 판정에 대해 쿼리할 수 있습니다. 이미지 분석, 232 페이지를 참조하십시오.
Workqueue count(작업 대기열 수)	`workqueue-count`	작업 대기열 수가 지정된 값과 같습니까, 더 작습니까, 아니면 더 큽니까? Workqueue-count 규칙, 181 페이지를 참조하십시오.
Body Scanning(본문 검색)	`body-contains(<regular expression>)`	지정된 패턴과 일치하는 텍스트 또는 첨부 파일이 메시지에 포함되어 있습니까? 패턴이 임계값에 대해 지정한 최소 횟수만큼 발생합니까? 엔진은 delivery-status 부분 및 관련 첨부 파일을 검사합니다. Body Scanning(본문 검색), 173 페이지를 참조하십시오.
Body Scanning(본문 검색)	`only-body-contains (<regular expression>)`	지정된 패턴과 일치하는 텍스트가 메시지 본문에 포함되어 있습니까? 패턴이 임계값에 대해 지정한 최소 횟수만큼 발생합니까? 첨부 파일은 검사되지 않습니다. Body Scanning(본문 검사) 규칙, 172 페이지를 참조하십시오.
Encryption Detection(암호화 탐지)	`encrypted`	메시지가 암호화되었습니까? 암호화 탐지 규칙, 173 페이지를 참조하십시오.

규칙	**Syntax**	설명
첨부 파일 파일 이름	`attachment-filename`	메시지에 파일 이름이 특정 패턴과 일치하는 첨부 파일이 포함되어 있습니까? Attachment Filename(첨부 파일의 파일 이름) 규칙, 174 페이지를 참조하십시오.
Attachment Type(첨부 파일 형식)a	`attachment-type`	메시지에 특별한 MIME 유형의 첨부 파일이 포함되어 있습니까? Attachment Type(첨부 파일 형식) 규칙, 174 페이지를 참조하십시오.
Attachment File Type	`attachment-filetype`	메시지에 지문을 기반으로 특정 패턴과 일치하는 파일 형식의 첨부 파일이 포함되어 있습니까(UNIX `file` 명령과 유사)? 첨부 파일이 Excel 또는 Word 문서이면 .exe , .dll, .bmp, .tiff, .pcx, .gif, .jpeg, png 및 Photoshop 이미지 등의 내장된 파일 형식도 검색할 수 있습니다. 유효한 필터를 만들려면 파일 형식을 따옴표로 감싸야 합니다. 작은따옴표 또는 큰따옴표를 사용할 수 있습니다. 예를 들어 .exe 첨부 파일을 검색하려면 다음 구문을 사용합니다. `if (attachment-filetype == "exe")` 자세한 내용은 아카이브 파일 내 첨부 파일의 파일 이름 및 단일 압축 파일, 175 페이지의 내용을 참고하십시오.

규칙	**Syntax**	설명
Attachment MIME Type	`attachment-mimetype`	메시지에 특정 MIME 유형의 첨부 파일이 포함되어 있습니까? MIME 첨부 파일에 의해 제공된 MIME 유형이 평가된다는 점을 제외하면 이 규칙은 `attachment-type` 규칙과 유사합니다. (명시적 유형이 제공되지 않은 경우 어플라이언스는 확장명으로 파일 형식을 "추측"하려고 시도하지 않습니다.) 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.
Attachment Protected	`attachment-protected`	메시지에 비밀번호로 보호되는 첨부 파일이 포함되어 있습니까? 보호된 첨부 파일 격리, 239 페이지를 참조하십시오.
Attachment Unprotected	`attachment-unprotected`	검사 엔진이 보호되지 않는 첨부 파일을 탐지하면 attachment-unprotected 필터 조건은 true를 반환합니다. 검사 엔진이 첨부 파일을 읽을 수 있으면 파일이 보호되지 않는 것으로 간주됩니다. 보호되지 않는 항목이 포함된 zip 파일은 보호되지 않는 것으로 간주됩니다. 참고 - attachment-unprotected 필터 조건과 attachment-protected 필터 조건은 상호 배타적이지 않습니다. 동일한 첨부 파일을 검사할 때 두 필터 조건에서 모두 true를 반환할 수 있습니다. 이는 zip 파일에 보호되는 항목과 보호되지 않는 항목이 모두 포함된 경우 발생할 수 있습니다. 보호되지 않은 첨부 파일 탐지, 239 페이지를 참조하십시오.

규칙	**Syntax**	설명
Attachment Scanning(첨부 파일 검사)a	`attachment-contains (<regular expression>)`	메시지에 포함된 첨부 파일에 특정 패턴과 일치하는 또 다른 첨부 파일 또는 텍스트가 포함되어 있습니까? 패턴이 임계값에 대해 지정한 최소 횟수만큼 발생합니까? 이 규칙은 `body-contains()` 규칙과 유사하지만, 메시지의 전체 "본문"에 대한 검사를 피하려고 시도합니다. 즉, 사용자가 첨부 파일로 보는 부분만 검사하려고 시도합니다. 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.
Attachment Scanning(첨부 파일 검사)	`attachment-binary-contains (<regular expression>)`	메시지에 특정 패턴과 일치하는 이진 데이터의 첨부 파일이 포함되어 있습니까? 이 규칙은 `attachment-contains()` 규칙과 유사하지만, 특별히 이진 데이터에서 패턴을 검색합니다.
Attachment Scanning(첨부 파일 검사)	`every-attachment-contains (<regular expression>)`	이 메시지의 첨부 파일에 특정 패턴과 일치하는 텍스트가 포함되어 있습니까? 텍스트는 모든 첨부 파일에 존재해야 하며, 수행된 작업은 결과적으로 각 첨부 파일에 대한 '`attachment-contains()`'의 논리적 AND 연산입니다. 본문은 검사되지 않습니다. 패턴이 임계값에 대해 지정한 최소 횟수만큼 발생합니까? 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.

규칙	**Syntax**	설명
Attachment Size(첨부 파일 크기)a	`attachment-size`	메시지에 크기가 일정 범위 내에 있는 첨부 파일이 포함되어 있습니까? 이 규칙은 `body-size` 규칙과 유사하지만, 메시지의 전체 "본문"에 대한 검사를 피하려고 시도합니다. 즉, 사용자가 첨부 파일로 간주할 부분만 검사하려고 시도합니다. 디코딩 전에 크기가 평가됩니다. 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.
Public Blacklists(퍼블릭 블랙리스트)	`dnslist(<query server>)`	발신자의 IP 주소가 퍼블릭 블랙리스트 서버(RBL)에 나타납니까? DNS List(DNS 리스트) 규칙, 175 페이지의 내용을 참조하십시오.
SenderBase Reputation	`reputation`	발신자의 SenderBase Reputation 점수는 몇 점입니까? SenderBase Reputation 규칙, 176 페이지를 참조하십시오.
No SenderBase Reputation(SenderBase Reputation 없음)	`no-reputation`	SenderBase Reputation 점수가 "None(없음)"인지 테스트하는 데 사용됩니다. SenderBase Reputation 규칙, 176 페이지를 참조하십시오.
사전	`dictionary-match (<dictionary_name>)`	메시지 본문에 *dictionary_name*이라는 콘텐츠 사전에 있는 용어 또는 정규식이 포함되어 있습니까? 패턴이 임계값에 대해 지정한 최소 횟수만큼 발생합니까? Dictionary(사전) 규칙, 177 페이지를 참조하십시오.
Attachment Dictionary Match(첨부 파일 사전 일치)	`attachment-dictionary-match (<dictionary_name>)`	첨부 파일에 *dictionary_name*이라는 콘텐츠 사전에 있는 정규식이 포함되어 있습니까? 패턴이 임계값에 대해 지정한 최소 횟수만큼 발생합니까? Dictionary(사전) 규칙, 177 페이지를 참조하십시오.

규칙	**Syntax**	설명
Subject Dictionary Match(제목 사전 일치)	`subject-dictionary-match (<dictionary_name>)`	Subject 헤더에 *dictionary name*이라는 콘텐츠 사전에 있는 정규식 또는 용어가 포함되어 있습니까? Dictionary(사전) 규칙, 177 페이지를 참조하십시오.
Header Dictionary Match(헤더 사전 일치)	`header-dictionary-match (<dictionary_name>, <header>)`	지정된 헤더(대/소문자 구분 없음)에 *dictionary name*이라는 콘텐츠 사전에 있는 정규식 또는 용어가 포함되어 있습니까? Dictionary(사전) 규칙, 177 페이지를 참조하십시오.
Body Dictionary Match(본문 사전 일치)	`body-dictionary-match (<dictionary_name>)`	메시지 본문에만 일치하는 사전 용어가 있는 경우 이 필터 조건은 true를 반환합니다. 이 필터는 첨부 파일이라고 간주되지 않는 MIME 부분 내에서 용어를 검색하고, 사용자 정의 임계값(기본 임계값은 1)이 충족되면 true를 반환합니다. Dictionary(사전) 규칙, 177 페이지를 참조하십시오.
Envelope Recipient Dictionary Match(봉투 수신자 사전 일치)	`rcpt-to-dictionary-match (<dictionary_name>)`	봉투 수신자에 *dictionary name*이라는 콘텐츠 사전에 있는 정규식 또는 용어가 포함되어 있습니까? Dictionary(사전) 규칙, 177 페이지를 참조하십시오.
Envelope Sender Dictionary Match(봉투 발신자 사전 일치)	`mail-from-dictionary-match (<dictionary_name>)`	봉투 발신자에 *dictionary name*이라는 콘텐츠 사전에 있는 정규식 또는 용어가 포함되어 있습니까? Dictionary(사전) 규칙, 177 페이지를 참조하십시오.
SMTP Authenticated User Match(SMTP 인증 사용자 일치)	`smtp-auth-id-matches (<target>[, <sieve-char>])`	봉투 발신자의 주소 및 메시지 헤더의 주소가 발신자의 인증된 SMTP 사용자 ID와 일치합니까? SMTP 인증 사용자 일치 규칙, 181 페이지를 참조하십시오.
True(참)	`true`	모든 메시지가 일치합니다. True 규칙, 165 페이지를 참조하십시오.

규칙	**Syntax**	설명
Valid(유효)	`valid`	메시지에 구문 분석할 수 없는/잘못된 MIME 부분이 포함되어 있으면 false, 그렇지 않으면 true를 반환합니다. 유효한 규칙, 165 페이지를 참조하십시오.
Signed(서명)	`signed`	메시지가 서명되었습니까? Signed 규칙, 183 페이지를 참조하십시오.
Signed Certificate(서명 인증서)	`signed-certificate (<field> [<operator> <regular expression>])`	메시지 서명자 또는 X.509 인증서 발급자가 특정 패턴과 일치합니까? Signed Certificate(서명 인증서) 규칙, 184 페이지를 참조하십시오.
Header Repeats(헤더 반복)	`header-repeats (<target>, <threshold> [, <direction>])`	특정 시점에 다음이 탐지되는 경우 `true`를 반환합니다. • 지난 1시간 동안 동일한 제목 헤더의 지정된 메시지 수가 탐지되는 경우 • 지난 1시간 동안 동일한 봉투 발신자로부터 지정된 메시지 수가 탐지되는 경우 Header Repeats(헤더 반복) 규칙, 186 페이지를 참조하십시오.
URL Reputation(URL 평판)	`url-reputation url-no-reputation`	메시지에 있는 URL의 평판 점수가 지정된 범위 내에 있습니까? URL의 평판 점수를 사용할 수 없습니까? URL Reputation(URL 평판) 규칙, 188 페이지 및 외부 피드 위협을 사용하도록 Cisco Email Security 게이트웨이 구성, 307 페이지 항목을 참고하십시오.
URL 범주	`url-category`	메시지에 있는 URL의 범주가 지정된 범주와 일치합니까? URL Category(URL 범주) 규칙, 189 페이지를 참조하십시오.

규칙	**Syntax**	설명
Corrupt Attachment(손상된 첨부 파일)	`attachment-corrupt`	메시지에 손상된 첨부 파일이 있습니까? Corrupt Attachment(손상된 첨부 파일) 규칙, 189 페이지를 참조하십시오.
메시지 언어	`message-language`	선택한 언어 중 하나의 메시지(제목 및 본문)입니까? 메시지 언어 규칙, 189 페이지의 내용을 참조하십시오.
매크로 탐지	`macro-detection-rule (['file_type-1', 'file_type-2', …,'file_type-n'])`	수신 또는 발신 메시지에 매크로가 활성화된 첨부 파일이 포함되어 있습니까? 매크로 탐지 규칙, 190 페이지를 참조하십시오.
위조 이메일 탐지	`forged-email-detection ("<dictionary_name>", <threshold>)`	메시지의 발신인 주소가 위조되었습니까? 이 규칙은 메시지의 발신인: 헤더가 콘텐츠 사전에 있는 임의 사용자와 유사한지 여부를 확인합니다. 위조 이메일 탐지 규칙, 191 페이지의 내용을 참조하십시오.
중복 경계 확인	`duplicate_boundaries`	메시지에 중복 MIME 경계가 포함되어 있습니까? 중복 경계 확인 규칙, 192 페이지의 내용을 참조하십시오.
잘못된 형식의 MIME 헤더 탐지	`malformed-header`	메시지에 잘못된 형식의 MIME 헤더가 포함되어 있습니까? 잘못된 형식의 MIME 헤더 탐지 규칙, 192 페이지를 참조하십시오.

규칙	**Syntax**	설명
지리위치	`geolocation-rule (['country_name-1', 'country_name-2', 'country_name-n'])`	수신 메시지가 선택한 국가에서 시작되었습니까? 참고 지리위치 콘텐츠 필터 규칙을 사용하기 전에 어플라이언스에서 안티 스팸 엔진을 활성화합니다. 지리위치 규칙, 193 페이지의 내용을 참조하십시오.

도메인 평판	`Sender Domain Reputation:`
	`- sdr-reputation (<'sdr_verdict_range'>, <'domain_exception_list'>)`
	`- sdr-age (<'unit'>, <'operator'> <'actual value'>)`
	`- sdr-unscannable (<'domain_exception_list'>)`
	
	`External Threat Feeds:`
	`domain-external-threat-feeds (<'external_threat_feed_source_name'>, <'header'> , <'domain_exception_list'>)`
		발신인 도메인이 지정한 기준과 일치합니까?
		• 발신인 도메인 평판
		• 외부 위협 피드
		ETF에 대한 도메인 평판 규칙, 193 페이지 또는 SDR에 대한 도메인 평판 규칙, 194 페이지를 참조하십시오.
		자세한 내용은 외부 피드 위협을 사용하도록 Cisco Email Security 게이트웨이 구성, 307 페이지 또는 발신자 도메인 평판 필터링, 323 페이지 항목을 참고하십시오.

메시지의 추가 처리를 중단하는 최종 작업을 지정하지 않는 한 Cisco 어플라이언스에 주입된 각 메시지는 모든 메시지 필터를 통해 순서대로 처리됩니다. (메시지 필터 작업, 138 페이지 참조) 필터는 또한 모든 메시지에 적용될 수 있으며, 규칙은 논리적 연결자(AND, OR, NOT)를 사용하여 결합할 수 있습니다.

규칙의 정규식

규칙 정의에 사용되는 몇몇 소규모 테스트는 정규식 일치를 사용합니다. 정규식은 복잡해질 수 있습니다. 메시지 필터 규칙 내에서 정규식을 적용하려면 다음 표를 지침으로 사용하십시오.

표 ***21:*** 규칙의 정규식

정규식(`abc`)	정규식에 있는 지시문의 시퀀스가 문자열의 일부와 일치하는 경우 필터 규칙의 정규식은 문자열과 일치합니다. 예를 들어 정규식 Georg는 `George Of The Jungle` 문자열, `Georgy Porgy`, `La Meson Georgette` 문자열 및 `Georg`와 일치합니다.

캐럿(^) 달러 기호($)	달러 기호 문자($)를 포함하는 규칙은 문자열의 끝에서만 일치하고, 캐럿 기호(^)를 포함하는 규칙은 문자열의 시작에서만 일치합니다. 예를 들어 `^Georg$`는 `Georg`와만 일치합니다. 빈 헤더에 대한 검색은 "^$"와 같을 수 있습니다.
문자, 공백 및 @ 기호 문자	문자, 공백 및 @ 기호를 포함하는 규칙은 그 자체와만 명시적으로 일치합니다. 예를 들어 `^George@admin$` 정규식은 `George@admin` 문자열과만 일치합니다.
마침표 문자(.)	마침표 문자(.)를 포함하는 규칙은 모든 문자와 일치합니다(새 줄 제외). 예를 들어 `^...admin$` 정규식은 `macadmin` 문자열 및 `sunadmin`과 일치하지만 `win32admin`과는 일치하지 않습니다.
별표(*) 지시문	별표(*)를 포함하는 규칙은 "0개 이상의 이전 지시문 일치"를 확인합니다. 특히 마침표와 별표 시퀀스(.*)는 모든 문자 시퀀스와 일치합니다(새 줄 제외). 예를 들어 정규식 `^P.*Piper$`는 `PPiper, Peter Piper, P.Piper` 및 `Penelope Penny Piper` 문자열과 모두 일치합니다.
백슬래시 특수 문자(\)	백슬래시 문자는 특수 문자를 이스케이프합니다. 따라서 `\.` 시퀀스는 리터럴 마침표와만 일치하고, `\$` 시퀀스는 리터럴 달러 기호와만 일치하고, `\^` 시퀀스는 리터럴 캐럿 기호와만 일치합니다. 예를 들어 `^ik\.ac\.uk$` 정규식은 `ik.ac.uk` 문자열과만 일치합니다. 중요 참고 사항**:** 백슬래시는 파서용 특수 이스케이프 문자이기도 합니다. 따라서 정규식에 백슬래시를 포함하려면 구문 분석 후 하나의 "진짜" 백슬래시만 남아 정규식 시스템으로 전달되도록 백슬래시를 *2*개 사용해야 합니다. 따라서 위의 도메인 예와 일치하도록 하려면 `^ik\\.ac\\.uk$`를 입력합니다.
대/소문자 구분 안 함 (`(?i)`)	정규식의 나머지를 나타내는 (?i) 토큰은 대/소문자를 구분하지 않는 모드에서 사용해야 합니다. 대/소문자를 구분하는 정규식의 시작 부분에 이 토큰을 사용하면 대/소문자 일치가 완전히 무시됩니다. 예를 들어 "`(?i)viagra`" 정규식은 `Viagra, vIaGrA 및 VIAGRA`와 일치합니다.
반복 수`{min,max}`	이전 토큰의 반복 수를 나타내는 정규식 표기법이 지원됩니다. 예를 들어 "`fo\{2,3\}`" 식은 `foo` 및 `fooo`와는 일치하지만 fo 또는 fofo와는 일치하지 않습니다. `if(header('To') == "^.{500,}")` 문은 문자가 500개 이상인 "To" 헤더를 검색합니다.

또는 (|)	대체 또는 "or" 연산자. A 및 B가 정규식이면 "A|B" 식은 "A" 또는 "B"와 일치하는 문자열과 일치합니다. 예를 들어 "foo|bar" 식은 foo 또는 bar와 일치하지만 foobar와는 일치하지 않습니다.

관련 주제

- 정규식을 사용하여 메시지 필터링, 160 페이지
- 정규식 사용 지침, 160 페이지
- 정규식 및 비 ASCII 문자 집합, 161 페이지
- n 테스트, 161 페이지
- 대/소문자 구분, 161 페이지
- 효율적인 필터 작성, 161 페이지
- PDF 및 정규식, 162 페이지

정규식을 사용하여 메시지 필터링

필터를 사용하면 비 ASCII 인코딩 메시지 내용(헤더와 본문 모두)에서 문자열과 패턴을 검색할 수 있습니다. 특히 시스템은 다음에서 비 ASCII 문자 집합을 검색하는 정규식(regex)을 지원합니다.

- 메시지 헤더
- MIME 첨부 파일의 파일 이름 문자열
- 메시지 본문
  - MIME 헤더가 없는 본문(즉, 기존 이메일)
  - MIME 헤더가 있는 본문(인코딩을 나타내지만 MIME 부분 없음)
  - 인코딩이 표시된 멀티파트 MIME 메시지
  - MIME 헤더에 인코딩이 지정되지 않은 위의 모두

정규식(regex)을 사용하면 첨부 파일을 포함하여 메시지나 본문의 어느 부분에서나 일치를 확인할 수 있습니다. 다양한 첨부 파일 형식에는 텍스트, HTML, MS Word, Excel 등이 포함됩니다. 문자 집합에는 gb2312, HZ, EUC, JIS, Shift-JIS, Big5, Unicode 등이 포함됩니다. 콘텐츠 필터 GUI를 통해 정규식이 포함된 메시지 필터 규칙을 만들 수 있습니다. 또는 텍스트 편집기를 사용하여 파일을 생성한 후 시스템으로 가져올 수 있습니다. 자세한 내용은 CLI를 사용하여 메시지 필터 관리, 240 페이지 및 검사 동작 구성, 263 페이지를 참조하십시오.

정규식 사용 지침

접두사 없이 문자열의 정확한 일치를 찾으려면 정규식을 캐럿(^)으로 시작하고 달러 기호($)로 끝내는 것이 중요합니다.

참고 빈 문자열 일치를 찾으려면 “”를 사용하지 마십시오. 이것은 실제로 모든 문자열과 일치합니다. 대신 "^ $"를 사용합니다. 예를 보려면 Subject(제목) 규칙, 165 페이지의 두 번째 예를 참조해 주십시오.

또한 리터럴 마침표 일치를 찾으려면 정규식에서 이스케이프된 마침표를 사용해야 합니다. 예를 들어 sun.com 정규식은 `thegodsunocommando` 문자열과 일치하지만, `^sun\.com$` 정규식은 `sun.com` 문자열과만 일치합니다.

기술적으로, 사용되는 정규식의 스타일은 **Python re Module** 스타일 정규식입니다. Python 스타일 정규식에 대한 자세한 내용은 Python Regular Expression HOWTO(`http://www.python.org/doc/howto/`)를 참고하십시오.

정규식 및 비 **ASCII** 문자 집합

일부 언어에는 단어나 단어 경계 또는 대/소문자라는 개념이 없습니다.

로캘이 알려지지 않았거나 인코딩이 확실히 알려지지 않은 경우 단어를 구성하는 문자가 무엇인가에 대한 개념에 의존하는 복잡한 정규식(regex 구문에서 "\w"로 표현)은 문제를 일으킵니다.

n 테스트

정규식에서 `==` 시퀀스를 사용하여 일치를, `!=` 시퀀스를 사용하여 비일치를 테스트할 수 있습니다. 예를 들면 다음과 같습니다.

```
rcpt-to ==
 "^goober@dev\\.null\\....$" (matching)


rcpt-to != "^goober@dev\\.null\\....$" (non-matching)
```

대/소문자 구분

달리 표기하지 않는 한 정규식은 대/소문자를 구분합니다. 따라서 정규식에서 `foo`를 검색하는 경우 `FOO` 또는 `Foo` 패턴은 일치하지 않습니다.

효율적인 필터 작성

다음 예는 동일한 작업을 수행하는 두 필터를 보여주지만, 첫 번째 필터가 CPU를 훨씬 많이 사용합니다. 두 번째 필터는 훨씬 효율적인 정규식을 사용합니다.

```
attachment-filter: if ((recv-listener == "Inbound") AND
((((((((((((((((((((((((((((((((((((((((((((((((((((attachment-filename ==


"\\.386$") OR (attachment-filename == "\\.exe$")) OR (attachment-filename == "\\.ad$")) OR

(attachment-filename == "\\.ade$")) OR (attachment-filename == "\\.adp$")) OR
(attachment-filename == "\\.asp$")) OR (attachment-filename == "\\.bas$")) OR
(attachment-filename == "\\.bat$")) OR (attachment-filename == "\\.chm$")) OR
(attachment-filename == "\\.cmd$")) OR (attachment-filename == "\\.com$")) OR
(attachment-filename == "\\.cpl$")) OR (attachment-filename == "\\.crt$")) OR
(attachment-filename == "\\.exe$")) OR (attachment-filename == "\\.hlp$")) OR
(attachment-filename == "\\.hta$")) OR (attachment-filename == "\\.inf$")) OR
(attachment-filename == "\\.ins$")) OR (attachment- filename == "\\.isp$")) OR
(attachment-filename == "\\.js$")) OR (attachment-filename == "\\.jse$")) OR
(attachment- filename == "\\.lnk$")) OR (attachment-filename == "\\.mdb$")) OR
(attachment-filename == "\\.mde$")) OR (attachment-filename == "\\.msc$")) OR
(attachment-filename == "\\.msi$")) OR (attachment-filename == "\\.msp$")) OR
```

```
(attachment-filename == "\\.mst$")) OR (attachment-filename == "\\.pcd$")) OR
(attachment-filename == "\\.pif$")) OR (attachment-filename == "\\.reg$")) OR
(attachment-filename == "\\.scr$")) OR (attachment-filename == "\\.sct$")) OR
(attachment-filename == "\\.shb$")) OR (attachment-filename == "\\.shs$")) OR
(attachment-filename == "\\.url$")) OR (attachment-filename == "\\.vb$")) OR
(attachment-filename == "\\.vbe$")) OR (attachment-filename == "\\.vbs$")) OR
(attachment-filename == "\\.vss$")) OR (attachment-filename == "\\.vst$")) OR
(attachment-filename == "\\.vsw$")) OR (attachment-filename == "\\.ws$")) OR
(attachment-filename == "\\.wsc$")) OR (attachment-filename == "\\.wsf$")) OR
(attachment-filename == "\\.wsh$"))) { bounce(); }
```

이 경우 AsyncOS는 각 첨부 파일 형식 및 recv-listener에 대해 한 번씩 정규식 엔진을 30번 시작해야 합니다.

대신 다음과 같은 필터를 작성할 수 있습니다.

```
attachment-filter: if (recv-listener == "Inbound") AND (attachment-filename == "\\.
(386|exe|ad|ade|adp|asp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|jse|l
nk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|
url|vb|vbe|vbs|vss|vst|vsw|ws|wsc|wsf|wsh)$") {
```

정규식 엔진은 두 번만 시작하면 됩니다. 또한 "()" 추가, 철자 오류에 대해 걱정할 필요가 없으므로 필터 유지 관리가 훨씬 더 쉽습니다. 위의 예와는 반대로 CPU 오버헤드가 감소합니다.

PDF 및 정규식

PDF의 생성 방식에 따라 공백이나 줄 바꿈이 포함되어 있지 않을 수 있습니다. 이 경우 검사 엔진은 페이지에서 단어의 위치를 기반으로 논리적 공백 및 줄 바꿈을 삽입하려고 시도합니다. 예를 들어 한 단어가 여러 글꼴 또는 글꼴 크기로 이루어진 경우, 검사 엔진은 렌더링된 PDF 코드에서 단어 및 줄 바꿈을 판단하기가 어려워집니다. 이런 방식으로 만들어진 PDF 파일에서 정규식 일치를 시도하면 검사 엔진은 예기치 못한 결과를 반환할 수 있습니다.

예를 들어 단어의 각 글자에 서로 다른 글꼴 및 글꼴 크기를 사용하는 PowerPoint 문서에 단어를 입력합니다. 검사 엔진은 이 애플리케이션에서 생성된 PDF를 읽고 논리적 공백과 줄 바꿈을 삽입합니다. PDF의 구성 때문에 검사 엔진은 "callout을 "call out" 또는 "c a l lout"으로 해석할 수 있습니다. "callout" 정규식으로 이러한 렌더링 중 하나의 일치를 확인하려고 시도하면 일치 결과가 반환되지 않을 수 있습니다.

스마트 식별자

메시지 내용을 검사하는 메시지 규칙을 사용할 때 스마트 식별자를 사용하면 데이터에서 특정 패턴을 탐지할 수 있습니다.

스마트 식별자는 데이터에서 다음 패턴을 탐지할 수 있습니다.

- 신용 카드 번호
- 미국 사회 보장 번호
- CUSIP(Committee on Uniform Security Identification Procedures) 번호
- ABA(American Banking Association) 라우팅 번호

필터에서 스마트 식별자를 사용하려면 본문 또는 첨부 파일 내용을 검사하는 필터 규칙에 다음 키워드를 입력하십시오.

표 *22:* 메시지 필터의 스마트 식별자

키워드	스마트 식별자	설명
*credit	신용카드 번호	14, 15 및 16자리 신용카드 번호를 식별합니다. 참고: 스마트 식별자는 enRoute 카드를 식별하지 않습니다.
*aba	ABA 라우팅 번호	ABA 라우팅 번호를 식별합니다.
*ssn	사회 보장 번호	미국 사회 보장 번호를 식별합니다. *ssn 스마트 식별자는 대시, 마침표 및 공백이 포함된 사회 보장 번호를 식별합니다.
*cusip	CUSIP 번호	CUSIP 번호를 식별합니다.

관련 주제

- 스마트 식별자 구문, 163 페이지

스마트 식별자 구문

필터 규칙에서 스마트 식별자를 사용할 때에는 다음 예와 같이, 본문 또는 첨부 파일을 검사하는 스마트 식별자 키워드를 필터 규칙 내에서 따옴표로 묶어 입력합니다.

```
ID_Credit_Cards:

if(body-contains("*credit")){

notify("legaldept@example.com");

}
.
```

스마트 식별자를 콘텐츠 필터에서 사용할 수 있으며 콘텐츠 사전의 일부로서 사용할 수도 있습니다.

참고 스마트 식별자 키워드는 일반 정규식 또는 다른 키워드와 결합할 수 없습니다. 예를 들어 `*credit|*ssn` 패턴은 유효하지 않습니다.

참고 *SSN 스마트 식별자 사용에 따른 오탐을 최소화하려면 *ssn 스마트 식별자를 다른 필터 기준과 함께 사용하는 것이 도움이 될 수 있습니다. 한 가지 필터 사용 예는 "only-body-contains" 필터 조건입니다. 이 조건은 메시지 본문 MIME 부분에 검색 문자열이 있는 경우에만 식을 true로 평가합니다. 예를 들면 다음 필터를 만들 수 있습니다.

```
SSN-nohtml: if only-body-contains(“*ssn”) { duplicate-quarantine(“Policy”);}
```

메시지 필터 규칙의 설명 및 예

다음 섹션에서는 사용 중인 다양한 메시지 필터 규칙을 설명하고 해당 예를 보여줍니다.

관련 주제

- 메시지 언어 규칙, 189 페이지
- 매크로 탐지 규칙, 190 페이지
- 위조 이메일 탐지 규칙, 191 페이지
- 중복 경계 확인 규칙, 192 페이지
- 잘못된 형식의 MIME 헤더 탐지 규칙, 192 페이지
- 지리위치 규칙, 193 페이지
- ETF에 대한 도메인 평판 규칙, 193 페이지
- SDR에 대한 도메인 평판 규칙, 194 페이지

True 규칙

true 규칙은 모든 메시지와 일치합니다. 예를 들어 다음 규칙은 테스트하는 모든 메시지에서 IP 인터페이스를 external로 변경합니다.

```
externalFilter:

   if (true)

   {

        alt-src-host('external');

   }
```

유효한 규칙

`valid` 규칙은 메시지에 구문 분석할 수 없는/잘못된 MIME 부분이 포함되어 있으면 false, 그렇지 않으면 true를 반환합니다. 예를 들어 다음 규칙은 테스트하는 규칙 중 구문 분석할 수 없는 규칙을 모두 삭제합니다.

```
not-valid-mime:

if not valid

{

drop();

}
```

Subject(제목) 규칙

`subject` 규칙은 제목 헤더의 값이 지정된 정규식과 일치하는 메시지를 선택합니다.

예를 들어 다음 필터는 제목이 Make Money... 구문으로 시작되는 모든 메시지를 삭제합니다.

```
not-valid-mime:

if not valid

{

drop();
```

```
}
```

헤더의 값에서 비 ASCII 문자를 검색하도록 지정할 수도 있습니다.

헤더로 작업할 때는 헤더의 현재 값에 처리 중 변경된 내용(예: 메시지 제목을 추가, 제거 또는 수정하는 필터 작업으로)이 포함되어 있다는 점을 기억해야 합니다. 자세한 내용은 메시지 헤더 규칙 및 평가, 141 페이지를 참조하십시오.

다음 필터는 헤더가 비어 있거나 메시지에서 누락되어 있으면 true를 반환합니다.

```
EmptySubject_To_filter:

if (header('Subject') != ".") OR

(header('To') != ".") {

drop();

}
```

참고 이 필터는 Subject 및 To 헤더에 대해 true를 반환하지만, 누락된 헤더에 대해서도 true를 반환합니다. 메시지에 지정된 헤더가 포함되어 있지 않아도 필터는 true를 반환합니다.

Envelope Recipient(봉투 수신자) 규칙

rcpt-to 규칙은 봉투 수신자가 지정된 정규식과 일치하는 메시지를 선택합니다. 예를 들어 다음 필터는 "scarface" 문자열이 포함된 이메일 주소로 전송된 모든 메시지를 삭제합니다.

참고 rcpt-to 규칙에 대한 정규식은 대/소문자를 구분하지 않습니다.

```
scarfaceFilter:

if (rcpt-to == 'scarface')

{

drop();

}
```

참고 rcpt-to 규칙은 메시지 기반입니다. 메시지 수신자가 여러 명인 경우, 메시지가 모든 수신자에게 영향을 미치려면 한 수신자만 지정된 작업에 대한 규칙과 일치해야 합니다.

Envelope Recipient in Group(그룹의 봉투 수신자) 규칙

rcpt-to-group 규칙은 봉투 수신자가 지정된 LDAP 그룹의 구성원인 것으로 발견된 메시지를 선택합니다. 예를 들어 다음 필터는 LDAP 그룹 "ExpiredAccounts" 내에 있는 이메일 주소로 전송된 모든 메시지를 삭제합니다.

```
expiredFilter:

if (rcpt-to-group == 'ExpiredAccounts')

{

drop();

}
```

참고 rcpt-to-group 규칙은 메시지 기반입니다. 메시지 수신자가 여러 명인 경우, 메시지가 모든 수신자에게 영향을 미치려면 한 수신자만 지정된 작업에 대한 규칙과 일치해야 합니다.

Envelope Sender(봉투 발신자) 규칙

mail-from 규칙은 봉투 발신자가 지정된 정규식과 일치하는 메시지를 선택합니다. 예를 들어 다음 필터는 admin@yourdomain.com에서 보낸 모든 메시지를 즉시 전달합니다.

참고 mail-from 규칙에 대한 정규식은 대/소문자를 구분하지 않습니다. 다음 예에서 마침표 문자는 이스케이프 처리됩니다.

```
kremFilter:

if (mail-from == '^admin@yourdomain\\.com$')

{

skip-filters();

}
```

Envelope Sender in Group(그룹의 봉투 발신자) 규칙

mail-from-group 규칙은 연산자 오른쪽에 있는 LDAP 그룹에서 봉투 발신자가 발견되는 메시지를 선택합니다(부등호가 사용된 경우 발신자의 이메일 주소는 지정된 LDAP 그룹에 있지 않음). 예를 들어 다음 필터는 LDAP 그룹 "KnownSenders"에 이메일 주소가 있는 사용자가 전송한 모든 메시지를 즉시 전달합니다.

```
SenderLDAPGroupFilter:

if (mail-from-group == 'KnownSenders')

{

skip-filters();

}
```

Sender Group(발신자 그룹) 규칙

sendergroup 메시지 필터는 리스너의 HAT(Host Access Table)에서 어떤 발신자 그룹이 일치하는가를 기반으로 메시지를 선택합니다. 이 규칙은 '=='(일치) 또는 '!='(불일치)를 사용하여 지정된 정규식(식의 오른쪽)의 일치 여부를 테스트합니다. 예를 들어 다음 메시지 필터 규칙은 메시지의 발신자 그룹이 Internal 정규식과 일치하면 true로 평가되고, 이 경우 메시지를 대체 메일 호스트로 전송합니다.

```
senderGroupFilter:

if (sendergroup == "Internal")

{

alt-mailhost("[172.17.0.1]");

}
```

Body Size(본문 크기) 규칙

본문 크기란 헤더와 첨부 파일을 모두 포함한 메시지의 크기를 말합니다. body-size 규칙은 본문 크기를 지정된 숫자와 비교해야 하는 메시지를 선택합니다. 예를 들어 다음 필터는 본문 크기가 5메가바이트보다 큰 메시지를 반송합니다.

```
BigFilter:

if (body-size > 5M)

{

bounce();

}
```

body-size는 다음과 같은 방법을 비교할 수 있습니다.

예	비교 유형
`body-size < 10M`	보다 작음
`body-size <= 10M`	보다 작거나 같음
`body-size > 10M`	보다 큼
`body-size >= 10M`	보다 크거나 같음
`body-size == 10M`	같음
`body-size != 10M`	같지 않음

편의상 크기 측정은 접미사로 지정될 수 있습니다.

수량	설명
`10b`	10바이트
`13k`	13킬로바이트
`5M`	5메가바이트
`40G`	40기가바이트(참고: Cisco 어플라이언스는 100메가바이트보다 큰 메시지를 수락하지 않습니다.)

Remote IP(원격 IP) 규칙

`remote-ip` 규칙은 메시지를 전송한 호스트의 IP 주소가 특정 패턴과 일치하는지를 테스트합니다. IP 주소는 IPv4(Internet Protocol version 4) 또는 IPv6(Internet Protocol version 6)일 수 있습니다. IP 주소 패턴은 "Sender Group Syntax"에 설명된 허용되는 호스트 표기법을 사용하여 지정됩니다(`SBO`, `SBRS`, `dnslist` 표기법 및 특수 키워드 `ALL` 제외).

허용되는 호스트 표기법은 IP 주소(호스트 이름 아님)의 시퀀스와 숫자 범위만 식별합니다. 예를 들어 다음 필터는 `10.1.1.x` 형식의 IP 주소(여기서 X는 `50`, `51`, `52`, `53`, `54` 또는 `55`)에서 주입되지 않은 모든 메시지를 반송합니다.

```
notMineFilter:

if (remote-ip != '10.1.1.50-55')

{

bounce();

}
```

Receiving Listener(수신 리스너) 규칙

`recv-listener` 규칙은 명명된 리스너에서 수신된 메시지를 선택합니다. 리스너 이름은 시스템에 현재 구성된 리스너 중 하나의 별칭이어야 합니다. 예를 들어 다음 필터는 expedite라는 이름의 리스너에서 도착하는 모든 메시지를 즉시 전달합니다.

```
expediteFilter:

if (recv-listener == 'expedite')

{

skip-filters();

}
```

Receiving IP Interface(수신 IP 인터페이스) 규칙

recv-int 규칙은 명명된 인터페이스를 통해 수신된 메시지를 선택합니다. 인터페이스 이름은 시스템에 대해 현재 구성된 인터페이스 중 하나의 별칭이어야 합니다. 예를 들어 다음 필터는 outside라는 이름의 인터페이스에서 도착하는 모든 메시지를 반송합니다.

```
outsideFilter:

if (recv-int == 'outside')

{

bounce();

}
```

Date(날짜) 규칙

date 규칙은 사용자가 지정한 시간과 날짜를 기준으로 현재 시간과 날짜를 확인합니다. 날짜 규칙은 *MM/DD/YYYY hh:mm:ss* 형식의 타임스탬프가 포함된 문자열과 비교됩니다. 이는 미국 형식의 특정 시간 전후에 수행할 작업을 지정하는 데 유용합니다. (미국 날짜 형식이 아닌 메시지를 검색하는 경우 문제가 될 수 있습니다.) 다음 필터는 2003년 7월 28일 오후 1시 이후 campaign1@yourdomain.com에서 주입된 모든 메시지를 반송합니다.

```
TimeOutFilter:

if ((date > '07/28/2003 13:00:00') and (mail-from ==

'campaign1@yourdomain\\.com'))

{

bounce();

}
```

참고 date 규칙을 $Date 메시지 필터 작업 변수와 혼동해서는 안 됩니다.

Header(헤더) 규칙

header() 규칙은 메시지 헤더에서 특정 헤더를 확인합니다. 이러한 헤더는 따옴표로 지정해야 합니다("*header name*"). 이 규칙은 정규식과 비교할 수도 있고(subject 규칙과 유사) 비교 없이 사용할 수도 있습니다. 이 경우 메시지에서 헤더가 발견되면 "true", 발견되지 않으면 "false"입니다. 다음 예에서는 X-Sample 헤더가 발견되는지, 해당 값에 "sample text"가 포함되어 있는지를 확인합니다. 일치가 확인되면 메시지가 반송됩니다.

```
FooHeaderFilter:

if (header('X-Sample') == 'sample text')

{

bounce();
```

```
}
```

헤더의 값에서 비 ASCII 문자를 검색하도록 지정할 수도 있습니다.

다음 예는 비교 없는 헤더 규칙을 보여줍니다. 이 경우 `X-DeleteMe` 헤더가 발견되면 메시지에서 제거됩니다.

```
DeleteMeHeaderFilter:

if header('X-DeleteMe')

{

strip-header('X-DeleteMe');

}
```

헤더로 작업할 때는 헤더의 현재 값에 처리 중 변경된 내용(예: 메시지 제목을 추가, 제거 또는 수정하는 필터 작업으로)이 포함되어 있다는 점을 기억해야 합니다. 자세한 내용은 메시지 헤더 규칙 및 평가, 141 페이지를 참조하십시오.

Random(난수) 규칙

`random` 규칙은 영(0)에서 N-1 사이의 난수를 생성합니다. 여기서 N은 규칙 뒤에 괄호로 제공하는 정수 값입니다. `header()` 규칙과 마찬가지로, 이 규칙을 비교에 사용할 수도 있고 단독의 "단항" 형식으로 사용할 수도 있습니다. 생성된 난수가 영(0)이 아니면 규칙은 단항 형식에서 `true`로 평가됩니다. 예를 들어 다음 필터는 모두 실질적으로 동일하지만 시간의 절반은 가상 게이트웨이 주소 A, 나머지 절반은 가상 게이트웨이 주소 B를 선택합니다.

```
load_balance_a:

if (random(10) < 5)
{

alt-src-host('interface_a');
}

else

{

alt-src-host('interface_b');

}

load_balance_b:

if (random(2))

{

alt-src-host('interface_a');

}

else

{

alt-src-host('interface_b');
```

```
}
```

Recipient Count(수신자 수) 규칙

rcpt-count 규칙은 body-size 규칙과 비슷한 방식을 통해 정수 값을 기준으로 메시지의 수신자 수를 비교합니다. 이는 사용자가 동시에 다수의 수신자에게 이메일을 전송하는 것을 방지하거나, 그런 대량 메일링 캠페인이 특정 가상 게이트웨이 주소를 통해 이루어지도록 하려는 경우 유용할 수 있습니다. 다음 예는 특정 가상 게이트웨이 주소를 통해 수신자 100명 이상의 이메일을 전송합니다.

```
large_list_filter:

if (rcpt-count > 100) {

alt-src-host('mass_mailing_interface');

}
```

Address Count(주소 수) 규칙

addr-count() 메시지 필터 규칙은 하나 이상의 헤더 문자열을 가져오고, 각 줄에서 수신자의 수를 계산하고, 누적된 수신자 수를 보고합니다. 이 필터는 봉투 수신자가 아니라 메시지 본문 헤더에 대해 작동된다는 점에서 rcpt-count 필터 규칙과 다릅니다. 다음 예는 긴 수신자 리스트를 "undisclosed-recipients" 별칭과 교체하는 데 사용되는 필터 규칙을 보여줍니다.

```
large_list_filter:


if (rcpt-count > 100) {

alt-src-host('mass_mailing_interface');

}
```

Body Scanning(본문 검사) 규칙

body-contains() 규칙은 수신 이메일 및 모든 해당 첨부 파일에서 파라미터에 정의된 특정 패턴을 검사합니다. 여기에는 delivery-status 부분 및 관련 첨부 파일이 포함됩니다. body-contains() 규칙은 여러 줄 일치 확인을 수행하지 않습니다. 검사할 MIME 유형 또는 검사하지 않을 MIME 유형을 정의하려면 Scan Behavior(검사 동작) 페이지에서 또는 CLI의 scanconfig 명령을 사용하여 검사 로직을 수정할 수 있습니다. 또한 검사가 true로 평가되기 위해 검사 엔진이 찾아야 할 최소 일치 수를 지정할 수 있습니다.

기본적으로 시스템은 video/*, audio/*, image/* MIME 유형을 제외한 모든 첨부 파일을 검사합니다. 시스템은 아카이브 첨부 파일, 즉 여러 파일이 포함된 .zip, .bzip, .compress, .tar 또는 .gzip 첨부 파일을 검사합니다. 검사할 "중첩된" 아카이브 첨부 파일(예: .zip 내에 포함된 .zip)의 수를 설정할 수 있습니다.

자세한 내용은 검사 동작 구성, 263 페이지를 참고하십시오.

Body Scanning(본문 검색)

AsyncOS는 본문 검사를 수행할 때 본문 텍스트와 첨부 파일에서 정규식을 검사합니다. 식에 대한 최소 임계값을 할당할 수 있으며, 검사 엔진이 최소 횟수만큼 정규식을 발견하면 식이 `true`로 평가됩니다.

AsyncOS는 메시지의 서로 다른 MIME 부분을 평가하고, 텍스트인 MIME 부분을 검사합니다. MIME 유형이 첫 번째 부분에서 텍스트를 지정하는 경우 AsyncOS는 텍스트 부분을 식별합니다. AsyncOS는 메시지에 지정된 인코딩을 기반으로 인코딩을 결정하고, 텍스트를 유니코드로 변환합니다. 그런 다음 유니코드 공간에서 정규식을 검색합니다. 메시지에 인코딩이 지정되어 있지 않으면 AsyncOS는 사용자가 Scan Behavior(검사 동작) 페이지에서 또는 `scanconfig` 명령으로 지정한 인코딩을 사용합니다.

AsyncOS에서 메시지를 검사할 때 MIME 부분을 평가하는 방법에 대한 자세한 내용은 메시지 본문과 메시지 첨부 파일 비교, 141 페이지 섹션을 참조해 주십시오.

MIME 부분이 텍스트이면 AsyncOS는 .zip 또는 .tar 아카이브에서 파일을 추출하거나 압축된 파일을 압축 해제합니다. 데이터가 추출되면 검사 엔진은 파일의 인코딩을 식별하고 파일의 데이터를 유니코드로 반환합니다. 그런 다음 AsyncOS는 유니코드 공간에서 정규식을 검색합니다.

다음 예는 본문 텍스트와 첨부 파일에서 "Company Confidential"을 검색합니다. 다음 예에서는 최소 임계값이 2로 지정됩니다. 따라서 검사 엔진이 구문을 둘 이상 발견하면 일치하는 메시지를 반송하고 법무 부서에 해당 시도를 알립니다.

```
ConfidentialFilter:

if (body-contains('Company Confidential',2)) {

notify ('legaldept@example.domain');

bounce();

}
```

메시지의 본문만 검사하려면 `only-body-contains`를 사용합니다.

```
disclaimer:

if (not only-body-contains('[dD]isclaimer',1) ) {

notify('hresource@example.com');

}
```

암호화 탐지 규칙

`encrypted` 규칙은 메시지 내용에서 암호화된 데이터를 검사합니다. 이 규칙은 암호화된 데이터를 디코딩하려고 시도하지 않고, 단지 메시지 내용에 암호화된 데이터가 있는지만 검사합니다. 이는 사용자가 암호화된 이메일을 보내지 못하도록 하는 데 유용할 수 있습니다.

참고 encrypted 규칙은 메시지 내용에서 암호화된 데이터만 탐지합니다. 암호화된 첨부 파일은 탐지하지 않습니다.

파라미터가 없으며 비교할 수 없다는 점에서 encrypted 규칙은 `true` 규칙과 유사합니다. 암호화된 데이터가 발견되면 `true`, 암호화된 데이터가 발견되지 않으면 `false`가 반환됩니다. 이 기능은 메시지를 검사해야 하므로 Scan Behavior(검사 동작) 페이지 또는 `scanconfig` 명령으로 정의된 검사 설정을 사용합니다. 이러한 옵션 구성에 대한 자세한 내용은 검사 동작 구성, 263 페이지 섹션을 참조해 주십시오.

다음 필터는 리스너를 통해 전송되는 모든 이메일을 확인하고, 메시지에 암호화된 데이터가 포함되어 있으면 해당 메시지를 법무 부서에 숨은 참조(BCC)로 전송한 후 반송합니다.

```
prevent_encrypted_data:

if (encrypted) {

bcc ('legaldept@example.domain');

bounce();

}
```

Attachment Type(첨부 파일 형식) 규칙

`attachment-type` 규칙은 메시지의 각 첨부 파일에서 MIME 유형이 지정된 패턴과 일치하는지 확인합니다. 검사 동작 구성, 263 페이지에 설명된 것처럼 패턴은 Scan Behavior(검사 동작) 페이지 또는 `scanconfig` 명령에 사용된 것과 동일한 형식이어야 하며, 슬래시(/) 양쪽 중 하나를 와일드카드로서 별표로 교체할 수 있습니다. 지정된 이 MIME 유형과 일치하는 첨부 파일이 메시지에 포함되어 있으면 규칙은 "true"를 반환합니다.

이 기능은 메시지를 검사하도록 요구하므로 검사 동작 구성, 263 페이지에 설명된 모든 옵션을 따릅니다.

메시지의 첨부 파일을 조작하기 위해 사용할 수 있는 메시지 필터 규칙에 대한 자세한 내용은 Attachment Scanning(첨부 파일 검사), 229 페이지 섹션을 참조해 주십시오.

다음 필터는 리스너를 통해 전송되는 모든 이메일을 확인하고, 메시지에 `video/*` MIME 유형의 첨부 파일이 포함되어 있으면 메시지를 반송합니다.

```
bounce_video_clips:

if (attachment-type == 'video/*') {

bounce();

}
```

Attachment Filename(첨부 파일의 파일 이름) 규칙

`attachment-filename` 규칙은 메시지에 있는 각 첨부 파일의 파일 이름이 지정된 정규식과 일치하는지 확인합니다. 이 비교는 대/소문자를 구분합니다. 그러나 이 비교는 공백도 구분하므로, 파일 이름

의 끝에 인코딩된 공백이 있으면 필터가 첨부 파일을 건너뜁니다. 메시지의 첨부 파일 중 하나에 일치하는 파일 이름이 있으면 규칙은 "true"를 반환합니다.

다음에 유의하십시오.

- 각 첨부 파일의 파일 이름은 MIME 헤더에서 캡처됩니다. MIME 헤더의 파일 이름 끝에 공백이 포함되어 있을 수 있습니다.
- 첨부 파일이 아카이브이면 Cisco 어플라이언스는 아카이브 내에서 파일 이름을 수집하고 검사 구성 규칙을 적절히 적용합니다(검사 동작 구성, 263 페이지 참고).
  - 첨부 파일이 단일 압축 파일이면(파일 확장명과 상관없이) 아카이브로 간주되지 않으며 압축된 파일의 파일 이름이 수집되지 않습니다. 즉, 이 파일은 `attachment-filename` 규칙으로 처리되지 않습니다. 이 유형의 파일 예는 `gzip`으로 압축된 실행 파일(.exe)입니다.
  - 단일 압축 파일로 구성된 첨부 파일(예: foo.exe.gz)에 대해서는 압축 파일 내 특정 파일 형식을 검색하는 정규식을 사용합니다. 아카이브 파일 내 첨부 파일의 파일 이름 및 단일 압축 파일, 175 페이지를 참조하십시오.

메시지의 첨부 파일을 조작하기 위해 사용할 수 있는 메시지 필터 규칙에 대한 자세한 내용은 Attachment Scanning(첨부 파일 검사), 229 페이지 섹션을 참조해 주십시오.

다음 필터는 리스너를 통해 전송되는 모든 이메일을 확인하고, 메시지에 `*.mp3` 파일 이름의 첨부 파일이 포함되어 있으면 메시지를 반송합니다.

```
block_mp3s:

if (attachment-filename == '(?i)\\.mp3$') {

bounce();

}
```

관련 주제

- 아카이브 파일 내 첨부 파일의 파일 이름 및 단일 압축 파일, 175 페이지

아카이브 파일 내 첨부 파일의 파일 이름 및 단일 압축 파일

다음 예는 아카이브에서 단일 압축 파일(예: gzip으로 만든 파일)의 일치를 확인하는 방법을 보여줍니다.

```
quarantine_gzipped_exe_or_pif:

if (attachment-filename == '(?i)\\.(exe|pif)($|.gz$)') {

quarantine("Policy");

}
```

DNS List(DNS 리스트) 규칙

`dnslist()` 규칙은 쿼리에 DNSBL 메서드("ip4r lookups"라고도 함)를 사용하는 퍼블릭 DNS 목록 서버를 쿼리합니다. 수신 연결의 IP 주소가 반전되고(IP 1.2.3.4는 4.3.2.1이 됨) 괄호의 서버 이름에 접두사로서 추가됩니다(서버 이름이 하나로 시작되지 않으면 둘을 구분하는 마침표가 추가됨). DNS 쿼리가

생성되면 서버에 DNS 실패 응답(연결의 IP 주소가 서버 목록에서 발견되지 않았음을 나타냄) 또는 IP 주소(주소가 발견되었음을 나타냄)가 반환됩니다. 반환된 IP 주소는 대개 `127.0.0.x` 형식입니다. 여기서 `x`의 범위는 0~255입니다(IP 주소 범위는 허용되지 않음). 일부 서버는 실제로 나열 이유를 기반으로 서로 다른 숫자를 반환하는 반면, 다른 서버는 모든 일치 항목에 대해 동일한 결과를 반환합니다.

`header()` 규칙과 마찬가지로 `dnslist()`도 단항 또는 이진 비교에 사용할 수 있습니다. 그 자체로 응답이 수신되면 `true`, 응답이 수신되지 않으면(예: DNS 서버에 도달할 수 없는 경우) `false`로 평가됩니다.

발신자가 Cisco Bonded Sender 정보 서버 프로그램과 연결된 경우 다음 필터는 즉시 메시지를 전달합니다.

```
whitelist_bondedsender:

if (dnslist('query.bondedsender.org')) {

skip-filters();

}
```

선택적으로, 등호(==) 또는 부등호(!=) 식을 사용하여 결과를 문자열과 비교할 수 있습니다.

다음 필터는 서버에서 "`127.0.0.2`" 응답을 받는 메시지를 삭제합니다. 다른 응답을 받으면 "false"가 반환되고 필터는 무시됩니다.

```
blacklist:

if (dnslist('dnsbl.example.domain') == '127.0.0.2') {

drop();

}
```

SenderBase Reputation 규칙

`reputation` 규칙은 다른 값을 기준으로 SenderBase Reputation 점수를 검사합니다. > , == , <= 등 모든 비교 연산자가 허용됩니다. 메시지에 SenderBase Reputation 점수가 없으면(확인한 적이 없거나, 시스템이 SenderBase Reputation Service 쿼리 서버에서 응답을 받지 못했기 때문에) 평판을 기준으로 하는 비교가 실패합니다(숫자가 임의의 값보다 크거나, 작거나, 같거나 같지 않은 결과가 나오지 않음). 아래에 설명한 `no-reputation` 규칙을 사용하여 SBRS 점수 "none"을 확인할 수 있습니다. 다음 예는 SenderBase Reputation Service에서 반환되는 평판 점수가 임계값 -7.5보다 낮으면 "`*** BadRep ***`" 접두사가 추가되도록 메시지의 "Subject:" 줄을 조정합니다.

```
note_bad_reps:

if (reputation < -7.5) {
strip-header ('Subject');
insert-header ('Subject', '*** BadRep $Reputation *** $Subject');
}
```

자세한 내용은 "발신자 평판 필터링" 장을 참조해 주십시오. 안티스팸 시스템 우회 작업, 223 페이지 섹션도 참조해 주십시오.

SenderBase Reputation 규칙의 값은 -10에서 10까지이지만, NONE 값이 반환될 수도 있습니다. `NONE` 값을 특별히 확인하려면 `no-reputation` 규칙을 사용합니다.

```
none_rep:

if (no-reputation) {

strip-header ('Subject');

insert-header ('Subject', '*** Reputation = NONE *** $Subject');

}
```

Dictionary(사전) 규칙

"*dictonary_name*"이라는 콘텐츠 사전에 있는 용어 또는 정규식이 메시지 본문에 포함되어 있는 경우 `dictionary-match(<dictonary_name>)` 규칙은 `true`로 평가됩니다. 해당 사전이 존재하지 않으면 규칙은 `false`로 평가됩니다. 사전 정의(대/소문자 및 단어 경계 설정 포함)에 대한 자세한 내용은 "텍스트 리소스" 장을 참조하십시오.

다음 필터는 Cisco에서 "secret_words"라는 이름의 사전에 있는 단어를 포함하는 메시지를 검사할 경우 관리자에게 숨은 참조로 보냅니다.

```
copy_codenames:

if (dictionary-match ('secret_words')) {

bcc('administrator@example.com');

}
```

다음 예는 "secret_words"라는 이름의 사전에 있는 단어가 메시지 본문에 포함된 경우 해당 메시지를 Policy(정책) 격리로 전송합니다. `only-body-contains` 조건과는 달리 `body-dictionary-match` 조건은 모든 콘텐츠 부분이 개별적으로 사전과 일치할 것을 요구하지 않습니다. 각 콘텐츠 부분(multipart/alternative 부분 고려)의 점수가 합산됩니다.

```
quarantine_data_loss_prevention:

if (body-dictionary-match ('secret_words'))

{

quarantine('Policy');

}
```

다음 필터에서는 지정된 사전에 있는 용어와 일치하는 제목이 격리됩니다.

```
quarantine_policy_subject:

if (subject-dictionary-match ('gTest'))

{

quarantine('Policy');

}
```

다음 예는 "to" 헤더에 있는 이메일 주소의 일치를 확인하고 관리자에게 숨은 참조로 전송합니다.

```
headerTest:

if (header-dictionary-match ('competitorsList', 'to'))

{

bcc('administrator@example.com');

}
```

`attachment-dictionary-match(<dictonary_name>)` 규칙은 첨부 파일에서 일치를 검색한다는 점을 제외하고 위의 `dictionary-match` 규칙과 유사하게 작동합니다.

다음 필터는 "secret_words"라는 이름의 사전에 있는 단어가 메시지 첨부 파일에 포함된 경우 해당 메시지를 Policy(정책) 격리로 전송합니다.

```
quarantine_codenames_attachment:

if (attachment-dictionary-match ('secret_words'))

{

quarantine('Policy');

}
```

`header-dictionary-match(<dictonary_name>, <header>)` 규칙은 <*header*>에 지정된 헤더에서 일치를 검색한다는 점을 제외하고 위의 dictionary-match 규칙과 유사하게 작동합니다. 헤더 이름은 대/소문자를 구분하지 않으므로 "subject"와 "Subject" 모두 가능합니다.

다음 필터는 "ex_employees"라는 이름의 사전에 있는 단어가 메시지의 "cc" 헤더에 포함된 경우 해당 메시지를 Policy(정책) 격리로 전송합니다.

```
quarantine_codenames_attachment:

if (header-dictionary-match ('ex_employees', 'cc'))

{

quarantine('Policy');

}
```

사전 용어 내에서 와일드카드를 사용할 수 있습니다. 이메일 주소에서 마침표를 이스케이프할 필요가 없습니다.

SPF-Status 규칙

SPF/SIDF 확인 메일을 받는 경우 SPF/SIDF 확인 결과에 따라 다른 작업을 수행할 수 있습니다. spf-status 규칙은 서로 다른 SPF 확인 결과에 대해 검토합니다. 자세한 내용은 확인 결과, 599 페이지 항목을 참조하십시오.

참고 SPF ID 없이 SPF 확인 메시지 필터 규칙을 구성한 경우 및 메시지에 판정이 각기 다른 여러 SPF ID가 포함된 경우 메시지의 판정 중 하나가 규칙과 일치하면 규칙이 트리거됩니다.

다음 구문을 사용하여 SPF/SIDF 확인 결과에 대해 검토할 수 있습니다.

```
if (spf-status == "Pass")
```

여러 상태 판정에 대해 단일 조건을 검토하려면 다음 구문을 사용할 수 있습니다.

```
if (spf-status == "PermError, TempError")
```

또한 다음 구문을 사용하여 HELO, MAIL FROM 및 PRA ID에 대해 확인 결과를 검사할 수 있습니다.

```
if (spf-status("pra") == "Fail")
```

다음 예는 사용 중인 spf-status 필터를 보여줍니다.

```
skip-spam-check-for-verified-senders:

if (sendergroup == "TRUSTED" and spf-status == "Pass"){

skip-spamcheck();

}

quarantine-spf-failed-mail:

if (spf-status("pra") == "Fail") {

if (spf-status("mailfrom") == "Fail"){

# completely malicious mail

quarantine("Policy");

} else {

if(spf-status("mailfrom") == "SoftFail") {

# malicious mail, but tempting

quarantine("Policy");

}

}

} else {

if(spf-status("pra") == "SoftFail"){

if (spf-status("mailfrom") == "Fail"

or spf-status("mailfrom") == "SoftFail"){
```

```
# malicious mail, but tempting

quarantine("Policy");

}

}

}

stamp-mail-with-spf-verification-error:

if (spf-status("pra") == "PermError, TempError"


or spf-status("mailfrom") == "PermError, TempError"

or spf-status("helo") == "PermError, TempError"){

# permanent error - stamp message subject

strip-header("Subject");

insert-header("Subject", "[POTENTIAL PHISHING] $Subject"); }

.
```

SPF-Passed 규칙

다음 예는 spf-passed로 표시되지 않은 이메일을 격리하는 데 사용되는 `spf-passed` 규칙을 보여줍니다.

```
quarantine-spf-unauthorized-mail:

if (not spf-passed) {

quarantine("Policy");

}
```

참고 `spf-status` 규칙과 달리 spf-passed 규칙은 SPF/SIDF 확인 값을 단순한 부울로 줄입니다. None, Neutral, Softfail, TempError, PermError 및 Fail 확인 결과는 `spf-passed` 규칙으로 전달되지 않은 것으로 취급됩니다. 좀 더 세부적인 결과를 기반으로 메시지에 대해 작업을 수행하려면 `spf-status` 규칙을 사용하십시오.

S/MIME Gateway Message(S/MIME 게이트웨이 메시지) 규칙

S/MIME Gateway Message(S/MIME 게이트웨이 메시지) 규칙은 메시지가 S/MIME으로 서명되거나, 암호화되거나, 서명 및 암호화되었는지를 검사합니다. 다음 메시지 필터는 메시지가 S/MIME 메시지인지를 검토한 후, S/MIME을 사용한 확인 또는 해독이 실패하는 경우 메시지를 격리합니다.

```
quarantine_smime_messages:
if (smime-gateway-message and not smime-gateway-verified) {
quarantine("Policy");
}
```

자세한 내용은 S/MIME 보안 서비스, 537 페이지를 참고하십시오.

S/MIME Gateway Verified(S/MIME 게이트웨이 확인됨) 규칙

S/MIME Gateway Message Verified(S/MIME 게이트웨이 확인) 규칙은 메시지가 성공적으로 확인되거나, 해독되거나, 해독 및 확인되었는지를 검사합니다. 다음 메시지 필터는 메시지가 S/MIME 메시지인지를 검토한 후, S/MIME을 사용한 확인 또는 해독이 실패하는 경우 메시지를 격리합니다.

```
quarantine_smime_messages:
if (smime-gateway-message and not smime-gateway-verified) {
quarantine("Policy");
}
```

자세한 내용은 S/MIME 보안 서비스, 537 페이지을 참조해 주십시오.

Workqueue-count 규칙

`workqueue-count` 규칙은 지정된 값을 기준으로 workqueue-count를 검사합니다. `>` , `==` , `<=` 등 모든 비교 연산자가 허용됩니다.

다음 필터는 작업 대기열 수를 검사하고, 대기열이 지정된 수보다 크면 스팸 검사를 건너뜁니다.

```
wqfull:

if (workqueue-count > 1000) {

skip-spamcheck();

}
```

SPF/SIDF에 대한 자세한 내용은 SPF 및 SIDF 확인 개요, 591 페이지 섹션을 참조해 주십시오.

SMTP 인증 사용자 일치 규칙

어플라이언스에서 SMTP 인증을 사용하여 메시지를 전송하는 경우 `smtp-auth-id-matches` (*<target> [, <sieve-char>]*) 규칙은 발신자의 SMTP 인증 사용자 ID를 기준으로 메시지 헤더 및 봉투 발신자를 검사하여 스푸핑된 헤더가 있는 발신 메시지를 식별합니다. 이 필터는 시스템이 스푸핑 가능성이 있는 메시지를 격리 또는 차단하도록 허용합니다.

`smtp-auth-id-matches` 규칙은 다음 대상을 기준으로 SMTP 인증 ID를 비교합니다.

대상	설명
*EnvelopeFrom	SMTP 변환에서 Envelope Sender(MAIL FROM이라고도 함)의 주소를 비교합니다.
*FromAddress	From 헤더에서 구문 분석된 주소를 비교합니다. From: 헤더에는 여러 주소가 허용되므로 하나만 일치해야 합니다.
*Sender	Sender 헤더에 지정된 주소를 비교합니다.
*Any	ID와 상관없이 인증된 SMTP 세션 중에 만들어진 메시지의 일치를 확인합니다.

대상	설명
*None	인증된 SMTP 세션 중에 만들어지지 않은 메시지의 일치를 확인합니다. 이는 인증이 선택 사항일 때 유용합니다(권장).

필터는 일치 확인을 느슨하게 수행합니다. 대/소문자를 구분하지 않습니다. 선택 사항인 *sieve-char* 매개변수가 제공되면 지정된 문자 뒤에 오는 주소의 마지막 부분이 비교에서 무시됩니다. 예를 들어 + 문자가 매개변수로 포함된 경우 필터는 `joe+folder@example.com` 주소에서 + 문자 뒤에 오는 부분을 무시합니다. 주소가 `joe+smith+folder@example.com`인 경우 `+folder` 부분만 무시됩니다. SMTP 인증 사용자 ID 문자열이 단순한 사용자 이름이고 인증된 이메일 주소가 아닌 경우 대상의 사용자 이름 부분만 일치 확인을 위해 검토됩니다. 도메인은 별도의 규칙에서 확인해야 합니다.

또한 $SMTPAuthID 변수를 사용하여 STMP 인증 사용자 ID를 헤더에 삽입할 수 있습니다.

다음 표에서는 SMTP 인증 ID 및 이메일 주소 간 비교의 예와 `smtp-auth-id-matches` 필터 규칙을 사용하여 일치를 확인할지 여부를 보여줍니다.

SMTP 인증 **ID**	**Sieve Char**	비교 주소	일치 여부
someuser		otheruser@example.com	아니요
someuser		someuser@example.com	예
someuser		someuser@another.com	예
SomeUser		someuser@example.com	예
someuser		someuser+folder@example.com	아니요
someuser	+	someuser+folder@example.com	예
someuser@example.com		someuser@forged.com	아니요
someuser@example.com		someuser@example.com	예
SomeUser@example.com		someuser@example.com	예

다음 필터는 인증된 SMTP 세션 중에 생성된 모든 메시지를 검사하여, From 헤더와 봉투 발신자에 있는 주소가 SMTP 인증 사용자 ID와 일치하는지를 확인합니다. 주소와 ID가 일치하면 필터는 도메인을 확인합니다. 일치하지 않으면 어플라이언스는 메시지를 격리합니다.

```
Msg_Authentication:

if (smtp-auth-id-matches("*Any"))

{

# Always include the original authentication credentials in a

# special header.

insert-header("X-Auth-ID","$SMTPAuthID");

if (smtp-auth-id-matches("*FromAddress", "+") and
```

```
smtp-auth-id-matches("*EnvelopeFrom", "+"))
{
# Username matches. Verify the domain
if header('from') != "(?i)@(?:example\\.com|alternate\\.com)" or
mail-from != "(?i)@(?:example\\.com|alternate\\.com)"
{
# User has specified a domain which cannot be authenticated
quarantine("forged");
}
} else {
# User claims to be an completely different user
quarantine("forged");
}
}
```

Signed 규칙

signed 규칙은 메시지에서 서명을 검사합니다. 이 규칙은 메시지의 서명 여부를 나타내기 위해 부울 값을 반환합니다. 이 규칙은 서명이 ASN.1 DER 인코딩 규칙에 따라 인코딩되었는지, 그리고 CMS SignedData Type 구조(RFC 3852, Section 5.1.)를 준수하는지를 평가합니다. 서명이 콘텐츠와 일치하는지 여부를 검증하거나 인증서의 유효성을 확인하지는 않습니다.

다음 예는 서명된 메시지에 헤더를 삽입하기 위해 사용되는 `signed` 규칙을 보여줍니다.

```
signedcheck: if signed { insert-header("X-Signed", "True"); }
```

다음 예는 특정 발신자 그룹의 서명되지 않은 메시지에서 첨부 파일을 삭제하는 데 사용되는 signed 규칙을 보여줍니다.

```
Signed: if ((sendergroup == "NOTTRUSTED") AND NOT signed) {
html-convert();
if (attachment_size > 0)
{
drop_attachments("");
}
}
```

Signed Certificate(서명 인증서) 규칙

signed-certificate 규칙은 X.509 인증서 발급자 또는 메시지 서명자가 지정된 정규식과 일치하는 S/MIME 메시지를 선택합니다. 이 규칙은 X.509 인증서만 지원합니다.

규칙의 구문은 signed-certificate (<field> [<operator> <regular expression>])입니다. 여기서

- <field>는 따옴표 문자열 “issuer” 또는 “signer”이고,
- <operator>는 == 또는 !=입니다.
- <regular expression>은 "issuer" 또는 "signer"와 일치하는 값입니다.

메시지가 여러 서명을 사용하여 서명된 경우 발급자 또는 서명자가 정규식과 일치하면 규칙은 true를 반환합니다. 이 규칙의 짧은 형식인 signed-certificate(“issuer”) 및 signed-certificate(“signer”)는 S/MIME 메시지에 발급자나 서명자가 포함되어 있으면 true를 반환합니다.

관련 주제

- 서명자, 184 페이지
- 발급자, 184 페이지
- 정규식에서 이스케이프, 184 페이지
- $CertificateSigners 작업 변수, 185 페이지
- 예 1, 186 페이지

서명자

메시지 서명자에 대해 규칙은 X.509 인증서의 subjectAltName 확장에서 rfc822Name 이름의 시퀀스를 추출합니다. 서명 인증서에 subjectAltName 필드가 없거나 이 필드에 rfc822Name 이름이 없으면 signed-certificate(“signer”) 규칙은 false로 평가됩니다. 드물기는 하지만 여러 rfc822Name 이름이 있는 경우 규칙은 정규식에 대해 모든 이름의 일치 여부를 확인하려고 시도하며 첫 번째 일치 항목에 대해 true로 평가합니다.

발급자

발급자는 X.509 인증서에 있는 비어 있지 않은 고유 이름입니다. AsyncOS는 인증서에서 발급자를 추출하고 LDAP-UTF8 유니코드 문자열로 변환합니다. 예를 들면 다음과 같습니다.

- C=US,S=CA,O=IronPort
- C=US,CN=Bob Smith

X.509 인증서에는 발급자 필드가 필요하므로 signed-certificate(“issuer”)는 S/MIME 메시지에 X.509 인증서가 포함되었는지를 평가합니다.

정규식에서 이스케이프

LDAP-UTF8은 정규식에서 사용할 수 있는 이스케이프에 대한 메커니즘을 정의합니다. LDAP-UTF8의 문자 이스케이프에 대한 자세한 내용은 LDAP(Lightweight Directory Access Protocol) 및 String Representation of Distinguished Names(http://www.ietf.org/rfc/rfc4514.txt에서 액세스 가능)를 참고하십시오.

signed-certificate 규칙의 정규식에 대한 이스케이프 규칙은 이스케이프가 필요한 문자로만 이스케이프를 제한한다는 점에서 LDAP-UTF8에 정의된 이스케이프 규칙과 다릅니다. LDAP-UTF8은 이스케이프 없이 표현할 수 있는 문자에 대한 선택적인 이스케이프를 허용합니다. 예를 들어 LDAP-UTF8 이스케이프 규칙을 사용하면 다음 두 가지 문자열은 "Example, Inc."에 대해 올바른 것으로 간주됩니다.

- Example\, Inc.
- Example\,\ Inc\.

그러나 signed-certificate 규칙은 Example\, Inc.와만 일치합니다. 공백과 마침표는 이스케이프가 필요하지 않으므로(LDAP-UTF8에서는 허용되더라도) 정규식은 일치를 위한 이러한 문자의 이스케이프를 허용하지 않습니다. signed-certificate 규칙용 정규식을 만들 때에는 이스케이프 없이 표현할 수 있는 경우 문자를 이스케이프하지 마십시오.

$CertificateSigners 작업 변수

`$CertificateSigners` 작업 변수는 서명 인증서의 `subjectAltName` 요소에서 얻을 수 있는, 쉼표로 구분된 서명자 리스트입니다. 단일 서명자의 여러 이메일 주소는 중복이 제거된 상태로 리스트에 포함됩니다.

예를 들어 Alice가 두 개의 인증서로 메시지에 서명합니다. Bob이 단일 인증서로 메시지에 서명합니다. 단일 회사 기관에서 모든 인증서가 발급됩니다. 메시지가 S/MIME 검사를 통과하면 추출된 데이터에는 세 항목이 포함됩니다.

```
[
{
'issuer': 'CN=Auth,O=Example\, Inc.',
'signer': ['alice@example.com', 'al@private.example.com']
},
{
'issuer': 'CN=Auth,O=Example\, Inc.',
'signer': ['alice@example.com', 'al@private.example.com']
},
{
'issuer': 'CN=Auth,O=Example\, Inc.',
'signer': ['bob@example.com', 'bob@private.example.com']
}
]
```

`$CertificateSigners` 변수는 다음으로 확장됩니다.

```
"alice@example.com, al@private.example.com, bob@example.com, bob@private.example.com"
```

예 1

다음 예는 인증서 발급자가 미국에 있는 경우 새 헤더를 삽입합니다.

```
Issuer: if signed-certificate("issuer") == "(?i)C=US" {

insert-header("X-Test", "US issuer");

}
```

다음 예는 서명자가 example.com에서 오지 않은 경우 관리자에게 알립니다.

```
NotOurSigners: if signed-certificate("signer") AND

signed-certificate("signer") != "example\\.com$" {

notify("admin@example.com");

}
```

다음 예는 메시지에 X.509 인증서가 있는 경우 헤더를 추가합니다.

```
AnyX509: if signed-certificate ("issuer") {

insert-header("X-Test", "X.509 present");

}
```

다음 예는 메시지의 인증서에 서명자가 없는 경우 헤더를 추가합니다.

```
NoSigner: if not signed-certificate ("signer") {

insert-header("X-Test", "Old X.509?");

}
```

Header Repeats(헤더 반복) 규칙

특정 시점에 다음이 탐지되는 경우 Header Repeats(헤더 반복) 규칙이 true로 평가됩니다.

- 지난 1시간 동안 동일한 제목의 지정된 메시지 수가 탐지되는 경우
- 지난 1시간 동안 동일한 봉투 발신자로부터 지정된 메시지 수가 탐지되는 경우

대량의 이메일을 탐지하려면 이 규칙을 사용할 수 있습니다. 예를 들어 특정 웹사이트를 통한 정치 캠페인에서 조직으로 대량의 이메일을 전송할 수 있습니다. 안티스팸 엔진은 그러한 이메일을 깨끗한 것으로 취급하여 이메일의 전달을 중단하지 않습니다.

이 규칙의 구문은 header-repeats (<target>, <threshold> [, <direction>])입니다. 여기서

- <target>은 subject 또는 mail-from입니다. AsyncOS는 대상의 값이 반복되는 횟수를 계산합니다.
- <threshold>는 지정된 대상에 대해 동일한 값을 갖는 지난 1시간 동안 수신된 메시지의 수입니다. 이 값이 초과되면 규칙이 true로 평가됩니다.
- <direction>은 incoming, outgoing 또는 둘 모두입니다. 이 규칙에 direction이 지정되지 않은 경우 수신 또는 발신 메시지가 규칙 평가를 위해 계산됩니다.

Header Repeats(헤더 반복) 규칙이 true로 평가될 때마다 시스템 경고문이 전송됩니다. 시스템 경보, 971 페이지를 참조하십시오.

참고 헤더 필드에 쉼표나 세미콜론으로 구분된 값이 포함되어 있으면 규칙은 전체 문자열을 추적해야 한다고 간주합니다. 제목 헤더가 비어 있는 메시지는 무시됩니다.

Header Repeats(헤더 반복) 규칙은 최대 1분의 정밀도로 메시지의 이동 합계를 유지 관리합니다. 그 결과 설정된 임계값에 도달한 후 규칙이 트리거되기 전에 1분의 지연이 발생할 수 있습니다.

관련 주제

- Header Repeats(헤더 반복) 규칙을 다른 규칙과 함께 사용, 187 페이지
- 예, 187 페이지

Header Repeats(헤더 반복) 규칙을 다른 규칙과 함께 사용

AND 또는 OR 연산자를 이용해 Header Repeats(헤더 반복) 규칙을 다른 규칙과 함께 사용할 수 있습니다. 예를 들면 다음 필터를 사용하여 메시지 하위 집합의 화이트리스트를 작성할 수 있습니다.

```
F1: if (recv_listener == 'Gray')  AND (header-repeats('subject', X, 'incoming') { drop();}
```

AND 또는 OR 연산자를 이용해 Header Repeats(헤더 반복) 규칙을 다른 규칙과 함께 사용할 경우 Header Repeats(헤더 반복) 규칙은 필요한 경우에만 마지막에 평가됩니다. 특정 메시지에 대해 Header Repeats(헤더 반복) 규칙이 평가되지 않는 경우, 제공된 임계값과 비교하는 데 subject 또는 mail-from이 계산되지 않습니다.

Header Repeats(헤더 반복) 규칙은 필요한 경우에만 마지막에 평가되므로, OR 연산자를 이용해 다른 규칙과 함께 사용할 때 이 규칙의 동작이 달라질 수 있습니다. 다음 샘플 필터는 Signed 및 Header Repeats(헤더 반복) 규칙의 OR 조건을 사용합니다.

```
f1: if signed OR (header-repeats('subject', 10)) { drop();}
```

이 예에서 이 필터로 처리되는 처음 9개 메시지가 동일한 제목의 서명된 메시지인 경우 Header Repeats(헤더 반복) 규칙은 해당 메시지를 처리하지 않습니다. 10번째 메시지가 이전의 9개 메시지와 제목 헤더가 동일한 서명되지 않은 메시지인 경우, 임계값에 도달했더라도 필터는 구성된 작업을 수행하지 않습니다.

예

다음 예에서 필터가 특정 시점에 지난 1시간 동안 동일한 제목의 수신 메시지를 X개 이상 탐지한 경우 동일한 제목의 후속 메시지는 Policy(정책) 격리로 전송됩니다.

```
f1 : if header-repeats('subject', X, 'incoming') { quarantine('Policy');}
```

다음 예에서 필터가 특정 시점에 지난 1시간 동안 동일한 봉투 발신자의 발신 메시지를 X개 이상 탐지한 경우 동일한 봉투 발신자에게서 오는 후속 메시지는 삭제됩니다.

```
f2 :  if header-repeats('mail-from', X, 'outgoing') {drop();}
```

다음 예에서 필터가 특정 시점에 지난 1시간 동안 동일한 제목의 발신 메시지를 X개 이상 탐지한 경우 동일한 제목의 모든 후속 메시지에 대해 관리자에게 알림이 전송됩니다.

```
f3: if header-repeats('subject', X) {notify('admin@xyz.com');}
```

URL Reputation(URL 평판) 규칙

메시지에 있는 URL의 평판 점수를 기반으로 메시지 작업을 정의하려면 URL 평판 규칙을 사용합니다. 자세한 내용은 악의적이거나 바람직하지 않은 URL로부터 보호, 425 페이지의 URL 평판 또는 URL 범주 필터링: 조건 및 규칙 , 433 페이지 섹션을 참조하십시오.

이러한 규칙에서

- `msg_filter_name`: 이 메시지 필터의 이름입니다.
- `whitelist`는 정의된 URL 리스트의 이름입니다(urllistconfig 명령을 통해). 화이트리스트 지정은 선택 사항입니다.

평판 서비스 공급업체에서 점수를 제공할 때 작업을 수행하려면

`url-reputation` 규칙을 사용합니다.

url-reputation 규칙 사용 시 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:

하는 경우 url reputation('<min_score'>, <'max_score'>, '<whitelist>',
'<include_attachments>','<include_message_body_subject>')

{<action>}
```

여기서 각 항목은 다음을 나타냅니다.

- `min_score` 및 `max_score`는 작업을 적용해야 하는 범위의 최소 및 최대 점수입니다. 지정하는 값은 범위에 포함됩니다.

최소 및 최대 점수는 `-10.0`에서 `10.0` 사이여야 합니다.

- `include_attachments`는 메시지 첨부 파일에서 URL을 검사합니다. 값이 '1'이면 메시지 첨부 파일에 대한 URL 검사가 활성화되었음을 나타내며 값이 '0'이면 메시지 첨부 파일에 대한 URL 검사가 활성화되지 않았음을 나타냅니다.
- `include_message_body_subject`는 메시지 본문 및 제목에서 URL을 검사합니다. 값이 '1'이면 메시지 본문 및 제목에 대한 URL 검사가 활성화되었음을 나타내며 값이 '0'이면 메시지 본문 및 제목에 대한 URL 검사가 활성화되지 않았음을 나타냅니다.

평판 서비스 공급업체에서 점수를 제공하지 않을 때 작업을 수행하려면

`url-no-reputation` 규칙을 사용합니다.

`url-no-reputation` 규칙 사용 시 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:

if url_no_reputation('<whitelist>', '<include_attachments>','<include_message_body_subject>')
```

```
{<action>}
```

URL Category(URL 범주) 규칙

메시지에 있는 URL의 범주를 기반으로 메시지 작업을 정의하려면 URL 범주를 사용합니다. 자세한 내용은 악의적이거나 바람직하지 않은 URL로부터 보호, 425 페이지의 URL 평판 또는 URL 범주 필터링: 조건 및 규칙 , 433 페이지 섹션을 참조하십시오.

`url-category` 규칙 사용 시 필터 구문은 다음과 같습니다.

```
<msg_filter_name>: if url-category (['<category-name1>','<category-name2>',...,
'<category-name3>'],'<url_white_list>','<include_attachments>','<include_message_body_subject>')

<action>
```

여기서 각 항목은 다음을 나타냅니다.

- `msg_filter_name`은 이 메시지 필터의 이름입니다.
- `action`은 메시지 필터 작업입니다.
- `category-name`은 URL 범주입니다. 여러 범주는 쉼표로 구분합니다. 정확한 범주 이름을 사용하려면 콘텐츠 필터에서 URL Category 조건 또는 작업을 찾아보십시오. 범주의 설명과 예는 URL 범주 정보, 446 페이지 섹션을 참조하십시오.
- `url_white_list`는 정의된 URL 리스트의 이름입니다(urllistconfig 명령을 통해).
- `include_attachments`는 메시지 첨부 파일에서 URL을 검사합니다. 값이 '1'이면 메시지 첨부 파일에 대한 URL 검사가 활성화되었음을 나타내며 값이 '0'이면 메시지 첨부 파일에 대한 URL 검사가 활성화되지 않았음을 나타냅니다.
- `include_message_body_subject`는 메시지 본문 및 제목에서 URL을 검사합니다. 값이 '1'이면 메시지 본문 및 제목에 대한 URL 검사가 활성화되었음을 나타내며 값이 '0'이면 메시지 본문 및 제목에 대한 URL 검사가 활성화되지 않았음을 나타냅니다.

Corrupt Attachment(손상된 첨부 파일) 규칙

메시지에 손상된 첨부 파일이 있으면 Corrupt Attachment(손상된 첨부 파일) 규칙이 true로 평가됩니다. 손상된 첨부 파일이란 검사 엔진이 검사할 수 없어서 손상된 것으로 식별한 첨부 파일입니다.

관련 주제

- 예, 189 페이지

예

다음 예에서는 필터가 메시지에서 손상된 첨부 파일을 탐지하면 메시지가 Policy Quarantine(정책 격리)으로 격리됩니다.

```
quar_corrupt_attach: if (attachment-corrupt) { quarantine("Policy"); }
```

메시지 언어 규칙

메시지 언어에 따라 서로 다른 메시지 작업을 수행할 수 있습니다. 예를 들어, 다음과 같은 작업을 할 수 있습니다.

- 러시아어에 있는 메시지에 러시아어의 면책조항 추가
- 해당 언어를 확인할 수 없는 메시지 삭제

메시지 제목 및 본문의 언어에 따라 메시지 작업을 수행하려면 메시지 언어 규칙을 사용합니다.

참고 이 규칙은 첨부 파일과 헤더에서 언어를 확인하지 않습니다.

언어 탐지 작동 방식

Cisco Email Security Appliance는 메시지의 언어를 탐지하기 위해 기본 언어 탐지 엔진을 사용합니다. 이 어플라이언스는 제목 및 메시지 본문을 추출하여 언어 탐지 엔진에 전달합니다.

언어 탐지 엔진은 각 언어의 가능성을 추출된 텍스트로 확인하고 다시 어플라이언스에 전달합니다. 어플라이언스는 가능성이 가장 높은 언어를 메시지의 언어로 간주합니다. 어플라이언스는 다음 시나리오 중 하나에서 메시지의 언어를 '확인되지 않음'으로 간주합니다.

- 탐지된 언어를 Cisco Email Security Appliance에서 지원하지 않는 경우
- 어플라이언스에서 메시지의 언어를 탐지할 수 없는 경우
- 언어 탐지 엔진으로 전송된 추출된 텍스트의 총 크기가 50바이트 미만인 경우

메시지 필터 구문

```
< msg_filter_name >: if (message language < operator > "< language1 >, < language2 >,...,
< language n >") {< action >}
```

여기서 각 항목은 다음을 나타냅니다.

- `msg_filter_name`은 이 메시지 필터의 이름입니다.
- operator는 `==` 또는 `!=` 입니다.
- `language`는 이 메시지 필터에서 지정하려는 메시지 언어의 값입니다. 항목이 여러 개인 경우 쉼표로 구분하십시오. 지원되는 메시지 언어 및 값 목록은 콘텐츠 필터의 메시지 언어 조건을 참고하십시오. 값은 대괄호([및])로 묶여 있습니다.
- `action`은 메시지 필터 작업입니다.

예

다음 예에서는 해당 언어를 확인할 수 없는 메시지를 삭제하는 방법을 보여 줍니다.

```
DropMessagesWithUndeterminedLanguage: if (message-language == "unknown") { drop(); }
```

다음 예에서는 러시아어의 메시지에 러시아어의 면책조항을 추가하는 방법을 보여 줍니다.

```
ussianDisclaimerRule: if (message-language == "ru") { add-heading("RussianDisclaimer");
```

매크로 탐지 규칙

매크로 탐지 규칙을 사용하면 지정한 파일 유형에서 매크로가 활성화된 첨부 파일을 탐지할 수 있습니다.

참고 아카이브 또는 임베디드 파일에 매크로가 포함된 경우 메시지에서 상위 파일이 삭제됩니다.

매크로 탐지 구문

```
<msg_filter_name>: if (macro-detection-rule (['file_type-1', 'file_type-2',...
,'file_type-n'])) {<action>}
```

여기서 각 항목은 다음을 나타냅니다.

- `msg_filter_name`은 이 메시지 필터의 이름입니다.
- `file_type`은 다음과 같은 지원되는 파일 유형 중 하나일 수 있습니다.
  - `Adobe Portable Document Format`
  - `Microsoft Office 파일`
  - `OLE 파일 유형`
- `action`은 메시지 필터 작업입니다.

예

다음 예에서는 매크로 사용 Microsoft Office 첨부 파일이 포함된 메시지를 삭제하는 방법을 보여 줍니다.

```
Drop_Messages_With_Macro-enabled_Office_Files: if (macro-detection-rule (['Microsoft Office
Files'])) { drop(); }
```

다음 예에서는 PDF 형식의 매크로 사용 첨부 파일이 포함된 메시지가 특정 사용자에게 전송되는 경우 메시지가 삭제됩니다.

```
Strip_Macro_enabled_PDF: if (rcpt-to == "joe@example.com") {
drop-macro-enabled-attachments(['Adobe Portable Document Format']); }
```

위조 이메일 탐지 규칙

위조된 발신자 주소(From: 헤더)를 사용하여 사기 메시지를 탐지하고 그러한 메시지에 대해 작업을 수행할 수 있습니다.

위조 이메일 탐지 규칙을 사용하여 이러한 메시지를 탐지합니다. 이 규칙을 구성하는 동안 콘텐츠 사전 및 메시지를 잠재적으로 위조된 것으로 간주할 임계값(1~100)을 지정해야 합니다.

forged-email-detection 규칙은 From: 헤더를 콘텐츠 사전에 있는 사용자와 비교합니다. 이 과정에서 유사성에 따라 어플라이언스에서 사전에 있는 각 사용자의 유사성 점수를 할당합니다. 알림의 몇 가지 예는 다음과 같습니다.

- From: 헤더가 <j0hn.sim0ns@example.com>이고 콘텐츠 사전에 사용자 'John Simons'가 포함된 경우 어플라이언스에서 사용자에게 유사성 점수 82를 할당합니다.

- From: 헤더가 <john.simons@diff-example.com>이고 콘텐츠 사전에 사용자 'John Simons'가 포함된 경우 어플라이언스에서 사용자에게 유사성 점수 100을 할당합니다.

유사성 점수가 높을수록 메시지 위조 가능성이 높아집니다. 유사성 점수가 지정된 임계값보다 크거나 같은 경우, 필터 작업이 트리거됩니다.

자세한 내용은 위조 이메일 탐지, 610 페이지의 내용을 참고하십시오.

메시지 필터 구문

```
<filter_name>: if (forged-email-detection("<content_dictionary>", threshold)) {<action>;}
```

여기서 각 항목은 다음을 나타냅니다.

- filter_name은 메시지 필터의 이름입니다.
- content_dictionary는 콘텐츠 사전의 이름입니다.
- threshold는 메시지를 잠재적으로 위조된 것으로 간주할 임계값(1~100)입니다.

예

다음 메시지 필터는 메시지의 From: 헤더를 사전에 있는 용어와 비교하여 콘텐츠 사전에서 사용자의 유사성 점수가 70보다 크거나 같은 경우 From: 헤더를 제거하고 봉투 발신자로 대체합니다.

```
FED_CF: if (forged-email-detection("Execs", 70)) { fed("from", ""); }
```

중복 경계 확인 규칙

duplicate_boundaries 규칙을 사용하여 중복 MIME 경계가 포함된 메시지를 탐지할 수 있습니다.

참고 첨부 파일 기반 규칙(예: attachment-contains) 또는 작업(예: drop-attachments-where-contains)은 형식이 잘못된 메시지(중복 MIME 경계가 있는 메시지)에서 작동하지 않습니다.

메시지 필터 구문

```
<filter_name>: if (duplicate_boundaries){<action>;}
```

예

다음 메시지 필터는 중복 MIME 경계가 포함된 모든 메시지를 격리합니다.

```
DuplicateBoundaries: if (duplicate_boundaries) { quarantine("Policy"); }
```

잘못된 형식의 **MIME** 헤더 탐지 규칙

malformed-header 규칙을 사용하여 잘못된 형식의 MIME 헤더가 포함된 메시지를 탐지할 수 있습니다.

메시지 필터 구문

```
<filter_name>: if (malformed-header){<action>;}
```

예

다음 예에서는 잘못된 형식의 MIME 헤더가 포함된 모든 메시지를 격리하는 방법을 보여 줍니다.

```
quarantine_malformed_headers: if (malformed-header)
{
quarantine("Policy");
}
```

지리위치 규칙

지리 위치 규칙을 사용하여 선택한 특정 국가에서 수신 메시지를 처리할 수 있습니다.

지리위치 구문

```
<msg_filter_name>: if (geolocation-rule (['country_name-1', 'country_name-2',...
,'country_name-n'])) {<action>}
```

여기서 각 항목은 다음을 나타냅니다.

- `msg_filter_name`은 이 메시지 필터의 이름입니다.
- `country_name`은 선택한 국가의 이름일 수 있습니다.
- `action`은 메시지 필터 작업입니다.

예

다음 예에서는 Country1 및 Country2에서 수신되는 메시지를 격리하는 방법을 보여 줍니다.

```
Quarantine_Incoming_Messages_from_Country1_and_Country2: if (geolocation-rule
(['Country1', 'Country2'])) {quarantine("Policy");}
```

ETF에 대한 도메인 평판 규칙

예를 들어, 다음 메시지 필터 규칙 구문을 사용하여 ETF 엔진을 통해 메시지에서 악성 도메인을 탐지하고 해당 메시지에 대해 적절한 조치를 취할 수 있습니다.

구문:

```
quarantine_msg_based_on_ETF: if (domain-external-threat-feeds (['etf_source1'],
 ['mail-from', 'from'], <'domain_exception_list'>)) { quarantine("Policy"); }
```

어디에서

- '`domain-external-threat-feeds`'는 도메인 평판 메시지 필터 규칙입니다.
- '`etf_source1`'은 메시지 헤더에서 악성 도메인을 탐지하는 데 사용되는 ETF 소스입니다.
- '`mail-from`','`from`'은 도메인의 평판을 확인하는 데 사용되는 필수 헤더입니다.

- 'domain_exception_list'는 도메인 예외 목록의 이름입니다. 도메인 예외 목록이 없으면 ""로 표시됩니다.

예

다음 예에서는 'Errors To:' 맞춤형 헤더의 도메인이 ETF 엔진에서 악성으로 탐지된 경우 메시지가 격리됩니다.

```
Quaranting_Messages_with_Malicious_Domains: if domain-external-threat-feeds
(['threat_feed_source'], ['Errors-To'], "")) {quarantine("Policy");}
```

SDR에 대한 도메인 평판 규칙

도메인 평판 규칙을 사용하여 SDR을 기준으로 메시지를 필터링하고 해당 메시지에 대해 적절한 조치를 취할 수 있습니다.

- 발신자 도메인 판정
- 발신자 도메인 기간
- 발신인 도메인 평판 검사 불가

발신자 도메인 판정을 기준으로 메시지 필터링

참고 권장되는 차단 임계값은 "Poor"입니다. SDR에 대한 자세한 내용은 Cisco Talos(https://www.talosintelligence.com)에 문의하십시오.

구문:

```
drop_msg_based_on_sdr_verdict:
if sdr-reputation (['awful', 'poor'], "<domain_exception_list>")
{drop();}
```

여기서:

- 'drop_msg_based_on_sdr_verdict'은 메시지 필터의 이름입니다.
- 'sdr-reputation'은 도메인 평판 메시지 필터 규칙입니다.
- 'awful','poor'는 SDR을 기준으로 메시지를 필터링하는 데 사용되는 발신자 도메인 판정의 범위입니다.
- 'domain_exception_list'는 도메인 예외 목록의 이름입니다. 도메인 예외 목록이 없으면 ""로 표시됩니다.
- 'drop'은 메시지에 적용된 작업입니다.

예

다음 메시지에서 SDR 판정이 'Unknownr'이면 메시지가 격리됩니다.

```
quarantine_unknown_sdr_verdicts:
if sdr-reputation (['unknown'], "")
{quarantine("Policy")}
```

발신자 도메인 기간을 기준으로 메시지 필터링

구문:

```
<msg_filter_name>
if sdr-age (<‘unit'>, <‘operator'> <‘actual value’>)
{<action>}
```

여기서:

- `'sdr-reputation'`은 도메인 평판 메시지 필터 규칙입니다.
- `'sdr_age'`는 SDR을 기준으로 메시지를 필터링하는 데 사용되는 발신자 도메인 기간입니다.
- ‘`unit'`은 발신자 도메인 기간을 기준으로 메시지를 필터링하는 데 사용되는 'days', 'years', 'months' 또는 'weeks' 수 옵션입니다.
- `'operator'`는 발신자 도메인 기간을 기준으로 메시지를 필터링하는 데 사용되는 다음 비교 연산자입니다.
  - – >(보다 큼)
  - – >=(보다 크거나 같음)
  - – <(보다 작음)
  - – <=(보다 작거나 같음)
  - – ==(같음)
  - – !=(같지 않음)
  - – Unknown(알 수 없음)
- ‘`actual value'`는 발신자 도메인 기간을 기준으로 메시지를 필터링하는 데 사용되는 번호입니다.

예

다음 메시지에서 발신자 도메인의 기간을 알 수 없는 경우 메시지가 삭제됩니다.

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("unknown", "")) {drop();}
```

다음 메시지에서 발신자 도메인의 기간이 한 달 미만이면 메시지가 삭제됩니다.

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("months", <, 1, "")) { drop(); }
```

발신자 도메인 스캔 불가를 기준으로 메시지 필터링

구문:

```
<msg_filter_name>
if sdr-unscannable (<'domain_exception_list'>)
{<action>}
```

여기서:

- `'sdr-unscannable'`은 도메인 평판 메시지 필터 규칙입니다.

`'domain_exception_list'`는 도메인 예외 목록의 이름입니다. 도메인 예외 목록이 없으면 ""로 표시됩니다.

예

다음 메시지에서 SDR 판정이 'Unknown'이면 메시지가 격리됩니다.

```
Quarantine_Messages_Based_On_Sender_Domain_Unscannable: if (sdr-unscannable (""))
{quarantine("Policy");}
```

메시지 필터 작업

메시지 필터의 목적은 선택한 메시지에 작업을 수행하는 것입니다.

작업에는 다음의 2가지 유형이 있습니다.

- 최종 작업(전달, 삭제 및 바운스)은 메시지 처리를 종료하고 다음 필터를 통한 추가 처리를 허용하지 않습니다.
- 최종 작업 이외의 작업은 메시지가 추가 처리되도록 허용합니다.

참고 최종 작업 이외의 메시지 필터 작업은 누적됩니다. 필터마다 다른 작업을 지정하는 여러 필터와 메시지가 일치하는 경우 모든 작업이 누적되어 적용됩니다. 그러나 동일한 작업을 지정하는 여러 필터와 메시지가 일치하는 경우, 이전 작업이 재정의되고 최종 필터 작업이 적용됩니다.

관련 주제

- 필터 작업 요약 표, 196 페이지
- 작업 변수, 206 페이지
- 일치 콘텐츠 가시성, 208 페이지
- 메시지 필터 작업의 설명 및 예, 209 페이지

필터 작업 요약 표

메시지 필터는 아래 표와 같이 다음 작업을 이메일 메시지에 적용할 수 있습니다.

표 ***23:*** 메시지 필터 작업

작업	**Syntax**	설명
소스 호스트 변경	alt-src-host	메시지 전송을 위한 소스 호스트 이름과 IP 인터페이스(가상 게이트웨이 주소)를 변경합니다. 소스 호스트(가상 게이트웨이 주소) 변경 작업, 218 페이지를 참조하십시오.

작업	**Syntax**	설명
수신자 변경	alt-rcpt-to	메시지의 수신자를 변경합니다. 수신자 변경 작업, 217 페이지를 참조하십시오.
메일호스트 변경	alt-mailhost	메시지에 대한 대상 메일 호스트를 변경합니다. 전달 호스트 변경 작업, 217 페이지를 참조하십시오.
Notify	notify	이 메시지를 또 다른 수신자에게 보고합니다. 알림 및 알림 복사 작업, 212 페이지를 참조하십시오.
복사 알림	notify-copy	notify와 유사한 작업을 수행하지만, bcc-scan 작업처럼 복사본을 전송합니다. 알림 및 알림 복사 작업, 212 페이지를 참조하십시오.
숨은 참조	bcc	또 다른 수신자에게 익명으로 이 메시지를 복사합니다(메시지 복제). 숨은 참조 작업, 214 페이지의 내용을 참조하십시오.
검사와 함께 숨은 참조	bcc-scan	또 다른 수신자에게 익명으로 이 메시지를 복사하고, 마치 새 메시지인 것처럼 작업 대기열을 통해 처리합니다. 숨은 참조 작업, 214 페이지를 참조하십시오.
보관	archive	이 메시지를 mbox 형식의 파일로 보관합니다. 아카이브 작업, 219 페이지를 참조하십시오.
격리	`quarantine (quarantine_name`	*quarantine_name*이라는 격리로 전송되도록 이 메시지에 플래그를 지정합니다. 격리 및 복제 작업, 216 페이지를 참조하십시오.
복제(격리)	`duplicate-quarantine (quarantine_name`	지정된 격리로 메시지 복사본을 전송합니다. 격리 및 복제 작업, 216 페이지를 참조하십시오.
헤더 제거	strip-header	전달 전에 메시지에서 지정된 헤더를 제거합니다. 헤더 제거 작업, 219 페이지를 참조하십시오.
헤더 삽입	insert-header	전달 전에 메시지에 헤더 및 값 쌍을 삽입합니다. 헤더 삽입 작업 , 220 페이지를 참조하십시오.

작업	**Syntax**	설명
헤더 텍스트 수정	edit-header-text	지정된 헤더 텍스트를 필터 조건에서 지정한 텍스트 문자열로 교체합니다. 헤더 텍스트 수정 작업, 221 페이지를 참조하십시오.
본문 텍스트 수정	edit-body-text()	메시지 본문에서 정규식을 분리한 후 지정한 텍스트로 교체합니다. 메시지 본문 내 URL과 같은 특정 내용을 제거 및 교체하려는 경우 이 필터를 사용할 수 있습니다. 본문 텍스트 수정 작업, 221 페이지를 참조하십시오.
HTML 변환	html-convert()	메시지 본문에서 HTML 태그를 제거하고 메시지의 일반 텍스트 내용을 남겨둡니다. 메시지에서 모든 HTML 텍스트를 일반 텍스트로 변환하려는 경우에도 이 필터를 사용할 수 있습니다. HTML 변환 작업, 222 페이지.
반송 프로필 할당	bounce-profile	메시지에 특정 반송 프로필을 할당합니다. 반송 프로필 작업, 222 페이지를 참조하십시오.
안티스팸 시스템 우회	skip-spamcheck	Cisco 시스템의 안티스팸 시스템이 이 메시지에 적용되지 않도록 합니다. 안티스팸 시스템 우회 작업, 223 페이지를 참조하십시오.
그레이메일 작업 우회	skip-marketingcheck	마케팅 이메일에서 작업을 우회합니다. 그레이메일 우회 작업, 223 페이지를 참조하십시오.
	skip-socialcheck	소셜 네트워크 이메일에서 작업을 우회합니다. 그레이메일 우회 작업, 223 페이지를 참조하십시오.
	skip-bulkcheck	대량 이메일에서 작업을 우회합니다. 그레이메일 우회 작업, 223 페이지를 참조하십시오.
안티바이러스 시스템 우회	`skip-viruscheck`	Cisco 시스템의 안티바이러스 시스템이 이 메시지에 적용되지 않도록 합니다. 안티바이러스 시스템 우회 작업, 224 페이지를 참조하십시오.

작업	**Syntax**	설명
파일 평판 필터링 및 파일 분석 우회	`skip-ampcheck`	파일 평판 필터링 및 파일 분석이 이 메시지에 적용되지 않도록 합니다. 파일 평판 필터링 및 파일 분석 시스템 우회 작업, 224 페이지를 참조하십시오.
Outbreak Filter 검사 건너뛰기	`skip-vofcheck`	이 메시지가 Outbreak Filter 검사로 처리되지 않도록 합니다. 안티바이러스 시스템 우회 작업, 224 페이지를 참조하십시오.
이름으로 첨부 파일 삭제	`drop-attachments-by-name`	지정된 정규식과 일치하는 파일 이름을 가지고 있는 메시지의 모든 첨부 파일을 삭제합니다. 아카이브 파일 첨부 파일(zip, tar), Microsoft Office 첨부 파일(doc, .docx) 및 이메일 첨부 파일(winmail.dat)은 일치하는 파일이 포함된 경우 삭제됩니다. 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.
유형으로 첨부 파일 삭제	`drop-attachments-by-type`	특정 MIME 유형(지정된 MIME 유형 또는 파일 확장명으로 판단)을 가지고 있는 메시지의 모든 첨부 파일을 삭제합니다. 일치하는 파일이 포함된 경우 아카이브 첨부 파일(zip, tar)을 삭제합니다. 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.
파일 형식으로 첨부 파일 삭제	`drop-attachments-by-filetype`	파일의 지정된 "지문"과 일치하는 메시지의 모든 첨부 파일을 삭제합니다. 일치하는 파일이 포함된 경우 아카이브 첨부 파일(zip, tar)을 삭제합니다. 자세한 내용은 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참고하십시오.
MIME 유형으로 첨부 파일 삭제	`drop-attachments-by-mimetype`	지정된 MIME 유형을 가지고 있는 메시지의 모든 첨부 파일을 삭제합니다. 이 작업은 파일 확장명으로 MIME 유형을 확정하려고 하지 않으며 아카이브의 내용을 검토하지도 않습니다. 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.

작업	**Syntax**	설명
크기로 첨부 파일 삭제	`drop-attachments-by-size`	원시 인코딩 형식으로, 지정된 크기(바이트 단위)보다 크거나 같은 메시지의 모든 첨부 파일을 삭제합니다. 아카이브 또는 압축된 파일의 경우, 이 작업은 압축 해제된 크기를 검사하지 않고 디코딩 전 실제 첨부 파일의 크기를 검사합니다. 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.
내용으로 첨부 파일 삭제	`drop-attachments-where-contains`	정규식을 포함하는 메시지의 모든 첨부 파일을 삭제합니다. 패턴이 임계값에 대해 지정한 최소 횟수만큼 발생합니까? 포함된 파일 중에 정규식 패턴이 있는 경우 아카이브 파일(zip, tar)을 삭제합니다. 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오. 선택적인 코멘트는 삭제된 첨부 파일 대신 사용되는 텍스트를 수정하기 위한 수단입니다. 첨부 파일 바닥글이 메시지에 추가됩니다.

작업	**Syntax**	설명
매크로가 포함된 첨부 파일 삭제	`drop-macro-enabled-attachments`	지정된 파일 형식의 매크로가 활성화된 모든 첨부 파일을 삭제합니다. 참고 아카이브 또는 임베디드 파일에 매크로가 포함된 경우 메시지에서 상위 파일이 삭제됩니다. **Syntax** `drop-macro-enabled-attachments (['file_type-1', 'file_type-2', …,'file_type-n'], "custom_replacement_message")` 여기서 각 항목은 다음을 나타냅니다. • `file_type`은 다음과 같은 지원되는 파일 유형 중 하나일 수 있습니다. • `Adobe Portable Document Format` • `Microsoft Office 파일` • `OLE 파일 유형` • 맞춤형 대체 메시지는 첨부 파일이 삭제될 때 메시지 본문의 하단에 추가되는 기본 시스템 생성 메시지를 대체하는 선택적 메시지입니다. 매크로 탐지 규칙, 190 페이지를 참조하십시오.
사전 일치로 첨부 파일 삭제	`drop-attachments-where-dictionary-match`	사전 용어에 대한 일치를 기반으로 첨부 파일을 제거합니다. 첨부 파일로 간주되는 MIME 부분의 용어가 사전 용어와 일치하면(그리고 사용자 정의 임계값이 충족되면) 이메일에서 첨부 파일이 제거됩니다. 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.
바닥글 추가	`add-footer(footer-name)`	메시지에 면책조항 텍스트를 바닥글로 추가합니다. 자세한 내용은 "텍스트 리소스" 장의 "메시지 면책조항 스탬프" 섹션을 참조하십시오.

작업	**Syntax**	설명
머리글 추가	`add-heading(heading-name)`	메시지에 면책조항 텍스트를 머리글로 추가합니다. 자세한 내용은 "텍스트 리소스" 장의 "메시지 면책조항 스탬프" 섹션을 참조하십시오.
전달 시 암호화	`encrypt-deferred`	전달 시 메시지를 암호화합니다. 즉, 메시지가 다음 처리 단계로 진행되며 모든 처리가 완료되면 메시지가 암호화되어 전달됩니다.
전달 시 S/MIME 서명/암호화	`smime-gateway-deferred ("sending_profile")`	전달 중 지정된 전송 프로필을 사용하여 메시지의 S/MIME 서명 또는 암호화를 수행합니다. 전달 시 S/MIME 서명 또는 암호화 작업, 211 페이지를 참조하십시오.
S/MIME 서명/암호화	`smime-gateway("sending_profile")`	지정된 전송 프로필을 사용하여 S/MIME 서명 또는 암호화를 수행하고 메시지를 전달하며, 추가 처리를 건너뜁니다. S/MIME 서명 또는 암호화 작업, 212 페이지를 참조하십시오.
메시지 태그 추가	`tag-message(tag-name)`	정책 필터링과 함께 사용할 수 있도록 메시지에 맞춤형 용어를 추가합니다. 메시지 태그가 있는 메시지로 검사를 제한하도록 DLP 정책을 구성할 수 있습니다. 메시지 태그는 수신자에게 보이지 않습니다. 메시지 태그 추가 작업, 225 페이지 및 "데이터 손실 방지" 장을 참조하십시오.
Add Log Entry	`log-entry`	INFO 수준에서 텍스트 메일 로그에 맞춤화 텍스트를 추가합니다. 텍스트는 작업 변수를 포함할 수 있습니다. 메시지 추적에 로그 항목이 나타납니다. 로그 항목 추가 작업, 225 페이지를 참조하십시오.

작업	**Syntax**	설명
URL 평판을 기반으로 URL을 텍스트와 교체	• `url-reputation-replace` • `url-no-reputation-replace`	URL의 평판을 기반으로 URL 또는 URL의 동작을 수정합니다. 평판 서비스에서 URL에 대한 점수를 제공하지 않는 경우에는 별도의 작업을 사용합니다. URL 평판 작업 , 226 페이지를 참조하십시오.
URL 평판을 기반으로 URL Defang	• `url-reputation-defang` • `url-no-reputation-defang`	
URL 평판을 기반으로 URL을 Cisco 보안 프록시로 리디렉션	• `url-reputation-proxy-redirect` • `url-no-reputation-proxy-redirect`	
URL 범주를 기반으로 URL을 텍스트로 교체	`url-category-replace`	URL의 범주를 기반으로 URL 또는 URL의 동작을 수정합니다. URL 범주 작업 , 228 페이지를 참조하십시오.
URL 범주를 기반으로 URL Defang	`url-category-defang`	
URL 범주를 기반으로 URL을 Cisco 보안 프록시로 리디렉션	`url-category-proxy-redirect`	
위조 이메일 탐지	`fed`	위조 메시지에서 발신인: 헤더를 제거하고 봉투 발신자로 대체합니다. 위조 이메일 탐지 작업, 229 페이지를 참조하십시오.
운영 없음	`no-op`	작업이 수행되지 않습니다. 운영 없음, 229 페이지를 참조하십시오.
*나머지 메시지 필터 건너뛰기	`skip-filters`	이 메시지가 다른 메시지 필터로 처리되지 않고 이메일 파이프라인을 계속 통과하도록 합니다. 나머지 메시지 필터 건너뛰기 작업, 210 페이지를 참조하십시오.
*메시지 삭제	`drop`	메시지를 삭제합니다. 삭제 작업, 210 페이지를 참조하십시오.
*메시지 반송	`bounce`	메시지를 발신자에게 다시 보냅니다. 반송 작업, 211 페이지를 참조하십시오.
*지금 암호화 및 전달	`encrypt`	Cisco 이메일 암호화를 사용하여 발신 메시지를 암호화합니다. 암호화 작업, 211 페이지를 참조하십시오.

작업	**Syntax**	설명
*최종 작업		

관련 주제

- 첨부 파일 그룹, 204 페이지

첨부 파일 그룹

`attachment-filetype` 및 `drop-attachments-by-filetype rules`에서 특별한 파일 형식(예: "exe" 파일) 또는 일반적인 첨부 파일 그룹을 지정할 수 있습니다. AsyncOS는 첨부 파일을 다음 표에 나열된 그룹으로 나눕니다.

특정 파일 형식의 첨부 파일이 포함되지 않은 메시지를 확인하기 위해 `!=` 연산자를 사용하는 메시지 필터를 만드는 경우, 필터링하려는 파일 형식의 첨부 파일이 하나라도 있으면 필터는 해당 메시지에 대해 작업을 수행하지 않습니다. 예를 들어 다음 필터는 **`.exe`** 파일 형식이 아닌 첨부 파일이 포함된 메시지를 삭제합니다.

```
exe_check: if (attachment-filetype != "exe") {

drop();

}
```

한 메시지에 여러 첨부 파일이 있는 경우 첨부 파일 중 적어도 하나가 .exe 파일이면 나머지 첨부 파일이 `.exe` 파일이 아니더라도 Email Security Appliance는 메시지를 삭제하지 않습니다.

표 ***24:*** 첨부 파일 그룹

첨부 파일 그룹 이름	검사되는 파일 형식
문서	• doc • docx • mdb • mpp • ole • pdf • ppt • pptx • rtf • wps • x-wmf • xls • xlsx

첨부 파일 그룹 이름	검사되는 파일 형식
실행 파일	• exe • java • msi • pif 참고 필터링 및 실행 파일 그룹은 .dll 및 .scr 파일도 검사하지만 이러한 파일 형식을 개별적으로 필터링할 수는 없습니다.
압축됨	• ace (ACE Archiver compressed file) • arc (SQUASH Compressed archive) • arj (Robert Jung ARJ compressed archive) • binhex • bz (Bzip compressed file) • bz2 (Bzip compressed file) • cab (Microsoft cabinet file) • gzip* (Compressed file - UNIX gzip) • lha (Compressed Archive [LHA/LHARC/LZH]) • rar (Compressed archive • sit (Compressed archive - Macintosh file [Stuffit]) • tar* (Compressed archive) • unix (UNIX compress file) • zip* (Compressed archive - Windows) • zoo (ZOO Compressed Archive File) * 이러한 파일 형식은 "body-scanned"일 수 있습니다.
텍스트	• txt • html • xml
이미지	• bmp • cur • gif • ico • jpeg • pcx • png • psd • psp • tga • tiff

첨부 파일 그룹 이름	검사되는 파일 형식
미디어	• aac • aiff • asf • avi • flash • midi • mov • mp3 • mpeg • ogg • ram • snd • wav • wma • wmv

작업 변수

bcc(), bcc-scan(), notify(), notify-copy(), add-footer(), add-heading() 및 insert-headers() 작업에는 파라미터가 있는데, 이러한 파라미터는 작업이 실행될 때 원본 메시지의 정보를 자동으로 교체할 특정 변수를 사용할 수 있습니다. 이러한 변수를 작업 변수라고 합니다. Cisco 어플라이언스는 다음과 같은 작업 변수를 지원합니다.

표 ***25:*** 메시지 필터 작업 변수

변수	**Syntax**	설명
모든 헤더	`$AllHeaders`	메시지 헤더를 반환합니다.
Body Size(본문 크기)	`$BodySize`	메시지의 크기를 바이트 단위로 반환합니다.
Certificate Signers(인증서 서명자)	`$CertificateSigners`	서명 인증서의 subjectAltName 요소로부터 서명자를 반환합니다. 자세한 내용은 $CertificateSigners 작업 변수, 185 페이지 항목을 참조하십시오.
날짜	`$Date`	MM/DD/YYYY 형식을 사용하여 현재 날짜를 반환합니다.
삭제된 파일 이름	`$dropped_filename`	가장 최근에 삭제된 파일 이름을 하나만 반환합니다.
Dropped File Names(삭제된 파일 이름)	`$dropped_filenames`	삭제된 파일 목록을 표시합니다($filenames와 유사).

변수	**Syntax**	설명
Dropped File Types(삭제된 파일 형식)	`$dropped_filetypes`	삭제된 파일 유형의 목록을 표시합니다($filetypes와 유사).
Envelope Sender(봉투 발신자)	`$EnvelopeFrom`	메시지의 Envelope Sender(Envelope From, <MAIL FROM>)를 반환합니다.
Envelope Recipients(봉투 수신자)	`$EnvelopeRecipients`	메시지의 모든 Envelope Recipient(Envelope To, <RCPT TO>)를 반환합니다.
파일 이름	`$filenames`	메시지 첨부 파일 이름의 쉼표로 구분된 리스트를 반환합니다.
File Sizes(파일 크기)	`$filesizes`	메시지 첨부 파일 크기의 쉼표로 구분된 리스트를 반환합니다.
파일 형식	`$filetypes`	메시지 첨부 파일 형식의 쉼표로 구분된 리스트를 반환합니다.
필터 이름	`$FilterName`	처리 중인 필터의 이름을 반환합니다.
GMTimeStamp	`$GMTimeStamp`	이메일 메시지의 Received: 줄에 나오는 대로 GMT를 사용하여 현재 시간 및 날짜를 반환합니다.
HAT 그룹 이름	`$Group`	메시지 주입 시 발신자 일치가 확인되는 발신자 그룹의 이름을 반환합니다. 그룹에 이름이 없으면 ">Unknown<" 문자열이 삽입됩니다.
일치하는 컨텐트	`$MatchedContent`	검사 필터 규칙을 트리거한 콘텐츠를 반환합니다(body-contains 및 콘텐츠 사전 같은 필터 규칙 포함).
메일 흐름 정책	`$Policy`	메시지 주입 시 발신자에게 적용되는 HAT 정책의 이름을 반환합니다. 사전 정의된 정책 이름이 사용되지 않으면 ">Unknown<" 문자열이 삽입됩니다.
헤더	`$Header['`*`string`*`']`	원본 메시지에 일치하는 헤더가 포함된 경우 인용된 헤더의 값을 반환합니다. 큰따옴표를 사용할 수도 있습니다.
호스트 이름	`$Hostname`	Cisco 어플라이언스의 호스트 이름을 반환합니다.
내부 메시지 ID	`$MID`	메시지 식별을 위해 내부적으로 사용되는 MID(Message ID)를 반환합니다. 검색에 $Header가 사용되는 RFC822 "Message-Id" 값과 혼동해서는 안 됩니다.
수신 리스너	`$RecvListener`	메시지를 수신한 리스너의 별칭으로 교체됩니다.

변수	Syntax	설명
수신 인터페이스	`$RecvInt`	메시지를 수신한 인터페이스의 별칭을 반환합니다.
원격 IP 주소	`$RemoteIP`	Cisco 어플라이언스로 메시지를 전송한 시스템의 IP 주소를 반환합니다.
원격 호스트 주소	`$remotehost`	Cisco 어플라이언스로 메시지를 전송한 시스템의 호스트 이름을 반환합니다.
SenderBase Reputation 점수	`$Reputation`	발신자의 SenderBase Reputation 점수를 반환합니다. 평판 점수가 없으면 "None"으로 교체됩니다.
제목	`$Subject`	메시지의 제목을 반환합니다.
시간	`$Time`	로컬 표준 시간대에서 현재 시간을 반환합니다.
타임스탬프	`$Timestamp`	이메일 메시지의 Received: 줄에 나오는 대로 로컬 표준 시간대를 사용하여 현재 시간 및 날짜를 반환합니다.

관련 주제

- 비 ASCII 문자 집합 및 메시지 필터 작업 변수, 208 페이지

비 ASCII 문자 집합 및 메시지 필터 작업 변수

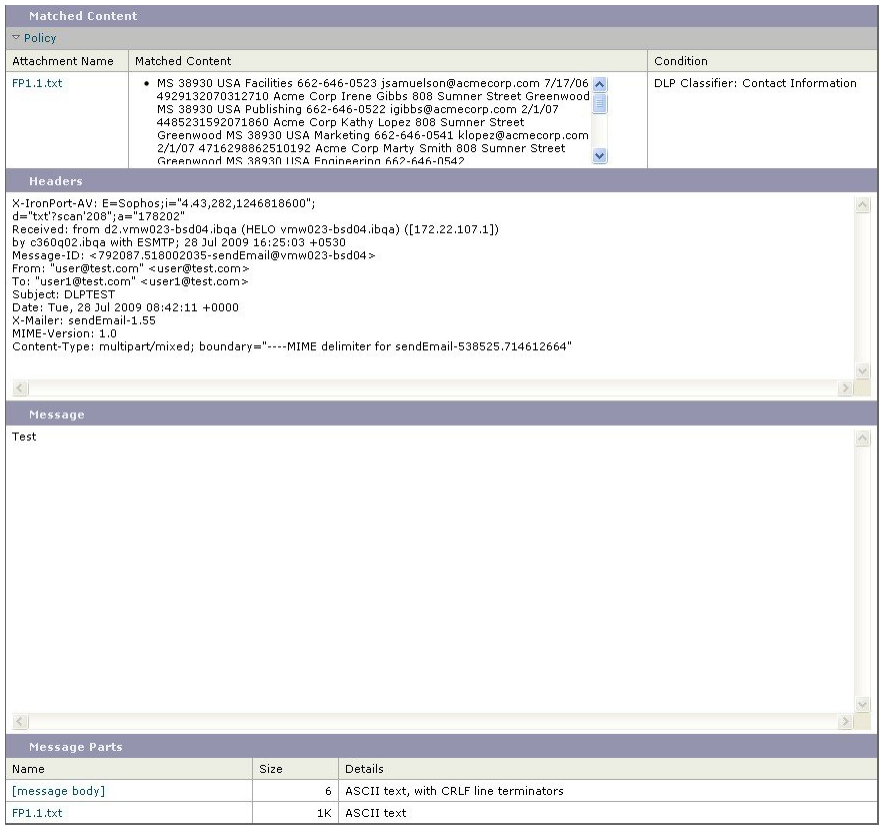
시스템은 ISO-2022 스타일 문자 코딩(헤더 값에 사용된 인코딩 스타일)을 포함하는 작업 변수의 확장을 지원하며, 알림에서 국제 텍스트도 지원합니다. 이들이 병합되어 알림을 생성하며, 이 알림은 UTF-8, QP(quoted printable) 메시지로 전송됩니다.

일치 콘텐츠 가시성

Attachment Content(첨부 파일 내용) 조건, Message Body or Attachment(메시지 본문 또는 첨부 파일) 조건, Message Body(메시지 본문) 조건, Attachment Content(첨부 파일 내용) 조건을 구성할 때 격리된 메시지에서 일치 콘텐츠를 볼 수 있습니다. 메시지 본문을 표시하면 일치 콘텐츠가 노란색으로 강조 표시됩니다. 메시지 제목의 일치 콘텐츠를 포함하려면 $MatchedContent 작업 변수를 사용할 수도 있습니다.

메시지 또는 콘텐츠 필터 규칙을 트리거한 로컬 격리에 있는 메시지를 볼 때, 실제로 필터 작업을 트리거하지 않은 내용이 필터 작업을 트리거한 내용과 함께 GUI에 표시될 수 있습니다. GUI 표시는 콘텐츠 일치를 찾기 위한 지침으로 사용해야 하지만, 콘텐츠 일치의 정확한 리스트를 반영하는 것은 아닙니다. 이런 일이 발생하는 이유는 GUI가 필터에 사용되는 것보다 덜 엄격한 콘텐츠 일치 논리를 사용하기 때문입니다. 이 문제는 메시지 본문의 강조 표시 부분에만 적용됩니다. 메시지 각 부분의 일치하는 문자열을 관련 필터 규칙과 함께 나열하는 테이블이 정확합니다.

그림 ***17:*** 정책 격리에 표시되는 일치 콘텐츠



메시지 필터 작업의 설명 및 예

다음 섹션에서는 사용 중인 다양한 메시지 필터 작업을 설명하고 해당 예를 보여줍니다.

나머지 메시지 필터 건너뛰기 작업

`skip-filters` 작업은 메시지가 메시지 필터의 추가 처리를 건너뛰고 이메일 파이프라인을 계속 통과하도록 합니다. `skip-filters` 작업을 일으키는 메시지는 안티스팸 검사 및 안티바이러스 검사(어플라이언스에서 사용 가능한 경우)를 거치게 됩니다. `skip-filters` 작업은 메시지 필터의 기본 최종 작업입니다.

다음 필터는 `customercare@example.com`에 알림을 보내고 `boss@admin`으로 주소가 지정된 메시지를 즉시 전달합니다.

```
bossFilter:

if(rcpt-to == 'boss@admin$')

{

notify('customercare@example.com');

skip-filters();

}
```

삭제 작업

`drop` 작업은 전달하지 않고 메시지를 삭제합니다. 메시지는 발신자에게 반환되지 않고, 원래 수신자에게 전송되지 않으며, 달리 추가로 처리되지도 않습니다.

다음 필터는 먼저 `george@whitehouse.gov`에 알림을 보낸 다음 제목이 `SPAM`으로 시작되는 메시지를 삭제합니다.

```
spamFilter:

if(subject == '^SPAM.*')

{
```

```
notify('george@whitehouse.gov');
drop();
}
```

반송 작업

bounce 작업은 추가 처리 없이 메시지를 발신자(Envelope Sender)에게 돌려보냅니다.

다음 필터는 @yahoo\\.com으로 끝나는 이메일 주소의 메시지를 반환(반송)합니다.

```
yahooFilter:
if(mail-from == '@yahoo\\.com$')
{
bounce();
}
```

암호화 작업

encrypt 작업은 구성된 암호화 프로파일을 사용하여 암호화된 메시지를 이메일 수신자에게 전달합니다.

다음 필터는 메시지 제목에 [encrypt] 용어가 포함된 경우 메시지를 암호화합니다.

```
Encrypt_Filter:
if ( subject == '\\[encrypt\\]' )
{
encrypt('My_Encryption_Profile');
}
```

참고 이 필터 작업을 사용하려면 네트워크에 Cisco 암호화 어플라이언스가 있거나 호스팅 키 서비스가 구성되어 있어야 합니다. 또한 이 필터 작업을 사용하려면 암호화 프로필이 구성되어 있어야 합니다.

전달 시 **S/MIME** 서명 또는 암호화 작업

smime-gateway-deferred 작업은 전달 중 지정된 전송 프로필을 사용하여 메시지의 S/MIME 서명 또는 암호화를 수행합니다. 즉, 메시지가 다음 처리 단계로 진행되며 모든 처리가 완료되면 메시지가 서명되거나 암호화되어 전달됩니다.

다음 필터는 전달 중 특정 발신자의 모든 발신 메시지에 대해 S/MIME 암호화를 수행합니다.

```
smime-deferred:if(mail-from == "user@example.com"){smime-gateway-deferred("smime-encrypt");}
```

S/MIME 서명 또는 암호화 작업

smime-gateway 작업은 지정된 전송 프로필을 사용하여 S/MIME 서명 또는 암호화를 수행하고 메시지를 전달하며, 추가 처리를 건너뜁니다.

다음 필터는 특정 발신자의 모든 발신 메시지에 대해 S/MIME 서명을 수행하고 메시지를 즉시 전달합니다.

```
smime-deliver-now:if(mail-from == "user@example.com"){smime-gateway("smime-sign");}
```

알림 및 알림 복사 작업

`notify` 및 `notify-copy` 작업은 지정된 이메일 주소로 메시지의 이메일 요약을 전송합니다. `notify-copy` 작업은 또한 원본 메시지의 복사본을 전송합니다(bcc-scan 작업과 유사). 알림 요약에는 다음이 포함되어 있습니다.

- 메시지의 메일 전송 프로토콜 변환에서 온 봉투 발신자 및 봉투 수신자(`MAIL FROM` 및 `RCPT TO`) 지침의 내용
- 메시지의 메시지 헤더
- 메시지와 일치한 메시지 필터의 이름

수신자, 제목 줄, 보낸 사람 주소 및 알림 템플릿을 지정할 수 있습니다. 다음 필터는 4메가바이트보다 큰 크기의 메시지를 선택하고, 일치하는 각 메시지의 알림 이메일을 `admin@example.com`으로 전송하고, 마지막으로 메시지를 삭제합니다.

```
bigFilter:

if(body-size >= 4M)

{

notify('admin@example.com');

drop();

}
```

또는

```
bigFilterCopy:

if(body-size >= 4M)

{

notify-copy('admin@example.com');

drop();

}
```

봉투 수신자 파라미터는 유효한 이메일 주소(예: 위의 예에서 admin@example.com)일 수도 있고, 메시지의 모든 봉투 수신자를 지정하는 작업 변수 $EnvelopeRecipients(작업 변수, 206 페이지 참고)일 수도 있습니다.

```
bigFilter:

if(body-size >= 4M)

{

notify('$EnvelopeRecipients');

drop();

}
```

notify 작업은 또한 최대 3개의 선택적인 추가 인수를 지원합니다. 이러한 인수를 통해 제목 헤더, 봉투 발신자, 그리고 알림 메시지에 사용할 사전 정의된 텍스트 리소스를 지정할 수 있습니다. 이러한 매개변수는 순서대로 나타나야 합니다. 따라서 봉투 발신자를 설정하거나 알림 템플릿을 지정하려면 제목을 제공해야 합니다.

제목 매개변수에는 원본 메시지의 데이터를 교체할 작업 변수(작업 변수, 206 페이지 참조)를 포함할 수 있습니다. 기본적으로 제목은 Message Notification으로 설정됩니다.

봉투 발신자 파라미터는 유효한 이메일 주소일 수도 있고, 메시지의 반환 경로를 원본 메시지와 동일하게 설정할 작업 변수 $EnvelopeFrom일 수도 있습니다.

알림 템플릿 매개변수는 기존 알림 템플릿의 이름입니다. 자세한 내용은 알림, 236 페이지를 참고하십시오.

이 예는 이전 예가 확장된 것이지만, 제목을 [bigFilter] Message too large와 같이 변경하고, 반환 경로를 원래 발신자로 설정하고, "message.too.large" 템플릿을 사용합니다.

```
bigFilter:

if (body-size >= 4M)

{

notify('admin@example.com', '[$FilterName] Message too large',

'$EnvelopeFrom', 'message.too.large');

drop();

}
```

발신자 또는 관리자에게 콘텐츠 필터가 트리거되었음을 알리기 위해 $MatchedContent 작업 변수를 사용할 수도 있습니다. $MatchedContent 작업 변수는 필터를 트리거한 콘텐츠를 표시합니다. 예를 들어 다음 필터는 이메일에 ABA 계정 정보가 포함되어 있으면 관리자에게 알림을 전송합니다.

```
ABA_filter:

if (body-contains ('*aba')){
```

```
notify('admin@example.com','[$MatchedContent]Account Information Displayed');
}
```

관련 주제

- Notification Template, 214 페이지

Notification Template

Text Resources(텍스트 리소스) 페이지 또는 `textconfig` CLI 명령을 사용하여 `notify()` 및 `notify-copy()` 작업과 함께 사용할 텍스트 리소스로서 맞춤화 알림 템플릿을 구성할 수 있습니다. 맞춤화 알림 템플릿을 만들지 않으면 기본 템플릿이 사용됩니다. 기본 템플릿은 메시지 헤더를 포함하지만, 맞춤화 알림 템플릿은 기본적으로 메시지 헤더를 포함하지 않습니다. 맞춤화 알림에 메시지 헤더를 포함하려면 `$AllHeaders` 작업 변수를 포함합니다.

자세한 내용은 "텍스트 리소스" 장을 참조하십시오.

다음 예에서, 큰 메시지가 아래에 표시된 필터를 트리거하면 메시지가 너무 크다고 설명하는 이메일이 원래 수신자에게 전송됩니다.

```
bigFilter:
if (body-size >= 4M)
{
notify('$EnvelopeRecipients', '[$FilterName] Message too large',
'$EnvelopeFrom', 'message.too.large');
drop();
}
```

숨은 참조 작업

`bcc` 작업은 익명의 메시지 복사본을 지정된 수신자에게 전송합니다. 이를 메시지 복제라고도 합니다. 원본 메시지에 복사본이라는 언급이 없으며 익명의 복사본은 수신자에게 성공적으로 반환되지 않으므로, 메시지의 원래 발신자 및 수신자는 복사본이 전송되었음을 알아야 할 필요가 없습니다.

다음 필터는 johnny에서 `sue`로 주소가 지정된 각 메시지에 대해 `mom@home.org`로 숨은 참조를 전송합니다.

```
momFilter:
if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))
{
bcc('mom@home.org');
}
```

bcc 작업은 또한 최대 3개의 선택적인 추가 인수를 지원합니다. 이러한 인수를 통해 복사된 메시지에 사용할 제목 헤더와 봉투 발신자 및 alt-mailhost를 지정할 수 있습니다. 이러한 매개변수는 순서대로 나타나야 합니다. 따라서 봉투 발신자를 설정하려면 제목을 제공해야 합니다.

제목 매개변수에는 원본 메시지의 데이터를 교체할 작업 변수(작업 변수, 206 페이지 참조)를 포함할 수 있습니다. 기본적으로, 이 파라미터는 원본 메시지의 제목(`$Subject`에 해당)으로 설정됩니다.

봉투 발신자 파라미터는 유효한 이메일 주소일 수도 있고, 메시지의 반환 경로를 원본 메시지와 동일하게 설정할 작업 변수 `$EnvelopeFrom`일 수도 있습니다.

이 예에서는 제목을 `[Bcc] <original subject>`, 반환 경로를 `badbounce@home.org`로 설정하여 이전 예를 확장합니다.

```
momFilter:

if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

{

bcc('mom@home.org', '[Bcc] $Subject', 'badbounce@home.org');

}
```

alt-mailhost는 네 번째 매개변수입니다.

```
momFilterAltM:

if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

{

bcc('mom@home.org', '[Bcc] $Subject', '$EnvelopeFrom',

'momaltmailserver.example.com');

}
```

주의 `Bcc()`, `notify()` 및 `bounce()` 필터 작업은 바이러스의 네트워크 통과를 허용할 수 있습니다. BCC 필터 작업은 원본 메시지의 완전한 복사본인 새 메시지를 생성합니다. 알림 필터 작업은 원본 메시지의 헤더를 포함하는 새 메시지를 생성합니다. 드물기는 하지만 헤더에는 바이러스가 포함될 수 있습니다. 반송 필터 작업은 원본 메시지의 처음 10k를 포함하는 새 메시지를 생성합니다. 세 가지 경우 모두 새 메시지에 대해 안티바이러스 또는 안티스팸 검사가 처리되지 않습니다.

여러 호스트로 전송하려면 `bcc()` 작업을 여러 번 호출해야 합니다.

```
multiplealthosts:

if (recv-listener == "IncomingMail")

{

insert-header('X-ORIGINAL-IP', '$remote_ip');
```

```
bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.4');
bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.5');
bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.6');
}
```

관련 주제

- 경쟁사로 전송되는 메일 검사 및 숨은 참조 처리, 257 페이지

bcc-scan() 작업

전송되는 메시지가 새 메시지로 취급되어 전체 이메일 파이프라인을 통과한다는 점을 제외하고 `bcc-scan` 작업은 bcc 작업과 유사하게 작동합니다.

```
momFilter:
if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))
{
bcc-scan('mom@home.org');
}
```

격리 및 복제 작업

`quarantine('quarantine_name')` 작업은 격리라는 대기열에 포함되도록 메시지에 플래그를 지정합니다. 격리에 대한 자세한 내용은 "격리" 장을 참조하십시오. `duplicate-quarantine('quarantine_name')` 작업은 메시지의 복사본을 지정된 격리로 즉시 이동합니다. 원본 메시지는 이메일 파이프라인을 계속 통과합니다. 격리 이름은 대/소문자를 구분합니다.

격리를 위해 플래그를 지정하면 메시지는 계속해서 이메일 파이프라인의 나머지를 지나갑니다. 하나 이상의 격리에 대해 플래그가 지정된 메시지는 파이프라인의 끝에 도달하면 해당 큐에 추가됩니다. 그렇지 않으면 전달됩니다. 메시지가 파이프라인의 끝에 도달하지 못하면 격리에 배치되지 않습니다.

따라서 메시지 필터에 `quarantine()` 작업과 그 뒤에 `bounce()` 또는 `drop()` 작업이 포함되어 있으면, 최종 작업이 메시지가 파이프라인의 끝에 도달하지 못하게 하므로 메시지는 격리로 들어가지 않습니다. 메시지 필터에 격리 작업이 포함되어 있지만 메시지가 나중에 안티스팸이나 안티바이러스 검사 또는 콘텐츠 필터에 의해 삭제되는 경우도 마찬가지입니다. `skip-filters()` 작업은 메시지가 나머지 메시지 필터를 건너뛰도록 하지만, 콘텐츠 필터는 여전히 적용될 수 있습니다. 예를 들어 메시지 필터가 메시지에 격리에 대한 플래그를 지정하며 `skip-filters()` 작업도 포함하는 경우, 이메일 파이프라인에서 또 다른 작업이 메시지 삭제를 일으키지 않는 한 해당 메시지는 나머지 메시지 필터를 모두 건너뛰고 격리됩니다.

다음 예에서는 "secret_word"라는 이름의 사전에 있는 단어가 메시지에 포함된 경우 해당 메시지가 Policy(정책) 격리로 전송됩니다.

```
quarantine_codenames:
```

```
if (dictionary-match ('secret_words'))

{

quarantine('Policy');

}
```

다음 예에서는 회사에 모든 .mp3 첨부 파일을 삭제하는 공식 정책이 있다고 가정합니다. 인바운드 메시지에 .mp3 첨부 파일이 있으면 해당 첨부 파일이 제거되고 나머지 메시지(원본 본문 및 나머지 첨부 파일)가 원래 수신자에게 전송됩니다. 모든 첨부 파일이 포함된 원본 메시지의 또 다른 복사본은 격리됩니다(Policy(정책) 격리로 전송됨). 차단된 첨부 파일을 수신해야 하는 경우 원래 수신자는 메시지를 격리에서 릴리스해달라고 요청할 수 있습니다.

```
strip_all_mp3s:

if (attachment-filename == '(?i)\\.mp3$') {

duplicate-quarantine('Policy');

drop-attachments-by-name('(?i)\\.mp3$');

}
```

수신자 변경 작업

`alt-rcpt-to` 작업은 전달 시 메시지의 모든 수신자를 지정된 수신자로 변경합니다.

다음 필터는 `.freelist.com`이 포함된 봉투 수신자 주소의 모든 메시지를 전송하고 메시지의 모든 수신자를 `system-lists@myhost.com`으로 변경합니다.

```
freelistFilter:

if(rcpt-to == '\\.freelist\\.com$')

{

alt-rcpt-to('system-lists@myhost.com');

}
```

전달 호스트 변경 작업

`alt-mailhost` 작업은 선택한 메시지의 모든 수신자에 대한 IP 주소를 숫자 IP 주소 또는 지정된 호스트 이름으로 변경합니다.

참고 `alt-mailhost` 작업은 안티스팸 검사 엔진에 의해 스팸으로 분류된 메시지가 격리되는 것을 방지합니다. `alt-mailhost` 작업은 `격리` 작업을 재정의하고 이를 지정된 메일 호스트로 전송합니다.

다음 필터는 모든 메시지에 대해 수신자 주소를 example.com으로 리디렉션합니다.

```
localRedirectFilter:

if(true)

{

alt-mailhost('example.com');

}
```

따라서 joe@anywhere.com으로 향하는 메시지는 Envelope To 주소 joe@anywhere.com과 함께 example.com의 메일 호스트로 전달됩니다. smtproutes 명령으로 지정된 추가 라우팅 정보는 여전히 메시지 라우팅에 영향을 미칩니다 (로컬 도메인용 이메일 라우팅, 665 페이지참조).

참고 alt-mailhost 작업은 포트 번호 지정을 지원하지 않습니다. 포트 번호를 지정하려면 대신 SMTP 경로를 추가하십시오.

다음 필터는 모든 메시지를 192.168.12.5로 리디렉션합니다.

```
local2Filter:

if(true)

{

alt-mailhost('192.168.12.5');

}
```

소스 호스트(가상 게이트웨이 주소) 변경 작업

alt-src-host 작업은 메시지에 대한 소스 호스트를 지정된 소스로 변경합니다. 소스 호스트는 메시지 전달이 시작되는 IP 인터페이스 또는 IP 인터페이스의 그룹으로 구성됩니다. IP 인터페이스의 그룹이 선택된 경우 시스템은 이메일을 전달할 때 그룹 내 모든 IP 인터페이스를 소스 인터페이스로 순환합니다. 기본적으로, 이를 통해 단일 Cisco Email Security Appliance에 여러 가상 게이트웨이 주소를 생성할 수 있습니다. 자세한 내용은 호스팅된 모든 도메인에 대한 메일 게이트웨이 구성에 Virtual Gateway™ 기술 사용, 718 페이지의 내용을 참고하십시오.

IP 인터페이스는 시스템에 현재 구성된 단일 IP 인터페이스 또는 인터페이스 그룹으로만 변경될 수 있습니다. 다음 필터는 IP 주소 1.2.3.4로 원격 호스트에서 수신된 모든 메시지에 대해 아웃바운드(전달) IP 인터페이스 outbound2를 사용하여 가상 게이트웨이를 만듭니다.

```
externalFilter:

if(remote-ip == '1.2.3.4')

{

alt-src-host('outbound2');
```

```
}
```

다음 필터는 IP 주소 1.2.3.4의 원격 호스트에서 수신된 모든 메시지에 대해 IP 인터페이스 그룹 Group1을 사용합니다.

```
groupFilter:

if(remote-ip == '1.2.3.4')

{

alt-src-host('Group1');

}
```

아카이브 작업

archive 작업은 모든 메시지 헤더와 수신자를 포함하여 원본 메시지의 복사본을 어플라이언스의 mbox 형식 파일에 저장합니다. 이 작업은 메시지를 저장할 로그 파일의 이름인 매개변수를 사용합니다. 사용자가 필터를 만들면 시스템은 지정된 파일 이름으로 로그 서브스크립션을 자동으로 만듭니다. 사용자는 기존 필터 로그 파일을 지정할 수도 있습니다. 필터 및 필터 로그 파일을 만들었으면 filters -> logconfig 하위 명령을 사용하여 수정할 수 있습니다.

참고 logconfig 명령은 filters의 하위 명령입니다. 이 하위 명령 사용 방법에 대한 자세한 내용은 CLI를 사용하여 메시지 필터 관리, 240 페이지 섹션을 참조하십시오.

mbox 형식은 표준 UNIX 사서함 형식이며, 메시지를 더욱 쉽게 보기 위해 사용할 수 있는 많은 유틸리티가 있습니다. 대부분의 UNIX 시스템에서는 "mail-f *mbox.filename*"을 입력하여 파일을 볼 수 있습니다. mbox 형식은 일반 텍스트이므로 단순한 텍스트 편집기를 사용해 메시지의 내용을 볼 수 있습니다.

다음 예에서는 봉투 발신자가 joesmith@yourdomain.com과 일치하면 메시지의 복사본이 joesmith라는 로그에 저장됩니다.

```
logJoeSmithFilter:

if(mail-from == '^joesmith@yourdomain\\.com$')

{

archive('joesmith');

}
```

헤더 제거 작업

strip-header 작업은 메시지에서 특정 헤더를 검사하여 전달 전에 해당 줄을 제거합니다. 여러 헤더가 있으면 모두 제거됩니다(예: "Received:" 헤더).

다음 예에서는 전송 전에 모든 메시지에서 `X-DeleteMe` 헤더가 제거됩니다.

```
stripXDeleteMeFilter:

if (true)

{

strip-header('X-DeleteMe');

}
```

헤더로 작업할 때는 헤더의 현재 값에 처리 중 변경된 내용(예: 메시지 제목을 추가, 제거 또는 수정하는 필터 작업으로)이 포함되어 있다는 점을 기억해야 합니다. 자세한 내용은 메시지 헤더 규칙 및 평가, 141 페이지를 참조하십시오.

헤더 삽입 작업

`insert-header` 작업은 메시지에 새 헤더를 삽입합니다. AsyncOS는 사용자가 삽입한 헤더가 표준을 준수하는지를 확인하지 않습니다. 따라서 결과 메시지가 이메일의 인터넷 표준을 준수하도록 하는 것은 사용자의 책임입니다.

다음 예에서는 메시지에서 헤더가 아직 발견되지 않은 경우 `My Company Name`으로 설정된 값과 함께 `X-Company`라는 이름의 헤더를 삽입합니다.

```
addXCompanyFilter:

if (not header('X-Company'))

{

insert-header('X-Company', 'My Company Name');

}
```

`insert-header()` 작업은 헤더의 텍스트에 비 ASCII 문자를 사용하도록 허용하는 반면, 헤더 이름은 ASCII로 제한합니다(표준 준수를 위해). 가독성을 최대화하기 위해 전송 인코딩은 QP(quoted printable)가 됩니다.

참고 원본 메시지에서 메시지 헤더를 재작성하기 위해 `strip-headers` 및 `insert-header` 작업을 함께 사용할 수 있습니다. 어떤 경우에는 동일한 헤더의 여러 인스턴스를 갖는 것이 유효하고(예: `Received:`), 다른 경우에는 동일한 헤더의 여러 인스턴스가 MUA에 혼동을 줄 수 있습니다(예: 여러 Subject: 헤더).

헤더로 작업할 때는 헤더의 현재 값에 처리 중 변경된 내용(예: 메시지 제목을 추가, 제거 또는 수정하는 필터 작업으로)이 포함되어 있다는 점을 기억해야 합니다. 자세한 내용은 메시지 헤더 규칙 및 평가, 141 페이지를 참조하십시오.

헤더 텍스트 수정 작업

`edit-header-text` 작업은 정규식 대체 함수를 사용하여 지정된 헤더 텍스트를 재작성하도록 허용합니다. 필터는 헤더 내에서 정규식의 일치를 확인한 다음 사용자가 지정한 정규식으로 교체합니다.

예를 들어 이메일에는 다음 제목 헤더가 포함됩니다.

```
Subject: SCAN Marketing Messages
```

다음 필터는 헤더에서 "SCAN" 텍스트를 제거하고 "Marketing Messages" 텍스트를 남겨둡니다.

```
Remove_SCAN: if true

{

edit-header-text ('Subject', '^SCAN\\s*','');

}
```

필터는 메시지를 처리한 후 다음 헤더를 반환합니다.

```
Subject: Marketing Messages
```

본문 텍스트 수정 작업

`edit-body-text()` 메시지 필터는 `Edit-Header-Text()` 필터와 유사하지만, 헤더 중 하나가 아니라 메시지 본문 전체에서 작동합니다.

`edit-body-text()` 메시지 필터는 첫 번째 매개변수가 검색할 정규식이고 두 번째 매개변수가 교체 텍스트인 다음 구문을 사용합니다.

```
Example: if true {

edit-body-text("parameter 1","parameter 2");

}
```

`edit-body-text()` 메시지 필터는 메시지 본문 부분에서만 작동합니다. 특정 MIME 부분을 메시지 "본문"으로 간주할지 메시지 "첨부 파일"로 간주할지에 대한 자세한 내용은 메시지 본문과 메시지 첨부 파일 비교, 141 페이지 섹션을 참조하십시오.

다음 예에서는 메시지에서 URL을 제거하고 'URL REMOVED'라는 텍스트로 교체합니다.

```
URL_Replaced: if true {

edit-body-text("(?i)(?:https?|ftp)://[^\\s\">]+", "URL REMOVED");

}
```

다음 예에서는 본문에서 사회 보장 번호를 제거하고 "XXX-XX-XXXX"라는 텍스트로 교체합니다.

```
ssn: if true {

edit-body-text("(?!000)(?:[0-6]\\d{2}|7(?:[0-6]\\d|7[012]))([
```

```
-]?)(?!00)\\d\\d\\1(?!0000)\\d{4}",

"XXX-XX-XXXX");

}
```

참고 여기에서는 스마트 식별자를 `edit-body-text()` 필터와 함께 사용할 수 없습니다.

HTML 변환 작업

RFC 2822는 이메일 메시지용 텍스트 형식을 정의하지만, RFC 2822 메시지 내 다른 콘텐츠의 전송을 제공하기 위한 확장(예: MIME)도 있습니다. AsyncOS는 이제 `html-convert()` 메시지 필터를 사용하여 다음 구문을 통해 HTML을 일반 텍스트로 변환할 수 있습니다.

```
Convert_HTML_Filter:

if (true)

{

html-convert();

}
```

Cisco 메시지 필터는 특정 MIME 부분을 메시지 "본문"으로 간주할지 메시지 "첨부 파일"로 간주할지에 대한 결정을 내립니다. `html-convert()` 필터는 메시지 본문 부분에서만 작동합니다. 메시지 본문 및 첨부 파일에 대한 자세한 내용은 메시지 본문과 메시지 첨부 파일 비교, 141 페이지 섹션을 참조하십시오.

`html-convert()` 필터는 형식에 따라 문서 내에서 HTML을 제거하는 서로 다른 방법을 사용합니다.

메시지가 일반 텍스트(text/plain)이면 변경 없이 필터를 통과합니다. 메시지가 단순한 HTML 메시지(text/html)이면 메시지에서 모든 HTML 태그가 제거되고 남은 본문이 HTML 메시지를 교체합니다. 줄의 형식은 바뀌지 않으며, 일반 텍스트에서는 HTML이 렌더링되지 않습니다. 구조가 MIME(multipart/alternative 구조)이고 동일한 내용의 text/plain 부분 및 text/html 부분을 모두 포함하고 있다면, 필터는 메시지의 text/html 부분을 제거하고 text/plain 부분을 남겨둡니다. 다른 모든 MIME 유형(예: multipart/mixed)의 경우 모든 HTML 본문 부분은 태그가 제거되어 메시지에 다시 삽입됩니다.

메시지 필터에서 발견되는 경우 `html-convert()` 필터 작업은 처리할 메시지에 대해 태그만 지정하고 메시지 구조를 즉시 변경하지는 않습니다. 모든 처리가 완료된 후에야 메시지에 대한 변경이 수행됩니다. 따라서 다른 필터 작업이 수정 전에 원본 메시지 본문을 처리할 수 있습니다.

반송 프로필 작업

`bounce-profile` 작업은 앞서 구성된 반송 프로필을 메시지에 할당합니다(반송된 이메일 전달, 694 페이지참조). 메시지를 전달할 수 없는 경우 반송 프로필을 통해 구성된 반송 옵션이 사용됩니다. 이 기능을 사용하면 리스너의 컨피그레이션에서 메시지로 할당된 반송 프로필이 재정의됩니다(할당된 경우).

다음 필터 예는 `X-Bounce-Profile: fastbounce` 헤더와 함께 전송된 모든 이메일에 반송 프로파일 "fastbounce"를 할당합니다.

```
fastbounce:

if (header ('X-Bounce-Profile') == 'fastbounce') {

bounce-profile ('fastbounce');

}
```

안티스팸 시스템 우회 작업

`skip-spamcheck` 작업을 사용하면 시스템은 메시지가 시스템에 구성된 콘텐츠 기반 안티 스팸 필터링을 우회하도록 허용합니다. 이 작업은 콘텐츠 기반 안티스팸 필터링이 구성되지 않은 경우 또는 처음에 스팸을 검사하도록 메시지에 플래그가 지정되지 않은 경우 메시지에 대해 아무것도 하지 않습니다.

다음 예는 SenderBase Reputation 점수가 높은 메시지가 콘텐츠 기반 안티스팸 필터링 기능을 우회하도록 허용합니다.

```
whitelist_on_reputation:

if (reputation > 7.5)

{

skip-spamcheck();

}
```

관련 주제

- 수신 릴레이가 기능에 영향을 미치는 방식 , 381 페이지
- 스팸 필터로부터 어플라이언스에서 생성된 메시지 보호, 369 페이지

그레이메일 우회 작업

특정 메시지에 그레이메일 작업을 적용하지 않으려면 다음 메시지 필터 작업을 사용하여 우회할 수 있습니다.

메시지 필터 작업	설명
`skip-marketingcheck`	마케팅 이메일에서 작업 우회
`skip-socialcheck`	소셜 네트워크 이메일에서 작업 우회
`skip-bulkcheck`	대량 이메일에서 작업 우회

다음 예에서는 "private_listener" 리스너에서 수신하는 메시지가 소셜 네트워크 이메일에 대한 그레이메일 작업을 우회하도록 지정합니다.

```
internal_mail_is_safe:

if (recv-listener == 'private_listener')

{

skip-socialcheck();

}
```

안티바이러스 시스템 우회 작업

`skip-viruscheck` 작업을 사용하면 시스템은 메시지가 시스템에 구성된 바이러스 차단 시스템을 우회하도록 허용합니다. 이 작업은 안티바이러스 시스템이 구성되지 않은 경우 또는 처음에 바이러스를 검사하도록 메시지에 플래그가 지정되지 않은 경우 메시지에 대해 아무것도 하지 않습니다.

다음 예에서는 "private_listener" 리스너에서 수신하는 메시지가 안티스팸 및 안티바이러스 시스템을 우회하도록 지정합니다.

```
internal_mail_is_safe:

if (recv-listener == 'private_listener')

{

skip-spamcheck();

skip-viruscheck();

}
```

파일 평판 필터링 및 파일 분석 시스템 우회 작업

skip-ampcheck 작업을 사용하면 시스템은 메시지가 시스템에 구성된 파일 평판 필터링 및 파일 분석을 우회하도록 허용합니다. 이 작업은 파일 평판 필터링 및 파일 분석이 구성되지 않은 경우 또는 처음에 파일 평판 필터링 및 파일 분석을 검사하도록 메시지에 플래그가 지정되지 않은 경우 메시지에 대해 아무것도 하지 않습니다.

다음 예에서는 PDF 첨부 파일이 있는 메시지가 파일 평판 필터링 및 파일 분석을 우회하도록 지정합니다.

```
skip_amp_scan:
if (attachment-filetype == 'pdf')
{
skip-ampcheck();
}
```

Outbreak Filter 검사 우회 작업

`skip-vofcheck` 작업을 사용하면 시스템은 메시지가 Outbreak Filter 검사를 우회하도록 허용합니다. 이 작업은 Outbreak Filter 검사가 활성화되지 않은 경우 메시지에 대해 아무것도 하지 않습니다.

다음 예에서는 "private_listener" 리스너에서 수신하는 메시지가 Outbreak Filter 검사를 우회하도록 지정합니다.

```
internal_mail_is_safe:

if (recv-listener == 'private_listener') Outbreak Filters

{

skip-vofcheck();

}
```

메시지 태그 추가 작업

`tag-message` 작업은 DLP 정책 필터링과 함께 사용할 수 있도록 맞춤화 용어를 발신 메시지에 삽입합니다. 메시지 태그가 있는 메시지로 검사를 제한하도록 DLP 정책을 구성할 수 있습니다. 메시지 태그는 수신자에게 보이지 않습니다. 태그 이름에는 `[a-zA-Z0-9_-.]` 집합에 있는 모든 문자 조합을 사용할 수 있습니다. .

메시지 필터링을 위해 DLP 정책을 구성하는 방법에 대한 자세한 내용은 "데이터 유출 방지" 장을 참조하십시오.

다음 예에서는 제목에 "`[Encrypt]`"가 있는 메시지에 메시지 태그를 삽입합니다. 그런 다음 Cisco 이메일 암호화를 사용할 수 있는 경우 전달 전에 이 메시지 태그로 메시지를 암호화할 DLP 정책을 만들 수 있습니다.

```
Tag_Message:

if (subject == '^\\[Encrypt\\]')

{

tag-message('Encrypt-And-Deliver');

}
```

로그 항목 추가 작업

`log-entry` 작업은 `INFO` 수준에서 텍스트 메일 로그에 맞춤화 텍스트를 삽입합니다. 텍스트는 작업 변수를 포함할 수 있습니다. 메시지 필터가 특정 작업을 수행한 이유에 대한 정보를 얻고 디버깅을 수행하는 데 유용한 텍스트를 삽입하기 위해 이 작업을 사용할 수 있습니다. 메시지 추적에도 로그 항목이 나타납니다.

다음 예는 회사의 기밀 정보가 포함되었을 가능성 때문에 메시지가 반송되었음을 설명하는 로그 항목을 삽입합니다.

```
CompanyConfidential:

if (body-contains('Company Confidential'))

{
```

```
log-entry('Message may have contained confidential information.');

bounce();

}
```

URL 평판 작업

URL 또는 URL의 동작을 수정하기 위해 메시지에 있는 URL의 평판 점수를 사용할 수 있습니다. 자세한 설명과 예는 악의적이거나 바람직하지 않은 URL로부터 보호, 425 페이지의 메시지의 URL 수정: URL 평판 및 필터의 URL 범주 작업 사용 , 434 페이지 섹션을 참조하십시오.

이러한 작업에는 규칙이 필요하지 않습니다.

URL 평판 작업에서

- `msg_filter_name`: 이 메시지 필터의 이름입니다.
- `min_score` 및 `max_score`는 작업을 적용해야 하는 범위의 최소 및 최대 점수입니다. 적용 범위는 사용자가 지정하는 값을 포함합니다.

최소 및 최대 점수는 `-10.0`에서 `10.0` 사이여야 합니다.

- 평판 서비스가 점수를 제공하지 않는 경우의 작업을 지정하려면 다음 하위 섹션에 나와 있는 것처럼 작업의 해당 "no-reputation" 버전을 사용합니다.
- `whitelist`는 정의된 URL 리스트의 이름입니다(`urllistconfig` 명령을 통해.) 화이트리스트 지정은 선택 사항입니다.
- `Preserve_signed`에 0 또는 1을 입력합니다.
  - 1 - 이 작업을 서명되지 않은 메시지에만 적용
  - 0 - 이 작업을 모든 메시지에 적용

`preserve_signed` 값을 지정하지 않으면 서명되지 않은 메시지에만 작업이 적용됩니다.

관련 주제

- URL 평판을 기반으로 URL을 텍스트와 교체, 226 페이지
- URL 평판을 기반으로 URL Defang, 227 페이지
- URL 평판을 기반으로 URL을 Cisco 보안 프록시로 리디렉션 , 227 페이지

URL 평판을 기반으로 URL을 텍스트와 교체

평판 서비스 공급업체에서 점수를 제공할 때 작업을 수행하려면

`url-reputation-replace` 작업을 사용합니다.

`url-reputation-replace` 작업을 사용하는 필터의 구문은 다음과 같습니다.

```
<msg_filter_name>:

if <condition>

{url-reputation-replace(<min_score>, <max_score>,'<replace_text>', '< whitelist>', <
Preserve_signed> );}
```

여기서 replace_text는 URL을 교체할 텍스트입니다.

평판 서비스 공급업체에서 점수를 제공하지 않을 때 작업을 수행하려면 url-no-reputation-replace 작업을 사용합니다.

url-no-reputation-replace 작업을 사용하는 필터의 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{url-no-reputation-replace ('<replace_text>', '<whitelist>', <Preserve_signed>);}
```

여기서 replace_text는 URL을 교체할 텍스트입니다.

URL 평판을 기반으로 URL Defang

평판 서비스 공급업체에서 점수를 제공할 때 작업을 수행하려면 url-reputation-defang 작업을 사용합니다.

url-reputation-defang 작업을 사용하는 필터의 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{url-reputation-defang (<min_score>, <max_score>, '<whitelist>', <Preserve_signed>);}
```

평판 서비스 공급업체에서 점수를 제공하지 않을 때 작업을 수행하려면 url-no-reputation-defang 작업을 사용합니다.

url-no-reputation-defang 작업을 사용하는 필터의 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{url-no-reputation-defang ('<whitelist>', <Preserve_signed>);}
```

URL 평판을 기반으로 URL을 Cisco 보안 프록시로 리디렉션

평판 서비스 공급업체에서 점수를 제공할 때 작업을 수행하려면 url-reputation-proxy-redirect 작업을 사용합니다.

url-reputation-proxy-redirect 작업을 사용하는 필터의 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{url-reputation-proxy-redirect (<min_score>, <max_score>, '<whitelist>', <Preserve_signed>);}
```

평판 서비스 공급업체에서 점수를 제공하지 않을 때 작업을 수행하려면 url-no-reputation-proxy-redirect 작업을 사용합니다.

`url-no-reputation-proxy-redirect` 작업을 사용하는 필터의 구문은 다음과 같습니다.

```
<msg_filter_name>:

if <condition>

{url-no-reputation-proxy-redirect ('<whitelist>', <Preserve_signed>);}
```

URL 범주 작업

URL 또는 URL의 동작을 수정하기 위해 메시지에 있는 URL의 범주를 사용할 수 있습니다. 자세한 내용은 악의적이거나 바람직하지 않은 URL로부터 보호, 425 페이지의 메시지의 URL 수정: URL 평판 및 필터의 URL 범주 작업 사용 , 434 페이지 섹션을 참조하십시오.

이러한 작업에는 규칙이 필요하지 않습니다.

모든 URL 범주 작업에서

- msg_filter_name: 메시지 필터의 이름입니다.
- category-name은 URL 범주입니다. 여러 범주는 쉼표로 구분합니다. 정확한 범주 이름을 사용하려면 콘텐츠 필터에서 URL Category 조건 또는 작업을 찾아보십시오. 범주의 설명과 예는 URL 범주 정보, 446 페이지 섹션을 참조하십시오.
- url_white_list는 정의된 URL 리스트의 이름입니다(urllistconfig 명령을 통해).
- unsigned-only: 0 또는 1을 입력합니다.
  - 1 - 이 작업을 서명되지 않은 메시지에만 적용
  - 0 - 이 작업을 모든 메시지에 적용

관련 주제

- URL 범주를 기반으로 URL을 텍스트로 교체 , 228 페이지
- URL 범주를 기반으로 URL Defang , 228 페이지
- URL 범주를 기반으로 URL을 Cisco 보안 프록시로 리디렉션 , 229 페이지

URL 범주를 기반으로 URL을 텍스트로 교체

`url-category-replace` 작업을 사용하는 필터의 구문은 다음과 같습니다.

```
<msg_filter_name>:

if <condition>

url-category-replace(['<category-name1>','<category-name2>',...,
'<category-name3>'],'<replacement-text>', '<url_white_list>', <unsigned-only>);
```

여기서 `replacement-text`는 URL을 교체하기 위해 사용할 텍스트입니다.

URL 범주를 기반으로 URL Defang

`url-category-defang` 작업을 사용하는 필터의 구문은 다음과 같습니다.

```
<msg_filter_name>:

if <condition>
```

```
url-category-defang(['<category-name1>','<category-name2>',..., '<category-name3>'],
'<url_white_list>', <unsigned-only>);
```

URL 범주를 기반으로 URL을 Cisco 보안 프록시로 리디렉션

`url-category-proxy-redirect` 작업을 사용하는 필터의 구문은 다음과 같습니다.

```
<msg_filter_name>:

if <condition>

url-category-proxy-redirect(['<category-name1>','<category-name2>',..., '<category-name3>'],
'<url_white_list>', <unsigned-only>);
```

운영 없음

No Operation(운영 없음) 작업은 아무 작업도 수행하지 않습니다. Notify(알림), Quarantine(격리), Drop(삭제) 등의 다른 작업을 사용하지 않으려는 경우 메시지 필터에서 이 작업을 사용할 수 있습니다. 예를 들어, 새로 만든 메시지 필터의 동작을 이해하려면 No Operation(운영 없음) 작업을 사용할 수 있습니다. 메시지 필터가 작동된 후 Message Filters(메시지 필터) 보고 페이지를 사용하여 새 메시지 필터의 동작을 모니터링하고 요구 사항에 맞게 필터를 세밀하게 조정할 수 있습니다.

다음 예는 메시지 필터에서 No Operation(운영 없음) 작업을 사용하는 방법을 보여줍니다.

```
new_filter_test: if header-repeats ('subject', X, 'incoming') {no-op();}
```

위조 이메일 탐지 작업

위조 메시지에서 발신인: 헤더를 제거하고 봉투 발신자로 대체합니다.

다음 메시지 필터는 메시지의 From: 헤더를 사전에 있는 용어와 비교하여 콘텐츠 사전에서 용어의 일치 점수가 70보다 크거나 같은 경우 From: 헤더를 제거하고 봉투 발신자로 대체합니다.

```
FED_CF: if (forged-email-detection("Execs", 70)) { fed("from", ""); }
```

Attachment Scanning(첨부 파일 검사)

Email Security Appliance는 콘텐츠 스캐너를 사용하여 회사 정책과 일치하지 않는 메시지의 첨부 파일을 제거하는 한편 원본 메시지 전달 기능은 그대로 유지합니다.

특정 파일 형식, 핑거프린트 또는 첨부 파일의 내용을 기반으로 첨부 파일을 필터링할 수 있습니다. 핑거프린트를 사용하여 정확한 첨부 파일 형식을 파악하면 악성 첨부 파일 확장명(예: .exe)에서 좀 더 일반적으로 사용되는 확장명(예: .doc)으로 이름을 변경하여 이름 변경된 파일이 첨부 파일 필터를 우회하도록 하려는 사용자의 의도를 차단할 수 있습니다.

첨부 파일에서 내용을 검사할 때 콘텐츠 스캐너는 첨부 파일에서 데이터를 추출하여 정규식을 검색합니다. 이 엔진은 첨부 파일에서 데이터와 메타데이터를 모두 검사합니다. Excel 또는 Word 문서를 검사하는 경우 이 첨부 파일 검사 엔진은 .exe, .dll, .bmp, .tiff, .pcx, .gif, .jpeg, .png 및 Photoshop 이미지 등의 내장된 파일 형식도 탐지할 수 있습니다.

어플라이언스의 콘텐츠 스캐너는 다음 아카이브 파일 형식에 대한 콘텐츠 검사를 수행할 수 있습니다.

- ACE 아카이브
- ALZ 아카이브
- Apple 디스크 이미지
- ARJ 아카이브
- bzip2 아카이브
- EGG 아카이브
- GNU Zip
- ISO 디스크 이미지
- Java 아카이브
- LZH
- Microsoft Cabinet 아카이브
- RAR 다중 파트 파일
- RedHat Package Manager 아카이브
- Roshal 아카이브(RAR)
- Unix AR 아카이브
- UNIX 압축 아카이브
- UNIX cpio
- UNIX Tar
- XZ 아카이브
- ZIP 아카이브
- 7-Zip

참고 웹 인터페이스에서 **Security Services** > **Scan Behavior(**검사 동작**)** 페이지를 사용하거나 CLI에서 contentscannerstatus 명령을 사용하여 콘텐츠 스캐너 관련 파일의 상세정보를 볼 수 있습니다. 이러한 파일은 업데이트 서버를 통해 자동으로 업데이트됩니다. 이러한 파일을 수동으로 업데이트하려면 검사 동작 구성, 263 페이지 항목을 참고하십시오.

관련 주제

- 첨부 파일 검사용 메시지 필터, 231 페이지

첨부 파일 검사용 메시지 필터

다음 표에 설명된 메시지 필터 작업은 비최종 작업입니다. (첨부 파일이 삭제되고 메시지 처리가 계속됩니다.)

선택 사항인 코멘트는 메시지에 추가되는 텍스트이며(바닥글과 매우 유사), 메시지 필터 작업 변수를 포함할 수 있습니다(첨부 파일 검사 메시지 필터의 예, 237 페이지 참조).

표 ***26:*** 첨부 파일 필터링용 메시지 필터 작업

작업	**Syntax**	설명
이름으로 첨부 파일 삭제	`drop-attachments-by-name (<regular expression >[, <optional comment >])`	지정된 정규식과 일치하는 파일 이름을 가지고 있는 메시지의 모든 첨부 파일을 삭제합니다. 일치하는 파일이 포함된 경우 아카이브 첨부 파일(zip, tar)을 삭제합니다. 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.
유형으로 첨부 파일 삭제	`drop-attachments-by-type (<MIME type >[, <optional comment >])`	특정 MIME 유형(지정된 MIME 유형 또는 파일 확장명으로 판단)을 가지고 있는 메시지의 모든 첨부 파일을 삭제합니다. 일치하는 파일이 포함된 경우 아카이브 첨부 파일(zip, tar)을 삭제합니다.
파일 형식으로 첨부 파일 삭제	`drop-attachments-by-filetype (<fingerprint name >[, <optional comment >])`	파일의 지정된 "지문"과 일치하는 메시지의 모든 첨부 파일을 삭제합니다. 일치하는 파일이 포함되어 있는 경우 아카이브 첨부 파일(zip, tar)이 삭제됩니다.
MIME 유형으로 첨부 파일 삭제	`drop-attachments-by-mimetype (<MIME type >[, <optional comment >])`	지정된 MIME 유형을 가지고 있는 메시지의 모든 첨부 파일을 삭제합니다. 이 작업은 파일 확장명으로 MIME 유형을 확정하려고 하지 않으며 아카이브의 내용을 검토하지도 않습니다.

작업	**Syntax**	설명
크기로 첨부 파일 삭제	`drop-attachments-by-size (<number >[, <optional comment >])`	지정된 파일 크기(바이트)와 같거나 큰(원시 인코딩 형식) 메시지의 모든 첨부 파일을 삭제합니다. 아카이브 또는 압축된 파일의 경우 이 작업은 압축 해제된 크기를 검토하지 않고 실제 첨부 파일 자체의 크기를 검토합니다.
첨부 파일 검사	`drop-attachments-where-contains (<regular expression >[, <optional comment >])`	정규식을 포함하는 메시지의 모든 첨부 파일을 삭제합니다. 포함된 파일 중에 정규식 패턴이 있는 경우 아카이브 파일(zip, tar)을 삭제합니다.
사전 일치로 첨부 파일 삭제	`drop-attachments-where-dictionary -match(<dictionary name>)`	이 필터는 사전 용어에 대한 일치를 기반으로 첨부 파일을 제거합니다. 첨부 파일로 간주되는 MIME 부분의 용어가 사전 용어와 일치하면(그리고 사용자 정의 임계값이 충족되면) 이메일에서 첨부 파일이 제거됩니다. 첨부 파일 검사 메시지 필터의 예, 237 페이지를 참조하십시오.

이미지 분석

일부 메시지에는 부적절한 내용을 검사해야 할 수 있는 이미지가 포함되어 있습니다. 이메일에서 부적절한 내용을 검색하려면 이미지 분석 엔진을 사용할 수 있습니다. 이미지 분석은 안티바이러스 및 안티스팸 검사 엔진을 보완하거나 대신하도록 설계되지 않았습니다. 이미지 분석의 목적은 이메일에서 부적절한 내용을 식별하여 선별적 사용을 시행하는 것입니다. 이미지 분석 검사 엔진을 사용하면 메일을 격리 및 분석하고 추세를 탐지할 수 있습니다.

이미지 분석을 위해 어플라이언스를 구성한 후에는 이미지 분석 필터 규칙을 사용하여 의심스럽거나 부적절한 이메일에 대해 작업을 수행할 수 있습니다. 이미지 검사에서는 BMP, JPG, TIF, PNG, GIF, TGA, PCX 등의 첨부 파일 형식을 검사할 수 있습니다. 이미지 분석기는 그래픽에 부적절한 내용이 포함되어 있을 가능성을 판단하기 위해 피부색, 신체 크기 및 곡률을 측정하는 알고리즘을 사용합니다. 이미지 첨부 파일을 검사하면 Cisco 지문은 파일 형식을 확인하고, 이미지 분석기는 알고리즘을 사용하여 이미지 내용을 분석합니다. 이미지가 다른 파일에 내장된 경우 콘텐츠 스캐너는 해당 파일을 추출합니다. 메시지에 대해 종합적으로 이미지 분석 판정이 계산됩니다. 메시지에 이미지가 포함되어 있지 않으면 "clean(깨끗)" 판정에 매핑되는 점수 "0"을 받게 됩니다. 따라서 이미지가 없는 메시지는 "clean(깨끗)" 판정을 받게 됩니다.

이미지 분석 검사 엔진 구성

GUI에서 이미지 분석을 활성화하려면

단계 **1** **Security Services(**보안 서비스**) > IronPort Image Analysis(IronPort** 이미지 분석**)**로 이동합니다.

단계 **2** **Enable(**활성화**)**을 클릭합니다.

성공 메시지가 표시되고, 이어 판정 설정이 표시됩니다.

이미지 분석 필터 규칙을 사용하면 다음 판정을 기반으로 수행할 작업을 결정할 수 있습니다.

- **Clean(**깨끗**):** 이미지에 부적절한 내용이 없습니다. 메시지에 대해 종합적으로 이미지 분석 판정이 계산되므로, 이미지가 없는 메시지는 검사 시 "clean(깨끗)" 판정을 받게 됩니다.
- **Suspect(**의심**)**: 이미지에 부적절한 내용이 포함되었을 가능성이 있습니다.
- **Inappropriate(**부적절**)**: 이미지에 부적절한 내용이 포함되어 있습니다.

이러한 판정은 부적절한 내용의 확률을 나타내기 위해 이미지 분석기 알고리즘에서 할당한 숫자 값입니다.

다음 값이 권장됩니다.

- Clean: 0~49
- Suspect: 50~74
- Inappropriate: 75~100

다음에 수행할 작업

오탐지 횟수를 줄이는 데 도움이 되는 감도 설정을 구성하여 이미지 검사를 세부적으로 조정할 수 있습니다. 예를 들어, 오탐지를 발견하는 경우 감도 설정을 낮출 수 있습니다. 반대로, 이미지 검사에서 부적절한 내용이 누락되는 것을 발견하는 경우 감도를 높게 설정할 수 있습니다. 감도 설정 범위는 0(감도 없음)에서 100(감도 높음) 사이입니다. 권장 감도 설정은 기본값인 65입니다.

관련 주제

- 이미지 분석 설정 조정, 233 페이지

이미지 분석 설정 조정

단계 **1** **Security Services(**보안 서비스**) > IronPort Image Analysis(IronPort** 이미지 분석**)**로 이동합니다.

단계 **2** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** 이미지 분석 감도의 설정을 구성합니다. 권장 감도 설정은 기본값인 65입니다.

단계 **4** Clean(깨끗), Suspect(의심) 및 Inappropriate(부적절) 판정에 대한 설정을 구성합니다.

값 범위를 구성할 때에는 값이 겹치지 않게 해야 하며 모두 정수를 사용해야 합니다.

단계 **5** 선택적으로, 최소 크기 요구 사항을 충족하지 않는 이미지의 검사를 우회하도록 AsyncOS를 구성합니다(권장). 기본적으로 이 설정은 100픽셀에 대해 구성됩니다. 100픽셀 미만의 이미지 검사는 더러 오탐으로 이어질 수 있습니다.

imageanalysisconfig 명령을 사용하여 CLI에서 이미지 분석 설정을 활성화할 수도 있습니다.

다음에 수행할 작업

관련 주제

- 특정 메시지의 판정 점수 보기, 234 페이지

특정 메시지의 판정 점수 보기

특정 메시지의 판정 점수를 확인하려면 메일 로그를 볼 수 있습니다. 메일 로그에는 이미지 이름 또는 파일 이름과 특정 메시지 첨부 파일의 점수가 표시됩니다. 또한 파일에 있는 이미지가 검사 가능한지에 대한 정보도 표시됩니다. 로그의 정보는 각 이미지가 아니라 각 메시지 첨부 파일에 대한 결과를 설명합니다. 예를 들어, 메시지에 JPEG 이미지가 포함된 zip 첨부 파일이 있다면 로그 항목에는 JPEG의 이름이 아니라 zip 파일의 이름이 포함됩니다. 또한 zip 파일에 여러 이미지가 포함되어 있으면 로그 항목에는 모든 이미지의 최대 점수가 포함됩니다. 검사 불가 알림은 전체 이미지 중 검사할 수 없는 이미지가 있는지 여부를 나타냅니다.

점수를 특정 판정(clean, suspect 또는 inappropriate)으로 변환하는 방법에 대한 정보는 로그에 포함되어 있지 않습니다. 그러나 메일 로그를 사용하여 특정 메시지 전달을 추적할 수 있으므로, 메시지에 대해 수행된 작업으로 메일에 부적절하거나 의심스런 이미지가 포함되었는지 여부를 판단할 수 있습니다.

예를 들어 다음 메일 로그는 이미지 분석 검사 결과 메시지 필터 규칙에 의해 삭제된 첨부 파일을 보여줍니다.

```
Thu Apr 3 08:17:56 2009 Debug: MID 154 IronPort Image Analysis: image 'Unscannable.jpg'
is unscannable.

Thu Apr 3 08:17:56 2009 Info: MID 154 IronPort Image Analysis: attachment
'Unscannable.jpg' score 0 unscannable

Thu Apr 3 08:17:56 2009 Info: MID 6 rewritten to MID 7 by
drop-attachments-where-image-verdict filter 'f-001'

Thu Apr 3 08:17:56 2009 Info: Message finished MID 6 done
```

이미지 분석 결과를 기반으로 작업을 수행하도록 메시지 필터 구성

이미지 분석을 활성화했으면 각 이미지 판정에 대해 서로 다른 작업을 수행하도록 메시지 필터를 만들어야 합니다. 예를 들어 깨끗하다고 판정된 메시지는 전달하고, 내용이 부적절한 것으로 판정된 메시지는 격리할 수 있습니다.

참고 Inappropriate(부적절) 또는 suspect(의심) 판정을 받은 메시지를 삭제하거나 반송하지 않는 것이 좋습니다. 대신, 나중에 검토하고 추세 분석을 더 잘 이해할 수 있도록 위반 메시지의 사본을 격리로 보내십시오.

다음 필터는 내용이 부적절하거나 의심스러운 메시지에 태그를 지정하는 방법을 보여줍니다.

```
image_analysis: if image-verdict == "inappropriate" {

strip-header("Subject");

insert-header("Subject", "[inappropriate image] $Subject");

}

else {

if image-verdict == "suspect" {

strip-header("Subject");


insert-header("Subject", "[suspect image] $Subject");

}

}
```

관련 주제

- 이미지 분석 판정을 기반으로 첨부 파일을 제거하기 위한 콘텐츠 필터 만들기 , 235 페이지

이미지 분석 판정을 기반으로 첨부 파일을 제거하기 위한 콘텐츠 필터 만들기

이미지 분석을 활성화했으면 이미지 분석 판정을 기반으로 첨부 파일을 제거하기 위한 콘텐츠 필터를 만들거나, 각 메시지 판정에 대해 서로 다른 작업을 수행하도록 필터를 구성할 수 있습니다. 예를 들면 부적절한 내용이 포함된 메시지를 격리하도록 설정할 수 있습니다.

이미지 분석 판정을 기반으로 첨부 파일을 제거하려면

단계 **1** Mail Policies(메일 정책) > Incoming Content Filters(수신 콘텐츠 필터)를 클릭합니다.

단계 **2** Add Filter(필터 추가)를 클릭합니다.

단계 **3** 콘텐츠 필터의 이름을 입력합니다.

단계 **4** Actions(작업) 아래에서 **Add Action(**작업 추가**)**을 클릭합니다.

단계 **5** Strip Attachment by File Info(파일 정보로 첨부 파일 제거) 아래에서 **Image Analysis Verdict is(**이미지 분석 판정 결과**)**를 클릭합니다.

단계 **6** 다음 이미지 분석 판정 중에서 선택합니다.

- 의심스러움
- 부적절함
- 의심 또는 부적절함
- 검색할 수 없음
- 정상

이미지 분석 판정을 기반으로 작업 구성

이미지 분석 판정을 기반으로 작업을 구성하려면

단계 **1** Mail Policies(메일 정책) > Incoming Content Filters(수신 콘텐츠 필터)를 클릭합니다.
단계 **2** Add Filter(필터 추가)를 클릭합니다.
단계 **3** 콘텐츠 필터의 이름을 입력합니다.
단계 **4** Conditions(조건) 아래에서 **Add Condition(**조건 추가**)**을 클릭합니다.
단계 **5** Attachment File Info(첨부 파일 정보) 아래에서 **Image Analysis Verdict(**이미지 분석 판정**)**을 클릭합니다.
단계 **6** 다음 판정 중 하나를 선택합니다.

- 의심스러움
- 부적절함
- 의심 또는 부적절함
- 검색할 수 없음
- 정상

단계 **7** **Add Action(**작업 추가**)**을 클릭합니다.
단계 **8** 이미지 분석 판정을 기반으로 메시지에 대해 수행할 작업을 선택합니다.
단계 **9** 변경 사항을 제출 및 커밋합니다.

알림

GUI의 Text Resources(텍스트 리소스) 페이지 또는 `textconfig` CLI 명령을 사용하여 맞춤화 알림 템플릿을 텍스트 리소스로 구성하는 방법을 첨부 파일 필터링 규칙과 함께 사용하는 것은 또 다른 유용한 툴입니다. 알림 템플릿은 비 ASCII 문자를 지원합니다(템플릿을 만드는 동안 인코딩을 선택하라는 프롬프트가 표시됨).

다음 예에서는 먼저 `textconfig` 명령을 사용하여 이름이 `strip.mp3`인 알림 템플릿을 만들고, 이를 알림 메시지의 본문에 삽입합니다. 그런 다음 .mp3 파일이 메시지에서 제거될 때 원래 수신자에게 알림 이메일을 전송하여 .mp3 파일이 삭제되었음을 설명하는 첨부 파일 필터링 규칙을 만듭니다.

```
drop-mp3s:

if (attachment-type == '*/mp3')

{ drop-attachments-by-filetype('Media');

notify ('$EnvelopeRecipients', 'Your mp3 has been removed', '$EnvelopeFrom',

'strip.mp3');

}
```

자세한 내용은 알림 및 알림 복사 작업, 212 페이지를 참고하십시오.

첨부 파일 검사 메시지 필터의 예

다음 예는 첨부 파일에 대해 수행되는 작업을 보여줍니다.

헤더 삽입

이러한 예에서 AsyncOS는 첨부 파일에 지정된 콘텐츠가 포함되어 있으면 헤더를 삽입합니다.

다음 예에서는 메시지에 있는 모든 첨부 파일에서 키워드를 검사합니다. 모든 첨부 파일에 키워드가 있으면 맞춤형 `X-Header`가 삽입됩니다.

```
attach_disclaim:

if (every-attachment-contains('[dD]isclaimer') ) {

insert-header("X-Example-Approval", "AttachOK");

}
```

다음 예에서는 첨부 파일에서 이진 데이터의 패턴을 검사합니다. 필터는 `attachment-binary-contains` 필터 규칙을 사용하여, PDF 문서가 암호화되었음을 나타내는 패턴을 검색합니다. 이진 데이터에 패턴이 있으면 맞춤화 헤더가 삽입됩니다.

```
match_PDF_Encrypt:

if (attachment-filetype == 'pdf' AND

attachment-binary-contains('/Encrypt')){

strip-header ('Subject');

insert-header ('Subject', '[Encrypted] $Subject');

}
```

파일 형식으로 첨부 파일 삭제

다음 예에서는 "실행 가능" 첨부 파일 그룹(`.exe`, `.dll` 및 `.scr`)이 메시지에서 제거되고, 삭제된 파일의 파일 이름을 나열하는(`$dropped_filename` 작업 변수 사용) 텍스트가 메시지에 추가됩니다.

`drop-attachments-by-filetype` 작업은 첨부 파일을 검토하고, 세 글자의 파일 이름 확장명만이 아니라 파일의 지문을 기반으로 첨부 파일을 제거합니다. 단일 파일 형식("mpeg")을 지정할 수도 있고 파일 형식의 모든 구성원("Media")을 가리킬 수도 있습니다.

```
strip_all_exes: if (true) {
```

```
drop-attachments-by-filetype ('Executable', “Removed attachment:

$dropped_filename”);

}
```

다음 예에서는 봉투 발신자가 `example.com` 도메인 내에 있지 않은 메시지로부터 동일한 "실행 가능" 첨부 파일 그룹(`.exe`, `.dll` 및 `.scr`)을 제거합니다.

```
strip_inbound_exes: if (mail-from != "@example\\.com$") {

drop-attachments-by-filetype ('Executable');

}
```

다음 예에서는 봉투 발신자가 `example.com` 도메인 내에 있지 않은 메시지로부터 동일한 "실행 가능" 첨부 파일 그룹(`.exe`, `.dll` 및 `.scr`) 및 특정 파일 형식 구성원("wmf")을 제거합니다.

```
strip_inbound_exes_and_wmf: if (mail-from != "@example\\.com$") {

drop-attachments-by-filetype ('Executable');

drop-attachments-by-filetype ('x-wmf');

}
```

다음 예에서는 더 많은 첨부 파일 이름을 포함하도록 사전 정의된 "실행 가능" 첨부 파일 그룹이 확장됩니다. (이 작업은 첨부 파일의 파일 형식을 검사하지 않습니다.)

```
strip_all_dangerous: if (true) {

drop-attachments-by-filetype ('Executable');

drop-attachments-by-name('(?i)\\.(cmd|pif|bat)$');

}
```

`drop-attachments-by-name` 작업은 비 ASCII 문자를 지원합니다.

참고 `drop-attachments-by-name` 작업은 MIME 헤더에서 캡처된 파일 이름을 기준으로 정규식을 확인합니다. MIME 헤더에서 캡처된 파일 이름 끝에 공백이 포함되어 있을 수 있습니다.

다음 예에서는 첨부 파일이 .exe 실행 가능 파일 형식이 아닌 경우 메시지가 삭제됩니다. 그러나 필터링하려는 파일 형식의 첨부 파일이 하나라도 있으면 필터는 해당 메시지에 대해 작업을 수행하지 않습니다. 예를 들어 다음 필터는 **.exe** 파일 형식이 아닌 첨부 파일이 포함된 메시지를 삭제합니다.

```
exe_check: if (attachment-filetype != "exe") {

drop();
```

```
}
```

한 메시지에 여러 첨부 파일이 있는 경우 첨부 파일 중 적어도 하나가 `.exe` 파일이면 나머지 첨부 파일이 `.exe` 파일이 아니더라도 Email Security Appliance는 메시지를 삭제하지 않습니다.

사전 일치로 첨부 파일 삭제

이 `drop-attachments-where-dictionary-match` 작업은 사전 용어에 대한 일치를 기반으로 첨부 파일을 제거합니다. 첨부 파일로 간주되는 MIME 부분의 용어가 사전 용어와 일치하면(그리고 사용자 정의 임계값이 충족되면) 이메일에서 첨부 파일이 제거됩니다. 다음 예에서는 첨부 파일에서 "secret_words" 사전의 단어가 탐지되는 경우 첨부 파일이 삭제되는 것을 보여줍니다. 일치의 임계값은 1로 설정됩니다.

```
Data_Loss_Prevention: if (true) {

drop-attachments-where-dictionary-match("secret_words", 1);

}
```

보호된 첨부 파일 격리

`attachment-protected` 필터는 메시지의 첨부 파일이 비밀번호로 보호되었는지를 테스트합니다. 첨부 파일이 검사 가능한지를 확인하기 위해 수신 메일에 이 필터를 사용할 수 있습니다. 이 정의에 따르면 포함된 항목 중 한 항목만 암호화되고 나머지는 암호화되지 않은 zip 파일은 보호된 것으로 간주됩니다. 마찬가지로, 공개 비밀번호가 없는 PDF 파일은 비밀번호로 복사 또는 인쇄를 제한하더라도, 보호된 것으로 간주됩니다. 다음 예는 보호된 첨부 파일이 정책 격리로 전송되는 것을 보여줍니다.

```
quarantine_protected:

if attachment-protected

{

quarantine("Policy");

}
```

보호되지 않은 첨부 파일 탐지

`attachment-unprotected` 필터는 메시지의 첨부 파일이 비밀번호로 보호되지 않았는지를 테스트합니다. 이 메시지 필터는 `attachment-protected` 필터를 보완합니다. 보호되지 않은 발신 메일을 탐지하기 위해 발신 메일에 이 필터를 사용할 수 있습니다. 다음 예는 AsyncOS가 발신 리스너에서 보호되지 않은 첨부 파일을 탐지하고 메시지를 격리하는 것을 보여줍니다.

```
quarantine_unprotected:

if attachment-unprotected

{
```

```
quarantine("Policy");

}
```

메시지 필터를 사용하여 메시지 첨부 파일에서 악성 파일 탐지

예를 들어, 다음 메시지 필터 규칙 구문을 사용하여 ETF 엔진에서 악성으로 분류된 메시지 첨부 파일을 탐지하고 해당 메시지에 대해 적절한 조치를 취할 수 있습니다.

구문:

```
Strip_malicious_files: if (file-hash-etf-rule (['etf_source1'], <'file_hash_exception_list'>))

{ file-hash-etf-strip-attachment-action (['etf_source1'], <'file_hash_exception_list>,
 "file stripped from message attachment"); }
```

여기서:

- ‘`file-hash-etf-rule`'은 첨부 파일 정보 메시지 필터 규칙입니다.
- ‘`etf_source1`'은 파일 해시를 기반으로 메시지에서 악성 파일을 탐지하는 데 사용되는 ETF 소스입니다.
- '`file_hash_exception_list`'는 파일 해시 예외 목록의 이름입니다. 파일 해시 예외 목록이 없으면 ""로 표시됩니다.
- '`file-hash-etf-strip-attachment-action`'은 악성 파일이 포함된 메시지에 적용하려는 작업의 이름입니다.

다음 예에서는 ETF 엔진에서 악성으로 탐지된 메시지 첨부 파일이 메시지에 포함된 경우 해당 첨부 파일이 제거됩니다.

```
Strip_Malicious_Attachment: if (true) {file-hash-etf-strip-attachment-action
(['threat_feed_source'], "", “Malicious message attachment has been stripped from
the message.");}
```

CLI를 사용하여 메시지 필터 관리

CLI를 사용하여 메시지 필터용 로깅 옵션을 추가, 삭제, 활성화/비활성화, 가져오기/내보내기 및 설정할 수 있습니다. 아래의 표는 명령 및 하위 명령의 요약을 보여줍니다. 아래의 표는 명령 및 하위 명령의 요약을 보여줍니다.

표 *27:* 메시지 필터 하위 명령

Syntax	설명
`filters`	기본 명령. 이 명령은 인터랙티브 방식으로서, 사용자에게 추가 정보를 묻습니다(예: new, delete, import).
`new`	새 필터를 만듭니다. 위치를 지정하지 않으면 현재 시퀀스에 추가됩니다. 위치를 지정하면 시퀀스의 특정 위치에 필터가 삽입됩니다. 자세한 내용은 새 메시지 필터 만들기, 242 페이지를 참고하십시오.
`delete`	이름 또는 시퀀스 번호로 필터를 삭제합니다. 자세한 내용은 메시지 필터 삭제, 243 페이지를 참고하십시오.
`move`	기존 필터를 다시 정돈합니다. 자세한 내용은 새 메시지 필터 만들기, 242 페이지를 참고하십시오.
`set`	필터를 활성 또는 비활성 상태로 설정합니다. 자세한 내용은 새 메시지 필터 만들기, 242 페이지를 참고하십시오.
`import`	현재 필터 집합을 파일에 저장된 새 집합으로 교체합니다(어플라이언스의 /configuration 디렉터리). 자세한 내용은 새 메시지 필터 만들기, 242 페이지를 참고하십시오.
`export`	현재 필터 집합을 파일로 내보냅니다(어플라이언스의 /configuration 디렉터리). 자세한 내용은 메시지 필터 내보내기, 247 페이지 장을 참조해 주십시오.
`list`	필터에 대한 정보를 나열합니다. 자세한 내용은 메시지 필터 리스트 표시, 247 페이지를 참고하십시오.
`detail`	필터 규칙 자체의 본문을 포함하여 특정 필터에 대한 자세한 정보를 출력합니다. 자세한 내용은 메시지 필터 세부사항 표시, 247 페이지 장을 참조해 주십시오.
`logconfig`	archive() 필터 작업에서의 로그 서브스크립션을 수정할 수 있는 필터의 logconfig 하위 메뉴로 들어갑니다. 자세한 내용은 필터 로그 서브스크립션 구성, 247 페이지의 내용을 참고하십시오.

참고 필터를 적용하려면 commit 명령을 실행해야 합니다.

세 가지 매개변수 유형은 다음과 같습니다.

표 *28:* 필터 관리 매개변수

seqnum	필터 리스트에서의 위치를 기반으로 필터를 나타내는 정수. 예를 들어 *seqnum* 2는 목록에서 두 번째 필터를 나타냅니다.
filtname	필터의 알기 쉬운 이름입니다.

range	range는 둘 이상의 필터를 나타내는 데 사용할 수 있으며 *X Y*의 형식으로 나타납니다. 여기서 X와 Y는 범위를 식별하는 첫 번째와 마지막 *seqnum*입니다. 예를 들어 `2-4`는 두 번째, 세 번째, 네 번째 위치의 필터를 나타냅니다. 끝이 지정되지 않은 리스트를 나타내려면 X 또는 Y를 비워둡니다. 예를 들어 `-4`는 처음 4개 필터를 나타내고 `2-`는 처음을 제외한 모든 필터를 나타냅니다. 필터 리스트의 모든 필터를 나타내려면 all 키워드를 사용할 수도 있습니다.

관련 주제

- 새 메시지 필터 만들기, 242 페이지
- 메시지 필터 삭제, 243 페이지
- 메시지 필터 이동, 243 페이지
- 메시지 필터 활성화 및 비활성화, 243 페이지
- 메시지 필터 가져오기, 246 페이지
- 메시지 필터 내보내기, 247 페이지
- 비 ASCII 문자 집합 보기, 247 페이지
- 메시지 필터 리스트 표시, 247 페이지
- 메시지 필터 세부사항 표시, 247 페이지
- 필터 로그 서브스크립션 구성, 247 페이지
- 메시지 인코딩 변경, 249 페이지
- 샘플 메시지 필터, 250 페이지

새 메시지 필터 만들기

`new [seqnum|filtname|last]`

새 필터를 삽입할 위치를 지정합니다. 생략하거나 last 키워드를 사용하면 입력한 필터가 필터 리스트에 추가됩니다. 시퀀스 번호에는 단절이 허용되지 않습니다. 현재 리스트 경계를 벗어난 *seqnum*은 입력할 수 없습니다. 알 수 없는 *filtname*을 입력하면 유효한 *filtname*, *seqnum* 또는 last를 입력하라는 메시지가 표시됩니다.

필터가 입력된 후 필터 스크립트를 수동으로 입력할 수 있습니다. 입력이 완료되면 자체 줄에 마침표(.)를 입력하여 종료할 수 있습니다.

다음 조건은 오류를 일으킬 수 있습니다.

- 현재 시퀀스 번호 범위를 넘어선 시퀀스 번호
- 고유하지 않은 *filtname*의 필터
- 예약어인 *filtname*의 필터
- 구문 오류가 있는 필터
- 존재하지 않는 시스템 리소스(예: 인터페이스)를 참조하는 작업이 있는 필터

메시지 필터 삭제

`delete [seqnum|filtname|range]`

식별된 필터를 삭제합니다.

다음 조건은 오류를 일으킬 수 있습니다.

- 지정된 필터 이름의 필터가 없음.
- 지정된 시퀀스 번호의 필터가 없음

메시지 필터 이동

`move [seqnum|filtname|rangeseqnum|last]`

첫 번째 매개변수로 식별된 필터를 두 번째 매개변수로 식별된 위치로 이동합니다. 두 번째 파라미터가 last 키워드인 경우 필터가 필터 리스트의 끝으로 이동합니다. 둘 이상의 필터가 이동되는 경우 순서는 바뀌지 않고 그대로 유지됩니다.

다음 조건은 오류를 일으킬 수 있습니다.

- 지정된 필터 이름의 필터가 없음.
- 지정된 시퀀스 번호의 필터가 없음
- 현재 시퀀스 번호 범위를 넘어선 시퀀스 번호
- 이동 결과 시퀀스 변화가 없는 경우

메시지 필터 활성화 및 비활성화

지정된 메시지 필터는 활성 상태 또는 비활성 상태이며, 유효한 상태 또는 유효하지 않은 상태입니다. 메시지 필터는 활성이며 유효한 경우에만 처리에 사용됩니다. 기존 필터를 활성에서 비활성으로 또는 그 반대로 변경하려면 CLI를 사용합니다. 존재하지 않는(또는 제거된) 리스너나 인터페이스를 참조하는 필터는 유효하지 않습니다.

참고 필터가 비활성 상태인지를 구문으로 파악할 수 있습니다. 비활성 필터의 경우 AsyncOS는 필터 이름 뒤의 콜론을 느낌표로 변경합니다. 필터를 입력하거나 가져올 때 이 구문을 사용하면 AsyncOS는 해당 필터를 비활성 상태로 표시합니다.

예를 들어 "filterstatus"라는 다음과 같은 필터를 입력합니다. 그런 다음 `filter -> set` 하위 명령을 사용하여 비활성 상태로 전환합니다. 필터의 세부사항이 표시될 때 콜론이 느낌표로(그리고 다음 예에서 굵은 글꼴로) 변경된 것을 알 수 있습니다.

```
mail3.example.com> filters


Choose the operation you want to perform:

- NEW - Create a new filter.
```

```
- IMPORT - Import a filter script from a file.
[]> new
Enter filter script. Enter '.' on its own line to end.
filterstatus: if true{skip-filters();}
.
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list
Num Active Valid Name
1 Y Y filterstatus
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> set
```

```
Enter the filter name, number, or range:
[all]> all
Enter the attribute to set:
[active]> inactive
1 filters updated.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> detail
Enter the filter name, number, or range:
[]> all
Num Active Valid Name
1 N Y filterstatus
filterstatus! if (true) {
skip-filters();
}
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
```

```
- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>
```

관련 주제

- 메시지 필터 활성화 또는 비활성화, 246 페이지

메시지 필터 활성화 또는 비활성화

`set [seqnum|filtname|range] active|inactive`

식별된 필터를 지정된 상태로 설정합니다. 사용 가능한 상태는 다음과 같습니다.

- active: 선택한 필터의 상태를 활성으로 설정합니다.
- inactive: 선택한 필터의 상태를 비활성으로 설정합니다.

다음 조건은 오류를 일으킬 수 있습니다.

- 지정된 *filtname*의 필터가 없음
- 지정된 시퀀스 번호의 필터가 없음

참고 비활성 상태의 필터는 구문에도 표시됩니다. 레이블(필터의 이름) 뒤의 콜론이 느낌표(!)로 바뀝니다.). CLI에서 수동으로 입력한 필터나 가져온 필터에 이 구문이 포함되어 있으면 자동으로 비활성으로 표시됩니다. 예를 들면 mailfrompm: 대신 mailfrompm!가 표시됩니다.

메시지 필터 가져오기

`import filename`

처리해야 할 필터를 포함하는 파일의 이름. 이 파일은 루트 디렉터리의 configuration 디렉터리에 있어야 합니다(`interfaceconfig` 명령으로 인터페이스에 대한 FTP/SCP 액세스를 활성화한 경우). 정보가 수집되고 구문 분석되며, 오류가 보고됩니다. 가져온 필터는 현재 필터 집합에 있는 모든 필터를 교체합니다. 자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지 항목을 참조하십시오. 현재 필터 리스트를 내보내고(메시지 필터 내보내기, 247 페이지 참조), 파일을 수정한 후 가져오는 것을 고려해보십시오.

메시지 필터를 가져올 때, 사용된 인코딩을 선택하라는 프롬프트가 표시됩니다.

다음 조건은 오류를 일으킬 수 있습니다.

- 파일이 없음
- 고유하지 않은 이름을 가진 필터
- 예약어인 *filtname*의 필터
- 구문 오류가 있는 필터
- 존재하지 않는 시스템 리소스(예: 인터페이스)를 참조하는 작업이 있는 필터

메시지 필터 내보내기

`export filename[seqnum|filtname|range]`

기존 필터의 서식이 지정된 버전을 어플라이언스 FTP/SCP 루트 디렉터리의 configuration 디렉터리에 있는 파일로 출력합니다. 자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지 항목을 참조하십시오.

메시지 필터를 내보낼 때, 사용된 인코딩을 선택하라는 프롬프트가 표시됩니다.

다음 조건은 오류를 일으킬 수 있습니다.

- 지정된 필터 이름의 필터가 없음.
- 지정된 시퀀스 번호의 필터가 없음

비 **ASCII** 문자 집합 보기

시스템은 비 ASCII 문자가 포함된 필터를 CLI에서 UTF-8로 표시합니다. 터미널/디스플레이에서 UTF-8을 지원하지 않으면 필터를 읽을 수 없습니다.

필터에 있는 비 ASCII 문자를 관리하는 가장 좋은 방법은 필터를 텍스트 파일에서 수정한 후 이 텍스트 파일을 다시 어플라이언스로 가져오는 것입니다(메시지 필터 가져오기, 246 페이지 참조).

메시지 필터 리스트 표시

`list [seqnum|filtname|range]`

필터 본문은 출력하지 않은 채 식별된 필터에 대한 요약 정보를 표 형식으로 보여줍니다. 다음과 같은 정보가 표시됩니다.

- 필터 이름
- 필터 시퀀스 번호
- 필터의 활성/비활성 상태
- 필터의 유효/유효하지 않음 상태

다음 조건은 오류를 일으킬 수 있습니다.

- 잘못된 범위 형식

메시지 필터 세부사항 표시

`detail [seqnum|filtname|range]`

필터 본문 및 추가적인 상태 정보를 포함하여 식별된 필터에 대한 모든 정보를 제공합니다.

필터 로그 서브스크립션 구성

`logconfig`

archive() 작업으로 생성된 사서함 파일에 대한 필터 로그 옵션을 구성할 수 있는 하위 메뉴로 들어갑니다. 이러한 옵션은 일반적인 logconfig 명령에 사용되는 것과 매우 유사하지만, 로그를 만들거나 삭제하려면 로그를 참조하는 필터를 추가 또는 제거해야 합니다.

각 필터 로그 서브스크립션의 기본값은 다음과 같으며, logconfig 하위 명령을 사용하여 수정할 수 있습니다.

- 검색 방법 - FTP Poll
- 파일 크기 - 10MB
- 최대 파일 수 - 10

자세한 내용은 "로깅" 장을 참조해 주십시오.

```
mail3.example.com> filters

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]> logconfig

Currently configured logs:

1. "joesmith" Type: "Filter Logs" Retrieval: FTP Poll

Choose the operation you want to perform:

- EDIT - Modify a log setting.

[]> edit

Enter the number of the log you wish to edit.

[]> 1

Choose the method to retrieve the logs.

1. FTP Poll

2. FTP Push

3. SCP Push
```

```
[1]> 1

Please enter the filename for the log:

[joesmith.mbox]>

Please enter the maximum file size:

[10485760]>

Please enter the maximum number of files:

[10]>

Currently configured logs:

1. "joesmith" Type: "Filter Logs" Retrieval: FTP Poll

Enter "EDIT" to modify or press Enter to go back.

[]>
```

메시지 인코딩 변경

메시지 처리 중 메시지 제목과 바닥글의 인코딩 수정과 관련하여 AsyncOS의 동작을 설정하려면 `localeconfig` 명령을 사용할 수 있습니다.

```
example.com> localeconfig

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]> setup

If a header is modified, encode the new header in the same encoding as the message body?
(Some MUAs incorrectly handle headers encoded in a different encoding than the body.
However, encoding a modified header in the same encoding as the message body may cause
certain
characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or
modified,
impose the encoding of the body on the header during processing and final representation
of the message?
(Many MUAs create non-RFC-compliant headers that are then handled in an undefined way.
Some MUAs handle headers encoded in character sets that differ from that of the main body
in an incorrect way.
Imposing the encoding of the body on the header may encode the header more precisely.
This will be used to interpret the content of headers for processing, it will not modify
or rewrite the
header unless that is done explicitly as part of the processing.) [Y]>

Disclaimers (as either footers or headings) are added in-line with the message body whenever
 possible.
```

```
However, if the disclaimer is encoded differently than the message body, and if imposing a
 single encoding
will cause loss of characters, it will be added as an attachment. The system will always
try to use the
message body's encoding for the disclaimer. If that fails, the system can try to edit the
message body to
use an encoding that is compatible with the message body as well as the disclaimer. Should
 the system try to
re-encode the message body in such a case? [Y]>

If the disclaimer that is added to the footer or header of the message generates an error
when decoding the message body,
it is added at the top of the message body. This prevents you to rewrite a new message
content that must merge with
the original message content and the header/footer-stamp. The disclaimer is now added as
an additional MIME part
that displays only the header disclaimer as an inline content, and the rest of the message
 content is split into
separate email attachments. Should the system try to ignore such errors when decoding the
message body? [N]>

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body
is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]>
```

첫 번째 프롬프트는 헤더가 변경된 경우(예: 필터를 통해) 헤더의 인코딩을 메시지 본문의 인코딩에 맞게 변경해야 할지 여부를 결정합니다.

두 번째 프롬프트는 헤더가 문자 집합으로 적절히 태그 처리되지 않은 경우 어플라이언스가 헤더에 메시지 본문의 인코딩을 적용해야 할지 여부를 제어합니다.

세 번째 프롬프트는 메시지 본문에서 면책조항 스탬프(및 다중 인코딩)의 작동 방식을 구성하는 데 사용됩니다. 자세한 내용은 "텍스트 리소스" 장의 "면책조항 스탬프 및 다중 인코딩" 섹션을 참조하십시오.

네 번째 프롬프트는 메시지 본문을 디코딩하는 동안 오류가 발생하는 경우 면책조항 스탬프의 동작을 구성하는 데 사용됩니다. 'Yes(예)'를 선택하면 디코딩 오류가 무시되고 면책조항이 스탬프 처리됩니다. 'No(아니요)'를 선택하면 면책조항 텍스트가 메시지에 첨부 파일로 추가됩니다.

샘플 메시지 필터

다음 예에서는 filter 명령을 사용하여 세 가지 새로운 필터를 만듭니다.

- 첫 번째 필터 이름은 **`big_messages`**입니다. 이 필터는 10메가바이트보다 큰 메시지를 삭제하기 위해 `body-size` 규칙을 사용합니다.
- 두 번째 필터의 이름은 **`no_mp3s`**입니다. 이 필터는 파일 이름 확장명이 `.mp3`인 첨부 파일이 포함된 메시지를 삭제하기 위해 `attachment-filename` 규칙을 사용합니다.
- 세 번째 필터의 이름은 **`mailfrompm`**입니다. 이 필터는 `postmaster@example.com`의 모든 메일을 검사하고 `administrator@example.com`에 숨은 참조로 보내기 위해 mail-from 규칙을 사용합니다.

`filter -> list` 하위 명령을 사용하여 필터가 나열되면 활성 상태이고 유효한지 확인합니다. `move` 하위 명령을 사용하여 첫 번째와 마지막 필터의 위치를 전환합니다. 마지막으로, 필터가 적용되도록 변경 사항을 커밋합니다.

```
mail3.example.com> filters

Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

big_messages:

if (body-size >= 10M) {

drop();

}

.

1 filters added.

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]> new

Enter filter script. Enter '.' on its own line to end.

no_mp3s:

if (attachment-filename == '(?i)\\.mp3$') {

drop();

}

.
```

```
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new
Enter filter script. Enter '.' on its own line to end.
mailfrompm:
if (mail-from == "^postmaster$")
{ bcc ("administrator@example.com");}
.
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list
Num Active Valid Name
```

```
1 Y Y big_messages

2 Y Y no_mp3s

3 Y Y mailfrompm

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]> move

Enter the filter name, number, or range to move:

[]> 1

Enter the target filter position number or name:

[]> last

1 filters moved.

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]> list
```

```
Num Active Valid Name
1 Y Y no_mp3s
2 Y Y mailfrompm
3 Y Y big_messages
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> move
Enter the filter name, number, or range to move:
[]> 2
Enter the target filter position number or name:
[]> 1
1 filters moved.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
```

```
- ROLLOVERNOW - Roll over a filter log file.

[]> list

Num Active Valid Name

1 Y Y mailfrompm

2 Y Y no_mp3s

3 Y Y big_messages

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>

mail3.example.com> commit

Please enter some comments describing your changes:

[]> entered and enabled 3 filters: no_mp3s, mailfrompm, big_messages

Do you want to save the current configuration for rollback? [Y]> n

Changes committed: Fri May 23 11:42:12 2014 GMT
```

메시지 필터 예

이 섹션에는 각 필터에 대한 간단한 설명과 함께 필터의 몇 가지 실제 예가 포함되어 있습니다.

관련 주제

- 오픈 릴레이 방지 필터, 256 페이지
- 정책 시행 필터, 256 페이지
- 라우팅 및 도메인 스푸핑, 260 페이지

오픈 릴레이 방지 필터

이 필터는 이메일 주소에 %, 별도의 @ 및 ! 문자를 사용하는 메시지를 반송합니다.

- `user%otherdomain@validdomain`
- `user@otherdomain@validdomain:`
- `domain!user@validdomain`

```
sourceRouted:

if (rcpt-to == "(%|@|!)(.*)@") {

bounce();

}
```

어플라이언스는 기존의 Sendmail/Qmail 시스템 공격에 종종 사용되는 이러한 서드파티 릴레이 해킹에 취약하지 않습니다. 이러한 기호 중 다수는(예: %) 완전히 합법적인 이메일 주소의 일부이므로, 어플라이언스는 이들을 유효한 주소로 수락하고, 구성된 수신자 목록을 기준으로 확인하고, 다음 내부 서버로 전달합니다. Cisco 어플라이언스는 이러한 메시지를 외부로 릴레이하지 않습니다.

이러한 필터는 이 메시지 유형의 릴레이를 허용하도록 잘못 구성된 오픈 소스 MTA를 가지고 있을 수 있는 사용자를 보호하기 위해 배치됩니다.

참고 이 주소 유형을 처리하도록 리스너를 구성할 수도 있습니다. 자세한 내용은 웹 인터페이스를 사용하여 리스너를 만들어 연결 요청 수신 대기, 75 페이지를 참조하십시오.

정책 시행 필터

제목 기반 알림 필터

이 필터는 제목에 특정 단어가 포함되었는지를 기반으로 알림을 전송합니다.

```
search_for_sensitive_content:

if (Subject == "(?i)plaintiff|lawsuit|judge" ) {

notify ("admin@company.com");

}
```

경쟁사로 전송되는 메일 검사 및 숨은 참조 처리

이 필터는 경쟁사로 전송되는 메시지를 검사하여 숨은 참조 처리합니다. 사전과 `header-dictionary-match()` 규칙을 사용하여 좀 더 유연한 경쟁사 목록을 지정할 수 있습니다 (Dictionary(사전) 규칙, 177 페이지 참고).

```
competitorFilter:

if (rcpt-to == '@competitor1.com|@competitor2.com') {

bcc-scan('legal@example.com');

}
```

특정 사용자 필터 차단

특정 주소의 이메일을 차단하려면 이 필터를 사용합니다.

```
block_harrasing_user:

if (mail-from == "ex-employee@hotmail\\.com") {

notify ("admin@company.com");

drop ();

}
```

메시지 보관 및 삭제 필터

일치하는 파일 형식이 있는 메시지만 기록 및 삭제합니다.

```
drop_attachments:

if (mail-from != "user@example.com") AND (attachment-filename ==

'(?i)\\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$')

{

archive("Drop_Attachments");

insert-header("X-Filter", "Dropped by: $FilterName MID: $MID");

drop-attachments-by-name("\\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$");
```

```
}
```

큰 "To:" 헤더 필터

"To" 헤더가 매우 큰 메시지를 찾습니다.

별도의 안전을 위해 drop()을 활성화 또는 비활성화하여 적절한 작업을 확인하려면 `archive()` 줄을 사용합니다.

```
toTooBig:

if(header('To') == "^.{500,}") {

archive('tooTooBigdropped');

drop();

}
```

빈 "From:" 필터

빈 "From:" 헤더를 식별합니다.

이 필터는 다양한 형식의 빈 "from" 주소를 줄일 수 있습니다.

```
blank_mail_from_stop:

if (recv-listener == "InboundMail" AND header("From") == "^$|<\\s*>") {

drop ();

}
```

빈 envelope from의 메시지를 삭제하려는 경우에도 이 필터를 사용합니다.

```
blank_mail_from_stop:

if (recv-listener == "InboundMail" AND (mail-from == "^$|<\\s*>" OR header ("From") ==
"^$|<\\s*>"))

{

drop ();
}
```

SRBS 필터

SenderBase Reputation 필터

```
note_bad_reps:
if (reputation < -2) {
strip-header ('Subject');
```

```
insert-header ('Subject', '***BadRep $Reputation *** $Subject');
}
```

SRBS 필터 변경

특정 도메인에 대한 SBRS(SenderBase Reputation Score) 임계값을 변경합니다.

```
mod_sbrs:
if ( (rcpt-count == 1) AND (rcpt-to == "@domain\\.com$") AND (reputation < -2) ) {
drop ();
}
```

파일 이름 Regex 필터

이 필터는 메시지 본문의 크기 범위를 지정하고, 정규식과 일치하는 첨부 파일을 찾습니다("readme.zip", "readme.exe", "attach.exe" 등의 파일 이름).

```
filename_filter:
if ((body-size >= 9k) AND (body-size <= 20k)) {
if (body-contains ("(?i)(readme|attach|information)\\.(zip|exe)$")) {
drop ();

}

}
```

헤더에 SenderBase Reputation 점수 표시 헤더

메일 로그에 나타나도록 헤더를 로깅해야 합니다("로깅" 장 참조).

```
Check_SBRS:

if (true) {

insert-header('X-SBRS', '$Reputation');

}
```

헤더에 정책 삽입 필터

연결을 수락한 메일 플로우 정책을 표시합니다.

```
Policy_Tracker:

if (true) {

insert-header ('X-HAT', 'Sender Group $Group, Policy $Policy applied.');

}
```

너무 많은 수신자 반송 필터

셋 이상의 고유한 도메인으로부터 수신자가 50명이 넘는 모든 아웃바운드 이메일 메시지를 반송합니다.

```
bounce_high_rcpt_count:

if ( (rcpt-count > 49) AND (rcpt-to != "@example\\.com$") ) {

bounce-profile ("too_many_rcpt_bounce"); bounce ();

}
```

라우팅 및 도메인 스푸핑

가상 게이트웨이 필터 사용

가상 게이트웨이를 사용하여 트래픽을 분할합니다. 시스템에 'public1'과 'public2'라는 두 인터페이스가 있으며 기본 전달 인터페이스는 'public1'이라고 가정합니다. 이렇게 하면 모든 아웃바운드 트래픽이 두 번째 인터페이스를 지나게 됩니다. 반송 및 기타 유사한 메일 유형은 필터를 지나가지 못하므로 public1에서 전달됩니다.

```
virtual_gateways:

if (recv-listener == "OutboundMail") {

alt-src-host ("public2");

}
```

전달과 수신에 동일한 리스너 필터

전달과 수신에 동일한 리스너를 사용합니다. 이 필터를 사용하면 퍼블릭 리스너 "listener1"에서 수신한 메시지를 인터페이스 "listener1" 외부로 전송할 수 있습니다(구성된 각 퍼블릭 리스너에 대해 고유한 필터를 설정해야 함).

```
same_listener:

if (recv-inj == 'listener1') {

alt-src-host('listener1');
```

```
}
```

단일 리스너 필터

필터가 단일 리스너에서 작동하도록 합니다. 예를 들면 시스템 전체에서 수행하는 대신 메시지 필터 처리를 위한 단일 특정 리스너를 지정합니다.

```
textfilter-new:

if (recv-inj == 'inbound' and body-contains("some spammy message")) {

alt-rcpt-to ("spam.quarantine@spam.example.com");

}
```

스푸핑된 도메인 삭제 필터(단일 리스너)

스푸핑된 도메인의 이메일을 삭제합니다(내부 주소에서 온 것처럼 가장, 단일 리스너에서 작동). 아래의 IP 주소는 mycompany.com에 대한 허구 도메인을 나타냅니다.

```
DomainSpoofed:

if (mail-from == "mycompany\\.com$") {

if ((remote-ip != "1.2.") AND (remote-ip != "3.4.")) {

drop();

}

}
```

스푸핑된 도메인 삭제 필터(다중 리스너)

위와 같지만, 다중 리스너로 작동합니다.

```
domain_spoof:

if ((recv-listener == "Inbound") and (mail-from == "@mycompany\\.com")) {

archive('domain_spoof');

drop ();

}
```

또 다른 스푸핑된 도메인 삭제 필터

요약: 안티 도메인 스푸핑 필터

```
reject_domain_spoof:
```

```
if (recv-listener == "MailListener") {

insert-header("X-Group", "$Group");

if ((mail-from == "@test\\.mycompany\\.com") AND (header("X-Group") != "RELAYLIST")) {

notify("me@here.com");

drop();

strip-header("X-Group");

}
```

루프 탐지 필터

이 필터는 메일 루프를 일으키는 것이 무엇인지를 탐지하고 결정하고 중단하는 데 사용됩니다. 이 필터는 Exchange Server 등에서 컨피그레이션 문제를 확인하는 데 도움이 될 수 있습니다.

```
External_Loop_Count:

if (header("X-ExtLoop1")) {


if (header("X-ExtLoopCount2")) {

if (header("X-ExtLoopCount3")) {

if (header("X-ExtLoopCount4")) {

if (header("X-ExtLoopCount5")) {

if (header("X-ExtLoopCount6")) {

if (header("X-ExtLoopCount7")) {

if (header("X-ExtLoopCount8")) {

if (header("X-ExtLoopCount9")) {

notify ('joe@example.com');

drop();

}

else {insert-header("X-ExtLoopCount9", "from
$RemoteIP");}}

else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}
```

```
else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}

else {insert-header("X-ExtLoop1", "1");

}
```

참고 기본적으로 AsyncOS는 자동으로 메일 루프를 탐지하고 100회 이후 메시지를 삭제합니다.

검사 동작 구성

검사 매개변수를 구성하여 본문 및 첨부 파일 검사의 동작(예: 검사 중 건너뛸 첨부 파일 형식)을 제어할 수 있습니다. 이러한 매개변수를 구성하려면 Scan Behavior(검사 동작) 페이지 또는 `scanconfig` 명령을 사용합니다. 검사 동작 설정은 전역 설정입니다. 즉, 모든 검사의 동작에 영향을 미칩니다.

참고 zip 또는 압축 파일에 포함되어 있을 수 있는 MIME 유형을 검사하려면 검사 리스트에 'compressed', 'zip' 또는 'application/zip'을 포함해야 합니다.

단계 **1** **Security Services(**보안 서비스**)** > **Scan Behavior(**검사 동작**)**를 클릭합니다.

단계 **2** 첨부 파일 형식 매핑을 정의합니다. 다음 중 하나를 수행합니다.

- 새 첨부 파일 형식 매핑을 추가합니다. **Add Mapping(**매핑 추가**)**을 클릭합니다.
- 컨피그레이션 파일을 사용하여 첨부 파일 형식 매핑 리스트를 가져옵니다. **Import List(**리스트 가져오기**)**를 클릭하고, configuration 디렉터리에서 원하는 컨피그레이션 파일을 가져옵니다.

  참고 이 단계를 수행하려면 어플라이언스의 configuration 디렉터리에 컨피그레이션 파일이 있어야 합니다. 구성 파일 관리, 935 페이지를 참조하십시오.

- 기존 첨부 파일 형식 매핑을 수정하려면 **Edit(**수정**)**를 클릭합니다.

단계 **3** 전역 설정을 구성합니다. 다음을 수행합니다.

a) Global Settings(전역 설정)에서 **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

b) 원하는 필드를 수정합니다.

필드	설명
Action for attachments with MIME types / fingerprints in table above(위의 표에 있는 **MIME** 유형/지문이 포함된 첨부 파일에 대한 작업**)**	첨부 파일 형식 매핑에 정의된 첨부 파일 형식을 검사할지 또는 건너뛸지를 선택합니다.

필드	설명
Maximum depth of attachment recursion to scan(검사할 첨부 파일 재귀의 최대 깊이**)**	검사할 재귀 첨부 파일의 최대 레벨을 지정합니다.
Maximum attachment size to scan(검사할 최대 첨부 파일 크기**)**	검사할 첨부 파일의 최대 크기를 지정합니다.
Attachment Metadata scan(첨부 파일 메타데이터 검사**)**	첨부 파일의 메타데이터를 검사할지 또는 건너뛸지를 지정합니다.
Attachment scanning timeout(첨부 파일 검사 시간 초과**)**	검사 시간 초과 기간을 지정합니다.
Assume attachment matches pattern if not scanned for any reason(어떤 이유로든 검사되지 않은 경우 첨부 파일이 패턴과 일치한다고 가정**)**	검사되지 않은 첨부 파일이 검색 패턴과 일치한다고 간주할지 여부를 지정합니다.
Action when message cannot be deconstructed to remove specified attachments(메시지를 분해하여 지정된 첨부 파일을 제거할 수 없는 경우의 작업**)**	메시지를 분해하여 지정된 첨부 파일을 제거할 수 없는 경우 수행할 작업을 지정합니다.
Bypass all filters in case of a content or message filter error(콘텐츠 또는 메시지 필터 오류가 발생할 경우 모든 필터 우회**)**	콘텐츠 또는 메시지 필터 오류가 발생할 경우 모든 필터를 우회할지 여부를 지정합니다.
Encoding to use when none is specified(지정된 인코딩이 없는 경우 사용할 인코딩**)**	지정된 인코딩이 없는 경우 사용할 인코딩을 지정합니다.
Convert opaque-signed messages to clear-signed (S/MIME unpacking)(불투명하게 서명된 메시지를 명확하게 서명된 메시지로 변환**(S/MIME** 압축 해제**))**	불투명하게 서명된 메시지를 명확하게 서명된 메시지로 변환(S/MIME 압축 해제)할지 여부를 지정합니다.
URL 필터링 작업 도중 발생한 디코딩 오류로 인해 검사할 수 없는 메시지에 대한 작업	URL 필터링 작업 중에 디코딩 오류가 발견되어 콘텐츠 스캐너에서 메시지를 검사할 수 없는 경우 수행할 작업을 지정합니다.
추출 오류로 인해 검사 불가 메시지가 나타난 경우의 작업	첨부 파일 추출 오류로 인해 콘텐츠 스캐너에서 메시지를 검사할 수 없는 경우 수행할 작업을 지정합니다.
RFC 위반으로 인해 검사 불가 메시지가 나타난 경우의 작업	RFC 위반으로 인해 콘텐츠 스캐너에서 메시지를 검사할 수 없는 경우 수행할 작업을 지정합니다.

c) **Submit(**제출**)**을 클릭합니다.

단계 **4** (선택 사항) 콘텐츠 스캐너 파일을 수동으로 업데이트합니다. **Current Content Scanner files(**현재 콘텐츠 스캐너 파일**)** 아래에서 **Update Now(**지금 업데이트**)**를 클릭합니다.

일반적으로 이러한 파일은 업데이트 서버를 통해 자동으로 업데이트됩니다.

참고 CLI에서 `contentscannerupdate`를 사용하여 이러한 파일을 수동으로 업데이트할 수도 있습니다.

단계 **5** 변경 사항을 커밋합니다.

검사 불가 메시지에 대한 메시지 처리 작업 구성

이제 어플라이언스의 콘텐츠 스캐너는 다음과 같은 이유로 검사되지 않은 메시지를 처리할 수 있습니다.

- 파일 추출 실패
- RFC 위반
- URL 필터링 작업 중에 발견된 디코딩 오류

콘텐츠 스캐너에서 검사되지 않은 메시지에 대해 다음 메시지 처리 작업 중 하나를 구성할 수 있습니다.

- 메시지 삭제
- 있는 그대로 메시지 전달
- 정책 격리에 메시지 전송

웹 인터페이스의 Security Services > Scan Behavior(검사 동작)에서 **Edit Global Settings(**전역 설정 수정**)** 버튼을 클릭하여 콘텐츠 스캐너에서 검사되지 않은 메시지에 대한 메시지 처리 작업을 활성화하고 구성할 수 있습니다.

메시지 전달

메시지를 전달하려는 경우 다음 추가 작업을 수행할 수 있습니다.

- 메시지 제목 수정
- 메시지에 맞춤형 헤더 추가
- 메시지 수신자 수정
- 대체 대상 호스트로 메시지 전송

참고 이러한 작업은 상호 배타적이지 않습니다. 사용자 그룹에 대한 서로 다른 처리 요구에 따라 서로 다른 수신 또는 발신 정책 내에서 각기 다르게 일부 또는 전체를 결합할 수 있습니다.

메시지 제목 수정

사용자가 메시지를 쉽게 식별하고 정렬할 수 있도록 특정 텍스트 문자열을 앞이나 뒤에 추가하여 콘텐츠 스캐너에서 검사되지 않은 메시지의 텍스트를 변경할 수 있습니다.

참고 "Modify message subject(메시지 제목 수정)" 필드에서는 공백이 무시되지 않습니다. 이 필드에 입력하는 텍스트의 뒤(뒤에 추가하는 경우) 또는 앞(앞에 추가하는 경우)에 공백을 추가하여 메시지의 원래 제목과 추가된 텍스트를 구분합니다. 예를 들어 앞에 추가하는 경우 `[WARNING: UNSCANNABLE EXTRACTION FAILURE]` 텍스트를 몇몇 후행 공백과 함께 추가합니다.

콘텐츠 스캐너에서 검사되지 않은 메시지의 제목에 추가되는 기본 텍스트입니다.

이유	제목에 추가할 기본 텍스트
추출 실패	[WARNING: UNSCANNABLE EXTRACTION FAILED(경고: 검사 불가 추출 실패)]
RFC 위반	[WARNING: UNSCANNABLE RFC NON-COMPLIANT(경고: 검사 불가 RFC 비호환)]
URL 필터링 작업 중에 발견된 디코딩 오류	[WARNING: DECODING ERRORS WHEN APPLYING URL FILTERING ACTIONS(경고: URL 필터링 작업을 적용할 때 디코딩 오류)]

메시지에 맞춤형 헤더 추가

콘텐츠 스캐너에서 검사되지 않은 모든 메시지에 추가할 맞춤형 헤더를 정의할 수 있습니다. **Yes(**예**)**를 클릭하고 헤더 이름과 텍스트를 정의합니다.

메시지 수신자 수정

콘텐츠 스캐너에서 검사되지 않은 메시지가 다른 주소로 전달되도록 메시지 수신자를 수정할 수 있습니다. **Yes(**예**)**를 클릭하고 새 수신자 주소를 입력합니다.

대체 대상 호스트로 메시지 전송

콘텐츠 스캐너에서 검사되지 않은 메시지에 대해 다른 수신자 또는 대상 호스트로 알림을 보내도록 선택할 수 있습니다. **Yes(**예**)**를 클릭하고 대체 주소 또는 호스트를 입력합니다.

예를 들어 후속 검사를 위해 콘텐츠 스캐너에서 검사되지 않은 메시지를 관리자의 사서함 또는 특수 메일 서버로 라우팅할 수 있습니다. 다중 수신자 메시지의 경우 단일 사본만 대체 수신자에게 전송됩니다.

정책 격리에 메시지 전송

격리를 위해 플래그를 지정한 경우 콘텐츠 스캐너에서 검사되지 않은 메시지는 계속해서 이메일 파이프라인의 나머지를 지나갑니다. 하나 이상의 격리에 대해 플래그가 지정된 메시지는 파이프라인

의 끝에 도달하면 해당 큐에 추가됩니다. 메시지가 파이프라인의 끝에 도달하지 못하면 격리에 배치되지 않습니다.

예를 들어, 콘텐츠 필터로 인해 메시지가 삭제되거나 반송되면 해당 메시지는 격리되지 않습니다.

참고 어플라이언스에 정책 격리가 정의되지 않은 경우 메시지를 격리로 전송할 수 없습니다.

메시지를 정책 격리로 전송하려는 경우 다음 추가 작업을 수행할 수 있습니다.

- 메시지 제목 수정
- 메시지에 맞춤형 헤더 추가

메시지 제목 헤더 수정

사용자가 메시지를 쉽게 식별하고 정렬할 수 있도록 특정 텍스트 문자열을 앞이나 뒤에 추가하여 정책 격리로 전송되는 메시지의 텍스트를 변경할 수 있습니다.

참고 "Modify message subject(메시지 제목 수정)" 필드에서는 공백이 무시되지 않습니다. 이 필드에 입력하는 텍스트의 뒤(뒤에 추가하는 경우) 또는 앞(앞에 추가하는 경우)에 공백을 추가하여 메시지의 원래 제목과 추가된 텍스트를 구분합니다. 예를 들어 앞에 추가하는 경우 `[WARNING: UNSCANNABLE EXTRACTION FAILURE]` 텍스트를 몇몇 후행 공백과 함께 추가합니다.

정책 격리로 전송되는 메시지의 제목에 추가되는 기본 텍스트입니다.

이유	제목에 추가할 기본 텍스트
추출 실패	[WARNING: UNSCANNABLE EXTRACTION FAILED(경고: 검사 불가 추출 실패)]
RFC 위반	[WARNING: UNSCANNABLE RFC NON-COMPLIANT(경고: 검사 불가 RFC 비호환)]
URL 필터링 작업 중에 발견된 디코딩 오류	[WARNING: DECODING ERRORS WHEN APPLYING URL FILTERING ACTIONS(경고: URL 필터링 작업을 적용할 때 디코딩 오류)]

메시지에 맞춤형 헤더 추가

정책 격리로 전송되는 모든 메시지에 추가할 맞춤형 헤더를 정의할 수 있습니다. **Yes(**예**)**를 클릭하고 헤더 이름과 텍스트를 정의합니다.

10 장

메일 정책

이 장에는 다음 섹션이 포함되어 있습니다.

메일 정책 개요

Email Security Appliance는 메일 정책을 사용하여 사용자가 주고받는 메시지에 대해 조직의 정책을 시행합니다. 이러한 정책은 조직의 네트워크로 들어오거나 네트워크에서 나가지 못하게 하려는 의심스런 콘텐츠, 민감한 콘텐츠 또는 악의적인 콘텐츠 유형을 지정하는 규칙의 집합입니다. 콘텐츠에는 다음이 포함될 수 있습니다.

- 스팸
- 합법적인 마케팅 메시지
- 그레이메일
- 바이러스
- 피싱 및 기타 대상 지정 메일 공격
- 기밀 회사 데이터
- 개인 식별 가능 정보

조직 내 각 사용자 그룹의 서로 다른 보안 요구를 충족하는 여러 정책을 만들 수 있습니다. Email Security Appliance는 이러한 정책에 정의된 규칙을 사용하여 각 메시지를 검사하고, 필요 시 사용자 보호를 위한 작업을 수행합니다. 예를 들면 정책에서 경영진에 대해서는 의심스런 스팸 메시지가 전달되는 것을 막고 IT 직원에게는 내용을 경고하는 수정된 제목과 함께 전달할 수 있습니다. 또는 System Administrator(시스템 관리자) 그룹 외에는 모든 사용자에 대해 위험한 실행 첨부 파일을 삭제할 수 있습니다.

사용자 단위로 메일 정책을 시행하는 방법

프로시저

	명령 또는 동작	목적
단계 **1**	Email Security Appliance가 수신 또는 발신 메시지에 사용할 콘텐츠 검사 기능을 활성화합니다.	다음 기능 중 하나 이상을 활성화 및 구성할 수 있습니다. • Anti-Virus, 335 페이지 • File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석), 461 페이지(수신 메시지 전용) • Anti-Spam, 355 페이지 • 그레이메일 탐지 및 안전한 수신 거부. 그레이메일 관리, 387 페이지의 내용을 참조하십시오. • 신종 바이러스 필터(Outbreak Filter), 399 페이지 • 데이터 유출 방지, 491 페이지 (발신 메시지 전용) • 콘텐츠 필터, 283 페이지
단계 **2**	(선택 사항) 특정 데이터를 포함하는 메시지에 대해 수행할 작업의 콘텐츠 필터를 만듭니다.	콘텐츠 필터, 283 페이지 항목을 참조하십시오.
단계 **3**	(선택 사항) 메일 정책 규칙을 적용할 사용자를 지정하기 위해 LDAP 그룹 쿼리를 정의합니다.	그룹 LDAP 쿼리를 사용하여 수신자가 그룹 구성원인지 확인, 756 페이지를 참조하십시오.
단계 **4**	(선택 사항) 수신 또는 발신 메시지에 대한 기본 메일 정책을 정의합니다.	수신 또는 발신 메시지에 대한 기본 메일 정책 구성 , 276 페이지를 참조하십시오.
단계 **5**	사용자별 메일 정책을 설정하려는 사용자 그룹을 정의합니다.	수신 또는 발신 메일 정책을 만듭니다. 자세한 내용은 메일 정책 구성, 276 페이지를 참조하십시오.
단계 **6**	콘텐츠 필터 기능 및 어플라이언스가 메시지에 대해 수행하는 콘텐츠 필터 작업을 구성합니다.	메일 정책에 대해 서로 다른 콘텐츠 보안 기능을 구성합니다. • 콘텐츠 필터: 특정 사용자 그룹에 대한 메시지에 콘텐츠 필터 적용, 303 페이지 • 안티바이러스: 사용자에 대한 바이러스 검사 작업 구성, 342 페이지 • 파일 평판 필터링 및 파일 분석: File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석), 461 페이지 • 안티스팸: 안티스팸 정책 정의 , 362 페이지 • 그레이메일 탐지 및 안전한 수신 거부: 그레이메일 탐지 및 안전한 수신 거부를 위한 수신 메일 정책 구성, 392 페이지

	명령 또는 동작	목적
		• 보안 침해 필터: Outbreak Filter 기능 및 Outbreak 격리, 419 페이지 • 데이터 유출 방지: 발신 메일 정책을 사용하여 DLP 정책을 발신자 및 수신자에게 할당 , 511 페이지.

수신 및 발신 메시지를 서로 다르게 처리

Email Security Appliance는 메시지 콘텐츠 보안을 위한 두 개의 서로 다른 메일 정책 집합을 사용합니다.

- 수신 메일 정책 메시지는 리스너의 ACCEPT HAT 정책과 일치하는 연결에서 오는 메시지입니다.
- 발신 메일 정책 메시지는 리스너의 RELAY HAT 정책과 일치하는 연결에서 오는 메시지입니다. 여기에는 SMTP AUTH로 인증된 연결이 포함됩니다.

별도의 정책 집합을 사용하면 사용자에게 전송된 메시지 및 사용자로부터 전송된 메시지에 대해 서로 다른 보안 규칙을 정의할 수 있습니다. GUI의 **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)** 또는 **Outgoing Mail Policies(**발신 메일 정책**)** 또는 CLI의 policyconfig 명령을 사용하여 이러한 정책을 관리합니다.

참고 일부 기능은 수신 또는 발신 메일 정책에만 적용할 수 있습니다. 예를 들어 데이터 유출 방지 검사는 발신 메시지에 대해서만 수행할 수 있습니다. Advanced Malware Protection(파일 평판 검사 및 파일 분석)은 수신 메일 정책에서만 사용할 수 있습니다.

특정 설치에서, Cisco 어플라이언스를 통해 라우팅되는 "내부" 메일은 모든 수신자가 내부 주소로 지정되어 있더라도 발신으로 간주될 수 있습니다. 예를 들어 기본적으로 C170 및 C190 어플라이언스의 경우, 시스템 설정 마법사는 인바운드 이메일 수신과 아웃바운드 이메일 릴레이를 위해 하나의 리스너로 하나의 물리적 이더넷 포트만 구성합니다.

메일 정책에 대해 사용자 일치 확인

메시지를 받으면 Email Security Appliance는 수신 메시지이든 발신 메시지이든, 수신 또는 발신 메일 정책 테이블에 있는 메일 정책에 대해 각 메시지 수신자 및 발신자를 확인하려고 시도합니다.

이러한 확인은 수신자의 주소, 발신자의 주소 또는 둘 모두를 기반으로 합니다.

- 수신자 주소가 봉투 수신자 주소와 일치하는지 확인

  수신자 주소 일치를 확인할 때, 입력된 수신자 주소는 이메일 파이프라인의 이전 부분이 처리된 후의 최종 주소입니다. 예를 들어 이 기능이 활성화된 경우 기본 도메인, LDAP 라우팅 또는 가장, 별칭 테이블, 도메인 맵, 메시지 필터 기능은 봉투 수신자 주소를 재작성할 수 있으며, 메시지가 메일 정책과 일치하는지에 영향을 미칠 수 있습니다.

- 발신자 주소가 다음과 일치하는지 확인:
  - 봉투 발신자(RFC821 MAIL FROM 주소)
  - RFC822 From: 헤더에 있는 주소
  - RFC822 Reply-To: 헤더에 있는 주소

주소는 전체 이메일 주소, 사용자, 도메인 또는 부분 도메인과 일치할 수 있으며, LDAP 그룹 멤버십과 일치할 수도 있습니다.

관련 주제

- 첫 번째 일치 항목 적용, 272 페이지
- 정책 일치의 예, 272 페이지

첫 번째 일치 항목 적용

각 사용자(발신자 또는 수신자)는 해당 메일 정책 테이블에 정의된 각 메일 정책에 대해 하향식으로 평가됩니다.

각 사용자에 대해 첫 번째 일치 항목이 적용됩니다. 사용자가 특정 정책과 일치하지 않으면 자동으로 테이블의 기본 정책이 적용됩니다.

발신자 주소를 기반으로 일치가 확인되며, 메시지의 모든 나머지 수신자에게 해당 정책이 적용됩니다. (메시지당 발신자는 한 명뿐이기 때문입니다.)

메시지를 메일 정책에 일치시키는 경우 봉투 발신자 및 봉투 수신자의 우선 순위가 발신자 헤더보다 높습니다. 메일 정책을 특정 사용자와 일치하도록 구성하는 경우 메시지가 자동으로 봉투 발신자 및 봉투 수신자에 기반한 메일 정책으로 분류됩니다.

정책 일치의 예

다음 예는 하향식으로 정책 테이블의 일치를 확인하는 방법을 보여줍니다.

다음 표의 수신 메일 보안 정책 테이블의 경우 수신 메시지는 여러 정책과 일치합니다.

표 ***29:*** 정책 일치 예

주문	정책 이름	사용자	
		발신자	**Recipient**
1	**special_people**	**ANY**	**joe@example.com** **ann@example.com**
2	**from_lawyers**	**@lawfirm.com**	**ANY**
3	**acquired_domains**	**ANY**	**@newdomain.com** **@anotherexample.com**

주문	정책 이름	사용자	
4	**engineering**	**ANY**	**PublicLDAP.ldapgroup: engineers**
5	**sales_team**	**ANY**	**jim@john@larry@**
6	**Default Policy**	**ANY**	**ANY**

관련 주제

- 예: 1:, 273 페이지
- 예: 2:, 273 페이지
- 예: 3:, 273 페이지

예 1

발신자 bill@lawfirm.com에서 수신자 jim@example.com으로 전송된 메시지는 다음과 일치합니다.

- 사용자 설명이 발신자(@lawfirm .com) 및 수신자(ANY)와 일치하는 경우 정책 2.
- 봉투 발신자가 bill@lawfirm.com인 경우 정책 2.
- 헤더 발신자는 bill@lawfirm.com이지만 봉투 발신자가 @lawfirm .com과 일치하지 않는 경우 정책 5.

예 2

발신자 joe@yahoo.com이 세 명의 수신자(john@example.com, jane@newdomain.com 및 bill@example.com)가 있는 수신 메시지를 전송합니다.

- 수신자 jane@newdomain.com에 대한 메시지에는 정책 #3에 정의된 안티스팸, 안티바이러스, 보안 침해 필터 및 콘텐츠 필터가 적용됩니다.
- 수신자 john@example.com에 대한 메시지에는 정책 #5에 정의된 설정이 적용됩니다.
- 수신자 bill@example.com은 엔지니어링 LDAP 쿼리와 일치하지 않으므로 기본 정책에 정의된 설정이 적용됩니다.

이 예는 다중 수신자의 메시지에서 어떻게 메시지 분리가 발생할 수 있는지를 보여줍니다. 자세한 내용은 메시지 분리, 274 페이지를 참조하십시오.

예 3

발신자 bill@lawfirm.com(bill@lawfirm.com은 봉투 발신자로 사용됨)이 수신자 ann@example.com 및 larry@example.com으로 메시지를 전송합니다.

- 수신자 ann@example.com에는 정책 1에 정의된 안티스팸, 안티바이러스, 보안 침해 필터 및 콘텐츠 필터가 적용됩니다.
- 발신자(@lawfirm.com)와 수신자(ANY)가 일치하므로 수신자 larry@example.com에는 정책 2에 정의된 안티스팸, 안티바이러스, 보안 침해 필터 및 콘텐츠 필터가 적용됩니다.

메시지 분리

지능적인 메시지 분리는 수신자가 여러 명인 메시지에 각기 다른 수신자 기반 콘텐츠 보안 규칙을 적용하도록 해주는 메커니즘입니다.

각 수신자는 해당 메일 정책 테이블(수신 또는 발신)의 각 정책에 대해 하향식으로 평가됩니다.

메시지와 일치하는 각 정책은 이러한 수신자의 새 메시지를 생성합니다. 이 프로세스를 메시지 분리라고 정의합니다.

- 일부 수신자가 서로 다른 정책과 일치하면 이들은 일치하는 정책에 따라 그룹화되며, 메시지는 일치하는 정책의 수와 동일한 수로 분리되고 수신자는 각각의 해당 "분리"로 설정됩니다.
- 모든 수신자가 동일한 정책과 일치하면 메시지가 분리되지 않습니다. 반대로, 최대 분리 시나리오는 단일 메시지가 각 메시지 수신자에 대해 분리되는 것입니다.
- 그런 다음 이메일 파이프라인과 상관없이, 각 메시지 분리에 대해 안티스팸, 안티바이러스, Advanced Malware Protection(수신 메시지만), DLP 검사(발신 메시지만), 보안 침해 필터 및 콘텐츠 필터가 적용됩니다.

다음 표는 이메일 파이프라인에서 메시지가 분리된 시점을 보여줍니다.

작업 큐	메시지 필터 **(filters)**	이메일 보안 관리자 검사(수신자당)	↓ 모든 수신자에 대한 메시지
	안티스팸 **(antispamconfig, antispamupdate)**		메시지 필터 처리 직후, 안티스팸 처리 전에 메시지가 분리됩니다. 정책 1과 일치하는 모든 수신자에 대한 메시지 정책 2와 일치하는 모든 수신자에 대한 메시지 다른 모든 수신자에 대한 메시지(기본 정책과 일치) 참고 DLP 검사는 발신 메시지에 대해서만 수행됩니다.
	안티바이러스 **(antivirusconfig, antivirusupdate)**		
	파일 평판 및 분석**(Advanced Malware Protection)** **(ampconfig)**		
	그레이메일 관리		
	콘텐츠 필터 **(policyconfig -> filters)**		
	신종 바이러스 필터**(Outbreak Filter)** **(outbreakconfig, outbreakflush, outbreakstatus, outbreakupdate)**		
	데이터 유출 방지 **(policyconfig)**		

참고 각 메시지 분리에 대해 새 MID(message ID)가 생성됩니다(예: MID 1이 MID 2 및 MID 3이 됨). 자세한 내용은 "로깅" 장을 참조하십시오. 또한 `trace` 기능은 어떤 정책이 메시지 분리를 일으키는지를 보여줍니다.

Email Security Manager(이메일 보안 관리자) 정책의 정책 일치 및 메시지 분리는 어플라이언스에서 사용 가능한 메시지 처리 관리 방법에 명백히 영향을 미칩니다.

관련 주제

- 관리되는 예외, 275 페이지

관리되는 예외

각 분리 메시지의 반복 처리는 성능에 영향을 미치므로 관리되는 예외 기반으로 콘텐츠 보안 규칙을 구성하는 것이 좋습니다. 다시 말하면, 조직의 요구를 평가한 후 다수의 메시지는 기본 메일 정책으

로 처리되고 소수의 메시지만 몇몇 추가 "예외" 정책으로 처리되도록 기능을 구성하는 것입니다. 이런 식으로 메시지 분리가 최소화되며, 작업 대기열에서 각 분리 메시지를 처리함으로써 시스템 성능에 미치는 영향을 줄일 수 있습니다.

메일 정책 구성

메일 정책은 서로 다른 사용자 그룹을 안티스팸 또는 안티바이러스와 같은 특정 보안 설정에 매핑합니다.

관련 주제

- 수신 또는 발신 메시지에 대한 기본 메일 정책 구성 , 276 페이지
- 발신자 및 수신자 그룹에 대한 메일 정책 만들기, 276 페이지
- 발신자 또는 수신자에게 어떤 정책이 적용되는지 알아보기, 280 페이지

수신 또는 발신 메시지에 대한 기본 메일 정책 구성

기본 메일 정책은 다른 메일 정책에서 다루어지지 않는 메시지에 적용됩니다. 다른 정책이 구성되어 있지 않으면 기본 정책이 모든 메시지에 적용됩니다.

시작하기 전에

메일 정책에 대한 개별 보안 서비스를 정의하는 방법을 이해합니다. 사용자 단위로 메일 정책을 시행하는 방법, 270 페이지를 참조하십시오.

단계 **1** 요구 사항에 따라 다음 중 하나를 선택합니다.

- **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)**
- **Mail Policies(**메일 정책**) > Outgoing Mail Policies(**발신 메일 정책**)**

단계 **2** 기본 메일 정책에 대해 구성할 보안 서비스의 링크를 클릭합니다.

참고 기본 보안 서비스 설정의 경우, 페이지의 첫 번째 설정은 정책에 대해 서비스를 활성화할지 여부를 정의합니다. 서비스를 완전히 비활성화하려면 "Disable(비활성)"을 클릭할 수 있습니다.

단계 **3** 보안 서비스에 대한 설정을 구성합니다.

단계 **4** **Submit(**제출**)**를 클릭합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

발신자 및 수신자 그룹에 대한 메일 정책 만들기

시작하기 전에

- 메일 정책에 대한 개별 보안 서비스를 정의하는 방법을 이해합니다. 사용자 단위로 메일 정책을 시행하는 방법, 270 페이지를 참조하십시오.

- 적절한 테이블(수신 또는 발신)에서 하향식으로 사용자를 각 정책에 대해 평가합니다. 자세한 내용은 첫 번째 일치 항목 적용, 272 페이지를 참조하십시오.
- (선택 사항) 메일 정책 관리를 책임질 위임된 관리자를 정의합니다. 위임된 관리자는 정책의 안티스팸, 안티바이러스, Advanced Malware Protection, 보안 침해 필터 설정을 수정할 수 있으며, 정책에 대해 콘텐츠 필터를 활성화 또는 비활성화할 수 있습니다. 운영자와 관리자만 메일 정책의 이름 또는 발신자, 수신자, 그룹을 수정할 수 있습니다. 메일 정책에 대한 완전한 액세스 권한이 있는 사용자 지정 사용자 역할은 자동으로 메일 정책에 할당됩니다.

단계 **1** **Mail Policies**(메일 정책) **> Incoming Mail Policies**(수신 메일 정책) 또는 **Mail Policies**(메일 정책) **> Outgoing Mail Policies**(발신 메일 정책)를 선택합니다.

단계 **2** **Add Policy**(정책 추가)를 클릭합니다.

단계 **3** 메일 정책의 이름을 입력합니다.

단계 **4** (선택 사항) Editable by (Roles)(수정 기준(역할)) 링크를 클릭하고, 메일 정책 관리를 책임질 위임된 관리자에 대한 사용자 지정 사용자 역할을 선택합니다.

단계 **5** 정책에 대한 사용자를 정의합니다. 사용자 정의에 대한 지침은 메일 정책에 대한 발신자 및 수신자 정의, 277 페이지 섹션을 참조하십시오.

단계 **6** **Submit**(제출)을 클릭합니다.

단계 **7** 메일 정책에 대해 구성할 콘텐츠 보안 서비스의 링크를 클릭합니다.

단계 **8** 기본 설정을 사용하는 대신 정책에 대한 설정을 사용자 지정할 옵션을 드롭다운 목록에서 선택합니다.

단계 **9** 보안 서비스 설정을 사용자 지정합니다.

단계 **10** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- 메일 정책에 대한 발신자 및 수신자 정의, 277 페이지
- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 356 페이지

메일 정책에 대한 발신자 및 수신자 정의

정책을 적용할 발신자 및 수신자를 다음과 같이 정의할 수 있습니다.

- 전체 이메일 주소: `user@example.com`
- 부분 이메일 주소: `user@`
- 도메인의 모든 사용자: `@example.com`
- 부분 도메인의 모든 사용자: `@.example.com`
- LDAP 쿼리를 확인하여

참고 사용자 항목은 AsyncOS의 GUI 및 CLI에서 모두 대/소문자를 구분합니다. 예를 들어 사용자에 수신자 `Joe@`를 입력하는 경우 `joe@example.com`으로 전송된 메시지가 일치합니다.

메일 정책의 발신자 및 수신자를 정의하는 동안 다음에 유의해야 합니다.

- 발신자 및 수신자를 하나 이상 지정해야 합니다.
- 다음과 같은 경우 일치를 확인할 정책을 설정할 수 있습니다.
  - 메시지가 임의의 발신자, 하나 이상의 지정된 발신자 또는 지정된 발신자 외의 발신자로부터 오는 경우
  - 메시지가 임의의 수신자, 하나 이상의 지정된 수신자 또는 지정된 수신자 외의 수신자에게 전송되는 경우

단계 **1** **Users(**사용자**)** 섹션에서 **Add User(**사용자 추가**)**를 클릭합니다.

단계 **2** 정책의 발신자를 정의합니다. 다음 옵션 중 하나를 선택합니다.

- **Any Sender(**임의의 발신자**)**. 메시지가 임의의 발신자로부터 오는 경우 정책이 일치합니다.
- **Following Senders(**다음 발신자**)**. 메시지가 하나 이상의 지정된 발신자로부터 오는 경우 정책이 일치합니다. 이 옵션을 선택하고 텍스트 상자에 발신자 세부사항을 입력하거나 LDAP 그룹 쿼리를 선택합니다.
- **Following Senders are Not(**다음의 발신자 제외**)**. 메시지가 지정된 발신자 이외의 발신자로부터 오는 경우 정책이 일치합니다. 이 옵션을 선택하고 텍스트 상자에 발신자 세부사항을 입력하거나 LDAP 그룹 쿼리를 선택합니다.

위의 필드를 선택하는 동안 발신자 조건을 설정하는 방법에 대해 알아보려면 예, 279 페이지를 참조하십시오.

단계 **3** 정책의 수신자를 정의합니다. 다음 옵션 중 하나를 선택합니다.

- **Any Recipient(**임의의 수신자**)**. 메시지가 임의의 수신자에게 전송되는 경우 정책이 일치합니다.
- **Following Recipients(**다음 수신자**)**. 메시지가 지정된 수신자에게 전송되는 경우 정책이 일치합니다. 이 옵션을 선택하고 텍스트 상자에 수신자 세부사항을 입력하거나 LDAP 그룹 쿼리를 선택합니다.

메시지가 하나 이상의 지정된 수신자에게 전송될 때 정책이 일치하도록 할지, 아니면 지정된 모든 수신자에게 전송될 때 정책이 일치하도록 할지를 선택할 수 있습니다. 드롭다운 목록에서 **If one more conditions match(**하나 이상의 조건이 일치하는 경우**)** 또는 **Only if all conditions match(**모든 조건이 일치하는 경우에만**)** 옵션 중 하나를 선택합니다.

- **Following Recipients are Not(**다음 수신자 제외**)**. 메시지가 지정된 수신자 이외의 수신자에게 전송되는 경우 정책이 일치합니다. 이 옵션을 선택하고 텍스트 상자에 수신자 세부사항을 입력하거나 LDAP 그룹 쿼리를 선택합니다.

참고 **Following Recipients(**다음 발신자**)**를 선택하고 드롭다운 목록에서 **Only if all conditions match(**모든 조건이 일치하는 경우에만**)**를 선택한 경우에만 이 옵션을 구성할 수 있습니다.

위의 필드를 선택하는 동안 수신자 조건을 설정하는 방법에 대해 알아보려면 예, 279 페이지를 참조하십시오.

단계 **4** **Submit(**제출**)**을 클릭합니다.

단계 **5** **Users(**사용자**)** 섹션에서 선택한 조건을 검토합니다.

다음에 수행할 작업

관련 주제

- 발신자 및 수신자 그룹에 대한 메일 정책 만들기, 276 페이지
- 예, 279 페이지

예

다음 표에서는 Add User(사용자 추가) 페이지에서 다양한 옵션을 선택할 때 조건이 어떻게 설정되는지를 설명합니다.

발신자			**Recipient**			조건
Any Sender(임의의 발신자**)**	**Following Senders(**다음 발신자**)**	**Following Senders are Not(**다음의 발신자 제외**)**	**Any Recipient(**임의의 수신자**)**	**Following Recipients(**다음 수신자**)**	**Following Recipients are Not(**다음 수신자 제외**)**	

선택됨	-	-	-	선택됨
				(기본값) **Only if all conditions match(**모든 조건이 일치하는 경우에만**)** 옵션이 선택됨
				값:
				`user1 @,`
				`user2 @`
					-	발신자: 임의
						Recipient:
						`user1@[AND]user2 @`

-	선택됨 값: u1@a.com, u2@a.com	-	-	선택됨 (기본값) **Only if all conditions match**(모든 조건이 일치하는 경우에만) 옵션이 선택됨 값: u1@b.com, u2@b.com	선택됨 값: u3@b.com, u4@b.com	**Sender**: u1@a.com [OR] u2@a.com **Recipient**: [u1@b.com[AND]u2@b.com] [AND] [[NOT] [u3@b.com[AND]u4@b.com]]
-	-	선택됨 값: u1@a.com, u2@a.com	-	선택됨 **If one or more conditions match**(하나 이상의 조건이 일치하는 경우) 옵션도 선택됨 값: u1@b.com, u2@b.com	-	**Sender**: [NOT] [u1@a.com[OR]u2@a.com] **Recipient**: u1@b.com [OR] u2@b.com

관련 주제

- 메일 정책에 대한 발신자 및 수신자 정의, 277 페이지

발신자 또는 수신자에게 어떤 정책이 적용되는지 알아보기

수신 또는 발신 메일 정책에 이미 정의된 사용자를 검색하려면 Mail Policies(메일 정책) 페이지 상단에 있는 Find Policies(정책 찾기) 섹션을 사용합니다.

예를 들어 bob@example.com을 입력하고 Find Policies(정책 찾기) 버튼을 클릭하면 정책과 일치하는 정의된 사용자가 어떤 정책에 포함되어 있는지를 보여주는 결과가 표시됩니다.

해당 정책의 사용자를 수정하려면 정책의 이름을 클릭합니다.

발신자 또는 수신자가 구성된 정책과 일치하지 않는 경우 항상 기본 정책과 일치하게 되므로 사용자를 검색할 때 항상 기본 정책이 표시됩니다.

관련 주제

- 관리되는 예외, 275 페이지

관리되는 예외

위의 두 예에 나온 단계를 사용하여 관리되는 예외를 기반으로 정책 만들기 및 구성을 시작할 수 있습니다. 다시 말해, 조직의 요구를 평가한 후 메시지의 대다수가 기본 정책에 의해 처리되도록 정책을 구성할 수 있습니다. 그런 다음 특정 사용자 또는 사용자 그룹에 대한 추가 "예외" 정책을 만들어, 필요에 따라 다른 정책을 관리할 수 있습니다. 이런 식으로 메시지 분리가 최소화되며, 작업 대기열에서 각 분리 메시지를 처리함으로써 시스템 성능에 미치는 영향을 줄일 수 있습니다.

스팸, 바이러스 및 정책 시행에 대한 조직 또는 사용자의 허용 범위를 기반으로 정책을 정의할 수 있습니다. 다음 표에는 몇 가지 정책 예가 요약되어 있습니다. "적극적인" 정책은 최종 사용자 사서함에 도달하는 스팸 및 바이러스의 양을 최소화하도록 설계되었습니다. "신중한" 정책은 오탐을 피하고 사용자가 정책과 상관없이 메시지를 놓치지 않도록 맞춤화되었습니다.

표 ***30:*** 적극적인/신중한 이메일 보안 관리자 설정

	적극적인 설정	신중한 설정
Anti-Spam	양성으로 식별된 스팸: 삭제 의심스런 스팸: 격리 마케팅 메일: 메시지 제목 앞에 "`[Marketing]`"을 첨부하고 전달	양성으로 식별된 스팸: 격리 의심스러운 스팸: 메시지 제목 앞에 "`[Suspected Spam]`"을 첨부하고 전달 마케팅 메일: 비활성화됨
Anti-Virus	복구된 메시지: 전달 암호화된 메시지: 삭제 검사되지 않은 메시지: 삭제 감염된 메시지: 삭제	복구된 메시지: 전달 암호화된 메시지: 격리 검사되지 않은 메시지: 격리 감염된 메시지: 삭제
AMP(Advanced Malware Protection) **(**파일 평판 필터링 및 파일 분석**)**	검사되지 않은 첨부 파일: 삭제 악성코드 첨부 파일이 있는 메시지: 삭제 파일 분석 보류 중인 메시지: 격리	검사되지 않은 첨부 파일: 메시지 제목 앞에 "`[WARNING: ATTACHMENT UNSCANNED]`"를 첨부하고 전달 악성코드 첨부 파일이 있는 메시지: 삭제 파일 분석 보류 중인 메시지: 메시지 제목 앞에 "`[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]`"를 첨부하고 전달
바이러스 필터	활성화됨, 우회가 허용되는 특정 파일 확장명 또는 도메인 없음 모든 메시지에 대한 메시지 수정 활성화	활성화됨, 우회가 허용되는 특정 파일 확장명 또는 도메인 있음 서명되지 않은 메시지에 대한 메시지 수정 활성화

메시지 헤더에 대한 우선순위 설정

어플라이언스의 수신 및 발신 메시지와 일치하도록 메시지 헤더의 우선순위를 설정할 수 있습니다.

SUMMARY STEPS

1. **Mail Policies(**메일 정책**) > Mail Policy Settings(**메일 정책 설정**)**로 이동합니다.
2. **Add Priority(**우선순위 추가**)**를 클릭하고 해당 헤더 이름(예: 헤더 "From") 확인란을 선택하여 새 우선순위를 추가합니다.
3. **Submit(**제출**)**을 클릭하여 변경 사항을 커밋합니다.

DETAILED STEPS

	명령 또는 동작	목적
단계 **1**	**Mail Policies(**메일 정책**) > Mail Policy Settings(**메일 정책 설정**)**로 이동합니다.	기본적으로 봉투 발신자 헤더는 우선순위 1로 설정됩니다. Envelope Sender(봉투 발신자) 링크를 클릭하여 우선순위를 변경할 수 있습니다.
단계 **2**	**Add Priority(**우선순위 추가**)**를 클릭하고 해당 헤더 이름(예: 헤더 "From") 확인란을 선택하여 새 우선순위를 추가합니다.	
단계 **3**	**Submit(**제출**)**을 클릭하여 변경 사항을 커밋합니다.	

11 장

콘텐츠 필터

이 장에는 다음 섹션이 포함되어 있습니다.

콘텐츠 필터 개요

콘텐츠 필터를 사용하여 안티바이러스 검사 또는 DLP와 같은 다른 콘텐츠 보안 기능에 의한 표준 루틴 처리를 초과하는 메시지 처리를 맞춤 설정할 수 있습니다. 예를 들어, 콘텐츠가 이후 검사를 위해 격리를 보장하거나 회사 정책에 따라 전달 전에 특정 메시지를 암호화해야 하는 경우 콘텐츠 필터를 사용할 수 있습니다.

콘텐츠 필터 작동 방식

콘텐츠 필터는 이메일 파이프라인에서 더 뒤에, 즉 메시지 필터링 후, 하나의 메시지가 일치하는 각 메일 정책에 대해 여러 개별 메시지로 "분리"된 후(자세한 내용은 메시지 분리, 274 페이지 참고) 및 메시지가 안티스팸 및 안티바이러스 검사를 받은 후에 적용된다는 점을 제외하면 메시지 필터와 유사합니다.

콘텐츠 필터는 수신 또는 발신 메시지 중 하나를 검사합니다. 두 메시지 유형을 모두 검사하는 필터를 정의할 수는 없습니다. Email Security Appliance에는 각 메시지 유형에 대한 별도의 콘텐츠 필터 "마스터 목록"이 있습니다. 마스터 리스트는 또한 어플라이언스가 콘텐츠 필터를 실행하는 순서를 결정합니다. 그러나 각 개별 메일 정책은 메시지가 정책과 일치할 때 어떤 특정 필터를 실행할지를 결정합니다.

콘텐츠 필터는 사용자(발신자 또는 수신자) 기준으로 메시지를 검사합니다.

콘텐츠 필터에는 다음 구성 요소가 있습니다.

- *conditions(조건)* - 어플라이언스가 콘텐츠 필터를 사용하여 메시지를 검사하는 경우를 결정함(선택 사항)
- *actions(작업)* - 어플라이언스가 메시지에 대해 수행함(필수)
- *action variables(작업 변수)* - 어플라이언스가 수정 시 메시지에 추가할 수 있음(선택 사항)

관련 주제

- 콘텐츠 필터를 사용하여 메시지 내용을 검사하는 방법, 284 페이지
- 콘텐츠 필터 조건, 284 페이지
- 콘텐츠 필터 작업, 293 페이지
- 작업 변수, 299 페이지

콘텐츠 필터를 사용하여 메시지 내용을 검사하는 방법

프로시저

	명령 또는 동작	목적
단계 **1**	(선택 사항) 콘텐츠 필터에 대해 지원되는 기능을 정의합니다.	다음 항목 중 콘텐츠 필터와 함께 사용할 항목을 만듭니다. • 암호화 프로필 • 면책조항 템플릿 • 알림 템플릿 • 정책 격리 • URL 화이트리스트
단계 **2**	수신 또는 발신 콘텐츠 필터를 정의합니다.	콘텐츠 필터는 다음으로 구성될 수 있습니다. • 콘텐츠 필터 조건, 284 페이지(선택 사항) • 콘텐츠 필터 작업, 293 페이지 • 작업 변수, 299 페이지(선택 사항) 콘텐츠 필터 만들기, 301 페이지
단계 **3**	콘텐츠 보안 규칙을 설정할 대상 사용자 그룹을 정의합니다.	수신 또는 발신 메일 정책을 만듭니다.
단계 **4**	수신 또는 발신 메시지에 필터를 사용할 대상 사용자 그룹에 콘텐츠 필터를 할당합니다.	메일 정책, 269 페이지를 참조하십시오.

콘텐츠 필터 조건

조건은 Email Security Appliance가 관련 메일 정책과 일치하는 메시지에 필터를 사용할지를 결정하는 "트리거"입니다. 콘텐츠 필터의 조건을 지정하는 것은 선택 사항입니다. 조건이 없는 콘텐츠 필터는 관련 메일 정책과 일치하는 모든 메시지에 적용됩니다.

콘텐츠 필터 조건에서, 메시지 본문 또는 첨부 파일에서 특정 패턴을 검색하는 필터 규칙을 추가할 때 패턴이 찾아야 할 횟수에 대한 최소 임계값을 지정할 수 있습니다. AsyncOS는 메시지를 검사할 때 메시지 및 첨부 파일에서 찾은 일치 횟수의 "점수"를 합산합니다. 최소 임계값이 충족되지 않으면 정규식이 true로 평가되지 않습니다. 텍스트, 스마트 식별자 또는 콘텐츠 사전 용어에 대해 이 임계값을 지정할 수 있습니다.

각 필터에 대해 여러 조건을 정의할 수 있습니다. 여러 조건이 정의되면 조건을 논리적 OR("다음 조건 중 하나...")로 연결할지, 논리적 AND("다음 조건 모두...")로 연결할지를 선택할 수 있습니다.

표 ***31:*** 콘텐츠 필터 조건

조건	설명
(조건 없음)	콘텐츠 필터에서 조건을 지정하는 것은 선택 사항입니다. 조건을 지정하지 않으면 암시적으로 true 규칙이 됩니다. true 규칙은 모든 메시지와 일치하며 해당 작업은 항상 수행됩니다.
메시지 본문 또는 첨부 파일	**Contains text(**텍스트 포함**):** 메시지 본문에 특정 패턴과 일치하는 텍스트 또는 첨부 파일이 포함되어 있습니까? **Contains smart identifier(**스마트 식별자 포함**):** 메시지 본문 또는 첨부 파일의 내용이 스마트 식별자와 일치합니까? **Contains term in content dictionary(**콘텐츠 사전의 용어 포함**):** 메시지 본문에 <*dictionary name*>이라는 콘텐츠 사전의 용어 또는 정규식이 포함되어 있습니까? 이 옵션이 활성화되려면 사전을 이미 만든 상태여야 합니다. 컨텐트 사전, 613 페이지를 참조하십시오. 참고 하나 이상의 사전을 활성화해야만 사전 관련 조건을 사용할 수 있습니다. 콘텐츠 사전 만들기에 대한 자세한 내용은 컨텐트 사전, 613 페이지 섹션을 참조하십시오. **Number of matches required(**필요한 일치 수**)**. 규칙이 true로 평가되기 위해 필요한 일치 수를 지정합니다. 텍스트, 스마트 식별자 또는 콘텐츠 사전 용어에 대해 이 임계값을 지정할 수 있습니다. 여기에는 delivery-status 부분 및 관련 첨부 파일이 포함됩니다.

조건	설명
메시지 본문	**Contains text(**텍스트 포함**):** 메시지 본문에 특정 패턴과 일치하는 텍스트가 포함되어 있습니까? **Contains smart identifier(**스마트 식별자 포함**):** 메시지 본문의 내용이 스마트 식별자와 일치합니까? 스마트 식별자는 다음 패턴을 탐지할 수 있습니다. • 신용 카드 번호 • 미국 사회 보장 번호 • CUSIP(Committee on Uniform Security Identification Procedures) 번호 • ABA(American Banking Association) 라우팅 번호 **Contains term in content dictionary(**콘텐츠 사전의 용어 포함**):** 메시지 본문에 *<dictionary name>*이라는 콘텐츠 사전의 용어 또는 정규식이 포함되어 있습니까? 이 옵션이 활성화되려면 사전을 이미 만든 상태여야 합니다. 컨텐트 사전, 613 페이지를 참조하십시오. 참고 하나 이상의 사전을 활성화해야만 사전 관련 조건을 사용할 수 있습니다. 콘텐츠 사전 만들기에 대한 자세한 내용은 컨텐트 사전, 613 페이지 섹션을 참조하십시오. **Number of matches required(**필요한 일치 수**)**. 규칙이 true로 평가되기 위해 필요한 일치 수를 지정합니다. 텍스트 또는 스마트 식별자에 대해 이 임계값을 지정할 수 있습니다. 이 규칙은 메시지 본문에만 적용됩니다. 첨부 파일이나 헤더는 포함되지 않습니다.
URL Category(URL 범주)	URL 평판 또는 URL 범주 필터링: 조건 및 규칙 , 433 페이지 및 URL 범주 정보, 446 페이지를 참조하십시오.
메시지 크기	본문 크기가 지정된 범위 내에 있습니까? 본문 크기는 헤더와 첨부 파일을 모두 포함한 메시지의 크기를 가리킵니다. body-size 규칙은 지침에 따라 본문 크기를 지정된 수와 비교할 메시지를 선택합니다.
매크로 탐지	수신 또는 발신 메시지에 매크로가 활성화된 첨부 파일이 포함되어 있습니까? 매크로 탐지 조건을 사용하면 선택한 파일 유형에서 매크로가 활성화된 첨부 파일을 탐지할 수 있습니다.

조건	설명
첨부 파일 콘텐츠	텍스트 포함**.** 메시지에 특정 패턴과 일치하는 또 다른 첨부 파일 또는 텍스트를 포함하는 첨부 파일이 포함되어 있습니까? 이 규칙은 body-contains() 규칙과 유사하지만, 메시지의 전체 "본문" 검사를 피하려고 시도합니다. 즉, 사용자가 첨부 파일로 보는 부분만 검사하려고 시도합니다. **Contains a smart identifier(**스마트 식별자 포함**).** 메시지 첨부 파일의 내용이 지정된 스마트 식별자와 일치합니까? **Contains terms in content dictionary(**콘텐츠 사전의 용어 포함**).** 첨부 파일에 <*dictionary name*>이라는 콘텐츠 사전의 용어 또는 정규식이 포함되어 있습니까? 사전 용어를 검색하려면 사전을 이미 만든 상태여야 합니다. 컨텐트 사전, 613 페이지를 참조하십시오. 참고 하나 이상의 사전을 활성화해야만 사전 관련 조건을 사용할 수 있습니다. 콘텐츠 사전 만들기에 대한 자세한 내용은 컨텐트 사전, 613 페이지 섹션을 참조하십시오. **Number of matches required(**필요한 일치 수**)**. 규칙이 true로 평가되기 위해 필요한 일치 수를 지정합니다. 텍스트, 스마트 식별자 또는 콘텐츠 사전 일치 항목에 대해 이 임계값을 지정할 수 있습니다.

조건	설명
첨부 파일 정보	파일 이름**.** 메시지에 특정 패턴과 일치하는 파일 이름의 첨부 파일이 있습니까? **Filename contains term in content dictionary(**파일 이름에 콘텐츠 사전의 용어 포함**).** 메시지에 *<dictionary name>*이라는 콘텐츠 사전의 용어 또는 정규식이 포함된 파일 이름의 첨부 파일이 있습니까? 이 옵션이 활성화되려면 사전을 이미 만든 상태여야 합니다. 컨텐트 사전, 613 페이지를 참조하십시오. 참고 하나 이상의 사전을 활성화해야만 사전 관련 조건을 사용할 수 있습니다. 콘텐츠 사전 만들기에 대한 자세한 내용은 컨텐트 사전, 613 페이지 섹션을 참조하십시오. **File type(**파일 형식**)**. 메시지에 지문(UNIX file 명령과 유사)을 기반으로 특정 패턴과 일치하는 파일 형식의 첨부 파일이 있습니까? **MIME type(MIME** 유형**)**. 메시지에 특정 MIME 유형의 첨부 파일이 있습니까? MIME 첨부 파일에 의해 제공되는 MIME 유형만 평가된다는 점을 제외하면 이 규칙은 attachment-type 규칙과 유사합니다. (명시적 유형이 제공되지 않은 경우 어플라이언스는 확장명으로 파일 형식을 "추측"하려고 시도하지 않습니다.) **Image Analysis(**이미지 분석**).** 메시지에 지정된 이미지 판정과 일치하는 이미지 첨부 파일이 있습니까? 유효한 이미지 분석 판정은 *Suspect(*의심스러움*), Inappropriate(*부적절함*), Suspect or Inappropriate(*의심스럽거나 부적절함*), Unscannable(*검사 불가*)* 또는 *Clean(*정상*)*입니다. **External Threat Feeds(**외부 위협 피드**)**: 파일이 선택한 외부 위협 피드 소스의 위협 정보와 일치합니까? **Select a File Hash Exception List(**파일 해시 예외 목록 선택**)**: (선택 사항) Cisco Email Security Gateway가 위협을 탐지하지 않도록 하려면 화이트리스트에 있는 파일 해시 목록을 선택합니다. 자세한 내용은 외부 피드 위협을 사용하도록 Cisco Email Security 게이트웨이 구성, 307 페이지을 참고하십시오. **Attachment is Corrupt(**첨부 파일이 손상됨**).** 이 메시지에 손상된 첨부 파일이 있습니까? 참고 손상된 첨부 파일이란 검사 엔진이 검사할 수 없어서 손상된 것으로 식별한 첨부 파일입니다.
첨부 파일 보호	비밀번호로 보호되거나 암호화된 첨부 파일이 포함됨 (예를 들어, 잠재적으로 검사할 수 없는 첨부 파일을 식별하려면 이 조건을 사용하십시오.) 비밀번호로 보호되거나 암호화되지 않은 첨부 파일이 포함됨

조건	설명
Subject Header(제목 헤더)	**Subject Header(**제목 헤더**):** 제목 헤더가 특정 패턴과 일치합니까? **Contains terms in content dictionary(**콘텐츠 사전의 용어 포함**)**: 제목 헤더에 <*dictionary name*>이라는 콘텐츠 사전의 용어 또는 정규식이 포함되어 있습니까? 사전 용어를 검색하려면 사전을 이미 만든 상태여야 합니다. 컨텐트 사전, 613 페이지를 참조하십시오. 참고 하나 이상의 사전을 활성화해야만 사전 관련 조건을 사용할 수 있습니다. 콘텐츠 사전 만들기에 대한 자세한 내용은 컨텐트 사전, 613 페이지 섹션을 참조하십시오.
Other Header	**Header name(**헤더 이름**)**: 메시지에 특정 헤더가 포함되어 있습니까? **Header value(**헤더 값**)**: 헤더의 값이 특정 헤더와 일치합니까? 헤더 값에 콘텐츠 사전의 용어 포함**.** 지정된 헤더에 <*dictionary name*>이라는 콘텐츠 사전의 용어 또는 정규식이 포함되어 있습니까? 사전 용어를 검색하려면 사전을 이미 만든 상태여야 합니다. 컨텐트 사전, 613 페이지 항목을 참조하십시오. 참고 하나 이상의 사전을 활성화해야만 사전 관련 조건을 사용할 수 있습니다. 콘텐츠 사전 만들기에 대한 자세한 내용은 컨텐트 사전, 613 페이지 섹션을 참조하십시오. 이 옵션의 사용 방법에 대한 자세한 내용은 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예 , 366 페이지 섹션을 참조해 주십시오.
봉투 발신자	**Envelope Sender(**봉투 발신자**).** Envelope Sender(봉투 발신자)(즉, Envelope From, <MAIL FROM>)가 지정된 패턴과 일치합니까? **Matches LDAP group(LDAP** 그룹과 일치**)**. Envelope Sender(봉투 발신자)(즉, Envelope From, <MAIL FROM>)가 지정된 LDAP 그룹에 있습니까? **Contains term in content dictionary(**콘텐츠 사전의 용어 포함**).** 봉투 발신자에 <*dictionary name*>이라는 콘텐츠 사전에 있는 정규식 또는 용어가 포함되어 있습니까? 사전 용어를 검색하려면 사전을 이미 만든 상태여야 합니다. 컨텐트 사전, 613 페이지를 참조하십시오. 참고 하나 이상의 사전을 활성화해야만 사전 관련 조건을 사용할 수 있습니다. 콘텐츠 사전 만들기에 대한 자세한 내용은 컨텐트 사전, 613 페이지 섹션을 참조하십시오.

조건	설명
봉투 수신자	**Envelope Recipient(봉투 수신자)**. Envelope Recipient(봉투 수신자)(즉, Envelope To, <RCPT TO>)가 지정된 패턴과 일치합니까? **Matches LDAP group(LDAP 그룹과 일치)**. Envelope Recipient(봉투 수신자)(즉, Envelope To, <RCPT TO>)가 지정된 LDAP 그룹에 있습니까? **Contains term in content dictionary(콘텐츠 사전의 용어 포함).** 봉투 수신자에 <*dictionary name*>이라는 콘텐츠 사전에 있는 정규식 또는 용어가 포함되어 있습니까? 사전 용어를 검색하려면 사전을 이미 만든 상태여야 합니다. 컨텐트 사전, 613 페이지를 참조하십시오. 참고 하나 이상의 사전을 활성화해야만 사전 관련 조건을 사용할 수 있습니다. 콘텐츠 사전 만들기에 대한 자세한 내용은 컨텐트 사전, 613 페이지 섹션을 참조하십시오. Envelope Recipient(봉투 수신자) 규칙은 메시지 기반입니다. 메시지 수신자가 여러 명인 경우, 모든 수신자에 대한 메시지에 영향을 미치려면 지정된 작업에 대한 그룹에서 한 수신자만 발견되어야 합니다. Envelope Sender(봉투 발신자)(즉, Envelope From, <MAIL FROM>)가 지정된 LDAP 그룹에 있습니까?
Receiving Listener(수신 리스너)	메시지가 명명된 리스너를 통해 도착했습니까? 리스너 이름은 시스템에 현재 구성된 리스너의 이름이어야 합니다.
Remote IP(원격 IP)	메시지가 지정된 IP 주소나 IP 블록과 일치하는 원격 호스트에서 전송되었습니까? Remote IP(원격 IP) 규칙은 메시지를 전송한 호스트의 IP 주소가 특정 패턴과 일치하는지를 테스트합니다. IPv4(Internet Protocol version 4) 또는 IPv6(version 6) 주소일 수 있습니다. IP 주소 패턴은 발신자 그룹 구문, 96 페이지에 설명된 허용되는 호스트 표기법을 사용하여 지정됩니다(SBO, SBRS, dnslist 표기법 및 특수 키워드 ALL 제외).
Reputation Score	발신자의 SenderBase Reputation 점수는 몇 점입니까? Reputation Score(Reputation 점수) 규칙은 지정된 다른 값을 기준으로 SenderBase Reputation 점수를 확인합니다.
DKIM 인증	인증을 통과했거나, 부분적으로 확인되었거나, 일시적으로 확인할 수 없게 반환되었거나, 영구적으로 실패했거나, 반환된 DKIM 결과가 없습니까?

조건	설명
위조 이메일 탐지	메시지의 발신인 주소가 위조되었습니까? 이 규칙은 메시지의 발신인: 헤더가 콘텐츠 사전에 있는 임의 사용자와 유사한지 여부를 확인합니다. 콘텐츠 사전을 선택하고 메시지를 잠재적으로 위조된 것으로 고려할 임계값(1 ~ 100)을 입력합니다. Forged Email Detection(위조 이메일 탐지) 조건은 From: 헤더를 콘텐츠 사전에 있는 사용자와 비교합니다. 이 과정에서 유사성에 따라 어플라이언스에서 사전에 있는 각 사용자의 유사성 점수를 할당합니다. 알림의 몇 가지 예는 다음과 같습니다. • From: 헤더가 <j0hn.sim0ns@example.com>이고 콘텐츠 사전에 사용자 'John Simons'가 포함된 경우 어플라이언스에서 사용자에게 유사성 점수 82를 할당합니다. • From: 헤더가 <john.simons@diff-example.com>이고 콘텐츠 사전에 사용자 'John Simons'가 포함된 경우 어플라이언스에서 사용자에게 유사성 점수 100을 할당합니다. 유사성 점수가 높을수록 메시지 위조 가능성이 높아집니다. 유사성 점수가 지정된 임계값보다 크거나 같은 경우, 필터 작업이 트리거됩니다. 특정 발신자가 보낸 메시지에 대한 위조 이메일 탐지 필터를 건너뛰려는 경우 **Exception List(**예외 목록**)** 드롭다운 목록에서 주소 목록을 선택합니다. 참고 전체 이메일 주소만 허용을 사용하여 만든 주소 목록만 선택할 수 있습니다. 자세한 내용은 위조 이메일 탐지, 610 페이지을 참고하십시오.
SPF 확인	SPF 확인 상태는 무엇이었습니까? 이 필터 규칙을 사용하면 서로 다른 SPF 확인 결과를 쿼리할 수 있습니다. SPF 확인에 대한 자세한 내용은 "이메일 인증" 장을 참조해 주십시오. 참고 SPF ID 없이 SPF 확인 콘텐츠 필터 조건을 구성한 경우 및 메시지에 판정이 각기 다른 여러 SPF ID가 포함된 경우 메시지의 판정 중 하나가 조건과 일치하면 조건이 트리거됩니다.
S/MIME 게이트웨이 메시지	메시지가 S/MIME 서명되거나, 인증되거나, 서명 및 인증되었습니까? 자세한 내용은 S/MIME 보안 서비스, 537 페이지를 참조해 주십시오.
S/MIME 게이트웨이 확인됨	메시지가 성공적으로 확인되거나, 해독되거나, 해독 및 확인되었습니까? 자세한 내용은 S/MIME 보안 서비스, 537 페이지를 참조해 주십시오.

조건	설명
메시지 언어	선택한 언어 중 하나의 메시지(제목 및 본문)입니까? 이 조건은 첨부 파일과 헤더에서 언어를 확인하지 않습니다. 언어 탐지는 어떻게 작동합니까**?** Cisco Email Security Appliance는 메시지의 언어를 탐지하기 위해 기본 언어 탐지 엔진을 사용합니다. 이 어플라이언스는 제목 및 메시지 본문을 추출하여 언어 탐지 엔진에 전달합니다. 언어 탐지 엔진은 각 언어의 가능성을 추출된 텍스트로 확인하고 다시 어플라이언스에 전달합니다. 어플라이언스는 가능성이 가장 높은 언어를 메시지의 언어로 간주합니다. 어플라이언스는 다음 시나리오 중 하나에서 메시지의 언어를 '확인되지 않음'으로 간주합니다. • 탐지된 언어를 Cisco Email Security Appliance에서 지원하지 않는 경우 • 어플라이언스에서 메시지의 언어를 탐지할 수 없는 경우 • 언어 탐지 엔진으로 전송된 추출된 텍스트의 총 크기가 50바이트 미만인 경우
중복 경계 확인	메시지에 중복 MIME 경계가 포함되어 있습니까? 중복 MIME 경계를 포함하는 메시지에 작업을 수행하려면 이 조건을 사용하십시오. 참고 형식이 잘못된 메시지(중복 MIME 경계)에서는 첨부 파일 기반 조건(예: 첨부 파일 콘텐츠) 또는 작업(예: 스트립 첨부 파일 제거)이 작동하지 않습니다.
지리위치	메시지가 선택한 국가에서 시작되었습니까? 지리 위치 조건을 사용하여 선택한 특정 국가에서 수신 메시지를 처리할 수 있습니다. 참고 지리 위치 콘텐츠 필터를 사용하기 전에 어플라이언스에서 안티스팸 엔진을 활성화합니다.
도메인 평판	발신인 도메인이 지정한 기준과 일치합니까? • 발신인 도메인 평판 • 외부 위협 피드 자세한 내용은 외부 피드 위협을 사용하도록 Cisco Email Security 게이트웨이 구성, 307 페이지 또는 발신자 도메인 평판 필터링, 323 페이지 섹션을 참조해 주십시오.

콘텐츠 필터 작업

이 작업은 Email Security Appliance가 콘텐츠 필터 조건과 일치하는 메시지에 대해 수행하는 작업입니다. 메시지 수정, 격리, 삭제 등 여러 유형의 작업을 수행할 수 있습니다. 메시지에 대해 수행되는 "최종 작업"(전달 또는 삭제)에 따라 Email Security Appliance는 즉시 작업을 수행하며, Outbreak Filter나 DLP 검사 등 이후의 처리는 모두 중단됩니다.

각 콘텐츠 필터에 대해 하나 이상의 작업을 정의해야 합니다.

메시지에 대해 순서대로 작업이 수행되므로, 콘텐츠 필터에 대해 여러 작업을 정의하는 경우 작업의 순서를 고려하십시오.

Attachment Content(첨부 파일 내용) 조건, Message Body or Attachment(메시지 본문 또는 첨부 파일) 조건, Message Body(메시지 본문) 조건, Attachment Content(첨부 파일 내용) 조건을 구성할 때 격리된 메시지에서 일치 콘텐츠를 볼 수 있습니다. 메시지 본문을 표시하면 일치 콘텐츠가 노란색으로 강조 표시됩니다. 메시지 제목의 일치 콘텐츠를 포함하려면 $MatchedContent 작업 변수를 사용할 수도 있습니다. 자세한 내용은 텍스트 리소스 장을 참조해 주십시오.

필터당 하나의 최종 작업만 정의할 수 있으며, 최종 작업은 마지막에 나열되는 작업이어야 합니다. 반송, 전달 및 삭제가 최종 작업입니다. 콘텐츠 필터에 대한 작업을 입력할 때 GUI 및 CLI는 최종 작업을 마지막에 배치합니다.

작업 변수, 299 페이지도 참조하십시오.

표 ***32:*** 콘텐츠 필터 작업

작업	설명
격리	**Quarantine(격리)**. 정책 격리 영역 중 하나에 보관되도록 메시지에 플래그를 지정합니다. **Duplicate message(메시지 복제)**: 메시지의 복사본을 지정된 격리로 전송하고 원본 메시지를 계속해서 처리합니다. 원본 메시지에 추가 작업이 적용됩니다.
전달 시 암호화	메시지가 다음 처리 단계로 계속 진행됩니다. 모든 처리가 완료되면 메시지가 암호화 및 전달됩니다. **Encryption rule(암호화 규칙)**: 메시지를 항상 암호화하거나, 먼저 TLS 연결을 통해 전송하려는 시도가 실패한 경우에만 암호화합니다. 자세한 내용은 암호화 대안으로 TLS 연결 사용, 529 페이지 항목을 참조하십시오. **Encryption Profile(암호화 프로필).** 처리가 완료되면 지정된 암호화 프로필을 사용하여 메시지를 암호화한 다음 전달합니다. 이 작업은 Cisco Encryption Appliance 또는 호스팅된 키 서비스와 사용하기 위한 것입니다. **Subject(제목)**. 암호화된 메시지의 제목. 기본값은 **`$Subject`**입니다.

작업	설명
콘텐츠별 첨부 파일 제거	**Attachment contains(**첨부 파일 포함**).** 정규식이 포함된 메시지의 모든 첨부 파일을 삭제합니다. 포함된 파일에 정규식 패턴과 일치하는 파일이 있는 경우 아카이브 파일(zip, tar)이 삭제됩니다. **Contains smart identifier(**스마트 식별자 포함**).** 지정된 스마트 식별자가 포함된 메시지의 모든 첨부 파일을 삭제합니다. **Attachment contains terms in the content dictionary(**첨부 파일에 콘텐츠 사전의 용어 포함**).** 첨부 파일에 <*dictionary name*>이라는 콘텐츠 사전의 용어 또는 정규식이 포함되어 있습니까? **Number of matches required(**필요한 일치 수**)**. 규칙이 true로 평가되기 위해 필요한 일치 수를 지정합니다. 텍스트, 스마트 식별자 또는 콘텐츠 사전 일치 항목에 대해 이 임계값을 지정할 수 있습니다. **Replacement message(**교체 메시지**).** 선택적인 코멘트는 삭제된 첨부 파일 대신 사용되는 텍스트를 수정하기 위한 수단입니다. 첨부 파일 바닥글이 메시지에 추가됩니다.

작업	설명
파일 정보별 첨부 파일 제거	**File name(**파일 이름**)**. 지정된 정규식과 일치하는 파일 이름이 있는 메시지의 모든 첨부 파일을 삭제합니다. 일치하는 파일이 포함되어 있는 경우 아카이브 첨부 파일(zip, tar)이 삭제됩니다. **File size(**파일 크기**)**. 지정된 파일 크기(바이트)와 같거나 큰(원시 인코딩 형식) 메시지의 모든 첨부 파일을 삭제합니다. 아카이브 또는 압축된 파일의 경우 이 작업은 압축 해제된 크기를 검토하지 않고 실제 첨부 파일 자체의 크기를 검토합니다. **File type(**파일 형식**)**. 파일의 지정된 "지문"과 일치하는 메시지의 모든 첨부 파일을 삭제합니다. 일치하는 파일이 포함되어 있는 경우 아카이브 첨부 파일(zip, tar)이 삭제됩니다. **MIME type(MIME** 유형**)**. 지정된 MIME 유형이 있는 메시지의 모든 첨부 파일을 삭제합니다. **Image Analysis Verdict(**이미지 분석 판정**)**. 지정된 이미지 판정과 일치하는 이미지 첨부 파일을 삭제합니다. 유효한 이미지 분석 판정으로는 *Suspect(*의심스러움*), Inappropriate(*부적절함*), Suspect or Inappropriate(*의심스럽거나 부적절함*), Unscannable(*검사 불가*)* 또는 *Clean(*정상*)* 등이 있습니다. **External Threat Feeds(**외부 위협 피드**)**. 파일이 ETF 엔진에 의해 악성으로 분류된 메시지의 모든 메시지 첨부 파일을 삭제합니다. **Select a File Hash Exception List(**파일 해시 예외 목록 선택**)**. (선택 사항) Cisco Email Security Gateway가 위협을 탐지하지 않도록 하려면 화이트리스트에 있는 파일 해시 목록을 선택합니다. 자세한 내용은 외부 피드 위협을 사용하도록 Cisco Email Security 게이트웨이 구성, 307 페이지을 참고하십시오. **Replacement message(**교체 메시지**).** 선택적인 코멘트는 삭제된 첨부 파일 대신 사용되는 텍스트를 수정하기 위한 수단입니다. 첨부 파일 바닥글이 메시지에 추가됩니다.

작업	설명
매크로를 포함하는 첨부 파일 제거	지정된 파일 형식의 매크로가 활성화된 모든 첨부 파일을 삭제합니다. 참고 아카이브 또는 임베디드 파일에 매크로가 포함된 경우 메시지에서 상위 파일이 삭제됩니다. **Custom Replacement Message(맞춤형 대체 메시지)(선택 사항)**: 기본적으로 시스템에서 생성된 메시지는 첨부 파일이 삭제될 때 메시지 본문의 하단에 추가됩니다. 다음은 메시지에서 매크로가 활성화된 첨부 파일을 삭제하는 경우 샘플 시스템에서 생성되는 메시지입니다. **`<application/vnd.ms-excel>`** 유형의 **`MIME`** 첨부 파일은 **`<mail.example.com>`** 호스트의 **`drop-macro-enabled-attachments`** 필터 규칙에 의해 여기서 제거되었습니다. **Custom Replacement Message(맞춤형 대체 메시지)** 필드에 입력하는 맞춤형 메시지는 시스템에서 생성된 메시지를 대체합니다.
URL Reputation(URL 평판)	메시지의 URL 수정: URL 평판 및 필터의 URL 범주 작업 사용 , 434 페이지 및 URL 필터링용 화이트리스트 만들기 , 430 페이지를 참조하십시오. 평판을 확인할 수 없는 URL에 대한 작업을 지정하려면 "No Score(점수 없음)"를 사용합니다. 참고 어플라이언스는 S/MIME을 사용하여 암호화되었거나 S/MIME 서명이 포함된 메시지를 서명된 메시지로 간주합니다.
URL Category(URL 범주)	메시지의 URL 수정: URL 평판 및 필터의 URL 범주 작업 사용 , 434 페이지 및 URL 범주 정보, 446 페이지를 참조하십시오. 참고 어플라이언스는 S/MIME을 사용하여 암호화되었거나 S/MIME 서명이 포함된 메시지를 서명된 메시지로 간주합니다.
경고문 텍스트 추가	**Above(위)**. 면책조항을 메시지 위에 추가합니다(머리글). **Below(아래).** 면책조항을 메시지 아래에 추가합니다(바닥글). 참고**:** 이 콘텐츠 필터 작업을 사용하려면 면책조항 텍스트를 이미 만든 상태여야 합니다. 자세한 내용은 면책조항 템플릿, 625 페이지를 참조하십시오.
신종 바이러스 필터 검사 Bypass	이 메시지에 대한 Outbreak Filter 검사를 우회합니다.
DKIM 서명 우회	이 메시지에 대한 DKIM 서명을 우회합니다.

작업	설명
사본 발송(Bcc:)	**Email addresses(**이메일 주소**)**. 지정된 수신자에 대한 메시지를 익명으로 복사합니다. **Subject(**제목**)**. 복사한 메시지의 제목을 추가합니다. **Return path (optional)(**반환 경로**(**선택 사항**)).** 반환 경로를 지정합니다. **Alternate mail host (optional)(**대체 메일 호스트**(**선택 사항**)).** 대체 메일 호스트를 지정합니다.
Notify	**Notify(**알림**).** 지정된 수신자에게 이 메시지를 보고합니다. 선택적으로 발신자 및 수신자에게 알릴 수 있습니다. **Subject(**제목**)**. 복사한 메시지의 제목을 추가합니다. **Return path (optional)(**반환 경로**(**선택 사항**)).** 반환 경로를 지정합니다. **Use template(**템플릿 사용**)**. 자신이 만든 템플릿 중 하나를 선택합니다. **Include original message as an attachment(**원본 메시지를 첨부 파일로 포함**)**. 원본 메시지를 첨부 파일로서 추가합니다.
수신자 변경	**Email address(**이메일 주소**)**. 지정된 이메일 주소로 메시지의 수신자를 변경합니다.
Send to Alternate Destination Host(대체 대상 호스트로 전송)	**Mail host(**메일 호스트**)**. 메시지의 대상 메일 호스트를 지정된 메일 호스트로 변경합니다. 참고 이 작업은 안티스팸 검사 엔진에 의해 스팸으로 분류된 메시지가 격리되는 것을 방지합니다. 이 작업은 격리를 재정의하고 지정된 메일 호스트로 전송합니다.
IP 인터페이스에서 전달	**IP** 인터페이스에서 전송합니다**.** 지정된 IP 인터페이스에서 발송. Deliver from IP Interface(IP 인터페이스에서 전달) 작업은 메시지에 대한 소스 호스트를 지정된 소스로 변경합니다. 소스 호스트는 메시지 전달을 시작해야 하는 IP 인터페이스로 구성됩니다.
헤더 제거	**Header name(**헤더 이름**).** 전달 전에 메시지에서 지정된 헤더를 제거합니다.

작업	설명
헤더 추가/수정	**Inserts a new header into the message or modifies an existing header(**메시지에 새 헤더를 삽입하거나 기존 헤더 수정**).** **Header name(**헤더 이름**)**. 기존 헤더 또는 새 헤더의 이름. **Specify value of new header(**새 헤더의 값 지정**).** 전달 전에 새 헤더의 값을 메시지에 삽입합니다. **Prepend to the Value of Existing Header(**기존 헤더 앞에 값 추가**).** 전달 전에 기존 헤더의 앞에 값을 추가합니다. **Append to the Value of Existing Header(**기존 헤더 뒤에 값 추가**).** 전달 전에 기존 헤더의 뒤에 값을 추가합니다. **Search & Replace from the Value of Existing Header(**기존 헤더 값으로부터 검색 및 교체**). Search for(**검색**)** 필드에 있는 기존 헤더를 교체할 값을 찾기 위한 검색어를 입력합니다. **Replace with(**교체**)** 필드의 헤더에 삽입할 값을 입력합니다. 값을 검색하는 데 정규식을 사용할 수 있습니다. 헤더에서 값을 삭제하려는 경우 **Replace with(**교체**)** 필드를 비워 둡니다.
위조 이메일 탐지	위조 메시지에서 발신인: 헤더를 제거하고 봉투 발신자로 대체합니다. 위조 이메일 탐지, 610 페이지를 참조하십시오.
메시지 태그 추가	DLP 정책 필터링과 사용할 메시지에 맞춤형 용어를 삽입합니다. 메시지 태그가 있는 메시지로 검사를 제한하도록 DLP 정책을 구성할 수 있습니다. 메시지 태그는 수신자에게 보이지 않습니다. DLP 정책에서의 메시지 태그 사용에 대한 자세한 내용은 데이터 손실 방지 정책, 494 페이지 섹션을 참조해 주십시오.
Add Log Entry	사용자 지정된 텍스트를 INFO 레벨에서 IronPort 텍스트 메일 로그에 삽입합니다. 텍스트는 작업 변수를 포함할 수 있습니다. 로그 항목은 메시지 추적에도 나타납니다.
전달 시 S/MIME 서명/암호화	전달 도중에 메시지의 S/MIME 서명 또는 암호화를 수행합니다. 즉, 메시지가 다음 처리 단계로 진행되며 모든 처리가 완료되면 서명 또는 암호화된 후 전달됩니다. **S/MIME Sending Profile(S/MIME** 전송 프로필**)**: 지정된 S/MIME 전송 프로필을 사용하여 S/MIME 서명 또는 암호화를 수행합니다. S/MIME 전송 프로필 관리, 547 페이지를 참조하십시오.

작업	설명
지금 암호화 및 전달(최종 작업)	메시지를 암호화 및 전달하며, 추가 처리를 건너뜁니다. **Encryption rule(**암호화 규칙**)**: 메시지를 항상 암호화하거나, 먼저 TLS 연결을 통해 전송하려는 시도가 실패한 경우에만 암호화합니다. 자세한 내용은 암호화 대안으로 TLS 연결 사용, 529 페이지 항목을 참조하십시오. **Encryption Profile(**암호화 프로필**).** 지정된 암호화 프로필을 사용하여 메시지를 암호화한 다음 전달합니다. 이 작업은 Cisco Encryption Appliance 또는 호스팅된 키 서비스와 사용하기 위한 것입니다. **Subject(**제목**)**. 암호화된 메시지의 제목. 기본값은 **`$Subject`**입니다.
S/MIME 서명/암호화(최종 작업)	S/MIME 서명 또는 암호화를 수행한 후 메시지를 전달하며, 추가 처리를 건너뜁니다. **S/MIME Sending Profile(S/MIME** 전송 프로필**)**: 지정된 S/MIME 전송 프로필을 사용하여 S/MIME 서명 또는 암호화를 수행합니다. S/MIME 전송 프로필 관리, 547 페이지를 참조하십시오.
바운스(최종 작업)	발신자에게 다시 메시지를 발송합니다.
나머지 콘텐츠 필터 생략(최종 작업)	메시지를 다음 처리 단계로 전달하며, 추가 콘텐츠 필터를 건너뜁니다. 구성에 따라 이것은 메시지를 수신자에게 또는 격리로 전달하는 것일 수도 있고, Outbreak Filter를 시작하는 것일 수도 있습니다.
Drop (Final Action)	메시지를 삭제하고 버립니다.

관련 주제

- 작업 변수, 299 페이지

작업 변수

콘텐츠 필터에 의해 처리된 메시지에 추가되는 헤더는 변수를 포함할 수 있으며, 이 변수는 작업이 실행될 때 원본 메시지의 정보와 자동으로 교체됩니다. 이러한 변수를 작업 변수라고 합니다. 어플라이언스는 다음의 작업 변수 집합을 지원합니다.

표 ***33:*** 작업 변수

변수	**Syntax**	설명
모든 헤더	`$AllHeaders`	메시지 헤더로 교체됩니다.
Body Size(본문 크기)	`$BodySize`	메시지의 크기로 교체됩니다(바이트 단위).

변수	**Syntax**	설명
날짜	`$Date`	MM/DD/YYYY 형식을 사용하여 현재 날짜로 교체됩니다.
삭제된 파일 이름	`$dropped_filename`	가장 최근에 삭제된 파일 이름만 반환합니다.
Dropped File Names(삭제된 파일 이름)	`$dropped_filenames`	$filenames와 같지만, 삭제된 파일의 리스트를 표시합니다.
Dropped File Types(삭제된 파일 형식)	`$dropped_filetypes`	$filetypes와 같지만, 삭제된 파일의 리스트를 표시합니다.
Envelope Sender(봉투 발신자)	`$envelopefrom` or `$envelopesender`	메시지의 Envelope Sender(봉투 발신자)(Envelope From, <MAIL FROM>)로 교체됩니다.
봉투 수신자	`$EnvelopeRecipients`	메시지의 모든 Envelope Recipients(봉투 수신자)(Envelope To, <RCPT TO>)로 교체됩니다.
파일 이름	`$filenames`	메시지 어태치 파일 이름의 쉼표로 구분된 리스트로 교체됩니다.
File Sizes(파일 크기)	`$filesizes`	메시지 어태치 파일 크기의 쉼표로 구분된 리스트로 교체됩니다.
파일 형식	`$filetypes`	메시지 어태치 파일 형식의 쉼표로 구분된 리스트로 교체됩니다.
필터 이름	`$FilterName`	처리 중인 필터의 이름으로 교체됩니다.
GMTimeStamp	`$GMTimeStamp`	이메일 메시지의 Received: 줄에 나타나는 현재 날짜 및 시간으로 교체됩니다(GMT 사용).
HAT 그룹 이름	`$Group`	메시지 주입 시 일치된 발송자 그룹의 이름으로 교체됩니다. 그룹에 이름이 없으면 ">Unknown<" 문자열이 삽입됩니다.
메일 흐름 정책	`$Policy`	메시지 주입 시 발송자에게 적용되는 HAT 정책의 이름으로 교체됩니다. 사전 정의된 정책 이름이 사용되지 않으면 ">Unknown<" 문자열이 삽입됩니다.
일치하는 컨텐트	`$MatchedContent`	콘텐츠 검사 필터를 트리거한 값으로 교체됩니다. 일치하는 콘텐츠는 콘텐츠 사전 일치, 스마트 식별자 또는 정규식 일치일 수 있습니다.
헤더	`$Header['`*string*`']`	원본 메시지에 일치하는 헤더가 포함된 경우 인용된 헤더의 값으로 교체됩니다. 큰따옴표를 사용할 수도 있습니다.

변수	**Syntax**	설명
호스트 이름	`$Hostname`	Email Security Appliance의 호스트 이름으로 교체됩니다.
내부 메시지 ID	`$MID`	메시지 식별을 위해 내부적으로 사용되는 MID(Message ID)로 교체됩니다. RFC822 "Message-Id" 값과 혼동해서는 안 됩니다(검색을 위해 $Header 사용).
수신 리스너	`$RecvListener`	메시지를 수신한 리스너의 별칭으로 교체됩니다.
수신 인터페이스	`$RecvInt`	메시지를 수신한 인터페이스의 별칭으로 교체됩니다.
원격 IP 주소	`$RemoteIP`	메시지를 Email Security Appliance로 전송한 시스템의 IP 주소로 교체됩니다.
원격 호스트 주소	`$remotehost`	메시지를 어플라이언스로 전송한 시스템의 호스트 이름으로 교체됩니다.
SenderBase Reputation 점수	`$Reputation`	발신자의 SenderBase Reputation 점수로 교체됩니다. 평판 점수가 없으면 "None"으로 교체됩니다.
제목	`$Subject`	메시지의 제목으로 교체됩니다.
시간	`$Time`	현지 시간으로 교체됩니다(현지 표준 시간대).
타임스탬프	`$Timestamp`	이메일 메시지의 Received: 줄에 나타나는 현재 날짜 및 시간으로 교체됩니다(현지 표준 시간대).

콘텐츠를 기준으로 메시지를 필터링하는 방법

관련 주제

- 콘텐츠 필터 만들기, 301 페이지
- 기본적으로 모든 수신자에 대해 콘텐츠 필터 활성화, 303 페이지
- 특정 사용자 그룹에 대한 메시지에 콘텐츠 필터 적용, 303 페이지
- GUI에서 콘텐츠 필터 구성 시 참고 사항, 304 페이지

콘텐츠 필터 만들기

시작하기 전에

- 콘텐츠 필터와 일치하는 메시지를 암호화하려면 암호화 프로필을 만듭니다.

- 일치하는 메시지에 면책조항을 추가하려면 면책조항 생성에 사용할 면책조항 템플릿을 만듭니다.
- 일치하는 메시지 때문에 사용자에게 알림 메시지를 전송하려면 알림 생성을 위한 알림 템플릿을 만듭니다.
- 메시지를 격리하려면 해당 메시지에 대한 새 정책 격리를 만들거나 기존 격리를 사용합니다.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)**를 클릭합니다.

또는

Mail Policies(메일 정책**) > Outgoing Mail Policies(**발신 메일 정책**)**.

단계 **2** **Add Filter(**필터 추가**)**를 클릭합니다.

단계 **3** 필터의 이름과 설명을 입력합니다.

단계 **4** (X-REF) **Editable By (Roles)(**수정 가능**(**역할**))** 링크를 클릭하고 Policy Administrator(정책 관리자)를 선택한 다음 **OK(**확인**)**를 클릭합니다.

Policy Administrator(정책 관리자) 사용자 역할에 속한 위임된 관리자는 이 콘텐츠 필터를 수정하고 메일 정책에서 사용할 수 있습니다.

단계 **5** (선택 사항) 필터를 트리거할 조건을 추가합니다.

a) Add Condition(조건 추가)을 클릭합니다.
b) 조건 유형을 선택합니다.
c) 조건 규칙을 정의합니다.
d) **OK(**확인**)**를 클릭합니다.
e) 필터에 추가할 다른 추가 조건에 대해 위 단계를 반복합니다. 콘텐츠 필터에 대해 둘 이상의 조건을 정의하는 경우 콘텐츠 필터를 일치로 간주하기 위해 정의된 작업 전체(논리적 AND)를 적용할지, 아니면 정의된 작업 중 하나(논리적 OR)를 적용할지를 정의할 수 있습니다.

참고 조건을 추가하지 않으면 필터와 관련된 메일 정책 중 하나가 일치하는 메시지에 대해 콘텐츠 필터 작업이 수행됩니다.

단계 **6** 어플라이언스가 필터의 조건과 일치하는 메시지에 대해 수행할 작업을 추가합니다.

a) Add Action(작업 추가)을 클릭합니다.
b) 작업 유형을 선택합니다.
c) 작업을 정의합니다.
d) **OK(**확인**)**를 클릭합니다.
e) 어플라이언스에서 수행할 추가 작업에 대해 위 단계를 반복합니다.
f) 여러 작업이 있는 경우 어플라이언스가 메시지에 적용할 순서대로 작업을 정돈합니다. 필터당 "최종" 작업은 하나만 있을 수 있으며, AsyncOS는 자동으로 최종 작업을 순서의 끝으로 이동합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

- 기본 수신 또는 발신 메일 정책에서 콘텐츠 필터를 활성화할 수 있습니다.
- 특정 사용자 그룹에 대한 메일 정책에서 콘텐츠 필터를 활성화할 수 있습니다.

기본적으로 모든 수신자에 대해 콘텐츠 필터 활성화

단계 **1** **Mail Policies**(메일 정책) > **Incoming Mail Policies**(수신 메일 정책)를 클릭합니다.

또는

Mail Policies(메일 정책) > **Outgoing Mail Policies**(발신 메일 정책).

단계 **2** 기본 정책 행에서 콘텐츠 필터 보안 서비스에 대한 링크를 클릭합니다.

단계 **3** 콘텐츠 필터링 보안 서비스 페이지에서 Content Filtering for Default Policy(기본 정책의 콘텐츠 필터링)의 값을 "Disable Content Filters(콘텐츠 필터 비활성화)"에서 "Enable Content Filters (Customize settings)(콘텐츠 필터 활성화(설정 사용자 지정))"로 변경합니다.

마스터 리스트에 정의된 콘텐츠 필터(콘텐츠 필터 개요 , 283 페이지에서 생성됨)가 이 페이지에 표시됩니다. 값을 "Enable Content Filters (Customize settings)(콘텐츠 필터 활성화(설정 사용자 지정))"로 변경하면 각 필터에 대한 확인란이 활성화됩니다.

단계 **4** 활성화할 각 콘텐츠 필터에 대해 **Enable**(활성화) 확인란을 선택합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

특정 사용자 그룹에 대한 메시지에 콘텐츠 필터 적용

시작하기 전에

- 메시지에 콘텐츠 필터를 사용하려는 사용자 그룹에 대한 수신 또는 발신 메일 정책을 만듭니다. 자세한 내용은 발신자 및 수신자 그룹에 대한 메일 정책 만들기, 276 페이지 항목을 참조하십시오.

단계 **1** **Mail Policies**(메일 정책) > **Incoming Mail Policies**(수신 메일 정책)를 클릭합니다.

또는

Mail Policies(메일 정책) > **Outgoing Mail Policies**(발신 메일 정책).

단계 **2** 콘텐츠 필터를 적용할 메일 정책의 콘텐츠 필터 보안 서비스(Content Filters 열)에 대한 링크를 클릭합니다.

단계 **3** 콘텐츠 필터링 보안 서비스 페이지에서 Content Filtering for Policy: Engineering(정책용 콘텐츠 필터링: 엔지니어링)의 값을 "Enable Content Filtering (Inherit default policy settings)(콘텐츠 필터링 활성화(기본 정책 설정 상속))"에서 "Enable Content Filtering (Customize settings)(콘텐츠 필터링 활성화(설정 사용자 지정))"으로 변경합니다.

단계 **4** 사용할 콘텐츠 필터에 대한 확인란을 선택합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

GUI에서 콘텐츠 필터 구성 시 참고 사항

- 콘텐츠 필터를 만들 때에는 조건을 지정할 필요가 없습니다. 작업을 정의하지 않으면 규칙에서 항상 기존의 정의된 작업이 적용됩니다. (조건을 지정하지 않는 것은 true() 메시지 필터 규칙을 사용하는 것과 같습니다. 콘텐츠 필터를 정책에 적용하면 모든 메시지가 일치됩니다.)
- 콘텐츠 필터에 사용자 지정 사용자 역할을 할당하지 않으면 콘텐츠 필터는 퍼블릭 필터가 되며, 메일 정책에 대해 위임된 관리자는 누구나 사용할 수 있습니다. 위임된 관리자 및 콘텐츠 필터에 대한 자세한 내용은 "일반적인 관리 작업" 장을 참조해 주십시오.
- 관리자와 운영자는 콘텐츠 필터에 사용자 지정 사용자 역할이 할당된 경우에도 어플라이언스에 있는 모든 콘텐츠 필터를 보고 수정할 수 있습니다.
- 필터 규칙과 작업에 대한 텍스트를 입력할 때 정규식 일치에서 다음 메타 문자는 특별한 의미를 가집니다. . ^ $ * + ? { [ ] \ | ( )

  정규식을 사용하지 않으려면 '\'(백슬래시)를 사용하여 이러한 문자를 이스케이프해야 합니다. 예: "*Warning*"

- "benign(정상)" 콘텐츠 필터를 만들어 메시지 분리 및 콘텐츠 필터를 테스트할 수 있습니다. 예를 들면 유일한 작업이 "deliver(전달)"인 콘텐츠 필터를 만들 수 있습니다. 이 콘텐츠 필터는 메일 처리에 영향을 미치지 않습니다. 그러나 이 필터를 사용하여 Email Security Manager(이메일 보안 관리자) 정책 처리가 시스템의 다른 요소(예: 메일 로그)에 어떤 영향을 미치는지를 테스트할 수 있습니다.
- 반대로, 수신 또는 발신 콘텐츠 필터의 "마스터 목록" 개념을 사용하면 어플라이언스에서 처리되는 모든 메일의 메시지 처리에 즉각적으로 영향을 미치는 매우 강력하고 포괄적인 콘텐츠 필터를 만들 수 있습니다. 이 필터의 프로세스는 다음과 같습니다.
  - Incoming or Outgoing Content Filters(수신 또는 발신 콘텐츠 필터) 페이지를 사용하여 순서가 1인 새 콘텐츠 필터를 만듭니다.
  - Incoming or Outgoing Mail Policies(수신 또는 발신 메일 정책) 페이지를 사용하여 기본 정책에 대한 새 콘텐츠 필터를 활성화합니다.
  - 모든 나머지 정책에 대해 콘텐츠 필터를 활성화합니다.
- 콘텐츠 필터에서 사용 가능한 Bcc: 및 격리 작업은 생성하는 격리의 보존 설정을 결정하는 데 도움이 될 수 있습니다. (정책, 바이러스, 보안 침해 격리, 847 페이지를 참조하십시오.) 메시지가 시스템에서 너무 빨리 릴리스되지 않도록(즉, 격리 영역이 할당된 디스크 공간을 너무 빨리 채우지 않도록) 정책 격리를 드나드는 메일 플로우를 시뮬레이션하는 필터를 만들 수 있습니다.
- "Entire Message(전체 메시지)" 조건은 Scan Behavior(검사 동작) 페이지 또는 **`scanconfig`** 명령과 동일한 설정을 사용하므로 메시지의 헤더를 검사하지 않습니다. "Entire Message(전체 메시지)"를 선택하면 메시지 본문과 첨부 파일만 검사합니다. 특정 헤더 정보를 검색하려면 "Subject(제목)" 또는 "Header(헤더)" 조건을 사용하십시오.

- 어플라이언스에서 LDAP 서버를 구성한 경우(즉, **ldapconfig** 명령을 사용하여 특정 문자열로 특정 LDAP 서버를 쿼리하도록 어플라이언스를 구성한 경우) LDAP 쿼리로 사용자를 구성하는 것은 GUI에만 나타납니다.
- 리소스가 미리 구성되지 않은 경우 콘텐츠 필터 규칙 빌더의 일부 섹션은 GUI에 나타나지 않습니다. 예를 들어, Text Resources(텍스트 리소스) 페이지 또는 CLI의 **textconfig** 명령으로 미리 구성하지 않은 경우 알림 템플릿 및 메시지 면책조항은 옵션으로서 나타나지 않습니다.
- 콘텐츠 필터 기능은 다음 문자 인코딩을 인식하고, 포함할 수 있으며, 해당 텍스트를 검사할 수 있습니다.
  - 유니코드(UTF-8)
  - 유니코드(UTF-16)
  - 서유럽/라틴-1(ISO 8859-1)
  - 서유럽/라틴-1(Windows CP1252)
  - 중국어 번체(Big 5)
  - 중국어 간체(GB 2312)
  - 중국어 간체(HZ GB 2312)
  - 한국어(ISO 2022-KR)
  - 한국어(KS-C-5601/EUC-KR)
  - 일본어(Shift-JIS (X0123))
  - 일본어(ISO-2022-JP)
  - 일본어(EUC)

  단일 콘텐츠 필터 내에서 여러 문자 집합을 혼합하여 사용할 수 있습니다. 여러 문자 인코딩으로 텍스트를 표시 및 입력하는 방법은 웹 브라우저의 설명서를 참조하십시오. 대부분의 브라우저는 여러 문자 집합을 동시에 렌더링할 수 있습니다.
- 콘텐츠 필터에 대해 표시되는 보기를 변경하려면 Incoming or Outgoing Content Filters(수신 또는 발신 콘텐츠 필터) 요약 페이지에서 "Description(설명)", "Rules(규칙)" 및 "Policies(정책)"에 대한 링크를 사용합니다.
  - **Description(**설명**)** 보기는 각 콘텐츠 필터에 대한 설명 필드에 입력한 텍스트를 표시합니다. (이것이 기본 보기입니다.)
  - **Rules(**규칙**)** 보기는 규칙 빌더 페이지에서 만든 규칙 및 정규식을 표시합니다.
  - **Policies(**정책**)** 보기는 각 콘텐츠 필터가 활성화된 대상 정책을 표시합니다.

12 장

외부 피드 위협을 사용하도록 Cisco Email Security 게이트웨이 구성

이 장에는 다음 섹션이 포함되어 있습니다.

외부 위협 피드 개요

ETF(외부 위협 피드) 프레임워크는 Cisco Email Security 게이트웨이에서 TAXII 프로토콜을 통해 통신하는 STIX 형식의 외부 위협 정보를 사용할 수 있도록 해줍니다.

Cisco Email Security 게이트웨이에서 외부 위협 정보를 사용하는 기능을 통해 조직에서는 다음을 수행할 수 있습니다.

- 악성코드, 랜섬웨어, 피싱 공격 및 표적 공격과 같은 사이버 위협에 능동적으로 대응할 수 있습니다.
- 로컬 및 서드파티 위협 인텔리전스 소스에 가입합니다.
- Cisco Email Security 게이트웨이의 효율성을 개선합니다.

Cisco Email Security 게이트웨어에서 ETF 기능을 사용하려면 유효한 기능 키가 필요합니다. 기능 키를 얻는 방법에 대한 자세한 내용은 Cisco 영업 담당자에게 문의하십시오.

STIX (Structured Threat Information eXpression)는 사이버 위협 정보를 나타내는 산업 표준의 구조적 언어입니다. STIX 소스는 악성 또는 의심스러운 사이버 활동을 탐지하는 데 사용되는 패턴이 포함된 지표로 구성됩니다.

다음은 이 릴리스에 지원되는 STIX IOC(보안 침해 지표) 목록입니다.

- 파일 해시 화이트리스트(의심스러운 악성 파일에 대한 해시 집합 설명)
- IP 화이트리스(의심스러운 악성 IP 주소 집합 설명)
- 도메인 화이트리스트(의심스러운 악성 도메인 집합 설명)
- URL 화이트리스트(의심스러운 악성 URL 집합 설명)

TAXII(Trusted Automated eXchange of Indicator Information)는 여러 조직 또는 제품 라인에서 서비스(TAXII 서버)를 통해 사이버 위협 정보를 교환하기 위한 사양 집합을 정의합니다.

이 릴리스에서는 버전 STIX 1.1.1 및 1.2와 TAXII 1.1이 지원됩니다.

외부 피드 위협을 사용하도록 **Cisco Email Security** 게이트웨이를 구성하는 방법

다음 단계를 순서대로 수행합니다.

단계	수행해야 할 작업	추가 정보
1단계	Cisco Email Security 게이트웨이에서 ETF 엔진을 활성화합니다.	Cisco Email Security 게이트웨이에서 외부 위협 피드 엔진 활성화, 309 페이지
2단계	Cisco Email Security 게이트웨이가 TAXII 서버에서 STIX 형식의 위협 피드를 가져올 수 있도록 ETF 소스를 구성합니다.	외부 위협 피드 소스 구성, 309 페이지
3단계	다음을 사용하여 위협이 포함된 메시지를 처리합니다. • HAT • 콘텐츠 또는 메시지 필터	위협이 포함된 메시지 처리, 312 페이지
4단계	메시지의 악성 도메인, URL 또는 파일 해시를 탐지하도록 구성한 콘텐츠 필터를 수신 메일 정책에 연결합니다.	수신 메일 정책에 콘텐츠 필터 연결, 320 페이지

Cisco Email Security 게이트웨이에서 외부 위협 피드 엔진 활성화

시작하기 전에

Cisco Email Security 게이트웨어에서 ETF 기능을 사용하려면 유효한 기능 키가 있어야 합니다.

단계 **1** **Security Services > External Threat Feeds(**외부 위협 피드**)**를 클릭합니다.

단계 **2** **Enable(**활성화**)**을 클릭합니다.

단계 **3** 라이센스 계약 페이지의 하단으로 스크롤하고 **Accept(**동의**)**를 클릭하여 계약에 동의합니다.

참고 라이선스 계약에 동의하지 않으면 Cisco Email Security 게이트웨이에서 ETF가 활성화되지 않습니다.

단계 **4** **Enable External Threat Feeds(**외부 위협 피드 활성화**)**를 선택합니다.

단계 **5** (선택 사항) ETF 엔진 조회 실패로 인해 ETF 엔진에서 위협을 검사하지 않는 모든 메시지에 맞춤형 헤더를 추가하려면 **Yes(**예**)**를 선택합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

ETF 소스를 구성합니다. 외부 위협 피드 소스 구성, 309 페이지를 참조하십시오.

외부 위협 피드 소스 구성

ETF 소스는 TAXII 서버에서 사용할 수 있는 위협 컬렉션에 대한 정보를 다운로드하는 데 사용됩니다. Cisco Email Security 게이트웨이가 TAXII 서버에서 STIX 형식의 위협 피드를 가져올 수 있도록 ETF 소스를 구성해야 합니다.

참고 Cisco Email Security 게이트웨이에서 최대 8개의 ETF 소스를 구성할 수 있습니다.

'폴링 경로' 및 '컬렉션 이름'으로 구성된 폴링 서비스를 사용하여 ETF 소스를 구성할 수 있습니다.

시작하기 전에

- Cisco Email Security 게이트웨이에서 ETF 엔진을 활성화해야 합니다.
- 게이트웨이가 외부 위협 피드를 사용할 수 있도록 방화벽에서 포트-80 HTTP 및 443 HTTPS를 열어야 합니다. 자세한 내용은 방화벽 정보, 1227 페이지의 내용을 참고하십시오.

단계 **1** **Mail Policies(**메일 정책**)** > **External Threat Feeds Manager(**외부 위협 피드 관리자**)**를 클릭합니다.

단계 **2** **Add Source(**소스 추가**)**를 클릭합니다.

단계 **3** 다음 표에 설명된 필수 파라미터를 입력하여 ETF 소스를 구성합니다.

파라미터 소스 상세정보	설명
소스 이름	ETF 소스의 이름을 입력합니다.
설명	ETF 소스에 대한 설명을 입력합니다.
TAXII 세부 정보	
호스트 이름	TAXII 서버의 호스트 이름(FQDN(Fully Qualified Domain Name) 또는 IP 주소)을 입력합니다.
폴링 경로	TAXII 서버에서 폴링 서비스를 식별하는 폴링 경로(예: /taxii-data)를 입력합니다.
컬렉션 이름	TAXII 서버에서 호스팅되는 위협 피드 컬렉션의 이름(예: guest.Abuse_ch)을 입력합니다.
Polling Interval(폴링 간격)	폴링 간격을 입력하여 TAXII 서버에서 위협 피드를 가져오는 빈도를 정의합니다. 최소값은 15분이고 기본값은 60분입니다.
위협 피드 기간	TAXII 서버에서 가져올 수 있는 위협 피드의 최대 기간을 입력합니다. 기간 값은 1~365일이어야 합니다.

파라미터 소스 상세정보	설명
폴링 세그먼트의 시간 범위	각 폴링 세그먼트에 대한 시간 범위를 입력합니다. 설문조사 세그먼트의 최소 기간은 1일입니다. 폴링 세그먼트의 최대 기간은 'Age of Threat Feeds(위협 피드 기간)'에 입력한 값입니다. 다음 시나리오에서는 'Time Span for Poll Segment(폴링 세그먼트의 시간 범위)' 옵션을 사용할 수 있습니다. • TAXII 서버의 위협 피드 기간에 대해 알려진 제한이 없는 경우 'Age of Threat Feeds(위협 피드 기간)' 옵션에 입력된 값을 사용합니다. • TAXII 서버의 위협 피드 기간에 대해 알려진 제한이 있는 경우 알려진 제한 값을 사용합니다. • TAXII 서버의 위협 피드 기간에 대해 알려진 제한을 모르는 경우 기본값 30일 사용합니다. • 'Age of Threat Feeds(위협 피드 기간)' 옵션에 입력한 값이 TAXII 서버에서 지원되지 않는 경우, 입력한 시간 범위에 따라 위협 피드의 기간을 여러 폴링 세그먼트로 분할할 수 있습니다. 예를 들어, 위협 피드 기간이 100일이고 TAXII 서버에 위협 피드 기간에 대한 제한(예: '40 days')이 고정되어 있는 경우 폴링 세그먼트에 대한 시간 범위를 40으로 입력합니다. 참고 폴링 세그먼트의 시간 범위가 작은 값(예: '5 days')인 경우 위협 피드 소스의 폴링을 완료 하는 데 시간이 오래 걸릴 수 있으며 이로 인해 게이트웨이의 성능이 저하될 수 있습니다.
HTTPS 사용	HTTPS를 사용하여 TAXII 서버에 연결하려면 **Yes(**예**)**를 선택합니다.
크리덴셜 구성	TAXII 서버에서 생성한 사용자 크리덴셜을 사용하여 TAXII 서버에 액세스하려면 **Yes(**예**)**를 선택합니다. 사용자 이름 및 비밀번호를 입력합니다.
프록시 세부 정보	

파라미터 소스 상세정보	설명
전역 프로시 사용	Cisco Email Security 게이트웨이가 프록시 서버를 통해 TAXII 서버에 연결하도록 하려면 **Yes(예)**를 선택합니다. 다음 방법 중 하나로 프록시 서버를 구성할 수 있습니다. • 웹 인터페이스의 Security Services > Service Updates(서비스 업데이트) 페이지 • CLI의 `updateconfig` 명령 **No(아니요)**를 선택하면 Cisco Email Security 게이트웨이가 TAXII 서버에 직접 연결됩니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

ETF 소스를 구성한 후에는 Cisco Email Security 게이트웨이가 TAXII 소스에서 위협 피드를 가져오기 시작합니다.

다음에 수행할 작업

- CLI의 **`threatfeedsconfig > sourceconfig`** 하위 명령을 사용하여 ETF 소스를 구성할 수도 있습니다.
- (선택 사항) Mail Policies(메일 정책) > External Threat Feeds Manager(외부 위협 피드 관리자) 페이지에서 **Suspend Polling(폴링 일시 중단)**( ) 아이콘을 클릭하여 구성된 ETF 소스에 대한 폴링 서비스를 일시 중단합니다.
- (선택 사항) Mail Policies(메일 정책) > External Threat Feeds Manager(외부 위협 피드 관리자) 페이지에서 **Resume Polling(폴링 재개)**( ) 아이콘을 클릭하여 구성된 ETF 소스에 대한 폴링 서비스를 재개합니다.
- (선택 사항) Mail Policies(메일 정책) > External Threat Feeds Manager(외부 위협 피드 관리자) 페이지에서 **Poll Now(지금 폴링)**을 클릭하여 마지막으로 성공한 폴링 간격에서 위협 피드를 즉시 가져옵니다.
- 위협이 포함된 메시지 처리, 312 페이지를 참조하십시오.

위협이 포함된 메시지 처리

다음을 사용하여 Cisco Email Security 게이트웨이에서 위협이 포함된 메시지를 처리할 수 있습니다.

- HAT
- 콘텐츠 또는 메시지 필터

관련 주제

- 위협이 포함된 메시지를 처리하기 위한 발신자 그룹 구성 , 313 페이지.
- 위협이 포함된 메시지를 처리하기 위한 콘텐츠 또는 메시지 필터 구성, 313 페이지.

위협이 포함된 메시지를 처리하기 위한 발신자 그룹 구성

EFT 엔진에서 가져온 판정을 사용하여 악성 IP에서 시작되는 메시지를 처리하도록 기존 발신자 그룹을 구성할 수 있습니다.

단계 **1** **Mail Policies(**메일 정책**) > HAT Overview(HAT** 개요**)** 페이지로 이동합니다.
단계 **2** 위협이 포함된 메시지를 처리하도록 구성하려는 기존 발신자 그룹을 클릭합니다.
단계 **3** **Edit Settings(**설정 편집**)**를 클릭합니다.
단계 **4** 악성 IP 주소를 필터링하는 데 필요한 ETF 소스를 선택합니다.
단계 **5** (선택 사항) 다른 ETF 소스를 추가하려면 **Add Row(**행 추가**)**를 클릭합니다.
단계 **6** 변경 사항을 제출 및 커밋합니다.

위협이 포함된 메시지를 처리하기 위한 콘텐츠 또는 메시지 필터 구성

다음과 같은 콘텐츠 또는 메시지 필터 중 하나 이상을 구성하여 ETF 엔진에서 가져온 판정을 기반으로 위협이 포함된 메시지에 대해 적절한 작업을 수행할 수 있습니다.

- URL 평판 - ETF 엔진에서 악성으로 분류된 URL을 탐지합니다.
- 도메인 평판 - ETF 엔진에서 악성으로 분류된 도메인을 탐지합니다.
- 파일 정보별 첨부 파일 - 파일 해시를 기반으로 ETF 엔진에서 악성으로 분류된 파일을 탐지합니다.

관련 주제

- 콘텐츠 필터를 사용하여 메시지에서 악성 도메인 탐지, 314 페이지.
- 메시지 필터를 사용하여 메시지에서 악성 도메인 탐지, 315 페이지
- 콘텐츠 필터를 사용하여 메시지에서 악성 URL 탐지, 315 페이지
- 메시지 필터를 사용하여 메시지에서 악성 URL 탐지, 317 페이지
- 콘텐츠 필터를 사용하여 메시지 첨부 파일에서 악성 파일 탐지, 318 페이지.

- 메시지 필터를 사용하여 메시지 첨부 파일에서 악성 파일 탐지 , 240 페이지.

콘텐츠 필터를 사용하여 메시지에서 악성 도메인 탐지

'도메인 평판' 콘텐츠 필터를 사용하여 ETF 엔진에서 악성으로 분류된 도메인을 탐지하고 해당 메시지에 대해 적절한 작업을 수행합니다.

시작하기 전에

- 선택 사항) 도메인만 포함된 주소 목록을 생성합니다. 웹 인터페이스에서 **Mail Policies(**메일 정책**) > Address Lists(**주소 목록**)** 페이지로 이동하거나 CLI에서 `addresslistconfig` 명령을 사용합니다. 자세한 내용은 메일 정책, 269 페이지의 내용을 참고하십시오.
- (선택 사항) 도메인 예외 목록을 생성합니다. 자세한 내용은 도메인 예외 목록 생성을 참고하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Content Filters(**수신 콘텐츠 필터**)**로 이동합니다.
단계 **2** **Add Filter(**필터 추가**)**를 클릭합니다.
단계 **3** 콘텐츠 필터의 이름과 설명을 입력합니다.
단계 **4** **Add Condition(**조건 추가**)**을 클릭합니다.
단계 **5** **Domain Reputation(**도메인 평판**)**을 클릭합니다.
단계 **6** **External Threat Feeds(**외부 위협 피드**)**를 선택합니다.
단계 **7** 메시지 헤더에서 악성 도메인을 탐지할 ETF 소스를 선택합니다.
단계 **8** 도메인의 평판을 확인할 필수 헤더를 선택합니다.
단계 **9** (선택 사항) Cisco Email Security 게이트웨이가 이 콘텐츠 필터에 대해 위협을 탐지하지 않도록 하려는 화이트리스트 도메인 목록을 선택합니다.
단계 **10** **OK(**확인**)**를 클릭합니다.
단계 **11** Add Action(작업 추가)을 클릭하여 악성 도메인이 포함된 메시지에 대해 수행할 적절한 조치를 구성합니다.
단계 **12** 변경 사항을 제출 및 커밋합니다.

도메인 예외 목록 생성

도메인 예외 목록은 도메인만 포함하는 주소 목록으로 구성됩니다. Cisco Email Security 게이트웨이에서 구성된 모든 도메인 평판 콘텐츠 또는 메시지 필터에 대한 도메인 확인을 건너뛰도록 하려는 경우 도메인 예외 목록을 사용할 수 있습니다.

단계 **1** **Security Services > Domain Reputation(**도메인 평판**)**으로 이동합니다.
단계 **2** 도메인 예외 목록 아래에서 **Edit Settings(**설정 수정**)**를 클릭합니다.
단계 **3** 도메인만 포함하는 필수 주소 목록을 선택합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

CLI에서 domainrepconfig 명령을 사용하여 도메인 예외 목록을 생성할 수도 있습니다. 자세한 내용은 *AsyncOS for Cisco Email Security Appliances CLI* 참조 가이드를 참고하십시오.

메시지 필터를 사용하여 메시지에서 악성 도메인 탐지

예를 들어, 다음 메시지 필터 규칙 구문을 사용하여 ETF 엔진을 통해 메시지에서 악성 도메인을 탐지하고 해당 메시지에 대해 적절한 조치를 취할 수 있습니다.

구문:

```
quarantine_msg_based_on_ETF: if (domain-external-threat-feeds (['etf_source1'],
 ['mail-from', 'from'], <'domain_exception_list'>)) { quarantine("Policy"); }
```

어디에서

- ‘`domain-external-threat-feeds`'는 도메인 평판 메시지 필터 규칙입니다.
- ‘`etf_source1`'은 메시지 헤더에서 악성 도메인을 탐지하는 데 사용되는 ETF 소스입니다.
- ‘`mail-from`','`from`'은 도메인의 평판을 확인하는 데 사용되는 필수 헤더입니다.
- '`domain_exception_list`'는 도메인 예외 목록의 이름입니다. 도메인 예외 목록이 없으면 ""로 표시됩니다.

예

다음 예에서는 'Errors To:' 맞춤형 헤더의 도메인이 ETF 엔진에서 악성으로 탐지된 경우 메시지가 격리됩니다.

```
Quaranting_Messages_with_Malicious_Domains: if domain-external-threat-feeds
(['threat_feed_source'], ['Errors-To'], "")) {quarantine("Policy");}
```

콘텐츠 필터를 사용하여 메시지에서 악성 **URL** 탐지

'URL 평판' 콘텐츠 필터를 사용하여 ETF 엔진에서 악성으로 분류된 URL을 탐지하고 해당 메시지에 대해 적절한 작업을 수행합니다.

다음 방법 중 하나로 ETF에 대한 'URL 평판' 콘텐츠 필터를 구성할 수 있습니다.

- 적절한 작업이 포함된 'URL 평판' 조건을 사용합니다.
- 조건에 상관없이 'URL 평판' 작업을 사용합니다.
- 'URL 평판' 조건 및 작업을 사용합니다.

다음 절차는 'URL 평판' 조건 및 작업을 사용하여 악성 URL을 탐지하는 데 사용됩니다.

참고

- 적절한 작업이 포함된 'URL 평판' 조건만 사용하려는 경우 절차의 11~20단계를 수행하지 마십시오.
- 조건에 상관없이 'URL 평판' 작업만 사용하려면 경우 절차의 4~10단계를 수행하지 마십시오.

시작하기 전에

- Cisco Email Security 게이트웨이에서 URL 필터링을 활성화해야 합니다. URL 필터링을 활성화하려면 웹 인터페이스에서 *Security Services* > *URL Filtering(URL* 필터링*)* 페이지로 이동합니다. 자세한 내용은 악의적이거나 바람직하지 않은 URL로부터 보호, 425 페이지의 내용을 참고하십시오.
- Cisco Email Security 게이트웨이에서 보안 침해 필터를 활성화해야 합니다. 보안 침해 필터를 활성화하려면 웹 인터페이스에서 *Security Services* > *Outbreak Filters(*보안 침해 필터*)* 페이지로 이동합니다. 자세한 내용은 신종 바이러스 필터(Outbreak Filter), 399 페이지의 내용을 참고하십시오.
- Cisco Email Security 게이트웨이에서 안티스팸 엔진을 활성화해야 합니다. 안티스팸 엔진을 활성화하려면 웹 인터페이스의 *Security Services* > *Anti-Spam(*안티스팸*)* 페이지로 이동합니다. 자세한 내용은 Anti-Spam, 355 페이지의 내용을 참고하십시오.
- (선택 사항) URL 목록을 생성합니다. 웹 인터페이스에서 *Mail Polices(Mail* 정책*)* > *URL Lists(URL* 목록*)* 페이지로 이동합니다. 자세한 내용은 악의적이거나 바람직하지 않은 URL로부터 보호, 425 페이지의 내용을 참고하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Content Filters(**수신 콘텐츠 필터**)**로 이동합니다.

단계 **2** **Add Filter(**필터 추가**)**를 클릭합니다.

단계 **3** 콘텐츠 필터의 이름과 설명을 입력합니다.

단계 **4** **Add Condition(**조건 추가**)**을 클릭합니다.

단계 **5** **URL Reputation(URL** 평판**)**을 클릭합니다.

단계 **6** **External Threat Feeds(**외부 위협 피드**)**를 선택합니다.

단계 **7** 악성 URL을 탐지할 ETF 소스를 선택합니다.

단계 **8** (선택 사항) Cisco Email Security 게이트웨이가 위협을 탐지하지 않도록 하려면 화이트리스트에 있는 URL 목록을 선택합니다.

단계 **9** 메시지 본문 및 제목 및/또는 메시지 첨부 파일에서 악성 URL을 탐지하려면 필수 **Check URLs within(**다음 범위 내에서 **URL** 확인**)** 옵션을 선택합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Add Action(**작업 추가**)**을 클릭합니다.

단계 **12** **URL Reputation(URL** 평판**)**을 클릭합니다.

단계 **13** **External Threat Feeds(**외부 위협 피드**)**를 선택합니다.

단계 **14** 조건에서 선택한 것과 동일한 ETF 소스를 선택해야 합니다(7단계).

단계 **15** (선택 사항) 8단계에서 선택한 화이트리스트 URL과 동일한 목록을 선택합니다.

단계 **16** '메시지 본문 및 제목' 및/또는 '메시지 첨부 파일'에서 악성 URL을 탐지하려면 필수 **Check URLs within(**다음 범위 내에서 **URL** 확인**)** 옵션을 선택합니다.

단계 **17** 메시지 본문 및 제목 및/또는 메시지 첨부 파일 내의 URL에 대해 수행할 필수 작업을 선택합니다.

참고 16단계에서 'Check URLs within(다음 범위 내에서 URL 확인)' 옵션을 'Attachments(첨부 파일)'로 선택한 경우 메시지에서 첨부 파일만 제거할 수 있습니다.

단계 **18** 모든 메시지 또는 서명되지 않은 메시지에 대해 작업을 수행할지 여부를 선택합니다.

단계 **19** **OK(**확인**)**를 클릭합니다.

단계 **20** 변경 사항을 제출 및 커밋합니다.

참고 어플라이언스에서 WBRS(웹 기반 평판 점수) 및 ETF에 대한 URL 평판 콘텐츠 필터를 구성한 경우, 어플라이언스의 성능을 높이기 위해 WBRS URL 평판 콘텐츠 필터의 순서를 ETF URL 평판 필터보다 높게 설정하는 것이 좋습니다.

메시지 필터를 사용하여 메시지에서 악성 **URL** 탐지

예를 들어, ETF 엔진을 사용하여 메시지에서 악성 URL을 탐지하고 해당 URL을 차단하려면 'URL 평판' 메시지 필터 규칙 구문을 사용합니다.

구문:

```
 defang_url_in_message: if (url-external-threat-feeds (['etf_source1'],
 <'URL_whitelist'>,
<'message_attachments'> , <'message_body_subject'> ,))
 { url-etf-defang(['etf-source1'], "", 0); } <'URL_whitelist'> ,
<'Preserve_signed'>)}
```

어디에서

- '`url-external-threat-feeds`'는 URL 평판 규칙입니다.
- '`etf_source1`'은 메시지 또는 메시지 첨부 파일에서 악성 URL을 탐지하는 데 사용되는 ETF 소스입니다.
- '`URL_whitelist`'는 URL 화이트리스트의 이름입니다. URL 화이트리스트가 없으면 ""로 표시됩니다.
- '`message_attachments`'는 메시지 첨부 파일에서 악성 URL을 확인하는 데 사용됩니다. 값 '1'은 메시지 첨부 파일에서 악성 URL을 탐지하는 데 사용됩니다.
- '`message_body_subject`'는 메시지 본문 및 제목에서 악성 URL을 확인하는 데 사용됩니다. 값 '1'은 메시지 본문 및 제목에서 악성 URL을 탐지하는 데 사용됩니다.

참고 값 "1,1"은 메시지 본문, 제목 및 메시지 첨부 파일에서 악성 URL을 탐지하는 데 사용됩니다.

- `'url-etf-defang'`은 악성 URL이 포함된 메시지에 대해 수행할 수 있는 작업 중 하나입니다.

  다음 예는 악성 URL이 포함된 메시지에 적용할 수 있는 ETF 기반 작업입니다.

  - url-etf-strip(['etf_source1'], "None", 1)
  - url-etf-defang-strip(['etf_source1'], "None", 1, "Attachment removed")
  - url-etf-defang-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1, " Attachment removed")
  - url-etf-replace(['etf_source1'], "", "None", 1)
  - url-etf-replace(['etf_source1'], "URL removed", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed ", "None", 1)
  - url-etf-replace-strip(['etf_source1'], "URL removed*", "None", 1, "Attachment removed")

- `'Preserve_signed'`는 '1' 또는 '0'으로 표시됩니다. '1'은 이 작업이 서명되지 않은 메시지에만 적용됨을 나타내고 '0'은 이 작업이 모든 메시지에 적용됨을 나타냅니다.

다음 예에서는 메시지 첨부 파일의 URL이 ETF 엔진에서 악성으로 탐지된 경우 해당 첨부 파일이 제거됩니다.

```
Strip_Malicious_URLs: if (true) {url-etf-strip(['threat_feed_source'], "", 0);}
```

콘텐츠 필터를 사용하여 메시지 첨부 파일에서 악성 파일 탐지

'첨부 파일 정보' 콘텐츠 필터를 사용하여 ETF 엔진에서 악성으로 분류된 메시지 첨부 파일의 파일을 탐지하고 해당 메시지에 대해 적절한 작업을 수행합니다.

참고 ETF 엔진은 파일의 파일 해시를 기반으로 조회를 수행합니다.

다음 방법 중 하나로 ETF에 대한 '첨부 파일 정보' 콘텐츠 필터를 구성할 수 있습니다.

- 적절한 작업이 포함된 '첨부 파일 정보' 조건을 사용합니다.
- 조건에 상관없이 '파일 정보별 첨부 파일 제거' 작업을 사용합니다.

- '첨부 파일 정보' 조건 및 '파일 정보별 첨부 파일 제거' 작업을 사용합니다.

다음 절차는 '파일 정보별 첨부 파일' 조건과 '파일 정보별 첨부 파일 제거' 작업을 사용하여 메시지 첨부 파일에서 악성 파일을 탐지하는 데 사용됩니다.

참고

- 적절한 작업이 포함된 '첨부 파일 정보' 조건만 사용하려는 경우 절차의 10~15단계를 수행하지 마십시오.
- 조건에 상관없이 '파일 정보별 첨부 파일 제거' 작업만 사용하려는 경우 절차의 4~9단계를 수행하지 마십시오.

시작하기 전에

(선택 사항) 파일 해시 예외 목록을 생성합니다. 웹 인터페이스에서 Mail Polices(Mail 정책) > File Hash Lists(파일 해시 목록) 페이지로 이동합니다. 자세한 내용은 파일 해시 목록 생성, 319 페이지의 내용을 참고하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Content Filters(**수신 콘텐츠 필터**)**로 이동합니다.
단계 **2** **Add Filter(**필터 추가**)**를 클릭합니다.
단계 **3** 콘텐츠 필터의 이름과 설명을 입력합니다.
단계 **4** **Add Condition(**조건 추가**)**을 클릭합니다.
단계 **5** **Attachment File Info(**첨부 파일 정보**)**를 클릭합니다.
단계 **6** **External Threat Feeds(**외부 위협 피드**)**를 선택합니다.
단계 **7** 파일 해시를 사용하여 악성 파일을 탐지할 ETF 소스를 선택합니다.
단계 **8** (선택 사항) Cisco Email Security 게이트웨이가 위협을 탐지하지 않도록 하려면 파일 해시 목록을 선택합니다.
단계 **9** **OK(**확인**)**를 클릭합니다.
단계 **10** **Add Action(**작업 추가**)**을 클릭합니다.
단계 **11** **Strip Attachment by File Info(**파일 정보별 첨부 파일 제거**)**를 클릭합니다.
단계 **12** **External Threat Feeds(**외부 위협 피드**)**를 선택합니다.
단계 **13** 조건에서 선택한 것과 동일한 etf 소스를 선택 했는지 확인 합니다 (7 단계).
단계 **14** (선택 사항) 8단계에서 선택한 파일 해시와 동일한 목록을 선택합니다.
단계 **15** 변경 사항을 제출 및 커밋합니다.

파일 해시 목록 생성

단계 **1** **Mail Policies(**메일 정책**) > File Hash Lists(**파일 해시 목록**)**로 이동합니다.
단계 **2** **Add File Hash List(**파일 해시 목록 추가**)**를 클릭합니다.

단계 **3** 필수 파일 해시 유형('SHA256' 또는 'MD5' 또는 둘 다)을 선택합니다.
단계 **4** 3단계에서 선택한 파일 해시를 쉼표로 구분하여 입력하거나 새 행으로 입력합니다.
단계 **5** 변경 사항을 제출 및 커밋합니다.

메시지 필터를 사용하여 메시지 첨부 파일에서 악성 파일 탐지

예를 들어, 다음 메시지 필터 규칙 구문을 사용하여 ETF 엔진에서 악성으로 분류된 메시지 첨부 파일을 탐지하고 해당 메시지에 대해 적절한 조치를 취할 수 있습니다.

구문:

```
Strip_malicious_files: if (file-hash-etf-rule (['etf_source1'], <'file_hash_exception_list'>))

{ file-hash-etf-strip-attachment-action (['etf_source1'], <'file_hash_exception_list>,
 "file stripped from message attachment"); }
```

여기서:

- ‘`file-hash-etf-rule`'은 첨부 파일 정보 메시지 필터 규칙입니다.
- ‘`etf_source1`'은 파일 해시를 기반으로 메시지에서 악성 파일을 탐지하는 데 사용되는 ETF 소스입니다.
- '`file_hash_exception_list`'는 파일 해시 예외 목록의 이름입니다. 파일 해시 예외 목록이 없으면 ""로 표시됩니다.
- '`file-hash-etf-strip-attachment-action`'은 악성 파일이 포함된 메시지에 적용하려는 작업의 이름입니다.

다음 예에서는 ETF 엔진에서 악성으로 탐지된 메시지 첨부 파일이 메시지에 포함된 경우 해당 첨부 파일이 제거됩니다.

```
Strip_Malicious_Attachment: if (true) {file-hash-etf-strip-attachment-action
(['threat_feed_source'], "", “Malicious message attachment has been stripped from
the message.");}
```

수신 메일 정책에 콘텐츠 필터 연결

메시지의 악성 도메인, URL 또는 파일 해시를 탐지하도록 구성한 하나 이상의 콘텐츠 필터를 수신 메일 정책에 연결할 수 있습니다.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)**로 이동합니다.
단계 **2** 특정 메일 정책의 **Content Filters(**콘텐츠 필터**)** 아래에 있는 링크를 클릭합니다.
단계 **3** **Enable Content Filters (Customize Settings)(**콘텐츠 필터 활성화**(**맞춤형 설정**))**를 선택합니다.
단계 **4** 악성 도메인, URL 또는 파일 해시를 탐지하기 위해 생성한 콘텐츠 필터를 선택합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

수신 메일 정책에 콘텐츠 필터를 연결한 후에는 Cisco Email Security 게이트웨이가 ETF 엔진에서 수신한 판정을 기반으로 메시지에 대한 작업을 수행하기 시작합니다.

외부 위협 피드 및 클러스터

중앙 집중식 관리를 사용할 경우 클러스터, 그룹 및 머신 수준에서 ETF 엔진과 메일 정책을 활성화할 수 있습니다.

외부 위협 피드 엔진 업데이트 모니터링

서비스 업데이트를 활성화한 경우 Cisco 업데이트 서버에서 ETF 엔진 업데이트가 검색됩니다. 그러나 일부 시나리오에서는(예: 자동 서비스 업데이트를 비활성화했거나 자동 서비스 업데이트가 작동하지 않는 경우) ETF 엔진 업데이트를 수동으로 확인할 수도 있습니다.

다음 방법 중 하나로 ETG 엔진을 수동으로 업데이트할 수 있습니다.

- 웹 인터페이스에서 **Security Services > External Threat Feeds(**외부 위협 피드**)** 페이지로 이동하여 **Update Now(**지금 업데이트**)**를 클릭합니다.
- CLI에서 `threatfeedupdate` 명령을 사용합니다.

기존 ETF 엔진의 상세정보를 확인하려면 웹 인터페이스에서 Security Services > External Threat Feeds(외부 위협 피드) 페이지의 'External Threat Feeds Engine Updates(외부 위협 피드 엔진 업데이트)' 섹션을 참조하거나 CLI에서 threatfeedstatus 명령을 사용합니다.

알림 보기

다음 표에는 알림에 대한 설명 및 알림 심각도를 포함하여 ETF 엔진에서 생성되는 알림이 나와 있습니다.

구성 요소/알림 이름	메시지 및 설명	매개변수
ETF 엔진 알림	세 번의 시도가 실패한 후에는 $source _name 소스에서 관찰 가능 개체를 가져올 수 없습니다. 실패 사유: $reason	**'source'** - TAXII 소스의 이름입니다. **'reason'** - 폴링이 실패한 이유입니다.
	Information(정보). TAXII 소스에서 피드를 폴링할 때 전송됩니다.	

구성 요소/알림 이름	메시지 및 설명	매개변수
ETF 엔진 알림	관찰 가능 유형 $type에 대해 $count개의 관찰 가능 개체의 스토리지 제한이 초과되었습니다.	**$count** - 유형당 허용되는 관찰 가능 개체 수입니다. **$ type** - 관찰 가능 개체의 유형입니다.
	Information(정보). 허용되는 관찰 가능 개체 수가 초과된 경우에 전송됩니다.	

메시지 추적에서 위협 상세정보 표시

선택한 ETF 소스에서 선택한 IOC에 해당하는 위협이 포함된 메시지 상세정보를 볼 수 있습니다.

시작하기 전에

- 이메일 게이트웨이에서 메시지 추적 기능을 활성화해야 합니다. 메시지 추적을 활성화하려면 웹 인터페이스에서 **Security Services > Centralized Services(**중앙 집중식 서비스**) > Message Tracking(**메시지 추적**)** 페이지로 이동합니다.
- 메시지에서 위협을 탐지하는 콘텐츠 또는 메시지 필터가 작동합니다.

단계 **1** **Monitor(**모니터**) > Message Tracking(**메시지 추적**)**으로 이동합니다.

단계 **2** **Advanced(**고급**)**를 클릭합니다.

단계 **3** Message Event(메시지 이벤트) 아래에서 **External Threat Feeds(**외부 위협 피드**)**를 선택합니다.

단계 **4** 선택한 IOC에 해당하는 위협이 포함된 메시지를 추적하기 위해 필요한 IOC를 선택합니다.

단계 **5** (선택 사항) Cisco Email Security 게이트웨이에 구성된 사용 가능한 ETF 소스 및 삭제된 ETF 소스를 기반으로 위협이 포함된 메시지를 보려면 **All External Threat Feed Sources(**모든 외부 위협 피드 소스**)**를 선택합니다.

단계 **6** (선택 사항) Cisco Email Security 게이트웨이에 구성된 사용 가능한 ETF 소스를 기반으로 위협이 포함된 메시지를 보려면 **Current External Threat Feed Sources(**현재 외부 위협 피드 소스**)**를 선택하고 필요한 ETF 소스를 선택합니다.

단계 **7** (선택 사항) 이 ETF 소스를 기반으로 위협이 포함된 메시지를 보려면 'External Threat Feed Sources(외부 위협 피드 소스)' 필드에 특정 ETF 소스의 이름을 입력합니다.

단계 **8** **Search(**검색**)**를 클릭합니다.

13 장

발신자 도메인 평판 필터링

이 장에는 다음 섹션이 포함되어 있습니다.

발신자 도메인 평판 필터링 개요

Cisco SDR(발신자 도메인 평판)은 발신자의 도메인 및 기타 속성을 기반으로 이메일 메시지에 대한 평판 판정을 제공하는 클라우드 서비스입니다.

Cisco SDR(발신자 도메인 평판)은 발신자의 도메인 및 기타 속성을 기반으로 이메일 메시지에 대한 평판 판정을 제공하는 클라우드 서비스입니다.

도메인 기반 평판 분석은 공유 IP 주소, 호스팅 또는 인프라 제공자의 평판을 확인하여 더 높은 탐지율을 지원하며, SMTP(Simple Mail Transfer Protocol) 대화 및 메시지 헤더에서 FQDN(Fully Qualified Domain Name) 및 기타 발신자 정보와 관련된 특성을 바탕으로 판정을 도출합니다.

자세한 내용은 Cisco 고객 연결 프로그램의 보안 트랙에서 Cisco Talos SDR(발신자 도메인 평판) 백서를 참고하십시오(http://www.cisco.com/go/ccp).

참고

- SDR 백서에 액세스하려면 Cisco 고객 연결 어카운트를 생성해야 합니다.
- Cisco IPAS 이의 제기와 마찬가지로 Cisco TAC(Technical Assistance Center)에서 지원 요청을 열어 SDR 이의 제기를 제출합니다.

SDR 판정

다음 표에는 SDR 판정 이름, 설명 및 권장 작업이 나열되어 있습니다.

표 ***34: SDR*** 판정

판정 이름	설명	권장 조치
매우 나쁨	최악의 평판 판정입니다. 차단 임계값이 보안보다 전달을 우선시하는 이 판정에만 설정된 경우 FN(미탐)이 표시됩니다.	메시지를 차단합니다.
나쁨	권장되는 차단 임계값입니다. 이렇게 하면 FN(미탐)과 FP(오탐) 간의 절충이 균형을 이룹니다. Talos는 SDR에 의해 차단된 메시지가 poor(나쁨) 또는 awful(매우 나쁨) 판정을 받도록 SDR을 조정합니다. 이 판정을 차단하지 않으면 보안보다 전달이 우선시되지만 이 판정에 따라 차단하지 않을 경우 고객이 허용하는 미탐이 발생합니다.	메시지를 차단합니다.
좋지 못함	발신자 평판은 의심입니다. 이러한 판정에 따른 차단은 적극적이며 Talos에서 권장되지 않습니다. 이는 전달보다 보안을 촉진하지만 이 판정에 따라 차단할 경우 사용자가 허용할 수 있는 오탐이 발생합니다.	어플라이언스에 구성된 다른 엔진으로 메시지를 검사합니다.
약함	중립 판정을 제외하는 약함 지표와 연관된 많은 도메인(적법 및 혼합 사용 포함)에 대한 일반적인 판정입니다. Talos는 이 판정에 따른 차단을 권장하지 않습니다. 이는 전달보다 보안을 우선시하지만 이 판정에 따라 메시지를 차단할 경우 허용되지 않는 수의 오탐(Talos에 따른)이 발생합니다.	어플라이언스에 구성된 다른 엔진으로 메시지를 검사합니다.

판정 이름	설명	권장 조치
알 수 없음	발신자가 새로 등록된 도메인 또는 SDR에서 인식할 수 없는 도메인을 사용하고 있습니다. 이 미확인 상태의 도메인에 대해 Talos는 추가 분석을 수행하여 신속하게 판정을 설정합니다. Talos는 이 판정에 따른 차단을 권장하지 않습니다. 이 판정에 따라 차단하면 이 판정에 대한 임계값을 조정할 때 사용자가 허용하는 많은 오탐이 발생합니다. Talos는 "unknown" 판정의 메시지를 격리하도록 권장합니다. 후속 엔진으로 메시지를 검사하기 전에 Talos에서 도메인을 조사할 수 있는 시간을 허용하기 위해 메시지 전달이 약간 지연됩니다.	메시지를 격리한 다음 격리가 종료되면 어플라이언스에 구성된 다른 엔진으로 검사합니다.
중간	발신자가 신규가 아닌 도메인을 사용하고 발신자 모범 사례를 준수하는 경우에 정상적으로 예상되는 판정입니다. 다음은 SPF, DKIM 서명, 스팸 전송 안 함 등을 사용하는 발신자 모범 사례입니다.	메시지를 허용하고 어플라이언스에 구성된 다른 엔진으로 메시지를 검사합니다.
Good	메시지가 DKIM 서명된 인증된 도메인을 사용하고 있음을 나타내는 드문 판정입니다("`From:`" 헤더 도메인에 맞춤).	메시지를 허용하고 어플라이언스에 구성된 다른 엔진으로 메시지를 검사합니다.

발신자 도메인 평판을 기준으로 메시지를 필터링하는 방법

단계	수행해야 할 작업	추가 정보
1단계	Cisco Email Security 게이트웨이에서 SDR 필터링을 활성화합니다. 참고 AsyncOS 12.0으로 업그레이드한 후 SDR 쿼리는 기본적으로 활성화됩니다.	Cisco Email Security 게이트웨이에서 발신자 도메인 평판 필터링 활성화, 326 페이지
2단계	SDR을 기반으로 메시지를 처리하도록 메시지 또는 콘텐츠 필터를 구성합니다.	발신자 도메인 평판을 기준으로 메시지를 처리하기 위한 메시지 또는 콘텐츠 필터 구성, 327 페이지
3단계	SDR을 기반으로 메시지를 필터링하도록 구성한 콘텐츠 필터를 수신 메일 정책에 연결합니다.	수신 메일 정책에 콘텐츠 필터 연결, 331 페이지

Cisco Email Security 게이트웨이에서 발신자 도메인 평판 필터링 활성화

참고 AsyncOS 12.0으로 업그레이드한 후 SDR 쿼리는 기본적으로 활성화됩니다.

단계 **1** **Security Services > Domain Reputation**(도메인 평판)으로 이동합니다.

단계 **2** **Enable**(활성화)을 클릭합니다.

단계 **3** **Enable Sender Domain Reputation Filtering**(발신자 도메인 평판 필터링 활성화)을 선택합니다.

단계 **4** (선택 사항) SDR 서비스가 메시지의 추가 특성을 기준으로 SDR을 확인하도록 하려면 **Include Additional Attributes**(추가 특성 포함)를 선택합니다.

이 옵션을 활성화하는 경우, 효율성을 개선하기 위해 메시지의 다음 추가 특성이 SDR 확인에 포함됩니다.

- `'Envelope From(봉투 발신자):'`, `'From(보낸 사람):'`, `'Reply-To(회신 대상):'` 헤더에 있는 이메일 주소의 일부인 사용자 이름입니다.
- `'From(보낸 사람):'` 및 `'Reply-To(회신 대상):'` 헤더에 있는 표시 이름입니다.

단계 **5** (선택 사항) SDR 쿼리 시간이 초과되기 전에 경과된 시간(초)을 입력합니다.

참고 SDR 쿼리 시간 제한 값을 수정하면 메일 처리 성능에 영향을 미칠 수 있습니다.

단계 **6** (선택 사항) 어플라이언스가 Envelope From(봉투 발신자): 헤더에 있는 도메인만을 기준으로 SDR 확인을 건너뛰도록 하려면 **Match Domain Exception List based on Domain in Envelope From Envelope From(**봉투 발신자의 도메인을 기준으로 한 일치하는 도메인 예외 목록**):**을 선택합니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

단계 **8** (선택 사항) SDR Include Additional Attributes Agreement(SDR에 추가 특성 포함 계약) 메시지에 동의하려면 **I Agree(**동의**)**를 클릭합니다.

참고 SDR Include Additional Attributes Agreement(SDR에 추가 특성 포함 계약) 메시지는 Include Additional Attributes(추가 특성 포함) 옵션을 선택한 경우에만 표시됩니다.

단계 **9** **Commit(**커밋**)**을 클릭하여 변경사항을 커밋합니다.

다음에 수행할 작업

SDR을 기반으로 메시지를 처리하도록 콘텐츠 또는 메시지 필터를 구성합니다. 발신자 도메인 평판을 기준으로 메시지를 처리하기 위한 메시지 또는 콘텐츠 필터 구성, 327 페이지를 참조하십시오.

발신자 도메인 평판을 기준으로 메시지를 처리하기 위한 메시지 또는 콘텐츠 필터 구성

다음 방법 중 하나로 '도메인 평판' 메시지 또는 콘텐츠 필터를 사용하여 SDR을 기준으로 메시지를 필터링하고 해당 메시지에 대해 적절한 작업을 수행할 수 있습니다.

- 발신자 도메인 판정
- 발신자 도메인 기간
- 발신인 도메인 평판 검사 불가

관련 주제

- 메시지 필터를 사용하여 발신자 도메인 평판을 기준으로 메시지 필터링, 328 페이지
- 콘텐츠 필터를 사용하여 발신자 도메인 평판을 기준으로 메시지 필터링, 330 페이지

메시지 필터를 사용하여 발신자 도메인 평판을 기준으로 메시지 필터링

발신자 도메인 판정을 기준으로 메시지 필터링

참고 권장되는 차단 임계값은 "Poor"입니다. SDR 판정에 대한 자세한 내용은 SDR 판정, 324 페이지 항목을 참고하십시오.

구문:

```
drop_msg_based_on_sdr_verdict:
if sdr-reputation (['awful', 'poor'], "<domain_exception_list>")
{drop();}
```

여기서:

- `'drop_msg_based_on_sdr_verdict'`는 메시지 필터의 이름입니다.
- `'sdr-reputation'`은 도메인 평판 메시지 필터 규칙입니다.
- `'awful','poor'`는 SDR을 기준으로 메시지를 필터링하는 데 사용되는 발신자 도메인 판정의 범위입니다.
- `'domain_exception_list'`는 도메인 예외 목록의 이름입니다. 도메인 예외 목록이 없으면 ""로 표시됩니다.
- `'drop'`은 메시지에 적용된 작업입니다.

예

다음 메시지에서 SDR 판정이 'Unknown'이면 메시지가 격리됩니다.

```
quarantine_unknown_sdr_verdicts:
if sdr-reputation (['unknown'], "")
{quarantine("Policy")}
```

발신자 도메인 기간을 기준으로 메시지 필터링

구문:

```
<msg_filter_name>
if sdr-age (<'unit'>, <'operator'> <'actual value'>)
{<action>}
```

여기서:

- `'sdr-reputation'`은 도메인 평판 메시지 필터 규칙입니다.
- `'sdr_age'`는 SDR을 기준으로 메시지를 필터링하는 데 사용되는 발신자 도메인 기간입니다.
- `'unit'`은 발신자 도메인 기간을 기준으로 메시지를 필터링하는 데 사용되는 'days', 'years', 'months' 또는 'weeks' 수 옵션입니다.
- `'operator'`는 발신자 도메인 기간을 기준으로 메시지를 필터링하는 데 사용되는 다음 비교 연산자입니다.

- – >(보다 큼)
- – >=(보다 크거나 같음)
- – <(보다 작음)
- – <=(보다 작거나 같음)
- – ==(같음)
- – !=(같지 않음)
- – Unknown(알 수 없음)

- ‘`actual value`'는 발신자 도메인 기간을 기준으로 메시지를 필터링하는 데 사용되는 번호입니다.

예

다음 메시지에서 발신자 도메인의 기간을 알 수 없는 경우 메시지가 삭제됩니다.

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("unknown", "")) {drop();}
```

다음 메시지에서 발신자 도메인의 기간이 한 달 미만이면 메시지가 삭제됩니다.

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("months", <, 1, "")) { drop(); }
```

발신자 도메인 스캔 불가를 기준으로 메시지 필터링

구문:

```
<msg_filter_name>
if sdr-unscannable (<'domain_exception_list'>)
{<action>}
```

여기서:

- '`sdr-unscannable`'은 도메인 평판 메시지 필터 규칙입니다.

  '`domain_exception_list`'는 도메인 예외 목록의 이름입니다. 도메인 예외 목록이 없으면 ""로 표시됩니다.

예

다음 메시지에서 SDR 판정이 'Unknown'이면 메시지가 격리됩니다.

```
Quarantine_Messages_Based_On_Sender_Domain_Unscannable: if (sdr-unscannable (""))
{quarantine("Policy");}
```

콘텐츠 필터를 사용하여 발신자 도메인 평판을 기준으로 메시지 필터링

시작하기 전에

- (선택 사항) 도메인만 포함된 주소 목록을 생성합니다. 웹 인터페이스에서 *Mail Policies(*메일 정책*)* > *Address Lists(*주소 목록*)* 페이지로 이동하거나 CLI에서 `addresslistconfig` 명령을 사용합니다. 자세한 내용은 메일 정책, 269 페이지의 내용을 참고하십시오.
- (선택 사항) 도메인 예외 목록을 생성합니다. 자세한 내용은 도메인 예외 목록 생성, 330 페이지의 내용을 참고하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Content Filters(**수신 콘텐츠 필터**)**로 이동합니다.

단계 **2** **Add Filter(**필터 추가**)**를 클릭합니다.

단계 **3** 콘텐츠 필터의 이름과 설명을 입력합니다.

단계 **4** **Add Condition(**조건 추가**)**을 클릭합니다.

단계 **5** **Domain Reputation(**도메인 평판**)**을 클릭합니다.

단계 **6** SDR을 기준으로 메시지를 필터링하려면 다음 조건 중 하나를 선택합니다.

- 판정 범위를 선택하여 SDR 서비스에서 수신한 판정을 기준으로 메시지를 필터링하려면 **Sender Domain Reputation Verdict(**발신자 도메인 평판 판정**)**를 선택합니다.

  참고 권장되는 차단 임계값은 "Poor"입니다. SDR 판정에 대한 자세한 내용은 SDR 판정, 324 페이지 항목을 참고하십시오.

- **Sender Domain Age(**발신자 도메인 기간**)**를 선택하고, 비교 연산자를 선택하고, 숫자를 입력하고, 발신자 도메인의 기간을 기준으로 메시지를 필터링할 기간을 선택합니다.
- SDR 확인에 실패한 메시지를 필터링하려면 **Sender Domain Reputation Unscannable(**발신자 도메인 평판 검사 불가**)**을 선택합니다.

단계 **7** (선택 사항) Cisco Email Security 게이트웨이가 SDR을 기준으로 메시지를 필터링하지 않도록 하려는 화이트리스트 도메인 목록을 선택합니다.

단계 **8** **Add Action(**작업 추가**)**을 클릭하여 SDR을 기준으로 메시지에 대해 수행할 적절한 작업을 구성합니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

도메인 예외 목록 생성

도메인 예외 목록은 도메인만 포함하는 주소 목록으로 구성됩니다. 도메인 예외 목록을 사용하여 Cisco Email Security 게이트웨이에 구성된 메일 정책에 관계없이 모든 수신 메시지에 대한 SDR 확인을 건너뛸 수 있습니다.

참고 특정 메일 정책에 대해 수신 메시지에서 SDR 콘텐츠 필터 작업을 건너뛰려면 도메인 평판 콘텐츠 필터에서 도메인 예외 목록을 선택해야 합니다.

도메인 예외 목록 사용 기준

SDR 검사를 건너뛰려면 기본적으로, 메시지의 `Envelope From(봉투 발신자):`, `From(보낸 사람):`, `Reply-To(회신 대상):` 내의 도메인은 도메인 예외 목록에 구성된 도메인과 일치해야 합니다. Envelope From(봉투 발신자): 헤더에 있는 도메인만을 기준으로 SDR 확인을 건너뛰려면 Domain Reputation settings(도메인 평판 설정) 페이지에서 'Match Domain Exception List based on Domain in Envelope From Envelope From(봉투 발신자의 도메인을 기준으로 한 일치하는 도메인 예외 목록)' 옵션을 선택합니다.

단계 **1** **Security Services > Domain Reputation(**도메인 평판**)**으로 이동합니다.

단계 **2** 도메인 예외 목록 아래에서 **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** 도메인만 포함하는 필수 주소 목록을 선택합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

CLI에서 `domainrepconfig` 명령을 사용하여 도메인 예외 목록을 생성할 수도 있습니다. 자세한 내용은 *AsyncOS for Cisco Email Security Appliance CLI* 참조 가이드를 참고하십시오.

수신 메일 정책에 콘텐츠 필터 연결

SDR을 기준으로 메시지를 필터링하도록 구성한 콘텐츠 필터를 수신 메일 정책에 연결할 수 있습니다.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)**로 이동합니다.

단계 **2** Content Filters(콘텐츠 필터) 아래의 링크를 클릭합니다.

단계 **3** **'Enable Content Filters (Customize Settings)(**콘텐츠 필터 활성화**(**맞춤형 설정**))'**를 선택해야 합니다.

단계 **4** SDR을 기준으로 메시지를 필터링하기 위해 생성한 콘텐츠 필터를 선택합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

발신자 도메인 평판 필터링 및 클러스터

중앙 집중식 관리를 사용할 경우 클러스터, 그룹 및 머신 수준에서 SDR 필터링과 메일 정책을 활성화할 수 있습니다.

메시지 추적에서 발신자 도메인 평판 상세정보 표시

메시지 추적을 사용하여 SDR을 기준으로 메시지 상세정보를 볼 수 있습니다.

시작하기 전에

- 이메일 게이트웨이에서 메시지 추적 기능을 활성화해야 합니다. 메시지 추적을 활성화하려면 웹 인터페이스에서 **Security Services > Message Tracking(**메시지 추적**)** 페이지로 이동합니다.
- SDR을 기준으로 메시지를 필터링하는 콘텐츠 또는 메시지 필터가 작동합니다.

단계 **1** **Monitor(**모니터**) > Message Tracking(**메시지 추적**)**으로 이동합니다.

단계 **2** **Advanced(**고급**)**를 클릭합니다.

단계 **3** Message Event(메시지 이벤트) 아래에서 **Sender Domain Reputation(**발신자 도메인 평판**)**을 선택합니다.

단계 **4** SDR 서비스에서 수신한 판정을 기반으로 메시지를 보려면 필요한 SDR 판정을 선택합니다.

단계 **5** (선택 사항) SDR 확인에 실패한 경우 메시지를 보려면 **Unscannable(**검사 불가**)**을 선택합니다.

단계 **6** (선택 사항) 위협 카테고리를 기준으로 메시지를 보려면 필요한 SDR 위협 카테고리를 선택합니다.

단계 **7** **Search(**검색**)**를 클릭합니다.

알림 보기

다음 표에는 알림에 대한 설명 및 알림 심각도를 포함하여 SDR에 대해 생성되는 시스템 알림이 나와 있습니다.

구성 요소/알림 이름	메시지 및 설명	매개변수
MAIL.IMH.SENDER_DOMAIN_LOOKUP_FAILURE_ALERTS	SDR 조회에 실패했습니다. 이유 - <$reason> Warning(경고) SDR 쿼리가 실패했을 때 전송됩니다.	**'reason'** - SDR 쿼리가 실패한 이유입니다.

로그 보기

SDR 필터링 정보가 메일 로그에 게시됩니다. 대부분의 정보는 Info(정보) 또는 Debug(디버그) 수준입니다.

SDR 필터링 로그 항목의 예

SDR 필터링 정보가 메일 로그에 게시됩니다. 대부분의 정보는 Info(정보) 또는 Debug(디버그) 수준입니다.

발신자 도메인 평판 인증 실패

이 예에서 로그는 SDR 서비스에 연결할 때의 인증 실패 때문에 SDR을 기준으로 필터링되지 않은 메시지를 표시합니다.

```
Mon Jul 2 08:57:18 2018 Info: New SMTP ICID 3 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 08:57:18 2018 Info: ICID 3 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS not enabled
 country not enabled
Mon Jul 2 08:57:18 2018 Info: Start MID 3 ICID 3
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 From: <sender1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 RID 0 To: <recipient1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>' Mon
 Jul 2 08:57:18 2018 Info: MID 3 Subject 'Message 001'
Mon Jul 2 08:57:19 2018 Info: MID 3 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Authentication failure.
```

해결책

CLI에서 `sdradvancedconfig` 명령을 사용하여 Cisco Email Security 게이트웨이를 SDR 서비스에 연결할 때 필요한 파라미터를 구성합니다.

발신인 도메인 평판 요청 시간 초과

이 예에서 로그는 SDR 서비스와 통신할 때의 요청 시간 초과 오류 때문에 SDR을 기준으로 필터링되지 않은 메시지를 표시합니다.

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com>
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Message 001'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Request timed out.
```

해결책

SDR 요청이 시간 초과되면 메시지가 검사 불가로 표시되고 구성된 작업이 메시지에 적용됩니다.

발신자 도메인 평판 잘못된 호스트

이 예에서 로그는 유효하지 않은 SDR 서비스 호스트가 Cisco Email Security 게이트웨이에 구성되어 있기 때문에 SDR을 기준으로 필터링되지 않은 메시지를 표시합니다.

```
Mon Jul 2 09:04:08 2018 Info: ICID 7 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS not enabled
 country not enabled
Mon Jul 2 09:04:08 2018 Info: Start MID 7 ICID 7
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 From: <sender1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>' Mon
 Jul 2 09:04:08 2018 Info: MID 7 Subject 'Message 001'
Mon Jul 2 09:04:08 2018 Info: MID 7 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Invalid host configured.
```

해결책

CLI에서 `sdradvancedconfig` 명령을 사용하여 Cisco Email Security 게이트웨이를 SDR 서비스에 연결할 때 필요한 파라미터를 구성합니다.

발신인 도메인 평판 일반 오류

이 예에서 로그는 알 수 없는 오류 때문에 SDR을 기준으로 필터링되지 않은 메시지를 표시합니다.

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Test mail'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Unknown error.
```

해결책

알 수 없는 오류가 발생하면 메시지가 검사 불가로 표시되고 구성된 작업이 메시지에 적용됩니다.

14 장

Anti-Virus

이 장에는 다음 섹션이 포함되어 있습니다.

안티바이러스 검사 개요

Cisco 어플라이언스에는 서드파티인 Sophos 및 McAfee의 통합 바이러스 검사 엔진이 포함되어 있습니다. 바이러스 검사 엔진 하나 또는 둘을 모두 사용하여 메시지에서 바이러스를 검사하기 위한 어플라이언스용 라이선스 키를 얻은 다음, 두 안티바이러스 검사 엔진 중 하나로 바이러스를 검사하도록 Cisco 어플라이언스를 구성할 수 있습니다.

McAfee 및 Sophos 엔진에는 특정 지점에서 파일을 검사하고, 파일에 있는 데이터를 사용해 바이러스 정의를 처리하고 패턴 매칭을 수행하며, 에뮬레이션 환경에서 바이러스 코드를 해독 및 실행하고, 신종 바이러스를 인식하기 위한 휴리스틱 기술을 적용하고, 합법적인 파일에서 감염된 코드를 제거하기 위한 프로그램 로직이 포함되어 있습니다.

일치하는 수신 또는 발신 메일 정책을 기반으로 메시지에서 바이러스를 검사하고 바이러스가 발견되면 메시지에 따라 서로 다른 작업을 수행하도록 어플라이언스를 구성할 수 있습니다. 이러한 작업에는 바이러스가 있는 메시지를 "복구"하고, 제목 헤더를 수정하고, X-header를 추가하고, 대체 주소나 메일호스트로 메시지를 전송하고, 메시지를 보관 또는 삭제하는 것이 포함됩니다.

활성화되면, 안티스팸 검사 직후 어플라이언스의 "작업 큐"에서 바이러스 검사가 수행됩니다 (이메일 파이프라인 및 보안 서비스, 63 페이지 참조).

기본적으로 바이러스 검사는 기본 수신 및 발신 메일 정책에 대해 활성화되어 있습니다.

관련 주제

평가 키

Cisco 어플라이언스는 사용 가능한 각 안티바이러스 검사 엔진에 대한 30일 무료 평가 키와 함께 제공됩니다. 시스템 설정 마법사나 Security Services(시스템 보안) > Sophos/McAfee Anti-Virus 페이지에서(GUI), 또는 `antivirusconfig`나 `systemsetup` 명령을 실행하여(CLI) 라이센스 계약에 액세스함으로써 평가 키를 활성화할 수 있습니다. 계약에 동의하면 기본적으로 안티바이러스 검사 엔진이 기본 수신 및 발신 메일 정책에 대해 활성화됩니다. 30일 평가 기간 이후에 기능을 활성화하는 방법에 대한 자세한 내용은 Cisco 세일즈 담당자에게 문의하십시오. **System Administration(시스템 관리) > Feature Keys(기능 키)** 페이지에서 또는 `featurekey` 명령을 실행하여 남은 평가 기간을 확인할 수 있습니다. (자세한 내용은 기능 키, 926 페이지를 참조하십시오.)

여러 안티바이러스 검사 엔진으로 메시지 검사

AsyncOS는 여러 안티바이러스 검사 엔진을 이용한 메시지 검사, 즉 다중 레이어 안티바이러스 검사를 지원합니다. 메일 정책 기준으로 하나 또는 두 개의 라이센스된 안티바이러스 검사 엔진을 사용하도록 Cisco 어플라이언스를 구성할 수 있습니다. 예를 들면 실행을 위한 메일 정책을 만들고, Sophos 및 McAfee 엔진으로 메일을 검사하도록 이 정책을 구성할 수 있습니다.

여러 검사 엔진으로 메시지를 검사하면 Sophos 및 McAfee 안티바이러스 검사 엔진의 이점을 결합하여 "심층적인 방어"를 제공할 수 있습니다. 각 엔진은 주도적인 안티바이러스 캡처 비율을 가지고 있지만 바이러스 탐지에 별도의 기술 기반을 사용하므로(McAfee Anti-Virus 필터링, 339 페이지 및 Sophos 안티 바이러스 필터링, 336 페이지 참조) 다중 검사 접근 방식이 훨씬 더 효과적일 수 있습니다. 여러 검사 엔진을 사용하면 시스템 처리량이 감소할 수 있습니다. 자세한 내용은 Cisco 지원 담당자에게 문의하십시오.

바이러스 검사의 순서는 구성할 수 없습니다. 멀티레이어 안티바이러스 검사를 활성화하면 McAfee 엔진이 먼저 바이러스를 검사하고, 그 다음에 Sophos 엔진이 바이러스를 검사합니다. McAfee 엔진이 특정 메시지에 바이러스가 없다고 판단하면, Sophos 엔진이 해당 메시지를 검사하고 두 번째 보호 레이어를 추가합니다. McAfee 엔진이 메시지에 바이러스가 있다고 판단하면 Cisco 어플라이언스는 Sophos 검사를 건너뛰고, 구성된 설정을 기반으로 바이러스 메시지에 대한 작업을 수행합니다.

Sophos 안티 바이러스 필터링

Cisco 어플라이언스에는 Sophos, Plc.의 통합 바이러스 검사 기술이 포함되어 있습니다. Sophos Anti-Virus는 플랫폼 간 안티바이러스 보호, 탐지 및 치료를 제공합니다.

Sophos Anti-Virus의 바이러스 탐지 엔진은 파일에서 바이러스, 트로이 목마 및 웜을 검사합니다. 이러한 프로그램은 "악성 소프트웨어"를 의미하는 악성코드라는 일반 용어로 정의됩니다. 모든 악성코드 유형 간 유사성 때문에 안티바이러스 스캐너는 바이러스뿐 아니라 모든 유형의 악성 소프트웨어를 탐지하고 제거할 수 있습니다.

관련 주제

- 바이러스 탐지 엔진, 337 페이지
- 바이러스 검사, 337 페이지
- 탐지 방법, 337 페이지

바이러스 탐지 엔진

Sophos 바이러스 탐지 엔진은 Sophos Anti-Virus 기술의 중심으로서, 잘 정의된 인터페이스의 여러 개체로 구성된 Microsoft의 COM(Component Object Model)과 유사한 독점적인 아키텍처를 사용합니다. 엔진에서 사용하는 모듈식 필터링 시스템은 별도의 자체 포함식 동적 라이브러리를 기반으로 합니다. 각 라이브러리는 예를 들면 파일 형식과 같은 서로 다른 "스토리지 클래스"를 처리합니다. 이 접근 방식 덕분에 유형과 상관없이 일반 데이터 소스에 바이러스 검사를 적용할 수 있습니다.

엔진에 포함된 데이터 로드 및 검색에 대한 전문화된 기술을 통해 매우 빠른 검사 속도가 구현됩니다. 여기에는 다음이 통합되어 있습니다.

- 다형성 바이러스 탐지를 위한 전체 코드 에뮬레이터
- 아카이브 파일 내부를 검사하기 위한 온라인 압축 해제 프로그램
- 매크로 바이러스를 탐지하고 치료하기 위한 OLE2 엔진

Cisco 어플라이언스는 SAV 인터페이스를 사용하여 바이러스 엔진을 통합합니다.

바이러스 검사

넓은 의미에서 엔진의 검사 기능은 중요한 두 구성 요소(어디를 살펴봐야 할지 아는 분류기 및 무엇을 살펴봐야 할지 아는 바이러스 데이터베이스)의 강력한 결합에 의해 관리됩니다. 엔진은 확장자에 의존하기보다는 형식으로 파일을 분류합니다.

바이러스 엔진은 시스템에서 수신한 메시지의 본문과 첨부 파일에서 바이러스를 검사합니다. 첨부 파일의 파일 형식은 검사를 결정하는 데 도움이 됩니다. 예를 들어, 메시지에 첨부된 파일이 실행 파일이면 엔진은 실행 코드가 시작되는 위치를 알려주는 헤더를 찾아 검사합니다. 파일이 Word 문서이면 매크로 스트림을 살펴봅니다. 메일 메시징에 사용되는 MIME 파일이면 첨부 파일이 저장된 곳을 살펴봅니다.

탐지 방법

바이러스를 탐지하는 방법은 유형에 따라 다릅니다. 검사 프로세스 중에 엔진은 각 파일을 분석하고 형식을 식별하고 관련 기술을 적용합니다. 모든 방법의 기반은 특정 지침 유형 또는 특정 지침 순서를 찾는 기본 개념입니다.

관련 주제

패턴 매칭

패턴 매칭 기술에서 엔진은 특별한 코드 시퀀스를 알고 있으며, 코드를 바이러스로 식별할 정확한 일치를 찾습니다. 엔진은 알려진 바이러스 코드 시퀀스와 유사한(동일할 필요는 없음) 코드 시퀀스를 찾는 경우가 더 많습니다. 검사 중 어떤 파일을 비교할지에 대한 설명을 만드는 과정에서 Sophos 바이러스 연구자들은 아래에 설명한 대로 휴리스틱을 사용하여 엔진이 원래 바이러스뿐 아니라 이후의 변종도 찾을 수 있도록 식별 코드를 최대한 일반적으로 유지하기 위해 노력합니다.

휴리스틱

Sophos 연구자들이 하나의 군에서 바이러스를 하나만 분석했더라도 동일한 군의 여러 바이러스를 탐지할 수 있도록, 바이러스 엔진은 기본 패턴 매칭 기술을 휴리스틱(특정 규칙보다는 일반 규칙을 사용하는 기술)과 결합할 수 있습니다. 이 기술에서는 한 바이러스의 여러 변종을 포착할 단일 설명을 만들 수 있습니다. Sophos는 휴리스틱을 다른 방법과 조율하여 오탐 발생을 최소화합니다.

에뮬레이션

에뮬레이션은 바이러스 엔진에 의해 다형성 바이러스에 적용되는 기술입니다. 다형성 바이러스는 스스로를 숨기기 위해 자신을 수정하는 암호화된 바이러스입니다. 시각적인 고정 바이러스 코드가 없으며, 바이러스는 확산될 때마다 스스로를 다르게 암호화합니다. 실행될 때 스스로 해독합니다. 바이러스 탐지 엔진의 에뮬레이터는 DOS 및 Windows 실행 파일에서 사용되는 반면, 다형성 매크로 바이러스는 Sophos의 Virus Description Language로 작성된 탐지 코드에 의해 발견됩니다.

이 해독의 출력은 실제 바이러스 코드이며, 에뮬레이터에서 실행된 후 Sophos 바이러스 탐지 엔진에 의해 탐지되는 것이 바로 이 출력입니다.

검사를 위해 엔진으로 전송되는 실행 파일은 에뮬레이터 내에서 실행되며, 에뮬레이터는 바이러스 본문이 메모리에 기록될 때 이의 해독을 추적합니다. 일반적으로 바이러스 엔트리 포인트는 파일 프런트 엔드에 있으며 처음 실행됩니다. 대부분의 경우 바이러스를 인식하는 데에는 소량의 바이러스 본문만 해독됩니다. 대부분의 정상 실행 파일은 몇 가지 지침 후 에뮬레이션을 중단하는데, 이 경우 오버헤드가 줄어듭니다.

에뮬레이터는 제한된 영역에서 실행되므로, 코드가 바이러스인 것으로 판명되는 경우 어플라이언스를 감염시키지 않습니다.

바이러스 설명

Sophos는 다른 신뢰할 수 있는 안티바이러스 회사와 매달 바이러스를 교환합니다. 또한 고객이 매달 수천 개의 의심스런 파일을 Sophos로 전송하며, 그중 약 30%는 바이러스로 판명됩니다. 각 샘플은 바이러스 여부를 확인하기 위해 매우 안전한 바이러스 랩에서 엄격한 분석을 거칩니다. 새로 발견된 각 바이러스 또는 바이러스의 그룹에 대해 Sophos는 설명을 만듭니다.

Sophos 알림

Cisco는 Sophos Anti-Virus 검사를 활성화한 고객에게 Sophos 사이트 http://www.sophos.com/virusinfo/notifications/에서 Sophos 알림을 구독할 것을 권장합니다. Sophos에서 직접 알림 수신을 구독하면 최근에 발생한 신종 바이러스 및 사용 가능한 해결책을 알 수 있습니다.

바이러스가 발견되는 경우

바이러스가 탐지되면 Sophos Anti-Virus는 파일을 복구(치료)할 수 있습니다. Sophos Anti-Virus는 대개 바이러스가 발견된 파일을 복구할 수 있으며, 그 후에는 해당 파일을 위험 없이 사용할 수 있습니다. 수행하는 정확한 작업은 바이러스에 따라 다릅니다.

파일을 원래 상태로 되돌리는 것이 항상 가능하지는 않으므로 치료에 제한이 따를 수 있습니다. 어떤 바이러스는 실행 프로그램의 일부를 덮어쓰는데, 이는 되돌릴 수 없습니다. 이러한 경우, 복구 불가능한 첨부 파일의 메시지를 처리하는 방법을 정의합니다. 이메일 보안 기능을 사용하여 수신자 단위로 이 설정을 구성합니다. **Mail Policies > Incoming or Outgoing Mail Policies**(메일 정책 > 수신 또는 발신 메일 정책) 페이지(GUI) 또는 `policyconfig -> antivirus` 명령(CLI)을 사용합니다. 이러한 설정의 구성에 대한 자세한 내용은 사용자에 대한 바이러스 검사 작업 구성, 342 페이지를 참조하십시오.

McAfee Anti-Virus 필터링

McAfee® 검사 엔진은 다음을 수행합니다.

- 파일에 있는 데이터를 이용한 패턴 매칭 바이러스 서명으로 파일을 검사합니다.
- 에뮬레이션 환경에서 바이러스 코드를 해독 및 실행합니다.
- 신종 바이러스를 인식하기 위해 휴리스틱 기술을 적용합니다.
- 파일에서 감염된 코드를 제거합니다.

관련 주제

- 패턴 매칭 바이러스 서명, 339 페이지
- 암호화된 다형성 바이러스 탐지, 339 페이지
- 휴리스틱 분석, 340 페이지
- 바이러스가 발견되는 경우, 339 페이지

패턴 매칭 바이러스 서명

McAfee는 특별한 바이러스, 바이러스 유형 또는 기타 잠재적으로 원치 않는 소프트웨어를 탐지하기 위해 검색 엔진과 함께 안티바이러스 정의(DAT) 파일을 사용합니다. 이 둘을 통해 파일의 알려진 위치에서 시작한 다음 바이러스 서명을 검색하여 간단한 바이러스를 탐지합니다. 파일에 바이러스가 없는지를 판단하기 위해 해당 파일의 일부만 검색해야 하는 경우도 종종 있습니다.

암호화된 다형성 바이러스 탐지

복잡한 바이러스는 두 가지 인기 있는 기술을 사용하여 서명 검사의 탐지를 회피합니다.

- 암호화. 바이러스 내부의 데이터는 안티바이러스 스캐너가 바이러스의 컴퓨터 코드 또는 메시지를 볼 수 없도록 암호화됩니다. 바이러스는 활성화되면 자체를 실행 버전으로 변환하여 실행합니다.
- 다형성. 바이러스가 자체 복제될 때 모양이 바뀐다는 점을 제외하면 이 프로세스는 암호화와 유사합니다.

그러한 바이러스에 대처하기 위해 에뮬레이션이라는 기술이 엔진에 사용됩니다. 파일에 그러한 바이러스가 포함되었다고 의심되면 엔진은 바이러스가 자체 해독을 통해 진짜 모습이 보이게 될 때까지 해를 입히지 않고 실행될 수 있는 인위적인 환경을 만듭니다. 그러면 엔진은 바이러스 서명을 검사하여 정상적으로 바이러스를 식별할 수 있습니다.

휴리스틱 분석

바이러스 서명만 사용하면 서명이 아직 알려지지 않았으므로 엔진에서 신종 바이러스를 탐지할 수 없습니다. 따라서 엔진은 휴리스틱 분석이라는 추가 기술을 사용할 수 있습니다.

바이러스를 운반하는 프로그램, 문서 또는 이메일 메시지는 종종 특이한 기능을 가지고 있습니다. 프롬프트 없이 파일을 수정하거나, 메일 클라이언트를 호출하거나, 자체 복제를 위한 다른 수단을 사용하려고 시도합니다. 엔진은 이러한 종류의 컴퓨터 명령을 탐지하기 위해 프로그램 코드를 분석합니다. 엔진은 또한 잘못된 경보를 피하기 위해, 작업 수행 전에 사용자에게 프롬프트를 표시하는 등의 바이러스 같지 않은 정상적인 동작도 검색합니다.

이러한 기술을 사용하여 엔진은 많은 신종 바이러스를 탐지할 수 있습니다.

바이러스가 발견되는 경우

바이러스가 탐지되면 Sophos Anti-Virus는 파일을 복구(치료)할 수 있습니다. Sophos Anti-Virus는 대개 바이러스가 발견된 파일을 복구할 수 있으며, 그 후에는 해당 파일을 위험 없이 사용할 수 있습니다. 수행하는 정확한 작업은 바이러스에 따라 다릅니다.

파일을 원래 상태로 되돌리는 것이 항상 가능하지는 않으므로 치료에 제한이 따를 수 있습니다. 어떤 바이러스는 실행 프로그램의 일부를 덮어쓰는데, 이는 되돌릴 수 없습니다. 이러한 경우, 복구 불가능한 첨부 파일의 메시지를 처리하는 방법을 정의합니다. 이메일 보안 기능을 사용하여 수신자 단위로 이 설정을 구성합니다. **Mail Policies > Incoming or Outgoing Mail Policies(**메일 정책 > 수신 또는 발신 메일 정책**)** 페이지(GUI) 또는 `policyconfig -> antivirus` 명령(CLI)을 사용합니다. 이러한 설정의 구성에 대한 자세한 내용은 사용자에 대한 바이러스 검사 작업 구성, 342 페이지를 참조하십시오.

바이러스를 검사하도록 어플라이언스를 구성하는 방법

메시지에서 바이러스를 검사하는 방법

	수행해야 할 작업	추가 정보
1단계	Email Security Appliance에서 안티바이러스 검사를 활성화합니다.	바이러스 검사 활성화 및 전역 설정 구성 , 341 페이지
2단계	메시지에서 바이러스를 검사할 사용자 그룹을 정의합니다.	발신자 및 수신자 그룹에 대한 메일 정책 만들기, 276 페이지
3단계	(선택 사항) 바이러스 격리에서 메시지를 처리할 방법을 구성합니다.	정책, 바이러스, Outbreak 격리 구성 , 852 페이지

	수행해야 할 작업	추가 정보
4단계	어플라이언스에서 바이러스가 포함된 메시지를 처리할 방법을 결정합니다.	사용자에 대한 바이러스 검사 작업 구성, 342 페이지
5단계	정의한 사용자 그룹에 대해 안티바이러스 검사 규칙을 구성합니다.	발신자 및 수신자의 서로 다른 그룹에 대해 안티바이러스 정책 구성, 347 페이지
6단계	(선택 사항) 컨피그레이션을 테스트하도록 이메일 메시지를 전송합니다.	안티바이러스 검사 테스트를 위해 이메일을 어플라이언스로 전송 , 351 페이지

관련 주제

- 바이러스 검사 활성화 및 전역 설정 구성 , 341 페이지
- 사용자에 대한 바이러스 검사 작업 구성, 342 페이지
- 발신자 및 수신자의 서로 다른 그룹에 대해 안티바이러스 정책 구성, 347 페이지
- 안티바이러스 구성에 대한 참고 사항, 348 페이지
- 안티바이러스 작업의 흐름도, 350 페이지

바이러스 검사 활성화 및 전역 설정 구성

시스템 설정 마법사를 실행할 때 바이러스 검사 엔진을 활성화했을 수 있습니다. 그것과 상관없이 다음 절차를 사용하여 설정을 구성합니다.

참고 기능 키에 따라 Sophos, McAfee 또는 둘 다를 활성화할 수 있습니다.

단계 **1** **Security Services(**보안 서비스**) > McAfee** 페이지로 이동합니다.

또는

Security Services(보안 서비스**) > Sophos** 페이지로 이동합니다.

단계 **2** **Enable(**활성화**)**을 클릭합니다.

참고 **Enable(**활성화**)**을 클릭하면 어플라이언스에 대해 기능이 전역적으로 활성화됩니다. 그러나 나중에 메일 정책에서 수신자별로 설정을 활성화해야 합니다.

단계 **3** 라이센스 정책을 읽은 후 페이지 하단으로 스크롤하고 **Accept(**동의**)**를 클릭하여 계약에 동의합니다.

단계 **4** **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **5** 최대 바이러스 검사 시간 초과 값을 선택합니다.

시스템이 메시지에 대해 안티바이러스 검사 수행을 중지할 시간 초과 값을 구성합니다. 기본값은 60초입니다.

단계 **6** (선택 사항) **Enable Automatic Updates(**자동 업데이트 활성화**)**를 클릭하여 엔진의 자동 업데이트를 활성화합니다.

어플라이언스는 업데이트 서버에서 특정 엔진의 필수 업데이트를 가져왔습니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

수신자 단위로 안티바이러스 설정을 구성합니다. 사용자에 대한 바이러스 검사 작업 구성, 342 페이지를 참조하십시오.

사용자에 대한 바이러스 검사 작업 구성

Cisco 어플라이언스에 통합된 바이러스 검사 엔진은 이메일 보안 관리자 기능을 사용하여 구성한 정책(구성 옵션)을 기반으로 수신 및 발신 메일에서 메시지의 바이러스를 처리합니다. 이메일 보안 기능을 사용하여 수신자 단위로 안티바이러스 작업을 활성화합니다. Mail Policies(메일 정책) > Incoming or Outgoing Mail Policies(수신 또는 발신 메일 정책) 페이지(GUI) 또는 `policyconfig > antivirus` 명령(CLI)을 사용합니다.

관련 주제

- 메시지 검사 설정, 342 페이지
- 메시지 처리 설정, 343 페이지
- 메시지 처리 작업에 대한 설정 구성, 344 페이지

메시지 검사 설정

- Scan for Viruses Only(바이러스 검사만 수행)

  시스템에서 처리하는 메시지에 대해 바이러스 검사가 수행됩니다. 감염된 첨부 파일에 대해서는 복구가 시도되지 않습니다. 첨부 파일을 삭제하고 바이러스가 포함되어 있거나 복구할 수 없는 메시지를 메일로 전달할지 여부를 선택할 수 있습니다.

- Scan and Repair Viruses(바이러스 검사 후 복구)

  시스템에서 처리하는 메시지에 대해 바이러스 검사가 수행됩니다. 첨부 파일에서 바이러스가 발견되면 시스템은 첨부 파일 "복구"를 시도합니다.

- Dropping Attachments(첨부 파일 삭제)

  감염된 첨부 파일을 삭제하도록 선택할 수 있습니다.

  안티바이러스 검사 엔진에서 감염된 메시지 첨부 파일을 검사하고 삭제한 경우 첨부 파일이 "제거된 첨부 파일"이라는 새 첨부 파일로 교체됩니다. 첨부 파일 형식은 일반 텍스트이며 다음을 포함합니다.

```
This attachment contained a virus and was stripped.
 Filename: filename
Content-Type: application/filetype
```

메시지가 불량 첨부 파일로 감염되어 수정되었다는 알림이 항상 사용자에게 제공됩니다. 보조 알림 작업도 구성할 수 있습니다(알림 전송, 346 페이지 참조). 감염된 첨부 파일을 삭제하기로 선택한 경우 사용자에게 메시지가 수정되었음을 알리기 위한 알림 작업이 필요하지 않습니다.

- X-IronPort-AV 헤더

  어플라이언스에서 안티바이러스 검사 엔진으로 처리된 모든 메시지에는 X-IronPort-AV: 헤더가 추가됩니다. 이 헤더는 안티바이러스 구성, 특히 "검사 불가"로 간주된 메시지에서 문제를 디버깅할 때 추가 정보를 제공합니다. 검사한 메시지에 X-IronPort-AV 헤더를 포함할지 여부를 전환할 수 있습니다. 이 헤더를 포함할 것을 권장합니다.

메시지 처리 설정

리스너에서 수신하는 서로 다른 메시지 클래스를 각각에 맞는 작업으로 처리하도록 바이러스 검사 엔진을 구성합니다. 그림 - 바이러스를 검사한 메시지 처리 옵션에는 바이러스 검사 엔진이 활성화될 때 시스템이 수행하는 작업이 요약되어 있습니다.

다음의 각 메시지 유형에 대해 어떤 작업을 수행할지를 선택할 수 있습니다. 작업은 아래에 설명되어 있습니다(메시지 처리 작업에 대한 설정 구성, 344 페이지 참조). 예를 들면 바이러스에 감염된 메시지에 대해 감염된 첨부 파일을 삭제하고, 이메일 제목을 수정하고, 메시지 수신자에게 맞춤형 알림을 전송하도록 안티바이러스 설정을 구성할 수 있습니다.

복구된 메시지 처리

메시지를 완전히 검사하여 모든 바이러스를 복구 또는 제거한 경우에는 복구된 메시지로 간주됩니다. 이러한 메시지는 있는 그대로 전달됩니다.

암호화된 메시지 처리

메시지의 암호화되거나 보호된 필드 때문에 엔진이 검사를 완료할 수 없는 경우에는 암호화된 메시지로 간주됩니다. 암호화된 것으로 표시된 메시지도 역시 복구할 수 있습니다.

암호화 탐지 메시지 필터 규칙(암호화 탐지 규칙, 173 페이지 참조)과 "암호화된" 메시지에 대한 바이러스 검사 작업 간에는 차이가 있습니다. 암호화된 메시지 필터 규칙은 PGP 또는 S/MIME으로 암호화된 메시지를 "참"으로 평가합니다. 암호화된 규칙은 PGP 및 S/MIME으로 암호화된 데이터만 탐지할 수 있습니다. 비밀번호로 보호된 ZIP 파일이나 암호화된 내용이 포함된 Microsoft Word 및 Excel 문서는 탐지하지 않습니다. 바이러스 검사 엔진은 비밀번호로 보호된 메시지나 첨부 파일을 "암호화된" 것으로 간주합니다.

참고 3.8 이하의 AsyncOS 버전에서 업그레이드하여 Sophos Anti-Virus 검사를 구성한 경우, 업그레이드 후 암호화된 메시지 처리 섹션을 구성해야 합니다.

검사 불가 메시지 처리

검사 시간 초과 값에 도달했거나 내부 오류 때문에 엔진을 사용할 수 없게 된 경우 메시지를 검사 불가로 간주합니다. 검사 불가로 표시된 메시지도 역시 복구할 수 있습니다.

바이러스 감염 메시지 처리

시스템에서는 첨부 파일을 삭제할 수 없거나 메시지를 완전히 복구하지 못할 수 있습니다. 이러한 경우, 여전히 바이러스가 포함되어 있을 수 있는 메시지를 시스템에서 처리하는 방법을 구성할 수 있습니다.

암호화된 메시지, 검사 불가 메시지 및 바이러스 메시지에 대한 컨피그레이션 옵션은 동일합니다.

메시지 처리 작업에 대한 설정 구성

적용할 작업

암호화된 메시지, 검사 불가 메시지 또는 바이러스 감염 메시지 등의 각 메시지 유형에 대해 수행할 작업을 선택합니다. 메시지를 삭제하거나, 메시지를 새 메시지의 첨부 파일로 전달하거나, 메시지를 그대로 전달하거나, 안티바이러스 격리 영역으로 메시지를 전송할 수 있습니다(격리 및 안티바이러스 검사, 345 페이지).

감염된 메시지를 새 메시지의 첨부 파일로 전달하도록 어플라이언스를 구성하는 경우 수신자가 감염된 원래 첨부 파일의 처리 방법을 선택하도록 할 수 있습니다.

메시지를 전달하거나 새 메시지의 첨부 파일로 전달하려는 경우 추가로 다음을 수행할 수 있습니다.

- 메시지 제목 수정
- 원본 메시지 보관
- 일반 알림 전송 다음 작업은 GUI의 "Advanced(고급)" 섹션에서 사용할 수 있습니다.
- 메시지에 사용자 지정 헤더 추가
- 메시지 수신자 수정
- 대체 대상 호스트로 메시지 전송
- 맞춤형 알림 전송

참고 이러한 작업은 상호 배타적이지 않습니다. 사용자 그룹에 대한 서로 다른 처리 요구에 따라 서로 다른 수신 또는 발신 정책 내에서 각기 다르게 일부 또는 전체를 결합할 수 있습니다. 이러한 옵션을 사용하여 다양한 검사 정책을 정의하는 방법에 대한 자세한 내용은 다음 섹션 및 안티바이러스 구성에 대한 참고 사항, 348 페이지 섹션을 참조하십시오.

복구된 메시지는 사용자 지정 헤더 추가 및 사용자 지정 알림 전송이라는 두 가지 고급 옵션만 사용할 수 있습니다. 다른 모든 메시지 유형은 모든 고급 옵션에 액세스할 수 있습니다.

격리 및 안티바이러스 검사

격리를 위해 플래그를 지정하면 메시지는 계속해서 이메일 파이프라인의 나머지를 지나갑니다. 하나 이상의 격리에 대해 플래그가 지정된 메시지는 파이프라인의 끝에 도달하면 해당 큐에 추가됩니다. 메시지가 파이프라인의 끝에 도달하지 못하면 격리에 배치되지 않습니다.

예를 들어, 콘텐츠 필터로 인해 메시지가 삭제되거나 반송되면 해당 메시지는 격리되지 않습니다.

원본 메시지 보관

바이러스가 포함되었다고(또는 그럴 가능성이 있다고) 시스템에서 식별한 메시지를 "avarchive" 디렉터리에 보관할 수 있습니다. 형식은 mbox 형식의 로그 파일입니다. 바이러스가 포함된 메시지 또는 완전히 검사되지 않았을 수 있는 메시지를 보관하려면 "Anti-Virus Archive" 로그 서브스크립션을 반드시 구성해야 합니다. 자세한 내용은 로깅, 1053 페이지을 참조해 주십시오.

참고 GUI에서 "Archive original message(원본 메시지 보관)" 설정을 표시하려면 "Advanced(고급)" 링크를 클릭해야 할 수 있습니다.

메시지 제목 헤더 수정

사용자들이 식별된 메시지를 좀 더 쉽게 식별 및 정렬할 수 있도록 특정 텍스트 문자열을 앞이나 뒤에 추가하여 식별된 메시지의 텍스트를 변경할 수 있습니다.

참고 "Modify message subject(메시지 제목 수정)" 필드에서는 공백이 무시되지 않습니다. 이 필드에 입력하는 텍스트의 뒤(뒤에 추가하는 경우) 또는 앞(앞에 추가하는 경우)에 공백을 추가하여 메시지의 원래 제목과 추가된 텍스트를 구분합니다. 예를 들어 앞에 추가하는 경우 `[WARNING: VIRUS REMOVED]` 텍스트를 몇몇 후행 공백과 함께 추가합니다.

기본 텍스트는 다음과 같습니다.

안티바이러스 제목 줄 수정을 위한 기본 제목 줄 텍스트

판정	제목에 추가할 기본 텍스트
Encrypted(암호화)	`[WARNING: MESSAGE ENCRYPTED]`

판정	제목에 추가할 기본 텍스트
Infected(감염됨)	`[WARNING: VIRUS DETECTED]`
Repaired(복구됨)	`[WARNING: VIRUS REMOVED]`
검색할 수 없음	`[WARNING: A/V UNSCANNABLE]`

다중 상태의 메시지는 어플라이언스가 메시지에 대해 어떤 작업을 수행했는지를 알려주는 다중 부분 알림 메시지가 될 수 있습니다(예: 사용자에게 메시지의 바이러스가 복구되었다는 알림이 제공되지만, 메시지의 또 다른 부분은 암호화됨).

알림 전송

메시지에 바이러스가 포함된 것으로 시스템에서 식별한 경우 발신자, 수신자 및/또는 추가 사용자에게 기본 알림을 전송할 수 있습니다. 알림을 전송할 추가 사용자를 지정하려면 쉼표로 여러 주소를 구분합니다(CLI와 GUI 모두). 기본 알림 메시지는 다음과 같습니다.

안티바이러스에 대한 기본 알림

판정	알림
Repaired(복구됨)	The following virus(es) was detected in a mail message: <virus name(s)>(메일 메시지에서 <virus name(s)> 바이러스가 탐지되었습니다.) Actions taken: Infected attachment dropped (or Infected attachment repaired)(수행 작업: 감염된 첨부 파일 삭제됨(또는 복구됨)).
Encrypted(암호화)	The following message could not be fully scanned by the anti-virus engine due to encryption(암호화 때문에 다음 메시지를 안티바이러스 엔진으로 충분히 검사하지 못했습니다).
Unscannable(검색할 수 없음)	The following message could not be fully scanned by the anti-virus engine(다음 메시지를 안티바이러스 엔진으로 충분히 검사하지 못했습니다).
Infectious(전염성)	The following unrepairable virus(es) was detected in a mail message: <virus name(s)>(메일 메시지에서 <virus name(s)>라는 복구 불가 바이러스가 탐지되었습니다).

메시지에 사용자 지정 헤더 추가

안티바이러스 검사 엔진으로 검사한 모든 메시지에 사용자 지정 헤더가 추가되도록 정의할 수 있습니다. **Yes(예)**를 클릭하고 헤더 이름과 텍스트를 정의합니다.

특정 메시지가 바이러스 검사를 우회할 수 있도록 `skip-viruscheck` 작업을 사용하는 필터를 만들 수도 있습니다. 안티바이러스 시스템 우회 작업, 224 페이지를 참조하십시오.

메시지 수신자 수정

메시지가 다른 주소로 전달되도록 메시지 수신자를 수정할 수 있습니다. **Yes(예)**를 클릭하고 새 수신자 주소를 입력합니다.

대체 대상 호스트로 메시지 전송

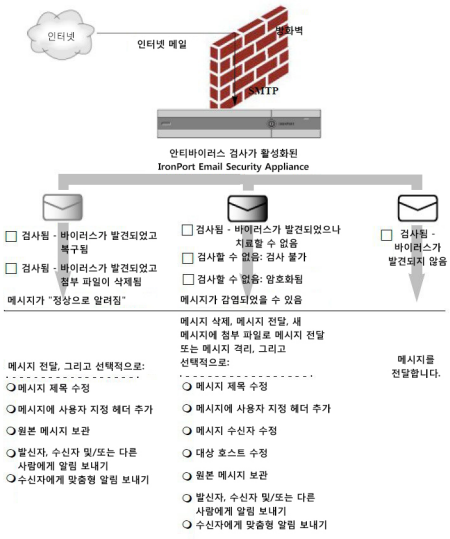
암호화된 메시지, 검사 불가 메시지 또는 바이러스 감염 메시지에 대해 서로 다른 수신자 또는 대상 호스트로 알림을 전송할 수 있습니다. **Yes(예)**를 클릭하고 대체 주소 또는 호스트를 입력합니다.

예를 들어, 추가 검사를 위해 의심스런 메시지를 관리자의 사서함이나 특수 메일 서버로 라우팅할 수 있습니다. 다중 수신자 메시지의 경우 단일 사본만 대체 수신자에게 전송됩니다.

맞춤형 알림 전송

발신자, 수신자 및/또는 기타 사용자(이메일 주소)로 맞춤형 알림을 전송할 수 있습니다. 그렇게 하려면 설정을 구성하기 전에 먼저 사용자 지정 알림을 만들어야 합니다. 자세한 내용은 텍스트 리소스 이해, 621 페이지를 참조하십시오.

그림 ***18:*** 바이러스를 검사한 메시지를 처리하기 위한 옵션



참고 기본적으로 안티바이러스 검사는 공개 리스너용 $TRUSTED 메일 플로우 정책에서 활성화되며, 이는 WHITELIST 발신자 그룹에서 참조됩니다. 메일 플로우 정책을 사용하여 이메일 발신자에 대한 액세스 규칙 정의, 101 페이지를 참조하십시오.

발신자 및 수신자의 서로 다른 그룹에 대해 안티바이러스 정책 구성

메일 정책에 대한 사용자별 안티바이러스 설정을 수정하기 위한 프로세스는 기본적으로 수신 또는 발신 메일에 대해 동일합니다.

기본 정책이 아닌 개별 정책에는 "Use Default(기본값 사용)" 설정에 대한 추가 필드가 있습니다. 기본 메일 정책 설정을 상속하려면 이 설정을 선택합니다.

수신 또는 발신 메일 정책을 사용하여 수신자 단위로 안티바이러스 작업을 활성화합니다. GUI 또는 CLI에서 policyconfig > antivirus 명령을 사용하여 메일 정책을 구성할 수 있습니다. 안티바이러스 설

정을 전역적으로 활성화한 후에는 자신이 만드는 각 메일 정책에 대해 이러한 작업을 별도로 구성합니다. 각 메일 정책에 대해 서로 다른 작업을 구성할 수 있습니다.

단계 **1** Mail Policies > Incoming Mail Policies(메일 정책 > 수신 메일 정책) 또는 Mail Policies > Outgoing Mail Policies(메일 정책 > 발신 메일 정책) 페이지로 이동합니다.

단계 **2** 구성하려는 정책의 안티바이러스 보안 서비스에 대한 링크를 클릭합니다.

참고 기본 정책의 설정을 수정하려면 기본 행의 링크를 클릭합니다.

단계 **3** **Yes(**예**)** 또는 **Use Default(**기본값 사용**)**를 클릭하여 정책에 대한 안티바이러스 검사를 활성화합니다.

페이지의 첫 번째 설정은 정책에 대해 서비스를 활성화할지 여부를 정의합니다. 서비스를 완전히 비활성화하려면 **Disable(**비활성**)**을 클릭할 수 있습니다.

기본 정책 이외의 메일 정책에서 "Yes(예)"를 선택하면 Repaired(복구됨), Encrypted(암호화됨), Unscannable(검사 불가) 및 Virus Infected(바이러스 감염) 메시지의 필드가 활성화됩니다.

단계 **4** 안티바이러스 검사 엔진을 선택합니다. McAfee 또는 Sophos 엔진을 선택할 수 있습니다.

단계 **5** Message Scanning(메시지 검사) 설정을 구성합니다.

자세한 내용은 메시지 검사 설정, 342 페이지를 참조하십시오.

단계 **6** Repaired(복구됨), Encrypted(암호화됨), Unscannable(검사 불가) 및 Virus Infected(바이러스 감염) 메시지의 설정을 구성합니다.

메시지 처리 설정, 343 페이지 및 메시지 처리 작업에 대한 설정 구성, 344 페이지 항목을 참조하십시오.

단계 **7** **Submit(**제출**)**를 클릭합니다.

단계 **8** 변경사항을 커밋합니다.

안티바이러스 구성에 대한 참고 사항

drop attachments 플래그는 안티바이러스 검사의 작동 방식에 상당한 차이를 가져옵니다. "Drop infected attachments if a virus is found and it could not be repaired(바이러스가 발견되고 복구할 수 없는 경우 감염된 첨부 파일 삭제)"로 시스템이 구성된 경우, 바이러스가 있거나 검사 불가한 MIME 부분이 메시지에서 제거됩니다. 그러면 안티바이러스 검사의 출력은 거의 항상 clean(깨끗한) 메시지입니다. 검사 불가 메시지에 대해 정의된 작업(GUI 창에 표시됨)은 거의 발생하지 않습니다.

"Scan for Viruses only(바이러스 검사만 수행)"에서 이러한 작업은 불량 메시지 부분을 삭제하여 메시지를 "clean(치료)"합니다. RFC822 헤더 자체가 공격을 받거나 다른 문제가 있는 경우에만 검사 불가 작업이 발생하게 됩니다. 그러나 안티바이러스 검사가 "Scan for Viruses only(바이러스 검사만 수행)"로 구성되어 있고 "Drop infected attachments if a virus is found and it could not be repaired(바이러스가 발견되고 복구할 수 없는 경우 감염된 첨부 파일 삭제)"가 선택되지 않은 경우 검사할 수 없는 작업이 거의 발생하지 않습니다.

다음 표에는 몇몇 일반적인 안티바이러스 구성 옵션이 나열되어 있습니다.

일반적인 안티바이러스 구성 옵션

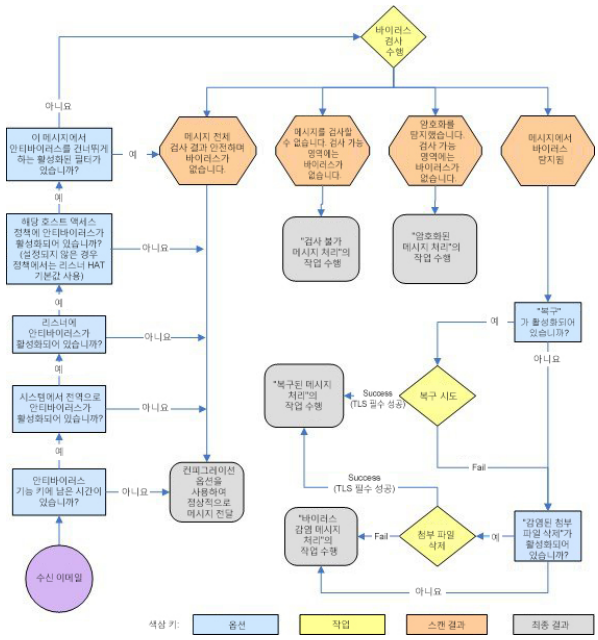
상태	안티바이러스 구성
바이러스가 널리 침투함 바이러스 메시지가 다른 처리 없이 시스템에서 단순히 삭제됩니다.	**Drop-attachments(**첨부 파일 삭제**):** NO(아니요) **Scanning(**검사**):** Scan-Only(검사만) **Cleaned messages(**치료된 메시지**)**: Deliver(전달) **Unscannable messages(**검사 불가 메시지**)**: DROP message(메시지 삭제) Encrypted messages(암호화된 메시지): Send to administrator or quarantine for review(검토를 위해 관리자에게 또는 격리로 전송) Viral messages(바이러스 메시지): Drop message(메시지 삭제)
자유로운 정책 가능한 한 많은 문서가 전송됩니다.	**Drop-attachments(**첨부 파일 삭제**):** YES(예) **Scanning(**검사**):** Scan and Repair(검사 후 복구) **Cleaned messages(**치료된 메시지**):** [VIRUS REMOVED] and Deliver([바이러스 제거] 후 전달) **Unscannable messages(**검사 불가 메시지**)**: Forward as attachment(첨부 파일로 전달) Encrypted messages(암호화된 메시지): Mark and forward(표시 후 전달) Viral messages(바이러스 메시지): Quarantine or mark and forward(격리 또는 표시 후 전달)
좀 더 신중한 정책	**Drop-attachments(**첨부 파일 삭제**)**: YES(예) **Scanning(**검사**):** Scan and Repair(검사 후 복구) **Cleaned messages(**치료된 메시지**):** [VIRUS REMOVED] and Deliver([바이러스 제거] 후 전달) (좀 더 신중한 정책의 경우 치료된 메시지 보관) **Unscannable messages(**검사 불가 메시지**)**: Send notification(s), quarantine, OR drop and archive(알림 전송, 격리 또는 삭제 후 보관) Encrypted messages(암호화된 메시지): Mark and forward OR treat as unscannable(표시 후 전달 또는 검사 불가로 처리) Viral messages(바이러스 메시지): Archive and drop(보관 및 삭제)

상태	안티바이러스 구성
신중하게 검토 관리자가 내용을 검토할 수 있도록 바이러스 가능성이 있는 메시지를 격리 사서함으로 전송합니다.	**Drop-attachments(**첨부 파일 삭제**):** NO(아니요) **Scanning(**검사**):** Scan-Only(검사만) **Cleaned messages(**치료된 메시지**):** Deliver(전송)(이 작업은 일반적으로 수행되지 않음) **Unscannable messages(**검사 불가 메시지**)**: Forward as attachment(첨부 파일로 전달), alt-src-host 또는 alt-rcpt-to 작업 Encrypted messages(암호화된 메시지): Treat as unscannable(검사 불가로 처리) Viral messages(바이러스 메시지): Forward to quarantine or administrator(격리로 또는 관리자에게 전달)

안티바이러스 작업의 흐름도

다음 그림에서는 안티바이러스 작업 및 옵션이 어플라이언스에서 처리되는 메시지에 어떤 영향을 미치는지 설명합니다.

그림 ***19:*** 안티바이러스 작업의 흐름도



참고 다중 레이어 안티바이러스 검사를 구성하면 Cisco 어플라이언스는 McAfee 엔진, Sophos 엔진 순서로 바이러스 검사를 수행합니다. McAfee 엔진이 바이러스를 탐지하지 않는 한 두 엔진을 사용하여 메시지를 검사합니다. McAfee 엔진이 바이러스를 탐지하면 Cisco 어플라이언스는 메일 정책에 대해 정의된 안티바이러스 작업(복구, 격리 등)을 수행합니다.

안티바이러스 검사 테스트를 위해 이메일을 어플라이언스로 전송

단계 **1** 메일 정책에 대해 바이러스 검사를 활성화합니다.

Security Services(보안 서비스**) > Sophos/McAfee Anti-virus** 페이지 또는 `antivirusconfig` 명령을 사용하여 전역 설정을 구성하고, Email Security Manager(이메일 보안 관리자) 페이지(GUI) 또는 `policyconfig`의 `antivirus` 하위 명령을 사용하여 특정 메일 정책의 설정을 구성합니다.

단계 **2** 표준 텍스트 편집기를 열고, 다음 문자 문자열을 공백이나 줄 바꿈 없이 한 줄에 입력합니다.

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

참고 위의 줄은 텍스트 편집기 창에 한 줄로 나타나야 합니다. 따라서 텍스트 편집기 창을 최대화하고 줄 바꿈을 삭제하십시오. 또한 테스트 메시지가 시작되는 "X5O..."에서 숫자 영(0)이 아니라 문자 O를 입력해야 합니다.

컴퓨터에서 이 설명서를 읽고 있다면 PDF나 HTML 파일에서 직접 줄을 복사하여 텍스트 편집기에 붙여넣을 수 있습니다. 줄을 복사할 때 별도의 캐리지 리턴이나 공백을 삭제하십시오.

단계 **3** 파일을 **`EICAR.COM`**이라는 이름으로 저장합니다.

파일 크기는 68 또는 70바이트입니다.

참고 이 파일은 바이러스가 아닙니다. 확산되거나, 다른 파일을 감염시키거나, 컴퓨터에 해를 입히지 않습니다. 그러나 다른 사용자에게 경보가 표시되지 않게 하려면 스캐너 테스트를 완료한 후 파일을 삭제해야 합니다.

단계 **4** `EICAR.COM` 파일을 이메일 메시지에 첨부하고, 1단계에서 구성한 메일 정책의 일치 여부를 확인할 리스너로 전송합니다.

테스트 메시지에 지정한 수신자가 리스너에서 허용되는지 확인합니다. (자세한 내용은 메시지를 수락할 도메인 및 사용자 추가, 131 페이지 섹션을 참조하십시오.)

Cisco 외의 게이트웨이(예: Microsoft Exchange 서버)에 발신 메일에 대한 바이러스 검사 소프트웨어가 설치된 경우, 파일을 이메일로 보내기가 어려울 수 있습니다.

참고 테스트 파일은 항상 복구 불가로 검사됩니다.

단계 **5** 리스너에서 바이러스 검사를 위해 구성한 작업을 평가하고, 이러한 작업이 활성화되었고 예상대로 작동하는지 확인합니다.

이는 다음 작업 중 하나를 통해 가장 쉽게 수행할 수 있습니다.

1. 바이러스 검사 설정을 Scan and Repair(검사 후 복구) 또는 Scan only(검사만) 모드로 구성합니다(첨부 파일을 삭제하지 않음).
   - Eicar 테스트 파일을 첨부하여 이메일을 전송합니다. 수행되는 작업이 바이러스 감염 메시지 처리(바이러스 감염 메시지 처리, 344 페이지의 설정)의 컨피그레이션과 일치하는지 확인합니다.
2. 바이러스 검사 설정을 Scan and Repair(검사 후 복구) 또는 Scan only(검사만) 모드로 구성합니다(첨부 파일을 삭제함).
   - Eicar 테스트 파일을 첨부하여 이메일을 전송합니다.
   - 수행되는 작업이 복구된 메시지 처리(복구된 메시지 처리, 343 페이지의 설정)의 컨피그레이션과 일치하는지 확인합니다.

안티바이러스 검사 테스트용 바이러스 파일을 얻는 방법에 대한 자세한 내용은 http://www.eicar.org/anti_virus_test_file.htm을 참고하십시오.

이 페이지에서는 다운로드용 파일 4개를 제공합니다. 클라이언트 측 바이러스 검사 소프트웨어가 설치되어 있는 경우 이러한 파일을 다운로드하여 압축 해제하는 것이 어려울 수 있습니다.

바이러스 정의 업데이트

관련 주제

- HTTP를 통한 안티바이러스 업데이트 검색 정보 , 352 페이지
- 업데이트 서버 설정 구성 , 353 페이지
- 안티바이러스 업데이트 모니터링 및 수동 확인, 353 페이지
- 어플라이언스에서 안티바이러스 파일이 업데이트되었는지 확인, 353 페이지

HTTP를 통한 안티바이러스 업데이트 검색 정보

Sophos 및 McAfee는 바이러스 정의를 새로 식별된 바이러스로 자주 업데이트합니다. 이러한 업데이트를 어플라이언스로 전달해야 합니다.

기본적으로 Cisco 어플라이언스는 5분마다 업데이트를 확인하도록 구성되어 있습니다. Sophos 및 McAfee 안티바이러스 엔진의 경우 동적인 웹사이트에서 서버 업데이트가 수행됩니다.

업데이트가 어플라이언스로 능동적으로 다운로드되는 한 시스템에서 업데이트에 대한 시간 초과가 발생하지 않습니다. 업데이트 다운로드가 오랫동안 중단되면 다운로드 시간 초과가 발생합니다.

시간 초과가 발생하기까지 시스템이 업데이트를 대기하는 최대 기간은 안티바이러스 업데이트 간격에서 1분을 뺀 값으로 정의되는 동적인 값입니다(Security Services > Service Updates(보안 업데이트 > 서비스 업데이트)에서 정의됨). 완료하는 데 10분 넘게 걸릴 수 있는 큰 업데이트를 다운로드하므로 이 컨피그레이션 값은 연결 속도가 느린 어플라이언스에 도움이 됩니다.

업데이트 서버 설정 구성

Security Services > Service Updates(보안 서비스 > 서비스 업데이트) 페이지를 통해 바이러스 업데이트 설정을 구성할 수 있습니다. 예를 들어, 시스템에서 안티바이러스 업데이트를 받는 방법 및 업데이트 확인 빈도를 구성할 수 있습니다. 추가 설정에 대한 자세한 내용은 서비스 업데이트 , 945 페이지를 참조하십시오.

안티바이러스 업데이트 모니터링 및 수동 확인

Security Services(보안 서비스) > Sophos 또는 **McAfee** 페이지를 사용하거나 `antivirusstatus` CLI 명령을 사용하여 어플라이언스에 최신 안티바이러스 엔진이 있는지, 파일이 설치되었는지, 마지막 업데이트가 수행되었는지를 확인할 수 있습니다.

업데이트를 수동으로 수행할 수도 있습니다. 안티바이러스 엔진 수동 업데이트 , 353 페이지를 참조하십시오.

안티바이러스 엔진 수동 업데이트

단계 **1** Security Services(보안 서비스) > Sophos 또는 McAfee Anti-Virus 페이지로 이동합니다.

단계 **2** Current McAfee/Sophos Anti-Virus Files(현재 McAfee/Sophos 안티바이러스 파일) 테이블에서 **Update Now(**지금 업데이트**)**를 클릭합니다.

어플라이언스가 최신 업데이트를 확인하고 다운로드합니다.

다음에 수행할 작업

CLI에서 antivirusstatus 및 antivirusupdate 명령을 사용하여 이를 구성할 수도 있습니다.

어플라이언스에서 안티바이러스 파일이 업데이트되었는지 확인

안티바이러스 파일이 성공적으로 다운로드, 추출 또는 업데이트되었는지를 확인하려면 Updater Logs(업데이터 로그)를 볼 수 있습니다. tail 명령을 통해 업데이터 로그 서브스크립션에서 최종 항목을 표시하여 바이러스 업데이트가 제대로 있는지 확인합니다.

15 장

Anti-Spam

이 장에는 다음 섹션이 포함되어 있습니다.

안티스팸 검사 개요

안티스팸 프로세스에서는 사용자가 구성하는 메일 정책을 바탕으로 수신(및 발송) 메일과 관련된 이메일을 검사합니다.

- 하나 이상의 검사 엔진이 필터링 모듈을 통해 메시지를 검사합니다.
- 검사 엔진은 각 메시지에 점수를 할당합니다. 점수가 높을수록 메시지가 스팸일 가능성이 큽니다.
- 각 메시지는 점수를 기준으로 다음 중 하나로 분류됩니다.
  - Not spam(스팸 아님)
  - Suspected spam(의심스런 스팸)
  - Positively-identified spam(양성으로 식별된 스팸)
- 결과에 따라 작업이 수행됩니다.

양성으로 식별된 스팸 메시지, 스팸으로 의심되는 메시지 또는 원치 않는 마케팅 메시지로 식별된 메시지에 대해 수행하는 작업은 상호 배타적이지 않습니다. 사용자 그룹에 대한 서로 다른 처리 요구에 따라 서로 다른 수신 또는 발신 정책 내에서 각기 다르게 일부 또는 전체를 결합할 수 있습니다. 또한

동일한 정책에서 양성으로 식별된 스팸을 의심스런 스팸과 다르게 취급할 수도 있습니다. 예를 들어, 양성으로 식별된 스팸 메시지는 삭제하되 의심스런 스팸 메시지는 격리할 수 있습니다.

메일 정책마다 일부 범주에 임계값을 지정하고 범주별로 수행할 작업을 결정할 수 있습니다. 또한, 사용자마다 다른 메일 정책에 할당하고, 정책마다 검사 엔진, 스팸 정의 임계값 및 스팸 처리 작업을 다르게 정의할 수 있습니다.

참고 안티스팸 검사가 적용되는 방식과 시기에 대한 자세한 내용은 이메일 파이프라인 및 보안 서비스, 63 페이지 항목을 참고하십시오.

관련 주제

- 안티 스팸 솔루션 , 356 페이지

안티 스팸 솔루션

Cisco 어플라이언스는 다음의 안티 스팸 솔루션을 제공합니다.

- IronPort Anti-Spam 필터링, 358 페이지.
- Cisco Intelligent Multi-Scan 필터링, 360 페이지.

Cisco 어플라이언스에서 이러한 솔루션 모두에 라이선스를 부여하고 활성화할 수 있으며, 한 솔루션만 특정 메일 정책에서 사용할 수 있습니다. 사용자 그룹마다 다른 안티스팸 솔루션을 지정할 수 있습니다.

메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법

프로시저

	명령 또는 동작	목적
단계 **1**	Email Security Appliance에서 안티스팸 검사를 활성화합니다.	참고 이 표의 나머지 단계는 두 가지 검사 엔진 옵션에 적용됩니다. Cisco IronPort Anti-Spam과 Intelligent Multi-Scan의 기능 키가 모두 있는 경우 어플라이언스에서 두 솔루션을 모두 활성화할 수 있습니다. • IronPort Anti-Spam 필터링, 358 페이지 • Cisco Intelligent Multi-Scan 필터링, 360 페이지

	명령 또는 동작	목적
단계 **2**	로컬 Email Security Appliance에서 스팸을 격리하거나 Security Management Appliance에서 외부 격리를 사용하도록 구성합니다.	• 로컬 스팸 격리 설정, 868 페이지 • 외부 스팸 격리 작업 , 1188 페이지
단계 **3**	스팸 검사 대상 메시지를 소유하는 사용자 그룹을 정의합니다.	발신자 및 수신자 그룹에 대한 메일 정책 만들기, 276 페이지
단계 **4**	정의한 사용자 그룹의 안티스팸 검사 규칙을 구성합니다.	안티스팸 정책 정의 , 362 페이지
단계 **5**	특정 메시지에서 Cisco Anti-Spam 검사를 건너뛰려면 skip-spamcheck 작업을 사용하는 메시지 필터를 생성합니다.	안티스팸 시스템 우회 작업, 223 페이지
단계 **6**	(권장) SenderBase Reputation 점수를 기준으로 연결을 거부하고 있지 않더라도 각 인바운드 메일 흐름 정책에 대한 SenderBase Reputation Service 점수 매기기를 활성화합니다.	각 인바운드 메일 흐름 정책에 대해 "Use SenderBase for Flow Control(흐름 정책에 Senderbase 사용)"이 설정되어 있는지 확인합니다. 메일 플로우 정책을 사용하여 수신 메시지에 대한 규칙 정의, 108 페이지를 참조하십시오.
단계 **7**	Email Security Appliance가 수신 메일을 받기 위해 외부 발신자에 직접 연결되지 않고, 대신 메일 교환기, 메일 전송 에이전트 또는 네트워크의 다른 머신을 통해 릴레이되는 메시지를 받는 경우 릴레이되는 수신 메시지에 원래 발신자 IP 주소가 포함되는지 확인합니다.	수신 릴레이 사용 배포 환경에서 발신자 IP 주소 확인 , 374 페이지
단계 **8**	경고 및 어플라이언스에서 생성된 기타 메시지가 스팸으로 잘못 확인되지 않도록 방지합니다.	스팸 필터로부터 어플라이언스에서 생성된 메시지 보호, 369 페이지
단계 **9**	(선택 사항) 메시지의 악성 URL에 대한 보호가 강화되도록 URL 필터링을 활성화합니다.	URL 필터링 활성화, 427 페이지
단계 **10**	구성을 테스트합니다.	안티스팸 테스트, 384 페이지
단계 **11**	(선택 사항) 서비스 업데이트를 위한 설정(안티스팸 규칙 포함)을 구성합니다.	두 안티 스팸 솔루션에 대한 검사 규칙은 모두 기본적으로 Cisco 업데이트 서버에서 검색됩니다. • 서비스 업데이트 , 945 페이지 • 프록시 서버를 통한 업데이트, 949 페이지 • 업그레이드 및 업데이트 다운로드를 위한 서버 설정 구성 , 949 페이지

IronPort Anti-Spam 필터링

관련 주제

- 평가 키, 358 페이지
- Cisco Anti-Spam: 개요 , 358 페이지
- IronPort Anti-Spam 검사 구성, 359 페이지

평가 키

Cisco 어플라이언스는 Cisco Anti-Spam 소프트웨어에 대한 30일 평가 키와 함께 제공됩니다. 이 키는 시스템 설치 마법사 또는 Security Services(보안 서비스) > IronPort Anti-Spam 페이지(GUI), 아니면 systemsetup 또는 antispamconfig 명령(CLI)으로 라이선스 계약에 동의하기 전까지는 활성화되지 않습니다. 계약에 동의하면 기본적으로 기본 수신 메일 정책에 대해 Cisco Anti-Spam이 활성화됩니다. Cisco Anti-Spam 라이선스가 30일 이내에 만료됨을 알리는 경고가 구성한 관리자 주소(시스템 설치 마법사, 2단계: 시스템, 31 페이지 참조)로 전송됩니다. 만료 30, 15, 5, 및 0일 전에 경고문이 전송됩니다. 30일 평가 기간 이후에 기능을 활성화하는 방법에 대한 자세한 내용은 Cisco 세일즈 담당자에게 문의하십시오. System Administration(시스템 관리) > Feature Keys(기능 키) 페이지에서 또는 featurekey 명령을 실행하여 남은 평가 기간을 확인할 수 있습니다. (자세한 내용은 기능 키, 926 페이지를 참조하십시오.)

Cisco Anti-Spam: 개요

IronPort Anti-Spam은 스팸, 피싱 및 좀비 공격을 비롯한 전 범위의 알려진 위협과 함께 탐지하기 어려운 소규모의 짧은 이메일 위협(예: "419" 스캠)을 처리합니다. 또한 IronPort Anti-Spam은 다운로드 URL 또는 실행 파일을 통해 악의적인 콘텐츠를 유포하는 새롭고 진화된 복합적 위협 요소(예: 스팸 공격)를 식별합니다.

이러한 위협 요소를 식별하기 위해 IronPort Anti-Spam은 메시지의 전체 컨텍스트 즉, 메시지 콘텐츠, 메시지 구성 방식, 발신자 신뢰도, 메시지에서 알려진 웹 사이트의 신뢰도 등을 검사합니다. 이메일과 웹 신뢰도 데이터의 강점이 결합된 IronPort Anti-Spam은 세계 최대의 이메일 및 웹 트래픽 모니터링 네트워크(SenderBase)를 활용하여 새로운 공격이 시작되는 즉시 이를 탐지합니다.

IronPort Anti-Spam은 다음 차원에 대해 100,000가지 이상의 메시지 특성을 분석합니다.

- 이메일 신뢰도 - 이 메시지를 보내는 사람은 누구입니까?
- 메시지 내용 - 메시지에 무슨 내용이 포함되었나?
- 메시지 구조 - 이 메시지가 어떻게 구성되었나?
- 웹 평판 - 어디서 실천 방안을 알려주나?

다차원 관계 분석을 통해 시스템은 정확도를 유지하면서 폭넓은 위협을 포착할 수 있습니다. 예를 들어 해당 콘텐츠가 정상적 금융 기관에서 보낸 것으로 표기되어 있지만, 소비자 광대역 네트워크의 IP 주소에서 전송되었거나 "좀비" PC에서 호스팅되는 URL이 포함된 메시지는 의심스러운 것으로 표시됩니다. 반대로, 만족스러운 신뢰도를 가진 제약 회사에서 보낸 메시지는, 메시지에 스팸과 밀접하게 상관된 단어가 포함되어 있더라도 스팸으로 태그 지정되지 않습니다.

관련 주제

- 해외 지역에 대한 스팸 검사 , 359 페이지
- URL 관련 보호 및 제어 , 425 페이지

해외 지역에 대한 스팸 검사

전 세계적으로 효과적으로 작용하는 Cisco Anti-Spam은 로캘별 콘텐츠 인식 위협 탐지 기술을 사용합니다. 또한, 국가별 규칙 프로필을 사용하여 특정 지역에 맞게 안티스팸 검사를 최적화할 수 있습니다.

- 미국 이외의 특정 지역에서 대량의 스팸을 수신한 경우 국가별 규칙 프로필을 사용하여 해당 지역에서 오는 스팸을 차단할 수 있습니다.

  예를 들어 중국과 대만에서부터 중국어 번체 및 간체로 이루어진 많은 양의 스팸을 수신하는 경우가 있습니다. 중국 국가별 규칙은 이러한 종류의 스팸에 맞게 최적화되어 있습니다. 주로 중국 본토, 대만 및 홍콩으로부터 메일을 받는 경우 안티스팸 엔진에 포함된 중국 국가별 규칙 프로필을 사용하는 것이 가장 좋습니다.

- 스팸이 주로 미국이나 특정 지역 외의 지역에서 오는 경우에는 국가별 규칙을 활성화하지 마십시오. 해당 기능을 활성화하는 경우 다른 스팸 유형의 캡처 속도가 줄어들 수 있습니다. 그 이유는 국가별 규칙 프로필은 특정 지역의 안티스팸 엔진을 최적화하기 때문입니다.

IronPort Anti-Spam 검사를 구성할 때 국가별 규칙 프로필을 활성화할 수 있습니다.

관련 주제

- IronPort Anti-Spam 검사 구성, 359 페이지

IronPort Anti-Spam 검사 구성

참고 IronPort Anti-Spam이 시스템 설치 중에 활성화된 경우 기본 수신 메일 정책에 대해 활성화되고 전역 설정에 대한 기본값이 사용됩니다.

시작하기 전에

- 국가별 검사를 사용할지 여부를 결정합니다. 해외 지역에 대한 스팸 검사 , 359 페이지를 참조하십시오.

단계 **1** **Security Services(**보안 서비스**) > IronPort Anti-Spam**을 선택합니다.

단계 **2** 시스템 설치 마법사에서 IronPort Anti-Spam을 활성화하지 않은 경우 다음을 수행합니다.

a) **Enable(**활성화**)**을 클릭합니다.

b) 라이센스 계약 페이지의 하단으로 스크롤하고 **Accept(**동의**)**를 클릭하여 계약에 동의합니다.

단계 **3** **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **4** **Enable IronPort Anti-Spam Scanning(IronPort Anti-Spam Scanning** 활성화**)**의 확인란을 선택합니다.

이 확인란을 선택하면 어플라이언스에 대해 전역으로 기능이 활성화됩니다.

단계 **5** 스패머가 발송한 대용량 메시지를 검사하는 동시에 어플라이언 처리량을 최적화하려면 Cisco Anti-Spam의 메시지 검사에 대한 임계값을 구성합니다.

옵션	설명
메시지 검사 임계값	**1.** 다음보다 작은 메시지는 항상 검사에 대한 값 입력 - 권장 값은 1MB 이하입니다. 항상 검사 크기보다 작은 메시지는 "조기 종료"를 제외하고 전체적으로 검사됩니다. 이 크기보다 큰 메시지는 검사 안 함 크기보다 작은 경우 부분적으로 검사됩니다. 항상 검사 메시지 크기는 3MB를 초과하지 않는 것이 좋습니다. 값이 클수록 성능이 저하될 수 있습니다. **2.** 다음보다 큰 메시지는 검사하지 않음에 대한 값 입력 - 권장 값은 2MB 이하입니다. 해당 크기보다 큰 메시지는 Cisco Anti-Spam에서 검사되지 않으며 X-IronPort-Anti-Spam-Filtered: true 헤더가 메시지에 추가되지 않습니다. 검사 안 함 메시지 크기는 10MB를 초과하지 않는 것이 좋습니다. 값이 클수록 성능이 저하될 수 있습니다. *always scan(*항상 검사*)* 크기보다 크거나 *never scan(*검사 안 함*)* 크기보다 작은 메시지에 대해서는 제한적이고 더 빠른 검사가 수행됩니다. 참고 Outbreak Filter 최대 메시지 크기가 Cisco Anti-Spam의 항상 검사 메시지보다 클 경우 Outbreak Filter 최대 크기보다 작은 메시지는 전체적으로 검사됩니다.
단일 메시지 검사 시간제한	메시지를 검사할 때 시간 초과 대기 시간(초)을 입력합니다. 1~120의 정수를 입력합니다. 기본값은 60초입니다.
국가별 검사	국가별 검사를 활성화 또는 비활성화하고, 해당하는 경우 사용 지역을 선택합니다. 이 기능은 지정된 지역에서 대량의 이메일을 받는 경우에만 활성화합니다. 이 기능은 특정 지역에 맞게 안티스팸 엔진을 최적화하므로 다른 스팸 유형의 캡처 속도가 줄어들 수 있습니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

Cisco Intelligent Multi-Scan 필터링

Cisco Intelligent Multi-Scan은 Cisco Anti-Spam을 비롯한 여러 안티 스팸 검사 엔진을 통합하여 다중 계층 안티 스팸 솔루션을 제공합니다.

Cisco Intelligent Multi-Scan으로 처리되는 경우:

- 메시지는 먼저 타사 안티스팸 엔진으로 검사됩니다.
- 그런 다음 Cisco Intelligent Multi-Scan은 메시지 및 타사 엔진의 판정을 최종 판정이 이루어지는 Cisco Anti-Spam으로 전달합니다.
- Cisco Anti-Spam이 검사를 수행하고 난 후 합산된 다중 검사 점수를 AsyncOS로 반환합니다.
- 타사 검사 엔진과 Cisco Anti-Spam의 이점이 결합하여 스팸 탐지율을 높이는 동시에 Cisco Anti-Spam의 긍정 오류 비율을 낮출 수 있습니다.

Cisco Intelligent Multi-Scan에 사용되는 검사 엔진의 순서는 구성할 수 없습니다. Cisco Anti-Spam은 항상 마지막으로 메시지를 검사하며, 타사 엔진이 메시지가 스팸이라고 판정하면 Cisco Intelligent Multi-Scan은 해당 메시지 검사를 건너뛰지 않습니다.

Cisco Intelligent Multi-Scan을 사용하면 시스템 처리량이 감소할 수 있습니다. 자세한 내용은 Cisco 지원 담당자에게 문의하십시오.

참고 또한, Intelligent Multi-Scan 기능 키는 어플라이언스의 Cisco Anti-Spam을 활성화하므로 메일 정책에 따라 Cisco Intelligent MultiScan 또는 Cisco Anti-Spam을 활성화할 수 있습니다.

관련 주제

- Cisco Intelligent Multi-Scan 구성 , 361 페이지

Cisco Intelligent Multi-Scan 구성

참고 Cisco Intelligent Multi-Scan이 시스템 설치 중에 활성화된 경우 기본 수신 메일 정책에 대해 활성화되고 전역 설정에 대한 기본값이 사용됩니다.

시작하기 전에

이 기능을 위한 기능 키를 활성화합니다. 기능 키, 926 페이지를 참조하십시오. 기능 키를 활성화한 경우에만 IronPort Intelligent Multi-Scan 옵션이 표시됩니다.

단계 **1** **Security Services(보안 서비스) > IronPort Intelligent Multi-Scan**을 선택합니다.

단계 **2** 시스템 설치 마법사에서 Cisco Intelligent Multi-Scan을 활성화하지 않은 경우 다음을 수행합니다.

a) **Enable(활성화)**을 클릭합니다.

b) 라이센스 계약 페이지의 하단으로 스크롤하고 **Accept(동의)**를 클릭하여 계약에 동의합니다.

단계 **3** **Edit Global Settings(전역 설정 수정)**를 클릭합니다.

단계 **4** **Enable IronPort Intelligent Multi-Scan(IronPort Intelligent Multi-Scan 활성화)**의 확인란을 선택합니다.

이 확인란을 선택하면 어플라이언스에 대해 전역으로 기능이 활성화됩니다. 그러나 나중에 Mail Policies(메일 정책)에서 수신자별 설정을 활성화해야 합니다.

단계 **5** Cisco Intelligent Multi-Scan의 검사 임계값을 선택합니다.

기본값은 다음과 같습니다.

- 512K 이하 항상 검사
- 1M 이상 검사 안 함

단계 **6** 메시지를 검사할 때 시간 초과 대기 시간(초)을 입력합니다.

초를 지정할 때 1~120까지의 정수를 입력합니다. 기본값은 60초입니다.

대부분의 사용자는 검사할 최대 메시지 크기 또는 시간제한 값을 변경할 필요가 없습니다. 즉, 최대 메시지 크기를 낮게 설정하여 어플라이언스 처리량을 최적화할 수 있습니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

안티스팸 정책 정의

메일 정책마다 스팸으로 간주할 메시지와 그러한 메시지에 수행할 작업을 결정하는 설정을 구성합니다. 정책이 적용되는 메시지를 검사할 엔진도 지정합니다.

기본 수신 메일 정책과 발송 메일 정책에 각기 다른 설정을 구성할 수 있습니다. 사용자마다 서로 다른 안티스팸 정책이 필요한 경우 안티스팸 설정을 다르게 한 여러 메일 정책을 사용합니다. 정책별로 하나의 안티스팸 솔루션만 활성화할 수 있으며 동일한 정책에 대해 두 가지 솔루션을 모두 활성화할 수는 없습니다.

시작하기 전에

- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 356 페이지의 표에 있는 이 지점까지 모든 단계를 완료합니다.
- 다음 사항을 숙지합니다.
  - 스팸 판정 임계값 및 의심스러운 스팸 임계값 이해, 365 페이지
  - 구성 예: 양성으로 식별된 스팸 대 의심스런 스팸에 대한 작업 , 365 페이지
  - 합법적인 소스에서 오는 원치 않는 마케팅 메시지, 366 페이지
  - 여러 안티스팸 솔루션을 활성화한 경우, 여러 메일 정책에서 서로 다른 안티스팸 검사 엔진 사용: 구성 예 , 367 페이지 항목을 참조하십시오.
  - 안티스팸 검사 중에 추가되는 헤더 , 369 페이지
- 스팸을 "안티스팸 보관소" 로그에 보관하는 경우, 로깅, 1053 페이지 항목을 참조하십시오.
- 메시지를 대체 메일 호스트로 보내는 경우, 전달 호스트 변경 작업, 217 페이지 항목을 참조하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)** 페이지로 이동합니다.

또는

단계 **2** **Mail Policies > Outgoing Mail Policies(**메일 정책 > 발신 메일 정책**)** 페이지로 이동합니다.

단계 **3** 임의의 메일 정책에서 **Anti-Spam(**안티스팸**)** 열 아래의 링크를 클릭합니다.

단계 **4** **Enable Anti-Spam Scanning for This Policy(**이 정책에 대해 안티스팸 검사 활성화**)** 섹션에서 정책에 대해 사용할 안티스팸 솔루션을 선택합니다.

표시되는 옵션은 활성화된 안티스팸 검사 솔루션에 따라 다릅니다.

기본값 이외의 다른 메일 정책의 경우, 기본 정책의 설정을 사용하면 페이지의 다른 옵션은 비활성화됩니다.

이 메일 정책에 대해 안티 스팸 검사를 모두 비활성화할 수 있습니다.

단계 **5** 양성으로 식별된 스팸, 의심스런 스팸 및 마케팅 메시지에 대한 설정을 구성합니다.

옵션	설명
Enable Suspected Spam Scanning(의심스러운 스팸 검사 활성화) Enable Marketing Email Scanning(마케팅 이메일 검사 활성화)	옵션을 선택합니다. 안티스팸 검사가 활성화된 경우 양성으로 식별된 스팸 검사는 항상 활성화됩니다.
Apply This Action to Message(메시지에 다음 작업 적용)	양성으로 식별된 스팸, 의심스런 스팸 또는 원치 않는 마케팅 메시지에 대해 수행할 전체적인 작업을 선택합니다. • 전달 • 드롭 • 반송 • 격리
(선택 사항) 대체 호스트로 전송	확인된 메시지를 대체 대상 메일 호스트(SMTP 경로 또는 DNS에 나열된 항목 이외의 다른 이메일 서버)로 보낼 수 있습니다. IP 주소 또는 호스트 이름을 입력합니다. 호스트 이름을 입력하는 경우 먼저 해당 MX(메일 교환기)가 쿼리됩니다. MX가 없는 경우 DNS 서버의 A 레코드가 사용됩니다(SMTP 경로와 동일). 메시지를 추가적으로 검사하기 위해 샌드박스 메일 서버 등으로 리디렉션하려는 경우에만 이 옵션을 사용합니다. 중요한 추가 정보는 전달 호스트 변경 작업, 217 페이지 섹션을 참조하십시오.
제목에 텍스트 추가	사용자들이 스팸 및 원치 않는 마케팅 메시지를 좀 더 쉽게 식별하고 정렬할 수 있도록 특정 텍스트 문자열을 앞이나 뒤에 추가하여 식별된 메시지 제목의 텍스트를 변경할 수 있습니다. 참고 이 필드에서 공백은 무시되지 않습니다. 이 필드에 입력하는 텍스트 뒤(앞에 추가하는 경우) 또는 앞(뒤에 추가하는 경우)에 공백을 추가하여 추가된 텍스트를 메시지의 원래 제목과 구분합니다. 예를 들어 앞에 추가하는 경우 일부 후행 공백과 함께 `[SPAM]` 텍스트를 추가합니다. "제목에 텍스트 추가"필드에서는 US-ASCII 문자만 허용됩니다.

옵션	설명
고급 옵션(사용자 지정 헤더 및 메시지 전송에 사용)	
(선택 사항) 사용자 지정 헤더 추가	사용자 지정 헤더를 확인된 메시지에 추가할 수 있습니다. **Advanced**(고급)를 클릭하고 헤더 및 값을 정의합니다. 콘텐츠 필터와 함께 사용자 지정 헤더를 사용하여 의심스러운 스팸 메시지의 URL 리디렉션과 같은 작업을 수행하여 Cisco Web Security 프록시 서비스를 통과하도록 할 수 있습니다. 자세한 내용은 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예 , 366 페이지를 참조하십시오.
(선택 사항) 대체 봉투 수신자로 전송	확인된 메시지가 대체 봉투 수신자 주소로 전송되도록 할 수 있습니다. **Advanced**(고급)를 클릭하고 대체 주소를 정의합니다. 예를 들어 후속 검사를 위해 스팸으로 확인된 메시지를 관리자의 사서함으로 라우팅할 수 있습니다. 다중 수신자 메시지인 경우 단일 복사본만 대체 수신자에게 전송됩니다.
메시지 보관	확인된 메시지를 "안티 스팸 보관소" 로그에 보관할 수 있습니다. 형식은 mbox 형식의 로그 파일입니다.
Spam Thresholds(스팸 임계값)	기본 임계값을 사용하거나, 양성으로 식별된 스팸 및 의심스런 스팸에 대한 임계값을 입력합니다.

단계 **6** 변경사항을 제출하고 커밋합니다.

다음에 수행할 작업

발송 메일에 대해 안티스팸 검사를 활성화한 경우 관련 Host Access Table의 안티스팸 설정, 특히 개인 리스너에 대한 설정을 확인하십시오. 메일 플로우 정책을 사용하여 이메일 발신자에 대한 액세스 규칙 정의, 101 페이지를 참조하십시오.

관련 주제

- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 356 페이지
- 스팸 판정 임계값 및 의심스러운 스팸 임계값 이해, 365 페이지
- 구성 예: 양성으로 식별된 스팸 대 의심스런 스팸에 대한 작업 , 365 페이지
- 합법적인 소스에서 오는 원치 않는 마케팅 메시지, 366 페이지
- 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예 , 366 페이지
- 여러 메일 정책에서 서로 다른 안티스팸 검사 엔진 사용: 구성 예 , 367 페이지

스팸 판정 임계값 및 의심스러운 스팸 임계값 이해

메시지가 스팸인지 평가할 때 두 가지 안티스팸 검사 솔루션은 모두 메시지의 전체 스팸 점수를 산출할 수 있도록 수천 개의 규칙을 적용합니다. 그런 다음 이 점수를 해당되는 메일 정책에 지정된 임계값과 비교하여 메시지가 스팸인지 결정합니다.

최고의 정확성을 위해 양성으로 식별된 스팸의 임계값은 기본적으로 상당히 높습니다. 점수가 90과 100 사이인 메시지는 양성으로 식별된 스팸으로 간주됩니다. 의심스러운 스팸에 대한 기본 임계값은 50입니다.

- 의심스러운 스팸 임계값 미만의 메시지는 정상 메시지로 간주됩니다.
- 의심스러운 스팸 임계값을 초과하지만 스팸 판정 임계값 미만의 메시지는 의심스러운 스팸으로 간주됩니다.

각 메일 정책에서 스팸 판정 및 의심스러운 스팸 임계값을 사용자 지정하여 조직의 스팸 허용 수준을 반영하도록 안티스팸 솔루션을 구성할 수 있습니다.

양성으로 식별된 스팸 임계값을 50~99 범위의 값으로 변경할 수 있습니다. 의심스런 스팸의 임계값을 25와 양성으로 식별된 스팸에 대해 지정한 값 사이의 값으로 변경할 수 있습니다.

임계값을 변경하는 경우:

- 낮은 값을 지정(더욱 적극적인 구성)할수록 스팸으로 확인되는 메시지가 증가하고 더 많은 긍정 오류가 발생할 수 있습니다. 이 경우 사용자에게 스팸이 표시될 위험은 낮아지지만, 정상 메일이 스팸으로 표시될 위험은 커집니다.
- 높은 값을 지정(더욱 보수적인 구성)할수록 스팸으로 확인되는 메시지가 감소하고 더 많은 스팸이 전달될 수 있습니다. 이 경우 사용자에게 스팸이 표시될 위험은 커지지만, 정상 메일이 스팸으로 분류될 위험은 낮아집니다. 올바르게 설정된 경우, 메시지 제목에 따라 스팸 가능성이 있는 메시지로 식별되어 메시지가 전달됩니다.

양성으로 식별된 스팸과 의심스런 스팸에 대해 수행할 작업을 별도로 정의할 수 있습니다. 예를 들어 "양성으로 식별된" 스팸은 삭제하고 "의심스런" 스팸은 격리할 수 있습니다.

관련 주제

- 안티 스팸 솔루션 , 356 페이지
- 구성 예: 양성으로 식별된 스팸 대 의심스런 스팸에 대한 작업 , 365 페이지

구성 예: 양성으로 식별된 스팸 대 의심스런 스팸에 대한 작업

스팸	샘플 작업 (적극적)	샘플 작업 (보수적)
양성으로 식별된 스팸	드롭	• 메시지 제목에 "[스팸으로 확인된 스팸]"을 추가한 상태로 전달 또는 • 격리
의심스러운 스팸	메시지 제목에 "[의심스러운 스팸]"을 추가한 상태로 전달	메시지 제목에 "[의심스러운 스팸]"을 추가한 상태로 전달

적극적인 예에서는 의심스런 스팸 메시지에만 태그를 달고 양성으로 식별된 스팸 메시지는 삭제합니다. 관리자 및 최종 사용자는 수신 메시지의 제목 줄에서 긍정 오류를 확인할 수 있으며 관리자는 의심스러운 스팸 임계값을 조정(필요한 경우)할 수 있습니다.

신중한 예에서는 양성으로 식별된 스팸과 의심스런 스팸이 변경된 제목과 함께 전달됩니다. 사용자는 의심스런 스팸과 양성으로 식별된 스팸을 삭제할 수 있습니다. 이 방법은 첫 번째 방법보다 더 보수적인 방법입니다.

메일 정책의 적극적인 정책 및 보수적인 정책에 대한 자세한 설명은 관리되는 예외, 281 페이지 섹션을 참조하십시오.

합법적인 소스에서 오는 원치 않는 마케팅 메시지

메일 정책의 안티스팸 설정 아래에서 Marketing Email Settings(마케팅 이메일 설정)를 구성한 경우, AsyncOS 9.5 for Email로 업그레이드하면 안티스팸 설정 아래의 Marketing Email Settings(마케팅 이메일 설정)가 동일한 정책의 회색 메일 설정 아래로 이동합니다. 그레이메일 관리, 387 페이지의 내용을 참조하십시오.

사용자지정헤더를사용하여의심스러운스팸의URL을CiscoWebSecurity 프록시로 리디렉션: 구성 예

수신자가 메시지의 링크를 클릭하면 해당 요청이 Cisco Web Security 프록시 서비스를 통해 라우팅되도록 의심스러운 스팸의 URL을 재작성할 수 있습니다. 이렇게 하면 클릭하는 시간에 사이트의 안전성이 평가되고 알려진 악성 사이트로의 액세스가 차단됩니다.

시작하기 전에

URL 필터링 기능 및 해당 사전 요구 사항을 활성화합니다. URL 필터링 설정, 426 페이지를 참조하십시오.

단계 **1** 의심스러운 스팸 메시지에 사용자 지정 헤더를 적용합니다.

a) **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)**를 선택합니다.
b) 기본 정책 등의 정책에서 **Anti-Spam(**안티스팸**)** 열의 링크를 클릭합니다.
c) Suspected Spam Settings(의심스러운 스팸 설정) 섹션에서 의심스러운 스팸 검사를 활성화합니다.
d) **Advanced(**고급**)**를 클릭하여 Add Custom Header(사용자 지정 헤더 추가) 옵션을 표시합니다.
e) url_redirect 등 맞춤형 헤더를 추가합니다.
f) 변경사항을 제출하고 커밋합니다.

단계 **2** 사용자 지정 헤더가 있는 메시지의 URL을 리디렉션하도록 다음과 같이 콘텐츠 필터를 생성합니다.

a) **Mail Policies > Incoming Content Filters(**메일 정책 > 수신 콘텐츠 필터**)**를 선택합니다.
b) **Add Filter(**필터 추가**)**를 클릭합니다.
c) 필터 이름으로 url_redirect를 지정합니다.
d) **Add Condition(**조건 추가**)**을 클릭합니다.
e) **Other Header(**기타 헤더**)**를 클릭합니다.

f) 헤더 이름으로 url_redirect를 입력합니다.

이 이름은 위에서 생성한 헤더와 정확히 일치해야 합니다.

g) **Header exists(**헤더 있음**)**를 선택합니다.
h) **OK(**확인**)**를 클릭합니다.
i) **Add Action(**작업 추가**)**을 클릭합니다.
j) **URL Category(URL** 범주**)**를 클릭합니다.
k) **Available Categories(**사용 가능한 범주**)**에서 모든 범주를 선택하고 이를 **Selected Categories(**선택한 범주**)**에 추가합니다.
l) Action on URL(URL에 대한 작업)에 **Redirect to Cisco Security Proxy(Cisco Security** 프록시로 리디렉션**)**를 선택합니다.
m) **OK(**확인**)**를 클릭합니다.

단계 **3** 메일 정책에 콘텐츠 필터를 추가합니다.

a) **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)**를 선택합니다.
b) 이 절차의 앞부분에서 선택한 정책에서 **Content Filters(**콘텐츠 필터**)** 열의 링크를 클릭합니다.
a) 아직 선택하지 않은 경우 **Enable Content Filters(**콘텐츠 필터 활성화**)**를 선택합니다.
b) **url_filtering** 콘텐츠 필터를 활성화할 확인란을 선택합니다.
c) 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- URL 리디렉션, 403 페이지
- 콘텐츠 필터, 283 페이지

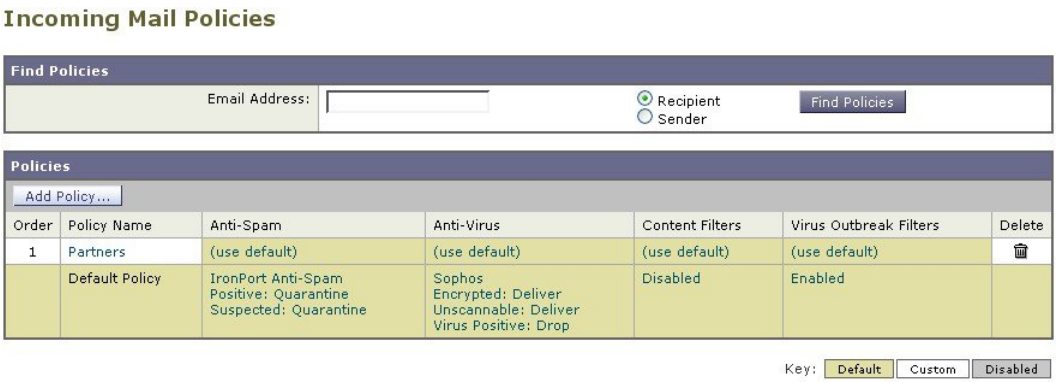
여러 메일 정책에서 서로 다른 안티스팸 검사 엔진 사용: 구성 예

시스템 설치 마법사를 사용(또는 CLI의 systemsetup 명령 사용)하는 경우 Cisco Intelligent Multi-Scan 또는 Cisco Anti-Spam 엔진을 활성화하는 옵션이 제공됩니다. 시스템 설치 중에 두 가지 솔루션을 모두 활성화할 수는 없지만, 시스템 설치가 완료되면 Security Services(보안 서비스) 메뉴를 사용하여 선택하지 않은 안티스팸 솔루션을 활성화할 수 있습니다.

시스템을 설정한 후에는 **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)** 페이지에서 수신 메일 정책에 맞게 안티 스팸 검사 솔루션을 구성할 수 있습니다. 발송 메일 정책의 경우 일반적으로 안티 스팸 검사는 비활성화됩니다. 안티스팸 검사는 특정 정책에 대해서도 비활성화할 수 있습니다.

이러한 경우 기본 메일 정책 및 "파트너" 정책에서 Cisco Anti-Spam 검사 엔진을 사용하여 스팸 판정 및 의심스러운 스팸을 격리하고 있습니다.

그림 ***20:*** 메일 정책 - 수신자별 안티 스팸 엔진

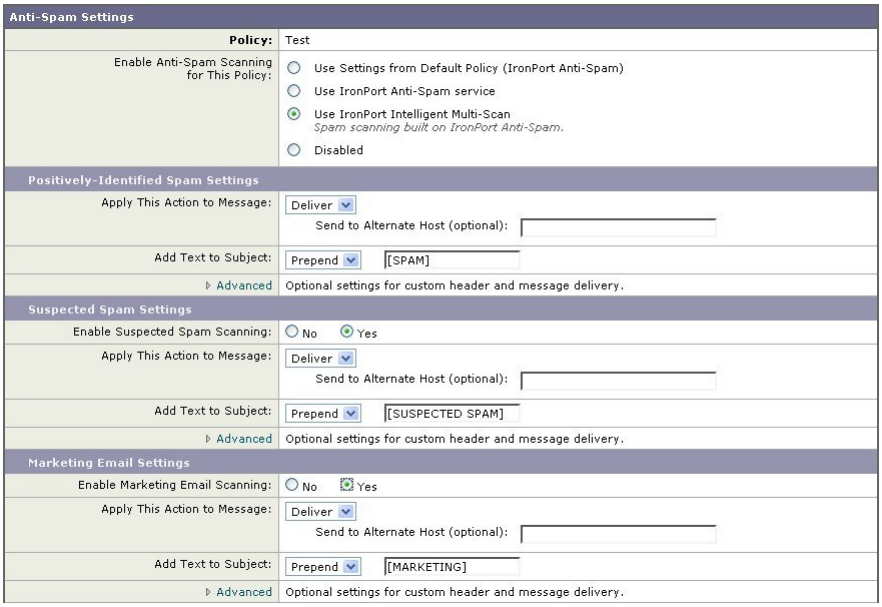


Cisco Intelligent Multi-Scan을 사용하고 원치 않는 마케팅 메시지를 검사하도록 파트너 정책을 변경하려면 Partners(파트너) 행에 해당하는 Anti-Spam(안티 스팸) 열의 항목을 클릭합니다("기본값 사용").

검사 엔진으로 Cisco Intelligent Multi-Scan을 선택하고 원치 않는 마케팅 메시지 탐지를 활성화하려면 Yes(예)를 선택합니다. 원치 않는 마케팅 메시지 탐지를 위한 기본 설정을 사용합니다.

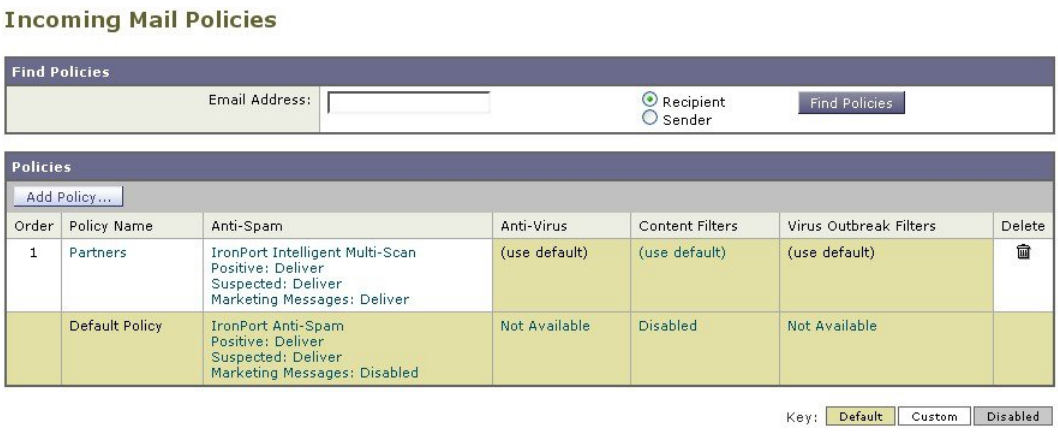
다음 그림에서는 해당 정책에서 활성화된 Cisco Intelligent Multi-Scan 및 원치 않는 마케팅 메시지 탐지를 보여줍니다.

그림 ***21: Mail Policies(***메일 정책***) - Cisco Intelligent Multi-Scan*** 활성화



변경사항을 제출하고 커밋한 후에 메일 정책은 다음과 같습니다.

그림 *22:* 메일 정책 - 정책에서 활성화된 ***Intelligent Multi-Scan***



스팸 필터로부터 어플라이언스에서 생성된 메시지 보호

Cisco IronPort 어플라이언스(예: 이메일 경고 및 예약 보고서)에서 전송된 자동화된 이메일 메시지에는 스팸으로 잘못 확인될 수 있게 하는 URL 또는 기타 정보가 포함될 수 있으므로 해당 이메일 메시지를 전송하려면 다음을 수행해야 합니다.

안티스팸 검사를 우회하는 수신 메일 정책에 이러한 메시지 발신자를 포함합니다. 발신자 및 수신자 그룹에 대한 메일 정책 만들기, 276 페이지 및 안티스팸 시스템 우회 작업, 223 페이지 섹션을 참조하십시오.

안티스팸 검사 중에 추가되는 헤더

- 메일 정책에서 안티스팸 검사 엔진이 활성화된 경우 해당 정책을 통과한 메시지마다 다음 헤더가 추가됩니다.

  X-IronPort-Anti-Spam-Filtered: true

  X-IronPort-Anti-Spam-Result

  두 번째 헤더에는 Cisco 지원에서 메시지 검사에 사용되는 규칙 및 엔진 버전을 식별할 수 있는 정보가 들어 있습니다. 결과 정보는 인코딩된 독점 정보이며 고객이 디코딩할 수 있습니다.

- Cisco Intelligent Multi-Scan은 타사 안티 스팸 검사 엔진에서도 헤더를 추가합니다.
- 지정된 메일 정책에서 양성으로 식별된 스팸, 의심스런 스팸 또는 원치 않는 마케팅 메일로 식별되는 모든 메시지에 추가할 사용자 지정 헤더를 추가로 정의할 수 있습니다. 안티스팸 정책 정의, 362 페이지를 참조하십시오.

관련 주제

- 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예, 366 페이지

Cisco에 잘못 분류된 메시지 보고

잘못 분류된 것으로 보이는 메시지는 분석을 위해 Cisco에 보고할 수 있습니다. 보고된 메시지는 제품의 정확성과 효율성을 개선하는 데 사용됩니다.

다음 카테고리에 속하는 잘못 분류된 메시지를 보고할 수 있습니다.

- 누락된 스팸
- 스팸으로 표시되었지만 스팸이 아닌 메시지
- 누락된 마케팅 메시지
- 마케팅 메시지로 표시되었지만 마케팅 메시지가 아닌 메시지
- 누락된 피싱 메시지

관련 주제

- Cisco에 잘못 분류된 메시지를 보고하는 방법, 370 페이지
- 제출을 추적하는 방법, 374 페이지

Cisco에 잘못 분류된 메시지를 보고하는 방법

시작하기 전에

잘못 분류된 메시지를 Cisco에 보고하기 전에 다음 단계를 수행해야 합니다. 이 단계는 한 번만 수행하면 됩니다.

단계 **1** 조직의 모든 어플라이언스에 대한 공통 등록 ID를 설정합니다. 등록 ID는 특정 조직에 속한 Cisco Email Security 게이트웨이에서의 제출을 식별하기 위한 고유 식별자입니다.

1. 웹 인터페이스를 사용하여 어플라이언스에 로그인합니다.
2. **System Administration**(시스템 관리) > **Email Submission and Tracking Portal Registration**(이메일 제출 및 추적 포털 등록)으로 이동합니다.
3. 어플라이언스가 클러스터의 일부인 경우에는 모드를 클러스터 수준으로 설정합니다.
4. **Set Registration ID**(등록 **ID** 설정)를 클릭합니다.
5. **Registration ID**(등록 **ID**) 필드에 값을 입력합니다. 입력하는 값은 16자 이상이어야 하지만 48자를 초과해서는 안 되며 영숫자, 하이픈(-) 및 밑줄(_)만 포함해야 합니다.
6. 변경 사항을 제출 및 커밋합니다.
7. 어플라이언스가 클러스터의 일부가 아닌 경우 조직의 모든 어플라이언스에서 1~6단계를 반복해야 합니다.

CLI에서 `portalregistrationconfig` 명령을 사용하여 등록 ID를 설정할 수도 있습니다.

단계 **2** 다음 방법 중 하나로 Cisco 이메일 제출 및 추적 포털에 관리자로 등록할 수 있습니다. Cisco 이메일 제출 및 추적 포털은 이메일 관리자가 잘못 분류된 메시지를 Cisco에 보고하고 추적할 수 있는 웹 기반 도구입니다.

참고 Cisco 이메일 제출 및 추적 포털은 이메일 관리자가 잘못 분류된 메시지를 Cisco에 보고하고 추적할 수 있는 웹 기반 도구입니다.

- 포털에 액세스할 수 있는 조직의 첫 번째 관리자인 경우 등록:
  1. Cisco 크리덴셜을 사용하여 Cisco 이메일 제출 및 추적 포털(https://email-submission.cisco.com)에 로그인합니다.
  2. 이메일 제출 및 추적 포털에서 **Register a new Registration ID**(새 등록 **ID** 등록)를 선택하고 **1**단계에서 생성한 등록 ID를 입력 한 후 **Register**(등록)를 클릭 합니다. 여기에 입력하는 등록 ID는 어플라이언스에서 이메일 제출 및 추적 포털 설정을 구성하는 동안 입력한 것과 동일해야 합니다.

- 조직의 관리자가 포털에 이미 등록된 경우의 등록:
  1. Cisco 크리덴셜을 사용하여 Cisco 이메일 제출 및 추적 포털(https://email-submission.cisco.com)에 로그인합니다.
  2. 이메일 제출 및 추적 포털에서 **Register as an administrator**(관리자로 등록)를 선택하고 포털에 이미 등록되어 있는 관리자의 이메일 주소를 입력한 후 **Register**(등록)를 클릭합니다.

Register(등록)를 클릭하면 포털에 이미 등록되어 있는 관리자에게 이메일 알림이 전송됩니다. 관리자는 등록 요청을 허용하거나 거부할 수 있도록 포털에 로그인하여 구성 패널에서 **Admin registration requests**(관리자 등록 요청)를 클릭해야 합니다.

단계 **3** Cisco 이메일 제출 및 추적 포털에 도메인을 등록합니다.

1. Cisco 이메일 제출 및 추적 포털로 이동합니다.
2. **Configuration**(구성) > **Domains**(도메인)를 클릭합니다.
3. **Add new domain**(새 도메인 추가)을 클릭합니다.
4. 조직의 도메인을 입력하고 **Add**(추가)를 클릭합니다.

참고 유효한 도메인 이름을 입력했는지 확인합니다. 예를 들어, `example.com`은 이메일 주소 `user@example.com`의 도메인 이름입니다. 조직에 여러 도메인이 있는 경우 모든 도메인을 추가해야 합니다.

도메인 추가 요청은 `postmaster@domain.com`으로 전송됩니다. 여기서 domain.com은 이 단계에서 입력한 도메인입니다. 이 도메인의 관리자가 요청을 검토하고 승인해야 합니다.

조직에서 `postmaster@domain.com`을 사용하지 않거나 관리자가 postmaster 사서함에 액세스할 수 없는 경우 모든 어플라이언스의 메시지 필터를 생성하여 `postmaster@domain.com`으로 전송되는 `SubmissionPortal@cisco.com`의 메시지를 다른 이메일 주소로 리디렉션합니다. 다음은 샘플 메시지 필터입니다.

```
redirect_postmaster: if (rcpt-to == "postmaster@domain.com") AND (mail-from ==
"^SubmissionPortal@cisco.com$") { alt-rcpt-to ("admin@domain.com"); }
```

Cisco에 잘못 분류된 메시지를 보고하는 방법

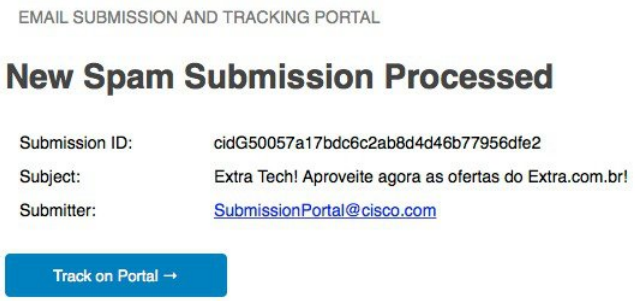
자세한 내용은 https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200648-ESA-FAQ-How-to-work-with-Cisco-Email-Su.html의 내용을 참고하십시오.

단계 **1** Cisco에 잘못 분류된 메시지를 보고하는 방법, 370 페이지의 시작하기 전에 섹션에 설명된 단계를 수행합니다.

단계 **2** 다음 방법 중 하나를 사용하여 Cisco에 잘못 분류된 메시지를 보고합니다.

- Cisco Email Security 플러그인 사용, 372 페이지
- Cisco 이메일 제출 및 추적 포털 사용, 373 페이지
- 잘못 분류된 메시지를 첨부 파일로 전달, 373 페이지

잘못 분류된 메시지를 Cisco에 보고하면 2시간 이내에 이메일 알림이 수신됩니다. 다음은 샘플 이메일 알림입니다.



2시간 이내에 이메일 알림을 받지 못한 경우 제출에 실패했을 수 있습니다. 트러블슈팅 지침을 보려면 포털에서 **Help**(도움말) > **Troubleshooting Instructions**(문제 해결 지침)을 클릭하십시오.

다음에 수행할 작업

제출을 추적하는 방법, 374 페이지

Cisco Email Security 플러그인 사용

Cisco Email Security 플러그인은 사용자(이메일 관리자 및 엔드 유저)가 Microsoft Outlook를 사용하여 Cisco에 잘못 분류된 메시지를 보고하는 데 사용할 수 있는 도구입니다. Microsoft Outlook의 일부분으로 이 플러그인을 구축하면 Microsoft Outlook 웹 인터페이스에 보고 메뉴가 추가됩니다. 플러그인 메뉴를 사용하여 잘못 분류된 메시지를 보고할 수 있습니다.

추가 정보

- https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=284900944&flowid=41782&softwareid=283090986 페이지에서 Cisco Email Security 플러그인을 다운로드할 수 있습니다.
- 자세한 내용은 Cisco Email Security 플러그인 관리자 가이드(http://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html)를 참고하십시오.

Cisco 이메일 제출 및 추적 포털 사용

Cisco 이메일 제출 및 추적 포털은 이메일 관리자가 잘못 분류된 메시지를 Cisco에 보고할 수 있는 웹 기반 도구입니다. 또한 관리자는 포털을 사용하여 조직의 제출을 추적할 수 있습니다.

참고 현재는 포털을 사용하여 잘못 분류된 스팸 메시지만 보고할 수 있습니다.

단계 **1** Cisco 크리덴셜을 사용하여 Cisco 이메일 제출 및 추적 포털(https://email-submission.cisco.com)에 로그인합니다.

단계 **2** 이메일 제출 및 추적 포털의 **Submissions(**제출**)** 탭에서 **New Submission(**새 제출**)**을 클릭합니다.

단계 **3** 잘못 분류된 메시지를 선택합니다. 이러한 메시지는 EML 형식이어야 하며 메시지의 총 크기는 15MB를 초과하지 않아야 합니다.

단계 **4** **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

추가 정보

Cisco 이메일 제출 및 추적 포털에 대한 자세한 내용은 다음 문서를 참고하십시오.

방법	확인
이메일 제출 및 추적 포털을 사용하여 Cisco에 잘못 분류된 메시지 보고	https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/117822-qanda-esa-00.html
Cisco 이메일 제출 및 추적 포털 사용	https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200648-ESA-FAQ-How-to-work-with-Cisco-Email-Su.html
Cisco 이메일 제출 및 추적 포털 트러블슈팅	https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200653-ESA-FAQ-Troubleshooting-Email-Submissio.html

잘못 분류된 메시지를 첨부 파일로 전달

메시지의 카테고리에 따라 잘못 분류된 각 메시지를 RFC 822 첨부 파일로 다음 주소에 전달할 수 있습니다.

- 누락된 스팸 - spam@access.ironport.com
- 스팸으로 표시되었지만 스팸이 아닌 메시지 - ham@access.ironport.com
- 누락된 마케팅 메시지 - ads@access.ironport.com
- 마케팅 메시지로 표시되었지만 마케팅 메시지가 아닌 메시지 - not_ads@access.ironport.com
- 누락된 피싱 메시지 - phish@access.ironport.com

다음 이메일 프로그램 중 하나를 사용하여 메시지를 전달하는 경우 최상의 결과를 얻을 수 있습니다.

- Apple Mail
- Microsoft Outlook for Mac
- Microsoft Outlook Web App
- Mozilla Thunderbird

주의 Microsoft Windows용 Microsoft Outlook 2010, 2013 또는 2016을 사용하는 경우, Cisco Email Security 플러그인 또는 Microsoft Outlook Web App을 사용하여 잘못 분류된 메시지를 보고해야 합니다. Windows용 Outlook은 필수 헤더가 그대로 유지되는 메시지를 전달하지 않을 수 있기 때문입니다. 또한 원본 메시지를 첨부 파일로 전달할 수 있는 경우에만 모바일 플랫폼을 사용합니다.

제출을 추적하는 방법

제출 상세정보가 포함된 이메일 알림을 받은 후에는 Cisco 이메일 제출 및 추적 포털에서 제출을 보고 추적할 수 있습니다.

단계 **1** Cisco 크리덴셜을 사용하여 Cisco 이메일 제출 및 추적 포털(https://email-submission.cisco.com)에 로그인합니다.

단계 **2** 이메일 제출 및 추적 포털에서 **Submission**(제출)을 클릭합니다.

단계 **3** 필터(기간, 제출 ID, 제목, 제출자 및 상태)를 사용하여 제출을 확인합니다.

다음에 수행할 작업

자세한 내용은 https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200648-ESA-FAQ-How-to-work-with-Cisco-Email-Su.html. 장을 참조해 주십시오.

수신 릴레이 사용 배포 환경에서 발신자 IP 주소 확인

하나 이상의 메일 교환/전송 에이전트(MX 또는 MTA), 필터링 서버 등이 네트워크 경계에서 Cisco 어플라이언스와 수신 메일을 보내는 외부 머신 사이에 있는 경우 어플라이언스는 전송 머신의 IP 주소를 확인할 수 없습니다. 대신 메일은 로컬 MX/MTA에서 발생한 것으로 표시됩니다. 그러나 IronPort Anti-Spam 및 Cisco Intelligent Multi-Scan(SenderBase Reputation Service 사용)은 외부 발신자의 정확한 IP 주소에 따라 달라집니다.

해결책은 수신 릴레이와 연동되도록 어플라이언스를 구성하는 것입니다. Cisco 어플라이언스에 연결된 모든 내부 MX/MTA의 이름 및 IP 주소와 함께 원래 IP 주소를 저장하는 데 사용되는 헤더를 지정합니다.

관련 주제

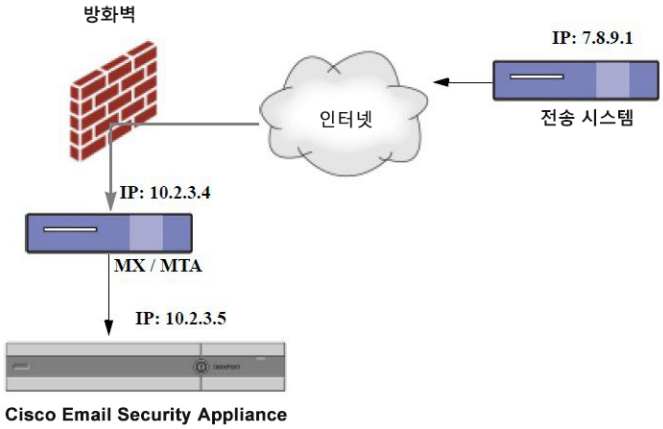
- 수신 릴레이를 사용하는 예제 환경 , 375 페이지
- 수신 릴레이와 연동되도록 어플라이언스 구성, 376 페이지
- 수신 릴레이가 기능에 영향을 미치는 방식 , 381 페이지

• 사용된 헤더를 지정하기 위한 로그 구성 , 383 페이지

수신 릴레이를 사용하는 예제 환경

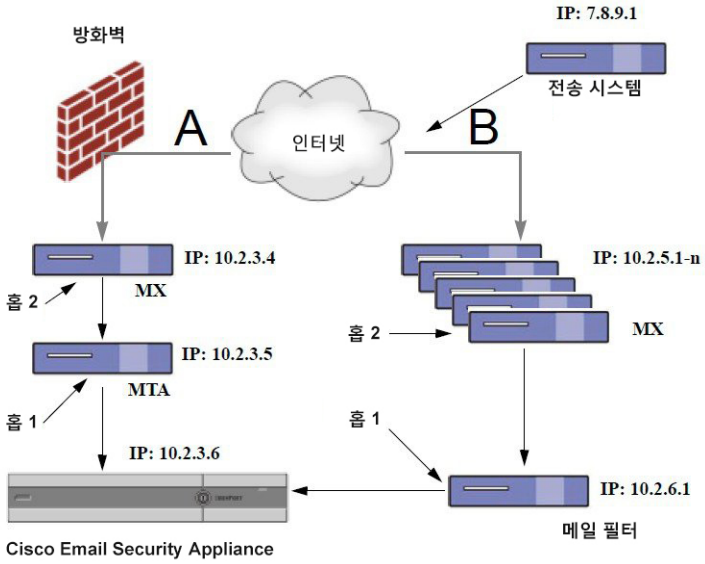
다음 그림은 수신 릴레이에 대한 기본적인 예를 보여줍니다. IP 주소 7.8.9.1에서 보낸 메일은 로컬 MX/MTA가 Cisco 어플라이언스에 메일을 릴레이하는 중이므로 IP 주소 10.2.3.4에서 오는 것으로 나타납니다.

그림 ***23: MX/MTA***로 릴레이되는 메일 - 기본



다음 그림은 메일이 Cisco 어플라이언스에 전달되기 전에 네트워크 내부에서 릴레이되는 방식과 메일이 네트워크 내부의 여러 서버에서 처리되는 방식에 대한 약간 더 복잡한 예를 보여줍니다. 예 A에서 7.8.9.1에서 전송된 메일은 방화벽을 통과하고 Cisco 어플라이언스로 전달되기에 앞서 MX 및 MTA에 의해 처리됩니다. 예 B에서는 7.8.9.1에서 전송된 메일은 로드 밸런서 또는 다른 유형의 트래픽 셰이핑 어플라이언스로 전송되며 Cisco 어플라이언스에 전달되기에 앞서 MX 주소 중 하나로 전송됩니다.

그림 ***24: MX/MTA***로 릴레이되는 메일 - 고급



수신 릴레이와 연동되도록 어플라이언스 구성

관련 주제

- 수신 릴레이 기능 활성화 , 376 페이지
- 수신 릴레이 추가 , 376 페이지
- 릴레이되는 메시지에 대한 메시지 헤더 , 378 페이지

수신 릴레이 기능 활성화

참고 로컬 MX/MTA가 메일을 Cisco 어플라이언스로 릴레이하는 경우에만 수신 릴레이 기능을 활성화해야 합니다.

단계 **1** **Network**(네트워크) > **Incoming Relays**(수신 릴레이)를 선택합니다.

단계 **2** **Enable**(활성화)을 클릭합니다.

단계 **3** 변경사항을 커밋합니다.

수신 릴레이 추가

수신 릴레이를 추가하여 다음을 확인할 수 있습니다.

- 네트워크에서 수신 메시지를 Email Security Appliance로 릴레이할 머신

- 원래 외부 발신자의 IP 주소에 레이블을 지정할 헤더

시작하기 전에

이러한 사전 요구 사항을 완료하는 데 필요한 내용은 릴레이되는 메시지에 대한 메시지 헤더 , 378 페이지 항목을 참조하십시오.

- 원래 외부 발신자의 IP 주소를 식별하는 데 사용자 지정 헤더를 사용할지 아니면 Received 헤더를 사용할지 결정합니다.
- 사용자 지정 헤더를 사용하는 경우 다음을 수행합니다.
  - 릴레이되는 메시지의 원래 IP 주소에 레이블을 지정할 정확한 헤더를 확인합니다.
  - 각 MX, MTA 또는 원래 외부 발신자에 연결되는 다른 머신의 경우 헤더 이름 및 원래 외부 발신자의 IP 주소를 수신 메시지에 추가하도록 머신을 설정합니다.

단계 **1** **Network**(네트워크) **> Incoming Relays**(수신 릴레이)를 선택합니다.

단계 **2** **Add Relay**(릴레이 추가)를 클릭합니다.

단계 **3** 이 릴레이의 이름을 입력합니다.

단계 **4** 수신 메시지를 릴레이하기 위해 Email Security Appliance에 연결되는 MTA, MX 또는 다른 머신의 IP 주소를 입력합니다.

IPv4나 IPv6 주소, 표준 CIDR 형식 또는 IP 주소를 사용할 수 있습니다. 예를 들어 이메일을 수신하는 네트워크 경계에 MTA가 여러 개 있는 경우, 모든 MTA를 포함하도록 IP 주소 범위를 입력할 수 있습니다(예: 10.2.3.1/8 또는 10.2.3.1~10).

IPv6 주소의 경우 AsyncOS는 다음 형식을 지원합니다.

- `2620:101:2004:4202::0-2620:101:2004:4202::ff`
- `2620:101:2004:4202::`
- `2620:101:2004:4202::23`
- `2620:101:2004:4202::/64`

단계 **5** 원래 외부 발신자의 IP 주소를 식별하는 헤더를 지정합니다.

헤더를 입력하는 경우 후행 콜론을 입력할 필요가 없습니다.

a) 헤더 유형을 선택합니다.

사용자 지정 헤더(권장) 또는 Received 헤더를 선택합니다.

b) 사용자 지정 헤더의 경우:

릴레이되는 메시지에 추가하기 위해 릴레이 머신을 구성한 헤더 이름을 입력합니다.

예를 들면 다음과 같습니다.

```
SenderIP
```

또는

```
X-CustomHeader
```

c) Received 헤더의 경우:

문자와 문자열을 입력하면 그 뒤에 IP 주소가 나타납니다. IP 주소를 확인하기 위한 "홉" 수를 입력합니다.

단계 **6** 변경사항을 제출하고 커밋합니다.

다음에 수행할 작업

다음을 수행해 보십시오.

- DHAP에 대해 무제한 메시지가 허용되는 메일 흐름 정책을 사용하여 발신자 그룹에 릴레이 머신을 추가합니다. 이에 대한 설명은 수신 릴레이 및 디렉토리 수집 공격 방지, 382 페이지 항목을 참조하십시오.
- 추적 및 문제 해결을 용이하게 하려면 사용되는 헤더를 표시하도록 어플라이언스 로그를 구성합니다. 사용된 헤더를 지정하기 위한 로그 구성 , 383 페이지를 참조하십시오.

관련 주제

- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 356 페이지

릴레이되는 메시지에 대한 메시지 헤더

다음 헤더 유형 중 하나를 사용하여 릴레이되는 메시지의 원래 발신자를 식별하도록 어플라이언스를 구성합니다.

- 사용자 지정 헤더 , 378 페이지
- 수신된 헤더, 379 페이지

사용자 지정 헤더

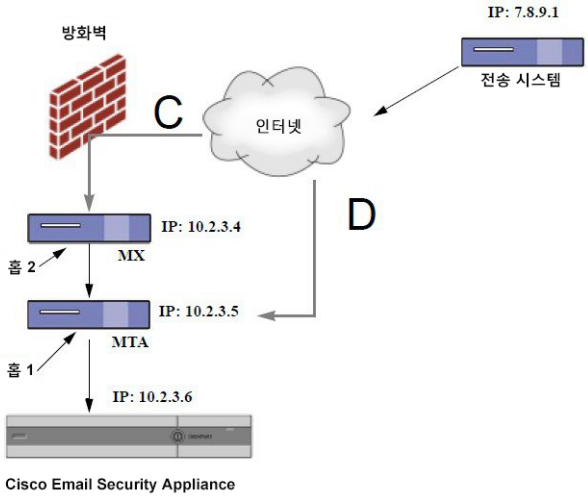
원래 발신자를 식별하는 방법으로 사용자 지정 헤더를 사용하는 것이 좋습니다. 원래 발신자에 연결하는 머신은 이 사용자 지정 헤더를 추가해야 합니다. 헤더 값은 외부 전송 머신의 IP 주소여야 합니다. 예를 들면 다음과 같습니다.

```
SenderIP: 7.8.9.1
```

```
X-CustomHeader: 7.8.9.1
```

로컬 MX/MTA는 가변적인 홉 수를 통해 메일을 받을 수 있지만, 사용자 지정 헤더를 삽입하는 것이 수신 릴레이 기능을 활성화하는 유일한 방법입니다. 예를 들어 다음 그림에서 경로 C 및 D는 IP 주소 10.2.3.5로 연결됩니다. 그러나 경로 C에는 2개의 홉이 있으며 경로 D에는 하나의 홉이 있습니다. 이 경우 홉 수가 달라질 수 있으므로 수신 릴레이를 올바르게 구성하려면 사용자 지정 헤더를 사용해야 합니다.

그림 ***25: MX/MTA***로 릴레이되는 메일 - 가변적인 홉 수



관련 주제

- 수신 릴레이 추가 , 376 페이지

수신된 헤더

전송 IP 주소가 들어 있는 사용자 지정 헤더를 포함하도록 MX/MTA를 구성하는 것이 선택 사항이 아닌 경우, 메시지에서 "Received:" 헤더를 검사하여 전송 IP 주소를 확인하도록 수신 릴레이 기능을 구성할 수 있습니다. "Received:" 헤더는 IP 주소에 대한 네트워크 "홉" 수가 항상 일정한 경우에만 사용할 수 있습니다. 즉, 첫 번째 홉(그림 - *MX/MTA*로 릴레이되는 메일 - 고급의 10.2.3.5)의 머신은 항상 네트워크 경계에서 벗어난 홉 수와 동일해야 합니다. 수신 메일이(그림 - *MX/MTA*로 릴레이되는 메일 - 가변적인 홉 수에 설명된 대로 홉 수가 달라짐) Cisco 어플라이언스에 연결된 머신에 대해 서로 다른 경로를 사용하는 경우 맞춤형 헤더를 사용해야 합니다(사용자 지정 헤더 , 378 페이지 참조).

다시 확인할 구문 분석 문자 또는 문자열 및 네트워크 홉 수(또는 Received: 헤더)를 지정합니다. 홉은 기본적으로 한 머신에서 다른 머신으로 이동하는 메시지입니다(Cisco 어플라이언스에서 수신하는 것은 홉으로 계산되지 않습니다. 자세한 내용은 사용된 헤더를 지정하기 위한 로그 구성 , 383 페이지 섹션을 참조하십시오. AsyncOS는 지정된 홉 수에 해당하는 Received: 헤더에서 구문 분석 문자 또는 문자열의 첫 번째 항목 다음에 오는 첫 번째 IP 주소를 찾습니다. 예를 들어 두 개의 홉을 지정하는 경우 Cisco 어플라이언스에서 역방향으로 동작하는 두 번째 Received: 헤더가 구문 분석됩니다. 구문 분석 문자 또는 유효한 IP 주소가 발견되지 않으면 Cisco 어플라이언스는 연결된 머신의 실제 IP 주소를 사용합니다.

다음 메일 헤더 예제에서 여는 대괄호([)와 두 개의 홉을 지정하는 경우 외부 머신의 IP 주소는 7.8.9.1입니다. 그러나 닫는 괄호(])를 구문 분석 문자로 지정하면 올바른 IP 주소를 찾을 수 없습니다. 이 경우 수신 릴레이 기능은 비활성화 상태로 판단되며 연결된 머신의 IP가 사용됩니다(10.2.3.5).

그림 - *MX/MTA*로 릴레이되는 메일 -고급 수신 릴레이의 예는 다음과 같습니다.

- 경로 A - 10.2.3.5(Received 헤더 사용 시 2개 홉)
- 경로 B - 10.2.6.1(Received 헤더 사용 시 2개 홉)

다음 표에서는 그림 - *MX/MTA*로 릴레이되는 메일 -고급에서처럼 여러 홉을 거쳐 Cisco 어플라이언스로 이동하는 메시지에 대한 이메일 헤더 예제를 보여줍니다. 이 예에서는 메시지가 수신자의 받은 편지함에 도착한 경우에 표시되는 잘못된 헤더(Cisco 어플라이언스에서 무시됨)를 보여줍니다. 지정하는 홉 수는 두 개입니다.

표 ***35:*** 일련의 ***Received:*** 헤더*(*경로 ***A*** 예 ***1)***

1	Microsoft Mail Internet Headers Version 2.0 Received: from smemail.rand.org ([10.2.2.7]) by smmail5.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713); Received: from ironport.customerdomain.org ([10.2.3.6]) by smemail.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713);
2	Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTP; 21 Sep 2005 13:46:07 -0700
3	Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4]) by mta.customerdomain.org (8.12.11/8.12.11) with ESMTP id j8LKkWu1008155 for <joefoo@customerdomain.org>
4	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTP id 4F3DA15AC22 for <joefoo@customerdomain.org>
5	Received: from linux1.thespammer.com (HELO linux1.thespammer.com) ([10.1.1.89]) by sending-machine.spamham.com with ESMTP; Received: from exchange1.thespammer.com ([10.1.1.111]) by linux1.thespammer.com with Microsoft SMTPSVC(6.0.3790.1830); Subject: Would like a bigger paycheck? Date: Wed, 21 Sep 2005 13:46:07 -0700 From: "A. Sender" <asend@otherdomain.com> To: <joefoo@customerdomain.org>

위 테이블에 대한 참고 사항:

- Cisco 어플라이언스는 이러한 헤더를 무시합니다.
- Cisco 어플라이언스는 메시지(홉으로 계산되지 않음)를 수신합니다.
- 첫 번째 홉(및 수신 릴레이).
- 두 번째 홉. 이는 전송 MTA입니다. IP 주소는 7.8.9.1입니다.
- Cisco 어플라이언스는 이러한 Microsoft Exchange 헤더를 무시합니다.

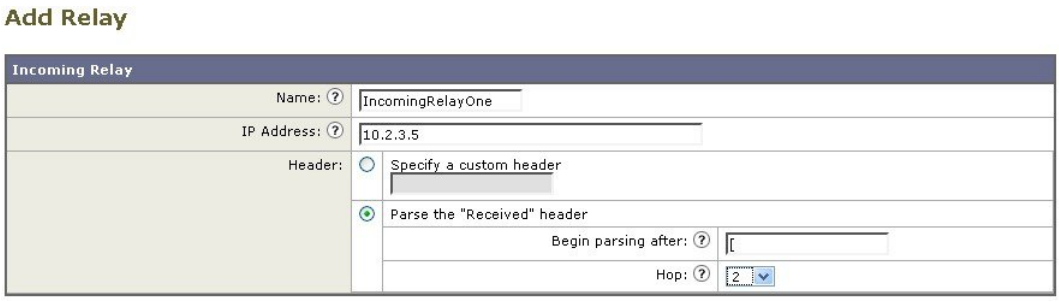
다음 표는 잘못된 헤더가 제외된 동일한 이메일 메시지의 헤더를 보여줍니다.

표 ***36:*** 일련의 ***Received:*** 헤더***(***경로 ***A*** 예 ***2)***

1	`Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTP; 21 Sep 2005 13:46:07 -0700`
2	`Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4]) by mta.customerdomain.org (8.12.11/8.12.11) with ESMTP id j8LKkWu1008155 for <joefoo@customerdomain.org>;`
3	`Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTP id 4F3DA15AC22 for <joefoo@customerdomain.org>;`

다음 그림은 GUI의 Add Relay(릴레이 추가) 페이지에 구성된 대로 경로 A(위)에 대한 수신 릴레이를 보여줍니다.

그림 ***26: Received*** 헤더와 함께 구성된 수신 릴레이



관련 주제

- 수신 릴레이 추가 , 376 페이지

수신 릴레이가 기능에 영향을 미치는 방식

- 수신 릴레이 및 필터, 381 페이지
- 수신 릴레이, HAT, SBRS 및 발신자 그룹, 382 페이지
- 수신 릴레이 및 디렉토리 수집 공격 방지, 382 페이지
- 수신 릴레이 및 추적, 382 페이지
- 수신 릴레이 및 이메일 보안 모니터(보고) , 382 페이지
- 수신 릴레이 및 메시지 추적, 382 페이지
- 수신 릴레이 및 로깅 , 382 페이지

수신 릴레이 및 필터

수신 릴레이 기능은 적절한 SenderBase Reputation 점수와 함께 다양한 SenderBase Reputation Service 관련 필터 규칙(reputation, no-reputation)을 제공합니다.

수신 릴레이, HAT, SBRS 및 발신자 그룹

HAT 정책 그룹은 현재 수신 릴레이의 정보를 사용하지 않습니다. 그러나 수신 릴레이 기능에서는 SenderBase Reputation 점수를 제공하므로 메시지 필터 및 $reputation 변수를 통해 HAT 정책 그룹 기능을 시뮬레이션할 수 있습니다.

수신 릴레이 및 디렉토리 수집 공격 방지

원격 호스트에서 네트워크의 수신 릴레이로 사용되는 MX 또는 MTA로 메시지를 전송하여 디렉토리 수집 공격을 시도하는 경우, 디렉토리 수집 공격 방지(DHAP)가 활성화되어 있는 메일 흐름 정책을 사용하여 릴레이가 발신자 그룹에 할당되어 있으면 어플라이언스는 수신 릴레이와의 연결을 끊습니다. 그러면 합법적인 메시지를 포함한 릴레이의 모든 메시지가 Email Security Appliance에 도달하지 못합니다. 따라서 어플라이언스는 원격 호스트를 공격자로 인식하지 못하며, 수신 릴레이로 동작하는 MX 또는 MTA는 공격 호스트에서 계속 메일을 받습니다. 이 문제를 해결하고 수신 릴레이로부터 계속 메시지를 받으려면 DHAP에 대한 무제한 메시지가 허용되는 메일 흐름 정책을 사용하여 릴레이를 발신자 그룹에 추가합니다.

수신 릴레이 및 추적

추적 기능은 소스 IP 주소의 평판 점수 대신 수신 릴레이의 SenderBase Reputation 점수를 반환합니다.

수신 릴레이 및 이메일 보안 모니터(보고)

수신 릴레이를 사용하는 경우:

- 이메일 보안 모니터 보고서는 외부 IP와 MX/MTA의 데이터를 모두 포함합니다. 예를 들어 외부 머신(IP 7.8.9.1)에서 내부 MX/MTA(IP 10.2.3.4)를 통해 이메일 5개를 전송한 경우, 메일 흐름 요약에는 IP 7.8.9.1에서 보낸 메시지 5개와 함께 내부 릴레이 MX/MTA(IP 10.2.3.5)에서 보낸 메시지 5개가 추가로 표시됩니다.
- 이메일 보안 모니터 보고서에서 SenderBase Reputation 점수는 정확하게 보고되지 않습니다. 또한,발신자 그룹도 정확하게 확인되지 않을 수 있습니다.

수신 릴레이 및 메시지 추적

수신 릴레이를 사용하는 경우 Message Tracking Details(메시지 추적 세부사항) 페이지에는 원래 외부 발신자의 IP 주소 및 평판 점수 대신 메시지에 대한 릴레이의 IP 주소 및 SenderBase Reputation 점수가 표시됩니다.

수신 릴레이 및 로깅

다음 로그 예에서는 발신자의 SenderBase Reputation 점수가 처음에 줄 1에 보고됩니다. 나중에 수신 릴레이가 처리된 후에 올바른 SenderBase Reputation 점수가 줄 5에 보고됩니다.

1	Fri Apr 28 17:07:29 2006 Info: ICID 210158 ACCEPT SG UNKNOWNLIST match nx.domain SBRS rfc1918
2	Fri Apr 28 17:07:29 2006 Info: Start MID 201434 ICID 210158
3	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 From: <joe@sender.com>

4	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 RID 0 To: <mary@example.com>
5	Fri Apr 28 17:07:29 2006 Info: MID 201434 IncomingRelay(senderdotcom): Header Received found, IP 192.192.108.1 being used, **SBRS 6.8**
6	Fri Apr 28 17:07:29 2006 Info: MID 201434 Message-ID '<7.0.1.0.2.20060428170643.0451be40@sender.com>'
7	Fri Apr 28 17:07:29 2006 Info: MID 201434 Subject 'That report...'
8	Fri Apr 28 17:07:29 2006 Info: MID 201434 ready 2367 bytes from <joe@sender.com>
9	Fri Apr 28 17:07:29 2006 Info: MID 201434 matched all recipients for per-recipient policy DEFAULT in the inbound table
10	Fri Apr 28 17:07:34 2006 Info: ICID 210158 close
11	Fri Apr 28 17:07:35 2006 Info: MID 201434 using engine: CASE spam negative
12	Fri Apr 28 17:07:35 2006 Info: MID 201434 antivirus negative
13	Fri Apr 28 17:07:35 2006 Info: MID 201434 queued for delivery

수신 릴레이 및 메일 로그

다음 예에서는 수신 릴레이 정보가 포함된 일반적인 로그 항목을 보여줍니다.

```
Wed Aug 17 11:20:41 2005 Info: MID 58298 IncomingRelay(myrelay): Header Received found, IP
 192.168.230.120 being used
```

사용된 헤더를 지정하기 위한 로그 구성

Cisco 어플라이언스는 메시지 수신 시 표시되는 헤더만 검사합니다. 따라서 로컬로 추가되었거나(예: Microsoft Exchange 헤더 등) Cisco 어플라이언스에서 메시지를 수신할 때 추가된 헤더는 처리되지 않습니다. 사용된 헤더를 확인하는 데 유용한 한 가지 방법은 사용하는 헤더를 포함하도록 AsyncOS 로깅을 구성하는 것입니다.

헤더에 대한 로깅 설정을 구성하는 방법은 전역 로깅 설정 구성, 1107 페이지를 참조하십시오.

규칙 업데이트 모니터링

라이선스 계약에 동의한 경우 Cisco Anti-Spam 및 Cisco Intelligent Multi-Scan 규칙의 최신 업데이트를 볼 수 있습니다.

단계 **1** **Security Services**(보안 서비스) > **IronPort Anti-Spam**을 선택합니다.

또는

단계 **2** **Security Services > IMS and Graymail(IMS** 및 그레이메일**)**을 선택합니다.

단계 **3** **Rule Updates(**규칙 업데이트**)** 섹션을 살펴보고 다음을 수행합니다.

하려는 작업	추가 정보
각 구성 요소에 대한 최근 업데이트 보기	업데이트가 발생하지 않았거나 서버가 구성되지 않은 경우 "Never Updated(업데이트되지 않음)"가 표시됩니다.
업데이트를 사용할 수 있는지 확인	—
업데이트를 사용할 수 있는 경우 규칙 업데이트	**Update Now(**지금 업데이트**)**를 클릭합니다.

다음에 수행할 작업

관련 주제

- 서비스 업데이트 , 945 페이지
- 프록시 서버를 통한 업데이트, 949 페이지
- 업그레이드 및 업데이트 다운로드를 위한 서버 설정 구성 , 949 페이지

안티스팸 테스트

변경 후	수행해야 할 작업	추가 정보
구성을 테스트합니다.	`X-advertisement: spam` 헤더를 사용하여 구성을 테스트합니다. Cisco Anti- Spam은 테스트 목적으로 X-header 형식이 `X-Advertisement: spam`으로 지정된 모든 메시지를 스팸으로 간주합니다.	이 헤더를 포함하여 보내는 테스트 메시지에는 Cisco Anti- Spam에 의해 플래그가 지정되며 메일 정책(안티스팸 정책 정의 , 362 페이지)에 대해 구성한 작업이 수행되도록 확인할 수 있습니다. 다음 중 한 방법으로 이 헤더를 사용합니다. • SMTP 명령을 사용하여 이 헤더와 함께 테스트 메시지를 보냅니다. 이메일을 어플라이언스에 전송하여 Cisco Anti-Spam 테스트, 385 페이지를 참조하십시오. • trace 명령을 사용하고 이 헤더를 포함합니다. 테스트 메시지를 사용하여 메일 플로우 디버깅: 추적, 1149 페이지를 참조하십시오.
안티스팸 엔진 효율성을 평가합니다.	인터넷에서 직접 라이브 메일 스트림을 사용하여 제품을 평가합니다.	피해야 할 비효율적인 평가 접근 방식의 목록은 안티 스팸 효율성을 테스트할 때 사용해서는 안 되는 방식, 386 페이지를 참조하십시오.

관련 주제

- 이메일을 어플라이언스에 전송하여 Cisco Anti-Spam 테스트, 385 페이지
- 안티 스팸 효율성을 테스트할 때 사용해서는 안 되는 방식, 386 페이지

이메일을 어플라이언스에 전송하여 Cisco Anti-Spam 테스트

시작하기 전에

안티스팸 구성 테스트: SMTP 사용 예, 385 페이지의 예를 검토합니다.

단계 1 메일 정책에서 Cisco Anti-Spam을 활성화합니다.

단계 2 해당 메일 정책에서 X-Advertisement: spam 헤더를 포함하는 테스트 이메일을 사용자에게 전송합니다.

SMTP 명령과 텔넷을 사용하여 이 메시지를 액세스할 수 있는 주소로 전송합니다.

단계 3 테스트 계정의 사서함을 확인하고 메일 정책에 대해 구성한 작업을 바탕으로 테스트 메시지가 정확하게 전달되었는지 확인합니다.

예를 들면 다음과 같습니다.

- 제목 줄이 변경되었습니까?
- 다른 사용자 지정 헤더가 추가되었습니까?
- 메시지가 대체 주소로 배달되었습니까?
- 메시지가 삭제되었습니까?

관련 주제

- 안티스팸 구성 테스트: SMTP 사용 예, 385 페이지

안티스팸 구성 테스트: SMTP 사용 예

이 예에서는 테스트 주소로 메시지를 수신하도록 메일 정책을 구성해야 하며 HAT는 테스트 연결을 허용해야 합니다.

```
# telnet IP_address_of_IronPort_Appliance_with_IronPort_Anti-Spam port

220 hostname ESMTP

helo example.com

250 hostname

mail from: <test@example.com>

250 sender <test@example.com> ok

rcpt to: <test@address>
```

```
250 recipient <test@address>
ok

data

354 go ahead

Subject: Spam Message Test


X-Advertisement: spam

spam test

.

250 Message MID accepted

221 hostname

quit
```

안티 스팸 효율성을 테스트할 때 사용해서는 안 되는 방식

IronPort Anti-Spam 및 Cisco Intelligent Multi-Scan 규칙은 활성 스팸 공격을 방지하기 위해 빠르게 추가되고 공격이 지나가면 빠르게 만료되므로 다음 방법을 사용하여 효율성을 테스트해서는 안 됩니다.

- 재전송되었거나 전달된 메일 또는 잘라내어 붙여넣은 스팸 메시지를 사용하여 평가합니다.

  적절한 헤더, 연결 IP, 서명 등이 없는 메일은 부정확한 점수를 도출합니다.

- "어려운 스팸"만 테스트합니다.

  SBRS, 차단 목록, 메시지 필터 등을 사용하여 "쉬운 스팸"을 제거하면 전반적인 탐지율이 저하됩니다.

- 다른 안티 스팸 벤더에 의해 탐지된 스팸을 재전송합니다.

- 이전 메시지를 테스트합니다.

  검사 엔진은 현재 위협 요소를 바탕으로 규칙을 빠르게 추가하고 제거합니다. 따라서 이전 메시지를 사용하여 테스트하면 부정확한 테스트 결과가 발생할 수 있습니다.

16 장

그레이메일 관리

이 장에는 다음 섹션이 포함되어 있습니다.

그레이메일 개요

그레이메일 메시지는 스팸 정의에 맞지 않는 메시지, 예를 들면 뉴스레터, 메일 리스트 서브스크립션, 소셜 미디어 알림 등입니다. 이러한 메시지는 어느 시점에는 유용했지만, 점차 가치가 줄어 이제 최종 사용자가 더 이상 수신을 원하지 않는 메시지입니다.

그레이메일과 스팸의 차이점은, 스팸은 최종 사용자가 수신을 요청하지 않은 반면 그레이메일은 최종 사용자가 특정 시점에 이메일 주소를 자발적으로 제공했다는 점입니다(예를 들어, 최종 사용자가 전자상거래 웹사이트에서 뉴스레터를 구독했거나 회의 중 특정 조직에 연락처 세부사항 제공).

Email Security Appliance의 그레이메일 관리 솔루션

Email Security Appliance의 그레이메일 관리 솔루션은 통합 그레이메일 검사 엔진 및 클라우드 기반 Unsubscribe Service(수신 거부 서비스), 이 두 가지 구성 요소로 이루어집니다.

그레이메일 관리 솔루션을 통해 조직은 다음을 수행할 수 있습니다.

- 통합 그레이메일 엔진을 사용하여 그레이메일을 식별하고 적절한 정책 제어를 적용합니다.
- 최종 사용자가 Unsubscribe Service(수신 거부 서비스)를 사용하여 원하지 않는 메시지의 수신을 거부할 수 있는 손쉬운 메커니즘을 제공합니다.

이것 외에도 그레이메일 관리 솔루션은 조직에서 다음을 제공하도록 지원합니다.

- 최종 사용자를 위한 안전한 수신 거부 옵션. 수신 거부 옵션을 가장하는 것은 널리 사용되는 피싱 기법입니다. 따라서 최종 사용자는 알 수 없는 수신 거부 링크를 클릭하는 데 일반적으로 신중을 기하게 됩니다. 그러한 시나리오에서 클라우드 기반 Unsubscribe Service(수신 거부 서비스)

는 원래 수신 거부 URL을 추출하고, URL의 평판을 확인하고, 최종 사용자 대신 수신 거부 프로세스를 수행합니다. 이렇게 하여 수신 거부 링크를 가장하는 악의적인 위협으로부터 최종 사용자를 보호합니다.

- 최종 사용자를 위한 일관된 서브스크립션 관리 인터페이스. 각 그레이메일 발신자는 사용자에게 수신 거부 링크를 표시하기 위한 서로 다른 레이아웃을 사용합니다. 사용자는 메시지 본문에서 수신 거부 링크를 찾아 수신 거부를 수행해야 합니다. 그레이메일 발신자와 상관없이 그레이메일 관리 솔루션은 사용자에게 수신 거부 링크를 표시하기 위한 공통된 레이아웃을 사용합니다.
- 관리자에게 다양한 그레이메일 범주에 대한 더 나은 가시성 제공. 그레이메일 엔진은 각 그레이메일을 세 범주로 분류하며(그레이메일 분류, 388 페이지 참조), 관리자는 그러한 범주를 기반으로 정책 제어를 설정할 수 있습니다.
- 스팸 효율성 개선

관련 주제

- 그레이메일 분류, 388 페이지

그레이메일 분류

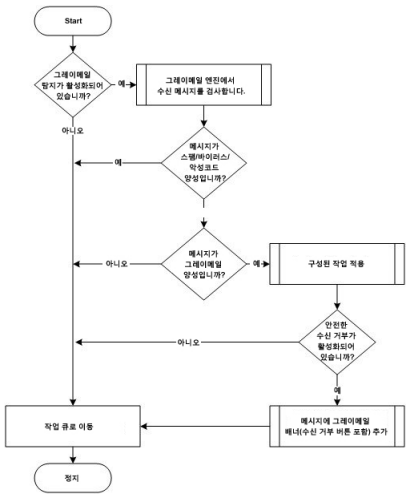
그레이메일 엔진은 각 그레이메일을 다음 범주 중 하나로 분류합니다.

- 마케팅 이메일. 전문 마케팅 그룹에서 전송하는 광고 메시지(예: 새로 출시한 제품에 대한 세부사항이 포함된 Amazon.com의 게시판)
- 소셜 네트워크 이메일. 소셜 네트워크, 데이트 웹사이트, 포럼 등에서 오는 알림 메시지. 예를 들면 다음에서 오는 경고문:
  - LinkedIn - 관심이 있을 수 있는 일자리
  - CNET 포럼 - 사용자가 게시물에 응답하는 경우
- 대량 이메일. 알 수 없는 마케팅 그룹에서 전송하는 광고 메시지(예: 기술 미디어 회사인 TechTarget의 뉴스레터)

그레이메일 관리 솔루션 작동 방식

다음 단계에서는 그레이메일 관리 솔루션의 워크플로를 설명합니다.

그림 ***27:*** 그레이메일 관리 솔루션 워크플로



워크플로

단계 **1** Email Security Appliance가 메시지를 수신합니다.

단계 **2** Email Security Appliance가 그레이메일 탐지 기능이 활성화되었는지 확인합니다. 그레이메일 탐지 기능이 활성화되었으면 3단계로 이동합니다. 그렇지 않으면 8단계로 이동합니다.

단계 **3** Email Security Appliance는 메시지가 스팸, 바이러스 또는 악성코드 양성인지 확인합니다. 양성이면 8단계로 이동합니다. 그렇지 않으면 4단계로 이동합니다.

단계 **4** Email Security Appliance는 메시지가 그레이메일인지 확인합니다. 메시지가 그레이메일이면 5단계로 이동합니다. 그렇지 않으면 8단계로 이동합니다.

단계 **5** Email Security Appliance는 삭제, 전달, 반송, 격리 등 구성된 정책 작업을 스팸 격리에 적용합니다.

단계 **6** Email Security Appliance는 안전한 수신 거부 기능이 활성화되었는지 확인합니다. 안전한 수신 거부 기능이 활성화되었으면 7단계로 이동합니다. 그렇지 않으면 8단계로 이동합니다.

단계 **7** Email Security Appliance는 메시지에 수신 거부 버튼이 있는 배너를 추가합니다. Email Security Appliance는 기존의 수신 거부 링크를 메시지 본문에 다시 작성합니다.

단계 **8** Email Security Appliance는 이메일 작업 대기열의 다음 단계를 통해 메시지를 처리합니다.

다음에 수행할 작업

수신에서 라우팅, 전달까지 시스템을 통해 이메일이 처리되는 방법에 대한 개요는 이메일 파이프라인 이해, 57 페이지를 참조하십시오.

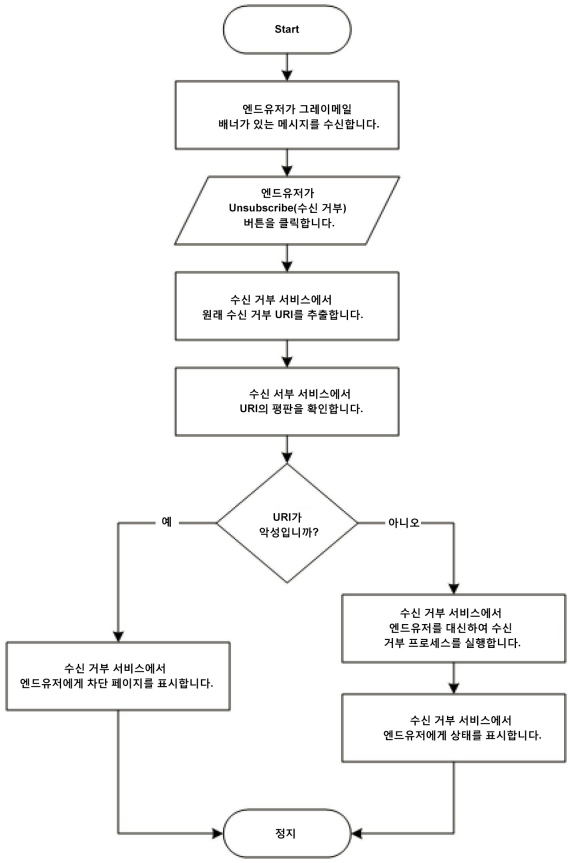
관련 주제

- 안전한 수신 거부 작동 방식, 390 페이지
- 이메일 파이프라인 이해, 57 페이지

안전한 수신 거부 작동 방식

다음 흐름도는 안전한 수신 거부 작동 방식을 보여줍니다.

그림 ***28:*** 안전한 수신 거부 워크플로



워크플로

단계 **1** 최종 사용자는 그레이메일 배너가 있는 메시지를 수신합니다.

단계 **2** 최종 사용자는 Unsubscribe(수신 거부) 링크를 클릭합니다.

단계 **3** Unsubscribe Service(수신 거부 서비스)는 원래 수신 거부 URI를 추출합니다.

단계 **4** Unsubscribe Service(수신 거부 서비스)는 URI의 평판을 확인합니다.

단계 **5** URI의 평판에 따라, Unsubscribe Service(수신 거부 서비스)는 다음 작업 중 하나를 수행합니다.

- URI가 악의적이면 Unsubscribe Service(수신 거부 서비스)는 수신 거부 프로세스를 수행하지 않고 최종 사용자에게 차단 페이지를 표시합니다.
- URI가 악의적이지 않으면 URI 유형(http 또는 mailto)에 따라 Unsubscribe Service(수신 거부 서비스)는 그레이메일 발신자에게 수신 거부 요청을 전송합니다.

- 요청이 성공적이면 Unsubscribe Service(수신 거부 서비스)는 최종 사용자에게 "Successfully unsubscribed(수신 거부 성공)" 상태를 표시합니다.
- 첫 번째 수신 거부 요청이 실패하면 Unsubscribe Service(수신 거부 서비스)는 "Unsubscribe process in progress(수신 거부 프로세스 진행 중)" 상태를 표시하고 수신 거부 상태를 추적하는 데 사용할 수 있는 URL을 제공합니다.

  최종 사용자는 나중에 이 URL을 사용하여 상태를 추적할 수 있습니다. 첫 번째 시도가 실패하면 Unsubscribe Service(수신 거부 서비스)는 4시간 동안 주기적으로 수신 거부 요청을 전송합니다.

  최종 사용자가 나중에 수신 거부 프로세스의 상태를 확인하는 경우

- 첫 번째 실패 시도로부터 1시간 내에 요청 중 하나가 성공하면, Unsubscribe Service(수신 거부 서비스)는 최종 사용자에게 "Successfully unsubscribed(수신 거부 성공)" 상태를 표시합니다.
- 첫 번째 실패 시도로부터 4시간 내에 요청이 모두 실패하면, Unsubscribe Service(수신 거부 서비스)는 최종 사용자에게 "Unable to subscribe(수신 거부 불가)" 상태를 표시하고 그레이메일을 수동으로 수신 거부하기 위해 사용할 수 있는 URL을 제공합니다.

그레이메일 탐지 및 안전한 수신 거부 구성

그레이메일 탐지 및 안전한 수신 거부 요구 사항

- 그레이메일을 탐지하려면 안티스팸 검사를 전역적으로 활성화해야 합니다. IronPort Anti-Spam, Intelligent Multi-Scan 기능 또는 Outbreak Filters 중 하나일 수 있습니다. Anti-Spam, 355 페이지의 내용을 참조하십시오.
- 안전한 수신 거부를 위해
  - 안전한 수신 거부 기능 키를 추가합니다.
  - 최종 사용자 시스템은 인터넷을 통해 클라우드 기반 Unsubscribe Service(수신 거부 서비스)에 연결할 수 있어야 합니다.

클러스터 컨피그레이션에서 그레이메일 탐지 및 안전한 수신 거부

시스템, 그룹 또는 클러스터 레벨에서 그레이메일 탐지 및 안전한 수신 거부를 활성화할 수 있습니다.

그레이메일 탐지 및 안전한 수신 거부 활성화

시작하기 전에

그레이메일 탐지 및 안전한 수신 거부 요구 사항, 391 페이지 섹션을 참조하십시오.

단계 **1** **Security Services(**보안 서비스**)** > **Detection and Safe Unsubscribe(**탐지 및 안전한 수신 거부**)**를 클릭합니다.

단계 **2** **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **3** **Enable Graymail Detection(**그레이메일 탐지 활성화**)**을 선택합니다.

단계 **4** (선택 사항) 그레이메일 발신자들이 전송하는 점점 많아지는 메시지를 검사하면서도 어플라이언스의 처리량을 최적화하려면 메시지 검사에 대한 임계값을 구성합니다.

- 어플라이언스에서 검사할 메시지의 최대 크기.
- 메시지를 검사할 때 시간 초과 대기 시간(초).

단계 **5** (선택 사항) **Enable Automatic Updates(**자동 업데이트 활성화**)**를 클릭하여 엔진의 자동 업데이트를 활성화합니다.

어플라이언스는 업데이트 서버에서 특정 엔진의 필수 업데이트를 가져왔습니다.

단계 **6** **Enable Safe Unsubscribe(**안전한 수신 거부 활성화**)**를 선택합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

CLI에서 그레이메일 탐지 및 안전한 수신 거부 전역 설정을 구성하려면 graymailconfig 명령을 사용하십시오. 자세한 내용은 *AsyncOS for Cisco Email Security Appliance*용 *CLI* 참조 설명서를 참조하십시오.

그레이메일 탐지 및 안전한 수신 거부를 위한 수신 메일 정책 구성

시작하기 전에

그레이메일 탐지 및 안전한 수신 거부 활성화, 392 페이지

단계 **1** **Mail Policies(**메일 정책**)** > **Incoming Mail Policies(**수신 메일 정책**)**를 클릭합니다.

단계 **2** 수정할 메일 정책의 **Graymail(**그레이메일**)** 열에서 링크를 클릭합니다.

단계 **3** 요구 사항에 따라 다음 옵션을 선택합니다.

- 그레이메일 탐지 활성화
- 안전한 수신 거부 활성화

- 위의 작업을 모든 메시지에 적용할지, 서명되지 않은 메시지에만 적용할지를 선택합니다.

  참고 어플라이언스는 S/MIME을 사용하여 암호화되었거나 S/MIME 서명이 포함된 메시지를 서명된 메시지로 간주합니다.

- 다양한 그레이메일 범주에 대해 수행할 작업(마케팅 이메일, 소셜 네트워크 이메일 및 대량 이메일)
  - 메시지 삭제, 전달, 반송 또는 격리(스팸 격리로)

    참고 안전한 수신 거부 옵션을 사용할 계획이면 전달 또는 격리 작업을 설정해야 합니다.

  - 메시지를 대체 호스트로 전송
  - 메시지의 제목 수정
  - 사용자 지정 헤더 추가
  - 대체 봉투 수신자에게 메시지 전송

    참고 그레이메일 양성 메시지를 대체 봉투 수신자에게 전송하는 경우 배너가 추가되지 않습니다.

  - 메시지 보관

    참고 탐지된 그레이메일만 모니터링할 계획이면 다양한 그레이메일 범주에 대한 작업을 구성하지 않고도 정책당 그레이메일 탐지를 활성화할 수 있습니다. 이 시나리오에서 Email Security Appliance는 탐지된 그레이메일에 대한 작업을 수행합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

참고 그레이메일 탐지를 위한 발신 메일 정책을 구성할 수도 있습니다. 이 시나리오에서는 안전한 수신 거부를 구성할 수 없다는 점에 유의하십시오.

CLI에서 그레이메일 탐지 및 안전한 수신 거부의 정책 설정을 구성하려면 **policyconfig** 명령을 사용하십시오. 자세한 내용은 *AsyncOS for Cisco Email Security Appliance*용 *CLI* 참조 설명서를 참조하십시오.

그레이메일 스캔 중에 추가된 **IronPort-PHdr** 헤더

IronPort-PHdr 헤더는 다음과 같은 경우 그레이메일 엔진에서 처리하는 모든 메시지에 추가됩니다.

- 그레이메일 엔진이 어플라이언스에서 전역적으로 활성화되어 있습니다.
- 특정 메일 정책에 대해 그레이메일 스캔이 활성화되어 있습니다.

참고 특정 메일 정책에 대해 그레이메일 스캔이 활성화되지 않은 경우에도 그레이메일 엔진이 어플라이언스에서 전역적으로 활성화되어 있다면 IronPort-PHdr 헤더가 모든 메시지에 추가됩니다.

IronPort-PHdr 헤더에는 인코딩된 독점 정보가 포함되어 있으며 고객이 디코딩할 수 없습니다. 이 헤더는 그레이메일 구성 문제 디버깅에 대한 추가 정보를 제공합니다.

참고 특정 메일 정책에 대해 안티 스팸 엔진 또는 보안 침해 필터가 활성화된 경우, 해당 특정 메일 정책을 통과하는 모든 메시지에 IronPort-PHdr 헤더가 추가됩니다.

메시지 필터를 사용하여 그레이메일 작업 우회

특정 메시지에 그레이메일 작업을 적용하지 않으려면 다음 메시지 필터를 사용하여 그레이메일 작업을 우회할 수 있습니다.

메시지 필터 작업	설명
skip-marketingcheck	마케팅 이메일에서 작업 우회
skip-socialcheck	소셜 네트워크 이메일에서 작업 우회
skip-bulkcheck	대량 이메일에서 작업 우회

다음 예에서는 "private_listener" 리스너에서 수신하는 메시지가 소셜 네트워크 이메일에 대한 그레이메일 작업을 우회하도록 지정합니다.

```
internal_mail_is_safe:
if (recv-listener == 'private_listener')
{
skip-socialcheck
();
}
```

그레이메일 모니터링

다음 보고서를 사용하여 탐지된 그레이메일에 대한 데이터를 볼 수 있습니다.

보고서	다음 그레이메일 데이터 포함	추가 정보
Overview(개요) 페이지 > Incoming Mail Summary(수신 메일 요약)	각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.	Overview(개요) 페이지, 799 페이지

보고서	다음 그레이메일 데이터 포함	추가 정보
Incoming Mail(수신 메일) 페이지 > Top Senders by Graymail Messages(그레이메일 메시지별 상위 전송자)	상위 그레이메일 발신자.	Incoming Mail(수신 메일) 페이지, 802 페이지
Incoming Mail(수신 메일) 페이지 > Incoming Mail Details(수신 메일 세부사항)	모든 IP 주소, 도메인 이름 또는 네트워크 소유자에 대한 각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.	
Incoming Mail(수신 메일) 페이지 > Incoming Mail Details(수신 메일 세부사항) > Sender Profile(발신자 프로필)(드릴다운 보기)	지정된 IP 주소, 도메인 이름 또는 네트워크 소유자에 대한 각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.	
Internal Users(내부 사용자) 페이지 > Top Users by Graymail(그레이메일별 상위 사용자)	그레이메일을 수신하는 상위 최종 사용자.	Internal Users(내부 사용자) 페이지, 811 페이지
Internal Users(내부 사용자) 페이지 > User Mail Flow Details(사용자 메일 플로우 세부사항)	모든 사용자에 대한 각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.	
Internal Users(내부 사용자) 페이지 > User Mail Flow Details(사용자 메일 플로우 세부사항) > Internal User(내부 사용자)(드릴다운 보기)	특정 사용자에 대한 각 그레이메일 범주(마케팅, 소셜 및 대량)별 수신 그레이메일 메시지의 수 및 전체 그레이메일 메시지의 수.	

AsyncOS 9.5 이상으로 업그레이드한 후 메일 정책에 대한 안티스팸 설정에서 Marketing Email Scanning(마케팅 이메일 검사)을 활성화한 경우 다음에 유의하십시오.

- 마케팅 메시지 수는 업그레이드 전후에 탐지된 마케팅 메시지의 합계입니다.
- 총 그레이메일 메시지 수에는 업그레이드 이전에 탐지된 마케팅 메시지의 수가 포함되지 않습니다.
- 총 시도된 메시지 수에는 또한 업그레이드 전에 탐지된 마케팅 메시지의 수가 포함됩니다.

그레이메일 규칙 업데이트

서비스 업데이트를 활성화한 경우 Cisco 업데이트 서버에서 그레이메일 관리 솔루션에 대한 검사 규칙이 검색됩니다. 그러나 일부 시나리오에서는(예: 자동 서비스 업데이트를 비활성화했거나 자동 서비스 업데이트가 작동하지 않는 경우) 그레이메일 규칙을 수동으로 업데이트할 수도 있습니다.

그레이메일 규칙을 수동으로 업데이트하려면 다음 중 하나를 수행합니다.

- 웹 인터페이스에서 **Security Service**(보안 서비스) > **IMS and Graymail**(**IMS** 및 그레이메일) 페이지로 이동하여 **Update Now**(지금 업데이트)를 클릭합니다.
- CLI,에서 graymailupdate 명령을 실행합니다.

기존 그레이메일 규칙에 대해 자세히 알아보려면 웹 인터페이스에서 **IMS and Graymail(IMS** 및 그레이메일**)** 페이지의 **Rule Updates(**규칙 업데이트**)** 섹션을 참고하거나 CLI에서 graymailstatus 명령을 사용하십시오.

최종 사용자를 위한 수신 거부 페이지 모양 사용자 지정

최종 사용자가 수신 거부 링크를 클릭하면 Unsubscribe Service(수신 거부 서비스)에서 수신 거부 프로세스의 상태를 나타내는, Cisco 브랜드의 Unsubscribe(수신 거부) 페이지를 표시합니다(안전한 수신 거부 작동 방식, 390 페이지 참조). **Security Services(**보안 서비스**)** > **Block Page Customization(**페이지 사용자 지정 차단**)**을 사용하여 Unsubscribe(수신 거부) 페이지의 모양을 사용자 지정하고 조직의 브랜드(예: 회사 로고, 연락처 정보 등)를 표시할 수 있습니다. 자세한 내용은 엔드 유저에게 사이트가 악의적인지 여부를 표시하는 알림 맞춤화 , 431 페이지 섹션을 참조하십시오.

최종 사용자 허용 리스트

조직의 최종 사용자가 자체 이메일 계정에 대한 허용 리스트를 구성한 경우, 허용 리스트의 발신자가 보내는 그레이메일 메시지는 그레이메일 검사 엔진에서 검사되지 않습니다. 허용 리스트에 대한 자세한 내용은 허용 목록 및 차단 목록을 사용하여 발신자 기준으로 이메일 전달 제어 , 873 페이지 섹션을 참조하십시오.

로그 보기

그레이메일 탐지 및 안전한 수신 거부 정보는 다음 로그에 게시됩니다.

- **Graymail Engine Logs(**그레이메일 엔진 로그**)**. 그레이메일 엔진, 상태, 컨피그레이션 등에 대한 정보를 포함합니다. 대부분의 정보는 Info(정보) 또는 Debug(디버그) 레벨입니다.
- **Graymail Archive(**그레이메일 아카이브**)**. 보관된 메시지(검사되고 "메시지 아카이브" 작업과 연결된 메시지)를 포함합니다. 형식은 mbox 형식의 로그 파일입니다.
- **Mail Logs(**메일 로그**)**. 안전한 수신 거부를 위한 그레이메일 탐지 및 배너 추가에 대한 정보를 포함합니다. 대부분의 정보는 Info(정보) 또는 Debug(디버그) 레벨입니다.

그레이메일 탐지 및 안전한 수신 거부 트러블슈팅

안전한 수신 거부를 수행할 수 없음

문제

엔드 유저가 Unsubscribe(수신 거부) 링크를 클릭하면 "Unable to unsubscribe from...(...에서 수신 거부할 수 없음)" 메시지가 표시됩니다.

솔루션

이 문제는 Unsubscribe Service(수신 거부 서비스)에서 사용자 대신 안전한 수신 거부를 수행할 수 없을 경우 발생할 수 있습니다. 다음은 Unsubscribe Service(수신 거부 서비스)에서 안전한 수신 거부를 수행할 수 없는 몇 가지 일반적인 시나리오입니다.

- 수신 거부 URI 또는 mailto 주소가 잘못됨
- 웹사이트에서 수신 거부할 최종 사용자의 Credential을 요구함
- 웹사이트에서 최종 사용자에게 이메일 계정에 로그인하여 수신 거부 요청을 확인하도록 요구함
- 웹사이트에서 captcha를 해결하도록 요구했지만 Unsubscribe Service(수신 거부 서비스)에서 captcha를 해결하지 못함
- 웹사이트에서 상호 작용 수신 거부를 요구함

최종 사용자는 수동으로 수신 거부하려면 수신 거부 페이지 하단에 제공되는 URL을 사용할 수 있습니다.

17 장

신종 바이러스 필터(Outbreak Filter)

이 장에는 다음 섹션이 포함되어 있습니다.

Outbreak Filter 개요

Outbreak Filter는 큰 규모의 바이러스 전파 확산 및 좀 더 작은 규모의 비 바이러스형 공격(예: 피싱 스캠 및 악성코드 배포)으로부터 네트워크를 보호합니다. 데이터가 수집되고 소프트웨어 업데이트가 게시될 때까지는 새로운 악성코드 전파 확산을 탐지할 수 없는 대부분의 악성코드 차단 보안 소프트웨어와는 달리, Cisco는 악성코드가 확산되는 동안 데이터를 수집하고 해당 메시지가 사용자에게 도달하지 못하도록 업데이트된 정보를 실시간으로 Email Security Appliance에 전송합니다.

Cisco는 전역 트래픽 패턴을 사용하여, 수신 메시지가 안전한지 아니면 악성코드 전파 확산의 일부인지를 판단하는 규칙을 개발합니다. 악성코드 전파 확산의 일부일 수 있는 메시지는 Cisco의 업데이트된 전파 확산 정보를 기반으로 안전하다고 판단될 때까지 또는 Sophos와 McAfee에서 새로운 안티바이러스 정의를 게시할 때까지 격리됩니다.

소규모 비 바이러스성 공격에 사용되는 메시지는 합법적으로 보이는 디자인, 수신자의 정보, 그리고 피싱 및 악성코드 웹사이트로 이동하는 사용자 지정 URL을 사용합니다. 이러한 웹사이트는 단기간만 온라인 상태이고 웹 보안 서비스에 알려져 있지 않습니다. Outbreak Filter는 메시지 내용을 분석하고, 이 유형의 비 바이러스성 공격을 탐지하기 위해 URL 링크를 검색합니다. Outbreak Filter는 URL을 재작성하여 웹 보안 프록시를 통해 잠재적으로 유해한 웹사이트로 트래픽을 리디렉션할 수 있습니다. 이로써 액세스하려는 웹사이트가 악성 사이트일 수 있음을 경고하거나 해당 웹사이트를 완전히 차단합니다.

Outbreak Filter 작동 방식

관련 주제

메시지 지연, 리디렉션 및 수정

Outbreak Filter 기능은 세 가지 전략을 사용하여 악성코드 전파 확산으로부터 사용자를 보호합니다.

- 지연. Outbreak Filter는 바이러스 전파 확산 또는 비 바이러스성 공격의 일부일 수 있는 메시지를 격리합니다. 격리된 상태에서 어플라이언스는 업데이트된 악성코드 전파 확산 정보를 수신하고 메시지를 다시 검사하여 공격의 일부인지 여부를 확인합니다.
- 리디렉션. Outbreak Filter는 비 바이러스성 공격 메시지의 URL을 재작성하여, 수신자가 링크된 웹사이트 중 한 곳에 액세스하려고 할 때 Cisco 웹 보안 프록시를 통해 수신자를 리디렉션합니다. 웹사이트가 여전이 운영되는 경우 프록시는 웹사이트에 악성코드가 포함되어 있을 수 있음을 사용자에게 경고하는 시작 화면을 표시합니다. 또는 웹사이트가 오프라인이 된 경우 오류 메시지를 표시합니다. URL 리디렉션에 대한 자세한 내용은 URL 리디렉션, 403 페이지 섹션을 참조하십시오.
- 수정. Outbreak Filter는 비 바이러스성 위협 메시지의 URL을 재작성하는 것 외에도, 메시지의 제목을 수정하고 메시지 본문 위에 면책조항을 추가하여 메시지 내용에 대해 사용자에게 경고할 수 있습니다. 자세한 내용은 메시지 수정, 404 페이지를 참조하십시오.

위협 범주

Outbreak Filter 기능은 메시지 기반 악성코드 전파 확산의 다음 두 가지 범주에서 보호를 제공합니다. 바이러스 전파 확산 범주의 메시지에는 첨부 파일에 전에 본 적이 없는 바이러스가 포함되어 있고, 비 바이러스성 위협 범주의 메시지에는 외부 웹사이트에 대한 링크를 통해 피싱 시도, 스캠 및 악성코드 배포가 포함되어 있습니다.

기본적으로 Outbreak Filter 기능은 수신 및 발신 메시지에서 악성코드 전파 확산 중 바이러스 가능성을 검사합니다. 어플라이언스에서 안티스팸 검사를 활성화하면 바이러스 전파 확산 외에 비 바이러스성 위협에 대한 검사도 활성화할 수 있습니다.

참고 Outbreak Filter에서 비 바이러스성 위협을 검사할 수 있으려면 어플라이언스에 Anti-Spam 또는 Intelligent Multi-Scan에 대한 기능 키가 필요합니다.

관련 주제

- Virus Outbreaks(바이러스 침투), 401 페이지
- 피싱, 악성코드 배포 및 기타 비 바이러스성 위협, 401 페이지

Virus Outbreaks(바이러스 침투)

Outbreak Filter 기능은 바이러스 전파 확산을 처리하기 위한 유리한 출발점을 제공합니다. 전에 본 적이 없는 바이러스가 포함된 첨부 파일의 메시지 또는 기존 바이러스의 변종이 사설 네트워크 및 인터넷을 통해 빠르게 퍼질 때 전파 확산이 이루어집니다. 신종 바이러스 또는 변종이 인터넷에 나타나는 경우 가장 중요한 시기는 바이러스가 릴리스되는 때와 안티바이러스 공급업체가 업데이트된 바이러스 정의를 출시하는 때 사이입니다. 악성코드나 바이러스의 전파를 억제하는 데에는 두세 시간 정도라도 사전 통지가 매우 중요합니다. 이 취약성 기간에 새로 발견된 바이러스가 전체적으로 전파되어 이메일 인프라를 중단시킬 수 있습니다.

피싱, 악성코드 배포 및 기타 비 바이러스성 위협

비 바이러스성 위협이 포함된 메시지는 합법적인 소스에서 온 메시지처럼 보이도록 디자인되며 종종 소수의 수신자에게 전송됩니다. 이러한 메시지는 신뢰할 수 있는 메시지처럼 보이기 위해 다음 특성 중 하나 이상을 가지고 있습니다.

- 수신자의 연락처 정보.
- 합법적인 소스(예: 소셜 네트워크 및 온라인 소매점)에서 온 이메일을 가장하도록 디자인된 HTML 콘텐츠.
- 새 IP 주소가 있고 단기간만 온라인 상태인 웹사이트를 가리키는 URL. 즉, 이메일 및 웹 보안 서비스에서 해당 웹사이트가 악성 사이트인지 판단하기 위한 정보가 충분하지 않습니다.
- URL 단축 서비스를 가리키는 URL.

이 모든 특성 때문에 해당 메시지를 스팸으로 탐지하기가 어렵습니다. Outbreak Filter 기능은 사용자가 악성코드를 다운로드하거나 의심스런 새 웹사이트에 개인 정보를 제공하지 않도록 이러한 비 바이러스성 위협에 대해 멀티레이어 방어를 제공합니다.

CASE는 메시지에서 URL을 발견하면 해당 메시지를 기존의 Outbreak 규칙과 비교하여, 메시지가 소규모 비 바이러스성 전파 확산의 일부인지 확인한 다음 위협 레벨을 할당합니다. 위협 레벨에 따라 Email Security Appliance는 더 많은 위협 데이터를 수집할 수 있을 때까지 전달을 지연하고, 수신자가 웹사이트에 액세스하려고 시도하면 메시지의 URL을 재작성하여 수신자를 Cisco 웹 보안 프록시로 리디렉션합니다. 프록시는 해당 웹사이트에 악성코드가 포함되어 있을 수 있음을 사용자에게 경고하는 시작 페이지를 표시합니다.

Cisco Security Intelligence Operations

Cisco SIO(Security Intelligence Operations)는 글로벌 위협 정보, 평판 기반 서비스 및 고급 분석을 Cisco 보안 어플라이언스에 연결하여 더욱 빠른 응답 시간과 함께 더욱 강력한 보호를 제공하는 보안 에코 시스템입니다.

SIO는 세 가지 구성 요소로 이루어집니다.

- SenderBase. 세계 최대 규모의 위협 모니터링 네트워크 및 취약성 데이터베이스
- TOC(Threat Operations Center). SenderBase에서 수집한 실행 가능한 인텔리전스를 추출하는 보안 분석 및 자동화 시스템의 글로벌 팀
- 동적 업데이트. 악성코드 전파 확산이 발생하면 어플라이언스로 자동 전달되는 실시간 업데이트

SIO는 전역 SenderBase 네트워크의 실시간 데이터를 일반적인 트래픽 패턴과 비교하여, 전파 확산을 예측하는 데 도움이 되는 이상 징후를 식별합니다. TOC는 데이터를 검토하고 가능한 전파 확산의 위협 레벨을 발급합니다. Email Security Appliance는 업데이트된 위협 수준 및 Outbreak 규칙을 다운로드하여 Outbreak 격리에 이미 있는 메시지 검사는 물론 수신 및 발신 메시지 검사에도 사용합니다.

현재 바이러스 전파 확산에 대한 정보는 다음 SenderBase 웹사이트에서 찾을 수 있습니다.

http://www.senderbase.org/

SIO 웹사이트는 스팸, 피싱 및 악성코드 배포 시도를 포함하여 현재 비 바이러스성 위협의 목록을 제공합니다.

http://tools.cisco.com/security/center/home.x

Context Adaptive Scanning Engine

Outbreak Filter는 Cisco의 고유한 CASE(Context Adaptive Scanning Engine)로 지원됩니다. CASE는 메시징 위협의 실시간 분석을 기반으로 자동으로 그리고 정기적으로 조정되는 100,000개가 넘는 적응형 메시지 특성을 활용합니다.

바이러스 전파 확산에 대해 CASE는 메시지 내용, 컨텍스트 및 구조를 분석하여 적응형 규칙 트리거 등을 정확히 판단합니다. CASE는 SIO에서 게시하는 실시간 Outbreak 규칙과 적응형 규칙을 결합하여 모든 메시지를 평가하고 고유한 위협 레벨을 할당합니다.

비 바이러스성 위협을 탐지하기 위해 CASE는 메시지에서 URL을 검사하고, 하나 이상의 URL이 발견되면 SIO의 Outbreak 규칙을 사용하여 메시지의 위협 레벨을 평가합니다.

메시지의 위협 레벨을 기반으로 CASE는 전파 확산을 방지하기 위해 메시지를 격리할 기간을 권장합니다. CASE는 또한 SIO의 업데이트된 Outbreak 규칙을 기반으로 메시지를 재평가할 수 있도록 재검사 간격을 결정합니다. 메시지가 격리되어 있는 동안 위협 레벨이 높을수록 메시지를 더 자주 재검사합니다.

CASE는 또한 격리에서 릴리스될 때 메시지를 재검사합니다. 재검사 시 CASE에서 스팸이라고 또는 바이러스가 포함되어 있다고 판단하면 메시지가 다시 격리될 수 있습니다.

CASE에 대한 자세한 내용은 Cisco Anti-Spam: 개요 , 358 페이지 섹션을 참조하십시오.

메시지 지연

전파 확산 또는 이메일 공격이 발생하는 때와 소프트웨어 공급업체가 업데이트된 규칙을 릴리스하는 때 사이가 네트워크와 사용자가 가장 취약한 시기입니다. 오늘날의 바이러스는 전역적으로 전파될 수 있으며 악성 웹사이트는 이 기간에 악성코드를 전달하거나 사용자의 민감 정보를 수집합니다. Outbreak Filter는 제한된 기간 동안 의심스런 메시지를 격리하고, Cisco 및 기타 공급업체에서 새 전파 확산을 조사할 시간을 제공함으로써 사용자와 네트워크를 보호합니다.

바이러스 전파 확산이 발생하면 업데이트된 Outbreak 규칙 및 새로운 안티바이러스 서명에서 이메일 첨부 파일이 바이러스가 아니라고 또는 깨끗하다고 입증할 때까지 첨부 파일이 있는 의심스런 메시지는 격리됩니다.

소규모 비 바이러스성 위협에는 웹 보안 서비스에 의한 탐지를 피하기 위해 단기간만 온라인 상태일 수 있는 또는 중간에 신뢰할 수 있는 웹사이트를 넣어 웹 보안을 회피하기 위한 URL 단축 서비스를 사용하는 악성 웹사이트에 대한 URL이 포함되어 있습니다. 위협 레벨 임계값을 충족하는 URL이 포함된 메시지를 격리함으로써 CASE에서는 SIO의 업데이트된 Outbreak 규칙을 기반으로 메시지 내용을 재평가할 기회를 갖게 되고, 해당 메시지는 연결된 웹사이트가 오프라인이 되거나 웹 보안 솔루션에 의해 차단될 때까지 격리에 남아 있게 됩니다.

Outbreak Filter가 의심스런 메시지를 격리하는 방법에 대한 자세한 내용은 동적 격리, 408 페이지 섹션을 참조하십시오.

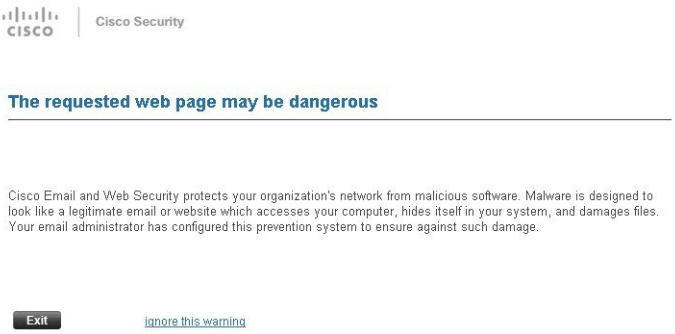
URL 리디렉션

CASE는 Outbreak Filter 단계에서 메시지를 검사할 때 메시지 본문에서 다른 의심스런 내용은 물론 URL도 검사합니다. CASE는 게시된 Outbreak 규칙을 사용하여 메시지가 위협인지를 평가한 다음 적절한 위협 레벨로 메시지에 점수를 매깁니다. 위협 레벨에 따라 Outbreak Filter는 Cisco 웹 보안 프록시로 리디렉션하도록 모든 URL을 재작성하고(우회 도메인을 가리키는 URL 제외) 좀 더 큰 전파 확산의 일부인 것으로 보일 경우 TOC에서 웹사이트에 대해 자세히 알아볼 수 있도록 메시지 전달을 지연하여 수신자를 보호합니다. 신뢰할 수 있는 도메인에 대한 URL 우회에 대한 자세한 내용은 URL 재작성 및 도메인 우회, 418 페이지 섹션을 참조하십시오.

Email Security Appliance에서 메시지를 릴리스하고 전달한 후 수신자가 웹사이트에 액세스하려고 시도하면 Cisco 웹 보안 프록시를 통해 리디렉션됩니다. 이는 Cisco에서 호스트하는 외부 프록시로서, 웹사이트가 여전히 운영 중일 경우 웹사이트가 위험할 수 있음을 사용자에게 경고하는 시작 화면을 표시합니다. 웹사이트가 오프라인으로 전환된 경우 시작 화면에 오류 메시지가 표시됩니다.

수신자가 메시지의 URL을 클릭하면 Cisco 웹 보안 프록시에서는 사용자의 웹 브라우저에 메시지 내용에 대해 경고하는 시작 화면을 표시합니다. 다음 그림은 시작 화면 경고의 예를 보여줍니다. 수신자는 **Ignore this warning**(이 경고 무시)을 클릭하여 웹사이트에서 계속 진행하거나 **Exit**(종료)를 클릭하여 브라우저를 안전하게 닫을 수 있습니다.

그림 ***29: Cisco*** 보안 시작 화면 경고***(proxy_splash_screen)***



Cisco 웹 보안 프록시에 액세스하는 유일한 방법은 메시지에 있는 재작성된 URL을 통해서입니다. 웹 브라우저에 URL을 입력하는 방식으로는 프록시에 액세스할 수 없습니다.

참고 이 시작 화면의 모양을 사용자 지정하고 조직의 브랜드(예: 회사 로고, 연락처 정보 등)를 표시할 수 있습니다. 엔드 유저에게 사이트가 악의적인지 여부를 표시하는 알림 맞춤화 , 431 페이지를 참조하십시오.

팁 의심스런 스팸 메시지의 모든 URL을 Cisco Web Security 프록시 서비스로 리디렉션하는 방법은 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예 , 366 페이지 섹션을 참조하십시오.

메시지 수정

Outbreak Filter 기능은 비 바이러스성 위협 메시지의 메시지 본문을 수정하여 URL을 재작성하는 것은 물론, 메시지가 위협으로 의심된다는 내용을 사용자에게 알립니다. Outbreak Filter 기능은 제목 헤더를 수정하고 메시지 본문 위에 메시지 내용에 대한 면책조항을 추가할 수 있습니다. 자세한 내용은 메시지 수정, 417 페이지를 참조하십시오.

위협 면책조항은 Mail Policies(메일 정책) > Text Resources(텍스트 리소스) 페이지에서 Disclaimer(면책조항) 템플릿을 사용하여 만들 수 있습니다. 자세한 내용은 텍스트 리소스 관리 개요, 622 페이지를 참조하십시오.

규칙 유형: 적응 및 **Outbreak**

잠재적인 전파 확산을 탐지하기 위해 Outbreak Filter에서는 Adaptive(적응) 및 Outbreak(전파 확산), 이 두 가지 유형의 규칙을 사용합니다. Outbreak Filter 기능은 이 두 가지 규칙 집합을 사용하여 특별한 전파 확산에 대해 필터가 고도로 집중할 수 있도록 하는 위협 탐지를 위한 최고의 효율성과 가장 집중된 기준을 제공합니다. Outbreak Filter 규칙과 작업은 다른 사용자에게는 표시되지 않고 관리자에게만 표시되며, 격리된 메시지에 즉시 액세스하여 격리된 이유를 제공합니다.

관련 주제

- 적응 규칙, 405 페이지
- 신종 바이러스 규칙, 405 페이지

신종 바이러스 규칙

Outbreak 규칙은 Cisco Security Intelligence Operations의 일부인 Cisco TOC(Threat Operations Center)에 의해 생성되며, 첨부 파일 형식만이 아니라 메시지 전체에 집중합니다. Outbreak 규칙은 SenderBase 데이터(실시간 및 과거 트래픽 데이터)와 첨부 파일 형식, 파일 이름 키워드, 안티바이러스 엔진 업데이트 등 임의의 메시지 파라미터 조합을 사용하여 전파 확산을 실시간으로 파악하여 차단합니다. Outbreak 규칙에는 GUI의 다양한 장소(예: Outbreak 격리)에 있는 규칙을 참조하는 데 사용되는 고유한 ID가 지정됩니다.

그런 다음 전역 SenderBase 네트워크의 실시간 데이터를 이 기본 정보와 비교하여 전파 확산을 예측하는 데 도움이 되는 이상 징후를 식별합니다. TOC는 데이터를 검토하고 위협 지표 또는 위협 레벨을 발급합니다. 위협 수준은 0(위협 없음)에서 5(매우 위험) 사이의 숫자 값으로, Cisco 고객에 의해 다른 게이트웨이 방어가 널리 구축되지 않은 상태에서 메시지가 위협일 가능성을 측정합니다(자세한 내용은 위협 레벨, 406 페이지 참고). 위협 레벨은 TOC에 의해 Outbreak 규칙으로서 게시됩니다.

Outbreak 규칙에서 결합할 수 있는 몇 가지 특성의 예는 다음과 같습니다.

- 파일 형식, 파일 형식과 크기, 파일 형식과 파일 이름 키워드 등
- 파일 이름 키워드와 파일 크기
- 파일 이름 키워드
- 메시지 URL
- 메시지 이름과 Sophos IDE

적응 규칙

적응 규칙은 메시지 특성을 알려진 바이러스 전파 확산 메시지의 특성과 정확히 비교하는 CASE 내 규칙 집합입니다. 이러한 규칙은 광범위한 바이러스 모음 내에서 알려진 위협 메시지와 알려진 양호한 메시지를 연구한 후 생성됩니다. 이 모음이 평가되는 빈도로 적응 규칙도 업데이트됩니다. 적응 규칙은 기존의 Outbreak 규칙을 보충하여 전파 확산 메시지를 상시 탐지합니다. Outbreak 규칙은 잠재적인 전파 확산이 발생할 때 가동되지만, 적응 규칙(Adaptive Rules)은 활성화된 후 "상시" 가동되어 완전한 이상 징후가 전역적으로 형성되기 전에 로컬에서 전파 확산 메시지를 포착합니다. 또한 적응 규칙은 이메일 트래픽과 구조의 작고 미묘한 변화에 지속적으로 반응하며 고객에게 업데이트된 보호 기능을 제공합니다.

Outbreaks

Outbreak Filter 규칙은 기본적으로 이메일 메시지 및 첨부 파일의 특성 집합(예: 파일 크기, 파일 형식, 파일 이름, 메시지 내용 등)과 관련된 위협 레벨(예: 4)입니다. 예를 들어, Cisco SIO에서 크기가 143킬로바이트이고 파일 이름에 특정 키워드(예: "hello")가 포함된 .exe 첨부 파일이 있는 의심스런 이메일 메시지가 점점 증가하는 것을 발견합니다. 이 기준과 일치하는 메시지에 대한 위협 레벨을 높이는 Outbreak 규칙이 게시됩니다. 어플라이언스에서는 기본적으로 새로 게시된 Outbreak 및 적응 규칙을 5분마다 확인하고 다운로드합니다(Outbreak Filter 규칙 업데이트, 414 페이지 참조). 적응 규칙은

Outbreak 규칙보다 덜 자주 업데이트됩니다. 사용자는 어플라이언스에서 의심스런 메시지를 격리하기 위한 임계값을 설정합니다. 메시지에 대한 위협 레벨이 격리 임계값과 같거나 크면 메시지가 *Outbreak(*보안 위협*)* 격리 영역으로 전송됩니다. 의심스런 메시지에 있는 URL을 재작성하기 위해 비 바이러스성 위협 메시지를 수정하거나 메시지 본문 상단에 알림을 추가하기 위한 임계값을 설정할 수도 있습니다.

위협 레벨

다음 표에서는 다양한 레벨 각각에 대한 기본적인 지침 또는 정의를 제공합니다.

레벨	리스크	의미
0	None	메시지가 위협일 위험이 없습니다.
1	Low	메시지가 위협일 위험이 낮습니다.
2	Low/Medium	메시지가 위협일 위험이 낮음에서 중간입니다. 위협이 "의심"됩니다.
3	Medium	메시지가 확인된 전파 확산의 일부이거나 내용이 위협일 위험이 중간에서 높음입니다.
4	High	메시지가 대규모 전파 확산의 일부로서 확인되었거나 내용이 매우 위험합니다.
5	Extreme	메시지 내용이 매우 대규모인 전파 확산 또는 대규모의 매우 위험한 전파 확산의 일부로 확인되었습니다.

위협 수준 및 신종 바이러스 규칙에 대한 자세한 내용은 Outbreak Filter 규칙, 414 페이지 항목을 참고하십시오.

관련 주제

- 격리 위협 레벨 임계값 설정에 대한 지침, 406 페이지
- 컨테이너: 특정 규칙 및 상시 규칙, 407 페이지

격리 위협 레벨 임계값 설정에 대한 지침

격리 위협 레벨 임계값을 통해 관리자는 의심스런 메시지를 어느 정도 적극적으로 격리할지를 설정할 수 있습니다. 낮은 설정(1 또는 2)은 좀 더 적극적이며 메시지를 더 많이 격리합니다. 반대로, 높은 설정(4 또는 5)은 덜 적극적이며 악성코드일 가능성이 매우 높은 메시지만 격리합니다.

동일한 임계값이 바이러스 전파 확산 및 비 바이러스 위협에 모두 적용되지만, 바이러스 공격 및 기타 위협에는 다른 격리 유지 시간을 지정할 수 있습니다. 자세한 내용은 동적 격리, 408 페이지를 참조하십시오.

Cisco에서는 기본값 3을 권장합니다.

컨테이너: 특정 규칙 및 상시 규칙

컨테이너 파일은 압축된(.zip) 아카이브와 같이 다른 파일을 포함하는 파일입니다. TOC는 아카이브 파일 내 특정 파일을 다루는 규칙을 게시할 수 있습니다.

예를 들어 TOC에서 .exe 파일이 포함된 .zip 파일로 이루어진 바이러스 전파 확산을 식별하면 .zip 파일 내 .exe 파일(.zip(exe))에 대한 위협 레벨을 설정하는 특정 Outbreak 규칙이 게시되지만, .zip 파일 내 포함된 다른 파일 형식(예: .txt 파일)에 대해서는 특정 위협 레벨이 설정되지 않습니다. 두 번째 규칙(.zip(*))이 해당 컨테이너 파일 형식 내 다른 모든 파일 형식을 다룹니다. 컨테이너에 대한 상시(Always) 규칙은 컨테이너 내부의 파일 형식과 상관없이 항상 메시지의 위협 레벨 계산에 사용됩니다. 모든 컨테이너 유형이 위험한 것으로 알려진 경우 SIO에서 상시 규칙을 게시합니다.

표 ***37:*** 대체 규칙 및 위협 레벨 점수

Outbreak 규칙	위협 수준	설명
.zip(exe)	4	이 규칙은 .zip 파일 내 .exe 파일에 대해 위협 레벨 4를 설정합니다.
.zip(doc)	0	이 규칙은 .zip 파일 내 .doc 파일에 대해 위협 레벨 0을 설정합니다.
zip(*)	2	이 규칙은 포함된 파일 형식과 상관없이 모든 .zip 파일에 대해 위협 레벨 2를 설정합니다.

Outbreak Filter 기능 작동 방식

어플라이언스에서 처리될 때 이메일 메시지는 "이메일 파이프라인"이라는 일련의 단계를 거치게 됩니다(이메일 파이프라인에 대한 자세한 내용은 이메일 파이프라인 이해, 57 페이지 참조). 안티스팸과 안티바이러스 검사 엔진이 해당 메일 정책에 대해 활성화된 경우, 이메일 파이프라인을 거치는 동안 메시지는 그러한 엔진도 통과합니다. 다시 말해, 알려진 스팸이나 인지된 바이러스가 포함된 메시지는 안티스팸 및 안티바이러스를 기반으로 메일 스트림에서 이미 제거되므로(삭제 또는 격리) Outbreak Filter 기능에 의해 검사되지 않습니다. 따라서 Outbreak Filter 기능에 도달한 메시지는 표시된 스팸과 바이러스가 없는 상태입니다. Outbreak Filter에 의해 격리된 메시지는 격리에서 릴리스되고 CASE에서 재검사될 때 업데이트된 스팸 규칙 및 바이러스 정의를 기반으로 스팸인 것으로 또는 바이러스를 포함한 것으로 표시될 수 있습니다.

참고 필터 또는 엔진이 비활성화되어 안티스팸 및 안티바이러스 검사를 건너뛰는 메시지도 여전히 Outbreak Filter에 의해 검사됩니다.

관련 주제

- 메시지 점수 매기기, 408 페이지
- 동적 격리, 408 페이지

메시지 점수 매기기

신종 바이러스 공격 또는 비 바이러스성 위협이 릴리스되면 아직 그러한 위협을 인식할 수 있는 안티바이러스 또는 안티스팸이 없으므로 Outbreak Filter 기능의 진가가 발휘됩니다. 게시된 Outbreak 및 적응 규칙을 사용하여 CASE에서 수신 메시지를 검사하고 점수를 매깁니다(규칙 유형: 적응 및 Outbreak, 404 페이지 참조). 메시지 점수는 메시지의 위협 레벨에 상응합니다. 메시지와 일치하는 규칙(있는 경우)을 기반으로 CASE는 해당 위협 레벨을 할당합니다. 연결된 위협 레벨이 없으면(메시지가 규칙과 일치하지 않으면) 해당 메시지에는 위협 레벨 0이 할당됩니다.

계산이 완료되면 Email Security Appliance는 해당 메시지의 위협 레벨이 격리 또는 메시지 수정 임계값을 충족 또는 초과하는지를 점검하고, 메시지를 격리하거나 URL을 재작성합니다. 위협 레벨이 임계값 미만이면 파이프라인에서 추가 처리 과정을 거치게 됩니다.

또한 CASE는 최신 규칙을 기준으로 기존의 격리된 메시지를 재평가하여 메시지의 최신 위협 레벨을 결정합니다. 따라서 전파 확산과 일관된 위협 레벨을 가지고 있는 메시지만 격리에 남아 있고, 더 이상 위협이 아닌 메시지는 자동 재평가 후 격리를 벗어나게 됩니다.

적응 규칙의 점수 하나(또는 여러 적응 규칙이 적용된 경우 최고 점수) 및 Outbreak 규칙의 점수 하나(또는 여러 Outbreak 규칙이 적용된 경우 최고 점수)와 같이 하나의 전파 확산 메시지에 대해 점수가 여러 개인 경우 최종 위협 레벨을 결정하기 위해 지능형 알고리즘이 사용됩니다.

어플라이언스에서 안티바이러스 검사를 활성화하지 않고도 Outbreak Filter 기능을 사용할 수 있습니다. 두 가지 보안 서비스는 상호 보완하면서 독자적으로도 작동하도록 설계되었습니다. 즉, 어플라이언스에서 안티바이러스 검사를 활성화하지 않은 경우 안티바이러스 공급업체의 업데이트를 모니터링하고 Outbreak 격리에서 일부 메시지를 수동으로 릴리스하거나 재평가해야 합니다. 안티바이러스 검사를 활성화하지 않고 Outbreak Filter를 사용하는 경우 다음에 유의해야 합니다.

- 적응 규칙을 비활성화해야 합니다.
- 메시지는 Outbreak 규칙에 의해 격리됩니다.
- 위협 레벨이 낮아지고 시간이 만료되면 메시지가 릴리스됩니다.

다운스트림 안티바이러스 공급업체(desktops/groupware)에서 릴리스 시 메시지를 잡아낼 수 있습니다.

참고 Outbreak Filter 기능으로 비 바이러스성 위협을 검사하려면 어플라이언스에서 안티스팸 검사를 전역적으로 활성화해야 합니다.

동적 격리

Outbreak Filter 기능의 Outbreak 격리는 메시지가 위협인지 아니면 사용자에게 전달할 수 있는 안전한 상태인지를 확인할 때까지 메시지를 일시적으로 저장하는 장소입니다. (자세한 내용은 Outbreak 수명 주기 및 규칙 게시, 409 페이지 섹션을 참조하십시오.) 격리된 메시지는 Outbreak 격리에서 여러 방법으로 릴리스될 수 있습니다. 새로운 규칙이 다운로드되면 CASE에서 계산된 권장 재검사 간격을 기반으로 Outbreak 격리의 메시지가 재평가됩니다. 수정된 메시지의 위협 레벨이 격리 유지 임계값보다 낮으면 메시지는 자동으로 릴리스되므로(Outbreak 격리의 설정과 상관없이) 격리에서 보내는 시간이 최소화됩니다. 메시지 재평가 중에 새 규칙이 게시되면 재검사가 다시 시작됩니다.

바이러스 공격으로 격리된 메시지는 새 안티바이러스 서명을 사용할 수 있을 때 보안 침해 격리에서 자동으로 릴리스되지 않습니다. 새 규칙은 새 안티바이러스 서명을 참조할 수도, 참조하지 않을 수도 있습니다. 그러나 보안 침해 규칙이 메시지의 위협 레벨을 현재 위협 레벨 임계값보다 낮은 점수로 변경하지 않는 한 안티바이러스 엔진 업데이트에 따라 메시지가 릴리스되지는 않습니다.

메시지는 또한 CASE의 권장 유지 기간이 경과한 후에도 Outbreak 격리에서 릴리스됩니다. CASE는 메시지의 위협 레벨을 기반으로 유지 기간을 계산합니다. 바이러스 전파 확산 및 비 바이러스성 위협에 대해 별도의 최대 유지 시간을 정의할 수 있습니다. CASE의 권장 유지 시간이 위협 유형에 대한 최대 유지 시간을 초과하면, 최대 유지 시간이 경과한 후 Email Security Appliance에서 메시지를 릴리스합니다. 바이러스성 메시지의 경우 기본 최대 격리 기간은 1일입니다. 비 바이러스성 위협 격리의 기본 기간은 4시간입니다. 이러한 메시지를 격리에서 수동으로 릴리스할 수 있습니다.

Email Security Appliance는 격리가 꽉 찬 상태에서 메시지를 더 삽입해야 하는 경우에도 메시지를 릴리스합니다(이를 오버플로라고 함). Outbreak 격리 용량이 100%인 상태에서 격리에 새 메시지가 추가되는 경우에만 오버플로가 발생합니다. 이 시점에는 다음의 우선순위로 메시지가 릴리스됩니다.

- 적응 규칙에 의해 격리된 메시지(가장 먼저 릴리스될 예정인 메시지 우선)
- Outbreak 규칙에 의해 격리된 메시지(가장 먼저 릴리스될 예정인 메시지 우선)

Outbreak 격리의 용량이 100% 아래로 떨어지면 오버플로 릴리스가 중단됩니다. 격리 오버플로 처리 방법에 대한 자세한 내용은 격리에서 메시지의 보유 시간 , 850 페이지 및 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 851 페이지 섹션을 참조하십시오.

Outbreak 격리에서 릴리스된 메시지는 안티바이러스 및 안티스팸 엔진(메일 정책에 대해 활성화된 경우)으로 다시 검사됩니다. 해당 메시지가 알려진 바이러스 또는 스팸으로 표시된 경우 메일 정책 설정을 따르게 됩니다(바이러스 격리 또는 스팸 격리에 다시 격리될 수도 있음). 자세한 내용은 Outbreak Filter 기능 및 Outbreak 격리, 419 페이지를 참고하십시오.

따라서 메시지는 수명 주기 동안 실제로 두 번 격리될 수 있습니다. 한 번은 Outbreak Filter 기능에 의해 격리되고, 한 번은 Outbreak 격리에서 릴리스될 때 격리되는 것입니다. 각 검사의 판정(Outbreak Filter 이전, 그리고 Outbreak 격리에서 릴리스될 때)이 일치하면 메시지가 두 번째로 격리되지 않습니다. 또한 Outbreak Filter 기능은 메시지에 대해 최종 작업을 수행하지 않는다는 점도 기억해야 합니다. Outbreak Filter 기능은 메시지를 격리하거나(추가 처리를 위해), 파이프라인의 다음 단계로 메시지를 이동합니다.

관련 주제

- Outbreak 수명 주기 및 규칙 게시, 409 페이지

Outbreak 수명 주기 및 규칙 게시

바이러스 Outbreak(전파 확산) 수명 주기의 매우 초기에는 메시지 격리를 위해 더 폭넓은 규칙이 사용됩니다. 더 많은 정보를 사용할 수 있게 되면 좀 더 집중적인 규칙이 게시되고 격리 대상에 대한 정의가 좁혀집니다. 새 규칙이 게시되면 더 이상 바이러스 메시지가 아니라고 간주되는 메시지는 격리에서 릴리스됩니다. 새 규칙이 게시되면 Outbreak 격리 메시지는 재검사됩니다.

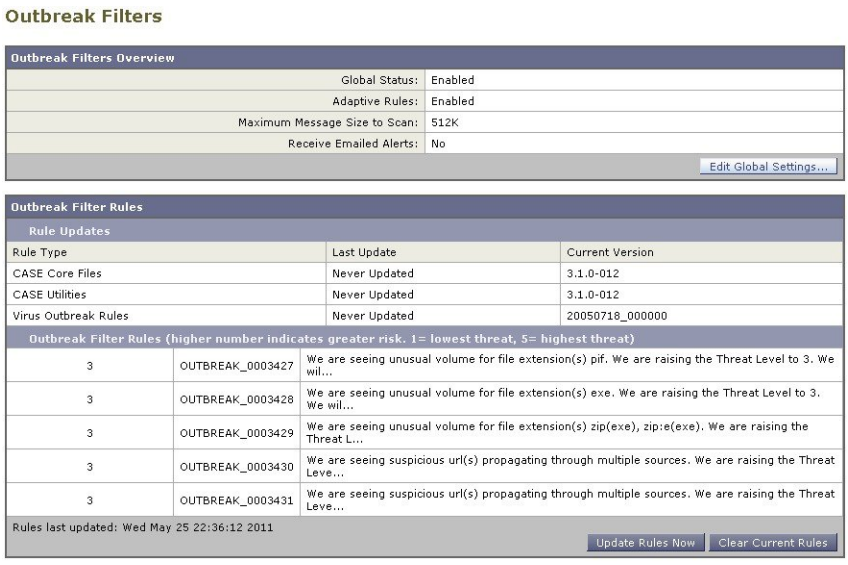
표 ***38: Outbreak*** 수명 주기에 대한 규칙 예

시간	규칙 유형	규칙 설명	조치
T=0	적응 규칙(과거 전파 확산 기반)	메시지 내용, 컨텍스트 및 구조를 분석하는 100,000개 이상의 메시지 특성을 기반으로 하는 통합 규칙 집합	적응 규칙과 일치하는 메시지는 자동으로 격리됨
T=5분	Outbreak 규칙	.zip(exe) 파일을 포함하는 메시지 격리	.exe가 포함된 .zip인 모든 첨부 파일 격리
T=10분	Outbreak 규칙	50KB보다 큰 .zip(exe) 파일인 메시지 격리	50KB보다 작은 .zip(exe) 파일이 포함된 메시지는 격리에서 릴리스됨
T=20분	Outbreak 규칙	50~55KB의 .zip(exe) 파일이 있고 파일 이름에 "Price"가 포함된 메시지 격리	이 기준과 일치하지 않는 메시지는 격리에서 릴리스됨
T=12시간	Outbreak 규칙	새 서명을 기준으로 검사	최신 안티바이러스 서명을 기준으로 모든 나머지 메시지 검사

Outbreak Filter 관리

GUI(Graphical User Interface)에 로그인하고, 메뉴에서 Security Services(보안 서비스)를 선택한 후 Outbreak Filters를 클릭합니다.

그림 ***30: Outbreak Filters*** 기본 페이지



Outbreak Filters 페이지에는 Outbreak Filters Overview(개요) 및 현재 Outbreak Filter Rules(규칙)의 목록(있는 경우), 이 두 섹션이 표시됩니다.

위 그림에서는 Outbreak Filter가 활성화되고, Adaptive Scanning(적응 검사)이 활성화되고, 최대 메시지 크기가 512k로 설정되었습니다. 이러한 설정을 변경하려면 **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다. 전역 설정 수정에 대한 자세한 내용은 Outbreak Filter 전역 설정 구성, 411 페이지 섹션을 참조하십시오.

Outbreak Filter Rules(규칙) 섹션에는 다양한 구성 요소(규칙 엔진과 규칙 자체)의 시간, 날짜 및 최신 업데이트 버전은 물론 현재 Outbreak Filter 규칙의 목록이 위협 레벨과 함께 나열됩니다.

Outbreak 규칙에 대한 자세한 내용은 Outbreak Filter 규칙, 414 페이지 섹션을 참조하십시오.

관련 주제

- Outbreak Filter 전역 설정 구성, 411 페이지
- Outbreak Filter 규칙, 414 페이지
- Outbreak Filter 기능 및 메일 정책, 415 페이지
- Outbreak Filter 기능 및 Outbreak 격리, 419 페이지

Outbreak Filter 전역 설정 구성

단계 **1** **Security Services(**보안 서비스**)** > **Outbreak Filters**를 클릭합니다.

단계 **2** **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **3** 요구 사항에 따라 다음을 수행합니다.

- Outbreak Filter를 전역적으로 활성화
- 적응 규칙 검사 활성화
- 검사할 파일의 최대 크기 설정(크기는 바이트 단위로 입력)
- Outbreak Filter에 대한 알림 활성화
- 웹 상호작용 추적 활성화. 웹 상호작용 추적 , 429 페이지를 참조하십시오.

단계 **4** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

이 기능은 outbreakconfig CLI 명령을 통해서도 사용할 수 있습니다(AsyncOS for Cisco Email Security Appliance용 CLI 참조 설명서 참조). 변경 후 제출하고 커밋합니다.

참고 웹 인터페이스를 사용하여 URL 로깅을 비활성화할 수 없습니다. CLI를 사용하여 URL 로깅을 활성화하는 방법은 URL 로깅 및 URL의 메시지 추적 세부 정보 활성화 , 412 페이지 섹션을 참조하십시오.

관련 주제

Outbreak Filter 기능 활성화

Outbreak Filter 기능을 전역적으로 활성화하려면 Outbreak Filters Global Settings(Outbreak Filter 전역 설정) 페이지에서 Enable Outbreak Filters(Outbreak Filter 활성화) 옆에 있는 확인란을 선택하고 **Submit(**제출**)**을 클릭합니다. 먼저 Outbreak Filters 라이센스 계약에 동의해야 합니다.

Outbreak Filter 기능을 전역적으로 활성화했으면 기본 정책을 포함하여 각 수신 및 발신 메일 정책에 대해 개별적으로 활성화 또는 비활성화할 수 있습니다. 자세한 내용은 Outbreak Filter 기능 및 메일 정책, 415 페이지 섹션을 참조하십시오.

안티 스팸 검사의 활성화 여부와 상관없이 Outbreak Filter 기능은 CASE(Context Adaptive Scanning Engine)를 사용하여 바이러스성 위협을 탐지합니다. 그러나 비 바이러스성 위협을 검사하려면 어플라이언스에서 Anti-Spam 또는 Intelligent Multi-Scan을 전역적으로 활성화해야 합니다.

참고 시스템 설정 중에 라이센스에 동의하지 않은 경우(4단계: 보안, 37 페이지 참조), Security Services(보안 서비스) > Outbreak Filters 페이지에서 **Enable(**활성화**)**을 클릭한 후 라이센스를 읽고 동의해야 합니다.

적응 규칙 활성화

Adaptive Scanning(적응 검사)은 Outbreak Filters에서 적응 규칙의 사용을 활성화합니다. 메시지 내용과 관련된 바이러스 서명 또는 스팸 기준을 사용할 수 없는 경우 메시지가 악성코드 전파 확산의 일부일 가능성을 판단하는 데 요소 또는 특성(파일 크기 등)의 집합이 사용됩니다. Adaptive Scanning(적응 검사)을 활성화하려면 Outbreak Filters Global Settings(Outbreak Filter 전역 설정) 페이지에서 Enable Adaptive Rules(적응 규칙 활성화) 옆에 있는 확인란을 선택하고 **Submit(**제출**)**을 클릭합니다.

Outbreak Filter에 대한 알림 활성화

Outbreak Filter 기능에 대한 알림을 활성화하려면 "Emailed Alerts(이메일 알림)"라는 확인란을 선택합니다. Outbreak Filter에 대한 이메일 알림을 활성화하면 Outbreak Filter와 관련된 알림을 전송하는 알림 엔진이 활성화될 뿐입니다. 어떤 알림을 어떤 이메일 주소로 전송할지는 System Administration(시스템 관리) 탭의 Alerts(알림) 페이지를 통해 구성됩니다. Outbreak Filter에 대해 알림을 구성하는 방법에 대한 자세한 내용은 알림, SNMP 트랩 및 Outbreak Filter, 422 페이지 섹션을 참조하십시오.

URL 로깅 및 URL의 메시지 추적 세부 정보 활성화

URL 관련 로그의 로깅 및 메시지 추적 세부 정보에 이 정보 표시는 기본적으로 비활성화됩니다. 여기에는 다음 이벤트에 대한 로그가 포함됩니다.

- 메시지에 있는 URL의 범주가 URL 범주 필터와 일치함
- 메시지에 있는 URL의 평판 점수가 URL 평판 필터와 일치함
- Outbreak Filter가 메시지에서 URL을 재작성함

이러한 이벤트의 로깅을 활성화하려면 CLI(command-line interface)에서 outbreakconfig 명령을 사용합니다.

관련 주제

- 예: outbreakconfig 명령을 사용하여 URL의 로깅 활성화 , 413 페이지
- Outbreak Filter 규칙 관리, 414 페이지
- 예: outbreakconfig 명령을 사용하여 URL의 로깅 활성화 , 413 페이지

예: outbreakconfig 명령을 사용하여 URL의 로깅 활성화

다음 예에서는 outbreakconfig 명령을 사용하여 URL의 로깅을 활성화하는 방법을 보여줍니다.

```
mail.example.com> outbreakconfig

Outbreak Filters: Enabled

Choose the operation you want to perform:

- SETUP - Change Outbreak Filters settings.

[]> setup

Outbreak Filters: Enabled

Would you like to use Outbreak Filters? [Y]>

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back
down below), meaning that new messages of

certain types could be quarantined or will no longer be quarantined, respectively.

Would you like to receive Outbreak Filter alerts? [N]>

What is the largest size message Outbreak Filters should scan?

[524288]>

Do you want to use adaptive rules to compute the threat level of messages? [Y]>

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N]> Y

Logging of URLs has been enabled.

The Outbreak Filters feature is now globally enabled on the system.  You must use the
'policyconfig' command in the CLI or the Email

Security Manager in the GUI to enable Outbreak Filters for the desired Incoming and Outgoing
 Mail Policies.

Choose the operation you want to perform:
```

```
- SETUP - Change Outbreak Filters settings.

[]>
```

Outbreak Filter 규칙

Outbreak 규칙은 Cisco Security Intelligence Operations에 의해 게시되며, 어플라이언스는 새 Outbreak 규칙을 5분마다 확인 및 다운로드합니다. 이 업데이트 간격을 변경할 수 있습니다. 자세한 내용은 업그레이드 및 업데이트 다운로드를 위한 서버 설정 구성 , 949 페이지 항목을 참고하십시오.

관련 주제

- Outbreak Filter 규칙 관리, 414 페이지

Outbreak Filter 규칙 관리

Outbreak Filters Rules(Outbreak Filter 규칙)는 자동으로 다운로드되므로 사용자 측에서 실제로 관리할 필요가 없습니다.

그러나 어떤 이유로 어플라이언스가 새 규칙을 다운로드하기 위해 Cisco의 업데이트 서버에 상당 기간 도달할 수 없는 경우 로컬에 캐시된 점수가 더 이상 유효하지 않을 수 있습니다(즉, 알려진 바이러스성 첨부 파일 형식이 안티바이러스 소프트웨어에서 업데이트되었거나 더 이상 위협이 아닌 경우). 이런 경우에는 메시지를 이러한 특성으로 더 이상 격리하지 않을 수 있습니다.

Update Rules Now(지금 규칙 업데이트**)**를 클릭하여 Cisco의 업데이트 서버에서 최신 Outbreak 규칙을 수동으로 다운로드할 수 있습니다.

참고 **Update Rules Now(**지금 규칙 업데이트**)** 버튼을 클릭한다고 해서 어플라이언스에 있는 기존의 모든 Outbreak 규칙이 "제거"되지는 않습니다. 업데이트된 Outbreak 규칙만 교체됩니다. Cisco의 업데이트 서버에서 사용할 수 있는 업데이트가 없는 경우에는 이 버튼을 클릭해도 어플라이언스에서 Outbreak 규칙을 다운로드하지 않습니다.

관련 주제

- Outbreak Filter 규칙 업데이트, 414 페이지

Outbreak Filter 규칙 업데이트

기본적으로 어플라이언스는 5분마다 새 Outbreak Filter 규칙을 다운로드하려고 시도합니다. Security Services(보안 서비스) > Service Updates(서비스 업데이트) 페이지에서 이 간격을 변경할 수 있습니다. 자세한 내용은 서비스 업데이트 , 945 페이지를 참고하십시오.

Outbreak Filter 기능 및 메일 정책

Outbreak Filter 기능에는 메일 정책당 구성할 수 있는 설정이 있습니다. Outbreak Filter 기능은 어플라이언스에서 각 메일 정책에 대해 활성화 또는 비활성화할 수 있습니다. 메일 정책별로 Outbreak Filter 기능 처리에서 특정 파일 확장명과 도메인을 제외할 수 있습니다. 이 기능은 Policyconfig CLI 명령을 통해서도 사용할 수 있습니다(AsyncOS for Cisco Email Security Appliance용 CLI 참조 설명서 참조).

참고 Outbreak Filter 기능으로 비 바이러스성 위협을 검사하려면 어플라이언스에서 Anti-Spam 또는 Intelligent Multi-Scan 검사를 전역적으로 활성화해야 합니다.

특정 메일 정책에 대해 Outbreak Filter 기능 설정을 수정하려면 변경할 정책의 Outbreak Filters 열에 있는 링크를 클릭합니다.

특정 메일 정책에 대해 Outbreak Filter 기능을 활성화 및 사용자 지정하려면 **Enable Outbreak Filtering (Customize Settings)(Outbreak Filtering** 활성화(설정 사용자 지정)**)**을 선택합니다.

메일 정책에 대해 다음 Outbreak Filter 설정을 구성할 수 있습니다.

- 격리 위협 레벨
- 최대 격리 유지 시간
- 비 바이러스성 위협 메시지를 격리에 추가하지 않고 즉시 전달
- 우회할 파일 확장명 유형
- 메시지 수정 임계값
- 맞춤형 텍스트 및 Outbreak Filter 변수(예: $threat_verdict, $threat_category, $threat_type, $threat_description 및 $threat_level)를 사용하여 제목 헤더 변경
- 다음 이메일 헤더 포함:
  - X-IronPort-Outbreak-Status
  - X-IronPort-Outbreak-Description
- 메시지를 Email Security Appliance 또는 Exchange Server 등 대체 대상으로 전송
- URL 재작성
- 위협 면책조항

기본 메일 정책에 대해 정의된 Outbreak Filters 설정을 사용하려면 **Enable Outbreak Filtering (Inherit Default mail policy settings)(Outbreak Filtering** 활성화(기본 메일 정책 설정 상속)**)**을 선택합니다. 기본 메일 정책에서 Outbreak Filter 기능이 활성화되어 있으면 다른 모든 메일 정책에서도(사용자 지정되지 않은 경우) 동일한 Outbreak Filter 설정을 사용합니다.

설정을 변경했으면 변경 사항을 커밋합니다.

관련 주제

- 격리 레벨 임계값 설정, 416 페이지
- 최대 격리 유지, 416 페이지
- 파일 확장명 유형 우회, 416 페이지
- 메시지 수정, 417 페이지

격리 레벨 임계값 설정

목록에서 전파 확산 위협에 대한 Quarantine Threat Level(격리 위협 레벨) 임계값을 선택합니다. 숫자가 작을수록 격리되는 메시지가 많아지고, 숫자가 클수록 격리되는 메시지가 적어집니다. Cisco에서는 기본값 3을 권장합니다.

자세한 내용은 격리 위협 레벨 임계값 설정에 대한 지침, 406 페이지를 참고하십시오.

최대 격리 유지

메시지가 Outbreak 격리에 머무는 최대 시간을 지정합니다. 바이러스성 첨부 파일을 포함할 수 있는 메시지와 피싱이나 악성코드 링크 등 기타 위협을 포함할 수 있는 메시지에 대해 유지 시간을 다르게 지정할 수 있습니다. 비 바이러스성 위협의 경우 격리에 추가하지 않고 즉시 메시지를 전달하려면 **Deliver messages without adding them to quarantine(**격리에 추가하지 않고 메시지 전달**)** 확인란을 선택합니다.

참고 정책에 대한 Message Modification(메시지 수정)을 활성화하지 않으면 비 바이러스성 위협을 격리할 수 없습니다.

CASE에서는 메시지에 위협 레벨을 할당할 때 격리 유지 기간을 권장합니다. 해당 위협 유형의 최대 격리 유지 시간을 초과하지 않는 한 Email Security Appliance는 CASE에서 권장하는 시간 동안 격리된 메시지를 보관합니다.

파일 확장명 유형 우회

특정 파일 형식을 우회하도록 정책을 수정할 수 있습니다. 우회된 파일 확장명은 CASE에서 메시지에 대한 위협 레벨을 계산할 때 포함되지 않습니다. 그러나 첨부 파일은 이메일 보안 파이프라인의 나머지에서 여전히 처리됩니다.

파일 확장명을 우회하려면 Bypass Attachment Scanning(첨부 파일 검사 우회)을 클릭하고 파일 확장명을 선택하거나 입력한 후 **Add Extension(**확장명 추가**)**을 클릭합니다. AsyncOS의 File Extensions to Bypass(우회할 파일 확장명) 목록에 확장명 유형이 표시됩니다.

우회할 확장명 목록에서 확장명을 제거하려면 File Extensions to Bypass(우회할 파일 확장명) 목록에서 확장명 옆에 있는 휴지통 아이콘을 클릭합니다.

관련 주제

- 파일 확장명 우회: 컨테이너 파일 형식, 416 페이지

파일 확장명 우회: 컨테이너 파일 형식

파일 확장명을 우회할 때, 확장명이 우회할 확장명 목록에 있으면 컨테이너 파일 내 파일(예: .zip 내부의 .doc 파일)도 우회됩니다. 예를 들어 우회할 확장명 목록에 .doc를 추가하면, 컨테이너 파일 내에 있더라도 모든 .doc 파일이 우회됩니다.

메시지 수정

어플라이언스가 피싱 시도나 악성 웹사이트에 대한 링크 등 비 바이러스성 위협을 메시지에서 검사하도록 하려면 Message Modification(메시지 수정)을 활성화합니다.

메시지의 위협 레벨을 기반으로 AsyncOS는 수신자가 메시지에서 웹사이트를 열려고 시도할 경우 Cisco 웹 보안 프록시로 리디렉션하도록 메시지를 수정하여 모든 URL을 재작성할 수 있습니다. 또한 메시지의 내용이 의심스럽거나 악의적임을 사용자에게 알리기 위해 메시지에 면책조항을 추가할 수도 있습니다.

비 바이러스성 위협 메시지를 격리하려면 메시지 수정을 활성화해야 합니다.

관련 주제

- 메시지 수정 위협 레벨, 417 페이지
- 메시지 제목, 417 페이지
- Outbreak Filter 이메일 헤더, 417 페이지
- 대체 대상 메일 호스트, 418 페이지
- URL 재작성 및 도메인 우회, 418 페이지
- 위협 면책조항, 419 페이지

메시지 수정 위협 레벨

목록에서 Message Modification Threat Level(메시지 수정 위협 레벨) 임계값을 선택합니다. 이 설정은 CASE에서 반환한 위협 레벨을 기반으로 메시지를 수정할지 여부를 결정합니다. 숫자가 작을수록 수정되는 메시지가 많아지고, 숫자가 클수록 수정되는 메시지가 적어집니다. Cisco에서는 기본값 3을 권장합니다.

메시지 제목

수정된 링크가 포함된 비 바이러스성 위협 메시지에서 제목 헤더의 텍스트를 변경하여, 사용자 보호를 위해 메시지가 수정되었음을 알릴 수 있습니다. 맞춤형 텍스트, Outbreak Filter(보안 침해 필터) 변수(예: `$threat_verdict`, `$threat_category`, `$threat_type`, `$threat_description`, `$threat_level`) 또는 두 가지 조합으로 제목 헤더를 앞이나 뒤에 추가합니다. 변수를 삽입하려면 **Insert Variables(**변수 삽입**)**를 클릭하고 변수 목록에서 선택합니다.

Message Subject(메시지 제목) 필드에서는 공백이 무시되지 않습니다. 이 필드에 입력하는 텍스트의 뒤(뒤에 추가하는 경우) 또는 앞(앞에 추가하는 경우)에 공백을 추가하여 메시지의 원래 제목과 추가된 텍스트를 구분합니다. 예를 들어 앞에 추가하는 경우 `[MODIFIED FOR PROTECTION]` 텍스트를 몇몇 후행 공백과 함께 추가합니다.

참고 Message Subject(메시지 제목) 필드에는 US-ASCII 문자만 사용 가능합니다.

Outbreak Filter 이메일 헤더

메시지에 다음 헤더를 추가할 수 있습니다.

헤더	형식	예	옵션
X-IronPort-Outbreak-Status	`X-IronPort-Outbreak-Status: $threat_verdict, level $threat_level, $threat_category - $threat_type`	`X-IronPort-Outbreak-Status: Yes, level 4, Phish - Password`	• 모든 메시지에 대해 활성화 • 비 바이러스성 전파 확산에 대해서만 활성화 • 비활성화
X-IronPort-Outbreak-Description	`X-IronPort-Outbreak-Description: $threat_description`	`X-IronPort-Outbreak-Description: It may trick victims into submitting their username and password on a fake website.`	• Enable(활성화) • 비활성화

참고 이러한 헤더를 기반으로 메시지를 필터링하려면 Outbreak Filter로 처리된 메시지를 Email Security Appliance로 돌려보내고(대체 대상 메일 호스트를 구성하여), 이러한 헤더와 일치하는 콘텐츠 필터를 사용하여 검사해야 합니다.

대체 대상 메일 호스트

Outbreak Filter로 처리된 메시지에 대해 콘텐츠 필터 기반 검사를 수행하려면, 처리된 메시지를 Email Security Appliance로 돌려보내도록 Outbreak Filter를 구성해야 합니다. 처리 파이프라인에서 콘텐츠 필터 검사 후에 Outbreak Filter 검사가 수행되기 때문입니다.

처리된 메시지를 추가로 검사하기 위해 전송할 어플라이언스의 IP 주소(IPv4 또는 IPv6) 또는 FQDN을 **Alternate Destination Mail Host(**대체 대상 메일 호스트**)** 필드에 입력합니다.

URL 재작성 및 도메인 우회

메시지의 위협 레벨이 메시지 수정 임계값을 초과하면, Outbreak Filter 기능은 사용자가 URL을 클릭할 경우 Cisco 웹 보안 프록시의 시작 화면으로 리디렉션하기 위해 메시지의 모든 URL을 재작성합니다. (자세한 내용은 URL 리디렉션, 403 페이지 섹션을 참조하십시오.) 메시지의 위협 레벨이 격리 임계값을 초과하면 어플라이언스는 또한 메시지를 격리합니다. 소규모 비 바이러스성 전파 확산이 진행 중인 경우 메시지를 격리하면 TOC에서는 전파 확산 가능 메시지에서 연결된 의심스런 웹사이트를 분석하고 악성 웹사이트인지 여부를 판단할 시간을 얻게 됩니다. CASE에서는 SIO의 업데이트된 Outbreak 규칙을 사용하여 메시지를 재검사함으로써 메시지가 전파 확산의 일부인지를 판단합니다. 유지 기간이 만료되면 어플라이언스는 격리에서 메시지를 릴리스합니다.

AsyncOS는 우회 도메인을 가리키는 URL을 제외하고 메시지 내 모든 URL을 재작성합니다.

URL 재작성에 대해 다음 옵션을 사용할 수 있습니다.

- **Enable only for unsigned messages(**서명되지 않은 메시지에 대해서만 활성화**)**. 이 옵션을 선택하면 AsyncOS는 메시지 수정 임계값을 충족하거나 초과하는 서명되지 않은 메시지의 URL을 재작성하되, 서명된 메시지의 URL은 재작성하지 않습니다. Cisco에서는 URL 재작성에 이 설정을 사용할 것을 권장합니다.

참고 Email Security Appliance에서는 DomainKeys/DKIM 서명 메시지의 URL을 재작성하고, 네트워크에서 Email Security Appliance 이외의 서버나 어플라이언스가 DomainKeys/DKIM 서명의 확인을 책임지는 경우 메시지 서명을 무효화합니다.

어플라이언스는 S/MIME을 사용하여 암호화되었거나 S/MIME 서명이 포함된 메시지를 서명된 메시지로 간주합니다.

- **Enable for all messages(**모든 메시지에 대해 활성화**).** 이 옵션을 선택하면 AsyncOS는 서명된 메시지를 포함하여 메시지 수정 임계값을 충족하거나 초과하는 모든 메시지의 URL을 재작성합니다. AsyncOS에서 서명된 메시지를 수정하면 서명이 무효화됩니다.
- **Disable(**비활성화**).** 이 옵션은 Outbreak Filter에 대한 URL 재작성을 비활성화합니다.

특정 도메인에 대한 URL의 수정을 제외하도록 정책을 수정할 수 있습니다. 도메인을 우회하려면 Bypass Domain Scanning(도메인 검사 우회) 필드에 IPv4 주소, IPv6 주소, CIDR 범위, 호스트 이름, 부분 호스트 이름 또는 도메인을 입력합니다. 항목이 여러 개인 경우 쉼표를 사용하여 구분합니다.

도메인 검사 우회 기능은 URL 필터링에 사용되는 전역 화이트리스트와 유사합니다(그러나 독립적임). 화이트리스트에 대한 자세한 내용은 URL 필터링용 화이트리스트 만들기 , 430 페이지 섹션을 참조하십시오.

위협 면책조항

Email Security Appliance는 사용자에게 내용에 대해 경고하기 위해 의심스런 메시지 제목 위에 면책조항 메시지를 추가할 수 있습니다. 메시지의 유형에 따라 이 면책조항은 HTML 형식이거나 일반 텍스트일 수 있습니다.

Threat Disclaimer(위협 면책조항) 목록에서 사용할 면책조항 텍스트를 선택하거나, Mail Policies(메일 정책) > Text Resources(텍스트 리소스) 링크를 클릭하고 Disclaimer Template(면책조항 템플릿)을 사용하여 새 면책조항을 만듭니다. 면책조항 템플릿에는 전파 확산 위협 정보에 대한 변수가 포함되어 있습니다. Preview Disclaimer(면책조항 미리 보기)를 클릭하여 위협 면책조항을 미리 볼 수 있습니다. 사용자 지정 면책조항 메시지의 경우 변수를 사용하여 메시지에 위협 레벨, 위협 유형 및 위협 설명을 표시할 수 있습니다. 면책조항 메시지 만들기에 대한 자세한 내용은 텍스트 리소스 관리 개요, 622 페이지 섹션을 참조하십시오.

Outbreak Filter 기능 및 Outbreak 격리

Outbreak Filter 기능으로 격리된 메시지는 Outbreak 격리로 전송됩니다. 이 격리는 "요약" 보기가 있다는 점을 제외하면 다른 격리와 동일하게 작동합니다(격리 작업에 대한 자세한 내용은 정책, 바이러스, 보안 침해 격리, 847 페이지 참조). 이 보기는 메시지를 격리로 보내는 데 사용된 규칙(예: Outbreak 규칙의 경우 Outbreak ID가 표시되고, 적응 규칙의 경우 일반 용어 표시)을 기반으로 격리에서 모든 메시지를 삭제하거나 릴리스하는 데 유용합니다. 요약 보기에 대한 자세한 내용은 Outbreak 격리 및 규칙 요약 보기로 관리, 421 페이지 섹션을 참조하십시오.

관련 주제

- Outbreak 격리 모니터링, 420 페이지
- Outbreak 격리 및 규칙 요약 보기로 관리, 421 페이지

Outbreak 격리 모니터링

제대로 구성된 격리는 모니터링이 거의 필요하지 않지만, 특히 바이러스 전파 확산 중에 그리고 그 이후에 합법적인 메시지가 지연될 수 있을 때에는 Outbreak 격리를 유심히 관찰하는 것이 좋습니다.

합법적인 메시지가 격리되는 경우 Outbreak 격리에 대한 설정에 따라 다음 중 하나가 발생합니다.

- 격리의 Default Action(기본 작업)이 Release(릴리스)로 설정된 경우 유지 기간이 만료되거나 격리가 오버플로될 때 메시지가 릴리스됩니다. 오버플로 때문에 메시지가 릴리스되기 전에 메시지에 대해 첨부 파일 제거, 제목 수정, X-Header 추가 등을 수행하도록 보안 침해 격리를 구성할 수 있습니다. 이러한 작업에 대한 자세한 내용은 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 851 페이지 섹션을 참조하십시오.
- 격리의 Default Action(기본 작업)이 Delete(삭제)로 설정된 경우 유지 기간이 만료되거나 격리가 오버플로될 때 메시지가 삭제됩니다.
- 격리가 꽉 찬 상태에서 메시지가 더 추가되면 오버플로가 발생합니다. 이 경우 새 메시지를 수용할 수 있는 충분한 여유가 생길 때까지 만료일에 가장 가까운 메시지(가장 오래된 메시지일 필요는 없음)가 먼저 릴리스됩니다. 오버플로 때문에 메시지가 릴리스되기 전에 메시지에 대해 첨부 파일 제거, 제목 수정, X-Header 추가 등을 수행하도록 보안 침해 격리를 구성할 수 있습니다.

새 규칙이 게시되면 격리된 메시지가 재검사되기 때문에, Outbreak 격리에 있는 메시지가 만료 시간 전에 릴리스될 가능성이 높습니다.

Default Action(기본 작업)이 Delete(삭제)로 설정된 경우에도 Outbreak 격리를 모니터링하는 것이 중요할 수 있습니다. 대부분의 사용자는 기본 작업을 Delete(삭제)로 설정하지 않는 것이 좋습니다. Outbreak 격리에서 메시지를 릴리스하거나 Outbreak 격리에 대한 기본 작업을 변경하는 방법에 대한 자세한 내용은 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 851 페이지 섹션을 참조하십시오.

반대로, 예를 들어 새 규칙 업데이트를 기다리는 동안 Outbreak 격리에 더 오래 보관하고 싶은 메시지가 있는 경우 해당 메시지의 만료일을 지연할 수 있습니다. 메시지의 유지 시간을 늘리면 격리의 크기가 커질 수 있습니다.

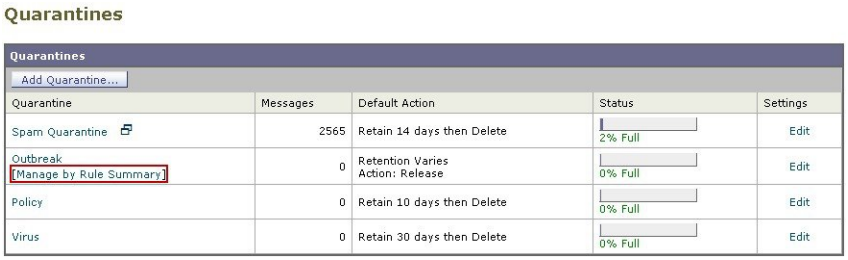
참고 메시지가 보안 침해 격리에 있는 동안 안티바이러스 검사가 전역적으로 비활성화되면(메일 정책을 통해서가 아니라), 메시지가 격리를 떠나기 전 안티바이러스 검사가 다시 활성화되더라도, 메시지가 격리를 떠날 때 안티바이러스 검사가 수행되지 않습니다.

참고 어플라이언스에서 안티바이러스 검사를 활성화하지 않고도 Outbreak Filters 기능을 사용할 수 있습니다. 그러나 어플라이언스에서 안티스팸 기능이 활성화되어 있지 않으면 Outbreak Filter로 비 바이러스성 위협을 검사할 수 없습니다.

Outbreak 격리 및 규칙 요약 보기로 관리

GUI의 Monitor(모니터) 메뉴에 있는 목록에서 격리의 이름을 클릭하여 Outbreak 격리의 내용을 볼 수 있습니다. Outbreak 격리에는 추가 보기인 Outbreak Quarantine Manage by Rule Summary Link(규칙 요약 링크로 Outbreak 격리 관리)도 있습니다.

그림 *31:* 규칙 요약 링크로 *Outbreak* 격리 관리



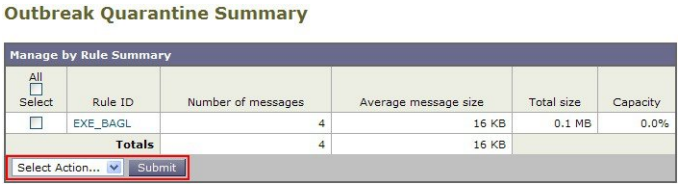
관련 주제

- 요약 보기를 사용하여 규칙 ID를 기반으로 Outbreak 격리의 메시지에 대해 메시지 작업 수행, 421 페이지

요약 보기를 사용하여 규칙 ID를 기반으로 Outbreak 격리의 메시지에 대해 메시지 작업 수행

규칙 ID로 그룹화된 Outbreak 격리의 내용 목록을 보려면 Manage by Rule Summary(규칙 요약으로 관리) 링크를 클릭합니다.

그림 *32:* 규칙 요약 보기로 *Outbreak* 격리 관리



이 보기에서 Outbreak 또는 적응 규칙과 관련된 모든 메시지에 대해(개별 메시지를 선택하기보다) 릴리스, 삭제 또는 종료 지연을 선택할 수 있습니다. 목록을 통해 검색하거나 목록을 정렬할 수도 있습니다.

quarantineconfig -> outbreakmanage CLI 명령을 통해서도 이 기능을 이용할 수 있습니다. 자세한 내용은 AsyncOS for Cisco Email Security Appliance용 CLI 참조 설명서를 참조하십시오.

Outbreak Filter 모니터링

어플라이언스에는 Outbreak Filter 기능의 성능과 활동을 모니터링하기 위한 여러 툴이 있습니다.

관련 주제

- Outbreak Filter 보고서, 422 페이지
- Outbreak Filter 개요 및 규칙 목록, 422 페이지

• 신종 바이러스 격리, 422 페이지
• 알림, SNMP 트랩 및 Outbreak Filter, 422 페이지

Outbreak Filter 보고서

Outbreak Filter 보고서에서는 어플라이언스에 있는 Outbreak Filter의 현재 상태와 컨피그레이션은 물론 현재 전파 확산에 대한 정보와 Outbreak Filter로 인해 격리된 메시지도 볼 수 있습니다. Monitor(모니터) > Outbreak Filters 페이지에서 이 정보를 볼 수 있습니다. 자세한 내용은 "이메일 보안 모니터" 장을 참고하십시오.

Outbreak Filter 개요 및 규칙 목록

개요 및 규칙 목록은 Outbreak Filter 기능의 현재 상태에 대한 유용한 정보를 제공합니다. Security Services(보안 서비스) > Outbreak Filters 페이지를 통해 이 정보를 볼 수 있습니다.

신종 바이러스 격리

Outbreak Filter 위협 레벨 임계값으로 플래그가 지정된 메시지 수를 모니터링하려면 Outbreak 격리를 사용합니다. 규칙별로 격리된 메시지의 목록도 사용할 수 있습니다. 자세한 내용은 Outbreak 격리 및 규칙 요약 보기로 관리, 421 페이지 및 정책, 바이러스, 보안 침해 격리, 847 페이지를 참조하십시오.

알림, SNMP 트랩 및 Outbreak Filter

Outbreak Filter 기능은 일반 AsyncOS 알림과 SNMP 트랩이라는 두 가지 유형의 알림을 지원합니다.

SNMP 트랩은 규칙 업데이트가 실패할 때 생성됩니다. AsyncOS의 SNMP 트랩에 대한 자세한 내용은 "CLI를 통한 관리 및 모니터링" 장을 참조하십시오.

AsyncOS에는 Outbreak Filter 기능에 대한 두 가지 유형의 알림(크기 및 규칙)이 있습니다.

Outbreak 격리의 크기가 최대 크기의 5, 50, 75 및 95를 넘을 때마다 AsyncOS 알림이 생성됩니다. 95% 임계값에 대해 생성된 알림의 심각도는 CRITICAL인 반면 나머지 알림 임계값은 WARNING입니다. 격리 크기가 증가하면서 임계값을 넘으면 알림이 생성됩니다. 격리 크기가 줄어들면서 임계값을 넘으면 알림이 생성되지 않습니다. 알림에 대한 자세한 내용은 알림, 962 페이지 섹션을 참조하십시오.

규칙이 게시되거나, 임계값이 변경되거나, 규칙 또는 CASE 엔진 업데이트 중 문제가 발생하는 경우에도 알림이 생성됩니다.

Outbreak Filter 기능 문제 해결

이 섹션에서는 Outbreak Filter 기능에 대한 몇 가지 기본적인 문제 해결 팁을 제공합니다.

관련 주제

• Cisco에 잘못 분류된 메시지 보고 , 423 페이지

• 여러 첨부 파일 및 우회되는 파일 형식, 423 페이지
• 메시지 및 콘텐츠 필터와 이메일 파이프라인, 423 페이지

Cisco에 잘못 분류된 메시지 보고

Cisco에 분류 오류를 알리려면 Outbreak 격리에 대한 Manage Quarantine(격리 관리) 페이지에 있는 확인란을 사용합니다.

여러 첨부 파일 및 우회되는 파일 형식

우회되는 파일 형식은 메시지의 유일한 첨부 파일이 해당 형식이거나, 첨부 파일이 여러 개이거나, 다른 첨부 파일에 기존 규칙이 없는 경우에만 제외됩니다. 그렇지 않은 경우에만 메시지가 검사됩니다.

메시지 및 콘텐츠 필터와 이메일 파이프라인

Outbreak Filter에 의한 검사 전에 메시지 및 콘텐츠 필터가 메시지에 적용됩니다. 필터에 따라 메시지는 Outbreak Filter 검사를 건너뛰거나 우회할 수 있습니다.

18 장

악의적이거나 바람직하지 않은 URL로부터 보호

이 장에는 다음 섹션이 포함되어 있습니다.

URL 관련 보호 및 제어

악의적이거나 바람직하지 않은 링크로부터의 보호 및 제어는 작업 대기열에서 안티스팸, 전파 확산, 콘텐츠 및 메시지 필터링 프로세스에 통합됩니다. 이를 통해 다음을 제어합니다.

- 메시지와 첨부 파일에 있는 악의적인 URL로부터 보호하는 효율성 증가

  URL 필터링은 Outbreak Filter에 통합됩니다. 이렇게 강화된 보호 기능은 조직에 이미 Cisco Web Security Appliance 또는 유사한 웹 기반 위협 방지 대안이 있더라도 유용한데, 그 이유는 엔트리 포인트에서 위협을 차단하기 때문입니다.

  또한 메시지에 있는 URL의 WBRS(Web Based Reputation Score)를 기반으로 콘텐츠 또는 메시지 필터를 사용할 수 있습니다. 예를 들면 클릭 시 안전을 평가하기 위해 Cisco Web Security Proxy로 리디렉션하도록 중립이거나 알 수 없는 평판의 URL을 재작성할 수 있습니다.

- 스팸을 더 잘 식별

어플라이언스는 스팸을 식별하기 위해 메시지에 있는 링크의 평판과 범주를 기타 스팸 식별 알고리즘과 함께 사용합니다. 예를 들어, 메시지의 링크가 마케팅 웹사이트에 속하는 경우 해당 메시지는 마케팅 메시지일 가능성이 높습니다.

- 기업에서 허용되는 사용 정책의 시행 지원

  기업에서 허용되는 사용 정책을 시행하기 위해 URL의 범주(예: 성인 콘텐츠 또는 불법 활동)를 콘텐츠 및 메시지 필터와 함께 사용할 수 있습니다.

- 조직에서 보호를 위해 재작성된 메시지의 URL을 가장 자주 클릭한 사용자는 물론 가장 자주 클릭된 링크도 식별할 수 있습니다.

관련 주제

- 평가되는 URL , 426 페이지
- Web Interaction Tracking(웹 상호 작용 추적) 페이지, 819 페이지

평가되는 URL

수신 및 발신 메시지(첨부 파일 포함)의 URL이 평가됩니다. 다음이 있는 문자열을 포함하여 URL에 대한 유효한 문자열이 평가됩니다.

- http, https 또는 www
- 도메인 또는 IP 주소
- 콜론(:)이 앞에 오는 포트 번호
- 대문자 또는 소문자

메시지가 스팸인지를 확인하기 위해 URL을 평가할 때, 로드 관리에 필요할 경우 시스템은 발신 메시지보다 수신 메시지에 우선 순위를 둡니다.

URL 필터링 설정

- URL 필터링 요구 사항 , 426 페이지
- URL 필터링 활성화, 427 페이지
- Cisco Web Security Services에 대한 연결 정보 , 428 페이지
- 웹 상호작용 추적 , 429 페이지
- 클러스터 구성의 URL 필터링, 429 페이지
- URL 필터링용 화이트리스트 만들기 , 430 페이지
- 엔드 유저에게 사이트가 악의적인지 여부를 표시하는 알림 맞춤화 , 431 페이지

URL 필터링 요구 사항

URL 필터링 활성화 외에도, 원하는 기능에 따라 다른 기능을 활성화해야 합니다.

스팸을 더 잘 차단하려면

- 안티스팸 검사를 전역적으로, 그리고 해당 메일 정책별로 활성화해야 합니다. IronPort Anti-Spam 또는 Intelligent Multi-Scan 기능 중 하나일 수 있습니다. 안티 스팸 장을 참조하십시오.

  악성코드를 더 잘 차단하려면

- Outbreak Filter 기능을 전역적으로, 그리고 해당 메일 정책별로 활성화해야 합니다. Outbreak Filter 장을 참조하십시오.

  URL 평판을 기반으로 작업을 수행하거나 메시지 및 콘텐츠 필터를 사용하여 허용되는 사용 정책을 시행하려면

- Outbreak Filter 기능을 전역적으로 활성화해야 합니다. Outbreak Filter 장을 참조하십시오.

URL 필터링 활성화

웹 인터페이스의 **Security Services(보안 서비스) > URL Filtering(URL 필터링)** 페이지 또는 CLI의 **`websecurityconfig`** 명령을 사용하여 URL 필터링을 활성화할 수 있습니다.

시작하기 전에

- 사용하고자 하는 개별 URL 필터링 기능에 대한 요구 사항이 충족되었는지 확인합니다. URL 필터링 요구 사항 , 426 페이지를 참조하십시오.
- (선택 사항) 모든 URL 필터링 기능에서 무시할 URL 목록을 만듭니다. URL 필터링용 화이트리스트 만들기 , 430 페이지를 참조하십시오.

단계 **1** **Security Services(보안 서비스) > URL Filtering(URL 필터링)**을 선택합니다.

단계 **2** **Enable(활성화)**을 클릭합니다.

단계 **3** **Enable URL Category and Reputation Filters(URL 범주 및 평판 필터 활성화)** 확인란을 선택합니다.

단계 **4** (선택 사항) 메시지에서 스팸과 악성코드를 평가할 때 URL 필터링을 제외하고 모든 콘텐츠 및 메시지 필터링을 제외할 URL 목록을 만들었으면 해당 목록을 선택합니다.

이 설정은 일반적으로 메시지가 안티스팸 또는 Outbreak Filter 처리를 우회하도록 하지 않습니다.

단계 **5** (선택 사항) 웹 상호작용 추적을 활성화합니다. 웹 상호작용 추적 , 429 페이지를 참조하십시오.

단계 **6** 변경 사항을 제출 및 커밋합니다.

해당 전제 조건을 충족했으며 Outbreak Filters 및 안티 스팸 방지를 이미 구성한 경우, 스팸 및 악의적인 URL의 고급 자동 탐지를 활용하기 위한 추가 구성이 필요하지 않습니다.

다음에 수행할 작업

- 메시지에 있는 URL의 평판을 기반으로 작업을 수행하려면 평판 또는 메시지의 URL 범주를 기반으로 작업 수행 , 432 페이지 섹션을 참조해 주십시오.
- 예를 들어 허용되는 사용 정책을 시행하기 위해 콘텐츠 및 메시지 필터의 URL 범주를 사용하려면 평판 또는 메시지의 URL 범주를 기반으로 작업 수행 , 432 페이지 섹션을 참조해 주십시오.

- 의심스런 스팸 메시지의 모든 URL을 Cisco Web Security 프록시 서비스로 리디렉션하는 방법은 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예 , 366 페이지 섹션을 참조하십시오.
- (선택 사항) 최종 사용자 알림 페이지의 모양을 맞춤화하려면 엔드 유저에게 사이트가 악의적인지 여부를 표시하는 알림 맞춤화 , 431 페이지 섹션을 참조해 주십시오.
- 이러한 기능과 관련된 문제에 대한 경고문을 수신하는지 확인합니다. 향후 URL 범주 집합 변경 , 459 페이지, AsyncOS 릴리스에 대한 릴리스 정보 및 알림 수신자 추가, 964 페이지 섹션을 참조해 주십시오.

Cisco Web Security Services에 대한 연결 정보

URL 평판 및 범주는 클라우드 기반 Cisco Web Security Services에 의해 제공됩니다.

Email Security Appliance는 방화벽 정보, 1227 페이지의 URL 필터링 서비스에 대해 지정된 포트를 사용하여 직접 또는 웹 프록시를 통해 Cisco Web Security Services에 연결합니다. 통신은 상호 인증서 인증으로 HTTPS를 통해 수행됩니다. 인증서는 자동으로 업데이트됩니다(서비스 업데이트 , 945 페이지 참조). 필수 인증서에 대한 자세한 내용은 URL 필터링 기능에 대한 인증서 , 428 페이지에 지정된 위치에서 이용할 수 있는 릴리스 정보를 참조해 주십시오.

Security Services(보안 서비스**) > Service Updates(**서비스 업데이트**)** 페이지에서 HTTP 또는 HTTPS 프록시가 구성된 경우 Email Security Appliance는 Cisco Web Security Services와 통신할 때 이를 사용합니다. 프록시 서버 사용에 대한 자세한 내용은 업그레이드 및 업데이트 다운로드를 위한 서버 설정 구성 , 949 페이지 섹션을 참조해 주십시오.

참고 인증서는 구성 파일과 함께 저장되지 않습니다.

관련 주제

- URL 필터링 기능에 대한 인증서 , 428 페이지
- 경고문: SDS: 등록 인증서 가져오기 오류 , 442 페이지
- 경고문: SDS: 인증서가 유효하지 않음 , 442 페이지

URL 필터링 기능에 대한 인증서

AsyncOS는 URL 필터링 기능에 사용되는 클라우드 서비스로 통신에 필요한 인증서를 자동으로 배포 및 업데이트하도록 설계되었습니다. 그러나 어떤 이유로든 시스템이 이러한 인증서를 업데이트할 수 없는 경우 직접 작업을 해야 한다는 경고문이 전송됩니다.

이러한 경고문(System 유형, Warning 심각도)을 전송할 수 있도록 어플라이언스를 구성해야 합니다. 자세한 내용은 알림, 962 페이지 섹션을 참조해 주십시오.

잘못된 인증서에 대한 경고문을 받은 경우 Cisco TAC에 문의하면 필요한 교체 인증서를 받을 수 있습니다. 교체 인증서 사용에 대한 지침은 Cisco Web Security Services와의 통신을 위해 수동으로 인증서 구성 , 445 페이지섹션을 참조해 주십시오.

웹 상호작용 추적

웹 상호작용 추적 기능은 재작성된 URL을 클릭하고 각 사용자 클릭과 관련된 작업(허용됨, 차단됨 또는 알 수 없음)을 수행한 최종 사용자에 대한 정보를 제공합니다. 이 기능을 활성화하면 Web Interaction Tracking(웹 상호작용 추적) 보고서를 사용하여 클릭 수 상위 악의적인 URL, 악의적인 URL 클릭 수 상위 사용자 등의 정보를 볼 수 있습니다. Web Interaction Tracking(웹 상호작용 추적) 보고서에 대한 자세한 내용은 Web Interaction Tracking(웹 상호 작용 추적) 페이지, 819 페이지 섹션을 참조해 주십시오.

웹 상호작용 추적 데이터는 Cisco Aggregator Server에 의해 제공됩니다.

관련 주제

- 웹 상호작용 추적 구성, 429 페이지
- Cisco Aggregator Server에 대한 연결 정보, 429 페이지

웹 상호작용 추적 구성

요구 사항에 따라 전역 설정 페이지 중 하나에서 웹 상호작용 추적을 활성화할 수 있습니다.

- **Outbreak Filter**. Outbreak Filter에 의해 재작성된 URL을 클릭한 최종 사용자를 추적합니다. Outbreak Filter 전역 설정 구성, 411 페이지를 참조하십시오.
- **URL Filtering(URL 필터링)**. 정책에 의해 재작성된(콘텐츠 및 메시지 필터 사용) URL을 클릭한 최종 사용자를 추적합니다. URL 필터링 활성화, 427 페이지를 참조하십시오.

Cisco Aggregator Server에 대한 연결 정보

Email Security Appliance는 방화벽 정보, 1227 페이지의 URL 필터링 서비스에 대해 지정된 포트를 사용하여 30분마다 직접 또는 웹 프록시를 통해 Cisco Aggregator Server에 연결합니다(구성할 수 없음). 통신은 상호 인증서 인증으로 HTTPS를 통해 수행됩니다. 인증서는 자동으로 업데이트됩니다(서비스 업데이트 , 945 페이지 참조).

Security Services(보안 서비스) > **Service Updates(서비스 업데이트)** 페이지에서 HTTP 또는 HTTPS 프록시가 구성된 경우 Email Security Appliance는 Cisco Aggregator Server와 통신할 때 이를 사용합니다. 프록시 서버 사용에 대한 자세한 내용은 업그레이드 및 업데이트 다운로드를 위한 서버 설정 구성 , 949 페이지 섹션을 참조해 주십시오.

참고 인증서는 구성 파일과 함께 저장되지 않습니다.

클러스터 구성의 URL 필터링

- 시스템, 그룹 또는 클러스터 레벨에서 URL 필터링을 활성화할 수 있습니다.
- URL 필터링이 시스템 레벨에서 활성화된 경우, URL 화이트리스트 및 웹 상호작용 추적을 시스템, 그룹 또는 클러스터 레벨에서 구성할 수 있습니다.

- URL 필터링이 그룹 레벨에서 활성화된 경우, URL 화이트리스트 및 웹 상호작용 추적을 그룹 또는 클러스터 레벨에서 구성해야 합니다.
- URL 필터링이 클러스터 레벨에서 활성화된 경우, URL 화이트리스트 및 웹 상호작용 추적을 클러스터 레벨에서 구성해야 합니다.
- 메시지 필터 및 콘텐츠 필터에 대한 클러스터의 표준 규칙이 적용됩니다.

URL 필터링용 화이트리스트 만들기

URL 필터링 기능을 구성할 때 전역 화이트리스트를 지정하면 화이트리스트의 URL에 대해서는 평판이나 범주, 안티스팸, Outbreak Filter, 콘텐츠 및 메시지 필터링 등이 평가되지 않습니다. 그러나 이러한 URL을 포함하는 메시지는 안티 스팸 검사와 Outbreak Filter에 의해 일반적으로 평가됩니다. 각 URL 필터링 조건(규칙)에서 URL 화이트리스트를 지정하고 콘텐츠 및 메시지 필터에서 작업을 지정하여 전역 URL 화이트리스트를 보완할 수 있습니다.

일반적으로 Outbreak Filter에서 URL을 화이트리스트에 추가하려면 Mail Policies(메일 정책) > Outbreak Filters 페이지에서 구성하는 Bypass Domain Scanning(도메인 검사 우회) 옵션을 사용합니다. URL 필터링용 URL 화이트리스트는 도메인 검사 우회와 유사하지만 의존적이지는 않습니다. 이 기능에 대한 자세한 내용은 URL 재작성 및 도메인 우회, 418 페이지 섹션을 참조하십시오.

이 섹션에서 설명한 URL 필터링 화이트리스트와 SBRS 점수 기반의 발신자 평판 필터링에 사용되는 화이트리스트 사이에는 아무런 관계도 없습니다.

시작하기 전에

웹 인터페이스에서 만드는 대신 URL 목록을 가져오는 것을 고려해보십시오. URL 리스트 가져오기, 431 페이지를 참조하십시오.

단계 1 **Mail Policies(메일 정책) > URL Lists(URL 리스트)**를 선택합니다.

단계 2 **Add URL List(URL 리스트 추가)**를 선택하거나 수정할 리스트를 클릭합니다.

전역적으로 화이트리스트에 추가하려는 모든 URL은 단일 리스트에 있어야 합니다. URL 필터링에 하나의 전역 화이트리스트만 선택할 수 있습니다.

단계 3 리스트를 만들고 제출합니다.

지원되는 URL 형식 목록을 보려면 **URLs** 상자에 세미콜론(;)을 입력하고 **Submit(제출)**을 클릭합니다. 그런 다음 나타나는 **more(더 보기)...** 링크를 클릭합니다.

각 URL, 도메인 또는 IP 주소는 별도의 줄에 두거나 쉼표로 각각을 구분할 수 있습니다.

단계 4 변경 사항을 커밋합니다.

다음에 수행할 작업

- URL 리스트를 전역 화이트리스트로서 지정하려면 URL 필터링 활성화, 427 페이지 섹션을 참조해 주십시오.

- URL 리스트를 콘텐츠 또는 메시지 필터의 특정 조건(규칙) 또는 작업에 대한 화이트리스트로서 지정하려면 평판 또는 메시지의 URL 범주를 기반으로 작업 수행 , 432 페이지 및 콘텐츠 필터 작업, 293 페이지 섹션을 참조해 주십시오. 메시지 필터에 대한 자세한 내용은 URL 범주 작업 , 228 페이지 및 URL Category(URL 범주) 규칙 , 189 페이지 섹션을 참조해 주십시오.

관련 주제

- URL 리스트 가져오기 , 431 페이지

URL 리스트 가져오기

URL 필터링용 화이트리스트로서 사용할 URL 리스트를 가져올 수 있습니다.

단계 **1** 가져올 텍스트 파일을 만듭니다.

- 첫 번째 줄은 URL 리스트의 이름이어야 합니다.
- 각 URL을 별도의 줄에 두어야 합니다.

단계 **2** 파일을 어플라이언스의 `/configuration` 디렉터리에 업로드합니다.

단계 **3** CLI의 `urllistconfig > new` 명령을 사용합니다.

엔드 유저에게 사이트가 악의적인지 여부를 표시하는 알림 맞춤화

Outbreak Filtering(보안 침해 필터링) 또는 정책(콘텐츠 필터 또는 메시지 필터 사용)으로 식별한 악의적인 URL을 엔드 유저가 클릭하면, Cisco Web Security Proxy는 엔드 유저의 웹 브라우저에 알림을 표시합니다. 이 알림은 해당 사이트가 악의적인 사이트이며 액세스가 차단되었음을 알립니다.

엔드 유저가 Outbreak Filtering(보안 침해 필터링)을 사용하여 재작성된 URL을 클릭하면 10초 동안 알림 페이지가 표시된 다음 클릭 시 평가를 위해 Cisco Web Security Proxy로 리디렉션됩니다.

이 알림 페이지의 모양을 맞춤화하고 조직의 브랜드(예: 회사 로고, 연락처 정보 등)를 표시할 수 있습니다.

참고 알림 페이지를 맞춤화하지 않으면 최종 사용자에게 Cisco 브랜드 알림 페이지가 표시됩니다.

시작하기 전에

- URL 필터링을 활성화합니다. URL 필터링 활성화, 427 페이지를 참조하십시오.

단계 **1** **Security Services(보안 서비스) > Block Page Customization(페이지 맞춤화 차단)**을 선택합니다.

단계 **2** **Enable(활성화)**을 클릭합니다.

단계 **3** **Enable Block Page customization(차단 페이지 맞춤화 활성화)** 확인란을 선택하고 다음 세부사항을 입력합니다.

- 조직 로고의 URL. 로고 이미지는 공개적으로 액세스 가능한 서버에 호스팅하는 것이 좋습니다.
- 조직의 이름
- 조직의 연락처 정보

단계 **4** 알림의 언어를 선택합니다. 웹 인터페이스에서 지원하는 언어는 어떤 것이든 선택할 수 있습니다.

참고 최종 사용자 브라우저의 기본 언어가 여기에서 선택한 언어보다 우선권을 갖습니다. 또한 최종 사용자 브라우저의 기본 언어가 AsyncOS에서 지원되지 않는 경우, 여기서 선택한 언어로 알림이 표시됩니다.

단계 **5** (선택 사항) **Preview Block Page Customization(**차단 페이지 사용자 지정 미리 보기**)** 링크를 클릭하여 알림 페이지를 미리 봅니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

다음 단계

다음 방법 중 하나로 URL 재작성을 설정합니다.

- Outbreak Filter 사용. URL 리디렉션, 403 페이지를 참조하십시오.
- 콘텐츠 또는 메시지 필터 사용 평판 또는 메시지의 URL 범주를 기반으로 작업 수행 , 432 페이지를 참조하십시오.

평판 또는 메시지의 URL 범주를 기반으로 작업 수행

수신 및 발신 메일 정책의 메시지 필터 및 콘텐츠 필터를 사용하여 평판 또는 메시지 본문 및 메시지 첨부 파일의 URL 링크 카테고리를 기반으로 작업을 수행할 수 있습니다.

Outbreak Filter는 메시지에서 악성코드를 평가할 때 많은 요인을 고려하며 URL 평판은 단독으로 적극적인 메시지 처리를 트리거하지 못할 수 있으므로, URL 평판을 기반으로 필터를 만들 수 있습니다.

예를 들면 다음을 위해 URL 필터를 만들 수 있습니다.

- (메시지 본문의 URL에만 해당) Neutral이거나 알 수 없는 평판의 URL을 재작성하여 클릭 시 평가를 위한 Cisco Cloud Web Security 프록시 서비스로 리디렉션합니다.
- Malicious(악성) 범위에 평판 점수가 있는 URL을 포함하는 메시지를 삭제합니다.

URL 범주 필터를 사용하여 다음을 수행할 수 있습니다.

- 허용되는 웹 사용에 대한 조직 정책(예: 사무실에서 근무하는 동안 성인 사이트 또는 도박 사이트 방문 금지)을 시행하기 위해 URL 범주를 필터링합니다.
- 악의적인 사이트(분류할 수 있을 만큼 길게 존재하지 않을 수 있음)에 대한 고급 보안 기능을 제공합니다. (메시지 본문의 URL에만 해당) Unclassified(미분류) 카테고리의 모든 URL을 사용자가 링크를 클릭할 때 평가하기 위한 Cisco Cloud Web Security 프록시 서비스로 리디렉션할 수 있습니다.

관련 주제

- URL 관련 조건(규칙) 및 작업 사용 , 433 페이지
- URL 평판 또는 URL 범주 필터링: 조건 및 규칙 , 433 페이지

• 메시지의 URL 수정: URL 평판 및 필터의 URL 범주 작업 사용 , 434 페이지
• 리디렉션된 URL: 최종 사용자가 경험하는 내용 , 436 페이지

URL 관련 조건(규칙) 및 작업 사용

하려는 작업	예	수행해야 할 작업
전체적으로 메시지에 대한 작업을 수행합니다.	메시지를 삭제 또는 격리합니다.	URL 평판 또는 URL 범주 조건이나 규칙을 만든 다음, URL 평판 또는 URL 범주 작업 이외의 작업과 페어링합니다. 예외: URL 평판 조건 또는 규칙을 반송 작업과 페어링하지 마십시오.
(메시지 본문의 URL에만 해당) 메시지의 URL을 수정하거나 동작을 수정합니다.	메시지의 URL을 텍스트 메모와 교체하거나 URL을 클릭할 수 없게 만듭니다.	URL 평판 또는 URL 범주 작업만 만듭니다. 별도의 URL 필터링 조건을 사용하지 마십시오.

늘 그렇듯이, 사용하려면 메일 정책에서 콘텐츠 필터를 지정해야 합니다.

관련 주제

• URL 평판 또는 URL 범주 필터링: 조건 및 규칙 , 433 페이지
• 메시지의 URL 수정: URL 평판 및 필터의 URL 범주 작업 사용 , 434 페이지

URL 평판 또는 URL 범주 필터링: 조건 및 규칙

메시지 본문 및 메시지 첨부 파일의 평판 또는 URL 카테고리를 기반으로 메시지에 대한 작업을 수행할 수 있습니다. URL 또는 해당 동작을 수정하는 것 이외의 작업을 수행하려면 **URL** 평판 또는 **URL** 카테고리 조건을 추가하고 평판 점수 또는 작업을 적용할 URL 카테고리를 선택합니다.

예를 들어 Adult(성인) 범주의 URL을 포함하는 모든 메시지에 대해 **Drop (Final Action)**(삭제(최종 작업)) 작업을 적용하려면, 선택한 **Adult**(성인) 범주와 함께 **URL Category**(URL 범주) 유형 조건을 추가합니다.

범주를 지정하지 않으면 선택한 작업이 모든 메시지에 적용됩니다.

정상 URL, 중립 URL 및 악의적 URL에 대한 URL 평판 점수 범위는 미리 정의되어 있으며 편집할 수 없습니다. 그러나 대신 맞춤화 범위를 지정할 수 있습니다. 지정된 엔드포인트가 지정한 범위에 포함됩니다. 예를 들어 -8 ~ -10의 맞춤화 범위를 만들면 -8 ~ -10이 범위에 포함됩니다. 평판 점수를 확인할 수 없는 URL에는 "No Score(점수 없음)"를 사용합니다.

참고 중립 URL 평판은 공격에 취약하기 때문에 현재 URL은 정상이지만 나중에 악성이 될 수 있음을 의미합니다. 그러한 URL의 경우, 관리자가 비차단 정책을 만들 수 있습니다. 예를 들어, 클릭 시 평가를 위해 Cisco Web Security 프록시로 리디렉션할 수 있습니다.

선택한 URL 화이트리스트 또는 전역 URL 화이트리스트에 포함된 URL은 평가되지 않습니다.

메시지에 있는 URL이 평판 점수 또는 조건에 지정된 범주와 일치하면 이 조건과 페어링하는 작업이 수행됩니다.

메시지의 URL을 수정하거나 해당 동작을 수정하려면 URL 평판 또는 URL 범주 작업만 구성합니다. 이를 위한 별도의 URL 평판 또는 URL 범주 조건이나 규칙은 필요하지 않습니다.

참고 URL 평판 조건을 반송 작업과 페어링하지 마십시오.

팁 특정 URL의 범주를 확인하려면 분류되지 않은 URL 또는 잘못 분류된 URL 보고 , 459 페이지의 링크를 방문해 주십시오.

관련 주제

- URL 필터링용 화이트리스트 만들기 , 430 페이지
- 콘텐츠 필터, 283 페이지
- URL Reputation(URL 평판) 규칙 , 188 페이지
- URL Category(URL 범주) 규칙 , 189 페이지

메시지의 URL 수정: URL 평판 및 필터의 URL 범주 작업 사용

URL의 평판 또는 범주를 기반으로 메시지의 URL 또는 해당 동작을 수정하려면 URL 평판 또는 URL 범주 작업을 사용합니다.

URL 평판 및 URL 범주 작업에는 별도의 조건이 필요하지 않습니다. 대신, 선택한 작업은 URL 평판 또는 URL 범주 작업에서 선택하는 평판 또는 범주를 기반으로 적용됩니다.

해당 작업은 작업에 지정된 기준을 충족하는 URL에만 적용됩니다. 메시지의 기타 URL은 수정되지 않습니다.

범주를 지정하지 않으면 선택한 작업이 모든 메시지에 적용됩니다.

정상 URL, 중립 URL 및 악의적 URL에 대한 URL 평판 점수 범위는 미리 정의되어 있으며 편집할 수 없습니다. 그러나 대신 맞춤화 범위를 지정할 수 있습니다. 지정된 엔드포인트가 지정한 범위에 포함됩니다. 예를 들어 -8 ~ -10의 맞춤화 범위를 만들면 -8 ~ -10이 범위에 포함됩니다. 평판 점수를 확인할 수 없는 URL에는 "No Score(점수 없음)"를 사용합니다.

참고 중립 URL 평판은 공격에 취약하기 때문에 현재 URL은 정상이지만 나중에 악성이 될 수 있음을 의미합니다. 그러한 URL의 경우, 관리자가 비차단 정책을 만들 수 있습니다. 예를 들어, 클릭 시 평가를 위해 Cisco Web Security 프록시로 리디렉션할 수 있습니다.

다음 URL 관련 작업은 메시지 본문의 URL에만 해당합니다.

- 클릭할 수 없도록 URL을 무효화합니다. 메시지 수신자는 여전히 URL을 보고 복사할 수 있습니다.
- 메시지 수신자가 링크를 클릭하면, 사이트가 악의적인 경우 액세스를 차단하는 클라우드의 Cisco Web Security Proxy로 트랜잭션이 라우팅되도록 URL을 리디렉션합니다.

  예: 피싱 공격에 사용되는 악의적인 사이트는 종종 분류할 수 있을 정도로 오래 존재하지 않으므로 **Uncategorized(**미분류**)** 카테고리의 모든 URL을 Cisco Cloud Web Security Proxy Service로 리디렉션할 수 있습니다.

  리디렉션된 URL: 최종 사용자가 경험하는 내용 , 436 페이지도 참조하십시오.

  URL을 다른 프록시로 리디렉션하려면 다음 불릿의 예를 참조해 주십시오.

  참고 Cisco Cloud Web Security 프록시 서비스에는 이 릴리스에서 구성 가능한 옵션이 없습니다. 예를 들면 조정할 점수 임계값 또는 위협 점수를 기반으로 지정할 작업이 없습니다.

- URL을 텍스트로 교체합니다.

  메시지에 나타나는 텍스트에 원래 URL을 포함하려면 $URL 변수를 사용합니다.

  예:

  - **Illegal Downloads(**불법 다운로드**)** 범주의 모든 URL을 다음과 같은 메모로 교체합니다.

    ```
    Message from your system administrator: A link to an illegal downloads web site has
    been removed from this message.
    ```

  - 경고와 함께 원래 URL을 포함합니다.

    ```
    WARNING! The following URL may contain malware: $URL
    ```

    다음으로 변경됨: WARNING: The following URL may contain malware: http://example.com.

  - 맞춤화 프록시 또는 웹 보안 서비스로 리디렉션합니다.

    ```
    http://custom_proxy/$URL
    ```

    다음으로 변경됨: http://custom_proxy/http://example.com

선택한 URL 화이트리스트 또는 전역 URL 화이트리스트에 포함된 URL의 평판 및 범주는 평가되지 않습니다.

URL을 무효화 또는 교체하는 경우 서명된 메시지에서 URL을 무시하도록 선택할 수 있습니다.

URL 평판 또는 URL 범주 작업을 URL 평판 또는 URL 범주 조건(또는 규칙)과 페어링하는 것은 권장되지 않습니다. 조건(규칙)을 서로 다른 범주가 포함된 작업과 페어링하면 일치가 발생하지 않습니다.

팁 특정 URL의 범주를 확인하려면 분류되지 않은 URL 또는 잘못 분류된 URL 보고 , 459 페이지의 링크를 방문해 주십시오.

관련 주제

- URL 필터링용 화이트리스트 만들기 , 430 페이지
- 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예 , 366 페이지
- 콘텐츠 필터, 283 페이지
- URL Reputation(URL 평판) 규칙 , 188 페이지
- URL Category(URL 범주) 규칙 , 189 페이지

리디렉션된 URL: 최종 사용자가 경험하는 내용

Cisco Cloud Web Security 프록시 서비스에 의한 평가를 기준으로:

- 사이트가 정상인 경우 사용자는 대상 웹사이트로 리디렉션되며, 링크가 리디렉션된 것을 알지 못합니다.
- 사이트가 악의적인 경우 사용자에게 사이트가 악의적이며 액세스가 차단되었다는 알림이 표시됩니다.

  최종 사용자 알림 페이지의 모양을 맞춤화하고 조직의 브랜드(예: 회사 로고, 연락처 정보 등)를 표시할 수 있습니다. 엔드 유저에게 사이트가 악의적인지 여부를 표시하는 알림 맞춤화 , 431 페이지를 참조하십시오.

- Cisco Cloud Web Security Proxy Service와의 통신이 시간 초과되면 사용자는 대상 웹사이트에 액세스할 수 있게 됩니다.
- 오류가 발생하면 사용자에게 알림이 표시됩니다.

관련 주제

- 메시지의 URL 수정: URL 평판 및 필터의 URL 범주 작업 사용 , 434 페이지

URL 필터링을 위한 스캔할 수 없는 메시지 처리

다음 시나리오에서는 URL 필터링 검사에 실패하고 *X-URL-ScanningError* 헤더가 메시지에 추가됩니다.

- URL 평판 및 카테고리를 가져올 수 없음
- 메시지에서 단축 URL을 확장할 수 없음
- 메시지 본문 또는 메시지 첨부 파일의 URL 수가 최대 URL 검사 제한을 초과함

콘텐츠 필터를 추가하고, Other Header(기타 헤더) 조건에서 *X-URL-LookUp-ScanningError* 헤더를 선택한 후 메시지에 대해 수행할 적절한 작업을 구성할 수 있습니다.

단축 URL에 대한 URL 필터링 활성화

이제 단축 URL에 대한 URL 필터링을 수행하고 단축 URL에서 실제 URL을 검색하도록 어플라이언스를 구성할 수 있습니다. 원래 URL의 URL 평판 점수를 기반으로 단축 URL에서 구성된 URL 작업이 수행됩니다.

단축 URL은 실제 URL을 확인하기 위해 최대 10개의 중첩된 단축 URL 제한으로 리디렉션될 수 있습니다. 단축 URL이 최대 10개의 중첩된 단축 URL 제한을 초과하는 경우 기본적으로 URL 평판 점수 -10이 단축 URL에 할당됩니다.

어플라이언스에서 단축 URL에 대한 필터링을 활성화하려면 CLI에서 websecurityadvancedconfig 명령을 사용합니다.

시작하기 전에

- URL 필터링을 활성화합니다. URL 필터링 활성화, 427 페이지를 참조하십시오.
- 적절한 URL 평판 규칙 및 악성 URL에 대해 수행할 작업을 사용하여 콘텐츠 필터를 구성합니다.
- 어플라이언스에서 사용 가능한 단축 URL 도메인과의 연결을 설정할 수 있는지 확인합니다. 어플라이언스와 사용 가능한 단축 URL 도메인 간의 연결을 허용하려면 HTTP 프록시 서버 설정 또는 네트워크 방화벽 규칙을 확인합니다.

예: 단축 URL에 대한 URL 필터링 활성화

다음 예에서는 `websecurityadvancedconfig` 명령을 사용하여 단축 URL에 대한 URL 필터링을 활성화합니다.

```
mail.example.com> websecurityadvancedconfig

Enter URL lookup timeout (includes any DNS lookup time) in seconds:
[5]>

Enter the URL cache size (no. of URLs):
[810000]>

Do you want to disable DNS lookups? [N]>

Enter the maximum number of URLs that should be scanned:
[100]>

Enter the Web security service hostname:
[v2.sds.cisco.com]>

Enter the threshold value for outstanding requests:
[50]>

Do you want to verify server certificate? [Y]>

Do you want to enable URL filtering for shortened URLs? [Y]> yes

For shortened URL support to work, please ensure that ESA is able to connect to the following
 domains:
bit.ly, tinyurl.com, ow.ly, tumblr.com, post/ly ……
```

```
Enter the default time-to-live value (seconds):
[30]>

Do you want to rewrite both the URL text and the href in the message? Y indicates that the
 full rewritten URL will appear in the email body.
N indicates that the rewritten URL will only be visible in the href for HTML messages. [N]>

Do you want to include additional headers? [N]>

Enter the default debug log level for RPC server:
[Info]>

Enter the default debug log level for URL cache:
[Info]>

Enter the default debug log level for HTTP client:
[Info]>
```

콘텐츠 필터를 사용하여 메시지에서 악성 URL 탐지

'URL 평판' 콘텐츠 필터를 사용하여 ETF 엔진에서 악성으로 분류된 URL을 탐지하고 해당 메시지에 대해 적절한 작업을 수행합니다.

다음 방법 중 하나로 ETF에 대한 'URL 평판' 콘텐츠 필터를 구성할 수 있습니다.

- 적절한 작업이 포함된 'URL 평판' 조건을 사용합니다.
- 조건에 상관없이 'URL 평판' 작업을 사용합니다.
- 'URL 평판' 조건 및 작업을 사용합니다.

다음 절차는 'URL 평판' 조건 및 작업을 사용하여 악성 URL을 탐지하는 데 사용됩니다.

참고

- 적절한 작업이 포함된 'URL 평판' 조건만 사용하려는 경우 절차의 11~20단계를 수행하지 마십시오.
- 조건에 상관없이 'URL 평판' 작업만 사용하려면 경우 절차의 4~10단계를 수행하지 마십시오.

시작하기 전에

- Cisco Email Security 게이트웨이에서 URL 필터링을 활성화해야 합니다. URL 필터링을 활성화하려면 웹 인터페이스에서 *Security Services* > *URL Filtering(URL* 필터링*)* 페이지로 이동합니다. 자세한 내용은 악의적이거나 바람직하지 않은 URL로부터 보호, 425 페이지의 내용을 참고하십시오.
- Cisco Email Security 게이트웨이에서 보안 침해 필터를 활성화해야 합니다. 보안 침해 필터를 활성화하려면 웹 인터페이스에서 *Security Services* > *Outbreak Filters(*보안 침해 필터*)* 페이지로 이동합니다. 자세한 내용은 신종 바이러스 필터(Outbreak Filter), 399 페이지의 내용을 참고하십시오.

- Cisco Email Security 게이트웨이에서 안티스팸 엔진을 활성화해야 합니다. 안티스팸 엔진을 활성화하려면 웹 인터페이스의 *Security Services* > *Anti-Spam(*안티스팸*)* 페이지로 이동합니다. 자세한 내용은 Anti-Spam, 355 페이지의 내용을 참고하십시오.
- (선택 사항) URL 목록을 생성합니다. 웹 인터페이스에서 *Mail Polices(Mail* 정책*)* > *URL Lists(URL* 목록*)* 페이지로 이동합니다. 자세한 내용은 악의적이거나 바람직하지 않은 URL로부터 보호, 425 페이지의 내용을 참고하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Content Filters(**수신 콘텐츠 필터**)**로 이동합니다.

단계 **2** **Add Filter(**필터 추가**)**를 클릭합니다.

단계 **3** 콘텐츠 필터의 이름과 설명을 입력합니다.

단계 **4** **Add Condition(**조건 추가**)**을 클릭합니다.

단계 **5** **URL Reputation(URL** 평판**)**을 클릭합니다.

단계 **6** **External Threat Feeds(**외부 위협 피드**)**를 선택합니다.

단계 **7** 악성 URL을 탐지할 ETF 소스를 선택합니다.

단계 **8** (선택 사항) Cisco Email Security 게이트웨이가 위협을 탐지하지 않도록 하려면 화이트리스트에 있는 URL 목록을 선택합니다.

단계 **9** 메시지 본문 및 제목 및/또는 메시지 첨부 파일에서 악성 URL을 탐지하려면 필수 **Check URLs within(**다음 범위 내에서 **URL** 확인**)** 옵션을 선택합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Add Action(**작업 추가**)**을 클릭합니다.

단계 **12** **URL Reputation(URL** 평판**)**을 클릭합니다.

단계 **13** **External Threat Feeds(**외부 위협 피드**)**를 선택합니다.

단계 **14** 조건에서 선택한 것과 동일한 ETF 소스를 선택해야 합니다(7단계).

단계 **15** (선택 사항) 8단계에서 선택한 화이트리스트 URL과 동일한 목록을 선택합니다.

단계 **16** '메시지 본문 및 제목' 및/또는 '메시지 첨부 파일'에서 악성 URL을 탐지하려면 필수 **Check URLs within(**다음 범위 내에서 **URL** 확인**)** 옵션을 선택합니다.

단계 **17** 메시지 본문 및 제목 및/또는 메시지 첨부 파일 내의 URL에 대해 수행할 필수 작업을 선택합니다.

참고 16단계에서 'Check URLs within(다음 범위 내에서 URL 확인)' 옵션을 'Attachments(첨부 파일)'로 선택한 경우 메시지에서 첨부 파일만 제거할 수 있습니다.

단계 **18** 모든 메시지 또는 서명되지 않은 메시지에 대해 작업을 수행할지 여부를 선택합니다.

단계 **19** **OK(**확인**)**를 클릭합니다.

단계 **20** 변경 사항을 제출 및 커밋합니다.

참고 어플라이언스에서 WBRS(웹 기반 평판 점수) 및 ETF에 대한 URL 평판 콘텐츠 필터를 구성한 경우, 어플라이언스의 성능을 높이기 위해 WBRS URL 평판 콘텐츠 필터의 순서를 ETF URL 평판 필터보다 높게 설정하는 것이 좋습니다.

메시지 필터를 사용하여 메시지에서 악성 **URL** 탐지

예를 들어, ETF 엔진을 사용하여 메시지에서 악성 URL을 탐지하고 해당 URL을 차단하려면 'URL 평판' 메시지 필터 규칙 구문을 사용합니다.

구문:

```
 defang_url_in_message: if (url-external-threat-feeds (['etf_source1'],
 <'URL_whitelist'>,
<'message_attachments'> , <'message_body_subject'> ,))
 { url-etf-defang(['etf-source1'], "", 0); } <'URL_whitelist'> ,
<'Preserve_signed'>)}
```

어디에서

- '`url-external-threat-feeds`'는 URL 평판 규칙입니다.
- '`etf_source1`'은 메시지 또는 메시지 첨부 파일에서 악성 URL을 탐지하는 데 사용되는 ETF 소스입니다.
- '`URL_whitelist`'는 URL 화이트리스트의 이름입니다. URL 화이트리스트가 없으면 ""로 표시됩니다.
- '`message_attachments`'는 메시지 첨부 파일에서 악성 URL을 확인하는 데 사용됩니다. 값 '1'은 메시지 첨부 파일에서 악성 URL을 탐지하는 데 사용됩니다.
- '`message_body_subject`'는 메시지 본문 및 제목에서 악성 URL을 확인하는 데 사용됩니다. 값 '1'은 메시지 본문 및 제목에서 악성 URL을 탐지하는 데 사용됩니다.

  참고 값 "1,1"은 메시지 본문, 제목 및 메시지 첨부 파일에서 악성 URL을 탐지하는 데 사용됩니다.

- '`url-etf-defang`'은 악성 URL이 포함된 메시지에 대해 수행할 수 있는 작업 중 하나입니다.

  다음 예는 악성 URL이 포함된 메시지에 적용할 수 있는 ETF 기반 작업입니다.

  - url-etf-strip(['etf_source1'], "None", 1)
  - url-etf-defang-strip(['etf_source1'], "None", 1, "Attachment removed")
  - url-etf-defang-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1, " Attachment removed")
  - url-etf-replace(['etf_source1'], "", "None", 1)
  - url-etf-replace(['etf_source1'], "URL removed", "None", 1)

- url-etf-replace-strip(['etf_source1'], "URL removed ", "None", 1)
- url-etf-replace-strip(['etf_source1'], "URL removed*", "None", 1, "Attachment removed")

- `'Preserve_signed'`는 '1' 또는 '0'으로 표시됩니다. '1'은 이 작업이 서명되지 않은 메시지에만 적용됨을 나타내고 '0'은 이 작업이 모든 메시지에 적용됨을 나타냅니다.

다음 예에서는 메시지 첨부 파일의 URL이 ETF 엔진에서 악성으로 탐지된 경우 해당 첨부 파일이 제거됩니다.

```
Strip_Malicious_URLs: if (true) {url-etf-strip(['threat_feed_source'], "", 0);}
```

URL 필터링 결과 모니터링

악성 및 중립적 URL에 대해 탐지된 데이터를 보려면 **Monitor(모니터)** > **URL Filtering(URL 필터링)**을 선택합니다. 이 페이지의 데이터에 대한 자세한 내용은 URL Filtering(URL 필터링) 페이지 , 818 페이지 섹션을 참조해 주십시오.

메시지 추적에서 URL 세부 정보 표시

보안 침해 필터 및 관련 콘텐츠 필터에 걸린 URL에 대한 메시지 추적의 세부 정보를 표시하려는 경우:

- 메시지 추적을 활성화해야 합니다.
- URL 평판 또는 URL 카테고리를 기반으로 보안 침해 필터 및/또는 콘텐츠 필터를 작동해야 합니다.
- 보안 침해 필터에 대한 URL 재작성을 활성화해야 합니다. URL 재작성 및 도메인 우회, 418 페이지를 참조하십시오.
- URL 로깅을 활성화해야 합니다. URL 로깅 및 URL의 메시지 추적 세부 정보 활성화 , 412 페이지를 참조하십시오.

표시되는 데이터에 대한 자세한 내용은 메시지 추적 세부 정보 , 842 페이지 섹션을 참조하십시오.

이러한 민감한 정보에 대한 관리 사용자 액세스를 관리하려면 메시지 추적 시 중요 정보의 액세스 제어, 898 페이지 섹션을 참조하십시오.

URL 필터링 트러블슈팅

관련 주제

- 로그 보기 , 442 페이지
- 경고문: SDS: 등록 인증서 가져오기 오류 , 442 페이지
- 경고문: SDS: 인증서가 유효하지 않음 , 442 페이지
- Cisco Web Security Services에 연결할 수 없음, 443 페이지

로그 보기

URL 필터링 정보가 다음 로그에 게시됩니다.

- 메일 로그(mail_logs). URL 검사 결과와 관련된 정보(URL에 따라 메시지에 수행된 작업)가 이 로그에 게시됩니다.
- URL 필터링 로그(web_client). URL 조회를 시도하는 동안 오류, 시간 초과, 네트워크 문제 등과 관련된 정보가 이 로그에 게시됩니다.

대부분의 정보는 Info(정보) 또는 Debug(디버그) 레벨입니다.

사용자가 메시지의 리디렉션된 링크를 클릭할 때 발생하는 일에 대한 정보는 로그에 포함되지 않습니다.

로그의 "SDS"는 URL 평판 서비스를 가리킵니다.

경고문: SDS: 등록 인증서 가져오기 오류

문제

등록 클라이언트 인증서 가져오기 오류에 대한 정보 레벨 경고문을 수신합니다.

솔루션

클라우드 기반 서비스인 Cisco Web Security Services(URL 평판 및 범주 가져오기) 및 Cisco Aggregator Server(웹 상호작용 추적 데이터 가져오기)에 연결하는 데 이 인증서가 필요합니다. 다음과 같이 해보십시오.

1. 부정확한 프록시 설정 또는 방화벽 문제와 같은 네트워킹 문제를 확인합니다.
2. URL 필터링 기능 키가 유효하며 활성 상태인지 확인합니다.
3. 문제가 계속되면 Cisco TAC에 문의해 주십시오.

경고문: SDS: 인증서가 유효하지 않음

문제

유효하지 않은 SDS 인증서에 대한 중요한 경고문을 수신합니다.

솔루션

이 인증서는 URL 평판 및 범주를 가져오기 위해 클라우드의 Cisco Web Security Services에 연결하는 데 필요합니다.

인증서를 가져와서 수동으로 설치하려면 Cisco Web Security Services와의 통신을 위해 수동으로 인증서 구성 , 445 페이지 섹션을 참조해 주십시오.

Cisco Web Security Services에 연결할 수 없음

문제

Security Services(보안 서비스**) > URL Filtering(URL** 필터링**)** 페이지에 지속적으로 Cisco Web Security Services 연결 문제가 나타납니다.

솔루션

- URL 필터링을 활성화했지만 변경 사항을 커밋하지 않은 경우 변경 사항을 커밋합니다.
- Cisco Web Security Services와의 연결과 관련된 최신 경고를 확인합니다. 최근 알림 보기, 966 페이지를 참조하십시오. 해당되는 경우 경고문: SDS: 등록 인증서 가져오기 오류 , 442 페이지 및 경고문: SDS: 인증서가 유효하지 않음 , 442 페이지 섹션을 참조해 주십시오.
- **Security Services > Service Updates(**서비스 업데이트**)**에 지정된 프록시를 통해 연결 중인 경우, 제대로 구성되어 작동되는지 확인합니다.
- 연결을 방해할 수 있는 기타 네트워크 문제를 확인합니다.
- SDS 클라이언트에 대한 시간 초과된 요청과 관련된 URL 필터링 로그에 오류가 있는 경우, sent 1-12 CLI에서 websecuritydiagnostics 명령 및 **`websecurityadvancedconfig`** 명령을 사용하여 확인하고 변경합니다.
  - Response Time(응답 시간) 또는 DNS Lookup Time(DNS 조회 시간)이 구성된 URL Lookup Timeout(URL 조회 시간 초과)보다 작지 않은 것으로 진단에 표시되면, URL Lookup Timeout(URL 조회 시간 초과) 값을 적절히 올립니다.
  - 캐시 크기가 고급 컨피그레이션 설정에 지정된 용량과 같거나 비슷한 것으로 진단에 표시되면 캐시 크기를 올립니다.
- URL 스캐너, Cisco Web Security Services 또는 SDS와의 통신에서 시간 초과 이외의 오류가 있는지를 URL 필터링 로그에서 확인합니다. 로그의 "SDS"는 Cisco Web Security Services를 나타냅니다. 그런 로그 메시지가 표시되면 TAC에 문의해 주십시오.

경고문: Cisco Aggregator Server에 연결할 수 없음

문제

Unable to Connect to the Cisco Aggregator Server(Cisco Aggregator Server에 연결할 수 없음)와 같은 경고 알림이 표시됩니다.

솔루션

다음을 수행합니다.

1. 어플라이언스에서 서버의 호스트 이름을 ping하여 어플라이언스와 Cisco Aggregator Server 간 연결을 확인합니다. CLI의 aggregatorconfig 명령을 사용하여 Cisco Aggregator Server의 호스트 이름을 표시합니다.
2. Security Services(보안 서비스) > Service Updates(서비스 업데이트)에 지정된 프록시를 통해 연결 중인 경우, 제대로 구성되어 작동되는지 확인합니다.
3. 연결을 방해할 수 있는 기타 네트워크 문제를 확인합니다.
4. DNS 서비스가 실행 중인지 확인합니다.
5. 문제가 계속되면 Cisco TAC에 문의해 주십시오.

경고문: Cisco Aggregator Server에서 웹 상호작용 추적 정보를 검색할 수 없음

문제

Unable to retrieve web interaction tracking information from the Cisco Aggregator Server(Cisco Aggregator Server에서 웹 상호작용 추적 정보를 검색할 수 없음)와 같은 경고 알림이 표시됩니다.

솔루션

다음을 수행합니다.

1. **Security Services > Service Updates(**서비스 업데이트**)**에 지정된 프록시를 통해 연결 중인 경우, 제대로 구성되어 작동되는지 확인합니다.
2. 연결을 방해할 수 있는 기타 네트워크 문제를 확인합니다.
3. DNS 서비스가 실행 중인지 확인합니다.
4. 문제가 계속되면 Cisco TAC에 문의해 주십시오.

websecurityadvancedconfig 명령 사용

이 문서에 명시적으로 기술된 것 외에는 TAC의 안내 없이 websecurityadvancedconfig 명령을 사용하여 다른 내용을 변경하지 마십시오.

메시지 추적 검색에서 지정된 범주의 메시지를 찾을 수 없음

문제

특정 범주의 URL을 포함하는 메시지는 해당 범주로 검색할 경우 발견되지 않습니다.

솔루션

검색 결과에 예상 메시지가 누락됨 , 845 페이지를 참조하십시오.

악의적인 URL 및 마케팅 메시지가 안티스팸 또는 Outbreak Filter로 검색되지 않음

문제

악의적인 URL 및 마케팅 링크가 포함된 메시지는 안티스팸 또는 Outbreak Filter로 검색되지 않습니다.

솔루션

- 이는 안티스팸 및 Outbreak Filter가 판정을 위해 사용하는 기준이 여러 기준 중에서 웹사이트 평판과 범주, 이 두 가지 기준뿐이기 때문에 발생합니다. URL을 텍스트로 교체 또는 재작성하거나, 메시지를 격리 또는 삭제하는 등의 작업을 수행하는 데 필요한 임계값을 낮게 설정하여 이러한 필터의 민감도를 높일 수 있습니다. 자세한 내용은 Outbreak Filter 기능 및 메일 정책, 415 페이지 및 안티스팸 정책 정의 , 362 페이지 섹션을 참조해 주십시오. 또는 URL 평판 점수를 기반으로 콘텐츠 또는 메시지 필터를 만듭니다.
- 이 문제는 Email Security Appliance에서 Cisco Web Security Services에 연결할 수 없는 경우에도 발생할 수 있습니다. Cisco Web Security Services에 연결할 수 없음, 443 페이지를 참조하십시오.

필터링된 범주의 URL을 올바르게 처리할 수 없음

문제

URL 범주를 기반으로 콘텐츠 또는 메시지 필터에 정의된 작업이 적용되지 않습니다.

솔루션

- 추적 기능(트러블슈팅 장에서 설명)을 사용하여 메시지 처리 경로를 따릅니다.
- 이 문제는 Email Security Appliance에서 Cisco Web Security Services에 연결할 수 없는 경우에 발생할 수 있습니다. Cisco Web Security Services에 연결할 수 없음, 443 페이지를 참조하십시오.
- 연결 문제가 없는 경우 URL이 아직 범주화되지 않았거나 잘못 범주화되었을 수 있습니다. 분류되지 않은 URL 또는 잘못 분류된 URL 보고 , 459 페이지를 참조하십시오. 이 사이트를 사용하여 URL의 범주를 확인할 수 있습니다.

최종 사용자가 재작성된 URL을 통해 악의적인 사이트에 도달함

문제

악의적인 URL은 Cisco Web Security Proxy로 리디렉션되지만 최종 사용자가 사이트에 액세스하지 못했습니다.

솔루션

이 문제는 다음과 같은 경우 발생할 수 있습니다.

- 해당 사이트가 아직 악의적인 사이트로 식별되지 않았습니다.
- 매우 드물게 발생하는 일이지만, Cisco Web Security Proxy에 대한 연결이 시간 초과되었습니다. 네트워크 문제가 연결을 방해하지 않는지 확인하십시오.

Cisco Web Security Services와의 통신을 위해 수동으로 인증서 구성

어플라이언스가 Cisco Web Security Services와 통신하기 위한 인증서를 자동으로 가져올 수 없는 경우 다음 절차를 사용해 주십시오.

단계 1 필수 인증서를 가져옵니다.
단계 2 **Network(네트워크) > Certificates(인증서)** 또는 CLI의 certconfig 명령을 사용하여 인증서를 업로드합니다.
단계 3 CLI에서 **websecurityconfig** 명령을 입력합니다.
단계 4 프롬프트에 따라 Cisco Web Security Services Authentication용 클라이언트 인증서를 설정합니다.
단계 5 인증서 설치 프로세스가 완료되면 **webcacheflush** 명령을 입력합니다.

URL 범주 정보

관련 주제

- URL 카테고리 설명 , 446 페이지
- URL의 범주 확인 , 459 페이지
- 분류되지 않은 URL 또는 잘못 분류된 URL 보고 , 459 페이지
- 향후 URL 범주 집합 변경 , 459 페이지

URL 카테고리 설명

다음 URL 범주는 Web Security Appliance용 AsyncOS의 최신 릴리스에 사용되는 것과 동일한 범주입니다.

URL Category(URL 범주)	약어	코드	설명	URL 예
성인	adlt	1006	성인을 대상으로 하지만 꼭 외설적인 게시물은 아닙니다. 성인 클럽(스트립 클럽, 스와핑 클럽, 사교모임 동반 서비스, 스트리퍼), 성에 대한 일반적인 정보, 실질적으로 외설 의도가 없는 콘텐츠, 생식기 피어싱, 성인용 제품 또는 축하 카드, 건강 또는 질병 이외의 성 관련 정보가 포함될 수 있습니다.	www.adultentertainmentexpo.com www.adultnetline.com

URL Category(URL 범주)	약어	코드	설명	URL 예
광고	adv	1027	종종 웹 페이지가 함께 열리는 배너 및 팝업 광고, 광고 콘텐츠를 제공하는 기타 광고 웹사이트입니다. 광고 서비스 및 세일즈는 "비즈니스 및 산업"으로 분류됩니다.	www.adforce.com www.doubleclick.com
주류	alc	1077	즐겁게 마시는 알코올, 맥주 및 와인 제조, 칵테일 제조법, 주류 판매업체, 와이너리, 포도원, 맥주 공장, 주류 유통회사가 해당됩니다. 알코올 중독은 "건강 및 영양"으로 분류됩니다. 술집과 식당은 "식당 및 주점"으로 분류됩니다.	www.samueladams.com www.whisky.com
예술	art	1002	갤러리 및 전시회, 예술가 및 예술, 사진, 문학 및 책, 공연 예술 및 극장, 뮤지컬, 발레, 박물관, 디자인, 건축이 해당됩니다. 영화 및 TV는 "엔터테인먼트"로 분류됩니다.	www.moma.org www.nga.gov
점성술	astr	1074	점성술, 별자리, 운세, 숫자점, 심령 상담, 타로 카드가 해당됩니다.	www.astro.com www.astrology.com
경매	auct	1088	온라인 및 오프라인 경매, 경매 주택 및 분류 광고가 해당됩니다.	www.craigslist.com www.ebay.com

URL Category(URL 범주)	약어	코드	설명	URL 예
비즈니스 및 산업	busi	1019	마케팅, 상거래, 기업, 비즈니스 관행, 인력, 인사, 수송, 급여, 보안 및 벤처 자금, 사무용품, 산업 장비(프로세스 장비), 기계 및 기계 관련 시스템, 난방 장비, 냉방 장비, 재료 처리 장비, 포장 장비, 제조: 고형물 처리, 금속 제조, 건설 및 건축, 승객 수송, 상거래, 산업 디자인, 건설, 건축 재료, 선적 및 운송(운송 서비스, 트럭 수송, 화물 운송업체, 전세화물 수송업체, 운송 및 수송 중개업자, 특송 서비스, 적재 및 운송 대조, 추적 및 기록, 철도 운송, 해운 배송, 복합 물류 서비스, 이송 및 보관)이 해당됩니다.	www.freightcenter.com www.staples.com
채팅 및 인스턴트 메시징	chat	1040	웹 기반 인스턴트 메시징 및 채팅방이 해당됩니다.	www.icq.com www.meebo.com
부정행위 및 표절	plag	1051	기말 리포트 같은 창작물을 표절할 수 있도록 창작 과제물의 부정 도용 및 판매를 조장	www.bestessays.com www.superiorpapers.com
아동 학대 콘텐츠	cprn	1064	전 세계의 불법 아동 성 학대 콘텐츠입니다.	—
컴퓨터 보안	csec	1065	기업 및 가정 사용자를 위한 보안 제품 및 서비스를 제공합니다.	www.computersecurity.com www.symantec.com
컴퓨터 및 인터넷	comp	1003	컴퓨터 및 소프트웨어에 대한 정보로 여기에는 하드웨어, 소프트웨어, 소프트웨어 지원, 소프트웨어 엔지니어를 위한 정보, 프로그래밍 및 네트워킹, 웹사이트 디자인, 일반적인 웹 및 인터넷 정보, 컴퓨터 공학, 컴퓨터 그래픽 및 클립아트 등이 포함됩니다. "프리웨어 및 셰어웨어"는 별도의 범주에 속합니다.	www.xml.com www.w3.org

URL Category(URL 범주)	약어	코드	설명	URL 예
데이트	date	1055	데이트 업체, 온라인 개인 상담 업체, 결혼중개업체가 해당됩니다.	www.eharmony.com www.match.com
디지털 엽서	card	1082	디지털 엽서 및 e-카드를 보낼 수 있는 사이트입니다.	www.all-yours.net www.delivr.net
식당 및 주점	food	1061	식사와 음주가 가능한 시설, 레스토랑, 바, 소규모 주점 및 펍, 레스토랑 가이드 및 평가가 포함됩니다.	www.hideawaybrewpub.com www.restaurantrow.com
동적 및 주거용	dyn	1091	일반적으로 홈 네트워크 액세스를 시도하는 사용자를 나타내는 광대역 링크의 IP 주소입니다. 가정용 컴퓨터에 대한 원격 세션을 예로 들 수 있습니다.	http://109.60.192.55 http://dynalink.co.jp http://ipadsl.net
교육	edu	1001	학교, 전문대학, 대학교, 수업 자료, 교사 리소스, 기술 및 직업 교육, 온라인 교육, 교육 문제 및 정책, 재정 지원, 학교 기금, 표준 및 테스트 등 교육과 관련된 콘텐츠입니다.	www.education.com www.greatschools.org
엔터테인먼트	ent	1093	영화에 대한 자세한 정보 또는 토론, 음악 및 밴드, TV, 유명인 및 팬 웹사이트, 엔터테인먼트 뉴스, 유명인 가십, 유흥 장소 등이 해당됩니다. "예술" 범주와 비교해 보십시오.	www.eonline.com www.ew.com
극단적인 내용	extr	1075	성폭력 또는 범죄 관련 자료, 폭력 및 폭력적인 행위, 유혈이 포함된 참혹한 사진(예: 부검 사진, 범죄 현장, 범죄 및 사고 희생자 사진, 과도하게 선정적인 자료), 충격적인 웹사이트가 해당됩니다.	www.car-accidents.com www.crime-scene-photos.com

URL Category(URL 범주)	약어	코드	설명	URL 예
패션	fash	1076	의상과 패션, 미용실, 화장품, 액세서리, 보석, 향수, 성형 관련 사진 및 텍스트, 문신 및 피어싱, 모델 에이전시가 해당됩니다. 피부과 제품은 "건강 및 영양"으로 분류됩니다.	www.fashion.net www.findabeautysalon.com
파일 전송 서비스	fts	1071	다운로드 서비스 및 호스팅된 파일 공유 제공을 기본적인 목적으로 하는 파일 전송 서비스입니다.	www.rapidshare.com www.yousendit.com
필터 회피	filt	1025	감지 불가능한 익명 웹 사용을 장려하고 지원하는 서비스로 여기에는 cgi, php, glype 익명 프록시 서비스가 포함됩니다.	www.bypassschoolfilter.com www.filterbypass.com
금융	fnnc	1015	회계 실무 및 회계사, 과세, 세금, 은행업무, 보험, 투자, 국가 경제, 모든 유형의 보험과 관련된 개인 금융, 신용카드, 퇴직 및 부동산 계획, 융자, 모기지 등의 재무 정보가 주로 해당됩니다. 증권 및 주식은 "온라인 거래"로 분류됩니다.	finance.yahoo.com www.bankofamerica.com
프리웨어 및 셰어웨어	free	1068	무료 및 셰어웨어 소프트웨어 다운로드를 제공합니다.	www.freewarehome.com www.shareware.com
도박	gamb	1049	카지노 및 온라인 도박, 마권업자 및 승률, 도박 정보, 도박 경주, 스포츠 예약, 스포츠 도박, 증권 및 주식 스프레드 베팅 서비스가 해당됩니다. 도박 중독을 다루는 웹사이트는 "건강 및 영양"으로 분류됩니다. 정부 운영 복권은 "복권"으로 분류됩니다.	www.888.com www.gambling.com

URL Category(URL 범주)	약어	코드	설명	URL 예
게임	game	1007	다양한 카드 게임, 보드 게임, 문자 게임, 비디오 게임, 전투 게임, 스포츠 게임, 다운로드 가능한 게임, 게임 평가, 치트 시트, 컴퓨터 게임 및 인터넷 게임(예: 롤플레잉 게임)이 해당됩니다.	www.games.com www.shockwave.com
정부 및 법	gov	1011	정부 웹사이트, 외교 문제, 정부/선거 관련 소식 및 정보, 법조계 관련 정보(예: 변호사, 로펌, 법률 공표, 법률 참조 자료, 법원, 사건 일람표, 법률 협회), 법령 및 법원 판결, 시민권 문제, 이민, 특허 및 저작권, 법 집행 및 교정 체계 관련 정보, 범죄 보고, 법 집행, 범죄 통계, 군사 정보(예: 군대, 군사 기지, 군사 조직), 대테러 관련 내용이 해당됩니다.	www.usa.gov www.law.com
해킹	hack	1050	웹사이트, 소프트웨어 및 컴퓨터의 보안을 우회하는 방법에 대해 모의하는 사이트입니다.	www.hackthissite.org www.gohacking.com
혐오 발언	hate	1016	사회 계층, 피부색, 종교, 성적 성향, 장애, 계급, 민족, 국적, 연령, 성별, 성 정체성을 기준으로 증오나 편견 또는 차별을 부추기는 웹사이트 그리고 인종차별, 성차별, 인종차별 신학, 인종차별 음악, 신나치주의 조직, 백인우월주의, 홀로코스트 부인론을 조장하는 사이트가 해당됩니다.	www.kkk.com www.nazi.org

URL Category(URL 범주)	약어	코드	설명	URL 예
건강 및 영양	hlth	1009	보건, 질병 및 장애, 의료 서비스, 병원, 의사, 의약품, 정신 건강, 정신 의학, 약리학, 운동 및 피트니스, 신체장애, 비타민 및 보충제, 성 건강(질병 및 보건), 흡연/음주/마약/도박 건강(질병 및 보건), 일반적인 식품 정보, 식음료, 요리 및 조리법, 식품 및 영양, 건강, 다이어트, 요리(조리법 및 조리 웹사이트 포함), 대체 의학이 해당됩니다.	www.health.com www.webmd.com
유머	lol	1079	농담, 촌극, 코미디 및 기타 재미있는 콘텐츠입니다. 불쾌감을 유발할 수 있는 성인 유머는 "성인"으로 분류됩니다.	www.humor.com www.jokes.com
불법 행위	ilac	1022	도난, 사기, 전화망 불법 액세스, 컴퓨터 바이러스, 테러, 폭탄, 무정부 상태 등의 범죄를 조장하는 사이트, 살인과 자살에 대한 설명뿐만 아니라 이를 실행하는 방법에 대한 내용이 서술된 웹사이트 등이 해당됩니다.	www.ekran.no www.thedisease.net
불법 다운로드	ildl	1084	저작권 계약을 위반하여 소프트웨어 보호 조치를 우회할 수 있도록 소프트웨어나 기타 자료, 시리얼 번호, 키 생성기 및 도구를 다운로드하는 기능을 제공합니다. 토렌트는 "피어 파일 전송"으로 분류됩니다.	www.keygenguru.com www.zcrack.com
불법 약물	drug	1047	환각제, 마약 용품, 마약 구매 및 제조에 대한 정보입니다.	www.cocaine.org www.hightimes.com

URL Category(URL 범주)	약어	코드	설명	URL 예
인프라 및 콘텐츠 전달 네트워크	infr	1018	콘텐츠 전달 인프라 및 동적으로 생성된 콘텐츠로, 현재 안전하거나 분류의 어려움으로 인해 보다 구체적으로 분류할 수 없는 웹사이트가 해당됩니다.	www.akamai.net www.webstat.net
인터넷 전화	voip	1067	인터넷을 사용하는 전화 서비스입니다.	www.evaphone.com www.skype.com
채용 정보 검색	job	1004	경력 조언, 이력서 작성 및 면접 요령, 직무 적성 서비스, 일자리 데이터뱅크, 상근직 및 임시직 에이전시, 고용업체 웹사이트가 해당됩니다.	www.careerbuilder.com www.monster.com
란제리 및 수영복	ling	1031	주로 모델이 등장하는 속옷 및 수영복 콘텐츠입니다.	www.swimsuits.com www.victoriassecret.com
복권	lotr	1034	로또, 시합 및 정부에서 주관하는 복권 사업입니다.	www.calottery.com www.flalottery.com
휴대 전화	cell	1070	SMS(문자 메시지 서비스), 전화 연결음 및 휴대폰 다운로드가 해당됩니다. 이동통신 사업자 웹사이트는 "비즈니스 및 산업" 범주에 포함됩니다.	www.cbfsms.com www.zedge.net
자연	natr	1013	천연 자원, 생태계 및 보존, 삼림, 황야, 식물, 화훼, 삼림 보존, 삼림, 황야, 임업 실무, 삼림 관리(재조림, 삼림 보호, 보존, 수확, 삼림 실태, 간벌, 계획 산불), 농업 실무(농업, 조원, 원예, 조경, 이식, 잡초 방제, 관개, 가지치기, 수확), 오염 문제(대기 청정도, 유해 폐기물, 오염 방지, 재활용, 폐기물 관리, 용수 품질, 환경 정화 산업), 동물, 애완동물, 가축, 동물학, 생물학, 식물학이 해당됩니다.	www.enature.com www.nature.org

URL Category(URL 범주)	약어	코드	설명	URL 예
뉴스	news	1058	뉴스, 헤드라인, 신문, TV 방송국, 잡지, 날씨, 기상 상태에 대한 콘텐츠입니다.	www.cnn.com news.bbc.co.uk
비정부 기구	ngo	1087	클럽, 압력 단체, 커뮤니티, 비영리 조직, 노동조합 같은 비정부 기구가 해당됩니다.	www.panda.org www.unions.org
나체주의	nsn	1060	나체주의 및 나체, 자연주의, 나체주의자 캠프, 예술적 누드가 해당됩니다.	www.artenuda.com www.naturistsociety.com
온라인 커뮤니티	comm	1024	동호회 단체, 특수한 관심사를 공유한 그룹, 웹 뉴스그룹, 게시판이 해당됩니다. "전문 네트워킹" 또는 "소셜 네트워킹"으로 분류된 웹사이트는 제외합니다.	www.igda.org www.ieee.org
온라인 스토리지 및 백업	osb	1066	백업, 공유, 호스팅을 지원하는 오프사이트 및 P2P(Peer-to-peer) 스토리지입니다.	www.adrive.com www.dropbox.com
온라인 거래	trad	1028	온라인 중개, 사용자가 온라인 주식 거래를 할 수 있는 웹사이트와 함께 주식 시장, 주식, 채권, 뮤추얼 펀드, 중개업자, 주식 분석 및 해석, 주식 선별, 주식 차트, IPO, 주식 분할과 관련된 정보가 해당됩니다. 증권 및 주식에 대한 스프레드 베팅 서비스는 "도박"으로 분류됩니다. 기타 금융 서비스는 "금융"으로 분류됩니다.	www.tdameritrade.com www.scottrade.com
조직 이메일	pem	1085	비즈니스 이메일에 액세스하는 데 사용되는 웹사이트입니다(종종 Outlook Web Access를 통해 실행).	—

URL Category(URL 범주)	약어	코드	설명	URL 예
파킹된 도메인	park	1092	광고 네트워크의 유료 리스팅을 사용하는 도메인의 트래픽을 통해 수익을 창출하거나, 수익을 목적으로 도메인 이름을 판매하고자 하는 "도메인 선점자"가 소유하고 있는 웹사이트입니다. 이러한 사이트에는 유료 광고 링크를 반환하는 허위 검색 웹사이트도 포함됩니다.	www.domainzaar.com www.parked.com
피어 파일 전송	p2p	1056	P2P(Peer-to-Peer) 파일 전송 웹사이트입니다. 이 사이트에서는 파일 전송을 자체적으로 추적하지 않습니다.	www.bittorrent.com www.limewire.com
개인 사이트	pers	1081	개인에 대한 웹사이트, 개인 홈페이지 서버, 개인 콘텐츠가 포함된 웹사이트, 특정한 주제가 없는 개인 블로그가 해당됩니다.	www.karymullis.com www.stallman.org
사진 검색 및 이미지	img	1090	이미지, 사진, 클립아트의 저장 및 검색을 지원하는 사이트입니다.	www.flickr.com www.photobucket.com
정치	pol	1083	정치인, 정당, 정치/선거/민주주의/투표에 대한 뉴스 및 정보를 다루는 웹사이트입니다.	www.politics.com www.thisnation.com
음란물	porn	1054	노골적인 성적 표현 또는 묘사가 수반됩니다. 여기에는 노골적인 애니메이션 및 만화, 전반적으로 노골적인 묘사, 기타 페티시 자료, 노골적인 채팅방, 성관계 시뮬레이터, 스트립 포커, 성인 영화, 외설적인 작품, 노골적인 표현이 포함된 웹 기반 이메일이 포함됩니다.	www.redtube.com www.youporn.com

URL Category(URL 범주)	약어	코드	설명	URL 예
전문 네트워킹	pnet	1089	경력 또는 전문성 개발을 위한 소셜 네트워킹이 해당됩니다. "소셜 네트워킹" 항목도 참조해 주십시오.	www.linkedin.com www.europeanpwn.net
부동산	rest	1045	부동산, 사무실 및 상업용 공간, 부동산 리스트(예: 임대 시설, 아파트, 주택, 가옥) 검색을 지원하는 정보입니다.	www.realtor.com www.zillow.com
참조	ref	1017	시/도 가이드, 지도, 역사, 참조 자료 출처, 사전, 라이브러리가 해당됩니다.	www.wikipedia.org www.yellowpages.com
종교	rel	1086	종교적 콘텐츠, 종교에 대한 정보, 종교 커뮤니티가 해당됩니다.	www.religionfacts.com www.religioustolerance.org
SaaS 및 B2B	saas	1080	온라인 비즈니스 서비스, 온라인 회의를 지원하는 웹 포털입니다.	www.netsuite.com www.salesforce.com
어린이 안전	kids	1057	어린이의 액세스가 허용되며 어린이를 대상으로 하는 사이트입니다.	kids.discovery.com www.nickjr.com
과학 및 기술	sci	1012	과학 및 기술 분야에 대한 내용으로 항공우주, 전자, 공학, 수학, 기타 유사 학문, 우주 탐사, 기상학, 지리학, 환경학, 에너지학(화석연료, 핵연료, 재생연료), 통신학(전화, 통신) 등이 포함됩니다.	www.physorg.com www.science.gov
검색 엔진 및 포털	srch	1020	검색 엔진 및 인터넷의 정보에 처음 액세스하는 기타 지점입니다.	www.bing.com www.google.com
성교육	sxed	1052	성, 성 건강, 피임, 임신에 대한 내용을 사실적으로 알려주는 웹사이트입니다.	www.avert.org www.scarleteen.com

URL Category(URL 범주)	약어	코드	설명	URL 예
쇼핑	shop	1005	물물교환, 온라인 구매, 쿠폰 및 무료 서비스, 일반적인 사무용품, 온라인 카탈로그, 온라인 몰이 해당됩니다.	www.amazon.com www.shopping.com
소셜 네트워킹	snet	1069	소셜 네트워킹. "전문 네트워킹" 항목도 참조해 주십시오.	www.facebook.com www.twitter.com
사회과학	socs	1014	사회, 고고학, 인류학, 문화 연구, 역사, 언어, 지리, 철학, 심리학, 여성학 연구와 관련된 과학 및 사학입니다.	www.archaeology.org www.anthropology.net
사회 및 문화	scty	1010	가족 및 관계, 민족, 사회 조직, 계보학, 노인, 보육이 해당됩니다.	www.childcare.gov www.familysearch.org
소프트웨어 업데이트	swup	1053	소프트웨어 패키지의 업데이트를 호스팅하는 웹사이트입니다.	www.softwarepatch.com www.versiontracker.com
스포츠 및 레크리에이션	sprt	1008	모든 스포츠, 전문가와 아마추어, 레크리에이션 활동, 낚시, 판타지 스포츠, 공원, 놀이공원, 워터파크, 테마파크, 동물원, 아쿠아리움, 스파가 해당됩니다.	www.espn.com www.recreation.gov
스트리밍 오디오	aud	1073	인터넷 라디오 및 오디오 피드를 비롯한 실시간 스트리밍 오디오 콘텐츠입니다.	www.live-radio.net www.shoutcast.com
스트리밍 비디오	vid	1072	인터넷 TV, 웹 캐스트, 비디오 공유를 비롯한 실시간 스트리밍 비디오입니다.	www.hulu.com www.youtube.com
담배	tob	1078	애연가 웹사이트, 담배 제조사, 파이프 및 흡연 제품(불법 약물 흡입을 위한 제품이 아님)이 해당됩니다. 담배 중독은 "건강 및 영양"으로 분류됩니다.	www.bat.com www.tobacco.org

URL Category(URL 범주)	약어	코드	설명	URL 예
운송	trns	1044	개인 운송 수단, 자동차 및 오토바이에 대한 정보, 신형 및 중고 자동차/오토바이 구매 정보, 자동차 동호회, 보트/항공기/RV(레크리에이션용 차량) 및 기타 유사 제품이 해당됩니다. 참고로, 자동차 및 오토바이 경주는 "스포츠 및 레크리에이션"으로 분류됩니다.	www.cars.com www.motorcycles.com
여행	trvl	1046	출장 및 개인 여행, 여행 정보, 여행 자료, 여행사, 휴가 패키지, 크루즈, 숙소 및 숙박시설, 여행 교통수단, 항공권 예약, 항공료, 자동차 렌트, 별장이 해당됩니다.	www.expedia.com www.lonelyplanet.com
분류되지 않음	—	—	Cisco 데이터베이스에 없는 웹사이트는 보고를 위해 미분류로 기록됩니다. 여기에는 잘못된 URL이 포함될 수도 있습니다.	—
무기	weap	1036	총포상, 총기 경매, 총기 분류 광고, 총 부속품, 총기류 전시회, 총기 교육, 총기 관련 일반 정보 등 재래식 무기를 구매하거나 사용하는 것과 관련된 정보가 해당되며, 여기에는 기타 무기류 및 사냥 지역 그래픽 정보가 포함될 수 있습니다. 정부 군사 웹사이트는 "정부 및 법률"로 분류됩니다.	www.coldsteel.com www.gunbroker.com
웹 호스팅	whst	1037	웹사이트 호스팅, 대역폭 서비스입니다.	www.bluehost.com www.godaddy.com
웹 페이지 번역	tran	1063	웹 페이지의 언어를 다른 언어로 번역해줍니다.	babelfish.yahoo.com translate.google.com

URL Category(URL 범주)	약어	코드	설명	URL 예
웹 기반 이메일	mail	1038	공용 웹 기반 이메일 서비스입니다. 개인이 소속 회사 또는 조직의 이메일 서비스에 액세스할 수 있는 웹사이트는 "조직 이메일"로 분류됩니다.	mail.yahoo.com www.hotmail.com

URL의 범주 확인

특정 URL의 범주를 조회하려면 분류되지 않은 URL 또는 잘못 분류된 URL 보고 , 459 페이지에 나와 있는 사이트를 방문해 주십시오.

분류되지 않은 URL 또는 잘못 분류된 URL 보고

잘못 분류된 URL 및 범주화되지 않았지만 범주화가 필요한 URL을 보고하려면 다음을 방문하십시오.

https://securityhub.cisco.com/web/submit_urls

제출된 URL의 상태를 확인하려면 이 페이지에 있는 **Status on Submitted URLs(**제출된 **URL**의 상태**)** 탭을 클릭합니다.

향후 URL 범주 집합 변경

드문 일이지만, 추세가 바뀌고 기술이 발전함에 따라 URL 범주 집합이 변경될 수 있습니다. 예를 들면 하나의 범주가 다른 범주에 추가되거나, 다른 범주와 병합되거나, 범주가 제거되거나, 이름이 변경되거나, 하나가 둘로 나뉠 수 있습니다. 이러한 변경 사항은 기존의 필터에서 오는 결과에 영향을 미칠 수 있으며, 변경 사항이 발생하는 경우 어플라이언스는 경고문(System 유형, Warning 심각도)을 전송합니다. 그러한 경고문을 받으면 콘텐츠 및 메시지 필터가 업데이트된 범주와 작동하는지 평가하고 필요 시 업데이트해야 합니다. 기존 필터는 자동으로 변경되지 않습니다. 이러한 알림을 받도록 하려면 알림 수신자 추가, 964 페이지 섹션을 참조하십시오.

다음 변경 사항의 경우 범주 집합 변경이 필요하지 않으며 경고문이 생성되지 않습니다.

- 새로 범주화된 사이트의 일상적인 범주화.
- 잘못 분류된 사이트의 재분류화.

19 장

File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석)

이 장에는 다음 섹션이 포함되어 있습니다.

파일 평판 필터링 및 파일 분석의 개요

Advanced Malware Protection은 다음을 통해 이메일 첨부 파일의 제로 데이 및 표적 파일 기반 위협으로부터 보호합니다.

- 알려진 파일의 평판 가져오기
- 아직 평판 서비스에 알려지지 특정 파일의 동작 분석
- 새로운 정보가 사용 가능하게 될 때 새로 발생하는 위협을 지속적으로 평가하고 네트워크에 들어온 후 위협으로 확인된 파일에 대해 알림

이 기능은 수신 및 발신 메시지.

파일 평판 서비스는 클라우드에 있습니다. 파일 분석 서비스에는 퍼블릭 또는 프라이빗 클라우드(온프레미스)에 대한 옵션이 있습니다.

- 프라이빗 클라우드 파일 평판 서비스는 "프록시" 또는 "에어 갭"(온프레미스) 모드에서 작동하는 Cisco AMP Virtual Virtual Private Cloud 어플라이언스에서 제공됩니다. 온프레미스 파일 평가 서버 구성, 466 페이지의 내용을 참조하십시오.
- 프라이빗 클라우드 파일 분석 서비스는 온프레미스 Cisco AMP Threat Grid 어플라이언스에서 제공됩니다. 온프레미스 파일 분석 서버 구성 , 467 페이지를 참조하십시오.

파일 위협 판정 업데이트

위협 판정은 새 정보가 나타나면 변경될 수 있습니다. 파일이 처음에 알 수 없음 또는 정상으로 평가될 수 있으므로 파일이 수신자에게 릴리스될 수 있습니다. 새 정보가 사용 가능하게 될 때 위협 판정이 변경되면 사용자에게 경고가 전달되고 파일과 파일의 새로운 판정이 AMP 판정 업데이트 보고서에 표시됩니다. 위협의 영향을 치료할 수 있는 시작점으로 진입점 메시지을 조사할 수 있습니다.

판정이 악성에서 클린으로 변경될 수도 있습니다.

파일 분석 후 파일에 동적 콘텐츠가 없는 경우 판정은 Low Risk(낮은 위험)입니다. 파일이 파일 분석을 위해 전송되지 않고, 메시지가 계속 이메일 파이프라인을 통과합니다.

어플라이언스가 동일한 파일의 후속 인스턴스를 처리할 경우 업데이트 판정이 즉시 적용됩니다.

판정 업데이트 타이밍에 대한 정보는 파일 평판 및 분석 서비스에 대해 지원되는 파일 , 463 페이지에서 참조되는 파일 기준 문서에 포함되어 있습니다.

관련 주제

- 파일 평판 및 파일 분석 보고 및 추적 , 484 페이지
- 파일 위협 판정 변경 시 조치 수행 , 487 페이지

파일 처리 개요

메시지에 대한 최종 작업이 수행되지 않은 경우 파일 평판 평가와 분석을 위한 파일 전송은 이전 검사 엔진의 판정과 관계없이 안티바이러스 검사 직후에 이루어집니다.

참고 기본적으로 메시지에 잘못된 형식의 MIME 헤더가 있는 경우 파일 평판 서비스는 "검사 불가" 판정을 반환합니다. 또한 어플라이언스는 이 메시지에서 첨부 파일을 추출하려고 시도합니다. 어플라이언스에서 첨부 파일을 추출할 수 없는 경우 판정은 "검사 불가"로 유지됩니다. 어플라이언스에서 첨부 파일을 추출할 수 있는 경우 첨부 파일의 평판이 평가됩니다. 첨부 파일이 악성인 경우 판정은 "검사 불가"에서 "악성"으로 변경됩니다.

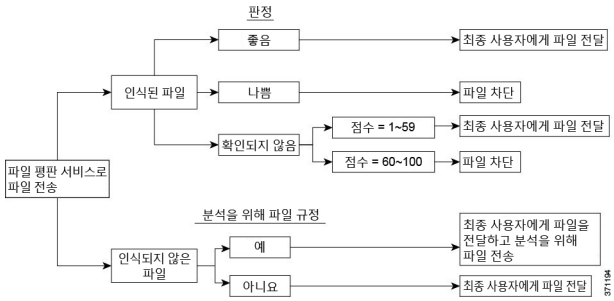
어플라이언스와 파일 평판 서비스 간의 통신은 암호화되어 변조로부터 보호됩니다.

파일의 평판이 평가된 후:

- 메시지에 첨부 파일이 포함되지 않은 경우 파일 평판 서비스는 "건너뜀" 판정을 반환합니다.
- 파일이 파일 평판 서비스에 알려지고 클린으로 확인되면 메시지가 workqueue를 통해 계속됩니다.
- 파일 평판 서비스가 메시지의 첨부 파일에 대해 악성코드 판정을 반환하면 사용자가 적용 가능한 메일 정책에서 지정한 작업을 어플라이언스가 적용합니다.
- 파일이 평판 서비스에 알려졌지만 확정 판정을 위한 정보가 부족한 경우 평판 서비스에서 위협 지문 및 동작 분석과 같은 파일의 특성을 기반으로 평판 점수를 반환합니다. 이 점수가 구성된 평판 임계값을 충족하거나 초과할 경우 사용자가 메일 정책에서 악성코드가 포함된 파일 에 대해 구성한 작업을 어플라이언스가 적용합니다.

- 평판 서비스에 파일에 대한 정보가 없고 파일이 분석 기준을 충족하지 않을 경우(파일 평판 및 분석 서비스에 대해 지원되는 파일 , 463 페이지 참고) 파일이 클린으로 간주되어 메시지가 workqueue를 통해 계속됩니다.
- 파일 분석 서비스를 활성화하고 평판 서비스에 파일에 대한 정보가 없으며 파일이 분석 가능한 파일에 대한 기준을 충족하면(파일 평판 및 분석 서비스에 대해 지원되는 파일 , 463 페이지 참고) 메시지가 격리되고(분석을 위해 전송된 첨부 파일이 포함된 메시지 격리, 479 페이지 참고) 파일이 분석을 위해 전송될 수 있습니다. 재시도가 아닌 BE(Best Effort)입니다. 첨부 파일이 분석을 위해 전송될 경우 메시지를 격리하도록 어플라이언스를 구성하지 않았거나 파일이 분석을 위해 전송되지 않은 경우 메시지가 사용자에게 릴리스됩니다.
- 온프레미스 파일 분석과 함께 구축할 경우 평판 평가와 파일 분석이 동시에 발생합니다. 평판 서비스에는 다양한 소스의 입력이 포함되므로 평판 서비스가 판정을 반환하면 해당 판정이 사용됩니다. 파일이 평판 서비스에 알려지지 않은 경우 해당 파일 분석 판정이 사용됩니다.
- 서버와의 연결이 시간 초과되어 파일 평판 판정 정보를 사용할 수 없는 경우, 해당 파일은 검사 불가로 간주되고 구성된 작업이 적용됩니다.

그림 ***33:*** 퍼블릭 클라우드 파일 분석 구축을 위한 ***Advanced Malware Protection*** 워크플로



파일이 분석을 위해 전송되는 경우:

- 파일이 분석을 위해 클라우드로 전송되는 경우: 파일이 HTTPS를 통해 전송됩니다.
- 분석은 일반적으로 몇 분이 소요되지만 더 오래 걸릴 수 있습니다.
- 파일 분석 후 악성으로 플래그가 지정된 파일이 평판 서비스에서 악성으로 식별되지 않을 수 있습니다. 파일 평판은 반드시 단일 파일 분석 판정만이 아니라 시간이 경과함에 따라 다양한 요인으로 결정됩니다.
- 온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용하여 분석된 파일에 대한 결과는 로컬로 캐시됩니다.

판정 업데이트에 대한 자세한 내용은 파일 위협 판정 업데이트 , 462 페이지를 참조하십시오.

파일 평판 및 분석 서비스에 대해 지원되는 파일

평판 서비스에서는 대부분의 파일 유형을 평가합니다. 파일 유형 ID는 파일 내용에 따라 결정되며 파일 이름 확장자에 종속되지 않습니다.

평판을 알 수 없는 일부 파일은 위협 특성을 분석할 수 있습니다. 파일 분석 기능을 구성할 때 분석할 파일 유형을 선택합니다. 새로운 유형이 동적으로 추가될 수 있으며 업로드 가능한 파일 유형의 목록이 변경되면 경고를 수신하게 되므로 업로드할 추가 파일 유형을 선택할 수 있습니다.

등록된 Cisco 고객만이 평판 및 분석 서비스에서 지원되는 파일에 대한 세부사항을 볼 수 있습니다. 평가 및 분석되는 파일에 대한 내용은 *Cisco* 콘텐츠 보안 제품용 *Advanced Malware Protection* 서비스의 파일 기준(https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html)을 참조하십시오. 파일의 평판 평가 및 분석을 위한 파일 전송에 대한 기준은 언제든지 변경될 수 있습니다.

이 문서에 액세스하려면 지원 계약을 통해 제공된 Cisco 고객 어카운트가 있어야 합니다. 등록하려면 https://tools.cisco.com/RPF/register/register.do를 방문하십시오.

Advanced Malware Protection에서 처리되지 않는 파일의 전송을 차단하도록 정책을 구성해야 합니다.

참고 분석을 위해 소스에서 이미 업로드된 파일(수신 메일 또는 발신 메일의 파일)은 다시 업로드되지 않습니다. 이러한 파일의 분석 결과를 보려면 File Analysis(파일 분석) 보고 페이지에서 SHA-256을 검색합니다.

관련 주제

- 파일 평판 및 분석 서비스 사용 및 구성 , 468 페이지
- Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 483 페이지
- 아카이브 또는 압축 파일 처리, 464 페이지

아카이브 또는 압축 파일 처리

파일이 압축 또는 아카이브될 경우

- 압축 또는 아카이브 파일의 평판이 평가됩니다.

파일 형식을 포함하여 검사되는 아카이브 및 압축 파일에 대한 내용은 파일 평판 및 분석 서비스에 대해 지원되는 파일 , 463 페이지에서 연결된 정보를 참조하십시오.

이 시나리오에서는

- 추출한 파일 중 하나가 악성인 경우 파일 평판 서비스가 압축 또는 아카이브 파일에 대해 악성 판정을 반환합니다.
- 압축 또는 아카이브 파일이 악성이고 추출된 모든 파일은 클린인 경우 파일 평판 서비스가 압축 또는 아카이브 파일에 대해 악성 판정을 반환합니다.
- 추출된 파일의 판정을 알 수 없는 경우 추출된 파일이 파일 분석을 위해 선택적으로 전송됩니다(구성되고 해당 파일 유형에 파일 분석이 지원되는 경우).
- 추출된 파일 또는 첨부 파일의 판정이 낮은 위험인 경우, 파일 분석을 위해 파일이 전송되지 않습니다.
- 압축 또는 아카이브 파일의 압축을 푸는 동안 파일 추출에 실패할 경우 파일 평판 서비스가 압축 또는 아카이브 파일에 대해 스캐닝 불가능 판정을 반환합니다. 이 시나리오에서는 추출된 파일 중 하나가 악성인 경우 파일 평판 서비스가 압축 또는 아카이브 파일에 대해 악성 판정을 반환한다는 점에 유의하십시오(악성 판정이 스캐닝 불가능 판정보다 우선함).
- 아카이브 또는 압축 파일은 다음 시나리오에서 스캔 불가로 처리됩니다.
  - 데이터 압축 비율이 20을 초과합니다.

- 아카이브 파일에 포함된 중첩 수준이 5를 초과합니다.
- 아카이브 파일에 포함된 하위 파일이 200개를 초과합니다.
- 아카이브 파일 크기가 50MB를 초과합니다.
- 아카이브 파일이 비밀번호로 보호되거나 읽을 수 없습니다.

참고 보안 MIME 유형(예: 텍스트/일반)으로 추출된 파일의 평판은 평가되지 않습니다.

클라우드에 전송된 정보의 개인 정보 보호

- 파일을 고유하게 식별하는 SHA만 클라우드의 평판 서비스에 전송됩니다. 파일 자체는 전송되지 않습니다.
- 클라우드에서 파일 분석 서비스를 사용 중이고 파일이 분석에 적합한 경우에는 파일 자체가 클라우드에 전송됩니다.
- 분석을 위해 클라우드로 전송되고 "악성" 판정을 받은 모든 파일에 대한 정보가 평판 데이터베이스에 추가됩니다. 이 정보를 다른 데이터와 함께 사용하여 평판 점수를 결정합니다.

  온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용하여 분석된 파일에 대한 정보는 평판 서비스와 공유되지 않습니다.
- 발신자 기반 평판 서비스로 데이터를 전송할 수 있도록 어플라이언스를 구성한 경우 특정 파일에 대한 정보가 전송됩니다. 자세한 내용은 Cisco Email Security Appliance 가이드의 "SenderBase 네트워크 참여" 장에서 AMP 클라우드에 대한 정보를 참고하십시오.

파일 평판 및 분석 기능 구성

• Advanced Malware Protection 기능에 대한 중앙 집중식 보고 구성 , 484 페이지

파일 평판 및 분석 서비스와의 통신을 위한 요건

- 이 서비스를 사용하는 모든 Email Security Appliance는 인터넷을 통해 직접 연결할 수 있어야 합니다. 단, 온프레미스 Cisco AMP Threat Grid Appliance를 사용하도록 구성된 파일 분석 서비스는 제외합니다.
- 기본적으로 파일 평판 및 분석 서비스 를 참조하십시오.
- 기본적으로 파일 평판 및 클라우드 기반 분석 서비스와의 통신은 기본 게이트웨이와 연계된 인터페이스를 통해 라우팅됩니다. 다른 인터페이스를 통해 이 트래픽을 라우팅하려면 Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석) 페이지의 고급 섹션에서 각 주소에 대해 정적 경로를 생성합니다.
- 다음과 같은 방화벽 포트를 열어야 합니다.

방화벽 포트	설명	프로토콜	In/Out	호스트 이름	어플라이언스 인터페이스
32137(기본) 또는 443	파일 평판을 얻기 위해 클라우드 서비스에 액세스합니다.	TCP	Out	Security Services(보안 서비스) > Anti-Malware and Reputation(안티맬웨어 및 평판), 고급 섹션에 구성된 대로 클라우드 서버 풀 매개변수.	관리, 데이터 포트를 통해 이 트래픽을 라우팅하도록 구성되지 않은 경우.
443	파일 분석을 위해 클라우드 서비스에 액세스합니다.	TCP	Out	Security Services(보안 서비스) > Anti-Malware and Reputation(악성코드 차단 및 평판), Advanced(고급) 섹션에 구성된 대로.	

온프레미스 파일 평가 서버 구성

Cisco AMP Virtual Private Cloud Appliance를 프라이빗 클라우드 파일 분석 서버로 사용할 경우:

- http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html 에서 FireAMP Private Cloud의 설치 및 구성 설명서를 포함한 Cisco Advanced Malware Protection Virtual Private Cloud Appliance 설명서를 받을 수 있습니다.

  이 설명서를 사용하여 이 주제에 설명된 작업을 수행합니다.

  추가 설명서는 AMP Virtual Private Cloud Appliance의 Help(도움말) 링크에서 사용할 수 있습니다.
- "프록시" 또는 "Air-Gap"(온-프레미스) 모드에서 Cisco AMP Virtual Private Cloud Appliance를 설정하고 구성합니다.

- Cisco AMP Virtual Private Cloud Appliance 소프트웨어 버전이 2.2인지 확인합니다. Cisco Email Security Appliance와 통합을 활성화합니다.
- 이 Email Security Appliance에 업로드할 해당 어플라이언스에 AMP Virtual Private Cloud 인증서 및 키 다운로드
- Email Security Appliance에서 신뢰할 수 있는 루트 인증 기관이 터널 프록시 서버 인증서에 서명하지 않은 경우 루트 인증서 옵션을 사용하여 표준 검증을 건너뜁니다.

참고 이 Email Security Appliance에서 연결을 구성하는 온프레미스 파일 평판 서버를 설정한 후 파일 평판 및 분석 서비스 사용 및 구성 , 468 페이지의 6단계를 참조하십시오.

온프레미스 파일 분석 서버 구성

Cisco AMP Threat Grid 어플라이언스를 프라이빗 클라우드 파일 분석 서버로 사용할 경우:

- Cisco AMP Threat Grid 어플라이언스 설정 및 구성 설명서와 Cisco AMP Threat Grid 어플라이언스 관리 설명서를 얻습니다. Cisco AMP Threat Grid Appliance 설명서는 http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides%20-list.html 에서 사용할 수 있습니다.

  이 주제에 설명된 작업을 수행하려면 이 문서를 사용합니다.

  추가 설명서는 AMP Threat Grid 어플라이언스의 Help(도움말) 링크에서 사용할 수 있습니다.

  관리 설명서에서 다른 Cisco 어플라이언스, CSA(Cisco Sandbox API), ESA(Email Security Appliance), 와의 통합에 대한 모든 정보를 검색합니다.

- Cisco AMP Threat Grid 어플라이언스를 설정하고 구성합니다.
- 필요한 경우 Cisco AMP Threat Grid Appliance 소프트웨어를 1.2.1 버전으로 업데이트하여 Cisco Email Security Appliance와의 통합을 지원합니다.

  버전 번호를 확인하고 업데이트를 수행하는 방법에 대한 지침은 AMP Thread Grid 설명서를 참조하십시오.

- 어플라이언스가 네트워크를 통해 서로 통신할 수 있는지 확인합니다. Cisco Email Security Appliance는 AMP Threat Grid Appliance의 CLEAN 인터페이스에 연결할 수 있어야 합니다.
- 자체 서명 인증서를 배포할 경우: Email Security Appliance 에서 사용할 Cisco AMP Threat Grid Appliance에서 자체 서명 SSL 인증서를 생성합니다. AMP Threat Grid 어플라이언스의 관리자 설명서에서 SSL 인증서 및 키 다운로드 지침을 참조하십시오. AMP Threat Grid 어플라이언스의 호스트 이름이 CN으로 지정된 인증서를 생성해야 합니다. AMP Threat Grid 어플라이언스의 기본 인증서는 작동하지 않습니다.
- 파일 평판 및 분석 서비스 사용 및 구성 , 468 페이지에서 설명한 대로 파일 분석용 구성을 제출할 때 Email Security Appliance 가 Threat Grid Appliance와 함께 자동으로 등록됩니다. 그러나 동일한 절차에 설명된 대로 등록을 활성화해야 합니다.

파일 평판 및 분석 서비스 사용 및 구성

시작하기 전에

- 파일 평판 서비스 및 파일 분석 서비스에 대한 기능 키를 받아 이 어플라이언스에 전송합니다.
- 파일 평판 및 분석 서비스와의 통신을 위한 요건 , 466 페이지를 충족해야 합니다.
- 업데이트 페이지에서 구성된 업데이트 서버에 대한 연결을 확인합니다.
- Cisco AMP Virtual Private Cloud Appliance를 프라이빗 클라우드 파일 평판 서버로 사용할 경우 온프레미스 파일 평가 서버 구성, 466 페이지 섹션을 참조하십시오.
- Cisco AMP Threat Grid Appliance를 프라이빗 클라우드 파일 분석 서버로 사용할 경우 온프레미스 파일 분석 서버 구성 , 467 페이지를 참조하십시오.

단계 **1** **Security Services(**보안 서비스**) > File Reputation and Analysis(**파일 평판 및 분석**)**를 선택합니다.

단계 **2** **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **3** **Enable File Reputation Filtering(**파일 평판 필터링 활성화**)**를 클릭하고 선택적으로 **Enable File Analysis(**파일 분석 활성화**)**를 클릭합니다.

- **Enable File Reputation Filtering(**파일 평판 필터링 활성화**)**을 선택하는 경우 외부 퍼블릭 평판 클라우드 서버의 URL을 선택하거나 프라이빗 평판 클라우드 서버 연결 정보를 제공하여 **File Reputation Server(**파일 평판 서버**)(6**단계) 섹션을 구성해야 합니다.
- 마찬가지로, **Enable File Analysis(**파일 분석 활성화**)**를 선택하는 경우 **File Analysis Server URL(**파일 분석 서버 **URL)(7**단계) 섹션을 구성하여 외부 클라우드 서버의 URL이나 프라이빗 분석 클라우드 연결 정보를 제공해야 합니다

  참고 업그레이드 후에 새 파일 유형이 추가될 수 있으며, 이러한 파일 유형은 기본적으로 활성화되지 않습니다. 파일 분석을 활성화한 상태에서 분석에 새 파일 유형을 포함해야 하는 경우 이를 활성화해야 합니다.

단계 **4** 라이센스 계약이 표시되는 동의합니다.

단계 **5** **File Analysis(**파일 분석**)** 섹션의 적절한 파일 그룹(예: "Microsoft 문서")에서 필수 파일 유형을 선택하여 파일 분석을 위해 전송합니다.

지원되는 파일 유형에 대한 자세한 내용은 다음에 설명된 문서를 참조하십시오. 파일 평판 및 분석 서비스에 대해 지원되는 파일 , 463 페이지

참고 Cisco는 정기적으로 잠재적으로 악성 파일 유형을 확인하여 제로 데이 위협을 방지합니다. 새로운 위협이 식별되는 경우 해당 파일 유형의 세부 정보가 업데이트 서버를 통해 어플라이언스에 전송됩니다. **Other potentially malicious file types(**기타 잠재적인 악성 파일 유형**)** 옵션을 선택하여 이 기능을 활성화합니다. 이 기능을 활성화하는 경우 선택한 파일 유형 외에도 어플라이언스에서 분석을 위해 해당 파일 유형을 전송합니다.

단계 **6** **Advanced Settings for File Reputation(**파일 평판 고급 설정**)** 패널을 펼치고 필요에 따라 다음 옵션을 조정합니다.

옵션	설명
클라우드 도메인	파일 평판 쿼리에 사용할 도메인의 이름입니다.
파일 평판 서버	퍼블릭 평판 클라우드 서버 또는 프라이빗 평판 클라우드의 호스트 이름 중에서 선택합니다. 프라이빗 평판 클라우드를 선택하는 경우 다음 정보를 제공합니다. • 서버 - Cisco AMP Virtual Private Cloud Appliance의 호스트 이름 또는 IP 주소입니다. • 퍼블릭 키 - 이 어플라이언스 및 프라이빗 클라우드 어플라이언스 간의 암호화된 통신에 유효한 퍼블릭 키를 제공합니다. 프라이빗 클라우드 서버에 사용되는 동일한 키여야 합니다. 이 어플라이언스에서 키 파일을 찾은 다음 **Upload File(파일 업로드)**를 클릭합니다. 참고 서버에서 이 어플라이언스로 키 파일을 이미 다운로드했어야 합니다.
AMP for Endpoints 콘솔 통합	**Register the Appliance with AMP for Endpoints(AMP for Endpoints**에 어플라이언스 등록**)**를 클릭하여 AMP for Endpoints Console에 어플라이언스를 통합합니다. 자세한 내용은 어플라이언스와 AMP for Endpoints Console 통합, 472 페이지를 참고하십시오.
파일 평판의 SSL 통신	기본 포트 32137이 아닌 포트 443에서 통신하려면 **Use SSL(Port 443)(SSL** 사용**(**포트 **443))**을 선택합니다. 서버에 대한 SSH 액세스를 활성화하는 방법에 대한 내용은 Cisco AMP Virtual Private Cloud Appliance 사용 설명서를 참조하십시오. 참고 방화벽에서 포트를 열려면 포트 32137을 통한 SSL 통신이 필요할 수 있습니다. 이 옵션을 사용하여 파일 평판 서비스와의 통신에 사용할 업스트림 프록시를 구성할 수도 있습니다. 이 옵션을 선택하는 경우 적절한 서버, 사용자 이름 및 암호 정보를 제공합니다. **Use SSL (Port 443)(SSL** 사용**(**포트 **443))**을 선택하는 경우 **Relax Certificate Validation(**인증서 확인 완화**)**을 선택하여 터널 프록시 서버의 인증서가 신뢰할 수 있는 루트 인증 기관에서 서명되지 않은 경우 표준 인증서 유효성 검사를 건너뛸 수도 있습니다. 예를 들어, 신뢰할 수 있는 내부 터널 프록시 서버에서 자체 서명된 인증서를 사용하는 경우 이 옵션을 선택하십시오. 참고 Advanced Settings for File Reputation(파일 평판 고급 설정)의 SSL Communication for File Reputation(파일 평판의 SSL 통신) 섹션에서 **Use SSL (Port 443)(SSL** 사용**(**포트 **443))**을 선택한 경우 CLI 명령 certconfig > CERTAUTHORITY > CUSTOM을 사용하거나 웹 인터페이스에서 Network(네트워크) > Certificates(인증서)(맞춤형 인증 기관)를 사용하여 AMP 온프레미스 평판 서버 CA 인증서를 이 어플라이언스의 인증서 저장소에 추가해야 합니다. 서버에서 이 인증서를 가져옵니다 (Configuration(구성) > SSL > Cloud server(클라우드 서버) > download(다운로드)).

옵션	설명
하트비트 간격	회귀 이벤트에 대해 ping하는 간격(분).
평판 임계값	허용되는 파일 평판 점수의 상한. 이 임계값 위의 점수는 해당 파일이 감염되었음을 나타냅니다. • 클라우드 서비스의 값**(60)** 사용 • **Enter Custom Value(**맞춤형 값 입력**)** -기본값은 60입니다.
쿼리 시간 초과	평판 쿼리 시간이 초과되기 전에 경과된 시간(초)입니다.
처리 시간 초과	파일 처리 시간이 초과되기 전에 경과된 시간(초)입니다.
파일 평판 클라이언트 ID	파일 평판 서버(읽기 전용)의 이 어플라이언스에 대한 클라이언트 ID입니다.
파일 회귀 분석	메시지 수신자에게 전달되지 않았거나, 삭제되었거나, 격리된 메시지에 대한 회귀 판정 경고를 표시하지 않으려면 **Suppress the retrospective verdict alerts(**회귀 판정 경고 표시 안 함**)**을 선택합니다.

참고 Cisco 지원의 지침 없이 이 섹션의 다른 설정을 변경하지 마십시오.

단계 **7** 파일 분석을 위해 클라우드 서비스를 사용할 경우 Advanced Settings for File Analysis(파일 분석 고급 설정) 패널을 펼치고 필요에 따라 다음 옵션을 조정합니다.

옵션	설명
파일 분석 서버 URL	외부 클라우드 서버 또는 **Private analysis cloud(**프라이빗 분석 클라우드**)**이름(URL) 중에서 선택합니다. 외부 클라우드 서버를 지정하는 경우 어플라이언스에 물리적으로 가장 가까운 서버를 선택합니다. 새로 제공된 서버가 표준 업데이트 프로세스를 사용하여 이 목록에 주기적으로 추가됩니다. 파일 분석에 대한 온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용할 프라이빗 분석 클라우드를 선택하고 다음 정보를 제공합니다. • 서버 - 온프레미스 프라이빗 분석 클라우드 서버의 URL입니다. • **TG** 서버 - 독립형 또는 클러스터형 Cisco AMP Threat Grid 어플라이언스의 IPv4 주소 또는 호스트 이름을 입력합니다. 최대 7개의 Cisco AMP Threat Grid 어플라이언스를 추가할 수 있습니다. 참고 시리얼 번호는 독립형 또는 클러스터형 Cisco AMP Threat Grid 어플라이언스를 추가하는 순서를 나타냅니다. 어플라이언스의 우선순위를 표시하지는 않습니다. • **Certificate Authority(**인증 기관**)** – **Use Cisco Default Certificate Authority(Cisco** 기본 인증 기관 사용**)** 또는 **Use Uploaded Certificate Authority(**업로드된 인증 기관 사용**)**중에서 선택합니다. **Use Uploaded Certificate Authority(**업로드된 인증 기관 사용**)**를 선택하는 경우 **Browse(**찾아보기**)**를 클릭하여 이 어플라이언스와 프라이빗 클라우드 어플라이언스 간에 암호화된 통신을 위해 유효한 인증서 파일을 업로드합니다. 이 인증서는 프라이빗 클라우드 서버에서 사용하는 것과 동일한 인증서여야 합니다. 참고 파일 분석을 위해 어플라이언스에서 Cisco AMP Threat Grid 포털을 구성한 경우, Cisco AMP Threat Grid 포털(예: https://panacea.threatgrid.eu)에 액세스하여 파일 분석을 위해 제출된 파일을 보고 추적할 수 있습니다. Cisco AMP Threat Grid 포털에 액세스하는 방법에 대한 자세한 내용은 Cisco TAC에 문의하십시오.
파일 분석 클라이언트 ID	파일 분석 서버(읽기 전용)의 이 어플라이언스에 대한 클라이언트 ID입니다.

단계 **8** (선택 사항) 파일 평판 처리 값에 대한 캐시 만료 기간을 구성하려는 경우 Cache Settings(캐시 설정) 패널을 펼칩니다.

단계 **9** 허용 가능한 파일 분석 점수에 대한 상한을 설정하려는 경우 Threshold Settings(임계값 설정) 패널을 펼칩니다. 이 임계값 위의 점수는 해당 파일이 감염되었음을 나타냅니다. 다음 옵션 중 하나를 선택합니다.

- Use value from Cloud Service (95)(클라우드 서비스의 값(95) 사용)
- Enter Custom Value(맞춤형 값 입력) -기본값은 95

단계 **10** 변경사항을 제출 및 커밋합니다.

단계 **11** 온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용할 경우 AMP Threat Grid 어플라이언스에서 이 어플라이언스에 대한 계정을 활성화합니다.

"사용자" 계정 활성화에 대한 자세한 지침은 AMP Threat Grid 문서에서 확인할 수 있습니다.

a) 페이지 섹션 하단에 파일 분석 클라이언트 ID가 나타납니다. 이를 통해 활성화할 "사용자"가 식별됩니다.
b) AMP Threat Grid 어플라이언스에 로그인합니다.
c) **Welcome...(**시작**...) > Manage Users(**사용자 관리**)**를 선택하고 User Details(사용자 세부 정보)로 이동합니다.
d) Email Security Appliance의 파일 분석 클라이언트 ID를 기반으로 "사용자" 계정을 찾습니다.
e) 어플라이언스의 이 "사용자" 계정을 활성화합니다.

어플라이언스와 AMP for Endpoints Console 통합

어플라이언스와 AMP for Endpoints Console을 통합하고 AMP for Endpoints Console에서 다음 작업을 수행할 수 있습니다.

- 단순 맞춤형 탐지 목록을 만듭니다.
- 단순 맞춤형 탐지 목록에 새 악성 파일 SHA를 추가합니다.
- 애플리케이션 화이트리스트를 만듭니다.
- 애플리케이션 화이트리스트 새 파일 SHA를 추가합니다.
- 맞춤형 정책을 만듭니다.
- 단순 맞춤형 탐지 목록 및 애플리케이션 화이트리스트를 맞춤형 정책에 연결합니다.
- 맞춤형 그룹을 만듭니다.
- 맞춤형 정책을 맞춤형 그룹에 연결합니다.
- 등록된 어플라이언스를 기본 그룹에서 맞춤형 그룹으로 이동합니다.
- 특정 파일 SHA의 파일 경로 분석 세부 정보를 봅니다.

어플라이언스와 AMP for Endpoints Console을 통합하려면, 이 콘솔에 어플라이언스를 등록해야 합니다.

통합 후에 파일 SHA가 파일 평판 서버로 전송되면 파일 평판 서버에서 파일 SHA에 대해 얻은 판정은 AMP for Endpoints Console의 동일한 파일 SHA에 대해 이미 사용 가능한 판정으로 재정의됩니다.

파일 SHA가 이미 전역에서 악의적이라고 표시된 경우 및 AMP for Endpoints Console에 대한 동일한 파일 SHA가 블랙리스트에 있는 경우 파일 상태는 악성입니다.

Advanced Malware Protection 보고서 페이지에 새 섹션 **Incoming Malware Files by Category(**카테고리별 수신 악성코드 파일**)**가 포함되어 **Custom Detection(**맞춤형 탐지**)**으로 표시된 AMP for Endpoints Console에서 수신한 블랙리스트에 있는 파일 SHA의 백분율을 볼 수 있습니다. 블랙리스트에 있는 파일 SHA의 위협 이름은 보고서의 Incoming Malware Threat Files(수신 악성코드 위협 파일) 섹션에서

Simple Custom Detection(단순 맞춤형 탐지**)**로 표시됩니다. 보고서의 More Details(추가 세부 정보) 섹션에 있는 링크를 클릭하여 AMP for Endpoints Console에서 블랙리스트에 있는 파일 SHA의 파일 경로 분석 세부 정보를 볼 수 있습니다.

시작하기 전에

AMP for Endpoints Console에 관리자 권한이 있는 사용자 계정이 있어야 합니다. AMP for Endpoints Console 사용자 계정을 생성하는 방법에 대한 자세한 내용은 Cisco TAC에 문의하십시오.

파일 평판 필터링을 활성화하고 구성해야 합니다. 파일 평판 필터링을 활성화하고 구성하는 방법을 알아보려면 파일 평판 및 분석 서비스 사용 및 구성 , 468 페이지 섹션을 참조하십시오.

단계 **1** **Security Services(**보안 서비스**) > File Reputation and Analysis(**파일 평판 및 분석**)**를 선택합니다.

단계 **2** **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **3** 웹 인터페이스의 File Reputation and File Analysis(파일 평판 및 파일 분석) 페이지에 있는 Advanced Settings for File Reputation(파일 평판 고급 설정) 패널에서 **Register Appliance with AMP for Endpoints(AMP for Endpoints**에 어플라이언스 등록**)**을 클릭합니다.

Register the Appliance with AMP for Endpoints(AMP for Endpoints에 어플라이언스 등록)을 클릭하면 AMP for Endpoints Console 로그인 페이지가 표시됩니다.

단계 **4** 사용자 크리덴셜을 사용하여 AMP for Endpoints Console에 로그인합니다.

단계 **5** 어플라이언스를 등록하려면 AMP for Endpoints 인증 페이지에서 **Allow(**허용**)**를 클릭합니다.

Allow(허용)를 클릭하면 등록이 완료되고 어플라이언스의 File Reputation and Analysis(파일 평판 및 분석) 페이지로 리디렉션됩니다. 어플라이언스 이름이 AMP for Endpoints Console Integration(AMP for Endpoints Console 통합) 필드에 표시됩니다. 어플라이언스 이름을 사용하여 AMP for Endpoints Console 페이지에서 어플라이언스 설정을 맞춤화할 수 있습니다.

다음에 수행할 작업

다음 단계:

- AMP for Endpoints Console 페이지의 Accounts(계정) > Applications(어플라이언스)로 이동하여 AMP for Endpoints Console에 등록되었는지 여부를 확인할 수 있습니다. 어플라이언스 이름은 AMP for Endpoints Console 페이지의 Applications(애플리케이션) 섹션에 표시됩니다.
- 등록하면 어플라이언스가 기본 정책(네트워크 정책)이 연결된 기본 그룹(감사 그룹)에 추가됩니다. 기본 정책에는 블랙리스트 또는 화이트리스트에 있는 파일 SHA 목록이 포함됩니다. 어플라이언스의 AMP for Endpoints 설정을 맞춤화하고 자신의 블랙리스트 또는 화이트리스트에 있는 파일 SHA를 추가하려면 https://console.amp.cisco.com/docs에서 AMP for Endpoints 사용자 설명서를 참조하십시오.
- AMP for Endpoints Console에서 어플라이언스 연결을 등록 취소하려면, 어플라이언스의 Advanced Settings for File Reputation(파일 평판 고급 설정) 섹션에 **Deregister(**등록 취소**)**를 클릭하거나

https://console.amp.cisco.com/에서 AMP for Endpoints Console 페이지로 이동해야 합니다. 자세한 내용은 https://console.amp.cisco.com/docs의 AMP for Endpoints 사용 설명서를 참조하십시오.

참고 파일 평판 서버를 다른 데이터 센터로 변경하면 어플라이언스가 AMP for Endpoints Console에서 자동으로 등록 취소됩니다. 파일 평판 서버에 대해 동일한 데이터 센터를 선택한 상태에서 AMP for Endpoints Console에 어플라이언스를 다시 등록해야 합니다.

참고 악성 파일 SHA가 정상 판정을 받은 경우 동일한 파일 SHA가 AMP for Endpoints Console의 화이트리스트에 있는지 확인해야 합니다.

클러스터 수준에서 **AMP for Endpoints** 콘솔에 어플라이언스 등록

클러스터링된 구성에서는 시스템 모드에서 AMP for Endpoints 콘솔을 사용하여 로그인한 어플라이언스만 등록할 수 있습니다.

독립형 모드에서 AMP for Endpoints 콘솔에 이미 어플라이언스를 등록한 경우 이를 클러스터에 가입하려면 먼저 수동으로 어플라이언스를 등록 취소해야 합니다.

시작하기 전에

AMP for Endpoints Console에 관리자 권한이 있는 사용자 계정이 있어야 합니다. AMP for Endpoints Console 사용자 계정을 생성하는 방법에 대한 자세한 내용은 Cisco TAC에 문의하십시오.

단계 **1** 클러스터 모드에 있는 어플라이언스에 로그인합니다.

단계 **2** **Security Services > File Reputation and Analysis(**파일 평판 및 분석**)** 페이지로 이동합니다.

단계 **3** **Centralized Management Options(**중앙 집중식 관리 옵션**)**를 클릭한 후 **Manage Settings(**설정 관리**)**를 클릭합니다.

단계 **4** **Copy settings to(**다음 대상에 설정 복사**):** 옵션을 선택한 후 로그인한 어플라이언스 이름을 선택하여 어플라이언스의 '파일 평판 및 분석' 구성 설정을 클러스터 모드에서 시스템 모드로 복사할 수 있습니다.

단계 **5** **Submit(**제출**)**을 클릭하여 변경 사항을 커밋합니다.

단계 **6** 어플라이언스를 클러스터 모드에서 시스템 모드로 전환합니다.

단계 **7** File Reputation and Analysi(파일 평판 및 분석) 페이지에서 **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **8** 웹 인터페이스의 File Reputation and File Analysis(파일 평판 및 파일 분석) 페이지에 있는 Advanced Settings for File Reputation(파일 평판 고급 설정) 패널에서 **Register Appliance with AMP for Endpoints(AMP for Endpoints**에 어플라이언스 등록**)**을 클릭합니다.

Register the Appliance with AMP for Endpoints(AMP for Endpoints에 어플라이언스 등록)을 클릭하면 AMP for Endpoints Console 로그인 페이지가 표시됩니다.

단계 **9** 사용자 크리덴셜을 사용하여 AMP for Endpoints Console에 로그인합니다.

단계 **10** 어플라이언스를 등록하려면 AMP for Endpoints 인증 페이지에서 **Allow(**허용**)**를 클릭합니다.

Allow(허용)를 클릭하면 등록이 완료되고 어플라이언스의 File Reputation and Analysis(파일 평판 및 분석) 페이지로 리디렉션됩니다. 어플라이언스 이름이 AMP for Endpoints Console Integration(AMP for Endpoints Console 통합) 필드에 표시됩니다. 어플라이언스 이름을 사용하여 AMP for Endpoints 콘솔 페이지에서 어플라이언스 설정을 맞춤화할 수 있습니다.

단계 **11** File Reputation and Analysi(파일 평판 및 분석) 페이지에서 **Submit(**제출**)**을 클릭합니다.

단계 **12** **Centralized Management Options(**중앙 집중식 관리 옵션**)**를 클릭한 후 **Manage Settings(**설정 관리**)**를 클릭합니다.

단계 **13** **Delete settings from(**다음 대상에서 설정 삭제**):** 옵션을 선택한 후 로그인한 어플라이언스 이름을 선택하여 시스템 시준에서 파일 평판 및 분석 구성 설정을 삭제합니다.

단계 **14** **Submit(**제출**)**을 클릭하여 변경 사항을 커밋합니다.

단계 **15** 어플라이언스를 시스템 모드에서 클러스터 모드로 전환합니다.

단계 **16** 클러스터의 각 시스템을 AMP for Endpoints 콘솔에 등록하려면 **1~15**단계를 반복합니다.

단계 **17** AMP for Endpoints 콘솔을 사용하여 등록한 후 모든 어플라이언스를 클러스터 모드에 연결합니다.

클러스터 수준에서 파일 평판 서버를 변경하면 로그인한 어플라이언스가 AMP for Endpoints 콘솔에서 자동으로 등록 취소됩니다. 클러스터에 있는 다른 모든 시스템의 등록을 취소해야 합니다. 파일 평판 서버에 대해 동일한 데이터 센터를 선택한 상태에서 AMP for Endpoints 콘솔에 모든 어플라이언스를 다시 등록해야 합니다.

중요! 파일 분석 설정에 필요한 변경 사항

새 퍼블릭 클라우드 파일 분석 서비스를 사용하려는 경우 데이터 센터 격리를 유지하기 위해 다음 지침을 읽어 주십시오.

- 기존 어플라이언스 그룹화 정보는 새 파일 분석 서버에서 유지되지 않습니다. 새 파일 분석 서버에서 어플라이언스를 다시 그룹화해야 합니다.
- 파일 분석 격리로 격리된 메시지는 보존 기간까지 유지됩니다. 격리 유지 기간 후에는 메시지가 파일 분석 격리에서 해제되고 AMP 엔진에서 다시 검사됩니다. 그런 다음 분석을 위해 파일이 새 파일 분석 서버에 업로드되지만 메시지는 파일 분석 격리로 다시 전송되지 않습니다.

자세한 내용은 Cisco AMP Thread Grid 설명서(
http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html)를 참고하십시오.

(퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성

조직의 모든 콘텐츠 보안 어플라이언스가 조직의 어플라이언스에서 분석을 위해 전송한 파일에 대해 클라우드에서 파일 분석 결과 세부사항을 볼 수 있게 하려면 모든 어플라이언스를 동일한 어플라이언스 그룹으로 묶어야 합니다.

참고 시스템 수준에서 어플라이언스 그룹을 구성할 수 있습니다. 어플라이언스 그룹은 클러스터 수준에서 구성할 수 없습니다.

단계 **1** **Security Services > File Reputation and Analysis(**파일 평판 및 분석**)**를 선택합니다.

단계 **2** Appliance Grouping for File Analysis Cloud Reporting(파일 분석 클라우드 보고를 위한 어플라이언스 그룹화) 섹션에서 File Analysis Group ID(파일 분석 클라우드 보고 그룹 ID)를 입력합니다.

- 그룹에 추가되는 첫 번째 어플라이언스인 경우 그룹에 대한 유용한 식별자를 제공합니다.
- 이 ID는 대/소문자를 구분하며 공백을 포함할 수 없습니다.
- 제공하는 ID는 분석을 위해 업로드된 파일에 대한 데이터를 공유하는 모든 어플라이언스에서 동일해야 합니다. 그러나 후속 그룹 어플라이언스에서는 ID가 검증되지 않습니다.
- 그룹 ID를 잘못 입력하거나 어떠한 이유로 인해 이를 변경해야 할 경우 Cisco TAC에서 케이스를 열어야 합니다.
- 이 변경사항은 즉시 적용되므로 커밋이 필요하지 않습니다.
- 그룹의 모든 어플라이언스가 클라우드에서 동일한 파일 분석 서버를 사용하도록 구성해야 합니다.
- 어플라이언스는 단 하나의 그룹에만 속할 수 있습니다.
- 언제든지 그룹에 머신을 추가할 수 있지만 한 번만 추가할 수 있습니다.

단계 **3** **Group Now(**지금 그룹화**)**을 클릭합니다.

분석 그룹에 어떤 어플라이언스가 있습니까?

단계 **1** **Security Services > File Reputation and Analysis(**파일 평판 및 분석**)**를 선택합니다.

단계 **2** Appliance Grouping for File Analysis Cloud Reporting(파일 분석 클라우드 보고를 위한 어플라이언스 그룹화) 섹션에서 **View Appliances(**어플라이언스 보기**)** 을 클릭합니다.

단계 **3** 특정 어플라이언스의 파일 분석 클라이언트 **ID**를 보려면 다음 위치에서 찾으십시오.

어플라이언스	파일 분석 클라이언트 **ID**의 위치
Email Security Appliance	**Security Services(**보안 서비스**) > File Reputation and Analysis(**파일 평판 및 분석**)** 페이지의 Advanced Settings for File Analysis(파일 분석을 위한 고급 설정) 섹션
Web Security Appliance	**Security Services > Anti-Malware and Reputation(**악성코드 차단 및 평판**)** 페이지의 Advanced Settings for File Analysis(파일 분석을 위한 고급 설정) 섹션
Security Management Appliance	**Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 서비스**) > Security Appliances(**보안 어플라이언스**)** 페이지의 하단

파일 평판 검사 및 파일 분석을 위한 메일 정책 구성

단계 **1** **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)** 또는 **Mail Policies(**메일 정책**) > Outgoing Mail Policies(**발신 메일 정책**)**를 선택합니다.

단계 **2** 수정할 메일 정책의 **Advanced Malware Protection** 열에 있는 링크를 클릭합니다.

단계 **3** 옵션을 선택합니다.

- 온프레미스 Cisco AMP Threat Grid Appliance가 없고 예를 들어 기밀성의 이유로 클라우드에 파일을 전송하지 않으려면 **Enable File Analysis(**파일 분석 활성화**)**를 선택 취소합니다.
- 첨부 파일이 검사 불능으로 간주될 경우 어플라이언스에서 수행해야 하는 작업을 선택합니다. 다음과 같은 이유로 인해 어플라이언스에서 파일을 검사할 수 없는 경우 첨부 파일은 검사 불가로 간주됩니다.
  - 메시지 오류**:**
    - 비밀번호로 보호된 아카이브 또는 압축 파일
    - RFC 위반이 발생한 메시지.
    - 200개가 넘는 하위 파일이 포함된 메시지
    - 하위 파일의 중첩 수준이 5가 넘는 메시지
    - 추출 오류가 발생한 메시지
  - 속도 제한 - 어플라이언스에서 파일 업로드 제한에 도달했으므로 파일 분석 서버에서 검사하지 않는 파일입니다.
  - **AMP** 서비스를 사용할 수 없음:
    - 파일 평판 서비스를 사용할 수 없습니다.
    - 파일 분석 서비스를 사용할 수 없습니다.
    - 파일 평판 쿼리 시간 초과
    - 파일 업로드 쿼리 시간 초과
- AMP 엔진에서 검사되지 않은 메시지에 대해 다음 메시지 처리 작업 중 하나를 구성할 수 있습니다.
  - 메시지 삭제
  - 있는 그대로 메시지 전달
  - 정책 격리에 메시지 전송
- 메시지를 전달하려는 경우 다음 추가 작업을 선택합니다.
  - 원본 메시지를 아카이브할지 여부 아카이브된 메시지는 mbox 형식의 로그 파일로 어플라이언스의 amparchive 디렉토리에 저장됩니다. 사전 구성된 AMP Archive(amparchive) 로그 서브스크립션이 필요합니다.

- 메시지 제목을 수정하여 최종 사용자에게 경고할지 여부(예: [경고: 첨부 파일에 악성코드가 포함되었을 수 있음])
- 관리자에게 세밀한 제어를 제공하기 위해 맞춤형 헤더를 추가할지 여부
- 메시지가 다른 주소로 전달되도록 메시지 수신자를 수정할지 여부 Yes(예)를 클릭하고 새 수신자 주소를 입력합니다.
- 대체 대상 호스트로 검사 불가 메시지를 보낼지 여부. Yes(예)를 클릭하고 대체 주소 또는 호스트 이름을 입력합니다.

- 메시지를 정책 격리로 전송하려는 경우 다음 추가 작업을 선택합니다.
  - 드롭다운에서 정책 격리를 선택할지 여부. 격리를 위해 플래그가 지정된 경우, 메시지는 이메일 파이프라인의 끝에 도달하면 격리에 배치되고 이메일 파이프라인의 다른 모든 엔진에 의해 검사됩니다.
  - 원본 메시지를 아카이브할지 여부 아카이브된 메시지는 mbox 형식의 로그 파일로 어플라이언스의 amparchive 디렉토리에 저장됩니다. 사전 구성된 AMP Archive(`amparchive`) 로그 서브스크립션이 필요합니다.
  - 메시지 제목을 수정하여 최종 사용자에게 경고할지 여부(예: [경고: 첨부 파일에 악성코드가 포함되었을 수 있음])
  - 관리자에게 세밀한 제어를 제공하기 위해 맞춤형 헤더를 추가할지 여부
- 첨부 파일이 악성으로 간주될 경우 AsyncOS에서 수행해야 하는 작업을 선택합니다. 다음을 선택합니다.
  - 메시지를 전송할지 또는 삭제할지 여부
  - 원본 메시지를 아카이브할지 여부 아카이브된 메시지는 mbox 형식의 로그 파일로 어플라이언스의 amparchive 디렉토리에 저장됩니다. 사전 구성된 AMP Archive(amparchive) 로그 서브스크립션이 필요합니다.
  - 악성코드 첨부 파일을 제거한 후 메시지를 전송할지 여부
  - 메시지 제목을 수정하여 최종 사용자에게 경고할지 여부(예: [경고: 첨부 파일에서 악성코드가 탐지되었음])
  - 관리자에게 세밀한 제어를 제공하기 위해 맞춤형 헤더를 추가할지 여부
  - 메시지가 다른 주소로 전달되도록 메시지 수신자를 수정할지 여부 **Yes(**예**)**를 클릭하고 새 수신자 주소를 입력합니다.
  - 대체 대상 호스트로 악성 메시지를 보낼지 여부. **Yes(**예**)**를 클릭하고 대체 주소 또는 호스트 이름을 입력합니다.
- 첨부 파일이 파일 분석을 위해 전송된 경우 AsyncOS에서 수행해야 하는 작업을 선택합니다. 다음을 선택합니다.
  - 메시지를 전송하거나 격리할지 여부

- 원본 메시지를 아카이브할지 여부 아카이브된 메시지는 mbox 형식의 로그 파일로 어플라이언스의 amparchive 디렉토리에 저장됩니다. 사전 구성된 AMP Archive(amparchive) 로그 서브스크립션이 필요합니다.
- 메시지 제목을 수정하여 엔드 유저에게 경고할지 여부(예: [경고: 첨부 파일에 악성코드가 포함되었을 수 있음])
- 관리자에게 세밀한 제어를 제공하기 위해 맞춤형 헤더를 추가할지 여부
- 메시지가 다른 주소로 전달되도록 메시지 수신자를 수정할지 여부 **Yes(예)**를 클릭하고 새 수신자 주소를 입력합니다.
- 파일 분석을 위해 전송된 메시지를 대체 대상 호스트로 보낼지 여부. **Yes(예)**를 클릭하고 대체 주소 또는 호스트 이름을 입력합니다.

- (수신 메일 정책에만 해당) 위협 판정이 악성으로 변경된 경우 엔드 유저에게 전달되는 메시지에 대해 수정 조치를 수행하도록 구성합니다. Enable Mailbox Auto Remediation(사서함 자동 치료 활성화)을 선택하고 다음 작업 중 하나를 선택합니다.
  - 이메일 주소로 전달합니다. 악성 첨부 파일이 포함된 메시지를 지정된 사용자(예: 이메일 관리자)에게 전달하려면 이 옵션을 선택합니다.
  - 메시지를 삭제합니다. 엔드 유저의 사서함에서 악성 첨부 파일이 포함된 메시지를 영구적으로 삭제하려면 이 옵션을 선택합니다.
  - 이메일 주소로 전달하고 메시지를 삭제합니다. 악성 첨부 파일이 포함된 메시지를 이메일 관리자 등 지정된 사용자에게 전달하고 엔드 유저의 사서함에서 해당 메시지를 영구적으로 삭제하려면 이 옵션을 선택합니다.

    참고 Office 365 서비스는 이러한 폴더에서 메시지 삭제를 지원하지 않으므로 특정 폴더(예: 지운 편지함)의 메시지는 삭제할 수 없습니다.

    중요 Mailbox Auto Remediation(사서함 자동 치료) 설정을 구성하기 전에 다음을 검토합니다. Office 365 사서함에서 자동으로 메시지 치료, 561 페이지

단계 **4** 변경 사항을 제출 및 커밋합니다.

분석을 위해 전송된 첨부 파일이 포함된 메시지 격리

분석을 위해 전송된 파일을 즉시 workqueue로 릴리스하지 않고 격리하도록 어플라이언스를 구성할 수 있습니다. 격리된 메시지와 해당 첨부 파일이 격리에서 릴리스되면 재검사를 통해 위협이 있는지 확인합니다. 파일 분석 결과가 평판 스캐너에 제공된 후에 메시지가 릴리스되면 확인된 위협이 재검사 도중 발견됩니다.

단계 **1** **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)** 또는 **Mail Policies(메일 정책) > Outgoing Mail Policies(발신 메일 정책)**를 선택합니다.

단계 **2** 수정할 메일 정책의 **Advanced Malware Protection** 열에 있는 링크를 클릭합니다.

단계 **3** Messages with File Analysis Pending(파일 분석이 보류 중인 메시지) 섹션의 Action Applied to Message(메시지에 적용된 작업) 드롭다운에서 **Quarantine(격리)**을 선택합니다.

격리된 메시지는 파일 분석 격리에 저장됩니다. 파일 분석 격리 사용, 480 페이지를 참조하십시오.

단계 **4** (선택 사항) 파일 분석이 보류 중인 메시지 섹션에서 다음과 같은 옵션을 선택합니다.

- 원본 메시지를 아카이브할지 여부 아카이브된 메시지는 mbox 형식의 로그 파일로 어플라이언스의 amparchive 디렉토리에 저장됩니다. 사전 구성된 AMP Archive(amparchive) 로그 서브스크립션이 필요합니다.
- 메시지 제목을 수정하여 최종 사용자에게 경고할지 여부(예: [경고: 첨부 파일에 악성코드가 포함되었을 수 있음])
- 관리자에게 세밀한 제어를 제공하기 위해 맞춤형 헤더를 추가할지 여부

참고 4단계에서 설명한 위 작업은 메시지가 격리에서 해제된 경우에만 적용되며 메시지가 격리로 전송되는 경우에는 적용되지 않습니다.

- 원본 메시지 보관.
- 메시지 제목 수정.
- 맞춤형 헤더 추가.

단계 **5** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

파일 분석 격리 사용, 480 페이지

파일 분석 격리 사용

파일 분석 격리 설정 수정

단계 **1** **Monitor(모니터링)** > **Policy, Virus, and Outbreak Quarantines(정책, 바이러스, 보안 침해 격리)**를 선택합니다.

단계 **2** **File Analysis(파일 분석)** 격리 링크를 클릭합니다.

단계 **3** 보관 기간을 지정합니다.

기본값을 1시간에서 변경하지 않는 것이 좋습니다.

단계 **4** 보관 기간이 경과된 후 AsyncOS에서 수행해야 할 기본 작업을 지정합니다.

단계 **5** 격리 디스크 공간이 꽉 차더라도 지정한 Retention Period(보유 기간)가 끝나기 전에 이 격리의 메시지가 처리되지 않도록 하려면 **Free up space by applying default action on messages upon space overflow(**공간 오버플로 시 메시지에 기본 작업을 적용하여 공간 비우기**)**의 선택을 취소합니다.

단계 **6** Default Action(기본 작업)으로 **Release(**릴리스**)**를 선택한 경우 보관 기간이 경과되기 전에 릴리스되는 메시지에 적용할 추가 작업을 선택적으로 지정합니다.

옵션	정보
제목 수정	추가할 텍스트를 입력하고 이를 원래 메시지 제목의 앞에 추가할지 뒤에 추가할지를 지정합니다. 예를 들어, 사용자가 수신자에게 메시지에 악성코드드 첨부 파일이 포함되었을 수 있다고 경고할 수 있습니다. 참고 제목에 비 ASCII 문자를 올바르게 표시하려면 RFC 2047에 따라 표현해야 합니다.
X-Header 추가	X-Header는 메시지에 대해 수행된 작업의 기록을 제공할 수 있습니다. 이는 예를 들어 특정 메시지가 전달된 이유에 대한 문의를 처리할 때 도움이 될 수 있습니다. 이름과 값을 입력합니다. 예: 이름 = Inappropriate-release-early Value = True
첨부 파일 제거	첨부 파일 제거를 통해 메시지의 악성코드 첨부 파일로부터 보호받을 수 있습니다.

단계 **7** 격리에 액세스할 수 있는 사용자를 지정합니다.

사용자	정보
로컬 사용자	로컬 사용자 목록에는 격리에 액세스할 수 있는 역할의 사용자만 포함됩니다. 모든 관리자는 격리에 대한 완전한 액세스 권한을 가지고 있으므로 리스트에는 관리자 권한의 사용자가 제외됩니다.
외부에서 인증된 사용자	외부 인증을 구성한 상태여야 합니다.
맞춤형 사용자 역할	격리 액세스 권한이 있는 맞춤형 사용자 역할을 하나 이상 만든 경우에만 이 옵션이 표시됩니다.

단계 **8** 변경 사항을 제출 및 커밋합니다.

파일 분석 격리의 메시지를 수동으로 처리

단계 **1** **Monitor(**모니터링**)** > **Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스**,** 보안 침해 격리**)**를 선택합니다.

단계 **2** 파일 분석 격리 표의 해당 행에서 메시지 열에 있는 파란색 숫자를 클릭합니다.

단계 **3** 요건에 따라 메시지에 대해 다음과 같은 작업을 수행합니다.

- Delete
- 릴리스
- 예약된 격리에서의 종료 지연
- 지정한 이메일 주소로 메시지의 사본 전송

중앙 집중식 파일 분석 격리

중앙 집중식 파일 분석 격리에 대한 자세한 내용은 *Cisco Email Security Appliance* 가이드의 "중앙 정책, 바이러스 및 보안 침해 격리" 장을 참고하십시오.

파일 평판 및 분석을 위한 X-헤더

X-헤더를 사용하여 메시지에 메시지 처리 단계의 작업 및 결과를 표시할 수 있습니다. 메일 정책에서 메시지에 X-헤더를 태그로 지정한 다음 콘텐츠 필터를 사용하여 이러한 메시지에 대한 처리 옵션과 최종 작업을 선택합니다.

값은 대/소문자를 구분합니다.

헤더 이름	가능한 값(대/소문자 구분)	설명
X-Amp-Result	정상 악성 Unscannable(검색할 수 없음)	파일 평판 서비스로 처리된 메시지에 적용된 판정
X-Amp-Original-Verdict	파일 알 수 없음 판정 알 수 없음	평판 임계값을 기반으로 한 조정 전에 판정. 이 헤더는 원래 판정이 가능한 값 중 하나인 경우에만 존재합니다.
X-Amp-File-Uploaded	참 거짓	메시지에 첨부된 파일을 분석을 위해 보낸 경우 이 헤더는 "참"입니다.

최종 사용자에게 삭제된 메시지 또는 첨부 파일에 대한 알림 전송

의심스러운 첨부 파일 또는 상위 메시지가 파일 평판 검사에 따라 삭제된 경우 최종 사용자에게 알림을 전송하려면 X-헤더 또는 맞춤형 헤더 및 콘텐츠 필터를 사용합니다.

Advanced Malware Protection 및 클러스터

중앙 집중식 관리를 사용할 경우 클러스터, 그룹 및 머신 수준에서 Advanced Malware Protection과 메일 정책을 활성화할 수 있습니다.

기능 키는 머신 수준에서 추가되어야 합니다.

클러스터 수준에서 어플라이언스 그룹을 구성할 수 없습니다.

Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인

Advanced Malware Protection과 관련된 경고를 보내도록 어플라이언스가 구성되었는지 확인합니다.

다음과 같은 경우에 경고를 수신하게 됩니다.

경고 설명	유형	심각도
온프레미스(프라이빗 클라우드) Cisco AMP Threat Grid Appliance에 대한 연결을 설정하고 다음에 설명된 대로 계정을 활성화해야 합니다. 파일 평판 및 분석 서비스 사용 및 구성 , 468 페이지	안티맬웨어	경고
기능 키 만료	(모든 기능에 기본으로 설정된 대로)	
파일 평판 또는 파일 분석 서비스에 연결할 수 없습니다.	안티바이러스 및 AMP	경고
클라우드 서비스와의 통신이 구성되었습니다.	안티바이러스 및 AMP	정보
평판 및 분석 엔진이 watchdog 서비스에 의해 다시 시작됩니다.	안티바이러스 및 AMP	정보
파일 평판 판정이 변경됩니다.	안티바이러스 및 AMP	정보
분석을 위해 전송할 수 있는 파일 유형이 변경되었습니다. 새 파일 유형의 업로드를 활성화할 수 있습니다.	안티바이러스 및 AMP	정보
일부 파일 유형에 대한 분석을 일시적으로 사용할 수 없습니다.	안티바이러스 및 AMP	경고
지원되는 모든 파일 유형에 대한 분석이 일시적인 중단된 후 복원됩니다.	안티바이러스 및 AMP	정보

관련 주제

- 파일 평판 또는 파일 분석 서버 연결 실패에 대한 여러 경고 , 488 페이지
- 파일 위협 판정 변경 시 조치 수행 , 487 페이지

Advanced Malware Protection 기능에 대한 중앙 집중식 보고 구성

Security Management Appliance에서 보고를 중앙 집중화할 경우 온라인 도움말의 이메일 보고 장 또는 관리 어플라이언스의 사용자 가이드에 있는 Advanced Malware Protection 섹션의 중요 구성 요구 사항을 참고하십시오.

파일 평판 및 파일 분석 보고 및 추적

SHA-256 해시로 파일 식별

파일 이름을 쉽게 변경할 수 있으므로 어플라이언스가 보안 해시 알고리즘(SHA-256)을 사용하여 각 파일에 대해 식별자를 생성합니다. 어플라이언스가 이름이 다른 동일한 파일을 처리할 경우 모든 인스턴스가 동일한 SHA-256으로 인식됩니다. 여러 어플라이언스가 동일한 파일을 처리하는 경우 해당 파일의 모든 인스턴스에 동일한 SHA-256 식별자가 있습니다.

대부분의 보고서에서는 파일이 SHA-256 값(단축 형식

파일 평판 및 파일 분석 보고서 페이지

보고서	설명
AMP(Advanced Malware Protection)	파일 평판 서비스에서 찾은 파일 기반 위협을 보여줍니다. 판정이 변경된 파일은 AMP 판정 업데이트 보고서를 참조하십시오. 그러한 판정은 Advanced Malware Protection 보고서에 적용되지 않습니다. 참고 압축 또는 아카이브 파일에서 추출된 파일 중 하나가 악성인 경우 압축 또는 아카이브 파일의 SHA 값만 Advanced Malware Protection 보고서에 포함됩니다. **Incoming Malware Files by Category(**카테고리별 수신 악성코드 파일**)** 섹션에는 카테고리가 **Custom Detection(**맞춤형 탐지**)**으로 지정된 AMP for Endpoints Console에서 수신한 블랙리스트에 있는 파일 SHA의 백분율이 표시됩니다. AMP for Endpoints Console에서 가져온 블랙리스트에 있는 파일 SHA의 위협 이름이 보고서의 Incoming Malware Threat Files(수신 악성코드 위협 파일) 섹션에서 **Simple Custom Detection(**단순 맞춤형 탐색**)**으로 표시됩니다. 임계값 설정으로 인해 차단된 파일은 보고서의 Incoming Malware Threat Files(수신 악성코드 위협 파일) 섹션에서 **Custom Threshold(**맞춤형 임계값**)**으로 표시됩니다. 보고서의 More Details(추가 세부 정보) 섹션에 있는 링크를 클릭하여 AMP for Endpoints Console에서 블랙리스트에 있는 파일 SHA의 파일 경로 분석 세부 정보를 볼 수 있습니다. 보고서의 AMP 섹션에서 수신 파일 전달에 낮은 위험 판정 세부 정보를 볼 수 있습니다.
Advanced Malware Protection 파일 분석	분석을 위해 전송된 각 파일의 시간 및 판정(또는 임시 판정)을 표시합니다. Cisco AMP Threat Grid 어플라이언스의 허용 목록에 나열된 파일은 "정상"으로 표시됩니다. 허용 목록에 대한 내용은 AMP Threat Grid 온라인 도움말을 참조하십시오. 1,000개가 넘는 파일 분석 결과를 보려면 데이터를 .csv 파일로 내보냅니다. 각 파일의 위협 특성 및 점수를 포함한 자세한 분석 결과를 보려면 드릴다운합니다. SHA를 검색하거나 파일 분석 세부사항 페이지의 하단에서 Cisco AMP Threat Grid 링크를 클릭하여 분석을 수행한 AMP Threat Grid 어플라이언스 또는 클라우드 서버에서 직접 SHA에 대한 추가 세부사항을 볼 수도 있습니다. 참고 압축 또는 아카이브 파일에서 추출된 파일이 분석을 위해 전송된 경우 이러한 추출된 파일의 SHA 값만 파일 분석 보고서에 포함됩니다.

보고서	설명
Advanced Malware Protection 판정 업데이트	이후에 판정이 변경되어 이 어플라이언스에서 처리한 파일을 표시합니다. 이 상황에 대한 내용은 파일 위협 판정 업데이트 , 462 페이지를 참조하십시오. 1,000개가 넘는 판정 업데이트를 보려면 데이터를 .csv 파일로 내보냅니다. 단일 SHA-256에 대해 여러 판정이 변경된 경우 이 보고서에 판정 기록이 아닌 최신 판정만 표시됩니다. SHA-256 링크를 클릭하면 보고서에 대해 선택된 시간 범위와 관계없이 최대 가용 시간 범위 내의 특정 SHA-256의 영향을 받는 모든 메시지를 보려면 SHA-256 링크를 클릭합니다.

다른 보고서의 파일 평판 필터링 데이터 보기

파일 평판 및 분석 데이터는 관련이 있는 경우 다른 보고서에서도 볼 수 있습니다. Detected by Advanced Malware Protection(Advanced Malware Protection에 의해 차단됨/탐지됨)" 열은 기본적으로 보고서에서 숨겨져 있을 수 있습니다. 추가 열을 표시하려면 표 아래의 Columns(열) 링크를 클릭합니다.

Message(메시지**)** 추적 및 **Advanced Malware Protection** 기능 정보

Message(메시지) 추적에서 파일 위협 정보를 검색할 경우 다음 사항에 유의하십시오.

- 파일 평판 서비스에서 찾은 악성 파일을 검색하려면 를 선택합니다. 웹 메시지 추적의 Advanced(고급) 섹션에서 Message Event(메시지 이벤트) 옵션으로 **Advanced Malware Protection Positive**를 선택합니다.
- Message(메시지) 추적에는 파일 평판 처리와 트랜잭션 메시지가 처리되었을 때 반환된 원래 파일 평판 판정에 대한 정보만 포함됩니다. 예를 들어, 파일이 처음에는 클린으로 확인되었으나 판정 업데이트에서는 파일이 악성으로 확인된 경우 클릭 판정만 추적 결과에 표시됩니다.

  메시지 추적 세부사항에 처리 세부사항 섹션이 표시됩니다.

  - 메시지의 각 첨부 파일의 SHA-256
  - 전체 메시지에 대한 최종 Advanced Malware Protection 판정
  - 악성코드가 포함된 것으로 확인된 첨부 파일

- 판정 업데이트는 AMP 판정 업데이트 보고서에서만 사용할 수 있습니다. 판정이 변경된 경우 Message(메시지) 추적의 원래 메시지 세부 정보가 업데이트되지 않습니다. 트랜잭션 특정 첨부 파일이 있는 메시지을(를) 보려면 판정 업데이트 보고서에서 SHA-256을 클릭합니다.
- 분석 결과 및 분석을 위해 파일이 전송되었는지 여부를 포함한 파일 분석에 대한 정보는 파일 분석 보고서에서만 사용할 수 있습니다.

  분석한 파일에 대한 추가 정보는 클라우드 또는 온프레미스 파일 분석 서버에서 사용할 수 있습니다. 파일에 대한 사용 가능한 파일 분석 정보를 보려면 **Reporting(**보고**) Monitor(**모니터링**)** > **File Analysis(**파일 분석**)**를 선택하고 SHA-256을 입력하여 해당 파일을 검색하거나 . 파일 분석

서비스가 임의의 소스에서 파일을 분석한 경우 세부사항을 볼 수 있습니다. 결과는 분석된 파일에 대해서만 표시됩니다.

어플라이언스가 분석을 위해 전송된 파일의 후속 인스턴스를 처리한 경우 그러한 인스턴스가 Message(메시지) 추적 검색 결과에 표시됩니다.

파일 위협 판정 변경 시 조치 수행

단계 **1** AMP 판정 업데이트 보고서를 봅니다.

단계 **2** 엔드 유저에게 전달되었을 가능성이 있는 파일을 포함한 메시지와 관련된 에 대해 메시지 추적 데이터를 보기 위해 관련 SHA-256 링크를 클릭합니다.

단계 **3** 추적 데이터를 사용하여 침해에 포함된 파일의 발신자와 같은 정보뿐 아니라 감염 가능성이 있는 사용자를 파악합니다.

단계 **4** 파일 분석 보고서를 검토하여 이 SHA-256이 분석을 위해 전송되었는지 확인하고 파일의 위협 동작을 더 자세히 이해합니다.

다음에 수행할 작업

관련 주제

파일 위협 판정 업데이트 , 462 페이지

파일 평판 및 분석 트러블슈팅

로그 파일

로그에서:

- `AMP` 및 `amp`는 파일 평판 서비스 또는 엔진을 나타냅니다.
- `Retrospective`는 판정 업데이트를 나타냅니다.
- `VRT` 및 `sandboxing`은 파일 분석 서비스를 나타냅니다.

파일 분석을 포함한 Advanced Malware Protection에 대한 정보가 AMP 엔진 로그에 기록됩니다.

파일 평판 필터링 및 분석 이벤트는 AMP 엔진 로그 및 메일 로그에 기록됩니다.

로그 메시지 "Response received for file reputation query(파일 평판 쿼리에 대해 수신한 응답)"에서 "upload action(업로드 조치)"에 가능한 값은 다음과 같습니다.

- 0: 파일이 평판 서비스에 알려졌으므로 분석을 위해 전송하지 마십시오.
- 1: 전송
- 2: 파일이 평판 서비스에 알려졌으므로 분석을 위해 전송하지 마십시오.

메일 로그에서 "Disposition(처리)"에 가능한 값은 다음과 같습니다.

- 1: 탐지된 악성코드 없음 또는 정상으로 간주됨(정상으로 처리됨)
- 2: 정상
- 3: 악성코드

Spyname은 위협 이름입니다.

추적 사용

파일 평판 필터링 및 분석 기능에는 추적을 사용할 수 없습니다. 그 대신 조직 외부의 계정에서 테스트 메시지를 보냅니다.

파일 평판 또는 파일 분석 서버 연결 실패에 대한 여러 경고

문제

클라우드에서 파일 평판 또는 분석 서비스에 연결하지 못할 경우 이에 대한 여러 경고를 수신하게 됩니다. (단일 경고는 일시적인 문제만을 나타낼 수 있습니다.)

솔루션

- 파일 평판 및 분석 서비스와의 통신을 위한 요건 , 466 페이지에서 요건을 충족했는지 확인합니다.
- 어플라이언스와 클라우드 서비스간의 통신을 차단할 수 있는 네트워크 문제를 확인합니다.
- 쿼리 시간 초과 값을 높입니다.

  Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)를 선택합니다. 쿼리 시간 초과 값은 의 Advanced(고급) 설정 영역에 있습니다.

API 키 오류(온프레미스 파일 분석)

문제

파일 분석 보고서 세부사항을 보려고 시도하거나 Email Security Appliance에서 AMP Threat Grid 서버에 연결하여 분석을 위해 파일을 업로드할 수 없는 경우 API 키 경고를 수신합니다.

솔루션

이 오류는 AMP Threat Grid 서버의 호스트 이름을 변경하고 AMP Threat Grid 서버에서 자체 서명 인증서를 사용할 경우에 발생할 수 있습니다(그 외의 상황에서도 발생할 수 있음). 문제를 해결하려면 다음을 수행합니다.

- 새로운 호스트 이름이 있는 AMP Threat Grid Appliance에서 새 인증서를 생성합니다.
- Email Security Appliance에 새 인증서를 업로드합니다.
- AMP Threat Grid 어플라이언스의 API 키를 재설정합니다. 자세한 내용은 AMP Threat Grid Appliance에 대한 온라인 도움말을 참조하십시오.

관련 주제

- 파일 평판 및 분석 서비스 사용 및 구성 , 468 페이지

파일이 예상대로 업로드되지 않음

문제

파일이 예상대로 평가되거나 분석되지 않습니다. 경고나 명시적인 오류가 없습니다.

솔루션

다음과 같은 변화에 주목하십시오.

- 다른 어플라이언스에서 분석을 위해 파일을 전송하여 파일 분석 서버 또는 파일을 처리 중인 어플라이언스의 캐시에 파일이 이미 존재할 수 있습니다.

분석을 위해 전송할 수 있는 파일 유형에 대한 경고

문제

파일 분석을 위해 전송할 수 있는 파일 유형에 대한 심각도 정보 경고를 수신합니다.

솔루션

이 경고는 지원되는 파일 유형이 변경되거나 어플라이언스에서 지원되는 파일 유형을 알아보기 위해 확인할 때 전송됩니다. 이 문제는 다음과 같은 경우 발생할 수 있습니다.

- 사용자 또는 다른 관리자가 분석을 위해 선택한 파일 유형을 변경합니다.
- 지원되는 파일 유형은 클라우드 서비스의 사용 가능성에 따라 일시적으로 변경됩니다. 이 경우 어플라이언스에서 선택한 파일 유형에 대한 지원이 가능한 즉시 복원됩니다. 두 프로세스 모두 동적이며 사용자의 조치가 필요하지 않습니다.
- 예를 들어, AsyncOS 업그레이드의 일부로 어플라이언스가 재시작됩니다.

분석을 위해 전송할 수 있는 파일 유형에 대한 경고

20 장

데이터 유출 방지

이 장에는 다음 섹션이 포함되어 있습니다.

데이터 유출 방지 개요

DLP(Data Loss Prevention) 기능은 조직의 독점 정보 및 지적 재산권을 보호하고, 사용자가 악의적으로 또는 실수로 네트워크에서 민감한 데이터를 이메일로 전송하지 못하도록 함으로써 정부의 규정을 준수합니다. 발신 메시지에서 법률 또는 회사 정책의 위반 가능성이 있는 데이터를 검사하는 데 사용되는 DLP 정책을 만들어, 직원이 이메일로 전송할 수 없는 데이터 유형을 정의할 수 있습니다.

관련 주제

- DLP 검사 프로세스 개요 , 492 페이지
- 데이터 유출 방지 작동 방식 , 492 페이지

DLP 검사 프로세스 개요

	작업	추가 정보
1.	조직의 사용자가 조직 외부의 수신자에게 이메일 메시지를 전송합니다.	Email Security Appliance는 네트워크로 들어가거나 네트워크를 떠나는 메시지를 처리하는 "게이트웨이" 어플라이언스입니다. 네트워크 내 다른 사용자에게 전송되는 메시지는 검사되지 않습니다.
2.	Email Security Appliance는 메시지가 DLP 검사 단계에 도달하기 전 이메일 "작업 대기열" 단계를 통해 메시지를 처리합니다.	예를 들어 DLP 검사 전 프로세스는 메시지에 스팸이나 악성코드가 없음을 보장합니다. 작업 대기열의 어디에서 DLP 처리가 발생하는지 알아보려면 이메일 파이프라인 플로우, 57 페이지의 작업 대기열 흐름도를 참조해 주십시오.
3.	어플라이언스는 DLP 정책에 명시된 민감한 내용을 메시지 본문, 헤더 및 첨부 파일에서 검사합니다.	데이터 유출 방지 작동 방식 , 492 페이지를 참조하십시오.
4.	민감한 내용이 발견되면 어플라이언스는 메시지 격리, 삭제 또는 제한적 전달 등 데이터 보호를 위한 작업을 수행합니다. 그렇지 않으면 메시지는 계속해서 어플라이언스의 작업 대기열을 통과하게 되며, 문제가 발견되지 않으면 Email Security Appliance가 메시지를 수신자에게 전달합니다.	수행할 작업을 정의합니다. 메시지 작업, 512 페이지를 참조하십시오.

데이터 유출 방지 작동 방식

조직의 누군가가 조직 외부의 수신자에게 메시지를 전송하면 어플라이언스는 정의된 규칙을 기반으로 메시지의 발신자 또는 수신자에게 적용할 발신 메일 정책을 결정합니다. 어플라이언스는 발신 메일 정책에 정의된 DLP 정책을 사용하여 메시지의 내용을 평가합니다.

특히 어플라이언스는 메시지 내용(헤더 및 첨부 파일 포함)에서 단어, 문구, 사전 정의된 패턴(예: 사회 보장 번호) 또는 해당 DLP 정책에서 민감한 내용으로 명시한 정규식을 검사합니다.

어플라이언스는 또한 오탐지 일치를 최소화하기 위해 허용되지 않는 내용의 상황 정보를 평가합니다. 예를 들어 신용카드 번호 패턴과 일치하는 숫자는 만료일, 신용카드 회사명((Visa, AMEX 등) 또는 개인의 이름과 주소와 함께 있는 경우에만 위반으로 평가됩니다.

메시지 내용이 둘 이상의 DLP 정책과 일치하면, 사용자가 지정한 순서를 기반으로 리스트에서 처음 일치하는 DLP 정책이 적용됩니다. 하나의 발신 메일 정책에 내용의 위반 여부를 결정하는 동일한 기준을 사용하는 여러 DLP 정책이 있는 경우, 모든 정책이 단일 내용 검사의 결과를 사용합니다.

민감한 내용이 메시지에 나타날 가능성이 있을 때 어플라이언스는 잠재적 위반에 0~100의 위험 요인 점수를 할당합니다. 이 점수는 메시지에 DLP 위반이 포함되어 있을 가능성을 나타냅니다.

그런 다음 어플라이언스는 이 위험 요인 점수에 대해 정의한 심각도 레벨(예: Critical 또는 Low)을 할당하고, 해당 DLP 정책에서 이 심각도 레벨에 대해 지정한 메시지 작업을 수행합니다.

데이터 유출 방지를 위한 시스템 요구 사항

데이터 유출 방지는 모든 C-Series 및 X-Series 어플라이언스에서 지원됩니다(D-Mode 라이센스를 사용하는 어플라이언스 제외).

데이터 유출 방지 설정 방법

다음 단계를 순서대로 수행합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	DLP 기능을 활성화합니다.	DLP(데이터 유출 방지) 활성화 , 494 페이지
단계 **2**	위반이 발견된 메시지 또는 의심되는 메시지에 대해 수행할 수 있는 작업을 정의합니다. 예를 들면 그러한 메시지를 격리할 수 있습니다.	메시지 작업, 512 페이지
단계 **3**	다음을 수행하는 DLP 정책을 만듭니다. • 조직에서 이메일로 전송해서는 안 되는 내용 식별 • 각 위반에 대해 수행할 작업 지정	방법을 선택합니다. • 마법사를 사용하여 DLP 방지 설정 , 496 페이지 • 사전 정의된 템플릿을 사용하여 DLP 정책 만들기 , 497 페이지 • 맞춤화 DLP 정책 만들기(고급) , 498 페이지
단계 **4**	내용이 둘 이상의 DLP 정책과 일치할 때 메시지가 DLP를 위반하는지를 평가하는 데 어떤 DLP 정책을 사용할지 결정하기 위한 DLP 정책의 순서를 설정합니다.	위반 일치를 위해 이메일 DLP 정책 순서 정돈 , 510 페이지
단계 **5**	DLP 위반을 검사할 메시지의 각 발신자 및 수신자 그룹에 대해 발신 메일 정책을 만들었는지 확인합니다.	메일 정책, 269 페이지을 참고해 주십시오. 개별 DLP 정책에서 허용되는/제한되는 메시지 발신자 및 수신자를 세부적으로 조정하는 방법은 DLP 정책에 대한 메시지 필터링, 509 페이지 섹션을 참조해 주십시오.

	명령 또는 동작	목적
단계 6	DLP 정책을 발신 메일 정책에 할당하여 어떤 DLP 정책을 어떤 발신자 및 수신자에게 적용할 것인지를 지정합니다.	DLP 정책을 발신 메일 정책과 연결, 511 페이지
단계 7	민감한 DLP 정보의 액세스 및 스토리지에 대한 설정을 구성합니다.	• 메시지 추적에서 민감한 DLP 데이터 표시 , 517 페이지 • 메시지 추적 시 중요 정보의 액세스 제어, 898 페이지

DLP(데이터 유출 방지) 활성화

단계 1 **Security Services**(보안 서비스) > **Data Loss Prevention**(데이터 유출 방지)을 선택합니다.

단계 2 **Enable**(활성화)을 클릭합니다.

단계 3 라이센스 계약 페이지의 하단으로 스크롤하고 **Accept**(동의)를 클릭하여 계약에 동의합니다.

참고 라이선스 계약에 동의하지 않으면 DLP가 어플라이언스에서 활성화되지 않습니다.

단계 4 **Data Loss Prevention Global Settings**(데이터 유출 방지 전역 설정)에서 **Enable Data Loss Prevention**(데이터 유출 방지 활성화)를 선택합니다.

단계 5 (권장 사항) 지금은 이 페이지에서 다른 옵션의 선택을 취소합니다.

이 장의 다른 곳에서 설명한 지침에 따라 이러한 설정을 나중에 변경할 수 있습니다.

단계 6 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

데이터 유출 방지 설정 방법 , 493 페이지를 참조하십시오.

관련 주제

- 메시지 추적에서 민감한 DLP 데이터 표시 , 517 페이지
- 마법사를 사용하여 DLP 방지 설정 , 496 페이지
- DLP 엔진 및 콘텐츠 일치 분류자 업데이트, 518 페이지

데이터 손실 방지 정책

관련 주제

- DLP 정책 설명 , 495 페이지
- 사전 정의된 DLP 정책 템플릿, 495 페이지
- 마법사를 사용하여 DLP 방지 설정 , 496 페이지

- 사전 정의된 템플릿을 사용하여 DLP 정책 만들기 , 497 페이지
- 맞춤화 DLP 정책 만들기(고급) , 498 페이지
- 콘텐츠 일치 분류자를 사용하여 허용되지 않는 콘텐츠 정의 , 499 페이지
- DLP 정책에 대한 메시지 필터링, 509 페이지
- 위반 심각도 평가 , 510 페이지
- 위반 일치를 위해 이메일 DLP 정책 순서 정돈 , 510 페이지
- DLP 정책을 기본 발신 메일 정책과 연결 , 511 페이지
- DLP 정책 수정 또는 삭제에 대한 중요한 정보 , 512 페이지

DLP 정책 설명

DLP 정책에는 다음이 포함되어 있습니다.

- 발신 메시지에 민감한 데이터가 포함되었는지 여부를 결정하는 조건 집합
- 메시지에 그러한 데이터가 포함된 경우 수행할 작업

다음을 기반으로 메시지 내용을 평가하는 방법을 지정합니다.

- 허용되지 않는 특정 내용 또는 정보 패턴. 정책에 따라, 식별 번호를 검색할 정규식을 만들어야 할 수 있습니다. 콘텐츠 일치 분류자를 사용하여 허용되지 않는 콘텐츠 정의 , 499 페이지를 참조하십시오.
- 메시지 필터링을 위한 특정 발신자 및 수신자 리스트. DLP 정책에 대한 메시지 필터링, 509 페이지를 참조하십시오.
- 메시지 필터링을 위한 첨부 파일 형식 리스트. DLP 정책에 대한 메시지 필터링, 509 페이지를 참조하십시오.
- 위반의 심각도를 기반으로 서로 다른 작업을 수행하도록 하는 설정. 위반 심각도 평가 , 510 페이지를 참조하십시오.

발신 메일 정책에서 DLP 정책을 활성화할 때 각 정책을 적용할 메시지 발신자 및 수신자를 결정합니다.

사전 정의된 DLP 정책 템플릿

DLP 정책을 간편하게 만들 수 있도록 사전 정의된 정책 템플릿의 대규모 모음이 어플라이언스에 포함되어 있습니다.

템플릿 범주는 다음과 같습니다.

- **Regulatory Compliance(**규정 준수**).** 이 범주의 템플릿은 개인 식별이 가능한 정보, 신용 정보 또는 기타 보호되거나 공개되지 않은 정보가 포함된 메시지와 첨부 파일을 식별합니다.
- **Acceptable Use(**허용되는 사용**).** 이 범주의 템플릿은 경쟁사 또는 제한된 수신자에게 보내는, 조직에 대한 민감한 정보가 포함된 메시지를 식별합니다.
- **Privacy Protection(**개인정보 보호**).** 이 범주의 템플릿은 금융 계좌, 세금 기록 또는 국가 ID의 식별 번호가 포함된 메시지와 첨부 파일을 식별합니다.
- **Intellectual Property Protection(**지적 재산권 보호**).** 이 범주의 템플릿은 조직에서 보호하려는 지적 재산권이 포함되어 있을 수 있는 인기 있는 출판 및 디자인 문서 파일 형식을 식별합니다.

- **Company Confidential(**회사 기밀**).** 이 범주의 템플릿은 회사 회계 정보 및 향후 인수 병합에 대한 정보가 포함된 메시지와 문서를 식별합니다.
- **Custom Policy(**맞춤화 정책**).** 이 "템플릿"을 사용하면 사전 정의된 콘텐츠 일치 분류자 또는 조직에서 지정한 위반 식별 기준을 사용하여 처음부터 고유한 정책을 만들 수 있습니다. 이것은 고급 옵션으로 간주되며, 사전 정의된 정책 템플릿이 네트워크 환경의 고유한 요구 사항을 충족하지 못하는 매우 드문 경우에만 사용해야 합니다.

일부 템플릿에는 맞춤화가 필요합니다.

마법사를 사용하여 **DLP** 방지 설정

DLP 평가 마법사에서는 일반적으로 사용되는 DLP 정책을 구성하고 이를 어플라이언스의 기본 발신 메일 정책에서 활성화할 수 있습니다.

참고 기본적으로 DLP 평가 마법사를 사용하여 추가된 DLP 정책은 탐지된 DLP 위반의 심각도와 상관없이 모든 메시지를 전달합니다. 마법사를 사용하여 만든 정책을 수정해야 합니다.

시작하기 전에

- 어플라이언스에서 기존의 DLP 정책을 제거합니다. 어플라이언스에 기존의 DLP 정책이 없는 경우에만 DLP 평가 마법사를 사용할 수 있습니다.
- 신용카드 번호, 미국 사회 보장 번호, 미국 운전면허증 번호 이외의 계정 번호나 학생 식별 번호가 포함된 메시지를 탐지해야 하는 경우 해당 번호를 식별하는 정규식을 만듭니다. 자세한 내용은 식별 번호 확인을 위한 정규식 , 503 페이지를 참고해 주십시오.

단계 **1** **Security Services(**보안 서비스**) > Data Loss Prevention(**데이터 유출 방지**)**을 선택합니다.

단계 **2** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** **Enable and configure DLP using the DLP Assessment Wizard(DLP** 평가 마법사를 사용하여 **DLP** 활성화 및 구성**)** 확인란을 선택합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

단계 **5** 마법사를 완료합니다.

다음에 유의해야 합니다.

- 캘리포니아에서 운영하며 캘리포니아 거주민의 전산화된 PII(personally identifying information) 데이터를 소유하거나 이에 대한 라이선스가 있는 기업은 미국 국가 규정**(California SB-1386)**을 따라야 합니다. 이 법은 마법사의 정책 선택 사항 중 하나입니다.
- 자동으로 생성된 예약 DLP Incident Summary 보고서를 수신할 이메일 주소를 입력하지 않으면 보고서가 생성되지 않습니다.
- 구성된 설정을 검토하는 동안 변경을 위해 특정 단계로 돌아가는 경우, 검토 페이지에 다시 도달할 때까지 나머지 단계를 다시 진행해야 합니다. 이전에 입력한 모든 설정이 기억됩니다.
- 마법사를 완료하면 기본 발신 메일 정책에서 활성화된 DLP 정책과 함께 Outgoing Mail Policies(발신 메일 정책) 페이지가 표시됩니다. DLP 정책 구성의 요약이 페이지 상단에 표시됩니다.

단계 **6** 변경 사항을 커밋합니다.

다음에 수행할 작업

- (선택 사항) 이러한 DLP 정책을 수정하거나, 추가 정책을 만들거나, 메시지에 대한 전체적인 작업을 변경하거나, 심각도 레벨 설정을 변경하려면 **Mail Policies(**메일 정책**) > DLP Policy Manager(DLP** 정책 관리자**)**를 선택합니다. 자세한 내용은 사전 정의된 템플릿을 사용하여 DLP 정책 만들기 , 497 페이지, 맞춤화 DLP 정책 만들기(고급) , 498 페이지 및 심각도 스케일 조정 , 510 페이지 섹션을 참조해 주십시오.
- (선택 사항) 기타 발신 메일 정책에 대해 기존의 DLP 정책을 활성화하려면 발신 메일 정책을 사용하여 DLP 정책을 발신자 및 수신자에게 할당 , 511 페이지 섹션을 참조하십시오.

관련 주제

- 사전 정의된 템플릿을 사용하여 DLP 정책 만들기 , 497 페이지
- 맞춤화 DLP 정책 만들기(고급) , 498 페이지

사전 정의된 템플릿을 사용하여 **DLP** 정책 만들기

단계 **1** **Mail Policies(**메일 정책**) > DLP Policy Manager(DLP** 정책 관리자**)**를 선택합니다.

단계 **2** **Add DLP Policy(DLP** 정책 추가**)**를 클릭합니다.

단계 **3** 카테고리 이름을 클릭하여 사용 가능한 DLP 정책 템플릿 리스트를 표시합니다.

참고 각 템플릿의 설명을 보려면 **Display Policy Descriptions(**정책 설명 표시**)**를 클릭합니다.

단계 **4** 사용할 DLP 정책 템플릿에 대해 **Add(**추가**)**를 클릭합니다.

단계 **5** (선택 사항) 템플릿의 기본 설정 이름 및 설명을 변경합니다.

단계 **6** 정책에서 하나 이상의 콘텐츠 일치 분류자를 맞춤화하도록 요구하거나 권장하는 경우, 조직의 식별 번호 지정 시스템 패턴을 정의하기 위한 정규식 및 식별 번호와 관련된 단어나 문구의 리스트(고유하게 식별되거나 일반적으로 관련성이 있는)를 입력합니다.

자세한 내용은 다음을 참조해 주십시오.

콘텐츠 일치 분류자를 사용하여 허용되지 않는 콘텐츠 정의 , 499 페이지및 식별 번호 확인을 위한 정규식 , 503 페이지.

참고 사전 정의된 템플릿을 기반으로 하는 정책에 대해서는 콘텐츠 일치 분류자를 추가 또는 제거할 수 없습니다.

단계 **7** (선택 사항) 특정 수신자, 발신자, 첨부 파일 형식 또는 전에 추가된 메시지 태그가 있는 메시지에만 DLP 정책을 적용합니다.

자세한 내용은 DLP 정책에 대한 메시지 필터링, 509 페이지를 참고해 주십시오.

항목이 여러 개인 경우 줄바꿈 또는 쉼표로 구분할 수 있습니다.

단계 **8** Severity Settings(심각도 설정) 섹션에서

- 각 위반 심각도 레벨에 대해 수행할 작업을 선택합니다. 자세한 내용은 위반 심각도 평가 , 510 페이지를 참조하십시오.
- (선택 사항) **Edit Scale(**스케일 수정**)**을 클릭하여 정책에 대한 위반 심각도 스케일을 조정합니다. 자세한 내용은 심각도 스케일 조정 , 510 페이지를 참고하십시오.

단계 **9** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- 마법사를 사용하여 DLP 방지 설정 , 496 페이지
- 맞춤화 DLP 정책 만들기(고급) , 498 페이지

맞춤화 **DLP** 정책 만들기(고급)

참고 맞춤화 정책을 만드는 과정은 매우 복잡합니다. 사전 정의된 DLP 정책 템플릿이 조직의 요구를 충족하지 못하는 경우에만 맞춤화 정책을 만드십시오.

맞춤화 정책 템플릿을 사용하여 처음부터 맞춤화 DLP 정책을 만들고, 사전 정의된 콘텐츠 일치 분류자 또는 맞춤화 분류자를 정책에 추가할 수 있습니다.

정책이 정의된 방식에 따라, 맞춤화 정책은 콘텐츠가 단일 분류자 또는 모든 분류자와 일치하는 경우 DLP 위반을 반환할 수 있습니다.

시작하기 전에

제안 사항: 콘텐츠 위반을 식별하는 기준을 정의합니다. 맞춤 DLP 정책용 콘텐츠 일치 분류자 만들기 , 502 페이지를 참조하십시오. 이 절차 내에서도 이러한 기준을 정의할 수 있습니다.

단계 **1** **Mail Policies(**메일 정책**) > DLP Policy Manager(DLP** 정책 관리자**)**를 선택합니다.

단계 **2** **Add DLP Policy(DLP** 정책 추가**)**를 클릭합니다.

단계 **3** **Custom Policy(**맞춤화 정책**)**를 클릭합니다.

단계 **4** Custom Policy(맞춤화 정책) 템플릿에 대해 **Add(**추가**)**를 클릭합니다.

단계 **5** 정책의 이름과 설명을 입력합니다.

단계 **6** DLP 위반을 구성하는 콘텐츠 및 상황 정보를 식별합니다.

a) 콘텐츠 일치 분류자를 선택합니다.

b) **Add(**추가**)**를 클릭합니다.

- **Create a Classifier(**분류자 만들기**)**를 선택한 경우 맞춤 DLP 정책용 콘텐츠 일치 분류자 만들기 , 502 페이지 섹션을 참조하십시오.
- 그렇지 않은 경우 선택한 분류자가 테이블에 추가됩니다.

c) (선택 사항) 정책에 분류자를 더 추가합니다.

예를 들면, 또 다른 분류자를 추가하고 NOT을 선택하여 오탐지를 일으킬 수 있는 알려진 일치를 제거할 수 있습니다.

d) 여러 분류자를 추가한 경우: 분류자 중 하나와 일치할 때 위반이 되는지 전체와 일치할 때 위반이 되는지를 지정하기 위한 테이블 제목에서 옵션을 선택합니다.

단계 **7** (선택 사항) 특정 수신자, 발신자, 첨부 파일 형식 또는 전에 추가된 메시지 태그가 있는 메시지에만 DLP 정책을 적용합니다.

자세한 내용은 DLP 정책에 대한 메시지 필터링, 509 페이지를 참고해 주십시오.

항목이 여러 개인 경우 줄바꿈 또는 쉼표로 구분할 수 있습니다.

단계 **8** Severity Settings(심각도 설정) 섹션에서

- 각 위반 심각도 레벨에 대해 수행할 작업을 선택합니다. 자세한 내용은 위반 심각도 평가 , 510 페이지을 참고하십시오.
- (선택 사항) **Edit Scale(**스케일 수정**)**을 클릭하여 정책에 대한 위반 심각도 스케일을 조정합니다. 자세한 내용은 심각도 스케일 조정 , 510 페이지을 참조해 주십시오.

단계 **9** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- 마법사를 사용하여 DLP 방지 설정 , 496 페이지
- 사전 정의된 템플릿을 사용하여 DLP 정책 만들기 , 497 페이지

콘텐츠 일치 분류자를 사용하여 허용되지 않는 콘텐츠 정의

콘텐츠 일치 분류자는 이메일로 전송할 수 없는 콘텐츠를 정의하고, 선택적으로 데이터 유출 방지 위반으로 간주하기 위해 콘텐츠가 발생해야 하는 상황 정보를 정의합니다.

조직에서 환자 식별 번호가 이메일로 유출되는 것을 방지하려 한다고 가정해보겠습니다.

어플라이언스가 이러한 번호를 인식하도록 하려면 하나 이상의 정규식을 사용하여 조직에서 사용되는 기록 번호 지정 시스템의 패턴을 지정해야 합니다. 또한 지원 정보로서 기록 번호에 동반될 수 있는 단어와 문구의 리스트를 추가할 수 있습니다. 발신 메시지에서 번호 패턴을 탐지하는 경우 분류자는 지원 정보를 검색하여 해당 패턴이 식별 번호이며 임의의 숫자 문자열이 아닌지 확인합니다. 상황 일치 정보를 포함하면 오탐지 일치가 줄어듭니다.

이 예의 경우 HIPAA 및 HITECH 템플릿을 사용하는 DLP 정책을 만들 수 있습니다. 이 템플릿에는 환자의 식별 번호를 탐지하기 위해 맞춤화할 수 있는 환자 식별 번호 콘텐츠 일치 분류자가 포함되어 있습니다. 123-CL456789 패턴의 번호를 탐지하려면 분류자에 대해 [0-9]{3}\-[A-Z]{2}[0-9]{6} 정규식을 입력할 수 있습니다. 관련 문구로 "Patient ID"를 입력합니다. 정책 만들기를 종료하고 발신 메일 정

책에서 활성화합니다. 변경 사항을 제출 및 커밋합니다. 이제 번호 패턴과 매우 유사한 "Patient ID"라는 문구가 있는 발신 메시지에서 번호 패턴이 탐지되면 DLP 정책은 DLP 위반을 반환합니다.

DLP 정책에서 콘텐츠 일치 분류자 사용

다수의 사전 정의된 DLP 정책 템플릿에는 RSA의 콘텐츠 일치 분류자가 포함되어 있습니다. 조직에서 데이터에 사용되는 패턴을 식별하도록 하려면 이러한 분류자 중 일부에 맞춤화가 필요합니다.

맞춤화 DLP 정책을 만드는 경우 사전 정의된 분류자를 선택할 수도 있고 분류자를 직접 만들 수도 있습니다.

관련 주제

- 콘텐츠 일치 분류자 예, 500 페이지
- 맞춤 DLP 정책용 콘텐츠 일치 분류자 만들기 , 502 페이지
- 민감한 콘텐츠 식별을 위한 분류자 탐지 규칙(맞춤화 DLP 정책 전용) , 503 페이지
- 식별 번호 확인을 위한 정규식 , 503 페이지
- 민감한 DLP 용어(맞춤화 DLP 정책 전용)의 맞춤화 사전 사용 , 505 페이지
- 의심스런 위반의 위험 요인 결정자 , 506 페이지
- 맞춤화 콘텐츠 분류자가 사용되는 정책 보기 , 508 페이지

콘텐츠 일치 분류자 예

다음은 분류자가 메시지 콘텐츠와 어떻게 일치하는가를 보여주는 예입니다.

- 신용 카드 번호, 500 페이지
- US Social Security Number(미국 사회 보장 번호), 501 페이지
- ABA 라우팅 번호, 501 페이지
- 드라이버 라이선스 번호(미국) , 501 페이지
- NPI(National Provider ID)(미국), 501 페이지
- 성적표(영어), 502 페이지
- 재무제표(영어), 502 페이지

신용 카드 번호

몇몇 DLP 정책 템플릿에는 Credit Card Number(신용카드 번호) 분류자가 포함되어 있습니다. 신용카드 번호 자체에는 숫자와 구두점 패턴, 발행자 접두사, 최종 검사 숫자 등 여러 제약 조건이 있습니다. 일치를 확인하려면 분류자에 만료일 또는 카드 발급자 이름과 같은 추가 지원 정보가 필요합니다. 이렇게 하면 오탐지의 수가 줄어듭니다.

예:

- `378734493671000`(지원 정보가 없으므로 일치하지 않음)
- `378734493671000 VISA`(일치)
- `378734493671000 만료: 12/2019`(일치)

US Social Security Number(미국 사회 보장 번호)

US Social Security Number(미국 사회 보장 번호) 분류자에는 생년월일, 이름, SSN 문자열 등 지원 데이터와 함께 적절한 형식의 번호가 필요합니다.

예:

- `321-02-3456`(지원 정보가 없으므로 일치하지 않음)
- `SSN: 132-45-6788`(일치)

ABA 라우팅 번호

ABA Routing Number(ABA 라우팅 번호) 분류자는 Credit Card Number(신용카드 번호) 분류자와 유사합니다.

예:

- `119999992`(지원 정보가 없으므로 일치하지 않음)
- `ABA No. 800000080`(일치)

드라이버 라이선스 번호(미국)

많은 정책에서 US Drivers License(미국 운전면허증) 분류자를 사용합니다. 기본적으로, 이 분류자는 미국에서 발급한 드라이버 라이선스를 검색합니다. California AB-1298 및 Montana HB-732와 같은 미국 주 전용 정책은 각 주의 미국 운전면허증만 검색합니다.

개별 주 분류자는 해당 주의 패턴을 기반으로 일치를 확인하며, 이때 해당 주 이름 또는 약어와 추가 지원 데이터가 필요합니다.

예:

- `CA DL# C3452362`(번호 및 지원 데이터에 대한 올바른 패턴이 있으므로 일치)
- `California DL# C3452362`(일치)
- `DL: C3452362`(지원 데이터가 충분하지 않으므로 일치하지 않음)
- `California C3452362`(지원 데이터가 충분하지 않으므로 일치하지 않음)
- `OR DL# C3452362`(일치)
- `OR DL# 3452362`(Oregon에 대한 잘못된 패턴이므로 일치하지 않음)
- `WV DL# D654321`(West Virginia에 대한 잘못된 패턴이므로 일치하지 않음)
- `WV DL# G654321`(일치)

NPI(National Provider ID)(미국)

US National Provider Identifier(미국 NPI) 분류자는 검사 숫자가 포함된 10자리 번호인 미국 NPI(National Provider Identifier) 번호를 검사합니다.

예:

- `NPI No. 1245319599`(NPI에 대해 일치)
- `NPI No. 1235678996`(NPI에 대해 일치)
- `3459872347`(지원 정보가 없으므로 일치하지 않음)
- `NPI: 3459872342`(검사 숫자가 올바르지 못하므로 일치하지 않음)

성적표(영어)

사전 정의된 FERPA(Family Educational Rights and Privacy Act) DLP 정책 템플릿은 Student Records(학생 기록) 분류자를 사용합니다. 이것을 맞춤화된 Student Identification Number(학생 식별 번호) 분류자와 결합하면 특정 학생 ID 패턴을 더 정확하게 탐지할 수 있습니다.

예:

- 가을 학기 과정 번호: CHEM101, ECON102, MATH103(일치)

재무제표(영어)

사전 정의된 SOX(Sarbanes-Oxley) 정책 템플릿은 Corporate Financials(기업 금융) 분류자를 사용하여 비공개 기업 금융 정보를 검색합니다.

예:

2016년 6월 30일에 종료된 분기의 총 수익, 현재 자산 및 현금흐름표입니다. (일치)

맞춤 DLP 정책용 콘텐츠 일치 분류자 만들기

맞춤화 분류자를 만들면 맞춤 DLP 정책을 만들 때 사용할 수 있는 분류자 리스트에 추가됩니다.

프로시저

	명령 또는 동작	목적
단계 1	콘텐츠 일치 분류자를 사용하여 잠재적 DLP 위반을 식별하는 방법을 이해합니다.	참조: • 콘텐츠 일치 분류자를 사용하여 허용되지 않는 콘텐츠 정의 , 499 페이지 • 콘텐츠 일치 분류자 예, 500 페이지
단계 2	**Mail Policies(메일 정책) > DLP Policy Customizations(DLP 정책 맞춤화)**를 선택하고 **Add Custom Classifier(맞춤 분류자 추가)**를 클릭합니다. 분류자 이름과 설명을 입력합니다.	—
단계 3	근사치와 최소 총 점수를 입력합니다.	의심스런 위반의 위험 요인 결정자 , 506 페이지 항목을 참조하십시오.
단계 4	다음 탐지 규칙 유형 중 하나를 선택하고 관련 콘텐츠 일치 기준을 정의합니다. • 단어 또는 구 • 사전의 텍스트 • 정규식 또는 • 기존 데이터 유출 방지 엔티티	참조: • 민감한 콘텐츠 식별을 위한 분류자 탐지 규칙(맞춤화 DLP 정책 전용) , 503 페이지 • 민감한 DLP 용어(맞춤화 DLP 정책 전용)의 맞춤화 사전 사용 , 505 페이지 • 식별 번호 확인을 위한 정규식 , 503 페이지
단계 5	(선택 사항) **Add Rule(규칙 추가)**을 클릭하여 규칙을 더 추가합니다.	Weight(가중치) 및 Max Score(최대 점수)에 대한 자세한 내용은 의심스런 위반의 위험 요인 결정자 , 506 페이지 섹션을 참조해 주십시오.

	명령 또는 동작	목적
단계 **6**	여러 규칙을 포함하는 경우 규칙이 모두 일치해야 할지(**All**) 아니면 하나만 일치하면 될지(**Any**)를 선택합니다.	이 설정은 Rules(규칙) 섹션의 상단에 있습니다.
단계 **7**	변경 사항을 제출 및 커밋합니다.	—

다음에 수행할 작업

맞춤화 DLP 정책에서 맞춤화 콘텐츠 분류자를 사용합니다. 맞춤화 DLP 정책 만들기(고급) , 498 페이지를 참조하십시오.

관련 주제

- 맞춤화 콘텐츠 분류자가 사용되는 정책 보기 , 508 페이지

민감한 콘텐츠 식별을 위한 분류자 탐지 규칙(맞춤화 **DLP** 정책 전용)

콘텐츠 일치 분류자에는 메시지 또는 문서에서 DLP 위반을 탐지하기 위한 규칙이 필요합니다. 분류자는 다음과 같은 탐지 규칙을 하나 이상 사용할 수 있습니다.

- 단어 또는 문구. 분류자가 찾아보아야 하는 단어 및 문구의 리스트. 항목이 여러 개인 경우 쉼표나 줄 바꿈으로 구분해 주십시오.
- 정규식. 메시지나 첨부 파일에 대한 검색 패턴을 정의하기 위한 정규식. 또한 오탐지를 방지하기 위해 일치에서 제외할 패턴을 정의할 수 있습니다. 자세한 내용은 식별 번호 확인을 위한 정규식 , 503 페이지 및 식별 번호 확인을 위한 정규식의 예 , 505 페이지 섹션을 참조하십시오.
- 사전. 관련 단어 및 문구의 사전. 어플라이언스에는 사전 정의된 사전을 포함할 수도 있고 직접 만들 수도 있습니다. 민감한 DLP 용어(맞춤화 DLP 정책 전용)의 맞춤화 사전 사용 , 505 페이지를 참조하십시오.
- 엔티티. 신용카드 번호, 주소, 사회 보장 번호, ABA 라우팅 번호와 같은 공통된 유형의 민감한 데이터를 식별하는 사전 정의된 패턴. 엔티티의 설명을 보려면 **Mail Policies(메일 정책) > DLP Policy Manager(DLP 정책 관리자)**로 이동한 다음 **Add DLP Policy(DLP 정책 추가)**, **Privacy Protection(개인정보 보호)**, **Display Policy Descriptions(정책 설명 표시)**를 차례로 클릭합니다.

식별 번호 확인을 위한 정규식

일부 정책 템플릿에서는 하나 이상의 콘텐츠 일치 분류자를 맞춤화해야 합니다. 여기에는 기밀 정보에 연결될 수 있는 식별 번호(맞춤화 계정 번호, 환자 식별 번호 또는 학생 ID) 검색을 위한 정규식을 만드는 것이 포함됩니다. **Perl Compatible Regular Expression(PCRE2)** 구문을 사용하여 콘텐츠 일치 분류자 또는 DLP 정책 템플릿을 위한 정규식을 추가할 수 있습니다. 어플라이언스에서 DLP 기능이 활성화된 경우에만 정규식의 PCRE2 호환성이 검증됩니다.

참고 정규식은 대/소문자를 구분하므로, 대문자와 소문자(예: `[a-zA-Z]`)를 포함해야 합니다. 특정 문자만 사용되는 경우 그에 따라 정규식을 정의할 수 있습니다.

패턴이 덜 구체적일수록(예: 8자리 숫자) 실제 고객 번호에서 임의의 8자리 숫자를 구별하기 위해 추가 단어와 문구를 정책에서 더 많이 검색해야 합니다.

다음 표를 분류자용 정규식을 만들기 위한 가이드로 사용하십시오.

요소	설명
정규식(abc)	정규식에 있는 지시문의 시퀀스가 문자열의 일부와 일치하는 경우 분류자용 정규식은 문자열과 일치합니다. 예를 들어 정규식 **ACC**는 문자열 **ACCOUNT** 및 **ACCT**와 일치합니다.
[ ]	문자 집합을 나타내려면 대괄호를 사용합니다. 문자는 개별적으로 또는 범위 내에서 정의할 수 있습니다. 예를 들어 **[a-z]**는 a에서 z까지의 모든 소문자와 일치하는 반면, **[a-zA-Z]**는 A에서 Z까지의 모든 대문자 및 소문자와 일치합니다. **[xyz]**는 x, y 또는 z 문자와만 일치합니다.
백슬래시 특수 문자(\)	백슬래시 문자는 특수 문자를 이스케이프합니다. 리터럴 마침표와만 일치하고, \$ 시퀀스는 리터럴 달러 기호와만 일치하고, \^ 시퀀스는 리터럴 캐럿 기호와만 일치합니다. 백슬래시 문자는 또한 \d와 같은 토큰으로 시작됩니다. 중요 참고 사항**:** 백슬래시는 파서용 특수 이스케이프 문자이기도 합니다. 따라서 정규식에 백슬래시를 포함하려면 구문 분석 후 하나의 "진짜" 백슬래시만 남아 정규식 시스템으로 전달되도록 백슬래시를 *2*개 사용해야 합니다.
\d	숫자(0-9)와 일치하는 토큰. 둘 이상의 숫자와 일치하도록 하려면 {}에 정수를 입력하여 숫자 길이를 정의합니다. 예를 들어 \d는 5와 같은 단일 숫자와만 일치하며 55와는 일치하지 않습니다. \d{2}는 55와 같은 두 자리 숫자와 일치하지만 5와는 일치하지 않습니다.
\D	숫자가 아닌 문자와 일치하는 토큰. 둘 이상의 숫자가 아닌 문자와 일치하도록 하려면 {}에 정수를 입력하여 숫자 길이를 정의합니다.
\w	영숫자 문자 및 밑줄과 일치하는 토큰(a-z, A-Z, 0-9 및 _).
반복 수{min,max}	이전 토큰의 반복 수를 나타내는 정규식 표기법이 지원됩니다. 예를 들어 " \d{8}" 식은 12345678 및 11223344와 일치하지만 8과는 일치하지 않습니다.
또는 (|)	대체 또는 "or" 연산자. A 및 B가 정규식이면 "A|B" 식은 "A" 또는 "B"와 일치하는 문자열과 일치합니다. 정규식에서 숫자 패턴을 결합하는 데 사용할 수 있습니다. 예를 들어 "foo|bar" 식은 foo 또는 bar와 일치하지만 foobar와는 일치하지 않습니다.

관련 주제

- 식별 번호 확인을 위한 정규식의 예 , 505 페이지

식별 번호 확인을 위한 정규식의 예

식별 또는 계정 번호에서 숫자와 문자의 패턴을 설명하는 단순한 정규식은 다음과 같을 수 있습니다.

- 8자리 숫자: `\d{8}`
- 숫자 집합 사이에 하이픈이 있는 식별 코드: `\d{3}-\d{4}-\d`
- 대문자 또는 소문자가 될 수 있는 단일 문자로 시작하는 식별 코드: `[a-zA-Z]\d{7}`
- 3자리 숫자로 시작하고 그 뒤에 9개 대문자가 오는 식별 코드: `\d{3}[A-Z]{9}`
- 검색할 서로 다른 숫자 패턴을 정의하기 위해 | 사용: `\d{3}[A-Z]{9}|\d{2}[A-Z]{9}-\d`

민감한 DLP 용어(맞춤화 DLP 정책 전용)의 맞춤화 사전 사용

AsyncOS는 사전 정의된 사전 집합과 함께 제공됩니다. 그러나 맞춤화 DLP 사전을 만들어서 DLP 검사 기능으로 검색할 용어를 지정할 수도 있습니다.

여러 가지 방법으로 맞춤화 DLP 사전을 만들 수 있습니다.

- 맞춤화 DLP 사전(Custom DLP Dictionaries) 직접 추가 , 505 페이지
- DLP 사전을 텍스트 파일로 만들기 , 505 페이지 및 DLP 사전 가져오기 , 506 페이지
- 다른 Email Security Appliance에서 DLP 사전 내보내기 , 506 페이지를 수행한 다음 DLP 사전 가져오기 , 506 페이지를 수행합니다.

맞춤화 DLP 사전(Custom DLP Dictionaries) 직접 추가

단계 1 **Mail Policies(메일 정책) > DLP Policy Manager(DLP 정책 관리자)**를 선택합니다.

단계 2 **Advanced Settings(고급 설정)** 섹션에서 **Custom DLP Dictionaries(맞춤화 DLP 사전)** 옆에 있는 링크를 클릭합니다.

단계 3 **Add Dictionary(사전 추가)**를 클릭합니다.

단계 4 맞춤화 사전의 이름을 입력합니다.

단계 5 용어 리스트에 새 사전 항목(단어 및 문구)을 입력합니다.

사전 용어는 대/소문자를 구분하며 비 ASCII 문자를 포함할 수 있습니다.

여러 항목을 입력할 경우 줄 바꿈으로 항목을 구분해 주십시오.

단계 6 **Add(추가)**를 클릭합니다.

단계 7 변경 사항을 제출 및 커밋합니다.

DLP 사전을 텍스트 파일로 만들기

자신의 사전을 로컬 시스템에 텍스트 파일로 만든 다음 어플라이언스로 가져올 수 있습니다. 사전 텍스트 파일에서 각 용어에 줄 바꿈을 사용하십시오. 사전 용어는 대/소문자를 구분하며 비 ASCII 문자를 포함할 수 있습니다.

DLP 사전 내보내기

참고 사전 정의된 DLP 사전은 내보낼 수 없습니다.

단계 1 **Mail Policies(**메일 정책**) > DLP Policy Manager(DLP** 정책 관리자**)**를 선택합니다.

단계 2 Advanced Settings(고급 설정) 아래에서 **Custom DLP Dictionaries(**맞춤화 **DLP** 사전**)** 섹션에 대한 링크를 클릭합니다.

단계 3 **Export Dictionary(**사전 내보내기**)**를 클릭합니다.

단계 4 내보낼 사전을 선택합니다.

단계 5 사전의 파일 이름을 입력합니다.

단계 6 내보낸 사전을 저장할 위치(로컬 컴퓨터 또는 어플라이언스의 구성 디렉터리)를 선택합니다.

단계 7 파일의 인코딩을 선택합니다.

단계 8 **Submit(**제출**)**을 클릭하고 파일을 저장합니다.

DLP 사전 가져오기

시작하기 전에

Email Security Appliance에서 비 DLP 사전에서 내보낸 파일을 가져오는 경우 먼저 텍스트 파일에서 가중치 값을 제거하고 정규식을 단어나 문구로 변환해야 합니다.

단계 1 **Mail Policies(**메일 정책**) > DLP Policy Manager(DLP** 정책 관리자**)**를 선택합니다.

단계 2 **Advanced Settings(**고급 설정**)** 섹션에서 **Custom DLP Dictionaries(**맞춤화 **DLP** 사전**)** 옆에 있는 링크를 클릭합니다.

단계 3 **Import Dictionary(**사전 가져오기**)**를 클릭합니다.

단계 4 로컬 컴퓨터 또는 어플라이언스의 구성 디렉터리에서 가져올 파일을 선택합니다.

단계 5 인코딩을 선택합니다.

단계 6 **Next(**다음**)**를 클릭합니다.

"Success(성공)" 메시지가 나타나고 Add Dictionary(사진 추가) 페이지에 가져온 사전이 표시됩니다. 그러나 아직 프로세스가 완료되지 않았습니다.

단계 7 사전의 이름을 지정하고 수정합니다.

단계 8 제출을 클릭합니다.

의심스런 위반의 위험 요인 결정자

어플라이언스는 메시지에서 DLP 위반을 검사할 때 메시지에 위험 요인 점수를 할당합니다. 이 점수는 메시지에 DLP 위반이 포함되어 있을 가능성을 나타냅니다. 0점은 메시지에 위반이 포함되어 있을 가능성이 거의 없음을 나타냅니다. 100점은 메시지에 위반이 포함된 것이 거의 확실함을 나타냅니다.

사전 정의된 템플릿 기반 **DLP** 정책의 경우

사전 정의된 템플릿에서 만든 DLP 정책에 대한 위험 요인 점수 매개변수는 보거나 수정할 수 없습니다. 그러나 특정 DLP 정책에 대해 오탐지 일치가 너무 많으면 해당 정책의 심각도 스케일을 조정할 수 있습니다. 위반 심각도 평가 , 510 페이지를 참조하십시오. SOX(Sarbanes-Oxley) 템플릿과 같이 콘텐츠 일치 분류자가 없는 템플릿 기반 정책의 경우, 검사 엔진은 메시지가 정책을 위반하면 항상 위험 요인 값 "75"를 반환합니다.

맞춤화 **DLP** 정책의 경우

맞춤화 DLP 정책에 대해 콘텐츠 일치 분류자를 만들 때 위험 요인 점수를 결정하기 위해 사용되는 값을 지정합니다.

- **Proximity(**근접성**)**. 메시지나 첨부 파일에서 위반으로 계산되기 위해 규칙 일치가 발생해야 하는 근접성 정도. 예를 들어 긴 메시지 상단 근처에 사회 보장 번호와 유사한 숫자 패턴이 발생하는 경우 및 하단의 발신자 서명에 주소가 나타나는 경우, 이 둘은 관련이 없는 것으로 간주되고 데이터가 일치로 계산되지 않습니다.
- **Minimum Total Score(**최소 총 점수**)**. 민감한 콘텐츠에 DLP 위반 레이블을 지정하기 위해 필요한 최소 위험 요인 점수. 메시지 일치의 점수가 최소 총 점수를 충족하지 못하면 민감한 데이터로 간주되지 않습니다.
- **Weight(**가중치**)**. 각 맞춤화 규칙을 만들 때 규칙의 중요도를 나타내기 위해 "가중치"를 지정합니다. 탐지 규칙 일치 수와 규칙의 가중치를 곱해 점수가 산출됩니다. 가중치가 10인 규칙 인스턴스가 2개이면 점수는 20입니다. 분류자 관점에서 한 규칙이 나머지 규칙보다 더 중요하면 더 큰 가중치를 할당해야 합니다.
- **Maximum Score(**최대 점수**)**. 규칙의 최대 점수는 가중치가 낮은 규칙에 대한 다수의 일치가 최종 검사 점수를 왜곡하지 못하게 합니다.
- **Minimum Score(**최소 점수**)**. DLP Policy Customizations(DLP 정책 맞춤화) 페이지의 Custom Classifiers Settings(맞춤형 분류자 설정) 섹션에서 선택한 **Use recommended minimum scores for entity-based rules(**엔티티 기반 규칙에 권장 최소 점수 사용**)** 확인란에 따라 권장 최소 점수를 사용하거나 가중치를 사용할 수 있습니다. 자세한 내용은 엔티티 기반 규칙에 대 한 최소 점수 사용 (맞춤형 DLP 정책만 해당), 508 페이지을 참조해 주십시오.

위험 요인을 계산하기 위해 분류자는 탐지 규칙에 대한 일치 수를 규칙의 가중치와 곱합니다. 이 값이 탐지 규칙의 최대 점수를 초과하면 분류자는 최대 점수 값을 사용합니다. 분류자에 둘 이상의 탐지 규칙이 있는 경우 모든 탐지 규칙에 대한 점수가 단일 값에 추가됩니다. 분류자는 위험 요인을 만들기 위해 다음 표에 있는 로그 스케일을 사용하여 스케일 10~100에서 탐지 규칙 점수(10~10,000)를 매핑합니다.

표 ***39:*** 탐지 규칙 점수에서 위험 요인 점수를 계산하는 방법

규칙 점수	위험 요인
10	18
20	28

규칙 점수	위험 요인
30	33
50	41
100	50
150	56
300	65
500	72
1000	82
10000	100

엔티티 기반 규칙에 대 한 최소 점수 사용 (맞춤형 DLP 정책만 해당)

단계 1 **Mail Policies**(메일 정책) > **DLP Policy Customizations**(DLP 정책 맞춤화)로 이동합니다.

단계 2 **Custom Classifiers Settings**(맞춤형 분류자 설정) 섹션에서 **Use recommended minimum scores for entity-based rules**(엔티티 기반 규칙에 권장 최소 점수 사용) 확인란을 선택합니다.

이 옵션을 선택하면 가중치 대신 구성된 최소 점수를 사용하여 엔티티 기반 규칙의 점수를 계산합니다.

예를 들어, 이 옵션을 비활성화한 경우 메시지에 가중치가 10으로 구성된 특정 엔터티의 규칙 일치 항목이 5개가 있으면 이 규칙은 5개의 일치 항목에 10을 곱한 값인 50으로 점수를 계산합니다. 엔티티의 최소 점수를 10으로 지정하여 이 옵션을 활성화한 경우에는 구성된 최소 점수와 부분 일치 및 전체 일치 수를 기준으로 점수가 계산됩니다.

참고 Use recommended minimum scores for entity-based rules(엔티티 기반 규칙에 권장 최소 점수 사용) 옵션을 선택한 경우 모든 분류자의 최소 총 점수를 엔티티 기반 규칙과 함께 검토해야 합니다.

단계 3 **Submit**(제출)을 클릭하여 변경 사항을 커밋합니다.

이 옵션을 활성화한 후에는 맞춤형 분류자의 엔티티 기반 규칙에 대한 최소 점수를 검토해야 합니다. 자세한 내용은 맞춤 DLP 정책용 콘텐츠 일치 분류자 만들기 , 502 페이지를 참고하십시오.

맞춤화 콘텐츠 분류자가 사용되는 정책 보기

단계 1 **Mail Policies**(메일 정책) > **DLP Policy Customizations**(DLP 정책 맞춤화)를 선택합니다.

단계 2 **Custom Classifiers**(맞춤화 분류자) 섹션에서 Custom Classifiers(맞춤화 분류자) 테이블의 제목에 있는 **Policies**(정책) 링크를 클릭합니다.

다음에 수행할 작업

관련 주제

- 맞춤 DLP 정책용 콘텐츠 일치 분류자 만들기 , 502 페이지

DLP 정책에 대한 메시지 필터링

성능과 정확성을 높이려면 다음 기준을 기반으로 특정 메시지에만 DLP 정책을 적용할 수 있습니다.

옵션	설명
발신자 및 수신자 기준 필터링	다음 중 하나를 사용하여 지정하는 발신자 또는 수신자를 포함하거나 포함하지 않는 메시지로 DLP 정책의 적용을 제한할 수 있습니다. • 전체 이메일 주소: `user@example.com` • 부분 이메일 주소: `user@` • 도메인의 모든 사용자: `@example.com` • 부분 도메인의 모든 사용자: `@.example.com` 항목이 여러 개인 경우 줄바꿈 또는 쉼표로 구분해 주십시오. AsyncOS는 먼저 발신 메일 정책을 기준으로 발신 메시지의 수신자 및 발신자를 확인한 다음, 해당 메일 정책에 대해 활성화된 DLP 정책에 지정된 발신자 및 수신자 필터를 기준으로 수신자 및 발신자를 확인합니다. 예를 들면 파트너 도메인의 수신자를 제외하고, 모든 발신자가 특정 유형의 정보를 보내지 못하게 할 수 있습니다. 파트너 도메인의 모든 사용자를 면제하는 필터를 포함하여 해당 정보에 대한 DLP 정책을 만들고, 모든 발신자에게 적용되는 발신 메일 정책에 이 DLP 정책을 포함하면 됩니다.
첨부 파일 형식 기준 필터링	특정 첨부 파일 형식을 포함하거나 포함하지 않은 메시지만 검사하는 것으로 DLP 정책을 제한할 수 있습니다. 첨부 파일 범주를 선택하고 사전 정의된 파일 형식을 선택하거나, 나열되지 않은 파일 형식을 지정합니다. 사전 정의되지 않은 파일 형식을 지정하면 AsyncOS는 첨부 파일의 확장명을 기반으로 파일 형식을 검색합니다. 최소 파일 크기의 첨부 파일로 DLP 검사를 제한할 수도 있습니다.
메시지 태그 기준 필터링	DLP 정책을 특정 문구가 포함된 메시지로 제한하려는 경우 메시지 또는 콘텐츠 필터를 사용하여 발신 메시지에서 문구를 검색하고 맞춤화 메시지 태그를 메시지에 삽입할 수 있습니다. 자세한 내용은 콘텐츠 필터 작업, 293 페이지 및 메시지 필터를 사용하여 이메일 정책 적용, 137 페이지 섹션을 참조하십시오.

위반 심각도 평가

DLP 검사 엔진은 잠재적인 DLP 위반을 탐지하면 해당 인스턴스가 실제로 DLP 위반일 가능성을 나타내는 위험 요인 점수를 계산합니다. 이 위험 요인 점수를 정책에 정의된 심각도 스케일과 비교하여 심각도 레벨(예: Low 또는 Critical)이 결정됩니다. 각 심각도 레벨에서 위반에 대해 수행할 작업을 지정합니다(아무런 작업도 수행하지 않는 Ignore 제외). 각 심각도 레벨에 도달하기 위해 필요한 위험 요인 점수를 조정할 수 있습니다.

관련 주제

- 심각도 스케일 조정 , 510 페이지

심각도 스케일 조정

모든 정책에는 기본 심각도 스케일이 있습니다. 각 정책에서 이 스케일을 조정할 수 있습니다.

예를 들어 기본적으로 위험 요인 점수가 90~100인 경우 위반의 심각도 레벨은 Critical(중대)입니다. 그러나 특정 정책과 일치하는 위반의 경우 잠재적 데이터 손실에 대한 민감도를 높일 수 있습니다. 이 DLP 정책의 경우 Critical(중대) 심각도 레벨을 위험 요인 점수 75~100의 위반으로 변경할 수 있습니다.

단계 **1** **Mail Policies(**메일 정책**) > DLP Policy Manager(DLP** 정책 관리자**)**를 선택합니다.
단계 **2** 수정할 정책의 이름을 클릭합니다.
단계 **3** **Severity Settings(**심각도 설정**)** 섹션에서 **Edit Scale(**스케일 수정**)**을 클릭합니다.
단계 **4** 스케일의 화살표를 사용하여 심각도 레벨의 점수를 조정합니다.
단계 **5** **Done(**완료**)**을 클릭합니다.
단계 **6** Severity Scale(심각도 스케일) 테이블에서 점수가 원하는 대로 지정되었는지 확인합니다.
단계 **7** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

관련 주제

- 위반 심각도 평가 , 510 페이지

위반 일치를 위해 이메일 **DLP** 정책 순서 정돈

DLP 위반이 발신 메일 정책에서 활성화된 둘 이상의 DLP 정책과 일치하는 경우 리스트에서 첫 번째 일치하는 DLP 정책만 사용됩니다.

단계 **1** DLP Policy Manager(DLP 정책 관리자) 페이지에서 **Edit Policy Order(**정책 순서 수정**)**를 클릭합니다.
단계 **2** 이동할 정책의 행을 클릭하고 순서의 새 위치로 끌어옵니다.

단계 3 정책 순서 변경을 완료했으면 변경 사항을 제출 및 커밋합니다.

DLP 정책을 발신 메일 정책과 연결

관련 주제

- DLP 정책을 기본 발신 메일 정책과 연결 , 511 페이지
- 발신 메일 정책을 사용하여 DLP 정책을 발신자 및 수신자에게 할당 , 511 페이지

DLP 정책을 기본 발신 메일 정책과 연결

발신자 또는 수신자와 일치하는 다른 발신 메일 정책이 없는 경우 기본 발신 메일 정책이 사용됩니다.

시작하기 전에

데이터 유출 방지 설정 방법 , 493 페이지의 표에서 현 시점까지의 모든 활동을 완료합니다. 예를 들어 기본 발신 메일 정책에 포함하려는 DLP 정책을 만들었는지 확인합니다.

단계 1 **Mail Policies**(메일 정책) > **Outgoing Mail Policies**(발신 메일 정책)를 선택합니다.

단계 2 표의 **Default Policy**(기본 정책) 행에서 **DLP** 열에 있는 **Disabled**(비활성) 링크를 클릭합니다.

단계 3 **Enable DLP (Customize Settings)**(DLP 활성화(맞춤화 설정))를 선택합니다.

단계 4 기본 발신 메일 정책에 대해 활성화할 DLP 정책을 선택합니다.

단계 5 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

추가 발신 메일 정책에 대한 DLP 정책을 선택합니다. 발신 메일 정책을 사용하여 DLP 정책을 발신자 및 수신자에게 할당 , 511 페이지를 참조하십시오.

발신 메일 정책을 사용하여 DLP 정책을 발신자 및 수신자에게 할당

발신 메일 정책에서 활성화하여 어떤 DLP 정책을 어떤 발신자 및 수신자에게 적용할지를 지정합니다. DLP 정책은 발신 메일 정책에만 사용할 수 있습니다.

시작하기 전에

기본 발신 메일 정책에 대해 DLP 정책 설정을 구성합니다. DLP 정책을 기본 발신 메일 정책과 연결 , 511 페이지를 참조하십시오.

단계 1 **Mail Policies**(메일 정책) > **Outgoing Mail Policies**(발신 메일 정책)를 선택합니다.

단계 2 표에 있는 임의의 행에서 DLP 열의 링크를 클릭합니다.

단계 3 이 발신 메일 정책과 연결할 DLP 정책을 선택합니다.

단계 **4** 변경 사항을 제출합니다.
단계 **5** 다른 발신 메일 정책에 대해서 필요한 만큼 반복합니다.
단계 **6** 변경 사항을 커밋합니다.

다음에 수행할 작업

데이터 유출 방지 설정 방법 , 493 페이지를 참조하십시오.

DLP 정책 수정 또는 삭제에 대한 중요한 정보

작업	정보
DLP 정책 수정	정책의 이름을 변경하는 경우 발신 메일 정책에서 해당 정책을 다시 활성화해야 합니다.
DLP 정책 삭제	정책을 삭제하면 하나 이상의 발신 메일 정책에서 DLP 정책이 사용되는 경우 알림을 수신하게 됩니다. DLP 정책을 삭제하면 이러한 메일 정책에서 제거됩니다.

메시지 작업

발신 메시지에서 DLP 위반 가능성을 탐지할 때 Email Security Appliance에서 수행할 기본 및 보조 작업을 지정합니다. 위반 유형 및 심각도에 따라 서로 다른 작업을 할당할 수 있습니다.

기본 작업은 다음과 같습니다.

- 전달
- 드롭
- 격리

보조 작업은 다음과 같습니다.

- 메시지를 전달하기로 선택하는 경우 정책 격리에 복사본 전송. 복사본은 메시지 ID를 포함하는 원본의 완벽한 복제본입니다. 복사본을 격리하면 DLP 위반을 모니터링하는 또 다른 방법이 제공되는 것 외에, 구축 전에 DLP 시스템을 테스트할 수 있습니다. 격리에서 복사본을 릴리스하면 어플라이언스는 이미 원본을 받았을 수신자에게 복사본을 전달합니다.
- 메시지 암호화. 어플라이언스는 메시지 본문만 암호화합니다. 메시지 헤더는 암호화하지 않습니다.
- DLP 위반이 포함된 메시지의 제목 헤더 변경.
- 메시지에 면책조항 텍스트 추가.
- 대체 대상 메일호스트에 메시지 전송.
- 메시지 복사본을 다른 수신자에게 전송(bcc). (예를 들면 중대한 DLP 위반이 있는 메시지를 검토를 위해 규정준수 담당자의 사서함으로 복사할 수 있습니다.)
- 발신자 또는 관리자나 DLP 규정준수 담당자 같은 다른 연락처로 DLP 위반 알림 메시지 전송. DLP 알림 초안 , 515 페이지를 참조하십시오.

참고 이러한 작업은 상호 배타적이지 않습니다. 서로 다른 사용자 그룹에 대한 다양한 처리 요구에 따라 각 DLP 정책 내에서 일부를 결합할 수 있습니다. 동일한 정책의 각 심각도 레벨을 기반으로 서로 다른 처리 방식을 구성할 수도 있습니다. 예를 들어 중대한 DLP 위반이 있는 메시지는 격리하고 규정준수 담당자에게 알림을 보낼 수 있지만, 낮은 심각도 레벨의 메시지는 전달할 수 있습니다.

관련 주제

- DLP 위반에 대해 수행할 작업 정의(메시지 작업) , 513 페이지
- 메시지 작업 보기 및 수정 , 514 페이지
- DLP 알림 초안 , 515 페이지

DLP 위반에 대해 수행할 작업 정의(메시지 작업)

시작하기 전에

- DLP 정책을 위반하는 메시지(또는 메시지의 복사본)를 수용할 하나 이상의 전용 격리를 만듭니다.

  Email Security Appliance의 로컬 격리일 수도 있고 Security Management Appliance의 중앙 집중식 격리일 수도 있습니다.

  자세한 내용은 정책, 바이러스, 보안 침해 격리, 847 페이지를 참조해 주십시오.

- 전달 전에 메시지를 암호화하려면 암호화 프로필을 설정했는지 확인해야 합니다. Cisco Email Encryption, 521 페이지을 참고해 주십시오.
- DLP 위반 또는 의심스런 위반이 포함된 메시지를 전달할 때 면책조항 텍스트를 포함하려면 **Mail Policies(메일 정책) > Text Resources(텍스트 리소스)**에서 면책조항 텍스트를 지정합니다. 자세한 내용은 면책조항 템플릿, 625 페이지 섹션을 참조해 주십시오.
- DLP 위반의 발신자 또는 규정준수 담당자 같은 또 다른 사람에게 알림을 전송하려면 먼저 DLP 알림 템플릿을 만듭니다. DLP 알림 초안 , 515 페이지를 참조하십시오.

단계 **1** **Mail Policies(메일 정책) > DLP Policy Customizations(DLP 정책 맞춤화)**를 선택합니다.

단계 **2** **Message Actions(메시지 작업)** 섹션에서 **Add Message Action(메시지 작업 추가)**을 클릭합니다.

단계 **3** 메시지 작업의 이름을 입력합니다.

단계 **4** 메시지 작업의 설명을 입력합니다.

단계 **5** DLP 위반이 포함된 메시지를 삭제할지, 전달할지 또는 격리할지를 선택합니다.

참고 전달을 선택하는 경우 메시지의 복사본을 정책 격리로 전송하도록 선택할 수 있습니다. 메시지 복사본은 메시지 ID를 포함하는 완벽한 복제본입니다.

단계 **6** 격리에서 전달하거나 릴리스할 때 메시지를 암호화하려면 **Enable Encryption(암호화 활성화)** 확인란을 선택하고 다음 옵션을 선택합니다.

- **Encryption Rule(**암호화 규칙**)**. 메시지를 항상 암호화하거나, 먼저 TLS 연결을 통해 전송하려는 시도가 실패한 경우에만 암호화합니다.
- **Encryption Profile(**암호화 프로필**)**. Cisco IronPort Encryption Appliance 또는 호스팅된 키 서비스를 사용하는 경우 지정된 암호화 프로필을 사용하여 메시지를 암호화하고 전달합니다.
- **Encrypted Message Subject(**암호화된 메시지 제목**)**. 암호화된 메시지의 제목. 기존 메시지 제목을 유지하려면 **`$Subject`** 값을 사용합니다.

단계 **7** 작업으로 Quarantine(격리)를 선택하는 경우 DLP 위반이 포함된 메시지에 사용할 정책 격리를 선택합니다.

단계 **8** 다음 옵션 중 하나를 사용하여 메시지를 수정하려면 **Advanced(**고급**)**를 클릭합니다.

- 맞춤화 헤더 추가
- 메시지 제목 수정
- 메시지를 대체 호스트로 전달
- 복사본을 다른 수신자에게 전송(bcc)
- DLP 알림 메시지 전송

단계 **9** 변경 사항을 제출 및 커밋합니다.

메시지 작업 보기 및 수정

단계 **1** **Mail Policies(**메일 정책**) > DLP Policy Customizations(DLP** 정책 맞춤화**)**를 선택합니다.

단계 **2** **Message Actions(**메시지 작업**)** 섹션에서 작업을 선택합니다.

변경 후	수행해야 할 작업
각 작업이 할당된 메일 정책 보기	Actions(메시지 작업) 테이블의 제목에서 **Policies(**정책**)**를 클릭합니다.
각 작업에 대해 입력한 설명 보기	Actions(메시지 작업) 테이블의 제목에서 **Description(**설명**)**을 클릭합니다.
메시지 작업의 세부사항 보기 또는 수정	메시지 작업의 이름을 클릭합니다.
메시지 작업 삭제	삭제할 메시지 작업 옆에 있는 휴지통 아이콘을 클릭합니다. 메시지 작업이 하나 이상의 DLP 정책에서 사용되는 경우 확인 메시지가 표시됩니다.

변경 후	수행해야 할 작업
메시지 작업 복제 이 기능을 사용하면 변경 전에 메시지 작업의 백업 복사본을 만들 수도 있고, 이러한 복사본을 새로운 또는 유사한 메시지 작업을 만들기 위한 시작점으로 사용할 수도 있습니다.	복제할 메시지 작업 옆에 있는 **Duplicate**(복제) 아이콘을 클릭합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

DLP 알림 초안

다음 절차를 사용하면 이메일에 조직의 데이터 유출 방지 정책을 위반하는 정보가 포함되어 있을 때 전송할 알림의 템플릿을 만들 수 있습니다. 이 알림을 DLP 정책을 위반한 메시지 발신자에게 또는 관리자나 DLP 규정준수 담당자 같은 다른 이메일 주소로 전송할 수 있습니다.

시작하기 전에

- DLP 알림 템플릿 변수 정의, 515 페이지의 내용을 숙지해 주십시오. 위반에 대한 특정 세부사항으로 알림을 맞춤화하는 데 이러한 변수를 사용할 수 있습니다.

단계 **1** **Mail Policies**(메일 정책) > **Text Resources**(텍스트 리소스)를 선택합니다.

단계 **2** **Add Text Resource**(텍스트 리소스 추가)를 클릭합니다.

단계 **3** **Type**(유형)에서 **DLP Notification Template**(**DLP** 알림 템플릿)을 선택합니다.

일반 알림 템플릿에는 DLP 변수를 사용할 수 없습니다.

단계 **4** 알림 텍스트와 변수를 입력합니다.

발신 메시지에 조직의 데이터 유출 방지 정책을 위반하는 민감한 데이터가 포함되어 있을 수 있음을 수신자에게 알려야 합니다.

다음에 수행할 작업

DLP 정책 관리자 DLP 정책의 메시지 작업에서 DLP 알림 템플릿을 지정합니다.

관련 주제

- DLP 알림 템플릿 변수 정의, 515 페이지

DLP 알림 템플릿 변수 정의

각 DLP 위반 관련 정보를 알림에 포함하기 위해 다음 변수를 사용합니다.

변수	교체
$DLPPolicy	위반된 이메일 DLP 정책 이름으로 교체됩니다.
$DLPSeverity	위반 심각도로 교체됩니다. "Low," "Medium," "High" 또는 "Critical."
$DLPRiskFactor	메시지 민감 재료의 위험 요인으로 교체됩니다(점수 0~100).
$To	메시지 To: 헤더로 교체됩니다(Envelope Recipient 아님).
$From	메시지 From: 헤더로 교체됩니다(Envelope Sender 아님).
$Subject	원본 메시지의 제목으로 교체됩니다.
$Date	MM/DD/YYYY 형식을 사용하여 현재 날짜로 교체됩니다.
$Time	현지 시간으로 교체됩니다(현지 표준 시간대).
$GMTimestamp	이메일 메시지의 Received: 줄에 나오는 대로 GMT를 사용하여 현재 시간 및 날짜로 교체됩니다.
$MID	메시지 식별을 위해 내부적으로 사용되는 MID(Message ID)로 교체됩니다. RFC822 "Message-Id" 값과 혼동해서는 안 됩니다(검색을 위해 $Header 사용).
$Group	메시지 주입 시 일치된 발송자 그룹의 이름으로 교체됩니다. 그룹에 이름이 없으면 ">Unknown<" 문자열이 삽입됩니다.
$Reputation	발신자의 SenderBase Reputation 점수로 교체됩니다. 평판 점수가 없으면 "None"으로 교체됩니다.
$filenames	메시지 어태치 파일 이름의 쉼표로 구분된 리스트로 교체됩니다.
$filetypes	메시지 어태치 파일 형식의 쉼표로 구분된 리스트로 교체됩니다.
$filesizes	메시지 어태치 파일 크기의 쉼표로 구분된 리스트로 교체됩니다.
$remotehost	메시지를 Cisco 어플라이언스로 전송한 시스템의 호스트 이름으로 교체됩니다.
$AllHeaders	메시지 헤더로 교체됩니다.
$EnvelopeFrom	메시지의 Envelope Sender(봉투 발신자)(Envelope From, <MAIL FROM>)로 교체됩니다.
$Hostname	Cisco 어플라이언스의 호스트 이름으로 교체됩니다.
$bodysize	메시지의 크기로 교체됩니다(바이트 단위).
$header['*string*']	원본 메시지에 일치하는 헤더가 포함된 경우 인용된 헤더의 값으로 교체됩니다. 큰따옴표를 사용할 수도 있습니다.
$remoteip	메시지를 Cisco 어플라이언스로 전송한 시스템의 IP 주소로 교체됩니다.

변수	교체
$recvlistener	메시지를 수신한 리스너의 별칭으로 교체됩니다.
$dropped_filenames	$filenames와 같지만, 삭제된 파일의 리스트를 표시합니다.
$dropped_filename	가장 최근에 삭제된 파일 이름만 반환합니다.
$recvint	메시지를 수신한 인터페이스의 별칭으로 교체됩니다.
$timestamp	이메일 메시지의 Received: 줄에 나타나는 현재 날짜 및 시간으로 교체됩니다(현지 표준 시간대).
$Time	현지 시간으로 교체됩니다(현지 표준 시간대).
$orgid	SenderBase Organization ID(정수 값)로 교체됩니다.
$enveloperecipients	메시지의 모든 Envelope Recipients(봉투 수신자)(Envelope To, <RCPT TO>)로 교체됩니다.
$dropped_filetypes	$filetypes와 같지만, 삭제된 파일의 리스트를 표시합니다.
$dropped_filetype	가장 최근에 삭제된 파일의 파일 형식만 반환합니다.

메시지 추적에서 민감한 DLP 데이터 표시

DLP 구축은 DLP 정책을 위반하는 콘텐츠를 주변 콘텐츠와 함께 로깅할 옵션을 제공합니다. 이를 나중에 메시지 추적에서 볼 수 있습니다. 여기에는 신용카드 번호 및 사회 보장 번호와 같은 민감한 데이터가 포함될 수 있습니다.

시작하기 전에

메시지 추적을 활성화합니다. 메시지 추적 활성화, 837 페이지을 참고해 주십시오.

단계 **1** **Security Services**(보안 서비스) > **Data Loss Prevention**(데이터 유출 방지)을 선택합니다.

단계 **2** **Edit Settings**(설정 편집)를 클릭합니다.

단계 **3** **Enable Matched Content Logging**(일치하는 콘텐츠 로깅 활성화) 확인란을 선택합니다.

단계 **4** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

이 정보를 볼 수 있는 관리 사용자를 지정합니다. 메시지 추적 시 중요 정보의 액세스 제어, 898 페이지를 참조하십시오.

관련 주제

- 메시지 추적 세부 정보 , 842 페이지

DLP 엔진 및 콘텐츠 일치 분류자 업데이트

어플라이언스에서 Cisco DLP 엔진 및 사전 정의된 콘텐츠 일치 분류자에 대한 업데이트는 다른 보안 서비스에 대한 업데이트와는 무관합니다.

관련 주제

- DLP 엔진의 현재 버전 확인 , 518 페이지
- DLP 엔진 및 콘텐츠 일치 분류자를 수동으로 업데이트 , 518 페이지
- 자동 업데이트 활성화(권장하지 않음) , 518 페이지
- 중앙 집중식(클러스터링된) 어플라이언스에서 DLP 업데이트 , 519 페이지

DLP 엔진의 현재 버전 확인

단계 1 **Security Services**(보안 서비스) > **Data Loss Prevention**(데이터 유출 방지)을 선택합니다.

단계 2 **Current DLP Version Files**(현재 **DLP** 버전 파일) 섹션을 살펴봅니다.

참고 `dlpstatus` CLI 명령을 사용하여 DLP 엔진의 현재 버전을 볼 수도 있습니다. 자세한 내용은 *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*를 참조하십시오.

DLP 엔진 및 콘텐츠 일치 분류자를 수동으로 업데이트

시작하기 전에

다음을 참조해 주십시오.

- (해당되는 경우) 중앙 집중식(클러스터링된) 어플라이언스에서 DLP 업데이트 , 519 페이지

단계 1 **Security Services**(보안 서비스) > **Data Loss Prevention**(데이터 유출 방지)을 선택합니다.

단계 2 **Current DLP Version Files**(현재 **DLP** 버전 파일) 섹션에서 **Update Now**(지금 업데이트)를 클릭합니다.

이 버튼은 다운로드 가능한 새 업데이트가 있는 경우에만 사용할 수 있습니다.

참고 `dlpupdate` CLI 명령을 사용하여 DLP 엔진을 업데이트할 수도 있습니다. 자세한 내용은 *CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*를 참조하십시오.

자동 업데이트 활성화(권장하지 않음)

다음 절차를 사용하면 어플라이언스가 일정한 간격으로 업데이트를 확인 및 다운로드하도록 설정할 수 있습니다.

참고 Cisco에서는 자동 업데이트를 활성화하지 않을 것을 권장합니다. 이러한 업데이트는 DLP 정책에 사용되는 콘텐츠 일치 분류자를 변경할 수 있습니다. 대신 실무에 사용되는 어플라이언스를 업데이트하기 전에 DLP 업데이트를 수동으로 다운로드하고 랩 환경에서 테스트해 주십시오.

시작하기 전에

- **Security Settings**(보안 설정) > **Service Updates**(서비스 업데이트) 페이지에서 자동 업데이트를 활성화했는지와 모든 서비스 업데이트에 대해 업데이트 간격을 지정했는지 확인합니다.
- 중앙 집중식(클러스터링된) 어플라이언스에서 DLP 업데이트 , 519 페이지를 참조하십시오.

단계 **1** **Security Services**(보안 서비스) > **Data Loss Prevention**(데이터 유출 방지)을 선택합니다.

단계 **2** **Edit Settings**(설정 편집)를 클릭합니다.

단계 **3** **Enable automatic updates**(자동 업데이트 활성화) 확인란을 선택합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

중앙 집중식(클러스터링된) 어플라이언스에서 DLP 업데이트

다음에 유의해 주십시오.

- 클러스터링된 구축에서는 어플라이언스에 대한 자동 DLP 업데이트를 활성화할 수 없습니다.
- DLP 업데이트는 항상 클러스터, 컴퓨터 또는 그룹 레벨에서 구성된 DLP와 상관없이 컴퓨터 수준에서 수행됩니다.
- 어플라이언스의 DLP 엔진 상태를 확인하려면 시스템 레벨에서 **dlpstatus** CLI 명령을 사용해야만 합니다.

DLP 인시던트 메시지 및 데이터 작업

참고 구축에 해당되는 Security Management Appliance에 대한 설명서도 참고하십시오.

변경 후	수행해야 할 작업
DLP 정책 이름, 위반 심각도 및 수행 작업과 같은 기준을 사용하여 DLP 위반이 포함된 메시지를 검색하고, 발견되는 메시지의 세부사항을 확인합니다.	메시지 추적, 837 페이지의 내용을 참조하십시오.
의심스런 DLP 위반으로 격리된 메시지 보기 또는 관리	정책, 바이러스 또는 보안 침해 격리의 메시지 작업, 858 페이지의 내용을 참조하십시오.

변경 후	수행해야 할 작업
DLP 인시던트 요약 보기	이메일 보안 모니터 사용, 793 페이지에서 DLP 인시던트 요약 보고서에 대한 정보를 참고하십시오.
발신 메일에서 발견되는 DLP 위반에 대한 정보 보기	이메일 보안 모니터 사용, 793 페이지에서 DLP 인시던트 보고서에 대한 정보를 참고하십시오.

관련 주제

- 메시지 추적에서 민감한 DLP 데이터 표시 , 517 페이지
- 메시지 추적 시 중요 정보의 액세스 제어, 898 페이지

Data Loss Prevention 트러블슈팅

- DLP가 이메일 첨부 파일에서 위반을 탐지하지 못함, 520 페이지

DLP가 이메일 첨부 파일에서 위반을 탐지하지 못함

문제

사전 정의된 DLP 정책 사용 시 DLP가 이메일 첨부 파일에서 위반을 탐지하지 못합니다. 원인은 다음과 같을 수 있습니다.

- 사전 정의된 DLP 정책에서 근접성 파라미터의 값이 작습니다.

  참고 사전 정의된 DLP 정책의 근접성은 변경할 수 없습니다.

- 사전 정의된 DLP 정책에 정의된 확장 파라미터의 심각도가 높습니다.

솔루션

- 맞춤화 정책을 만들고 필요에 따라 근접성을 조정합니다. 맞춤화 DLP 정책 만들기(고급) , 498 페이지를 참조하십시오.
- 사전 정의된 DLP 정책의 심각도 지수 파라미터를 낮춥니다. 심각도 스케일 조정 , 510 페이지를 참조하십시오.

21 장

Cisco Email Encryption

이 장에는 다음 섹션이 포함되어 있습니다.

Cisco Email Encryption의 개요

AsyncOS는 인바운드 및 아웃바운드 이메일 보안을 위한 암호화 사용을 지원합니다. 이 기능을 사용하려면 암호화된 메시지의 특성과 키 서버에 대한 연결 정보를 지정하는 암호화 프로필을 만들어야 합니다. 키 서버는 다음 중 하나일 수 있습니다.

- Cisco Registered Envelope Service(관리되는 서비스) 또는
- Cisco Encryption Appliance(로컬에서 관리되는 서버)

그런 다음 콘텐츠 필터, 메시지 필터, 그리고 암호화할 메시지를 결정하는 데이터 유출 방지 정책을 만들어야 합니다.

1. 필터 조건을 충족하는 발신 메시지는 암호화 처리를 위해 Email Security Appliance의 대기열에 추가됩니다.
2. 메시지가 암호화되면, 암호화에 사용된 키가 암호화 프로필에 지정된 키 서버에 저장되고 암호화된 메시지가 전달을 위해 대기열에 추가됩니다.
3. 대기열에 있는 이메일의 암호화를 금지하는 일시적인 조건이 존재하는 경우(즉, 일시적으로 C-Series가 사용 중이거나 CRES를 사용할 수 없음) 메시지가 다시 대기열에 추가되고 나중에 재시도됩니다.

참고 암호화 전에 TLS 연결을 통한 첫 번째 전송을 시도하도록 어플라이언스를 설정할 수도 있습니다. 자세한 내용은 암호화 대안으로 TLS 연결 사용, 529 페이지를 참고하십시오.

로컬 키 서버로 메시지를 암호화하는 방법

표 **40:** 로컬 키 서버로 메시지를 암호화하는 방법

단계	수행해야 할 작업	추가 정보
1단계	네트워크에 Cisco IronPort Encryption Appliance를 설정합니다.	설정 및 설치, 15 페이지 참조.
2단계	메시지 암호화를 활성화합니다.	Email Security Appliance에서 메시지 암호화 활성화, 524 페이지.
3단계	암호화 프로필을 만들어 사용할 암호화 키 서버 및 암호화된 메시지에 대한 보안 설정을 지정합니다.	키 서비스에서 암호화된 메시지를 처리하는 방법 구성, 524 페이지.
4단계	어플라이언스가 메시지를 암호화하기 위해 충족해야 할 조건을 정의합니다.	암호화할 메시지 결정, 528 페이지.
5단계	이메일 워크플로에서 메시지를 암호화할 시기를 결정합니다.	• 콘텐츠 필터를 사용하여 메시지를 암호화하고 즉시 전달, 529 페이지. 또는 • 콘텐츠 필터를 사용하여 전달 시 메시지 암호화, 530 페이지.
6단계	(선택 사항) 추가 보안을 위해 메시지에 플래그를 지정합니다.	암호화 헤더를 메시지에 삽입, 531 페이지.
7단계	메시지를 암호화할 사용자 그룹을 정의합니다.	메일 정책을 만듭니다. 메일 정책, 269 페이지을 참고해 주십시오.
8단계	정의한 암호화 작업을 정의한 사용자 그룹과 연결합니다.	콘텐츠 필터를 메일 정책과 연결합니다. 메일 정책, 269 페이지를 참고하십시오.

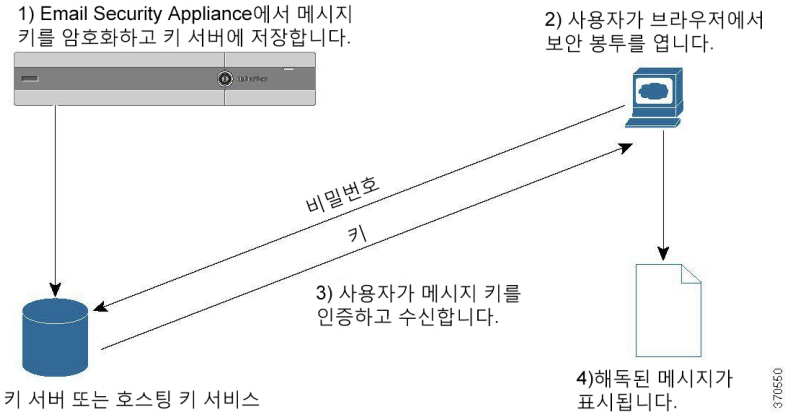
관련 주제

- 암호화 워크플로, 522 페이지

암호화 워크플로

이메일 암호화를 사용하면 Cisco Email Security Appliance는 메시지를 암호화하고 메시지 키를 로컬 키 서버 또는 호스팅된 키 서비스에 저장합니다. 수신자가 암호화된 메시지를 열면 키 서비스에 의해 인증이 수행된 후 해독된 메시지가 표시됩니다.

그림 *34:* 암호화 워크플로



암호화된 메시지 열기의 기본 워크플로는 다음과 같습니다.

1. 암호화 프로필을 구성할 때 메시지 암호화를 위한 매개변수를 지정합니다. 암호화된 메시지에 대해 Email Security Appliance는 메시지 키를 만들고 로컬 키 서버 또는 호스팅된 키 서비스(Cisco Registered Envelope Service)에 저장합니다.
2. 수신자는 브라우저에서 안전한 봉투를 엽니다.
3. 수신자가 브라우저에서 암호화된 메시지를 열면 사용자 ID 인증을 위해 비밀번호가 필요할 수 있습니다. 키 서버는 메시지와 관련된 암호화 키를 반환합니다.

참고 암호화된 이메일 메시지를 처음 여는 경우 수신자는 안전한 봉투를 열기 위해 키 서비스에 등록해야 합니다. 등록한 후에는 암호화 프로필에 구성된 설정에 따라 수신자는 인증 없이 암호화된 메시지를 열 수도 있습니다. 암호화 프로필은 비밀번호가 필요하지 않다고 지정할 수 있지만, 특정 기능은 사용할 수 없습니다.

4. 해독된 메시지가 표시됩니다.

Email Security Appliance를 사용하여 메시지 암호화

Email Security Appliance에서 암호화를 사용하려면 암호화 프로필을 구성해야 합니다. encryptionconfig CLI 명령을 사용하거나 GUI의 Security Services(보안 서비스) > Cisco IronPort Email Encryption을 통해 암호화 프로필을 활성화 및 구성할 수 있습니다.

참고 어플라이언스에서 PXE 및 S/MIME 암호화가 활성화된 경우 AsyncOS는 먼저 S/MIME을 사용하여, 다음에는 PXE를 사용하여 메시지를 암호화합니다.

관련 주제

- Email Security Appliance에서 메시지 암호화 활성화, 524 페이지

• 키 서비스에서 암호화된 메시지를 처리하는 방법 구성, 524 페이지
• 봉투의 기본 로캘 구성, 527 페이지
• PXE 엔진의 최신 버전으로 업데이트, 528 페이지

Email Security Appliance에서 메시지 암호화 활성화

단계 **1** **Security Services(**보안 서비스**) > Cisco IronPort Email Encryption**을 클릭합니다.

단계 **2** **Enable(**활성화**)**을 클릭합니다.

단계 **3** (선택 사항) **Edit Settings(**설정 수정**)**를 클릭하여 다음 옵션을 구성합니다.

- 암호화할 최대 메시지 크기. Cisco의 권장 메시지 크기는 10MB입니다. 어플라이언스가 암호화할 최대 메시지 크기는 25MB입니다.

  참고 권장 10MB 제한보다 큰 메시지를 암호화하면 어플라이언스의 성능이 저하될 수 있습니다. Cisco Registered Envelope Service를 사용 중인 경우, 메시지 수신자는 10MB가 넘는 첨부 파일이 있는 암호화된 메시지에 응답하지 못하게 됩니다.

- 암호화 계정 사용자의 이메일 주소. 암호화 프로필을 프로비저닝할 때 이 이메일 주소가 암호화 서버에 자동으로 등록됩니다.
- 프록시 서버를 구성합니다.

키 서비스에서 암호화된 메시지를 처리하는 방법 구성

키 서비스를 사용하면 하나 이상의 암호화 프로필을 만들 수 있습니다. 각 이메일 그룹에 대해 서로 다른 보안 레벨을 사용하려면 서로 다른 암호화 프로필을 만들 수 있습니다. 예를 들어, 민감한 자료가 포함된 메시지는 높은 보안 레벨로 전송하고, 나머지 메시지는 중간 보안 레벨로 전송할 수 있습니다. 이 경우 특정 키워드(예: 'confidential')가 포함된 메시지와 연결하기 위한 높은 보안 레벨의 암호화 프로필을 만들고, 나머지 발신 메시지를 위한 또 다른 암호화 프로필을 만들 수 있습니다.

암호화 프로필을 맞춤화 사용자 역할에 할당하여, 해당 역할에 할당된 위임 관리자가 DLP 정책 및 콘텐츠 필터와 함께 암호화 프로필을 사용하도록 할 수 있습니다. DLP 정책 및 콘텐츠 필터를 구성할 경우 관리자, 운영자 및 위임 사용자만 암호화 프로필을 사용할 수 있습니다. 맞춤화 역할에 할당되지 않은 암호화 프로필은 메일 또는 DLP 정책 권한이 있는 모든 위임 관리자가 사용할 수 있습니다. 자세한 내용은 관리 작업 배포, 893 페이지를 참조해 주십시오.

참고 하나의 호스팅된 키 서비스에 대해 여러 암호화 프로필을 구성할 수 있습니다. 이 기능을 사용하면 조직에 여러 브랜드가 있는 경우 PXE 봉투에 대한 키 서버에 저장된 서로 다른 로고를 참조할 수 있습니다.

암호화 프로필은 다음과 같은 설정을 저장합니다.

- 키 서버 설정. 키 서버 및 해당 키 서버에 연결하기 위한 정보를 지정합니다.
- 봉투 설정. 보안 레벨, 수신 확인 반환 여부, 시간 제한 전에 메시지가 암호화를 위해 대기열에서 기다리는 시간, 사용할 암호화 알고리즘 유형, 브라우저에서 실행할 해독 애플릿 활성화 여부 등 메시지 봉투에 대한 세부사항을 지정합니다.
- 메시지 설정. 보안 메시지 전달 및 보안 Reply All(전체 회신) 활성화 여부 등 메시지에 대한 세부사항을 지정합니다.
- 알림 설정. 암호화 실패 알림은 물론, 텍스트 및 HTML 알림에 사용할 알림 템플릿을 지정합니다. 텍스트 리소스로 템플릿을 만들고, 암호화 프로필을 만들 때 템플릿을 선택합니다. 또한 봉투를 현지화하고 암호화 실패 알림에 대한 메시지 제목을 지정할 수 있습니다. 알림에 대한 자세한 내용은 암호화 알림 템플릿, 636 페이지 및 바운스 및 암호화 실패 알림 템플릿, 634 페이지 섹션을 참조해 주십시오.

단계 **1** Email Encryption Profiles(이메일 암호화 프로필) 섹션에서 **Add Encryption Profile(**암호화 프로필 추가**)**을 클릭합니다.

단계 **2** 암호화 프로필의 이름을 입력합니다.

단계 **3** **Used By (Roles)(**사용자**(**역할**))** 링크를 클릭하고, 암호화 프로필에 대한 액세스를 허용할 맞춤화 사용자 역할을 선택한 후 **OK(**확인**)**를 클릭합니다.

이 맞춤화 역할에 할당된 위임 관리자는 자신이 책임지는 DLP 정책 및 콘텐츠 필터에 대한 암호화 프로필을 사용할 수 있습니다.

단계 **4** Key Server Settings(키 서버 설정) 섹션에서 다음 키 서버 중 선택합니다.

- Cisco Encryption Appliance(네트워크)
- Cisco Registered Envelope Service(호스팅된 키 서비스)

단계 **5** Encryption Appliance(로컬 키 서비스)를 선택하는 경우 다음 설정을 입력합니다.

- **Internal URL(**내부 **URL).** 이 URL은 Cisco Email Security Appliance가 네트워크 내 Cisco Encryption Appliance에 연결하는 데 사용됩니다.
- **External URL(**외부 **URL)**. 이 URL은 수신자의 메시지가 Cisco Encryption Appliance에서 키 및 기타 서비스에 액세스하는 데 사용됩니다. 수신자는 이 URL을 사용하여 인바운드 HTTP 또는 HTTPS 요청을 수행합니다.

단계 **6** Cisco Registered Envelope Service를 선택하는 경우 호스팅된 키 서비스의 URL을 입력합니다. 키 서비스 URL은 https://res.cisco.com입니다.

단계 **7** Key Server Settings(키 서버 설정) 아래의 **Advanced(**고급**)**를 클릭하여, 수신자가 봉투를 열 때 봉투의 암호화된 페이로드를 전송하는 데 HTTP를 사용할지 HTTPS를 사용할지를 지정합니다. 다음 중 하나를 선택합니다.

- **Use the Key Service with HTTP(HTTP**와 함께 키 서비스 사용**)**. 수신자가 봉투를 열 때 HTTP를 사용하여 키 서비스에서 암호화된 페이로드를 전송합니다. Cisco Registered Envelope Service를 사용하는 경우 이는 6단계에서 지정한 URL입니다. Cisco Encryption Appliance를 사용하는 경우 이는 5단계에서 지정한 외부 URL입니다.
- 페이로드는 이미 암호화되었으므로 HTTP를 통해 전송해도 안전하며 HTTPS를 통해 전송하는 것보다 더 빠릅니다. HTTPS를 통해 이미지 요청을 전송하는 것보다 성능이 더 뛰어납니다.

- **Use the Key Service with HTTPS(HTTPS**와 함께 키 서비스 사용**)**. 수신자가 봉투를 열 때 HTTPS를 사용하여 키 서비스에서 암호화된 페이로드를 전송합니다. Cisco Registered Envelope Service를 사용하는 경우 이는 6단계에서 지정한 URL입니다. Cisco Encryption Appliance를 사용하는 경우 이는 5단계에서 지정한 외부 URL입니다.
- **Specify a separate URL for payload transport(**페이로드 전송을 위한 별도의 **URL** 지정**)**. 암호화된 페이로드에 대해 키 서버를 사용하지 않으려는 경우 또 다른 URL을 사용할 수 있으며, 페이로드 전송에 HTTP와 HTTPS 중 어떤 것을 사용할지 지정할 수 있습니다.

단계 **8** Envelope Settings(봉투 설정) 섹션에서 메시지 보안의 레벨을 선택합니다.

- **High Security(**높은 보안**)**. 수신자가 암호화된 메시지를 열기 위해 항상 암호를 입력해야 합니다.
- **Medium Security(**중간 보안**)**. 수신자 Credential이 캐시된 경우 수신자는 암호화된 메시지를 열기 위해 Credential을 입력할 필요가 없습니다.
- 필요한 암호가 없습니다. 이것은 암호화된 메시지 보안의 최저 레벨입니다. 수신자는 암호화된 메시지를 열기 위해 암호를 입력할 필요가 없습니다. 암호로 보호되지 않은 봉투에 대해 여전히 수신 확인, 보안 전체 회신 및 보안 메시지 전달 기능을 활성화할 수 있습니다.

단계 **9** 사용자가 로고를 클릭하여 조직의 URL을 열도록 하려면 로그에 대한 링크를 추가할 수 있습니다. 다음 옵션 중에서 선택합니다.

- **No link(**링크 없음**).** 메시지 봉투에 라이브 링크가 추가되지 않습니다.
- **Custom link URL(**맞춤화 링크 **URL)**. 메시지 봉투에 라이브 링크를 추가할 URL을 입력합니다.

단계 **10** (선택 사항) 수신 확인을 활성화합니다. 이 옵션을 활성화하면 수신자가 보안 봉투를 열 때 발신자는 확인 메시지(receipt)를 받습니다.

단계 **11** (선택 사항) 다음 설정을 구성하려면 Edit Settings(설정 수정) 아래에서 **Advanced(**고급**)**를 클릭합니다.

- 시간 초과되기 전까지 메시지가 암호화 대기열에 머물 수 있는 시간(초)을 입력합니다. 메시지가 시간 초과되면 어플라이언스는 메시지를 반송하고 발신자에게 알림을 전송합니다.
- 암호화 알고리즘을 선택합니다.
  - **ARC4**. ARC4는 일반적으로 선택하는 옵션으로, 메시지 수신자에 대한 해독 지연 최소화와 함께 강력한 암호화를 제공합니다.
  - **AES**. AES는 좀 더 강력한 암호화 방법이지만, 해독에 시간이 좀 더 걸려서 수신자에게 지연이 발생합니다. AES는 일반적으로 정부 및 은행 애플리케이션에 사용됩니다.
- 해독 애플릿을 활성화 또는 비활성화합니다. 이 옵션을 활성화하면 메시지 첨부 파일이 브라우저 환경에서 열립니다. 이 옵션을 비활성화하면 메시지 첨부 파일이 키 서버에서 해독됩니다. 이 옵션을 비활성화하면 메시지를 여는 데 시간이 좀 더 걸릴 수 있지만 메시지가 브라우저 환경에 의존하지 않습니다.

단계 **12** Message Settings(메시지 설정) 섹션에서 다음을 수행합니다.

- 보안 전체 회신 기능을 활성화하려면 **Enable Secure Reply All(**보안 전체 회신 활성화**)** 확인란을 선택합니다.

- 보안 메시지 전달 기능을 활성화하려면 **Enable Secure Message Forwarding(**보안 메시지 전달 활성화**)** 확인란을 선택합니다.

단계 **13** (선택 사항) Cisco Registered Envelope Service를 선택했으며 이 서비스가 봉투 현지화를 지원하는 경우 봉투 현지화를 활성화합니다. Notification Settings(알림 설정) 섹션에서 **Use Localized Envelope(**현지화된 봉투 사용**)** 확인란을 선택합니다.

참고 봉투 현지화를 활성화하는 경우 암호화된 메시지 HTML 또는 메시지 알림을 선택할 수 없습니다.

봉투의 기본 로캘을 설정하려면 봉투의 기본 로캘 구성, 527 페이지 섹션을 참조해 주십시오.

단계 **14** HTML 및 텍스트 알림 템플릿을 선택합니다.

참고 키 서버는 수신자의 이메일 애플리케이션을 기반으로 HTML 또는 텍스트 알림을 사용합니다. 둘 모두에 대한 알림을 구성해야 합니다.

다음을 수행합니다.

a) HTML 알림 템플릿을 선택합니다. 텍스트 리소스에서 구성한 HTML 알림 중에서 선택합니다. 템플릿을 구성하지 않은 경우 시스템은 기본 템플릿을 사용합니다.

b) 텍스트 알림 템플릿을 선택합니다. 텍스트 리소스에서 구성한 텍스트 알림 중에서 선택합니다. 템플릿을 구성하지 않은 경우 시스템은 기본 템플릿을 사용합니다.

참고 현지화된 봉투를 사용하는 경우 이러한 옵션을 사용할 수 없습니다.

단계 **15** 암호화 실패 알림을 위한 제목 헤더를 입력합니다. 암호화 프로세스가 시간 초과되면 어플라이언스가 알림을 전송합니다.

단계 **16** 메시지 본문에 대한 암호화 실패 알림 템플릿을 선택합니다. 텍스트 리소스에서 구성한 암호화 실패 알림 템플릿 중에 선택합니다. 템플릿을 구성하지 않은 경우 시스템은 기본 템플릿을 사용합니다.

단계 **17** 변경 사항을 제출 및 커밋합니다.

단계 **18** Cisco Registered Envelope Service를 사용하는 경우 어플라이언스 프로비저닝의 추가 단계를 수행해야 합니다. 어플라이언스 프로비저닝은 호스팅된 키 서비스로 암호화 프로필을 등록합니다. 어플라이언스를 프로비저닝하려면 등록할 암호화 프로필에 대한 **Provision(**프로비전**)** 버튼을 클릭합니다.

봉투의 기본 로캘 구성

봉투의 기본 로캘은 영어입니다. Cisco Registered Envelope Service를 선택했으며 이 서비스가 봉투 현지화를 지원하는 경우 봉투의 로캘을 다음 중 하나로 변경할 수 있습니다.

- 영어
- 프랑스어
- 독일어
- 일본어
- 포르투갈어
- 스페인어

시작하기 전에

- Key Service Type(키 서비스 유형) 및 봉투 현지화가 활성화되면 Cisco Registered Envelope Service로 암호화 프로필을 만듭니다. 키 서비스에서 암호화된 메시지를 처리하는 방법 구성, 524 페이지를 참조하십시오.
- Cisco Registered Envelope Service가 봉투 현지화를 지원하는지 확인해 주십시오.

단계 **1** **Security Services(**보안 서비스**)** > **Cisco IronPort Email Encryption**을 클릭합니다.

단계 **2** 기존 암호화 프로필을 엽니다.

단계 **3** **Notification Settings(**알림 설정**)** 섹션의 **Localized Envelopes(**현지화된 봉투**)** 드롭다운 리스트에서 로캘을 선택합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

단계 **5** **Commit Changes(**변경 커밋**)**를 클릭합니다.

PXE 엔진의 최신 버전으로 업데이트

Cisco Email Encryption Settings(Cisco Email Encryption 설정) 페이지에는 어플라이언스에서 사용하는 PXE 엔진 및 Domain Mappings 파일의 현재 버전이 표시됩니다. Email Security Appliance가 PXE 엔진을 자동으로 업데이트하도록 구성하려면 **Security Services > Service Updates(**서비스 업데이트**)** 페이지(또는 CLI의 updateconfig 명령)를 사용할 수 있습니다. 자세한 내용은 서비스 업데이트, 945 페이지를 참고해 주십시오.

IronPort Email Encryption Settings(IronPort Email Encryption 설정) 페이지(또는 CLI의 **`encryptionupdate`** 명령)의 PXE Engine Updates(PXE 엔진 업데이트) 섹션에 있는 **Update Now(**지금 업데이트**)** 버튼을 사용하여 엔진을 수동으로 업데이트할 수도 있습니다.

암호화할 메시지 결정

암호화 프로필을 만든 후에는 어떤 이메일 메시지를 암호화할지를 결정하는 발신 콘텐츠 필터를 만들어야 합니다. 콘텐츠 필터는 발신 이메일을 검사하고, 메시지가 지정된 조건과 일치하는지를 결정합니다. 메시지가 조건과 일치한다고 콘텐츠 필터에서 결정하면 Cisco Email Security Appliance는 메시지를 암호화하고 생성된 키를 키 서버로 전송합니다. 어플라이언스는 암호화 프로필에 지정된 설정을 사용하여 사용할 키 서버 및 기타 암호화 설정을 결정합니다.

데이터 유출 방지 검사 후 릴리스된 메시지를 암호화할 수도 있습니다. 자세한 내용은 DLP 위반에 대해 수행할 작업 정의(메시지 작업), 513 페이지를 참고하십시오.

관련 주제

- 암호화 대안으로 TLS 연결 사용, 529 페이지
- 콘텐츠 필터를 사용하여 메시지를 암호화하고 즉시 전달, 529 페이지
- 콘텐츠 필터를 사용하여 전달 시 메시지 암호화, 530 페이지

암호화 대안으로 TLS 연결 사용

TLS 연결이 사용 가능한 경우, Email Security Appliance는 도메인에 대해 지정된 대상 제어를 기반으로 암호화 대신 TLS 연결을 통해 메시지를 안전하게 릴레이할 수 있습니다. 어플라이언스는 메시지를 암호화할지 아니면 대상 제어의 TLS 설정(Required(필수), Preferred(기본 설정) 또는 None(없음)) 및 암호화 콘텐츠 필터에 정의된 작업을 기반으로 TLS 연결을 통해 메시지를 전송할지를 결정합니다.

콘텐츠 필터를 만들 때 메시지를 항상 암호화할지 아니면 먼저 TLS 연결을 통해 전송하도록 시도한 다음 TLS 연결을 사용할 수 없을 때 메시지를 암호화할지를 지정할 수 있습니다. 다음 표에서는 암호화 제어 필터가 먼저 TLS 연결을 통해 메시지를 전송하려고 시도할 경우 Email Security Appliance가 도메인의 대상 제어를 위해 TLS 설정을 기반으로 메시지를 전송하는 방법을 보여줍니다.

표 ***41: ESA*** 어플라이언스에서 ***TLS*** 지원

대상 제어 **TLS** 설정	**TLS** 연결을 사용할 수 있는 경우의 작업	**TLS** 연결을 사용할 수 없는 경우의 작업
None	봉투 암호화 및 전송	봉투 암호화 및 전송
TLS Preferred(TLS 기본 설정)	TLS를 통해 전송	봉투 암호화 및 전송
TLS Required(TLS 필수)	TLS를 통해 전송	메시지 재시도/반송

대상 제어에서 TLS를 활성화하는 방법에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지을 참조해 주십시오.

콘텐츠 필터를 사용하여 메시지를 암호화하고 즉시 전달

시작하기 전에

- 콘텐츠 필터를 위한 조건을 만드는 개념을 이해하려면 콘텐츠 필터 개요 , 283 페이지 섹션을 참조하십시오.
- (선택 사항) 암호화 헤더를 메시지에 삽입, 531 페이지 섹션을 참조하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Outgoing Content Filters(**발신 콘텐츠 필터**)**로 이동합니다.

단계 **2** 필터 섹션에서 **Add Filter(**필터 추가**)**를 클릭합니다.

단계 **3** Conditions(조건) 섹션에서 **Add Condition(**조건 추가**)**을 클릭합니다.

단계 **4** 암호화할 메시지를 필터링하기 위한 조건을 추가합니다. 예를 들어 민감한 자료를 암호화하기 위해 특정 단어나 문구(예: "Confidential")가 포함된 메시지를 식별하는 조건을 추가할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** 선택적으로, 추가 암호화 설정을 지정하기 위해 메시지에 암호화 헤더를 삽입하려면 **Add Action(**작업 추가**)** 및 **Add Header(**헤더 추가**)**를 클릭합니다.

단계 **7** Actions(작업) 섹션에서 **Add Action(**작업 추가**)**을 클릭합니다.

단계 **8** **Add Action**(작업 추가) 리스트에서 **Encrypt and Deliver Now (Final Action)**(지금 암호화 및 전달(최종 작업))를 선택합니다.

단계 **9** 조건을 충족하는 메시지를 항상 암호화할지, 아니면 TLS 연결을 통해 전송하려는 시도가 실패할 경우에만 메시지를 암호화할지를 선택합니다.

단계 **10** 콘텐츠 필터와 관련된 암호화 프로필을 선택합니다.

암호화 프로필은 사용할 키 서버, 보안 레벨, 메시지 봉투의 서식에 대한 설정 및 기타 메시지 설정을 지정합니다. 암호화 프로필을 콘텐츠 필터와 연결하면 콘텐츠 필터는 이러한 저장된 설정을 사용하여 메시지를 암호화합니다.

단계 **11** 메시지의 제목을 입력합니다.

단계 **12** **OK**(확인)를 클릭합니다.

다음 그림의 콘텐츠 필터는 메시지 본문에서 ABA 콘텐츠를 검색하는 콘텐츠 필터를 보여줍니다. 콘텐츠 필터에 대해 정의된 작업은 이메일을 암호화하여 전달하도록 지정합니다.

그림 ***35:*** 암호화 콘텐츠 필터

단계 **13** 암호화 작업을 추가한 후 **Submit**(제출)을 클릭합니다.

단계 **14** 변경 사항을 커밋합니다.

다음에 수행할 작업

콘텐츠 필터를 추가한 후 발신 메일 정책에 필터를 추가해야 합니다. 조직의 요구에 따라, 기본 정책에서 콘텐츠 필터를 활성화하거나 특정 메일 정책에 필터를 적용하고자 할 수 있습니다. 메일 정책 작업에 대한 자세한 내용은 메일 정책 개요, 269 페이지 섹션을 참조해 주십시오.

콘텐츠 필터를 사용하여 전달 시 메시지 암호화

전달 시 메시지를 암호화하기 위한 콘텐츠 필터를 만듭니다. 즉, 메시지가 다음 처리 단계로 진행되며 모든 처리가 완료되면 메시지가 암호화되어 전달됩니다.

시작하기 전에

- 콘텐츠 필터를 위한 조건을 만드는 개념을 이해하려면 콘텐츠 필터 개요 , 283 페이지 섹션을 참조하십시오.
- (선택 사항) 암호화 헤더를 메시지에 삽입, 531 페이지 섹션을 참조하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Outgoing Content Filters(**발신 콘텐츠 필터**)**로 이동합니다.

단계 **2** 필터 섹션에서 **Add Filter(**필터 추가**)**를 클릭합니다.

단계 **3** Conditions(조건) 섹션에서 **Add Condition(**조건 추가**)**을 클릭합니다.

단계 **4** 암호화할 메시지를 필터링하기 위한 조건을 추가합니다. 예를 들어 민감한 자료를 암호화하기 위해 특정 단어나 문구(예: "Confidential")가 포함된 메시지를 식별하는 조건을 추가할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** 선택적으로, 추가 암호화 설정을 지정하기 위해 메시지에 암호화 헤더를 삽입하려면 **Add Action(**작업 추가**)** 및 **Add Header(**헤더 추가**)**를 클릭합니다.

단계 **7** Actions(작업) 섹션에서 **Add Action(**작업 추가**)**을 클릭합니다.

단계 **8** **Add Action(**작업 추가**)** 리스트에서 **Encrypt on Delivery(**전달 시 암호화**)**를 선택합니다.

단계 **9** 조건을 충족하는 메시지를 항상 암호화할지, 아니면 TLS 연결을 통해 전송하려는 시도가 실패할 경우에만 메시지를 암호화할지를 선택합니다.

단계 **10** 콘텐츠 필터와 관련된 암호화 프로필을 선택합니다.

암호화 프로필은 사용할 키 서버, 보안 레벨, 메시지 봉투의 서식에 대한 설정 및 기타 메시지 설정을 지정합니다. 암호화 프로필을 콘텐츠 필터와 연결하면 콘텐츠 필터는 이러한 저장된 설정을 사용하여 메시지를 암호화합니다.

단계 **11** 메시지의 제목을 입력합니다.

단계 **12** **OK(**확인**)**를 클릭합니다.

단계 **13** 암호화 작업을 추가한 후 **Submit(**제출**)**을 클릭합니다.

단계 **14** 변경 사항을 커밋합니다.

다음에 수행할 작업

콘텐츠 필터를 추가한 후 발신 메일 정책에 필터를 추가해야 합니다. 조직의 요구에 따라, 기본 정책에서 콘텐츠 필터를 활성화하거나 특정 메일 정책에 필터를 적용하고자 할 수 있습니다. 메일 정책 작업에 대한 자세한 내용은 메일 정책 개요, 269 페이지 섹션을 참조해 주십시오.

암호화 헤더를 메시지에 삽입

AsyncOS에서는 콘텐츠 필터 또는 메시지 필터를 사용하여 메시지에 SMTP 헤더를 삽입함으로써 메시지에 암호화 설정을 추가할 수 있습니다. 암호화 헤더는 관련 암호화 프로필에 정의된 암호화 설정을 재정의할 수 있으며, 지정된 암호화 기능을 메시지에 적용할 수 있습니다.

참고 플래그 지정된 메시지를 처리하도록 Cisco Ironport Encryption Appliance를 설정해야 합니다.

단계 **1** **Mail Policies(**메일 정책**) > Outgoing Content Filters(**발신 콘텐츠 필터**)** 또는 **Incoming Content Filters(**수신 콘텐츠 필터**)**로 이동합니다.

단계 **2** Filters(필터) 섹션에서 **Add Filter(**필터 추가**)**를 클릭합니다.

단계 **3** 추가 암호화 설정을 지정하기 위해 메시지에 암호화 헤더를 삽입하려면 Actions(작업) 섹션에서 **Add Action(**작업 추가**)** 및 **Add Header(**헤더 추가**)**를 클릭합니다.

예를 들어 Registered Envelope(등록된 봉투)을 전송 후 24시간이 지나 만료되도록 하려면 헤더 이름으로 X-PostX-ExpirationDate, 헤더 값으로 +24:00:00을 입력합니다.

다음에 수행할 작업

관련 주제

- 암호화 헤더, 532 페이지
- 암호화 헤더 예, 534 페이지
- 암호화 콘텐츠 필터 만들기에 대한 자세한 내용은 콘텐츠 필터를 사용하여 메시지를 암호화하고 즉시 전달, 529 페이지 섹션을 참조해 주십시오.
- 메시지 필터를 사용하여 헤더를 삽입하는 방법에 대한 자세한 내용은 메시지 필터를 사용하여 이메일 정책 적용, 137 페이지을 참조해 주십시오.

암호화 헤더

다음 표에는 메시지에 추가할 수 있는 암호화 헤더가 나와 있습니다.

표 ***42:*** 이메일 암호화 헤더

MIME 헤더	설명	값
`X-PostX-Reply- Enabled`	메시지의 보안 회신 활성화 여부를 나타내며 메시지 표시줄에 Reply(회신) 버튼을 표시합니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.	Reply(회신) 버튼 표시 여부에 대한 부울. 버튼을 표시하려면 true로 설정합니다. 기본값은 false입니다.
`X-PostX-Reply-All-Enabled`	메시지의 보안 "전체 회신" 활성화 여부를 나타내며 메시지 표시줄에 Reply(회신) 버튼을 표시합니다. 이 헤더는 기본 프로필 설정을 재정의합니다.	Reply All(전체 회신) 버튼 표시 여부에 대한 부울. 버튼을 표시하려면 true로 설정합니다. 기본값은 false입니다.
`X-PostX-Forward-Enabled`	메시지의 보안 전달 활성화 여부를 나타내며 메시지 표시줄에 Forward(전달) 버튼을 표시합니다. 이 헤더는 기본 프로필 설정을 재정의합니다.	Forward(전달) 버튼 표시 여부에 대한 부울. 버튼을 표시하려면 true로 설정합니다. 기본값은 false입니다.

MIME 헤더	설명	값
`X-PostX-Send-Return-Receipt`	수신 확인 활성화 여부를 나타냅니다. 수신자가 보안 봉투를 열 때 발신자는 확인 메시지(receipt)를 받습니다. 이 헤더는 기본 프로필 설정을 재정의합니다.	수신 확인 전송 여부에 대한 부울. 버튼을 표시하려면 true로 설정합니다. 기본값은 false입니다.
`X-PostX-Expiration Date`	전송 전 Registered Envelope(등록된 봉투)의 만료 날짜를 정의합니다. 키 서버는 만료 날짜가 지난 후 등록된 봉투에 대한 액세스를 제한합니다. 등록된 봉투에는 메시지가 만료되었음을 나타내는 메시지가 표시됩니다. 이 헤더는 메시지에 암호화 설정을 추가합니다. Cisco Registered Envelope Service를 사용하는 경우 웹사이트(http://res.cisco.com)에 로그인하고, 메시지 관리 기능을 사용하여 메시지 전송 후 메시지의 만료일을 설정, 조정 또는 제거할 수 있습니다.	관련 날짜 또는 시간을 포함하는 문자열 값. 상대적인 시간, 분, 초에 +HH:MM:SS 형식을 사용하고 상대적인 날에 대해 +D 형식을 사용합니다. 기본적으로 만료일이 없습니다.
`X-PostX-ReadNotification Date`	전송 전 Registered Envelope(등록된 봉투)의 "읽음" 날짜를 정의합니다. 등록된 봉투를 이 날짜까지 읽지 않은 경우 로컬 키 서버는 알림을 생성합니다. 이 헤더의 등록된 봉투는 Cisco Registered Envelope Service와 작동하지 않으며 로컬 키 서버와만 작동합니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.	관련 날짜 또는 시간을 포함하는 문자열 값. 상대적인 시간, 분, 초에 +HH:MM:SS 형식을 사용하고 상대적인 날에 대해 +D 형식을 사용합니다. 기본적으로 만료일이 없습니다.
`X-PostX-Suppress-Applet-For-Open`	해독 애플릿의 비활성화 여부를 나타냅니다. 해독 애플릿을 활성화하면 첨부 파일을 브라우저 환경에서 열 수 있습니다. 이 애플릿을 비활성화하면 메시지 첨부 파일이 키 서버에서 해독됩니다. 이 옵션을 비활성화하면 메시지를 여는 데 시간이 좀 더 걸릴 수 있지만 메시지가 브라우저 환경에 의존하지 않습니다. 이 헤더는 기본 프로필 설정을 재정의합니다.	해독 애플릿의 비활성화 여부에 대한 부울. 애플릿을 비활성화하려면 true로 설정합니다. 기본값은 false입니다.

MIME 헤더	설명	값
X-PostX-Use-Script	JavaScript 없는 봉투의 전송 여부를 나타냅니다. JavaScript 없는 봉투란 수신자 컴퓨터에서 로컬로 봉투를 여는 데 사용되는 JavaScript가 포함되지 않은 Registered Envelope(등록된 봉투)입니다. 수신자는 메시지를 보기 위해 Open Online(온라인 열기) 방법 또는 Open by Forwarding(전달하여 열기) 방법을 사용해야 합니다. 수신자 도메인의 게이트웨이가 JavaScript를 제거하고 암호화된 메시지를 열 수 없도록 하는 경우 이 헤더를 사용합니다. 이 헤더는 암호화 설정을 메시지에 추가합니다.	JavaScript 애플릿의 포함 여부를 나타내는 부울. JavaScript 없는 봉투를 전송하려면 false로 설정합니다. 기본값은 true입니다.
X-PostX-Remember-Envelope-Key-Checkbox	봉투를 오프라인으로 열기 위한 봉투 전용 키 캐싱의 허용 여부를 나타냅니다. 봉투 키 캐싱을 사용하면 수신자가 올바른 암호를 입력하고 "Remember the password for this envelope(이 봉투에 대한 비밀번호 기억)" 확인란을 선택하는 경우 특정 봉투에 대한 암호화 키가 수신자의 컴퓨터에 캐시됩니다. 그 후에 수신자는 컴퓨터에서 봉투를 다시 열기 위해 암호를 다시 입력할 필요가 없습니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.	봉투 키 캐싱 활성화 여부에 대한 부울. "Remember the password for this envelope(이 봉투에 대한 비밀번호 기억)" 확인란을 표시합니다. 기본값은 false입니다.

암호화 헤더 예

이 섹션에서는 암호화 헤더의 예를 제공합니다.

관련 주제

- JavaScript 없는 봉투 활성화, 535 페이지
- 오프라인 열기를 위해 암호화 키 캐싱 활성화, 534 페이지
- 메시지 만료 활성화, 535 페이지
- 해독 애플릿 비활성화, 535 페이지

오프라인 열기를 위해 암호화 키 캐싱 활성화

암호화 키 캐싱을 활성화하여 등록된 봉투를 전송하려면 메시지에 다음 헤더를 삽입합니다.

```
X-PostX-Remember-Envelope-Key-Checkbox: true
```

"Remember the password for this envelope(이 봉투에 대한 비밀번호 기억)" 확인란이 등록된 봉투에 표시됩니다.

JavaScript 없는 봉투 활성화

JavaScript 없는 등록된 봉투를 전송하려면 메시지에 다음 헤더를 삽입합니다.

```
X-PostX-Use-Script: false
```

수신자가 securedoc.html 첨부 파일을 열면 Open Online(온라인 열기) 링크에 등록된 봉투가 표시되고 Open(열기) 버튼이 표시됩니다.

메시지 만료 활성화

전송 후 24시간이 지나 만료되도록 메시지를 구성하려면 메시지에 다음 헤더를 삽입합니다.

```
X-PostX-ExpirationDate: +24:00:00
```

수신자는 전송 후 24시간 동안 암호화된 메시지를 열고 내용을 볼 수 있습니다. 그 후에는 등록된 봉투에 봉투가 만료되었음을 나타내는 메시지가 표시됩니다.

해독 애플릿 비활성화

해독 애플릿을 비활성화하고 메시지 첨부 파일이 키 서버에서 해독되도록 하려면 메시지에 다음 헤더를 삽입합니다.

```
X-PostX-Suppress-Applet-For-Open: true
```

참고 해독 애플릿을 비활성화하면 메시지를 여는 데 시간이 더 걸릴 수 있지만 메시지가 브라우저 환경에 의존하지 않습니다.

22 장

S/MIME 보안 서비스

이 장에는 다음 섹션이 포함되어 있습니다.

S/MIME 보안 서비스 개요

S/MIME(Secure/Multipurpose Internet Mail Extensions)은 확인된 안전한 이메일 메시지를 주고받기 위한 표준 기반의 방법입니다. S/MIME은 공개/개인 키 쌍을 사용하여 메시지를 암호화하거나 서명합니다. 따라서

- 메시지가 암호화된 경우 메시지 수신자만 암호화된 메시지를 열 수 있습니다.
- 메시지가 서명된 경우 메시지 수신자는 발신자의 도메인 ID를 검증하고 메시지가 전송 중에 변경되지 않았음을 확인할 수 있습니다.

S/MIME에 대한 자세한 내용은 다음 RFC를 참조해 주십시오.

- RFC 5750: S/MIME(Secure/Multipurpose Internet Mail Extensions) 버전 3.2 - 인증서 처리
- RFC 5751: MIME(Secure/Multipurpose Internet Mail Extensions) 버전 3.2 - 메시지 사양
- RFC 3369: 암호화 메시지 구문

Email Security Appliance의 S/MIME 보안 서비스

모든 최종 사용자가 자체 인증서를 소유하지 않고도 S/MIME을 사용하여 안전하게 통신할 수 있도록 하려는 조직이 있을 수 있습니다. 그러한 조직을 위해 Email Security Aappliance는 개별 사용자가 아니라 조직을 식별하는 인증서를 사용하여 게이트웨이 레벨에서 S/MIME 보안 서비스(서명, 암호화, 확인 및 해독)를 지원합니다.

Email Security Aappliance는 B2B(Business-to-Business) 및 B2C(Business-to-Consumer) 시나리오에서 다음과 같은 S/MIME 보안 서비스를 제공합니다.

- S/MIME을 사용하여 메시지 서명, 암호화 또는 서명 및 암호화 S/MIME을 사용하여 발신 메시지 서명, 암호화 또는 서명 및 암호화, 540 페이지를 참조하십시오.
- S/MIME을 사용하여 메시지 확인, 해독 또는 해독 및 확인 S/MIME을 사용하여 수신 메시지 확인, 해독 또는 해독 및 확인, 551 페이지를 참조하십시오.

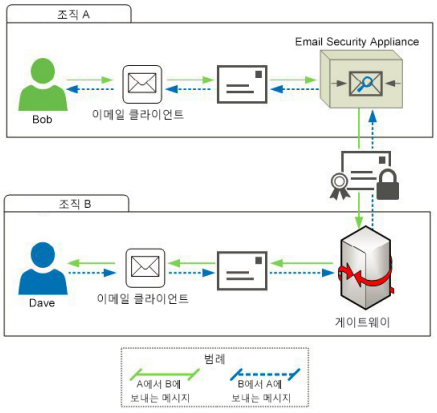
관련 주제

- S/MIME 보안 서비스 작동 방식 이해, 538 페이지

S/MIME 보안 서비스 작동 방식 이해

- 시나리오: Business-to-Business, 538 페이지
- 시나리오: Business-to-Consumer, 539 페이지

시나리오: Business-to-Business



조직 A와 B는 S/MIME을 사용하여 모든 메시지를 서명 및 암호화하여 통신할 수 있기를 원합니다. 조직 A는 게이트웨이 레벨에서 S/MIME 보안 서비스를 수행하도록 Email Security Appliance를 구성했습니다. 조직 A는 게이트웨이 레벨에서 S/MIME 보안 서비스를 수행하도록 서드파티 어플라이언스를 구성했습니다.

참고 현재 예에서는 조직 B가 S/MIME 보안 서비스를 수행하기 위해 서드파티 애플리케이션을 사용하고 있다고 가정합니다. 실제로 이것은 게이트웨이 레벨에서 S/MIME 보안 서비스를 수행할 수 있는 어떤 애플리케이션 또는 어플라이언스(Email Security Appliance 포함)일 수도 있습니다.

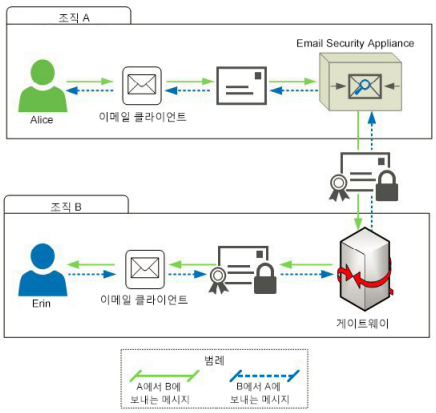
조직 **A**가 조직 **B**에 메시지를 전송합니다.

1. Bob(조직 A)은 이메일 클라이언트를 사용하여 Dave(조직 B)에게 서명되지 않고 암호화되지 않은 메시지를 전송합니다.
2. 조직 A의 Email Security Appliance가 메시지를 서명 및 암호화하여 조직 B로 전송합니다.
3. 조직 B의 게이트웨이에 있는 서드파티 애플리케이션이 메시지를 해독 및 확인합니다.
4. Dave는 암호 해독되고 서명되지 않은 메시지를 수신합니다.

조직 **B**가 조직 **A**에 메시지를 전송합니다.

1. Dave(조직 B)는 이메일 클라이언트를 사용하여 Bob(조직 A)에게 서명되지 않고 암호화되지 않은 메시지를 전송합니다.
2. 조직 B의 게이트웨이에 있는 서드파티 애플리케이션이 메시지를 서명 및 암호화하여 조직 A로 전송합니다.
3. 조직 A의 Email Security Appliance가 메시지를 해독 및 확인합니다.
4. Bob은 암호 해독되고 서명되지 않은 메시지를 수신합니다.

시나리오: Business-to-Consumer



조직 A와 B는 S/MIME을 사용하여 모든 메시지를 서명 및 암호화하여 통신할 수 있기를 원합니다. 조직 A는 게이트웨이 레벨에서 S/MIME 보안 서비스를 수행하도록 Email Security Appliance를 구성했습니다. 조직 B는 S/MIME 보안 서비스를 수행하도록 모든 사용자의 이메일 클라이언트를 구성했습니다.

조직 **A**가 조직 **B**에 메시지를 전송합니다.

1. Alice(조직 A)는 이메일 클라이언트를 사용하여 Erin(조직 B)에게 서명되지 않고 암호화되지 않은 메시지를 전송합니다.
2. 조직 A의 Email Security Appliance가 메시지를 서명 및 암호화하여 조직 B로 전송합니다.
3. 조직 B의 이메일 클라이언트가 메시지를 해독 및 확인하여 Erin에게 표시합니다.

조직 **B**가 조직 **A**에 메시지를 전송합니다.

1. Erin(조직 B)은 이메일 클라이언트를 사용하여 메시지를 서명 및 암호화하여 Alice(조직 A)에게 전송합니다.
2. 조직 A의 Email Security Appliance가 메시지를 해독 및 확인합니다.
3. Alice는 암호 해독되고 서명되지 않은 메시지를 수신합니다.

S/MIME을 사용하여 발신 메시지 서명, 암호화 또는 서명 및 암호화

참고 Email Security Appliance를 사용하여 발신 및 수신 메시지를 서명, 암호화, 서명 및 암호화할 수 있습니다.

Email Security Appliance에서의 S/MIME 서명 및 암호화 워크플로

S/MIME 서명 워크플로

다음 프로세스는 Email Security Appliance에서 S/MIME 서명을 수행하는 방법을 설명합니다.

1. 메시지에 해시 알고리즘을 적용하여 MD(Message Digest)를 만듭니다.
2. 어플라이언스 S/MIME 인증서의 개인 키를 사용하여 MD를 암호화합니다.
3. 어플라이언스 S/MIME 인증서의 개인 키 및 암호화된 MD로 PKCS7 서명을 만듭니다.
4. 메시지에 PKCS7 서명을 어태치하여 메시지를 서명합니다.
5. 서명된 메시지를 수신자에게 전송합니다.

S/MIME 암호화 워크플로

다음 프로세스는 Email Security Appliance에서 S/MIME 암호화를 수행하는 방법을 설명합니다.

1. 의사 난수 세션 키를 만듭니다.
2. 세션 키를 사용하여 메시지 본문을 암호화합니다.
3. 수신자(게이트웨이 또는 소비자) S/MIME 인증서의 공개 키를 사용하여 세션 키를 암호화합니다.
4. 암호화된 세션 키를 메시지에 어태치합니다.
5. 암호화된 메시지를 수신자에게 전송합니다.

참고 어플라이언스에서 PXE 및 S/MIME 암호화가 활성화된 경우 Email Security Appliance는 먼저 S/MIME을 사용하여, 다음에는 PXE를 사용하여 메시지를 암호화합니다.

S/MIME을 사용하여 발신 메시지를 서명, 암호화 또는 서명 및 암호화하는 방법

단계	수행해야 할 작업	추가 정보
1단계	S/MIME 인증서 요구 사항 이해	S/MIME 인증서 요구 사항, 556 페이지를 참조하십시오.
2단계	요구 사항에 따라 다음 중 하나를 수행합니다. • S/MIME 서명의 경우 S/MIME 서명 인증서를 설정합니다. • S/MIME 암호화의 경우 수신자 S/MIME 인증서의 공개 키를 설정합니다. • S/MIME 서명 및 암호화의 경우 S/MIME 서명 인증서 및 수신자 S/MIME 인증서의 공개 키를 각각 설정합니다.	참조: • S/MIME 서명을 위한 인증서 설정, 542 페이지 • S/MIME 암호화를 위한 공개 키 설정, 545 페이지
3단계	메시지를 서명, 암호화 또는 서명 및 암호화하기 위한 프로필을 만듭니다.	메시지의 서명, 암호화 또는 서명 및 암호화용 S/MIME 전송 프로필 만들기, 547 페이지를 참조하십시오.

단계	수행해야 할 작업	추가 정보
4단계	어플라이언스가 메시지를 서명, 암호화 또는 서명 및 암호화하기 위해 충족해야 할 조건을 정의합니다.	서명, 암호화 또는 서명 및 암호화할 메시지 결정, 549 페이지를 참조하십시오.
5단계	이메일 워크플로에서 언제 메시지를 서명, 암호화 또는 서명 및 암호화할지를 결정합니다.	참조: • 콘텐츠 필터를 사용하여 메시지를 서명, 암호화 또는 서명 및 암호화한 후 즉시 전달, 549 페이지 • 콘텐츠 필터를 사용하여 전달 시 메시지를 서명, 암호화 또는 서명 및 암호화, 550 페이지
6단계	메시지를 서명 또는 암호화할 사용자 그룹을 정의합니다.	메일 정책을 만듭니다. 메일 정책, 269 페이지을 참고하십시오.
7단계	정의한 서명 및 암호화 작업을 정의한 사용자 그룹과 연결합니다.	콘텐츠 필터를 메일 정책과 연결합니다. 메일 정책, 269 페이지을 참고하십시오.

참고 CLI를 사용하여 S/MIME 서명, 암호화 또는 서명 및 암호화를 수행하려면 **smimeconfig** 명령을 사용합니다. *AsyncOS for Cisco Email Security Appliances CLI* 참조 가이드를 참고하십시오.

S/MIME 서명을 위한 인증서 설정

메시지 서명을 위한 S/MIME 인증서를 설정해야 합니다. Email Security Appliance에서는 다음 방법 중 하나를 사용하여 S/MIME 서명 인증서를 설정할 수 있습니다.

- 어플라이언스를 사용하여 자체 서명 S/MIME 인증서를 만듭니다. 자체 서명 S/MIME 인증서 만들기, 543 페이지를 참조하십시오.
- 기존의 S/MIME 인증서를 어플라이언스로 가져옵니다. S/MIME 서명 인증서 가져오기, 544 페이지를 참조하십시오.

참고 조직 내에서 또는 테스트 환경에서 사용자에게 서명된 메시지를 보내는 데에는 자체 서명 S/MIME 인증서를 사용하는 것이 좋습니다. 서명된 메시지를 외부 사용자에게 또는 프로덕션 환경에서 전송하려면 신뢰할 수 있는 CA에서 취득한 유효한 S/MIME 인증서를 사용하십시오.

S/MIME에 대한 인증서 요구 사항은 S/MIME 인증서 요구 사항, 556 페이지 섹션을 참조해 주십시오.

자체 서명 S/MIME 인증서 만들기

웹 인터페이스 또는 CLI를 사용하여 RFC 5750(S/MIME(Secure/Multipurpose Internet Mail Extensions) 버전 3.2 - 인증서 처리)을 준수하는 자체 서명 S/MIME 인증서를 생성할 수 있습니다.

참고 조직 내에서 또는 테스트 환경에서 사용자에게 서명된 메시지를 보내는 데에는 자체 서명 S/MIME 인증서를 사용하는 것이 좋습니다.

단계 **1** **Network(**네트워크**)** > **Certificates(**인증서**)**를 클릭합니다.

단계 **2** **Add Certificate(**인증서 추가**)**를 클릭합니다.

단계 **3** **Create Self-Signed S/MIME Certificate(**자체 서명 **S/MIME** 인증서 만들기**)**를 선택합니다.

단계 **4** 자체 서명 인증서에 대해 다음 정보를 입력합니다.

공용 이름	인증된 도메인 이름
조직	조직의 정확한 법인명
조직 단위	조직의 섹션
군/구	조직이 법적으로 위치한 도시
주/도:	조직이 법적으로 위치한 시/도 또는 지역
국가	조직이 법적으로 위치한 국가의 2자 ISO 약어
만료 전까지 기간	인증서가 만료될 때까지 남은 일수
주체 대체 이름(도메인)	이 필드를 구성하면 지정된 도메인의 사용자는 누구나 서명된 메시지를 전송할 수 있습니다. 서명된 메시지를 전송하고자 하는 시작 도메인의 이름. 예를 들어 domain.com 및 *.domain.net 등을 지정할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용하십시오.
주체 대체 이름(이메일)	이 필드를 구성하면 지정된 사용자만 서명된 메시지를 전송할 수 있습니다. 서명된 메시지를 전송하고자 하는 사용자의 이메일 주소(예: user@somedomain.com). 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용하십시오.
개인 키 크기	CSR(Certificate Signing Request)을 생성하기 위한 개인 키의 크기

참고 서명 인증서에는 주체 대체 이름(도메인) 및 주체 대체 이름(이메일)을 모두 포함할 수 있습니다.

단계 **5** 인증서 및 서명 정보를 보려면 **Next(**다음**)**를 클릭합니다.

단계 **6** 요구 사항에 따라 다음을 수행합니다.

- 인증서의 이름을 입력합니다.
- 자체 서명 인증서용 CSR을 CA에 제출하려면 **Download Certificate Signing Request(**인증서 서명 요청 다운로드**)**를 클릭하여 로컬 또는 네트워크 시스템에 CSR을 PEM 형식으로 저장합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

참고 CLI를 사용하여 자체 서명 S/MIME 인증서를 생성하려면 **certconfig** 명령을 사용합니다.

S/MIME 서명 인증서 가져오기

메시지 서명용 S/MIME 인증서를 이미 가지고 있는 경우 가져와서 어플라이언스에 추가할 수 있습니다.

시작하기 전에

가져오려는 S/MIME 인증서가 S/MIME 인증서 요구 사항, 556 페이지에 설명된 요구 사항을 충족하는지 확인합니다.

단계 **1** **Network(**네트워크**)** > **Certificates(**인증서**)**를 클릭합니다.

단계 **2** **Add Certificate(**인증서 추가**)**를 클릭합니다.

단계 **3** **Import Certificate(**인증서 가져오기**)**를 선택합니다.

단계 **4** 네트워크 또는 로컬 컴퓨터에 있는 인증서 파일 경로를 입력합니다.

단계 **5** 파일의 암호를 입력합니다.

단계 **6** **Next(**다음**)**를 클릭하여 인증서 정보를 봅니다.

단계 **7** 인증서의 이름을 입력합니다.

단계 **8** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

참고 CLI를 사용하여 S/MIME 인증서를 가져오려면 **certconfig** 명령을 사용합니다.

S/MIME 암호화를 위한 공개 키 설정

메시지를 암호화하려면 수신자 S/MIME 인증서의 공개 키를 어플라이언스에 추가해야 합니다. 조직의 정책 및 프로세스에 따라 다음 방법 중 하나를 사용하여 공개 키를 어플라이언스에 추가할 수 있습니다.

- 수신자에게 전자 채널(예: 이메일)을 사용하여 공개 키를 전송하도록 요청합니다. 그런 다음 웹 인터페이스 또는 CLI를 사용하여 공개 키를 추가할 수 있습니다.

  공개 키 추가에 대한 자세한 내용은 S/MIME 암호화를 위한 공개 키 추가, 545 페이지 섹션을 참조해 주십시오.

- 웹 인터페이스 또는 CLI를 사용한 공개 키 수집을 활성화하고 수신자에게 서명된 메시지를 전송하도록 요청합니다. Email Security Appliance는 서명된 메시지에서 공개 키를 수집할 수 있습니다.

  서명된 수신 메시지에서 공개 키를 수집하는 방법에 대한 자세한 내용은 공개 키 수집, 546 페이지 섹션을 참조해 주십시오.

S/MIME 암호화를 위한 공개 키 추가

시작하기 전에

- 공개 키가 S/MIME 인증서 요구 사항, 556 페이지에서 명시된 요구 사항을 만족하는지 합니다.
- 공개 키가 EM 형식인지 확인합니다.

단계 **1** **Mail Policies**(메일 정책) > **Public Keys**(공개 키)를 클릭합니다.

단계 **2** **Add Public Key**(공개 키 추가)를 클릭합니다.

단계 **3** 공개 키의 이름을 입력합니다.

단계 **4** 공개 키를 입력합니다.

단계 **5** 변경 사항을 제출하고 커밋합니다.

다음에 수행할 작업

참고 **smimeconfig** 명령을 사용하여 CLI를 통해 공개 키를 추가할 수 있습니다.

S/MIME 수집된 공개 키

들어오는 S/MIME 서명된 메시지에서 공개 키를 검색(수집)하고 수집된 키를 사용하여 수집된 키의 소유자(비즈니스 또는 소비자)에게 암호화된 메시지를 전송하도록 Email Security Appliance를 구성할 수 있습니다.

공개 키 수집은 메일 플로우 정책에서 활성화할 수 있습니다. 수집된 모든 공개 키는 S/MIME Harvested Public Keys(S/MIME 수집된 공개 키) 페이지에 나열됩니다.

관련 항목

- 공개 키 수집, 546 페이지

공개 키 수집

들어오는 S/MIME 서명된 메시지에서 공개 키를 검색(수집)하고 이를 사용하여 수집된 키의 소유자(비즈니스 또는 소비자)에게 암호화된 메시지를 전송하도록 Email Security Appliance를 구성할 수 있습니다.

참고 기본적으로 만료된 또는 자체 서명 S/MIME 인증서의 공개 키는 수집되지 않습니다.

시작하기 전에

발신자의 S/MIME 인증서의 공개 키가 S/MIME 인증서 요구 사항, 556 페이지에 설명된 요구 사항을 충족하는지 확인합니다.

단계 **1** **Mail Policies(**메일 정책**)** > **Mail Flow Policies(**메일 플로우 정책**)**를 클릭합니다.

단계 **2** 새 메일 플로우 정책을 만들거나 기존 정책을 수정합니다.

단계 **3** **Security Features(**보안 기능**)** 섹션으로 스크롤합니다.

단계 **4** S/MIME Public Key Harvesting(S/MIME 공개 키 수집) 아래에서 다음을 수행합니다.

- S/MIME 공개 키 수집을 활성화합니다.
- (선택 사항) 서명된 수신 메시지의 확인에 실패할 경우 공개 키를 수집할지 여부를 선택합니다.
- (선택 사항) 업데이트된 공개 키를 수집할지 여부를 선택합니다.

참고 어플라이언스가 동일한 도메인 또는 메시지로부터 48시간 내에 업데이트된 공개 키를 두 번 이상 수신할 경우 경고문이 전송됩니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

참고 어플라이언스에 있는 수집된 공개 키 저장소의 크기는 512MB입니다. 저장소가 꽉 차면 Email Security Appliance는 사용되지 않은 공개 키를 자동으로 제거합니다.

CLI를 사용하여 키 수집을 활성화하려면 **`listenerconfig`** 명령을 사용합니다.

다음 단계

서명된 메시지를 Email Security Appliance 관리자에게 전송하도록 수신자에게 요청합니다. Email Security Appliance는 서명된 메시지에서 공개 키를 수집하고 Mail Policies(메일 정책) > Harvested Public Keys(수집된 공개 키) 페이지에 표시합니다.

관련 주제

- S/MIME 수집된 공개 키, 545 페이지

S/MIME 전송 프로필 관리

S/MIME 전송 프로필을 사용하면 다음과 같은 매개변수를 정의할 수 있습니다.

- 사용할 S/MIME 모드(예: 서명, 암호화 등)
- 서명을 위한 S/MIME 인증서
- 사용할 S/MIME 서명 모드(예: opaque 또는 detached)
- 수신자 S/MIME 인증서의 공개 키를 어플라이언스에서 사용할 수 없는 경우 수행할 작업

모든 메시지를 서명하여 전송하도록 요구하는 조직과, 모든 메시지를 서명 및 암호화하여 전송하도록 요구하는 조직이 있다고 가정해보겠습니다. 이 시나리오에서는 두 개의 서명 프로필(하나는 서명 전용, 다른 하나는 서명 및 암호화용)을 만들어야 합니다.

웹 인터페이스 또는 CLI를 사용하여 S/MIME 전송 프로필을 생성, 수정, 삭제, 가져오기, 내보내기 및 검색할 수 있습니다.

관련 주제

- 메시지의 서명, 암호화 또는 서명 및 암호화용 S/MIME 전송 프로필 만들기, 547 페이지
- S/MIME 전송 프로필 수정, 549 페이지

메시지의 서명, 암호화 또는 서명 및 암호화용 S/MIME 전송 프로필 만들기

단계 **1** **Mail Policies**(메일 정책) > **Sending Profiles**(전송 프로필)를 클릭합니다.

단계 **2** **Add Profile**(프로필 추가)을 클릭합니다.

단계 **3** 다음 필드를 구성합니다.

S/MIME Profile Name(S/MIME 프로필 이름)	전송 프로필의 이름을 입력합니다.
S/MIME Mode(S/MIME 모드)	S/MIME 모드를 선택합니다. 가능한 값은 다음과 같습니다. • **Sign** • **Encrypt** • **Sign/Encrypt**. 서명 후 암호화 • **Triple**. 서명, 암호화 후 다시 서명 참고 S/MIME 모드 **Sign**, **Sign/Encrypt** 또는 **Triple** 중 하나를 사용하는 경우 서명이 실패하면 메시지가 발신자에게 반송됩니다.

S/MIME Profile Name(S/MIME 프로필 이름)	전송 프로필의 이름을 입력합니다.
서명 인증서	사용할 서명 인증서를 선택합니다. 참고 S/MIME 모드 **Sign**, **Sign/Encrypt** 또는 **Triple** 중 하나를 선택하는 경우에만 이 필드를 설정해야 합니다.
S/MIME Sign Mode(S/MIME 서명 모드)	S/MIME 서명 모드를 선택합니다. 가능한 값은 다음과 같습니다. • **Opaque.** 불투명 서명(opaque-signed) 메시지는 단일 부분에 결합된 메시지 및 서명을 포함하며 서명이 확인되어야만 읽을 수 있습니다. • **Detached.** 서명 정보가 서명되는 텍스트와 분리됩니다. 이것의 MIME 유형은 multipart/signed이며 두 번째 부분의 MIME 하위 유형은 application/(x-)pkcs7-signature입니다. 참고 S/MIME 모드 **Sign**, **Sign/Encrypt** 또는 **Triple** 중 하나를 선택하는 경우에만 이 필드를 설정해야 합니다.
S/MIME Action(S/MIME 작업)	수신자의 공개 키를 사용할 수 없는 경우 Email Security Appliance에서 수행해야 할 작업을 선택합니다. 가능한 값은 다음과 같습니다. • **Bounce**. 수신자의 공개 키 중 하나를 사용할 수 없는 경우 메시지가 발신자에게 반송됩니다. • **Drop**. 수신자의 공개 키 중 하나를 사용할 수 없는 경우 메시지가 삭제됩니다. • **Split**. 메시지가 분리됩니다. 공개 키를 사용할 수 없는 수신자에게 가는 메시지는 암호화 없이 전달되며, 공개 키를 사용할 수 있는 수신자에게 가는 메시지는 암호화되어 전달됩니다. 예: bob@example1.com 및 dave@example2.com으로 메시지를 전송 중이며, dave@example2.com의 공개 키를 사용할 수 없다고 가정해보겠습니다. 이 시나리오에서 **Split**을 선택한 경우 Email Security Appliance는 다음을 수행합니다. • bob@example1.com으로 가는 메시지는 암호화 후 전달합니다. • dave@example2.com으로 가는 메시지는 암호화 없이 전달합니다. 참고 S/MIME 모드 **Encrypt**, **Sign/Encrypt** 또는 **Triple** 중 하나를 선택하는 경우에만 이 필드를 설정해야 합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

참고 CLI를 사용하여 전송 프로필을 만들려면 **smimeconfig** 명령을 사용합니다.

S/MIME 전송 프로필 수정

단계 1 **Mail Policies(**메일 정책**) > Sending Profiles(**전송 프로필**)**를 클릭합니다.

단계 2 수정할 전송 프로필을 클릭합니다.

단계 3 메시지의 서명, 암호화 또는 서명 및 암호화용 S/MIME 전송 프로필 만들기, 547 페이지에 설명된 대로 필드를 수정합니다.

단계 4 변경 사항을 제출 및 커밋합니다.

서명, 암호화 또는 서명 및 암호화할 메시지 결정

전송 프로필을 만든 후에는 어떤 이메일 메시지를 서명, 암호화 또는 서명 및 암호화할지를 결정하는 발신 콘텐츠 필터를 만들어야 합니다. 콘텐츠 필터는 발신 이메일을 검사하고, 메시지가 지정된 조건과 일치하는지를 결정합니다. 메시지가 조건과 일치한다고 콘텐츠 필터가 결정하면 Email Security Appliance는 메시지를 서명, 암호화 또는 서명 및 암호화합니다.

관련 주제

- 콘텐츠를 기준으로 메시지를 필터링하는 방법, 301 페이지

콘텐츠 필터를 사용하여 메시지를 서명, 암호화 또는 서명 및 암호화한 후 즉시 전달

시작하기 전에

콘텐츠 필터의 조건을 구성하는 개념을 이해합니다. 콘텐츠 필터 작동 방식, 283 페이지를 참조하십시오.

단계 1 **Mail Policies(**메일 정책**) > Outgoing Content Filters(**발신 콘텐츠 필터**)**로 이동합니다.

단계 2 필터 섹션에서 **Add Filter(**필터 추가**)**를 클릭합니다.

단계 3 Conditions(조건) 섹션에서 **Add Condition(**조건 추가**)**을 클릭합니다.

단계 4 서명, 암호화 또는 서명 및 암호화할 메시지를 필터링하기 위한 조건을 추가합니다. 예를 들어 민감한 자료를 암호화하기 위해 특정 단어나 문구(예: "Confidential")가 포함된 메시지를 식별하는 조건을 추가할 수 있습니다.

단계 5 **OK(**확인**)**를 클릭합니다.

단계 6 Actions(작업) 섹션에서 **Add Action(**작업 추가**)**을 클릭합니다.

단계 7 **Add Action(**작업 추가**)** 목록에서 **S/MIME Sign/Encrypt (Final Action)(S/MIME** 서명/암호화**(**최종 작업**))**를 선택합니다.

단계 8 콘텐츠 필터와 관련된 전송 프로필을 선택합니다.

단계 9 **OK(**확인**)**를 클릭합니다.

단계 **10** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

콘텐츠 필터를 추가한 후 발신 메일 정책에 필터를 추가해야 합니다. 조직의 요구에 따라, 기본 정책에서 콘텐츠 필터를 활성화하거나 특정 메일 정책에 필터를 적용하고자 할 수 있습니다. 메일 정책 작업에 대한 자세한 내용은 메일 정책 개요, 269 페이지 섹션을 참조해 주십시오.

콘텐츠 필터를 사용하여 전달 시 메시지를 서명, 암호화 또는 서명 및 암호화

전달 시 메시지를 서명, 암호화 또는 서명 및 암호화하기 위한 콘텐츠 필터를 만듭니다. 즉, 메시지가 계속해서 처리의 다음 단계로 이동하다가 처리가 완료되면 서명, 암호화 또는 서명 및 암호화되어 전달됩니다.

시작하기 전에

- 콘텐츠 필터의 조건을 구성하는 개념을 이해합니다. 콘텐츠 필터 개요 , 283 페이지를 참조하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Outgoing Content Filters(**발신 콘텐츠 필터**)**로 이동합니다.

단계 **2** 필터 섹션에서 **Add Filter(**필터 추가**)**를 클릭합니다.

단계 **3** Conditions(조건) 섹션에서 **Add Condition(**조건 추가**)**을 클릭합니다.

단계 **4** 서명, 암호화 또는 서명 및 암호화할 메시지를 필터링하기 위한 조건을 추가합니다. 예를 들어 민감한 자료를 암호화하기 위해 특정 단어나 문구(예: "Confidential")가 포함된 메시지를 식별하는 조건을 추가할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** Actions(작업) 섹션에서 **Add Action(**작업 추가**)**을 클릭합니다.

단계 **7** **Add Action(**작업 추가**)** 목록에서 **S/MIME Sign/Encrypt on Delivery(**전달 시 **S/MIME** 서명/암호화**)**를 선택합니다.

단계 **8** 콘텐츠 필터와 관련된 전송 프로필을 선택합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

콘텐츠 필터를 추가한 후 발신 메일 정책에 필터를 추가해야 합니다. 조직의 요구에 따라, 기본 정책에서 콘텐츠 필터를 활성화하거나 특정 메일 정책에 필터를 적용하고자 할 수 있습니다. 메일 정책 작업에 대한 자세한 내용은 메일 정책 개요, 269 페이지 섹션을 참조해 주십시오.

S/MIME을 사용하여 수신 메시지 확인, 해독 또는 해독 및 확인

참고 수신 및 발신 메시지를 확인, 해독 또는 해독 및 확인하는 데 Email Security Appliance S/MIME 보안 서비스를 사용할 수 있습니다.

Email Security Appliance에서의 S/MIME 확인 및 해독 워크플로

S/MIME 확인 워크플로

다음 프로세스는 Email Security Appliance가 S/MIME 확인을 수행하는 방법을 설명합니다.

1. 서명된 메시지에 해시 알고리즘을 적용하여 MD(Message Digest)를 만듭니다.
2. 전송자 S/MIME 인증서의 공개 키를 사용하여 서명된 메시지에 어태치된 PKCS7 서명을 해독하고, MD(Message Digest)를 얻습니다.
3. 서명된 메시지에서 검색한 MD와 생성된 MD를 비교합니다. MD가 일치하면 메시지가 확인됩니다.
4. 인증 기관을 사용하여 발신자 도메인의 S/MIME 인증서를 검증합니다.

S/MIME 해독 워크플로

다음 프로세스는 Email Security Appliance에서 S/MIME 해독을 수행하는 방법을 설명합니다.

1. 어플라이언스 S/MIME 인증서의 개인 키를 사용하여 세션 키를 해독합니다.
2. 세션 키를 사용하여 메시지 본문을 해독합니다.

S/MIME을 사용하여 수신 메시지를 확인, 해독 또는 해독 및 확인하는 방법

단계	수행해야 할 작업	추가 정보
1단계	S/MIME 인증서 요구 사항 이해	S/MIME 인증서 요구 사항, 556 페이지를 참조하십시오.

2단계	요구 사항에 따라 다음 중 하나를 수행합니다.
	• S/MIME 해독을 위해 조직의 S/MIME 인증서(해독 수행에 필요한 개인 키 포함)를 어플라이언스에 추가합니다.
	• S/MIME 확인을 위해, 확인 수행에 필요한 발신자 S/MIME 인증서의 공개 키를 어플라이언스에 추가합니다.
	• S/MIME 해독 및 확인을 위해 다음을 어플라이언스에 추가합니다.
	  • 조직의 S/MIME 인증서(해독 수행에 필요한 개인 키 포함)
	  • 발신자 도메인의 인증 기관.
	  • 확인 수행에 필요한 발신자 S/MIME 인증서의 공개 키
		참조:
		• 메시지 해독을 위해 인증서 설정, 552 페이지
		• 서명된 메시지 확인을 위한 공개 키 설정, 553 페이지
		• 사용자 지정 인증 기관 목록 가져오기, 663 페이지

3단계	S/MIME을 사용하여 수신 메시지를 확인, 해독 또는 해독 및 확인하기 위한 메일 플로우 정책을 구성합니다.	S/MIME 해독 및 확인 활성화, 555 페이지를 참조하십시오.
4단계	(선택 사항) 해독 또는 확인된 메시지에 대해 Email Security Appliance에서 수행하는 작업을 정의합니다.	S/MIME 해독 또는 확인 메시지를 위한 작업 구성, 556 페이지를 참조하십시오.

참고 CLI를 사용하여 S/MIME 확인, 해독 또는 해독 및 확인을 수행하려면 **`listenerconfig > hostaccess`** 명령을 사용합니다. 자세한 내용은 CLI 온라인 도움말을 참조하십시오.

메시지 해독을 위해 인증서 설정

조직의 S/MIME 인증서(해독 수행에 필요한 개인 키 포함)를 어플라이언스에 추가해야 합니다.

시작하기 전에

- 다음 중 한 가지 방법으로 어플라이언스 S/MIME 인증서의 공개 키를 발신자와 공유합니다.

- 전자 채널(예: 이메일)을 사용하여 공개 키를 전송합니다.
- 키 수집을 사용하여 공개 키를 검색하도록 발신자에게 요청합니다.

발신자는 이 공개 키를 사용하여 어플라이언스에 암호화된 메시지를 전송할 수 있습니다.

참고 B2C 시나리오에서 조직의 S/MIME 인증서가 도메인 인증서이면, 일부 이메일 클라이언트(예: Microsoft Outlook)는 조직의 S/MIME 인증서의 공개 키를 사용하여 암호화된 메시지를 전송하지 못할 수 있습니다. 이러한 이메일 클라이언트는 도메인 인증서의 공개 키를 사용하여 암호화를 지원하지 않기 때문입니다.

- 가져오려는 S/MIME 인증서가 S/MIME 인증서 요구 사항, 556 페이지에 설명된 요구 사항을 충족하는지 확인합니다.

단계 **1** **Network**(네트워크) > **Certificates**(인증서)를 클릭합니다.

단계 **2** **Add Certificate**(인증서 추가)를 클릭합니다.

단계 **3** **Import Certificate**(인증서 가져오기)를 선택합니다.

단계 **4** 네트워크 또는 로컬 컴퓨터에 있는 인증서 파일 경로를 입력합니다.

단계 **5** 파일의 암호를 입력합니다.

단계 **6** **Next**(다음)를 클릭하여 인증서 정보를 봅니다.

단계 **7** 인증서의 이름을 입력합니다.

단계 **8** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

참고 CLI를 사용하여 S/MIME 인증서를 추가하려면 **certconfig** 명령을 사용합니다.

서명된 메시지 확인을 위한 공개 키 설정

서명된 메시지를 확인하려면 발신자 S/MIME 인증서의 공개 키를 어플라이언스에 추가해야 합니다. 조직의 정책 및 프로세스에 따라 다음 방법 중 하나를 사용하여 공개 키를 어플라이언스에 추가할 수 있습니다.

- 발신자에게 전자 채널(예: 이메일)을 사용하여 공개 키를 전송하도록 요청합니다. 그런 다음 웹 인터페이스 또는 CLI를 사용하여 공개 키를 추가할 수 있습니다.

  공개 키 추가에 대한 자세한 내용은 S/MIME 암호화를 위한 공개 키 추가, 545 페이지 섹션을 참조하십시오.

- 키 수집을 사용하여 공개 키를 검색합니다. 공개 키 수집, 546 페이지를 참조하십시오.

S/MIME 확인을 위한 공개 키 추가

시작하기 전에

- 공개 키가 S/MIME 인증서 요구 사항, 556 페이지에서 명시된 요구 사항을 만족하는지 합니다.
- 공개 키가 EM 형식인지 확인합니다.

단계 1 **Mail Policies**(메일 정책) > **Public Keys**(공개 키)를 클릭합니다.
단계 2 **Add Public Key**(공개 키 추가)를 클릭합니다.
단계 3 공개 키의 이름을 입력합니다.
단계 4 공개 키를 입력합니다.
단계 5 변경 사항을 제출하고 커밋합니다.

다음에 수행할 작업

참고 **smimeconfig** 명령을 사용하여 CLI를 통해 공개 키를 추가할 수 있습니다.

S/MIME 확인을 위한 공개 키 수집

들어오는 S/MIME 서명된 메시지에서 공개 키를 검색(수집)하고 이를 사용하여 수집된 키의 소유자(비즈니스 또는 소비자)에게서 오는 암호화된 메시지를 확인하도록 Email Security Appliance를 구성할 수 있습니다.

참고 기본적으로 만료된 또는 자체 서명 S/MIME 인증서의 공개 키는 수집되지 않습니다.

1. 웹 인터페이스 또는 CLI를 사용한 공개 키 수집을 활성화합니다. 공개 키 수집 활성화, 554 페이지를 참조하십시오.
2. 서명된 메시지를 전송하도록 발신자에게 요청합니다.
3. 수집이 완료되면 수집된 공개 키를 어플라이언스에 추가합니다. S/MIME 확인을 위해 수집된 공개 키 추가, 555 페이지를 참조하십시오.

이 단계는 게이트웨이 레벨에서 메시지를 확인하기 위한 것입니다.

공개 키 수집 활성화

단계 1 **Mail Policies**(메일 정책) > **Mail Flow Policies**(메일 플로우 정책)를 클릭합니다.
단계 2 새 메일 플로우 정책을 만들거나 기존 정책을 수정합니다.
단계 3 **Security Features**(보안 기능) 섹션으로 스크롤합니다.

단계 **4** S/MIME Public Key Harvesting(S/MIME 공개 키 수집) 아래에서 다음을 수행합니다.

- S/MIME 공개 키 수집을 활성화합니다.
- (선택 사항) 서명된 수신 메시지의 확인에 실패할 경우 공개 키를 수집할지 여부를 선택합니다.
- (선택 사항) 업데이트된 공개 키를 수집할지 여부를 선택합니다.

참고 어플라이언스가 동일한 도메인 또는 메시지로부터 48시간 내에 업데이트된 공개 키를 두 번 이상 수신할 경우 경고문이 전송됩니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

참고 어플라이언스에 있는 수집된 공개 키 저장소의 크기는 512MB입니다. 저장소가 꽉 차면 Email Security Appliance는 사용되지 않은 공개 키를 자동으로 제거합니다.

CLI를 사용하여 키 수집을 활성화하려면 **`listenerconfig`** 명령을 사용합니다.

S/MIME 확인을 위해 수집된 공개 키 추가

단계 **1** **Mail Policies(**메일 정책**)** > **Harvested Public Keys(**수집된 공개 키**)**를 클릭합니다.

단계 **2** 의도적으로 수집한 공개 키를 클릭하고 공개 키를 복사합니다.

단계 **3** 공개 키를 어플라이언스에 추가합니다. S/MIME 확인을 위한 공개 키 추가, 554 페이지를 참조하십시오.

단계 **4** 변경 사항을 제출 및 커밋합니다.

S/MIME 해독 및 확인 활성화

단계 **1** **Mail Policies(**메일 정책**)** > **Mail Flow Policies(**메일 플로우 정책**)**를 클릭합니다.

단계 **2** 새 메일 플로우 정책을 만들거나 기존 정책을 수정합니다.

단계 **3** **Security Features(**보안 기능**)** 섹션으로 스크롤합니다.

단계 **4** S/MIME Decryption/Verification(S/MIME 해독/확인) 아래에서 다음을 수행합니다.

- S/MIME 해독 및 확인을 활성화합니다.
- S/MIME 확인 후 메시지에서 디지털 서명을 유지할지 제거할지를 선택합니다. 최종 사용자가 S/MIME 게이트웨이 확인에 대해 알지 못하게 하려면 **Remove(**제거**)**를 선택합니다.

삼중 래핑(triple wrapped) 메시지의 경우 내부 서명만 유지 또는 제거됩니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

팁 메일 플로우 정책에서 S/MIME 해독 및 확인이 활성화된 경우 해독 및 확인의 상태와 상관없이 모든 S/MIME 메시지가 전달됩니다. S/MIME 해독 또는 확인 메시지를 처리하기 위한 작업을 구성하려면 메시지 필터 규칙 smime-gateway-verified 및 smime-gateway를 사용할 수 있습니다. 자세한 내용은 S/MIME 해독 또는 확인 메시지를 위한 작업 구성, 556 페이지를 참고하십시오.

S/MIME 해독 또는 확인 메시지를 위한 작업 구성

Email Security Appliance에서 S/MIME 해독, 확인 또는, 해독 및 확인을 완료한 후 결과에 따라 서로 다른 작업을 수행할 수 있습니다. 해독, 확인 또는 둘 모두의 결과를 기반으로 메시지 필터 규칙 smime-gateway-verified 및 smime-gateway를 사용하여 메시지에 대해 작업을 수행할 수 있습니다. 자세한 내용은 메시지 필터를 사용하여 이메일 정책 적용, 137 페이지 섹션을 참조하십시오.

참고 해독, 확인 또는 둘 모두의 결과를 기반으로 콘텐츠 필터 조건 **S/MIME Gateway Message** 및 **S/MIME Gateway Verified**를 사용할 수도 있습니다. 자세한 내용은 콘텐츠 필터, 283 페이지 섹션을 참조하십시오.

예: 해독, 확인 또는 둘 모두에 실패한 S/MIME 메시지 격리

다음 메시지 필터는 메시지가 S/MIME 메시지인지를 검토한 후, S/MIME을 사용한 확인 또는 해독이 실패하는 경우 메시지를 격리합니다.

```
quarantine_smime_messages:if (smime-gateway-message and not smime-gateway-verified)
{ quarantine("Policy"); }
```

S/MIME 인증서 요구 사항

서명을 위한 인증서 요구 사항

서명을 위한 S/MIME 인증서에는 다음 정보가 포함됩니다.

공용 이름	인증된 도메인 이름
조직	조직의 정확한 법인명

공용 이름	인증된 도메인 이름
조직 단위	조직의 섹션
군/구	조직이 법적으로 위치한 도시
주/도:	조직이 법적으로 위치한 시/도 또는 지역
국가	조직이 법적으로 위치한 국가의 2자 ISO 약어
만료 전까지 기간	인증서가 만료될 때까지 남은 일수
주체 대체 이름(도메인)	서명된 메시지를 전송하고자 하는 시작 도메인의 이름. 예를 들어 domain.com 및 *.domain.net 등을 지정할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용하십시오.
주체 대체 이름(이메일)	서명된 메시지를 전송하고자 하는 사용자의 이메일 주소(예: user@somedomain.com). 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용하십시오.
개인 키 크기	CSR에 대해 생성할 개인 키의 크기
키 사용	키 사용은 어떤 인증서가 사용 가능한지를 결정하는 제한 방법입니다. 키 사용 확장을 지정하는 경우 digitalSignature 및 nonRepudiation 비트를 설정해야 합니다. 키 사용 확장이 지정되어 있지 않으면 수신 클라이언트는 digitalSignature 및 nonRepudiation 비트가 설정된 것으로 가정합니다.

S/MIME 인증서에 대한 자세한 내용은 RFC 5750: S/MIME(Secure/Multipurpose Internet Mail Extensions) 버전 3.2 - 인증서 처리를 참조해 주십시오.

암호화를 위한 인증서 요구 사항

암호화를 위한 S/MIME 인증서에는 다음 정보가 포함됩니다.

공용 이름	인증된 도메인 이름
조직	조직의 정확한 법인명
조직 단위	조직의 섹션
군/구	조직이 법적으로 위치한 도시
주/도:	조직이 법적으로 위치한 시/도 또는 지역
국가	조직이 법적으로 위치한 국가의 2자 ISO 약어
만료 전까지 기간	인증서가 만료될 때까지 남은 일수

공용 이름	인증된 도메인 이름
주체 대체 이름(도메인)	암호화된 메시지를 전송하고자 하는 대상 도메인의 이름 예를 들어 domain.com 및 *.domain.net 등을 지정할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용하십시오. 암호화된 메시지를 도메인의 모든 사용자에게 전송하려면 공개 키에 SAN Domain이 포함되어 있어야 합니다.
주체 대체 이름(이메일)	암호화된 메시지를 전송하고자 하는 사용자의 이메일 주소(예: user@somedomain.com). 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용하십시오.
개인 키 크기	CSR에 대해 생성할 개인 키의 크기
키 사용	키 사용은 어떤 인증서가 사용 가능한지를 결정하는 제한 방법입니다. 키 사용 확장을 지정해야 하며 keyEncipherment 비트를 설정해야 합니다.

S/MIME 인증서에 대한 자세한 내용은 RFC 5750: S/MIME(Secure/Multipurpose Internet Mail Extensions) 버전 3.2 - 인증서 처리를 참조해 주십시오.

공개 키 관리

Email Security Appliance에는 다음이 필요합니다.

- 발신 메시지 암호화를 위한 수신자 S/MIME 암호화 인증서의 공개 키
- 서명된 수신 메시지 확인을 위한 발신자 S/MIME 서명 인증서의 공개 키

다음 방법 중 하나를 사용하여 어플라이언스에 공개 키를 추가할 수 있습니다.

- 의도적인 공개 키가 PEM 형식인 경우 웹 인터페이스 또는 CLI를 사용하여 추가할 수 있습니다. 공개 키 추가, 558 페이지를 참조하십시오.
- 내보내기 파일에 의도적인 공개 키가 포함된 경우, 내보내기 파일을 /configuration 디렉터리로 복사한 다음 웹 인터페이스 또는 CLI를 사용하여 가져올 수 있습니다. 기존의 내보내기 파일에서 공개 키 가져오기, 559 페이지를 참조하십시오.

Email Security Appliance는 또한 키 수집을 지원합니다(서명된 수신 메시지에서 공개 키를 자동으로 검색). 자세한 내용은 S/MIME 수집된 공개 키, 545 페이지를 참고하십시오.

공개 키 추가

시작하기 전에

- 공개 키가 S/MIME 인증서 요구 사항, 556 페이지에서 명시된 요구 사항을 만족하는지 합니다.
- 공개 키가 EM 형식인지 확인합니다.

단계 **1** **Mail Policies**(메일 정책) > **Public Keys**(공개 키)를 클릭합니다.
단계 **2** **Add Public Key**(공개 키 추가)를 클릭합니다.
단계 **3** 공개 키의 이름을 입력합니다.
단계 **4** 공개 키를 입력합니다.
단계 **5** 변경 사항을 제출하고 커밋합니다.

다음에 수행할 작업

참고 **smimeconfig** 명령을 사용하여 CLI를 통해 공개 키를 추가할 수 있습니다.

기존의 내보내기 파일에서 공개 키 가져오기

시작하기 전에

내보내기 파일을 어플라이언스의 /configuration 디렉터리로 복사합니다. 내보내기 파일을 만드는 방법에 대한 자세한 내용은 공개 키 내보내기, 559 페이지 섹션을 참조하십시오.

단계 **1** **Mail Policies** > **Public Keys**(메일 정책 > 공개 키)를 클릭합니다.
단계 **2** **Import Public Keys**(공개 키 가져오기)를 클릭합니다.
단계 **3** 내보내기 파일을 선택하고 **Submit**(제출)을 클릭합니다.

참고 공개 키의 수가 많은 파일을 가져오는 경우 가져오기 프로세스가 오래 걸릴 수 있습니다. 웹 인터페이스 또는 CLI 비활성 시간 초과를 적절히 조정해야 합니다.

단계 **4** 변경사항을 커밋합니다.

공개 키 내보내기

어플라이언스의 모든 공개 키는 단일 텍스트 파일에서 함께 내보내어 /configuration 디렉터리에 저장됩니다.

단계 **1** **Mail Policies**(메일 정책) > **Public Keys**(공개 키)를 선택합니다.
단계 **2** **Export Public Keys**(공개 키 내보내기)를 클릭합니다.
단계 **3** 파일 이름을 입력하고 **Submit**(제출)을 클릭합니다.

23 장

Office 365 사서함에서 자동으로 메시지 치료

이 장에는 다음 섹션이 포함되어 있습니다.

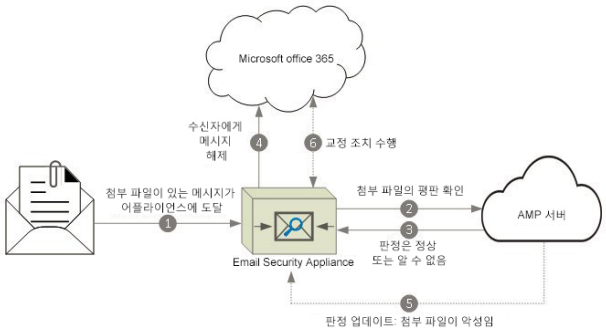
위협 판정이 악성으로 변경된 경우 엔드 유저에게 전달되는 메시지에 대한 치료 작업 수행

파일은 사용자의 사서함에 도달한 후에도 언제든지 악성코드를 켤 수 있습니다. AMP는 이를 새 정보로 식별하고 검토 알림을 어플라이언스에 푸시할 수 있습니다. 이 릴리스에서는 단순한 알림 이상의 기능을 제공받을 수 있습니다. 조직에서 Office 365를 사용하여 사서함을 관리하는 경우 위협 판정이 변경되면 사용자 사서함의 메시지에 대한 자동 치료 작업을 수행하도록 어플라이언스를 구성할 수 있습니다. 예를 들어 첨부 파일의 판정이 정상에서 악성으로 변경된 경우 수신자의 사서함에서 메시지를 삭제하도록 어플라이언스를 구성할 수 있습니다.

목차

워크플로

그림 ***36:*** 사서함 자동 치료 워크플로



1. 첨부 파일이 포함된 메시지가 어플라이언스에 도달했습니다.
2. 어플라이언스는 AMP 서버를 쿼리하여 첨부 파일의 평판을 평가합니다.
3. AMP 서버는 판정을 어플라이언스로 전송합니다. 판정은 정상 또는 알 수 없음입니다.
4. 어플라이언스는 수신자에게 메시지를 릴리스합니다.
5. 특정 기간이 지나면 어플라이언스는 AMP 서버에서 판정 업데이트를 수신합니다. 새로운 판정은 악성코드입니다.
6. 어플라이언스는 수신자의 사서함에 있는 메시지(악성 첨부 파일 포함)에서 구성된 치료 작업을 수행합니다.

위협 판정이 악성으로 변경된 경우 엔드 유저에게 전달되는 메시지에 대해 치료 작업을 수행하는 방법

	수행해야 할 작업	추가 정보
1단계	사전 요구 사항을 검토합니다.	사전 요구 사항, 563 페이지
2단계	Azure AD(Azure 관리 포털)의 애플리케이션으로 Email Security Appliance를 등록합니다.	어플라이언스를 Azure AD에 애플리케이션으로 등록, 564 페이지
3단계	어플라이언스에서 Office 365 사서함 설정을 구성합니다.	Cisco Email Security 어플라이언스에서 Office 365 사서함 설정 구성, 566 페이지
4단계	위협 판정이 악성으로 변경된 경우 엔드 유저에게 전달되는 메시지에 대한 치료 작업을 수행하도록 어플라이언스를 구성합니다.	위협 판정이 악성으로 변경된 경우 엔드 유저에게 전달되는 메시지에 대한 치료 작업 구성, 567 페이지

사전 요구 사항

파일 평판 서비스 및 파일 분석 서비스에 대한 기능 키

다음을 확인하십시오.

- 파일 평판 서비스 및 파일 분석 서비스에 대한 기능 키를 추가했습니다.
- 어플라이언스에서 파일 평판 및 분석 기능을 활성화했습니다. File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석), 461 페이지를 참조하십시오.

Office 365 어카운트

어플라이언스를 Azure AD에 등록하는 데 필요한 다음 어카운트가 있는지 확인합니다.

- Office 365 비즈니스 어카운트
- Office 365 비즈니스 어카운트와 연결된 Azure AD 서브스크립션

자세한 내용은 Office 365 관리자에 게 문의하십시오.

보안 통신용 인증서

Office 365 서비스와 어플라이언스 간의 통신을 보호하려면 다음 방법 중 하나로 인증서를 설정해야 합니다. 자체 서명 인증서를 생성하거나 신뢰할 수 있는 CA에서 인증서를 가져옵니다.

다음이 있어야 합니다.

- .crt 또는. p12 형식의 공개 키. emailAddress가 Office 365 관리자의 이메일 주소(<admin_username>@<domain>.com)로 설정되었는지 확인합니다.
- pem 형식의 연결된 개인 키(키 크기는 2048비트 이상).

참고 암호가 포함된 개인 키는 이 릴리스에서 지원되지 않습니다.

어플라이언스를 Azure AD에 애플리케이션으로 등록

Office 365 서비스는 Azure AD(Azure Active Directory)를 사용하여 사용자의 사서함에 대한 보안 액세스를 제공합니다. 어플라이언스에서 Office 365 사서함에 액세스하려면 어플라이언스를 Azure AD에 등록해야 합니다. 어플라이언스를 Azure AD에 등록하기 위해 수행해야 하는 개략적인 단계는 다음과 같습니다. 자세한 지침은 Microsoft 설명서 (https://msdn.microsoft.com/en-us/office/office365/howto/add-common-consent-manually)를 참고하십시오.

시작하기 전에

사전 요구 사항, 563 페이지에 설명된 작업을 수행합니다.

단계 **1** Office 365 비즈니스 어카운트 크리덴셜을 사용하여 Azure 관리 포털에 로그인합니다.

단계 **2** Office 365 서브스크립션에 연결된 디렉터리에 새 애플리케이션을 추가합니다. 새 애플리케이션을 추가하는 동안 다음을 확인합니다.

- 웹 애플리케이션 및/또는 웹 API로 애플리케이션 유형을 선택합니다.
- 다음 파라미터를 지정합니다.
  - 로그온 URL. 이 URL은 사용자가 로그인하여 어플라이언스를 사용할 수 있는 URL입니다(예: `https://<company_domain>/ManualRegistration`).
  - 앱 ID URI. Microsoft Azure AD가 어플라이언스에 사용할 수 있는 고유한 URI입니다(예: `https://<company_domain>`).

단계 **3** 애플리케이션 및 애플리케이션에 필요한 권한을 구성합니다. 새로 생성된 애플리케이션의 Configure (구성) 탭에서 Office 365 Exchange Online을 애플리케이션으로 추가하고 다음 권한을 설정합니다.

- 애플리케이션 권한
  - 모든 사용자로 메일 전송
  - 모든 사서함의 메일 읽기 및 쓰기
  - 모든 사서함에서 메일 읽기
  - 모든 사서함에 대한 전체 액세스 권한으로 Exchange Web Services 사용
- 위임된 권한
  - 사용자로 메일 보내기
  - 사용자 메일 읽기 및 쓰기
  - 사용자 메일 읽기
  - Exchange Web Services를 통해 로그인한 사용자로 사서함 액세스

단계 **4** 공개 키 인증서의 키 크리덴셜을 사용하여 애플리케이션 매니페스트를 업데이트하여 Office 365 서비스와 어플라이언스 간의 통신을 보호합니다. 다음 단계를 수행하십시오.

a) Windows PowerShell 프롬프트를 사용하여 공개 키 인증서에서 `$base64Thumbprint`, `$base64Value` 및 `$keyid` 값을 가져옵니다. 다음 예를 참조하십시오.

Windows PowerShell 프롬프트에서 공개 키 인증서가 포함된 디렉터리로 이동하여 다음을 실행합니다.

예제:

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import(".\mycer.cer")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()
```

위 명령을 실행한 후 다음 명령을 실행하여 값을 추출합니다.

- `$keyid`
- `$base 64value`
- `$base 64thumbprint`

b) Azure 관리 포털에서 애플리케이션 매니페스트를 다운로드합니다.

c) 텍스트 수정기를 사용하여 다운로드한 매니페스트를 열고 비어 있는 keycredentials 속성을 다음 JSON으로 대체합니다.

예제:

```
"keyCredentials": [
     {
        "customKeyIdentifier" : "$base64Thumbprint_from_step_1",
        "keyId": "$keyid_from_step1",
        "type": "AsymmetricX509Cert",
        "usage": "Verify",
        "value": "$base64Value_from_step1"
     }
],
```

위의 JSON 조각에서 `$base 64thumbprint`의 값을 `$base 64thumbprint`로, 그리고 `$keyid` a 단계에서 구한 값으로 대체해야 합니다. 각 값은 한 줄에 입력해야 합니다.

d) 변경 사항을 저장하고 수정된 매니페스트를 Azure 관리 포털에 업로드합니다.

단계 **5** Azure AD를 사용하여 어플라이언스를 등록한 후 Azure 관리 포털에서 다음 세부 정보를 기록해 둡니다.

- Configure(구성) 탭의 클라이언트 ID.
- View Endpoints(엔드포인트 보기) > App Endpoints(애플리케이션 엔드포인트) 페이지의 테넌트 ID. 테넌트 ID는 이 페이지에 나열된 모든 URL에서 사용할 수 있는 고유한 값입니다. 예를 들어 이 페이지에 나열된 URL은 다음과 같습니다.
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/federationmetadata/2007-06/federationmetadata.xml
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/wsfed
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/saml2

이 경우 테넌트 ID는 abcd1234-bcdd-469d-8545-a0662708cbc3입니다.

다음에 수행할 작업

Cisco Email Security 어플라이언스에서 Office 365 사서함 설정 구성, 566 페이지

Cisco Email Security 어플라이언스에서 Office 365 사서함 설정 구성

시작하기 전에

다음을 확인하십시오.

- 어플라이언스에서 파일 평판 및 분석 기능을 활성화했습니다. File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석), 461 페이지의 내용을 참조하십시오.
- pem 형식으로 인증서의 개인 키를 가져왔습니다. 보안 통신용 인증서, 563 페이지의 내용을 참조하십시오.
- 다음 파라미터 값:
  - Azure 관리 포털에 등록한 애플리케이션의 클라이언트 ID 및 테넌트 ID. 어플라이언스를 Azure AD에 애플리케이션으로 등록, 564 페이지의 5단계를 참고하십시오.
  - 인증서 핑거프린트($base 64thumbprint). 어플라이언스를 Azure AD에 애플리케이션으로 등록, 564 페이지의 4단계를 참고하십시오.

단계 **1** 어플라이언스에 로그인합니다.

단계 **2** **System Administration**(시스템 관리) > **Mailbox Settings**(사서함 설정)를 클릭합니다.

단계 **3** **Enable**(활성화)을 클릭합니다.

단계 **4** **Enable Office 365 Mailbox Settings**(**Office 365** 사서함 설정 활성화)를 선택합니다.

단계 **5** 다음 세부사항을 입력합니다.

- Azure 관리 포털에 등록한 애플리케이션의 클라이언트 ID 및 테넌트 ID.
- 인증서 핑거프린트(base64Thumbprint 값).

단계 **6** 인증서의 개인 키를 업로드합니다. **Choose File**(파일 선택)을 클릭하고 .pem 파일을 선택합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

단계 **8** 어플라이언스를 통해 Office 365 서비스에 연결할 수 있는지 확인합니다.

1. **Check Connection**(연결 확인)을 클릭합니다.
2. Office 365 이메일 주소를 입력합니다. 이 주소는 Office 365 도메인의 유효한 이메일 주소여야 합니다.
3. **Test Connection**(테스트 연결)을 클릭합니다.

어플라이언스를 통해 Office 365 서비스에 연결할 수 있는지 여부가 표시된 팝업이 나타납니다. 연결에 실패하면 다음을 확인합니다.

- 클라이언트 ID, 테넌트 ID 및 지문 값이 올바른지 여부.

- 업로드한 개인 키가 올바르고 만료되지 않았는지 여부.

다음에 수행할 작업

위협 판정이 악성으로 변경된 경우 엔드 유저에게 전달되는 메시지에 대한 치료 작업 구성, 567 페이지

위협 판정이 악성으로 변경된 경우 엔드 유저에게 전달되는 메시지에 대한 치료 작업 구성

시작하기 전에

어플라이언스에서 Office 365 사서함 설정을 구성했는지 확인합니다. Cisco Email Security 어플라이언스에서 Office 365 사서함 설정 구성, 566 페이지의 내용을 참조하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)**를 선택합니다.

단계 **2** 수정할 메일 정책의 **Advanced Malware Protection** 열에 있는 링크를 클릭합니다.

단계 **3** **Enable Mailbox Auto Remediation(**사서함 자동 치료 활성화**)**을 선택합니다.

단계 **4** 위협 판정이 악성으로 변경된 경우 엔드 유저에게 전달되는 메시지에 대해 수행할 작업을 지정합니다. 요구 사항에 따라 다음 치료 작업 중 하나를 선택합니다.

- 이메일 주소로 전달합니다. 악성 첨부 파일이 포함된 메시지를 지정된 사용자(예: 이메일 관리자)에게 전달하려면 이 옵션을 선택합니다.
- 메시지를 삭제합니다. 엔드 유저의 사서함에서 악성 첨부 파일이 포함된 메시지를 영구적으로 삭제하려면 이 옵션을 선택합니다.
- 이메일 주소로 전달하고 메시지를 삭제합니다. 악성 첨부 파일이 포함된 메시지를 이메일 관리자 등 지정된 사용자에게 전달하고 엔드 유저의 사서함에서 해당 메시지를 영구적으로 삭제하려면 이 옵션을 선택합니다.

참고 Office 365 서비스는 이러한 폴더에서 메시지 삭제를 지원하지 않으므로 특정 폴더(예: 지운 편지함)의 메시지는 삭제할 수 없습니다.

단계 **5** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- 사서함 치료 결과 모니터링, 568 페이지
- 메시지 추적에서 사서함 치료 상세정보 보기, 568 페이지
- 사서함 치료 트러블슈팅, 568 페이지

사서함 치료 결과 모니터링

Mailbox Auto Remediation(사서함 자동 치료) 보고서 페이지(**Monitor(모니터)** > **Mailbox Auto Remediation(사서함 자동 치료)**)를 사용하여 사서함 치료 결과의 세부 정보를 볼 수 있습니다. 이 보고서를 사용하여 다음과 같은 세부 정보를 봅니다.

- 사서함 치료에 성공했거나 실패한 수신자 목록
- 메시지에 수행된 교정 조치
- SHA-256 해시와 관련된 파일 이름

Recipients for whom remediation was unsuccessful(치료에 실패한 수신자**)** 필드는 다음과 같은 시나리오에서 업데이트됩니다.

- 수신자가 유효한 Office 365 사용자가 아니거나 수신자가 어플라이언스에 구성된 Office 365 도메인 계정에 속하지 않습니다.
- 사서함에서 첨부 파일이 포함된 메시지를 더 이상 사용할 수 없습니다. 예를 들어, 엔드 유저가 메시지를 삭제했습니다.
- 어플라이언스에 구성된 교정 조치를 수행하려 했을 때 어플라이언스와 Office 365 서비스 간의 연결 문제가 있었습니다.

메시지 추적에서 관련된 메시지를 보려면 SHA-256 해시를 클릭합니다.

메시지 추적에서 사서함 치료 상세정보 보기

메시지 추적에서 사서함 치료에 대한 상세정보를 표시하려면

- 메시지 추적을 활성화해야 합니다. 메시지 추적, 837 페이지를 참조하십시오.
- Office 365 사서함 설정(**System Administration(**시스템 관리**)** > **Mailbox Settings(**사서함 설정**)**)을 구성해야 합니다. Cisco Email Security 어플라이언스에서 Office 365 사서함 설정 구성, 566 페이지의 내용을 참조하십시오.
- 사서함 치료 작업(**Security Services** > **Mailbox Auto Remediation(**사서함 자동 치료**)**)이 구성되어 있어야 합니다. 위협 판정이 악성으로 변경된 경우 엔드 유저에게 전달되는 메시지에 대한 치료 작업 구성, 567 페이지를 참조하십시오.

표시되는 데이터에 대한 자세한 내용은 메시지 추적 세부 정보 , 842 페이지 섹션을 참조하십시오.

사서함 치료 트러블슈팅

- 어플라이언스와 Office 365 서비스 간의 연결을 확인할 수 없음, 569 페이지
- 로그 보기, 569 페이지
- 알림, 570 페이지
- 구성된 치료 작업이 수행되지 않음, 570 페이지

어플라이언스와 **Office 365** 서비스 간의 연결을 확인할 수 없음

문제

Mailbox Settings(사서함 설정) 페이지(**System Administration(**시스템 관리**)** > **Mailbox Settings(**사서함 설정**)**)에서 어플라이언스 및 Office 365 서비스 간의 연결을 확인하는 중에 `Connection Unsuccessful(연결 실패)` 오류 메시지가 표시됩니다.

솔루션

서버의 응답에 따라 다음 중 하나를 수행합니다.

오류 메시지	이유 및 솔루션
`The SMTP address has no mailbox associated with it`	Office 365 도메인에 속하지 않는 이메일 주소를 입력했습니다. 유효한 이메일 주소를 입력하고 연결을 다시 확인하십시오.
`Application with identifier '<client_id>' was not found in the directory <tenant_id>`	유효하지 않은 클라이언트 ID를 입력했습니다. 사서함 설정 페이지에서 클라이언트 ID를 수정하고 연결을 다시 확인하십시오.
`No service namespace named '<tenant_id>' was found in the data store.`	유효하지 않은 테넌트 ID를 입력했습니다. 사서함 설정 페이지에서 테넌트 ID를 수정하고 연결을 다시 확인하십시오.
`Error validating credentials. Credential validation failed`	유효하지 않은 인증서 지문을 입력했습니다. 사서함 설정 페이지에서 인증서 지문을 수정하고 연결을 다시 확인하십시오.
`Error validating credentials. Client assertion contains an invalid signature.`	잘못된 인증서 지문을 입력했거나 유효하지 않거나 잘못된 인증서 개인 키를 업로드했습니다. 다음을 확인하십시오. • 올바른 지문을 입력했습니다. • 올바른 인증서 개인 키를 업로드했습니다. • 인증서 개인 키가 만료되지 않았습니다. • 어플라이언스의 표준 시간대가 인증서 개인 키의 표준 시간대와 일치합니다.

로그 보기

사서함 치료 정보가 다음 로그에 게시됩니다.

- 메일 로그(mail_logs). 사서함 치료 프로세스가 시작된 시간이 이 로그에 게시됩니다.
- 사서함 자동 치료 로그(mar). 치료 상태, 수행된 작업, 오류 등의 정보가 이 로그에 게시됩니다.

알림

알림: 어플라이언스 및 **Office 365** 서비스 간의 연결 문제가 탐지됨

문제

어플라이언스와 Office 365 서비스 간에 연결 문제가 있어 어플라이언스에서 구성된 치료 작업을 수행할 수 없음을 나타내는 정보 수준 알림이 제공됩니다.

솔루션

다음을 수행합니다.

- 어플라이언스와 Office 365 서비스 간의 통신을 방해할 수 있는 네트워크 문제를 확인합니다.

  어플라이언스의 네트워크 설정을 검토합니다. 네트워크 설정 변경, 986 페이지의 내용을 참조하십시오.
- 방화벽 문제를 확인합니다. 방화벽 정보, 1227 페이지를 참조하십시오.
- Office 365 서비스가 작동 중인지 확인합니다.

구성된 치료 작업이 수행되지 않음

문제

AMP 서버에서 회귀 알림을 받은 후 Office 365 사서함의 악성 메시지에 대해 구성된 치료 작업이 수행되지 않습니다.

솔루션

다음을 수행합니다.

- 어플라이언스와 Office 365 서비스 간의 연결을 테스트합니다. Cisco Email Security 어플라이언스에서 Office 365 사서함 설정 구성, 566 페이지의 8단계를 참고하십시오.
- 어플라이언스 및 Office 365 서비스 간의 연결 문제가 탐지됨 알림을 받았는지 확인합니다. 알림, 570 페이지를 참조하십시오.

24 장

이메일 인증

이 장에는 다음 섹션이 포함되어 있습니다.

이메일 인증 개요

AsyncOS는 이메일 확인 및 이메일 위조 방지를 위한 서명을 지원합니다. 수신 메일을 확인하기 위해 AsyncOS는 SPF(Sender Policy Framework), SIDF(Sender ID Framework), DKIM(DomainKeys Identified Mail), DMARC(Domain-based Message Authentication, Reporting and Conformance) 및 위조 이메일 탐지를 지원합니다. 아웃바운드 메일을 인증하기 위해 AsyncOS는 DomainKeys 및 DKIM 서명을 지원합니다.

관련 주제

- DomainKeys 및 DKIM 인증, 572 페이지
- SPF 및 SIDF 확인 개요, 591 페이지
- DMARC 확인, 602 페이지
- 위조 이메일 탐지, 610 페이지

DomainKeys 및 DKIM 인증

DomainKeys 또는 DKIM 이메일 인증 환경에서 발신자는 공개 키 암호화를 사용하여 이메일에 서명할 수 있습니다. 그러면 확인된 도메인을 이메일의 From:(또는 Sender:) 헤더에 있는 도메인과 비교하여 위조를 탐지할 수 있습니다.

DomainKeys 및 DKIM은 서명과 확인이라는 두 개의 주요 부분으로 구성되어 있습니다. AsyncOS는 DomainKeys의 경우 프로세스의 "서명" 절반을 지원하고, DKIM의 경우 서명과 확인을 모두 지원합니다. 또한 DomainKeys 및 DKIM 서명을 사용하여 반송과 지연 메시지를 활성화할 수 있습니다.

관련 주제

- DomainKeys 및 DKIM 인증 워크플로, 572 페이지
- AsyncOS에서 DomainKeys 및 DKIM 서명, 572 페이지

DomainKeys 및 DKIM 인증 워크플로

그림 ***37:*** 인증 워크플로

1. 관리자(도메인 소유자)는 공개 키를 DNS 이름 공간에 게시합니다.
2. 관리자는 아웃바운드 MTA(Mail Transfer Agent)에서 개인 키를 로드합니다.
3. 해당 도메인의 인증된 사용자가 제출한 이메일은 개별 개인 키를 사용해 디지털 방식으로 서명됩니다. DomainKey 또는 DKIM 서명 헤더로서 서명이 이메일에 삽입되고 이메일이 전송됩니다.
4. MTA를 수신하면 헤더에서 DomainKeys 또는 DKIM 서명이 추출되고 이메일에서 클레임된 전송 도메인(Sender: 또는 From: 헤더를 통해)이 추출됩니다. DomainKeys 또는 DKIM 서명 헤더 필드에서 추출된 클레임된 서명 도메인에서 공개 키가 검색됩니다.
5. 공개 키는 DomainKeys 또는 DKIM 서명이 적절한 개인 키로 생성되었는지를 판단하는 데 사용됩니다.

발신 DomainKeys 서명을 테스트하려면 Yahoo! 또는 Gmail 주소를 사용할 수 있습니다. 이러한 주소는 무료이며 DomainKeys로 서명된 수신 메시지에 대한 검증을 제공하기 때문입니다.

AsyncOS에서 DomainKeys 및 DKIM 서명

AsyncOS에서 DomainKeys 및 DKIM 서명은 도메인 프로필을 통해 구현되며 메일 플로우 정책(일반적으로 발신 "릴레이" 정책)을 통해 활성화됩니다. 자세한 내용은 "이메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오. 메시지 서명은 어플라이언스에서 메시지 전송 전에 수행하는 마지막 작업입니다.

도메인 프로필은 도메인을 도메인 키 정보(서명 키 및 관련 정보)와 연결합니다. 이메일은 어플라이언스의 메일 플로우 정책을 통해 전송되므로 도메인 프로필과 일치하는 발신자 이메일 주소는 도메인 프로필에 지정된 서명 키와 함께 DomainKeys로 서명됩니다. DKIM 및 DomainKeys 서명을 모두

활성화하면 DKIM 서명이 사용됩니다. CLI의 domainkeysconfig 명령 또는 GUI의 Mail Policies(메일 정책) > Domain Profiles(도메인 프로필) 및 Mail Policies(메일 정책) > Signing Keys(서명 키) 페이지를 통해 DomainKeys 및 DKIM 프로필을 구현합니다.

DomainKeys 및 DKIM 서명의 작동 방식은 다음과 같습니다. 도메인 소유자가 두 개의 키를 생성합니다. 하나는 공개 DNS에 저장되는 공개 키이고(DNS TXT 레코드가 해당 도메인과 연결됨), 다른 하나는 어플라이언스에 저장되는 개인 키입니다. 개인 키는 해당 도메인에서 전송되는(메일이 시작되는) 메일에 서명하는 데 사용됩니다.

메시지는 메시지 전송(아웃바운드)에 사용되는 리스너에서 수신되므로 어플라이언스는 도메인 프로필이 존재하는지를 확인합니다. 어플라이언스에서 생성된(그리고 메일 플로우 정책에 대해 구현된) 도메인 프로필이 있는 경우 메시지에서 유효한 Sender: 또는 From: 주소가 검색됩니다. 둘 다 존재하는 경우 Sender: 헤더는 항상 도메인 키 및 dkim 서명에 사용되지만, From: 헤더는 DKIM 서명에 사용되지 않는 경우에도 필요합니다. Sender: 헤더만 있는 경우에는 DomainKeys 또는 DKIM 서명 프로파일이 일치하지 않습니다. From: 헤더는 다음과 같은 경우에만 사용됩니다.

- Sender: 헤더가 없습니다.
- 웹 인터페이스의 DKIM Global Setting(DKIM 전역 설정) 페이지에서 Use From Header for DKIM Signing(DKIM 서명에 From 헤더 사용) 옵션을 선택합니다.

참고 Async0S 10.0 이상에서는 웹 인터페이스의 DKIM Global Setting(DKIM 전역 설정) 페이지에서 DKIM 서명에 From: 헤더를 사용할지 여부를 선택할 수 있습니다. 적절한 DMARC 확인을 위해서는 DKIM 서명과 함께 From: 헤더를 사용해야 합니다.

유효한 주소가 발견되지 않으면 메시지가 서명되지 않으며 mail_logs에 이벤트가 기록됩니다.

참고 DomainKey 및 DKIM 프로필을 모두 만드는 경우(그리고 메일 플로우 정책에서 서명을 활성화하는 경우) AsyncOS는 DomainKeys 및 DKIM 서명 모두를 사용하여 발신 메시지에 서명합니다.

유효한 전송 주소가 발견되면 기존 도메인 프로필을 기준으로 전송 주소가 일치하는지 확인됩니다. 일치가 발견되면 메시지가 서명됩니다. 그렇지 않으면 메시지가 서명 없이 전송됩니다. 메시지에 기존 DomainKeys("DomainKey-Signature:" 헤더)가 있으면, 원래 서명 이후 새 발신자 주소가 추가된 경우에만 메시지가 서명됩니다. 메시지에 기존 DKIM 서명이 있으면 새 DKIM 서명이 메시지에 추가됩니다.

AsyncOS는 도메인을 기반으로 이메일에 서명하고 서명 키를 관리하기 위한(새로 만들기 또는 기존 키 입력) 메커니즘을 제공합니다.

이 문서의 컨피그레이션 설명은 서명 및 확인의 가장 일반적인 사용 사례를 보여줍니다. 인바운드 이메일에 대해 메일 플로우 정책에서 DomainKeys 및 DKIM 서명을 활성화하거나, 아웃바운드 이메일에 대해 메일 플로우 정책에서 DKIM 확인을 활성화할 수 있습니다.

참고 클러스터링된 환경에서 도메인 프로필 및 서명 키를 구성할 때에는 Domain Key Profile(도메인 키 프로필) 설정과 Signing Key(서명 키) 설정이 연결되어 있다는 점에 유의하십시오. 따라서 서명 키를 복사, 이동 또는 삭제하면 연결된 프로필에서도 동일한 작업이 수행됩니다.

DomainKeys 및 DKIM 서명 구성

관련 주제

- 서명 키, 574 페이지
- 공용 키, 575 페이지
- 도메인 프로파일, 575 페이지
- 반송 및 지연 메시지에 대해 서명 활성화, 576 페이지
- 발신 메일에 대한 서명 활성화, 576 페이지
- DomainKeys/DKIM 서명 구성(GUI), 577 페이지
- DomainKeys 및 로깅, 586 페이지

서명 키

서명 키는 어플라이언스에 저장되는 개인 키입니다. 서명 키를 만들 때 키 크기를 지정합니다. 키 크기가 클수록 더 안전합니다. 그러나 키가 클수록 성능에 영향을 미칠 수 있습니다. 어플라이언스는 512비트부터 최대 2048비트까지의 키를 지원합니다. 오늘날 대부분의 발신자가 사용하며 안전하다고 할 수 있는 키 크기의 범위는 768~1024비트입니다. 더 큰 크기의 키는 성능에 영향을 미칠 수 있으며 2048비트가 넘는 키는 지원되지 않습니다. 서명 키 만들기에 대한 자세한 내용은 서명 키 만들기 및 수정, 580 페이지 섹션을 참조하십시오.

기존 키를 입력할 경우에는 단순히 양식에 붙여 넣으면 됩니다. 기존 서명 키를 사용하는 또 다른 방법은 텍스트 파일로 키를 가져오는 것입니다. 기존 서명 키 추가에 대한 자세한 내용은 기존 서명 키 가져오기 또는 입력 , 581 페이지 섹션을 참조하십시오.

입력한 키는 도메인 프로필에서 사용 가능하며, 도메인 프로필의 Signing Key(서명 키) 드롭다운 목록에 나타납니다.

관련 주제

- 서명 키 내보내기 및 가져오기, 574 페이지

서명 키 내보내기 및 가져오기

어플라이언스의 텍스트 파일로 서명 키를 내보낼 수 있습니다. 키를 내보내면 현재 어플라이언스에 있는 모든 키가 텍스트 파일에 추가됩니다. 키 내보내기에 대한 자세한 내용은 서명 키 내보내기, 581 페이지 섹션을 참조하십시오.

내보낸 키를 가져올 수도 있습니다.

참고 키를 가져오면 어플라이언스에 있는 모든 현재 키가 교체됩니다.

자세한 내용은 기존 서명 키 가져오기 또는 입력 , 581 페이지를 참고하십시오.

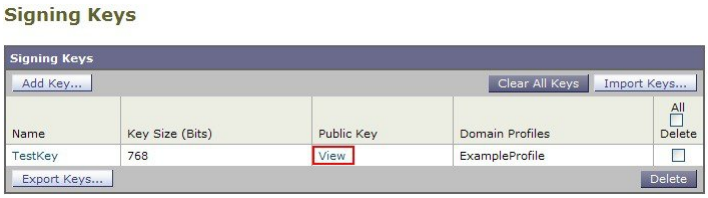
공용 키

서명 키를 도메인 프로파일과 연결하면 공개 키를 포함하는 DNS 텍스트 기록을 생성할 수 있습니다. 도메인 프로필 목록에 있는 DNS Text Record(DNS 텍스트 레코드) 열의 Generate(생성) 링크를 통해 (또는 CLI의 **`domainkeysconfig -> profiles -> dnstxt`**를 통해) 만들면 됩니다.

DNS 텍스트 레코드 생성에 대한 자세한 내용은 DNS 텍스트 레코드 생성 , 583 페이지 섹션을 참조하십시오.

Signing Keys(서명 키) 페이지의 View(보기) 링크를 통해 공개 키를 볼 수도 있습니다.

그림 ***38: Signing Keys(서명 키)*** 페이지의 공개 키 보기 링크



도메인 프로파일

도메인 프로필은 서명에 필요한 몇 가지 다른 정보와 함께 발신자 도메인을 서명 키와 연결합니다.

- 도메인 프로필의 이름.
- 도메인 이름("d=" 헤더에 포함할 도메인).
- 선택자(선택자는 공개 키에 대한 쿼리를 만드는 데 사용됩니다. DNS 쿼리 유형에서 이 값은 발신 도메인의 "_domainkey." 네임 공간 앞에 추가됩니다.)
- 정규화(canonicalization) 방법(헤더 및 콘텐츠를 서명 알고리즘에 표시하기 위해 준비하는 방법) AsyncOS는 DomainKeys에 대해서는 "simple" 및 "nofws"를 지원하고, DKIM에 대해서는 "relaxed" 및 "simple"을 지원합니다.
- 서명 키(자세한 내용은 서명 키, 574 페이지 참조).
- 헤더 목록 및 서명할 본문 길이(DKIM 전용).
- 서명 헤더에 포함할 태그의 목록(DKIM 전용). 이러한 태그는 다음 정보를 저장합니다.
  - 메시지가 서명된 사용자 또는 에이전트(예: 메일 목록 관리자)의 ID.
  - 공개 키 검색에 사용되는 쉼표로 구분된 쿼리 방법 목록.
  - 서명이 생성된 타임스탬프.
  - 서명의 만료 시간(초 단위).
  - 메시지가 언제 서명되었는지를 나타내는, 세로 막대(|)로 구분된 헤더 필드의 목록.

- 서명에 포함할 태그(DKIM 전용).
- 프로필 사용자 목록(서명에 도메인 프로필을 사용하도록 허용된 주소).

참고 프로필 사용자에 지정된 주소의 도메인은 Domain(도메인) 필드에 지정된 도메인과 일치해야 합니다.

특정 기간 동안 기존의 모든 도메인 프로필에서 검색할 수 있습니다. 자세한 내용은 도메인 프로필 검색, 585 페이지를 참조하십시오.

또한 다음 여부를 선택할 수 있습니다.

- DKIM 서명으로 시스템 생성 메시지에 서명
- DKIM 서명에 From 헤더 사용

자세한 내용은 DKIM 전역 설정 수정, 585 페이지 섹션을 참조해 주십시오.

관련 주제

- 도메인 프로필 내보내기 및 가져오기, 576 페이지

도메인 프로필 내보내기 및 가져오기

어플라이언스의 텍스트 파일로 기존 도메인 프로필을 내보낼 수 있습니다. 도메인 프로필을 내보내면 현재 어플라이언스에 있는 모든 프로필이 단일 텍스트 파일에 추가됩니다. 도메인 프로필 내보내기, 584 페이지를 참조하십시오.

앞서 내보낸 도메인 프로필을 가져올 수 있습니다. 도메인 프로필을 가져오면 시스템에 있는 모든 현재 도메인 프로필이 교체됩니다. 도메인 프로필 가져오기, 584 페이지를 참조하십시오.

발신 메일에 대한 서명 활성화

아웃바운드 메일에 대한 메일 플로우 정책에서 DomainKeys 및 DKIM 서명이 활성화됩니다. 자세한 내용은 "이메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

단계 **1** Mail Policies(메일 정책) 메뉴의 Mail Flow Policies(메일 플로우 정책) 페이지에서 RELAYED 메일 플로우 정책(발신)을 클릭합니다.

단계 **2** Security Features(보안 기능) 섹션에서 On(켜기)을 선택하여 DomainKeys/DKIM Signing(DomainKeys/DKIM 서명)을 활성화합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

반송 및 지연 메시지에 대해 서명 활성화

아웃바운드 메시지에 서명하는 것 외에 반송 및 지연 메시지에도 서명할 수 있습니다. 자신의 회사에서 보내는 반송 및 지연 메시지가 합법적인 것임을 수신자에게 알리기 위해 이렇게 할 수 있습니다.

반송 및 지연 메시지에 대해 DomainKeys 및 DKIM 서명을 활성화하려면, 퍼블릭 리스너와 연결된 반송 프로필에 대해 DomainKeys/DKIM 서명을 활성화합니다.

단계 **1** 서명된 아웃바운드 메시지를 전송할 퍼블릭 리스너와 연결된 반송 프로필에서 Hard Bounce and Delay Warning Messages(하드 반송 및 지연 경고 메시지)로 이동합니다.

단계 **2** "Use Domain Key Signing for Bounce and Delay Messages(반송 및 지연 메시지에 DomainKeys 서명 사용)"를 활성화합니다.

참고 반송 및 지연 메시지에 서명하려면 DomainKeys/DKIM 서명 구성(GUI), 577 페이지에 나열된 모든 단계를 완료해야 합니다.

도메인 프로필의 From: 주소는 반송 반환 주소에 사용되는 주소와 일치해야 합니다. 이러한 주소가 일치하도록 하려면 반송 프로필에 대한 반환 주소를 구성하고(System Administration(시스템 관리) > Return Addresses(반환 주소)), 도메인 프로필의 Profile Users(프로필 사용자) 목록에서 동일한 이름을 사용할 수 있습니다. 예를 들면 반송 반환 주소에 대해 MAILER-DAEMON@example.com 반환 주소를 구성하고, 도메인 프로필의 프로필 사용자로 MAILER-DAEMON@example.com을 추가할 수 있습니다.

DomainKeys/DKIM 서명 구성(GUI)

단계 **1** 새 개인 키를 만들거나 기존의 개인 키를 가져옵니다. 서명 키 만들기 또는 가져오기에 대한 자세한 내용은 서명 키, 574 페이지 섹션을 참조하십시오.

단계 **2** 도메인 프로필을 만들고 키를 도메인 프로필과 연결합니다. 도메인 프로필 만들기에 대한 자세한 내용은 도메인 프로파일, 575 페이지 섹션을 참조하십시오.

단계 **3** DNS 텍스트 레코드를 만듭니다. DNS 텍스트 레코드 만들기에 대한 자세한 내용은 DNS 텍스트 레코드 생성 , 583 페이지 섹션을 참조하십시오.

단계 **4** 아직 하지 않은 경우, 아웃바운드 메일에 대한 메일 플로우 정책에서 DomainKeys/DKIM 서명을 활성화합니다(발신 메일에 대한 서명 활성화, 576 페이지 참조).

단계 **5** 선택적으로, 반송 및 지연 메시지에 대해 DomainKeys/DKIM 서명을 활성화합니다. 반송 및 지연 메시지에 대해 서명을 활성화하는 방법에 대한 자세한 내용은 반송 및 지연 메시지에 대해 서명 활성화, 576 페이지 섹션을 참조하십시오.

단계 **6** 이메일을 전송합니다. 도메인 프로필과 일치하는 도메인에서 전송된 메일은 DomainKeys/DKIM으로 서명됩니다. 또한 반송 및 지연 메시지에 대한 서명을 구성한 경우에도 반송 및 지연 메시지가 서명됩니다.

참고 DomainKey 및 DKIM 프로필을 모두 만드는 경우(그리고 메일 플로우 정책에서 서명을 활성화하는 경우) AsyncOS는 DomainKeys 및 DKIM 서명 모두를 사용하여 발신 메시지에 서명합니다.

다음에 수행할 작업

관련 주제

DomainKeys 서명을 위한 도메인 프로필 만들기

단계 1 **Mail Policies**(메일 정책) > **Signing Profiles**(서명 프로필)를 선택합니다.

단계 2 **Domain Signing Profiles**(도메인 서명 프로필) 섹션에서 **Add Profile**(프로필 추가)을 클릭합니다.

단계 3 프로필의 이름을 입력합니다.

단계 4 **Domain Key Type**(도메인 키 유형)에 대해 **Domain Keys**(도메인 키)를 선택합니다.

페이지에 추가 옵션이 나타납니다.

단계 5 도메인 이름을 선택합니다.

단계 6 선택자를 입력합니다. 선택자는 "_domainkey" 네임 공간 앞에 추가되는 임의의 이름으로서, 전송 도메인당 여러 동시 공개 키를 지원하기 위해 사용됩니다. 선택자 값과 길이는 세미콜론을 포함할 수 없다는 추가 조건과 함께 DNS 네임 공간 및 이메일 헤더에서 규칙을 준수해야 합니다.

단계 7 정규화를 선택합니다(no forwarding whitespaces 또는 simple).

단계 8 이미 서명 키를 만든 경우 서명 키를 선택합니다. 그렇지 않은 경우 다음 단계로 건너뜁니다. 서명 키를 목록에서 선택할 수 있으려면 하나 이상의 서명 키를 만들어야(또는 가져와야) 합니다. 서명 키 만들기 및 수정, 580 페이지를 참조하십시오.

단계 9 서명에 도메인 프로필을 사용할 사용자(이메일 주소, 호스트 등)를 입력합니다.

단계 10 변경 사항을 제출 및 커밋합니다.

단계 11 아직 하지 않았다면 지금 발신 메일 플로우 정책에서 DomainKeys/DKIM 서명을 활성화해야 합니다(발신 메일에 대한 서명 활성화, 576 페이지 참조).

참고 DomainKeys 및 DKIM 프로필을 모두 만든 경우 AsyncOS는 발신 메일에서 DomainKeys 및 DKIM 서명을 모두 수행합니다.

DKIM 서명을 위한 새 도메인 프로필 만들기

단계 1 **Mail Policies**(메일 정책) > **Signing Profiles**(서명 프로필)를 선택합니다.

단계 2 **Domain Signing Profiles**(도메인 서명 프로필) 섹션에서 **Add Profile**(프로필 추가)을 클릭합니다.

단계 3 프로필의 이름을 입력합니다.

단계 4 **Domain Key Type**(도메인 키 유형)에 대해 **DKIM**을 선택합니다.

페이지에 추가 옵션이 나타납니다.

단계 **5** 도메인 이름을 선택합니다.

단계 **6** 선택자를 입력합니다. 선택자는 "_domainkey." 네임 공간 앞에 추가되는 임의의 이름으로서, 전송 도메인당 여러 동시 공개 키를 지원하기 위해 사용됩니다. 선택자 값과 길이는 세미콜론을 포함할 수 없다는 추가 조건과 함께 DNS 네임 공간 및 이메일 헤더에서 규칙을 준수해야 합니다.

단계 **7** 헤더에 대한 정규화를 선택합니다. 다음 옵션 중에서 선택합니다.

- **Relaxed**. "relaxed" 헤더 정규화 알고리즘은 다음을 수행합니다. 헤더 이름이 소문자로 변경되고, 헤더가 확장되고, 여러 선형 공백이 단일 공백으로 줄고, 앞뒤 공백이 제거됩니다.
- **Simple**. 헤더가 변경되지 않습니다.

단계 **8** 본문에 대한 정규화를 선택합니다. 다음 옵션 중에서 선택합니다.

- **Relaxed**. "relaxed" 헤더 정규화 알고리즘은 다음을 수행합니다. 본문 끝에서 빈 줄이 제거되고, 줄 내에서 여러 공백이 단일 공백으로 줄고, 줄에서 뒤의 공백이 제거됩니다.
- **Simple.** 본문 끝의 빈 줄이 제거됩니다.

단계 **9** 이미 서명 키를 만든 경우 서명 키를 선택합니다. 그렇지 않은 경우 다음 단계로 건너뜁니다. 서명 키를 목록에서 선택할 수 있으려면 하나 이상의 서명 키를 만들어야(또는 가져와야) 합니다. 서명 키 만들기 및 수정, 580 페이지를 참조하십시오.

단계 **10** 서명할 헤더 목록을 선택합니다. 다음 헤더 중에서 선택할 수 있습니다.

- **All**. AsyncOS는 서명 당시 존재하는 모든 헤더에 서명합니다. 전송 중에 헤더가 추가 또는 제거될 것으로 예상되지 않는 경우 모든 헤더에 서명할 수 있습니다.
- **Standard**. 전송 중에 헤더가 추가 또는 제거될 것으로 예상되는 경우 표준 헤더를 선택할 수 있습니다. AsyncOS는 다음 표준 헤더에만 서명합니다(메시지에 헤더가 없는 경우 DKIM 서명은 헤더에 대한 null 값을 나타냅니다).
  - From
  - Sender, Reply To-
  - Subject
  - Date, Message-ID
  - To, Cc
  - MIME-Version
  - Content-Type, Content-Transfer-Encoding, Content-ID, Content-Description
  - Resent-Date, Resent-From, Resent-Sender, Resent-To, Resent-cc, Resent-Message-ID
  - In-Reply-To, References
  - List-Id, List-Help, List-Unsubscribe, LIst-Subscribe, List-Post, List-Owner, List-Archive

참고 "Standard"를 선택한 경우 서명할 헤더를 추가할 수 있습니다.

단계 **11** 메시지 본문에 서명할 방법을 지정합니다. 본문에 서명하도록 선택할 수 있으며, 서명할 바이트 크기를 선택할 수도 있습니다. 다음 옵션 중 하나를 선택합니다.

- **Whole Body Implied(**전체 본문 암시**)**. 본문 길이를 결정하는 데 "l=" 태그를 사용하지 마십시오. 전체 메시지가 서명되며 변경이 허용되지 않습니다.
- **Whole Body Auto-determined(**전체 본문 자동 결정**)**. 전체 메시지 본문이 서명되며, 전송 중 본문 끝에 일부 추가 데이터를 첨부하는 것이 허용됩니다.
- **Sign first _ bytes(**처음 _바이트에 서명**).** 지정된 바이트 수만큼의 메시지 본문에 서명합니다.

단계 **12** 메시지 서명의 본문 필드에 포함할 태그를 선택합니다. 이러한 태그에 저장되는 정보는 메시지 서명 확인에 사용됩니다. 다음 옵션 중 하나 이상을 선택합니다.

- **"i"** 태그. 해당 메시지가 서명된 사용자 또는 에이전트(예: 메일 목록 관리자)의 ID. @ 기호 뒤에 도메인 이름을 입력합니다(예: @example.com).
- **"q"** 태그. 공개 키 검색에 사용되는 콜론으로 구분된 쿼리 방법 목록. 현재 유효한 값은 dns/txt뿐입니다.
- **"t"** 태그. 서명이 생성된 때에 대한 타임스탬프.
- **"x"** 태그. 서명이 만료되는 절대 날짜 및 시간. 서명의 만료 시간(초)을 지정합니다. 기본값은 31536000초입니다.
- **"z"** 태그. 메시지가 언제 서명되었는지를 나타내는, 세로 막대(|)로 구분된 헤더 필드의 목록. 여기에는 헤더 필드의 이름 및 값이 포함됩니다. 예를 들면 다음과 같습니다.

z=From:admin@example.come|To:joe@example.com|
Subject:test%20message|Date:Date:August%2026,%202011%205:30:02%20PM%20-0700

단계 **13** 서명에 도메인 프로필을 사용할 사용자(이메일 주소, 호스트 등)를 입력합니다.

참고 도메인 프로필을 만들 때, 특정 사용자와 연결할 프로필을 결정하는 데 계층 구조가 사용된다는 점에 유의하십시오. 예를 들면 example.com에 대한 프로필을 만들고 joe@example.com에 대한 또 다른 프로필을 만듭니다. joe@example.com에서 메일을 전송할 때 joe@example.com에 대한 프로필이 사용됩니다. 그러나 adam@example.com에서 메일을 전송할 때는 example.com에 대한 프로필이 사용됩니다.

단계 **14** 변경 사항을 제출 및 커밋합니다.

단계 **15** 아직 하지 않았다면 지금 발신 메일 플로우 정책에서 DomainKeys/DKIM 서명을 활성화해야 합니다(발신 메일에 대한 서명 활성화, 576 페이지 참조).

참고 DomainKeys 및 DKIM 프로필을 모두 만든 경우 AsyncOS는 발신 메일에서 DomainKeys 및 DKIM 서명을 모두 수행합니다.

서명 키 만들기 및 수정

새 서명 키 만들기

DomainKeys 및 DKIM 서명용 도메인 프로필에 서명 키가 필요합니다.

단계 **1** **Mail Policies**(메일 정책) > **Signing Keys**(서명 키)를 선택합니다.
단계 **2** **Add Key**(키 추가)를 클릭합니다.
단계 **3** 키의 이름을 입력합니다.
단계 **4** **Generate**(생성)를 클릭하고 키 크기를 선택합니다.
단계 **5** 변경 사항을 제출 및 커밋합니다.

참고 아직 하지 않은 경우, 키 할당을 위해 도메인 프로필을 수정해야 할 수 있습니다.

기존 서명 키 수정

단계 **1** **Mail Policies**(메일 정책) > **Signing Keys**(서명 키)를 선택합니다.
단계 **2** 원하는 서명 키를 클릭합니다.
단계 **3** 새 서명 키 만들기, 580 페이지에 설명된 대로 원하는 필드를 수정합니다.
단계 **4** 변경 사항을 제출 및 커밋합니다.

서명 키 내보내기

내보내기를 수행하면 어플라이언스의 모든 키가 단일 텍스트 파일에 저장됩니다.

단계 **1** **Mail Policies**(메일 정책) > **Signing Keys**(서명 키)를 선택합니다.
단계 **2** **Export Keys**(키 내보내기)를 클릭합니다.
단계 **3** 파일 이름을 입력하고 **Submit**(제출)을 클릭합니다.

기존 서명 키 가져오기 또는 입력

관련 주제

- 키 붙여넣기 , 581 페이지
- 기존의 내보내기 파일에서 키 가져오기 , 582 페이지

키 붙여넣기

단계 **1** **Mail Policies**(메일 정책) > **Signing Keys**(서명 키)를 선택합니다.
단계 **2** **Add Key**(키 추가)를 클릭합니다.
단계 **3** Paste Key(키 붙여넣기) 필드에 키를 붙여넣습니다(PEM 형식이거나 RSA 키만 가능).

단계 **4** 변경 사항을 제출 및 커밋합니다.

기존의 내보내기 파일에서 키 가져오기

참고 키 파일을 가져오려면 서명 키 내보내기, 581 페이지 섹션을 참조하십시오.

단계 **1** **Mail Policies(**메일 정책**) > Signing Keys(**서명 키**)**를 선택합니다.

단계 **2** **Import Keys(**키 가져오기**)**를 클릭합니다.

단계 **3** 내보낸 서명 키가 포함된 파일을 선택합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다. 가져오기를 수행하면 기존의 모든 서명 키가 교체된다는 경고가 표시됩니다. 텍스트 파일의 모든 키를 가져오게 됩니다.

단계 **5** **Import(**가져오기**)**를 클릭합니다.

서명 키 삭제

관련 주제

- 선택한 서명 키 제거 , 582 페이지
- 모든 서명 키 제거 , 582 페이지

선택한 서명 키 제거

단계 **1** **Mail Policies(**메일 정책**) > Signing Keys(**서명 키**)**를 선택합니다.

단계 **2** 제거할 각 서명 키의 오른쪽에 있는 확인란을 선택합니다.

단계 **3** **Delete(**삭제**)**를 클릭합니다.

단계 **4** 삭제를 확인합니다.

모든 서명 키 제거

단계 **1** **Mail Policies(**메일 정책**) > Signing Keys(**서명 키**)**를 선택합니다.

단계 **2** Signing Keys(서명 키) 페이지에서 **Clear All Keys(**모든 키 지우기**)**를 클릭합니다.

단계 **3** 삭제를 확인합니다.

DNS 텍스트 레코드 생성

단계 **1** **Mail Policies**(메일 정책) > **Signing Profiles**(서명 프로필)를 선택합니다.

단계 **2** Domain Signing Profiles(도메인 서명 프로필) 섹션의 DNS Text Record(DNS 텍스트 레코드) 열에서 해당 도메인 프로필에 대한 **Generate**(생성) 링크를 클릭합니다.

단계 **3** DNS 텍스트 레코드에 포함할 특성의 확인란을 선택합니다.

단계 **4** 변경한 내용으로 키를 다시 생성하려면 **Generate Again**(다시 생성)을 클릭합니다.

단계 **5** 창 하단의 텍스트 필드에 DNS 텍스트 레코드가 표시됩니다(여기에서 복사할 수 있음). 경우에 따라 다중 문자열 DNS 텍스트 레코드가 생성되기도 합니다. 다중 문자열 DNS 텍스트 레코드, 583 페이지를 참조하십시오.

단계 **6** **Done**(완료)을 클릭합니다.

다음에 수행할 작업

관련 주제

- 다중 문자열 DNS 텍스트 레코드, 583 페이지

다중 문자열 DNS 텍스트 레코드

DNS 텍스트 레코드 생성에 사용된 서명 키의 크기가 1024비트보다 크면 다중 문자열 DNS 텍스트 레코드가 생성됩니다. 이는 DNS 텍스트 레코드의 단일 문자열에서는 문자가 255개까지만 허용되기 때문입니다. 일부 DNS 서버에서는 다중 문자열 DNS 텍스트 레코드를 지원하지 않기 때문에 DKIM 인증이 실패할 수 있습니다.

이런 경우를 피하려면 큰따옴표를 사용해 다중 문자열 DNS 텍스트 레코드를 255바이트 이하의 더 작은 여러 문자열로 나누는 것이 좋습니다. 예를 들면 다음과 같습니다.

```
s._domainkey.domain.com. IN TXT "v=DKIM1;"
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQE"
"A4Vbhjq2n/3DbEk6EHdeVXlIXFT7OEl81amoZLbvwMX+bej"
"CdxcsFV3uS7G8oOJSWBP0z++nTQmy9ZDWfaiopU6k7tzoi"
"+oRDlKkhCQrM4oP2B2F5sTDkYwPY3Pen2jgC2OgbPnbo3o"
"m3c1wMWgSoZxoZUE4ly5kPuK9fTtpeJHNiZAqkFICiev4yrkL"
"R+SmFsJn9MYH5+lchyZ74BVm+16Xq2mptWXEwpiwOxWI"
"YHXsZo2zRjedrQ45vmgb8xUx5ioYY9/yBLHudGc+GUKTj1i4"
"mQg48yCD/HVNfsSRXaPinliEkypH9cSnvgvWuIYUQz0dHU;"
```

DKIM 구현 시 처리 전에, 이렇게 나뉜 DNS 텍스트 레코드가 원래의 전체 단일 문자열로 다시 조립됩니다.

도메인 프로필 테스트

서명 키를 만든 다음 도메인 프로파일과 연결하고 DNS 텍스트를 인증된 DNS에 삽입했으면 도메인 프로파일을 테스트할 수 있습니다.

단계 **1** **Mail Policies**(메일 정책) > **Signing Profiles**(서명 프로필)를 선택합니다.

단계 **2** **Domain Signing Profiles(**도메인 서명 프로필**)** 섹션의 Test Profile(프로필 테스트) 열에서 도메인 프로필에 대한 **Test(**테스트**)** 링크를 클릭합니다.

단계 **3** 성공 또는 실패를 나타내는 메시지가 페이지 상단에 표시됩니다. 테스트가 실패하면 오류 텍스트를 포함한 경고 메시지가 표시됩니다.

도메인 프로필 내보내기

내보내기를 수행하면 어플라이언스의 모든 도메인 프로필이 단일 텍스트 파일에 저장됩니다.

단계 **1** **Mail Policies(**메일 정책**) > Signing Profiles(**서명 프로필**)**를 선택합니다.

단계 **2** **Export Domain Profiles(**도메인 프로필 내보내기**)**를 클릭합니다.

단계 **3** 파일 이름을 입력하고 **Submit(**제출**)**을 클릭합니다.

도메인 프로필 가져오기

단계 **1** **Mail Policies(**메일 정책**) > Signing Profiles(**서명 프로필**)**를 선택합니다.

단계 **2** **Import Domain Profiles(**도메인 프로필 가져오기**)**를 클릭합니다.

단계 **3** 내보낸 도메인 프로필이 포함된 파일을 선택합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다. 가져오기를 수행하면 기존의 모든 도메인 프로필이 교체된다는 경고가 표시됩니다. 텍스트 파일의 모든 도메인 프로필을 가져오게 됩니다.

단계 **5** **Import(**가져오기**)**를 클릭합니다.

도메인 프로필 삭제

관련 주제

- 선택한 도메인 프로필 제거 , 584 페이지
- 모든 도메인 프로필 제거 , 585 페이지

선택한 도메인 프로필 제거

단계 **1** **Mail Policies(**메일 정책**) > Signing Profiles(**서명 프로필**)**를 선택합니다.

단계 **2** 제거할 각 도메인 프로필의 오른쪽에 있는 확인란을 선택합니다.

단계 **3** **Delete(**삭제**)**를 클릭합니다.

단계 **4** 삭제를 확인합니다.

모든 도메인 프로필 제거

단계 **1** **Mail Policies(**메일 정책**) > Signing Profiles(**서명 프로필**)**를 선택합니다.
단계 **2** **Clear All Profiles(**모든 프로필 지우기**)**를 클릭합니다.
단계 **3** 삭제를 확인합니다.

도메인 프로필 검색

단계 **1** **Mail Policies(**메일 정책**) > Signing Profiles(**서명 프로필**)**를 선택합니다.
단계 **2** Find Domain Profiles(도메인 프로필 찾기)에서 검색 용어를 지정합니다.
단계 **3** **Find Profiles(**프로필 찾기**)**를 클릭합니다.
단계 **4** 각 도메인 프로필에서 이메일, 도메인, 선택자 및 서명 키 이름 등의 필드가 검색됩니다.

참고 검색어를 입력하지 않으면 검색 엔진은 모든 도메인 프로필을 반환합니다.

DKIM 전역 설정 수정

DKIM 전역 설정을 사용하여 다음을 수행할지 여부를 선택할 수 있습니다.

- DKIM 서명으로 시스템 생성 메시지에 서명 어플라이언스는 다음 메시지에 서명합니다.
  - Cisco IronPort Spam Quarantine 알림
  - 콘텐츠 필터 생성 알림
  - 컨피그레이션 메시지
  - 지원 요청
- DKIM 서명에 From 헤더 사용

단계 **1** **Mail Policies(**메일 정책**) > Signing Profiles(**서명 프로필**)**를 선택합니다.
단계 **2** DKIM 전역 설정에서 **Edit Settings(**설정 수정**)**를 클릭합니다.
단계 **3** 요구 사항에 따라 다음 필드를 구성합니다.

- 시스템 생성 메시지의 DKIM 서명
- DKIM 서명에 From 헤더 사용

참고 DKIM 서명에 From 헤더를 사용하지 않거나 유효한 From 헤더가 누락된 경우 Sender 헤더가 사용됩니다. DKIM 서명된 메시지에 대한 DMARC 확인의 경우 DKIM 서명 중에 From 헤더를 사용해야 합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

DomainKeys 및 로깅

DomainKeys 서명 시 다음과 같은 줄이 메일 로그에 추가됩니다.

```
Tue Aug 28 15:29:30 2007 Info: MID 371 DomainKeys: signing with dk-profile - matches
user123@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DomainKeys: cannot sign - no profile matches
user12@example.com
```

DKIM 서명 시 다음과 같은 줄이 메일 로그에 추가됩니다.

```
Tue Aug 28 15:29:54 2007 Info: MID 372 DKIM: signing with dkim-profile - matches
user@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DKIM: cannot sign - no profile matches
user2@example.com
```

DKIM을 사용하여 수신 메시지를 확인하는 방법

DKIM을 사용하여 수신 메시지를 확인하는 방법

	수행해야 할 작업	추가 정보
1단계	DKIM을 사용하여 메시지를 확인하기 위한 프로필을 만듭니다.	DKIM 확인 프로필 만들기, 588 페이지
2단계	(선택 사항) DKIM을 사용하여 수신 메시지 확인에 사용할 사용자 지정 메일 플로우 정책을 만듭니다.	메일 플로우 정책을 사용하여 수신 메시지에 대한 규칙 정의, 108 페이지
3단계	DKIM을 사용하여 수신 메시지를 확인하기 위한 메일 플로우 정책을 구성합니다.	메일 플로우 정책에서 DKIM 확인 구성, 590 페이지
4단계	확인된 메시지에 대해 Email Security Appliance가 수행할 작업을 정의합니다.	DKIM 확인 메일에 대한 작업 구성, 591 페이지
5단계	작업을 특정 발신자 또는 수신자의 그룹과 연결합니다.	메일 정책 구성, 276 페이지

관련 주제

- AsyncOS에 의해 수행되는 DKIM 확인 검사, 587 페이지
- DKIM 확인 프로필 관리, 587 페이지
- 메일 플로우 정책에서 DKIM 확인 구성, 590 페이지
- DKIM 확인 메일에 대한 작업 구성, 591 페이지

AsyncOS에 의해 수행되는 DKIM 확인 검사

DKIM 확인을 위해 AsyncOS 어플라이언스를 구성할 때 다음과 같은 검사가 수행됩니다.

단계 **1** AsyncOS는 수신 메일에서 DKIM-Signature 필드, 서명 헤더의 구문, 유효한 태그 값 및 필요한 태그를 확인합니다. 서명이 이러한 검사에서 실패하면 AsyncOS는 *permfail*을 반환합니다.

단계 **2** 서명 검사가 수행된 후 공개 DNS 레코드에서 공개 키가 검색되고 TXT 레코드가 검증됩니다. 이 프로세스에서 오류가 발생하면 AsyncOS는 *permfail*을 반환합니다. 공개 키에 대한 DNS 쿼리가 응답을 받지 못하면 *tempfail*이 발생합니다.

단계 **3** 공개 키를 검색한 후 AsyncOS는 해시된 값을 검사하고 서명을 확인합니다. 이 단계에서 오류가 발생하면 AsyncOS는 *permfail*을 반환합니다.

단계 **4** 모든 검사를 통과하면 AsyncOS는 *pass*를 반환합니다.

참고 메시지 본문이 지정된 길이보다 크면 AsyncOS는 다음 판정을 반환합니다.

```
dkim = pass (partially verified [x bytes])
```

여기서 *X*는 확인된 바이트 수를 나타냅니다.

최종 확인 결과는 *Authentication-Results* 헤더로 입력됩니다. 예를 들면 다음 중 하나와 유사한 헤더가 표시될 수 있습니다.

```
Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=pass (signature verified)

Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=pass (partially verified [1000 bytes])

Authentication-Results: example1.com

header.from=From:user123@example.com; dkim=permfail (body hash did not verify)
```

참고 현재 DKIM 확인은 유효한 첫 번째 서명에서 중단됩니다. 마지막으로 발견된 서명을 사용하여 확인하는 것은 불가능합니다. 이 기능은 이후의 릴리스에서 지원될 수 있습니다.

도메인의 DNS TXT 레코드가 DKIM 테스트 모드(`t = y`)에 있는 경우, 어플라이언스는 DKIM 확인 및 작업을 완전히 건너뜁니다.

DKIM 확인 프로필 관리

DKIM 확인 프로필은 Email Security Appliance의 메일 플로우 정책이 DKIM 서명을 확인하는 데 사용하는 매개변수 목록입니다. 예를 들면 두 개의 확인 프로필을 만들 수 있습니다. 하나는 쿼리 시간 초과까지 30초를 허용하고, 다른 하나는 3초만 허용합니다. DDoS의 경우 연결 고갈을 방지하기 위한 Throttled 메일 플로우 정책에 두 번째 확인 프로필을 할당할 수 있습니다. 확인 프로필은 다음 정보로 구성됩니다.

- 확인 프로필의 이름.

- 가장 작은/가장 큰 허용되는 공개 키 크기. 기본 키 크기는 각각 512 및 2048입니다.
- 메시지에서 확인할 최대 서명 수. 메시지에 있는 서명이 정의된 최대값을 초과하면 어플라이언스는 나머지 서명의 확인을 건너뛰고 메시지를 계속 처리합니다. 기본 서명은 5개입니다.
- 발신자의 시스템 시간과 확인자의 시스템 시간 사이에 허용되는 최대값(초). 예를 들어 메시지 서명은 05:00:00에 만료되고 확인자의 시스템 시간은 05:00:30에 만료되는 경우, 허용되는 시간 차이가 60초이면 메시지 서명은 여전히 유효하지만 10초이면 유효하지 않습니다. 기본값은 60초입니다.
- 본문 길이 매개변수 사용 여부에 대한 옵션.
- 일시적인 장애 시 수행할 SMTP 작업.
- 영구적인 장애 시 수행할 SMTP 작업.

기존의 모든 확인 프로필을 프로필 이름으로 검색할 수 있습니다.

DKIM 확인 프로필을 어플라이언스 configuration 디렉터리의 텍스트 파일로서 내보낼 수 있습니다. 확인 프로필을 내보내면 현재 어플라이언스에 있는 모든 프로필이 단일 텍스트 파일에 추가됩니다. 자세한 내용은 DKIM 확인 프로필 내보내기, 589 페이지를 참조하십시오.

앞서 내보낸 DKIM 확인 프로필을 가져올 수 있습니다. DKIM 확인 프로필을 가져오면 시스템에 있는 모든 현재 DKIM 확인 프로필이 교체됩니다. 자세한 내용은 DKIM 확인 프로필 가져오기, 589 페이지을 참조하십시오.

관련 주제

- DKIM 확인 프로필 만들기, 588 페이지
- DKIM 확인 프로필 내보내기, 589 페이지
- DKIM 확인 프로필 가져오기, 589 페이지
- DKIM 확인 프로필 삭제, 589 페이지
- DKIM 확인 프로필 선택, 590 페이지

DKIM 확인 프로필 만들기

단계 **1** **Mail Policies**(메일 정책) > **Verification Profiles**(확인 프로필)를 클릭합니다.

단계 **2** **Add Profile**(프로필 추가)을 클릭합니다.

단계 **3** 프로필의 이름을 입력합니다.

단계 **4** 어플라이언스가 서명 키에 대해 수락할 최소 키 크기를 선택합니다.

단계 **5** 어플라이언스가 서명 키에 대해 수락할 최대 키 크기를 선택합니다.

단계 **6** 단일 메시지에서 확인할 최대 서명 수를 선택합니다. 서명 기본값은 5입니다.

단계 **7** 키 쿼리 시간 초과 값(초 단위)을 선택합니다. 기본값은 10초입니다.

단계 **8** 발신자의 시스템 시간과 확인자의 시스템 시간 사이에 허용되는 최대값(초)을 선택합니다. 기본값은 60초입니다.

단계 **9** 메시지를 확인하는 데 서명의 body-length 매개변수를 사용할지 여부를 선택합니다.

단계 **10** 서명을 확인할 때 일시적인 장애가 발생하는 경우 Email Security Appliance에서 메시지의 수락 여부를 선택합니다. 어플라이언스가 메시지를 거부하도록 하려면, 기본값인 451 SMTP 응답 코드 또는 또 다른 SMTP 응답 코드와 텍스트를 전송하도록 선택할 수 있습니다.

단계 **11** 서명을 확인할 때 영구적인 장애가 발생하는 경우 Email Security Appliance에서 메시지의 수락 여부를 선택합니다. 어플라이언스가 메시지를 거부하도록 하려면, 기본값인 451 SMTP 응답 코드 또는 또 다른 SMTP 응답 코드와 텍스트를 전송하도록 선택할 수 있습니다.

단계 **12** 변경 사항을 제출합니다.

DKIM Verification Profiles(DKIM 확인 프로필) 테이블에 새 프로필이 나타납니다.

단계 **13** 변경 사항을 커밋합니다.

단계 **14** 이제 수신 메일 플로우 정책에서 DKIM 확인을 활성화하고 사용할 확인 프로필을 선택해야 합니다.

DKIM 확인 프로필 내보내기

어플라이언스에서 DKIM 확인 프로필을 내보내면 어플라이언스의 configuration 디렉터리에 단일 파일로서 저장됩니다.

단계 **1** **Mail Policies(**메일 정책**) > Verification Profiles(**확인 프로필**)**를 선택합니다.

단계 **2** **Export Profiles(**프로필 내보내기**)**를 클릭합니다.

단계 **3** 파일 이름을 입력하고 **Submit(**제출**)**을 클릭합니다.

DKIM 확인 프로필 가져오기

단계 **1** **Mail Policies(**메일 정책**) > Verification Profiles(**확인 프로필**)**를 선택합니다.

단계 **2** **Import Profiles(**프로필 가져오기**)**를 클릭합니다.

단계 **3** DKIM 확인 프로필이 포함된 파일을 선택합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다. 가져오기를 수행하면 기존의 모든 DKIM 확인 프로필이 교체된다는 경고가 표시됩니다.

단계 **5** **Import(**가져오기**)**를 클릭합니다.

DKIM 확인 프로필 삭제

관련 주제

- 선택한 DKIM 확인 프로필 제거 , 589 페이지
- 모든 DKIM 확인 프로필 제거, 590 페이지

선택한 DKIM 확인 프로필 제거

단계 **1** **Mail Policies(**메일 정책**) > Verification Profiles(**확인 프로필**)**를 선택합니다.

단계 **2** 삭제할 각 DKIM 확인 프로필의 오른쪽에 있는 확인란을 선택합니다.

단계 **3** **Delete(**삭제**)**를 클릭합니다.
단계 **4** 삭제를 확인합니다.

모든 **DKIM** 확인 프로필 제거

단계 **1** **Mail Policies(**메일 정책**) > Verification Profiles(**확인 프로필**)**를 선택합니다.
단계 **2** **Clear All Profiles(**모든 프로필 지우기**)**를 클릭합니다.
단계 **3** 삭제를 확인합니다.

DKIM 확인 프로필 선택

모든 DKIM 확인 프로필에서 프로필 이름의 특정 용어를 검색하려면

단계 **1** **Mail Policies(**메일 정책**) > Verification Profiles(**확인 프로필**)**를 선택합니다.
단계 **2** **Search DKIM Verification Profiles(DKIM** 확인 프로필 검색**)** 섹션에서 검색어를 지정합니다.
단계 **3** **Find Profiles(**프로필 찾기**)**를 클릭합니다.

각 DKIM 확인 프로필에 대한 프로필 이름이 검색됩니다.

검색어를 입력하지 않으면 검색 엔진은 모든 DKIM 확인 프로필을 반환합니다.

메일 플로우 정책에서 **DKIM** 확인 구성

수신 이메일에 대한 메일 플로우 정책에서 DKIM 확인이 활성화됩니다.

단계 **1** **Mail Policies(**메일 정책**) > Mail Flow Policies(**메일 플로우 정책**)**를 선택합니다.
단계 **2** 확인을 수행할 리스너에 대한 수신 메일 정책을 클릭합니다.
단계 **3** 메일 플로우 정책의 Security Features(보안 기능) 섹션에서 **On(**켜기**)**을 선택하여 DKIM Verification(DKIM 확인)을 활성화합니다.
단계 **4** 정책에 사용할 DKIM 확인 프로필을 선택합니다.
단계 **5** 변경 사항을 커밋합니다.

다음에 수행할 작업

관련 주제

- DKIM 확인 및 로깅, 591 페이지

DKIM 확인 및 로깅

DKIM 확인 시 다음과 같은 줄이 메일 로그에 추가됩니다.

```
mail.current:Mon Aug 6 13:35:38 2007 Info: MID 17 DKIM: no signature

mail.current:Mon Aug 6 15:00:37 2007 Info: MID 18 DKIM: verified pass
```

DKIM 확인 메일에 대한 작업 구성

DKIM 메일을 확인하면 *Authentication-Results* 헤더가 메일에 추가되지만, 인증 결과와 상관없이 메일이 수락됩니다. 이러한 인증 결과를 기반으로 작업을 구성하려면 DKIM 인증 메일에서 작업을 수행하기 위한 콘텐츠 필터를 만들 수 있습니다. 예를 들어 DKIM 확인이 실패할 경우 메일을 전달하거나 반송하거나 삭제하거나 격리로 보내도록 구성할 수 있습니다. 이렇게 하려면 콘텐츠 필터를 사용하여 작업을 구성해야 합니다.

단계 **1** **Mail Policies(**메일정책**) > Incoming Content Filters(**수신 콘텐츠 필터**)**를 선택합니다.

단계 **2** **Add Filter(**필터 추가**)**를 클릭합니다.

단계 **3** Conditions(조건) 섹션에서 **Add Condition(**조건 추가**)**을 클릭합니다.

단계 **4** 조건 목록에서 **DKIM Authentication(DKIM** 인증**)**을 선택합니다.

단계 **5** DKIM 조건을 선택합니다. 다음 옵션 중 하나를 선택합니다.

- **Pass.** 메시지가 인증 테스트를 통과함.
- Neutral. 인증이 수행되지 않음.
- **Temperror**. 복구 가능한 오류가 발생함.
- **Permerror**. 복구할 수 없는 오류가 발생함.
- **Hardfail**. 인증 테스트에 실패함.
- **None**. 메시지가 서명되지 않음.

단계 **6** 조건과 연결할 작업을 선택합니다. 예를 들어 DKIM 검사가 실패할 경우 수신자에게 알리고 메시지를 반송할 수 있습니다. 또는 DKIM 검사에 통과할 경우 추가 처리 없이 메시지를 즉시 전달할 수 있습니다.

단계 **7** 새 콘텐츠 필터를 제출합니다.

단계 **8** 적절한 수신 메일 정책에서 콘텐츠 필터를 활성화합니다.

단계 **9** 변경사항을 커밋합니다.

SPF 및 SIDF 확인 개요

AsyncOS는 SPF(Sender Policy Framework) 및 SIDF(Sender ID Framework) 확인을 지원합니다. SPF 및 SIDF는 DNS 레코드를 기반으로 이메일의 신뢰성을 확인하기 위한 방법입니다. SPF 및 SIDF에서 인터넷 도메인 소유자는 특수 형식의 DNS TXT 레코드를 사용하여, 해당 도메인에 대한 이메일을 전송

하도록 인증된 시스템을 지정할 수 있습니다. 호환 메일 수신자는 게시된 SPF 레코드를 사용하여 메일 트랜잭션 과정에서 전송 MTA(Mail Transfer Agent) ID의 인증을 테스트합니다.

SPF/SIDF 인증을 사용할 경우 발신자는 자신의 이름을 사용하도록 허락할 호스트를 지정하는 SPF 레코드를 게시하고, 호환 메일 수신자는 게시된 SPF 레코드를 사용하여 메일 트랜잭션 과정에서 전송 MTA(Mail Transfer Agent) ID의 인증을 테스트합니다.

참고 SPF에는 구문 분석 및 평가가 필요하므로 AsyncOS 성능이 저하될 수 있습니다. 또한 SPF 점검으로 인해 DNS 인프라의 로드가 증가한다는 점에도 유의하십시오.

SPF 및 SIDF로 작업할 때 SIDF는 SPF와 비슷하지만 약간 다릅니다. SIDF와 SPF의 차이점에 대해 자세히 알아보려면 RFC 4406을 참조하십시오. 이 문서에서는 한 가지 확인 유형만 적용되는 경우를 제외하고는 두 가지 용어를 함께 사용합니다.

참고 AsyncOS는 수신 지연에 대해 SPF를 지원하지 않습니다.

관련 주제

- 유효한 SPF 레코드에 대한 참고 사항, 592 페이지

유효한 SPF 레코드에 대한 참고 사항

어플라이언스에서 SPF 및 SIDF를 사용하려면 RFC 4406, 4408 및 7208에 따라 SPF 레코드를 게시하십시오. PRA ID가 확인되는 방법의 정의에 대해서는 RFC 4407을 검토하십시오. 또한 SPF 및 SIDF 레코드를 만들 때 일반적으로 어떤 실수를 하는지 알아보려면 다음 웹사이트를 참조할 수 있습니다.

http://www.openspf.org/FAQ/Common_mistakes

관련 주제

- 유효한 SPF 레코드, 592 페이지
- 유효한 SIDF 레코드, 593 페이지
- SPF 레코드 테스트, 593 페이지

유효한 SPF 레코드

SPF HELO 검사를 통과하려면 각각의 전송 MTA(도메인과는 별도)에 대해 "v=spf1 a –all" SPF 레코드를 포함해야 합니다. 이 레코드를 포함하지 않으면 HELO 검사에서 HELO ID에 대해 None 판정이 나올 수 있습니다. 도메인에 대한 SPF 발신자 중 다수가 None 판정을 반환한다면 이들은 각 전송 MTA에 대해 "v=spf1 a –all" SPF 레코드를 포함하지 않았을 수 있습니다.

유효한 SIDF 레코드

SIDF 프레임워크를 지원하려면 "v=spf1" 및 "spf2.0" 레코드를 모두 게시해야 합니다. 예를 들어 DNS 레코드는 다음과 같이 보일 수 있습니다.

```
example.com. TXT "v=spf1 +mx a:colo.example.com/28 -all"

smtp-out.example.com TXT "v=spf1 a -all"

example.com. TXT "spf2.0/mfrom,pra +mx a:colo.example.com/28 -all"
```

SIDF는 HELO ID를 확인하지 않으므로 이 경우 각각의 전송 MTA에 대해 SPF v2.0 레코드를 게시할 필요가 없습니다.

참고 SIDF를 지원하지 않도록 선택하는 경우 "spf2.0/pra ~all" 레코드를 게시하십시오.

SPF 레코드 테스트

RFC를 검토하는 것 외에도 Email Security Appliance에서 SPF 확인을 구현하기 전에 SPF 레코드를 테스트하는 것이 좋습니다. 몇 가지 사용 가능한 툴을 openspf.org 웹사이트에서 제공합니다.

http://www.openspf.org/Tools

다음 툴을 사용하여 SPF 레코드 확인에서 이메일이 실패한 이유를 알아볼 수 있습니다.

http://www.openspf.org/Why

또한 테스트 리스너에서 SPF를 활성화하고 Cisco의 trace CLI 명령을 사용하여(또는 GUI에서 추적을 수행하여) SPF 결과를 볼 수 있습니다. 추적을 사용하면 서로 다른 전송 IP를 손쉽게 테스트할 수 있습니다.

SPF/SDIF를 사용하여 수신 메시지를 확인하는 방법

	수행해야 할 작업	추가 정보
1단계	(선택 사항) SPF/SDIF를 사용하여 수신 메시지 확인에 사용할 맞춤형 메일 플로우 정책을 만듭니다.	메일 플로우 정책을 사용하여 수신 메시지에 대한 규칙 정의, 108 페이지
2단계	SPF/SDIF를 사용하여 수신 메시지를 확인하기 위한 메일 플로우 정책을 구성합니다.	SPF 및 SIDF 활성화, 594 페이지
3단계	확인된 메시지에 대해 Email Security Appliance가 수행할 작업을 정의합니다.	SPF/SIDF 확인 메일에 대해 수행할 작업 결정, 598 페이지
4단계	작업을 특정 발신자 또는 수신자의 그룹과 연결합니다.	메일 정책 구성, 276 페이지
5단계	(선택 사항) 메시지 확인 결과를 테스트합니다.	SPF/SIDF 결과 테스트, 601 페이지

주의 Cisco는 전역적으로 이메일 인증을 보증하지만, 현재 업계 채택 상황을 고려하여 Cisco는 SPF/SIDF 인증 실패에 신중하게 대처할 것을 제안합니다. 더 많은 조직이 인증된 메일 전송 인프라를 더 잘 제어하게 될 때까지 Cisco는 이메일 반송을 피하고 대신 SPF/SIDF 확인에 실패하는 메일을 격리하도록 권장합니다.

참고 AsyncOS CLI(command line interface)는 웹 인터페이스보다 SPF 레벨에 대해 더 많은 제어 설정을 제공합니다. SPF 판정을 기반으로, 어플라이언스는 SMTP 대화에서 리스너 단위로 메시지를 수락 또는 거부할 수 있습니다. listenerconfig 명령을 사용하여 리스너의 Host Access Table에 대한 기본 설정을 수정할 때 SPF 설정을 수정할 수 있습니다. 설정에 대한 자세한 내용은 CLI를 통해 SPF 및 SIDF 활성화, 595 페이지 섹션을 참조하십시오.

SPF 및 SIDF 활성화

SPF/SIDF를 사용하려면 수신 리스너에서 메일 플로우 정책에 대해 SPF/SIDF를 활성화해야 합니다. 기본 메일 플로우 정책에서 리스너에 대해 SPF/SIDF를 활성화할 수도 있고, 특정 수신 메일 플로우 정책에 대해 활성화할 수도 있습니다.

단계 **1** **Mail Policies(**메일 정책**) > Mail Flow Policy(**메일 플로우 정책**)**를 선택합니다.

단계 **2** **Default Policy Parameters(**기본 정책 매개변수**)**를 클릭합니다.

단계 **3** 기본 정책 매개변수에서 Security Features(보안 기능) 섹션으로 이동합니다.

단계 **4** **SPF/SIDF Verification(SPF/SIDF** 확인**)** 섹션에서 **On(**켜기**)**을 클릭합니다.

단계 **5** 적합성 레벨을 설정합니다(기본값은 SIDF-compatible). 이 옵션을 사용하면 어떤 SPF 또는 SIDF 확인의 표준을 사용할지를 결정할 수 있습니다. SIDF 적합성 외에, SPF와 SIDF를 결합하는 SIDF-compatible을 선택할 수 있습니다.

SPF/SIDF 적합성 레벨

적합성 레벨	설명
SPF	SPF/SIDF 확인은 RFC4408 및 RFC7208에 따라 작동합니다. - PRA(purported responsible address) ID 확인이 발생하지 않습니다. 참고: HELO ID를 기준으로 테스트하려면 이 적합성 옵션을 선택하십시오.
SIDF	SPF/SIDF 확인은 RFC4406에 따라 작동합니다. - 표준에 대한 완전한 적합성과 함께 PRA ID가 결정됩니다. - SPF v1.0 레코드는 spf2.0/mfrom,pra로 취급됩니다. - 도메인이 존재하지 않거나 ID 형식이 잘못된 경우 Fail 판정이 반환됩니다.

적합성 레벨	설명
SIDF Compatible(SIDF 호환)	다음의 차이를 제외하면 SPF/SIDF 확인은 RFC4406에 따라 작동합니다. - SPF v1.0 레코드는 spf2.0/mfrom으로 취급됩니다. - 도메인이 존재하지 않거나 ID 형식이 잘못된 경우 None 판정이 반환됩니다. 참고: 이 적합성 옵션은 OpenSPF 커뮤니티(www.openspf.org)의 요청으로 도입되었습니다.

참고 CLI를 통해 더 많은 설정을 사용할 수 있습니다. 자세한 내용은 CLI를 통해 SPF 및 SIDF 활성화, 595 페이지를 참조하십시오.

단계 **6** SIDF Compatible(SIDF 호환)의 적합성 레벨을 선택할 때, 메시지에 Resent-Sender: 또는 Resent-From: 헤더가 있을 경우 확인에서 PRA ID의 Pass 결과를 None으로 다운그레이드할지 여부를 구성합니다. 보안을 위해 이 옵션을 선택할 수 있습니다.

단계 **7** SPF의 적합성 레벨을 선택하는 경우, HELO ID를 기준으로 테스트를 수행할지 여부를 구성합니다. HELO 검사를 비활성화하여 성능을 높이려면 이 옵션을 사용할 수 있습니다. spf-passed 필터 규칙은 PRA 또는 MAIL FROM ID를 먼저 검사하므로 이 옵션은 유용할 수 있습니다. 어플라이언스는 SPF 적합성 레벨에 대해 HELO 검사만 수행합니다.

다음에 수행할 작업

관련 주제

- Received-SPF 헤더, 598 페이지
- CLI를 통해 SPF 및 SIDF 활성화, 595 페이지

CLI를 통해 SPF 및 SIDF 활성화

AsyncOS CLI는 각 SPF/SIDF 적합성 레벨에 대한 더 많은 설정을 지원합니다. 리스너의 Host Access Table에 대해 기본 설정을 구성할 경우, SPF/SIDF 확인 결과를 기반으로 어플라이언스가 수행할 리스너의 SPF/SIDF 적합성 레벨 및 SMTP 작업(ACCEPT 또는 REJECT)을 선택할 수 있습니다. 또한 어플라이언스가 메시지 거부 시 전송하는 SMTP 응답을 정의할 수 있습니다.

적합성 레벨에 따라 어플라이언스는 HELO ID, MAIL FROM ID 또는 PRA ID에 대한 검사를 수행합니다. 각 ID 검사에 대한 다음 SPF/SIDF 확인 결과에 따라 어플라이언스가 세션을 계속 진행할지(ACCEPT) 또는 세션을 끝낼지(REJECT)를 지정할 수 있습니다.

- **None(없음).** 정보가 부족해 확인을 수행할 수 없습니다.
- **Neutral.** 클라이언트가 특정 ID를 사용하도록 승인되었는지 여부를 도메인 소유자가 주장하지 않습니다.
- **SoftFail.** 도메인 소유자는 호스트가 특정 ID를 사용하도록 승인되지 않았다고 믿고 있지만 이를 확고하게 밝히지 않습니다.

- **Fail.** 클라이언트가 특정 ID를 사용하도록 승인되지 않았습니다.
- **TempError.** 확인 중에 일시적인 오류가 발생했습니다.
- **PermError.** 확인 중에 영구적인 오류가 발생했습니다.

메시지에 Resent-Sender: 또는 Resent-From: 헤더가 있을 경우, PRA ID의 Pass 결과를 None으로 다운그레이드하도록 SIDF Compatible 적합성 레벨을 구성하지 않는 한 어플라이언스는 Pass 결과의 메시지를 수락합니다. 그런 다음 어플라이언스는 PRA 검사가 None을 반환할 경우에 대해 지정된 SMTP 작업을 수행합니다.

ID 검사에 대한 SMTP 작업을 정의하지 않는 경우 어플라이언스는 Fail을 비롯한 모든 확인 결과를 자동으로 수락합니다.

활성화된 ID 검사에 대해 ID 확인 결과가 REJECT 작업과 일치하는 경우 어플라이언스는 세션을 종료합니다. 예를 들어 관리자는 Fail을 포함하여 HELO ID 확인 결과를 기반으로 메시지를 수신하되, MAIL FROM ID 확인에서 Fail 결과를 받은 메시지는 거부하도록 리스너를 구성합니다. 메시지가 HELO ID 확인에 실패하면 어플라이언스가 해당 결과를 수락하므로 세션이 계속 진행됩니다. 그런 다음 메시지가 MAIL FROM ID 확인에서 실패하면 리스너는 세션을 종료하고 REJECT 작업에 대한 STMP 응답을 반환합니다.

SMTP 응답은 SPF/SIDF 확인 결과를 기반으로 메시지를 거부할 때 어플라이언스가 반환하는 코드 번호 및 메시지입니다. TempError 결과는 기타 확인 결과와 다른 SMTP 응답을 반환합니다. TempError의 경우 결과 응답 코드는 451이고 기본 메시지 텍스트는 `#4.4.3 Temporary error occurred during SPF verification`입니다. 다른 모든 확인 결과의 경우 기본 응답 코드는 550이고 기본 메시지 텍스트는 `#5.7.1 SPF unauthorized mail is prohibited`입니다. TempError 및 기타 확인 결과에 대해 고유한 응답 코드 및 메시지 텍스트를 지정할 수 있습니다.

선택적으로, Neutral, SoftFail 또는 Fail 확인 결과에 대해 REJECT 작업을 수행하는 경우 SPF 게시자 도메인에서 서드파티 응답을 반환하도록 어플라이언스를 구성할 수 있습니다. 기본적으로 어플라이언스는 다음 응답을 반환합니다.

```
550-#5.7.1 SPF unauthorized mail is prohibited.

550-The domain example.com explains:

550 <Response text from SPF domain publisher>
```

이러한 SPF/SIDF 설정을 사용하려면 `listenerconfig -> edit` 하위 명령을 사용하고 리스너를 선택합니다. 그런 다음 `hostaccess -> default` 하위 명령을 사용하여 Host Access Table의 기본 설정을 수정합니다.

Host Access Table에 대해 다음 SPF 제어 설정을 사용할 수 있습니다.

CLI를 통해 SPF 제어 설정

적합성 레벨	사용 가능한 **SPF** 제어 설정

SPF 전용	• HELO ID 검사 수행 여부
	• 다음 ID 검사의 결과를 기반으로 수행되는 SMTP 작업
	  • HELO identity (if enabled)
	  • MAIL FROM Identity
	• REJECT 작업에 대해 반환된 SMTP 응답 코드 및 텍스트
	• 확인 시간 초과(초)

SIDF Compatible(SIDF 호환)	• HELO ID 검사 수행 여부
	• 메시지에 Resent-Sender: 또는 Resent-From: 헤더가 있을 경우 확인에서 PRA ID의 Pass 결과를 None으로 다운그레이드할지 여부
	• 다음 ID 검사의 결과를 기반으로 수행되는 SMTP 작업
	  • HELO identity (if enabled)
	  • MAIL FROM Identity
	  • PRA Identity
	• REJECT 작업에 대해 반환된 SMTP 응답 코드 및 텍스트
	• 확인 시간 초과(초)

SIDF Strict	• 다음 ID 검사의 결과를 기반으로 수행되는 SMTP 작업
	  • MAIL FROM Identity
	  • PRA Identity
	• SPF REJECT 작업의 경우 반환된 SMTP 응답 코드 및 텍스트
	• 확인 시간 초과(초)

어플라이언스는 HELO ID 검사를 수행하고, None 및 Neutral 확인 결과는 수락하고 나머지는 거부합니다. SMTP 작업에 대한 CLI 프롬프트는 모든 ID 유형에 대해 동일합니다. 사용자는 MAIL FROM ID에 대한 SMTP 작업을 정의하지 않습니다. 어플라이언스는 ID에 대한 모든 확인 결과를 자동으로 수락합니다. 어플라이언스는 모든 REJECT 결과에 대한 기본 거부 코드 및 텍스트를 사용합니다.

CLI에서 `listenerconfig` 명령을 사용하여 이를 구성할 수도 있습니다.

Received-SPF 헤더

SPF/SIDF 확인을 위해 AsyncOS를 구성하면 SPF/SIDF 확인 헤더(`Received-SPF`)가 이메일에 추가됩니다. `Received-SPF` 헤더에는 다음 정보가 포함됩니다.

- 확인 결과 - SPF 확인 결과(확인 결과, 599 페이지 참조).
- **ID** - SPF 확인에서 검사한 ID: HELO, MAIL FROM 또는 PRA.
- **receiver** - 검사를 수행하는 확인 호스트 이름
- 클라이언트 **IP** 주소 - SMTP 클라이언트의 IP 주소.
- **ENVELOPE FROM** - 봉투 발신자 사서함. (MAIL FROM ID는 비워둘 수 없으므로 이는 MAIL FROM ID와 다를 수 있습니다.)
- **x-sender** - HELO, MAIL FROM 또는 PRA ID의 값.
- **x-conformance** - 적합성 수준(표 - *SPF/SIDF* 적합성 수준 참고) 및 PRA 검사의 다운그레이드가 수행되었는지 여부.

다음 예는 SPF/SIDF 검사를 전달한 메시지에 대해 추가된 헤더를 보여줍니다.

```
Received-SPF: Pass identity=pra; receiver=box.example.com;

client-ip=1.2.3.4; envelope-from="alice@fooo.com";

x-sender="alice@company.com"; x-conformance=sidf_compatible
```

참고 `spf-status` 및 `spf-passed` 필터 규칙은 received-SPF 헤더를 사용하여 SPF/SIDF 확인의 상태를 결정합니다.

SPF/SIDF 확인 메일에 대해 수행할 작업 결정

SPF/SIDF 확인 메일을 받는 경우 SPF/SIDF 확인 결과에 따라 다른 작업을 수행할 수 있습니다. 다음 메시지 및 콘텐츠 필터 규칙을 사용하여 SPF/SIDF 확인 메일의 상태를 확인하고, 확인 결과를 기반으로 메시지에 대해 작업을 수행할 수 있습니다.

- `spf-status`. 이 필터 규칙은 SPF/SIDF 상태를 기반으로 작업을 결정합니다. 각각의 유효한 SPF/SIDF 반환 값에 대해 서로 다른 작업을 입력할 수 있습니다.
- `spf-passed`. 이 필터 규칙은 SPF/SIDF 결과를 부울 값으로 생성합니다.

참고 `spf-passed` 필터 규칙은 메시지 필터에서만 사용 가능합니다.

세부 결과를 더 많이 확인하려면 `spf-status` 규칙을 사용하고, 단순한 부울을 만들려면 spf-passed 규칙을 사용할 수 있습니다.

관련 주제

- 확인 결과, 599 페이지
- CLI에서 spf-status 필터 규칙 사용, 599 페이지
- GUI의 spf-status 콘텐츠 필터 규칙, 601 페이지
- spf-passed 필터 규칙 사용, 601 페이지

확인 결과

`spf-status` 필터 규칙을 사용하는 경우 다음 구문을 사용하여 SPF/SIDF 확인 결과에 대해 검사할 수 있습니다.

```
if (spf-status == "Pass")
```

여러 상태 판정에 대해 단일 조건을 검토하려면 다음 구문을 사용할 수 있습니다.

```
if (spf-status == "PermError, TempError")
```

또한 다음 구문을 사용하여 HELO, MAIL FROM 및 PRA ID에 대해 확인 결과를 검사할 수 있습니다.

```
if (spf-status("pra") == "Fail")
```

참고 HELO, MAIL FROM 및 PRA ID에 대해 결과를 검사하려면 `spf-status` 메시지 필터 규칙만 사용할 수 있습니다. ID에 대해 검사하려면 `spf-status` 콘텐츠 필터 규칙을 사용할 수 없습니다. `spf-status` 콘텐츠 필터는 PRA ID만 검사합니다.

다음 확인 결과 중 하나를 수신할 수 있습니다.

- None - 정보가 부족해 확인을 수행할 수 없습니다.
- Pass - 클라이언트가 특정 ID를 사용하도록 승인되었습니다.
- Neutral - 클라이언트가 특정 ID를 사용하도록 승인되었는지 여부를 도메인 소유자가 주장하지 않습니다.
- SoftFail - 도메인 소유자는 호스트가 특정 ID를 사용하도록 승인되지 않았다고 믿고 있지만 이를 확고하게 밝히지 않습니다.
- Fail - 클라이언트가 특정 ID를 사용하도록 승인되지 않았습니다.
- TempError - 확인 중에 일시적인 오류가 발생했습니다.
- PermError - 확인 중에 영구적인 오류가 발생했습니다.

CLI에서 spf-status 필터 규칙 사용

다음 예는 사용 중인 `spf-status` 메시지 필터를 보여줍니다.

```
skip-spam-check-for-verified-senders:

if (sendergroup == "TRUSTED" and spf-status == "Pass"){
```

```
skip-spamcheck();
}
quarantine-spf-failed-mail:
if (spf-status("pra") == "Fail") {
if (spf-status("mailfrom") == "Fail"){
# completely malicious mail
quarantine("Policy");
} else {
if(spf-status("mailfrom") == "SoftFail") {
# malicious mail, but tempting
quarantine("Policy");
}
}
} else {
if(spf-status("pra") == "SoftFail"){
if (spf-status("mailfrom") == "Fail"
or spf-status("mailfrom") == "SoftFail"){
# malicious mail, but tempting
quarantine("Policy");
}
}
}
stamp-mail-with-spf-verification-error:
if (spf-status("pra") == "PermError, TempError"
or spf-status("mailfrom") == "PermError, TempError"
or spf-status("helo") == "PermError, TempError"){
# permanent error - stamp message subject
strip-header("Subject");
insert-header("Subject", "[POTENTIAL PHISHING] $Subject");
}
.
```

GUI의 spf-status 콘텐츠 필터 규칙

GUI에서 콘텐츠 필터로부터 spf-status 규칙을 활성화할 수도 있습니다. 그러나 spf-status 콘텐츠 필터 규칙을 사용할 경우에는 HELO, MAIL FROM 및 PRA ID에 대해 결과를 검사할 수 없습니다.

GUI에서 spf-status 콘텐츠 필터 규칙을 추가하려면 **Mail Policies(**메일 정책**)** > **Incoming Content Filters(**수신 콘텐츠 필터**)**를 클릭합니다. 그런 다음 Add Condition(조건 추가) 대화 상자에서 SPF Verification(SPF 확인) 필터 규칙을 추가합니다. 조건에 대해 하나 이상의 검사 결과를 지정합니다.

SPF Verification(SPF 확인) 조건을 추가한 후 SPF 상태를 기반으로 수행할 작업을 지정합니다. 예를 들어 SPF 상태가 SoftFail인 경우 메시지를 격리할 수 있습니다.

spf-passed 필터 규칙 사용

`spf-passed` 규칙은 SPF 확인의 결과를 부울 값으로 보여줍니다. 다음 예는 `spf-passed`로 표시되지 않은 이메일을 격리하는 데 사용되는 `spf-passed` 규칙을 보여줍니다.

```
quarantine-spf-unauthorized-mail:

if (not spf-passed) {


quarantine("Policy");

}
```

참고 `spf-status` 규칙과 달리 `spf-passed` 규칙은 SPF/SIDF 확인 값을 단순한 부울로 줄입니다. None, Neutral, Softfail, TempError, PermError 및 Fail 확인 결과는 `spf-passed` 규칙으로 전달되지 않은 것으로 취급됩니다. 좀 더 세부적인 결과를 기반으로 메시지에 대해 작업을 수행하려면 `spf-status` 규칙을 사용하십시오.

SPF/SIDF 결과 테스트

SPF/SIDF 확인의 결과를 테스트하고 SPF/SIDF 실패를 처리하는 방법을 결정합니다. 각 조직에서 SPF/SIDF를 서로 다른 방식으로 구현하기 때문입니다. SPF/SIDF 확인 결과를 테스트하려면 콘텐츠 필터, 메시지 필터, Email Security Monitor - Content Filters(이메일 보안 모니터 - 콘텐츠 필터) 보고서를 조합하여 사용합니다.

SPF/SIDF 확인에 대한 의존도가 SPF/SIDF 결과를 테스트하는 세분화의 레벨을 결정합니다.

관련 주제

- SPF/SIDF 결과의 기본 세분화 테스트, 602 페이지
- SPF/SIDF 결과의 더 큰 세분화 테스트, 602 페이지

SPF/SIDF 결과의 기본 세분화 테스트

수신 메일에 대한 SPF/SIDF 확인 결과의 기본 측정치를 가져오려면 콘텐츠 필터 및 Email Security Monitor - Content Filters(이메일 보안 모니터 - 콘텐츠 필터) 페이지를 사용할 수 있습니다. 이 테스트는 각 SPF/SIDF 확인 결과 유형에 대해 수신된 메시지 수의 보기를 제공합니다.

단계 **1** 수신 리스너에서 메일 플로우 정책에 대한 SPF/SIDF 확인을 활성화하고, 콘텐츠 필터를 사용하여 수행할 작업을 구성합니다. SPF/SIDF 활성화에 대한 자세한 내용은 SPF 및 SIDF 활성화, 594 페이지 섹션을 참조하십시오.

단계 **2** 각 SPF/SIDF 확인 유형에 대해 **spf-status** 콘텐츠 필터를 만듭니다. 확인 유형을 나타내는 명명 규칙을 사용합니다. 예를 들면 SPF/SIDF 확인을 통과한 메시지에는 "SPF-Passed"를 사용하고, 확인 중 일시적인 오류 때문에 통과하지 못한 메시지에는 "SPF-TempErr"을 사용합니다. **spf-status** 콘텐츠 필터 만들기에 대한 자세한 내용은 GUI의 spf-status 콘텐츠 필터 규칙, 601 페이지 섹션을 참조하십시오.

단계 **3** 여러 SPF/SIDF 확인 메시지를 처리한 후 **Monitor(모니터) > Content Filters(콘텐츠 필터)**를 클릭하여 각 SPF/SIDF 확인 콘텐츠 필터를 트리거한 메시지 수를 확인합니다.

SPF/SIDF 결과의 더 큰 세분화 테스트

SPF/SIDF 확인 결과에 대한 정보가 더 포괄적일수록, 특정 발신자 그룹에 대해서만 SPF/SIDF 확인을 활성화하고, 해당 특정 발신자에 대한 결과를 검토합니다. 그런 다음 해당 특정 그룹에 대한 메일 정책을 만들고 이에 대해 SPF/SIDF 확인을 활성화합니다. SPF/SIDF 결과의 기본 세분화 테스트, 602 페이지에 설명된 대로 콘텐츠 필터를 만들고 콘텐츠 필터 보고서를 검토합니다. 확인이 효과적인 것으로 판단되면, 지정된 발신자 그룹에 대한 이메일을 삭제할지 아니면 반송할지를 결정하기 위한 기반으로 SPF/SIDF 확인을 사용할 수 있습니다.

단계 **1** SPF/SIDF 확인에 대한 메일 플로우 정책을 만듭니다. 수신 리스너에서 메일 플로우 정책에 대한 SPF/SIDF 확인을 활성화합니다. SPF/SIDF 활성화에 대한 자세한 내용은 SPF 및 SIDF 활성화, 594 페이지 섹션을 참조하십시오.

단계 **2** SPF/SIDF 확인을 위한 발신자 그룹을 만들고 SPF/SIDF 확인을 나타내는 명명 규칙을 사용합니다. 발신자 그룹 만들기에 대한 자세한 내용은 "이메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

단계 **3** 각 SPF/SIDF 확인 유형에 대해 **spf-status** 콘텐츠 필터를 만듭니다. 확인 유형을 나타내는 명명 규칙을 사용합니다. 예를 들면 SPF/SIDF 확인을 통과한 메시지에는 "SPF-Passed"를 사용하고, 확인 중 일시적인 오류 때문에 통과하지 못한 메시지에는 "SPF-TempErr"을 사용합니다. **spf-status** 콘텐츠 필터 만들기에 대한 자세한 내용은 GUI의 spf-status 콘텐츠 필터 규칙, 601 페이지 섹션을 참조하십시오.

단계 **4** 여러 SPF/SIDF 확인 메시지를 처리한 후 **Monitor(모니터) > Content Filters(콘텐츠 필터)**를 클릭하여 각 SPF/SIDF 확인 콘텐츠 필터를 트리거한 메시지 수를 확인합니다.

DMARC 확인

DMARC(Domain-based Message Authentication, Reporting and Conformance)는 이메일 기반 남용의 가능성을 줄이기 위해 만든 기술 사양입니다. DMARC는 이메일 수신자가 SPF 및 DKIM 메커니즘을 사

용하여 이메일 인증을 수행하는 방법을 표준화합니다. DMARC 확인을 통과하려면 이메일이 이러한 인증 메커니즘 중 하나 이상을 통과해야 하며 인증 식별자가 RFC 5322를 준수해야 합니다.

Email Security Appliance에서는 다음 작업을 수행할 수 있습니다.

- DMARC를 사용하여 수신 이메일 확인
- 도메인 소유자 정책을 재정의(수락, 격리 또는 거부)할 프로필 정의
- 인증 구축을 강화하는 데 도움이 되는 피드백 보고서를 도메인 소유자에게 전송
- DMARC 집계 보고서 크기가 10MB 또는 DMARC 레코드의 RUA 태그에 지정된 크기를 초과하는 경우 도메인 소유자에게 전달 오류 보고서 전송

AsyncOS는 2013년 3월 31일 IETF(Internet Engineering Task Force)에 제출된 DMARC 사양을 따르는 이메일을 처리할 수 있습니다. 자세한 내용은 http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02를 참조하십시오.

참고 Email Security Appliance는 DMARC 레코드의 형식이 잘못된 도메인에서 보낸 메시지의 DMARC 확인을 수행하지 않습니다. 그러나 이 어플라이언스에서 그러한 메시지를 수신하고 처리할 수는 있습니다.

관련 주제

- DMARC 확인 워크플로, 603 페이지
- DMARC를 사용하여 수신 메시지를 확인하는 방법, 604 페이지

DMARC 확인 워크플로

다음은 AsyncOS에서 DMARC 확인을 수행하는 방법에 대한 설명입니다.

1. AsyncOS에 구성된 리스너가 SMTP 연결을 수신합니다.
2. AsyncOS는 메시지에 대해 SPF 및 DKIM 확인을 수행합니다.
3. AsyncOS는 DNS에서 발신자 도메인에 대한 DMARC 레코드를 가져옵니다.
   - 레코드가 발견되지 않으면 AsyncOS는 DMARC 확인을 건너뛰고 계속 처리를 진행합니다.
   - DNS 조회에 실패하면 AsyncOS는 지정된 DMARC 확인 프로필을 기준으로 작업을 수행합니다.
4. DKIM 및 SPF 확인 결과에 따라 AsyncOS는 메시지에 대해 DMARC 확인을 수행합니다.

참고 DKIM 및 SPF 확인이 활성화된 경우, DMARC 확인은 DKIM 및 SPF 확인 결과를 재사용합니다.

5. DMARC 확인 결과 및 지정된 DMARC 확인 프로필에 따라, AsyncOS는 메시지를 수락, 격리 또는 거부합니다. DMARC 확인 실패 때문에 메시지가 거부되지 않는 경우, AsyncOS는 계속 처리를 진행합니다.
6. AsyncOS는 적절한 SMTP 응답을 전송하고 계속 처리를 진행합니다.

7. 집계 보고서의 전송이 활성화된 경우 AsyncOS는 DMARC 확인 데이터를 모으고, 이를 도메인 소유자에게 전송하는 일일 보고서에 포함합니다. DMARC 집계 피드백 보고서에 대한 자세한 내용은 DMARC 집계 보고서, 609 페이지 섹션을 참조하십시오.

참고 집계 보고서 크기가 10MB 또는 DMARC 레코드의 RUA 태그에 지정된 크기를 초과하는 경우 AsyncOS는 도메인 소유자에게 전달 오류 보고서를 전송합니다.

DMARC를 사용하여 수신 메시지를 확인하는 방법

DMARC를 사용하여 수신 메시지를 확인하는 방법

	수행해야 할 작업	추가 정보
1단계	새 DMARC 확인 프로필을 만들거나 기존 DMARC 확인 프로필을 요구 사항에 맞게 수정합니다.	DMARC 확인 프로필 만들기, 605 페이지 DMARC 확인 프로필 수정, 606 페이지
2단계	(선택 사항) 요구 사항에 맞게 전역 DMARC 설정을 구성합니다.	전역 DMARC 설정 구성, 607 페이지
3단계	DMARC를 사용하여 수신 메시지를 확인하기 위한 메일 플로우 정책을 구성합니다.	메일 플로우 정책에서 DMARC 확인 구성, 608 페이지
4단계	(선택 사항) DMARC 피드백 보고서의 반환 주소를 구성합니다.	DMARC 피드백 보고서의 반환 주소 구성, 609 페이지
5단계	(선택 사항) 다음을 검토합니다. • DMARC 확인 및 수신 메일 보고서 • 메시지 추적을 사용하여 DMARC 확인에 실패한 메시지	• DMARC Verification(DMARC 확인) 페이지, 815 페이지 • Incoming Mail(수신 메일) 페이지, 802 페이지 • 메시지 검색 , 838 페이지

관련 주제

- DMARC 확인 프로필 관리, 605 페이지
- DMARC 집계 보고서, 609 페이지
- 전역 DMARC 설정 구성, 607 페이지
- 메일 플로우 정책에서 DMARC 확인 구성, 608 페이지
- DMARC 피드백 보고서의 반환 주소 구성, 609 페이지

DMARC 확인 프로필 관리

DMARC 확인 프로필은 Email Security Appliance의 메일 플로우 정책이 DMARC 확인에 사용하는 매개변수 목록입니다. 예를 들면 특정 도메인에서 오는 모든 비호환 메시지를 거부하는 엄격한 프로필과 또 다른 도메인에서 오는 모든 비호환 메시지를 격리하는 덜 엄격한 프로필을 만들 수 있습니다.

DMARC 확인 프로필은 다음 정보로 구성됩니다.

- 확인 프로필의 이름.
- DMARC 레코드의 정책이 '거부'인 경우 수행할 메시지 작업
- DMARC 레코드의 정책이 '격리'인 경우 수행할 메시지 작업
- 일시적인 장애 시 수행할 메시지 작업
- 영구적인 장애 시 수행할 메시지 작업

관련 주제

- DMARC 확인 프로필 만들기, 605 페이지
- DMARC 확인 프로필 수정, 606 페이지
- DMARC 확인 프로필 내보내기, 606 페이지
- DMARC 확인 프로필 가져오기, 606 페이지
- DKIM 확인 프로필 삭제, 589 페이지

DMARC 확인 프로필 만들기

새 DMARC 확인 프로필을 만들려면 이 절차를 사용합니다.

참고 기본적으로 AsyncOS는 기본 DMARC 확인 프로필을 제공합니다. 새 DMARC 확인 프로필을 만들지 않으려는 경우 기본 DMARC 확인 프로필을 사용할 수 있습니다. 기본 DMARC 확인 프로필은 **Mail Policies(**메일 정책**)** > **DMARC** 페이지에서 사용할 수 있습니다. 기본 DMARC 확인 프로필 수정에 대한 자세한 내용은 DMARC 확인 프로필 수정, 606 페이지 섹션을 참조하십시오.

단계 **1** **Mail Policies(**메일 정책**)** > **DMARC**를 선택합니다.

단계 **2** **Add Profile(**프로필 추가**)**을 클릭합니다.

단계 **3** 프로필의 이름을 입력합니다.

단계 **4** DMARC 레코드의 정책이 '거부'인 경우 AsyncOS가 수행할 메시지 작업을 설정합니다. 다음 중 하나를 선택합니다.

- **No Action(**작업 없음**)**. AsyncOS가 DMARC 확인에 실패한 메시지에 대해 아무 작업도 수행하지 않습니다.
- **Quarantine(**격리**)**. AsyncOS가 DMARC 확인에 실패한 메시지를 지정된 격리에 격리합니다.
- **Reject(**거부**)**. AsyncOS가 DMARC 확인에 실패한 모든 메시지를 거부하고 지정된 SMTP 코드 및 응답을 반환합니다. 기본값은 각각 `550`및 `#5.7.1 DMARC unauthenticated mail is prohibited`입니다.

단계 **5** DMARC 레코드의 정책이 '격리'인 경우 AsyncOS가 수행할 메시지 작업을 설정합니다. 다음 중 하나를 선택합니다.

- **No Action(**작업 없음**)**. AsyncOS가 DMARC 확인에 실패한 메시지에 대해 아무 작업도 수행하지 않습니다.

- **Quarantine(**격리**)**. AsyncOS가 DMARC 확인에 실패한 메시지를 지정된 격리에 격리합니다.

단계 **6** DMARC 확인 중 일시적인 장애 상태의 메시지에 대해 AsyncOS가 수행할 메시지 작업을 설정합니다. 다음 중 하나를 선택합니다.

- **Accept(**수락**)**. AsyncOS가 DMARC 확인 중 일시적인 장애 상태의 메시지를 수락합니다.
- **Reject(**거부**)**. AsyncOS가 DMARC 확인 중 일시적인 장애 상태의 메시지를 거부하고 지정된 SMTP 코드 및 응답을 반환합니다. 기본값은 각각 `451` 및 `#4.7.1 Unable to perform DMARC verification`입니다.

단계 **7** DMARC 확인 중 영구적인 장애 상태의 메시지에 대해 AsyncOS가 수행할 메시지 작업을 설정합니다. 다음 중 하나를 선택합니다.

- **Accept(**수락**)**. AsyncOS가 DMARC 확인 중 영구적인 장애 상태의 메시지를 수락합니다.
- **Reject(**거부**)**. AsyncOS가 DMARC 확인 중 영구적인 장애 상태의 메시지를 거부하고 지정된 SMTP 코드 및 응답을 반환합니다. 기본값은 각각 `550` 및 `#5.7.1 DMARC verification failed`입니다.

단계 **8** 변경 사항을 제출 및 커밋합니다.

DMARC 확인 프로필 수정

단계 **1** **Mail Policies(**메일 정책**)** > **DMARC**를 선택합니다.

단계 **2** 원하는 확인 프로필 이름을 클릭합니다.

단계 **3** DMARC 확인 프로필 만들기, 605 페이지에 설명된 대로 원하는 필드를 수정합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

DMARC 확인 프로필 내보내기

어플라이언스의 모든 DMARC 확인 프로필을 configuration 디렉터리의 단일 텍스트 파일로 내보낼 수 있습니다.

단계 **1** **Mail Policies(**메일 정책**)** > **DMARC**를 선택합니다.

단계 **2** **Export Profiles(**프로필 내보내기**)**를 클릭합니다.

단계 **3** 파일의 이름을 입력합니다.

단계 **4** 제출을 클릭합니다.

DMARC 확인 프로필 가져오기

단계 **1** **Mail Policies(**메일 정책**)** > **DMARC**를 선택합니다.

단계 **2** **Import Profiles(**프로필 가져오기**)**를 클릭합니다.

단계 **3** DMARC 확인 프로필이 포함된 파일을 선택합니다.

단계 **4** **Submit**(제출)을 클릭합니다. 가져오기를 수행하면 기존의 모든 DMARC 확인 프로필이 교체된다는 경고가 표시됩니다.

단계 **5** **Import**(가져오기)를 클릭합니다.

단계 **6** 변경사항을 커밋합니다.

DMARC 확인 프로필 삭제

단계 **1** **Mail Policies**(메일 정책) > **DMARC**를 선택합니다.

단계 **2** 삭제할 확인 프로필을 선택합니다.

단계 **3** **Delete**(삭제)를 클릭합니다.

단계 **4** 삭제를 확인합니다.

전역 DMARC 설정 구성

단계 **1** **Mail Policies**(메일 정책) > **DMARC**를 선택합니다.

단계 **2** **Edit Global Settings**(전역 설정 수정)를 클릭합니다.

단계 **3** 다음 표에 정의된 설정을 변경합니다.

DMARC 전역 설정

전역 설정	설명
Specific senders bypass address list(특정 발신자 우회 메일 목록)	특정 발신자가 보낸 메시지의 DMARC 확인을 건너뜁니다. 드롭다운 목록에서 주소 목록을 선택합니다. 참고 전체 이메일 주소 또는 도메인만 사용하여 생성되는 주소 목록은 DMARC 확인을 우회하는 데 사용할 수 있습니다. 자세한 내용은 수신 연결 규칙에 발신자 주소 리스트 사용, 116 페이지를 참고하십시오.
Bypass verification for messages with headers(헤더가 있는 메시지에 대한 확인 우회)	특정 헤더가 포함된 메시지의 DMARC 확인을 건너뜁니다. 예를 들어 메일 목록 및 신뢰받는 전달자가 보낸 메시지에 대해 DMARC 검증을 건너뛰려면 이 옵션을 사용합니다. 하나의 헤더 또는 쉼표로 구분된 여러 헤더를 입력합니다.
Schedule for report generation(보고서 생성 예약)	AsyncOS에서 DMARC 집계 보고서를 생성해야 하는 시간. 예를 들면 메일 플로우에 영향을 미치지 않기 위해 집계 보고서 생성에 피크 시간 이외의 시간을 선택할 수 있습니다.
Entity generating reports(보고서를 생성하는 엔티티)	DMARC 집계 보고서를 생성하는 엔티티. DMARC 집계 보고서를 수신하는 도메인 소유자가 보고서를 생성한 엔티티를 식별하는 데 도움이 됩니다. 유효한 도메인 이름을 입력합니다.

전역 설정	설명
Additional contact information for reports(보고서의 추가 연락처 정보)	DMARC 집계 보고서를 수신하는 도메인 소유자가 보고서를 생성한 엔티티에 연락하려는 경우 사용할 수 있는 추가 연락처 정보(예: 조직의 고객 지원 세부사항).
Send copy of all aggregate reports to(모든 집계 보고서의 복사본 전송 대상)	모든 DMARC 집계 보고서의 복사본을 특정 사용자(예: 집계 보고서에 대한 분석을 수행하는 내부 사용자)에게 전송합니다. 하나의 이메일 주소 또는 쉼표로 구분된 여러 이메일 주소를 입력합니다.
Error Reports(오류 보고서)	DMARC 집계 보고서 크기가 10MB 또는 DMARC 레코드의 RUA 태그에 지정된 크기를 초과하는 경우 도메인 소유자에게 전달 오류 보고서 전송. 확인란을 선택합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

메일 플로우 정책에서 **DMARC** 확인 구성

단계 **1** **Mail Policies(**메일 정책**)** > **Mail Flow Policies(**메일 플로우 정책**)**를 선택합니다.

단계 **2** 확인을 수행할 리스너에 대한 수신 메일 정책을 클릭합니다.

단계 **3** 메일 플로우 정책의 Security Features(보안 기능) 섹션에서 **On(**켜기**)**을 선택하여 DMARC Verification(DMARC 확인)을 활성화합니다.

단계 **4** 정책에 사용할 DMARC 확인 프로필을 선택합니다.

단계 **5** (선택 사항) 메시지를 보낸 DMARC 활성화 도메인의 RUA 태그에 있는 이메일 주소로 DMARC 집계 피드백 보고서를 전송하도록 활성화합니다.

집계 피드백 보고서는 매일 생성됩니다.

단계 **6** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- DMARC 확인 로그, 608 페이지

DMARC 확인 로그

DMARC 확인의 다음 단계 중에 로그 메시지가 메일 로그에 추가됩니다.

- 메시지에서 DMARC 확인이 시도됨
- DMARC 확인이 완료됨
- DKIM 및 SPF 정렬 결과를 포함하는 DMARC 확인 세부사항

- 메시지에 대한 DMARC 확인을 건너뜀
- DMARC 레코드를 가져와서 구문 분석하거나 DNS 실패
- DMARC 집계 보고서가 도메인에 전달되지 않음
- 도메인에 대해 오류 보고서가 생성됨
- 도메인에 오류 보고서가 전달됨
- 도메인에 오류 보고서가 전달되지 않음

DMARC 피드백 보고서의 반환 주소 구성

단계 **1** **System Administration**(시스템 관리) > **Return Addresses**(반환 주소)를 선택합니다.

단계 **2** **Edit Settings**(설정 수정)를 클릭합니다.

단계 **3** DMARC 집계 피드백 보고서의 반환 주소를 제공합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

DMARC 집계 보고서

DMARC는 피드백 메커니즘을 통해 도메인 소유자 정책을 안전하게 확장 가능한 방식으로 시행합니다. 이 피드백 메커니즘은 도메인 소유자가 인증 구축을 강화하는 데 도움이 됩니다.

AsyncOS를 사용하여 DMARC 확인을 수행하며 메일 플로우 정책에서 집계 피드백 보고서의 전송을 활성화한 경우, AsyncOS는 집계 피드백 보고서를 매일 생성하여 도메인 소유자에게 전송합니다. 이런 보고서는 XML 형식이며 GZip 파일에 보관됩니다.

참고 AsyncOS에서 생성하는 DMARC 집계 피드백 보고서는 DMARC를 준수합니다.

DMARC 집계 피드백 보고서에는 다음 섹션이 포함되어 있습니다.

- 이메일 주소 및 보고서 ID 번호와 같은 보고서 발신자의 메타데이터
- 게시된 DMARC 정책의 세부사항
- 소스 IP 주소 및 처리 요약 등 DMARC 정책 처리의 세부사항
- 도메인 식별자
- DMARC 확인 결과 및 인증 요약

관련 주제

- 샘플 DMARC 집계 피드백 보고서, 609 페이지

샘플 DMARC 집계 피드백 보고서

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <version>1.0</version>
  <report_metadata>
```

```
    <org_name>cisco.com</org_name>
    <email>noreply-dmarc-support@cisco.com</email>
    <extra_contact_info>http://cisco.com/dmarc/support</extra_contact_info>
    <report_id>b1d925$4ecceab=0694614b826605cd@cisco.com</report_id>
    <date_range>
      <begin>1335571200</begin>
      <end>1335657599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>1.1.1.1</source_ip>
      <count>2</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
   <envelope_from>example.com</envelope_from>
      <header_from>example.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com</domain>
     <selector>ny</selector>
        <result>fail</result>
      </dkim>
      <dkim>
        <domain>example.net</domain>
<selector></selector>
        <result>pass</result>
      </dkim>
      <spf>
        <domain>example.com</domain>
<scope>mfrom</scope>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
</feedback>
```

위조 이메일 탐지

이메일 위조(스푸핑, CEO 사기 또는 비즈니스 이메일의 감염이라고도 함)는 발신자의 실제 신원을 숨기고 아는 사람이 보낸 합법적인 메시지처럼 보이도록 메시지 헤더를 변경하는 프로세스입니다. 조직의 임원으로 가장한 사기꾼이 직원에게 클라이언트 목록 및 해당 PII(개인 식별 정보)를 전송하도록 요청하는 위조된 메시지를 보내는 것으로 추정합니다. 발신자의 실제 신원을 인식하지 못한 직원이 클라이언트와 해당 PII 목록을 제공합니다. 사기꾼은 PII를 사용하여 신원 도용을 수행합니다.

Cisco Email Security Appliance는 위조된 발신자 주소(From: 헤더)를 사용하여 사기 메시지를 탐지하고 그러한 메시지에 대해 지정된 작업을 수행할 수 있습니다. 예를 들어, 어플라이언스에서 위조된 발신자 주소를 사용하는 메시지를 탐지하여 From: 헤더를 봉투 발신자로 교체할 수 있습니다. 이 경우 직원에게는 위조된 이메일 주소 대신 실제 발신자(사기꾼)의 이메일 주소가 표시됩니다.

관련 주제

- 위조 이메일 탐지 설정, 611 페이지
- 위조 이메일 탐지 결과 모니터링, 612 페이지
- 메시지 추적에서 위조 이메일 탐지 세부 정보 표시, 612 페이지

위조 이메일 탐지 설정

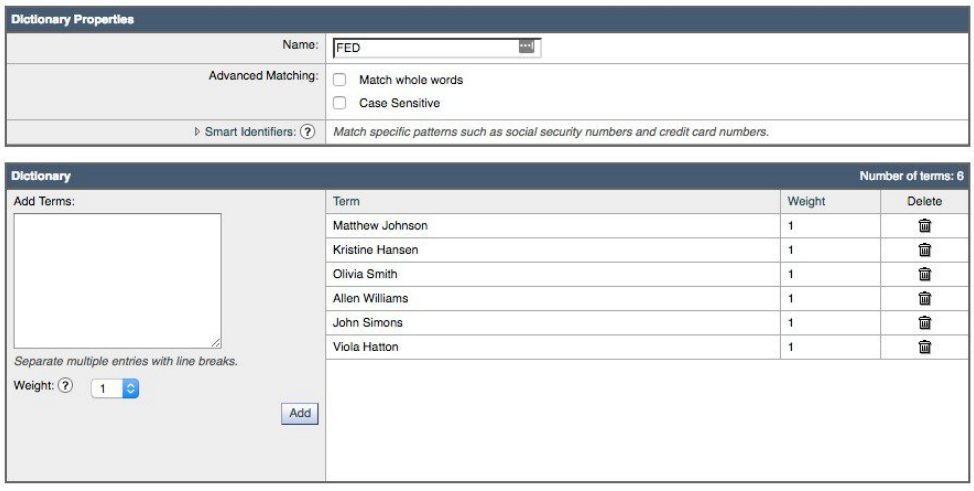
1. 메시지가 위조될 가능성이 있는 조직에서 사용자(예: 경영진)를 식별합니다. 새 콘텐츠 사전을 생성하고 식별된 사용자 이름을 추가합니다.

   콘텐츠 사전을 생성하는 동안

   - 이메일 주소가 아니라 사용자의 이름을 입력합니다. 예를 들어, "olivia.smith@example.com"이 아니라 "Olivia Smith"를 입력합니다.
   - 고급 일치 및 스마트 식별자는 구성하지 마십시오.
   - 사용되는 용어의 가중치는 선택하지 마십시오.
   - 정규 표현식은 사용하지 마십시오.

   다음 그림은 위조 이메일 탐지를 위해 생성된 샘플 콘텐츠 사전입니다.

   그림 ***39:*** 위조 이메일 탐지를 위한 콘텐츠 사전



   콘텐츠 사전 구성 지침은 사전 추가, 617 페이지 섹션을 참조하십시오.

2. 위조된 메시지 및 어플라이언스는 이러한 메시지에 수행 해야 하는 작업을 탐지하기 위해 수신 콘텐츠 또는 메시지 필터를 만듭니다. 다음을 사용하십시오.

- 조건/규칙: 위조 이메일 탐지(콘텐츠 필터 조건, 284 페이지 및 메시지 필터 규칙, 138 페이지 참조)
- 작업: 위조 이메일 탐지 또는 요구 사항에 따른 다른 작업. (콘텐츠 필터 조건, 284 페이지 및 메시지 필터 규칙, 138 페이지 참조)

3. 새로 만든 콘텐츠 필터를 수신 메일 정책에 추가합니다. 사용자 단위로 메일 정책을 시행하는 방법, 270 페이지를 참조하십시오.

위조 이메일 탐지 결과 모니터링

탐지된 위조 메시지에 대한 데이터를 보려면 Forged Email Matches(위조 이메일 일치 항목) 보고서 페이지(**Monitor(**모니터**)** > **Forged Email Matches(**위조 이메일 일치 항목**)**)를 참조하십시오. 이 보고서 페이지에는 다음 보고서가 포함됩니다.

- **Top Forged Email Matches(**상위 위조 이메일 일치 항목**)** 수신 메시지의 위조된 From(보낸 사람): 헤더와 일치하는 콘텐츠 사전의 사용자 상위 10명이 표시됩니다.
- **Forged Email Matches(**위조 이메일 일치 항목**): Details(**세부 정보**)** 수신 메시지의 위조된 From(보낸 사람): 헤더와 일치하는 콘텐츠 사전의 모든 사용자 목록과, 지정한 사용자에 대해 일치하는 메시지 수가 표시됩니다. Message Tracking(메시지 추적)에서 메시지의 목록을 보려면 해당 숫자를 클릭합니다.

메시지 추적에서 위조 이메일 탐지 세부 정보 표시

메시지 추적에서 어플라이언스가 탐지한 위조된 메시지의 세부 정보를 표시하려면 다음 사항을 확인합니다.

- 메시지 추적이 활성화되어 있습니다. 메시지 추적, 837 페이지를 참조하십시오.
- 위조된 메시지 탐지를 위해 콘텐츠 또는 메시지 필터가 작동합니다.

25 장

텍스트 리소스

이 장에는 다음 섹션이 포함되어 있습니다.

텍스트 리소스 개요

이 장에서는 콘텐츠 사전, 면책조항, 템플릿 등 다양한 텍스트 리소스를 만들고 관리하는 방법에 대해 설명합니다.

관련 주제

- 컨텐트 사전, 613 페이지
- 텍스트 리소스, 614 페이지
- 메시지 면책조항 스탬프, 614 페이지
- 민감한 DLP 용어(맞춤화 DLP 정책 전용)의 맞춤화 사전 사용 , 505 페이지

컨텐트 사전

콘텐츠 사전은 어플라이언스의 Body Scanning(본문 검사) 기능과 함께 작동하며 콘텐츠 필터와 메시지 필터에서 모두 사용 가능한 단어나 항목의 그룹입니다. 사전을 사용하면 메시지, 메시지 헤더 및 메시지 어태치 파일에서 사전에 포함된 용어를 검사하여 회사 정책에 따라 적절한 작업을 하도록 정의할 수 있습니다. 예를 들어 기밀 단어나 비속어 리스트를 만들고, 메시지에서 리스트의 단어를 검사하는 필터 규칙을 사용하여 해당 메시지를 삭제, 아카이브 또는 격리할 수 있습니다.

AsyncOS 운영 체제에서는 GUI(Mail Policies(메일 정책) > Dictionaries(사전)) 또는 CLI의 **dictionaryconfig** 명령을 사용하여 총 100개의 콘텐츠 사전을 정의할 수 있는 기능을 제공합니

다. 사전을 만들고 삭제하고 볼 수 있으며, 사전에서 항목을 추가 및 삭제할 수 있고, 전체 사전을 가져오고 내보낼 수 있습니다.

콘텐츠 사전을 사용하면 메시지 필터나 콘텐츠 필터로 메시지를 검사하여 회사 정책에 따라 적절한 작업을 할 수 있습니다. 사전을 만들고 삭제하고 볼 수 있으며, 사전에서 항목을 추가 및 삭제할 수 있고, 전체 사전을 가져오고 내보낼 수 있습니다. 또한 각 사전에 대해 대/소문자 구문 및 단어 경계 탐지를 결정할 수 있습니다. 예를 들어 기밀 단어나 비속어 리스트를 만들고, 메시지에서 리스트의 단어를 검사하는 필터 규칙을 사용하여 일치하는 단어가 포함된 메시지를 삭제 또는 아카이브할 수 있습니다. 또한 특정 용어가 필터 작업을 좀 더 쉽게 트리거하도록 사전에 "가중치" 용어를 추가할 수 있습니다.

사전에는 비 ASCII 문자를 포함할 수 있습니다.

효율적인 처리를 위해 다음 콘텐츠 사전 항목은 단어로 취급됩니다.

- 영숫자 문자만 포함하는 항목
- 0-9, A-Z, a-z, 점, 밑줄, 하이픈 및 @ 기호 문자를 포함하는 이메일 주소
- 0-9, A-Z, a-z, 점, 밑줄, 하이픈 및 @ 기호 문자를 포함하는 도메인 이름

어플라이언스에서 그러한 단어를 정규식으로 취급하도록 하려면 (user@example.com)과 같이 해당 단어를 괄호로 묶어 주십시오.

관련 주제

- 사전 콘텐츠, 615 페이지
- 사전을 텍스트 파일로 가져오기 및 내보내기, 616 페이지
- 사전 추가, 617 페이지
- 사전 삭제, 618 페이지
- 사전 가져오기, 618 페이지
- 사전 내보내기, 619 페이지

텍스트 리소스

텍스트 리소스란 면책조항, 알림 템플릿, 안티바이러스 템플릿과 같은 텍스트 개체입니다. AsyncOS의 다양한 구성 요소에서 사용할 새 개체를 만들 수 있습니다. 텍스트 리소스를 가져오고 내보낼 수 있습니다.

메시지 면책조항 스탬프

메시지 면책조항 스탬프 기능을 사용하면 메시지에 면책조항 텍스트 리소스를 추가할 수 있습니다. 예를 들면 기업 내에서 전송되는 모든 메시지에 저작권 안내문, 프로모션 메시지 또는 면책조항을 추가할 수 있습니다.

컨텐트 사전

콘텐츠 사전은 어플라이언스의 Body Scanning(본문 검사) 기능과 함께 작동하며 콘텐츠 필터와 메시지 필터에서 모두 사용 가능한 단어나 항목의 그룹입니다. 사전을 사용하면 메시지, 메시지 헤더 및 메시지 어태치 파일에서 사전에 포함된 용어를 검사하여 회사 정책에 따라 적절한 작업을 하도록 정의할 수 있습니다. 예를 들어 기밀 단어나 비속어 리스트를 만들고, 메시지에서 리스트의 단어를 검사하는 필터 규칙을 사용하여 해당 메시지를 삭제, 아카이브 또는 격리할 수 있습니다.

AsyncOS 운영 체제에서는 GUI(Mail Policies(메일 정책) > Dictionaries(사전)) 또는 CLI의 **dictionaryconfig** 명령을 사용하여 총 100개의 콘텐츠 사전을 정의할 수 있는 기능을 제공합니다. 사전을 만들고 삭제하고 볼 수 있으며, 사전에서 항목을 추가 및 삭제할 수 있고, 전체 사전을 가져오고 내보낼 수 있습니다.

콘텐츠 사전을 사용하면 메시지 필터나 콘텐츠 필터로 메시지를 검사하여 회사 정책에 따라 적절한 작업을 할 수 있습니다. 사전을 만들고 삭제하고 볼 수 있으며, 사전에서 항목을 추가 및 삭제할 수 있고, 전체 사전을 가져오고 내보낼 수 있습니다. 또한 각 사전에 대해 대/소문자 구문 및 단어 경계 탐지를 결정할 수 있습니다. 예를 들어 기밀 단어나 비속어 리스트를 만들고, 메시지에서 리스트의 단어를 검사하는 필터 규칙을 사용하여 일치하는 단어가 포함된 메시지를 삭제 또는 아카이브할 수 있습니다. 또한 특정 용어가 필터 작업을 좀 더 쉽게 트리거하도록 사전에 "가중치" 용어를 추가할 수 있습니다.

사전에는 비 ASCII 문자를 포함할 수 있습니다.

효율적인 처리를 위해 다음 콘텐츠 사전 항목은 단어로 취급됩니다.

- 영숫자 문자만 포함하는 항목
- 0-9, A-Z, a-z, 점, 밑줄, 하이픈 및 @ 기호 문자를 포함하는 이메일 주소
- 0-9, A-Z, a-z, 점, 밑줄, 하이픈 및 @ 기호 문자를 포함하는 도메인 이름

어플라이언스에서 그러한 단어를 정규식으로 취급하도록 하려면 (user@example.com)과 같이 해당 단어를 괄호로 묶어 주십시오.

관련 주제

- 사전 콘텐츠, 615 페이지
- 사전을 텍스트 파일로 가져오기 및 내보내기, 616 페이지
- 사전 추가, 617 페이지
- 사전 삭제, 618 페이지
- 사전 가져오기, 618 페이지
- 사전 내보내기, 619 페이지

사전 콘텐츠

사전의 단어는 한 줄에 하나의 텍스트 문자열로 생성되며, 항목은 일반 텍스트 형식이거나 정규식 형식일 수 있습니다. 또한 사전에는 비 ASCII 문자를 포함할 수 있습니다. 정규식의 사전을 정의하면 용어 일치 확인에서 좀 더 유연할 수 있지만, 이 경우 단어의 경계를 적절히 정하는 방법을 이해해야 합

니다. Python 스타일 정규식에 대한 자세한 내용은 다음 사이트에서 Python Regular Expression HOWTO를 참조해 주십시오.

http://www.python.org/doc/howto/

참고 사전 항목 시작 부분에 # 특수 문자를 사용하려면 코멘트로 취급되지 않도록 [#] 문자 클래스를 사용할 수 있습니다.

특정 용어가 필터 조건을 좀 더 쉽게 트리거할 수 있도록 각 용어에 대해 "가중치"를 지정할 수 있습니다. AsyncOS는 메시지에서 콘텐츠 사전 용어를 검사할 때 항목이 나타나는 수에 용어의 가중치를 곱해 메시지 "점수"를 매깁니다. 가중치 3인 용어가 두 번 나오면 점수는 6점입니다. 그러면 AsyncOS는 이 점수를 콘텐츠 또는 메시지 필터와 연결된 임계값과 비교하여, 메시지가 필터 작업을 트리거해야 할지를 결정합니다.

콘텐츠 사전에 스마트 식별자를 추가할 수도 있습니다. 스마트 식별자는 주민등록번호, ABA 라우팅 번호 등 일반적인 숫자 패턴에 해당하는 데이터의 패턴을 검색하는 알고리즘입니다. 이러한 식별자는 정책 시행에 유용할 수 있습니다. 정규식에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 시행" 장에서 "규칙의 정규식" 섹션을 참조해 주십시오. 스마트 식별자에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 시행" 장에서 "스마트 식별자" 섹션을 참조해 주십시오.

참고 비 ASCII 문자가 포함된 사전은 터미널의 CLI에서 제대로 표시되지 않을 수 있습니다. 비 ASCII 문자가 포함된 사전을 보고 변경하는 가장 좋은 방법은 사전을 텍스트 파일로 내보내고, 텍스트 파일을 수정한 다음, 새 파일을 어플라이언스로 다시 가져오는 것입니다. 자세한 내용은 사전을 텍스트 파일로 가져오기 및 내보내기, 616 페이지를 참고하십시오.

관련 주제

- 단어 경계 및 더블 바이트 문자 집합, 616 페이지

단어 경계 및 더블 바이트 문자 집합

일부 언어(더블 바이트 문자 집합)에는 단어나 단어 경계 또는 대/소문자라는 개념이 없습니다. 로캘이 알려지지 않았거나 인코딩이 확실히 알려지지 않은 경우 단어를 구성하는 문자가 무엇인가에 대한 개념에 의존하는 복잡한 정규식(regex 구문에서 "\w"로 표현)은 문제를 일으킵니다. 이러한 이유로 단어 경계 적용을 비활성화할 수 있습니다.

사전을 텍스트 파일로 가져오기 및 내보내기

콘텐츠 사전 기능에는 또한 어플라이언스의 configuration 디렉터리에 있는 다음 텍스트 파일이 기본적으로 포함됩니다.

- **config.dtd**
- **profanity.txt**
- **proprietary_content.txt**

- **sexual_content.txt**

이러한 텍스트 파일은 새 사전을 만드는 데 도움이 되는 콘텐츠 사전 기능과 함께 사용할 수 있습니다. 데이터의 패턴을 더 잘 탐지하고 패턴이 규정준수 문제를 나타낼 때 필터를 트리거하도록 이러한 콘텐츠 사전은 가중되며 스마트 식별자를 사용합니다.

참고 사전을 가져오고 내보내는 경우 Match Whole Words(전체 단어 일치) 및 Case Sensitive(대/소문자 구분) 설정이 보존되지 않습니다. 이러한 설정은 구성 파일에만 보존됩니다.

구성 디렉터리 액세스에 대한 자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지를 참조하십시오.

자신의 고유한 사전 파일을 만들어서 어플라이언스로 가져올 수도 있습니다. 비 ASCII 문자를 사전에 추가하는 가장 좋은 방법은 어플라이언스 외부의 텍스트 파일의 사전에 용어를 추가하고, 이 파일을 어플라이언스로 이동한 다음 새 사전으로서 가져오는 것입니다. 사전 가져오기에 대한 자세한 내용은 사전 가져오기, 618 페이지 섹션을 참조하십시오. 사전 내보내기에 대한 자세한 내용은 사전 내보내기, 619 페이지 섹션을 참조하십시오.

주의 이러한 텍스트 파일에는 음란하고 외설적이며 공격적이라고 생각될 수 있는 용어가 포함되어 있습니다. 이러한 파일의 용어를 콘텐츠 사전으로 가져오는 경우, 나중에 어플라이언스에서 구성한 콘텐츠 사전을 볼 때 해당 용어가 표시됩니다.

사전 추가

단계 **1** **Mail Policies**(메일 정책) > **Dictionaries**(사전) 페이지로 이동합니다.

단계 **2** **Add Dictionary**(사전 추가)를 클릭합니다.

단계 **3** 사전의 이름을 입력합니다.

단계 **4** (선택 사항) Advanced Matching(고급 일치)을 구성합니다.

참고 **Match Whole Words**(전체 단어 일치) 및 **Case Sensitive**(대/소문자 구분) 설정은 구성 파일에 저장할 때 보존됩니다. 그러나 사전을 가져오고 내보낼 경우에는 이러한 설정이 보존되지 않습니다.

단계 **5** (선택 사항) 사전에 스마트 식별자를 추가합니다.

스마트 식별자는 주민등록번호, ABA 라우팅 번호 등 일반적인 숫자 패턴에 해당하는 데이터의 패턴을 검색하는 알고리즘입니다. 스마트 식별자에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 시행" 장을 참조하십시오.

단계 **6** 용어 리스트에 새 사전 항목을 입력합니다.

추가할 새 항목이 여러 개이고 이들이 각각 동일한 가능성으로 필터 작업을 트리거하도록 하려면 각각을 개별 줄에 추가합니다.

참고 콘텐츠 사전 항목의 시작이나 끝 부분에 정규식 ".*"가 포함된 경우 "word" MIME 부분에 대한 일치가 발견되면 시스템이 잠깁니다. 콘텐츠 사전 항목의 시작이나 끝 부분에 ".*"를 사용하지 않는 것이 좋습니다.

단계 **7** 용어에 대한 가중치를 지정합니다.

특정 사전 용어가 다른 용어보다 필터 작업을 트리거할 가능성을 높이려면 해당 용어에 "가중치"를 줄 수 있습니다. 필터 작업을 결정하는 데 가중치가 사용되는 방법에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 시행" 장에서 "콘텐츠 사전용 임계값 점수" 섹션을 참조하십시오.

단계 **8** **Add(**추가**)**를 클릭합니다.

단계 **9** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- 사전 콘텐츠, 615 페이지.

사전 삭제

시작하기 전에

AsyncOS에서는 삭제된 사전을 참조하는 메시지 필터를 모두 잘못된 것으로 표시합니다. AsyncOS에서는 삭제된 사전을 참조하는 필터를 활성화 상태로 유지하지만, 이러한 필터는 거짓으로 평가됩니다.

단계 **1** **Mail Policies(**메일 정책**)** > **Dictionaries(**사전**)** 페이지로 이동합니다.

단계 **2** 사전 리스트에서 삭제할 사전 옆에 있는 휴지통 아이콘을 클릭합니다.

확인 메시지에는 현재 사전을 참조하는 필터가 나열됩니다.

단계 **3** 확인 메시지에서 **Delete(**삭제**)**를 클릭합니다.

단계 **4** 변경사항을 커밋합니다.

사전 가져오기

시작하기 전에

가져올 파일이 어플라이언스의 configuration 디렉터리에 있는지 확인합니다.

단계 **1** **Mail Policies(**메일 정책**)** > **Dictionaries(**사전**)** 페이지로 이동합니다.

단계 **2** **Import Dictionary(**사전 가져오기**)**를 클릭합니다.

단계 **3** 가져올 위치를 선택합니다.

단계 **4** 가져올 파일을 선택합니다.

단계 **5** 사전 용어에 사용할 기본 가중치를 선택합니다.

가중치가 지정되지 않은 용어의 경우 AsyncOS에서는 기본 가중치를 할당합니다. 파일을 가져온 후 가중치를 수정할 수 있습니다.

단계 **6** 인코딩을 선택합니다.

단계 **7** **Next**(다음)를 클릭합니다.

단계 **8** 사전의 이름을 지정하고 수정합니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

사전 내보내기

단계 **1** **Mail Policies**(메일 정책) > Dictionaries(사전) 페이지로 이동합니다.

단계 **2** **Export Dictionary**(사전 내보내기)를 클릭합니다.

단계 **3** 내보낼 사전을 선택합니다.

단계 **4** 내보낸 사전에 대한 파일 이름을 입력합니다.

이것은 어플라이언스의 configuration 디렉터리에 생성될 파일의 이름입니다.

단계 **5** 내보낼 위치를 선택합니다.

단계 **6** 텍스트 파일의 인코딩을 선택합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

콘텐츠 사전 필터 규칙 사용 및 테스트

사전은 다양한 dictionary-match() 메시지 필터 규칙 및 콘텐츠 필터와 함께 사용할 수 있습니다.

관련 주제

- 사전 일치 필터 규칙, 619 페이지

사전 일치 필터 규칙

*dictionary_name*이란 이름의 콘텐츠 사전에 있는 정규식 중 하나가 메시지 본문에 포함되어 있으면 `dictionary-match(<`*dictionary_name*`>)`라는 이름의 메시지 필터 규칙(및 관련 내용)은 참으로 평가됩니다. 해당 사전이 존재하지 않으면 규칙은 거짓으로 평가됩니다.

`dictionary-match()` 규칙은 `body-contains()` 본문 검사 규칙과 유사하게 작동합니다. 메시지의 본문과 어태치 파일만 검사하고 헤더는 검사하지 않습니다.

헤더를 검사하려면 `*-dictionary-match()` 유형의 규칙을 사용할 수 있습니다. `subject-dictionary-match()`와 같은 특정 헤더에 대한 규칙이 있고, `header-dictionary-match()`와 같은 좀 더 일반적인 규칙이 있습니다. 일반적인 규칙에서는 맞춤형 헤더를 비롯한 모든 헤더를 지정

할 수 있습니다. 사전 일치에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 시행" 장에서 "사전 규칙" 섹션을 참조하십시오.

표 **43:** 콘텐츠 사전용 메시지 필터 규칙

규칙	**Syntax**	설명
사전 일치	`dictionary-match (<dictionary_name>)`	명명된 디렉터리에 나열된 모든 정규식과 일치하는 단어가 메시지에 포함되어 있습니까?

다음 예에서는 어플라이언스가 "secret_words"라는 이름의 디렉터리(이전 예에서 생성) 내에서 특정 단어를 포함하는 메시지를 검사할 때 관리자에게 숨은 참조로 보내도록 `dictionary-match()` 규칙을 사용한 새 메시지 필터가 생성됩니다. 설정 때문에 대/소문자를 포함하여 정확하게 "`codename`" 전체 단어를 포함하는 메시지만 이 필터에 대해 true로 평가됩니다.

```
bcc_codenames:

if (dictionary-match ('secret_words'))

{

bcc('administrator@example.com');

}
```

이 예에서는 Policy(정책) 격리로 메시지를 전송합니다.

```
quarantine_codenames:

if (dictionary-match ('secret_words'))

{

quarantine('Policy');


}
```

관련 주제

- 디렉터리 항목 예, 620 페이지
- 콘텐츠 사전 테스트, 621 페이지

디렉터리 항목 예

표 **44:** 디렉터리 항목 예

설명	예
와일드카드	
앵커	다음으로 끝남: foo $ 다음으로 시작: ^ foo
이메일 주소(마침표를 이스케이프하지 않음)	**foo@example.com**, **@example.com** **example.com$** (ends with)**@example.***

설명	예
제목	이메일 제목(이메일 제목에서 ^ 앵커를 사용하는 경우 해당 제목 앞에 종종 "RE:" 또는 "FW:" 등이 추가됩니다.)

콘텐츠 사전 테스트

`trace` 함수는 `dictionary-match()` 규칙을 사용하는 메시지 필터에 대한 빠른 피드백을 제공할 수 있습니다. 자세한 내용은 테스트 메시지를 사용하여 메일 플로우 디버깅: 추적, 1149 페이지를 참조하십시오. 위의 `quarantine_codenames` 필터 예에서와 같이 `quarantine()` 작업을 사용하여 필터를 테스트할 수도 있습니다.

텍스트 리소스 이해

텍스트 리소스는 메시지에 어태치하거나 메시지로서 전송할 수 있는 텍스트 템플릿입니다. 텍스트 리소스 유형은 다음 중 하나일 수 있습니다.

- 메시지 면책조항 - 메시지에 추가된 텍스트. 자세한 내용은 면책조항 템플릿, 625 페이지를 참고하십시오.
- 알림 템플릿 - notify() 및 notify-bcc() 작업과 함께 사용되고 알림으로서 전송된 메시지. 자세한 내용은 알림 템플릿, 631 페이지를 참고하십시오.
- 안티바이러스 알림 템플릿 - 메시지에서 바이러스가 발견될 때 알림으로 전송되는 메시지. 컨테이너용 템플릿(원본 메시지 첨부)을 만들거나 메시지 첨부 없이 전송되는 알림으로서의 템플릿을 만들 수 있습니다. 자세한 내용은 안티바이러스 알림 템플릿, 631 페이지를 참고하십시오.
- 바운스 및 암호화 실패 알림 템플릿 - 메시지가 바운스되거나 메시지 암호화가 실패할 때 알림으로 전송되는 메시지. 자세한 내용은 바운스 및 암호화 실패 알림 템플릿, 634 페이지를 참고하십시오.
- 암호화 알림 템플릿 - 발신 이메일을 암호화하기 위해 어플라이언스를 구성할 때 전송되는 메시지. 이 메시지는 수신자에게 암호화된 메시지가 수신되었음을 알리고 이를 읽기 위한 지침을 제공합니다. 자세한 내용은 암호화 알림 템플릿, 636 페이지를 참고하십시오.

CLI(**textconfig**) 또는 GUI를 사용하여 추가, 삭제, 수정, 가져오기, 내보내기 등 텍스트 리소스를 관리할 수 있습니다. GUI를 사용하여 텍스트 리소스를 관리하는 방법에 대한 자세한 내용은 텍스트 리소스 관리 개요, 622 페이지 섹션을 참조하십시오.

텍스트 리소스에는 비 ASCII 문자를 포함할 수 있습니다.

참고 비 ASCII 문자가 포함된 텍스트 리소스는 터미널의 CLI에서 제대로 표시되지 않을 수 있습니다. 비 ASCII 문자가 포함된 텍스트 리소스를 보고 변경하려면 텍스트 리소스를 텍스트 파일로 내보내고, 텍스트 파일을 수정한 다음, 새 파일을 어플라이언스로 다시 가져오십시오. 자세한 내용은 사전을 텍스트 파일로 가져오기 및 내보내기, 616 페이지를 참고하십시오.

관련 주제

- 사전을 텍스트 파일로 가져오기 및 내보내기, 616 페이지

텍스트 리소스를 텍스트 파일로 가져오기 및 내보내기

어플라이언스의 configuration 디렉터리에 액세스할 수 있어야 합니다. 가져온 텍스트 파일은 어플라이언스의 configuration 디렉터리에 있어야 합니다. 내보낸 텍스트 파일은 configuration 디렉터리에 저장됩니다.

configuration 디렉터리 액세스에 대한 자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지 섹션을 참조하십시오.

비 ASCII 문자를 텍스트 리소스에 추가하려면 어플라이언스 외부의 텍스트 파일의 텍스트 리소스에 용어를 추가하고, 이 파일을 어플라이언스로 이동한 다음 새 텍스트 리소스로 가져오십시오. 텍스트 리소스 가져오기에 대한 자세한 내용은 텍스트 리소스 가져오기, 623 페이지 섹션을 참조하십시오. 텍스트 리소스 내보내기에 대한 자세한 내용은 텍스트 리소스 내보내기, 624 페이지 섹션을 참조하십시오.

텍스트 리소스 관리 개요

GUI 또는 CLI를 사용하여 텍스트 리소스를 관리할 수 있습니다. 이 섹션은 GUI에 초점을 맞춥니다.

`textconfig` 명령을 사용하여 CLI로부터 텍스트 리소스를 관리합니다.

텍스트 리소스 관리에는 다음 작업이 포함됩니다.

- 추가
- 수정 및 삭제
- 내보내기 및 가져오기
- 모든 텍스트 리소스 유형에 대한 일반 텍스트 메시지 정의
- 일부 텍스트 리소스 유형에 대한 HTML 기반 메시지 정의

관련 항목

- 텍스트 리소스 추가, 622 페이지
- 텍스트 리소스 삭제, 623 페이지
- 텍스트 리소스 내보내기, 624 페이지
- 텍스트 리소스 가져오기, 623 페이지
- HTML 기반 텍스트 리소스 개요, 624 페이지.

텍스트 리소스 추가

단계 **1** **Mail Policies**(메일 정책) > **Text Resources**(텍스트 리소스)로 이동합니다.

단계 **2** **Add Text Resource**(텍스트 리소스 추가)를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 텍스트 리소스에 대한 이름을 입력합니다.

단계 **4** **Type(**유형**)** 필드에서 텍스트 리소스의 유형을 선택합니다.

단계 **5** **Text(**텍스트**)** 또는 **HTML and Plain Text(HTML** 및 일반 텍스트**)** 필드에 메시지 텍스트를 입력합니다.

텍스트 리소스에서 일반 텍스트 메시지만 허용하는 경우 **Text(**텍스트**)** 필드를 사용합니다. 텍스트 리소스가 HTML과 일반 텍스트 메시지를 모두 허용하는 경우 **HTML and Plain Text(HTML** 및 일반 텍스트**)** 필드를 사용합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 항목

- HTML 기반 텍스트 리소스 개요, 624 페이지.

텍스트 리소스 삭제

시작하기 전에

텍스트 리소스를 삭제하는 경우

- 삭제된 텍스트 리소스를 참조하는 메시지 필터는 잘못된 것으로 표시됩니다.
- 삭제된 텍스트 리소스를 참조하는 콘텐츠 필터는 활성화 상태가 유지되지만 거짓으로 평가됩니다.

단계 **1** **Mail Policies(**메일 정책**)** > **Text Resources(**텍스트 리소스**)** 페이지에서 삭제할 텍스트 리소스에 대한 Delete(삭제) 열 아래에 있는 휴지통 아이콘을 클릭합니다. 확인 메시지가 표시됩니다.

단계 **2** 텍스트 리소스를 삭제하려면 **Delete(**삭제**)**를 클릭합니다.

단계 **3** 변경사항을 커밋합니다.

텍스트 리소스 가져오기

시작하기 전에

가져올 파일이 어플라이언스의 configuration 디렉터리에 있는지 확인합니다.

단계 **1** **Mail Policies(**메일 정책**)** > **Text Resources(**텍스트 리소스**)** 페이지에서 **Import Text Resource(**텍스트 리소스 가져오기**)**를 클릭합니다.

단계 **2** 가져올 파일을 선택합니다.

단계 **3** 인코딩을 지정합니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** 이름을 선택하고, 수정하고, 텍스트 리소스 유형을 선택합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

텍스트 리소스 내보내기

시작하기 전에

텍스트 리소스를 내보내면 어플라이언스의 configuration 디렉터리에 텍스트 파일이 생성됩니다.

단계 **1** **Mail Policies(**메일 정책**)** > **Text Resources(**텍스트 리소스**)** 페이지에서 **Export Text Resource(**텍스트 리소스 내보내기**)**를 클릭합니다.

단계 **2** 내보낼 텍스트 리소스를 선택합니다.

단계 **3** 텍스트 리소스의 이름을 입력합니다.

단계 **4** 텍스트 파일의 인코딩을 선택합니다.

단계 **5** **Submit(**제출**)**을 클릭하여 텍스트 리소스가 포함된 텍스트 파일을 configuration 디렉터리에 만듭니다.

HTML 기반 텍스트 리소스 개요

HTML 기반 및 일반 텍스트 메시지로 면책조항과 같은 몇몇 텍스트 리소스를 만들 수 있습니다. HTML 기반 및 일반 텍스트 메시지를 모두 포함하는 텍스트 리소스를 이메일 메시지에 적용하면 HTML 기반 텍스트 리소스 메시지는 이메일 메시지의 text/html 부분에 적용되고, 일반 텍스트 메시지는 이메일 메시지의 text/plain 부분에 적용됩니다.

HTML 기반 텍스트 리소스를 추가 또는 수정할 때 GUI에는 HTML 코드를 수정으로 작성하지 않고도 리치 텍스트를 입력할 수 있는 리치 텍스트 편집기가 포함되어 있습니다.

HTML 기반 텍스트 리소스를 추가 및 수정할 때는 다음 정보를 고려하십시오.

- HTML 버전을 기반으로 메시지의 일반 텍스트 버전이 자동으로 생성되도록 할 수도 있고, 일반 텍스트 버전을 독립적으로 정의할 수도 있습니다.
- **Code View(**코드 보기**)** 버튼을 클릭하여 리치 텍스트 편집기와 HTML 코드 간에 전환할 수 있습니다.
- GUI의 리치 텍스트 편집기에서 지원되지 않는 HTML 코드를 입력하려면 코드 보기로 전환하여 수동으로 HTML 코드를 입력합니다. 예를 들어 **`<img src>`** HTML 태그를 사용하여 외부 서버에 있는 이미지 파일에 대한 참조를 삽입하려는 경우 이렇게 할 수 있습니다.

관련 주제

- HTML 기반 텍스트 리소스 가져오기 및 내보내기, 624 페이지

HTML 기반 텍스트 리소스 가져오기 및 내보내기

텍스트 파일 HTML 기반 텍스트 리소스로 내보내거나 여기에서 가져올 수 있습니다. HTML 기반 텍스트 리소스를 파일로 내보내면 텍스트 리소스의 각 버전에 대해 다음 섹션이 파일에 포함됩니다.

- `[html_version]`
- `[text_version]`

이러한 섹션의 순서는 중요하지 않습니다.

예를 들어 내보낸 파일에는 다음 텍스트가 포함될 수 있습니다.

```
[html_version]
 <p>Sample <i>message.</i></p>
 [text_version]
 Sample message.
```

HTML 기반 텍스트 리소스를 내보내고 가져올 때에는 다음 규칙과 지침을 고려해 주십시오.

- HTML 버전에서 일반 텍스트 메시지가 자동으로 생성되는 HTML 기반 텍스트 리소스를 내보내면 내보낸 파일에는 `[text_version]` 섹션이 포함되지 않습니다.
- 텍스트 파일에서 가져오면, 텍스트 리소스 유형이 HTML 메시지를 지원하는 경우 [html_version] 섹션 아래의 HTML 코드는 생성된 텍스트 리소스에서 HTML 메시지로 변환됩니다. 마찬가지로 `[text_version]` 섹션 아래의 텍스트는 생성된 텍스트 리소스에서 일반 텍스트 메시지로 변환됩니다.
- 비어 있거나 존재하지 않는 `[html_version]` 섹션이 포함된 파일에서 HTML 기반 텍스트 리소스를 생성하기 위해 가져오는 경우 어플라이언스에서는 `[text_version]` 섹션의 텍스트를 사용하여 HTML 메시지와 일반 텍스트 메시지를 모두 만듭니다.

텍스트 리소스 사용

Text Resource(텍스트 리소스) 페이지 또는 textconfig CLI 명령을 사용하여 모든 유형의 텍스트 리소스가 동일한 방식으로 생성됩니다. 생성된 후에는 각 유형이 다른 방식으로 사용됩니다. 면책조항 및 알림 템플릿은 필터 및 리스너와 함께 사용되며, 안티바이러스 알림 템플릿은 메일 정책 및 안티바이러스 설정과 함께 사용됩니다.

관련 주제

- 면책조항 템플릿, 625 페이지
- 면책조항 스탬프 및 다중 인코딩, 628 페이지
- 알림 템플릿, 631 페이지
- 안티바이러스 알림 템플릿, 631 페이지
- 바운스 및 암호화 실패 알림 템플릿, 634 페이지
- 암호화 알림 템플릿, 636 페이지

면책조항 템플릿

어플라이언스는 리스너가 수신하는 일부 또는 모든 메시지에 대해 텍스트(머리글 또는 바닥글) 위나 아래에 기본 면책조항을 추가할 수 있습니다. 다음 방법을 사용하여 어플라이언스에서 메시지에 면책조항을 추가할 수 있습니다.

- 리스너, GUI 또는 `listenerconfig` 명령 사용(리스너를 통해 면책조항 텍스트 추가, 626 페이지 참조).
- 콘텐츠 필터 작업, `Add Disclaimer Text` 사용(콘텐츠 필터 작업, 293 페이지 참조).
- 메시지 필터 작업, `add-footer()` 사용("메시지 필터를 사용하여 이메일 정책 시행" 장 참조).
- 데이터 유출 방지 프로필 사용(데이터 유출 방지, 491 페이지 참조).
- 메시지가 피싱 또는 악성코드를 배포할 수 있음을 사용자에게 알리는 Outbreak Filter용 메시지 수정 사용(메시지 수정, 404 페이지 참조). 이 알림 유형에 추가되는 면책조항은 텍스트 위에 추가됩니다.

예를 들면 기업 내에서 전송되는 모든 메시지에 저작권 안내문, 프로모션 메시지 또는 면책조항을 추가할 수 있습니다.

면책조항 텍스트를 사용하기 전에 면책조항 템플릿을 만들어야 합니다. GUI의 Text Resources(텍스트 리소스) 페이지(텍스트 리소스 추가, 622 페이지 참조) 또는 `textconfig` 명령(AsyncOS for Cisco Email Security Appliance용 CLI 참조 설명서 참조)을 통해 사용할 텍스트 문자열 집합을 만들고 관리합니다.

관련 주제

- 필터를 통해 면책조항 추가, 626 페이지
- 리스너를 통해 면책조항 텍스트 추가, 626 페이지
- 면책조항 및 필터 작업 변수, 627 페이지

리스너를 통해 면책조항 텍스트 추가

면책조항 텍스트 리소스를 만들었으면 리스너에서 수신하는 메시지에 어떤 텍스트 문자열을 추가할지 선택합니다. 면책조항 텍스트는 메시지의 위나 아래에 추가할 수 있습니다. 이 기능은 퍼블릭(인바운드) 및 프라이빗(아웃바운드) 리스너에서 모두 사용 가능합니다.

텍스트 및 HTML로 구성된 메시지를 전송하는 경우(Microsoft Outlook에서는 이 유형의 메시지를 "멀티파트 대체"라고 함) 어플라이언스에서는 메시지의 두 부분에 면책조항 스탬프를 추가합니다. 그러나 메시지에 서명된 콘텐츠가 있는 경우, 수정은 서명을 무효화하므로 콘텐츠는 수정되지 않습니다. 대신 새 부분은 "Content-Disposition inline attachment"라는 면책조항 스탬프로 생성됩니다. 멀티파트 메시지에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 시행" 장에서 "메시지 본문 대 메시지 첨부 파일" 섹션을 참조해 주십시오.

필터를 통해 면책조항 추가

필터 작업 `add-footer()` 또는 콘텐츠 필터 작업 "Add Disclaimer Text"를 사용하여 사전 정의된 특정 텍스트 문자열을 메시지의 면책조항에 추가할 수도 있습니다. 예를 들어 다음 메시지 필터 규칙은 LDAP 그룹 "Legal"의 사용자들이 전송하는 모든 메시지에 `legal.disclaimer`라는 이름의 텍스트 문자열을 추가합니다.

```
Add-Disclaimer-For-Legal-Team:

if (mail-from-group == 'Legal')

{

add-footer('legal.disclaimer');
```

}

면책조항 및 필터 작업 변수

메시지 필터 작업 변수를 사용할 수도 있습니다(자세한 내용은 "메시지 필터를 사용하여 이메일 정책 시행" 장에서 "작업 변수" 참조).

면책조항 템플릿에 대해 다음 변수를 사용할 수 있습니다.

표 ***45:*** 안티바이러스 알림 변수

변수	교체
$To	메시지 To: 헤더로 교체됩니다(Envelope Recipient 아님).
$From	메시지 From: 헤더로 교체됩니다(Envelope Sender 아님).
$Subject	원본 메시지의 제목으로 교체됩니다.
$Date	MM/DD/YYYY 형식을 사용하여 현재 날짜로 교체됩니다.
$Time	현지 시간으로 교체됩니다(현지 표준 시간대).
$GMTimestamp	이메일 메시지의 Received: 줄에 나오는 대로 GMT를 사용하여 현재 시간 및 날짜로 교체됩니다.
$MID	메시지 식별을 위해 내부적으로 사용되는 MID(Message ID)로 교체됩니다. RFC822 "Message-Id" 값과 혼동해서는 안 됩니다(검색을 위해 $Header 사용).
$Group	메시지 주입 시 일치된 발송자 그룹의 이름으로 교체됩니다. 그룹에 이름이 없으면 ">Unknown<" 문자열이 삽입됩니다.
$Policy	메시지 주입 시 발송자에게 적용되는 HAT 정책의 이름으로 교체됩니다. 사전 정의된 정책 이름이 사용되지 않으면 ">Unknown<" 문자열이 삽입됩니다.
$Reputation	발신자의 SenderBase Reputation 점수로 교체됩니다. 평판 점수가 없으면 "None"으로 교체됩니다.
$filenames	메시지 어태치 파일 이름의 쉼표로 구분된 리스트로 교체됩니다.
$filetypes	메시지 어태치 파일 형식의 쉼표로 구분된 리스트로 교체됩니다.
$filesizes	메시지 어태치 파일 크기의 쉼표로 구분된 리스트로 교체됩니다.
$remotehost	메시지를 Email Security Appliance로 전송한 시스템의 호스트 이름으로 교체됩니다.
$AllHeaders	메시지 헤더로 교체됩니다.
$EnvelopeFrom	메시지의 Envelope Sender(봉투 발신자)(Envelope From, <MAIL FROM>)로 교체됩니다.

변수	교체
$Hostname	Email Security Appliance의 호스트 이름으로 교체됩니다.
$header['*string*']	원본 메시지에 일치하는 헤더가 포함된 경우 인용된 헤더의 값으로 교체됩니다. 큰따옴표를 사용할 수도 있습니다.
$enveloperecipients	메시지의 모든 Envelope Recipients(봉투 수신자)(Envelope To, <RCPT TO>)로 교체됩니다.
$bodysize	메시지의 크기로 교체됩니다(바이트 단위).
$FilterName	처리 중인 필터의 이름을 반환합니다.
$MatchedContent	검사 필터 규칙을 트리거한 콘텐츠를 반환합니다(body-contains 및 콘텐츠 사전 같은 필터 규칙 포함).
$DLPPolicy	위반된 이메일 DLP 정책 이름으로 교체됩니다.
$DLPSeverity	위반 심각도로 교체됩니다. "Low," "Medium," "High" 또는 "Critical."
$DLPRiskFactor	메시지 민감 재료의 위험 요인으로 교체됩니다(점수 0~100).
$threat_category	피싱, 바이러스, 사기, 악성코드 등 Outbreak Filter 위협 유형으로 교체됩니다.
$threat_type	Outbreak Filter 위협 범주의 하위 범주로 교체됩니다. 예를 들면 자선 사기, 재정적 피싱 시도, 가짜 거래 등이 있습니다.
$threat_description	Outbreak Filter 위협의 설명으로 교체됩니다.
$threat_level	메시지의 위협 레벨로 교체됩니다(점수 0~5).
$threat_verdict	Message Modification Threat Level(메시지 수정 위협 레벨) 임계값에 따라 Yes(예) 또는 No(아니요)로 교체됩니다. 메시지의 바이러스성 또는 비 바이러스성 위협 레벨이 메시지 수정 위협 레벨 임계값보다 크거나 같으면 이 변수의 값은 Yes(예)로 설정됩니다.

면책조항에서 메시지 필터 작업 변수를 사용하려면 GUI의 Text Resource(텍스트 리소스) 페이지 또는 **textconfig** 명령을 통해 메시지 면책조항을 만들고 변수를 참조해 주십시오.

add-footer() 작업은 바닥글을 인라인, 코딩된 UTF-8, QP(quoted printable) 첨부 파일로 추가하여 비 ASCII 텍스트를 지원합니다.

면책조항 스탬프 및 다중 인코딩

AsyncOS에는 서로 다른 문자 인코딩의 면책조항 스탬프가 작동하는 방식을 수정하는 데 사용되는 설정이 포함되어 있습니다. 기본적으로 AsyncOS는 추가하는 면책조항을 이메일 메시지 본문 내에 어태치하려고 시도합니다. 본문과 면책조항의 인코딩이 서로 다를 경우 동작을 구성하기 위해

`localeconfig` 명령 내에 구성된 설정을 사용할 수 있습니다. 이 설정을 이해하려면 이메일 메시지를 여러 부분으로 구성된 상태로 보는 것이 도움이 됩니다.

To: joe@example.com From: mary@example.com 제목: 안녕하세요!	헤더
<빈 줄>	
안녕하세요!	본문 부분
이 메시지는 검사되었습니다.	첫 번째 어태치 파일 부분
Example.zip	두 번째 어태치 파일 부분

첫 번째 빈 줄 뒤의 메시지 본문에는 여러 MIME 부분이 포함될 수 있습니다. 첫 번째 부분을 종종 "본문" 또는 "텍스트"라고 하며, 두 번째 및 그 이후의 부분을 종종 "어태치 파일"이라고 합니다.

면책조항은 이메일에 어태치 파일(위)로서 또는 본문의 일부로서 포함될 수 있습니다.

To: joe@example.com From: mary@example.com 제목: 안녕하세요!	헤더
<빈 줄>	
안녕하세요!	본문 부분
이 메시지는 검사되었습니다.	이제 본문에 포함된 면책조항
Example.zip	첫 번째 어태치 파일 부분

일반적으로 메시지 본문과 면책조항 사이에 인코딩이 일치하지 않으면 AsyncOS는 면책조항이 본문("inline"(인라인))에 포함되고 별도의 어태치 파일로 포함되지 않도록 동일한 인코딩의 전체 메시지를 메시지 본문으로 인코딩하려고 시도합니다. 다시 말해, 면책조항의 인코딩이 본문의 인코딩과 일치하거나 면책조항의 텍스트에 본문에 인라인으로 표시할 수 있는 문자가 포함되어 있으면 면책조항은 인라인으로 포함됩니다. 예를 들면 US-ASCII 문자만 포함하는, ISO-8859-1로 인코딩된 면책조항이 있을 수 있습니다. 이러한 면책조항은 아무 문제 없이 "인라인"으로 표시됩니다.

그러나 면책조항을 본문과 결합할 수 없는 경우 `localeconfig` 명령을 사용하여, 본문 텍스트를 면책조항의 인코딩과 일치시켜 면책조항을 메시지 본문에 포함하기 위해 프로모션 또는 변환을 시도하도록 AsyncOS를 구성할 수 있습니다.

```
example.com> localeconfig

Behavior when modifying headers: Use encoding of message body
```

```
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]> setup

If a header is modified, encode the new header in the same encoding as the message body?
(Some MUAs incorrectly handle headers encoded in a different encoding than the body.
However, encoding a modified header in the same encoding as the message body may cause
certain
characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or
modified,
impose the encoding of the body on the header during processing and final representation
of the message?
(Many MUAs create non-RFC-compliant headers that are then handled in an undefined way.
Some MUAs handle headers encoded in character sets that differ from that of the main body
in an incorrect way.
Imposing the encoding of the body on the header may encode the header more precisely.
This will be used to interpret the content of headers for processing, it will not modify
or rewrite the
header unless that is done explicitly as part of the processing.) [Y]>

Disclaimers (as either footers or headings) are added in-line with the message body whenever
 possible.
However, if the disclaimer is encoded differently than the message body, and if imposing a
 single encoding
will cause loss of characters, it will be added as an attachment. The system will always
try to use the
message body's encoding for the disclaimer. If that fails, the system can try to edit the
message body to
use an encoding that is compatible with the message body as well as the disclaimer. Should
 the system try to
re-encode the message body in such a case? [Y]>

If the disclaimer that is added to the footer or header of the message generates an error
when decoding the message body,
it is added at the top of the message body. This prevents you to rewrite a new message
content that must merge with
the original message content and the header/footer-stamp. The disclaimer is now added as
an additional MIME part
that displays only the header disclaimer as an inline content, and the rest of the message
 content is split into
separate email attachments. Should the system try to ignore such errors when decoding the
message body? [N]>

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body
is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]>
```

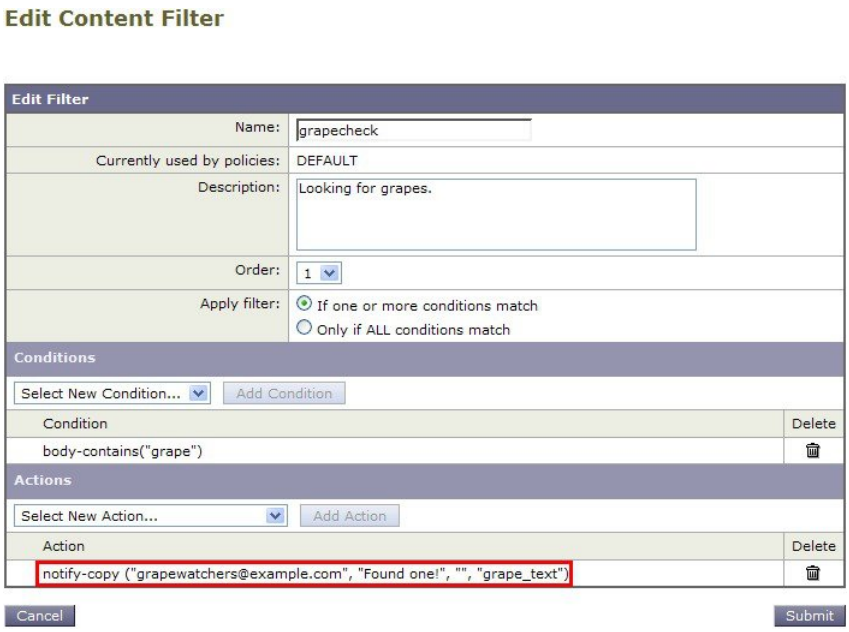
`localeconfig` 명령에 대한 자세한 내용은 "메일을 수신하도록 어플라이언스 구성" 장을 참고하십시오.

알림 템플릿

알림 템플릿은 **`notify()`** 및 **`notify-copy()`** 필터 작업과 함께 사용됩니다. 알림 템플릿에는 안티바이러스 알림에 사용된 안티바이러스 관련 변수를 비롯한 비 ascii 텍스트 및 작업 변수가 포함될 수 있습니다("메시지 필터를 사용하여 이메일 정책 시행" 장에서 "작업 변수" 참조). 예를 들면 원본 메시지에서 헤더를 포함하기 위해 **`$Allheaders`** 작업 변수를 사용할 수 있습니다. 알림을 위한 From: 주소 구성에 대한 자세한 내용은 어플라이언스 생성 메시지에 대한 반환 주소 구성, 960 페이지 섹션을 참조해 주십시오.

알림 템플릿을 만들었으면 콘텐츠 및 메시지 필터에서 이를 참조할 수 있습니다. 다음 그림은 **`notify-copy()`** 필터 작업이 "grape_text" 알림을 "grapewatchers@example.com"으로 전송하도록 설정된 콘텐츠 필터를 보여줍니다.

그림 ***40:*** 콘텐츠 필터의 알림 예



안티바이러스 알림 템플릿

두 가지 유형의 안티바이러스 알림 템플릿이 있습니다.

- 안티바이러스 알림 템플릿. 원본 메시지가 바이러스 알림에 어태치되지 않은 경우 안티바이러스 알림 템플릿이 사용됩니다.
- 안티바이러스 컨테이너 템플릿. 원본 메시지가 어태치 파일로 전송되는 경우 컨테이너 템플릿이 사용됩니다.

안티바이러스 알림 템플릿은 필터 대신 안티바이러스 엔진과 사용되는 경우를 제외하고는 기본적으로 알림 템플릿과 동일한 방식으로 사용됩니다. 메일 정책을 수정하는 한편 전송할 맞춤형 알림을 지

정할 수 있습니다. 안티바이러스 알림용 From: 주소를 구성할 수 있습니다. 자세한 내용은 어플라이언스 생성 메시지에 대한 반환 주소 구성, 960 페이지를 참조하십시오.

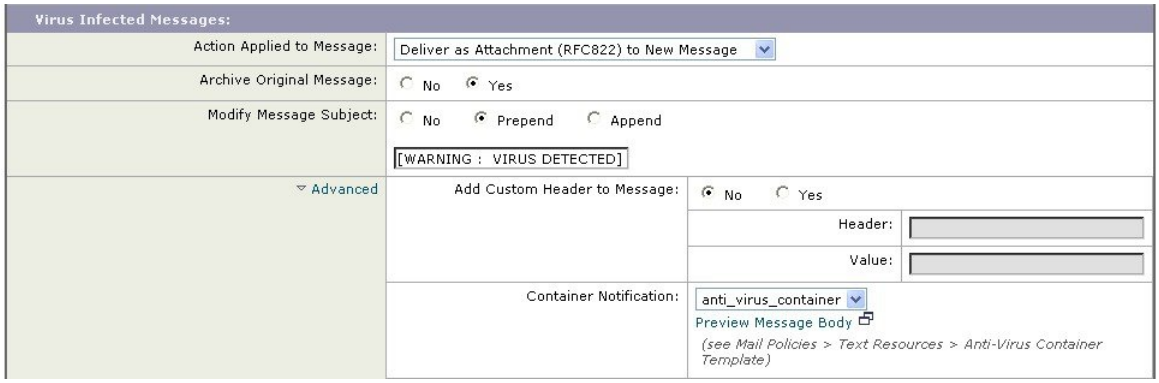
관련 주제

- 맞춤형 안티바이러스 알림 템플릿, 632 페이지

맞춤형 안티바이러스 알림 템플릿

다음 그림은 맞춤형 안티바이러스 알림이 지정된 메일 정책을 보여줍니다.

그림 ***41:*** 메일 정책의 안티바이러스 컨테이너 템플릿 알림 예



관련 주제

- 안티바이러스 알림 변수, 632 페이지

안티바이러스 알림 변수

안티바이러스 알림을 만들 때 다음 표에 나열된 알림 변수를 사용할 수 있습니다.

표 ***46:*** 안티바이러스 알림 변수

변수	교체
$To	메시지 To: 헤더로 교체됩니다(Envelope Recipient 아님).
$From	메시지 From: 헤더로 교체됩니다(Envelope Sender 아님).
$Subject	원본 메시지의 제목으로 교체됩니다.
$AV_VIRUSES	메시지에서 발견되는 모든 바이러스 리스트로 교체됩니다. “Unix/Apache.Trojan”, “W32/Bagel-F”

변수	교체
$AV_VIRUS_TABLE	각 부분에서 MIME-Part/Attachment 이름 및 바이러스의 테이블로 교체됩니다. “HELLO.SCR” : “W32/Bagel-F” <unnamed part of the message> : “Unix/Apache.Trojan”
$AV_VERDICT	안티바이러스 판정으로 교체됩니다.
$AV_DROPPED_TABLE	삭제된 어태치 파일의 테이블로 교체됩니다. 각 행은 부분 또는 파일 이름, 그리고 그 뒤에 해당 부분과 연결된 바이러스 리스트로 구성됩니다. “HELLO.SCR” : “W32/Bagel-f”, “W32/Bagel-d” “Love.SCR” : “Netsky-c”, “W32/Bagel-d”
$AV_REPAIRED_VIRUSES	발견되고 복구된 모든 바이러스 리스트로 교체됩니다.
$AV_REPAIRED_TABLE	발견되고 복구된 모든 부분 및 바이러스의 테이블로 교체됩니다. “HELLO.SCR” : “W32/Bagel-F”
$AV_DROPPED_PARTS	삭제된 파일 이름의 리스트로 교체됩니다. “HELLO.SCR”, “CheckThisOut.exe”
$AV_REPAIRED_PARTS	복구된 부분 또는 파일 이름의 리스트로 교체됩니다.
$AV_ENCRYPTED_PARTS	암호화된 부분 또는 파일 이름의 리스트로 교체됩니다.
$AV_INFECTED_PARTS	바이러스가 포함된 파일에 대한 파일 이름의 쉼표로 구분된 리스트로 교체됩니다.
$AV_UNSCANNABLE_PARTS	검사하지 못한 부분 또는 파일 이름의 리스트로 교체됩니다.
$Date	MM/DD/YYYY 형식을 사용하여 현재 날짜로 교체됩니다.
$Time	현지 시간으로 교체됩니다(현지 표준 시간대).
$GMTimestamp	이메일 메시지의 Received: 줄에 나오는 대로 GMT를 사용하여 현재 시간 및 날짜로 교체됩니다.
$MID	메시지 식별을 위해 내부적으로 사용되는 MID(Message ID)로 교체됩니다. RFC822 "Message-Id" 값과 혼동해서는 안 됩니다(검색을 위해 $Header 사용).
$Group	메시지 주입 시 일치된 발송자 그룹의 이름으로 교체됩니다. 그룹에 이름이 없으면 ">Unknown<" 문자열이 삽입됩니다.
$Policy	메시지 주입 시 발송자에게 적용되는 HAT 정책의 이름으로 교체됩니다. 사전 정의된 정책 이름이 사용되지 않으면 ">Unknown<" 문자열이 삽입됩니다.

변수	교체
$Reputation	발신자의 SenderBase Reputation 점수로 교체됩니다. 평판 점수가 없으면 "None"으로 교체됩니다.
$filenames	메시지 어태치 파일 이름의 쉼표로 구분된 리스트로 교체됩니다.
$filetypes	메시지 어태치 파일 형식의 쉼표로 구분된 리스트로 교체됩니다.
$filesizes	메시지 어태치 파일 크기의 쉼표로 구분된 리스트로 교체됩니다.
$remotehost	메시지를 Email Security Appliance로 전송한 시스템의 호스트 이름으로 교체됩니다.
$AllHeaders	메시지 헤더로 교체됩니다.
$EnvelopeFrom	메시지의 Envelope Sender(봉투 발신자)(Envelope From, <MAIL FROM>)로 교체됩니다.
$Hostname	Email Security Appliance의 호스트 이름으로 교체됩니다.

참고 변수 이름은 대/소문자를 구분하지 않습니다. 예를 들어 텍스트 리소스에서 "$to" 지정은 "$To" 지정과 같습니다. 원본 메시지에서 "AV_" 변수가 비어 있으면 <None> 문자열이 대체됩니다.

텍스트 리소스가 정의되었으면 **Mail Policies(**메일 정책**(** > **Incoming/Outgoing Mail Policies(**수신/발신 메일 정책**)** > **Edit Anti-Virus Settings(**안티바이러스 설정 수정**)** 페이지 또는 **`policyconfig -> edit -> antivirus`** 명령을 사용하여, 원본 메시지를 Repaired, Unscannable, Encrypted 또는 Virus Positive 메시지에 대한 RFC 822 어태치 파일로 포함할지를 지정합니다. 자세한 내용은 맞춤형 알림 전송, 347 페이지를 참조하십시오.

바운스 및 암호화 실패 알림 템플릿

바운스 및 암호화 실패 알림 템플릿은 바운스 알림 및 메시지 암호화 실패 알림과 함께 사용된다는 점을 제외하고는 기본적으로 알림 템플릿과 동일한 방법으로 사용됩니다. 바운스 프로필을 수정하는 동안 전송할 맞춤형 바운스 알림, 그리고 암호화 프로필을 수정하는 동안 전송할 맞춤형 메시지 암호화 실패 알림을 지정할 수 있습니다.

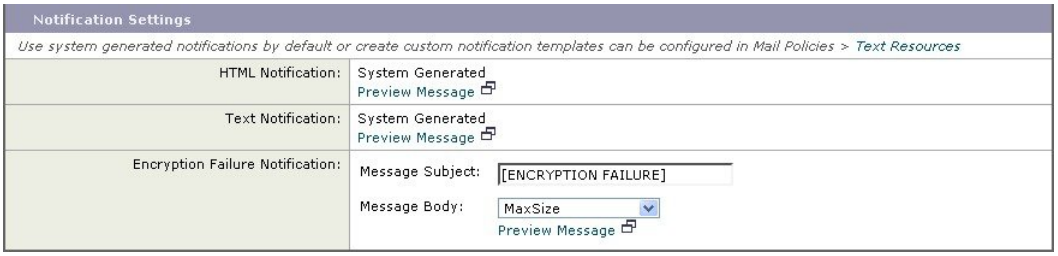
다음 그림은 바운스 프로필에 지정된 바운스 알림 템플릿을 보여줍니다.

그림 **42:** 바운스 프로필의 바운스 알림 템플릿

참고 맞춤형 템플릿을 사용하려면 RFC-1891 DSN을 사용해야 합니다.

다음 그림은 암호화 프로필에 지정된 암호화 실패 템플릿을 보여줍니다.

그림 **43:** 암호화 프로필의 암호화 실패 알림 예



관련 주제

- 바운스 및 암호화 실패 알림 변수, 635 페이지

바운스 및 암호화 실패 알림 변수

바운스 또는 암호화 실패 알림을 만들 때 다음 표에 나열된 알림 변수를 사용할 수 있습니다.

표 **47:** 바운스 알림 변수

변수	교체
$Subject	원본 메시지의 제목.
$Date	MM/DD/YYYY 형식을 사용하여 현재 날짜로 교체됩니다.
$Time	현지 시간으로 교체됩니다(현지 표준 시간대).
$GMTimeStamp	이메일 메시지의 Received: 줄에 나오는 대로 GMT를 사용하여 현재 시간 및 날짜로 교체됩니다.
$MID	메시지 식별을 위해 내부적으로 사용되는 MID(Message ID)로 교체됩니다. RFC822 "Message-Id" 값과 혼동해서는 안 됩니다(검색을 위해 $Header 사용).

변수	교체
$BouncedRecipient	바운스된 수신자 주소
$BounceReason	이 알림의 이유
$remotehost	메시지를 Email Security Appliance로 전송한 시스템의 호스트 이름으로 교체됩니다.

암호화 알림 템플릿

암호화 알림 템플릿은 아웃바운드 이메일을 암호화하기 위해 Cisco Email Encryption을 구성할 때 사용됩니다. 알림은 수신자에게 암호화된 메시지가 수신되었음을 알리고 이를 읽기 위한 지침을 제공합니다. 암호화된 메시지와 함께 전송할 맞춤형 암호화 알림을 지정할 수 있습니다. 암호화 프로필을 만들 때 HTML과 텍스트 암호화 알림을 모두 지정합니다. 따라서 맞춤형 프로필을 만들 때 텍스트와 HTML 알림을 모두 만들어야 합니다.

26 장

SMTP 서버를 사용하여 수신자 검증

이 장에는 다음 섹션이 포함되어 있습니다.

SMTP Call-Ahead 수신자 검증 개요

SMTP call-ahead 수신자 검증 기능은 수신자에 대한 수신 메일을 수락하기 전에 외부 SMTP 서버에 쿼리합니다. LDAP 수락 또는 RAT(Recipient Access Table)를 사용할 수 없을 때 수신자를 검증하려면 이 기능을 사용할 수 있습니다. 예를 들어, 여러 사서함에 대한 메일을 호스트하며 각각 별도의 도메인을 사용하는데, LDAP 인프라에서 각 수신자 검증을 위해 LDAP 서버에 쿼리하는 것을 허용하지 않는 경우를 가정해볼 수 있습니다. 이 경우 Email Security Appliance는 SMTP 서버에 쿼리하고, SMTP 대화를 계속 진행하기 전에 수신자를 검증합니다.

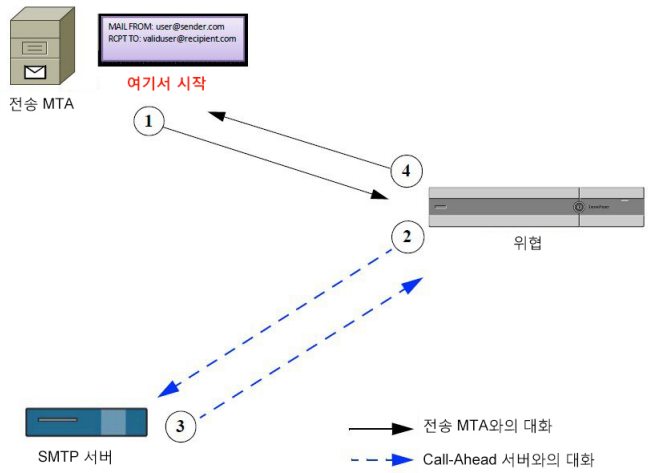
메시지에서 잘못된 수신자에 대한 처리를 줄이려면 SMTP call-ahead 수신자 검증을 사용할 수 있습니다. 일반적으로 잘못된 수신자에 대한 메시지는 삭제되기 전에 작업 대기열을 통과하게 됩니다. 또는 잘못된 메시지는 추가 처리가 필요 없도록 이메일 파이프라인의 수신 부분 중에 삭제되거나 반송될 수도 있습니다.

SMTP Call-Ahead 수신자 검증 워크플로

SMTP call-ahead 수신자 검증을 구성할 경우 Email Security Appliance는 전송 MTA와의 SMTP 대화를 일시 중단하고 수신자 확인을 위해 SMTP 서버에 "미리 연락(call ahead)"합니다. SMTP 서버에 쿼리하면 SMTP 서버의 응답이 Email Security Appliance로 반환되며, 구성한 설정에 따라 메일을 수락할 수도 있고 코드 및 사용자 지정 응답으로 연결을 삭제할 수도 있습니다.

다음 그림은 SMTP call-head 검증 대화의 기본 워크플로를 보여줍니다.

그림 ***44: SMTP Call Ahead*** 서버 대화 워크플로



1. 전송 MTA는 SMTP 대화를 시작합니다.
2. Email Security Appliance는 SMTP 대화를 일시 중단하는 한편 수신자 *validuser@recipient.com*의 확인을 위해 SMTP 서버에 쿼리를 전송합니다.

참고 SMTP 경로 또는 LDAP 라우팅 쿼리가 구성되어 있으면 SMTP 서버에 쿼리하는 데 해당 경로가 사용됩니다.

3. SMTP 서버는 Email Security Appliance에 쿼리 응답을 반환합니다.
4. Email Security Appliance는 SMTP 대화를 다시 시작하고 전송 MTA에 응답을 전송하여, SMTP 서버 응답(그리고 SMTP Call-Ahead 프로필에 구성한 설정)을 기반으로 대화를 계속 진행하도록 허용하거나 연결을 삭제합니다.

이메일 파이프라인의 프로세스 순서 때문에, 특정 수신자에 대한 메시지가 RAT에 의해 거부되면 SMTP call-ahead 수신자 검증이 발생하지 않습니다. 예를 들어 *example.com*에 대한 메일만 수락하도록 RAT에 지정한 경우, *recipient@domain2.com*에 대한 메일은 SMTP call-ahead 수신자 검증이 발생하기 전에 거부됩니다.

참고 HAT에서 DHAP(Directory Harvest Attack Prevention)를 구성한 경우 SMTP call-ahead 서버 거부는 시간당 유효하지 않은 최대 수신자 수에 포함된 거부 수의 일부라는 점에 유의하십시오. 추가 SMTP 서버 거부를 고려하여 이 수치를 조정해야 할 수 있습니다. DHAP에 대한 자세한 내용은 "이메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

외부 SMTP 서버를 사용하여 수신자를 검증하는 방법

	수행해야 할 작업	추가 정보
1단계	어플라이언스를 SMTP 서버에 연결하고 서버의 응답을 해석하는 방법을 결정합니다.	Call-Ahead 서버 프로필 구성, 639 페이지
2단계	SMTP 서버를 사용하여 수신자를 검증하도록 퍼블릭 리스너를 구성합니다.	SMTP 서버를 통해 오는 수신 메일을 검증하도록 리스너 활성화, 642 페이지
3단계	(선택 사항) 메일을 다른 호스트로 라우팅할 때 사용할 SMTP 서버를 확인하기 위해 LDAP 라우팅 쿼리를 업데이트합니다.	LDAP 라우팅 쿼리 설정 구성, 642 페이지
4단계	(선택 사항) 특정 수신자에 대한 call-ahead 검증을 우회하도록 어플라이언스를 구성합니다.	특정 사용자 또는 그룹에 대해 SMTP Call-Ahead 검증 우회, 644 페이지

관련 주제

- Call-Ahead 서버 프로필 구성, 639 페이지

Call-Ahead 서버 프로필 구성

SMTP Call-Ahead 서버 프로필을 구성할 때 Email Security Appliance가 SMTP 서버와 연결되는 방법 및 SMTP 서버에서 반환되는 응답을 해석하는 방법을 결정하는 설정을 지정합니다.

단계 **1** **Network**(네트워크) > **SMTP Call-Ahead**를 클릭합니다.

단계 **2** **Add Profile**(프로필 추가)을 클릭합니다.

단계 **3** 프로필의 설정을 입력합니다. 자세한 내용은 표 - *SMTP Call-Ahead* 서버 프로파일 설정을 참고하십시오.

단계 **4** 프로필의 고급 설정을 구성합니다. 자세한 내용은 표 - *SMTP Call-Ahead* 서버 프로파일 고급 설정을 참고하십시오.

단계 **5** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

- SMTP Call-Ahead 서버 프로필 설정, 640 페이지
- Call Ahead 서버 응답, 641 페이지

SMTP Call-Ahead 서버 프로필 설정

SMTP Call-Ahead 서버 프로필을 구성할 때 Email Security Appliance가 SMTP 서버와 연결되는 방법을 결정하는 설정을 구성해야 합니다.

표 ***48: SMTP Call-Ahead*** 서버 프로필 설정

설정	설명
Profile Name(프로필 이름)	Call-Ahead 서버 프로필의 이름.
Call-Ahead Server Type(Call-Ahead 서버 유형)	Call-Ahead 서버에 연결하기 위한 다음 방법 중 하나를 선택합니다. • **Use Delivery Host(**전달 호스트 사용**)**. 전달 이메일 주소용 호스트가 SMTP call-ahead 쿼리에 사용되도록 지정하려면 이 옵션을 선택합니다. 예를 들어 메일 수신자 주소가 *recipient@example.com*이면 *example.com*과 연결된 SMTP 서버에 대해 SMTP 쿼리가 실행됩니다. SMTP 경로 또는 LDAP 라우팅 쿼리를 구성한 경우 쿼리할 SMTP 서버를 결정하는 데 이러한 경로가 사용됩니다. LDAP 라우팅 쿼리 구성에 대한 자세한 내용은 LDAP 라우팅 쿼리 설정 구성, 642 페이지 섹션을 참조하십시오. • **Static Call-Ahead Server(**고정 **Call-Ahead** 서버**)**. 쿼리할 call-ahead 서버의 고정 리스트를 만들려면 이 옵션을 사용합니다. Call-ahead 서버의 이름과 위치가 자주 변경되지 않을 것으로 예상되는 경우 이 옵션을 사용할 수 있습니다. 이 옵션을 선택하면 Email Security Appliance는 나열된 첫 번째 고정 call-ahead 서버로 시작하여 라운드로빈 방식으로 호스트에 쿼리합니다. 참고 고정 call-ahead 서버 유형을 선택하는 경우 쿼리에 SMTP 경로가 적용되지 않습니다. 대신 고정 서버의 call-ahead IP 주소를 가져오기 위해 MX 조회와 A 조회가 차례로 수행됩니다.
Static Call-Ahead Servers(고정 Call-Ahead 서버)	고정 call-ahead 서버 유형을 사용하도록 선택하는 경우 이 필드에 호스트와 포트 조합의 리스트를 입력합니다. 다음 구문을 사용하여 서버와 포트를 나열합니다. ironport.com:25 입력 항목이 여럿인 경우에는 쉼표로 구분하십시오.

다음 표에서는 서버 프로파일 고급 설정에 대해 설명합니다.

표 *49: SMTP Call-Ahead* 서버 프로필 고급 설정

설정	설명
인터페이스	SMTP 서버와 SMTP 대화를 시작하기 위해 사용되는 인터페이스. Management 인터페이스 또는 Auto를 선택합니다. Auto를 선택하는 경우 Email Security Appliance는 사용할 인터페이스를 자동으로 탐지하려고 시도합니다. Cisco IronPort 인터페이스는 다음과 같은 방법으로 SMTP 서버에 연결하려고 시도합니다. • 구성된 인터페이스 중 하나와 동일한 서브넷에 call-ahead 서버가 있으면 일치하는 인터페이스에 의해 연결이 시작됩니다. • 구성된 SMTP 경로는 쿼리 라우팅에 사용됩니다. • 그렇지 않으면 기본 게이트웨이와 동일한 서브넷에 있는 인터페이스가 사용됩니다.
MAIL FROM Address(MAIL FROM 주소)	SMTP 서버와의 SMTP 대화에 사용될 MAIL FROM: 주소.
Validation Request Timeout(검증 요청 시간 초과)	SMTP 서버에서 결과를 기다리기 위한 시간(초). 이 시간 초과 값은 여러 call-ahead 서버 접속에 관여할 수 있는 단일 수신자 검증 요청에 대한 것입니다. Call Ahead 서버 응답, 641 페이지를 참조하십시오.
Validation Failure Action(검증 실패 작업)	수신자 검증 요청이 실패할 때 수행할 작업(시간 초과, 서버 실패, 네트워크 문제 또는 알 수 없는 응답 때문에). Email Security Appliance에서 여러 응답을 처리하는 방법을 구성할 수 있습니다. Call Ahead 서버 응답, 641 페이지를 참조하십시오.
Temporary Failure Action(일시적인 실패 작업)	수신자 검증 요청이 일시적으로 실패할 때(그리고 원격 SMTP 서버에서 4xx 응답이 반환될 때) 수행할 작업. 이는 사서함이 꽉 찼거나, 사서함 또는 서비스를 사용할 수 없을 때 발생할 수 있습니다. Call Ahead 서버 응답, 641 페이지를 참조하십시오.
Max. Recipients per Session(세션당 최대 수신자 수)	단일 SMTP 세션에서 검증할 최대 수신자 수. 1~25,000개 세션을 지정합니다.
Max. Connections per Server(서버당 최대 연결 수)	단일 call-ahead SMTP 서버에 대한 최대 연결 수. 1~100개 연결을 지정합니다.
캐시	SMTP 응답을 위한 캐시 크기. 100~1,000,000개 항목을 지정합니다.
Cache TTL(캐시 TTL)	캐시에 있는 항목의 TTL(time-to-live) 값. 이 필드의 기본값은 900초입니다. 60~86,400초를 지정합니다.

Call Ahead 서버 응답

SMTP 서버는 다음 응답을 반환할 수 있습니다.

- **2xx**: Call-ahead 서버에서 2로 시작하는 SMTP 코드가 수신되면 수신자가 수락됩니다. 예를 들어 응답 250은 메일링 작업을 계속 진행하도록 허용합니다.
- **4xx**: 4로 시작하는 SMTP 코드는 SMTP 요청을 처리하는 동안 일시적인 장애가 발생했음을 의미합니다. 나중에 재시도하면 성공적으로 처리될 수 있습니다. 예를 들어 응답 451은 요청한 작업이 취소되었거나 처리 중에 로컬 오류가 발생했음을 의미합니다.
- **5xx**: 5로 시작하는 SMTP 코드는 SMTP 요청을 처리하는 동안 영구적인 장애가 발생했음을 의미합니다. 예를 들어 응답 550은 요청한 작업이 수행되지 않았거나 사서함을 사용할 수 없음을 의미합니다.
- **Timeout(**시간 초과**).** Call-ahead 서버에서 응답이 반환되지 않는 경우 시간 초과가 발생하기 전에 얼마 동안 재시도를 시도할지를 구성할 수 있습니다.
- **Connection error(**연결 오류**)**. Call-ahead 서버에 대한 연결이 실패할 경우 수신자 주소에 대한 연결을 수락할지 아니면 거절할지를 구성할 수 있습니다.
- 고객 응답. 맞춤형 SMTP 응답(코드 및 텍스트)과 검증 실패 및 일시적인 장애에 대한 연결을 거부하도록 구성할 수 있습니다.

SMTP 서버를 통해 오는 수신 메일을 검증하도록 리스너 활성화

SMTP Call-Ahead 서버 프로필을 만들었으면 리스너에서 활성화하여, 리스너가 SMTP 서버를 통해 오는 수신 메일을 검증하도록 해야 합니다. 퍼블릭 리스너에 대해서는 수신자 검증이 필요하지 않으므로 SMTP call-ahead 기능은 퍼블릭 리스너에서만 사용 가능합니다.

단계 **1** **Network(**네트워크**)** > **Listeners(**리스너**)**로 이동합니다.

단계 **2** SMTP call-ahead 기능을 활성화할 리스너의 이름을 클릭합니다.

단계 **3** **SMTP Call Ahead Profile(SMTP Call Ahead** 프로필**)** 필드에서 활성화할 SMTP Call-Ahead 프로필을 선택합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

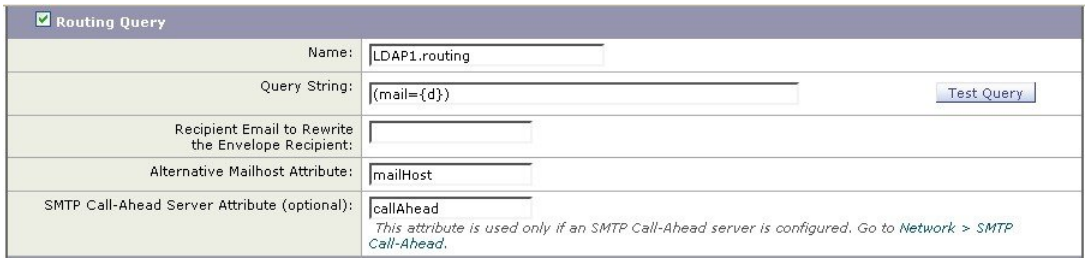
LDAP 라우팅 쿼리 설정 구성

LDAP 라우팅 쿼리를 사용하여 메일을 다른 메일 호스트로 라우팅하면 AsyncOS에서는 Alternate Mailhost Attribute를 사용하여 쿼리할 SMTP 서버를 결정합니다. 그러나 이렇게 하지 않으려는 경우도 있습니다. 예를 들어 다음 스키마의 경우 메일 호스트 특성(mailHost)에 나열된 SMTP 주소가 call-ahead SMTP 서버 특성(callAhead)에 나열된 것과 다릅니다.

```
dn: mail=cisco.com, ou=domains
mail: cisco.com
mailHost: smtp.mydomain.com
policy: ASAV
callAhead: smtp2.mydomain.com,smtp3.mydomain.com:9025
```

이 경우 **SMTP Call-Ahead** 필드를 사용하여, SMTP call-ahead 쿼리를 callAhead 특성에 나열된 서버로 전환하는 라우팅 쿼리를 만들 수 있습니다. 예를 들면 다음과 같은 특성의 라우팅 쿼리를 만들 수 있습니다.

그림 ***45: SMTP Call-Ahead***에 대해 구성된 ***LDAP*** 라우팅 쿼리



이 쿼리에서 {d}는 수신자 주소의 도메인 부분을 나타내고 SMTP Call-Ahead Server Attribute는 call-ahead 서버의 값 및 쿼리에 사용해야 할 포트의 값을 반환합니다(포트 9025의 smtp2.mydomain.com, smtp3.mydomain.com).

참고 이 예는 LDAP 라우팅 쿼리를 사용하여 SMTP call-ahead 쿼리를 올바른 SMTP 서버로 전환할 수 있도록 쿼리를 구성하는 한 방법에 불과합니다. 이 예에서 설명한 쿼리 문자열 또는 특정 LDAP 특성을 반드시 사용해야 하는 것은 아닙니다.

SMTP Call-Ahead 쿼리 라우팅

SMTP call-ahead 쿼리를 라우팅하면 AsyncOS는 다음 순서로 정보를 확인합니다.

1. 도메인 이름을 확인합니다.
2. LDAP 라우팅 쿼리를 확인합니다.
3. SMTP 경로를 확인합니다.
4. DNS 조회를 수행합니다(MX 조회와 A 조회를 차례로 수행).

도메인에 대해 구성된 LDAP 라우팅 쿼리 또는 SMTP 경로가 없는 경우 이전 상태의 결과가 다음 단계로 전달됩니다. 어느 경우든 SMTP 경로가 없으면 DNS 조회가 수행됩니다.

SMTP call-ahead 쿼리에 대해 LDAP 라우팅 쿼리를 사용하며 SMTP 경로도 구성되어 있는 경우 라우팅 동작은 라우팅 쿼리에 의해 반환되는 값에 따라 달라집니다.

- LDAP 라우팅 쿼리가 포트 없는 단일 호스트 이름을 반환하면 SMTP call-ahead 쿼리는 SMTP 경로를 적용합니다. SMTP 경로가 호스트 이름으로 대상 호스트만 나열하는 경우 SMTP 서버의 IP 주소를 가져오기 위해 DNS 조회가 수행됩니다.
- LDAP 라우팅 쿼리가 포트 있는 단일 호스트 이름을 반환하면 SMTP 경로가 사용되지만, SMTP 경로에 지정된 포트에 대해 LDAP 쿼리에 의해 반환되는 포트가 사용됩니다. SMTP 경로가 호스트 이름으로 대상 호스트만 나열하는 경우 SMTP 서버의 IP 주소를 가져오기 위해 DNS 조회가 수행됩니다.

- LDAP 라우팅 쿼리가 포트 있는 또는 없는 여러 호스트를 반환하면 SMTP 경로가 적용되지만, SMTP 경로에 있는 포트에 대해 LDAP 라우팅 쿼리에 의해 반환된 포트가 사용됩니다. SMTP 경로가 호스트 이름으로 대상 호스트만 나열하는 경우 SMTP 서버의 IP 주소를 가져오기 위해 DNS 조회가 수행됩니다.

특정 사용자 또는 그룹에 대해 SMTP Call-Ahead 검증 우회

리스너에서 SMTP call-ahead 검증을 활성화하되 특정 사용자 또는 그룹에 대한 SMTP call-ahead 검증을 건너뛰고자 할 수 있습니다.

SMTP call-ahead 쿼리 중 메일이 지연되어서는 안 되는 수신자에 대해서는 SMTP call-ahead 검증을 건너뛰고자 할 수 있습니다. 예를 들면 유효하다는 것을 알고 있으며 즉각적인 주의가 필요한 고객 서비스 별칭에 대해 RAT 항목을 추가할 수 있습니다.

GUI를 통해 SMTP call-ahead 검증을 우회하려면 RAT 항목을 추가하거나 수정할 때 **Bypass SMTP Call-Ahead(SMTP Call-Ahead** 우회**)**를 선택합니다

27 장

다른 MTA와의 통신 암호화

이 장에는 다음 섹션이 포함되어 있습니다.

다른 MTA와의 통신 암호화 개요

엔터프라이즈 게이트웨이(또는 Message Transfer Agent, 즉 MTA)는 일반적으로 인터넷을 통해 "있는 그대로" 통신합니다. 즉, 통신이 암호화되지 않습니다. 몇몇 시나리오에서 악의적인 에이전트가 발신자 또는 수신자 모르게 이 통신을 가로챌 수 있습니다. 서드파티에서 통신을 모니터링할 수 있으며 심지어 변경할 수도 있습니다.

TLS(Transport Layer Security)는 SSL(Secure Socket Layer) 기술의 개선된 버전으로, 인터넷을 통해 SMTP 대화를 암호화하는 데 널리 사용되는 메커니즘입니다. AsyncOS는 RFC 3207(RFC 2487을 대신함)에 설명된 대로, SMTP(Secure SMTP over TLS)로 STARTTLS를 확장하도록 지원합니다.

AsyncOS에서 TLS를 구현하면 암호화를 통해 개인정보를 보호할 수 있습니다. X.509 인증서 및 개인 키를 인증 기관 서비스에서 가져오거나 어플라이언스에서 사용할 자체 서명 인증서를 만들 수 있습니다. AsyncOS는 퍼블릭 및 프라이빗 리스너에 대한 별도의 TLS 인증서, 인터페이스에서의 보안 HTTP(HTTPS) 관리 액세스, LDAP 인터페이스, 모든 발신 TLS 연결을 지원합니다.

관련 주제

- TLS를 사용하여 SMTP 대화를 암호화하는 방법, 645 페이지

TLS를 사용하여 SMTP 대화를 암호화하는 방법

TLS를 사용하여 SMTP 대화를 암호화하는 방법

	수행해야 할 작업	추가 정보
1단계	알려진 인증 기관에서 X.509 인증서 및 개인 키를 가져옵니다.	인증서 작업, 646 페이지
2단계	Email Security Appliance에 인증서를 설치합니다.	다음 중 하나로 인증서 설치 • 셀프 서명 인증서 만들기 , 648 페이지 • 인증서 가져오기 , 650 페이지
3단계	메시지 수신, 메시지 전달 또는 둘 모두를 위해 TLS를 활성화합니다.	• 인증서의 HAT에서 TLS 활성화, 651 페이지 • 전달 시 TLS 및 인증서 확인 활성화, 654 페이지
4단계	(선택 사항) 도메인의 자격 증명을 설정하기 위해 어플라이언스가 원격 도메인에서 온 인증서를 확인하는 데 사용하는 신뢰할 수 있는 인증 기관의 목록을 사용자 지정합니다.	인증 기관 목록 관리, 661 페이지
5단계	(선택 사항) TLS 연결을 요구하는 도메인에 메시지를 전달할 수 없을 때 알림을 전송하도록 Email Security Appliance를 구성합니다.	필수 TLS 연결 실패 시 알림 전송, 657 페이지

인증서 작업

TLS를 사용하려면 Email Security Appliance에 수신 및 전달을 위한 X.509 인증서 및 일치하는 개인 키가 필요합니다. SMTP 수신 및 전달 모두에 동일한 인증서를 사용하고, 인터페이스의 HTTPS 서비스, LDAP 인터페이스 및 대상 도메인에 대한 모든 발신 TLS 연결에 서로 다른 인증서를 사용할 수 있습니다. 또는 이 모두에 단일 인증서를 사용할 수도 있습니다.

전체 인증서 목록을 보려면 웹 인터페이스에서 Network(네트워크) > Certificates(인증서) 페이지를 사용하거나 CLI에서 certconfig를 사용하여 인증서를 구성한 후 print 명령을 사용할 수 있습니다. print 명령을 사용할 경우 중간 인증서는 표시되지 않습니다.

⚠

주의 TLS 및 HTTPS 기능을 테스트하기 위한 데모 인증서가 어플라이언스와 함께 제공되지만, 데모 인증서로 두 서비스 중 하나를 활성화하는 것은 안전하지 않으며 일반적인 사용에 권장되지 않습니다. 데모 인증서로 두 서비스 중 하나를 활성화하면 CLI에 경고 메시지가 표시됩니다.

관련 주제

- 서명 인증서 구축 , 647 페이지
- 자체 서명 인증서 구축 , 647 페이지

서명 인증서 구축

Email Security Appliance와 다른 시스템 간에 자체 서명 인증서를 교환할 수 없는 경우(예: 시스템이 자신의 도메인에 없음) 서명 인증서를 사용합니다. 회사 보안 부서의 요구 사항은 다를 수 있습니다.

	수행해야 할 작업	추가 정보
1단계	클러스터를 구축 중인 경우 지침을 따릅니다.	인증서 및 중앙 집중식 관리, 648 페이지
2단계	자체 서명 인증서 및 CSR(Certificate Signing Request)을 생성합니다.	셀프 서명 인증서 만들기 , 648 페이지
3단계	생성된 인증서를 서명을 위해 알려진 인증 기관으로 전송합니다.	인증 기관에 CSR(Certificate Signing Request) 전송 정보 , 649 페이지
4단계	서명 인증서를 업로드합니다.	인증 기관에서 서명한 인증서 업로드 , 650 페이지
5단계	인증서에 서명한 인증 기관이 신뢰할 수 있는 기관 목록에 있는지 확인합니다.	인증 기관 목록 관리, 661 페이지
6단계	해당되는 경우 중간 인증서를 사용합니다.	중간 인증서, 648 페이지

자체 서명 인증서 구축

일반적으로 회사 방화벽 뒤에 있는 어플라이언스 간 통신에는 자체 서명 인증서를 사용할 수 있습니다. 회사 보안 부서의 요구 사항은 다를 수 있습니다.

	수행해야 할 작업	추가 정보
1단계	클러스터를 구축 중인 경우 지침을 따릅니다.	인증서 및 중앙 집중식 관리, 648 페이지
2단계	Email Security Appliance에서 자체 서명 인증서를 생성합니다.	셀프 서명 인증서 만들기 , 648 페이지
3단계	자체 서명 인증서를 내보냅니다.	인증서 내보내기 , 651 페이지
4단계	Email Security Appliance와 통신할 시스템으로 자체 서명 인증서를 가져옵니다.	다른 시스템용 문서를 참조하십시오.
5단계	다른 시스템에서 자체 서명 인증서를 생성하고 내보냅니다.	다른 시스템용 문서를 참조하십시오.

	수행해야 할 작업	추가 정보
6단계	다른 시스템에서 Email Security Appliance로 자체 서명 인증서를 가져옵니다.	인증서 가져오기 , 650 페이지 또는 이 가이드에서 해당 시스템과의 통신 구성에 대한 장을 참조하십시오. 예를 들어 Cisco AMP Threat Grid Appliance와의 보안 통신을 구성하려면 온프레미스 파일 분석 서버 구성 , 467 페이지의 고급 설정 구성에 대한 지침을 참조하십시오.

인증서 및 중앙 집중식 관리

인증서는 일반적으로 인증서의 CN에 로컬 시스템의 호스트 이름을 사용합니다. Email Security Appliance가 클러스터의 일부인 경우 각 클러스터 구성원에 대한 인증서를 시스템 레벨에서 가져와야 합니다(클러스터 레벨에서 설치할 수 있는 와일드카드 인증서 또는 SAN(Subject Alternative Name) 인증서 제외). 구성원의 리스너가 다른 시스템과 통신할 때 클러스터가 참조할 수 있도록 각 클러스터 구성원의 인증서는 동일한 인증서 이름을 사용해야 합니다.

중간 인증서

루트 인증서 확인 외에 AsyncOS는 중간 인증서 확인 사용을 지원합니다. 중간 인증서는 신뢰할 수 있는 루트 인증 기관에서 발급한 인증서로서 추가 인증서를 만드는 데 사용되므로, 연결된 신뢰 라인을 효과적으로 만들 수 있습니다. 예를 들면 신뢰할 수 있는 루트 인증 기관에서 인증서 발급 권한을 부여받은 godaddy.com에서 인증서를 발급할 수 있습니다. godaddy.com에서 발급한 인증서는 godaddy.com의 개인 키 및 신뢰할 수 있는 루트 인증 기관의 개인 키에 대해 검증해야 합니다.

셀프 서명 인증서 만들기

다음과 같은 이유 때문에 어플라이언스에서 자체 서명 인증서를 만들 수 있습니다.

- TLS를 사용하는 다른 MTA와의 SMTP 대화(인바운드와 아웃바운드 대화 모두)를 암호화하기 위해
- HTTPS를 사용하여 GUI에 액세스하기 위해 어플라이언스에서 HTTPS 서비스를 활성화하기 위해
- LDAP 서버에서 클라이언트 인증서를 요구하는 경우 LDAPS에 대한 클라이언트 인증서로서 사용하기 위해
- 어플라이언스와 Cisco AMP Threat Grid Appliance 간에 안전한 통신을 허용하기 위해

CLI를 사용하여 자체 서명 인증서를 만들려면 certconfig 명령을 사용합니다.

단계 **1** **Network**(네트워크) > **Certificates**(인증서)를 선택합니다.

단계 **2** **Add Certificate**(인증서 추가)를 클릭합니다.

단계 **3** **Create Self-Signed Certificate**(자체 서명 인증서 만들기)를 선택합니다.

단계 4 자체 서명 인증서에 대해 다음 정보를 입력합니다.

공용 이름	인증된 도메인 이름
조직	조직의 정확한 법인명
조직 단위	조직의 섹션
군/구	조직이 법적으로 위치한 도시
주/도:	조직이 법적으로 위치한 시/도 또는 지역
국가	조직이 법적으로 위치한 국가의 2자 ISO 약어
만료 전까지 기간	인증서가 만료될 때까지 남은 일수
개인 키 크기	CSR에 대해 생성할 개인 키의 크기 2048비트 및 1024비트만 지원됩니다.

단계 5 **Next(**다음**)**를 클릭합니다.

단계 6 인증서의 이름을 입력합니다. 기본적으로 AsyncOS는 전에 입력한 CN을 할당합니다.

단계 7 이 인증서를 CSR(Certificate Signing Request)로서 제출하려면 **Download Certificate Signing Request(**인증서 서명 요청 다운로드**)**를 클릭하여 로컬 또는 네트워크 시스템에 CSR을 PEM 형식으로 저장합니다.

단계 8 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

적절한 다음 단계를 참조합니다.

- 서명 인증서 구축 , 647 페이지
- 자체 서명 인증서 구축 , 647 페이지

인증 기관에 **CSR(Certificate Signing Request)** 전송 정보

인증 기관은 ID를 확인하고 공개 키를 배포하는 데 사용되는 디지털 인증서를 발급하는 서드파티 조직 또는 회사입니다. 인증서가 유효하고 신뢰할 수 있는 주체에 의해 발급되므로 더욱 안심할 수 있습니다. 알려진 인증 기관으로부터 인증서와 개인 키를 구매할 수 있습니다. Cisco는 다른 서비스에 비해 특정 서비스를 권장하지 않습니다.

Email Security Appliance는 자체 서명 인증서를 만들고, 인증 기관에 제출하여 공개 인증서를 얻기 위해 CSR(Certificate Signing Request)을 생성할 수 있습니다. 인증 기관은 개인 키에 의해 서명된 신뢰할 수 있는 공개 인증서를 반환합니다. 자체 서명 인증서를 만들고, CSR을 생성하고, 신뢰할 수 있는 공개 인증서를 설치하려면 웹 인터페이스의 Network(네트워크) > Certificates(인증서) 페이지 또는 CLI의 certconfig 명령을 사용합니다.

처음으로 인증서를 획득하는 경우 인터넷에서 "certificate authority services SSL Server Certificates(인증 기관 서비스 SSL 서버 인증서)"를 검색하고 조직의 요구에 가장 적합한 서비스를 선택합니다. 인증서를 가져오려면 서비스 지침을 따르십시오.

향후 작업

서명 인증서 구축 , 647 페이지를 참조하십시오.

인증 기관에서 서명한 인증서 업로드

인증 기관이 개인 키로 서명된 신뢰할 수 있는 공개 인증서를 반환하면 이 인증서를 어플라이언스에 업로드합니다.

퍼블릭 또는 프라이빗 리스너, IP 인터페이스의 HTTPS 서비스, LDAP 인터페이스 또는 대상 도메인에 대한 모든 발신 TLS 연결에서 이 인증서를 사용할 수 있습니다.

단계 **1** 어플라이언스로 업로드하기 전에, 수신한 신뢰할 수 있는 공개 인증서가 PEM 형식인지 또는 PEM으로 변환할 수 있는 형식인지 확인합니다. (이를 위한 툴은 http://www.openssl.org에서 무료로 다운로드할 수 있는 OpenSSL에 포함되어 있습니다.)

단계 **2** 서명 인증서를 어플라이언스에 업로드합니다.

참고 인증 기관에서 온 인증서를 업로드하면 기존의 자체 서명 인증서를 덮어쓰게 됩니다.

a) **Network**(네트워크) > **Certificates**(인증서)를 선택합니다.
b) 서명을 위해 인증 기관으로 보낸 인증서의 이름을 클릭합니다.
c) 로컬 시스템 또는 네트워크 볼륨에 있는 파일의 경로를 입력합니다.

단계 **3** 자체 서명 인증서와 관련된 중간 인증서도 업로드할 수 있습니다.

다음에 수행할 작업

관련 주제

- 서명 인증서 구축 , 647 페이지

인증서 가져오기

AsyncOS에서는 PKCS #12 형식으로 저장된 타 시스템의 인증서를 현재 어플라이언스에서 사용하기 위해 가져오도록 허용합니다.

CLI를 사용하여 인증서를 가져오려면 **certconfig** 명령을 사용합니다.

참고 서명 인증서를 구축하려는 경우 이 절차를 사용하여 서명 인증서를 가져오지 마십시오. 대신 인증 기관에서 서명한 인증서 업로드 , 650 페이지 섹션을 참조하십시오.

단계 **1** **Network**(네트워크) > **Certificates**(인증서)를 선택합니다.

단계 **2** **Add Certificate**(인증서 추가)를 클릭합니다.

단계 **3** **Import Certificate**(인증서 가져오기) 옵션을 선택합니다.

단계 4 네트워크 또는 로컬 컴퓨터에 있는 인증서 파일 경로를 입력합니다.
단계 5 파일의 암호를 입력합니다.
단계 6 **Next**(다음)를 클릭하여 인증서 정보를 봅니다.
단계 7 인증서의 이름을 입력합니다.

AsyncOS는 기본적으로 CN을 할당합니다.

단계 8 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

- 자체 서명 인증서를 구축하려면 자체 서명 인증서 구축 , 647 페이지 섹션을 참조하십시오.

인증서 내보내기

AsyncOS에서는 또한 인증서를 내보내고 PKCS #12 형식으로 저장하도록 허용합니다.

참고 서명 인증서를 구축하려는 경우 이 절차를 사용하여 CSR(Certificate Signing Request)을 생성하지 마십시오. 대신 서명 인증서 구축 , 647 페이지 섹션을 참조하십시오.

단계 1 **Network**(네트워크) > **Certificates**(인증서) 페이지로 이동합니다.
단계 2 **Export Certificate**(인증서 내보내기)를 클릭합니다.
단계 3 내보낼 인증서를 선택합니다.
단계 4 인증서의 파일 이름을 입력합니다.
단계 5 인증서 파일의 암호를 입력하고 확인합니다.
단계 6 **Export**(내보내기)를 클릭합니다.
단계 7 파일을 로컬 또는 네트워크 시스템에 저장합니다.
단계 8 인증서를 더 내보낼 수도 있고, **Cancel**(취소)을 클릭하여 Network(네트워크) > Certificates(인증서) 페이지로 돌아갈 수도 있습니다.

다음에 수행할 작업

- 자체 서명 인증서를 구축하려면 자체 서명 인증서 구축 , 647 페이지 섹션을 참조하십시오.

인증서의 HAT에서 TLS 활성화

암호화가 필요한 리스너에 대해 TLS를 활성화해야 합니다. 인터넷과 접한 리스너(즉, 퍼블릭 리스너)에서는 TLS를 활성화하고 내부 시스템용 리스너(즉, 프라이빗 리스너)에서는 활성화하지 않을 수 있습니다. 또는 모든 리스너에 대해 암호화를 활성화할 수도 있습니다.

리스너에서 TLS에 대해 다음 설정을 지정할 수 있습니다.

표 50: 리스너에 대한 TLS 설정

TLS 설정	의미
1. 아니요	수신 연결에 TLS가 허용되지 않습니다. 리스너에 대한 어떤 연결에서도 암호화된 SMTP 대화를 요구하지 않습니다. 어플라이언스에서 구성하는 모든 리스너에서는 이것이 기본 설정입니다.
2. Preferred	MTA에서 오는 리스너에 대한 수신 연결에 TLS가 허용됩니다.
3. 필수	MTA에서 오는 리스너에 대한 수신 연결에 TLS가 허용되며, STARTTLS 명령을 수신할 때까지 어플라이언스는 NOOP, EHLO 또는 QUIT 이외의 모든 명령 대해 오류 메시지로 응답합니다. 이 동작은 Transport Layer Security의 보안 SMTP에 대해 SMTP Service Extension을 정의하는 RFC 3207에 지정되어 있습니다. TLS를 "요구"한다는 것은, 발신자가 TLS로 암호화하지 않는 이메일은 전송 전에 어플라이언스에서 거부한다는 뜻입니다. 따라서 암호화 없이 전송되는 것이 방지됩니다.

기본적으로 프라이빗 리스너와 퍼블릭 리스너 모두 TLS 연결을 허용하지 않습니다. 인바운드(수신) 또는 아웃바운드(발신) 이메일에 대해 TLS를 활성화하려면 리스너의 HAT에서 TLS를 활성화해야 합니다. 또한 프라이빗 및 퍼블릭 리스너에 대한 모든 기본 메일 플로우 정책 설정에서는 tls가 "off"로 설정되어 있습니다.

리스너를 만들 때 TLS 연결에 대한 특정 인증서를 개별 퍼블릭 리스너에 할당할 수 있습니다. 자세한 내용은 웹 인터페이스를 사용하여 리스너를 만들어 연결 요청 수신 대기, 75 페이지를 참고하십시오.

관련 주제

- GUI를 사용하여 TLS 연결을 위한 퍼블릭 또는 프라이빗 리스너에 인증서 할당, 652 페이지
- CLI를 사용하여 TLS 연결을 위한 퍼블릭 또는 프라이빗 리스너에 인증서 할당, 653 페이지
- 로깅, 657 페이지
- GUI 예: 리스너 HAT에 대한 TLS 설정 변경, 653 페이지
- CLI 예: 리스너 HAT에 대한 TLS 설정 변경, 653 페이지

GUI를 사용하여 TLS 연결을 위한 퍼블릭 또는 프라이빗 리스너에 인증서 할당

단계 **1** Network(네트워크) > Listeners(리스너) 페이지로 이동합니다.

단계 **2** 수정할 리스너의 이름을 클릭합니다.

단계 **3** Certificate(인증서) 필드에서 인증서를 선택합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

CLI를 사용하여 **TLS** 연결을 위한 퍼블릭 또는 프라이빗 리스너에 인증서 할당

단계 **1** `listenerconfig -> edit` 명령을 사용하여 구성할 리스너를 선택합니다.

단계 **2** `certificate` 명령을 사용하여 사용 가능한 인증서를 표시합니다.

단계 **3** 프롬프트가 표시되면 리스너에 할당할 인증서를 선택합니다.

단계 **4** 리스너 구성이 완료되면 `commit` 명령을 실행하여 변경 사항을 활성화합니다.

로깅

Email Security Appliance는 TLS가 필요하지만 리스너에서 사용할 수 없는 경우 메일 로그에 인스턴스를 기록합니다. 다음 조건이 충족되면 메일 로그가 업데이트됩니다.

- 리스너에 대해 TLS가 "required(필수)"로 설정됨
- Email Security Appliance가 "Must issue a STARTTLS command first(STARTTLS 명령을 먼저 실행해야 함)" 명령을 전송함
- 성공적인 수신자 없이 연결이 닫힘

TLS 연결이 실패한 이유에 대한 정보가 메일 로그에 포함됩니다.

GUI 예: 리스너 **HAT**에 대한 **TLS** 설정 변경

단계 **1** Mail Policies(메일 정책) > Mail Flow Policies(메일 플로우 정책) 페이지로 이동합니다.

단계 **2** 정책을 수정할 리스너를 선택한 다음 수정할 정책의 이름에 대한 링크를 클릭합니다. (기본 정책 매개변수를 수정할 수도 있습니다.)

단계 **3** "Encryption and Authentication(암호화 및 인증)" 섹션의 "TLS:" 필드에서 리스너에 대해 원하는 TLS의 레벨을 선택합니다.

단계 **4** 변경 사항을 제출하고 커밋합니다.

리스너에 대한 메일 플로우 정책이 선택한 TLS 설정으로 업데이트됩니다.

CLI 예: 리스너 **HAT**에 대한 **TLS** 설정 변경

단계 **1** `listenerconfig -> edit` 명령을 사용하여 구성할 리스너를 선택합니다.

단계 **2** `hostaccess -> default` 명령을 사용하여 리스너의 기본 HAT 설정을 수정합니다.

단계 **3** 다음과 같은 질문이 표시되면 다음 항목 중 하나를 입력하여 TLS 설정을 변경합니다.

```
Do you want to allow encrypted TLS connections?

1. No

2. Preferred

3. Required

[1]> 3

You have chosen to enable TLS. Please use the 'certconfig' command to

ensure that there is a valid certificate configured.
```

단계 **4** 이 예에서는 `certconfig` 명령을 통해 리스너와 함께 사용할 수 있는 유효한 인증서가 있는지 확인하도록 요구합니다. 인증서를 만들지 않은 경우 리스너는 어플라이언스에 미리 설치된 데모 인증서를 사용합니다. 테스트 목적으로는 데모 인증서로 TLS를 활성화할 수 있지만, 데모 인증서는 안전하지 않으며 일반적인 용도로서 권장되지 않습니다. 리스너에 인증서를 할당하려면 `listenerconfig -> edit -> certificate` 명령을 사용합니다. TLS를 구성했으면, CLI에서 리스너의 요약에 설정이 반영됩니다.

```
Name: Inboundmail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain map: disabled

TLS: Required
```

단계 **5** `commit` 명령을 실행하여 변경 사항을 활성화합니다.

전달 시 **TLS** 및 인증서 확인 활성화

Destination Controls(대상 제어) 페이지 또는 `destconfig` 명령을 사용하여 특정 도메인에 이메일을 전달하도록 TLS의 활성화를 요구할 수 있습니다.

TLS 외에도, 도메인 서버 인증서를 확인하도록 요구할 수 있습니다. 이 도메인 확인은 도메인 자격 증명을 설정하는 데 사용되는 디지털 인증서를 기반으로 합니다. 확인 프로세스에는 두 가지 확인 요구 사항이 관련됩니다.

- SMTP 세션에 대한 발급자 인증서 체인은 신뢰할 수 있는 CA(인증 기관)에서 발급한 인증서로 끝납니다.
- 인증서에 나열된 CN(Common Name)은 수신 시스템의 DNS 이름 또는 메시지의 대상 도메인과 일치합니다.

  -또는-

RFC 2459에 설명된 대로, 메시지의 대상 도메인은 인증서 subjectAltName(Subject Alternative Name) 확장의 DNS 이름 중 하나와 일치합니다. RFC 2818의 섹션 3.1에 설명된 대로, 일치에서 와일드카드가 지원됩니다.

신뢰할 수 있는 CA는 ID를 확인하고 공개 키를 배포하는 데 사용되는 디지털 인증서를 발급하는 서드파티 조직 또는 회사입니다. 인증서가 유효하고 신뢰할 수 있는 주체에 의해 발급되므로 더욱 안심할 수 있습니다.

봉투 암호화에 대한 대안으로 TLS 연결을 통해 도메인에 메시지를 전송하도록 Email Security Appliance를 구성할 수 있습니다. 자세한 내용은 "Cisco Email Encryption" 장을 참조하십시오.

어플라이언스에서 모든 발신 TLS 연결에 사용할 인증서를 지정할 수 있습니다. 인증서를 지정하려면 Destination Controls(대상 제어) 페이지에서 **Edit Global Settings(**전역 설정 수정**)**를 클릭하거나 CLI의 `destconfig -> setup`을 사용합니다. 인증서는 도메인 단위 설정이 아니라 전역 설정입니다.

Destination Controls(대상 제어) 페이지 또는 `destconfig` 명령을 사용하여 도메인을 포함할 때 특정 도메인에 대해 TLS의 서로 다른 설정을 5개 지정할 수 있습니다. 도메인과의 교류에 TLS 인코딩이 필수(required)인지 기본 설정(preferred)인지를 지정하는 것 외에도, 도메인 검증의 필요 여부를 지정할 수 있습니다. 설정에 대한 설명은 다음 표를 참조하십시오.

표 ***51:*** 전달에 대한 ***TLS*** 설정

TLS 설정	의미
기본	Destination Controls(대상 제어) 페이지 또는 `destconfig -> default` 하위 명령을 통해 설정되는, 리스너에서 도메인에 대한 MTA로의 발신 연결에 사용되는 기본 TLS 설정. "Do you wish to apply a specific TLS setting for this domain?(이 도메인에 특정 TLS 설정을 적용하시겠습니까?)"이라는 질문에 "no(아니요)"로 답하는 경우 "Default(기본값)"가 설정됩니다.
1. No	인터페이스에서 도메인에 대한 MTA로의 발신 연결에 대해 TLS가 협상되지 않습니다.
2. Preferred	Email Security Appliance 인터페이스에서 도메인에 대한 MTA로의 연결에 대해 TLS가 협상됩니다. 그러나 TLS 협상이 실패하면(220 응답을 받기 전에) SMTP 트랜잭션이 "있는 그대로"(암호화되지 않고) 진행됩니다. 인증서가 신뢰할 수 있는 인증 기관에서 온 것인지를 확인하려고 시도하지 않습니다. 220 응답 수신 후 오류가 발생하는 경우 SMTP 트랜잭션이 일반 텍스트로 돌아가지 않습니다.
3. Required	Email Security Appliance 인터페이스에서 도메인에 대한 MTA로의 연결에 대해 TLS가 협상됩니다. 도메인 인증서를 확인하려고 시도하지 않습니다. 협상에 실패하면 연결을 통해 이메일이 전송되지 않습니다. 협상에 성공하면 암호화된 세션을 통해 메일이 전달됩니다.

TLS 설정	의미
4. Preferred (Verify)(권장(확인))	Email Security Appliance에서 도메인에 대한 MTA로의 연결에 대해 TLS가 협상됩니다. 어플라이언스가 도메인의 인증서를 확인하려고 시도합니다. 세 가지 결과가 나올 수 있습니다. • TLS가 협상되고 인증서가 확인됩니다. 암호화된 세션을 통해 메일이 전달됩니다. • TLS가 협상되지만 인증서가 확인되지 않습니다. 암호화된 세션을 통해 메일이 전달됩니다. • TLS 연결이 이루어지지 않고, 이어 인증서가 확인되지 않습니다. 이메일 메시지가 일반 텍스트로 전달됩니다.
5. Required (Verify)(필수(확인))	어플라이언스에서 도메인에 대한 MTA로의 연결에 대해 TLS가 협상됩니다. 도메인 인증서의 확인이 필요합니다. 다음 결과가 나올 수 있습니다. • TLS 연결이 협상되고 인증서가 확인됩니다. 암호화된 세션을 통해 이메일 메시지가 전달됩니다. • TLS 연결이 협상되지만, 신뢰할 수 있는 CA(인증 기관)에 의해 인증서가 확인되지 않습니다. 메일이 전달되지 않습니다. • TLS 연결이 협상되지 않습니다. 메일이 전달되지 않습니다.
6. 필수 - 호스팅 도메인 확인	ID 확인 과정에서 TLS Required - Verify(TLS 필수 - 확인) 옵션과 TLS Required - Verify Hosted Domain(TLS 필수 - 호스팅된 도메인 확인) 옵션의 차이가 나타납니다. 표시되는 ID가 처리되는 방식 및 사용할 수 있는 참조 식별자 유형은 최종 결과에 대한 변화를 만들 수 있습니다. 표시되는 ID는 `dNSName`의 `subjectAltName` 확장에서 파생됩니다. `dNSName`과 수락된 참조 ID(`REF ID`) 중 하나 사이에 일치하는 게 없으면 제목 필드에 `CN`이 있는지 여부에 관계없이 확인에 실패하고 추가 ID 확인을 통과할 수 있습니다. 제목 필드에서 파생된 `CN`은 인증서에 `dNSName` 유형의 `subjectAltName` 확장이 포함되지 않은 경우에만 확인됩니다.

양호한 인접 테이블에 특정 수신자 도메인에 대한 특정 항목이 없거나 특정 항목이 있지만 이 항목에 대한 특정 TLS 설정이 없는 경우, Destination Controls(대상 제어) 페이지 또는 `destconfig -> default` 하위 명령("No," "Preferred," "Required," "Preferred (Verify)" 또는 "Required (Verify)")으로 설정된 동작이 사용됩니다.

관련 주제

- 필수 TLS 연결 실패 시 알림 전송, 657 페이지
- 로깅, 657 페이지
- 인증 기관 목록 관리, 661 페이지

필수 TLS 연결 실패 시 알림 전송

TLS 연결을 요구하는 도메인에 메시지를 전달할 때 TLS 협상이 실패하는 경우 Email Security Appliance에서 알림을 전송할지 여부를 지정할 수 있습니다. 알림 메시지에는 실패한 TLS 협상에 대한 대상 도메인의 이름이 포함됩니다. Email Security Appliance는 시스템 알림 유형에서 Warning(경고) 심각도 레벨 알림을 수신하도록 설정된 모든 수신자에게 알림 메시지를 전송합니다. GUI의 System Administration(시스템 관리) > Alerts(알림) 페이지(또는 CLI의 alertconfig 명령)를 통해 알림 수신자를 관리할 수 있습니다.

관련 주제

• TLS 연결 알림 활성화 , 657 페이지

TLS 연결 알림 활성화

단계 **1** Mail Policies Destination Controls(메일 정책 대상 제어) 페이지로 이동합니다.

단계 **2** **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **3** "Send an alert when a required TLS connection fails(필수 TLS 연결 실패 시 알림 전송)"에 대해 **Enable(**활성화**)**을 클릭합니다.

이것은 도메인 단위 설정이 아니라 전역 설정입니다. 어플라이언스가 전달하려고 시도한 메시지에 대해 알아보려면 Monitor(모니터) > Message Tracking(메시지 추적) 페이지 또는 메일 로그를 사용하십시오.

단계 **4** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

이를 CLI에서 구성하려면 destconfig -> setup 명령을 사용하여 TLS 연결 알림을 활성화합니다.

로깅

Email Security Appliance는 도메인에 TLS가 필요하지만 사용할 수 없는 경우 메일 로그에 인스턴스를 기록합니다. TLS 연결을 사용할 수 없는 이유에 대한 정보가 포함됩니다. 다음 조건 중 하나가 충족되면 메일 로그가 업데이트됩니다.

- 원격 MTA는 ESMTP를 지원하지 않음(예를 들면 Email Security Appliance의 EHLO 명령을 이해하지 못함)
- 원격 MTA가 ESMTP를 지원하지만, EHLO 응답에서 광고한 확장 목록에 "STARTTLS"가 없음
- 원격 MTA가 "STARTTLS" 확장을 광고했지만, Email Security Appliance에서 STARTTLS 명령을 전송할 때 오류로 응답함

명명된 엔티티의 DNS 기반 인증

명명된 엔티티의 SMTP DNS 기반 인증 개요

인증서를 사용하여 인증된 TLS 연결은 다음 중 한 가지 방법으로 보안 침해에 취약해질 수 있습니다.

- 신뢰할 수 있는 CA(인증 기관)는 어떤 도메인 이름에도 인증서를 발급할 수 있습니다.
- 공격자는 MITM(메시지 가로채기) 공격을 사용하여 TLS 연결을 일반 텍스트 통신으로 다운그레이드할 수 있습니다.
- DNS 서버에 DNSSEC가 구성되지 않은 경우 공격자는 가짜 DNS MX 레코드를 사용하여 DNS 응답을 위조하고 메시지를 안전하지 않은 서버로 리디렉션하여 DNS 캐시 손상 공격을 유발할 수 있습니다.
- 수신된 MTA(Mail Transfer Agent)가 신뢰할 수 있는 인증 기관 목록으로 구성되지 않은 경우, 개인 인증 기관(CA)에서 발급한 자체 서명 인증서 또는 인증서를 사용할 수 있습니다.

SMTP DANE(명명된 엔티티의 DNS 기반 인증) 프로토콜은 DNS 서버에 구성된 DNSSEC(Domain Name System Security) 확장 및 TLSA 레코드라고도 하는 DNS 리소스 레코드를 사용하여 DNS 이름으로 x.509 인증서를 검증합니다.

TLSA 레코드는 CA(인증 기관), 종료 엔티티 인증서 또는 *RFC 6698*에 설명된 DNS 이름에 사용되는 신뢰 앵커에 대한 세부 사항을 포함하는 인증서에 추가됩니다. 자세한 내용은 TLSA 레코드 생성, 659 페이지의 내용을 참고하십시오. DNSSEC(Domain Name System Security) 확장은 DNS 보안의 취약점을 해결하여 DNS에 추가 보안을 제공합니다. 암호화 키 및 디지털 서명을 사용하는 DNSSEC는 조회 데이터가 정확하고 합법적인 서버에 연결되는지 확인합니다.

다음은 발신 TLS 연결에 SMTP DANE를 사용하는 경우의 이점입니다.

- MITM(메시지 가로채기) 다운그레이드 공격, 도청 및 DNS 캐시 손상 공격을 방지하여 메시지의 보안 전달을 제공합니다.
- DNSSEC로 보호되는 경우 TLS 인증서 및 DNS 정보의 신뢰성을 제공합니다.

관련 주제

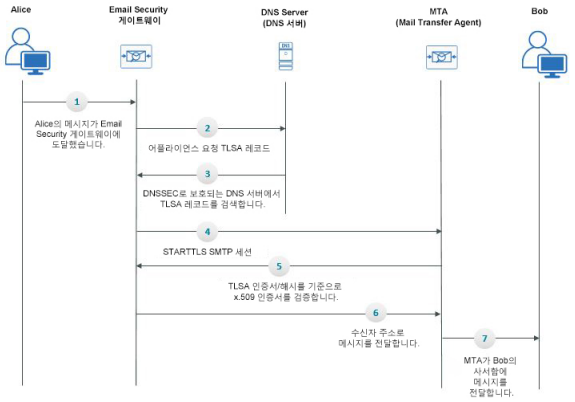
• SMTP DANE 워크플로, 659 페이지
• TLSA 레코드 생성, 659 페이지
• DANE 지원 전달을 위한 TLS 활성화, 660 페이지

• DANE 실패 시 알림 전송, 661 페이지

SMTP DANE 워크플로

다음 그림은 발신 TLS와 DANE 지원과의 연결을 사용하는 메시지의 플로우에 대해 설명합니다.

그림 ***46: DANE*** 지원과 함께 ***TLS***를 사용하는 메시지 전달



1. 발신자(Alice)는 조직 외부의 수신자(Bob)에게 메시지를 보냅니다.
2. 메시지가 Email Security 게이트웨이에 도착합니다.
3. Email Security 게이트웨이에서 DNS 리소스 레코드(DNS 서버의 DNS에 대한 TLSA 레코드라고도 함)를 요청합니다.
4. 인증서 및 TLSA 레코드는 DNSSEC에 의해 보호되는 DNS 서버에서 검색됩니다.
5. 어플라이언스는 수신자의 주소에 대한 STARTTLS SMTP 세션을 설정합니다.
6. x.509 인증서는 받는 사람 주소의 전체 TLSA 레코드 또는 해당 해시 값을 기준으로 검증됩니다. 검증이 성공적으로 완료되면 메시지는 수신자의 MTA(Mail Transfer Agent)에 전달됩니다. 인증서 확인에 실패하면 메시지는 나중에 전달되거나 메시지가 반송됩니다.
7. MTA는 수신자의 사서함으로 메시지를 전달합니다.

TLSA 레코드 생성

DNSSEC로 서명된 DNS 레코드에서 기본 CA(인증 기관)에 대한 TLSA 레코드를 생성할 수 있습니다. 다음은 FQDN(Fully Qualified Domain Name) `www.example.com`에 대한 샘플 TLSA 레코드입니다.

```
_443. _tcp. .com. IN TLSA (0 0 1
91751cee0a1ab8414400238a761411daa29643ab4b8243e9a91649e25be53ada)
```

위 예에서 TLSA 레코드에는 다음과 같은 필드가 암호화되어 있습니다.

- **Certificate Usage**(인증서 사용): 인증서 유형을 지정합니다.
  - 지정된 샘플에서 첫 번째 '0' 자리는 RFC 6698에 설명된 대로 PKIX 인증 경로와 일치해야 하는 CA 인증서를 지정합니다.

- '1'인 경우, TLS의 서버에서 제공하는 최종 엔티티 인증서와 일치해야 하는 최종 엔티티 인증서를 지정합니다.
- '2'인 경우, TLS의 서버에서 제공하는 최종 엔티티 인증서를 검증하는 동안 신뢰 앵커로 사용해야 하는 인증서를 지정합니다.
- 이 값이 '3'이면 TLS에서 서버에서 제공하는 최종 엔티티 인증서와 일치해야 하는 인증서를 지정합니다.

- **Selector Field(선택기 필드)**: 연결 데이터와 일치하는 TLS 인증서의 부분을 지정합니다.
  - 지정된 샘플에서 두 번째 '0'은 전체 인증서가 일치해야 함을 지정합니다.
  - '1'인 경우 'SubjectPublicKeyInfo' 필드만 일치해야 합니다.

- **Matching Type(일치 유형)**: 사용되는 해시 값의 유형을 지정합니다.
  - 지정된 샘플에서 세 번째 '1'은 선택한 콘텐츠의 SHA-256 해시를 지정합니다.
  - 이 값이 '0'이면 선택한 콘텐츠에서 정확하게 일치하는 항목을 지정합니다.
  - '2'인 경우 선택한 콘텐츠의 SHA-512 해시를 지정합니다.

DANE 지원 전달을 위한 TLS 활성화

시작하기 전에

- 봉투 발신자 및 TLSA 리소스 레코드가 DNSSEC로 확인되었는지 확인합니다.
- 어플라이언스에서 DANE를 구성하려면 TLS를 활성화해야 합니다. 자세한 내용은 전달 시 TLS 및 인증서 확인 활성화, 654 페이지의 내용을 참고하십시오.

단계 **1** **Mail Policies(메일 정책) > Destination Controls(대상 제어)** 페이지로 이동합니다.

단계 **2** **Add Destination Controls(대상 제어 추가)**를 클릭하거나 기존 항목을 수정합니다.

단계 **3** **TLS Support(TLS 지원)** 필드에서 어플라이언스의 DANE 지원을 활성화하려면 **Preferred(기본)**, **Required(필요)** 또는 **Mandatory(필수)**를 선택해야 합니다.

단계 **4** **DANE Support(DANE 지원)** 필드에서 지정된 TLS 연결의 DANE에 대해 다음 설정을 지정할 수 있습니다.

DANE 설정	설명
기본	Destination Controls(대상 제어) 페이지에서 설정된 기본 DANE 설정은 리스너에서 도메인에 대한 MTA로의 발신 TLS 연결에 사용됩니다. "Default" DANE 설정은 대상 제어의 기본 TLS 설정에서 상속됩니다. 이 설정을 맞춤형 대상 제어 항목으로 재정의할 수 있습니다.

DANE 설정	설명
None	인터페이스에서 도메인에 대한 MTA로의 발신 연결을 협상하는 데 DANE를 사용하지 않으려면 "None"을 선택합니다.
기회주의적	"Opportunistic"을 선택하고 원격 호스트가 DANE를 지원하지 않는 경우 SMTP 대화를 암호화하는 데 더 적합한 TLS가 사용됩니다. "Opportunistic"를 선택하고 원격 호스트가 DANE를 지원하는 경우 이는 SMTP 대화를 암호화하는 기본 모드가 됩니다.
필수	"Mandatory"를 선택하고 원격 호스트가 DANE를 지원하지 않는 경우 대상 호스트에 대한 연결이 설정되지 않습니다. "Mandatory"를 선택하고 원격 호스트가 DANE를 지원하는 경우 이는 SMTP 대화를 암호화하는 기본 모드가 됩니다.

단계 **5** 변경 사항을 제출하고 커밋합니다.

DANE 실패 시 알림 전송

DANE를 지원하는 TLS 연결을 요구하는 도메인에 메시지를 전달할 때 모든 MX 호스트에서 DANE 협상이 실패하는 경우 Email Security Appliance에서 알림을 전송할지 여부를 지정할 수 있습니다. Email Security Appliance는 시스템 알림 유형에서 Warning(경고) 심각도 레벨 알림을 수신하도록 설정된 모든 수신자에게 알림 메시지를 전송합니다.

DANE 알림 활성화

단계 **1** **System Administration(**시스템 관리**) > Alerts(**알림**)** 페이지로 이동합니다.

단계 **2** 알림을 활성화하려는 알림 수신자를 선택합니다.

단계 **3** 알림 유형에 해당하는 **Message Delivery(**메시지 전달**)** 확인란을 선택합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

인증 기관 목록 관리

도메인의 자격 증명을 설정하기 위해 어플라이언스가 원격 도메인에서 온 인증서를 확인하는 데 사용하는 신뢰할 수 있는 저장된 인증 기관을 사용합니다. 다음의 신뢰할 수 있는 인증 기관을 사용하도록 어플라이언스를 구성할 수 있습니다.

- 사전 설치된 목록**.** 어플라이언스에는 신뢰할 수 있는 인증 기관의 사전 설치된 목록이 있습니다. 이를 시스템 목록이라고 합니다.

- 사용자 정의 목록. 신뢰할 수 있는 인증 기관의 목록을 사용자 지정한 다음 어플라이언스로 가져올 수 있습니다.

시스템 목록 또는 사용자 지정된 목록을 사용할 수 있으며, 원격 도메인에서 오는 인증서를 확인하는 데 두 목록을 모두 사용할 수도 있습니다.

GUI의 Network(네트워크) > Certificates(인증서) > Edit Certificate Authorities(인증 기관 수정) 페이지 또는 CLI의 certconfig > certauthority 명령을 사용하여 목록을 관리합니다.

Network(네트워크) > Certificates(인증서) > Edit Certificate Authorities(인증 기관 수정) 페이지에서 다음 작업을 수행할 수 있습니다.

- 인증 기관의 시스템 목록(사전 설치)을 봅니다. 자세한 내용은 인증 기관의 사전 설치된 목록 보기, 662 페이지를 참고하십시오.
- 시스템 목록의 사용 여부를 선택합니다. 시스템 목록을 활성화 또는 비활성화할 수 있습니다. 자세한 내용은 시스템 인증 기관 목록 비활성화, 662 페이지를 참고하십시오.
- 사용자 지정 인증 기관 목록의 사용 여부를 선택합니다. 사용자 지정 목록을 사용하도록 어플라이언스를 활성화한 다음 텍스트 파일에서 목록을 가져올 수 있습니다. 자세한 내용은 사용자 지정 인증 기관 목록 가져오기, 663 페이지를 참고하십시오.
- 인증 기관의 목록을 파일로 내보냅니다. 인증 기관의 시스템 목록 또는 사용자 지정된 목록을 텍스트 파일로 내보낼 수 있습니다. 자세한 내용은 인증 기관 목록 내보내기, 663 페이지를 참고하십시오.

관련 주제

- 인증 기관의 사전 설치된 목록 보기, 662 페이지
- 시스템 인증 기관 목록 비활성화, 662 페이지
- 사용자 지정 인증 기관 목록 가져오기, 663 페이지
- 인증 기관 목록 내보내기, 663 페이지

인증 기관의 사전 설치된 목록 보기

단계 **1** Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.

단계 **2** Certificate Authorities(인증 기관) 섹션에서 **Edit Settings**(설정 수정)를 클릭합니다.

단계 **3** **View System Certificate Authorities**(시스템 인증 기관 보기)를 클릭합니다.

시스템 인증 기관 목록 비활성화

사전 설치된 시스템 인증 기관 목록은 어플라이언스에서 제거할 수 없지만, 활성화 또는 비활성화할 수 있습니다. 어플라이언스가 원격 호스트에서 오는 인증서를 확인하는 데 사용자 지정 목록만 사용하도록 하려면 이를 비활성화할 수 있습니다.

단계 **1** Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.

단계 **2** Certificate Authorities(인증 기관) 섹션에서 **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** System List(시스템 목록)에 대해 **Disable(**비활성화**)**을 클릭합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

사용자 지정 인증 기관 목록 가져오기

신뢰할 수 있는 인증 기관의 사용자 지정 목록을 만들고 어플라이언스로 가져올 수 있습니다. 파일은 PEM 형식이어야 하며, 어플라이언스에서 신뢰하도록 할 인증 기관에 대한 인증서를 포함해야 합니다.

단계 **1** Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.

단계 **2** Certificate Authorities(인증 기관) 섹션에서 **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** Custom List(사용자 지정 목록)에 대해 **Enable(**활성화**)**을 클릭합니다.

단계 **4** 로컬 또는 네트워크 시스템에서 사용자 지정 목록에 대한 전체 경로를 입력합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

인증 기관 목록 내보내기

시스템에서 신뢰할 수 있는 인증 기관의 하위 집합만 사용하려는 경우 또는 기존 사용자 지정 목록을 수정하려는 경우, 목록을 .txt 파일로 내보낸 다음 인증 기관을 추가 또는 제거하여 수정할 수 있습니다. 목록 수정이 완료되면 파일을 사용자 지정 목록으로 어플라이언스로 다시 가져올 수 있습니다.

단계 **1** Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.

단계 **2** Certificate Authorities(인증 기관) 섹션에서 **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** **Export List(**목록 내보내기**)**를 클릭합니다.

AsyncOS에 Export Certificate Authority List(인증 기관 목록 내보내기) 페이지가 표시됩니다.

단계 **4** 내보낼 목록을 선택합니다.

단계 **5** 목록의 파일 이름을 입력합니다.

단계 **6** **Export(**내보내기**)**를 클릭합니다.

AsyncOS에 목록을 .txt 파일로 열지 또는 저장할지를 묻는 대화 상자가 표시됩니다.

HTTPS용 인증서 활성화

GUI의 **Network**(네트워크) > **IP Interfaces**(IP 인터페이스) 페이지 또는 CLI의 **interfaceconfig** 명령을 사용하여 IP 인터페이스에서 HTTPS 서비스용 인증서를 활성화할 수 있습니다.

단계 **1** **Network**(네트워크) > **IP Interfaces**(IP 인터페이스) 페이지로 이동합니다.

단계 **2** HTTPS 서비스를 활성화할 인터페이스를 선택합니다.

단계 **3** Appliance Management(어플라이언스 관리) 아래에서 **HTTPS** 확인란을 선택하고 포트 번호를 입력합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

참고 데모 인증서는 어플라이언스에 미리 설치됩니다. 테스트 목적으로는 데모 인증서로 HTTPS 서비스를 활성화할 수 있지만, 데모 인증서는 안전하지 않으며 일반적인 용도로서 권장되지 않습니다.

GUI에서 시스템 설정 마법사를 사용하여 HTTPS 서비스를 활성화할 수 있습니다. 자세한 내용은 설정 및 설치, 15 페이지를 참조하십시오.

28 장

라우팅 및 전달 기능 구성

이 장에는 다음 섹션이 포함되어 있습니다.

로컬 도메인용 이메일 라우팅

이메일을 수신하도록 게이트웨이 구성, 69 페이지에서, 엔터프라이즈 게이트웨이 구성을 위한 SMTP 연결 서비스를 제공하기 위해 프라이빗 및 퍼블릭 리스너를 사용자 지정했습니다. 이러한 리스너는 특정 연결을 처리하고(HAT 수정을 통해) 특정 도메인에 대한 메일을 수신하도록(퍼블릭 리스너의 RAT 수정을 통해) 사용자 지정됩니다.

어플라이언스는 **Network(네트워크) > SMTP Routes(SMTP 경로)** 페이지(또는 `smtproutes` 명령)에서 지정한 로컬 도메인, 호스트로 메일을 라우팅합니다. 이 기능은 sendmail `mailertable` 기능과 비슷합니다.

참고 "설정 및 설치" 장에서 설명한 GUI의 시스템 설정 마법사(또는 명령행 인터페이스 `systemsetup` 명령)를 완료하고 변경 사항을 커밋했으면, 그 당시 입력한 각 RAT 항목에 대해 어플라이언스에 첫 번째 SMTP 경로 항목이 정의되어 있습니다.

관련 주제

SMTP 경로 개요

SMTP 경로를 사용하면 특정 도메인에 대한 모든 이메일을 다른 MX(mail exchange) 호스트로 리디렉션할 수 있습니다. 예를 들면 `example.com`에서 `groupware.example.com`으로의 매핑을 만들 수 있습니다. 이렇게 매핑하면 봉투 수신자 주소의 `@example.com` 이메일이 groupware.example.com으로 대신 전달됩니다. 시스템은 `groupware.example.com`에서 "MX" 조회를 수행한 다음, 일반 메일 전달과 마찬가지로 호스트에서 "A" 조회를 수행합니다. 이 대체 MX 호스트는 DNS MX 레코드에 나열될 필요가 없으며, 이메일이 리디렉션되는 도메인의 구성원일 필요도 없습니다. AsyncOS 운영 체제에서는 어플라이언스에 대해 최대 40,000개의 SMTP 경로 매핑을 구성할 수 있습니다. (SMTP 경로 제한, 668 페이지 참조)

이 기능은 또한 호스트 "글로빙(globbing)"을 허용합니다. `example.com`과 같은 부분 도메인을 지정하면 `example.com`으로 끝나는 모든 도메인이 이 항목과 매칭합니다. 예를 들어 `fred@foo.example.com` 및 `wilma@bar.example.com`은 모두 매핑과 일치합니다.

SMTP 경로 테이블에서 호스트가 발견되지 않으면 DNS를 사용하여 MX 조회가 수행됩니다. 결과는 SMTP 경로 테이블에 대해 다시 확인되지 않습니다. `foo.domain`에 대한 DNS MX 항목이 `bar.domain`인 경우, `foo.domain`으로 전송된 이메일은 호스트 `bar.domain`으로 전달됩니다. 일부 다른 호스트에 대해 `bar.domain`의 매핑을 생성하는 경우 `foo.domain`으로 보낼 이메일에는 영향을 미치지 않습니다.

즉, 재귀 항목은 허용되지 않습니다. `b.domain`으로 리디렉션할 `a.domain`에 대한 항목이 있으며 b.domain에 대한 이메일을 `a.domain`으로 리디렉션하는 후속 항목이 있는 경우, 메일 루프가 생성되지 않습니다. 이 경우 `a.domain`으로 주소가 지정된 이메일은 `b.domain`에 의해 지정된 MX 호스트로 전달되지 않으며, 반대로 `b.domain`으로 주소가 지정된 이메일은 `a.domain`에 의해 지정된 MX 호스트로 전달됩니다.

모든 이메일 전달 시 SMTP 경로 테이블을 위에서 아래로 읽습니다. 매핑과 일치하는 가장 구체적인 항목이 선정됩니다. SMTP 경로 테이블에 `host1.example.com`과 `.example.com` 모두에 대한 매핑이 있는 경우, 덜 구체적인 `.example.com` 항목 뒤에 나타나더라도 `host1.example.com`에 대한 항목이 좀 더 구체적이므로 이 항목이 사용됩니다. 그렇지 않으면 시스템은 봉투 수신자의 도메인에서 일반적인 MX 조회를 수행합니다.

기본 SMTP 경로

특수 키워드 ALL을 사용하여 기본 SMTP 경로를 정의할 수도 있습니다. 도메인이 SMTP 경로 목록에 있는 이전 매핑과 일치하지 않는 경우, 기본적으로 ALL 항목에 의해 지정된 MX 호스트로 리디렉션됩니다.

SMTP 경로 항목을 출력하면 기본 SMTP 경로가 ALL:로 나열됩니다. 기본 SMTP 경로는 삭제할 수 없습니다. 여기에 대해 입력한 값만 지울 수 있습니다.

Network(네트워크) > SMTP Routes(SMTP 경로) 페이지 또는 smtproutes 명령을 통해 기본 SMTP 경로를 구성합니다.

SMTP 경로 정의

Network(네트워크) > SMTP Routes(SMTP 경로) 페이지(또는 smtproutes 명령)를 사용하여 경로를 작성합니다. 새 경로를 만들 경우, 먼저 영구 경로를 만들 도메인 또는 부분 도메인을 지정합니다. 그런 다음 대상 호스트를 지정합니다. 대상 호스트는 인증된 호스트 이름 또는 IP 주소로서 입력할 수 있습니다. IP 주소는 IPv4(Internet Protocol version 4) 또는 IPv6(version 6)일 수 있습니다.

IPv6 주소의 경우 AsyncOS는 다음 형식을 지원합니다.

- 2620:101:2004:4202::0-2620:101:2004:4202::ff
- 2620:101:2004:4202::
- 2620:101:2004:4202::23
- 2620:101:2004:4202::/64

항목과 일치하는 메시지를 삭제하려면 /dev/null의 특수 대상 호스트를 지정할 수도 있습니다. (따라서 기본 경로에 대해 /dev/null을 지정하면 어플라이언스에서 수신하는 메일이 전혀 전달되지 않습니다.)

수신 도메인에는 여러 대상 호스트가 있을 수 있으며, MX 레코드와 마찬가지로 각각에 우선 순위 번호가 할당됩니다. 가장 낮은 번호의 대상 호스트는 수신 도메인에 대한 기본 대상 호스트로 식별됩니다. 나열된 다른 대상 호스트는 백업으로 사용됩니다.

동일한 우선 순위의 대상은 "라운드로빈" 방식으로 사용됩니다. 라운드로빈 프로세스는 SMTP 연결을 기반으로 하며 메시지 기반일 필요가 없습니다. 또한 하나 이상의 대상 호스트가 응답하지 않는 경우 메시지는 도달 가능한 호스트 중 하나로 전달됩니다. 구성된 대상 호스트 중 응답하지 않는 것이 있으면 메일은 수신 도메인에 대해 대기열에 추가되며, 대상 호스트에 대한 전달이 나중에 시도됩니다. (MX 레코드 사용으로 장애 조치되지 않습니다).

CLI의 smtproutes 명령을 사용하여 경로를 작성할 때, 호스트 이름 또는 IP 주소 뒤에 우선 순위를 할당하려면 /pri=과 0~65535의 정수를 차례로 사용하여 각 대상 호스트의 우선 순위를 지정할 수 있습니다(0이 최상위 우선 순위). 예를 들어 host1.example.com/pri=0은 host2.example.com/pri=10보다 우선 순위가 높습니다. 항목이 여러 개인 경우 쉼표로 구분하십시오.

SMTP 경로 제한

최대 40,000개의 경로를 정의할 수 있습니다. ALL의 최종 기본 경로는 이 제한에 대한 경로로 계산됩니다. 따라서 최대 39,999개의 맞춤형 경로와 특수 키워드 ALL을 사용하는 하나의 경로를 정의할 수 있습니다.

SMTP 경로 및 DNS

어플라이언스에서 MX 조회를 수행하여 특정 도메인에 대한 다음 홉(hop)을 확인하도록 하려면 특수 키워드 USEDNS를 사용합니다. 이는 하위 도메인에 대한 메일을 특정 호스트로 라우팅해야 할 경우 유용합니다. 예를 들어 example.com에 대한 메일을 회사의 Exchange 서버로 전송하려는 경우 다음 SMTP 경로와 유사한 것이 있을 것입니다.

example.com exchange.example.com

그러나 다양한 하위 도메인(foo.example.com)에 대한 메일에는 다음과 같은 SMTP 경로를 추가합니다.

.example.com USEDNS

SMTP 경로 및 경고문

어플라이언스에서 System Administration(시스템 관리) > Alerts(경고문) 페이지(또는 alertconfig 명령)에 지정된 주소로 전송되는 경고문은 해당 대상에 대해 정의된 SMTP 경로를 따릅니다.

SMTP 경로, 메일 전달 및 메시지 분리

수신: 한 메시지의 수신자가 10명이고 이들이 모두 동일한 Exchange 서버에 있는 경우, AsyncOS는 하나의 TCP 연결을 열고 메일 저장소에 10개의 개별 메시지가 아니라 정확히 하나의 메시지를 제시합니다.

발신: 유사하게 작동하지만, 한 메시지가 10개의 서로 다른 도메인에 있는 10명의 수신자에게 가는 경우 AsyncOS는 10개의 MTA에 대한 10개의 연결을 열고 각각에 하나의 이메일을 전달합니다.

분리: 수신 메시지 하나의 수신자가 10명이고 이들이 각각 별도의 수신 정책 그룹에 속한 경우(그룹 10개), 10명의 수신자가 모두 동일한 Exchange 서버에 있더라도 메시지가 분리됩니다. 따라서 단일 TCP 연결을 통해 10개의 개별 이메일이 전달됩니다.

SMTP 경로 및 아웃바운드 SMTP 인증

아웃바운드 SMTP 인증 프로필을 만든 경우 SMTP 경로에 적용할 수 있습니다. 이는 어플라이언스가 네트워크 에지에 있는 메일 릴레이 서버 뒤에 있는 경우 발신 메일에 대한 인증을 허용합니다. 아웃바운드 SMTP 인증에 대한 자세한 내용은 발송 SMTP 인증, 772 페이지 섹션을 참조해 주십시오.

GUI를 사용하여 아웃바운드 이메일을 전송하도록 SMTP 경로 관리

어플라이언스에서 SMTP 경로를 관리하려면 Network(네트워크) > SMTP Routes(SMTP 경로) 페이지를 사용합니다. 이 테이블에서 매핑을 추가, 수정 및 삭제할 수 있습니다. SMTP 경로 항목을 내보내거나 가져올 수 있습니다.

관련 주제

- SMTP 경로 추가, 669 페이지
- SMTP 경로 내보내기, 669 페이지
- SMTP 경로 가져오기, 669 페이지

SMTP 경로 추가

단계 **1** Network(네트워크) > SMTP Routes(SMTP 경로) 페이지에서 **Add Route(**경로 추가**)**를 클릭합니다.

단계 **2** 수신 도메인을 입력합니다. 호스트 이름, 도메인, IPv4 주소 또는 IPv6 주소일 수 있습니다.

단계 **3** 대상 호스트를 입력합니다. 호스트 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다. **Add Row(**행 추가**)**를 클릭하고 새 행에 다음 대상 호스트를 입력하여 여러 대상 호스트를 추가할 수 있습니다.

참고 ":<*port number*>"를 목적지 호스트 example.com:25에 추가하여 포트 번호를 지정할 수 있습니다.

단계 **4** 대상 호스트를 여러 개 추가하는 경우 0~65535 정수를 입력하여 호스트에 우선순위를 할당합니다. 0의 우선 순위가 가장 높습니다. 자세한 내용은 SMTP 경로 정의, 667 페이지를 참조하십시오.

단계 **5** 변경 사항을 제출 및 커밋합니다.

SMTP 경로 내보내기

HAT(Host Access Table) 및 RAT(Recipient Access Table)와 마찬가지로 파일을 내보내고 가져와서 SMTP 경로 매핑을 수정할 수 있습니다. SMTP 경로를 내보내려면

단계 **1** SMTP Routes(SMTP 경로) 페이지에서 **Export SMTP Routes(SMTP** 경로 내보내기**)**를 클릭합니다.

단계 **2** 파일 이름을 입력하고 **Submit(**제출**)**을 클릭합니다.

SMTP 경로 가져오기

HAT(Host Access Table) 및 RAT(Recipient Access Table)와 마찬가지로 파일을 내보내고 가져와서 SMTP 경로 매핑을 수정할 수 있습니다. SMTP 경로를 가져오려면

단계 **1** SMTP Routes(SMTP 경로) 페이지에서 **Import SMTP Routes(SMTP** 경로 가져오기**)**를 클릭합니다.

단계 **2** 내보낸 SMTP 경로를 포함하는 파일을 선택합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다. 가져오기를 수행하면 기존의 모든 SMTP 경로가 교체된다는 경고가 표시됩니다. 텍스트 파일의 모든 SMTP 경로를 가져오게 됩니다.

단계 **4** **Import(**가져오기**)**를 클릭합니다.

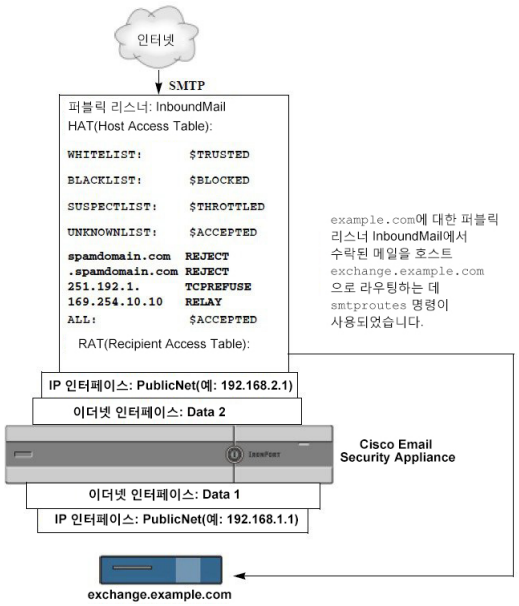
파일에 "코멘트"를 추가할 수 있습니다. '#' 문자로 시작되는 줄은 코멘트로 간주되어 AsyncOS에서 무시됩니다. 예를 들면 다음과 같습니다.

```
# this is a comment, but the next line is not

ALL:
```

다음에 수행할 작업

이 시점에서 이메일 게이트웨이 구성은 다음과 같습니다.

그림 ***47:*** 퍼블릭 리스너에 대해 정의된 ***SMTP*** 경로



주소 재작성

AsyncOS는 이메일 파이프라인에서 봉투 발신자 및 수신자 주소를 재작성하기 위한 여러 가지 방법을 제공합니다. 주소 재작성은 예를 들어 파트너 도메인으로 전송되는 메일을 리디렉션하거나 내부 인프라를 숨기기 위해("마스크 처리") 사용할 수 있습니다.

다음 표에서는 발신자 및 수신자 이메일 주소 재작성에 사용되는 각종 기능의 개요를 제공합니다.

표 **52:** 주소 재작성을 위한 방법

원래 주소	변경 주소	기능	작동
*@anydomain	user@domain	별칭 테이블(별칭 테이블 만들기, 671 페이지 참고)	• 봉투 수신자 전용 • 전역적으로 적용됨 • 이메일 주소 또는 기타 별칭에 대한 맵 별칭
*@olddomain	*@newdomain	도메인 매핑(도메인 맵 기능, 688 페이지 참조)	• 봉투 수신자 전용 • 리스너당 적용됨
*@olddomain	*@newdomain	가장(가장 구성, 678 페이지 참조)	• 봉투 발신자와 To:, From: 및/또는 CC: 헤더 • 리스너당 적용됨

별칭 테이블 만들기

별칭 테이블은 메시지를 하나 이상의 수신자에게 리디렉션하는 메커니즘을 제공합니다. 일부 Unix 시스템에 있는 sendmail 컨피그레이션의 `/etc/mail/aliases` 기능과 비슷한 방식으로 사용자 이름에 대한 별칭 및 기타 별칭의 매핑 테이블을 작성할 수 있습니다.

리스너가 수락한 이메일의 Envelope Recipient(봉투 수신자)(Envelope To 또는 `RCPT TO`라고도 함)가 별칭 테이블에 정의된 별칭과 일치하면 봉투 수신자의 이메일 주소가 재작성됩니다.

참고 리스너는 별칭 테이블을 확인하고, RAT 확인 후 및 메시지 필터 전에 수신자를 수정합니다. "이메일 파이프라인 이해" 장을 참조해 주십시오.

참고 별칭 테이블 기능은 실제로 이메일의 봉투 수신자를 재작성합니다. 이는 이메일의 봉투 수신자를 재작성하지 않고 단순히 이메일을 지정된 도메인으로 재라우팅하는 `smtproutes` 명령(반송된 이메일 전달, 694 페이지 참조)과 다릅니다.

관련 주제

- 명령줄에서 별칭 테이블 구성, 672 페이지
- 별칭 테이블 내보내기 및 가져오기 , 673 페이지
- 별칭 테이블에서 항목 삭제, 673 페이지

명령줄에서 별칭 테이블 구성

별칭 테이블은 섹션에서 다음과 같이 정의됩니다. 각 섹션의 시작 부분에는 해당 섹션과 관련된 도메인 목록인 도메인 컨텍스트가 있고, 그 뒤에는 맵의 목록이 나옵니다.

도메인 컨텍스트는 쉼표로 구분하고 대괄호('[' 및 ']')로 표시하는 하나 이상의 도메인 또는 부분 도메인 목록입니다. 도메인은 RFC 1035, 섹션 2.3.1., "Preferred name syntax"에 정의된 문자, 숫자, 하이픈 및 마침표를 포함하는 문자열입니다. .example.com과 같은 부분 도메인은 마침표로 시작되는 도메인입니다. 부분 도메인과 일치하는 하위 문자열로 끝나는 모든 도메인은 일치 항목으로 간주됩니다. 예를 들어 도메인 컨텍스트 `.example.com`은 `mars.example.com` 및 `venus.example.com`과 일치합니다. 도메인 컨텍스트 아래에는 맵 목록이 있으며, 이러한 별칭 뒤에는 수신자 목록이 나옵니다. 지도는 다음과 같이 작성됩니다.

표 ***53:*** 별칭 테이블 구문

LHS(Left-hand Side)	구분자	**RHS(Right-hand Side)**
확인할 하나 이상의 별칭의 목록	콜론 문자(":")	하나 이상의 수신자 주소 또는 별칭의 목록

LHS(Left-hand Side)의 별칭은 다음 형식을 포함할 수 있습니다.

`username`	확인할 별칭을 지정합니다. 앞에 오는 "domains" 특성이 테이블에 지정되어 있어야 합니다. 이 매개변수가 없으면 오류가 발생합니다.
`user@domain`	확인할 정확한 이메일 주소를 지정합니다.

단일 LHS(Left-hand Side) 줄에 쉼표로 구분하여 여러 별칭을 입력할 수 있습니다.

RHS(Right-hand Side)의 각 수신자는 전체 `user@domain` 이메일 주소이거나 다른 별칭일 수 있습니다.

별칭 파일은 암시적 도메인이 없는 "전역" 별칭(특정 도메인이 아니라 전역적으로 적용되는 별칭)을 포함하거나, 별칭이 하나 이상의 암시적 도메인을 가지는 도메인 컨텍스트를 포함하거나, 둘을 모두 포함할 수 있습니다.

별칭의 "체인"(또는 재귀 항목)을 만들 수 있지만, 각각은 전체 이메일 주소로 끝나야 합니다.

sendmail 컨피그레이션의 컨텍스트와 호환되도록, 메시지 삭제를 위한 `/dev/null`의 특수 대상이 지원됩니다. 메시지가 `/dev/null`에 매핑되면 삭제됨(dropped) 카운터가 증가합니다. (자세한 내용은 "CLI를 통한 관리 및 모니터링" 장을 참조해 주십시오.) 수신자는 수락되지만 대기열에 추가되지 않습니다.

관련 주제

- 별칭 테이블 예, 673 페이지
- aliasconfig 명령 예, 675 페이지

별칭 테이블 내보내기 및 가져오기

별칭 테이블을 가져오려면 먼저 FTP, SSH 및 SCP 액세스, 1199 페이지 항목을 참조하여 어플라이언스에 액세스할 수 있는지 확인합니다.

`aliasconfig` 명령의 `export` 하위 명령을 사용하여 기존 별칭 테이블을 저장합니다. 이름을 지정한 파일이 리스너에 대한 `/configuration` 디렉터리에 기록됩니다. CLI 외부에서 이 파일을 수정한 다음 다시 가져올 수 있습니다. (파일에 형식이 잘못된 항목이 있으면 파일을 가져오려고 할 때 오류가 표시됩니다.)

별칭 테이블 파일을 `/configuration` 디렉터리에 두고, `aliasconfig` 명령의 `import` 하위 명령을 사용하여 파일을 업로드합니다.

각 줄의 앞에 숫자 기호(#)를 사용하여 테이블에서 줄을 코멘트 처리합니다.

별칭 테이블 파일을 가져온 후 컨피그레이션 변경 사항을 적용하려면 `commit` 명령을 실행해야 합니다.

별칭 테이블에서 항목 삭제

CLI(command line interface)를 통해 별칭 테이블에서 항목을 삭제하면 먼저 도메인 그룹을 선택하라는 프롬프트가 표시됩니다. 모든 도메인에 적용되는, 번호가 지정된 별칭 목록을 보려면 "ALL (any domain)" 항목을 선택합니다. 그런 다음 삭제할 별칭의 번호를 선택합니다.

별칭 테이블 예

참고 이 테이블 예의 모든 항목은 코멘트 처리되었습니다.

```
# sample Alias Table file

# copyright (c) 2001-2005, IronPort Systems, Inc.

#

# Incoming Envelope To addresses are evaluated against each

# entry in this file from top to bottom. The first entry that

# matches will be used, and the Envelope To will be rewritten.

#

# Separate multiple entries with commas.

#

# Global aliases should appear before the first domain

# context. For example:

#

# admin@example.com: administrator@example.com
```

```
# postmaster@example.net: administrator@example.net
#
# This alias has no implied domain because it appears
# before a domain context:
#
# someaddr@somewhere.dom: specificperson@here.dom
#
# The following aliases apply to recipients @ironport.com and
# any subdomain within .example.com because the domain context
# is specified.
#
# Email to joe@ironport.com or joe@foo.example.com will
# be delivered to joseph@example.com.
#
# Similarly, email to fred@mx.example.com will be
# delivered to joseph@example.com
#
# [ironport.com, .example.com]
#
# joe, fred: joseph@example.com
#
# In this example, email to partygoers will be sent to
# three addresses:
#
# partygoers: wilma@example.com, fred@example.com, barney@example.com
#
# In this example, mail to help@example.com will be delivered to
# customercare@otherhost.dom. Note that mail to help@ironport.com will
# NOT be processed by the alias table because the domain context
# overrides the previous domain context.
#
# [example.com]
```

```
#
# help: customercare@otherhost.dom
#
# In this example, mail to nobody@example.com is dropped.
#
# nobody@example.com: /dev/null
#
# "Chains" may be created, but they must end in an email address.
# For example, email to "all" will be sent to 9 addresses:
#
# [example.com]
#
# all: sales, marketing, engineering
# sales: joe@example.com, fred@example.com, mary@example.com
# marketing:bob@example.com, advertising
# engineering:betty@example.com, miles@example.com, chris@example.com
# advertising:richard@example.com, karen@advertising.com
```

aliasconfig 명령 예

이 예에서는 별칭 테이블을 작성하는 데 `aliasconfig` 명령이 사용됩니다. 먼저 **example.com**의 도메인 컨텍스트가 지정됩니다. 그러면 `customercare@example.com`으로 전송된 이메일이 `bob@example.com`, `frank@example.com` 및 `sally@example.com`으로 리디렉션되도록 **customercare**의 별칭이 작성됩니다. 그런 다음 admin으로 전송된 이메일이 `administrator@example.com`으로 리디렉션되도록 **admin**의 전역 별칭이 작성됩니다. 마지막으로 확인을 위해 별칭 테이블이 출력됩니다.

테이블이 출력되면 admin의 전역 별칭이 `example.com`의 첫 번째 도메인 컨텍스트 전에 나타납니다.

```
mail3.example.com> aliasconfig

No aliases in table.

Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import aliases from a file.

[]> new


How do you want your aliases to apply?

1. Globally
```

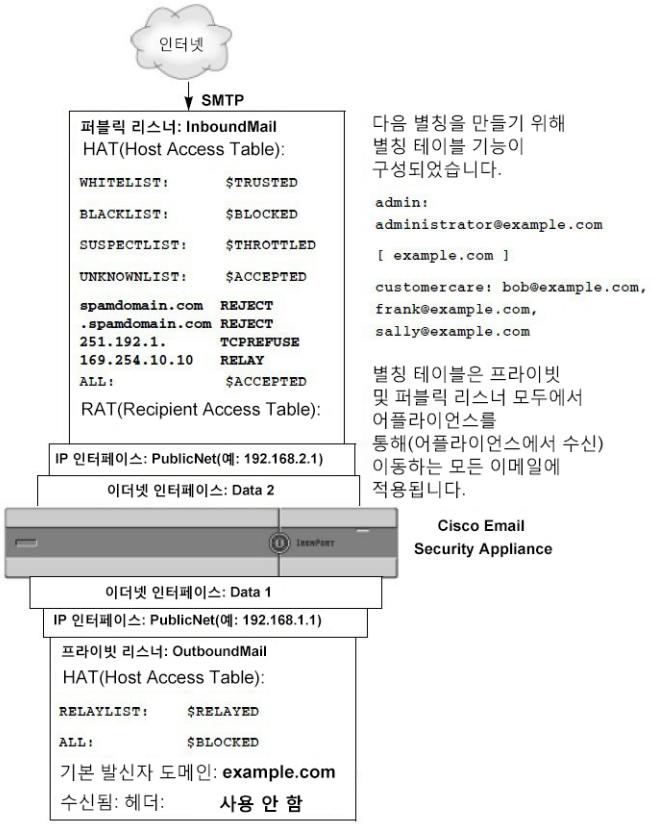
```
2. Add a new domain context

[1]> 2

Enter new domain context.

Separate multiple domains with commas.

Partial domains such as .example.com are allowed.

[]> example.com

Enter the alias(es) to match on.

Separate multiple aliases with commas.

Allowed aliases:

- "user" - This user in this domain context.

- "user@domain" - This email address.

[]> customercare

Enter address(es) for "customercare".

Separate multiple addresses with commas.

[]> bob@example.com, frank@example.com, sally@example.com

Adding alias customercare: bob@example.com,frank@example.com,sally@example.com

Do you want to add another alias? [N]> n

There are currently 1 mappings defined.

Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- PRINT - Display the table.

- IMPORT - Import aliases from a file.

- EXPORT - Export table to a file.

- CLEAR - Clear the table.

[]> new

How do you want your aliases to apply?

1. Globally

2. Add a new domain context
```

```
3. example.com
[1]> 1
Enter the alias(es) to match on.
Separate multiple aliases with commas.
Allowed aliases:
- "user@domain" - This email address.
- "user" - This user for any domain
- "@domain" - All users in this domain.
- "@.partialdomain" - All users in this domain, or any of its sub domains.
[]> admin
Enter address(es) for "admin".
Separate multiple addresses with commas.
[]> administrator@example.com
Adding alias admin: administrator@example.com
Do you want to add another alias? [N]> n

There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]> print
admin: administrator@example.com
[ example.com ]
customercare: bob@example.com, frank@example.com, sally@example.com
There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
```

```
- EDIT - Modify an entry.

- DELETE - Remove an entry.

- PRINT - Display the table.

- IMPORT - Import aliases from a file.

- EXPORT - Export table to a file.

- CLEAR - Clear the table.

[]>
```

이 시점에서 이메일 게이트웨이(Email Gateway) 컨피그레이션은 다음과 같습니다.

그림 ***48:*** 어플라이언스에 대해 정의된 별칭 테이블



가장 구성

Masquerading(가장)은 작성한 테이블에 따라 리스너에서 처리되는 이메일에서 Envelope Sender(봉투 발신자)(발신자 또는 MAIL FROM이라고도 함)와 To:, From:, 및/또는 CC: 헤더를 재작성합니다. 이 기능의 일반적인 구현 예는 단일 사이트에서 여러 도메인을 호스팅할 수 있는 "가상 도메인"입니다. 또 다른 일반적인 구현은 이메일 헤더의 문자열에서 하위 도메인을 "제거"하여 네트워크 인프라를 "숨기는 것"입니다. 가장 기능은 프라이빗 및 퍼블릭 리스너에서 모두 사용 가능합니다.

참고 전체 시스템에 대해 구성되는 별칭 테이블 기능과는 달리 가장 기능은 리스너 단위로 구성됩니다.

리스너는 가장 테이블에서 일치를 확인하고 메시지가 작업 대기열에 있는 동안, LDAP 수신자 수락 쿼리 직후, LDAP 라우팅 쿼리 전에 수신자를 수정합니다. "이메일 파이프라인 이해" 장을 참조해 주십시오.

가장 기능은 봉투 발신자의 주소 및 수신된 이메일의 To:, From:, CC: 필드를 실제로 재작성합니다. 만든 각 리스너에 대해 두 가지 방법 중 하나를 사용하여 서로 다른 가장 매개변수를 지정할 수 있습니다.

- 만든 매핑의 고정 테이블을 통해
- LDAP 쿼리를 통해

이 섹션에서는 고정 테이블 방법에 대해 설명합니다. 테이블 형식은 일부 Unix 시스템에 있는 sendmail 컨피그레이션의 /etc/mail/genericstable 기능과 정방향으로 호환됩니다. LDAP 가장 쿼리에 대한 자세한 내용은 LDAP 쿼리, 735 페이지 항목을 참고하십시오.

관련 주제

- 가장 및 altsrchost, 679 페이지

가장 및 altsrchost

일반적으로 가장 기능은 봉투 발신자를 재작성하며, 메시지에 대해 수행되는 후속 작업은 가장 주소로부터 "트리거"됩니다. 그러나 CLI에서 altscrchost 명령을 실행하면 원래 주소에서(수정되고 가장된 주소가 아님) altsrchost 매핑이 트리거됩니다.

자세한 내용은 호스팅된 모든 도메인에 대한 메일 게이트웨이 구성에 Virtual Gateway™ 기술 사용, 718 페이지및 검토: 이메일 파이프라인, 730 페이지를 참조하십시오.

관련 주제

- 고정 가장 테이블 구성, 679 페이지
- 프라이빗 리스너용 샘플 가장 테이블, 681 페이지
- 가장 테이블 가져오기 , 681 페이지
- 가장 예 , 681 페이지

고정 가장 테이블 구성

listenerconfig 명령의 edit -> masquerade 하위 명령을 사용하여 정적 마스커레이드 매핑 테이블을 구성합니다. 또는 매핑이 포함된 파일을 가져올 수 있습니다. 가장 테이블 가져오기 , 681 페이지를 참조하십시오. 이 하위 명령은 입력 주소, 사용자 이름 및 도메인을 새 주소와 도메인에 매핑하는 테이블을 만들고 유지 관리합니다. LDAP 가장 쿼리에 대한 자세한 내용은 LDAP 쿼리, 735 페이지 항목을 참고하십시오.

메시지가 시스템에 주입될 때 헤더에서 일치가 발견되면 테이블을 참조하여 메시지가 재작성됩니다.

도메인 가장 테이블은 다음과 같이 작성됩니다.

표 ***54:*** 가장 테이블 구문

LHS(Left-hand Side)	구분자	**RHS(Right-hand Side)**
확인할 하나 이상의 사용자 이름 및/또는 도메인의 목록	공백(스페이스 또는 탭 문자)	재작성된 사용자 이름 및/또는 도메인

다음 표에는 가장 테이블에 있는 유효한 항목이 나열되어 있습니다.

LHS(Left-hand Side)	**RHS(Right-hand Side)**
`username`	`username@domain`
이 항목은 확인할 사용자 이름을 지정합니다. LHS(Left-hand Side)의 사용자 이름을 확인하는 수신 이메일 메시지는 RHS(Right-hand Side)의 주소와 확인되고 재작성됩니다. RHS(Right-hand Side)는 전체 주소여야 합니다.	
`user@domain`	`username@domain`
이 항목은 확인할 정확한 주소를 지정합니다. LHS(Left-hand Side)의 전체 주소를 확인하는 수신 메시지는 RHS(Right-hand Side)에 나열된 주소로 재작성됩니다. RHS(Right-hand Side)는 전체 주소여야 합니다.	
`@domain`	`@domain`
이 항목은 지정된 도메인의 주소를 지정합니다. LHS(Left-hand Side)의 원래 도메인은 RHS(Right-hand Side)의 도메인으로 교체되고 사용자 이름은 그대로 유지됩니다.	
`@.partialdomain`	`@domain`
이 항목은 지정된 도메인의 주소를 지정합니다. LHS(Left-hand Side)의 원래 도메인은 RHS(Right-hand Side)의 도메인으로 교체되고 사용자 이름은 그대로 유지됩니다.	
`ALL`	`@domain`
ALL 항목은 베어(bare) 주소를 확인하고 RHS(Right-hand Side)의 주소로 재작성합니다. RHS(Right-hand Side)는 "@"이 앞에 오는 도메인이어야 합니다. 이 항목은 테이블에 있는 위치와 상관없이 우선 순위가 항상 최하위입니다. 참고 `ALL` 항목은 프라이빗 리스너에만 사용할 수 있습니다.	

- 규칙은 가장 테이블에 나타나는 순서대로 확인됩니다.
- 헤더에 있는 From:, To: 및 CC: 필드의 주소는 기본적으로 수신될 때 확인 및 재작성됩니다. 봉투 발신자를 확인 및 재작성할 옵션을 구성할 수도 있습니다. config 하위 명령을 사용하여 봉투 발신자 및 재작성할 헤더를 활성화 및 비활성화합니다.
- 각 줄의 앞에 숫자 기호(#)를 사용하여 테이블에서 줄을 코멘트 처리할 수 있습니다. # 뒤에서 해당 줄 끝 사이의 모든 내용은 코멘트로 간주되어 무시됩니다.

- 가장 테이블은 `new` 하위 명령을 사용하여 생성하든, 아니면 파일에서 가져오든 상관없이 400,000개 항목으로 제한됩니다.

프라이빗 리스너용 샘플 가장 테이블

```
# sample Masquerading file

@.example.com @example.com # Hides local subdomains in the header

sales sales_team@success.com

@techsupport tech_support@biggie.com

user@localdomain user@company.com

ALL @bigsender.com
```

가장 테이블 가져오기

기존의 sendmail `/etc/mail/genericstable` 파일을 가져올 수 있습니다. `genericstable` 파일을 가져오려면 먼저 FTP, SSH 및 SCP 액세스, 1199 페이지 항목을 참고하여 어플라이언스에 액세스할 수 있는지 확인합니다.

`genericstable` 파일을 configuration 디렉터리에 두고, `masquerade` 명령의 `import` 하위 명령을 사용하여 파일을 업로드합니다. 다음 순서로 명령을 사용합니다.

```
listenerconfig -> edit -> listener_number -> masquerade -> import
```

또는 `export` 하위 명령을 사용하여 기존의 컨피그레이션을 다운로드할 수 있습니다. 이름을 지정한 파일이 configuration 디렉터리에 기록됩니다. CLI 외부에서 이 파일을 수정한 다음 다시 가져올 수 있습니다.

`import` 하위 명령을 사용할 경우 파일에 유효한 항목만 포함되어 있는지 확인하십시오. 잘못된 항목(예: right-hand side 없는 left-hand side)이 포함되어 있으면 파일을 가져올 때 CLI에서 구문 오류를 보고합니다. 가져오는 동안 구문 오류가 발생하면 전체 파일의 매핑을 가져올 수 없습니다.

리스너에 대한 컨피그레이션 변경 사항을 적용하려면 `genericstable` 파일을 가져온 후 `commit` 명령을 실행해야 합니다.

가장 예

이 예에서는 `listenerconfig`의 `masquerade` 하위 명령을 사용하여 PrivateNet 인터페이스에 "OutboundMail"이라는 프라이빗 리스너에 대한 도메인 가장 테이블을 작성합니다.

먼저, 가장에 LDAP를 사용하는 옵션을 비활성화합니다. (LDAP 가상 쿼리 구성에 대한 자세한 내용은 LDAP 쿼리, 735 페이지 항목을 참고하십시오.)

그런 다음, `.example.com`의 하위 도메인에 있는 시스템에서 전송된 이메일이 `example.com`에 매핑되도록 **`@.example.com`**의 부분 도메인 표기법을 **`@example.com`**에 매핑합니다. 그런 다음 사용자 이름 **`joe`**를 도메인 **`joe@example.com`**에 매핑합니다. 두 항목을 모두 확인할 수 있도록 도메인 가장 테이블을 출력한 후 `masquerade.txt`라는 파일로 내보냅니다. `config` 하위 명령을 사용하여 CC: 필드에 있는 주소 재작성을 비활성화하고, 마지막으로 변경 사항을 커밋합니다.

```
mail3.example.com> listenerconfig
```

```
Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit

Enter the name or number of the listener you wish to edit.

[]> 2

Name: OutboundMail

Type: Private

Interface: PrivateNet (192.168.1.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.
```

```
- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should
be accepted or bounced/dropped.

- LDAPROUTING - Configure an LDAP query to reroute messages.

- LDAPGROUP - Configure an LDAP query to determine whether a sender or

recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.

[]> masquerade

Do you want to use LDAP for masquerading? [N]> n

Domain Masquerading Table

There are currently 0 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> new


Enter the source address or domain to masquerade.

Usernames like "joe" are allowed.

Full addresses like "user@example.com" are allowed.

Full addresses with subdomain wildcards such as "username@.company.com" are allowed.

Domains like @example.com and @.example.com are allowed.

Hosts like @training and @.sales are allowed.

[]> @.example.com

Enter the masqueraded address or domain.

Domains like @example.com are allowed.

Full addresses such as user@example.com are allowed.

[]> @example.com

Entry mapping @.example.com to @example.com created.
```

```
Domain Masquerading Table

There are currently 1 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> new


Enter the source address or domain to masquerade.

Usernames like "joe" are allowed.

Full addresses like "user@example.com" are allowed.

Full addresses with subdomain wildcards such as "username@.company.com" are allowed.

Domains like @example.com and @.example.com are allowed.

Hosts like @training and @.sales are allowed.

[]> joe

Enter the masqueraded address.

Only full addresses such as user@example.com are allowed.

[]> joe@example.com

Entry mapping joe to joe@example.com created.

Domain Masquerading Table

There are currently 2 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.
```

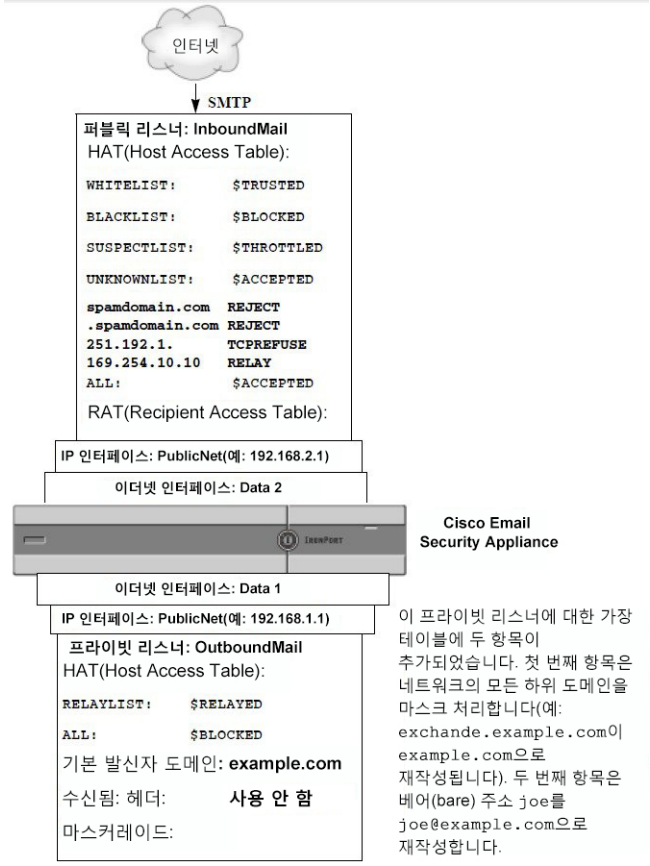
```
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]> print
@.example.com @example.com

joe joe@example.com
Domain Masquerading Table
There are currently 2 entries.
Masqueraded headers: To, From, Cc
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]> export
Enter a name for the exported file:
[]> masquerade.txt
Export completed.
Domain Masquerading Table
There are currently 2 entries.
Masqueraded headers: To, From, Cc
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
```

```
[]> config

Do you wish to masquerade Envelope Sender?

[N]> y

Do you wish to masquerade From headers?

[Y]> y

Do you wish to masquerade To headers?

[Y]> y

Do you wish to masquerade CC headers?

[Y]> n

Do you wish to masquerade Reply-To headers?

[Y]> n

Domain Masquerading Table

There are currently 2 entries.

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]>

Name: OutboundMail

Type: Private

Interface: PrivateNet (192.168.1.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default
```

```
Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should
be accepted or bounced/dropped.

- LDAPROUTING - Configure an LDAP query to reroute messages.

- LDAPGROUP - Configure an LDAP query to determine whether a sender or
recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.


[]>

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.


[]>
```

이제 엔터프라이즈 게이트웨이(Enterprise Gateway) 컨피그레이션은 다음과 같습니다.

그림 ***49:*** 프라이빗 리스너에 대해 정의된 가장



도메인 맵 기능

리스너에 대한 "도메인 맵"을 구성할 수 있습니다. 구성하는 각 리스너에 대해 도메인 맵 테이블을 작성할 수 있습니다. 그러면 도메인 맵 테이블의 도메인과 일치하는 메시지에서 각 수신자에 대한 봉투 수신자가 재작성됩니다. 이 기능은 sendmail "도메인 테이블" 또는 Postfix "가상 테이블" 기능과 유사합니다. 봉투 수신자만 영향을 받으며 "To:" 헤더는 이 기능으로 재작성되지 않습니다.

참고 도메인 맵 기능의 처리는 RAT 직전 및 기본 도메인 평가 직후에 발생합니다. "이메일 파이프라인 이해" 장을 참조하십시오.

도메인 맵 기능의 일반 구현은 둘 이상의 레거시 도메인에 대한 수신 메일을 수락하는 것입니다. 예를 들어 회사에서 다른 회사를 인수한 경우, 인수한 회사에 대한 메시지를 수락하기 위해 어플라이언스에 도메인 맵을 작성하고 회사의 현재 도메인에 대한 봉투 수신자를 재작성할 수 있습니다.

참고 최대 20,000개의 고유한 도메인 매핑을 구성할 수 있습니다.

표 ***55:*** 도메인 맵 테이블 구문 예

Left Side	**Right Side**	코멘트
`username@example.com`	**username2@example.net**	Right Side에 대한 완전한 주소만
`user@.example.com`	**user2@example.net**	
`@example.com`	**user@example.net** 또는 **@example.net**	완전한 주소 또는 인증된 도메인 이름
`@.example.com`	**user@example.net** 또는 **@example.net**	

다음 예에서는 퍼블릭 리스너 "InboundMail"에 대한 도메인 맵을 작성하기 위해 `listenerconfig` 명령의 `domainmap` 하위 명령이 사용됩니다. `oldcompanyname.com`의 도메인 및 하위 도메인에 대한 메일이 도메인 `example.com`에 매핑됩니다. 확인을 위해 매핑이 출력됩니다. 이 예는 두 도메인을 모두 리스너의 RAT에 두는 구성과 대조됩니다. 도메인 맵 기능은 실제로 `joe@oldcomapanyname.com`의 봉투 수신자를 `joe@example.com`으로 재작성합니다. 반면 도메인 `oldcompanyname.com`을 리스너의 RAT에 두면 `joe@oldcompanyname.com`에 대한 메시지가 수락되고 봉투 수신자 재작성 없이 라우팅됩니다. 또한 이 예는 별칭 테이블 기능과도 대조됩니다. 별칭 테이블은 반드시 명시적 주소로 환원되어야 하며, "임의의 사용자 이름`@domain`"이 "동일한 사용자 이름`@newdomain`"에 매핑되도록 작성할 수 없습니다.

```
mail3.example.com> listenerconfig

Currently configured listeners:

1. Inboundmail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

2. Outboundmail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit

Enter the name or number of the listener you wish to edit.

[]> 1
```

```
Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

[]> domainmap

Domain Map Table

There are currently 0 Domain Mappings.

Domain Mapping is: disabled

Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import domain mappings from a file.

[]> new
```

```
Enter the original domain for this entry.
Domains such as "@example.com" are allowed.
Partial hostnames such as "@.example.com" are allowed.
Email addresses such as "test@example.com" and "test@.example.com"
are also allowed.
[]> @.oldcompanyname.com
Enter the new domain for this entry.
The new domain may be a fully qualified
such as "@example.domain.com" or a complete
email address such as "test@example.com"
[]> @example.com
Domain Map Table
There are currently 1 Domain Mappings.
Domain Mapping is: enabled
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display all domain mappings.
- IMPORT - Import domain mappings from a file.
- EXPORT - Export domain mappings to a file.
- CLEAR - Clear all domain mappings.
[]> print
@.oldcompanyname.com --> @example.com
Domain Map Table
There are currently 1 Domain Mappings.
Domain Mapping is: enabled
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display all domain mappings.
```

```
- IMPORT - Import domain mappings from a file.

- EXPORT - Export domain mappings to a file.

- CLEAR - Clear all domain mappings.

[]>

Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Enabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

[]>
```

관련 주제

- 도메인 맵 테이블 가져오기 및 내보내기 , 693 페이지

도메인 맵 테이블 가져오기 및 내보내기

도메인 맵 테이블을 가져오거나 내보내려면 FTP, SSH 및 SCP 액세스, 1199 페이지 항목을 참고하여 어플라이언스에 액세스할 수 있는지 확인하십시오.

매핑할 도메인 항목의 텍스트 파일을 만듭니다. 항목은 공백(탭 문자 또는 공백)으로 구분합니다. 각 줄의 앞에 숫자 기호(#)를 사용하여 테이블에서 줄을 코멘트 처리합니다.

파일을 configuration 디렉터리에 두고, `domain` 명령의 import 하위 명령을 사용하여 파일을 업로드합니다. 다음 순서로 명령을 사용합니다.

```
listenerconfig ->  edit ->  inejctor_number -> domainmap -> import
```

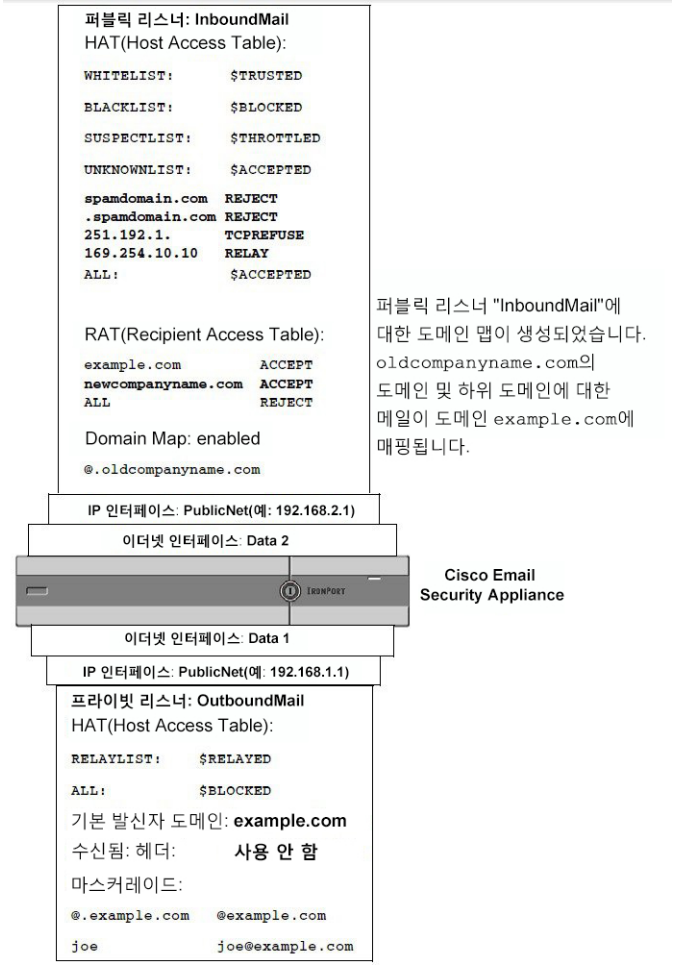
또는 `export` 하위 명령을 사용하여 기존의 컨피그레이션을 다운로드할 수 있습니다. 이름을 지정한 파일이 configuration 디렉터리에 기록됩니다. CLI 외부에서 이 파일을 수정한 다음 다시 가져올 수 있습니다.

`import` 하위 명령을 사용할 경우 파일에 유효한 항목만 포함되어 있는지 확인하십시오. 잘못된 항목(예: right-hand side 없는 left-hand side)이 포함되어 있으면 파일을 가져올 때 CLI에서 구문 오류를 보고합니다. 가져오는 동안 구문 오류가 발생하면 전체 파일의 매핑을 가져올 수 없습니다.

리스너에 대한 컨피그레이션 변경 사항을 적용하려면 도메인 맵 테이블 파일을 가져온 후 `commit` 명령을 실행해야 합니다.

이제 엔터프라이즈 게이트웨이(Enterprise Gateway) 컨피그레이션은 다음과 같습니다.

그림 ***50:*** 퍼블릭 리스너에 대해 정의된 도메인 맵



반송된 이메일 전달

반송된 이메일은 이메일 전달에서 피할 수 없는 부분입니다. 어플라이언스는 고도로 구성 가능한 여러 방법으로 반송된 이메일을 처리할 수 있습니다.

어플라이언스가 수신 메일을 기반으로 발신 반송을 생성하는 방법을 어떻게 제어하는지에 대해 설명합니다. 어플라이언스가 발신 메일을 기반으로 수신 반송을 제어하는 방법을 제어하려면 반송 확인을 사용합니다(반송 확인, 703 페이지 참조).

관련 주제

- 전달 불가 이메일 처리, 695 페이지
- 새 반송 프로필 만들기, 701 페이지
- 리스너에 반송 프로필 적용, 702 페이지

전달 불가 이메일 처리

운영 체제는 전달 불가 이메일 또는 "반송된 메시지"를 다음 범주로 분류합니다.

"대화형" 반송: 원격 도메인은 초기 **SMTP** 대화 중에 메시지를 반송합니다.	
소프트 반송	일시적으로 전달할 수 없는 메시지. 예를 들어 사용자 사서함이 꽉 찼을 수 있습니다. 이러한 메시지는 나중에 재시도될 수 있습니다. (예: SMTP 4XX 오류 코드.)
하드 반송	영구적으로 전달할 수 없는 메시지. 예를 들면 사용자가 해당 도메인에 더 이상 존재할 수 없습니다. 이러한 메시지는 재시도되지 않습니다. (예: SMTP 5XX 오류 코드.)
"지연된"(또는 "비대화형") 반송: 원격 도메인은 전달할 메시지를 일단 수락하고, 나중에 반송합니다.	
소프트 반송	일시적으로 전달할 수 없는 메시지. 예를 들어 사용자 사서함이 꽉 찼을 수 있습니다. 이러한 메시지는 나중에 재시도될 수 있습니다. (예: SMTP 4XX 오류 코드.)
하드 반송	영구적으로 전달할 수 없는 메시지. 예를 들면 사용자가 해당 도메인에 더 이상 존재할 수 없습니다. 이러한 메시지는 재시도되지 않습니다. (예: SMTP 5XX 오류 코드.)

사용자가 만드는 각 리스너에 대해 AsyncOS가 하드 및 소프트 대화형 반송을 처리하는 방법을 구성하려면 GUI에서 Network(네트워크) 메뉴의 Bounce Profiles(반송 프로필) 페이지(또는 `bounceconfig` 명령)를 사용합니다. 반송 프로파일을 만든 다음 `Network(네트워크) > Listeners(리스너)` 페이지(또는 `listenerconfig` 명령)를 통해 각 리스너에 프로파일을 적용합니다. 메시지 필터를 사용하여 반송 프로필을 특정 메시지에 할당할 수도 있습니다. (자세한 내용은 메시지 필터를 사용하여 이메일 정책 적용, 137 페이지 항목을 참고하십시오.)

관련 주제

- 소프트 및 하드 반송에 대한 참고 사항, 695 페이지
- 반송 프로필 매개변수, 696 페이지
- 하드 반송 및 status 명령, 699 페이지
- 대화형 반송 및 SMTP 경로 메시지 필터 작업, 700 페이지
- 반송 프로필 예, 700 페이지
- 전달 상태 알림 형식, 700 페이지
- 지연 경고 메시지, 701 페이지
- 지연 경고 메시지 및 하드 반송, 701 페이지

소프트 및 하드 반송에 대한 참고 사항

- 대화형 소프트 반송의 경우, 수신자 전달이 일시적으로 실패할 때마다 소프트 반송 이벤트가 정의됩니다. 단일 수신자가 여러 번의 소프트 반송 이벤트를 일으킬 수 있습니다. 각 소프트 반송

이벤트에 대한 매개변수를 구성하려면 Bounce Profiles(반송 프로필) 페이지 또는 bounceconfig 명령을 사용합니다. (반송 프로필 매개변수, 696 페이지 참조.)

- 기본적으로 각 하드 반송된 수신자에 대해 시스템에서는 반송 메시지를 생성하여 원래 발신자에게 전송합니다. 메시지 봉투의 Envelope Sender(봉투 발신자)에 정의된 주소로 메시지가 전송됩니다. Envelope Sender(봉투 발신자)를 Envelope From으로 지칭하기도 합니다. 이 기능을 비활성화하고, 대신 하드 반송에 대한 정보를 로그 파일에서 찾을 수도 있습니다. ("로깅" 장을 참조해 주십시오.)
- 대기열에서 최대 시간이 지나거나 최대 재시도 횟수에 도달하면(먼저 오는 것이 적용됨) 소프트 반송은 하드 반송이 됩니다.

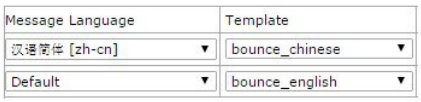
반송 프로필 매개변수

반송 프로필을 구성할 때 다음 매개변수는 메시지 단위로 대화형 반송이 처리되는 방식을 제어합니다.

표 ***56:*** 반송 프로필 매개변수

Maximum number of retries(최대 재시도 횟수**)**	소프트 반송된 메시지가 하드 반송된 메시지로 전화되기 전, 시스템이 해당 메시지를 다시 전달하기 위해 수신자 호스트에 다시 연결하려고 시도하는 횟수. 기본값은 100입니다.
Maximum number of seconds in queue(대기열에 머무는 최대 초 단위 시간**)**	소프트 반송된 메시지가 하드 반송된 메시지로 전화되기 전, 시스템이 해당 메시지를 다시 전달하기 위해 수신자 호스트에 연결하려고 시도하는 데 사용하는 기간. 기본값은 259,200초(72시간)입니다,
Initial number of seconds to wait before retrying a message(메시지 재시도 전에 기다리는 초기 초 단위 시간**)**	소프트 반송된 메시지를 다시 전달하려고 처음 시도하기 전 시스템이 기다려야 하는 시간. 기본값은 60초입니다. 소프트 반송 시도 빈도를 줄이려면 초기 재시도 시간을 높은 값으로 설정하십시오. 반대로, 빈도를 높이려면 값을 낮게 설정하십시오.
Maximum number of seconds to wait before retrying a message(메시지 재시도 전에 기다리는 최대 초 단위 시간**)**	소프트 반송된 메시지를 다시 전달하려고 재시도하기 전 시스템이 기다려야 하는 최대 시간. 기본값은 3,600초(1시간)입니다. 이 값은 각 후속 시도 사이의 간격이 아니라, 재시도 횟수를 제어하는 데 사용할 수 있는 또 다른 매개변수입니다. 초기 재시도 간격은 최대 재시도 간격에 의해 하이엔드에서 제한됩니다. 계산된 재시도 간격 기간이 최대 재시도 간격을 초과하면, 최대 재시도 간격이 대신 사용됩니다.

하드 반송 메시지 전송	하드 반송을 위해 반송 메시지를 보낼지 여부를 지정합니다. 이 옵션을 활성화한 경우 반송 메시지의 형식을 선택할 수 있습니다. 반송 메시지는 기본적으로 DSN 형식(RFC 1894)을 사용합니다. 원본 메시지(제목 및 본문)의 언어를 기반으로 맞춤형 반송 메시지로 보낼 수도 있습니다. 예를 들어, 중국어로 된 메시지에 대해 중국어로 된 반송 메시지를 전송하고, 다른 언어로 된 모든 메시지에 대해 영어로 된 반송 메시지를 전송할 수 있습니다. **Notification Template(**알림 템플릿)에서 **Add Row(**행 추가**)**를 클릭하고 사용할 메시지 언어 및 템플릿을 선택합니다. 참고 기본 항목(**Default(**기본값**)**로 설정된 **Message Language(**메시지 언어**))**을 삭제하지 않아야 합니다. 기본 항목에 대한 반송 알림 템플릿을 변경할 수 있습니다. 다음 시나리오에서 메시지의 언어는 기본값으로 간주됩니다. • 메시지의 언어가 다른 알림 템플릿 항목에서 선택한 언어와 다른 경우. • 메시지의 언어를 Cisco Email Security Appliance에서 지원하지 않는 경우. • 어플라이언스에서 메시지의 언어를 탐지할 수 없는 경우. • 메시지의 내용(제목 및 본문)이 50바이트보다 작은 경우. 위의 예(중국어로 된 메시지에 대해 중국어로 된 반송 메시지를 전송하고, 다른 언어로 된 모든 메시지에 대해 영어로 된 반송 메시지를 전송)를 구성하는 동안 알림 템플릿 테이블은 다음과 같이 표시됩니다.  또한 반송 응답에서 DSN 상태 필드를 구문 분석할지 여부를 선택할 수 있습니다. "Yes(예)"를 선택하면 어플라이언스는 반송 응답에서 DSN 상태 코드(RFC 3436)를 검색하고, 전달 상태 알림의 Status(상태) 필드에 있는 코드를 사용합니다.

Send Delay Warning Messages(지연 경고 메시지 전송)	지연 전달에 대해 경고 메시지를 보낼지 여부를 지정합니다. 이 옵션을 활성화한 경우 원본 메시지(제목 및 본문)의 언어를 기반으로 맞춤형 지연 경고 메시지를 구성할 수 있습니다. 예를 들어, 중국어로 된 메시지에 대해 중국어로 된 지연 경고 메시지를 전송하고, 다른 언어로 된 모든 메시지에 대해 영어로 된 지연 경고 메시지를 전송할 수 있습니다. **Notification Template**(알림 템플릿)에서 **Add Row**(행 추가)를 클릭하고 사용할 메시지 언어 및 템플릿을 선택합니다. 참고 기본 항목(**Default**(기본값)로 설정된 **Message Language**(메시지 언어))을 삭제하지 않아야 합니다. 기본 항목에 대한 반송 알림 템플릿을 변경할 수 있습니다. 다음 시나리오에서 메시지의 언어는 기본값으로 간주됩니다. • 메시지의 언어가 다른 알림 템플릿 항목에서 선택한 언어와 다른 경우. • 메시지의 언어를 Cisco Email Security Appliance에서 지원하지 않는 경우. • 어플라이언스에서 메시지의 언어를 탐지할 수 없는 경우. • 메시지의 내용(제목 및 본문)이 50바이트보다 작은 경우. 위의 예(중국어로 된 메시지에 대해 중국어로 된 지연 경고 메시지를 전송하고, 다른 언어로 된 모든 메시지에 대해 영어로 된 지연 경고 메시지를 전송)를 구성하는 동안 알림 템플릿 테이블은 다음과 같이 표시됩니다.  또한 메시지 간 최소 간격 및 최대 전송 재시도 횟수를 지정할 수 있습니다.
Specify Recipient for Bounces(반송할 수신자 지정)	Envelope Sender(봉투 발신자) 주소의 기본값이 아닌 대체 주소로 메시지를 반송할 수 있습니다.
Use DomainKeys signing for bounce and delay messages(반송 및 지연 메시지에 **DomainKeys** 서명 사용)	반송 및 지연 메시지 서명에 사용할 DomainKeys 프로필을 선택할 수 있습니다. DomainKeys에 대한 자세한 내용은 DomainKeys 및 DKIM 인증, 572 페이지 섹션을 참조해 주십시오.
전역 설정	
Bounce Profiles(반송 프로파일) 페이지의 **Edit Global Settings**(전역 설정 수정) 링크를 통해 또는 **CLI**의 `bounceconfig` 명령을 통해 기본 반송 프로파일을 수정하여 이러한 설정을 구성합니다.	

Initial number of seconds to wait before retrying an unreachable host(도달할 수 없는 호스트에 대한 재시도 전에 기다리는 초기 초 단위 시간**)**	도달할 수 없는 호스트에 대해 재시도하기 전에 시스템이 기다려야 하는 시간. 기본값은 60초입니다.
Max interval allowed between retries to an unreachable host(도달할 수 없는 호스트에 대한 재시도 사이에 허용되는 최대 간격**)**	도달할 수 없는 호스트에 대한 재시도 전에 시스템이 기다려야 하는 최대 시간입니다. 기본값은 3,600초(1시간)입니다. 호스트가 다운되어 초기 전달이 실패하면 초 단위 최소 재시도 값이 지난 후 재시도가 시작되며, 다운된 호스트에 대한 이후의 각 재시도에서 이 최대값(초 단위)까지 기간이 증가합니다.

하드 반송 및 **status** 명령

하드 반송 메시지 생성이 활성화되면 어플라이언스가 전달할 하드 반송 메시지를 생성할 때마다 status 및 status detail 명령의 다음 카운터가 증가합니다.

Counters:	Reset	Uptime	Lifetime
Receiving			
Messages Received	0	0	0
Recipients Received	0	0	0
Gen. Bounce Recipients	0	0	0

자세한 내용은 "CLI를 통한 관리 및 모니터링" 장을 참조해 주십시오. 하드 반송 메시지 생성이 비활성화되면 수신자가 하드 반송될 때 이러한 카운트가 증가하지 않습니다.

참고 메시지 봉투의 Envelope Sender(봉투 발신자) 주소는 메시지 헤더의 From:과 다릅니다. 봉투 발신자 주소와 다른 이메일 주소로 하드 반송 메시지를 전송하도록 AsyncOS를 구성할 수 있습니다.

대화형 반송 및 **SMTP** 경로 메시지 필터 작업

SMTP 경로 및 메시지 필터 작업에 대한 매핑은 대화형 반송 결과로 어플라이언스에서 생성하는 SMTP 반송 메시지의 라우팅에 적용되지 않습니다. 어플라이언스는 대화형 반송 메시지를 수신하면 원래 메시지의 봉투 발신자에 대한 SMTP 반송 메시지를 생성합니다. 이 경우 어플라이언스는 실제로 메시지를 생성하므로, 릴레이를 위해 주입된 메시지에 적용되는 SMTP 경로가 적용되지 않습니다.

반송 프로필 예

서로 다른 반송 프로필 매개변수를 사용하는 다음 두 가지 예를 살펴보십시오.

표 ***57:*** 예 ***1:*** 반송 프로필 매개변수

매개변수	값
Max number of retries(최대 재시도 횟수)	2
Max number of seconds in queue(대기열에 머무는 최대 초 단위 시간)	259,200초(72시간)
Initial number of seconds before retrying(재시도 전 초기 초 단위 시간)	60초
Max number of seconds to wait before retrying(재시도 전에 기다리는 최대 초 단위 시간)	60초

예 1에서 첫 번째 수신자 전달 시도는 메시지가 어플라이언스에 주입된 직후인 t=0에 수행됩니다. 기본 초기 재시도 시간 60초에서는 첫 번째 재시도가 약 1분 후인 t=60에 수행됩니다. 재시도 간격이 계산되고, 최대 재시도 간격 60초를 사용하도록 결정됩니다. 따라서 두 번째 재시도는 약 t=120에 수행됩니다. 최대 재시도 횟수는 2이므로 이 재시도 직후 시스템은 해당 수신자에 대한 하드 반송 메시지를 생성합니다.

표 ***58:*** 예 ***2:*** 반송 프로필 매개변수

매개변수	값
Max number of retries(최대 재시도 횟수)	100
Max number of seconds in queue(대기열에 머무는 최대 초 단위 시간)	100초
Initial number of seconds before retrying(재시도 전 초기 초 단위 시간)	60초
Max number of seconds to wait before retrying(재시도 전에 기다리는 최대 초 단위 시간)	120초

예 2에서 첫 번째 전달 시도는 t=0, 첫 번째 재시도는 t=60에 수행됩니다. 다음 전달 시도(t=120에 발생하도록 예약됨) 직전에 시스템은 메시지를 하드 반송합니다. 대기열에 머무는 최대 시간인 100초를 초과했기 때문입니다.

전달 상태 알림 형식

시스템에서 생성하는 반송 메시지는 하드 및 소프트 반송 모두에 기본적으로 DSN(Delivery Status Notification) 형식을 사용합니다. DSN은 RFC 1894(see http://www.faqs.org/rfcs/rfc1894.html 참조)에서

정의한 형식으로, "메시지를 하나 이상의 수신자에게 전달하려는 시도의 결과를 보고하기 위해 MTA(message transfer agent) 또는 전자 메일 게이트웨이에 사용될 수 있는 MIME content-type을 정의합니다." 기본적으로, 메시지 크기가 10k 미만인 경우 전달 상태 알림에는 전달 상태 및 원본 메시지에 대한 설명이 포함됩니다. 메시지 크기가 10k를 초과하면 전달 상태 알림에 메시지 헤더만 포함됩니다. 메시지 헤더가 10k를 초과하면 전달 상태 알림이 헤더를 자릅니다. DSN에서 10k를 초과하는 메시지(또는 메시지 헤더)를 포함하려면 bounceconfig 명령의 max_bounce_copy 매개변수를 사용할 수 있습니다(이 매개변수는 CLI에서만 사용 가능).

지연 경고 메시지

시스템에서 생성하는 대기열 메시지의 시간(지연 알림 메시지)도 DSN 형식을 사용합니다. 기존/새 반송 프로필을 수정하거나 만들고 다음의 기본값을 변경하려면 Network(네트워크) 메뉴의 Bounce Profiles(반송 프로필) 페이지(또는 bounceconfig 명령)를 사용하여 기본 매개변수를 변경합니다.

- 지연 경고 메시지 전송 사이의 최소 간격
- 수신자당 전송할 최대 지연 경고 메시지 수

지연 경고 메시지 및 하드 반송

"Maximum Time in Queue(대기열에 머무는 최대 시간)" 설정과 "Send Delay Warning Messages(지연 경고 메시지 전송)"의 최소 간격에 대해 기간을 매우 짧게 설정하면 동일한 메시지에 대해 지연 경고 및 하드 반송을 동시에 수신할 수 있습니다. Systems에서는 지연 경고 메시지의 전송을 활성화한 경우 이러한 설정의 최소값으로 기본값을 사용할 것을 권장합니다.

또한 어플라이언스에서 생성하는 지연 경고 메시지 및 반송 메시지는 처리 중에 15분까지 지연될 수 있습니다.

새 반송 프로필 만들기

다음 예에서는 Bounce Profiles(반송 프로필) 페이지를 사용하여 bouncepr1이라는 반송 프로필을 만듭니다. 이 프로필에서, 하드 반송된 모든 메시지는 대체 주소인 bounce-mailbox@example.com으로 전송됩니다. 지연 경고 메시지가 활성화됩니다. 수신자당 경고 메시지 하나가 전송되며, 경고 메시지 간 4시간(14400초) 기본값이 수락됩니다.

관련 주제

- 기본 반송 프로필 수정, 701 페이지
- Minimalist 반송 프로필의 예, 702 페이지

기본 반송 프로필 수정

Bounce Profiles(반송 프로필) 목록에서 이름을 클릭하여 원하는 반송 프로필을 수정할 수 있습니다. 기본 반송 프로필을 수정할 수도 있습니다. 이 예에서는 `maximum number of seconds to wait before retrying unreachable hosts(연결할 수 없는 호스트에 재시도할 때까지 대기해야 하는 최대 시간(초))`를 3600(1시간)에서 10800(3시간)으로 올려 기본 프로필을 수정합니다.

Minimalist 반송 프로필의 예

다음 예에서는 minimalist라는 이름의 반송 프로필을 만듭니다. 이 프로필에서는 반송 시 메시지가 재시도되지 않으며(최대 재시도 횟수 0), 재시도 전 기다려야 할 최대 시간이 지정됩니다. 하드 반송 메시지가 비활성화되고, 소프트 반송 경고가 전송되지 않습니다.

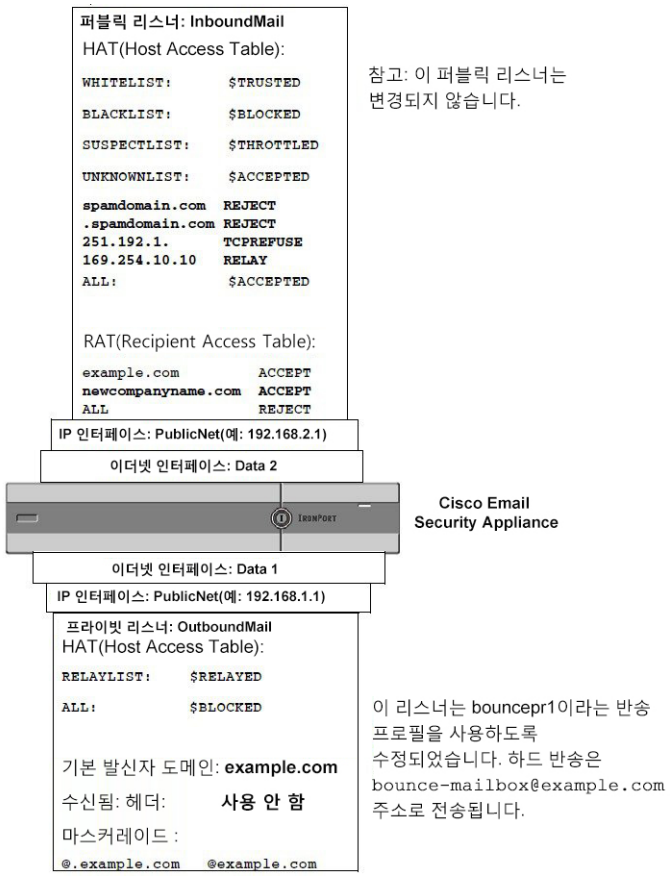
리스너에 반송 프로필 적용

반송 프로파일을 만들었으면 **Network(**네트워크**) > Listeners(**리스너**)** 페이지 또는 **`listenerconfig`** 명령을 사용하여 해당 프로파일을 리스너에 적용할 수 있습니다.

다음 예에서는 OutgoingMail 리스너에 bouncepr1 프로파일이 적용됩니다.

이 시점에서 이메일 게이트웨이 컨피그레이션은 다음과 같습니다.

그림 ***51:*** 프라이빗 리스너에 반송 프로필 적용



대상 제어를 사용하여 이메일 전달 제어

제어되지 않는 대용량 이메일 전달은 수신자 도메인을 마비시킬 수 있습니다. AsyncOS에서는 어플라이언스에서 열 연결 수를 정의하거나 어플라이언스가 각 대상 도메인에 전송할 메시지 수를 정의하여 메시지 전달을 완전히 제어할 수 있습니다.

Destination Controls(대상 제어) 기능(GUI의 Mail Policies(메일 정책) > Destination Controls(대상 제어) 또는 CLI의 destconfig 명령)을 사용하여 다음을 제어할 수 있습니다.

- 속도 제한, 703 페이지
- TLS, 703 페이지
- 반송 확인, 703 페이지
- 반송 프로필, 703 페이지

속도 제한

- Concurrent Connections(동시 연결 수): 어플라이언스가 열기를 시도할 원격 호스트에 대한 동시 연결 수.
- Maximum Messages Per Connection(연결당 최대 메시지 수): 어플라이언스가 새 연결을 시작하기 전 대상 도메인으로 전송할 메시지 수.
- Recipients(수신자): 어플라이언스가 지정된 시간에 지정된 원격 호스트로 전송할 수신자 수.
- Limits(제한): 대상 단위 및 MGA 호스트 이름 단위로 지정한 제한을 적용하는 방법.

TLS

- 원격 호스트에 대한 TLS 연결을 수락할지, 허용할지 또는 요청할지 여부(TLS 제어, 707 페이지 참조).
- TLS 연결을 요청하는 원격 호스트로 메시지를 전달할 때 TLS 협상이 실패하는 경우 알림을 전송할지 여부. 이것은 도메인 단위 설정이 아니라 전역 설정입니다.
- 모든 아웃바운드 TLS 연결에 사용할 TLS 인증서를 원격 호스트에 할당합니다.

반송 확인

- 반송 확인을 통해 주소 태깅을 수행할지 여부(반송 확인, 711 페이지 참조).

반송 프로필

- 지정된 원격 호스트에 대해 어플라이언스에서 사용해야 할 반송 프로필(기본 반송 프로필은 Network(네트워크) > Bounce Profiles(반송 프로필)를 통해 설정).

또한 지정된 도메인에 대한 기본 설정을 제어할 수 있습니다.

관련 주제

- 메일 전달에 사용할 인터페이스 결정, 704 페이지
- 기본 전달 제한, 704 페이지
- 대상 제어 작업, 704 페이지

메일 전달에 사용할 인터페이스 결정

`deliveryconfig` 명령이나 메시지 필터(`alt-src-host`)를 통해 또는 가상 게이트웨이를 사용하여 출력 인터페이스를 지정하지 않는 한, AsyncOS 라우팅 테이블에 의해 출력 인터페이스가 선택됩니다. 기본적으로 "auto"를 선택한다는 것은 AsyncOS에 결정을 맡긴다는 뜻입니다.

더 자세히 말하면, 로컬 주소는 인터페이스 넷마스크를 인터페이스 IP 주소에 적용하여 식별됩니다. 두 가지 모두 Network(네트워크) > Interfaces(인터페이스) 페이지 또는 `interfaceconfig` 명령을 통해 (또는 시스템 설정 중에) 설정됩니다. 주소 공간이 중첩되면 가장 구체적인 넷마스크가 사용됩니다. 대상이 로컬이면 적절한 로컬 인터페이스를 통해 패킷이 전송됩니다.

대상이 로컬이 아니면 패킷은 기본 라우터로 전송됩니다(Network(네트워크) > Routing(라우팅) 페이지 또는 `setgateway` 명령을 통해 설정). 기본 라우터의 IP 주소는 로컬입니다. 출력 인터페이스는 로컬 주소에 대한 출력 인터페이스를 선택하기 위한 규칙에 의해 결정됩니다. 예를 들면 AsyncOS는 기본 라우터의 IP 주소가 포함된 가장 구체적인 IP 주소 및 넷마스크를 선택합니다.

라우팅 테이블은 Network(네트워크) > Routing(라우팅) 페이지(또는 `routeconfig` command명령)를 통해 구성합니다. 라우팅 테이블의 일치 항목이 기본 경로보다 우선 적용됩니다. 더 구체적인 경로가 덜 구체적인 경로보다 우선 적용됩니다.

기본 전달 제한

각 아웃바운드 대상 도메인은 자체 아웃바운드 대기열을 가지고 있습니다. 따라서 각 도메인은 Destination Controls(대상 제어) 테이블에 지정된 대로 별도의 동시성 제한 집합을 가지고 습니다. Destination Controls(대상 제어) 테이블에 구체적으로 나열되지 않은 각각의 고유한 도메인은 테이블에 설정된 또 다른 "기본" 제한 집합을 사용합니다.

대상 제어 작업

Destination Control(대상 제어) 항목을 만들고 수정하고 삭제하려면 GUI의 Policies(정책) > Destination Controls(대상 제어) 페이지 또는 CLI의 destconfig 명령을 사용합니다.

관련 주제

- 인터넷 프로토콜 주소의 버전 제어, 705 페이지
- 도메인에 대한 연결, 메시지 및 수신자 수 제어, 705 페이지
- TLS 제어, 707 페이지
- 반송 알림 태깅 제어, 707 페이지
- 반송 제어, 707 페이지
- 새 대상 제어 항목 추가, 707 페이지

• 대상 제어 컨피그레이션 가져오기 및 내보내기, 708 페이지
• 대상 제어 및 CLI, 711 페이지

인터넷 프로토콜 주소의 버전 제어

도메인에 연결하는 데 인터넷 프로토콜 주소의 어떤 버전을 사용할지를 구성할 수 있습니다. Email Security Appliance는 IPv4(Internet Protocol version 4) 및 IPv6(Internet Protocol version 6)을 모두 사용합니다. 이 두 프로토콜 중 하나 또는 둘 모두를 사용하도록 어플라이언스에서 리스너를 구성할 수 있습니다.

Pv4 또는 IPv6에 대해 "Required(필수)" 설정이 지정된 경우 어플라이언스는 지정된 버전의 주소를 사용하여 도메인에 대한 연결을 협상합니다. 도메인이 해당 IP 주소 버전을 사용하지 않는 경우 이메일이 전송되지 않습니다. Pv4 또는 IPv6에 대해 "Preferred(기본 설정)" 설정이 지정된 경우 어플라이언스는 우선 지정된 버전의 주소를 사용하여 도메인에 대한 연결 협상을 시도하고, 첫 번째로 도달할 수 없는 경우 나머지를 사용합니다.

도메인에 대한 연결, 메시지 및 수신자 수 제어

어플라이언스에서 보내는 이메일 때문에 원격 호스트 또는 자체 내부 그룹웨어가 마비되는 상황을 피하려면 어플라이언스가 이메일을 전달하는 방법을 제한할 수 있습니다.

각 도메인에 대해 지정된 시간 동안 시스템에서 초과할 수 없는 최대 연결, 아웃바운드 메시지 및 수신자 수를 할당할 수 있습니다. 이 "good neighbor" 테이블은 Destination Controls(대상 제어) 기능(**Mail Policies(**메일 정책**) > Destination Controls(**대상 제어**)** 또는 `destconfig` 명령 - 이전의 `setgoodtable` 명령)을 통해 정의됩니다. 다음 구문을 사용하여 도메인 이름을 지정할 수 있습니다.

```
domain.com
```

또는

```
.domain.com
```

이 구문을 실행할 경우 AsyncOS는 각 전체 하위 도메인 주소를 개별적으로 입력하지 않은 채 sample.server.domain.com과 같은 하위 도메인에 대한 대상 제어를 지정합니다.

연결, 메시지 및 수신자의 경우 정의하는 제한을 각 가상 게이트웨이 주소에 대해 시행할지 전체 시스템에 대해 시행할지를 설정합니다. (가상 게이트웨이 주소 제한은 IP 인터페이스당 동시 연결 수를 제어합니다. 시스템 전체 제한은 어플라이언스에서 허용할 총 연결 수를 제어합니다.)

또한 정의한 제한을 전체 도메인에 적용할지 여부를 설정할 수 있습니다.

참고 현재 시스템 기본값은 도메인당 연결 500개 및 연결당 메시지 50개입니다.

이러한 값은 다음 표에 설명되어 있습니다.

표 ***59:*** 대상 제어 테이블의 값

필드	설명
동시 연결	어플라이언스가 지정된 호스트에 대해 수행할 최대 아웃바운드 연결 수. (도메인은 내부 그룹웨어 호스트를 포함할 수 있습니다.)
Maximum Messages Per Connection(연결당 최대 메시지 수)	새 연결을 시작하기 전 어플라이언스에서 지정된 호스트로의 단일 아웃바운드 연결에 대해 허용되는 최대 메시지 수.
Recipients(수신자)	지정된 기간 내에 허용되는 최대 수신자 수. "None(없음)"은 지정된 도메인에 대한 수신자 제한이 없음을 나타냅니다. 어플라이언스가 수신자 수를 계산할 1분에서 60분 사이의 최소 기간. "0"을 지정하면 이 기능이 비활성화됩니다. 참고 수신자 제한을 변경하면 AsyncOS는 이미 대기열에 있는 모든 메시지에 대해 카운터를 재설정합니다. 어플라이언스는 새 수신자 제한을 기반으로 메시지를 전달합니다.
Apply Limits(제한 적용)	제한을 전체 도메인에 적용할지 여부를 지정합니다. 이 설정은 연결, 메시지 및 수신자 제한에 적용됩니다. 제한을 시스템 전체에 적용할지 아니면 각 가상 게이트웨이 주소에 적용할지를 지정합니다. 참고 IP 주소의 그룹을 구성했지만 가상 게이트웨이는 구성하지 않은 경우, 각 가상 게이트웨이에 제한을 적용하도록 구성하지 마십시오. 이 설정은 가상 게이트웨이를 사용하도록 구성된 시스템에서만 사용할 수 있습니다. 가상 게이트웨이 구성에 대한 자세한 내용은 호스팅된 모든 도메인에 대한 메일 게이트웨이 구성에 Virtual Gateway™ 기술 사용, 718 페이지 섹션을 참조하십시오.

참고 각 가상 게이트웨이 주소에 제한이 적용되는 경우에도, 원하는 시스템 전체 제한을 가능한 가상 게이트웨이 수로 나누어 가상 게이트웨이 제한을 설정함으로써 시스템 전체 제한을 효과적으로 구현할 수 있습니다. 예를 들어 가상 게이트웨이 주소 4개를 구성했으며 도메인 `yahoo.com`에 대한 동시 연결이 100개를 넘지 않도록 하려는 경우 가상 게이트웨이 제한을 25개 동시 연결로 설정합니다.

`delivernow` 명령은(모든 도메인에 작동할 경우) `destconfig` 명령으로 추적된 모든 카운터를 재설정합니다.

TLS 제어

TLS(Transport Layer Security)를 도메인 단위로 구성할 수도 있습니다. "Required(필수)" 설정이 지정된 경우 TLS 연결은 어플라이언스 리스너에서 도메인에 대한 MTA로 협상됩니다. 협상에 실패하면 연결을 통해 이메일이 전송되지 않습니다. 자세한 내용은 전달 시 TLS 및 인증서 확인 활성화, 654 페이지를 참고하십시오.

TLS 연결을 요구하는 도메인에 메시지를 전달할 때 TLS 협상이 실패하는 경우 어플라이언스에서 알림을 전송할지 여부를 지정할 수 있습니다. 알림 메시지에는 실패한 TLS 협상에 대한 대상 도메인의 이름이 포함됩니다. 어플라이언스는 시스템 알림 유형에서 Warning(경고) 심각도 레벨 알림을 수신하도록 설정된 모든 수신자에게 알림 메시지를 전송합니다. GUI의 System Administration(시스템 관리) > Alerts(알림) 페이지(또는 CLI의 alertconfig 명령)를 통해 알림 수신자를 관리할 수 있습니다.

TLS 연결 알림을 활성화하려면 Destination Controls(대상 제어) 페이지에서 **Edit Global Settings(**전역 설정 수정**)**를 클릭하거나 destconfig -> setup 하위 명령을 사용합니다. 이것은 도메인 단위 설정이 아니라 전역 설정입니다. 어플라이언스가 전달하려고 시도한 메시지에 대해 알아보려면 Monitor(모니터) > Message Tracking(메시지 추적) 페이지 또는 메일 로그를 사용하십시오.

모든 발신 TLS 연결에 사용할 인증서를 지정해야 합니다. 인증서를 지정하려면 Destination Controls(대상 제어) 페이지에서 **Edit Global Settings(**전역 설정 수정**)**를 클릭하거나 destconfig -> setup 하위 명령을 사용합니다. 인증서 가져오기에 대한 자세한 내용은 인증서 작업, 646 페이지 섹션을 참조하십시오.

알림에 대한 자세한 내용은 "시스템 관리" 장을 참조하십시오.

반송 알림 태깅 제어

전송된 메일을 반송 확인을 위해 태깅할지 여부를 지정할 수 있습니다. 기본 대상은 물론 특정 대상에 대해서도 이를 지정할 수 있습니다. Cisco에서는 기본 대상에 대해 반송 확인을 활성화한 다음 특정 예외를 위한 새 대상을 만들 것을 권장합니다. 자세한 내용은 반송 확인, 711 페이지를 참조하십시오.

반송 제어

원격 호스트로 전달할 연결 및 수신자의 수를 제어하는 것 외에도 해당 도메인에 대해 사용될 반송 프로필을 지정할 수 있습니다. 반송 프로필을 지정하면 destconfig 명령의 다섯 번째 열에 나타납니다. 반송 프로필을 지정하지 않으면 기본 반송 프로필이 사용됩니다. 자세한 내용은 새 반송 프로필 만들기, 701 페이지를 참고하십시오.

새 대상 제어 항목 추가

단계 **1** **Add Destination(**대상 추가**)**을 클릭합니다.

단계 **2** 항목을 구성합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

대상 제어 컨피그레이션 가져오기 및 내보내기

여러 도메인을 관리 중인 경우 모든 도메인에 대한 대상 제어 항목을 정의한 다음 어플라이언스로 가져올 수 있습니다. 컨피그레이션 파일의 형식은 Windows INI 컨피그레이션 파일과 유사합니다. 도메인에 대한 매개변수는 섹션 이름으로서의 도메인 이름과 함께 섹션에서 그룹화됩니다. 예를 들면 도메인 example.com에 대한 파라미터를 그룹화하려면 섹션 이름 `[example.com]`을 사용합니다. 정의되지 않은 매개변수는 기본 대상 제어 항목에서 상속됩니다. 컨피그레이션 파일에 `[DEFAULT]` 섹션을 포함하여 기본 대상 제어 항목에 대한 매개변수를 정의할 수 있습니다.

컨피그레이션 파일을 가져오면, 컨피그레이션 파일에 `[DEFAULT]` 섹션이 포함되지 않은 경우 기본 항목을 제외하고, 어플라이언스의 모든 대상 제어 항목을 덮어씁니다. 다른 모든 기존 대상 제어 항목은 삭제됩니다.

컨피그레이션 파일에서 도메인에 대해 다음 매개변수 중 하나를 정의할 수 있습니다. `bounce_profile` 매개변수를 제외한 모든 매개변수가 `[DEFAULT]` 섹션에 필요합니다.

표 ***60:*** 대상 제어 컨피그레이션 파일 매개변수

매개 변수 이름	설명
`ip_sort_pref`	도메인에 대한 인터넷 프로토콜 버전을 지정합니다. 다음 값 중 하나를 입력합니다. • "IPv6 Preferred"에는 `PREFER_V6` • "IPv6 Required"에는 `REQUIRE_v6` • "IPv4 Preferred"에는 `PREFER_V4` • "IPv4 Required"에는 `REQUIRE_v4`
`max_host_concurrency`	어플라이언스가 지정된 호스트에 대해 수행할 최대 아웃바운드 연결 수. 도메인에 대해 이 매개변수를 정의한 경우 `limit_type` 및 `limit_apply` 매개변수도 정의해야 합니다.
`max_messages_per_connection`	새 연결을 시작하기 전 어플라이언스에서 지정된 호스트로의 단일 아웃바운드 연결에 대해 허용되는 최대 메시지 수.
`recipient_minutes`	어플라이언스가 수신자 수를 계산할 1분에서 60분 사이의 기간. 정의하지 않으면 수신자 제한이 적용되지 않습니다.
`recipient_limit`	지정된 기간 내에 허용되는 최대 수신자 수. 정의하지 않으면 수신자 제한이 적용되지 않습니다. 도메인에 대해 이 파라미터를 정의한 경우 `recipient_minutes`, `limit_type` 및 `limit_apply` 파라미터도 정의해야 합니다.

매개 변수 이름	설명
`limit_type`	제한을 전체 도메인에 적용할지 아니면 해당 도메인에 대해 지정된 각 MX IP 주소에 적용할지를 지정합니다. 다음 값 중 하나를 입력합니다. • 도메인에 대해 `0(또는 host)` • MX IP 주소에 대해 `1(또는 MXIP)`
`limit_apply`	제한을 시스템 전체에 적용할지 아니면 각 가상 게이트웨이 주소에 적용할지를 지정합니다. 다음 값 중 하나를 입력합니다. • 시스템 전체에 대해 `0(또는 system)` • 가상 게이트웨이에 대해 `1(또는 VG)`
`bounce_validation`	반송 확인 주소 태깅의 활성화 여부를 지정합니다. 다음 값 중 하나를 입력합니다. • `0(또는 off)` • `1(또는 on)`
`table_tls`	도메인에 대한 TLS 설정을 지정합니다. 자세한 내용은 전달 시 TLS 및 인증서 확인 활성화, 654 페이지를 참조하십시오. 다음 값 중 하나를 입력합니다. • 0(또는 `off`) • "Preferred(기본 설정)"에 대해 1(또는 `on`) • "Required(필수)에 대해 2(또는 `required`) • "Preferred (Verify)(기본 설정(확인))"에 대해 3(또는 `on_verify`) • "Required (Verify)(필수(확인))"에 대해 4(또는 `require_verify`) 문자열은 대/소문자를 구분하지 않습니다.
`bounce_profile`	사용할 반송 프로필의 이름. 이 값은 `[DEFAULT]` 대상 제어 항목에서 사용할 수 없습니다.
`send_tls_req_alert`	필수 TLS 연결이 실패할 경우 알림을 전송할지 여부. 다음 값 중 하나를 입력합니다. • `0(또는 off)` • `1(또는 on)` 이 값은 전역 설정이며 [DEFAULT] 대상 제어 항목에서만 사용할 수 있습니다.

매개 변수 이름	설명
certificate	발신 TLS 연결에 사용되는 인증서. 이 값은 전역 설정이며 [DEFAULT] 대상 제어 항목에서만 사용할 수 있습니다. 참고 인증서를 지정하지 않으면 AsyncOS는 데모 인증서를 할당합니다. 그러나 데모 인증서 사용은 안전하지 않으며 일반적인 용도로서 권장되지 않습니다.

다음 예는 기본 대상 제어 항목과 함께 도메인 example1.com 및 example2.com에 대한 컨피그레이션 파일을 보여줍니다.

```
[DEFAULT]

ip_sort_pref = PREFER_V6

max_host_concurrency = 500

max_messages_per_connection = 50

recipient_minutes = 60

recipient_limit = 300

limit_type = host

limit_apply = VG

table_tls = off

bounce_validation = 0

send_tls_req_alert = 0

certificate = example.com

[example1.com]

ip_sort_pref = PREFER_V6

recipient_minutes = 60

recipient_limit = 100

table_tls = require_verify

limit_apply = VG

bounce_profile = tls_failed

limit_type = host

[example2.com]

table_tls = on

bounce_profile = tls_failed
```

위 예의 결과로 example1.com and example2.com에 대한 다음 대상 제어 항목이 표시됩니다.

```
example1.com

IP Address Preference: IPv6 Preferred

Maximum messages per connection: 50

Rate Limiting:

500 concurrent connections

100 recipients per 60 minutes

Limits applied to entire domain, across all virtual gateways

TLS: Required (Verify)

Bounce Profile: tls_failed

example2.com

IP Address Preference: IPv6 Preferred

Maximum messages per connection: Default

Rate Limiting: Default

TLS: Preferred

Bounce Profile: tls_failed
```

구성 파일을 가져오려면 Destination Controls(대상 제어) 페이지의 **Import Table(**테이블 가져오기**)** 버튼 또는 `destconfig -> import` 명령을 사용합니다. Destination Controls(대상 제어) 페이지의 **Export Table(**테이블 내보내기**)** 버튼 또는 `destconfig -> export` 명령을 사용하여 대상 제어 항목을 INI 파일로 내보낼 수도 있습니다. AsyncOS는 내보낸 INI 파일에 `[Default]` 도메인 제어 항목을 포함합니다.

대상 제어 및 **CLI**

CLI의 destconfig 명령을 사용하여 대상 제어 항목을 구성할 수 있습니다. 이러한 명령은 AsyncOS for Cisco Email Security Appliances CLI 참조 가이드에 설명되어 있습니다.

반송 확인

"반송" 메시지는 원본 이메일의 Envelope Sender(봉투 발신자)를 새 Envelope Recipient(봉투 수신자)로 사용하여 수신 MTA에 의해 전송되는 새 메시지입니다. 원본 메시지를 전달할 수 없는 경우(대개 존재하지 않는 수신자 주소 때문) 이러한 반송이 빈 봉투 발신자(MAIL FROM: <>)와 함께 봉투 수신자(일반적으로)에게 다시 전송됩니다.

잘못 전달된 반송 공격을 통해 이메일 인프라를 공격하는 스패머가 늘고 있습니다. 이러한 공격은 합법적인 메일 서버가 알지 못하고 전송하는 수많은 반송 메시지로 구성됩니다. 기본적으로 스패머가 사용하는 프로세스는 오픈 릴레이 및 "좀비" 네트워크를 통해 다양한 도메인의 잠재적으로 유효하지

않은 여러 주소(봉투 수신자)로 이메일을 전송하는 것입니다. 스팸이 합법적인 도메인에서 오는 것처럼 보이도록 이러한 메시지에서는 봉투 발신자가 위조됩니다(이를 "Joe Job"이라고 함).

이제 잘못된 봉투 수신자의 각 수신 이메일에 대해, 수신 메일 서버는 새 이메일(반송 메시지)을 생성한 다음 이를 아무것도 모르는 도메인의 봉투 발신자(봉투 발신자 주소가 위조된)에게 전송합니다. 그 결과 이 대상 도메인은 수많은 "잘못 전달된" 반송(잠재적으로 수백만 개의 메시지)을 수신합니다. 이 유형의 분산형 메시지 거부 공격은 이메일 인프라를 다운시키고 공격 대상이 합법적인 이메일을 주고받지 못하게 할 수 있습니다.

이런 잘못 전달된 반송 공격에 대응하기 위해 AsyncOS는 반송 확인을 포함합니다. 이 기능을 활성화하면, 반송 확인은 어플라이언스를 통해 전송되는 메시지에 봉투 발신자 주소를 태깅합니다. 그러면 어플라이언스가 수신한 반송 메시지에 대한 봉투 수신자는 이 태그의 존재 여부를 확인합니다. 합법적인 반송(이 태그를 포함해야 함)은 태그가 제거되고 전달됩니다. 태그가 포함되지 않은 반송 메시지는 별도로 처리할 수 있습니다.

반송 확인을 사용하면 발신 메일을 기반으로 수신 반송 메시지를 관리할 수 있습니다. 어플라이언스가 수신 메일을 기반으로 발신 반송을 생성하는 방법을 제어하려면 반송된 이메일 전달, 694 페이지 섹션을 참조하십시오.

관련 주제

- 개요: 태깅 및 반송 확인, 712 페이지
- 반송 확인을 사용하여 반송 메시지 폭풍 방지, 714 페이지
- 태그 없는 합법적인 반송 메시지 수락, 713 페이지

개요: 태깅 및 반송 확인

반송 확인을 활성화하고 이메일을 전송하면 어플라이언스는 메시지에 봉투 발신자 주소를 재작성합니다. 예를 들어 MAIL FROM: joe@example.com은 MAIL FROM: prvs=joe=123ABCDEFG@example.com이 됩니다. 이 예에서 123... 문자열은 어플라이언스에서 전송할 때 봉투 발신자에 추가되는 "반송 확인 태그"입니다. 태그는 Bounce Verification(반송 확인) 설정에 정의된 키를 사용하여 생성됩니다(키 지정에 대한 자세한 내용은 바운스 확인 Address Tagging 키, 713 페이지 참고). 이 메시지가 반송되는 경우, 반송 메시지의 봉투 수신자 주소에 이 반송 확인 태그가 포함됩니다.

반송 확인 태깅을 기본적으로 시스템 전체에서 활성화 또는 비활성화할 수 있습니다. 또한 특정 도메인에 대한 반송 확인 태그도 활성화 또는 비활성화할 수 있습니다. 대부분의 경우 기본적으로 이 기능을 활성화한 다음, Destination Controls(대상 제어) 테이블에서 제외할 특정 도메인을 나열할 수 있습니다(대상 제어 작업, 704 페이지 참조).

메시지에 이미 태깅된 주소가 포함되어 있으면 AsyncOS는 또 다른 태그를 추가하지 않습니다(어플라이언스가 DMZ 내 어플라이언스로 반송 메시지를 전달하는 경우).

관련 주제

- 수신 반송 메시지 처리, 713 페이지
- 바운스 확인 Address Tagging 키, 713 페이지

수신 반송 메시지 처리

유효한 태그가 포함된 반송 메시지는 전달됩니다. 태그가 제거되고 봉투 수신자가 복원됩니다. 이는 이메일 파이프라인에서 도메인 맵 단계 직후 발생합니다. 어플라이언스에서 태그가 없거나 유효하지 않은 반송을 처리하는 방법(거부 또는 사용자 지정 헤더 추가)을 정의할 수 있습니다. 자세한 내용은 반송 확인 설정 구성, 715 페이지를 참조하십시오.

반송 확인 태그가 없거나, 태그 생성에 사용된 키가 변경되었거나, 메시지가 7일보다 더 오래된 경우 해당 메시지는 반송 확인에 대해 정의된 설정에 따라 처리됩니다.

예를 들어 다음 메일 로그는 어플라이언스에 의해 거부된 반송 메시지를 보여줍니다.

```
Fri Jul 21 16:02:19 2006 Info: Start MID 26603 ICID 125192

Fri Jul 21 16:02:19 2006 Info: MID 26603 ICID 125192 From: <>

Fri Jul 21 16:02:40 2006 Info: MID 26603 ICID 125192 invalid bounce, rcpt address
<bob@example.com> rejected by bounce verification.
Fri Jul 21 16:03:51 2006 Info: Message aborted MID 26603 Receiving aborted by sender

Fri Jul 21 16:03:51 2006 Info: Message finished MID 26603 aborted
```

참고 비반송 메일을 내부 메일 서버(예: Exchange)로 전달할 때에는 해당 내부 도메인에 대해 반송 확인 태깅을 비활성화해야 합니다.

AsyncOS는 반송 메시지를 null Mail From 주소(<>)의 메일로 간주합니다. 태깅된 봉투 수신자가 포함되어 있을 수 있는 비반송 메시지에 대해 AsyncOS는 좀 더 관대한 정책을 적용합니다. 그러한 경우 AsyncOS는 7일 키 만료를 무시하고 더 오래된 키에서도 일치를 찾아보려고 시도합니다.

바운스 확인 **Address Tagging** 키

태깅 키는 반송 확인 태그 생성 시 어플라이언스가 사용하는 텍스트 문자열입니다. 도메인을 떠나는 모든 메일이 일관성 있게 태깅되도록 모든 어플라이언스에서 동일한 키를 사용하는 것이 가장 이상적입니다. 그렇게 하면 한 어플라이언스가 발신 메시지에 대해 봉투 발신자를 태깅할 경우, 반송을 다른 어플라이언스에서 수신하더라도 수신 반송이 확인되고 전달됩니다.

태그 유예 기간은 7일입니다. 예를 들면 7일 기간 내에 태깅 키를 여러 번 변경하도록 선택할 수 있습니다. 그런 경우 어플라이언스는 7일이 안 된 모든 이전 키를 사용하여 태깅된 메시지를 확인하려고 시도합니다.

태그 없는 합법적인 반송 메시지 수락

태그 없는 반송이 유효한 경우를 고려하여 AsyncOS는 또한 반송 확인과 관련된 HAT 설정도 포함합니다. 기본 설정은 "No(아니요)"입니다. 즉, 태그 없는 반송은 유효하지 않은 것으로 간주되며, **Mail Policies(메일 정책) > Bounce Verification(반송 확인)** 페이지에서 선택한 작업에 따라 어플라이언스는 메시지를 거부하거나 맞춤형 헤더를 적용합니다. "Yes(예)"를 선택하면 어플라이언스는 태그 없는 반송을 유효한 것으로 간주하여 수락합니다. 이는 다음 시나리오에서 사용될 수 있습니다.

메일 목록으로 이메일을 전송하려는 사용자가 있다고 가정해보겠습니다. 그러나 메일 목록은 봉투 발신자의 고정 집합에서 오는 메시지만 수락합니다. 그러한 경우 사용자의 태깅된 메시지는 수락되지 않습니다(태그가 정기적으로 변경되므로).

단계 **1** 사용자가 대상 제어 테이블로 메일을 전송하려고 하는 도메인을 추가하고 해당 도메인에 대해 태깅을 비활성화합니다. 이 시점에서는 사용자가 문제없이 메일을 전송할 수 있습니다.

단계 **2** 그러나 해당 도메인에서 오는 반송의 수신을 적절히 지원하기 위해(태깅되지 않았으므로), 해당 도메인에 대한 발신자 그룹을 만들고 "Accept(수락)" 메일 플로우 정책에서 Consider Untagged Bounces to be Valid(태그 없는 반송을 유효한 것으로 간주) 매개변수를 활성화합니다.

반송 확인을 사용하여 반송 메시지 폭풍 방지

단계 **1** 태깅 키를 입력합니다. 자세한 내용은 반송 확인 주소 태깅 키 구성, 714 페이지를 참고하십시오.

단계 **2** 반송 확인 설정을 수정합니다. 자세한 내용은 반송 확인 설정 구성, 715 페이지를 참고하십시오.

단계 **3** 대상 제어를 통해 반송 확인을 활성화합니다. 자세한 내용은 대상 제어 작업, 704 페이지를 참고하십시오.

다음에 수행할 작업

관련 주제

- 반송 확인 주소 태깅 키 구성, 714 페이지
- 반송 확인 설정 구성, 715 페이지
- CLI를 사용하여 반송 확인 구성, 715 페이지
- 반송 확인 및 클러스터 컨피그레이션, 715 페이지

반송 확인 주소 태깅 키 구성

반송 확인 주소 태깅 키 목록은 현재 키 및 과거에 사용한 삭제되지 않은 키를 보여줍니다. 새 키를 추가하려면 다음의 절차를 따릅니다.

단계 **1** **Mail Policies(**메일 정책**) > Bounce Verification(**반송 확인**)** 페이지에서 **New Key(**새 키**)**를 클릭합니다.

단계 **2** 텍스트 문자열을 입력하고 **Submit(**제출**)**을 클릭합니다.

단계 **3** 변경 사항을 **Commit(**커밋**)**합니다.

다음에 수행할 작업

관련 주제

- 키 삭제, 715 페이지

키 삭제

풀다운 메뉴에서 삭제할 규칙을 선택하고 **Purge(**삭제**)**를 클릭하여 오래된 주소 태깅 키를 삭제할 수 있습니다.

반송 확인 설정 구성

반송 확인 설정은 잘못된 반송을 수신할 때 수행할 작업을 결정합니다.

단계 **1** **Mail Policies(**메일 정책**) > Bounce Verification(**반송 확인**)**을 선택합니다.

단계 **2** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** 잘못된 반송을 거부할지, 아니면 사용자 지정 헤더를 메시지에 추가할지를 선택합니다. 헤더를 추가하려면 헤더 이름과 값을 입력합니다.

단계 **4** 선택적으로, 스마트 예외를 활성화합니다. 이 설정을 선택하면 수신 메일 메시지와 내부 메일 서버에 의해 생성된 반송 메시지를 반송 확인 처리에서 자동으로 제외할 수 있습니다(수신 및 발신 메일 모두에 단일 리스너를 사용하는 경우에도).

단계 **5** 변경 사항을 제출 및 커밋합니다.

CLI를 사용하여 반송 확인 구성

CLI의 bvconfig 명령 destconfig 명령을 사용하여 반송 확인을 구성할 수 있습니다. 이러한 명령은 *AsyncOS for Cisco Email Security Appliances CLI* 참조 가이드에 설명되어 있습니다.

반송 확인 및 클러스터 컨피그레이션

두 어플라이언스가 동일한 "반송 키"를 사용하는 한 반송 확인은 클러스터 컨피그레이션에서 작동합니다. 동일한 키를 사용하면 두 시스템 중 하나는 합법적인 반송을 다시 수락할 수 있습니다. 수정된 헤더 태그/키는 각 어플라이언스에 해당되지 않습니다.

이메일 전달 매개변수 설정

deliveryconfig 명령은 어플라이언스에서 오는 이메일을 전달할 때 사용할 매개변수를 설정합니다.

어플라이언스는 다중 메일 프로토콜(SMTP 및 QMQP)을 사용하여 이메일을 수락합니다. 그러나 모든 발송 이메일은 SMTP를 사용하여 전송됩니다. 따라서 deliveryconfig 명령에서 프로토콜을 지정할 필요가 없습니다.

참고 이 섹션에서 설명하는 몇 가지 기능 또는 명령은 라우팅 우선 순위에 영향을 미치거나 영향을 받습니다. 자세한 내용은 "네트워크 및 IP 주소 할당" 부록을 참조하십시오.

관련 주제

- 기본 전달 IP 인터페이스, 716 페이지
- Possible Delivery(가능한 전달) 기능, 716 페이지
- 기본 최대 동시성, 716 페이지
- deliveryconfig 예, 717 페이지

기본 전달 IP 인터페이스

기본적으로 시스템은 이메일 전달에 IP 인터페이스 또는 IP 인터페이스 그룹을 사용합니다. 현재 구성된 IP 인터페이스 또는 IP 인터페이스 그룹을 설정할 수 있습니다. 특정 인터페이스가 식별되지 않으면 AsyncOS는 수신자 호스트와 통신할 때 SMTP HELO 명령의 기본 전달 인터페이스와 연결된 호스트 이름을 사용합니다. IP 인터페이스를 구성하려면 interfaceconfig 명령을 사용합니다.

다음은 이메일 전달 인터페이스에서 Auto(자동)를 선택할 경우 사용되는 규칙입니다.

- 원격 이메일 서버가 구성된 인터페이스 중 하나와 동일한 서브넷에 있으면 트래픽은 일치하는 인터페이스에서 이동합니다.
- auto-select로 설정된 경우 routeconfig를 사용하여 구성한 고정 경로가 적용됩니다.
- 그렇지 않으면 기본 게이트웨이와 동일한 서브넷에 있는 인터페이스가 사용됩니다. 모든 IP 주소가 대상으로 가는 동일한 경로를 가지고 있으면 시스템은 사용 가능한 가장 효율적인 인터페이스를 사용합니다.

Possible Delivery(가능한 전달) 기능

주의 이 기능을 활성화하면 메시지 전달이 안정적이지 않으며 메시지 손실이 발생할 수 있습니다. 또한 어플라이언스는 RFC 5321을 준수하지 않게 됩니다. 자세한 내용은 http://tools.ietf.org/html/rfc5321#section-6.1.의 내용을 참고하십시오.

Possible Delivery(가능한 전달) 기능이 활성화되면 AsyncOS는 메시지 본문이 전달된 후, 그러나 수신자 호스트가 메시지 수신을 인식하기 전 시간 초과되는 메시지를 "possible delivery(가능한 전달)"로 취급합니다. 이 기능은 수신자 호스트에서 발생하는 연속 오류 때문에 수신을 인식할 수 없을 때 수신자가 메시지의 여러 복사본을 수신하지 않도록 해줍니다. AsyncOS는 이 수신자를 메일 로그에 가능한 전달로 기록하고 메시지를 완료됨 상태로 계산합니다.

기본 최대 동시성

어플라이언스가 아웃바운드 메시지 전달을 위해 만들 수 있는 기본 최대 동시 연결 수를 지정합니다. (시스템 전체 연결 기본값은 별도의 도메인에 대해 10,000개입니다.) 리스너당 최대 아웃바운드 메시지 전달 동시성과 함께 제한이 모니터링됩니다(리스너당 연결 기본값은 프라이빗 리스너 600개, 퍼블릭 리스너 1,000개입니다). 값을 기본값보다 낮게 설정하면 게이트웨이가 더 약한 네트워크를 제어할 수 없습니다. 예를 들어 특정 방화벽은 다수의 연결을 지원하지 않으며, 이러한 환경에서는 DoS(Denial of Service) 경고가 발생할 수 있습니다.

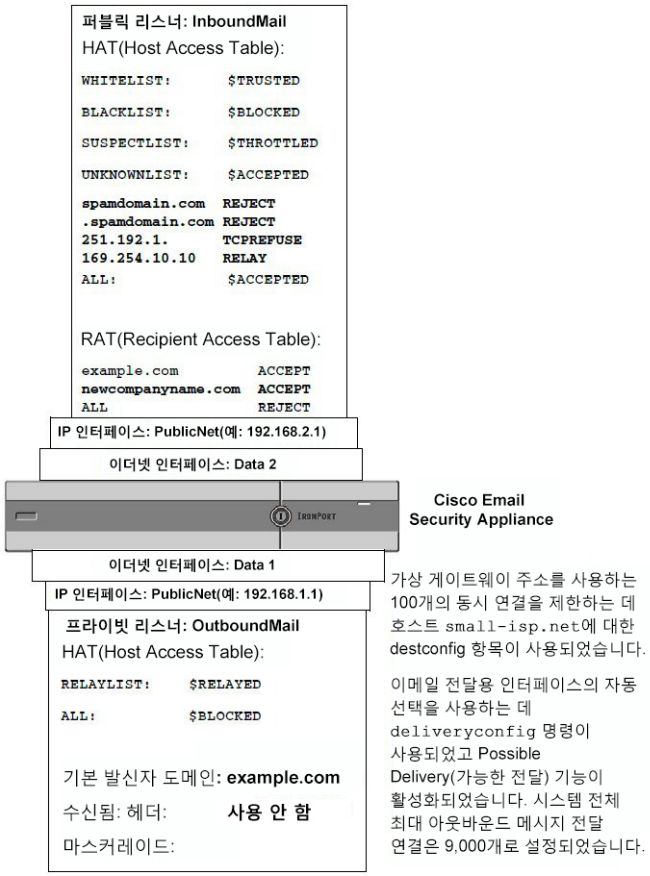
deliveryconfig 예

다음 예에서는 deliveryconfig 명령을 사용하여 기본 인터페이스를 "Possible Delivery(가능한 전달)"가 활성화된 "Auto(자동)"로 설정합니다. 시스템 전체 최대 아웃바운드 메시지 전달 연결은 9,000개로 설정됩니다.

```
mail3.example.com> deliveryconfig

Choose the operation you want to perform:

- SETUP - Configure mail delivery.

[]> setup

Choose the default interface to deliver mail.

1. Auto

2. PublicNet2 (192.168.3.1/24: mail4.example.com)

3. Management (192.168.42.42/24: mail3.example.com)

4. PrivateNet (192.168.1.1/24: mail3.example.com)

5. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Enable "Possible Delivery" (recommended)? [Y]> y

Please enter the default system wide maximum outbound message delivery

concurrency

[10000]> 9000

mail3.example.com>
```

이제 이메일 게이트웨이 컨피그레이션은 다음과 같습니다.

그림 ***52:*** 대상 및 전달 매개변수 설정



호스팅된 모든 도메인에 대한 메일 게이트웨이 구성에 **Virtual Gateway™** 기술 사용

이 섹션에서는 Cisco Virtual Gateway™ 기술과 그 이점, 가상 게이트웨이 주소 설정 방법, 그리고 가상 게이트웨이 주소의 모니터링 및 관리 방법에 대해 설명합니다.

Cisco 가상 게이트웨이 기술을 사용하면 호스팅하는 모든 도메인에 대해 엔터프라이즈 메일 게이트웨이를 구성하고(고유한 IP 주소, 호스트 이름 및 도메인으로), 이러한 도메인에 대한 별도의 기업 이메일 정책 시행 및 안티스팸 전략을 만들 수 있습니다(동일한 물리적 어플라이언스 내에 호스팅). 모든 Email Security Appliance 모델에서 사용할 수 있는 가상 게이트웨이 주소의 수는 255개입니다.

관련 주제

- 개요, 719 페이지
- 가상 게이트웨이 주소 설정, 719 페이지
- 가상 게이트웨이 주소 모니터링, 726 페이지
- 가상 게이트웨이 주소 단위로 전달 연결 관리, 726 페이지

개요

Cisco에서는 기업이 이메일을 통해 고객과 안심하고 통신할 수 있도록 지원하는 고유한 가상 게이트웨이 기술을 개발했습니다. 가상 게이트웨이 기술을 통해 사용자는 하나의 어플라이언스를 이메일을 보내고 받을 수 있는 여러 가상 게이트웨이 주소로 분리할 수 있습니다. 각 가상 게이트웨이 주소에는 고유한 IP 주소, 호스트 이름과 도메인 및 이메일 대기열이 제공됩니다.

각 가상 게이트웨이 주소에 고유한 IP 주소 및 호스트 이름을 할당하면, 수신자 호스트에서 게이트웨이를 통해 전달되는 이메일의 올바른 식별이 보장되며 중요한 이메일이 스팸으로 차단되는 것을 막을 수 있습니다. 어플라이언스는 각각의 가상 게이트웨이 주소에 대한 SMTP HELO 명령에 올바른 호스트 이름을 제공할 수 있는 인텔리전스를 가지고 있습니다. 따라서 수신 ISP(Internet Service Provider)가 역방향 DNS 조회를 수행하는 경우, 어플라이언스는 가상 게이트웨이 주소를 통해 전송되는 이메일의 IP 주소를 확인합니다. 많은 ISP에서 원치 않는 이메일 탐지에 역방향 DNS 조회를 사용하므로 이 기능은 매우 중요합니다. 역방향 DNS의 IP 주소가 전송 호스트의 IP 주소와 일치하지 않으면, ISP는 발신자를 불법 사용자로 간주하고 이메일을 빈번하게 삭제하게 됩니다. Cisco 가상 게이트웨이 기술은 역방향 DNS 조회가 항상 전송 IP 주소와 일치하도록 보장함으로써, 메시지가 예기치 않게 차단되는 것을 방지합니다.

각 가상 게이트웨이 주소의 메시지는 별도의 메시지 대기열에 할당됩니다. 특정 수신자 호스트가 한 가상 게이트웨이 주소의 이메일을 차단하면 해당 호스트로 가야 하는 메시지는 대기열에 남아 있게 되며 결국 시간 초과됩니다. 그러나 동일한 도메인으로 가야 하지만 다른 가상 게이트웨이 대기열(차단되지 않은)에 있는 메시지는 정상적으로 전달됩니다. 이러한 대기열은 전달을 위해 별도로 취급되지만 시스템 관리, 로깅 및 보고 기능은 여전히 모든 가상 게이트웨이 대기열에 대한 전체적인 보기를 마치 하나인 것처럼 제공합니다.

가상 게이트웨이 주소 설정

Cisco 가상 게이트웨이 주소를 설정하기 전에 이메일 전송에 사용할 IP 주소 집합을 할당해야 합니다. (자세한 내용은 "네트워크 및 IP 주소 할당" 부록을 참조하십시오.) 또한 IP 주소가 유효한 호스트 이름으로 확인되도록 DNS 서버를 적절히 구성해야 합니다. DNS 서버를 적절히 구성하면 수신자 호스트가 역방향 DNS 조회를 수행할 때 유효한 IP/호스트 이름 쌍으로 확인됩니다.

관련 주제

- 가상 게이트웨이와 함께 사용할 새 IP 인터페이스 만들기, 719 페이지
- 메시지를 전달용 IP 인터페이스에 매핑, 722 페이지
- altsrchost 파일 가져오기, 723 페이지
- altsrchost 제한, 723 페이지
- altsrchost 명령에 대한 유효한 매핑이 있는 텍스트 파일 예, 723 페이지
- CLI를 통해 altsrchost 매핑 추가, 724 페이지

가상 게이트웨이와 함께 사용할 새 IP 인터페이스 만들기

IP 주소와 호스트 이름을 설정한 후 가상 게이트웨이 주소를 구성하는 첫 번째 단계는 GUI의 Network(네트워크) > IP Interfaces(IP 인터페이스) 페이지 또는 CLI의 interfaceconfig 명령을 사용하여 IP/호스트 이름 쌍의 새 IP 인터페이스를 만드는 것입니다.

IP 인터페이스를 구성했으면 여러 IP 인터페이스를 인터페이스 그룹으로 결합할 수 있습니다. 그런 다음 이러한 그룹에 시스템이 이메일을 전달할 때 "라운드로빈" 방식으로 순환할 특정 가상 게이트웨이 주소를 할당할 수 있습니다.

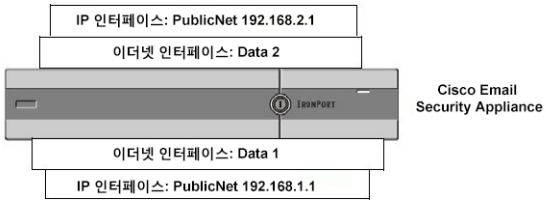
필요한 IP 인터페이스를 만든 후에는 가상 게이트웨이 주소를 설정하고 각 IP 인터페이스 또는 인터페이스 그룹에서 전송할 이메일 캠페인을 정의하기 위한 두 가지 옵션이 제공됩니다.

- altsrchost 명령을 사용하면 특정 발신자 IP 주소 또는 봉투 발신자 주소 정보에서 전달을 위한 호스트 IP 인터페이스(가상 게이트웨이 주소) 또는 인터페이스 그룹으로 이메일을 매핑할 수 있습니다.
- 메시지 필터를 사용하면, 특정 호스트 IP 인터페이스(가상 게이트웨이 주소) 또는 인터페이스 그룹을 사용하여 플래그 지정 메시지를 전달하도록 특정 필터를 설정할 수 있습니다. 소스 호스트(가상 게이트웨이 주소) 변경 작업, 218 페이지를 참조하십시오. (이 방법이 위 방법보다 더 유연하고 강력합니다.)

IP 인터페이스 만들기에 대한 자세한 내용은 "어플라이언스에 액세스" 부록을 참조하십시오.

지금까지 다음 그림에 나와 있는 대로, 다음과 같은 정의된 인터페이스와 함께 이메일 게이트웨이 구성을 사용했습니다.

그림 ***53:*** 퍼블릭 및 프라이빗 인터페이스 예



다음 예에서 IP Interfaces(IP 인터페이스) 페이지는 Management 인터페이스 외에 두 인터페이스(PrivateNet 및 PublicNet)가 구성되었음을 보여줍니다.

그림 ***54: IP Interfaces(IP*** 인터페이스***)*** 페이지

IP Interfaces

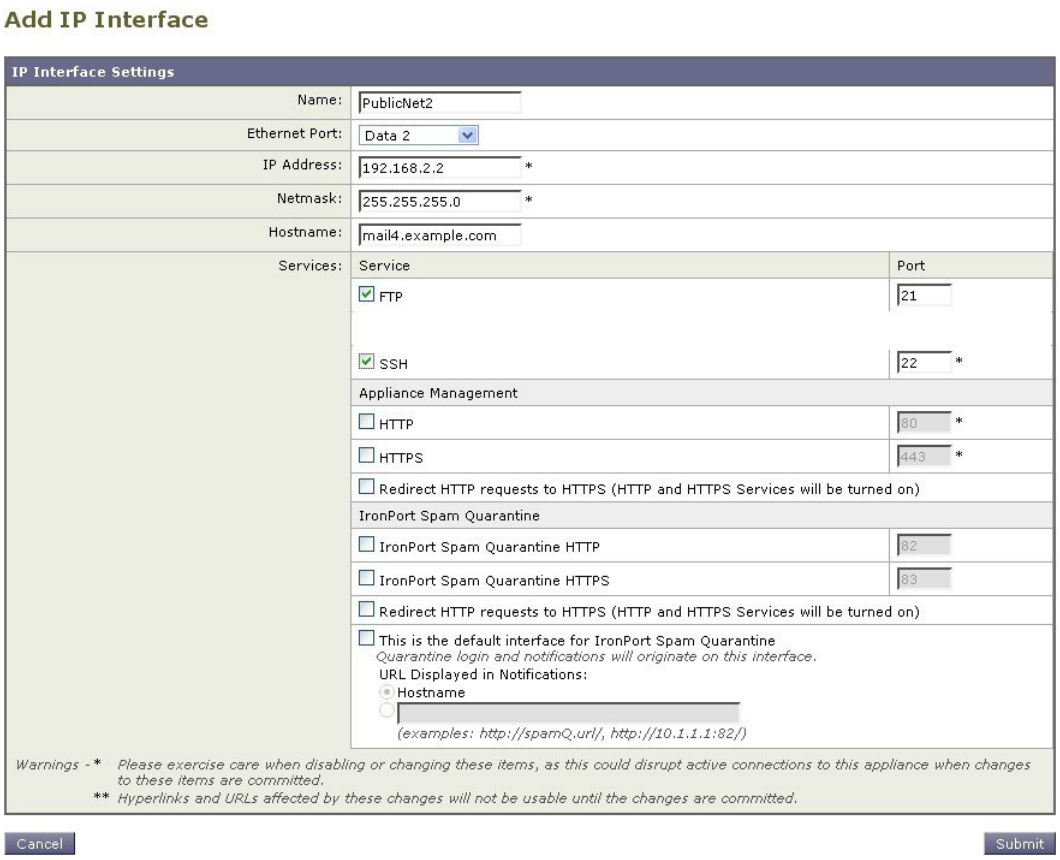
Network Interfaces and IP Addresses

Add IP Interface...

Name	IP Address	Hostname	Delete
Management	192.168.42.42/24	mail3.example.com	
PrivateNet	192.168.1.1/24	mail3.example.com	
PublicNet	192.168.2.1/24	mail3.example.com	

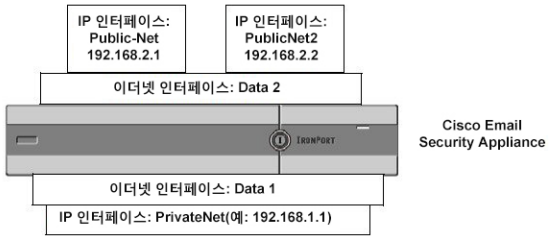
이제 Data2 이더넷 인터페이스에 PublicNet2라는 새 인터페이스를 만드는 데 Add IP Interface(IP 인터페이스 추가) 페이지가 사용됩니다. IP 주소 192.168.2.2가 사용되고 호스트 이름 mail4.example.com이 지정됩니다. 그런 다음 FTP(포트 21) 및 SSH(포트 22)에 대한 서비스가 활성화됩니다.

그림 ***55: Add IP Interface(IP*** 인터페이스 추가**)** 페이지



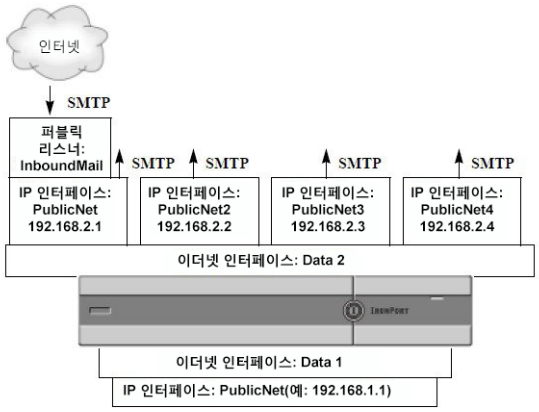
이제 이메일 게이트웨이 컨피그레이션은 다음과 같습니다.

그림 ***56:*** 또 다른 퍼블릭 인터페이스 추가



가상 게이트웨이 주소를 사용하면 다음 그림에 보이는 것과 같은 구성도 가능합니다.

그림 ***57:*** 하나의 이더넷 인터페이스에 네 개의 가상 게이트웨이 주소



메일을 전달하는 데 네 개의 서로 다른 IP 인터페이스를 사용할 수 있으며, 여기에서 하나의 퍼블릭 리스너만 인터넷에서 오는 메시지를 수락하도록 구성됩니다.

메시지를 전달용 IP 인터페이스에 매핑

`altsrchost` 명령은 각 어플라이언스를 메일 전달이 가능한 여러 IP 인터페이스(가상 게이트웨이 주소)로 분할하기 위한 가장 간단명료한 방법을 제공합니다. 그러나 메시지를 특정 가상 게이트웨이에 매핑하는 좀 더 강력하고 유연한 방법이 필요한 사용자는 메시지 필터 사용을 고려해야 합니다. 자세한 내용은 메시지 필터를 사용하여 이메일 정책 적용, 137 페이지를 참조하십시오.

`altsrchost` 명령을 사용하면 다음 중 하나를 기반으로 이메일 전달 중에 어떤 IP 인터페이스 또는 인터페이스 그룹을 사용할지를 제어할 수 있습니다.

- 발신자의 IP 주소
- 봉투 발신자 주소

시스템이 어떤 IP 인터페이스 또는 인터페이스 그룹에서 이메일을 전달할지를 지정하려면, 발신자의 IP 주소 또는 봉투 발신자 주소를 IP 인터페이스 또는 인터페이스 그룹에 페어링하는(인터페이스 이름 또는 그룹 이름으로 지정) 매핑 키를 만들어야 합니다.

AsyncOS는 IP 주소와 봉투 발신자 주소를 모두 매핑 키와 비교합니다. IP 주소 또는 봉투 발신자 주소가 키 중 하나와 일치하면 아웃바운드 전달에 해당 IP 인터페이스가 사용됩니다. 일치하는 키가 없으면 기본 아웃바운드 인터페이스가 사용됩니다.

시스템은 다음 키 중 하나를 확인하며 다음 순서로 우선 순위를 정합니다.

발신자의 **IP** 주소	발신자의 IP 주소는 정확히 일치해야 합니다. 예: `192.168.1.5`
완전한 형식의 봉투 발신자	봉투 발신자는 전체 주소가 정확히 일치해야 합니다. 예: `username@example.com`
사용자 이름	시스템은 사용자 이름 구문을 봉투 발신자 주소에 대해 최대 `@` 기호까지 확인합니다. `@` 기호를 반드시 포함해야 합니다. 예: `username@`

도메인	시스템은 도메인 이름 구문을 봉투 발신자 주소에 대해 최대 @ 기호부터 확인합니다. @ 기호를 반드시 포함해야 합니다. 예: @example.com

참고 리스너는 altsrchost 테이블의 정보를 확인하고, 가장 정보를 확인한 후 그리고 메시지 필터가 점검되기 전에 이메일을 특정 인터페이스로 전달합니다.

CLI를 통해 가상 게이트웨이에서 매핑을 만들려면 altsrchost 명령의 다음 하위 명령을 사용합니다.

Syntax	설명
new	수동으로 새 매핑을 만듭니다.
print	현재 매핑 목록을 표시합니다.
delete	테이블에서 매핑 중 하나를 제거합니다.

altsrchost 파일 가져오기

HAT, RAT, smtproutes, 가장 및 별칭 테이블과 마찬가지로 파일을 내보내고 가져와서 altsrchost 항목을 수정할 수 있습니다.

단계 **1** altsrchost 명령의 export 하위 명령을 사용하여 기존 항목을 파일(이름은 사용자가 지정)로 내보냅니다.

단계 **2** CLI 외부에서 파일을 가져옵니다. (자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지를 참조하십시오.)

단계 **3** 텍스트 편집기를 이용해 파일에서 새 항목을 만듭니다. 규칙이 altsrchost 테이블에 나타나는 순서는 중요합니다.

단계 **4** 파일을 저장한 다음, 가져올 수 있도록 인터페이스의 "altsrchost" 디렉터리에 둡니다. (자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지 항목을 참고하십시오.)

단계 **5** altsrchost의 import 하위 명령을 사용하여 편집된 파일을 가져옵니다.

altsrchost 제한

최대 1,000개의 altsrchost 항목을 정의할 수 있습니다.

altsrchost 명령에 대한 유효한 매핑이 있는 텍스트 파일 예

```
# Comments to describe the file

@example.com DemoInterface

paul@ PublicInterface

joe@ PublicInterface

192.168.1.5, DemoInterface
```

```
steve@example.com PublicNet
```

import 및 export 하위 명령은 한 줄씩 작동하며 발신자 IP 주소 또는 봉투 발신자 주소 줄을 인터페이스 이름에 매핑합니다. 키는 공백 아닌 문자의 첫 번째 블록에 있어야 하며, 그 뒤 공백 아닌 문자의 두 번째 블록에 인터페이스 이름이 쉼표(,) 또는 공백( )으로 구분되어 표시되어야 합니다. 코멘트 줄은 숫자 기호(#)로 시작되며 무시됩니다.

CLI를 통해 altsrchost 매핑 추가

다음 예는 altsrchost 테이블 출력에서 기존 매핑이 없음을 보여줍니다. 두 항목이 생성됩니다.

- @exchange.example.com이라는 그룹웨어 서버 호스트의 메일이 PublicNet 인터페이스에 매핑됩니다.
- 발신자 IP 주소 192.168.35.35에서 오는 메일(예: 마케팅 캠페인 메시징 시스템)이 PublicNe2t 인터페이스에 매핑됩니다.

마지막으로 altsrchost 매핑이 확인을 위해 출력되고 변경 사항이 커밋됩니다.

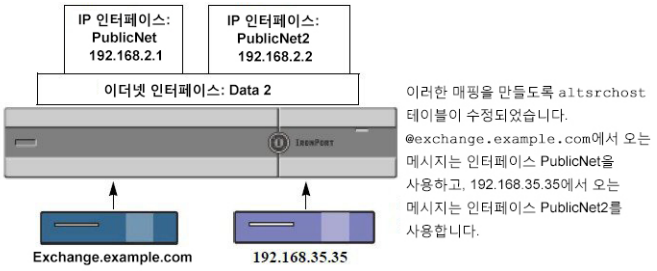
```
mail3.example.com> altsrchost

There are currently no mappings configured.

Choose the operation you want to perform:

- NEW - Create a new mapping.

- IMPORT - Load new mappings from a file.

[]> new

Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping. Partial addresses such as "@example.com" or "user@" are
allowed.

[]> @exchange.example.com

Which interface do you want to send messages for @exchange.example.com from?

1. PublicNet2 (192.168.2.2/24: mail4.example.com)

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail4.example.com)

[1]> 4

Mapping for @exchange.example.com on interface PublicNet created.

Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.
```

```
- EXPORT - Export all mappings to a file.

- PRINT - Display all mappings.

- CLEAR - Remove all mappings.


[]> new


Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping. Partial addresses such as "@example.com" or "user@" are
allowed.


[]> 192.168.35.35

Which interface do you want to send messages for 192.168.35.35 from?

1. PublicNet2 (192.168.2.2/24: mail4.example.com)

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail4.example.com)

[1]> 1


Mapping for 192.168.35.35 on interface PublicNet2 created.

Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.

- EXPORT - Export all mappings to a file.

- PRINT - Display all mappings.

- CLEAR - Remove all mappings.

[]> print

1. 192.168.35.35 -> PublicNet2

2. @exchange.example.com -> PublicNet

Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.
```

```
- EXPORT - Export all mappings to a file.

- PRINT - Display all mappings.

- CLEAR - Remove all mappings.

[]>

mail3.example.com> commit

Please enter some comments describing your changes:


[]> Added 2 altsrchost mappings

Do you want to save the current configuration for rollback? [Y]> n

Changes committed: Fri May 23 11:42:12 2014 GMT
```

이 예의 구성 변경에 대한 설명이 다음 그림에 나와 있습니다.

그림 ***58:*** 예*:*사용할 ***IP*** 인터페이스 또는 인터페이스 그룹 선택



가상 게이트웨이 주소 모니터링

각 가상 게이트웨이 주소는 전달을 위한 고유한 이메일 대기열을 가지고 있지만 시스템 관리, 로깅 및 보고 기능은 여전히 모든 가상 게이트웨이 대기열에 대한 전체적인 보기를 마치 하나인 것처럼 제공합니다. 각 가상 게이트웨이 대기열에 대한 수신자 호스트 상태를 모니터링하려면 hoststatus 및 hostrate 명령을 사용합니다. "CLI를 사용한 관리 및 모니터링" 장의 "사용 가능한 모니터링 구성 요소 읽기" 섹션을 참조하십시오.

hoststatus 명령은 특정 수신자 호스트와 관련된 이메일 작업에 대한 모니터링 정보를 반환합니다.

가상 게이트웨이 기술을 사용 중인 경우 각 가상 게이트웨이 주소에 대한 정보도 표시됩니다. 반환할 호스트 정보의 도메인을 입력하라는 프롬프트가 표시됩니다. AsyncOS 캐시에 저장된 DNS 정보 및 수신자 호스트에서 반환된 마지막 오류도 제공됩니다. 반환된 데이터는 마지막 resetcounters 명령 이후 누적된 것입니다.

반환된 통계는 카운터와 게이지라는 두 범주로 그룹화됩니다. 반환되는 기타 데이터에는 마지막 활동, MX 레코드 및 마지막 5XX 오류가 포함됩니다.

가상 게이트웨이 주소 단위로 전달 연결 관리

특정 시스템 매개변수는 시스템 및 가상 게이트웨이 주소 레벨에서 설정을 요구합니다.

예를 들면 일부 ISP는 각 클라이언트 호스트에 대해 허용하는 연결 수를 제한합니다. 따라서 여러 가상 게이트웨이 주소를 통해 이메일을 전달하는 경우에는 특히 ISP와의 관계를 관리하는 것이 중요합니다.

destconfig 명령 및 가상 게이트웨이 주소가 어떤 영향을 받는지에 대한 자세한 내용은 대상 제어를 사용하여 이메일 전달 제어, 703 페이지 항목을 참고하십시오.

가상 게이트웨이 주소의 "그룹"을 만들면, 그룹이 254개 IP 주소로 구성된 경우에도 가상 게이트웨이에 대한 good neighbor 테이블 설정이 그룹에 적용됩니다.

예를 들어 "라운드로빈" 방식으로 순환하기 위한 그룹으로서 254개 아웃바운드 IP 주소의 그룹을 만들었으며, small-isp.com에 대한 good neighbor 테이블이 시스템에 대한 동시 연결 100개, 가상 게이트웨이 주소에 대한 연결 10개라고 가정해보겠습니다. 이 컨피그레이션에서는 해당 그룹의 모든 254개 IP 주소에 대한 총 연결 수가 절대 10을 넘지 않습니다. 그룹은 단일 가상 게이트웨이 주소로서 취급됩니다.

전역 수신 거부 사용

특정 수신자, 수신자 도메인 또는 IP 주소에서 어플라이언스의 메시지를 수신하지 않도록 하려면 AsyncOS Global Unsubscribe(전역 수신 거부) 기능을 사용합니다. unsubscribe 명령을 사용하면 전역 수신 거부 목록에 주소를 추가하거나 삭제할 수 있으며, 이 기능을 활성화 및 비활성화할 수도 있습니다. AsyncOS는 "전역적으로 수신 거부된" 사용자, 도메인, 이메일 주소 및 IP 주소의 목록을 기준으로 모든 수신자 주소를 점검합니다. 특정 수신자가 목록의 주소와 일치하는 경우, 해당 수신자는 삭제 또는 하드 반송되며 GUS(Global Unsubscribe) 카운터가 증가합니다. (일치하는 수신자가 삭제되었는지, 하드 반송되었는지가 로그 파일이 기록됩니다.) 수신자에게 이메일을 전송하려고 시도하기 직전에 GUS 점검이 발생하므로 시스템에서 전송하는 모든 메시지가 검사됩니다.

참고 전역 수신 거부는 이름 제거 및 메일 목록의 일반적인 유지 관리를 대신하기 위한 것이 아닙니다. 이 기능은 이메일이 부적절한 엔티티로 전달되지 않도록 하기 위한 안전장치 역할을 합니다.

전역 수신 거부의 최대 주소 제한 수는 10,000개입니다. 전역 수신 거부 주소는 다음 네 가지 형태 중 하나일 수 있습니다.

표 ***61:*** 전역 수신 거부 구문

username@example.com	완전한 형식의 이메일 주소 특정 도메인에서 특정 수신자를 차단하는 데 이 구문이 사용됩니다.
username@	사용자 이름 사용자 이름 구문은 모든 도메인에서 지정된 사용자 이름을 가진 모든 수신자를 차단합니다. 구문은 사용자 이름과 그 뒤의 @ 기호로 구성됩니다.

@example.com	도메인 도메인 구문은 특정 도메인으로 향하는 모든 수신자를 차단하는 데 사용됩니다. 구문은 특정 도메인과 그 앞의 @ 기호로 구성됩니다.
@.example.com	부분 도메인 부분 도메인 구문은 특정 도메인 및 모든 하위 도메인으로 향하는 모든 수신자를 차단하는 데 사용됩니다.
10.1.28.12	IP 주소 IP 주소 구문은 특정 IP 주소로 향하는 모든 수신자를 차단하는 데 사용됩니다. 이 구문은 단일 IP 주소가 여러 도메인을 호스팅하는 경우 유용할 수 있습니다. 구문은 일반 점 옥텟 IP 주소로 구성됩니다.

관련 주제

- CLI를 사용하여 전역 수신 거부 주소 추가, 728 페이지
- 전역 수신 거부 파일 가져오기 및 내보내기, 730 페이지

CLI를 사용하여 전역 수신 거부 주소 추가

이 예에서는 주소 `user@example.net`이 전역 수신 거부 목록에 추가되고, 메시지를 하드 반송하도록 기능이 구성됩니다. 이 주소로 전송된 메시지는 반송됩니다. 어플라이언스는 전달 직전에 메시지를 반송합니다.

```
mail3.example.com> unsubscribe


Global Unsubscribe is enabled. Action: drop.

Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import entries from a file.

- SETUP - Configure general settings.

[]> new

Enter the unsubscribe key to add. Partial addresses such as

"@example.com" or "user@" are allowed, as are IP addresses. Partial hostnames such as

"@.example.com" are allowed.

[]> user@example.net
```

```
Email Address 'user@example.net' added.
Global Unsubscribe is enabled.
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]> setup
Do you want to enable the Global Unsubscribe feature? [Y]> y
Would you like matching messages to be dropped or bounced?
1. Drop
2. Bounce
[1]> 2
Global Unsubscribe is enabled. Action: bounce.
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]>

mail3.example.com> commit
Please enter some comments describing your changes:
[]> Added username “user@example.net” to global unsubscribe
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

전역 수신 거부 파일 가져오기 및 내보내기

HAT, RAT, smtproutes, 고정 가장 테이블, 별칭 테이블, 도메인 맵 테이블 및 altsrchost 항목과 마찬가지로 파일을 내보내고 가져와서 전역 수신 거부 항목을 수정할 수 있습니다.

단계 **1** unsubscribe 명령의 export 하위 명령을 사용하여 기존 항목을 파일(이름은 사용자가 지정)로 내보냅니다.

단계 **2** CLI 외부에서 파일을 가져옵니다. (자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지를 참조하십시오.)

단계 **3** 텍스트 편집기를 이용해 파일에서 새 항목을 만듭니다.

파일의 항목을 새 줄로 구분합니다. 모든 표준 운영 체제의 반환 표시를 사용할 수 있습니다(<CR>, <LF> 또는 <CR><LF>). 코멘트 줄은 숫자 기호(#)로 시작되며 무시됩니다. 예를 들어 다음 파일은 단일 수신자 이메일 주소(test@example.com), 특정 도메인의 모든 수신자(@testdomain.com), 여러 도메인에서 동일한 이름을 가진 모든 사용자(testuser@), 특정 IP 주소의 수신자(11.12.13.14)를 제외합니다.

```
# this is an example of the global_unsubscribe.txt file
test@example.com
@testdomain.com
testuser@
11.12.13.14
```

단계 **4** 파일을 저장한 다음, 가져올 수 있도록 인터페이스의 configuration 디렉터리에 둡니다. (자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지를 참조하십시오.)

단계 **5** unsubscribe의 import 하위 명령을 사용하여 수정한 파일을 가져옵니다.

검토: 이메일 파이프라인

다음 표에서는 수신에서 라우팅, 전달까지 시스템을 통해 이메일이 라우팅되는 방법에 대한 개요를 제공합니다. 각 기능은 순서대로(위에서 아래로) 처리되며 간단하게 요약됩니다. 표 - *Email Security Appliance*의 이메일 파이프라인: 라우팅 및 전달 기능의 음영 영역은 작업 대기열에서 발생하는 처리를 나타냅니다.

trace 명령을 사용하여 이 파이프라인에 있는 기능의 컨피그레이션을 대부분 테스트할 수 있습니다. 자세한 내용은 문제 해결 장의 "테스트 메시지를 사용하여 메일 플로우 디버깅: 추적"을 참조하십시오.

참고 발신 메일에 대해서는 보안 침해 필터 단계 후에 데이터 손실 방지 검사가 수행됩니다.

표 ***62: Email Security Appliance***에 대한 이메일 파이프라인*:* 이메일 수신 기능

기능	설명
HAT(Host Access Table) 호스트 DNS 발신자 확인 그룹 봉투 발신자 확인 발신자 확인 예외 테이블 메일 흐름 정책	ACCEPT, REJECT, RELAY 또는 TCPREFUSE 연결 최대 아웃바운드 연결 수 IP 주소당 최대 동시 인바운드 연결 수 연결당 최대 메시지 크기 및 메시지 수 메시지 및 시간당 최대 수신자 수 TCP 수신 대기열 크기 TLS: no/preferred/required(없음/기본 설정/필수) SMTP AUTH: no/preferred/required(없음/기본 설정/필수) 형식이 잘못된 FROM 헤더의 이메일 삭제 발신자 확인 예외 테이블의 항목에서 오는 메일을 항상 수락 또는 거부합니다. SenderBase 켜기/끄기(IP profiling/흐름도)
Received 헤더	수락한 이메일에 Received 헤더를 추가합니다(on/off).
기본 도메인	"베어(bare)" 사용자 주소에 대한 기본 도메인 추가
반송 확인	수신 반송 메시지를 합법적인 것으로 확인하는 데 사용됩니다.
도메인 맵	도메인 맵 테이블의 도메인과 일치하는 메시지에서 각 수신자에 대한 봉투 수신자를 재작성합니다.
Recipient Access Table(RAT)	(퍼블릭 리스너 전용) RCPT TO 및 사용자 지정 SMTP 응답에서 수신자를 수락(ACCEPT) 또는 거부(REJECT)합니다. 특정 수신자가 조절(throttling)을 우회하도록 허용합니다.
별칭 테이블	봉투 수신자를 재작성합니다. (시스템 전체에서 구성됩니다. aliasconfig는 listenerconfig의 하위 명령입니다.)
LDAP 수신자 수락	수신자 수락을 위한 LDAP 검증이 SMTP 대화 내에서 발생합니다. 수신자가 LDAP 디렉터리에 없으면 메시지가 삭제 또는 반송됩니다. LDAP 검증이 대신 작업 대기열 내에서 발생하도록 구성할 수 있습니다.

표 ***63: Email Security Appliance***에 대한 이메일 파이프라인*:* 라우팅 및 전달 기능

작업 큐	**LDAP** 수신자 수락		수신자 수락을 위한 LDAP 검증이 작업 대기열 내에서 발생합니다. 수신자가 LDAP 디렉터리에 없으면 메시지가 삭제 또는 반송됩니다. LDAP 검증이 대신 SMTP 대화 내에서 발생하도록 구성할 수 있습니다.
	마스커레이드 또는 **LDAP** 가장		가장은 작업 대기열에서 발생하며, 고정 테이블에서 또는 LDAP 쿼리를 통해 봉투 발신자, To:, From: 및/또는 CC: 헤더를 재작성합니다.
	LDAP 라우팅		메시지 라우팅 또는 주소 재작성을 위해 LDAP 쿼리가 수행됩니다. 그룹 LDAP 쿼리는 메시지 필터 규칙 mail-from-group 및 rcpt-to-group과 함께 동작합니다.
	메시지 필터*		메시지 필터는 메시지 "분리" 전에 적용됩니다. * 메시지를 격리로 보낼 수 있습니다.
	안티스팸**	수신자 단위 검사	안티스팸 검사 엔진은 메시지를 검사하고 추가 처리를 위해 판정을 반환합니다.
	안티바이러스*		안티바이러스 검사는 메시지에서 바이러스를 검사합니다. 메시지가 검사되고 가능한 경우 선택적으로 복구됩니다. * 메시지를 격리로 보낼 수 있습니다.
	AMP(Advanced Malware Protection)		Advanced Malware Protection은 첨부 파일에서 악성코드를 탐지하기 위해 파일 평판 검사 및 파일 분석을 수행합니다.
	콘텐츠 필터*		콘텐츠 필터가 적용됩니다. * 메시지를 격리로 보낼 수 있습니다.
	보안 침해 필터*		보안 침해 필터는 바이러스 보안 침해로부터 보호합니다. * 메시지를 격리로 보낼 수 있습니다.
	가상 게이트웨이		특정 IP 인터페이스 또는 IP 인터페이스 그룹을 통해 메일을 전송합니다.
	전달 제한		1. 기본 전달 인터페이스를 설정합니다. 2. 최대 아웃바운드 연결 수를 설정합니다.
	도메인 기반 제한		도메인 단위로 정의합니다. 각 가상 게이트웨이 및 전체 시스템에 대한 최대 아웃바운드 연결 수, 사용할 반송 프로필, 전달을 위한 TLS 기본 설정: no/preferred/required(없음/기본 설정/필수)
	도메인 기반 라우팅		봉투 발신자를 재작성하지 않은 채 도메인을 기반으로 메일을 라우팅합니다.

	전역 수신 거부		특정 목록에 따라 수신자를 삭제합니다(시스템 전체에서 구성).
	반송 프로필		전달할 수 없는 메시지 처리. 리스너 단위, 대상 제어 항목 단위 및 메시지 필터를 통해 구성 가능

* 이러한 기능은 메시지를 격리라는 특수 대기열로 전송할 수 있습니다.

29 장

LDAP 쿼리

이 장에는 다음 섹션이 포함되어 있습니다.

LDAP 쿼리의 개요

사용자 정보를 네트워크 인프라의 LDAP 디렉터리(예: Microsoft Active Directory, SunONE Directory Server 또는 OpenLDAP 디렉터리) 내에 저장하는 경우, 메시지를 수락하고 라우팅하고 인증하기 위해 LDAP 서버를 쿼리하도록 어플라이언스를 구성할 수 있습니다. 하나 또는 여러 LDAP 서버와 작동하도록 어플라이언스를 구성할 수 있습니다.

다음 섹션에서는 사용자가 수행할 수 있는 LDAP 쿼리 유형, 메시지의 인증, 수락 및 라우팅을 위해 LDAP가 어플라이언스와 작동하는 방법, 그리고 LDAP와 작동하도록 어플라이언스를 구성하는 방법에 대한 개요를 제공합니다.

관련 주제

- LDAP 쿼리 이해, 736 페이지
- LDAP가 AsyncOS와 작동하는 방식 이해, 737 페이지
- LDAP 서버와 작동하도록 Cisco IronPort 어플라이언스 구성, 738 페이지
- LDAP 서버에 대한 정보를 저장할 LDAP 서버 프로필 만들기, 739 페이지
- LDAP 서버 테스트, 740 페이지
- 특정 리스너에서 실행할 LDAP 쿼리 활성화, 740 페이지
- Microsoft Exchange 5.5에 대한 고급 지원, 743 페이지

LDAP 쿼리 이해

사용자 정보를 네트워크 인프라의 LDAP 디렉터리 내에 저장하는 경우 다음에 대해 LDAP 서버를 쿼리하도록 어플라이언스를 구성할 수 있습니다.

- 수락 쿼리. 기존의 LDAP 인프라를 사용하여 수신 메시지의 수신자 이메일 주소(퍼블릭 리스너에서)를 처리하는 방법을 정의할 수 있습니다. 자세한 내용은 수신자 검증을 위해 수락 쿼리 사용, 752 페이지를 참고하십시오.
- 라우팅(별칭 사용)**.** 네트워크의 LDAP 디렉터리에서 사용 가능한 정보를 기반으로 적절한 주소 및/또는 메일 호스트로 메시지를 라우팅하도록 어플라이언스를 구성할 수 있습니다. 자세한 내용은 라우팅 쿼리를 사용하여 여러 대상 주소에 메일 전송, 754 페이지를 참고하십시오.
- 인증서 인증**.** 사용자의 메일 클라이언트와 Email Security Appliance 간 SMTP 세션을 인증하기 위해 클라이언트 인증서의 유효성을 확인하는 쿼리를 만들 수 있습니다. 자세한 내용은 클라이언트 인증서의 유효성 확인, 785 페이지를 참고하십시오.
- 가장. 봉투 발신자(발신 메일용) 및 메시지 헤더(To:, Reply To:, From: 또는 CC:와 같은 수신 메일용)를 가장(masquerade)할 수 있습니다. 가장에 대한 자세한 내용은 가장 쿼리를 사용하여 봉투 발신자 재작성, 755 페이지 섹션을 참조하십시오.
- 그룹 쿼리. LDAP 디렉터리에 있는 그룹을 기반으로 메시지에 대해 작업을 수행하도록 어플라이언스를 구성할 수 있습니다. 그룹 쿼리를 메시지 필터와 연결하면 됩니다. 메시지 필터에 대해 사용 가능한 메시지 작업을 정의된 LDAP 그룹과 일치하는 메시지에 대해 수행할 수 있습니다. 자세한 내용은 그룹 LDAP 쿼리를 사용하여 수신자가 그룹 구성원인지 확인, 756 페이지를 참고하십시오.
- 도메인 기반 쿼리. 어플라이언스가 단일 리스너에서 서로 다른 도메인에 대해 서로 다른 쿼리를 수행하도록 하려면 도메인 기반 쿼리를 만들 수 있습니다. Email Security Appliance는 도메인 기반 쿼리를 수행할 때 도메인을 기반으로 사용할 쿼리를 결정하고, 해당 도메인과 연결된 LDAP 서버를 쿼리합니다.
- 체인 쿼리**.** 어플라이언스가 일련의 쿼리를 순서대로 수행하도록 체인 쿼리를 만들 수 있습니다. 체인 쿼리를 구성하면, 어플라이언스는 LDAP 어플라이언스가 긍정적인 결과를 반환할 때까지 각 쿼리를 순서대로 실행합니다. 체인 라우팅 쿼리의 경우, 어플라이언스에서 재작성된 각 이메일 주소에 대해 구성된 동일한 체인 쿼리를 순서대로 다시 실행합니다.
- 디렉터리 수집 방지. LDAP 디렉터리를 사용한 디렉터리 수집 공격을 차단하도록 어플라이언스를 구성할 수 있습니다. SMTP 대화 중에 또는 네트워크 대기열 내에 디렉터리 수집 방지를 구성할 수 있습니다. LDAP 디렉터리에서 수신자가 발견되지 않으면 지연된 반송을 수행하거나 메시지를 완전히 삭제하도록 시스템을 구성할 수 있습니다. 그 결과 스패머는 유효한 이메일 주소와

유효하지 않은 이메일 주소를 구분할 수 없게 됩니다. 디렉터리 수집 공격 방지에 LDAP 사용, 763 페이지를 참조하십시오.

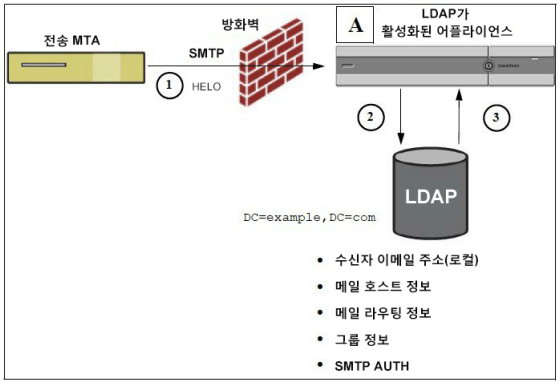
- **SMTP** 인증. AsyncOS는 SMTP 인증에 대한 지원을 제공합니다. SMTP 인증은 SMTP 서버에 연결된 클라이언트를 인증하기 위한 메커니즘입니다. 조직의 사용자가 원격으로 연결되어 있는 경우에도(집에서 또는 출장 중에) 메일 서버를 사용하여 메일을 전송하도록 하려면 이 기능을 사용할 수 있습니다. 자세한 내용은 SMTP 인증을 위해 AsyncOS 구성, 765 페이지를 참고하십시오.
- 외부 인증. 어플라이언스에 로그인한 사용자를 인증하기 위해 LDAP 디렉터리를 사용하도록 어플라이언스를 구성할 수 있습니다. 자세한 내용은 사용자를 위한 외부 LDAP 인증 구성, 773 페이지를 참고하십시오.
- 스팸 격리 최종 사용자 인증. 최종 사용자 격리에 로그인하는 사용자를 검증하도록 어플라이언스를 구성할 수 있습니다. 자세한 내용은 스팸 격리의 최종 사용자 인증, 776 페이지를 참고하십시오.
- 스팸 격리 별칭 통합. 스팸에 대한 이메일 알림을 사용하는 경우 이 쿼리는 최종 사용자가 각 별칭 이메일 주소에 대해 격리 알림을 수신하지 못하도록 최종 사용자 별칭을 통합합니다. 자세한 내용은 스팸 격리 별칭 통합 쿼리, 778 페이지를 참고하십시오.

LDAP가 AsyncOS와 작동하는 방식 이해

LDAP 디렉터리 작업 시 수신자 수락, 메시지 라우팅 및/또는 헤더 가장을 위해 어플라이언스를 LDAP 디렉터리 서버와 함께 사용할 수 있습니다. 또한 LDAP 그룹 쿼리를 메시지 필터와 함께 사용하여, 어플라이언스에서 수신할 때 메시지를 처리하기 위한 규칙을 만들 수 있습니다.

다음 그림은 어플라이언스와 LDAP의 작동 방식을 보여줍니다.

그림 ***59: LDAP*** 구성



1. 전송 MTA는 SMTP를 통해 메시지를 퍼블릭 리스너 "A"로 전송합니다.
2. 어플라이언스는 **System Administration**(시스템 관리) > **LDAP** 페이지(또는 전역 **`ldapconfig`** 명령)를 통해 정의된 LDAP 서버를 쿼리합니다.
3. LDAP 디렉터리에서, 그리고 **System Administration**(시스템 관리자) > **LDAP** 페이지(또는 **`ldapconfig`** 명령)에서 정의하고 리스너가 사용하는 쿼리에 따라 데이터가 수신됩니다.
   - 메시지는 새로운 수신자 주소로 라우팅되거나 삭제되거나 반송됩니다.
   - 메시지는 새로운 수신자에 대한 적절한 메일 호스트로 라우팅됩니다.
   - From:, To: 및 CC: 메시지 헤더는 쿼리를 기반으로 재작성됩니다.

- **rcpt-to-group** 또는 **mail-from-group** 메시지 필터 규칙으로 추가 작업이 정의됩니다(구성된 그룹 쿼리와 함께 사용됨).

참고 여러 LDAP 서버에 연결하기 위해 어플라이언스를 구성할 수 있습니다. 이렇게 할 때 부하분산 또는 장애 조치에 대한 LDAP 프로필 설정을 구성할 수 있습니다. 여러 LDAP 서버 작업에 대한 자세한 내용은 여러 LDAP 서버와 작동하도록 AsyncOS 구성, 780 페이지 섹션을 참조하십시오.

LDAP 서버와 작동하도록 Cisco IronPort 어플라이언스 구성

LDAP 디렉터리와 작동하도록 어플라이언스를 구성할 때 AsyncOS 어플라이언스에서 수락, 라우팅, 별칭 사용 및 가장을 구성하려면 다음 단계를 완료해야 합니다.

단계 **1** **LDAP** 서버 프로필을 구성합니다. 서버 프로필에는 AsyncOS가 LDAP 서버에 연결하기 위해 필요한 다음과 같은 정보가 포함됩니다.

- 서버의 이름 및 쿼리를 전송할 포트
- 기본 DN
- 서버에 바인딩하기 위한 인증 요구 사항

서버 프로필 구성에 대한 자세한 내용은 LDAP 서버에 대한 정보를 저장할 LDAP 서버 프로필 만들기, 739 페이지 섹션을 참조하십시오.

LDAP 서버 프로필 구성 시 하나 또는 여러 LDAP 서버에 연결하도록 AsyncOS를 구성할 수 있습니다.

여러 서버에 연결하도록 AsyncOS를 구성하는 방법에 대한 자세한 내용은 여러 LDAP 서버와 작동하도록 AsyncOS 구성, 780 페이지 섹션을 참조하십시오.

단계 **2** **LDAP** 쿼리를 구성합니다. LDAP 서버 프로필에서 LDAP 쿼리를 구성합니다. 구성하는 쿼리는 특별한 LDAP 구현 및 스키마에 맞춰야 합니다.

만들 수 있는 LDAP 쿼리 유형에 대한 자세한 내용은 LDAP 쿼리 이해, 736 페이지 섹션을 참조하십시오.

쿼리 작성에 대한 자세한 내용은 LDAP 쿼리 작업, 745 페이지 섹션을 참조하십시오.

단계 **3** 퍼블릭 리스너 또는 프라이빗 리스너에서 **LDAP** 서버 프로필을 활성화합니다. 리스너가 메시지를 수락, 라우팅 또는 전송할 때 LDAP 쿼리를 실행하도록 하려면 리스너에서 LDAP 서버 프로필을 활성화해야 합니다.

자세한 내용은 특정 리스너에서 실행할 LDAP 쿼리 활성화, 740 페이지를 참고하십시오.

참고 그룹 쿼리를 구성할 때 AsyncOS가 LDAP 서버와 작동하도록 구성하기 위한 추가 단계를 수행해야 합니다. 그룹 쿼리 구성에 대한 자세한 내용은 그룹 LDAP 쿼리를 사용하여 수신자가 그룹 구성원인지 확인, 756 페이지 섹션을 참조하십시오. 최종 사용자 인증 또는 스팸 알림 통합 쿼리를 구성할 때 스팸 격리에 대한 LDAP 최종 사용자 액세스를 활성화해야 합니다. 스팸 격리에 대한 자세한 내용은 스팸 격리 장을 참조하십시오.

LDAP 서버에 대한 정보를 저장할 LDAP 서버 프로필 만들기

AsyncOS가 LDAP 디렉터리를 사용하도록 구성할 때 LDAP 서버에 대한 정보를 저장할 LDAP 서버 프로필을 만들어야 합니다.

단계 **1** **System Administration(**시스템 관리**) > LDAP** 페이지에서 **Add LDAP Server Profile(LDAP** 서버 프로필 추가**)**을 클릭합니다.

단계 **2** 서버 프로필의 이름을 입력합니다.

단계 **3** LDAP 서버의 호스트 이름을 입력합니다.

LDAP 서버에서 장애 조치 또는 부하분산을 구성하려면 여러 호스트 이름을 입력할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분하십시오. 자세한 내용은 여러 LDAP 서버와 작동하도록 AsyncOS 구성, 780 페이지를 참고하십시오.

단계 **4** 인증 방법을 선택합니다. 익명 인증을 사용하거나 사용자 이름과 암호를 지정할 수 있습니다.

단계 **5** LDAP 서버 유형(Active Directory, OpenLDAP, Unknown 또는 Other)을 선택합니다.

단계 **6** 포트 번호를 입력합니다.

Active Directory 또는 Unknown(알 수 없음)/Other(기타) 서버 유형의 경우 기본 포트는 SSL을 사용하지 않는 3268과 SSL을 사용하는 3269입니다.

Open LDAP 서버 유형의 경우 기본 포트는 SSL을 사용하지 않는 389와 SSL을 사용하는 636입니다.

단계 **7** LDAP 서버의 기본 DN(distinguishing name)을 입력합니다.

사용자 이름 및 암호로 인증하는 경우, 사용자 이름은 암호가 포함된 항목에 대한 전체 DN을 포함해야 합니다. 예를 들어 사용자가 마케팅 그룹 구성원이며 이메일 주소는 joe@example.com입니다. 이 사용자에 대한 항목은 다음과 같을 수 있습니다.

```
uid=joe, ou=marketing, dc=example dc=com
```

단계 **8** LDAP 서버와 통신할 때 SSL 사용 여부를 선택합니다.

단계 **9** Advanced(고급) 아래에 캐시 TTL(time-to-live)을 입력합니다. 이 값은 캐시를 보유할 시간을 나타냅니다.

단계 **10** 보유되는 최대 캐시 항목 수를 입력합니다.

참고 이 캐시는 LDAP 서버 단위로 유지 관리됩니다. 둘 이상의 LDAP 서버를 구성하는 경우 더 나은 성능을 얻으려면 LDAP 캐시 값을 더 작게 설정해야 합니다. 또한 어플라이언스에서 각종 프로세스의 메모리 사용량이 큰 경우 이 값을 높이면 시스템 성능이 저하될 수 있습니다.

단계 **11** 동시 연결 수를 입력합니다.

LDAP 서버 프로필에서 부하분산을 구성하는 경우 이러한 연결은 나열된 LDAP 서버 중에 분산됩니다. 예를 들어 10개의 동시 연결을 구성하며 3개 서버를 통해 연결의 부하를 분산하는 경우 AsyncOS는 각 서버에 대해 10개씩 총 30개의 연결을 만듭니다.

참고 최대 동시 연결 수에는 LDAP 쿼리에 사용되는 LDAP 연결이 포함됩니다. 그러나 스팸 격리에 대해 LDAP 인증을 사용하는 경우 어플라이언스는 더 많은 연결을 엽니다.

단계 **12** Test Server(s)(서버 테스트) 버튼을 클릭하여 서버에 대한 연결을 테스트합니다. 여러 LDAP 서버를 지정한 경우 모든 서버가 테스트됩니다. 테스트 결과는 Connection Status(연결 상태) 필드에 나타납니다. 자세한 내용은 LDAP 서버 테스트, 740 페이지을 참고하십시오.

단계 **13** 확인란을 선택하고 필드를 완료하여 쿼리를 만듭니다. Accept(수락), Routing(라우팅), Masquerade(가장), Group(그룹), SMTP Authentication(SMTP 인증), External Authentication(외부 인증), Spam Quarantine End-User Authentication(스팸 격리 최종 사용자 인증) 및 Spam Quarantine Alias Consolidation(스팸 격리 별칭 통합)을 선택할 수 있습니다.

참고 메시지를 수신 또는 송신할 때 어플라이언스에서 LDAP 쿼리를 실행하도록 하려면 적절한 리스너에서 LDAP 쿼리를 활성화해야 합니다. 자세한 내용은 특정 리스너에서 실행할 LDAP 쿼리 활성화, 740 페이지를 참고하십시오.

단계 **14** **Test Query(**쿼리 테스트**)** 버튼을 클릭하여 쿼리를 테스트합니다.

테스트 매개변수를 입력하고 Run Test(테스트 실행)를 클릭합니다. 테스트 결과는 Connection Status(연결 상태) 필드에 나타납니다. 쿼리 정의 또는 특성을 변경하려면 **Update(**업데이트**)**를 클릭합니다. 자세한 내용은 LDAP 서버 테스트, 740 페이지를 참고하십시오.

참고 비어 있는 암호와 바인딩하도록 LDAP 서버를 구성한 경우 쿼리는 비어 있는 암호 필드의 테스트를 통과할 수 있습니다.

단계 **15** 변경 사항을 제출 및 커밋합니다.

참고 서버 구성의 수는 무제한이지만 서버당 수신자 수락, 라우팅, 가장 및 그룹 쿼리는 하나씩만 구성할 수 있습니다.

LDAP 서버 테스트

LDAP 서버에 대한 연결을 테스트하려면 Add/Edit LDAP Server Profile(LDAP 서버 프로필 추가/수정) 페이지에 있는 Test Server(s)(서버 테스트) 버튼(또는 CLI에서 ldapconfig 명령의 test 하위 명령)을 사용합니다. AsyncOS는 서버 포트에 대한 연결의 성공 여부를 나타내는 메시지를 표시합니다. 여러 LDAP 서버를 구성한 경우 AsyncOS는 각 서버를 테스트하고 개별 결과를 표시합니다.

특정 리스너에서 실행할 LDAP 쿼리 활성화

메시지를 수신 또는 송신할 때 어플라이언스에서 LDAP 쿼리를 실행하도록 하려면 적절한 리스너에서 LDAP 쿼리를 활성화해야 합니다.

관련 주제

- LDAP 쿼리에 대한 전역 설정 구성, 741 페이지
- LDAP 서버 프로필 만들기 예, 741 페이지
- 퍼블릭 리스너에서 LDAP 쿼리 활성화, 742 페이지
- 프라이빗 리스너에서 LDAP 쿼리 활성화, 743 페이지

LDAP 쿼리에 대한 전역 설정 구성

LDAP 전역 설정은 어플라이언스가 모든 LDAP 트래픽을 처리하는 방법을 정의합니다.

단계 **1** **System Administration**(시스템 관리) > **LDAP** 페이지에서 **Edit Settings**(설정 수정)를 클릭합니다.

단계 **2** LDAP 트래픽에 사용할 IP 인터페이스를 선택합니다. 기본적으로 어플라이언스가 자동으로 인터페이스를 선택합니다.

단계 **3** LDAP 인터페이스에 사용할 TLS 인증서를 선택합니다. **Network**(네트워크) > **Certificates**(인증서) 페이지 또는 CLI의 **certconfig** 명령을 통해 추가된 TLS 인증서를 목록에서 사용할 수 있습니다. 다른 MTA와의 통신 암호화 개요, 645 페이지 섹션을 참조하십시오.

단계 **4** LDAP 서버 인증서의 유효성을 검사하려는 경우 적절한 옵션을 선택합니다.

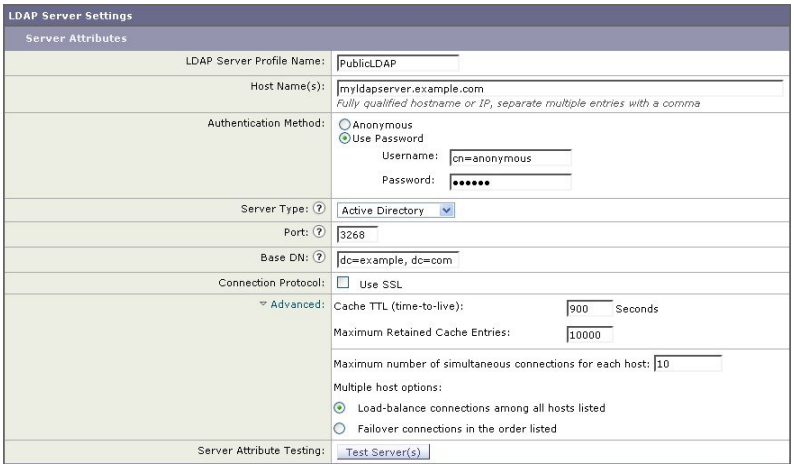
단계 **5** 변경 사항을 제출 및 커밋합니다.

LDAP 서버 프로필 만들기 예

다음 예에서는 System Administration(시스템 관리) > LDAP 페이지를 사용하여 바인딩할 어플라이언스에 대한 LDAP 서버를 정의하고 수신자 수락, 라우팅 및 가장을 구성합니다.

참고 LDAP 연결에 대한 60초 연결 시도 시간 초과가 있습니다(여기에는 DNS 조회, 연결 자체, 그리고 해당되는 경우 어플라이언스 자체에 대한 인증 바인딩이 포함됨). 첫 번째 실패 이후 AsyncOS는 동일한 서버의 다른 호스트에 대한 시도를 즉시 시작합니다(쉼표로 구분된 목록에 둘 이상 지정한 경우). 서버에 호스트가 하나뿐이면 AsyncOS는 계속해서 연결을 시도합니다.

그림 ***60: LDAP*** 서버 프로필 구성***(1/2)***

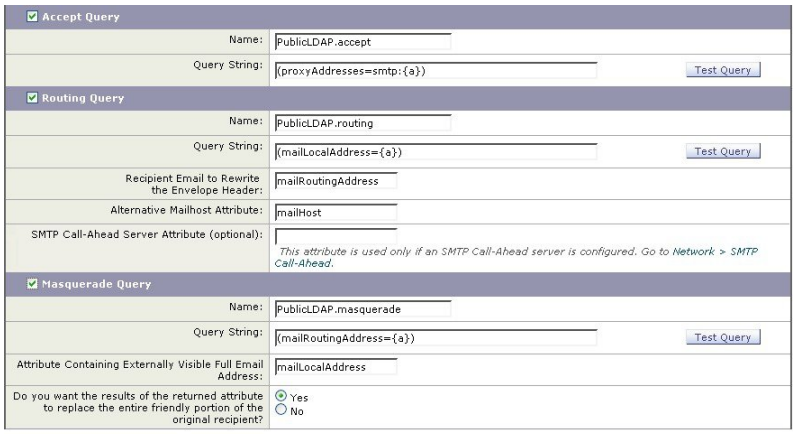


우선 myldapserver.example.com LDAP 서버에 "PublicLDAP"라는 별칭이 지정됩니다. 연결 수가 10(기본값)으로 설정되고, 다중 LDAP 서버(호스트) 부하분산 옵션이 기본값으로 남겨집니다. 쉼표로 구분된 이름 목록을 제공하여 여러 호스트를 지정할 수 있습니다. Queries are directed to port 3268 (the

default). SSL은 이 호스트에 대한 연결 프로토콜로서 활성화되지 않습니다. example.com의 기본 DN이 정의됩니다(dc=example,dc=com). 캐시 TTL(time-to-live)이 900초, 최대 캐시 항목 수가 10000, 인증 방법이 passphrase로 설정됩니다.

수신자 수락, 메일 라우팅 및 가장에 대한 쿼리가 정의됩니다. 쿼리 이름은 대/소문자를 구분하며 정확히 매치해야 알맞은 결과가 반환됩니다.

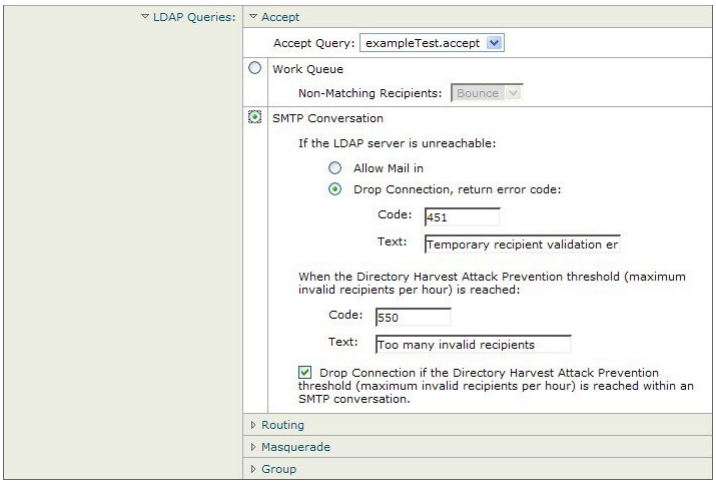
그림 ***61: LDAP*** 서버 프로필 구성***(2/2)***



퍼블릭 리스너에서 LDAP 쿼리 활성화

이 예에서는 퍼블릭 리스너 "InboundMail"이 수신자 수락에 LDAP 쿼리를 사용하도록 업데이트됩니다. 추가로, SMTP 대화 중에 이루어질 수신자 수락이 구성됩니다(자세한 내용은 수신자 검증을 위해 수락 쿼리 사용, 752 페이지 참조).

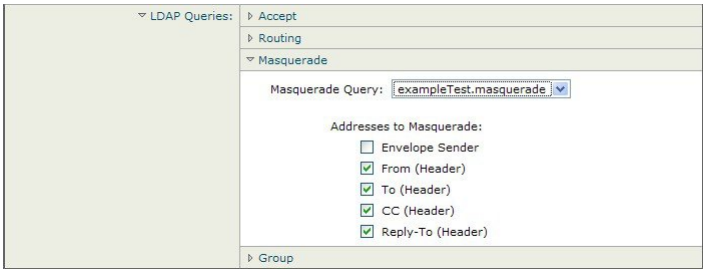
그림 ***62:*** 리스너에서 수락 및 라우팅 쿼리 활성화



프라이빗 리스너에서 LDAP 쿼리 활성화

이 예에서는 프라이빗 리스너 OutboundMail"이 가장에 LDAP 쿼리를 사용하도록 업데이트됩니다. 가장 필드에는 From, To, CC 및 Reply-To가 포함됩니다.

그림 ***63:*** 리스너에서 가장 쿼리 활성화



Microsoft Exchange 5.5에 대한 고급 지원

AsyncOS에는 Microsoft Exchange 5.5에 대한 지원을 제공하기 위한 구성 옵션이 포함되어 있습니다. Microsoft Exchange의 최신 버전을 사용하는 경우 이 옵션을 활성화할 필요가 없습니다. LDAP 서버를 구성할 때 `ldapconfig -> edit -> server -> compatibility` 하위 명령에서 프롬프트에 "y"로 답하여 Microsoft Exchange 5.5를 활성화하도록 선택할 수 있습니다(CLI를 통해서만 사용 가능).

```
mail3.example.com> ldapconfig

Current LDAP server configurations:

1. PublicLDAP: (ldapexample.com:389)


Choose the operation you want to perform:

- NEW - Create a new server configuration.

- EDIT - Modify a server configuration.

- DELETE - Remove a server configuration.


[]> edit

Enter the name or number of the server configuration you wish to edit.

[]> 1

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Choose the operation you want to perform:

- SERVER - Change the server for the query.
```

```
- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.

- LDAPROUTING - Configure message routing.

- MASQUERADE - Configure domain masquerading.

- LDAPGROUP - Configure whether a sender or recipient is in a specified group.

- SMTPAUTH - Configure SMTP authentication.

[]> server

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com


Microsoft Exchange 5.5 Compatibility Mode: Disabled

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]> compatibility
Would you like to enable Microsoft Exchange 5.5 LDAP compatibility mode? (This is not
recommended for versions of Microsoft Exchange later than 5.5, or other LDAP servers.)


[N]> y

Do you want to configure advanced LDAP compatibility settings? (Typically not required)

[N]>

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Microsoft Exchange 5.5 Compatibility Mode: Enabled (attribute "objectClass")

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.
```

```
- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]>
```

LDAP 쿼리 작업

LDAP 서버 프로필에서 수행할 LDAP 쿼리의 각 유형에 대해 항목을 만듭니다. LDAP 쿼리를 만들 때 LDAP 서버에 대한 쿼리 구문을 입력해야 합니다. 특히 디렉터리의 고유한 요구를 수용하기 위해 새로운 개체 클래스와 특성으로 디렉터리를 확장한 경우에는 LDAP 디렉터리 서비스의 특별한 구현에 맞게 쿼리를 작성해야 합니다.

관련 주제

- LDAP 쿼리의 유형, 745 페이지
- 기본 DN(Distinguishing Name), 746 페이지
- LDAP 쿼리 구문, 746 페이지
- 보안 LDAP(SSL), 747 페이지
- 라우팅 쿼리, 747 페이지
- 클라우드가 LDAP 서버에 익명으로 바인딩되도록 허용 , 747 페이지
- LDAP 쿼리 테스트, 750 페이지
- LDAP 서버에 대한 연결 문제 해결, 752 페이지

LDAP 쿼리의 유형

- 수락 쿼리. 자세한 내용은 수신자 검증을 위해 수락 쿼리 사용, 752 페이지를 참고하십시오.
- 라우팅 쿼리. 자세한 내용은 라우팅 쿼리를 사용하여 여러 대상 주소에 메일 전송, 754 페이지를 참고하십시오.
- 인증서 인증 쿼리. 자세한 내용은 클라이언트 인증서의 유효성 확인, 785 페이지를 참고하십시오.
- 가장 쿼리. 자세한 내용은 가장 쿼리를 사용하여 봉투 발신자 재작성, 755 페이지를 참고하십시오.
- 그룹 쿼리. 자세한 내용은 그룹 LDAP 쿼리를 사용하여 수신자가 그룹 구성원인지 확인, 756 페이지를 참고하십시오.
- 도메인 기반 쿼리. 자세한 내용은 도메인 기반 쿼리를 사용하여 특정 도메인으로 라우팅, 760 페이지를 참고하십시오.
- 체인 쿼리. 자세한 내용은 체인 쿼리를 사용하여 일련의 LDAP 쿼리 수행, 761 페이지를 참고하십시오.

다음을 위해 쿼리를 구성할 수도 있습니다.

- 디렉터리 수집 방지. 자세한 내용은 LDAP 쿼리 이해, 736 페이지를 참고하십시오.
- **SMTP** 인증**.** 자세한 내용은 SMTP 인증을 위해 AsyncOS 구성, 765 페이지를 참고하십시오.
- 외부 인증. 자세한 내용은 사용자를 위한 외부 LDAP 인증 구성, 773 페이지를 참조하십시오.
- 스팸 격리 최종 사용자 인증 쿼리**.** 자세한 내용은 스팸 격리의 최종 사용자 인증, 776 페이지를 참고하십시오.
- 스팸 격리 별칭 통합 쿼리**.** 자세한 내용은 스팸 격리 별칭 통합 쿼리, 778 페이지을 참고하십시오.

지정하는 검색 쿼리는 시스템에 구성한 모든 리스너에서 사용할 수 있습니다.

기본 DN(Distinguishing Name)

디렉터리의 루트 레벨을 기본(base)이라고 합니다. 기본(base)의 이름이 DN(distinguishing name)입니다. Active Directory에 대한 기본 DN 형식(및 RFC 2247에 대한 표준)에는 도메인 구성 요소(dc=)로 변환된 DNS 도메인이 있습니다. 예를 들어 example.com의 기본 DN은 dc=example, dc=com과 같을 수 있습니다. DNS 이름의 각 부분은 순서대로 나타납니다. 여기에는 구성의 LDAP 설정이 반영될 수도 있고 반영되지 않을 수도 있습니다.

디렉터리에 여러 도메인이 포함되어 있는 경우 쿼리에 대해 단일 BASE만 입력하는 것이 불편할 수 있습니다. 이 경우 LDAP 서버 설정을 구성할 때 BASE를 NONE으로 설정합니다. 그러나 이 경우 검색 효율성이 떨어집니다.

LDAP 쿼리 구문

LDAP 경로에는 공백을 사용할 수 있으며 따옴표는 필요하지 않습니다. CN 및 DC 구문은 대/소문자를 구분하지 않습니다.

Cn=First Last,oU=user,dc=domain,DC=COM

쿼리에 대해 입력하는 변수는 대/소문자를 구분하며, 제대로 작동하려면 LDAP 구현과 일치해야 합니다. 예를 들어 프롬프트에서 **mailLocalAddress**를 입력하면 **maillocaladdress**를 입력하는 경우와 다른 쿼리를 수행합니다.

관련 주제

- 토큰:, 746 페이지

토큰:

LDAP 쿼리에 다음 토큰을 사용할 수 있습니다.

- {a} username@domainname
- {d} domainname
- {dn} distinguished name
- {g} groupname
- {u} username
- {f} MAIL FROM: address

참고 {f} 토큰은 수락 쿼리에서만 유효합니다.

예를 들면 Active Directory LDAP 서버에 대한 메일을 수락하기 위해 다음 쿼리를 사용할 수 있습니다.

(|(mail={a})(proxyAddresses=smtp:{a}))

참고 Cisco에서는 작성하는 모든 쿼리를 테스트하는 데 LDAP 페이지의 Test(테스트) 기능(또는 **ldapconfig** 명령의 **test** 하위 명령)을 사용하고, 리스너에서 LDAP 기능을 활성화하기 전에 예상 결과가 반환되는지 확인할 것을 적극 권장합니다. 자세한 내용은 LDAP 쿼리 테스트, 750 페이지를 참조하십시오.

보안 LDAP(SSL)

AsyncOS에서 LDAP 서버와 통신할 때 SSL을 사용하도록 지정할 수 있습니다. SSL을 사용하도록 LDAP 서버 프로필을 구성하는 경우

- AsyncOS는 CLI에서 certconfig를 통해 구성된 LDAPS 인증서를 사용합니다(셀프 서명 인증서 만들기 , 648 페이지 참조).

  LDAPS 인증서를 사용하여 지원할 LDAP 서버를 구성해야 할 수 있습니다.
- LDAPS 인증서가 구성되지 않은 경우 AsyncOS는 데모 인증서를 사용합니다.

라우팅 쿼리

LDAP 라우팅 쿼리에 대한 재귀 제한은 없습니다. 라우팅은 완전히 데이터 기반입니다. 그러나 AsyncOS는 라우팅의 무한 루프를 방지하기 위해 순환 참조 데이터를 확인합니다.

클라우드가 LDAP 서버에 익명으로 바인딩되도록 허용

익명 쿼리를 허용하도록 LDAP 디렉터리 서버를 구성해야 할 수 있습니다. (즉, 클라이언트를 서버에 익명으로 바인딩하고 쿼리를 수행할 수 있습니다.) 익명 쿼리를 허용하도록 Active Directory를 구성하는 특별한 지침은 다음 URL에서 "Microsoft Knowledge Base Article - 320528"을 참조하십시오.

```
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320528
```

임의의 클라이언트에서 오는 익명 쿼리를 위해 LDAP 디렉터리 서버를 여는 대신 쿼리를 인증하고 수행하기 위한 목적으로만 하나의 "user(사용자)"를 구성할 수 있습니다.

단계의 요약이 여기 포함되었으며, 다음과 같은 내용입니다.

- "anonymous(익명)" 인증을 허용하도록 Microsoft Exchange 2000 서버를 설정하는 방법.
- "anonymous bind(익명 바인드)"를 허용하도록 Microsoft Exchange 2000 서버를 설정하는 방법.

- "anonymous bind(익명 바인드)"와 "anonymous(익명)"를 모두 사용하여 Microsoft Exchange 2000 서버에서 LDAP 데이터를 검색하도록 AsyncOS를 설정하는 방법.

사용자 이메일 주소를 쿼리하기 위해 "anonymous(익명)" 또는 "anonymous bind(익명 바인드)" 인증을 허용하려면 Microsoft Exchange 2000 서버에 대해 특정 권한을 설정해야 합니다. 이 방법은 SMTP 게이트웨이에 대한 수신 이메일 메시지의 유효성을 확인하기 위해 LDAP 쿼리를 사용할 때 매우 유용할 수 있습니다.

관련 주제

- 익명 인증 설정, 748 페이지
- Active Directory에 대한 익명 바인드 설정, 749 페이지
- Active Directory 구현 참고 사항, 750 페이지

익명 인증 설정

다음 설정 지침을 따르면 특정 데이터를 Microsoft Windows Active Directory에서 Active Directory 및 Exchange 2000 서버의 인증되지 않은 쿼리에 사용하도록 지정할 수 있습니다. Active Directory에 "익명 바인드"를 허용하려면 Active Directory에 대한 익명 바인드 설정, 749 페이지 섹션을 참조하십시오.

단계 **1** 필수 Active Directory 권한을 결정합니다.

ADSI Edit 스냅인 또는 LDP 유틸리티를 사용하여 다음 Active Directory 개체의 특성에 대한 권한을 수정해야 합니다.

- 쿼리하려는 도메인에 대한 도메인 명명 컨텍스트의 루트
- 이메일 정보를 쿼리할 사용자를 포함하는 모든 OU 및 CN 개체.

다음 표는 필요한 모든 컨테이너에 적용할 필수 권한을 보여줍니다.

사용자 개체	권한	**Inheritance**	권한 유형
모든 사람	콘텐츠 나열	컨테이너 개체	객체
모든 사람	콘텐츠 나열	OU(Organizational Unit) 개체	객체
모든 사람	공개 정보 읽기	사용자 개체	속성
모든 사람	전화 및 메일 옵션 읽기	사용자 개체	속성

단계 **2** Active Directory 권한 설정

- Windows 2000 Support Tools에서 ADSIEdit를 엽니다.
- **Domain Naming Context(**도메인 명명 컨텍스트**)** 폴더를 찾습니다. 이 폴더에는 도메인의 LDAP 경로가 있습니다.
- **Domain Naming Context(**도메인 명명 컨텍스트**)** 폴더를 마우스 오른쪽 버튼으로 클릭하고 **Properties(**속성**)**를 클릭합니다.
- **Security(**보안**)**를 클릭합니다.
- **Advanced(**고급**)**를 클릭합니다.

- **Add(**추가**)**를 클릭합니다.
- **User Object(**사용자 개체**)** Everyone을 클릭하고 **OK(**확인**)**를 클릭합니다.
- **Permission Type(**권한 유형**)** 탭을 클릭합니다.
- **Apply onto(**적용 대상**)** 상자에서 **Inheritance(**상속**)**를 클릭합니다.
- **Permission(**권한**)**에 대해 Allow(허용) 확인란을 클릭하여 선택합니다.

단계 **3** Cisco Messaging Gateway 구성

CLI(Command Line Interface)에서 **`ldapconfig`**를 사용하여 다음 정보로 LDAP 서버 항목을 만듭니다.

- Active Directory 또는 Exchange 서버의 호스트 이름
- 포트 3268
- 도메인의 루트 명명 컨텍스트와 일치하는 기본 DN
- 인증 유형 익명

Active Directory에 대한 익명 바인드 설정

다음 설정 지침을 따르면 특정 데이터를 Microsoft Windows Active Directory에서 Active Directory 및 Exchange 2000 서버의 익명 바인드 쿼리에 사용하도록 지정할 수 있습니다. Active Directory 서버의 익명 바인드는 비어 있는 암호와 함께 사용자 이름 anonymous를 전송합니다.

참고 익명 바인드 시도 중에 Active Directory 서버로 암호가 전송되면 인증이 실패할 수 있습니다.

단계 **1** 필수 Active Directory 권한을 결정합니다.

ADSI Edit 스냅인 또는 LDP 유틸리티를 사용하여 다음 Active Directory 개체의 특성에 대한 권한을 수정해야 합니다.

- 쿼리하려는 도메인에 대한 도메인 명명 컨텍스트의 루트
- 이메일 정보를 쿼리할 사용자를 포함하는 모든 OU 및 CN 개체.

다음 표는 필요한 모든 컨테이너에 적용할 필수 권한을 보여줍니다.

사용자 개체	권한	**Inheritance**	권한유형
ANONYMOUS LOGON	콘텐츠 나열	컨테이너 개체	객체
ANONYMOUS LOGON	콘텐츠 나열	OU(Organizational Unit) 개체	객체
ANONYMOUS LOGON	공개 정보 읽기	사용자 개체	속성
ANONYMOUS LOGON	전화 및 메일 옵션 읽기	사용자 개체	속성

단계 **2** Active Directory 권한 설정

- Windows 2000 Support Tools에서 ADSIEdit를 엽니다.
- **Domain Naming Context(**도메인 명명 컨텍스트**)** 폴더를 찾습니다. 이 폴더에는 도메인의 LDAP 경로가 있습니다.
- **Domain Naming Context(**도메인 명명 컨텍스트**)** 폴더를 마우스 오른쪽 버튼으로 클릭하고 **Properties(**속성**)**를 클릭합니다.
- **Security(**보안**)**를 클릭합니다.
- **Advanced(**고급**)**를 클릭합니다.
- **Add(**추가**)**를 클릭합니다.
- **User Object(**사용자 개체**)** ANONYMOUS LOGON을 클릭하고 **OK(**확인**)**를 클릭합니다.
- **Permission Type(**권한 유형**)** 탭을 클릭합니다.
- **Apply onto(**적용 대상**)** 상자에서 **Inheritance(**상속**)**를 클릭합니다.
- **Permission(**권한**)**에 대해 **Allow(**허용**)** 확인란을 클릭하여 선택합니다.

단계 **3** Cisco Messaging Gateway 구성

System Administration(시스템 관리**) > LDAP** 페이지(또는 CLI의 **`ldapconfig`**)를 사용하여 다음 정보로 LDAP 서버 항목을 만듭니다.

- Active Directory 또는 Exchange 서버의 호스트 이름
- 포트 3268
- 도메인의 루트 명명 컨텍스트와 일치하는 기본 DN
- 비어 있는 암호의 사용자로서 cn=anonymous를 사용하는 인증 유형 암호

Active Directory 구현 참고 사항

- Active Directory 서버는 포트 3268 및 389에서 LDAP 연결을 수락합니다. 전역 카탈로그에 액세스하기 위한 기본 포트는 3268입니다.
- Active Directory 서버는 포트 636 및 3269에서 LDAPS 연결을 수락합니다. Microsoft는 Windows Server 2003 이상에서 LDAPS를 지원합니다.
- 어플라이언스는 동일한 서버를 사용하여 서로 다른 기본(base)에 대한 쿼리를 수행할 수 있도록, 역시 전역 카탈로그인 도메인 컨트롤러에 연결해야 합니다.
- 쿼리에 성공하려면 Active Directory 내에서 그룹 "Everyone"의 디렉터리 개체에 대한 읽기 권한을 허용해야 할 수 있습니다. 여기에는 도메인 명명 컨텍스트의 루트가 포함됩니다.
- 일반적으로 많은 Active Directory 구현에서 mail 특성 항목의 값에는 일치하는 값 "ProxyAddresses" 특성 항목이 있습니다.
- 인프라 내에서 서로 인식하는 Microsoft Exchange 환경은 일반적으로 원래 MTA로 돌아오는 경로가 없어도 서로 메일을 라우팅할 수 있습니다.

LDAP 쿼리 테스트

구성한 LDAP 서버에 대한 쿼리를 테스트하려면 각 쿼리 유형의 Add/Edit LDAP Server Profile(LDAP 서버 프로필 추가/수정) 페이지에 있는 Test Query(쿼리 테스트) 버튼(또는 CLI의 `test` 하위 명령)을

사용합니다. AsyncOS는 결과는 물론 쿼리 연결 테스트의 각 단계에 대한 세부사항도 표시합니다. 각 쿼리 유형을 테스트할 수 있습니다.

`ldaptest` 명령을 일괄 명령으로 사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
ldaptest LDAP.ldapaccept foo@ironport.com
```

LDAP 서버 특성의 Host Name(호스트 이름) 필드에 여러 호스트를 입력한 경우, 어플라이언스는 각 LDAP 서버에서 쿼리를 테스트합니다.

표 ***64: LDAP*** 쿼리 테스트

쿼리 유형	수신자가 일치하는 경우**(PASS)...**	수신자가 일치하지 않는 경우**(FAIL)...**
수신자 수락(Accept, `ldapaccept`)	메시지를 수락합니다.	잘못된 수신자: 대화 또는 지연된 반송 또는 리스너 설정 단위로 메시지 삭제. DHAP: Drop.
라우팅 (Routing, `ldaprouting`)	쿼리 설정을 기반으로 라우팅합니다.	메시지를 계속 처리합니다.
가장(Masquerade, `masquerade`)	쿼리에 의해 정의된 변수 매핑으로 헤더를 변경합니다.	메시지를 계속 처리합니다.
그룹 멤버십(Group, `ldapgroup`)	메시지 필터 규칙에 대해 true"를 반환합니다.	메시지 필터 규칙에 대해 false"를 반환합니다.
SMTP 인증 (SMTP Authentication, `smtpauth`)	암호가 LDAP 서버에서 반환되고 인증에 사용됩니다. SMTP 인증이 발생합니다.	일치하는 암호 없음이 발생할 수 있습니다. SMTP 인증 시도가 실패합니다.
외부 인증(`externalauth`)	바인드, 사용자 레코드 및 사용자의 그룹 멤버십에 대해 개별적으로 "match positive"를 반환합니다.	바인드, 사용자 레코드 및 사용자의 그룹 멤버십에 대해 개별적으로 "match negative"를 반환합니다.
스팸 격리 엔드 유저 인증 (`isqauth`)	최종 사용자 계정에 대해 "match positive"를 반환합니다.	일치하는 암호 없음이 발생할 수 있습니다. 엔드 유저 인증 시도가 실패합니다.
스팸 격리 별칭 통합 (`isqalias`)	통합된 스팸 알림이 전송될 이메일 주소를 반환합니다.	스팸 알림 통합 없음이 발생할 수 있습니다.

참고 쿼리에 대해 입력하는 변수는 대/소문자를 구분하며, 제대로 작동하려면 LDAP 구현과 일치해야 합니다. 예를 들어 프롬프트에서 **`mailLocalAddress`**를 입력하면 **`maillocaladdress`**를 입력하는 경우와 다른 쿼리를 수행합니다. Systems에서는 ldapconfig 명령의 test 하위 명령을 사용하여, 작성한 모든 쿼리를 테스트하고 적절한 결과가 반환되는지 확인할 것을 적극 권장합니다.

LDAP 서버에 대한 연결 문제 해결

어플라이언스에서 LDAP 서버에 도달할 수 없는 경우 다음 오류 중 하나가 표시됩니다.

- `Error: LDAP authentication failed: <LDAP Error "invalidCredentials" [0x31]>`
- `Error: Server unreachable: unable to connect`
- `Error: Server unreachable: DNS lookup failure`

서버 구성에 잘못된 포트가 입력되었거나 방화벽에서 포트가 열리지 않아 서버에 도달하지 못할 수 있습니다. LDAP 서버는 일반적으로 포트 3268 또는 389를 통해 통신합니다. Active Directory는 다중 서버 환경에서 사용되는 전역 카탈로그에 액세스하기 위해 포트 3268을 사용합니다(자세한 내용은 "방화벽 정보" 부록 참조). AsyncOS 4.0에서는 SSL을 통해 LDAP 서버와 통신하는 기능(일반적으로 포트 636에서)이 추가되었습니다. 자세한 내용은 보안 LDAP(SSL), 747 페이지를 참고하십시오.

입력한 호스트 이름을 확인할 수 없으므로 서버에 도달하지 못할 수도 있습니다.

LDAP 서버에 대한 연결을 테스트하려면 Add/Edit LDAP Server Profile(LDAP 서버 프로필 추가/수정) 페이지에 있는 Test Server(s)(서버 테스트)(또는 CLI에서 `ldapconfig` 명령의 `test` 하위 명령)를 사용할 수 있습니다. 자세한 내용은 LDAP 서버 테스트, 740 페이지를 참고하십시오.

LDAP 서버에 도달할 수 없다면:

- 작업 대기열에 LDAP Accept(수락), Masquerading(가장) 또는 Routing(라우팅)이 활성화되어 있으면 메일이 작업 대기열 내에 남아 있게 됩니다.
- LDAP Accept(수락)가 활성화되지 않았지만 다른 쿼리(그룹 정책 확인 등)가 필터에서 사용되는 경우, 필터가 false로 평가됩니다.

수신자 검증을 위해 수락 쿼리 사용

기존의 LDAP 인프라를 사용하여 수신 메시지의 수신자 이메일 주소(퍼블릭 리스너에서)를 처리하는 방법을 정의할 수 있습니다. 디렉터리에서 사용자 데이터를 변경하면 어플라이언스가 다음에 디렉터리 서버를 쿼리할 때 업데이트됩니다. 캐시의 크기 및 어플라이언스가 검색하는 데이터를 저장할 시간을 지정할 수 있습니다.

참고 특별한 수신자(예: administrator@example.com)에 대해서는 LDAP 수락 쿼리를 우회할 수 있습니다. RAT(Recipient Access Table)에서 이 설정을 구성할 수 있습니다. 이 설정 구성에 대한 자세한 내용은 "이메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

관련 주제

- 샘플 수락 쿼리, 753 페이지
- Lotus Notes용 수락 쿼리 구성, 753 페이지

샘플 수락 쿼리

다음 표는 샘플 수락 쿼리를 보여줍니다.

표 ***65:*** 일반 ***LDAP*** 구현을 위한 ***LDAP*** 쿼리 문자열 예***:*** 수락

쿼리 내용**:**	수신자 검증

OpenLDAP	`(mailLocalAddress={a})`
	`(mail={a})`
	`(mailAlternateAddress={a})`

Microsoft Active Directory Address Book **Microsoft Exchange**	`(|(mail={a})(proxyAddresses=smtp:{a}))`

SunONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

Lotus NotesLotus Domino	`(|(|(mail={a})(uid={u}))(cn={u}))` `(|(ShortName={u})(InternetAddress={a})(FullName={u}))`

사용자 이름을 검증할 수도 있습니다(Left Hand Side). 이는 디렉터리에 메일을 수락할 도메인이 일부 포함되지 않은 경우 유용합니다. Accept(수락) 쿼리를 (uid={u})로 설정합니다.

Lotus Notes용 수락 쿼리 구성

LDAPACCEPT 및 Lotus Notes는 복잡할 수 있습니다. Notes LDAP에 다음과 같은 특성의 사용자가 포함된 경우

```
mail=juser@example.com

cn=Joe User

uid=juser

cn=123456

location=New Jersey
```

Lotus는 LDAP 디렉터리에 없는 "Joe_User@example.com"과 같이, 지정된 것 이외에 다양한 양식의 이메일 주소에 대해 해당 사용자의 이메일을 수락합니다. 따라서 AsyncOS는 해당 사용자에 대한 일부 유효한 사용자 이메일 주소를 찾지 못할 수 있습니다.

가능한 해결책 중 하나는 다른 주소 양식을 게시해보는 것입니다. 자세한 내용은 Lotus Notes 관리자에게 문의하십시오.

라우팅 쿼리를 사용하여 여러 대상 주소에 메일 전송

AsyncOS는 별칭 확장을 지원합니다(여러 대상 주소가 있는 LDAP 라우팅). AsyncOS는 원래 이메일 메시지를 각 별칭 대상에 대한 별도의 새 메시지와 교체합니다(예: recipient@yoursite.com을 newrecipient1@hotmail.com 및 recipient2@internal.yourcompany.com 등에 대한 별도의 새 메시지와 교체). 다른 메일 처리 시스템에서는 라우팅 쿼리가 별칭 쿼리로 알려진 경우도 있습니다.

관련 주제

- 샘플 라우팅 쿼리, 754 페이지

샘플 라우팅 쿼리

표 ***66:*** 일반 ***LDAP*** 구현을 위한 ***LDAP*** 쿼리 문자열 예***:*** 라우팅

쿼리 내용:	또 다른 메일 호스트로 라우팅
OpenLDAP	`(mailLocalAddress={a})`
Microsoft Active Directory Address Book **Microsoft Exchange**	해당되지 않을 수 있음

SunONE Directory Server	`(mail={a})`
	`(mailForwardingAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailRoutingAddress={a})`
	`(otherMailbox={a})`
	`(rfc822Mailbox={a})`

Active Directory 구현은 `proxyAddresses` 특성에 대해 여러 항목을 가지고 있을 수 있지만 AD는 이 특성 값을 `smtp:user@domain.com`으로 지정하며, LDAP 라우팅/별칭 확장에 해당 데이터를 사용할 수 없습니다. 각 대상 주소는 별도의 `attribute:value` 쌍을 이루어야 합니다. 인프라 내에서 서로 인식하는 Microsoft Exchange 환경은 일반적으로 원래 MTA로 돌아오는 경로가 없어도 서로 메일을 라우팅할 수 있습니다.

관련 주제

- 라우팅: MAILHOST 및 MAILROUTINGADDRESS, 755 페이지

라우팅: MAILHOST 및 MAILROUTINGADDRESS

Routing(라우팅) 쿼리의 경우 MAILHOST의 값은 IP 주소일 수 없으며, 확인 가능한 호스트 이름이어야 합니다. 일반적으로 내부 DNSconfig의 사용이 필요합니다.

MAILHOST는 라우팅 쿼리에서 선택 사항입니다. MAILHOST가 설정되지 않은 경우 MAILROUTINGADDRESS는 필수 사항입니다.

가장 쿼리를 사용하여 봉투 발신자 재작성

Masquerading(가장)은 작성한 쿼리를 기반으로 이메일에서 Envelope Sender(봉투 발신자)(발신자 또는 MAIL FROM이라고도 함)와 To:, From:, 및/또는 CC: 헤더를 재작성합니다. 이 기능의 일반적인 구현 예는 단일 사이트에서 여러 도메인을 호스팅할 수 있는 "가상 도메인"입니다. 또 다른 일반적인 구현은 이메일 헤더의 문자열에서 하위 도메인을 "제거"하여 네트워크 인프라를 "숨기는 것"입니다.

관련 주제

- 샘플 가장 쿼리 , 755 페이지
- "친숙한 이름" 가장, 755 페이지

샘플 가장 쿼리

표 *67:* 일반 ***LDAP*** 구현을 위한 ***LDAP*** 쿼리 문자열 예*:* 가장

쿼리 내용:	**Masquerade**
OpenLDAP	`(mailRoutingAddress={a})`
Microsoft Active Directory Address Book	`(proxyaddresses=smtp:{a})`

SunONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

"친숙한 이름" 가장

일부 사용자 환경에서 LDAP 디렉터리 서버 스키마는 메일 라우팅 주소 또는 로컬 메일 주소 외에 "친숙한 이름"도 저장할 수 있습니다. 유효한 이메일 주소에서 일반적으로 허용되지 않는 특수 문자(예: 인용부호, 공백 및 쉼표)가 친숙한 주소에 포함된 경우에도, AsyncOS에서는 봉투 발신자(발신 메일용) 및 메시지 헤더(To:, Reply To:, From:, CC: 등 수신 메일용)를 "친숙한 이름"으로 가장할 수 있습니다.

LDAP 쿼리를 통해 헤더의 가장을 사용할 때 이제 친숙한 이메일 문자열 전체를 LDAP 서버의 결과로 교체할지 여부를 구성하는 옵션이 제공됩니다. 이 동작이 활성화되었어도 봉투 발신자에 대해서는 user@domain 부분만 사용됩니다(친숙한 이름은 금지됨).

일반 LDAP 가장과 마찬가지로, LDAP 쿼리에서 빈 결과(0 길이 또는 전체 공백)가 반환되면 가장이 발생하지 않습니다.

이 기능을 활성화하려면 리스너에 대해 LDAP 기반 가장 쿼리를 구성할 때(LDAP 페이지 또는 `ldapconfig` 명령) 다음 질문에 "y"로 대답합니다.

```
Do you want the results of the returned attribute to replace the entire
friendly portion of the original recipient? [N]
```

예를 들면 다음 LDAP 항목의 예를 생각해볼 수 있습니다.

특성	값
mailRoutingAddress	admin\@example.com
mailLocalAddress	joe.smith\@example.com
mailFriendlyAddress	“Administrator for example.com,” <joe.smith\@example.com>

이 기능이 활성화되면 (mailRoutingAddress={a})의 LDAP 쿼리 및 (mailLocalAddress)의 가장 특성은 다음으로 대체됩니다.

원래 주소**(From, To, CC, Reply-to)**	가장된 헤더	가장된 봉투 발신자
admin@example.com	From: “Administrator for example.com,” <joe.smith@example.com>	MAIL FROM: <joe.smith@example.com>

그룹 LDAP 쿼리를 사용하여 수신자가 그룹 구성원인지 확인

수신자가 LDAP 디렉터리에 정의된 그룹의 구성원인지 확인하기 위해 LDAP 서버에 대한 쿼리를 정의할 수 있습니다.

단계 **1** 메시지에 대해 작동하는 rcpt-to-group 또는 mail-from-group 규칙을 사용하는 메시지 필터를 만듭니다.

단계 **2** 그런 다음 **System Administration(**시스템 관리**) > LDAP** 페이지(또는 **`ldapconfig`** 명령)를 사용하여, 그룹 멤버십에 대한 쿼리를 바인딩 및 구성할 수 있도록 어플라이언스에 대한 LDAP 서버를 정의합니다.

단계 **3** **Network(**네트워크**) > Listeners(**리스너**)** 페이지(또는 **`listenerconfig -> edit -> ldapgroup`** 하위 명령)를 사용하여 리스너에 대한 그룹 쿼리를 활성화합니다.

다음에 수행할 작업

관련 주제

- 샘플 그룹 쿼리 , 757 페이지
- 그룹 조회 구성, 757 페이지

샘플 그룹 쿼리

표 ***68:*** 일반 ***LDAP*** 구현을 위한 ***LDAP*** 쿼리 문자열 예***:*** 그룹

쿼리 내용:	그룹
OpenLDAP	OpenLDAP는 기본적으로 memberOf 특성을 지원하지 않습니다. LDAP 관리자는 이 특성 또는 유사한 특성을 스키마에 추가할 수 있습니다.
Microsoft Active Directory	`(&(memberOf={g})(proxyAddresses=smtp:{a}))`
SunONE Directory Server	`(&(memberOf={g})(mailLocalAddress={a}))`

예를 들면 LDAP 디렉터리에서 "Marketing" 그룹의 구성원을 ou=Marketing으로 분류한다고 가정해보겠습니다. 이 그룹 구성원이 주고받는 메시지를 특별한 방법으로 다루기 위해 이 분류를 사용할 수 있습니다. 1단계는 메시지에 대해 작동할 메시지 필터를 만드는 것이고, 2단계와 3단계는 LDAP 조회 메커니즘을 활성화하는 것입니다.

그룹 조회 구성

다음 예에서 Marketing 그룹(LDAP 그룹 "Marketing"에 의해 정의됨) 멤버의 메일은 대체 전달 호스트 `marketingfolks.example.com`으로 전달됩니다.

단계 **1** 먼저 그룹 멤버십과 긍정적으로 일치하는 메시지에 대해 작동하도록 메시지 필터를 만듭니다. 이 예에서는 `mail-from-group` 규칙을 사용하는 필터가 생성됩니다. 봉투 발신자가 LDAP 그룹 "marketing-group1"에 있는 것으로 확인되는 모든 메시지는 대체 전달 호스트(필터 `alt-mailhost` 작업)와 함께 전달됩니다.

그룹 멤버십 필드 변수(groupName)는 2단계에서 정의합니다. 그룹 특성 "groupName"은 `marketing-group1` 값으로 정의됩니다.

```
mail3.example.com> filters


Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.
```

```
MarketingGroupfilter:

if (mail-from-group == "marketing-group1") {

alt-mailhost ('marketingfolks.example.com');}

.

1 filters added.

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>
```

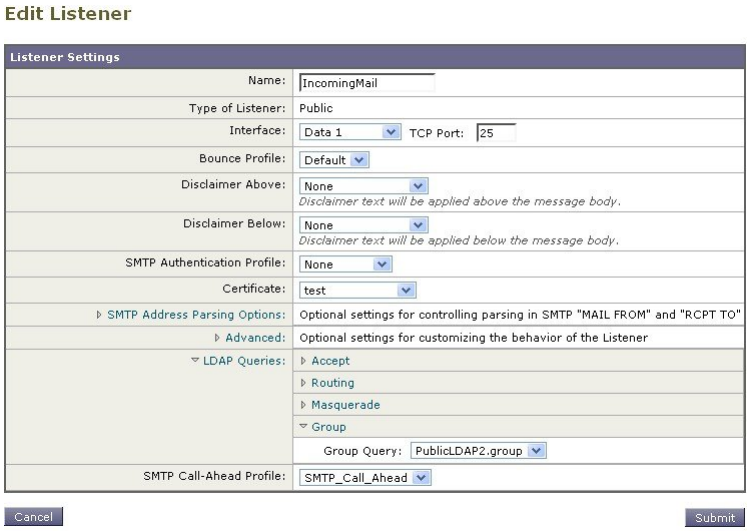
`mail-from-group` 및 `rcpt-to-group` 메시지 필터 규칙에 대한 자세한 내용은 메시지 필터 규칙, 138 페이지 섹션을 참조하십시오.

단계 **2** Add LDAP Server Profile(LDAP 서버 프로필 추가) 페이지를 사용하여 바인딩할 어플라이언스의 LDAP 서버를 정의하고, 그룹 멤버십에 대한 초기 쿼리를 구성합니다.

단계 **3** 퍼블릭 리스너 "InboundMail"이 그룹 라우팅에 LDAP 쿼리를 사용하도록 업데이트됩니다. 위에서 지정한 LDAP 쿼리를 활성화하는 데 Edit Listener(리스너 수정) 페이지가 사용됩니다.

이 쿼리의 결과, 리스너에서 수락한 메시지가 LDAP 서버에 대한 쿼리를 트리거하여 그룹 멤버십을 결정합니다. 앞에서 **System Administration(**시스템 관리**) > LDAP** 페이지를 통해 PublicLDAP2.group 쿼리를 정의했습니다.

그림 *64:* 리스너에서 그룹 쿼리 지정



단계 **4** 변경 사항을 제출 및 커밋합니다.

예: 그룹 쿼리를 사용하여 스팸 및 바이러스 검사 건너뛰기

메시지 필터는 파이프라인에서 일찍 발생하므로 지정된 그룹에 대해 바이러스 및 스팸 검사를 건너뛰려면 그룹 쿼리를 사용할 수 있습니다. 예를 들면 IT 그룹에서 모든 메시지를 수신하고 스팸 및 바이러스 검사를 건너뛰도록 할 수 있습니다. LDAP 레코드에서 DN을 그룹 이름으로 사용하는 그룹 항목을 만듭니다. 그룹 이름은 다음 DN 항목으로 구성됩니다.

cn=IT, ou=groups, o=sample.com

다음 그룹 쿼리로 LDAP 서버 프로필을 만듭니다.

(&(memberOf={g})(proxyAddresses=smtp:{a}))

그런 다음, 리스너에서 메시지를 수신할 때 그룹 쿼리가 트리거되도록 리스너에서 이 쿼리를 활성화합니다.

IT 그룹 구성원에 대해 바이러스 및 스팸 필터링을 건너뛰려면 LDAP 그룹에 대해 수신 메시지를 확인하도록 다음 메시지 필터를 만듭니다.

```
[]> - NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

IT_Group_Filter:

if (rcpt-to-group == "cn=IT, ou=groups, o=sample.com"){

skip-spamcheck();
```

```
skip-viruscheck();

deliver();

}

.
1 filters added.
```

참고 이 메시지 필터의 rcpt-to-group은 그룹 이름으로 입력된 DN을 반영합니다(cn=IT, ou=groups, o=sample.com). 필터가 LDAP 디렉터리에 있는 이름과 일치하는지 확인하려면 메시지 필터에서 올바른 그룹 이름을 사용해야 합니다.

리스너에서 수락한 메시지가 LDAP 서버에 대한 쿼리를 트리거하여 그룹 멤버십을 결정합니다. 메시지 수신자가 IT 그룹의 구성원이면 메시지 필터는 바이러스 및 스팸 검사를 건너뛰고 메시지를 수신자에게 전달합니다. 필터가 LDAP 쿼리 결과를 검사하도록 하려면 LDAP 서버에 LDAP 쿼리를 만들고 리스너에서 LDAP 쿼리를 활성화해야 합니다.

도메인 기반 쿼리를 사용하여 특정 도메인으로 라우팅

도메인 기반 쿼리는 유형별로 그룹화되고, 도메인과 연결되며, 특정 리스너에 할당되는 LDAP 쿼리입니다. 서로 다른 도메인과 연결된 서로 다른 LDAP 서버가 있지만 동일한 리스너의 모든 LDAP 서버에 대해 쿼리를 실행하려는 경우 도메인 기반 쿼리를 사용할 수 있습니다. 예를 들어 "MyCompany" 회사가 "HisCompany" 회사 및 "HerCompany" 회사를 매입한다고 가정하겠습니다. MyCompany는 MyCompany.example.com이라는 자체 도메인은 물론 HisCompany.example.com 및 HerCompany.example.com에 대한 도메인도 유지 관리하며, 각 도메인과 관련된 직원에 대해 서로 다른 LDAP 서버를 운영합니다. 이 세 도메인에 대한 메일을 모두 수락하기 위해 MyCompany는 도메인 기반 쿼리를 만듭니다. 이를 통해 MyCompany.example.com은 동일한 리스너에서 Mycompany.example.com, HisCompany.example.com 및 HerCompany.example.com에 대한 이메일을 수락합니다.

단계 **1** 도메인 기반 쿼리에서 사용할 각 도메인에 대한 서버 프로필을 만듭니다. 각 서버 프로필에 대해 도메인 기반 쿼리에 사용할 쿼리를 구성합니다(수락, 라우팅 등). 자세한 내용은 LDAP 서버에 대한 정보를 저장할 LDAP 서버 프로필 만들기, 739 페이지을 참고하십시오.

단계 **2** 도메인 기반 쿼리를 만듭니다. 도메인 기반 쿼리를 만들 때에는 각 서버 프로필에서 쿼리를 선택하고, 어플라이언스가 Envelope To 필드에서 도메인을 기반으로 실행할 쿼리를 결정하도록 합니다. 쿼리 만들기에 대한 자세한 내용은 도메인 기반 쿼리 만들기, 761 페이지 섹션을 참조하십시오.

단계 **3** 퍼블릭 또는 프라이빗 리스너에서 도메인 기반 쿼리를 활성화합니다. 리스너 구성에 대한 자세한 내용은 "이메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

참고 LDAP 최종 사용자 액세스에 대해 도메인 기반 쿼리를 활성화하거나 스팸 격리에 대해 스팸 알림을 활성화할 수 있습니다. 자세한 내용은 스팸 격리 장을 참조하십시오.

다음에 수행할 작업

관련 주제

- 도메인 기반 쿼리 만들기, 761 페이지

도메인 기반 쿼리 만들기

System Administration(시스템 관리) > LDAP > LDAP Server Profiles(LDAP 서버 프로필) 페이지에서 도메인 기반 쿼리를 만듭니다.

단계 **1** LDAP Server Profiles(LDAP 서버 프로필) 페이지에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Add Domain Assignments(**도메인 할당 추가**)**를 클릭합니다.

단계 **3** 도메인 기반 쿼리의 이름을 입력합니다.

단계 **4** 쿼리 유형을 선택합니다.

참고 도메인 기반 쿼리를 만들면 서로 다른 여러 쿼리 유형을 선택할 수 없습니다. 쿼리 유형을 선택하면 어플라이언스는 사용 가능한 서버 프로필에서 해당 유형의 쿼리로 쿼리 필드를 채웁니다.

단계 **5** Domain Assignments(도메인 할당) 필드에 도메인을 입력합니다.

단계 **6** 도메인과 관련된 쿼리를 선택합니다.

단계 **7** 쿼리에 모든 도메인을 추가할 때까지 행을 계속 추가합니다.

단계 **8** 다른 모든 쿼리가 실패할 경우 실행할 기본 쿼리를 입력할 수 있습니다. 기본 쿼리를 입력하지 않으려면 **None(**없음**)**을 선택합니다.

단계 **9** Test Query(쿼리 테스트) 버튼을 클릭하고 Test Parameters(테스트 매개변수) 필드에 테스트할 사용자 로그인과 암호 또는 이메일 주소를 입력하여 쿼리를 테스트합니다. Connection Status(연결 상태) 필드에 결과가 나타납니다.

단계 **10** 선택적으로, 수락 쿼리에 {f} 토큰을 사용하는 경우 쿼리 테스트에 봉투 발신자 주소를 추가할 수 있습니다.

참고 도메인 기반 쿼리를 만들면 이를 퍼블릭 또는 프라이빗 리스너와 연결해야 합니다.

단계 **11** 변경 사항을 제출 및 커밋합니다.

체인 쿼리를 사용하여 일련의 **LDAP** 쿼리 수행

체인 쿼리는 어플라이언스가 연속해서 실행할 수 있는 일련의 LDAP 쿼리입니다. 어플라이언스는 LDAP 서버가 긍정적인 응답을 반환할 때까지(또는 "체인"의 최종 쿼리가 부정적인 응답을 반환하거나 실패할 때까지) "체인"의 각 쿼리를 실행하려고 시도합니다. 체인 라우팅 쿼리의 경우, 어플라이언스에서 재작성된 각 이메일 주소에 대해 구성된 동일한 체인 쿼리를 순서대로 다시 실행합니다. 체인 쿼리는 LDAP 디렉터리의 항목이 서로 다른 특성을 사용하여 유사한(또는 같은) 값을 저장하는 경우

유용할 수 있습니다. 예를 들면 사용자 이메일 주소를 저장하는 데 maillocaladdress 및 mail 특성을 사용했을 수 있습니다. 이 두 가지 특성에 대해 쿼리가 실행되도록 하려면 체인 쿼리를 사용할 수 있습니다.

단계 **1** 체인 쿼리에서 사용할 각 쿼리에 대한 서버 프로필을 만듭니다. 각 서버 프로필에 대해 체인 쿼리에 사용할 쿼리를 구성합니다. 자세한 내용은 LDAP 서버에 대한 정보를 저장할 LDAP 서버 프로필 만들기, 739 페이지을 참고하십시오.

단계 **2** 체인 쿼리를 만듭니다. 자세한 내용은 체인 쿼리 만들기, 762 페이지를 참고하십시오.

단계 **3** 퍼블릭 또는 프라이빗 리스너에서 체인 쿼리를 활성화합니다. 리스너 구성에 대한 자세한 내용은 "이메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

참고 LDAP 최종 사용자 액세스에 대해 도메인 기반 쿼리를 활성화하거나 스팸 격리에 대해 스팸 알림을 활성화할 수 있습니다. 자세한 내용은 스팸 격리 장을 참조하십시오.

다음에 수행할 작업

관련 주제

- 체인 쿼리 만들기, 762 페이지

체인 쿼리 만들기

System Administration(시스템 관리) > LDAP > LDAP Server Profiles(LDAP 서버 프로필) 페이지에서 체인 쿼리를 만듭니다.

단계 **1** LDAP Server Profiles(LDAP 서버 프로필) 페이지에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Add Chain Query(**체인 쿼리 추가**)**를 클릭합니다.

단계 **3** 체인 쿼리의 이름을 추가합니다.

단계 **4** 쿼리 유형을 선택합니다.

체인 쿼리를 만들면 서로 다른 여러 쿼리 유형을 선택할 수 없습니다. 쿼리 유형을 선택하면 어플라이언스는 사용 가능한 서버 프로필에서 해당 유형의 쿼리로 쿼리 필드를 채웁니다.

단계 **5** 체인 쿼리에 추가할 쿼리를 선택합니다.

구성한 순서대로 어플라이언스에서 쿼리가 실행됩니다. 따라서 체인 쿼리에 여러 쿼리를 추가하는 경우 좀 더 일반적인 쿼리 뒤에 좀 더 구체적인 쿼리가 오도록 쿼리 순서를 정할 수 있습니다.

단계 **6** Test Query(쿼리 테스트) 버튼을 클릭하고 Test Parameters(테스트 매개변수) 필드에 테스트할 사용자 로그인과 암호 또는 이메일 주소를 입력하여 쿼리를 테스트합니다. Connection Status(연결 상태) 필드에 결과가 나타납니다.

단계 **7** 선택적으로, 수락 쿼리에 {f} 토큰을 사용하는 경우 쿼리 테스트에 봉투 발신자 주소를 추가할 수 있습니다.

참고 체인 쿼리를 만들면 이를 퍼블릭 또는 프라이빗 리스너와 연결해야 합니다.

단계 **8** 변경 사항을 제출 및 커밋합니다.

디렉터리 수집 공격 방지에 LDAP 사용

악의적인 발신자가 일반적인 이름으로 수신자에게 메시지를 전송하려고 시도하고, 이메일 게이트웨이는 수신자가 해당 위치에 유효한 사서함 가지고 있음을 확인하여 응답할 때 디렉터리 수집 공격이 발생합니다. 대규모로 수행할 경우 악의적인 발신자는 스패밍을 위해 이런 유효한 주소를 "수집"함으로써 메일을 전송할 대상을 결정합니다.

Email Security Appliance는 LDAP 수집 검증 쿼리를 사용하여 DHA(Directory Harvest Attack)를 탐지 및 방지할 수 있습니다. SMTP 대화 내에서 또는 작업 대기열 내에서 디렉터리 수집 공격을 방지하도록 LDAP 수락을 구성할 수 있습니다.

관련 주제

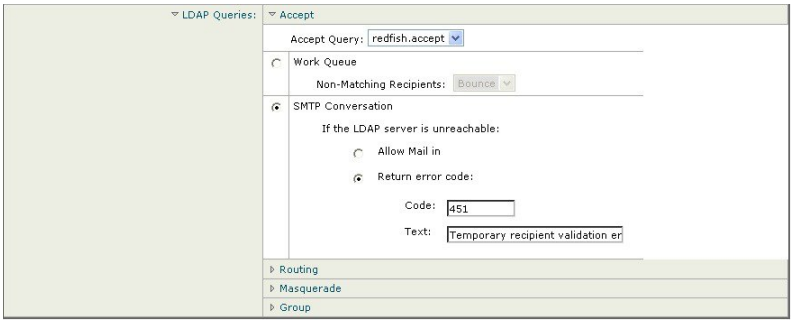
- SMTP 대화 내에서 디렉터리 수집 공격 방지, 763 페이지
- 작업 대기열 내에서 디렉터리 수집 공격 방지, 764 페이지

SMTP 대화 내에서 디렉터리 수집 공격 방지

RAT(Recipient Access Table)에 도메인만 입력하고 SMTP 대화에서 LDAP 수락 검증을 수행함으로써 DHA를 방지할 수 있습니다.

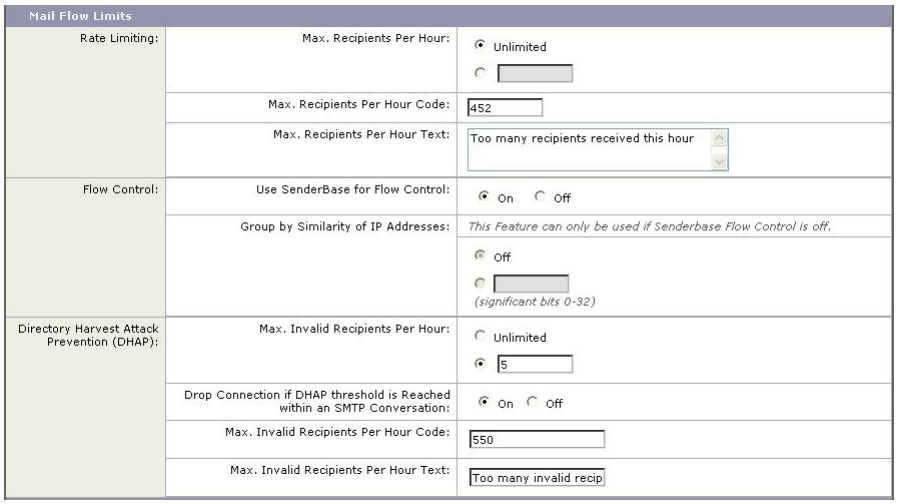
SMTP 대화 중 메시지를 삭제하려면 LDAP 수락용 LDAP 서버 프로필을 구성합니다. 그런 다음 SMTP 대화 중에 LDAP 수락 쿼리를 수행하도록 리스너를 구성합니다.

그림 ***65: SMTP*** 대화에서 수락 쿼리 구성



리스너에 대해 LDAP 수락 쿼리를 구성했으면 리스너와 관련된 메일 플로우 정책에서 LDAP 설정을 구성해야 합니다.

그림 ***66: SMTP*** 대화에서 연결을 삭제하도록 메일 플로우 정책 구성



리스너와 관련된 메일 플로우 정책에서 다음 DHAP(Directory Harvest Attack Prevention) 설정을 구성합니다.

- **Max. Invalid Recipients Per hour(**시간당 최대 잘못된 수신자 수**)**. 이 리스너가 원격 호스트에서 수신할 시간당 최대 잘못된 수신자 수. 이 임계값은 RAT 거부의 총계를 SMTP 대화에서 삭제되거나 작업 대기열에서 반송된 잘못된 LDAP 수신자에 대한 총 메시지 수와 결합하여 표시합니다. 예를 들어 임계값을 5로 구성하면, 카운터는 2개의 RAT 거부 및 3개의 삭제된 메시지를 잘못된 LDAP 수신자로 계산합니다. 이 시점에서 어플라이언스가 임계값에 도달한 것으로 확인하면 연결이 삭제됩니다. 기본적으로 공개 리스너에 대한 시간당 최대 수신자 수는 25입니다. 기본적으로 프라이빗 리스너의 경우 시간당 최대 수신자 수는 무제한입니다. 값을 "Unlimited(무제한)"로 설정하면 해당 메일 플로우 정책에 대해 DHAP가 활성화되지 않습니다.
- **Drop Connection if DHAP Threshold is reached within an SMTP conversation(SMTP** 대화 내에 **DHAP** 임계값에 도달하면 연결 삭제**)**. DHAP(Directory Harvest Attack Prevention) 임계값에 도달할 경우 연결을 삭제하도록 어플라이언스를 구성합니다.
- **Max. Recipients Per Hour Code(**시간당 최대 수신자 수 코드**)**. 연결 삭제 시 사용할 코드를 지정합니다. 기본 코드는 550입니다.
- **Max. Recipients Per Hour Text(**시간당 최대 수신자 수 코드**)**. 삭제된 연결에 사용할 텍스트를 지정합니다. 기본 텍스트는 "Too many invalid recipients(잘못된 수신자가 너무 많음)"입니다.

임계값에 도달하면, 수신자가 유효하지 않을 경우 메시지의 봉투 발신자는 반송 메시지를 받지 못합니다.

작업 대기열 내에서 디렉터리 수집 공격 방지

RAT(Recipient Access Table)에 도메인만 입력하고 작업 대기열 내에서 LDAP 수락 검증을 수행함으로써 대부분의 DHA를 방지할 수 있습니다. 이 방법은 악의적인 발신자가 SMTP 대화 중에 수신자의 유효성 여부를 알지 못하게 합니다. (수락 쿼리가 구성된 경우 시스템은 메시지를 수락하고 작업 대기열 내에서 LDAP 수락 검증을 수행합니다.) 그러나 수신자가 유효하지 않은 경우 메시지의 봉투 발신자는 여전히 반송 메시지를 받게 됩니다.

관련 주제

- 작업 대기열에서 디렉터리 수집 방지 구성, 765 페이지

작업 대기열에서 디렉터리 수집 방지 구성

디렉터리 수집 공격을 방지하려면 LDAP 서버 프로필을 구성하고 (LDAP 수락을 활성화해야 합니다. LDAP 수락 쿼리를 활성화했으면, 수락 쿼리를 사용하고 일치하지 않는 수신자에 대한 메일을 반송하도록 리스너를 구성합니다.

이제 지정된 기간에 전송 IP 주소당 시스템에서 허용할 유효하지 않은 수신자 주소 수를 정의하도록 메일 플로우 정책을 구성합니다. 숫자가 초과되면 시스템은 현재 상황을 DHA로 파악하고 알림 메시지를 전송합니다. 알림 메시지에는 다음 정보가 포함됩니다.

```
LDAP: Potential Directory Harvest Attack from host=('IP-address', 'domain_name
'), dhap_limit=n, sender_group=sender_group,

listener=listener_name, reverse_dns=(reverse_IP_address, 'domain_name
', 1), sender=envelope_sender, rcpt=envelope_recipients
```

시스템은 메일 플로우 정책에 지정된 임계값까지 메시지를 반송한 다음 나머지를 자동으로 수락 및 삭제하여, 주소가 잘못된 합법적인 발신자에게는 알림을 제공하고 악의적인 발신자는 수락되는 주소를 파악하지 못하도록 합니다.

이 잘못된 수신자 카운터는 AsyncOS에서 현재 사용 가능한 속도 제한과 비슷한 방식으로 작동합니다. 사용자는 이 기능을 활성화하고 퍼블릭 리스너의 HAT에서 메일 플로우 정책의 일부로서 제한을 정의합니다(HAT에 대한 기본 메일 플로우 정책 포함).

CLI에서 `listenerconfig` 명령을 사용하여 이를 구성할 수도 있습니다.

해당 리스너에 LDAP 쿼리가 구성되어 있는 경우, GUI에서 메일 플로우 정책을 수정할 때에도 이 기능이 표시됩니다.

시간당 잘못된 수신자 수를 입력하면 해당 메일 플로우 정책에 대해 DHAP가 활성화됩니다. 기본적으로 퍼블릭 리스너에서 시간당 허용되는 잘못된 수신자 수는 25입니다. 기본적으로 프라이빗 리스너의 경우 시간당 허용되는 잘못된 수신자 수는 무제한입니다. 값을 "Unlimited(무제한)"로 설정하면 해당 메일 플로우 정책에 대해 DHAP가 활성화되지 않습니다.

SMTP 인증을 위해 AsyncOS 구성

AsyncOS는 SMTP 인증에 대한 지원을 제공합니다. SMTP 인증은 SMTP 서버에 연결된 클라이언트를 인증하기 위한 메커니즘입니다.

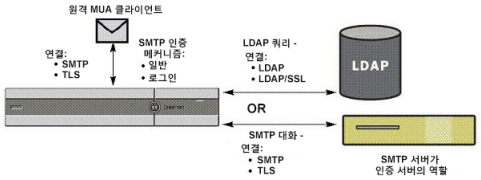
이 메커니즘의 사용 예는 조직의 사용자가 원격으로 연결되어 있는 경우에도(집에서 또는 출장 중에) 엔티티의 메일 서버를 사용하여 메일을 전송할 수 있도록 하는 것입니다. MUA(Mail User Agent)는 메일 전송을 시도할 때 인증 요청(challenge/response)을 실행할 수 있습니다.

사용자는 발신 메일 릴레이에 대해 SMTP 인증을 사용할 수도 있습니다. 따라서 어플라이언스가 네트워크 에지에 없는 구성에서도 어플라이언스는 릴레이 서버에 안전하게 연결할 수 있습니다.

AsyncOS는 사용자 자격 증명 인증을 위한 두 가지 방법을 지원합니다.

- LDAP 디렉터리를 사용할 수 있습니다.
- 다른 SMTP 서버(SMTP 인증 전달 및 SMTP 인증 발신)를 사용할 수 있습니다.

그림 ***67: SMTP*** 인증 지원***: LDAP*** 디렉터리 저장소 또는 ***SMTP*** 서버



구성된 SMTP 인증 방법은 smtpauthconfig 명령을 통해 HAT 메일 플로우 정책 내에서 사용할 SMTP 인증 프로필을 만들기 위해 사용됩니다(리스너에서 SMTP 인증 활성화, 769 페이지 참조).

관련 주제

- SMTP 인증 구성, 766 페이지
- SMTP 인증 쿼리 구성, 767 페이지
- 보조 SMTP 서버를 통한 SMTP 인증(전달로 SMTP 인증), 768 페이지
- LDAP로 SMTP 인증, 769 페이지
- 클라이언트 인증서를 사용하여 SMTP 세션 인증, 772 페이지
- 발송 SMTP 인증, 772 페이지
- 로깅 및 SMTP 인증, 773 페이지

SMTP 인증 구성

LDAP 서버로 인증하려는 경우, Add/Edit LDAP Server Profile(LDAP 서버 프로필 추가/수정) 페이지(또는 **ldapconfig** 명령)에서 SMTPAUTH 쿼리 유형을 선택하여 SMTP 인증 쿼리를 만듭니다. 구성하는 각 LDAP 서버에 대해 SMTP 인증 프로필로서 사용할 SMTPAUTH 쿼리를 구성할 수 있습니다.

SMTP 인증 쿼리에는 두 가지 종류, 즉 LDAP bind(LDAP 바인드) 및 passphrase as attribute(특성으로서의 암호)가 있습니다. 암호를 특성으로 사용하면 어플라이언스는 LDAP 디렉터리의 비밀번호 필드를 가져옵니다. 암호는 일반 텍스트로 저장하거나, 암호화하거나, 해시 상태로 저장할 수 있습니다. LDAP 바인드를 사용하면 어플라이언스는 클라이언트가 제공한 크리덴셜을 사용하여 LDAP 서버에 로그인하려고 시도합니다.

관련 주제

- 암호를 특성으로 지정, 766 페이지

암호를 특성으로 지정

RFC 2307 기반의 OpenLDAP 표기 규칙은 인코딩된 암호에 중괄호 접두사가 붙는 코딩 유형입니다(예: "{SHA}5en6G6MezRroT3XKqkdPOmY/BfQ="). 이 예에서 암호 부분은 SHA 적용 후 일반 텍스트 암호의 base64 인코딩입니다.

어플라이언스는 암호를 얻기 전에 SASL 메커니즘을 MUA와 협상합니다. 어플라이언스와 MUA는 방법을 결정합니다(LOGIN, PLAIN, MD5, SHA, SSHA, 및 CRYPT SASL 메커니즘이 지원됨). 그런 다음 어플라이언스는 암호를 가져오기 위해 LDAP 데이터베이스에 쿼리합니다. LDAP에서 암호는 괄호의 접두사를 포함할 수 있습니다.

- 접두사가 없으면 어플라이언스는 암호가 LDAP에 일반 텍스트로 저장되었다고 간주합니다.
- 접두사가 있으면 어플라이언스는 해시된 암호를 가져오고, MUA가 제공하는 사용자 이름 및/또는 암호에서 해시를 수행하고, 해시된 버전을 비교합니다. 어플라이언스는 암호 필드에서 해시 메커니즘 유형을 해시된 암호 앞에 붙이는 RFC 2307 표기 규칙 기반의 SHA1 및 MD5 해시 유형을 지원합니다.
- 일부 LDAP 서버(예: OpenWave LDAP 서버)는 암호화된 암호에 암호화 유형을 접두사로 사용하지 않습니다. 대신 암호화 유형을 별도의 LDAP 특성으로 저장합니다. 이러한 경우 암호를 SMTP 대화에서 얻은 암호와 비교할 때 어플라이언스가 추정하는 기본 SMTP AUTH 암호화 방법을 지정할 수 있습니다.

어플라이언스는 SMTP 인증 교환에서 임의의 사용자 이름을 가져오고 이를 일반 또는 해시된 암호 필드를 가져오는 LDAP 쿼리로 변환합니다. 그런 다음 SMTP 인증 크리덴셜에서 제공된 암호에 대해 필요한 해싱을 수행하고 그 결과를 LDAP에서 검색한 것과 비교합니다(해시 유형 태그가 있는 경우 이를 제거). 일치하는 경우 SMTP 인증 대화가 계속 진행됩니다. 실패하는 경우 오류 코드가 반환됩니다.

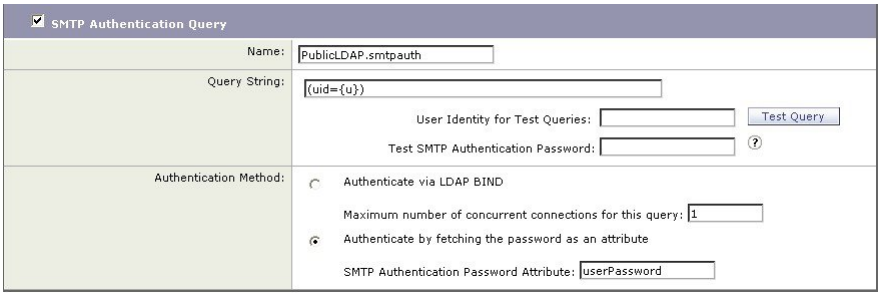
SMTP 인증 쿼리 구성

표 ***69: SMTP*** 인증 ***LDAP*** 쿼리 필드

이름	쿼리의 이름**.**
Query String(쿼리 문자열)	LDAP 바인드를 통해 인증할지 아니면 암호를 특성으로 가져옴으로써 인증할지를 선택할 수 있습니다. **Bind(**바인드**)**: 클라이언트가 제공하는 자격 증명을 사용하여 LDAP 서버에 로그인을 시도합니다(이를 LDAP 바인드라고 함). SMTP 인증 쿼리에서 사용할 최대 동시 연결 수를 지정합니다. 이 수는 위의 LDAP 서버 특성에서 지정한 수를 초과하지 않아야 합니다. 바인드 인증에 대한 다수의 세션 시간 초과를 피하려면 여기에서 최대 동시 연결 수를 늘리십시오(일반적으로 거의 모든 연결이 SMTP 인증에 할당될 수 있음). 각 바인드 인증에 새 연결이 사용됩니다. 나머지 연결은 다른 LDAP 쿼리 유형이 공유합니다. 암호를 특성으로: 암호를 가져와 인증하려면 아래의 SMTP AUTH 암호 특성 필드에 암호를 지정합니다. 두 종류의 인증에 사용할 LDAP 쿼리를 지정합니다. Active Directory 쿼리 예: (&(samaccountname={u})(objectCategory=person)(objectClass=user))
SMTP Auth Passphrase Attribute(SMTP 인증 암호 특성)	"Authenticate by fetching the password as an attribute(암호를 특성으로 가져와서 인증)"를 선택한 경우 여기에서 암호 특성을 지정할 수 있습니다.

다음 예에서는 System Administration(시스템 관리) > LDAP 페이지를 사용하여, SMTPAUTH 쿼리를 포함하도록 "PublicLDAP"라는 이름의 LDAP 구성을 수정할 수 있습니다. userPassword 특성과 일치하도록 쿼리 문자열(uid={u})이 작성됩니다.

그림 ***68: SMTP*** 인증 쿼리



SMTPAUTH 프로필이 구성되면, 리스너가 SMTP 인증에 해당 쿼리를 사용하도록 지정할 수 있습니다.

보조 SMTP 서버를 통한 SMTP 인증(전달로 SMTP 인증)

다른 SMTP 서버와 함께 또 다른 SMTP 인증 대화에 제공된 사용자 이름과 암호를 확인하도록 어플라이언스를 구성할 수 있습니다.

인증하는 서버는 메일을 전송하는 서버가 아니라, 오히려 SMTP 인증 요청에 응답하는 서버입니다. 인증에 성공하면 전용 메일 서버를 이용한 SMTP의 메일 전송을 계속 진행할 수 있습니다. 자격 증명만이 인증을 위해 또 다른 SMTP 서버로 전달(또는 "프록시")되므로 이 기능을 "전달로 SMTP 인증"이라고도 합니다.

단계 **1** **Network(네트워크) > SMTP Authentication(SMTP 인증)**을 선택합니다.

단계 **2** **Add Profile(프로필 추가)**을 클릭합니다..

단계 **3** SMTP 인증 프로필의 고유한 이름을 입력합니다.

단계 **4** **Profile Type(프로필 유형)**에서 **Forward(전달)**를 선택합니다.

단계 **5** **Next(다음)**을 클릭합니다.

단계 **6** 호스트 이름/IP 주소 및 전달 서버의 포트를 입력합니다. 인증 요청 전달에 사용할 전달 인터페이스를 선택합니다. 최대 동시 연결 수를 지정합니다. 그런 다음 어플라이언스에서 전달 서버로의 연결에 TLS가 필요한지 여부를 구성할 수 있습니다. 또한 사용 가능한 경우 원하는 SASL 방법(PLAIN 또는 LOGIN)을 선택할 수 있습니다. 각 전달 서버에 대해 이러한 선택 사항이 구성됩니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

단계 **8** 인증 프로필을 만든 후 리스너에서 프로필을 활성화할 수 있습니다. 자세한 내용은 리스너에서 SMTP 인증 활성화, 769 페이지를 참조하십시오.

LDAP로 SMTP 인증

System Administration(시스템 관리) > LDAP 페이지를 사용하여 LDAP 서버 프로필과 함께 SMTP 인증 쿼리를 미리 만든 경우에만 LDAP 기반 SMTP 인증 프로필을 만들 수 있습니다. 그런 다음 이 프로필을 사용하여 SMTP 인증 프로필을 만들 수 있습니다. LDAP 프로필 만들기에 대한 자세한 내용은 LDAP 쿼리 이해, 736 페이지 섹션을 참조하십시오.

단계 **1** **Network(**네트워크**) > SMTP Authentication(SMTP** 인증**)**을 선택합니다.

단계 **2** **Add Profile(**프로필 추가**)**을 클릭합니다.

단계 **3** SMTP 인증 프로필의 고유한 이름을 입력합니다.

단계 **4** Profile Type(프로필 유형)에서 **LDAP**를 선택합니다.

단계 **5** **Next(**다음**)**를 클릭합니다.

단계 **6** 이 인증 프로필에 사용할 LDAP 쿼리를 선택합니다.

단계 **7** 드롭다운 메뉴에서 기본 암호화 방법을 선택합니다. SHA, Salted SHA, Crypt, Plain 또는 MD5 중에서 선택할 수 있습니다. LDAP 서버가 암호화된 암호에 암호화 유형으로 접두사를 추가하는 경우 'None(없음)'을 선택된 상태로 둡니다. LDAP 서버가 암호화 유형을 별도의 엔티티로 저장하는 경우(예: OpenWave LDAP 서버) 메뉴에서 암호화 방법을 선택합니다. LDAP 쿼리가 바인드를 사용하는 경우 기본 암호화 설정이 사용되지 않습니다.

단계 **8** **Finish(**마침**)**를 클릭합니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

단계 **10** 인증 프로필을 만든 후 리스너에서 프로필을 활성화할 수 있습니다. 자세한 내용은 리스너에서 SMTP 인증 활성화, 769 페이지를 참조하십시오.

다음에 수행할 작업

관련 주제

- 리스너에서 SMTP 인증 활성화, 769 페이지

리스너에서 SMTP 인증 활성화

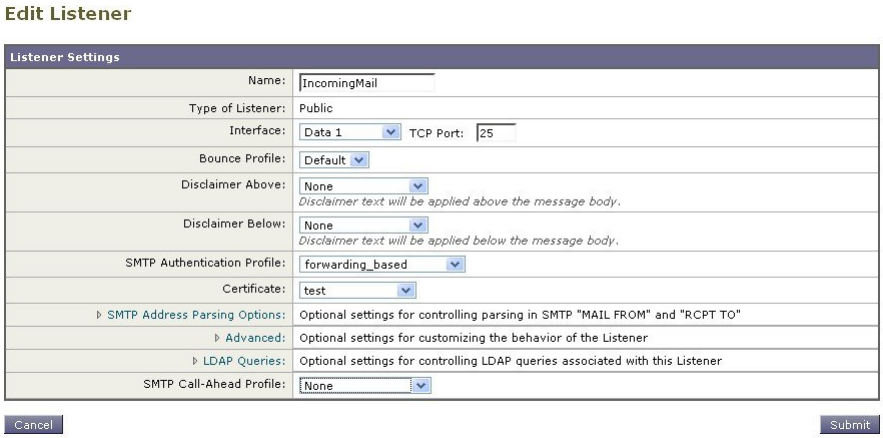
Network(네트워크**) > SMTP Authentication(SMTP** 인증**)** 페이지를 사용하여 수행하려는 SMTP 인증 유형을 지정하는 SMTP 인증 "프로필"을 만들었으면(LDAP 기반 또는 SMTP 전달 기반), **Network(**네트워크**) > Listeners(**리스너**)** 페이지(또는 **`listenerconfig`** 명령)를 사용하여 해당 프로필을 리스너와 연결해야 합니다.

참고 인증된 사용자는 현재 메일 플로우 정책 내에서 RELAY 연결 동작이 허용됩니다.

프로필에 전달 서버를 두 개 이상 지정할 수 있습니다. 어플라이언스와 전달 서버 간에는 SASL 메커니즘 CRAM-MD5 및 DIGEST-MD5가 지원되지 않습니다.

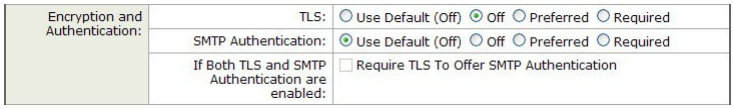
다음 예에서는 Edit Listener(리스너 수정) 페이지를 통해 구성한 SMTPAUTH 프로필을 사용하도록 리스너 "InboundMail"이 수정됩니다.

그림 ***69: Edit Listener(*리스너 수정*)*** 페이지를 통해 ***SMTP*** 인증 프로필 선택



프로필을 사용하도록 리스너가 구성되면, 리스너에서 SMTP 인증을 허용, 불허 또는 요구하도록 Host Access Table 기본 설정을 변경할 수 있습니다.

그림 ***70:*** 메일 플로우 정책에서 ***SMTP*** 인증 활성화



숫자	설명
1.	SMTP 인증 필드는 SMTP 인증을 위한 리스너 레벨 제어를 제공합니다. "No"를 선택하면 구성한 다른 SMTP 인증 설정과 상관없이 리스너에서 인증이 활성화되지 않습니다.
2.	두 번째 프롬프트(SMTP Authentication:)에서 "Required"를 선택하는 경우, TLS가 협상될 때까지(클라이언트가 두 번째 EHLO 명령을 실행한 후) AUTH 키워드가 발급되지 않습니다.

관련 주제

- SMTP 인증 및 HAT 정책 설정, 770 페이지
- HAT 지연 거부, 771 페이지

SMTP 인증 및 HAT 정책 설정

SMTP 인증 협상이 시작되기 전에 발신자는 적절한 발신자 그룹으로 그룹화되므로 HAT(Host Access Table) 설정은 영향을 받지 않습니다. 원격 메일 호스트가 연결되면 어플라이언스는 먼저 어떤 발신자 그룹을 적용할지를 결정하고 해당 발신자 그룹에 메일 정책을 부과합니다. 예를 들어 SUSPECTLIST 발신자 그룹에 원격 MTA "suspicious.com"이 있으면, "suspicious.com's" SMTPAUTH 협상 결과와 상관없이 THROTTLE 정책이 적용됩니다.

그러나 SMTPAUTH를 사용하여 인증되는 발신자는 "일반" 발신자와 다르게 취급됩니다. 성공적인 SMTPAUTH 세션을 위한 연결 동작은 "RELAY"로 변경되어, RAT(Recipient Access Table) 및 LDAPACCEPT를 효과적으로 우회합니다. 이렇게 하여 발신자는 어플라이언스를 통해 메시지를 릴레이할 수 있습니다. 설명한 대로, 적용되는 Rate Limiting(속도 제한) 또는 조절(throttling)은 그대로 유지됩니다.

HAT 지연 거부

HAT 지연 거부가 구성되면 HAT 발신자 그룹 및 메일 플로우 정책 구성을 기반으로 삭제될 수 있는 연결이 여전히 성공적으로 인증되고 RELAY 메일 플로우 정책이 허용될 수 있습니다.

메시지 수신자 레벨에서 HAT 거부를 수행할지 여부를 구성합니다. 기본적으로 HAT 거부 연결은 SMTP 대화가 시작될 때 배너 메시지와 함께 닫힙니다.

HAT "Reject(거부)" 설정 때문에 이메일이 거부되는 경우 AsyncOS는 SMTP 대화가 시작될 때보다는 메시지 수신자 레벨(RCPT TO)에서 거부를 수행할 수 있습니다. 이렇게 메시지를 거부하면 메시지 거부가 지연되고 메시지가 반송되어, AsyncOS는 거부된 메시지에 대해 좀 더 자세한 정보를 보유하게 됩니다. 예를 들어 메시지가 차단된 주소 및 각 수신자 주소에서 온 메일을 볼 수 있습니다. HAT 거부를 지연하면 MTA 전송이 여러 재시도를 수행할 가능성이 줄어듭니다.

HAT 지연 거부를 활성화하면 다음 동작이 발생합니다.

- MAIL FROM 명령이 수락되면 메시지 개체가 생성되지 않습니다.
- 이메일 전송 액세스 권한이 거부됨을 설명하는 텍스트와 함께 모든 RCPT TO 명령이 거부됩니다.
- 전송 MTA가 SMTP AUTH로 인증되는 경우 RELAY 정책이 부여되고 정상적인 메일 전달이 허용됩니다.

`listenerconfig --> setup` CLI 명령을 사용하여 지연된 거부를 구성할 수 있습니다. 이 동작은 기본적으로 비활성화되어 있습니다.

다음 표는 HAT에 대해 지연된 거부를 구성하는 방법을 보여줍니다.

```
example.com> listenerconfig

Currently configured listeners:

1. listener1 (on main, 172.22.138.17) QMQP TCP Port 628 Private

2. listener2 (on main, 172.22.138.17) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> setup

Enter the global limit for concurrent connections to be allowed across all listeners.
```

```
[300]>

[...]


By default HAT rejected connections will be closed with a banner
message at the start of the SMTP conversation. Would you like to do the rejection at the
message recipient level instead for more detailed logging of rejected mail?

[N]> y

Do you want to modify the SMTP RCPT TO reject response in this case?

[N]> y

Enter the SMTP code to use in the response. 550 is the standard code.

[550]> 551

Enter your custom SMTP response. Press Enter on a blank line to finish.

Sender rejected due to local mail policy.

Contact your mail admin for assistance.
```

클라이언트 인증서를 사용하여 **SMTP** 세션 인증

Email Security Appliance는 클라이언트 인증서를 사용하여 Email Security Appliance와 사용자의 메일 클라이언트 간 SMTP 세션을 인증하도록 지원합니다.

SMTP 인증 프로필을 만들 때 인증서 확인에 사용할 인증서 인증 LDAP 쿼리를 선택합니다. 또한 클라이언트 인증서를 사용할 수 없는 경우 Email Security Appliance가 사용자 인증을 위해 SMTP AUTH 명령으로 대체할지 여부를 지정할 수 있습니다.

조직에서 클라이언트 인증서를 사용하여 사용자를 인증하는 경우 SMTP 인증 쿼리를 사용하여, 클라이언트 인증서가 없는 사용자라도 레코드에 허용된다고 지정되어 있는 한 메일을 전송할 수 있도록 할지를 확인하는 옵션이 제공됩니다.

발송 **SMTP** 인증

SMTP 인증은 사용자 이름과 암호를 사용하여 아웃바운드 메일 릴레이에 대한 검증을 제공하는 데에도 사용할 수 있습니다. '발신' SMTP 인증 프로필을 만든 다음 모든 도메인에 대한 SMTP 경로에 첨부합니다. 각 메일 전달 시도에서 어플라이언스는 필요한 자격 증명을 사용하여 업스트림 메일 릴레이에 로그온합니다. SMTP 인증은 PLAIN 및 LOGIN 인증 프로토콜을 지원합니다.

단계 **1** 발신 SMTP 인증 프로필을 만듭니다.

1. **Network(**네트워크**) > SMTP Authentication(SMTP** 인증**)**을 선택합니다.
2. **Add Profile(**프로필 추가**)**을 클릭합니다.

3. SMTP 인증 프로필의 고유한 이름을 입력합니다.
4. Profile Type(프로필 유형)에서 **Outgoing(**발신**)**을 선택합니다.
5. **Next(**다음**)**를 클릭합니다.
6. 인증 프로필을 위한 인증 사용자 이름 및 암호를 입력합니다.
7. **Finish(**마침**)**를 클릭합니다.

단계 **2** 1단계에서 만든 발신 SMTP 인증 프로필을 사용하여 SMPT 경로를 구성합니다.

1. **Network(**네트워크**) > SMTP Routes(SMTP** 경로**)**를 선택합니다.
2. 테이블의 **Receiving Domain(**수신 도메인**)** 열에서 **All Other Domains(**다른 모든 도메인**)** 링크를 클릭합니다.
3. SMTP 경로에 대해 Destination Host(대상 호스트)의 이름을 입력합니다. 이것은 발신 메일 전달에 사용된 외부 메일 릴레이의 호스트 이름입니다.
4. 드롭다운 메뉴에서 발신 SMTP 인증 프로필을 선택합니다.
5. 변경 사항을 제출 및 커밋합니다.

로깅 및 **SMTP** 인증

어플라이언스에 SMTP 인증 메커니즘(LDAP 기반, SMTP 전달 서버 기반 또는 SMTP 발신)이 구성되면 다음 이벤트가 메일 로그에 기록됩니다.

- [정보] 성공적인 SMTP 인증 시도 - 인증된 사용자 및 사용된 메커니즘 포함. 일반 텍스트 암호는 기록되지 않습니다.
- [정보] 실패한 SMTP 인증 시도 - 인증된 사용자 및 사용된 메커니즘 포함.
- [경고] 인증 서버에 연결할 수 없음 - 서버 이름 및 메커니즘 포함.
- [경고] 전달 서버(업스트림, 주입 어플라이언스와 대화)가 인증 요청을 기다리는 동안 시간 초과될 때 시간 초과 이벤트.

사용자를 위한 외부 **LDAP** 인증 구성

LDAP 사용자 이름 및 암호로 로그인하도록 허용함으로써 네트워크의 LDAP 디렉터리를 사용하여 사용자를 인증하도록 어플라이언스를 구성할 수 있습니다. LDAP 서버에 대한 인증 쿼리를 구성한 후, GUI의 **System Administration(**시스템 관리**) > Users(**사용자**)** 페이지에서(또는 CLI의 **`userconfig`** 명령을 사용하여) 외부 인증을 사용하도록 어플라이언스를 구성합니다.

단계 **1** 사용자 계정을 찾기 위한 쿼리를 만듭니다**.** LDAP 서버 프로필에서 LDAP 디렉터리의 사용자 계정을 검색하기 위한 쿼리를 만듭니다.

단계 **2** 그룹 멤버십 쿼리를 만듭니다**.** 사용자가 디렉터리 그룹의 구성원인지를 확인하는 쿼리를 만듭니다.

단계 **3** **LDAP** 서버를 사용하기 위한 외부 인증을 설정합니다**.** 사용자 인증에 LDAP 서버를 사용하고 사용자 역할을 LDAP 디렉터리의 그룹에 할당하도록 어플라이언스를 구성합니다. 자세한 내용은 "관리 작업 배포" 장의 "사용자 추가" 섹션을 참조하십시오.

참고 쿼리가 예상 결과를 반환하는지 확인하려면 LDAP 페이지의 Test Query(쿼리 테스트) 버튼(또는 **ldaptest** 명령)을 사용합니다. 자세한 내용은 LDAP 쿼리 테스트, 750 페이지를 참고하십시오.

다음에 수행할 작업

관련 주제

- 사용자 계정 쿼리, 774 페이지
- 그룹 멤버십 쿼리, 775 페이지

사용자 계정 쿼리

외부 사용자를 인증하기 위해 AsyncOS는 LDAP 디렉터리의 사용자 레코드 및 사용자 전체 이름이 포함된 특성을 검색하는 쿼리를 사용합니다. 선택하는 서버 유형에 따라 AsyncOS는 기본 쿼리 및 기본 특성을 입력합니다. RFC 2307, LDAP 사용자 레코드에 특성이 정의된 경우(shadowLastChange, shadowMax 및 shadowExpire) 어플라이언스에서 만료된 계정의 사용자를 거부하도록 할 수 있습니다. 사용자 레코드가 상주하는 도메인 레벨에 대해 기본 DN이 필요합니다.

다음 표에는 AsyncOS가 Active Directory 서버에서 사용자 계정을 검색할 때 사용하는 기본 쿼리 문자열 및 전체 사용자 이름 특성이 표시됩니다.

표 ***70:*** 기본 사용자 계정 쿼리 문자열 및 특성***: Active Directory***

서버 유형	**Active Directory**
기본 DN	[비어 있음] (사용자 레코드를 찾으려면 특정 기본 DN을 사용해야 합니다.)
쿼리 문자열	(&(objectClass=user)(sAMAccountName={u}))
사용자의 전체 이름을 포함하는 특성	displayName

다음 표에는 AsyncOS가 OpenLDAP 서버에서 사용자 계정을 검색할 때 사용하는 기본 쿼리 문자열 및 전체 사용자 이름 특성이 표시됩니다.

표 ***71:*** 기본 사용자 계정 쿼리 문자열 및 특성***: OpenLDAP***

서버 유형	**OpenLDAP**
기본 DN	[비어 있음] (사용자 레코드를 찾으려면 특정 기본 DN을 사용해야 합니다.)
쿼리 문자열	(&(objectClass=posixAccount)(uid={u}))
사용자의 전체 이름을 포함하는 특성	gecos

그룹 멤버십 쿼리

AsyncOS는 또한 쿼리를 사용하여 사용자가 디렉터리 그룹의 구성원인지를 확인합니다. 디렉터리 그룹의 멤버십은 시스템 내 사용자의 권한을 결정합니다. GUI의 System Administration(시스템 관리) > Users(사용자) 페이지(또는 CLI의 userconfig)에서 외부 인증을 활성화할 때 LDAP 디렉터리의 그룹에 사용자 역할을 할당합니다. 사용자 역할은 사용자가 시스템에서 보유하는 권한을 결정하며, 외부에서 인증된 사용자의 경우 개별 사용자 대신 디렉터리 그룹에 역할이 할당됩니다. 예를 들면 IT 디렉터리 그룹의 사용자를 Administrator 사용자 역할에 할당하고 Support 디렉터리 그룹의 사용자를 Help Desk User 역할에 할당할 수 있습니다.

한 사용자가 서로 다른 사용자 역할의 여러 LDAP 그룹에 속해 있으면 AsyncOS는 해당 사용자에게 가장 제한적인 역할에 대한 권한을 부여합니다. 예를 들어 한 사용자가 Operator 권한의 그룹과 Help Desk User 권한의 그룹에 속해 있으면 AsyncOS는 해당 사용자에게 Help Desk User 역할에 대한 권한을 부여합니다.

그룹 멤버십을 쿼리하도록 LDAP 프로필을 구성할 때 그룹 레코드를 찾을 수 있는 디렉터리 레벨에 대한 기본 DN, 그룹 구성원의 사용자 이름을 가지고 있는 특성 및 그룹 이름을 가지고 있는 특성을 입력합니다. LDAP 서버 프로필에 대해 선택하는 서버 유형을 기반으로, AysncOS는 사용자 이름 및 그룹 이름 특성에 대한 기본값과 기본 쿼리 문자열을 입력합니다.

참고 Active Directory 서버의 경우 사용자가 그룹의 구성원인지를 확인하는 기본 쿼리 문자열은 (&(objectClass=group)(member={u}))입니다. 그러나 LDAP 스키마가 "memberof" 목록에서 사용자 이름 대신 DN을 사용하는 경우 {u} 대신 {dn}을 사용할 수 있습니다.

다음 표에서는 AsyncOS가 Active Directory 서버에서 그룹 멤버십을 검색할 때 사용하는 기본 쿼리 문자열 및 특성을 보여줍니다.

표 ***72:*** 기본 그룹 멤버십 쿼리 문자열 및 특성***: Active Directory***

서버 유형	**Active Directory**
기본 DN	[비어 있음] (그룹 레코드를 찾으려면 특정 기본 DN을 사용해야 합니다.)
사용자가 그룹 구성원인지 여부를 확인하는 쿼리 문자열	(&(objectClass=group)(member={u})) 참고 LDAP 스키마가 memberOf 목록에서 사용자 이름 대신 DN을 사용하는 경우 {u}를 {dn}으로 교체할 수 있습니다.
각 구성원의 사용자 이름을 가지고 있는 특성(또는 사용자 레코드에 대한 DN)	member
그룹 이름을 포함하는 특성	cn

다음 표에서는 AsyncOS가 OpenLDAP 서버에서 그룹 멤버십을 검색할 때 사용하는 기본 쿼리 문자열 및 특성을 보여줍니다.

표 *73:* 기본 그룹 멤버십 쿼리 문자열 및 특성*: OpenLDAP*

서버 유형	**OpenLDAP**
기본 DN	[비어 있음] (그룹 레코드를 찾으려면 특정 기본 DN을 사용해야 합니다.)
사용자가 그룹 구성원인지 여부를 확인하는 쿼리 문자열	(&(objectClass=posixGroup)(memberUid={u}))
각 구성원의 사용자 이름을 가지고 있는 특성(또는 사용자 레코드에 대한 DN)	memberUid
그룹 이름을 포함하는 특성	cn

스팸 격리의 최종 사용자 인증

스팸 격리 최종 사용자 인증 쿼리는 사용자가 스팸 격리에 로그인할 때 사용자를 검증합니다. 토큰 {u}는 사용자를 지정합니다(사용자의 로그인 이름을 나타냄). 토큰 {a}는 사용자의 이메일 주소를 지정합니다. LDAP 쿼리는 이메일 주소에서 "SMTP:"를 제거하지 않습니다. AsyncOS가 주소에서 해당 부분을 제거합니다.

스팸 격리가 최종 사용자 액세스를 위해 LDAP 쿼리를 사용하도록 하려면 "Designate as the active query(활성 쿼리로 지정)" 확인란을 선택합니다. 기존의 활성 쿼리는(있는 경우) 비활성화됩니다. **System Administration(**시스템 관리**) > LDAP** 페이지를 열면 활성 쿼리 옆에 별표(*)가 표시됩니다.

서버 유형을 기반으로 AsyncOS는 최종 사용자 인증 쿼리에 다음의 기본 쿼리 문자열 중 하나를 사용합니다.

- **Active Directory:** (sAMAccountName={u})
- **OpenLDAP**: (uid={u})
- 알 수 없음 또는 기타**:** [비어 있음]

기본적으로 주 이메일 특성은 Active Directory 서버의 경우 proxyAddresses, OpenLDAP 서버의 경우 mail입니다. 고유한 쿼리 및 이메일 특성을 입력할 수 있습니다. CLI에서 쿼리를 만들려면 ldapconfig 명령의 isqauth 하위 명령을 사용합니다.

참고 사용자가 전체 이메일 주소로 로그인하도록 하려면 Query String(쿼리 문자열)에 (mail=smtp:{a})를 사용합니다.

관련 주제

- 샘플 Active Directory 최종 사용자 인증 설정, 777 페이지
- 샘플 OpenLDAP 별칭 통합 설정, 779 페이지
- 스팸 격리에 대한 최종 사용자 액세스 구성 , 884 페이지

샘플 Active Directory 최종 사용자 인증 설정

이 섹션에서는 Active Directory 서버 및 최종 사용자 인증 쿼리에 대한 샘플 설정을 보여줍니다. 이 예에서는 Active Directory 서버에 대한 암호 인증, mail 및 proxyAddresses 이메일 특성, Active Directory 서버 엔드 유저 인증을 위한 기본 쿼리 문자열을 사용합니다.

표 ***74: LDAP*** 서버 및 스팸 격리 최종 사용자 인증 설정 예***: Active Directory***

인증 방법	암호 사용(검색을 위해 바인딩할 낮은 권한의 사용자를 만들거나 익명 검색을 구성해야 함)
서버 유형	Active Directory
포트	3268
기본 DN	[공백]
연결 프로토콜	[공백]
쿼리 문자열	(sAMAccountName={u})
이메일 특성	mail,proxyAddresses

샘플 OpenLDAP 엔드유저 인증 설정

이 섹션에서는 OpenLDAP 서버 및 최종 사용자 인증 쿼리에 대한 샘플 설정을 보여줍니다. OpenLDAP 서버용 익명 인증, mail 및 mailLocalAddress 이메일 특성, 그리고 OpenLDAP 서버에 대한 최종 사용자 인증용 기본 쿼리 문자열이 다음 예에 사용됩니다.

표 ***75: LDAP*** 서버 및 스팸 격리 최종 사용자 인증 설정 예***: OpenLDAP***

인증 방법	**Anonymous**
서버 유형	OpenLDAP
포트	389
기본 DN	[비어 있음] (일부 오래된 스키마는 특정 기본 DN을 사용하고자 함.)
연결 프로토콜	[공백]
쿼리 문자열	(uid={u})
이메일 특성	mail,mailLocalAddress

스팸 격리 별칭 통합 쿼리

스팸 격리를 사용하는 경우 스팸 격리 별칭 통합 쿼리는 수신자가 각 별칭에 대해 격리 알림을 받지 않도록 이메일 별칭을 통합합니다. 예를 들어 john@example.com, jsmith@example.com 및 john.smith@example.com 이메일 주소에 대한 메일을 받는 수신자가 있다고 가정해보겠습니다. 별칭 통합을 사용하면 수신자는 모든 사용자 별칭으로 전송되는 메시지에 대해 선택된 기본 이메일 주소로 단일 스팸 알림을 수신합니다.

메시지를 기본 이메일 주소로 통합하려면 수신자의 대체 이메일 별칭을 검색할 쿼리를 만들고, Email Attribute(이메일 특성) 필드에 수신자의 기본 이메일 주소에 대한 특성을 입력합니다.

스팸 격리가 스팸 알림을 위해 LDAP 쿼리를 사용하도록 하려면 "Designate as the active query(활성 쿼리로 지정)" 확인란을 선택합니다. 기존의 활성 쿼리는(있는 경우) 비활성화됩니다. System Administration(시스템 관리) > LDAP 페이지를 열면 활성 쿼리 옆에 별표(*)가 표시됩니다.

Active Directory 서버의 경우 기본 쿼리 문자열은 (|(proxyAddresses={a})(proxyAddresses=smtp:{a}))이고 기본 이메일 특성은 mail입니다. OpenLDAP 서버의 경우 기본 쿼리 문자열은 (mail={a})이고 기본 이메일 특성은 mail입니다. 쉼표로 구분된 여러 특성을 포함하여, 고유한 쿼리 및 이메일 특성을 정의할 수 있습니다. 이메일 특성을 둘 이상 입력하는 경우 proxyAddresses와 같이 변경될 수 있는 여러 값을 가진 특성 대신 mail과 같은 단일 값을 사용하는 고유한 특성을 첫 번째 이메일 특성으로 입력하는 것이 좋습니다.

CLI에서 쿼리를 만들려면 ldapconfig 명령의 isqalias 하위 명령을 사용합니다.

관련 주제

- 샘플 Active Directory 별칭 통합 설정, 778 페이지
- 샘플 OpenLDAP 별칭 통합 설정, 779 페이지

샘플 **Active Directory** 별칭 통합 설정

이 섹션에서는 Active Directory 서버 및 별칭 통합 쿼리에 대한 샘플 설정을 보여줍니다. Active Directory 서버에 대한 익명 인증, Active Directory 서버에 대한 별칭 통합용 쿼리 문자열, 그리고 mail 이메일 특성이 다음 예에 사용됩니다.

표 ***76: LDAP*** 서버 및 스팸 격리 별칭 통합 설정 예***: Active Directory***

인증 방법	**Anonymous**
서버 유형	Active Directory
포트	3268
기본 DN	[공백]
연결 프로토콜	SSL 사용

인증 방법	**Anonymous**
쿼리 문자열	(|(mail={a})(mail=smtp:{a}))
이메일 특성	mail

참고 이 예는 보여주기 위한 것입니다. 쿼리 및 OU 또는 트리 설정은 환경과 구성에 따라 달라질 수 있습니다.

샘플 **OpenLDAP** 별칭 통합 설정

이 섹션에서는 OpenLDAP 서버 및 별칭 통합 쿼리에 대한 샘플 설정을 보여줍니다. OpenLDAP 서버에 대한 익명 인증, OpenLDAP 서버에 대한 별칭 통합용 쿼리 문자열, 그리고 mail 이메일 특성이 다음 예에 사용됩니다.

표 ***77: LDAP*** 서버 및 스팸 격리 별칭 통합 설정 예***: OpenLDAP***

인증 방법	**Anonymous**
서버 유형	OpenLDAP
포트	389
기본 DN	[비어 있음] (일부 오래된 스키마는 특정 기본 DN을 사용하고자 함.)
연결 프로토콜	SSL 사용
쿼리 문자열	(mail={a})
이메일 특성	mail

참고 이 예는 보여주기 위한 것입니다. 쿼리 및 OU 또는 트리 설정은 환경과 구성에 따라 달라질 수 있습니다.

샘플 사용자 **DN** 설정

이 섹션에서는 Active Directory 서버 및 사용자 DN 쿼리에 대한 샘플 설정을 보여줍니다. Active Directory 서버에 대한 익명 인증 및 Active Directory 서버에 대한 사용자 DN 검색용 쿼리 문자열이 다음 예에 사용됩니다.

표 *78: LDAP* 서버 및 스팸 격리 별칭 통합 설정 예*: Active Directory*

인증 방법	**Anonymous**
서버 유형	Active Directory
포트	3268
기본 DN	[공백]
연결 프로토콜	SSL 사용
쿼리 문자열	`(proxyAddresses=smtp:{a})`

참고 이 예는 보여주기 위한 것입니다. 쿼리 및 OU 또는 트리 설정은 환경과 구성에 따라 달라질 수 있습니다.

여러 LDAP 서버와 작동하도록 AsyncOS 구성

LDAP 프로필을 구성할 때 여러 LDAP 서버 목록에 연결되도록 어플라이언스를 구성할 수 있습니다. 여러 LDAP 서버를 사용하려면 동일한 정보를 포함하고, 동일한 구조를 사용하며, 동일한 인증 정보를 사용하도록 LDAP 서버를 구성해야 합니다. (레코드를 통합할 수 있는 서드파티 제품이 있습니다.)

이중화 LDAP 서버에 연결하도록 어플라이언스를 구성할 때 장애 조치 또는 부하분산에 대해 LDAP 구성을 구성할 수 있습니다.

다음 결과를 얻기 위해 여러 LDAP 서버를 사용할 수 있습니다.

- 장애 조치. LDAP 프로필에서 장애 조치를 구성하는 경우, 어플라이언스는 첫 번째 LDAP 서버에 연결할 수 없을 때 목록에 있는 다음 LDAP 서버로 장애 조치됩니다.
- 부하분산. LDAP 프로필에서 부하분산을 구성하는 경우, 어플라이언스는 LDAP 쿼리를 수행할 때 LDAP 서버 목록 전체에 연결을 분산합니다.

System Administration(시스템 관리) > LDAP 페이지 또는 CLI ldapconfig 명령을 통해 이중화 LDAP 서버를 구성할 수 있습니다.

서버 및 쿼리 테스트

LDAP 서버에 대한 연결을 테스트하려면 Add/Edit LDAP Server Profile(LDAP 서버 프로필 추가/수정) 페이지에 있는 **Test Server(s)(**서버 테스트**)** 버튼(또는 CLI의 **`test`** 하위 명령)을 사용합니다. 여러 LDAP 서버를 사용하는 경우 AsyncOS는 각 서버를 테스트하고 각 서버에 대한 개별 결과를 표시합니다. AsyncOS는 또한 각 LDAP 서버에서 쿼리를 테스트하고 개별 결과를 표시합니다.

관련 주제

- 페일오버, 781 페이지
- 부하 균형, 782 페이지

페일오버

LDAP 쿼리가 해결되었는지 확인하려면 LDAP 프로필에서 장애 조치를 구성할 수 있습니다. LDAP 서버와의 연결에 실패한 경우 또는 쿼리에서 특정 오류 코드(예: Unavailable 또는 Busy)를 반환하는 경우 어플라이언스는 목록에 지정된 다음 LDAP 서버에 대해 쿼리를 시도합니다.

어플라이언스는 지정된 기간에 LDAP 서버 목록에서 첫 번째 서버에 연결하려고 시도합니다. 어플라이언스가 목록에 있는 첫 번째 LDAP 서버에 연결하지 못한 경우 또는 쿼리에서 특정 오류 코드(예: Unavailable 또는 Busy)를 반환하는 경우 어플라이언스는 목록에 있는 다음 LDAP 서버에 연결하려고 시도합니다. 기본적으로 어플라이언스는 항상 목록에 있는 첫 번째 서버에 연결하려고 시도하며, 나열된 순서대로 각각의 다음 서버에 연결하려고 시도합니다. 어플라이언스가 기본적으로 주 LDAP 서버에 연결하도록 하려면 LDAP 서버 목록에 해당 서버를 첫 번째 서버로 입력하십시오.

어플라이언스는 두 번째 또는 그 이후의 LDAP 서버에 연결하는 경우 시간 초과 기간에 도달할 때까지 해당 서버에 연결된 상태를 유지합니다. 시간 초과에 도달하면 목록의 첫 번째 서버에 다시 연결하려고 시도합니다.

참고 지정된 LDAP 서버를 쿼리하는 시도만 페일오버합니다. 지정된 LDAP 서버와 연결된 리퍼럴 또는 연속 서버에 대한 쿼리 시도는 페일오버하지 않습니다.

관련 주제

- 어플라이언스에서 LDAP 장애 조치 구성, 781 페이지

어플라이언스에서 LDAP 장애 조치 구성

어플라이언스에서 LDAP 장애 조치를 구성하려면 GUI에서 다음 단계를 수행합니다.

단계 **1** System Administration(시스템 관리) > LDAP에서 수정할 LDAP 서버 프로필을 선택합니다.

단계 **2** LDAP 서버 프로필에서 다음 설정을 구성합니다.

숫자	설명
1	LDAP 서버 나열
2	최대 연결 수 구성

단계 **3** 다른 LDAP 설정을 구성하고 변경 사항을 커밋합니다.

부하 균형

LDAP 연결을 LDAP 서버 그룹으로 분산하려면 LDAP 프로필에서 부하분산을 구성할 수 있습니다.

LDAP 프로필에서 부하분산을 구성하면 어플라이언스는 나열된 LDAP 서버로 연결을 분산합니다. 연결이 실패하거나 시간이 초과되면 어플라이언스는 어떤 LDAP 서버가 사용 가능한지 확인한 후 사용 가능한 서버에 다시 연결합니다. 어플라이언스는 사용자가 구성한 최대 연결 수를 기반으로 설정할 수 있는 동시 연결 수를 결정합니다.

나열된 LDAP 서버 중 하나가 응답하지 않으면 어플라이언스는 나머지 LDAP 서버로 연결을 분산합니다.

관련 항목

- 어플라이언스에서 부하 분산 구성, 782 페이지

어플라이언스에서 부하 분산 구성

단계 **1** **System Administration**(시스템 관리) **> LDAP**에서 수정할 LDAP 서버 프로파일을 선택합니다.

단계 **2** LDAP 서버 프로필에서 다음 설정을 구성합니다.

숫자	설명
1	LDAP 서버 나열
2	최대 연결 수 구성

단계 **3** 다른 LDAP 설정을 구성하고 변경 사항을 커밋합니다.

30 장

클라이언트 인증서를 사용하여 SMTP 세션 인증

이 장에는 다음 섹션이 포함되어 있습니다.

인증서 및 SMTP 인증 개요

Email Security Appliance는 클라이언트 인증서를 사용하여 Email Security Appliance와 사용자의 메일 클라이언트 간 SMTP 세션을 인증하도록 지원합니다. Email Security Appliance는 애플리케이션이 메시지를 전송하기 위해 어플라이언스에 연결을 시도할 때 사용자의 메일 클라이언트로부터 클라이언트 인증서를 요청할 수 있습니다. 어플라이언스는 클라이언트 인증서를 수신하면 인증서가 유효한지, 만료되지 않았는지, 폐기되지 않았는지를 확인합니다. 인증서가 유효하면 Email Security Appliance는 TLS를 통한 메일 애플리케이션의 SMTP 연결을 허용합니다.

사용자들에게 메일 클라이언트에 CAC(Common Access Card)를 사용하도록 요구하는 조직은 CAC 및 ActivClient 미들웨어 애플리케이션이 어플라이언스에 제공할 인증서를 요청하도록 Email Security Appliance를 구성하기 위해 이 기능을 사용할 수 있습니다.

사용자에게 메일을 전송할 때 인증서를 제공하도록 요청하되 일부 사용자는 제외하도록 Email Security Appliance를 구성할 수 있습니다. 이러한 사용자에 대해서는 SMTP 인증 LDAP 쿼리를 사용하여 사용자를 인증하도록 어플라이언스를 구성할 수 있습니다.

사용자는 안전한 연결(TLS)을 통해 메시지를 전송하고 어플라이언스에서 오는 서버 인증서를 수락하도록 메일 클라이언트를 구성해야 합니다.

관련 주제

- 클라이언트 인증서로 사용자를 인증하는 방법, 784 페이지

클라이언트 인증서로 사용자를 인증하는 방법

표 ***79:*** 클라이언트 인증서로 사용자를 인증하는 방법

	수행해야 할 작업	추가 정보
1단계	LDAP 서버용 인증서 쿼리를 정의합니다.	클라이언트 인증서의 유효성 확인, 785 페이지
2단계	인증서 기반 SMTP 인증 프로필을 만듭니다.	클라이언트 인증서를 사용하여 TLS를 통해 SMTP 연결 인증, 786 페이지
3단계	인증서 SMTP 인증 프로필을 사용하도록 리스너를 구성합니다.	웹 인터페이스를 사용하여 리스너를 만들어 연결 요청 수신 대기, 75 페이지
4단계	TLS, 클라이언트 인증서 및 SMTP 인증을 요청하도록 RELAYED 메일 플로우 정책을 수정합니다.	어플라이언스에서 TLS 연결 설정, 787 페이지

SMTP 인증 LDAP 쿼리로 사용자를 인증하는 방법

표 ***80: SMTP*** 인증 ***LDAP*** 쿼리로 사용자를 인증하는 방법

	수행해야 할 작업	추가 정보
1단계	허용 쿼리 문자열을 사용하는 서버에 대한 SMTP 인증 쿼리를 정의하고 인증 방법에 바인딩합니다.	LDAP Directory를 사용하여 사용자 인증, 786 페이지
2단계	LDAP 기반 SMTP 인증 프로필을 만듭니다.	SMTP 인증을 위해 AsyncOS 구성, 765 페이지
3단계	LDAP SMTP 인증 프로필을 사용하도록 리스너를 구성합니다.	연결에 LDAP 기반 SMTP 인증을 사용하도록 허용되지 않은 사용자의 경우 어플라이언스에서 연결을 거부할지, 아니면 모든 활동을 로깅하면서 일시적으로 연결을 허용할지를 선택할 수 있습니다.
4단계	TLS 및 SMTP 인증을 요청하도록 RELAYED 메일 플로우 정책을 수정합니다.	어플라이언스에서 TLS 연결 설정, 787 페이지

클라이언트 인증서가 유효하지 않은 경우 LDAP SMTP 인증 쿼리로 사용자를 인증하는 방법

표 ***81:*** 클라이언트 인증서 또는 ***LDAP SMTP*** 인증 쿼리로 사용자를 인증하는 방법

	수행해야 할 작업	추가 정보
1단계	허용 쿼리 문자열을 사용하는 서버에 대한 SMTP 인증 쿼리를 정의하고 인증 방법에 바인딩합니다.	LDAP Directory를 사용하여 사용자 인증, 786 페이지
2단계	LDAP 서버용 인증서 기반 쿼리를 정의합니다.	클라이언트 인증서의 유효성 확인, 785 페이지
3단계	인증서 기반 SMTP 인증 프로필을 만듭니다.	클라이언트 인증서를 사용하여 TLS를 통해 SMTP 연결 인증, 786 페이지
4단계	LDAP SMTP 인증 프로필을 만듭니다.	SMTP 인증을 위해 AsyncOS 구성, 765 페이지
5단계	인증서 SMTP 인증 프로필을 사용하도록 리스너를 구성합니다.	웹 인터페이스를 사용하여 리스너를 만들어 연결 요청 수신 대기, 75 페이지
6단계	1. 다음 설정을 사용하도록 RELAYED 메일 흐름 정책을 수정합니다. 2. TLS Preferred(TLS 기본 설정) 3. SMTP authentication required(필수 SMTP 인증) 4. Require TLS for SMTP authentication(SMTP 인증에 TLS 필요)	어플라이언스에서 TLS 연결 설정, 787 페이지

클라이언트 인증서의 유효성 확인

Certificate Authentication LDAP 쿼리는 사용자의 메일 클라이언트와 Email Security Appliance 간 SMTP 세션을 인증하기 위해 클라이언트 인증서의 유효성을 확인합니다. 이 쿼리를 만들 때에는 인증할 인증서 필드 리스트를 선택하고, 사용자 ID 특성을 지정하고(기본값은 uid), 쿼리 문자열을 입력합니다.

예를 들어, 인증서의 CN 및 일련 번호를 검색하는 쿼리 문자열은 `(&(objectClass-posixAccount)(caccn={cn})(cacserial={sn})`과 같습니다. 쿼리를 만든 다음 인증서 SMTP 인증 프로필에서 사용할 수 있습니다. 이 LDAP 쿼리는 OpenLDAP, Active Directory 및 Oracle Directory를 지원합니다.

LDAP 서버 구성에 대한 자세한 내용은 LDAP 쿼리, 735 페이지를 참조해 주십시오.

단계 **1** **System Administration**(시스템 관리) > **LDAP**를 선택합니다.

단계 **2** 새 LDAP 프로필을 만듭니다. 자세한 내용은 LDAP 서버에 대한 정보를 저장할 LDAP 서버 프로필 만들기, 739 페이지를 참조해 주십시오.

단계 **3** **Certificate Authentication Query**(인증서 인증 쿼리) 확인란을 선택합니다.

단계 4 쿼리 이름을 입력합니다.

단계 5 사용자 인증서를 인증하기 위한 쿼리 문자열을 입력합니다. 예: **(&(objectClass=user)(cn={cn}))**

단계 6 **sAMAccountName**과 같은 사용자 ID 특성을 입력합니다.

단계 7 변경 사항을 제출 및 커밋합니다.

LDAP Directory를 사용하여 사용자 인증

SMTP 인증 LDAP 쿼리에는 허용 쿼리 문자열(Allowance Query String)이 있습니다. 이 문자열을 통해 Email Security Appliance는 LDAP 디렉터리에 있는 사용자의 레코드를 기반으로 사용자의 메일 클라이언트가 어플라이언스를 통해 메일을 전송하도록 허용되는지를 확인할 수 있습니다. 따라서 허용된다고 지정한 레코드가 있는 한, 클라이언트 인증서가 없는 사용자도 메일을 전송할 수 있습니다.

다른 특성을 기반으로 결과를 필터링할 수도 있습니다. 예를 들어 `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))` 쿼리 문자열은 사용자에 대해 다음 조건이 true인지 확인합니다.

- CAC가 사용자에게 발급되지 않음 `(caccn=*)`
- CAC가 exempt임 `(cacexempt=*)`
- 사용자가 CAC 없이 일시적으로 메일을 전송할 수 있는 기간이 미래에 만료됨 `(cacemergency>={t})`

SMTP 인증 쿼리 사용에 대한 자세한 내용은 SMTP 인증을 위해 AsyncOS 구성, 765 페이지 항목을 참고하십시오.

단계 1 **System Administration**(시스템 관리) > **LDAP**를 선택합니다.

단계 2 LDAP 프로파일을 정의합니다. 자세한 내용은 LDAP 서버에 대한 정보를 저장할 LDAP 서버 프로필 만들기, 739 페이지를 참조하십시오.

단계 3 LDAP 프로파일에 대한 SMTP 인증 쿼리를 정의합니다.

단계 4 SMTP Authentication Query(SMTP 인증 쿼리) 확인란을 선택합니다.

단계 5 쿼리 이름을 입력합니다.

단계 6 사용자 ID를 쿼리할 문자열을 입력합니다. 예: `(uid={u})`

단계 7 인증 방법으로 LDAP BIND를 선택합니다.

단계 8 허용 쿼리 문자열을 입력합니다. 예: `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`

단계 9 변경 사항을 제출 및 커밋합니다.

클라이언트 인증서를 사용하여 TLS를 통해 SMTP 연결 인증

인증서 기반 SMTP 인증 프로필은 Email Security Appliance가 클라이언트 인증서를 사용하여 TLS를 통해 SMTP 연결을 인증하도록 허용합니다. 프로필을 만들 때 인증서 확인에 사용할 인증서 인증 LDAP 쿼리를 선택합니다. 또한 클라이언트 인증서를 사용할 수 없는 경우 Email Security Appliance가 사용자 인증을 위해 **SMTP AUTH** 명령으로 대체할지 여부를 지정할 수 있습니다.

LDAP를 사용한 SMTP 연결 인증에 대한 자세한 내용은 SMTP 인증을 위해 AsyncOS 구성, 765 페이지 섹션을 참조해 주십시오.

단계 **1** **Network**(네트워크) > **SMTP Authentication**(SMTP 인증)을 선택합니다.

단계 **2** **Add Profile**(프로필 추가)을 클릭합니다.

단계 **3** SMTP 인증 프로파일의 이름을 입력합니다.

단계 **4** Profile Type(프로필 유형)으로 **Certificate**(인증서)를 선택합니다.

단계 **5** **Next**(다음)를 클릭합니다.

단계 **6** 프로파일 이름을 입력합니다.

단계 **7** 이 SMTP 인증 프로필과 함께 사용할 인증서 LDAP 쿼리를 선택합니다.

참고 클라이언트 인증서를 사용할 수 없을 경우 SMTP AUTH 명령을 허용하기 위한 옵션을 선택하지 않습니다.

단계 **8** **Finish**를 클릭합니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

어플라이언스에서 **TLS** 연결 설정

RELAYED 메일 플로우 정책의 Verify Client Certificate(클라이언트 인증서 확인) 옵션은 클라이언트 인증서가 유효한 경우 사용자 메일 애플리케이션에 대한 TLS 연결을 설정하도록 Email Security Appliance에 지시합니다. TLS Preferred(TLS 기본 설정) 설정에 이 옵션을 선택한 경우, 사용자에게 인증서가 없으면 어플라이언스는 비 TLS 연결을 허용하지만 사용자가 잘못된 인증서를 가지고 있으면 연결을 거부합니다. TLS Required(TLS 필수) 설정에 이 옵션을 선택하는 경우, 어플라이언스에서 연결을 허용하려면 사용자에게 유효한 인증서가 있어야 합니다.

클라이언트 인증서로 사용자의 SMTP 세션을 인증하려면 다음 설정을 선택합니다.

- TLS - Required(TLS - 필수)
- Verify Client Certificate(클라이언트 인증서 확인)
- Require SMTP Authentication(SMTP 인증 요청)

참고 SMTP 인증이 필요하더라도 Email Security Appliance는 인증서 인증을 사용하므로 SMTP 인증 LDAP 쿼리를 사용하지 않습니다.

클라이언트 인증서 대신 SMTP 인증 쿼리를 사용하여 사용자의 SMTP 세션을 인증하려면 RELAYED 메일 플로우 정책에 대해 다음 설정을 선택합니다.

- TLS - Required(TLS - 필수)
- Require SMTP Authentication(SMTP 인증 요청)

Email Security Appliance에서 특정 사용자에게는 클라이언트 인증서를 요구하고 다른 사용자로부터는 LDAP 기반 SMTP 인증을 허용하도록 하려면 RELAYED 메일 플로우 정책에 대해 다음 설정을 선택합니다.

- TLS - Preferred(TLS - 기본 설정)
- Require SMTP Authentication(SMTP 인증 요청)
- Require TLS to Offer SMTP Authentication(TLS에 SMTP 인증을 제공하도록 요구)

폐기된 인증서 리스트 업데이트

Email Security Appliance는 사용자의 인증서가 폐기되지 않았는지를 확인하기 위한 인증서 폐기 과정의 일부로 폐기된 인증서 리스트(일명 Certificate Revocation List)를 확인합니다. 서버에 이 리스트의 최신 버전을 올려두면 Email Security Appliance는 지정된 일정에 따라 이를 다운로드합니다.

단계 **1** **Network(**네트워크**) > CRL Sources(CRL** 소스**)**로 이동합니다.

단계 **2** SMTP TLS 연결에 대한 CRL 확인을 활성화합니다.

a) Global Settings(전역 설정) 아래에서 Edit Settings(설정 수정)를 클릭합니다.

b) (선택 사항) 모든 옵션을 선택하려면 **Global Settings(**전역 설정**)** 확인란을 선택합니다.

- 인바운드 SMTP TLS에 대한 CRL 확인
- 아웃바운드 SMTP TLS에 대한 CRL 확인
- 웹 인터페이스에 대한 CRL 확인

c) 'CRL check for inbound SMTP TLS(인바운드 SMTP TLS에 대한 CRL 확인)', 'CRL check for outbound SMTP TLS(아웃바운드 SMTP TLS에 대한 CRL 확인)' 또는 'CRL Check for Web Interface(웹 인터페이스에 대한 CRL 확인)' 옵션에 대한 확인란을 선택합니다.

d) 변경사항을 제출합니다.

단계 **3** **Add CRL Source(CRL** 소스 추가**)**를 클릭합니다.

단계 **4** CRL 소스의 이름을 입력합니다.

단계 **5** 파일 형식을 선택합니다. ASN.1 또는 PEM이 될 수 있습니다.

단계 **6** 파일 이름을 포함하여 파일의 주요 소스에 대한 URL을 입력합니다. 예: **`https://crl.example.com/certs.crl`**

단계 **7** 선택적으로, 어플라이언스가 주요 소스에 연결할 수 없는 경우 사용할 보조 소스의 URL을 입력합니다.

단계 **8** CRL 소스를 다운로드할 일정을 지정합니다.

단계 **9** CRL 소스를 활성화합니다.

단계 **10** 변경 사항을 제출 및 커밋합니다.

클라이언트 인증서로 사용자의 **SMTP** 세션 인증

단계 **1** **System Administration(**시스템 관리**) > LDAP**로 이동하여 LDAP 서버 프로파일을 구성합니다.

단계 **2** LDAP 프로파일에 대한 인증서 쿼리를 정의합니다.

a) 쿼리 이름을 입력합니다.
b) 일련 번호 및 일반 이름과 같이 인증을 위한 인증서 필드를 선택합니다.
c) 쿼리 문자열을 입력합니다. 예: **`(&(caccn={cn})(cacserial={sn}))`**
d) uid와 같은 사용자 ID 필드를 입력합니다.
e) 변경 사항을 제출합니다.

단계 **3** **Network > SMTP Authentication(**네트워크 **> SMTP** 인증**)**으로 이동하여 Certificate SMTP 인증 프로필을 구성합니다.

a) 프로필 이름을 입력합니다.
b) 사용할 인증서 LDAP 쿼리를 선택합니다.
c) 클라이언트 인증서를 사용할 수 없을 경우 **`SMTP AUTH`** 명령을 허용하기 위한 옵션을 선택하지 않습니다.
d) 변경 사항을 제출합니다.

단계 **4** **Network > Listeners(**네트워크 **>** 리스너**)**로 이동하여, 자신이 만든 인증서 SMTP 인증 프로필을 사용할 리스너를 구성합니다.

단계 **5** TLS, 클라이언트 인증서 및 SMTP 인증을 요청하도록 RELAYED 메일 플로우 정책을 수정합니다.

참고 SMTP 인증이 필요하더라도 Email Security Appliance는 인증서 인증을 사용하므로 SMTP AUTH 명령을 사용하지 않습니다. Email Security Appliance는 사용자 인증을 위해 메일 애플리케이션으로부터 클라이언트 인증서를 요청합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

SMTP AUTH 명령으로 사용자의 **SMTP** 세션 인증

Email Security Appliance는 클라이언트 인증서 대신 사용자의 SMTP 세션을 인증하기 위해 SMTP AUTH 명령을 사용할 수 있습니다. 연결에 SMTP AUTH를 사용하도록 허용되지 않은 사용자의 경우 어플라이언스에서 연결을 거부할지, 아니면 모든 활동을 로깅하면서 일시적으로 연결을 허용할지를 선택할 수 있습니다.

단계 **1** **System Administration(**시스템 관리**) > LDAP**로 이동하여 LDAP 서버 프로필을 구성합니다.

단계 **2** LDAP 프로필에 대한 SMTP 인증 쿼리를 정의합니다.

a) 쿼리 이름을 입력합니다.
b) 쿼리 문자열을 입력합니다. 예: **`(uid={u})`**
c) 인증 방법으로 LDAP BIND를 선택합니다.
d) 허용 쿼리 문자열을 입력합니다. 예:
`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`.

e) 변경 사항을 제출합니다.

단계 **3** **Network > SMTP Authentication(**네트워크 **> SMTP** 인증**)**으로 이동하여 LDAP SMTP 인증 프로필을 구성합니다.

a) 프로필 이름을 입력합니다.
b) 사용할 SMTP 인증 LDAP 쿼리를 선택합니다.
c) 사용자가 SMTP AUTH 명령을 사용하도록 허용하려면 Check with LDAP(LDAP로 확인)를 선택하고, 사용자 활동을 모니터링 및 보고하도록 선택합니다.
d) 변경 사항을 제출합니다.

단계 **4** **Network > Listeners(**네트워크 **>** 리스너**)**로 이동하여, 자신이 만든 LDAP SMTP 인증 프로필을 사용할 리스너를 구성합니다.

단계 **5** TLS 및 SMTP 인증을 요청하도록 RELAYED 메일 플로우 정책을 수정합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

클라이언트 인증서 또는 **SMTP AUTH**로 사용자의 **SMTP** 세션 인증

이 컨피그레이션에서 Email Security Appliance는 클라이언트 인증서가 있는 사용자에게는 클라이언트 인증서를 요청하고, 클라이언트 인증서가 없거나 이를 이메일 전송에 사용할 수 없는 사용자에게는 SMTP AUTH를 허용합니다.

허용되지 않은 사용자가 SMTP AUTH 명령을 사용하려는 시도는 금지됩니다.

단계 **1** **System Administration(**시스템 관리**) > LDAP**로 이동하여 LDAP 서버 프로필을 구성합니다.

단계 **2** 프로필에 대한 SMTP 인증 쿼리를 정의합니다.

a) 쿼리 이름을 입력합니다.
b) 쿼리 문자열을 입력합니다. 예: **`(uid={u})`**
c) 인증 방법으로 LDAP BIND를 선택합니다.
d) 허용 쿼리 문자열을 입력합니다. 예:
`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`.

단계 **3** LDAP 프로파일에 대한 인증서 쿼리를 정의합니다.

a) 쿼리 이름을 입력합니다.
b) 일련 번호 및 일반 이름과 같이 인증을 위한 클라이언트 인증서 필드를 선택합니다.
c) 쿼리 문자열을 입력합니다. 예: **`(&(caccn={cn})(cacserial={sn}))`**
d) 사용자 ID 필드를 입력합니다(예: uid).
e) 변경 사항을 제출합니다.

단계 **4** **Network > SMTP Authentication(**네트워크 **> SMTP** 인증**)**으로 이동하여 LDAP SMTP 인증 프로필을 구성합니다.

a) 프로필 이름을 입력합니다.
b) 사용할 SMTP 인증 LDAP 쿼리를 선택합니다.
c) 사용자가 SMTP AUTH 명령을 사용할 수 있고 연결을 거부하도록 선택한 경우 Check with LDAP(LDAP를 사용하여 검사)를 선택합니다

d) 맞춤형 SMTP AUTH 응답을 입력합니다. 예를 들어 다음과 같이 입력합니다. 525, “Dear user, please use your CAC to send email.”
e) 변경사항을 제출합니다.

단계 **5** 인증서 SMTP 인증 프로파일을 구성합니다.

a) 프로파일 이름을 입력합니다.
b) 사용할 인증서 LDAP 쿼리를 선택합니다.
c) 클라이언트 인증서를 사용할 수 없는 경우 SMTP AUTH 명령을 허용하는 옵션을 선택하십시오.
d) 사용자에게 클라이언트 인증서가 없는 경우 어플라이언스에서 사용할 LDAP SMTP 인증 프로파일을 선택합니다.
e) 변경 사항을 제출합니다.

단계 **6** **Network > Listeners(**네트워크 > 리스너**)**로 이동하여, 자신이 만든 인증서 SMTP 인증 프로필을 사용할 리스너를 구성합니다.

단계 **7** 다음 옵션을 선택하도록 RELAYED 메일 흐름 정책을 수정합니다.

- TLS 기본 설정
- SMTP 인증 필요
- SMTP 인증에 TLS 필요

단계 **8** 변경 사항을 제출 및 커밋합니다.

31 장

이메일 보안 모니터 사용

이 장에는 다음 섹션이 포함되어 있습니다.

이메일 보안 모니터 개요

Email Security Monitor(이메일 보안 모니터) 기능은 이메일 전달 프로세스의 각 단계에서 데이터를 수집합니다. 데이터베이스는 IP 주소별로 각 이메일 발신자를 식별 및 기록하는 한편, SenderBase Reputation Service와 실시간 식별 정보에 대해 상호 작용합니다. 이메일 발신자의 로컬 메일 플로우 기록에 대해 즉시 보고할 수 있으며 인터넷에 있는 발신자의 전역 레코드를 포함하는 프로필을 표시할 수 있습니다. 이메일 보안 모니터 기능을 이용하여 보안 팀은 회사 사용자에게 메일을 보내는 사람, 회사 사용자가 보내고 받는 메일의 양, 보안 정책의 효율성 등을 "확실히 정리"할 수 있습니다.

이 장에서는 다음 방법에 대해 설명합니다.

- 인바운드 및 아웃바운드 메시지 플로우를 모니터링하기 위해 이메일 보안 모니터 기능에 액세스하는 방법.
- 발신자의 SBRS(SenderBase Reputation Score)를 쿼리하여 메일 플로우 정책 결정을 내리는 방법(화이트리스트, 블랙리스트 및 그레이리스트 업데이트). 네트워크 소유자, 도메인 및 심지어 개별 IP 주소도 쿼리할 수 있습니다.
- 메일 플로우, 시스템 상태, 네트워크에서 보내고 받는 메일에 대해 보고하는 방법.

수신 메일에 대한 특정 이메일 발신자에 대해 이메일 보안 모니터 데이터베이스는 다음과 같은 중요한 매개변수를 캡처합니다.

- 메시지 볼륨
- 연결 기록
- 수락된 연결 대 거부된 연결
- 수락 비율 및 조절(throttle) 제한

- 발신자 평판 필터 일치
- 의심스런 스팸과 명확하게 식별된 스팸에 대한 안티스팸 메시지 수
- 안티바이러스 검사에서 탐지된 바이러스 양성 메시지 수

안티스팸 검사에 대한 자세한 내용은 Anti-Spam, 355 페이지, 안티바이러스 검사에 대한 자세한 내용은 Anti-Virus, 335 페이지 항목을 참고하십시오.

또한 이메일 보안 모니터 기능은 메시지를 주고받는 내부 사용자(이메일 수신자)를 포함하여 특정 메시지가 어떤 콘텐츠 필터를 트리거하는지에 대한 정보를 캡처합니다.

이메일 보안 모니터 기능은 GUI에서만 사용할 수 있으며, 이메일 트래픽 및 어플라이언스의 상태(격리, 작업 대기열 및 전파 확산 포함)에 대한 보기를 제공합니다. 어플라이언스는 발신자가 정상적인 트래픽 프로필을 언제 벗어나는지를 식별합니다. 인터페이스에서 강조 표시되지 않은 사용자에 대해서는 발신자 그룹에 할당하거나 발신자의 액세스 프로필을 수정하여 올바른 작업을 수행할 수 있습니다. 또는 AsyncOS의 보안 서비스에서 계속 반응하고 대처하도록 할 수도 있습니다. 아웃바운드 메일에도 유사한 모니터링 기능이 있어서, 이를 통해 메일 대기열에 있는 상위 도메인 및 수신 호스트의 상태를 볼 수 있습니다(Delivery Status Details(전달 상태 세부사항) 페이지, 811 페이지 참조).

참고 어플라이언스가 재부팅될 때 작업 대기열에 있던 메시지에 대한 정보는 이메일 보안 모니터 기능에서 보고하지 않습니다.

관련 주제

- 이메일 보안 모니터 및 중앙 집중식 관리, 794 페이지

이메일 보안 모니터 및 중앙 집중식 관리

집계된 보고서 데이터를 보려면 Cisco Content Security Management Appliance를 배포합니다.

클러스터링된 어플라이언스의 이메일 보안 모니터 보고서는 집계할 수 없습니다. 모든 보고서는 시스템 레벨로 제한됩니다. 즉, 그룹 또는 클러스터 레벨에서는 실행할 수 없고 개별 시스템에서만 실행할 수 있습니다.

Archived Reports(보관된 보고서) 페이지도 마찬가지입니다. 각 해당 시스템에 자체 아카이브가 있습니다. 따라서 "Generate Report(보고서 생성)" 기능은 선택한 시스템에서 실행됩니다.

Scheduled Reports(예약된 보고서) 페이지는 시스템 레벨로 제한되지 않으므로, 설정을 여러 시스템에서 공유할 수 있습니다. 개별 예약된 보고서는 대화형 보고서처럼 시스템 레벨에서 실행되므로, 클러스터 레벨에서 예약된 보고서를 구성하는 경우 클러스터의 각 시스템이 자체 보고서를 전송합니다.

"Preview This Report(이 보고서 미리 보기)" 버튼은 항상 로그인 호스트에 대해 실행됩니다.

이메일 보안 모니터 페이지

이메일 보안 모니터 기능은 Quarantines(격리) 페이지를 제외하고 Monitor(모니터) 메뉴에서 사용할 수 있는 모든 페이지로 구성됩니다.

GUI에서 이러한 페이지를 사용하여 어플라이언스의 리스너에 연결된 도메인을 모니터링할 수 있습니다. 어플라이언스의 "메일 플로우"를 모니터링, 정렬, 분석 및 분류할 수 있고, 합법적인 메일의 대용량 발신자와 잠재적인 "스패머"(대용량의 원치 않는 상업 이메일 발신자) 또는 바이러스 발신자와 구별할 수 있습니다. 이러한 페이지는 시스템에 대한 인바운드 연결 문제를 해결하는 데에도 도움이 됩니다(SBRS 점수, 도메인에 대한 최신 발신자 그룹 일치 등 중요한 정보 포함).

또한 어플라이언스를 기준으로 메일을 분류하고 게이트웨이 범위를 넘어 존재하는 서비스, 즉 SenderBase Reputation Service, 안티스팸 검사 서비스, 안티바이러스 검사 보안 서비스, 콘텐츠 필터, Outbreak Filter 등을 기준으로 메일을 분류하는 데에도 도움이 됩니다.

페이지 상단 우측에 있는 Printable PDF(인쇄 가능한 PDF) 링크를 클릭하여 이메일 보안 모니터 페이지 중 하나에 대해 인쇄하여 보기 편한 형식의 .PDF 버전을 생성할 수 있습니다. 영어 이외의 언어로 PDF를 생성하는 방법에 대한 자세한 내용은 보고서에 대한 참고 사항, 832 페이지 섹션을 참조하십시오.

Export(내보내기**)** 링크를 통해 그래프 및 기타 데이터를 CSV(comma separated values) 형식으로 내보낼 수 있습니다.

내보낸 CSV 데이터는 Email Security Appliance의 설정과 상관없이 모든 메시지 추적 및 보고 데이터를 GMT로 표시합니다. GMT 시간 변환의 목적은 어플라이언스와 독립적으로 또는 여러 표준 시간대의 어플라이언스에서 데이터를 참조하는 시기와 독립적으로 데이터를 사용하도록 하려는 것입니다.

참고

현지화된 CSV 데이터를 내보내는 경우 일부 브라우저에서 제목이 제대로 표시되지 않을 수 있습니다. 이 문제는 일부 브라우저에서 현지화된 텍스트의 정확한 문자 집합을 사용하지 않았기 때문에 발생할 수 있습니다. 이 문제를 해결하려면 파일을 디스크에 저장하고 File(파일) > Open(열기)을 사용하여 열 수 있습니다. 파일을 열 때 현지화된 텍스트를 표시하기 위한 문자 집합을 선택합니다.

보고서 데이터 내보내기의 자동화에 대한 자세한 내용은 CSV 데이터 검색, 829 페이지 섹션을 참조하십시오.

이메일 보안 모니터 페이지의 목록

- My Dashboard(내 대시보드) 페이지 , 797 페이지
- Overview(개요) 페이지, 799 페이지
- Incoming Mail(수신 메일) 페이지, 802 페이지
- Outgoing Destinations(발신 대상), 809 페이지
- Outgoing Senders(발신 발신자), 809 페이지
- Delivery Status(전달 상태) 페이지, 810 페이지
- Internal Users(내부 사용자) 페이지, 811 페이지
- DLP Incidents(DLP 인시던트) 페이지, 813 페이지
- Content Filters(콘텐츠 필터) 페이지, 814 페이지

검색 및 이메일 보안 모니터

다수의 이메일 보안 모니터 페이지에는 검색 양식이 포함되어 있습니다. 서로 다른 항목 유형을 검색할 수 있습니다.

- IP 주소(IPv4 및 IPv6)
- 도메인
- 네트워크 소유자
- 내부 사용자
- 대상 도메인
- 내부 발신자 도메인
- 내부 발신자 IP 주소
- 발신 도메인 전달 상태

도메인, 네트워크 소유자 및 내부 사용자 검색의 경우 검색 텍스트와 정확한 일치를 찾을지 아니면 입력한 텍스트로 시작하는 항목을 찾을지(예: "ex"로 시작하면 "example.com"이 검색됨)를 선택합니다.

IPv4 주소 검색의 경우, 입력한 텍스트는 점 십진수 형식에서 최대 4개의 IP 옥텟으로 시작하는 것으로 해석됩니다. 예를 들어 "17"은 17.0.0.0~17.255.255.255 범위에서 검색하므로, 17.0.0.1은 일치하지만 172.0.0.1은 일치하지 않습니다. 정확한 일치를 검색하려면 네 개의 옥텟을 모두 입력하면 됩니다. IP 주소 검색은 CIDR 형식(17.16.0.0/12)도 지원합니다.

IPv6 주소 검색의 경우, AsyncOS는 다음 형식을 지원합니다.

- 2001:db8:2004:4202::0-2001:db8:2004:4202::ff
- 2001:db8:2004:4202::
- 2001:db8:2004:4202::23
- 2001:db8:2004:4202::/64

모든 검색은 페이지에 현재 선택된 시간 범위의 영향을 받습니다.

보고서에 포함된 메시지 세부사항 보기

이 기능은 보고와 추적이 모두 로컬인 경우에만 작동합니다(Cisco Content Security Management Appliance의 중앙 집중식이 아니라).

단계 **1** 보고서 페이지 테이블에서 파란색 숫자를 클릭합니다.

(모든 테이블이 이러한 링크가 있는 것은 아닙니다.)

해당 숫자에 포함된 메시지가 Message Tracking(메시지 추적)에 표시됩니다.

단계 **2** 아래로 스크롤하여 목록을 표시합니다.

다음에 수행할 작업

관련 주제

- 메시지 추적 검색 결과 작업 , 841 페이지

My Dashboard(내 대시보드) 페이지

기존 보고서 페이지의 차트(그래프)와 테이블을 조합하여 맞춤형 이메일 보안 보고서 페이지를 생성할 수 있습니다.

변경 후	수행해야 할 작업
맞춤형 보고서 페이지에 모듈 추가	1. **Monitor(**모니터**) > Email or Web(**이메일 또는 웹**) > Reporting(**보고**) > My Dashboard(**내 대시보드**)**로 이동하고, 모듈 상단 우측에 있는 **[X]**를 클릭하여 필요 없는 샘플 모듈을 삭제합니다. 2. 다음 중 하나를 수행합니다. • Monitor(모니터) 메뉴 아래에서 보고서 페이지의 모듈에 대한 **[+]** 버튼을 클릭하여 맞춤형 보고서에 모듈을 추가합니다. • **Monitor(**모니터**) > Email or Web(**이메일 또는 웹**) > Reporting(**보고**) > My Dashboard(**내 대시보드**)**로 이동하고, 섹션 중 하나에서 **[+]** 버튼을 클릭한 다음, 추가할 보고서 모듈을 선택합니다. 원하는 보고서를 찾으려면 각 섹션에서 **+ Report Module in(**다음의 보고서 모듈 **+)**을 선택해야 할 수 있습니다. 3. 모듈이 기본 설정으로 추가됩니다. 사용자 지정한 모듈을 추가하는 경우(예: 열을 추가, 삭제 또는 순서 변경), 추가한 후 이러한 모듈을 다시 사용자 지정합니다. 원래 모듈의 시간 범위는 유지되지 않습니다. 4. 별도의 범례가 포함된 차트를 추가하는 경우(예: Overview(개요) 페이지의 그래프) 범례를 따로 추가합니다. 필요한 경우, 설명하는 데이터 옆으로 끌어다 놓습니다. 참고: • 일부 보고서 페이지의 몇몇 모듈은 위의 방법 중 하나를 통해서만 사용할 수 있습니다. 한 방법으로 모듈을 추가할 수 없으면 다른 방법을 시도해보십시오. • 각 모듈을 한 번만 추가할 수 있습니다. 보고서에 특정 모듈을 이미 추가한 경우, 해당 추가 옵션은 사용할 수 없는 상태가 됩니다.
사용자 지정 보고서 페이지 보기	1. **Monitor(**모니터**) > Email or Web(**이메일 또는 웹**) > Reporting(**보고**) > My Dashboard(**내 대시보드**)**를 선택합니다. 2. Time Range(시간 범위) 섹션의 보고서: 모든 보고서 페이지에 대해 선택한 시간 범위는 My Dashboard(내 대시보드) 페이지에 있는 모든 모듈에 적용됩니다. 보려는 시간 범위를 선택합니다. 새로 추가된 모듈은 관련 섹션의 상단에 나타납니다.
맞춤형 보고서 페이지에서 모듈 정돈	모듈을 원하는 위치로 끌어다 놓습니다.
맞춤형 보고서 페이지에서 모듈 삭제	모듈의 상단 우측에 있는 [X]를 클릭합니다.

Overview(개요) 페이지

Overview(개요) 페이지는 격리의 개요와 Outbreak Filter 상태(페이지의 System Overview(시스템 개요) 섹션)를 포함하여 어플라이언스의 메시지 활동 요약을 제공합니다. 개요 페이지에는 수신 및 발신 메시지에 대한 자세한 메시지 개수 및 그래프도 포함되어 있습니다. 이 페이지를 사용하여 게이트웨이를 드나드는 모든 메일의 플로우를 모니터링할 수 있습니다.

Overview(개요) 페이지에서는 수신 메일에 대해 어플라이언스가 SenderBase Reputation Service와 통합된 방식이 강조 표시됩니다(예: 메시지가 평판 필터링에 의해 중단됨). **Overview(**개요**)** 페이지에서 다음을 수행할 수 있습니다.

- 게이트웨이를 드나드는 모든 메일 "플로우"의 메일 추세 그래프를 볼 수 있습니다.
- 시도된 메시지, 발신자 평판 필터링(SBRS)에 의해 중단된 메시지, 수신자가 잘못된 메시지, 스팸으로 표시된 메시지, 바이러스 양성으로 표시된 메시지, 깨끗한 메시지 등의 수를 시간별로 보여주는 그래프를 볼 수 있습니다.
- 시스템 상태 및 로컬 격리의 요약을 볼 수 있습니다.
- TOC(Threat Operations Center)에서 사용 가능한 정보를 기반으로 현재 바이러스 및 비 바이러스 전파 확산 정보를 볼 수 있습니다.

Overview(개요) 페이지는 System Overview(시스템 개요)와 Incoming and Outgoing Mail(수신 및 발신 메일) 그래프와 요약의 두 섹션으로 나누어집니다.

관련 주제

- 시스템 개요, 799 페이지
- 수신 및 발신 요약과 그래프, 800 페이지
- 이메일 범주화, 801 페이지
- 메시지 범주화 방법, 802 페이지

시스템 개요

Overview(개요) 페이지의 System Overview(시스템 개요) 섹션은 시스템 대시보드 역할을 하며 시스템과 작업 대기열 상태, 격리 상태, 전파 확산 활동 등 어플라이언스에 대한 세부사항을 제공합니다.

관련 주제

- Status(상태), 799 페이지
- 시스템 격리, 800 페이지
- 바이러스 위협 수준, 800 페이지

Status(상태)

이 섹션에서는 어플라이언스의 현재 상태 및 인바운드 메일 처리에 대한 개요를 제공합니다.

System Status(시스템 상태**)**: 다음 상태 중 하나

- 온라인
- 리소스 보존(conservation)
- 전송 일시 중단

- 수신 일시 중단
- 작업 대기열 일시 중지
- 오프라인

자세한 내용은 CLI를 사용한 관리 및 모니터링, 997 페이지을 참조하십시오.

Incoming Messages(수신 메시지**)**: 시간당 수신 메일의 평균 속도.

Work Queue(작업 대기열**)**: 작업 대기열에서 처리를 기다리고 있는 메시지의 수.

System Status(시스템 상태) 페이지로 이동하려면 System Status Details(시스템 상태 세부사항) 링크를 클릭합니다.

시스템 격리

이 섹션에는 어플라이언스의 디스크 사용량을 기준으로 상위 3개 격리에 대한 정보가 표시되며, 여기에는 격리 이름, 격리의 용량(디스크 공간), 현재 격리에 있는 메시지 수 등이 포함됩니다.

Local Quarantines(로컬 격리) 페이지로 이동하려면 Local Quarantines(로컬 격리) 링크를 클릭합니다.

바이러스 위협 수준

이 섹션에서는 TOC(Threat Operations Center)에서 보고한 Outbreak(전파 확산) 상태를 보여줍니다. 격리의 용량(디스크 공간), 현재 격리에 있는 메시지 수를 비롯한 Outbreak 격리의 상태도 보여줍니다. 어플라이언스에서 Outbreak Filters 기능을 활성화한 경우 Outbreak 격리만 표시됩니다.

참고 Threat Level(위협 수준) 표시기가 작동하려면 방화벽의 포트 80이 "**downloads.ironport.com**"에 대해 열려 있어야 합니다. 또는 로컬 업데이트 서버를 지정한 경우 Threat Level(위협 레벨) 표시기는 해당 주소를 사용하려고 시도합니다. Service Updates(서비스 업데이트) 페이지를 통해 다운로드하도록 프록시를 구성한 경우 위협 레벨 표시기가 올바르게 업데이트됩니다. 자세한 내용은 서비스 업데이트 , 945 페이지를 참고하십시오.

외부 TOC(Threat Operations Center) 웹사이트를 보려면 Outbreak Details(Outbreak 세부사항) 링크를 클릭합니다. 이 링크가 작동하려면 어플라이언스가 인터넷에 액세스할 수 있어야 합니다. Separate Window(별도의 창) 아이콘은 클릭 시 링크가 별도의 창에서 열림을 나타냅니다. 이러한 창을 허용하려면 브라우저의 팝업 차단 설정을 구성해야 할 수 있습니다.

수신 및 발신 요약과 그래프

요약 섹션에서는 시스템에서 수행되는 모든 실시간 메일 활동에 액세스할 수 있습니다. 요약 섹션은 Outgoing Mail Graphs(발신 메일 그래프) 및 Mail Summaries(메일 요약)로 구성됩니다. Time Range(시간 범위) 메뉴를 통해 보고할 기간을 선택할 수 있습니다. 여기에서 선택한 시간 범위는 Email Security Monitor(이메일 보안 모니터) 페이지 전체에서 사용됩니다. 메시지의 각 유형 또는 범주에 대한 설명은 아래에 나와 있습니다(이메일 범주화, 801 페이지 참조).

메일 추세 그래프는 메일 플로우를 시각적으로 표현하는 반면, 요약 테이블은 동일한 정보를 숫자로 표시합니다. 요약 테이블에는 시도된 메시지, 위협 메시지 및 깨끗한 메시지의 총 개수와 함께 각 메시지 유형의 비율과 실제 수가 포함되어 있습니다.

발신 그래프 및 요약에서는 아웃바운드 메일에 대한 유사한 정보를 보여줍니다.

관련 주제

- 이메일 보안 모니터에서 메시지 수 계산 방법에 대한 참고 사항, 801 페이지

이메일 보안 모니터에서 메시지 수 계산 방법에 대한 참고 사항

이메일 보안 모니터가 수신 메일의 계산에 사용하는 방법은 메시지당 수신자 수를 기반으로 합니다. 예를 들어 example.com에서 오는 하나의 수신 메시지가 세 명의 수신자에게 전송되면 해당 발신자로부터 3개의 메시지가 오는 것으로 계산됩니다.

발신자 평판 필터링에 의해 차단된 메시지는 실제로 작업 대기열에 들어가지 못하므로, 어플라이언스는 수신 메시지에 대한 수신자 목록에 액세스하지 못합니다. 이 경우 수신자 수를 추적하기 위해 승수가 사용됩니다. 승수는 기존 고객 데이터의 대규모 샘플링을 조사하여 Cisco에서 결정합니다.

이메일 범주화

Overview and Incoming Mail(개요 및 수신 메일) 페이지에서 보고되는 메시지는 다음과 같이 범주화됩니다.

- **Stopped by Reputation Filtering(**평판 필터링에 의해 차단됨**)**: HAT 정책에 의해 차단된 모든 연결을 고정 승수로 곱하고(이메일 보안 모니터에서 메시지 수 계산 방법에 대한 참고 사항, 801 페이지 참조) 여기에 수신자 조절(throttling)에 의해 차단된 모든 수신자를 더한 수
- **Invalid Recipients(**잘못된 수신자**)**: 대화형 LDAP 거부에 의해 거부된 모든 수신자와 모든 RAT 거부를 더한 수
- **Spam Messages Detected(**탐지된 스팸 메시지**)**: 안티 스팸 검사 엔진에 의해 양성이거나 의심스러운 것으로 탐지된 메시지와 스팸 및 바이러스 모두 양성인 메시지의 총 개수
- **Virus Messages Detected(**탐지된 바이러스 메시지**)**: 바이러스 양성이며 스팸은 아닌 것으로 탐지된 메시지의 총 개수 및 비율

참고 검사할 수 없는 메시지 또는 암호화된 메시지를 전달하도록 안티바이러스 설정을 구성한 경우 이러한 메시지는 바이러스 양성이 아닌 정상 메시지로 계산됩니다. 그렇지 않은 경우 메시지는 바이러스 양성으로 계산됩니다.

- **Detected by Advanced Malware Protection(AMP**에 의해 탐지됨**)**: 파일 평판 필터링에 의해 악의적인 것으로 확인된 메시지 첨부 파일. 이 값에는 파일 분석에 의해 악의적인 것으로 확인된 판정 업데이트 또는 파일이 포함되어 있지 않습니다.
- **Messages with Malicious URLs(**악의적인 **URL**이 포함된 메시지**)**: URL 필터링에 의해 악의적인 것으로 확인된 메시지 내 하나 이상의 URL.
- **Stopped by Content Filter(**콘텐츠 필터에 의해 중단됨**)**: 콘텐츠 필터에 의해 중단된 총 메시지 수.
- **Stopped by DMARC(DMARC**에 의해 중단됨**)**: DMARC 확인 후 중단된 총 메시지 수.
- **S/MIME Verification/Decryption Failed(S/MIME** 확인/해독 실패**)**: S/MIME 확인, 해독 또는 둘 모두에 실패한 총 메시지 수.

- **S/MIME Verification/Decryption Successful(S/MIME** 확인/해독 성공**)**: S/MIME을 사용하여 성공적으로 확인, 해독, 또는 해독 및 확인된 총 메시지 수.
- **Clean Messages(**정상 메시지**)**: 수락되고 바이러스와 스팸이 없는 것으로 간주된 메일. 수신자별 검사 작업(예: 별도의 메일 정책으로 처리되는 분리된 메시지)을 고려하여 수락되는 깨끗한 메시지의 가장 정확한 표현. 그러나 스팸 또는 바이러스 양성으로 표시되지만 전달되는 메시지는 포함되지 않으므로 전달되는 실제 메시지 수는 정상 메시지 수와 다를 수 있습니다.
- 그레이메일 메시지
  - **Marketing Messages(**마케팅 메시지**)**: 전문 마케팅 그룹(예: Amazon.com)에서 전송한 총 광고 메시지 수.
  - **Social Networking Messages(**소셜 네트워킹 메시지**)**: 소셜 네트워크, 데이트 웹사이트, 포럼 등에서 온 총 알림 메시지 수. 예를 들면 LinkedIn 및 CNET 포럼이 있습니다.
  - **Bulk Messages(**대량 메시지**)**: 알 수 없는 마케팅 그룹(예: 기술 미디어 회사인 TechTarget)에서 전송하는 총 광고 메시지 수.

Message Tracking(메시지 추적)을 사용하여 해당 범주에 속한 메시지 목록을 보려면 위에서 언급한 그레이메일 범주 중 하나에 해당하는 번호를 클릭합니다.

참고 메시지 필터와 일치하며 필터에 의해 삭제 또는 반송되지 않은 메시지는 깨끗한 것으로 취급됩니다. 메시지 필터에 의해 삭제 또는 반송된 메시지는 합계에 포함되지 않습니다.

메시지 범주화 방법

이메일 파이프라인을 통해 진행되는 동안 메시지는 여러 범주에 적용될 수 있습니다. 예를 들어, 메시지는 스팸, 바이러스 또는 악성코드 양성으로 표시될 수 있으며, 콘텐츠 필터와 일치할 수도 있습니다. 다양한 판정은 Outbreak 격리(이 경우, 격리에서 해제되고 작업 대기열을 통해 다시 처리될 때까지 메시지는 계산되지 않음), 그 뒤에 스팸 양성, 바이러스 양성, 악성코드 양성 및 콘텐츠 필터 일치의 규칙 우선순위를 따릅니다.

예를 들어, 메시지가 스팸 양성으로 표시되고 안티 스팸 설정이 스팸 양성 메시지를 삭제하도록 설정된 경우, 메시지가 삭제되고 스팸 카운터가 늘어납니다. 스팸 양성 메시지가 파이프라인에서 계속 진행되도록 안티 스팸 설정이 구성되었으며 후속 콘텐츠 필터가 메시지를 삭제, 반송 또는 격리하는 경우에도 스팸 수가 증가합니다. 메시지가 스팸, 바이러스 또는 악성코드 양성이 아닌 경우에만 콘텐츠 필터 수가 증가합니다.

Incoming Mail(수신 메일) 페이지

Incoming Mail(수신 메일**)** 페이지는 어플라이언스에 연결된 모든 원격 호스트에 대해 이메일 보안 모니터 기능이 수집하는 실시간 정보에 대해 보고하는 메커니즘을 제공합니다. 이 페이지에서는 메일을 보내는 IP 주소, 도메인 및 조직(네트워크 소유자)에 대한 추가 정보를 수집할 수 있습니다. 메일을 보낸 IP 주소, 도메인 또는 조직에 대해 발신자 프로필 검색을 수행할 수 있습니다.

Incoming Mail(수신 메일) 페이지는 Domain(도메인), IP Address(IP 주소), Network Owner(네트워크 소유자)의 세 가지 보기로 구성되어 있으며, 선택한 보기의 컨텍스트에서 시스템에 연결된 원격 호스트의 스냅샷을 제공합니다.

또한 어플라이언스에 구성된 모든 퍼블릭 리스너에 메일을 전송한 상위 도메인(또는 보기에 따라 IP 주소나 네트워크 소유자)의 테이블(수신 메일 세부사항)을 표시합니다. 게이트웨이로 가는 모든 메일의 플로우를 모니터링할 수 있습니다. 자세히 알아볼 도메인/IP/네트워크 소유자를 클릭하면 Sender Profile(발신자 프로필) 페이지에서 이 발신자에 대한 세부사항에 액세스할 수 있습니다. 이 페이지는 클릭한 도메인/IP/네트워크 소유자에 대한 Incoming Mail(수신 메일) 페이지입니다.

기본적으로, 사용 가능한 모든 열이 표시되지는 않습니다. 테이블 아래에 있는 Columns(열) 링크를 클릭하여 서로 다른 정보 집합을 표시할 수 있습니다. 예를 들면, 기본적으로 숨겨진 "Detected by Advanced Malware Protection(AMP에 의해 탐지됨)" 열을 표시할 수 있습니다.

Incoming Mail(수신 메일) 페이지는 Incoming Mail(수신 메일), Sender Profiles(발신자 프로필), Sender Group Report(발신자 그룹 보고서) 등의 페이지 그룹을 포함하도록 확장됩니다. **Incoming Mail(**수신 메일**)** 페이지에서 다음을 수행할 수 있습니다.

- 메일을 보낸 IP 주소, 도메인 또는 조직(네트워크 소유자)에 대한 검색을 수행할 수 있습니다.
- 특정 발신자 그룹 및 메일 플로우 정책 작업을 통해 연결을 확인할 발신자 그룹 보고서를 볼 수 있습니다. 자세한 내용은 발신자 그룹 보고서, 808 페이지를 참조하십시오.
- 시도된 메시지 수를 발신자 평판 필터링, 안티 스팸, 안티바이러스, 그레이메일 등의 보안 서비스별로 구분한 내용을 포함하여, 메일을 보낸 발신자에 대한 자세한 통계를 볼 수 있습니다.
- 안티스팸 또는 안티바이러스 보안 서비스에 의해 확인된 대용량 스팸 또는 바이러스 이메일을 보낸 발신자별로 정렬할 수 있습니다.
- SenderBase Reputation Service를 통해 특정 IP 주소, 도메인 및 조직 사이의 관계를 자세히 알아보고 점검하여 발신자에 대한 더 많은 정보를 얻을 수 있습니다.
- SenderBase Reputation Service에서 발신자의 SBRS(SenderBase Reputation Score) 및 가장 최근에 도메인과 일치한 발신자 그룹 등 발신자에 대한 추가 정보를 얻기 위해 특정 발신자에 대해 자세히 알아볼 수 있습니다. 발신자를 발신자 그룹에 추가할 수 있습니다.
- 안티스팸 또는 안티바이러스 보안 서비스에 의해 확인된 대용량 스팸 또는 바이러스 이메일을 보낸 특정 발신자에 대해 자세히 알아볼 수 있습니다.
- 도메인에 대한 정보를 수집했으면 도메인, IP 주소 또는 네트워크 소유자 프로필 페이지에서 "Add to Sender Group(발신자 그룹에 추가)"을 클릭하여 기존 발신자 그룹에 IP 주소, 도메인 또는 조직을 추가할 수 있습니다(필요한 경우). 이메일을 수신하도록 게이트웨이 구성, 69 페이지를 참조하십시오.

관련 주제

- Incoming Mail(수신 메일), 804 페이지
- 수신 메일 세부사항 목록, 804 페이지
- 데이터로 채워진 보고 페이지: 발신자 프로필 페이지, 806 페이지
- 발신자 그룹 보고서, 808 페이지

Incoming Mail(수신 메일)

Incoming Mail(수신 메일) 페이지는 시스템에 구성된 모든 퍼블릭 리스너의 실시간 활동에 대한 액세스를 제공하며 두 개의 주요 섹션으로 구성됩니다. 하나는 메일을 보낸 상위 발신자 도메인을 요약한 메일 추세 그래프(위협 메시지 합계, 깨끗한 메시지 합계, 그레이메일 메시지 합계 기준)이고 다른 하나는 수신 메일 세부사항 목록입니다.

수신 메일 세부사항 목록에 포함된 데이터에 대한 설명은 수신 메일 세부사항 목록, 804 페이지 섹션을 참조하십시오.

관련 주제

메일 추세 그래프의 시간 범위에 대한 참고 사항, 804 페이지

메일 추세 그래프의 시간 범위에 대한 참고 사항

이메일 보안 모니터 기능은 게이트웨이로 가는 메일 플로우에 대한 데이터를 지속적으로 기록합니다. 데이터는 60초마다 업데이트되지만, 현재 시스템 시간보다 120초 늦게 표시됩니다. 표시되는 결과에 포함할 시간 범위를 지정할 수 있습니다. 데이터는 실시간으로 모니터링되므로, 데이터베이스에서 주기적으로 정보가 업데이트 및 요약됩니다.

다음 표의 시간 범위 옵션 중에서 선택합니다.

표 ***82:*** 이메일 보안 모니터 기능에서 사용 가능한 시간 범위

GUI에서 선택 가능한 시간 범위	정의되는 결과
시	마지막 60분 + 최대 5분
교육일	마지막 24시간 + 최대 60분
주	마지막 7일 + 금일 경과 시간
30일	마지막 30일 + 금일 경과 시간
90일	마지막 90일 + 금일 경과 시간
과거	00:00 ~ 23:59(자정~11:59 PM)
이전 달	달의 첫날 00:00에서 마지막 날 23:59까지
사용자 지정 범위	지정한 시작 날짜/시간과 종료 날짜/시간 사이의 범위

Centralized Reporting(중앙 집중식 보고)을 활성화한 경우 표시되는 시간 범위 옵션이 달라집니다. 중앙 집중식 보고 모드에 대한 자세한 내용은 Cisco Content(M-Series) Security Management Appliance에서 서비스 중앙 집중화, 1187 페이지를 참조하십시오.

수신 메일 세부사항 목록

선택한 보기를 기반으로, 어플라이언스의 퍼블릭 리스너에 연결된 상위 발신자가 Incoming Mail(수신 메일) 페이지 하단에 있는 External Domains Received listing(수신된 외부 도메인 목록) 테이블에 나

열됩니다. 데이터를 정렬하려면 열 머리글을 클릭합니다. 다양한 범주에 대한 설명은 이메일 범주화, 801 페이지 섹션을 참조하십시오.

시스템은 이중 *DNS* 조회를 수행하여 원격 호스트 IP 주소(즉, 도메인)의 유효성을 획득하고 확인합니다. 이중 DNS 조회 및 발신자 확인에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지 섹션을 참조하십시오.

Sender Detail listing(발신자 세부사항 목록)에는 Summary(요약)와 All(전체)의 두 가지 보기가 있습니다.

기본 Sender Detail(발신자 세부 정보) 보기는 각 발신자에 대해 시도된 메시지의 합계를 표시하며, 카테고리별 분석을 포함합니다(Overview(개요) 페이지의 Incoming Mail Summary(수신 메일 요약) 그래프와 같은 카테고리).

Stopped by Reputation Filtering(평판 필터링에 의해 중단됨)에 대한 값은 여러 요인을 기반으로 계산됩니다.

- 해당 발신자가 보낸 "조절된(throttled)" 메시지의 수
- 거부된 또는 TCP 거절된 연결의 수(부분 개수일 수 있음)
- 연결당 메시지 수에 대한 보수적 승수

어플라이언스가 과부하 상태인 경우 거부된 연결의 정확한 수가 발신자 기준으로 유지되지 않습니다. 대신 거부된 연결 수는 각 시간 간격에서 가장 중요한 발신자에 대해서만 유지됩니다. 이 상황에서는 표시된 값을 "바닥(floor)"으로 해석할 수 있습니다. 즉, 최소 이 숫자의 메시지가 중단된 것입니다.

참고 Overview(개요) 페이지의 Stopped by Reputation Filtering(평판 필터링에 의해 중단됨) 합계는 항상 거부된 모든 연결의 전체 개수를 기반으로 합니다. 발신자 기준 연결 개수만 부하 때문에 제한됩니다.

표시할 수 있는 추가 열은 다음과 같습니다.

Connections Rejected(거부된 연결**)**: HAT 정책에 의해 차단된 모든 연결. 어플라이언스가 과부하 상태인 경우 거부된 연결의 정확한 수가 발신자 기준으로 유지되지 않습니다. 대신 거부된 연결 수는 각 시간 간격에서 가장 중요한 발신자에 대해서만 유지됩니다.

Connections Accepted(수락된 연결**)**: 수락된 모든 연결

Stopped by Recipient Throttling(수신자 조절에 의해 중단됨**)**: Stopped by Reputation Filtering(평판 필터링에 의해 중단됨)의 구성 요소. 시간당 최대 수신자 수, 메시지당 최대 수신자 수 또는 연결당 최대 메시지 수 등 HAT 제한 중 하나가 초과되어 차단된 수신자 메시지 수를 나타냅니다. 이 수는 거부된 또는 TCP 거절된 연결과 관련이 있는 수신자 메시지의 추정치와 합산되어 Stopped by Reputation Filtering(평판 필터링에 의해 차단됨)을 산출합니다.

Detected by Advanced Malware Protection(AMP에 의해 탐지됨**)**: 파일 평판 필터링에 의해 악의적인 것으로 확인된 첨부 파일의 메시지. 이 값에는 파일 분석에 의해 악의적인 것으로 확인된 판정 업데이트 또는 파일이 포함되어 있지 않습니다.

Total Threat(위협 합계**)**: 총 위협 메시지 수(발신자 평판에 의해 중단됨, 잘못된 수신자, 스팸 및 바이러스로서 중단됨).

테이블 하단에 있는 Column(열) 링크를 클릭하여 열을 표시하거나 숨깁니다.

열 제목 링크를 클릭하여 목록을 정렬합니다. 제목 옆에 작은 삼각형이 있는 열은 데이터가 현재 정렬되었음을 나타냅니다.

관련 주제

- "No Domain Information(도메인 정보 없음)", 806 페이지
- 추가 정보 쿼리, 806 페이지

"No Domain Information(도메인 정보 없음)"

어플라이언스와 연결되어 있으며 이중 DNS 조회로 확인할 수 없는 도메인은 자동으로 특수 도메인인 "No Domain Information(도메인 정보 없음)"으로 그룹화됩니다. Sender Verification(발신자 확인)을 통해 이런 유형의 확인되지 않은 호스트를 관리하는 방법을 제어할 수 있습니다. 이메일을 수신하도록 게이트웨이 구성, 69 페이지를 참조하십시오.

Items Displayed(표시된 항목) 메뉴를 통해 목록에 표시할 발신자 수를 선택할 수 있습니다.

추가 정보 쿼리

이메일 보안 모니터 테이블에 나열된 발신자 중 특정 발신자에 대해 자세히 알아보려면 해당 발신자(또는 "No Domain Information(도메인 정보 없음)" 링크)를 클릭합니다. SenderBase Reputation Service에서 오는 실시간 정보를 포함하는 Sender Profile(발신자 프로필) 페이지에 결과가 표시됩니다. Sender Profile(발신자 프로필) 페이지에서 특정 IP 주소 또는 네트워크 소유자에 대해 자세히 알아볼 수 있습니다(데이터로 채워진 보고 페이지: 발신자 프로필 페이지, 806 페이지 참조).

또한 Incoming Mail(수신 메일) 페이지 하단에 있는 Sender Groups report(발신자 그룹 보고서) 링크를 클릭하여 또 다른 보고서인 발신자 그룹 보고서를 볼 수 있습니다. 발신자 그룹 보고서에 대한 자세한 내용은 발신자 그룹 보고서, 808 페이지 섹션을 참조하십시오.

데이터로 채워진 보고 페이지: 발신자 프로필 페이지

Incoming Mail(수신 메일) 페이지에서 Incoming Mail Details(수신 메일 세부사항) 테이블에 있는 발신자를 클릭하면 특정 IP 주소, 도메인 또는 조직(네트워크 소유자)에 대한 데이터와 함께 *Sender Profile(*발신자 프로필*)* 페이지가 나열됩니다. 발신자 프로필 페이지에는 발신자에 대한 자세한 정보가 표시됩니다. Incoming Mail(수신 메일) 또는 기타 발신자 프로필 페이지에서 지정된 항목을 클릭하여 네트워크 소유자, 도메인 또는 IP 주소에 대한 Sender Profile(발신자 프로필) 페이지에 액세스할 수 있습니다. 네트워크 소유자는 도메인을 포함하는 항목이고, 도메인은 IP 주소를 포함하는 항목입니다. 이 관계 및 이것이 SenderBase Reputation Service와 연결된 방식에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지 섹션을 참조하십시오.

IP 주소, 네트워크 소유자 및 도메인에 대해 표시되는 발신자 프로필 페이지는 약간 다릅니다. 각 페이지에는 해당 발신자가 보낸 수신 메일에 대한 그래프 및 요약 테이블이 포함됩니다. 그래프 아래에는 발신자와 연결된 도메인 또는 IP 주소가 나열된 테이블(개별 IP 주소에 대한 발신자 프로필 페이지에는 자세한 목록이 포함되지 않음) 및 현재 SenderBase, 발신자 그룹 및 발신자에 대한 네트워크 정보가 포함된 정보 섹션이 있습니다.

- 네트워크 소유자 프로필 페이지에는 네트워크 소유자는 물론 네트워크 소유자와 연결된 도메인 및 IP 주소에 대한 정보가 포함됩니다.

- 도메인 프로필 페이지에는 도메인 및 해당 도메인과 연결된 IP 주소에 대한 정보가 포함됩니다.
- IP 주소 프로필 페이지에는 IP 주소에 대한 정보만 포함되어 있습니다.

각 발신자 프로필 페이지의 하단에 있는 Current Information(현재 정보) 테이블에는 다음 데이터가 포함됩니다.

- SenderBase Reputation Service에서 제공하는 전역 정보:
  - IP 주소, 도메인 이름 및/또는 네트워크 소유자
  - 네트워크 소유자 범주(네트워크 소유자만)
  - CIDR 범위(IP 주소만)
  - IP 주소, 도메인 이름 및/또는 네트워크 소유자에 대한 일일 규모 및 월간 규모
  - 해당 발신자로부터 첫 메시지를 수신한 후 경과일
  - 마지막 발신자 그룹 및 DNS 확인 여부(IP 주소 발신자 프로필 페이지만)

  일일 규모는 지난 24시간 동안 도메인이 보낸 메시지 수 측정값입니다. 리히터 지진계가 지진을 측정하는 것과 마찬가지로 SenderBase 규모는 10을 기준으로 로그 스케일을 사용하여 계산된 메시지 볼륨 측정치입니다. 이론상 최대 스케일 값은 10으로 설정되며, 이는 세계 이메일 메시지 볼륨의 100%와 같습니다(하루 약 100억 개 메시지). 로그 스케일을 사용할 경우, 규모가 1 증가하는 것은 실제 볼륨이 10배 증가하는 것과 같습니다.

  월간 규모는 일일 규모와 동일한 접근법을 사용하여 계산되지만, 비율이 지난 30일 동안 전송된 이메일의 볼륨을 기반으로 계산된다는 점만 다릅니다.

  - 평균 규모(IP 주소만)
  - 수명 주기 볼륨/30일 볼륨(IP 주소 프로필 페이지만)
  - Bonded Sender 상태(IP 주소 프로필 페이지만)
  - SenderBase Reputation Score(IP 주소 프로필 페이지만)
  - 첫 번째 메시지 후 경과일(네트워크 소유자 및 도메인 프로필 페이지만)
  - 이 네트워크 소유자와 연결된 도메인의 수(네트워크 소유자 및 도메인 프로필 페이지만)
  - 이 네트워크 소유자의 IP 주소 수(네트워크 소유자 및 도메인 프로필 페이지만)
  - 이메일 전송에 사용된 IP 주소 수(네트워크 소유자 페이지만)

  SenderBase Reputation Service에서 제공하는 모든 정보가 포함된 페이지를 보려면 "More from SenderBase(SenderBase에서 더 보기)"를 클릭합니다.

- **Mail Flow Statistics(**메일 플로우 통계**)** 및 지정한 시간 범위 동안 발신자에 대해 수집된 이메일 보안 모니터 정보.
- 이 네트워크 소유자가 제어하는 도메인 및 IP 주소에 대한 세부 정보는 네트워크 소유자 프로필 페이지에 표시됩니다. 도메인의 IP 주소에 대한 세부사항은 도메인 페이지에 표시됩니다.

  도메인 프로필 페이지에서 특정 IP 주소로 드릴다운하거나 조직 프로필 페이지를 보기 위해 드릴업할 수 있습니다. 테이블 하단에 있는 Columns(열) 링크를 클릭하여 IP Addresses(IP 주소) 테이블의 각 발신자 주소에 대해 DNS Verified(DNS 확인됨) 상태, SBRS(SenderBase Reputation Score) 및 Last Sender Group(마지막 발신자 그룹)을 표시할 수 있습니다. 해당 테이블에서 열을 숨길 수도 있습니다.

  네트워크 소유자 프로필 페이지에서 해당 테이블 하단의 Columns(열) 링크를 클릭하여 Domains(도메인) 테이블의 각 도메인에 대한 Connections Rejected(거부된 연결), Connections Accepted(수락

된 연결), Stopped by Recipient Throttling(수신자 조절에 의해 중단됨), Detected by Advanced Malware Protection(AMP에 의해 탐지됨)과 같은 정보를 표시할 수 있습니다. 해당 테이블에서 열을 숨길 수도 있습니다.

엔티티에 대한 확인란을 클릭하고(필요한 경우) Add to Sender Group(발신자 그룹에 추가)을 클릭하여 시스템 관리자인 경우 이러한 각 페이지에서 네트워크 소유자, 도메인 또는 IP 주소를 발신자 그룹에 추가하도록 선택할 수 있습니다.

Current Information(현재 정보) 테이블의 Sender Group Information(발신자 그룹 정보) 아래에 있는 **Add to Sender Group(**발신자 그룹에 추가**)** 링크를 클릭하고 Add to Sender Group(발신자 그룹에 추가)을 클릭하여 발신자를 발신자 그룹에 추가할 수도 있습니다. 발신자를 발신자 그룹에 추가하는 방법에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지 섹션을 참조하십시오. 물론 아무것도 변경하지 않고, 보안 서비스가 수신 메일을 처리하도록 내버려둘 수도 있습니다.

관련 주제

- 발송인 프로파일 검색, 808 페이지

발송인 프로파일 검색

특정 발신자를 검색하려면 Quick Search(빠른 검색) 상자에 IP 주소, 도메인 또는 조직 이름을 입력합니다.

발신자에 대한 정보가 포함된 발신자 프로필 페이지가 표시됩니다. 데이터로 채워진 보고 페이지: 발신자 프로필 페이지, 806 페이지를 참조하십시오.

발신자 그룹 보고서

Sender Groups(발신자 그룹) 보고서는 발신자 그룹 및 메일 플로우 정책 작업별로 연결 요약을 제공하므로, SMTP 연결 및 메일 플로우 정책 추세를 검토할 수 있습니다. Mail Flow by Sender Group(발신자 그룹별 메일 플로우) 목록은 각 발신자 그룹에 대한 연결 비율과 수를 보여줍니다. Connections by Mail Flow Policy Action(메일 플로우 정책 작업별 연결) 차트는 각 메일 플로우 정책 작업에 대한 연결의 비율을 보여줍니다. 이 페이지는 HAT(Host Access Table) 정책 효과의 개요를 제공합니다. HAT에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지 섹션을 참조하십시오.

Sender Domain Reputation(발신인 도메인 평판) 페이지

Sender Domain Reputation(발신자 도메인 평판 보고서) 페이지를 사용하여 다음을 볼 수 있습니다.

- SDR 서비스에서 받은 판정에 기반한 수신 메시지를 그래픽 형식으로 봅니다.
- SDR 서비스에서 받은 위협 카테고리 및 판정에 기반한 수신 메시지를 표 형식으로 봅니다.
- SDR 서비스에서 받은 위협 카테고리에 기반한 수신 메시지를 그래픽 형식으로 봅니다.

참고 SDR 판정이 '매우 나쁨' 또는 '나쁨'인 메시지만 '스팸', '악성' 등과 같은 SDR 위협 카테고리에 따라 분류됩니다.

- SDR 서비스에서 받은 위협 카테고리에 기반한 수신 메시지를 표 형식으로 봅니다.

SDR 섹션에서 처리된 수신 메시지의 요약에서는, 특정 판정에 해당하는 메시지의 수를 클릭하여 메시지 추적의 관련 메시지를 볼 수 있습니다.

Outgoing Destinations(발신 대상)

Outgoing Destinations(발신 대상) 페이지는 회사가 메일을 보내는 대상 도메인에 대한 정보를 제공합니다. 이 페이지는 두 섹션으로 구성됩니다. 페이지 상단 절반은 발신 위협 메시지별 상위 대상과 발신 깨끗한 메시지별 상위 대상을 설명하는 그래프로 구성됩니다. 페이지 하단 절반은 수신자 합계별로 정렬된 모든 열을 보여주는 차트를 표시합니다(기본 설정).

보고할 시간 범위(예: 시간, 주 또는 사용자 지정 범위)를 선택할 수 있습니다. 모든 보고서에 대해 **Export(**내보내기**)** 링크를 통해 그래프에 대한 데이터 또는 세부사항 목록을 CSV 형식으로 내보낼 수 있습니다.

다음 유형의 질문에 답하는 데 Outgoing Destinations(발신 대상) 페이지를 사용할 수 있습니다.

- 어플라이언스가 어떤 도메인으로 메일을 전송합니까?
- 각 도메인으로 얼마나 많은 메일이 전송됩니까?
- 이 메일 중에 콘텐츠 필터에 의해 중단된 메일, 악성코드, 바이러스 양성, 스팸 양성 또는 정상 메일은 얼마나 됩니까?
- 전달된 메시지는 몇 개이며 대상 서버에 의해 하드 반송된 메시지는 몇 개입니까?

Outgoing Senders(발신 발신자)

Outgoing Senders(발신 발신자) 페이지는 네트워크의 IP 주소 및 도메인에서 전송되는 메일의 양과 유형에 대한 정보를 제공합니다. 이 페이지에서 도메인 또는 IP 주소별로 결과를 볼 수 있습니다. 각 도메인에서 전송하는 메일의 볼륨을 보려면 도메인별 결과를 볼 수 있습니다. 또는 어떤 IP 주소에서 바이러스 메시지를 가장 많이 전송하거나 콘텐츠 필터를 가장 많이 트리거하는지 보려면 IP 주소별로 결과를 볼 수 있습니다.

이 페이지는 두 섹션으로 구성됩니다. 페이지의 왼쪽에는 위협 메시지 합계별로 상위 발신자를 보여주는 그래프가 있습니다. 위협 메시지 합계에는 스팸 양성, 바이러스 양성 또는 악성코드이거나 콘텐츠 필터를 트리거한 메시지가 포함됩니다. 페이지의 오른쪽 상단 절반에는 깨끗한 메시지별 상위 발신자를 표시하는 그래프가 있습니다. 페이지 하단 절반은 메시지 합계별로 정렬된 모든 열을 보여주는 차트를 표시합니다(기본 설정).

참고 이 페이지에는 메시지 전달에 대한 정보가 표시되지 않습니다. 특정 도메인에서 몇 개의 메시지가 반송되었는지 등의 전달 정보는 Delivery Status(전달 상태) 페이지를 사용하여 추적할 수 있습니다.

보고할 시간 범위(예: 시간, 주 또는 사용자 지정 범위)를 선택할 수 있습니다. 모든 보고서에 대해 **Export(내보내기)** 링크를 통해 그래프에 대한 데이터 또는 세부사항 목록을 CSV 형식으로 내보낼 수 있습니다.

다음 유형의 질문에 답하는 데 Outgoing Senders(발신 발신자) 페이지를 사용할 수 있습니다.

- 대부분의 바이러스 양성, 스팸 양성 또는 악성코드 이메일을 전송하는 IP 주소는 무엇입니까?
- 가장 자주 콘텐츠 필터를 트리거하는 IP 주소는 무엇입니까?
- 대부분의 메일을 전송하는 도메인은 무엇입니까?

Geo Distribution(지리적 분포) 페이지

Geo Distribution(지리적 분포) 보고서 페이지를 사용하여 다음을 볼 수 있습니다.

- 그래픽 형식의 발신지 국가별 상위 수신 메일 연결입니다.
- 표 형식의 발신지 국가별 상위 수신 메일 연결입니다.

특정 지리위치에 대한 수신 메일 연결 수를 클릭하여 메시지 추적에서 관련 메시지를 볼 수 있습니다.

"Total Messages(총 메시지)" 열에는 SMTP 연결 수준에서 허용된 메시지만 표시됩니다.

참고 보고서 생성 시:

- 하나 이상의 수신 메일 연결이 프라이빗 IP 주소로 탐지되면 수신 메일 연결은 보고서에서 "프라이빗 IP 주소"로 분류됩니다.
- 하나 이상의 수신 메일 연결이 유효한 SBRS 점수가 아닌 것으로 탐지되면 수신 메일 연결은 보고서에 'No Country Info(국가 정보 없음)'로 분류됩니다.

Delivery Status(전달 상태) 페이지

특정 수신자 도메인에 전달 문제가 있는 것으로 의심되거나 가상 게이트웨이 주소에 대한 정보를 수집하려는 경우, Monitor(모니터) > Delivery Status(전달 상태) 페이지는 특정 수신자 도메인과 관련된 이메일 운영에 대한 모니터링 정보를 제공합니다.

Delivery Status(전달 상태) 페이지는 CLI의 tophosts 명령과 동일한 정보를 표시합니다. (자세한 내용은 CLI를 사용한 관리 및 모니터링, 997 페이지의 "이메일 대기열의 구성 확인"을 참조하십시오.)

이 페이지는 지난 3시간 내에 시스템에서 전달한 메시지에 대한 상위 수신자 도메인 20, 50 또는 100개 목록을 표시합니다. 각 통계의 열 머리글에 있는 링크를 클릭하여 최신 호스트 상태, 활성 수신자(기본값), 외부 연결, 전달된 수신자, 소프트 바운스된 이벤트, 하드 바운스된 수신자 등을 기준으로 정렬할 수 있습니다.

- 특정 도메인을 검색하려면 Domain Name(도메인 이름): 필드에 도메인의 이름을 입력하고 **Search(검색)**를 클릭합니다.
- 표시된 도메인으로 드릴다운하려면 도메인 이름 링크를 클릭합니다.

결과는 Delivery Status Details(전달 상태 세부사항) 페이지에 표시됩니다.

참고 수신자 도메인에 대한 활동은 해당 도메인에 "active(활성)" 상태로 나타나며 개요 페이지에도 표시됩니다. 메일이 전달 문제 때문에 아웃바운드 대기열에 남아 있으면 수신자 도메인은 발신 메일 개요에 계속 나열됩니다.

관련 주제

- 전달 재시도, 811 페이지
- Delivery Status Details(전달 상태 세부사항) 페이지, 811 페이지

전달 재시도

나중에 전달하도록 예약된 메시지는 **Retry All Delivery(**모든 전달 재시도**)**를 클릭하여 즉시 재시도할 수 있습니다. Retry All Delivery(모든 전달 재시도)를 사용하면 대기열에 있는 메시지를 즉시 전달하도록 다시 예약할 수 있습니다. "Down(다운)" 상태로 표시된 모든 도메인과 예약된 메시지 또는 소프트 반송된 메시지가 즉시 전달을 위해 대기열에 추가됩니다.

특정 대상 도메인으로의 전달을 재시도하려면 도메인 이름 링크를 클릭합니다. Delivery Status Details(전달 상태 세부사항) 페이지에서 **Retry Delivery(**전달 재시도**)**를 클릭합니다.

또한 CLI의 delivernow 명령을 사용하여 메시지를 즉시 전달하도록 다시 예약할 수도 있습니다. 자세한 내용은 즉시 전달하도록 이메일 예약, 1020 페이지를 참고하십시오.

Delivery Status Details(전달 상태 세부사항) 페이지

특정 수신자 도메인에 대한 통계를 조회하려면 **Delivery Status Details(**전달 상태 세부사항**)** 페이지를 사용합니다. 이 페이지는 Mail Status(메일 상태), Counters(카운터) 및 Gauges(게이지)에 대해 CLI의 **`hoststatus`** 명령과 동일한 정보를 표시합니다. (자세한 내용은 CLI를 사용한 관리 및 모니터링, 997 페이지 참고) 특정 도메인을 검색하려면 Domain Name(도메인 이름): 필드에 도메인의 이름을 입력하고 **Search(**검색**)**를 클릭합니다. **`altsrchost`** 기능을 사용 중인 경우 가상 게이트웨이 주소 정보가 표시됩니다.

Internal Users(내부 사용자) 페이지

Internal Users(내부 사용자) 페이지는 내부 사용자가 주고받은 메일에 대한 정보를 메일 주소 단위로 제공합니다(단일 사용자가 나열된 여러 이메일 주소를 가지고 있을 수 있으며, 이러한 이메일 주소는 보고서에서 결합되지 않습니다).

이 페이지는 두 섹션으로 구성됩니다.

- 하나는 깨끗한 수신/발신 메시지별 상위 사용자 그래프이고 다른 하나는 그레이메일 수신 상위 사용자 그래프입니다.
- 사용자 메일 플로우 세부사항

보고할 시간 범위(시간, 일, 주 또는 월)를 선택할 수 있습니다. 모든 보고서에 대해 **Export(**내보내기**)** 링크를 통해 그래프에 대한 데이터 또는 세부사항 목록을 CSV 형식으로 내보낼 수 있습니다. 테이블

아래에 있는 Columns(열) 링크를 클릭하여 숨겨진 테이블 열을 표시하거나 기본 열을 숨길 수 있습니다.

User Mail Flow Details(사용자 메일 플로우 세부사항) 목록은 각 이메일 주소로 주고받은 메일을 깨끗한 메일, 스팸(수신 전용), 바이러스, 악성코드, 콘텐츠 필터 일치 및 그레이메일(수신 전용)로 구분합니다. 열 제목을 클릭하여 목록을 정렬할 수 있습니다.

Internal Users(내부 사용자) 보고서를 사용하면 다음과 같은 종류의 질문에 답할 수 있습니다.

- 외부 이메일을 가장 많이 보내는 사람은?
- 정상 이메일을 가장 많이 받는 사람은?
- 그레이메일 메시지를 가장 많이 받는 사람은?
- 스팸을 가장 많이 받는 사람은?
- 누가 어떤 콘텐츠 필터를 트리거하나?
- 누구의 이메일이 콘텐츠 필터에서 가장 많이 포착되는가?

Inbound Internal Users(인바운드 내부 사용자)란 Rcpt To: 주소를 기반으로 이메일을 수신한 사용자입니다. Outbound Internal Users(아웃바운드 내부 사용자)는 Mail From: 주소를 기반으로 하며 내부 네트워크의 발신자가 전송하는 이메일 유형을 추적할 때 유용합니다.

일부 아웃바운드 메일(예: 반송)에는 null 발신자가 있습니다. 이러한 메일은 아웃바운드 및 "unknown(알 수 없음)"으로 계산됩니다.

내부 사용자에 대한 Internal User detail(내부 사용자 세부사항) 페이지를 보려면 해당 사용자를 클릭합니다.

Incoming Detected by Advanced Malware Protection(Advanced Malware Protection에서 탐지된 수신 메시지) 열 또는 Outgoing Detected by Advanced Malware Protection(Advanced Malware Protection에서 탐지된 발신 메시지) 열과 같이 기본적으로 숨겨진 열을 표시하려면 표 아래의 Columns(열) 링크를 클릭합니다.

관련 주제

- 내부 사용자 세부사항, 812 페이지
- 특정 내부 사용자 검색, 813 페이지

내부 사용자 세부사항

Internal User detail(내부 사용자 세부사항) 페이지는 각 범주(스팸 탐지됨, 바이러스 탐지됨, AMP에 의해 탐지됨, 콘텐츠 필터에 의해 중단됨, 그레이메일 탐지됨, 깨끗함 등)의 메시지 수를 보여주는 수신 및 발신 메시지 분류를 포함하여, 지정된 사용자에 대한 자세한 정보를 보여줍니다. 선택적으로, 수신 메시지의 경우 테이블 아래에 있는 Columns(열) 링크를 클릭하여 Incoming Detected by Advanced Malware Protection(AMP로 탐지된 수신) 열을 표시할 수 있습니다. 이 값은 파일 평판 필터링에서 악의적인 것으로 판단한 첨부 파일이 포함된 메시지 수를 나타냅니다. 이 값에는 파일 분석에 의해 악의적인 것으로 확인된 판정 업데이트 또는 파일이 포함되어 있지 않습니다. 수신 및 발신 콘텐츠 필터와 DLP 정책 일치도 표시됩니다.

해당 콘텐츠 필터 정보 페이지에서 해당 필터에 대한 자세한 정보를 보려면 콘텐츠 필터 이름을 클릭합니다(Content Filters(콘텐츠 필터) 페이지, 814 페이지 참조). 특정 콘텐츠 필터와 일치한 메일을 보내거나 받은 사용자 목록을 표시하려면 이 방법을 사용할 수 있습니다.

특정 내부 사용자 검색

Internal Users(내부 사용자) 페이지 및 Internal User detail(내부 사용자 세부사항) 페이지 하단에 있는 검색 양식을 통해 특정 내부 사용자(이메일 주소)를 검색할 수 있습니다. 검색 텍스트와 정확한 일치를 찾을지 아니면 입력한 텍스트로 시작하는 항목을 찾을지(예: "ex"로 시작하면 "example.com"이 검색됨)를 선택합니다.

DLP Incidents(DLP 인시던트) 페이지

DLP Incidents(DLP 인시던트) 페이지는 발신 메일에서 발생하는 DLP(data loss prevention) 정책 위반에 대한 정보를 보여줍니다. 어플라이언스는 사용자가 전송한 민감한 데이터를 탐지하기 위해 Outgoing Mail Policies(발신 메일 정책) 테이블에서 활성화된 DLP 이메일 정책을 사용합니다. DLP 정책을 위반하는 모든 발신 메시지는 인시던트로 보고됩니다.

DLP Incidents(DLP 인시던트) 보고서를 사용하면 다음과 같은 종류의 질문에 답할 수 있습니다.

- 사용자들이 어떤 유형의 민감한 데이터를 전송합니까?
- 이러한 DLP 인시던트가 얼마나 심각합니까?
- 이러한 메시지 중 몇 개가 전달되었습니까?
- 이러한 메시지 중 몇 개가 삭제되었습니까?
- 누가 이러한 메시지를 전송합니까?

DLP Incidents(DLP 인시던트) 페이지는 두 개의 주요 섹션으로 구성됩니다.

- 심각도(Low, Medium, High, Critical) 및 정책 일치별로 상위 DLP 인시던트를 요약한 DLP 인시던트 추세 그래프
- DLP Incidents Details(DLP 인시던트 세부 사항) 목록

보고할 시간 범위(예: 시간, 주 또는 사용자 지정 범위)를 선택할 수 있습니다. 모든 보고서에 대해 **Export(내보내기)** 링크를 통해 CSV 형식으로 또는 **Printable (PDF)(인쇄 가능(PDF))** 링크를 클릭하여 PDF 형식으로 그래프에 대한 데이터 또는 세부사항 목록을 내보낼 수 있습니다. 영어 이외의 언어로 PDF를 생성하는 방법에 대한 자세한 내용은 보고서에 대한 참고 사항, 832 페이지 섹션을 참조하십시오.

정책에 의해 탐지된 DLP 인시던트에 대한 자세한 정보를 보려면 DLP 정책의 이름을 클릭합니다. 정책에서 탐지한 민감한 데이터가 포함된 메일을 전송한 사용자 목록을 표시하려면 이 방법을 사용할 수 있습니다.

관련 주제

- DLP 인시던트 세부사항, 813 페이지
- DLP 정책 세부사항 페이지, 814 페이지

DLP 인시던트 세부사항

어플라이언스의 발신 메일 정책에서 현재 활성화된 DLP 정책은 DLP Incidents(DLP 인시던트) 페이지의 하단에 있는 DLP Incidents Details(DLP 인시던트 세부사항) 테이블에 나열됩니다. 자세한 정보를 표시하려면 DLP 정책의 이름을 클릭합니다.

DLP Incident Details(DLP 인시던트 세부 정보) 테이블에는 심각도 수준으로 구분된 정책당총 DLP 인시던트 수가 표시됩니다. 심각도 수준에는 반송된 메시지 수 및 정상 상태로 전달되거나 암호화 상태로 전달되거나 삭제된 메시지 수도 포함됩니다. 데이터를 정렬하려면 열 머리글을 클릭합니다.

DLP 정책 세부사항 페이지

DLP Incidents Details(DLP 인시던트 세부사항) 테이블에서 DLP 정책의 이름을 클릭하면 DLP Policy Detail(DLP 정책 세부사항) 페이지에 정책에 대한 DLP 세부사항 데이터가 표시됩니다. 이 페이지는 심각도를 기반으로 DLP 인시던트에 대한 그래프를 표시합니다.

또한 DLP 정책을 위반한 메시지를 전송한 각 내부 사용자가 나열된 Incidents by Sender(발신자별 인시던트) 목록이 페이지 하단에 포함되어 있습니다. 이 목록에는 또한 심각도 레벨로 구분된 정책의 사용자당 총 DLP 인시던트 수와 메시지가 일반 텍스트로 전달되었는지, 암호화되어 전달되었는지 또는 삭제되었는지가 표시됩니다. 어떤 사용자가 조직의 민감한 데이터를 네트워크 외부의 사람들에게 전송하는지를 알아내려면 Incidents by Sender(발신자별 인시던트) 목록을 사용할 수 있습니다.

발신자 이름을 클릭하면 Internal Users(내부 사용자) 페이지가 열립니다. 자세한 내용은 Internal Users(내부 사용자) 페이지, 811 페이지를 참조하십시오.

Content Filters(콘텐츠 필터) 페이지

Content Filters(콘텐츠 필터) 페이지에는 상위 수신 및 발신 콘텐츠 필터 일치(일치하는 메시지가 가장 많은 콘텐츠 필터)에 대한 정보가 막대 차트와 목록의 두 가지 형식으로 표시됩니다. Content Filters(콘텐츠 필터) 페이지를 사용하면 콘텐츠 필터 또는 사용자 단위로 회사 정책을 검토하고 다음과 같은 질문에 답할 수 있습니다.

- 수신 또는 발신 메일에 의해 가장 많이 트리거되는 콘텐츠 필터는 무엇입니까?
- 특정 콘텐츠 필터를 트리거하는 메일을 보내거나 받는 상위 사용자는 누구입니까?

Content Filter detail(콘텐츠 필터 세부사항) 페이지에서 특정 콘텐츠 필터에 대한 자세한 정보를 보려면 목록에서 해당 필터의 이름을 클릭할 수 있습니다.

관련 주제

- 콘텐츠 필터 세부사항, 814 페이지

콘텐츠 필터 세부사항

Content Filter detail(콘텐츠 필터 세부사항) 페이지에는 시간별 해당 필터에 대한 일치 및 내부 사용자별 일치가 표시됩니다.

Matches by Internal User(내부 사용자별 일치) 섹션에서 내부 사용자(이메일 주소)의 Internal User details(내부 사용자 세부사항) 페이지를 보려면 해당 사용자의 이름을 클릭할 수 있습니다(내부 사용자 세부사항, 812 페이지 참조).

DMARC Verification(DMARC 확인) 페이지

DMARC Verification(DMARC 확인) 페이지에는 DMARC 확인에 실패한 상위 도메인 및 DMARC 확인에 실패한 메시지에 대해 AsyncOS에서 수행한 작업의 세부사항이 표시됩니다. 이 보고서를 사용하면 DMARC 설정을 세부적으로 조정하고 다음과 같은 종류의 질문에 답할 수 있습니다.

- DMARC를 준수하지 않는 메시지를 가장 많이 전송한 도메인은 무엇입니까?
- 각 도메인에서, DMARC 확인에 실패한 메시지에 대해 AsyncOS에서 수행한 작업은 무엇입니까?

DMARC Verification(DMARC 확인) 페이지에는 다음이 포함되어 있습니다.

- DMARC 확인 실패 기준 상위 도메인을 표시하는 막대 차트.
- 각 도메인에 대한 다음 내용을 테이블 형식으로 표시.
  - 아무런 작업 없이 거부되거나 격리되거나 수락된 메시지의 수. 선택한 범주의 메시지 목록을 보려면 숫자를 클릭합니다.
  - DMARC 확인을 통과한 메시지 수.
  - 총 DMARC 확인 시도 수.

보고할 시간 범위(예: 시간, 주 또는 사용자 지정 범위)를 선택할 수 있습니다. 모든 보고서에 대해 **Export(**내보내기**)** 링크를 통해 CSV 형식으로 또는 **Printable (PDF)(**인쇄 가능**(PDF))** 링크를 클릭하여 PDF 형식으로 그래프에 대한 데이터 또는 세부사항 목록을 내보낼 수 있습니다.

Macro Detection(매크로 탐지) 페이지

Macro Detection(매크로 탐지) 보고서 페이지를 사용하여 다음을 볼 수 있습니다.

- 파일 형식별 상위 수신 매크로 사용 첨부 파일을 그래픽 형식과 표 형식으로 봅니다.
- 파일 형식별 상위 발신 매크로 사용 첨부 파일을 그래픽 형식과 표 형식으로 봅니다.

매크로 사용 첨부 파일의 수를 클릭하여 메시지 추적에서 관련 메시지를 볼 수 있습니다.

참고 보고서 생성 시:

- 아카이브 파일 내에서 하나 이상의 매크로가 탐지되면 아카이브 파일 파일 형식이 1씩 증가합니다. 아카이브 파일 내 매크로 사용 첨부 파일의 수는 계산되지 않습니다.
- 내장 파일 내에서 하나 이상의 매크로가 탐지되면 상위 파일 형식이 1씩 증가합니다. 내장 파일 내 매크로 사용 첨부 파일의 수는 계산되지 않습니다.

External Threat Feeds(외부 위협 피드) 페이지

External Threat Feeds(외부 위협 피드) 보고서 페이지를 사용하여 다음을 볼 수 있습니다.

- 메시지에서 위협을 탐지하는 데 사용되는 그래픽 형식의 상위 ETF 소스

- 메시지에서 위협을 탐지하는 데 사용되는 표 형식의 ETF 소스 요약
- 메시지에서 탐지된 위협과 일치하는 그래픽 형식의 상위 IOC
- 악의적인 수신 메일 연결을 필터링하는 데 사용되는 그래픽 형식의 상위 ETF 소스
- 악의적인 수신 메일 연결을 필터링하는 데 사용되는 표 형식의 ETF 소스 요약

'Summary of External Threat Feed Sources(외부 위협 피드 소스 요약)' 섹션에서 다음 작업을 수행할 수 있습니다.

- 특정 ETF 소스에 대한 메시지 수를 클릭하여 메시지 추적에서 관련 메시지를 볼 수 있습니다.
- 특정 위협 피드 소스를 클릭하여 IOC를 기준으로 ETF 소스의 배포를 볼 수 있습니다.

'Summary of Indicator of Compromise (IOC) Matches(IOC(Indicator of Compromise) 매치 요약)' 섹션에서 다음 작업을 수행할 수 있습니다.

- 특정 ETF 소스에 대한 IOC 수를 클릭하여 메시지 추적에서 관련 메시지를 볼 수 있습니다.
- 특정 IOC를 클릭하여 ETF 소스를 기준으로 IOC 배포를 볼 수 있습니다.

Outbreak Filters 페이지

Outbreak Filters 페이지에서는 어플라이언스에 있는 Outbreak Filter의 현재 상태와 컨피그레이션은 물론 최신 전파 확산에 대한 정보와 Outbreak Filter로 인해 격리된 메시지도 볼 수 있습니다. 이 페이지를 사용하면 대상이 지정된 바이러스, 스캠 및 피싱 공격에 대한 방어를 모니터링할 수 있습니다.

Threats By Type(유형별 위협) 섹션에는 어플라이언스에서 수신한 두 가지 유형의 위협 메시지가 표시됩니다.

Threat Summary(위협 요약) 섹션에는 Malware(악성코드), Phish(피싱), Scam(스캠) 및 Virus(바이러스)별로 구분된 위협 메시지가 표시됩니다. Message Tracking(메시지 추적)을 사용하여 번호에 포함된 모든 메시지의 목록을 보려면 해당 번호를 클릭합니다.

Past Year Outbreak Summary(지난해 Outbreak 요약)에는 지난해의 로컬 및 전역 전파 확산 정보가 나열되어 있으므로, 로컬 네트워크 추세를 전역 추세와 비교할 수 있습니다. 전역 전파 확산의 목록은 모든 전파 확산(바이러스 및 비 바이러스)의 상위 집합인 반면, 로컬 전파 확산은 어플라이언스에 영향을 미친 바이러스 전파 확산으로 제한됩니다. 로컬 전파 확산 데이터에는 비 바이러스 위협이 포함되어 있지 않습니다. 전역 전파 확산 데이터는 Outbreak 격리에 대해 현재 구성된 임계값을 초과한, Threat Operations Center에 의해 탐지된 모든 전파 확산을 나타냅니다. 로컬 전파 확산 데이터는 Outbreak 격리에 대해 현재 구성된 임계값을 초과한, 이 어플라이언스에서 탐지된 모든 바이러스 전파 확산을 나타냅니다. Total Local Protection Time(총 로컬 보호 시간)은 항상 Threat Operations Center에서 탐지된 각 바이러스 전파 확산과 주요 공급업체의 안티바이러스 서명 릴리스 사이의 차이를 기반으로 합니다. 모든 전역 전파 확산이 어플라이언스에 영향을 미치는 것은 아닙니다. 값 "--"는 보호 시간이 없음을 나타내거나, 안티바이러스 공급업체에서 사용 가능한 서명 시간이 없었음을 나타냅니다(일부 공급업체는 서명 시간을 보고하지 않을 수 있음). 보호 시간이 영(0)임을 나타낸다기보다는, 보호 시간 계산에 필요한 정보를 사용할 수 없음을 나타냅니다.

Outbreak Filter 격리가 요약되어 있는 Quarantined Messages(격리된 메시지) 섹션은 Outbreak Filter가 파악하는 잠재적 위협 메시지의 수를 측정하는 데 유용합니다. 격리된 메시지는 릴리스될 때 계산됩니다. 일반적으로 메시지는 안티바이러스 및 안티스팸 규칙을 사용할 수 있기 전에 격리됩니다. 메시지가 릴리스되면 안티바이러스 및 안티스팸 소프트웨어로 검사되고 양성 또는 깨끗한 메시지로 확인됩니다. Outbreak 추적의 동적 속성 때문에 메시지를 격리하는 규칙(및 관련 전파 확산)은 메시지가 격리에 있는 동안 변경될 수 있습니다. 릴리스될 때(격리에 들어갈 때보다) 메시지를 계산하면 숫자가 늘고 주는 데서 오는 혼동을 피할 수 있습니다.

Threat Details(위협 세부사항) 목록에는 위협 범주(바이러스, 스캠 또는 피싱), 위협 이름, 위협 설명, 식별된 메시지 수를 포함하여 특정 전파 확산에 대한 정보가 표시됩니다. 바이러스 전파 확산의 경우, Past Year Virus Outbreaks(지난해 바이러스 Outbreaks)에는 Outbreak 이름과 ID, 바이러스 전파 확산이 처음 전역적으로 발견된 시간과 날짜, Outbreak Filter가 제공한 보안 시간 및 격리된 메시지의 수가 포함됩니다. 전역 또는 로컬 전파 확산은 물론 왼쪽 메뉴를 통해 표시할 메시지 수도 선택할 수도 있습니다. 열 제목을 클릭하여 목록을 정렬할 수 있습니다. Message Tracking(메시지 추적)을 사용하여 번호에 포함된 모든 메시지의 목록을 보려면 해당 번호를 클릭합니다.

First Seen Globally(처음 전역적으로 발견) 시간은 세계 최대 이메일 및 웹 트래픽 모니터링 네트워크인 SenderBase에서 제공하는 데이터를 기반으로 Threat Operations Center에 의해 결정됩니다. 보호 시간은 Threat Operations Center에서 탐지된 각 위협과 주요 공급업체의 안티바이러스 서명 릴리스 사이의 차이를 기반으로 합니다.

값 "--"는 보호 시간이 없음을 나타내거나, 안티바이러스 공급업체에서 사용 가능한 서명 시간이 없었음을 나타냅니다(일부 공급업체는 서명 시간을 보고하지 않을 수 있음). 보호 시간이 영(0)임을 나타내지는 않습니다. 오히려 보호 시간 계산에 필요한 정보를 사용할 수 없음을 나타냅니다.

Hit Messages from Incoming Messages(내부 메시지에서 오는 적중 메시지) 섹션은 바이러스 첨부 파일, 기타 위협(비 바이러스) 및 깨끗한 수신 메시지의 비율과 숫자를 보여줍니다.

Hit Messages by Threat Level(위협 레벨별 적중 메시지) 섹션은 위협 레벨(레벨 1~5)을 기반으로 수신 위협 메시지(바이러스 및 비 바이러스)의 비율과 숫자를 보여줍니다.

Messages resided in Outbreak Quarantine(Outbreak 격리에 상주한 메시지) 섹션은 기간을 기반으로 Outbreak 격리에 상주한 위협 메시지의 수를 보여줍니다.

Top URL's Rewritten(재작성된 상위 URL) 섹션은 발생 횟수를 기반으로 재작성된 상위 10개 URL 목록을 보여줍니다. 재작성된 URL을 더 보려면 Items Displayed(표시된 항목) 드롭다운을 사용합니다. 번호를 클릭하면 Message Tracking(메시지 추적) 페이지에서 선택한 재작성된 URL을 포함하는 모든 메시지의 목록을 보여줍니다.

Outbreak Filters 페이지를 사용하면 다음과 같은 질문에 답할 수 있습니다.

- 격리 중인 메시지는 몇 개이며 이들은 어떤 유형의 위협입니까?
- Outbreak Filter 기능이 바이러스 전파 확산에 제공한 리드 타임은 얼마입니까?
- 로컬 바이러스 전파 확산을 전역 전파 확산과 어떻게 비교합니까?

Virus Types(바이러스 유형) 페이지

Virus Types(바이러스 유형) 페이지는 네트워크에 들어가고 네트워크에서 전송되는 바이러스의 개요를 제공합니다. Virus Types(바이러스 유형) 페이지에는 어플라이언스에서 실행 중인 바이러스 검사 엔진이 탐지한 바이러스가 표시됩니다. 특정 바이러스에 대해 특정 동작을 수행하려면 이 보고서를

사용할 수 있습니다. 예를 들어 PDF 파일에 포함된 것으로 알려진 대량의 바이러스를 수신하고 있다면 PDF 첨부 파일이 있는 메시지를 격리하는 필터 작업을 만들 수 있습니다.

여러 바이러스 검사 엔진을 실행 중인 경우 Virus Types(바이러스 유형) 페이지에는 활성화된 모든 바이러스 검사 엔진에서 온 결과가 포함됩니다. 페이지에 표시되는 바이러스의 이름은 바이러스 검사 엔진에서 확인한 이름입니다. 둘 이상의 검사 엔진에서 바이러스를 탐지하는 경우 동일한 바이러스에 대한 항목이 둘 이상 있을 수 있습니다.

Virus Types(바이러스 유형) 페이지는 네트워크에 들어가거나 네트워크에서 전송되는 바이러스의 개요를 제공합니다. Top Incoming Virus Detected(탐지된 상위 수신 바이러스) 섹션에서는 네트워크로 전송된 바이러스의 차트 보기를 내림차순으로 보여줍니다. Top Outgoing Virus Detected(탐지된 상위 발신 바이러스) 섹션에서는 네트워크로부터 전송된 바이러스의 차트 보기를 내림차순으로 보여줍니다.

참고 어떤 호스트에서 바이러스에 감염된 메시지를 네트워크로 전송했는지를 보려면 Incoming Mail(수신 메일) 페이지로 이동하고, 동일한 보고 기간을 지정하고, 바이러스 양성으로 정렬합니다. 마찬가지로, 어떤 IP 주소가 네트워크 내에서 바이러스 양성 이메일을 전송했는지 알아보려면 Outgoing Senders(발신 발신자) 페이지로 이동하여 바이러스 양성 메시지로 정렬할 수 있습니다.

VirusTypes Details(바이러스 유형 세부사항) 목록은 감염된 수신 및 발신 메시지와 감염된 총 메시지 수를 포함하여 특정 바이러스에 대한 정보를 표시합니다. 감염된 수신 메시지의 세부사항 목록에는 바이러스의 이름 및 이 바이러스로 감염된 수신 메시지의 수가 표시됩니다. 마찬가지로, 발신 메시지의 세부사항 목록에는 바이러스의 이름 및 이 바이러스로 감염된 발신 메시지의 수가 표시됩니다. Incoming Messages(수신 메시지), Outgoing Messages(발신 메시지) 또는 Total Infected Messages(감염된 총 메시지 수) 기준으로 Virus Type details(바이러스 유형 세부사항)를 정렬할 수 있습니다.

URL Filtering(URL 필터링) 페이지

- URL Filtering(URL 필터링) 보고서 모듈은 URL 필터링이 활성화된 경우에만 채워집니다.
- URL Filtering(URL 필터링) 보고서는 수신 및 발신 메시지에 대해 사용 가능합니다.
- URL 필터링 엔진으로 검사된(안티스팸/Outbreak Filter 검사의 일환으로 또는 메시지/콘텐츠 필터를 통해) 메시지만 이러한 모듈에 포함됩니다. 그러나 모든 결과가 URL 필터링 기능으로 인한 것이라 할 수는 없습니다.
- Top URL Categories(상위 URL 범주) 모듈은 검사된 메시지에서 발견된 모든 범주(콘텐츠 또는 메시지 필터와의 매치 여부와 상관없이)를 포함합니다.
- 각 메시지는 URL 평판 레벨 하나와만 연결할 수 있습니다. 여러 URL이 포함된 메시지의 경우 통계는 메시지에 있는 URL의 최하 평판을 반영합니다.
- Security Services(보안 서비스) > URL Filtering(URL 필터링)에 구성된 전역 화이트리스트의 URL은 보고서에 포함되지 않습니다.

  개별 필터에서 사용되는 화이트리스트의 URL은 보고서에 포함됩니다.

- 악성 URL은 Outbreak Filter가 평판이 좋지 않다고 판단한 URL입니다. 일반 URL은 Outbreak Filter에서 클릭 시 보호가 필요하다고 결정한 URL입니다. 따라서 일반 URL은 Cisco Web Security 프록시로 리디렉션하도록 재작성되었습니다.

- URL 범주 기반 필터의 결과는 콘텐츠 및 메시지 필터 보고서에서 반영됩니다.
- Cisco Web Security 프록시에 의한 클릭 시 URL 평가의 결과는 보고서에 반영되지 않습니다.

Web Interaction Tracking(웹 상호 작용 추적) 페이지

- Web Interaction Tracking(웹 상호 작용 추적) 보고서 모듈은 웹 상호 작용 추적 기능이 활성화된 경우에만 채워집니다.
- Web Interaction Tracking(웹 상호 작용 추적) 보고서 모듈은 실시간으로 업데이트되지 않으며 30분마다 새로 고쳐집니다. 또한 재작성된 URL을 클릭한 후 Web Interaction Tracking(웹 상호 작용 추적) 보고서에서 이 이벤트를 보고하는 데 최대 2시간이 걸릴 수 있습니다.
- Web Interaction Tracking(웹 상호 작용 추적) 보고서는 실시간으로 업데이트되지 않습니다. 클라우드에서 리디렉션되고 재작성된 URL을 클릭한 후 Web Interaction Tracking(웹 상호 작용 추적) 보고서에서 이 이벤트를 보고하는 데 최대 2시간이 걸릴 수 있습니다.
- Web Interaction Tracking(웹 상호 작용 추적) 보고서는 수신 및 발신 메시지에 대해 사용 가능합니다.
- 엔드 유저가 클릭한, 클라우드에서 리디렉션되고 재작성된 URL만(정책에 의해서든 Outbreak Filter에 의해서든) 이러한 모듈에 포함됩니다.
- Web Interaction Tracking(웹 상호 작용 추적) 페이지에는 다음과 같은 보고서가 포함되어 있습니다.

Top Rewritten Malicious URLs clicked by End Users(최종 사용자가 클릭한 재작성된 악의적인 상위 **URL)**. 다음 정보가 포함된 자세한 보고서를 보려면 URL을 클릭합니다.

- 재작성된 악의적인 URL을 클릭한 최종 사용자 목록.
- URL을 클릭한 날짜 및 시간.
- URL이 정책 또는 Outbreak Filter에 의해 재작성되었는지 여부.
- 재작성된 URL을 클릭했을 때 수행된 작업(허용, 차단 또는 알 수 없음). URL이 Outbreak Filter에 의해 재작성되었거나 최종 판정을 사용할 수 없는 경우 상태는 unknown(알 수 없음)으로 표시됩니다.

Top End Users who clicked on Rewritten Malicious URLs(재작성된 악의적인 **URL**을 클릭한 상위 최종 사용자**)**

Web Interaction Tracking Details(웹 상호 작용 추적 세부사항**)**. 다음 정보가 포함됩니다.

- 클라우드에서 리디렉션되고 재작성된 모든 URL(악의적인 URL 또는 악의적이지 않은 URL)의 목록. 자세한 보고서를 보려면 URL을 클릭합니다.
- 클라우드에서 리디렉션되고 재작성된 URL을 클릭했을 때 수행된 작업(허용, 차단 또는 알 수 없음).

표시할 데이터에 대해 다음 작업을 수행합니다.

- **Incoming Mail Policies(**수신 메일 정책**) > Outbreak Filters**를 선택하여 보안 침해 필터를 구성하고 메시지 수정 및 URL 재작성을 활성화합니다.
- **Cisco Security Proxy**로 리디렉션작업으로 콘텐츠 필터를 구성합니다.

최종 사용자가 클릭했을 때 URL(깨끗한 URL 또는 악의적인 URL)의 판정을 알 수 없는 경우 상태는 unknown(알 수 없음)으로 표시됩니다. 이는 사용자가 클릭한 시점에 URL이 추가 정밀 조사 중이었거나 웹 서버가 다운되었거나 도달할 수 없는 상태였기 때문에 발생할 수 있습니다.

- 최종 사용자가 재작성된 URL에서 클릭한 횟수. 클릭된 URL을 포함하는 모든 메시지의 목록을 보려면 번호를 클릭합니다.
- Web Interaction Tracking(웹 상호 작용 추적) 보고서를 사용하는 동안 다음과 같은 제한 사항에 유의해야 합니다.
  - 악의적 URL을 재작성한 후 메시지를 전달하고 다른 사용자(예: 관리자)에게 알리도록 콘텐츠 또는 메시지 필터를 구성한 경우, 알림을 받은 사용자가 재작성된 URL을 클릭하더라도 원래 수신자의 웹 상호 작용 추적 데이터가 증가합니다.
  - 재작성된 URL을 포함하는 격리된 메시지의 복사본을 웹 인터페이스를 통해 사용자(예: 관리자)에게 전송하는 경우, 이 사용자(메시지 복사본을 전송한 대상 사용자)가 재작성된 URL을 클릭하더라도 원래 수신자의 웹 상호 작용 추적 데이터가 증가합니다.
  - 언제든 어플라이언스의 시간을 수정할 계획이면 시스템 시간을 협정 세계시(UTC)와 동기화해야 합니다.

위조 이메일 일치 항목 보고서

위조 이메일 탐지 결과 모니터링, 612 페이지를 참조하십시오.

파일 평판 및 파일 분석 보고서

다음 보고서에 대한 자세한 내용은 파일 평판 및 파일 분석 보고 및 추적 , 484 페이지 섹션을 참조하십시오.

- AMP(Advanced Malware Protection)
- 파일 분석
- AMP 판정 업데이트

사서함 자동 치료 보고서

Mailbox Auto Remediation(사서함 자동 치료) 보고서 페이지(**Monitor(**모니터**)** > **Mailbox Auto Remediation(**사서함 자동 치료**)**)를 사용하여 사서함 치료 결과의 세부 정보를 볼 수 있습니다. 이 보고서를 사용하여 다음과 같은 세부 정보를 봅니다.

- 사서함 치료에 성공했거나 실패한 수신자 목록
- 메시지에 수행된 교정 조치
- SHA-256 해시와 관련된 파일 이름

메시지 추적에서 관련된 메시지를 보려면 SHA-256 해시를 클릭합니다.

자세한 내용은 Office 365 사서함에서 자동으로 메시지 치료, 561 페이지을 참조해 주십시오.

TLS Connections(TLS 연결) 페이지

TLS Connections(TLS 연결) 페이지는 주고받은 메일에 대한 TLS 연결의 전체 사용량을 보여줍니다. 보고서에서는 또한 TLS 연결을 사용하여 메일을 전송하는 각 도메인에 대한 세부사항도 보여줍니다.

TLS Connections(TLS 연결) 페이지는 다음 정보를 확인하는 데 사용할 수 있습니다.

- 전반적으로 어떤 수신 및 발신 연결 부분에서 TLS를 사용합니까?
- 어떤 파트너와의 TLS 연결에 성공했습니까?
- 어떤 파트너와의 TLS 연결에 실패했습니까?
- DANE 지원을 사용하여 어떤 파트너와의 TLS 연결에 성공했습니까?
- DANE 지원을 사용하여 어떤 파트너와의 TLS 연결에 실패했습니까?
- 어떤 파트너가 TLS 인증서에 문제가 있습니까?
- 파트너별 TLS를 사용하는 전체 메일 비율은 어떻게 됩니까?
- DANE 지원을 사용하여 발신 TLS 연결에 성공한 비율은 어떻게 됩니까?
- DANE 지원을 사용하여 발신 연결에 실패한 비율은 어떻게 됩니까?

TLS Connections(TLS 연결) 페이지는 수신 연결용 섹션 및 발신 연결용 섹션으로 구분됩니다. 각 섹션에는 그래프, 요약, 그리고 세부사항이 포함된 테이블이 있습니다.

그래프에는 지정한 시간 범위 동안 TLS로 암호화된/암호화되지 않은 수신 또는 발신 연결의 보기가 표시됩니다. 그래프에는 총 메시지 볼륨, 암호화된/암호화되지 않은 메시지의 볼륨, 성공한/실패한 TLS 암호화 메시지 볼륨, 성공한/실패한 DANE 연결 볼륨이 표시됩니다. 그래프는 TLS가 필수인 연결과 TLS가 기본 설정일 뿐인 연결 간에 구분됩니다.

암호화된 메시지를 보내거나 받는 도메인에 대한 세부사항이 테이블에 표시됩니다. 각 도메인에 대해 성공한/실패한 필수 및 기본 설정 TLS 연결 수, 시도된 총 TLS 연결 수(성공 또는 실패), 암호화되지 않은 총 연결 수 및 총 DANE 연결 수(성공 또는 실패에 따라)를 볼 수 있습니다. 또한 TLS가 시도된 모든 연결의 비율 및 성공적으로 전송된 암호화된 총 메시지 수(TLS가 기본 설정이든 필수이든 상관없이)도 볼 수 있습니다. 이 테이블 하단에 있는 Column(열) 링크를 클릭하여 열을 표시하거나 숨길 수 있습니다.

Inbound SMTP Authentication(인바운드 SMTP 인증) 페이지

Inbound SMTP authentication(인바운드 SMTP 인증) 페이지는 클라이언트 인증서의 사용 및 ESA와 사용자 메일 클라이언트 간 SMTP 세션 인증을 위한 SMTP AUTH 명령을 보여줍니다. 어플라이언스는 인증서 및 SMTP AUTH 명령을 수락하는 경우 메일 클라이언트에 대한 TLS 연결을 설정합니다. 클라이언트는 메시지를 전송하는 데 이 연결을 사용합니다. 어플라이언스는 사용자 단위로 이러한 시도를 추적할 수 없으므로, 보고서는 도메인 이름 및 도메인 IP 주소를 기반으로 SMTP 인증에 대한 세부사항을 표시합니다.

이 보고서를 사용하면 다음 정보를 확인할 수 있습니다.

- 전체적으로 SMTP 인증을 사용하는 수신 연결은 몇 개입니까?

- 인증된 클라이언트를 사용하는 연결은 몇 개입니까?
- SMTP AUTH를 사용하는 연결은 몇 개입니까?
- SMTP 인증을 사용하려고 시도할 때 어떤 도메인이 연결에 실패합니까?
- SMTP 인증에 실패할 때 대안을 사용하여 성공한 연결은 몇 개입니까?

Inbound SMTP Authentication(인바운드 SMTP 인증) 페이지에는 수신된 연결에 대한 그래프, SMTP 인증 연결을 시도한 메일 수신자에 대한 그래프, 그리고 연결 인증 시도에 대한 세부사항을 보여주는 테이블이 포함되어 있습니다.

Received Connections(수신된 연결) 그래프는 지정한 시간 범위 동안 SMTP 인증을 사용하여 연결을 인증하려고 시도한 메일 클라이언트로부터의 수신 연결을 보여줍니다. 이 그래프에는 어플라이언스가 수신한 총 연결 수, SMTP 인증을 사용하여 인증하려고 시도하지 않은 횟수, 클라이언트 인증서를 사용하여 연결을 인증하는 데 실패한/성공한 횟수, 그리고 SMTP AUTH 명령을 사용하여 인증하는 데 실패한/성공한 횟수가 표시됩니다.

Received Recipients(수신된 수신자) 그래프는 해당 메일 클라이언트가 SMTP 인증을 사용하여 메시지를 전송하기 위해 ESA에 대한 연결을 인증하려고 시도한 수신자 수를 보여줍니다. 또한 연결이 인증된 수신자 수 및 연결이 인증되지 않은 수신자 수도 보여줍니다.

SMTP Authentication details(SMTP 인증 세부사항 테이블)는 해당 사용자가 메시지를 전송하기 위해 ESA에 대한 연결을 인증하려고 시도한 도메인에 대한 세부사항을 표시합니다. 각 도메인에 대해 클라이언트 인증서를 사용하여 성공 또는 실패한 연결 시도 횟수, SMTP AUTH 명령을 사용하여 성공 또는 실패한 연결 시도 횟수, 그리고 클라이언트 인증서 연결 시도 실패 후 SMTP AUTH로 전환한 횟수를 볼 수 있습니다. 도메인 이름 또는 도메인 IP 주소로 이 정보를 표시하려면 페이지 상단에 있는 링크를 사용할 수 있습니다.

Rate Limits(속도 제한) 페이지

봉투 발신자에 의한 속도 제한 기능을 사용하면 mail-from 주소를 기반으로 개별 발신자의 시간 간격당 이메일 메시지 수신자의 수를 제한할 수 있습니다. Rate Limits(속도 제한) 보고서는 가장 눈에 띄게 이 제한을 초과한 발신자를 보여줍니다.

이 보고서를 사용하면 다음을 식별할 수 있습니다.

- 대량 스팸 발신에 사용되었을 수 있는 손상된 사용자 계정.
- 알림, 자동화된 발표 등에 이메일을 사용하는 조직의 제어 불가능한 애플리케이션.
- 내부 결제 또는 리소스 관리 목적으로 조직에서 이메일 활동이 과중한 소스.
- 달리 스팸으로 간주되지 않을 수 있는 대량 인바운드 이메일 트래픽의 소스.

Internal Users(내부 사용자) 또는 Outgoing Senders(외부 발신자) 등 내부 발신자에 대한 통계를 포함하는 기타 보고서는 전송된 메시지의 수만 측정합니다. 소수의 메시지를 다수의 수신자에게 보내는 발신자는 식별하지 않습니다.

Top Offenders by Incident(인시던트별 상위 위반자) 차트는 구성된 제한보다 더 많은 수신자에게 메시지를 보내려고 가장 자주 시도한 봉투 발신자를 보여줍니다. 각 시도가 하나의 인시던트입니다. 이 차트는 모든 리스너로부터 인시던트 수를 집계합니다.

Top Offenders by Rejected Recipients(거부된 수신자별 상위 위반자) 차트는 구성된 제한을 넘어 최대 수신자에게 메시지를 보낸 봉투 전송자를 보여줍니다. 이 차트는 모든 리스너로부터 수신자 수를 집계합니다.

봉투 발신자별로 속도 제한을 구성하거나 기존 속도 제한을 수정하려면 메일 플로우 정책을 사용하여 수신 메시지에 대한 규칙 정의, 108 페이지 섹션을 참조하십시오.

System Capacity(시스템 용량) 페이지

System Capacity(시스템 용량) 페이지는 작업 대기열에 있는 메시지, 작업 대기열에서 사용된 평균 시간, 수신/발신 메시지(볼륨, 크기 및 수), 전체 CPU 사용량, 기능별 CPU 사용량, 메모리 페이지 스와핑 정보 등 시스템 로드에 대한 자세한 내용을 제공합니다.

System Capacity(시스템 용량) 페이지는 다음 정보를 확인하는 데 사용할 수 있습니다.

- 어플라이언스가 권장 용량을 초과하며 컨피그레이션 최적화 또는 추가 어플라이언스가 필요한 시기를 식별합니다.
- 앞으로의 용량 문제를 보여주는 시스템 동작의 기록 추세를 식별합니다.
- 문제 해결에 도움이 되도록, 시스템의 어떤 부분이 가장 많은 리소스를 사용하는지를 식별합니다.

용량이 메시지 볼륨에 적절한지 확인하려면 어플라이언스를 모니터링하는 것이 중요합니다. 시간이 지나면 볼륨이 불가피하게 증가하므로, 적절한 모니터링을 통해 추가 용량 또는 컨피그레이션 변경을 사전에 적용해야 합니다. 시스템 용량을 모니터링하는 가장 효과적인 방법은 전체적인 볼륨, 작업 대기열의 메시지 수 및 리소스 절약 모드의 인시던트 수를 추적하는 것입니다.

- **Volume(볼륨)**: 현재 환경에서 "정상적인" 메시지 볼륨 및 "일상적인" 급증을 이해하는 것이 중요합니다. 시간의 경과에 따라 이 데이터를 추적하여 볼륨 증가를 측정하십시오. 시간의 경과에 따른 볼륨을 추적하려면 Incoming Mail(수신 메일) 및 Outgoing Mail(발신 메일) 페이지를 사용할 수 있습니다. 자세한 내용은 시스템 용량 - 수신 메일, 824 페이지 및 시스템 용량 - 발신 메일, 825 페이지를 참조하십시오.
- **Work Queue(작업 대기열)**: 작업 대기열은 스팸 공격을 흡수 및 필터링하고 특별한 ham 메시지의 증가를 처리하는 "충격 흡수자" 역할을 하도록 설계되었습니다. 그러나 작업 대기열은 스트레스를 받는 시스템에 대한 최고의 표시기이며, 빈번한 작업 대기열 백업은 용량 문제를 나타낼 수 있습니다. 메시지가 작업 대기열에 머무는 평균 시간 및 작업 대기열에서의 활동을 추적하려면 WorkQueue(작업 대기열) 페이지를 사용할 수 있습니다. 자세한 내용은 시스템 용량 - 작업 대기열, 824 페이지를 참고하십시오.
- **Resource Conservation Mode(리소스 절약 모드)**: 어플라이언스는 과부하 상태가 되면 RCM(Resource Conservation Mode) 모드로 들어가며 CRITICAL 시스템 알림을 전송합니다. 이 기능은 디바이스를 보호하고 메시지의 백로그를 처리하도록 설계되었습니다. 어플라이언스가 RCM에 들어가는 경우는 매우 드물게, 메일 볼륨이 매우 크거나 비정상적으로 증가하는 동안에만 발생해야 합니다. 빈번한 RCM 알림은 시스템이 과부하 상태임을 나타내는 것일 수 있습니다. 시스템 용량 - 시스템 로드, 825 페이지를 참조하십시오.

관련 주제

- 시스템 용량 - 작업 대기열, 824 페이지

시스템 용량 - 작업 대기열

Workqueue(작업 대기열) 페이지는 메시지가 작업 대기열에 머무는 평균 시간을 보여줍니다(스팸 대기열 또는 정책, 바이러스, 전파 확산 대기열에 머무는 시간 제외). 1시간에서 1개월 사이의 기간을 볼 수 있습니다. 이러한 평균은 메일 전달을 지연시키는 단기 이벤트와 시스템 워크로드의 장기 추세를 모두 파악하는 데 도움이 될 수 있습니다.

참고 메시지가 격리에서 작업 대기열로 릴리스되면 "작업 대기열의 평균 시간" 메트릭이 이 시간을 무시합니다. 이렇게 되면 격리에서 사용되는 시간이 연장되어 이중 계산 및 왜곡된 통계가 방지됩니다.

보고서에는 또한 지정된 기간에 작업 대기열에 포함된 메시지의 볼륨과, 동일한 기간 전체에서 작업 대기열의 최대 메시지 수가 표시됩니다. 작업 대기열에 포함된 최대 메시지 수가 그래픽으로 표시되어 작업 대기열 임계값 레벨도 보여줍니다.

작업 대기열에 더러 나타나는 급증은 예상되는 정상적인 현상입니다. 작업 대기열의 메시지 수가 구성된 임계값보다 장시간 높게 유지되면 이는 용량 문제를 나타낼 수 있습니다. 이 시나리오에서는 임계값 조정을 고려해보거나 시스템 구성을 검토하십시오.

작업 대기열 임계값 레벨 변경에 대한 지침은 시스템 상태 파라미터에 대한 임계값 설정, 961 페이지 섹션을 참조하십시오.

팁 작업 대기열 페이지를 검토할 때 작업 대기열 백업의 빈도를 측정하고 메시지 10,000개를 초과하는 작업 대기열 백업을 메모해둘 수 있습니다.

시스템 용량 - 수신 메일

Incoming Mail(수신 메일) 페이지는 수신 연결, 총 수신 메시지 수, 평균 메시지 크기 및 총 수신 메시지 크기를 보여줍니다. 지정한 시간 범위로 결과를 제한할 수 있습니다. 현재 환경에서 정상적인 메시지 볼륨 및 급증의 추세를 이해하는 것이 중요합니다. 시간에 따른 볼륨 증가를 추적하고 시스템 용량을 계획하려면 Incoming Mail(수신 메일) 페이지를 사용할 수 있습니다. 특정 도메인에서 현재 네트워크로 전송되는 이메일 볼륨의 추세를 보려면 Incoming Mail(수신 메일) 데이터를 Sender Profile(발신자 프로필) 데이터와 비교할 수도 있습니다.

참고 수신 연결 수의 증가가 반드시 시스템 로드에 영향을 미치는 것은 아닙니다.

시스템 용량 - 발신 메일

Outgoing Mail(발신 메일) 페이지는 발신 연결, 총 발신 메시지 수, 평균 메시지 크기 및 총 발신 메시지 크기를 보여줍니다. 지정한 시간 범위로 결과를 제한할 수 있습니다. 현재 환경에서 정상적인 메시지 볼륨 및 급증의 추세를 이해하는 것이 중요합니다. 시간에 따른 볼륨 증가를 추적하고 시스템 용량을 계획하려면 Outgoing Mail(발신 메일) 페이지를 사용할 수 있습니다. 특정 도메인 또는 IP 주소에서 전송되는 이메일 볼륨의 추세를 보려면 Outgoing Mail(발신 메일) 데이터를 Outgoing Destinations(발신 대상) 데이터와 비교할 수도 있습니다.

시스템 용량 - 시스템 로드

시스템 로드 보고서는 다음을 보여줍니다.

- 전체 CPU 사용
- 메시지 페이지 스와핑
- 리소스 절약 활동

전체 **CPU** 사용

Email Security Appliance는 메시지 처리량 개선을 위해 유휴 CPU 리소스를 사용하도록 최적화됩니다. 높은 CPU 사용량은 시스템 용량 문제를 나타내지 않을 수 있습니다. 높은 CPU 사용량이 지속적인 높은 볼륨의 메모리 페이지 스와핑과 결합되면 이는 용량 문제일 수 있습니다.

참고 이 그래프는 또한 CPU 사용량에 대한 임계값 레벨을 보여줍니다. 임계값 레벨을 변경하려면 웹 인터페이스의 **System Administration**(시스템 관리) > **System Health**(시스템 상태) 페이지 또는 CLI의 **healthconfig** 명령을 사용합니다. 시스템 상태 파라미터에 대한 임계값 설정, 961 페이지를 참조하십시오.

메일 처리, 스팸 및 바이러스 엔진, 보고, 격리 등의 여러 기능에 사용된 CPU의 양을 보여주는 그래프도 이 페이지에 표시됩니다. 기능별 CPU 그래프는 제품의 어떤 영역에서 시스템의 리소스를 가장 많이 사용하는지를 보여주는 훌륭한 지표입니다. 어플라이언스를 최적화해야 하는 경우 어떤 기능을 조정 또는 비활성화해야 할지를 결정하는 데 이 그래프가 도움이 될 수 있습니다.

메시지 페이지 스와핑

메모리 페이지 스와핑 그래프는 시스템이 디스크에 페이징해야 하는 빈도를 보여줍니다. 이 그래프는 또한 메모리 페이지 스와핑에 대한 임계값 레벨도 보여줍니다. 임계값 레벨을 변경하려면 웹 인터페이스의 **System Administration**(시스템 관리) > **System Health**(시스템 상태) 페이지 또는 CLI의 **healthconfig** 명령을 사용합니다. 시스템 상태 파라미터에 대한 임계값 설정, 961 페이지를 참조하십시오.

리소스 절약 활동

리소스 절약 활동 그래프는 어플라이언스가 RCM(Resource Conservation Mode)으로 들어간 횟수를 보여줍니다. 예를 들어 그래프에 n번이 표시되면 이는 어플라이언스가 RCM에 n번 들어갔으며 적어도 n-1번 RCM에서 빠져나왔음을 의미합니다.

어플라이언스가 RCM에 들어가는 경우는 매우 드물게, 메일 볼륨이 매우 크거나 비정상적으로 증가하는 동안에만 발생해야 합니다. 리소스 절약 활동 그래프에 어플라이언스가 RCS에 자주 들어가는 것으로 표시되면, 이는 시스템이 과부화되고 있음을 나타내는 것일 수 있습니다.

메모리 페이지 스와핑에 대한 참고 사항

시스템은 메모리를 정기적으로 스와핑하도록 설계되었으므로, 어느 정도의 메모리 스와핑은 발생할 수 있으며 이것이 어플라이언스의 문제를 나타내지는 않습니다. 시스템이 일관되게 대량의 메모리를 서로 바꾸지 않는 한 메모리 스와핑은 정상이며 예상된 동작입니다(특히 C170 및 C190 어플라이언스에서). 성능을 높이려면 네트워크에 어플라이언스를 추가하거나 최대 처리량이 보장되도록 컨피그레이션을 조정해야 할 수 있습니다.

시스템 용량 - 전체

All(전체) 페이지는 서로 다른 보고서 사이의 관계를 파악할 수 있도록 모든 이전 시스템 용량 보고서를 단일 페이지로 통합합니다. 예를 들면, 과도한 메모리 스와핑이 발생할 때 메시지 대기열의 볼륨이 동시에 높아지는 것을 볼 수 있습니다. 이는 용량 문제를 나타내는 것일 수 있습니다. 이 페이지를 PDF로 저장하여 나중에 참조하도록(또는 지원 담당자와 공유하기 위해) 시스템 성능의 스냅샷을 보관할 수 있습니다. 영어 이외의 언어로 PDF를 생성하는 방법에 대한 자세한 내용은 보고서에 대한 참고 사항, 832 페이지 섹션을 참조하십시오.

System Status(시스템 상태) 페이지

System Status(시스템 상태**)** 페이지에는 시스템에 대한 실시간 메일 및 DNS 활동이 자세히 표시됩니다. CLI의 status detail 및 **dnsstatus** 명령을 통해서도 동일한 정보를 이용할 수 있습니다. 자세한 내용은 CLI를 사용한 관리 및 모니터링, 997 페이지에서 status detail 명령의 "자세한 이메일 상태 모니터링" 및 **dnsstatus** 명령의 "DNS 상태 확인"을 참조하십시오.

System Status(시스템 상태) 페이지는 System Status(시스템 상태), Gauges(게이지), Rates(속도) 및 Counters(카운터)의 네 섹션으로 구성됩니다.

관련 주제

- System Status, 826 페이지
- 센서, 827 페이지
- 비율, 827 페이지
- 카운터, 827 페이지

System Status

System Status(시스템 상태) 섹션은 Mail System Status(메일 시스템 상태) 및 Version Information(버전 정보)을 보여줍니다.

관련 주제

- 메일 시스템 상태, 827 페이지
- 버전 정보, 827 페이지

메일 시스템 상태

Mail System Status(메일 시스템 상태) 섹션에는 다음이 포함됩니다.

- 시스템 상태(시스템 상태에 대한 자세한 내용은 Status(상태), 799 페이지 참조)
- 상태가 마지막으로 보고된 시간
- 어플라이언스의 가동 시간
- 아직 전달을 위해 대기열에 추가되지 않은 메시지를 포함하여, 시스템에서 가장 오래된 메시지

버전 정보

Version Information(버전 정보) 섹션에는 다음이 포함됩니다.

- 어플라이언스 모델 이름
- 설치된 AsyncOS 운영 체제의 버전 및 빌드 날짜
- AsyncOS 운영 체제 설치 날짜
- 연결된 시스템의 일련 번호

이러한 정보는 Cisco 고객 지원에 문의할 때 유용합니다. (기술 지원 이용, 1171 페이지참조.)

센서

Gauges(게이지) 섹션은 대기열 및 리소스 사용률을 보여줍니다.

- 메일 처리 대기열
- 큐에 있는 활성 수신자
- 대기열 공간
- CPU 사용률

Mail Gateway Appliance는 AsyncOS 프로세스가 사용하는 CPU의 비율을 참조합니다. CASE는 안티스팸 검사 엔진 및 Outbreak Filter 프로세스를 비롯한 여러 항목을 참조합니다.

- 일반 리소스 사용률
- 로깅 디스크 사용률

비율

Rates(속도) 섹션은 수신자에 대한 처리 속도를 보여줍니다.

- 메일 처리율
- 완료 비율

카운터

시스템 통계에 대한 누적 이메일 모니터링 카운터를 재설정하고 카운터가 마지막으로 재설정된 시간을 볼 수 있습니다. 재설정은 도메인 단위 카운터는 물론 시스템 카운터에도 영향을 미칩니다. 재시도 예약과 관련된 전달 대기열에 있는 메시지에 대한 카운터에는 재설정이 영향을 미치지 않습니다.

참고 관리자 또는 운영자 그룹에 있는 사용자 계정만 카운터 재설정 기능에 액세스할 수 있습니다. 게스트 그룹에서 만드는 사용자 계정은 카운터를 재설정할 수 없습니다. 자세한 내용은 사용자 계정 작업, 893 페이지를 참고하십시오.

카운터를 재설정하려면 Reset Counters(카운터 재설정)를 클릭합니다. 이 버튼은 CLI의 **resetcounters** 명령과 동일한 기능을 제공합니다. 자세한 내용은 이메일 모니터링 카운터 재설정, 1013 페이지의 내용을 참고하십시오.

- 메일 처리 이벤트
- 완료 이벤트
- 도메인 키 이벤트
- DNS 상태

High Volume Mail(대용량 메일) 페이지

참고 High Volume Mail(대용량 메일) 페이지에는 Header Repeats(헤더 반복) 규칙을 사용하는 메시지 필터에서 오는 데이터만 표시됩니다.

High Volume Mail(대용량 메일) 페이지에는 다음 보고서가 막대 차트 형식으로 포함됩니다.

- **Top Subjects(**상위 제목**)**. AsyncOS에서 수신한 메시지의 상위 제목을 파악하려면 이 차트를 사용할 수 있습니다.
- **Top Envelope Senders(**상위 봉투 발신자**)**. AsyncOS에서 수신한 메시지의 상위 봉투 발신자를 파악하려면 이 차트를 사용할 수 있습니다.
- **Top Message Filters by Number of Matches(**일치 수 기준 상위 메시지 필터**)**. 상위 메시지 필터(헤더 반복 규칙 사용) 일치를 파악하려면 이 차트를 사용할 수 있습니다.

High Volume Mail(대용량 메일) 페이지는 또한 상위 메시지 필터 및 개별 메시지 필터에 대한 일치 수를 테이블 형식으로 제공합니다. Message Tracking(메시지 추적)을 사용하여 번호에 포함된 모든 메시지의 목록을 보려면 해당 번호를 클릭합니다.

보고할 시간 범위(예: 시간, 주 또는 사용자 지정 범위)를 선택할 수 있습니다. 모든 보고서에 대해 **Export(**내보내기**)** 링크를 통해 CSV 형식으로 또는 **Printable (PDF)(**인쇄 가능**(PDF))** 링크를 클릭하여 PDF 형식으로 그래프에 대한 데이터 또는 세부사항 목록을 내보낼 수 있습니다.

Message Filters(메시지 필터) 페이지

Message Filters(메시지 필터) 페이지에는 상위 메시지 필터 일치(일치하는 메시지가 가장 많은 메시지 필터)에 대한 정보가 막대 차트와 테이블의 두 가지 형식으로 표시됩니다.

막대 차트를 사용하면 수신 및 발신 메시지에 의해 가장 많이 트리거되는 메시지 필터를 찾을 수 있습니다. 테이블 형식은 상위 메시지 필터 및 개별 메시지 필터에 대한 일치 수를 보여줍니다. Message

Tracking(메시지 추적)을 사용하여 번호에 포함된 모든 메시지의 목록을 보려면 해당 번호를 클릭합니다.

보고할 시간 범위(예: 시간, 주 또는 사용자 지정 범위)를 선택할 수 있습니다. 모든 보고서에 대해 **Export(**내보내기**)** 링크를 통해 CSV 형식으로 또는 **Printable (PDF)(**인쇄 가능**(PDF))** 링크를 클릭하여 PDF 형식으로 그래프에 대한 데이터 또는 세부사항 목록을 내보낼 수 있습니다.

CSV 데이터 검색

Email Security Monitor(이메일 보안 모니터)에서 차트 및 그래프 작성에 사용된 데이터를 CSV 형식으로 검색할 수 있습니다. CSV 데이터에 두 가지 방식으로 액세스할 수 있습니다.

- 이메일을 통해 전달되는 **CSV** 보고서. 이메일을 통해 전달되거나 보관되는 CSV 보고서를 생성할 수 있습니다. 이 전달 방법은 Email Security Monitor(이메일 보안 모니터) 페이지에 표시되는 각 테이블에 대해 별도의 보고서를 만들려는 경우 또는 내부 네트워크에 액세스하지 못하는 사용자에게 CSV 데이터를 전송하려는 경우에 유용합니다.

  CSV(comma-separated values) 보고서 유형은 예약된 보고서의 테이블 형식 데이터를 포함하는 ASCII 텍스트 파일입니다. 각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 한 보고서에 두 가지 이상의 테이블 유형이 포함되어 있으면 각 테이블에 대해 별도의 CSV 파일이 생성됩니다. 단일 보고서에 대한 여러 CSV 파일은 보관된 파일 스토리지 옵션의 경우 단일 .zip 파일로 압축되고, 이메일 전달의 경우 별도의 이메일 메시지로 모두 첨부됩니다.

  예약된 보고서 또는 온디맨드 보고서 구성에 대한 자세한 내용은 보고 개요, 831 페이지 섹션을 참조하십시오.

- **HTTP**를 통해 검색되는 **CSV** 파일. Email Security Monitor(이메일 보안 모니터) 기능에서 차트 및 그래프 작성에 사용된 데이터를 HTTP를 통해 검색할 수 있습니다. 이 전달 방법은 다른 툴을 사용하여 데이터를 추가로 분석하려는 경우 유용합니다. 예를 들면 원시 데이터를 다운로드하고, 처리하고, 다른 시스템에서 결과를 표시하는 자동 스크립트를 사용하여 이 데이터의 검색을 자동화할 수 있습니다.

관련 주제

- 자동화된 프로세스를 통해 CSV 데이터 검색, 829 페이지

자동화된 프로세스를 통해 CSV 데이터 검색

필요한 HTTP 쿼리를 가져오는 가장 쉬운 방법은 원하는 데이터 유형을 표시하도록 이메일 보안 모니터 페이지 중 하나를 구성하는 것입니다. 그런 다음 **Export(**내보내기**)** 링크를 복사할 수 있습니다. 이것이 다운로드 URL입니다. 이와 같이 데이터 검색을 자동화할 경우 다운로드 URL에서 어떤 매개변수를 수정할지, 어떤 것을 변경할지에 유의해야 합니다(아래 참조).

다운로드 URL은 동일한 쿼리를 실행하고(적절한 HTTP 인증 사용) 유사한 데이터 집합을 가져올 수 있는 외부 스크립트로 복사할 수 있도록 인코딩됩니다. 스크립트는 기본 HTTP 인증 또는 쿠키 인증을 사용할 수 있습니다. 자동화된 프로세스를 통해 CSV 데이터를 검색할 때 다음에 유의하십시오.

- URL을 다시 사용할 때와 관련된 시간 범위 선택(지정된 시간, 일, 주 등이 지난 후). "Past Day(지정된 일수 이후)"에 대해 설정된 CSV 데이터를 검색하도록 URL을 복사하는 경우 다음에 이 URL

을 사용할 때, URL을 다시 전송하는 시기로부터 "Past Day(지정된 일수 이후)"에 해당하는 새로운 데이터 집합을 가져올 수 있습니다. 시간 범위 선택은 유지되며 CSV 쿼리 문자열에 나타납니다(예: date_range=current_day).

- 데이터 집합에 대한 필터링 및 그룹화 기본 설정. 필터는 쿼리 문자열에 유지되고 나타납니다. 보고서의 필터는 드뭅니다(예: Outbreaks(전파 확산) 보고서의 "Global / Local" 전파 확산 선택자).
- CVS 다운로드는 선택한 시간 범위에 대해 모든 데이터 행을 테이블에서 반환합니다.
- CSV 다운로드는 타임스탬프와 키로 정렬된 데이터 행을 테이블에서 반환합니다. 별도의 단계에서 추가로 정렬할 수 있습니다(예: 스프레드시트 애플리케이션을 통해).
- 첫 번째 열에는 보고서에 있는 표시 이름과 일치하는 열 헤더가 포함됩니다. 타임스탬프(타임스탬프, 830 페이지 참조) 및 키(키, 831 페이지 참조)도 나타납니다.

관련 주제

- 샘플 URL, 830 페이지
- 기본 HTTP 인증 자격 증명 추가, 830 페이지
- 파일 형식, 830 페이지
- 타임스탬프, 830 페이지
- 키, 831 페이지
- 스트리밍, 831 페이지

샘플 URL

http://example.com/monitor/content_filters?format=csv&sort_col_ss_0_0_0=
MAIL_CONTENT_FILTER_INCOMING.RECIPIENTS_MATCHED&section=ss_0_0_0
&date_range=current_day&sort_order_ss_0_0_0=desc&report_def_id=mga_content_filters

기본 HTTP 인증 자격 증명 추가

URL에 대한 기본 HTTP 인증 자격 증명을 지정하려면

`http://example.com/monitor/`

다음으로 전환:

`http://username:password@example.com/monitor/`

파일 형식

다운로드 파일은 CSV 형식이며 파일 확장명은 .csv입니다. 파일 헤더에는 보고서의 이름으로 시작되는 기본 파일 이름이 있고, 그 뒤에 보고서 섹션이 나옵니다.

타임스탬프

스트림 데이터를 내보내면 각각의 원시 시간 "간격"에 대한 시작 및 종료 타임스탬프가 표시됩니다. 시작 및 종료 타임스탬프가 각각 두 개씩 제공됩니다. 하나는 숫자 형식이고 다른 하나는 사람이 읽을 수 있는 문자열 형식입니다. 타임스탬프는 GMT 시간입니다. 따라서 여러 표준 시간대의 어플라이언스가 있는 경우 로그 집계가 더 쉬워집니다.

매우 드물기는 하지만 데이터가 다른 소스의 데이터와 병합되는 경우 내보내기 파일에 타임스탬프가 포함되지 않을 수 있습니다. 예를 들어 Outbreak Details(Outbreak 세부사항) 내보내기는 보고서 데

이터를 TOC(Threat Operations Center) 데이터와 병합하는데, 이 경우 간격이 없으므로 타임스탬프가 무의미합니다.

키

내보내기에는 보고서 테이블 키도 포함됩니다(보고서에서 키가 보이지 않는 경우에도). 키가 보이는 경우, 보고서에서 보이는 표시 이름이 열 헤더로서 사용됩니다. 그렇지 않은 경우 "key0," "key1" 등의 열 헤더가 표시됩니다.

스트리밍

대부분의 내보내기는 데이터의 양이 잠재적으로 매우 크므로 클라이언트로 다시 데이터를 스트리밍합니다. 그러나 일부 내보내기는 스트리밍 데이터보다는 전체 결과 집합을 반환합니다. 이 경우는 일반적으로 보고서 데이터가 보고서 이외의 데이터와 집계될 때입니다(예: Outbreak 세부사항).

보고 개요

AsyncOS에서의 보고는 다음의 세 가지 기본 작업과 관련됩니다.

- 매일, 매주 또는 매달 실행할 예약된 보고서를 만들 수 있습니다.
- 보고서를 즉시 생성할 수 있습니다("온디맨드" 보고서).
- 전에 실행한 보고서의 보관된 버전을 볼 수 있습니다(예약 및 온디맨드 모두).

Monitor(모니터) > Scheduled Reports(예약된 보고서) 페이지를 통해 예약된 보고서 및 온디맨드 보고서를 구성합니다. Monitor(모니터) > Archived Reports(보관된 보고서) 페이지를 통해 보관된 보고서를 봅니다.

어플라이언스에는 가장 최근에 생성된 보고서(모든 보고서의 총 버전 최대 1,000개)가 보존됩니다. 0명을 포함하여 원하는 만큼 보고서의 수신자를 정의할 수 있습니다. 이메일 수신자를 지정하지 않더라도 시스템에서는 여전히 보고서를 보관합니다. 그러나 보고서를 대량의 주소로 전송하려면 수신자를 개별적으로 나열하는 것보다 메일 목록을 작성하는 것이 더 쉬울 수 있습니다.

기본적으로 어플라이언스는 각 예약된 보고서의 가장 최신 보고서 12개를 보관합니다. 보고서는 어플라이언스의 /saved_reports 디렉터리에 저장됩니다. (자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지를 참조해 주십시오.)

관련 주제

- 예약된 보고서 유형, 831 페이지
- 보고서의 반환 주소 설정, 832 페이지

예약된 보고서 유형

다음 보고서 유형 중에서 선택할 수 있습니다.

- Content Filters(콘텐츠 필터)
- 전송 상태
- DLP 인시던트 요약

- Executive Summary
- 수신 메일 요약
- 내부 사용자 요약
- Outgoing Destinations(발신 대상)
- 발송 메일 요약
- Outgoing Senders: Domains(발신 발신자: 도메인)
- 그룹
- 시스템 용량
- TLS 연결
- Outbreak Filters
- Virus Types(바이러스 유형)

각 보고서는 해당 Email Security Monitor(이메일 보안 모니터) 페이지의 요약으로 구성됩니다. 따라서 예를 들어 Content Filters(콘텐츠 필터) 보고서는 **Monitor(모니터) > Content Filters(콘텐츠 필터)** 페이지에 표시된 정보의 요약을 제공합니다. Executive Summary(실행 요약) 보고서는 **Monitor(모니터) > Overview(개요)** 페이지를 기반으로 합니다.

관련 주제

- 보고서에 대한 참고 사항, 832 페이지

보고서에 대한 참고 사항

PDF 형식의 Content Filter(콘텐츠 필터) 보고서는 최대 40개의 콘텐츠 필터로 제한됩니다. CSV 형식의 보고서를 통해 전체 목록을 가져올 수 있습니다.

참고 Windows 컴퓨터에서 중국어, 일본어 또는 한국어로 PDF를 생성하려면 Adobe.com에서 해당 글꼴 팩을 다운로드하여 로컬 컴퓨터에 설치해야 합니다.

보고서의 반환 주소 설정

보고서 반환 주소 설정에 대한 자세한 내용은 어플라이언스 생성 메시지에 대한 반환 주소 구성, 960 페이지 섹션을 참조하십시오. CLI에서 **addressconfig** 명령을 사용합니다.

보고서 관리

보관된 예약된 보고서를 만들고 수정하고 삭제하고 볼 수 있습니다. 보고서를 즉시 실행할 수도 있습니다(온디맨드 보고서). Content Filters(콘텐츠 필터), DLP Incident Summary(DLP 인시던트 요약), Executive Summary(실행 요약), Incoming Mail Summary(수신 메일 요약), Internal Users Summary(내부 사용자 요약), Outgoing Mail Summary(발신 메일 요약), Sender Groups(발신자 그룹) 및 Outbreak Filters 등의 보고서 유형을 이용할 수 있습니다. 이러한 보고서를 관리하고 보는 방법은 아래에서 설명합니다.

참고 클러스터 모드에서는 보고서를 볼 수 없습니다. 시스템 모드에서는 보고서를 볼 수 있습니다.

Monitor(모니터) > Scheduled Reports(예약된 보고서) 페이지에는 어플라이언스에서 이미 생성된 예약된 보고서 목록이 표시됩니다.

관련 주제

- 예약 보고서, 833 페이지
- Archived Reports(보관된 보고서), 834 페이지

예약 보고서

매일, 매주 또는 매달 실행하도록 보고서를 예약할 수 있습니다. 보고서를 실행할 시간을 선택할 수 있습니다. 보고서를 언제 실행하든, 지정한 기간(예: 3일 또는 이전 달)의 데이터만 보고서에 포함됩니다. 예를 들어 오전 1시에 실행하도록 예약된 일일 보고서에는 전날 자정부터 자정까지의 데이터가 포함됩니다.

예약된 보고서의 기본 집합이 어플라이언스에 포함되어 있으며, 이를 사용하거나 수정하거나 삭제할 수 있습니다.

관련 주제

- 자동으로 생성되도록 보고서 예약 , 833 페이지
- 예약된 보고서 편집 , 834 페이지
- 예약된 보고서 삭제, 834 페이지

자동으로 생성되도록 보고서 예약

단계 **1** Monitor(모니터) > Scheduled Reports(예약된 보고서) 페이지에서 **Add Scheduled Report(**예약된 보고서 추가**)**를 클릭합니다.

단계 **2** 보고서 유형을 선택합니다. 선택하는 보고서 유형에 따라 다른 옵션을 이용할 수 있습니다.

예약된 보고서의 사용 가능한 유형에 대한 자세한 내용은 예약된 보고서 유형, 831 페이지 섹션을 참조하십시오.

단계 **3** 알기 쉬운 보고서 제목을 입력합니다. AsyncOS는 보고서 이름의 고유성을 확인하지 않습니다. 혼동을 피하려면 동일한 이름의 여러 보고서를 만들지 마십시오.

단계 **4** 보고서 데이터의 시간 범위를 선택합니다. (Outbreak Filters 보고서에는 이 옵션을 사용할 수 없습니다.)

단계 **5** 보고서의 형식을 선택합니다.

- PDF. 전달용, 보관용 또는 둘 모두를 위한 형식이 지정된 PDF 문서를 만듭니다. Preview PDF Report(PDF 보고서 미리 보기)를 클릭하여 보고서를 PDF 파일로 즉시 볼 수 있습니다.

  영어 이외의 언어로 PDF를 생성하는 방법에 대한 자세한 내용은 보고서에 대한 참고 사항, 832 페이지 섹션을 참조하십시오.

- CSV. 표 형식의 데이터 및 쉼표로 구분된 값을 포함하는 ASCII 텍스트 파일을 만듭니다. 각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 한 보고서에 두 가지 이상의 테이블 유형이 포함되어 있으면 각 테이블에 대해 별도의 CSV 파일이 생성됩니다.

단계 **6** 사용 가능한 경우 보고서 옵션을 지정합니다. 일부 보고서에는 보고서 옵션이 없습니다.

단계 **7** 예약 및 전달 옵션을 지정합니다. 이메일 주소를 지정하지 않으면 보고서가 보관되기는 하지만 수신자에게 전송되지는 않습니다.

참고 외부 계정(예: Yahoo, Gmail 등)으로 보고서를 전송하는 경우, 보고서 이메일이 스팸으로 잘못 분류되지 않도록 하려면 외부 계정의 화이트리스트에 보고 반환 주소를 추가해야 할 수 있습니다.

단계 **8** **Submit(**제출**)**을 클릭합니다. 변경사항을 커밋합니다.

예약된 보고서 편집

단계 **1** Services(서비스) > Centralized Reporting(중앙 집중식 보고) 페이지의 목록에서 보고서 제목을 클릭합니다.

단계 **2** 변경 사항을 적용합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

예약된 보고서 삭제

단계 **1** Services(서비스) > Centralized Reporting(중앙 집중식 보고) 페이지에서 삭제할 보고서에 해당하는 확인란을 선택합니다.

참고 예약된 보고서를 모두 제거하려면 All(모두) 확인란을 선택합니다.

단계 **2** 삭제를 클릭합니다.

단계 **3** 삭제를 확인한 다음 변경 사항을 커밋합니다.

삭제된 보고서의 보관된 버전은 자동으로 삭제되지 않습니다.

Archived Reports(보관된 보고서)

Monitor(모니터) > Archived Reports(보관된 보고서) 페이지에는 사용 가능한 보관된 보고서가 나열됩니다. Report Title(보고서 제목) 열에서 이름을 클릭하여 보고서를 볼 수 있습니다. **Generate Report Now(**지금 보고서 생성**)**를 클릭하여 보고서를 즉시 생성할 수 있습니다.

Show(표시) 메뉴를 사용하여 나열할 보고서 유형을 필터링합니다. 열 머리글을 클릭하여 목록을 정렬합니다.

보관된 보고서는 자동으로 삭제됩니다. 각 예약된 보고서의 최대 30개 인스턴스가 보관되고, 새 보고서가 추가되면 1,000개를 유지하기 위해 오래된 보고서는 삭제됩니다. 30개 인스턴스 제한은 보고서 유형이 아니라 각각의 개별 예약된 보고서에 적용됩니다.

관련 주제

- 온디맨드 보고서 생성, 835 페이지

온디맨드 보고서 생성

예약하지 않고 보고서를 생성할 수 있습니다. 이러한 온디맨드 보고서는 여전히 지정된 기간을 기반으로 하지만 즉시 생성됩니다.

단계 **1** Archived Reports(보관된 보고서) 페이지에서 **Generate Report Now(**지금 보고서 생성**)**를 클릭합니다.

단계 **2** 보고서 유형을 선택하고 필요 시 제목을 수정합니다. AsyncOS는 보고서 이름의 고유성을 확인하지 않습니다. 혼동을 피하려면 동일한 이름의 여러 보고서를 만들지 마십시오.

예약된 보고서의 사용 가능한 유형에 대한 자세한 내용은 예약된 보고서 유형, 831 페이지 섹션을 참조하십시오.

단계 **3** 보고서 데이터의 시간 범위를 선택합니다. (Virus Outbreak 보고서에는 이 옵션을 사용할 수 없습니다.)

사용자 지정 범위를 만들면 그 범위가 링크로 나타납니다. 범위를 수정하려면 링크를 클릭합니다.

단계 **4** 보고서의 형식을 선택합니다.

- PDF. 전달용, 보관용 또는 둘 모두를 위한 형식이 지정된 PDF 문서를 만듭니다. Preview PDF Report(PDF 보고서 미리 보기)를 클릭하여 보고서를 PDF 파일로 즉시 볼 수 있습니다.

  영어 이외의 언어로 PDF를 생성하는 방법에 대한 자세한 내용은 보고서에 대한 참고 사항, 832 페이지 섹션을 참조하십시오.

- CSV. 표 형식의 데이터 및 쉼표로 구분된 값을 포함하는 ASCII 텍스트 파일을 만듭니다. 각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 한 보고서에 두 가지 이상의 테이블 유형이 포함되어 있으면 각 테이블에 대해 별도의 CSV 파일이 생성됩니다. 보고서 옵션을 지정합니다.

단계 **5** 보고서의 보관 여부를 선택합니다. 보고서를 보관하면 Archived Reports(보관된 보고서) 페이지에 나타납니다.

단계 **6** 보고서를 이메일로 전송할지 여부 및 어떤 이메일 주소로 전송할지를 지정합니다.

단계 **7** **Deliver this Report(**이 보고서 전송**)**를 클릭하여 보고서를 생성하고 수신자에게 전달하거나 보관합니다.

단계 **8** 변경사항을 커밋합니다.

이메일 보고서 문제 해결

- 메시지 추적 링크가 예기치 못한 결과로 이어짐 , 836 페이지
- 클라우드의 파일 분석 세부사항이 불완전함, 836 페이지

메시지 추적 링크가 예기치 못한 결과로 이어짐

문제

메시지 추적에서 세부사항을 보기 위해 보고서에서 드릴다운할 때 예기치 못한 결과가 발생합니다.

솔루션

보고 및 메시지 추적이 동시에 활성화되지 않은 경우, 제대로 작동하지 않는 경우, 그리고 데이터를 로컬에 저장하지 않은 경우(Security Management Appliance에서 중앙에 저장하는 것과 반대) 이 문제가 발생할 수 있습니다. 각 기능(보고 및 메시지 추적)에 대한 데이터는, 다른 기능(보고 또는 메시지 추적)이 활성화되고 작동하는지와 상관없이, 해당 기능이 활성화되고 어플라이언스에서 작동하는 동안에만 저장됩니다. 따라서 보고서에 메시지 추적에서 사용할 수 없는 데이터가 포함될 수 있으며 그 반대의 경우도 마찬가지입니다.

클라우드의 파일 분석 세부사항이 불완전함

문제

퍼블릭 클라우드의 완전한 파일 분석 결과는 조직의 다른 Email Security Appliance에서 업로드한 파일에 대해서는 사용할 수 없습니다.

솔루션

파일 분석 결과 데이터를 공유할 모든 어플라이언스를 그룹화해야 합니다. (퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성 , 475 페이지를 참조하십시오. 그룹의 각 어플라이언스에서 이 컨피그레이션을 수행해야 합니다.

32 장

메시지 추적

이 장에는 다음 섹션이 포함되어 있습니다.

메시지 추적 개요

메시지 추적은 메시지 플로우의 세부적인 보기를 제공하므로 헬프 데스크 문의 시 문제 해결에 도움이 됩니다. 예를 들어 메시지가 예상대로 전달되지 않은 경우 바이러스가 포함된 것인지, 스팸 격리에 보관된 것인지 또는 메일 스트림의 다른 곳에 있는 것인지 확인할 수 있습니다.

지정한 기준과 일치하는 특정 메일 메시지 또는 메시지 그룹을 검색할 수 있습니다.

참고 메시지 추적을 사용하여 메시지 내용을 읽을 수는 없습니다.

메시지 추적 활성화

참고 메시지 추적 데이터는 이 기능을 활성화한 후 처리되는 메시지에 대해서만 유지됩니다.

시작하기 전에

- 메시지 추적에서 첨부 파일 이름을 검색하고 표시하며 로그 파일에서 첨부 파일 이름을 보려면, 메시지 필터나 콘텐츠 필터와 같은 본문 검사 프로세스를 하나 이상 구성 및 활성화해야 합니다.

- 제목별 검색을 지원하려면 제목 헤더를 기록하도록 로그 파일을 구성해야 합니다. 자세한 내용은 로깅, 1053 페이지을 참고하십시오.
- 중앙 집중식 추적을 설정하는 경우: 이 Email Security Appliance에 대한 중앙 집중식 메시지 추적을 지원하도록 Security Management Appliance를 설정합니다. Cisco Content Security Management Appliance 사용 설명서를 참조하십시오.

단계 **1** **Services(**서비스**) > Centralized Services(**중앙 집중식 서비스**) > Message Tracking(**메시지 추적**)**을 클릭합니다.

이 서비스를 중앙 집중화하려는 경우가 아니더라도 이 경로를 사용합니다.

단계 **2** **Enable Message Tracking Service(**메시지 추적 서비스 활성화**)**를 선택합니다.

단계 **3** 시스템 설정 마법사를 실행한 후 처음 메시지 추적을 활성화하는 경우 최종 사용자 라이선스 계약을 읽고 **Accept(**동의**)**를 클릭합니다.

단계 **4** 메시지 추적 서비스를 선택합니다.

옵션	설명
로컬 추적	이 어플라이언스에서 메시지 추적을 사용합니다.
중앙 추적	Security Management Appliance를 사용하여 이 메시지를 포함한 여러 Email Security Appliance에 대한 메시지를 추적합니다.

단계 **5** (선택 사항) 거부된 연결에 대한 정보를 저장하기 위한 확인란을 선택합니다.

성능을 최적화하려면 이 설정을 선택하지 마십시오.

단계 **6** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

Local Tracking(로컬 추적)을 선택한 경우

- DLP 위반과 관련된 내용에 액세스할 수 있는 사용자를 선택합니다. 메시지 추적 시 중요 정보의 액세스 제어, 898 페이지를 참조하십시오.
- (선택 사항) 메시지 저장을 위한 디스크 공간 할당을 조정합니다. 디스크 공간 관리 , 941 페이지를 참조하십시오.

메시지 검색

단계 **1** **Email(**이메일**) > Message Tracking(**메시지 추적**) > Message Tracking(**메시지 추적**)**을 선택합니다.

단계 **2** 검색 기준을 입력합니다.

- 모든 옵션을 보려면 **Advanced(**고급**)** 링크를 클릭합니다.
- 추적에서는 와일드카드 문자나 정규식이 지원되지 않습니다.
- 추적 검색은 대/소문자를 구분하지 않습니다.
- 달리 지정되어 있지 않으면 쿼리는 "AND" 검색입니다. 즉, 검색 필드에 지정된 모든 조건과 일치하는 메시지가 반환됩니다. 예를 들어, 봉투 수신자 및 제목 줄 매개변수에 대한 텍스트 문자열을 지정하는 경우 지정된 봉투 수신자 및*(and)* 제목 줄과 모두 일치하는 메시지만 반환됩니다.
- 검색 기준은 다음과 같습니다.

옵션	설명
Envelope Sender(봉투 발신자**)**	**Begins With**, **Is** 또는 **Contains**를 선택한 다음 검색할 이메일 주소, 사용자 이름 또는 메시지 발신자의 도메인을 입력합니다. 임의의 문자를 입력할 수 있습니다. 입력에 대한 검증이 수행되지 않습니다.
Envelope Recipient(봉투 수신자**)**	**Begins With**, **Is** 또는 **Contains**를 선택한 다음 검색할 이메일 주소, 사용자 이름 또는 메시지 수신자의 도메인을 입력합니다. 임의의 문자를 입력할 수 있습니다. 입력에 대한 검증이 수행되지 않습니다.
제목	**Begins With**, **Is** 또는 **Contains**를 선택한 다음 메시지 제목 줄에서 검색할 텍스트 문자열을 입력합니다. 경고: 그러한 추적을 금지하는 규정이 있는 환경에서는 이 검색 유형을 사용하지 마십시오.
Message Received(수신된 메시지**)**	날짜 및 시간 범위를 지정합니다. 날짜를 지정하지 않으면 모든 날짜의 데이터가 반환됩니다. 시간 범위만 지정하는 경우 사용 가능한 모든 날짜에서 해당 시간 범위의 데이터가 반환됩니다. Email Security Appliance에서 메시지를 수신한 로컬 날짜와 시간을 사용하십시오.
고급 옵션**:**	
Sender IP Address/Domain/Network Owner(발신자 **IP** 주소/도메인/네트워크 소유자**)**	원격 호스트의 IP 주소, 도메인 또는 네트워크 소유자를 지정합니다. 거부된 연결 내에서만 검색할 수도 있고 모든 메시지를 검색할 수도 있습니다.

옵션	설명
첨부 파일	**Begins With**, **Is** 또는 **Contains**를 선택한 다음 찾으려는 하나의 첨부 파일에 대한 ASCII 또는 유니코드 텍스트 문자열을 입력합니다. 입력한 텍스트에서 전후 공백이 제거되지 않습니다. 다음을 수행한 경우에만 첨부 파일의 파일 이름으로 메시지를 검색할 수 있습니다. • 메시지 필터를 사용하여 본문 검사 • 콘텐츠 필터를 사용하여 본문 검사 • AMP(Advanced Malware Protection) 검사 SHA-256 해시를 기반으로 파일을 식별하는 방법에 대한 자세한 내용은 SHA-256 해시로 파일 식별 , 484 페이지 섹션을 참조하십시오. 위협 이름을 기준으로 Advanced Malware Protection 엔진에서 악의적인 것으로 탐지된 메시지를 검색할 수 있습니다. **Threat Name(위협 이름)** 필드에 *Simple_Custom_ Detection* 또는 *Custom_Threshold*를 입력하여 Custom Detection(맞춤형 탐지) 및 Custom Threshold(맞춤형 임계값) 카테고리로 탐지된 메시지를 검색합니다. 특정 파일이 Advanced Malware Protection 엔진에서 바이러스 양성으로 탐지된 경우 바이러스 이름으로 메시지를 검색할 수도 있습니다.
메시지 이벤트	하나 이상의 메시지 처리 이벤트를 선택합니다. 예를 들면 전달되거나 격리되거나 하드 반송된 메시지를 검색할 수 있습니다. 메시지 이벤트는 "OR" 연산자로 추가됩니다. 여러 이벤트를 선택하면 지정한 조건 중 하나와 일치하는 메시지가 검색됩니다.
메시지 **ID** 헤더	SMTP 메시지 ID 헤더에 대한 텍스트 문자열을 입력합니다. 이 RFC 822 메시지 헤더는 각 이메일 메시지를 고유하게 식별하며, 메시지를 처음 만들 때 메시지에 삽입됩니다.
Cisco IronPort MID	검색할 메시지 번호를 입력합니다. IronPort MID는 Email Security Appliance에서 각 이메일 메시지를 고유하게 식별합니다.
Cisco IronPort Host(Cisco IronPort 호스트)	Email Security Appliance를 선택하여 해당 어플라이언스로 처리된 메시지를 검색하도록 제한하거나, 모든 어플라이언스를 선택합니다.

단계 **3** 쿼리를 제출하려면 **Search(검색)**를 클릭합니다.

쿼리 결과가 페이지 하단에 표시됩니다.

다음에 수행할 작업

관련 주제

- 메시지 추적 검색 결과 작업 , 841 페이지

메시지 추적 검색 결과 작업

다음에 유의해야 합니다.

- Email Security Appliance에 기록되고 Security Management Appliance에 의해 검색된 후에야 비로소 메시지가 결과에 나타납니다. 로그의 크기 및 폴링 빈도에 따라 이메일 메시지가 전송된 시간과 추적 및 보고 결과에 실제로 나타나는 시간 사이에 약간의 차이가 생길 수 있습니다.
- Advanced Malware Protection(파일 평판 검사 및 파일 분석) 관련 검색에 대한 자세한 내용은 Message(메시지) 추적 및 Advanced Malware Protection 기능 정보 , 486 페이지 섹션을 참조하십시오.

검색 결과로 작업할 때 다음을 수행할 수 있습니다.

- 검색 기준으로 돌아가서 Advanced(고급)를 클릭하고, Query Settings(쿼리 설정)로 스크롤하여 최대 결과 수를 1000으로 설정하면 250개보다 많은 검색 결과를 표시할 수 있습니다.
- 검색 결과 섹션의 오른쪽 상단에서 옵션을 선택하여 페이지당 더 많은 결과를 표시할 수 있습니다.
- 검색 결과 섹션의 오른쪽 상단에서 검색 결과의 여러 페이지를 탐색할 수 있습니다.
- 조건으로 추가할 검색 결과의 값 위로 커서를 이동하여 검색 결과를 좁힐 수 있습니다. 주황색 하이라이트가 나타나면 값을 클릭하여 해당 기준으로 검색을 좁힐 수 있습니다. 이렇게 하면 검색 기준에 새 기준에 추가됩니다. 예를 들어 특정 수신자에게 전송되는 메시지를 검색하려면, 원래 지정된 시간 범위(및 다른 기준 충족) 내에서 해당 발신자로부터 해당 수신자에게 가는 모든 메시지를 찾도록 검색 결과에서 발신자 이름을 클릭할 수 있습니다.
- 검색 기준과 일치하는 메시지가 1,000개가 넘으면 Export All(모두 내보내기)(검색 결과 섹션의 오른쪽 상단에 있는 링크)을 클릭하고 최대 50,000개의 검색 결과를 쉼표로 구분된 값의 파일로 내보낸 다음 다른 애플리케이션에서 데이터로 작업할 수 있습니다.
- 해당 메시지의 행에 있는 Show Details(세부사항 표시)를 클릭하여 메시지에 대한 세부사항을 볼 수 있습니다. 메시지 세부사항과 함께 새 브라우저 창이 열립니다.
- 격리된 메시지의 경우 메시지 추적 검색 결과의 링크를 클릭하여, 메시지가 격리된 이유와 같은 세부사항을 볼 수 있습니다.

참고 Message Tracking(메시지 추적)에서 메시지 세부 정보를 보기 위해 보고서 페이지의 링크를 클릭했는데 예상했던 것과 다른 결과 집합이 표시되는 경우, 검토 기간 중에 보고와 추적이 동시에 계속해서 활성화되지 않았기 때문일 수 있습니다.

관련 주제

- 메시지 추적 세부 정보 , 842 페이지

메시지 추적 세부 정보

항목	설명
Envelope and Header Summary(봉투 및 헤더 요약) 섹션	
Received Time(수신 시간)	Email Security Appliance가 메시지를 수신한 시간. Email Security Appliance에 구성된 로컬 시간을 사용하여 날짜 및 시간이 표시됩니다.
MID	고유한 IronPort 메시지 ID.
메시지 크기	메시지 크기.
제목	메시지의 제목 줄. 메시지에 제목이 없는 경우 또는 로그 파일이 제목 헤더를 기록하도록 구성되지 않은 경우 추적 결과의 제목 줄에 "(No Subject)" 값이 표시될 수 있습니다. 자세한 내용은 로깅, 1053 페이지 을 참조해 주십시오.
Envelope Sender(봉투 발신자)	SMTP 봉투에 있는 발신자의 주소.
Envelope Recipients(봉투 수신자)	구축에서 별칭 확장용 별칭 테이블을 사용하는 경우 원래 봉투 주소보다는 확장된 수신자 주소가 검색됩니다. 별칭 테이블에 대한 자세한 내용은 "라우팅 및 전달 기능 구성" 장에서 "별칭 테이블 만들기"를 참조해 주십시오. 다른 모든 경우에는 메시지 추적 조회에서 원래 봉투 수신자 주소가 검색됩니다.
메시지 **ID** 헤더	RFC 822 메시지 헤더.
SMTP 인증 사용자 **ID**	발신자가 SMTP 인증을 사용하여 메시지를 전송한 경우 발신자의 SMTP 인증 사용자 이름. 그렇지 않으면 값은 N/A"입니다.

항목	설명
첨부 파일	메시지에 첨부된 파일의 이름. 쿼리된 첨부 파일이 하나 이상 포함된 메시지가 검색 결과에 나타납니다. 일부 첨부 파일은 추적되지 않을 수 있습니다. 성능상의 이유로, 첨부 파일 이름 검사는 메시지 또는 콘텐츠 필터링, DLP, 면책조항 스탬프 등 다른 검사 운영의 일부로서만 발생합니다. 본문 검사를 통과하고 첨부 파일이 여전히 첨부되어 있는 메시지에 대해서만 첨부 파일 이름을 사용할 수 있습니다. 첨부 파일 이름이 검색 결과에 나타나지 않는 상황은 다음과 같습니다(이에 제한되지 않음). • 시스템에서 콘텐츠 필터만 사용하고, 안티스팸 또는 안티바이러스 필터에 의해 메시지가 삭제되거나 첨부 파일이 제거된 경우 • 메시지 분리 정책에 따라 본문 검사가 발생하기 전에 일부 메시지에서 첨부 파일이 제거된 경우 성능상의 이유로 첨부 파일 내의 파일 이름(OLE 개체 또는 .ZIP 파일과 같은 아카이브)은 검색되지 않습니다.
Sending Host Summary(발신자 호스트 요약) 섹션	
역방향 **DNS** 호스트 이름	역방향 DNS(PTR) 조회로 확인된 전송 호스트의 이름.
IP 주소	전송 호스트의 IP 주소.
SBRS 점수	SenderBase Reputation 점수. 범위는 10(신뢰할 수 있는 발신자) ~ -10(명백한 스패머)입니다. 점수는 메시지가 처리된 시점에 이 호스트에 대한 정보가 없음을 나타냅니다. SBRS에 대한 자세한 내용은 발신자 평판 필터링 , 85 페이지를 참조하십시오.
Processing Details(세부사항 처리) 섹션	
Summary(요약**)** 정보 (아래 탭 중 하나가 표시되는 경우 이 정보는 탭에 표시됩니다. Summary(요약) 정보는 항상 표시됩니다.)	Summary(요약) 탭에는 메시지 처리 중에 로깅된 상태 이벤트가 표시됩니다. 항목에는 메일 정책 처리에 대한 정보(예: 안티 스팸 및 안티바이러스 검사)와 기타 이벤트(예: 콘텐츠 또는 메시지 필터에 의해 추가된 메시지 분리 및 맞춤화 로그 항목)가 포함됩니다. 메시지가 전달된 경우 전달 세부사항이 여기에 표시됩니다. 마지막에 기록된 이벤트가 처리 세부사항에 강조 표시됩니다.

항목	설명
DLP Matched Content(DLP 일치 콘텐츠**)** 탭	DLP 정책으로 식별된 메시지에 대해서만 이 탭이 표시됩니다. 이 탭에는 DLP 정책 일치를 트리거한 민감한 콘텐츠 및 일치에 대한 정보가 포함됩니다. 이 정보를 표시하도록 어플라이언스를 구성해야 합니다. 메시지 추적에서 민감한 DLP 데이터 표시 , 517 페이지를 참고하십시오. 이 탭에 대한 액세스를 제어하려면 메시지 추적 시 중요 정보의 액세스 제어, 898 페이지 섹션을 참조하십시오.
URL Details(URL 세부 정보**)** 탭	이 탭은 URL 평판 및 URL 카테고리 콘텐츠 필터에 걸린 메시지에 대해, 그리고 보안 침해 필터에 걸린 메시지에 대해서만 표시됩니다. 이 탭에는 다음 정보가 표시됩니다. • 평판 점수 또는 URL과 관련된 카테고리 • URL에서 수행한 작업(재작성, 무해화 또는 리디렉션) • 메시지에 여러 URL이 포함된 경우 필터 작업을 트리거하는 URL 이 정보를 표시하도록 어플라이언스를 구성해야 합니다. 메시지 추적에서 URL 세부 정보 표시 , 441 페이지를 참고하십시오. 이 탭에 대한 액세스를 제어하려면 메시지 추적 시 중요 정보의 액세스 제어, 898 페이지 섹션을 참조하십시오.

관련 주제

- 메시지 검색 , 838 페이지

메시지 추적 데이터 가용성 확인

메시지 추적 데이터에 포함되는 날짜 범위를 결정하고, 해당 데이터에서 누락된 간격을 식별할 수 있습니다.

단계 **1** **Monitor(**모니터**) > Message Tracking(**메시지 추적**)**을 선택합니다.

단계 **2** Search(검색) 상자의 오른쪽 상단에서 **Data in time range(**시간 범위의 데이터**):**를 찾아봅니다.

단계 **3** **Data in time range(**시간 범위의 데이터**):**에 대해 표시되는 값을 클릭합니다.

다음에 수행할 작업

관련 주제

• 메시지 추적 및 업데이트 정보 , 845 페이지

메시지 추적 및 업데이트 정보

새로운 메시지 추적 기능은 업그레이드 전에 처리된 메시지에는 적용되지 않을 수 있습니다. 필수 데이터가 그러한 메시지에 포함되어 있지 않기 때문일 수 있습니다. 메시지 추적 데이터 및 업그레이드와 관련되어 나타날 수 있는 제한 사항은 해당 릴리스의 릴리스 정보를 참조해 주십시오.

메시지 추적 트러블슈팅

관련 주제

• 첨부 파일이 검색 결과에 나타나지 않음 , 845 페이지
• 검색 결과에 예상 메시지가 누락됨 , 845 페이지

첨부 파일이 검색 결과에 나타나지 않음

문제

첨부 파일 이름이 검색 결과에 나타나지 않으며 찾을 수 없습니다.

솔루션

구성 요구 사항은 메시지 추적 활성화, 837 페이지 을 참고하십시오. 메시지 추적 세부 정보 , 842 페이지에 나와 있는 첨부 파일 이름 검색의 제한 사항도 참조해 주십시오.

검색 결과에 예상 메시지가 누락됨

문제

기준을 충족했을 메시지가 검색 결과에 포함되지 않았습니다.

솔루션

- 많은 검색, 특히 메시지 이벤트와 관련된 검색의 결과는 어플라이언스 컨피그레이션에 따라 달라집니다. 예를 들어 필터링하지 않은 URL 범주를 검색하는 경우, 해당 범주에 URL이 메시지에 포함되었더라도 결과에 아무것도 표시되지 않습니다. 예상한 동작이 수행되도록 Email Security Appliance를 적절히 구성했는지 확인하십시오. 예를 들면 메일 정책, 콘텐츠 및 메시지 필터, 격리 설정을 점검해 주십시오.
- 보고서의 링크를 클릭한 후 예상 정보가 누락된 경우 이메일 보고서 문제 해결, 835 페이지 섹션을 참조해 주십시오.

33 장

정책, 바이러스, 보안 침해 격리

이 장에는 다음 섹션이 포함되어 있습니다.

정책, 바이러스 및 **Outbreak** 격리 개요

"정책, 바이러스 및 전파 확산 격리"에는 File Analysis(파일 분석) 격리를 비롯한 모든 비 스팸 격리가 포함됩니다.

수신 또는 발신 메시지에서 조직이 허용하지 않는 내용이나 잠재적인 악성코드가 탐지되는 경우 Email Security Appliance에서는 이러한 메시지를 즉시 삭제하는 대신 격리로 전송합니다. 격리는 그러한 메시지를 Email Security Appliance 또는 Cisco Content Security Management Appliance에 일정 기간 보관하여 사람이 검토할 수 있도록 하거나, 메시지의 안전 여부를 더 잘 평가할 수 있는 업데이트를 기다립니다.

조직에서 비 스팸 격리를 사용할 수 있는 방법의 예는 다음과 같습니다.

- 정책 시행. 인사 담당자나 법무 부서에서 모욕적인 정보, 기밀 정보 또는 기타 허용되지 않는 정보가 포함되어 있을 수 있는 메시지를 검토하도록 합니다.
- 바이러스 격리. 사용자에게 바이러스가 퍼지는 것을 막기 위해 감염되었거나 암호화되었거나 안티바이러스 검사 엔진에서 검사할 수 없는 메시지를 저장합니다.
- **Outbreak** 방지. 바이러스 발생 또는 소규모 악성코드 공격 가능성이 있는 것으로 Outbreak Filter 플래그가 지정된 메시지를 안티바이러스 또는 안티스팸 업데이트가 릴리스될 때까지 보관합니다.
- **File Analysis(**파일 분석**)** 격리. 판정이 도달할 때까지, 악성코드가 포함되었을 수 있는 어태치 파일 또는 분석을 위해 전송된 어태치 파일이 있는 메시지를 저장합니다.

관련 항목

- 스팸 격리, 867 페이지

격리 유형

격리 유형	격리 이름	시스템에서 기본적으로 생성되는지 여부	설명	추가 정보
AMP(Advanced Malware Protection)	파일 분석	예	판정이 돌아올 때까지 파일 분석을 위해 전송된 메시지를 보관합니다.	• 정책, 바이러스 및 Outbreak 격리 관리 • 정책, 바이러스 또는 보안 침해 격리의 메시지 작업
바이러스	바이러스	예	안티바이러스 엔진의 결정에 따라, 악성코드를 전송할 가능성이 있는 메시지를 보관합니다.	
Outbreak	Outbreak	예	Outbreak Filter에서 잠재적으로 스팸 또는 악성코드로서 포착된 메시지를 보관합니다.	
정책	Policy	예	메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업으로 포착된 메시지를 보관합니다. 기본 Policy(정책) 격리가 자동으로 생성됩니다.	
	분류되지 않음	예	메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업에 지정된 격리가 삭제된 경우에만 메시지를 보관합니다. 이 격리를 다른 필터나 메시지 작업에 할당할 수 없습니다.	
	(자신이 만든 정책 격리)	아니요		

격리 유형	격리 이름	시스템에서 기본적으로 생성되는지 여부	설명	추가 정보
			메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업에 사용하기 위해 자신이 만든 Policy(정책) 격리.	
스팸	스팸	예	메시지 수신자 또는 관리자 검토를 위해 스팸이나 스팸으로 의심되는 메시지를 보관합니다. 스팸 격리는 정책, 바이러스 및 전파 확산 격리의 그룹에 포함되지 않으며 다른 모든 격리와 별도로 관리됩니다.	스팸 격리, 867 페이지

정책, 바이러스 및 Outbreak 격리 관리

정책, 바이러스 및 Outbreak 격리를 위한 디스크 공간 할당

정책, 바이러스 및 보안 침해 격리를 위한 디스크 공간 정보는 디스크 공간 관리 , 941 페이지 섹션을 참조해 주십시오.

격리가 중앙 집중화된 경우에도 정책, 바이러스 및 보안 침해 격리는 Email Security Appliance에서 일부 디스크 공간을 사용합니다.

여러 격리의 메시지는 단일 격리의 메시지와 동일한 디스크 공간을 사용합니다.

Outbreak Filter 및 Centralized Quarantines(중앙 집중식 격리)가 모두 활성화된 경우

- 보안 침해 규칙이 업데이트될 때마다 해당 메시지를 검사하기 위해, 로컬 정책, 바이러스 및 보안 침해 격리에 할당되었을 Email Security Appliance의 모든 디스크 공간이 보안 침해 격리에 메시지 복사본을 유지하는 데 대신 사용됩니다.
- 특정 관리되는

관련 주제

- 격리 상태, 용량 및 활동 모니터링 , 855 페이지
- 격리 디스크 공간 사용량에 대한 알림 , 856 페이지
- 격리에서 메시지의 보유 시간 , 850 페이지

격리에서 메시지의 보유 시간

다음 상황에서는 메시지가 격리에서 자동으로 제거됩니다.

- 정상 만료 - 구성된 보유 시간이 격리에 있는 메시지에 대해 충족됩니다. 각 격리의 메시지에 대해 보유 시간을 지정합니다. 각 메시지에는 고유한 특정 만료 시간이 있으며, 이는 격리 리스트에 표시됩니다. 이 항목에 설명된 또 다른 상황이 발생하지 않는 한 메시지는 지정된 기간 동안 저장됩니다.

  참고 Outbreak Filter 격리에 있는 메시지의 정상 보유 시간은 전파 확산 격리가 아니라 각 메일 정책의 Outbreak Filter 섹션에서 구성합니다.

- 조기 만료 - 구성된 보유 시간에 도달하기 전에 격리에서 메시지에 적용됩니다. 다음과 같은 경우 발생할 수 있습니다.
  - 정책, 바이러스 및 Outbreak 격리를 위한 디스크 공간 할당 , 850 페이지에 정의된 대로 모든 격리에 대한 크기 제한에 도달합니다.

    크기 제한에 도달하면 격리와 상관없이 가장 오래된 메시지부터 처리되고, 모든 격리의 크기가 다시 크기 제한보다 작아질 때까지 각 메시지에 대해 기본 작업이 수행됩니다. FIFO(First In First Out) 정책이 적용됩니다. 여러 격리의 메시지는 최신 만료 시간을 기반으로 만료됩니다.

(선택 사항) 디스크 공간 부족으로 인한 릴리스 또는 삭제가 면제되도록 개별 격리를 구성할 수 있습니다. 면제되도록 모든 격리를 구성한 상태에서 디스크 공간 용량에 도달하면 새 메시지를 위한 공간을 마련하기 위해 격리의 메시지가 전달됩니다.

디스크 공간 주요 시점에 알림을 받게 됩니다. 격리 디스크 공간 사용량에 대한 알림 , 856 페이지를 참조하십시오.

- 메시지를 여전히 보유하고 있는 격리를 삭제합니다.

격리에서 메시지가 자동으로 제거되면 해당 메시지에 대한 기본 작업이 수행됩니다. 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 851 페이지를 참조하십시오.

참고 위 시나리오 외에도 검사 작업(신종 바이러스 필터(Outbreak Filter) 또는 파일 분석)의 결과에 따라 메시지가 격리에서 자동으로 제거될 수 있습니다.

보유 시간에 대한 시간 조정의 효과

- 일광 절약 시간 및 어플라이언스 표준 시간대 변경은 보유 기간에 영향을 미치지 않습니다.
- 격리의 보유 시간을 변경하면 새 메시지만 새 만료 시간의 적용을 받습니다.
- 시스템 시계가 변경되는 경우, 과거에 만료되었을 메시지는 가장 적절한 다음 시간에 만료됩니다.
- 만료가 진행 중인 메시지에는 시스템 시계 변경이 적용되지 않습니다.

자동으로 처리되는 격리 메시지에 대한 기본 작업

격리에서 메시지의 보유 시간 , 850 페이지에 설명된 상황이 발생하면 정책, 바이러스 또는 전파 확산 격리의 메시지에 대해 기본 작업이 수행됩니다.

두 가지 주요 기본 작업이 있습니다.

- 삭제 - 메시지가 삭제됩니다.
- 릴리스 - 전달을 위해 메시지가 릴리스됩니다.

릴리스되면 메시지에서 위협을 다시 검사할 수 있습니다. 자세한 내용은 격리된 메시지 재검사 정보 , 863 페이지를 참고해 주십시오.

또한 예상 보유 기간이 지나기 전에 릴리스된 메시지에 대해서는 X-Header 추가와 같은 별도의 작업이 수행될 수 있습니다. 자세한 내용은 정책, 바이러스, Outbreak 격리 구성 , 852 페이지를 참고해 주십시오.

시스템 생성 격리의 설정 확인

격리를 사용하기 전에 Unclassified(미분류) 격리를 포함한 기본 격리의 설정을 맞춤화하십시오.

관련 주제

- 정책, 바이러스, Outbreak 격리 구성 , 852 페이지

정책, 바이러스, Outbreak 격리 구성

시작하기 전에

- 기존 격리를 수정하는 경우 정책, 바이러스 및 Outbreak 격리 설정의 수정에 대한 정보 , 854 페이지 섹션을 참조해 주십시오.
- 보유 시간과 기본 작업을 포함하여 격리의 메시지가 자동으로 관리되는 방법을 이해합니다. 격리에서 메시지의 보유 시간 , 850 페이지 및 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 851 페이지 섹션을 참조해 주십시오.
- 각 격리에 액세스할 수 있도록 할 사용자를 결정하고, 그에 따라 사용자 및 맞춤형 사용자 역할을 만듭니다. 자세한 내용은 정책, 바이러스 및 보안 침해 격리에 액세스할 수 있는 사용자 그룹 , 857 페이지 섹션을 참조해 주십시오.

단계 **1** **Monitor(**모니터링**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 신종 바이러스 격리**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Policy Quarantine(**정책 격리 추가**)**을 클릭합니다.
- 수정할 격리를 클릭합니다.

단계 **3** 정보를 입력합니다.

다음에 유의해야 합니다.

- 파일 분석 격리의 보존 기간을 기본값인 1시간에서 변경하는 것은 권장되지 않습니다.
- 격리 디스크 공간이 꽉 차더라도 지정한 Retention Period(보유 기간)가 끝나기 전에 이 격리의 메시지가 처리되지 않도록 하려면 **Free up space by applying default action on messages upon space overflow(**공간 오버플로 시 메시지에 기본 작업을 적용하여 공간 비우기**)**의 선택을 취소합니다.

  이 옵션을 모든 격리에 대해 선택하지 마십시오. 시스템이 하나 이상의 격리에서 메시지를 삭제하여 공간을 마련할 수 있어야 합니다.
- 기본 작업으로 **Release(**릴리스**)**를 선택하는 경우 보유 기간이 지나기 전에 릴리스되는 메시지에 적용할 추가 작업을 지정할 수 있습니다.

옵션	정보
제목 수정	추가할 텍스트를 입력하고 이를 원래 메시지 제목의 앞에 추가할지 뒤에 추가할지를 지정합니다. 예를 들면 수신자에게 메시지에 부적절한 내용이 포함되어 있을 수 있다고 경고할 수 있습니다. 참고 제목에 비 ASCII 문자를 올바르게 표시하려면 RFC 2047에 따라 표현해야 합니다.
X-Header 추가	X-Header는 메시지에 대해 수행된 작업의 기록을 제공할 수 있습니다. 이는 예를 들어 특정 메시지가 전달된 이유에 대한 문의를 처리할 때 도움이 될 수 있습니다. 이름과 값을 입력합니다. 예: 이름 = Inappropriate-release-early Value = True
첨부 파일 제거	어태치된 파일 제거는 해당 파일에 있을 수 있는 바이러스로부터 보호합니다.

단계 **4** 격리에 액세스할 수 있는 사용자를 지정합니다.

사용자	정보
로컬 사용자	로컬 사용자 목록에는 격리에 액세스할 수 있는 역할의 사용자만 포함됩니다. 모든 관리자는 격리에 대한 완전한 액세스 권한을 가지고 있으므로 리스트에는 관리자 권한의 사용자가 제외됩니다.
외부에서 인증된 사용자	외부 인증을 구성한 상태여야 합니다.
맞춤형 사용자 역할	격리 액세스 권한이 있는 맞춤형 사용자 역할을 하나 이상 만든 경우에만 이 옵션이 표시됩니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

메시지 및 콘텐츠 필터, 그리고 메시지를 격리로 이동할 DLP 메시지 작업을 만듭니다. 참조

정책, 바이러스 및 **Outbreak** 격리 설정의 수정에 대한 정보

참고
- 격리의 이름은 변경할 수 없습니다.
- 격리에서 메시지의 보유 시간 , 850 페이지도 참조해 주십시오.

격리 설정을 변경하려면 에서 Monitor(모니터) > Policy, Virus, and Outbreak Quarantines를 선택하고 격리의 이름을 클릭합니다.

정책 격리를 할당할 필터 및 메시지 작업 결정

정책 격리와 관련된 메시지 필터, 콘텐츠 필터, DLP(Data Loss Prevention) 메시지 작업 및 DMARC 확인 프로필, 그리고.

단계 **1** **Monitor(모니터) > Policy, Virus, and Outbreak Quarantines**를 선택합니다.

단계 **2** 확인할 정책 격리의 이름을 클릭합니다.

단계 **3** 페이지 하단으로 스크롤하여 **Associated Message Filters/Content Filters/DLP Message Actions(**관련 메시지 필터/콘텐츠 필터**/DLP** 메시지 작업**)**를 봅니다.

정책 격리 삭제 정보

- 정책 격리를 삭제하기 전에 활성 필터 또는 메시지 작업과 연결되어 있는지 확인해 주십시오. 정책 격리를 할당할 필터 및 메시지 작업 결정 , 854 페이지를 참조하십시오.
- 필터 또는 메시지 작업에 할당되었더라도 정책 격리를 삭제할 수 있습니다.
- 디스크가 꽉 찼을 때 메시지를 삭제하지 않도록 하는 옵션을 선택했더라도, 비어 있지 않은 격리를 삭제하면 격리에 정의된 기본 작업이 모든 메시지에 적용됩니다. 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 851 페이지를 참조하십시오.
- 필터 또는 메시지 작업과 연결된 격리를 삭제한 이후에 해당 필터나 메시지 작업으로 격리된 메시지는 Unclassified(미분류) 격리로 전송됩니다. 격리를 삭제하기 전에 Unclassified(미분류) 격리의 기본 설정을 맞춤화해야 합니다.
- Unclassified(미분류) 격리는 삭제할 수 없습니다.

격리 상태, 용량 및 활동 모니터링

보려는 내용	수행해야 할 작업
모든 비 스팸 격리에 할당된 총 공간	**Monitor(모니터) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 보안 침해 격리)**를 선택하고 페이지의 첫 번째 섹션을 살펴봅니다. 할당을 변경하려면 디스크 공간 관리 , 941 페이지 섹션을 참조해 주십시오.
모든 비 스팸 격리에 대해 현재 사용 가능한 공간	**Monitor(모니터) > Policy, Virus, and Outbreak Quarantines**)를 선택하고 테이블 바로 아래를 살펴봅니다.
현재 모든 격리에서 사용되고 있는 총 공간	**Monitor(모니터) > System Status(시스템 상태)**를 선택하고 **Queue Space Used by Quarantine(격리에 사용된 대기열 공간)**을 살펴봅니다.
각 격리에 현재 사용된 공간	**Monitor(모니터) > Policy, Virus, and Outbreak Quarantines**를 선택하고, 격리 이름을 클릭하고, 격리 이름 바로 아래에 있는 테이블 행에서 이 정보를 살펴봅니다.
현재 모든 격리에 있는 총 메시지 수	**Monitor(모니터) > System Status(시스템 상태)**를 선택하고 **Active Messages in Quarantine(격리의 활성 메시지)**을 살펴봅니다.
현재 각 격리에 있는 메시지 수	**Monitor(모니터) > Policy, Virus, and Outbreak Quarantines**를 선택하고 격리에 대한 테이블 행을 살펴봅니다.
모든 격리의 총 CPU 사용량	**Monitor(모니터) > System Status(시스템 상태)**를 선택하고 **CPU Utilization(CPU 사용률)** 섹션을 살펴봅니다.
마지막 메시지가 각 격리에 들어간 날짜와 시간(정책 격리 간 이동 제외)	**Monitor(모니터) > Policy, Virus, and Outbreak Quarantines**를 선택하고 격리에 대한 테이블 행을 살펴봅니다.
정책 격리를 만든 날짜 정책 격리 만든 사람의 이름	**Monitor(모니터) > Policy, Virus, and Outbreak Quarantines**를 선택하고, 격리 이름을 클릭하고, 격리 이름 바로 아래에 있는 테이블 행에서 이 정보를 살펴봅니다. 시스템 생성 격리에 대해서는 만든 날짜와 만든 사람 이름을 사용할 수 없습니다.
정책 격리와 연결된 필터 및 메시지 작업	정책 격리를 할당할 필터 및 메시지 작업 결정 , 854 페이지를 참조하십시오.

정책 격리 성능

정책 격리에 저장된 메시지는 하드 드라이브 공간 외에 시스템 메모리도 사용합니다. 단일 어플라이언스의 정책 격리에 수십만 개의 메시지를 저장하면 과도한 메모리 사용 때문에 어플라이언스의 성능이 저하될 수 있습니다. 어플라이언스에서 메시지를 격리, 삭제 및 릴리스하는 데 시간이 더 걸리며, 이에 따라 메시지 처리 및 이메일 파이프라인 백업 속도가 느려집니다.

Email Security Appliance에서 이메일을 정상적인 속도로 처리하도록 하려면 정책 격리에 평균 20,000개 미만의 메시지를 보관하는 것이 좋습니다.

격리에 있는 메시지의 수를 확인하려면 격리 상태, 용량 및 활동 모니터링 , 855 페이지 섹션을 참조해 주십시오.

격리 디스크 공간 사용량에 대한 알림

정책, 바이러스, 보안 침해 격리의 총 크기가 용량의 75%, 85%, 95%에 도달하거나 이를 초과할 때마다 알림이 전송됩니다. 메시지가 격리에 놓일 때 확인이 수행됩니다. 예를 들어, 격리에 메시지를 추가하여 크기가 총 용량의 75%로 증가하거나 이를 초과하면 알림이 전송됩니다.

알림에 대한 자세한 내용은 알림, 962 페이지 섹션을 참조하십시오.

정책 격리 및 로깅

AsyncOS는 격리된 모든 메시지를 개별적으로 로깅합니다.

Info: MID 482 quarantined to "Policy" (message filter:policy_violation)

메시지를 격리시킨 메시지 필터 및 Outbreak Filter 기능은 괄호로 표시됩니다. 메시지가 있는 각 격리에 대해 별도의 로그 항목이 생성됩니다.

AsyncOS는 또한 격리에서 제거된 메시지를 개별적으로 로깅합니다.

Info: MID 483 released from quarantine "Policy" (queue full)

Info: MID 484 deleted from quarantine "Anti-Virus" (expired)

시스템은 모든 격리에서 제거되고 영구 삭제되거나 전달이 예약된 메시지를 개별적으로 로깅합니다. 예를 들면 다음과 같습니다.

Info: MID 483 released from all quarantines

Info: MID 484 deleted from all quarantines

메시지가 다시 주입되면 시스템은 새 MID(Message ID)로 새로운 Message 개체를 만듭니다. 이는 기존 로그 메시지를 사용하여 새 MID "byline"으로 로깅됩니다. 예를 들면 다음과 같습니다.

Info: MID 483 rewritten to 513 by Policy Quarantine

메시지 처리 작업을 다른 사용자들에게 분산

메시지 검토 및 처리 작업을 다른 관리 사용자들에게 분산할 수 있습니다. 예를 들면 다음과 같습니다.

- 인사 팀에서는 Policy Quarantine(정책 격리)을 검토 및 관리할 수 있습니다.
- 법무 팀에서는 Confidential Material Quarantine(기밀 자료 격리)을 관리할 수 있습니다.

격리에 대한 설정을 지정할 때 이러한 사용자에게 액세스 권한을 할당합니다. 사용자를 격리에 추가하려면 사용자가 존재해야 합니다.

각 사용자는 전체 또는 일부 격리에 액세스하거나 액세스하지 못할 수 있습니다. 격리를 볼 수 있는 권한이 없는 사용자는 GUI 또는 CLI의 격리 리스트 어디에서도 격리의 존재를 확인할 수 없습니다.

관련 주제

- 정책, 바이러스 및 보안 침해 격리에 액세스할 수 있는 사용자 그룹 , 857 페이지
- 관리 작업 배포, 893 페이지

정책, 바이러스 및 보안 침해 격리에 액세스할 수 있는 사용자 그룹

관리 사용자가 격리에 액세스하도록 허용하는 경우 이들이 수행할 수 있는 작업은 사용자 그룹에 따라 다릅니다.

- 관리자 그룹의 사용자는 격리를 만들고 구성하고 삭제하고 중앙 집중화할 수 있으며 격리된 메시지를 관리할 수 있습니다.
- Operators, Guests, Read-Only Operators, Help Desk Users 그룹의 사용자와 격리 관리 권한이 있는 맞춤형 사용자 역할의 사용자는 격리에서 메시지를 검색하고 보고 처리할 수 있지만, 격리의 설정을 변경할 수 없고 격리를 만들거나 삭제하거나 중앙 집중화할 수도 없습니다. 이러한 사용자 중 누가 해당 격리에 액세스할 수 있는지를 각 격리에서 지정합니다.
- Technicians 그룹의 사용자는 격리에 액세스할 수 없습니다.

관련 기능(예: Message Tracking 및 Data Loss Prevention)에 대한 액세스 권한도 관리 사용자가 Quarantine(격리) 페이지에서 볼 수 있는 옵션과 정보에 영향을 미칩니다. 예를 들어 사용자가 Message Tracking(메시지 추적)에 액세스할 수 없으면 해당 사용자는 격리된 메시지에 대한 메시지 추적 링크 및 정보를 볼 수 없습니다.

최종 사용자는 정책, 바이러스 및 전파 확산 격리를 볼 수 없거나 이에 대한 액세스 권한이 없습니다.

클러스터 구성의 정책, 바이러스 및 Outbreak 격리 정보

정책, 바이러스 및 전파 확산 격리는 중앙 집중식 관리 구축의 머신 레벨에서만 구성할 수 있습니다.

중앙 집중식 정책, 바이러스 및 Outbreak 격리 정보

Cisco Content Security Management Appliance에서 정책, 바이러스 및 보안 침해 격리를 중앙 집중화할 수 있습니다. 자세한 내용은 정책, 바이러스 및 Outbreak 격리 중앙 집중화을 참조해 주십시오.

정책, 바이러스 또는 보안 침해 격리의 메시지 작업

관련 주제

격리의 메시지 보기

변경 후	수행해야 할 작업
격리에 있는 모든 메시지 보기	**Monitor(모니터) > Policy, Virus, and Outbreak Quarantines**를 선택합니다. 관련 격리에 대한 행에서 테이블의 **Messages(메시지)** 열에 있는 파란색 번호를 클릭합니다.
Outbreak 격리에 있는 메시지 보기	**Monitor(모니터) > Policy, Virus, and Outbreak Quarantines**를 선택합니다. 관련 격리에 대한 행에서 테이블의 **Messages(메시지)** 열에 있는 파란색 번호를 클릭합니다. [새 웹 인터페이스에만 해당] Manage by Rule Summary(규칙 요약에 의한 관리) 링크, 865 페이지.
격리에 있는 메시지의 리스트 탐색	Previous(이전), Next(다음), 페이지 번호 또는 이중 화살표 링크를 클릭합니다. 이중 화살표를 클릭하면 리스트의 첫 페이지(<<) 또는 마지막 페이지(>>)로 이동합니다.
격리에 있는 메시지의 리스트 정렬	머리글을 클릭합니다(여러 항목을 포함할 수 있는 열 또는 "In other quarantines(기타 격리에)" 열 제외).
테이블 열 크기 조정	머리글 사이의 구분 기호를 드래그합니다.
메시지 격리를 일으킨 내용 보기	일치 콘텐츠 보기 , 862 페이지를 참조하십시오.

관련 주제

격리된 메시지 및 국제 문자 집합

제목에 국제 문자 집합(더블 바이트, 변수 길이, 비 ASCII 인코딩)의 문자가 포함된 메시지의 경우 Policy Quarantine(정책 격리) 페이지의 제목 줄은 디코딩된 형식의 비 ASCII 문자로 표시됩니다.

참고
- 사용자는 액세스 권한이 있는 격리의 메시지만 찾고 볼 수 있습니다.
- 정책, 바이러스 및 Outbreak 격리에서 검색할 경우 스팸 격리의 메시지는 찾을 수 없습니다.

단계 **1** **Monitor(**모니터링**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 신종 바이러스 격리**)**를 선택합니다.

단계 **2** **Search Across Quarantines(**여러 격리에서 검색**)** 버튼을 클릭합니다.

팁 Outbreak 격리의 경우, 각 전파 확산 규칙에 의해 격리된 모든 메시지를 찾을 수도 있습니다. Outbreak(전파 확산) 테이블 행에서 **Manage by Rule Summary(**규칙 요약에 의한 관리**)** 링크를 클릭하고 관련 규칙을 클릭합니다.

단계 **3** (선택 사항) 기타 검색 기준을 입력합니다.

- Envelope Sender(봉투 발신자) 및 Envelope Recipient(봉투 수신자)의 경우: 아무 문자나 입력할 수 있습니다. 입력에 대한 검증이 수행되지 않습니다.
- 검색 결과에는 지정한 모든 기준과 일치하는 메시지만 포함됩니다. 예를 들어 Envelope Recipient(봉투 수신자) 및 Subject(제목)를 지정하면 Envelope Recipient(봉투 수신자) 및 Subject(제목)에 지정한 용어와 일치하는 메시지만 반환됩니다.

다음에 수행할 작업

격리 리스트를 사용하는 것과 동일한 방법으로 검색 결과를 사용할 수 있습니다. 자세한 내용은 격리에 있는 메시지 수동 처리, 859 페이지를 참고하십시오.

격리에 있는 메시지 수동 처리

메시지를 수동으로 처리한다는 것은 Message Actions(메시지 작업) 페이지에서 메시지에 대한 Message Action(메시지 작업)을 수동으로 선택한다는 뜻입니다.

메시지에 대해 다음 작업을 수행할 수 있습니다.

- 삭제
- Release
- 격리에서 Delay Scheduled Exit(예약된 종료 지연)

- 지정한 이메일 주소로 메시지 복사본 전송
- 한 격리에서 다른 격리로 메시지 이동

일반적으로 다음을 수행할 때 표시되는 리스트의 메시지에 대해 작업을 수행할 수 있습니다. 그러나 모든 상황에서 모든 작업을 사용할 수 있는 것은 아닙니다.

- **Monitor(모니터) > Policy, Virus, and Outbreak Quarantines** 또는 페이지의 격리 리스트에서 격리에 있는 메시지의 수를 클릭합니다.
- **Search Across Quarantines(**여러 격리에서 검색**)**를 클릭합니다.
- 격리 이름을 클릭하고 격리 내에서 검색합니다.

다음과 같이 하여 한 번에 여러 메시지에서 이러한 작업을 수행할 수 있습니다.

- 메시지 리스트 상단에 있는 선택 리스트에서 옵션을 선택합니다.
- 페이지에 나열된 각 메시지 옆에 있는 확인란을 선택합니다.
- 메시지 리스트 상단에 있는 테이블 머리글의 확인란을 선택합니다. 이렇게 하면 화면에 보이는 모든 메시지에 작업이 적용됩니다. 다른 페이지의 메시지는 영향을 받지 않습니다.

전파 확산 격리에 있는 메시지에 대해 추가 옵션을 사용할 수 있습니다. 를 참조하십시오.

관련 주제

- 메시지의 복사본 전송, 860 페이지
- 정책 격리 간 메시지 이동 정보 , 860 페이지
- 여러 격리에 있는 메시지 , 861 페이지
- 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 851 페이지

메시지의 복사본 전송

Administrators 그룹에 속한 사용자만 메시지의 복사본을 전송할 수 있습니다.

메시지의 복사본을 전송하려면 Send Copy To:(복사본 전송 대상:) 필드에 이메일 주소를 입력하고 **Submit(**제출**)**을 클릭합니다. 메시지의 복사본을 전송할 경우 메시지에 대한 다른 작업이 수행되지는 않습니다.

정책 격리 간 메시지 이동 정보

단일 어플라이언스의 한 정책 격리에서 다른 정책 격리로 메시지를 수동으로 이동할 수 있습니다.

메시지를 다른 격리로 이동하는 경우

- 만료 시간이 변경되지 않습니다. 메시지에서 원래 격리의 보유 시간이 유지됩니다.
- 내용과 기타 관련 세부사항 불일치 등 메시지가 격리된 이유가 변경되지 않습니다.

- 한 메시지가 여러 격리에 있는 상태에서 이 메시지의 복사본이 이미 있는 대상으로 메시지를 이동하는 경우, 이동한 메시지 복사본의 만료 시간과 격리 이유가 원래 대상 격리에 있던 메시지 복사본의 내용을 덮어씁니다.

여러 격리에 있는 메시지

한 메시지가 하나 이상의 다른 격리에 있는 경우, 그러한 격리에 액세스 권한이 있는지와 상관없이 격리 메시지 리스트의 "In other quarantines(다른 격리에)" 열에 "Yes(예)"가 표시됩니다.

한 메시지가 여러 격리에 있는 경우

- 상주하는 모든 격리에서 릴리스되지 않는 한 전달되지 않습니다. 한 격리에서 메시지가 삭제되면 해당 메시지는 전달되지 않습니다.
- 상주하는 모든 격리에서 삭제 또는 릴리스되기 전에는 어떤 격리에서도 삭제되지 않습니다.

메시지를 릴리스하려는 사용자가 메시지가 상주하는 모든 격리에 액세스하지는 못할 수 있으므로 다음 규칙이 적용됩니다.

- 상주하는 모든 격리에서 릴리스되기 전에는 어떤 격리에서도 릴리스되지 않습니다.
- 한 격리에서 메시지가 Deleted(삭제됨)로 표시된 경우, 상주하는 다른 모든 격리에서 전달될 수 없습니다. (여전히 릴리스는 가능합니다.)

한 메시지가 여러 격리의 대기열에 있는 상태에서 사용자가 하나 이상의 다른 격리에 액세스할 수 없는 경우

- 사용자가 액세스할 수 있는 각 격리에 메시지가 있는지 여부에 대한 알림이 제공됩니다.
- GUI에는 사용자가 액세스할 수 있는 격리에서의 예약된 종료 시간만 표시됩니다. (어떤 메시지의 경우 각 격리에 대한 별도의 종료 시간이 있습니다.)
- 메시지가 있는 다른 격리의 이름은 사용자에게 표시되지 않습니다.
- 사용자는 자신이 액세스할 수 없는 격리로 메시지를 보낸 일치 콘텐츠를 볼 수 없습니다.
- 메시지의 릴리스는 사용자가 액세스할 수 있는 대기열에만 영향을 미칩니다.
- 사용자가 액세스할 수 없는 다른 격리의 대기열에도 메시지가 있는 경우, 나머지 격리에 대해 필요한 액세스 권한이 있는 사용자가 조치를 취할 때까지(또는 조기 만료나 정상 만료를 통해 "정상적으로" 릴리스될 때까지) 해당 메시지는 현재 상태 그대로 격리에 남아 있게 됩니다.

메시지 세부사항 및 메시지 내용 보기

메시지의 내용을 보고 Quarantined Message(격리된 메시지) 페이지에 액세스하려면 메시지의 제목 줄을 클릭합니다.

Quarantined Message(격리된 메시지) 페이지에는 Quarantine Details(격리 세부사항) 및 Message Details(메시지 세부사항)의 두 섹션이 있습니다.

Quarantined Message(격리된 메시지) 페이지에서 메시지를 읽거나, Message Action(메시지 작업)을 선택하거나메시지의 복사본을 전송하거나, 바이러스를 테스트할 수 있습니다. Encrypt on Delivery(전달 시 암호화) 필터 작업에 따라 격리에서 릴리스될 때 메시지가 암호화될지 여부를 확인할 수도 있습니다.

Message Details(메시지 세부사항) 섹션에는 메시지 본문, 메시지 헤더 및 어태치 파일이 표시됩니다. 메시지 본문의 처음 100K만 표시됩니다. 메시지가 더 길면 처음 100K만 표시되고 그 뒤에 줄임표(...)가 나옵니다. 실제 메시지는 잘리지 않습니다. 단지 표시를 위한 것입니다. Message Details(메시지 세부사항) 하단의 Message Parts(메시지 부분) 섹션에서 [message body]를 클릭하여 메시지 본문을 다운로드할 수 있습니다. 어태치 파일의 이름을 클릭하여 메시지 어태치 파일을 다운로드할 수도 있습니다.

컴퓨터에 안티바이러스 소프트웨어를 설치한 상태에서 바이러스가 포함된 메시지를 보는 경우, 안티바이러스 소프트웨어에 바이러스 검색 알림이 표시될 수 있습니다. 이는 컴퓨터에 위협이 되지 않으며 안전하게 무시할 수 있습니다.

메시지에 대한 추가 세부사항을 보려면 **Message Tracking(**메시지 추적**)** 링크를 클릭합니다.

참고 특수 Outbreak 격리의 경우 추가 기능을 사용할 수 있습니다. Outbreak 격리, 864 페이지를 참조하십시오.

관련 주제

- 일치 콘텐츠 보기 , 862 페이지
- 어태치 파일 다운로드 , 863 페이지
- 바이러스 테스트, 863 페이지

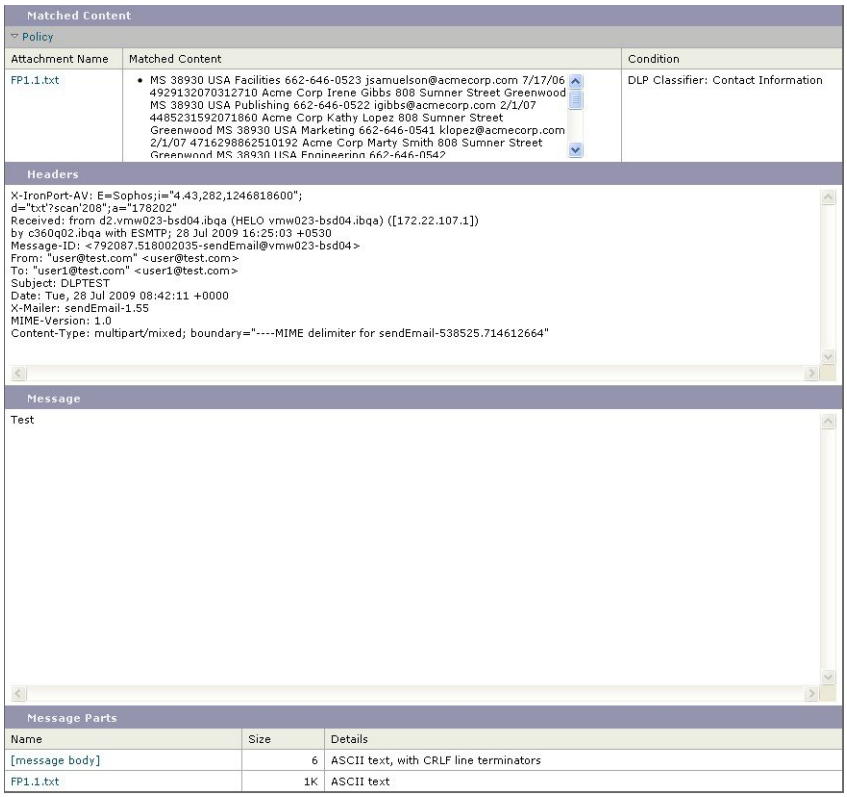
일치 콘텐츠 보기

Attachment Content(어태치 파일 내용) 조건, Message Body or Attachment(메시지 본문 또는 어태치 파일) 조건, Message Body(메시지 본문) 조건, Attachment Content(어태치 파일 내용) 조건을 구성할 때 격리된 메시지에서 일치 콘텐츠를 볼 수 있습니다. 메시지 본문을 표시하면 DLP 정책 위반 일치를 제외하고, 일치 콘텐츠가 노란색으로 강조 표시됩니다. 메시지의 일치 콘텐츠 또는 메시지 제목의 콘텐츠 필터 일치를 포함하려면 $MatchedContent 작업 변수를 사용할 수도 있습니다.

어태치 파일에 일치 콘텐츠가 포함되어 있으면 어태치 파일의 내용과 함께 DLP 정책 위반, 콘텐츠 필터 조건, 메시지 필터 조건, Image Analysis(이미지 분석) 판정 등의 격리된 이유가 표시됩니다.

메시지 또는 콘텐츠 필터 규칙을 트리거한 로컬 격리에 있는 메시지를 볼 때, 실제로 필터 작업을 트리거하지 않은 내용이 필터 작업을 트리거한 내용과 함께 GUI에 표시될 수 있습니다. GUI 표시는 콘텐츠 일치를 찾기 위한 지침으로 사용해야 하지만, 콘텐츠 일치의 정확한 리스트를 반영하는 것은 아닙니다. 이런 일이 발생하는 이유는 GUI가 필터에 사용되는 것보다 덜 엄격한 콘텐츠 일치 논리를 사용하기 때문입니다. 이 문제는 메시지 본문의 강조 표시 부분에만 적용됩니다. 메시지 각 부분의 일치하는 문자열을 관련 필터 규칙과 함께 나열하는 테이블이 정확합니다.

그림 ***71:*** 정책 격리에 표시되는 일치 콘텐츠



어태치 파일 다운로드

Message Parts(메시지 부분) 또는 Matched Content(일치 콘텐츠) 섹션에서 어태치 파일의 이름을 클릭하여 메시지 어태치 파일을 다운로드할 수 있습니다. AsyncOS는 알 수 없는 소스의 어태치 파일에 바이러스가 포함되어 있을 수 있다는 경고를 표시하고 계속 진행할지를 물어봅니다. 바이러스가 포함되어 있을 수 있는 어태치 파일을 다운로드할 경우 스스로 위험을 감수해야 합니다. Message Parts(메시지 부분) 섹션에서 [message body]를 클릭하여 메시지 본문을 다운로드할 수도 있습니다.

바이러스 테스트

메시지에서 바이러스를 테스트하려면 **Start Test(**테스트 시작**)**를 클릭합니다. 안티바이러스 서명이 업데이트된 것을 확인할 때까지 격리를 사용하여 메시지를 보유합니다.

바이러스를 테스트하면 메시지 자체가 아니라 복사본이 안티바이러스 엔진으로 전송됩니다. 안티바이러스 엔진에서 판정이 반환되어 Quarantines(격리) 영역 위에 표시됩니다.

격리된 메시지 재검사 정보

격리된 모든 대기열에서 메시지가 릴리스되면, 메시지를 원래 격리한 메일 정책 및 어플라이언스에 대해 활성화된 기능에 따라 다음 재검사가 발생합니다.

- 정책 및 바이러스 격리에서 릴리스된 메시지는 안티바이러스, AMP(Advanced Malware Protection) 및 그레이메일 엔진을 통해 검사됩니다.
- Outbreak 격리에서 릴리스된 메시지는 안티스팸 및 안티바이러스 엔진에 의해 재검사됩니다. 보안 침해 격리에 있는 동안 메시지 재검사에 대한 자세한 내용은 를 참조하십시오.)
- File Analysis(파일 분석) 격리에서 릴리스된 메시지에 대해서는 위협이 재검사됩니다.
- 어태치 파일이 있는 메시지는 Policy(정책), Virus(바이러스) 및 Outbreak 격리에서 릴리스될 때 파일 평판 서비스에 의해 재검사됩니다.

재검사 시, 현재의 판정이 이전 메시지 처리 시의 판정과 일치하면 메시지가 재격리되지 않습니다. 반대로, 판정이 다르면 메시지가 또 다른 격리로 전송될 수 있습니다.

이렇게 하는 이론적 근거는 메시지가 격리로 무제한 루프백되는 것을 방지하기 위함입니다. 예를 들어, 메시지가 암호화되어 Virus(바이러스) 격리로 전송된다고 가정해보겠습니다. 관리자가 메시지를 릴리스하면 안티바이러스 엔진에서는 여전히 이를 해독할 수 없습니다. 그러나 메시지를 재격리해서는 안 됩니다. 루프가 생성되어 메시지가 격리에서 영구적으로 릴리스되지 않을 것이기 때문입니다. 두 판정이 동일하면 시스템은 두 번째에 Virus(바이러스) 격리를 우회합니다.

Outbreak 격리

유효한 Outbreak Filter 기능 라이선스 키를 입력하면 Outbreak 격리가 표시됩니다. Outbreak Filter 기능은 설정된 임계값에 따라 Outbreak 격리로 메시지를 전송합니다. 자세한 내용은 을 참조하십시오.

Outbreak 격리의 작동 방식은 다른 격리와 유사합니다. 메시지를 검색, 릴리스 또는 삭제할 수 있습니다.

- Standard(표준)
- 규칙 요약

보안 침해 격리에는 Manage by Rule Summary(규칙 요약에 의한 관리) 링크, 메시지 세부사항을 볼 때 Send to Cisco(Cisco로 전송) 기능, Scheduled Exit(예약된 종료) 시간별로 검색 결과의 메시지를 정렬하는 옵션 등 다른 격리에서 사용할 수 없는 몇 가지 추가 기능이 있습니다.

Outbreak Filter 기능에 대한 라이선스가 만료되면 Outbreak 격리에 메시지를 더 이상 추가할 수 없습니다. 현재 격리에 있는 메시지가 만료되어 Outbreak 격리가 비게 되면 GUI의 Quarantines(격리) 리스트에 더 이상 표시되지 않습니다.

관련 주제

- Outbreak 격리에 있는 메시지 재검사 , 864 페이지
- Manage by Rule Summary(규칙 요약에 의한 관리) 링크, 865 페이지
- Cisco Systems에 오탐 또는 의심스런 메시지 보고, 865 페이지

Outbreak 격리에 있는 메시지 재검사

격리된 메시지가 더 이상 위협이 아니라고 새로 게시된 규칙에서 결정하면 Outbreak 격리에 있는 메시지는 자동으로 릴리스됩니다.

어플라이언스에서 안티스팸과 안티바이러스가 활성화되어 있으면, 검사 엔진은 메시지에 적용된 메일 플로우 정책을 기반으로 Outbreak 격리에서 릴리스된 모든 메시지를 검사합니다.

Manage by Rule Summary(규칙 요약에 의한 관리) 링크

Manage by Rule Summary(규칙 요약에 의한 관리) 페이지를 보려면 격리 리스트에서 Outbreak 격리 옆에 있는 Manage by Rule Summary(규칙 요약에 의한 관리) 링크를 클릭합니다. 메시지를 격리시킨 전파 확산 규칙을 기반으로 격리에 있는 모든 메시지에 대해 메시지 작업(Release, Delete, Delay Exit)을 수행할 수 있습니다. 이것은 Outbreak 격리에서 상당수의 메시지를 삭제하기 위한 이상적인 방법입니다. 자세한 내용은 Outbreak Quarantine(보안 침해 격리) 및 Manage by Rule Summary(규칙 요약에 의한 관리) 보기의 주제를 참조하십시오.

Cisco Systems에 오탐 또는 의심스런 메시지 보고

Outbreak 격리의 메시지에 대한 메시지 세부사항을 볼 때 오탐 또는 의심스런 메시지를 보고하기 위해 Cisco에 메시지를 전송할 수 있습니다.

단계 **1** Outbreak 격리에 있는 메시지로 이동합니다.

단계 **2** Message Details(메시지 세부사항) 섹션에서 **Send a Copy to Cisco Systems(Cisco Systems**에 복사본 전송**)** 확인란을 선택합니다.

단계 **3** **Send(**보내기**)**를 클릭합니다.

34 장

스팸 격리

이 장에는 다음 섹션이 포함되어 있습니다.

스팸 격리 개요

스팸 격리(ISQ라고도 함) 및 엔드 유저 격리(EUQ라고도 함)는 이메일 메시지가 합법적이지만 어플라이언스에서 스팸으로 간주하는 "오탐"을 우려하는 조직을 위한 안전 메커니즘을 제공합니다. 어플라이언스에서 메시지가 스팸인지 또는 의심스러운 스팸인지를 확인할 때, 메시지를 전달 또는 삭제하기 전에 수신자나 관리자가 검토하도록 할 수 있습니다. 스팸 격리는 이 목적으로 메시지를 저장합니다.

Email Security Appliance의 관리 사용자는 스팸 격리의 모든 메시지를 볼 수 있습니다. 최종 사용자(대개 메시지 수신자)는 약간 다른 웹 인터페이스에서 자신의 격리된 메시지를 볼 수 있습니다.

스팸 격리는 정책, 바이러스 및 보안 침해 격리와 다릅니다.

관련 주제

- Anti-Spam, 355 페이지
- 정책, 바이러스, 보안 침해 격리, 847 페이지

로컬 대 외부 스팸 격리

로컬 스팸 격리는 Email Security Appliance에 스팸 및 의심스러운 스팸을 저장합니다. 외부 스팸 격리는 이러한 메시지를 별도의 Cisco Content Security Management Appliance에 저장할 수 있습니다.

다음과 같은 경우에는 외부 스팸 격리의 사용을 고려해볼 수 있습니다.

- 여러 Email Security Appliance에서 오는 스팸을 저장 및 관리할 중앙 집중식 위치가 필요한 경우.
- Email Security Appliance에 보관할 수 있는 것보다 더 많은 스팸을 저장하려는 경우.
- 스팸 격리 및 해당 메시지를 정기적으로 백업하려는 경우

관련 주제

- 스팸 격리에 대한 디스크 공간 , 892 페이지
- 외부 스팸 격리 작업 , 1188 페이지

로컬 스팸 격리 설정

다음 표에는 스팸 격리에 메시지를 전송하는 방법이 나와 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	아직 하지 않았다면 Anti-Spam(안티스팸) 기능을 활성화합니다.	자세한 내용은 Anti-Spam, 355 페이지을 참고하십시오.
단계 **2**	격리 설정을 활성화 및 구성합니다.	자세한 내용은 스팸 격리 활성화 및 구성 , 869 페이지을 참고하십시오.
단계 **3**	스팸 격리에 할당된 디스크 공간을 조정합니다.	자세한 내용은 디스크 공간 관리 , 941 페이지을 참조해 주십시오.
단계 **4**	격리에 대한 브라우저 액세스를 활성화합니다.	자세한 내용은 브라우저가 스팸 격리에 액세스하도록 IP 인터페이스 구성 , 871 페이지을 참조해 주십시오.
단계 **5**	스팸을 격리로 전송하도록 Email Security Appliance를 구성합니다.	자세한 내용은 다음을 참조하십시오. • 스팸을 격리하기 위한 메일 정책 구성 , 872 페이지 • 메일을 격리할 수신자 제한 , 872 페이지
단계 **6**	제목에 이 정보가 없는 메시지에 대한 기본 문자 인코딩을 지정합니다.	자세한 내용은 메시지 텍스트가 올바르게 표시되는지 확인 , 872 페이지을 참조해 주십시오.

다음에 수행할 작업

관련 주제

스팸 격리 활성화 및 구성

참고 외부 스팸 격리를 사용하는 경우 Security Management Appliance의 이 섹션에 설명된 설정을 구성하게 됩니다.

단계 **1** **Monitor(**모니터**) >Spam Quarantine(**스팸 격리**)**을 선택합니다.

단계 **2** 전에 스팸 격리를 활성화하지 않은 경우 **Enable Spam Quarantine(**스팸 격리 활성화**)**을 선택합니다.

스팸 격리 설정을 수정하는 경우 Spam Quarantine(스팸 격리) 섹션의 Quarantine Name(격리 이름) 열에서 **Spam Quarantine(**스팸 격리**)** 링크를 클릭합니다.

단계 **3** 옵션을 지정합니다.

옵션	설명
Deliver Messages Via(메시지 전달 경로)	모든 발신 격리 관련 이메일(예: 스팸 알림 및 스팸 격리에서 릴리스된 메시지)은 메시지를 전송하도록 구성된 서버 또는 다른 어플라이언스를 통해 전달해야 합니다. SMTP 또는 그룹웨어 서버를 통해 이러한 메시지를 라우팅하거나, Email Security Appliance의 아웃바운드 리스너 인터페이스(일반적으로 Data 2 인터페이스)를 지정할 수 있습니다. 로드 밸런싱 및 장애 조치에 대체 주소가 사용됩니다. 여러 Email Security Appliance가 있는 경우, 기본 및 대체 주소에 대해 관리되는 Email Security Appliance의 아웃바운드 리스너 인터페이스를 사용할 수 있습니다. 아웃바운드 리스너로 동일한 인터페이스(Data 1 또는 Data 2)를 사용해야 합니다. 이러한 주소에 대한 추가 주의 사항은 화면의 지침을 참조하십시오.

옵션	설명
쿼런틴 크기	**When storage space is full, automatically delete oldest messages first**(스토리지 공간이 꽉 차면 가장 오래된 메시지부터 자동으로 삭제)의 선택을 취소하면 꽉 찬 격리에 새 메시지가 추가되지 않습니다. 꽉 찬 격리 때문에 메시지가 어플라이언스에서 대기열에 추가(백업)되지 않도록 하려면 이 옵션을 활성화하는 것이 좋습니다. 격리에 대한 디스크 공간 관리는 디스크 공간 관리 , 941 페이지 섹션을 참조하십시오.
Schedule Delete After(삭제 기준 일정)	삭제 전에 메시지를 유지할 일수를 지정합니다. 격리의 용량이 꽉 차는 것을 방지하기 위해 오래된 메시지를 삭제하도록 격리를 구성하는 것이 좋지만, 자동 삭제를 예약하지 않을 수도 있습니다.
Notify Cisco Upon Message Release(메시지 릴리스 시 Cisco에 알림)	—
Spam Quarantine Appearance(스팸 격리 모양)	로고 기본적으로 사용자가 격리된 메시지를 보기 위해 로그인하면 스팸 격리 페이지 상단에 Cisco 로고가 표시됩니다. 대신 맞춤형 로고를 사용하려면 해당 로그를 업로드합니다. 로고는 최대 50픽셀(세로) X 500픽셀(가로)의 .jpg, .gif 또는 .png 파일이어야 합니다.
	로그인 페이지 메시지 (선택 사항) 로그인 페이지 메시지를 지정합니다. 이 메시지는 격리를 보기 위해 로그인하는 관리자 및 최종 사용자에게 표시됩니다. 메시지를 지정하지 않으면 다음 메시지가 나타납니다. Enter your login information below. If you are unsure what to enter, please contact your administrator.(아래에 로그인 정보를 입력하십시오. 입력할 정보를 모르면 관리자에게 문의하십시오.)
관리자	스팸 격리에 대한 관리 사용자 액세스 구성 , 871 페이지를 참조하십시오.

단계 **4** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

- 다음으로 돌아갑니다. 로컬 스팸 격리 설정, 868 페이지

브라우저가 스팸 격리에 액세스하도록 IP 인터페이스 구성

관리자와 최종 사용자가 스팸 격리에 액세스하면 별도의 브라우저 창이 열립니다.

단계 **1** **Network**(네트워크) > **IP Interfaces**(IP 인터페이스)를 선택합니다.

단계 **2** 인터페이스 이름을 클릭합니다(이 예에서는 Management 인터페이스 사용).

단계 **3** Spam Quarantine(스팸 격리) 섹션에서 스팸 격리에 액세스하기 위한 설정을 구성합니다.

- 기본적으로 HTTP는 포트 82를 사용하고 HTTPS는 포트 83을 사용합니다.
- 알림 및 스팸 격리 브라우저 창에 나타나는 URL을 지정합니다.

  Security Management Appliance의 호스트 이름을 최종 사용자에게 노출하지 않으려면 대체 호스트 이름을 지정할 수 있습니다.

단계 **4** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

스팸 격리 액세스를 위해 지정한 호스트 이름을 DNS 서버가 인식할 수 있는지 확인합니다.

스팸 격리에 대한 관리 사용자 액세스 구성

관리자 권한이 있는 모든 사용자는 스팸 격리 설정을 변경하고 스팸 격리의 메시지를 보고 관리할 수 있습니다. 관리자 사용자에 대해서는 스팸 격리 액세스를 구성할 필요가 없습니다.

다음 역할의 사용자에 대해 스팸 격리에 대한 액세스를 구성하는 경우 해당 사용자는 스팸 격리의 메시지를 보고 릴리스하고 삭제할 수 있습니다.

- 운영자
- Read-only operator
- Help desk user
- 게스트
- 스팸 격리 권한을 가진 맞춤형 사용자 역할

이러한 사용자는 스팸 격리 설정에 액세스할 수 없습니다.

시작하기 전에

스팸 격리에 액세스할 수 있는 사용자 또는 맞춤형 사용자 역할을 만듭니다. 자세한 내용은 관리 작업 배포, 893 페이지 정보를 참조하십시오.

단계 **1** 아직 스팸 격리 설정 페이지를 수정하고 있지 않은 경우

a) **Monitor**(모니터) > **Spam Quarantine**(스팸 격리)을 선택합니다.

b) **Edit Settings**(설정 수정) 링크를 클릭합니다.

단계 **2** 추가할 사용자 유형(로컬, 외부 인증 또는 맞춤형 역할)에 대한 링크를 클릭합니다.

사용자 또는 역할을 이미 추가한 경우 모든 해당 사용자 또는 역할을 보려면 사용자 이름이나 역할을 클릭합니다.

단계 **3** 추가할 사용자 또는 역할을 선택합니다.

관리자 권한을 가진 사용자는 스팸 격리에 자동으로 전체 액세스 권한을 가지므로 나열되지 않습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

스팸 격리에 대한 최종 사용자 액세스 구성 , 884 페이지

스팸을 격리하기 위한 메일 정책 구성

스팸 격리를 활성화했으면 스팸이나 의심스런 스팸을 해당 격리로 전송하기 위한 메일 정책을 구성할 수 있습니다. 메일을 스팸 격리로 전송하려면 메일 정책에서 안티 스팸 검사를 활성화해야 합니다.

단계 **1** **Mail Policies(**메일 정책**) > Incoming Mail Policies(**수신 메일 정책**)** 페이지에서 해당 메일 정책에 대한 Anti-Spam(안티 스팸) 열의 링크를 클릭합니다.

단계 **2** Anti-Spam Settings(안티 스팸 설정) 섹션에서 **Use IronPort Anti-Spam service(IronPort** 안티스팸 서비스 사용**)**를 선택합니다.

단계 **3** Positively-Identified Spam Settings(양성으로 식별된 스팸 설정) 섹션에서 **Apply This Action to Message(**메시지에 이 작업 적용**)** 옵션에 대해 **Spam Quarantine(**스팸 격리**)**을 선택합니다.

단계 **4** 의심스런 스팸 및 마케팅 이메일에 대한 설정을 구성합니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

메일을 격리할 수신자 제한

메일을 격리하지 않을 수신자 주소 목록을 지정하려면 Email Security Appliance에서 여러 메일 정책(Mail Policies(메일 정책) > Incoming Mail Policy(수신 메일 정책))을 사용할 수 있습니다. 메일 정책의 안티스팸 설정을 구성할 때 격리 대신 'Deliver(전달)' 또는 'Drop(삭제)'을 선택합니다.

메시지 텍스트가 올바르게 표시되는지 확인

AsyncOS는 메시지 헤더에 지정된 인코딩을 기반으로 메시지의 문자 집합을 확인하려고 시도합니다. 그러나 헤더에 지정된 인코딩이 실제 텍스트의 인코딩과 일치하지 않으면 스팸 격리에서 볼 때 메시지가 제대로 표시되지 않습니다. 이런 상황은 스팸 메시지에서 발생할 가능성이 높습니다.

이러한 메시지에 대해 메시지 텍스트가 올바르게 표시되는지 확인하려면 을 참조하십시오.

관련 항목

- 기본 인코딩 지정 , 873 페이지

기본 인코딩 지정

수신 메시지의 헤더에 문자 집합 인코딩이 지정되어 있지 않으면, 기본 인코딩을 지정하도록 어플라이언스를 구성할 수 있습니다.

그렇게 하면 이러한 유형의 메시지를 스팸 격리에서 제대로 표시하는 데 도움이 됩니다. 그러나 기본 인코딩을 지정하면 다른 문자 집합의 메시지가 올바르게 표시되지 않을 수 있습니다. 이 설정은 메시지 헤더에 인코딩이 지정되지 않은 메시지에만 적용됩니다. 일반적으로 이 범주에 속하는 메일 대다수가 하나의 특정 인코딩이라고 예상되는 경우에만 기본 인코딩을 설정합니다.

예를 들어 메시지 헤더의 문자 집합 인코딩이 지정되지 않은 대부분의 격리 메시지가 일본어(ISO-2022-JP)인 경우, Scan Behavior(검사 동작) 페이지에서 인코딩을 **Japanese (ISO-2022-JP)**로 설정할 수 있습니다.

단계 **1** **Security Services(**보안 서비스**)** > **Scan Behavior(**검사 동작**)**를 클릭합니다.

단계 **2** Global Settings(전역 설정)에서 **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **3** **Encoding to use when none is specified(**지정된 인코딩이 없는 경우 사용할 인코딩**)** 드롭다운 목록에서 원하는 인코딩 유형을 선택합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

단계 **5** **Commit Changes(**변경 커밋**)**를 클릭합니다.

스팸 격리 언어

최종 사용자는 창 오른쪽 상단에 있는 Options(옵션) 메뉴에서 스팸 격리의 언어를 선택합니다.

허용 목록 및 차단 목록을 사용하여 발신자 기준으로 이메일 전달 제어

관리자 및 최종 사용자는 스팸 메시지를 식별하는 데 허용 목록과 차단 목록을 사용할 수 있습니다. 허용 목록은 스팸으로 취급되지 않을 발신자 및 도메인을 지정합니다. 차단 목록은 항상 스팸으로 취급될 발신자 및 도메인을 지정합니다.

최종 사용자(이메일 사용자)가 각자의 이메일 계정에 대해 허용 목록과 차단 목록을 관리하도록 허용할 수 있습니다. 예를 들어, 최종 사용자가 더 이상 관심이 없는 메일 목록에서 이메일을 수신할 수 있습니다. 이 발신자의 이메일이 메일 목록에서 자신의 받은 편지함으로 전송되지 않도록 하려면 해당 발신자를 차단 목록에 추가할 수 있습니다. 반면, 스팸으로 취급하고 싶지 않은 특정 발신자의 이메

일이 스팸 격리로 전송되는 경우를 발견할 수 있습니다. 이러한 발신자의 메시지가 격리되지 않도록 하려면 해당 발신자를 허용 목록에 추가할 수 있습니다.

최종 사용자 및 관리자는 설정을 변경할 수 있으며 이러한 변경 사항을 볼 수 있습니다.

관련 주제

- 허용 목록 및 차단 목록의 메시지 처리 , 874 페이지
- 허용 목록 및 차단 목록 활성화 , 875 페이지
- 외부 스팸 격리 및 허용 목록/차단 목록 , 875 페이지
- 허용 목록 및 차단 목록에 발신자 및 도메인 추가(관리자) , 876 페이지
- 허용 목록 및 차단 목록에 대한 최종 사용자 액세스 정보 , 878 페이지
- 여러 Email Security Appliance에서 허용 목록 또는 차단 목록 동기화(Security Management Appliance 없이 구축) , 879 페이지
- 허용 목록/차단 목록 백업 및 복원 , 880 페이지
- 허용 목록 및 차단 목록 문제 해결, 880 페이지

허용 목록 및 차단 목록의 메시지 처리

허용 목록 또는 차단 목록에 있는 발신자에 대해서도 어플라이언스는 메시지에서 바이러스를 검사하며, 메시지가 콘텐츠 관련 메일 정책의 기준을 충족하는지 확인합니다. 메시지 발신자가 수신자의 허용 목록에 있더라도 검사 설정 및 결과에 따라 메시지가 최종 사용자에게 전달되지 않을 수 있습니다.

허용 목록 및 차단 목록을 활성화하면 어플라이언스는 안티스팸 검사 직전에 허용 목록/차단 목록 데이터베이스를 기준으로 메시지를 검사합니다. 어플라이언스가 허용 목록 또는 차단 목록과 일치하는 발신자나 도메인을 검색하면, 다중 수신자인 경우(그리고 수신자의 허용 목록/차단 목록 설정이 다른 경우) 메시지가 분리됩니다. 예를 들어 메시지가 수신자 A 및 수신자 B에게 전송되는데, 수신자 A는 해당 발신자를 허용 목록에 추가한 반면 수신자 B는 허용 목록이나 차단 목록에 해당 발신자의 항목이 없습니다. 이 경우 메시지는 두 개의 메시지 ID와 함께 둘로 분리됩니다. 수신자 A에게 전송되는 메시지는 *X-SLBL-Result-Safelist* 헤더와 함께 허용 목록 항목으로 표시되는 반면, 수신자 B에 대한 메시지는 안티 스팸 검사 엔진의 검사를 받게 됩니다. 두 메시지는 계속해서 파이프라인을 따라 이동하며(안티바이러스 검사, 콘텐츠 정책 등) 구성된 설정에 따라 처리됩니다.

메시지 발신자 또는 도메인이 차단 목록에 있으면, 허용 목록/차단 목록 기능을 활성화할 때 지정한 차단 목록 작업을 기반으로 전달 동작이 수행됩니다. 허용 목록 전달과 마찬가지로, 서로 다른 허용 목록/차단 목록 설정의 서로 다른 수신자가 있는 경우 메시지가 분리됩니다. 차단 목록에 따라 분리된 메시지는 차단 목록 작업 설정에 따라 격리되거나 삭제됩니다. 차단 목록 작업이 격리로 구성된 경우 메시지가 검사되고 결국 격리됩니다. 차단 목록 작업이 삭제로 구성된 경우 허용 목록/차단 목록 검사 직후 메시지가 삭제됩니다.

허용 목록 및 차단 목록은 스팸 격리에서 유지 관리되므로 전달 동작도 다른 안티스팸 설정에 따라 달라집니다. 예를 들어 안티스팸 검사를 건너뛰도록 HAT(Host Access Table)의 "Accept(수락)" 메일 플로우 정책을 구성한 경우, 해당 리스너에서 메일을 수신하는 사용자는 수신한 메일에 허용 목록 및 차단 목록 설정을 적용할 수 없습니다. 마찬가지로, 특정 메시지 수신자에 대해 안티스팸 검사를 건너뛰는 메일 플로우 정책을 만들면 해당 수신자에게는 허용 목록 및 차단 목록 설정이 적용되지 않습니다.

관련 주제

- 허용 목록 및 차단 목록 활성화 , 875 페이지
- 외부 스팸 격리 및 허용 목록/차단 목록 , 875 페이지

허용 목록 및 차단 목록 활성화

시작하기 전에

- 스팸 격리를 활성화해야 합니다. 로컬 스팸 격리 설정, 868 페이지를 참조하십시오.
- 외부 허용 목록/차단 목록을 사용하도록 Email Security Appliance를 구성합니다. Email Security Appliance에 대한 문서에서 외부 스팸 격리 설정에 대한 지침을 참조하십시오.

단계 **1** **Monitor**(모니터) > **Spam Quarantine**(스팸 격리)을 선택합니다.

단계 **2** **End-User Safelist/Blocklist (Spam Quarantine)**(최종 사용자 허용 목록/차단 목록(스팸 격리)) 섹션에서 **Enable**(활성화)을 선택합니다.

단계 **3** **Enable End User Safelist/Blocklist Feature**(최종 사용자 허용 목록/차단 목록 기능 활성화)를 선택합니다.

단계 **4** Blocklist Action(차단 목록 작업)에 대해 **Quarantine**(격리) 또는 **Delete**(삭제)를 선택합니다.

단계 **5** **Maximum List Items Per User**(사용자당 최대 목록 항목)를 지정합니다.

이 값은 각 목록에서 각 수신자별 최대 주소 또는 도메인 수입니다. 사용자당 다수의 목록 항목을 허용하면 시스템 성능이 저하될 수 있습니다.

단계 **6** 업데이트 빈도를 선택합니다. 이 값은 AsyncOS가 외부 스팸 격리를 사용하는 Email Security Appliance에서 허용 목록/차단 목록을 업데이트하는 빈도를 결정합니다. 이 설정의 중요성에 대해서는 외부 스팸 격리 및 허용 목록/차단 목록 , 875 페이지에 설명되어 있습니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

외부 스팸 격리 및 허용 목록/차단 목록

Security Management Appliance에서 외부 스팸 격리를 사용하는 경우 허용 목록/차단 목록이 관리 어플라이언스에 저장됩니다. 따라서 단일 위치에서 모든 어플라이언스에 대해 허용 및 차단 발신자를 관리할 수 있습니다.

Email Security Appliance는 수신 메일을 처리할 때 허용 목록 및 차단 목록의 발신자를 평가하므로, 수신 메일에 적용하려면 Security Management Appliance에 저장된 허용 목록 및 차단 목록을 Email Security Appliance로 전송해야 합니다. Security Management Appliance에서 허용 목록/차단 목록 기능을 구성할 때 이러한 업데이트의 빈도를 구성합니다.

Security Management Appliance에서 외부 허용 목록 및 차단 목록 작업에 대한 자세한 내용은 *Cisco Content Security Management Appliance* 사용 설명서의 주제를 참조하십시오.

허용 목록 및 차단 목록에 발신자 및 도메인 추가(관리자)

허용 목록 및 차단 목록은 스팸 격리 인터페이스를 통해 관리합니다.

많은 수신자(조직의 최종 사용자)가 특정 발신자 또는 도메인을 화이트리스트 또는 블랙리스트에 추가했는지도 확인할 수 있습니다.

관리자는 각 최종 사용자가 보고 작업하는 동일한 항목의 상위 집합을 보고 관리합니다.

시작하기 전에

- 스팸 격리에 액세스할 수 있는지 확인합니다. 스팸 격리에 액세스(관리 사용자), 890 페이지를 참조하십시오.
- 허용 목록/차단 목록에 대한 액세스를 활성화합니다. 허용 목록 및 차단 목록 활성화 , 875 페이지를 참조하십시오.
- (선택 사항) 이 섹션의 절차를 사용하여 이러한 목록을 작성하는 대신 허용 목록/차단 목록을 가져오려면 허용 목록/차단 목록 백업 및 복원 , 880 페이지에 설명된 프로세스를 사용합니다.
- 허용 목록 및 차단 목록 항목의 필수 형식을 이해합니다. 허용 목록 및 차단 목록 항목의 구문 , 877 페이지를 참조하십시오.

단계 **1** 브라우저를 사용하여 스팸 격리에 액세스합니다.

단계 **2** 로그인합니다.

단계 **3** 페이지의 오른쪽 상단에 있는 **Options(**옵션**)** 드롭다운 메뉴를 선택합니다.

단계 **4** **Safelist(**허용 목록**)** 또는 **Blocklist(**차단 목록**)**를 선택합니다.

단계 **5** (선택 사항) 발신자 또는 수신자를 검색합니다.

단계 **6** 다음 중 하나를 수행합니다.

변경 후	수행해야 할 작업
한 명의 수신자에 대해 여러 발신자 추가	1. **View by: Recipient(**보기 기준**:** 수신자**)**를 선택합니다. 2. **Add(**추가**)**를 클릭하거나, 수신자에 대해 **Edit(**수정**)**을 클릭합니다. 3. 수신자 이메일 주소를 입력하거나 수정합니다. 4. 발신자 이메일 주소 및 도메인을 입력합니다. 각 항목을 별도의 줄에 입력하거나, 쉼표로 각 항목을 구분합니다. 5. **Submit(**제출**)**을 클릭합니다.

변경 후	수행해야 할 작업
한 명의 발신자에 대해 여러 수신자 추가	1. **View by: Sender(**보기 기준**:** 발신자**)**를 선택합니다. 2. **Add(**추가**)**를 클릭하거나, 발신자에 대해 **Edit(**수정**)**을 클릭합니다. 3. 발신자 주소 또는 도메인을 입력하거나 수정합니다. 4. 수신자 이메일 주소를 입력합니다. 각 항목을 별도의 줄에 입력하거나, 쉼표로 각 항목을 구분합니다. 5. **Submit(**제출**)**을 클릭합니다.
한 명의 수신자와 관련된 모든 발신자 삭제 한 명의 발신자와 관련된 모든 수신자 삭제	1. **View by(**보기 기준**)** 옵션을 선택합니다. 2. 테이블 행 전체를 삭제하려면 휴지통 아이콘을 클릭합니다.
한 명의 수신자에 대해 개별 발신자 삭제 한 명의 발신자에 대해 개별 수신자 삭제	1. View by(보기 기준) 옵션을 선택합니다. 2. 개별 수신자 또는 발신자에 대해 **Edit(**수정**)**을 클릭합니다. 3. 텍스트 상자에서 항목을 추가 또는 제거합니다. 항목을 적어도 하나는 남겨두어야 합니다. 4. **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

관련 주제

- 허용 목록 및 차단 목록 항목의 구문 , 877 페이지
- 모든 허용 목록 및 차단 목록 지우기 , 878 페이지

허용 목록 및 차단 목록 항목의 구문

다음 형식을 사용하여 허용 목록 및 차단 목록에 발신자를 추가할 수 있습니다.

- user@domain.com
- server.domain.com
- domain.com
- [10.1.1.0]
- [ipv6:2001:DB8:1::1]
- user@[1.2.3.4]
- user@[ipv6:2001:db8::1]

동일한 항목(예: 발신자 주소 또는 도메인)을 동시에 허용 목록과 차단 목록에 모두 포함할 수는 없습니다. 그러나 어떤 도메인이 허용 목록에 있고 그 도메인에 속한 발신자 이메일 주소가 차단 목록에 포함되는 것은(또는 그 반대의 경우도) 가능하며, 두 규칙 모두 적용됩니다. 예를 들어 *example.com*이

허용 목록에 있더라도 *george@example.com*을 차단 목록에 추가할 수 있습니다. 이 경우 어플라이언스는 *example.com*에서 오는 모든 메일을 스팸 검사 없이 전달하되, *george@example.com*의 메일만 스팸으로 처리합니다.

.domain.com 구문을 사용하여 하위 도메인의 범위를 허용하거나 차단할 수는 없습니다. 그러나 *server.domain.com* 구문을 사용하여 특정 도메인을 차단하는 것은 가능합니다.

모든 허용 목록 및 차단 목록 지우기

모든 발신자와 모든 수신자를 포함하여 모든 허용 목록 및 차단 목록 항목을 삭제해야 하는 경우 허용 목록/차단 목록 백업 및 복원 , 880 페이지의 절차를 사용하여 항목이 없는 파일을 가져옵니다.

허용 목록 및 차단 목록에 대한 최종 사용자 액세스 정보

최종 사용자는 스팸 격리를 통해 허용 목록 및 차단 목록에 액세스합니다. 스팸 격리에 대한 최종 사용자 액세스를 구성하려면 최종 사용자가 웹 브라우저를 통해 스팸 격리에 액세스하도록 설정 , 883 페이지 섹션을 참조하십시오.

최종 사용자에게 스팸 격리의 URL과 그 아래에 설명(해당되는 경우)을 제공할 수 있습니다.

관련 주제

- 허용 목록에 항목 추가(최종 사용자) , 878 페이지
- 차단 목록에 발신자 추가(최종 사용자) , 879 페이지

허용 목록에 항목 추가(최종 사용자)

참고 허용 목록에 있는 발신자가 보낸 메시지 전달은 시스템에 구성된 설정에 따라 다릅니다. 허용 목록 및 차단 목록의 메시지 처리 , 874 페이지를 참조하십시오.

두 가지 방법으로 허용 목록에 발신자를 추가할 수 있습니다.

- 격리된 메시지의 발신자를 허용 목록에 추가 , 878 페이지
- 격리된 메시지 없는 허용 목록에 발신자 추가 , 879 페이지

격리된 메시지의 발신자를 허용 목록에 추가

메시지가 스팸 격리로 전송된 경우 최종 사용자는 허용 목록에 발신자를 추가할 수 있습니다.

단계 **1** Spam Quarantine(스팸 격리)을 선택합니다.

단계 **2** 드롭다운 메뉴에서 **Safelist(**허용 목록**)**를 선택하고 **Release and Add to Safelist(**릴리스한 후 허용 목록에 추가**)**를 선택합니다.

지정된 메일의 봉투 발신자 및 from 헤더 모두 허용 목록에 추가되고 릴리스된 메시지는 대상 대기열로 직접 이동하며, 이메일 파이프라인에서 추가 작업 대기열 처리를 건너뜁니다.

격리된 메시지 없는 허용 목록에 발신자 추가

단계 **1** 브라우저를 통해 스팸 격리에 액세스합니다.

단계 **2** 페이지의 오른쪽 상단에 있는 **Options(**옵션**)** 드롭다운 메뉴를 선택합니다.

단계 **3** **Safelist(**허용 목록**)**를 선택합니다.

단계 **4** Safelist(허용 목록) 대화 상자에서 이메일 주소 또는 도메인을 입력합니다. 쉼표로 구분하여 여러 도메인 및 이메일 주소를 입력할 수 있습니다.

단계 **5** **Add to List(**목록에 추가**)**를 클릭합니다.

차단 목록에 발신자 추가(최종 사용자)

차단 목록의 발신자가 보낸 메시지는 관리자가 정의한 허용 목록/차단 목록 작업 설정에 따라 거부되거나 격리됩니다.

참고 차단 목록 항목은 이 절차를 사용해서만 추가할 수 있습니다.

단계 **1** 스팸 격리에 로그인합니다.

단계 **2** 페이지의 오른쪽 상단에 있는 **Options(**옵션**)** 드롭다운 메뉴에서 **Blocklist(**차단 목록**)**를 선택합니다.

단계 **3** 차단 목록에 추가할 도메인 또는 이메일 주소를 입력합니다. 쉼표로 구분하여 여러 도메인 및 이메일 주소를 입력할 수 있습니다.

단계 **4** **Add to List(**목록에 추가**)**를 클릭합니다.

여러 **Email Security Appliance**에서 허용 목록 또는 차단 목록 동기화 **(Security Management Appliance** 없이 구축**)**

Security Management Appliance 없이 여러 Email Security Appliance를 사용하는 경우 서로 다른 Email Security Appliance 간에 허용 목록/차단 목록 및 해당 구성 설정을 수동으로 동기화해야 할 수 있습니다.

허용 목록/차단 목록 백업 및 복원 , 880 페이지의 절차를 사용하여 .csv 파일 내보내기 및 가져오기를 수행한 다음, FTP를 사용하여 파일을 업로드 및 다운로드할 수 있습니다.

허용 목록/차단 목록 백업 및 복원

어플라이언스를 업그레이드하거나 설치 마법사를 실행하기 전에 허용 목록/차단 목록 데이터베이스를 백업해야 합니다. 허용 목록/차단 목록 정보는 어플라이언스 구성 설정을 포함하는 기본 XML 구성 파일에 포함되지 않습니다.

또한 여러 Email Security Appliance를 동기화하려면 이 절차를 사용하여 허용 목록/차단 목록의 복사본을 저장할 수 있습니다.

단계 **1** **System Administration**(시스템 관리) > **Configuration File**(구성 파일)을 선택합니다.

단계 **2** **End-User Safelist/Blocklist Database (Spam Quarantine)**(최종 사용자 허용 목록/차단 목록 데이터베이스(스팸 격리)) 섹션으로 스크롤합니다.

변경 후	수행해야 할 작업
허용 목록/차단 목록 내보내기	.csv 파일의 경로 및 파일 이름을 확인하고 필요한 대로 수정합니다. **Backup Now**(지금 백업)를 클릭합니다. 어플라이언스에서는 다음 명명 규칙을 사용하여 .csv 파일을 /configuration 디렉터리에 저장합니다. *slbl<serial number><timestamp>.csv*
허용 목록/차단 목록 가져오기	주의 이 프로세스는 모든 사용자에 대한 허용 목록 및 차단 목록에 있는 모든 기존 항목을 덮어씁니다. **Select File to Restore**(복원할 파일 선택)를 클릭합니다. configuration 디렉터리의 파일 목록에서 원하는 파일을 선택합니다. 복원할 허용 목록/차단 목록 백업 파일을 선택합니다. **Restore**(복원)를 클릭합니다.

허용 목록 및 차단 목록 문제 해결

허용 목록 및 차단 목록의 문제를 해결하려면 로그 파일 또는 시스템 알림을 볼 수 있습니다.

허용 목록/차단 목록 설정 때문에 이메일이 차단되면 ISQ_log 파일 또는 antispam 로그 파일에 작업이 기록됩니다. 허용 목록에 있는 이메일은 *X-SLBL-Result-Safelist* 헤더와 함께 허용 목록 항목으로 표시됩니다. 차단 목록에 있는 이메일은 *X-SLBL-Result-Blocklist* 헤더와 함께 차단 목록 항목으로 표시됩니다.

데이터베이스가 생성되거나 업데이트될 때 또는 데이터베이스를 수정하거나 허용 목록/차단 목록 프로세스를 실행하는 동안 오류가 발생하는 경우 알림이 전송됩니다.

알림에 대한 자세한 내용은 알림, 962 페이지 섹션을 참조하십시오.

로그 파일에 대한 자세한 내용은 로깅, 1053 페이지를 참조하십시오.

관련 주제

- 허용 목록 발신자의 메시지가 전달되지 않음 , 881 페이지

허용 목록 발신자의 메시지가 전달되지 않음

문제

허용 목록 발신자의 메시지가 전달되지 않았습니다.

솔루션

가능한 원인

- 악성코드 또는 콘텐츠 위반 때문에 메시지가 삭제되었습니다. 허용 목록 및 차단 목록의 메시지 처리 , 874 페이지를 참조하십시오.
- 여러 어플라이언스가 있고 발신자가 최근에 허용 목록에 추가된 경우, 메시지가 처리된 시점에 허용 목록/차단 목록이 동기화되지 않았을 수 있습니다. 외부 스팸 격리 및 허용 목록/차단 목록 , 875 페이지 및 여러 Email Security Appliance에서 허용 목록 또는 차단 목록 동기화(Security Management Appliance 없이 구축) , 879 페이지를 참조하십시오.

최종 사용자에 대한 스팸 관리 기능 구성

변경 후	확인
최종 사용자의 스팸 관리 기능 액세스에 대한 여러 인증 방법의 이점과 한계를 이해합니다.	스팸 격리에 대한 최종 사용자 액세스 구성 , 884 페이지 및 하위 섹션
최종 사용자가 브라우저를 통해 직접 스팸 격리에 액세스하도록 허용합니다.	스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 882 페이지
사용자에게 주소가 지정된 메시지가 스팸 격리로 라우팅될 때 해당 사용자에게 알림을 전송합니다. 스팸 격리에 액세스하기 위한 링크를 알림에 포함할 수 있습니다.	최종 사용자에게 격리된 메시지에 대해 알리기 , 886 페이지
사용자가 안전하다고 생각하는 발신자 및 스팸이나 기타 원치 않는 메일을 전송한다고 생각하는 발신자의 이메일 주소와 도메인을 지정하도록 허용합니다.	허용 목록 및 차단 목록을 사용하여 발신자 기준으로 이메일 전달 제어 , 873 페이지

관련 주제

- 스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 882 페이지
- 최종 사용자가 웹 브라우저를 통해 스팸 격리에 액세스하도록 설정 , 883 페이지
- 최종 사용자에게 격리된 메시지에 대해 알리기 , 886 페이지

스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션

참고 사서함 인증을 사용하는 경우 사용자는 이메일 별칭으로 주소가 지정된 메시지를 볼 수 없습니다.

엔드 유저 스팸 격리 액세스의 경우	수행해야 할 작업
웹 브라우저를 통해 직접, 인증 필요 및 알림의 링크를 통해, 인증 필요	1. End User Quarantine Access(엔드 유저 격리 액세스) 설정에서 **LDAP, SAML 2.0** 또는 **Mailbox (IMAP/POP)**(사서함 **(IMAP/POP))**를 선택합니다. 2. Spam Notifications(스팸 알림) 설정에서 **Enable login without credentials for quarantine access**(격리 액세스를 위한 자격 증명 없이 로그인 활성화)의 선택을 취소합니다.
웹 브라우저를 통해 직접, 인증 필요 및 알림의 링크를 통해, 인증 필요 없음	1. End User Quarantine Access(엔드 유저 격리 액세스) 설정에서 **LDAP, SAML 2.0** 또는 **Mailbox (IMAP/POP)**(사서함 **(IMAP/POP))**를 선택합니다. 2. Spam Notifications(스팸 알림) 설정에서 **Enable login without credentials for quarantine access**(격리 액세스를 위한 자격 증명 없이 로그인 활성화)를 선택합니다.
알림의 링크를 통해서만, 인증 필요 없음	End User Quarantine Access(최종 사용자 격리 액세스) 설정에서 인증 방법으로 **None**(없음)을 선택합니다.
액세스 없음	End User Quarantine Access(최종 사용자 격리 액세스) 설정에서 **Enable End-User Quarantine Access**(최종 사용자 격리 액세스 활성화)의 선택을 취소합니다.

관련 주제

- LDAP 인증 프로세스 , 882 페이지
- 스팸 격리에 대한 최종 사용자 액세스 구성 , 884 페이지
- 최종 사용자에게 격리된 메시지에 대해 알리기 , 886 페이지
- 스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 882 페이지
- 허용 목록 및 차단 목록에 대한 최종 사용자 액세스 정보 , 878 페이지

LDAP 인증 프로세스

1. 사용자가 웹 UI 로그인 페이지에 자신의 사용자 이름 및 암호를 입력합니다.
2. 익명 검색을 수행하여 또는 지정된 "서버 로그인" DN 및 암호가 있는 인증된 사용자로서 스팸 격리가 지정된 LDAP 서버에 연결합니다. Active Directory의 경우 일반적으로 "전역 카탈로그 포트"(6000s에 있음)에서 서버를 연결하거나, 검색을 수행하기 위해 스팸 격리가 바인딩할 수 있는 권한이 낮은 LDAP 사용자를 만들어야 합니다.

3. 그러면 스팸 격리는 지정된 BaseDN 및 쿼리 문자열을 사용하여 사용자를 검색합니다. 사용자의 LDAP 레코드가 발견되면 스팸 격리는 해당 레코드의 DN을 추출하고, 사용자가 원래 입력한 사용자 레코드의 DN 및 암호를 사용하여 디렉터리에 바인딩하려고 시도합니다. 암호 확인이 성공하면 사용자가 적절하게 인증되지만, 스팸 격리는 여전히 해당 사용자에게 어떤 사서함의 내용을 보여줄지를 결정해야 합니다.
4. 메시지는 수신자의 봉투 주소를 사용하여 스팸 격리에 저장됩니다. LDAP에 대해 사용자의 암호가 검증되면 스팸 격리는 LDAP 레코드에서 "기본 메일 특성"을 검색하여 사용자에게 어떤 격리 메시지를 보여줄지를 결정합니다. "기본 이메일 특성"은 여러 이메일 주소를 포함할 수 있으며, 이러한 주소는 인증된 사용자에 대해 격리에서 어떤 봉투 주소를 표시해야 할지를 결정하는 데 사용됩니다.

관련 주제

- 스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 882 페이지

IMAP/POP 인증 프로세스

1. 메일 서버 구성에 따라 사용자는 웹 UI 로그인 페이지에 사용자 이름(joe) 또는 이메일 주소(joe@example.com) 및 암호를 입력합니다. 전체 이메일 주소를 입력해야 할지 사용자 이름만 입력하면 될지를 사용자에게 알려주기 위해 로그인 페이지 메시지를 수정할 수 있습니다(스팸 격리에 대한 최종 사용자 액세스 구성 , 884 페이지 참조).
2. 스팸 격리는 IMAP 또는 POP 서버에 연결하고, 입력된 로그인(사용자 이름 또는 이메일 주소) 및 암호를 사용하여 IMAP/POP 서버에 로그인하려고 시도합니다. 암호가 수락되면 사용자는 인증된 것으로 간주되며, IMAP/POP 서버에서 스팸 격리가 즉시 로그아웃됩니다.
3. 사용자가 인증되면 스팸 격리는 이메일 주소를 기반으로 사용자의 이메일을 나열합니다.
   - 베어(bare) 사용자 이름(예: joe)에 추가할 도메인을 지정하도록 스팸 격리를 구성한 경우 해당 도메인이 추가되며 격리에서 일치하는 봉투를 검색하는 데 인증된 이메일 주소가 사용됩니다.
   - 그렇지 않은 경우 스팸 격리는 입력된 이메일 주소를 사용하여 일치하는 봉투를 검색합니다.

IMAP에 대한 자세한 내용은 University of Washington 웹사이트를 참조하십시오.

http://www.washington.edu/imap/

최종 사용자가 웹 브라우저를 통해 스팸 격리에 액세스하도록 설정

프로시저

	명령 또는 동작	목적
단계 **1**	최종 사용자의 스팸 관리 기능 액세스에 대한 여러 인증 방법의 이점과 한계를 이해합니다.	*Cisco Content Security Management Appliance* 설명서에서 *SAML 2.0*을 사용하는 *SSO* 섹션을 참조하십시오.
단계 **2**	LDAP를 사용하여 엔드 유저를 인증하려면 **System Administration**(시스템 관리) **> LDAP > LDAP Server Profile**(**LDAP** 서버 프로필) 페이지의 **Spam Quarantine**	

	명령 또는 동작	목적
	End-User Authentication Query(스팸 격리 엔드 유저 인증 쿼리) 설정을 비롯한 LDAP 서버 프로필을 구성합니다. 예제: `If you will authenticate end users using SAML 2.0 (SSO), configure the settings on the **System Administration** > **SAML** page.`	
단계 **3**	스팸 격리에 대한 최종 사용자 액세스를 구성합니다.	스팸 격리에 대한 최종 사용자 액세스 구성 , 884 페이지
단계 **4**	스팸 격리에 대한 최종 사용자 액세스용 URL을 결정합니다.	스팸 격리에 대한 최종 사용자 액세스용 URL 결정, 885 페이지

다음에 수행할 작업

관련 주제

- 스팸 격리에 대한 최종 사용자 액세스 구성 , 884 페이지
- 스팸 격리에 대한 최종 사용자 액세스용 URL 결정, 885 페이지
- 최종 사용자에게 표시할 메시지 , 885 페이지

스팸 격리에 대한 최종 사용자 액세스 구성

최종 사용자 액세스의 활성화 여부와 상관없이 관리 사용자는 스팸 격리에 액세스할 수 있습니다.

시작하기 전에

스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 882 페이지의 요구 사항을 참조하십시오.

단계 **1** **Monitor**(모니터) **>Spam Quarantine**(스팸 격리)을 선택합니다.

단계 **2** Spam Quarantine(스팸 격리) 섹션의 Quarantine Name(격리 이름) 열에서 **Spam Quarantine**(스팸 격리) 링크를 클릭합니다.

단계 **3** **End-User Quarantine Access**(최종 사용자 격리 액세스) 섹션으로 스크롤합니다.

단계 **4** **Enable End-User Quarantine Access**(최종 사용자 격리 액세스 활성화)를 선택합니다.

단계 **5** 최종 사용자가 격리된 메시지를 보려고 할 때 이들을 인증하는 데 사용할 방법을 지정합니다.

선택 옵션	추가 정보
None	—

선택 옵션	추가 정보
Mailbox(IMAP/POP)	인증에 사용할 LDAP 디렉터리가 없는 사이트의 경우 격리는 사서함이 있는 표준 기반 IMAP 또는 POP 서버에 대해 이메일 주소와 암호를 검증할 수 있습니다. 스팸 격리에 로그인할 때 엔드 유저는 전체 이메일 주소 및 사서함 암호를 입력합니다. POP 서버가 배너에서 APOP 지원을 광고하는 경우 보안상의 이유로(즉, 암호를 암호화 없이 전송하지 않도록) Cisco 어플라이언스는 APOP만 사용합니다. APOP가 일부 또는 전체 사용자에 대해 지원되지 않으면 APOP를 광고하지 않도록 POP 서버를 다시 구성해야 합니다. SSL을 사용하도록 서버를 구성한 경우 SSL을 선택합니다. 사용자가 사용자 이름만 입력하는 경우 자동으로 이메일 주소를 완성하기 위해 추가할 도메인을 지정할 수 있습니다. "인증되지 않은 사용자 이름에 도메인 추가"에 로그인하는 사용자를 위한 봉투의 도메인을 입력합니다.
LDAP	이 항목의 '시작하기 전에' 섹션에서 참조하는 섹션에 설명된 대로 LDAP 설정을 구성합니다.
SAML 2.0	스팸 격리에 대해 Single Sign-On을 활성화합니다. 이 옵션을 사용하기 전에 Management Appliance(관리 어플라이언스) > System Administration(시스템 관리) > SAML 페이지에서 모든 설정을 구성했는지 확인입니다. *Cisco Content Security Management Appliance* 설명서에서 *SAML 2.0*을 사용하는 *SSO* 섹션을 참조하십시오.

단계 **6** 메시지가 릴리스되기 전에 메시지 본문을 표시할지 여부를 지정합니다.

이 확인란을 선택하면 사용자는 스팸 격리 페이지를 통해 메시지 본문을 볼 수 없습니다. 격리된 메시지의 본문을 보려면 사용자는 메시지를 릴리스하고 각자의 메일 애플리케이션(예: Microsoft Outlook)을 이용해야 합니다. 정책 및 규정 준수에 이 기능을 사용할 수 있습니다(예: 규정에서 모든 검토한 이메일을 보관하도록 요구하는 경우).

단계 **7** 변경 사항을 제출 및 커밋합니다.

스팸 격리에 대한 최종 사용자 액세스용 **URL** 결정

최종 사용자가 스팸 격리에 직접 액세스하기 위해 사용할 수 있는 URL은 시스템의 호스트 이름 및 격리가 활성화된 IP 인터페이스에 구성된 설정(HTTP/S 및 포트 번호)으로 만들어집니다. 예:
`HTTP://mail3.example.com:82`

최종 사용자에게 표시할 메시지

일반적으로 최종 사용자는 스팸 격리에서 자신의 메시지만 볼 수 있습니다.

액세스 방법(알림을 통해 또는 웹 브라우저를 통해 직접) 및 인증 방법(LDAP 또는 IMAP/POP)에 따라 사용자는 스팸 격리에서 여러 이메일 주소의 메일을 볼 수 있습니다.

LDAP 인증이 사용될 때 Primary Email(기본 이메일) 특성에 LDAP 디렉터리의 여러 값이 포함되어 있으면 그러한 모든 값(주소)이 사용자와 연결됩니다. 따라서 LDAP 디렉터리의 최종 사용자와 연결된 모든 이메일 주소로 지정된 격리된 메시지가 격리에 표시됩니다.

인증 방법이 IMAP/POP인 경우 또는 사용자가 알림을 통해 직접 격리에 액세스하는 경우 격리에는 해당 사용자의 이메일 주소(또는 알림이 전송된 주소)에 대한 메시지만 표시됩니다.

사용자가 구성원으로 속해 있는 별칭으로 전송되는 메시지에 대한 자세한 내용은 수신자 이메일 메일 목록 별칭 및 스팸 알림 , 887 페이지 섹션을 참조하십시오.

관련 주제

- 스팸 격리에 대한 최종 사용자 액세스 구성 , 884 페이지
- 수신자 이메일 메일 목록 별칭 및 스팸 알림 , 887 페이지

최종 사용자에게 격리된 메시지에 대해 알리기

스팸 격리에 스팸 메시지 및 의심스런 스팸 메시지가 있는 일부 또는 전체 사용자에게 알림 이메일을 전송하도록 시스템을 구성할 수 있습니다.

기본적으로 스팸 알림은 사용자의 격리된 메시지를 나열합니다. 또한 알림에 스팸 격리에서 격리된 메시지를 보기 위해 사용자가 클릭할 수 있는 링크를 포함할 수 있습니다. 이러한 링크는 만료되지 않습니다. 사용자는 격리된 메시지를 보고 이를 받은 편지함으로 전달할지 아니면 삭제할지를 결정할 수 있습니다.

참고 클러스터 구성에서, 시스템 레벨에서만 알림을 수신할 사용자를 선택할 수 있습니다.

시작하기 전에

- 최종 사용자는 알림에 나열된 메시지를 관리하려면 스팸 격리에 액세스할 수 있어야 합니다. 스팸 격리에 대한 최종 사용자 액세스 구성 , 884 페이지를 참조하십시오.
- 알림을 사용하여 스팸을 관리하기 위한 인증 옵션을 이해합니다. 스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 882 페이지를 참조하십시오.
- 최종 사용자가 여러 별칭으로 이메일을 받는 경우 수신자 이메일 메일 목록 별칭 및 스팸 알림 , 887 페이지 섹션을 참조하십시오.

단계 **1** **Monitor(**모니터**) >Spam Quarantine(**스팸 격리**)**을 선택합니다.

단계 **2** Spam Quarantine(스팸 격리) 섹션의 Quarantine Name(격리 이름) 열에서 **Spam Quarantine(**스팸 격리**)** 링크를 클릭합니다.

단계 **3** **Spam Notifications(**스팸 알림**)** 섹션으로 스크롤합니다.

단계 **4** **Enable Spam Notification(**스팸 알림 활성화**)**을 선택합니다.

단계 **5** 옵션을 지정합니다.

메시지 본문을 맞춤화하려면

a) (선택 사항) 기본 텍스트 및 변수를 맞춤화합니다.

변수를 삽입하려면 삽입할 위치에 커서를 두고 오른쪽의 Message Variables(메시지 변수) 목록에서 변수의 이름을 클릭합니다. 또는 변수를 입력합니다.

다음 메시지 변수는 특정 최종 사용자에 대한 실제 값으로 확장됩니다.

- 새 메시지 개수(%new_message_count%) - 사용자가 마지막으로 로그인한 이후 새 메시지 수입니다.
- 총 메시지 개수(%total_message_count%) - 사용자에 대한 스팸 격리에 있는 메시지 수입니다.
- 메시지 만료까지 남은 일수(%days_until_expire%)
- 격리 **URL**(%quarantine_url%) - 격리에 로그인하여 메시지를 보기 위한 URL입니다.
- 사용자 이름(%username%)
- 새 메시지 테이블(%new_quarantine_messages%) - 사용자의 새로 격리된 메시지 목록으로, 발신자, 메시지 제목, 날짜 및 메시지를 릴리스할 링크를 보여줍니다. 사용자가 메시지 제목을 클릭하여 스팸 격리의 메시지를 봅니다.
- 제목이 없는 새 메시지 테이블(%new_quarantine_messages_no_subject%) - 새 메시지 테이블과 유사하지만 각 메시지의 제목 대신 "View Message(메시지 보기)" 링크만 표시됩니다.

b) 이 페이지의 End User Quarantine Access(최종 사용자 격리 액세스) 섹션에서 인증 방법을 활성화한 경우

- 사용자가 알림의 링크를 클릭하여 액세스할 때 자동으로 스팸 격리에 로그인되도록 하려면 **Enable login without credentials for quarantine access(**격리 액세스를 위한 자격 증명 없이 로그인 활성화**)**를 선택합니다. 최종 사용자는 알림의 "Release" 링크를 클릭하여 간단하게 메시지를 릴리스할 수 있습니다.
- 사용자가 알림의 링크를 클릭하여 액세스할 때 스팸 격리에 로그인하도록 요구하려면 이 옵션의 선택을 취소합니다. 최종 사용자는 알림의 "Release" 링크를 클릭하여 간단하게 메시지를 릴리스할 수 없습니다.

c) 메시지가 원하는 모습인지 확인하려면 **Preview Message(**메시지 미리 보기**)**를 클릭합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

최종 사용자가 이러한 알림을 받는지 확인하려면, 메일 애플리케이션(예: Microsoft Outlook 또는 Mozilla Thunderbird)의 정크 메일 설정에서 "화이트리스트"에 스팸 격리 알림 이메일에 대한 From: 주소를 추가하도록 권장할 수 있습니다.

관련 주제

- 수신자 이메일 메일 목록 별칭 및 스팸 알림 , 887 페이지
- 알림 테스트, 888 페이지
- 스팸 알림 문제 해결 , 888 페이지

수신자 이메일 메일 목록 별칭 및 스팸 알림

메일 목록 및 기타 별칭을 포함하여 격리된 이메일이 있는 각 봉투 수신자에게 알림이 전송됩니다. 각 메일 목록은 단일 digest를 수신합니다. 메일 목록으로 알림을 전송하면 해당 목록의 모든 구독자가 알림을 수신합니다. 여러 이메일 별칭에 속한 사용자, 알림을 수신하는 LDAP 그룹에 속한 사용자

또는 여러 이메일 주소를 사용하는 사용자는 여러 스팸 알림을 받을 수 있습니다. 다음 표에서는 사용자가 여러 알림을 받을 수 있는 상황의 예를 보여줍니다.

표 ***83:*** 주소/별칭당 알림 수

사용자	이메일 주소	별명	알림
Sam	sam@example.com	—	1
Mary	mary@example.com	dev@example.com qa@example.com pm@example.com	4
Joe	joe@example.com, admin@example.com	hr@example.com	3

LDAP 인증을 사용하는 경우 메일 목록 별칭으로 알림을 전송하지 않도록 선택할 수 있습니다. 메일 목록 별칭에 스팸 알림을 전송하도록 선택하는 경우 여러 알림의 발생을 어느 정도 막을 수 있습니다. 스팸 격리 별칭 통합 쿼리, 778 페이지을 참조하십시오.

어플라이언스가 이메일 알림에 대해 스팸 격리 별칭 통합을 사용하지 않는 한, 알림의 링크를 클릭하여 스팸 격리에 액세스하는 사용자는 자신이 가지고 있을 수 있는 다른 별칭에 대한 격리된 메시지를 볼 수 없습니다. 어플라이언스에 의한 처리 이후 확장되는 배포 목록으로 알림이 전송된 경우 여러 수신자가 해당 목록에 대한 동일한 격리에 액세스할 수 있습니다.

즉, 모든 메일 목록 구독자가 알림을 수신하며 격리에 로그인하여 메시지를 릴리스 또는 삭제할 수 있습니다. 이 경우 알림에 나와 있는 메시지를 보기 위해 격리를 방문하는 최종 사용자는 해당 메시지가 이미 다른 사용자에 의해 삭제된 것을 발견할 수 있습니다.

참고 LDAP를 사용하지 않으며 최종 사용자가 여러 이메일 알림을 받지 않도록 하려면, 알림을 비활성화하고 대신 최종 사용자가 격리에 직접 액세스하여 LDAP 또는 POP/IMAP를 통해 인증을 받도록 할 수 있습니다.

알림 테스트

테스트 메일 정책을 구성하고 단일 사용자에 대해서만 스팸을 격리하여 알림을 테스트할 수 있습니다. 그런 다음 스팸 격리 알림 설정을 구성합니다. **Enable Spam Notification(**스팸 알림 활성화**)** 확인란을 선택하고 **Enable End-User Quarantine Access(**최종 사용자 격리 액세스 활성화**)**를 선택하지 않습니다. 그러면 **Deliver Bounced Messages To(**반송 메시지 전달**)** 필드에 구성된 관리자에게만 격리의 새 스팸에 대한 알림이 제공됩니다.

스팸 알림 문제 해결

관련 주제

- 사용자가 여러 알림 수신 , 889 페이지

- 수신자가 알림을 수신하지 못함 , 889 페이지
- 사용자가 여러 알림 수신 , 889 페이지
- 수신자가 알림을 수신하지 못함 , 889 페이지

사용자가 여러 알림 수신

문제

한 사용자가 단일 메시지에 대해 여러 스팸 알림을 수신합니다.

솔루션

가능한 원인

- 사용자가 여러 이메일 주소를 가지고 있고 스팸 메시지가 그러한 주소 중 둘 이상으로 전송되었습니다.
- 사용자가 스팸 메시지를 수신한 둘 이상의 이메일 별칭에 속한 구성원입니다. 중복을 최소화하는 방법에 대한 자세한 내용은 수신자 이메일 메일 목록 별칭 및 스팸 알림 , 887 페이지 섹션을 참조하십시오.

수신자가 알림을 수신하지 못함

문제

수신자가 알림을 수신하지 못합니다.

솔루션

- 알림이 스팸 수신자 대신 "Deliver Bounce Messages To(반송 메시지 전달):" 주소로 전송되고 있다면, 이는 스팸 알림은 활성화되었지만 스팸 격리 액세스는 활성화되지 않았음을 나타냅니다. 스팸 관리 기능에 액세스하는 최종 사용자를 위한 인증 옵션 , 882 페이지를 참조하십시오.
- 사용자에게 이메일 클라이언트의 정크 메일 설정을 확인하도록 안내합니다.

스팸 격리의 메시지 관리

이 섹션에서는 로컬 또는 외부 스팸 격리의 메시지로 작업하는 방법에 대해 설명합니다.

관리 사용자는 스팸 격리의 모든 메시지를 보고 관리할 수 있습니다.

관련 주제

- 스팸 격리에 액세스(관리 사용자), 890 페이지
- 스팸 격리에서 메시지 검색, 890 페이지
- 스팸 격리의 메시지 보기, 891 페이지
- 스팸 격리의 메시지 전달, 891 페이지
- 스팸 격리에서 메시지 삭제, 891 페이지

스팸 격리에 액세스(관리 사용자)

관리 사용자는 스팸 격리의 모든 메시지를 보고 관리할 수 있습니다.

스팸 격리에 액세스(관리 사용자)

관리 사용자는 스팸 격리의 모든 메시지를 보고 관리할 수 있습니다.

Monitor(모니터) > **Spam Quarantine**(스팸 격리)을 선택한 다음 Messages(메시지) 열에서 숫자를 클릭합니다.

스팸 격리에서 메시지 검색

단계 **1** 봉투 수신자를 지정합니다.

참고 부분 주소를 입력할 수 있습니다.

단계 **2** 검색 결과가 입력한 수신자와 정확히 일치해야 하는지, 또는 검색 결과가 입력한 항목을 포함해야 하는지, 입력한 항목으로 시작해야 하는지 또는 끝나야 하는지를 선택합니다.

단계 **3** 검색할 날짜 범위를 입력합니다. 날짜를 선택할 달력 아이콘을 클릭합니다.

단계 **4** From: 주소를 지정하고, 검색 결과가 입력한 항목을 포함해야 하는지, 입력한 항목으로 시작해야 하는지 또는 끝나야 하는지를 선택합니다.

단계 **5** **Search**(검색)를 클릭합니다. 검색 기준과 일치하는 메시지가 페이지의 Search(검색) 섹션 아래에 표시됩니다.

다음에 수행할 작업

관련 주제

매우 큰 메시지 컬렉션 검색, 890 페이지

매우 큰 메시지 컬렉션 검색

스팸 격리에 매우 큰 메시지 컬렉션이 있는 경우 그리고 검색 조건이 좁게 정의되지 않은 경우, 쿼리에서 정보를 반환하는 데 시간이 오래 걸리거나 시간 초과가 발생할 수도 있습니다.

검색을 다시 제출할지를 확인하는 프롬프트가 표시됩니다. 큰 규모의 검색을 여러 개 동시에 실행하면 성능이 저하될 수 있습니다.

스팸 격리의 메시지 보기

메시지 목록은 스팸 격리의 메시지를 보여줍니다. 한 번에 표시할 메시지 수를 선택할 수 있습니다. 열 제목을 클릭하여 표시를 정렬할 수 있습니다. 정렬 순서를 반대로 하려면 동일한 열을 다시 클릭합니다.

본문과 헤더를 포함하여 메시지를 보려면 메시지의 제목을 클릭합니다. Message Details(메시지 세부사항) 페이지에 메시지가 표시됩니다. 메시지의 처음 20K가 표시됩니다. 메시지가 더 길면 20K에서 잘리며, 메시지 하단에 있는 링크를 통해 메시지를 다운로드할 수 있습니다.

Message Details(메시지 세부사항) 페이지에서 메시지를 삭제하거나(**Delete** 선택) 릴리스할 수 있습니다(**Release** 선택). 메시지를 릴리스하면 메시지가 전달됩니다.

메시지에 대한 추가 세부사항을 보려면 **Message Tracking(**메시지 추적**)** 링크를 클릭합니다.

다음에 유의하십시오.

- 첨부 파일이 있는 메시지 보기

  첨부 파일이 포함된 메시지를 볼 경우 메시지 본문이 표시되고 그 뒤에 첨부 파일 목록이 표시됩니다.

- **HTML** 메시지 보기

  스팸 격리는 HTML 기반 메시지에 가깝게 렌더링하려고 시도합니다. 이미지는 표시되지 않습니다.

- 인코딩된 메시지 보기

  Base64 인코딩 메시지는 해독된 후 표시됩니다.

스팸 격리의 메시지 전달

메시지를 릴리스하여 전달하려면, 릴리스할 메시지 옆에 있는 확인란을 클릭하고 드롭다운 메뉴에서 **Release(**릴리스**)**를 선택합니다. 그런 후 **Submit(**제출**)**을 클릭합니다.

페이지에 현재 표시된 모든 메시지를 자동으로 선택하려면 머리글 행의 확인란을 클릭합니다.

릴리스된 메시지는 대상 대기열로 직접 이동하며, 이메일 파이프라인에서 추가 작업 대기열 처리를 건너뜁니다.

스팸 격리에서 메시지 삭제

일정한 시간이 지난 후 메시지를 자동으로 삭제하도록 스팸 격리를 구성할 수 있습니다. 격리가 최대 크기에 도달하면 가장 오래된 메시지를 자동으로 삭제하도록 스팸 격리를 구성할 수 있습니다. 스팸 격리에서 메시지를 수동으로 삭제할 수도 있습니다.

특정 메시지를 삭제하려면 삭제할 메시지 옆에 있는 확인란을 클릭하고 드롭다운 메뉴에서 **Delete(**삭제**)**를 선택합니다. 그런 후 **Submit(**제출**)**을 클릭합니다. 페이지에 현재 표시된 모든 메시지를 자동으로 선택하려면 머리글 행의 확인란을 클릭합니다.

스팸 격리의 모든 메시지를 삭제하려면 격리를 비활성화하고(외부 스팸 격리 비활성화 소개 , 892 페이지 참조) **Delete All Messages(**모든 메시지 삭제**)** 링크를 클릭합니다. 링크의 끝에 있는 괄호의 숫자는 스팸 격리에 있는 메시지의 수입니다.

스팸 격리에 대한 디스크 공간

기본적으로 스팸 격리의 메시지는 지정된 시간이 지나면 자동으로 삭제됩니다. 격리가 꽉 차면 오래된 스팸이 삭제됩니다.

관련 주제

- 디스크 공간 관리 , 941 페이지

외부 스팸 격리 비활성화 소개

스팸 격리를 비활성화하려면

- 비활성화된 스팸 격리에 메시지가 있으면 메시지를 모두 삭제할 수 있습니다.
- 스팸 또는 의심스런 스팸을 격리하도록 설정된 메일 정책이 메시지를 전달하도록 설정됩니다. 메일 정책을 조정해야 할 수 있습니다.
- 외부 스팸 격리를 완전히 비활성화하려면 Email Security Appliance 및 Security Management Appliance 에서 모두 비활성화합니다.

Email Security Appliance에서만 외부 스팸 격리를 비활성화하면 외부 격리 또는 해당 메시지와 데이터가 삭제되지 않습니다.

스팸 격리 기능 문제 해결

- 허용 목록 및 차단 목록 문제 해결, 880 페이지
- 스팸 알림 문제 해결 , 888 페이지
- 메시지 텍스트가 올바르게 표시되는지 확인 , 872 페이지

35 장

관리 작업 배포

이 장에는 다음 섹션이 포함되어 있습니다.

사용자 계정 작업

Cisco 어플라이언스는 사용자 어카운트를 추가하는 두 가지 방법을 제공합니다. 첫 번째는 Cisco 어플라이언스 자체에서 사용자 어카운트를 생성하는 것이고, 두 번째는 고유한 중앙 집중식 인증 시스템(LDAP 또는 RADIUS 디렉터리)을 사용하여 사용자 인증을 활성화하는 것입니다. GUI의 **System Administration(**시스템 관리**) > Users(**사용자**)** 페이지에서(또는 CLI에서 **`userconfig`** 명령을 사용하여) 외부 인증 소스에 대한 연결 및 사용자를 관리할 수 있습니다. 외부 디렉터리를 사용하여 사용자를 인증하는 방법에 대한 자세한 내용은 외부 인증, 909 페이지를 참조하십시오.

선택적으로, 다음을 통해 특정 사용자 역할에 대한 이중 인증을 활성화할 수 있습니다.

- 웹 인터페이스의 System Administration(시스템 관리) > Users(사용자) 페이지 이중 인증, 912 페이지의 내용을 참조하십시오.
- CLI의 `userconfig > twofactorauth` 명령 *AsyncOS for Cisco Email Security Appliances CLI* 참조 가이드를 참고하십시오.

시스템의 기본 사용자 계정인 admin은 모든 관리 권한을 갖습니다. admin 사용자 어카운트는 삭제할 수 없지만, 암호를 변경하거나 어카운트 잠금을 설정할 수 있습니다.

새 사용자 계정을 생성하는 경우 사전 정의된 사용자 역할 또는 사용자 지정 사용자 역할에 사용자를 할당합니다. 각 역할은 시스템에서 다른 수준의 권한을 갖습니다.

어플라이언스에서 생성할 수 있는 사용자 계정의 수에는 제한이 없지만, 시스템에 예약된 이름으로 사용자 계정을 생성할 수 없습니다. 예를 들어 “operator” 또는 “root” 이름의 사용자 계정은 생성할 수 없습니다.

사용자 역할

표 ***84:*** 사용자 역할 목록

사용자 역할	설명
admin	admin 사용자는 시스템의 기본 사용자 계정으로 모든 관리 권한을 갖습니다. 관리 사용자 어카운트가 편의상 여기에 나열되어 있지만, 이 어카운트는 사용자 역할을 통해 할당할 수 없으며 수정하거나 삭제할 수도 없습니다. 단, 암호 변경은 가능합니다. admin 사용자만 **`resetconfig`** 및 revert 명령을 실행할 수 있습니다.
Administrator(관리자)	관리자 역할의 사용자 계정은 시스템의 모든 구성 설정에 대한 모든 액세스 권한을 갖습니다. 그러나 admin 사용자만 **`resetconfig`** 및 **`revert`** 명령을 사용할 수 있습니다. 참고 AsyncOS는 여러 관리자가 GUI에서 Email Security Appliance를 동시에 구성하는 것을 지원하지 않습니다.
Technician	기사 역할의 사용자 계정은 시스템을 업그레이드하고, 어플라이언스를 재부팅하고, 기능 키를 관리할 수 있습니다. 기사는 어플라이언스를 업그레이드하기 위해 다음의 작업을 수행할 수 있습니다. • 이메일 전달 및 수신 일시 중지. • 작업 큐 및 리스너 상태 보기. • 구성 파일 저장 및 이메일 전송. • 허용 목록 및 차단 목록 백업. 기사는 이러한 목록을 복원할 수 없습니다. • 클러스터에서 어플라이언스 연결 끊기. • Cisco 기술 지원을 위한 원격 서비스 액세스 활성화 또는 비활성화. • 지원 요청 생성.

사용자 역할	설명
Operator(운영자)	운영자 역할의 사용자 계정은 다음 작업에 제한이 있습니다. • 사용자 계정 생성 또는 편집. • **resetconfig** 명령 실행. • 어플라이언스 업그레이드. • **systemsetup** 명령 실행 또는 시스템 설치 마법사 실행. • **adminaccessconfig** 명령 실행. • 일부 격리 기능 수행(격리 생성, 편집, 삭제 및 중앙 집중식 처리 포함). • 외부 인증에 LDAP를 사용하는 경우 사용자 이름 및 암호를 제외한 LDAP 서버 프로파일 설정 수정. 또한, 이 역할은 관리자 역할과 동일한 권한을 갖습니다.
게스트	게스트 역할의 사용자 계정은 상태 정보 및 보고서만 볼 수 있습니다. 게스트 역할의 사용자는 격리된 메시지에 대한 액세스가 활성화된 경우 격리된 메시지도 관리할 수 있습니다. 게스트 역할의 사용자는 메시지 추적 기능을 사용할 수 없습니다.
Read-Only Operator(읽기 전용 운영자)	읽기 전용 작업자 역할의 사용자 계정은 구성 정보를 볼 수 있습니다. 읽기 전용 작업자 역할의 사용자는 구성을 변경하고 이를 제출하여 기능 구성 방식을 확인할 수 있지만, 변경사항을 커밋할 수는 없습니다. 읽기 전용 작업자 역할의 사용자는 격리된 메시지에 대한 액세스가 활성화된 경우 격리된 메시지도 관리할 수 있습니다. 이 역할의 사용자는 다음 항목에 액세스할 수 없습니다. • 파일 시스템, FTP 또는 SCP. • 격리 생성, 수정, 삭제 또는 중앙 집중화를 위한 설정.
Help Desk User	Help Desk 사용자 역할의 사용자 계정의 작업은 다음으로 제한됩니다. • 메시지 추적. • 격리된 메시지 관리. 이 역할의 사용자는 CLI를 포함한 나머지 시스템에 액세스할 수 없습니다. 이 역할의 사용자가 메시지를 관리하려면 격리마다 액세스를 활성화해야 합니다.

사용자 역할	설명
사용자 지정 사용자 역할	사용자 지정 사용자 역할의 사용자 계정은 해당 역할에 할당된 이메일 보안 기능에만 액세스할 수 있습니다. 이러한 기능은 DLP 정책, 이메일 정책, 보고서, 격리, 로컬 메시지 추적, 암호화 프로파일 및 추적 디버깅 도구를 사용하여 구성할 수 있습니다. 사용자는 시스템 구성 기능에 액세스할 수 없으며 기능을 전역으로 활성화할 수 없습니다. 관리자만 사용자 지정 사용자 역할을 정의할 수 있습니다. 자세한 내용은 위임 관리를 위한 사용자 지정 사용자 역할 관리, 899 페이지를 참조하십시오. 참고 사용자 지정 역할에 할당된 사용자는 CLI에 액세스할 수 없습니다.

GUI에만 액세스할 수 있는 Help Desk User 역할 및 맞춤형 사용자 역할을 제외하고, 위 표에 정의된 모든 역할은 GUI와 CLI에 모두 액세스할 수 있습니다.

LDAP 디렉토리로 사용자를 인증하는 경우 개별 사용자 대신 디렉토리 그룹을 사용자 역할에 할당합니다. 디렉토리 그룹을 사용자 역할에 할당하는 경우 해당 그룹의 각 사용자는 해당 사용자 역할에 정의된 권한을 받습니다. 자세한 내용은 외부 인증, 909 페이지를 참고하십시오.

관련 주제

- 사용자 관리, 896 페이지

사용자 관리

Users(사용자) 페이지에는 사용자 이름, 전체 이름 및 사용자 유형 또는 그룹이 포함된 시스템의 기존 사용자가 나열됩니다.

Users(사용자) 페이지에서는 다음을 수행할 수 있습니다.

- 새 사용자를 추가합니다. 자세한 내용은 사용자 추가 , 897 페이지를 참고하십시오.
- 사용자를 삭제합니다. 자세한 내용은 사용자 삭제, 898 페이지를 참고하십시오.
- 사용자 암호 변경, 사용자 어카운트 잠금 및 잠금 해제 등 사용자를 수정합니다. 자세한 내용은 사용자 편집, 897 페이지의 내용을 참고하십시오.
- 사용자가 암호를 변경하도록 강제 실행합니다. 사용자가 암호를 변경하도록 강제 실행, 897 페이지의 내용을 참조하십시오.
- 로컬 계정에 대한 사용자 어카운트 및 암호 설정을 구성합니다. 자세한 내용은 제한적인 사용자 어카운트 및 암호 설정 구성, 908 페이지를 참고하십시오.
- 어플라이언스에서 LDAP 또는 RADIUS 디렉토리를 사용하여 사용자를 인증할 수 있습니다. 자세한 내용은 외부 인증, 909 페이지의 내용을 참고하십시오.
- 특정 사용자 역할에 대한 이중 인증을 활성화합니다. 자세한 내용은 이중 인증, 912 페이지의 내용을 참고하십시오.

- 비관리자가 메시지 추적의 DLP 일치 콘텐츠에 액세스할 수 있습니다. 자세한 내용은 메시지 추적 시 중요 정보의 액세스 제어, 898 페이지을 참조하십시오.

사용자 추가

시작하기 전에

- 사용하고자 하는 사용자 역할을 확인합니다.
  - 사전 정의 사용자 역할에 대한 설명은 사용자 역할 , 894 페이지를 참조하십시오.
  - 사용자 지정 역할을 생성하려면 위임 관리를 위한 사용자 지정 사용자 역할 관리, 899 페이지 항목을 참조하십시오.
- 암호 요구 사항을 지정합니다. 제한적인 사용자 어카운트 및 암호 설정 구성, 908 페이지의 내용을 참조하십시오.

단계 **1** **System Administration**(시스템 관리) > **Users**(사용자)를 선택합니다.
단계 **2** **Add User**(사용자 추가)를 클릭합니다.
단계 **3** 사용자의 로그인 이름을 입력합니다. 일부 이름은 예약되어 있습니다(예: “operator” 또는 “root”).
단계 **4** 사용자의 전체 이름을 입력합니다.
단계 **5** 사전 정의된 사용자 역할 또는 사용자 지정 사용자 역할을 선택합니다.
단계 **6** 새 암호를 생성하거나 입력합니다.
단계 **7** 변경 사항을 제출 및 커밋합니다.

사용자 편집

이 절차는 암호 등을 변경하는 데 사용합니다.

단계 **1** **System Administration**(시스템 관리) > **Users**(사용자)를 선택합니다.
단계 **2** 사용자 목록에서 사용자 이름을 클릭합니다.
단계 **3** 사용자를 변경합니다.
단계 **4** 변경 사항을 제출 및 커밋합니다.

사용자가 암호를 변경하도록 강제 실행

단계 **1** **System Administration**(시스템 관리) > **Users**(사용자)를 선택합니다.
단계 **2** 사용자 목록에서 사용자를 선택합니다.
단계 **3** **Enforce Passphrase Change**(암호 변경 적용)를 클릭합니다.
단계 **4** 사용자가 암호를 다음 로그인 시에 변경해야 할지, 또는 지정된 기간(일)이 지난 후에 변경해야 할지를 선택합니다.

단계 **5** (선택 사항) 지정된 기간 후에 강제로 암호를 변경하도록 하는 경우 암호가 만료된 후 암호를 재설정하도록 유예 기간(일)을 설정합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

사용자 삭제

단계 **1** 사용자 목록의 사용자 이름에 해당하는 휴지통 아이콘을 클릭합니다.

단계 **2** 나타나는 경고 대화 상자에서 **Delete(**삭제**)**를 클릭하여 삭제를 확인합니다.

단계 **3** 변경사항을 커밋합니다.

메시지 추적 시 중요 정보의 액세스 제어

중요 정보가 포함되어 있을 수 있는 메시지 세부 정보에 대한 관리 액세스를 제한할 수 있습니다.

- DLP(데이터 유출 방지) 정책을 위반하는 메시지에는 회사 기밀 정보 또는 개인 정보(신용 카드 번호 및 건강 기록 등)와 같은 중요 정보가 포함되어 있을 수 있습니다. 기본적으로 이러한 콘텐츠는 어플라이언스에 액세스할 수 있는 모든 사용자에게 표시됩니다.
- URL 평판 또는 카테고리에 기반한 Outbreak Filter 또는 콘텐츠 필터에 걸린 URL도 중요 정보로 간주될 수 있습니다. 기본적으로 관리자 권한이 있는 사용자만 이 콘텐츠를 볼 수 있습니다.

이러한 중요 콘텐츠는 Message Tracking(메시지 추적) 결과에 나열되는 메시지에 대한 Message Details(메시지 세부 정보) 페이지의 전용 탭에 나타납니다.

사용자 역할에 따라 관리 사용자가 이러한 탭과 해당 콘텐츠를 숨길 수 있습니다. 그러나 관리자 역할이 있는 사용자에게 이 중요 콘텐츠를 숨기는 옵션이 있음에도 관리자 역할이 있는 사용자는 언제든지 이러한 권한을 변경할 수 있으므로 중요 정보를 볼 수 있습니다.

시작하기 전에

이러한 기능에 대한 사전 요구 사항을 충족했는지 확인합니다. 메시지 추적에서 URL 세부 정보 표시 , 441 페이지를 참조하십시오.

단계 **1** **System Administration(**시스템 관리**) > Users(**사용자**)** 페이지로 이동합니다.

단계 **2** **Access to Sensitive Information in Message Tracking(**메시지 추적 시 중요 정보의 액세스**)**아래에서 **Edit Settings(**설정 수정**)**을 클릭합니다.

단계 **3** 각 유형의 중요 정보에 대한 액세스를 허용할 역할을 선택합니다.

메시지 추적에 액세스할 수 없는 사용자 지정 역할은 이 정보를 볼 수 없으므로 해당 정보 목록이 표시되지 않습니다.

단계 **4** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- 메시지 추적 세부 정보 , 842 페이지
- 메시지 추적에서 민감한 DLP 데이터 표시 , 517 페이지
- 메시지 추적에서 URL 세부 정보 표시 , 441 페이지

위임 관리를 위한 사용자 지정 사용자 역할 관리

맞춤형 사용자 역할을 설계하고 조직 내 사용자 역할에 따라 사용자에게 특정 책임을 위임할 수 있습니다. 위임 관리자는 자신이 담당하는 이메일 보안 기능에만 액세스할 수 있으며 자신의 역할과 관련 없는 시스템 구성 기능에는 액세스할 수 없습니다. 위임 관리자는 사전 정의된 관리자, 운영자 및 Help Desk 사용자 역할보다 어플라이언스의 이메일 보안 기능에 대한 사용자 액세스를 더 유연한 방식으로 제어할 수 있습니다.

예를 들어 Email Security Appliance에서 특정 도메인에 대한 메일 정책 관리를 책임지는 사용자가 있는데, 이들이 시스템 관리 및 보안 서비스 컨피그레이션 기능(사전 정의된 Administrator 및 Operator 역할이 허용)에는 액세스하지 못하게 하고 싶을 수 있습니다. 메일 정책 관리자가 자신이 관리하는 메일 정책에 이러한 사용자 액세스 권한을 부여할 수 있도록 사용자 지정 사용자 역할을 생성할 수 있습니다. 또한, 메시지 추적 및 정책 격리 등의 정책으로 처리되는 메시지를 관리하는 데 사용하는 기타 이메일 보안 기능에 대한 액세스도 부여할 수 있습니다.

맞춤형 사용자 역할을 정의하고 자신이 책임지는 이메일 보안 기능(예: 메일 정책, RSA 이메일 ELP 정책, 이메일 보고서 및 격리)을 관리하려면 GUI의 **System Administration(**시스템 관리**) > User Roles(**사용자 역할**)** 페이지(또는 CLI의 **`userconfig -> role`** 명령)를 사용합니다. 위임 관리자가 관리할 수 있는 이메일 보안 기능의 전체 목록은 액세스 권한 할당, 900 페이지를 참조하십시오. **System Administration(**시스템 관리**) > Users(**사용자**)** 페이지를 사용하여 로컬 사용자 어카운트를 추가 또는 수정할 때에도 맞춤형 역할을 만들 수 있습니다. 자세한 내용은 사용자 계정 추가 시 사용자 지정 사용자 역할 정의, 905 페이지를 참조하십시오.

사용자 지정 사용자 역할을 생성할 때 해당 책임이 다른 위임 관리자의 책임과 지나치게 겹치지 않도록 확인해야 합니다. 예를 들어 여러 위임 관리자가 동일한 콘텐츠 필터를 담당하는 경우 각기 다른 메일 정책으로 콘텐츠 필터를 사용하면 한 위임 관리자가 적용한 필터 변경사항으로 인해 다른 위임 관리자가 관리하는 메일 정책에 예기치 않은 부작용이 발생할 수 있습니다.

사용자 지정 사용자 역할을 생성한 경우 다른 사용자 역할과 마찬가지로 로컬 사용자 및 외부 인증 그룹을 할당할 수 있습니다. 자세한 내용은 사용자 계정 작업, 893 페이지를 참조하십시오. 사용자 지정 역할에 할당된 사용자는 CLI에 액세스할 수 없습니다.

관련 주제

- 계정 권한 페이지, 900 페이지
- 액세스 권한 할당, 900 페이지
- 사용자 지정 사용자 역할 정의, 905 페이지
- 사용자 계정 추가 시 사용자 지정 사용자 역할 정의, 905 페이지
- 사용자 지정 사용자 역할에 대한 책임 업데이트 , 906 페이지

- 사용자 지정 사용자 역할 편집, 906 페이지
- 사용자 지정 사용자 역할 복제, 906 페이지
- 사용자 지정 사용자 역할 삭제, 907 페이지

계정 권한 페이지

위임 관리자가 어플라이언스에 로그인하면 Account Privileges(계정 권한) 페이지에는 위임 관리자가 담당하는 보안 기능의 링크 및 해당 액세스 권한에 대한 간략한 설명이 표시됩니다. 위임 관리자는 Options(옵션) 메뉴에서 계정 권한을 선택하여 이 페이지로 돌아올 수 있습니다. 위임 관리자는 또한 웹 페이지 상단에 있는 관리 메뉴를 사용하여 자신이 관리하는 기능에 액세스할 수 있습니다.

다음 그림에서는 메일 정책, 이메일 보고, 메시지 추적 및 격리에 액세스 권한이 있는 위임 관리자의 Account Privileges(어카운트 권한) 페이지를 보여줍니다.

그림 ***72:*** 위임 관리자의 계정 권한 페이지

액세스 권한 할당

사용자 지정 사용자 역할을 생성할 때 위임 관리자가 담당하는 보안 기능에 대한 액세스 수준을 정의합니다.

위임 관리자가 관리할 수 있는 보안 기능은 다음과 같습니다.

- 수신 및 발송 메일 정책과 콘텐츠 필터.
- DLP(데이터 유출 방지) 정책.
- 이메일 보고.
- 메시지 추적.
- 추적 디버깅 도구.
- 스팸, 정책, 바이러스 및 신종 바이러스 격리.
- Cisco 이메일 암호화 프로파일.

사용자 지정 사용자 역할의 액세스 수준을 정의한 이후 위임 관리자가 책임지게 될 특정 메일 정책, 콘텐츠 필터, DLP 정책, 격리 또는 암호화 프로파일을 할당합니다.

예를 들어 서로 다른 DLP 정책을 담당할 2가지 DLP 정책 관리자 역할을 생성할 수 있습니다. 한 역할은 회사 기밀 및 사용 허용과 관련된 DLP 위반을 담당하고 다른 역할은 개인 정보 보호와 관련된 DLP 위반을 관리합니다. DLP 정책 액세스 외에도 이러한 사용자 지정 사용자 역할에는 메시지 데이터를 추적하고 격리 및 보고서를 확인할 수 있는 권한을 할당할 수 있습니다. 메시지 추적을 사용하여 담당하는 정책과 관련된 DLP 위반을 검색할 수 있습니다.

User Roles(사용자 역할) 페이지의 위임 관리를 위한 사용자 지정 사용자 역할 테이블에 있는 할당된 권한의 링크를 클릭하여 사용자 지정 사용자 역할에 할당할 수 있는 책임을 볼 수 있습니다. 사용자 지정 사용자 역할에 대한 책임 업데이트 , 906 페이지를 참조하십시오.

관련 주제

- 메일 정책 및 콘텐츠 필터, 901 페이지
- DLP 정책, 902 페이지
- 이메일 보고서, 903 페이지
- Message Tracking(메시지 추적), 904 페이지
- Trace, 904 페이지
- 쿼런틴, 904 페이지
- 암호화 프로파일, 905 페이지

메일 정책 및 콘텐츠 필터

메일 정책 및 콘텐츠 필터 액세스 권한에서는 Email Security Appliance의 수신 및 발송 메일 정책 및 콘텐츠 필터에 대한 위임 관리자의 액세스 수준을 정의합니다. 특정 메일 정책 및 콘텐츠 필터를 사용자 지정 사용자 역할에 할당하여, 운영자 및 관리자와 이 역할에 속하는 위임 관리자만 메일 정책 및 콘텐츠 필터를 관리하도록 할 수 있습니다.

이 액세스 권한을 가진 모든 위임 관리자는 기본 수신 및 발송 메일 정책을 볼 수 있지만 전체 액세스 권한을 가진 경우에만 해당 정책을 편집할 수 있습니다.

액세스 권한을 가진 모든 위임 관리자는 메일 정책에 사용할 새 콘텐츠 필터를 생성할 수 있습니다. 위임 관리자가 생성한 콘텐츠 필터는 사용자 지정 사용자 역할에 할당된 다른 위임 관리자가 사용할 수 있습니다. 사용자 지정 사용자 역할에 할당되지 않은 콘텐츠 필터는 공용이며, 따라서 메일 정책 액세스 권한을 가진 모든 위임 관리자가 볼 수 있습니다. 운영자 및 관리자가 생성한 콘텐츠 필터는 기본적으로 공용입니다. 위임 관리자는 사용자 지정 사용자 역할에 할당된 메일 정책에 대한 모든 기존 콘텐츠 필터를 활성화하거나 비활성화할 수 있지만, 공용 콘텐츠 필터는 수정하거나 삭제할 수 없습니다.

위임 관리자가 자신의 메일 정책 이외의 다른 메일 정책에 사용된 콘텐츠 필터를 삭제하거나 콘텐츠 필터가 다른 사용자 지정 사용자 역할에 할당된 경우, AsyncOS는 시스템에서 콘텐츠 필터를 삭제하지 않습니다. 대신 AsyncOS는 콘텐츠 필터를 사용자 지정 사용자 역할에서 연결 해제하고 위임 관리자의 메일 정책에서 제거합니다. 다른 사용자 지정 사용자 역할 및 메일 정책에서는 그대로 콘텐츠 필터를 사용할 수 있습니다.

위임 관리자는 콘텐츠 필터에서 텍스트 리소스 또는 사전을 사용할 수 있지만, GUI의 Text Resources(텍스트 리소스) 또는 Dictionaries(사전) 페이지에 액세스하여 해당 항목을 보거나 수정할 수는 없습니다. 위임 관리자는 또한 새 텍스트 리소스 또는 사전을 생성할 수 없습니다.

발송 메일 정책에 있어 위임 관리자는 DLP 정책을 활성화하거나 비활성화할 수 있지만, DLP 정책 권한이 없으면 DLP 설정을 사용자 지정할 수 없습니다.

사용자 지정 사용자 역할에 메일 정책 및 콘텐츠 필터에 관련하여 다음의 액세스 수준을 할당할 수 있습니다.

- 액세스 없음: 위임 관리자는 Email Security Appliance의 메일 정책 및 콘텐츠 필터를 보거나 수정할 수 없습니다.
- 할당된 항목 보기, 할당된 항목 편집: 위임 관리자는 사용자 지정 사용자 역할에 할당된 메일 정책 및 콘텐츠 필터를 보거나 편집하고 새 콘텐츠 필터를 생성할 수 있습니다. 위임 관리자는 정책의 안티스팸, 안티바이러스 및 신종 바이러스 필터(Outbreak Filter) 설정을 편집할 수 있습니다. 위임 관리자는 정책의 담당 여부와 관계없이 정책에 대한 콘텐츠 필터를 활성화할 수 있으며 정책에 할당된 기존 콘텐츠 필터를 비활성화할 수 있습니다. 위임 관리자는 메일 정책의 이름 또는 발신자, 수신자 또는 그룹을 수정할 수 없습니다. 위임 관리자는 사용자 지정 사용자 역할에 할당된 메일 정책에 대한 콘텐츠 필터의 순서를 수정할 수 있습니다.
- 모든 항목 보기, 할당된 항목 편집: 위임 관리자는 어플라이언스의 모든 메일 정책 및 콘텐츠 필터를 볼 수 있지만, 사용자 지정 사용자 역할에 할당된 항목만 편집할 수 있습니다.

모든 항목 보기, 모든 항목 편집(전체 액세스): 위임 관리자는 기본 메일 정책을 비롯하여 어플라이언스의 모든 메일 정책 및 콘텐츠 필터에 대한 전체 액세스 권한을 가지며, 새 메일 정책을 생성할 수 있습니다. 위임 관리자는 발신자, 수신자 및 모든 메일 정책 그룹을 수정할 수 있습니다. 메일 정책의 순서를 바꿀 수도 있습니다.

Email Security Manager를 사용하거나 User Roles(사용자 역할) 페이지의 위임 관리를 위한 사용자 지정 사용자 역할 테이블을 사용하여 사용자 지정 사용자 역할에 개별 메일 정책 및 콘텐츠 필터를 할당할 수 있습니다.

위임 관리를 위한 사용자 지정 사용자 역할 테이블을 사용하여 메일 정책 및 콘텐츠 필터를 할당하는 방법에 대한 자세한 내용은 사용자 지정 사용자 역할에 대한 책임 업데이트 , 906 페이지 항목을 참조하십시오.

DLP 정책

DLP 정책 액세스 권한에서는 Email Security Appliance의 DLP 정책 관리자를 통해 DLP 정책에 대한 위임 관리자의 액세스 수준을 정의합니다. DLP 정책을 특정 사용자 지정 사용자 역할에 할당하여 운영자 및 관리자와 위임 관리자가 이러한 정책을 관리할 수 있습니다. DLP 액세스 권한을 가진 위임 관리자는 또한 Data Loss Prevention Global Settings(데이터 유출 방지 전역 설정) 페이지에서 DLP 구성 파일을 내보낼 수 있습니다.

위임 관리자가 메일 정책 권한도 보유하고 있는 경우 DLP 정책을 맞춤 설정할 수 있습니다. 위임 관리자는 해당 DLP 정책에 모든 맞춤형 DLP 사전을 사용할 수 있지만, 맞춤형 DLP 사전을 보거나 수정할 수는 없습니다.

맞춤형 사용자 역할에 DLP 정책과 관련하여 다음의 액세스 수준을 할당할 수 있습니다.

- **No access**(액세스 없음): 위임 관리자가 Email Security Appliance에서 DLP 정책을 보거나 수정할 수 없습니다.
- **View assigned, edit assigned**(보기 할당됨, 수정 할당됨): 위임 관리자가 DLP 정책 관리자를 사용하여 맞춤형 사용자 역할에 할당된 DLP 정책을 보고 수정할 수 있습니다. 위임 관리자는 DLP 정

책 관리자의 DLP 정책의 이름을 바꾸거나 순서를 바꿀 수 없습니다. 위임 관리자는 DLP 구성을 내보낼 수 있습니다.

- **View all, edit assigned(**모두 보기**,** 수정 할당됨**)**: 위임 관리자가 맞춤형 사용자 역할에 할당된 DLP 정책을 보고 수정할 수 있습니다. DLP 구성을 내보낼 수 있습니다. 위임 관리자는 맞춤형 사용자 역할에 할당되지 않은 모든 DLP 정책을 볼 수 있지만 수정할 수는 없습니다. 위임 관리자는 DLP 정책 관리자에서 DLP 정책 순서를 바꾸거나 정책의 이름을 바꿀 수 없습니다.
- **View all, edit all (full access)(**모두 보기**,** 모두 수정**(**완전한 액세스**))**: 위임 관리자는 새 정책 만들기를 포함하여, 어플라이언스의 모든 DLP 정책에 대한 완전한 액세스 권한을 보유합니다. 위임 관리자는 DLP 정책 관리자에서 DLP 정책의 순서를 바꿀 수 없습니다. 어플라이언스에서 사용하는 DLP 모드를 변경할 수 없습니다.

DLP 정책 관리자를 사용하거나 User Roles(사용자 역할) 페이지의 위임 관리를 위한 맞춤형 사용자 역할 테이블을 사용하여 맞춤형 사용자 역할에 개별 DLP 정책을 할당할 수 있습니다.

DLP 정책 및 DLP 정책 관리자에 대한 자세한 내용은 데이터 유출 방지, 491 페이지 항목을 참고하십시오.

Custom User Roles for Delegated Administration(위임 관리용 맞춤형 사용자 역할) 목록을 사용하여 DLP 정책을 할당하는 방법에 대한 자세한 내용은 사용자 지정 사용자 역할에 대한 책임 업데이트 , 906 페이지 항목을 참고하십시오.

이메일 보고서

이메일 보고 액세스 권한에서는 메일 정책, 콘텐츠 필터 및 DLP 정책에 대한 맞춤형 사용자 역할의 액세스 권한에 따라 위임 관리자가 볼 수 있는 보고서 및 Email Security Monitor(이메일 보안 모니터) 페이지를 정의할 수 있습니다. 할당된 정책에 대한 보고서는 필터링되지 않습니다. 위임 관리자는 자신이 담당하지 않는 메일 및 DLP 정책에 대한 보고서를 볼 수 있습니다.

사용자 지정 사용자 역할에 이메일 보고와 관련하여 다음의 액세스 수준을 할당할 수 있습니다.

- **No access(**액세스 없음**)**: 위임 관리자가 Email Security Appliance에서 보고서를 볼 수 없습니다.
- **View relevant reports(**관련 보고서 보기**)**: 위임 관리자가 메일 정책 및 콘텐츠 필터 그리고 DLP 정책 액세스 권한과 관련된 Email Security Monitor(이메일 보안 모니터) 페이지에서 보고서를 볼 수 있습니다. 메일 정책 및 콘텐츠 필터 액세스 권한을 가진 위임 관리자는 다음 Email Security Monitor(이메일 보안 모니터) 페이지를 볼 수 있습니다.
  - Overview(개요)
  - Incoming Mail(수신 메일)
  - Outgoing Destinations(발신 대상)
  - Outgoing Senders(발신 발신자)
  - Internal Users(내부 사용자)
  - Content Filters(콘텐츠 필터)
  - Virus Outbreaks(바이러스 침투)
  - 바이러스 유형
  - Archived Reports(보관된 보고서)

  DLP 정책 액세스 권한을 가진 위임 관리자는 다음 Email Security Monitor(이메일 보안 모니터) 페이지를 볼 수 있습니다.

- Overview(개요)
- DLP Incidents(DLP 인시던트)
- Archived Reports(보관된 보고서)

- **View all reports(**모든 보고서 보기**)**: 위임 관리자가 Email Security Appliance에서 모든 보고서 및 Email Security Monitor(이메일 보안 모니터) 페이지를 볼 수 있습니다.

이메일 보고 및 이메일 보안 모니터에 대한 자세한 내용은 이메일 보안 모니터 사용, 793 페이지를 참조하십시오.

Message Tracking(메시지 추적)

System Administration(시스템 관리**) > Users(**사용자**)** 페이지에서 DLP Tracking Policies(DLP 추적 정책) 옵션이 활성화되었고 맞춤형 사용자 역할에 DLP 정책 액세스 권한이 있는 경우, 메시지 추적 액세스 권한은 조직의 DLP 정책을 위반할 수 있는 메시지 내용을 포함하여 맞춤형 사용자 역할에 할당된 위임 관리자가 메시지 추적에 액세스할 수 있는지 여부를 정의합니다.

위임 관리자는 자신에게 할당된 DLP 정책에 대한 DLP 위반 사항만 검색할 수 있습니다.

메시지 추적에 대한 자세한 내용은 메시지 추적, 837 페이지를 참조하십시오.

위임 관리자가 메시지 추적에서 일치하는 DLP 콘텐츠를 볼 수 있도록 허용하는 정보에 대해서는 메시지 추적 시 중요 정보의 액세스 제어, 898 페이지 항목을 참조하십시오.

Trace

추적 액세스 권한에서는 사용자 지정 사용자 역할에 할당된 위임 관리자가 추적을 사용하여 시스템을 통과하는 메시지 흐름을 디버깅 할지 여부를 정의합니다. 액세스 권한이 있는 위임 관리자는 추적을 실행하고 생성된 모든 출력을 볼 수 있습니다. 추적 결과는 위임 관리자의 메일 또는 DLP 정책 권한에 따라 필터링되지 않습니다.

추적 사용에 대한 자세한 내용은 테스트 메시지를 사용하여 메일 플로우 디버깅: 추적, 1149 페이지를 참조하십시오.

쿼런틴

격리 액세스 권한에서는 위임 관리자가 할당된 격리를 관리할지 여부를 정의합니다. 위임 관리자는 할당된 격리에 있는 모든 메시지를 확인하고 이에 대한 작업(메시지 해제 또는 삭제)을 수행할 수 있습니다. 그러나 격리의 구성(예: 크기, 보존 기간 등)을 변경할 수 없으며 격리를 생성하거나 삭제할 수도 없습니다.

Monitor(모니터) > Quarantines(격리) 페이지 또는 User Roles(사용자 역할) 페이지의 Custom User Roles for Delegated Administration(위임 관리용 사용자 지정 사용자 역할) 테이블을 사용하여 사용자 지정 사용자 역할에 격리를 할당할 수 있습니다.

관리 사용자에게 격리 관리 작업을 할당하는 방법에 대한 자세한 내용은 메시지 처리 작업을 다른 사용자들에게 분산 , 856 페이지 및 스팸 격리에 대한 관리 사용자 액세스 구성 , 871 페이지를 참조하십시오.

위임 관리를 위한 사용자 지정 사용자 역할 목록을 사용한 격리 할당에 대한 자세한 내용은 사용자 지정 사용자 역할에 대한 책임 업데이트 , 906 페이지 항목을 참조하십시오.

암호화 프로파일

암호화 프로파일 액세스 권한에서는 콘텐츠 필터 또는 DLP 정책을 편집할 때 위임 관리자가 사용자 지정 사용자 역할에 할당된 암호화 프로파일을 사용할지 여부를 정의합니다. 암호화 프로파일은 메일 또는 DLP 정책 액세스 권한이 있어야 사용자 지정 사용자 역할에 할당할 수 있습니다. 사용자 지정 역할에 할당되지 않은 암호화 프로파일은 메일 또는 DLP 정책 권한을 가진 모든 위임 관리자가 사용할 수 있습니다. 위임 관리자는 암호화 프로파일을 보거나 수정할 수 없습니다.

Security Services(보안 서비스) > IronPort Email Encryption 페이지를 사용하여 암호화 프로필을 만들거나 수정할 때 암호화 프로필을 할당할 수 있습니다.

사용자 지정 사용자 역할 정의

GUI의 User Roles(사용자 역할) 페이지(또는 CLI의 userconfig -> role 명령)에서 새 사용자 역할을 정의하고 해당 액세스 권한을 할당합니다. User Roles(사용자 역할) 페이지에는 어플라이언스에 있는 기존 모든 사용자 지정 사용자 역할 및 각 역할에 대한 액세스 권한이 표시됩니다.

단계 **1** **System Administration(**시스템 관리**) > User Roles(**사용자 역할**)**를 선택합니다.

단계 **2** **Add User Role(**사용자 역할 추가**)**을 클릭합니다.

단계 **3** 사용자 역할의 이름을 입력합니다.

단계 **4** 사용자 역할 및 해당 권한에 대한 설명을 입력합니다.

단계 **5** 사용자 역할의 액세스 권한을 선택합니다. (각 액세스 권한 유형에 대한 자세한 내용은 액세스 권한 할당, 900 페이지를 참조하십시오.)

단계 **6** 변경 사항을 제출 및 커밋합니다.

사용자 계정 추가 시 사용자 지정 사용자 역할 정의

Email Security Appliance에서 로컬 사용자 계정을 추가하거나 수정할 때 새로운 사용자 지정 사용자 역할을 만들 수 있습니다.

사용자 계정 추가에 대한 자세한 내용은 사용자 관리, 896 페이지 항목을 참조하십시오.

단계 **1** **System Administration(**시스템 관리**) > Users(**사용자**)** 페이지로 이동합니다.

단계 **2** **Add User(**사용자 추가**)**를 클릭합니다.

단계 **3** 사용자 계정을 생성할 때 사용자 지정 역할을 선택합니다.

단계 **4** **Add Role(**역할 추가**)**을 선택합니다.

단계 **5** 새 역할의 이름을 입력합니다.

단계 **6** 새 사용자 계정을 제출합니다.

AsyncOS는 새 사용자 계정 및 사용자 지정 사용자 역할이 추가되었음을 알리는 알림을 표시합니다.

단계 **7** **System Administration(**시스템 관리 > **User Roles(**사용자 역할**)** 페이지로 이동합니다.

단계 **8** 위임 관리를 위한 사용자 지정 사용자 역할 표에서 사용자 지정 사용자 역할의 이름을 클릭합니다.

단계 **9** 사용자 역할 및 해당 권한에 대한 설명을 입력합니다.

단계 **10** 사용자 역할의 액세스 권한을 선택합니다. (각 액세스 권한 유형에 대한 자세한 내용은 액세스 권한 할당, 900 페이지를 참조하십시오.)

단계 **11** 변경 사항을 제출 및 커밋합니다.

사용자 지정 사용자 역할에 대한 책임 업데이트

단계 **1** **System Administration**(시스템 관리) > **User Roles**(사용자 역할) 페이지로 이동합니다.

단계 **2** 업데이트하려는 사용자 지정 사용자 역할의 액세스 권한의 이름을 클릭합니다.

AsyncOS는 할당된 다른 사용자 지정 사용자 역할의 이름과 함께 어플라이언스에서 사용 가능한 모든 메일 정책, 콘텐츠 필터, DLP 정책 또는 격리 목록을 표시합니다.

단계 **3** 위임 관리자에게 할당하려는 메일 정책, 콘텐츠 필터, DLP 정책 또는 격리를 선택합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

사용자 지정 사용자 역할 편집

단계 **1** **System Administration**(시스템 관리) > **User Roles**(사용자 역할) 페이지로 이동합니다.

단계 **2** 위임 관리를 위한 사용자 지정 사용자 역할 목록에서 사용자 역할의 이름을 클릭합니다.

단계 **3** 사용자 역할을 변경합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

사용자 지정 사용자 역할 복제

유사한 액세스 권한을 가진 여러 사용자 지정 사용자 역할을 생성하되 사용자 집합마다 각기 다른 책임을 할당할 수 있습니다. 예를 들어, Email Security Appliance가 여러 도메인의 메시지를 처리하는 경우, 액세스 권한은 비슷하지만 도메인을 기반으로 서로 다른 메일 정책에 대한 사용자 지정 사용자 역할을 만들 수 있습니다. 이렇게 하면 위임 관리자가 다른 위임 관리자의 책임에 영향을 주지 않으면서 도메인에 대한 메일 정책을 관리할 수 있습니다.

단계 **1** **System Administration**(시스템 관리) > **User Roles**(사용자 역할) 페이지로 이동합니다.

단계 **2** 위임 관리를 위한 사용자 지정 사용자 역할 목록에서 복제할 사용자 역할의 복제 아이콘을 클릭합니다.

단계 **3** 사용자 지정 사용자 역할의 이름을 변경합니다.

단계 **4** 새 사용자 지정 사용자 역할에 맞게 액세스 권한을 변경합니다.
단계 **5** 변경 사항을 제출 및 커밋합니다.

사용자 지정 사용자 역할 삭제

사용자 지정 역할을 삭제하면 사용자는 할당 해제 상태가 되고 어플라이언스에 액세스할 수 없습니다. 사용자 한 명 이상에게 할당된 맞춤형 사용자 역할을 삭제하더라도 경고 메시지가 발송되지 않습니다. 삭제한 사용자 지정 사용자 역할에 할당된 사용자를 다시 할당해야 합니다.

단계 **1** **System Administration**(시스템 관리) > **User Roles**(사용자 역할) 페이지로 이동합니다.
단계 **2** 위임 관리를 위한 사용자 지정 사용자 역할 목록에서 삭제할 사용자 역할의 휴지통 아이콘을 클릭합니다.
단계 **3** 나타나는 경고 대화 상자에서 **Delete**(삭제)를 클릭하여 삭제를 확인합니다.
단계 **4** 변경사항을 커밋합니다.

암호

암호 변경

관리 사용자는 GUI 상단에 있는 Options(옵션) > Change Passphrase(암호 변경) 링크를 통해 암호를 변경할 수 있습니다.

새 암호를 제출하는 즉시 로그아웃되고 로그인 화면으로 연결됩니다.

CLI에서는 passphrase 또는 passwd 명령을 사용하여 암호를 변경합니다. admin 사용자 계정의 암호를 잊은 경우 암호를 재설정하려면 고객 지원 업체에 문의하십시오.

passphrase 명령을 사용할 경우 보안을 위해 기존 암호를 입력해야 합니다.

참고 암호 변경 사항은 즉시 적용되므로 변경 사항을 커밋할 필요가 없습니다.

사용자 계정 잠금 및 잠금 해제

사용자 계정을 잠그면 로컬 사용자가 어플라이언스에 로그인할 수 없습니다. 다음 방법 중 하나로 사용자 계정을 잠글 수 있습니다.

- AsyncOS는 사용자가 Local User Account & Passphrase Settings(로컬 사용자 어카운트 및 암호 설정) 섹션에 정의된 최대 로그인 실패 횟수를 초과한 경우 사용자 어카운트를 잠급니다.
- 관리자는 System Administration(시스템 관리) > Users(사용자) 페이지를 사용하여 보안 목적으로 사용자 계정을 수동으로 잠글 수 있습니다.

AsyncOS는 사용자가 Edit User(사용자 편집) 페이지에서 사용자 계정을 확인할 때 사용자 계정을 잠근 이유를 표시합니다.

사용자 계정을 잠금 해제하려면 사용자 목록에서 사용자 이름을 클릭하여 사용자 계정을 열고 **Unlock Account(**계정 잠금 해제**)**를 클릭합니다.

로컬 사용자 계정을 수동으로 잠그려면 Users(사용자) 목록에서 사용자 이름을 클릭하여 사용자 계정을 열고 **Lock Account(**계정 잠금**)**를 클릭합니다. AsyncOS는 사용자가 어플라이언스에 로그인할 수 없다는 메시지를 표시하고 계속할지 여부를 묻습니다.

또한, 구성된 시도 횟수를 초과한 이후 사용자가 로그인에 실패하면 모든 로컬 사용자 계정이 잠기도록 구성할 수 있습니다. 자세한 내용은 제한적인 사용자 어카운트 및 암호 설정 구성, 908 페이지를 참고하십시오.

참고 admin 계정을 잠근 경우에는 직렬 통신으로 직렬 콘솔 포트에 연결하고 admin으로 로그인해야만 잠금을 해제할 수 있습니다. admin 사용자는 admin 계정이 잠긴 경우에도 항상 직렬 콘솔 포트를 사용하여 어플라이언스에 액세스할 수 있습니다. 직렬 콘솔 포트를 사용하여 어플라이언스에 액세스하는 방법에 대한 자세한 내용은 어플라이언스에 연결, 23 페이지를 참조하십시오.

제한적인 사용자 어카운트 및 암호 설정 구성

사용자 어카운트와 암호 제한을 정의하여 조직의 암호 정책을 적용할 수 있습니다. 사용자 어카운트 및 암호 제한 사항은 Cisco 어플라이언스에 정의된 로컬 사용자에 적용됩니다. 다음과 같은 설정을 구성할 수 있습니다.

- 사용자 계정 잠금**.** 사용자 계정이 잠기도록 로그인 실패 횟수를 정의할 수 있습니다
- 암호 수명 규칙**.** 사용자가 로그인한 후 암호를 변경해야 하기 전까지 암호를 유지할 수 있는 기간을 정의할 수 있습니다.
- 암호 규칙**.** 사용자가 선택할 수 있는 암호의 종류(예: 선택 문자 또는 필수 문자)를 정의할 수 있습니다.

System Administration(시스템 관리) > Users(사용자) 페이지 Local User Account and Passphrase Settings(로컬 사용자 어카운트 및 암호 설정) 섹션에서 사용자 어카운트와 암호 제한을 정의할 수 있습니다.

외부 인증

네트워크의 LDAP 또는 RADIUS 디렉터리에 사용자 정보를 저장하는 경우 외부 디렉터리를 사용하여 어플라이언스에 로그인한 사용자를 인증하도록 Cisco 어플라이언스를 구성할 수 있습니다. 인증에 외부 디렉터리를 사용하도록 어플라이언스를 설정하려면 GUI의 System Administration(시스템 관리) > Users(사용자) 페이지 또는 CLI의 userconfig 명령 및 external 하위 명령을 사용합니다.

외부 인증이 활성화된 상태에서 사용자가 Email Security Appliance에 로그인하면, 어플라이언스는 먼저 해당 사용자가 시스템 정의 "admin" 계정인지를 확인합니다. admin 계정이 아니면 어플라이언스는 첫 번째로 구성된 외부 서버를 확인하여 사용자가 그곳에 정의되어 있는지 확인합니다. 어플라이언스에서 첫 번째 외부 서버에 연결할 수 없는 경우 어플라이언스는 목록의 다음 외부 서버를 확인합니다.

LDAP 서버의 경우, 외부 서버에서 사용자 인증에 실패하면 어플라이언스는 Email Security Appliance에 정의된 로컬 사용자로서 사용자를 인증하려고 시도합니다. 사용자가 외부 서버 또는 어플라이언스에 존재하지 않거나 잘못된 암호를 입력하면 어플라이언스에 대한 액세스가 거부됩니다.

외부 RADIUS 서버에 연결할 수 없는 경우 목록의 다음 서버를 시도합니다. 모든 서버에 연결할 수 없으면 어플라이언스는 Email Security Appliance에 정의된 로컬 사용자로서 사용자를 인증하려고 시도합니다. 그러나 외부 RADIUS 서버에서 어떤 이유(예: 잘못된 암호 또는 사용자 부재)로든 사용자를 거부하는 경우 어플라이언스에 대한 액세스가 거부됩니다.

관련 주제

- LDAP 인증 사용, 909 페이지
- RADIUS 인증 활성화, 910 페이지

LDAP 인증 사용

LDAP 디렉터리를 사용하여 사용자를 인증하는 것은 물론 LDAP 그룹을 Cisco 사용자 역할에 할당할 수 있습니다. 예를 들어 IT 그룹의 사용자를 관리자 사용자 역할에 할당하고, 지원 그룹의 사용자를 Help Desk User 역할에 할당할 수 있습니다. 한 사용자가 서로 다른 사용자 역할의 여러 LDAP 그룹에 속해 있으면 AsyncOS는 해당 사용자에게 가장 제한적인 역할에 대한 권한을 부여합니다. 예를 들어 한 사용자가 Operator 권한의 그룹과 Help Desk User 권한의 그룹에 속해 있으면 AsyncOS는 해당 사용자에게 Help Desk User 역할에 대한 권한을 부여합니다.

참고 외부 사용자가 LDAP 그룹의 사용자 역할을 변경하는 경우 사용자는 어플라이언스를 로그아웃한 뒤 다시 로그인해야 합니다. 그러면 사용자는 새 역할의 권한을 갖게 됩니다.

시작하기 전에

LDAP 서버 프로파일 및 LDAP 서버에 대한 외부 인증 쿼리를 정의합니다. 자세한 내용은 LDAP 쿼리, 735 페이지를 참조하십시오.

단계 **1** **System Administration**(시스템 관리) **> Users**(사용자)를 선택합니다.

단계 **2** 아래로 스크롤하여 **External Authentication**(외부 인증) 섹션으로 이동합니다.

단계 **3** **Enable(**활성화**)**을 클릭합니다.

단계 **4** **Enable External Authentication(**외부 인증 활성화**)** 확인란을 선택합니다.

단계 **5** 인증 유형으로 **LDAP**를 선택합니다.

단계 **6** 웹 사용자 인터페이스에서 외부 인증 자격 증명을 저장할 시간을 입력합니다.

단계 **7** 사용자를 인증하는 LDAP 외부 인증 쿼리를 선택합니다.

단계 **8** 어플라이언스가 시간 초과되기 전까지 서버의 응답을 기다리는 시간(초)을 입력합니다

단계 **9** 어플라이언스가 인증할 LDAP 디렉터리에서 그룹의 이름을 입력하고, 그룹의 사용자에 대한 역할을 선택합니다.

단계 **10** 선택적으로, **Add Row(**행 추가**)**를 클릭하여 또 다른 디렉터리 그룹을 추가합니다. 어플라이언스에서 인증할 각 디렉터리 그룹에 대해 9 및 10단계를 반복합니다.

단계 **11** 변경 사항을 제출 및 커밋합니다.

RADIUS 인증 활성화

또한 RADIUS 디렉터리를 사용하여 사용자를 인증하고 사용자 그룹을 Cisco 역할에 할당할 수 있습니다. RADIUS 디렉터리의 사용자를 Cisco 사용자 역할에 할당하기 위해 AsyncOS에서 사용하는 CLASS 특성을 RADIUS 서버에서 지원해야 합니다. AsyncOS는 RADIUS 서버와 통신하기 위한 2가지 인증 프로토콜 즉, PAP(비밀번호 인증 프로토콜)와 CHAP(챌린지 핸드셰이크 인증 프로토콜)를 지원합니다.

RADIUS 사용자를 Cisco 사용자 역할에 할당하려면 먼저 RADIUS 서버에서 문자열 값 <radius-group>을 사용하여 CLASS 특성을 설정합니다. 이 특성은 Cisco 사용자 역할에 매핑됩니다. CLASS 특성은 문자, 숫자 및 대시를 포함할 수 있지만 대시로 시작할 수는 없습니다. AsyncOS는 CLASS 특성으로 다중 값을 지원하지 않습니다. CLASS 특성이 없거나 CLASS 특성이 매핑되지 않은 그룹에 속하는 RADIUS 사용자는 어플라이언스에 로그인할 수 없습니다.

어플라이언스가 RADIUS 서버와 통신할 수 없는 경우 사용자는 어플라이언스에서 로컬 사용자 계정을 사용하여 로그인할 수 있습니다.

참고 외부 사용자가 RADIUS 그룹의 사용자 역할을 변경하는 경우 사용자는 어플라이언스를 로그아웃한 뒤 다시 로그인해야 합니다. 그러면 사용자는 새 역할의 권한을 갖게 됩니다.

단계 **1** **System Administration(**시스템 관리**)** > **Users(**사용자**)** 페이지에서 **Enable(**활성화**)**을 클릭합니다.

단계 **2** 활성화되어 있지 않은 경우에는 Enable External Authentication(외부 인증 활성화) 옵션을 선택합니다.

단계 **3** RADIUS 서버의 호스트 이름을 입력합니다.

단계 **4** RADIUS 서버의 포트 번호를 입력합니다. 기본 포트 번호는 1812입니다.

단계 **5** RADIUS 서버의 공유 암호를 입력합니다.

단계 **6** 어플라이언스가 시간 초과되기 전까지 서버의 응답을 기다리는 시간(초)을 입력합니다.

단계 **7** (선택 사항) 또 다른 RADIUS 서버를 추가하려면 **Add Row(**행 추가**)**를 클릭합니다. 각 RADIUS 서버에 대해 3~6 단계를 반복합니다.

참고 최대 10대의 RADIUS 서버를 추가할 수 있습니다.

단계 **8** AsyncOS가 재인증을 위해 RADIUS 서버에 다시 연결하기 전 외부 인증 자격 증명을 저장하는 시간(초)을 "External Authentication Cache Timeout(외부 인증 캐시 시간 초과)" 필드에 입력합니다. 기본값은 0입니다.

참고 RADIUS 서버에서 일회용 비밀번호(예: 토큰으로 생성된 비밀번호)를 사용하는 경우 0을 입력합니다. 값을 0으로 설정하면 AsyncOS는 현재 세션 중에는 인증을 위해 RADIUS 서버에 다시 연결하지 않습니다.

단계 **9** 그룹 매핑 구성:

설정	설명
외부에서 인증된 사용자를 여러 로컬 역할에 매핑합니다.	AsyncOS는 RADIUS CLASS 특성에 따라 RADIUS 사용자를 어플라이언스 역할에 할당합니다. CLASS 특성 요구 사항: • 최소 3자 • 최대 253자 • 콜론, 쉼표 또는 줄 바꿈 문자 없음 • RADIUS 사용자마다 하나 이상의 매핑된 CLASS 특성이 있음(이 설정을 사용하는 경우 AsyncOS는 매핑된 CLASS 특성이 없는 RADIUS 사용자의 액세스를 거부합니다.) 여러 CLASS 특성이 있는 RADIUS 사용자의 경우 AsyncOS는 제한이 가장 많은 역할을 할당합니다. 예를 들어 RADIUS 사용자에게 운영자 및 읽기 전용 작업자 역할에 매핑되어 있는 CLASS 특성 2개가 있는 경우 AsyncOS는 운영자 역할보다 제한이 많은 읽기 전용 작업자 역할에 RADIUS 사용자를 할당합니다. 어플라이언스 역할은 가장 제한이 적은 역할에서 가장 제한이 많은 역할 순으로 정렬됩니다. • admin • Administrator • Technician • Operator cloudadmin • 읽기 전용 작업자 • Help Desk User • 게스트
Map all externally authenticated users to the Administrator role(외부에서 인증된 모든 사용자를 Administrator 역할에 매핑)	AsyncOS는 RADIUS 사용자를 관리자 역할에 할당합니다.

단계 **10** 외부에서 인증된 모든 사용자를 관리자 역할에 매핑할지, 아니면 각기 다른 어플라이언스 사용자 역할 유형에 매핑할지 선택합니다.

단계 **11** 사용자를 각기 다른 역할 유형에 매핑하는 경우 Group Name(그룹 이름) 또는 Directory(사전) 필드의 RADIUS CLASS 특성에 정의된 그룹 이름을 입력하고 Role(역할) 필드에서 어플라이언스 역할 유형을 선택합니다. **Add Row(**행 추가**)**를 클릭하여 역할 매핑을 더 추가할 수 있습니다.

사용자 역할 유형에 대한 자세한 내용은 사용자 계정 작업, 893 페이지를 참조하십시오.

단계 **12** 변경 사항을 제출 및 커밋합니다.

이중 인증

RADIUS 디렉터리를 사용하여 특정 사용자 역할에 대해 이중 인증을 구성할 수 있습니다. 어플라이언스는 RADIUS 서버와의 통신에 대해 다음 인증 프로토콜을 지원합니다.

- PAP(Password Authentication Protocol)
- CHAP(Challenge Handshake Authentication Protocol)

다음 사용자 역할에 대해 이중 인증을 활성화할 수 있습니다.

- 미리 정의됨
- custom

기능을 테스트하는 데 사용된 인증 방식:

- RSA Authentication Manager v8.2
- FreeRADIUS v1.1.7 이상
- ISE v1.4 이상

관련 주제

- 이중 인증 활성화, 912 페이지
- 이중 인증 비활성화, 913 페이지

이중 인증 활성화

시작하기 전에

IT 관리자로부터 이중 인증에 대한 필수 RADIUS 서버 세부 정보를 가져와야 합니다.

단계 **1** **System Administration(**시스템 관리**) > Users(**사용자**)**에서 Two-Factor Authentication(이중 인증) 아래의 **Enable(**활성화**)**을 클릭합니다.

단계 **2** RADIUS 서버의 호스트 이름 또는 IP 주소를 입력합니다.

단계 **3** RADIUS 서버의 포트 번호를 입력합니다.

단계 **4** RADIUS 서버의 공유 암호를 입력합니다.

단계 **5** 시간 초과되기 전에 서버의 응답을 기다리는 시간(초)을 입력합니다.

단계 **6** 적합한 인증 프로토콜을 선택합니다.

단계 **7** (선택 사항) 또 다른 RADIUS 서버를 추가하려면 **Add Row(**행 추가**)**를 클릭합니다. 각 RADIUS 서버에 대해 2~6단계를 반복합니다.

참고 최대 10대의 RADIUS 서버를 추가할 수 있습니다.

단계 **8** 이중 인증을 활성화하는 데 필요한 사용자 역할을 선택합니다.

단계 **9** 변경사항을 제출 및 커밋합니다.

이중 인증이 활성화되면 사용자 이름 및 암호를 입력한 후 비밀번호를 입력하여 어플라이언스에 로그인하라는 메시지가 표시됩니다.

이중 인증 비활성화

시작하기 전에

어플라이언스에서 이중 인증을 활성화했는지 확인합니다.

단계 **1** **System Administration(**시스템 관리**) > Users(**사용자**)**에서 Two-Factor Authentication(이중 인증) 아래의 **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **2** **Enable Two-Factor Authentication(**이중 인증 활성화**)**을 선택 취소합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

Email Security Appliance에 대한 액세스 구성

AsyncOS는 Email Security Appliance에 대한 사용자 액세스를 관리하기 위한 관리자 제어 기능을 제공합니다, 여기에는 Web UI 세션에 대한 시간 초과, 사용자 및 조직의 프록시 서버가 어플라이언스에 액세스할 수 있는 IP 주소를 지정하는 액세스 목록 등이 포함됩니다.

관련 주제

- IP 기반 네트워크 액세스 구성, 913 페이지
- 세션 시간제한 구성, 916 페이지

IP 기반 네트워크 액세스 구성

어플라이언스에 직접 연결하는 사용자 및 역 프록시를 통해 연결하는 사용자(조직에서 원격 사용자용 역 프록시를 사용하는 경우)를 위한 액세스 목록을 만들어서 Email Security Appliance에 액세스하는 사용자의 IP 주소를 제어할 수 있습니다.

관련 주제

- 직접 연결, 914 페이지
- 프록시를 통한 연결, 914 페이지
- 네트워크 액세스 제한 시 중요한 예방 조치 , 914 페이지
- 액세스 목록 만들기 , 915 페이지

직접 연결

Email Security Appliance에 연결할 수 있는 시스템에 대한 IP 주소, 서브넷 또는 CIDR 주소를 지정할 수 있습니다. 사용자는 액세스 목록의 IP 주소를 사용하는 머신에서 어플라이언스에 액세스할 수 있습니다. 목록에 포함되어 있지 않은 주소에서 어플라이언스에 연결하려고 하는 사용자의 액세스는 거부됩니다.

프록시를 통한 연결

조직의 네트워크가 원격 사용자의 시스템과 Email Security Appliance 간에 역 프록시 서버를 사용하는 경우 AsyncOS에서는 어플라이언스에 연결할 수 있는 프록시의 IP 주소로 액세스 목록을 만들도록 허용합니다.

역 프록시를 사용하는 경우에도 AsyncOS는 사용자 연결이 허용된 IP 주소의 목록을 기준으로 원격 사용자 시스템의 IP 주소를 확인합니다. 원격 사용자의 IP 주소를 Email Security Appliance로 전송하려면, 프록시는 어플라이언스에 대한 연결 요청에 x-forwarded-for HTTP 헤더를 포함해야 합니다.

x-forwarded-for 헤더는 다음과 같은 형식의 비 RFC 표준 HTTP 헤더입니다.

x-forwarded-for: client-ip, proxy1, proxy2,... CRLF .

이 헤더의 값은 쉼표로 구분된 IP 주소 목록으로 맨 왼쪽의 주소는 원격 사용자 머신의 주소이며, 연결 요청을 전달한 일련의 프록시의 주소가 이어집니다. (헤더 이름은 구성할 수 있습니다.) Email Security Appliance는 헤더에 있는 원격 사용자의 IP 주소 및 연결하는 프록시의 IP 주소를 액세스 목록에 있는 허용되는 사용자 및 프록시 IP 주소와 비교합니다.

참고 AsyncOS는 x-forwarded-for 헤더에서 IPv4 주소만 지원합니다.

네트워크 액세스 제한 시 중요한 예방 조치

주의! 다음 조건 중 하나에 해당하는 경우 변경 사항을 제출 및 커밋한 후 어플라이언스에 액세스하지 못하게 될 수 있습니다.

- **Only Allow Specific Connections**(특정 조건만 허용)를 선택하고 목록에 현재 시스템(PC, 클러스터된 환경의 Email Security Appliance 또는 Security Management Appliance 등)의 IP 주소를 포함하지 않는 경우입니다.
- **Only Allow Specific Connections Through Proxy**(프록시를 통한 특정 연결만 허용)를 선택한 상태에서, 어플라이언스에 현재 연결된 프록시의 IP 주소가 프록시 목록에 없고 Origin IP 헤더의 값이 허용되는 IP 주소의 목록에 없는 경우.

- **Only Allow Specific Connections Directly or Through Proxy(**직접 또는 프록시를 통한 특정 연결만 허용**)**를 선택한 상태에서
  - 원래 IP 헤더의 값이 허용되는 IP 주소 목록에 없음.

    또는

  - 원래 IP 헤더 값이 허용되는 IP 주소 목록에 없으며 어플라이언스에 연결된 프록시의 IP 주소가 허용되는 프록시 목록에 없음.

액세스 목록 만들기

GUI 또는 **`adminaccessconfig > ipaccess`** CLI 명령을 사용하여 네트워크 액세스 목록을 생성할 수 있습니다.

시작하기 전에

네트워크 액세스 설정을 변경한 후에는 어플라이언스에서 사용자를 잠그지 않도록 합니다. 네트워크 액세스 제한 시 중요한 예방 조치 , 914 페이지의 내용을 참조하십시오.

단계 **1** **System Administration(**시스템 관리**) > Network Access(**네트워크 액세스**)**를 선택합니다.

단계 **2** **Edit Settings(**설정 편집**)**를 클릭합니다.

단계 **3** 액세스 목록에 대한 제어 모드를 선택합니다.

옵션	설명
Allow All(모두 허용**)**	이 모드에서는 어플라이언스에 대한 모든 연결을 허용합니다. 이는 초기 작동 모드입니다.
특정 연결만 허용	이 모드에서는 사용자 IP 주소가 액세스 목록에 포함된 IP 주소, IP 범위 또는 CIDR 범위와 일치하는 경우 어플라이언스에 대한 사용자 연결을 허용합니다.
프록시를 통한 특정 연결만 허용	이 모드에서는 다음 조건을 만족하는 경우 사용자는 역방향 프록시를 통해 어플라이언스에 연결할 수 있습니다. • 연결 프록시의 IP 주소가 액세스 목록의 IP Address of Proxy Server(프록시 서버의 IP 주소) 필드에 포함되어 있습니다. • 프록시의 연결 요청에 **`x-forwarded-header`** HTTP 헤더를 포함합니다. • **`x-forwarded-header`** 값은 비어 있지 않습니다. • 원격 사용자의 IP 주소가 x-forwarded-header에 포함되어 있고, 액세스 목록의 사용자에 대해 정의된 IP 주소, IP 범위 또는 CIDR 범위와 일치합니다.

옵션	설명
Only Allow Specific Connections Directly or Through Proxy(직접 또는 프록시를 통한 특정 연결만 허용**)**	이 모드에서는 IP 주소가 액세스 목록에 포함된 IP 주소, IP 범위 또는 CIDR 범위와 일치하는 경우 사용자가 역방향 프록시를 통해 또는 직접 어플라이언스에 연결할 수 있습니다. 프록시를 통한 연결에 필요한 조건은 프록시를 통한 특정 연결만 허용 모드와 동일합니다.

단계 **4** 사용자가 어플라이언스에 연결하는 데 사용할 수 있는 IP 주소를 입력합니다.

IP 주소, IP 주소 범위 또는 CIDR 범위를 입력할 수 있습니다. 여러 항목을 구분하려면 쉼표를 사용합니다.

단계 **5** 프록시를 통한 연결이 허용되는 경우 다음 정보를 입력합니다.

1. 어플라이언스에 연결할 수 있는 프록시의 IP 주소 여러 항목을 구분하려면 쉼표를 사용합니다.
2. 프록시가 어플라이언스에 전송하는 원래 IP 헤더의 이름. 원격 사용자 머신 및 요청을 전달한 프록시 서버의 IP 주소를 포함합니다. 기본적으로 헤더의 이름은 x-forwarded-for입니다.

단계 **6** 변경 사항을 제출하고 커밋한 후에 어플라이언스에서 잠기는 변경 사항을 구성하지 않았는지 확인합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

세션 시간제한 구성

웹 **UI** 세션 시간 초과 구성

비활성 때문에 AsyncOS에서 사용자를 로그아웃하기까지 Email Security Appliance의 웹 UI에서 사용자가 로그인을 유지할 수 있는 시간을 지정할 수 있습니다. 이 웹 UI 세션 시간제한이 적용되는 대상은 다음과 같습니다.

- 관리자를 포함한 모든 사용자
- HTTP 및 HTTPS 세션
- Cisco 스팸 격리

AsyncOS에서 사용자가 로그아웃되면 어플라이언스는 사용자의 웹 브라우저를 로그인 페이지로 리디렉션합니다.

단계 **1** **System Administration(**시스템 관리**) > Network Access(**네트워크 액세스**)**를 선택합니다.

단계 **2** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** **Web UI Inactivity Timeout(**웹 **UI** 비활성 시간제한**)** 필드에 사용자가 로그아웃되기 전까지 비활성 상태를 유지할 수 있는 시간(분)을 입력합니다. 5~1440분의 시간제한 시간을 정의할 수 있습니다.

단계 **4** 변경사항을 제출하고 커밋합니다.

다음에 수행할 작업

또한 CLI의 adminaccessconfig 명령을 사용하여 웹 UI 세션 시간제한을 구성할 수 있습니다. *AsyncOS for Cisco Email Security Appliances CLI* 참조 가이드를 참고하십시오.

CLI 세션 시간제한 구성

비활성 때문에 AsyncOS에서 사용자를 로그아웃하기까지 Email Security Appliance의 CLI에서 사용자가 로그인을 유지할 수 있는 시간을 지정할 수 있습니다. CLI 세션 시간제한이 적용되는 대상은 다음과 같습니다.

- 관리자를 포함한 모든 사용자
- SSH(Secure Shell), SCP 및 직접 직렬 연결을 사용한 연결만

참고 CLI 세션의 시간 초과 시점에 커밋되지 않은 구성 변경사항은 손실됩니다. 따라서 구성을 변경한 후 즉시 구성 변경사항을 커밋해야 합니다.

단계 **1** **System Administration**(시스템 관리) > **Network Access**(네트워크 액세스)를 선택합니다.

단계 **2** **Edit Settings**(설정 수정)를 클릭합니다.

단계 **3** **CLI Inactivity Timeout**(웹 **UI** 비활성 시간제한) 필드에 사용자가 로그아웃되기 전까지 비활성 상태를 유지할 수 있는 시간(분)을 입력합니다. 5~1440분의 시간제한 시간을 정의할 수 있습니다.

단계 **4** 변경사항을 제출하고 커밋합니다.

다음에 수행할 작업

CLI의 adminaccessconfig 명령을 사용하여 CLI 세션 시간 초과를 구성할 수도 있습니다. *AsyncOS for Cisco Email Security Appliances CLI* 참조 가이드를 참고하십시오.

관리자에게 메시지 표시

로그인 전 메시지 표시

사용자가 SSH, FTP 또는 웹 UI를 통해 어플라이언스에 로그인을 시도하기 전에 메시지를 표시하도록 Email Security Appliance를 구성할 수 있습니다. 로그인 배너는 로그인 프롬프트 위에 나타나는 사용자 지정 가능한 텍스트입니다. 로그인 배너를 사용하여 내부 보안 정보 또는 어플라이언스의 모범

사례를 표시할 수 있습니다. 예를 들어, 어플라이언스의 무단 사용이 금지되어 있다고 알려주는 간단한 메모나 어플라이언스에 대해 사용자가 변경한 검토 변경 사항에 대한 조직 권한에 관련한 자세한 경고를 만들 수 있습니다.

CLI의 adminaccessconfig > banner 명령을 사용하여 로그인 배너를 생성합니다. 로그인 배너의 최대 길이는 80x25 콘솔에 맞는 2000자입니다. 로그인 배너는 어플라이언스의 /data/pub/configuration 디렉토리에 있는 파일에서 가져올 수 있습니다. 배너를 만든 후 변경 사항을 커밋합니다.

로그인 후 메시지 표시

사용자가 SSH, FTP 또는 웹 UI를 통해 어플라이언스에 성공적으로 로그인한 후 환영 배너를 표시하도록 AsyncOS를 구성할 수 있습니다. 내부 보안 정보 또는 어플라이언스에 대한 모범 사례 지침을 표시하기 위해 환영 배너를 사용할 수 있습니다.

CLI의 adminaccessconfig > welcome 명령을 사용하여 시작 배너를 생성합니다. 시작 배너의 최대 길이는 1,600자입니다.

시작 배너는 어플라이언스의 /data/pub/configuration 디렉토리에 있는 파일에서 가져올 수 있습니다. 배너를 만든 후 변경 사항을 커밋합니다.

자세한 내용은 *AsyncOS for Cisco Email Security Appliance*용 *CLI* 참조 설명서를 참조하십시오.

SSH(Secure Shell) 키 관리

sshconfig 명령을 사용하여 다음을 수행할 수 있습니다.

- admin 계정을 포함하여 시스템에 구성되어 있는 사용자 계정의 authorized_keys 파일에 SSH(Secure Shell) 공개 사용자 키를 추가하거나 삭제합니다. 이러한 방식으로 암호 챌린지가 아닌 SSH 키를 사용하여 사용자 어카운트를 인증할 수 있습니다.
- 다음과 같은 SSH 서버 구성 설정을 편집합니다.
  - 공개 키 인증 알고리즘
  - 암호 알고리즘
  - KEX 알고리즘
  - MAC 방법
  - 최소 서버 키 크기

참고 Cisco 어플라이언스에서 다른 호스트 컴퓨터로 로그 파일을 SCP 푸시할 때 사용할 호스트 키를 구성하려면 **logconfig -> hostkeyconfig**를 사용합니다. 자세한 내용은 로깅, 1053 페이지의 내용을 참고하십시오.

hostkeyconfig를 사용하여 원격 호스트 키를 검색하고 이를 Cisco 어플라이언스에 추가할 수 있습니다.

관련 주제

- 예: 새 공개 키 설치, 919 페이지
- 예: SSH 서버 구성 편집, 919 페이지

예: 새 공개 키 설치

다음 예에서는 관리자 계정에 대해 새 공개 키가 설치됩니다.

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> userkey
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new
Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
[-paste public key for user authentication here-]
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]>
```

예: SSH 서버 구성 편집

다음 예는 SSH 서버를 구성하는 방법을 보여줍니다.

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> sshd
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        arcfour256
        arcfour128
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        arcfour
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
```

```
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]> setup
Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]> rsa1
Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,
cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se]> aes192-ctr
Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,
hmac-md5-96]> hmac-sha1
Enter the Minimum Server Key Size do you want to use
[1024]> 2048
Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group1-sha1]> diffie-hellman-group-exchange-sha1
ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
Cipher Algorithms:
        aes192-ctr
MAC Methods:
        hmac-sha1
Minimum Server Key Size:
        2048
KEX Algorithms:
        diffie-hellman-group-exchange-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]>
```

원격 **SSH** 명령 실행

CLI에서는 원격 SSH 명령 실행을 통해 명령을 실행할 수 있습니다. 예를 들어 Cisco 어플라이언스에서 admin 계정에 대한 SSH 공개 키가 구성된 경우 챌린지되지 않은 원격 호스트에서 다음 명령을 실행할 수 있습니다.

```
# ssh admin@mail3.example.com status

Enter "status detail" for more information.

Status as of: Mon Jan 20 17:24:15 2003

Last counter reset: Mon Jan 20 17:08:21 2003

System status: online

[rest of command deleted]
```

관리자 사용자 액세스 모니터링

변경 후	수행해야 할 작업
어플라이언스의 모든 활성 사용자에 대한 세션 세부 정보 보기	페이지 오른쪽 상단에서 **Options(**옵션**) > Active Sessions(**활성 세션**)**를 클릭합니다. 명령줄 인터페이스에서 w , whoami 및 who 명령을 사용합니다.
최근에 어플라이언스에 로그인한 사용자를 확인합니다. 원격 호스트의 IP 주소, 로그인 시간, 로그아웃 시간 및 총 시간도 표시됩니다.	명령줄 인터페이스에서 l ast 명령을 사용합니다.

36 장

시스템 관리

이 장에는 다음 섹션이 포함되어 있습니다.

참고 이 섹션에서 설명하는 몇 가지 기능 또는 명령은 라우팅 우선 순위에 영향을 미치거나 영향을 받습니다. 자세한 내용은 부록 *B "IP* 주소 인터페이스 및 라우팅"을 참고하십시오.

어플라이언스의 관리

다음 작업을 통해 어플라이언스 내에서 일반적인 기능을 손쉽게 관리할 수 있습니다.

어플라이언스 종료 및 재부팅

종료 또는 재부팅 후, 전달 대기열에 있는 메시지의 손실 없이 나중에 어플라이언스를 다시 시작할 수 있습니다.

CLI에서 shutdown 또는 reboot 명령을 사용하거나 웹 인터페이스를 사용할 수 있습니다.

단계 **1** **System Administration**(시스템 관리) > **Shutdown/Suspend**(종료/일시 중단)를 선택합니다.

단계 **2** **System Operations**(시스템 운영) 섹션의 **Operation**(운영) 드롭다운 목록에서 **Shutdown**(종료) 또는 **Reboot**(재부팅)를 선택합니다.

단계 **3** 강제로 종료되기 전 열린 연결이 완료되도록 기다릴 시간(초)을 입력합니다.

기본 지연은 30초입니다.

단계 **4** **Commit**(커밋)을 클릭합니다.

이메일 수신 및 전달 일시 중단

AsyncOS에서는 이메일의 수신 및 전달을 일시 중단할 수 있습니다. 다음을 일시 중단할 수 있습니다.

- 하나의 특정 리스너 또는 여러 개의 리스너에서 이메일의 수신.
- 하나의 특정 도메인 또는 여러 개의 도메인으로 가는 일부 또는 전체 이메일의 전달.

CLI에서 suspend 명령을 사용하거나 웹 인터페이스에서 다음을 수행합니다.

단계 **1** **System Administration**(시스템 관리) > **Shutdown/Suspend**(종료/일시 중단)를 선택합니다.

단계 **2** 하나의 특정 리스너 또는 여러 개의 리스너에서 이메일의 수신을 일시 중단합니다.

Mail Operations(메일 운영) 섹션에서 일시 중단할 기능 및/또는 리스너를 선택합니다. 어플라이언스에 여러 리스너가 있는 경우 개별 리스너에서 이메일 수신을 일시 중단할 수 있습니다.

단계 **3** 하나의 특정 도메인 또는 여러 개의 도메인으로 가는 일부 또는 전체 이메일의 전달을 일시 중단합니다. 요구 사항에 따라 다음 중 하나를 수행합니다.

1. 모든 이메일의 전달을 일시 중단하려면 **Specify Domain(s)/Subdomain(s)**(도메인/하위 도메인 지정) 필드에 ALL을 입력하고 **Enter**를 누릅니다.

2. 특정 도메인 또는 하위 도메인에 대한 이메일의 전달을 일시 중단하려면 **Specify Domain(s)/Subdomain(s)(**도메인/하위 도메인 지정**)** 필드에 해당 도메인/하위 도메인 이름 또는 IP 주소를 입력하고 **Enter**를 누릅니다. 여러 항목을 추가하려면 쉼표로 구분된 텍스트를 사용합니다.

단계 **4** 강제로 종료되기 전 열린 연결이 완료되도록 기다릴 시간(초)을 입력합니다.

열린 연결이 없는 경우 시스템은 즉시 오프라인이 됩니다.

기본 지연은 30초입니다.

단계 **5** **Commit(**커밋**)**을 클릭합니다.

다음에 수행할 작업

일시 중단된 서비스를 다시 시작할 준비가 되었으면 일시 중단된 이메일 수신 및 전달 다시 시작 , 925 페이지 섹션을 참조하십시오.

일시 중단된 이메일 수신 및 전달 다시 시작

일시 중단된 이메일의 수신 및 전달을 다시 시작하려면 Shutdown/Suspend(종료/일시 중단) 페이지 또는 resume 명령을 사용합니다.

단계 **1** **System Administration(**시스템 관리**)** > **Shutdown/Suspend(**종료/일시 중단**)**를 선택합니다.

단계 **2** **Mail Operations(**메일 운영**)** 섹션에서 다시 시작할 기능 및/또는 리스너를 선택합니다.

어플라이언스에 여러 리스너가 있는 경우 개별 리스너에서 이메일 수신을 다시 시작할 수 있습니다.

단계 **3** 하나의 특정 도메인 또는 여러 개의 도메인으로 가는 일부 또는 전체 이메일의 전달을 다시 시작합니다.

Specify Domain(s)/Subdomain(s)(도메인/하위 도메인 지정**)** 필드에서 원하는 항목의 닫기 아이콘을 클릭합니다.

단계 **4** **Commit(**커밋**)**을 클릭합니다.

공장 기본값으로 재설정

⚠

주의 Serial 인터페이스 또는 Management 포트의 기본 설정을 사용하여 기본 Admin 사용자 계정으로 웹 인터페이스 또는 CLI에 다시 연결할 수 없는 경우에는 공장 기본값으로 재설정하지 마십시오.

어플라이언스를 물리적으로 옮기는 경우 공장 기본 설정으로 시작하길 원할 수 있습니다. 공장 기본값으로 재설정하면 모든 정보가 손실되므로, 이 기능은 장치를 전송하는 경우 또는 구성 문제 해결을 위한 최후의 수단으로서만 사용해야 합니다. 공장 기본값으로 재설정하면 웹 인터페이스 또는 CLI에서 연결이 해제되며, 어플라이언스에 연결하기 위해 사용하던 서비스(FTP, SSH, HTTP, HTTPS)가 비

활성화되고, 만들었던 추가 사용자 계정도 제거됩니다. 다음을 통해 공장 기본값으로 재설정할 수 있습니다.

- 웹 인터페이스의 **System Administration**(시스템 관리) > **Configuration File**(구성 파일) 페이지에서 Reset(재설정) 버튼을 클릭하거나, **System Administration**(시스템 관리) > **System Setup Wizard**(시스템 설정 마법사)에서 Reset Configuration(구성 재설정) 버튼을 클릭합니다.
- CLI에서 **resetconfig** 명령을 사용합니다.

참고 **resetconfig** 명령은 어플라이언스가 오프라인 상태일 때만 작동합니다. 공장 기본값으로 재설정한 후 어플라이언스는 온라인 상태로 돌아갑니다.

다음 단계

- 시스템 설정 마법사를 실행합니다. 자세한 내용은 시스템 설정 마법사 사용 , 28 페이지 섹션을 참조하십시오.
- 메일 전달을 켜서 메일 전달을 다시 시작합니다.

AsyncOS에 대한 버전 정보 표시

현재 어플라이언스에 어떤 AsyncOS 버전이 설치되었는지 확인하려면 웹 인터페이스에서 Monitor(모니터) 메뉴의 System Overview(시스템 개요) 페이지를 사용하거나(System Status, 826 페이지 참고), CLI에서 version 명령을 사용합니다.

Cisco Email Security Appliance 라이선스

기능 키

기능 키 추가 및 관리

물리적 어플라이언스에서 기능 키는 어플라이언스의 일련 번호와 관련이 있으며 활성화 상태인 기능과도 관련이 있습니다(한 시스템의 키를 다른 시스템에서 재사용할 수 없음).

CLI에서 기능 키로 작업하려면 **featurekey** 명령을 사용합니다.

단계 **1** **System Administration**(시스템 관리) > **Feature Keys**(기능 키)를 선택합니다.

단계 **2** 다음 작업을 수행합니다.

변경 후	수행해야 할 작업
활성 기능 키의 상태 보기	**Feature Keys for <serial number>**(<일련 번호>의 기능 키) 섹션을 살펴봅니다.
어플라이언스에 대해 발급되었지만 아직 활성화되지 않은 기능 키 보기	**Pending Activation**(활성화 대기 중) 섹션을 살펴봅니다. 자동 다운로드와 활성화를 지정한 경우 이 목록에 기능 키가 나타나지 않습니다.
최근에 발급된 기능 키 검토	Pending Activation(활성화 대기 중) 섹션에서 **Check for New Keys**(새 키 검토) 버튼을 클릭합니다. 이 방법은 기능 키의 자동 다운로드 및 활성화를 설정하지 않은 경우 또는 다음 자동 검토 전에 기능 키를 다운로드해야 하는 경우 유용합니다.
발급된 기능 키 활성화	**Pending Activation**(활성화 대기 중) 목록에서 키를 선택하고 **Activate Selected Keys**(선택한 키 활성화)를 클릭합니다.
새 기능 키 추가	**Feature Activation**(기능 활성화) 섹션을 사용합니다.

다음에 수행할 작업

관련 주제

- 기능 키 다운로드 및 활성화 자동 실행 , 927 페이지
- Configuration File(구성 파일) 페이지, 941 페이지

기능 키 다운로드 및 활성화 자동 실행

어플라이언스에 대해 발급된 기능 키를 자동으로 검토, 다운로드 및 활성화하도록 설정할 수 있습니다.

단계 **1** **System Administration**(시스템 관리) > **Feature Key Settings**(기능 키 설정)를 선택합니다.

단계 **2** **Edit Feature Key Settings**(기능 키 설정 수정)를 클릭합니다.

단계 **3** 새 기능 키의 검토 빈도를 확인하려면 (?) 도움말 버튼을 클릭합니다.

단계 **4** 설정을 지정합니다.

단계 **5** 변경사항을 제출 및 커밋합니다.

다음에 수행할 작업

관련 주제

- 기능 키 추가 및 관리 , 926 페이지

만료된 기능 키

기능 키가 만료되는 경우 어플라이언스는 키 만료 90일, 60일, 30일, 15일, 5일 및 하루 전에 알림을 전송하고 만료 시점에도 알림을 전송합니다. 이러한 알림을 받으려면 System Alerts(시스템 알림)를 구독해야 합니다. 자세한 내용은 알림, 962 페이지를 참고하십시오.

웹 인터페이스를 사용하여 액세스하려고 하는 기능에 대한 기능 키가 만료된 경우 Cisco 담당자 또는 지원 조직에 문의하십시오.

Smart Software Licensing

개요

Smart Software Licensing을 사용하면 Cisco Email Security Appliance 라이선스를 원활하게 관리하고 모니터링할 수 있습니다. Smart Software Licensing을 활성화하려면 구매하고 사용하는 모든 Cisco 제품에 대한 라이선싱 세부 정보를 유지하는 중앙 집중식 데이터베이스인 CSSM(Cisco Smart Software Manager)에 어플라이언스를 등록해야 합니다. Smart Licensing을 사용하면 PAK(Product Authorization Key)를 사용하여 웹 사이트에서 개별적으로 등록하는 대신 단일 토큰으로 등록할 수 있습니다.

어플라이언스를 등록한 후 어플라이언스 라이선스를 추적하고 CSSM 포털을 통해 라이선스 사용량을 모니터링할 수 있습니다. 어플라이언스에 설치된 Smart Agent는 어플라이언스를 CSSM에 연결하고 CSSM에 라이선스 사용량 정보를 전달하여 사용량을 추적합니다.

Cisco Smart Software Manager에 대한 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html 항목을 참고하십시오.

시작하기 전에

- 어플라이언스에 인터넷이 연결되어 있는지 확인합니다.
- Cisco Smart Software Manager 포털(https://software.cisco.com/#module/SmartLicensing)에서 스마트 어카운트를 생성하거나 네트워크에 Cisco Smart Software Manager Satellite를 설치하려면 Cisco 세일즈 팀에 문의하십시오.

  Cisco Smart Software Manager 사용자 계정 생성 및 Cisco Smart Software Manager Satellite 설치에 대한 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html을 참조하십시오.

  인터넷에 직접 라이선스 사용량 정보를 전송하지 않으려는 사용자의 경우, 사내에 Smart Software Manager Satellite를 설치하고 이를 통해 CSSM 기능의 하위 집합을 제공할 수 있습니다. Satellite 애플리케이션을 다운로드하고 구축하면 인터넷을 사용하여 CSSM에 데이터를 전송하지 않고 로컬로 안전하게 라이선스를 관리할 수 있습니다. CSSM Satellite는 주기적으로 클라우드에 정보를 전송합니다.

  참고 Smart Software Manager Satellite를 사용하려는 경우 Smart Software Manager Satellite Enhanced Edition 6.1.0을 사용합니다.

- 기본 라이선스(기존)의 기존 사용자는 해당 기본 라이선스를 스마트 라이선스에 마이그레이션해야 합니다.

  https://video.cisco.com/detail/video/5841741892001/convert-classic-licenses-to-smart-licenses?autoStart=true&q=classic를 참조하십시오.

- 어플라이언스의 시스템 클록이 CSSM의 시스템 클록과 동기화되어 있어야 합니다. 어플라이언스의 시스템 클록에 있는 모든 편차를 CSSM과 함께 사용하면 Smart Licensing 작업이 실패합니다.

참고 인터넷에 연결되어 있고 프록시를 통해 CSSM에 연결하려는 경우 **Security Services -> Service updates(**서비스 업데이트**)**를 사용하여 어플라이언스에 대해 구성된 것과 동일한 프록시를 사용해야 합니다.

참고 가상 사용자의 경우 새 PAK 파일(신규 또는 갱신)을 받을 때마다 라이선스 파일을 생성하여 어플라이언스에서 로드합니다. 파일을 로드한 후에는 PAK를 Smart Licensing으로 변환해야 합니다. Smart Licensing 모드에서는 파일을 로드하는 동안 라이선스 파일의 feature keys 섹션이 무시되며 인증서 정보만 사용됩니다.

어플라이언스에 대한 Smart Software Licensing을 활성화하려면 다음 절차를 수행해야 합니다.

	수행해야 할 작업	추가 정보
1단계	Smart Software Licensing 활성화	Smart Software Licensing 사용활성화, 930 페이지
2단계	Cisco Smart Software Manager에 어플라이언스 등록	Cisco Smart Software Manager에 어플라이언스 등록, 931 페이지
3단계	라이선스(기능 키) 요청	라이선스 요청, 931 페이지

Smart Software Licensing 사용활성화

단계 **1** **System Administration(시스템 관리) > Smart Software Licensing**을 선택합니다.

단계 **2** **Enable Smart Software Licensing(스마트 소프트웨어 라이선싱 활성화)**을 클릭합니다.

Smart Software Licensing에 대해 알아보려면 Smart Software Licensing에 대해 자세히 알아보기 링크를 클릭합니다.

단계 **3** Smart Software Licensing에 대한 정보를 읽은 후 **OK(확인)**를 클릭합니다.

단계 **4** 변경 사항을 커밋합니다.

다음에 수행할 작업

Smart Software Licensing을 활성화하면 Smart Licensing(스마트 라이선싱) 모드에서 Classic Licensing(기본 라이선싱) 모드의 모든 기능을 자동으로 사용할 수 있게 됩니다. Classic Licensing(기본 라이선싱) 모드의 기존 사용자는 90일 평가 기간 동안 CSSM에 어플라이언스를 등록하지 않고도 Smart Software Licensing 기능을 사용할 수 있습니다.

평가 기간 만료 전과 만료 시에 주기적인 간격(90일, 60일, 30일, 15일, 5일 및 말일)으로 알림을 받게 됩니다. 평가 기간 중이나 후에는 CSSM에 어플라이언스를 등록할 수 있습니다.

참고 Classic Licensing(기본 라이선싱) 모드에 활성 라이선스가 없는 새 가상 어플라이언스 사용자는 Smart Software Licensing 기능을 활성화하더라도 평가 기간을 이용할 수 없습니다. Classic Licensing(기본 라이선싱) 모드에 활성 라이선스가 있는 기존 가상 어플라이언스 사용자만 평가 기간을 사용할 수 있습니다. 새 가상 어플라이언스 사용자가 스마트 라이선싱 기능을 평가하려는 경우 스마트 어카운트에 평가 라이선스를 추가하려면 Cisco 세일즈 팀에 문의해 주십시오. 평가 라이선스는 등록 후에 평가용으로 사용됩니다.

참고 어플라이언스에서 Smart Licensing 기능을 활성화한 후에는 Smart Licensing 모드에서 Classic Licensing 모드로 롤백할 수 없게 됩니다.

Cisco Smart Software Manager에 어플라이언스 등록

어플라이언스에 Cisco Smart Software Manager를 등록하려면 System Administration(시스템 관리) 메뉴에서 Smart Software Licensing 기능을 활성화해야 합니다.

단계 **1** **System Administration(**시스템 관리**) > Smart Software Licensing**을 선택합니다.

단계 **2** **Transport Settings(**전송 설정**)**를 변경하려면 **Edit(**편집**)**을 클릭합니다. 사용 가능한 옵션은 다음과 같습니다.

- 직접: HTTP를 통해 Cisco Smart Software Manager에 직접 어플라이언스를 연결합니다. 이 옵션은 기본적으로 선택되어 있습니다.
- 전송 게이트웨이: 전송 게이트웨이 또는 Smart Software Manager Satellite를 통해 Cisco Smart Software Manager에 어플라이언스를 연결합니다. 이 옵션을 선택한 경우 전송 게이트웨이 또는 Smart Software Manager Satellite의 URL을 입력하고 OK(확인)를 클릭해야 합니다. 이 옵션은 HTTP 및 HTTPS를 지원합니다. FIPS 모드에서는 전송 게이트웨이가 HTTPS만 지원합니다. 전송 게이트웨이에 대한 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_ Deployment_Guide.html을 참조하십시오.

  로그인 크리덴셜을 사용하여 Cisco Smart Software Manager

  포털(https://software.cisco.com/#module/SmartLicensing)에 액세스합니다. 포털의 Virtual Accounts(가상 어카운트) 페이지로 이동하고 General(일반) 탭에 액세스하여 새 토큰을 생성합니다. 어플라이언스에 대한 제품 인스턴스 등록 토큰을 복사합니다.

  제품 인스턴스 등록 토큰 생성에 대한 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_ Deployment_Guide.html을 참조하십시오.

단계 **3** 어플라이언스로 다시 전환하고 제품 인스턴스 등록 토큰을 붙여 넣습니다.

단계 **4** **Register(**등록**)**를 클릭합니다.

단계 **5** 어플라이언스를 다시 등록하려면 Smart Software Licensing 페이지에서 Reregister this product instance if it is already registered(이미 등록된 경우 이 제품 인스턴스를 등록합니다) 확인란을 선택하면 됩니다. Smart Cisco Software Manager에서 어플라이언스 다시 등록 , 932 페이지를 참조하십시오.

다음에 수행할 작업

제품 등록 프로세스는 몇 분 정도 걸리고 Smart Software Licensing 페이지에서 등록 상태를 볼 수 있습니다.

라이선스 요청

등록 프로세스가 성공적으로 완료되면 필요에 따라 어플라이언스의 기능에 대한 라이선스를 요청해야 합니다.

단계 **1** **System Administration(**시스템 관리**) > Licenses(**라이선스**)**를 선택합니다.

단계 2 **Edit Settings(**설정 편집**)**를 클릭합니다.

단계 3 요청할 라이선스에 해당하는 License Request/Release(라이선스 요청/릴리스) 열에서 확인란을 선택합니다.

단계 4 **Submit(**제출**)**을 클릭합니다.

참고 기본적으로 메일 처리를 위한 라이선스 및 Email Security Appliance 반송 확인을 사용할 수 있습니다. 이 라이선스를 활성화하거나, 비활성화하거나, 릴리스할 수 없습니다.

메일 처리 및 Email Security Appliance 반송 확인 라이선스에 대한 평가 기간이 없거나 규정을 준수하지 않습니다. 이는 가상 어플라이언스에는 적용되지 않습니다.

다음에 수행할 작업

라이선스가 과도하게 사용되거나 만료되면 규정 준수 위반(OOC) 모드가 되고 각 라이선스에 30일의 유예 기간이 제공됩니다. OOC 유예 기간 만료 전과 만료 시에 주기적인 간격(30일, 15일, 5일 및 말일)으로 알림을 받게 됩니다.

OOC 유예 기간 만료 후에는 라이선스를 사용할 수 없고 기능을 사용할 수 없게 됩니다. 이 기능에 다시 액세스하려면 CSSM 포털에서 라이선스를 업데이트하고 권한을 갱신해야 합니다.

Smart Cisco Software Manager에서 어플라이언스 등록 취소

단계 1 **System Administration(**시스템 관리**) > Smart Software Licensing**을 선택합니다.

단계 2 **Action(**작업**)** 드롭다운 목록에서 **Deregister(**등록 취소**)**를 선택하고 **Go(**이동**)**를 클릭 합니다.

단계 3 제출을 클릭합니다.

Smart Cisco Software Manager에서 어플라이언스 다시 등록

단계 1 **System Administration(**시스템 관리**) > Smart Software Licensing**을 선택합니다.

단계 2 **Action(**작업**)** 드롭다운 목록에서 **Reregister(**다시 등록**)**를 선택하고 **Go(**이동**)**를 클릭 합니다.

다음에 수행할 작업

등록 프로세스에 대한 자세한 내용은 Cisco Smart Software Manager에 어플라이언스 등록, 931 페이지을 참조하십시오.

반드시 등록해야 하는 경우에는 어플라이언스 구성을 재설정한 후 어플라이언스를 다시 등록할 수 있습니다.

전송 설정 변경

CSSM에 어플라이언스를 등록하기 전에만 전송 설정을 변경할 수 있습니다.

참고 Smart Licensing 기능을 활성화한 경우에만 전송 설정을 변경할 수 있습니다. 어플라이언스를 이미 등록한 경우 전송 설정을 변경하려면 어플라이언스 등록을 취소해야 합니다. 전송 설정을 변경한 후 어플라이언스를 다시 등록해야 합니다.

전송 설정을 변경하는 방법은 Cisco Smart Software Manager에 어플라이언스 등록을 참고하십시오.

권한 및 인증서 갱신

어플라이언스에 Smart Cisco Software Manager를 등록한 후에 인증서를 갱신할 수 있습니다.

참고 어플라이언스를 성공적으로 등록한 후에만 권한을 갱신할 수 있습니다.

단계 **1** **System Administration**(시스템 관리) **> Smart Software Licensing**을 선택합니다.

단계 **2** **Action**(작업) 드롭다운 목록에서 적절한 옵션을 선택합니다.

- 지금 권한 부여 갱신
- 지금 인증서 갱신

단계 **3** **Go**(이동)를 클릭합니다.

알림

다음과 같은 경우에 알림을 받게 됩니다.

- Smart Software Licensing 활성화에 성공 시
- Smart Software Licensing 활성화에 실패 시
- 평가 기간 시작 시
- 평가 기간 만료 시(평가 기간 동안 및 만료 시 주기적 간격으로)
- 등록에 성공 시
- 등록에 실패했습니다.
- 권한 부여에 성공 시
- 권한 부여에 실패 시
- 등록 해제에 성공 시
- 등록 해제에 실패 시
- ID 인증서 갱신에 성공 시

- ID 인증서 갱신에 실패 시
- 권한 부여 만료 시
- ID 인증서 만료 시
- OOC 유예 기간 만료 시(OOC 유예 기간 중과 만료 시 주기적 간격으로)
- 기능 만료의 첫 번째 인스턴스에서

Smart Agent 업데이트

어플라이언스에 설치된 Smart Agent 버전을 업데이트하려면 다음 단계를 수행합니다.

단계 **1** **System Administration(시스템 관리) > Smart Software Licensing**을 선택합니다.

단계 **2** **Smart Agent Update Status(Smart Agent** 업데이트 상태**)** 섹션에서 **Update Now(**지금 업데이트**)**를 클릭하고 프로세스를 수행합니다.

참고 CLI 명령 `saveconfig`를 사용하거나 웹 인터페이스에서 **System Administration(**시스템 관리**) > Configuration Summary(**구성 요약**)**를 통해 구성 변경사항을 저장하려고 하면 Smart Licensing 관련 구성이 저장되지 않습니다.

클러스터 모드의 Smart Licensing

참고 Smart Licensing 기능의 클러스터 관리는 시스템 모드에서만 발생합니다. Smart Licensing 클러스터 모드에서는 어플라이언스 중 하나에 로그인하여 Smart Licensing 기능을 구성할 수 있습니다. 어플라이언스 하나에 로그인한 후 클러스터의 다른 어플라이언스에 하나씩 액세스하여 첫 번째 어플라이언스에서 로그오프하지 않고도 Smart Licensing 기능을 구성할 수 있습니다.

자세한 내용은 클러스터를 사용한 중앙 집중식 관리, 1117 페이지를 참고하십시오.

Cisco Email Security Virtual Appliance 라이센스

Email Security Virtual Appliance의 설정 및 라이센스에 대한 자세한 내용은 *Cisco Content Security Virtual Appliance* 설치 가이드를 참고하십시오. 이 문서는 설명서 에 지정된 위치에서 사용할 수 있습니다.

참고 가상 어플라이언스 라이센스를 설치하기 전에는 기술 지원 터널을 열거나 시스템 설정 마법사를 실행할 수 없습니다.

가상 어플라이언스 라이센스 만료

가상 어플라이언스 라이센스가 만료된 후 어플라이언스는 180일 동안 보안 서비스 없이 메일을 계속 배달합니다. 이 기간에는 보안 서비스 업데이트가 발생하지 않습니다.

라이센스 만료 180일, 150일, 120일, 90일, 60일, 30일, 15일, 5일, 1일 및 0초 전에 그리고 유예 기간 종료 전에 동일한 간격으로 알림이 전송됩니다. 이러한 알림은 심각도 레벨 "Critical"에서 "System" 유형입니다. 이러한 알림을 받도록 하려면 알림 수신자 추가, 964 페이지 섹션을 참조하십시오.

시스템 로그에도 이러한 알림이 기록됩니다.

개별 기능 키는 가상 어플라이언스 라이센스보다 일찍 만료될 수 있습니다. 개별 키의 만료일이 다가올 때에도 알림을 받게 됩니다.

관련 주제

- 가상 어플라이언스에서 AsyncOS를 복귀하면 라이센스에 영향이 미칠 수 있음 , 959 페이지

구성 파일 관리

어플라이언스 내 모든 구성 설정은 단일 구성 파일을 통해 관리할 수 있습니다. 파일은 XML(Extensible Markup Language) 형식으로 유지 관리됩니다.

몇 가지 방법으로 이 파일을 사용할 수 있습니다.

- 중요 구성 데이터를 백업 및 보존하려면 구성 파일을 다른 시스템에 저장할 수 있습니다. 어플라이언스를 구성하는 동안 실수한 경우 최근에 저장된 구성 파일로 "롤백"할 수 있습니다.
- 어플라이언스의 전체 구성을 빠르게 검토하려면 기존 구성 파일을 다운로드할 수 있습니다. (다수의 최신 브라우저에서는 XML 파일을 직접 렌더링할 수 있습니다.) 이는 현재 구성에 존재할 수 있는 작은 오류(예: 오타)를 해결하는 데 도움이 될 수 있습니다.
- 기존 구성 파일을 다운로드하고 내용을 변경하고 동일한 어플라이언스에 업로드할 수 있습니다. 이렇게 하면 CLI와 웹 인터페이스를 "우회"하여 구성을 변경할 수 있습니다.
- FTP 액세스를 통해 전체 구성 파일을 업로드하거나, 전체 구성 파일의 일부를 CLI에 직접 붙여넣을 수 있습니다.
- 파일이 XML 형식이므로, 구성 파일의 모든 XML 엔티티를 설명하는 관련 DTD(document type definition)도 함께 제공됩니다. 업로드 전 XML 구성 파일을 검증하려면 DTD를 다운로드할 수 있습니다. (인터넷에서 XML 검증 툴을 쉽게 이용할 수 있습니다.)

XML 컨피그레이션 파일로 여러 어플라이언스 관리

- 한 어플라이언스에서 기존의 컨피그레이션 파일을 다운로드하고, 내용을 변경한 후 다른 어플라이언스에 업로드할 수 있습니다. 이렇게 하면 여러 어플라이언스의 설치를 좀 더 쉽게 관리할 수 있습니다. 현재 C/X-Series 어플라이언스에서 M-Series 어플라이언스로 구성 파일을 로드할 수 없습니다.

- 한 어플라이언스에서 다운로드한 기존의 컨피그레이션 파일을 여러 하위 섹션으로 나눌 수 있습니다. 모든 어플라이언스에 공통된 이러한 섹션을 수정하고(다중 어플라이언스 환경에서), 하위 섹션이 업데이트되면 다른 어플라이언스에 로드할 수 있습니다.

예를 들면 Global Unsubscribe 명령을 테스트하기 위한 테스트 환경에서 어플라이언스를 사용할 수 있습니다. Global Unsubscribe(전역 수신 거부) 목록을 적절히 구성한 후 테스트 어플라이언스의 Global Unsubscribe(전역 수신 거부) 섹션을 모든 프로덕션 어플라이언스에 로드할 수 있습니다.

구성 파일 관리

어플라이언스에서 컨피그레이션 파일을 관리하려면 System Administration(시스템 관리) > Configuration File(컨피그레이션 파일)을 클릭합니다.

Configuration File(컨피그레이션 파일) 페이지에는 다음 섹션이 포함되어 있습니다.

- **Current Configuration(현재 컨피그레이션)** - 현재 컨피그레이션 파일을 저장하고 내보내는 데 사용됩니다.
- **Load Configuration(컨피그레이션 로드)** - 전체 또는 부분 컨피그레이션 파일을 로드하는 데 사용됩니다.
- **End-User Safelist/Blocklist Database (Spam Quarantine)(최종 사용자 허용 목록/차단 목록 데이터베이스(스팸 격리))** - 자세한 내용은 허용 목록 및 차단 목록을 사용하여 발신자 기준으로 이메일 전달 제어 , 873 페이지 및 허용 목록/차단 목록 백업 및 복원 , 880 페이지 섹션을 참조하십시오.
- **Reset Configuration(컨피그레이션 재설정)** - 현재 컨피그레이션을 공장 기본값으로 재설정하는 데 사용됩니다(재설정 전에 컨피그레이션을 저장해야 합니다).

참고 개인 키와 인증서는 암호화된 암호의 구성 파일과 함께 암호화되지 않은 PEM 형식에 포함됩니다.

관련 주제

- 현재 구성 파일 저장 및 내보내기, 936 페이지
- 구성 파일 로드, 937 페이지
- 컨피그레이션 파일 메일로 전송, 937 페이지
- 현재 구성 재설정, 940 페이지

현재 구성 파일 저장 및 내보내기

System Administration(시스템 관리) > Configuration File(구성 파일) 페이지의 **Current Configuration(현재 구성)**을 사용하여 현재 구성 파일을 로컬 시스템에 저장하거나, 어플라이언스에 저장하거나(FTP/SCP 루트의 configuration 디렉터리), 이메일을 통해 지정된 주소로 전송할 수 있습니다.

다음 정보는 컨피그레이션 파일과 함께 저장되지 않습니다.

- URL 필터링 기능이 사용하는 서비스와의 보안 통신에 사용되는 인증서.
- 기술 지원 문의 페이지에 저장되는 CCO 사용자 ID 및 계약 ID.

Mask passphrases in the Configuration Files(구성 파일에서 암호 마스크 처리**)** 확인란을 클릭하여 사용자의 암호를 마스크 처리할 수 있습니다. 암호를 마스크 처리하면 내보내거나 저장한 파일에서 원래의 암호화된 암호가 "*****"로 교체됩니다. 그러나 마스크 처리된 암호의 구성 파일은 AsyncOS로 다시 로드할 수 없습니다.

Encrypt passphrases in the Configuration Files(구성 파일에서 암호 암호화**)** 확인란을 클릭하여 사용자의 암호를 암호화할 수 있습니다. 다음은 암호화될 컨피그레이션 파일의 주요 보안 매개변수입니다.

- 인증서 개인 키
- RADIUS 비밀번호
- LDAP 바인드 비밀번호
- 로컬 사용자의 비밀번호 해시
- SNMP 비밀번호
- DK/DKIM 서명 키
- 발신 SMTP 인증 비밀번호
- PostX 암호화 키
- PostX 암호화 프록시 비밀번호
- FTP 푸시 로그 서브스크립션 비밀번호
- IPMI LAN 비밀번호
- 업데이터 서버 URL

CLI에서 saveconfig 명령을 사용하여 이를 구성할 수도 있습니다.

컨피그레이션 파일 메일로 전송

System Administration(시스템 관리) > Configuration File(구성 파일)의 Email file to(이메일로 파일 전송) 필드 또는 mailconfig 명령을 사용하여 현재 구성을 첨부 파일로서 사용자에게 이메일로 전송할 수 있습니다.

구성 파일 로드

System Administration(시스템 관리**) > Configuration File(**컨피그레이션 파일**)** 페이지의 Load Configuration(컨피그레이션 로드) 섹션을 사용하여 새 컨피그레이션 정보를 어플라이언스에 로드합니다. CLI에서 `loadconfig` 명령을 사용하여 이를 구성할 수도 있습니다.

다음 세 가지 방법 중 하나로 정보를 로드할 수 있습니다.

- `configuration` 디렉터리에 정보를 두고 이를 업로드합니다.
- 로컬 시스템에서 직접 컨피그레이션 파일을 업로드합니다.
- 컨피그레이션 정보를 직접 붙여넣습니다.

참고 마스크 처리된 암호가 있는 구성 파일은 로드할 수 없습니다.

클러스터 모드에서 클러스터용 컨피그레이션을 로드할지, 어플라이언스용 컨피그레이션을 로드할지를 선택할 수 있습니다. 클러스터 컨피그레이션 로드에 대한 지침은 클러스터링된 어플라이언스에서 컨피그레이션 로드, 1139 페이지 섹션을 참조하십시오.

방법과 상관없이 구성 상단에 다음 태그를 포함해야 합니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

... your configuration information in valid XML

</config>
```

컨피그레이션 정보 뒤에 닫는 `</config>` 태그를 사용해야 합니다. 어플라이언스의 `configuration` 디렉터리에 있는 DTD(document type definition)를 기준으로 XML 구문의 값이 구문 분석 및 검증됩니다. DTD 파일의 이름은 `config.dtd`입니다. `loadconfig` 명령을 사용할 때 명령줄에서 검증 오류가 보고되면 변경 사항이 로드되지 않습니다. 업로드 전 어플라이언스 외부에서 구성 파일을 검증하려면 DTD를 다운로드할 수 있습니다.

어떤 방법을 사용하든 선언 태그(위)를 포함하며 `<config></config>` 태그 내에 포함되어 있는 한, 전체 구성 파일(최고 레벨 태그인 `<config></config>` 사이에 정의된 정보) 또는 구성 파일의 *complete* 및 *unique* 하위 섹션을 가져올 수 있습니다.

"Complete"란 DTD에 정의된 대로 지정된 하위 섹션에 대한 전체 시작 및 종료 태그가 포함되어 있음을 의미합니다. 예를 들어 다음을 업로드하거나 붙여넣으면

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

<autosupport_enabled>0</autosu

</config>
```

업로드하는 동안 검증 오류가 발생합니다. 그러나 다음의 경우

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>
```

```
<autosupport_enabled>0</autosupport_enabled>

</config>
```

오류가 발생하지 않습니다.

"Unique"란 업로드하거나 붙여넣는 컨피그레이션 파일의 하위 집합이 컨피그레이션에 대해 모호하지 않다는 의미입니다. 예를 들어 시스템은 호스트 이름을 하나만 가질 수 있으므로 다음(선언 및 `<config></config>` 태그 포함)

```
<hostname>mail4.example.com</hostname>
```

태그의 업로드가 허용됩니다. 그러나 한 시스템에 대해 여러 리스너가 정의될 수 있으며 각각에 대해 서로 다른 Recipient Access Table이 정의되므로 다음

```
<rat>

       <rat_entry>

              <rat_address>ALL</rat_address>

         <access>RELAY</access>

     </rat_entry>

</rat>
```

태그는 "complete" 구문이라도 모호하므로 허용되지 않습니다.

⚠

주의 컨피그레이션 파일 또는 컨피그레이션 파일의 하위 섹션을 업로드하거나 구문 분석할 때 커밋되지 않은(대기 중일 수 있는) 변경 사항을 지울 가능성이 있습니다.

컨피그레이션 파일의 디스크 공간 할당이 현재 어플라이언스에 저장된 데이터의 양보다 작으면 컨피그레이션 파일에 지정된 할당량을 맞추기 위해 가장 오래된 데이터부터 삭제됩니다.

빈 태그 대 생략된 태그

구성 파일의 섹션을 업로드하거나 구분 분석할 때는 주의해야 합니다. 태그를 포함하지 않으면 구성 파일을 로드할 때 구성의 해당 값이 수정되지 않습니다. 그러나 빈 태그를 포함하면 해당 구성 설정이 지워집니다.

예를 들어 다음을 업로드하면

```
<listeners></listeners>
```

시스템에서 모든 리스너가 제거됩니다.

주의 컨피그레이션 파일의 하위 섹션을 업로드하거나 구문 분석할 때, 웹 인터페이스나 CLI에서 연결이 끊어지고 대량의 컨피그레이션 데이터가 손실될 가능성이 있습니다. 또 다른 프로토콜, Serial 인터페이스 또는 Management 포트의 기본 설정을 사용하여 어플라이언스에 다시 연결할 수 있는 경우가 아니면 이 명령으로 서비스를 비활성화하지 마십시오. 또한 DTD에 의해 정의된 정확한 구성 구문을 확실히 알고 있지 않다면 이 명령을 사용하지 마십시오. 새 컨피그레이션 파일을 로드하기 전에 항상 컨피그레이션 데이터를 백업하십시오.

로그 서브스크립션용 암호 로드에 대한 참고 사항

암호(예: FTP 푸시를 사용할 암호)가 필요한 로그 서브스크립션이 포함된 구성 파일을 로드하려고 하는 경우 loadconfig 명령은 암호 누락에 대해 경고하지 않습니다. logconfig 명령을 사용하여 올바른 암호를 구성할 때까지 FTP 푸시가 실패하고 알림이 생성됩니다.

문자 집합 인코딩에 대한 참고 사항

오프라인으로 파일을 조작하기 위해 사용하는 문자 집합과 상관없이, XML 구성 파일의 "encoding" 특성은 "ISO-8859-1"이어야 합니다. showconfig, saveconfig 또는 mailconfig 명령을 실행할 때마다 파일에 인코딩 특성이 지정됩니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

현재 이 인코딩의 컨피그레이션 파일만 로드할 수 있습니다.

관련 주제

- 클러스터링된 어플라이언스에서 컨피그레이션 로드, 1139 페이지

현재 구성 재설정

현재 컨피그레이션을 재설정하면 어플라이언스가 원래 공장 기본값으로 되돌아갑니다. 재설정하기 전에 컨피그레이션을 저장해야 합니다. GUI에서 이 버튼을 통해 컨피그레이션을 재설정하는 것은 클러스터링 환경에서 지원되지 않습니다.

공장 기본값으로 재설정, 925 페이지를 참조하십시오.

컨피그레이션 파일 보기

컨피그레이션 파일 세부사항을 보려면 showconfig 명령만 사용할 수 있습니다. showconfig 명령은 현재 구성을 화면에 출력합니다.

```
mail3.example.com> showconfig


Do you want to include passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig.
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
Product: IronPort model number Messaging Gateway Appliance(tm)
```

```
Model Number: model number
Version: version of AsyncOS installed
Serial Number: serial number

Current Time: current time and date

[The remainder of the configuration file is printed to the screen.]
```

Configuration File(구성 파일) 페이지

- 구성 파일 관리, 935 페이지
- 공장 기본값으로 재설정, 925 페이지
- 허용 목록/차단 목록 백업 및 복원 , 880 페이지

디스크 공간 관리

- (가상 어플라이언스 전용) 사용 가능한 디스크 공간 늘리기 , 941 페이지
- 디스크 공간 사용량 보기 및 할당 , 942 페이지
- 기타 할당량에 대한 디스크 공간 관리 , 942 페이지
- 디스크 공간에 대한 알림을 수신하는지 확인 , 943 페이지

(가상 어플라이언스 전용) 사용 가능한 디스크 공간 늘리기

ESXi 5.5 및 VMFS 5를 실행하는 가상 어플라이언스의 경우 2TB가 넘는 디스크 공간을 할당할 수 있습니다. ESXi 5.1을 실행하는 어플라이언스의 경우 제한은 2TB입니다.

가상 어플라이언스 인스턴스에 디스크 공간을 추가하려면

참고 디스크 공간 감소는 지원되지 않습니다. 자세한 내용은 VMware 문서를 참조하십시오.

시작하기 전에

필요한 디스크 공간 증가를 신중하게 결정합니다.

단계 **1** Email Security Appliance 인스턴스를 줄입니다.

단계 **2** VMware에서 제공하는 유틸리티 또는 관리 도구를 사용하여 디스크 공간을 늘립니다.

VMware 문서에서 가상 디스크 구성 변경에 대한 정보를 참조하십시오. 릴리스 당시 ESXi 5.5에 대한 이 정보는 http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html에서 제공했습니다.

단계 **3** **System Administration**(시스템 관리) > **Disk Management**(디스크 관리)로 이동하여 변경 사항이 적용되었는지 확인합니다.

디스크 공간 사용량 보기 및 할당

배포에서 사용하는 기능 가운데에서 어플라이언스에 디스크 공간을 할당하여 디스크 사용량을 최적화할 수 있습니다.

변경 후	수행해야 할 작업
• 디스크 공간 할당량 및 각 서비스에 대한 현재 사용량 보기 • 언제든 어플라이언스에 디스크 공간 재할당	**System Administration**(시스템 관리) > **Disk Management**(디스크 관리)로 이동합니다.
데이터 볼륨 관리	• 보고 및 추적 서비스와 스팸 격리의 경우 가장 오래된 데이터가 자동으로 삭제됩니다. • 정책, 바이러스 및 보안 침해 격리의 경우 격리에 구성된 기본 작업이 수행됩니다. 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 851 페이지를 참조하십시오. • 기타 할당량의 경우, 설정하게 될 새 할당량 아래로 사용량을 줄이려면 먼저 수동으로 데이터를 삭제해야 합니다. 기타 할당량에 대한 디스크 공간 관리 , 942 페이지를 참조하십시오.

기타 할당량에 대한 디스크 공간 관리

기타 할당량은 시스템 데이터 및 사용자 데이터를 포함합니다. 시스템 데이터는 삭제할 수 없습니다. 관리할 수 있는 사용자 데이터에는 다음과 같은 파일 유형이 포함됩니다.

관리할 내용	수행해야 할 작업
로그 파일	**System Administration**(시스템 관리) > **Log Subscriptions**(로그 서브스크립션)로 이동합니다. • 어떤 로그 디렉터리가 디스크 공간을 가장 많이 사용하는지 확인합니다. • 생성되고 있는 모든 로그 서브스크립션이 필요한지 확인합니다. • 로그 레벨이 필요 이상으로 자세하지 않은지 확인합니다. • 가능한 경우 롤오버 파일 크기를 줄입니다.
패킷 캡처	**Help and Support**(도움말 및 지원)(화면의 오른쪽 상단 근처) > **Packet Capture**(패킷 캡처)로 이동합니다.

관리할 내용	수행해야 할 작업
구성 파일 (이러한 파일은 디스크 공간 사용량이 많지 않을 수 있습니다.)	FTP를 통해 어플라이언스의 /data/pub 디렉터리로 이동합니다. 어플라이언스에 대한 FTP 액세스 구성 방법은 FTP, SSH 및 SCP 액세스, 1199 페이지를 참조하십시오.
할당량 크기	**System Administration**(시스템 관리) > **Disk Management**(디스크 관리)로 이동합니다.

디스크 공간에 대한 알림을 수신하는지 확인

Miscellaneous(기타) 디스크 사용량이 할당량의 75%에 도달하면 경고 레벨에서 시스템 알림을 수신하기 시작합니다. 이러한 알림을 받으면 조치를 취해야 합니다.

이러한 알림을 받도록 하려면 알림, 962 페이지 섹션을 참조하십시오.

디스크 공간 및 중앙 집중식 관리

디스크 공간 관리는 시스템 모드에서만 사용 가능하며, 그룹 또는 클러스터 모드에서는 사용할 수 없습니다.

Security Services 관리

Services Overview(서비스 개요) 페이지에는 다음 엔진의 현재 서비스 및 규칙 버전이 나열됩니다.

- 그레이메일
- McAfee
- Sophos

Services Overview(서비스 개요) 페이지에서 다음 작업을 수행할 수 있습니다.

- 엔진을 수동으로 업데이트합니다. 자세한 내용은 엔진 수동 업데이트, 944 페이지을 참조해 주십시오.
- 엔진의 이전 버전으로 롤백합니다. 자세한 내용은 이전 버전의 엔진으로 롤백, 944 페이지을 참조해 주십시오.

Auto Update(자동 업데이트) 열에는 특정 엔진의 자동 업데이트 상태가 표시됩니다. 자동 업데이트를 활성화하거나 비활성화하려면 특정 엔진의 **Global Settings**(전역 설정) 페이지로 이동합니다.

이제 특정 서비스 엔진에 대해 자동 업데이트가 비활성화된 경우 주기적으로 알림을 받을 수 있습니다. 알림 간격을 변경하려면 Security Services > Service updates(서비스 업데이트) 페이지의 **Alert Interval for Disabled Automatic Engine Updates**(자동 엔진 업데이트 비활성화에 대한 알림 간격) 옵션을 사용합니다.

참고 롤백이 적용되는 엔진에 대해서는 자동 업데이트가 자동으로 비활성화됩니다.

관련 주제

- 엔진 수동 업데이트, 944 페이지
- 이전 버전의 엔진으로 롤백, 944 페이지
- 로그 보기, 944 페이지
- 시스템 경보, 971 페이지

엔진 수동 업데이트

단계 **1** **Security Services** > **Services Overview(**서비스 개요**)** 페이지로 이동합니다.

단계 **2** 서비스 엔진의 최신 서비스 또는 규칙 버전에 대한 **Available Updates(**사용 가능한 업데이트**)** 열에서 **Update(**업데이트**)**를 클릭합니다.

참고 **Update (**업데이트**)** 옵션은 특정 엔진에 대해 새 업데이트를 사용할 수 있는 경우에만 사용할 수 있습니다.

이전 버전의 엔진으로 롤백

단계 **1** **Security Services** > **Services Overview(**서비스 개요**)** 페이지로 이동합니다.

단계 **2** **Modify Versions(**버전 수정**)** 열에서 **Change(**변경**)**를 클릭합니다.

단계 **3** 업데이트의 필수 규칙 및 서비스 버전을 선택하고 **Apply(**적용**)**를 클릭합니다.

어플라이언스가 이전 버전으로 엔진을 롤백합니다.

참고 서비스 업데이트에는 서비스 버전 및 규칙 버전이 패키지로 함께 포함됩니다.

Apply(적용**)**를 클릭하면 특정 엔진에 대한 자동 업데이트가 자동으로 비활성화됩니다. 자동 업데이트를 활성화하려면 특정 엔진의 Global Settings(전역 설정) 페이지로 이동합니다.

로그 보기

엔진 롤백 및 자동 업데이트 비활성화에 대한 정보는 다음 로그에 게시됩니다.

- **Updater Logs(**업데이터 로그**)**: 엔진 롤백 및 엔진 자동 업데이트에 대한 정보를 포함합니다. 대부분의 정보는 Info(정보) 또는 Debug(디버그) 레벨입니다.

  자세한 내용은 업데이트 로그 예, 1101 페이지를 참고하십시오.

서비스 업데이트

다음 서비스는 효과를 최대한 얻으려면 업데이트가 필요합니다.

- 기능 키
- McAfee Anti-Virus 정의
- PXE 엔진
- Sophos Anti-Virus 정의
- IronPort 안티스팸 규칙
- 보안 침해 필터 규칙
- 표준 시간대 규칙
- URL 범주(URL 필터링 기능에 사용됨. 자세한 내용은 향후 URL 범주 집합 변경 , 459 페이지 참조)
- 등록 클라이언트(URL 필터링 기능에 사용된 클라우드 기반 서비스와의 통신에 필요한 인증서 업데이트에 사용됨. 자세한 내용은 Cisco Web Security Services에 대한 연결 정보 , 428 페이지 참조)
- 그레이메일 규칙

참고 DLP 엔진 및 콘텐츠 일치 분류자에 대한 설정은 **Security Services(보안 서비스) > Data Loss Prevention(데이터 유출 방지)** 페이지에서 처리됩니다. 자세한 내용은 DLP 엔진 및 콘텐츠 일치 분류자 업데이트, 518 페이지를 참조하십시오.

DLP 업데이트를 제외하고, 업데이트를 수신하는 모든 서비스에 대해 서비스 업데이트 설정이 사용됩니다. DLP 업데이트를 제외한 개별 서비스에 대해서는 고유한 설정을 지정할 수 없습니다.

이런 중요한 업데이트를 얻을 수 있도록 네트워크와 어플라이언스를 설정하는 방법은 업그레이드 및 업데이트를 얻기 위한 설정 , 945 페이지 섹션을 참조하십시오.

업그레이드 및 업데이트를 얻기 위한 설정

업그레이드 및 업데이트 배포를 위한 옵션

AsyncOS 업그레이드 및 업데이트 파일을 어플라이언스에 배포하기 위한 몇 가지 방법이 있습니다.

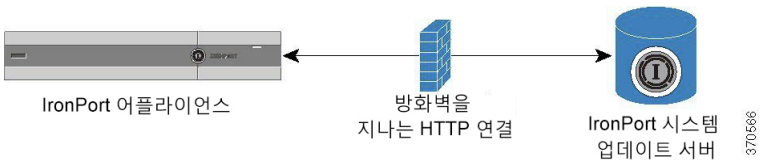
- 각 어플라이언스는 Cisco 업데이트 서버에서 직접 파일을 다운로드할 수 있습니다. 이것이 기본 방법입니다.
- Cisco에서 파일을 다운로드한 다음 네트워크 내 한 서버에서 여러 어플라이언스로 배포할 수 있습니다. 로컬 서버에서 업그레이드 및 업데이트, 947 페이지를 참조하십시오.

방법을 선택하고 구성하려면 업그레이드 및 업데이트 다운로드를 위한 서버 설정 구성 , 949 페이지 섹션을 참조하십시오.

Cisco 서버에서 업그레이드와 업데이트를 다운로드하도록 네트워크 구성

어플라이언스는 Cisco 업데이트 서버에 직접 연결하여 업그레이드와 업데이트를 찾고 다운로드합니다.

그림 ***73:*** 스트리밍 업데이트 방법



Cisco 업데이트 서버는 동적 IP 주소를 사용합니다. 엄격한 방화벽 정책이 있는 경우 대신 고정 위치를 구성해야 할 수 있습니다. 자세한 내용은 엄격한 방화벽 환경에서 업그레이드 및 업데이트를 위해 어플라이언스 구성, 946 페이지를 참고하십시오.

포트 80 및 443을 통해 Cisco 업데이트 서버에서 업그레이드를 다운로드하도록 허용하는 방화벽 규칙을 만듭니다.

엄격한 방화벽 환경에서 업그레이드 및 업데이트를 위해 어플라이언스 구성

Cisco IronPort 업그레이드 및 업데이트 서버는 동적 IP 주소를 사용합니다. 엄격한 방화벽 정책이 있는 경우 업데이트 및 AsyncOS 업그레이드를 위한 고정 위치를 구성해야 할 수 있습니다.

단계 **1** Cisco 고객 지원에 문의하여 고정 URL 주소를 얻습니다.

단계 **2** 포트 80을 통해 고정 IP 주소에서 업그레이드와 업데이트를 다운로드하도록 허용하는 방화벽 규칙을 만듭니다.

단계 **3** **Security Services**(서비스 보안) > **Service Updates**(서비스 업데이트)를 선택합니다.

단계 **4** **Edit Update Settings**(업데이트 설정 수정)를 클릭합니다.

단계 **5** Edit Update Settings(업데이트 설정 수정) 페이지의 "Update Servers(업데이트 서버)(이미지)" 섹션에서 Local Update Servers(로컬 업데이트 서버)를 선택하고, AsyncOS 업그레이드 및 McAfee Anti-Virus 정의용 Base URL(기본 URL) 필드에 1단계에서 수신한 고정 URL을 입력합니다.

단계 **6** "Update Servers(업데이트 서버)(목록)" 섹션에 대해 IronPort Update Servers(IronPort 업데이트 서버)가 선택되었는지 확인합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

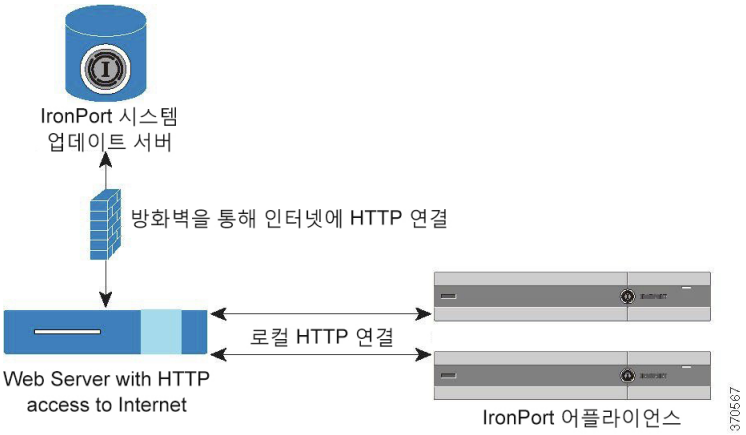
로컬 서버에서 업그레이드 및 업데이트

Cisco의 업데이트 서버에서 직접 업그레이드를 가져오는 대신 네트워크 내부로부터 AsyncOS 업그레이드 이미지를 로컬 서버 및 호스트 업그레이드로 다운로드할 수 있습니다. 이 기능을 사용하면 업그레이드 이미지가 HTTP를 통해 네트워크의 인터넷 액세스 가능한 서버로 다운로드됩니다. 업그레이드 이미지를 다운로드하기로 한 경우 AsyncOS 이미지를 어플라이언스로 호스트하도록 내부 HTTP 서버("업데이트 관리자")를 구성할 수 있습니다.

어플라이언스가 인터넷에 액세스할 수 없는 경우 또는 조직에서 다운로드에 사용되는 미러 사이트에 대한 액세스를 제한하는 경우 로컬 서버를 사용합니다. 로컬 서버에서 각 어플라이언스로 AsyncOS 업그레이드를 다운로드하는 것이 Cisco IronPort 서버에서 다운로드하는 것보다 일반적으로 더 빠릅니다.

참고 AsyncOS 업그레이드에 대한 로컬 서버만 사용하는 것이 좋습니다. 보안 업데이트 이미지에 로컬 업데이트 서버를 사용하는 경우 로컬 서버는 Cisco IronPort에서 보안 업데이트를 자동으로 수신하지 않으므로, 네트워크의 어플라이언스가 항상 최신 보안 서비스를 가지고 있지는 않을 수도 있습니다.

그림 ***74:*** 원격 업데이트 방법



단계 **1** 업그레이드 파일을 검색하여 제공하도록 로컬 서버를 구성합니다.

단계 **2** 업그레이드 파일을 다운로드합니다.

단계 **3** GUI의 **Security Services**(보안 서비스) **> Service Updates**(서비스 업데이트) 페이지 또는 CLI의 **updateconfig** 명령을 통해 로컬 서버를 사용하도록 어플라이언스를 구성합니다.

단계 **4** **System Administration**(시스템 관리) **> System Upgrade**(시스템 업그레이드) 페이지 또는 CLI의 upgrade 명령을 사용하여 어플라이언스를 업그레이드합니다.

로컬 서버에서 업그레이드 및 업데이트하기 위한 하드웨어 및 소프트웨어 요구 사항

AsyncOS 업그레이드 및 업데이트 파일을 다운로드하려면 다음이 지원되는 내부 네트워크의 시스템이 필요합니다.

- Cisco Systems 업데이트 서버에 대한 내부 액세스
- 웹 브라우저(브라우저 요구 사항, 11 페이지 참조)

참고 이 릴리스에서 이 주소에 대한 HTTP 액세스를 허용하도록 방화벽 설정을 구성해야 하는 경우, 특정 IP 주소가 아니라 DNS 이름을 사용하여 구성해야 합니다.

AsyncOS 업데이트 파일을 호스팅하려면 다음이 지원되는 내부 네트워크의 서버가 필요합니다.

- 다음과 같은 웹 서버(예: Microsoft IIS(Internet Information Services) 또는 Apache 오픈 소스 서버):
  - 24자가 넘는 디렉터리 또는 파일 이름의 표시 지원
  - 디렉터리 찾아보기 가능
  - 익명(인증 없음) 또는 기본("단순") 인증을 위해 구성됨
  - 각 AsyncOS 업데이트 이미지용 최소 350MB 빈 디스크 공간 포함

로컬 서버에 업그레이드 이미지 호스트

로컬 서버를 설정한 후 http://updates.ironport.com/fetch_manifest.html로 이동하여 업그레이드 이미지의 ZIP 파일을 다운로드합니다. 이미지를 다운로드하려면 어플라이언스의 일련 번호(물리적 어플라이언스용) 또는 VLN(가상 어플라이언스용) 및 버전 번호를 입력합니다. 그러면 사용 가능한 업그레이드 목록이 표시됩니다. 다운로드할 업그레이드 버전을 클릭하고, 디렉터리 구조를 유지한 채 로컬 서버의 루트 디렉터리에 ZIP 파일의 압축을 해제합니다. 업그레이드 이미지를 사용하려면, Edit Update Settings(업데이트 설정 수정) 페이지(또는 CLI의 updateconfig)에서 로컬 서버를 사용하도록 어플라이언스를 구성합니다.

로컬 서버는 또한 네트워크의 어플라이언스에 대해 사용 가능한 AsyncOS 업그레이드를 다운로드된 업그레이드 이미지로 제한하는 XML 파일을 호스트합니다. 이 파일을 "매니페스트"라고 합니다. 매니페스트는 업그레이드 이미지 ZIP 파일의 asyncos 디렉터리에 있습니다. 로컬 서버의 루트 디렉터리

에 있는 ZIP 파일의 압축을 해제한 후 Edit Update Settings(업데이트 설정 수정) 페이지(또는 CLI의 updateconfig)에서 파일 이름을 포함한 XML 파일의 전체 URL을 입력합니다.

원격 업그레이드에 대한 자세한 내용은 기술 자료를 참고하거나, Cisco 지원 공급업체에 문의하십시오.

프록시 서버를 통한 업데이트

어플라이언스는 기본적으로 Cisco의 업데이트 서버에 직접 연결하여 업데이트를 수신하도록 구성되어 있습니다. 이 연결은 포트 80에서 HTTP에 의해 이루어지며 내용이 암호화됩니다. 방화벽에서 이 포트를 열지 않으려면, 어플라이언스가 업데이트 규칙을 수신할 수 있는 프록시 서버 및 특정 포트를 정의할 수 있습니다.

프록시 서버를 사용하기로 한 경우 선택적인 인증 및 포트를 지정할 수 있습니다.

참고 프록시 서버를 정의하면, 프록시 서버를 사용하도록 구성된 모든 서비스 업데이트에 대해 자동으로 사용됩니다. 개별 서비스에 대한 업데이트용 프록시 서버를 끌 수 있는 방법은 없습니다.

업그레이드 및 업데이트 다운로드를 위한 서버 설정 구성

업그레이드와 업데이트를 어플라이언스로 다운로드하는 데 필요한 서버 및 연결 정보를 지정합니다.

AsyncOS 업그레이드 및 서비스 업데이트에 대해 같은 설정을 사용할 수도 있고 서로 다른 설정을 사용할 수도 있습니다.

시작하기 전에

어플라이언스가 Cisco에서 직접 업그레이드와 업데이트를 다운로드하도록 할지, 아니면 네트워크의 로컬 서버에서 이러한 이미지를 호스트할지를 결정합니다. 그런 다음 선택한 방법을 지원하도록 네트워크를 설정합니다. 업그레이드 및 업데이트를 얻기 위한 설정 , 945 페이지 아래의 모든 항목을 참조하십시오.

단계 **1** **Security Services(**서비스 보안**) > Service Updates(**서비스 업데이트**)**를 선택합니다.

단계 **2** **Edit Update Settings(**업데이트 설정 수정**)**를 클릭합니다.

단계 **3** 옵션을 입력합니다.

설정	설명
Update Servers(업데이트 서버**)(**이미지**)**	Cisco IronPort AsyncOS 업그레이드 이미지와 서비스 업데이트를 Cisco IronPort 업데이트 서버에서 다운로드할지, 아니면 네트워크의 로컬 서버에서 다운로드할지를 선택합니다. 기본값은 업그레이드와 업데이트를 모두 Cisco IronPort 업데이트 서버에서 다운로드하는 것입니다. 업그레이드와 업데이트에 동일한 설정을 사용하려면 보이는 필드에 정보를 입력합니다. 로컬 업데이트 서버를 선택하는 경우 업그레이드와 업데이트를 다운로드하는 데 사용되는 서버에 대한 기본 URL 및 포트 번호를 입력합니다. 서버에 인증이 필요한 경우 유효한 사용자 이름과 암호를 입력할 수도 있습니다. AsyncOS 업그레이드 및 McAfee Anti-Virus 정의에 대해서만 다른 설정을 입력하려면 **Click to use different settings for AsyncOS(**클릭하여 **AsyncOS**에 대해 다른 설정 사용**)** 링크를 클릭합니다. 참고 Cisco Intelligent Multi-Scan의 경우 서드파티 안티 스팸 규칙에 대한 업데이트를 다운로드하는 데 두 번째 로컬 서버가 필요합니다.
업데이트 서버(목록)	각 어플라이언스에서 배포에 적합한 업그레이드 및 업데이트만 사용할 수 있도록 하기 위해 Cisco IronPort는 관련 파일의 매니페스트 목록을 생성합니다. 사용 가능한 업그레이드 및 서비스 업데이트 목록을 Cisco IronPort 업데이트 서버에서 다운로드할지, 아니면 네트워크의 로컬 서버에서 다운로드할지를 선택합니다. 업데이트 및 AsyncOS 업그레이드용 서버를 지정하기 위한 별도의 섹션이 있습니다. 업그레이드 및 업데이트에 대한 기본값은 Cisco IronPort 업데이트 서버입니다. 로컬 업데이트 서버를 선택하는 경우, 파일 이름과 서버의 HTTP 포트 번호를 포함하여 각 목록에 대한 매니페스트 XML 파일의 전체 경로를 입력합니다. 포트 필드를 비워두면 AsyncOS에서는 포트 80을 사용합니다. 서버에 인증이 필요한 경우 유효한 사용자 이름과 암호를 입력합니다.
자동 업데이트	Sophos 및 McAfee Anti-Virus 정의, Cisco Anti-Spam 규칙, Cisco Intelligent Multi-Scan 규칙, PXE Engine 업데이트, 보안 침해 필터 규칙, 표준 시간대 규칙에 대한 자동 업데이트 및 업데이트 간격(어플라이언스가 업데이트를 확인하는 빈도)을 활성화합니다. 끝에 오는 s, m 또는 h는 초, 분 또는 시간을 나타냅니다. 자동 업데이트를 비활성화하려면 영(0)을 입력합니다. 참고 DLP에 대한 자동 업데이트를 켜려면 **Security Services(**보안 서비스**) > Data Loss Prevention(**데이터 유출 방지**)** 페이지를 사용해야 합니다. 그러나 먼저 모든 서비스에 대해 자동 업데이트를 활성화해야 합니다. 자세한 내용은 DLP 엔진 및 콘텐츠 일치 분류자 업데이트, 518 페이지를 참조하십시오.

설정	설명
자동 엔진 업데이트 비활성화에 대한 알림 간격	특정 엔진에 대한 '자동 업데이트' 기능이 비활성화될 때 전송할 경고의 구체적 빈도를 입력합니다. 뒤에 m, h 또는 d를 포함하여 월, 시간 또는 일을 나타냅니다. 기본값은 30일입니다.
Interface(인터페이스**)**	나열된 보안 구성 요소 업데이트에 대한 업데이트 서버에 연결할 때 사용할 네트워크 인터페이스를 선택합니다. 사용 가능한 프록시 데이터 인터페이스가 표시됩니다. 기본적으로 어플라이언스는 사용할 인터페이스를 선택합니다.
HTTP 프록시 서버**:**	GUI에 나열된 서비스에 사용되는 선택적인 프록시 서버. 프록시 서버를 지정하면 모든 서비스를 업데이트하는 데 사용됩니다.
HTTPS Proxy Server((HTTPS 프록시 서버**)**	HTTPS를 사용하는 선택적인 프록시 서버. HTTPS 프록시 서버를 정의하면 GUI에 나열된 서비스를 업데이트하는 데 사용됩니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

자동 업데이트 구성

단계 **1** **Security Services(**보안 서비스**) > Service Updates(**서비스 업데이트**)** 페이지로 이동하여 **Edit Update Settings(**업데이트 설정 수정**)**를 클릭합니다.

단계 **2** 자동 업데이트를 활성화하기 위한 확인란을 선택합니다.

단계 **3** 업데이트 간격(업데이트 확인 사이에 대기하는 시간)을 입력합니다. 분에는 **m**, 시간에는 **h**를 끝에 추가합니다. 최대 업데이트 간격은 1시간입니다.

업데이터 서버 인증서의 유효성을 확인하도록 어플라이언스 구성

Email Security Appliance는 업데이터 서버와 통신할 때마다 Cisco 업데이터 서버 인증서의 유효성을 확인할 수 있습니다. 이 옵션을 구성하고 확인에 실패하면, 업데이트가 다운로드되지 않으며 세부사항이 업데이터 로그에 기록됩니다.

이 옵션을 구성하려면 updateconfig 명령을 사용합니다. 다음 예에서는 이 옵션을 구성하는 방법을 보여 줍니다.

```
mail.example.com> updateconfig
Service (images):                                   Update URL:
-------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
```

```
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Service (list):                                     Update URL:
-----------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Service (list):                                     Update URL:
-----------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> validate_certificates
Should server certificates from Cisco update servers be validated?
[Yes]>
Service (images):                                   Update URL:
-----------------------------------------------------------------------------------------
Feature Key updates                                 http://downloads.ironport.com/asyncos
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Service (list):                                     Update URL:
-----------------------------------------------------------------------------------------
Timezone rules                                      Cisco IronPort Servers
Enrollment Client Updates                           Cisco IronPort Servers
Support Request updates                             Cisco IronPort Servers
Service (list):                                     Update URL:
-----------------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades                     Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>
```

프록시 서버 통신을 신뢰하도록 어플라이언스 구성

투명하지 않은 프록시 서버를 사용 중인 경우, 프록시 인증서 서명에 사용된 CA 인증서를 어플라이언스에 추가할 수 있습니다. 그렇게 함으로써 어플라이언스는 프록시 서버 통신을 신뢰합니다.

이 옵션을 구성하려면 updateconfig 명령을 사용합니다. 다음 예에서는 이 옵션을 구성하는 방법을 보여 줍니다.

```
mail.example.com> updateconfig
...
...
...
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> trusted_certificates
Choose the operation you want to perform:
```

```
- ADD - Upload a new trusted certificate for updates.
[]> add
Paste certificates to be trusted for secure updater connections, blank to quit
Trusted Certificate for Updater:
Paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MMIICiDCCAfGgAwIBAgIBATANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCSU4x
DDAKBgNVBAgTA0tBUjENM.....................................
-----END CERTIFICATE-----
.
Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]>
```

AsyncOS 업그레이드

프로시저

	명령 또는 동작	목적
단계 **1**	아직 하지 않았으면, 모든 업데이트 및 업그레이드 다운로드에 적용되는 설정을 구성하고, 지원할 네트워크를 설정하고, 선택적으로 이러한 다운로드를 배포합니다.	업그레이드 및 업데이트를 얻기 위한 설정 , 945 페이지
단계 **2**	언제 업그레이드를 사용할 수 있는지를 이해하고 설치 여부를 결정합니다.	사용 가능한 업그레이드 알림, 953 페이지
단계 **3**	각 업그레이드 전에 필수 및 권장 작업을 수행합니다.	AsyncOS 업그레이드 준비, 954 페이지 클러스터에서 시스템 업그레이드, 1129 페이지
단계 **4**	업그레이드를 수행합니다.	업그레이드 다운로드 및 설치 , 955 페이지

클러스터링된 시스템 업그레이드 정보

클러스터링된 시스템을 업그레이드하려는 경우 클러스터에서 시스템 업그레이드, 1129 페이지 섹션을 참조하십시오.

업그레이드 절차의 배치 명령 정보

업그레이드 절차를 위한 배치 명령은 *AsyncOS for Cisco Email Security Appliances CLI* 참조 가이드 (http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html)에 나와 있습니다.

사용 가능한 업그레이드 알림

기본적으로 관리자 및 기술자 권한이 있는 사용자는 어플라이언스에서 AsyncOS 업그레이드를 사용할 수 있을 때 웹 인터페이스 상단에 표시되는 알림을 볼 수 있습니다.

클러스터링된 시스템에서는 사용자가 로그인한 시스템에만 작업이 적용됩니다.

변경 후	수행해야 할 작업
최신 업그레이드에 대한 자세한 정보 보기	업그레이드 알림 위에 마우스를 올려놓습니다.
사용 가능한 업그레이드 목록 보기	알림에서 아래쪽 화살표를 클릭합니다.
현재 알림 해제. 새 업그레이드를 사용할 수 있을 때까지 어플라이언스에 또 다른 알림이 표시되지 않습니다.	아래쪽 화살표를 클릭하고 **Clear the notification(**알림 지우기**)**을 선택한 다음 **Close(**닫기**)**를 클릭합니다.
앞으로의 알림 방지(사용자 및 관리자 권한만 가능)	**Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > System Upgrade(**시스템 업그레이드**)**로 이동합니다.

사용 가능한 업그레이드 알림

기본적으로 관리자 및 기술자 권한이 있는 사용자는 어플라이언스에서 AsyncOS 업그레이드를 사용할 수 있을 때 웹 인터페이스 상단에 표시되는 알림을 볼 수 있습니다.

클러스터링된 시스템에서는 사용자가 로그인한 시스템에만 작업이 적용됩니다.

변경 후	수행해야 할 작업
최신 업그레이드에 대한 자세한 정보 보기	업그레이드 알림 위에 마우스를 올려놓습니다.
사용 가능한 업그레이드 목록 보기	알림에서 아래쪽 화살표를 클릭합니다.
현재 알림 해제. 새 업그레이드를 사용할 수 있을 때까지 어플라이언스에 또 다른 알림이 표시되지 않습니다.	아래쪽 화살표를 클릭하고 **Clear the notification(**알림 지우기**)**을 선택한 다음 **Close(**닫기**)**를 클릭합니다.
앞으로의 알림 방지(사용자 및 관리자 권한만 가능)	**Management Appliance(**관리 어플라이언스**) > System Administration(**시스템 관리**) > System Upgrade(**시스템 업그레이드**)**로 이동합니다.

AsyncOS 업그레이드 준비

다음 단계를 수행하여 업그레이드를 준비하는 것이 가장 좋은 방법입니다.

시작하기 전에

작업 대기열에 있는 모든 메시지를 지웁니다. 작업 대기열을 지우지 않으면 업그레이드를 수행할 수 없습니다.

단계 **1** XML 컨피그레이션 파일을 오프박스에 저장합니다. 어떤 이유로든 이전 업그레이드 릴리스로 돌아가야 할 경우 이 파일이 필요합니다.

단계 **2** 허용 목록/차단 목록 기능을 사용 중인 경우 목록을 오프박스로 내보냅니다.

단계 **3** 모든 리스너를 일시 중단합니다. CLI에서 업그레이드를 수행하는 경우 suspendlistener 명령을 사용합니다. GUI에서 업그레이드를 수행하는 경우 리스너가 자동으로 일시 중단됩니다.

단계 **4** 대기열이 비워질 때까지 기다립니다. 작업 대기열에 있는 메시지의 수를 보려면 CLI의 workqueue 명령을 사용하고, 어플라이언스에서 메시지 처리량을 모니터링하려면 rate 명령을 사용합니다.

참고 업그레이드 후 리스너를 다시 활성화합니다.

업그레이드 다운로드 및 설치

다운로드와 설치를 동시에 수행할 수도 있고, 백그라운드에서 다운로드한 후 나중에 설치할 수도 있습니다.

참고 Cisco IronPort 서버가 아니라 로컬 서버에서 AsyncOS의 다운로드와 업그레이드를 동시에 수행하는 경우, 다운로드 중에 업그레이드가 즉시 설치됩니다. 업그레이드 프로시스 시작 시 10초 동안 배너가 표시됩니다. 이 배너가 표시되어 있을 때, Ctrl-C를 입력하면 다운로드가 시작되기 전 업그레이드 프로세스를 종료할 수 있습니다.

시작하기 전에

- Cisco에서 업그레이드를 직접 다운로드할지, 아니면 네트워크의 서버에서 업그레이드 이미지를 호스트할지를 선택합니다. 그런 다음 선택한 방법을 지원하도록 네트워크를 설정합니다. 그런 다음 선택한 소스에서 업그레이드를 가져오도록 어플라이언스를 구성합니다. 업그레이드 및 업데이트를 얻기 위한 설정 , 945 페이지 및 업그레이드 및 업데이트 다운로드를 위한 서버 설정 구성 , 949 페이지를 참조하십시오.
- 지금 업그레이드를 설치하려면 AsyncOS 업그레이드 준비, 954 페이지의 지침을 수행합니다.
- 클러스터링된 시스템에서 업그레이드를 설치하려면 클러스터에서 시스템 업그레이드, 1129 페이지 섹션을 참조하십시오.
- 업그레이드를 다운로드만 하려는 경우 설치 준비가 될 때까지 아무런 전제 조건도 없습니다.

단계 **1** **System Administration**(시스템 관리) > **System Upgrade**(시스템 업그레이드)를 선택합니다.

단계 **2** **Upgrade Options**(업그레이드 옵션)를 클릭합니다.

시스템은 상태 로그의 기록 데이터(최대 3개월)를 분석하여 어플라이언스의 상태를 확인하고, 어플라이언스를 업그레이드할 수 있는지에 대한 권장 사항을 제공합니다.

참고 시스템이 이 분석을 수행하려면 시스템 로그에 최대 1개월 분량의 로깅 데이터가 포함되어 있어야 합니다.

단계 **3** 분석 결과에 따라 다음 중 하나를 수행합니다.

- 지난 몇 개월 동안 시스템에서 다음 문제 중 하나가 발생한 것이 분석에서 탐지되는 경우 표시된 권장 사항을 따릅니다.
  - 리소스 절약 모드
  - 메일 프로세스의 지연
  - 높은 CPU 사용률
  - 높은 메모리 사용률
  - 높은 메모리 페이지 스와핑
- 상태 로그의 데이터가 부족하여 시스템에 분석을 수행할 수 없는 경우 권장 사항이 제공되지 않습니다. 이 시나리오에서는 최근에 어플라이언스에 아무 문제도 발생하지 않은 경우에만 어플라이언스의 업그레이드를 고려하십시오.
- 분석에서 아무 문제도 탐지되지 않으면 4단계로 이동합니다.

단계 **4** 옵션을 선택합니다.

변경 후	수행해야 할 작업
업그레이드의 다운로드 및 설치를 한 번에 진행	**Download and Install(**다운로드 및 설치**)**을 클릭합니다. 이미 설치 프로그램을 다운로드한 경우 기존 다운로드를 덮어쓴다는 메시지가 표시됩니다.
업그레이드 설치 프로그램 다운로드	**Download only(**다운로드만**)**를 클릭합니다. 이미 설치 프로그램을 다운로드한 경우 기존 다운로드를 덮어쓴다는 메시지가 표시됩니다. 서비스 중단 없이 설치 프로그램이 백그라운드에서 다운로드됩니다.
다운로드한 업그레이드 설치 프로그램 설치	**Install(**설치**)**을 클릭합니다. 설치 프로그램이 다운로드된 경우에만 이 옵션이 나타납니다. 설치될 AsyncOS 버전이 Install(설치) 옵션 아래에 표시됩니다.

단계 **5** 전에 다운로드한 설치 프로그램을 설치하지 않은 경우 사용 가능한 업그레이드 목록에서 AsyncOS 버전을 선택합니다.

단계 **6** 설치 중인 경우

a) 현재 구성을 어플라이언스의 configuration 디렉터리에 저장할지 여부를 선택합니다.

b) 구성 파일에서 암호를 마스크 처리할지 여부를 선택합니다.

참고 마스킹된 암호의 구성 파일은 GUI의 Configuration File(구성 파일) 페이지 또는 CLI의 loadconfig 명령으로 로드할 수 없습니다.

c) 구성 파일의 복사본을 이메일로 전송하려면 해당 이메일 주소를 입력합니다. 여러 이메일 주소를 입력하는 경우 쉼표를 사용하여 구분합니다.

단계 **7** **Proceed(**진행**)**를 클릭합니다.

단계 **8** 설치 중인 경우

a) 프로세스 중에 프롬프트에 응답할 준비를 합니다.

응답할 때까지 프로세스가 일시 중지됩니다.

페이지 상단 근처에 진행률 표시줄이 나타납니다.

b) 프롬프트에서 **Reboot Now**(지금 재부팅)를 클릭합니다.

c) 약 10분 후에 어플라이언스에 다시 액세스하여 로그인합니다.

업그레이드 문제 해결을 위해 어플라이언스의 전원을 껐다가 켜야 하는 경우 재부팅 후 적어도 20분이 지난 후에 그렇게 하십시오.

다음에 수행할 작업

- 프로세스가 중단된 경우 프로세스를 다시 시작해야 합니다.
- 업그레이드를 다운로드했지만 설치하지 않은 경우:

  업그레이드를 설치할 준비가 되면 '시작하기 전에' 섹션의 전제 조건을 포함하여 처음부터 이러한 지침을 수행하되, Install(설치) 옵션을 선택합니다.

- 업그레이드를 설치한 경우:
  - 리스너를 다시 활성화(다시 시작)합니다.
  - 새 시스템용 컨피그레이션 파일을 저장합니다. 자세한 내용은 구성 파일 관리, 935 페이지를 참조하십시오.
- 업그레이드가 완료되면 리스너를 다시 활성화합니다.

백그라운드 다운로드 상태 보기, 취소 또는 삭제

단계 **1** **System Administration**(시스템 관리) > **System Upgrade**(시스템 업그레이드)를 선택합니다.

단계 **2** **Upgrade Options**(업그레이드 옵션)를 클릭합니다.

단계 **3** 옵션을 선택합니다.

변경 후	수행해야 할 작업
다운로드 상태 보기	페이지 중간 부분을 살펴봅니다. 진행 중인 다운로드가 없으며 설치를 기다리는 완료된 다운로드가 없으면 다운로드 상태 정보가 표시되지 않습니다.
다운로드 취소	페이지 중간에 있는 **Cancel Download**(다운로드 취소) 버튼을 클릭합니다. 이 옵션은 다운로드가 진행 중인 경우에만 나타납니다.
다운로드된 설치 프로그램 삭제	페이지 중간의 **Delete File**(파일 삭제) 버튼을 클릭합니다. 설치 프로그램이 다운로드된 경우에만 이 옵션이 나타납니다.

단계 **4** (선택 사항) 업그레이드 로그를 봅니다.

원격 전원 제어 활성화

어플라이언스 섀시에 대한 전원을 원격으로 재설정하는 기능은 80- 및 90- 시리즈 하드웨어에서만 사용 가능합니다.

어플라이언스 전원을 원격으로 재설정하려면 이 섹션에 설명된 절차를 사용하여 미리 이 기능을 활성화 및 구성해야 합니다.

시작하기 전에

- RPC(전용 원격 전원 제어) 포트를 안전한 네트워크에 직접 연결합니다. 자세한 내용은 Hardware Installation Guide를 참조하십시오.
- 어플라이언스에 원격에서 액세스 가능한지 확인합니다. 예를 들어 방화벽을 통해 필요한 포트를 엽니다.
- 이 기능을 사용하려면 전용 원격 전원 제어 인터페이스에 대한 고유한 IPv4 주소가 필요합니다. 이 인터페이스는 이 섹션에 설명된 절차를 통해서만 구성 가능하며, **ipconfig** 명령을 사용하여 구성할 수 없습니다.
- 어플라이언스 전원을 껐다가 켜려면 IPMI(Intelligent Platform Management Interface) 버전 2.0을 지원하는 디바이스를 관리할 수 있는 서드파티 툴이 필요합니다. 그러한 툴을 사용할 준비가 되었는지 확인합니다.
- CLI(Command Line Interface)에 액세스하는 방법에 대한 자세한 내용은 CLI 참조 가이드를 참조하십시오.

단계 **1** SSH 또는 직렬 콘솔 포트를 사용하여 CLI에 액세스합니다.

단계 **2** 관리자 액세스 권한이 있는 계정을 사용하여 로그인합니다.

단계 **3** 다음과 같은 명령을 입력합니다.

```
remotepower
setup
```

단계 **4** 프롬프트를 따라 다음을 지정합니다.

1. 이 기능의 전용 IP 주소와 넷마스크 및 게이트웨이.
2. power-cycle 명령을 실행하는 데 필요한 사용자 이름과 암호.

   이러한 자격 증명은 어플라이언스에 액세스하는 데 사용되는 다른 자격 증명과 다릅니다.

단계 **5** Commit을 입력하여 변경 사항을 저장합니다.

단계 **6** 구성을 테스트하여 어플라이언스 전원을 원격으로 관리할 수 있는지 확인합니다.

단계 **7** 입력한 자격 증명을 불확실한 미래에 사용할 수 있는지 확인합니다. 예를 들면 이 정보를 안전한 곳에 보관하고, 이 작업을 수행해야 하는 관리자가 필요한 자격 증명에 액세스할 수 있는지 확인합니다.

다음에 수행할 작업

관련 주제

- 어플라이언스 전원 원격 초기화 , 1170 페이지

AsyncOS의 이전 버전으로 복귀

AsyncOS에는 긴급한 용도로 AsyncOS 운영 체제를 이전의 정식 빌드로 복귀할 수 있는 기능이 포함되어 있습니다.

복귀 영향력

어플라이언스에서 revert 명령을 사용하는 것은 매우 위험합니다. 이 명령을 사용하면 모든 컨피그레이션 로그와 데이터베이스가 삭제됩니다. 관리 인터페이스에 대한 네트워크 정보만 보존되고 다른 모든 네트워크 컨피그레이션은 삭제됩니다. 또한 복귀할 경우 어플라이언스를 다시 구성할 때까지 메일 처리가 중단됩니다. revert 명령을 실행하면 네트워크 컨피그레이션이 소멸되므로, 이 명령을 실행하려면 어플라이언스에 대한 물리적 로컬 액세스가 필요할 수 있습니다.

⚠

주의 복귀할 버전의 컨피그레이션 파일이 있어야 합니다. 컨피그레이션 파일은 이전 버전과 호환되지 않습니다.

가상 어플라이언스에서 AsyncOS를 복귀하면 라이센스에 영향이 미칠 수 있음

AsyncOS 9.0 for Email에서 AsyncOS 8.5 for Email로 복귀하면 라이센스가 변경되지 않습니다.

AsyncOS 9.0 for Email에서 AsyncOS 8.0 for Email로 복귀하면, 어플라이언스가 보안 기능 없이 메일을 전달하는 동안 180일의 유예 기간이 더 이상 제공되지 않습니다.

두 경우 모두 기능 키 만료 날짜가 변경되지 않습니다.

관련 주제

- 가상 어플라이언스 라이센스 만료 , 935 페이지

AsyncOS 복귀

단계 **1** 복귀할 버전의 컨피그레이션 파일이 있는지 확인합니다. 컨피그레이션 파일은 이전 버전과 호환되지 않습니다. 이렇게 하려면 이메일을 통해 파일을 자신에게 전송하거나 FTP를 통해 파일을 올릴 수 있습니다. 자세한 내용은 컨피그레이션 파일 메일로 전송, 937 페이지를 참조하십시오.

단계 **2** 어플라이언스의 현재 구성의 백업 복사본을 다른 시스템에 저장합니다(암호 마스킹 없이).

참고 이것은 복귀 후 로드할 구성 파일이 아닙니다.

단계 **3** 허용 목록/차단 목록 기능을 사용하는 경우 허용 목록/차단 목록 데이터베이스를 다른 시스템에 저장합니다.

단계 **4** 메일 대기열이 비워질 때까지 기다립니다.

단계 **5** 복귀할 어플라이언스의 CLI에 로그인합니다.

revert 명령을 실행하면 몇 가지 경고 프롬프트가 표시됩니다. 이러한 경고 프롬프트에 동의하면 즉시 복귀 작업이 수행됩니다. 따라서 복귀 전 단계를 완료하기 전에는 복귀 프로세스를 시작하지 마십시오.

단계 **6** CLI에서 **revert** 명령을 실행합니다.

참고 복귀 프로세스는 시간이 많이 걸리는 작업입니다. 복귀가 완료될 때까지 15분에서 20분 정도 소요될 수 있으며, 어플라이언스에 대한 콘솔 액세스가 다시 사용 가능해집니다.

단계 **7** 어플라이언스가 두 번 재부팅될 때까지 기다립니다.

단계 **8** 시스템이 두 번 재부팅되면 직렬 콘솔에서 **interfaceconfig** 명령을 사용하여 액세스 가능한 IP 주소의 인터페이스를 구성합니다.

단계 **9** 구성된 인터페이스 중 하나에서 FTP 또는 HTTP를 활성화합니다.

단계 **10** 만든 XML 컨피그레이션 파일을 FTP에 올리거나 GUI 인터페이스에 붙여넣습니다.

단계 **11** 복귀하려는 버전의 XML 컨피그레이션 파일을 로드합니다.

단계 **12** 허용 목록/차단 목록 기능을 사용하는 경우 허용 목록/차단 목록 데이터베이스를 가져오고 복원합니다.

단계 **13** 변경 사항을 커밋합니다.

복귀된 어플라이언스가 이제 선택한 AsyncOS 버전을 사용하여 실행됩니다.

어플라이언스 생성 메시지에 대한 반환 주소 구성

다음 환경에 대해 AsyncOS에 의해 생성된 메일의 봉투 발신자를 구성할 수 있습니다.

- 안티바이러스 알림
- 반송
- DMARC 피드백
- 알림(notify() 및 notify-copy() 필터 작업)
- 격리 알림(그리고 격리 관리의 "Send Copy")
- 보고서
- 기타 모든 메시지

반환 주소의 표시, 사용자 및 도메인 이름을 지정할 수 있습니다. 도메인 이름에 가상 게이트웨이 도메인을 사용하도록 선택할 수도 있습니다.

GUI에서 또는 CLI에서 addressconfig 명령을 사용하여 시스템 생성 이메일 메시지에 대한 반환 주소를 수정할 수 있습니다.

단계 **1** System Administration(시스템 관리) > Return Addresses(반환 주소) 페이지로 이동합니다.

단계 **2** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** 수정할 주소를 변경합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

시스템 상태 파라미터에 대한 임계값 설정

조직의 요구 사항에 따라 CPU 사용량, 작업 대기열의 최대 메시지 수 등 어플라이언스의 다양한 상태 매개변수에 대한 임계값을 구성할 수 있습니다. 지정된 임계값을 초과할 때 알림을 전송하도록 어플라이언스를 구성할 수도 있습니다.

참고 시스템 상태 파라미터의 임계값을 구성하려면 CLI의 healthconfig 명령을 사용합니다. 자세한 내용은 CLI 인라인 도움말 또는 *AsyncOS for Cisco Email Security Appliance CLI* 참조 가이드를 참고하십시오.

시작하기 전에

임계값을 신중하게 결정합니다.

단계 **1** **System Administration(**시스템 관리**)** > **System Health(**시스템 상태**)**를 클릭합니다.

단계 **2** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** 다음 옵션을 구성합니다.

- CPU 사용량의 임계값 레벨을 지정합니다(백분율로).

  또한 현재 CPU 사용량이 구성된 임계값을 초과할 때 알림을 수신할지 여부를 지정합니다. 첫 번째 알림이 전송된 후 15분이 지나 CPU 사용량이 첫 번째 알림을 트리거한 시점의 평균을 5퍼센트 초과하면 추가 알림이 전송됩니다.

  참고 이러한 알림은 메일 처리 프로세스의 CPU 사용량만을 기준으로 트리거됩니다.

- 메모리 페이지 스와핑에 대한 임계값 수준(백분율 단위)을 지정합니다.

  또한 전체 메모리 스왑 사용량이 구성된 임계값을 초과할 때 알림을 수신할지 여부를 지정합니다. 첫 번째 알림이 전송된 후 15분 내에 메모리 페이지 스와핑이 첫 번째 알림을 트리거한 값을 150퍼센트 초과하면 추가 알림이 전송됩니다. 예를 들어, 임계값이 10으로 설정된 경우

  - 메모리 스왑 사용량이 10.1%에 도달하면 첫 번째 알림이 전송됩니다.
  - 메모리 스왑 사용량이 15분 내에 15.1%에 도달하면 하나 이상의 알림이 전송됩니다.

- 작업 대기열의 최대 메시지 수에 대한 임계값 레벨을 지정합니다(메시지 수 단위로).

  또한 작업 대기열의 메시지 수가 구성된 임계값을 초과할 때 알림을 수신할지 여부를 지정합니다. 첫 번째 알림이 전송된 후 15분 내에 작업 대기열의 최대 메시지 수가 첫 번째 알림을 트리거한 값을 150퍼센트 초과하면 추가 알림이 전송됩니다. 예를 들어 임계값이 1000으로 설정된 경우

  - 작업 대기열의 최대 메시지 수가 1002에 도달하면 첫 번째 알림이 전송됩니다.
  - 15분 내에 작업 대기열의 최대 메시지 수가 1510에 도달하면 또 다른 알림이 전송됩니다.

참고 이 기능의 모든 알림은 시스템 알림 범주에 속합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

다음에 수행할 작업

이 기능에 대한 알림을 구성했으면 시스템 알림을 구독하도록 설정했는지 확인합니다. 자세한 내용은 알림 수신자 추가, 964 페이지 섹션을 참조하십시오.

Email Security Appliance의 상태 확인

상태 확인 기능을 사용하여 Email Security Appliance의 상태를 확인할 수 있습니다. 상태 확인을 실행하면 시스템은 현재 상태 로그에서 기록 데이터를 분석하여(최대 3개월) 어플라이언스의 상태를 판단합니다.

참고 시스템이 이 분석을 수행하려면 시스템 로그에 최대 1개월 분량의 로깅 데이터가 포함되어 있어야 합니다.

상태 확인을 실행하려면

- 웹 인터페이스에서 **System Administration**(시스템 관리) > **System Health**(시스템 상태) 페이지로 이동하여 **Run Health Check**(상태 확인 실행)를 클릭합니다.
- CLI에서 **`healthconfig`** 명령을 실행합니다.

지난 몇 개월 동안 시스템에서 다음 문제 중 하나가 발생했는지가 분석 결과에 나타납니다.

- 리소스 절약 모드
- 메일 프로세스의 지연
- 높은 CPU 사용률
- 높은 메모리 사용률
- 높은 메모리 페이지 스와핑

상태 검사 결과 어플라이언스에 위의 문제 중 하나 이상이 발생한 것으로 나타나면 시스템 컨피그레이션을 검토하고 조정하는 것이 좋습니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118881-technote-esa-00.html 을 참고하십시오.

알림

알림 메시지는 어플라이언스에서 발생하는 이벤트에 대한 정보를 포함하는 자동으로 생성된 표준 이메일 메시지입니다. 이러한 이벤트는 중요도(또는 심각도) 레벨이 낮음에서 높음까지 다양할 수 있으며, 일반적으로 어플라이언스의 특정 구성 요소 또는 기능과 관련이 있습니다. 알림은 어플라이언스에 의해 생성됩니다. 어떤 알림 메시지를 어떤 사용자에게 전송할지, 이벤트의 어떤 심각도에서 전

송할지를 훨씬 더 세부적인 레벨에서 지정할 수 있습니다. GUI의 System Administration(시스템 관리) > Alerts(알림) 페이지(또는 CLI의 alertconfig 명령)를 통해 알림을 관리합니다.

알림 심각도

다음과 같은 심각도에 대해 알림을 전송할 수 있습니다.

- Critical(중대): 즉각적인 조치 필요.
- Warning(경고): 추가 모니터링 및 잠재적으로 즉각적인 조치가 필요한 문제 또는 오류.
- Information(정보): 이 디바이스의 일반적인 작동 중에 생성되는 정보.

AutoSupport

Cisco에서 더 나은 지원을 제공하고 향후 시스템 변경을 더 잘 설계하도록 돕기 위해, 시스템에 의해 생성되는 모든 알림 메시지의 복사본을 Cisco Systems로 전송하도록 어플라이언스를 구성할 수 있습니다. AutoSupport라고 하는 이 기능은 Cisco 팀이 사용자의 요구를 사전 대처식으로 지원하도록 도와주는 유용한 방법입니다. AutoSupport는 또한 시스템의 가동 시간, **`status`** 명령의 출력 및 사용된 AsyncOS 버전을 알려주는 주간 보고서를 전송합니다.

기본적으로 시스템 알림 유형에 대해 정보 심각도 레벨 알림을 수신하도록 설정된 알림 수신자는 Cisco로 전송되는 모든 메시지의 복사본을 수신합니다. 주간 알림 메시지를 내부적으로 전송하지 않으려는 경우 이 기능을 비활성화할 수 있습니다. 이 기능을 활성화 또는 비활성화하려면 알림 설정 구성, 965 페이지 섹션을 참조하십시오.

알림 전달

어플라이언스로부터 Alert Recipient(알림 수신자)에 지정된 주소로 전송되는 알림은 대상에 대해 정의된 SMTP 경로를 따릅니다.

알림 메시지는 어플라이언스 내 문제를 알려주기 위해 사용될 수 있으므로 AsyncOS의 일반 메일 전달 시스템을 사용하여 전송되지 않습니다. 대신 알림 메시지는 AsyncOS에서 중요한 시스템 실패가 발생할 경우 작동하도록 설계된 별도의 평행 이메일 시스템을 통해 전달됩니다.

알림 메일 시스템은 AsyncOS와 동일한 구성을 공유하지 않습니다. 즉, 알림 메시지는 다른 메일 전달과 약간 다르게 작동할 수 있습니다.

- 알림 메시지는 표준 DNS MX 및 A 레코드 조회를 사용하여 전달됩니다.
  - 알림 메시지는 DNS 항목을 30분 동안 캐시하며 캐시는 30분마다 새로 고쳐지므로, DNS 실패가 발생해도 알림은 전송됩니다.
- 알림 메시지는 작업 대기열을 거치지 않으므로 바이러스나 스팸 검사가 수행되지 않습니다. 메시지 필터 또는 콘텐츠 필터도 거치지 않습니다.
- 알림 메시지는 전달 대기열을 거치지 않으므로 반송 프로필 또는 대상 제어 제한의 영향을 받지 않습니다.

알림 메시지 예

```
Date: 23 Mar 2005 21:10:19 +0000

To: joe@example.com

From: IronPort C60 Alert [alert@example.com]

Subject: Critical-example.com: (Anti-Virus) update via http://newproxy.example.com
failed

The Critical message is:

update via http://newproxy.example.com failed

Version: 4.5.0-419

Serial Number: XXXXXXXXXXXX-XXXXXXX

Timestamp: Tue May 10 09:39:24 2005

For more information about this error, please see
http://support.ironport.com

If you desire further information, please contact your support provider.
```

알림 수신자 추가

알림 엔진을 사용하면 어떤 알림 수신자에게 어떤 알림을 전송할 것인지를 세부적으로 제어할 수 있습니다. 예를 들면 알림 수신자에게 특정 알림만 전송하도록 시스템을 구성하여, System(알림 유형)에 대한 Critical(심각도) 정보가 전송될 때만 알림을 받도록 알림 수신자를 구성할 수 있습니다.

참고 시스템 설정 중에 AutoSupport를 활성화한 경우, 기본적으로 모든 심각도 및 클래스에 대한 알림이 지정된 이메일 주소로 전송됩니다. 언제든 이 구성을 변경할 수 있습니다.

단계 **1** **System Administration(**시스템 관리**) > Alerts(**알림**)**를 선택합니다.

단계 **2** **Add Recipient(**수신자 추가**)**를 클릭합니다.

단계 **3** 수신자의 이메일 주소를 입력합니다. 여러 주소를 쉼표로 구분하여 입력할 수 있습니다.

단계 **4** (선택 사항) Cisco 지원에서 소프트웨어 릴리스 및 중요한 지원 알림 메시지를 수신하려면 **Release and Support Notifications(**릴리스 및 지원 알림**)** 확인란을 선택합니다.

단계 **5** 이 수신자가 수신할 알림 유형 및 심각도를 선택합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

알림 설정 구성

다음 설정은 모든 알림에 적용됩니다.

참고 나중에 보기 위해 어플라이언스에 저장할 알림 수를 정의하려면 alertconfig CLI 명령을 사용하십시오.

단계 **1** Alerts(알림) 페이지에서 **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **2** 알림을 전송할 때 사용할 Header From: 주소를 입력하거나 Automatically Generated(자동 생성)("alert@<호스트 이름>")를 선택합니다.

단계 **3** 중복 알림 전송 사이에 대기할 시간(초)을 지정하려면 확인란을 선택합니다. 자세한 내용은 중복 알림 전송, 965 페이지를 참고하십시오.

- 중복 알림을 전송하기 전 기다릴 초기 시간(초)을 지정합니다.
- 중복 알림을 전송하기 전 기다릴 최대 시간(초)을 지정합니다.

단계 **4** IronPort AutoSupport 옵션을 선택하여 AutoSupport를 활성화할 수 있습니다. AutoSupport에 대한 자세한 내용은 AutoSupport, 963 페이지 섹션을 참조하십시오.

- AutoSupport를 활성화하면, Information(정보) 레벨에서 System(시스템) 알림을 수신하도록 설정된 알림 수신자에게 주간 AutoSupport 보고서가 전송됩니다. 확인란을 통해 이를 비활성화할 수 있습니다.

단계 **5** 변경 사항을 제출 및 커밋합니다.

경고 설정

알림 설정은 다음을 포함하여 알림의 일반 동작 및 컨피그레이션을 제어합니다.

- 알림 전송 시 RFC 2822 Header From:(주소를 입력하거나 기본값인 "alert@<호스트 이름>" 사용). CLI의 alertconfig -> from 명령을 통해 설정할 수도 있습니다.
- 중복 알림을 전송하기 전 기다릴 초기 시간(초)
- 중복 알림을 전송하기 전 기다릴 최대 시간(초)
- AutoSupport의 상태(활성화됨 또는 비활성화됨)
- Information(정보) 레벨에서 System(시스템) 알림을 수신하도록 설정된 알림 수신자에게 AutoSupport 주간 상태 보고서 전송

중복 알림 전송

AsyncOS가 중복 알림을 전송하기 전 기다릴 초기 시간(초)을 지정할 수 있습니다. 중복 알림 요약이 전송되지 않고 대신 모든 중복 알림이 지연 없이 전송됩니다(이 경우 짧은 시간 동안 대량의 이메일이 전송될 수 있음). 중복 알림 전송 사이에 기다릴 시간(초)(알림 간격)은 각 알림이 전송된 후 늘어납

니다. 대기 시간(초)에 마지막 간격의 두 배를 더한 값이 늘어납니다. 따라서 5초 대기의 경우 5초, 15초, 35초, 75초, 155초, 315초 등에 알림이 전송됩니다.

결국 간격이 상당히 커질 수 있습니다. 중복 알림을 전송하기 전 기다릴 최대 시간(초) 필드를 통해 간격 사이에 기다릴 시간(초)의 최대값을 설정할 수 있습니다. 예를 들어 초기값을 5초로 설정하고 최대값을 60초로 설정하면 5초, 15초, 35초, 60초, 120초 등에 알림이 전송됩니다.

최근 알림 보기

Email Security Appliance는 사용자가 알림 메시지를 손실하거나 삭제할 경우에 대비하여 GUI 및 CLI에서 모두 볼 수 있도록 최신 알림을 저장합니다. 이러한 알림은 어플라이언스에서 다운로드할 수 없습니다.

최신 알림 목록을 보려면 Alerts(알림) 페이지에서 **View Top Alerts(**상위 알림 보기**)** 버튼을 클릭하거나 CLI에서 displayalerts 명령을 사용합니다. GUI에서 알림을 날짜, 레벨, 클래스, 텍스트 및 수신자별로 정돈할 수 있습니다.

기본적으로 어플라이언스는 **Top Alerts(**상위 알림**)** 창에 표시할 알림을 최대 50개 저장합니다. 어플라이언스가 저장할 알림 수를 수정하려면 CLI에서 alertconfig -> setup 명령을 사용합니다. 이 기능을 비활성화하려면 알림 수를 0으로 변경합니다.

알림 설명

다음 표에는 알림 이름(Cisco에서 사용하는 내부 설명자), 알림의 실제 텍스트, 설명, 심각도(critical(중대) information(정보) 또는 warning(경고)), 메시지 텍스트에 포함된 파라미터(있는 경우) 등의 분류별로 알림이 나열되어 있습니다. 매개변수의 값은 알림의 실제 텍스트로 교체됩니다. 예를 들어 아래의 알림 메시지는 메시지 텍스트에 "$ip"가 포함될 수 있습니다. "$ip"는 알림이 생성될 때 실제 IP 주소로 교체됩니다.

- 안티스팸 알림, 967 페이지
- 안티바이러스 알림, 967 페이지
- DHAP(Directory Harvest Attack Prevention) 알림, 968 페이지
- 하드웨어 알림, 968 페이지
- 스팸 격리 알림, 969 페이지
- 허용 목록/차단 목록 알림, 971 페이지
- 시스템 경보, 971 페이지
- 업데이트 프로그램 경고, 981 페이지
- 보안 침해 필터 알림, 982 페이지
- 클러스터링 알림, 983 페이지

안티스팸 알림

다음 표에는 알림에 대한 설명과 알림 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 안티스팸 알림의 목록이 포함되어 있습니다.

표 ***85:*** 가능한 안티스팸 알림 목록

알림 이름	메시지 및 설명	매개변수
AS.SERVER.ALERT	$engine anti-spam - $message $tb Critical(중대). Sent when the anti-spam engine fails.	'**engine**' - 안티스팸 엔진의 유형입니다. '**message**' - 로그 메시지. '**tb**' - 이벤트의 역추적(traceback).
AS.TOOL.INFO_ALERT	Update - $engine - $message Information(정보). 안티스팸 엔진에 문제가 있을 경우 전송됨.	'**engine**' - 안티스팸 엔진 이름입니다. '**message**' - 메시지
AS.TOOL.ALERT	Update - $engine - $message Critical(중대). 안티스팸 엔진을 관리하는 데 사용된 툴 중 하나에 문제가 발생하여 업데이트가 취소될 경우 전송됨.	'**engine**' - 안티스팸 엔진 이름입니다. '**message**' - 메시지

안티바이러스 알림

다음 표에는 알림에 대한 설명과 알림 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 안티바이러스 알림의 목록이 포함되어 있습니다.

표 ***86:*** 가능한 안티바이러스 알림 목록

알림 이름	메시지 및 설명	매개변수
AV.SERVER.ALERT /AV.SERVER.CRITICAL	$engine antivirus - $message $tb Critical(중대). 안티바이러스 검사 엔진에 중대한 문제가 있을 경우 전송됨.	'**engine**' - 안티바이러스 엔진의 유형. '**message**' - 로그 메시지. '**tb**' - 이벤트의 역추적(traceback).
AV.SERVER.ALERT.INFO	$engine antivirus - $message $tb Information(정보). 안티바이러스 검사 엔진에 정보 이벤트가 발생할 경우 전송됨.	'**engine**' - 안티바이러스 엔진의 유형. '**message**' - 로그 메시지. '**tb**' - 이벤트의 역추적(traceback).
AV.SERVER.ALERT.WARN	$engine antivirus - $message $tb Warning(경고) 안티바이러스 검사 엔진에 문제가 있을 경우 전송됨.	'**engine**' - 안티바이러스 엔진의 유형. '**message**' - 로그 메시지. '**tb**' - 이벤트의 역추적(traceback).

알림 이름	메시지 및 설명	매개변수
MAIL.ANTIVIRUS.ERROR_MESSAGE	MID $mid antivirus $what error $tag	'**mid**' - MID '**what**' - 발생한 오류. '**tag**' - 설정된 경우 바이러스 보안 침해 이름.
	Critical(중대). 안티바이러스 엔진이 메시지 검사에서 오류가 발생할 경우 전송됨.	
MAIL.SCANNER. PROTOCOL_MAX_RETRY	MID $mid is malformed and cannot be scanned by $engine.	'**mid**' - MID '**engine**' - 사용되고 있는 엔진
	Critical(중대). 메시지 형식이 잘못되어, 메시지를 검사하려고 시도한 검사 엔진이 성공하지 못함. 최대 재시도 수가 초과되어, 메시지가 이 엔진의 검사 없이 처리됩니다.	

DHAP(Directory Harvest Attack Prevention) 알림

다음 표에는 알림에 대한 설명과 알림 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 DHAP 알림의 목록이 포함되어 있습니다.

표 ***87:*** 가능한 ***Directory Harvest Attack Prevention*** 알림 목록

알림 이름	메시지 및 설명	매개변수
LDAP.DHAP_ALERT	LDAP: Potential Directory Harvest Attack detected. See the system mail logs for more information about this attack.	
	Warning(경고) 가능한 디렉터리 수집 공격이 탐지될 때 전송됨.	

하드웨어 알림

다음 표에는 알림에 대한 설명과 알림 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 하드웨어 알림의 목록이 포함되어 있습니다.

표 **88:** 가능한 하드웨어 알림 목록

알림 이름	메시지 및 설명	매개변수
INTERFACE.ERRORS	Port $port: has detected $in_err input errors, $out_err output errors, $col collisions please check your media settings. Warning(경고) 인터페이스 오류가 탐지될 때 전송됨.	'**port**' - 인터페이스 이름. '**in_err**' - 마지막 메시지 이후 입력 메시지의 수. '**out_err**' - 마지막 메시지 이후 출력 오류의 수. '**col**' - 마지막 메시지 이후 패킷 충돌의 수.
MAIL.MEASUREMENTS_FILESYSTEM	The $file_system partition is at $capacity% capacity Warning(경고) 디스크 파티션이 용량에 근접할 때(75%) 전송됨.	'**file_system**' - 파일 시스템의 이름. '**capacity**' - 파일 시스템이 사용된 비율.
MAIL.MEASUREMENTS_FILESYSTEM.위험	The $file_system partition is at $capacity% capacity Critical(중대). 디스크 파티션이 용량의 90%(95%, 96%, 97% 등)에 도달할 때 전송됨.	'**file_system**' - 파일 시스템의 이름. '**capacity**' - 파일 시스템이 사용된 비율.
SYSTEM.RAID_EVENT_ALERT	A RAID-event has occurred: $error Warning(경고) 중대한 RAID 이벤트가 발생할 경우 전송됨.	'**error**' - RAID 오류의 텍스트.
SYSTEM.RAID_EVENT_ALERT_INFO	A RAID-event has occurred: $error Information(정보). RAID 이벤트가 발생할 경우 전송됨.	'**error**' - RAID 오류의 텍스트.

스팸 격리 알림

다음 표에는 알림에 대한 설명과 알림 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 스팸 격리 알림의 목록이 포함되어 있습니다.

표 **89:** 가능한 스팸 격리 알림 목록

알림 이름	메시지 및 설명	매개변수
ISQ.CANNOT_CONNECT_OFF_BOX	ISQ: Could not connect to off-box quarantine at $host:$port Information(정보). AsyncOS가 (오프박스) IP 주소에 연결할 수 없는 경우 전송됨.	'**host**' - 오프박스 격리의 주소 '**port**' - 오프박스 격리에 연결할 포트

알림 이름	메시지 및 설명	매개변수
ISQ.CRITICAL	ISQ: $msg Critical(중대). 중대한 스팸 격리 오류가 발생할 경우 전송됨.	'**msg**' - 표시할 메시지
ISQ.DB_APPROACHING_FULL	ISQ: Database over $threshold% full Warning(경고) 스팸 격리 데이터베이스가 거의 꽉 찰 경우 전송됨.	'**threshold**' - 알림이 시작되는 전체 임계값 비율
ISQ.DB_FULL	ISQ: database is full Critical(중대). 스팸 격리 데이터베이스가 꽉 찰 경우 전송됨.	
ISQ.MSG_DEL_FAILED	ISQ: Failed to delete MID $mid for $rcpt: $reason Warning(경고) 스팸 격리에서 이메일이 성공적으로 삭제되지 않을 경우 전송됨.	'**mid**' - MID '**rcpt**' - 수신자 또는 "all" '**reason**' - 메시지가 삭제되지 않은 이유
ISQ.MSG_NOTIFICATION_FAILED	ISQ: Failed to send notification message: $reason Warning(경고) 알림 메시지가 성공적으로 전송되지 않을 경우 전송됨.	'**reason**' - 알림이 전송되지 않은 이유
ISQ.MSG_QUAR_FAILED	Warning(경고) 메시지가 성공적으로 격리되지 않을 경우 전송됨.	
ISQ.MSG_RLS_FAILED	ISQ: Failed to release MID $mid to $rcpt: $reason Warning(경고) 메시지가 성공적으로 릴리스되지 않을 경우 전송됨.	'**mid**' - MID '**rcpt**' - 수신자 또는 "all" '**reason**' - 메시지가 릴리스되지 않은 이유
ISQ.MSG_RLS_FAILED_UNK_RCPTS	ISQ: Failed to release MID $mid: $reason Warning(경고) 수신자를 알 수 없어 메시지가 성공적으로 릴리스되지 않을 경우 전송됨.	'**mid**' - MID '**reason**' - 메시지가 릴리스되지 않은 이유
ISQ.NO_EU_PROPS	ISQ: Could not retrieve $user's properties. Setting defaults Information(정보). AsyncOS가 사용자에 대한 정보를 검색할 수 없을 경우 전송됨.	'**user**' - 최종 사용자 이름
ISQ.NO_OFF_BOX_HOST_SET	ISQ: Setting up off-box ISQ without setting host Information(정보). AsyncOS가 외부 격리를 참조하도록 구성되었지만 외부 격리가 정의되지 않은 경우 전송됨.	

허용 목록/차단 목록 알림

다음 표에는 알림의 설명과 심각도를 비롯하여 AsyncOS에 의해 생성될 수 있는 각종 허용 목록/차단 목록 알림 목록이 포함되어 있습니다.

표 ***90:*** 가능한 허용 목록/차단 목록 알림 목록

알림 이름	메시지 및 설명	매개변수
SLBL.DB.RECOVERY_FAILED	SLBL: Failed to recover End-User Safelist/Blocklist database: '$error'.	'**error**' - 오류 이유
	Critical(중대). 허용 목록/차단 목록 데이터베이스를 복구하지 못했습니다.	
SLBL.DB.SPACE_LIMIT	SLBL: End-User Safelist/Blocklist database exceeded allowed disk space: $current of $limit.	'**current**' - 사용된 양(MB 단위)
	Critical(중대). 허용 목록/차단 목록 데이터베이스가 허용된 디스크 공간을 초과했습니다.	'**limit**' - 구성된 제한(MB 단위)

시스템 경보

다음 표에는 알림에 대한 설명과 알림 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 시스템 알림의 목록이 포함되어 있습니다.

표 ***91:*** 가능한 시스템 알림 목록

구성 요소/알림 이름	메시지 및 설명	매개변수
AMP.ENGINE.ALERT	Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 483 페이지를 참조하십시오.	-
AsyncOS API Alerts	*AsyncOS API for Cisco Email Security Appliances* - 시작 가이드의 "알림" 섹션을 참고하십시오.	-
사서함 자동 치료 알림	"알림" 섹션 참고 Office 365 사서함에서 자동으로 메시지 치료, 561 페이지	-
COMMON.APP_FAILURE	An application fault occurred: $error	'**error**' - 오류의 텍스트(일반적으로 역추적).
	Warning(경고) 알 수 없는 애플리케이션 실패가 발생할 경우 전송됨.	

구성 요소/알림 이름	메시지 및 설명	매개변수
COMMON.ENGINE_AUTO_UPDATE_ENABLED	<$level>: <$class> Information: Automatic updates have been enabled for the particular engine <$engine>. You will now receive automatic engine updates for this engine.	'**$engine**' - 서비스 엔진의 이름입니다. 값은 다음과 같을 수 있습니다. • Sophos • McAfee • Graymail
COMMON.ENGINE_AUTO_UPDATE_DISABLED	<$level>: <$class> Information: Automatic updates have been disabled for the particular engine <$engine>. You will not receive any automatic updates for this engine, unless you enable automatic updates in the global setting page of the particular engine.	'**$engine**' - 서비스 엔진의 이름입니다. 값은 다음과 같을 수 있습니다. • Sophos • McAfee • Graymail
COMMON.KEY_EXPIRED_ALERT	Your "$feature" key has expired. Please contact your authorized Cisco sales representative. Warning(경고) 기능 키가 만료된 경우 전송됨.	'**feature**' - 만료를 앞둔 기능의 이름.
COMMON.KEY_EXPIRING_ALERT	Your "$feature" key will expire in under $days day(s). Cisco 영업 담당자에게 문의하십시오. Warning(경고) 기능 키가 곧 만료되는 경우 전송됨.	'**feature**' - 만료를 앞둔 기능의 이름. '**days**' - 만료될 때까지 남은 일수.
COMMON.KEY_FINAL_EXPIRING_ALERT	This is a final notice. Your "$feature" key will expire in under $days day(s). Cisco 영업 담당자에게 문의하십시오. Warning(경고) 기능 키가 곧 만료된다는 최종 알림으로 전송됨.	'**feature**' - 만료를 앞둔 기능의 이름. '**days**' - 만료될 때까지 남은 일수.
KEYS.GRACE_EXPIRING_ALERT	All security services licenses for this Cisco Email Security Appliance have expired. The appliance will continue to deliver mail without security services for $days days. To renew security services licenses, Please contact your authorized Cisco sales representative. Critical(중대). 가상 어플라이언스 라이센스 만료에 대한 유예 기간이 시작될 때부터 주기적으로 전송됨.	'**days**' - 알림 전송 시점에 남아 있는 유예 기간 일수. 유예 기간에 대한 자세한 내용은 가상 어플라이언스 라이센스 만료 , 935 페이지 섹션을 참조하십시오.

구성 요소/알림 이름	메시지 및 설명	매개변수
KEYS.GRACE_FINAL_EXPIRING_ALERT	This is the final notice. All security services licenses for this Cisco Email Security Appliancehave expired. The appliance will continue to deliver mail without security services for 1 day. To renew security services licenses, Please contact your authorized Cisco sales representative.	유예 기간에 대한 자세한 내용은 가상 어플라이언스 라이센스 만료 , 935 페이지 섹션을 참조하십시오.
	Critical(중대). 가상 어플라이언스 라이센스가 만료되기 하루 전에 전송됨.	
KEYS.GRACE_EXPIRED_ALERT	Your grace period has expired. All security sevice have expired, and your appliance is non-functional. The appliance will no longer deliver mail until a new license is applied. To renew security services licenses, Please contact your authorized Cisco sales representative.	유예 기간에 대한 자세한 내용은 가상 어플라이언스 라이센스 만료 , 935 페이지 섹션을 참조하십시오.
	Critical(중대). 가상 어플라이언스의 유예 기간이 만료된 경우 전송됨.	
DNS.BOOTSTRAP_FAILED	Failed to bootstrap the DNS resolver. Unable to contact root servers.	
	Warning(경고) 어플라이언스가 루트 DNS 서버에 연결할 수 없을 경우 전송됨.	
COMMON.INVALID_FILTER	Invalid $class: $error	'**class**' - "Filter", "SimpleFilter" 등. '**error**' - 필터가 유효하지 않은 이유에 대한 추가 정보.
	Warning(경고) 잘못된 필터가 발견될 경우 전송됨.	

구성 요소/알림 이름	메시지 및 설명	매개변수
IPBLOCKD.HOST_ADDED_TO_WHITELIST IPBLOCKD.HOST_ADDED_TO_BLACKLIST IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST	The host at $ip has been added to the blacklist because of an SSH DOS attack. The host at $ip has been permanently added to the ssh whitelist. The host at $ip has been removed from the blacklist	'**ip**' - 로그인 시도가 발생한 IP 주소.
	Warning(경고) SSH를 통해 어플라이언스에 연결하려고 시도하지만 유효한 자격 증명을 제공하지 않는 IP 주소는 10분 내에 실패한 시도 수가 10을 넘으면 SSH 블랙리스트에 추가됩니다. 사용자가 동일한 IP 주소에서 성공적으로 로그인하면 해당 IP 주소는 화이트리스트에 추가됩니다. 화이트리스트의 주소는 블랙리스트에서도 발견되더라도 액세스가 허용됩니다. 약 하루가 지나면 항목이 자동으로 블랙리스트에서 제거됩니다.	
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP: Failed group query $name, comparison in filter will evaluate as false	'**name**' - 쿼리의 이름.
	Critical(중대). LDAP 그룹 쿼리가 실패할 경우 전송됨.	
LDAP.HARD_ERROR	LDAP: work queue processing error in $name reason $why	'**name**' - 쿼리의 이름. '**why**' - 오류가 발생한 이유.
	Critical(중대). LDAP 쿼리가 완전히 실패할 경우 전송됨(모든 서버 시도 후).	
LOG.ERROR.*	Critical(중대). 각종 로깅 오류.	
MAIL.FILTER.RULE_MATCH_ALERT	MID $mid matched the $rule_name rule. \n Details: $details	'**mid**' - 메시지의 고유 식별 번호. '**rule_name**' - 일치하는 규칙의 이름. '**details**' - 메시지 또는 규칙에 대한 자세한 정보.
	Information(정보). Header Repeats(헤더 반복) 규칙이 true로 평가될 때마다 전송됨.	

구성 요소/알림 이름	메시지 및 설명	매개변수
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	LDAP group query failure during per-recipient scanning, possible LDAP misconfiguration or unreachable server. Critical(중대). 수신자별 검사 중에 LDAP 그룹 쿼리가 실패할 경우 전송됨.	
MAIL.QUEUE.ERROR.*	Critical(중대). 각종 메일 대기열 하드 오류.	
MAIL.OMH.DELIVERY_RETRY	Subject - 'Alert: Message Delivery failed for $hostname. DANE verification failed for one or more Domain(s).' Message - The message delivery failed due to DANE verification failure for all mail exchange (MX) hosts in $hostname. The appliance will attempt message delivery again or bounce the message.	'host' - DANE 확인에 실패한 호스트
MAIL.RES_CON_START_ALERT. 메모리	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. RAM utilization for this system has exceeded the resource conservation threshold of $memory_threshold_start%. The allowed receiving rate for this system will be gradually decreased as RAM utilization approaches $memory_threshold_halt%. Critical(중대). RAM 사용률이 시스템 리소스 절약 임계값을 초과할 경우 전송됨.	'**hostname**' - 호스트의 이름. '**memory_threshold_start**' - 메모리 타피팅이 시작되는 임계값 비율. '**memory_threshold_halt**' - 메모리가 꽉 차서 시스템이 멈추게 될 임계값 비율.
MAIL.RES_CON_START_ALERT. QUEUE_SLOW	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. The queue is overloaded and is unable to maintain the current throughput. Critical(중대). 메일 대기열이 과부화되어 시스템 리소스 보존이 활성화될 경우 전송됨.	'**hostname**' - 호스트의 이름.

구성 요소/알림 이름	메시지 및 설명	매개변수
MAIL.RES_CON_START_ ALERT. QUEUE	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. Queue utilization for this system has exceeded the resource conservation threshold of $queue_threshold_start%. The allowed receiving rate for this system will be gradually decreased as queue utilization approaches $queue_threshold_halt%.	'**hostname**' - 호스트의 이름. '**queue_threshold_start**' - 대기열 타피팅이 시작되는 임계값 비율. '**queue_threshold_halt**' - 대기열이 꽉 차서 시스템이 멈추게 될 임계값 비율.
	Critical(중대). 대기열 사용률이 시스템 리소스 절약 임계값을 초과할 경우 전송됨.	
MAIL.RES_CON_START_ ALERT. WORKQ	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources. Listeners have been suspended because the current work queue size has exceeded the threshold of $suspend_threshold. Listeners will be resumed once the work queue size has dropped to $resume_threshold. These thresholds may be altered via use of the 'tarpit' command on the system CLI.	'**hostname**' - 호스트의 이름. '**suspend_threshold**' - 그 위면 리스너가 일시 중단되는 작업 대기열 크기. '**resume_threshold**' - 그 아래면 리스너가 다시 시작되는 작업 대기열 크기.
	Information(정보). 작업 대기열 크기가 너무 커서 리스너가 일시 중단되는 경우 전송됨.	
MAIL.RES_CON_START_ ALERT	This system (hostname: $hostname) has entered a 'resource conservation' mode in order to prevent the rapid depletion of critical system resources.	'**hostname**' - 호스트의 이름.
	Critical(중대). 어플라이언스가 "리소스 절약" 모드로 들어갈 경우 전송됨.	
MAIL.RES_CON_STOP_ALERT	This system (hostname: $hostname) has exited 'resource conservation' mode as resource utilization has dropped below the conservation threshold.	'**hostname**' - 호스트의 이름.
	Information(정보). 어플라이언스가 "리소스 절약" 모드에서 나올 경우 전송됨.	

구성 요소/알림 이름	메시지 및 설명	매개변수
MAIL.SDS.CATEGORY_CHANGE	향후 URL 범주 집합 변경 , 459 페이지를 참조하십시오.	—
MAIL.SDS.CERTIFICATE_INVALID	URL 필터링 트러블슈팅, 441 페이지의 내용을 참조하십시오.	
MAIL.SDS.ERROR_FETCHING_CERTIFICATE		
MAIL.WORK_QUEUE_PAUSED_NATURAL	work queue paused, $num msgs, $reason Critical(중대). 작업 대기열이 일시 중지될 경우 전송됨.	'**num**' - 작업 대기열에 있는 메시지의 수. '**reason**' - 작업 대기열이 일시 중지된 이유.
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	work queue resumed, $num msgs Critical(중대). 작업 대기열이 다시 시작될 경우 전송됨.	'**num**' - 작업 대기열에 있는 메시지의 수.
NTP.NOT_ROOT	Not running as root, unable to adjust system time Warning(경고) NTP가 루트로 실행되고 있지 않아서 어플라이언스가 시간을 조정할 수 없을 경우 전송됨.	
QUARANTINE.ADD_DB_ERROR	Unable to quarantine MID $mid - quarantine system unavailable Critical(중대). 메시지를 격리로 보낼 수 없을 경우 전송됨.	'**mid**' - MID
QUARANTINE.DB_UPDATE_FAILED	Unable to update quarantine database (current version: $version; target $target_version) Critical(중대). 격리 데이터베이스를 업데이트할 수 없는 경우 전송됨.	'**version**' - 탐지된 스키마 버전. '**target_version**' - 대상 스키마 버전.
QUARANTINE.DISK_SPACE_LOW	The quarantine system is unavailable due to a lack of space on the $file_system partition. Critical(중대). 격리용 디스크 공간이 꽉 찰 경우 전송됨.	'**file_system**' - 파일 시스템의 이름.
QUARANTINE.THRESHOLD_ALERT	Quarantine "$quarantine" is $full% full Warning(경고) 격리가 용량의 5%, 50% 또는 75%에 도달할 경우 전송됨.	'**quarantine**' - 격리의 이름. '**full**' - 격리의 꽉 찬 정도를 나타내는 비율.

구성 요소/알림 이름	메시지 및 설명	매개변수
QUARANTINE.THRESHOLD_ALERT.SERIOUS	Quarantine "$quarantine" is $full% full	'**quarantine**' - 격리의 이름. '**full**' - 격리의 꽉 찬 정도를 나타내는 비율.
	Critical(중대). 격리가 용량의 95%에 도달할 경우 전송됨.	
REPORTD.DATABASE_OPEN_FAILED_ALERT	The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: $err_msg	'**err_msg**' - 표시되는 오류 메시지
	Critical(중대). 보고 엔진이 데이터베이스를 열 수 없을 경우 전송됨.	
REPORTD.AGGREGATION_DISABLED_ALERT	Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc.). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	'**threshold**' - 임계값
	Warning(경고) 시스템에 디스크 공간이 부족할 경우 전송됨. 로그 항목에 대한 디스크 사용량이 로그 사용량 임계값을 초과하면 보고용 집계가 비활성화되고 알림이 전송됩니다.	
REPORTING.CLIENT.UPDATE_FAILED_ALERT	Reporting Client: The reporting system has not responded for an extended period of time ($duration).	'**duration**' - 클라이언트가 보고 데몬에 연결하려고 시도한 시간의 길이. 사람이 읽을 수 있는 형식의 문자열입니다('1h 3m 27s').
	Warning(경고) 보고 엔진이 보고 데이터를 저장할 수 없을 경우 전송됨.	
REPORTING.CLIENT.JOURNAL.FULL	Reporting Client: The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.	
	Critical(중대). 보고 엔진이 새 데이터를 저장할 수 없을 경우 전송됨.	
REPORTING.CLIENT.JOURNAL.무료	Reporting Client: The reporting system is now able to handle new data.	
	Information(정보). 보고 엔진이 새 데이터를 다시 저장할 수 있게 될 경우 전송됨.	

구성 요소/알림 이름	메시지 및 설명	매개변수
PERIODIC_REPORTS.REPORT_TASK.BUILD_FAILURE	A failure occurred while building periodic report '$report_title'. This subscription has been removed from the scheduler.	'**report_title**' - 보고서 제목
	Critical(중대). 보고 엔진이 보고서를 작성할 수 없을 경우 전송됨.	
PERIODIC_REPORTS.REPORT_TASK.EMAIL_FAILURE	A failure occurred while emailing periodic report '$report_title'. This subscription has been removed from the scheduler.	'**report_title**' - 보고서 제목
	Critical(중대). 보고서를 이메일로 보낼 수 없을 경우 전송됨.	
PERIODIC_REPORTS.REPORT_TASK.ARCHIVE_FAILURE	A failure occurred while archiving periodic report '$report_title'. This subscription has been removed from the scheduler.	'**report_title**' - 보고서 제목
	Critical(중대). 보고서를 보관할 수 없을 경우 전송됨.	
SENDERBASE.ERROR	Error processing response to query $query: response was $response	'**query**' - 쿼리 주소. '**response**' - 원시 응답 데이터를 수신함.
	Information(정보). SenderBase로부터의 응답을 처리하는 동안 오류가 발생할 경우 전송됨.	
SMTPAUTH.FWD_SERVER_FAILED_ ALERT	SMTP Auth: could not reach forwarding server $ip with reason: $why	'**ip**' - 원격 서버의 IP. '**why**' - 오류가 발생한 이유.
	Warning(경고) SMTP 인증 전달 서버에 도달할 수 없을 경우 전송됨.	
SMTPAUTH.LDAP_QUERY_FAILED	SMTP Auth: LDAP query failed, see LDAP debug logs for details.	
	Warning(경고) LDAP 쿼리에 실패할 경우 전송됨.	
SYSTEM.HERMES_SHUTDOWN_FAILURE. REBOOT	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=reboot	'**error**' - 발생한 오류.
	Warning(경고) 재부팅 시 시스템 종료에 문제가 있을 경우 전송됨.	
SYSTEM.HERMES_SHUTDOWN_FAILURE. SHUTDOWN	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=shut down	'**error**' - 발생한 오류.
	Warning(경고) 시스템 종료에 문제가 있을 경우 전송됨.	

구성 요소/알림 이름	메시지 및 설명	매개변수
SYSTEM.LOGIN_FAILURES_LOCK_ALERT	User "$user" is locked after $numlogins consecutive login failures. Last login attempt was from $rhost Information: Sent when the user account is locked because of maximum number of failed login attempts	'user' - 사용자의 이름 'numlogins' - 구성된 알림 임계값 'rhost' - 원격 호스트의 주소
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	Error updating recipient validation data: $why Critical(중대). 수신자 검증 업데이트가 실패할 경우 전송됨.	'why' - 오류 메시지.
SYSTEM.SERVICE_TUNNEL. 사용 안 함	Tech support: Service tunnel has been disabled Information(정보). Cisco 지원 서비스용으로 생성된 터널이 비활성화될 경우 전송됨.	
SYSTEM.SERVICE_TUNNEL. 사용활성화됨	Tech support: Service tunnel has been enabled, port $port Information(정보). Cisco 지원 서비스용으로 생성된 터널이 활성화될 경우 전송됨.	'**port**' - 서비스 터널에 사용되는 포트.
IPBLOCKD.HOST_ADDED_TO_WHITELIST IPBLOCKD.HOST_ADDED_TO_BLACKLIST IPBLOCKD.HOST_REMOVED_FROM_BLACKLIST	The host at $ip has been added to the blacklist because of an SSH DOS attack. The host at $ip has been permanently added to the ssh whitelist. The host at $ip has been removed from the blacklist Warning(경고) SSH를 통해 어플라이언스에 연결하려고 시도하지만 유효한 자격 증명을 제공하지 않는 IP 주소는 10분 내에 실패한 시도 수가 10을 넘으면 SSH 블랙리스트에 추가됩니다. 사용자가 동일한 IP 주소에서 성공적으로 로그인하면 해당 IP 주소는 화이트리스트에 추가됩니다. 화이트리스트의 주소는 블랙리스트에서도 발견되더라도 액세스가 허용됩니다. 약 하루가 지나면 항목이 자동으로 블랙리스트에서 제거됩니다.	'**ip**' - 로그인 시도가 발생한 IP 주소.

구성 요소/알림 이름	메시지 및 설명	매개변수
WATCHDOG_RESTART_ALERT_MSG	<$level>: <$class>, <$hostname>: $subject $text Warning(경고) Cisco Email Security Appliance는 watchdog 서비스를 사용하여 다음 엔진의 상태 조건을 모니터링합니다. • Anti-Spam • Anti-Virus • 악성코드 방지 • 그레이메일 위 엔진이 특정 기간 동안 watchdog 서비스에 응답하지 않을 경우, watchdog 서비스는 엔진을 재시작하고 관리자에게 알림을 보냅니다.	**'subject'** - 엔진에 특정한 Watchdog 알림 제목 **'text'** - 엔진에 특정한 Watchdog 알림 텍스트
MAIL.IMH.GEODB_UPDATE_COUNTRIES'	Warning(경고) Geolocation Update - the list of supported countries has changed. Added Countries - <$added> Deleted Countries - <$deleted> Review your HAT sender groups, Message Filters, and Content Filters settings accordingly.	'added' - The following countries are added: <iso_code1>:<country_name1>,<iso_code2>:<country_name2>, 'deleted' - The following countries are deleted: <iso_code1>:<country_name1>:<iso_code2>:<country_name2>,
MAIL.UPDATED_SHORT_URL_DOMAIN_LIST	Info. The list of shortened URL domains has been updated.. Added Domains: <$added_domains> Deleted Domains - <$deleted_domains>	'added_domains': The following domains are added: <domains_1>, <domain_2> 'deleted_domains' : The following domains are deleted: <domain_3>, <domain_4>
MAIL.DOMAINS_NOT_REACHABLE	Warning(경고) The following domains are not reachable by the appliance for shortened URL support: <$domains> Check your firewall rules to allow your appliance to connect to these domains.	<$domains>: comma separated list of domains

업데이트 프로그램 경고

다음 표에는 AsyncOS에 의해 생성될 수 있는 각종 업데이트 알림 목록이 포함되어 있습니다.

표 ***92:*** 가능한 업데이터 알림 목록

알림 이름	메시지 및 설명	매개변수
UPDATER.APP.UPDATE_ ABANDONED	$app abandoning updates until a new version is published. The $app application tried and failed $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage	'**app**' - 애플리케이션 이름. '**attempts**' - 시도 횟수.
	Warning(경고) 애플리케이션이 업데이트를 포기합니다.	
UPDATER.UPDATERD. ANIFEST_FAILED_ALERT	The updater has been unable to communicate with the update server for at least $threshold.	'**threshold**' - 사람이 읽을 수 있는 임계값 문자열.
	Warning(경고) 서버 매니페스트 가져오기 실패.	
UPDATER.UPDATERD. RELEASE_NOTIFICATION	$mail_text	'**mail_text**' - 알림 텍스트. '**notification_subject**' - 알림 텍스트.
	Warning(경고) 릴리스 알림.	
UPDATER.UPDATERD. UPDATE_FAILED	Unknown error occured: $traceback	'**traceback**' - 역추적(traceback).
	Critical(중대). 업데이트 실행 실패.	

보안 침해 필터 알림

다음 표에는 알림에 대한 설명과 알림 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 보안 침해 필터 알림의 목록이 포함되어 있습니다. 보안 침해 필터는 격리용(특히 보안 침해 격리) 시스템 알림에서도 참조될 수 있습니다.

표 ***93:*** 가능한 보안 침해 필터 알림 목록

알림 이름	메시지 및 설명	매개변수
VOF.GTL_THRESHOLD_ALERT	Outbreak Filters Rule Update Alert:$text All rules last updated at: $time on $date.	'**text**' - 업데이트 알림 텍스트.
	Information(정보). 보안 침해 필터 임계값이 변경될 경우 전송됨.	'**time**' - 마지막 업데이트 시간. '**date**' - 마지막 업데이트 날짜.

알림 이름	메시지 및 설명	매개변수
AS.UPDATE_FAILURE	$engine update unsuccessful. This may be due to transient network or DNS issues, HTTP proxy configuration causing update transmission errors or unavailability of downloads.ironport.com. The specific error on the appliance for this failure is: $error	'**engine**' - 업데이트에 실패한 엔진. '**error**' - 발생한 오류.
	Warning(경고) 안티스팸 엔진 또는 CASE 규칙이 업데이트에 실패할 경우 전송됨.	

클러스터링 알림

다음 표에는 알림에 대한 설명과 알림 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 클러스터링 알림의 목록이 포함되어 있습니다.

표 ***94:*** 가능한 클러스터링 알림 목록

알림 이름	메시지 및 설명	매개변수
CLUSTER.CC_ERROR.AUTH_ERROR	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Machine does not appear to be in the cluster	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**ip**' - 원격 호스트의 IP. '**why**' - 오류에 대한 자세한 텍스트.
	Critical(중대). 인증 오류가 발생할 경우 전송됨. 이 오류는 시스템이 클러스터의 구성원이 아닌 경우 발생할 수 있습니다.	
CLUSTER.CC_ERROR.DROPPED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Existing connection dropped	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**ip**' - 원격 호스트의 IP. '**why**' - 오류에 대한 자세한 텍스트.
	Warning(경고) 클러스터에 대한 연결이 삭제될 경우 전송됨.	
CLUSTER.CC_ERROR.FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Connection failure	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**ip**' - 원격 호스트의 IP. '**why**' - 오류에 대한 자세한 텍스트.
	Warning(경고) 클러스터에 대한 연결이 실패할 경우 전송됨.	
CLUSTER.CC_ERROR.FORWARD_FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Message forward failed, no upstream connection	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**ip**' - 원격 호스트의 IP. '**why**' - 오류에 대한 자세한 텍스트.
	Critical(중대). 어플라이언스가 데이터를 클러스터의 시스템으로 전달할 수 없을 경우 전송됨.	

알림 이름	메시지 및 설명	매개변수
CLUSTER.CC_ERROR.NOROUTE	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=No route found Critical(중대). 시스템이 클러스터에 있는 또 다른 시스템에 대한 경로를 얻을 수 없을 경우 전송됨.	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**ip**' - 원격 호스트의 IP. '**why**' - 오류에 대한 자세한 텍스트.
CLUSTER.CC_ERROR.SSH_KEY	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Invalid host key Critical(중대). 잘못된 SSH 호스트 키가 있을 경우 전송됨.	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**ip**' - 원격 호스트의 IP. '**why**' - 오류에 대한 자세한 텍스트.
CLUSTER.CC_ERROR.TIMEOUT	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Operation timed out Warning(경고) 지정된 작업이 시간 초과될 경우 전송됨.	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**ip**' - 원격 호스트의 IP. '**why**' - 오류에 대한 자세한 텍스트.
CLUSTER.CC_ERROR_NOIP	Error connecting to cluster machine $name - $error - $why Critical(중대). 어플라이언스가 클러스터에 있는 또 다른 시스템에 대한 유효한 IP 주소를 얻을 수 없을 경우 전송됨.	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**why**' - 오류에 대한 자세한 텍스트.
CLUSTER.CC_ERROR_NOIP. AUTH_ERROR	Error connecting to cluster machine $name - $error - whyerror:=Machine does not appear to be in the cluster Critical(중대). 클러스터의 시스템에 연결 시 인증 오류가 발생할 경우 전송됨. 이 오류는 시스템이 클러스터의 구성원이 아닌 경우 발생할 수 있습니다.	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**why**' - 오류에 대한 자세한 텍스트.
CLUSTER.CC_ERROR_NOIP. DROPPED	Error connecting to cluster machine $name - $error - whyerror:=Existing connection dropped Warning(경고) 시스템이 클러스터에 있는 또 다른 시스템에 대한 유효한 IP 주소를 가져올 수 없을 경우, 그리고 클러스터에 대한 연결이 삭제될 경우 전송됨.	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**why**' - 오류에 대한 자세한 텍스트.

알림 이름	메시지 및 설명	매개변수
CLUSTER.CC_ERROR_NOIP.FAILED	Error connecting to cluster machine $name - $error - whyerror:=Connection failure	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**why**' - 오류에 대한 자세한 텍스트.
	Warning(경고) 알 수 없는 연결 실패가 발생할 경우, 그리고 시스템이 클러스터에 있는 또 다른 시스템에 대한 유효한 IP 주소를 가져올 수 없을 경우 전송됨.	
CLUSTER.CC_ERROR_NOIP.FORWARD_FAILED	Error connecting to cluster machine $name - $error - whyerror:=Message forward failed, no upstream connection	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**why**' - 오류에 대한 자세한 텍스트.
	Critical(중대). 시스템이 클러스터에 있는 또 다른 시스템에 대한 유효한 IP 주소를 가져올 수 없을 경우, 그리고 어플라이언스가 시스템에 데이터를 전달할 수 없을 경우 전송됨.	
CLUSTER.CC_ERROR_NOIP.NOROUTE	Error connecting to cluster machine $name - $error - whyerror:=No route found	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**why**' - 오류에 대한 자세한 텍스트.
	Critical(중대). 시스템이 클러스터에 있는 또 다른 시스템에 대한 유효한 IP 주소를 가져올 수 없을 경우, 그리고 해당 시스템에 대한 경로를 가져올 수 없을 경우 전송됨.	
CLUSTER.CC_ERROR_NOIP.SSH_KEY	Error connecting to cluster machine $name - $error - whyerror:=Invalid host key	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**why**' - 오류에 대한 자세한 텍스트.
	Critical(중대). 시스템이 클러스터에 있는 또 다른 시스템에 대한 유효한 IP 주소를 가져올 수 없을 경우, 그리고 유효한 SSH 호스트 키를 가져올 수 없을 경우 전송됨.	
CLUSTER.CC_ERROR_NOIP.TIMEOUT	Error connecting to cluster machine $name - $error - whyerror:=Operation timed out	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**why**' - 오류에 대한 자세한 텍스트.
	Warning(경고) 시스템이 클러스터에 있는 또 다른 시스템에 대한 유효한 IP 주소를 가져올 수 없을 경우, 그리고 지정된 작업이 시간 초과될 경우 전송됨.	
CLUSTER.SYNC.PUSH_ALERT	Overwriting $sections on machine $name	'**name**' - 시스템의 호스트 이름 및/또는 일련 번호. '**sections**' - 전송되는 클러스터 섹션의 목록.
	Critical(중대). 컨피그레이션 데이터가 동기화되지 않고 원격 호스트로 전송될 경우 전송됨.	

네트워크 설정 변경

이 섹션에서는 어플라이언스의 네트워크 작업을 구성하는 데 사용되는 기능에 대해 설명합니다. 이러한 기능을 사용하면 시스템 설정 마법사 사용 , 28 페이지의 시스템 설정 마법사(또는 **systemsetup** 명령)를 통해 구성한 호스트 이름, DNS 및 라우팅 설정에 직접 액세스할 수 있습니다.

다음과 같은 기능에 대해 설명합니다.

- **sethostname**
- DNS 컨피그레이션(GUI 또는 **dnsconfig** 명령을 통해)
- 라우팅 구성(GUI와 **routeconfig** 및 **setgateway** 명령을 통해)
- **dnsflush**
- Passphrase(암호 문구)
- 네트워크 액세스
- 로그인 배너

시스템 호스트 이름 변경

호스트 이름은 시스템을 식별하는 데 사용됩니다. 인증된 호스트 이름을 입력해야 합니다. 호스트 이름을 변경하려면 다음을 수행합니다.

- 웹 인터페이스에서 Network(네트워크) > IP Interfaces(IP 인터페이스)를 클릭하고, Management(관리)를 클릭하고, Hostname(호스트 이름)에서 호스트 이름을 변경합니다.
- CLI에서 sethostname 명령을 사용합니다.

참고 새 호스트 이름은 변경 사항을 커밋할 때까지 적용되지 않습니다.

DNS(Domain Name System) 설정 구성

GUI의 Network(네트워크) 메뉴에서 DNS 페이지를 통해 또는 dnsconfig 명령을 통해 어플라이언스의 DNS 설정을 구성할 수 있습니다.

다음 설정을 구성할 수 있습니다.

- 인터넷의 DNS 서버를 사용할지 아니면 자신의 서버를 사용할지 여부, 그리고 사용할 특정 서버
- DNS 트래픽에 사용할 인터페이스
- 역방향 DNS 조회가 시간 초과될 때까지 기다릴 시간(초)
- DNS 캐시 지우기

DNS 서버 지정

AsyncOS에서는 인터넷 루트 DNS 서버, 조직의 자체 DNS 서버 또는 사용자가 지정한 공인 DNS 서버를 사용할 수 있습니다. 인터넷 루트 서버를 사용할 때 특정 도메인에 대해 사용할 대체 서버를 지정

할 수 있습니다. 대체 DNS 서버는 단일 도메인에 적용되므로, 해당 도메인에 대해 신뢰할 수 있는 서버여야 합니다(확정된 DNS 레코드 제공).

인터넷의 DNS 서버를 사용하지 않을 경우 AsyncOS는 DNS 서버의 "분리"를 지원합니다. 자체 내부 서버를 사용 중인 경우 예외 도메인 및 관련된 DNS 서버를 지정할 수 있습니다.

"분리 DNS"를 설정할 때 in-addr.arpa(PTR) 항목도 설정해야 합니다. 따라서 예를 들어 ".eng" 쿼리를 네임서버 1.2.3.4로 리디렉션하고자 하며 현재 .eng 항목이 172.16 네트워크에 있는 경우, 분리 DNS 컨피그레이션에서 도메인으로 "eng,16.172.in-addr.arpa"를 지정해야 합니다.

여러 항목 및 우선 순위

입력하는 각 DNS 서버에 대해 숫자 우선 순위를 지정할 수 있습니다. AsyncOS는 0과 가장 가까운 우선 순위의 DNS 서버를 사용하려고 시도합니다. 해당 DNS 서버가 응답하지 않으면 AsyncOS는 다음 우선 순위의 서버를 사용하려고 시도합니다. 동일한 우선 순위의 DNS 서버에 대해 여러 항목을 지정하는 경우 시스템은 쿼리를 수행할 때마다 해당 우선 순위의 DNS 서버 목록을 임의로 지정합니다. 시스템은 첫 번째 쿼리가 만료 또는 "시간 초과"될 때까지 잠깐 기다리고, 두 번째 쿼리에 대해서는 조금 더 기다립니다. 대기 시간은 DNS 서버 수 및 구성된 우선 순위에 따라 달라집니다. 대기 시간 길이는 특정 우선 순위의 모든 IP 주소에 대해 동일합니다. 첫 번째 우선 순위의 시간 초과가 가장 짧고, 이후의 우선 순위는 시간 초과가 조금씩 길어집니다. 시간 초과 기간은 약 60초입니다. 우선 순위가 하나 있는 경우 해당 우선 순위에서 각 서버에 대한 시간 초과는 60초입니다. 우선 순위가 2개 있는 경우 첫 번째 우선 순위에서 각 서버의 시간 초과는 15초이고, 두 번째 우선 순위에서 각 서버의 시간 초과는 45초입니다. 우선 순위가 3개 있는 경우 시간 초과는 각각 5, 10, 45입니다.

예를 들어 4개의 DNS 서버를 구성하고 있으며 그중 2개의 우선 순위는 0, 하나는 1, 하나는 2라고 가정해보겠습니다.

표 ***95: DNS*** 서버**,** 우선 순위 및 시간 초과 간격의 예

Priority(우선순위**)**	서버	시간 초과 **(**초**)**
0	1.2.3.4, 1.2.3.5	5, 5
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS는 우선 순위 0인 두 서버 가운데에서 임의로 하나를 선택합니다. 우선 순위 0 서버 중 하나가 다운되면 나머지가 사용됩니다. 우선 순위 0 서버가 둘 다 다운되면 우선 순위 1 서버(1.2.3.6)가 사용되고, 그런 다음 최종적으로 우선 순위 2(1.2.3.7) 서버가 사용됩니다.

시간 초과 기간은 우선 순위 0 서버 둘에 대해 동일하며, 우선 순위 1 서버에 대해서는 좀 더 길고, 우선 순위 2 서버에 대해 더 깁니다.

인터넷 루트 서버 사용

AsyncOS DNS 확인자는 고성능 이메일 전달을 위해 필요한 대량의 동시 DNS 연결을 수용하도록 설계되었습니다.

참고 기본 DNS 서버를 인터넷 루트 서버가 아닌 다른 서버로 설정하기로 선택하는 경우, 해당 서버는 자신이 인증된 서버로 있지 않은 도메인에 대한 쿼리를 재귀적으로 확인할 수 있어야 합니다.

역방향 DNS 조회 시간 초과

어플라이언스는 이메일을 전송 또는 수신하기 위해 리스너에 연결된 모든 원격 호스트에서 "이중 DNS 조회"를 수행하려고 시도합니다. 즉, 시스템은 이중 DNS 조회를 수행하여 원격 호스트 IP 주소의 유효성을 획득하고 확인합니다. 이는 연결하는 호스트의 IP 주소에 대한 역방향 DNS(PTR) 조회 및 그 뒤에 오는 PTR 조회의 결과에 대한 정방향 DNS(A) 조회로 구성됩니다. 그런 다음 시스템은 A 조회의 결과가 PTR 조회의 결과와 일치하는지를 확인합니다. 결과가 일치하지 않거나 A 레코드가 존재하지 않으면 시스템은 IP 주소만 사용하여 HAT(Host Access Table)의 항목 일치를 확인합니다. 이 특별한 시간 초과 기간은 이 조회에만 적용되며 여러 항목 및 우선 순위, 987 페이지에서 설명한 일반 DNS 시간 초과와는 관련이 없습니다.

기본값은 각 DNS 서버에 대해 20초입니다. DNS 서버에 대한 항목이 여러 개인 경우 총 시간 초과 값은 (DNS 서버 수와 역방향 DNS 조회 시간 초과 값을 곱한 값) 초입니다. 예를 들어, DNS 서버가 8개 있고 역방향 DNS 조회 시간 초과 값이 20초인 경우, 총 시간 초과 값은 (8 * 20) = 160초입니다.

시간(초)으로 '0'을 입력하여 모든 리스너에서 전역적으로 역방향 DNS 조회 시간 초과를 비활성화할 수 있습니다. 값을 0초로 설정하면, 역방향 DNS 조회가 시도되지 않으며 대신 표준 시간 초과 응답이 즉시 반환됩니다. 또한 수신 호스트의 인증서에 호스트 IP 조회에 매핑되는 CN(common name)이 있는 경우 TLS 검증 연결을 요구하는 도메인에 대에 어플라이언스가 메일을 전달하는 것도 차단됩니다.

DNS 알림

때때로 어플라이언스가 재부팅될 때 "Failed to bootstrap the DNS cache(DNS 캐시 부트스트랩 실패)"라는 메시지와 함께 알림이 생성될 수 있습니다. 이러한 메시지는 시스템이 기본 DNS 서버에 연결할 수 없음을 나타냅니다. 이는 네트워크 연결이 설정되기 전 DNS 하위 시스템이 온라인 상태가 되는 경우 부팅 시 발생할 수 있습니다. 이 메시지가 다른 때에 나타나면 네트워크 문제를 나타내거나 DNS 구성이 유효한 서버를 가리키고 있지 않음을 나타낼 수 있습니다.

DNS 캐시 지우기

GUI의 Clear Cache(캐시 지우기) 버튼 또는 dnsflush 명령(dnsflush 명령에 대한 자세한 내용은 AsyncOS for Cisco Email Security Appliances CLI 참조 가이드 참고)은 DNS 캐시의 모든 정보를 지웁니다. 로컬 DNS 시스템이 변경되었을 때 이 기능을 사용하도록 선택할 수 있습니다. 이 명령은 즉시 수행되며, 캐시가 다시 채워지는 동안 일시적으로 성능 저하가 발생할 수 있습니다.

그래픽 사용자 인터페이스를 통해 DNS 설정 구성

단계 **1** **Network**(네트워크) **> DNS**를 선택합니다.

단계 **2** **Edit Settings**(설정 수정)를 클릭합니다.

단계 **3** 인터넷 루트 DNS 서버를 사용할지 아니면 조직 자체의 내부 DNS 서버를 사용할지를 선택한 다음 대체 DNS 서버를 지정합니다.

단계 **4** 조직 자체의 DNS 서버를 사용하려면 서버 ID를 입력하고 **Add Row(**행 추가**)**를 클릭합니다. 각 서버에 대해 이를 반복합니다. 자체 DNS 서버를 입력할 때 우선 순위도 지정합니다. 자세한 내용은 DNS 서버 지정, 986 페이지을 참고하십시오.

단계 **5** 특정 도메인에 대해 대체 DNS 서버를 지정할 경우 도메인 및 대체 DNS 서버 IP 주소를 입력합니다. 도메인을 추가하려면 **Add Row(**행 추가**)**를 클릭합니다.

참고 쉼표로 도메인 이름을 구분하여 단일 DNS 서버에 대해 여러 도메인을 입력할 수 있습니다. 또한 쉼표로 여러 IP 주소를 구분하여 여러 DNS 서버를 입력할 수 있습니다.

단계 **6** DNS 트래픽에 대한 인터페이스를 선택합니다.

단계 **7** 역방향 DNS 조회를 취소하기 전에 기다릴 시간(초)을 입력합니다.

단계 **8** 또한 **Clear Cache(**캐시 지우기**)**를 클릭하여 DNS 캐시를 지울 수 있습니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

TCP/IP 트래픽 경로 구성

일부 네트워크 환경에서는 표준 기본 게이트웨이 이외의 트래픽 경로를 사용해야 합니다.

Email Security Appliance는 IPv4(Internet Protocol version 4) 및 IPv6(Internet Protocol version 6) 고정 경로를 모두 사용할 수 있습니다.

CLI의 routeconfig 명령을 통해 고정 경로를 관리하거나 다음 절차를 사용할 수 있습니다.

단계 **1** **Network(**네트워크**) > Routing(**라우팅**)**을 선택합니다.

단계 **2** 만들려는 고정 경로 유형(IPv4 또는 IPv6)에 대해 **Add Route(**경로 추가**)**를 클릭합니다.

단계 **3** 경로의 이름을 입력합니다.

단계 **4** 대상 IP 주소를 입력합니다.

단계 **5** 게이트웨이 IP 주소를 입력합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

기본 게이트웨이 구성

CLI의 setgateway 명령을 사용하여 기본 게이트웨이를 구성하거나 다음 절차를 사용할 수 있습니다.

단계 **1** **Network(**네트워크**) > Routing(**라우팅**)**을 선택합니다.

단계 **2** 수정할 인터넷 프로토콜 버전의 경로 목록에서 **Default Route(**기본 경로**)**를 클릭합니다.

단계 **3** 게이트웨이 IP 주소를 변경합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

SSL 설정 구성

SSL Configuration Settings(SSL 컨피그레이션 설정) 페이지 또는 sslconfig 명령을 사용하여 어플라이언스에 대한 SSL 설정을 구성할 수 있습니다.

단계 **1** **System Administration(**시스템 관리**)** > **SSL Configuration Settings(SSL** 컨피그레이션 설정**)**를 클릭합니다.

단계 **2** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** 요구 사항에 따라 다음을 수행합니다.

- GUI HTTPS SSL 설정을 지정합니다. GUI HTTPS 아래에서 사용할 SSL 방법 및 암호를 지정합니다.
- 인바운드 SMTP SSL 설정을 지정합니다. Inbound SMTP(인바운드 SMTP) 아래에서 사용할 SSL 방법 및 암호를 지정합니다.
- 아웃바운드 SMTP SSL 설정을 지정합니다. Outbound SMTP(아웃바운드 SMTP) 아래에서 사용할 SSL 방법 및 암호를 지정합니다.

지금까지는

- SSL v2 및 TLS v1 방법을 동시에 활성화할 수 없습니다. 그러나 이러한 방법을 SSL v3 방법과 함께 활성화할 수 있습니다.
- TLS v1.0 및 v1.1 방법을 동시에 활성화할 수 없습니다. 그러나 이러한 방법을 TLS v1.2 방법과 함께 활성화할 수 있습니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

단계 **5** **Commit Changes(**변경 커밋**)**를 클릭합니다.

고급 보안에 대해 SSLv3 비활성화

고급 보안의 경우 다음 서비스에 대해 SSLv3을 비활성화할 수 있습니다.

- Updater
- URL 필터링
- 최종 사용자 격리
- LDAP

위 서비스에 대해 SSLv3을 활성화 또는 비활성화하려면 sslv3config 명령을 사용합니다. 다음 예는 최종 사용자 격리에 대해 SSLv3을 비활성화하는 방법을 보여줍니다.

```
mail.example.com> sslv3config
     Current SSLv3 Settings:
```

```
    ------------------------------------------------
                UPDATER     :     Enabled
            WEBSECURITY     :     Enabled
                    EUQ     :     Enabled
                   LDAP     :     Enabled
    ------------------------------------------------
Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]> setup
Choose the service to toggle SSLv3 settings:
1. EUQ Service
2. LDAP Service
3. Updater Service
4. Web Security Service
[1]>
Do you want to enable SSLv3 for EUQ Service ? [Y]>n
Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]>
```

시스템 시간

어플라이언스에서 시스템 시간을 설정하려면 사용할 표준 시간대를 설정하거나, NTP 서버 및 쿼리 인터페이스를 선택하고, GUI에서 System Administration(시스템 관리) 메뉴의 Time Zone or Time Settings(표준 시간대 또는 시간 설정) 페이지를 사용합니다. CLI에서는 ntpconfig, settime 및 settz 명령을 사용할 수 있습니다.

또한 **System Administration(**시스템 관리**) > Time Settings(**시간 설정**)** 페이지에서 또는 tzupdate CLI 명령을 사용하여 AsyncOS에서 사용할 표준 시간대 파일을 확인할 수 있습니다.

표준 시간대 선택

GUI의 System Administration(시스템 관리) 메뉴를 통해 사용 가능한 Time Zone(표준 시간대) 페이지에는 어플라이언스에 대한 표준 시간대가 표시됩니다. 특정 표준 시간대 또는 GMT 오프셋을 선택할 수 있습니다.

단계 **1** **System Administration(**시스템 관리**) > Time Zone(**표준 시간대**)** 페이지에서 **Edit Settings(**설정 수정**)**를 클릭합니다.
단계 **2** 풀다운 메뉴에서 지역, 국가 및 표준 시간대를 선택합니다.
단계 **3** 변경 사항을 제출 및 커밋합니다.

GMT 차감 시간 선택

단계 **1** **System Administration(**시스템 관리**) > Time Zone(**표준 시간대**)** 페이지에서 **Edit Settings(**설정 수정**)**를 클릭합니다.
단계 **2** 지역 목록에서 GMT Offset(GMT 오프셋)을 선택합니다.

단계 **3** Time Zone(표준 시간대) 목록에서 오프셋을 선택합니다. 오프셋이란 GMT(본초자오선)에 도달하기 위해 추가하거나 빼야 할 시간을 가리킵니다. 앞에 빼기 기호("-")가 오는 시간은 본초자오선의 동쪽입니다. 더하기 기호("+")는 본초자오선의 왼쪽을 가리킵니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

시간 설정 수정

다음 방법 중 하나를 사용하여 어플라이언스에 대한 시간 설정을 수정할 수 있습니다.

- (권장 사항) NTP(Network Time Protocol)를 사용하여 어플라이언스 시스템 시간 설정, 992 페이지
- 수동으로 어플라이언스 시스템 시간 설정 , 992 페이지

(권장 사항) NTP(Network Time Protocol)를 사용하여 어플라이언스 시스템 시간 설정

이것은 특히 어플라이언스가 다른 디바이스와 통합된 경우 권장되는 시간 유지 방법입니다. 모든 통합된 디바이스는 동일한 NTP 서버를 사용해야 합니다.

단계 **1** System Administration(시스템 관리) > Time Settings(시간 설정) 페이지로 이동합니다.

단계 **2** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** Time Keeping Method(시간 유지 방법) 섹션에서 Use Network Time Protocol(NTP 사용)을 선택합니다.

단계 **4** NTP 서버 주소를 입력하고 **Add Row(**행 추가**)**를 클릭합니다. 여러 NTP 서버를 추가할 수 있습니다.

단계 **5** 목록에서 NTP 서버를 삭제하려면 해당 서버의 휴지통 아이콘을 클릭합니다.

단계 **6** NTP 쿼리를 위한 인터페이스를 선택합니다. 이것은 NTP 쿼리가 시작되는 IP 주소입니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

수동으로 어플라이언스 시스템 시간 설정

이 시간 유지 방법은 일반적으로 권장되지 않습니다. 대신 Network Time Protocol 서버를 사용하십시오.

단계 **1** System Administration(시스템 관리) > Time Settings(시간 설정) 페이지로 이동합니다.

단계 **2** **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** Time Keeping Method(시간 유지 방법) 섹션에서 Set Time Manually(수동으로 시간 설정)를 선택합니다.

단계 **4** 월, 일, 년, 시, 분 및 초를 입력합니다.

단계 **5** A.M 또는 P.M을 선택합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

보기 맞춤화

즐겨찾기 페이지 사용

(로컬 인증 관리자 사용자만) 가장 많이 사용하는 페이지의 빠른 액세스 목록을 만들 수 있습니다.

변경 후	수행해야 할 작업
즐겨찾기 목록에 페이지 추가	추가할 페이지로 이동하고, 창의 상단 오른쪽에 있는 My Favorites(내 즐겨찾기) 메뉴에서 **Add This Page To My Favorites(**이 페이지를 내 즐겨찾기에 추가**)**를 선택합니다. My Favorites(내 즐겨찾기)를 변경하는 경우에는 커밋이 필요하지 않습니다.
즐겨찾기 순서 바꾸기	**My Favorites(**내 즐겨찾기**) > View All My Favorites(**내 즐겨찾기 모두 보기**)**를 선택하고 즐겨찾기를 원하는 순서로 끌어옵니다.
즐겨찾기 삭제	**My Favorites(**내 즐겨찾기**) > View All My Favorites(**내 즐겨찾기 모두 보기**)**를 선택하고 즐겨찾기를 삭제합니다.
즐겨찾기 페이지로 이동	창의 오른쪽 상단 근처에 있는 **My Favorites(**내 즐겨찾기**)** 메뉴에서 페이지를 선택합니다.
맞춤형 보고 페이지 보기 또는 작성	My Dashboard(내 대시보드) 페이지 , 797 페이지를 참조하십시오.

사용자 기본 설정 지정

로컬 사용자는 각 계정에 대해 언어 등의 기본 설정을 정의할 수 있습니다. 이러한 설정은 사용자가 어플라이언스에 처음 로그인할 때 기본적으로 적용됩니다. 기본 설정은 각 사용자에 대해 저장되며, 사용자가 어떤 클라이언트 시스템에서 어플라이언스에 로그인하든 동일합니다.

사용자가 이러한 설정을 변경하고 커밋하지 않으면, 다시 로그인할 때 기본값으로 되돌아갑니다.

참고 외부에서 인증되는 사용자는 이 기능을 이용할 수 없습니다. 이러한 사용자는 Options(옵션) 메뉴에서 직접 언어를 선택할 수 있습니다.

단계 **1** 기본 설정을 정의할 사용자 계정으로 어플라이언스에 로그인합니다.

단계 **2** **Options(**옵션**) > Preferences(**기본 설정**)**를 선택합니다. 옵션 메뉴는 창의 오른쪽 상단에 있습니다.

단계 **3** **Edit Preferences(**기본 설정 수정**)**를 클릭합니다.

단계 **4** 설정을 구성합니다.

기본 설정	설명
Language Display(언어 표시)	웹 인터페이스 및 CLI에서 AsyncOS for Web이 사용하는 언어
Landing Page(랜딩 페이지)	사용자가 어플라이언스에 로그인할 때 표시되는 페이지
Reporting Time Range Displayed(보고 시간 범위 표시)(기본값)	Reporting(보고) 탭의 보고서에 대해 표시되는 기본 시간 범위
Number of Reporting Rows Displayed(보고 행 수 표시)	기본적으로 각 보고서에 대해 표시되는 데이터 행의 수

단계 **5** 변경 사항을 제출 및 커밋합니다.

단계 **6** 페이지 하단에 있는 **Return to previous page(**이전 페이지로 돌아가기**)** 링크를 클릭합니다.

Internet Explorer 호환성 모드 재정의

웹 인터페이스 렌더링을 개선하려면 Internet Explorer 호환성 모드 재정의를 활성화하는 것이 좋습니다.

참고 이 기능 활성화가 조직의 정책과 맞지 않으면 이 기능을 비활성화할 수 있습니다.

단계 **1** **System Administration(**시스템 관리**) > General Settings(**일반 설정**)**를 클릭합니다.

단계 **2** **Override IE Compatibility Mode(IE** 호환성 모드 재정의**)** 확인란을 선택합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

최대 HTTP 헤더 크기 구성

이제 CLI에서 `adminaccessconfig > maxhttpheaderfieldsize` 명령을 사용하여 어플라이언스로 전송되는 HTTP 요청의 최대 HTTP 헤더 크기를 구성할 수 있습니다.

HTTP 헤더 필드 크기의 기본값은 4096(4KB)이고 최대값은 33554432(32MB)입니다.

서비스 엔진 다시 시작 및 상태 보기

CLI에서 `diagnostic > services`sub 명령을 사용하여 다음 작업을 수행할 수 있습니다.

- 어플라이언스를 재부팅하지 않고도 어플라이언스에서 활성화된 서비스 엔진을 다시 시작합니다.
- 어플라이언스에서 활성화된 서비스 엔진의 상태를 봅니다.

예: DLP 엔진의 상태 보기

다음 예에서는 `services` 명령을 사용하여 어플라이언스에서 활성화된 DLP 엔진의 상태를 확인합니다.

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> services

Choose one of the following services:
- ANTISPAM - Anti-Spam services
- ANTIVIRUS - Anti-Virus services
- DLP - Cisco Data Loss Prevention services
- ENCRYPTION - Encryption services
- GRAYMAIL - Graymail services
- REPORTING - Reporting associated services
- SBRS - Reputation Engine services
- TRACKING - Tracking associated services
- URLFILTERING - URL Filtering
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> dlp

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> status

Cisco Data Loss Prevention has been up for 3s.
```

예: 그레이메일 엔진 다시 시작

다음 예에서는 `services` 명령을 사용하여 어플라이언스에 활성화된 그레이메일을 다시 시작합니다.

```
mail.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
```

```
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> services

Choose one of the following services:
- ANTISPAM - Anti-Spam services
- ANTIVIRUS - Anti-Virus services
- DLP - Cisco Data Loss Prevention services
- ENCRYPTION - Encryption services
- GRAYMAIL - Graymail services
- REPORTING - Reporting associated services
- SBRS - Reputation Engine services
- TRACKING - Tracking associated services
- URLFILTERING - URL Filtering
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> graymail

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> restart
```

37 장

CLI를 사용한 관리 및 모니터링

이 장에는 다음 섹션이 포함되어 있습니다.

CLI를 사용한 관리 및 모니터링 개요

CLI를 이용한 Email Security Appliance의 관리 및 모니터링에는 다음과 같은 작업 유형이 포함됩니다.

- 메시지 활동 모니터링.
  - 이메일 파이프라인에서 어플라이언스가 처리 중인 메시지, 수신자 및 반송 수신자의 원시 숫자
  - 마지막 1분, 5분 또는 15분 기반으로 시간당 메시지 전달 또는 메시지 반송 속도
- 시스템 리소스 모니터링 예:
  - 메모리 사용량
  - 디스크 공간
  - 연결 수
- SNMP(Simple Network Management Protocol)를 사용하여 가능한 시스템 기능 장애 모니터링 예:
  - 팬 장애
  - 업데이트 실패
  - 비정상적으로 높은 어플라이언스 온도
- 파이프라인 내에서 이메일 관리. 예:
  - 대기열에서 수신자 삭제
  - 다른 호스트로 메시지 리디렉션
  - 수신자를 삭제하거나 메시지를 리디렉션하여 대기열 지우기

- 이메일 수신, 전달 또는 작업 대기열 처리 일시 중단 또는 다시 시작
- 특정 메시지 찾기

사용 가능한 모니터링 구성 요소 읽기

이벤트 카운터 읽기

카운터는 시스템에서 발생하는 각종 이벤트의 누계를 제공합니다. 각 카운터에 대해 카운터 재설정 이후, 마지막 재부팅 이후, 그리고 시스템 수명 주기 전체에서 발생한 총 이벤트 수를 볼 수 있습니다.

카운터는 이벤트가 발생할 때마다 증가하며 세 가지 버전으로 표시됩니다.

초기화	**resetcounters** 명령으로 마지막 카운터 재설정 이후
실행 시간	마지막 시스템 재부팅 이후
수명 주기	Cisco 어플라이언스의 수명 주기 전체

다음 표에서는 Cisco 어플라이언스를 모니터링할 때 사용 가능한 카운터 및 해당 설명을 보여줍니다.

참고 여기에 나열된 것이 전체 목록입니다. 선택하는 표시 옵션 또는 명령에 따라 표시되는 카운터가 다릅니다. 이 목록은 참조용으로 사용하십시오.

표 ***96:*** 카운터

통계	설명
Receiving(수신)	
수신 메시지	전달 대기열에서 수신된 메시지 수.
수신된 수신자	수신된 모든 메시지의 수신자 수.
생성된 바운스 수신자	시스템에 의해 반송이 생성되어 전달 대기열에 삽입된 수신자 수.
Rejection(거부)	
거부된 수신자	RAT(Recipient Access Table) 또는 조기 연결 종료를 비롯한 예기치 못한 프로토콜 협상 때문에 전달 대기열에서의 수신이 거부된 수신자 수.

통계	설명
삭제(drop)된 메시지	필터 삭제 작업 때문에 전달 대기열에서의 수신이 거부되었거나 Black Hole 대기열 리스너에 의해 수신된 메시지 수. 별칭 테이블의 /dev/null 항목으로 전달된 메시지도 삭제된 메시지로 간주됩니다. 안티스팸 필터링에 의해 삭제된 메시지(시스템에서 활성화된 경우)도 이 카운터를 증가시킵니다.
Queue(대기열)	
Soft Bounced Events(소프트 반송된 이벤트)	소프트 반송 이벤트의 수 - 여러 번 소프트 반송된 메시지는 소프트 반송 이벤트도 여러 번 계산됩니다.
Completion(완료)	
완료된 수신자	하드 반송된 수신자, 전달된 수신자 및 삭제된 수신자 전체 합계. 전달 대기열에서 제거된 수신자.
Hard Bounced Recipients(하드 반송된 수신자)	DNS 하드 반송, 5XX 하드 반송, 필터 하드 반송, 만료된 하드 반송 및 기타 하드 반송 전체 합계. 수신자에게 메시지를 전달하려다 해당 전달이 즉시 종료된 실패한 시도.
DNS 하드 바운스	수신자에게 메시지를 전달하려고 시도하다가 발생한 DNS 오류.
5XX 하드 바운스	수신자에게 메시지를 전달하려고 시도하는 동안 대상 메일 서버에서 "5XX" 응답 코드 반환.
만료된 하드 바운스	전달 대기열에서 허용되는 최대 시간 또는 최대 연결 시도 횟수를 초과한 메시지 수신자.
필터 하드 바운스	수신자 전달이 일치하는 필터 bounce 작업에 의해 선점되었습니다. 안티스팸 필터링에 의해 삭제된 메시지(시스템에서 활성화된 경우)도 이 카운터를 증가시킵니다.
기타 하드 바운스	메시지 전달 중에 예기치 않은 오류가 발생했거나 bouncerecipients 명령을 통해 메시지가 수신자에게 명시적으로 반송되었습니다.
Delivered Recipients(전달된 수신자)	메시지가 수신자에게 성공적으로 전달되었습니다.
삭제된 수신자	deleterecipients 명령을 통해 명시적으로 삭제되었거나 Global Unsubscribe Hit(전역 수신 거부 히트)에 해당된 총 메시지 수신자 수.
전역 가입 취소 횟수	일치하는 전역 수신 거부 설정 때문에 메시지 수신자가 삭제되었습니다.

통계	설명
Current IDs(현재 ID)	메시지에 할당된 마지막 메시지 ID가 전달 대기열에 삽입됨. MID는 Cisco 어플라이언스에서 수신한 모든 메시지와 연결되며 메일 로그에서 추적할 수 있습니다. MID는 231에서 영(0)으로 재설정됩니다.
메시지 ID(MID)	
ICID(Injection Connection ID)	리스너 인터페이스에 대한 연결에 할당된 마지막 Injection Connection ID. ICID는 231에서 롤오버됩니다(0으로 재설정).
DCID(Delivery Connection ID)	대상 메일 서버에 대한 연결에 할당된 마지막 Delivery Connection ID. DCID는 231에서 롤오버됩니다(0으로 재설정).

시스템 게이지 읽기

게이지는 메모리, 디스크 공간, 활성 연결 등과 같은 시스템 리소스의 현재 사용률을 보여줍니다.

다음 표에서는 Cisco 어플라이언스를 모니터링할 때 사용 가능한 게이지 및 해당 설명을 보여줍니다.

참고 여기에 나열된 것이 전체 목록입니다. 선택하는 표시 옵션 또는 명령에 따라 표시되는 게이지가 다릅니다. 이 목록은 참조용으로 사용하십시오.

표 ***97:*** 센서

통계	설명
System Gauges(시스템 게이지)	시스템에서 사용 중인 물리적 RAM(Random Access Memory)의 비율.
RAM 사용률	
CPU 사용률	CPU 사용의 비율.

통계	설명
디스크 I/O 사용률	사용 중인 디스크 I/O의 비율. 참고 Disk I/O Utilization(디스크 I/O 사용률) 게이지는 알려진 값의 규모를 기준으로 수치를 표시하지 않습니다. 대신 마지막 재부팅 이후 시스템에서 확인한 I/O 사용률 및 최대값을 기준으로 한 규모를 표시합니다. 따라서 게이지가 100%를 표시하면 시스템은 재부팅 이후 가장 높은 I/O 사용률을 경험하는 것입니다(이는 전체 시스템의 물리적 디스크 I/O의 100%를 나타내는 것이 아닐 수 있음).
리소스 보존(conservation)	값은 0에서 60 또는 999 사이입니다. 0~60의 수는 시스템이 주요 시스템 리소스의 급속한 고갈을 막기 위해 메시지 수락을 줄이고 있음을 나타냅니다. 숫자가 높을수록 수락 감소 수준이 더 높음을 나타냅니다. 영(0)은 수락이 감소되지 않음을 나타냅니다. 이 게이지가 999를 표시하면 시스템은 "리소스 절약 모드"로 들어가고 메시지를 수락하지 않게 됩니다. 시스템이 리소스 절약 모드로 들어가거나 이 모드에서 나올 때마다 알림 메시지가 전송됩니다.
디스크 사용률: 로그	상태 로그에서 LogUsd로 표시되고 XML 상태에서 log_used로 표시되는, 로그에 사용되고 있는 디스크의 비율.
Connections Gauges(연결 게이지)	
현재 인바운드 연결	리스너 인터페이스에 대한 현재 인바운드 연결.
현재 아웃바운드 연결	대상 메일 서버에 대한 현재 아웃바운드 연결.
Queue Gauges(대기열 게이지)	
Active Recipients(활성 수신자)	전달 대기열에 있는 메시지 수신자. Unattempted Recipients(시도되지 않은 수신자) 및 Attempted Recipients(시도된 수신자) 합계.
전달을 시도하지 않은 수신자	Active Recipients(활성 수신자)의 하위 범주. 아직 전달이 시도되지 않은 대기열의 메시지 수신자.
전달을 시도했던 수신자	Active Recipients(활성 수신자)의 하위 범주. 전달을 시도했지만 소프트 반송 이벤트 때문에 실패한 대기열의 메시지 수신자.
작업 대기열에 있는 메시지	대기열에 추가되기 전 별칭 테이블 확장, 가장, 안티스팸, 안티바이러스 검사, 메시지 필터, LDAP 쿼리 등으로 처리되기를 기다리는 메시지의 수.

통계	설명
Messages in Quarantine(격리에 있는 메시지)	격리에 있는 고유한 메시지 및 릴리스 또는 삭제했지만 아직 처리되지 않은 메시지 수. 예를 들어 Outbreak(보안 침해)의 모든 격리된 메시지를 릴리스하는 경우 보안 침해의 총 메시지 수는 즉시 영(0)이 되지만, 모두 전달될 때까지 이 필드는 격리된 메시지를 반영합니다.
Destinations in Memory(메모리에 있는 대상)	메모리에 있는 대상 도메인의 수. 전달해야 할 메시지가 있는 각 도메인의 경우 대상 개체는 메모리에서 생성됩니다. 해당 도메인에 대한 메일이 모두 전달된 후 대상 개체는 3시간 더 유지됩니다. 3시간 후 해당 도메인에 대해 반송되는 새 메시지가 없으면 개체가 만료되어 대상이 더 이상 보고되지 않습니다(예: tophosts 명령으로). 한 도메인에만 메일을 전달하면 이 카운터는 "1"이 됩니다. 보내거나 받은 메시지가 없으면(몇 시간 동안 어플라이언스에서 처리한 메시지가 없으면) 카운터는 "0"이 됩니다. 가상 게이트웨이를 사용 중인 경우 각 가상 게이트웨이에 대한 대상 도메인은 별도의 대상 개체를 갖게 됩니다. (예를 들어 3개의 서로 다른 가상 게이트웨이에서 yahoo.com으로 전달하는 경우 yahoo.com은 3개의 대상 개체로 계산됩니다.)
사용된 킬로바이트	사용된 대기열 스토리지(킬로바이트 단위).
Kilobytes in Quarantine(격리의 킬로바이트)	격리된 메시지에 사용된 대기열 스토리지. 값은 메시지 크기와 수신자당 30바이트를 더해 계산되고, 위에 계산된 "Messages in Quarantine(격리에 있는 메시지)"에 합산됩니다. 일반적으로 이 계산은 사용된 공간을 과대평가합니다.
사용 가능한 킬로바이트	남은 대기열 스토리지(킬로바이트 단위).

전달된 메시지 및 반송된 메시지의 속도 읽기

모든 속도는 쿼리가 생성된 특정 시점에서 시간당 이벤트가 발생하는 평균 속도로 표시됩니다. 지난 1분, 5분, 그리고 15분 동안의 시간당 평균 속도, 이 세 개의 간격에 대해 속도가 계산됩니다.

예를 들어 Cisco 어플라이언스가 1분 동안 100개의 수신자 메시지를 받은 경우 1분에 대한 속도는 시간당 6,000이 됩니다. 같은 메시지가 5분 간격에 대한 속도라면 시간당 1,200이 되고, 15분 속도라면 시간당 400이 됩니다. 1분 동안의 속도가 계속될 경우 시간당 평균 속도는 어떨지를 나타내도록 계산됩니다. 따라서 1분마다 100개의 메시지를 받는다면 15분 동안 100개의 메시지를 받는 것보다 속도가 빨라집니다.

다음 표에서는 Cisco 어플라이언스를 모니터링할 때 사용 가능한 속도 및 해당 설명을 보여줍니다.

참고 여기에 나열된 것이 전체 목록입니다. 선택하는 표시 옵션 또는 명령에 따라 표시되는 속도가 다릅니다. 이 목록은 참조용으로 사용하십시오.

표 *98:* 비율

통계	설명
Messages Received(수신 메시지)	시간당 전달 대기열에 삽입되는 메시지 속도.
Recipients Received(수신된 수신자)	시간당 전달 대기열에 삽입되는 모든 메시지에 대한 수신자 수의 속도.
Soft Bounced Events(소프트 반송된 이벤트)	시간당 소프트 반송 이벤트 수의 속도. (여러 번 소프트 반송된 메시지는 소프트 반송 이벤트도 여러 번 계산됩니다.)
Completed Recipients(완료된 수신자)	하드 반송된 수신자, 전달된 수신자 및 삭제된 수신자 전체 합계의 속도. 전달 대기열에서 제거된 수신자는 완료된 것으로 간주됩니다.
Hard Bounced Recipients(하드 반송된 수신자)	시간당 DNS 하드 반송, 5XX 하드 반송, 필터 하드 반송, 만료된 하드 반송 및 기타 하드 반송 전체 합계의 속도. 수신자에게 메시지를 전달하려다 해당 전달이 즉시 종료된 실패한 시도는 하드 반송입니다.
Delivered Recipients(전달된 수신자)	시간당 수신자에게 성공적으로 전달된 메시지의 속도.

CLI를 사용한 모니터링

이메일 상태 모니터링

Cisco 어플라이언스에서 이메일 운영 상태를 모니터링할 수 있습니다. status 명령은 이메일 작업에 대한 모니터링된 정보의 하위 집합을 반환합니다. 반환된 통계는 두 가지 방식, 즉 카운터와 게이지 중 하나로 표시됩니다. 카운터는 시스템에서 발생하는 각종 이벤트의 누계를 제공합니다. 각 카운터에 대해 카운터 재설정 이후, 마지막 재부팅 이후, 그리고 시스템 수명 주기 전체에서 발생한 총 이벤트 수를 볼 수 있습니다. 게이지는 메모리, 디스크 공간, 활성 연결 등과 같은 시스템 리소스의 현재 사용률을 보여줍니다.

각 항목에 대한 설명은 CLI를 사용한 관리 및 모니터링 개요, 997 페이지 섹션을 참조하십시오.

표 ***99:*** 메일 상태

통계	설명
Status as of(날짜/시간)	현재 시스템의 시간과 날짜를 표시합니다.
Last counter reset(마지막 카운터 재설정)	카운터가 재설정된 마지막 시간을 표시합니다.
System status(시스템 상태)	Online(온라인), offline(오프라인), receiving suspended(수신 일시 중단) 또는 delivery suspended(전달 일시 중단). 모든 리스너가 일시 중단된 경우에만 "receiving suspended(수신 일시 중단)" 상태가 됩니다. 모든 리스너에 대해 수신 및 전달이 일시 중단된 경우 "offline(오프라인)" 상태가 됩니다.
Oldest Message(가장 오래된 메시지)	시스템 전달을 기다리는 가장 오래된 메시지를 표시합니다.
Features(기능)	featurekey 명령에 의해 시스템에 설치된 특수 기능을 표시합니다.

예

```
mail3.example.com> status

Status as of:               Thu Oct 21 14:33:27 2004 PDT
Up since:                     Wed Oct 20 15:47:58 2004 PDT (22h 45m 29s)
Last counter reset:         Never
System status:              Online
Oldest Message:              4 weeks 46 mins 53 secs
Counters:                     Reset          Uptime        Lifetime
  Receiving
    Messages Received       62,049,822          290,920      62,049,822
    Recipients Received     62,049,823          290,920      62,049,823
  Rejection
    Rejected Recipients      3,949,663           11,921       3,949,663
    Dropped Messages        11,606,037              219      11,606,037
  Queue
    Soft Bounced Events      2,334,552           13,598       2,334,552
  Completion
    Completed Recipients    50,441,741          332,625      50,441,741
```

```
  Current IDs
    Message ID (MID)                                    99524480
    Injection Conn. ID (ICID)                           51180368
    Delivery Conn. ID (DCID)                            17550674
Gauges:                                Current
  Connections
    Current Inbound Conn.                        0
    Current Outbound Conn.                      14
  Queue
    Active Recipients                        7,166
    Messages In Work Queue                       0
    Messages In Quarantine                  16,248
    Kilobytes Used                         387,143
      Kilobytes In Quarantine              338,206
    Kilobytes Free                      39,458,745
mail3.example.com>
```

자세한 이메일 상태 모니터링

status detail 명령은 이메일 운영에 대한 전체 모니터링 정보를 반환합니다. 반환된 범주는 카운터, 속도 및 게이지라는 세 범주에 표시됩니다. 카운터는 시스템에서 발생하는 각종 이벤트의 누계를 제공합니다. 각 카운터에 대해 카운터 재설정 이후, 마지막 재부팅 이후, 그리고 시스템 수명 주기 전체에서 발생한 총 이벤트 수를 볼 수 있습니다. 게이지는 메모리, 디스크 공간, 활성 연결 등과 같은 시스템 리소스의 현재 사용률을 보여줍니다. 모든 속도는 쿼리가 생성된 특정 시점에서 시간당 이벤트가 발생하는 평균 속도로 표시됩니다. 지난 1분, 5분, 그리고 15분 동안의 시간당 평균 속도, 이 세 개의 간격에 대해 속도가 계산됩니다. 각 항목에 대한 설명은 CLI를 사용한 관리 및 모니터링 개요, 997 페이지 섹션을 참조하십시오.

예

```
mail3.example.com> status detail
Status as of:           Thu Jun 30 13:09:18 2005 PDT
Up since:                Thu Jun 23 22:21:14 2005 PDT (6d 14h 48m 4s)
Last counter reset:             Tue Jun 29 19:30:42 2004 PDT
System status:                  Online
Oldest Message:                 No Messages
Feature - IronPort Anti-Spam:  17 days
Feature - Sophos:               Dormant/Perpetual
Feature - Outbreak Filters: Dormant/Perpetual
Feature - Central Mgmt:         Dormant/Perpetual
Counters:                        Reset          Uptime        Lifetime
  Receiving
    Messages Received       2,571,967          24,760       3,113,176
    Recipients Received     2,914,875          25,450       3,468,024
    Gen. Bounce Recipients      2,165               0           7,451
  Rejection
    Rejected Recipients     1,019,453             792       1,740,603
    Dropped Messages        1,209,001              66       1,209,028
  Queue
    Soft Bounced Events        11,236               0          11,405
  Completion
    Completed Recipients    2,591,740          49,095       3,145,002
      Hard Bounced Recipients   2,469               0           7,875
        DNS Hard Bounces          199               0           3,235
        5XX Hard Bounces        2,151               0           4,520
        Expired Hard Bounces      119               0             120
        Filter Hard Bounces         0               0               0
```

```
        Other Hard Bounces           0               0               0
      Delivered Recipients   2,589,270          49,095       3,137,126
      Deleted Recipients             1               0               1
        Global Unsub. Hits           0               0               0
    DomainKeys Signed Msgs          10               9              10
  Current IDs
    Message ID (MID)                                             7615199
    Injection Conn. ID (ICID)                                    3263654
    Delivery Conn. ID (DCID)                                     1988479
Rates (Events Per Hour):       1-Minute       5-Minutes      15-Minutes
  Receiving
    Messages Received             180             300             188
    Recipients Received           180             300             188
  Queue
    Soft Bounced Events             0               0               0
  Completion
    Completed Recipients          360             600             368
      Hard Bounced Recipients       0               0               0
      Delivered Recipients        360             600             368
Gauges:                                Current
  System
    RAM Utilization                          1%
    CPU Utilization
      MGA                                    0%
      AntiSpam                               0%
      AntiVirus                              0%
    Disk I/O Utilization                     0%
    Resource Conservation                    0
  Connections
    Current Inbound Conn.                    0
    Current Outbound Conn.                   0
  Queue
    Active Recipients                        0
      Unattempted Recipients                 0
      Attempted Recipients                   0
    Messages In Work Queue                   0
    Messages In Quarantine                  19
    Destinations In Memory                   3
    Kilobytes Used                         473
      Kilobytes In Quarantine              473
    Kilobytes Free                39,845,415
```

참고 가장 오래된 메시지 카운터가 메시지를 표시하지만, 실제로 카운터에 표시된 수신자가 없는 경우가 새로 설치된 어플라이언스에 존재할 수 있습니다. 원격 호스트가 연결 중이고 메시지 수신 속도가 매우 느린 경우(메시지 하나를 수신하는 데 몇 분 정도 소요) 수신자 수신 카운터는 "0"으로 표시되지만 가장 오래된 카운터는 "1"로 표시될 수 있습니다. 이는 가장 오래된 메시지 카운터가 진행 중인 메시지를 표시하기 때문입니다. 연결이 결국 삭제되면 카운터가 재설정됩니다.

메일 호스트의 상태 모니터링

특정 수신자 도메인에 전달 문제가 있는 것으로 의심되거나 가상 게이트웨이 주소에 대한 정보를 수집하려는 경우, hoststatus 명령을 실행하면 해당 정보가 표시됩니다. hoststatus 명령은 특정 수신자 호스트와 관련된 이메일 작업에 대한 모니터링 정보를 반환합니다. 반환할 호스트 정보의 도메인을 입력하라는 프롬프트가 표시됩니다. AsyncOS 캐시에 저장된 DNS 정보 및 수신자 호스트에서 반환된 마지막 오류도 제공됩니다. 반환된 데이터는 마지막 resetcounters 명령 이후 누적된 것입니다. 반환된

통계는 카운터와 게이지라는 두 범주에 표시됩니다. 각 항목에 대한 설명은 CLI를 사용한 관리 및 모니터링 개요, 997 페이지 섹션을 참조하십시오.

또한 hoststatus 명령을 실행하면 다음과 같은 다른 데이터가 반환됩니다.

표 ***100: hoststatus*** 명령의 추가 데이터

통계	설명
보류 중인 아웃바운드 연결	열려 있으며 작동하는 연결과 반대되는, 대상 메일 호스트에 대한 대기 중인 또는 "초기 상태의" 연결. Pending Outbound Connection(대기 중인 아웃바운드 연결)은 프로토콜 greeting 단계에 아직 도달하지 못한 연결입니다.
Oldest Message(가장 오래된 메시지)	이 도메인의 전달 대기열에 있는 가장 오래된 활성 수신자의 기간. 이 카운터는 대기열에 있으면서 소프트 반송 이벤트 및/또는 다운된 호스트 때문에 전달될 수 없는 메시지의 기간을 확인하는 데 유용합니다.
최근 활동	해당 호스트에 대한 메시지 전달이 시도될 때마다 이 필드가 업데이트됩니다.
정렬된 IP 주소	이 필드에는 IP 주소에 대한 TTL(time to live), MX 레코드에 따른 기본 설정 및 실제 주소가 포함되어 있습니다. MX 레코드는 도메인에 대한 메일 서버 IP 주소를 지정합니다. 한 도메인에 여러 MX 레코드가 있을 수 있습니다. 각 MX 레코드 메일 서버에 우선 순위가 할당됩니다. 우선 순위 번호가 가장 낮은 MX 레코드에 우순권이 제공됩니다.
Last 5XX error(마지막 5XX 오류)	이 필드에는 호스트에 의해 반환된 가장 최근 "5XX" 상태 모드 및 설명이 포함되어 있습니다. 5XX 오류가 있는 경우에만 이것이 표시됩니다.
MX 레코드	MX 레코드는 도메인에 대한 메일 서버 IP 주소를 지정합니다. 한 도메인에 여러 MX 레코드가 있을 수 있습니다. 각 MX 레코드 메일 서버에 우선 순위가 할당됩니다. 우선 순위 번호가 가장 낮은 MX 레코드에 우순권이 제공됩니다.
이 호스트의 SMTP 경로	이 도메인에 대해 SMTP 경로가 정의되면 여기에 나열됩니다.
Last TLS Error(마지막 TLS 오류)	이 필드에는 가장 최근 발신 TLS 연결 오류의 설명 및 어플라이언스가 설정하려고 시도한 TLS 연결 유형이 포함되어 있습니다. TLS 오류가 있는 경우에만 이것이 표시됩니다.

가상 게이트웨이

다음의 가상 게이트웨이 정보는 가상 게이트웨이 주소를 설정한 경우에만 표시됩니다(이메일을 수신하도록 게이트웨이 구성, 69 페이지 참고).

표 ***101: hoststatus*** 명령의 추가 가상 게이트웨이 데이터

통계	설명
호스트 up/down	같은 이름의 hoststatus 필드와 동일한 정의 - 가상 게이트웨이 주소 단위로 추적됨.
최근 활동	같은 이름의 hoststatus 필드와 동일한 정의 - 가상 게이트웨이 주소 단위로 추적됨.
Recipients(수신자)	이 필드는 전역 hoststatus 명령과 동일한 정의에도 해당됩니다. Active Recipients(활성 수신자) 필드 - 가상 게이트웨이 주소 단위로 추적됨.
Last 5XX error(마지막 5XX 오류)	이 필드에는 호스트에 의해 반환된 가장 최근 5XX 상태 모드 및 설명이 포함되어 있습니다. 5XX 오류가 있는 경우에만 이것이 표시됩니다.

예

```
mail3.example.com> hoststatus

Recipient host:
[]> aol.com
Host mail status for: 'aol.com'
Status as of:          Tue Mar 02 15:17:32 2010
Host up/down:         up
Counters:
  Queue
    Soft Bounced Events                       0
  Completion
    Completed Recipients                      1
      Hard Bounced Recipients                 1
        DNS Hard Bounces                      0
        5XX Hard Bounces                      1
        Filter Hard Bounces                   0
        Expired Hard Bounces                  0
        Other Hard Bounces                    0
      Delivered Recipients                    0
      Deleted Recipients                      0
Gauges:
  Queue
    Active Recipients                         0
      Unattempted Recipients                  0
      Attempted Recipients                    0
    Connections
      Current Outbound Connections            0
      Pending Outbound Connections            0
Oldest Message        No Messages
Last Activity         Tue Mar 02 15:17:32 2010
Ordered IP addresses: (expiring at Tue Mar 02 16:17:32 2010)
    Preference   IPs
    15           64.12.137.121    64.12.138.89     64.12.138.120
    15           64.12.137.89     64.12.138.152    152.163.224.122
    15           64.12.137.184    64.12.137.89     64.12.136.57
    15           64.12.138.57     64.12.136.153    205.188.156.122
    15           64.12.138.57     64.12.137.152    64.12.136.89
    15           64.12.138.89     205.188.156.154  64.12.138.152
```

```
    15          64.12.136.121    152.163.224.26   64.12.137.184
    15          64.12.138.120    64.12.137.152    64.12.137.121
MX Records:
    Preference  TTL        Hostname
    15          52m24s     mailin-01.mx.aol.com
    15          52m24s     mailin-02.mx.aol.com
    15          52m24s     mailin-03.mx.aol.com
    15          52m24s     mailin-04.mx.aol.com
    Last 5XX Error:
    ----------
    550 REQUESTED ACTION NOT TAKEN: DNS FAILURE
 (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10
    ----------
Last TLS Error:             Required - Verify
    ----------
    TLS required, STARTTLS unavailable
    (at Tue Mar 02 15:17:32 2010 GMT) IP: 10.10.10.10
Virtual gateway information:
============================================================
example.com (PublicNet_017):
    Host up/down:         up
    Last Activity         Wed June 22 13:47:02 2005
    Recipients            0
```

참고 altsrchost 기능을 사용 중인 경우에만 가상 게이트웨이 주소 정보가 표시됩니다.

이메일 대기열의 구성 확인

이메일 대기열에 대한 즉각적인 정보를 얻고 특정 수신자 호스트에 전달 문제(예: 대기열 빌드업)가 있는지를 확인하려면 tophosts 명령을 사용합니다. tophosts 명령은 대기열에 있는 상위 20 수신자 호스트 목록을 반환합니다. 활성 수신자, 연결 발신, 전달된 수신자, 소프트 반송된 이벤트, 하드 반송된 수신자 등 여러 통계를 기준으로 목록을 정렬할 수 있습니다. 각 항목에 대한 설명은 CLI를 사용한 관리 및 모니터링 개요, 997 페이지 섹션을 참조하십시오.

예

```
mail3.example.com> tophosts

Sort results by:
1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Soft Bounced Events
5. Hard Bounced Recipients
[1]> 1
Status as of:         Mon Nov 18 22:22:23 2003
                    Active    Conn.    Deliv.    Soft      Hard
#  Recipient Host   Recip     Out      Recip.    Bounced   Bounced
1  aol.com          365       10       255       21         8
2  hotmail.com      290        7       198       28        13
3  yahoo.com        134        6       123       11        19
4  excite.com        98        3        84        9         4
5  msn.com           84        2        76       33        29
mail3.example.com>
```

실시간 활동 표시

Cisco 어플라이언스는 실시간 모니터링을 제공하며, 이를 통해 시스템에서 이루어지는 이메일 활동의 진행 상황을 볼 수 있습니다. rate 명령은 이메일 작업에 대한 실시간 모니터링 정보를 반환합니다. 이 정보는 사용자가 지정한 주기적인 간격으로 업데이트됩니다. Ctrl-C를 누르면 **rate** 명령을 중지할 수 있습니다.

다음 필드가 테이블에 표시됩니다.

표 ***102: rate*** 명령의 데이터

통계	설명
Connections In(연결 수신)	인바운드 연결의 수
Connections Out(연결 발신)	아웃바운드 연결의 수
Recipients Received(수신된 수신인)	시스템에서 수신된 총 수신자 수
Recipients Completed(완료된 수신자)	완료된 총 수신자 수
델타	마지막 데이터 업데이트 이후 수신된/완료된 수신자의 차이 변경
Queue Used(사용된 대기열)	메시지 대기열의 크기(킬로바이트 단위)

예

```
mail3.example.com> rate

Enter the number of seconds between displays.
[10]> 1
Hit Ctrl-C to return to the main prompt.
Time     Connections Recipients          Recipients               Queue
             In    Out   Received    Delta  Completed    Delta     K-Used
23:37:13    10      2   41708833        0   40842686        0         64
23:37:14     8      2   41708841        8   40842692        6        105
23:37:15     9      2   41708848        7   40842700        8         76
23:37:16     7      3   41708852        4   40842705        5         64
23:37:17     5      3   41708858        6   40842711        6         64
23:37:18     9      3   41708871       13   40842722       11         67
23:37:19     7      3   41708881       10   40842734       12         64
23:37:21    11      3   41708893       12   40842744       10         79
^C
```

hostrate 명령은 특정 메일 호스트에 대한 실시간 모니터링 정보를 반환합니다. 이 정보는 status detail 명령의 하위 집합입니다. (자세한 이메일 상태 모니터링, 1005 페이지 참조.)

표 ***103: hostrate*** 명령의 데이터

통계	설명
Host Status(호스트 상태)	특정 호스트의 현재 상태: up(가동), down(다운) 또는 unknown(알 수 없음)
Current Connections Out(현재 연결 발신)	호스트에 대한 현재 아웃바운드 연결 수
Active Recipients in Queue(큐에 있는 활성 수신자)	대기열에 있는 특정 호스트에 대한 총 활성 수신자 수
Active Recipients in Queue Delta(대기열의 활성 수신자 델타)	마지막 알려진 호스트 상태 이후 대기열에 있는 특정 호스트에 대한 총 활성 수신자 수의 차이
Delivered Recipients Delta(전달된 수신자 델타)	마지막 알려진 호스트 상태 이후 대기열에 있는 특정 호스트에 대한 전달된 총 수신자 수의 차이
Hard Bounced Recipients Delta(하드 반송된 수신자 델타)	마지막 알려진 호스트 상태 이후 대기열에 있는 특정 호스트에 대한 하드 반송된 총 수신자 수의 차이
Soft Bounce Events Delta(소프트 반송 이벤트 델타)	마지막 알려진 호스트 상태 이후 대기열에 있는 특정 호스트에 대한 소프트 반송된 총 수신자 수의 차이

Ctrl-C를 누르면 hostrate 명령을 중지할 수 있습니다.

예

```
mail3.example.com> hostrate
Recipient host:
[]> aol.com
Enter the number of seconds between displays.
[10]> 1
    Time   Host  CrtCncOut  ActvRcp ActvRcp  DlvRcp HrdBncRcp SftBncEvt
           Status                    Delta   Delta     Delta     Delta
23:38:23       up          1         0       0       4         0         0
23:38:24       up          1         0       0       4         0         0
23:38:25       up          1         0       0      12         0         0
^C
```

인바운드 이메일 연결 모니터링

대용량 발신자를 식별하거나 시스템에 대한 인바운드 연결의 문제를 해결하려면 Cisco 어플라이언스에 연결한 호스트를 모니터링할 수 있습니다. topin 명령은 시스템에 연결된 원격 호스트의 스냅샷을 제공하며, 특정 리스너에 연결된 각 원격 IP 주소에 대한 한 행이 있는 테이블을 표시합니다. 동일한 IP 주소에서 서로 다른 리스너로 가는 두 개의 연결이 있으면 다음 테이블에 행이 2개 나타납니다. 이 테이블은 topin 명령을 사용할 때 표시되는 필드를 설명합니다.

표 ***104: topin*** 명령의 데이터

통계	설명
Remote Hostname(원격 호스트 이름)	역방향 DNS 조회에서 파생된 원격 호스트의 호스트 이름.
원격 IP 주소	원격 호스트의 IP 주소.
리스너	연결을 수신 중인 Cisco 어플라이언스에 있는 리스너의 별칭입니다.
Connections In(연결 수신)	명령이 실행될 때 열린 지정된 IP 주소가 있는 원격 호스트에서의 동시 연결 수.

시스템은 원격 호스트 이름을 찾기 위해 역방향 DNS 조회를 수행한 다음, 이름을 검증하기 위해 정방향 DNS 조회를 수행합니다. 정방향 조회 결과 원래 IP 주소가 나타나지 않거나 역방향 DNS 조회가 실패하면 테이블의 호스트 이름 열에 IP 주소가 나타납니다. 발신자 확인 처리에 대한 자세한 내용은 발신자 확인, 119 페이지 섹션을 참조하십시오.

예

```
mail3.example.com> topin

Status as of:                  Sat Aug 23 21:50:54 2003
#  Remote hostname             Remote IP addr.   listener        Conn. In
1  mail.remotedomain01.com     172.16.0.2        Incoming01            10
2  mail.remotedomain01.com     172.16.0.2        Incoming02            10
3  mail.remotedomain03.com     172.16.0.4        Incoming01             5
4  mail.remotedomain04.com     172.16.0.5        Incoming02             4
5  mail.remotedomain05.com     172.16.0.6        Incoming01             3
6  mail.remotedomain06.com     172.16.0.7        Incoming02             3
7  mail.remotedomain07.com     172.16.0.8        Incoming01             3
8  mail.remotedomain08.com     172.16.0.9        Incoming01             3
9  mail.remotedomain09.com     172.16.0.10       Incoming01             3
10 mail.remotedomain10.com     172.16.0.11       Incoming01             2
11 mail.remotedomain11.com     172.16.0.12       Incoming01             2
12 mail.remotedomain12.com     172.16.0.13       Incoming02             2
13 mail.remotedomain13.com     172.16.0.14       Incoming01             2
14 mail.remotedomain14.com     172.16.0.15       Incoming01             2
15 mail.remotedomain15.com     172.16.0.16       Incoming01             2
16 mail.remotedomain16.com     172.16.0.17       Incoming01             2
17 mail.remotedomain17.com     172.16.0.18       Incoming01             1
18 mail.remotedomain18.com     172.16.0.19       Incoming02             1
19 mail.remotedomain19.com     172.16.0.20       Incoming01             1
20 mail.remotedomain20.com     172.16.0.21       Incoming01             1
```

DNS 상태 확인

dnsstatus 명령은 DNS 조회 및 캐시 정보의 통계를 표시하는 카운터를 반환합니다. 각 카운터에 대해 카운터 마지막 재설정 이후, 마지막 시스템 재부팅 이후, 그리고 시스템 수명 주기 전체에서 발생한 총 이벤트 수를 볼 수 있습니다.

다음 표에는 사용 가능한 카운터의 목록이 나와 있습니다.

표 ***105: dnsstatus*** 명령의 데이터

통계	설명
DNS 요청	도메인 이름 확인을 위해 시스템 DNS 캐시에 대한 상위 레벨의 비재귀적 요청.
네트워크 요청	DNS 정보 검색을 위해 네트워크(로컬 아님)에 요청.
캐시 성공률	레코드가 발견되고 반환되는 DNS 캐시에 대한 요청.
캐시 실패	레코드가 발견되지 않은 DNS 캐시에 대한 요청.
캐시 예외 사항	레코드가 발견되었지만 도메인을 알 수 없는 DNS 캐시에 대한 요청.
캐시 만료	레코드가 캐시에서 발견되고, 사용이 고려되고, 너무 오래돼서 취소된 DNS 캐시에 대한 요청. TTL(time to live)이 지났더라도 많은 항목이 캐시에 존재할 수 있습니다. 이러한 항목은 사용되지 않는 한 만료 카운터에 포함되지 않습니다. 캐시가 플러시되면 유효한 항목과 유효하지 않은(너무 오래된) 항목이 모두 삭제됩니다. 플러시 작업은 만료 카운터를 변경하지 않습니다.

예

```
mail3.example.com> dnsstatus
Status as of: Sat Aug 23 21:57:28 2003
Counters:                    Reset          Uptime        Lifetime
  DNS Requests         211,735,710       8,269,306     252,177,342
  Network Requests     182,026,818       6,858,332     206,963,542
  Cache Hits           474,675,247      17,934,227     541,605,545
  Cache Misses         624,023,089      24,072,819     704,767,877
  Cache Exceptions      35,246,211       1,568,005      51,445,744
  Cache Expired            418,369           7,800         429,015
mail3.example.com>
```

이메일 모니터링 카운터 재설정

resetcounters 명령은 누적된 이메일 모니터링 카운터를 재설정합니다. 재설정은 호스트 단위 카운터는 물론 전역 카운터에도 영향을 미칩니다. 재시도 예약과 관련된 전달 대기열에 있는 메시지에 대한 카운터에는 재설정이 영향을 미치지 않습니다.

참고 GUI에서도 카운터를 재설정할 수 있습니다. System Status(시스템 상태) 페이지, 826 페이지를 참조하십시오.

예

```
mail3.example.com> resetcounters
Counters reset: Mon Jan 01 12:00:01 2003
```

활성 TCP/IP 서비스 식별

Email Security Appliance에서 사용되는 활성 TCP/IP 서비스를 식별하려면 CLI에서 tcpservices 명령을 사용합니다.

이메일 대기열 관리

Cisco AsyncOS에서는 이메일 대기열에 있는 메시지에 대해 작업을 수행할 수 있습니다. 이메일 대기열에서 메시지를 삭제, 반송, 일시 중단 또는 리디렉션할 수 있습니다. 또한 대기열에 있는 오래된 메시지를 찾고 제거하고 보관할 수 있습니다.

대기열의 수신자 삭제

특정 수신자가 전달되지 않는 경우 또는 이메일 대기열에서 지우려는 경우 deleterecipients 명령을 사용합니다. deleterecipients 명령을 사용하면 전달을 기다리는 특정 수신자를 삭제하여 이메일 전달 대기열을 관리할 수 있습니다. 삭제할 수신자는 수신자의 목적지인 수신자 호스트에 의해 또는 메시지 봉투의 Envelope From 줄에 있는 특정 주소로 식별된 메시지 발신자에 의해 식별됩니다. 또는 전달 대기열에 있는 모든 메시지(모든 활성 수신자)를 동시에 삭제할 수 있습니다.

참고 deleterecipients 기능을 수행하려면 Cisco 어플라이언스를 오프라인 상태로 전환하거나 전달을 일시 중단하는 것이 좋습니다(이메일 수신 및 전달 일시 중단 , 924 페이지 참고).

참고 이 기능은 모든 상태에서 지원되지만, 특정 메시지는 기능이 수행되는 동안에만 전달할 수 있습니다.

수신자 호스트 및 발신자가 일치하려면 문자열이 동일해야 합니다. 와일드카드는 허용되지 않습니다. deleterecipients 명령은 삭제된 총 메시지 수를 반환합니다. 또한 메일 로그 서브스크립션(IronPort 텍스트 형식만)이 구성된 경우 메시지 삭제는 별도의 줄에 기록됩니다.

예

```
mail3.example.com> deleterecipients
Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>
```

Cisco 어플라이언스는 필요에 따라 수신자를 삭제할 수 있도록 다양한 옵션을 제공합니다. 다음 예는 수신자 호스트별 수신자 삭제, Envelope From 주소별 수신자 삭제 및 대기열에 있는 모든 수신자 삭제를 보여줍니다.

수신자 도메인별 삭제

```
Please enter the hostname for the messages you wish to delete.
[]> example.com
Are you sure you want to delete all messages being delivered to "example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.
```

Envelope From 주소별 삭제

```
Please enter the Envelope From address for the messages you wish to delete.
[]> mailadmin@example.com
Are you sure you want to delete all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.
```

모두 삭제

```
Are you sure you want to delete all messages in the delivery queue (all active recipients)?
 [N]> Y
Deleting messages, please wait.
1000 messages deleted.
```

대기열의 수신자 반송

deleterecipients 명령과 마찬가지로 bouncerecipients 명령을 사용해도 전달을 기다리는 특정 수신자를 하드 반송하여 이메일 전달 대기열을 관리할 수 있습니다. 메시지 반송은 bounceconfig 명령에서 지정한 일반 반송 메시지 컨피그레이션을 따릅니다.

참고 bouncerecipients 기능을 수행하려면 Cisco 어플라이언스를 오프라인 상태로 전환하거나 전달을 일시 중단하는 것이 좋습니다(이메일 수신 및 전달 일시 중단 , 924 페이지 참고).

참고 이 기능은 모든 상태에서 지원되지만, 특정 메시지는 기능이 수행되는 동안에만 전달할 수 있습니다.

수신자 호스트 및 발신자가 일치하려면 문자열이 동일해야 합니다. 와일드카드는 허용되지 않습니다. bouncerecipients 명령은 반송된 총 메시지 수를 반환합니다.

참고 bouncerecipients 기능은 리소스를 많이 사용하며 완료하는 데 몇 분 정도 걸릴 수 있습니다. 오프라인 또는 전달 일시 중단 상태에서 반송 메시지(하드 반송 생성이 켜진 경우)의 실제 전송은, resume 명령을 사용하여 Cisco AsyncOS를 다시 온라인 상태로 전환한 후에야 시작됩니다.

예

```
mail3.example.com> bouncerecipients
Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>
```

바운스할 수신자는 목적지 수신자 호스트 또는 메시지 발신자로 식별합니다. 후자의 경우 메시지 엔벨로프의 Envelope From 라인에 지정된 주소로 식별됩니다. 또는 전달 대기열에 있는 모든 메시지를 동시에 삭제할 수 있습니다.

수신자 호스트별 반송

```
Please enter the hostname for the messages you wish to bounce.
[]> example.com
Are you sure you want to bounce all messages being delivered to "example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

Envelope From 주소별 반송

```
Please enter the Envelope From address for the messages you wish to bounce.
[]> mailadmin@example.com
Are you sure you want to bounce all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

모두 반송

```
Are you sure you want to bounce all messages in the queue? [N]> Y
Bouncing messages, please wait.
1000 messages bounced.
```

대기열의 메시지 리디렉션

redirectrecipients 명령을 사용하면 이메일 전달 대기열에 있는 모든 메시지를 다른 릴레이 호스트로 리디렉션할 수 있습니다. 대용량 SMTP 메일을 수락할 준비가 되지 않은 호스트 또는 IP 주소로 수신자를 리디렉션하면 메시지가 반송되고 메일이 손실될 수도 있습니다.

주의 대상으로 /dev/null을 가지고 있는 수신 도메인으로 메시지를 리디렉션하면 메시지가 손실됩니다. 그런 도메인으로 메일을 리디렉션하면 CLI에서 경고를 표시하지 않습니다. 메시지를 리디렉션하기 전에 수신 도메인에 대한 SMTP 경로를 확인하십시오.

예

다음 예는 모든 메일을 example2.com 호스트로 리디렉션합니다.

```
mail3.example.com> redirectrecipients
Please enter the hostname or IP address of the machine you want to send all mail to.
[]> example2.com
WARNING: redirecting recipients to a host or IP address that is not prepared to accept large
 volumes of SMTP mail from this host will cause messages to bounce and possibly result in
the loss of mail.
Are you sure you want to redirect all mail in the queue to "example2.com"? [N]> y
Redirecting messages, please wait.
246 recipients redirected.
```

대기열의 수신자를 기반으로 메시지 표시

수신자 호스트 또는 Envelope From 주소별로 이메일 전달 대기열의 메시지를 표시하려면 showrecipients 명령을 사용합니다. 대기열의 모든 메시지를 표시할 수도 있습니다.

예

```
mail3.example.com> showrecipients
Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 3
Showing messages, please wait.
MID/     Bytes/    Sender/                 Subject
[RID]    [Atmps]   Recipient
1527     1230      user123456@ironport.com Testing
[0]      [0]       9554@example.com
1522     1230      user123456@ironport.com Testing
[0]      [0]       3059@example.com
1529     1230      user123456@ironport.com Testing
[0]      [0]       7284@example.com
1530     1230      user123456@ironport.com Testing
[0]      [0]       8243@example.com
1532     1230      user123456@ironport.com Testing
[0]      [0]       1820@example.com
1531     1230      user123456@ironport.com Testing
[0]      [0]       9595@example.com
1518     1230      user123456@ironport.com Testing
[0]      [0]       8778@example.com
1535     1230      user123456@ironport.com Testing
[0]      [0]       1703@example.com
1533     1230      user123456@ironport.com Testing
[0]      [0]       3052@example.com
```

```
1536     1230      user123456@ironport.com Testing
[0]      [0]       511@example.com
```

다음 예는 모든 수신자 호스트에 대한 대기열의 메시지를 표시합니다.

이메일 전달 일시 중단

유지 관리 또는 문제 해결을 위해 이메일 전달을 일시적으로 중단하려면 suspenddel 명령을 사용합니다. suspenddel 명령을 사용하면 Cisco AsyncOS는 전달 일시 중단 상태로 전환됩니다. 이 상태의 특성은 다음과 같습니다.

- 아웃바운드 이메일 전달이 중지됨
- 인바운드 이메일 연결이 수락됨
- 로그 전송이 계속됨
- CLI에는 계속 액세스할 수 있음

suspenddel 명령을 사용하면 열린 아웃바운드 연결을 닫을 수 있으며, 이렇게 하면 새 연결 열기가 중지됩니다. suspenddel 명령은 즉시 시작되며, 설정된 연결을 성공적으로 닫을 수 있습니다. 전달 일시 중단 상태에서 정상적인 작동으로 돌아가려면 resumedel 명령을 사용합니다.

참고 "전달 일시 중단" 상태는 시스템 재부팅 시 유지됩니다. suspenddel 명령을 사용한 다음 어플라이언스를 재부팅하는 경우, resumedel 명령을 사용하여 재부팅한 후 전달을 다시 시작해야 합니다.

예

```
mail3.example.com> suspenddel
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

이메일 전달 다시 시작

suspenddel 명령 사용 후 resumedel 명령을 사용하면 Cisco AsyncOS가 정상적인 운영 상태로 돌아갑니다.

구문

resumedel

```
mail3.example.com> resumedel
Mail delivery resumed.
```

이메일 수신 일시 중단

모든 리스너에서 이메일 수신을 일시적으로 중단하려면 suspendlistener 명령을 사용합니다. 수신이 일시 중단되면 시스템은 리스너의 특정 포트에 대한 연결을 수락하지 않습니다.

AsyncOS의 이번 릴리스에서 이 동작이 변경되었습니다. 이전 릴리스에서는 시스템이 연결을 수락하고 다음과 같이 반응한 후 연결을 끊었습니다.

- SMTP: 421 *hostname* Service not available, closing transaction channel
- QMQP: ZService not available

참고 "수신 일시 중단" 상태는 시스템 재부팅 시 유지됩니다. suspendlistener 명령을 사용한 후 어플라이언스를 재부팅하는 경우, 리스너가 메시지 수신을 다시 시작하기 전에 resumelistener 명령을 사용해야 합니다.

Syntax

```
suspendlistener mail3.example.com> suspendlistener
Choose the listener(s) you wish to suspend.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for listeners to exit...
Receiving suspended.
mail3.example.com>
```

이메일 수신 다시 시작

suspendlistener 명령 사용 후 resumelistener 명령을 사용하면 Cisco AsyncOS가 정상적인 운영 상태로 돌아갑니다.

Syntax

```
resumelistener


mail3.example.com> resumelistener
Choose the listener(s) you wish to resume.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1
Receiving resumed.
mail3.example.com>
```

이메일의 전달 및 수신 다시 시작

resume 명령은 전달 및 수신을 모두 다시 시작합니다.

Syntax

```
resume
```

```
mail3.example.com> resume
Receiving resumed.
Mail delivery resumed.
mail3.example.com>
```

즉시 전달하도록 이메일 예약

나중에 전달하도록 예약된 수신자 및 호스트는 delivernow 명령을 사용하여 즉시 재시도할 수 있습니다. delivernow 명령을 사용하면 대기열에 있는 이메일을 즉시 전달하도록 다시 예약할 수 있습니다. Down(다운) 상태로 표시된 모든 도메인과 예약된 메시지 또는 소프트 반송된 메시지가 즉시 전달을 위해 대기열에 추가됩니다.

대기열의 모든 수신자 또는 특정 수신자(예약됨 및 활성)에 대해 delivernow 명령을 호출할 수 있습니다. 특정 수신자를 선택할 때 즉시 전달을 위해 예약하려면 수신자의 도메인 이름을 입력해야 합니다. 시스템은 전체 문자열에서 문자와 길이를 확인합니다.

Syntax

```
delivernow
```

```
mail3.example.com> delivernow
Please choose an option for scheduling immediate delivery.
1. By recipient host
2. All messages
[1]> 1
Please enter the domain to schedule for immediate delivery.
[]> recipient.example.com
Rescheduling all messages to recipient.example.com for immediate delivery.
mail3.example.com>
```

작업 대기열 일시 중지

LDAP 수신자 액세스, 가장, LDAP 재라우팅, 메시지 필터, 안티스팸 및 안티바이러스 검사 엔진에 대한 처리는 모두 "작업 대기열"에서 수행됩니다. 처리 플로우는 라우팅 및 전달 기능 구성, 665 페이지를 참조하십시오. "작업 대기열의 메시지" 게이지의 설명은 시스템 게이지 읽기, 1000 페이지를 참조하십시오. workqueue 명령을 사용하면 메시지 처리의 작업 대기열 부분을 수동으로 일시 중지할 수 있습니다.

예를 들어 작업 대기열에 많은 메시지가 있는 동안 LDAP 서버 컨피그레이션을 변경하고자 한다고 가정해보겠습니다. LDAP 수신자 액세스 쿼리를 기반으로 메시지의 반송에서 삭제로 전환하고자 할 수 있습니다. 또는 최신 안티바이러스 검사 엔진 정의 파일을 수동으로 검사하는 동안(antivirusupdate

명령을 통해) 대기열을 일시 중지하고자 할 수 있습니다. workqueue 명령을 사용하면 다른 컨피그레이션 변경을 수행하는 동안 작업 대기열을 일시 중지 및 다시 시작할 수 있습니다.

작업 대기열을 일시 중지 및 다시 시작하면 이벤트가 기록됩니다. 예를 들면

```
Sun Aug 17 20:01:36 2003 Info: work queue paused, 1900 msgs S
Sun Aug 17 20:01:39 2003 Info: work queue resumed, 1900 msgs
```

다음 예에서는 작업 대기열이 일시 중지됩니다.

```
mail3.example.com> workqueue
Status as of:  Sun Aug 17 20:02:30 2003 GMT
Status:   Operational
Messages: 1243
Choose the operation you want to perform:
- STATUS - Display work queue status
- PAUSE - Pause the work queue
- RATE - Display work queue statistics over time
[]> pause
Manually pause work queue?  This will only affect unprocessed messages.  [N]> y
Reason for pausing work queue:
[]> checking LDAP server
Status as of:  Sun Aug 17 20:04:21 2003 GMT
Status:   Paused by admin: checking LDAP server
Messages: 1243
```

참고 이유를 입력하는 것은 선택 사항입니다. 이유를 입력하지 않으면 시스템에서는 "Manually paused by user(사용자가 수동으로 일시 중단)"라고 기록합니다.

이 예에서는 작업 대기열이 다시 시작됩니다.

```
mail3.example.com> workqueue
Status as of:  Sun Aug 17 20:42:10 2003 GMT
Status:   Paused by admin: checking LDAP server
Messages: 1243
Choose the operation you want to perform:
- STATUS - Display work queue status
- RESUME - Resume the work queue
- RATE - Display work queue statistics over time
[]> resume
Status:   Operational
Messages: 1243
```

오래된 메시지 찾기 및 보관

전달할 수 없기 때문에 오래된 메시지가 대기열에 남아 있는 경우가 더러 있습니다. 이러한 메시지를 제거 및 보관할 수 있습니다. 이렇게 하려면 showmessage CLI 명령을 사용하여 지정된 메시지 ID의 메시지를 표시합니다. 시스템에 있는 가장 오래된 비격리 메시지를 표시하려면 oldmessage CLI 명령을 사용합니다. 그런 다음 선택적으로 removemessage를 사용하여 지정된 메시지 ID의 메시지를 안전하게 제거할 수 있습니다. 작업 대기열, 재시도 대기열 또는 대상 대기열에 있는 메시지만 제거됩니다. 이러한 대기열 이외의 대기열에 있는 메시지는 제거되지 않습니다.

또한 archivemessage[mid] CLI 명령을 사용하여 지정된 메시지 ID의 메시지를 configuration 디렉터리의 mbox 파일에 보관할 수 있습니다.

oldmessage 명령을 사용하여 격리에 있는 메시지의 메시지 ID를 가져올 수는 없습니다. 그러나 메시지 ID를 알고 있는 경우 지정된 메시지를 표시하거나 보관할 수 있습니다. 작업 대기열, 재시도 대기열 또는 대상 대기열에 있지 않은 메시지는 removemessage 명령을 사용하여 제거할 수 없습니다.

참고 Cisco 스팸 격리에 있는 메시지에 대해서는 이러한 대기열 관리 명령을 수행할 수 없습니다.

Syntax

```
archivemessage
```

```
example.com> archivemessage
Enter the MID to archive and remove.
[0]> 47
 MID 47 has been saved in file oldmessage_47.mbox in the configuration directory
example.com>
```

Syntax

```
oldmessage
```

```
example.com> oldmessage
MID 9: 1 hour 5 mins 35 secs old
Received: from example.com ([172.16.0.102])
  by example.com with SMTP; 14 Feb 2007 22:11:37 -0800
From: user123@example.com
To: 4031@test.example2.com
Subject: Testing
Message-Id: <20070215061136.68297.16346@example.com>
```

시스템 내에서 메시지 추적

findevent CLI 명령은 온박스 메일 로그 파일을 사용하여 시스템 내 메시지를 추적하는 프로세스를 간소화합니다. findevent CLI 명령을 사용하면 제목 헤더, 봉투 발신자 또는 봉투 수신자에 대해 메시지 ID 또는 정규식 일치를 검색하는 방식으로 메일 로그에서 특정 메시지를 검색할 수 있습니다. 현재 로그 파일 또는 모든 로그 파일의 결과를 표시하거나 날짜별로 로그 파일을 표시할 수 있습니다. 날짜별로 로그 파일을 보려면 특정 날짜 또는 날짜 범위를 지정할 수 있습니다.

로그를 볼 메시지를 식별한 후 findevent 명령을 사용하여 분리 정보를 비롯한 해당 메시지 ID의 로그 정보를 표시합니다(분리 로그 메시지, 반송 및 시스템 생성 메시지). 다음 예는 제목 헤더에 "confidential"이 있는 메시지의 수신 및 전달을 추적하는 findevent CLI 명령을 보여줍니다.

```
example.com>
findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
```

```
3. Search by Subject
4. Search by envelope TO
[1]> 3
Enter the regular expression to search for.
[]> confidential
Currently configured logs:
1. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to use for message tracking.
[]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 3
The following matching message IDs were found. Please choose one to
show additional log information:
1. MID 4 (Tue Jul 31 17:37:35 2007) sales: confidential
[1]> 1
Tue Jul 31 17:37:32 2007 Info: New SMTP ICID 2 interface Data 1 (172.19.1.86) address
10.251.20.180 reverse dns host unknown verified no
Tue Jul 31 17:37:32 2007 Info: ICID 2 ACCEPT SG None match ALL SBRS None
Tue Jul 31 17:37:35 2007 Info: Start MID 4 ICID 2
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 From: <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 ICID 2 RID 0 To: <ljohnson@example02.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 Subject 'sales: confidential'
Tue Jul 31 17:37:35 2007 Info: MID 4 ready 4086 bytes from <user@example.com>
Tue Jul 31 17:37:35 2007 Info: MID 4 matched all recipients for per-recipient policy DEFAULT
 in the inbound table
Tue Jul 31 17:37:35 2007 Info: ICID 2 close
Tue Jul 31 17:37:37 2007 Info: MID 4 interim verdict using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 using engine: CASE spam negative
Tue Jul 31 17:37:37 2007 Info: MID 4 interim AV verdict using Sophos CLEAN
Tue Jul 31 17:37:37 2007 Info: MID 4 antivirus negative
Tue Jul 31 17:37:37 2007 Info: MID 4 queued for delivery
Tue Jul 31 17:37:37 2007 Info: Delivery start DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: Message done DCID 0 MID 4 to RID [0]
Tue Jul 31 17:37:37 2007 Info: MID 4 RID [0] Response '/null'
Tue Jul 31 17:37:37 2007 Info: Message finished MID 4 done
```

SNMP를 사용하여 시스템 상태 모니터링

AsyncOS 운영 체제는 SNMP(Simple Network Management Protocol)를 통한 시스템 상태 모니터링을 지원합니다. 이 릴리스는 RFC 1213 및 1907에 정의된 대로 MIB-II의 읽기 전용 하위 집합을 구현합니다. (SNMP에 대한 자세한 내용은 RFCs 1065, 1066 및 1067을 참조하십시오.) 참고:

- SNMP는 기본적으로 **off**입니다.
- SNMP SET 작업(컨피그레이션)은 구현되지 않습니다.
- AsyncOS는 SNMPv1, v2 및 v3을 지원합니다.
- 메시지 인증 및 암호화는 SNMPv3 활성화 시 필수 사항입니다. 인증과 암호화를 위한 암호는 서로 달라야 합니다. 암호화 알고리즘은 AES(권장) 또는 DES일 수 있습니다. 인증 알고리즘은 SHA-1(권장) 또는 MD5일 수 있습니다. snmpconfig 명령은 다음에 실행할 때 암호를 "기억"합니다.
- SNMPv3 사용자 이름: v3get

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a SHA -A ironport mail.example.com
```

- SNMPv1 또는 SNMPv2만 사용하는 경우 커뮤니티 문자열을 설정해야 합니다. 커뮤니티 문자열은 기본값이 public이 아닙니다.
- SNMPv1 및 SNMPv2에 대해 SNMP GET 요청을 수락할 네트워크를 지정해야 합니다.
- 트랩을 사용하려면 SNMP 관리자(AsyncOS에 포함되지 않음)를 실행하고 트랩 대상으로 해당 IP 주소를 입력해야 합니다. (호스트 이름을 사용할 수 있지만, 그럴 경우 DNS가 작동하는 경우에만 트랩이 작동합니다.)

어플라이언스에 대한 SNMP 모니터링을 활성화하고 구성하려면 snmpconfig명령을 사용합니다. 인터페이스에 대한 값의 선택 및 구성이 완료되면 어플라이언스는 SNMPv3 GET 요청에 응답합니다. 이러한 버전 3 요청에는 일치하는 암호가 포함되어야 합니다. 기본적으로 버전 1 및 2 요청은 거부됩니다. 활성화된 경우 버전 1 및 2 요청에 일치하는 커뮤니티 문자열을 포함해야 합니다.

MIB 파일

다음 Cisco Email Security Appliance용 MIB 파일은 http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html 에서 다운로드할 수 있습니다. 사용 가능한 최신 MIB 파일을 사용합니다.

- ASYNCOS-MAIL-MIB.txt - Cisco 어플라이언스에 대한 엔터프라이즈 MIB의 SNMPv2 호환성 설명입니다.
- AsyncOS-SMI.txt (IRONPORT-SMI.txt) - Cisco 콘텐츠 보안 제품에서 ASYNCOS-MAIL-MIB의 역할을 정의하는 "SMI(Structure of Management Information)" 파일.

하드웨어 개체

IPMI(Intelligent Platform Management Interface) 사양을 준수하는 하드웨어 센서는 온도, 팬 속도 및 전원 공급 장치 상태와 같은 정보를 보고합니다.

하드웨어 상태에 대해 폴링하고 문제가 심각해지기 전에 가능한 하드웨어 장애를 식별하는 것이 좋습니다. 심각한 상태 값의 10퍼센트 이내로 온도가 변경되면 주의해야 할 수 있습니다.

전원 공급 장치 수 및 어플라이언스의 작동 온도 범위와 같은 정보는 모델의 하드웨어 가이드를 참고하십시오. 하드웨어 가이드의 위치는 설명서 , 6 페이지 항목을 참고하십시오.

하드웨어 트랩

상태가 변경되면 상태 변경 트랩이 전송됩니다. 팬 장애 및 고온 트랩은 5초마다 전송됩니다. 기타 트랩은 장애 조건 경보 트랩입니다. 이들은 상태가 변경되면 전송됩니다(정상에서 장애로).

예를 들어 C170 어플라이언스에서는 다음 임계값에 도달할 경우 트랩이 전송됩니다.

표 ***106: C170*** 어플라이언스의 하드웨어 트랩*:* 온도 및 하드웨어 조건

모델	고온(CPU)	고온(주변)	고온(백플레인)	고온(라이저)	팬 장애	전력 공급 장치	RAID	링크
C170	90C	47C	해당 없음	해당 없음	0 RPMs	상태 변경	상태 변경	상태 변경

어플라이언스에서 사용 가능한 트랩 및 임계값을 보려면 명령줄 인터페이스에서 snmpconfig 명령을 실행합니다.

장애 조건 경보 트랩은 개별 구성 요소의 심각한 장애를 나타내지만, 총체적인 시스템 장애를 일으키지는 않을 수 있습니다. 예를 들어 팬 또는 전원 공급 장치가 여러 개인 경우 단일 팬 또는 전원 공급 장치에 장애가 발생해도 어플라이언스는 계속 작동합니다.

관련 주제

• 예: snmpconfig 명령 , 1025 페이지

SNMP 트랩

SNMP는 하나 이상의 조건이 충족될 때 관리 애플리케이션(대개 SNMP 관리 콘솔)에 트랩을 전송하여 알릴 수 있습니다. 트랩이란 트랩을 전송하는 시스템의 구성 요소와 관련된 데이터를 포함하는 네트워크 패킷입니다. 트랩은 SNMP 에이전트(이 경우 Email Security Appliance)에서 조건이 충족될 때 생성됩니다. 조건이 충족되면 SNMP 에이전트가 SNMP 패킷을 만들어 SNMP 관리 콘솔 소프트웨어를 실행 중인 호스트에 전송합니다.

SNMP 트랩을 활성화하고 구성하려면 snmpconfig 명령을 사용합니다.

여러 트랩 대상을 지정하려면, 트랩 대상에 대한 프롬프트가 표시될 때 쉼표로 구분된 IP 주소를 최대 10개 입력할 수 있습니다.

예: snmpconfig 명령

다음 예에서는 포트 161의 "PublicNet" 인터페이스에서 SNMP를 활성화하는 데 snmpconfig 명령이 C690 하드웨어 어플라이언스에 사용됩니다. 버전 1 및 2의 GET 요청에 대해 public 커뮤니티 문자열을 입력합니다.

```
esa.example.com> snmpconfig
Current SNMP settings:
SNMP Disabled.
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP
Do you want to enable SNMP?
[Y]>
Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: esa.example.com)
[1]>
Which port shall the SNMP daemon listen on interface "Management"?
[161]>
Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2
Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2
Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>
```

```
Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>
Service SNMP V1/V2c requests?
[N]> Y
Enter the SNMP V1/V2c community string.
[ironport]> public
Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>
From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>
Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1
Enter the Trap Community string.
[ironport]> tcomm
Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y
Do you want to disable any of these traps?
[Y]> n
Do you want to enable any of these traps?
[Y]> y
Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 1,7,12
What threshold would you like to set for CPU utilization?
[95]>
What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>
What threshold would you like to set for memory utilization?
[95]>
Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3
Enter the System Contact string.
[snmp@localhost]> esa-admin@example.com
Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: esa-admin@example.com
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>
```

```
esa.example.com> commit
Please enter some comments describing your changes:
[]> Enable and configure SNMP
Changes committed: Fri Nov 06 18:13:16 2015 GMT
esa.example.com>
```

38 장

SenderBase 네트워크 참여

이 장에는 다음 섹션이 포함되어 있습니다.

SenderBase 네트워크 참여 개요

SenderBase는 이메일 관리자가 발신자를 조사하고 이메일의 합법적인 소스를 식별하고 스패머를 차단하도록 지원하기 위해 설계된 이메일 평가 서비스입니다.

SenderBase 네트워크에 참여하는 고객은 모든 사용자에게 서비스 유용성을 높일 수 있도록 Cisco가 조직에 대해 집계된 이메일 트래픽 통계를 수집하는 것을 허용하게 됩니다. 참여는 자발적입니다. Cisco는 Cisco 어플라이언스에서 서로 다른 유형의 메시지 처리 방식에 대한 정보 및 메시지 특성에 대한 요약 데이터만 수집합니다. 예를 들어 Cisco는 메시지 본문이나 메시지 제목은 수집하지 않습니다. 개인 식별이 가능한 정보 및 조직을 식별하는 정보는 기밀이 유지됩니다.

SenderBase와 통계 공유

단계 **1** **Security Services(**보안 서비스**) > SenderBase**로 이동합니다.

단계 **2** **Edit Global Settings(**전역 설정 수정**)**를 클릭합니다.

단계 **3** SenderBase Information Service와 통계 데이터를 공유하려면 확인란을 선택합니다.

이 확인란을 선택하면 어플라이언스에 대한 기능이 전역적으로 활성화됩니다. 활성화되면, 데이터를 수집하고 보고하는 데 CASE(Context Adaptive Scanning Engine)가 사용됩니다(Cisco 안티스팸 검사의 활성화 여부와 상관없이). CLI에서 **`senderbaseconfig`** 명령을 사용하여 동일한 설정을 구성할 수도 있습니다.

단계 **4** (선택 사항) SenderBase Information Service와 통계 데이터를 공유하기 위한 프록시 서버를 활성화합니다.

규칙 업데이트를 검색하도록 프록시 서버를 정의하는 경우 제공된 추가 필드에서 프록시 서버에 연결할 때 필요한 인증된 사용자 이름, 암호 및 특정 포트도 구성할 수 있습니다. 이러한 설정을 수정하려면 업그레이드 및 업데이트

다운로드를 위한 서버 설정 구성 , 949 페이지 섹션을 참조해 주십시오. CLI에서 **updateconfig** 명령을 사용하여 동일한 설정을 구성할 수도 있습니다.

FAQ(자주 묻는 질문)

Cisco는 사용자 개인정보의 중요성을 인식하고 있으므로 이에 대한 보호를 염두에 두고 서비스를 설계 및 운영합니다. SenderBase 네트워크 참여에 등록하면 Cisco는 조직 이메일 트래픽에 대한 집계된 통계를 수집합니다. 그러나 개인 식별이 가능한 정보는 수집하거나 사용하지 않습니다. Cisco에서 수집하는 정보 중 사용자 또는 조직을 식별하는 정보는 기밀로 취급됩니다.

참여해야 하는 이유

SenderBase 네트워크에 참여하면 사용자 지원에 도움이 됩니다. 데이터 공유는 스팸, 바이러스 및 디렉터리 수집 공격 같은 이메일 기반 공격이 조직에 영향을 미치지 못하도록 하는 데 중요한 역할을 합니다. 참여의 중요성을 보여주는 예는 다음과 같습니다.

- 특히 사용자의 조직을 대상으로 한 이메일 공격. 이 경우 사용자가 제공한 데이터가 사용자를 보호할 수 있는 정보의 기본 소스를 제공합니다.
- 사용자의 조직이 새로운 전역 이메일 공격을 받는 첫 번째 대상 중 하나인 경우. 이 경우 공유하는 데이터가 새로운 위협에 대응할 수 있는 속도를 크게 높여줍니다.

공유하는 데이터

Cisco 어플라이언스에서 서로 다른 메시지 유형을 처리한 방식에 대한 정보 및 메시지 특성에 대한 요약 정보가 공유됩니다. 메시지의 전체 본문은 수집하지 않습니다. 다시 강조하지만, Cisco에 제공되는 정보 중 사용자 또는 조직을 식별하는 정보는 기밀로 취급됩니다. (아래의 공유하는 데이터의 보안을 보장하기 위해 Cisco에서 하는 일 , 1034 페이지 섹션을 참조해 주십시오).

다음 표에서는"사용자에게 익숙한" 형식으로 샘플 로그 항목을 설명합니다.

표 ***107: Cisco*** 어플라이언스별로 공유되는 통계

항목	샘플 데이터
MGA 식별자	MGS 10012
타임스탬프	2005년 7월 1일, 오전 8시~오전 8시 5분의 데이터
소프트웨어 버전 번호	MGA 버전 4.7.0
규칙 세트 버전 번호	안티스팸 규칙 세트 102
안티바이러스 업데이트 간격	10분마다 업데이트
쿼런틴 크기	500MB

항목	샘플 데이터
쿼런틴된 메시지 수	쿼런틴의 현재 메시지 50개
바이러스 점수 임계값	위협 수준 3 이상에서 쿼런틴되는 메시지 보내기
쿼런틴되는 메시지의 바이러스 점수 합계	120
쿼런틴되는 메시지 수	30(평균 4점 산출)
최대 쿼런틴 시간	12시간
쿼런틴 시작 및 종료 이유, 안티바이러스와 상관관계 결과 별로 분석된쿼런틴 발생 메시지 수	.exe 규칙 때문에 격리에 들어간 메시지 50개 수동 릴리스 때문에 격리를 떠난 메시지 30개, 30개 모두 바이러스 양성
격리를 떠날 때 수행한 작업별로 분석된 Outbreak 격리 메시지의 수	쿼런틴을 종료한 후 10개 메시지의 첨부파일이 제거됨
메시지가 쿼런틴된 시간 합계	20시간

표 ***108:*** 발신자 ***IP*** 주소별로 공유되는 통계

항목	샘플 데이터
어플라이언스 내 다양한 단계의 메시지 수	안티바이러스 엔진별 표시: 100 안티스팸 엔진별 표시: 80
안티스팸 및 안티바이러스 점수 및 판정 합계	2,000(표시된 모든 메시지에 대한 안티스팸 점수 합계)
다른 안티스팸 및 안티바이러스 규칙 조합에 적중하는 메시지 수	100개의 메시지가 규칙 A와 B에 적중 50개의 메시지가 규칙 A에만 적중
연결 수	20 SMTP 연결
전체 수 및 올바르지 않은 수신인	전체 수신자 50명 잘못된 수신자 10명
해시된 파일 이름: (a)	<one-way-hash>.pif 파일이 <one-way-hash>.zip이라는 아카이브 첨부 파일 안에서 발견됨
난독 처리된 파일 이름: (b)	aaaaaaa0.aaa.pif 파일이 aaaaaaa.zip 파일 안에서 발견됨

항목	샘플 데이터
URL 호스트 이름 (c)	메시지 안에 www.domain.com에 대한 링크가 있습니다.
난독 처리된 URL 경로 (d)	메시지 안에 www.domain.com 호스트 이름에 대한 링크와 aaa000aa/aa00aaa 경로가 있음
스팸 및 바이러스 검사 결과에 의한 메시지 수	스팸 양성 10개 스팸 음성 10개 스팸 의심 5개 바이러스 양성 4개 바이러스 음성 16개 바이러스 검사 불가 5개
다른 안티스팸 및 안티바이러스 판정에 의한 메시지 수	스팸 500개, HAM 300개
크기 범위의 메시지 수	30K-35K 범위에서 125개
다른 확장명 유형 수	".exe" 첨부 파일 300개
첨부파일 유형의 상관 관계, 참 파일 유형 및 컨테이너 유형	".doc" 확장명을 가지고 있지만 실제로는 ".exe"인 첨부 파일 100개 zip 내에 ".exe" 확장명 첨부 파일 50개
확장명 및 참 파일 유형과 첨부파일 크기의 상관 관계	50-55K 범위 ".exe" 첨부 파일 30개
파일 평판 서비스에 업로드된 첨부 파일 수 (AMP 클라우드)	파일 평판 서비스에 업로드된 파일 1110개
파일 평판 서비스에 업로드된 파일에 대한 판정(AMP 클라우드)	악성으로 발견된 파일 10개 정상으로 발견된 파일 100개 파일 평판 서비스에서 알 수 없는 파일 1000개
파일 평판 서비스에 업로드된 파일의 평판 점수(AMP 클라우드)	평판 점수가 37인 파일 50개 평판 점수가 57인 파일 50개 평판 점수가 61인 파일 1개 평판 점수가 99인 파일 9개
파일 평판 서비스에 업로드된 파일의 이름 (AMP 클라우드)	example.pdf testfile.doc

항목	샘플 데이터
파일 평판 서비스에서 탐지한 악성코드 위협 이름(AMP 클라우드)	Trojan-Test

표 *109:* 메시지별로 공유되는 통계

메시지 식별자	내부 메시지 식별자 - 10010
수신자 수	메시지의 수신자 수 - 15
거부된 수신자 수	유효하지 않은 것으로 발견되고 거부된 수신자 수 - 5
안티바이러스 판정	안티바이러스 엔진에서 수신된 판정
AMP 판정	Advanced Malware Protection 엔진의 판정이 악성코드 양성인 경우
대용량 메일	메시지가 헤더 반복 메시지 필터 규칙과 일치하는 경우
내부 Ironport 안티스팸 데이터	Ironport 안티스팸 엔진에서 메시지를 검사한 경우 Ironport 안티스팸 점수 및 메시지 식별자

(a) 파일 이름이 1방향 해시로 인코딩됩니다(MD5).

(b) 파일 이름이 난독 처리된 형식으로 전송됩니다. 모든 소문자 ASCII 문자([a-z])는 "a"로 교체되고 모든 대문자 ASCII 문자([A-Z])는 "A"로 교체되며, 멀티바이트 UTF-8 문자는 "x"로 교체되고(다른 문자 집합에 대한 기밀성 제공), 모든 ASCII 숫자([0-9])는 "0"으로 교체되고, 다른 모든 단일 바이트 문자(공백, 구두점 등)는 유지됩니다. 예를 들어 Britney1.txt.pif 파일은 Aaaaaaa0.aaa.pif로 표시됩니다.

(c) URL 호스트 이름은 IP 주소처럼 콘텐츠를 제공하는 웹 서버를 가리킵니다. 사용자 이름 및 비밀번호 같은 기밀 정보는 포함되지 않습니다.

(d) 사용자의 개인 정보가 노출되지 않도록 호스트 이름 다음에 나오는 URL 정보는 난독 처리됩니다.

AsyncOS 8.5 for Email 이후부터, IronPort Anti-Spam 또는 Intelligent Multi-Scan 기능 키가 활성 상태이고 SenderBase 네트워크 참여가 활성화되면 AsyncOS는 제품 효율성을 높이기 위해 다음 작업을 수행합니다.

- 메시지에서 특정 헤더가 반복되는 것에 대한 정보를 수집하고, 수집된 정보를 암호화하고, 암호화된 정보를 각 메시지에 헤더로서 추가합니다.

  이렇게 처리된 메시지를 분석을 위해 Cisco에 제출할 수 있습니다. 각 메시지는 분석가 팀에서 검토하며 제품의 효율성을 높이기 위해 사용됩니다. 분석을 위해 Cisco에 메시지를 제출하는 방법에 대한 자세한 내용은 Cisco에 잘못 분류된 메시지 보고, 370 페이지 섹션을 참조해 주십시오.

- 발신자의 SBRS와 상관없이, 임의의 메시지 샘플을 안티스팸 검사를 위해 CASE에 전송합니다. CASE는 이러한 메시지를 검사하고 그 결과를 제품 효율성 향상에 사용합니다. AsyncOS는 유휴

상태일 때에만 이 작업을 수행합니다. 따라서 이 피드백 메커니즘은 메시지 처리에 심각한 영향을 미치지 않습니다.

공유하는 데이터의 보안을 보장하기 위해 Cisco에서 하는 일

SenderBase 네트워크 참여에 동의할 경우:

- Cisco 어플라이언스에서 전송되는 데이터는 보안 프로토콜 HTTPS를 사용하여 Cisco SenderBase Network 서버로 전송됩니다.
- Cisco에서는 모든 고객 데이터를 신중하게 처리합니다. 이 데이터는 안전한 장소에 저장되며, 회사의 이메일 보안 제품 및 서비스를 개선하거나 고객 지원을 제공하기 위해 액세스가 필요한 Cisco의 직원 및 계약 직원만이 이 데이터에 액세스할 수 있습니다.
- 데이터를 기반으로 보고서나 통계를 생성할 때 이메일 수신자 또는 고객 회사를 식별하는 정보는 Cisco Systems 외부에서 공유되지 않습니다.

데이터 공유가 내 Cisco 어플라이언스의 성능에 영향을 미칩니까?

대부분의 고객이 경험하는 성능 영향은 최소 수준에 그칠 것으로 Cisco는 확신합니다. Cisco는 메일 전달 프로세스의 일부로서 이미 존재하는 데이터를 기록합니다. 그런 다음 어플라이언스에서 고객 데이터가 집계되어 일반적으로 5분마다 SenderBase 서버로 일괄 전송됩니다. HTTPS를 통해 전송되는 총 데이터 크기는 일반적인 회사 이메일 트래픽 대역폭의 1% 미만일 것으로 예상합니다.

활성화되면, 데이터를 수집하고 보고하는 데 CASE(Context Adaptive Scanning Engine)가 사용됩니다 (Cisco 안티스팸 검사의 활성화 여부와 상관없이).

참고 SenderBase 네트워크 참여에 동의할 경우 각 메시지에 대해 "본문 검사"가 수행됩니다. 이는 메시지에 적용되는 필터 또는 기타 작업이 본문 검사를 트리거했는지 여부와 상관없이 발생합니다. 본문 검사에 대한 자세한 내용은 "Body Scanning(본문 검사) 규칙, 172 페이지" 섹션을 참조해 주십시오.

추가 질문이 있으면 Cisco 고객 지원에 문의하십시오. Cisco Support Community, 7 페이지를 참조하십시오.

더 많은 데이터를 공유하는 다른 방법

Cisco에서 최고 품질의 보안 서비스를 제공하도록 더 많은 도움을 제공하고자 하는 고객은 추가 데이터 공유를 허용하는 명령을 사용할 수 있습니다. 더 높은 레벨의 이 데이터 공유 방식에서는 첨부 파일 이름이 해시되지 않은 일반 텍스트로 제공되며 메시지에 있는 URL의 호스트 이름도 제공됩니다. 이 기능에 대해 자세히 알아보려면 사내 시스템 엔지니어와 상의하거나 Cisco 고객 지원에 문의하십시오.

39 장

GUI 기타 작업

이 장에는 다음 섹션이 포함되어 있습니다.

그래픽 사용자 인터페이스(GUI)

그래픽 사용자 인터페이스(GUI)는 시스템 모니터링 및 구성을 위한 일부 CLI(Command Line Interface) 명령 대신 사용할 수 있는 웹 기반 방법입니다. GUI를 사용하면 AsyncOS 명령 구문에 대해 알지 못해도 간단한 웹 기반 인터페이스를 사용하여 시스템을 모니터링할 수 있습니다. 인터페이스에 대해 HTTP 및/또는 HTTPS 서비스가 활성화된 후 GUI에 액세스하여 로그인할 수 있습니다. 자세한 내용은 "어플라이언스에 액세스" 장을 참조하십시오.

인터페이스의 GUI 활성화

기본적으로 시스템은 Management 인터페이스에서 HTTP가 활성화된 상태로 제공됩니다.

GUI를 활성화하려면 CLI에서 interfaceconfig 명령을 실행하고, 연결할 인터페이스를 수정한 다음, HTTP 서비스 활성화나 HTTP 서비스 보안 조치를 수행하거나 둘을 모두 수행합니다.

참고 다른 인터페이스에서 GUI를 활성화한 경우 Network(네트워크) > IP Interfaces(IP 인터페이스) 페이지를 사용하여 인터페이스에서 GUI를 활성화 또는 비활성화할 수 있습니다. 자세한 내용은 IP 인터페이스, 1199 페이지를 참조하십시오.

참고 인터페이스에서 보안 HTTP를 활성화하는 경우 인증서를 설치해야 합니다. 자세한 내용은 "HTTPS용 인증서 활성화"를 참조하십시오.

어떤 서비스든, 서비스를 활성화할 포트를 지정합니다. 기본적으로 포트 80에서는 HTTP가 활성화되고 포트 443에서는 HTTPS가 활성화됩니다. 한 인터페이스에 대해 두 서비스를 모두 활성화하는 경우 HTTP 요청을 자동으로 안전한 서비스로 리디렉션할 수 있습니다.

또한 이 인터페이스에서 HTTP 또는 HTTPS를 통해 GUI에 액세스하려는 모든 사용자(사용자 계정 작업, 893 페이지 참고)는 표준 사용자 이름 및 암호 로그인 페이지에서 인증을 받아야 합니다.

참고 GUI에 액세스하려면 먼저 commit 명령을 사용하여 변경 사항을 저장해야 합니다.

다음 예에서는 Data 1 인터페이스에 대해 GUI가 활성화됩니다. 포트 80에서 HTTP 및 포트 443에서 HTTPS를 활성화하는 데에는 interfaceconfig 명령이 사용됩니다. (certconfig 명령을 실행할 수 있을 때까지 HTTP에 대해 데모 인증서가 임시로 사용됩니다. 자세한 내용은 "Cisco 어플라이언스에 인증서 설치"를 참고하십시오.) 포트 80의 HTTP 요청은 Data1 인터페이스에 대해 포트 443으로 자동으로 리디렉션됩니다.

GUI에서의 시스템 정보

- **System Overview(**시스템 개요**)** 페이지에서 다음을 수행할 수 있습니다.
  - 몇몇 주요 시스템 상태 및 성능 정보를 표시하는 기록 그래프 및 테이블을 볼 수 있습니다.
  - 어플라이언스에 설치된 AsyncOS 운영 체제의 버전을 볼 수 있습니다.
  - 주요 통계의 하위 집합을 볼 수 있습니다.
- **System Status(**시스템 상태**)** 페이지에는 시스템에 대한 실시간 메일 및 DNS 활동이 자세히 표시됩니다. 시스템 통계에 대한 카운터를 재설정하고 카운터가 마지막으로 재설정된 시간을 볼 수도 있습니다.

GUI에서 XML 상태 수집

XML 페이지를 통해 상태를 보거나, 프로그래밍 방식으로 XML 상태 정보에 액세스합니다.

XML 상태 기능은 이메일 모니터링 통계에 프로그래밍 방식으로 액세스할 수 있는 방법을 제공합니다. 일부 최신 브라우저는 XML 데이터를 직접 렌더링할 수도 있습니다.

이 표에 있는 GUI 페이지의 정보는 해당 URL에 액세스하여 동적 XML 출력으로도 이용할 수 있습니다.

GUI 페이지 이름	해당 **XML** 상태 **URL**
Mail Status(메일 상태)	http:// *hostname* /xml/status
Host Mail Status for a Specified Host(지정된 호스트에 대한 호스트 메일 상태)	http:// *hostname* /xml/hoststatus?hostname= *host*
DNS Status(DNS 상태)	http:// *hostname* /xml/dnsstatus

GUI 페이지 이름	해당 XML 상태 URL
Top Incoming Domains(상위 수신 도메인)	http:// *hostname* /xml/topin
Top Outgoing Domains(상위 발신 도메인)[1]	http:// *hostname* /xml/tophosts

[1] 이 페이지의 기본 정렬 순서는 활성 수신자의 번호순입니다. URL에 "?sort=order"를 첨부하여 순서를 변경할 수 있습니다. 여기서 order는 conn_out, deliv_recip, soft_bounced 또는 hard_bounced입니다.

40 장

고급 네트워크 컨피그레이션

이 장에는 다음 섹션이 포함되어 있습니다.

이더넷 인터페이스의 미디어 설정

이더넷 인터페이스의 미디어 설정은 etherconfig 명령을 사용하여 액세스할 수 있습니다. 각 이더넷 인터페이스가 현재 설정과 함께 나열됩니다. 인터페이스를 선택하면 사용 가능한 미디어 설정이 표시됩니다. 예는 미디어 설정 편집 예, 1040 페이지 항목을 참조하십시오.

etherconfig를 사용하여 이더넷 인터페이스의 미디어 설정 편집

etherconfig 명령을 사용하여 양방향 설정(전이중/반이중)과 이더넷 인터페이스의 속도(10/100/1,000Mbps)를 설정할 수 있습니다. 기본적으로 이 인터페이스는 미디어 설정을 자동으로 선택하지만, 이 설정을 재정의해야 할 경우도 있습니다.

참고 "설정 및 설치" 장에 설명한 것처럼 GUI의 시스템 설치 마법사(또는 Command Line Interface의 systemsetup 명령)를 완료하고 변경사항을 커밋하면 기본 이더넷 인터페이스 설정이 어플라이언스에 구성됩니다.

일부 어플라이언스에는 광섬유 네트워크 인터페이스 옵션이 있습니다. 사용 가능한 경우, 해당 어플라이언스의 사용 가능한 인터페이스 목록에 이더넷 인터페이스 2개(데이터 3 및 데이터 4)가 추가로 표시됩니다. 이러한 기가비트 광섬유 인터페이스는 이기종 구성에서 구리(데이터 1, 데이터 2 및 관리) 인터페이스와 페어링될 수 있습니다. NIC(Network Interface Card) 페어링/티밍, 1040 페이지를 참조하십시오.

미디어 설정 편집 예

```
mail3.example.com> etherconfig

Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.

[]> media
Ethernet interfaces:
1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d
2. Data 2 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e
3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da

Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]> edit
Enter the name or number of the ethernet interface you wish to edit.
[]> 2
Please choose the Ethernet media options for the Data 2 interface.
1. Autoselect
2. 10baseT/UTP half-duplex
3. 10baseT/UTP full-duplex
4. 100baseTX half-duplex

5. 100baseTX full-duplex


6. 1000baseTX half-duplex
7. 1000baseTX full-duplex
[1]> 5
Ethernet interfaces:
1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d
2. Data 2 (100baseTX full-duplex: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e
3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da
Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]>
```

NIC(Network Interface Card) 페어링/티밍

NIC 페어링을 사용하면 NIC에서 업스트림 이더넷 포트로 연결되는 데이터 경로에 장애가 발생하는 경우 백업 이더넷 인터페이스를 제공하도록 물리적 데이터 포트 2개를 결합할 수 있습니다. 기본적으로 페어링에서는 기본 인터페이스와 백업 인터페이스를 지정하여 이더넷 인터페이스를 구성합니다. 기본 인터페이스에 오류가 발생(즉, NIC와 업스트림 노드 간 캐리어 중단)하면, 백업 인터페이스

가 활성화되고 경고가 전송됩니다. 기본 인터페이스가 다시 동작하면 이 인터페이스가 자동으로 활성화됩니다. 이 제품의 설명서에서 NIC 페어링과 NIC 티밍은 동일합니다.

참고 Email Security 가상 어플라이언스에서는 NIC 페어링을 사용할 수 없습니다.

데이터 포트가 충분히 있는 경우 여러 NIC 쌍을 생성할 수 있습니다. NIC 쌍을 생성하는 경우 두 데이터 포트를 함께 사용할 수 있습니다. 예를 들면 다음과 같습니다.

데이터 1 및 데이터 2

데이터 3 및 데이터 4

데이터 2 및 데이터 3

기타

일부 Cisco 어플라이언스에는 광섬유 네트워크 인터페이스 옵션이 있습니다. 사용 가능한 경우, 해당 어플라이언스의 사용 가능한 인터페이스 목록에 이더넷 인터페이스 2개(데이터 3 및 데이터 4)가 추가로 표시됩니다. 이러한 기가비트 광섬유 인터페이스는 이기종 구성에서 구리(데이터 1, 데이터 2 및 관리) 인터페이스와 페어링될 수 있습니다.

NIC 페어링 및 VLAN

VLAN(VLAN(Virtual Local Area Network), 1043 페이지 참조)은 기본 인터페이스에서만 허용됩니다.

NIC 쌍 이름 지정

NIC 쌍을 생성하는 경우 해당 쌍을 참조하는 데 사용할 이름을 지정해야 합니다. AsyncOS 버전 4.5 이전에 생성된 NIC 쌍의 경우 업그레이드 후에 자동으로 기본 이름인 'Pair 1'이 지정됩니다.

NIC 페어링과 관련해 생성된 모든 경고는 특정 NIC 쌍을 이름별로 참조합니다.

NIC 페어링 및 기존 리스너

리스너가 할당되어 있는 인터페이스에서 NIC 페어링을 사용하는 경우 백업 인터페이스에 할당된 모든 리스너를 삭제, 재할당 또는 비활성화할지 묻는 프롬프트가 표시됩니다.

etherconfig 명령을 통해 NIC 페어링 활성화

참고 Email Security 가상 어플라이언스에서는 NIC 페어링을 사용할 수 없습니다.

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.
```

```
- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]> pairing

Paired interfaces:

Choose the operation you want to perform:

- NEW - Create a new pairing.

[]> new

Please enter a name for this pair (Ex: "Pair 1"):

[]> Pair 1

Warning: The backup (Data 2) for the NIC Pair is currently configured with one or more
IP addresses. If you continue, the Data 2 interface will be deleted.

Do you want to continue? [N]> y

The interface you are deleting is currently used by listener "OutgoingMail".

What would you like to do?

1. Delete: Remove the listener and all its settings.

2. Change: Choose a new interface.

3. Ignore: Leave the listener configured for interface "Data 2" (the listener will be
disabled until you add a new interface named "Data 2" or edit the listener's settings).


[1]>

Listener OutgoingMail deleted for mail3.example.com.

Interface Data 2 deleted.

Paired interfaces:

1. Pair 1:


Primary (Data 1) Active, Link is up

Backup (Data 2) Standby, Link is up

Choose the operation you want to perform:

- DELETE - Delete a pairing.

- STATUS - Refresh status.
```

```
[]>
```

VLAN(Virtual Local Area Network)

어플라이언스의 물리적 네트워크 포트에서 여러 VLAN(Virtual Local Area Network)을 구성할 수 있습니다.

VLAN을 사용하면 다음이 가능합니다.

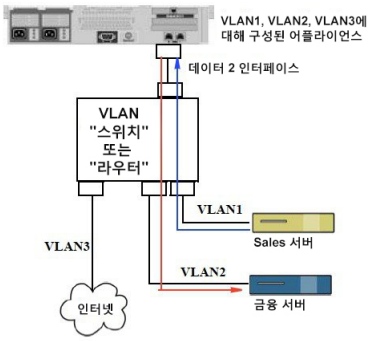
- 어플라이언스가 연결할 수 있는 네트워크의 수를 어플라이언스에 있는 물리적 인터페이스의 수보다 늘릴 수 있습니다.
- 기존 리스너에 있는 별도의 "포트"에 더 많은 네트워크를 정의할 수 있습니다.
- 보안 목적으로, 관리 편이성을 위해 또는 대역폭 증가를 위해 네트워크를 세그먼트화할 수 있습니다.

사용 사례:

VLAN 제한 때문에 직접 통신할 수 없는 두 개의 메일 서버가 Email Security Appliance를 통해 메일을 보낼 수 있습니다. 어플라이언스의 Data 2 인터페이스는 VLAN1 및 VLAN2로 구성됩니다. 파란색 선은 Sales 네트워크(VLAN1)에서 어플라이언스로의 메일을 보여줍니다. 어플라이언스는 메일을 정상적으로 처리한 다음, 전달 시 대상 VLAN2 정보(빨간색 선)로 패킷에 태그를 지정합니다.

어플라이언스 간 통신을 위해 VLAN 사용

그림 ***75: VLAN***을 사용하여 어플라이언스 간 통신 효율 증대



VLAN 구성 정보

일부 어플라이언스 모델에서 사용할 수 있는 광섬유 데이터 포트와 "Data" 및 "Management" 포트 등 어플라이언스의 물리적 네트워크 포트에 여러 VLAN을 구성할 수 있습니다. AsyncOS는 최대 30개의 VLAN을 지원합니다.

VLAN에 두기 위해 물리적 포트에 IP 주소가 구성되어 있을 필요는 없습니다. VLAN을 만든 물리적 포트는 비 VLAN 트래픽을 수신할 IP를 가질 수 있습니다. 따라서 동일한 인터페이스에서 VLAN과 비 VLAN 트래픽이 모두 있을 수 있습니다.

VLAN은 NIC 페어링(페어링된 NIC에서 사용 가능) 및 DSR(Direct Server Return)과 함께 사용할 수 있습니다.

VLAN은 "VLAN DDDD" 형식의 레이블이 붙은 동적 "데이터 포트"로 나타납니다. 여기서 "DDDD"는 ID이며 최대 4자리 길이의 정수입니다(예: VLAN 2 또는 VLAN 4094). VLAN ID는 어플라이언스에서 고유해야 합니다.

관련 주제

FTP, SSH 및 SCP 액세스, 1199 페이지

VLAN 관리

etherconfig 명령을 통해 VLAN을 만들고 수정하고 삭제할 수 있습니다. VLAN을 만들었으면 Network > Interfaces(네트워크 > 인터페이스) 페이지 또는 CLI의 interfaceconfig 명령을 통해 구성할 수 있습니다. 모든 변경사항을 커밋해야 합니다.

etherconfig 명령을 통해 새 VLAN 생성

이 예에서는 데이터 1 포트에 VLAN 2개를 생성(이름: VLAN 31 및 VLAN 34)합니다.

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]> vlan

VLAN interfaces:

Choose the operation you want to perform:

- NEW - Create a new VLAN.

[]> new

VLAN ID for the interface (Ex: "34"):

[]> 34

Enter the name or number of the ethernet interface you wish bind to:

1. Data 1

2. Data 2

3. Management

[1]> 1
```

```
VLAN interfaces:
1. VLAN 34 (Data 1)
Choose the operation you want to perform:

- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]> new
VLAN ID for the interface (Ex: "34"):
[]> 31
Enter the name or number of the ethernet interface you wish bind to:
1. Data 1
2. Data 2
3. Management
[1]> 1
VLAN interfaces:
1. VLAN 31 (Data 1)
2. VLAN 34 (Data 1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]>
```

interfaceconfig 명령을 통해 VLAN에서 IP 인터페이스 생성

이 예에서는 VLAN 31 이더넷 인터페이스에서 새 IP 인터페이스를 생성합니다.

인터페이스를 변경하면 어플라이언스와의 연결이 종료될 수 있습니다.

```
mail3.example.com> interfaceconfig

Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]> new


Please enter a name for this IP interface (Ex: "InternalNet"):


[]> InternalVLAN31

Would you like to configure an IPv4 address for this interface (y/n)? [Y]>

IPv4 Address (Ex: 10.10.10.10):

[]> 10.10.31.10

Netmask (Ex: "255.255.255.0" or "0xffffff00"):

[255.255.255.0]>

Would you like to configure an IPv6 address for this interface (y/n)? [N]>

Ethernet interface:

1. Data 1

2. Data 2

3. Management

4. VLAN 31

5. VLAN 34

[1]> 4

Hostname:

[]> mail31.example.com

Do you want to enable SSH on this interface? [N]>
```

```
Do you want to enable FTP on this interface? [N]>

Do you want to enable HTTP on this interface? [N]>

Do you want to enable HTTPS on this interface? [N]>

Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. InternalVLAN31 (10.10.31.10/24: mail31.example.com)

3. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]>
```

웹 인터페이스를 사용하여 **VLAN** 구성

etherconfig 명령을 사용하여 VLAN을 만들었으면 Network > Listeners(네트워크 > 리스너) 페이지를 사용하여 구성할 수 있습니다.

Direct Server Return

DSR(Direct Server Return)은 동일한 VIP(가상 IP)를 공유하는 여러 Email Security Appliance 간 로드 밸런싱을 위해 경량 로드 밸런싱 메커니즘에 대한 지원을 제공하는 방법입니다.

DSR은 어플라이언스의 “루프백” 이더넷 인터페이스에서 생성된 IP 인터페이스를 통해 구현됩니다.

참고 Email Security Appliance에 대해 로드 밸런싱을 구성하는 것은 이 문서의 범위를 벗어납니다.

DSR(Direct Server Return) 활성화

참여하는 각 어플라이언스에서 "루프백" 이더넷 인터페이스를 활성화하여 DSR을 활성화합니다. 그런 다음 CLI의 **interfaceconfig** 명령 또는 GUI의 Network > Interfaces(네트워크 > 인터페이스) 페이지를 통해 VIP(가상 IP)로 루프백 인터페이스에서 IP 인터페이스를 만듭니다. 마지막으로 CLI의 **listenerconfig** 명령 또는 GUI의 Network > Listeners(네트워크 > 리스너) 페이지를 통해 새 IP 인터페이스에서 리스너를 만듭니다. 모든 변경 사항은 반드시 커밋해야 합니다.

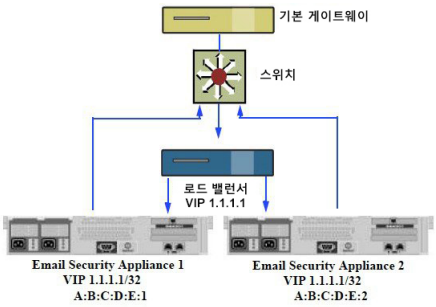
참고 루프백 인터페이스를 사용하면 어플라이언스에서 특정 인터페이스의 ARP 응답을 실행하지 못하게 됩니다.

DSR을 활성화하는 경우 다음과 같은 규칙이 적용됩니다.

모든 시스템이 동일한 VIP(가상 IP) 주소를 사용합니다.

모든 시스템은 로드 밸런서와 동일한 스위치 및 서브넷에 있어야 합니다.

그림 ***76:*** 한 스위치의 여러 ***Email Security Appliance*** 간 로드 밸런싱을 위해 ***DSR*** 사용



한 스위치의 여러 Email Security Appliance 간 로드 밸런싱을 위해 DSR 사용

etherconfig 명령을 통해 루프백 인터페이스 활성화

활성화된 경우, 루프백 인터페이스는 다른 인터페이스(예: 데이터 1)처럼 처리됩니다.

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.


[]> loopback

Currently configured loopback interface:

Choose the operation you want to perform:


- ENABLE - Enable Loopback Interface.

[]> enable

Currently configured loopback interface:
```

```
1. Loopback

Choose the operation you want to perform:

- DISABLE - Disable Loopback Interface.

[]>

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]>
```

interfaceconfig 명령을 통해 루프백에서 IP 인터페이스 생성

다음과 같이 루프백 인터페이스에서 IP 인터페이스를 생성합니다.

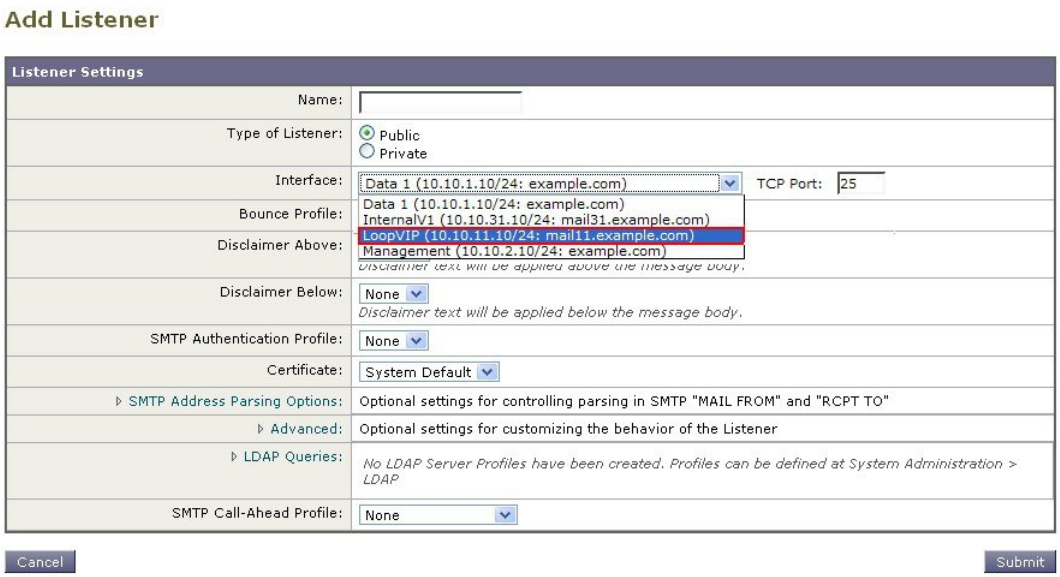
```
mail3.example.com> interfaceconfig

Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. InternalV1 (10.10.31.10/24: mail31.example.com)

3. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]> new

Please enter a name for this IP interface (Ex: "InternalNet"):

[]> LoopVIP

Would you like to configure an IPv4 address for this interface (y/n)? [Y]>

IPv4 Address (Ex: 10.10.10.10):

[]> 10.10.1.11
```

```
Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]> 255.255.255.255
Would you like to configure an IPv6 address for this interface (y/n)? [N]>
Ethernet interface:
1. Data 1
2. Data 2
3. Loopback
4. Management
5. VLAN 31
6. VLAN 34
[1]> 3
Hostname:
[]> example.com
Do you want to enable SSH on this interface? [N]>

Do you want to enable FTP on this interface? [N]>

Do you want to enable HTTP on this interface? [N]>
Do you want to enable HTTPS on this interface? [N]>

Currently configured interfaces:
1. Data 1 (10.10.1.10/24: example.com)
2. InternalV1 (10.10.31.10/24: mail31.example.com)
3. LoopVIP (10.10.1.11/24: example.com)
4. Management (10.10.0.10/24: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]>
```

새 IP 인터페이스에서 리스너 생성

GUI에서 또는 CLI를 통해 새 IP 인터페이스에서 리스너를 생성할 수 있습니다. 예를 들어 다음 그림에서는 GUI의 Add Listener(리스너 추가) 페이지에서 생성할 수 있는 새로 생성된 IP 인터페이스를 보여줍니다.

그림 *77:* 새 루프백 *IP* 인터페이스에서 리스너 생성



이더넷 인터페이스의 최대 전송 단위

MTU(최대 전송 단위)는 이더넷 인터페이스가 수락하는 데이터의 최대 단위입니다. etherconfig 명령을 사용하여 이더넷 인터페이스의 MTU를 줄일 수 있습니다. 기본 MTU 크기는 1,500바이트로, 이는 이더넷 인터페이스가 수락할 수 있는 최대 MTU입니다.

인터페이스의 MTU를 편집하려면 다음을 수행합니다.

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

- MTU - View and configure MTU.

- MULTICAST - Accept or reject ARP replies with a multicast address.

[]> mtu

Ethernet interfaces:
```

```
1. Data 1 mtu 1400

2. Data 2 default mtu 1500

3. Management default mtu 1500

Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[]> edit

Enter the name or number of the ethernet interface you wish to edit.

[]> 2

Please enter a non-default (1500) MTU value for the Data 2 interface.

[]> 1200

Ethernet interfaces:

1. Data 1 mtu 1400

2. Data 2 mtu 1200

3. Management default mtu 1500

Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[]>
```

멀티캐스트 주소를 사용하여 **ARP** 응답 수락 또는 거부

이제 멀티캐스트 주소를 사용하여 ARP 응답을 수락할지 거부할지를 지정할 수 있습니다. 이 기능을 구성하려면 MULTICAST 하위 명령을 사용합니다.

다음 예에서는 멀티캐스트 주소를 사용하여 ARP 응답을 수락하도록 어플라이언스를 구성하는 방법을 보여줍니다.

```
mail.example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> multicast
ARP replies with a multicast address will be rejected.
Choose the operation you want to perform:
- ACCEPT - Accept ARP replies with a multicast address.
[]> accept
ARP replies with a multicast address will be accepted.
```

41 장

로깅

이 장에는 다음 섹션이 포함되어 있습니다.

개요

로그 파일 및 로그 서브스크립션 이해

로그는 AsyncOS의 이메일 작업에 대한 중요한 정보를 수집하기 위한 간결하고 효과적인 방법입니다. 이러한 로그는 어플라이언스의 활동에 대한 정보를 기록합니다. 어떤 로그를 보는가에 따라 정보가 달라집니다(예: 반송 로그 또는 전달 로그).

대부분의 로그는 일반 텍스트(ASCII) 형식으로 기록되지만 전달 로그는 리소스 효율성을 위해 이진 방식으로 기록됩니다. ASCII 텍스트 정보는 텍스트 편집기에서 읽을 수 있습니다.

Cisco는 여러 Email Security Appliance에서 오는 로그를 중앙에서 보고하고 추적하기 위한 툴인 M-Series Content Security Management 어플라이언스를 제공합니다. 자세한 내용은 Cisco 담당자에게 문의하십시오.

로그 서브스크립션은 로그 유형을 이름, 로깅 레벨 및 기타 제약 조건(크기 및 대상 정보)과 연결합니다. 동일한 로그 유형에 여러 서브스크립션이 허용됩니다.

로그 유형

로그 유형은 생성된 로그 내에 어떤 정보가 기록될지를 나타냅니다(예: 메시지 데이터, 시스템 통계, 이진 또는 텍스트 데이터). 로그 서브스크립션을 만들 때 로그 유형을 선택합니다. 자세한 내용은 로그 서브스크립션, 1105 페이지를 참조하십시오.

AsyncOS는 다음 로그 유형을 생성합니다.

표 ***110:*** 로그 유형

로그	설명
텍스트 메일 로그	텍스트 메일 로그는 이메일 시스템 운영에 대한 정보를 기록합니다. 예를 들면 메시지 수신, 메시지 전달 시도, 시작된 연결과 종료된 연결, 반송, TLS 연결 등이 있습니다.
qmail 형식 메일 로그	qmail 형식 전달 로그는 이메일 시스템 운영과 관련하여 다음의 전달 로그와 동일한 정보를 기록하지만 qmail 형식으로 저장합니다.
Delivery Logs	전달 로그는 Email Security Appliance의 이메일 전달 운영에 대한 중요한 정보를 기록합니다(예: 각 수신자 전달 및 전달 시도 시 반송에 대한 정보). 로그 메시지는 "무상태(stateless)"입니다. 즉, 모든 관련 정보는 각 로그 메시지에 기록되며 사용자는 현재 전달 시도에 대한 정보의 이전 로그 메시지를 참조할 필요가 없습니다. 전달 로그는 리소스 효율성을 위해 이진 형식으로 기록됩니다. 전달 로그 파일을 XML 또는 CSV(comma-separated values) 형식으로 변환하려면 제공된 유틸리티를 사용하여 사후 처리해야 합니다. 변환 툴은 다음 사이트에서 이용할 수 있습니다. https://supportforums.cisco.com/document/33721/cisco-ironport-systems-contributed-tools
반송 로그	반송 로그는 반송된 수신자에 대한 정보를 기록합니다. 반송된 각 수신자에 대해 기록되는 정보에는 메시지 ID, 수신자 ID, Envelope From 주소, Envelope To 주소, 수신자 반송 사유, 수신자 호스트로부터의 응답 코드 등이 포함됩니다. 또한 반송된 각 수신자 메시지의 고정된 양을 로깅하도록 선택할 수 있습니다. 이 양은 바이트 단위로 정의되며 기본값은 영(0)입니다.
Status Logs	이 로그 파일은 CLI 상태 명령(status detail 및 dnsstatus 포함)에서 발견되는 시스템 통계를 기록합니다. 기록 기간은 logconfig의 setup 하위 명령을 사용하여 설정합니다. 상태 로그에 보고되는 각 카운터 또는 점수는 카운터가 마지막으로 재설정된 이후의 값입니다.
Domain Debug Logs	도메인 디버그 로그는 Email Security Appliance와 지정된 수신자 호스트 간 SMTP 변환 중 클라이언트와 서버 통신을 기록합니다. 특정 수신자 호스트의 문제를 디버그하는 데 이 로그 유형을 사용할 수 있습니다. 로그 파일에 기록할 총 SMTP 세션 수를 지정해야 합니다. 세션이 기록됨에 따라 이 숫자가 줄어듭니다. 로그 서브스크립션을 삭제 또는 수정함으로써 모든 세션이 기록되기 전에 도메인 디버그를 중단할 수 있습니다.
Injection Debug Logs	주입 디버그 로그는 Email Security Appliance와 시스템에 연결된 지정된 호스트 간 SMTP 대화를 기록합니다. 주입 디버그 로그는 Email Security Appliance와 인터넷의 호스트 간 통신 문제를 해결하는 데 유용합니다.

로그	설명
시스템 로그	시스템 로그는 부팅 정보, 가상 어플라이언스 라이센스 만료 알림, DNS 상태 정보, 사용자가 commit 명령으로 입력한 코멘트 등을 기록합니다. 시스템 로그는 어플라이언스의 기본 상태 문제를 해결하는 데 유용합니다.
CLI Audit Logs	CLI 감사 로그는 시스템의 모든 CLI 활동을 기록합니다.
FTP 서버 로그	FTP 로그는 인터페이스에서 활성화된 FTP 서비스에 대한 정보를 기록합니다. 연결 세부사항 및 사용자 활동이 기록됩니다.
GUI 로그	HTTP 로그를 참조하십시오.
HTTP 로그	HTTP 로그는 인터페이스에서 활성화된 HTTP 및/또는 보안 HTTP 서비스에 대한 정보를 기록합니다. GUI는 HTTP를 통해 액세스하므로, GUI의 HTTP 로그는 표면적으로 CLI 감사 로그와 같습니다. GUI에서 액세스하는 세션 데이터(새 세션, 만료된 세션) 및 페이지가 기록됩니다. 이러한 로그에는 SMTP 트랜잭션에 대한 정보도 포함됩니다(예: 어플라이언스에서 이메일로 보내는 예약된 보고서에 대한 정보).
NTP 로그	NTP 로그는 어플라이언스 및 구성된 NTP(Network Time Protocol) 서버 간 대화를 기록합니다. 자세한 내용은 "시스템 관리" 장의 "NTP(Network Time Protocol) 컨피그레이션 수정(시간 유지 방법)"을 참조하십시오.
LDAP 디버그 로그	LDAP 디버그 로그는 LDAP 설치 디버그용입니다. ("LDAP 쿼리" 장을 참조하십시오.) Email Security Appliance가 LDAP 서버로 전송하는 쿼리에 대한 유용한 정보가 여기에 기록됩니다.
Anti-Spam Logs	안티스팸 로그는 최신 안티스팸 규칙 업데이트 수신에 대한 상태를 비롯하여 시스템의 안티스팸 검사 기능 상태를 기록합니다. Context Adaptive Scanning Engine과 관련된 로그도 여기에 기록됩니다.
Anti-Spam Archive	안티스팸 검사 기능을 활성화하면 검사되고 "메시지 아카이브" 작업과 연결된 메시지가 여기에 보관됩니다. 형식은 mbox 형식의 로그 파일입니다. 안티스팸 엔진에 대한 자세한 내용은 "안티스팸" 장을 참조하십시오.
그레이메일 엔진 로그	그레이메일 엔진, 상태, 컨피그레이션 등에 대한 정보를 포함합니다. 대부분의 정보는 Info(정보) 또는 Debug(디버그) 레벨입니다.
그레이메일 아카이브	아카이브된 메시지(검사되고 "메시지 아카이브" 작업과 연결된 메시지)를 포함합니다. 형식은 mbox 형식의 로그 파일입니다.
Anti-Virus Logs	안티바이러스 로그는 최신 안티바이러스 파일 업데이트 수신에 대한 상태를 비롯하여 시스템의 안티바이러스 검사 기능 상태를 기록합니다.

로그	설명
안티바이러스 아카이브	안티바이러스 엔진을 활성화하면 검사되고 "메시지 아카이브" 작업과 연결된 메시지가 여기에 보관됩니다. 형식은 mbox 형식의 로그 파일입니다. 자세한 내용은 "안티바이러스" 장을 참고하십시오.
AMP 엔진 로그	AMP Engine 로그는 시스템의 Advanced Malware Protection 기능에 대한 상태를 기록합니다. 자세한 내용은 File Reputation Filtering and File Analysis(파일 평판 필터링 및 파일 분석), 461 페이지을 참조해 주십시오.
AMP 아카이브	Advanced Malware Protection 엔진이 검사할 수 없는 첨부 파일이 있다고 또는 악성코드가 포함되었다고 확인한 메시지를 보관하도록 메일 정책을 구성한 경우 해당 메시지가 여기에 보관됩니다. 형식은 mbox 형식의 로그 파일입니다.
Scanning Logs	검사 로그에는 검사 엔진에 대한 모든 LOG 및 COMMON 메시지가 포함됩니다(알림, 962 페이지 참조). 이러한 메시지는 일반적으로 애플리케이션 장애, 전송 알림, 실패 알림 및 로그 오류 메시지입니다. 이 로그는 시스템 전체 알림에 적용되지 않습니다.
스팸 격리 로그	스팸 격리 로그는 스팸 격리 프로세스와 관련된 작업을 기록합니다.
스팸 격리 GUI 로그	스팸 격리 로그는 GUI를 통한 컨피그레이션, 최종 사용자 인증, 최종 사용자 작업(이메일 릴리스 등)을 포함하여 스팸 격리와 관련된 작업을 기록합니다.
SMTP 대화 로그	SMTP 대화 로그는 수신 및 발신 SMTP 대화의 모든 부분을 기록합니다.
허용 목록/차단 목록 로그	허용 목록/차단 목록 로그는 허용 목록/차단 목록 설정 및 데이터베이스에 대한 데이터를 기록합니다.
보고 로그	보고 로그는 중앙 집중식 보고 서비스의 프로세스와 관련된 작업을 기록합니다.
쿼리 보고 로그	보고 쿼리 로그는 어플라이언스에서 실행되는 보고 쿼리와 관련된 작업을 기록합니다.
업데이터 로그	업데이터 로그는 McAfee Anti-Virus 정의 업데이트와 같은 시스템 서비스의 업데이트와 관련된 이벤트를 기록합니다.
Tracking Logs	추적 로그는 추적 서비스의 프로세스와 관련된 작업을 기록합니다. 추적 로그는 메일 로그의 하위 집합입니다.
인증 로그	인증 로그는 사용자 로그인 시도의 성공과 실패를 기록합니다.
구성 기록 로그	컨피그레이션 기록 로그는 Email Security Appliance에서 무엇이 언제 변경되었는지에 대한 정보를 기록합니다. 사용자가 변경 사항을 커밋할 때마다 새 컨피그레이션 기록 로그가 생성됩니다.

로그	설명
업그레이드 로그	업그레이드 다운로드 및 설치에 대한 상태 정보.
API 로그	API 로그는 AsyncOS API for Cisco Email Security Appliances와 관련된 다음과 같은 다양한 이벤트를 기록합니다. • API 시작 또는 중지 • 실패 또는 종료된 API에 대한 연결(응답을 제공한 후) • 인증 성공 또는 실패 • 오류가 있는 요청 • AsyncOS API에 네트워크 구성 변경 사항을 알리는 중 오류 발생

로그 유형 특성

다음 표에는 각 로그 유형의 서로 다른 특성이 요약되어 있습니다.

표 ***111:*** 로그 유형 비교

						Contains(포함**)**								
	트랜잭션	상태 비저장	텍스트로 기록됨	사서함 파일로 기록됨	이진으로 기록됨	주기적 상태 정보	메시지 수신 정보	전달 정보	개별 하드 반송	개별 소프트 반송	주입 SMTP 대화	헤더 기록	전달 SMTP 대화	구성 정보
메일 로그	•		•			•	•	•	•	•		•		
qmail 형식 전달 로그		•			•		•	•	•			•		
전달 로그		•			•		•	•	•			•		
반송 로그	•		•						•	•		•		
상태 로그		•	•			•								

						Contains(포함)								
Domain Debug Logs	•		•					•	•	•			•	
Injection Debug Logs	•		•				•				•			
시스템 로그	•		•			•								
CLI 감사 로그	•		•			•								
FTP 서버 로그	•		•			•								
HTTP 로그	•		•			•								
NTP 로그	•		•			•								
LDAP 로그	•		•											
안티스팸 로그	•		•			•								
Anti-Spam Archive				•										
그레이메일 엔진 로그	•		•			•								
그레이메일 아카이브				•										
안티바이러스 로그	•		•			•								
안티바이러스 아카이브				•										

						Contains(포함)								
AMP 엔진 로그	•		•			•								
AMP 아카이브				•										
Scanning Logs	•		•			•								•
스팸 격리	•		•			•								
스팸 격리 GUI	•		•			•								
허용 목록/차단 목록 로그	•		•			•								
보고 로그	•		•		•									
쿼리 보고 로그	•		•		•									
Updater Logs			•											
Tracking Logs	•				•	•	•	•	•	•		•		
인증 로그	•		•											
구성 기록 로그	•		•											•
API 로그	•		•											

로그 검색 방법

로그 파일은 다음과 같은 파일 전송 프로토콜 중 하나를 기반으로 검색할 수 있습니다. 로그 서브스크립션 프로세스 중에 GUI에서 또는 logconfig 명령을 통해 로그 서브스크립션을 만들거나 수정하면서 프로토콜을 설정합니다.

참고 특정 로그에서 log Push 메서드를 사용하는 경우, 해당 로그는 CLI를 통해 트러블슈팅하거나 검색하기 위해 로컬에서 사용할 수 없게 됩니다.

표 ***112:*** 로그 전송 프로토콜

수동으로 다운로드	이 방법을 사용하면 Log Subscriptions(로그 서브스크립션) 페이지에서 로그 디렉터리에 대한 링크를 클릭하고 액세스할 로그 파일을 클릭하여 언제든지 로그 파일에 액세스할 수 있습니다. 브라우저에 따라 브라우저 창에서 파일을 보거나, 텍스트 파일로 열거나 저장할 수 있습니다. 이 방법은 HTTP(S) 프로토콜을 사용하며 기본 검색 방법입니다. 참고 CLI에서 지정하더라도, 이 방법을 사용하면 클러스터의 컴퓨터에 대해서는 레벨(시스템, 그룹 또는 클러스터)과 상관없이 로그를 검색할 수 없습니다.
FTP Push	이 방법은 원격 컴퓨터의 FTP 서버로 로그 파일을 주기적으로 푸시합니다. 서브스크립션에는 사용자 이름, 암호, 원격 컴퓨터의 대상 디렉터리가 필요합니다. 사용자가 설정한 롤오버 일정을 기반으로 로그 파일이 전송됩니다.
SCP Push	이 방법은 원격 컴퓨터의 SCP 서버로 로그 파일을 주기적으로 푸시합니다. 이 방법을 사용하려면 SSH1 또는 SSH2 프로토콜을 사용하는 원격 컴퓨터에 SSH SCP 서버가 있어야 합니다. 서브스크립션에는 사용자 이름, SSH 키, 원격 컴퓨터의 대상 디렉터리가 필요합니다. 사용자가 설정한 롤오버 일정을 기반으로 로그 파일이 전송됩니다.
Syslog Push	이 방법은 원격 syslog 서버로 로그 메시지를 전송합니다. 이 방법은 RFC 3164를 준수합니다. Syslog 서버에 대한 호스트 이름을 제출하고 UDP 또는 TCP를 로그 전송에 사용하도록 선택해야 합니다. 사용되는 포트는 514입니다. 로그를 위한 기능(facility)을 선택해야 합니다. 그러나 로그 유형의 기본값이 드롭다운 메뉴에 미리 선택되어 있습니다. 텍스트 기반 로그만 syslog push를 사용하여 전송할 수 있습니다.

로그 파일 이름 및 디렉터리 구조

AsyncOS는 로그 서브스크립션 이름을 기반으로 각 로그 서브스크립션에 대한 디렉터리를 만듭니다. 디렉터리에서 로그 파일의 실제 이름은 사용자가 지정한 로그 파일 이름, 로그가 시작된 타임스탬프 및 단일 문자 상태 코드로 구성됩니다. 로그의 파일 이름은 다음 공식을 사용하여 만들어집니다.

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

상태 코드는 .current 또는 .s(saved를 의미함)일 수 있습니다. 저장된 상태의 로그 파일만 전송 또는 삭제할 수 있습니다.

로그 롤오버 및 전송 예약

로그 파일은 로그 서브스크립션으로 만들어지고, 도달하는 첫 번째 사용자 지정 조건(최대 파일 크기 또는 예약된 롤오버)을 기반으로 롤오버(푸시 기반 검색 옵션을 선택한 경우 전송)됩니다. 최대 파일 크기 및 예약된 롤오버용 간격을 구성하려면 CLI의 logconfig 명령 또는 GUI의 Log Subscriptions(로그 서브스크립션) 페이지를 사용합니다. 또한 선택한 로그 서브스크립션을 롤오버하려면 GUI의 **Rollover Now(**지금 롤오버**)** 버튼 또는 CLI의 rollovernow 명령을 사용할 수 있습니다. 롤오버 예약에 대한 자세한 내용은 로그 서브스크립션 롤오버, 1109 페이지 섹션을 참조하십시오.

수동 다운로드를 사용하여 검색한 로그는 지정한 최대 수에 도달할 때까지(기본값은 파일 10개) 또는 시스템에 로그 파일을 위한 공간이 더 필요할 때까지 저장됩니다.

기본적으로 활성화된 로그

Email Security Appliance는 기본적으로 활성화된 많은 로그 서브스크립션에 의해 미리 구성됩니다(다른 로그는 사용자가 적용한 라이센스 키에 따라 구성될 수 있음). 기본적으로 검색 방법은 "Manually Download(수동으로 다운로드)"입니다.

미리 구성된 모든 로그 서브스크립션은 로그 레벨이 3입니다. 단, error_logs는 1로 설정되어 있어 오류만 포함됩니다. 자세한 내용은 로그 레벨, 1106 페이지를 참조하십시오. 새 로그 서브스크립션 만들기 또는 기존 로그 서브스크립션 수정에 대한 자세한 내용은 로그 서브스크립션, 1105 페이지 섹션을 참조하십시오.

로그 유형

- 허용 목록/차단 목록 로그 사용, 1097 페이지
- 보고 로그 사용, 1098 페이지
- 보고 쿼리 로그 사용, 1099 페이지
- 업데이트 로그 사용, 1100 페이지
- 추적 로그 이해, 1101 페이지
- 인증 로그 사용, 1102 페이지
- 구성 기록 로그 사용, 1103 페이지
- 외부 위협 피드 엔진 로그 사용, 1104 페이지

로그 파일의 타임스탬프

다음 로그 파일에는 로그 자체의 시작 날짜와 종료 날짜, AsyncOS의 버전 및 GMT 오프셋(초 단위로 제공, 로그의 시작 부분에만)이 포함됩니다.

- 안티바이러스 로그
- LDAP 로그
- 시스템 로그
- 메일 로그

텍스트 메일 로그 사용

텍스트 메일 로그는 이메일 수신, 이메일 전달 및 반송의 세부사항을 포함합니다. 이러한 로그는 특정 메시지의 전달을 이해하고 시스템 성능을 분석하는 데 유용한 정보 소스입니다.

여기에는 특별한 구성이 필요하지 않습니다. 그러나 첨부 파일 이름을 보려면 시스템을 적절히 구성해야 합니다. 첨부 파일 이름은 항상 기록되지는 않을 수 있습니다. 자세한 내용은 메시지 추적 활성화, 837 페이지 및 메시지 추적 개요 , 837 페이지 섹션을 참조하십시오.

다음 표는 텍스트 메일 로그에 표시되는 정보를 보여줍니다.

표 ***113:*** 텍스트 메일 로그 상태

통계	설명
ICID	Injection Connection ID. 개별 SMTP의 시스템 연결에 대한 숫자 식별자입니다. 이를 통해 1~1000의 개별 메시지가 전송될 수 있습니다.
DCID	Delivery Connection ID. 1~1000개 메시지 전달을 위한 개별 SMTP의 또 다른 서버 연결에 대한 숫자 식별자입니다. 각각의 경우 단일 메시지 전송에서 RID의 일부 또는 전체가 전달됩니다.
RCID	RPC Connection ID. 개별 RPC의 스팸 격리 연결에 대한 숫자 식별자입니다. 스팸 격리를 드나드는 메시지 추적에 사용됩니다.
MID	Message ID. 로그를 통해 흐르는 메시지 추적에 사용됩니다.
RID	Recipient ID. 각 메시지 수신자에게 ID가 할당됩니다.

통계	설명
New	새 연결이 시작되었습니다.
Start	새 메시지가 시작되었습니다.

텍스트 메일 로그 해석

다음 샘플을 로그 파일 해석을 위한 가이드로 사용하십시오.

참고 로그 파일의 각 줄에 번호가 매겨지지는 않습니다. 샘플의 편의상 여기에서만 번호를 매긴 것입니다.

표 ***114:*** 텍스트 메일 로그 세부사항

1	`Mon Apr 17 19:56:22 2003 Info:`
	`New SMTP ICID 5 interface Management (10.1.1.1)`
	`address 10.1.1.209 reverse dns host remotehost.com verified yes`

2	`Mon Apr 17 19:57:20 2003 Info:` `Start MID 6 ICID 5`
3	`Mon Apr 17 19:57:20 2003 Info:` `MID 6 ICID 5 From: <sender@remotehost.com>`
4	`Mon Apr 17 19:58:06 2003 Info:` `MID 6 ICID 5 RID 0 To: <mary@yourdomain.com>`
5	`Mon Apr 17 19:59:52 2003 Info:` `MID 6 ready 100 bytes from <sender@remotehost.com>`
6	`Mon Apr 17 19:59:59 2003 Info: ICID 5 close`
7	`Mon Mar 31 20:10:58 2003 Info:` `New SMTP DCID 8 interface 192.168.42.42 address 10.5.3.25`
8	`Mon Mar 31 20:10:58 2003 Info:` `Delivery start DCID 8 MID 6 to RID [0]`
9	`Mon Mar 31 20:10:58 2003 Info:` `Message done DCID 8 MID 6 to RID [0]`
10	`Mon Mar 31 20:11:03 2003 Info: DCID 8 close`

다음 표를 위 로그 파일을 읽기 위한 가이드로 사용하십시오.

표 ***115:*** 텍스트 메일 로그 세부사항 예

라인 번호	설명
1	시스템에 대한 새 연결이 시작되고 ICID(Injection ID) "5"가 할당됩니다. 연결이 Management IP 인터페이스에서 수신되었고 10.1.1.209의 원격 호스트에서 시작되었습니다.
2	MAIL FROM 명령이 실행된 후 메시지에 MID(Message ID) "6"이 할당되었습니다.
3	발신자 주소가 식별 및 수락됩니다.
4	수신자가 식별되고 RID(Recipient ID) "0"이 할당됩니다.
5	MID 5가 수락되고 디스크에 기록되고 인식됩니다.
6	수신에 성공하고 수신 연결이 종료됩니다.
7	그런 다음 메시지 전달 프로세스가 시작됩니다. 192.168.42.42에서 10.5.3.25로 DCID(Delivery Connection ID) "8"이 할당됩니다.
8	RID "0"으로 메시지 전달이 시작됩니다.
9	MID 6의 RID "0"에 대한 전달이 성공합니다.
10	전달 연결이 종료됩니다.

텍스트 메일 로그 항목의 예

다음은 다양한 상황을 기반으로 한 몇 가지 샘플 로그 항목입니다.

메시지 주입 및 전달

단일 수신자에 대한 메시지가 Email Security Appliance에 주입됩니다. 메시지가 성공적으로 전달됩니다.

```
Wed Jun 16 21:42:34 2004 Info: New SMTP ICID 282204970 interface mail.example.com
(1.2.3.4) address 2.3.4.5 reverse dns host unknown verified no

Wed Jun 16 21:42:34 2004 Info: ICID 282204970 SBRS None

Wed Jun 16 21:42:35 2004 Info: Start MID 200257070 ICID 282204970

Wed Jun 16 21:42:35 2004 Info: MID 200257070 ICID 282204970 From: <someone@foo.com>

Wed Jun 16 21:42:36 2004 Info: MID 200257070 ICID 282204970 RID 0 To: <user@example.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Message-ID
'<37gva9$5uvbhe@mail.example.com>'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 Subject 'Hello'

Wed Jun 16 21:42:38 2004 Info: MID 200257070 ready 24663 bytes from <someone@foo.com>

Wed Jun 16 21:42:38 2004 Info: MID 200257070 antivirus negative
```

```
Wed Jun 16 21:42:38 2004 Info: MID 200257070 queued for delivery

Wed Jun 16 21:42:38 2004 Info: New SMTP DCID 2386069 interface 1.2.3.4 address 1.2.3.4

Wed Jun 16 21:42:38 2004 Info: Delivery start DCID 2386069 MID 200257070 to RID [0]

Wed Jun 16 21:42:38 2004 Info: ICID 282204970 close

Wed Jun 16 21:42:38 2004 Info: Message done DCID 2386069 MID 200257070 to RID [0]
[('X-SBRS', 'None')]

Wed Jun 16 21:42:38 2004 Info: MID 200257070 RID [0] Response 2.6.0
<37gva9$5uvbhe@mail.example.com> Queued mail for delivery

Wed Jun 16 21:42:43 2004 Info: DCID 2386069 close
```

메시지 전달 성공

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

메시지 전달 실패(하드 반송)

수신자가 2명인 메시지가 Email Security Appliance에 주입됩니다. 전달 시 대상 호스트가 둘 중 한 수신자에게 메시지를 전달할 수 없음을 나타내는 5XX 오류를 반환합니다. 어플라이언스는 발신자에게 알리고 대기열에서 수신자를 제거합니다.

```
Mon Mar 31 20:00:23 2003 Info: New SMTP DCID 3 interface 172.19.0.11 address
64.81.204.225

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 0 - 5.1.0 - Unknown address
error ('550', ['<george@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:27 2003 Info: Bounced: DCID 3 MID 4 to RID 1 - 5.1.0 - Unknown address
error ('550', ['<jane@yourdomain.com>... Relaying denied']) []
Mon Mar 31 20:00:32 2003 Info: DCID 3 close
```

소프트 반송 후 전달 성공

메시지가 Email Security Appliance에 주입됩니다. 첫 번째 전달 시도에서 메시지가 소프트 반송되고 향후 전달을 위해 대기열에 추가됩니다. 두 번째 시도에서 메시지가 성공적으로 전달됩니다.

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:00:23 2003 Info: Delivery start DCID 3 MID 4 to RID [0, 1]

Mon Mar 31 20:00:23 2003 Info: Delayed: DCID 5 MID 4 to RID 0 - 4.1.0 - Unknown address
error ('466', ['Mailbox temporarily full.'])[]

Mon Mar 31 20:00:23 2003 Info: Message 4 to RID [0] pending till Mon Mar 31 20:01:23
2003
```

```
Mon Mar 31 20:01:28 2003 Info: DCID 5 close

Mon Mar 31 20:01:28 2003 Info: New SMTP DCID 16 interface PublicNet address 172.17.0.113

Mon Mar 31 20:01:28 2003 Info: Delivery start DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:28 2003 Info: Message done DCID 16 MID 4 to RID [0]

Mon Mar 31 20:01:33 2003 Info: DCID 16 close
```

scanconfig 명령에 대한 메시지 검사 결과

메시지를 구성 요소 부분으로 분해할 수 없을 때(첨부 파일 제거 시) 시스템 동작을 결정하려면 scanconfig 명령을 사용할 수 있습니다. 옵션은 Deliver, Bounce 또는 Drop입니다.

다음 예는 scanconfig가 Deliver로 설정된 텍스트 메일 로그를 보여줍니다.

```
Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 From: <test@virus.org>

Tue Aug 3 16:36:29 2004 Info: MID 256 ICID 44784 RID 0 To: <joe@example.com>

Tue Aug 3 16:36:29 2004 Info: MID 256 Message-ID '<137398.@virus.org>'

Tue Aug 3 16:36:29 2004 Info: MID 256 Subject 'Virus Scanner Test #22'

Tue Aug 3 16:36:29 2004 Info: MID 256 ready 1627 bytes from <test@virus.org>

Tue Aug 3 16:36:29 2004 Warning: MID 256, Message Scanning Problem: Continuation line
seen before first header


Tue Aug 3 16:36:29 2004 Info: ICID 44784 close

Tue Aug 3 16:36:29 2004 Info: MID 256 antivirus positive 'EICAR-AV-Test'

Tue Aug 3 16:36:29 2004 Info: Message aborted MID 256 Dropped by antivirus

Tue Aug 3 16:36:29 2004 Info: Message finished MID 256 done
```

다음 예는 scanconfig가 drop으로 설정된 텍스트 메일 로그를 보여줍니다.

```
Tue Aug 3 16:38:53 2004 Info: Start MID 257 ICID 44785

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 From: test@virus.org

Tue Aug 3 16:38:53 2004 Info: MID 257 ICID 44785 RID 0 To: <joe@example.com>
Tue Aug 3 16:38:53 2004 Info: MID 257 Message-ID '<392912.@virus.org>'
Tue Aug 3 16:38:53 2004 Info: MID 25781 Subject 'Virus Scanner Test #22'
Tue Aug 3 16:38:53 2004 Info: MID 257 ready 1627 bytes from <test@virus.org>
Tue Aug 3 16:38:53 2004 Warning: MID 257, Message Scanning Problem: Continuation line
seen before first header
Tue Aug 3 16:38:53 2004 Info: Message aborted MID 25781 Dropped by filter 'drop_zip_c'
Tue Aug 3 16:38:53 2004 Info: Message finished MID 257 done
Tue Aug 3 16:38:53 2004 Info: ICID 44785 close
```

첨부 파일이 있는 메시지

이 예에서는 첨부 파일 이름 식별을 활성화하기 위해 "Message Body Contains" 조건의 콘텐츠 필터가 구성되었습니다.

```
Sat Apr 23 05:05:42 2011 Info: New SMTP ICID 28 interface Management (192.0.2.10)
address 224.0.0.10 reverse dns host test.com verified yes

Sat Apr 23 05:05:42 2011 Info: ICID 28 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0]
SBRS 0.0

Sat Apr 23 05:05:42 2011 Info: Start MID 44 ICID 28
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 From: <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 ICID 28 RID 0 To: <recipient1@example.org>
Sat Apr 23 05:05:42 2011 Info: MID 44 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Sat Apr 23 05:05:42 2011 Info: MID 44 Subject 'Message 001'
Sat Apr 23 05:05:42 2011 Info: MID 44 ready 240129 bytes from <sender1@example.com>
Sat Apr 23 05:05:42 2011 Info: MID 44 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Sat Apr 23 05:05:42 2011 Info: ICID 28 close
Sat Apr 23 05:05:42 2011 Info: MID 44 interim verdict using engine: CASE
spam negative
Sat Apr 23 05:05:42 2011 Info: MID 44 using engine: CASE spam negative
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Banner.gif'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment '=D1=82=D0=B5=D1=81=D1=82.rst'
Sat Apr 23 05:05:43 2011 Info: MID 44 attachment 'Test=20Attachment.docx'
Sat Apr 23 05:05:43 2011 Info: MID 44 queued for delivery
```

세 첨부 파일 중 두 번째는 유니코드입니다. 유니코드를 표시할 수 없는 터미널에서는 이러한 첨부 파일이 QP(quoted-printable) 형식으로 표시됩니다.

DANE 지원을 통한 메시지 전달 성공

단일 수신자에 대한 메시지가 어플라이언스에 도달합니다. 어플라이언스는 DNS 서버에서 보안 DNS MX 레코드, DNS A 레코드 및 TLSA 레코드를 요청합니다. DANE를 "Mandatory"로 선택하면 수신자 도메인의 x.509 인증서 값과 비교하여 TLSA 레코드가 검증됩니다. TLSA 레코드 검증에 성공하면 수신자에게 메시지가 전달됩니다.

```
Tue Nov 13 12:13:33 2018 Debug: Trying DANE MANDATORY for example.org
Tue Nov 13 12:13:33 2018 Debug: SECURE MX record(mail.example.org) found for example.org
Tue Nov 13 12:13:33 2018 Debug: DNS query: Q('mail.example.org', 'CNAME')
Tue Nov 13 12:13:33 2018 Debug: DNS query: QN('mail.example.org', 'CNAME',
'recursive_nameserver0.parent')
Tue Nov 13 12:13:33 2018 Debug: DNS query: QIP  ('mail.example.org','CNAME','8.8.8.8',60)
Tue Nov 13 12:13:33 2018 Debug: DNS query: Q  ('mail.example.org', 'CNAME', '8.8.8.8')
Tue Nov 13 12:13:34 2018 Debug: DNSSEC Response data([], , 0, 1799)
Tue Nov 13 12:13:34 2018 Debug: Received NODATA for domain mail.example.org type CNAME
Tue Nov 13 12:13:34 2018 Debug: No CNAME record(NoError) found for domain(mail.example.org)
Tue Nov 13 12:13:34 2018 Debug: SECURE A record (4.31.198.44) found for
MX(mail.example.org) in example.org
Tue Nov 13 12:13:34 2018 Info: New SMTP DCID 92 interface 10.10.1.191 address 4.31.198.44
port 25
Tue Nov 13 12:13:34 2018 Info: ICID 13 lost
Tue Nov 13 12:13:34 2018 Info: ICID 13 close
Tue Nov 13 12:13:34 2018 Debug: DNS query: Q('_25._tcp.mail.example.org', 'TLSA')
Tue Nov 13 12:13:34 2018 Debug: DNS query: QN('_25._tcp.mail.example.org', 'TLSA',
'recursive_nameserver0.parent')
Tue Nov 13 12:13:34 2018 Debug: DNS query: QIP
('_25._tcp.mail.example.org','TLSA','8.8.8.8',60)
Tue Nov 13 12:13:34 2018 Debug: DNS query: Q  ('_25._tcp.mail.example.org', 'TLSA', '8.8.8.8')
Tue Nov 13 12:13:35 2018 Debug: DNSSEC Response data(['0301010c72ac70b745ac19998811b13
1d662c9ac69dbdbe7cb23e5b514b56664c5d3d6'], secure, 0, 1799)
Tue Nov 13 12:13:35 2018 Debug: DNS encache (_25._tcp.mail.example.org, TLSA,
[(2550119024205761L, 0,
'SECURE', '0301010c72ac70b745ac19998811b131d662c9ac69dbdbe7cb23e5b514b56664c5d3d6')])
```

```
Tue Nov 13 12:13:35 2018 Debug: SECURE TLSA Record found for MX(mail.example.org) in
example.org
Tue Nov 13 12:13:36 2018 Info: DCID 92 Certificate verification successful
Tue Nov 13 12:13:36 2018 Info: DCID 92 TLS success protocol TLSv1.2 cipher
Tue Nov 13 12:13:36 2018 Info: DCID 92 TLS success protocol TLSv1.2 cipher
ECDHE-RSA-AES256-GCM-SHA384 for example.org
Tue Nov 13 12:13:36 2018 Info: Delivery start DCID 92 MID 23 to RID [0]
```

인증서 확인 실패로 인한 메시지 전달 실패

단일 수신자에 대한 메시지가 어플라이언스에 도달합니다. 어플라이언스는 DNS 서버에서 보안 DNS MX 레코드, DNS A 레코드 및 TLSA 레코드를 요청합니다. DANE를 "Mandatory"로 선택하면 수신자 도메인의 x.509 인증서 값과 비교하여 TLSA 레코드가 검증됩니다. 인증서 확인에 실패하면 메시지는 나중에 전달됩니다. 보안 TLSA 레코드를 찾을 수 없는 경우 메시지는 반송됩니다.

```
Wed Nov 14 05:52:08 2018 Debug: DNS query: QN('server1.example.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 05:52:08 2018 Debug: DNS query: QIP
('server1.example.net','CNAME','10.10.2.184',60)
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q  ('server1.example.net', 'CNAME', '10.10.2.184')
Wed Nov 14 05:52:08 2018 Debug: DNSSEC Response data([], , 0, 284)
Wed Nov 14 05:52:08 2018 Debug: Received NODATA for domain server1.example.net type CNAME
Wed Nov 14 05:52:08 2018 Debug: No CNAME record(NoError) found for domain(server1.example.net)
Wed Nov 14 05:52:08 2018 Debug: Secure CNAME(server1.example.net) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Debug: SECURE A record (10.10.1.198) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Info: New SMTP DCID 102 interface 10.10.1.191 address 10.10.1.198
 port 25
Wed Nov 14 05:52:08 2018 Debug: Fetching TLSA records with CNAME(server1.example.net) for
MX(someone.cs2.example.net) in example.net
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q('_25._tcp.server1.example.net', 'TLSA')
Wed Nov 14 05:52:08 2018 Debug: SECURE TLSA Record found for MX(server1.example.net) in
example.net
Wed Nov 14 05:52:08 2018 Debug: DCID 102 All TLSA records failed for certificate not trusted
Wed Nov 14 05:52:08 2018 Debug: Fetching TLSA records with initial
name(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Debug: DNS query: Q('_25._tcp.someone.cs2.example.net', 'TLSA')
Wed Nov 14 05:52:08 2018 Debug: SECURE TLSA Record found for MX(someone.cs2.example.net)
in example.net
Wed Nov 14 05:52:08 2018 Info: DCID 102 Certificate verification successful
Wed Nov 14 05:52:08 2018 Info: DCID 102 TLS success protocol TLSv1.2 cipher
DHE-RSA-AES128-SHA256
for example.net
Wed Nov 14 05:52:08 2018 Info: Delivery start DCID 102 MID 26 to RID [0]
Wed Nov 14 05:52:08 2018 Info: Message done DCID 102 MID 26 to RID [0]
Wed Nov 14 05:52:08 2018 Info: MID 26 RID [0] Response 'ok:  Message 31009 accepted'
Wed Nov 14 05:52:08 2018 Info: Message finished MID 26 done

Wed Nov 14 06:36:22 2018 Debug: Trying DANE MANDATORY for example.net
Wed Nov 14 06:36:22 2018 Debug: SECURE MX record(someone.cs2.example.net) found for
example.net
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q('someone.cs2.example.net', 'CNAME')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QN('someone.cs2.example.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QIP
('someone.cs2.example.net','CNAME','10.10.2.184',60)
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q  ('someone.cs2.example.net', 'CNAME',
'10.10.2.184')
Wed Nov 14 06:36:22 2018 Debug: DNSSEC Response data(['mail.example2.net.'], secure, 0,
```

```
3525)
Wed Nov 14 06:36:22 2018 Debug: DNS encache (someone.cs2.example.net, CNAME,
[(2692348132363369L, 0,
'SECURE', 'mail.example2.net')])
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q('mail.example2.net', 'CNAME')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QN('mail.example2.net', 'CNAME',
'recursive_nameserver0.parent')
Wed Nov 14 06:36:22 2018 Debug: DNS query: QIP  ('mail.example2.net','CNAME','10.10.2.184',60)
Wed Nov 14 06:36:22 2018 Debug: DNS query: Q  ('mail.example2.net', 'CNAME', '10.10.2.184')
Wed Nov 14 06:36:22 2018 Debug: DNSSEC Response data([], , 0, 225)
Wed Nov 14 06:36:22 2018 Debug: Received NODATA for domain mail.example2.net type CNAME
Wed Nov 14 06:36:22 2018 Debug: No CNAME record(NoError) found for domain(mail.example2.net)
Wed Nov 14 06:36:22 2018 Debug: Secure CNAME(mail.example2.net) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 06:36:22 2018 Debug: INSECURE A record (10.10.1.197) found for
MX(someone.cs2.example.net)
in example.net
Wed Nov 14 06:36:22 2018 Debug: Fetching TLSA records with initial
name(someone.cs2.example.net) in example.net
Wed Nov 14 06:36:22 2018 Info: New SMTP DCID 104 interface 10.10.1.191 address 10.10.1.197
 port 25
Wed Nov 14 06:36:36 2018 Debug: DNS query: Q('_25._tcp.someone.cs2.example.net', 'TLSA')
Wed Nov 14 06:36:36 2018 Debug: SECURE TLSA Record found for MX(someone.cs2.example.net)
in example.net
Wed Nov 14 06:36:36 2018 Debug: DCID 104 All TLSA records failed for certificate not trusted
Wed Nov 14 06:36:36 2018 Info: MID 27 DCID 104 DANE failed for the domain example.net:
DANE Certificate verification failed
Wed Nov 14 06:36:36 2018 Info: Failed for all MX hosts in example.net
```

잘못된 **TLSA** 레코드로 인한 메시지 전달 실패

단일 수신자에 대한 메시지가 어플라이언스에 도달합니다. 어플라이언스는 DNS 서버에서 보안 DNS MX 레코드, DNS A 레코드 및 TLSA 레코드를 요청합니다. DANE를 "Mandatory"로 선택하면 수신자 도메인의 x.509 인증서 값과 비교하여 TLSA 레코드가 검증됩니다. 잘못된 TLSA 레코드가 발견되면 나중에 메시지 전달을 시도하거나 메시지가 반송됩니다.

```
Tue Aug 7 05:15:18 2018 Debug: Trying DANE MANDATORY for example-dane.net
Tue Aug 7 05:15:18 2018 Debug: SECURE MX record (someone.example-dane.net) found for
test-tlsabogus.net
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('someone.example-dane.net', 'CNAME')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QN ('someone.example-dane.net', 'CNAME',
'recursive_nameserver0.parent')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QIP
('someone.example-dane.net','CNAME','10.10.2.183', 60)
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('someone.example-dane.net', 'CNAME',
'10.10.2.183')
Tue Aug 7 05:15:18 2018 Debug: DNSSEC Response data ([], , 0, 300)
Tue Aug 7 05:15:18 2018 Debug: SECURE A record (10.10.1.198) found for MX
(someone.example-dane.net)
in example-dane.net
Tue Aug 7 05:15:18 2018 Info: ICID 32 close
Tue Aug 7 05:15:18 2018 Info: New SMTP DCID 61 interface 10.10.1.194 address 10.10.1.198
port 25
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('_25._tcp.someone.example-dane.net', 'TLSA')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QN ('_25._tcp.someone.example-dane.net', 'TLSA',

'recursive_nameserver0.parent')
Tue Aug 7 05:15:18 2018 Debug: DNS query: QIP
('_25._tcp.someone.example-dane.net','TLSA','10.10.2.183', 60)
Tue Aug 7 05:15:18 2018 Debug: DNS query: Q ('_25._tcp.someone.example-dane.net', 'TLSA',
'10.10.2.183')
Tue Aug 7 05:15:18 2018 Debug: DNSSEC Response data
```

```
(['03010160b3f16867357cdfef37bb6acd687af54f
225e3bfa945e1d37bfd37bd4eb6020'], bogus, 0, 60)
Tue Aug 7 05:15:18 2018 Debug: DNS encache (_25._tcp.someone.example-dane.net, TLSA,
[(11065394975822091L,
 0, 'BOGUS', '03010160b3f16867357cdfef37bb6acd687af54f225e3bfa945e1d37bfd37bd4eb6020')])
Tue Aug 7 05:15:18 2018 Debug: BOGUS TLSA Record is found for MX (someone.example-dane.net)

in example-dane.net
Tue Aug 7 05:15:18 2018 Debug: Trying next MX record in example-dane.net
Tue Aug 7 05:15:18 2018 Info: MID 44 DCID 61 DANE failed: TLSA record BOGUS
Tue Aug 7 05:15:18 2018 Debug: Failed for all MX hosts in example-dane.net
```

TLSA 레코드를 찾을 수 없어 편의적 TLS로 롤백

단일 수신자에 대한 메시지가 어플라이언스에 도달합니다. 어플라이언스는 DNS 서버에서 보안 DNS MX 레코드, DNS A 레코드 및 TLSA 레코드를 요청합니다. DANE를 "Opportunistic"으로 선택하면 수신자 도메인의 x.509 인증서 값과 비교하여 TLSA 레코드가 검증됩니다. 수신자의 도메인에 대해 TLSA 레코드를 찾을 수 없는 경우 SMTP 대화를 암호화하는 데 더 적합한 TLS가 사용됩니다.

```
Wed Sep 12 06:51:32 2018 Debug: Trying DANE OPPORTUNISTIC for example-dane.com
Wed Sep 12 06:51:32 2018 Debug: SECURE MX record (mx.example-dane.com) found for
digitalhellion.com
Wed Sep 12 06:51:32 2018 Debug: DNS query: Q ('mx.example-dane.com', 'CNAME')
Wed Sep 12 06:51:32 2018 Debug: DNS query: QN ('mx.example-dane.com', 'CNAME',
'recursive_nameserver0.parent')
Wed Sep 12 06:51:32 2018 Debug: DNS query: QIP ('mx.example-dane.com', 'CNAME','8.8.8.8',60)
Wed Sep 12 06:51:32 2018 Debug: DNS query: Q ('mx.example-dane.com', 'CNAME', '8.8.8.8')
Wed Sep 12 06:51:32 2018 Debug: DNSSEC Response data ([], , 0, 1799)
Wed Sep 12 06:51:32 2018 Debug: Received NODATA for domain mx.example-dane.com type CNAME
Wed Sep 12 06:51:32 2018 Debug: No CNAME record (NoError) found for domain
(mx.example-dane.com)
Wed Sep 12 06:51:32 2018 Debug: SECURE A record (162.213.199.115) found for MX
(mx.example-dane.com)
in example-dane.com
Wed Sep 12 06:51:32 2018 Info: ICID 1 lost
Wed Sep 12 06:51:32 2018 Info: ICID 1 close
Wed Sep 12 06:51:33 2018 Info: New SMTP DCID 2 interface 10.10.1.173 address 162.213.199.115
 port 25
Wed Sep 12 06:51:33 2018 Debug: DNS query: Q ('_25._tcp.mx.example-dane.com', 'TLSA')
Wed Sep 12 06:51:33 2018 Debug: DNS query: QN ('_25._tcp.mx.example-dane.com', 'TLSA',
'recursive_nameserver0.parent')
Wed Sep 12 06:51:33 2018 Debug: DNS query: QIP
('_25._tcp.mx.example-dane.com','TLSA','8.8.8.8', 60)
Wed Sep 12 06:51:33 2018 Debug: DNS query: Q ('_25._tcp.mx.example-dane.com', 'TLSA',
'8.8.8.8')
Wed Sep 12 06:51:34 2018 Debug: DNSSEC Response data ([], , 3, 1798)
Wed Sep 12 06:51:34 2018 Debug: Received NXDomain for domain _25._tcp.mx.example-dane.com'
 type TLSA
Wed Sep 12 06:51:34 2018 Debug: No TLSA record (NXDomain) found for MX (mx.example-dane.com)
Wed Sep 12 06:51:34 2018 Debug: Falling back to conventional TLS for MX (mx.example-dane.com)

in example-dane.com
Wed Sep 12 06:51:34 2018 Info: MID 1 DCID 2 DANE failed for the domain example-dane.com:
No TLSA Record
Wed Sep 12 06:51:34 2018 Info: DCID 2 TLS success protocol TLSv1.2 cipher
ECDHE-RSA-AES256-GCM-SHA384
Wed Sep 12 06:51:35 2018 Info: Delivery start DCID 2 MID 1 to RID [0]
```

발신자의 발신지 국가에 따라 수신된 메시지

이 예에서 로그에는 특정 발신자 그룹의 발신지 국가를 기준으로 수신된 메시지가 표시됩니다.

```
Thu Apr  6 06:50:18 2017 Info: ICID 73 ACCEPT SG WHITELIST match country[us] SBRS -10.0
country United States
```

메시지 첨부 파일의 최대 **URL**이 **URL** 스캔 제한을 초과함

이 예에서 로그는 URL 검사 제한을 초과한 메시지 첨부 파일의 URL 수를 표시합니다.

```
Wed Nov 8 13:35:48 2017 Info: MID 976 not completely scanned by SDS.
Error: The number of URLs in the message attachments exceeded the URL scan limit.
```

메시지 본문의 최대 **URL**이 **URL** 스캔 제한을 초과함

이 예에서 로그는 URL 검사 제한을 초과한 메시지 본문의 URL 수를 표시합니다.

```
Wed Nov 8 13:37:42 2017 Info: MID 976 not completely scanned by SDS.
Error: The number of URLs in the message body exceeded the URL scan limit.
```

악성 단축 **URL**이 **Cisco** 프록시 서버로 리디렉션됨

이 예에서 로그는 URL 평판 점수가 -3인 악성으로 표시된 단축 URl를 표시하며 Cisco Security Proxy 서버로 리디렉션됩니다.

```
Tue Nov 7 10:42:41 2017 Info: MID 9 having URL: http://ow.ly/Sb6O30fJvVn has been expanded
 to http://bit.ly/2frAl1x
Tue Nov 7 10:42:42 2017 Info: MID 9 having URL: http://bit.ly/2frAl1x has been expanded to
 http://thebest01.wayisbetter.cn/?cMFN
Tue Nov 7 10:42:42 2017 Info: MID 9 URL http://thebest01.wayisbetter.cn/?cMFN has reputation
 -3.854 matched Action: URL redirected to Cisco Security proxy
Tue Nov 7 10:42:42 2017 Info: MID 9 rewritten to MID 10 by
url-reputation-proxy-redirect-action filter 'aa'
```

메시지에서 단축 **URL**을 확장할 수 없음

이 예에서 로그는 메시지의 단축 URL을 실제 URL로 확장할 수 없다는 것을 보여 줍니다.

```
Mon Oct 30 10:58:59 2017 Info: MID 36 having URL: http://ow.ly/P0Kw30fVst3 has been expanded
 to http://bit.ly/2ymYWPR
Mon Oct 30 10:59:00 2017 Info: MID 36 having URL: http://bit.ly/2ymYWPR has been expanded
to http://ow.ly/cTS730fVssH
Mon Oct 30 10:59:01 2017 Info: MID 36 having URL: http://ow.ly/cTS730fVssH has been expanded
 to http://bit.ly/2xK8PD9
Mon Oct 30 10:59:01 2017 Info: MID 36 having URL: http://bit.ly/2xK8PD9 has been expanded
to http://ow.ly/lWOi30fVssl
Mon Oct 30 10:59:02 2017 Info: MID 36 having URL: http://ow.ly/lWOi30fVssl has been expanded
 to http://bit.ly/2ggHv9e
Mon Oct 30 10:59:03 2017 Info: MID 36 having URL: http://bit.ly/2ggHv9e has been expanded
to http://ow.ly/4fSO30fVsqx
Mon Oct 30 10:59:04 2017 Info: MID 36 having URL: http://ow.ly/4fSO30fVsqx has been expanded
 to http://bit.ly/2hKEFcW
Mon Oct 30 10:59:05 2017 Info: MID 36 having URL: http://bit.ly/2hKEFcW has been expanded
to http://ow.ly/NyH830fVsq6
Mon Oct 30 10:59:06 2017 Info: MID 36 having URL: http://ow.ly/NyH830fVsq6 has been expanded
 to http://bit.ly/2ysnsNi
Mon Oct 30 10:59:06 2017 Info: MID 36 having URL: http://bit.ly/2ysnsNi has been expanded
to http://ow.ly/JhUN30fVsnL
Mon Oct 30 10:59:07 2017 Info: MID 36 having URL: http://ow.ly/JhUN30fVsnL has been expanded
 to http://bit.ly/2hKQmAe
Mon Oct 30 10:59:07 2017 Info: MID 36 URL http://bit.ly/2hKQmAe is marked malicious due to
 : URL depth exceeded
Mon Oct 30 11:04:48 2017 Warning: MID 40 Failed to expand URL http://mail1.example.com/abcd
```

```
 Reason: Error while trying to retrieve expanded URL
Mon Oct 30 11:04:48 2017 Info: MID 40 not completely scanned for URL Filtering. Error:
Message has a shortened URL that could not be expanded
```

메시지 첨부 파일의 악성 **URL**에 대한 로그 항목

이 예에서 로그는 평판 점수가 -9.5인 악성 메시지 첨부 파일에 있는 URL을 표시합니다.

```
Mon Nov 6 06:50:18 2017 Info: MID 935 Attachment file_1.txt URL http://jrsjvysq.net has
reputation -9.5 matched
Condition: URL Reputation Rule
```

추출 오류로 인해 **Unscannable(**스캔 불가**)**로 표시된 메시지

이 예에서는 첨부 파일 추출 오류로 인해 콘텐츠 스캐너에서 검사하지 않는 메시지를 로그에 표시합니다.

```
Tue Oct 24 08:28:58 2017 Info: Start MID 811 ICID 10
Tue Oct 24 08:28:58 2017 Info: MID 811 ICID 10 From: <sender@example.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 ICID 10 RID 0 To: <recipient@example.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 Message-ID '<example@cisco.com>'
Tue Oct 24 08:28:58 2017 Info: MID 811 Subject 'Test mail'
Tue Oct 24 08:28:58 2017 Info: MID 811 ready 5242827 bytes from <user2@sender.com>
Tue Oct 24 08:28:58 2017 Info: MID 811 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Tue Oct 24 08:28:59 2017 Info: MID 811 attachment 'gzip.tar.gz'
Tue Oct 24 08:28:59 2017 Info: MID 811 was marked as unscannable due to extraction failures.
 Reason: Error in extraction process - Decoding Errors.
Tue Oct 24 08:28:59 2017 Info: ICID 10 close
Tue Oct 24 08:28:59 2017 Info: MID 811 quarantined to "Policy" (Unscannable: due to Extraction
 Failure)
Tue Oct 24 08:28:59 2017 Info: Message finished MID 811 done
```

RFC 위반으로 인해 **Unscannable(**스캔 불가**)**로 표시된 메시지

이 예에서는 RFC 위반으로 인해 콘텐츠 스캐너에서 검사하지 않는 메시지를 로그에 표시합니다.

```
Tue Oct 24 08:23:26 2017 Info: Start MID 807 ICID 6
Tue Oct 24 08:23:26 2017 Info: MID 807 ICID 6 From: <sender@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 ICID 6 RID 0 To: <recipient@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 Subject ‘Test Mail'
Tue Oct 24 08:23:26 2017 Info: MID 807 ready 427 bytes from <sender@example.com>
Tue Oct 24 08:23:26 2017 Info: MID 807 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Tue Oct 24 08:23:26 2017 Info: MID 807 was marked as unscannable due to an RFC violation.
Reason: A Unix-From header was found in the middle of a header block.
Tue Oct 24 08:23:26 2017 Info: MID 807 queued for delivery
Tue Oct 24 08:23:26 2017 Info: ICID 6 close
```

생성된 또는 재작성된 메시지를 위한 로그 항목

재작성/리디렉션 작업과 같은 일부 기능(alt-rcpt-to 필터, 안티스팸 rcpt 재작성, bcc() 작업, 안티바이러스 리디렉션 등)은 새 메시지를 생성합니다. 로그를 살펴보면서 결과를 확인하여 MID를 더 추가해야 할 수 있습니다(DCID도 필요할 수 있음). 항목은 다음과 같을 수 있습니다.

```
Tue Jun  1 20:02:16 2004 Info: MID 14 generated based on MID 13 by bcc filter 'nonetest'
```

또는

```
Tue Jan 6 15:03:18 2004 Info: MID 2 rewritten to 3 by antispam

Fri May 14 20:44:43 2004 Info: MID 6 rewritten to 7 by alt-rcpt-to-filter filter
'testfilt'
```

'rewritten' 항목에 대해 유의해야 할 흥미로운 점은, 로그에서 새 MID 사용을 나타내는 줄 뒤에 나타날 수 있다는 것입니다.

스팸 격리로 전송되는 메시지

메시지를 격리로 전송하면 메일 로그는 RPC 연결을 식별하기 위해 RCID(RPC connection ID)를 사용하여 격리로 드나드는 이동을 추적합니다. 다음 메일 로그에서 메시지는 스팸으로 태그가 지정되어 스팸 격리로 전송됩니다.

```
Wed Feb 14 12:11:40 2007 Info: Start MID 2317877 ICID 15726925

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 From: <HLD@chasehf.bfi0.com>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 ICID 15726925 RID 0 To:
<stevel@healthtrust.org>
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Message-ID
'<W1TH05606E5811BEA0734309D4BAF0.323.14460.pimailer44.DumpShot.2@email.chase.com>'
Wed Feb 14 12:11:40 2007 Info: MID 2317877 Subject 'Envision your dream home - Now make
it a reality'

Wed Feb 14 12:11:40 2007 Info: MID 2317877 ready 15731 bytes from <HLD@chasehf.bfi0.com>

Wed Feb 14 12:11:40 2007 Info: MID 2317877 matched all recipients for per-recipient
policy DEFAULT in the inbound table

Wed Feb 14 12:11:41 2007 Info: MID 2317877 using engine: CASE spam suspect

Wed Feb 14 12:11:41 2007 Info: EUQ: Tagging MID 2317877 for quarantine
Wed Feb 14 12:11:41 2007 Info: MID 2317877 antivirus negative
Wed Feb 14 12:11:41 2007 Info: MID 2317877 queued for delivery
Wed Feb 14 12:11:44 2007 Info: RPC Delivery start RCID 756814 MID 2317877 to local
IronPort Spam Quarantine


Wed Feb 14 12:11:45 2007 Info: EUQ: Quarantined MID 2317877

Wed Feb 14 12:11:45 2007 Info: RPC Message done RCID 756814 MID 2317877

Wed Feb 14 12:11:45 2007 Info: Message finished MID 2317877 done
```

외부 위협 피드 메일 로그의 예

메일 로그에는 수신 메시지에서 탐지된 위협 및 해당 메시지에 대해 수행된 작업에 대한 정보가 포함되어 있습니다. 대부분의 정보는 Info(정보) 또는 Debug(디버그) 수준입니다.

```
Thu Jun 7 20:48:10 2018 Info: MID 91 Threat feeds source 'S1' detected malicious URL:
'http://digimobil.mobi/' in attachment(s): malurl.txt. Action: Attachment stripped
```

SDR 필터링 로그 항목의 예

SDR 필터링 정보가 메일 로그에 게시됩니다. 대부분의 정보는 Info(정보) 또는 Debug(디버그) 수준입니다.

발신자 도메인 평판 인증 실패

이 예에서 로그는 SDR 서비스에 연결할 때의 인증 실패 때문에 SDR을 기준으로 필터링되지 않은 메시지를 표시합니다.

```
Mon Jul 2 08:57:18 2018 Info: New SMTP ICID 3 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 08:57:18 2018 Info: ICID 3 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS not enabled
 country not enabled
Mon Jul 2 08:57:18 2018 Info: Start MID 3 ICID 3
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 From: <sender1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 ICID 3 RID 0 To: <recipient1@example.com>
Mon Jul 2 08:57:18 2018 Info: MID 3 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>' Mon
 Jul 2 08:57:18 2018 Info: MID 3 Subject 'Message 001'
Mon Jul 2 08:57:19 2018 Info: MID 3 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Authentication failure.
```

해결책

CLI에서 `sdradvancedconfig` 명령을 사용하여 Cisco Email Security 게이트웨이를 SDR 서비스에 연결할 때 필요한 파라미터를 구성합니다.

발신인 도메인 평판 요청 시간 초과

이 예에서 로그는 SDR 서비스와 통신할 때의 요청 시간 초과 오류 때문에 SDR을 기준으로 필터링되지 않은 메시지를 표시합니다.

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com>
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Message 001'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Request timed out.
```

해결책

SDR 요청이 시간 초과되면 메시지가 검사 불가로 표시되고 구성된 작업이 메시지에 적용됩니다.

발신자 도메인 평판 잘못된 호스트

이 예에서 로그는 유효하지 않은 SDR 서비스 호스트가 Cisco Email Security 게이트웨이에 구성되어 있기 때문에 SDR을 기준으로 필터링되지 않은 메시지를 표시합니다.

```
Mon Jul 2 09:04:08 2018 Info: ICID 7 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS not enabled
 country not enabled
```

```
Mon Jul 2 09:04:08 2018 Info: Start MID 7 ICID 7
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 From: <sender1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 ICID 7 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:04:08 2018 Info: MID 7 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>' Mon
 Jul 2 09:04:08 2018 Info: MID 7 Subject 'Message 001'
Mon Jul 2 09:04:08 2018 Info: MID 7 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Invalid host configured.
```

해결책

CLI에서 `sdradvancedconfig` 명령을 사용하여 Cisco Email Security 게이트웨이를 SDR 서비스에 연결할 때 필요한 파라미터를 구성합니다.

발신인 도메인 평판 일반 오류

이 예에서 로그는 알 수 없는 오류 때문에 SDR을 기준으로 필터링되지 않은 메시지를 표시합니다.

```
Mon Jul 2 09:00:13 2018 Info: New SMTP ICID 4 interface Management (192.0.2.10) address
224.0.0.10 reverse dns host unknown verified no
Mon Jul 2 09:00:13 2018 Info: ICID 4 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS not enabled
 country not enabled
Mon Jul 2 09:00:13 2018 Info: Start MID 4 ICID 4
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 From: <sender1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 ICID 4 RID 0 To: <recipient1@example.com >
Mon Jul 2 09:00:13 2018 Info: MID 4 Message-ID '<000001cba32e$f24ff2e0$d6efd8a0$@com>'
Mon Jul 2 09:00:13 2018 Info: MID 4 Subject 'Test mail'
Mon Jul 2 09:00:13 2018 Info: MID 4 SDR: Message was not scanned for Sender Domain Reputation.
 Reason: Unknown error.
```

해결책

알 수 없는 오류가 발생하면 메시지가 검사 불가로 표시되고 구성된 작업이 메시지에 적용됩니다.

전달 로그 사용

전달 로그는 AsyncOS의 이메일 전달 작업에 대한 중요한 정보를 기록합니다. 로그 메시지는 "무상태(stateless)"입니다. 즉, 모든 관련 정보는 각 로그 메시지에 기록되며 사용자는 현재 전달 시도에 대한 정보의 이전 로그 메시지를 참조할 필요가 없습니다.

전달 로그는 각 수신자에 대한 이메일 전달 작업과 관련된 모든 정보를 기록합니다. Cisco에서 제공하는 유틸리티로 변환한 후에는 모든 정보가 논리적 방식으로, 사람이 읽을 수 있는 형태로 정돈됩니다. 변환 툴은 다음 사이트에서 이용할 수 있습니다. https://supportforums.cisco.com/document/33721/cisco-ironport-systems-contributed-tools

전달 로그는 리소스 효율성을 위해 이진 형식으로 기록 및 전송됩니다. 다음 표에서는 전달 로그에 기록되는 정보를 보여줍니다.

표 ***116:*** 전달 로그 통계

통계	설명
Delivery status	성공(메시지를 성공적으로 전달) 또는 반송(메시지가 하드 반송됨)
Del_time	전달 시간

통계	설명
Inj_time	Injection time. del_time - inj_time = 수신자 메시지가 대기열에 머무는 시간
Bytes	메시지 크기
Mid	메시지 ID
Ip	수신자 호스트 IP. 수신자 메시지를 수신 또는 반송한 호스트의 IP 주소
From	Envelope From(Envelope Sender 또는 MAIL FROM이라고도 함)
Source_ip	소스 호스트 IP. 수신 메시지 호스트의 IP 주소
코드	수신자 호스트에서의 SMTP 응답 코드
답글	수신자 호스트에서의 SMTP 응답 메시지
Rcpt Rid	수신자 ID. 수신자 ID는 <0>으로 시작되고, 여러 수신자가 있는 메시지에는 여러 수신자 ID가 있음
하려는 작업	Envelope To
시도	전달 시도 횟수

전달 상태가 반송이면 전달 로그에 다음과 같은 추가 정보가 나타납니다.

표 ***117:*** 전달 로그 반송 정보

통계	설명
이유	전달 도중 SMTP 응답의 RFC 1893 Enhanced Mail Status Code 해석
코드	수신자 호스트에서의 SMTP 응답 코드
오류	수신자 호스트에서의 SMTP 응답 메시지

logheaders를 설정한 경우(메시지 헤더 로깅, 1108 페이지 참조) 전달 정보 뒤에 헤더 정보가 나타납니다.

표 ***118:*** 전달 로그 헤더 정보

통계	설명
Customer_data	로깅된 헤더의 시작을 표시하는 XML 태그
헤더 이름	헤더의 이름
값	로깅된 헤더의 내용

전달 로그 항목의 예

이 섹션의 예는 다양한 전달 로그 항목을 보여줍니다.

메시지 전달 성공

```
Mon Mar 31 20:10:58 2003 Info: New SMTP DCID 5 interface 172.19.0.11 address
63.251.108.110

Mon Mar 31 20:10:58 2003 Info: Delivery start DCID 5 MID 4 to RID [0]

Mon Mar 31 20:10:58 2003 Info: Message done DCID 5 MID 4 to RID [0]

Mon Mar 31 20:11:03 2003 Info: DCID 5 close
```

전달 상태 반송

```
<bounce del_time="Sun Jan 05 08:28:33.073 2003" inj_time="Mon Jan 05 08:28:32.929 2003"

bytes="4074" mid="94157762" ip="0.0.0.0" from="campaign1@yourdomain.com"

source_ip="192.168.102.1 "reason="5.1.0 - Unknown address error" code="550"

error="["Requested action not taken: mailbox unavailable"]">


<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

</bounce>
```

Logheaders가 있는 전달 로그 항목

```
<success del_time="Tue Jan 28 15:56:13.123 2003" inj_time="Tue Jan 28 15:55:17.696 2003"
bytes="139" mid="202" ip="10.1.1.13" from="campaign1@yourdomain.com" source_ip="192.168.102.1"
 code="250" reply="sent">


<rcpt rid="0" to="user@sampledomain.com" attempts="1" />

<customer_data>

<header name="xname" value="sh"/>

</customer_data>

</success>
```

반송 로그 사용

반송 로그는 반송된 각 수신자와 관련된 모든 정보를 기록합니다. 다음 표에서는 반송 로그에 기록되는 정보를 보여줍니다.

표 ***119:*** 반송 로그 통계

통계	설명
타임스탬프	반송 이벤트의 시간
Log level	이 반송 로그에 있는 세부사항의 레벨
Bounce type	반송됨 또는 지연됨(예: 하드 반송 또는 소프트 반송)
MID/RID	Message ID 및 Recipient ID
From	Envelope From
하려는 작업	Envelope To
이유	전달 도중 SMTP 응답의 RFC 1893 Enhanced Mail Status Code 해석
응답	SMTP 응답 코드 및 수신자 호스트의 메시지

또한 **logheaders**의 로깅 또는 설정을 위해 메시지 크기를 지정한 경우(메시지 헤더 로깅, 1108 페이지 참고) 반송 정보 뒤에 메시지 및 헤더 정보가 나타납니다.

표 ***120:*** 반송 로그 헤더 정보

헤더	헤더 이름 및 헤더의 내용
메시지	로깅된 메시지의 내용

반송 로그 항목의 예

Soft-Bounced Recipient (Bounce Type = Delayed)

```
Thu Dec 26 18:37:00 2003 Info: Delayed: 44451135:0
From:<campaign1@yourdomain.com> To:<user@sampledomain.com>


Reason: "4.1.0 - Unknown address error" Response: "('451',
['<user@sampledomain.com> Automated block triggered by suspicious
activity from your IP address (10.1.1.1). Have your system administrator
send e-mail to postmaster@sampledomain.com if you believe this block is
in error'])"
```

Hard-Bounced Recipient (Bounce Type = Bounced)

```
Thu Dec 26 18:36:59 2003 Info: Bounced: 45346670:0 From:<campaign1@yourdomain.com>
To:<user2@sampledomain.com>


Reason: "5.1.0 - Unknown address error" Response: "('550', ['There is no such active
account.'])"
```

Bounce Log with Message Body and Logheaders

```
Wed Jan 29 00:06:30 2003 Info: Bounced: 203:0 From:<campaign1@yourdomain.com>
To:<user@sampledomain.com>


Reason:"5.1.2 - Bad destination host" Response: "('000', [])" Headers: ['xname:
userID2333']' Message: Message-Id:



<1u5jak$6b@yourdomain.com>\015\012xname: userID2333\015\012subject:
Greetings.\015\012\015\012Hi Tom:'
```

참고 텍스트 문자열 \015\012는 줄 바꿈을 나타냅니다(예: CRLF).

상태 로그 사용

상태 로그는 CLI status 명령(status, status detail, dnsstatus 포함)에서 발견되는 시스템 통계를 기록합니다. 기록 기간은 logconfig의 setup 하위 명령을 사용하여 설정합니다. 상태 로그에 보고되는 각 카운터 또는 점수는 카운터가 마지막으로 재설정된 이후의 값입니다.

상태 로그 읽기

다음 표는 상태 로그 레이블 및 일치하는 시스템 통계를 보여줍니다.

표 ***121:*** 상태 로그 통계

통계	설명
CPULd	CPU 사용률
DskIO	디스크 I/O 사용률
RAMUtil	RAM 사용률
QKUsd	Queue Kilobytes Used(사용된 대기열 킬로바이트)
QKFre	Queue Kilobytes Free(여유 대기열 킬로바이트)
CrtMID	메시지 ID(MID)
CrtICID	ICID(Injection Connection ID)
CRTDCID	DCID(Delivery Connection ID)
InjBytes	주입된 총 메시지 크기(바이트)
InjMsg	Injected Messages(주입된 메시지)
InjRcp	Injected Recipients(주입된 수신자)

통계	설명
GenBncRcp	생성된 바운스 수신인
RejRcp	거부된 수신자
DrpMsg	삭제(drop)된 메시지
SftBncEvnt	Soft Bounced Events
CmpRcp	완료된 수신자
HrdBncRcp	Hard Bounced Recipients
DnsHrdBnc	DNS 하드 바운스
5XXHrdBnc	5XX 하드 바운스
FltrHrdBnc	필터 하드 바운스
ExpHrdBnc	만료된 하드 바운스
OtrHrdBnc	기타 하드 바운스
DlvRcp	Delivered Recipients
DelRcp	삭제된 수신자
GlbUnsbHt	전역 가입 취소 횟수
ActvRcp	Active Recipients
UnatmptRcp	전달을 시도하지 않은 수신자
AtmptRcp	전달을 시도했던 수신자
CrtCncIn	현재 인바운드 연결
CrtCncOut	현재 아웃바운드 연결
DnsReq	DNS 요청
NetReq	네트워크 요청
CchHit	캐시 성공률
CchMis	캐시 실패
CchEct	캐시 예외 사항
CchExp	캐시 만료
CPUTTm	애플리케이션에서 사용한 총 CPU 시간

통계	설명
CPUETm	애플리케이션 시작 이후 경과 시간
MaxIO	메일 프로세스에 대한 초당 최대 디스크 I/O 작업
RamUsd	할당된 메모리(바이트)
SwIn	메모리 스왑 인
SwOut	메모리 스왑 아웃
SwPgIn	메모리 페이지 인
SwPgOut	메모리 페이지 아웃
MMLen	시스템에 있는 총 메시지 수
DstInMem	메모리에 있는 대상 개체의 수
ResCon	리소스 보존 타핏(tarpit) 값. 과중한 시스템 로드 때문에 수신 메일의 수락이 지정된 시간(초)만큼 지연됩니다.
WorkQ	현재 작업 대기열에 있는 메시지의 수
QuarMsgs	정책, 바이러스 또는 Outbreak 격리에 있는 개별 메시지의 수(여러 격리에 있는 메시지는 한 번만 계산됨)
QuarQKUsd	정책, 바이러스 또는 Outbreak 격리 메시지에 사용된 킬로바이트
LogUsd	사용된 로그 파티션의 비율
BMLd	안티바이러스 검사에 사용된 CPU 비율
CmrkLd	Cloudmark 안티스팸 검사에 사용된 CPU 비율
SophLd	Sophos 안티스팸 검사에 사용된 CPU 비율
McafLd	McAfee 안티바이러스 검사에 사용된 CPU 비율
CASELd	CASE 검사에 사용된 CPU 비율
TotalLd	총 CPU 사용량
LogAvail	로그 파일에 사용 가능한 디스크 공간의 양
EuQ	스팸 격리에 있을 것으로 추정되는 메시지 수
EuqRls	스팸 격리 릴리스 대기열에 있을 것으로 추정되는 메시지 수
RptLD	보고 프로세스 중 CPU 로드

통계	설명
QtnLd	격리 프로세스 중 CPU 로드
EncrQ	암호화 대기열의 메시지

상태 로그 예

```
Fri Feb 24 15:14:39 2006 Info: Status: CPULd 0 DskIO 0 RAMUtil 2 QKUsd 0 QKFre 8388608
CrtMID 19036 CrtICID 35284 CrtDCID 4861
InjMsg 13889 InjRcp 14230 GenBncRcp 12 RejRcp 6318 DrpMsg 7437 SftBncEvnt 1816 CmpRcp 6813
 HrdBncRcp 18 DnsHrdBnc 2 5XXHrdBnc
15 FltrHrdBnc 0 ExpHrdBnc 1 OtrHrdBnc 0 DlvRcp 6793 DelRcp 2 GlbUnsbHt 0 ActvRcp 0 UnatmptRcp
 0 AtmptRcp 0 CrtCncIn 0 CrtCncOut
0 DnsReq 143736 NetReq 224227 CchHit 469058 CchMis 504791 CchEct 15395 CchExp 55085 CPUTTm
 228 CPUETm 181380 MaxIO 350 RAMUsd
21528056 MMLen 0 DstInMem 4 ResCon 0 WorkQ 0 QuarMsgs 0 QuarQKUsd 0 LogUsd 3 AVLd 0 BMLd 0
 CASELd 3 TotalLd 3 LogAvail 17G EuQ 0
EuqRls 0
```

도메인 디버그 로그 사용

도메인 디버그 로그는 Email Security Appliance와 지정된 수신자 호스트 간 SMTP 변환 중 클라이언트와 서버 통신을 기록합니다. 이 로그 유형은 주로 특정 수신자 호스트의 문제를 디버그하는 데 사용됩니다.

표 ***122:*** 도메인 디버그 로그 통계

통계	설명
타임스탬프	반송 이벤트의 시간
Log level	이 반송 로그에 있는 세부사항의 레벨
From	Envelope From
하려는 작업	Envelope To
이유	전달 도중 SMTP 응답의 RFC 1893 Enhanced Mail Status Code 해석
응답	SMTP 응답 코드 및 수신자 호스트의 메시지

도메인 디버그 로그 예

```
Sat Dec 21 02:37:22 2003 Info: 102503993 Sent: 'MAIL FROM:<daily@dailyf-y-i.net>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'RCPT TO:<LLLSMILE@aol.com>'

Sat Dec 21 02:37:23 2003 Info: 102503993 Rcvd: '250 OK'

Sat Dec 21 02:37:23 2003 Info: 102503993 Sent: 'DATA'
```

```
Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '354 START MAIL INPUT, END WITH "." ON A
LINE BY ITSELF'

Sat Dec 21 02:37:24 2003 Info: 102503993 Rcvd: '250 OK'
```

주입 디버그 로그 사용

주입 디버그 로그는 Email Security Appliance와 시스템에 연결된 지정된 호스트 간 SMTP 대화를 기록합니다. 주입 디버그 로그는 Email Security Appliance 및 인터넷에서 연결을 시작하는 클라이언트 간 통신 문제 해결에 유용합니다. 로그에는 두 시스템 간에 전송된 모든 바이트가 기록되며, 연결하는 호스트로 전송("Sent to") 또는 연결하는 호스트에서 수신("Received from")으로 분류됩니다.

IP 주소, IP 범위, 호스트 이름 또는 부분 호스트 이름을 지정하여 기록할 호스트 대화를 지정해야 합니다. IP 범위 내 모든 연결 IP 주소는 기록됩니다. 부분 도메인 내 모든 호스트는 기록됩니다. 시스템은 호스트 이름으로 변환하기 위해 연결 IP 주소에서 역 DNS 조회를 수행합니다. DNS에 해당 PTR 레코드가 없는 IP 주소는 호스트 이름과 일치되지 않습니다.

기록할 세션의 수도 지정해야 합니다.

주입 디버그 로그 내 각 줄에는 다음 표의 다음 정보가 포함되어 있습니다.

표 ***123:*** 주입 디버그 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
ICID	Injection Connection ID는 다른 로그 서브스크립션에 있는 동일한 연결에 연결할 수 있는 고유한 식별자입니다.
Sent/Received	"Sent to"로 표시된 줄은 연결하는 호스트에 전송되는 실제 바이트입니다. "Received from"으로 표시된 줄은 연결하는 호스트에서 수신되는 실제 바이트입니다.
IP 주소	연결하는 호스트의 IP 주소

주입 디버그 로그 예

```
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '220 postman.example.com
ESMTP\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'HELO
mail.remotehost.com\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250
postman.example.com\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'MAIL
FROM:<sender@remotehost.com>\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 sender
<sender@remotehost.com> ok\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'RCPT
TO:<recipient@example.com>\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '250 recipient
```

```
<recipient@example.com> ok\015\012'
Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'DATA\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '354 go ahead\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'To:
recipient@example.com\015\012Date: Apr 02 2003 10:09:44\015\012Subject: Test
Subject\015\012From: Sender <sender@remotehost.com>\015\012'

Wed Apr 2 14:30:04 2003 Info: 6216 Rcvd from '172.16.0.22': 'This is the content of the
message'
Wed Apr 2 14:30:04 Info: 6216 Sent to '172.16.0.22': '250 ok\015\012'

Wed Apr 2 14:30:04 Info: 6216 Rcvd from '172.16.0.22': 'QUIT\015\012'
Wed Apr 2 14:30:04 2003 Info: 6216 Sent to '172.16.0.22': '221
postman.example.com\015\012'
```

시스템 로그 사용

표 ***124:*** 시스템 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	로깅된 이벤트

시스템 로그 예

이 예에서 시스템 로그는 커밋을 실행한 사용자의 이름 및 입력된 코멘트를 비롯한 몇몇 커밋 항목을 보여줍니다.

```
Wed Sep 8 18:02:45 2004 Info: Version: 4.0.0-206 SN: XXXXXXXXXXXX-XXX

Wed Sep 8 18:02:45 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:02:45 2004 Info: System is coming up

Wed Sep 8 18:02:49 2004 Info: bootstrapping DNS cache

Wed Sep 8 18:02:49 2004 Info: DNS cache bootstrapped

Wed Sep 8 18:13:30 2004 Info: PID 608: User admin commit changes: SSW:Password

Wed Sep 8 18:17:23 2004 Info: PID 608: User admin commit changes: Completed Web::SSW

Thu Sep 9 08:49:27 2004 Info: Time offset from UTC: -25200 seconds

Thu Sep 9 08:49:27 2004 Info: PID 1237: User admin commit changes: Added a second CLI
log for examples

Thu Sep 9 08:51:53 2004 Info: PID 1237: User admin commit changes: Removed example CLI
log.
```

CLI 감사 로그 사용

표 *125: CLI* 감사 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
PID	명령이 입력된 특정 CLI 세션에 대한 Process ID
메시지	메시지는 입력한 CLI 명령, CLI 출력(메뉴, 목록 등 포함) 및 표시된 프롬프트로 구성됩니다.

CLI 감사 로그 예

이 예에서 CLI 감사 로그는 PID 16434에 대해 who, textconfig CLI 명령이 입력되었음을 보여줍니다.

```
Thu Sep 9 14:35:55 2004 Info: PID 16434: User admin entered 'who'; prompt was
'\nmail3.example.com> '


Thu Sep 9 14:37:12 2004 Info: PID 16434: User admin entered 'textconfig'; prompt was
'\nUsername Login Time Idle Time Remote Host What\n======== ========== =========
========== ====\nadmin Wed 11AM 3m 45s 10.1.3.14 tail\nadmin 02:32PM
0s 10.1.3.14 cli\nmail3.example.com> '


Thu Sep 9 14:37:18 2004 Info: PID 16434: User admin entered ''; prompt was '\nThere are
no text resources currently defined.\n\n\nChoose the operation you want to perform:\n-
NEW - Create a new text resource.\n- IMPORT - Import a text resource from a file.\n[]> '
```

FTP 서버 로그 사용

표 *126: FTP* 서버 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
ID	Connection ID. 각 FTP 연결에 대한 별도의 ID
메시지	로그 항목의 메시지 섹션은 logfile 상태 정보 또는 FTP 연결 정보(로그인, 업로드, 다운로드, 로그아웃 등)일 수 있습니다.

FTP 서버 로그 예

이 예에서 FTP 서버 로그는 연결(ID:1)을 기록합니다. 수신 연결의 IP 주소, 활동(파일 업로드 및 다운로드) 및 로그아웃이 표시됩니다.

```
Wed Sep 8 18:03:06 2004 Info: Begin Logfile
```

```
Wed Sep 8 18:03:06 2004 Info: Version: 4.0.0-206 SN: 00065BF3BA6D-9WFWC21

Wed Sep 8 18:03:06 2004 Info: Time offset from UTC: 0 seconds

Wed Sep 8 18:03:06 2004 Info: System is coming up

Fri Sep 10 08:07:32 2004 Info: Time offset from UTC: -25200 seconds

Fri Sep 10 08:07:32 2004 Info: ID:1 Connection from 10.1.3.14 on 172.19.0.86

Fri Sep 10 08:07:38 2004 Info: ID:1 User admin login SUCCESS

Fri Sep 10 08:08:46 2004 Info: ID:1 Upload wording.txt 20 bytes

Fri Sep 10 08:08:57 2004 Info: ID:1 Download words.txt 1191 bytes

Fri Sep 10 08:09:06 2004 Info: ID:1 User admin logout
```

HTTP 로그 사용

표 ***127: HTTP*** 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
ID	세션 ID
req	연결하는 시스템의 IP 주소
user	연결하는 사용자의 사용자 이름
메시지	수행된 작업에 대한 정보. GET 또는 POST 명령, 시스템 상태 등이 포함될 수 있습니다.

HTTP 로그 예

이 예에서 HTTP 로그는 관리자 사용자와 GUI의 상호 작용을 보여줍니다(시스템 설정 마법사 실행 등).

```
Wed Sep 8 18:17:23 2004 Info: http service on 192.168.0.1:80 redirecting to https port 443

Wed Sep 8 18:17:23 2004 Info: http service listening on 192.168.0.1:80

Wed Sep 8 18:17:23 2004 Info: https service listening on 192.168.0.1:443

Wed Sep 8 11:17:24 2004 Info: Time offset from UTC: -25200 seconds

Wed Sep 8 11:17:24 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg POST
/system_administration/system_setup_wizard HTTP/1.1 303

Wed Sep 8 11:17:25 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/system_administration/ssw_done HTTP/1.1 200

Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/incoming_mail_overview HTTP/1.1 200
```

```
Wed Sep 8 11:18:45 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/mail_flow_graph?injector=&width=365&interval=0&type=recipientsin&height=190
HTTP/1.1 200

Wed Sep 8 11:18:46 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/classification_graph?injector=&width=325&interval=0&type=recipientsin&height=19
0 HTTP/1.1 200

Wed Sep 8 11:18:49 2004 Info: req:10.10.10.14 user:admin id:iaCkEh2h5rZknQarAecg GET
/monitor/quarantines HTTP/1.1 200
```

NTP 로그 사용

표 ***128: NTP*** 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 서버에 대한 SNTP(Simple Network Time Protocol) 쿼리 또는 adjust: 메시지로 구성됩니다.

NTP 로그 예

이 예에서 NTP 로그는 어플라이언스가 NTP 호스트를 두 번 폴링하는 것을 보여줍니다.

```
Thu Sep 9 07:36:39 2004 Info: sntp query host 10.1.1.23 delay 653 offset -652

Thu Sep 9 07:36:39 2004 Info: adjust: time_const: 8 offset: -652us next_poll: 4096

Thu Sep 9 08:44:59 2004 Info: sntp query host 10.1.1.23 delay 642 offset -1152

Thu Sep 9 08:44:59 2004 Info: adjust: time_const: 8 offset: -1152us next_poll: 4096
```

검사 로그 사용

검사 로그에는 어플라이언스의 검사 엔진에 대한 모든 LOG 및 COMMON 메시지가 포함됩니다. 사용 가능한 COMMON 및 LOG 알림 메시지 목록은 "시스템 관리" 장의 알림 섹션을 참조하십시오.

표 ***129:*** 검사 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 애플리케이션 장애, 전송 알림, 실패 알림 또는 검사 엔진 중 하나에 대한 로그 오류 메시지로 구성됩니다.

검사 로그 예

이 예에서 로그는 Sophos 안티바이러스에 대한 경고 알림을 전송하는 어플라이언스의 기록을 보여줍니다.

```
Wed Feb 23 22:05:48 2011 Info: Internal SMTP system attempting to send a message to
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...' (attempt #0).


Wed Feb 23 22:05:48 2011 Info: Internal SMTP system successfully sent a message to
alerts@example.com with subject 'Warning <Anti-Virus> mail3.example.com: sophos
antivirus - The Anti-Virus database on this system is...'.


Wed Feb 23 22:05:48 2011 Info: A Anti-Virus/Warning alert was sent to alerts@example.com
with subject "Warning <Anti-Virus> mail3.example.com: sophos antivirus - The Anti-Virus
database on this system is...".
```

안티 스팸 로그 사용

표 ***130:*** 안티스팸 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 안티스팸 업데이트에 대한 확인 및 결과로 구성됩니다(엔진 또는 안티스팸 규칙의 업데이트가 필요한지 여부 등).

안티 스팸 로그 예

이 예에서 안티스팸 로그는 스팸 정의 업데이트 및 CASE 업데이트를 확인하는 안티스팸 엔진을 보여줍니다.

```
Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19103) : case-daemon: server
successfully spawned child process, pid 19111

Fri Apr 13 18:59:47 2007 Info: case antispam - engine (19111) : startup: Region profile:
Using profile global

Fri Apr 13 18:59:59 2007 Info: case antispam - engine (19111) : fuzzy: Fuzzy plugin v7
successfully loaded, ready to roll

Fri Apr 13 19:00:01 2007 Info: case antispam - engine (19110) : uribllocal: running URI
blocklist local

Fri Apr 13 19:00:04 2007 Info: case antispam - engine (19111) : config: Finished loading
configuration
```

그레이메일 로그 사용

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 그레이메일 엔진, 상태, 구성 등에 대한 정보를 포함합니다.

그레이메일 로그 예

```
Tue Mar 24 08:56:45 2015 Info: graymail [BASE] Logging at DEBUG level

Tue Mar 24 08:56:45 2015 Info: graymail [HANDLER] Initializing request handler

Tue Mar 24 08:56:50 2015 Info: graymail [ENGINE] Loaded graymail scanner library

Tue Mar 24 08:56:50 2015 Info: graymail [ENGINE] Created graymail scanner instance

Tue Mar 24 08:56:50 2015 Info: graymail [HANDLER] Debug mode disabled on graymail process

Tue Mar 24 08:56:50 2015 Info: graymail [HANDLER] Starting thread WorkerThread_0
```

안티 바이러스 로그 사용

표 ***131:*** 안티바이러스 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 안티바이러스 업데이트에 대한 확인 및 결과로 구성됩니다(엔진 또는 바이러스 정의의 업데이트가 필요한지 여부 등)

안티 바이러스 로그 예

이 예에서 안티바이러스 로그는 바이러스 정의(IDE) 및 엔진 자체에 대한 업데이트를 확인하는 Sophos 안티바이러스 엔진을 보여줍니다.

```
Thu Sep 9 14:18:04 2004 Info: Checking for Sophos Update

Thu Sep 9 14:18:04 2004 Info: Current SAV engine ver=3.84. No engine update needed

Thu Sep 9 14:18:04 2004 Info: Current IDE serial=2004090902. No update needed.
```

안티바이러스 엔진이 지정된 메시지에 대해 특정 판정을 반환한 이유를 진단하는 데 도움이 되도록 이것을 일시적으로 DEBUG 레벨로 설정할 수 있습니다. DEBUG 로깅 정보는 자세하므로 신중하게 사용해야 합니다.

AMP 엔진 로그 사용

AMP 엔진 로그에는 다음 세부 사항이 포함되어 있습니다.

- 파일 평판 서버에 전송된 파일 평판 쿼리 및 파일 평판 서버에서 수신된 응답
- 파일 분석(파일이 파일 분석 서버에 업로드된 경우) 파일 분석의 상태는 파일 분석 서버에서 응답을 수신할 때까지 주기적으로 기록됩니다.

AMP 엔진 로그 항목의 예

다음은 특정 시나리오를 기반으로 하는 샘플 AMP 엔진 로그 항목입니다.

- 파일 평판 및 파일 분석 서버 초기화, 1090 페이지
- 파일 평판 서버가 구성되지 않음, 1090 페이지
- 파일 평판 쿼리 초기화, 1090 페이지
- 파일 평판 서버에서 파일 평판 쿼리에 대한 응답이 수신됨, 1091 페이지
- 분석 및 파일 분석 프로세스를 위한 파일이 업로드됨, 1092 페이지
- 분석을 위한 파일이 업로드되지 않음, 1093 페이지
- 파일 업로드 제한으로 인해 파일 분석을 위한 파일 업로드를 건너뜀 , 1093 페이지
- 파일 분석 서버 오류로 인해 파일 분석을 위한 파일 업로드를 건너뜀, 1094 페이지
- 파일 회귀 판정이 수신됨, 1094 페이지

파일 평판 및 파일 분석 서버 초기화

```
Wed Oct 5 15:17:31 2016 Info: File reputation service initialized successfully
Wed Oct 5 15:17:31 2016 Info: The following file type(s) can be sent for File Analysis:
Microsoft Windows / DOS Executable, Microsoft Office 97-2004 (OLE), Microsoft Office 2007+
 (Open XML), Other potentially malicious file types, Adobe Portable Document Format (PDF).
 To allow analysis of new file type(s), go to Security Services > File Reputation and
Analysis.
Wed Oct 5 15:17:31 2016 Info: File Analysis service initialized successfully
```

파일 평판 서버가 구성되지 않음

```
Tue Oct 4 23:15:24 2016 Warning: MID 12 reputation query failed for attachment 'Zombies.pdf'
 with error "Cloud query failed"
```

파일 평판 쿼리 초기화

```
Fri Oct 7 09:44:04 2016 Info: File reputation query initiating. File Name = 'mod-6.exe',
MID = 5, File Size = 1673216 bytes,
File Type = application/x-dosexec
```

통계	설명
파일 이름	SHA-256 해시 식별자가 파일 평판 서버에 전송되는 파일의 이름입니다. 파일 이름을 사용할 수 없는 경우 알 수 없음으로 표시됩니다.

통계	설명
MID	이메일 파이프라인을 통해 전송되는 메시지를 추적하는 데 사용되는 메시지 ID입니다.
파일 크기	SHA-256 해시 식별자가 파일 평판 서버에 전송되는 파일의 크기입니다.
파일 유형	SHA-256 해시 식별자가 파일 평판 서버에 전송되는 파일의 유형입니다. 지원되는 파일 유형은 다음과 같습니다. • Microsoft Windows / DOS Executable • Microsoft Office 97-2004(OLE) • Microsoft Office 2007+(Open XML) • 그 외의 잠재적인 악성 파일 유형 • Adobe PDF(Portable Document Format)

파일 평판 서버에서 파일 평판 쿼리에 대한 응답이 수신됨

```
Fri Oct 7 09:44:06 2016 Info: Response received for file reputation query from Cloud. File
Name = 'mod-6.exe', MID = 5, Disposition = MALICIOUS, Malware = W32.061DEF69B5-100.SBX.TG,
Reputation Score = 73, sha256 =
061def69b5c100e9979610fa5675bd19258b19a7ff538b5c2d230b467c312f19, upload_action = 2
```

통계	설명
파일 이름	SHA-256 해시 식별자가 파일 평판 서버에 전송되는 파일의 이름입니다. 파일 이름을 사용할 수 없는 경우 알 수 없음으로 표시됩니다.
MID	이메일 파이프라인을 통해 전송되는 메시지를 추적하는 데 사용되는 메시지 ID입니다.
속성	파일 평판 상태 값은 다음과 같습니다. • MALICIOUS • Clean • FILE UNKNOWN - 평판 점수가 0 인 경우. • VERDICT UNKNOWN - 상태가 FILE UNKNOWN이고 점수가 0이 아닌 경우.
악성코드	악성코드 위협의 이름입니다.
평판 점수	파일 평판 서버에 의해 파일에 할당된 평판 점수입니다. 파일 상태가 **VERDICT UNKNOWN**인 경우 어플라이언스는 평판 점수 및 임계값에 따라 파일 평판 판정을 조정합니다.

통계	설명
업로드 작업	지정된 파일에서 수행할 파일 평판 서버의 권장 업로드 작업 값: • 0 - 업로드를 위해 전송할 필요 없음 • 1 - 업로드를 위해 파일 전송. 참고 업로드 작업 값이 '1'인 경우 어플라이언스는 파일을 업로드합니다. • 2 - 업로드를 위해 파일을 전송하지 않음 • 3 - 업로드를 위해 메타데이터만 전송

분석 및 파일 분석 프로세스를 위한 파일이 업로드됨

```
Wed Sep 28 11:31:58 2016 Info: File uploaded for analysis. SHA256:
e7ae35a8227b380ca761c0317e814e4aaa3d04f362c6b913300117241800f0ea

Wed Sep 28 11:36:58 2016 Info: File Analysis is running for SHA:
e7ae35a8227b380ca761c0317e814e4aaa3d04f362c6b913300117241800f0ea

Fri Oct 7 07:39:13 2016 Info: File Analysis complete. SHA256:
16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc, Submit Timestamp:
1475825466, Update Timestamp: 1475825953, Disposition: 3 Score: 100, run_id: 194926004
Details: Analysis is completed for the File
SHA256[16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc]
Spyname:[W32.16454AFF50-100.SBX.TG]
```

통계	설명
SHA256	해당 파일에 대한 SHA-256 해시 식별자입니다.
제출 타임스탬프	어플라이언스에서 파일을 파일 분석 서버에 업로드한 날짜와 시간입니다.
업데이트 타임스탬프	파일에 대한 파일 분석이 완료된 날짜 및 시간입니다.
속성	파일 평판 상태 값입니다. • 1 - 탐지된 맬웨어 없음 • 2 - 정상 • 3 - 악성코드
점수	파일 분석 서버에 의해 파일에 할당된 분석 점수입니다.
실행 ID	특정 파일 분석을 위해 파일 분석 서버에서 파일에 할당한 숫자 값(ID)입니다.
세부 사항	파일 분석 중에 오류가 보고되는 경우의 추가 정보입니다. 그렇지 않으면 파일에 대한 최종 분석이 완료되었음을 나타냅니다.

통계	설명
스파이 이름	파일 분석 중 파일에서 악성코드가 발견된 경우 위협의 이름입니다.

분석을 위한 파일이 업로드되지 않음

```
Wed Sep 14 12:27:52 2016 Info: File not uploaded for analysis. MID = 0 File
SHA256[a5f28f1fed7c2fe88bcdf403710098977fa12c32d13bfbd78bbe27e95b245f82] file
mime[text/plain] Reason: No active/dynamic contents exists
```

통계	설명
MID	이메일 파이프라인을 통해 전송되는 메시지를 추적하는 데 사용되는 메시지 ID입니다.
파일 MIME	파일의 MIME 유형입니다.
이유	다음은 upload_action이 '1'로 설정된 경우에도 파일 분석 서버에 파일이 업로드되지 않은 이유 중 하나입니다. • 파일이 다른 노드에 의해 이미 업로드되었습니다. 파일이 다른 어플라이언스를 통해 파일 분석 서버에 이미 업로드되었습니다. • 파일 분석 진행 중 - 진행 중인 업로드에 대해 파일이 이미 선택되었습니다. • 파일이 파일 분석 서버에 이미 업로드되었습니다. • 지원되는 파일 유형이 아님 • 파일 크기가 범위를 벗어남 - 업로드 파일 크기가 파일 분석 서버에서 설정한 임계값 제한을 초과합니다. • 업로드 대기열이 꽉 참 • 파일 분석 서버 오류 • 활성/동적 콘텐츠가 없음 • 일반/알 수 없는 오류

파일 업로드 제한으로 인해 파일 분석을 위한 파일 업로드를 건너뜀

```
Tue Jun 20 13:22:56 2017 Info: File analysis upload skipped. SHA256:
b5c7e26491983baa713c9a2910ee868efd891661c6a0553b28f17b8fdc8cc3ef,Timestamp[1454782976]
details[File SHA256[b5c7e26491983baa713c9a2910ee868efd891661c6a0553b28f17b8fdc8cc3ef] file
mime[application/pdf], upload priority[Low] not uploaded, re-tries[3], backoff[986]
discarding ...]
Tue Jun 20 13:22:56 2017 Critical: The attachment could not be uploaded to the
File Analysis server because the appliance exceeded the upload limit
```

통계	설명
SHA256	해당 파일에 대한 SHA-256 해시 식별자입니다.
타임스탬프	파일을 파일 분석 서버에 업로드하지 못한 날짜와 시간입니다.
세부 사항	파일 분석 서버 오류에 대한 세부 정보입니다.

통계	설명
파일 MIME	파일의 MIME 유형입니다.
업로드 우선순위	업로드 우선순위 값은 다음과 같습니다. • High - PDF 파일 유형을 제외하고 선택된 모든 파일 유형 • Low - PDF 파일 유형만
Retries(재시도)	지정된 파일에서 수행된 업로드 시도 횟수입니다. 참고 지정된 파일에서 최대 3번의 업로드 시도를 수행할 수 있습니다.
백오프(x)	파일 분석 서버에 파일 업로드를 시도하기 전에 어플라이언스에서 대기해야 하는 시간((x)초)입니다. 이는 어플라이언스가 일일 업로드 제한에 도달한 경우에 발생합니다.
위험(이유)	어플라이언스에서 업로드 제한을 초과했기 때문에 첨부 파일을 파일 분석 서버에 업로드할 수 없습니다.

파일 분석 서버 오류로 인해 파일 분석을 위한 파일 업로드를 건너뜀

```
Sat Feb 6 13:22:56 2016 Info:SHA256:
69e17e213732da0d0cbc48ae7030a4a18e0c1289f510e8b139945787f67692a5,Timestamp[1454959409]
details[Server Response HTTP code:[502]]
```

통계	설명
SHA256	해당 파일에 대한 SHA-256 해시 식별자입니다.
타임스탬프	파일 분석 서버에 파일을 업로드하려고 시도한 날짜와 시간입니다.
세부 사항	파일 분석 서버 오류에 대한 정보

파일 회귀 판정이 수신됨

```
Fri Oct 7 07:39:13 2016 Info: Retrospective verdict received. SHA256:
16454aff5082c2e9df43f3e3b9cdba3c6ae1766416e548c30a971786db570bfc, Timestamp: 1475832815.7,
Verdict: MALICIOUS, Reputation Score: 0, Spyname: W32.16454AFF50-100.SBX.
```

통계	설명
SHA256	해당 파일에 대한 SHA-256 해시 식별자입니다.
타임스탬프	파일 분석 서버에서 파일 검토 판정이 수신된 날짜와 시간입니다.
판정	파일 검토 판정 값은 악성 또는 정상입니다.
Reputation Score	파일 평판 서버에 의해 파일에 할당된 평판 점수입니다.
Spyname	파일 분석 중 파일에서 악성코드가 발견된 경우 위협의 이름입니다.

스팸 격리 로그 사용

표 ***132:*** 스팸 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 수행한 작업으로 구성됩니다(메시지 격리, 격리에서 릴리스 등).

스팸 격리 로그 예

이 예에서 로그는 격리에서 admin@example.com으로 릴리스되는 메시지(MID 8298624)를 보여줍니다.

```
Mon Aug 14 21:41:47 2006 Info: ISQ: Releasing MID [8298624, 8298625] for all

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298624 (skipping work
queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID 8298624 to admin@example.com

Mon Aug 14 21:41:47 2006 Info: ISQ: Delivering released MID 8298625 (skipping work
queue)

Mon Aug 14 21:41:47 2006 Info: ISQ: Released MID8298625 to admin@example.com
```

스팸 격리 **GUI** 로그 사용

표 ***133:*** 스팸 ***GUI*** 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 사용자 인증 등을 비롯하여 수행한 작업으로 구성됩니다.

스팸 격리 **GUI** 로그 예

이 예에서 로그는 성공적인 인증, 로그인 및 로그아웃을 보여줍니다.

```
Fri Aug 11 22:05:28 2006 Info: ISQ: Serving HTTP on 192.168.0.1, port 82

Fri Aug 11 22:05:29 2006 Info: ISQ: Serving HTTPS on 192.168.0.1, port 83

Fri Aug 11 22:08:35 2006 Info: Authentication OK, user admin

Fri Aug 11 22:08:35 2006 Info: logout:- user:pqufOtL6vyI5StCqhCfO session:10.251.23.228

Fri Aug 11 22:08:35 2006 Info: login:admin user:pqufOtL6vyI5StCqhCfO
session:10.251.23.228
```

```
Fri Aug 11 22:08:44 2006 Info: Authentication OK, user admin
```

LDAP 디버그 로그 사용

표 ***134: LDAP*** 디버그 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	LDAP 디버그 메시지

LDAP 디버그 로그 예

참고 로그 파일의 각 줄에 번호가 매겨지지는 않습니다. 샘플의 편의상 여기에서만 번호를 매긴 것입니다.

1	`Thu Sep  9 12:24:56 2004 Begin Logfile`
2	`Thu Sep  9 12:25:02 2004 LDAP:` `Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa`
3	`Thu Sep  9 12:25:02 2004 LDAP:` `Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa`
4	`Thu Sep  9 12:25:02 2004 LDAP:` `Masquerade query sun.masquerade address employee@routing.qa to employee@mail.qa`
5	`Thu Sep  9 12:28:08 2004 LDAP: Clearing LDAP cache`
6	`Thu Sep  9 13:00:09 2004 LDAP:` `Query '(&(ObjectClass={g})(mailLocalAddress={a}))' to server sun (sun.qa:389)`

7	`Thu Sep  9 13:00:09 2004 LDAP:`
	`After substitute, query is '(&(ObjectClass=inetLocalMailRecipient)`
	`(mailLocalAddress=rroute.d00002b.loc@ldap.route.local.add00002.qa))'`

8	`Thu Sep  9 13:00:09 2004 LDAP: connecting to server`
9	`Thu Sep  9 13:00:09 2004 LDAP: connected`

10	`Thu Sep  9 13:00:09 2004 LDAP:`
	`Query (&(ObjectClass=inetLocalMailRecipient)`
	`(mailLocalAddress=rroute.d00002b.loc@ldap.route.local.add00002.qa)) returned 1`
	` results`

11	`Thu Sep  9 13:00:09 2004 LDAP: returning: [<LDAP:>]`

위 로그 파일을 읽기 위한 가이드로 사용하십시오.

표 ***135: LDAP*** 디버그 로그 세부사항 예

라인 번호	설명
1	로그 파일이 초기화됩니다.
2 3 4	리스너가 가장을 위해 LDAP를 사용하도록 구성됩니다(특히 "sun.masquerade"라는 LDAP 쿼리로). employee@routing.qa 주소가 LDAP 서버에서 조회되고, 일치가 발견되고, 결과적으로 가장 주소 employee@mail.qa가 됩니다. 가상 컨피그레이션에 따라 이 주소는 메시지 헤더 및/또는 envelope from에 기록됩니다.
5	사용자는 수동으로 ldapflush를 실행합니다.
6	sun.qa, 포트 389로 쿼리를 보내려고 합니다. 쿼리 템플릿은 (&(ObjectClass={g})(mailLocalAddress={a}))입니다. {g}는 호출 필터 rcpt-to-group 또는 mail-from-group 규칙에 지정된 그룹 이름으로 교체됩니다. {a}는 문제의 주소로 교체됩니다.
7	위에 설명한 교체가 발생합니다. 이것은 LDAP 서버로 전송되기 전 쿼리의 모습입니다.
8	아직 서버에 연결되지 않아서 연결하는 중입니다.
9	서버에 전송된 데이터입니다.
10	결과는 빈 긍정(empty positive)입니다. 즉, 하나의 레코드가 반환되었지만 쿼리가 필드를 요구하지 않았으므로 보고된 데이터가 없습니다. 이것은 데이터베이스에 일치 항목이 있는지 확인할 때 그룹 및 수락 쿼리에 모두 사용됩니다.

허용 목록/차단 목록 로그 사용

다음 표는 허용 목록/차단 목록 로그에 기록된 통계를 보여줍니다.

표 ***136:*** 허용 목록/차단 목록 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 사용자 인증 등을 비롯하여 수행한 작업으로 구성됩니다.

허용 목록/차단 목록 로그 예

이 예에서 허용 목록/차단 목록 로그는 어플라이언스가 두 시간마다 데이터베이스 스냅샷을 만드는 것을 보여줍니다. 또한 발신자가 데이터베이스에 추가된 시간을 보여줍니다.

```
Fri Sep 28 14:22:33 2007 Info: Begin Logfile Fri Sep 28 14:22:33 2007 Info: Version:
6.0.0-425 SN: XXXXXXXXXXXX-XXX Fri Sep 28 14:22:33 2007 Info: Time offset from UTC:
10800 seconds Fri Sep 28 14:22:33 2007 Info: System is coming up.


Fri Sep 28 14:22:33 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 16:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 18:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 20:22:34 2007 Info: SLBL: The database snapshot has been created.

Fri Sep 28 22:22:35 2007 Info: SLBL: The database snapshot has been created.

.........................

Mon Oct 1 14:16:09 2007 Info: SLBL: The database snapshot has been created.

Mon Oct 1 14:37:39 2007 Info: SLBL: The database snapshot has been created.

Mon Oct 1 15:31:37 2007 Warning: SLBL: Adding senders to the database failed.

Mon Oct 1 15:32:31 2007 Warning: SLBL: Adding senders to the database failed.

Mon Oct 1 16:37:40 2007 Info: SLBL: The database snapshot has been created.
```

보고 로그 사용

다음 표는 보고 로그에 기록된 통계를 보여줍니다.

표 ***137:*** 보고 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 사용자 인증 등을 비롯하여 수행한 작업으로 구성됩니다.

보고 로그 예

이 예에서 보고 로그는 어플라이언스가 정보 로그 레벨에서 설정된 것을 보여줍니다.

```
Wed Oct 3 13:39:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:39:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-40

Wed Oct 3 13:40:53 2007 Info: Pages found in cache: 1304596 (99%). Not found: 1692

Wed Oct 3 13:40:53 2007 Info: Period hour using 36800 (KB)
```

```
Wed Oct 3 13:40:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:40:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:40:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:40:53 2007 Info: HELPER checkpointed in 0.00580507753533 seconds

Wed Oct 3 13:41:02 2007 Info: Update 2 registered appliance at 2007-10-03-13-41

Wed Oct 3 13:41:53 2007 Info: Pages found in cache: 1304704 (99%). Not found: 1692

Wed Oct 3 13:41:53 2007 Info: Period hour using 36800 (KB)

Wed Oct 3 13:41:53 2007 Info: Period day using 2768 (KB)

Wed Oct 3 13:41:53 2007 Info: Period minute using 0 (KB)

Wed Oct 3 13:41:53 2007 Info: Period month using 1328 (KB)

Wed Oct 3 13:42:03 2007 Info: Update 2 registered appliance at 2007-10-03-13-42
```

보고 쿼리 로그 사용

다음 표는 보고 쿼리 로그에 기록된 통계를 보여줍니다.

표 ***138:*** 보고 쿼리 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 사용자 인증 등을 비롯하여 수행한 작업으로 구성됩니다.

보고 쿼리 로그 예

이 예에서 보고 쿼리 로그는 어플라이언스가 2007년 8월 29일에서 10월 10일까지 매일 발신 이메일 트래픽 쿼리를 실행한 것을 보여줍니다.

```
Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804479.

Tue Oct 2 11:30:02 2007 Info: Query: Closing interval handle 811804480.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610228.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610229 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

DETECTED_SPAM', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_VIRUS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.THREAT_CONTENT_FILTER',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_PROCESSED'] for rollup period "day" with
interval range 2007-08-29 to 2007-10-01
with key constraints

None sorting on ['MAIL_OUTGOING_TRAFFIC_SUMMARY.DETECTED_SPAM'] returning results from
```

```
0 to 2 sort_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610229.

Tue Oct 2 11:30:02 2007 Info: Query: Merge query with handle 302610230 for
['MAIL_OUTGOING_TRAFFIC_SUMMARY.

TOTAL_HARD_BOUNCES', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS_DELIVERED',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval
range 2007-08-29 to
2007-10-01 with key constraints None sorting on
['MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_HARD_BOUNCES'] returning
results from 0 to 2 sort_ascending=False.

Tue Oct 2 11:30:02 2007 Info: Query: Closing query handle 302610230.
```

업데이트 로그 사용

표 ***139:*** 업데이트 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 시스템 서비스 업데이트 정보, 그리고 AsyncOS에서 업데이트 및 다음 업데이트 예약 날짜/시간을 확인한 내용으로 구성됩니다.

업데이트 로그 예

이 예에서 로그는 어플라이언스가 새로운 McAfee Anti-Virus 정의로 업데이트되는 것을 보여줍니다.

```
Fri Sep 19 11:07:51 2008 Info: Starting scheduled update

Fri Sep 19 11:07:52 2008 Info: Acquired server manifest, starting update 11

Fri Sep 19 11:07:52 2008 Info: Server manifest specified an update for mcafee

Fri Sep 19 11:07:52 2008 Info: mcafee was signalled to start a new update

Fri Sep 19 11:07:52 2008 Info: mcafee processing files from the server manifest

Fri Sep 19 11:07:52 2008 Info: mcafee started downloading files

Fri Sep 19 11:07:52 2008 Info: mcafee downloading remote file
"http://stage-updates.ironport.com/mcafee/dat/5388"

Fri Sep 19 11:07:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:12:52
2008

Fri Sep 19 11:08:12 2008 Info: mcafee started decrypting files

Fri Sep 19 11:08:12 2008 Info: mcafee decrypting file
"mcafee/dat/5388" with method "des3_cbc"

Fri Sep 19 11:08:17 2008 Info: mcafee started decompressing files

Fri Sep 19 11:08:17 2008 Info: mcafee started applying files

Fri Sep 19 11:08:17 2008 Info: mcafee applying file "mcafee/dat/5388"
```

```
Fri Sep 19 11:08:18 2008 Info: mcafee verifying applied files

Fri Sep 19 11:08:18 2008 Info: mcafee updating the client manifest

Fri Sep 19 11:08:18 2008 Info: mcafee update completed

Fri Sep 19 11:08:18 2008 Info: mcafee waiting for new updates

Fri Sep 19 11:12:52 2008 Info: Starting scheduled update

Fri Sep 19 11:12:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:17:52
2008

Fri Sep 19 11:17:52 2008 Info: Starting scheduled update

Fri Sep 19 11:17:52 2008 Info: Scheduled next update to occur at Fri Sep 19 11:22:52
2008
```

업데이트 로그 예

이 예에서 로그는 비활성화된 자동 업데이트와 Sophos 안티바이러스 정의에 적용된 백업을 보여줍니다.

```
Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “postx”

Fri Mar 10 15:05:55 2017 Debug: postx updates disabled

Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “postx”

Fri Mar 10 15:05:55 2017 Trace: command session starting

Fri Mar 10 15:05:55 2017 Info: Automatic updates disabled for engine Sophos engine

Fri Mar 10 15:05:55 2017 Info: Sophos: Backup update applied successfully

Fri Mar 10 15:05:55 2017 Info: Internal SMTP system attempting to send a message to
abshastr@ironport.com
with subject ‘Automatic updates are now disabled for sophos’ attempt #0).

Fri Mar 10 15:05:55 2017 Debug: amp feature key disabled

Fri Mar 10 15:05:55 2017 Debug: Skipping update request for “amp”

Fri Mar 10 15:05:55 2017 Debug: amp feature key disabled
```

추적 로그 이해

추적 로그는 AsyncOS의 이메일 작업에 대한 정보를 기록합니다. 로그 메시지는 메일 로그에 기록된 메시지의 하위 집합입니다.

추적 로그는 어플라이언스의 메시지 추적 구성 요소가 메시지 추적 데이터베이스를 구축하는 데 사용됩니다. 로그 파일은 데이터베이스 구축 과정에서 소모되므로 추적 로그는 일시적입니다. 추적 로그의 정보는 사람이 보거나 분석하도록 설계되지 않습니다.

또한 Cisco Security Management 어플라이언스를 사용하면 여러 Email Security Appliance의 추적 정보를 볼 수 있습니다.

인증 로그 사용

인증 로그는 사용자 로그인 시도의 성공과 실패를 기록합니다.

표 ***140:*** 인증 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간.
메시지	메시지는 어플라이언스에 로그인을 시도한 사용자의 사용자 이름 및 인증의 성공 여부로 구성됩니다.

인증 로그 예

이 예에서 로그는 "admin," "joe" 및 "dan" 사용자의 로그인 시도를 보여줍니다.

```
Wed Sep 17 15:16:25 2008 Info: Begin Logfile

Wed Sep 17 15:16:25 2008 Info: Version: 6.5.0-262 SN: XXXXXXX-XXXXX

Wed Sep 17 15:16:25 2008 Info: Time offset from UTC: 0 seconds

Wed Sep 17 15:18:21 2008 Info: User admin was authenticated successfully.

Wed Sep 17 16:26:17 2008 Info: User joe failed authentication.

Wed Sep 17 16:28:28 2008 Info: User joe was authenticated successfully.

Wed Sep 17 20:59:30 2008 Info: User admin was authenticated successfully.

Wed Sep 17 21:37:09 2008 Info: User dan failed authentication.
```

잘못된 암호로 인한 이중 인증 로그인 실패의 예

이 예에서 로그는 잘못된 암호 입력으로 인한 이중 인증 로그인 실패를 보여줍니다.

```
Thu Mar 16 05:47:47 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:48:18 2017 Info: Two-Factor RADIUS Authentication failed.

Thu Mar 16 05:48:48 2017 Info: An authentication attempt by the user **** from
21.101.210.150 failed
```

시간 초과로 인한 이중 인증 로그인 실패의 예

이 예에서 로그는 시간 초과로 인한 이중 인증 로그인 실패를 보여줍니다.

```
Thu Mar 16 05:46:04 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:46:59 2017 Info: RADIUS server example.cisco.com communication error. No
valid responses from server (timeout).

Thu Mar 16 05:46:59 2017 Info: Two-Factor Authentication RADIUS servers timed out.
Authentication could fail due to this.
```

이중 인증 로그인 성공의 예

이 예에서 로그는 성공적인 이중 인증 로그인을 보여줍니다.

```
Thu Mar 16 05:49:05 2017 Info: Trying RADIUS server example.cisco.com

Thu Mar 16 05:49:05 2017 Info: Two-Factor RADIUS Authentication was successful.

Thu Mar 16 05:49:05 2017 Info: The user admin successfully logged on from 21.101.210.150
using an HTTPS connection.
```

구성 기록 로그 사용

구성 기록 로그는 사용자 이름이 나열된 추가 섹션이 있는 구성 파일, 구성에서 사용자가 어디를 변경했는가에 대한 설명, 사용자가 변경을 커밋할 때 입력한 코멘트로 구성됩니다. 사용자가 변경을 커밋할 때마다 변경 후 구성 파일을 포함하는 새 로그가 생성됩니다.

컨피그레이션 기록 로그 예

이 예에서 구성 기록 로그는 사용자(admin)가 시스템에 로그인이 허용된 로컬 사용자를 정의하는 테이블에 게스트 사용자를 추가한 것을 보여줍니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<!--

XML generated by configuration change.

Change comment: added guest user

User: admin

Configuration are described as:

This table defines which local users are allowed to log into the system.

Product: Cisco IronPort M160 Messaging Gateway(tm) Appliance

Model Number: M160

Version: 6.7.0-231

Serial Number: 000000000ABC-D000000

Number of CPUs: 1

Memory (GB): 4

Current Time: Thu Mar 26 05:34:36 2009

Feature "Cisco IronPort Centralized Configuration Manager": Quantity = 10, Time
Remaining = "25 days"

Feature "Centralized Reporting": Quantity = 10, Time Remaining = "9 days"

Feature "Centralized Tracking": Quantity = 10, Time Remaining = "30 days"

Feature "Centralized Spam Quarantine": Quantity = 10, Time Remaining = "30 days"
```

```
Feature "Receiving": Quantity = 1, Time Remaining = "Perpetual"

-->

<config>
```

외부 위협 피드 엔진 로그 사용

ETF 로그는 ETF 엔진, 상태, 구성 등에 대한 정보를 포함합니다. 대부분의 정보는 Info(정보) 또는 Debug(디버그) 수준입니다.

외부 위협 피드 엔진 로그의 예

```
Thu Jun 7 04:54:15 2018 Info: THREAT_FEEDS: Job failed with exception: Invalid URL or Port
 Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: A delta poll is scheduled for the source: S1
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: A delta poll has started for the source: S1,
domain: s1.co, collection: sss
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: Observables are being fetched from the source:
 S1 between 2018-06-07 04:34:13+00:00 and 2018-06-07 05:04:13.185909+00:00
Thu Jun 7 05:04:13 2018 Info: THREAT_FEEDS: 21 observables were fetched from the source:
S1
Thu Jun 7 05:19:14 2018 Info: THREAT_FEEDS: A delta poll is scheduled for the source: S1
Thu Jun 7 05:19:14 2018 Info: THREAT_FEEDS: A delta poll has started for the source: S1,
domain: s1.co, collection: sss
```

ETF 소스 구성 실패 **-** 잘못된 컬렉션 이름

이 예에서 로그는 유효하지 않은 컬렉션 이름 때문에 어플라이언스가 외부 위협 피드 소스에서 위협 피드를 가져올 수 없음을 보여줍니다.

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com, cause of failure: Invalid Collection name
```

해결책

웹 인터페이스에서 *Mail Policies(*메일 정책*)* > *External Threat Feeds Manager(*외부 위협 피드 관리자*)* 페이지로 이동하거나 CLI에서 `threatfeedsconfig > sourceconfig` 하위 명령을 사용하여 구성된 외부 위협 피드 소스의 올바른 컬렉션 이름을 입력합니다.

ETF 소스 구성 실패 **- HTTP** 오류

이 예에서 로그는 HTTP 오류 때문에 어플라이언스가 외부 위협 피드 소스에서 위협 피드를 가져올 수 없음을 보여줍니다.

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com , cause of failure: HTTP Error
```

해결책

웹 인터페이스에서 *Mail Policies(*메일 정책*)* > *External Threat Feeds Manager(*외부 위협 피드 관리자*)* 페이지로 이동하거나 CLI에서 `threatfeedsconfig > sourceconfig` 하위 명령을 사용하여 구성된 외부 위협 피드 소스의 폴링 경로 또는 사용자 인증 크리덴셜을 입력합니다.

ETF 소스 구성 실패 - 잘못된 URL

이 예에서 로그는 유효하지 않은 URL 때문에 어플라이언스가 외부 위협 피드 소스에서 위협 피드를 가져올 수 없음을 보여줍니다.

```
Info: THREAT_FEEDS: [TaxiiClient] Failed to poll threat feeds from following source:
hailataxii.com , cause of failure: HTTP Error
```

해결책

웹 인터페이스에서 *Mail Policies(*메일 정책*)* > *External Threat Feeds Manager(*외부 위협 피드 관리자*)* 페이지로 이동하거나 CLI에서 `threatfeedsconfig > sourceconfig` 하위 명령을 사용하여 구성된 외부 위협 피드 소스의 올바른 호스트 이름 또는 포트 번호를 입력합니다.

로그 서브스크립션

로그 서브스크립션 구성

System Administration(시스템 관리) 메뉴의 Log Subscriptions(로그 서브스크립션) 페이지(또는 CLI의 **`logconfig`** 명령)를 사용하여 로그 서브스크립션을 구성합니다. 로그 서브스크립션은 AsyncOS 활동에 대한 정보(오류 포함)를 저장하는 로그 파일을 생성합니다. 로그 서브스크립션은 검색되거나 다른 컴퓨터로 전달(푸시)됩니다. 일반적으로 로그 서브스크립션은 다음과 같은 특성을 가지고 있습니다.

표 ***141:*** 로그 파일 특성

속성	설명
Log type(로그 유형)	기록할 정보 유형 및 로그 서브스크립션의 형식을 정의합니다. 자세한 내용은 표: 로그 유형을 참고하십시오.
Log Name(로그 이름)	향후 참조를 위해 사용할 로그 서브스크립션의 별칭.
파일 이름	디스크에 기록할 때 파일의 물리적 이름에 사용됩니다. 여러 Email Security Appliance가 사용되고 있는 경우 로그 파일을 생성한 시스템을 식별하려면 로그 파일 이름이 고유해야 합니다.
Rollover by File Size(파일 크기별 롤오버)	롤오버 전에 파일이 도달할 수 있는 최대 크기.
Rollover by Time(시간별 롤오버)	파일 롤오버를 위한 시간 간격을 설정합니다.

속성	설명
속도 제한	지정된 시간 범위 내에서 로그 파일에 기록되는 최대 이벤트 수를 초 단위로 설정합니다. 기본 시간 범위 값은 10초입니다.
Log level(로그 레벨)	각 로그 서브스크립션을 위한 세부사항의 레벨을 설정합니다.
Retrieval method(검색 방법)	Email Security Appliance에서 로그 서브스크립션을 얻는 방법을 정의합니다.

로그 레벨

로그 레벨은 로그에서 전달하는 정보의 양을 결정합니다. 로그는 다섯 가지 세부사항 레벨 중 하나일 수 있습니다. 더 자세한 설정일수록 로그 파일 크기가 더 커지고 시스템 성능에도 더 많은 영향을 미칩니다. 더 자세한 설정에는 덜 자세한 설정에 포함된 모든 메시지 외에 추가 메시지가 포함됩니다. 세부사항 레벨이 높아질수록 시스템 성능이 저하됩니다.

참고 모든 메일 로그 유형에 대해 로그 레벨을 선택할 수 있습니다.

표 ***142:*** 로그 레벨

로그 레벨	설명
Critical(중대)	가장 덜 자세한 설정. 오류만 기록됩니다. 이 설정을 사용하면 성능 및 기타 중요한 활동을 모니터링할 수 없습니다. 그러나 로그 파일이 최대 크기에 빠르게 도달하지는 않습니다. 이 로그 레벨은 syslog 레벨 "Alert"과 같습니다.
경고	시스템에서 생성하는 모든 오류 및 경고. 이 설정을 사용하면 성능 및 기타 중요한 활동을 모니터링할 수 없습니다. 이 로그 레벨은 syslog 레벨 "Warning"과 같습니다.
정보	정보 설정은 연결 열기 또는 전달 시도 등 시스템 작동을 일일이 캡처합니다. Information(정보) 레벨은 로그에 대한 권장 설정입니다. 이 로그 레벨은 syslog 레벨 "Info"와 같습니다.
디버그	오류의 원인을 찾으려는 경우 디버그 로그 레벨을 사용합니다. 이 설정은 임시로 사용한 다음 기본 레벨로 돌려놓으십시오. 이 로그 레벨은 syslog 레벨 "Debug"와 같습니다.
추적	추적 로그 레벨은 개발자들에게만 권장됩니다. 이 레벨을 사용하면 시스템 성능이 심각하게 저하되므로 사용하지 않는 것이 좋습니다. 이 로그 레벨은 syslog 레벨 "Debug"와 같습니다.

GUI에서 로그 서브스크립션 만들기

단계 **1** **System Administration**(시스템 관리) **> Log Subscriptions**(로그 서브스크립션)를 선택합니다.

단계 **2** **Add Log Subscription**(로그 서브스크립션 추가)을 클릭합니다.

단계 **3** 로그 유형을 선택하고 로그 이름(로그 디렉터리의) 및 로그 파일 자체의 이름을 선택합니다.

단계 **4** AsyncOS가 로그 파일을 롤오버하기 전 최대 파일 크기 및 롤오버 사이의 시간 간격을 지정합니다. 로그 파일 롤오버에 대한 자세한 내용은 로그 서브스크립션 롤오버, 1109 페이지 섹션을 참조하십시오.

단계 **5** 로그 레벨을 선택합니다. 사용 가능한 옵션은 Critical(중대), Warning(경고), Information(정보), Debug(디버그) 또는 Trace(추적)입니다.

단계 **6** 로그 검색 방법을 구성합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

로그 서브스크립션 수정

단계 **1** **System Administration**(시스템 관리) **> Log Subscriptions**(로그 서브스크립션)를 선택합니다.

단계 **2** Log Settings(로그 설정) 열에서 로그의 이름을 클릭합니다.

단계 **3** 로그 서브스크립션을 변경합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

전역 로깅 설정 구성

텍스트 메일 로그 및 상태 로그 내에 시스템 측정이 주기적으로 기록됩니다. **System Administration**(시스템 관리) **> Log Subscriptions**(로그 서브스크립션) 페이지의 Global Settings(전역 설정) 섹션에 있는 **Edit Settings**(설정 수정) 버튼(또는 CLI의 `logconfig -> setup` 명령)을 사용하여 다음을 구성할 수 있습니다.

- 시스템 메트릭 빈도. 시스템이 측정 기록 간에 대기하는 시간(초)입니다.
- 메시지 ID 헤더의 기록 여부.
- 원격 응답 상태 코드의 기록 여부.
- 원본 메시지 제목 헤더의 기록 여부.
- 각 메시지에 대해 기록해야 할 헤더 목록.

모든 로그는 선택적으로 다음의 세 가지 데이터를 포함합니다.

1. 메시지 ID

   이 옵션이 구성되면 모든 메시지의 메시지 ID 헤더(사용 가능한 경우)가 기록됩니다. 이 메시지 ID는 수신된 메시지에서 올 수도 있고 AsyncOS 자체에서 생성될 수도 있습니다. 예를 들면 다음과 같습니다.

```
Tue Apr 6 14:38:34 2004 Info: MID 1 Message-ID Message-ID-Content
```

2. 원격 응답

   이 옵션이 구성되면 모든 메시지의 원격 응답 상태 코드(사용 가능한 경우)가 기록됩니다. 예를 들면 다음과 같습니다.

   ```
   Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
   ```

   원격 응답 문자열은 사람이 읽을 수 있는 텍스트로, 전달 SMTP 대화 중에 DATA 명령에 대한 응답 후 수신됩니다. 이 예에서 연결 호스트가 데이터 명령을 실행한 후 원격 응답은 "queued as 9C8B425DA7"입니다.

   ```
   [...]

   250 ok hostname

   250 Ok: queued as 9C8B425DA7
   ```

   문자열의 시작에서 공백, 구두점 및 OK 문자(250 응답의 경우)가 제거됩니다. 문자열의 끝에서는 공백만 제거됩니다. 예를 들어 Email Security Appliance는 기본적으로 "250 Ok: Message MID accepted" 문자열로 DATA 명령에 응답합니다. 따라서 원격 호스트가 또 다른 Email Security Appliance인 경우 "Message MID accepted" 문자열이 기록됩니다.

3. 원래 제목 헤더

   이 옵션이 활성화되면 각 메시지의 원래 제목 헤더가 로그에 포함됩니다.

   ```
   Tue May 31 09:20:27 2005 Info: Start MID 2 ICID 2

   Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 From: <mary@example.com>

   Tue May 31 09:20:27 2005 Info: MID 2 ICID 2 RID 0 To: <joe@example.com>

   Tue May 31 09:20:27 2005 Info: MID 2 Message-ID '<44e4n$2@example.com>'

   Tue May 31 09:20:27 2005 Info: MID 2 Subject 'Monthly Reports Due'
   ```

메시지 헤더 로깅

경우에 따라 메시지가 시스템을 통과할 때 메시지 헤더의 존재와 내용을 기록해야 합니다. Log Subscriptions Global Settings(로그 서브스크립션 전역 설정) 페이지에서(또는 CLI의 logconfig -> logheaders 하위 명령을 통해) 기록할 헤더를 지정합니다. Email Security Appliance는 지정된 메시지 헤더를 텍스트 메일 로그, 전달 로그 및 반송 로그에 기록합니다. 헤더가 있으면 시스템은 헤더의 이름과 값을 기록합니다. 헤더가 없으면 로그에 아무것도 기록되지 않습니다.

참고 시스템은 헤더에 대해 로깅이 지정되었는지와 상관없이 메시지 기록을 처리하는 동안 언제든지 메시지에 있는 모든 헤더를 평가합니다.

SMTP 프로토콜에 대한 RFC는 http://www.faqs.org/rfcs/rfc2821.html에 있으며 사용자 정의 헤더를 정의합니다.

logheaders 명령을 통해 기록할 헤더를 구성한 경우 전달 정보 후 헤더 정보가 나타납니다.

표 ***143:*** 헤더 로그

헤더 이름	헤더의 이름
값	로깅된 헤더의 내용

예를 들어, 로깅할 헤더로 "date, x-subject"를 지정하면 메일 로그에 다음 줄이 나타납니다.

```
Tue May 31 10:14:12 2005 Info: Message done DCID 0 MID 3 to RID [0]
[('date', 'Tue, 31 May 2005 10:13:18 -0700'), ('x-subject', 'Logging this header')]
```

GUI를 사용하여 로깅할 전역 설정 구성

단계 **1** **System Administration**(시스템 관리) > **Log Subscriptions**(로그 서브스크립션)를 선택합니다.

단계 **2** **Global Settings**(전역 설정) 섹션으로 스크롤합니다.

단계 **3** **Edit Settings**(설정 수정)를 클릭합니다.

단계 **4** 시스템 측정 빈도, 메일 로그에 메시지 ID 헤더를 포함할지 여부, 원격 응답을 포함할지 여부, 각 메시지의 원래 제목 헤더를 포함할지 여부 등의 정보를 지정합니다.

단계 **5** 로그에 포함할 다른 헤더를 입력합니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

로그 서브스크립션 롤오버

어플라이언스의 로그 파일이 너무 커지지 않게 하기 위해 AsyncOS는 "롤오버"를 수행하고, 로그 파일이 사용자 지정 최대 파일 크기 또는 시간 간격에 도달하면 로그 파일을 보관하고 수신 로그 데이터를 위한 새 파일을 만듭니다. 로그 서브스크립션을 위해 정의된 검색 방법을 기반으로 오래된 로그 파일은 검색을 위해 어플라이언스에 저장되거나 외부 컴퓨터로 전달됩니다. 어플라이언스에서 로그 파일을 검색하는 방법에 대한 자세한 내용은 로그 검색 방법, 1059 페이지 섹션을 참조하십시오.

AsyncOS는 로그 파일을 롤오버할 때 다음 작업을 수행합니다.

- 현재 로그 파일의 이름을 롤오버 타임스탬프와 저장된 상태를 의미하는 “**s**” 확장명으로 변경합니다.

- 새 로그 파일을 만들고 "**current**" 확장명으로 파일을 현재로 지정합니다.
- 새로 저장된 로그 파일을 원격 호스트로 전송합니다(푸시 기반 검색 방법을 사용하는 경우).
- 동일한 서브스크립션에서 전에 실패한 로그 파일을 전송합니다(푸시 기반 검색 방법을 사용하는 경우).
- 보관할 수 있는 총 파일 수가 초과된 경우 로그 서브스크립션에서 가장 오래된 파일을 삭제합니다(폴링 기반 검색 방법을 사용하는 경우).

GUI의 **System Administration(**시스템 관리**) > Log Subscriptions(**로그 서브스크립션**)** 페이지 또는 CLI의 logconfig 명령을 사용하여 서브스크립션을 만들거나 수정할 때 로그 서브스크립션의 롤오버 설정을 정의합니다. 로그 파일 롤오버를 트리거하는 데 사용할 수 있는 두 가지 설정은 다음과 같습니다.

- 최대 파일 크기
- 시간 간격

Rollover By File Size(파일 크기별 롤오버)

AsyncOS는 로그 파일이 최대 파일 크기에 도달하면 디스크 공간을 너무 많이 차지하는 것을 방지하기 위해 해당 파일을 롤오버합니다. 롤오버를 위한 최대 파일 크기를 정의할 때 메가바이트의 m과 킬로바이트의 k를 사용합니다. 예를 들어 로그 파일이 10메가바이트에 도달할 때 롤오버하려면 10m을 입력합니다.

Rollover By Time(시간별 롤오버)

롤오버가 정기적으로 이루어지도록 예약하려면 다음 시간 간격 중 하나를 선택할 수 있습니다.

- **None(**없음**).** AsyncOS는 로그 파일이 최대 파일 크기에 도달할 때만 롤오버를 수행합니다.
- **Custom Time Interval(**맞춤형 시간 간격**).** AsyncOS는 이전 롤오버 이후 지정된 시간이 지나면 롤오버를 수행합니다. 예약된 롤오버를 위한 맞춤형 시간 간격을 만들려면 d, h 및 m 접미사를 사용하여 롤오버 간 일, 시간, 분의 값을 입력합니다.
- **Daily Rollover(**매일 롤오버**).** AsyncOS는 지정된 시간에 매일 롤오버를 수행합니다. 매일 롤오버를 선택한 경우 24시간 형식(HH:MM)을 사용하여 AsyncOS가 롤오버를 수행할 시간을 입력합니다.

  Daily Rollover(매일 롤오버) 옵션은 GUI에서만 제공됩니다. CLI에서 logconfig 명령을 사용하여 매일 롤오버를 구성하려면 Weekly Rollover(매주 롤오버) 옵션을 선택하고 별표(*)를 사용하여 AsyncOS가 모든 요일에 롤오버를 수행하도록 지정합니다.

- **Weekly Rollover(**매주 롤오버**).** AsyncOS는 매주 하루 이상 지정된 시간에 롤오버를 수행합니다. 예를 들면 매주 수요일과 금요일 자정에 로그 파일을 롤오버하도록 AsyncOS를 설정할 수 있습니다. 매주 롤오버를 구성하려면 롤오버를 수행할 요일 및 24시간 형식(HH:MM)의 시간을 선택합니다.

  CLI를 사용하는 경우 요일 범위를 지정하려면 대시(-)를, 모든 요일을 지정하려면 별표(*)를, 여러 요일과 시간을 구분하려면 쉼표(,)를 사용합니다.

  다음 표에서는 CLI를 사용하여 수요일과 금요일 자정(00:00)에 로그 서브스크립션용 파일을 롤오버하는 방법을 보여줍니다.

표 ***144: CLI***에서 매주 로그 롤오버 설정

```
Do you want to configure time-based log files rollover? [N]> y

Configure log rollover settings:

1. Custom time interval.

2. Weekly rollover.

[1]> 2

1. Monday

2. Tuesday

3. Wednesday

4. Thursday

5. Friday

6. Saturday

7. Sunday

Choose the day of week to roll over the log files.  Separate multiple days with comma,

or use "*" to specify every day of a week.
Also you can use dash to specify a range like "1-5":

[]> 3, 5

Enter the time of day to rollover log files in 24-hour format (HH:MM).
You can specify hour as "*" to match every hour, the same for minutes.
Separate multiple times of day with comma:

[]> 00:00
```

온디맨드 방식의 로그 서브스크립션 롤오버

GUI를 사용하여 로그 서브스크립션을 즉시 롤오버하려면

단계 **1** System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션) 페이지에서 롤오버할 로그 오른쪽에 있는 확인란을 선택합니다.

단계 **2** 선택적으로, 모든 로그를 롤오버하려면 All(모두) 확인란을 선택할 수 있습니다.

단계 **3** 하나 이상의 로그를 롤오버하도록 선택하면 **Rollover Now(**지금 롤오버**)** 버튼이 활성화됩니다. 선택한 로그를 롤오버하려면 **Rollover Now(**지금 롤오버**)** 버튼을 클릭합니다.

GUI에서 최근 로그 항목 보기

시작하기 전에

GUI를 통해 로그를 보려면 Management 인터페이스에서 HTTP 또는 HTTPS 서비스를 활성화해야 합니다.

단계 **1** **System Administration(**시스템 관리**) > Log Subscriptions(**로그 서브스크립션**)**를 선택합니다.

단계 **2** 테이블의 **Log Files(**로그 파일**)** 열에 있는 로그 서브스크립션을 선택합니다.

단계 **3** 로그인합니다.

단계 **4** 브라우저에서 보거나 디스크에 저장할 로그 파일을 선택합니다.

CLI에서 최근 로그 항목 보기(tail 명령)

AsyncOS는 어플라이언스에 있는 구성된 로그의 최신 항목을 보여주는 tail 명령을 지원합니다. tail 명령을 실행하고 최근에 구성한 로그를 선택하여 확인합니다. tail 명령을 종료하려면 Ctrl-C를 사용합니다.

예

다음 예에서 tail 명령은 시스템 로그를 보는 데 사용됩니다. (이 로그는 무엇보다 commit 명령에서 오는 사용자 코멘트를 추적합니다.) 또한 tail 명령은 파라미터 tail mail_logs로 표시되는 로그의 이름을 수락합니다.

```
mail3.example.com> tail

Currently configured logs:


1. "antispam" Type: "Anti-Spam Logs" Retrieval: Manual Download

2. "antivirus" Type: "Anti-Virus Logs" Retrieval: Manual Download

3. "asarchive" Type: "Anti-Spam Archive" Retrieval: Manual Download

4. "authentication" Type: "Authentication Logs" Retrieval: Manual Download

5. "avarchive" Type: "Anti-Virus Archive" Retrieval: Manual Download
```

```
6. "bounces" Type: "Bounce Logs" Retrieval: Manual Download
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: Manual Download
8. "encryption" Type: "Encryption Logs" Retrieval: Manual Download
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: Manual Download
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: Manual Download
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: Manual Download
13. "gui_logs" Type: "HTTP Logs" Retrieval: Manual Download
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: Manual Download
15. "reportd_logs" Type: "Reporting Logs" Retrieval: Manual Download
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: Manual Download
17. "scanning" Type: "Scanning Logs" Retrieval: Manual Download
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: Manual Download
19. "sntpd_logs" Type: "NTP logs" Retrieval: Manual Download
20. "status" Type: "Status Logs" Retrieval: Manual Download
21. "system_logs" Type: "System Logs" Retrieval: Manual Download
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: Manual Download
23. "updater_logs" Type: "Updater Logs" Retrieval: Manual Download

Enter the number of the log you wish to tail.
[]> 19
Press Ctrl-C to stop.
Mon Feb 21 12:25:10 2011 Info: PID 274: User system commit changes: Automated Update for
Quarantine Delivery Host
Mon Feb 21 23:18:10 2011 Info: PID 19626: User admin commit changes:
Mon Feb 21 23:18:10 2011 Info: PID 274: User system commit changes: Updated filter logs
config
Mon Feb 21 23:46:06 2011 Info: PID 25696: User admin commit changes: Receiving
suspended.
^Cmail3.example.com>
```

호스트 키 구성

Email Security Appliance에서 다른 서버로 로그를 푸시할 때 SSH와 함께 사용할 호스트 키를 관리하려면 `logconfig -> hostkeyconfig` 하위 명령을 사용합니다. SSH 서버에는 호스트 키 쌍(개인 키 및

공개 키)이 있어야 합니다. 개인 호스트 키는 SSH 서버에 있으며 원격 시스템에서 읽을 수 없습니다. 공개 호스트 키는 SSH 서버와 상호 작용해야 할 클라이언트 시스템에 배포됩니다.

참고 사용자 키 관리에 대한 자세한 내용은 SSH(Secure Shell) 키 관리, 918 페이지 섹션을 참조하십시오.

`hostkeyconfig` 하위 명령은 다음 기능을 수행합니다.

표 ***145:*** 호스트 키 관리 - 하위 명령 목록

Command(명령**)**	설명
New	새 키를 추가합니다.
Edit	기존 키를 수정합니다.
Delete	기존 키를 삭제합니다.
Scan	호스트 키를 자동으로 다운로드합니다.
Print	키를 표시합니다.
Host	시스템 호스트 키를 표시합니다. 이 값은 원격 시스템의 'known_hosts' 파일에 저장됩니다.
Fingerprint	시스템 호스트 키 지문을 표시합니다.
User	로그를 원격 시스템으로 푸시하는 시스템 계정의 공개 키를 표시합니다. 이것은 SCP 푸시 서브스크립션을 설정할 때 표시되는 것과 동일한 키입니다. 이 값은 원격 시스템의 'authorized_keys' 파일에 저장됩니다.

다음 예에서 AsyncOS는 호스트 키를 검사하고 호스트에 대해 추가합니다.

```
mail3.example.com> logconfig

Currently configured logs:

[ list of logs ]

Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- SETUP - General settings.

- LOGHEADERS - Configure headers to log.

- HOSTKEYCONFIG - Configure SSH host keys.

[]> hostkeyconfig
```

```
Currently installed host keys:
1. mail3.example.com ssh-dss [ key displayed ]
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> scan
Please enter the host or IP address to lookup.
[]> mail3.example.com
Choose the ssh protocol type:
1. SSH1:rsa
2. SSH2:rsa
3. SSH2:dsa
4. All
[4]>
SSH2:dsa
mail3.example.com ssh-dss
[ key displayed ]
SSH2:rsa
mail3.example.com ssh-rsa
[ key displayed ]
SSH1:rsa
mail3.example.com 1024 35
[ key displayed ]

Add the preceding host key(s) for mail3.example.com? [Y]>
Currently installed host keys:
```

```
1. mail3.example.com ssh-dss [ key displayed ]

2. mail3.example.com ssh-rsa [ key displayed ]

3. mail3.example.com 1024 35 [ key displayed ]

Choose the operation you want to perform:

- NEW - Add a new key.

- EDIT - Modify a key.

- DELETE - Remove a key.

- SCAN - Automatically download a host key.

- PRINT - Display a key.

- HOST - Display system host keys.

- FINGERPRINT - Display system host key fingerprints.

- USER - Display system user keys.

[]>

Currently configured logs:

[ list of configured logs ]

Choose the operation you want to perform:

- NEW - Create a new log.

- EDIT - Modify a log subscription.

- DELETE - Remove a log subscription.

- SETUP - General settings.

- LOGHEADERS - Configure headers to log.

- HOSTKEYCONFIG - Configure SSH host keys.

[]>
```

42 장

클러스터를 사용한 중앙 집중식 관리

이 장에는 다음 섹션이 포함되어 있습니다.

클러스터를 사용한 중앙 집중식 관리 개요

Cisco 중앙 집중식 관리 기능을 사용하면 여러 어플라이언스를 동시에 관리 및 구성함으로써 관리 시간을 줄이고 네트워크 전체에서 일관된 구성을 보장할 수 있습니다. 여러 어플라이언스를 관리하기 위한 추가 하드웨어를 구매할 필요가 없습니다. 중앙 집중식 관리 기능을 통해 네트워크 내에서 신뢰성, 유연성 및 확장성이 향상되므로, 로컬 정책을 준수하는 한편 전역적인 관리를 수행할 수 있습니다.

컨피그레이션 정보를 공유하는 시스템(machine) 집합으로서 클러스터가 정의됩니다. 클러스터 내에서 시스템(Cisco 어플라이언스)은 그룹으로 나뉩니다. 모든 클러스터에는 그룹이 하나 이상 포함됩니다. 특정 시스템은 한 그룹의 구성원이며 한 그룹에만 속합니다. 관리자 사용자는 클러스터 전체, 그룹 전체 또는 시스템 단위로 서로 다른 요소를 구성함으로써 네트워크, 지리, 사업 부서 또는 기타 논리적 관계를 기반으로 Cisco 어플라이언스의 세그멘테이션을 활성화할 수 있습니다.

클러스터는 *peer-to-peer* 아키텍처로 구현되며, 클러스터 내에는 마스터/슬레이브 관계가 없습니다. 클러스터를 제어 및 관리할 시스템에 로그인할 수 있습니다. (그러나 일부 컨피그레이션 명령은 제한됩니다. 제한되는 명령, 1131 페이지 섹션을 참조해 주십시오.)

사용자 데이터베이스는 클러스터의 모든 시스템에서 공유됩니다. 즉, 전체 클러스터에 하나의 사용자 집합 및 단일 관리자 사용자(연결된 암호 사용)만 있습니다. 클러스터에 속한 모든 시스템은 클러스터의 관리자 암호라는 단일 관리자 암호를 공유합니다.

참고 클러스터에 있는 어플라이언스 수가 20개를 넘으면 클러스터 통신에서 오류가 발생할 수 있습니다.

클러스터 요구 사항

- 클러스터의 시스템은 DNS에서 확인 가능한 호스트 이름을 가지고 있어야 합니다. 또는 IP 주소를 대신 사용할 수 있지만 두 가지를 혼용할 수는 없습니다.

  DNS 및 호스트 이름 확인, 1135 페이지를 참조하십시오. 클러스터 통신은 일반적으로 시스템의 DNS 호스트 이름을 사용하여 시작됩니다.

- 클러스터는 동일한 AsyncOS 버전을 실행하는 시스템으로만 구성해야 합니다.

  클러스터 구성원을 업그레이드하는 방법은 클러스터에서 시스템 업그레이드, 1129 페이지 섹션을 참조해 주십시오.

- SSH(일반적으로 포트 22) 또는 CCS(Cluster Communication Service)를 통해 클러스터에 시스템을 추가할 수 있습니다.

  클러스터 통신, 1135 페이지를 참조하십시오.

- 클러스터에 추가된 시스템은 SSH 또는 CCS(Cluster Communication Service)를 통해 통신할 수 있습니다. 사용 포트는 구성 가능합니다. SSH는 일반적으로 포트 22에서 활성화되고 CCS의 포트는 기본적으로 2222이지만, 이러한 서비스를 다른 포트에 구성할 수도 있습니다.

  어플라이언스에 대해 열려 있어야 하는 일반 방화벽 포트 외에도 CCS를 통해 통신하는 클러스터링된 시스템은 CCS 포트를 통해 상호 연결할 수 있어야 합니다. 클러스터 통신, 1135 페이지를 참조하십시오.

- 시스템의 클러스터 만들기, 가입 또는 구성을 수행하려면 CLI(Command Line Interface) 명령 **`clusterconfig`**를 사용해야 합니다.

  클러스터를 만들었으면 GUI 또는 CLI에서 클러스터 외의 구성 설정을 관리할 수 있습니다.

  클러스터 만들기 및 가입, 1120 페이지 및 GUI에서 클러스터 관리, 1132 페이지를 참조하십시오.

- 어플라이언스에서 이중 인증을 활성화한 경우 사전 공유 키를 사용하여 클러스터 컴퓨터에 가입시킬 수 있습니다. 이 설정을 구성하려면 CLI에서 `clusterconfig > prepjoin` 명령을 사용합니다.

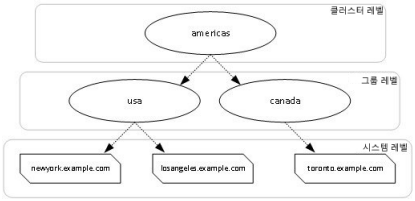
  또는

  클러스터를 생성하거나 클러스터에 가입하기 전에 Email Security Appliance에서 이중 인증을 비활성화합니다. 자세한 내용은 이중 인증 비활성화, 913 페이지를 참고하십시오.

클러스터 조직

클러스터 내의 구성 정보는 3개의 그룹 또는 수준으로 나뉩니다. 상위 레벨은 클러스터 설정을, 중간 레벨은 그룹 설정을, 하위 레벨은 시스템 관련 설정을 설명합니다.

그림 ***78:*** 클러스터 레벨 계층 구조



각 레벨 내에는 설정을 구성할 수 있는 하나 이상의 특정 구성원이 있는데, 이를 모드라고 합니다. 모드란 지정된 레벨에 있는 명명된 구성원을 가리킵니다. 예를 들어 "usa" 그룹은 다이어그램에 있는 두 그룹 모드 중 하나를 나타냅니다. 레벨은 일반적인 용어이지만 모드는 구체적입니다. 모드는 항상 이름으로 참조됩니다. 위 그림에 나와 있는 클러스터에는 6개 모드가 있습니다.

설정은 특정 레벨에서 구성되지만 항상 특정 모드에 대해 구성됩니다. 한 레벨 내 모든 모드에 대해 설정을 구성할 필요는 없습니다. 클러스터 모드는 특수한 경우입니다. 클러스터는 하나뿐이므로 클러스터 모드에 대해 구성된 모든 설정은 클러스터 레벨에서 구성된다고 말할 수 있습니다.

일반적으로 대부분의 설정을 클러스터 레벨에서 구성해야 합니다. 그러나 더 낮은 레벨에서 구체적으로 구성된 설정은 더 높은 레벨에서 구성된 설정을 재정의합니다. 따라서 그룹 모드(group-mode) 또는 시스템 모드(machine-mode) 설정으로 클러스터 모드(cluster-mode) 설정을 재정의할 수 있습니다.

예를 들어 클러스터 모드에서 Good Neighbor Table을 구성하며 시작할 수 있습니다. 클러스터의 모든 시스템은 해당 컨피그레이션을 사용합니다. 그런 다음 시스템 모드에서 newyork 시스템에 사용하도록 이 테이블을 구성할 수도 있습니다. 이 경우 클러스터의 다른 모든 머신은 클러스터 수준에서 정의된 양호한 인접 테이블을 사용하지만, newyork 머신은 클러스터 설정을 개별 머신 모드 설정으로 재정의합니다.

특정 그룹 또는 시스템에 대해 클러스터 설정을 덮어쓸 수 있는 기능은 뛰어난 유연성을 제공합니다. 시스템 모드에서 개별적으로 많은 설정을 구성하는 경우 클러스터에서 제공할 수 있는 관리 편의성을 상당 부분 놓치게 됩니다.

초기 컨피그레이션 설정

대부분의 기능에서 새 모드에 대한 설정을 구성하기 시작할 때 이러한 설정은 처음에 기본적으로 비어 있습니다. 모드에서 설정이 비어 있는 것과 없는 것에는 차이가 있습니다. 예를 들어 그룹 하나와 시스템 하나로 구성된 매우 간단한 클러스터가 있다고 가정해보겠습니다. 클러스터 레벨에서 LDAP 쿼리를 구성했다면 그룹 또는 시스템 레벨에서는 구성된 설정이 없는 것입니다.

Cluster	(ldap queries: a, b, c)
Group	

Machine	

이제 그룹에 대해 새로운 LDAP 쿼리 설정을 만들면 다음과 같은 상태가 됩니다.

Cluster	(ldap queries: a, b, c)
Group	(ldap queries: None)
Machine	

그룹 레벨 설정은 클러스터 레벨 설정을 재정의하지만, 새 그룹 설정은 처음에 비어 있습니다. 그룹 모드에는 실제로 자체적으로 구성된 LDAP 쿼리가 없습니다. 이 그룹 내 시스템은 그룹에서 LDAP 쿼리의 "빈" 집합을 상속합니다.

이제 다음과 같이 그룹에 LDAP 쿼리를 추가할 수 있습니다.

Cluster	(ldap queries: a, b, c)
Group	(ldap queries: d)
Machine	

이제 클러스터 레벨에도 쿼리 집합 하나가 구성되어 있고 그룹에도 또 다른 쿼리 집합이 있습니다. 시스템은 그룹에서 쿼리를 상속합니다.

클러스터 만들기 및 가입

GUI(Graphical User Interface)에서는 클러스터 만들기 또는 가입을 수행할 수 없습니다. 시스템의 클러스터 만들기, 가입 또는 구성을 수행하려면 CLI(Command Line Interface)를 사용해야 합니다. 클러스터를 만들었으면 GUI 또는 CLI에서 컨피그레이션 설정을 변경할 수 있습니다.

⚠

주의 어플라이언스에서 이중 인증을 활성화한 경우 사전 공유 키를 사용하여 클러스터 컴퓨터에 가입시킬 수 있습니다. 이 설정을 구성하려면 CLI에서 `clusterconfig > prepjoin` 명령을 사용합니다.

또는

클러스터를 생성하거나 클러스터에 가입하기 전에 Email Security Appliance에서 이중 인증을 비활성화합니다. 자세한 내용은 이중 인증 비활성화, 913 페이지를 참고하십시오.

clusterconfig 명령

시스템은 `clusterconfig` 명령을 통해 클러스터를 만들거나 클러스터에 가입할 수 있습니다.

- 새 클러스터를 만들면 해당 클러스터의 모든 초기 설정이 클러스터를 만든 시스템에서 상속됩니다. 시스템이 전에 "독립형" 모드로 구성된 경우, 클러스터를 만들면 해당 독립형 설정이 사용됩니다.

- 시스템이 클러스터에 가입하면 해당 시스템의 클러스터 가능한 설정은 모두 클러스터 레벨에서 상속됩니다. 다시 말해서, 특정 시스템 관련 설정(예: IP 주소)을 제외한 모든 것이 손실되고 클러스터 및/또는 해당 시스템이 가입하기 위해 선택한 그룹의 설정으로 교체됩니다. 시스템이 전에 "독립형" 모드로 구성된 경우 클러스터를 만들면 해당 독립형 설정이 사용되며, 시스템 레벨의 설정은 아무것도 유지되지 않습니다.

현재 시스템이 아직 클러스터에 속하지 않은 경우 `clusterconfig` 명령을 실행하면 기존 클러스터에 가입할지 새 클러스터를 만들지에 대한 옵션이 표시됩니다.

이 시점에서 새 클러스터에 시스템을 추가할 수 있습니다. 이러한 시스템은 SSH 또는 CCS를 통해 통신할 수 있습니다.

```
newyork.example.com> clusterconfig

Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 2

Enter the name of the new cluster.

[]> americas

New cluster committed: Wed Jun 22 10:02:04 2005 PDT

Creating a cluster takes effect immediately, there is no need to commit.

Cluster americas

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>
```

기존 클러스터에 가입

클러스터에 추가하려는 호스트에서 clusterconfig 명령을 실행하여 기존 클러스터에 가입합니다. SSH 또는 CCS(cluster communication service)를 통해 클러스터에 가입할 수 있습니다 .

호스트를 기존 클러스터에 추가하려면

- 클러스터에 있는 시스템의 SSH 호스트 키를 검증할 수 있어야 합니다.
- 클러스터에 있는 시스템의 IP 주소를 알아야 하며 클러스터에서 이 시스템에 연결할 수 있어야 합니다(예: SSH 또는 CCS를 통해).
- 클러스터에 속한 시스템에서 admin 사용자에 대한 관리자 암호를 알아야 합니다.

SSH를 통해 기존 클러스터에 가입

다음은 SSH 옵션을 사용하여 losangeles.example.com 시스템을 클러스터에 추가하는 방법을 보여줍니다.

```
losangeles.example.com> clusterconfig


Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 3


While joining a cluster, you will need to validate the SSH host key of the remote
machine to which you are joining. To get the public host key

fingerprint of the remote host, connect to the cluster and run: logconfig ->
hostkeyconfig -> fingerprint.


WARNING: All non-network settings will be lost. System will inherit the values set at
the group or cluster mode for the non-network settings. Ensure that the cluster
settings are compatible with your network settings (e.g. dnsconfig settings)

Do you want to enable the Cluster Communication Service on
losangeles.example.com? [N]> n

Enter the IP address of a machine in the cluster.

[]> IP address is entered

Enter the remote port to connect to. The must be the normal admin ssh
port, not the CCS port.

[22]> 22

Enter the admin passphrase for the cluster.
The administrator passphrase for the clustered machine is entered

Please verify the SSH host key for IP address:
```

```
Public host key fingerprint: xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx

Is this a valid key for this host? [Y]> y

Joining cluster group Main_Group.

Joining a cluster takes effect immediately, there is no need to commit.

Cluster americas

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>

(Cluster americas)>
```

CCS를 통해 기존 클러스터에 가입

SSH를 사용할 수 없는 경우 SSH 대신 CCS를 사용합니다. CCS의 유일한 장점은 클러스터 통신이 해당 포트를 통해서만 발생한다는 것입니다(사용자 로그인, SCP 등 없음). CCS를 통해 기존 클러스터에 또 다른 시스템을 추가하려면 clusterconfig의 `prepjoin` 하위 명령을 사용하여 클러스터에 추가할 시스템을 준비합니다. 이 예에서는 newyork 시스템에서 `prepjoin` 명령을 실행하여 losangeles 시스템을 클러스터에 추가하도록 준비합니다.

`prepjoin` 명령에는 호스트의 CLI에서 `clusterconfig prepjoin print`를 입력하여 클러스터에 추가할 호스트의 사용자 키를 가져와서 현재 클러스터에 있는 호스트의 명령줄에 복사하는 작업이 포함됩니다.

시스템이 이미 클러스터의 일부인 경우 `clusterconfig` 명령을 사용하면 클러스터의 여러 설정을 구성할 수 있습니다.

```
Choose the operation you want to perform:


- ADDGROUP - Add a cluster group.
```

```
- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]> prepjoin

Prepare Cluster Join Over CCS

No host entries waiting to be added to the cluster.

Choose the operation you want to perform:

- NEW - Add a new host that will join the cluster.

[]> new

Enter the hostname of the system you want to add.

[]> losangeles.example.com

Enter the serial number of the host mail3.example.com.

[]> unique serial number is added

Enter the user key of the host losangeles.example.com. This can be obtained by typing
"clusterconfig prepjoin print" in the CLI on mail3.example.com. Press enter on a blank
line to finish.


unique user key from output of prepjoin print is pasted

Host losangeles.example.com added.

Prepare Cluster Join Over CCS

1. losangeles.example.com (serial-number)

Choose the operation you want to perform:

- NEW - Add a new host that will join the cluster.

- DELETE - Remove a host from the pending join list.

[]>


(Cluster Americas)> clusterconfig

Cluster americas
```

```
Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>
```

사전 공유 키를 사용하여 **SSH**를 통해 기존 클러스터에 가입

다음 표는 사전 공유 키를 사용하여 SSH를 통해 시스템(testmachine.example.com)을 클러스터(test_cluster)에 가입시키는 방법을 보여줍니다.

```
testmachine.example.com> clusterconfig


Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 3


While joining a cluster, you will need to validate the SSH host key of the remote
machine to which you are joining. To get the public host key

fingerprint of the remote host, connect to the cluster and run: logconfig ->
hostkeyconfig -> fingerprint.


WARNING: All non-network settings will be lost. System will inherit the values set at
the group or cluster mode for the non-network settings. Ensure that the cluster
settings are compatible with your network settings (e.g. dnsconfig settings)

Do you want to enable the Cluster Communication Service on
testmachine.example.com? [N]>
```

```
Enter the IP address of a machine in the cluster.

[]> IP address entered

Enter the remote port to connect to. The must be the normal admin ssh
port, not the CCS port.

[22]>

Would you like to join this appliance to a cluster using pre-shared keys?
Use this option if you have enabled two-factor authentication on the appliance.) [Y]> yes

To join this appliance to a cluster using pre-shared keys, log in to the cluster machine,
run the clusterconfig > prepjoin > command, enter the
following details, and commit your changes.
Host: pod1226-esa07.ibesa
Serial Number: 42291A18D741EDB4C601-BC14E5579F34
User Key:

ssh-dss
AAAAB3NzaC1kc3MAAACBAJ6Xm+ja4aau9n4DOcJs/gGwEDEUWgERYchhgWApKt6IW+s58I7knGM81rQgQbNdNCO58D
EqaVGmP0Vyb0TTpgvh6f0mr80OuTgWh9bqg4uiOJvbKvlTvDt0o7//mTklm159zr2KT/qFH+9L5i+8iIMX62R5y+a
6E8JV0BrJCNAAAAFQCmK+WOu9HSribsC0f/5dVoADdxEwAAAIA5p7NR74rlSrs0JWWYItNAtE1SamAN+gqCOdUWGPPHT
qdrtBIlPQ9tfFoThZElqY4Tx8lku9laasoRLruQ2Z36R3bQGzIn4jzQqujvvbxTvLK9eLoSr8yFbEE3ZvuUo0+vhDn
LIDX2N65AQSQsTaOrKX+yQZ8yAVt48CsctpsDrgAAAIAVROGlWoSl8g3FFm2eRTa+/oZ+cMjv+pSZiZoiUCoaIlouc
u1ZDpN413QBnf6p/3D8wVD8m5uo8O4N/HXasAMektZvGoP4Sf+shItPuISRv3lrMTEYsD0sqVcMc7vIXUeD2jpOk7MB
ooVkTZB/rdTbNMfXrhDkNJ2IAPQQiUKVnw==

Before you proceed to the next step, make sure you add the 'Host', Serial Number' and 'User
Key'
details to the cluster machine.

Would you like to continue? [Y]> yes

Joining cluster group Main_Group.

Joining a cluster takes effect immediately, there is no need to commit.

Cluster test_cluster

Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.
```

```
[]>

(Cluster test_cluster)>
```

그룹 추가

모든 클러스터에는 그룹이 하나 이상 포함되어야 합니다. 새 클러스터를 만들면 **Main_Group**이라는 기본 그룹이 자동으로 만들어집니다. 그러나 클러스터 내에 그룹을 더 만들 수도 있습니다. 다음 예는 기존 클러스터 내에서 추가 그룹을 만들고 새 그룹에 시스템을 할당하는 방법을 보여줍니다.

단계 **1** **clusterconfig** 명령을 실행합니다.

단계 **2** **addgroup** 하위 명령을 선택하고 새 그룹의 이름을 입력합니다.

단계 **3** **setgroup** 하위 명령을 사용하여 새 그룹에 대한 시스템을 선택합니다.

클러스터 관리

CLI에서 클러스터 관리

클러스터에 속해 있는 머신의 경우 CLI를 다른 모드로 전환할 수 있습니다. 다시 설명하지만, 모드란 레벨의 명명된 특정 구성원을 가리킵니다.

CLI 모드는 컨피그레이션을 정확히 어디에서 수정할지를 결정합니다. 기본값은 사용자가 로그인한 시스템인 "login host"에 대한 "machine" 모드입니다.

서로 다른 모드 간에 전환하려면 clustermode 명령을 사용합니다.

표 ***146:*** 클러스터 관리

명령 예	설명
`clustermode`	클러스터 모드를 전환하기 위한 프롬프트
`clustermode group northamerica`	"northamerica"라는 그룹에 대한 그룹 모드로 전환
`clustermode machine losangeles.example.com`	"losangeles" 시스템에 대한 시스템 모드로 전환

현재 모드를 나타내도록 CLI의 프롬프트가 변경됩니다.

```
(Cluster Americas)>
```

또는

```
(Machine losangeles.example.com)>
```

시스템 모드에서 프롬프트는 시스템의 인증된 도메인 이름을 포함합니다.

설정 복사 및 이동

모든 제한 없는(제한되는 명령, 1131 페이지 참고) 명령에는 **CLUSTERSHOW** 및 **CLUSTERSET**라는 새 작업이 있습니다. **CLUSTERSHOW**는 명령이 구성된 모드를 표시하는 데 사용됩니다(추가된 새 작업 , 1130 페이지 참조). **CLUSTERSET** 작업을 사용하면 한 모드에서 다른 모드로 또는 레벨 간(예: 시스템에서 그룹으로)에 현재 설정(현재 명령으로 구성 가능)을 이동하거나 복사할 수 있습니다.

복사는 현재 모드에 대한 설정을 유지합니다. 이동은 현재 모드의 컨피그레이션을 재설정합니다(지웁니다). 즉, 이동하면 현재 모드에 대해 어떤 설정도 구성되지 않습니다.

예를 들어 **northamerica** 그룹에 대해 Good Neighbor Table 설정(**destconfig** 명령)을 구성했으며 전체 클러스터에서 이 설정을 공유하려는 경우, **destconfig** 명령 내에서 **clusterset** 작업을 사용하여 현재 설정을 클러스터 모드로 복사(또는 이동)할 수 있습니다. (새 컨피그레이션으로 실험, 1128 페이지 참조.)

⚠

주의 일관성 없는 종속성을 피하려면 컨피그레이션 설정을 이동하거나 복사할 때 주의를 기울여야 합니다. 예를 들어 면책조항 스탬프가 구성된 리스너를 또 다른 시스템으로 이동하거나 복사하는 경우 새로운 시스템에 동일한 면책조항이 구성되어 있지 않으면, 새 시스템에서는 면책조항 스탬프가 활성화되지 않습니다.

새 컨피그레이션으로 실험

클러스터를 사용하는 가장 유용한 방법 중 하나는 새 컨피그레이션 설정으로 실험해보는 것입니다. 먼저 독립된 환경을 마련하여 시스템 모드에서 설정을 변경합니다. 컨피그레이션이 만족스러우면 해당 컨피그레이션 변경 사항을 클러스터 모드로 이동하여 모든 시스템에서 사용할 수 있도록 합니다.

다음 예는 한 시스템에서 리스너 설정을 변경한 다음 준비가 되면 클러스터의 나머지로 설정을 게시하는 단계를 보여줍니다. 리스너는 일반적으로 클러스터 레벨에서 구성되므로, 다음 예는 설정을 변경 및 테스트하기 전에 컨피그레이션을 한 시스템의 시스템 모드로 가져오는 것으로 시작됩니다. 클러스터의 다른 시스템에 변경 사항을 적용하기 전에 한 시스템에서 이 유형의 실험적 변경 사항을 테스트해야 합니다.

단계 **1** **clustermode cluster** 명령을 사용하여 클러스터 모드로 변경합니다.

clustermode 명령은 모드를 클러스터, 그룹 및 시스템 레벨로 변경하기 위해 사용하는 CLI 명령입니다.

단계 **2** **listenerconfig**를 입력하여 클러스터에 대해 구성된 리스너 설정을 표시합니다.

단계 **3** 실험하기 위한 머신을 선택한 다음 clusterset 명령을 사용하여 클러스터에서 머신 모드로 설정을 복사합니다.

단계 **4** clustermode 명령을 사용하여 실험적 머신의 머신 모드로 이동합니다. 예를 들면 다음과 같습니다.

```
clustermode machine newyork.example.com
```

단계 **5** 시스템 모드의 실험용 시스템에서 listenerconfig 명령을 실행하여 실험용 시스템에 맞게 구체적으로 변경합니다.

단계 **6** 변경 사항을 커밋합니다.

단계 **7** 변경 사항을 커밋해야 한다는 점을 기억하면서, 실험용 시스템에서 계속해서 컨피그레이션 변경을 실험합니다.

단계 **8** 새 설정을 모든 시스템에 적용할 준비가 되면 clusterset 명령을 사용하여 설정을 클러스터 모드로 이동합니다.

단계 **9** 변경 사항을 커밋합니다.

클러스터에서 영구적으로 나가기(제거)

클러스터에서 시스템을 영구적으로 제거하려면 clusterconfig의 REMOVEMACHINE 작업을 사용합니다. 클러스터에서 시스템이 영구적으로 제거되면 컨피그레이션이 "플랫화"되어, 해당 시스템은 클러스터의 일부였을 때와 동일하게 작동하게 됩니다. 예를 들어 클러스터 모드의 Global Unsubscribe 테이블만 있는 경우, 클러스터에서 시스템이 제거될 때 Global Unsubscribe 테이블 데이터가 시스템의 로컬 컨피그레이션으로 복사됩니다.

클러스터에서 시스템 업그레이드

클러스터는 연결된 시스템에서 AsyncOS의 서로 다른 버전을 허용하지 않습니다.

AsyncOS 업그레이드를 설치하기 전에 clusterconfig 명령을 통해 클러스터에서 각 시스템의 연결을 끊어야 합니다. 모든 시스템을 업그레이드하면 clusterconfig 명령을 통해 클러스터를 다시 연결해야 합니다. 시스템을 동일한 버전으로 업그레이드하는 동안 별개의 두 클러스터를 실행할 수 있습니다. GUI의 Upgrades(업그레이드) 페이지에서 클러스터링된 시스템을 업그레이드할 수도 있습니다.

업그레이드를 설치할 준비가 될 때까지 클러스터 시스템의 연결을 끊을 필요가 없도록 업그레이드를 백그라운드에서 다운로드할 수 있습니다.

참고 사용자가 클러스터에서 개별 시스템의 연결을 끊기 전에 업그레이드 명령을 사용하는 경우, AsyncOS는 클러스터에 있는 모든 시스템의 연결을 끊습니다. Cisco Systems에서는 업그레이드하기 전에 클러스터에서 각 시스템의 연결을 끊을 것을 권장합니다. 그러면 각 시스템에 대한 연결 끊기 및 업그레이드가 수행될 때까지 나머지 시스템은 클러스터에서 계속해서 작동할 수 있습니다.

단계 **1** 클러스터의 시스템에서 clusterconfig의 disconnect 작업을 사용합니다. 예를 들어 losangeles.example.com 시스템의 연결을 끊으려면 clusterconfig disconnectlosangeles.example.com을 입력합니다. 커밋(commit)은 필요하지 않습니다.

단계 **2** suspendlistener 명령을 사용하여 선택적으로 업그레이드 프로세스 중에 새 연결 및 메시지의 수락을 중지합니다.

단계 **3** upgrade 명령을 실행하여 AsyncOS를 신규 버전으로 업그레이드합니다.

참고 클러스터에서 모든 시스템의 연결을 끊는다는 경고 또는 확인 프롬프트를 모두 무시하십시오. 해당 시스템의 연결을 끊었으므로 AsyncOS는 현 시점에서 클러스터에 있는 다른 시스템의 연결을 끊지 않습니다.

단계 **4** 시스템의 AsyncOS 버전을 선택합니다. 업그레이드가 완료되면 시스템이 재부팅됩니다.

단계 **5** 업그레이드된 머신에서 새 메시지를 수락하도록 resume 명령을 실행합니다.

단계 **6** 클러스터의 각 시스템에 대해 1~5단계를 반복합니다.

참고 클러스터에서 시스템의 연결을 끊으면 다른 시스템의 컨피그레이션을 변경하기 위해 해당 시스템을 사용할 수 없습니다. 클러스터 컨피그레이션을 수정할 수는 있지만, 설정이 비동기화될 수 있으므로 다른 시스템의 연결이 끊어진 동안에는 설정을 변경하지 마십시오.

단계 **7** 모든 시스템의 업그레이드가 완료되면 업그레이드된 각 시스템에서 clusterconfig의 reconnect 작업을 사용하여 다시 연결합니다. 예를 들어 losangeles.example.com 시스템을 다시 연결하려면 clusterconfig reconnectlosangeles.example.com을 입력합니다. AsyncOS의 동일한 버전을 실행 중인 클러스터에만 시스템을 연결할 수 있습니다.

CLI 명령 지원

모든 명령은 클러스터 인식

AsyncOS의 모든 CLI 명령은 이제 클러스터를 인식합니다. 일부 명령의 동작은 클러스터 모드에서 실행하는 경우 약간 변경됩니다. 예를 들어, 클러스터에 속한 시스템에서 실행하는 경우 다음 명령의 동작이 변경됩니다.

commit 및 clearchanges 명령

commit

사용자가 현재 어떤 모드에 있든, commit 명령은 클러스터의 세 레벨 모두에 대한 모든 변경 사항을 커밋합니다.

commitdetail

commitdetail 명령은 구성 변경사항이 클러스터 내 모든 머신으로 전파되면 그에 대한 세부사항을 제공합니다.

clearchanges

사용자가 현재 어떤 모드에 있든, clearchanges(clear) 명령은 클러스터의 세 레벨 모두에 대한 모든 변경 사항을 지웁니다.

추가된 새 작업

CLUSTERSHOW

이제 각 명령 내에 CLUSTERSHOW 작업이 있어서, 명령이 어떤 모드에서 구성되고 있는지를 알 수 있습니다.

더 낮은 레벨의 기존 설정에 의해 재정의될 작업을 수행하기 위해 CLI 명령을 입력하는 경우 알림이 표시됩니다. 예를 들어 클러스터 모드에서 명령을 입력하면 다음과 같은 알림이 표시될 수 있습니다.

```
Note: Changes to these settings will not affect the following groups and machines
because they are overriding the cluster-wide settings:

East_Coast, West_Coast

facilities_A, facilities_B, receiving_A
```

그룹 모드에 대한 설정을 수정하는 경우에도 유사한 메시지가 출력될 수 있습니다.

제한되는 명령

대부분의 CLI 명령 및 해당 GUI 페이지는 클러스터, 그룹, 시스템 등 어떤 모드에서나 실행 가능합니다. 그러나 일부 명령 및 페이지는 한 모드로만 제한됩니다.

시스템 인터페이스(GUI 및 CLI)는 명령이 제한된다는 점과 어떻게 제한되는지를 항상 분명하게 알려줍니다. 명령을 구성하기 위한 적절한 모드로 손쉽게 전환할 수 있습니다.

- GUI에서 모드를 전환하려면 "Change Mode(모드 변경)" 메뉴 또는 "Settings for this features are currently defined at(이 기능에 대한 설정이 현재 정의된 곳):" 링크를 사용합니다.
- CLI에서 모드를 전환하려면 clustermode 명령을 사용합니다.

표 ***147:*** 클러스터 모드로 제한되는 명령

clusterconfig	sshconfig
clustercheck	userconfig
passwd	

그룹 또는 시스템 모드에서 이러한 명령 중 하나를 실행하려고 하면 경고 메시지와 함께 적절한 모드로 전환할 수 있는 프롬프트가 표시됩니다.

참고 passwd 명령은 게스트 사용자가 사용할 수 있어야 하므로 특수한 경우입니다. 게스트 사용자가 클러스터의 머신에서 passwd 명령을 실행하는 경우, 경고 메시지가 출력되지 않는 대신 사용자 모드가 변경하지 않고 클러스터 수준 데이터에서 자동으로 동작합니다. 다른 모든 사용자에게는 위에서 설명한 동작이 수행됩니다(다른 제한되는 컨피그레이션 명령과 같음).

다음 명령은 시스템 모드로 제한됩니다.

antispamstatus	etherconfig	resume	suspenddel
antispamupdate	featurekey	resumedel	suspendlistener
antivirusstatus	hostrate	resumelistener	techsupport
antivirusupdate	hoststatus	rollovernow	tophosts

bouncerecipients	interfaceconfig	routeconfig	topin
deleterecipients	ldapflush	sbstatus	trace
delivernow	ldaptest	setgateway	version
diagnostic	nslookup	sethostname	vofflush
dnsflush	quarantineconfig	settime	vofstatus
dnslistflush	rate	shutdown	workqueue
dnslisttest	reboot	status	
dnsstatus	resetcounters	suspend	

클러스터 또는 그룹 모드에서 이러한 명령 중 하나를 실행하려고 하면 경고 메시지와 함께 적절한 모드로 전환할 수 있는 프롬프트가 표시됩니다.

다음 명령은 더 나아가 로그인 호스트(즉 로그온한 특정 시스템)로 제한됩니다. 이러한 명령을 실행하려면 로컬 파일 시스템에 액세스해야 합니다.

표 ***148:*** 로그인 호스트 모드로 제한되는 명령

last	resetconfig	tail	upgrade
ping	supportrequest	텔넷(telnet)	who

GUI에서 클러스터 관리

GUI(**clusterconfig** 명령에 해당)에서 클러스터 만들기나 가입을 수행하거나 클러스터 전용 설정을 관리할 수는 없지만, 클러스터에서 시스템을 탐색할 수 있으며, GUI 내부에서 설정을 생성 및 삭제하거나 클러스터, 그룹 및 시스템 간에 설정을 복사 및 이동(**clustermode** 및 **clusterset** 명령에 해당하는 작업 수행)할 수 있습니다.

표시되는 Mail Flow Monitoring(메일 플로우 모니터링) 데이터는 로컬 시스템에 저장되므로 Incoming Mail Overview(수신 메일 개요) 페이지는 로그인 호스트로 제한되는 명령의 예입니다. 다른 시스템에 대한 Incoming Mail Overview(수신 메일 개요) 보고서를 보려면 해당 시스템의 GUI에 로그인해야 합니다.

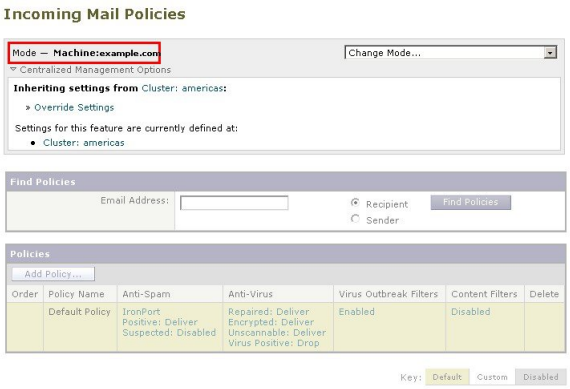
어플라이언스에서 클러스터링이 활성화되었을 때 브라우저 주소 필드의 URL을 적어두십시오. 이 URL에는 **machine, group** 또는 **cluster**라는 단어가 적절히 포함됩니다. 예를 들어 처음 로그인하면 Incoming Mail Overview(수신 메일 개요) 페이지의 URL은 다음과 같습니다.

https:// *hostname***machine**/*serial_number* **/monitor/incoming_mail_overview**

참고 Monitor(모니터) 메뉴의 Incoming Mail Overview(수신 메일 개요) 및 Incoming Mail Details(수신 메일 세부사항) 페이지는 로그인 시스템으로 제한됩니다.

Mail Policies(메일 정책), Security Services(보안 서비스), Network(네트워크) 및 System Administration(시스템 관리) 탭에는 로컬 시스템으로 제한되지 않은 페이지가 포함되어 있습니다. Mail Policies(메일 정책) 탭을 클릭하면 GUI의 중앙 집중식 관리 정보가 변경됩니다.

그림 ***79: GUI***의 중앙 집중식 관리 기능*:* 정의된 설정 없음



위 그림에서 시스템은 현재 기능에 대한 모든 구성 설정을 클러스터 모드에서 상속합니다. 상속되는 설정은 밝은 회색(미리 보기)으로 표시되어 있습니다. 이러한 설정을 유지할 수도 있고, 이 시스템에 대한 클러스터 레벨 설정을 재정의하도록 변경할 수도 있습니다.

참고 상속된 설정(미리 보기 표시)은 항상 클러스터에서 상속된 설정을 표시합니다. 그룹 및 클러스터 레벨에서 의존적인 서비스를 활성화 또는 비활성화할 때는 각별히 유의해야 합니다. 자세한 내용은 설정 복사 및 이동, 1128 페이지를 참고해 주십시오.

Override Settings(설정 재정의) 링크를 클릭하면 해당 기능의 새 페이지가 표시됩니다. 이 페이지에서 시스템 모드에 대한 새 컨피그레이션 설정을 만들 수 있습니다. 기본 설정으로 시작할 수도 있고, 다른 모드에서 이미 설정을 구성한 경우 이를 현재 시스템으로 복사할 수도 있습니다.

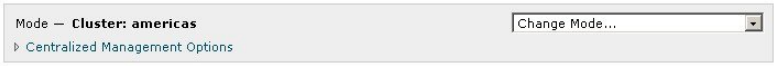
그림 ***80: GUI***의 중앙 집중식 관리 기능*:* 새 설정 만들기

또는 그림 - *GUI*의 중앙 집중식 관리 기능*:* 정의된 설정 없음에 표시된 대로, 이 구성 설정이 이미 정의된 모드로 이동할 수도 있습니다. 모드는 중앙 집중식 관리 상자의 하단, "Settings for this feature are currently defined at(이 기능에 대한 설정이 현재 정의된 곳):" 아래에 나열됩니다. 설정이 실제로 정의

된 모드만 여기에 나열됩니다. 다른 모드에서 정의되거나 다른 모드에서 상속된 설정에 대한 페이지를 볼 때에는 해당 설정이 페이지에 표시됩니다.

나열된 모드 중 하나를 클릭하면(예: 그림 - *GUI*의 중앙 집중식 관리 기능: 정의된 설정 없음에 나와 있는 Cluster: Americas 링크) 해당 모드에 대한 설정을 보고 관리할 수 있는 새 페이지가 표시됩니다.

그림 ***81: GUI***의 중앙 집중식 관리 기능*:* 정의된 설정



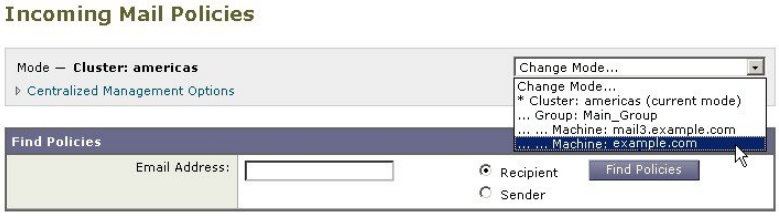
특정 모드에 대한 설정이 정의되면 모든 페이지에 중앙 집중식 관리 상자가 최소화된 상태로 표시됩니다. 현재 페이지와 관련하여 현재 모드에서 사용 가능한 옵션 리스트를 표시하려면 "Centralized Management Options(중앙 집중식 관리 옵션)" 링크를 클릭하여 상자를 확장합니다. "Manage Settings(설정 관리)" 버튼을 클릭하면 현재 설정을 다른 모드로 복사 또는 이동하거나 완전히 삭제할 수 있습니다.

예를 들어 다음 그림에서는 Centralized Management Options(중앙 집중식 관리 옵션) 링크를 클릭하여 사용 가능한 옵션을 표시했습니다.

그림 ***82: GUI***의 중앙 집중식 관리 기능*:* 설정 관리

상자의 오른쪽에는 "Change Mode(모드 변경)" 메뉴가 있습니다. 이 메뉴에는 현재 모드가 표시되며, 이를 통해 언제든지 다른 모드(클러스터, 그룹 또는 시스템)로 이동할 수 있습니다.

그림 ***83: Change Mode(***모드 변경*)* 메뉴



다른 모드를 표시하는 페이지로 이동하면 중앙 집중식 관리 상자 왼쪽에 있는 "Mode —" 텍스트가 노란색으로 잠시 깜박이며 모드가 변경되었음을 알려줍니다.

특정 탭 내에 있는 일부 페이지는 시스템 모드로 제한됩니다. 그러나 현재 로그인 호스트로 제한되는 Incoming Mail Overview(수신 메일 개요) 페이지와는 달리 이러한 페이지는 클러스터의 어떤 시스템에서도 사용할 수 있습니다.

그림 ***84:*** 중앙 집중식 관리 기능*:* 제한되는 시스템

Change Mode(모드 변경) 메뉴에서 관리할 시스템을 선택합니다. 모드가 변경되었음을 알리는 텍스트가 잠시 깜박이는 것을 볼 수 있습니다.

클러스터 통신

클러스터 내 시스템은 메시 네트워크를 사용하여 서로 통신합니다. 기본적으로 모든 시스템은 다른 모든 시스템과 연결됩니다. 링크 하나가 비활성화되면 다른 시스템들은 업데이트를 수신하지 못하게 됩니다.

기본적으로 모든 클러스터 간 통신은 SSH로 보호됩니다. 각 시스템은 경로 테이블의 복사본을 메모리에 보관하며, 링크가 활성화 또는 비활성화되면 필요에 따라 메모리를 변경합니다. 또한 각 시스템은 클러스터에 있는 다른 모든 시스템에 대해 주기적으로 "ping"(1분마다)을 수행합니다. 이렇게 함으로써 최신 링크 상태를 확인하고 라우터 또는 NAT가 시간 초과될 때 연결을 유지할 수 있습니다.

참고 어플라이언스가 클러스터 모드에 있는 경우 다른 어플라이언스의 원격 데이터(격리에 있는 메시지를 보거나 빠른 속도로 보고서를 새로 고치는 등 구성과 관련 없는 데이터) 액세스를 계획합니다. 알림과 오류를 생성할 수 있는 클러스터 재연결 시도가 발생합니다. 어플라이언스는 자동으로 다시 연결되므로 수동 개입이 필요하지 않습니다.

DNS 및 호스트 이름 확인

DNS는 클러스터에 시스템을 연결하는 데 필요합니다. 클러스터 통신은 일반적으로 시스템의 DNS 호스트 이름(시스템에 있는 인터페이스의 호스트 이름이 아니라)을 사용하여 시작됩니다. 확인할 수 없는 호스트 이름의 시스템은 기술적으로 클러스터의 일부일지라도 실제로 클러스터의 다른 시스템과 통신할 수 없습니다.

호스트 이름이 SSH 또는 CCS가 활성화된 어플라이언스의 올바른 IP 인터페이스를 가리키도록 DNS를 구성해야 합니다. 이 점은 매우 중요합니다. DNS가 SSH 또는 CCS가 활성화되지 않은 다른 IP 주소를 가리키는 경우 호스트를 찾을 수 없습니다. 중앙 집중식 관리는 인터페이스별 호스트 이름이 아니라 sethostname 명령으로 설정된 "기본 호스트 이름"을 사용합니다.

IP 주소를 사용하여 클러스터의 다른 시스템에 연결하는 경우, 해당 시스템은 연결하는 IP 주소를 역방향으로 조회할 수 있어야 합니다. IP 주소가 DNS에 없어서 역방향 조회가 시간 초과되면 해당 시스템은 클러스터에 연결할 수 없습니다.

클러스터링, 인증된 도메인 이름 및 업그레이드

DNS를 변경하면 AsyncOS 업그레이드 후 연결이 손실될 수 있습니다. 클러스터에 있는 시스템의 인터페이스 호스트 이름이 아니라 클러스터에 있는 시스템의 인증된 도메인 이름을 변경해야 하는 경우, sethostname을 통해 호스트 이름 설정을 변경한 후 AsyncOS를 업그레이드하기 전에 해당 시스템의 DNS 기록을 업데이트해야 합니다.

CCS(Cluster Communication Security)

CCS(Cluster Communication Security)는 일반 SSH 서비스와 유사한 보안 셸 서비스입니다. Cisco는 클러스터 통신에서 일반 SSH를 사용하는 것과 관련된 우려에 대응하여 CCS를 구현했습니다. 두 시스템 간 SSH 통신은 동일한 포트에서 일반 로그인(admin 등)을 엽니다. 클러스터링된 시스템에서 일반 로그인을 여는 것을 선호하지 않는 관리자가 많습니다.

팁: 일부 클러스터링된 시스템 간에 포트 22를 차단하는 방화벽이 없다면 CCS(Cluster Communication Security) 서비스가 기본값이더라도 이를 활성화하지 마십시오. 클러스터링은 포트 22에서 모든 시스템 간에 완전한 SSH 터널 메시를 사용합니다. CCS 활성화에 대해 Yes로 답한 시스템이 이미 있는 경우 클러스터에서 모든 시스템을 제거한 후 다시 시작하십시오. 클러스터에서 마지막 시스템을 제거하면 클러스터가 제거됩니다.

CCS는 관리자가 클러스터 통신을 열지만 CLI 로그인은 열지 않을 수 있는 향상된 기능을 제공합니다. 기본적으로 이 서비스는 비활성화되어 있습니다. 다른 서비스의 활성화 여부를 묻는 프롬프트가 표시될 때 interfaceconfig 명령에서 CSS 활성화에 대한 프롬프트가 표시됩니다. 예를 들면 다음과 같습니다.

```
Do you want to enable SSH on this interface? [Y]>

Which port do you want to use for SSH?

[22]>

Do you want to enable Cluster Communication Service on this interface?

[N]> y

Which port do you want to use for Cluster Communication Service?

[2222]>
```

CCS에 대한 기본 포트 번호는 2222입니다. 원하는 경우 사용되지 않은 다른 열린 포트로 변경할 수 있습니다. 가입이 완료되고 가입한 시스템에 클러스터의 모든 컨피그레이션 데이터가 상속되면 다음과 같은 질문이 표시됩니다.

```
Do you want to enable Cluster Communication Service on this interface? [N]> y


Which port do you want to use for Cluster Communication Service?

[2222]>
```

클러스터 일관성

"클러스터를 인식"하는 시스템은 클러스터 내 다른 시스템에 대한 네트워크 연결을 계속해서 확인합니다. 이 확인은 클러스터 내 다른 시스템에 주기적으로 "ping"을 전송하여 수행됩니다.

특정 시스템과의 통신 시도가 모두 실패하면, 통신을 시도한 시스템은 원격 호스트의 연결이 끊어졌다는 메시지를 로깅합니다. 시스템은 관리자에게 원격 호스트가 다운되었다는 경고문을 전송합니다.

시스템이 다운되어도 확인 ping은 계속 전송됩니다. 시스템이 클러스터 네트워크에 다시 가입하면 오프라인 상태였던 시스템이 업데이트를 다운로드할 수 있도록 동기화 명령이 실행됩니다. 동기화

명령은 또한 일부 시스템에서만 변경된 내용이 있는지를 확인합니다. 그런 경우 다운되었던 시스템은 업데이트를 자동으로 다운로드합니다.

연결 끊기/다시 연결

클러스터에서 시스템의 연결이 끊어질 수 있습니다. 경우에 따라 고의로 시스템의 연결을 끊을 수도 있습니다(예: 시스템 업그레이드를 위해). 사고로 연결이 끊어질 수도 있습니다(예: 정전 또는 기타 소프트웨어/하드웨어 오류). 한 어플라이언스가 세션에서 허용되는 최대 SSH 연결 수를 초과하여 연결하려고 시도하는 경우 연결이 끊어질 수 있습니다. 클러스터에서 연결이 끊어진 시스템에 여전히 직접 액세스해서 구성할 수 있습니다. 그러나 연결이 끊긴 시스템을 다시 연결할 때까지는 변경 사항이 다른 시스템에 전파되지 않습니다.

클러스터에 다시 연결된 시스템은 동시에 모든 시스템에 다시 연결하려고 시도합니다.

이론적으로 연결이 끊어진 클러스터의 두 시스템은 해당 로컬 데이터베이스에 대해 동시에 유사한 변경 사항을 커밋할 수 있습니다. 시스템이 클러스터에 다시 연결되면 이러한 변경 사항을 동기화하려는 시도가 이루어집니다. 충돌이 있는 경우 최신 변경 사항이 기록됩니다(다른 변경 사항 대체).

커밋 중에 어플라이언스는 변경 중인 모든 변수를 확인합니다. 커밋 데이터에는 버전 정보, 시퀀스 식별 번호 및 비교 가능한 기타 정보가 포함됩니다. 변경하려는 정보가 이전 변경 사항과 충돌하는 것이 발견되면 변경을 취소할 수 있는 옵션이 제공됩니다. 예를 들면 다음과 같은 내용이 표시될 수 있습니다.

```
(Machine mail3.example.com)> clustercheck

This command is restricted to "cluster" mode. Would you like to switch to "cluster"

mode? [Y]> y

Checking Listeners (including HAT, RAT, bounce profiles)...

Inconsistency found!

Listeners (including HAT, RAT, bounce profiles) at Cluster enterprise:

mail3.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on

mail3.example.com

test.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on

mail3.example.com

How do you want to resolve this inconsistency?

1. Force entire cluster to use test.example.com version.


2. Force entire cluster to use mail3.example.com version.

3. Ignore.

[1]>
```

변경을 취소하지 않도록 선택하면 변경 사항이 그대로 유지되지만 커밋되지는 않습니다. 변경 사항을 현재 설정과 비교해보고 처리 방법을 결정할 수 있습니다.

언제든 `clustercheck` 명령을 사용하여 클러스터가 올바르게 작동하는지 확인할 수 있습니다.

```
losangeles> clustercheck

Do you want to check the config consistency across all machines in the cluster? [Y]> y

Checking losangeles...

Checking newyork...

No inconsistencies found.
```

상호 의존적인 설정

Cloud Email Security Appliance에서는 다음과 같은 설정을 구성하지 않는 것이 좋습니다.

중앙에서 관리되는 환경에서는 일부 상호 의존적인 설정이 서로 다른 모드에서 구성됩니다. 구성 모델의 유연성 덕분에 여러 모드에서 설정을 구성할 수 있으며, 각 시스템에 어떤 설정이 사용될지는 상속 규칙으로 결정됩니다. 그러나 일부 설정은 다른 설정에 의존하며, 의존적인 설정의 컨피그레이션 가용성은 동일한 모드의 설정으로 제한되지 않습니다. 따라서 다른 레벨의 특정 시스템에 대해 구성된 설정을 참조하는 한 레벨의 설정을 구성할 수 있습니다.

상호 의존적인 설정의 가장 일반적인 예는 다른 클러스터 섹션에서 데이터를 가져오는 페이지의 특정 필드입니다. 예를 들면 다음 기능을 서로 다른 모드에서 구성할 수 있습니다.

- LDAP 쿼리 사용
- 사전 또는 텍스트 리소스 사용
- 반송 또는 SMTP 인증 프로필 사용

중앙 집중식 관리 내에는 제한되는 명령 및 제한 없는 명령이 있습니다. (제한되는 명령, 1131 페이지 참조.) 제한 없는 명령은 일반적으로 클러스터에서 공유할 수 있는 컨피그레이션 명령입니다.

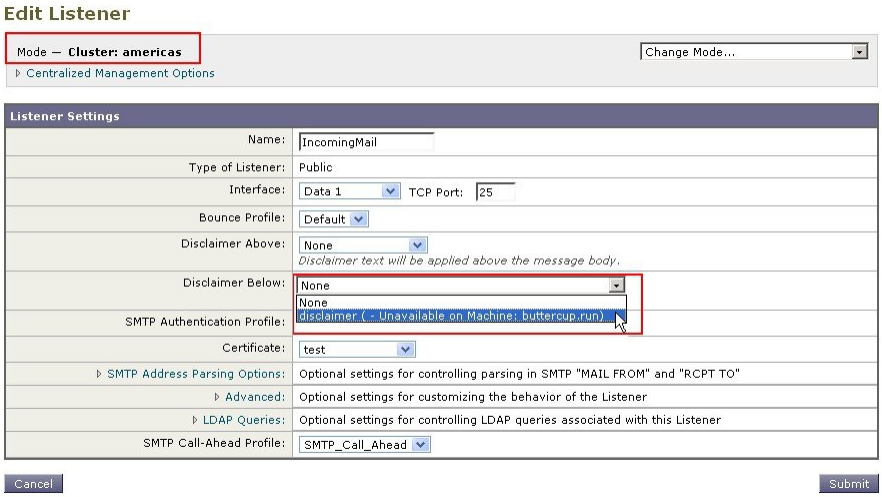
`listenerconfig` 명령은 클러스터의 모든 시스템에 대해 구성할 수 있는 명령의 예입니다. 제한 없는 명령은 클러스터의 모든 시스템에서 반복할 수 있으며 시스템 단위로 데이터를 수정할 필요가 없는 명령을 말합니다.

반면 제한되는 명령은 특정 모드에만 적용되는 명령입니다. 예를 들어, 사용자는 여러 시스템에 대해 구성할 수 없으며 전체 클러스터에서 한 사용자만 설정할 수 있습니다. 그렇지 않으면 동일한 로그인으로 원격 시스템에 로그인하는 것이 불가능할 것입니다. 마찬가지로 Mail Flow Monitor(메일 플로우 모니터) 데이터, System Overview(시스템 개요) 카운터 및 로그 파일은 시스템 단위로만 유지 관리되므로 이러한 명령 및 페이지는 특정 시스템으로 제한됩니다.

Scheduled Reports(예약된 보고서)는 전체 클러스터에서 동일하게 구성할 수 있지만 보고서 보기는 시스템마다 다르다는 것을 알 수 있습니다. 따라서 GUI의 단일 Scheduled Reports(예약된 보고서) 페이지 내에서, 컨피그레이션은 클러스터 모드에서 수행해야 하지만 보고서 보기는 시스템 모드에서 수행해야 합니다.

System Time(시스템 시간) 페이지는 **`settz`**, **`ntpconfig`** 및 **`settime`** 명령을 포함하므로, 제한되는 명령과 제한 없는 명령이 혼합되어 나타납니다. 이 경우 settime은 시스템 전용 모드로 제한되는 반면(시간 설정은 시스템마다 다르므로), **`settz`** 및 **`ntpconfig`**는 클러스터 또는 그룹 모드에서 구성할 수 있습니다.

그림 ***85:*** 상호 의존적인 설정의 예



위의 예에서 "IncomingMail" 리스너는 시스템 레벨에서만 구성된 "disclaimer"라는 이름의 바닥글을 참조합니다. 사용 가능한 바닥글 리소스의 드롭다운 리스트를 보면, 역시 클러스터에서 사용 가능한 "buttercup.run" 시스템에서는 바닥글을 사용할 수 없음을 알 수 있습니다. 이 딜레마를 해결하기 위한 두 가지 방법이 있습니다.

- "disclaimer" 바닥글을 시스템 레벨에서 클러스터 레벨로 올리기
- 리스너를 시스템 레벨로 내려 상호 의존성 제거하기

중앙에서 관리되는 시스템의 기능을 최대한 활용하려면 첫 번째 방법이 더 좋습니다. 클러스터링된 시스템의 컨피그레이션을 맞춤화하므로 설정 간 상호 의존성에 유의해야 합니다.

클러스터링된 어플라이언스에서 컨피그레이션 로드

AsyncOS에서는 클러스터링된 어플라이언스에서 클러스터 컨피그레이션을 로드할 수 있습니다. 다음과 같은 시나리오에서 클러스터 컨피그레이션을 로드할 수 있습니다.

- 온프레미스 환경에서 호스팅된 환경으로 마이그레이션 중이며, 온프레미스 클러스터 컨피그레이션을 호스팅된 환경으로 마이그레이션하려는 경우
- 클러스터의 어플라이언스가 다운되었거나 어플라이언스를 중단해야 하며, 이 어플라이언스에서 클러스터에 추가할 계획인 새 어플라이언스로 컨피그레이션을 로드하려는 경우
- 클러스터에 어플라이언스를 더 추가하고 있으며, 클러스터에 있는 기존 어플라이언스 중 하나에서 새로 추가된 어플라이언스로 컨피그레이션을 로드하려는 경우
- 백업 컨피그레이션을 클러스터로 로드하려는 경우

요구 사항에 따라 유효한 클러스터 컨피그레이션 파일로부터 클러스터 컨피그레이션 또는 어플라이언스 컨피그레이션을 로드할 수 있습니다.

참고 클러스터링된 어플라이언스에서 독립형 어플라이언스의 컨피그레이션은 로드할 수 없습니다.

시작하기 전에

- 유효하며 완전한 XML 컨피그레이션이 있는지 확인합니다. 구성 파일 로드, 937 페이지를 참조하십시오.
- 컨피그레이션을 로드할 대상 어플라이언스의 현재 컨피그레이션을 백업합니다. 현재 구성 파일 저장 및 내보내기, 936 페이지를 참조하십시오.
- 사용하려는 모든 어플라이언스로 클러스터 설정을 만듭니다. 클러스터 만들기 및 가입, 1120 페이지를 참조하십시오.

참고 모든 어플라이언스를 한 그룹에 둘 수 있습니다. 설정에서 클러스터 통신에 사용할 인터페이스가 XML 컨피그레이션과 동일한 이름 및 SSH/CCS 설정을 가지고 있는지 확인합니다.

단계 **1** **System Administration**(시스템 관리) > **Configuration File**(컨피그레이션 파일)을 클릭합니다.

단계 **2** **Mode**(모드) 드롭다운 메뉴에서 클러스터를 선택합니다.

단계 **3** 클러스터 컨피그레이션을 로드할지 어플라이언스 컨피그레이션을 로드할지에 따라 다음 중 하나를 수행합니다.

- 클러스터 컨피그레이션 로드

  1. Load Configuration(컨피그레이션 로드) 섹션의 드롭다운 리스트에서 **Cluster**(클러스터)를 선택합니다.
  2. 클러스터 컨피그레이션을 로드하고 **Load**(로드)를 클릭합니다. 구성 파일 로드, 937 페이지를 참조하십시오.
  3. 로드된 컨피그레이션에서 클러스터의 어플라이언스로 그룹을 할당하고, 선택한 그룹의 어플라이언스에서 개별 어플라이언스로 어플라이언스 컨피그레이션을 복사합니다. **Group Configuration**(그룹 컨피그레이션) 및 **Appliance Configuration**(어플라이언스 컨피그레이션) 드롭다운 리스트를 사용합니다.

     어플라이언스 컨피그레이션을 복사하지 않으려면 **Appliance Configuration**(어플라이언스 컨피그레이션) 드롭다운 리스트에서 **Don't Copy**(복사하지 않음)를 선택합니다.

     1. 구성을 검토합니다. **Review**(검토)를 클릭합니다.
     2. **OK**(확인)를 클릭합니다.
     3. **Continue**(계속)를 클릭합니다.

- 어플라이언스 컨피그레이션 로드

  1. Load Configuration(구성 로드) 섹션의 드롭다운 리스트에서 **Appliance in cluster**(클러스터의 어플라이언스)를 선택합니다.
  2. 컨피그레이션을 로드하고 **Load**(로드)를 클릭합니다. 구성 파일 로드, 937 페이지를 참조하십시오. 클러스터링된 어플라이언스에서 독립형 어플라이언스의 컨피그레이션을 로드할 수는 없습니다.
  3. 로드된 컨피그레이션에서 어플라이언스 컨피그레이션을 선택하고, 컨피그레이션을 로드할 클러스터의 원하는 어플라이언스를 선택합니다. 드롭다운 리스트를 사용합니다.
  4. **OK**(확인)를 클릭합니다.
  5. **Continue**(계속)를 클릭합니다.
  6. 어플라이언스 구성을 더 많은 어플라이언스로 로드하려면 **a~e** 단계를 반복합니다.

단계 **4** 클러스터링된 어플라이언스의 네트워크 설정을 검토하고 변경 사항을 커밋합니다.

모범 사례 및 FAQ

모범 사례

클러스터를 만들면, 현재 로그인해 있는 시스템이 첫 번째 시스템으로서 클러스터에 자동으로 추가되고 Main_Group에도 추가됩니다. 시스템 레벨 설정이 클러스터 레벨로 최대한 효과적으로 이동합니다. 그룹 레벨에는 설정이 없으며, 클러스터 레벨에서 의미가 없으며 클러스터링할 수 없는 설정만 시스템 레벨에 남게 됩니다. 예를 들면 IP 주소, 기능 키 등입니다.

가능한 한 많은 설정을 클러스터 레벨에 남겨두십시오. 클러스터의 한 시스템에만 다른 설정이 필요하면 해당 클러스터 설정을 해당 시스템의 시스템 레벨로 복사하십시오. 해당 설정을 이동하지 마십시오. 공장 기본값이 없는 설정(예: HAT 테이블, SMTPROUTES 테이블, LDAP 서버 프로필 등)을 이동하면, 클러스터 설정을 상속하는 시스템은 빈 테이블을 갖게 되며 이메일을 처리하지 못하게 될 것입니다.

해당 시스템에서 클러스터 설정을 다시 상속하도록 하려면 CM 설정을 관리하고 시스템 설정을 삭제하십시오. 다음이 표시되어야 비로소 시스템이 클러스터 설정을 재정의한 것을 알게 될 것입니다.

Settings are defined:

To inherit settings from a higher level: Delete Settings for this feature at this mode.

You can also Manage Settings.

Settings for this feature are also defined at:

Cluster: xxx

또는 다음 내용입니다.

Delete settings from:

Cluster: xxx

Machine: yyyy.domain.com

복사와 이동 비교

복사해야 하는 경우: 설정을 클러스터에 두고, 그룹 또는 시스템에는 설정을 두지 않거나 다른 설정을 두려는 경우

이동해야 하는 경우: 클러스터에 설정을 전혀 두지 않고, 그룹 또는 시스템에 설정을 두려는 경우

뛰어난 CM 설계 연습

CM 시스템을 나열(LIST)하면 다음과 같은 내용이 표시됩니다.

cluster = CompanyName

Group Main_Group:

Machine lab1.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab2.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Group Paris:

Machine lab3.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab4.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Group Rome:

Machine lab5.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Machine lab6.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

변경을 수행하는 레벨의 추적을 놓치지 않도록 주의해 주십시오. 예를 들어 Main_Group의 이름을 London으로 변경한 경우(RENAMEGROUP 사용) 다음과 같이 표시됩니다.

cluster = CompanyName

Group London:

Machine lab1.cable.nu (Serial #: 000F1FF7B3F0-CF2SX51)

...

그러나 이 컨피그레이션은 London 시스템에 대한 변경을 그룹 레벨에서 시작하며 기본 설정에 대한 일반 컨피그레이션 레벨로서 클러스터 레벨을 사용하여 중지하기 때문에 많은 관리자에게 혼동을 줄 수 있습니다.

팁: 클러스터와 그룹에 동일한 이름을 사용하는 것은 좋지 않습니다(예: 클러스터 London, 그룹 London). 그룹 이름에 사이트 이름을 사용하는 경우, 위치를 가리키는 클러스터 이름을 사용하는 것은 좋지 않습니다.

위에서 설명한 대로, 올바른 방법은 가능한 한 많은 설정을 클러스터 레벨에 남겨두는 것입니다. 대부분의 경우 기본 사이트 또는 주요 시스템 모음을 Main_Group에 남겨두고, 추가 사이트에 대해 그룹을 사용해야 합니다. 두 사이트가 "동급"이라고 생각하는 경우에도 마찬가지입니다. CM에는 기본/보조 또는 마스터/슬레이브 서버가 없으며, 모든 시스템이 피어(peer)임을 기억하십시오.

팁: 추가 그룹을 사용하려는 경우, 해당 추가 시스템을 클러스터에 가입시키기 전에 손쉽게 그룹을 준비할 수 있습니다.

클러스터 설정의 스팸 또는 정책 격리에 액세스하기 위한 모범 사례

로그인한 어플라이언스에서 클러스터에 있는 다른 어플라이언스의 스팸 또는 정책 격리에 액세스하면, 로그인한 어플라이언스에서 과도한 CPU 사용이 발생할 수 있습니다. 이러한 시나리오를 피하려면 각각의 어플라이언스에 로그인하여 스팸 또는 정책 격리에 액세스할 수 있습니다.

절차: 클러스터 예 구성

이 클러스터 예를 구성하려면 clusterconfig를 실행하기 전에 모든 시스템의 모든 GUI에서 로그아웃합니다. 기본 사이트 머신 중 한 곳에서 clusterconfig를 실행합니다. 그런 다음 설정을 최대한 많이 공유해야 하는 기타 로컬 및 원격 시스템(시스템에는 IP 주소 같은 설정만 남겨둠)을 이 클러스터에 가입시킵니다. clusterconfig 명령은 원격 머신을 클러스터에 조인시키는 데 사용할 수 없습니다. 원격 머신에서는 CLI를 사용하여 clusterconfig("기존 클러스터에 조인")를 실행해야 합니다.

위의 예에서는 lab1에 로그인하고 clusterconfig를 실행한 다음 CompanyName이라는 클러스터를 생성합니다. 요구 사항이 동일한 하나의 시스템만 있으므로, lab2에 로그인하고, saveconfig로 기존 컨피그레이션을 저장합니다(lab1 설정을 대부분 상속할 경우 크게 변경될 것입니다). 그런 다음 lab2에서 clusterconfig를 사용하여 기존 클러스터에 가입할 수 있습니다. 이 사이트에 유사한 정책 및 설정이 필요한 추가 시스템이 있는 경우 이 과정을 반복합니다.

CONNSTATUS를 실행하여 DNS가 올바르게 확인되었는지 확인합니다. 시스템이 클러스터에 가입됨에 따라, 새로운 시스템은 lab1에서 거의 모든 설정을 상속하고 이전 설정은 손실됩니다. 이들이 프로덕션 시스템인 경우, 이전 컨피그레이션이 아니라 새 컨피그레이션을 사용하여 메일이 여전히 처리되는지 확인해야 합니다. 클러스터에서 제거하는 경우 이전의 프라이빗 컨피그레이션으로 돌아가지 않습니다.

이제 예외적인 시스템의 수를 계산합니다. 하나뿐인 경우, 여기에서 몇몇 별도의 시스템 레벨 설정을 수신해야 하며 사용자는 이에 대한 별도의 그룹을 만들어야 합니다. 이 시스템을 클러스터에 가입시키고 시스템 레벨로 설정 복사를 시작합니다. 이 시스템이 기존의 프로덕션 시스템인 경우 컨피그레이션을 백업해야 하며, 위와 같이 메일 처리를 변경할 것을 고려해야 합니다.

예외적인 시스템이 둘 이상인 경우 이 예에서와 같이, 클러스터와 공유되지 않은 설정을 두 개의 해당 시스템이 서로 공유할지를 결정합니다. 이 경우 하나 이상의 그룹을 만들어야 합니다. 그렇지 않으면 각각에 대해 시스템 레벨 설정을 만들어야 하며, 별도의 그룹을 만들 필요는 없습니다.

이 경우에는 이미 클러스터에 있는 시스템 중 하나에서 CLI의 clusterconfig를 실행하고 ADDGROUP을 선택합니다. 이 작업을 Paris와 Rome에 각각 한 번씩 모두 두 번 수행합니다.

이제 GUI 및 CLI를 사용하여 클러스터 및 모든 그룹(그룹에 아직 시스템이 없더라도)에 대한 컨피그레이션 설정을 구성하기 시작할 수 있습니다. 시스템에 대한 전용 설정은 시스템이 클러스터에 가입한 후에 시작할 수 있습니다.

재정의 또는 예외적인 설정을 만드는 최상의 방법은 더 높은(예: 클러스터) 레벨에서 더 낮은(예: 그룹) 레벨로 설정을 복사하는 것입니다.

예를 들어 클러스터를 만든 후 dnsconfig 설정은 처음에 다음과 같습니다.

Configured at mode:

Cluster: Yes

Group Main_Group: No

Group Paris: No

Group Rome: No

Machine lab2.cable.nu: No

DNS 설정에 "그룹을 복사"하는 경우에는 다음과 같습니다.

Configured at mode:

Cluster: Yes

Group Main_Group: No

Group Paris: Yes

Group Rome: No

Machine lab2.cable.nu: No

이제 Paris 그룹 레벨 DNS 설정을 수정할 수 있으며, Paris 그룹의 다른 시스템은 이를 상속하게 됩니다. 비 Paris 시스템은 시스템 전용 설정이 없는 경우 클러스터 설정을 상속합니다. DNS 설정 외에도, SMTPROUTES에 대한 그룹 레벨 설정을 만드는 것이 일반적입니다.

팁 다양한 메뉴에서 CLI CLUSTERSET 기능을 사용하는 경우 설정을 모든 그룹으로 복사하는 특수 옵션(GUI를 통해 사용 불가)을 이용할 수 있습니다.

그룹 또는 클러스터로부터 전체 리스너가 자동으로 상속되며, 사용자는 대개 클러스터의 첫 번째 시스템에서 이들을 만들기만 하면 됩니다. 이를 통해 관리 부담이 상당히 줄어듭니다. 그러나 이를 활용하려면 그룹 또는 클러스터 전체에서 인터페이스의 이름을 동일하게 지정해야 합니다.

그룹 레벨에서 설정이 올바르게 정의되면 시스템을 클러스터에 가입시키고 이 그룹의 일부로 만들 수 있습니다. 이렇게 하려면 두 단계가 필요합니다.

첫째, 나머지 4개 시스템을 클러스터에 가입시키기 위해 각각에서 clusterconfig를 실행합니다. 클러스터가 더 크고 복잡할수록 가입에 시간이 더 오래 걸리며, 몇 분 정도 걸릴 수 있습니다. LIST 및 CONNSTATUS 하위 명령으로 가입 프로세스를 모니터링할 수 있습니다. 가입이 완료되면 SETGROUP을 사용하여 시스템을 Main_Group에서 Paris 및 Rome으로 이동할 수 있습니다. 처음에는 클러스터에 추가된 모든 시스템이 Paris 및 Rome 설정이 아니라 Main_Group 설정을 상속한다는 것은 피할 수 없는 사실입니다. 새 시스템이 이미 프로덕션 상태인 경우 이는 메일 플로우 트래픽에 영향을 미칠 수 있습니다.

팁 랩 시스템을 프로덕션 시스템과 동일한 클러스터에 속하게 만들지 마십시오. 랩 시스템에는 새 클러스터 이름을 사용하십시오. 이는 예기치 않은 변경(예: 누군가가 랩 시스템을 변경하여 실수로 프로덕션 메일이 손실됨)에 대한 추가 방어막을 제공합니다.

클러스터 기본값 외 **CM** 설정 사용을 위한 **GUI** 옵션 요약

설정을 재정의하고 기본 설정으로 시작합니다. 예를 들어 SMTPROUTES 컨피그레이션의 기본 설정은 빈 테이블이므로 처음부터 작성할 수 있습니다.

설정을 재정의하되, 클러스터 xxx 또는 그룹 yyy에서 현재 상속된 설정의 복사본으로 시작할 수 있습니다. 예를 들면 처음에 클러스터 테이블과 동일한 그룹 레벨에서 SMTPROUTES 테이블의 새로운 복사본을 원할 수 있습니다. 동일한 그룹(SETGROUP)에 포함된 모든 Cisco 어플라이언스는 이 테이블을 얻게 됩니다. 이 그룹에 속하지 않은 시스템은 여전히 클러스터 레벨 설정을 사용하게 됩니다. 이 독립된 테이블 복사본에서 SMTPROUTES를 변경하면 다른 그룹, 클러스터 설정을 상속하는 시스템 또는 개별 시스템 레벨에서 설정이 정의된 시스템에 영향이 미치지 않습니다. 이것이 가장 일반적인 선택입니다.

Centralized Management Options(중앙 집중식 관리 옵션)의 하위 메뉴에서 설정을 관리합니다. 이 메뉴에서 위와 같이 복사할 수 있지만 설정을 이동하거나 삭제할 수도 있습니다. SMTPROUTES를 그룹 또는 시스템 레벨로 이동하면, 경로 테이블은 클러스터 레벨에서 빈 상태가 되지만 좀 더 구체적인 레벨에 존재하게 됩니다.

설정을 관리합니다. SMTPROUTES 예에서, 삭제 옵션을 사용하면 클러스터에 대해 SMTPROUTES 테이블이 비워집니다. 전에 그룹 레벨 또는 시스템 레벨에서 SMTPROUTES에 대한 정의를 구성했다면 상관없습니다. 클러스터 레벨 설정을 삭제하고 그룹 또는 시스템 설정에만 의존하는 것은 좋은 방법이 아닙니다. 클러스터 전체의 설정은 새로 추가된 시스템의 기본값으로 유용하며, 이를 유지하면 유지 관리해야 하는 그룹 또는 사이트 설정의 수가 하나로 줄어듭니다.

설정 및 컨피그레이션 질문

Q. 전에 구성된 독립형 시스템이 있는데 기존 클러스터에 가입하면 설정이 어떻게 됩니까?

A. 시스템이 클러스터에 가입하면 해당 시스템의 클러스터 가능한 설정은 모두 클러스터 레벨에서 상속됩니다. 클러스터에 가입하면 로컬에서 구성된 모든 비 네트워크 설정은 손실되며, 클러스터 및 연결된 그룹의 설정이 이를 대신합니다. 여기에는 사용자/암호 테이블이 포함되는데, 암호와 사용자는 클러스터 내에서 공유됩니다.

Q. 클러스터링된 시스템이 있는데 이를 클러스터에서 영구적으로 제거하면 설정이 어떻게 됩니까?

A. 클러스터에서 시스템이 영구적으로 제거되면 구성 계층 구조가 "플랫화"되어, 해당 시스템은 클러스터의 일부였을 때와 동일하게 계속해서 작동합니다. 시스템이 상속한 모든 설정이 독립형 설정의 시스템에 적용됩니다.

예를 들어 클러스터 모드의 Global Unsubscribe 테이블만 있는 경우, 클러스터에서 시스템이 제거되면 해당 Global Unsubscribe 테이블 데이터가 시스템의 로컬 컨피그레이션으로 복사됩니다.

일반 질문

Q. 로그 파일은 중앙에서 관리되는 시스템 내에서 집계됩니까?

A. 아니요. 로그 파일은 여전히 각각의 개별 시스템에 대해 유지됩니다. 추적 및 보고를 위해 여러 시스템에서 메일 로그를 집계하는 데 Security Management Appliance를 사용할 수 있습니다.

Q. 사용자 액세스는 어떻게 작동합니까?

A. Cisco 어플라이언스는 전체 클러스터에 대해 하나의 데이터베이스를 공유합니다. 특히 전체 클러스터에 대해 관리자 계정(및 암호)만 있습니다.

Q. 데이터 센터를 어떻게 클러스터화해야 합니까?

A. 데이터 센터가 자체 클러스터가 아닌 클러스터 내 "그룹"인 것이 가장 좋습니다. 그러나 여러 데이터 센터가 공유하는 데이터가 많지 않으면 각 데이터 센터에 대해 별도의 클러스터를 만드는 것이 나을 수 있습니다.

Q. 오프라인 상태인 시스템을 다시 연결하면 어떤 일이 발생합니까?

A. 클러스터에 다시 연결하면 시스템이 동기화를 시도합니다.

네트워크 질문

Q. 중앙 집중식 관리 기능은 "peer-to-peer" 아키텍처인가요, 아니면 "마스터/슬레이브" 아키텍처인가요?

A. 각 시스템에는 모든 시스템의 모든 데이터가 있으므로(사용할 일이 없는 모든 시스템 전용 설정 포함), 중앙 집중식 관리 기능은 peer-to-peer 아키텍처라고 생각할 수 있습니다.

Q. 피어가 되지 않도록 설정할 수 있는 방법이 있습니까? "슬레이브" 시스템을 원하기 때문입니다.

A. 이 아키텍처에서는 진정한 "슬레이브" 시스템을 만드는 것이 불가능합니다. 그러나 시스템 레벨에서 HTTP(GUI) 및 SSH(CLI) 액세스를 비활성화할 수 있습니다. 이렇게 하면 clusterconfig 명령으로 GUI 또는 CLI 액세스가 없는 시스템만 구성됩니다(즉, 로그인 호스트가 될 수 없음). 이는 슬레이브를 가지고 있는 것과 유사하지만, 로그인 액세스를 다시 켜면 컨피그레이션이 무효화됩니다.

Q. 세그먼트화된 여러 클러스터를 만들 수 있습니까?

A. 클러스터의 고립된 "섬"은 가능합니다. 실제로 예를 들면 성능상의 이유로 이런 클러스터를 만드는 것이 유리한 상황도 있을 수 있습니다.

Q. 클러스터링된 어플라이언스 중 하나에서 IP 주소와 호스트 이름을 다시 구성하고 싶습니다. 이렇게 하면 reboot 명령을 실행하기 전에 GUI/CLI 세션이 손실됩니까?

A. 다음 단계를 수행합니다.

1. 새 IP 주소를 추가합니다.
2. 리스너를 새 주소로 이동합니다.
3. 클러스터에서 나갑니다.
4. 호스트 이름을 변경합니다.
5. 임의의 시스템에서 볼 때 이전 시스템 이름이 clusterconfig 연결 리스트에 나타나지 않는지 확인합니다.
6. 모든 GUI 세션이 로그아웃되었는지 확인합니다.
7. CCS가 인터페이스에서 활성화되지 않았는지 확인합니다(interfaceconfig 또는 Network(네트워크) > Listeners(리스너) 통해 확인).
8. 시스템을 클러스터에 다시 추가합니다.

Q. 대상 제어 기능은 클러스터 레벨에서 적용 가능합니까, 아니면 로컬 시스템 전용입니까?

A. 클러스터 레벨에서 설정할 수 있지만, 시스템 단위에서는 제한이 있습니다. 따라서 50개 연결로 제한하는 경우 그것이 클러스터의 각 시스템에 대해 설정되는 제한입니다.

계획 및 컨피그레이션

Q. 클러스터를 설정할 때 효율성을 최대화하고 문제를 최소화하려면 무엇을 해야 합니까?

1. 초기 계획
   - 클러스터 레벨에서 최대한 많은 것을 구성하려고 노력합니다.
   - 예외적인 내용만 시스템에서 관리합니다.
   - 예를 들어 여러 데이터 센터가 있는 경우, 클러스터 전체에 해당하는 것도 아니고 반드시 시스템과 관련된 것도 아닌 사항을 공유하려면 그룹을 사용합니다.
   - 각 어플라이언스에서 인터페이스 및 리스너에 대해 동일한 이름을 사용합니다.
2. 제한되는 명령을 확실히 이해합니다.
3. 설정 간 상호 의존성에 유의합니다.

예를 들어 listenerconfig 명령은(클러스터 레벨에서도) 시스템 레벨에만 존재하는 인터페이스에 의존합니다. 클러스터의 모든 시스템에서 시스템 레벨에 인터페이스가 존재하지 않으면 해당 리스너는 비활성화됩니다.

인터페이스를 삭제하면 listenerconfig에도 영향이 미칩니다.

4. 설정에 유의합니다.

   전에 구성된 시스템은 클러스터에 가입할 경우 독립된 설정을 잃게 됩니다. 전에 구성된 이러한 설정 중 일부를 시스템 레벨에서 다시 적용하려는 경우, 클러스터에 가입하기 전에 모든 설정을 별도로 적어두어야 합니다.

   "연결이 끊긴" 시스템도 여전히 클러스터의 일부입니다. 다시 연결하면 오프라인 상태였을 때 수행된 모든 변경 사항이 클러스터의 나머지와 동기화됩니다.

   클러스터에서 시스템을 영구적으로 제거하는 경우 해당 클러스터의 일부였을 때 가지고 있던 모든 설정이 유지됩니다. 그러나 마음이 바뀌어 클러스터에 다시 가입하면 시스템의 모든 독립형 설정이 손실됩니다.

   설정의 기록을 유지하려면 saveconfig 명령을 사용합니다.

43 장

테스트 및 트러블슈팅

이 장에는 다음 섹션이 포함되어 있습니다.

테스트 메시지를 사용하여 메일 플로우 디버깅: 추적

System Administration(시스템 관리) > **Trace**(추적) 페이지(CLI에서 trace 명령을 사용해도 됨)를 사용하여 테스트 메시지 전송을 에뮬레이션해 시스템의 메시지 흐름을 디버깅합니다. Trace(추적) 페이지(및 **trace** CLI 명령)는 리스너가 메시지를 수락한 것으로 에뮬레이트하고, 시스템의 현재 구성에 의해 "트리거된" 또는 영향을 받은 기능의 요약 내용을 출력합니다(커밋되지 않은 변경 사항 포함). 테스트 메시지는 실제로 전송되지 않습니다. 특히 Cisco 어플라이언스에서 사용 가능한 많은 고급 기능을 결합한 경우 Trace(추적) 페이지(및 **trace** CLI 명령)는 강력한 트러블슈팅 또는 디버깅 툴이 될 수 있습니다.

참고 파일 평판 검사 테스트에는 추적이 효과적이지 않습니다.

Trace(추적) 페이지(및 **trace** CLI 명령)에는 다음 표에 나열된 입력 매개변수가 표시됩니다.

표 ***149: Trace(추적)*** 페이지의 입력

Value	설명	예
소스 IP 주소	원격 도메인의 소스를 모방할 원격 클라이언트의 IP 주소를 입력합니다. IPv4(Internet Protocol version 4) 또는 IPv6(version 6) 주소일 수 있습니다. 참고: trace 명령을 입력하면 IP 주소 및 정규화된 도메인 이름 프롬프트가 표시됩니다. IP 주소가 정규화된 도메인 이름과 일치하는지 알아보기 위해 IP 주소 반전을 시도하지 않습니다 trace 명령을 사용할 경우 정규화된 도메인 이름 필드를 비워 둬서는 안 되므로 DNS가 일치하는 이름을 적절히 반전하지 않는 시나리오를 테스트할 수 없습니다.	**203.45.98.109** **2001:0db8:85a3::8a2e:0370:7334**
Fully Qualified Domain Name of the Source IP(소스 IP의 정규화된 도메인 이름)	모방할 정규화된 원격 도메인 이름을 입력합니다. Null로 남겨둘 경우 소스 IP 주소에 대해 역방향 DNS 조회가 수행됩니다.	**smtp.example.com**
Listener to Trace Behavior on(동작을 추적할 리스너)	테스트 메시지 전송을 에뮬레이트할 시스템에 구성된 리스너 목록에서 선택합니다.	**InboundMail**
SenderBase Network Owner Organization ID(SenderBase 네트워크 소유자 조직 ID)	SenderBase 네트워크 소유자의 고유한 ID 번호를 입력하거나, 시스템이 소스 IP 주소와 연결된 네트워크 소유자 ID를 조회하도록 허용합니다. GUI를 통해 발신자 그룹에 네트워크 소유자를 추가한 경우 이 정보를 볼 수 있습니다.	**34**
SenderBase Reputation Score (SBRS scores)(SenderBase Reputation 점수(SBRS 점수))	스푸핑된 도메인에 대해 제공할 SBRS 점수를 입력하거나, 시스템이 소스 IP 주소와 연결된 SBRS 점수를 조회하도록 허용합니다. 이는 SBRS 점수를 사용하는 정책을 테스트할 때 유용할 수 있습니다. 수동으로 입력한 SBRS 점수는 CASE(Context Adaptive Scanning Engine)로 전달되지 않습니다. 자세한 내용은 리스너에 대한 발신자 평판 필터링 점수 임계값 수정 , 88 페이지를 참조하십시오.	**-7.5**

Value	설명	예
Envelope Sender(봉투 발신자)	테스트 메시지의 Envelope Sender(봉투 발신자)를 입력합니다.	**admin@example.net**
Envelope Recipients(봉투 수신자)	테스트 메시지의 수신자 목록을 입력합니다. 항목이 여러 개인 경우 쉼표로 구분하십시오.	**joe** **frank@example.com**
메시지 본문	헤더를 포함하여 테스트 메시지의 본문을 입력합니다. 메시지 본문 입력을 끝내려면 별도의 줄에 마침표를 입력합니다."헤더"는 메시지 본문의 일부(빈 줄로 분리)로 간주되며, 헤더를 생략하거나 형식이 잘못된 헤더를 포함하면 예기치 않은 추적 결과가 발생할 수 있습니다.	**To: 1@example.com** From: ralph Subject: Test **this is a test message** **.**

값을 입력한 후 **Start Trace(**추적 시작**)**를 클릭합니다. 시스템에 구성되어 메시지에 영향을 미치는 모든 기능의 요약이 출력됩니다.

로컬 파일 시스템에서 메시지 본문을 업로드할 수 있습니다. (CLI에서 **`/configuration`** 디렉터리에 업로드한 메시지 본문으로 테스트할 수 있습니다. Cisco 어플라이언스로 가져올 파일 배치에 대한 자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지를 참조해 주십시오.)

요약이 출력되면 결과 메시지를 보고 테스트 메시지를 다시 실행할지 묻는 프롬프트가 표시됩니다. 또 다른 테스트 메시지를 입력하면 Trace(추적) 페이지 및 trace 명령은 위 표에서 입력한 이전 값을 사용합니다.

참고 다음 표에 나열된, trace 명령으로 테스트된 구성의 섹션이 순서대로 수행됩니다. 이는 한 기능의 구성이 다른 기능의 구성에 미치는 영향을 이해하는 데 매우 유용할 수 있습니다. 예를 들어 도메인 맵 기능으로 변환된 수신자 주소는 RAT에 의해 평가될 때 주소에 영향을 미칩니다. RAT의 영향을 받은 수신자는 별칭 테이블에 의해 평가될 때 주소에 영향을 미칩니다.

표 *150:* 추적 수행 시 출력 보기

trace 명령 섹션	산출물
HAT(Host Access Table) 및 메일 플로우 정책 처리	지정한 리스너의 Host Access Table 설정이 처리됩니다. 시스템은 HAT의 어떤 항목이 사용자가 입력한 원격 IP 주소 및 원격 도메인 이름에서 일치하는지를 보고합니다. 기본 메일 플로우 정책과 발신자 그룹, 그리고 지정된 항목과 무엇이 일치하는지를 알 수 있습니다. Cisco 어플라이언스가 연결을 거부하도록 구성된 경우(REJECT 또는 TCPREFUSE 액세스 규칙을 통해), trace 명령은 처리 시점에 종료됩니다. HAT 매개변수 설정에 대한 자세한 내용은 사전 정의된 발신자 그룹 및 메일 플로우 정책 이해, 103 페이지 섹션을 참조해 주십시오.
봉투 발신자 주소 처리 이러한 섹션에는 어플라이언스 구성이 사용자가 제공하는 Envelope Sender(봉투 발신자)에 미치는 영향이 요약되어 있습니다. (즉, 어플라이언스의 구성에 의해 MAIL FROM 명령이 해석되는 방법.) **trace** 명령은 이 섹션 앞에 "**Processing MAIL FROM:**"을 출력합니다.	
기본 도메인	리스너에서 수신하는 메시지의 기본 발신자 도메인을 변경하도록 지정한 경우 봉투 발신자에 대한 변경 사항이 이 섹션에 출력됩니다. 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지 장을 참조해 주십시오.
마스커레이드	메시지의 봉투 발신자를 변환하도록 지정한 경우 여기에 변경 사항이 기록됩니다. **listenerconfig -> edit -> masquerade -> config** 하위 명령을 사용하여 프라이빗 리스너에서 봉투 발신자의 마스커레이드를 활성화합니다. 자세한 내용은 라우팅 및 전달 기능 구성, 665 페이지을 참고하십시오.
봉투 수신인 처리 이러한 섹션에는 어플라이언스가 사용자가 제공하는 Envelope Recipients(봉투 수신자)에 미치는 영향이 요약되어 있습니다. (즉, 어플라이언스의 구성에 의해 RCPT TO 명령이 해석되는 방법.) trace 명령은 이 섹션 앞에 "Processing Recipient List:"를 출력합니다.	
기본 도메인	리스너에서 수신하는 메시지의 기본 발신자 도메인을 변경하도록 지정한 경우 봉투 발신자에 대한 변경 사항이 이 섹션에 출력됩니다. 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지을 참고하십시오.

trace 명령 섹션	산출물
도메인 맵 변환	도메인 맵 기능은 수신자 주소를 대체 주소로 변환합니다. 사용자가 도메인 맵 변경 사항을 지정했고 지정된 수신자 주소가 일치하면 이 섹션에 변환이 출력됩니다. 자세한 내용은 라우팅 및 전달 기능 구성, 665 페이지을 참고하십시오.
RAT(Recipient Access Table)	정책과 매개변수 외에 RAT의 항목과 일치하는 각 봉투 수신자가 이 섹션에 출력됩니다. (예를 들어, 리스너의 RAT에 있는 제한을 우회하도록 수신자가 지정한 경우.) 수락하는 수신자 지정에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지 장을 참조해 주십시오.
별칭 테이블	어플라이언스에 구성된 별칭 테이블의 항목과 일치하는 각 봉투 수신자(및 하나 이상의 수신자 주소에 대한 후속 변환)가 이 섹션에 출력됩니다. 자세한 내용은 라우팅 및 전달 기능 구성, 665 페이지을 참고하십시오.
사전 대기열 메시지 작업 이 섹션에는 메시지 내용을 수신된 후, 그러나 작업 대기열에 메시지가 추가되기 전 어플라이언스가 각 메시지에 미치는 영향이 요약되어 있습니다. 원격 MTA에 최종 **250 ok** 명령이 반환되기 전에 이 처리가 발생합니다. **trace** 명령은 이 섹션 앞에 "Message Processing:"을 출력합니다.	
가상 게이트웨이	**altsrchost** 명령은 봉투 발신자의 전체 주소, 도메인, 이름 또는 IP 주소 일치를 기반으로 특정 인터페이스에 메시지를 할당합니다. 봉투 발신자가 **altsrchost** 명령의 항목과 일치하면 해당 정보가 이 섹션에 출력됩니다. 아래의 메시지 필터 처리가 이 시점에 할당된 가상 게이트웨이 주소를 덮어쓸 수 있습니다. 자세한 내용은 라우팅 및 전달 기능 구성, 665 페이지을 참고하십시오.
반송 프로필	반송 프로필은 처리시 서로 다른 세 시점에 적용됩니다. 이것이 첫 번째 발생입니다. 리스너에 할당된 반송 프로필이 있는 경우 처리 과정의 이 시점에 할당됩니다. 해당 정보는 이 섹션에 출력됩니다. 자세한 내용은 라우팅 및 전달 기능 구성, 665 페이지을 참고하십시오.

trace 명령 섹션	산출물
작업 대기열 작업 작업 대기열의 메시지에 대해 다음 기능 그룹이 수행됩니다. 이는 클라이언트에서 메시지가 수락된 후, 그러나 전송을 위해 메시지가 대상 대기열에 추가되기 전에 발생합니다. status 및 status detail 명령을 실행하면 "Messages in Work Queue"가 보고됩니다.	
마스커레이드	메시지의 To:, From: 및 CC: 헤더를 표시하도록 지정한 경우(리스너에서 입력한 고정 테이블에서 또는 LDAP 쿼리를 통해) 변경 사항이 여기에 표시됩니다. **`listenerconfig -> edit -> masquerade -> config`** 하위 명령을 사용하여 프라이빗 리스너에서 메시지 헤더의 마스커레이드를 활성화합니다. 자세한 내용은 라우팅 및 전달 기능 구성, 665 페이지을 참고하십시오.
LDAP 라우팅	리스너에서 LDAP 쿼리가 활성화된 경우 LDAP 수락, 재라우팅, 마스커레이드 및 그룹 쿼리의 결과가 이 섹션에 출력됩니다. 자세한 내용은 LDAP 쿼리, 735 페이지를 참고하십시오.
메시지 필터 처리	시스템에서 활성화된 모든 메시지 필터는 이 시점에서 테스트 메시지에 의해 평가됩니다. 각 필터에 대해 규칙이 평가되며, 최종 결과가 "true"이면 해당 필터의 각 작업이 순서대로 수행됩니다. 한 필터에는 다른 여러 필터가 작업으로 포함될 수 있으며, 필터의 중첩에는 제한이 없습니다. 규칙이 "false"로 평가되고 작업 리스트가 else 절과 연결되어 있으면 해당 작업이 대신 평가됩니다. 순서대로 처리된 메시지 필터의 결과가 이 섹션에 출력됩니다. 메시지 필터를 사용하여 이메일 정책 적용, 137 페이지를 참조하십시오.
메일 정책 처리 메일 정책 처리 섹션에는 사용자가 제공하는 모든 수신자에 대한 안티스팸, 안티바이러스, Outbreak Filter 기능 및 면책조항 스탬프가 표시됩니다. Email Security Manager(이메일 보안 관리자)에서 여러 수신자가 여러 정책과 일치하면 일치하는 각 정책에 대해 다음 섹션이 반복됩니다. "Message Going to" 문자열은 어떤 수신자가 어떤 정책과 일치하는지를 정의합니다.	

trace 명령 섹션	산출물
안티스팸	이 섹션에는 안티스팸 검사로 처리하도록 플래그가 지정되지 않은 메시지가 표시됩니다. 리스너에 대한 안티스팸 검사로 메시지를 처리하는 경우, 해당 메시지가 처리되고 반환된 판정이 출력됩니다. 판정을 기반으로 메시지를 반송 또는 삭제하도록 Cisco 어플라이언스가 구성된 경우 해당 정보가 출력되고 **trace** 명령 처리가 중단됩니다. 참고: 시스템에서 안티스팸 검사를 사용할 수 없는 경우 이 단계가 생략됩니다. 안티스팸 검사가 사용 가능하지만 기능 키와 함께 활성화되지 않은 경우 해당 정보도 이 섹션에 출력됩니다. Anti-Spam, 355 페이지의 내용을 참조하십시오.
안티바이러스	이 섹션에는 안티바이러스 검사로 처리하도록 플래그가 지정되지 않은 메시지가 표시됩니다. 리스너에 대한 안티바이러스 검사로 메시지를 처리하는 경우, 해당 메시지가 처리되고 반환된 판정이 출력됩니다. 감염된 메시지를 "치료"하도록 Cisco 어플라이언스를 구성한 경우 해당 정보가 표시됩니다. 판정을 기반으로 메시지를 반송 또는 삭제하도록 구성된 경우 해당 정보가 출력되고 trace 명령 처리가 중단됩니다. 참고: 시스템에서 안티바이러스 검사를 사용할 수 없는 경우 이 단계가 생략됩니다. 안티바이러스 검사가 사용 가능하지만 기능 키와 함께 활성화되지 않은 경우 해당 정보도 이 섹션에 출력됩니다. Anti-Virus, 335 페이지를 참조하십시오.
콘텐츠 필터 처리	시스템에서 활성화된 모든 콘텐츠 필터는 이 시점에서 테스트 메시지에 의해 평가됩니다. 각 필터에 대해 규칙이 평가되며, 최종 결과가 "true"이면 해당 필터의 각 작업이 순서대로 수행됩니다. 한 필터에는 다른 여러 필터가 작업으로 포함될 수 있으며, 필터의 중첩에는 제한이 없습니다. 순서대로 처리된 콘텐츠 필터의 결과가 이 섹션에 출력됩니다. 콘텐츠 필터, 283 페이지를 참조하십시오.
Outbreak Filter 처리	이 섹션에는 첨부 파일을 포함하는 메시지가 Outbreak Filter 기능을 우회할 것임이 표시됩니다. 수신자용 Outbreak Filter로 메시지를 처리하려는 경우, 해당 메시지가 처리 및 평가됩니다. 판정을 기반으로 메시지를 격리, 반송 또는 삭제하도록 어플라이언스가 구성된 경우 해당 정보가 출력되고 처리가 중단됩니다. 신종 바이러스 필터(Outbreak Filter), 399 페이지를 참조하십시오.

trace 명령 섹션	산출물
바닥글 스탬프	이 섹션에는 바닥글 텍스트 리소스가 메시지에 첨부되었는지 여부가 표시됩니다. 텍스트 리소스의 이름이 표시됩니다. 텍스트 리소스, 613 페이지의 메시지 면책조항 스탬프, 614 페이지 섹션을 참조해 주십시오.
전달 작업 다음 섹션에는 메시지가 전달될 때 발생하는 작업이 표시됩니다. trace 명령은 이 섹션 앞에 "Message Enqueued for Delivery"를 출력합니다.	
도메인 및 사용자 단위 전역 수신 거부	trace 명령에 대한 입력으로 지정한 수신자가 전역 수신 거부 기능에 나열된 수신자, 수신자 도메인 또는 IP 주소와 일치하는 경우 수신 거부된 수신자 주소가 이 섹션에 출력됩니다. 라우팅 및 전달 기능 구성, 665 페이지를 참조하십시오.
최종 결과 모든 처리가 출력되면 최종 결과 프롬프트가 표시됩니다. 결과 메시지를 보려면 CLI에서 "Would you like to see the resulting message?(결과 메시지를 보시겠습니까?)"라는 질문에 **y**로 답해 주십시오.	

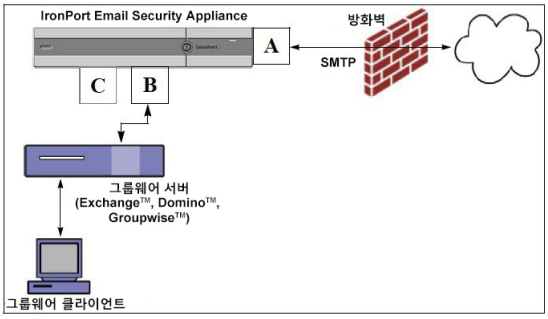
리스너를 사용하여 어플라이언스 테스트

"블랙홀" 리스너를 사용하면 메시지 생성 시스템을 테스트하고 수신 성능을 대략적으로 측정할 수 있습니다. 블랙홀 리스너의 두 가지 유형은 *queueing* 및 *non-queueing*입니다.

- 대기열(queueing) 리스너는 메시지를 대기열에 저장하지만, 그런 다음 즉시 삭제합니다. 메시지 생성 시스템의 전체 주입 부분 성능을 측정하는 데 관심이 있는 경우 대기열 리스너를 사용해 주십시오.
- 비대기열(non-queueing) 리스너는 메시지를 수락한 다음 저장하지 않고 즉시 삭제합니다. 메시지 생성 시스템과 어플라이언스의 연결과 관련된 트러블슈팅을 하려는 경우 비대기열 리스너를 사용해 주십시오.

예를 들어 다음 그림에서 "B"라는 프라이빗 리스너를 미러링하는 블랙홀 리스너 "C"를 만들 수 있습니다. 비대기열 버전은 그룹웨어 클라이언트에서 그룹웨어 서버 및 어플라이언스에 이르기까지 시스템의 성능 경로를 테스트합니다. 대기열 버전은 동일한 경로 및 메시지를 대기열에 추가하고 SMTP를 통해 전달하도록 준비하는 어플라이언스의 기능을 테스트합니다.

그림 ***86: Enterprise Gateway***용 블랙홀 리스너



이 예에서는 listenerconfig 명령을 사용하여 Management 인터페이스에 BlackHole_1이라는 블랙홀 대기열 리스너를 만듭니다. 그런 후 다음 호스트의 연결을 수락하도록 리스너의 HAT(Host Access Table)를 수정합니다.

- **yoursystem.example.com**
- **10.1.2.29**
- **badmail.tst**
- **.tst**

참고 최종 항목 .tst는 .tst 도메인의 모든 호스트가 BlackHole_1이라는 이름의 리스너로 이메일을 전송하도록 리스너를 구성합니다.

예

```
mail3.example.com> listenerconfig

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> new

Please select the type of listener you want to create.

1. Private

2. Public
```

```
3. Blackhole

[2]> 3

Do you want messages to be queued onto disk? [N]> y

Please create a name for this listener (Ex: "OutboundMail"):

[]> BlackHole_1

Please choose an IP interface for this Listener.

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Choose a protocol.

1. SMTP

2. QMQP

[1]> 1

Please enter the IP port for this listener.

[25]> 25

Please specify the systems allowed to relay email through the IronPort C60.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addressed are allowed.

Separate multiple entries with commas.


[]> yoursystem.example.com, 10.1.2.29, badmail.tst, .tst

Do you want to enable rate limiting per host? (Rate limiting defines
the maximum number of recipients per hour you are willing to receive from a remote
domain.) [N]> n

Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control: No
```

```
Spam Detection Enabled: No

Virus Detection Enabled: Yes

Allow TLS Connections: No

Allow SMTP Authentication: No

Require TLS To Offer SMTP authentication: No

Would you like to change the default host access policy? [N]> n

Listener BlackHole_1 created.

Defaults have been set for a Black Hole Queuing listener.

Use the listenerconfig->EDIT command to customize the listener.

Currently configured listeners:

1. BlackHole_1 (on Management, 192.168.42.42) SMTP Port 25 Black Hole Queuing

2. InboundMail (on PublicNet, 192.1681.1) SMTP Port 25 Public

3. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]>
```

참고 이러한 변경 사항을 적용하려면 commit 명령을 실행해야 합니다.

블랙홀 대기열 리스너를 구성했고 주입 시스템에서의 연결을 수락하도록 HAT를 수정했으면, 주입 시스템을 사용하여 어플라이언스로의 이메일 전송을 시작할 수 있습니다. 시스템 성능을 모니터링하려면 status, status detail 및 rate 명령을 사용합니다. GUI(Graphical User Interface)를 통해 시스템을 모니터링할 수도 있습니다. 자세한 내용은 다음 링크를 참조하십시오.

- CLI를 사용한 모니터링, 1003 페이지
- GUI 기타 작업, 1035 페이지

네트워크 트러블슈팅

어플라이언스에 네트워크 연결 문제가 있으면 먼저 어플라이언스가 제대로 작동하는지 확인해 주십시오.

어플라이언스의 네트워크 연결 테스트

단계 **1** 시스템에 연결하고 관리자로 로그인합니다. 로그인에 성공하면 다음 메시지가 표시됩니다.

```
Last login: day month date hh:mm:ss from IP address

Copyright (c) 2001-2003, IronPort Systems, Inc.

AsyncOS x.x for Cisco


Welcome to the Cisco Messaging Gateway Appliance(tm)
```

단계 **2** status 또는 status detail 명령을 사용합니다.

```
mail3.example.com> status
```

또는

```
mail3.example.com> status detail
```

status 명령은 이메일 작업에 대한 모니터링된 정보의 하위 집합을 반환합니다. 반환된 통계는 카운터와 게이지라는 두 범주로 그룹화됩니다. 속도를 포함한 이메일 운영에 대한 전체 모니터링 정보를 보려면 status detail 명령을 사용해 주십시오. 카운터는 시스템에서 발생하는 각종 이벤트의 누계를 제공합니다. 각 카운터에 대해 카운터 재설정 이후, 마지막 재부팅 이후, 그리고 시스템 수명 주기 전체에서 발생한 총 이벤트 수를 볼 수 있습니다. (자세한 내용은 CLI를 사용한 모니터링, 1003 페이지 섹션을 참조하십시오.)

단계 **3** `mailconfig` 명령을 사용하여 알려진 사용 가능 주소로 메일을 전송합니다.

`mailconfig` 명령은 어플라이언스에 대해 사용 가능한 모든 컨피그레이션 설정이 포함된, 사람이 읽을 수 있는 파일을 생성합니다. 어플라이언스가 네트워크를 통해 이메일을 전송할 수 있는지 확인하려면 어플라이언스에서 알려진 사용 가능 이메일 주소로 파일을 전송해보십시오.

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send the
configuration file.


Separate multiple addresses with commas.

[]> user@example.com

Do you want to include passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig. [N]> y


The configuration file has been sent to user@example.com.

mail3.example.com>
```

문제 해결

네트워크에서 어플라이언스가 활성 상태임을 확인했으면 다음 명령을 사용하여 네트워크 문제를 파악합니다.

- `netstat` 명령을 사용하여 다음 정보를 포함한 네트워크 연결(수신 및 발송 모두), 라우팅 테이블, 네트워크 인터페이스 수 통계를 표시할 수 있습니다.
  - 활성 소켓 리스트
  - 네트워크 인터페이스 상태
  - 라우팅 테이블 내용
  - 수신 대기열 크기
  - 패킷 트래픽 정보
- `diagnostic -> network -> flush` 명령을 사용하면 모든 네트워크 관련 캐시를 플러시할 수 있습니다.
- `diagnostic -> network -> arpshow` 명령을 사용하면 시스템 ARP 캐시를 표시할 수 있습니다.
- `packetcapture` 명령을 사용하면 컴퓨터가 연결된 네트워크를 통해 전송되거나 수신되는 TCP/IP 및 기타 패킷을 가로채고 표시할 수 있습니다.

  `packetcapture`를 사용하려면 네트워크 인터페이스 및 필터를 설정합니다. 필터는 동일한 형식 및 UNIX `tcpdump` 명령을 사용합니다. 패킷 캡처를 시작하려면 start, 끝내려면 stop을 사용합니다. 캡처를 중단한 후 SCP 또는 FTP를 사용하여 /pub/captures 디렉터리에서 파일을 다운로드해야 합니다. 자세한 내용은 패킷 캡처 실행, 1174 페이지를 참고하십시오.
- 알려진 사용 가능 호스트에 대해 `ping` 명령을 사용하여 네트워크에서 어플라이언스의 연결이 활성 상태이고 어플라이언스가 네트워크의 특정 세그먼트에 도달할 수 있는지를 확인합니다.

  `ping` 명령을 사용하면 어플라이언스에서 네트워크 호스트와의 연결을 테스트할 수 있습니다.

```
mail3.example.com> ping

Which interface do you want to send the pings from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Please enter the host you wish to ping.

[]> anotherhost.example.com

Press Ctrl-C to stop.
```

```
PING anotherhost.example.com (x.x.x.x): 56 data bytes
64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms
64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms
^C
--- anotherhost.example.com ping statistics ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
```

참고 ping 명령을 끝내려면 Ctrl-C를 사용해야 합니다.

- `traceroute` 명령을 사용하여 어플라이언스에서 네트워크 호스트로의 연결을 테스트하고 네트워크 홉과의 라우팅 문제를 디버그합니다.

```
mail3.example.com> traceroute
Which interface do you want to trace from?
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Please enter the host to which you want to trace the route.
[]> 10.1.1.1
Press Ctrl-C to stop.
traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets
1 gateway (192.168.0.1) 0.202 ms 0.173 ms 0.161 ms
2 hostname (10.1.1.1) 0.298 ms 0.302 ms 0.291 ms
mail3.example.com>
```

- `diagnostic -> network -> smtpping` 명령을 사용하여 원격 SMTP 서버를 테스트합니다.
- `nslookup` 명령을 사용하여 DNS 기능을 확인합니다.

  `nslookup` 명령은 어플라이언스에서 작동 중인 DNS(Domain Name Service) 서버에 연결하여 호스트 이름 및 IP 주소를 확인하는 것이 가능한지 확인할 수 있습니다.

```
mail3.example.com> nslookup
Please enter the host or IP to resolve.
```

```
[]> example.com

Choose the query type:

1. A

2. CNAME

3. MX

4. NS

5. PTR

6. SOA

7. TXT

[1]>

A=192.0.34.166 TTL=2d
```

표 ***151: DNS*** 기능 확인*:* 쿼리 유형

A	호스트의 인터넷 주소
CNAME	별칭(alias)에 대한 정규 이름(canonical name)
MX	메일 교환기
NS	이름이 지정된 영역의 이름 서버
PTR	쿼리가 인터넷 주소인 경우 호스트 이름, 그렇지 않은 경우 다른 정보에 대한 포인터
SOA	도메인의 "인증 기관 시작" 정보
TXT	텍스트 정보

- CLI 또는 GUI를 통해 `tophosts` 명령을 사용하고 Active Recipients(활성 수신자) 기준으로 정렬합니다.

  `tophosts` 명령은 대기열에 있는 상위 20 수신자 호스트 리스트를 반환합니다. 이 명령은 네트워크 연결 문제가 이메일을 전송하고자 하는 단일 호스트 또는 호스트 그룹에 한정되는지를 판단하는 데 도움이 될 수 있습니다. (자세한 내용은 "메일 대기열의 구성 확인"을 참고하십시오.)

```
mail3.example.com> tophosts

Sort results by:

1. Active Recipients

2. Connections Out

3. Delivered Recipients
```

```
4. Soft Bounced Events

5. Hard Bounced Recipients

[1]> 1

Status as of: Mon Nov 18 22:22:23 2003

ActiveConn.Deliv.SoftHard

# Recipient HostRecipOutRecip.BouncedBounced

1 aol.com36510255218

2 hotmail.com29071982813

3 yahoo.com13461231119

4 excite.com9838494

5 msn.com8427633 29

^C
```

- tophosts 명령 결과로 나열된 상위 도메인에 대해 `hoststatus` 명령을 사용하도록 "드릴다운"합니다.

  `hoststatus` 명령은 특정 수신자 호스트와 관련된 이메일 작업에 대한 모니터링 정보를 반환합니다. AsyncOS 캐시에 저장된 DNS 정보 및 수신자 호스트에서 반환된 마지막 오류도 제공됩니다. 반환된 데이터는 마지막 `resetcounters` 명령 이후 누적된 것입니다. (자세한 내용은 메일 호스트의 상태 모니터링, 1006 페이지 섹션을 참조하십시오.)

  상위 도메인에서 `hoststatus` 명령을 사용하면 DNS 확인 관련 성능 문제를 어플라이언스 또는 인터넷으로 격리할 수 있습니다. 예를 들어 상위 활성 수신자 호스트에 대해 `hoststatus` 명령을 실행한 결과 다수의 대기 중 발신 연결이 표시되면 특정 호스트가 다운되었거나 도달할 수 없는 상태인지 또는 어플라이언스가 전체 또는 대다수 호스트에 연결할 수 없는지를 확인해보십시오.

- 방화벽 권한을 확인합니다.

  어플라이언스가 제대로 작동하려면 20, 21, 22, 23, 25, 53, 80, 123, 443 및 628 포트가 모두 열려야 할 수 있습니다. (방화벽 정보, 1227 페이지 참조.)

- 네트워크의 어플라이언스에서 dnscheck@ironport.com으로 이메일을 전송합니다.

  시스템에서 기본 DNS 확인을 수행하려면 네트워크 내에서 dnscheck@ironport.com으로 이메일을 전송합니다. 그러면 다음과 같은 네 가지 테스트의 결과 및 세부사항과 함께 자동 응답 메일이 전송됩니다.

DNS PTR 레코드 - 봉투 발신자의 IP 주소가 도메인의 PTR 레코드와 일치합니까?

DNS A 기록 - 도메인의 PTR 기록이 Envelope From의 IP 주소와 일치합니까?

HELO 일치 - `SMTP HELO` 명령에 나열된 도메인이 Envelope From의 DNS 호스트 이름과 일치합니까?

지연된 반송 메시지를 수락하는 메일 서버 - `SMTP HELO` 명령에 나열된 도메인에 해당 도메인의 IP 주소를 확인하는 MX 기록이 있습니까?

리스너 트러블슈팅

이메일 주입에 문제가 있는 것 같으면 다음 전략을 사용할 수 있습니다.

- 주입하는 시작 IP 주소를 확인한 후 `listenerconfig` 명령을 사용하여 허용되는 호스트를 검토합니다.

  허용되는 IP 주소가 자신이 생성한 리스너에 연결되어 있습니까? 리스너에 대한 HAT(Host Access Table)를 점검하려면 `listenerconfig` 명령을 사용합니다. 리스너에 대한 HAT를 출력하려면 다음 명령을 사용합니다.

  ```
  listenerconfig -> edit -> listener_number -> hostaccess -> print
  ```

  IP 주소, IP 주소 블록, 호스트 이름 또는 도메인 단위로 연결을 거부하도록 HAT를 구성할 수 있습니다. 자세한 내용은 "연결이 허용되는 호스트 지정"을 참고하십시오.

  또한 리스너에 대해 허용되는 최대 연결 수를 확인하려면 `limits` 하위 명령을 사용할 수 있습니다.

  ```
  listenerconfig -> edit -> listener_number -> limits
  ```

- 주입이 시작되는 시스템에서 텔넷 또는 FTP를 사용하여 수동으로 어플라이언스에 연결합니다. 예를 들면 다음과 같습니다.

  ```
  injection_machine% telnet appliance_name
  ```

  리스너에서 실제 어플라이언스로 연결하려면 어플라이언스 자체 내에서 `telnet` 명령을 사용할 수도 있습니다.

  ```
  mail3.example.com> telnet

  Please select which interface you want to telnet from.

  1. Auto

  2. Management (192.168.42.42/24: mail3.example.com)

  3. PrivateNet (192.168.1.1/24: mail3.example.com)

  4. PublicNet (192.168.2.1/24: mail3.example.com)

  [1]> 3

  Enter the remote hostname or IP.

  []> 193.168.1.1

  Enter the remote port.

  [25]> 25

  Trying 193.168.1.1...

  Connected to 193.168.1.1.

  Escape character is '^]'.
  ```

한 인터페이스에서 다른 인터페이스로 연결할 수 없으면 어플라이언스의 Management, Data1 및 Data2 인터페이스가 네트워크에 연결된 방식에 문제가 있는 것일 수 있습니다. 자세한 내용은 FTP, SSH 및 SCP 액세스, 1199 페이지를 참조하십시오. 리스너의 포트 25로 텔넷을 지정하고 SMTP 명령을 수동으로 입력할 수 있습니다(프로토콜에 익숙한 경우).

- IronPort 텍스트 메일 로그 및 주입 디버그 로그를 점검하여 수신 오류를 확인합니다.

  주입 디버그 로그는 어플라이언스와 시스템에 연결된 지정된 호스트 간 SMTP 대화를 기록합니다. 주입 디버그 로그는 어플라이언스 및 인터넷에서 연결을 시작하는 클라이언트 간 통신 트러블슈팅에 유용합니다. 로그에는 두 시스템 간에 전송된 모든 바이트가 기록되며, 연결하는 호스트로 전송("Sent to") 또는 연결하는 호스트에서 수신("Received from")으로 분류됩니다.

  자세한 내용은 텍스트 메일 로그 사용, 1062 페이지 및 주입 디버그 로그 사용, 1083 페이지를 참조하십시오.

어플라이언스로부터의 이메일 전송 트러블슈팅

어플라이언스로부터의 이메일 전송에 문제가 있는 것 같으면 다음 전략을 시도해볼 수 있습니다.

- 문제가 도메인과 관련된 것인지 확인합니다.

  `tophosts` 명령을 사용하면 이메일 대기열에 대한 즉각적인 정보를 얻어, 특정 수신자 도메인에 전송 문제가 있는지를 확인할 수 있습니다.

  "Active Recipients(활성 수신자)" 기준으로 정렬할 때 반환되는 문제의 도메인이 있습니까?

  Connections Out (연결 중단)으로 정렬할 때 어느 한 도메인이 리스너에 대해 지정된 최대 연결 수에 도달합니까? 리스너에 대한 기본 최대 연결 수는 600입니다. 시스템 전체의 기본 최대 연결 수는 10,000입니다(`deliveryconfig` 명령으로 설정). 다음 명령을 사용하여 리스너에 대한 최대 연결 수를 확인할 수 있습니다.

  ```
  listenerconfig -> edit -> listener_number -> limits
  ```

  리스너에 대한 연결을 `destconfig` 명령으로 더 제한할 수 있습니까(시스템 최대값 또는 Virtual Gateway 주소 기준)? `destconfig` 연결 제한을 확인하려면 다음 명령을 사용합니다.

  ```
  destconfig -> list
  ```

- `hoststatus` 명령을 사용합니다.

  `tophosts` 명령 결과로 나열된 상위 도메인에 대해 `hoststatus` 명령을 사용하여 "드릴다운"합니다.

  호스트가 사용 가능하며 연결을 수락합니까?

  지정된 호스트에서 하나의 특정 MX 기록 메일 서버에 문제가 있습니까?

  지정된 호스트에 5XX 오류가 있는 경우(Permanent Negative Completion 응답) `hoststatus` 명령은 호스트에서 반환한 마지막 "5XX" 상태 코드 및 설명을 보고합니다. 호스트에 대한 마지막 발신 TLS 연결이 실패하면 `hoststatus` 명령은 실패 이유를 표시합니다.

- 도메인 디버그, 반송 및 텍스트 메일 로그를 구성 및/또는 검토하여 수신자 호스트가 사용 가능한지 확인합니다.

  도메인 디버그 로그는 어플라이언스와 지정된 수신자 호스트 간 SMTP 대화 중에 클라이언트와 서버의 통신을 기록합니다. 특정 수신자 호스트의 문제를 디버그하는 데 이 로그 파일 형식을 사용할 수 있습니다.

  자세한 내용은 도메인 디버그 로그 사용, 1082 페이지를 참고하십시오.

  반송 로그는 반송된 각 수신자와 관련된 모든 정보를 기록합니다.

  자세한 내용은 반송 로그 사용, 1077 페이지를 참고하십시오.

  텍스트 메일 로그는 이메일 수신, 이메일 전송 및 반송의 세부사항을 포함합니다. 이러한 로그는 특정 메시지의 전송을 이해하고 시스템 성능을 분석하는 데 유용한 정보 소스입니다.

  자세한 내용은 텍스트 메일 로그 사용, 1062 페이지를 참고하십시오.

- `telnet` 명령을 사용하여 어플라이언스에서 문제의 도메인으로 연결합니다.

```
mail3.example.com> telnet

Please select which interface you want to telnet from.

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Enter the remote hostname or IP.

[]> problemdomain.net

Enter the remote port.

[25]> 25
```

- 온디맨드 방식으로 아웃바운드 TLS 연결을 설정하고 대상 도메인과 관련된 TLS 연결 문제를 디버그하려면 `tlsverify` 명령을 사용할 수 있습니다. 연결을 생성하려면 확인 대상이 될 도메인 및 목적지 호스트를 지정합니다. AsyncOS는 Required (Verify) TLS 설정을 기반으로 TLS 연결을 확인합니다.

```
mail3.example.com> tlsverify

Enter the TLS domain to verify against:

[]> example.com

Enter the destination host to connect to. Append the port (example.com:26) if you are

not connecting on port 25:
```

```
[example.com]> mxe.example.com:25

Connecting to 1.1.1.1 on port 25.

Connected to 1.1.1.1 from interface 10.10.10.10.

Checking TLS connection.

TLS connection established: protocol TLSv1, cipher RC4-SHA.

Verifying peer certificate.

Verifying certificate common name mxe.example.com.

TLS certificate match mxe.example.com

TLS certificate verified.

TLS connection to 1.1.1.1 succeeded.

TLS successfully connected to mxe.example.com.

TLS verification completed.
```

성능 트러블슈팅

어플라이언스에 성능 문제가 있는 경우 다음 전략을 사용할 수 있습니다.

- rate 및 `hostrate` 명령을 사용하여 현재 시스템 활동을 검토합니다.

  rate 명령은 이메일 운영에 대한 실시간 모니터링 정보를 반환합니다. 자세한 내용은 실시간 활동 표시, 1010 페이지를 참고하십시오.

  `hostrate` 명령은 특정 호스트에 대한 실시간 모니터링 정보를 반환합니다.

- status 명령을 사용하여 속도 기록을 교차 확인해 성능 저하가 있는지 확인합니다.

- `status detail` 명령을 사용하여 RAM 사용률을 확인합니다.

  시스템의 RAM, CPU 및 디스크 I/O 사용률을 빠르게 확인하려면 `status detail` 명령을 사용할 수 있습니다.

  참고 RAM 사용률은 항상 45% 미만이어야 합니다. RAM 사용률이 45%를 넘으면 어플라이언스는 "리소스 절약 모드"로 들어가며, 리소스의 초과 서브스크립션을 방지하기 위해 "back-off" 알고리즘을 시작하고 다음 이메일 경고문을 전송합니다.

```
This system (hostname: hostname) has entered a 'resource conservation' mode in order
to
prevent the rapid depletion of critical system resources.


RAM utilization for this system has exceeded the resource conservation threshold of
45%.
```

```
The allowed injection rate for this system will be gradually decreased as RAM
utilization approaches 60%.
```

이는 전송 가능성이 낮은 시설에서 공격적인 주입을 사용할 경우에만 발생합니다. RAM 사용률이 45%를 넘으면 대기열의 메시지 수를 확인하고 특정 도메인이 다운되었는지 또는 전송이 불가능한지를 확인합니다(`hoststatus` 또는 `hostrate` 명령을 통해). 또한 시스템 상태를 점검하고 전송이 중단되지 않도록 합니다. 주입 중단 후에도 RAM 사용률이 계속 높으면 Cisco 고객 지원에 문의하십시오.

- 문제가 한 도메인에서만 발생합니까?

  `tophosts` 명령을 사용하면 이메일 대기열에 대한 즉각적인 정보를 얻어, 특정 수신자 도메인에 전송 문제가 있는지를 확인할 수 있습니다.

  대기열의 크기를 확인합니다. 이메일 대기열의 메시지를 삭제, 반송, 일시 중단 또는 리디렉션하여 대기열의 크기를 관리하거나, 특정 문제 도메인의 수신자를 처리할 수 있습니다. 자세한 내용은 이메일 대기열 관리, 1014 페이지를 참고하십시오. 다음 명령을 사용합니다.

  - `deleterecipients`
  - `bouncerecipients`
  - `redirectrecipients`
  - `suspenddel / resumedel`
  - `suspendlistener / resumelistener`

  `tophosts` 명령을 사용하여 소프트 및 하드 반송의 수를 확인합니다. "Soft Bounced Events"(옵션 4) 또는 "Hard Bounced Recipients"(옵션 5)로 정렬합니다. 특정 도메인의 성능에 문제가 있으면 위 명령을 사용하여 해당 도메인으로의 전달을 관리합니다.

웹 인터페이스 모양 및 렌더링 문제

Internet Explorer 호환성 모드 재정의, 994 페이지를 참조하십시오.

경고문에 응답

경고문: C380 또는 C680 하드웨어의 배터리 재인식 시간 초과(RAID 이벤트)

문제

C380 또는 C680 하드웨어가 있으며 "Battery Relearn Timed Out" (RAID event)(배터리 재인식 시간 초과(RAID 이벤트)) 경고문을 수신합니다.

솔루션

이 경고문은 문제를 나타낼 수도 있고 그렇지 않을 수도 있습니다. 배터리 재인식 시간 초과 자체가 RAID 컨트롤러에 문제가 있음을 의미하지는 않습니다. 후속 재인식에서 컨트롤러가 복구될 수 있습니다. 이것이 다른 문제의 부작용이 아닌지 확인하려면 앞으로 48시간 동안 다른 RAID 경고문이 이 메일로 전달되는지 모니터링하십시오. 시스템에서 다른 RAID 관련 경고문이 없으면 이 경고문을 무시할 수 있습니다.

기타 디스크 사용량이 할당량에 가까워진다는 경고문 트러블슈팅

문제

기타 디스크 사용량이 할당량에 가까워진다는 경고문을 수신합니다.

솔루션

할당량을 늘리거나 파일을 삭제할 수 있습니다. 기타 할당량에 대한 디스크 공간 관리 , 942 페이지를 참조하십시오.

하드웨어 문제 트러블슈팅

하드웨어 어플라이언스의 전면 및/또는 후면 패널에 있는 표시등은 어플라이언스의 상태를 나타냅니다. 이러한 지표에 대한 설명은 *Cisco x90 Series Content Security Appliances* 설치 및 유지 보수 가이드 (http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html)와 같은 하드웨어 가이드를 참고하십시오.

어플라이언스 사양(예: 온도 범위)도 이러한 문서에서 확인할 수 있습니다.

어플라이언스 전원 원격 초기화

어플라이언스를 하드 초기화해야 하는 경우 서드파티 IPMI(Intelligent Platform Management Interface) 툴을 사용하여 어플라이언스 섀시를 원격으로 재부팅할 수 있습니다.

제한 사항

- 원격 전원 제어는 특정 하드웨어에서만 이용할 수 있습니다.

  자세한 내용은 원격 전원 제어 활성화 , 958 페이지를 참조하십시오.

- 이 기능을 사용하려면 먼저 활성화해야 합니다.

  자세한 내용은 원격 전원 제어 활성화 , 958 페이지를 참조하십시오.

- 다음 IPMI 명령만 지원됩니다.
  - **`status, on, off, cycle, reset, diag, soft`**
  - 지원되지 않는 명령을 실행하면 "insufficient privileges(권한 부족)" 오류가 표시됩니다.

시작하기 전에

- IPMI 버전 2.0을 사용하여 장비를 관리할 수 있는 유틸리티를 구해 설치합니다.
- 지원되는 IPMI 명령 사용 방법을 이해합니다. IPMI 툴에 대한 문서를 참조해 주십시오.

단계 **1** IPMI를 사용하여 필요한 크리덴셜과 함께 초기에 구성된 원격 전력 제어 포트에 할당된 IP 주소에 대해 지원되는 power-cycling 명령을 실행합니다.

예를 들어 IPMI가 지원되는 UNIX 유형의 머신에서는 다음 명령을 실행할 수 있습니다.

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

여기서 **192.0.2.1**은 원격 전원 제어 포트에 할당된 IP 주소이고 **remoteresetuser** 및 password는 이 기능을 사용하도록 설정하는 동안 입력한 크리덴셜입니다.

단계 **2** 어플라이언스가 재부팅될 때까지 11분 이상 기다립니다.

기술 지원 이용

가상 어플라이언스에 대한 기술 지원

가상 어플라이언스에 대한 기술 지원을 받기 위한 요구 사항은 Cisco Content Security Virtual Appliance 설치 가이드 (http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html)에서 확인할 수 있습니다.

어플라이언스에서 지원 사례 열기 또는 업데이트

시작하기 전에

- 긴급한 문제인 경우 이 방법을 사용하지 마십시오. 대신 Cisco 고객 지원, 7 페이지에 나열된 다른 방법 중 하나를 사용하여 고객 지원에 문의하십시오.

  해결 방안이 있지만 대체 솔루션을 알고 싶은 문제 또는 정보 요청 등에만 다음 절차를 사용하십시오.

- 도움을 받을 수 있는 다른 옵션을 고려합니다.
  - 기술 자료, 7 페이지
  - Cisco Support Community, 7 페이지
- 어플라이언스에서 Cisco 기술 지원에 직접 액세스하려면, Cisco.com 사용자 ID가 이 어플라이언스의 서비스 동의 계약에 연결되어 있어야만 합니다. 현재 Cisco.com 프로필과 연결된 서비스 계

약의 목록을 보려면 Cisco.com 프로필 관리자(https://sso.cisco.com/autho/forms/CDClogin.html)를 방문하십시오. Cisco.com 사용자 ID가 없는 경우, 등록하고 받으십시오. Cisco 계정 등록 , 8 페이지를 참조하십시오.

Cisco.com 사용자 ID 및 지원 계약 ID는 안전한 장소에 저장해야 합니다.

- 이 절차를 사용하여 지원 사례를 열면 어플라이언스 구성 파일이 Cisco 고객 지원으로 전송됩니다. 어플라이언스 구성을 전송하지 않으려면 다른 방법을 사용하여 고객 지원에 연락할 수 있습니다.
- 클러스터 구성에서는 지원 요청 및 저장된 값이 시스템마다 다릅니다.
- 어플라이언스가 인터넷에 연결되어 있고 이메일을 전송할 수 있어야 합니다.
- 기존 사례에 대한 정보를 전송하는 경우 사례 번호가 있어야 합니다.

단계 **1** 어플라이언스에 로그인합니다.

단계 **2** **Help and Support**(도움말 및 지원) > **Contact Technical Support**(기술 지원에 문의)를 선택합니다.

단계 **3** 양식을 작성합니다.

단계 **4** **Send**(보내기)를 클릭합니다.

참고 CCO User ID 및 최근에 입력한 Contract ID는 향후 사용을 위해 어플라이언스에 저장됩니다.

Cisco 고객 지원 담당자를 위한 원격 액세스 활성화

Cisco 고객 지원에서만 이러한 방법을 사용하여 사용자 어플라이언스에 액세스할 수 있습니다.

인터넷이 연결되는 어플라이언스에 대한 원격 액세스 활성화

기술 지원에서는 이 절차에서 어플라이언스와 **upgrades.ironport.com** 서버 간에 생성하는 SSH 터널을 통해 어플라이언스에 액세스합니다.

시작하기 전에

인터넷에서 도달할 수 있는 포트를 식별합니다. 기본값은 포트 25입니다. 시스템에서도 이메일 메시지를 전송하기 위해 해당 포트를 통한 일반 액세스가 필요하므로이는 대부분의 환경에서 작동합니다. 대부분의 방화벽 구성에서 이 포트를 통한 연결이 허용됩니다.

단계 **1** 어플라이언스에 로그인합니다.

단계 **2** GUI 창의 오른쪽에서 **Help and Support**(도움말 및 지원) > **Remote Access**(원격 액세스)를 선택합니다.

단계 **3** **Enable**(활성화)을 클릭합니다.

단계 **4** 다음 정보를 입력합니다.

옵션	설명
Seed String(시드 문자열)	시드 문자열은 Cisco 고객 지원팀에서 이 어플라이언스에 액세스하는 데 사용할 안전한 공유 암호를 생성하는 데 사용합니다.
Secure Tunnel(보안 터널)	원격 액세스 연결을 위한 보안 터널 사용 확인란을 선택합니다. 연결을 위한 포트를 입력합니다. 기본값은 포트 25이며, 대부분의 환경에서 작동합니다.

단계 **5** **Submit**(제출)을 클릭합니다.

다음에 수행할 작업

지원 담당자의 원격 액세스가 더 이상 필요하지 않은 경우 기술 지원 터널 비활성화 , 1174 페이지 섹션을 참조해 주십시오.

직접 인터넷에 연결되지 않은 어플라이언스에 대한 원격 액세스 활성화

직접 인터넷에 연결되지 않은 어플라이언스의 경우 인터넷에 연결된 두 번째 어플라이언스를 통해 액세스할 수 있습니다.

시작하기 전에

- 문제의 어플라이언스는 포트 22에서 인터넷에 연결된 두 번째 어플라이언스에 연결할 수 있어야 합니다.
- 인터넷이 연결되는 어플라이언스에서 인터넷이 연결되는 어플라이언스에 대한 원격 액세스 활성화 , 1172 페이지의 절차에 따라 문제의 어플라이언스에 대한 지원 터널을 생성합니다.

단계 **1** 지원이 필요한 어플라이언스의 CLI에서 **techsupport** 명령을 입력합니다.

단계 **2** **sshaccess**를 입력합니다.

단계 **3** 프롬프트에 따라 수행합니다.

다음에 수행할 작업

지원 담당자의 원격 액세스가 더 이상 필요하지 않은 경우 다음을 참조하십시오.

- 원격 액세스 비활성화 , 1174 페이지
- 기술 지원 터널 비활성화 , 1174 페이지

기술 지원 터널 비활성화

활성화된 techsupport 터널은 7일 동안 upgrades.ironport.com에 연결되어 있습니다. 그 이후에는 설정된 연결이 끊어지는 것이 아니라, 끊어진 터널에 다시 연결할 수 없게 됩니다.

터널을 수동으로 비활성화하려면

단계 **1** 어플라이언스에 로그인합니다.

단계 **2** GUI 창의 오른쪽에서 **Help and Support(**도움말 및 지원**) > Remote Access(**원격 액세스**)**를 선택합니다.

단계 **3** **Disable(**비활성화**)**을 클릭합니다.

원격 액세스 비활성화

techsupport 명령을 사용하여 만든 원격 액세스 계정은 비활성화할 때까지 활성 상태가 유지됩니다.

단계 **1** CLI에서 techsupport 명령을 입력합니다.

단계 **2** sshaccess를 입력합니다.

단계 **3** disable을 입력합니다.

지원 연결의 상태 확인

단계 **1** CLI에서 techsupport 명령을 입력합니다.

단계 **2** status를 입력합니다.

패킷 캡처 실행

패킷 캡처를 사용하면 지원 담당자가 어플라이언스에서 들어가고 나오는 TCP/IP 데이터 및 기타 패킷을 볼 수 있습니다. 이를 통해 고객 지원에서는 네트워크 설정을 디버그하고 어떤 네트워크 트래픽이 어플라이언스에 도달하는지 또는 어플라이언스를 떠나는지를 확인할 수 있습니다.

단계 **1** **Help and Support(**도움말 및 지원**) > Packet Capture(**패킷 캡처**)**를 선택합니다.

단계 **2** 패킷 캡처 설정을 지정합니다.

a) **Packet Capture Settings(**패킷 캡처 설정**)** 섹션에서 **Edit Settings(**설정 수정**)**를 클릭합니다.

b) (선택 사항) 패킷 캡처의 기간, 제한 사항 및 필터를 입력합니다.

지원 담당자가 이러한 설정을 안내해줄 수 있습니다.

시간 단위를 지정하지 않고 캡처 기간을 입력하면 기본적으로 초 단위가 사용됩니다.

Filters(필터**)** 섹션에서

- 맞춤 필터는 UNIX tcpdump 명령에서 지원하는 구문(예: host 10.10.10.10 && port 80)을 사용할 수 있습니다.
- 클라이언트 IP는 어플라이언스에 연결하는 머신(예: Email Security Appliance를 통해 메시지를 전송하는 메일 클라이언트)의 IP 주소입니다.
- 서버 IP는 어플라이언스가 연결하는 머신(예: 어플라이언스가 메시지를 전달하는 Exchange Server)의 IP 주소입니다.
- Email Security Appliance를 중간에 둔 특정 클라이언트와 특정 서버 간 트래픽을 추적하려면 클라이언트 및 서버 IP 주소를 사용할 수 있습니다.

c) **Submit(**제출**)**을 클릭합니다.

단계 **3** **Start Capture(**캡처 시작**)**를 클릭합니다.

- 한 번에 캡처를 하나만 실행할 수 있습니다.
- 패킷 캡처가 실행 중이면 현재 통계(예: 파일 크기 및 경과 시간)와 함께 Packet Capture(패킷 캡처) 페이지에 진행 중인 캡처의 상태가 표시됩니다.
- GUI에는 CLI가 아니라 GUI에서 시작된 패킷 캡처만 표시됩니다. 마찬가지로 CLI에는 CLI에서 시작된 현재 패킷 캡처의 상태만 표시됩니다.
- 패킷 캡처 파일은 10개 부분으로 나누어집니다. 패킷 캡처가 끝나기 전에 파일이 최대 크기 제한에 도달하면 파일의 가장 오래된 부분이 삭제되고(데이터가 삭제됨) 현재 패킷 캡처 데이터로 새 부분이 시작됩니다. 한 번에 패킷 캡처 파일의 1/10만 삭제됩니다.
- GUI에서 시작되어 실행 중인 캡처는 세션 간에 유지됩니다. (CLI에서 시작되어 실행 중인 캡처는 세션이 끝나면 중단됩니다.)

단계 **4** 지정된 기간에 캡처가 실행되도록 합니다. 또는 캡처가 무한정 실행되도록 한 경우 **Stop Capture(**캡처 중단**)**를 클릭하여 캡처를 수동으로 중단합니다.

단계 **5** 패킷 캡처 파일에 액세스합니다.

- **Manage Packet Capture Files(**패킷 캡처 파일 관리**)** 리스트에서 파일을 클릭하고 **Download File(**파일 다운로드**)**을 클릭합니다.
- 어플라이언스의 captures 하위 디렉터리에 있는 파일에 액세스하려면 FTP 또는 SCP를 사용합니다.

다음에 수행할 작업

고객 지원에서 파일을 사용할 수 있도록 합니다.

- 어플라이언스에 대한 원격 액세스를 허용하면 기술 지원 담당자가 FTP 또는 SCP를 사용하여 패킷 캡처 파일에 액세스할 수 있습니다. Cisco 고객 지원 담당자를 위한 원격 액세스 활성화 , 1172 페이지를 참조하십시오.
- 이메일로 파일을 고객 지원에 전송합니다.

44 장

D-Mode를 사용하여 아웃바운드 메일 전달용 어플라이언스 최적화

이 장에는 다음 섹션이 포함되어 있습니다.

기능 요약: 최적화된 아웃바운드 전달용 D-Mode

D-Mode는 아웃바운드 이메일 전달을 위해 특정 Email Security Appliance를 최적화하는 기능으로, 기능 키에 의해 활성화됩니다. 인바운드 메일 처리와 관련된 기능은 D-Mode에서 비활성화됩니다.

D-Mode 활성화 어플라이언스의 고유한 기능

- 256 가상 게이트웨이 주소(Virtual Gateway Address) - Cisco Virtual Gateway 기술을 사용하면 호스팅하는 모든 도메인에 대해 엔터프라이즈 메일 게이트웨이를 구성하고(고유한 IP 주소, 호스트 이름 및 도메인으로), 이러한 도메인에 대한 별도의 기업 이메일 정책 시행 및 안티스팸 전략을 만들 수 있습니다(동일한 물리적 어플라이언스 내에 호스팅). 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지의 "Customizing Listeners(리스너 맞춤화)"을 참조해 주십시오.
- IPMM(IronPort Mail Merge) - IPMM(IronPort Mail Merge)은 고객 시스템에서 개인화된 개별 메시지를 생성해야 하는 부담을 없애줍니다. 수천 개의 개별 메시지를 생성하여 메시지 생성 시스템과 이메일 게이트웨이 간에 전송해야 할 필요가 없으므로, 사용자는 시스템 부하 감소 및 이메일 전달 처리량 증가라는 이점을 누릴 수 있습니다. 자세한 내용은 IPMM(IronPort Mail Merge)을 사용하여 대량 메일 전송, 1180 페이지를 참고해 주십시오.
- 리소스 보존 반송 설정 - D-Mode 활성화 어플라이언스를 구성하여 잠재적인 차단 대상을 탐지하고 해당 대상으로 가려는 모든 메시지를 반송할 수 있습니다. 자세한 내용은 리소스 보존 반송 설정 구성, 1179 페이지를 참고해 주십시오.

- 아웃바운드 전달 성능 향상

D-Mode 활성화 어플라이언스에서 비활성화되는 표준 기능

- IronPort Anti-Spam Scanning 및 On/Off 상자 스팸 격리 - 안티스팸 검사는 대부분 수신 메일과 관련이 있으므로 IronPort Anti-Spam Scanning 엔진은 비활성화됩니다. 따라서 안티스팸 장은 적용되지 않습니다.
- Outbreak Filter - Outbreak Filter 기능은 수신 메일 격리에 사용되므로 D-Mode 활성화 어플라이언스에서는 비활성화됩니다. 따라서 Outbreak Filter 장의 정보는 적용되지 않습니다.
- SenderBase Network Participation 기능 - SenderBase Network Participation는 수신 메일에 대한 정보를 보고하므로 D-Mode 활성화 어플라이언스에서는 비활성화됩니다. SenderBase Network Participation에 대한 정보는 적용되지 않습니다.
- 보고 - 보고는 제한적입니다. 일부 보고서는 사용할 수 없으며, 수행되는 보고는 성능상의 이유로 매우 제한적인 레벨에서 이루어지도록 설정됩니다.

참고 D-Mode 활성화 어플라이언스에 대한 Email Security Monitor Overview(이메일 보안 모니터 개요) 보고서에 표시되는 총계에 포함된 스팸 및 의심스런 스팸 수에는 오류가 있을 수 있습니다(이러한 기능이 D-Mode 활성화 어플라이언스에서 비활성화된 경우에도).

- Data Loss Prevention - 발신 메시지에 대한 DLP 검사는 D-Mode 활성화 어플라이언스에서 비활성화됩니다.

D-Mode 활성화 어플라이언스에 적용되는 표준 기능

표 ***152: D-Mode*** 활성화 어플라이언스에 포함된 ***AsyncOS*** 기능

기능	추가 정보
안티바이러스 검사	Anti-Virus, 335 페이지 항목을 참조하십시오.
도메인 키 서명	DKIM/도메인 키는 발신자가 사용하는 서명 키를 기반으로 이메일의 신뢰성을 확인하기 위한 방법입니다. 이메일 인증, 571 페이지을 참고해 주십시오.
중앙 집중식 관리	클러스터를 사용한 중앙 집중식 관리, 1117 페이지 항목을 참조하십시오.
전달 조절	각 도메인에 대해 지정된 시간 동안 시스템에서 초과할 수 없는 최대 연결 및 수신자 수를 할당할 수 있습니다. destconfig 명령을 통해 "Good Neighbor" Table이 정의됩니다. 자세한 내용은 대상 제어를 사용하여 이메일 전달 제어, 703 페이지를 참고해 주십시오.

기능	추가 정보
반송 확인	반송 메시지의 신뢰성을 확인합니다. 반송 확인, 703 페이지를 참조하십시오.
위임 관리	관리 작업 배포, 893 페이지 항목을 참조하십시오.
추적(디버그)	테스트 메시지를 사용하여 메일 플로우 디버깅: 추적, 1149 페이지를 참조하십시오.
VLAN, NIC 페어링	고급 네트워크 컨피그레이션, 1039 페이지을 참고해 주십시오.
선택적인 안티바이러스 엔진	아웃바운드 메시지의 무결성을 확인하기 위해 선택적인 안티바이러스 검사를 추가할 수 있습니다. 안티바이러스 검사 개요, 335 페이지를 참조하십시오.

최적화된 아웃바운드 메일 전달을 위한 어플라이언스 설정

단계 **1** 제공된 기능 키를 적용합니다. 시스템 설정 마법사를 실행하기 전에(어플라이언스를 구성하기 전에) Cisco Email Security Appliance에 키를 적용해야 합니다. System Administration(시스템 관리) > Feature Key(기능 키) 페이지를 통해 또는 CLI에서 featurekey 명령을 실행하여 키를 적용합니다.

참고 이러한 기능 키에는 아웃바운드 메일에서 안티바이러스 검사를 테스트하는 데 사용할 수 있는 30일 Sophos 또는 McAfee Anti-Virus 라이센스가 포함되어 있습니다.

단계 **2** 어플라이언스를 재부팅합니다.

단계 **3** 시스템 설정 마법사를 실행하고(GUI 또는 CLI) 어플라이언스를 구성합니다.

아웃바운드 전달에 최적화된 어플라이언스에는 안티스팸 검사 또는 보안 침해 필터 기능이 포함되지 않는다는 점에 유의해 주십시오. (이러한 장은 무시해 주십시오.)

참고 클러스터링된 환경에서 D-Mode 기능 키로 구성된 어플라이언스를 전달 성능 패키지로 구성된 AsyncOS 어플라이언스와 결합할 수 없습니다.

리소스 보존 반송 설정 구성

최적화된 아웃바운드 메일 전달을 위해 어플라이언스를 구성했으면, 잠재적인 전달 문제를 탐지하고 해당 대상으로 가려는 모든 메시지를 반송하도록 시스템을 구성할 수 있습니다.

참고 이 설정을 사용하면 전달 불가로 간주되는 대상 도메인에 대한 대기열에 있는 모든 메시지가 반송됩니다. 전달 문제가 해결된 후 메시지를 다시 전송해야 합니다.

리소스 보존 반송 설정 활성화의 예

```
mail3.example.com> bounceconfig

Choose the operation you want to perform:

- NEW - Create a new profile.

- EDIT - Modify a profile.

- DELETE - Remove a profile.

- SETUP - Configure global bounce settings.

[]> setup

Do you want to bounce all enqueued messages bound for a domain if the host is down? [N]>

y
```

이 기능을 사용하면 최소 10회 연속 연결 시도가 실패한 후 호스트가 "다운"된 것으로 간주됩니다. AsyncOS는 15분마다 다운된 호스트를 검사하므로, 대기열이 삭제되기 전에 10회 넘는 시도가 이루어질 수 있습니다.

IPMM(IronPort Mail Merge)을 사용하여 대량 메일 전송

참고 IronPort Mail Merge는 D-Mode가 활성화된 어플라이언스에서만 사용할 수 있습니다.

IronPort Mail Merge 개요

IronPort Mail Merge는 고객 시스템에서 개인화된 개별 메시지를 생성해야 하는 부담을 없애줍니다. 수천 개의 개별 메시지를 생성하여 메시지 생성 시스템과 이메일 게이트웨이 간에 전송해야 할 필요가 없으므로, 시스템 부하가 감소하고 이메일 전달 처리량이 증가합니다.

IPMM을 사용하면 단일 메시지 본문을 만들고 메시지에서 위치를 나타내는 변수를 각 개인에 맞게 교체할 수 있습니다. 각 개별 메시지 수신자에 대해 수신자 이메일 주소 및 변수 치환만 이메일 게이트웨이에 전송하면 됩니다. 또한 IPMM을 사용하면 특정 수신자에 해당하는 메시지 본문의 "부분"을 전송하는 한편 다른 수신자에 대해서는 해당 부분을 제외할 수 있습니다. (예를 들어 두 개의 다른 국가 수신자에게는 메시지 끝에 다른 저작권 문장을 포함해야 할 수 있습니다.)

메일 병합 기능의 이점

- 메일 관리자의 편의성. IPMM은 일반적인 여러 언어로 변수 치환 및 추상화된 인터페이스를 제공하므로 각 수신자에 대해 개인화된 메시지를 만드는 복잡성이 사라집니다.

- 메시지 생성 시스템의 부하 감소. 메시지 본문 복사본 하나와 필수 치환 테이블만 필요하며, 메시지 생성 "작업" 대부분이 메시지 생성 시스템에서 분리되어 최적화된 아웃바운드 메일 전송을 위해 구성된 어플라이언스로 이동합니다.
- 전달 처리량 향상. 수천 개의 수신 메시지를 수락하고 대기열에 추가하기 위해 필요한 리소스가 감소하므로 어플라이언스의 아웃바운드 전달 성능이 크게 향상될 수 있습니다.
- 대기열 저장소 효율성. 각 메시지 수신자에 대한 정보를 덜 저장하므로 사용자는 D-Mode 활성화 어플라이언스에서 대기열 스토리지 사용을 몇십 배 개선할 수 있습니다.

메일 병합 사용

SMTP 주입

IPMM은 SMTP를 전송 프로토콜로 확장합니다. 어플라이언스에 대해 수행해야 하는 특별한 컨피그레이션이 없습니다. (D-Mode 활성화 어플라이언스에서 기본적으로 IPMM을 프라이빗 리스너에 대해서는 활성화하고 퍼블릭 리스너에 대해서는 비활성화할 수 있습니다.) 그러나 현재 SMTP를 주입 프로토콜로 사용하지 않는 경우, D-Mode 활성화 어플라이언스 인터페이스를 통해 SMTP를 활용하는 새로운 프라이빗 리스너를 만들어야 합니다.

리스너에서 IPMM을 활성화하려면 listenerconfig의 setipmm 하위 명령을 사용합니다. 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 69 페이지을 참조해 주십시오.

IPMM은 두 가지 명령(MAIL FROM 및 DATA)을 변경하고 또 다른 명령(XDFN)을 추가하여 SMTP를 수정합니다. MAIL FROM 명령은 XMRG FROM으로 교체되고 DATA 명령은 XPRT로 교체됩니다.

메일 병합 메시지를 생성하려면 메시지 생성에 사용된 명령을 특정 시퀀스에서 실행해야 합니다.

1. 전송 호스트를 식별하는 초기 EHLO 문.
2. 각 메시지는 발신자 주소를 나타내는 XMRG FROM: 문으로 시작됩니다.
3. 그런 다음 각 수신자가 정의됩니다.
4. 부분(XDFN *PART=1,2,3…) 및 기타 수신자 관련 변수를 포함하는 하나 이상의 XDFN 변수 할당문이 만들어집니다.
5. 수신자 이메일 주소는 RCPT TO: 문으로 정의됩니다. RCPT TO: 명령 이전 및 XMRG FROM 또는 RCPT TO 명령 이후에 할당되는 변수는 이 수신자 이메일 주소에 매핑됩니다.
6. 각 부분은 XPRT n 명령을 사용하여 정의되며, DATA 명령과 유사하게 마침표(.) 문자로 끝납니다. 마지막 부분은 XPRT n LAST 명령으로 정의됩니다.

변수 대체

메시지 헤더를 포함한 메시지 본문의 부분은 치환용 변수를 포함할 수 있습니다. 변수는 HTML 메시지에도 나타날 수 있습니다. 변수는 사용자가 정의하며, 앰퍼샌드 문자(&)로 시작하고 세미콜론 문자(;)로 끝나야 합니다. 별표(*)로 시작되는 변수 이름은 예약되어 있으므로 사용할 수 없습니다.

예약된 변수

IPMM에는 미리 정의된 다섯 개의 특수한 "예약된" 변수가 있습니다.

표 ***153: IPMM:*** 예약된 변수

*FROM	예약된 변수 *FROM은 "Envelope From" 매개변수에서 파생됩니다. "Envelope From" 매개변수는 "XMRG FROM:" 명령으로 설정됩니다.
*TO	예약 변수 *TO는 "RCPT TO:" 명령을 사용하여 설정된 대로 봉투 수신자 값에서 파생됩니다.
*PARTS	예약 변수 *PARTS는 쉼표로 구분된 파트 목록을 보유합니다. 이 변수는 RCPT TO:"로 수신자를 정의하기 전에 설정되며, 지정된 사용자가 어떤 "XPRT n" 메시지 본문 블록을 수신할지를 결정합니다.
*DATE	예약 변수 *DATE는 현재 날짜 스탬프로 대체됩니다.
*DK	예약된 변수 *DK는 DomainKeys Signing 프로필 정의에 사용됩니다(이 프로필은 AsyncOS에 이미 있음). DomainKeys Signing 프로필 만들기에 대한 자세한 내용은 이메일 인증, 571 페이지을 참조해 주십시오.

메시지 예 1

다음 메시지 본문 예(헤더 포함)에는 최종 메시지에서 교체될 변수 4개 및 치환 위치 5개가 포함되어 있습니다. 메시지 본문에서 동일한 변수를 두 번 이상 사용할 수 있습니다. 또한 수신자 이메일 주소로 교체될 예약된 변수 &*TO;가 사용됩니다. 이 예약된 변수는 별도의 변수로서 전달할 필요가 없습니다. 다음 예에서 변수는 굵게 표시됩니다.

```
From: Mr.Spacely <spacely@example.com>

To: &first_name;&last_name;&*TO;


Subject: Thanks for Being an Example.Com Customer

Dear &first_name;,
Thank you for purchasing a &color; sprocket.
```

어플라이언스에 이 메시지를 한 번만 주입하면 됩니다. 각 수신자에 대해 다음의 추가 정보가 필요합니다.

- 수신자 이메일 주소
- 변수 치환용 이름-값 쌍

부분 조립

SMTP는 각 메시지 본문에 단일 DATA 명령을 사용하지만, IPMM은 하나 이상의 XPRT 명령을 사용하여 메시지를 구성합니다. 수신자 단위로 지정된 순서에 따라 부분이 조립됩니다. 각 수신자는 메시지 부분의 일부 또는 전부를 수신할 수 있습니다. 부분은 순서에 따라 조립될 수 있습니다.

특수 변수 *PARTS는 쉼표로 구분된 부분의 리스틀를 보유합니다.

예를 들어 다음 메시지 예에는 2개의 부분이 포함되어 있습니다.

첫 번째 부분에는 메시지 헤더와 메시지 본문 일부가 포함되어 있습니다. 두 번째 부분에는 특정 고객을 위해 변수로 포함할 수 있는 내용이 포함되어 있습니다.

메시지 예 2, 부분 1

```
From: Mr. Spacely <spacely@example.com>


To: &first_name; &last_name; &*TO;

Subject: Thanks for Being an Example.Com Customer

Dear &first_name;,

Thank you for purchasing a &color; sprocket.
```

메시지 예 2, 부분 2

```
Please accept our offer for 10% off your next sprocket purchase.
```

어플라이언스에 메시지 부분을 한 번만 주입하면 됩니다. 이 경우에는 각 수신자에게 다음과 같은 추가 정보가 필요합니다.

- 최종 메시지에 포함할 부분의 순서가 지정된 리스트
- 수신자 이메일 주소
- 변수 치환용 이름-값 쌍

IPMM 및 DomainKeys Signing

IPMM은 DomainKeys Signing을 지원합니다. DomainKeys 프로필을 지정하려면 예약된 변수 *DK를 사용합니다. 예를 들면 다음과 같습니다.

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2 *DK=mass_mailing_1
```

이 예에서 "mail_mailing_1"은 전에 구성한 DomainKeys 프로필의 이름입니다.

명령 설명

클라이언트는 리스너에 IPMM 메시지를 주입할 때 다음 키 명령과 함께 확장된 SMTP를 사용합니다.

XMRG FROM

구문:

```
XMRG FROM: <sender email address>
```

이 명령은 SMTP MAIL FROM: 명령을 교체하며, 다음에 오는 것이 IPMM 메시지임을 나타냅니다. IPMM 작업이 XMRG FROM: 명령으로 시작됩니다.

XDFN

구문:

```
XDFN <KEY=VALUE> [KEY=VALUE]
```

XDFN 명령은 수신자별 메타데이터를 설정합니다. 선택적으로 키-값 쌍을 꺾쇠괄호 또는 대괄호로 묶을 수 있습니다.

*PARTS는 XPRT 명령으로 정의된 인덱스 번호를 나타내는 특수 예약된 변수입니다(아래에서 설명). *PARTS 변수는 쉼표로 구분된 정수 리스트입니다. 정수는 전송할 본문 부분(XPRT 명령으로 정의)과 일치합니다. 다른 예약된 변수는 *FROM, *TO 및 *DATE입니다.

XPRT

구문:

```
XPRT index_number LAST

Message

.
```

XPRT 명령은 SMTP DATA 명령을 교체합니다. 이 명령은 명령 실행 후 메시지 전송을 수락합니다. 이 명령은 줄 바꿈한 줄의 단일 마침표로 완료됩니다(SMTP DATA 명령이 완료되는 것과 같은 방법).

특수 키워드 **LAST**는 메일 병합 작업의 끝을 나타내며, 주입될 최종 부분을 지정하는 데 사용해야 합니다.

LAST 키워드가 사용된 후 메시지가 대기열에 추가되고 전달이 시작됩니다.

변수 정의 참고 사항

- XDFN 명령으로 변수를 정의할 때, 실제 명령줄이 시스템의 물리적 제한을 초과할 수 없다는 점에 유의해야 합니다. D-Mode 활성화 어플라이언스의 경우 이 제한은 줄당 4킬로바이트입니다. 다른 호스트 시스템의 임계값은 더 작을 수 있습니다. 매우 큰 줄에 여러 변수를 정의할 때는 각별히 주의해야 합니다.
- 키-값 쌍 변수를 정의할 때 슬래시 문자("/")를 사용하여 특수 문자를 이스케이프할 수 있습니다. 이는 메시지 본문에 실수로 변수 정의와 교체될 수 있는 HTML 문자 엔티티가 포함된 경우 유용합니다. 예를 들어 문자 엔티티 ™는 상표 문자에 대한 HTML 문자 엔티티를 정의합니다. XDFN trade=foo 명령을 만든 후 HTML 문자 엔티티 “ ™ ”이 포함된 IPMM 메시지를 만든 경우, 조립된 메시지에는 상표 문자 대신 변수 치환("foo")이 포함됩니다. GET 명령을 포함하는 URL에 더러 사용되는 앰퍼샌드 문자 "&"에도 동일한 개념이 적용됩니다.

IPMM 변환 예

다음은 메시지 예 #2(위)의 IPMM 변환 예입니다. 이 예에서는 메시지가 두 명의 수신자, 즉 "Jane User" 및 "Joe User"에게 전송됩니다.

이 예에서 **bold** 텍스트는 D-Mode 활성화 어플라이언스에서 수동 SMTP 변환에 입력할 내용을 나타내고, monospaced type 텍스트는 SMTP 서버로부터의 응답, *italic type*은 코멘트나 변수를 나타냅니다.

연결이 설정됩니다.

```
220 ESMTP
```

```
EHLO foo

250 - ehlo responses from the listener enabled for IPMM
```

대화가 시작됩니다.

```
XMRG FROM:<user@domain.com> [Note: This replaces the MAIL FROM: SMTP command.]

250 OK
```

각 수신자에 대한 변수 및 부분이 설정됩니다.

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2

[Note: This line defines three variables (first_name, last_name, and color) and then
uses the *PARTS reserved variable to define that the next recipient defined will receive
message parts numbers 1 and 2.]

250 OK

RCPT TO:<jane@company.com>

250 recipient <jane@company.com> ok

XDFN first_name="Joe" last_name="User" color="black" *PARTS=1

[Note: This line defines three variables (first_name, last_name, and color) and then
uses the *PARTS reserved variable to define that the next recipient defined will receive
message parts numbers 1 only.]

RCPT TO:<joe@company1.com>

250 recipient <joe@company1.com> ok
```

이제 부분 1이 전송됩니다.

```
XPRT 1 [Note: This replaces the DATA SMTP command.]

354 OK, send part

From: Mr. Spacely <spacely@example.com>

To: &first_name; &last_name; &*TO;

Subject: Thanks for Being an Example.Com Customer

&*DATE;

Dear &first_name;,

Thank you for purchasing a &color; sprocket.

.
```

그런 다음 부분 2가 전송됩니다. LAST 키워드는 조립할 최종 부분으로 부분 2를 식별하는 데 사용됩니다.

```
XPRT 2 LAST
```

```
Please accept our offer for 10% off your next sprocket purchase.

.

250 Ok, mailmerge message enqueued
```

"250 Ok, mailmerge message queued"는 메시지가 수락되었음을 나타냅니다.

이 예의 경우 수신자 Jane User가 이 메시지를 수신합니다.

```
From: Mr. Spacely <spacely@example.com>

To: Jane User <jane@company.com>

Subject: Thanks for Being an Example.Com Customer

message date

Dear Jane,

Thank you for purchasing a red sprocket.

Please accept our offer for 10% off your next sprocket purchase.
```

수신자 Joe User가 이 메시지를 수신합니다.

```
From: Mr. Spacely <spacely@example.com>

To: Joe User <joe@company1.com>

Subject: Thanks for Being an Example.Com Customer

message date

Dear Joe,

Thank you for purchasing a black sprocket.
```

코드 예

Cisco에서는 IPMM에 대해 활성화된 어플라이언스 리스너에 IPMM 메시지를 주입하는 작업을 추상화하기 위해 일반 프로그래밍 언어로 라이브러리를 만들었습니다. IPMM 라이브러리 사용 방법의 예는 Cisco 고객 지원에 문의하십시오. 코드 구문을 설명하기 위해 코멘트가 광범위하게 사용됩니다.

45 장

Cisco Content(M-Series) Security Management Appliance에서 서비스 중앙 집중화

이 장에는 다음 섹션이 포함되어 있습니다.

Cisco Content Security Management Appliance Services 개요

Cisco Content Security Management Appliance(M-Series 어플라이언스)는 여러 Email Security Appliance에서 특정 서비스에 대한 단일 인터페이스를 제공하는 외부 또는 "오프 박스" 위치에 있습니다.

Security Management Appliance에는 다음 기능이 포함되어 있습니다.

- 외부 스팸 격리. 최종 사용자를 위해 스팸 및 스팸 의심 메시지를 보관하며, 최종 사용자 및 관리자는 최종 결정을 내리기 전에 스팸으로 플래그가 지정된 메시지를 검토할 수 있습니다.
- 중앙 집중식 정책, 바이러스 및 Outbreak 격리. 안티바이러스 검사, Outbreak 필터 및 정책별로 격리된 메시지를 저장하고 관리하기 위한 방화벽 뒤의 단일 위치를 제공합니다.
- 중앙 집중식 보고. Email Security Appliance에서 온 집계된 데이터에 대한 보고서를 실행합니다.
- 중앙 집중식 추적. 여러 Email Security Appliance에서 이메일 메시지를 추적합니다.

Cisco Content Security Management Appliance를 구성하고 사용하는 방법에 대한 전체 정보는 Cisco Content Security Management Appliance 사용자 가이드를 참고하십시오.

주의 Email Security Appliance에서 이중 인증을 활성화한 경우 사전 공유 키를 사용하여 이를 Security Management Appliance에 추가할 수 있습니다. 이 설정을 구성하려면 CLI에서 `smaconfig > add` 명령을 사용합니다.

OR

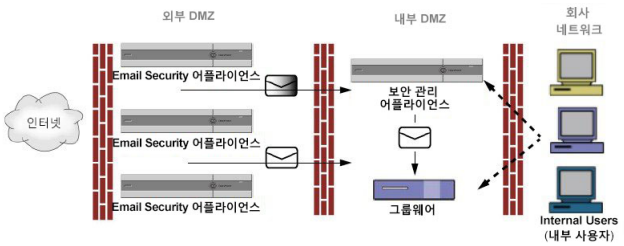
Email Security Appliance에서 이중 인증을 비활성화한 후 Security Management Appliance에 추가합니다. 자세한 내용은 이중 인증 비활성화, 913 페이지를 참고하십시오.

네트워크 계획

Cisco Content Security Management Appliance에서는 엔드 유저 인터페이스(예: 메일 애플리케이션)를 각종 DMZ에 상주하는 좀 더 안전한 게이트웨이 시스템과 분리할 수 있습니다. 2-레이어 방화벽을 사용하면 최종 사용자가 외부 DMZ에 직접 연결하지 않도록 네트워크를 유연하게 계획할 수 있습니다.

다음 그림은 Security Management Appliance 및 여러 DMZ를 통합하는 일반적인 네트워크 구성을 보여줍니다.

그림 ***87: Cisco Content Security Management Appliance***의 일반적인 네트워크 구성



대기업 데이터 센터는 하나 이상의 Email Security Appliance에 대한 외부 스팸 격리 역할을 하는 하나의 Security Management Appliance를 공유할 수 있습니다. 한편, 원격 사무실은 로컬 사용을 위한 Email Security Appliance에서 로컬 스팸 격리를 유지할 수 있습니다.

외부 스팸 격리 작업

- 메일 플로우 및 외부 스팸 격리 , 1189 페이지
- 로컬 스팸 격리를 외부 격리로 마이그레이션, 1189 페이지
- 외부 스팸 격리 및 외부 허용 목록/차단 목록 활성화 , 1190 페이지
- 로컬 스팸 격리를 비활성화하여 외부 격리 활성화 , 1191 페이지
- 외부 스팸 격리 문제 해결 , 1191 페이지

메일 플로우 및 외부 스팸 격리

네트워크가 네트워크 계획, 1188 페이지에 설명된 대로 구성된 경우 인터넷의 수신 메일은 외부 DMZ의 어플라이언스에서 수신됩니다. 깨끗한 메일은 내부 DMZ의 MTA(mail transfer agent)(그룹웨어)로 전송되고 궁극적으로 회사 네트워크 내 최종 사용자에게 전송됩니다.

스팸 또는 의심스러운 스팸(메일 플로우 정책 설정에 따라)은 Security Management Appliance의 스팸 격리로 전송됩니다. 그러면 최종 사용자는 격리에 액세스하여 스팸을 삭제하고, 자신에게 전달되도록 할 메시지를 릴리스할 수 있습니다. 스팸 격리에 남아 있는 메시지는 구성된 시간이 지나면 자동으로 삭제됩니다.

Security Management Appliance의 외부 격리에서 릴리스된 메시지는 전달을 위해 원래 Email Security Appliance로 반환됩니다. 이러한 메시지는 일반적으로 전달 전에 HAT 및 기타 정책 또는 검사 설정, RAT, 도메인 예외, 별칭, 수신 필터, 가장, 반송 확인, 작업 대기열의 프로세스를 거치지 않습니다.

Security Management Appliance로 메일을 전송하도록 구성된 Email Security Appliance는 Security Management Appliance에서 릴리스된 메일을 자동으로 수신하며, 다시 수신할 경우 메시지를 재처리하지 않습니다. 이를 위해서는 Security Management Appliance의 IP 주소가 변경되지 않아야 합니다. Security Management Appliance의 IP 주소가 변경되면 수신 Email Security Appliance는 다른 수신 메시지와 마찬가지 방식으로 메시지를 처리합니다. Security Management Appliance에서 수신 및 전달하려면 항상 동일한 IP 주소를 사용해야 합니다.

Security Management Appliance는 스팸 격리 설정에 지정된 IP 주소의 격리에서 오는 메일을 수락합니다. Security Management Appliance의 스팸 격리를 구성하려면 Cisco Content Security Management Appliance 사용 설명서를 참조하십시오.

Security Management Appliance에서 릴리스된 메일은 스팸 격리 설정에 정의된 기본 및 보조 호스트(Content Security Appliance 또는 기타 그룹웨어 호스트)로 전달됩니다(Cisco Content Security Management Appliance 사용 설명서 참조). 따라서 Security Management Appliance에 메일을 전달하는 Email Security Appliance의 수와 상관없이, 릴리스된 모든 메일, 알림 및 경고는 단일 호스트(그룹웨어 또는 Content Security Appliance)로 전송됩니다. Security Management Appliance에서의 전달로 기본 호스트에 과부하가 걸리지 않도록 주의하십시오.

로컬 스팸 격리를 외부 격리로 마이그레이션

현재 Email Security Appliance에서 로컬 스팸 격리를 사용 중이지만 로컬 격리의 메시지에 대한 액세스를 유지한 상태로 Security Management Appliance에 호스팅된 외부 스팸 격리로 마이그레이션하려는 경우 전환 중에 새 메시지가 로컬 격리로 들어가지 못하게 해야 합니다.

다음의 가능한 전략을 고려해보십시오.

- 안티 스팸 설정 구성 - Security Management Appliance를 대체 호스트로 지정하는 메일 정책에서 안티 스팸 설정을 구성합니다. 이 작업은 로컬 격리에 대한 액세스를 허용하는 한편 외부 격리로 새 스팸을 전송합니다.
- 만료 시간을 더 짧게 설정 - 로컬 격리에서 Schedule Delete After(삭제 예약) 설정을 더 짧은 기간으로 구성합니다.
- 나머지 메시지 모두 삭제 - 로컬 격리에서 나머지 메시지를 모두 삭제하려면 격리를 비활성화하고 로컬 격리 페이지에서 "Delete All(모두 삭제)" 링크를 클릭합니다(스팸 격리에서 메시지 삭제,

891 페이지 참조). 여전히 메시지를 포함하고 있는 로컬 스팸 격리가 비활성화된 경우에만 이 링크를 사용할 수 있습니다.

이제 외부 격리를 활성화하고 로컬 격리를 비활성화할 준비가 되었습니다.

참고 로컬 격리와 외부 격리가 모두 활성화되면 로컬 격리가 사용됩니다.

외부 스팸 격리 및 외부 허용 목록/차단 목록 활성화

Email Security Appliance에서 외부 스팸 격리를 하나만 활성화할 수 있습니다.

시작하기 전에

- 메일 플로우 및 외부 스팸 격리 , 1189 페이지의 정보를 검토합니다.
- 로컬 스팸 격리를 외부 격리로 마이그레이션, 1189 페이지의 정보를 검토하고 작업을 수행합니다.
- 중앙 집중식 스팸 격리 및 허용 목록/차단 목록 기능을 지원하도록 Security Management Appliance를 구성합니다. Security Management Appliance에 대한 설명서를 참조하십시오.
- Email Security Appliance에 대해 전에 다른 외부 스팸 격리를 구성한 경우 먼저 외부 스팸 격리 설정을 비활성화합니다.

각 Email Security Appliance에서 다음 절차를 완료합니다.

단계 **1** **Security Services(**보안 서비스**) > Centralized Services(**중앙 집중식 서비스**) > Spam Quarantine(**스팸 격리**)**을 선택합니다.

단계 **2** **Configure(**구성**)**를 클릭합니다.

단계 **3** **Enable External Spam Quarantine(**외부 스팸 격리 활성화**)**을 선택합니다.

단계 **4** Name(이름) 필드에 Security Management Appliance의 이름을 입력합니다.

이 이름은 중요하지 않으며 참조용으로만 사용됩니다. 예를 들어 Security Management Appliance의 호스트 이름을 입력합니다.

단계 **5** IP 주소 및 포트 번호를 입력합니다.

입력한 내용은 Spam Quarantines Settings(스팸 격리 설정) 페이지(**Management Appliance(**관리 어플라이언스**) > Centralized Services(**중앙 집중식 서비스**) > Spam Quarantine(**스팸 격리**)**)에서 Security Management Appliance에 대해 지정한 IP 주소 및 포트 번호와 일치해야 합니다.

단계 **6** (선택 사항) **External Safelist/Blocklist(**외부 허용 목록/차단 목록**)** 기능을 활성화하기 위한 확인란을 선택하고 해당 차단 목록 작업을 지정합니다.

단계 **7** 변경 사항을 제출 및 커밋합니다.

단계 **8** 관리할 각 Email Security Appliance에 대해 이 절차를 반복합니다.

다음에 수행할 작업

로컬 격리를 사용 중이었던 경우 로컬 스팸 격리를 비활성화하여 외부 격리 활성화 , 1191 페이지 섹션을 참조하십시오.

관련 주제

- 로컬 대 외부 스팸 격리 , 868 페이지
- 스팸 격리, 867 페이지
- Anti-Spam, 355 페이지
- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 356 페이지

로컬 스팸 격리를 비활성화하여 외부 격리 활성화

외부 스팸 격리를 활성화하기 전에 로컬 스팸 격리를 사용하고 있었다면 메시지를 외부 격리로 보내기 위해 로컬 격리를 비활성화해야 합니다.

시작하기 전에

시작하기 전에 섹션의 정보를 포함하여 외부 스팸 격리 및 외부 허용 목록/차단 목록 활성화 , 1190 페이지의 모든 지침을 수행합니다.

단계 **1** **Monitor(**모니터**) > Spam Quarantine(**스팸 격리**)**을 선택합니다.

단계 **2** Spam Quarantine(스팸 격리) 섹션에서 **Spam Quarantine(**스팸 격리**)** 링크를 클릭합니다.

단계 **3** **Enable Spam Quarantine(**스팸 격리 활성화**)**의 선택을 취소합니다.

이 변경의 결과로 메일 정책이 조정된다는 경고를 무시하십시오. 외부 격리 설정을 구성한 경우 메일 정책은 메시지를 자동으로 외부 스팸 격리로 전송합니다.

단계 **4** 변경 사항을 제출 및 커밋합니다.

외부 스팸 격리 문제 해결

외부 격리에서 릴리스된 메시지를 재처리하는 **Email Security Appliance**

문제: Security Management Appliance에서 릴리스된 메시지가 Email Security Appliance에서 불필요하게 다시 처리됩니다.

솔루션: 이 문제는 Security Management Appliance의 IP 주소가 변경되는 경우에 발생할 수 있습니다. 메일 플로우 및 외부 스팸 격리 , 1189 페이지를 참조하십시오.

정책, 바이러스 및 **Outbreak** 격리 중앙 집중화 정보

- 중앙 정책, 바이러스, 보안 침해 격리 , 1192 페이지
- 정책, 바이러스 및 Outbreak 격리의 마이그레이션 정보 , 1193 페이지

중앙 정책, 바이러스, 보안 침해 격리

Security Management Appliance에서 정책, 바이러스 및 보안 침해 격리를 중앙 집중화할 수 있습니다. 메시지는 Email Security Appliance를 통해 처리되지만 Security Management Appliance의 격리에 저장됩니다.

정책, 바이러스 및 Outbreak 격리 중앙 집중화의 이점은 다음과 같습니다.

- 관리자는 여러 Email Security Appliance에서 온 격리된 메시지를 한 장소에서 관리할 수 있습니다.
- 격리된 메시지는 DMZ 대신 방화벽 뒤에 저장되므로 보안 위험이 줄어듭니다.
- Security Management Appliance에서 표준 백업 기능을 사용하여 중앙 집중식 격리를 백업할 수 있습니다.

자세한 내용은 Security Management Appliance의 사용자 가이드 또는 온라인 도움말을 참고하십시오.

중앙 집중식 정책, 바이러스 및 **Outbreak** 격리의 제한 사항

- 각 Email Security Appliance에서 모든 정책, 바이러스 및 Outbreak 격리를 중앙 집중화하거나, 모두를 로컬에 저장해야 합니다.
- Security Management Appliance에서는 검사 엔진을 사용할 수 없으므로 정책, 바이러스 또는 Outbreak 격리에서 메시지의 바이러스를 수동으로 테스트할 수 없습니다.

클러스터 컨피그레이션에서 중앙 집중식 정책, 바이러스 및 **Outbreak** 격리의 요구 사항

클러스터링된 어플라이언스의 어떤 레벨에서든 중앙 집중식 정책, 바이러스 및 Outbreak 격리를 활성화할 수 있습니다.

요건:

- 특정 수준(시스템, 그룹 또는 클러스터)의 EmailSecurity appliance에서 중앙 집중식 정책, 바이러스 및 Outbreak 격리를 활성화하기 전에, 먼저 동일한 수준에 속한 모든 어플라이언스를 Security Management Appliance에 추가해야 합니다.
- 콘텐츠 및 메시지 필터와 DLP 메시지 작업은 동일한 레벨에서 구성해야 하며 해당 레벨 아래의 레벨에서 재정의되어서는 안 됩니다.
- 중앙 집중식 정책, 바이러스 및 Outbreak 격리 설정은 동일한 레벨에서 구성해야 하며 구성된 레벨 아래의 레벨에서 재정의되어서는 안 됩니다.
- Security Management Appliance와의 통신에 사용할 인터페이스는 그룹 또는 클러스터에 있는 모든 어플라이언스에서 이름이 동일해야 합니다.

예를 들면 다음과 같습니다.

클러스터 또는 그룹 레벨에서 중앙 집중식 정책, 바이러스 및 Outbreak 격리를 활성화하고자 하지만 클러스터에 연결된 Email Security Appliance에서는 시스템 레벨에서 이러한 설정이 정의된 경우, 시

스템 레벨에서 구성된 중앙 집중식 격리 설정을 제거해야만 클러스터 또는 그룹 레벨에서 이 기능을 활성화할 수 있습니다.

정책, 바이러스 및 Outbreak 격리의 마이그레이션 정보

정책, 바이러스 및 Outbreak 격리를 중앙 집중화하는 경우 mail Security appliance의 기존 정책, 바이러스 및 Outbreak 격리가 SecurityManagement appliance로 마이그레이션됩니다.

SecurityManagement appliance에서 마이그레이션을 구성하게 되지만, Email Security Appliance에서 중앙 집중식 정책, 바이러스 및 Outbreak 격리를 활성화하는 변경 사항을 커밋할 때 마이그레이션이 발생합니다.

변경 사항을 커밋하자마자 다음이 발생합니다.

- Email Security Appliance의 로컬 정책, 바이러스 및 Outbreak 격리가 비활성화됩니다. 이 격리로 들어가는 모든 새 메시지는 Security Management Appliance에서 격리됩니다.
- Security Management Appliance에 대한 기존의 비 스팸 격리 마이그레이션이 시작됩니다.
- 모든 로컬 정책, 바이러스 및 Outbreak 격리가 삭제됩니다. 사용자 지정 마이그레이션을 구성한 경우 마이그레이션하지 않도록 선택한 로컬 정책 격리도 삭제됩니다. 정책 격리 삭제의 효과는 정책 격리 삭제 정보 , 854 페이지 섹션을 참조하십시오.
- 마이그레이션 전에 여러 격리에 있던 메시지는 마이그레이션 후 해당 중앙 집중식 격리로 이동됩니다.
- 마이그레이션은 백그라운드에서 수행됩니다. 소요되는 시간은 격리의 크기 및 네트워크에 따라 달라집니다. Email Security Appliance에서 중앙 집중식 격리를 활성화할 때 마이그레이션 완료 시 알림을 수신할 이메일 주소를 하나 이상 입력할 수 있습니다.
- 원래 로컬 격리의 설정이 아니라 중앙 집중식 격리의 설정이 메시지에 적용됩니다. 그러나 각 메시지에는 원래 만료 시간이 적용됩니다.

참고 마이그레이션 중에 자동으로 생성되는 모든 중앙 집중식 격리에는 기본 격리 설정이 있습니다.

정책, 바이러스 및 Outbreak 격리 중앙 집중화

시작하기 전에

참고 이 절차는 유지 관리 기간 중에 또는 바쁘지 않은 시간에 수행하십시오.

- 먼저 정책, 바이러스 및 신종 바이러스 격리를 중앙 집중화하도록 Security Management Appliance를 구성해야 합니다. Security Management Appliance에 대한 온라인 도움말 또는 사용 설명서에서 "중앙 집중식 정책, 바이러스 및 Outbreak 격리" 장의 "정책, 바이러스 및 Outbreak 중앙 집중화" 섹션에 있는 표를 참고하십시오.

- Security Management Appliance에서 중앙 집중식 격리에 할당된 공간이 기존 로컬 격리가 전체적으로 차지하던 공간보다 작으면 Security Management Appliance의 격리 설정을 기반으로 메시지가 조기에 만료됩니다. 마이그레이션 전에 수동으로 격리 크기를 줄이는 것을 고려해보십시오. 조기 만료에 대한 자세한 내용은 자동으로 처리되는 격리 메시지에 대한 기본 작업 , 851 페이지 섹션을 참조하십시오.
- 자동 마이그레이션을 선택했거나 마이그레이션하는 동안 중앙 집중식 격리를 만들도록 맞춤형 마이그레이션을 구성한 경우 Email Security Appliance의 현재 격리 설정을 적어두었다가 중앙 집중식 격리를 구성하기 위한 지침으로 사용할 수 있습니다.
- Email Security Appliance를 클러스터 구성에 구축하는 경우 클러스터 컨피그레이션에서 중앙 집중식 정책, 바이러스 및 Outbreak 격리의 요구 사항 , 1192 페이지 항목을 참고하십시오.
- 이 절차에서 변경 사항을 커밋하자마자 어떤 내용이 변경되는지 숙지합니다. 정책, 바이러스 및 Outbreak 격리의 마이그레이션 정보 , 1193 페이지를 참조하십시오.

단계 **1** **Security Services(**보안 서비스**) > Centralized Services(**중앙 집중식 서비스**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 **Outbreak** 격리**)**를 선택합니다.

단계 **2** **Enable(**활성화**)**을 클릭합니다.

단계 **3** SecurityManagement appliance와의 통신에 사용할 인터페이스 및 포트를 입력합니다.

SecurityManagement appliance에서 인터페이스와 포트에 도달할 수 있는지 확인하십시오.

Email Security Appliance가 클러스터링된 경우 선택하는 인터페이스는 클러스터의 모든 시스템에서 사용 가능해야 합니다.

단계 **4** 마이그레이션이 완료될 때 알림을 수신하려면 하나 이상의 이메일 주소를 입력합니다.

단계 **5** 마이그레이션할 격리에 대한 정보가 올바른지 확인합니다.

단계 **6** 사용자 지정 마이그레이션을 완료하는 경우 이 절차에서 변경 사항을 커밋할 때 삭제될 격리를 확인합니다.

단계 **7** 업데이트할 콘텐츠 및 메시지 필터와 DLP 메시지 작업에 대한 정보가 올바른지 확인합니다.

참고 클러스터 컨피그레이션에서 필터 및 메시지 작업은 필터 및 메시지 작업이 특정 레벨에서 정의되고 그 아래의 레벨에서 재정의되지 않는 경우에만 해당 레벨에서 자동으로 업데이트할 수 있습니다. 마이그레이션 후 중앙 집중식 격리 이름으로 필터 및 메시지 작업을 수동으로 재구성해야 할 수 있습니다.

단계 **8** 마이그레이션 매핑을 재구성해야 하는 경우

a) Security Management Appliance로 돌아갑니다.

b) 마이그레이션 매핑을 재구성합니다.

관리 어플라이언스에서 리맵할 격리를 선택한 다음 **Remove from Centralized Quarantine(**중앙 집중식 격리에서 제거**)**을 클릭합니다. 그런 다음 격리를 리맵할 수 있습니다.

c) Security Management Appliance에서 새 마이그레이션 구성을 커밋합니다.

d) 처음부터 이 절차를 시작합니다.

중요**! Security Services(**보안 서비스**) > Centralized Services(**중앙 집중식 서비스**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 **Outbreak** 격리**)** 페이지를 다시 로드해야 합니다.

단계 **9** **Submit(**제출**)**를 클릭합니다.

단계 **10** 마이그레이션 매핑을 재구성해야 하는 경우 8단계의 절차를 수행합니다.

단계 **11** 변경 사항을 커밋합니다.

참고 마이그레이션이 진행 중인 동안에는 Email Security Appliance 또는 Security Management Appliance에서 구성을 변경하지 마십시오.

단계 **12** 페이지 상단에서 마이그레이션 상태를 모니터링합니다. 또는 마이그레이션을 구성할 때 이메일 주소를 입력한 경우 마이그레이션이 완료되었음을 알리는 이메일을 기다립니다.

다음에 수행할 작업

Security Management Appliance에 대한 온라인 도움말 또는 사용 설명서에서 "정책, 바이러스 및 Outbreak 격리 중앙 집중화" 항목의 테이블에 설명된 나머지 작업을 수행합니다.

관련 주제

• 정책, 바이러스 및 보안 침해 격리에 액세스할 수 있는 사용자 그룹 , 857 페이지

중앙 집중식 정책, 바이러스 및 Outbreak 격리 비활성화 정보

Email Security Appliance에서 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리를 비활성화할 경우:

- Email Security Appliance에서 로컬 격리가 작동으로 활성화됩니다.
- 시스템 생성 격리 및 메시지 필터, 콘텐츠 필터, DLP 메시지 작업에서 참조되는 격리가 Email Security Appliance에 자동으로 생성됩니다. 중앙 집중화되기 전과 동일한 설정(할당된 사용자 역할 포함)으로 Virus(바이러스), Outbreak(보안 침해) 및 Unclassified(미분류) 격리가 생성됩니다. 다른 모든 격리는 기본 설정으로 생성됩니다.
- 새로 격리된 메시지는 로컬 격리로 직접 이동합니다.
- 비활성화되는 시점에 중앙 집중식 격리에 있던 메시지는 다음 중 하나가 발생할 때까지 계속 그 자리에 보관됩니다.
  - 메시지가 만료될 때 수동으로 또는 자동으로 삭제됩니다.
  - 다음 중 하나가 true일 때 메시지가 수동으로 또는 자동으로 릴리스됩니다.

* Security Management Appliance에 대체 릴리스 어플라이언스가 구성됩니다. Security Management Appliance에 대한 온라인 도움말 또는 설명서를 참고하십시오.

* Email Security Appliance에서 중앙 집중식 격리가 다시 활성화됩니다.

중앙 집중식 정책, 바이러스 및 Outbreak 격리 비활성화

시작하기 전에

- 중앙 집중식 정책, 바이러스 및 Outbreak 격리 비활성화의 영향을 이해합니다.
- 다음 중 하나를 수행합니다.
  - 현재 중앙 집중식 정책, 바이러스 및 Outbreak 격리에 있는 모든 메시지를 처리합니다.

- 비활성화 후 중앙 집중식 격리에서 릴리스되는 메시지를 처리하기 위한 대체 릴리스 어플라이언스를 지정했는지 확인합니다. 자세한 내용은 Security Management Appliance의 온라인 도움말 또는 사용자 가이드를 참고하십시오.

단계 **1** Email Security Appliance에서 **Security Services(**보안 서비스**) > Centralized Services(**중앙 집중식 서비스**) > Policy, Virus, and Outbreak Quarantines(**정책**,** 바이러스 및 **Outbreak** 격리**)**를 선택합니다.

단계 **2** 중앙 집중식 정책, 바이러스 및 Outbreak 격리를 비활성화합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

단계 **4** 새로 생성된 로컬 격리의 설정을 사용자 지정합니다.

중앙 집중식 정책, 바이러스 및 **Outbreak** 격리 문제 해결

Cisco Content Security Management Appliance 서비스가 중단되는 경우

정책, 바이러스 및 Outbreak 격리가 서비스 중단된 Security Management Appliance에서 중앙 집중화된 경우 Email Security Appliance에서 이러한 중앙 집중식 격리를 비활성화해야 합니다.

대체 보안 관리 어플라이언스를 구축하는 경우에는 Security Management Appliance 및 각 Email Security Appliance에서 격리 마이그레이션을 재구성해야 합니다. Security Management Appliance에 대한 온라인 도움말 또는 사용 설명서에서 "중앙 집중식 정책, 바이러스 및 Outbreak 격리" 장의 "정책, 바이러스 및 Outbreak 중앙 집중화" 섹션에 있는 표를 참고하십시오.

중앙 집중식 보고 구성

시작하기 전에

- Security Management Appliance에서 중앙 집중식 보고를 활성화하고 구성합니다. Cisco Content Security Management Appliance 사용자 가이드에서 사전 요구 사항 및 지침을 참고하십시오.
- Security Management Appliance에서 보고 서비스에 충분한 디스크 공간이 할당되었는지 확인합니다.

단계 **1** **Security Services(**보안 서비스**) > Reporting(**보고**)**을 클릭합니다.

단계 **2** Reporting Service(보고 서비스) 섹션에서 Centralized Reporting(중앙 집중식 보고) 옵션을 선택합니다.

단계 **3** 변경 사항을 제출 및 커밋합니다.

Advanced Malware Protection 보고 요구 사항

Security Management Appliance에서 Advanced Malware Protection(파일 평판 및 파일 분석) 기능에 대한 완전한 보고를 위한 필수 구성은 사용 중인 Security Management Appliance 소프트웨어 버전에 대

한 온라인 도움말 또는 사용 설명서에 있는 이메일 보고 장에서 Advanced Malware Protection 보고서에 대한 정보를 참고하십시오.

중앙 집중식 보고에 대한 변경 후 보고 정보 가용성

Email Security Appliance에서 중앙 집중식 보고가 활성화된 경우:

- 월간 보고서에 대한 Email Security Appliance의 기존 데이터는 Security Management Appliance로 전송되지 않습니다.
- Email Security Appliance의 아카이브된 보고서는 사용할 수 없습니다.
- Email Security Appliance는 일주일 분량의 데이터만 저장합니다.
- 월간 및 연간 보고서의 새 데이터가 Security Management Appliance에 저장됩니다.
- Email Security Appliance의 예약된 보고서는 일시 중단됩니다.
- Email Security Appliance의 예약된 보고서 구성 페이지에 더 이상 액세스할 수 없습니다.

중앙 집중식 보고 비활성화 정보

Email Security Appliance에서 중앙 집중식 보고를 비활성화하면 Email Security Appliance는 새로운 월 보고서 데이터를 저장하기 시작하고, 예약된 보고서가 다시 시작되며, 사용자는 보관된 보고서에 액세스할 수 있습니다. 중앙 집중식 보고를 비활성화하면 어플라이언스는 지나간 시간 및 일 단위 데이터만 표시하고 지나간 주 또는 월 단위 데이터는 표시하지 않습니다. 이는 일시적입니다. 충분한 데이터가 축적되면 지나간 주 및 월에 대한 보고서가 표시됩니다. Email Security Appliance를 중앙 집중식 보고 모드로 전환하면 인터랙티브 보고서에 지나간 주에 대한 데이터가 표시됩니다.

중앙 집중식 메시지 추적 구성

시작하기 전에

참고 Email Security Appliance에서 중앙 집중식 추적과 로컬 추적을 모두 활성화할 수는 없습니다.

단계 **1** **Security Services(**보안 서비스**) > Message Tracking(**메시지 추적**)**을 클릭합니다.

단계 **2** Message Tracking Service(메시지 추적 서비스) 섹션에서 **Edit Settings(**설정 수정**)**를 클릭합니다.

단계 **3** **Enable Message Tracking Service(**메시지 추적 서비스 활성화**)** 확인란을 선택합니다.

단계 **4** Centralized Tracking(중앙 집중식 추적) 옵션을 선택합니다.

단계 **5** (선택 사항) 거부된 연결에 대한 정보를 저장하기 위한 확인란을 선택합니다.

참고 거부된 연결에 대한 추적 정보를 저장하면 Security Management Appliance의 성능이 저하될 수 있습니다.

단계 **6** 변경 사항을 제출 및 커밋합니다.

향후 작업

중앙 집중식 추적을 사용하려면 Email Security Appliance 및 Security Management Appliance에서 이 기능을 활성화해야 합니다. Security Management Appliance에서 중앙 집중식 추적을 활성화하려면 Cisco Content Security Management Appliance 사용자 가이드를 참고하십시오.

중앙 집중식 서비스 사용

중앙 집중식 서비스 사용에 대한 지침은 Cisco Content Security Management Appliance 사용자 가이드를 참고하십시오.

A 부록

FTP, SSH 및 SCP 액세스

이 부록에는 다음 섹션이 포함되어 있습니다.

IP 인터페이스

IP 인터페이스에는 네트워크에 개별적으로 연결하는 데 필요한 네트워크 구성 데이터가 포함되어 있습니다. 하나의 물리적 이더넷 인터페이스에 대해 여러 IP 인터페이스를 구성할 수 있습니다. IP 인터페이스에 IPv4(Internet Protocol version 4), IPv6(version 6) 또는 둘 모두를 할당할 수 있습니다.

표 ***154:*** 인터페이스에서 기본적으로 활성화되는 서비스

		기본적으로 활성화되는지 여부	
서비스	기본 포트	Management interface[2]	새로 만드는 인터페이스
FTP	21	아니요	아니요
SSH	22	예	아니요
HTTP	80	예	아니요
HTTPS	443	예	아니요

[2] 여기에 표시된 "Management Interface" 설정은 C170어플라이언스에서 Data 1 Interface에 대한 기본 설정이기도 합니다.

- GUI(graphical user interface)를 통해 어플라이언스에 액세스해야 하는 경우 인터페이스에서 HTTP 및/또는 HTTPS를 활성화해야 합니다.
- 컨피그레이션 파일을 업로드 또는 다운로드하기 위해 어플라이언스에 액세스해야 하는 경우 인터페이스에서 FTP를 활성화해야 합니다.

• scp(secure copy)를 사용하여 파일을 업로드 또는 다운로드할 수도 있습니다.

IP 인터페이스를 통해 스팸 격리에 대한 HTTP 또는 HTTPS 액세스를 구성할 수 있습니다.

이메일 전달 및 Virtual Gateway의 경우 각 IP 인터페이스는 특정 IP 주소 및 호스트 이름과 함께 하나의 Virtual Gateway 주소로 작동합니다. 또한 여러 인터페이스를 별개의 그룹으로 "결합"할 수 있으며(CLI를 통해), 이 경우 시스템은 이메일 전달 시 이러한 그룹을 순환합니다.

Virtual Gateway의 결합 또는 그룹화는 여러 인터페이스에 걸친 대규모 이메일 캠페인의 부하 균형에 유용합니다. 또한 VLAN을 만들고 다른 인터페이스처럼 구성할 수 있습니다(CLI를 통해). 자세한 내용은 고급 네트워크 컨피그레이션, 1039 페이지을 참조해 주십시오.

관련 주제

• AsyncOS에서 기본 IP 인터페이스를 선택하는 방법, 1200 페이지

AsyncOS에서 기본 IP 인터페이스를 선택하는 방법

AsyncOS는 **Network(네트워크) > IP Interfaces(IP 인터페이스)** 페이지에 또는 `ifconfig` CLI 명령으로 나타나는 IP 인터페이스의 최하위 IP 주소를 기준으로 기본 IP 인터페이스를 선택합니다. 문제의 서브넷에 상주하는 리스트의 첫 번째 IP 인터페이스가 사용됩니다.

동일한 서브넷 내에 기본 게이트웨이로서 여러 IP 주소가 구성되어 있으면 가장 낮은 번호의 IP 주소가 사용됩니다. 예를 들어 동일한 서브넷 내에 다음과 같은 IP 주소가 구성되어 있으면

• `10.10.10.2/24`
• `10.10.10.30/24`
• `10.10.10.100/24`
• `10.10.10.105/24`

AsyncOS는 기본 IP 인터페이스로 `10.10.10.2/24`를 선택합니다.

Email Security Appliance에 대한 FTP 액세스 구성

단계 **1** **Network(네트워크) > IP Interfaces(IP 인터페이스)** 페이지 또는 `interfaceconfig` 명령을 사용하여 인터페이스에 대한 FTP 액세스를 활성화합니다.

위험 `interfaceconfig` 명령을 통해 서비스를 비활성화하면, 어플라이언스에 연결되어 있는 방식에 따라 CLI에서 연결을 끊을 수 있습니다. 또 다른 프로토콜, Serial 인터페이스 또는 Management 포트의 기본 설정을 사용하여 어플라이언스에 다시 연결할 수 있는 경우가 아니면 이 명령으로 서비스를 비활성화하지 마십시오.

단계 **2** 변경 사항을 제출 및 커밋합니다.

단계 **3** FTP를 통해 인터페이스에 액세스합니다. 인터페이스에 대한 IP 주소가 올바른지 확인하십시오. 예를 들면 다음과 같습니다.

```
$ ftp 192.168.42.42
```

참고 또한 많은 브라우저에서도 FTP를 통한 인터페이스 액세스를 허용합니다.

단계 **4** 수행하려는 특정 작업에 대한 디렉터리로 이동합니다. FTP를 통해 인터페이스에 액세스한 경우 다음 디렉터리로 이동하여 파일을 복사 및 추가("GET" 및 PUT")할 수 있습니다. 다음 표를 참조하십시오.

디렉터리 이름	설명
/configuration	다음 명령을 통해 데이터를 내보내거나 가져올 수 있는 디렉터리: • 가상 게이트웨이 매핑(`altsrchost`) • XML 형식의 구성 데이터(`Saveconfig, loadconfig`) • HAT(Host Access Table)(`hostaccess`) • RAT(Recipient Access Table)(`rcptaccess`) • SMTP 경로 항목(`smtproutes`) • 별칭 테이블(`aliasconfig`) • 가장 테이블(`masquerade`) • 메시지 필터(`filters`) • 전역 수신 거부 데이터(`unsubscribe`) • `trace` 명령에 대한 테스트 메시지 • *slbl<timestamp><serial number>.csv* 형식으로 저장된 허용 리스트/차단 리스트 백업 파일
/antivirus	안티바이러스 엔진 로그 파일이 보관된 디렉터리 이 디렉터리의 로그 파일을 검사하여 성공적으로 다운로드한 최신 바이러스 정의 파일(`scan.dat`)을 수동으로 확인할 수 있습니다.

디렉터리 이름	설명
/configuration /system_logs /cli_logs /status /reportd_logs reportqueryd_logs /ftpd_logs /mail_logs /asarchive /bounces /error_logs /avarchive /gui_logs /sntpd_logs /RAID.output /euq_logs /scanning /antispam /antivirus /euqgui_logs /ipmitool.output	`logconfig` 및 `rollovernow` 명령을 통해 자동으로 생성된 로깅. 각 로그에 대한 자세한 설명은 로깅, 1053 페이지을 참조해 주십시오. 각 로그 파일 형식 간 차이점은 "로그 파일 유형 비교"를 참조해 주십시오.

단계 **5** 해당 디렉터리에서 파일을 업로드 및 다운로드하려면 FTP 프로그램을 사용해 주십시오.

scp(Secure Copy) 액세스

클라이언트 운영 체제에서 `scp`(secure copy) 명령을 지원하는 경우 이전 표에 나열된 디렉터리에서/디렉터리로 파일을 복사할 수 있습니다. 예를 들면 다음 예에서 `/tmp/test.txt` 파일은 클라이언트 시스템에서 호스트 이름이 `mail3.example.com`인 어플라이언스의 구성 디렉터리로 복사됩니다.

이 명령을 실행하면 사용자(admin)의 암호를 입력하라는 메시지가 표시됩니다. 다음 예는 참조용입니다. scp(secure copy) 구현은 운영 체제에 따라 다를 수 있습니다.

```
% scp /tmp/test.txt admin@mail3.example.com:configuration

The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.
```

```
DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.

Are you sure you want to continue connecting (yes/no)? yes


Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.

admin@mail3.example.com's passphrase: (type the passphrase)

test.txt 100% |*****************************| 1007 00:00

%
```

다음 예에서는 동일한 파일이 어플라이언스에서 클라이언트 시스템으로 복사됩니다.

```
% scp admin@mail3.example.com:configuration/text.txt .

admin@mail3.example.com's passphrase: (type the passphrase)

test.txt 100% |*****************************| 1007 00:00

%
```

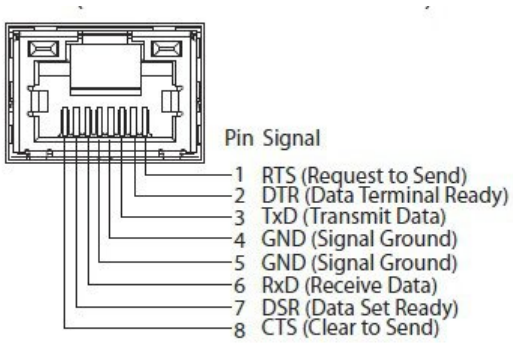
Cisco 어플라이언스와 파일을 주고받기 위해 FTP 대신 `scp`(secure copy)를 사용할 수 있습니다.

참고 Operators 및 Administrators 그룹의 사용자만이 secure copy(`scp`)를 사용하여 어플라이언스에 액세스할 수 있습니다. 자세한 내용은 사용자 추가 , 897 페이지를 참고하십시오.

시리얼 연결을 통해 이메일 보안 어플라이언스 액세스

시리얼 연결을 통해 어플라이언스에 연결하는 경우 콘솔 포트에 대해 다음 정보를 사용하십시오. 이 포트에 대한 자세한 정보는 사용 중인 어플라이언스의 하드웨어 설치 가이드에 나와 있습니다.

80-Series 및 90-Series 하드웨어에서 시리얼 포트에 대한 핀아웃 세부사항



70-Series 하드웨어에서 시리얼 포트에 대한 핀아웃 세부사항

다음 그림에서는 시리얼 포트 커넥터에 대한 핀 번호를 보여주고, 다음 표에서는 시리얼 포트 커넥터에 대한 핀 할당 및 인터페이스 신호를 정의합니다.

그림 ***88:*** 시리얼 포트에 대한 핀아웃 번호

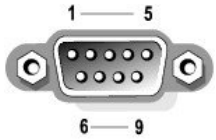


표 ***155:*** 시리얼 포트 핀 할당

PIN	신호	**I/O**	정의
1	DCD		Data carrier detect
2	SIN		Serial input
3	SOUT		Serial output
4	DTR		데이터 터미널 대기
5	GND	해당 없음	Signal ground
6	DSR		데이터 세트 대기
7	RTS		전송 요청
8	CTS		전송 제거
9	RI		Ring indicator
Shell	해당 없음	해당 없음	섀시 접지

B 부록

네트워크 및 IP 주소 할당

이 부록에는 다음 섹션이 포함되어 있습니다.

이더넷 인터페이스

Cisco CSA(Content Security Appliance)는 구성(선택 사항인 광 네트워크 인터페이스 유무)에 따라 시스템의 후면 패널에 최대 4개의 이더넷 인터페이스가 장착되어 있습니다. 다음과 같은 레이블이 지정됩니다.

- Management
- Data1
- Data2
- Data3
- Data4

IP 주소 및 넷마스크 선택

네트워크를 구성할 때 CSA는 발신 패킷을 전송할 고유 인터페이스를 선택할 수 있어야 합니다. 이 요구 사항에 따라 이더넷 인터페이스의 IP 주소 및 넷마스크 선택에서 몇 가지가 결정됩니다. 하나의 네트워크(인터페이스의 IP 주소에 넷마스크를 적용하여 결정됨)에는 하나의 인터페이스만 있다는 것이 규칙입니다.

IP 주소는 지정된 네트워크에서 물리적 인터페이스를 식별합니다. 물리적 이더넷 인터페이스는 패킷을 수신하는 IP 주소를 여러 개 가질 수 있습니다. IP 주소가 여러 개 있는 이더넷 인터페이스는 패킷의 소스 주소와 같은 IP 주소를 사용하는 인터페이스를 통해 패킷을 전송할 수 있습니다. 이러한 특성은 가상 게이트웨이 기술을 구현하는 데 사용됩니다.

넷마스크의 목적은 IP 주소를 네트워크 주소와 호스트 주소로 구분하는 것입니다. 네트워크 주소는 IP 주소의 네트워크 파트(넷마스크와 일치하는 비트)로 간주될 수 있습니다. 호스트 주소는 IP 주소의

나머지 비트입니다. 중요한 네 개 옥텟 주소의 비트 수는 때때로 CIDR(Classless Inter-Domain Routing) 스타일로 표현됩니다. 이는 비트 수(1-32) 뒤의 슬래시입니다.

이러한 수를 이진으로 계산하여 넷마스크를 표현할 수 있습니다. 따라서 255.255.255.0은 "/24"가 되고 255.255.240.0은 "/20"이 됩니다. ”

인터페이스 구성 샘플

이 섹션에서는 일부 일반 네트워크를 기반으로 한 샘플 인터페이스 구성을 보여줍니다. 다음 예에는 Int1 및 Int2라는 두 인터페이스가 사용됩니다. CSA의 경우 이 인터페이스 이름은 3개의 인터페이스(Management, Data1, Data2) 중 2개를 나타낼 수 있습니다.

Network 1:

각 인터페이스는 별도의 네트워크에 있는 것으로 표시되어야 합니다.

인터페이스	**IP** 주소	**Netmask**	네트워크주소
Int1	192.168.1.10	255.255.255.0	192.168.1.0/24
Int2	192.168.0.10	255.255.255.0	192.168.0.0/24

주소가 192.168.1.X(여기서 X는 1-255의 숫자, 자체 주소 제외, 이 경우 10)로 지정된 데이터는 Int1을 이용합니다. 주소가 192.168.0.X로 지정된 데이터는 Int2를 이용합니다. 이러한 형식이 아닌 다른 주소로 지정된 패킷(대부분 WAN이나 인터넷)은 이러한 네트워크 중 하나에 있는 기본 게이트웨이로 전송됩니다. 그러면 기본 게이트웨이는 해당 패킷을 전달합니다.

Network 2:

다른 두 인터페이스의 네트워크 주소(IP 주소의 네트워크 부분)는 동일할 수 없습니다.

이더넷인터페이스	**IP** 주소	**Netmask**	네트워크주소
Int1	192.168.1.10	255.255.0.0	192.168.0.0/16
Int2	192.168.0.10	255.255.0.0	192.168.0.0/16

이 상황은 두 가지 다른 이더넷 인터페이스의 네트워크 주소가 동일하여 충돌이 발생한 경우입니다. CSA의 패킷이 192.168.1.11로 전송되면 패킷을 전달하기 위해 어떤 이더넷 인터페이스를 사용해야 할지를 결정할 방법이 없습니다. 두 이더넷 인터페이스가 서로 다른 두 물리적 네트워크에 연결되어 있는 경우 해당 패킷은 잘못된 네트워크로 전달되어 목적지를 찾지 못할 수 있습니다. CSA에서는 충돌이 발생하도록 네트워크를 구성할 수 없습니다.

두 이더넷 인터페이스를 동일한 물리적 네트워크에 연결할 수 있지만, CSA가 고유한 전달 인터페이스를 선택할 수 있도록 IP 주소와 넷마스크를 구성해야 합니다.

IP 주소, 인터페이스 및 라우팅

GUI 또는 CLI에서 인터페이스를 선택하도록 허용하는 명령이나 기능(예: AsyncOS 업그레이드 또는 DNS 구성 등)을 수행하기 위해 인터페이스를 선택할 때 선택에 앞서 라우팅(기본 게이트웨이)이 발생합니다.

예를 들어 각각 서로 다른 네트워크 세그먼트에 3개의 네트워크 인터페이스가 구성된 CSA가 있다고 가정해보겠습니다(모두 /24로 가정).

이더넷	IP
Management	192.19.0.100
Data1	192.19.1.100
Data2	192.19.2.100

기본 게이트웨이는 192.19.0.1입니다.

이제 AsyncOS 업그레이드(또는 인터페이스 선택을 허용하는 다른 명령이나 기능)를 수행하면서 Data1(192.19.1.100)에 있는 IP를 선택하면, 모든 TCP 트래픽이 Data1 이더넷 인터페이스에서 발생할 것이라고 예상할 수 있습니다. 그러나 트래픽은 기본 게이트웨이로 설정된 인터페이스(이 경우 Management)에서 나가지만, Data1에서 IP의 소스 주소로 스탬프 처리됩니다.

요약

CSA는 패킷이 전달되는 고유한 인터페이스를 항상 식별할 수 있어야 합니다. 이 결정을 내리기 위해 CSA는 패킷의 목적지 IP 주소, 이더넷 인터페이스의 네트워크와 IP 주소 설정을 함께 사용합니다. 다음 표에는 위의 예가 요약되어 있습니다.

	동일한 네트워크	다른 네트워크
동일한 물리적 인터페이스	허용됨	허용됨
다른 물리적 인터페이스	허용되지 않음	허용됨

CSA 연결을 위한 전략

어플라이언스를 연결할 때 다음 사항을 염두에 두어야 합니다.

- 관리 트래픽(CLI, 웹 인터페이스, 로그 전달)은 이메일 트래픽에 비해 일반적으로 규모가 작습니다.
- 이더넷 인터페이스가 동일한 네트워크 스위치에 연결되어 있지만 또 다른 호스트 다운스트림의 단일 인터페이스로 끝나는 경우 또는 모든 데이터가 모든 포트로 에코되는 네트워크 허브에 연결된 경우 두 인터페이스 사용에 따른 이점이 없습니다.

네트워크 및 IP 주소 할당

- 1000Base-T에서 작동하는 인터페이스를 통한 SMTP 대화는 100Base-T에서 작동하는 동일한 인터페이스를 통한 대화보다 약간 빠르지만, 이상적인 조건에서 그렇습니다.
- 전달 네트워크의 다른 부분에 병목이 있으면 네트워크에 대한 연결 최적화가 도움이 되지 않습니다. 병목은 인터넷 연결에서, 더 나아가 연결 공급업체에서 가장 자주 발생합니다.

연결하기 위해 선택하는 인터페이스의 수 및 이를 확인하는 방법은 기반 네트워크의 복잡성에 의해 결정됩니다. 네트워크 토폴로지 또는 데이터 볼륨에서 요구하지 않는 경우 여러 인터페이스에 연결할 필요가 없습니다. 게이트웨이에 친숙해질 때까지 우선 연결을 간단하게 유지한 다음, 볼륨 및 네트워크 토폴로지에서 요구할 때 연결을 확장할 수도 있습니다.

C 부록

메일 정책 및 콘텐츠 필터의 예

이 부록에는 다음 섹션이 포함되어 있습니다.

수신 메일 정책 개요

이 장의 예는 다음과 같은 작업을 설명하면서 메일 정책의 기능을 보여줍니다.

1. 기본 수신 메일 정책에 대한 안티스팸, 안티바이러스, 보안 침해 필터 및 콘텐츠 필터를 수정합니다.
2. 두 개의 서로 다른 사용자 집합(영업 조직 및 엔지니어링 조직)에 대해 새로운 정책을 2개 추가하고, 각각에 대해 서로 다른 이메일 보안 설정을 구성합니다.
3. 수신 메일 개요 정책 테이블에 사용할 새 콘텐츠 필터 3개를 만듭니다.
4. 일부 그룹에 대해서는 콘텐츠 필터를 활성화하고 나머지에 대해서는 활성화하지 않도록 정책을 다시 수정합니다.

이 예는 메일 정책에 대한 안티스팸, 안티바이러스, 보안 침해 필터 및 콘텐츠 필터의 서로 다른 수신자 기반 설정을 관리할 수 있는 강력한 기능과 유연성을 보여주기 위한 것입니다. 이 예에서는 메일 정책 및 콘텐츠 필터 액세스 권한이 있는 "Policy Administrator(정책 관리자)"라는 사용자 지정 사용자 역할에 이러한 기능을 할당합니다. 안티스팸, 안티바이러스, 보안 침해 필터 및 위임된 관리의 작동 방식에 대한 자세한 내용은 다음을 참고하십시오.

- Anti-Spam, 355 페이지
- Anti-Virus, 335 페이지
- 신종 바이러스 필터(Outbreak Filter), 399 페이지
- 관리 작업 배포, 893 페이지

메일 정책 액세스

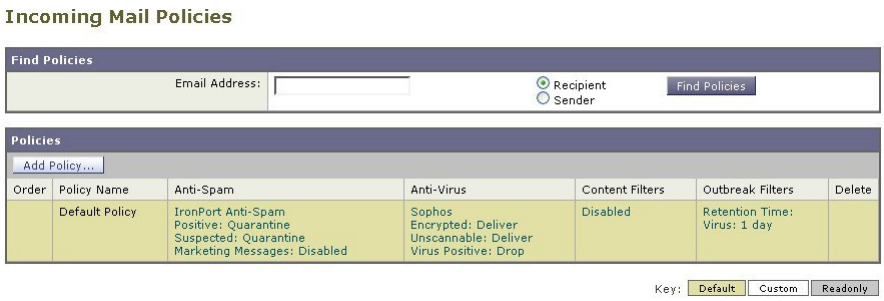
Mail Policies(메일 정책) 메뉴를 사용하여 수신 및 발신 메일 정책에 액세스할 수 있습니다.

새로운 시스템에서 시스템 설정 마법사의 모든 단계를 완료하고 Anti-Spam, Sophos 또는 McAfee Anti-Virus, Outbreak Filters(보안 침해 필터)를 활성화하도록 선택하면 Incoming Mail Policies(수신 메일 정책) 페이지는 다음 그림과 같이 보입니다.

기본적으로 이러한 설정은 기본 수신 메일 정책에 대해 활성화됩니다.

- 안티스팸(스팸 격리가 활성화된 경우): 활성화됨
  - 양성으로 식별된 스팸: 격리, 메시지 제목 앞에 추가
  - 의심스런 스팸: 격리, 메시지 제목 앞에 추가
  - 마케팅 이메일: 검사가 활성화되지 않음
- 안티스팸(스팸 격리가 활성화되지 않은 경우): 활성화됨
  - 양성으로 식별된 스팸: 전달, 메시지 제목 앞에 추가
  - 의심스런 스팸: 전달, 메시지 제목 앞에 추가
  - 마케팅 이메일: 검사가 활성화되지 않음
- 안티바이러스: 활성화됨, 바이러스 검사 및 복구, 안티바이러스 검사 결과와 함께 X-header 포함
  - 복구된 메시지: 전달, 메시지 제목 앞에 추가
  - 암호화된 메시지: 전달, 메시지 제목 앞에 추가
  - 검사할 수 없는 메시지: 전달, 메시지 제목 앞에 추가
  - 바이러스에 감염된 메시지: 삭제
- 보안 침해: 활성화됨
  - 어떤 파일 확장명도 제외되지 않음
  - 바이러스 의심 첨부 파일 메시지의 보유 시간은 1일
  - 메시지 수정이 활성화되지 않음
- 콘텐츠 필터: 비활성화

그림 ***89: Incoming Mail Policies(수신 메일 정책) 페이지: 새 어플라이언스의 기본값***



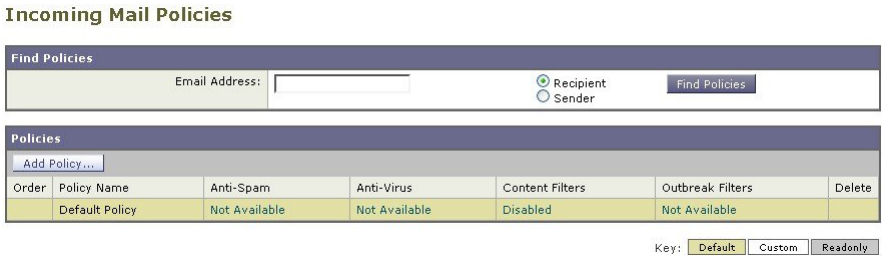
참고 이 예에서 Incoming Mail Policy(수신 메일 정책)는 스팸 격리가 활성화될 때 기본 안티스팸 설정을 사용합니다.

Enabled(활성화됨), Disabled(비활성화됨) 및 "Not Available(사용 불가)"

메일 정책 테이블의 열(수신 또는 발신)에는 각 정책 이름의 보안 서비스 상태에 대한 링크가 표시됩니다. 서비스가 활성화된 경우 "Enabled"란 단어 또는 컨피그레이션의 요약이 표시됩니다. 마찬가지로, 서비스가 비활성화된 경우 "Disabled"란 단어가 표시됩니다.

서비스에 대한 라이센스 계약에 아직 동의하지 않았거나 서비스가 만료된 경우 "Not Available"이 링크로서 표시됩니다. 이 경우 "Not Available" 링크를 클릭하면 서비스에 대해 정책 단위 설정을 구성할 수 있는 페이지가 아니라 Security Services(보안 서비스) 탭 내에 전역 페이지가 표시됩니다. 페이지가 다른 탭으로 변경되었음을 알리는 메시지가 표시됩니다. 다음 그림을 참조하십시오.

그림 ***90: Security Services Not Available***(보안 서비스 사용 불가)



수신 메시지에 대한 기본 안티스팸 정책 구성

메일 정책 테이블의 각 행은 각기 다른 정책을 나타냅니다. 각 열은 각기 다른 보안 서비스를 나타냅니다.

- 기본 정책을 수정하려면 수신 또는 발신 메일 정책 테이블의 맨 아래 행에 있는 보안 서비스의 링크 중 하나를 클릭합니다.

이 예에서는 수신 메일의 기본 정책에 대한 안티스팸 설정을 좀 더 적극적인 것으로 변경합니다. 기본값은 마케팅 이메일 검사를 비활성화한 채 양성으로 식별된 스팸 메시지 및 의심스런 스팸 메시지를 격리하는 것입니다. 이 예는 양성으로 식별된 스팸이 삭제되도록 설정을 변경하는 방법을 보여줍니다. 의심스런 스팸은 계속 격리됩니다. 마케팅 이메일 검사가 활성화되고, 마케팅 메시지는 의도된 수신자에게 전달됩니다. 마케팅 메시지 제목 앞에 [MARKETING]이란 텍스트가 추가됩니다.

단계 **1** 안티스팸 보안 서비스의 링크를 클릭합니다.

참고 기본 보안 서비스 설정의 경우, 페이지의 첫 번째 설정은 정책에 대해 서비스를 활성화할지 여부를 정의합니다. 서비스를 완전히 비활성화하려면 "Disable(비활성)"을 클릭할 수 있습니다.

단계 **2** "Positively Identified Spam Settings(양성으로 식별된 스팸 설정)" 섹션에서 "Action to apply to this message(이 메시지에 적용할 작업)"를 Drop(삭제)으로 변경합니다.

단계 **3** "Marketing Email Settings(마케팅 이메일 설정)" 섹션에서 **Yes(**예**)**를 클릭하여 마케팅 이메일 검사를 활성화합니다.

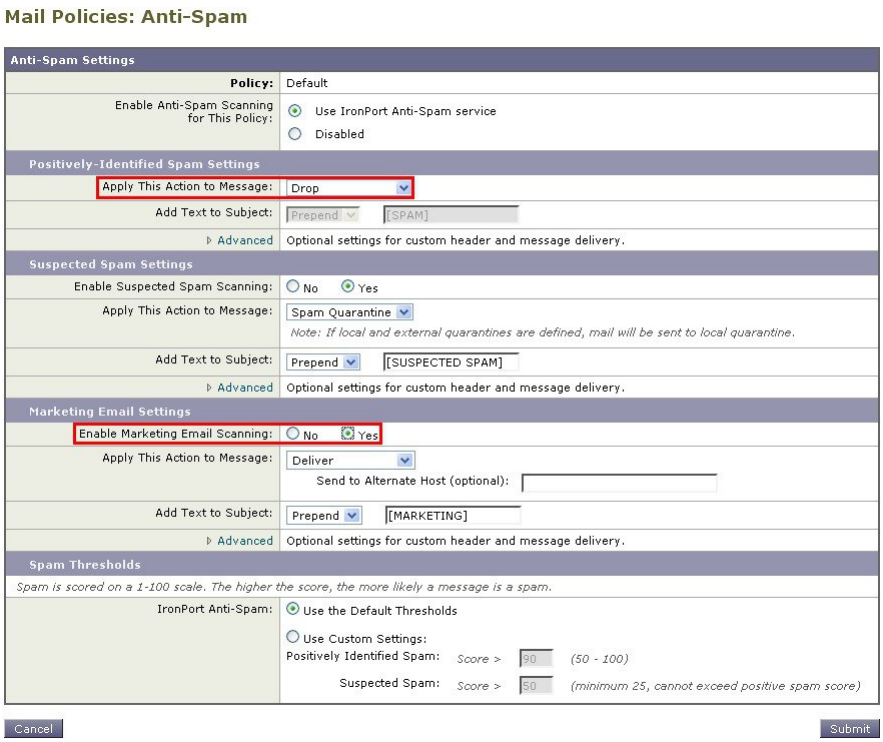
활성화할 경우 기본 작업은 제목 앞에 [MARKETING] 텍스트를 추가하고 합법적인 마케팅 메시지를 전달하는 것입니다.

"Add text to message(메시지에 텍스트 추가)" 필드는 US-ASCII 문자만 수락합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다. Incoming Mail Policies(수신 메일 정책) 테이블의 안티스팸 보안 서비스에 대한 요약 링크는 새 값을 반영하여 변경됩니다.

위의 단계와 마찬가지로, 기본 정책에 대한 기본 안티바이러스 및 바이러스 보안 침해 필터 설정을 변경할 수 있습니다.

그림 ***91: Anti-Spam Settings(***안티스팸 설정***)*** 페이지



발신자 및 수신자 그룹에 대한 메일 정책 만들기

이 부분에서는 새 정책 2개를 만듭니다. 하나는 영업 조직(LDAP 수락 쿼리로 구성원을 정의할 것임)에 대한 것이고 다른 하나는 엔지니어링 조직에 대한 것입니다. 이 역할에 속한 위임된 관리자가 정책을 관리할 수 있도록 두 정책 모두 Policy Administrator(정책 관리자) 사용자 지정 사용자 역할에 할당됩니다. 그런 다음 각각에 대해 서로 다른 이메일 보안 설정을 구성합니다.

단계 **1** **Add Policy(**정책추가**)** 버튼을 클릭하여 새 정책 만들기를 시작합니다.

단계 **2** 정책의 고유한 이름을 정의하고 순서를 조정합니다(필요할 경우).

정책 이름은 정책이 정의된 메일 정책 테이블(수신 또는 발신 모두)에서 고유해야 합니다.

적절한 테이블(수신 또는 발신)에서 하향식으로 사용자를 각 정책에 대해 평가합니다.

단계 **3** Editable by (Roles)(수정 기준(역할)) 링크를 클릭하고, 메일 정책 관리를 책임질 위임된 관리자에 대한 사용자 지정 사용자 역할을 선택합니다.

링크를 클릭하면 AsyncOS는 메일 정책에 대한 권한을 수정한 위임된 관리자에 대한 사용자 지정 역할을 표시합니다. 위임된 관리자는 정책의 안티스팸, 안티바이러스 및 보안 침해 필터 설정을 수정할 수 있으며, 정책에 대해 콘텐츠 필터를 활성화 또는 비활성화할 수 있습니다. 운영자와 관리자만 메일 정책의 이름 또는 발신자, 수신자, 그룹을

수정할 수 있습니다. 메일 정책에 대한 완전한 액세스 권한이 있는 사용자 지정 사용자 역할은 자동으로 메일 정책에 할당됩니다.

위임된 관리에 대한 자세한 내용은 관리 작업 배포, 893 페이지를 참조하십시오.

단계 **4** 정책에 대한 사용자를 정의합니다.

사용자가 발신자인지 수신자인지를 정의합니다. (자세한 내용은 정책 일치의 예, 272 페이지 섹션을 참조하십시오.) 다음 그림의 양식은 기본적으로 수신 메일 정책에는 수신자가 되고, 발신 메일 정책에는 발신자가 됩니다.

특정 정책의 사용자는 다음과 같은 방법으로 정의할 수 있습니다.

- 전체 이메일 주소: user@example.com
- 부분 이메일 주소: user@
- 도메인의 모든 사용자: @example.com
- 부분 도메인의 모든 사용자: @.example.com
- LDAP 쿼리를 확인하여

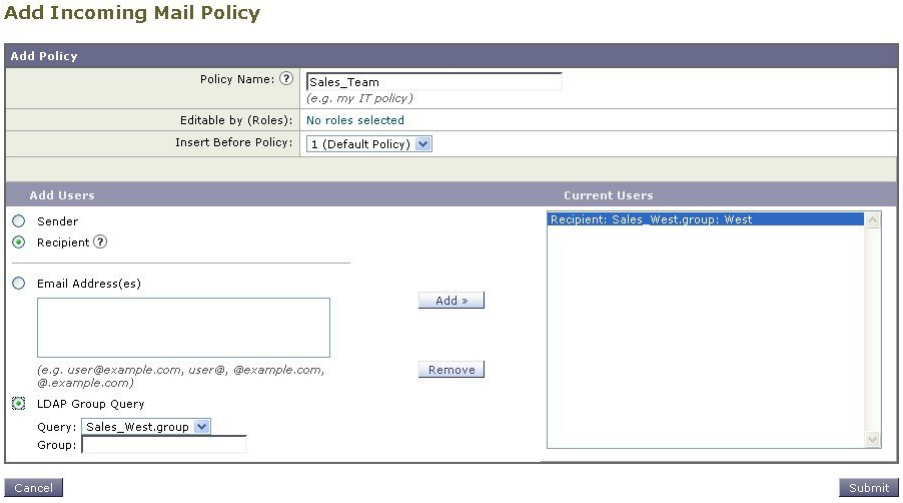
참고 사용자 항목은 AsyncOS의 GUI 및 CLI에서 모두 대/소문자를 구분합니다. 예를 들어 사용자에 수신자 Joe@를 입력하는 경우 joe@example.com으로 전송된 메시지가 일치합니다.

사용자 정보를 네트워크 인프라의 LDAP 디렉터리(예: Microsoft Active Directory, SunONE Directory Server(이전의 "iPlanet Directory Server") 또는 OpenLDAP 디렉터리) 내에 저장하는 경우 수신자 주소를 수락하고, 메시지를 대체 주소 및/또는 메일 호스트로 재라우팅하고, 헤더를 가장하고, 메시지에 특정 그룹의 수신자 또는 발신자가 있는지를 확인하도록 어플라이언스를 구성할 수 있습니다.

어플라이언스를 그렇게 구성한 경우 구성된 쿼리를 사용하여 메일 정책에 대한 사용자를 정의할 수 있습니다.

자세한 내용은 LDAP 쿼리, 735 페이지를 참조하십시오.

그림 ***92:*** 정책에 대한 사용자 정의



단계 **5** **Add(추가)** 버튼을 클릭하여 Current Users(현재 사용자) 목록에 사용자를 추가합니다.

정책에는 발신자, 수신자 및 LDAP 쿼리를 혼합하여 포함할 수 있습니다.

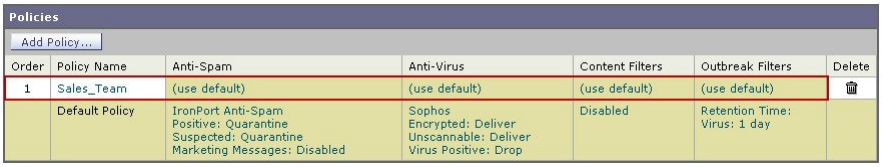
현재 사용자 목록에서 정의된 사용자를 제거하려면 **Remove(제거)** 버튼을 사용합니다.

메일 정책 및 콘텐츠 필터의 예

단계 **6** 사용자 추가를 완료했으면 **Submit(**제출**)**을 클릭합니다.

정책을 처음 추가하면 모든 보안 서비스 설정이 기본값을 사용하도록 설정됩니다.

그림 ***93:*** 새로 추가된 정책 **-** 영업 그룹



단계 **7** **Add Policy(**정책 추가**)** 버튼을 다시 클릭하여 또 다른 새 정책을 추가합니다.

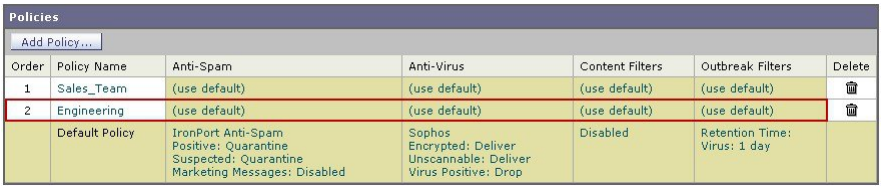
이 정책에서는 엔지니어링 팀의 구성원에 대해 개별 이메일 주소를 정의합니다.

그림 ***94:*** 엔지니어링 팀에 대한 정책 만들기

단계 **8** 엔지니어링 정책에 대한 사용자 추가를 완료했으면 **Submit(**제출**)**을 클릭합니다.

단계 **9** 변경 사항을 커밋합니다.

그림 ***95:*** 새로 추가된 정책 **-** 엔지니어링 팀



참고 이 시점에서는 새로 만든 정책에 기본 정책의 설정과 동일한 설정이 적용됩니다. 두 정책 중 하나에 속한 사용자에게 전송되는 메시지가 일치합니다. 그러나 메일 처리 설정은 기본 정책과 다르지 않습니다. 따라서 "Sales_Group" 또는 "Engineering" 정책의 사용자와 일치하는 메시지는 기본 정책과 다르지 않게 처리됩니다.

기본값, 사용자 지정 및 비활성화됨

테이블 하단의 키는 특정 정책용 셀의 컬러 코딩이 기본 행에 대해 정의된 정책과 어떤 관련이 있는지를 보여줍니다.

- 노란색 음영은 정책이 기본 정책과 동일한 설정을 사용하고 있음을 보여줍니다.
- 음영 없음(흰색)은 정책이 기본 정책과 다른 설정을 사용하고 있음을 보여줍니다.
- 회색 음영은 정책에 대해 보안 서비스가 비활성화되었음을 보여줍니다.

발신자 및 수신자의 서로 다른 그룹에 대한 메일 정책 만들기

이 부분에서는 이전 섹션에서 만든 두 개의 정책을 수정합니다.

- 영업 그룹에 대해서는 안티스팸 설정을 기본 정책보다 훨씬 더 적극적인 것으로 변경합니다. (수신 메시지에 대한 기본 안티스팸 정책 구성, 1211 페이지 참조.) 양성으로 식별된 스팸 메시지를 삭제하는 기본 정책은 유지됩니다. 그러나 이 예에서는 마케팅 메시지를 스팸 격리로 전송하도록 설정을 변경합니다.

  적극적인 정책은 영업팀의 받은 편지함으로 원치 않는 메시지가 전송되는 것을 최소화하는 효과가 있습니다.

  안티스팸 설정에 대한 자세한 내용은 Anti-Spam, 355 페이지 항목을 참고하십시오.

- 엔지니어링 팀의 경우, 의심스런 메시지의 URL을 수정하도록(example.com에 대한 링크 제외) 보안 침해 필터 기능 설정을 사용자 지정합니다. 확장명 "dwg"의 첨부 파일은 보안 침해 필터 검사를 우회합니다.

  보안 침해 필터 구성에 대한 자세한 내용은 신종 바이러스 필터(Outbreak Filter), 399 페이지를 참조하십시오.

  영업팀 정책에 대한 안티스팸 설정을 수정하려면

단계 **1** 영업 정책 행에서 안티스팸 보안 서비스(Anti-Spam) 열에 대한 링크를 클릭합니다.

정책을 방금 추가했으므로 링크 이름은 (use default)입니다.

단계 **2** 안티스팸 보안 서비스 페이지에서 "Enable Anti-Spam Scanning for this Policy(이 정책에 대한 안티스팸 검사 활성화)"의 값을 "Use Default Settings(기본 설정 사용)"에서 "Use Anti-Spam service(안티스팸 서비스 사용)"로 변경합니다.

여기서 "Use Anti-Spam service(안티스팸 서비스 사용)"를 선택하면 기본 정책에 정의된 설정을 재정의할 수 있습니다.

단계 **3** "Positively-Identified Spam Settings(양성으로 식별된 스팸 설정)" 섹션에서 "Apply This Action to Message(메시지에 이 작업 적용)"를 Drop(삭제)으로 변경합니다.

단계 **4** "Suspected Spam Settings(의심스런 스팸 설정)" 섹션에서 **Yes(**예**)**를 클릭하여 의심스런 스팸 검사를 활성화합니다.

단계 **5** "Suspected Spam Settings(의심스런 스팸 설정)" 섹션에서 "Apply This Action to Message(메시지에 이 작업 적용)"를 "Spam Quarantine(스팸 격리)"으로 변경합니다.

참고 스팸 격리를 선택하면 스팸 격리 장에 정의된 설정에 따라 메시지가 전달됩니다.

단계 **6** "Add text to subject(제목에 텍스트 추가)" 필드에 **None(**없음**)**을 클릭합니다.

스팸 격리로 전달된 메시지의 경우 제목에 태그가 추가되지 않습니다.

단계 **7** "Marketing Email Settings(마케팅 이메일 설정)" 섹션에서 **Yes(**예**)**를 클릭하여 합법적인 소스에서 오는 마케팅 메일에 대한 검사를 활성화합니다.

단계 **8** "Apply This Action to Message(메시지에 이 작업 적용)" 섹션에서 "Spam Quarantine(스팸 격리)"을 선택합니다.

단계 **9** 변경 사항을 제출 및 커밋합니다.

음영은 정책이 기본 정책과 다른 설정을 사용하고 있음을 보여줍니다.

이 시점에서는 의심스런 스팸인 메시지 및 수신자가 영업팀 정책에 대해 정의된 LDAP 쿼리와 일치하는 메시지가 스팸 격리로 전달됩니다.

발신자 및 수신자의 서로 다른 그룹에 대한 메일 정책 만들기

엔지니어링 팀 정책에 대한 Outbreak Filter(보안 침해 필터) 설정을 수정하려면

단계 **1** 엔지니어링 정책 행에서 보안 침해 필터 기능 보안 서비스(Outbreak Filters 열)에 대한 링크를 클릭합니다.

정책을 방금 추가했으므로 링크 이름은 (use default)입니다.

단계 **2** 보안 침해 필터 기능 보안 서비스 페이지에서 정책에 대한 검사 설정을 "Enable Outbreak Filtering (Customize settings)(보안 침해 필터 활성화(설정 사용자 지정))"으로 변경합니다.

여기서 "(Customize settings)"를 선택하면 기본 정책에 정의된 설정을 재정의할 수 있습니다.

이렇게 하면 페이지의 나머지도 다른 설정을 선택할 수 있도록 활성화됩니다.

단계 **3** 페이지의 "Bypass Attachment Scanning(첨부 파일 검사 우회)" 섹션에서 파일 확장명 필드에 **dwg**를 입력합니다.

파일 확장명인 “dwg”는 어플라이언스가 첨부 파일을 검사할 때 지문을 사용하여 인식할 수 있는 알려진 파일 유형 목록에는 포함되어 있지 않습니다.

참고 파일 확장명의 세 글자 앞에 점(.)을 입력할 필요가 없습니다.

단계 **4** **Add Extension(**확장명 추가**)**을 클릭하고 보안 침해 필터 기능 검사를 우회할 파일 확장명 목록에 .dwg 파일을 추가합니다.

단계 **5** **Enable Message Modification(**메시지 수정 활성화**)**을 클릭합니다.

메시지 수정을 활성화하면 어플라이언스는 대상이 지정된 위협(예: 피싱, 스캠, 의심스럽거나 악의적인 웹사이트에 대한 URL)을 검사합니다. 어플라이언스는 메시지의 링크가 웹사이트에 액세스하려고 시도할 경우 Cisco Security 프록시로 리디렉션하도록 해당 링크를 재작성할 수 있습니다.

참고 보안 침해 필터가 대상이 지정된 비 바이러스성 위협을 검사하도록 하려면 메일 정책에서 안티스팸 검사를 활성화해야 합니다.

메일 정책 및 콘텐츠 필터의 예

단계 **6** **Enable for Unsigned Messages(**서명되지 않은 메시지에 대해 활성화**)**에 대해 선택합니다.

이렇게 하면 어플라이언스는 서명된 메시지의 URL을 재작성합니다. 다른 메시지 수정 설정 및 비 바이러스성 위협으로 확인된 메시지가 릴리스되기 전 격리에 머물 기간을 구성하려면 URL 재작성을 활성화해야 합니다. 이 예에서는 기본 보유 시간인 4시간을 사용합니다.

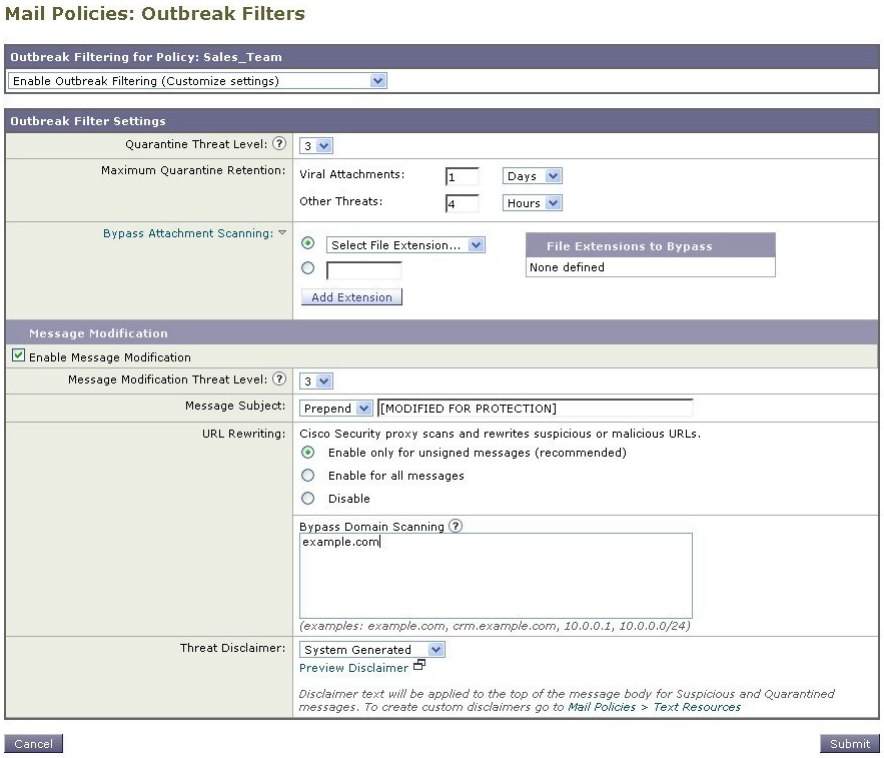
단계 **7** **Bypass Domain Scanning(**도메인 검사 우회**)** 필드에 example.com을 입력합니다.

어플라이언스는 example.com에 대한 링크를 수정하지 않습니다.

단계 **8** **Threat Disclaimer(**위협 면책조항**)**에 대해 System Generated(시스템 생성)를 선택합니다.

어플라이언스는 사용자에게 메시지 내용에 대해 경고하기 위해 메시지 본문 위에 면책조항을 삽입할 수 있습니다. 다음 예에서는 시스템 생성 위협 면책조항을 사용합니다.

그림 ***96:*** 보안 침해 필터 설정



단계 **9** 변경 사항을 제출 및 커밋합니다.

음영은 정책이 기본 정책과 다른 설정을 사용하고 있음을 보여줍니다.

이 시점에서는 파일 확장명이 dwg인 첨부 파일이 포함된 메시지(그리고 수신자가 엔지니어링 팀 정책에 대해 정의된 수신자와 일치하는 메시지)가 보안 침해 필터 검사를 우회하고 계속 처리됩니다. 도메인 example.com에 대한 링크가 포함된 메시지는 Cisco Security 프록시로 리디렉션되도록 링크가 수정되지 않으며 의심스러운 것으로 간주되지 않습니다.

메일 정책에서 발신자 또는 수신자 찾기

Incoming(수신) 또는 Outgoing Mail Policies(발신 메일 정책) 페이지의 정책에 이미 정의된 사용자를 검색하려면 "Find Policies(정책 찾기)" 버튼을 사용합니다.

예를 들어 joe@example.com을 입력하고 Find Policies(정책 찾기) 버튼을 클릭하면 정책과 일치하는 정의된 사용자가 어떤 정책에 포함되어 있는지를 보여주는 결과가 표시됩니다.

Edit Policy(정책 수정) 페이지로 이동하여 해당 정책의 사용자를 수정하려면 정책의 이름을 클릭합니다.

발신자 또는 수신자가 구성된 정책과 일치하지 않는 경우 항상 기본 정책과 일치하게 되므로 사용자를 검색할 때 항상 기본 정책이 표시됩니다.

관리되는 예외

위의 두 예에 나온 단계를 사용하여 관리되는 예외를 기반으로 정책 만들기 및 구성을 시작할 수 있습니다. 다시 말해, 조직의 요구를 평가한 후 메시지의 대다수가 기본 정책에 의해 처리되도록 정책을 구성할 수 있습니다. 그런 다음 특정 사용자 또는 사용자 그룹에 대한 추가 "예외" 정책을 만들어, 필요에 따라 다른 정책을 관리할 수 있습니다. 이런 식으로 메시지 분리가 최소화되며, 작업 대기열에서 각 분리 메시지를 처리함으로써 시스템 성능에 미치는 영향을 줄일 수 있습니다.

스팸, 바이러스 및 정책 시행에 대한 조직 또는 사용자의 허용 범위를 기반으로 정책을 정의할 수 있습니다. 다음 표에는 몇 가지 정책 예가 요약되어 있습니다. "적극적인" 정책은 최종 사용자 사서함에 도달하는 스팸 및 바이러스의 양을 최소화하도록 설계되었습니다. "신중한" 정책은 오탐을 피하고 사용자가 정책과 상관없이 메시지를 놓치지 않도록 맞춤화되었습니다.

표 ***156:*** 적극적인/신중한 메일 정책 설정

	적극적인 설정	신중한 설정
Anti-Spam	양성으로 식별된 스팸: 삭제 의심스런 스팸: 격리 마케팅 메일: 메시지 제목 앞에 "[Marketing]"을 첨부하고 전달	양성으로 식별된 스팸: 격리 의심스러운 스팸: 메시지 제목 앞에 "[Suspected Spam]"을 첨부하고 전달 마케팅 메일: 비활성화됨
Anti-Virus	복구된 메시지: 전달 암호화된 메시지: 삭제 검사되지 않은 메시지: 삭제 감염된 메시지: 삭제	복구된 메시지: 전달 암호화된 메시지: 격리 검사되지 않은 메시지: 격리 감염된 메시지: 삭제
바이러스 필터	활성화됨, 우회가 허용되는 특정 파일 확장명 또는 도메인 없음 모든 메시지에 대한 메시지 수정 활성화	활성화됨, 우회가 허용되는 특정 파일 확장명 또는 도메인 있음 서명되지 않은 메시지에 대한 메시지 수정 활성화

콘텐츠를 기반으로 메시지 필터링

메시지의 이 부분에서는 수신 메일 정책 테이블에서 사용할 새 콘텐츠 필터 3개를 만듭니다. Policy Administration(정책 관리) 사용자 지정 사용자 역할에 속한 위임된 관리자는 이러한 콘텐츠 필터를 모두 수정할 수 있습니다. 다음을 만듭니다.

1. "scan_for_confidential"

   이 필터는 메시지에서 "confidential" 문자열을 검사합니다. 이 문자열이 발견되면 메시지 복사본이 이메일 별칭 hr@example.com으로 전송되고 메시지는 정책 격리 영역으로 전송됩니다.

2. "no_mp3s"

   이 필터는 MP3 첨부 파일을 제거하고, 수신자에게 MP3 파일이 제거되었음을 알립니다.

3. "ex_employee"

   이 콘텐츠 필터는 메시지에서 특정 봉투 수신자 주소(ex-employee)를 검사합니다. 메시지가 일치하면 메시지 발신자에게 특정 알림 메시지가 전송되고 메시지는 반송됩니다.

콘텐츠 필터를 만든 후, 여러 조합으로 특정 콘텐츠 필터를 활성화하도록 각 정책(기본 정책 포함)을 구성합니다.

제목에 **"Confidential"**이 있는 메시지 격리

첫 번째 콘텐츠 필터 예에는 하나의 조건과 두 개의 작업이 포함되어 있습니다.

단계 **1** Mail Policies(메일 정책) 탭을 클릭합니다.

단계 **2** Incoming Content Filters(수신 콘텐츠 필터)를 클릭합니다.

단계 **3** **Add Filter(**필터 추가**)** 버튼을 클릭합니다.

단계 **4** Name(이름) 필드에 새 필터 이름으로 scan_for_confidential을 입력합니다.

필터 이름에는 ASCII 문자, 숫자, 밑줄 또는 대시를 포함할 수 있습니다. 콘텐츠 필터 이름의 첫 문자는 글자 또는 밑줄이어야 합니다.

단계 **5** **Editable By (Roles)(**수정 가능**(**역할**))** 링크를 클릭하고 Policy Administrator(정책 관리자)를 선택한 다음 **OK(**확인**)**를 클릭합니다.

Policy Administrator(정책 관리자) 사용자 역할에 속한 위임된 관리자는 이 콘텐츠 필터를 수정하고 메일 정책에서 사용할 수 있습니다.

단계 **6** Description(설명) 필드에 설명을 입력합니다. 예: scan all incoming mail for the string 'confidential'.

단계 **7** Add Condition(조건 추가)을 클릭합니다.

단계 **8** Message Body(메시지 본문)를 선택합니다.

단계 **9** Contains text(텍스트 포함): 필드에 confidential을 입력하고 **OK(**확인**)**를 클릭합니다.

Add Content Filter(콘텐츠 필터 추가) 페이지에 추가된 조건이 표시됩니다.

단계 **10** Add Action(작업 추가)을 클릭합니다.

단계 **11** Send Copy To (Bcc:)(복사본 전송 대상(Bcc:))를 선택합니다.

단계 **12** Email Addresses(이메일 주소) 필드에 hr@example.com을 입력합니다.

단계 **13** Subject(제목) 필드에 [message matched confidential filter]를 입력합니다.

단계 **14** **OK(**확인**)**를 클릭합니다.

Add Content Filter(콘텐츠 필터 추가) 페이지에 추가된 작업이 표시됩니다.

단계 **15** Add Action(작업 추가)을 클릭합니다.

단계 **16** Quarantine(격리)을 선택합니다.

단계 **17** 드롭다운 메뉴에서 Policy(정책) 격리 영역을 선택합니다.

단계 **18** **OK(**확인**)**를 클릭합니다.

Add Content Filter(콘텐츠 필터 추가) 페이지에 추가된 두 번째 작업이 표시됩니다.

단계 **19** 변경 사항을 제출 및 커밋합니다.

이 시점에서 콘텐츠 필터는 수신 메일 정책에 대해 활성화되어 있지 않습니다. 이 예에서는 마스터 목록에 새 콘텐츠 필터를 방금 추가했습니다. 아직 정책에 적용되지 않았으므로 어플라이언스에서 처리하는 이메일은 이 필터의 영향을 받지 않습니다.

메시지에서 **MP3** 첨부 파일 제거

두 번째 콘텐츠 필터 예에는 조건 없이 하나의 작업만 포함되어 있습니다.

단계 **1** **Add Filter(**필터 추가**)** 버튼을 클릭합니다.

단계 **2** Name(이름) 필드에 새 필터 이름으로 no_mp3s를 입력합니다.

단계 **3** **Editable By (Roles)(**수정 가능**(**역할**))** 링크를 클릭하고 Policy Administrator(정책 관리자)를 선택한 다음 **OK(**확인**)**를 클릭합니다.

단계 **4** Description(설명) 필드에 설명을 입력합니다. 예: strip all MP3 attachments.

단계 **5** Add Action(작업 추가)을 클릭합니다.

단계 **6** Strip Attachment by File Info(파일 정보로 첨부 파일 제거)를 선택합니다.

단계 **7** File type is(파일 유형)를 선택합니다.

단계 **8** 드롭다운 필드에서 -- mp3를 선택합니다.

단계 **9** 원하는 경우 대체 메시지를 입력합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** 변경 사항을 제출 및 커밋합니다.

참고 콘텐츠 필터를 만들 때에는 조건을 지정할 필요가 없습니다. 조건을 정의하지 않으면 규칙에서 항상 기존의 정의된 작업이 적용됩니다. (조건을 지정하지 않는 것은 true() 메시지 필터 규칙을 사용하는 것과 같습니다. 콘텐츠 필터를 정책에 적용하면 모든 메시지가 일치됩니다.)

퇴사 직원에게 전송된 메시지 반송

세 번째 콘텐츠 필터 예에서는 하나의 조건과 두 개의 작업을 사용합니다.

단계 **1** **Add Filter(**필터 추가**)** 버튼을 클릭합니다.

단계 **2** Name(이름): 필드에 새 필터 이름으로 **`ex_employee`**를 입력합니다.

단계 **3** **Editable By (Roles)(**수정 가능**(**역할**))** 링크를 클릭하고 Policy Administrator(정책 관리자)를 선택한 다음 **OK(**확인**)**를 클릭합니다.

단계 **4** Description(설명): 필드에 설명을 입력합니다. 예: **`bounce messages intended for Doug`**.

단계 **5** **Add Condition(**조건 추가**)**을 클릭합니다.

단계 **6** **Envelope Recipient(**봉투 수신자**)**를 선택합니다.

단계 **7** 봉투 수신자에 대해 **`Begins with`**를 선택하고 **`doug@`**을 입력합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

Content Filters(콘텐츠 필터) 페이지가 새로 고쳐지며 추가된 조건이 표시됩니다. 퇴사 직원들의 이메일 주소가 포함된 LDAP 디렉터리를 만들 수 있습니다. 퇴사 직원이 해당 디렉터리에 추가되면 이 콘텐츠 필터가 동적으로 업데이트됩니다.

단계 **9** Add Action(작업 추가)을 클릭합니다.

단계 **10** Notify(알림)를 선택합니다.

단계 **11** Sender(발신자)에 대한 확인란을 선택하고, **Subject(**제목**)** 필드에 message bounced for ex-employee of **`example.com`**을 입력합니다.

단계 **12** Use template(템플릿 사용) 섹션에서 알림 템플릿을 선택합니다.

참고 리소스가 미리 구성되지 않은 경우 콘텐츠 필터 규칙 빌더의 일부 섹션은 사용자 인터페이스에 나타나지 않습니다. 예를 들어, **Mail Policies(**메일 정책**) > Dictionaries(**사전**)** 페이지 또는 CLI의 **`dictionaryconfig`** 명령으로 미리 구성하지 않은 경우 콘텐츠 사전, 알림 템플릿 및 메시지 면책조항은 옵션으로서 나타나지 않습니다. 사전 만들기에 대한 자세한 내용은 컨텐트 사전, 613 페이지 섹션을 참조하십시오.

단계 **13** **OK(**확인**)**를 클릭합니다.

Add Content Filters(콘텐츠 필터 추가) 페이지에 추가된 작업이 표시됩니다.

단계 **14** Add Action(작업 추가)을 클릭합니다.

단계 **15** Bounce (Final Action)(반송(최종 작업))를 선택하고 OK(확인)를 클릭합니다.

콘텐츠 필터마다 하나의 최종 작업만 지정할 수 있습니다. 최종 작업을 두 개 이상 추가하려고 시도하면 GUI에 오류가 표시됩니다.

이 작업을 추가하면 퇴사 직원에게 메시지를 보낸 발신자가 두 개의 메시지를 받을 수 있습니다. 하나는 알림 템플릿에 대한 메시지이고 다른 하나는 반송 알림 템플릿에 대한 메시지입니다.

단계 **16** 변경 사항을 제출 및 커밋합니다.

서로 다른 수신자 그룹에 개별 콘텐츠 필터 적용

위 예에서는 Incoming Content Filters(수신 콘텐츠 필터) 페이지를 사용하여 세 개의 콘텐츠 필터를 만들었습니다. Incoming Content Filters(수신 콘텐츠 필터) 및 Outgoing Content filters(발신 콘텐츠 필터) 페이지에는 정책에 적용할 수 있는 모든 가능한 콘텐츠 필터의 "마스터 목록"이 있습니다.

그림 ***97: Incoming Content Filters(***수신 콘텐츠 필터***):*** 생성된 필터 ***3***개

메시지의 이 부분에서는 수신 메일 정책 테이블에서 사용할 새 콘텐츠 필터 3개를 적용합니다.

- 기본 정책은 콘텐츠 필터 3개를 모두 받습니다.
- 엔지니어링 그룹은 no_mp3s 필터를 받지 않습니다.
- 영업 그룹은 기본 수신 메일 정책으로서 콘텐츠 필터를 받습니다.

기본적으로 모든 수신자에 대해 콘텐츠 필터 활성화

활성화할 링크를 클릭하고 개별 정책에 대해 콘텐츠 필터를 선택합니다.

단계 **1** Incoming Mail Policies(수신 메일 정책)를 클릭하여 Incoming Mail Policy(수신 메일 정책) 테이블로 돌아갑니다.

페이지가 새로 고쳐지며 발신자 및 수신자 그룹에 대한 메일 정책 만들기, 1212 페이지에서 추가한 두 정책과 기본 정책이 표시됩니다. 콘텐츠 필터는 기본적으로 모든 정책에 대해 비활성화됩니다.

단계 **2** 기본 정책 행에서 콘텐츠 필터 보안 서비스(Content Filters 열)에 대한 링크를 클릭합니다.

단계 **3** 콘텐츠 필터링 보안 서비스 페이지에서 Content Filtering for Default Policy(기본 정책의 콘텐츠 필터링)의 값을 "Disable Content Filters(콘텐츠 필터 비활성화)"에서 "Enable Content Filters (Customize settings)(콘텐츠 필터 활성화(설정 사용자 지정))"로 변경합니다.

마스터 목록에 정의된 콘텐츠 필터(콘텐츠 필터 개요 , 283 페이지에서 Incoming Content Filters(수신 콘텐츠 필터) 페이지를 사용하여 생성됨)가 이 페이지에 표시됩니다. 값을 "Enable Content Filters (Customize settings)(콘텐츠 필터 활성화(설정 사용자 지정))"로 변경하면 각 필터에 대한 확인란이 비활성(회색)에서 활성으로 변경됩니다.

단계 **4** 각 콘텐츠 필터에 대해 **Enable(**활성화**)** 확인란을 선택합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

Incoming Mail Policies(수신 메일 정책) 페이지의 테이블에 기본 정책에 대해 활성화된 필터의 이름이 표시됩니다.

엔지니어링의 수신자에 대해 **MP3** 첨부 파일 허용

"engineering" 정책에 대해 "no_mp3s" 콘텐츠 필터를 비활성화하려면

단계 **1** 엔지니어링 팀 정책 행에서 콘텐츠 필터 보안 서비스(Content Filters 열)에 대한 링크를 클릭합니다.

단계 **2** 콘텐츠 필터링 보안 서비스 페이지에서 Content Filtering for Policy: Engineering(정책용 콘텐츠 필터링: 엔지니어링)의 값을 "Enable Content Filtering (Inherit default policy settings)(콘텐츠 필터링 활성화(기본 정책 설정 상속))"에서 "Enable Content Filtering (Customize settings)(콘텐츠 필터링 활성화(설정 사용자 지정))"으로 변경합니다.

이 정책은 기본값을 사용하므로 "Use Default Settings(기본 설정 사용)"의 값을 "Yes(예)"로 변경하면 각 필터에 대한 확인란이 비활성(회색)에서 활성으로 변경됩니다.

단계 **3** "no_mp3s" 필터에 대한 확인란의 선택을 취소합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

Incoming Mail Policies(수신 메일 정책) 페이지의 테이블에 엔지니어링 정책에 대해 활성화된 필터의 이름이 표시됩니다.

단계 **5** 변경 사항을 커밋합니다.

다음에 수행할 작업

이 시점에서, 엔지니어링 정책에 대한 사용자 목록과 일치하는 수신 메시지에서는 MP3 첨부 파일이 제거되지 않습니다. 그러나 다른 모든 수신 메시지에서는 MP3 첨부 파일이 제거됩니다.

GUI에서 콘텐츠 필터 구성 시 참고 사항

- 콘텐츠 필터를 만들 때에는 조건을 지정할 필요가 없습니다. 작업을 정의하지 않으면 규칙에서 항상 기존의 정의된 작업이 적용됩니다. (작업을 지정하지 않는 것은 true() 메시지 필터 규칙을 사용하는 것과 같습니다. 콘텐츠 필터를 정책에 적용하면 모든 메시지가 일치됩니다.)
- 콘텐츠 필터에 사용자 지정 사용자 역할을 할당하지 않으면 콘텐츠 필터는 퍼블릭 필터가 되며, 메일 정책에 대해 위임된 관리자는 누구나 사용할 수 있습니다. 위임된 관리자 및 콘텐츠 필터에 대한 자세한 내용은 관리 작업 배포, 893 페이지를 참조하십시오.
- 관리자와 운영자는 콘텐츠 필터에 사용자 지정 사용자 역할이 할당된 경우에도 어플라이언스에 있는 모든 콘텐츠 필터를 보고 수정할 수 있습니다.
- 필터 규칙과 작업에 대한 텍스트를 입력할 때 정규식 일치에서 다음 메타 문자는 특별한 의미를 가집니다. . ^ $ * + ? { [ ] \ | ( )

  정규식을 사용하지 않으려면 '\'(백슬래시)를 사용하여 이러한 문자를 이스케이프해야 합니다. 예: "*Warning*"

- 콘텐츠 필터에 대해 둘 이상의 조건을 정의하는 경우 콘텐츠 필터를 일치로 간주하기 위해 정의된 작업 전체(논리적 AND)를 적용할지, 아니면 정의된 작업 중 하나(논리적 OR)를 적용할지를 정의할 수 있습니다.
- "benign(정상)" 콘텐츠 필터를 만들어 메시지 분리 및 콘텐츠 필터를 테스트할 수 있습니다. 예를 들면 유일한 작업이 "deliver(전달)"인 콘텐츠 필터를 만들 수 있습니다. 이 콘텐츠 필터는 메일 처리에 영향을 미치지 않습니다. 그러나 이 필터를 사용하여 메일 정책 처리가 시스템의 다른 요소(예: 메일 로그)에 어떤 영향을 미치는지를 테스트할 수 있습니다.

메일 정책 및 콘텐츠 필터의 예

- 반대로, 수신 또는 발신 콘텐츠 필터의 "마스터 목록" 개념을 사용하면 어플라이언스에서 처리되는 모든 메일의 메시지 처리에 즉각적으로 영향을 미치는 매우 강력하고 포괄적인 콘텐츠 필터를 만들 수 있습니다. 이 필터의 프로세스는 다음과 같습니다.
  - Incoming or Outgoing Content Filters(수신 또는 발신 콘텐츠 필터) 페이지를 사용하여 순서가 1인 새 콘텐츠 필터를 만듭니다.
  - Incoming or Outgoing Mail Policies(수신 또는 발신 메일 정책) 페이지를 사용하여 기본 정책에 대한 새 콘텐츠 필터를 활성화합니다.
  - 모든 나머지 정책에 대해 콘텐츠 필터를 활성화합니다.

- 콘텐츠 필터에서 사용 가능한 Bcc: 및 격리 작업은 생성하는 격리의 보존 설정을 결정하는 데 도움이 될 수 있습니다. (정책, 바이러스, 보안 침해 격리, 847 페이지를 참조하십시오.) 메시지가 시스템에서 너무 빨리 릴리스되지 않도록(즉, 격리 영역이 할당된 디스크 공간을 너무 빨리 채우지 않도록) 정책 격리를 드나드는 메일 플로우를 시뮬레이션하는 필터를 만들 수 있습니다.
- "Entire Message(전체 메시지)" 조건은 Scan Behavior(검사 동작) 페이지 또는 scanconfig 명령과 동일한 설정을 사용하므로 메시지의 헤더를 검사하지 않습니다. "Entire Message(전체 메시지)"를 선택하면 메시지 본문과 첨부 파일만 검사합니다. 특정 헤더 정보를 검색하려면 "Subject(제목)" 또는 "Header(헤더)" 조건을 사용하십시오.
- 어플라이언스에서 LDAP 서버를 구성한 경우(즉, ldapconfig 명령을 사용하여 특정 문자열로 특정 LDAP 서버를 쿼리하도록 어플라이언스를 구성한 경우) LDAP 쿼리로 사용자를 구성하는 것은 GUI에만 나타납니다.
- 리소스가 미리 구성되지 않은 경우 콘텐츠 필터 규칙 빌더의 일부 섹션은 GUI에 나타나지 않습니다. 예를 들어, Text Resources(텍스트 리소스) 페이지 또는 CLI의 textconfig 명령으로 미리 구성하지 않은 경우 알림 템플릿 및 메시지 면책조항은 옵션으로서 나타나지 않습니다.
- 콘텐츠 필터 기능은 다음 문자 인코딩을 인식하고, 포함할 수 있으며, 해당 텍스트를 검사할 수 있습니다.
  - 유니코드(UTF-8)
  - 유니코드(UTF-16)
  - 서유럽/라틴-1(ISO 8859-1)
  - 서유럽/라틴-1(Windows CP1252)
  - 중국어 번체(Big 5)
  - 중국어 간체(GB 2312)
  - 중국어 간체(HZ GB 2312)
  - 한국어(ISO 2022-KR)
  - 한국어(KS-C-5601/EUC-KR)
  - 일본어(Shift-JIS (X0123))
  - 일본어(ISO-2022-JP)
  - 일본어(EUC)

단일 콘텐츠 필터 내에서 여러 문자 집합을 혼합하여 사용할 수 있습니다. 여러 문자 인코딩으로 텍스트를 표시 및 입력하는 방법은 웹 브라우저의 설명서를 참조하십시오. 대부분의 브라우저는 여러 문자 집합을 동시에 렌더링할 수 있습니다.

메일 정책 및 콘텐츠 필터의 예

그림 ***98:*** 콘텐츠 필터의 여러 문자 집합

- 콘텐츠 필터에 대해 표시되는 보기를 변경하려면 Incoming or Outgoing Content Filters(수신 또는 발신 콘텐츠 필터) 요약 페이지에서 "Description(설명)", "Rules(규칙)" 및 "Policies(정책)"에 대한 링크를 사용합니다.
  - **Description(**설명**)** 보기는 각 콘텐츠 필터에 대한 설명 필드에 입력한 텍스트를 표시합니다. (이것이 기본 보기입니다.)
  - **Rules(**규칙**)** 보기는 규칙 빌더 페이지에서 만든 규칙 및 정규식을 표시합니다.
  - **Policies(**정책**)** 보기는 각 콘텐츠 필터가 활성화된 대상 정책을 표시합니다.

메일 정책 및 콘텐츠 필터의 예

D 부 록

방화벽 정보

이 장에는 다음 섹션이 포함되어 있습니다.

방화벽 정보

다음 표에는 Cisco Content Security Appliance의 적절한 작동을 위해 열어야 할 수 있는 가능한 포트가 기본값으로 나열되어 있습니다.

표 ***157:*** 방화벽 포트

기본 포트	**Protocol(**프로토콜**)**	**In/Out**	**Hostname**	목적
20/21	TCP	In/Out	AsyncOS IP, FTP 서버	로그 파일의 어그리게이션을 위한 FTP. 데이터 포트 TCP 1024 이상은 모두 열려 있어야 합니다. 자세한 내용은 기술 자료의 FTP 포트 정보를 검색하십시오. 기술 자료, 7 페이지를 참조하십시오.
22	TCP	In	AsyncOS IP	CLI에 대한 SSH 액세스, 로그 파일의 어그리게이션.
22	TCP	Out	SSH 서버	로그 파일의 SSH 어그리게이션.
22	TCP	Out	SCP 서버	로그 서버에 SCP 푸시.
25	TCP	Out	모두	이메일을 전송하기 위한 SMTP입니다.

방화벽 정보

25	TCP	In	AsyncOS IP	반송된 메일 또는 방화벽 외부에서 주입되는 메일을 수신하기 위한 SMTP.
53	UDP/TCP	Out	DNS 서버	인터넷 루트 서버 또는 방화벽 외부의 다른 DNS 서버를 사용하도록 구성된 경우 DNS. SenderBase 쿼리에도 해당.
80	HTTP	In	AsyncOS IP	시스템 모니터링용 GUI에 대한 HTTP 액세스.
80	HTTP	Out	downloads.ironport.com	및 McAfee 정의 외의 서비스 업데이트
80	HTTP	Out	updates.ironport.com	AsyncOS 업그레이드 및 McAfee Anti-Virus 정의.
80	HTTP	Out	cdn-microupdates.cloudmark.com	Intelligent MultiScan에서 서드파티 스팸 구성 요소에 대한 업데이트에 사용됨. 서드파티 phone home 업데이트를 위해 어플라이언스를 CIDR 범위 208.83.136.0/22에도 연결해야 합니다.
80	HTTP	Out	TAXII 서버	게이트웨이가 외부 위협 피드를 사용하도록 허용하는 데 사용됩니다.
82	HTTP	In	AsyncOS IP	스팸 격리를 보는 데 사용.
83	HTTPS	In	AsyncOS IP	스팸 격리를 보는 데 사용.
110	TCP	Out	POP 서버	스팸 격리를 위한 엔드유저 POP 인증.
123	UDP	In 및 Out	NTP 서버	시간 서버가 방화벽 외부에 있는 경우 NTP.
143	TCP	Out	IMAP 서버	스팸 격리를 위한 엔드유저 IMAP 인증.
161	UDP	In	AsyncOS IP	SNMP 쿼리.
162	UDP	Out	관리 스테이션	SNMP 트랩.

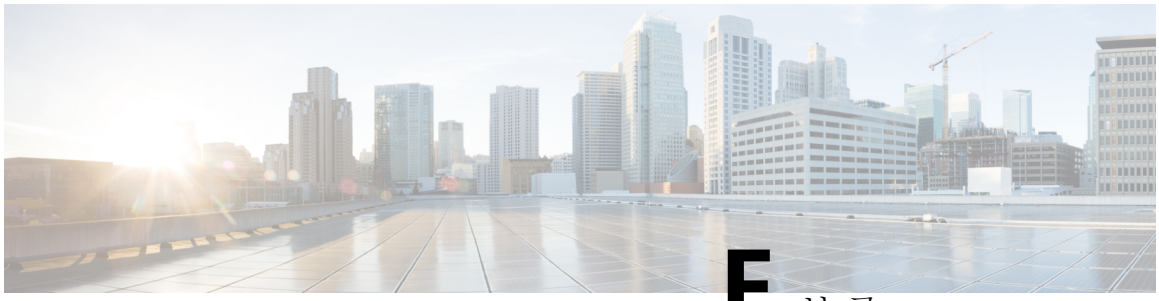
389 또는 3268	LDAP	Out	LDAP 서버	LDAP 디렉터리 서버가 방화벽 외부에 있는 경우 LDAP. Cisco Spam Quarantine을 위한 LDAP 인증.
636 또는 3269	LDAPS	Out	LDAPS	LDAPS - ActiveDirectory의 Global Catalog Server(SSL 사용).
443	TCP	In	AsyncOS IP	시스템 모니터링용 GUI에 대한 보안 HTTP(https) 액세스.
443	TCP	Out	res.cisco.com	업데이트 서버에 대한 최신 파일을 확인합니다.
443	TCP	Out	update-manifests.ironport.com	업데이트 서버에서 최신 파일 목록을 가져옵니다(물리적 하드웨어 어플라이언스용).
443	TCP	Out	update-manifests.sco.cisco.com	업데이트 서버에서 최신 파일 목록을 가져옵니다(가상 어플라이언스용).
443	TCP	Out	phonehome.senderbase.org	Outbreak Filter 수신/전송.
443	TCP	Out	CLI(command-line interface)에서 websecurityadvancedconfig 명령을 실행하고 모든 기본값을 수락합니다. 웹 보안 서비스 호스트 이름이 표시됩니다.	URL 평판 및 URL 필터링용 범주 정보를 가져오기 위한 클라우드 서비스.
443	TCP	Out	Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석), Advanced Settings for File Reputation(파일 평판용 고급 설정) 섹션, Cloud Server Pool(클라우드 서버 풀) 매개변수에서 구성.	구성된 경우, 파일 평판을 가져오기 위해 클라우드 서비스에 액세스하기 위한 포트. 기본 포트는 32137입니다. 파일 분석 서비스는 포트 443을 참조하십시오.
443	TCP	Out	Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석), Advanced Settings for File Reputation(파일 평판용 고급 설정) 섹션에서 구성.	파일 분석을 위해 클라우드 서비스 액세스. 파일 평판 서비스는 포트 443 또는 32137을 참조하십시오.

방화벽 정보

443	TCP	In 및 Out	Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석), Advanced Settings for File Reputation(파일 평판용 고급 설정) 섹션, AMP for Endpoints Console 통합 매개변수에서 구성. api.amp.sourcefire.com api.eu.amp.sourcefire.com api.apjc.amp.sourcefire.com api.amp.cisco.com api.eu.amp.cisco.com api.apjc.amp.cisco.com	AMP for Endpoints Console 서버에 대한 액세스.
443	TCP	In 및 Out	outlook.office365.com login.microsoftonline.com.	사서함 자동 치료용 Office 365 서비스에 대한 액세스.
443	TCP	Out	aggregator.cisco.com	Cisco Aggregator Server에 대한 액세스.
443	HTTPS	Out	logapi.ces.cisco.com	Cisco TAC에서 수집한 디버그 로그 업로드.
443	HTTPS	Out	TAXII 서버	게이트웨이가 외부 위협 피드를 사용하도록 허용하는 데 사용됩니다.
514	UDP/TCP	Out	Syslog 서버	Syslog 로깅.
628	TCP	In & In	AsyncOS IP	방화벽 외부에서 이메일을 주입하는 경우 QMQP.
990	TCP/FTP	Out	support-ftp.cisco.com	Cisco TAC에서 수집한 디버그 로그 업로드.
1024 이상	—	—	—	포트 21(FTP)은 위 정보를 참조하십시오.
2222	CCS	In & In	AsyncOS IP	클러스터 통신 서비스(중앙 관리용).
	TCP	Out	AsyncOS IP	Cisco Spam Quarantine.

7025	TCP	In/Out	AsyncOS IP	이 기능이 중앙에서 관리되는 경우 Email Security Appliance 와 Security Management Appliance 간 통과 정책, 바이러스 및 보안 침해 격리 데이터.

방화벽 정보



부록 E

최종 사용자 라이센스 계약

이 부록에는 다음 섹션이 포함되어 있습니다.

Cisco Systems 최종 사용자 라이센스 계약

중요: 본 최종 사용자 라이센스 계약을 주의 깊게 읽으십시오. 귀하가 **CISCO** 소프트웨어 또는 장비를 승인된 소스로부터 구매하고 있는지, 그리고 귀하 또는 귀하가 대표하는 실체("고객"으로 통칭)가 본 **CISCO** 최종 사용자 라이센스 계약의 목적에 맞게 최종 사용자로 등록되었는지를 확인하는 것이 매우 중요합니다. 귀하는 최종 사용자로 등록되어 있지 않은 경우 소프트웨어를 사용할 라이센스가 없으며 본 최종 사용자 라이센스 계약의 제한된 보증이 적용되지 않습니다. **CISCO** 또는 **CISCO** 제공 소프트웨어를 승인된 소스로부터 구매하고 다운로드, 설치 또는 사용하는 경우 귀하는 본 계약에 동의하는 것입니다.

Cisco Systems, Inc. 또는 CISCO SYSTEMS, INC. 대신 소프트웨어를 라이센싱하는 자회사("CISCO")는 귀하가 소프트웨어를 승인된 소스로부터 구매한 경우 그리고 본 최종 사용자 라이센스 계약에 포함된 모든 약관 및 제품에 수반되거나 주문 시 사용 가능한 보충 라이센스 계약("계약"으로 통칭)에 명시된 모든 추가 제한 사항에 동의하는 경우에만 본 소프트웨어의 라이센스를 부여합니다. 본 최종 사용자 라이센스 계약 및 보충 라이센스 계약의 조건이 상충하는 경우 보충 라이센스 계약이 적용됩니다. 소프트웨어를 다운로드, 설치 또는 사용함으로써 귀하는 소프트웨어를 승인된 소스로부터 구매하였으며 계약을 준수할 것임을 나타내는 것입니다. 귀하가 계약의 모든 조건에 동의하지 않는 경우 CISCO는 귀하에게 소프트웨어에 대한 라이센스를 부여하지 않으며, (A) 귀하는 소프트웨어를 다운로드, 설치 또는 사용할 수 없고 (B) 귀하는 전액 환불을 위해 소프트웨어를 반환(개봉하지 않은 CD 패키지 및 서면 자료 포함)할 수 있으며, 소프트웨어 및 서면 자료가 다른 제품의 일부로 제공된 경우 귀하는 전액 환불을 위해 전체 제품을 반환할 수 있습니다. 귀하의 반환 및 환불 권리는 승인된 소스로부터 구매한 지 30일 후에 만료되며, 귀하가 등록되어 있는 원래 최종 사용자 구매자인 경우에만 적용됩니다. 본 최종 사용자 라이센스 계약에서 "승인된 소스"란 (A) CISCO 또는 (B) 해당 지역 내에서 최종 사용자에게 CISCO 장비, 소프트웨어 및 서비스를 배포하도록 CISCO에서 승인한 총판사 또는 시스템 통합업체 또는 (C) 그러한 총판사 또는 시스템 통합업체에서 CISCO와 총판사의 계약 조건에 따라 해당 지역 내에서 최종 사용자에게 CISCO 장비, 소프트웨어 및 서비스를 배포/판매하도록 승인한 리셀러를 의미합니다.

최종 사용자 라이센스 계약

다음의 계약 조건은 고객의 소프트웨어 사용*(*아래에 정의*)*을 제어하되, *(A)* 고객과 고객의 소프트웨어 사용을 제어하는 *CISCO* 간에 별도의 서명된 계약이 있는 경우 또는 *(B)* 고객의 소프트웨어 사용을 제어하는 설치 또는 다운로드 프로세스의 일부로서 소프트웨어에 별도의 *"*클릭-동의*"* 라이센스 계약 또는 서드파티 라이센스 계약이 포함된 경우는 예외입니다. 앞서 언급한 문서의 조항이 상충하는 경우 우선순위는 *(1)* 서명된 계약, *(2)* 클릭-동의 계약 또는 서드파티 라이센스 계약, *(3)* 본 계약입니다. 본 계약에서 *"*소프트웨어*"*란 컴퓨터 프로그램*(*승인된 소스에서 고객에게 제공된 *CISCO* 장비에 내장된 펌웨어 및 컴퓨터 프로그램 포함*)*, 업그레이드, 업데이트, 버그 픽스 또는 이에 따른 수정 버전*(*"업그레이드"로 통칭*)*, *CISCO* 소프트웨어 양도 및 재라이센싱 정책*(CISCO*에서 수시로 수정 가능*)*에 따라 재라이센스된 것 또는 그러한 것의 백업 사본을 의미합니다.

라이센스. 본 계약의 약관을 준수하는 범위에서 Cisco는 고객이 승인된 소스에 필요한 라이센스 요금을 지불한 소프트웨어 및 문서를 고객의 내부 비즈니스 목적으로 사용할 비독점적이고 양도 불가능한 라이센스를 부여합니다. "문서"란 소프트웨어에 관해 작성되어 승인된 소스에서 어떤 방식으로든 (CD-ROM 또는 온라인) 소프트웨어와 함께 사용하도록 제공하는 정보(사용자 또는 기술 매뉴얼, 교육 자료, 사양 등)를 의미합니다. 소프트웨어를 사용하려면 고객은 등록 번호나 제품 인증 키를 입력하고 Cisco 웹사이트에서 소프트웨어의 고객 사본을 온라인으로 등록하여 필요한 라이센스 키 또는 라이센스 파일을 얻어야 할 수 있습니다.

고객의 소프트웨어 사용 라이센스 및 소프트웨어 사용 범위는 단일 하드웨어 섀시나 카드로 제한되거나, 해당 보충 라이센스 계약에 명시되거나 승인된 소스가 동의했고 고객이 승인된 소스에 필요한 라이센스 요금을 지불한 해당 구매 발주서("구매 발주서")에 명시된 기타 제한 사항으로 제한됩니다.

문서 또는 해당되는 보충 라이센스 계약에 달리 명시하지 않는 한 고객은 소프트웨어를 내장된 대로 실행에 사용하거나, (해당 문서에서 비 Cisco 장비에 설치를 허용한 경우) 고객이 소유하거나 임대한 Cisco 장비와의 통신 및 고객의 내부 비즈니스 용도로 사용할 수 있습니다. 암시, 금반언 등에 의해 다른 어떤 라이센스도 부여되지 않습니다.

Cisco에서 라이센스 요금을 부과하지 않는 평가판 또는 베타 사본의 경우 위의 라이센스 요금 지불 요건이 적용되지 않습니다.

일반 제한 사항. 타이틀의 양도가 아니라 소프트웨어 및 문서에 대한 라이센스이므로 Cisco는 소프트웨어 및 문서의 모든 사본에 대한 소유권을 보유합니다. 소프트웨어 및 문서에는 개별 프로그램의 특정 내부 설계와 구조 및 관련 인터페이스 정보를 포함하여(이에 제한되지 않음) Cisco 또는 공급업체나 라이센스 허가업체의 영업 비밀이 포함되어 있음을 고객은 인지합니다. 계약에 달리 명시하지 않는 한 고객은 승인된 소스로부터 구매한 Cisco 장비의 사용과 연결해서만 소프트웨어를 사용하며, 고객은 다음에 대해 권리가 없고 다음을 수행하지 않을 것에 특별히 동의합니다.

(i) 타인 또는 다른 실체에 라이센스 권리를 양도하거나 하위 라이센스를 부여하거나(Cisco 재라이센싱/양도 정책 적용의 준수 외), 고객이 승인된 소스로부터 구매하지 않은 Cisco 장비 또는 중고 Cisco 장비에서 소프트웨어를 사용하는 행위. 고객은 양도, 하위 라이센스 부여 또는 사용을 시도하는 행위가 무효임을 인지합니다.

(ii) 오류를 고치거나 소프트웨어를 달리 수정 또는 각색하거나 소프트웨어를 기반으로 파생물을 만들거나 서드파티에 동일한 일을 하도록 허용하는 행위.

(iii) 소프트웨어를 리버스 엔지니어링 또는 디컴파일, 해독, 디스어셈블하거나 인간이 읽을 수 있는 형식으로 축소하는 행위. 단, 이러한 제한에도 불구하고 적용법에 따라 명시적으로 허가되거나 적용되는 오픈 소스 라이센스에 따라 Cisco가 특정 활동을 허가해야 하는 경우는 예외입니다.

(iv) 소프트웨어에서 실행되는 벤치마크 테스트의 결과를 게시하는 행위.

(v) Cisco의 명시적인 서면 인증 없이 서비스 사무소에서 또는 시간 공유 기반으로 서드파티의 서비스를 수행하는 데 소프트웨어를 사용하거나 사용하도록 허가하는 행위.

(vi) Cisco의 사전 서면 승인 없이 소프트웨어 및 문서 내에 포함된 영업 비밀을 서드파티에서 사용할 수 있도록 공개, 제공 또는 달리 조작하는 행위. 고객은 그러한 영업 비밀을 보호하기 위해 합당한 보안 조치를 취해야 합니다.

적용법의 요구에 따라 그리고 고객의 서면 요청에 따라 Cisco는 해당 요금을 Cisco에 지불하는 경우 소프트웨어와 다른 독립적으로 생성된 프로그램 간 상호 운용성을 위해 필요한 인터페이스 정보를 고객에게 제공합니다. 고객은 그러한 정보와 관련된 기밀 유지의 책임을 엄격히 준수해야 하며, Cisco에서 그러한 정보를 사용 가능하게 하는 해당 약관에 따라 그러한 정보를 사용해야 합니다.

소프트웨어, 업그레이드 및 추가 사본. 계약의 다른 조항에도 불구하고: (1) 사본이나 업그레이드를 만들거나 얻은 시점에 고객이 이미 원본 소프트웨어에 대한 유효한 라이센스를 보유하고 있으며 업그레이드 또는 추가 사본에 대해 승인된 소스에 해당 요금을 이미 지불한 경우가 아닌 한, 고객은 추가 사본 또는 업그레이드를 만들거나 사용할 라이센스 또는 권리가 없습니다. (2) 업그레이드 사용은 고객이 원래 최종 사용자 구매자 또는 임차인이거나 업그레이드할 소프트웨어 사용에 대한 유효한 라이센스를 보유하고 있는, 승인된 소스가 제공한 CISCO 장비로 제한됩니다. (3) 추가 사본을 만들고 사용하는 것은 필요한 백업용으로만 제한됩니다.

소유 자산 통지. 고객은 어떤 형식이든 모든 저작권, 소유 자산 및 기타 통지를, 그러한 저작권 및 기타 소유 자산 통지가 소프트웨어에 포함되어 있는 것과 동일한 형식과 방법으로, 소프트웨어의 모든 사본에서 유지 및 재현할 것에 동의합니다. 계약에 명시적으로 승인된 경우를 제외하고, 고객은 Cisco의 사전 서면 승인 없이 소프트웨어의 사본이나 복제본을 만들지 않습니다.

기간 및 종료. 계약 및 여기에 부여된 라이센스는 종료될 때까지 유효합니다. 고객은 소프트웨어와 문서의 모든 사본을 폐기함으로써 언제든지 계약과 라이센스를 종료할 수 있습니다. 고객이 계약의 조항을 준수하지 않으면 계약에 따른 고객의 권리는 Cisco에서의 통보 없이 즉시 종료됩니다. 종료 시 고객은 소유 또는 제어하는 모든 소프트웨어 및 문서의 사본을 폐기해야 합니다. 고객의 모든 기밀 유지 책임, "일반 제한 사항" 섹션에서 고객에게 부여된 모든 제약 조건과 제한 사항 그리고 모든 책임과 면책조항과 보증의 제한과 제약은 계약의 종료 이후에도 유지됩니다. 또한 "미국 정부 최종 사용자 구매자" 및 "제한된 보증 안내문 및 최종 사용자 라이센스 계약에 적용되는 일반 약관" 섹션의 조항은 계약 종료 이후에도 유지됩니다.

고객 레코드. 고객은 본 계약의 준수 여부를 확인하기 위해 정상 영업시간에 고객의 장부, 레코드 및 회계를 검토할 권리를 Cisco 및 해당 독립 회계업체에 부여합니다. 그러한 감사에서 본 계약의 위반이 발견되면 고객은 적절한 라이센스 요금 및 감사에 따른 합당한 비용을 즉시 Cisco에 지불해야 합니다.

수출, 재수출, 양도 및 규제 사용. 계약에 따라 Cisco에서 제공하는 소프트웨어, 문서와 기술 또는 그에 따른 직접 제품(이후 "소프트웨어 및 기술")은 미국의 법률과 규정 및 기타 해당 국가의 법률과 규정에 따라 수출 규제의 대상이 됩니다. 고객은 Cisco 소프트웨어 및 기술의 수출, 재수출, 양도, 사용을 관장하는 관련 법률과 규정을 준수해야 하며 미국 및 현지의 모든 필요한 승인, 허가 또는 라이센스를 얻어야 합니다. Cisco와 고객은 권한 또는 라이센스의 보호와 관련하여 상대방에 합리적으로 요구할 수 있는 기타 정보, 지원 문서 및 지원을 제공할 것에 각각 동의합니다. 수출, 재수출, 양도 및 사용의 규정준수와 관련된 정보는 다음 URL에서 찾을 수 있습니다.

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

최종 사용자 라이센스 계약

미국 정부 최종 사용자 구매자. 소프트웨어 및 문서는 Federal Acquisition Regulation("FAR")(48 C.F.R.) 2.101에 정의된 대로 "상용 품목"이며, FAR 12.212에 사용된 "상용 컴퓨터 소프트웨어" 및 "상용 컴퓨터 소프트웨어 문서" 같은 용어로 구성되어 있습니다. FAR 12.212 및 DoD FAR Supp. 227.7202-1~227.7202-4와 일치하고 계약에 통합되어 있을 수 있는 다른 계약에 반하는 FAR 또는 기타 계약 조항이 있더라도, 고객은 정부 최종 사용자에게 소프트웨어 및 문서를 제공할 수 있으며, 계약이 직접적인 경우 정부 최종 사용자는 계약에 명시된 권리만으로 소프트웨어 및 문서를 취득하게 됩니다. 소프트웨어나 문서 또는 둘을 모두 사용하는 경우 소프트웨어 및 문서는 "상용 컴퓨터 소프트웨어" 및 "상용 컴퓨터 소프트웨어 문서"라는 정부와의 계약이 성립되고, 여기에 명시된 권리와 제약 조건을 따르는 것으로 간주됩니다.

식별된 구성 요소*:* 추가 용어. 소프트웨어는 하나 이상의 구성 요소를 포함하거나 그러한 구성 요소와 함께 제공될 수 있으며, 그러한 구성 요소에는 Cisco가 문서, readme.txt 파일, 서드파티 클릭-동의 또는 다른 곳(예: http://www.cisco.com/)에서 식별한 서드파티 구성 요소("식별된 구성 요소")가 포함될 수 있고, 여기에 명시된 것과 다른 라이센스 계약 조건, 워런티의 면책조항, 제한된 워런티 또는 기타 약관("추가 조건"으로 통칭)이 적용될 수 있습니다. 귀하는 그러한 식별된 구성 요소에 적용되는 추가 조건에 동의합니다.

제한된 보증

여기에 명시된 제한 사항과 조건에 따라 Cisco는 (a) 소프트웨어를 담아 제공하는 미디어는 정상적으로 사용할 경우 재질 및 제조상 결함이 없으며, (b) 소프트웨어는 실제로 문서와 일치한다는 점을, 고객에게 배송된 날짜부터 시작(Cisco 이외의 승인된 소스에 의해 재판매되는 경우 Cisco의 원래 배송일 이후 90일 기간에 시작)하여 (a) 90일 동안 또는 (b) 소프트웨어가 포함된 제품("제품")에 동봉된 보증 카드에 소프트웨어에 대해 특별히 명시된 보증 기간(있는 경우) 동안 보증합니다. Cisco 제품 배송 날짜는 제품이 배송되는 포장 재료에 명시됩니다. 상기 내용을 제외하고 소프트웨어는 "있는 그대로" 제공됩니다. 본 제한된 보증은 처음 등록된 최종 사용자인 고객이 승인된 소스로부터 구매한 소프트웨어에만 적용됩니다. 본 제한된 보증에 따라 고객의 유일한 보상 및 Cisco와 공급업체의 전체 책임은 (i) 결함 있는 미디어의 교체 및/또는 (ii) Cisco의 선택에 따른 수리, 교체 또는 소프트웨어 구매 가격의 환불이며, 두 경우 모두 본 제한된 보증의 위반을 구성하는 오류나 결함은 보증된 기간 내에 고객에게 소프트웨어를 제공한 승인된 소스로 보고된 것이어야 합니다. Cisco 또는 고객에게 소프트웨어를 제공하는 승인된 소스는 보상의 조건으로서 선택적으로 소프트웨어 및/또는 문서의 반환을 요구할 수 있습니다. 어떤 경우에도 Cisco는 소프트웨어에 오류가 없음과 고객이 문제 또는 중단 없이 소프트웨어를 작동할 수 있을 것임을 보증합니다. 또한 네트워크 침입과 공격을 위한 지속적인 신기술 개발 때문에 Cisco는 소프트웨어 또는 소프트웨어가 사용되는 장비, 시스템 또는 네트워크가 침입이나 공격에 취약하지 않을 것이라고 보증하지 않습니다.

제약 조건. 소프트웨어, 제품 또는 소프트웨어 사용이 인증된 기타 장비가 (a) 변경된 경우(Cisco 또는 공인 대리점에서 변경한 경우 제외), (b) Cisco에서 제공한 지침에 따라 설치, 작동, 수리 또는 유지 관리된 경우, (c) 비정상적인 물리적 또는 전기적 스트레스, 비정상적인 환경 조건, 오용, 부주의, 사고를 겪은 경우 또는 (d) 베타, 평가, 테스트 또는 데모 목적으로 라이센스가 부여된 경우에는 본 보증이 적용되지 않습니다. 또한 (e) 임시 소프트웨어 모듈, (f) Cisco 소프트웨어 센터에 게시되지 않은 소프트웨어, (g) Cisco가 Cisco 소프트웨어 센터에 "있는 그대로" 기반으로 명시적으로 제공하는 소프트웨어, (h) 승인된 소스에서 라이센스 요금을 받지 않는 소프트웨어, (i) 승인된 소스가 아닌 서드파티에서 제공하는 소프트웨어에도 소프트웨어 보증이 적용되지 않습니다.

최종 사용자 라이센스 계약

보증의 면책조항

본 보증 섹션에 지정된 내용을 제외하고, 상업성, 특정 목적에의 적합성, 비위반, 만족스런 품질, 비간섭, 정보 내용의 정확성을 포함하여(이에 제한되지 않음) 또는 거래, 법률, 사용 또는 무역 관행에서 발생하는 모든 명시적 또는 암시적 조건, 표현 및 보증은 적용법에서 허용하는 한도까지 제외되며 **CISCO,** 공급업체 또는 라이센스 허가업체에 의해 명시적으로 부인됩니다**.** 동일한 것 중 어떤 것도 제외할 수 없는 경우**,** 그러한 암시적 조건**,** 표현 및/또는 보증은 위의 "제한적 보증" 섹션에 나와 있는 명시적 보증 기간까지로 제한됩니다**.** 일부 국가나 관할 지역에서는 암시적 보증의 지속 기간에 대한 제한을 허용하지 않으므로 위의 제한 사항이 적용되지 않을 수 있습니다**.** 본 보증은 고객에게 특별한 법적 권리를 제공하며**,** 고객은 관할 지역에 따라 다른 권리를 보유할 수 있습니다**.** 위에 기술한 명시적 보증이 본질적 목적에 맞지 않는 경우에도 본 면책조항 및 예외는 적용됩니다.

책임의 면책조항 - 책임의 제한 사항. 미국, 라틴아메리카, 캐나다, 일본 또는 카리브해에서 소프트웨어를 구매한 경우 계약에 반대되는 내용이 있더라도, Cisco, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체의 고객에 대한 모든 책임은 계약, 불법 행위(태만 포함), 워런티 위반 등 무엇이든 고객이 클레임의 원인이 된 소프트웨어에 대해 승인된 소스에 지불한 가격을 넘지 않으며, 소프트웨어가 또 다른 제품의 일부인 경우 해당 제품에 대해 지불한 가격을 넘지 않습니다. 소프트웨어에 대한 이 책임의 제한은 누적되며 사건당 적용되지 않습니다(즉, 클레임이 둘 이상 있는 경우에도 이 제한이 확대되지 않습니다).

유럽, 중동, 아프리카, 아시아 및 오세아니아에서 소프트웨어를 구매한 경우 계약에 반대되는 내용이 있더라도, CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체의 고객에 대한 모든 책임은 계약, 불법 행위(태만 포함), 보증 위반 등 무엇이든 고객이 클레임의 원인이 된 소프트웨어에 대해 CISCO에 지불한 가격을 넘지 않으며, 소프트웨어가 또 다른 제품의 일부인 경우 해당 제품에 대해 지불한 가격을 넘지 않습니다. 소프트웨어에 대한 이 책임의 제한은 누적되며 사건당 적용되지 않습니다(즉, 클레임이 둘 이상 있는 경우에도 이 제한이 확대되지 않습니다). 계약의 어떤 내용도 (I) 과실로 인한 개인 상해 또는 사망에 대해 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체의 고객에 대한 책임을 제한하지 않고, (II) CISCO의 기만적 허위진술에 대한 책임을 제한하지 않으며, 또는 (III) 적용법에 따라 제외할 수 없는 CISCO의 책임을 제한하지 않습니다.

책임의 면책조항 - 결과적 손해 및 기타 손실의 면제. 미국, 라틴아메리카, 카리브해 또는 캐나다에서 소프트웨어를 구매한 경우 여기에 명시된 보상이 본질적 목적 또는 다른 것과 맞는지 여부와 상관없이 어떤 경우에도, CISCO 및 공급업체는 책임 이론과 상관없이 또는 소프트웨어의 사용 또는 사용 불가로 인해 발생하는지 여부와 상관없이 그리고 CISCO와 공급업체 또는 라이센스 허가업체에서 그러한 손해의 가능성에 대해 조언한 경우라도 수익 손실, 데이터 손실이나 손상, 비즈니스 중단, 자본 손실, 특수, 간접, 결과, 우연 또는 징벌적 손해에 대해 책임지지 않습니다. 일부 국가나 관할 지역에서는 결과적 또는 우연적 손해의 제한 또는 예외를 허용하지 않으므로 위의 제한 사항이 귀하에게 적용되지 않을 수 있습니다.

일본에서 소프트웨어를 구매한 경우 사망이나 개인 상해, 기만적 허위진술로 인해 발생하거나 이와 관련된 책임을 제외하고, 여기에 명시된 보상이 본질적 목적 또는 다른 것과 맞는지 여부와 상관없이 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체는 책임 이론과 상관없이 또는 소프트웨어의 사용 또는 사용 불가로 인해 발생하는지 여부와 상관없이 그리고 CISCO, 승인된 소스, 해당 공급업체 또는 라이센스 허가업체에서 그러한 손해의 가능성에 대해 조언한 경우라도 수익 손실, 데이터 손실이나 손상, 비즈니스 중단, 자본 손실, 특수, 간접, 결과, 우연 또는 징벌적 손해에 대해 책임지지 않습니다.

유럽, 중동, 아프리카, 아시아 또는 오세아니아에서 소프트웨어를 구매한 경우 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체는 계약, 불법 행위(태만 포함)로 인해 발생하든

최종 사용자 라이센스 계약

소프트웨어의 사용 또는 사용 불가로 인해 발생하든 상관없이 그리고 CISCO, 계열사, 임원, 이사, 직원, 에이전트, 공급업체 및 라이센스 허가업체에서 그러한 손해의 가능성에 대해 조언한 경우라도 수익 손실, 데이터 손실이나 손상, 비즈니스 중단, 자본 손실, 특수, 간접, 결과, 우연 또는 징벌적 손해에 대해 책임지지 않습니다. 일부 국가나 관할 지역에서는 결과적 또는 우연적 손해의 제한 또는 예외를 허용하지 않으므로 위의 제한 사항이 귀하에게 충분히 적용되지 않을 수 있습니다. 위의 예외는 다음과 관련하여 발생하는 책임에는 적용되지 않습니다. (I) 사망 또는 개인 상해, (II) 기만적 허위진술, 또는 (III) 적용법에서 제외할 수 없는 조건과 관련된 CISCO의 책임.

고객은 Cisco가 여기에 명시된 보증의 면책조항 및 책임의 제한 사항에 의존하여 가격을 책정하고 계약을 체결했으며, 동일한 내용이 양방 간 위험의 할당을 반영하며(계약 보상이 본질적 목적에 맞지 않고 결과적 손해를 초래할 위험 포함), 동일한 내용이 쌍방 간 거래의 필수적인 기초를 형성함을 인지하고 이에 동의합니다.

규제 법률, 관할지. 승인된 소스에서 수락한 구매 발주서의 주소를 참조하여 미국, 라틴아메리카 또는 카리브해에서 소프트웨어를 취득한 경우 계약 및 보증("보증")은, 법 조항에 충돌이 있더라도, 미국 캘리포니아 주의 법에 따라 제어되고 해석됩니다. 캘리포니아 주 및 연방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 캐나다에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은 법 조항에 충돌이 있더라도, 캐나다 온타리오 주의 법에 따라 제어되고 해석됩니다. 온타리오 주 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 유럽, 중동, 아프리카, 아시아 또는 오세아니아(오스트레일리아 제외)에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 영국의 법에 따라 제어되고 해석됩니다. 영국 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 또한 계약이 영국 법에 의해 제어되는 경우 계약 당사자가 아닌 사람은 Contracts(Rights of Third Parties) Act 1999 조건의 적용 또는 혜택을 받을 수 없습니다. 소프트웨어를 일본에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 일본 법에 따라 제어되고 해석됩니다. 일본 도쿄 지방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 오스트레일리아에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 오스트레일리아 뉴 사우스 웨일스 주의 법에 따라 제어되고 해석됩니다. 뉴 사우스 웨일스 주 및 연방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다. 소프트웨어를 기타 국가에서 취득한 경우 현지 법에서 명시적으로 금지하지 않는 한 계약 및 보증은, 법 조항에 충돌이 있더라도, 미국 캘리포니아 주의 법에 따라 제어되고 해석됩니다. 캘리포니아 주 및 연방 법원은 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 배타적 관할권을 보유합니다.

위에서 언급한 모든 국가에서 당사자들은 국제물품매매계약에 관한 국제연합협약(UN Convention on Contracts for the International Sale of Goods)을 부인합니다. 위의 내용에도 불구하고, 당사자는 자신의 지적 재산권 또는 소유권의 위반 혐의와 관련하여 해당 관할 지역의 법원에 임시 금지 명령 구제를 요청할 수 있습니다. 계약 및 보증의 일부가 무효이거나 집행 불가능한 것으로 판명되는 경우 나머지 조항은 완전한 효력을 유지합니다. 명시적으로 기술된 경우를 제외하고, 본 계약은 소프트웨어 및 문서의 라이센스에 대한 양방 간 완전한 합의를 구성하며, 구매 발주서 등에 포함된 충돌하는 조건 또는 추가 조건에 우선하며, 그러한 모든 조건은 제외됩니다. 본 계약은 영어로 작성되었으며, 양방은 영어 버전이 적용됨에 동의합니다.

Cisco 제품에 적용되는 제품 보증 조항 및 기타 정보는 다음 URL에서 확인할 수 있습니다.

http://www.cisco.com/go/warranty

Cisco Systems Content Security 소프트웨어에 대한 보충 최종 사용자 라이센스 계약

중요: 신중하게 읽어보십시오.

본 보충 최종 사용자 라이센스 계약("SEULA")에는 귀하(여기에서 "귀하"란 귀하 및 귀하가 대표하는 기업체 또는 "회사"를 의미함)와 Cisco 간 최종 사용자 라이센스 계약("EULA")("계약"으로 통칭)에 따라 라이센스가 부여된 소프트웨어에 대한 추가 약관이 포함되어 있습니다. 본 SEULA에 사용되었지만 정의되지 않은 대문자로 표시된 용어는 EULA에서 정의된 의미로 사용됩니다. EULA와 본 SEULA의 약관 사이에 충돌이 있는 경우 본 SEULA의 약관이 우선 적용됩니다.

소프트웨어의 액세스 및 사용에 대해 EULA에 명시된 제한 사항 외에도 귀하는 언제나 본 SEULA에 제공된 약관을 준수할 것에 동의합니다.

소프트웨어를 다운로드, 설치 또는 사용하는 것은 계약에 대한 동의를 의미하며, 귀하 및 귀하가 대표하는 사업체는 계약을 준수해야 합니다. 귀하가 계약의 모든 조건에 동의하지 않는 경우 CISCO는 귀하에게 소프트웨어에 대한 라이센스를 부여하지 않으며, (A) 귀하는 소프트웨어를 다운로드, 설치 또는 사용할 수 없고 (B) 귀하는 전액 환불을 위해 소프트웨어를 반환(개봉하지 않은 CD 패키지 및 서면 자료 포함)할 수 있으며, 소프트웨어 및 서면 자료가 다른 제품의 일부로 제공된 경우 귀하는 전액 환불을 위해 전체 제품을 반환할 수 있습니다. 귀하의 반환 및 환불 권리는 CISCO 또는 승인된 CISCO 리셀러로부터 구매한 지 30일 후에 만료되며, 귀하가 원래 최종 사용자 구매자인 경우에만 적용됩니다.

본 SEULA에서, 귀하가 주문한 제품 이름 및 제품 설명은 Cisco Systems Email Security Appliance("ESA"), Cisco Systems Web Security Appliance("WSA") 및 Cisco Systems Security Management Application("SMA")("Content Security"로 통칭) 및 가상 어플라이언스 해당 제품("소프트웨어") 중 하나입니다.

Cisco AsyncOS for Email

Cisco AsyncOS for Web

Cisco AsyncOS for Management

Cisco Email Anti-Spam, Sophos Anti-Virus

Cisco Email Outbreak Filters

Cloudmark Anti-Spam

Cisco Image Analyzer

McAfee Anti-Virus

Cisco Intelligent Multi-Scan

Cisco Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

최종 사용자 라이센스 계약

Cisco Web Reputation

Sophos Anti-Malware

Webroot Anti-Malware

McAfee Anti-Malware

Cisco Email Reporting

Cisco Email Message Tracking

Cisco Email Centralized Quarantine

Cisco Web Reporting

Cisco Web Policy and Configuration Management

Cisco Advanced Web Security Management with Splunk

Email Encryption for Encryption Appliances

Email Encryption for System Generated Bulk Email

Email Encryption and Public Key Encryption for Encryption Appliances

Large Attachment Handling for Encryption Appliances

Secure Mailbox License for Encryption Appliances

정의

본 SEULA에서는 다음과 같은 의미로 용어가 사용되었습니다.

"회사 서비스"란 회사의 내부 비즈니스 수행을 위해 최종 사용자에게 제공되는 회사의 이메일, 인터넷, 보안 관리 서비스를 의미합니다.

"최종 사용자"란 (1) WSA와 SMA의 경우, 회사에서 회사 서비스를 통해 인터넷 및 SMA에 액세스하도록 승인한 직원, 계약직원 및 기타 에이전트를 의미하고, (2) ESA의 경우, 회사에서 회사 서비스를 통해 이메일 서비스에 액세스하고 사용하도록 승인한 직원, 계약직원 또는 기타 에이전트의 이메일 편지함을 의미합니다.

주문 문서란 회사와 Cisco 또는 회사와 Cisco 리셀러 간 구매 계약, 평가 계약, 베타, 사전 릴리스 계약 또는 유사한 계약, 또는 본 계약에서 허용한 소프트웨어 라이센스에 대한 구매 조건을 포함하여 이와 따라 Cisco에서 수락하는 모든 구매 발주서의 유효한 조건을 의미합니다.

"개인 식별 가능 정보"란 개인의 이름, 사용자 이름, 이메일 주소 및 기타 개인 식별이 가능한 정보를 포함하여(이에 제한되지 않음) 개인을 식별하는 데 사용할 수 있는 정보를 의미합니다.

"서버"란 여러 사용자를 위한 네트워크 리소스를 관리 또는 제공하는 네트워크상의 단일 물리적 컴퓨터 또는 디바이스를 의미합니다.

"서비스"란 Cisco 소프트웨어 구독 서비스를 의미합니다.

"서비스 설명"은 소프트웨어 서브스크립션 지원 서비스에 대한 설명을 의미합니다.
http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html

"텔레메트리 데이터"란 회사 이메일 및 웹 트래픽의 샘플을 의미합니다. 여기에는 이메일 메시지 및 웹 요청 특성에 대한 데이터, 그리고 회사의 Cisco 하드웨어 제품에서 서로 다른 유형의 이메일 메시지 및 웹 요청이 처리된 방식에 대한 정보가 포함됩니다. 텔레메트리 데이터에 포함된 이메일 메시지

메타데이터 및 웹 요청은 개인 식별 가능 정보를 제거하기 위해 알아볼 수 없도록 익명으로 처리됩니다.

"기간"이란 주문 문서에 표시된 대로 귀하가 주문한 소프트웨어 구독의 기간을 의미합니다.

"가상 어플라이언스"란 Cisco Email Security Appliance, Web Security Appliance 및 Security Management Appliance의 가상 버전을 의미합니다.

"가상 머신"이란 자체 운영 체제를 실행할 수 있고 서버처럼 애플리케이션을 실행할 수 있는 소프트웨어 컨테이너를 의미합니다.

추가 라이센스 약관

데이터 수집 조건에 대한 라이센스 허가 및 승낙

소프트웨어 라이센스

소프트웨어 및 문서를 사용함으로써 회사는 본 계약의 조건을 준수할 것에 동의하며, 회사가 본 계약을 준수하는 한 Cisco는 Cisco 하드웨어 제품에서만, 또는 가상 어플라이언스의 경우 최종 사용자에 대한 회사 서비스의 조항과 관련하여 가상 머신에서만 지정된 기간 동안 소프트웨어를 사용하도록, 하위 라이센스 부여나 양도가 불가능한 비배타적이며 세계적인 라이센스를 회사에 부여합니다. 소프트웨어를 사용할 수 있는 라이센스가 부여되는 최종 사용자의 수는 주문 문서에 지정된 최종 사용자의 수로 제한됩니다. 회사 서비스 조항과 관련된 최종 사용자의 수가 주문 문서에 지정된 최종 사용자의 수를 초과하면 회사는 승인된 소스에 연락하여 소프트웨어의 추가 라이센스를 구매해야 합니다. 본 라이센스의 기간과 범위는 주문 문서에 자세히 정의되어 있습니다. 주문 문서는 소프트웨어 라이센스의 조건과 관련하여 EULA에 우선합니다. 여기에서 부여된 라이센스 권리 외에 Cisco, Cisco의 리셀러 또는 개별 라이센스 허가업체는 회사에 어떤 권리, 타이틀 또는 이권도 부여하지 않습니다. 귀하의 소프트웨어 업그레이드 자격은 서비스 설명의 적용을 받습니다. 본 계약과 서비스는 동시에 종료됩니다.

데이터 사용에 대한 동의 및 라이센스

Cisco 개인정보 보호정책(http://www.cisco.com/web/siteassets/legal/privacy.html)에 따라 회사는 Cisco가 회사에서 텔레메트리 데이터를 수집하고 사용하도록 허락하며 해당 권한을 부여합니다. Cisco는 텔레메트리 데이터에서 개인 식별 가능 정보를 수집하거나 사용하지 않습니다. 사용자 환경과 소프트웨어, 그리고 기타 Cisco 보안 제품 및 서비스의 개선을 위해 Cisco는 집계된 익명의 텔레메트리 데이터를 서드파티와 공유할 수 있습니다. 회사는 소프트웨어에서 SenderBase 네트워크 참여를 비활성화하여 언제든지 Cisco의 텔레메트리 데이터 수집 권리를 종료할 수 있습니다. SenderBase 네트워크 참여의 활성화 또는 비활성화에 대한 지침은 소프트웨어 구성 가이드에서 찾아볼 수 있습니다.

기타 권리 및 의무에 대한 설명

Cisco Systems, Inc. 최종 사용자 라이센스 계약, 개인정보 취급방침 및 소프트웨어 구독 지원 서비스의 서비스 설명을 참조하십시오.

최종 사용자 라이센스 계약