Cisco AsyncOS 9.1 for Email 사용 설명서

2016년 2월 2일

Cisco Systems, Inc.
www.cisco.com

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다.
주소, 전화 번호 및 팩스 번호는
Cisco 웹사이트
www.cisco.com/go/offices에서 확인하십시오.

Cisco AsyncOS 9.1 for Email 사용 설명서

목 차

Cisco Email Security 어플라이언스 시작

이 릴리스의 새로운 사항

Cisco AsyncOS 9.1 for Email의 새로운 사항

기능	설명
새로운 기능	
파일 분석 격리 개선	메시지는 이제 분석 판정에 따라 Content Security Management Appliance에 있는 중앙 집중식 파일 분석 격리에서 자동으로 해제되거나 삭제될 수 있습니다.
업데이터 개선	Email Security 어플라이언스에는 다음의 업데이터 개선사항이 포함됩니다. • Email Security 어플라이언스는 어플라이언스가 업데이터 서버와 통신할 때마다 Cisco 업데이터 서버 인증서의 유효성을 확인할 수 있습니다. 업데이트 서버 인증서의 유효성을 확인하도록 어플라이언스 구성, 33-23페이지 항목을 참조하십시오. • 비투명 프록시 서버를 사용 중인 경우, 프록시 인증서를 서명하는 데 사용되는 CA 인증서를 어플라이언스에 추가할 수 있습니다. 이렇게 하면, 어플라이언스가 프록시 서버 통신을 신뢰합니다. 신뢰할 수 있는 프록시 서버 통신을 수행하도록 어플라이언스 구성, 33-24페이지 항목을 참조하십시오.

SSLv3 비활성화	보안을 강화하기 위해 다음 서비스에 대해 SSLv3를 비활성화할 수 있습니다. • 업데이터 • URL 필터링 • 최종 사용자 격리 • LDAP 보안 강화를 위해 SSLv3 비활성화, 33-56페이지 항목을 참조하십시오.
변경된 동작	
제목 크기를 기준으로 메시지 승인 또는 거부	리스너의 전역 설정을 구성하면서 제목의 크기에 따라 메시지를 승인 또는 거부할지를 지정할 수 있습니다. 이 매개변수를 지정하는 경우, 제목 크기가 지정된 한계값을 벗어나지 않는 메시지는 수락되지만 그 밖의 메시지는 거부됩니다. 지침에 대해서는 리스너의 전역 설정 구성, 5-4페이지 항목을 참조하십시오.

Cisco AsyncOS 9.0 for Email의 새로운 사항

기능	설명
새로운 기능	
가상 어플라이언스 개선	현재 다음이 지원됩니다. • ESXi 5.5 및 VMFS 5를 실행하는 가상 어플라이언스의 2TB가 넘는 디스크 공간에 액세스 • ESXi 5.5 하이퍼바이저 • 씬 프로비저닝 또한, 이제 가상 어플라이언스 라이센스와는 별도로 만료되는 기능 키를 사용할 수 있어 평가 기능 키가 가상 어플라이언스에 구축됩니다.
릴리스 및 지원 알림	이제 Cisco 지원팀에서 보내는 소프트웨어 릴리스 및 주요 지원 알림을 수신할 수 있습니다(알림 형식). 알림 수신자 추가, 33-35페이지 항목을 참조하십시오.
S/MIME 보안 서비스	AsyncOS for Email을 통해 조직은 모든 최종 사용자가 고유한 인증서를 소유할 필요 없이 S/MIME를 사용하여 안전하게 통신할 수 있습니다. 조직은 개인 대신 조직을 식별하는 인증서를 사용하여 게이트웨이 수준에서 메시지 서명, 암호화, 확인 및 암호 해독을 처리할 수 있습니다. AsyncOS는 다음의 S/MIME 보안 서비스를 제공합니다. • S/MIME를 사용하여 메시지 서명, 암호화 또는 서명 및 암호화합니다. S/MIME를 사용하여 메시지 서명 또는 암호화 또는 서명 및 암호화, 19-4페이지 항목을 참조하십시오. • S/MIME를 사용하여 메시지 확인, 암호 해독 또는 암호 해독 및 확인합니다. S/MIME를 사용하여 수신 메시지 확인 또는 암호 해독 또는 암호 해독 및 확인, 19-13페이지 항목을 참조하십시오.
Cisco AsyncOS API for Email	Cisco AsyncOS API for Email(또는 AsyncOS API)은 Email Security 어플라이언스 보고서 및 보고 카운터에 안전하고 인증된 액세스를 제공하는 REST(Representational StateTransfer) 기반의 작업 집합입니다. 이 API를 사용하여 Email Security 어플라이언스 보고 데이터를 검색할 수 있습니다. *Cisco AsyncOS API for Email - 시작 가이드*를 참조하십시오.

기능	설명
Advanced Malware Protection 격리	AsyncOS for Email에는 이제 Advanced Malware Protection을 위한 격리가 포함됩니다. 분석을 위해 전송된 첨부 파일이 있는 메시지를 격리하도록 어플라이언스를 구성할 수 있습니다. 분석을 위해 전송된 첨부 파일이 포함된 메시지 격리, 16-9페이지 항목을 참조하십시오.
개선 사항	
Advanced Malware Protection 개선	• 이제 Advanced Malware Protection 기능을 사용하여 아카이브 또는 압축된 이메일 첨부파일에서 악성코드를 탐지할 수 있습니다. 자세한 내용은 아카이브 또는 압축 파일 처리, 16-4페이지 항목을 참조하십시오. 지원되는 아카이브 및 압축된 형식의 목록은 *Cisco 콘텐츠 보안 제품의 Advanced Malware Protection 서비스를 위한 파일 기준* (http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html에서 확인 가능)을 참조하십시오. • 파일 분석 기능을 구성할 때 분석을 위해 전송할 파일 유형을 선택할 수 있습니다. 파일 평판 및 분석 서비스와의 통신을 위한 요건, 16-5페이지 항목을 참조하십시오. • 새로운 유형이 동적으로 추가되었으므로 업로드 가능한 파일 유형 목록이 변경되면 알림을 수신하며 업로드하기 위해 추가된 파일 유형을 선택할 수 있습니다. Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 16-13페이지 항목을 참조하십시오. • 일부 파일 유형 분석을 일시적으로 사용할 수 없는 경우 알림을 수신합니다. Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 16-13페이지 항목을 참조하십시오. • 모든 지원되는 파일 유형 분석이 일시 중단된 이후에 복원되는 경우 알림을 수신합니다. Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 16-13페이지 항목을 참조하십시오. • Cisco AsyncOS for Email에는 새로운 메시지 필터링 작업 (`skip-ampcheck`)이 포함되어 이제 메시지가 시스템에 구성되어 있는 파일 평판 필터링 및 파일 분석을 우회할 수 있습니다. 파일 평판 필터링 및 파일 분석 시스템 우회 작업, 9-71페이지 항목을 참조하십시오.
가상 게이트웨이 개선	이제 모든 Email Security 어플라이언스 모델에서 사용 가능한 가상 게이트웨이 주소의 수는 255개입니다. 가상 게이트웨이™ 기술을 사용하여 모든 호스팅된 도메인에 대한 메일 게이트웨이 구성, 24-56페이지 항목을 참조하십시오.
사용자당 스팸 알림	LDAP 그룹을 기준으로 어떤 사용자가 스팸 알림을 수신할지 지정할 수 있습니다.
URL 필터링을 위한 사용자 지정 가능한 최종 사용자 알림 페이지	URL 필터링에 사용된 최종 사용자 알림 페이지 모양을 사용자 지정하고 로고, 조직 이름, 연락처 정보 등 조직의 브랜드 정보를 표시할 수 있습니다. 최종 사용자 알림 페이지의 모양 사용자 지정, 15-6페이지 항목을 참조하십시오.

기능	설명
디스크 공간 관리 개선	이제 물리적 하드웨어와 ESXi 5.5 및 VMFS 5를 실행하는 가상 어플라이언스에서 2TB가 넘는 디스크 공간을 사용할 수 있습니다. 이제 조직에서 사용하는 기능(스팸 및 시스템 격리, 데이터 보고 및 추적 등)에 따라 어플라이언스에 디스크 공간을 할당할 수 있습니다. 격리 크기에 대한 이전의 제한사항이 제거되었습니다. 가상 어플라이언스의 경우, VMWare 툴을 사용하여 Email Security 어플라이언스 인스턴스에 사용 가능한 디스크 공간을 늘릴 수 있습니다. 자세한 내용은 디스크 공간 관리, 33-15페이지 항목을 참조하십시오.
FIPS 모드에서 구성 가능한 SSL 설정	이제 FIPS 모드에서 CLI의 `sslconfig` 명령을 사용하여 SSL 설정에서 암호 그룹을 구성할 수 있습니다. 자세한 내용은 *Cisco AsyncOS for Email CLI 참조 설명서*를 참조하십시오. **참고** FIPS 모드에서는 서버와 클라이언트 방식을 변경할 수 없습니다.
구성 가능한 SSH 서버 설정	이제 CLI의 `sshconfig` 명령을 사용하여 다음 SSH 서버 설정을 구성할 수 있습니다. • 공개 키 인증 알고리즘 • 암호 알고리즘 • KEX 알고리즘 • MAC 방법 • 최소 서버 키 크기 SSH(Secure Shell) 키 관리, 32-28페이지 항목을 참조하십시오.
FIPS 모드에서 민감한 데이터 암호화	이제 FIPS 모드에서는 다음을 암호화할 수 있습니다. • 어플라이언스의 주요 보안 매개변수 • 어플라이언스의 스왑 공간 이 기능은 어플라이언스의 물리적 보안이 위협받는 경우 무단 액세스 또는 포렌식 공격을 방지하는 데 유용합니다. CLI의 `fipsconfig` 명령을 사용하여 어플라이언스에서 민감한 데이터 암호화 기능을 활성화합니다. FIPS 모드에서 민감한 데이터 암호화, 27-3페이지 항목을 참조하십시오.
구성 파일에서 민감한 데이터 암호화	이제 어플라이언스 구성 파일의 중요한 보안 매개변수를 암호화할 수 있으며 이러한 구성 파일을 내보내기, 이메일 전송 또는 표시할 수 있습니다. 현재 구성 파일 저장 및 내보내기, 33-8페이지 항목을 참조하십시오.
어플라이언스에서 민감한 데이터 영구 삭제	이제 CLI의 다음 명령 중 하나를 사용하여 어플라이언스에서 민감한 데이터(주요 보안 매개변수)를 영구적으로 삭제할 수 있습니다. • `wipedata` • `diagnostic > reload` *Cisco AsyncOS for Email CLI 참조 설명서*를 참조하십시오.
AsyncOS 업데이트 및 업그레이드 보안 강화	보안을 강화하기 위해 AsyncOS는 이제 더욱 강력한 해싱 알고리즘인 SHA-384를 사용하여 수신한 업데이트 및 업그레이드를 확인합니다.

기능	설명
구성 가능한 CLI 세션 시간 제한	이제 비활성화로 인해 AsyncOS에서 사용자가 로그아웃하기 전에 Email Security 어플라이언스의 CLI에 로그인할 수 있는 시간을 지정할 수 있습니다. CLI 세션 시간제한 구성, 32-27페이지 항목을 참조하십시오. **참고** CLI 세션 시간 제한은 SSH(Secure Shell), SCP 및 직접 직렬 연결을 사용하는 연결에만 적용됩니다.
FIPS 모드에서 DKIM 서명 키에 대한 보안 강화	보안을 강화하기 위해 어플라이언스에서 민감한 데이터 암호화 기능이 FIPS 모드에서 활성화된 경우, • 개인 키는 기존의 서명 키를 편집하는 동안 일반 텍스트로 표시되지 않습니다. 기존 서명 키 편집, 20-11페이지 항목을 참조하십시오. • 서명 키는 내보내기 하는 동안 암호화됩니다. 서명 키 내보내기, 20-11페이지 항목을 참조하십시오.
FIPS 모드에서 DSA 호스트 키에 대한 보안 강화	보안을 강화하기 위해 AsyncOS for Email은 FIPS 모드에서 2048비트 DSA 호스트 키를 사용합니다.
데모 인증서에 대한 보안 강화	데모 인증서는 FIPS 모드 및 비FIPS 모드에서 각각 2048비트 및 1024비트인 키를 사용하도록 업데이트되었습니다.
향상된 비밀번호 옵션	사용자 계정을 생성하고 비밀번호를 변경하는 경우, 이제 구성된 요구 사항을 만족하는 비밀번호를 자동으로 생성하는 옵션이 있습니다.
시작 배너	사용자가 SSH, 텔넷, FTP 또는 웹 인터페이스를 통해 어플라이언스에 성공적으로 로그인한 후 시작 배너를 표시하도록 Cisco AsyncOS for Email을 구성할 수 있습니다. 시작 배너를 사용하여 어플라이언스에 대한 내부 보안 정보 또는 모범 사례 지침을 표시할 수 있습니다. 로그인 후 메시지 표시, 32-27페이지 항목을 참조하십시오.
발송 SMTP 인증을 위한 새로운 인증 프로토콜	발송 SMTP 인증은 이제 추가 인증 프로토콜인 LOGIN을 지원합니다.
향상된 스팸 방지 기능	Cisco AsyncOS는 이제 새로운 스팸 캠페인(예: snowshoe 스팸)을 탐지하고 이를 보호하는 향상된 기능을 제공합니다.
수신 또는 발송 정책에 대한 사용자를 선택하는 경우 유연성 향상	이번 릴리스 이전에는 정책의 지정된 값(발신자, 수신자 도메인 또는 LDAP 그룹 이름) 중 하나가 일치하면 수신 또는 발송 정책이 일치합니다. Cisco AsyncOS 9.0 for Email에서는 수신 또는 발송 정책에 대한 사용자를 더욱 유연하게 선택할 수 있습니다. 다음에 해당하는 경우 정책이 일치하도록 설정할 수 있습니다. • 임의의 발신자, 한 명 이상의 지정된 발신자 또는 지정되지 않은 발신자가 보낸 메시지. • 임의의 수신자, 한 명 이상의 지정된 수신자 또는 모든 지정된 수신자 및 지정되지 않은 수신자에게 발송된 메시지. **참고** Cisco AsyncOS 9.0 for Email부터는 최소한 한 명의 발신자 및 수신자를 지정해야 합니다. 메일 정책에 대한 발신자 및 수신자 정의, 10-8페이지 항목을 참조하십시오.
향상된 URL 무해화 기능	URL 무해화를 위해 메시지 및 콘텐츠 필터는 이제 DNS 스푸핑을 처리하고 URL에 있는 "."을 "[.]"로 교체합니다. 예를 들어, 무해화 이후에 www.defangurl.com은 BLOCKEDwww[.]defangurl[.]comBLOCKED가 됩니다.

기능	설명
변경된 동작	
disk_usage 명령은 사용 중단됩니다.	`disk_usage` 하위 명령(`diagnostics`의 하위 명령)은 사용 중단됩니다. 디스크 공간 할당량을 보거나 구성하려면 `diskquotaconfig` 명령을 사용합니다.
어플라이언스에서 지원 사례 열기	어플라이언스에서 지원 사례를 열려면, CCOID 및 지원 계약 번호가 필요합니다. 이전에는 이 정보를 다른 방법을 사용하여 수집했습니다. 또한, 사례를 보다 효율적으로 라우팅하기 위해 기술 및 하위 기술 옵션이 이전 릴리스와 다를 수 있으며 언제든지 변경될 수 있습니다.
비밀번호 변경 옵션의 변경	비밀번호 변경을 적용할 때 다음 로그인 시 또는 지정된 기간 이후에 비밀번호를 변경해야 하는지를 선택할 수 있습니다. 지정된 기간 이후에 비밀번호를 변경하도록 적용하는 경우, 비밀번호가 만료된 후 비밀번호를 재설정하도록 유예 기간을 설정할 수 있습니다. 사용자가 비밀번호를 변경하도록 강제 실행, 32-5페이지 항목을 참조하십시오.
로컬 사용자 계정 및 비밀번호 설정 변경	로컬 사용자 계정 및 비밀번호 설정을 구성할 때, 비밀번호가 만료된 후 비밀번호를 재설정하도록 유예 기간을 설정할 수 있습니다. 제한적인 사용자 계정 및 비밀번호 설정 구성, 32-17페이지 항목을 참조하십시오.
격리를 위한 디스크 공간	이제 **System Administration(시스템 관리) > Disk Management(디스크 관리)** 메뉴에서 격리를 위한 디스크 공간을 할당해야 합니다.
URL 필터링을 위한 새로운 로그	URL 필터링 정보는 다음 로그에 게시됩니다. • 메일 로그(`mail_logs`). URL(URL에 따라 메시지에 수행되는 작업) 검사 결과와 관련된 정보가 이 로그에 게시됩니다. • URL 필터링 로그(`web_client`). 오류, 시간 제한, 네트워크 문제 등과 관련된 정보가 URL 조회를 시도할 때 이 로그에 게시됩니다.
더 엄격한 비밀번호 규칙	더 엄격한 비밀번호 규칙이 시스템 설정 마법사를 실행한 후 바로 적용됩니다.

추가 정보 확인 위치

Cisco는 어플라이언스에 대해 자세히 알아볼 수 있도록 다음의 리소스를 제공합니다.

문서

오른쪽 상단에 있는 도움말 및 지원을 클릭하면 어플라이언스 GUI에서 직접 사용 설명서의 온라인 도움말 버전에 액세스할 수 있습니다.

Cisco Email Security 어플라이언스에 대한 문서에는 다음 문서 및 책이 포함되어 있습니다.

- 릴리스 정보
- Email Security 어플라이언스에 대한 빠른 시작 설명서
- *Cisco AsyncOS for Email 사용 설명서*(본 책)
- *Cisco Content Security Virtual Appliance 설치 설명서*
- *Cisco AsyncOS CLI 참조 설명서*
- *Cisco AsyncOS API for Email - 시작 가이드*

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

Cisco Content Security 제품용 문서	장소
하드웨어 및 가상 어플라이언스	이 표에서 해당 제품을 참조하십시오.
Cisco Email Security	http://www.cisco.com/c/en/us/support/security/content-security-management-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/email-security-appliance/tsd-products-support-series-home.html
Cisco Content Security Appliance에 대한 CLI 참조 설명서	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-encryption/tsd-products-support-series-home.html

교육

교육에 대한 자세한 내용은 다음에서 확인할 수 있습니다.

- http://www.cisco.com/web/learning/le31/email_sec/index.html
- http://www.cisco.com/web/learning/training-index.html

Cisco 알림 서비스

보안 권고 사항, 현장 통지, 판매 중단 및 지원 종료 안내와 소프트웨어 업데이트 및 알려진 문제점 정보 등 Cisco Content Security Appliance와 관련된 알림을 수신하려면 등록하십시오.

수신할 정보의 알림 빈도 및 유형 등의 옵션을 지정할 수 있습니다. 사용하는 제품마다 알림을 별도로 등록해야 합니다.

등록하려면 https://sso.cisco.com/autho/forms/CDClogin.html을 방문하십시오.

Cisco.com 계정이 필요합니다. 계정이 없는 경우 Cisco 계정 등록, 1-9페이지 항목을 참조하십시오.

기술 자료

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

2단계 이름에서 **TechNotes**가 있는 링크를 검색하십시오.

Cisco 지원 커뮤니티

Cisco 지원 커뮤니티는 Cisco 고객, 파트너 및 직원을 위해 마련된 온라인 포럼입니다. 이 커뮤니티에서는 일반적인 이메일 및 웹 보안 문제뿐만 아니라 특정한 Cisco 제품에 대한 기술 정보를 논의할 수 있습니다. 질문을 하거나 다른 Cisco 사용자와 정보를 공유하기 위해 포럼에 주제를 게시할 수 있습니다.

다음 URL의 고객 지원 포털에 있는 Cisco 지원 커뮤니티를 방문하십시오.

- 이메일 보안 및 관련된 관리 업무:
  https://supportforums.cisco.com/community/netpro/security/email
- 웹 보안 및 관련된 관리 업무:
  https://supportforums.cisco.com/community/netpro/security/web

Cisco 고객 지원

지원을 얻으려면 다음을 이용할 수 있습니다.

미국: 1 (408) 526-7209 또는 1 (800) 553-2447(무료 전화)로 문의

전 세계: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

지원 사이트: http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

리셀러 또는 다른 공급업체를 통해 지원 서비스를 구매한 경우, 제품 지원 문제에 대한 문의는 해당 업체에 직접 하십시오.

타사 지원업체

Cisco AsyncOS에 포함되는 일부 소프트웨어는 FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc. 및 기타 타사 지원업체의 소프트웨어 라이센스 계약 약관, 통지 및 조건에 따라 배포되며 이러한 모든 약관과 조건은 Cisco 라이센스 계약에 통합됩니다.

이 계약에 대한 전체 내용은 다음에서 확인할 수 있습니다.

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

Cisco AsyncOS에 포함되는 소프트웨어 일부는 Tobi Oetiker가 명시적으로 서면 동의한 RRDtool을 기반으로 합니다.

이 문서의 일부는 Dell Computer Corporation의 허가 하에 복제되었습니다. 이 문서의 일부는 McAfee, Inc.의 허가 하에 복제되었습니다. 이 문서의 일부는 Sophos Plc.의 허가 하에 복제되었습니다.

Cisco 의견 보내기

Cisco 기술 발행팀은 제품 문서의 품질을 개선하고자 합니다. 의견이나 제안사항이 있으시면 언제든지 보내주십시오. 다음 이메일 주소로 의견을 보내주세요.

contentsecuritydocs@cisco.com

메시지 제목에 제품 이름, 릴리스 번호 및 문서 발행일이 포함해 주십시오.

Cisco 계정 등록

Cisco.com에 있는 많은 리소스에 액세스하려면 Cisco 계정이 필요합니다.

Cisco.com 사용자 ID가 없는 경우, https://tools.cisco.com/IDREG/guestRegistration.do에서 등록할 수 있습니다.

관련 주제

- Cisco 알림 서비스, 1-7페이지
- 기술 자료, 1-8페이지

Cisco Email Security 어플라이언스 개요

Cisco AsyncOS™ 운영 체제는 다음 기능을 제공합니다.

- **안티스팸** - SenderBase 평판 필터와 Cisco Anti-Spam을 통합하여 고유한 다중 계층 접근 방식을 사용하여 게이트웨이에서 안티스팸 기능을 제공합니다.
- **안티바이러스** - 게이트웨이에서 Sophos와 McAfee 안티바이러스 검사 엔진을 사용합니다.
- **신종 바이러스 필터(Outbreak Filter)™** 기능 - 신종 바이러스, 스캠 및 피싱 침투를 방지하는 Cisco의 고유한 예방 보호 기능을 통해 새로운 업데이트가 적용될 때까지 위험한 메시지를 격리하여 새로운 메시지 위협에 대한 취약성이 향상되었습니다.
- **정책, 바이러스 및 침투 격리** - 관리자가 평가하도록 의심스러운 메시지를 저장하기 위한 안전한 장소를 제공합니다.
- **스팸 격리** - 온박스(On-box)를 설정 또는 해제하여 격리된 스팸 및 의심스러운 스팸에 대한 최종 사용자 액세스를 제공합니다.
- **이메일 인증** - Cisco AsyncOS는 다양한 형태의 이메일 인증을 지원합니다. 예를 들어, SPF(Sender Policy Framework), SIDF(Sender ID Framework) 및 수신 메일에 대한 DKIM(DomainKeys Identified Mail) 확인뿐만 아니라 발송 메일의 DomainKeys 및 DKIM 서명 등이 있습니다.
- **Cisco 이메일 암호화** - 발송 메일을 암호화하여 HIPAA, GLBA 및 유사한 규정에 대응합니다. 이를 위해, Email Security 어플라이언스에서 암호화 정책을 구성하고 로컬 키 서버 또는 호스트 키 서비스를 사용하여 메시지를 암호화합니다.
- **Email Security Manager** - 어플라이언스에서 모든 이메일 보안 서비스 및 애플리케이션을 관리하기 위한 포괄적인 단일 대시보드입니다. Email Security Manager는 사용자 그룹에 기반하여 이메일 보안을 적용할 수 있으며 고유한 인바운드 및 아웃바운드 정책을 통해 Cisco 평판 필터, 신종 바이러스 필터(Outbreak Filter), 안티스팸, 안티바이러스 및 이메일 콘텐츠 정책을 관리할 수 있습니다.
- **온박스(On-box) 격리 영역** - 이메일 정책을 위반하는 메시지를 보류합니다. 격리는 신종 바이러스 필터(Outbreak Filter) 기능과 원활하게 상호 작용합니다.

- **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 도메인에 기반한 인바운드 발신자를 제어합니다.
- **메시지 필터링** - 광범위한 메시지 필터링 기술을 활용하면 회사 정책을 적용하고 회사 인프라에 메시지가 들어오거나 나갈 때 특정 메시지에 작업을 수행할 수 있습니다. 필터 규칙에 따라 메시지 또는 첨부 파일 콘텐츠, 네트워크 정보, 메시지 봉투, 메시지 헤더 또는 메시지 본문을 기준으로 메시지를 식별합니다. 필터 작업을 통해 메시지를 삭제, 바운스, 아카이브, BCC(숨은 참조) 또는 변경하거나 알림을 생성할 수 있습니다.
- **Transport Layer Security(전송 계층 보안)에서 보안 SMTP를 통한 메시지 암호화** - 회사 인프라 및 기타 신뢰할 수 있는 호스트 사이를 이동하는 메시지를 암호화합니다.
- **가상 게이트웨이™** - 이 기술을 활용하면 Email Security 어플라이언스가 단일 서버 내에서 여러 이메일 게이트웨이로 작동할 수 있어 다양한 소스 또는 캠페인의 이메일을 분할하여 개별 IP 주소를 통해 전송할 수 있습니다. 이렇게 하면 단일 IP 주소에 영향을 미치는 전달 문제가 다른 주소에는 영향을 미치지 않습니다.

AsyncOS for Email은 RFC 2821규격 SMTP(Simple Mail Transfer Protocol)를 지원하여 메시지를 수락 및 전달합니다.

대부분의 보고, 모니터링 및 구성 명령은 HTTP 또는 HTTPS를 통한 웹 기반 GUI를 통해 사용할 수 있습니다. 또한 SSH(Secure Shell), 텔넷 또는 직접 직렬 연결을 통해 사용자가 액세스하는 인터랙티브 CLI(Command Line Interface)가 시스템에 제공됩니다.

또한 보안 관리 어플라이언스를 설치하여 여러 Email Security 어플라이언스에 대한 보고, 추적 및 격리 관리를 통합할 수 있습니다.

관련 주제

- 지원되는 언어, 1-10페이지

지원되는 언어

AsyncOS는 다음 언어로 GUI 및 CLI를 제공합니다.

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

2 장

어플라이언스 액세스

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 *CLI에서만* 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.

- Firefox 3.6
- Windows XP 및 Vista: Internet Explorer 7 및 8
- Windows 7: Internet Explorer 8 및 9, Google Chrome, Firefox 4
- Mac OS X: Safari 4 이상, Firefox 4

어플라이언스를 변경할 때 여러 브라우저 창 또는 탭을 동시에 사용하면 안 됩니다. GUI와 CLI 세션을 동시에 사용하면 안 됩니다. 이러한 경우 예기치 못한 동작이 발생할 수 있으므로 현재 이 기능은 지원되지 않습니다.

인터페이스의 일부 버튼 또는 링크를 사용하면 창이 추가로 열리므로 GUI를 사용하려면 브라우저의 팝업 차단 설정을 구성해야 합니다.

GUI 액세스

새 시스템에서 GUI에 액세스하려면 다음 URL을 확인합니다.

http://192.168.42.42

로그인 페이지가 표시되면 기본 사용자 이름과 비밀번호를 사용하여 시스템에 로그인합니다.

관련 주제

- 공장 기본 사용자 이름 및 비밀번호, 2-2페이지
- 중앙 집중식 관리, 2-2페이지

공장 기본 사용자 이름 및 비밀번호

- 사용자 이름: **admin**
- 비밀번호: **ironport**

예를 들면 다음과 같습니다.

그림 2-1 로그인 화면

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 인터페이스의 HTTPS가 활성화된 경우(또는 HTTP 요청이 보안 서비스로 리디렉션되지 *않는* 경우) "`https://`" 접두사를 사용하여 GUI에 액세스할 수 있습니다.

관련 주제

- 사용자 추가, 32-4페이지

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, 39-15페이지 항목을 참조하십시오.

구성 설정 변경

구성 변경

이메일 작업이 정상적으로 처리되는 동안 구성을 변경할 수 있습니다.

변경사항 커밋 또는 취소

대부분의 구성 변경사항을 저장해야 합니다.

변경사항이 커밋 보류 중인 경우 Commit Changes(변경사항 커밋) 버튼이 주황색으로 바뀝니다.

그림 2-2 Commit Changes(변경사항 커밋) 버튼

이러한 변경사항을 지우거나 커밋하려면 **Commit Changes(변경사항 커밋)**를 클릭합니다.

관련 주제

- 구성 변경사항 지우기, 2-8페이지

명령줄 인터페이스(CLI)

명령줄 인터페이스는 IP 인터페이스의 SSH 또는 텔넷을 통해(해당 서비스가 활성화된 경우) 액세스하거나 시리얼 포트에서 터미널 에뮬레이션 소프트웨어를 통해 액세스할 수 있습니다. 기본적으로 SSH 및 텔넷은 관리 포트에서 구성합니다. `interfaceconfig` 명령를 사용하여 이러한 서비스를 비활성화할 수 있습니다.

특정 CLI 명령에 대한 자세한 내용은 *Cisco AsyncOS CLI 참조 설명서* 항목을 참조하십시오.

관련 주제

- 명령줄 인터페이스 규칙, 2-3페이지
- 범용 CLI 명령, 2-7페이지

명령줄 인터페이스 규칙

이 섹션에서는 AsyncOS CLI 규칙에 대해 설명합니다.

명령 프롬프트

최상위 명령 프롬프트는 정규화된 호스트 이름, > 기호, 공백 순으로 구성됩니다. 예를 들면 다음과 같습니다.

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

어플라이언스가 클러스터 일부로 구성된 경우 CLI 프롬프트가 현재 모드가 표시되도록 변경됩니다. 예를 들면 다음과 같습니다.

```
(Cluster Americas) >
```

또는

```
(Machine losangeles.example.com) >
```

자세한 내용은 중앙 집중식 관리, 2-2페이지 항목을 참조하십시오.

명령을 실행하면 CLI는 사용자 입력을 요청합니다. CLI에서 사용자 입력을 요청할 때 명령 프롬프트에는 대괄호([])와 > 기호로 구성된 기본 입력이 표시됩니다. 기본 입력이 없는 경우 빈 명령 프롬프트가 표시됩니다.

예를 들면 다음과 같습니다.

```
Please create a fully-qualified hostname for this Gateway

(Ex: "mail3.example.com"):
[]> mail3.example.com
```

기본 설정이 있는 경우 설정은 명령 프롬프트 괄호 안에 표시됩니다. 예를 들면 다음과 같습니다.

```
Ethernet interface:
1. Data 1
2. Data 2
3. Management
[1]> 1
```

기본 설정이 표시된 경우 Return을 입력하는 것은 기본값을 입력하는 것과 동일합니다.

```
Ethernet interface:
1. Data 1
2. Data 2
3. Management
[1]> (type Return)
```

명령 구문

인터랙티브 모드에서 동작하는 경우 CLI 명령 구문은 공백과 인수 또는 매개변수 없이 단일 명령으로 구성됩니다. 예를 들면 다음과 같습니다.

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

목록 선택

입력 선택사항이 여러 개 있는 경우 일부 명령에서는 번호가 매겨진 목록을 사용합니다. 프롬프트에 선택할 번호를 입력합니다.

예를 들면 다음과 같습니다.

```
Log level:
1. Error
2. Warning
3. Information
4. Debug
5. Trace
[3]> 3
```

Yes/No 쿼리

Yes 또는 No 옵션이 제공되는 경우 질문과 함께 기본값이 괄호 안에 표시됩니다. **Y**, **N** 또는 **Yes**, **No**로 답할 수 있습니다. 대소문자는 구분하지 않습니다.

예를 들면 다음과 같습니다.

```
Do you want to enable FTP on this interface?  [Y]> n
```

하위 명령

일부 명령에는 하위 명령이 있습니다. 하위 명령에는 NEW, EDIT 및 DELETE와 같은 지시문이 포함됩니다. EDIT 및 DELETE의 경우 이전에 시스템에 구성한 레코드 목록을 제공합니다.

예를 들면 다음과 같습니다.

```
mail3.example.com> interfaceconfig


Currently configured interfaces:

1. Management (192.168.42.42/24: mail3.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.

[]>
```

하위 명령에서 빈 프롬프트에 Enter 또는 Return을 입력하면 기본 명령으로 돌아갑니다.

이스케이프

하위 명령에서 언제든지 Ctrl-C 키보드 바로 가기를 사용하여 해당 명령을 종료한 후 즉시 CLI의 최상위 레벨로 돌아갈 수 있습니다.

기록

CLI는 세션 중에 입력한 모든 명령의 기록을 보관합니다. 키보드의 위쪽 및 아래쪽 화살표 키를 사용하거나 Ctrl-P 및 Ctrl-N 키 조합을 사용하여 실행되고 있는 최근에 사용한 명령의 목록을 스크롤할 수 있습니다.

```
mail3.example.com> (type the Up arrow key)


mail3.example.com> interfaceconfig (type the Up arrow key)


mail3.example.com> topin (type the Down arrow key)
```

명령 완료

Cisco AsyncOS CLI는 명령 완성 기능을 지원합니다. 일부 명령의 처음 몇 글자를 입력하고 Tab 키를 누르면 CLI가 고유 명령에 해당하는 문자열을 완성합니다. 입력하는 글자가 명령과 일치하지 않는 경우, CLI는 범위를 "줄입니다". 예를 들면 다음과 같습니다.

```
mail3.example.com> set (type the Tab key)
setgateway, sethostname, settime, settz
mail3.example.com> seth (typing the Tab again completes the entry with sethostname)
```

CLI의 기록 및 파일 완성 기능을 확인하려면 Enter 또는 Return을 입력하여 해당 명령을 호출해야 합니다.

구성 변경

이메일 작업이 정상적으로 진행되는 동안 Cisco AsyncOS의 구성을 변경할 수 있습니다.

구성 변경사항은 다음을 완료할 때까지 적용되지 않습니다.

1. 명령 프롬프트에서 `commit` 명령을 실행합니다.
2. `commit` 명령에 필요한 명령을 입력합니다.
3. CLI에서 `commit` 절차에 대한 확인을 수신합니다.

커밋되지 않은 구성 변경사항은 기록되지만, commit 명령을 실행할 때까지 적용되지 않습니다.

참고 AsyncOS의 모든 명령에 commit 명령을 실행할 필요는 없습니다. 변경사항을 적용하기 위해 commit을 실행해야 할 명령에 대한 요약 정보는 *Cisco AsyncOS CLI 참조 설명서*를 참조하십시오.

CLI 세션을 종료하거나 시스템을 종료하거나, 재부팅을 하거나 오류가 발생하거나 clear 명령을 실행하면 아직 커밋되지 않은 변경사항은 지워집니다.

범용 CLI 명령

이 섹션에서는 변경사항 커밋 및 지우기, 도움말 찾기, 명령줄 인터페이스 종료에 사용하는 명령에 대해 설명합니다.

- 구성 변경사항 커밋, 2-7페이지
- 구성 변경사항 지우기, 2-8페이지
- 구성 변경사항 롤백, 2-8페이지
- 명령줄 인터페이스 세션 종료, 2-9페이지
- 명령줄 인터페이스에서 도움말 찾기, 2-9페이지

구성 변경사항 커밋

commit 명령은 어플라이언스의 구성 변경사항을 저장하는 필수 명령입니다. 구성 변경사항의 대부분이 commit 명령을 입력할 때까지 적용되지 않습니다. (일부 명령의 경우 변경사항을 적용하기 위해 commit 명령을 사용하지 않아도 됩니다.) commit 명령은 Cisco AsyncOS에 마지막 commit 명령 또는 마지막 clear 명령이 실행된 이후의 구성 변경사항을 적용합니다. 최대 255자의 주석을 포함할 수 있습니다. 타임스탬프로 확인을 받을 때까지 변경사항은 커밋되지 않습니다.

commit 명령 다음에 주석을 입력하는 것은 선택 사항입니다.

```
mail3.example.com> commit


Please enter some comments describing your changes:


[]> Changed "psinet" IP Interface to a different IP address


Do you want to save the current configuration for rollback? [Y]> n

Changes committed: Fri May 23 11:42:12 2014 GMT
```

참고 변경사항을 성공적으로 커밋하려면 최상위 명령 프롬프트에서 수행해야 합니다. 빈 프롬프트에 Return을 입력하면 명령줄 계층에서 한 수준 위로 이동합니다 .

구성 변경사항 지우기

clear 명령은 Cisco AsyncOS에 마지막 commit 또는 clear 명령을 실행한 이후의 변경사항을 지웁니다.

```
mail3.example.com> clear


Are you sure you want to clear all changes since the last commit? [Y]> y


Changes cleared: Mon Jan 01 12:00:01 2003

mail3.example.com>
```

구성 변경사항 롤백

rollbackconfig 명령은 커밋된 구성 중 마지막 구성 10개를 나열하여 롤백하려는 항목을 선택할 수 있습니다.

관리자만 이 명령을 사용할 수 있습니다.

참고 클러스터된 어플라이언스에서는 이 명령이 동작하지 않습니다. 어플라이언스를 이전 AsyncOS 버전으로 되돌린 경우 어플라이언스에서 구성이 복원되지 않습니다.

```
mail.example.com> rollbackconfig


Previous Commits :

   Committed On               User             Description

 --------------------------------------------------------------------------------

1. Wed Sep 19 22:03:10 2012     admin            Enabled anti-spam

2. Wed Sep 19 21:51:14 2012     admin           Updated envelope encry...

3. Wed Sep 19 18:50:41 2012     admin


Enter the number of the config to revert to.

[]> 1
```

```
Reverted to Wed Sep 19 18:50:41 2012     admin

Do you want to commit this configuration now? [N]> y


Committed the changes successfully
```

명령줄 인터페이스 세션 종료

quit 명령을 사용하면 CLI 애플리케이션에서 로그아웃됩니다. 커밋되지 않은 구성 변경사항은 지워집니다. 이메일 작업에는 quit 명령이 적용되지 않습니다. 로그아웃 정보는 로그 파일에 기록됩니다. (exit 명령은 quit 명령과 동일합니다.)

```
mail3.example.com> quit


Configuration changes entered but not committed.  Exiting will lose changes.

Type 'commit' at the command prompt to commit changes.

Are you sure you wish to exit?  [N]> Y
```

명령줄 인터페이스에서 도움말 찾기

help 명령은 사용 가능한 모든 CLI 명령을 나열하고 각 명령에 대한 간략한 설명을 제공합니다. help 명령은 명령 프롬프트에 help 또는 물음표 하나(?)를 입력하여 호출할 수 있습니다.

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

3 장

설정 및 설치

설치 계획

계획 결정에 영향을 미치는 정보 검토

- 가상 Email Security 어플라이언스를 구성할 경우 이 장을 계속하기 전에 *Cisco Content Security Virtual Appliance 설치 설명서*를 참조하십시오.
- M-Series Content Security Management Appliance를 구성할 경우에는 42 장, "Cisco Content Security Management Appliance에서 서비스 중앙 집중화"를 참조하십시오.
- 일부 특성 및 기능이 인프라 내의 어플라이언스 배치에 영향을 미칠 수 있으므로 Cisco에서는 설치 전에 4 장, "이메일 파이프라인 이해"를 참조할 것을 권장합니다.

네트워크 경계에 **Email Security** 어플라이언스를 배치하기 위한 계획

Email Security 어플라이언스는 SMTP 게이트웨이 역할을 하도록 설계되었으며 MX(메일 교환)라고도 합니다. 최상의 결과를 얻기 위해서 일부 기능은 어플라이언스가 인터넷에 직접 액세스하여 메일을 발신 및 수신할 수 있는 IP 주소(즉, 외부 IP 주소)를 사용하는 첫 번째 머신일 경우에만 작동합니다.

수신자별 평판 필터, 안티스팸, 안티바이러스, 신종 바이러스 필터(Outbreak Filter) 기능(SenderBase Reputation Service, 6-1페이지, IronPort Anti-Spam 필터링, 13-3페이지, Sophos Anti-Virus 필터링, 12-2페이지 및 신종 바이러스 필터(Outbreak Filter), 14-1페이지 참조)은 인터넷

및 내부 네트워크의 *직접 메시지 흐름*과 함께 작동할 수 있도록 고안되었습니다. 엔터프라이즈로 들어가거나 엔터프라이즈에서 나오는 모든 이메일 트래픽에 대해 정책을 시행하도록 어플라이언스를 구성할 수 있습니다(연결할 수 있는 호스트 정의 개요, 7-1페이지).

Email Security 어플라이언스가 공용 인터넷을 통해 액세스 가능하며 이메일 인프라의 "첫 번째 홉"인지 확인합니다. 다른 MTA가 네트워크의 경계에 배치되고 모든 외부 연결을 처리하도록 허용하면 Email Security 어플라이언스가 발신자의 IP 주소를 파악할 수 없습니다. 발신자의 IP 주소는 메일 흐름 모니터링에서 발신자를 식별하고 구별하거나, SenderBase Reputation Service에 SBRS(SenderBase Reputation 점수)를 쿼리하거나, 안티스팸 및 신종 바이러스 필터(Outbreak Filter) 기능의 효율성을 높이는 데 필요합니다.

참고 어플라이언스를 인터넷에서 이메일을 수신하는 *첫 번째* 머신으로 구성할 수 없는 경우에도 어플라이언스에서 지원되는 일부 보안 서비스를 실행할 수 있습니다. 자세한 내용은 수신 릴레이 사용 배포 환경에서 발신자 IP 주소 확인, 13-15페이지를 참고하십시오.

Email Security 어플라이언스를 SMTP 게이트웨이로 사용할 경우:

- 메일 흐름 모니터링 기능(28 장, "이메일 보안 모니터링 사용" 참조)을 사용하여 내부 및 외부 발신자가 엔터프라이즈에 전송한 트래픽을 완전히 파악할 수 있습니다.
- 라우팅, 앨리어싱, 마스커레이드에 대한 LDAP 쿼리(25 장, "LDAP 쿼리" 참조)를 통해 디렉토리 인프라를 통합하고 업데이트를 더 간단하게 수행할 수 있습니다.
- 별칭 테이블(별칭 테이블 생성, 24-7페이지 참조), 도메인 기반 라우팅(도메인 맵 기능, 24-27페이지) 및 마스커레이드(마스커레이드 구성, 24-15페이지)와 같은 친숙한 툴을 사용해 오픈 소스 MTA 전환을 더 쉽게 수행할 수 있습니다.

DNS에 Email Security 어플라이언스 등록

악성 이메일 발신자가 새로운 희생자를 찾기 위해 공용 DNS 레코드를 적극적으로 검색합니다. 안티스팸, 신종 바이러스 필터(Outbreak Filter), McAfee 안티바이러스 및 Sophos 안티바이러스의 모든 기능을 활용하려면 Email Security 어플라이언스가 DNS에 등록되었는지 확인합니다.

어플라이언스를 DNS에 등록하려면 어플라이언스를 해당 IP 주소에 매핑하는 A 레코드와 공용 도메인을 어플라이언스의 호스트 이름에 매핑하는 MX 레코드를 생성합니다. Email Security 어플라이언스를 도메인의 기본 또는 백업 MTA로 보급하려면 MX 레코드의 우선순위를 지정해야 합니다.

다음 예제에서는 MX 레코드의 우선순위 값(20)이 더 높으므로 Email Security 어플라이언스(ironport.example.com)가 도메인 example.com의 백업 MTA입니다. 다시 말해서, 숫자 값이 높을수록 MTA의 우선순위가 낮아집니다.

```
$ 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
```

DNS에 Email Security 어플라이언스를 등록하면 MX 레코드에 지정한 우선순위에 관계없이 스팸 공격을 유발하게 됩니다. 그러나 바이러스 공격이 백업 MTA를 대상으로 하는 경우는 드뭅니다. 이러한 점을 고려할 때 안티바이러스 엔진이 최대한 활용되고 있는지 평가하려면 MX 레코드의 우선순위를 나머지 MTA와 같거나 그보다 높게 지정하도록 Email Security 어플라이언스를 구성합니다.

설치 시나리오

여러 가지 방법을 이용해 Email Security 어플라이언스를 기존 네트워크 인프라에 설치할 수 있습니다.

대부분의 고객 네트워크 구성은 다음과 같은 시나리오에 해당됩니다. 네트워크 구성이 크게 다르고 설치 지원 계획을 세우려면 Cisco 고객 지원(Cisco 고객 지원, 1-8페이지 참조)에 문의하십시오.

구성 개요

다음 그림에는 엔터프라이즈 네트워크 환경에서 Email Security 어플라이언스를 배치하는 일반적인 방식이 나와 있습니다.

일부 시나리오에서는 Email Security 어플라이언스가 네트워크 "DMZ" 내에 상주하며 이 경우 추가 방화벽은 Email Security 어플라이언스와 그룹웨어 서버 사이에 배치됩니다.

다음과 같은 네트워크 시나리오를 설명합니다.

- 방화벽 뒤: 2개의 리스너 구성(그림 3-1(3-6페이지))

현재 인프라에 가장 적합한 구성을 선택합니다. 그런 후에 다음 섹션인 시스템 설정 준비, 3-8페이지로 이동합니다.

수신

- 수신 메일은 사용자가 지정한 로컬 도메인에서 수락됩니다.
- 다른 모든 도메인은 거부됩니다.
- 외부 시스템이 Email Security 어플라이언스에 직접 연결하여 로컬 도메인의 이메일을 전송하고, Email Security 어플라이언스가 SMTP 경로를 통해 메일을 해당 그룹웨어 서버(예: Exchange™, Groupwise™, Domino™)로 전달합니다. (로컬 도메인의 이메일 라우팅, 24-1페이지를 참조하십시오.)

발송

- 내부 사용자가 보낸 발송 메일은 그룹웨어 서버를 통해 Email Security 어플라이언스에 라우팅됩니다.
- Email Security 어플라이언스가 사설 리스너의 Host Access Table에 있는 설정에 따라 아웃바운드 이메일을 수락합니다. (자세한 내용은 리스너 작업, 5-2페이지를 참조하십시오.)

이더넷 인터페이스

이러한 구성에는 Email Security 어플라이언스에서 사용 가능한 이더넷 인터페이스 중 1개만 필요합니다. 그러나 2개의 이더넷 인터페이스를 구성하고 외부 인터넷 네트워크 연결에서 내부 네트워크를 분리할 수 있습니다.

사용 가능한 인터페이스에 여러 개의 IP 주소를 할당하는 방법에 대한 자세한 내용은 가상 게이트웨이™ 기술을 사용하여 모든 호스팅된 도메인에 대한 메일 게이트웨이 구성, 24-56페이지 및 부록 B, "네트워크 및 IP 주소 할당"을 참조하십시오.

하드웨어 포트

하드웨어 어플라이언스의 포트 수 및 유형은 모델에 따라 다릅니다.

포트	유형	C170	C370	C670	X1070	C380	C680
관리	이더넷	0	1	1	1	1	1
데이터	이더넷	2*	3	3	3	3	3
콘솔	일련번호	9핀	9핀	9핀	9핀	RJ-45	RJ-45
RPC(원격 전력 관리)	이더넷	아니요	아니요	아니요	아니요	다	다

* 전용 관리 포트가 없는 어플라이언스의 경우 데이터1 포트를 관리용 포트로 사용하십시오.

포트에 대한 자세한 내용은 해당 어플라이언스 모델의 *하드웨어 설치 설명서*를 참조하십시오.

관련 주제

- 네트워크 인터페이스 구성, 3-17페이지
- 직렬 연결을 통한 Email Security 어플라이언스 액세스, A-5페이지
- 원격 전력 관리 활성화, 33-29페이지

고급 구성

그림 3-1 및 그림 3-2에 표시된 구성 외에 다음과 같은 구성도 할 수 있습니다.

- 중앙 집중식 관리 기능을 사용하는 여러 Email Security 어플라이언스. 39 장, "클러스터를 사용한 중앙 집중식 관리"를 참조하십시오.
- Email Security 어플라이언스에서 NIC 페어링 기능을 사용해 2개의 이더넷 인터페이스를 "티밍"하여 네트워크 인터페이스 카드 수준에서 이중화. 37 장, "고급 네트워크 구성"을 참조하십시오.

방화벽 설정(NAT, 포트)

SMTP 및 DNS 서비스는 인터넷에 액세스할 수 있어야 합니다. 다른 서비스는 개방형 방화벽 포트가 필요할 수도 있습니다. 자세한 내용은 부록 D, "방화벽 정보"를 참조하십시오.

Email Security 어플라이언스를 네트워크에 물리적으로 연결

구성 시나리오

Email Security 어플라이언스의 일반적인 구성 시나리오는 다음과 같습니다.

- **인터페이스** - 대부분의 네트워크 환경에는 Email Security 어플라이언스에서 사용 가능한 3개의 이더넷 인터페이스 중 1개만 필요합니다. 그러나 2개의 이더넷 인터페이스를 구성하고 외부 인터넷 네트워크 연결에서 내부 네트워크를 분리할 수 있습니다.
- **공용 리스너(수신 이메일)** - 공용 리스너가 여러 외부 호스트의 연결을 수신하고 메시지를 제한된 수의 내부 그룹웨어 서버에 전달합니다.
  - HAT(Host Access Table)의 설정에 따라 외부 메일 호스트의 연결을 수락합니다. 기본적으로 HAT는 모든 외부 메일 호스트의 연결을 수락하도록 구성되어 있습니다.
  - RAT(Recipient Access Table)에 지정된 로컬 도메인에 대해 전송된 경우에만 수신 메일을 수락합니다. 다른 모든 도메인은 거부됩니다.
  - SMTP 경로에 정의된 대로 메일을 해당 내부 그룹웨어 서버에 전달합니다.
- **사설 리스너(발송 이메일)** - 사설 리스너는 제한된 수의 내부 그룹웨어 서버의 연결을 수신하고 메시지를 여러 외부 메일 호스트에 전달합니다.
  - 내부 그룹웨어 서버는 발송 메일을 Cisco C-Series 또는 X-Series 어플라이언스로 라우팅하도록 구성되어 있습니다.
  - Email Security 어플라이언스는 HAT의 설정에 따라 내부 그룹웨어 서버의 연결을 수락합니다. 기본적으로 HAT는 모든 내부 메일 호스트의 연결을 전달하도록 구성되어 있습니다.

관련 주제

- 수신 및 발송 메일 분리, 3-5페이지

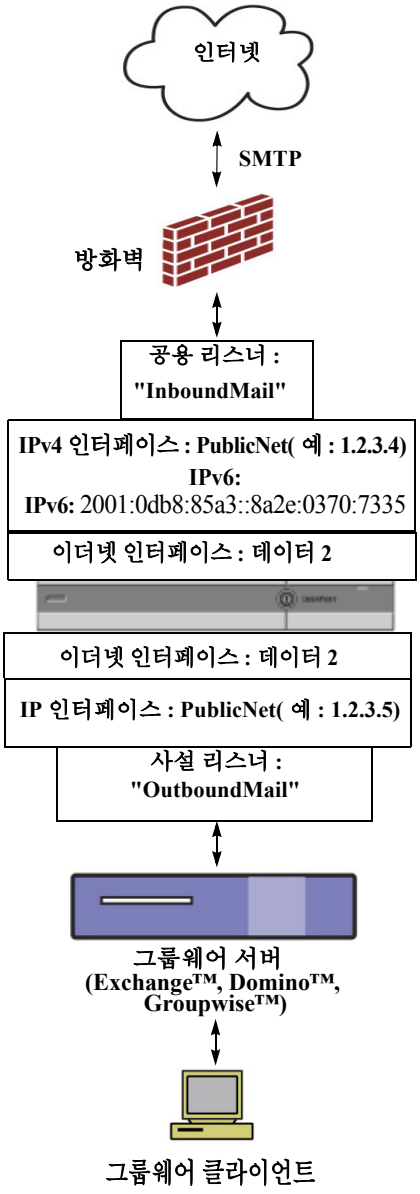
수신 및 발송 메일 분리

별도의 리스너와 별도의 IP 주소를 통해 수신 및 발송 이메일 트래픽을 분리할 수 있습니다. IPv4(인터넷 프로토콜 버전 4) 및 IPv6(인터넷 프로토콜 버전 6) 주소를 사용할 수 있습니다. 그러나 어플라이언스의 시스템 설정 마법사는 다음과 같은 구성의 초기 구성을 지원합니다.

- *별도의* 물리적 인터페이스에 구성된 2개의 논리 IPv4 주소와 2개의 IPv6 주소의 별도의 리스너 2개
  - 수신 및 발송 트래픽 분리
  - 각 리스너에 IPv4 주소 1개와 IPv6 주소 1개를 할당할 수 있음
- 1개의 물리적 인터페이스에 구성된 1개의 논리 IPv4 주소의 리스너 1개
  - 수신 및 발송 트래픽 모두 결합
  - 해당 리스너에 IPv4 주소 1개와 IPv6 주소 1개를 할당할 수 있음

1개의 리스너와 2개의 리스너에 대한 구성 워크시트가 아래에 나와 있습니다(설정 정보 수집, 3-11페이지 참조). 대부분의 구성 시나리오는 다음 3개의 그림 중 하나에 해당됩니다.

그림 3-1 방화벽 시나리오 뒤/2개의 리스너 구성



참고:

- 2개의 리스너
- 2개의 IPv4 주소
- 2개의 IPv6 주소
- 1개 또는 2개의 이더넷 인터페이스(1개의 인터페이스만 표시됨)
- SMTP 경로 구성

인바운드 리스너: **"InboundMail"(공용)**

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

아웃바운드 리스너: **"OutboundMail"(사설)**

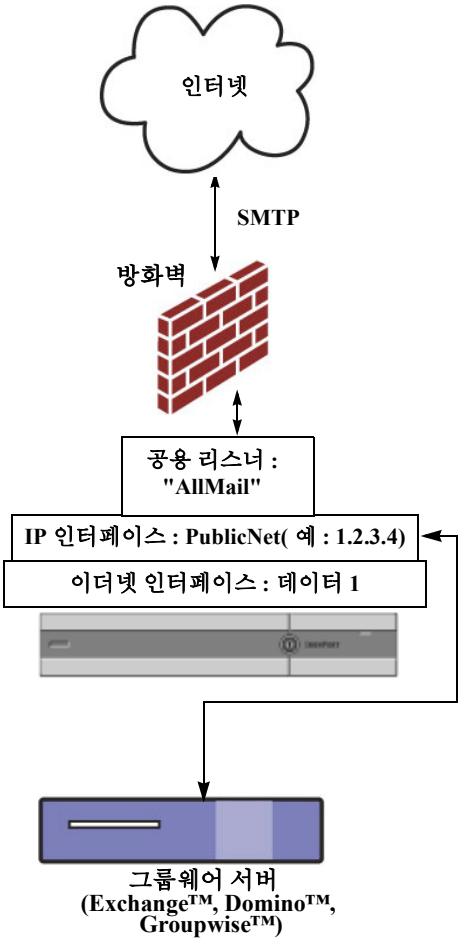
- IP 주소: 1.2.3.5
- IPv6 주소: 2001:0db8:85a3::8a2e:0370:7335
- 포트 25에서 수신 대기하는 Data2 인터페이스의 리스너
- HAT(로컬 도메인의 릴레이, 모두 거부)

인터넷 루트 서버 또는 내부 DNS 서버를 사용하도록 DNS를 구성할 수 있음

SMTP 경로가 메일을 올바른 그룹웨어 서버에 전달

방화벽 포트가 Email Security 어플라이언스에서 주고받은 해당 서비스에 대해 열려 있음

그림 3-2 1개의 리스너 구성



참고:

- 1개의 리스너
- 1개의 IP 주소
- 1개의 이더넷 인터페이스
- SMTP 경로 구성

인바운드 리스너: **"InboundMail"**(공용)

- IP 주소: 1.2.3.4
- 포트 25에서 수신 대기하는 Data2 인터페이스의 리스너
- HAT(모두 수락)에는 RELAYLIST의 그룹웨어 서버 항목이 포함됨
- RAT(로컬 도메인의 메일 수락, 모두 거부)

인터넷 루트 서버 또는 내부 **DNS** 서버를 사용하도록 **DNS**를 구성할 수 있음

SMTP 경로가 메일을 올바른 그룹웨어 서버에 전달

방화벽 포트가 어플라이언스에서 주고받은 해당 서비스에 대해 열려 있음

시스템 설정 준비

	수행할 작업	추가 정보
1단계	어플라이언스에 연결하는 방법을 결정합니다.	어플라이언스에 연결하는 방법 결정, 3-8페이지를 참조하십시오.
2단계	네트워크 및 IP 주소 할당을 결정합니다. 어플라이언스를 이미 네트워크에 연결한 경우 Email Security 어플라이언스의 기본 IP 주소가 네트워크의 다른 IP 주소와 충돌하지 않는지 확인합니다.	네트워크 및 IP 주소 할당, 3-9페이지 어플라이언스에 연결하는 방법 결정, 3-8페이지
3단계	시스템 설정에 대한 정보를 수집합니다.	설정 정보 수집, 3-11페이지를 참조하십시오.
4단계	사용 중인 어플라이언스의 최신 제품 릴리스 노트를 검토합니다.	릴리스 노트는 문서, 1-7페이지의 해당 링크에서 사용할 수 있습니다.
5단계	어플라이언스를 개봉하고 랙에 물리적으로 설치한 다음 전원을 켭니다.	사용 중인 어플라이언스의 *빠른 시작 설명서*를 참조하십시오. 이 설명서는 문서, 1-7페이지의 링크에서 사용할 수 있습니다.
6단계	웹 인터페이스 또는 CLI(Command Line Interface)를 사용해 어플라이언스에 액세스합니다.	• 웹 브라우저를 실행하고 어플라이언스의 IP 주소를 입력합니다. 또는 • CLI(Command Line Interface) 시스템 설정 마법사 실행, 3-24페이지를 참조하십시오.
7단계	가상 Email Security 어플라이언스를 설정할 경우 가상 어플라이언스 라이센스를 로드합니다.	`loadlicense` 명령을 사용합니다. 자세한 내용은 *Cisco Content Security Virtual Appliance 설치 설명서*(문서, 1-7페이지의 링크에서 사용 가능)를 참조하십시오.
8단계	시스템의 기본 설정을 구성합니다.	시스템 설정 마법사 사용, 3-13페이지를 참조하십시오.

어플라이언스에 연결하는 방법 결정

현재 환경에서 Email Security 어플라이언스를 성공적으로 설정하려면 네트워크 관리자에게서 Email Security 어플라이언스를 네트워크에 연결하는 방법에 대한 중요한 네트워크 정보를 수집해야 합니다.

관련 주제

어플라이언스에 연결

초기 설정 도중 다음 두 가지 방법 중 하나를 사용해 어플라이언스에 연결할 수 있습니다.

표 3-1 어플라이언스에 연결하는 옵션

이더넷	PC와 네트워크 사이, 네트워크와 관리 포트 사이의 이더넷 연결. 출고 시 관리 포트에 할당된 IPv4 주소는 `192.168.42.42`입니다. 이는 네트워크 구성에서 작동할 경우 가장 쉽게 연결할 수 있는 방법입니다.
일련 번호	PC와 직렬 콘솔 포트 사이의 직렬 통신 연결. 이더넷 방법을 사용할 수 없는 경우 대체 네트워크 설정을 관리 포트에 적용할 수 있을 때까지 컴퓨터와 어플라이언스 사이의 직선 직렬-직렬 연결이 작동됩니다. 핀아웃에 대한 내용은 직렬 연결을 통한 Email Security 어플라이언스 액세스, A-5페이지를 참조하십시오. 직렬 포트의 통신 설정은 다음과 같습니다. **초당 비트:** 9600 **데이터 비트:** 8 **패리티:** 없음 **정지 비트:** 1 **흐름 제어:** 하드웨어

참고 초기 연결 방법을 마지막에도 사용할 필요는 없습니다. 이 프로세스는 초기 구성에만 적용됩니다. 다른 연결 방법을 사용할 수 있도록 나중에 네트워크 설정을 변경할 수 있습니다. (자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스"를 참조하십시오.) 어플라이언스 액세스 관리 권한이 서로 다른 여러 개의 사용자 계정을 생성할 수도 있습니다. (자세한 내용은 사용자 추가, 32-4페이지를 참조하십시오.)

네트워크 및 IP 주소 할당

IPv4 및 IPv6 주소를 모두 사용할 수 있습니다.

관리 및 데이터 포트의 IP 주소

관리 포트(C170 어플라이언스의 데이터 1 포트)에 미리 구성된 IP 주소는 `192.168.42.42`입니다.

이메일 수신 및 전송에 사용할 네트워크 연결 선택

대부분의 사용자는 어플라이언스에서 2개의 네트워크에 연결하여 이더넷 보안 어플라이언스에 있는 2개의 데이터 이더넷 포트를 활용합니다.

- 사설 네트워크는 메시지를 수락하고 내부 시스템에 전송합니다.

- 공용 네트워크는 메시지를 수락하고 인터넷에 전송합니다.

다른 사용자가 1개의 데이터 포트만 사용하여 두 기능을 모두 제공하려 할 수 있습니다. 관리 이더넷 포트는 모든 기능을 지원할 수 있지만 그래픽 사용자 인터페이스와 명령줄 인터페이스에 액세스할 수 있도록 미리 구성되어 있습니다.

물리적 이더넷 포트에 논리 IP 주소 바인딩

별도의 리스너와 별도의 IP 주소를 통해 수신 및 발송 이메일 트래픽을 분리할 수 있습니다. IPv4(인터넷 프로토콜 버전 4) 및 IPv6(인터넷 프로토콜 버전 6) 주소를 사용할 수 있습니다. 그러나 어플라이언스의 시스템 설정 마법사는 다음과 같은 구성의 초기 구성을 지원합니다.

- *별도의* 물리적 인터페이스에 구성된 2개의 논리 IPv4 주소와 2개의 IPv6 주소의 별도의 리스너 2개
  - 수신 및 발송 트래픽 분리
  - 각 리스너에 IPv4 주소 1개와 IPv6 주소 1개를 할당할 수 있음
- 1개의 물리적 인터페이스에 구성된 1개의 논리 IPv4 주소의 리스너 1개
  - 수신 및 발송 트래픽 모두 결합
  - 해당 리스너에 IPv4 주소 1개와 IPv6 주소 1개를 할당할 수 있음

Email Security 어플라이언스는 단일 리스너에서 IPv4 및 IPv6 주소를 모두 지원할 수 있습니다. 리스너가 두 주소 모두에서 메일을 수락할 수 있습니다. 리스너의 모든 설정이 IPv4 및 IPv6 주소 모두에 적용됩니다.

연결의 네트워크 설정 선택

사용하기로 선택한 각 네트워크 포트에 대한 다음 네트워크 정보가 필요합니다.

- IP 주소(IPv4 또는 IPv6 또는 둘 다)
- CIDR 형식의 IPv4 주소의 넷마스크
- CIDR 형식의 IPv6 주소의 접두사

또한 전체 네트워크에 대한 다음 정보가 필요합니다.

- 네트워크의 기본 라우터(게이트웨이)의 IP 주소
- DNS 서버의 IP 주소 및 호스트 이름(인터넷 루트 서버를 사용할 경우에는 필요하지 않음)
- NTP 서버의 호스트 이름 또는 IP 주소(Cisco의 시간 서버를 사용할 경우에는 필요하지 않음)

자세한 내용은 부록 B, "네트워크 및 IP 주소 할당"을 참조하십시오.

참고 네트워크 상에서 인터넷과 Email Security 어플라이언스 사이에 방화벽을 실행할 경우 올바르게 작동하려면 어플라이언스의 특정 포트를 열어야 할 수 있습니다. 자세한 내용은 부록 D, "방화벽 정보"를 참조하십시오.

설정 정보 수집

이 섹션을 읽으면서 이제 시스템 설정 마법사에서 필요한 항목을 선택할 때의 요건 및 전략과 다음 표를 사용하여 시스템 설정에 대한 정보를 수집하는 방법을 이해했을 것입니다.

네트워크 및 IP 주소에 대한 자세한 내용은 부록 B, "네트워크 및 IP 주소 할당"을 참조하십시오. 42 장, "Cisco Content Security Management Appliance에서 서비스 중앙 집중화"를 참조하면 Cisco Content Security Management 어플라이언스를 구성할 때 유용한 정보를 얻을 수 있습니다.

표 3-2 시스템 설정 워크시트: 이메일 트래픽을 분리하는 2개의 리스너

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

표 3-2 시스템 설정 워크시트: 이메일 트래픽을 분리하는 2개의 리스너 (계속)

접두사:		
전체(Fully Qualified) 호스트 이름:		
수신 메일 수락:	**도메인**	**대상**
발송 메일 중계:	**시스템**	
메시지 보안		
SenderBase 평판 필터:	활성화/비활성화	
안티스팸 검사 엔진	없음/IronPort	
McAfee 안티바이러스 검사 엔진	활성화/비활성화	
Sophos 안티바이러스 검사 엔진	활성화/비활성화	
신종 바이러스 필터(Outbreak Filter)	활성화/비활성화	

표 3-3 시스템 설정 워크시트: 모든 이메일 트래픽에 사용되는 1개의 리스너

시스템 설치		
기본 시스템 호스트 이름:		
다음 사용자에게 이메일로 시스템 경보 보내기:		
예약 보고서 배달 대상:		
표준 시간대:		
NTP 서버:		
관리자 암호:		
SenderBase 네트워크 참여:	활성화/비활성화	
자동지원:	활성화/비활성화	
네트워크 통합		
게이트웨이:		
DNS(인터넷 또는 직접 지정):		
인터페이스		
데이터2 포트		
IPv4 주소/넷마스크:		
IPv6 주소/접두사:		
전체(Fully Qualified) 호스트 이름:		
수신 메일 수락:	**도메인**	**대상**
발송 메일 중계:	**시스템**	
데이터1 포트		
IPv4 주소/넷마스크:		
IPv6 주소/접두사:		

표 3-3 시스템 설정 워크시트: 모든 이메일 트래픽에 사용되는 1개의 리스너 (계속)

전체(Fully Qualified) 호스트 이름:	
메시지 보안	
SenderBase 평판 필터:	활성화/비활성화
안티스팸 검사 엔진	없음/IronPort
McAfee 안티바이러스 검사 엔진	활성화/비활성화
Sophos 안티바이러스 검사 엔진	활성화/비활성화
신종 바이러스 필터(Outbreak Filter)	활성화/비활성화

시스템 설정 마법사 사용

- 웹 기반 GUI(그래픽 사용자 인터페이스) 액세스, 3-14페이지
- 웹 기반 시스템 설정 마법사를 사용하여 기본 구성 정의, 3-14페이지
- Active Directory에 대한 연결 설정, 3-22페이지
- 다음 단계로 진행, 3-23페이지
- CLI(Command Line Interface) 액세스, 3-23페이지
- CLI(Command Line Interface) 시스템 설정 마법사 실행, 3-24페이지
- 시스템을 엔터프라이즈 게이트웨이로 구성, 3-37페이지

완벽한 구성을 보장하려면 초기 설정 시 시스템 설정 마법사를 사용해야 합니다. 나중에 시스템 설정 마법사에서 사용할 수 없는 사용자 지정 옵션을 구성할 수 있습니다.

브라우저 또는 CLI(Command Line Interface)를 사용하여 시스템 설정 마법사를 실행할 수 있습니다. 자세한 내용은 웹 기반 GUI(그래픽 사용자 인터페이스) 액세스, 3-14페이지 또는 CLI(Command Line Interface) 시스템 설정 마법사 실행, 3-24페이지를 참조하십시오.

시작하기 전에 시스템 설정 준비, 3-8페이지의 요구 사항을 모두 충족해야 합니다.

주의 가상 Email Security 어플라이언스를 설정할 경우 시스템 설정 마법사를 실행하기 전에 `loadlicense` 명령을 사용해 가상 어플라이언스 라이센스를 로드해야 합니다. 자세한 내용은 *Cisco Content Security Virtual Appliance 설치 설명서*를 참조하십시오.

주의 시스템 설정 마법사가 시스템을 완전히 재구성합니다. 어플라이언스를 처음 설치하거나 기존 구성을 완전히 덮어쓰려는 경우에만 시스템 설정 마법사를 사용해야 합니다.

주의 이메일 보안 어플라이언스는 모든 하드웨어의 관리 포트에 기본 IP 주소인 `192.168.42.42`가 내장되어 있습니다. 단, C170 어플라이언스는 여기에서 제외되며 대신 데이터 1을 사용합니다. 어플라이언스를 네트워크에 연결하기 전에 다른 디바이스의 IP 주소가 이 공장 기본 설정과 충돌하지 않는지 확인합니다. Cisco Content Security Management 어플라이언스를 구성할 경우 Cisco Content Security Management Appliance에서 서비스 중앙 집중화, 42-1페이지를 참조하십시오.

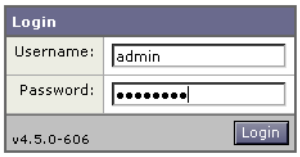
공장에서 구성된 여러 콘텐츠 보안 어플라이언스를 네트워크에 연결할 경우 각 어플라이언스의 기본 IP 주소를 재구성하면서 한 번에 하나씩 추가합니다.

웹 기반 GUI(그래픽 사용자 인터페이스) 액세스

웹 기반 GUI(그래픽 사용자 인터페이스)에 액세스하려면 웹 브라우저를 열고 192.168.42.42를 가리키도록 합니다.

로그인 화면이 표시됩니다.

그림 3-3 어플라이언스에 로그인



아래에 사용자 이름과 비밀번호를 입력하여 어플라이언스에 로그인합니다.

관련 주제

- 공장 기본 사용자 이름 및 비밀번호, 3-14페이지

공장 기본 사용자 이름 및 비밀번호

- 사용자 이름: **admin**
- 비밀번호: **ironport**

참고 세션의 시간이 초과되면 사용자 이름과 비밀번호를 다시 입력하라는 메시지가 표시됩니다. 시스템 설정 마법사를 실행한 상태에서 세션의 시간이 초과되면 처음부터 다시 시작해야 합니다.

웹 기반 시스템 설정 마법사를 사용하여 기본 구성 정의

절차

1단계 시스템 설정 마법사를 시작합니다.

- 웹 기반 GUI(그래픽 사용자 인터페이스) 액세스, 3-14페이지에 설명된 대로 그래픽 사용자 인터페이스에 로그인합니다.
- 새로운(이전 AsyncOS 릴리스에서 업그레이드되지 않은) 시스템에서는 브라우저가 자동으로 시스템 설정 마법사로 리디렉션됩니다.
- 그렇지 않을 경우 시스템 관리 탭의 왼쪽에 있는 링크 목록에서 System Setup Wizard(시스템 설정 마법사)를 클릭합니다.

2단계 시작. 1단계: 시작을 참조하십시오.

- 라이센스 계약을 읽고 동의합니다.

3단계 시스템. 2단계: 시스템을 참조하십시오.

- 어플라이언스의 호스트 이름 설정
- 경고 설정, 보고서 전송 설정 및 AutoSupport 구성
- 시스템 시간 설정 및 NTP 서버 설정

- 관리자 비밀번호 리셋
- SenderBase 네트워크 참여 활성화

4단계 네트워크. 3단계: 네트워크을 참조하십시오.

- 기본 라우터 및 DNS 설정 정의
- 다음과 같은 네트워크 인터페이스 구성 및 활성화
  수신 메일 구성(인바운드 리스너)
  SMTP 경로 구성(선택 사항)
  발송 메일 구성(아웃바운드 리스너) 및 어플라이언스를 통해 메일을 전달할 수 있도록 시스템 정의(선택 사항)

5단계 보안. 4단계: 보안을 참조하십시오.

- SenderBase 평판 필터링 활성화
- 안티스팸 서비스 활성화
- 스팸 격리 활성화
- 안티바이러스 서비스 활성화
- Advanced Malware Protection(파일 평판 및 분석 서비스) 활성화
- 신종 바이러스 필터(Outbreak Filter) 서비스 활성화

6단계 검토. 5단계: 검토를 참조하십시오.

- 설정 검토 및 구성 설치
- 프로세스가 완료되면 메시지가 표시됨

7단계 변경 사항을 커밋합니다.

커밋되어야만 변경 사항이 적용됩니다.

1단계: 시작

먼저 라이센스 계약을 읽습니다. 라이센스 계약을 읽고 동의하면 동의를 나타내는 상자를 선택한 **Begin Setup(설정 시작)**을 클릭해 계속 진행합니다.

여기에서도 계약 내용을 볼 수 있습니다.
`https://support.ironport.com/license/eula.html`

2단계: 시스템

- 호스트 이름 설정, 3-16페이지
- 시스템 경고 구성, 3-16페이지
- 보고서 전송 구성, 3-16페이지
- 시간 설정, 3-16페이지
- 비밀번호 설정, 3-16페이지
- SenderBase 네트워크에 참여, 3-16페이지
- AutoSupport 활성화, 3-17페이지

호스트 이름 설정

Email Security 어플라이언스의 정규화된 호스트 이름을 정의합니다. 이 이름은 네트워크 관리자가 지정해야 합니다.

시스템 경고 구성

Cisco 사용자의 개입이 필요한 시스템 오류가 발생한 경우 AsyncOS가 이메일을 통해 경고 메시지를 보냅니다. 그러한 경고를 보낼 이메일 주소를 입력합니다.

시스템 경고를 받을 이메일 주소를 최소한 하나 이상 추가해야 합니다. 단일 이메일 주소를 입력하거나 여러 개의 주소를 쉼표로 구분합니다. 이메일 수신자는 디렉토리 수집 공격 방지 경고를 제외하고 처음에 모든 수준에서 모든 유형의 경고를 수신합니다. 나중에 경고 구성에 더 세부적인 내용을 추가할 수 있습니다. 자세한 내용은 경고, 33-34페이지를 참고하십시오.

보고서 전송 구성

기본 예약 보고서를 전송할 주소를 입력합니다. 이 값을 비워 둬도 예약 보고서는 계속 실행됩니다. 이 경우 예약 보고서가 전송되지 않고 어플라이언스에 아카이브됩니다.

시간 설정

메시지 헤더와 로그 파일의 타임스탬프가 올바르게 표시되도록 Email Security 어플라이언스에서 표준 시간대를 설정합니다. 드롭다운 메뉴를 사용하여 해당 표준 시간대를 찾거나 GMT 오프셋(자세한 내용은 GMT 오프셋 선택, 33-57페이지 참조)을 통해 표준 시간대를 정의합니다.

나중에 수동으로 시스템 클럭 시간을 설정하거나 NTP(Network Time Protocol)를 사용하여 네트워크 또는 인터넷의 다른 서버와 시간을 동기화할 수 있습니다. 기본적으로, Cisco 시스템 시간 서버(`time.ironport.com`)를 통해 어플라이언스의 시간을 동기화할 수 있는 항목이 이미 구성되어 있습니다.

비밀번호 설정

관리자 계정의 비밀번호를 설정합니다. 이는 필수 단계입니다. Cisco AsyncOS 관리 계정의 비밀번호를 변경할 경우 새 비밀번호는 6자 이상이어야 합니다. 비밀번호는 안전한 위치에 보관해 두십시오.

SenderBase 네트워크에 참여

SenderBase는 이메일 관리자가 발신자를 조사하고 이메일의 정상적인 소스를 파악하고 스패머를 차단할 수 있도록 설계된 이메일 평판 서비스입니다.

사용자가 SenderBase 네트워크에 참여하는 데 동의할 경우 Cisco는 사용자의 조직에 대한 집계된 이메일 트래픽 통계를 수집합니다. 여기에는 메시지 특성에 대한 요약 데이터와 Email Security 어플라이언스에서 처리한 메시지 유형에 대한 정보만 포함됩니다. 예를 들어, Cisco는 메시지 본문 또는 메시지 제목을 수집하지 않습니다. 개인 식별 정보 또는 조직을 식별할 수 있는 정보는 기밀로 유지됩니다. 수집되는 데이터의 예를 포함해 SenderBase에 대해 자세히 알아보려면 **Click here for more information about what data is being shared...(공유되는 데이터에 대한 자세한 내용을 보려면 여기를 클릭...)** 링크(FAQ(자주 묻는 질문), 35-2페이지 참조)를 따라가십시오.

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(이메일 기반 위협을 식별하고 중지하기 위해 IronPort가 이메일에 대한 익명 통계를 수집하여 SenderBase에 보고하도록 허용)" 옆의 상자를 선택하고 **Accept(동의)**를 클릭합니다.

자세한 내용은 35 장, "SenderBase 네트워크 참여"를 참조하십시오.

AutoSupport 활성화

AutoSupport 기능(기본적으로 활성화됨)을 통해 Cisco 고객 지원팀이 어플라이언스의 문제를 지속적으로 파악할 수 있으므로 Cisco에서 더 나은 지원을 제공할 수 있습니다. (자세한 내용은 AutoSupport, 33-34페이지를 참조하십시오.)

계속하려면 **Next(다음)**를 클릭합니다.

3단계: 네트워크

3단계에서는 기본 라우터(게이트웨이)를 정의하고 DNS 설정을 구성한 다음 데이터 1, 데이터 2 및 관리 인터페이스를 구성하여 이메일을 수신하거나 전달하도록 어플라이언스를 설정합니다.

DNS 및 기본 게이트웨이 구성

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

그런 다음 DNS(Domain Name Service) 설정을 구성합니다. Cisco AsyncOS에는 인터넷의 루트 서버에 직접 쿼리하거나 시스템에서 사용자가 지정한 DNS 서버를 사용할 수 있는 고성능 내부 DNS 확인자/캐시가 포함되어 있습니다. 자체 서버를 사용하기로 선택할 경우 각 DNS 서버의 IP 주소와 호스트 이름을 입력해야 합니다. 시스템 설정 마법사를 통해 최대 4개의 DNS 서버를 입력할 수 있습니다. 입력한 DNS 서버의 초기 우선순위가 0으로 지정됩니다. 자세한 내용은 DNS(Domain Name System) 설정 구성, 33-52페이지를 참고하십시오.

참고 어플라이언스가 수신 연결에 대한 DNS 조회를 수행하기 위해서는 작동 중인 DNS 서버에 액세스해야 합니다. 어플라이언스를 설정하는 동안 어플라이언스에서 연결할 수 있는 작동 중인 DNS 서버를 지정할 수 없는 경우 "Use Internet Root DNS Servers(인터넷 루트 DNS 서버 사용)"를 선택하거나 시스템 설정 마법사를 완료할 수 있도록 관리 인터페이스의 IP 주소를 임시로 지정하여 문제를 해결할 수 있습니다.

네트워크 인터페이스 구성

Email Security 어플라이언스에는 머신의 물리적인 이더넷 포트와 연결된 네트워크 인터페이스가 있습니다.

인터페이스를 사용하려면 "활성화" 확인란을 선택한 다음 IP 주소, 네트워크 마스크, 정규화된 호스트 이름을 지정합니다. 입력하는 IP 주소는 DNS 레코드에 반영된 대로 인바운드 메일에 사용되는 주소여야 합니다. 일반적으로 이 주소는 DNS에 관련 MX 레코드가 있습니다. IPv4 주소, IPv6 주소 또는 둘 다 사용할 수 있습니다. 둘 다 사용할 경우 인터페이스가 이 두 가지 유형의 연결을 모두 수락합니다.

메일(수신), 릴레이 이메일(발송) 또는 어플라이언스 관리를 수락하도록 각 인터페이스를 구성할 수 있습니다. 설정 중에는 각 인터페이스 중 하나만 사용할 수 있습니다. 대부분의 어플라이언스에서는 수신, 발송 및 어플라이언스 관리에 인터페이스를 하나씩 사용합니다. C170 어플라이언스에서는 일반적으로 수신 및 발송 메일에 하나의 인터페이스를 사용하고 다른 인터페이스는 관리 목적으로 사용합니다.

이메일을 수신하는 인터페이스 1개를 구성해야 합니다.

로컬 IP 주소를 구성해서 어플라이언스의 물리적 이더넷 인터페이스 중 하나에 할당합니다. 데이터 1 이더넷 포트와 데이터 2 이더넷 포트를 모두 사용하기로 결정할 경우 두 연결 모두에 이 정보가 필요합니다.

C370, C670, X1070, C380, C680 어플라이언스의 경우: Cisco에서는 공용 리스너를 통해 인바운드 이메일을 수신하려면 물리적인 이더넷 포트 중 하나를 사용해 인터넷에 직접 연결하고, 사설 리스너를 통해 아웃바운드 이메일을 전달하려면 다른 물리적 이더넷 포트를 사용해 내부 네트워크에 직접 연결할 것을 권장합니다.

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

물리적 이더넷 포트에 논리 IP 주소 바인딩, 3-10페이지를 참조하십시오.

다음 정보가 필요합니다.

- 네트워크 관리자가 할당한 **IP 주소**. 이는 IPv4 주소, IPv6 주소 또는 둘 다일 수 있습니다.
- IPv4 주소의 경우: 인터페이스의 **넷마스크**. AsyncOS는 CIDR 형식의 넷마스크만 허용합니다. 예를 들어, `255.255.255.0` 서브넷의 경우는 `/24`를 사용합니다.

  IPv6 주소의 경우: CIDR 형식의 **접두사**. 예를 들어, 64비트 접두사의 경우는 `/64`를 사용합니다.
- (선택 사항) IP 주소의 정규화된 호스트 이름.

참고 동일한 서브넷 내의 IP 주소는 별도의 물리적 이더넷 인터페이스에서 구성할 수 없습니다. 네트워크 및 IP 주소 구성에 대한 자세한 내용은 부록 B, "네트워크 및 IP 주소 할당"을 참조하십시오.

메일 수락

메일을 수락할 인터페이스를 구성할 경우 다음을 정의합니다.

- 메일을 수락할 도메인
- 각 도메인의 대상(SMTP 경로), 이는 선택 사항임

메일을 수락할 인터페이스를 구성하려면 수신 메일 수락 확인란을 선택합니다. 메일을 수락할 도메인의 이름을 입력합니다.

대상을 입력합니다. 이는 지정한 도메인의 이메일을 라우팅할 머신의 이름 또는 SMTP 경로입니다.

이는 첫 번째 SMTP 경로 항목입니다. SMTP 경로 표를 사용하여 특정 MX(메일 교환) 호스트에 입력하는 각 도메인(RAT(Recipient Access Table) 항목이라고도 함)의 모든 이메일을 리디렉션할 수 있습니다. 일반 설치에서는 SMTP 경로 표가 특정 그룹웨어(예: Microsoft Exchange) 서버 또는 인프라의 이메일 전송의 "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 도메인과 대상을 입력할 수 있습니다. 다른 도메인을 추가하려면 **Add Row(행 추가)**를 클릭합니다. 행을 제거하려면 휴지통 아이콘을 클릭합니다.

참고 원하는 경우 이 단계에서 SMTP 경로를 구성할 수 있습니다. SMTP 경로가 정의되지 않은 경우 시스템이 DNS를 사용하여 리스너에서 수신하는 수신 메일의 전송 호스트를 조회하고 결정합니다. (로컬 도메인의 이메일 라우팅, 24-1페이지 참조)

Recipient Access Table에 최소한 하나 이상의 도메인을 추가해야 합니다. 예를 들어, 도메인 example.com을 입력합니다. example.net의 하위 도메인으로 전송되는 메일이 Recipient Access Table의 정보와 일치하려면 도메인 이름뿐 아니라 .example.net도 입력합니다. 자세한 내용은 수신자 주소 정의, 8-4페이지를 참고하십시오.

메일 전달(선택 사항)

메일을 전달할 인터페이스를 구성할 경우 어플라이언스를 통해 이메일을 전달할 수 있도록 시스템을 정의합니다.

이는 리스너의 Host Access Table의 RELAYLIST에 있는 항목입니다. 자세한 내용은 발신자 그룹 구문, 7-4페이지를 참조하십시오.

메일을 전달할 인터페이스를 구성하려면 발송 메일 전달 확인란을 선택합니다. 어플라이언스를 통해 메일을 전달할 수 있는 호스트를 입력합니다.

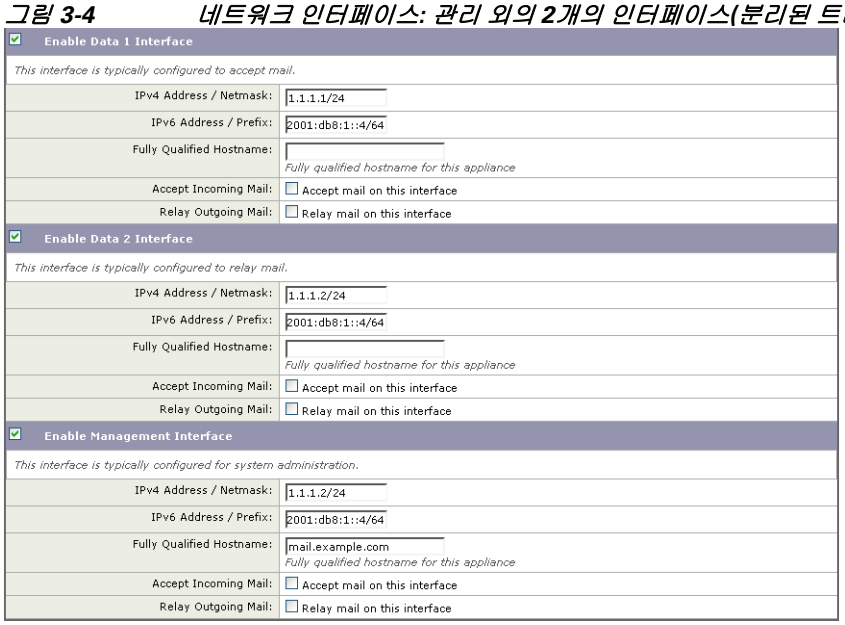
발송 메일을 전달할 인터페이스를 구성할 경우 인터페이스를 사용하도록 구성된 공용 리스너가 없으면 시스템 설정 마법사가 인터페이스에 대해 SSH를 활성화합니다.

다음 예제에서는 IPv4 주소를 사용하는 2개의 인터페이스를 생성합니다.

- 192.168.42.42가 관리 인터페이스에 구성된 상태로 유지됩니다.
- 192.168.1.1이 데이터 1 이더넷 인터페이스에 대해 활성화됩니다. .example.com으로 끝나는 도메인의 메일을 수락하도록 구성되어 있으며 SMTP 경로가 exchange.example.com에 대해 정의되어 있습니다.
- 192.168.2.1이 데이터 2 이더넷 인터페이스에 대해 활성화됩니다. exchange.example.com에서 메일을 전달하도록 구성되어 있습니다.

참고 다음 예제는 C370, C670, X1070, C380, C680 어플라이언스와만 관계가 있습니다. C170 어플라이언스의 경우 데이터 2 인터페이스가 일반적으로 메일을 수신 및 발송하도록 구성되어 있으며 데이터 1 인터페이스가 어플라이언스 관리에 사용됩니다(C170 설치, 3-20페이지 참조).

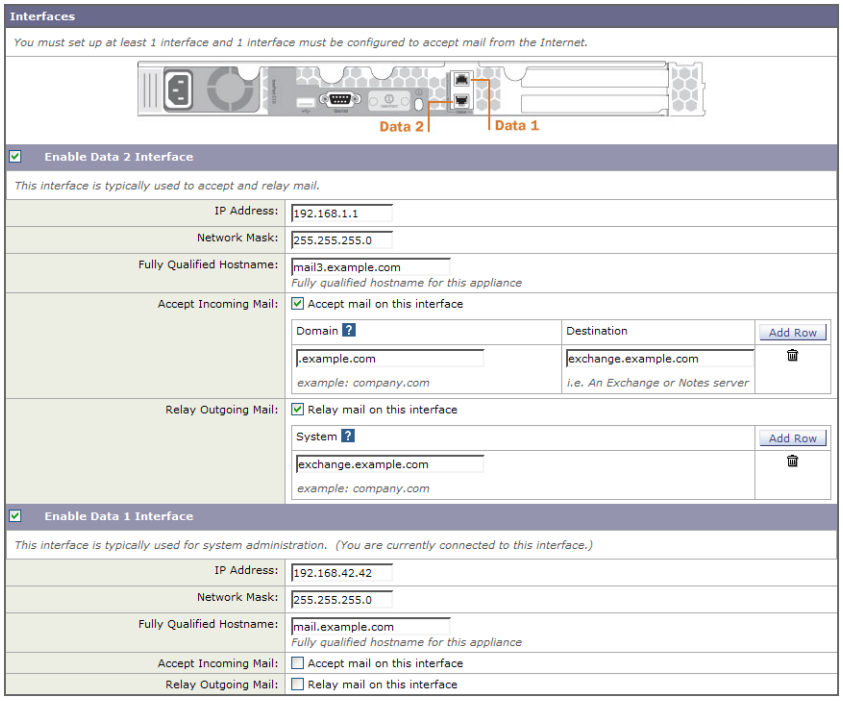
그림 3-4 네트워크 인터페이스: 관리 외의 2개의 인터페이스(분리된 트래픽)



C170 설치

모든 이메일에 대한 단일 IP 주소를 구성할 경우(분리되지 않은 트래픽) 시스템 설정 마법사의 3단계가 다음과 같이 표시됩니다.

그림 3-5 네트워크 인터페이스: 분리되지 않은 트래픽을 수신 및 발송하는 1개의 IP 주소



계속하려면 **Next(다음)**를 클릭합니다.

4단계: 보안

4단계에서 안티스팸 및 안티바이러스 설정을 구성합니다. 안티스팸 옵션에는 SenderBase 평판 필터링과 안티스팸 검사 엔진 선택이 포함됩니다. 안티바이러스의 경우 신종 바이러스 필터(Outbreak Filter)와 Sophos 또는 McAfee 안티바이러스 검사를 사용할 수 있습니다.

- SenderBase 평판 필터링 활성화, 3-21페이지
- 안티스팸 검사 활성화, 3-21페이지
- 안티바이러스 검사 활성화, 3-21페이지
- Advanced Malware Protection(파일 평판 및 분석 서비스) 활성화, 3-22페이지
- 신종 바이러스 필터(Outbreak Filter) 활성화, 3-22페이지

SenderBase 평판 필터링 활성화

SenderBase Reputation Service는 독립 실행형 안티스팸 솔루션으로 사용될 수 있지만 기본적으로 안티스팸과 같은 콘텐츠 기반 안티스팸 시스템의 효율성을 향상시키도록 설계되었습니다.

SenderBase Reputation Service(http://www.senderbase.org)를 통해 사용자가 원격 호스트의 연결 IP 주소를 기준으로 정확하고 유연하게 의심스러운 스팸을 거부하거나 제한할 수 있습니다. SenderBase Reputation Service는 지정된 소스의 메시지가 스팸일 가능성에 따라 점수를 반환합니다. SenderBase Reputation Service는 이메일 메시지 볼륨에 대한 전역 보기를 제공하고 이메일의 관련 소스를 손쉽게 식별하고 그룹화할 수 있도록 데이터를 구성한다는 점에서 고유합니다. Cisco에서는 SenderBase 평판 필터링을 활성화할 것을 적극 권장합니다.

SenderBase 평판 필터링은 한 번 활성화하면 수신(수락) 리스너에 적용됩니다.

안티스팸 검사 활성화

어플라이언스에 안티스팸 소프트웨어에 대한 30일 평가 키가 포함될 수 있습니다. 시스템 설정 마법사의 이 부분에서 어플라이언스에서 전역적으로 안티스팸을 활성화할 수 있습니다. 서비스를 활성화하지 않기로 선택할 수도 있습니다.

안티스팸 서비스를 활성화하기로 선택한 경우 스팸과 의심스러운 스팸 메시지를 로컬 스팸 격리로 보내도록 AsyncOS를 구성할 수 있습니다. 스팸 격리는 어플라이언스의 최종 사용자 격리로 사용됩니다. 최종 사용자 액세스가 구성될 때까지 관리자만 격리에 액세스할 수 있습니다.

어플라이언스에서 사용할 수 있는 모든 안티스팸 구성 옵션은 13 장, "안티스팸"을 참조하십시오. 정책, 바이러스 및 신종 바이러스 격리, 30-1페이지를 참조하십시오.

안티바이러스 검사 활성화

어플라이언스에 Sophos 안티바이러스 또는 McAfee 안티바이러스 검사 엔진에 대한 30일 평가 키가 포함될 수 있습니다. 시스템 설정 마법사의 이 부분에서 어플라이언스에서 전역적으로 안티바이러스 검사 엔진을 활성화할 수 있습니다.

안티바이러스 검사 엔진을 활성화하기로 선택할 경우 이 엔진이 기본 수신 및 기본 발송 메일 정책 *모두*에 대해 활성화됩니다. 어플라이언스가 메일에 바이러스가 있는지 검사하지만 감염된 첨부 파일을 복구하지는 않습니다. 어플라이언스가 감염된 메시지를 삭제합니다.

어플라이언스에서 사용할 수 있는 모든 안티바이러스 구성 옵션은 12 장, "안티바이러스"를 참조하십시오.

Advanced Malware Protection(파일 평판 및 분석 서비스) 활성화

Advanced Malware Protection이 클라우드 기반 서비스에서 첨부된 파일에 대한 평판 정보를 수집합니다.

자세한 내용은 16 장, "파일 평판 필터링 및 파일 분석"을 참조하십시오.

신종 바이러스 필터(Outbreak Filter) 활성화

어플라이언스에 신종 바이러스 필터(Outbreak Filter)에 대한 30일 평가 키가 포함될 수 있습니다. 신종 바이러스 필터(Outbreak Filter)는 기존의 안티바이러스 보안 서비스를 새 바이러스 서명 파일로 업데이트할 수 있을 때까지 의심스러운 메시지를 격리하여 신종 바이러스에 대한 "1차 방어선"을 제공합니다.

자세한 내용은 14 장, "신종 바이러스 필터(Outbreak Filter)"를 참조하십시오.

계속하려면 **Next(다음)**를 클릭합니다.

5단계: 검토

구성 정보에 대한 요약이 표시됩니다. **Previous(이전)** 버튼을 클릭하거나 각 섹션의 오른쪽 위에서 해당 **Edit(편집)** 링크를 클릭하여 시스템 설정, 네트워크 통합 및 메시지 보안 정보를 편집할 수 있습니다. 변경 단계로 돌아갈 경우 이 검토 페이지가 다시 나타날 때까지 나머지 단계를 진행해야 합니다. 이전에 입력한 모든 설정이 저장됩니다.

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

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

이제 어플라이언스가 이메일을 보낼 준비가 되었습니다.

참고 **Install(설치)**을 클릭하면 어플라이언스에 연결하는 데 사용한 인터페이스(C370, C670, X1070, C380, C680 어플라이언스의 관리 인터페이스 또는 C170 어플라이언스의 데이터 1 인터페이스)의 IP 주소를 기본값에서 변경한 경우 현재 URL(http://192.168.42.42)에 대한 연결이 손실됩니다. 그러나 브라우저가 새 IP 주소로 리디렉션됩니다.

시스템 설정이 완료되면 여러 경고 메시지가 전송됩니다. 자세한 내용은 즉각적인 경고, 3-36페이지를 참조하십시오.

Active Directory에 대한 연결 설정

시스템 설정 마법사가 Email Security 어플라이언스에 구성을 올바르게 설치한 경우 Active Directory 마법사가 나타납니다. 네트워크에서 Active Directory 서버를 실행 중인 경우 Active Directory 마법사를 사용하여 Active Directory 서버의 LDAP 서버 프로필을 구성하고 수신자 검증에 사용할 리스너를 할당할 수 있습니다. Active Directory를 사용하고 있지 않거나 나중에 구성하려면 **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 Directory와 다른 LDAP 프로필을 구성할 수도 있습니다.

Active Directory 마법사가 인증 방법, 포트, 기본 DN, SSL 지원 여부 등 LDAP 서버 프로필을 생성하는 데 필요한 시스템 정보를 검색합니다. Active Directory 마법사는 LDAP 서버 프로필에 대한 LDAP 수락 및 그룹 쿼리도 생성합니다.

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

절차

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

2단계 Active Directory 서버의 호스트 이름을 입력합니다.

3단계 인증 요청의 사용자 이름 및 비밀번호를 입력합니다.

4단계 계속하려면 **Next(다음)**를 클릭합니다.

Active Directory 마법사가 Active Directory 서버에 대한 연결을 테스트합니다. 테스트에 성공하면 테스트 디렉토리 설정 페이지가 표시됩니다.

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

6단계 **Done(완료)**을 클릭합니다.

다음 단계로 진행

Active Directory 마법사를 사용할 수 있도록 어플라이언스를 성공적으로 구성했거나 프로세스를 건너뛰면 시스템 설정 다음 단계 페이지가 나타납니다.

시스템 설정 다음 단계 페이지에서 링크를 클릭하여 어플라이언스 구성을 진행합니다.

CLI(Command Line Interface) 액세스

CLI에 대한 액세스는 어플라이언스에 연결, 3-9페이지에서 선택한 관리 연결 방법에 따라 다릅니다. 공장 기본 사용자 이름과 비밀번호가 다음에 표시됩니다. 처음에는 관리자 계정에만 CLI에 대한 액세스 권한이 있습니다. 관리자 계정을 통해 명령줄 인터페이스에 처음으로 액세스한 후 권한 수준이 서로 다른 기타 사용자를 추가할 수 있습니다. (사용자 추가에 대한 내용은 사용자 추가, 32-4페이지를 참조하십시오.) 시스템 설정 마법사가 관리자 계정의 비밀번호를 변경할지 묻는 메시지를 표시합니다. 비밀번호 명령을 사용하여 언제든지 직접 관리자 계정의 비밀번호를 리셋할 수도 있습니다.

이더넷을 통해 연결하려면 공장 기본 IP 주소인 192.168.42.42를 사용하여 SSH 또는 Telnet을 시작합니다. SSH는 포트 22를 사용하도록 구성되어 있습니다. 텔넷은 포트 23을 사용하도록 구성되어 있습니다. 아래에 사용자 이름과 비밀번호를 입력합니다.

직렬 연결을 통해 연결하려면 직렬 케이블이 연결된 개인 컴퓨터의 통신 포트를 사용하여 터미널 세션을 시작합니다. 어플라이언스에 연결, 3-9페이지에 설명된 직렬 포트의 설정을 사용합니다. 아래에 사용자 이름과 비밀번호를 입력합니다.

사용자 이름과 비밀번호를 입력하여 어플라이언스에 로그인합니다.

관련 주제

- 공장 기본 사용자 이름 및 비밀번호, 3-24페이지

공장 기본 사용자 이름 및 비밀번호

- 사용자 이름: **admin**
- 비밀번호: **ironport**

예를 들면 다음과 같습니다.

```
login: admin
password: ironport
```

CLI(Command Line Interface) 시스템 설정 마법사 실행

시스템 설정 마법사의 CLI 버전은 기본적으로 다음과 같은 몇 가지 사소한 예외를 제외하고 GUI 버전의 단계와 유사합니다.

- CLI 버전은 웹 인터페이스를 활성화하는 프롬프트를 포함합니다.
- CLI 버전을 사용하면 생성하는 각 리스너의 기본 메일 흐름 정책을 편집할 수 있습니다.
- CLI 버전은 전역 안티바이러스 및 신종 바이러스 필터(Outbreak Filter) 보안 설정을 구성하는 프롬프트를 포함합니다.
- CLI 버전은 시스템 설정이 완료된 후 LDAP 프로필을 생성하라는 메시지를 표시하지 않습니다. `ldapconfig` 명령을 사용하여 LDAP 프로필을 생성할 수 있습니다.

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

```
IronPort> systemsetup
```

시스템 설정 마법사가 사용자에게 시스템 재구성에 대해 경고합니다. 어플라이언스를 처음으로 설치하거나 기존 구성을 완전히 덮어쓰려면 이 질문에 "예"라고 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 나머지 시스템 설정 단계가 아래에 설명되어 있습니다. CLI 시스템 설정 마법사 대화 상자의 예는 위의 웹 기반 시스템 설정 마법사를 사용하여 기본 구성 정의, 3-14페이지에 설명된 GUI 시스템 설정 마법사에서 파생된 섹션에만 포함됩니다.

관련 주제

- 관리자 비밀번호 변경, 3-25페이지
- 라이센스 계약 동의, 3-25페이지
- 호스트 이름 설정, 3-25페이지
- 논리 IP 인터페이스 할당 및 구성, 3-25페이지

관리자 비밀번호 변경

먼저 AsyncOS 관리자 계정의 비밀번호를 변경합니다. 계속하려면 이전 비밀번호를 입력해야 합니다. 새 비밀번호는 6자 이상이어야 합니다. 비밀번호는 안전한 위치에 보관해 두십시오. 변경한 비밀번호는 시스템 설정 프로세스가 완료되면 적용됩니다.

라이센스 계약 동의

표시되는 소프트웨어 라이센스 계약을 읽고 동의합니다.

호스트 이름 설정

그런 다음 Email Security 어플라이언스의 정규화된 호스트 이름을 정의합니다. 이 이름은 네트워크 관리자가 지정해야 합니다.

논리 IP 인터페이스 할당 및 구성

다음 단계로 관리(C370, C670, X1070, C380, C680 어플라이언스) 또는 데이터 1(C170 어플라이언스)이라는 물리적 이더넷 인터페이스에서 논리 IP 인터페이스를 할당 및 구성한 다음 어플라이언스에서 사용할 수 있는 다른 물리적 이더넷 인터페이스에서 논리 IP 인터페이스를 구성합니다.

각 인터페이스에 여러 개의 IP 인터페이스를 할당할 수 있습니다. IP 인터페이스는 IP 주소 및 호스트 이름을 물리적 이더넷 인터페이스와 연결하는 논리적 구조입니다. 데이터 1 및 데이터 2 이더넷 포트를 모두 사용하기로 결정한 경우 두 연결의 IP 주소와 호스트 이름이 필요합니다.

C370, C670, X1070, C380, C680 어플라이언스의 경우: Cisco에서는 공용 리스너를 통해 인바운드 이메일을 수신하려면 물리적인 이더넷 포트 중 하나를 사용해 인터넷에 직접 연결하고, 사설 리스너를 통해 아웃바운드 이메일을 전달하려면 다른 물리적 이더넷 포트를 사용해 내부 네트워크에 직접 연결할 것을 권장합니다.

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

참고 발송 메일을 전달할 인터페이스를 구성할 경우 인터페이스를 사용하도록 구성된 공용 리스너가 없으면 시스템이 인터페이스에 대해 SSH를 활성화합니다.

다음 정보가 필요합니다.

- 나중에 IP 인터페이스를 나타내기 위해 사용자가 생성하는 **이름**(별칭). 예를 들어, 사설 네트워크에 하나의 이더넷 포트를 사용하고 공용 네트워크에 다른 이더넷 포트를 사용할 경우 이름을 각각 PrivateNet과 PublicNet으로 지정할 수 있습니다.

참고 인터페이스에 대해 정의하는 이름은 대/소문자를 구분합니다. AsyncOS에서는 2개의 동일한 인터페이스 이름을 생성할 수 없습니다. 예를 들어, **`Privatenet`** 및 **`PrivateNet`**이라는 이름은 *서로 다른* (고유한) 2개의 이름으로 간주됩니다.

- 네트워크 관리자가 할당한 **IP 주소**. IPv4 또는 IPv6 주소일 수 있으며, 두 유형의 IP 주소를 단일 IP 인터페이스에 지정할 수 있습니다.
- 인터페이스의 **넷마스크**. 넷마스크는 CIDR 형식이어야 합니다. 예를 들어, 255.255.255.0 서브넷의 경우는 `/24`를 사용합니다.

참고 동일한 서브넷 내의 IP 주소는 별도의 물리적 이더넷 인터페이스에서 구성할 수 없습니다. 네트워크 및 IP 주소 구성에 대한 자세한 내용은 부록 B, "네트워크 및 IP 주소 할당"을 참조하십시오.

참고 C170 어플라이언스의 경우 데이터 2 인터페이스를 먼저 구성합니다.

기본 게이트웨이 지정

`systemsetup` 명령의 다음 부분에서 네트워크의 기본 라우터(게이트웨이)의 IP 주소를 입력합니다.

웹 인터페이스 활성화

`systemsetup` 명령의 다음 부분에서 어플라이언스(관리 이더넷 인터페이스)의 웹 인터페이스를 활성화합니다. 보안 HTTP(`https`)를 통해 웹 인터페이스를 실행하기로 선택할 수도 있습니다. HTTPS를 사용하기로 선택할 경우 자체 인증서를 업로드할 때까지 시스템이 데모 인증서를 사용합니다. 자세한 내용은 HTTPS에 대한 인증서 활성화하기, 23-17페이지를 참고하십시오.

DNS 설정 구성

그런 다음 DNS(Domain Name Service) 설정을 구성합니다. Cisco AsyncOS에는 인터넷의 루트 서버에 직접 쿼리하거나 시스템에서 사용자의 자체 DNS 서버를 사용할 수 있는 고성능 내부 DNS 확인자/캐시가 포함되어 있습니다. 자체 서버를 사용하기로 선택할 경우 각 DNS 서버의 IP 주소와 호스트 이름을 입력해야 합니다. 필요한 만큼 DNS 서버를 입력할 수 있습니다(각 서버의 우선순위가 0으로 지정됨). 기본적으로 `systemsetup`은 자체 DNS 서버의 주소를 입력하라는 메시지를 표시합니다.

리스너 생성

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

C370, C670, X1070, C380, C680 어플라이언스의 경우: 기본적으로 `systemsetup` 명령은 2개의 리스너(고용 및 사설)를 구성합니다. (사용 가능한 리스너 유형에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 5-1페이지를 참조하십시오.)

C170 어플라이언스의 경우: 기본적으로 `systemsetup` 명령은 인터넷에서 메일을 수신하고 내부 네트워크에서 이메일을 전달하는 공용 리스너 1개를 구성합니다. C170 어플라이언스의 리스너 예, 3-31페이지를 참조하십시오.

리스너를 정의할 때 다음과 같은 특정을 지정합니다.

- 나중에 리스너를 나타내기 위해 사용자가 생성하는 **이름**(별칭). 예를 들어, 내부 시스템에서 인터넷으로 전송되는 이메일을 수락하는 리스너는 OutboundMail이라고 부를 수 있습니다.
- 이메일을 수신할 IP 인터페이스 중 1개(`systemsetup` 명령의 초기 단계에서 생성한 인터페이스)
- 이메일을 라우팅할 머신의 이름(공용 리스너만 해당). (이는 첫 번째 `smtproutes` 항목입니다. 로컬 도메인의 이메일 라우팅, 24-1페이지를 참조하십시오.)
- 공용 리스너의 SBRS(SenderBase Reputation 점수)에 따라 필터링을 활성화할지 여부. 활성화한 경우 보수적, 소극적 또는 공격적 설정을 선택하라는 메시지도 표시됩니다.
- 호스트별 속도 제한: 원격 호스트에서 수신하려는 시간당 최대 수신자 수(공용 리스너만 해당)
- 공용 리스너 또는 어플라이언스를 통해 이메일을 전달하도록 허용된 시스템의 이메일을 수신할 수신자 도메인 또는 특정 주소(사설 리스너). (이는 리스너의 첫 번째 Recipient Access Table 및 Host Access Table입니다. 자세한 내용은 발신자 그룹 구문, 7-4페이지 및 메시지를 수락할 도메인 및 사용자 추가, 8-3페이지를 참조하십시오.)

관련 주제

- 공용 리스너, 3-27페이지
- 사설 리스너, 3-30페이지
- C170 어플라이언스의 리스너 예, 3-31페이지

공용 리스너

참고 다음의 공용 및 사설 리스너 생성 예제는 C370, C670, X1070, C380, C680 어플라이언스에만 적용됩니다. C170 어플라이언스의 경우 다음 섹션인 C170 어플라이언스의 리스너 예, 3-31페이지를 건너뛰십시오.

`systemsetup` 명령의 이 예제 부분에서 InboundMail이라는 이름의 공용 리스너가 PublicNet IP 인터페이스에서 실행되도록 구성됩니다. 그런 다음 도메인 `example.com`의 모든 이메일을 수락하도록 구성됩니다. 메일 교환 `exchange.example.com`의 초기 SMTP 경로가 구성됩니다. 속도 제한이 활성화되고 단일 호스트의 시간당 최대 수신자 값인 4,500이 공용 리스너에 대해 지정됩니다.

참고 원격 호스트에서 수신하려는 시간당 최대 수신자에 대해 입력하는 값은 전적으로 임의의 값이며 일반적으로 사용자가 이메일을 관리하는 엔터프라이즈의 규모에 상대적입니다. 예를 들어, 1시간에 200개의 메시지를 보내는 발신자는 "스패머"(원치 않는 대량 이메일 발신자)로 간주될 수 있지만 직원이 10,000명인 회사의 모든 이메일을 처리하도록 Email Security 어플라이언스를 구성할 경우 시간당 원격 호스트에서 수신할 메시지 수는 200개가 적당할 수 있습니다. 반대로 50명 규모의 회사라면 시간당 200개의 메시지를 보내는 사람은 명백한 스패머일 수 있습니다. 엔터프라이즈의 공용 리스너(제한) 인바운드 이메일에 대한 속도 제한을 활성화할 경우 적절한 값을 선택해야 합니다. 기본 호스트 액세스 정책에 대한 자세한 내용은 발신자 그룹 구문, 7-4페이지를 참조하십시오.

그러면 리스너의 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.

주소가 여러 개인 경우 쉼표로 구분하십시오.

[]> 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. 항
목이 여러 개인 경우 쉼표로 구분하십시오.

[]> 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


기본 정책 설정

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

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.

*****
```

사설 리스너

systemsetup 명령의 이 예제 부분에서 OutboundMail이라는 이름의 사설 리스너가 PublicNet IP 인터페이스에서 실행되도록 구성됩니다. 그런 다음 도메인 example.com 내에서 모든 호스트의 모든 이메일을 전달하도록 구성됩니다. 항목의 시작 부분에 있는 점에 유의하십시오(.example.com).

그러면 속도 제한의 기본값(활성화되지 않음)과 이 리스너의 기본 호스트 액세스 정책이 수락됩니다.

사설 리스너의 기본값은 앞서 생성된 공용 리스너와 다릅니다. 자세한 내용은 리스너 작업, 5-2페이지를 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.

항목이 여러 개인 경우 쉼표로 구분하십시오.

[]> .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


기본 정책 설정

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

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 어플라이언스의 리스너 예

참고 다음의 리스너 생성 예제는 C170 어플라이언스에만 적용됩니다.

`systemsetup` 명령의 이 예제 부분에서 MailInterface라는 이름의 리스너가 MailNet IP 인터페이스에서 실행되도록 구성됩니다. 그런 다음 도메인 `example.com`의 모든 이메일을 수락하도록 구성됩니다. 메일 교환 `exchange.example.com`의 초기 SMTP 경로가 구성됩니다. 그런 후에 동일한 리스너가 도메인 `example.com` 내에서 모든 호스트의 모든 이메일을 전달하도록 구성됩니다. 항목의 시작 부분에 있는 점에 유의하십시오(`.example.com`).

속도 제한이 활성화되고 단일 호스트의 시간당 최대 수신자 값인 450이 공용 리스너에 대해 지정됩니다.

참고 원격 호스트에서 수신하려는 시간당 최대 수신자에 대해 입력하는 값은 전적으로 임의의 값이며 일반적으로 사용자가 이메일을 관리하는 엔터프라이즈의 규모에 상대적입니다. 예를 들어, 1시간에 200개의 메시지를 보내는 발신자는 "스패머"(원치 않는 대량 이메일 발신자)로 간주될 수 있지만 직원이 10,000명인 회사의 모든 이메일을 처리하도록 어플라이언스를 구성할 경우 시간당 원격 호스트에서 수신할 메시지 수는 200개가 적당할 수 있습니다. 반대로 50명 규모의 회사라면 시간당 200개의 메시지를 보내는 사람은 명백한 스패머일 수 있습니다. 엔터프라이즈의 공용 리스너(제한) 인바운드 이메일에 대한 속도 제한을 활성화할 경우 적절한 값을 선택해야 합니다. 기본 호스트 액세스 정책에 대한 자세한 내용은 발신자 그룹 구문, 7-4페이지를 참조하십시오.

그러면 리스너의 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.

주소가 여러 개인 경우 쉼표로 구분하십시오.

[]> 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.
항목이 여러 개인 경우 쉼표로 구분하십시오.

[]> 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.
```

```
항목이 여러 개인 경우 쉼표로 구분하십시오.

[]> .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


기본 정책 설정

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

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 어플라이언스의 인바운드 및 아웃바운드 메일 모두에 대해 1개의 리스너만 구성하므로 모든 발송 메일이 메일 흐름 모니터링 기능(일반적으로 인바운드 메시지에 사용됨)을 통해 계산됩니다. 28 장, "이메일 보안 모니터링 사용"을 참조하십시오.

안티스팸 활성화

어플라이언스에 안티스팸 소프트웨어에 대한 30일 평가 키가 포함되어 있습니다. systemsetup 명령의 이 부분에서 라이센스 계약에 동의하고 어플라이언스에서 전역적으로 안티스팸을 활성화하기로 선택할 수 있습니다.

그러면 안티스팸 검사가 수신 메일 정책에 사용됩니다.

참고 라이센스 계약에 동의하지 않으면 안티스팸이 어플라이언스에서 활성화되지 않습니다.

어플라이언스에서 사용할 수 있는 모든 안티스팸 구성 옵션은 13 장, "안티스팸"을 참조하십시오.

기본 안티스팸 검사 엔진 선택

2개 이상의 안티스팸 검사 엔진을 활성화한 경우 기본 수신 메일 정책에 사용하기 위해 활성화할 엔진을 선택하라는 메시지가 표시됩니다.

스팸 격리 활성화

안티스팸 서비스를 활성화하기로 선택할 경우 수신 메일 정책을 활성화해 스팸과 의심스러운 스팸 메시지를 로컬 스팸 격리로 보낼 수 있습니다. 스팸 격리를 활성화하면 어플라이언스에서 최종 사용자 격리도 활성화됩니다. 최종 사용자 액세스가 구성될 때까지 관리자만 최종 사용자 격리에 액세스할 수 있습니다.

로컬 스팸 격리 설정, 31-2페이지를 참조하십시오.

안티바이러스 검사 활성화

어플라이언스에 바이러스 검사 엔진에 대한 30일 평가 키가 포함되어 있습니다. systemsetup 명령의 이 부분에서 하나 이상의 라이센스 계약에 동의하고 어플라이언스에서 안티바이러스 검사를 활성화하기로 선택할 수 있습니다. 어플라이언스에서 활성화할 각 안티바이러스 검사 엔진에 대한 라이센스 계약에 동의해야 합니다.

계약에 동의하면 선택한 안티바이러스 검사 엔진이 수신 메일 정책에 사용됩니다. Email Security 어플라이언스가 수신 메일에 바이러스가 있는지 검사하지만 감염된 첨부 파일을 복구하지는 않습니다. 어플라이언스가 감염된 메시지를 삭제합니다.

어플라이언스에서 사용할 수 있는 안티바이러스 구성 옵션은 12 장, "안티바이러스"를 참조하십시오.

신종 바이러스 FiltersOutbreak 필터 및 SenderBase 이메일 트래픽 모니터링 네트워크 활성화

이 다음 단계에서 SenderBase 참여와 신종 바이러스 필터(Outbreak Filter)를 모두 활성화하라는 메시지가 표시됩니다. 어플라이언스에 신종 바이러스 필터(Outbreak Filter)에 대한 30일 평가 키가 포함되어 있습니다.

관련 주제

- 신종 바이러스 필터(Outbreak Filter), 3-35페이지
- SenderBase 참여, 3-35페이지

신종 바이러스 필터(Outbreak Filter)

신종 바이러스 필터(Outbreak Filter)는 기존의 안티바이러스 보안 서비스를 새 바이러스 서명 파일로 업데이트할 수 있을 때까지 의심스러운 메시지를 격리하여 신종 바이러스에 대한 "1차 방어선"을 제공합니다. 활성화한 경우 신종 바이러스 필터(Outbreak Filter)가 기본 수신 메일 정책에 사용됩니다.

신종 바이러스 필터(Outbreak Filter)를 활성화하기로 선택할 경우 임계값과 신종 바이러스 필터(Outbreak Filter) 경고 수신 여부를 입력합니다. 신종 바이러스 필터(Outbreak Filter)와 임계값에 대한 자세한 내용은 신종 바이러스 필터(Outbreak Filter), 14-1페이지를 참조하십시오.

SenderBase 참여

SenderBase는 이메일 관리자가 발신자를 조사하고 이메일의 정상적인 소스를 파악하고 스패머를 차단할 수 있도록 설계된 이메일 평판 서비스입니다.

사용자가 SenderBase 이메일 트래픽 모니터링 네트워크에 참여하는 데 동의할 경우 Cisco는 사용자의 조직에 전송된 이메일에 대한 집계된 통계를 수집합니다. 여기에는 메시지 특성에 대한 요약 데이터와 Email Security 어플라이언스에서 처리한 메시지 유형에 대한 정보가 포함됩니다.

자세한 내용은 35 장, "SenderBase 네트워크 참여"를 참조하십시오.

경고 설정 및 AutoSupport 구성

Cisco 사용자의 개입이 필요한 시스템 오류가 발생한 경우 AsyncOS가 이메일을 통해 사용자에게 경고 메시지를 보냅니다. 시스템 경고를 받을 이메일 주소를 최소한 하나 이상 추가합니다. 주소가 여러 개인 경우 쉼표로 구분하십시오. 사용자가 입력하는 이메일 주소는 처음에 디렉토리 수집 공격 방지 경고를 제외하고 모든 수준에서 모든 유형의 경고를 수신합니다. 나중에 CLI에서 `alertconfig` 명령을 사용하거나 GUI의 System Administration(시스템 관리) > Alerts(경고) 페이지에서 경고 구성에 더 세부적인 내용을 추가할 수 있습니다. 자세한 내용은 경고, 33-34페이지를 참고하십시오.

AutoSupport 기능을 통해 Cisco 고객 지원팀이 어플라이언스의 문제를 지속적으로 파악할 수 있으므로 Cisco에서 사용자에게 업계 최고의 지원을 제공할 수 있습니다. Cisco 지원 경고와 주별 상태 업데이트를 보내려면 "예"라고 답하십시오. (자세한 내용은 AutoSupport, 33-34페이지를 참조하십시오.)

예약 보고 구성

기본 예약 보고서를 전송할 주소를 입력합니다. 이 값을 비워 둘 수 있으며 이 경우 보고서가 이메일을 통해 전송되지 않고 어플라이언스에 아카이브됩니다.

시간 설정 구성

Cisco AsyncOS를 통해 사용자가 NTP(Network Time Protocol)를 이용해 네트워크 또는 인터넷의 다른 서버와 시간을 동기화하거나 시스템 클럭을 수동으로 설정할 수 있습니다. 또한 메시지 헤더와 로그 파일의 타임스탬프가 올바르게 표시되도록 어플라이언스에서 표준 시간대를 설정해야 합니다. Cisco 시스템 시간 서버를 사용하여 어플라이언스에서 시간을 동기화할 수도 있습니다.

대륙, 국가, 표준 시간대와 사용할 NTP 서버의 이름을 포함한 NTP 사용 여부를 선택합니다.

변경 사항 커밋

마지막으로 시스템 설정 마법사가 절차를 진행하는 동안 수행한 구성 변경을 커밋할 것인지 묻습니다. 변경 사항을 커밋하려면 "예"라고 답합니다.

시스템 설정 마법사를 성공적으로 완료한 경우 다음 메시지가 나타나고 명령 프롬프트가 표시됩니다.

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

mail3.example.com>
```

이제 어플라이언스가 이메일을 보낼 준비가 되었습니다.

구성 테스트

Cisco AsyncOS 구성을 테스트하려면 곧바로 `mailconfig` 명령을 사용하여 `systemsetup` 명령을 통해 생성한 시스템 구성 데이터가 포함된 테스트 이메일을 보낼 수 있습니다.

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send

the configuration file. 주소가 여러 개인 경우 쉼표로 구분하십시오.

[]> user@example.com


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

mail3.example.com>
```

액세스할 수 있는 사서함에 구성을 전송하여 시스템이 네트워크에서 이메일을 전송할 수 있는지 확인합니다.

즉각적인 경고

Email Security 어플라이언스는 기능 키를 사용하여 기능을 활성화합니다. 처음으로 `systemsetup` 명령을 사용해 리스너를 생성하고 안티스팸, Sophos 또는 McAfee 안티바이러스 또는 신종 바이러스 필터(Outbreak Filter)를 활성화하면 경고가 생성되어 사용자가 2단계: 시스템, 3-15페이지에서 지정한 주소로 전송됩니다.

이 경고는 사용자에게 키에 남아 있는 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 기간이 경과한 후에도 기능을 사용할 수 있는 방법은 Cisco 영업 담당자에게 문의하시시오. System Administration(시스템 관리) > Feature Keys(기능 키) 페이지를 통해 또는 `featurekey` 명령을 실행해 키에 남아 있는 시간을 확인할 수 있습니다. (자세한 내용은 기능 키, 33-5페이지를 참조하십시오.)

시스템을 엔터프라이즈 게이트웨이로 구성

시스템을 엔터프라이즈 게이트웨이(인터넷에서 이메일 수락)로 구성하려면 먼저 이 장을 완료한 다음 5 장, "이메일을 수신하도록 게이트웨이 구성"에서 자세한 내용을 확인하십시오.

구성 및 다음 단계 확인

이제 시스템 설정이 완료되었으며 Email Security 어플라이언스가 이메일을 보내고 받을 수 있어야 합니다. 안티바이러스, 안티스팸 및 신종 바이러스 필터(Outbreak Filter) 보안 기능을 활성화한 경우 시스템이 수신 및 발송 메일에 스팸 및 바이러스가 있는지도 검사합니다.

다음 단계는 어플라이언스의 구성을 사용자 지정하는 방법을 이해하는 것입니다. 4 장, "이메일 파이프라인 이해"에 시스템을 통해 이메일을 라우팅하는 방법에 대한 자세한 개요가 나와 있습니다. 각 기능은 순서대로(처음부터 끝까지) 처리되며 이 설명서의 나머지 장에 설명되어 있습니다.

이메일 파이프라인 이해

이메일 파이프라인 개요

이메일 파이프라인은 어플라이언스에서 처리되는 이메일의 흐름입니다. 이메일 파이프라인은 다음 3가지 단계로 구성됩니다.

- 수신 - 어플라이언스가 수신 이메일을 받기 위해 원격 호스트에 연결할 때 구성된 제한과 기타 수신 정책을 준수합니다. 예를 들어, 수신 연결 및 메시지 제한을 적용하고 메시지의 수신자를 검증하여 호스트가 사용자 메일을 전송할 수 있는지 확인합니다.
- 작업 큐 - 어플라이언스가 필터링, 허용 목록/차단 목록 검사, 안티스팸 및 안티바이러스 검사, 신종 바이러스 필터(Outbreak Filter) 및 격리와 같은 작업을 수행하여 수신 및 발송 메일을 처리합니다.
- 전송 - 어플라이언스가 발송 이메일을 전송하기 위해 연결할 때 구성된 전송 제한 및 정책을 준수합니다. 예를 들어, 아웃바운드 연결 제한을 적용하고 전송할 수 없는 메시지를 지정된 대로 처리합니다.

이메일 파이프라인 흐름

그림 4-1, 그림 4-1 및 그림 4-3에서는 수신에서 라우팅 및 전송에 이르기까지 이메일이 시스템을 통해 처리되는 방식에 대한 개요를 제공합니다. 각 기능이 순서대로(위에서 아래로) 처리됩니다. `trace` 명령을 사용하여 이 파이프라인에서 기능의 구성을 대부분 테스트할 수 있습니다.

그림 4-1 이메일 파이프라인 - 이메일 연결 수신

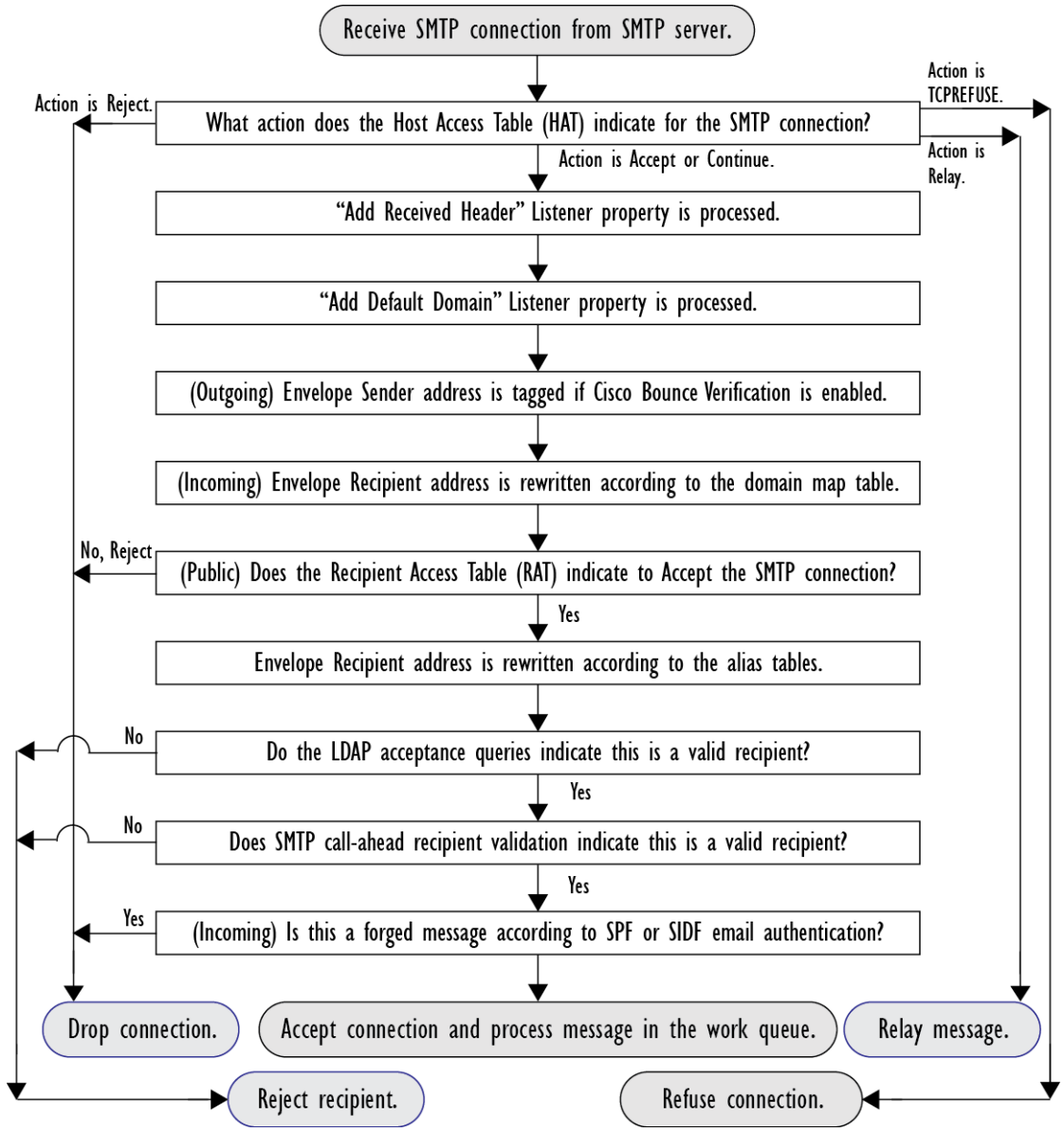


그림 4-2 이메일 파이프라인 - 작업 큐

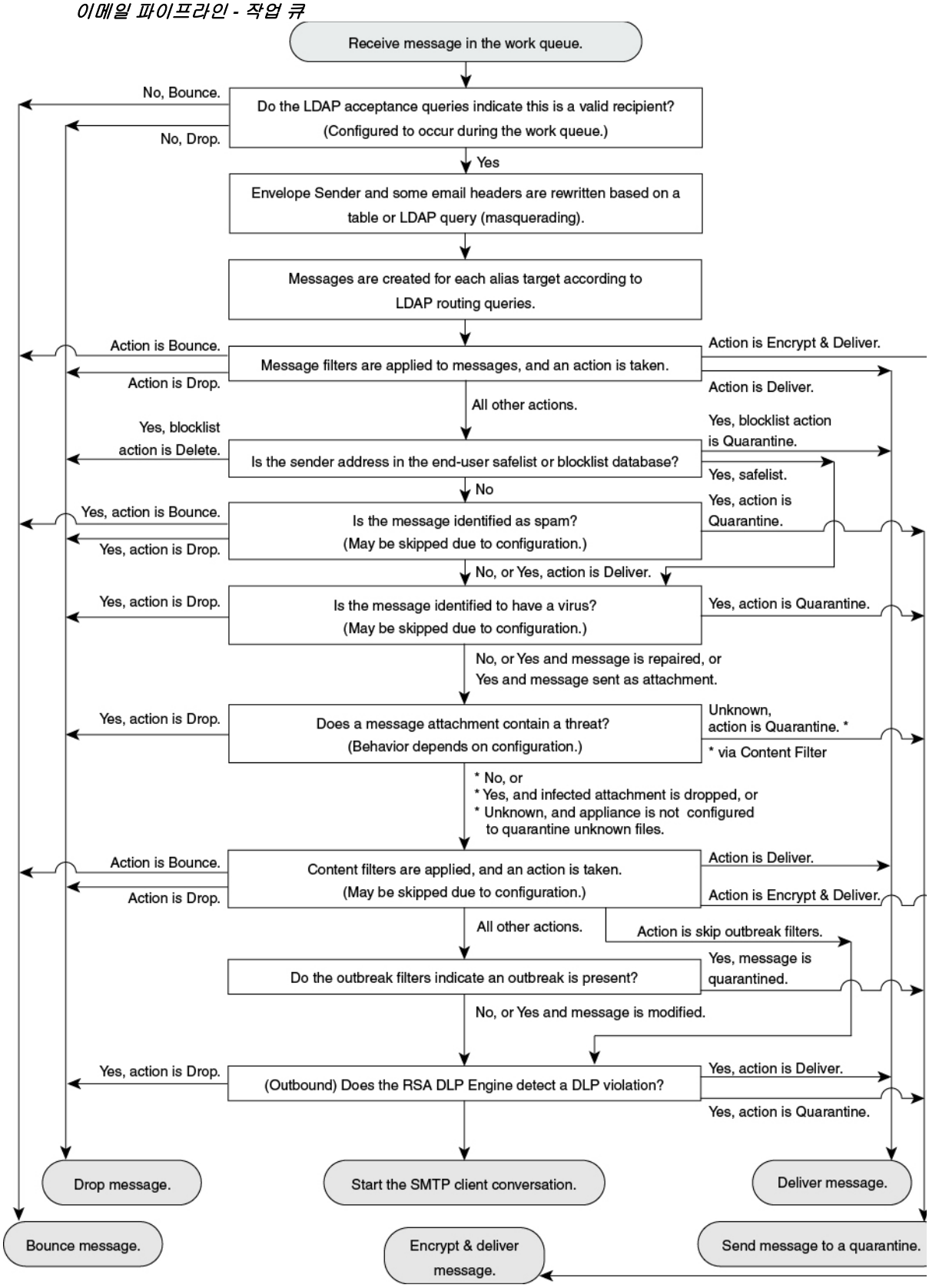
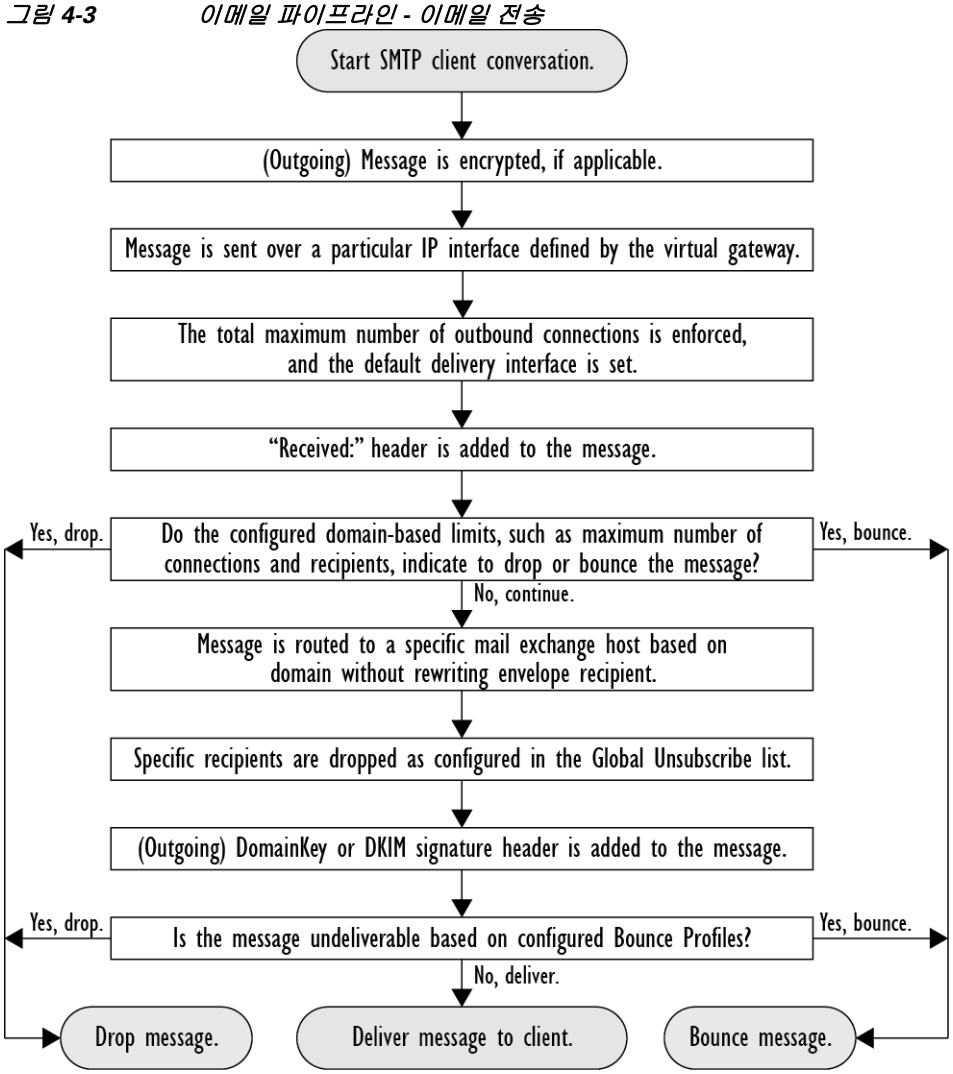


그림 4-3 이메일 파이프라인 - 이메일 전송



수신/수신

이메일 파이프라인의 수신 단계에는 발신자 호스트에서의 초기 연결이 포함됩니다. 각 메시지 도메인을 설정할 수 있으며 수신자를 확인하고 메시지가 작업 큐로 전달합니다.

관련 주제

- HAT(Host Access Table), 발신자 그룹 및 메일 흐름 정책, 4-5페이지
- 수신됨: 헤더, 4-5페이지
- 기본 도메인, 4-5페이지
- 바운스 확인, 4-5페이지
- 도메인 맵, 4-6페이지
- Recipient Access Table (RAT), 4-6페이지
- 별칭 테이블, 4-6페이지

- LDAP 수신자 수락, 4-6페이지
- SMTP Call-Ahead 수신자 검증, 4-6페이지

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

HAT를 통해 리스너에 연결할 수 있는 호스트를 지정할 수 있습니다(즉, 이메일 전송을 허용할 호스트).

발신자 그룹은 한 명 이상의 발신자를 그룹에 연결하는 데 사용되며, 사용자는 이 그룹에 메시지 필터와 다른 메일 흐름 정책을 적용할 수 있습니다. 메일 흐름 정책은 HAT 매개변수 그룹(액세스 규칙, 그 이후에 나오는 속도 제한 매개변수 및 사용자 지정 SMTP 코드 및 응답)을 표현하는 방식입니다.

또한 발신자 그룹과 메일 흐름 정책은 리스너의 HAT에 정의됩니다.

발신자 그룹의 호스트 DNS 확인 설정을 통해 SMTP 대화 전에 확인되지 않은 발신자를 분류하고, 다양한 발신자 그룹의 여러 유형의 확인되지 않은 발신자를 포함할 수 있습니다.

연결 호스트는 SMTP 대화 전에 발신자 그룹의 호스트 DNS 확인을 거치나, 봉투 발신자의 도메인 부분은 메일 흐름 정책에서 DNS 확인을 거치고 SMTP 대화 도중 확인이 이루어집니다. 형식이 올바르지 않은 봉투 발신자 메시지는 무시될 수 있습니다. 발신자 확인 예외 테이블에 항목을 추가할 수 있습니다. 발신자 확인 예외 테이블이란 봉투 발신자 DNS 확인 설정에 관계없이 메일을 수락하거나 거부하기 위한 도메인 및 이메일 주소 목록입니다.

발신자 평판 필터링을 통해 이메일 발신자를 분류하고 Cisco SenderBase Reputation Service에서 결정한 대로 발신자의 신뢰성에 따라 이메일 인프라에 대한 액세스를 제한합니다.

자세한 내용은 사전 정의 발신자 그룹 및 메일 흐름 정책 이해, 7-11페이지를 참고하십시오.

수신됨: 헤더

`listenerconfig` 명령을 사용하여 리스너가 수신하는 모든 메시지에 수신됨: 헤더를 기본적으로 포함하지 않도록 리스너를 구성할 수 있습니다.

자세한 내용은 "리스너 사용자 지정" 장의 "고급 구성 옵션"을 참조하십시오.

기본 도메인

자격 증명 도메인 이름을 포함하지 않는 발신자 주소에 기본 도메인을 자동으로 첨부하도록 리스너를 구성할 수 있습니다. 이러한 주소를 "베어" 주소라고도 합니다 (예: "joe" 대 "joe@example.com" 등).

자세한 내용은 "리스너 사용자 지정" 장의 "SMTP 주소 분석 옵션"을 참조하십시오.

바운스 확인

발송 메일에는 특수 키로 태그되므로 해당 메일이 바운스로 다시 전송될 경우 태그가 인식되어 메일이 전송됩니다. 자세한 내용은 "라우팅 및 전송 기능 구성" 장의 "바운스 확인"을 참조하십시오.

도메인 맵

사용자가 구성하는 각 리스너에 대해 도메인 맵 테이블의 도메인과 일치하는 메시지의 각 수신자에 대한 봉투 수신자를 재작성하는 도메인 맵 테이블을 생성할 수 있습니다. 예를 들어, joe@old.com을 joe@new.com으로 지정할 수 있습니다.

자세한 내용은 "라우팅 및 전송 기능 구성" 장의 "도메인 맵 기능"을 참조하십시오.

Recipient Access Table (RAT)

인바운드 이메일 전용의 경우 RAT를 사용하여 어플라이언스가 메일을 수락할 모든 로컬 도메인의 목록을 지정할 수 있습니다.

자세한 내용은 수신자의 주소에 따라 연결 수락 또는 거부 개요, 8-1페이지를 참고하십시오.

별칭 테이블

별칭 테이블에서는 한 명 이상의 수신자에게 메시지를 리디렉션하는 메커니즘을 제공합니다. 별칭은 매핑 테이블에 저장됩니다. 이메일의 봉투 수신자(Envelope To 또는 RCPT TO라고도 함)가 별칭 테이블에 정의된 별칭과 일치할 경우 이메일의 봉투 수신자 주소가 재작성됩니다.

별칭 테이블에 대한 자세한 내용은 "라우팅 및 전송 기능 구성" 장의 "별칭 테이블 생성"을 참조하십시오.

LDAP 수신자 수락

기존 LDAP 인프라를 사용하여 SMTP 대화 도중 또는 작업 큐 내에서 (공용 리스너의) 수신 메시지의 수신자 이메일 주소를 처리하는 방식을 정의할 수 있습니다. "리스너 사용자 지정" 장의 "쿼리 수락"을 참조하십시오. 이를 통해 어플라이언스가 고유한 방식으로 디렉토리 수집 공격(DHAP, directory harvest attacks)을 차단할 수 있습니다. 즉, 시스템이 메시지를 수락하고 SMTP 대화 또는 작업 큐 내에서 LDAP 수락 검증을 수행합니다. 수신자가 LDAP 디렉토리에 없는 경우 지연된 바운스를 수행하거나 메시지를 완전히 삭제하도록 시스템을 구성할 수 있습니다.

자세한 내용은 "LDAP 쿼리" 장을 참조하십시오.

SMTP Call-Ahead 수신자 검증

SMTP call-ahead 수신자 검증을 수행하도록 Email Appliance 어플라이언스를 구성할 경우 Email Appliance 어플라이언스가 수신자를 확인하기 위해 SMTP 서버를 "미리 호출"하는 동안 전송 MTA와의 SMTP 대화를 일시 중지합니다. 어플라이언스가 SMTP 서버에 쿼리하면 SMTP 서버의 응답을 Email Appliance 어플라이언스에 반환합니다. Email Appliance 어플라이언스가 SMTP 대화를 다시 시작하고 전송 MTA에 응답을 보내, SMTP 서버 응답(및 SMTP Call-Ahead 프로필에 구성한 설정)에 따라 대화가 계속되거나 연결이 삭제될 수 있습니다.

자세한 내용은 22 장, "SMTP 서버를 사용하여 수신자 검증"을 참조하십시오.

작업 큐/라우팅

작업 큐는 수신된 메시지가 전송 단계로 이동하기 전에 처리되는 곳입니다. 처리에는 마스커레이드, 라우팅, 필터링, 허용 목록/차단 목록 검사, 안티스팸 및 안티바이러스 검사, 파일 평판 검사 및 분석, 신종 바이러스 필터(Outbreak Filter) 및 격리가 포함됩니다.

참고 데이터 손실 방지(data loss prevention, DLP) 검사는 발송 메시지에만 사용할 수 있습니다. 작업 큐에서 DLP 메시지 검사가 이루어지는 위치에 대한 자세한 내용은 메시지 분리, 10-5페이지를 참조하십시오.

관련 주제

- 이메일 파이프라인 및 보안 서비스, 4-7페이지
- LDAP 수신자 수락, 4-8페이지
- 마스커레이드 또는 LDAP 마스커레이드, 4-8페이지
- LDAP 라우팅, 4-8페이지
- 메시지 필터, 4-8페이지
- Email Security Manager(수신자별 검사), 4-8페이지
- 격리, 4-10페이지

이메일 파이프라인 및 보안 서비스

일반적으로 보안 서비스(안티스팸 검사, 안티바이러스 검사 및 신종 바이러스 필터(Outbreak Filter) 변경은 작업 큐에 이미 있는 메시지에 영향을 미치지 않습니다. 예를 들면 다음과 같습니다.

메시지가 다음과 같은 이유 중 하나로 파이프라인에 처음 들어갈 때 안티바이러스 검사를 우회할 경우:

- 안티바이러스 검사를 어플라이언스에 대해 전역적으로 활성화하지 않았음
- HAT 정책이 안티바이러스 검사를 건너뛰었음
- 메시지가 안티바이러스 검사를 우회하게 한 메시지 필터가 있었음

안티바이러스 검사가 다시 활성화되었는지 여부와 관계없이 메시지가 격리에서 릴리스될 때 안티바이러스 검사를 거치지 않습니다. 그러나 메시지가 격리에 있을 때 메일 정책의 설정이 변경되었을 수 있으므로 메일 정책에 의해 안티바이러스 검사를 우회하는 메시지가 격리에서 릴리스될 때 안티바이러스 검사를 거칠 수 있습니다. 예를 들어, 메일 정책에 의해 메시지가 안티바이러스 검사를 우회하고 격리되었는데 격리에서 릴리스되기 전에 안티바이러스 검사를 포함하도록 메일 정책이 업데이트된 경우, 메시지가 격리에서 릴리스될 때 안티바이러스 검사를 거치게 됩니다.

마찬가지로, 부주의로 안티스팸 검사를 전역적으로(또는 HAT 내에서) 비활성화했는데, 메일이 작업 큐에 들어간 후에 이를 알아차린다고 가정해 보십시오. 이 시점에서 안티스팸을 활성화하면 작업 큐의 메시지가 안티스팸 검사를 받지 않게 됩니다.

LDAP 수신자 수락

기존 LDAP 인프라를 사용하여 SMTP 대화 도중 또는 작업 큐 내에서 (공용 리스너의) 수신 메시지의 수신자 이메일 주소를 처리하는 방식을 정의할 수 있습니다. "리스너 사용자 지정" 장의 "쿼리 수락"을 참조하십시오. 이를 통해 어플라이언스가 고유한 방식으로 DHAP(디렉토리 수집 공격)를 차단할 수 있습니다. 즉, 시스템이 메시지를 수락하고 SMTP 대화 또는 작업 큐 내에서 LDAP 수락 검증을 수행합니다. 수신자가 LDAP 디렉토리에 없는 경우 지연된 바운스를 수행하거나 메시지를 완전히 삭제하도록 시스템을 구성할 수 있습니다.

자세한 내용은 "LDAP 쿼리" 장을 참조하십시오.

마스커레이드 또는 LDAP 마스커레이드

마스커레이드는 봉투 발신자(발신자 또는 메일 보내는 사람이라고도 함)와 사용자가 생성하는 테이블에 따라 사설 또는 공용 리스너에서 처리하는 이메일의 받는 사람:, 보내는 사람: 및/또는 CC: 헤더를 재작성하는 기능입니다. 정적 매핑 테이블 또는 LDAP 쿼리를 통해 각 리스너에 대해 다양한 마스커레이드 매개변수를 지정할 수 있습니다.

정적 매핑 테이블을 통한 마스커레이드에 대한 자세한 내용은 "라우팅 및 전송 기능 구성" 장의 "마스커레이드 구성"을 참조하십시오.

LDAP 쿼리를 통한 마스커레이드에 대한 자세한 내용은 "LDAP 쿼리" 장을 참조하십시오.

LDAP 라우팅

네트워크의 LDAP 디렉토리에서 제공되는 정보에 따라 메시지를 해당 주소 및/또는 메일 호스트로 라우팅하도록 어플라이언스를 구성할 수 있습니다.

자세한 내용은 "LDAP 쿼리" 장을 참조하십시오.

메시지 필터

메시지 필터를 사용하여 메시지 수신 시 메시지와 첨부 파일을 처리하는 방법을 설명하는 특별 규칙을 생성할 수 있습니다. 필터 규칙은 메시지 또는 첨부 파일의 내용, 네트워크, 메시지 봉투, 메시지 헤더 또는 메시지 본문에 대한 정보에 따라 메시지를 식별합니다. 필터 작업을 통해 메시지가 삭제, 바운스, 아카이브, 격리, 숨은 참조 또는 변경될 수 있습니다.

자세한 내용은 "메시지 필터를 사용하여 이메일 정책 적용" 장을 참조하십시오.

이 단계 후에 그리고 Email Security Manager 전에 다중 수신자 메시지가 "분할됩니다". 메시지 분할은 Email Security Manager를 통해 처리할 수 있도록 단일 수신자의 이메일 조각 사본을 생성하는 것을 나타냅니다.

Email Security Manager(수신자별 검사)

- 허용 목록/차단 목록 검사, 4-9페이지
- 안티스팸, 4-9페이지
- 안티바이러스, 4-9페이지
- 파일 평판 검사 및 파일 분석, 4-9페이지

- 콘텐츠 필터, 4-10페이지
- 신종 바이러스 필터(Outbreak Filter), 4-10페이지

허용 목록/차단 목록 검사

최종 사용자 허용 목록 및 차단 목록은 최종 사용자가 생성하며 안티스팸 검사 전에 확인된 데이터베이스에 저장됩니다. 각 최종 사용자가 항상 스팸으로 처리하거나 스팸으로 처리하지 않을 도메인, 하위 도메인 또는 이메일 주소를 식별할 수 있습니다. 발신자 주소가 최종 사용자의 허용 목록에 있는 경우에는 안티스팸 검사가 생략되고, 반면 발신자 주소가 차단 목록에 있는 경우에는 관리자 설정에 따라 메시지가 격리되거나 삭제될 수 있습니다. 허용 목록 및 차단 목록 구성에 대한 자세한 내용은 "스팸 격리" 장을 참조하십시오.

안티스팸

안티스팸 검사는 인터넷 전반에 걸친 완벽한 서버 측 안티스팸 보호를 제공합니다. 또한 스팸 공격으로 인해 사용자가 불편을 겪고 네트워크에 부담 또는 손상을 주기 전에 스팸 공격을 적극적으로 식별하고 제거하므로 스팸 공격이 사용자의 받은 편지함에 도달하기 전에 개인정보 보호를 위반하지 않고 원하지 않는 메일을 제거할 수 있습니다.

메일을 스팸 격리로 전송하도록 안티스팸 검사를 구성할 수 있습니다(온박스 또는 오프박스). 스팸 격리에서 릴리스된 메시지가 대상 큐로 바로 가기 때문에 이메일 파이프라인의 추가 작업 큐 처리가 생략됩니다.

자세한 내용은 13 장, "안티스팸"을 참조하십시오.

안티바이러스

어플라이언스에 통합 바이러스 검사 엔진이 포함되어 있습니다. "메일별 정책"에 따라 메시지 및 첨부 파일 바이러스 검사를 수행하도록 어플라이언스를 구성할 수 있습니다. 바이러스가 발견될 경우 다음과 같은 작업을 수행하도록 어플라이언스를 구성할 수 있습니다.

- 첨부 파일 복구 시도
- 첨부 파일 삭제
- 제목 헤더 수정
- 추가 X-헤더 추가
- 다른 주소 또는 메일호스트로 메시지 전송
- 메시지 아카이브
- 메시지 삭제

격리에서 릴리스된 메시지(격리, 4-10페이지 참조)는 바이러스 검사를 거칩니다. 안티바이러스 검사에 대한 자세한 내용은 12 장, "안티바이러스"를 참조하십시오.

파일 평판 검사 및 파일 분석

메시지 첨부 파일에 새로운 위협 및 표적 위협이 있는지 검사하도록 어플라이언스를 구성할 수 있습니다. 사용 가능한 작업은 안티바이러스 검사와 유사합니다.

자세한 내용은 16 장, "파일 평판 필터링 및 파일 분석"을 참조하십시오.

콘텐츠 필터

수신자별 또는 발신자별로 메시지에 적용할 콘텐츠 필터를 생성할 수 있습니다. 콘텐츠 필터는 이메일 파이프라인에서 나중에(일치하는 각 Email Security Manager 정책에 따라 메시지가 여러 개의 개별 메시지로 "분할된" 후에) 적용된다는 점을 제외하고 메시지 필터와 유사합니다. 콘텐츠 필터 기능은 메시지에 대해 메시지 필터 처리와 안티스팸 및 안티바이러스 검사가 수행된 후에 적용됩니다.

콘텐츠 필터에 대한 자세한 내용은 콘텐츠 필터 개요, 11-1페이지를 참조하십시오.

신종 바이러스 필터(Outbreak Filter)

Cisco의 신종 바이러스 필터(Outbreak Filter) 기능에는 신종 바이러스에 대한 중요한 첫 번째 방어층을 제공하기 위해 능동적으로 작용하는 특수 필터가 포함됩니다. Cisco에서 게시한 신종 바이러스 규칙에 따라 특정 파일 유형의 첨부 파일이 포함된 메시지가 신종 바이러스라는 이름의 격리로 전송될 수 있습니다.

신종 바이러스 격리 내 메시지는 격리의 다른 메시지와 마찬가지로 처리됩니다. 격리 및 작업 큐에 대한 자세한 내용은 격리, 4-10페이지를 참조하십시오.

자세한 내용은 14 장, "신종 바이러스 필터(Outbreak Filter)"를 참조하십시오.

격리

수신 또는 발송 메시지를 필터링하고 격리에 보관할 수 있습니다. 격리는 메시지 보류 및 처리에 사용되는 특별 큐 또는 저장소입니다. 격리 내 메시지는 사용자가 격리를 구성하는 방식에 따라 전송되거나 삭제될 수 있습니다.

다음 작업 큐 기능을 사용하여 메시지를 격리로 전송할 수 있습니다.

- 스팸 필터
- 메시지 필터
- 안티바이러스
- 신종 바이러스 필터(Outbreak Filter)
- 콘텐츠 필터
- 파일 분석(Advanced Malware Protection)

격리에서 전송된 메시지는 위협이 있는지 다시 검사합니다.

관련 주제

- 30 장, "정책, 바이러스 및 신종 바이러스 격리"
- 31 장, "스팸 격리"

전송

이메일 파이프라인의 전송 단계는 연결, 바운스 및 수신자 제한을 포함한 이메일 처리의 마지막 단계에 초점을 맞춥니다.

관련 주제

- 가상 게이트웨이, 4-11페이지
- 전송 제한, 4-11페이지

가상 게이트웨이

가상 게이트웨이 기술을 통해 사용자가 어플라이언스를 이메일을 주고받을 여러 가상 게이트웨이 주소로 나눌 수 있습니다. 각 가상 게이트웨이 주소에는 고유한 IP 주소, 호스트 이름 및 도메인, 이메일 전송 큐가 지정됩니다.

자세한 내용은 "라우팅 및 전송 기능 구성" 장의 "가상 게이트웨이 사용"을 참조하십시오.

전송 제한

`deliveryconfig` 명령을 사용하여 전송 시 사용할 IP 인터페이스와 어플라이언스가 아웃바운드 메시지 전송에 대해 구성하는 최대 동시 연결 수에 따라 전송에 대한 제한을 설정할 수 있습니다.

자세한 내용은 "라우팅 및 전송 기능 구성" 장의 "이메일 전송 매개변수 설정"를 참조하십시오.

도메인 기반 제한

각 도메인에 대해 지정된 기간 동안 시스템이 절대 초과하지 않을 최대 연결 및 수신자 수를 지정할 수 있습니다. "양호한 인접" 테이블은 Mail Policies(메일 정책) > Destination Controls(대상 제어) 페이지(또는 `destconfig` 명령)를 통해 정의됩니다.

자세한 내용은 "라우팅 및 전송 기능 구성" 장의 "이메일 전송 제어"를 참조하십시오.

도메인 기반 라우팅

Network(네트워크) > SMTP Routes(SMTP 경로) 페이지(또는 `smtproutes` 명령)를 사용하여 봉투 수신자를 다시 작성하지 않고 특정 도메인의 모든 이메일을 특정 MX(메일 교환) 호스트로 리디렉션할 수 있습니다.

자세한 내용은 "라우팅 및 전송 기능 구성" 장의 "로컬 도메인의 이메일 라우팅"을 참조하십시오.

전역 가입 취소

전역 가입 취소를 사용하여 특정 수신자, 수신자 도메인 또는 IP 주소가 어플라이언스에서 절대 메시지를 수신하지 못하도록 할 수 있습니다. 전역 가입 취소를 활성화하면 시스템에서 "전역 가입 취소된" 사용자, 도메인, 이메일 주소 및 IP 주소 목록을 기준으로 모든 수신자 주소를 확인합니다. 일치하는 이메일은 전송되지 않습니다.

자세한 내용은 "라우팅 및 전송 기능 구성" 장의 "전역 가입 취소 사용"을 참조하십시오.

바운스 제한

Network(네트워크) > Bounce Profiles(바운스 프로필) 페이지(또는 `bounceconfig` 명령)를 사용하여 AsyncOS에서 사용자가 생성하는 각 리스너의 하드 및 소프트 대화 바운스를 처리하는 방식을 구성할 수 있습니다. 바운스 프로필을 생성한 다음 Network(네트워크) > Listeners(리스너) 페이지(또는 `listenerconfig` 명령)를 사용하여 각 리스너에 프로필을 적용합니다. 또한 메시지 필터를 사용하여 특정 메시지에 바운스 프로필을 할당할 수 있습니다.

바운스 프로필에 대한 자세한 내용은 "라우팅 및 전송 기능 구성"장의 "바운스된 이메일 전달"을 참조하십시오.

5 장

이메일을 수신하도록 게이트웨이 구성

이메일을 수신하도록 게이트웨이 구성 개요

이 어플라이언스는 조직의 이메일 게이트웨이 역할을 하면서, 이메일 연결을 서비스하고 메시지를 수락하여 적절한 시스템으로 릴레이합니다. 어플라이언스는 인터넷에서 네트워크 내 수신자 호스트로, 그리고 네트워크 내 시스템에서 인터넷으로 이메일 연결을 서비스할 수 있습니다. 일반적으로 이메일 연결 요청에서는 SMTP(Simple Mail Transfer Protocol)를 사용합니다. 어플라이언스는 기본적으로 SMTP 연결을 서비스하고, 네트워크용 메일 교환기 또는 "MX"라고도 하는 SMTP 게이트웨이로 동작합니다.

이 어플라이언스는 *리스너*를 사용하여 수신 SMTP 연결 요청을 서비스하고, 리스너는 특정 IP 인터페이스에서 구성된 이메일 처리 서비스를 설명합니다. 리스너는 인터넷에서 또는 네트워크 내의 인터넷 연결을 시도하는 시스템에서 어플라이언스로 들어오는 이메일에 적용됩니다. 리스너를 사용하여 메시지 및 연결이 허용되고 메시지가 수신자 호스트로 릴레이되기 위해 만족해야 하는 기준을 지정합니다. 리스너는 지정된 각 IP 주소의 특정 포트에서 실행되는 "SMTP 데몬"으로 간주할 수 있습니다. 또한, 리스너는 이메일을 어플라이언스로 보내려하는 시스템과 어플라이언스의 통신 방식을 정의합니다.

다음과 같은 유형의 리스너를 만들 수 있습니다.

- **공용.** 인터넷에서 들어오는 이메일 메시지를 수신 대기하고 수락합니다. 공용 리스너는 많은 호스트에서 연결을 수신하고 메시지를 제한된 수의 수신자로 보냅니다.
- **개인.** 네트워크 내 시스템, 일반적으로 인터넷 네트워크 외부의 수신자를 위한 내부 그룹웨어 및 이메일 서버(POP/IMAP)에서 들어오는 이메일 메시지를 수신 대기하고 수락합니다. 개인 리스너는 제한된(알려진) 수의 호스트에서 연결을 수신하여 메시지를 여러 수신자에게 보냅니다.

리스너를 생성할 때는 다음 정보를 지정해야 합니다.

- **리스너 속성.** 모든 리스너에 적용되는 전역 속성 및 리스너별 속성을 정의합니다. 예를 들어 리스너에 사용할 IP 인터페이스 및 포트를 지정할 수 있고, 공용 리스너 또는 개인 리스너로 지정할 수 있습니다. 이를 수행하는 방법에 대한 자세한 내용은 리스너 작업, 5-2페이지 항목을 참조하십시오.

- **리스너로의 연결이 허용되는 호스트.** 원격 호스트에서 들어오는 연결을 제어하는 규칙 집합을 정의합니다. 예를 들어 원격 호스트를 정의하고 해당 원격 호스트의 리스너 연결 가능 여부를 정의할 수 있습니다. 이를 수행하는 방법에 대한 자세한 내용은 HAT(Host Access Table)를 사용하여 연결할 수 있는 호스트 정의, 7-1페이지 항목을 참조하십시오.
- **(공용 리스너에만 해당) 리스너가 메시지를 수락하는 로컬 도메인.** 공용 리스너가 허용하는 수신자를 정의합니다. 예를 들어 조직에서 현재 `currentcompany.com` 도메인을 사용하고 있지만, 이전에는 `oldcompany.com`을 사용한 경우 `currentcompany.com`과 `oldcompany.com` 메시지를 모두 수락할 수 있습니다. 이를 수행하는 방법에 대한 자세한 내용은 도메인 이름 또는 수신자 주소에 따라 연결 수락 또는 거부, 8-1페이지 항목을 참조하십시오.

Host Access Table 및 Recipient Access Table을 비롯하여 리스너에 구성된 설정은 SMTP 대화 중에 SMTP 서버와 리스너의 통신 방식에 영향을 미칩니다. 이를 통해 어플라이언스는 연결이 종료되기 전에 스팸 발송 호스트를 차단할 수 있습니다.

그림 5-1 리스너, IP 인터페이스 및 물리적 이더넷 인터페이스와의 관계

리스너 작업

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

모든 리스너에 적용되는 전역 설정을 정의할 수 있습니다. 자세한 내용은 리스너의 전역 설정 구성, 5-4페이지 항목을 참조하십시오.

어플라이언스에서 리스너를 사용하고 리스너를 구성하는 경우 다음과 같은 규칙과 지침을 고려하십시오.

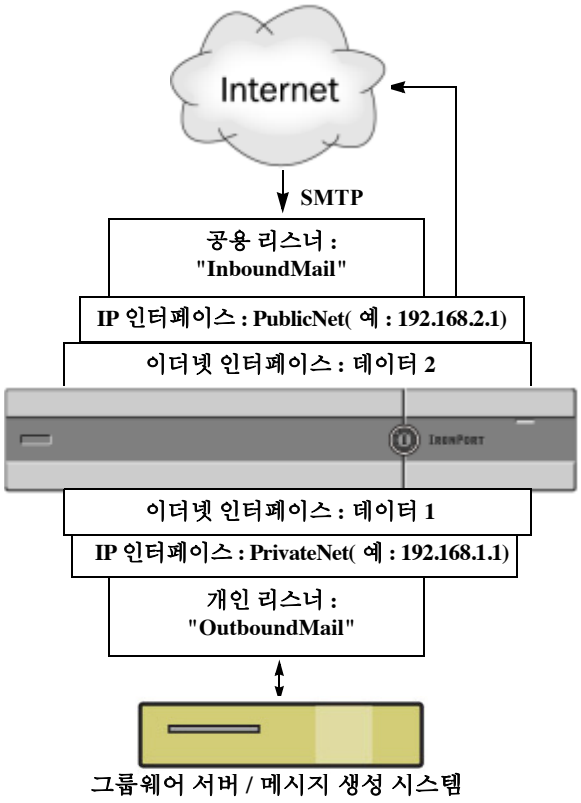
- 구성된 IP 인터페이스별로 여러 리스너를 정의할 수 있지만, 리스너마다 각기 다른 포트를 사용해야 합니다.
- 기본적으로 리스너는 이메일 연결을 서비스하는 메일 프로토콜로 SMTP를 사용합니다. 그러나 QMQP(Quick Mail Queuing Protocol)를 사용하여 이메일 연결을 서비스하도록 어플라이언스를 구성할 수도 있습니다. 이를 위해서는 `listenerconfig` CLI 명령을 사용합니다.
- 리스너는 인터넷 프로토콜 버전 4(IPv4) 및 버전 6(IPv6) 주소를 모두 지원합니다. 하나의 리스너에서 하나의 프로토콜 버전을 사용하거나 두 가지 모두를 사용할 수도 있습니다. 리스너는 메일 전송을 위해 연결 호스트와 동일한 프로토콜 버전을 사용합니다. 예를 들어 리스너가 IPv4 및 IPv6 모두를 사용하도록 구성되어 있고 IPv6을 사용하는 호스트에 연결되면, 리스너는 IPv6을 사용합니다. 그러나 IPv6 주소만 사용하도록 구성된 리스너는 IPv4 주소만 사용하는 호스트에 연결될 수 없습니다.
- 시스템 설치 마법사를 실행한 후에는 적어도 하나의 리스너(기본값 사용)를 어플라이언스에 구성해야 합니다. 그러나 리스너를 수동으로 생성하는 경우 AsyncOS는 이러한 기본 SBRS 값을 사용하지 않습니다.

- **C170 어플라이언스:** 기본적으로 시스템 설치 마법사는 인터넷에서 메일을 수신하고 내부 네트워크의 이메일을 릴레이할 수 있는 하나의 공용 리스너를 구성하는 과정을 안내합니다. 즉, 하나의 리스너로 두 가지 기능을 모두 수행할 수 있습니다.
- 어플라이언스를 테스트하고 문제를 해결하기 위해서는 공용 또는 개인 리스너 대신 "블랙홀" 유형의 리스너를 생성합니다. 블랙홀 리스너를 생성하는 경우 메시지를 삭제하기 전에 디스크에 기록할지 여부를 선택합니다. (자세한 내용은 "테스트 및 문제 해결" 장을 참조하십시오.) 메시지를 삭제하기 전에 디스크에 쓰도록 설정하면 수신율 및 큐 속도를 측정할 수 있습니다. 메시지를 디스크에 쓰지 않도록 설정하면 메시지 생성 시스템의 순수 수신율을 측정할 수 있습니다. 이 리스너 유형은 CLI의 `listenerconfig` 명령을 통해서만 사용할 수 있습니다.

그림 5-2에서는 2개 이상의 이더넷 인터페이스가 있는 어플라이언스 모델에서 시스템 설치 마법사에 의해 생성된 일반적인 이메일 게이트웨이 구성을 보여줍니다. 한 인터페이스에서 인바운드 연결을 처리하는 공용 리스너와 두 번째 IP 인터페이스에서 아웃바운드 연결을 처리하는 개인 리스너, 총 2개의 리스너가 생성되었습니다.

그림 5-3에서는 2개의 이더넷 인터페이스만 있는 어플라이언스 모델에서 시스템 설치 마법사에 의해 생성된 일반적인 이메일 게이트웨이 구성을 보여줍니다. 단일 IP 인터페이스에서 인바운드 연결과 아웃바운드 연결을 모두 처리하는 하나의 공용 리스너가 생성되었습니다.

그림 5-2 2개 이상의 이더넷 인터페이스가 있는 어플라이언스 모델의 공용 및 개인 리스너

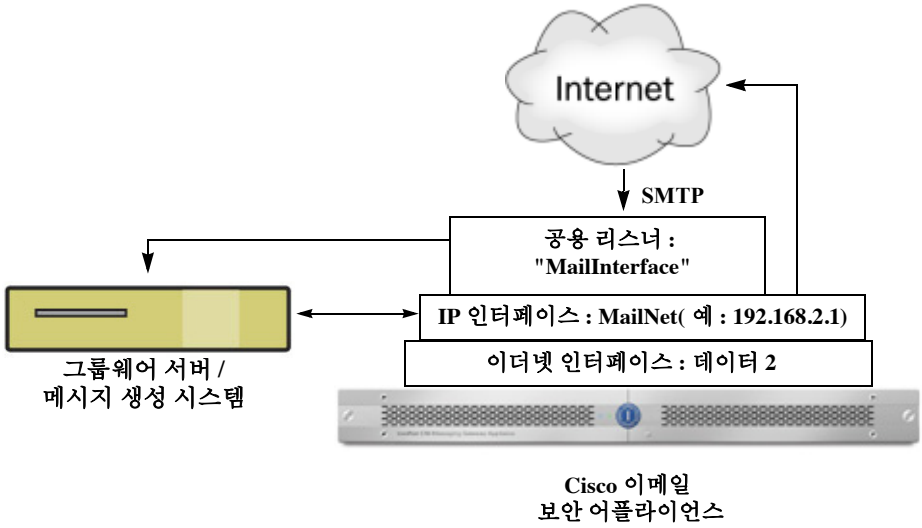


참고 이 공용 리스너는 Data2 이더넷 인터페이스의 PublicNet IP 인터페이스 포트 25에서 SMTP 프로토콜을 사용하여 인터넷의 메시지를 수락합니다. PublicNet IP 인터페이스는 메시지를 인터넷의 대상 호스트로 보냅니다.

PrivateNet IP 인터페이스는 메시지를 내부 메일 호스트로 보냅니다.

참고 이 개인 리스너는 Data1 이더넷 인터페이스의 PrivateNet IP 인터페이스 포트 25에서 SMTP 프로토콜을 사용하여 `.example.com` 도메인의 내부 시스템에서 전송된 메시지를 수락합니다.

그림 5-3 2개의 이더넷 인터페이스만 있는 어플라이언스 모델의 공용 리스너



참고 이 공용 리스너는 Data2 이더넷 인터페이스의 PublicNet IP 인터페이스 포트 25에서 SMTP 프로토콜을 사용하여 인터넷의 메시지를 수락하고 `.example.com` 도메인의 내부 시스템에서 전송된 메시지를 릴레이합니다. MailNet IP 인터페이스는 메시지를 인터넷의 대상 호스트와 내부 메일 호스트로 보냅니다.

리스너의 전역 설정 구성

리스너의 전역 설정은 어플라이언스에 구성된 모든 리스너에 영향을 줍니다. 리스너가 인터넷 프로토콜 버전 4(IPv4) 및 버전 6(IPv6) 주소가 모두 있는 인터페이스를 사용하는 경우 리스너 설정은 IPv4 및 IPv6 트래픽에 모두 적용됩니다.

절차

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

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

3단계 다음 표에 정의된 설정을 변경합니다.

표 5-1 리스너 전역 설정

전역 설정	설명
최대 동시 연결 수	리스너의 최대 동시 연결 수를 설정합니다. 기본값은 300입니다. 리스너가 IPv4 및 IPv6 연결을 모두 허용하는 경우 최대 동시 연결 수가 둘로 나뉩니다. 예를 들어 최대 동시 연결 수가 300인 경우 IPv4 및 IPv6 연결 합계는 300을 초과할 수 없습니다.
최대 동시 TLS 연결 수	모든 리스너의 최대 동시 TLS 연결 수를 설정합니다. 기본값은 100입니다. 리스너가 IPv4 및 IPv6 TLS 연결을 모두 허용하는 경우 최대 동시 TLS 연결 수는 둘로 나뉩니다. 예를 들어 최대 동시 연결 수가 100인 경우 IPv4 및 IPv6 TLS 연결 합계는 100을 초과할 수 없습니다.

표 5-1 리스너 전역 설정

전역 설정	설명
수신 카운터 리셋 기간	수신 제어 카운터가 재설정되는 시점을 조정할 수 있습니다. 대량의 IP 주소를 가지는 카운터를 유지 관리하는 시스템의 사용량이 매우 높을 경우 카운터를 더 자주 재설정하도록 구성(예: 60분이 아닌 15분마다 재설정)하면 데이터가 관리할 수 없는 크기로 증가하지 않으므로 시스템 성능에 영향을 주지 않습니다. 현재 기본값은 1시간입니다. 짧게는 1분(60초)에서 길게는 4시간(14,400초)까지 시간을 지정할 수 있습니다. 수신 제어 주기성, 7-25페이지 항목을 참조하십시오.
인바운드 연결 실패 시 시간제한 기간	AsyncOS가 실패한 인바운드 연결을 닫기 전까지 그대로 유지하는 시간을 설정합니다. 실패한 연결은 성공 메시지가 수신되지 않고 SMTP 또는 ESMTP 명령이 계속 실행되는 SMTP 대화일 수 있습니다. 지정된 시간제한에 도달하면 오류를 보내고 연결이 끊어집니다. "421 Timed out waiting for successful message injection, disconnecting.(성공 메시지 수신을 기다리는 동안 시간이 초과되었습니다. 연결을 끊는 중.)" 메시지를 성공적으로 수신할 때까지 연결은 실패한 것으로 간주됩니다. 공용 리스너의 SMTP 연결에만 사용할 수 있습니다. 기본값은 5분입니다.
모든 인바운드 연결에 대한 총 시간제한	AsyncOS가 인바운드 연결을 종료하기 전까지 그대로 유지하는 시간을 설정합니다. 이 설정은 최대 허용 연결 시간을 적용하여 시스템 리소스를 보존하기 위한 것입니다. 이 최대 연결 시간의 약 80%에 도달하면 다음과 같은 메시지가 표시됩니다. "421 Exceeded allowable connection time, disconnecting.(허용 연결 시간이 초과되었습니다. 연결을 끊는 중.)" 어플라이언스는 연결 시간이 최대 연결 시간의 80%를 초과하면 메시지 중간에 연결이 끊기지 않도록 연결 끊기를 시도합니다. 최대 연결 시간의 80%에 도달할 때까지 열려 있는 인바운드 연결에는 문제가 발생할 가능성이 큽니다. 시간제한을 지정할 때 이 임계값을 염두에 둬야 합니다. 공용 리스너의 SMTP 연결에만 사용할 수 있습니다. 기본값은 15분입니다.

표 5-1 리스너 전역 설정

전역 설정	설명
최대 제목 크기	제목 크기가 지정된 한계값을 벗어나지 않는 메시지는 수락되지만 그 밖의 메시지는 거부됩니다. 이 값을 0으로 설정하면 제한이 적용되지 않습니다.
HAT 거부 지연	메시지 수신자 수준에서 HAT 거부를 수행할지 여부를 구성합니다. 기본적으로 HAT가 거부된 연결은 SMTP 대화 시작 시 배너 메시지가 표시되면서 종료됩니다. HAT "거부" 설정으로 이메일이 거부되면 AsyncOS는 SMTP 대화 시작 지점이 아닌 메시지 수신자 수준(RCPT TO)에서 메시지를 거부합니다. 이런 방식으로 메시지가 거부되면 메시지 거부가 지연되고 메시지가 바운스되므로 AsyncOS는 거부된 메시지에 대한 자세한 정보를 유지할 수 있습니다. 예를 들어 차단된 메시지의 주소 및 각 수신자 주소에서 들어오는 메일을 볼 수 있습니다. 또한, HAT 거부가 지연되면 MTA 전송 시 재시도가 여러 번 발생할 확률이 낮아집니다. HAT 거부 지연을 활성화하면 다음과 같은 동작이 발생합니다. • MAIL FROM 명령이 허용되지만 메시지 객체는 생성되지 않습니다. • 모든 RCPT TO 명령이 거부되고 이메일 전송을 위한 액세스 권한이 거부되었음을 알리는 텍스트가 표시됩니다. • SMTP AUTH를 사용하여 MTA 인증을 보내는 경우, RELAY 정책이 부여되며 메일을 정상적으로 전달할 수 있습니다. **참고** CLI의 `listenerconfig --> setup` 명령을 통해서만 구성할 수 있습니다.

4단계 변경사항을 제출하고 커밋합니다.

관련 주제

- 여러 인코딩이 포함된 메시지 설정: localeconfig, 5-6페이지

여러 인코딩이 포함된 메시지 설정: localeconfig

메시지 처리 중에 메시지 머리글 및 바닥글의 인코딩을 수정하는 AsyncOS 동작을 설정할 수 있습니다. 이 설정은 GUI를 통해 구성되지 않습니다. 대신 CLI의 `localeconfig`를 통해 구성됩니다.

GUI를 통해 리스너를 생성하여 연결 요청 수신 대기

절차

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

2단계 **Add Listener(리스너 추가)**를 클릭합니다.

3단계 다음 표에 정의된 설정을 구성합니다.

표 5-2 리스너 설정

이름	이후에 참조할 수 있도록 리스너에 제공하는 고유 별칭입니다. 리스너에 정의하는 이름은 대소문자를 구분합니다. AsyncOS에서는 동일한 리스너 이름을 생성할 수 없습니다.
리스너 유형	다음 리스너 유형 중 하나를 선택합니다. • **공용.** 공용 리스너는 인터넷으로부터 이메일을 수신하기 위한 기본 특성을 포함합니다. • **개인.** 개인 리스너는 사설(내부) 네트워크에 사용됩니다.
인터페이스	리스너를 생성하기 위해 구성한 어플라이언스 IP 인터페이스 및 TCP 포트를 선택합니다. 인터페이스에 사용되는 IP 주소 버전에 따라 리스너는 IPv4 주소나 IPv6 주소 또는 두 가지 모두에서의 연결을 허용합니다. 기본적으로 SMTP는 포트 25를 사용하고 QMQP는 포트 628을 사용합니다.
바운스 프로파일	바운스 프로파일을 선택합니다(CLI의 `bounceconfig` 명령을 사용하여 생성한 바운스 프로파일은 목록에서 사용 가능, 새 바운스 프로파일 생성, 24-39페이지 참조).
경고문을 위로	이메일 위 또는 아래에 첨부할 경고문을 선택합니다(Mail Policies(메일 정책) > Text Resources(텍스트 리소스) 페이지 또는 CLI의 `textconfig` 명령을 사용하여 생성한 경고문은 목록에서 확인 가능, "텍스트 리소스" 장 참조).
경고문을 아래로	이메일 위 또는 아래에 첨부할 경고문을 선택합니다(Mail Policies(메일 정책) > Text Resources(텍스트 리소스) 페이지 또는 CLI의 `textconfig` 명령을 사용하여 생성한 고지 사항은 목록에서 확인 가능, "텍스트 리소스" 장 참조).
SMTP 인증 프로파일	SMTP 인증 프로파일을 지정합니다.
인증서	리스너의 TLS 연결에 사용할 인증서를 지정합니다(Network(네트워크) > 인증서(Certificates) 페이지 또는 CLI의 `certconfig` 명령을 사용하여 추가된 인증서는 목록에서 확인 가능, 다른 MTA와의 통신 암호화에 대한 개요, 23-1페이지 참조).

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

설정	설명
주소 구문 분석 유형	다음 구문 분석 유형 중 하나를 사용하여 어플라이언스의 RFC2821 표준 준수 수준을 선택합니다. **Strict 모드:** Strict 모드에서는 RFC 2821을 준수합니다. Strict 모드에서 주소 구문 분석은 RFC 2821 규칙을 준수하며 다음과 같은 예외와 개선 사항이 적용됩니다. • "MAIL FROM: <joe@example.com>"처럼 콜론 뒤에 공백을 사용할 수 있습니다. • 도메인 이름에 밑줄을 사용할 수 있습니다. • "MAIL FROM" 및 "RCPT TO" 명령은 대소문자를 구분하지 않습니다. • 마침표는 특수하게 처리되지 않습니다(예: RFC 2821에서는 사용자 이름 "J.D"를 사용할 수 없음). 아래의 추가 옵션 중 일부는 활성화될 수 있지만 이 경우 기술적으로 RFC 2821을 위반하게 됩니다. **Loose 모드:** Loose 구문 분석은 기본적으로 이전 AsyncOS 버전에 존재하는 동작입니다. 이메일 주소를 "찾기" 위해 최선의 노력을 기울이며 다음과 같은 특성을 갖습니다. • 주석을 무시합니다. 중첩된 주석(괄호 안에 있는 모든 항목)을 지원하지만 이를 무시합니다. • "RCPT TO" 및 "MAIL FROM" 명령에 제공된 이메일 주소를 둘러싸는 꺾쇠괄호가 필요 없습니다. • 중첩된 꺾쇠괄호 여러 개를 사용할 수 있습니다(가장 깊이 중첩된 수준에서 이메일 주소 검색).
8비트 사용자 이름을 허용합니다.	활성화된 경우, 주소의 사용자 이름 부분에 이스케이프 없이 8비트 문자를 사용할 수 있습니다.
8비트 도메인 이름 허용	활성화된 경우, 주소의 도메인 부분에 8비트 문자를 사용할 수 있습니다.

설정	설명
부분 도메인 허용	활성화된 경우 부분 도메인이 허용됩니다. 부분 도메인은 도메인이 전혀 없거나 점이 없는 도메인입니다. 다음 주소는 부분 도메인의 예입니다. • foo • foo@ • foo@bar 기본 도메인 기능이 제대로 동작하려면 이 옵션을 *활성화해야* 합니다. **기본 도메인 추가:** 정규화된 도메인 이름 없이 이메일 주소에 사용할 기본 도메인입니다. 이 옵션은 SMTP Address Parsing(SMTP 주소 구문 분석) 옵션에서 Allow Partial Domains(부분 도메인 허용)가 활성화된 경우를 제외하고 비활성화됩니다(GUI를 통해 리스너를 생성하여 연결 요청 수신 대기, 5-6페이지 참조). 이는 정규화된 도메인 이름을 포함하지 않은 발신자 및 수신자 주소에 "기본 발신자 도메인"을 추가하여 이메일을 릴레이하는 리스너가 이메일을 수정하는 방식에 영향을 줍니다. (즉, 리스너가 "Bare" 주소를 처리하는 방식을 사용자 지정할 수 있습니다.) 회사 도메인을 발신자 주소에 추가(덧붙이기)하지 않고 이메일을 보내는 레거시 시스템이 있는 경우 이 옵션을 사용하여 기본 발신자 도메인을 추가할 수 있습니다. 예를 들어 레거시 시스템은 "joe" 문자열만 이메일 발신자로 입력하는 이메일을 자동으로 생성할 수 있습니다. 기본 발신자 도메인을 변경하면 "@yourdomain.com"에 "joe"가 추가되어 정규화된 발신자 이름인 joe@yourdomain.com이 생성됩니다.
원본 라우팅	"MAIL FROM" 및 "RCPT TO" 주소에서 원본 라우팅이 탐지되는 경우의 동작을 결정합니다. 원본 라우팅은 여러 '@' 문자를 사용하여 라우팅을 지정하는 특수한 이메일 주소 형식(예: @one.dom@two.dom:joe@three.dom)입니다. "거부"로 설정된 경우 주소가 거부됩니다. "제거"로 설정된 경우 주소의 원본 라우팅 부분이 삭제되고 메시지가 정상적으로 삽입됩니다.
알 수 없는 주소 리터럴	시스템에서 처리할 수 없는 주소 리터럴이 수신되는 경우의 동작을 결정합니다. 현재는 IPv4를 제외한 모든 항목으로 설정되어 있습니다. 예를 들어 IPv6 주소 리터럴의 경우, 주소 리터럴을 프로토콜 수준에서 거부하거나, 허용하는 즉시 하드 바운스할 수 있습니다. 리터럴이 포함된 수신자 주소는 즉각적으로 하드 바운스됩니다. 발신자 주소는 전달될 수 있습니다. 메시지를 전달할 수 없는 경우 하드 바운스가 하드 바운스(이중 하드 바운스)됩니다. 거부되는 경우 발신자 주소와 수신자 주소가 모두 프로토콜 수준에서 즉시 거부됩니다.
사용자 이름에 다음 문자 사용 금지	여기에 입력한 문자(예: % 또는 !)가 포함된 사용자 이름은 거부됩니다.

5단계 (선택 사항) 다음 표에 정의된 리스너의 동작을 사용자 지정하기 위한 고급 설정을 구성합니다.

설정	설명
최대 동시 연결 수	허용되는 최대 연결 수입니다.
TCP 수신 대기 큐 크기	SMTP 서버에서 연결을 허용하기 전에 AsyncOS가 관리하는 연결에 대한 백로그입니다.

설정	설명
CR 및 LF 처리	Bare CR(캐리지 리턴) 및 LF(줄 바꿈) 문자가 포함된 메시지를 처리하는 방법을 선택합니다. • **정상.** 메시지를 허용하지만, Bare CR 및 LF 문자를 CRLF 문자로 변환합니다. • **거부.** 메시지를 거부합니다. • **허용.** 메시지를 허용합니다.
Received 헤더 추가	수신된 모든 이메일에 Received 헤더를 추가합니다. 리스너는 또한 각 메시지에 Received: 헤더를 추가하여 릴레이하는 이메일을 수정합니다. Received: 헤더를 포함하지 않으려면 이 옵션을 사용하여 비활성화할 수 있습니다. **참고** 작업 큐 처리 중 Received: 헤더가 메시지에 추가되지 않습니다. 그 대신 전달할 메시지가 큐에 저장될 때 추가됩니다. Received 헤더 비활성화는 인프라 외부로 이동하는 메시지에 내부 서버의 IP 주소 또는 호스트 이름을 표시하여 네트워크의 토폴로지가 노출되지 않도록 하는 방법입니다. Received 헤더를 비활성화할 때는 주의해야 합니다.
SenderBase IP 프로파일링 사용	SenderBase IP 프로파일링을 활성화할지 여부를 선택하고 다음 설정을 구성합니다. • **쿼리 시간 제한.** 어플라이언스가 SBRS(SenderBase Reputation Service)에서 쿼리된 정보를 캐시하는 시간을 정의합니다. • **연결당 SenderBase 시간 제한.** 어플라이언스가 SMTP 연결당 SenderBase 정보를 캐시하는 시간을 정의합니다.

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

리스너에서 LDAP 쿼리를 활성화하려면 이러한 설정을 사용하십시오. 이 옵션을 사용하기 전에 먼저 LDAP 쿼리를 생성해야 합니다. 쿼리 유형별로 구성할 하위 섹션이 있습니다. 쿼리 유형을 클릭하여 하위 섹션을 확장합니다.

LDAP 쿼리 생성에 대한 자세한 내용은 LDAP 쿼리, 25-1페이지 항목을 참조하십시오.

쿼리 유형	설명
Accept 쿼리	Accept 쿼리의 경우 목록에서 사용할 쿼리를 선택합니다. LDAP Accept를 작업 큐 처리 중에 발생시킬지, 아니면 SMTP 대화 중에 발생시킬지 지정할 수 있습니다. 작업 큐 처리 중에 발생하는 LDAP Accept와 관련하여 일치하지 않는 수신자에 대한 동작(바운스 또는 삭제)을 지정합니다. SMTP 대화 중에 발생하는 LDAP Accept와 관련하여 LDAP 서버에 연결할 수 없는 경우의 메일 처리 방식을 지정합니다. 메시지를 허용하거나 코드 및 사용자 지정 응답이 포함된 연결을 삭제하도록 선택할 수 있습니다. 마지막으로 SMTP 대화 중 디렉토리 수집 공격 방지(DHAP) 임계값에 도달하는 경우 연결을 삭제할지 여부를 선택합니다. SMTP 대화에서 수신자 검증을 수행하면 여러 LDAP 쿼리 사이의 대기 시간을 줄일 수 있습니다. 따라서 대화 LDAP Accept를 활성화하면 디렉토리 서버에서 증가하는 로드를 파악할 수 있습니다. 자세한 내용은 LDAP 쿼리 개요, 25-1페이지 항목을 참조하십시오.
라우팅 쿼리	라우팅 쿼리의 경우 목록에서 해당 쿼리를 선택합니다. 자세한 내용은 LDAP 쿼리 개요, 25-1페이지 항목을 참조하십시오.
마스커레이드 (Masquerade) 쿼리	마스커레이드 쿼리의 경우 목록에서 쿼리를 선택하고 From 또는 CC 헤더 주소와 같이 마스커레이드할 주소를 선택합니다. 자세한 내용은 LDAP 쿼리 개요, 25-1페이지 항목을 참조하십시오.
그룹 쿼리	그룹 쿼리의 경우 목록에서 해당 쿼리를 선택합니다. 자세한 내용은 LDAP 쿼리 개요, 25-1페이지 항목을 참조하십시오.

7단계 변경사항을 제출하고 커밋합니다.

관련 주제

- 부분 도메인, 기본 도메인 및 잘못된 형식의 MAIL FROM, 5-11페이지

부분 도메인, 기본 도메인 및 잘못된 형식의 MAIL FROM

봉투 발신자 확인을 활성화한 경우 또는 리스너의 SMTP 주소 구문 분석 옵션에서 부분 도메인 허용을 비활성화한 경우 해당 리스너의 기본 도메인 설정은 더 이상 사용되지 않습니다.

이러한 기능은 함께 사용할 수 없습니다.

CLI를 통해 리스너를 생성하여 연결 요청 수신 대기

표 5-3에는 리스너 생성 및 편집과 관련된 작업에 사용되는 몇 가지 `listenerconfig` 하위 명령이 나와 있습니다.

표 5-3 리스너 생성 작업

리스너 생성 작업	명령 및 하위 명령	참조
새 리스너 생성	`listenerconfig -> new`	
리스너의 전역 설정 편집	`listenerconfig -> setup`	리스너의 전역 설정 구성, 5-4페이지
리스너에 대한 바운스 프로파일 지정	`bounceconfig, listenerconfig -> edit -> bounceconfig`	새 바운스 프로파일 생성, 24-39페이지
리스너에 고지 사항 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)의 이메일 수락(공용 리스너에만 해당)	`listenerconfig -> edit -> rcptaccess`	
리스너의 대화 암호화(TLS)	`certconfig, settls, listenerconfig -> edit`	다른 MTA와의 통신 암호화에 대한 개요, 23-1페이지
인증서 선택(TLS)	`listenerconfig -> edit -> certificate`	다른 MTA와의 통신 암호화에 대한 개요, 23-1페이지

이메일 라우팅 및 전송 구성에 대한 자세한 내용은 24 장, "라우팅 및 전달 기능 구성" 항목을 참조하십시오.

관련 주제

고급 HAT 매개변수, 5-13페이지

고급 HAT 매개변수

표 5-4에서는 고급 HAT 매개변수 구문을 정의합니다. 아래의 숫자 값에서 후행 **k**를 추가하여 킬로바이트를 나타내거나 후행 **M**을 추가하여 메가바이트를 나타낼 수 있습니다. 문자가 없는 값은 바이트로 간주됩니다. 별표로 표시된 매개변수는 표 5-4에 표시된 변수 구문을 지원합니다.

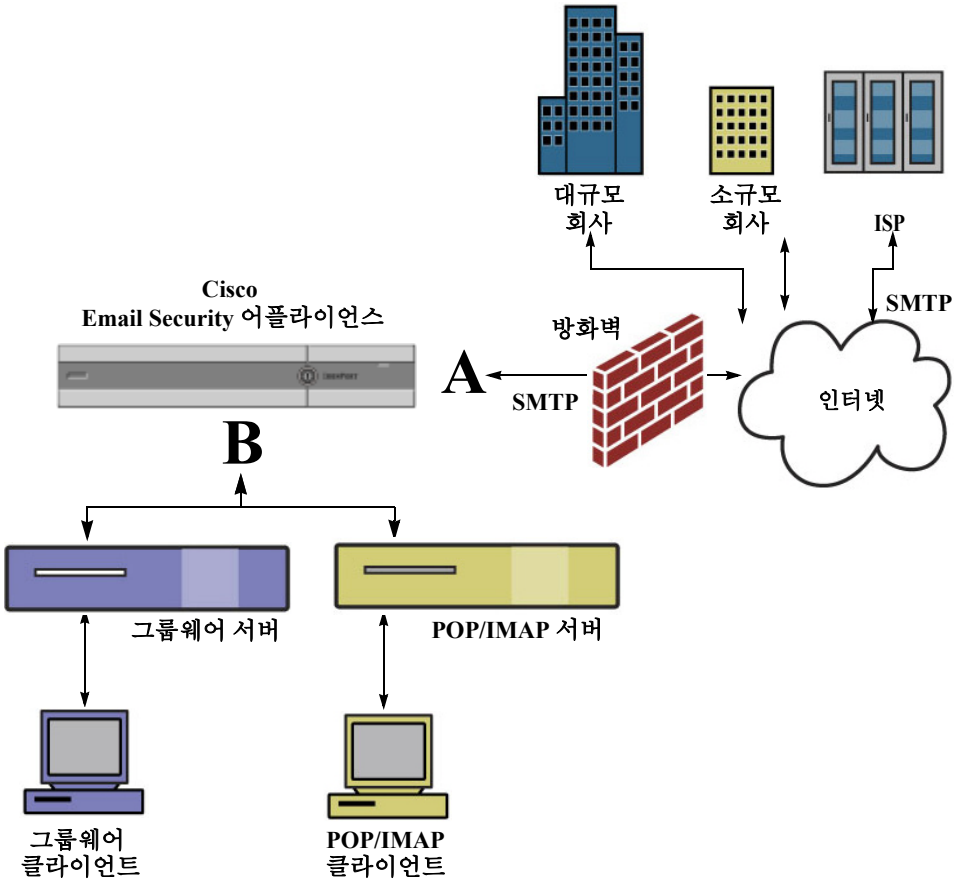
표 5-4 고급 HAT 매개변수 구문

매개변수	구문	가치	예제 값
연결당 최대 메시지 수	max_msgs_per_session	번호	1000
메시지당 최대 수신자 수	max_rcpts_per_msg	번호	10000 1k
최대 메시지 크기	max_message_size	번호	1048576 20M
이 리스너에 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
SMTP 거부 배너 텍스트(*)	smtp_banner_text	문자열	Rejected
SMTP 배너 호스트 이름 덮어쓰기	use_override_hostname	on | off | default	default
	override_hostname	문자열	newhostname
TLS 사용	tls	on | off | required	on
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
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 many recipients
SenderBase 사용	use_sb	on | off	on
SenderBase Reputation 점수 정의	sbrs[*value1*:*value2*]	-10.0- 10.0	sbrs[-10:-7.5]
디렉토리 수집 공격 방지: 시간당 올바르지 않은 최대 수신자 수	dhap_limit	번호	150

엔터프라이즈 게이트웨이 구성

이 구성에서 엔터프라이즈 게이트웨이 구성은 인터넷에서 이메일을 수락하고 이 이메일을 그룹웨어 서버, POP/IMAP 서버 또는 다른 MTA로 릴레이합니다. 동시에 엔터프라이즈 게이트웨이는 그룹웨어 서버 및 다른 이메일 서버에서 SMTP 메시지를 수락하여 인터넷의 수신자에게 릴레이합니다.

그림 5-4 엔터프라이즈 게이트웨이용 공용 및 개인 리스너



이 구성에서는 최소 2개의 리스너가 필요합니다.

- 인터넷*에서* 메일을 수락하도록 특별하게 구성된 리스너 하나
- 내부 그룹웨어 및 이메일 서버(POP/IMAP)*에서* 메일을 수락하도록 특별하게 구성된 리스너 하나

서로 다른 공용 네트워크와 개인 네트워크에 대해 고유한 공용 및 개인 리스너를 생성하여 보안, 정책 시행, 보고 및 관리를 위한 이메일을 구분할 수 있습니다. 예를 들어 공용 리스너에서 수신되는 이메일은 기본적으로 사용자가 구성한 안티스팸 엔진 및 안티바이러스 검사 엔진으로 검사되지만, 개인 리스너에 수신된 이메일은 검사되지 않습니다.

그림 5-4에서는 이 엔터프라이즈 게이트웨이 구성에서 어플라이언스에 구성된 공용 리스너(A) 하나와 개인 리스너(B) 하나를 보여줍니다.

6 장

발신자 평판 필터링

발신자 평판 필터링 개요

발신자 평판 필터링은 첫 번째 스팸 보호 계층으로, Cisco SenderBase™ Reputation Service에 의해 결정된 발신자의 신뢰도에 따라 이메일 게이트웨이를 거쳐서 들어오는 메시지를 관리할 수 있습니다.

어플라이언스가 알려져 있거나 평판이 높은 발신자(고객 및 파트너 등)의 메시지를 수락하고 콘텐츠 검사 없이 이 메시지를 직접 최종 사용자에게 전송할 수 있습니다. 알 수 없거나 평판이 낮은 발신자의 메시지는 콘텐츠 검사(안티스팸 및 안티바이러스 검사 등)를 거칠 수 있으며 각 발신자에게서 수락할 메시지의 수를 제한할 수도 있습니다. 평판이 나쁜 이메일 발신자는 환경 설정에 따라 연결을 거부하거나 메시지를 바운스할 수 있습니다.

참고 파일 평판 필터링은 별도의 서비스입니다. 관련 내용은 16 장, "파일 평판 필터링 및 파일 분석"을 참조하십시오.

SenderBase Reputation Service

Cisco SenderBase Reputation Service는 SenderBase 제휴 네트워크의 전역 데이터를 사용하여 불만율, 메시지 볼륨 통계, 공용 차단 목록 및 오픈 프록시 목록의 데이터에 따라 이메일 발신자에게 SenderBase Reputation 점수를 지정합니다. SenderBase Reputation 점수를 통해 스팸 소스와 정상적인 발신자를 구별할 수 있습니다. 평판 점수가 낮은 발신자의 메시지를 차단하는 임계값을 결정할 수 있습니다.

SenderBase Security Network 웹사이트(`www.senderbase.org`)는 최신 이메일 및 웹 기반 위협의 전역 개요를 제공하고, 현재 이메일 트래픽 볼륨을 국가별로 표시하므로 사용자가 IP 주소, URI 또는 도메인별로 평판 점수를 조회할 수 있습니다.

참고 SenderBase Reputation Service는 최신 안티스팸 기능 키와 함께 사용할 수 있습니다.

관련 주제

- SBRS(SenderBase Reputation 점수), 6-2페이지
- SenderBase 평판 필터 작동 원리, 6-3페이지
- 다양한 발신자 평판 필터링 접근법의 권장 설정, 6-4페이지
- 신종 바이러스 필터(Outbreak Filter), 14-1페이지
- 28 장, "이메일 보안 모니터링 사용"

SBRS(SenderBase Reputation 점수)

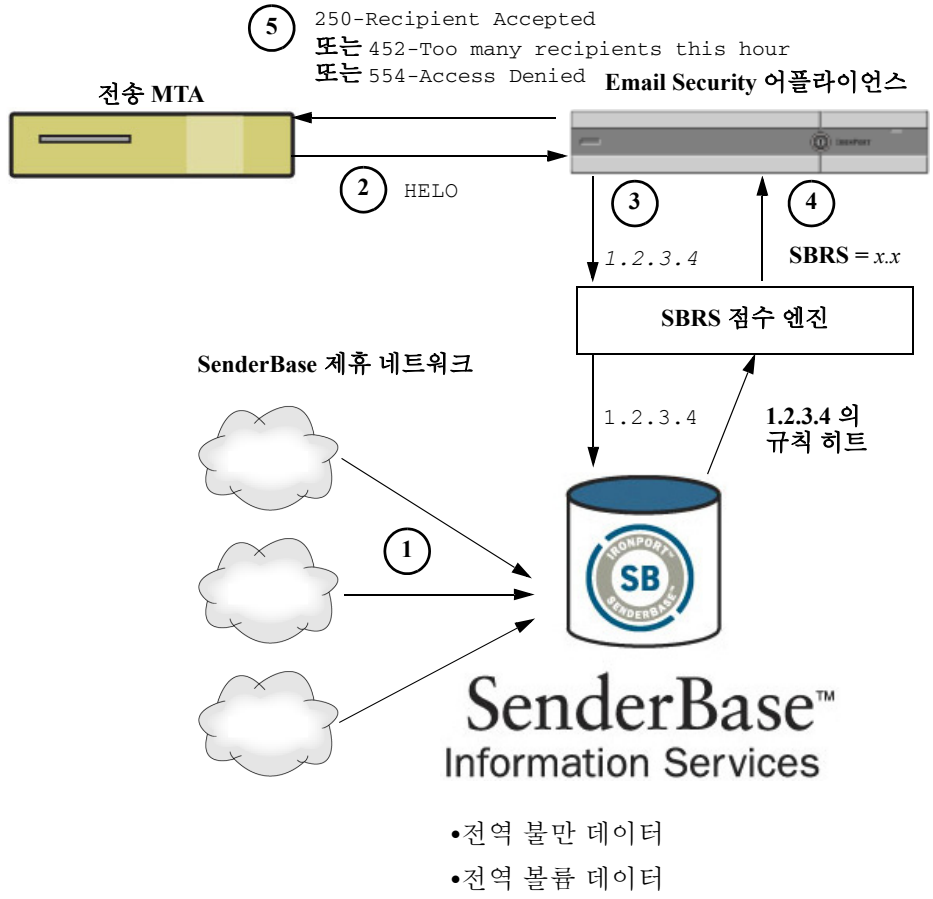
SBRS(SenderBase Reputation 점수)는 SenderBase Reputation Service의 정보에 따라 IP 주소에 지정된 숫자 값입니다. SenderBase Reputation Service는 25개 이상의 공용 차단 목록과 오픈 프록시 목록의 데이터를 집계하고 이 데이터와 SenderBase의 전역 데이터를 결합하여 다음과 같이 -10.0~+10.0의 점수를 지정합니다.

점수	의미
-10.0	스팸 소스일 가능성이 가장 높음
0	보통 또는 권장하기에는 충분하지 않은 정보
+10.0	신뢰할 수 있는 발신자일 가능성이 가장 높음

점수가 낮을수록(부정적일수록) 메시지가 스팸일 가능성이 높아집니다. 점수 -10.0은 이 메시지가 스팸이 "확실함"을 의미하고, 점수 10.0은 해당 메시지가 정상적인 메시지가 "확실함"을 의미합니다.

SBRS를 사용하여 발신자의 신뢰도에 따라 발신자에게 메일 흐름 정책을 적용하도록 어플라이언스를 구성합니다. (시스템에서 처리된 메시지에 대해 추가 작업을 수행하는 SenderBase Reputation 점수의 "임계값"을 지정하는 메시지 필터를 생성할 수도 있습니다. 자세한 내용은 "SenderBase Reputation 규칙, 9-34페이지" 및 "안티스팸 시스템 우회 작업, 9-70페이지"를 참조하십시오.)

그림 6-1 SenderBase Reputation Service



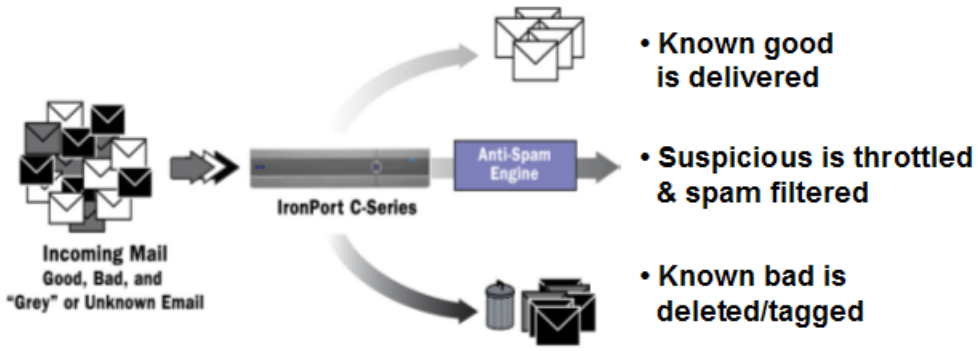
1. SenderBase 제휴 네트워크에서 실시간 전역 데이터를 전송합니다.
2. 전송 MTA가 어플라이언스와의 연결을 엽니다.
3. 어플라이언스가 연결 IP 주소의 전역 데이터를 확인합니다.
4. SenderBase Reputation Service가 이 메시지가 스팸일 가능성을 계산하고 SenderBase Reputation 점수를 지정합니다.
5. Cisco가 SenderBase Reputation 점수에 따라 응답을 반환합니다.

SenderBase 평판 필터 작동 원리

발신자 평판 필터 기술은 어플라이언스에서 사용할 수 있는 나머지 보안 서비스 처리에서 최대한 많은 메일을 이동하는 것을 목표로 합니다. (이메일 파이프라인 이해, 4-1페이지 참조)

발신자 평판 필터링이 활성화되면 알려진 나쁜 발신자의 메일이 거부됩니다. 2,000개의 글로벌 기업에서 발송한 알려진 좋은 메일은 자동으로 스팸 필터를 경유하므로 잘못된 긍정의 가능성이 낮아집니다. 알 수 없는 이메일 또는 "회색" 이메일은 안티스팸 검사 엔진을 경유합니다. 이 접근법을 사용하여 발신자 평판 필터가 콘텐츠 필터의 부담을 50%까지 줄일 수 있습니다.

그림 6-2 발신자 평판 필터링 예



다양한 발신자 평판 필터링 접근법의 권장 설정

기업의 목표에 따라 보수적, 소극적 또는 공격적 접근법을 적용할 수 있습니다.

접근 방식	특징	허용 목록	차단 목록	의심 목록	알 수 없는 목록
		발신자 기본 평판 점수 범위:			
보수적	0에 가까운 잘못된 긍정, 양호한 성능	7 ~ 10	-10 ~ -4	-4 ~ -2	-2 ~ 7
사회 (설치 기본값)	매우 낮은 잘못된 긍정, 높은 성능	발신자 기본 평판 점수가 사용되지 않습니다.	-10 ~ -3	-3 ~ -1	-1 ~ +10
공격적	약간의 잘못된 긍정, 최대 성능 이 옵션은 안티스팸 처리에서 대부분의 메일을 이동합니다.	4 ~ 10	-10 ~ -2	-2 ~ -1	-1 ~ 4
		메일 흐름 정책:			
모든 접근법		신뢰성	차단됨	제한됨	승인됨

리스너의 발신자 평판 필터링 점수 임계값 편집

기본 SBRS(SenderBase Reputation Service) 점수 임계값을 변경하거나 발신자 평판 필터링 그룹을 추가하려면 이 절차를 사용합니다.

참고 SBRS 점수 임계값과 관련된 기타 설정과 메일 흐름 정책 설정은 7 장, "HAT(Host Access Table)를 사용하여 연결할 수 있는 호스트 정의"에 설명되어 있습니다.

시작하기 전에

- 어플라이언스가 로컬 MX/MTA의 메일을 수신하도록 설정된 경우 발신자의 IP 주소를 마스크 처리할 수 있는 업스트림 호스트를 식별합니다. 자세한 내용은 수신 릴레이 사용 배포 환경에서 발신자 IP 주소 확인, 13-15페이지를 참조하십시오.
- 발신자 기본 평판 점수를 이해합니다. SenderBase Reputation 점수별로 발신자 그룹 정의, 7-6페이지를 참조하십시오.
- 조직의 필터링 접근법을 선택하고 해당 접근법에 대한 권장 설정을 확인합니다. 다양한 발신자 평판 필터링 접근법의 권장 설정, 6-4페이지를 참조하십시오.

절차

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

2단계 **발신자 그룹(리스너)** 메뉴에서 공용 리스너를 선택합니다.

3단계 발신자 그룹의 링크를 클릭합니다.

예를 들어, "SUSPECTLIST" 링크를 클릭합니다.

4단계 **Edit Settings(설정 편집)**를 클릭합니다.

5단계 이 발신자 그룹에 대한 SenderBase Reputation 점수 범위를 입력합니다.

예를 들어, "WHITELIST"의 경우 범위 7.0~10을 입력합니다.

6단계 **Submit(제출)**을 클릭합니다.

7단계 필요에 따라 이 리스너의 각 발신자 그룹에 대해 반복합니다.

8단계 변경 사항을 커밋합니다.

관련 주제

- SBRS를 사용하여 발신자 평판 필터링 테스트, 6-6페이지
- SenderBase Reputation Service의 상태 모니터링, 6-7페이지
- 7 장, "HAT(Host Access Table)를 사용하여 연결할 수 있는 호스트 정의"
- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 13-2페이지

SBRS를 사용하여 발신자 평판 필터링 테스트

정기적으로 대량의 스팸을 수신하거나 특별히 조직의 스팸을 수신하는 "dummy" 계정을 설정한 경우를 제외하고 적용한 SBRS 정책을 즉시 테스트하기는 어렵습니다. 그러나 표 6-1에 표시된 대로 리스너의 HAT에 SenderBase Reputation 점수와 함께 평판 필터링의 항목을 추가할 경우 인바운드 메일이 "분류되지 않는" 비율이 더 적어집니다.

trace 명령을 사용하여 임의의 SBRS로 정책을 테스트합니다. 테스트 메시지를 사용한 메일 흐름 디버깅: 추적, 40-1페이지를 참조하십시오. trace 명령은 GUI뿐 아니라 CLI에서도 사용할 수 있습니다.

표 6-1 SBRS 적용을 위해 제안된 메일 흐름 정책

정책 이름	기본 동작 (액세스 규칙)	매개변수	값
$BLOCKED	REJECT	없음	
$THROTTLED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: 스팸 탐지 사용: TLS 사용: Maximum recipients / hour: SenderBase 사용:	10 20 1 MB 10 ON 할인 **20***(권장)* ON
$ACCEPTED (공용 리스너)	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: 스팸 탐지 사용: TLS 사용: SenderBase 사용:	1,000 1,000 100 MB 1,000 ON 할인 ON
$TRUSTED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: 스팸 탐지 사용: TLS 사용: Maximum recipients / hour: SenderBase 사용:	1,000 1,000 100 MB 1,000 할인 할인 -1*(비활성화됨)* 할인

참고 $THROTTLED 정책에서 원격 호스트의 시간당 최대 수신자는 기본적으로 시간당 20명의 수신자로 설정됩니다. 이 설정은 사용 가능한 최대 제한을 제어합니다. 이 매개변수가 너무 공격적일 경우 시간당 수신할 수신자 수를 늘릴 수 있습니다. 기본 호스트 액세스 정책에 대한 자세한 내용은 사전 정의 발신자 그룹 및 메일 흐름 정책 이해, 7-11페이지를 참조하십시오.

SenderBase Reputation Service의 상태 모니터링

보안 서비스 메뉴의 SenderBase 페이지에는 연결 상태와 어플라이언스에서 SenderBase Network Status Server 및 SenderBase Reputation Score Service로 전송된 가장 최근 쿼리의 타임스탬프가 표시됩니다. SenderBase Reputation Score Service는 어플라이언스에 SRBS 점수를 전송합니다. SenderBase Network Server는 사용자에게 메일을 보내는 IP 주소, 도메인 및 조직에 대한 정보를 어플라이언스에 보냅니다. AsyncOS는 보고 및 이메일 모니터링 기능에 이 데이터를 사용합니다.

그림 6-3 SenderBase 페이지의 SenderBase 네트워크 상태

SenderBase Network Status		
Type	Status	Last Status Check
SenderBase Network Server	up	Wed Sep 10 13:44:52 2008 PDT
SenderBase Reputation Score Service	up	Wed Sep 10 13:44:52 2008 PDT

CLI에서 `sbstatus` 명령을 실행하면 동일한 정보가 표시됩니다.

메시지 제목에 낮은 SBRS 점수 입력

Cisco에서는 제한을 권장하지만 SenderBase Reputation Service를 사용하는 대안은 의심스러운 스팸 메시지의 제목 줄을 수정하는 것입니다. 이렇게 하려면 메시지 필터(표 6-2에 표시됨)를 사용합니다. 이 필터는 평판 필터 규칙과 `strip-header` 및 `insert-header` 필터 작업을 사용하여 -2.0 미만의 SenderBase Reputation 점수(**`{Spam`** *SBRS*`}`로 표시되는 실제 SenderBase Reputation 점수 포함)가 있는 제목 줄을 대체합니다. 이 예제의 *listener_name*을 공용 리스너의 이름으로 바꿉니다. (자체 줄의 기간이 포함되어 이 텍스트를 잘라서 `filters` 명령의 인터페이스에 직접 붙여 넣을 수 있습니다.)

표 6-2 SBRS가 포함된 제목 헤더를 수정하는 메시지 필터: 예제 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

- 9 장, "메시지 필터를 사용하여 이메일 정책 적용".

HAT(Host Access Table)를 사용하여 연결할 수 있는 호스트 정의

연결할 수 있는 호스트 정의 개요

모든 구성된 리스너에 대해 원격 호스트에서 수신 연결을 제어하는 규칙 집합을 정의해야 합니다. 예를 들어 원격 호스트를 정의하고 해당 원격 호스트의 리스너 연결 가능 여부를 정의할 수 있습니다. AsyncOS를 통해 어떤 호스트가 HAT(Host Access Table)를 사용하여 리스너에 연결될 수 있는지 정의할 수 있습니다.

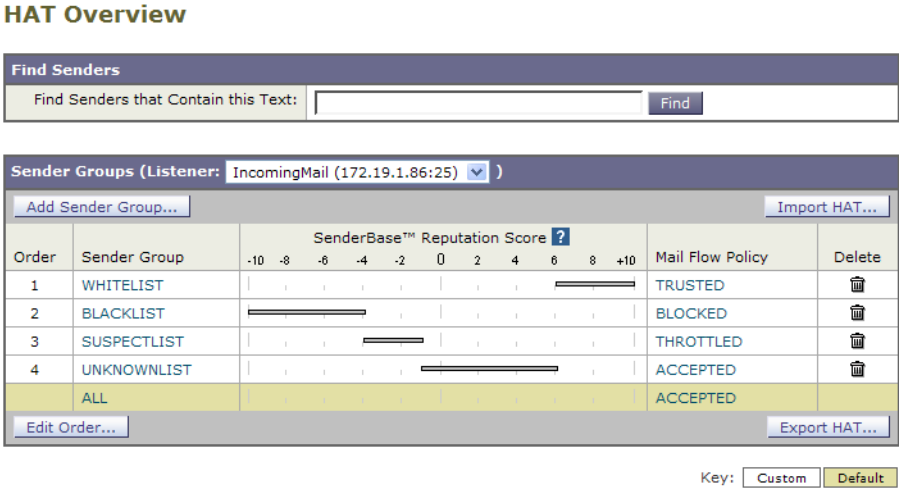
HAT는 리스너에 대한 원격 호스트에서의 수신 연결을 제어하는 규칙 집합을 유지 관리합니다. 구성된 각 리스너는 고유한 HAT를 보유합니다. 공용 및 개인 리스너에 대해 HAT를 구성합니다.

원격 호스트에서 수신되는 연결을 제어하려면, 다음 정보를 정의합니다.

- **원격 호스트.** 원격 호스트가 리스너에 연결을 시도하는 방식을 정의합니다. 원격 호스트 정의를 *발신자 그룹*으로 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 원격 호스트를 발신자 그룹으로 정의, 7-3페이지 항목을 참조하십시오.
- **액세스 규칙.** 발신자 그룹의 정의된 원격 호스트가 리스너에 연결 가능한지 여부 및 연결 조건을 정의할 수 있습니다. *메일 흐름 정책*을 사용하여 액세스 규칙을 정의합니다. 예를 들어, 특정한 발신자 그룹이 리스너에 연결될 수 있지만 연결당 최대 메시지 수만 허용하도록 정의할 수 있습니다. 자세한 내용은 메일 흐름 정책을 사용하여 이메일 발신자에 대한 액세스 규칙 정의, 7-8페이지 항목을 참조하십시오.

Mail Policies(메일 정책) > HAT Overview(HAT 개요) 페이지에서 어떤 호스트가 리스너에 연결될 수 있는지 정의합니다. 그림 7-1은 HAT 개요와 공용 리스너에 대해 기본값으로 정의되어 있는 발신자 그룹 및 메일 흐름 정책을 보여줍니다.

그림 7-1 메일 정책 > HAT 요약 페이지 — 공용 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 내용을 발견하는 경우 구성된 메일 흐름 정책을 해당 연결에 적용합니다. 발신자 그룹 내에 여러 조건을 구성한 경우 이 조건 중 하나라도 일치하면 해당 발신자 그룹은 일치합니다.

리스너를 만들 때 AsyncOS는 해당 리스너에 대한 사전 정의 발신자 그룹 및 메일 흐름 정책을 생성합니다. 사전 정의 발신자 그룹 및 메일 흐름 정책을 편집하고 새 발신자 그룹 및 메일 흐름 정책을 만들 수 있습니다. 자세한 내용은 사전 정의 발신자 그룹 및 메일 흐름 정책 이해, 7-11페이지 항목을 참조하십시오.

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 Host Access Table 구성 작업, 7-20페이지 항목을 참조하십시오.

관련 주제

- 기본 HAT 항목, 7-2페이지

기본 HAT 항목

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

- **공용 리스너.** HAT가 이메일 *모든* 호스트의 이메일을 *수락*하도록 설정됩니다.
- **개인 리스너.** 지정한 호스트의 이메일을 *릴레이*하고 모든 기타 호스트는 거부하도록 HAT가 설정됩니다.

HAT 개요에서 기본 항목의 이름은 "ALL"입니다. Mail Policies(메일 정책) > HAT Overview(HAT 개요) 페이지에서 ALL 발신자 그룹의 메일 흐름 정책을 클릭하여 기본 항목을 편집할 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.

원격 호스트를 발신자 그룹으로 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, 7-4페이지 항목을 참조하십시오.

SMTP 서버가 어플라이언스와의 SMTP 연결을 시도하는 경우 리스너는 이 서버가 SenderBase Reputation 점수, 도메인 또는 IP 주소 등 발신자 그룹의 *모든* 기준과 일치하는 경우, 순서대로 발신자 그룹을 평가하고 이 연결을 발신자 그룹에 할당합니다.

참고 시스템은 이중 DNS 조회를 수행하여 원격 호스트 IP 주소의 유효성을 확보하고 확인합니다. 이중 DNS 조회는 연결 호스트의 IP 주소에 대한 역방향 DNS(PTR) 조회와 이어지는 PTR 조회 결과에 대한 Forward DNS(A) 조회로 구성됩니다. 그런 다음 시스템은 A 조회의 결과가 PTR 조회의 결과와 일치하는지 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, 7-4페이지
- 네트워크 소유자, 도메인 및 IP 주소별로 정의되는 발신자 그룹, 7-5페이지
- SenderBase Reputation 점수별로 발신자 그룹 정의, 7-6페이지
- DNS 목록을 쿼리하여 정의한 발신자 그룹, 7-7페이지

발신자 그룹 구문

표 7-1 HAT에서 원격 호스트 정의: 발신자 그룹 구문

구문	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. 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	IPv4 주소 범위
yourhost.example.com	정규화된 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 점수. 자세한 내용은 SenderBase Reputation 점수별로 발신자 그룹 정의, 7-6페이지 항목을 참조하십시오.
SBO:n	SenderBase 네트워크 소유자 식별 번호. 자세한 내용은 SenderBase Reputation 점수별로 발신자 그룹 정의, 7-6페이지 항목을 참조하십시오.
dnslist[dnsserver.domain]	DNS 목록 쿼리. 자세한 내용은 DNS 목록을 쿼리하여 정의한 발신자 그룹, 7-7페이지 항목을 참조하십시오.
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 이메일의 발신자를 인증하기 위한 내장형 방법이 없기 때문에 요청하지 않은 대량 이메일의 발신자가 자신의 ID를 숨기기 위해 다양한 전술을 성공적으로 활용해 왔습니다. 해당하는 예로는 메시지에 대한 봉투 발신자 주소의 스푸핑, 위조된 HELO 주소 사용 또는 단순하게 다양한 도메인 이름을 사용하여 순환하는 방법이 있습니다. 그 결과 많은 메일 관리자들이 "이 이메일을 모두 누가 보내고 있습니까?"라는 기본적인 의문을 갖게 되었습니다. 이 질문에 대한 답변으로, SenderBase Reputation Service에서 연결 호스트의 IP 주소에 기반하여 ID 기반 정보를 집계하기 위한 고유한 계층 구조를 개발했으며 이러한 구조에서는 발신자가 메시지를 위조하는 것이 사실상 불가능합니다.

IP 주소는 전송 메일 호스트의 IP 주소로 정의됩니다. Email Security 어플라이언스는 인터넷 프로토콜 버전 4(IPv4) 및 버전 6(IPv6 주소)을 모두 지원합니다.

도메인은 IP 주소에 대한 역방향(PTR) 조회에 따라 결정되며 지정된 두 번째 레벨의 도메인 이름(예: yahoo.com)과 함께 호스트 이름을 사용하는 엔터티로 정의됩니다.

네트워크 소유자는 ARIN(미국 인터넷 번호 등록 협회) 및 기타 소스와 같은 글로벌 등록 기관의 IP 주소 공간 할당에 기반하여 결정되며 IP 주소의 블록을 제어하는 엔터티(일반적으로 회사)로 정의됩니다.

조직은 SenderBase에 따라 결정되며 네트워크 소유자의 IP 블록 내에 있는 메일 게이트웨이의 특정한 그룹을 가장 밀접하게 제어하는 엔터티로 정의됩니다. 조직은 네트워크 소유자, 해당 네트워크 소유자 내부의 부서 또는 해당 네트워크 소유자의 고객과 동일할 수 있습니다.

관련 주제

- HAT 기반 정책 설정, 7-5페이지

HAT 기반 정책 설정

표 7-2는 네트워크 소유자 및 조직의 예를 보여줍니다.

표 7-2 네트워크 소유자 및 조직의 예

예 유형	네트워크 소유자	조직
네트워크 서비스 공급자	레벨 3 통신	Macromedia Inc. AllOutDeals.com GreatOffers.com
이메일 서비스 공급자	GE	GE Appliances GE Capital GE Mortgage
상업적 발신자	The Motley Fool	The Motley Fool

네트워크 소유자의 범위가 매우 다양할 수 있으므로 사용자의 메일 흐름 정책에 기반하는 적절한 엔터티는 조직입니다. SenderBase Reputation Service는 조직 레벨에 속하는 이메일 소스를 고유한 방식으로 이해하며 어플라이언스는 조직에 기반하는 정책을 자동으로 적용하기 위해 이러한 조직 레벨을 활용합니다. 위의 예에서 사용자가 "레벨 3 통신"을 HAT(Host Access Table)의 발신자 그룹으로 지정한 경우, SenderBase는 네트워크 소유자가 제어하는 개별 조직에 기반하는 정책을 적용합니다.

예를 들어, 위 표에서 사용자가 레벨 3에 대해 시간당 수신자 10명의 제한을 입력하는 경우, 어플라이언스는 Macromedia Inc., Alloutdeals.com 및 Greatoffers.com(레벨 3 네트워크 소유자에 대해 시간당 총 수신자 30명)에 대해 시간당 최대 10명의 수신자를 허용합니다. 이러한 방식의 이점은 해당 조직 중 하나에서 스팸을 시작하는 경우 레벨 3으로 제어되는 다른 조직이 영향을 받지 않는 것입니다. 이것은 "The Motley Fool" 네트워크 소유자의 예와 대조됩니다. 사용자가 속도 제한을 시간당 수신자 10명으로 제한하도록 설정한 경우 The Motley Fool 네트워크 소유자는 시간당 총 수신자 10명을 수신합니다.

메일 흐름 모니터링 기능은 발신자를 정의하고 발신자에 대한 메일 흐름 정책 의사결정을 내리기 위해 모니터링 툴을 제공하는 방법입니다. 지정된 발신자에 대한 메일 흐름 정책 의사결정을 내리려면 다음에 대해 질문해야 합니다.

- **이 발신자는 어떤 IP 주소를 제어합니까?**

  인바운드 이메일 처리를 제어하기 위해 메일 흐름 모니터 기능에서 사용하는 첫 번째 정보는 이 질문에 대한 답변입니다. 답변은 SenderBase Reputation Service를 쿼리하여 얻을 수 있습니다. SenderBase Reputation Service는 발신자(SenderBase 네트워크 소유자 또는 SenderBase 조직)의 상대적 크기에 대한 정보를 제공합니다. 이 질문에 대한 답변은 다음을 가정합니다.

  - 대규모 조직일수록 더 많은 IP 주소를 제어하고 보다 정상적인 이메일을 전송합니다.

- **조직의 크기에 따라 어떻게 전체 연결을 이 발신인에게 할당합니까?**

  - 대규모 조직일수록 더 많은 IP 주소를 제어하고 보다 정상적인 이메일을 전송합니다. 따라서, 대규모 조직은 어플라이언스에 더 많은 연결을 할당 받아야 합니다.
  - 대량 이메일 소스는 아웃소싱된 이메일 제공을 관리하는 ISP, NSP, 회사 또는 요청하지 않은 대량 이메일 소스인 경우가 많습니다. 아웃소싱된 이메일 제공을 관리하는 ISP, NSP 및 회사는 많은 IP 주소를 제어하는 조직이며 어플라이언스에 더 많은 연결을 할당받아야 합니다. 요청하지 않은 대량 이메일 발신자는 일반적으로 많은 IP 주소를 제어하지 않으며 대신 이보다 적은 수의 IP 주소를 통해 대량 메일을 전송합니다. 따라서 이러한 발신자는 어플라이언스에 더 적은 연결을 할당받아야 합니다.

메일 흐름 모니터 기능은 SenderBase 네트워크 소유자 및 SenderBase 조직 간의 차별화를 사용하여 SenderBase의 논리를 기반으로 발신자당 연결을 할당하는 방법을 결정합니다. 메일 흐름 모니터 기능의 사용에 대한 자세한 내용은 "이메일 보안 모니터링 사용" 장을 참조하십시오.

SenderBase Reputation 점수별로 발신자 그룹 정의

어플라이언스는 SenderBase Reputation Service에 쿼리하여 발신자의 평판 점수(SBRS)를 확인할 수 있습니다. SBRS는 SenderBase Reputation Service의 정보에 기반하여 IP 주소, 도메인 또는 조직에 할당된 숫자 값입니다. 점수 범위는 -10.0~+10.0이며 표 7-3에 설명되어 있습니다.

표 7-3 SenderBase Reputation 점수의 정의

점수	의미
-10.0	스팸 소스일 가능성이 가장 높음
0	보통 또는 권장할 정보로는 부족함
+10.0	신뢰할 만한 발신자일 가능성이 가장 큼
없음	이 발신자(일반적으로 스팸 소스)가 사용할 수 있는 정보가 없음

SBRS를 사용하여 발신자의 신뢰도에 기반하여 발신자에게 메일 흐름 정책을 적용하도록 어플라이언스를 구성합니다. 예를 들어, 점수가 -7.5 미만인 모든 발신자는 거부될 수 있습니다. 이 작업은 GUI를 사용할 경우 가장 쉽게 수행할 수 있습니다. 자세한 내용은 메시지 처리를 위해 발신자 그룹 만들기, 7-13페이지 항목을 참조하십시오. 그러나, 텍스트 파일로 내보낸 HAT를 수정하는 경우 SenderBase Reputation 점수를 포함하기 위한 구문은 표 7-4에 설명되어 있습니다.

표 7-4 SenderBase Reputation 점수에 대한 구문

`SBRS[n:n]`	SenderBase Reputation 점수. 발신자는 SenderBase Reputation Service를 쿼리하여 확인되며 범위 내에서 점수가 정의됩니다.
SBRS[none]	SBRS를 지정하지 않습니다(완전히 새로운 도메인은 SenderBase Reputation 점수가 없을 수 있음).

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

Network(네트워크) > Listener(리스너) 페이지 또는 CLI의 `listenerconfig -> setup` 명령을 사용하여 SenderBase Reputation Service를 쿼리하기 위해 리스너를 활성화합니다. 또한 SenderBase Reputation Service를 쿼리할 때 어플라이언스가 대기해야 하는 시간제한 값을 정의할 수 있습니다. 그런 다음 SenderBase Reputation Service를 조회하기 위해 GUI의 Mail Policies(메일 정책) 페이지의 값 또는 CLI의 `listenerconfig -> edit -> hostaccess` 명령을 사용하여 다양한 정책을 구성할 수 있습니다.

참고 SenderBase Reputation 점수에 대한 "임계값"을 지정하도록 메시지 필터를 생성하여 시스템에서 처리된 메시지에 추가 작업을 수행할 수 있습니다. 자세한 내용은 안티스팸 및 안티바이러스 장의 "SenderBase Reputation 규칙", "안티스팸 우회 시스템 작업" 및 "안티바이러스 우회 시스템 작업"을 참조하십시오.

DNS 목록을 쿼리하여 정의한 발신자 그룹

리스너의 HAT에서 발신자 그룹을 특정한 DNS 목록 서버에 대한 쿼리와 일치하도록 정의하는 기능을 사용할 수 있습니다. 이 쿼리는 원격 클라이언트 연결 시 DNS를 통해 수행됩니다. 원격 목록을 쿼리하기 위한 기능은 현재 메시지 필터 규칙("메시지 필터를 사용하여 이메일 정책 적용" 관련 장에서 "DNS 목록 규칙" 참조)으로도 존재하지만 메시지 콘텐츠 전체를 수신한 경우로만 한정됩니다.

이러한 메커니즘을 통해 DNS 목록을 쿼리하는 그룹에서 발신자를 구성하여 메일 흐름 정책을 이에 따라 조정할 수 있습니다. 예를 들어, 연결을 거부하거나 도메인 연결 동작을 제한할 수 있습니다.

참고 일부 DNS 목록은 다양한 응답(예: "127.0.0.1", "127.0.0.2", "127.0.0.3" 간 비교)을 사용하여 쿼리 대상인 IP 주소에 대한 다양한 정보를 표시합니다. 메시지 필터 DNS 목록 규칙("메시지 필터를 사용하여 이메일 정책 적용" 관련 장에서 "DNS 목록 규칙" 참조)을 사용하는 경우 다양한 값에 대한 쿼리 결과를 비교할 수 있습니다. 그러나, HAT에서 DNS 목록 서버가 쿼리되도록 지정하는 경우 간소화(즉 목록에 IP 주소가 나타나거나 나타나지 않음)를 위해 부울 연산만 지원됩니다.

참고 CLI에서의 쿼리에는 대괄호를 포함해야 합니다. 대괄호는 DNS 목록 쿼리를 GUI에서 지정할 때는 필요하지 않습니다. 쿼리를 테스트하려면 CLI의 `dnslistconfig` 명령을 사용하고 DNL 쿼리에 대해 일반 설정을 구성하거나 현재 DNS 목록 캐시를 플러시합니다.

이러한 메커니즘은 "올바른" 연결뿐만 아니라 "잘못된" 연결을 식별하는 데도 사용될 수 있습니다. 예를 들어, query.bondedsender.org에 대한 쿼리는 이메일 캠페인의 무결성을 보장하도록 Cisco 시스템의 Bonded Sender™ 프로그램을 사용하여 금융 채권을 게시한 연결 호스트에서 일치합니다. Bonded Sender 프로그램의 DNS 서버(자의에 의해 채권을 게시한 정상적인 이메일 발신자 나열)를 쿼리하도록 기본 화이트리스트 발신자 그룹을 수정하고 이에 따라 메일 흐름 정책을 조정할 수 있습니다.

메일 흐름 정책을 사용하여 이메일 발신자에 대한 액세스 규칙 정의

메일 흐름 정책을 통해 SMTP 대화 중에 발신자가 리스너에 보낸 이메일 메시지의 흐름을 제어하거나 제한할 수 있습니다. 메일 흐름 정책에서 다음 유형의 매개변수를 정의하여 SMTP 대화를 제어합니다.

- 연결 매개변수(예: 연결당 최대 메시지 수)
- 속도 제한 매개변수(예: 시간당 최대 수신자 수)
- SMTP 대화 중에 통신한 사용자 지정 SMTP 코드 및 응답 수정
- 스팸 탐지 활성화
- 바이러스 보호 활성화
- 암호화(예: TLS 사용하여 SMTP 연결 암호화)
- 인증 매개변수(예: DKIM 사용하여 수신 메일 확인)

최종적으로, 메일 흐름 정책은 원격 호스트의 연결에서 다음 작업 중 하나를 수행합니다.

- **ACCEPT.** 연결이 수락되고 그 이후에 이메일 수락이 Recipient Access Table(공용 리스너용)을 비롯한 리스너 설정에 따라 제한됩니다.
- **REJECT.** 연결이 처음에는 수락되지만 연결을 시도하는 클라이언트가 4XX 또는 5XX SMTP 상태 코드를 받습니다. 어떠한 이메일도 수락되지 않습니다.

참고 또한 SMTP 대화 시작 지점이 아닌 메시지 수신자 수준(RCPT To)에서 메시지를 거부하도록 AsyncOS를 구성할 수 있습니다. 이런 방식으로 메시지가 거부되면 메시지 거부가 지연되고 메시지가 바운스되므로 AsyncOS는 거부된 메시지에 대한 자세한 정보를 유지할 수 있습니다. 이 설정은 CLI의 `listenerconfig > setup` 명령을 통해 구성됩니다. 자세한 내용은 CLI를 통해 리스너를 생성하여 연결 요청 수신 대기, 5-12페이지 항목을 참조하십시오.

- **TCPREFUSE.** TCP 수준에서 연결이 거부됩니다.
- **RELAY.** 연결이 수락됩니다. 모든 수신자 수신이 허용되며 이는 Recipient Access Table에 따라 제한되지 않습니다.
- **CONTINUE.** HAT에서의 매핑이 무시되며 HAT 처리가 계속됩니다. 수신 연결이 CONTINUE에 해당하지 않는 이후 항목과 일치하는 경우, 해당 항목이 대신 사용됩니다. CONTINUE 규칙은 GUI에서 HAT를 쉽게 편집하는 데 사용됩니다. 자세한 내용은 메시지 처리를 위해 발신자 그룹 만들기, 7-13페이지 항목을 참조하십시오.

관련 주제

- HAT 변수 구문, 7-9페이지

HAT 변수 구문

표 7-5는 메일 흐름 정책에 정의된 사용자 지정 SMTP 및 속도 제한 배너와 결합하여 사용될 수 있는 변수 집합을 정의합니다. 변수 이름은 대소문자를 구분하지 않습니다. (즉 `$group`은 `$Group`과 동일합니다.)

표 7-5 HAT 변수 구문

변수	정의
`$Group`	HAT에서 일치하는 발신자 그룹의 이름으로 대체됩니다. 발신자 그룹에 이름이 없는 경우 "None(없음)"이 표시됩니다.
`$Hostname`	어플라이언스에서 검증된 경우 원격 호스트 이름으로 대체됩니다. IP 주소의 역방향 DNS 조회에는 성공했지만 호스트 이름을 반환하지 않는 경우 "None(없음)"이 표시됩니다. 역방향 DNS 조회에 실패하는 경우(예: DNS 서버에 연결할 수 없는 경우 또는 DNS 서버가 구성되지 않은 경우) "Unknown(알 수 없음)"이 표시됩니다.
`$OrgID`	SenderBase 조직 ID(정수 값)로 대체됩니다. 어플라이언스가 SenderBase 조직 ID를 얻을 수 없거나, SenderBase Reputation Service에서 값을 반환하지 않은 경우, "None(없음)"이 표시됩니다.
`$RemoteIP`	원격 클라이언트의 IP 주소로 대체됩니다.
`$HATEntry`	원격 클라이언트와 일치하는 HAT의 항목으로 대체됩니다.

관련 주제

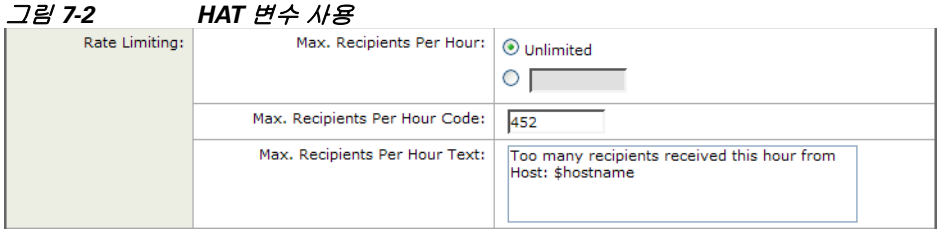
- HAT 변수 사용, 7-9페이지
- HAT 변수 테스트, 7-10페이지

HAT 변수 사용

참고 이 변수는 "이메일을 수신하도록 게이트웨이 구성" 장에 설명된 대로 `smtp_banner_text` 및 `max_rcpts_per_hour_text` 고급 HAT 매개변수와 함께 사용할 수 있습니다.

이러한 변수를 사용하여 다음과 같이 GUI에서 $TRUSTED 정책에서 승인된 연결에 대해 사용자 지정 SMTP 배너 응답 텍스트를 편집할 수 있습니다.

그림 7-2 HAT 변수 사용



또는 이와 유사하게 CLI에서 다음을 수행할 수 있습니다.

```
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 알려진 신뢰할 수 있는 머신의 IP 주소를 어플라이언스에 있는 리스너의 $WHITELIST 발신자 그룹에 추가합니다. 그런 다음 텔넷을 통해 해당 시스템에 연결합니다. SMTP 응답에서 변수 대체를 확인할 수 있습니다. 예를 들면 다음과 같습니다.

```
# telnet IP_address_of_Email_Security_Appliance

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 정의 발신자 그룹 및 메일 흐름 정책 이해

표 7-6은 공용 리스너를 만들 때 구성된 사전 정의 발신자 그룹 및 메일 흐름 정책을 나열한 것입니다.

표 7-6 공용 리스너를 위한 사전 정의 발신자 그룹 및 메일 흐름 정책

사전 정의 발신자 그룹	설명	기본 구성 메일 흐름 정책
WHITELIST	신뢰하는 발신자를 화이트리스트 발신자 그룹에 추가합니다. $TRUSTED 메일 흐름 정책은 신뢰하는 발신자의 이메일에 대해 속도 제한을 사용하지 않고 해당 발신자가 보낸 콘텐츠를 안티스팸 또는 안티바이러스 소프트웨어에서 검사하지 않도록 구성됩니다.	$TRUSTED
BLACKLIST	BLACKLIST 발신자 그룹에 속하는 발신자가 거부됩니다($BLOCKED 메일 흐름 정책에 설정된 매개변수 기준). 발신자를 이 그룹에 추가하면 SMTP HELO 명령에서 5XX SMTP 응답을 반환하여 해당 호스트에서의 연결을 거부합니다.	$BLOCKED
SUSPECTLIST	SUSPECTLIST 발신자 그룹은 수신 메일의 속도를 제한하거나 저하시키는 메일 흐름 정책을 포함합니다. 발신자가 의심스러운 경우, SUSPECTLIST 발신자 그룹에 이 발신자를 추가할 수 있으며 이때 메일 흐름 정책은 다음을 지정합니다. • 속도 제한은 세션당 최대 메시지 수, 메시지당 최대 수신자 수, 최대 메시지 크기, 원격 호스트에서 수락할 최대 동시 연결 수를 제한합니다. • 원격 호스트에서 시간당 최대 수신자는 시간당 수신자 20명으로 설정됩니다. 이 설정은 사용 가능한 최대 제한 값입니다. 이 매개변수가 적극적인 경우 시간당 수신할 수신자 수를 늘릴 수 있습니다. • 메시지 콘텐츠는 안티스팸 검사 엔진 및 안티바이러스 검사 엔진(이 시스템에서 이 기능을 활성화한 경우)에서 검사합니다. • SenderBase Reputation Service는 발신자에 대한 자세한 정보를 얻기 위해 쿼리됩니다.	$THROTTLED

표 7-6 공용 리스너를 위한 사전 정의 발신자 그룹 및 메일 흐름 정책 (계속)

사전 정의 발신자 그룹	설명	기본 구성 메일 흐름 정책
UNKNOWNLIST	알 수 없는 목록 발신자 그룹은 지정된 발신자에 사용해야 하는 메일 흐름 정책을 결정하지 못한 경우 유용하게 사용할 수 있습니다. 이 그룹의 메일 흐름 정책에서 이 그룹의 발신자에 대해 메일이 수락된다고 지정했지만 안티스팸 소프트웨어(시스템에서 활성화된 경우), 안티바이러스 검사 엔진 및 SenderBase Reputation Service를 모두 사용하여 발신자 및 메시지 콘텐츠에 대한 자세한 정보를 얻어야 합니다. 이 그룹의 발신자에 대한 속도 제한은 기본값으로 활성화됩니다. 바이러스 검사 엔진에 대한 자세한 내용은 안티바이러스 검사 개요, 12-1페이지 항목을 참조하십시오. SenderBase Reputation Service에 대한 자세한 내용은 SenderBase Reputation Service, 6-1페이지 항목을 참조하십시오.	$ACCEPTED
ALL	다른 발신자 모두에 적용되는 기본 발신자 그룹입니다. 자세한 내용은 기본 HAT 항목, 7-2페이지 항목을 참조하십시오.	$ACCEPTED

표 7-7은 개인 리스너를 만들 때 구성된 사전 정의 발신자 그룹 및 메일 흐름 정책을 나열한 것입니다.

표 7-7 개인 리스너를 위한 사전 정의 발신자 그룹 및 메일 흐름 정책

사전 정의 발신자 그룹	설명	기본 구성 메일 흐름 정책
RELAYLIST	릴레이하도록 허용해야 하는 발신자를 릴레이 목록 발신자 그룹에 추가합니다. $RELAYED 메일 흐름 정책은 릴레이하도록 허용한 발신자의 이메일에 대해 속도 제한을 사용하지 않고 해당 발신자가 보낸 콘텐츠를 안티스팸 검사 엔진 또는 안티바이러스 소프트웨어에서 검사하지 않도록 구성됩니다. **참고** 릴레이 목록 발신자 그룹은 시스템 설치 마법사를 실행할 때 이메일을 릴레이하도록 허용한 시스템을 포함합니다.	$RELAYED
ALL	다른 발신자 모두에 적용되는 기본 발신자 그룹입니다. 자세한 내용은 기본 HAT 항목, 7-2페이지 항목을 참조하십시오.	$BLOCKED

참고 이더넷 포트가 2개만 있는 어플라이언스 모델에서 시스템 설치 마법사를 실행하는 경우 하나의 리스너만 만들도록 프롬프트가 표시됩니다. 내부 시스템에 메일을 릴레이하는 데 사용되는 $RELAYED 메일 흐름 정책도 포함하는 공용 리스너를 만듭니다. 이더넷 포트가 2개 이상인 어플라이언스 모델의 경우 릴레이 목록 발신자 그룹 및 $RELAYED 메일 흐름 정책은 개인 리스너에만 나타납니다.

발신자 그룹의 메시지를 동일한 방식으로 처리

Mail Policies(메일 정책) > HAT Overview(HAT 개요) 및 Mail Flow Policy(메일 흐름 정책) 페이지에서 리스너가 발신자의 메시지를 처리하는 방법을 구성합니다. 발신자 그룹 및 메일 흐름 정책 생성, 편집 및 삭제를 통해 구성할 수 있습니다.

관련 주제

- 메시지 처리를 위해 발신자 그룹 만들기, 7-13페이지
- 기존 발신자 그룹에 발신자 추가, 7-14페이지
- 수신 연결에서 수행할 규칙의 순서 재정렬, 7-14페이지
- 발신자 검색, 7-15페이지
- 메일 흐름 정책을 사용하여 수신 메시지에 대한 규칙 정의, 7-15페이지
- 메일 흐름 정책에 대한 기본값 정의, 7-20페이지

메시지 처리를 위해 발신자 그룹 만들기

절차

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

2단계 Listener(리스너) 필드에서 편집할 리스너를 선택합니다.

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

4단계 발신자 그룹의 이름을 입력합니다.

5단계 발신자 그룹 목록에서 위치하는 순서를 선택합니다.

6단계 (선택 사항) 주석을 입력합니다(예: 이 발신자 그룹에 대한 정보 또는 설정 등).

7단계 이 발신자 그룹에 적용할 메일 흐름 정책을 선택합니다.

참고 이 그룹에 적용할 메일 흐름 정책을 모르는 경우(또는 메일 흐름 정책이 아직 없는 경우) 기본 "CONTINUE(정책 없음)" 메일 흐름 정책을 사용합니다.

8단계 (선택 사항) DNS 목록을 선택합니다.

9단계 (선택 사항) SBRS에 어떠한 정보도 없는 발신자를 포함합니다. 이것은 "없음"이라고 하며 일반적으로 의심스러운 발신자를 나타냅니다.

10단계 (선택 사항) DNS 목록을 입력합니다.

11단계 (선택 사항) 호스트 DNS 확인 설정을 구성합니다.

자세한 내용은 발신자 확인 구현 — 예 설정, 7-30페이지 항목을 참조하십시오.

12단계 **Submit and Add Senders(발신자 제출 및 추가)**를 클릭하여 그룹을 만들고 이 그룹에 발신자를 추가하기 시작합니다.

13단계 IPv4 주소, IPv6 주소 또는 호스트 이름을 사용하여 발신자를 입력합니다. 발신자는 IP 주소와 부분 호스트 이름의 범위를 포함할 수 있습니다.

참고 단일 발신자 그룹에서 중복 항목(동일한 도메인 또는 IP 주소)을 입력하려고 하면 중복된 항목이 삭제됩니다.

14단계 (선택 사항) 주석을 입력합니다.

15단계 변경사항을 제출하고 커밋합니다.

관련 주제

- 리스너의 발신자 평판 필터링 점수 임계값 편집, 6-5페이지

기존 발신자 그룹에 발신자 추가

절차

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

2단계 리스너마다 정의된 목록에서 발신자 그룹을 선택합니다.

3단계 변경사항을 제출하고 커밋합니다.

참고 발신자 그룹에 도메인을 추가하는 경우 실제 도메인 2개가 GUI에 나열됩니다. 예를 들어, Add to Sender Group(발신자 그룹에 추가) 페이지에서 `example.net` 도메인을 추가하는 경우 `example.net` 및 `.example.net`이 모두 추가됩니다. 두 번째 항목은 `example.net`의 하위 도메인에 있는 모든 호스트가 발신자 그룹에 추가되는 것을 의미합니다. 자세한 내용은 발신자 그룹 구문, 7-4페이지 항목을 참조하십시오.

참고 발신자 그룹에 추가하는 하나 이상의 발신자가 해당 발신자 그룹에 이미 존재하는 발신자와 중복되는 경우, 중복된 발신자는 추가되지 않고 확인 메시지가 표시됩니다.

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

관련 주제

- 스팸 필터로부터 어플라이언스에서 생성된 메시지 보호, 13-14페이지
- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 13-2페이지

수신 연결에서 수행할 규칙의 순서 재정렬

리스너에 발신자 그룹을 추가한 경우, 발신자 그룹 순서를 편집할 수 있습니다.

리스너에 연결을 시도하는 각 호스트에 대해 위에서부터 아래로 HAT를 읽습니다. 규칙이 연결 호스트와 일치하는 경우, 해당 연결에 대해 즉시 작업을 수행합니다.

절차

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

2단계 Listener(리스너) 필드에서 편집할 리스너를 선택합니다.

3단계 **Edit Order(순서 편집)**를 클릭합니다.

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

릴레이 목록(특정 하드웨어 모델만 해당) 다음에 WHITELIST, BLACKLIST, SUSPECTLIST 및 UNKNOWNLIST가 오는 기본 순서를 유지하는 것이 좋습니다.

5단계 변경사항을 제출하고 커밋합니다.

발신자 검색

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

메일 흐름 정책을 사용하여 수신 메시지에 대한 규칙 정의

메일 흐름 정책을 만들기 전에 다음 규칙 및 지침을 고려합니다.

- 정책의 기본값은 "Use Default(기본값 사용)" 라디오 버튼을 선택한 경우 "회색"으로 표시됩니다. 기본값을 덮어쓰려면 "On(켜기)" 라디오 버튼을 선택하고 현재 액세스 가능한 값을 변경하여 기능 또는 설정을 활성화합니다. 기본값을 정의하려면 메일 흐름 정책에 대한 기본값 정의, 7-20페이지 항목을 참조하십시오.
- 일부 매개변수는 특정한 사전 구성에 따라 다릅니다. (예를 들어, 디렉토리 수집 공격 방지를 설정하려면 LDAP 인수 쿼리를 구성해야 합니다.)

절차

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

2단계 **Add Policy(정책 추가)**를 클릭합니다.

3단계 표 7-8에 설명된 정보를 입력합니다.

표 7-8 메일 흐름 정책 매개변수

매개변수	설명
연결	
최대 메시지 크기	리스너에서 수락할 최대 메시지 크기입니다. 가장 작은 최대 메시지 크기는 1킬로바이트입니다.
단일 IP의 최대 동시 연결	단일 IP 주소에서 이 리스너에 연결하기 위해 허용되는 최대 동시 연결 수입니다.
연결당 최대 메시지 수	원격 호스트에서 연결당 이 리스너를 통해 전송할 수 있는 최대 메시지 수입니다.

표 7-8 메일 흐름 정책 매개변수 (계속)

매개변수	설명
메시지당 최대 수신자 수	이 호스트에서 수락할 메시지당 최대 수신자 수입니다.
SMTP 배너	
사용자 지정 SMTP 배너 코드	이 리스너를 통해 연결이 설정된 경우 반환되는 SMTP 코드입니다.
사용자 지정 SMTP 배너 텍스트	이 리스너를 통해 연결이 설정된 경우 반환되는 SMTP 배너 텍스트입니다. **참고** 이 필드에서 몇 가지 변수를 사용할 수 있습니다. 자세한 내용은 HAT 변수 구문, 7-9페이지 항목을 참조하십시오.
사용자 지정 SMTP 거부 배너 코드	이 리스너에서 연결을 거부하는 경우 반환되는 SMTP 코드입니다.
사용자 지정 SMTP 거부 배너 텍스트	이 리스너에서 연결을 거부하는 경우 반환되는 SMTP 배너 텍스트입니다.
SMTP 배너 호스트 이름 재정의	기본적으로, 어플라이언스는 원격 호스트에 SMTP 배너를 표시할 때 리스너의 인터페이스와 연결되어 있는 호스트 이름을 포함합니다(예: `220-`*hostname* `ESMTP`). 여기에서 다른 호스트 이름을 입력하여 이 배너를 재정의하도록 선택할 수 있습니다. 또한, 이 배너에서 호스트 이름을 표시하지 *않도록* 호스트 이름 필드를 비워둘 수 있습니다.
호스트에 대한 속도 제한	
시간당 최대 수신자 수	이 리스너가 원격 호스트로부터 수신할 때의 시간당 최대 수신자 수입니다. 발신자 IP 주소당 수신자의 수는 전역으로 추적됩니다. 각 리스너는 고유한 속도 제한 임계값을 추적하지만 모든 리스너가 단일 카운터를 대상으로 검증하기 때문에 동일한 IP 주소(발신자)가 여러 리스너에 연결하는 경우 속도 제한을 초과할 가능성이 큽니다. **참고** 이 필드에서 몇 가지 변수를 사용할 수 있습니다. 자세한 내용은 HAT 변수 구문, 7-9페이지 항목을 참조하십시오.
시간당 최대 수신자 코드	호스트가 이 리스너에 정의된 시간당 최대 수신자 수를 초과하는 경우 반환되는 SMTP 코드입니다.
시간당 최대 수신자 초과 텍스트	호스트가 이 리스너에 정의된 시간당 최대 수신자 수를 초과하는 경우 반환되는 SMTP 배너 텍스트입니다.
발신자에 대한 속도 제한	
시간 간격당 최대 수신자 수	MAIL FROM 주소에 기반하여 이 리스너가 고유한 봉투 발신자로부터 지정된 시간 동안 수신하는 최대 수신자 수입니다. 수신자 수는 전역으로 추적됩니다. 각 리스너는 고유한 속도 제한 임계값을 추적하지만 모든 리스너가 단일 카운터를 대상으로 검증하기 때문에 동일한 MAIL FROM 주소의 메시지를 여러 리스너에서 수신하는 경우 속도 제한을 초과할 가능성이 큽니다. 기본 최대 수신자 수를 사용할지 여부를 선택하고 무제한 수신자를 수락하거나 다른 최대 수신자 수를 지정합니다. 기본 메일 흐름 정책 설정을 사용하여 다른 메일 흐름 정책에 따라 기본적으로 사용할 시간 간격 및 최대 수신자 수를 지정합니다. 시간 간격은 기본 메일 흐름 정책을 사용하는 경우에만 지정할 수 있습니다.

표 7-8 메일 흐름 정책 매개변수 (계속)

매개변수	설명
발신자 속도 제한 초과 오류 코드	봉투 발신자가 이 리스너에 정의된 시간 간격 동안 최대 수신자 수를 초과하는 경우 반환되는 SMTP 코드입니다.
발신자 속도 제한 초과 오류 텍스트	봉투 발신자가 이 리스너에 정의된 시간 간격 동안 최대 수신자 수를 초과하는 경우 반환되는 SMTP 배너 텍스트입니다.
예외	특정한 봉투 발신자를 정의된 속도 제한에서 제외하려는 경우, 해당 봉투 발신자가 포함된 주소 목록을 선택합니다. 자세한 내용은 수신 연결 규칙에 대해 발신자 주소 목록 사용, 7-21페이지 항목을 참조하십시오.
흐름 제어	
흐름 제어에 SenderBase 사용	이 리스너에 대한 SenderBase Reputation Service "조회"를 활성화합니다.
IP 주소의 유사성을 기준으로 그룹화: (주요 비트 0~32)	대형 CIDR 블록에서 리스너의 HAT(Host Access Table)에 있는 항목을 관리하면서 IP별 주소에 기반하여 수신 메일을 추적하고 수신을 제한하는 데 사용됩니다. 이 기준에 따라 속도 제한을 위해 유사한 IP 주소를 그룹화하여 주요 비트(0~32)의 범위를 정의합니다. 이때 해당 범위의 각 IP 주소에 대한 개별 카운터는 유지합니다. "SenderBase 사용"을 비활성화해야 합니다. HAT 주요 비트에 대한 자세한 내용은 "라우팅 및 전달 기능 구성" 장의 "HAT 주요 비트 기능"을 참조하십시오.
DHAP(디렉토리 수집 공격 방지)	
디렉토리 수집 공격 방지: 시간당 올바르지 않은 최대 수신자 수	이 리스너가 원격 호스트로부터 수신할 때의 시간당 올바르지 않은 최대 수신자 수입니다. 이 임계값은 SMTP 대화에서 삭제되었거나 작업 큐에서 바운스된(연결된 리스너의 LDAP 수락 설정에 구성된 대로) 올바르지 않은 LDAP 수신자에 대한 총 메시지 수와 RAT 거부 및 SMTP Call-Ahead 서버 거부의 총 수를 나타냅니다. LDAP 수락 쿼리의 DHAP 구성에 대한 자세한 내용은 "LDAP 쿼리" 장을 참조하십시오.
디렉토리 수집 공격 방지: SMTP 대화 도중에 DHAP 임계값에 도달하면 연결 삭제	올바르지 않은 수신자 임계값에 도달하는 경우 어플라이언스가 호스트에 대한 연결을 삭제합니다.
시간당 올바르지 않은 최대 수신자 코드:	연결을 삭제할 때 사용할 코드를 지정합니다. 기본 코드는 550입니다.
시간당 올바르지 않은 최대 수신인 텍스트:	삭제된 연결에 사용할 텍스트를 지정합니다. 기본 텍스트는 "Too many invalid recipients."입니다.
SMTP 대화 도중에 DHAP 임계값에 도달하면 연결 삭제	SMTP 대화 도중에 DHAP 임계값에 도달하면 연결 삭제를 활성화합니다.
시간당 올바르지 않은 최대 수신자 코드	SMTP 대화 도중 DHAP 때문에 연결을 삭제할 때 사용하는 코드를 지정합니다. 기본 코드는 550입니다.
시간당 올바르지 않은 최대 수신인 텍스트:	SMTP 대화 도중 DHAP 때문에 연결을 삭제할 때 사용하는 텍스트를 지정합니다.
스팸 탐지	
안티스팸 검사	이 리스너에서 안티스팸 검사를 활성화합니다.
바이러스 탐지	

표 7-8 메일 흐름 정책 매개변수 (계속)

매개변수	설명
안티바이러스 검사	이 리스너에서 안티바이러스 검사를 활성화합니다.
암호화 및 인증	
TLS	이 리스너에 대한 SMTP 대화에서 TLS(전송 계층 보안)를 거부, 기본 설정 또는 필수로 지정합니다. Preferred를 선택한 경우 해당 도메인 및 이메일 주소를 지정하는 주소 목록을 선택하여 특정 도메인 또는 특정 이메일 주소를 사용하는 봉투 발신자에 대해 TLS를 필수로 설정할 수 있습니다. 이 목록에 있는 도메인 또는 주소와 일치하는 봉투 발신자가 TLS를 사용하지 않는 연결을 통해 메시지를 전송하려고 시도하는 경우 어플라이언스가 이 연결을 거부하므로 발신자는 TLS를 사용하여 다시 시도해야 합니다. Verify Client Certificate(클라이언트 인증서 확인) 옵션을 사용하면 클라이언트 인증서가 유효한 경우 Email Security 어플라이언스가 사용자 메일 애플리케이션에 대한 TLS 연결을 설정합니다. TLS Preferred(TLS 기본 설정) 옵션을 선택하면, 사용자에게 인증서가 없더라도 어플라이언스는 계속 비TLS 연결을 허용하지만 사용자의 인증서가 유효하지 않은 경우에는 연결을 거부합니다. TLS Required(TLS 필수) 옵션을 선택하면, 어플라이언스가 연결을 허용하기 위해서는 사용자에게 유효한 인증서가 있어야 합니다. 주소 목록 만들기에 대한 자세한 내용은 수신 연결 규칙에 대해 발신자 주소 목록 사용, 7-21페이지 항목을 참조하십시오. TLS 연결을 위한 클라이언트 인증서 사용에 대한 자세한 내용은 어플라이언스에서 TLS 연결 설정, 26-53페이지 항목을 참조하십시오.
SMTP 인증	원격 호스트에서 리스너에 연결할 때 SMTP 인증을 허용, 허용 안 함 또는 필수로 지정합니다. SMTP 인증에 대해서는 "LDAP 쿼리" 장에 자세히 설명되어 있습니다.
TLS와 SMTP 인증이 모두 사용 가능한 경우:	SMTP 인증을 위해 TLS가 필요합니다.
도메인 키 서명	
도메인 키/DKIM 서명	이 리스너에서 도메인 키 또는 DKIM 서명을 활성화합니다(수락 및 릴레이만 해당).
DKIM 확인	DKIM 확인을 활성화합니다.
S/MIME 암호 해독 및 확인	
S/MIME 암호 해독/확인	• S/MIME 암호 해독 또는 확인을 활성화합니다. • S/MIME 확인 후 메시지에서 디지털 서명을 유지하거나 제거할지를 선택합니다. 3중으로 래핑된 메시지의 경우 내부 서명만 유지 또는 제거됩니다.
S/MIME 공개 키 수집	
S/MIME 공개 키 수집	S/MIME 공개 키 수집을 활성화합니다.
확인 실패 시 인증서 수집	수신 서명 메시지의 확인에 실패하는 경우 공개 키를 수집할지 여부를 선택합니다.
업데이트된 인증서 저장	업데이트된 공개 키를 수집할지 여부를 선택합니다.

표 7-8 메일 흐름 정책 매개변수 (계속)

매개변수	설명
SPF/SIDF 확인	
SPF/SIDF 확인 활성화	이 리스너에서 SPF/SIDF 서명을 활성화합니다. 자세한 내용은 "이메일 인증" 장을 참조하십시오.
적합성 수준	SPF/SIDF 적합성 수준을 설정합니다. SPF, SIDF 또는 SIDF 호환 가능에서 선택할 수 있습니다. 자세한 내용은 "이메일 인증" 장을 참조하십시오.
'Resent-Sender:' 또는 'Resent-From:'이 사용된 경우 PRA 다운그레이드 확인 결과:	SIDF 호환 가능 적합성 수준을 선택하는 경우, 메시지에 Resent-Sender: 또는 Resent-From: 헤더가 있으면 PRA ID 확인의 통과 결과를 None으로 다운그레이드할지 여부를 구성합니다. 보안을 위해 이 옵션을 선택할 수 있습니다.
HELO 테스트	HELO ID를 대상으로 테스트를 수행할지 여부를 구성합니다(SPF 및 SIDF 호환 가능 적합성 수준 사용).
DMARC 확인	
DKIM 확인을 활성화합니다.	이 리스너에서 DMARC 확인을 활성화합니다. 자세한 내용은 DMARC 확인, 20-35페이지 항목을 참조하십시오.
DMARC 확인 프로파일 사용	이 리스너에서 사용할 DMARC 확인 프로파일을 선택합니다.
DMARC 피드백 보고서	DMARC 집계 피드백 보고서 전송을 활성화합니다. DMARC 집계 피드백 보고서에 대한 자세한 내용은 DMARC 집계 보고서, 20-41페이지 항목을 참조하십시오. **참고** DMARC 사양에서는 피드백 보고서 메시지가 DMARC를 준수해야 합니다. 이러한 메시지에 DKIM 서명을 하거나 적절한 SPF 레코드를 게시해야 합니다.
태그가 지정되지 않은 바운스	
다음과 같은 태그 없는 바운드가 유효할 수 있습니다.	바운스 확인 태그 지정("라우팅 및 제공 기능 구성" 장에 설명되어 있음)이 활성화된 경우에만 적용됩니다. 기본적으로, 어플라이언스는 바운스 확인 설정에 따라 태그가 지정되지 않은 바운스를 유효하지 않다고 판단하여 해당 바운스를 거부하거나 사용자 지정 헤더를 추가합니다. 태그가 지정되지 않은 바운스를 유효하다고 판단하도록 선택한 경우 어플라이언스는 바운스 메시지를 수락합니다.
봉투 발신자 DNS 확인	
	발신자 확인, 7-27페이지 항목을 참조하십시오.
예외 테이블	
예외 테이블 사용	발신자 확인 도메인 예외 테이블을 사용합니다. 단 하나의 예외 테이블만 사용 가능하며 메일 흐름 정책마다 이 테이블을 활성화할 수 있습니다. 자세한 내용은 발신자 확인 예외 테이블, 7-30페이지 항목을 참조하십시오.

참고 안티스팸 또는 안티바이러스 검사가 HAT에서 전역으로 활성화된 경우, 어플라이언스에서 메시지를 수락하기 때문에 안티스팸 또는 안티바이러스 검사를 위해 메시지에 플래그가 지정됩니다. 메시지를 수락한 이후에 안티스팸 또는 안티바이러스 검사가 비활성화되면 메시지는 작업 큐를 떠날 때도 여전히 검사를 받게 됩니다.

4단계 변경사항을 제출하고 커밋합니다.

메일 흐름 정책에 대한 기본값 정의

절차

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

2단계 Listener(리스너) 필드에서 편집할 리스너를 선택합니다.

3단계 구성한 메일 흐름 정책 아래의 **Default Policy Parameters(기본 정책 매개변수)** 링크를 클릭합니다.

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

속성에 대한 자세한 내용은 메일 흐름 정책을 사용하여 수신 메시지에 대한 규칙 정의, 7-15페이지 항목을 참조하십시오.

5단계 변경사항을 제출하고 커밋합니다.

Host Access Table 구성 작업

Host Access Table에 저장된 모든 정보를 파일로 내보내고 파일에 저장된 Host Access Table 정보를 리스너의 어플라이언스로 가져와 기존의 모든 Host Access Table 정보를 재정의할 수 있습니다.

관련 주제

- Host Access Table 구성을 외부 파일로 내보내기, 7-20페이지
- 외부 파일에서 Host Access Table 구성 가져오기, 7-21페이지

Host Access Table 구성을 외부 파일로 내보내기

절차

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

2단계 Listener(리스너) 메뉴에서 수정할 리스너를 선택합니다.

3단계 **Export HAT(HAT 내보내기)**를 클릭합니다.

4단계 내보낸 HAT 파일의 파일 이름을 입력합니다. 어플라이언스의 구성 디렉토리에 생성할 파일의 이름입니다.

5단계 변경사항을 제출하고 커밋합니다.

외부 파일에서 **Host Access Table** 구성 가져오기

HAT를 가져올 때 기존의 모든 HAT 항목은 현재 HAT에서 제거됩니다.

절차

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

2단계 Listener(리스너) 메뉴에서 수정할 리스너를 선택합니다.

3단계 **Import HAT(HAT 가져오기)**를 클릭합니다.

4단계 목록에서 파일을 선택합니다.

참고 가져올 파일은 어플라이언스의 구성 디렉토리에 있어야 합니다.

5단계 **Submit(제출)**을 클릭합니다. 기존 HAT 항목을 모두 제거할 것인지 확인하는 경고 메시지가 표시됩니다.

6단계 **Import(가져오기)**를 클릭합니다.

7단계 변경사항을 커밋합니다.

파일에 "주석"을 추가할 수 있습니다. '#' 문자로 시작하는 줄은 주석으로 처리되며 AsyncOS에서 무시됩니다. 예를 들면 다음과 같습니다.

```
# File exported by the GUI at 20060530T215438

$BLOCKED

    REJECT {}

[ ... ]
```

수신 연결 규칙에 대해 발신자 주소 목록 사용

메일 흐름 정책을 사용하면 속도 제한 예외 및 필수 TLS 연결 등 봉투 발신자 그룹에 적용되는 특정한 설정에 주소 목록을 사용할 수 있습니다. 주소 목록은 이메일 주소, 도메인, 부분 도메인 및 IP 주소로 구성됩니다. GUI의 **Mail Policies(메일 정책) > Address Lists(주소 목록)** 페이지 또는 CLI의 `addresslistconfig` 명령을 사용하여 주소 목록을 만들 수 있습니다. Address Lists(주소 목록) 페이지에는 주소 목록을 사용하는 모든 메일 흐름 정책과 어플라이언스에 있는 모든 주소 목록이 표시됩니다.

절차

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

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

3단계 주소 목록의 이름을 입력합니다.

4단계 주소 목록의 설명을 입력합니다.

5단계 (선택 사항) 주소 목록에서 전체 이메일 주소를 사용하도록 적용하려면 **Allow only full Email Addresses(전체 이메일 주소만 허용)**를 선택합니다.

6단계 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 주소는 사용할 수 없습니다.

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

도메인 및 IP 주소는 `@` 문자로 시작해야 합니다.

이메일 주소를 쉼표로 구분합니다. 새로운 행을 사용하여 주소를 구분하는 경우, AsyncOS는 입력한 항목을 쉼표로 구분된 목록으로 자동 변환합니다.

7단계 변경사항을 제출하고 커밋합니다.

SenderBase 설정 및 메일 흐름 정책

어플라이언스에 대한 연결을 분류하고 메일 흐름 정책을 적용하기 위해(속도 제한 포함 또는 포함 안 함) 리스너는 다음 방법을 사용합니다.

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

자세한 내용은 네트워크 소유자, 도메인 및 IP 주소별로 정의되는 발신자 그룹, 7-5페이지 항목을 참조하십시오.

"분류" 단계에서는 발송 호스트 IP 주소를 사용하여 인바운드 SMTP 세션(공용 리스너에서 수신됨)을 발신자 그룹으로 분류합니다. 해당 발신자 그룹과 연결된 메일 흐름 정책은 활성화된 속도 제한에 대한 매개변수를 보유할 수 있습니다. (속도 제한은 세션당 최대 메시지 수, 메시지당 최대 수신자 수, 최대 메시지 크기, 원격 호스트에서 수락할 최대 동시 연결 수를 제한합니다.)

일반적으로 이 프로세스에서 수신자는 이름이 지정된 발신자 그룹의 각 발신자를 기준으로 계산됩니다. 동일한 시간 이내에 여러 발신자로부터 메일을 수신하는 경우 모든 발신자에 대한 총 수신자 수가 한계값과 비교됩니다.

이 계산 방법에는 다음과 같이 몇 가지 예외가 있습니다.

- 네트워크 소유자가 분류를 수행하는 경우 SenderBase Reputation Service는 자동으로 대형 주소 블록을 소형 블록으로 나눕니다.

  수신자 계산 및 수신자 속도 제한은 소형 블록별로 개별적으로 수행됩니다(일반적으로, /24 CIDR 블록과 동일하나 모든 경우에 해당하지는 않음).
- HAT 주요 비트 기능이 사용되는 경우, 정책과 연결된 주요 비트 매개변수를 적용하여 주소의 대형 블록을 소형 블록으로 나눌 수 있습니다.

이 매개변수는 **Mail Flow Policy(메일 흐름 정책) -> Rate Limiting(속도 제한)** 단계와 관련이 있습니다. 이것은 발신자 그룹에서 IP 주소를 구분하는 데 사용될 수 있는 "네트워크/비트" CIDR 표기법의 "비트" 필드와 동일하지 않습니다.

기본적으로, SenderBase Reputation Service 및 IP 프로파일링 지원은 공용 리스너에 대해 *활성화*되고 개인 리스너에 대해 *비활성화*됩니다.

관련 주제

- SenderBase 쿼리에 대한 시간 제한, 7-23페이지
- HAT 주요 비트 기능, 7-23페이지

SenderBase 쿼리에 대한 시간 제한

리스너를 구성할 때 어플라이언스가 SenderBase Reputation Service에서 쿼리된 정보를 캐시하는 기간을 결정할 수 있습니다. 그런 다음 메일 흐름 정책을 구성할 때 SenderBase를 활성화하여 리스너에 대한 메일 흐름을 제어할 수 있습니다.

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

HAT 주요 비트 기능

AsyncOS 3.8.3 릴리스부터 대형 CIDR 블록에서 리스너의 HAT(Host Access Table)에 있는 발신자 그룹 항목을 관리하면서 IP별 주소에 기반하여 수신 메일을 추적하고 수신을 제한할 수 있습니다. 예를 들어, 수신 연결이 호스트 "10.1.1.0/24"와 일치하는 경우, 카운터는 모든 트래픽을 하나의 대형 카운터로 집계하는 대신 해당 범위 내에서 개별 주소마다 생성될 수 있습니다.

참고 주요 비트 HAT 정책 옵션을 적용하려면, HAT의 Flow Control(흐름 제어) 옵션에서 "사용자 SenderBase"를 활성화하지 *않아야 합니다*(또는 CLI의 경우 "SenderBase 평판 필터 및 IP 프로파일링 지원을 활성화하시겠습니까?"라는 질문에 **No**라고 대답합니다. 이 질문을 통해 `listenerconfig -> setup` 명령에서 SenderBase Information Service가 비활성화됩니다). 즉, HAT 주요 비트 기능 및 SenderBase IP 프로파일링 지원 활성화는 함께 처리될 수 없습니다.

대부분의 경우, 이 기능을 사용하여 발신자 그룹을 *폭넓게* 정의할 수 있습니다(즉, "10.1.1.0/24" 또는 "10.1.0.0/16"과 같은 대형 IP 주소 그룹). 반면 메일 흐름 속도 제한은 소형 IP 주소 그룹에 *한정적으로* 적용합니다.

HAT 주요 비트 기능은 시스템의 다음 구성 요소에 해당합니다.

- HAT 구성, 7-24페이지
- 주요 비트 HAT 정책 옵션, 7-24페이지
- 수신 제어 주기성, 7-25페이지

HAT 구성

HAT 구성은 발신자 그룹 및 메일 흐름 정책으로 이루어집니다. 발신자 그룹 구성은 발신자의 IP 주소가 "분류"되는 방법을 정의합니다(발신자 그룹에 속함). 메일 흐름 정책 구성은 해당 IP 주소에서 SMTP 세션이 제어되는 방법을 정의합니다. 이 기능을 사용하는 경우, IP 주소는 "CIDR 블록(예 10.1.1.0/24) 발신자 그룹으로 분류된" 상태에서 개별 호스트로 제어됩니다(/32). 이러한 구성은 "signficant_bits" 정책 구성 설정에서 수행할 수 있습니다.

주요 비트 HAT 정책 옵션

HAT 구문은 signficant_bits 구성 옵션에 사용할 수 있습니다. HAT에서 기본값 또는 특정한 메일 흐름 정책을 편집하는 경우(예:`listenerconfig -> edit -> hostaccess -> default` 명령 실행) 다음 조건에서 아래 질문이 나타납니다.

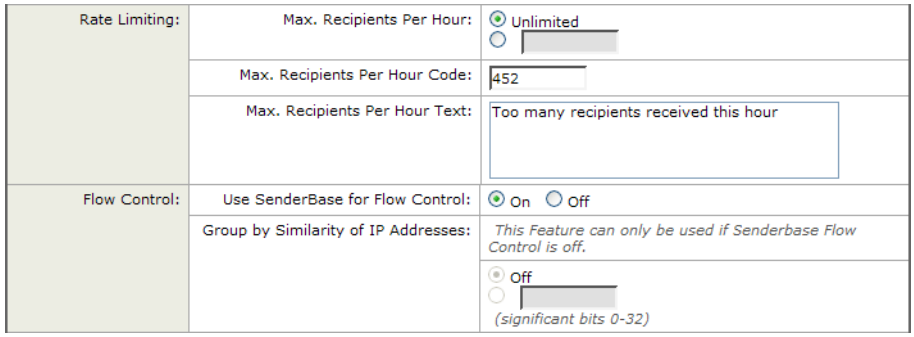
- 속도 제한이 활성화된 경우
  - 흐름 제어에 SenderBase 사용이 비활성화된 경우
  - DHAP(디렉토리 수집 공격 방지)가 메일 흐름 정책(기본값 또는 특정 메일 흐름 정책)에 활성화된 경우

예를 들면 다음과 같습니다.

```
Do you want to enable rate limiting per host?  [N]> y


Enter the maximum number of recipients per hour from a remote host.

[]> 2345


Would you like to specify a custom SMTP limit exceeded response? [Y]> n


Would you like to use SenderBase for flow control by default?  [N]> n


Would you like to group hosts by the similarity of their IP addresses?  [N]> y


Enter the number of bits of IP address to treat as significant, from 0 to 32.

[24]>
```

이 기능은 Mail Policies(메일 정책) > Mail Flow Policies(메일 흐름 정책) 페이지의 GUI에서도 확인할 수 있습니다.

그림 7-3 HAT 주요 비트 기능 활성화



흐름 제어를 위해 SenderBase 사용 옵션이 "OFF(끄기)"로 설정된 경우 또는 디렉토리 수집 공격 방지가 활성화된 경우, "주요 비트" 값은 연결 중인 발신자의 IP 주소에 적용되고 결과물인 CIDR 표기법은 HAT에 정의되어 있는 발신자 그룹과 일치시키기 위한 토큰으로 사용됩니다. CIDR 블록에 포함되는 가장 오른쪽 비트는 문자열을 구성할 때 "zero out(제로 아웃)" 됩니다. 따라서, IP 주소 1.2.3.4에서 연결되고 significant_bits 옵션이 24로 설정된 정책에서 일치하는 경우, 결과로 생성되는 CIDR 블록은 1.2.3.0/24입니다. 이 기능을 사용하여 HAT 발신자 그룹 항목(예: 10.1.1.0/24)은 해당 그룹(위의 예제에서 32)에 할당된 정책의 주요 비트 항목에서 다양한 네트워크 주요 비트(24)를 가질 수 있습니다.

수신 제어 주기성

전역 구성 옵션은 수신 제어 카운터의 재설정 시기를 조정하기 위해 사용됩니다. 대량의 IP 주소를 가지는 카운터를 유지 관리하는 시스템의 사용량이 매우 높을 경우 카운터를 더 자주 재설정하도록 구성(예: 60분이 아닌 15분마다 재설정)하면 데이터가 관리할 수 없는 크기로 증가하지 않으므로 시스템 성능에 영향을 주지 않습니다.

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

GUI에서 전역 설정을 사용하여 이 시간을 조정할 수 있습니다(자세한 내용은 리스너의 전역 설정 구성, 5-4페이지 참조).

또한 CLI의 `listenerconfig -> setup` 명령을 사용하여 시간을 조정할 수 있습니다.

```
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.

[]> setup


Enter the global limit for concurrent connections to be allowed across all listeners.

[300]>


Enter the global limit for concurrent TLS connections to be allowed across all listeners.

[100]>


Enter the maximum number of message header lines.  0 indicates no limit.

[1000]>


1. Allow SenderBase to determine cache time (Recommended)

2. Don't cache SenderBase data.

3. Specify your own cache time.

[1]> 3


Enter the time, in seconds, to cache SenderBase data:

[300]>


Enter the rate at which injection control counters are reset.

[1h]> 15m


Enter the timeout for unsuccessful inbound connections.

[5m]>


Enter the maximum connection time for inbound connections.

[15m]>
```

```
What hostname should Received: headers be stamped with?
1. The hostname of the Virtual Gateway(tm) used for delivering the message
2. The hostname of the interface the message is received on

[2]>


The system will always add a Message-ID header to outgoing messages that don't already
have one.  Would you like to do the same for incoming messages? (Not recommended.) [N]>


By default connections with a HAT REJECT policy 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]>


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


[]>
```

발신자 확인

DNS에서 확인할 수 없는 도메인 또는 IP 주소를 가진 발신자가 스팸 및 원치 않는 메일을 자주 전송합니다. DNS 확인을 통해 발신자 및 프로세스 메일에 대해 신뢰할 수 있는 정보를 얻을 수 있습니다. SMTP 대화(발신자의 IP 주소에 대한 DNS 조회에 따라 연결 필터링)를 수행하기 전에 발신자를 확인하면 어플라이언스에서 메일 파이프라인을 통해 처리되는 정크 메일의 양을 줄일 수 있습니다.

확인되지 않은 발신자가 보낸 메일은 자동으로 삭제되지 않습니다. 대신, AsyncOS는 발신자 확인 설정을 제공하여 어플라이언스에서 확인되지 않은 발신자가 보낸 메일을 처리하는 방법을 결정할 수 있습니다. 예를 들어, SMTP 대화를 수행하기 전에 확인되지 않은 발신자가 보낸 모든 메일을 자동으로 차단하거나 확인되지 않은 발신자를 제한하도록 어플라이언스를 구성할 수 있습니다.

발신자 확인 기능은 다음 구성 요소로 이루어집니다.

- **연결 호스트 확인.** SMTP 대화 이전에 수행됩니다. 자세한 내용은 발신자 확인: 호스트, 7-28페이지 항목을 참조하십시오.
- **봉투 발신자의 도메인 영역 확인.** SMTP 대화 중에 수행됩니다. 자세한 내용은 발신자 확인: 봉투 발신자, 7-28페이지 항목을 참조하십시오.

관련 주제

- 발신자 확인: 호스트, 7-28페이지
- 발신자 확인: 봉투 발신자, 7-28페이지

발신자 확인: 호스트

발신자는 다양한 이유로 확인이 안되는 경우가 있습니다. 예를 들어, DNS 서버가 "다운"되거나 응답하지 않을 수 있으며 또는 도메인이 존재하지 않는 경우가 있습니다. 발신자 그룹에 대한 호스트 DNS 확인 설정을 사용하면 SMTP 대화를 수행하기 전에 확인되지 않은 발신자를 분류하고 다양한 발신자 그룹에 확인되지 않은 발신자의 여러 가지 유형을 포함할 수 있습니다.

어플라이언스는 수신 메일에 대한 DNS를 통해 연결의 전송 도메인을 확인하려고 합니다. 이 확인 작업은 SMTP 대화 이전에 수행됩니다. 시스템은 *이중 DNS 조회*를 수행하여 원격 호스트 IP 주소(즉, 도메인)의 유효성을 확보하고 확인합니다. 이중 DNS 조회는 연결 호스트의 IP 주소에 대한 역방향 DNS(PTR) 조회와 이어지는 PTR 조회의 결과에 대한 Forward DNS(A) 조회로 정의됩니다. 그런 다음 어플라이언스는 A 조회의 결과가 PTR 조회의 결과와 일치하는지 확인합니다. PTR 또는 A 조회에 실패하거나 결과가 일치하지 않는 경우, 시스템은 IP 주소만 사용하여 HAT의 항목을 일치시키고 발신자는 확인되지 않은 것으로 간주합니다.

확인되지 않은 발신자는 다음 범주로 분류됩니다.

- 연결 호스트의 PTR 레코드가 DNS에 존재하지 않습니다.
- 연결 호스트의 PTR 레코드 찾기가 일시적인 DNS 장애로 실패했습니다.
- 연결 호스트의 DNS 역방향 조회(PTR)가 Forward DNS 조회(A)와 일치하지 않습니다.

발신자 그룹의 "Connecting Host DNS Verification(연결 호스트의 DNS 확인)" 설정을 사용하여 확인되지 않은 발신자의 동작을 지정할 수 있습니다(SUSPECTLIST 발신자 그룹을 사용하여 확인되지 않은 발신자의 메시지 제한, 7-31페이지 참조).

발신자 그룹 설정에서 모든 발신자 그룹에 대한 호스트 DNS 확인을 활성화할 수 있지만 호스트 DNS 확인 설정을 발신자 그룹에 추가하는 것은 해당 그룹에서 확인되지 않은 발신자를 *포함*하는 것을 의미합니다. 이는 스팸 및 기타 원치 않는 메일이 포함될 수 있다는 것을 의미합니다. 따라서, 발신자를 거부하거나 제한하는 데 사용되는 발신자 그룹에서만 이 설정을 활성화해야 합니다. 예를 들어 화이트리스트 발신자 그룹에서 호스트 DNS 확인을 활성화하면 확인되지 않은 발신자가 보낸 메일을 화이트리스트에 있는 신뢰할 수 있는 발신자가 보낸 메일과 동일하게 처리하고 수신합니다(메일 흐름 정책의 구성에 따른 안티스팸/안티바이러스 검사, 속도 제한 등의 우회 포함).

발신자 확인: 봉투 발신자

봉투 발신자 확인을 통해 봉투 발신자의 도메인 일부의 DNS가 확인됩니다. (봉투 발신자 도메인을 확인합니까? 봉투 발신자 도메인에 대한 DNS에 A 또는 MX 레코드가 있습니까?) DNS에서 도메인을 조회하려고 할 때 일시적으로 오류 상태(예: 시간 초과 또는 DNS 서버 장애)가 발생하는 경우 도메인이 확인되지 않습니다. 반면, 도메인을 조회하려고 할 때 분명하게 "도메인이 없습니다." 상태를 반환하는 경우 도메인은 존재하지 않습니다. 호스트 DNS 확인이 SMTP 대화를 시작하기 전에 발생하는 것과는 달리 도메인 확인은 SMTP 대화 중에 발생하며 연결 중인 SMTP 서버의 IP 주소에 적용됩니다.

자세하게 설명하면, AsyncOS는 발신자 주소의 도메인에 대해 MX 레코드 쿼리를 수행합니다. 그런 다음 AsyncOS는 MX 레코드 조회의 결과에 따라 A 레코드 조회를 수행합니다. DNS 서버가 "NXDOMAIN"(이 도메인에 대한 레코드 없음)을 반환하면 AsyncOS는 해당 도메인이 존재하지 않는 것으로 처리합니다. 이는 "도메인이 존재하지 않는 봉투 발신자" 범주로 분류됩니다. NXDOMAIN은 루트 이름 서버가 이 도메인에 대해 어떠한 권한 이름 서버도 제공하지 않음을 의미합니다.

그러나 DNS 서버가 "SERVFAIL"을 반환하면 "도메인이 확인되지 않는 봉투 발신자"로 분류됩니다. SERVFAIL은 도메인이 존재하지만 DNS에서 레코드를 조회하는 데 일시적인 문제가 있음을 의미합니다.

메일의 스패머 및 기타 정상적인 발신자와 관련한 일반적인 기술은 MAIL FROM 정보(봉투 발신자 내)를 위조하여 수락된 확인되지 않은 발신자의 메일을 처리하는 것입니다. 이로 인해 MAIL FROM 주소로 전송된 바운스 메시지를 제공할 수 없는 문제가 발생할 수 있습니다. 봉투 발신자 확인을 사용하여, 잘못된 형식의(비어 있지는 않음) MAIL FROM 메일을 거부하도록 어플라이언스를 구성할 수 있습니다.

각 메일 흐름 정책에 다음 작업을 수행할 수 있습니다.

- 봉투 발신자 DNS 확인 활성화.
- 잘못된 형식의 봉투 발신자에 대한 사용자 지정 SMTP 코드 및 응답 제공. 봉투 발신자 DNS 확인을 활성화한 경우 잘못된 형식의 봉투 발신자가 차단됩니다.
- 확인되지 않는 봉투 발신자 도메인에 대해 사용자 지정 응답 제공.
- DNS에 존재하지 않는 봉투 발신자 도메인에 대해 사용자 지정 응답 제공.

발신자 확인 예외 테이블을 사용하여 메일을 자동으로 허용하거나 거부할 도메인 목록 또는 주소를 저장할 수 있습니다(발신자 확인 예외 테이블, 7-30페이지 참조). 발신자 확인 예외 테이블은 봉투 발신자 확인과는 별도로 활성화할 수 있습니다. 따라서 예를 들어, 봉투 발신자 확인을 활성화하지 않은 상태에서 예외 테이블에서 지정한 특정한 주소 또는 도메인을 계속해서 거부할 수 있습니다. 또한 별도로 확인하지 않은 경우에도 내부 또는 테스트 도메인의 메일을 항상 허용할 수 있습니다.

대부분의 스팸은 확인되지 않는 발신자가 보내지만 경우에 따라 확인되지 않는 발신자가 보낸 메일을 수락해야 할 이유가 있습니다. 예를 들어, DNS 조회를 통해 모든 정상적인 이메일을 확인할 수 없습니다. 즉, 임시 DNS 서버 문제로 인해 발신자 확인이 중지될 수 있습니다.

확인되지 않는 발신자가 메일을 보내려고 시도할 경우, 발신자 확인 예외 테이블과 메일 흐름 정책의 봉투 발신자 DNS 확인 설정을 통해 SMTP 대화 중에 봉투 발신자를 분류합니다. 예를 들어, DNS에 없어 확인되지 않는 도메인에서 보낸 메일을 수락하고 제한할 수 있습니다. 일단 해당 메일을 수락하면 잘못된 형식의 MAIL FROM 메시지가 사용자 지정 SMTP 코드 및 응답을 통해 거부됩니다. SMTP 대화 중에 수행됩니다.

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

관련 주제

- 부분 도메인, 기본 도메인 및 잘못된 형식의 MAIL FROM, 7-29페이지
- 사용자 지정 SMTP 코드 및 응답, 7-30페이지
- 발신자 확인 예외 테이블, 7-30페이지

부분 도메인, 기본 도메인 및 잘못된 형식의 MAIL FROM

봉투 발신자 확인을 활성화한 경우 또는 리스너의 SMTP Address Parsing(SMTP 주소 구문 분석) 옵션에서 부분 도메인 허용을 비활성화한 경우("이메일을 수신하도록 게이트웨이 구성" 장의 SMTP 주소 구문 분석 옵션 섹션 참조) 해당 리스너에 대한 기본 도메인 설정을 더 이상 사용할 수 없습니다.

이러한 기능은 함께 사용할 수 없습니다.

사용자 지정 SMTP 코드 및 응답

DNS에 없는 봉투 발신자 및 DNS 쿼리를 통해 확인되지 않는(예: DNS 서버가 다운됨) 봉투 발신자에 대해 잘못된 형식의 봉투 발신자가 포함된 메시지를 위한 SMTP 코드 및 응답 메시지를 지정할 수 있습니다.

SMTP 응답에 변수 `$EnvelopeSender`를 포함할 수 있으며 이 변수는 사용자 지정 응답이 전송될 때 봉투 발신자의 값으로 확장됩니다.

일반적으로 "도메인이 없습니다." 결과는 영구적이지만 일시적인 조건에서도 가능합니다. 이러한 경우를 처리하기 위해 "보수적인" 사용자는 기본값인 5XX에서 4XX 코드로 오류 코드를 변경할 수 있습니다.

발신자 확인 예외 테이블

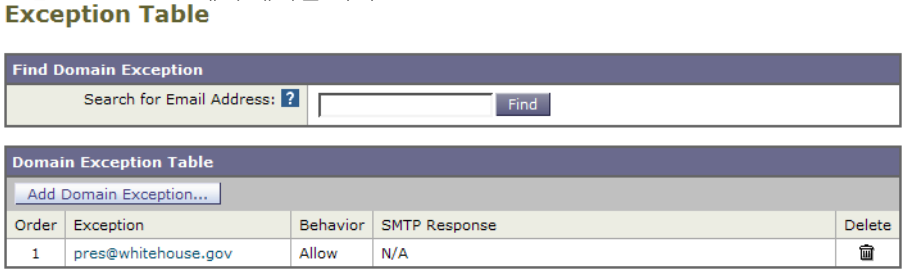
발신자 확인 예외 테이블은 SMTP 대화 도중에 자동으로 허용되거나 거부되는 도메인 또는 이메일 주소 목록입니다. 또한 SMTP 코드 옵션을 지정하고 거부된 도메인에 대한 응답을 거부할 수 있습니다. 어플라이언스당 하나의 발신자 확인 예외 테이블만 사용 가능하며 메일 흐름 정책별로 활성화됩니다.

발신자 확인 예외 테이블은 분명하게 위조되었으나 메일을 거부할 올바른 형식의 도메인 또는 이메일 주소를 나열하는 데 사용될 수도 있습니다. 예를 들어, 올바른 형식의 MAIL FROM: `pres@whitehouse.gov`는 발신자 확인 예외 테이블에 나열되고 자동으로 거부하도록 설정될 수 있습니다. 또한 자동으로 허용할 도메인(예: 내부 및 테스트 도메인)을 나열할 수 있습니다. 이것은 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) 페이지(또는 CLI의 `exceptionconfig` 명령)에 정의되며 GUI(ACCEPTED 메일 흐름 정책을 사용하여 확인되지 않은 발신자에게 전송할 메시지 정의, 7-34페이지 참조) 또는 CLI(*Cisco AsyncOS CLI 참조 설명서* 참조)를 통해 정책별로 활성화됩니다.

발신자 확인 예외 테이블의 항목에는 다음 구문이 포함되어 있습니다.

그림 7-4 예외 테이블 목록



예외 테이블 수정에 대한 자세한 내용은 발신자 이메일 주소에 따라 발신자 확인 규칙에서 확인되지 않은 발신자 제외, 7-35페이지 항목을 참조하십시오.

발신자 확인 구현 — 예 설정

이 섹션에서는 호스트 및 봉투 발신자 확인을 구현하기 위한 일반적인 보수적 방법을 제공합니다.

이 예에서 호스트 발신자 확인을 구현하는 경우 연결 호스트에서 역방향 DNS 조회를 위해 보낸 메일은 기존의 SUSPECTLIST 발신자 그룹 및 THROTTLED 메일 흐름 정책을 통해 제한됩니다.

새로운 발신자 그룹(UNVERIFIED) 및 새로운 메일 흐름 정책(THROTTLEMORE)이 생성됩니다. 확인되지 않은 연결 호스트의 메일은 SMTP 대화를 수행하기 전에 제한됩니다(확인되지 않은 발신자 그룹 및 보다 적극적인 THROTTLEMORE 메일 흐름 정책 사용).

봉투 발신자 확인은 ACCEPTED 메일 흐름 정책에 대해 활성화됩니다.

표 7-9는 발신자 확인을 구현하기 위한 권장 설정을 보여줍니다.

표 7-9 발신자 확인: 권장 설정

발신자 그룹	정책	포함
UNVERIFIED	THROTTLEMORE	SMTP 대화 이전: 연결 호스트의 PTR 레코드가 DNS에 존재하지 않습니다.
SUSPECTLIST	THROTTLED	연결 호스트의 DNS 역방향 조회(PTR)가 Forward DNS 조회(A)와 일치하지 않습니다.
	ACCEPTED	SMTP 대화 중 봉투 발신자 확인: - 잘못된 형식의 MAIL FROM: - 봉투 발신자가 DNS에 없습니다. - 봉투 발신자 DNS를 확인할 수 없습니다.

관련 주제

- SUSPECTLIST 발신자 그룹을 사용하여 확인되지 않은 발신자의 메시지 제한, 7-31페이지
- 확인되지 않은 발신자를 위해 보다 엄격한 제한 설정 구현, 7-33페이지
- ACCEPTED 메일 흐름 정책을 사용하여 확인되지 않은 발신자에게 전송할 메시지 정의, 7-34페이지
- 발신자 이메일 주소에 따라 발신자 확인 규칙에서 확인되지 않은 발신자 제외, 7-35페이지
- 발신자 확인 예외 테이블에서 주소 검색, 7-35페이지

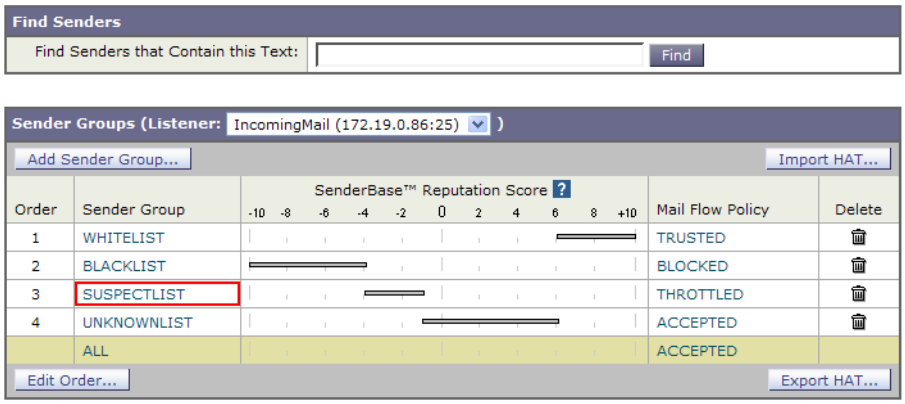
SUSPECTLIST 발신자 그룹을 사용하여 확인되지 않은 발신자의 메시지 제한

절차

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

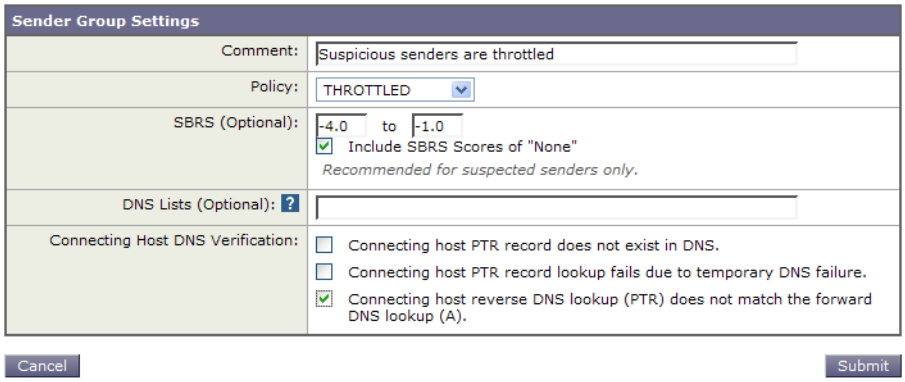
2단계 발신자 그룹 목록에서 **SUSPECTLIST**를 클릭합니다.

그림 7-5 HAT 개요 페이지



3단계 **Edit Settings(설정 편집)**를 클릭합니다.

그림 7-6 발신자 그룹: SUSPECTLIST: 설정 편집



4단계 목록에서 THROTTLED 정책을 선택합니다.

5단계 Connecting Host DNS Verification(연결 호스트의 DNS 확인)에서 "연결 호스트의 역방향 DNS 조회(PTR)가 Forward DNS 조회(A)와 일치하지 않습니다." 확인란을 선택합니다.

6단계 변경사항을 제출하고 커밋합니다.

이제 역방향 DNS 조회에 실패한 발신자는 SUSPECTLIST 발신자 그룹과 일치하게 되며 THROTTLED 메일 흐름 정책에서 기본 동작을 수신하게 됩니다.

참고 또한 CLI를 통해 호스트 DNS 확인을 구성할 수 있습니다. 자세한 내용은 CLI를 통한 호스트 DNS 확인 활성화, 7-38페이지 항목을 참조하십시오.

확인되지 않은 발신자를 위해 보다 엄격한 제한 설정 구현

절차

1단계 새 메일 흐름 정책(이 예에서는 THROTTLEMORE라고 부름)을 만들고 보다 엄격한 제한 설정으로 구성합니다.

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

b. 메일 흐름 정책 이름을 입력하고, 연결 동작에 대해 Accept(수락)를 선택합니다.

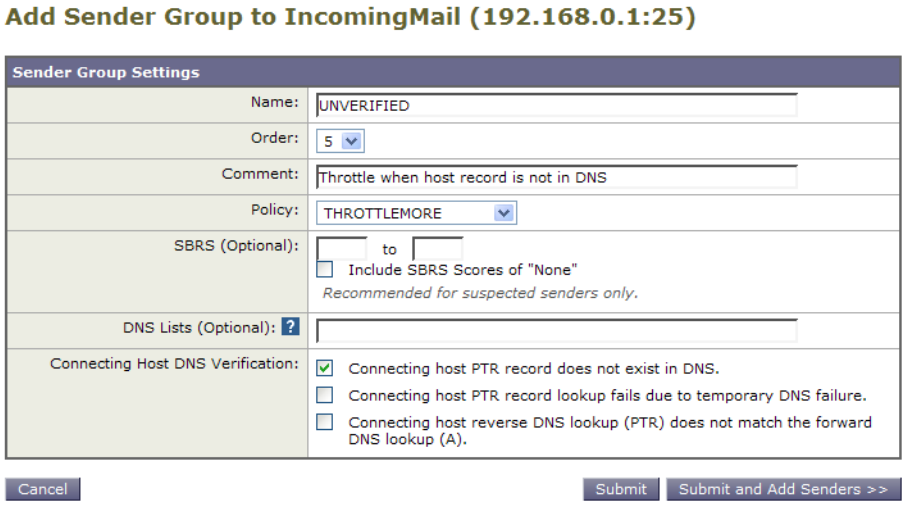
c. 메일을 제한하도록 정책을 구성합니다.

d. 변경사항을 제출하고 커밋합니다.

2단계 새 발신자 그룹(이 예에서는 UNVERIFIED라고 부름)을 만들고 다음과 같이 THROTTLEMORE 정책을 사용하도록 구성합니다.

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

그림 7-7 발신자 그룹 추가: THROTTLEMORE

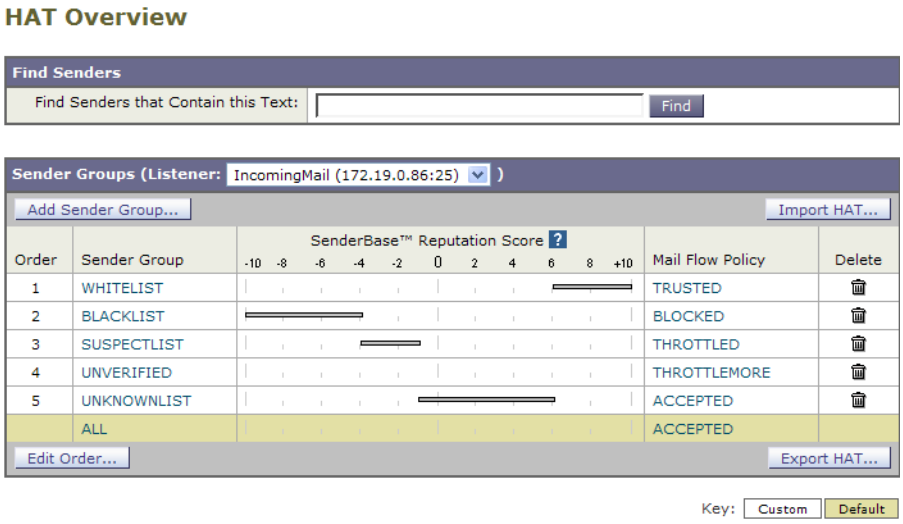


b. 목록에서 THROTTLEMORE 정책을 선택합니다.

c. Connecting Host DNS Verification(연결 호스트의 DNS 확인)에서 "연결 호스트의 PTR 레코드가 DNS에 존재하지 않습니다." 확인란을 선택합니다.

d. 변경사항을 제출하고 커밋합니다.

그림 7-8 HAT 개요



ACCEPTED 메일 흐름 정책을 사용하여 확인되지 않은 발신자에게 전송할 메시지 정의

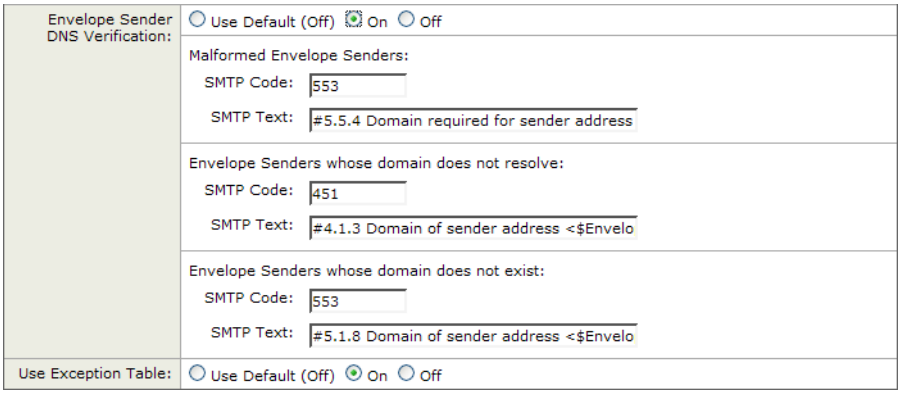
절차

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

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

3단계 메일 흐름 정책의 맨 아래로 스크롤합니다.

그림 7-9 ACCEPTED 메일 흐름 정책의 봉투 발신자 DNS 확인 설정



4단계 **On(켜기)**을 선택하여 이 메일 흐름 정책의 봉투 발신자 DNS 확인을 활성화합니다.

5단계 또한 사용자 지정 SMTP 코드 및 응답을 정의할 수 있습니다.

6단계 "도메인 예외 테이블 사용"에 대해 **On(켜기)**을 선택하여 도메인 예외 테이블을 활성화합니다.

7단계 변경사항을 제출하고 커밋합니다.

발신자 이메일 주소에 따라 발신자 확인 규칙에서 확인되지 않은 발신자 제외

절차

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

참고 예외 테이블은 "예외 테이블 사용"이 활성화된 모든 메일 흐름 정책 전역에 적용됩니다.

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

3단계 이메일 주소를 입력합니다. 특정 주소(pres@whitehouse.gov), 이름(user@), 도메인(@example.com 또는 @.example.com) 또는 대괄호로 묶은 IP 주소(user@[192.168.23.1])가 있는 주소를 입력할 수 있습니다.

4단계 이 주소에서 메시지를 허용 또는 거부할지를 지정합니다. 메일을 거부하는 경우 SMTP 코드 및 사용자 지정 응답도 지정할 수 있습니다.

5단계 변경사항을 제출하고 커밋합니다.

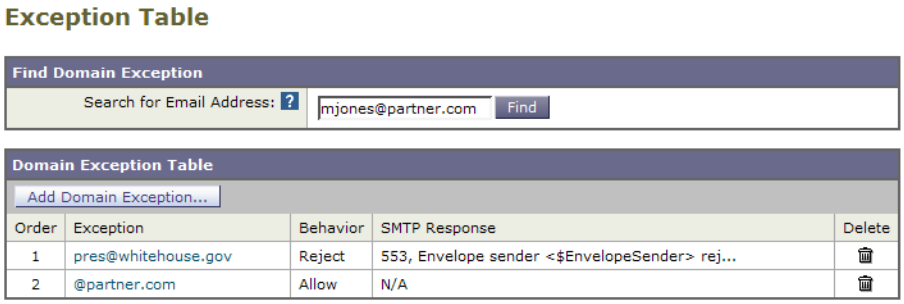
발신자 확인 예외 테이블에서 주소 검색

절차

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

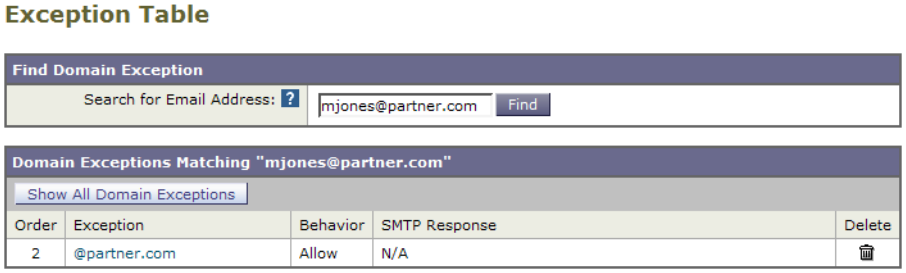
2단계 **Find(찾기)**를 클릭합니다.

그림 7-10 예외 테이블에서 일치하는 항목 검색



주소가 테이블의 항목과 일치하는 경우 첫 번째 일치 항목이 표시됩니다.

그림 7-11 예외 테이블에서 일치하는 항목 나열



확인되지 않은 발신자의 메시지에 대한 설정 테스트

발신자 확인 설정을 구성했으므로 어플라이언스의 동작을 확인할 수 있습니다.

DNS 관련 설정에 대한 테스트는 이 문서의 범위에 포함되지 않습니다.

관련 주제

- 잘못된 형식의 MAIL FROM 발신자 주소를 가진 테스트 메시지 전송, 7-36페이지
- 발신자 확인 규칙에서 제외된 주소에서 메시지 전송하기, 7-37페이지

잘못된 형식의 MAIL FROM 발신자 주소를 가진 테스트 메시지 전송

THROTTLED 정책에 대한 다양한 DNS 관련 설정을 테스트하는 것은 어려울 수 있지만 잘못된 형식의 MAIL FROM 설정은 테스트할 수 있습니다.

절차

1단계 어플라이언스에서 텔넷 세션을 엽니다.

2단계 SMTP 명령을 사용하여 잘못된 형식의 MAIL FROM(도메인 없는 "admin" 등)을 가진 테스트 메시지를 전송합니다.

참고 이메일을 전송하거나 수신할 때 어플라이언스에서 기본 도메인을 사용하거나 부분 도메인을 특별하게 허용하도록 구성한 경우 또는 주소 구문 분석("이메일을 수신하도록 게이트웨이 구성" 장 참조)을 활성화한 경우, 누락되었거나 잘못된 형식의 도메인을 통해 이메일을 만들고 전송하거나 수신할 수 없습니다.

3단계 메시지가 거부되었는지 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 응답이 THROTTLED 메일 흐름 정책의 봉투 발신자 확인 설정을 위해 구성되었습니다.

발신자 확인 규칙에서 제외된 주소에서 메시지 전송하기

발신자 확인 예외 테이블에 나열된 이메일 주소에서 보낸 메일이 봉투 발신자 확인을 거치지 않는다는 것을 확인하려면 다음을 수행합니다.

절차

1단계 다음 주소를 "Allow" 동작이 있는 예외 테이블에 추가합니다. `admin@zzzaaazzz.com`

2단계 변경사항을 커밋합니다.

3단계 어플라이언스에서 텔넷 세션을 엽니다.

4단계 SMTP 명령을 사용하여 발신자 확인 예외 테이블(admin@zzzaaazzz.com)에 입력한 이메일 주소의 테스트 메시지를 전송합니다.

5단계 메시지가 수락되었는지 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 제거하는 경우 봉투 발신자의 도메인 영역의 DNS를 확인할 수 없기 때문에 해당 발신자가 보낸 메일이 거부됩니다.

발신자 확인 및 로깅

다음 로그 항목은 발신자 확인을 판별하는 예를 보여줍니다.

관련 주제

- 봉투 발신자 확인, 7-38페이지

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 없습니다(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 않습니다(SERVFAIL):

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

CLI를 통한 호스트 DNS 확인 활성화

CLI에서 호스트 DNS 확인을 활성화하려면, `listenerconfig > edit > hostaccess` 명령을 사용합니다. 자세한 내용은 *Cisco AsyncOS CLI 참조 설명서* 항목을 참조하십시오.

표 7-10은 확인되지 않은 발신자 유형과 해당하는 CLI 설정을 보여줍니다.

표 7-10 발신자 그룹 설정 및 해당하는 CLI 값

연결 호스트의 DNS 확인	동일한 CLI 설정
연결 호스트의 PTR 레코드가 DNS에 존재하지 않습니다.	`nx.domain`
연결 호스트의 PTR 레코드 찾기가 일시적인 DNS 장애로 실패했습니다.	`serv.fail`
연결 호스트의 DNS 역방향 조회(PTR)가 Forward DNS 조회(A)와 일치하지 않습니다.	`not.double.verified`

8 장

도메인 이름 또는 수신자 주소에 따라 연결 수락 또는 거부

수신자의 주소에 따라 연결 수락 또는 거부 개요

AsyncOS가 각 리스너에 대해 RAT(Recipient Access Table)를 사용하여 수신자 주소에 대한 수락 및 거부 작업을 관리합니다. 수신자 주소는 다음과 같습니다.

- 도메인
- 이메일 주소
- 이메일 주소 그룹

시스템 설정 마법사가 관리자에게 어플라이언스에서 최소한 하나 이상의 공용 리스너(기본값 사용)를 구성하는 과정을 안내합니다. 설정 도중 공용 리스너를 구성하는 과정에는 메일을 수락할 기본 로컬 도메인 또는 특정 주소를 지정하는 작업이 포함됩니다. 이러한 로컬 도메인 또는 특정 주소는 해당 공용 리스너의 RAT의 첫 번째 항목입니다.

각 공용 리스너의 경우 기본 항목인 "다른 모든 수신자"가 모든 수신자의 이메일을 거부합니다. 관리자가 어플라이언스가 메시지를 수락할 모든 로컬 도메인을 정의합니다. 또는 어플라이언스가 메시지를 수락하거나 거부할 특정 사용자도 정의할 수 있습니다. AsyncOS를 통해 RAT(Recipient Access Table)를 사용하여 허용되는 로컬 도메인 및 특정 사용자를 정의할 수 있습니다.

여러 도메인의 메시지를 수락하도록 리스너를 구성해야 합니다. 예를 들어, 조직에서 `currentcompanyname.com`을 사용하고 있고 이전에는 `oldcompanyname.com`을 사용한 경우 `currentcompanyname.com` 및 `oldcompanyname.com`의 메시지를 모두 수락할 수 있습니다. 이 경우 공용 리스너의 RAT에 두 로컬 도메인을 모두 포함합니다.

(참고: 도메인 맵 기능을 사용하여 한 도메인에서 다른 도메인으로 메시지를 매핑할 수 있습니다. "라우팅 및 전송 기능 구성" 장의 도메인 맵 기능 섹션을 참조하십시오.)

RAT(Recipient Access Table) 개요

Recipient Access Table은 공용 리스너에서 수락하는 수신자를 정의합니다. 최소한, 이 테이블은 주소와 주소를 수락할지 또는 거부할지를 지정합니다.

RAT(Recipient Access Table) 페이지에는 순서, 기본 작업, 해당 항목이 LDAP 수락 쿼리를 우회하도록 구성되었는지 여부를 포함해 RAT의 항목 목록이 표시됩니다.

RAT 액세스

GUI

1단계 **Mail Policies(메일 정책) > RAT(Recipient Access Table)**로 이동합니다.

CLI

1단계 `listenerconfig` 명령과 `edit > rcptaccess > new` 하위 명령을 함께 사용합니다.

기본 RAT 항목 편집

시작하기 전에

- 공용 리스너를 설정합니다.
- 인터넷에서 *오픈 릴레이*를 생성하지 않도록 주의해서 편집을 계획합니다. 오픈 릴레이(때로는 "비보안 릴레이" 또는 "타사" 릴레이라고 함)는 타사 이메일 메시지 릴레이를 허용하는 SMTP 이메일 서버입니다. 오픈 릴레이는 로컬 사용자에 대한 메일뿐 아니라 로컬 사용자에게서 전송된 메일도 처리하지 않음으로써 악의적인 사용자가 게이트웨이를 통해 대량의 스팸을 라우팅할 수 없게 만듭니다. 기본적으로 RAT는 오픈 릴레이 생성을 방지하기 위해 모든 수신자를 *거부*합니다.
- RAT에서 기본 항목을 삭제할 수 없습니다.

절차

1단계 Mail Policies(메일 정책) > RAT(Recipient Access Table)로 이동합니다.

2단계 **All Other Recipients(다른 모든 수신자)**를 클릭합니다.

도메인 및 사용자

RAT를 사용하여 메시지를 수락할 도메인 수정

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

- RAT의 항목을 추가, 삭제, 수정합니다.
- 항목의 순서를 변경합니다.
- RAT 항목을 텍스트 파일로 내보냅니다.
- 텍스트 파일에서 RAT 항목을 가져옵니다. 텍스트 파일에서 가져오기는 기존 항목을 덮어씁니다.

관련 주제

- 메시지를 수락할 도메인 및 사용자 추가, 8-3페이지
- Recipient Access Table의 도메인 및 사용자 순서 다시 정렬, 8-5페이지
- Recipient Access Table을 외부 파일로 내보내기, 8-5페이지
- 외부 파일에서 Recipient Access Table 가져오기, 8-6페이지

메시지를 수락할 도메인 및 사용자 추가

절차

1단계 Mail Policies(메일 정책) > RAT(Recipient Access Table) 페이지로 이동합니다.

2단계 리스너 개요 필드에서 편집할 리스너를 선택합니다.

3단계 **Add Recipient(수신자 추가)**를 클릭합니다.

4단계 항목의 순서를 선택합니다.

5단계 수신자 주소를 입력합니다.

6단계 수신자를 수락하거나 거부합니다.

7단계 (선택 사항) 수신자에 대한 LDAP 수락 쿼리를 우회하도록 선택합니다.

8단계 (선택 사항) 이 항목에 대해 사용자 지정 SMTP 응답을 사용합니다.

a. 사용자 지정 SMTP 응답에 대해 예를 선택합니다.

b. SMTP 응답 코드와 텍스트를 입력합니다. 수신자에 대한 RCPT TO 명령에 SMTP 응답을 포함합니다.

9단계 (선택 사항) 수신 제어 우회에 예를 선택하여 제한 우회를 선택합니다.

10단계 변경 사항을 제출하고 커밋합니다.

관련 주제

- 수신자 주소 정의, 8-4페이지
- 특별 수신자에 대해 LDAP 수락 우회, 8-4페이지
- 특별 수신자에 대해 제한 우회, 8-5페이지

수신자 주소 정의

RAT를 사용하여 수신자 또는 수신자 그룹을 정의할 수 있습니다. 전체 이메일 주소, 도메인, 부분 도메인, 사용자 이름 또는 IP 주소로 수신자를 정의할 수 있습니다.

[IPv4 주소]	호스트의 특정 IPv4(인터넷 프로토콜 버전 4) 주소입니다. IP 주소는 "[]" 문자 사이에 있어야 합니다.
[IPv6 주소]	호스트의 특정 IPv6(인터넷 프로토콜 버전 6) 주소입니다. IP 주소는 "[]" 문자 사이에 있어야 합니다.
division.example.com	정규화된 도메인 이름입니다.
.partialhost	"partialhost" 도메인 내의 모든 요소입니다.
user@domain	전체 이메일 주소입니다.
user@	지정된 사용자 이름을 사용하는 주소입니다.
user@[*IP_address*]	특정 IPv4 또는 IPv6 주소의 사용자 이름입니다. IP 주소는 "[]" 문자 사이에 있어야 합니다. "user@*IP_address*"(대괄호 문자가 없음)는 올바른 주소가 아닙니다. 시스템은 메시지를 수신할 때 대괄호를 추가하여 올바른 주소를 생성하며 이는 수신자가 RAT에서 일치하는지에 영향을 미칠 수 있습니다.

참고 GUI에서 시스템 설정 마법사의 4단계에서 Recipient Access Table에 도메인을 추가할 경우(3단계: 네트워크, 3-17페이지 참조) 두 번째 항목을 추가하여 하위 도메인을 지정합니다. 예를 들어, 도메인 example.net을 입력하면 .example.net을 입력할 수도 있습니다. 메일이 example.net의 하위 도메인으로 전송되도록 하는 두 번째 항목이 Recipient Access Table에서 일치됩니다. RAT에서 .example.com *만* 지정하면 .example.com의 모든 하위 도메인의 메일이 수락되지만 하위 도메인(예: joe@example.com)이 *없는* 전체 이메일 주소 수신자의 메일은 수락되지 *않습니다*.

특별 수신자에 대해 LDAP 수락 우회

LDAP 수락 쿼리를 구성하면 특정 수신자에 대해 수락 쿼리를 우회할 수 있습니다. 이 기능은 LDAP 쿼리 도중 지연하고 싶지 않거나 큐에 대기 중인 이메일(customercare@example.com 등)을 수신할 수신자가 있는 경우에 유용할 수 있습니다.

LDAP 수락 쿼리(앨리어싱 또는 도메인 맵 사용 등) 전에 작업 큐에서 재작성할 수신자 주소를 구성할 경우 재작성된 주소가 LDAP 수락 쿼리를 우회하지 않습니다. 예를 들어, 별칭 테이블을 사용하여 customercare@example.com을 bob@example.com 및 sue@example.com에 매핑할 수 있습니다. customercare@example.com에 대해 LDAP 수락을 우회하도록 구성할 경우 앨리어싱이 발생한 후에도 LDAP 수락 쿼리가 여전히 bob@example.com 및 sue@example.com에 대해 실행됩니다.

GUI를 통해 LDAP 수락을 우회하도록 구성할 경우 RAT를 추가하거나 편집할 때 **Bypass LDAP Accept Queries for this Recipient(이 수신자에게 대해 LDAP 수락 쿼리 우회)**를 선택합니다.

CLI를 통해 LDAP 수락 쿼리를 우회하도록 구성할 경우 listenerconfig -> edit -> rcptaccess 명령을 사용하여 수신자를 입력할 때 다음 질문에 예라고 답합니다.

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

LDAP 수락을 우회하도록 RAT 항목을 구성할 경우 RAT 항목의 순서가 수신자 주소가 일치되는 방식에 영향을 미칩니다. RAT는 수신자 주소와 적격한 첫 번째 RAT 항목을 일치시킵니다. 예를 들어, RAT 항목 postmaster@ironport.com 및 ironport.com이 있습니다. LDAP 수락 쿼리를 우회하도록 postmaster@ironport.com의 항목을 구성하고 ACCEPT에 대해 ironport.com의 항목을 구성합니다. postmaster@ironport.com의 메일을 수신하면 postmaster@ironport.com의 항목이 ironport.com의 항목 앞에 있는 경우에만 LDAP 수락 우회가 발생합니다. ironport.com의 항목이 postmaster@ironport.com 항목의 앞에 있는 경우 RAT가 수신자 주소를 이 항목에 일치시키고 ACCEPT 작업을 적용합니다.

특별 수신자에 대해 제한 우회

수신자 항목의 경우 수신자가 리스너에서 활성화된 제한 제어 메커니즘을 우회하도록 지정할 수 있습니다.

이 기능은 메시지를 제한하지 않을 특정 수신자가 있는 경우에 유용합니다. 예를 들어, 메일 흐름 정책에 정의된 수신 제어에 따라 전송 도메인이 제한되는 경우에도 많은 사용자가 리스너에서 "postmaster@domain" 주소의 이메일 수신하려고 합니다. 이 수신자가 리스너의 RAT에서 수신 제어를 우회하도록 지정하면 동일한 도메인의 다른 수신자에 대해 메일 흐름 정책을 유지하는 동시에 리스너에서 수신자 "postmaster@domain"의 메시지를 무제한으로 수신할 수 있습니다. 전송 도메인이 제한될 경우 수신자가 시스템에서 유지하는 시간당 수신자 카운터를 통해 계산되지 않습니다.

GUI를 통해 수신 제어를 우회하도록 특정 수신자를 지정하려면 RAT 항목을 추가하거나 편집할 때 "수신 제어 우회" 설정에 대해 예를 선택합니다.

CLI를 통해 수신 제어를 우회하도록 특정 수신자를 지정하려면 `listenerconfig > edit > rcptaccess` 명령을 사용하여 수신자를 입력할 때 다음 질문에 예라고 답합니다.

```
Would you like to bypass receiving control for this entry?  [N]> y
```

Recipient Access Table의 도메인 및 사용자 순서 다시 정렬

절차

1단계 Mail Policies(메일 정책) > RAT(Recipient Access Table) 페이지로 이동합니다.

2단계 리스너 개요 필드에서 편집할 리스너를 선택합니다.

3단계 **Edit Order(순서 편집)**를 클릭합니다.

4단계 주문 열의 값을 다시 정렬하여 순서를 변경합니다.

5단계 변경 사항을 제출하고 커밋합니다.

Recipient Access Table을 외부 파일로 내보내기

절차

1단계 Mail Policies(메일 정책) > RAT(Recipient Access Table) 페이지로 이동합니다.

2단계 리스너 개요 필드에서 편집할 리스너를 선택합니다.

3단계 **Export RAT(RAT 내보내기)**를 클릭합니다.

4단계 내보낸 항목의 파일 이름을 입력합니다.

이는 어플라이언스의 구성 디렉토리에 생성될 파일의 이름입니다.

5단계 변경 사항을 제출하고 커밋합니다.

외부 파일에서 **Recipient Access Table** 가져오기

텍스트 파일에서 Recipient Access Table을 가져올 경우 기존의 모든 항목이 Recipient Access Table에서 제거됩니다.

절차

1단계 Mail Policies(메일 정책) > RAT(Recipient Access Table) 페이지로 이동합니다.

2단계 리스너 개요 필드에서 편집할 리스너를 선택합니다.

3단계 **Import RAT(RAT 가져오기)**를 클릭합니다.

4단계 목록에서 파일을 선택합니다.

AsyncOS가 어플라이언스의 구성 디렉토리에 모든 텍스트 파일을 나열합니다.

5단계 **Submit(제출)**을 클릭합니다.

기존 Recipient Access Table 항목을 모두 제거할지 묻는 경고 메시지가 표시됩니다.

6단계 **가져오기**를 클릭합니다.

7단계 변경 사항을 커밋합니다.

파일에 "주석"을 넣을 수 있습니다. '#' 문자로 시작하는 행은 주석으로 간주되어 AsyncOS에서 무시됩니다. 예를 들면 다음과 같습니다.

```
# 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 규칙에 따라 메시지 또는 첨부 파일 콘텐츠, 네트워크 정보, 메시지 봉투, 메시지 헤더 또는 메시지 본문를 기준으로 메시지를 식별합니다. 필터 작업을 통해 알림을 생성하거나 메시지를 삭제, 바운스, 아카이브, BCC(숨은 참조) 또는 변경할 수 있습니다. 자세한 내용은 메시지 필터의 구성 요소, 9-2페이지 항목을 참조하십시오.
- **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, 9-4페이지 항목을 참조하십시오.

- **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, 9-9페이지 항목을 참조하십시오.
- **메시지 필터 작업**. 각 필터에는 규칙이 `true`로 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, 9-47페이지 항목을 참조하십시오.
- **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 첨부 파일 검사, 9-75페이지 항목을 참조하십시오.
- **CLI를 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, 9-86페이지 항목을 참조하십시오.
- **메시지 필터 예**. 이 섹션에는 각 필터에 대한 간단한 설명과 함께 필터의 몇 가지 실제 예가 포함되어 있습니다. 자세한 내용은 메시지 필터 예, 9-104페이지 항목을 참조하십시오.

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, 9-2페이지
- 메시지 필터 작업, 9-2페이지
- 메시지 필터 예제 구문, 9-3페이지

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.

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
`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, 9-4페이지 항목을 참조하십시오.
- **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, 9-5페이지 항목을 참조하십시오.
- **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, 9-5페이지 항목을 참조하십시오.
- **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, 9-6페이지 항목을 참조하십시오.
- **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, 9-8페이지 항목을 참조하십시오.

관련 주제

- 메시지 필터 순서, 9-4페이지
- 메시지 헤더 규칙 및 평가, 9-5페이지
- 메시지 본문과 메시지 첨부 파일 비교, 9-5페이지
- 콘텐츠 검사 시 일치를 위한 임계값, 9-6페이지
- 메시지 필터에서 AND 테스트 및 OR 테스트, 9-8페이지

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.

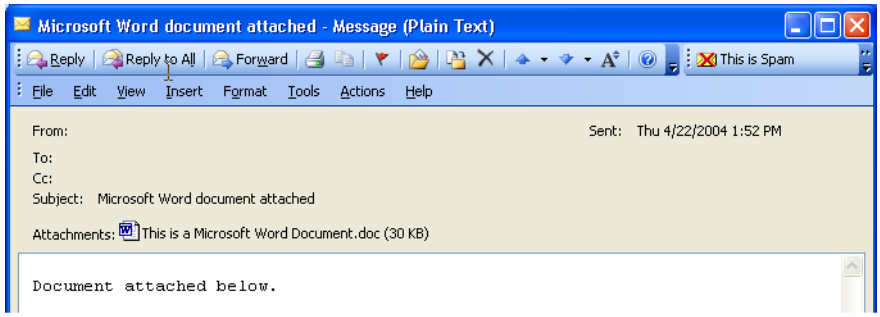
메시지 본문과 메시지 첨부 파일 비교

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 *본문*으로 간주되며 이 본문의 콘텐츠는 본문 내에 포함된 MIME 부분의 첫 번째 텍스트로 간주됩니다. 콘텐츠 다음의 모든 요소(즉, 모든 추가 MIME 부분)는 *첨부 파일*로 간주됩니다. AsyncOS는 메시지의 다양한 MIME 부분을 평가하고 첨부 파일로 처리되는 파일 부분을 식별합니다.

예를 들어, 그림 9-1은 "`Document attached below.`"라는 문장이 일반 텍스트 메시지의 *본문*이고 "`This is a Microsoft Word document.doc`"이라는 문서가 *첨부 파일*인 Microsoft Outlook MUA를 보여줍니다. 많은 사용자들이 이메일을 이러한 방식으로 개념화하므로(첫 번째 부분이 일반 텍스트이고 두 번째 부분이 이진 파일로 구성되는 메시지 대신) Cisco는 RFCS 1521과 1522에서 사용되는 언어에 따라 메시지의 *본문*이 모든 MIME로 구성되는 경우에도 메시지의 "본문"(첫 번째, 일반 텍스트)과 반대로 .doc 파일(기본적으로 두 번째 MIME)을 구분하고 여기에 적용할 규칙을 생성하도록 메시지 필터에서 "첨부 파일"이라는 용어를 사용합니다.

그림 9-1 "첨부 파일"이 포함된 메시지



Cisco 어플라이언스가 여러 부분으로 구성되는 메시지에서 *본문*과 *첨부 파일*을 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 파일*로 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 확인된 일치 항목의 개수에 해당하는 "점수"를 계산합니다. 최소 임계값을 만족하지 못할 경우 정규식은 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, 9-6페이지
- 메시지 본문 및 첨부 파일에 대한 임계값 점수, 9-7페이지
- 여러 부분으로 구성된 MIME/대체 MIME에 대한 임계값 점수, 9-7페이지
- 콘텐츠 사전에 대한 임계값 점수, 9-8페이지

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 있는 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 9-1 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 적게 드는 테스트가 먼저 수행되기 때문에 테스트에서 항목의 순서를 변경해도 영향을 미치지 않습니다. 테스트 수행 순서를 보장하려는 경우 중첩된 `if` 문을 사용합니다. 다음은 가능한 한 비용이 많이 드는 테스트를 피할 수 있는 가장 좋은 방법입니다.

```
expensiveAvoid:

if (<simple tests>)

  { if (<expensive test>)

    { <action> }

  }
```

더 복잡한 예제는 다음과 같습니다.

```
if (test1 AND test2 AND test3) { ... }
```

시스템은 표현식을 왼쪽에서 오른쪽으로 그룹화합니다. 따라서 다음과 같습니다.

```
if ((test1 AND test2) AND test3) { ... }
```

이는 시스템의 첫 번째 작업이 두 번째 AND를 먼저 평가하면서 `(test1 AND test2)` 비용을 `test3` 비용과 비교합니다. 3가지 테스트 모두 비용이 동일한 경우, `test3`가 먼저 수행되는 데 그 이유는 `(test1 AND test2)`가 비용이 2배 비싸기 때문입니다.

메시지 필터 규칙

각 필터에는 필터가 동작하는 대상인 메시지 모음을 정의하는 규칙이 포함됩니다. 필터 규칙을 정의한 다음 `true`를 반환하는 메시지에 대해 필터 작업을 정의합니다.

관련 주제

- 필터 규칙 요약 테이블, 9-10페이지
- 규칙의 정규식, 9-16페이지
- 스마트 식별자, 9-20페이지
- 메시지 필터 작업에 대한 설명 및 예, 9-56페이지

필터 규칙 요약 테이블

표 9-2에는 메시지 필터에서 사용할 수 있는 규칙이 요약되어 있습니다.

표 9-2 메시지 필터 규칙

규칙	구문	설명
제목 헤더	`subject`	제목 헤더가 특정 패턴과 일치합니까? 제목 규칙, 9-23페이지 항목을 참조하십시오.
본문 크기	`body-size`	본문 크기가 일부 범위 안에 있습니까? 본문 크기 규칙, 9-25페이지 항목을 참조하십시오.
봉투 발신자	`mail-from`	봉투 발신자(예: Envelope From, <MAIL FROM>)가 지정된 패턴과 일치합니까? 봉투 발신자 규칙, 9-24페이지 항목을 참조하십시오.
그룹의 봉투 발신자	`mail-from-group`	봉투 발신자(예: Envelope From, <MAIL FROM>)가 지정된 LDAP 그룹에 있습니까? 그룹 규칙의 봉투 발신자, 9-25페이지 항목을 참조하십시오.
발신자 그룹	`sendergroup`	리스너의 HAT(Host Access Table)에서 어떤 발신자 그룹이 일치합니까? 발신자 그룹 규칙, 9-25페이지 항목을 참조하십시오.
봉투 수신자	`rcpt-to`	봉투 수신자(예: Envelope To, <RCPT TO>)가 지정된 패턴과 일치합니까? 봉투 수신자 규칙, 9-23페이지 항목을 참조하십시오. **참고:** `rcpt-to` 규칙은 메시지를 기반으로 합니다. 메시지에 수신자가 여러 명일 경우 모든 수신자에게 메시지를 적용하려면 한 명의 수신자만이 지정된 작업에 대한 해당 규칙과 일치해야 합니다.
봉투 수신자 그룹의	`rcpt-to-group`	봉투 수신자(예: Envelope To, <RCPT TO>)가 지정된 LDAP 그룹에 있습니까? 그룹 규칙의 봉투 수신자, 9-24페이지 항목을 참조하십시오. **참고:** `rcpt-to-group` 규칙은 메시지를 기반으로 합니다. 메시지에 수신자가 여러 명일 경우 모든 수신자에게 메시지를 적용하려면 지정된 작업에 대해 한 명의 수신자만 있어야 합니다.
원격 IP	`remote-ip`	메시지가 지정된 IP 주소 또는 IP 블록과 일치하는 원격 호스트에서 발송되었습니까? 원격 IP 규칙, 9-26페이지 항목을 참조하십시오.
수신 인터페이스	`recv-int`	메시지가 이름이 지정된 수신 인터페이스를 통해 도착했습니까? IP 인터페이스 규칙 수신, 9-27페이지 항목을 참조하십시오.
수신 리스너	`recv-listener`	메시지가 명명된 리스너를 통해 도착했습니까? 리스너 규칙 수신, 9-26페이지 항목을 참조하십시오.
날짜	`date`	현재 시간은 특정 시간 및 날짜 이전 또는 이후입니까? 날짜 규칙, 9-27페이지 항목을 참조하십시오.

표 9-2 메시지 필터 규칙

규칙	구문	설명
헤더	`header(<string>)`	메시지에 특정 헤더가 포함되어 있습니까? 해당 헤더의 값이 특정 패턴과 일치합니까? 헤더 규칙, 9-28페이지 항목을 참조하십시오.
임의	`random(<integer>)`	난수가 일정한 범위 내에 있습니까? 임의 규칙, 9-28페이지 항목을 참조하십시오.
수신자 수	`rcpt-count`	얼마나 많은 수신자에게 이메일이 전송됩니까? 수신자 수 규칙, 9-29페이지 항목을 참조하십시오.
주소 수	`addr-count()`	누적 수신자 수는 몇 명입니까? 이 필터는 봉투 수신자 대신 메시지 본문 헤더에서 동작하는 rcpt-count 필터 규칙과 다릅니다. 주소 수 규칙, 9-29페이지 항목을 참조하십시오.
SPF 상태	`spf-status`	SPF 확인 상태는 어땠습니까? 이 필터 규칙을 통해 다양한 SPF 확인 결과를 쿼리할 수 있습니다. 유효한 SPF/SIDF 반환 값마다 다양한 작업을 입력할 수 있습니다. SPF-Status 규칙, 9-36페이지 항목을 참조하십시오.
통과된 SPF	`spf-passed`	SPF/SIDF 확인을 통과했습니까? 이 필터 규칙은 SPF/SIDF 결과를 부울 값으로 일반화합니다. SPF-Passed 규칙, 9-38페이지 항목을 참조하십시오.
S/MIME 게이트웨이 메시지	`smime-gateway`	S/MIME 메시지가 서명되었습니까, 암호화되었습니까, 아니면 서명되고 암호화되었습니까? S/MIME 게이트웨이 메시지 규칙, 9-38페이지 항목을 참조하십시오.
S/MIME 게이트웨이 확인됨	`smime-gateway-verified`	S/MIME 메시지가 성공적으로 확인되었습니까, 암호가 해독되었습니까, 아니면 암호가 해독되고 확인되었습니까? S/MIME 게이트웨이 확인 규칙, 9-38페이지 항목을 참조하십시오.
이미지 판정	`image-verdict`	이미지 검사 판정 결과는 무엇입니까? 이 필터 규칙을 통해 다양한 이미지 분석 결과를 쿼리할 수 있습니다. 이미지 분석, 9-77페이지 항목을 참조하십시오.
작업 큐 수	`workqueue-count`	작업 큐의 수가 지정된 값과 동일합니까, 이 값보다 더 작습니까, 아니면 더 큽니까? Workqueue-count 규칙, 9-38페이지 항목을 참조하십시오.
본문 검사	`body-contains(<regular expression>)`	메시지에 지정된 패턴과 일치하는 텍스트 또는 첨부 파일이 포함되어 있습니까? 패턴이 임계값으로 지정한 최소 횟수만큼 발생합니까? 엔진은 delivery-status 부분과 관련된 첨부 파일을 검사합니다. 본문 검사 규칙, 9-30페이지 항목을 참조하십시오.

표 9-2 메시지 필터 규칙

규칙	구문	설명
본문 검사	`only-body-contains(<regular expression>)`	메시지 본문에 지정된 패턴과 일치하는 텍스트가 포함되어 있습니까? 패턴이 임계값으로 지정한 최소 횟수만큼 발생합니까? 첨부 파일은 검사되지 않습니다. 본문 검사, 9-30페이지 항목을 참조하십시오.
암호화 탐지	`encrypted`	메시지가 암호화되었습니까? 암호화 탐지 규칙, 9-31페이지 항목을 참조하십시오.
첨부 파일 파일 이름[a]	`attachment-filename`	메시지에 특정 패턴과 일치하는 파일 이름을 가진 첨부 파일이 포함되어 있습니까? 첨부 파일 파일 이름 규칙, 9-32페이지 항목을 참조하십시오.
첨부 파일 유형[a]	`attachment-type`	메시지에 특정 MIME 유형의 첨부 파일이 있습니까? 첨부 파일 유형 규칙, 9-31페이지 항목을 참조하십시오.
첨부 파일[a] **유형**	`attachment-filetype`	메시지에 해당 지문(UNIX `file` 명령과 유사)을 기준으로 하는 특정 패턴과 일치하는 파일 유형의 첨부 파일이 있습니까? 첨부 파일이 Excel 또는 Word 문서인 경우, 다음의 내장 파일 유형을 검색할 수 있습니다. .exe , .dll, .bmp, .tiff, .pcx, .gif, .jpeg, png 및 Photoshop 이미지. 유효한 필터를 생성하려면 파일 유형을 따옴표로 묶어야 합니다. 작은따옴표 또는 큰따옴표를 사용할 수 있습니다. 예를 들어, .exe 첨부 파일을 검색하려면 다음 구문을 사용합니다. `if (attachment-filetype == "exe")` 자세한 내용은 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.
첨부 파일 MIME 유형[a]	`attachment-mimetype`	메시지에 특정 MIME 유형의 첨부 파일이 있습니까? 이 규칙은 MIME 첨부 파일에 지정된 MIME 유형이 평가된다는 것만 제외하고 `attachment-type` 규칙과 유사합니다. (이 어플라이언스는 명시적 유형이 지정되지 않은 경우 파일 유형을 확장명으로 "추측"하지 않습니다.) 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.
보호되는 첨부 파일	`attachment-protected`	메시지에 비밀번호로 보호되는 첨부 파일이 있습니까? 보호된 첨부 파일 격리, 9-86페이지 항목을 참조하십시오.

표 9-2 메시지 필터 규칙

규칙	구문	설명
보호되지 않는 첨부 파일	`attachment-unprotected`	검사 엔진에서 보호되지 않는 첨부 파일을 탐지한 경우 attachment-unprotected 필터 조건은 true를 반환합니다. 검사 엔진에서 첨부 파일을 읽을 수 있는 경우 파일은 보호되지 않는 것으로 간주됩니다. zip 파일 멤버가 보호되지 않는 경우 zip 파일은 보호되지 않는 것으로 간주됩니다. **참고 —** attachment-unprotected 필터 조건은 attachment-protected 필터 조건과 함께 사용할 수 있습니다. 동일한 첨부 파일을 검사하는 경우 두 가지 필터 조건 모두 true를 반환할 수 있습니다. 예를 들어 zip 파일에 보호되는 멤버와 보호되지 않는 멤버가 모두 포함되는 경우 이러한 상황이 발생할 수 있습니다. 보호되지 않는 첨부 파일 탐지, 9-86페이지 항목을 참조하십시오.
첨부 파일 검사 [a]	`attachment-contains(<regular expression>)`	메시지에 특정 패턴과 일치하는 텍스트 또는 다른 첨부 파일을 포함하는 첨부 파일이 있습니까? 패턴이 임계값으로 지정한 최소 횟수만큼 발생합니까? 이 규칙은 `body-contains()` 규칙과 비슷하지만, 메시지의 전체 "본문" 검사를 회피하려고 합니다. 즉, 사용자가 첨부 파일로 보는 부분만 검사하려고 시도합니다. 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.
첨부 파일 검사	`attachment-binary-contains(<regular expression>)`	메시지에 특정 패턴과 일치하는 이진 데이터를 가진 첨부 파일이 포함되어 있습니까? 이 규칙은 `attachment-contains ()` 규칙과 비슷하지만, 특별히 이진 데이터에서 패턴을 검색합니다.
첨부 파일 검사	`every-attachment-contains(<regular expression>)`	이 메시지의 모든 첨부 파일에 특정 패턴과 일치하는 텍스트가 포함되어 있습니까? 모든 첨부 파일에 텍스트가 있어야 하며 수행되는 작업은 각 첨부 파일에 대한 'attachment-contains()'의 논리적 AND 연산입니다. 본문은 검사되지 않습니다. 패턴이 임계값으로 지정한 최소 횟수만큼 발생합니까? 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.
첨부 파일 크기 [a]	`attachment-size`	메시지에 일정 범위에 해당하는 크기의 첨부 파일이 포함되어 있습니까? 이 규칙은 `body-size` 규칙과 비슷하지만, 메시지의 전체 "본문" 검사를 회피하려고 합니다. 즉, 사용자가 첨부 파일로 보는 부분만 검사하려고 시도합니다. 크기는 디코딩하기 전에 평가됩니다. 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.
공용 블랙리스트	`dnslist(<query server>)`	발신자의 IP 주소가 공용 블랙리스트 서버(RBL)에 나타납니까? DNS 목록 규칙, 9-33페이지 항목을 참조하십시오.

표 9-2 메시지 필터 규칙

규칙	구문	설명
SenderBase Reputation	`reputation`	발신자의 SenderBase Reputation 점수란 무엇입니까? SenderBase Reputation 규칙, 9-34페이지 항목을 참조하십시오.
SenderBase Reputation 없음	`no-reputation`	SenderBase Reputation 점수가 "None"인 경우 테스트를 수행하기 위해 사용됩니다. SenderBase Reputation 규칙, 9-34페이지 항목을 참조하십시오.
사전[b]	`dictionary-match(<dictionary_name>)`	메시지 본문이 *dictionary_name*이라는 이름의 콘텐츠 사전의 정규식 또는 용어를 포함하고 있습니까? 패턴이 임계값으로 지정한 최소 횟수만큼 발생합니까? 사전 규칙, 9-34페이지 항목을 참조하십시오.
첨부 파일 사전 일치	`attachment-dictionary-match(<dictionary_name>)`	첨부 파일이 *dictionary_name*이라는 콘텐츠 사전의 정규식을 포함하고 있습니까? 패턴이 임계값으로 지정한 최소 횟수만큼 발생합니까? 사전 규칙, 9-34페이지 항목을 참조하십시오.
제목 사전 일치	`subject-dictionary-match(<dictionary_name>)`	제목 헤더가 *dictionary_name*이라는 콘텐츠 사전의 정규식 또는 용어를 포함하고 있습니까? 사전 규칙, 9-34페이지 항목을 참조하십시오.
헤더 사전 일치	`header-dictionary-match(<dictionary_name>, <header>)`	지정된 헤더(대소문자 구분 안 함)가 *dictionary_name*이라는 콘텐츠 사전의 정규식 또는 용어를 포함하고 있습니까? 사전 규칙, 9-34페이지 항목을 참조하십시오.
본문 사전 일치	`body-dictionary-match(<dictionary_name>)`	이 필터 조건은 사전 용어가 메시지 본문의 콘텐츠와 일치하는 경우에만 true를 반환합니다. 필터는 첨부 파일로 간주되지 않는 MIME에서 용어를 검색하며 사용자 정의 임계값을 만족(기본 임계값은 1임)하는 경우 true를 반환합니다. 사전 규칙, 9-34페이지 항목을 참조하십시오.
봉투 수신자 사전 일치	`rcpt-to-dictionary-match(<dictionary_name>)`	봉투 수신자가 *dictionary_name*이라는 콘텐츠 사전의 정규식 또는 용어를 포함하고 있습니까? 사전 규칙, 9-34페이지 항목을 참조하십시오.
봉투 발신자 사전 일치	`mail-from-dictionary-match(<dictionary_name>)`	봉투 발신자가 *dictionary_name*이라는 콘텐츠 사전의 정규식 또는 용어를 포함하고 있습니까? 사전 규칙, 9-34페이지 항목을 참조하십시오.
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, 9-39페이지 항목을 참조하십시오.
참	`true`	모든 메시지와 일치합니다. True 규칙, 9-22페이지 항목을 참조하십시오.
유효함	`valid`	메시지에 구문 분석이 불가능하고 유효하지 않은 MIME가 포함되어 있는 경우 false를 반환하고 아니면 true를 반환합니다. 유효한 규칙, 9-22페이지 항목을 참조하십시오.

표 9-2 메시지 필터 규칙

규칙	구문	설명
서명	`signed`	메시지가 서명되어 있습니까? 서명된 규칙, 9-41페이지 항목을 참조하십시오.
서명된 인증서	`signed-certificate(<field> [<operator> <regular expression>])`	메시지 서명자 또는 X.509 인증서 발급자가 특정 패턴과 일치합니까? 서명된 인증서 규칙, 9-41페이지 항목을 참조하십시오.
헤더 반복	`header-repeats (<target>, <threshold> [, <direction>])`	지정된 시점에 지정된 수의 메시지가 다음 상태인 경우 `true`를 반환합니다. • 동일한 제목 헤더가 지난 1시간 이내에 탐지되었습니다. • 동일한 봉투 발신자가 지난 1시간 이내에 탐지되었습니다. 헤더 반복 규칙, 9-44페이지 항목을 참조하십시오.
URL 평판	`url-reputation` `url-no-reputation`	메시지에 있는 모든 URL의 평판 점수가 지정된 범위 이내에 있습니까? URL의 평판 점수를 사용할 수 없습니까? URL 평판 규칙, 9-45페이지 항목을 참조하십시오.
URL 범주	`url-category`	메시지에 있는 모든 URL의 범주가 지정된 범주와 일치합니까? URL 범주 규칙, 9-46페이지 항목을 참조하십시오.
손상된 첨부 파일	`attachment-corrupt`	이 메시지에 손상된 첨부 파일이 있습니까? 손상된 첨부 파일 규칙, 9-46페이지 항목을 참조하십시오.

a.첨부 파일 필터링에 대해서는 첨부 파일 검사, 9-75페이지 섹션에 자세히 설명되어 있습니다.
b.콘텐츠 사전은 "텍스트 리소스" 장에 자세히 설명되어 있습니다.

Cisco 어플라이언스에 삽입된 각 메시지는 메시지가 추가로 처리되는 것을 중지하는 최종 작업을 지정하지 않은 한, 모든 메시지 필터를 통해 순서대로 처리됩니다. (메시지 필터 작업, 9-2페이지 참조.) 필터는 모든 메시지에 적용될 수 있으며 규칙은 논리 커넥터(AND, OR, NOT)를 사용하여 결합될 수 있습니다.

규칙의 정규식

규칙을 정의하는 데 사용되는 여러 원자 테스트는 *정규식 일치* 방식을 사용합니다. 정규식이 복잡해질 수 있습니다. 메시지 필터 규칙의 정규식을 적용하기 위해서는 다음 표를 가이드로 사용할 수 있습니다.

표 9-3 규칙의 정규식

정규식(abc)	정규식의 지시문 시퀀스가 문자열의 일부와 일치하는 경우 필터 규칙의 정규식이 문자열과 일치합니다. 예를 들어, 정규식 `Georg`는 `George Of The Jungle`, `Georgy Porgy`, `La Meson Georgette` 및 `Georg`와 일치합니다.
캐럿(^) **달러 기호($)**	달러 기호 문자($)를 포함하는 규칙은 오직 문자열의 끝과 일치하며 캐럿 기호(^)를 포함하는 규칙은 오직 문자열의 시작과 일치합니다. 예를 들어, 정규식 `^Georg$`는 오직 문자열 `Georg`와 일치합니다. 비어 있는 헤더를 검색하면 결과는 다음과 같습니다. `"^$"`
문자, 공백 및 @ 기호 문자	문자, 공백 및 `@` 기호 문자를 포함하는 규칙은 자신의 문자와 정확하게 일치합니다. 예를 들어, 정규식 `^George@admin$`는 오직 문자열 `George@admin`과 일치합니다.
마침표 문자(.)	마침표 문자(.)를 포함하는 규칙은 모든 문자(새 줄 제외)와 일치합니다. 예를 들어 `^...admin$` 정규식은 `macadmin` 문자열 및 `sunadmin` 문자열과 일치하지만 `win32admin`과는 일치하지 않습니다.
별표(*) 지시문	별표(*)를 포함하는 규칙은 "이전 지시문과 0개 이상 일치하는 문자"와 일치합니다. 특히 마침표 및 별표 시퀀스(`.*`)는 문자의 모든 시퀀스(새 줄 포함은 제외)와 일치합니다. 예를 들어 `^P.*Piper$` 정규식은 다음 문자열 모두와 일치합니다. `PPiper`, `Peter Piper`, `P.Piper` 및 `Penelope Penny Piper`.
백슬래시 특수 문자(\)	백슬래시 문자는 특수 문자를 *이스케이프*합니다. 따라서 `\.` 시퀀스는 오직 리터럴 마침표와 일치하고 `\$` 시퀀스는 오직 리터럴 달러 기호와 일치하며 `\^` 시퀀스는 오직 리터럴 캐럿 기호와 일치합니다. 예를 들어, 정규식 `^ik\.ac\.uk$`는 오직 문자열 `ik.ac.uk`와 일치합니다. **참고:** 백슬래시는 구문 분석에 사용되는 특수 이스케이프 문자입니다. 따라서 백슬래시를 정규식에 포함하려면 백슬래시 *두 개*를 사용하여 구문 분석 후 하나의 "실제" 백슬래시만 남아 정규식 시스템에 전달되도록 해야 합니다. 따라서 위의 예제 도메인과 일치시키려면 `^ik\\.ac\\.uk$`를 입력합니다.
대소문자 구분 사용 안 함((?i))	정규식의 나머지를 나타내는 `(?i)` 토큰은 대소문자 구분 사용 안 함 모드로 처리해야 합니다. 대소문자 구분 정규식의 시작 부분에 이 토큰을 두면 완벽하게 대소문자를 구분하지 않는 일치 결과를 반환합니다. 예를 들어, 정규식 `"(?i)viagra"`는 `Viagra`, `vIaGrA` 및 `VIAGRA`와 일치합니다.

표 9-3 규칙의 정규식

반복 횟수{min,max}	이전 토큰의 반복 횟수를 나타내는 정규식 표기법이 지원됩니다. 예를 들어, 표현식 "fo{2,3}"은 foo 및 fooo와 일치하지만 fo 또는 fofo와는 일치하지 않습니다. 명령문 if(header('To') == "^.{500,}")은 500개 이상의 문자를 갖는 "To" 헤더를 검색합니다.
또는(|)	대안 또는 "or" 연산자입니다. A와 B가 정규식인 경우, 표현식 "A|B"는 "A" 또는 "B" 중 하나와 일치하는 모든 문자열과 일치합니다. 예를 들어 "foo|bar"는 foo 또는 bar와 일치하지만 foobar와는 일치하지 않습니다.

관련 주제

- 정규식을 사용하여 메시지 필터링, 9-17페이지
- 정규식 사용을 위한 지침, 9-18페이지
- 정규식 및 비ASCII 문자 집합, 9-18페이지
- n 테스트, 9-18페이지
- 대소문자 구분, 9-18페이지
- 효율적인 필터 작성, 9-19페이지
- PDF 및 정규식, 9-19페이지

정규식을 사용하여 메시지 필터링

필터를 사용하여 비ASCII로 인코딩된 메시지 콘텐츠(헤더 및 본문 모두)의 문자열과 패턴을 검색할 수 있습니다. 특히, 다음에 포함된 비ASCII 문자 집합에 대한 정규식(regex) 검색을 지원합니다.

- 메시지 헤더
- MIME 첨부 파일의 파일 이름 문자열
- 메시지 본문:
  - MIME 헤더(예: 기존 이메일)가 없는 본문
  - 인코딩은 표시하지만 MIME 부분은 표시하지 않는 MIME 헤더가 있는 본문
  - 인코딩이 표시되며 여러 부분으로 구성된 MIME 메시지
  - MIME 헤더에 지정된 인코딩이 없는 상위 항목 모두

일치하는 첨부 파일을 포함하여 메시지 또는 본문의 모든 부분과 일치하도록 정규식(regexes)을 사용할 수 있습니다. 다양한 첨부 파일 유형에는 텍스트, HTML, MS Word, Excel 및 기타 유형이 있습니다. 관련된 문자 집합의 예로는 gb2312, HZ, EUC, JIS, Shift-JIS, Big5 및 유니코드가 있습니다. 정규식을 사용하는 메시지 필터 규칙은 콘텐츠 필터를 통해 생성하거나 텍스트 편집기를 사용하여 파일을 생성하여 시스템으로 가져올 수 있습니다. 자세한 내용은 CLI를 사용하여 메시지 필터 관리, 9-86페이지 및 검사 동작 구성, 9-112페이지 항목을 참조하십시오.

정규식 사용을 위한 지침

접두사를 제외한 문자열과 정확하게 일치하려면 항상 정규식을 캐럿(^)으로 시작하고 달러 기호($)로 마쳐야 합니다.

참고 빈 문자열과 일치할 경우 ""를 실제로 *모든* 문자열과 일치하지 않도록 사용해야 합니다. 대신 "^$"를 사용합니다. 예는 제목 규칙, 9-23페이지의 두 번째 예를 참조하십시오.

리터럴 마침표와 일치하려면 정규식에서 이스케이프된 마침표를 사용해야 합니다. 예를 들어, 정규식 sun.com은 문자열 thegodsunocommando와 일치하지만 정규식 ^sun\.com$은 오직 문자열 sun.com.과 일치합니다.

기술적으로, 사용되는 정규식 유형은 **Python re Module** 유형의 정규식입니다. Python 유형의 정규식에 대한 자세한 내용은 다음에서 확인할 수 있는 Python Regular Expression HOWTO를 참조하십시오. http://www.python.org/doc/howto/

정규식 및 비**ASCII** 문자 집합

일부 언어에는 단어, 단어 경계 또는 대소문자 개념이 존재하지 않습니다.

로케일을 알 수 없거나 인코딩을 확실하게 모르는 경우 단어(regex 구문에서 "\w"로 표시됨)를 구성하는 문자를 구분하는 개념에 따른 복합 정규식으로 인해 문제가 발생할 수 있습니다.

n 테스트

시퀀스 ==를 사용하는 일치와 시퀀스 !=를 사용하는 비일치에 대해 각각 정규식을 테스트할 수 있습니다. 예를 들면 다음과 같습니다.

```
rcpt-to == "^goober@dev\\.null\\....$" (matching)


rcpt-to != "^goober@dev\\.null\\....$" (non-matching)
```

대소문자 구분

별도로 지정하지 않는 한, 정규식은 대소문자를 구분합니다. 따라서 정규식에서 foo를 검색하는 경우, FOO 또는 Foo 패턴과 일치하지 않습니다.

효율적인 필터 작성

이 예는 동일한 작업을 수행하는 필터 2개를 보여줍니다. 그러나 첫 번째 예에서 CPU가 더 많이 사용됩니다. 두 번째 필터에서는 더욱 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 예에서 AsyncOS는 각 첨부 파일 유형 및 recv-listener에 대해 한 번씩, 정규식 엔진을 30번 시작해야 합니다.

대신, 다음과 같이 필터를 작성합니다.

```
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)$") {

    bounce();

  }
```

정규식 엔진은 두 번만 시작하면 되고 필터는 유지 관리하기 쉽기 때문에 "()" 추가나 철자 오류에 대해 걱정할 필요가 없습니다. 위의 예에서와 달리, 이 정규식은 CPU 오버헤드 감소를 보여줍니다.

PDF 및 정규식

PDF가 생성되는 방법에 따라 공백이나 줄 바꿈이 없을 수 있습니다. 이 경우, 검사 엔진은 페이지의 단어 위치에 따라 논리적 공간 및 줄 바꿈 삽입을 시도합니다. 예를 들어, 단어가 여러 글꼴 또는 글꼴 크기로 구성된 경우 PDF 코드는 검사 엔진이 단어 및 줄 바꿈을 확인하기 어려운 방식으로 렌더링됩니다. 이러한 방식으로 구성된 PDF 파일과 달리 정규식을 일치시키려고 시도하는 경우 검사 엔진에서 예기치 않은 결과를 반환할 수 있습니다.

예를 들어, 단어의 문자마다 다른 글꼴과 다른 글꼴 크기를 사용하는 PowerPoint 문서에 단어를 입력하는 경우, 검사 엔진은 이 애플리케이션에서 생성된 PDF를 읽으면서 논리적 공간과 줄 바꿈을 삽입합니다. PDF 구조 때문에 "callout"이 "call out" 또는 "c a l lout"으로 해석될 수 있습니다. 정규식 "callout"을 렌더링 방식 중 하나와 일치하려고 하는 경우 일치하는 결과가 없을 수 있습니다.

스마트 식별자

메시지 콘텐츠를 검사하는 메시지 규칙을 사용할 때 스마트 식별자를 사용하여 데이터의 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

필터의 스마트 식별자를 사용하려면 본문 또는 첨부 파일 콘텐츠를 검사하는 필터 규칙에 다음 키워드를 입력합니다.

표 9-4 메시지 필터의 스마트 식별자

키워드	스마트 식별자	설명
*credit	신용 카드 번호	14자리, 15자리, 16자리 신용 카드 번호를 식별합니다. 참고: 스마트 식별자는 enRoute 또는 JCB 카드를 식별하지 않습니다.
*aba	ABA 은행 식별 번호	ABA 은행 식별 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, 9-20페이지

스마트 식별자 구문

필터 규칙의 스마트 식별자를 사용할 때 본문 또는 첨부 파일을 검사하는 필터 규칙의 따옴표 안에 스마트 식별자 키워드를 아래 예와 같이 입력합니다.

```
ID_Credit_Cards:

if(body-contains("*credit")){

notify("legaldept@example.com");

}
.
```

또한 콘텐츠 필터에서 또는 콘텐츠 사전에 스마트 식별자를 사용할 수 있습니다.

참고 일반 정규식 또는 다른 키워드와 스마트 식별자 키워드를 결합할 수 없습니다. 예를 들어 패턴 `*credit|*ssn`은 유효하지 않습니다.

참고 *SSN 스마트 식별자를 사용하여 긍정 오류를 최소화하려면 다른 필터 기준과 함께 *ssn 스마트 식별자를 사용하는 것이 유용합니다. 사용할 수 있는 필터 예에는 "only-body-contains" 필터 조건이 있습니다. 검색 문자열이 메시지 본문의 모든 MIME 부분에 존재하는 경우 표현식을 true로만 평가합니다. 예를 들어, 다음 필터를 생성할 수 있습니다.

```
SSN-nohtml: if only-body-contains("*ssn") { duplicate-quarantine("Policy");}
```

메시지 필터 규칙에 대한 설명 및 예

다음 섹션에서는 사용 중인 다양한 메시지 필터 규칙과 예에 관해 설명합니다.

관련 주제

True 규칙

true인 규칙은 모든 메시지와 일치합니다. 예를 들어, 다음 규칙은 테스트하는 모든 메시지에 대한 IP 인터페이스를 외부로 변경합니다.

```
externalFilter:

   if (true)

   {

        alt-src-host('external');

   }
```

유효한 규칙

유효한 규칙은 메시지에 구문 분석이 불가능하고 유효하지 않은 MIME가 포함되어 있는 경우 false를 반환하고 아니면 true를 반환합니다. 예를 들어, 다음 규칙은 테스트하는 모든 구문 분석이 불가능 메시지를 삭제합니다.

```
not-valid-mime:

   if not valid

   {

        drop();

   }
```

제목 규칙

subject 규칙은 제목 헤더의 값이 지정된 정규식과 일치하는 메시지를 선택합니다.

예를 들어, 다음 필터는 Make Money... 구문으로 시작하는 제목이 있는 모든 메시지를 버립니다.

```
scamFilter:

   if (subject == '^Make Money')

   {

        drop();

   }
```

헤더 값에서 검색할 비ASCII 문자를 지정할 수 있습니다.

헤더에 작업을 수행할 경우, 헤더의 현재 값에 처리하는 동안 발생한 변경사항이 포함됩니다(예: 메시지 제목을 추가, 제거 또는 수정하는 필터 작업). 자세한 내용은 메시지 헤더 규칙 및 평가, 9-5 페이지 항목을 참조하십시오.

다음 필터는 헤더가 비어 있거나 헤더가 메시지에서 누락된 경우 true를 반환합니다.

```
EmptySubject_To_filter:

if (header('Subject') != ".") OR

   (header('To') != ".") {

   drop();

}
```

참고 이 필터는 비어 있는 제목 및 To 헤더에 대해 true를 반환하지만 누락된 헤더에 대해서도 true를 반환합니다. 메시지에 지정된 헤더가 없는 경우 필터는 역시 true를 반환합니다.

봉투 수신자 규칙

rcpt-to 규칙은 봉투 수신자가 지정된 정규식과 일치하는 메시지를 선택합니다. 예를 들어, 다음 필터는 문자열 "scarface"를 포함하는 이메일 주소로 전송된 모든 메시지를 삭제합니다.

참고 rcpt-to 규칙에 대한 정규식은 대소문자를 *구분하지 않습니다.*

```
scarfaceFilter:

   if (rcpt-to == 'scarface')

   {
```

```
        drop();

    }
```

참고 rcpt-to 규칙은 메시지를 기반으로 합니다. 메시지에 수신자가 여러 명일 경우 모든 수신자에게 메시지를 적용하려면 한 명의 수신자만이 지정된 작업에 대한 해당 규칙과 일치해야 합니다.

그룹 규칙의 봉투 수신자

rcpt-to-group 규칙은 봉투 수신자가 지정된 LDAP 그룹의 멤버인 메시지를 선택합니다. 예를 들어, 다음 필터는 LDAP 그룹 "ExpiredAccounts" 내에서 이메일 주소로 전송된 모든 메시지를 삭제합니다.

```
expiredFilter:

    if (rcpt-to-group == 'ExpiredAccounts')

    {

        drop();

    }
```

참고 rcpt-to-group 규칙은 메시지를 기반으로 합니다. 메시지에 수신자가 여러 명일 경우 모든 수신자에게 메시지를 적용하려면 한 명의 수신자만이 지정된 작업에 대한 해당 규칙과 일치해야 합니다.

봉투 발신자 규칙

mail-from 규칙은 봉투 발신자가 지정된 정규식과 일치하는 메시지를 선택합니다. 예를 들어, 다음 필터는 admin@yourdomain.com 에서 전송된 모든 메시지를 즉시 전달합니다.

참고 mail-from 규칙에 대한 정규식은 대소문자를 *구분하지 않습니다*. 마침표 문자는 다음 예에서 이스케이프됩니다.

```
kremFilter:

    if (mail-from == '^admin@yourdomain\\.com$')

    {

 skip-filters();

    }
```

그룹 규칙의 봉투 발신자

mail-from-group 규칙은 봉투 발신자가 연산자 오른쪽의 LDAP 그룹에 속하는 메시지를 선택합니다(또는 발신자의 이메일 주소가 지정된 LDAP 그룹에 있지 *않은* 경우와 같이 일치하지 않은 경우). 예를 들어, 다음 필터는 LDAP 그룹 "KnownSenders"에 이메일 주소가 포함되어 있는 사용자가 전송한 모든 메시지를 즉시 전달합니다.

```
SenderLDAPGroupFilter:

   if (mail-from-group == 'KnownSenders')

   {

 skip-filters();

   }
```

발신자 그룹 규칙

sendergroup 메시지 필터는 어떤 발신자 그룹이 리스너의 HAT(Host Access Table)의 일치하는지에 따라 메시지를 선택합니다. 이 규칙에서는 '==' (일치하는 경우) 또는 '!='(일치하지 않는 경우)을 사용하여 지정된 정규식과 일치하는지 테스트합니다(표현식의 오른쪽). 예를 들어, 다음 메시지 필터 규칙은 메시지의 발신자 그룹이 정규식 Internal과 일치하는 경우 true로 평가되며 이 경우 메시지를 대체 메일 호스트에 전송합니다.

```
senderGroupFilter:

      if (sendergroup == "Internal")

      {

        alt-mailhost("[172.17.0.1]");

      }
```

본문 크기 규칙

본문 크기는 헤더와 첨부 파일 모두를 포함한 메시지의 크기를 나타냅니다. body-size 규칙은 본문 크기와 지정된 숫자를 지정된 방식으로 비교하는 메시지를 선택합니다. 예를 들어, 다음 필터는 본문 크기가 5MB보다 큰 모든 메시지를 바운스합니다.

```
BigFilter:

   if (body-size > 5M)

   {

        bounce();

   }
```

body-size는 다음 방법으로 식별될 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(10과 동일)
13k	13킬로바이트
5M	5메가바이트
40G	40기가바이트(참고: Cisco 어플라이언스에서는 100MB보다 큰 메시지는 수락하지 않습니다.)

원격 IP 규칙

remote-ip 규칙은 테스트를 통해 해당 메시지를 전송한 호스트의 IP 주소가 특정 패턴과 일치하는지 확인합니다. IP 주소는 인터넷 프로토콜 버전 4(IPv4) 또는 버전 6(IPv6)을 사용할 수 있습니다. IP 주소 패턴은 "발신자 그룹 구문"에 설명되어 있는 **허용된 호스트** 표기법을 사용하여 지정되며 이때 SBO, SBRS, dnslist 표기법과 특수 키워드인 ALL은 제외됩니다.

허용된 호스트 표기법은 IP 주소(호스트 이름 아님)의 숫자 범위 및 시퀀스만 식별할 수 있습니다. 예를 들어, 다음 필터는 IP 주소에서 삽입되지 *않은* 모든 메시지를 바운스합니다. 이때 IP 주소의 양식은 10.1.1.*x*이며, x는 50, 51, 52, 53, 54 또는 55입니다.

```
notMineFilter:

   if (remote-ip != '10.1.1.50-55')

   {

        bounce();

   }
```

리스너 규칙 수신

recv-listener 규칙은 이름이 지정된 리스너에서 수신한 메시지를 선택합니다. 리스너 이름은 시스템에 현재 구성되어 있는 리스너 중 하나의 별칭이어야 합니다. 예를 들어, 다음 필터는 이름이 expedite인 리스너에서 도착하는 모든 메시지를 즉시 전달합니다.

```
expediteFilter:

   if (recv-listener == 'expedite')
```

```
   {
 skip-filters();
   }
```

IP 인터페이스 규칙 수신

recv-int 규칙은 이름이 지정된 인터페이스를 통해 수신한 해당하는 메시지를 선택합니다. 인터페이스 이름은 현재 시스템에 구성되어 있는 인터페이스 중 하나의 별칭이어야 합니다. 예를 들어, 다음 필터는 이름이 outside인 인터페이스에서 도착하는 모든 메시지를 바운스합니다.

```
outsideFilter:
   if (recv-int == 'outside')
   {
        bounce();
   }
```

날짜 규칙

date 규칙은 지정한 시간 및 날짜와 비교하여 현재 시간 및 날짜를 확인합니다. 날짜 규칙은 다음 형식의 타임스탬프를 포함하는 문자열과 비교합니다.
MM/DD/YYYY hh:mm:ss. 이 형식은 미국에서 사용하는 형식으로 특정 시간 이전 또는 이후에 수행할 작업을 지정할 때 유용합니다 (미국 날짜 형식이 아닌 메시지를 검색 중인 경우 문제가 발생할 수 있음). 다음 필터는 2003년 7월 28일 오후 1:00시 이후에 삽입된 campaign1@yourdomain.com의 모든 메시지를 바운스합니다.

```
TimeOutFilter:
   if ((date > '07/28/2003 13:00:00') and (mail-from ==
      'campaign1@yourdomain\\.com'))
   {
        bounce();
   }
```

참고 date 규칙과 $Date 메시지 필터 작업 변수와 혼동하지 않도록 주의해야 합니다.

헤더 규칙

header() 규칙은 특정 헤더에 대한 메시지 헤더를 확인합니다. 이 헤더는 괄호 안에 따옴표를 포함해야 합니다("*헤더 이름*"). 이 규칙은 정규식과 비교되며(subject 규칙과 매우 유사하게) 또는 비교 없이 사용될 수 있습니다. 이 경우, 헤더가 메시지에서 확인되면 "true"이고 확인되지 않으면 "false"입니다. 예를 들어, 다음 예에서는 헤더 X-Sample이 있는지 확인하며 해당 값에 문자열 "sample text"가 포함되는지 확인합니다. 일치하는 항목이 있는 경우 메시지가 바운스됩니다.

```
FooHeaderFilter:

   if (header('X-Sample') == 'sample text')

   {

        bounce();

   }
```

헤더 값에서 검색할 비ASCII 문자를 지정할 수 있습니다.

다음의 예는 비교하지 않는 헤더 규칙을 보여줍니다. 이 경우, 헤더 X-DeleteMe가 확인되면 메시지에서 제거됩니다.

```
DeleteMeHeaderFilter:

   if header('X-DeleteMe')

   {

        strip-header('X-DeleteMe');

   }
```

헤더에 작업을 수행할 경우, 헤더의 현재 값에 처리하는 동안 발생한 변경사항이 포함됩니다(예: 메시지 제목을 추가, 제거 또는 수정하는 필터 작업). 자세한 내용은 메시지 헤더 규칙 및 평가, 9-5 페이지 항목을 참조하십시오.

임의 규칙

random 규칙은 0~N-1의 난수를 생성하며 이때 N은 규칙 다음에 괄호 안에 제공되는 정수 값입니다. header() 규칙과 마찬가지로 비교에 사용되거나 단독으로 "단항" 양식에 사용될 수 있습니다. 규칙은 생성된 난수가 0이 아닌 경우 단항 양식에서 true로 평가합니다. 예를 들어, 다음 필터 모두 실제로 동일하며 가상 게이트웨이 주소 A를 선택하면 절반의 시간을, 가상 게이트웨이 주소 B를 선택하면 나머지 절반의 시간을 사용합니다.

```
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');

   }
```

수신자 수 규칙

rcpt-count 규칙은 메시지의 수신자 수를 정수 값과 비교합니다(body-size 규칙과 유사한 방식으로). 이는 사용자가 한 번에 여러 명의 수신자에게 이메일을 전송하는 것을 방지하거나 해당하는 대량 메일링 캠페인이 특정 가상 게이트웨이 주소를 통해 발송되게 하는 데 유용할 수 있습니다. 다음 예에서는 특정 가상 게이트웨이 주소를 통해 수신자가 100명 이상인 모든 이메일을 전송합니다.

```
large_list_filter:

   if (rcpt-count > 100) {

        alt-src-host('mass_mailing_interface');

   }
```

주소 수 규칙

addr-count() 메시지 필터 규칙은 하나 이상의 헤더 문자열을 가져오며 각 행에서 수신자 수를 세고 수신자의 누적 수를 보고합니다. 이 필터는 봉투 수신자 대신 메시지 본문 헤더에서 동작하는 rcpt-count 필터 규칙과 다릅니다. 다음 예는 필터 규칙을 사용하여 수신자의 긴 목록을 별칭 "undisclosed-recipients"로 대체하는 것을 보여줍니다.

```
count: if (addr-count("To", "Cc") > 30) {

            strip-header("To");

            strip-header("Cc");

            insert-header("To", "undisclosed-recipients");

           }
```

본문 검사 규칙

body-contains() 규칙은 매개변수를 사용하여 정의된 특정 패턴에 대해 수신 이메일과 모든 첨부 파일을 검사합니다. 여기에는 delivery-status 부분과 관련된 첨부 파일이 포함됩니다. body-contains() 규칙은 여러 행과의 일치 여부를 확인하지 않습니다. 검사 논리는 검사해야 하거나 검사해서는 안되는 MIME 유형을 정의하기 위해 Scan Behavior(검사 동작) 페이지 또는 CLI의 scanconfig 명령을 통해 수정할 수 있습니다. 또한 검사 엔진에서 검사를 true로 평가하기 위해 찾아야 할 최소 일치 횟수를 지정할 수 있습니다.

기본적으로 시스템은 특정한 MIME 유형을 포함하는 첨부 파일을 *제외한* 모든 첨부 파일을 검사합니다(video/*, audio/*, image/*). 시스템은 아카이브 첨부 파일을 검사합니다(예: 여러 파일을 포함하는 .zip, .bzip, .compress, .tar 또는 gzip). 검사할 "중첩된" 아카이브 첨부 파일 수를 설정할 수 있습니다(예: .zip에 포함된 .zip).

자세한 내용은 검사 동작 구성, 9-112페이지 항목을 참조하십시오.

본문 검사

AsyncOS는 본문 검사를 수행할 때 본문 텍스트 및 첨부 파일과 정규식을 비교하여 검사합니다. 표현식에 대해 최소 임계값을 할당할 수 있으며 검사 엔진에서 정규식을 최소 횟수만큼 확인한 경우 표현식은 true로 평가합니다.

AsyncOS는 메시지의 다른 MIME 부분을 평가하고 텍스트 형식의 모든 MIME 부분을 검사합니다. AsyncOS는 MIME 유형이 첫 번째 부분에 텍스트가 명시되어 있는 경우 텍스트 부분을 식별합니다. AsyncOS는 메시지에 지정된 인코딩에 따라 인코딩을 결정하고 이 인코딩은 텍스트를 유니코드 문자로 변환합니다. 그런 다음 유니코드 공백에서 정규식을 검색합니다. 메시지에 인코딩이 지정되지 않은 경우, AsyncOS는 Scan Behavior(검사 동작) 페이지 또는 scanconfig 명령을 사용하여 지정한 인코딩을 사용합니다.

메시지 검사 시 AsyncOS가 MIME 부분을 평가하는 방법에 대한 자세한 내용은 메시지 본문과 메시지 첨부 파일 비교, 9-5페이지 항목을 참조하십시오.

MIME 부분이 텍스트가 아닌 경우, AsyncOS는 .zip 또는 .tar 아카이브에서 파일을 추출하거나 압축된 파일의 압축을 풉니다. 데이터를 추출한 후, 검사 엔진은 파일의 인코딩을 식별하고 파일의 데이터를 유니코드로 반환합니다. 그런 다음 AsyncOS는 유니코드 공백에서 정규식을 검색합니다.

다음 예에서는 "회사 기밀" 구문에 대해 본문 텍스트 및 첨부 파일을 검색합니다. 이 예에서는 인스턴스 2개에 최소 임계값을 지정하며 검사 엔진에서 구문 인스턴스 2개 이상을 찾는 경우, 일치하는 모든 메시지를 바운스하고 이러한 시도를 법률 부서에 알립니다.

```
ConfidentialFilter:

   if (body-contains('Company Confidential',2)) {

        notify ('legaldept@example.domain');

        bounce();

   }
```

메시지 본문만 검사하려면 only-body-contains를 사용합니다.

```
disclaimer:

    if (not only-body-contains('[dD]isclaimer',1) ) {

        notify('hresource@example.com');

    }
```

암호화 탐지 규칙

encrypted 규칙은 메시지 콘텐츠에서 암호화된 데이터를 검사합니다. 암호화된 데이터를 디코딩하려고 시도하지는 않지만 단순히 메시지 콘텐츠에 암호화된 데이터가 존재하는지를 검사합니다. 이 검사는 사용자가 암호화된 이메일을 전송하는 것을 방지하는 데 유용합니다.

참고 암호화된 규칙은 메시지 콘텐츠에서 암호화된 데이터만 탐지할 수 있습니다. 암호화된 첨부 파일은 탐지하지 않습니다.

encrypted 규칙은 매개변수를 사용하지 않고 비교되지 않는 true 규칙과 유사합니다. 이 규칙은 암호화된 데이터가 확인되면 true를 반환하고 암호화된 데이터를 확인하지 못하면 false를 반환합니다. 이 기능에는 검사할 메시지가 필요하기 때문에 Scan Behavior(검사 동작) 페이지에서 또는 scanconfig 명령을 통해 정의한 검사 설정을 사용합니다. 이 옵션의 구성에 대한 자세한 내용은 검사 동작 구성, 9-112페이지를 참조하십시오.

다음 필터는 리스너를 통해 전송된 모든 이메일을 검사하며, 메시지에 암호화된 데이터가 포함된 경우 해당 메시지는 법률 부서에 BCC(숨은 참조)된 다음 바운스됩니다.

```
prevent_encrypted_data:

    if (encrypted) {

         bcc ('legaldept@example.domain');

         bounce();

      }
```

첨부 파일 유형 규칙

attachment-type 규칙은 메시지에서 각 첨부 파일이 지정된 패턴과 일치하는지를 확인하기 위해 첨부 파일의 MIME 유형을 검사합니다. 이 패턴은 Scan Behavior(검사 동작) 페이지 또는 scanconfig 명령에서 사용되는 패턴과 동일한 양식이어야 하며(검사 동작 구성, 9-112페이지 설명 참조) 슬래시(/)의 한 쪽을 와일드카드인 별표로 대체할 수 있습니다. 메시지에 지정된 MIME 유형과 일치하는 첨부 파일이 포함된 경우, 이 규칙은 "true"를 반환합니다.

이 기능에는 검사할 메시지가 필요하기 때문에 검사 동작 구성, 9-112페이지에 설명된 모든 옵션을 준수해야 합니다.

메시지의 첨부 파일을 조작할 때 사용할 수 있는 메시지 필터 규칙에 대한 자세한 내용은 첨부 파일 검사, 9-75페이지 항목을 참조하십시오.

다음 필터는 리스너를 통해 전송된 모든 이메일을 검사하며, 메시지에 MIME 유형이 `video/*`인 첨부 파일이 포함된 경우 메시지가 바운스됩니다.

```
bounce_video_clips:

   if (attachment-type == 'video/*') {

        bounce();

   }
```

첨부 파일 파일 이름 규칙

`attachment-filename` 규칙은 메시지에서 각 첨부 파일이 지정된 정규식과 일치하는지를 확인하기 위해 첨부 파일의 파일 이름을 검사합니다. 이 규칙은 대소문자를 구분합니다. 그러나 이 규칙은 공백을 구분하기 때문에 파일 이름의 끝에 인코딩된 공백이 있는 경우 필터는 첨부 파일을 건너뜁니다. 메시지의 첨부 파일 중 하나가 파일 이름과 일치하는 경우, 이 규칙은 "true"를 반환합니다.

다음 정보를 확인합니다.

- 각 첨부 파일의 파일 이름은 MIME 헤더에서 캡처됩니다. MIME 헤더의 파일 이름은 후행 공백을 포함할 수 있습니다.
- 첨부 파일이 아카이브인 경우, Cisco 어플라이언스는 아카이브 내부에서 파일 이름을 수집하고 이에 따라 검사 구성 규칙(검사 동작 구성, 9-112페이지 참조)을 적용합니다.
  - 첨부 파일이 단일 압축 파일인 경우(파일 확장명에도 불구하고), 아카이브 파일로 간주되지 않으며 압축된 파일의 파일 이름은 수집되지 않습니다. 이것은 파일이 `attachment-filename` 규칙을 사용하여 처리되지 않았음을 의미합니다. 이러한 파일 유형의 예로는 `gzip`으로 압축된 실행 파일(.exe)이 있습니다.
  - 단일 압축 파일로 구성된 첨부 파일의 경우(예: foo.exe.gz) 정규식을 사용하여 압축된 파일에서 특정 파일 유형을 검색합니다. 아카이브 파일에 있는 단일 압축 파일 및 첨부 파일 파일 이름, 9-33페이지 항목을 참조하십시오.

메시지의 첨부 파일을 조작할 때 사용할 수 있는 메시지 필터 규칙에 대한 자세한 내용은 첨부 파일 검사, 9-75페이지 항목을 참조하십시오.

다음 필터는 리스너를 통해 전송된 모든 이메일을 검사하며, 메시지에 파일 이름이 `*.mp3`인 첨부 파일이 포함된 경우 메시지가 바운스됩니다.

```
block_mp3s:

   if (attachment-filename == '(?i)\\.mp3$') {

        bounce();

   }
```

관련 주제

- 아카이브 파일에 있는 단일 압축 파일 및 첨부 파일 파일 이름, 9-33페이지

아카이브 파일에 있는 단일 압축 파일 및 첨부 파일 파일 이름

이 예는 gzip으로 생성된 압축 파일 등 아카이브에 있는 단일 압축 파일과 일치하는 방법을 보여줍니다.

```
quarantine_gzipped_exe_or_pif:

if (attachment-filename == '(?i)\\.(exe|pif)($|.gz$)') {

  quarantine("Policy");

}
```

DNS 목록 규칙

dnslist() 규칙은 쿼리를 위해 DNSBL 방법(경우에 따라 "ip4r 조회"라고도 함)을 사용하는 공용 DNS 목록 서버를 쿼리합니다. 수신 연결의 IP 주소가 역방향이 되고(따라서 IP 1.2.3.4는 4.3.2.1이 됨) 괄호로 묶인 서버 이름에 접두사로 추가됩니다(서버 이름이 1로 시작되지 않는 경우 2와 구분하기 위해 마침표가 추가됨). DNS 쿼리가 생성되고 시스템이 DNS 오류 응답(연결의 IP 주소를 서버 목록에서 찾을 수 없음을 표시) 또는 IP 주소(주소를 찾았음을 의미) 중 하나와 함께 반환됩니다. 반환된 IP 주소는 *일반적으로* 127.0.0.*x* 양식이며 이때 x는 0~255의 모든 숫자가 가능합니다(IP 주소 범위는 허용되지 않음). 일부 서버는 목록에 따라 실제로 다른 숫자를 반환하며 다른 서버는 모든 일치 항목과 동일한 결과를 반환합니다.

header() 규칙과 마찬가지로 dnslist()는 단항 또는 이진 비교에서 사용할 수 있습니다. 이 규칙은 응답을 수신한 경우 단순하게 true로 평가하며 응답을 수신하지 못한 경우(예, DNS 서버에 연결할 수 없는 경우) false로 평가합니다.

다음 필터는 발신자가 Cisco Bonded Sender 정보 서비스 프로그램과 연결되어 있는 경우 메시지를 즉시 전송합니다.

```
whitelist_bondedsender:

   if (dnslist('query.bondedsender.org')) {

 skip-filters();

   }
```

선택적으로, 같음(==) 또는 같지 않음(!=) 표현식을 사용하여 결과와 문자열을 비교할 수 있습니다.

다음 필터는 서버에서 "127.0.0.2" 응답을 보내는 메시지를 삭제합니다. 응답이 다른 경우 이 규칙은 "false"를 반환하며 필터는 무시됩니다.

```
blacklist:

   if (dnslist('dnsbl.example.domain') == '127.0.0.2') {

        drop();

   }
```

SenderBase Reputation 규칙

reputation 규칙은 다른 값에 대한 SenderBase Reputation 점수를 확인합니다. 모든 비교 연산자가 허용됩니다(예: >, ==, <=, 등). 메시지에 SenderBase Reputation 점수가 없는 경우(이 점수를 확인하지 않았거나 시스템에서 SenderBase Reputation Service 쿼리 서버로부터 응답을 받지 못했기 때문에), 평판 비교에 실패합니다(이 값은 특정 값보다 크거나 작거나 같거나 같지 않음). 아래에서 설명된 no-reputation 규칙을 사용하여 "None"에 대한 SBRS 점수를 확인할 수 있습니다. 다음의 예는 SenderBase Reputation Service에서 반환된 평판 점수가 임계값 -7.5보다 낮은 경우 메시지의 "Subject:" 행의 앞에 "*** BadRep ***"가 추가되도록 조정합니다.

```
note_bad_reps:

   if (reputation < -7.5) {

        strip-header ('Subject');

        insert-header ('Subject', '*** BadRep $Reputation *** $Subject');

   }
```

자세한 내용은 "발신자 평판 필터링" 장을 참조하십시오. 안티스팸 시스템 우회 작업, 9-70페이지 도 참조하십시오.

SenderBase Reputation 규칙의 값은 -10에서 10까지 가능하지만 NONE 값이 반환될 수도 있습니다. 특히 NONE 값을 확인하려면 no-reputation 규칙을 사용합니다.

```
none_rep:

   if (no-reputation) {

       strip-header ('Subject');

        insert-header ('Subject', '*** Reputation = NONE *** $Subject');

   }
```

사전 규칙

dictionary-match(<*dictonary_name*>) 규칙은 다음의 경우 true로 평가합니다(메시지 본문에 정규식 또는 "*dictonary_name*"이라는 콘텐츠 사전의 용어를 포함하는 경우). 사전이 없는 경우, 규칙은 false로 평가합니다. 사전 정의에 대한 자세한 내용은(대소문자 구분 및 단어 경계 설정 포함) "텍스트 리소스" 장을 참조하십시오.

다음 필터는 Cisco에서 "secret_words"라는 이름의 사전 안에 있는 임의의 단어를 포함하는 메시지를 검사할 때 관리자에게 BCC(숨은 참조)를 보냅니다.

```
copy_codenames:

   if (dictionary-match ('secret_words')) {

       bcc('administrator@example.com');

       }
```

다음의 예는 메시지 본문에 "secret_words"라는 사전에 있는 임의의 단어가 포함된 경우, 정책 격리에 메시지를 전송합니다. only-body-contains 조건과 달리 body-dictionary-match 조건은 모든 콘텐츠가 사전과 개별적으로 일치하지 않아도 됩니다. 각 콘텐츠 부분의 점수는(여러 부분/대체 부분을 고려) 함께 추가됩니다.

```
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');

        }
```

이 예는 "To" 헤더의 이메일 주소와 비교하고 관리자에게 다음과 같이 BCC(숨은 참조)를 보냅니다.

```
headerTest:

    if (header-dictionary-match ('competitorsList', 'to'))

        {

        bcc('administrator@example.com');

        }
```

attachment-dictionary-match(<dictonary_name>) 규칙은 첨부 파일에 있는 일치 항목을 검색하는 점을 제외하고 위의 dictionary-match 규칙과 동일하게 동작합니다.

다음의 필터는 메시지 첨부 파일에 "secret_words"라는 사전에 있는 임의의 단어가 포함된 경우, 정책 격리에 메시지를 전송합니다.

```
quarantine_codenames_attachment:

   if (attachment-dictionary-match ('secret_words'))

       {

       quarantine('Policy');

       }
```

header-dictionary-match(<*dictonary_name*>, <*header*>) 규칙은 <*header*>에 지정된 헤더에서 일치 항목을 검색하는 점을 제외하고 위의 dictionary-match 규칙과 동일하게 동작합니다. 헤더 이름은 대소문자를 구분하지 않습니다. 예를 들어 "subject"와 "Subject" 모두 동일하게 동작합니다.

다음의 필터는 메시지의 "cc" 헤더에 "ex_employees"라는 사전에 있는 임의의 단어가 포함된 경우, 정책 격리에 메시지를 전송합니다.

```
quarantine_codenames_attachment:

   if (header-dictionary-match ('ex_employees', 'cc'))

       {

       quarantine('Policy');

       }
```

사전 용어에 있는 와일드카드를 사용할 수 있습니다. 이메일 주소에서 마침표를 이스케이프할 필요가 없습니다.

SPF-Status 규칙

SPF/SIDF 인증 메일을 받으면 SPF/SIDF 확인 결과에 따라 다른 작업을 수행할 수 있습니다. spf-status 규칙은 다른 SPF 확인 결과를 확인합니다. 자세한 내용은 확인 결과, 20-31페이지 항목을 참조하십시오.

다음 구문을 사용하여 SPF/SIDF 확인 결과를 확인할 수 있습니다.

```
if (spf-status == "Pass")
```

단일 조건으로 여러 상태의 판정을 검사하려면 다음 구문을 사용할 수 있습니다.

```
if (spf-status == "PermError, TempError")
```

다음 구문을 사용하여 HELO, MAIL FROM 및 PRA ID에 대한 확인 결과를 검사할 수도 있습니다.

```
if (spf-status("pra") == "Fail")
```

다음의 예시는 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

다음의 예시는 spf-passed 규칙을 사용하여 spf-passed로 표시되지 않은 이메일을 격리하는 것을 보여줍니다.

```
quarantine-spf-unauthorized-mail:

    if (not spf-passed) {

        quarantine("Policy");

    }
```

참고 spf-status 규칙과는 달리 spf-passed 규칙은 SPF/SIDF 확인 값을 단순한 부울 값으로 축소합니다. None, Neutral, Softfail, TempError, PermError 및 Fail 확인 결과는 spf-passed 규칙에서 통과되지 않은 것으로 처리됩니다. 더 세분화된 결과에 따라 메시지에 대한 작업을 수행하려면 spf-status 규칙을 사용합니다.

S/MIME 게이트웨이 메시지 규칙

S/MIME 게이트웨이 메시지 규칙은 메시지가 S/MIME로 서명되었거나 암호화되었는지 또는 S/MIME로 서명되면서 동시에 암호화되었는지를 확인합니다. 다음 메시지 필터는 메시지가 S/MIME 메시지이며 S/MIME를 사용하여 확인 및 암호 해독에 실패하는 경우 해당 메시지를 격리하는지를 확인합니다.

```
quarantine_smime_messages:
if (smime-gateway-message and not smime-gateway-verified) {
quarantine("Policy");
}
```

자세한 내용은 19 장, "S/MIME 보안 서비스" 항목을 참조하십시오.

S/MIME 게이트웨이 확인 규칙

S/MIME 게이트웨이 메시지 확인 규칙은 메시지가 성공적으로 확인되었거나 암호 해독되었는지 또는 암호 해독되면서 동시에 확인되었는지를 확인합니다. 다음 메시지 필터는 메시지가 S/MIME 메시지이며 S/MIME를 사용하여 확인 및 암호 해독에 실패하는 경우 해당 메시지를 격리하는지를 확인합니다.

```
quarantine_smime_messages:
if (smime-gateway-message and not smime-gateway-verified) {
quarantine("Policy");
}
```

자세한 내용은 19 장, "S/MIME 보안 서비스" 항목을 참조하십시오.

Workqueue-count 규칙

workqueue-count 규칙은 지정된 값에 대한 workqueue-count를 확인합니다. 모든 비교 연산자가 허용됩니다(예: >, ==, <=, 등).

다음 필터는 작업 큐 수를 확인하고 큐가 지정된 수보다 큰 경우 스팸 확인을 건너뜁니다.

```
 wqfull:

if (workqueue-count > 1000) {

 skip-spamcheck();

}
```

SPF/SIDF에 대한 자세한 내용은 SPF 및 SIDF 확인 개요, 20-22페이지 항목을 참조하십시오.

SMTP 인증 사용자 일치 규칙

Cisco 어플라이언스가 SMTP 인증을 사용하여 메시지를 전송하는 경우, `smtp-auth-id-matches (<target> [, <sieve-char>])` 규칙은 발신자의 SMTP 인증 사용자 ID에 대한 메시지 헤더 및 봉투 발신자를 확인하여 스푸핑된 헤더가 있는 발송 메시지를 식별할 수 있습니다. 이 필터를 사용하면 시스템에서 잠재적으로 스푸핑된 메시지를 격리하거나 차단할 수 있습니다.

`smtp-auth-id-matches` 규칙은 다음 대상과 SMTP 인증 ID를 비교합니다.

Target	설명
*EnvelopeFrom	SMTP 대화에서 봉투 발신자(MAIL FROM이라고도 함)의 주소를 비교합니다.
*FromAddress	From 헤더에서 분석한 주소를 비교합니다. 여러 주소가 From: 헤더에서 허용되기 때문에 하나만 일치해야 합니다.
*Sender	발신자 헤더에 지정되어 있는 주소를 비교합니다.
*Any	ID에 관계없이 인증된 SMTP 세션 중에 생성된 메시지와 일치하는지 확인합니다.
*None	인증된 SMTP 세션 중에 생성되지 않은 메시지와 일치하는지 확인합니다. 이것은 인증이 선택사항인 경우(기본 설정)에 유용합니다.

필터는 일치 확인 작업을 대략적으로 수행합니다. 여기서는 대소문자를 구분하지 않습니다. 선택사항인 *sieve-char* 매개변수가 제공된 경우, 지정된 문자 뒤에 오는 주소의 마지막 부분이 비교를 위해 무시됩니다. 예를 들어, + 문자가 매개변수로 포함된 경우, 필터는 + 문자 뒤에 오는 `joe+folder@example.com`에서 주소 부분을 무시합니다. 주소가 `joe+smith+folder@example.com`인 경우, `+folder` 부분만 무시됩니다. SMTP 인증 사용자 ID의 문자열이 간단한 사용자 이름이나 정규화된 이메일 주소가 아닌 경우, 일치하는지 확인하기 위해 대상의 사용자 이름의 일부만 검토됩니다. 도메인은 개별 규칙에서 확인해야 합니다.

또한 $SMTPAuthID 변수를 사용하여 SMTP 인증 사용자 ID를 헤더에 삽입할 수 있습니다.

다음 표는 SMTP 인증 ID와 이메일 주소를 비교하고 `smtp-auth-id-matches` 필터 규칙을 사용하여 일치하는지 확인하는 작업을 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

SMTP 인증 ID	Sieve Char	비교 주소	일치 여부
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 From 헤더의 주소와 봉투 발신자가 SMTP 인증 사용자 ID와 일치하는지 확인하기 위해 인증된 SMTP 세션 동안 생성된 모든 메시지를 확인합니다. 주소와 ID가 일치하면 필터는 도메인을 확인합니다. 주소와 ID가 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");
```

```
    }

}
```

서명된 규칙

signed 규칙은 서명을 위해 메시지를 확인합니다. 이 규칙은 메시지의 서명 여부를 표시하기 위해 부울 값을 반환합니다. 이 규칙은 서명이 ASN.1 DER 인코딩 규칙에 따라 인코딩되었는지와 CMS SignedData 유형 구조(RFC 3852, Section 5.1)를 준수하는지를 평가합니다. 이는 서명이 콘텐츠와 일치하는지 검증하거나 인증서의 유효성을 확인하기 위한 것은 아닙니다.

다음의 예는 signed 규칙을 사용하여 헤더를 서명된 메시지에 삽입하는 것을 보여줍니다.

```
signedcheck: if signed { insert-header("X-Signed", "True"); }
```

다음의 예는 signed 규칙을 사용하여 특정한 발신자 그룹의 서명되지 않은 메시지에서 첨부 파일을 삭제하는 것을 보여줍니다.

```
Signed: if ((sendergroup == "NOTTRUSTED") AND NOT signed) {

 html-convert();

    if (attachment_size > 0)

    {

        drop_attachments("");

    }

}
```

서명된 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.

이 규칙의 구문은 signed-certificate (<field> [<operator> <regular expression>])입니다.

- 이 때, <field>에는 따옴표로 묶인 "발급자" 또는 "서명자" 중 하나가 옵니다.
- <operator>는 == 또는 != 중 하나가 사용되며,
- <regular expression>에는 "발급자" 또는 "서명자"와의 일치 확인에 사용되는 값입니다.

메시지가 여러 서명을 사용하여 서명된 경우, 발급자 또는 서명자 중 하나가 정규식과 일치하는 경우 true를 반환합니다. 이 규칙을 짧은 형식으로 나타낸 signed-certificate("issuer") 및 signed-certificate("signer")는 S/MIME 메시지가 발급자 또는 서명자를 포함하는 경우 true를 반환합니다.

관련 주제

- 서명자, 9-42페이지
- 발급자, 9-42페이지
- 정규식의 이스케이프, 9-42페이지

서명자

메시지 서명자의 경우, 규칙은 `rfc822Name` 이름의 시퀀스를 X.509 인증서의 `subjectAltName` 확장명에서 추출합니다. 서명 인증서에 `subjectAltName` 필드가 없거나 이 필드에 `rfc822Name` 이름이 없는 경우, `signed-certificate("signer")` 규칙은 false로 평가합니다. 드문 경우지만 여러 `rfc822Name` 이름이 있는 경우 규칙은 모든 이름과 정규식이 일치하는지 확인하고 첫 번째 일치 항목을 true로 평가합니다.

발급자

발급자는 X.509 인증서의 비어 있지 않은 고유한 이름입니다. AsyncOS는 인증서에서 발급자를 추출하여 LDAP-UTF8 유니코드 문자열로 변환합니다. 예를 들면 다음과 같습니다.

- C=US,S=CA,O=IronPort
- C=US,CN=Bob Smith

X.509 인증서에 발급자 필드가 필요하기 때문에 `signed-certificate("issuer")`는 S/MIME 메시지에 X.509 인증서가 포함되어 있는지를 평가합니다.

정규식의 이스케이프

LDAP-UTF8은 정규식에 사용할 이스케이프에 대한 메커니즘을 정의합니다. LDAP-UTF8의 이스케이프 문자에 대한 자세한 내용은 LDAP(Lightweight Directory Access Protocol): 고유한 이름의 문자열 표시(`http://www.ietf.org/rfc/rfc4514.txt`)를 참조하십시오.

`signed-certificate` 규칙의 정규식에 대한 이스케이프 규칙은 이스케이프가 필요한 문자로만 이스케이프하도록 제한하는 LDAP-UTF8에 정의된 이스케이프 규칙과 다릅니다. LDAP-UTF8을 사용하면 이스케이프 없이 표시할 수 있는 문자에 대해 선택적인 이스케이프가 가능합니다. 예를 들어, 다음의 2가지 문자열은 LDAP-UTF8 이스케이프 규칙을 사용하는 "Example, Inc."에 대해 올바른 것으로 간주됩니다.

- `Example\, Inc.`
- `Example\,\ Inc\.`

그러나 `signed-certificate` 규칙은 오직 `Example\, Inc.`와 일치합니다. 이 정규식이 LDAP-UTF8에서 허용되더라도 이러한 문자에는 이스케이프가 필요하지 않기 때문에 일치 확인을 위해 공백과 마침표에서 이스케이프하는 것은 허용되지 않습니다. `signed-certificate` 규칙의 정규식을 생성할 때 이스케이프 없이 문자를 표시할 수 있는 경우 문자를 이스케이프하지 않아야 합니다.

$CertificateSigners 작업 변수

작업 변수 `$CertificateSigners`는 서명 인증서의 `subjectAltName` 요소에서 얻은 서명자가 쉼표로 구분된 목록입니다. 단일 서명자의 여러 이메일 주소(중복 항목 제거)가 목록에 포함됩니다.

예를 들어, Alice는 자신의 인증서 2개를 사용하여 메시지에 서명합니다. Bob은 자신의 인증서 1개를 사용하여 메시지에 서명합니다. 모든 인증서는 한 기관에서 발급되었습니다. 메시지가 S/MIME 검사를 통과한 후 추출된 데이터에는 다음의 3가지 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 다음과 같이 확장됩니다.

```
"alice@example.com, al@private.example.com, bob@example.com, bob@private.example.com"
```

예

다음의 예에서는 인증서 발급자가 미국 업체인 경우 새 헤더를 삽입합니다.

```
Issuer: if signed-certificate("issuer") == "(?i)C=US" {
    insert-header("X-Test", "US issuer");
}
```

다음의 예에서는 서명자가 example.com에서 오지 않은 경우 관리자에게 알립니다.

```
NotOurSigners: if signed-certificate("signer") AND
      signed-certificate("signer") != "example\\.com$" {
    notify("admin@example.com");
}
```

다음의 예에서는 메시지에 X.509 인증서가 있는 경우 헤더를 추가합니다.

```
AnyX509: if signed-certificate ("issuer") {
```

```
    insert-header("X-Test", "X.509 present");

}
```

다음의 예에서는 메시지 인증서에 서명자가 없는 경우 헤더를 추가합니다.

```
NoSigner: if not signed-certificate ("signer") {

    insert-header("X-Test", "Old X.509?");

}
```

헤더 반복 규칙

지정된 시점에 지정된 수의 메시지가 다음 상태인 경우 헤더 반복 규칙은 `true`로 평가합니다.

- 동일한 제목이 지난 1시간 이내에 탐지되었습니다.
- 동일한 봉투 발신자가 지난 1시간 이내에 탐지되었습니다.

이 규칙을 사용하여 대용량의 이메일을 탐지할 수 있습니다. 예를 들어, 특정 웹 사이트에서 이루어지는 정치 캠페인에서 대량의 이메일을 조직에 전송할 수 있습니다. 안티스팸 엔진은 이러한 이메일을 안전한 메일로 처리하고 메일 전달을 중지하지 않습니다.

이 규칙의 구문은 `header-repeats (<target>, <threshold> [, <direction>])`이며, 이러한 경우

- `<target>`은 `subject` 또는 `mail-from`입니다. AsyncOS는 반복되는 대상 값을 계산합니다.
- `<threshold>`는 최근 1시간 이내에 수신한 특정 대상으로 향하는 동일한 값을 가지는 메시지 수를 나타내며 이 값을 초과하는 경우 규칙은 true로 평가합니다.
- `<direction>`은 `incoming`, `outgoing` 또는 두 가지 모두 가능합니다. 방향이 규칙에 지정되지 않은 경우, 수신 또는 발송 메시지가 규칙 평가를 위해 계산됩니다.

헤더 반복 규칙이 `true`로 평가할 때마다 시스템 경고가 전송됩니다. 시스템 경고, 33-41페이지 항목을 참조하십시오.

참고 헤더 필드에 쉼표 또는 세미콜론으로 구분된 값이 포함된 경우, 규칙은 추적을 위해 전체 문자열을 검토합니다. 이 규칙은 제목 헤더가 비어 있는 메시지는 무시합니다.

헤더 반복 규칙은 유동적으로 변하는 메시지 수를 1분의 정밀도로 유지합니다. 따라서 설정한 임계값에 도달한 경우, 이 규칙을 시작하기 전에 1분의 지연이 발생할 수 있습니다.

관련 주제

- 기타 규칙과 함께 헤더 반복 규칙 사용, 9-44페이지
- 예, 9-45페이지

기타 규칙과 함께 헤더 반복 규칙 사용

헤더 반복 규칙을 AND 또는 OR 연산이 포함된 다른 규칙과 함께 사용할 수 있습니다. 예를 들어, 다음 필터를 사용하여 메시지 하위 집합의 화이트리스트를 확인할 수 있습니다.

```
F1: if (recv_listener == 'Gray')  AND (header-repeats('subject', X, 'incoming') {
drop();}
```

헤더 반복 규칙을 AND 또는 OR 연산자이 포함된 다른 규칙과 함께 사용하는 경우, 헤더 반복 규칙은 필요한 경우에만 마지막에 평가됩니다. 헤더 반복 규칙이 지정된 메시지에 대해 평가되지 않는 경우, `subject` 또는 `mail-from`은 제공된 임계값과 비교하기 위해 계산되지 않습니다.

헤더 반복 규칙이 마지막에 필요한 경우에만 평가되기 때문에 OR 연산자가 포함된 다른 규칙과 함께 사용할 경우 이 규칙은 다양한 결과를 반환할 수 있습니다. 다음 샘플 필터는 서명된 헤더 반복 규칙의 OR 조건을 사용합니다.

```
f1: if signed OR (header-repeats('subject', 10)) { drop();}
```

이 예에서 이 필터가 처리하는 처음 메시지 9개가 동일한 제목을 지닌 서명된 메시지인 경우, 헤더 반복 규칙은 이러한 메시지를 처리하지 않습니다. 10번째 메시지가 이전 메시지 9개와 동일한 제목 헤더를 가진 서명되지 않은 메시지인 경우, 필터는 임계값에 도달한 경우에도 구성된 작업을 수행하지 않습니다.

예

다음 예에서 지정된 시점에 필터가 마지막 1시간 동안 동일한 제목을 가진 수신 메시지를 `x`개 이상 탐지하는 경우, 동일한 제목을 지닌 후속 메시지가 정책 격리로 전송됩니다.

```
f1 : if header-repeats('subject', X, 'incoming') { quarantine('Policy');}
```

다음 예에서 지정된 시점에 필터가 마지막 1시간 동안 동일한 봉투 발신자를 가진 발송 메시지를 `x`개 이상 탐지하는 경우, 동일한 봉투 발신자의 후속 메시지가 삭제되고 버려집니다.

```
f2 :  if header-repeats('mail-from', X, 'outgoing') {drop();}
```

다음 예에서 지정된 시점에 필터가 마지막 1시간 동안 동일한 제목을 가진 수신 또는 발송 메시지를 `x`개 이상 탐지하는 경우, 동일한 제목을 지닌 모든 후속 메시지에 대해 관리자가 알림을 받습니다.

```
f3: if header-repeats('subject', X) {notify('admin@xyz.com');}
```

URL 평판 규칙

URL 평판 규칙을 사용하여 메시지의 임의의 URL에 대한 평판 점수에 기반하여 메시지 작업을 정의할 수 있습니다. 중요한 정보에 대해서는 URL 평판 또는 URL 범주를 통한 필터링: 조건 및 규칙, 15-8 페이지(15 장, "URL 필터링") 항목을 참조하십시오.

이 규칙에 대한 내용은 다음과 같습니다.

- `msg_filter_name`:은 이 메시지 필터의 이름입니다.
- `whitelist`는 정의된 URL 목록(`urllistconfig` 명령 사용)의 이름입니다. 화이트리스트 지정은 선택 사항입니다.

평판 서비스에서 점수를 제공할 때 수행해야 할 작업은 다음과 같습니다.

`url-reputation` 규칙을 사용합니다.

`url-reputation` 규칙을 사용할 경우 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if url-reputation(<min_score>, <max_score>, '<whitelist>')
{<action>}
```

여기서 각 항목은 다음을 나타냅니다.

- `min_score` 및 `max_score` 는 작업을 적용해야 하는 범위에서의 최소 점수 및 최대 점수입니다. 지정한 값은 범위에 포함됩니다.

  최소 및 최대 점수는 `-10.0~10.0`이어야 합니다.

평판 서비스에서 점수를 제공하지 않을 때 수행해야 할 작업은 다음과 같습니다.

`url-no-reputation` 규칙을 사용합니다.

`url-no-reputation` 규칙을 사용할 경우 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if url_no_reputation('<whitelist>')
{<action>}
```

URL 범주 규칙

URL 범주를 사용하여 메시지의 URL 범주에 기반하여 메시지 작업을 정의할 수 있습니다. 중요한 정보에 대해서는 URL 평판 또는 URL 범주를 통한 필터링: 조건 및 규칙, 15-8페이지(15 장, "URL 필터링") 항목을 참조하십시오.

`url-category` 규칙을 사용할 경우 필터 구문은 다음과 같습니다.

```
<msg_filter_name>: if url-category (['<category-name1>','<category-name2>',…,
'<category-name3>'],'<url_white_list>')
{
<action>
}
```

여기서 각 항목은 다음을 나타냅니다.

- `msg_filter_name`은 메시지 필터의 이름입니다.
- `action`은 모든 메시지 필터 작업입니다.
- `category-name`은 URL 범주입니다. 범주가 여러 개인 경우 쉼표로 구분합니다. 정확한 범주 이름을 가져오기 위해 콘텐츠 필터에서 URL 범주 조건 또는 작업을 확인합니다. 범주에 대한 설명 및 예에 대해서는 URL 범주 정보, 15-13페이지 항목을 참조하십시오.
- `url_white_list`는 정의된 URL 목록(`urllistconfig` 명령 사용)의 이름입니다.

손상된 첨부 파일 규칙

손상된 첨부 파일 규칙은 메시지에 손상된 첨부 파일이 포함된 경우 `true`로 평가합니다. 손상된 첨부 파일이란 검사 엔진이 검사할 수 없거나 손상된 것으로 식별한 첨부 파일을 의미합니다.

관련 주제

- 예, 9-46페이지

예

다음 예에서는 필터가 메시지에서 손상된 첨부 파일을 탐지하는 경우 메시지는 정책 격리에 격리됩니다.

```
quar_corrupt_attach: if (attachment-corrupt) { 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.

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 테이블, 9-47페이지
- 작업 변수, 9-53페이지
- 일치하는 콘텐츠 가시성, 9-55페이지
- 메시지 필터 작업에 대한 설명 및 예, 9-56페이지

필터 작업 요약 테이블

메시지 필터는 표 9-5에 표시된 다음 작업을 이메일 메시지에 적용할 수 있습니다.

표 9-5 메시지 필터 작업

작업	구문	설명
소스 호스트 변경	`alt-src-host`	메시지를 전송하기 위해 소스 호스트 이름 및 IP 인터페이스(가상 게이트웨이 주소)를 변경합니다. 소스 호스트(가상 게이트웨이 주소) 변경 작업, 9-65페이지 항목을 참조하십시오.
수신자 변경	`alt-rcpt-to`	메시지 수신자를 변경합니다. 수신자 변경 작업, 9-64페이지 항목을 참조하십시오.
메일 호스트 변경	`alt-mailhost`	메시지에 대한 대상 메일 호스트를 변경합니다. 전송 호스트 변경 작업, 9-64페이지 항목을 참조하십시오.
알림	`notify`	다른 수신자에게 이 메시지를 보고합니다. 알림 및 복사본 알림 작업, 9-59페이지 항목을 참조하십시오.
복사 알림	`notify-copy`	`notify` 작업과 동일하게 수행되지만 `bcc-scan` 작업을 통해 복사본을 전송합니다. 알림 및 복사본 알림 작업, 9-59페이지 항목을 참조하십시오.
BCC(숨은 참조)	`bcc`	다른 수신자에게 이 메시지(메시지 복제)를 익명으로 복사합니다. BCC(숨은 참조) 작업, 9-61페이지 항목을 참조하십시오.
검사를 통한 BCC(숨은 참조)	`bcc-scan`	다른 수신자에게 이 메시지를 익명으로 복사하고 새 메시지처럼 작업 큐를 통해 처리합니다. BCC(숨은 참조) 작업, 9-61페이지 항목을 참조하십시오.
보관	`archive`	mbox 형식 파일로 이 메시지를 보관합니다. 아카이브 작업, 9-66페이지 항목을 참조하십시오.

표 9-5 메시지 필터 작업

작업	구문	설명
격리	`quarantine (quarantine_name)`	이 메시지에 플래그를 지정하여 *quarantine_name*이라는 격리로 전송합니다. 격리 및 중복 작업, 9-63페이지 항목을 참조하십시오.
중복(격리)	`duplicate-quarantine(quarantine_name)`	메시지 복사본을 지정된 격리에 전송합니다. 격리 및 중복 작업, 9-63페이지 항목을 참조하십시오.
헤더 제거	`strip-header`	전달 전 메시지에서 지정된 헤더를 제거합니다. 헤더 제거 작업, 9-66페이지 항목을 참조하십시오.
헤더 삽입	`insert-header`	전달 전 메시지에 헤더 및 값 쌍을 삽입합니다. 헤더 삽입 작업, 9-67페이지 항목을 참조하십시오.
헤더 텍스트 편집	`edit-header-text`	지정된 헤더 텍스트를 필터 조건에 지정한 텍스트 문자열로 대체합니다. 헤더 텍스트 편집 작업, 9-67페이지 항목을 참조하십시오.
본문 텍스트 편집	`edit-body-text()`	메시지 본문에서 정규식을 제거하고 지정한 텍스트로 대체합니다. 이 필터를 사용하여 특정한 콘텐츠(예: 메시지 본문의 URL)를 제거하고 대체할 수 있습니다. 본문 텍스트 수정 작업, 9-68페이지 항목을 참조하십시오.
HTML 변환	`html-convert()`	메시지 본문에서 HTML 태그를 제거하고 메시지의 일반 텍스트 콘텐츠는 그대로 둡니다. 이 필터를 사용하여 메시지에 있는 모든 HTML 텍스트를 일반 텍스트로 변환할 수 있습니다. HTML 변환 작업, 9-69페이지.
바운스 프로파일 할당	`bounce-profile`	특정한 바운스 프로파일을 메시지에 할당합니다. 바운스 프로파일 작업, 9-69페이지 항목을 참조하십시오.
안티스팸 시스템 우회	`skip-spamcheck`	Cisco 시스템에서 안티스팸 시스템이 이 메시지에 적용되지 *않습니다*. 안티스팸 시스템 우회 작업, 9-70페이지 항목을 참조하십시오.
안티바이러스 시스템 우회	`skip-viruscheck`	Cisco 시스템에서 안티바이러스 시스템이 이 메시지에 적용되지 *않습니다*. 안티바이러스 시스템 우회 작업, 9-70페이지 항목을 참조하십시오.
파일 평판 필터링 및 파일 분석 우회	`skip-ampcheck`	파일 평판 필터링 및 파일 분석이 이 메시지에 적용되지 *않습니다*. 파일 평판 필터링 및 파일 분석 시스템 우회 작업, 9-71페이지 항목을 참조하십시오.
신종 바이러스 필터(Outbreak Filter) 검사 건너뛰기	`skip-vofcheck`	신종 바이러스 필터(Outbreak Filter) 검사가 이 메시지에 적용되지 않습니다. 안티바이러스 시스템 우회 작업, 9-70페이지 항목을 참조하십시오.
이름별로 첨부 파일 삭제	`drop-attachments-by-name`	지정된 정규식과 일치하는 파일 이름을 가진 메시지의 첨부 파일을 모두 삭제합니다. 일치하는 파일이 있는 경우 아카이브 파일 첨부(zip, tar)가 삭제됩니다. 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.
유형별로 첨부 파일 삭제	`drop-attachments-by-type`	지정된 MIME 유형 또는 파일 확장명에 의해 결정된 MIME 유형이 있는 메시지의 모든 첨부 파일을 삭제합니다. 일치하는 파일이 있는 경우 아카이브 파일 첨부(zip, tar)가 삭제됩니다. 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.

표 9-5 메시지 필터 작업

작업	구문	설명
파일 유형별로 첨부 파일 삭제	`drop-attachments-by-filetype`	파일의 지정된 "지문"과 일치하는 메시지의 첨부 파일을 모두 삭제합니다. 일치하는 파일이 있는 경우 아카이브 파일 첨부(zip, tar)가 삭제됩니다. 자세한 내용은 첨부 파일 검사, 9-75페이지 항목을 참조하십시오.
MIME 유형별로 첨부 파일 삭제	`drop-attachments-by-mimetype`	지정된 MIME 유형을 가진 메시지의 첨부 파일을 모두 삭제합니다. 이 작업에서는 파일 확장명에 따라 MIME 유형을 확인하지 않으므로 아카이브 콘텐츠도 검사하지 않습니다. 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.
크기별로 첨부 파일 삭제	`drop-attachments-by-size`	원시 인코딩 형식이며 지정된 크기(바이트)보다 크거나 같은 메시지의 첨부 파일을 모두 삭제합니다. 아카이브 또는 압축 파일의 경우 이 작업은 압축되지 않은 크기를 검사하는 대신 디코딩하기 전 실제 첨부 파일 자체의 크기를 검사합니다. 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.
콘텐츠별로 첨부 파일 삭제	`drop-attachments-where-contains`	정규식이 포함된 메시지의 모든 첨부 파일을 삭제합니다. 패턴이 임계값으로 지정한 최소 횟수만큼 발생합니까? 포함된 파일이 정규식 패턴과 일치하는 경우 아카이브 파일(zip, tar)이 삭제됩니다. 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오. 선택적 주석을 통해 삭제된 첨부 파일을 대체하는 데 사용된 텍스트를 수정할 수 있습니다. 첨부 파일 바닥글은 메시지에 간단하게 추가됩니다.
사전 일치별로 첨부 파일 삭제	`drop-attachments-where-dictionary-match`	사전 용어와 일치하는 항목에 따라 첨부 파일을 제거합니다. 첨부 파일로 간주되는 MIME 부분의 용어가 사전 용어와 일치하는 경우(또한 사용자 정의 임계값을 만족하는 경우) 첨부 파일이 이메일에서 제거됩니다. 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.
바닥글 추가	`add-footer(`*`footer-name`*`)`	고지 사항 텍스트를 바닥글로 메시지에 추가합니다. 자세한 내용은 "텍스트 리소스" 장의 "메시지 고지 사항 스탬프"를 참조하십시오.
머리글 추가	`add-heading(`*`heading-name`*`)`	고지 사항 텍스트를 머리글로 메시지에 추가합니다. 자세한 내용은 "텍스트 리소스" 장의 "메시지 고지 사항 스탬프"를 참조하십시오.
전달 시 암호화	`encrypt-deferred`	전달 시 메시지를 암호화합니다. 이는 메시지가 계속 다음 단계로 이동되며 모든 절차가 완료되면 메시지가 암호화되어 전달됨을 의미합니다.
전달 시 S/MIME 서명/암호화	`smime-gateway-deferred ("sending_profile")`	전달 중에 지정된 전송 프로파일을 사용하여 메시지에 대한 S/MIME 서명 또는 암호화를 수행합니다. 전달 시 S/MIME 서명 또는 암호화 작업, 9-58페이지 항목을 참조하십시오.

표 9-5 메시지 필터 작업

작업	구문	설명
S/MIME 서명/암호화	`smime-gateway("sending_profile")`	지정된 전송 프로파일을 사용하여 S/MIME 서명 또는 암호화를 수행하고 메시지를 전달하여 이후 처리 작업을 건너뜁니다. S/MIME 서명 또는 암호화 작업, 9-58페이지 항목을 참조하십시오.
메시지 태그 추가	`tag-message(tag-name)`	RSA 이메일 DLP 정책 필터링에 사용할 메시지에 사용자 지정 용어를 추가합니다. 메시지 태그를 포함하는 메시지로 검사를 제한하도록 RSA 이메일 DLP 정책을 구성할 수 있습니다. 수신자에게는 메시지 태그가 보이지 않습니다. 메시지 태그 추가 작업, 9-71페이지 및 "데이터 유출 방지" 장을 참조하십시오.
로그 항목 추가	`log-entry`	`INFO` 수준의 텍스트 메일 로그에 사용자 지정 텍스트를 삽입합니다. 텍스트는 작업 변수를 포함할 수 있습니다. 로그 항목은 메시지 추적 시 표시됩니다. 로그 항목 추가 작업, 9-72페이지 항목을 참조하십시오.
URL 평판을 기준으로 URL을 텍스트로 대체	• url-reputation-replace • url-no-reputation-replace	URL 평판을 기준으로 URL 또는 동작을 수정합니다. 개별 작업을 사용하여 평판 서비스가 URL에 점수를 제공하지 않는 문제를 해결할 수 있습니다. URL 평판 작업, 9-72페이지 항목을 참조하십시오.
URL 평판을 기준으로 URL 무해화	• url-reputation-defang • url-no-reputation-defang	
URL 평판을 기준으로 Cisco 보안 프록시에 URL 리디렉션	• url-reputation-proxy-redirect • url-no-reputation-proxy-redirect	
URL 범주를 기준으로 URL을 텍스트로 대체	`url-category-replace`	URL 범주를 기준으로 URL 또는 동작을 수정합니다. URL 범주 작업, 9-74페이지 항목을 참조하십시오.
URL 범주를 기준으로 URL 무해화	`url-category-defang`	
URL 범주를 기준으로 Cisco 보안 프록시에 URL 리디렉션	`url-category-proxy-redirect`	
작업 없음	`no-op`	작업이 수행되지 않습니다. 작업 없음, 9-75페이지 항목을 참조하십시오.
***나머지 메시지 필터 건너뛰기**	`skip-filters`	이 메시지가 다른 메시지 필터에서 처리되지 않고 이메일 파이프라인을 통해 계속 처리됩니다. 나머지 메시지 필터 작업 건너뛰기, 9-57페이지 항목을 참조하십시오.
***메시지 삭제**	`drop`	메시지를 삭제하고 버립니다. 삭제 작업, 9-57페이지 항목을 참조하십시오.
***메시지 바운스**	`bounce`	발신자에게 다시 메시지를 전송합니다. 바운스 작업, 9-58페이지 항목을 참조하십시오.

표 9-5 메시지 필터 작업

작업	구문	설명
***지금 암호화 및 전송**	`encrypt`	Cisco 이메일 암호화를 사용하여 발송 메시지를 암호화합니다. 암호화 작업, 9-58페이지 항목을 참조하십시오.

****최종 작업***

관련 주제

- 첨부 파일 그룹, 9-51페이지

첨부 파일 그룹

`attachment-filetype` 및 `drop-attachments-by-filetype rules`에서 특정 파일 유형(예: "exe" 파일) 또는 첨부 파일의 일반적인 그룹을 지정할 수 있습니다. AsyncOS는 첨부 파일을 표 9-6에 나열된 그룹으로 나눕니다.

특정 파일 유형의 첨부 파일을 포함하지 않는 메시지와 일치하도록 `!=` 연산자를 사용하는 메시지 필터를 생성하는 경우, 이 필터는 필터링할 파일 유형의 첨부 파일이 1개 이상 있는 경우 메시지에 어떠한 작업도 수행하지 않습니다. 예를 들어, 다음 필터는 *.exe* 파일이 아닌 첨부 파일의 모든 메시지를 삭제합니다.

```
exe_check: if (attachment-filetype != "exe") {

                    drop();

                }
```

메시지에 첨부 파일이 여러 개 있는 경우, Email Security 어플라이언스는 다른 첨부 파일이 `.exe` 파일이 아니어도 첨부 파일 하나 이상이 `.exe` 파일인 경우 메시지를 삭제하지 않습니다.

표 9-6 첨부 파일 그룹

첨부 파일 그룹 이름	검사된 파일 유형
문서	• doc • docx • mdb • mpp • ole • pdf • ppt • pptx • rtf • wps • x-wmf • xls • xlsx
실행 파일	• exe • java • msi • pif **참고** 실행 파일 그룹을 필터링할 때 .dll 및 .scr 파일을 검사하지만 이러한 파일 유형은 개별적으로 필터링할 수 없습니다.
압축됨	• ace(ACE 아카이버 압축 파일) • arc(SQUASH 압축 아카이브) • arj(Robert Jung ARJ 압축 아카이브) • binhex • bz(Bzip 압축 파일) • bz2(Bzip 압축 파일) • cab(Microsoft 캐비닛 파일) • gzip*(압축 파일 - UNIX gzip) • lha(압축 아카이브 [LHA/LHARC/LHZ]) • rar(압축 아카이브) • sit(압축 아카이브 - Macintosh 파일 [Stuffit]) • tar*(압축 아카이브) • unix(UNIX 압축 파일) • zip*(압축 아카이브 - Windows) • zoo(ZOO 압축 아카이브 파일) * 이러한 파일 유형은 "body-scanned"가 가능합니다.
텍스트	• txt • html • xml

표 9-6 첨부 파일 그룹 (계속)

첨부 파일 그룹 이름	검사된 파일 유형
이미지	• bmp • cur • gif • ico • jpeg • pcx • png • psd • psp • tga • tiff
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 작업이 실행될 때 원본 메시지의 정보로 자동으로 대체되는 특정한 변수를 사용할 수 있는 매개변수가 있습니다. 이 특수 변수를 *작업 변수*라고 합니다. Cisco 어플라이언스는 다음과 같은 작업 변수 집합을 지원합니다.

표 9-7 메시지 필터 작업 변수

변수	구문	설명
모든 헤더	$AllHeaders	메시지 헤더를 반환합니다.
본문 크기	$BodySize	메시지의 크기(바이트)를 반환합니다.
인증서 서명자	$CertificateSigners	서명 인증서의 subjectAltName 요소에서 서명자를 반환합니다. 자세한 내용은 $CertificateSigners 작업 변수, 9-42페이지 항목을 참조하십시오.

표 9-7 메시지 필터 작업 변수 (계속)

변수	구문	설명
날짜	`$Date`	MM/DD/YYYY 형식을 사용하여 현재 날짜를 반환합니다.
삭제된 파일 이름	`$dropped_filename`	최근에 삭제된 파일 이름만 반환합니다.
삭제된 파일 이름	`$dropped_filenames`	삭제된 파일 목록을 표시합니다 (`$filenames`와 유사).
삭제된 파일 형식	`$dropped_filetypes`	삭제된 파일 유형의 목록을 표시합니다 (`$filetypes`와 유사).
봉투 발신자	`$EnvelopeFrom`	메시지의 봉투 발신자(Envelope From, <MAIL FROM>)를 반환합니다.
봉투 수신자	`$EnvelopeRecipients`	메시지의 모든 봉투 수신자(Envelope To, <RCPT TO>)를 반환합니다.
파일 이름	`$filenames`	메시지 첨부 파일의 파일 이름의 쉼표로 구분된 목록을 반환합니다.
파일 크기	`$filesizes`	메시지 첨부 파일의 파일 크기의 쉼표로 구분된 목록을 반환합니다.
파일 형식	`$filetypes`	메시지 첨부 파일의 파일 유형의 쉼표로 구분된 목록을 반환합니다.
필터 이름	`$FilterName`	처리 중인 필터 이름을 반환합니다.
GMTimeStamp	`$GMTimeStamp`	GMT를 사용하여 이메일 메시지의 Received: 줄에서 발견되는 현재 시간 및 날짜를 반환합니다.
HAT 그룹 이름	`$Group`	메시지를 삽입할 때 일치하는 발신자가 속한 발신자 그룹의 이름을 반환합니다. 발신자 그룹에 이름이 없는 경우 `">Unknown<"` 문자열이 삽입됩니다.
일치하는 콘텐츠	`$MatchedContent`	검사 필터 규칙(`body-contains` 및 콘텐츠 사전 등의 필터 규칙 포함)을 트리거한 콘텐츠를 반환합니다.
메일 흐름 정책	`$Policy`	메시지를 삽입할 때 발신자에 적용되는 HAT 정책의 이름을 반환합니다. 사전 정의된 정책 이름이 사용된 경우 `">Unknown<"` 문자열이 삽입됩니다.
헤더	`$Header['string']`	원본 메시지에 일치하는 헤더가 있는 경우 작은따옴표가 붙은 헤더 값으로 반환합니다. 큰따옴표도 사용될 수 있습니다.
호스트 이름	`$Hostname`	Cisco 어플라이언스의 호스트 이름을 반환합니다.
내부 메시지 ID	`$MID`	내부에서 메시지를 식별하는 데 사용되는 메시지 ID 또는 "MID"를 반환합니다. RFC822 "Message-Id" 값과 혼동하지 않도록 주의합니다($Header를 사용하여 해당 항목 검색).

표 9-7 메시지 필터 작업 변수 (계속)

변수	구문	설명
수신 리스너	`$RecvListener`	메시지를 수신한 리스너의 별칭으로 대체됩니다.
수신 인터페이스	`$RecvInt`	메시지를 수신한 인터페이스의 별칭을 반환합니다.
원격 IP 주소	`$RemoteIP`	메시지를 Cisco 어플라이언로 전송한 시스템의 IP 주소를 반환합니다.
원격 호스트 주소	`$remotehost`	메시지를 Cisco 어플라이언스로 전송한 시스템의 호스트 이름을 반환합니다.
SenderBase Reputation 점수	`$Reputation`	발신자의 SenderBase Reputation 점수를 반환합니다. 평판 점수가 없는 경우 "None"으로 대체됩니다.
제목	`$Subject`	메시지 제목을 반환합니다.
시간	`$Time`	로컬 시간대의 현재 시간을 반환합니다.
타임스탬프	`$Timestamp`	로컬 시간대를 사용하여 이메일 메시지의 Received: 줄에서 확인되는 현재 시간 및 날짜를 반환합니다.

관련 주제

- 비ASCII 문자 집합 및 메시지 필터 작업 변수, 9-55페이지

비ASCII 문자 집합 및 메시지 필터 작업 변수

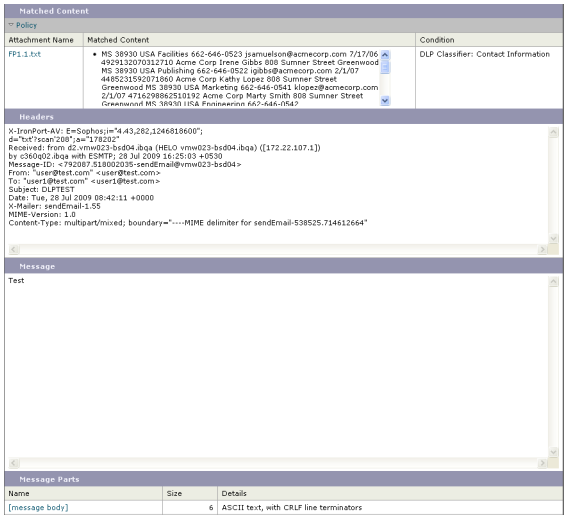
시스템은 ISO-2022 유형의 문자 인코딩(헤더 값에서 사용된 인코딩 유형)을 포함된 작업 변수의 확장을 지원하며 알림의 국제 범용 텍스트를 지원합니다. 이 기능은 함께 병합되어 알림을 생성하며, 이 알림은 quoted-printable 형식으로 UTF-8로 전송됩니다.

일치하는 콘텐츠 가시성

첨부 파일 콘텐츠 조건, 메시지 본문이나 첨부 파일 조건, 메시지 본문 조건 또는 첨부 파일 콘텐츠 조건과 일치하는 메시지에 대해 격리 작업을 구성하는 경우 격리된 메시지에서 일치하는 콘텐츠를 볼 수 있습니다. 메시지 본문을 표시하면 일치하는 콘텐츠가 노란색으로 강조 표시됩니다. 또한 $MatchedContent 작업 변수를 사용하여 메시지 제목에 일치하는 콘텐츠를 포함할 수 있습니다.

메시지 또는 콘텐츠 필터 규칙을 트리거한 로컬 격리에 있는 메시지를 볼 때, GUI는 실제로 필터 작업을 트리거하지 않은 콘텐츠를 표시합니다(필터 작업을 트리거한 콘텐츠 포함). 이러한 GUI 표시는 콘텐츠 일치 항목을 찾기 위한 지침으로 사용되지만, 정확한 콘텐츠 일치 목록을 반드시 반영하지는 않습니다. 이는 GUI가 필터에서 사용되는 것보다 덜 엄격한 콘텐츠 일치 논리를 사용하기 때문입니다. 이 문제는 메시지 본문의 강조 표시 부분에만 적용됩니다. 연결된 필터 규칙과 함께 메시지의 각 부분에서 일치하는 문자열을 나열하는 테이블은 정확한 정보를 보여줍니다.

그림 9-2 정책 격리에서 표시되는 일치 콘텐츠



메시지 필터 작업에 대한 설명 및 예

다음 섹션에서는 사용 중인 다양한 메시지 필터 작업과 예에 대해 설명합니다.

- 로그 항목 추가 작업, 9-72페이지
- URL 평판 작업, 9-72페이지
- URL 범주 작업, 9-74페이지
- 작업 없음, 9-75페이지

나머지 메시지 필터 작업 건너뛰기

skip-filters 작업은 메시지가 메시지 필터에서 모든 추가 처리 작업을 건너뛰고 이메일 파이프라인을 통해 계속 처리됩니다. skip-filters 작업을 유발하는 메시지는 어플라이언스에서 사용 가능한 경우 안티스팸 검사 및 안티바이러스 검사를 받습니다. skip-filters 작업은 메시지 필터의 기본적인 최종 작업입니다.

다음 필터는 customercare@example.com에게 알림을 전송하고 boss@admin으로 주소가 지정된 모든 메시지를 즉시 전달합니다.

```
bossFilter:

   if(rcpt-to == 'boss@admin$')

   {

        notify('customercare@example.com');

 skip-filters();

   }
```

삭제 작업

drop 작업은 메시지를 전달하지 않고 버립니다. 메시지는 발신자에게 반환되지 않고 원하는 수신자에게도 전송되지 않으며 어떤 방식으로도 추가로 처리되지 않습니다.

다음 필터는 먼저 george@whitehouse.gov에게 알림을 전송하고 제목이 SPAM으로 시작되는 모든 메시지를 버립니다.

```
spamFilter:

   if(subject == '^SPAM.*')

   {

        notify('george@whitehouse.gov');

        drop();

   }
```

바운스 작업

bounce 작업은 추가 처리 작업 없이 발신자(봉투 발신자)에게 메시지를 다시 전송합니다.

다음 필터는 @yahoo\\.com으로 끝나는 이메일 주소의 모든 메시지를 반환(바운스)합니다.

```
yahooFilter:

   if(mail-from == '@yahoo\\.com$')

   {

        bounce();

   }
```

암호화 작업

암호화 작업은 구성된 암호화 프로파일을 사용하여 암호화된 메시지를 이메일 수신자에게 전송합니다.

다음 필터는 제목에 [encrypt]를 포함한 경우 메시지를 암호화합니다.

```
Encrypt_Filter:

  if ( subject == '\\[encrypt\\]' )

   {

       encrypt('My_Encryption_Profile');

   }
```

참고 이 필터 작업을 사용하려면 네트워크에 Cisco 암호화 어플라이언스가 있어야 하며 또는 호스팅된 주요 서비스를 구성해야 합니다. 또한 이 필터 작업을 사용하려면 암호화 프로파일을 구성해야 합니다.

전달 시 S/MIME 서명 또는 암호화 작업

smime-gateway-deferred 작업은 전달 중에 지정된 전송 프로파일을 사용하여 메시지의 S/MIME 서명 또는 암호화를 수행합니다. 이는 메시지가 다음 처리 단계로 진행되고 모든 처리 작업이 완료되면 메시지가 서명되거나 암호화되어 전달된다는 의미입니다.

다음 필터는 전달 중에 특정한 발신자의 모든 발송 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 프로파일을 사용하여 S/MIME 서명 또는 암호화를 수행하고 메시지를 전달하여 이후 처리 작업을 건너뜁니다.

다음 필터는 특정한 발신자의 모든 발송 메시지에 대해 S/MIME 서명을 수행하고 메시지를 즉시 전송합니다.

```
smime-deliver-now:if(mail-from == "user@example.com"){smime-gateway("smime-sign");}
```

알림 및 복사본 알림 작업

notify 및 notify-copy 작업은 지정된 이메일 주소로 메시지의 이메일 요약을 전송합니다. notify-copy 작업은 bcc-scan 작업과 유사하게 원본 메시지의 복사본도 전송합니다. 알림 요약에는 다음 내용이 포함됩니다.

- 메시지의 메일 전송 프로토콜 대화의 봉투 발신자 및 봉투 수신자(MAIL FROM 및 RCPT TO) 지시문의 내용.
- 메시지의 메시지 헤더.
- 메시지와 일치하는 메시지 필터의 이름.

수신자, 제목 줄, 발신 주소 및 알림 템플릿을 지정할 수 있습니다. 다음 필터는 4MB보다 큰 메시지를 선택하고 일치 메시지의 알림 이메일을 admin@example.com으로 전송하고 최종적으로 메시지를 버립니다.

```
bigFilter:

   if(body-size >= 4M)

   {

        notify('admin@example.com');

        drop();

   }
```

또는

```
bigFilterCopy:

   if(body-size >= 4M)

   {

        notify-copy('admin@example.com');

        drop();

   }
```

봉투 수신자 매개변수는 유효한 이메일 주소(예: 위의 예에서 admin@example.com) 또는 작업 변수인 $EnvelopeRecipients(작업 변수, 9-53페이지 참조)이며 메시지의 모든 봉투 수신자를 지정합니다.

```
bigFilter:

   if(body-size >= 4M)

   {
```

```
        notify('$EnvelopeRecipients');

        drop();

    }
```

notify 작업은 또한 알림 메시지에 사용할 제목 헤더, 봉투 발신자 및 사전 정의된 텍스트 리소스를 지정하는 데 사용되는 최대 3개의 추가 인수(선택 사항)를 지원합니다. 이 매개변수는 순서대로 표시되어야 하므로 봉투 발신자가 설정되거나 알림 템플릿이 지정된 경우 제목이 제공되어야 합니다.

제목 매개변수에는 작업 변수(작업 변수, 9-53페이지 참조)가 포함되며 이 변수는 원본 메시지의 데이터로 대체될 수 있습니다. 기본적으로, 제목은 Message Notification으로 설정됩니다.

봉투 발신자 매개변수는 유효한 이메일 주소 또는 $EnvelopeFrom 작업 변수이며 이 변수는 메시지의 반환 경로를 원본 메시지와 동일하게 설정합니다.

알림 템플릿 매개변수는 기존의 알림 템플릿 이름입니다. 자세한 내용은 알림, 9-83페이지 항목을 참조하십시오.

이 예는 이전의 예를 확장한 것이지만 제목을 [bigFilter] Message too large와 같이 변경하고 반환 경로를 원래 발신자로 설정하며 "message.too.large" 템플릿을 사용합니다.

```
bigFilter:

    if (body-size >= 4M)

    {

        notify('admin@example.com', '[$FilterName] Message too large',

               '$EnvelopeFrom', 'message.too.large');

        drop();

    }
```

또한 $MatchedContent 작업 변수를 사용하여 콘텐츠 필터가 트리거되었음을 발신자 또는 관리자에게 알릴 수 있습니다. $MatchedContent 작업 변수는 필터를 트리거한 콘텐츠를 표시합니다. 예를 들어, 다음 필터는 이메일에 ABA 계정 정보가 포함된 경우 관리자에게 알림을 전송합니다.

```
ABA_filter:

if (body-contains ('*aba')){

notify('admin@example.com','[$MatchedContent]Account Information Displayed');

}
```

관련 주제

- 알림 템플릿, 9-61페이지

알림 템플릿

Text Resources(텍스트 리소스) 페이지 또는 `textconfig` CLI 명령을 사용하여 `notify()` 및 `notify-copy()` 작업과 함께 사용할 텍스트 리소스로 사용자 지정 알림 템플릿을 구성할 수 있습니다. 사용자 지정 알림 템플릿을 생성하지 않으면, 기본 템플릿이 사용됩니다. 기본 템플릿은 메시지 헤더를 포함하지만 사용자 지정 알림 템플릿은 기본적으로 메시지 헤더를 포함하지 않습니다. 사용자 지정 알림에 메시지 헤더를 포함하려면 `$AllHeaders` 작업 변수를 포함시킵니다.

자세한 내용은 "텍스트 리소스" 장을 참조하십시오.

이 예에서는 대량 메시지가 아래에 표시된 필터를 트리거할 때 메시지 크기가 너무 크다는 알리는 이메일이 원하는 수신자에게 전송됩니다.

```
bigFilter:

   if (body-size >= 4M)

   {

        notify('$EnvelopeRecipients', '[$FilterName] Message too large',

               '$EnvelopeFrom', 'message.too.large');

        drop();

   }
```

BCC(숨은 참조) 작업

`bcc` 작업은 지정된 수신자에게 메시지의 익명 복사본을 전송합니다. 이 작업은 경우에 따라 메시지 복제라고도 합니다. 원본 메시지에서 복사본에 대한 언급이 없으며 익명 복사본이 수신자에게 성공적으로 다시 바운스되지 않기 때문에 해당 메시지의 원래 발신자와 수신자는 복사본이 전송되었는지 여부를 반드시 알 필요가 없습니다.

다음 필터는 주소가 `johnny`에서 `sue`로 지정된 메시지마다 `mom@home.org`로 BCC(숨은 참조)를 전송합니다.

```
momFilter:

   if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

   {

        bcc('mom@home.org');

   }
```

`bcc` 작업은 또한 alt-mailhost 뿐만 아니라 복사된 메시지에 사용할 제목 헤더 및 봉투 발신자를 지정하는 데 사용되는 최대 3개의 추가 인수(선택 사항)를 지원합니다. 이 매개변수는 순서대로 표시되어야 하므로 봉투 발신자가 설정된 경우 제목이 제공되어야 합니다.

제목 매개변수에는 작업 변수(작업 변수, 9-53페이지 참조)가 포함되며 이 변수는 원본 메시지의 데이터로 대체될 수 있습니다. 기본적으로, 이 매개변수는 원본 메시지의 제목(`$Subject`에 해당)으로 설정됩니다.

봉투 발신자 매개변수는 유효한 이메일 주소 또는 $EnvelopeFrom 작업 변수이며 이 변수는 메시지의 반환 경로를 원본 메시지와 동일하게 설정합니다.

이 예에서는 제목을 [Bcc] <original subject>로 설정하여 이전 제목을 확장한 다음 반환 경로를 badbounce@home.org로 설정합니다.

```
momFilter:

   if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

   {

        bcc('mom@home.org', '[Bcc] $Subject', 'badbounce@home.org');

   }
```

alt-mailhost는 4번째 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 작업을 수행하면 네트워크를 통해 바이러스가 침투할 수 있습니다. BCC(숨은 참조) 작업은 원본 메시지의 전체 복사본인 새 메시지를 생성합니다. 알림 필터 작업은 원본 메시지의 헤더를 포함하는 새 메시지를 생성합니다. 드문 경우이기는 하지만 헤더에 바이러스가 포함될 수 있습니다. 바운스 필터 작업은 원본 메시지의 첫 번째 10k를 포함하는 새 메시지를 생성합니다. 이 3가지 경우에서는 모두 새 메시지가 안티바이러스 또는 안티스팸 검사에서 처리되지 않습니다.

여러 호스트로 전송하기 위해 bcc() 작업을 여러 번 호출할 수 있습니다.

```
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

- bcc-scan() 작업, 9-63페이지

bcc-scan() 작업

bcc-scan 작업은 전송된 메시지가 완전히 새로운 메시지로 처리되므로 전체 메일 파이프라인을 통해 전송된다는 점을 제외하고 bcc(숨은 참조) 작업과 유사한 역할을 수행합니다.

```
momFilter:

   if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

   {

        bcc-scan('mom@home.org');

   }
```

격리 및 중복 작업

quarantine('quarantine_name') 작업은 격리라는 큐에 포함하기 위해 메시지에 플래그를 지정합니다. 격리에 대한 자세한 내용은 "격리" 장을 참조하십시오.
duplicate-quarantine('quarantine_name') 작업은 메시지 복사본을 즉시 지정된 격리에 두며 원본 메시지는 이메일 파이프라인을 통해 계속 처리됩니다. 격리 이름은 대소문자를 구분합니다.

격리를 위해 플래그가 지정된 경우에도 메시지는 이메일 파이프라인의 나머지 작업을 계속 진행합니다. 메시지가 파이프라인 끝에 도달하였고 해당 메시지가 하나 이상의 격리를 위해 플래그가 지정되었다면 해당 큐로 메시지가 들어갑니다. 그렇지 않으면, 메시지가 전송됩니다. 메시지가 파이프라인 끝에 도달하지 않으면 격리로 이동하지 않습니다.

따라서 메시지 필터에 quarantine() 작업과 뒤이어 bounce() 또는 drop() 작업이 오는 경우, 최종 작업을 통해 메시지가 파이프라인의 끝에 도달하지 않으므로 메시지는 격리를 시작하지 않습니다. 메시지 필터가 격리 작업을 포함하는 경우도 이와 마찬가지로 동작하지만, 메시지는 안티스팸 또는 안티바이러스 검사 또는 콘텐츠 필터에 의해 나중에 삭제됩니다. skip-filters() 작업을 통해 메시지는 나머지 모든 메시지 필터를 건너뛰지만 콘텐츠 필터는 계속 적용됩니다. 예를 들어, 메시지 필터가 격리를 위해 메시지에 플래그를 지정하고 skip-filters() 작업을 포함하는 경우, 이메일 파이프라인의 다른 작업으로 인해 메시지가 삭제되지 않는 한 메시지는 나머지 모든 메시지 필터를 건너뛰고 격리됩니다.

다음의 예는 메시지에 "secret_words"라는 사전에 있는 임의의 단어가 포함된 경우, 정책 격리에 메시지가 전송됩니다.

```
quarantine_codenames:

   if (dictionary-match ('secret_words'))

       {

       quarantine('Policy');

       }
```

다음 예는 모든 .mp3 파일 첨부 파일을 삭제하는 공식 정책을 실시하고 있는 회사를 보여줍니다. 인바운드 메시지에 .mp3 첨부 파일이 있는 경우, 이 첨부 파일은 제거되고 나머지 메시지(원본 본문 및 나머지 첨부 파일)는 원래 수신자에게 전송됩니다. 모든 첨부 파일이 포함된 원본 메시지의 다른 복사본은 격리됩니다(정책 격리에 전송됨). 차단된 첨부 파일을 수신해야 하는 경우 원래 수신자는 해당 메시지를 격리에서 해제할 것을 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`을 포함하는 봉투 수신자 주소로 모든 메시지를 전송하며 메시지의 모든 수신자를 다음과 같이 변경합니다.
`system-lists@myhost.com`:

```
freelistFilter:

   if(rcpt-to == '\\.freelist\\.com$')

   {

        alt-rcpt-to('system-lists@myhost.com');

   }
```

전송 호스트 변경 작업

`alt-mailhost` 작업은 선택된 메시지의 모든 수신자의 IP 주소를 지정된 숫자 IP 주소 또는 호스트 이름으로 변경합니다.

참고 `alt-mailhost` 작업은 안티스팸 검사 엔진에서 스팸으로 분류된 메시지가 격리되지 않도록 합니다. `alt-mailhost` 작업은 격리 작업을 재정의하며 지정된 메일 호스트로 작업을 전송합니다.

다음 필터는 수신자 주소를 모든 메시지에 대한 호스트 `example.com`으로 리디렉션합니다.

```
localRedirectFilter:

   if(true)

   {
```

```
        alt-mailhost('example.com');

    }
```

따라서 joe@anywhere.com으로 전달된 메시지는 Envelope To 주소가 joe@anywhere.com인 메일 호스트 example.com으로 전달됩니다. smtproutes 명령을 사용하여 지정된 모든 추가 라우팅 정보는 메시지 라우팅에 적용됩니다. (로컬 도메인의 이메일 라우팅, 24-1페이지 참조.)

참고 alt-mailhost 작업은 포트 번호 지정 기능은 지원하지 않습니다. 포트 번호를 지정하려면 대신 SMTP 경로를 추가합니다.

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 메시지의 소스 호스트를 지정된 소스로 변경합니다. 소스 호스트는 메시지 전달에 사용되는 IP 인터페이스 또는 IP 인터페이스 그룹으로 구성됩니다. IP 인터페이스 그룹을 선택한 경우, 시스템은 이메일을 전달할 때의 소스 인터페이스와 마찬가지로 그룹 내의 모든 IP 인터페이스를 통해 라운드 로빈을 수행합니다. 기본적으로 이 방법을 통해 여러 가상 게이트웨이 주소를 단일 Cisco Email Security 어플라이언스에서 생성할 수 있습니다. 자세한 내용은 가상 게이트웨이™ 기술을 사용하여 모든 호스팅된 도메인에 대한 메일 게이트웨이 구성, 24-56페이지 항목을 참조하십시오.

IP 인터페이스는 현재 시스템에 구성되어 있는 IP 인터페이스 또는 인터페이스 그룹으로만 변경될 수 있습니다. 다음 필터는 IP 주소 1.2.3.4를 사용하는 원격 호스트 에서 수신한 모든 메시지에 대해 아웃바운드(전달) IP 인터페이스인 outbound2를 사용합니다.

```
externalFilter:

    if(remote-ip == '1.2.3.4')

    {

        alt-src-host('outbound2');

    }
```

다음 필터는 IP 주소 1.2.3.4를 사용하는 원격 호스트에서 수신한 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 헤더 및 수신자를 포함하는 원본 메시지의 복사본을 mbox 형식 파일로 어플라이언스에 저장합니다. 이 작업은 메시지를 저장하는 로그 파일의 이름인 매개변수를 사용합니다. 필터를 생성할 때 시스템은 지정된 파일 이름의 로그 서브스크립션을 자동으로 생성합니다. 또는 기존 필터 로그 파일을 지정할 수 있습니다. 필터 및 필터 로그 파일을 생성한 후에 filters -> logconfig 하위 명령을 사용하여 필터 로그 옵션을 편집할 수 있습니다.

참고 logconfig 명령은 filters의 하위 명령입니다. 이 하위 명령을 사용하는 방법에 대한 자세한 설명은 CLI를 사용하여 메시지 필터 관리, 9-86페이지 항목을 참조하십시오.

mbox 형식은 표준 UNIX 메일함 형식이며 메시지를 보다 쉽게 확인할 수 있는 여러 유틸리티가 있습니다. 대부분의 UNIX 시스템에서
파일을 확인하기 위해 "mail -f *mbox.filename*"을 입력할 수 있습니다. mbox 형식은 일반 텍스트이므로 간단한 텍스트 편집기를 사용하여 메시지 콘텐츠를 확인할 수 있습니다.

다음 예에서 메시지 복사본은 joesmith라는 로그에 저장됩니다(봉투 발신자가 joesmith@yourdomain.com과 일치하는 경우).

```
logJoeSmithFilter:

   if(mail-from == '^joesmith@yourdomain\\.com$')

   {

        archive('joesmith');

   }
```

헤더 제거 작업

strip-header 작업은 메시지에서 특정 헤더를 검사하고 메시지를 전송하기 전에 해당하는 줄을 제거합니다. 여러 헤더가 있는 경우, 헤더의 모든 인스턴스가 제거됩니다(예: "Received:" 헤더).

다음 예에서는 전송되기 전에 모든 메시지에서 X-DeleteMe 헤더가 제거됩니다.

```
stripXDeleteMeFilter:

   if (true)
```

```
{
     strip-header('X-DeleteMe');
}
```

헤더에 작업을 수행할 경우, 헤더의 현재 값에 처리하는 동안 발생한 변경사항이 포함됩니다(예: 메시지 제목을 추가, 제거 또는 수정하는 필터 작업). 자세한 내용은 메시지 헤더 규칙 및 평가, 9-5 페이지 항목을 참조하십시오.

헤더 삽입 작업

insert-header 작업은 새 헤더를 메시지에 삽입합니다. AsyncOS는 삽입하는 헤더의 표준을 준수하는지 확인하지 않습니다. 결과 메시지가 이메일에 대한 인터넷 표준을 준수하는지 여부는 사용자가 확인해야 합니다.

다음 예는 아직 헤더를 메시지에서 확인하지 못한 경우 X-Company라는 헤더를 My Company Name으로 설정된 값과 함께 삽입합니다.

```
addXCompanyFilter:
   if (not header('X-Company'))
   {
        insert-header('X-Company', 'My Company Name');
   }
```

insert-header() 작업에서는 비ASCII 문자를 헤더 텍스트에서 사용할 수 있지만, 표준을 준수하도록 헤더 이름은 ASCII로 제한됩니다. 전송 인코딩은 가독성을 극대화하기 위해 quoted-printable을 사용합니다.

참고

strip-headers 및 insert-header 작업은 원본 메시지에서 메시지 헤더를 재작성할 수 있도록 결합하여 사용할 수 있습니다. 경우에 따라 동일한 헤더(예:Received:)에 대해 여러 인스턴스를 보유할 수 있습니다. 반면에 동일한 헤더가 여러 인스턴스를 가지면 MUA(예: 여러 Subject: 헤더)가 혼동될 수 있습니다.

헤더에 작업을 수행할 경우, 헤더의 현재 값에 처리하는 동안 발생한 변경사항이 포함됩니다(예: 메시지 제목을 추가, 제거 또는 수정하는 필터 작업). 자세한 내용은 메시지 헤더 규칙 및 평가, 9-5 페이지 항목을 참조하십시오.

헤더 텍스트 편집 작업

edit-header-text 작업을 통해 정규식 대체 함수를 사용하여 지정된 헤더 텍스트를 재작성할 수 있습니다. 이 필터는 헤더에 있는 정규식과 일치 여부를 확인하며 해당 정규식은 지정한 정규식으로 대체할 수 있습니다.

예를 들어, 이메일에는 다음 제목 헤더가 포함됩니다.

```
Subject: SCAN Marketing Messages
```

다음 필터는 "SCAN" 텍스트를 제거하고 헤더의 "Marketing Messages" 텍스트는 그대로 둡니다.

```
Remove_SCAN: if true

   {

      edit-header-text ('Subject', '^SCAN\\s*','');

}
```

필터에서 메시지를 처리한 후 다음 헤더를 반환합니다.

```
Subject: Marketing Messages
```

본문 텍스트 수정 작업

`edit-body-text()` 메시지 필터는 `Edit-Header-Text()` 필터와 비슷하지만 한 가지 헤더 대신 메시지 본문 전체에서 동작합니다.

`edit-body-text()` 메시지 필터는 첫 번째 매개변수가 검색할 정규식이며 두 번째 매개변수가 대체 텍스트인 경우 다음 구문을 사용합니다.

```
Example: if true {

edit-body-text("parameter 1",

"parameter 2");

       }
```

`edit-body-text()` 메시지 필터는 메시지 본문에서만 작업합니다. 지정된 MIME 부분이 메시지 "본문"인지 또는 메시지 "첨부 파일"인지를 판단하는 데에 대한 자세한 내용은 메시지 본문과 메시지 첨부 파일 비교, 9-5페이지 항목을 참조하십시오.

다음 예는 메시지에서 제거되고 'URL REMOVED' 텍스트로 대체된 URL을 보여줍니다.

```
URL_Replaced: if true {



 edit-body-text("(?i)(?:https?|ftp)://[^\\s\">]+", "URL REMOVED");

       }
```

다음 예는 메시지 본문에서 제거되고 "XXX-XX-XXXX' 텍스트로 대체된 사회 보장 번호를 보여줍니다.

```
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 이때 edit-body-text() 필터와 함께 스마트 식별자를 사용할 수 없습니다.

HTML 변환 작업

RFC 2822는 이메일 메시지를 위한 텍스트 형식을 정의하며, RFC 2822 메시지 내의 다른 콘텐츠를 전송하는 확장명(예: MIME)이 있습니다. AsyncOS는 현재 html-convert() 메시지 필터를 사용하여 다음 구문을 통해 HTML을 일반 텍스트로 변환할 수 있습니다.

```
Convert_HTML_Filter:

if (true)

{

html-convert();

}
```

Cisco 메시지 필터는 지정된 MIME 부분이 메시지 "본문"인지 또는 메시지 "첨부 파일"인지를 판단합니다. html-convert() 필터는 메시지 본문 부분에서만 작업합니다. 메시지 본문 및 첨부 파일에 대한 자세한 내용은 메시지 본문과 메시지 첨부 파일 비교, 9-5페이지 항목을 참조하십시오.

형식에 따라 html-convert() 필터는 문서에서 HTML을 제거할 때 다양한 방법을 사용합니다.

메시지가 일반 텍스트(text/plain)인 경우, 메시지는 변경되지 않은 상태로 필터를 통과합니다. 메시지가 간단한 HTML 메시지(text/html)인 경우 모든 HTML 태그가 메시지에서 제거되며 결과로 남은 본문이 HTML 메시지를 대체합니다. 줄에는 서식이 다시 지정되지 않으며 HTML은 일반 텍스트로 렌더링되지 않습니다. 구조가 MIME(여러 부분/대체 구조가 있음)이며 동일한 콘텐츠와 함께 text/plain 부분 및 텍스트/html 부분을 모두 포함하는 경우, 필터는 메시지에서 text/html 부분을 제거하고 메시지의 text/plain 부분은 그대로 둡니다. 기타 모든 MIME 유형(예: 여러 부분/혼합)의 경우 모든 HTML 본문 부분에서 태그가 제거되고 메시지에 다시 삽입됩니다.

html-convert() 필터 작업이 메시지 필터에서 수행되는 경우, 처리할 메시지에만 태그를 지정하며 메시지 구조는 즉시 변경되지 않습니다. 메시지 변경사항은 모든 처리가 완료된 이후에만 적용됩니다. 따라서 기타 필터 작업에서 수정되기 전에 원본 메시지 본문을 처리할 수 있습니다.

바운스 프로파일 작업

bounce-profile 작업은 사전에 구성한 바운스 프로파일을 메시지에 할당합니다. (바운스된 이메일 전달, 24-34페이지 참조.) 메시지를 전달할 수 없는 경우, 바운스 프로파일을 통해 구성된 바운스 옵션이 사용됩니다. 이 기능을 사용하면 리스너 구성(할당된 경우)에서 메시지에 할당된 바운스 프로파일을 재정의합니다.

다음 필터의 예는 바운스 프로파일인 "fastbounce"를 `X-Bounce-Profile: fastbounce` 헤더를 사용하여 전송된 모든 이메일에 할당합니다.

```
fastbounce:

   if (header ('X-Bounce-Profile') == 'fastbounce') {

        bounce-profile ('fastbounce');

   }
```

안티스팸 시스템 우회 작업

`skip-spamcheck` 작업을 사용하면 메시지가 시스템에 구성되어 있는 모든 콘텐츠 기반 안티스팸 필터링을 우회할 수 있습니다. 이 작업은 콘텐츠 기반 안티스팸 필터링이 구성되지 않은 경우 또는 메시지가 처음부터 스팸 검사를 위해 플래그가 지정되지 않은 경우 메시지에 아무 작업도 수행하지 않습니다.

다음 예에서는 높은 SenderBase Reputation 점수를 가진 메시지가 콘텐츠 기반 안티스팸 필터링 기능을 우회합니다.

```
whitelist_on_reputation:

   if (reputation > 7.5)

   {

        skip-spamcheck();

   }
```

관련 주제

- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 13-2페이지
- 스팸 필터로부터 어플라이언스에서 생성된 메시지 보호, 13-14페이지

안티바이러스 시스템 우회 작업

`skip-viruscheck` 작업을 사용하면 메시지가 시스템에 구성되어 있는 모든 바이러스 보호 시스템을 우회할 수 있습니다. 이 작업은 안티바이러스 시스템이 구성되지 않은 경우 또는 메시지가 처음부터 바이러스 검사를 위해 플래그가 지정되지 않은 경우 메시지에 아무 작업도 수행하지 않습니다.

다음 예는 리스너인 "private_listener"에서 수신한 메시지가 안티스팸 및 안티바이러스 시스템을 우회합니다.

```
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 메시지가 시스템에 구성되어 있는 파일 평판 필터링 및 파일 분석을 우회할 수 있습니다. 이 작업은 파일 평판 필터링 및 파일 분석이 구성되지 않은 경우 또는 메시지가 처음부터 파일 평판 필터링 및 파일 분석을 위해 플래그가 지정되지 않은 경우 메시지에 아무 작업도 수행하지 않습니다.

다음 예는 PDF 첨부 파일이 있는 메시지가 파일 평판 필터링 및 파일 분석을 우회합니다.

```
skip_amp_scan:
if (attachment-filetype == 'pdf')
{
skip-ampcheck();
}
```

신종 바이러스 필터(Outbreak Filter) 검사 우회 작업

skip-vofcheck 작업을 사용하면 메시지가 신종 바이러스 필터(Outbreak Filter) 검사를 우회할 수 있습니다. 이 작업은 신종 바이러스 필터(Outbreak Filter) 검사가 활성화되지 않은 경우 메시지에 아무 작업도 수행하지 않습니다.

다음 예는 리스너인 "private_listener"에서 수신한 메시지가 신종 바이러스 필터(Outbreak Filter) 검사를 우회합니다.

```
internal_mail_is_safe:

   if (recv-listener == 'private_listener') Outbreak Filters

   {

        skip-vofcheck();

   }
```

메시지 태그 추가 작업

tag-message 작업은 RSA 이메일 DLP 정책 필터링에 사용할 발송 메시지에 사용자 지정 용어를 삽입합니다. 메시지 태그를 포함하는 메시지로 검사를 제한하도록 RSA 이메일 DLP 정책을 구성할 수 있습니다. 수신자에게는 메시지 태그가 보이지 않습니다. 태그 이름은 [a-zA-Z0-9_-.]로 구성된 모든 문자 조합을 사용할 수 있습니다.

메시지 필터링을 위한 DLP 정책 구성에 대한 자세한 정보는 "데이터 유출 방지" 장을 참조하십시오.

다음 예는 제목에 "[Encrypt]"가 있는 메시지에 메시지 태그를 삽입합니다. 그런 다음 Cisco 이메일 암호화가 사용 가능한 경우 메시지를 전달하기 전에 이 메시지 태그를 사용하여 메시지를 암호화하는 DLP 정책을 생성할 수 있습니다.

```
Tag_Message:

   if (subject == '^\\[Encrypt\\]')
```

```
{
     tag-message('Encrypt-And-Deliver');
}
```

로그 항목 추가 작업

log-entry 작업은 INFO 수준의 텍스트 메일 로그에 사용자 지정 텍스트를 삽입합니다. 텍스트는 작업 변수를 포함할 수 있습니다. 이 작업을 사용하여 디버깅에 유용한 텍스트 및 메시지 필터에서 특정한 작업을 수행한 이유에 대한 정보를 삽입할 수 있습니다. 로그 항목은 메시지 추적에도 표시됩니다.

다음 예에서는 메시지에 회사 기밀 정보가 포함되었을 가능성이 있어 메시지가 바운스되었음을 설명하는 로그 항목을 삽입합니다.

```
CompanyConfidential:
   if (body-contains('Company Confidential'))
   {
        log-entry('Message may have contained confidential information.');
        bounce();
   }
```

URL 평판 작업

메시지의 URL 평판 점수를 사용하여 URL 또는 동작을 수정합니다. 중요한 세부 사항 및 예에 대해서는 필터에서 URL 평판 및 URL 범주 작업을 사용하여 메시지의 URL 수정, 15-8페이지(15 장, "URL 필터링") 항목을 참조하십시오.

이 작업에서는 규칙이 필요하지 않습니다.

URL 평판 작업의 항목은 다음과 같습니다.

- msg_filter_name:은 이 메시지 필터의 이름입니다.
- min_score 및 max_score는 작업을 적용해야 하는 범위에서의 최소 점수 및 최대 점수입니다. 적용 가능한 범위에는 지정한 값이 포함됩니다.

  최소 및 최대 점수는 -10.0~10.0이어야 합니다.
- 평판 서비스에서 점수를 제공하지 않는 경우 작업을 지정하려면 다음의 하위 섹션에 표시된 것처럼 작업에 대해 해당하는 "no-reputation" 버전을 사용합니다.
- whitelist는 정의된 URL 목록(urllistconfig 명령 사용)의 이름입니다. 화이트리스트 지정은 선택 사항입니다.
- Preserve_signed 대신 0 또는 1을 입력합니다.
  - 1 - 서명되지 않은 메시지에만 이 작업을 적용합니다.
  - 0 - 모든 메시지에 이 작업을 적용합니다.

  preserve_signed 값을 지정하지 않은 경우 이 작업은 서명되지 않은 메시지에만 적용됩니다.

관련 주제

- URL 평판을 기준으로 URL을 텍스트로 대체, 9-73페이지
- URL 평판을 기준으로 URL 무해화, 9-73페이지
- URL 평판을 기준으로 Cisco 보안 프록시에 URL 리디렉션, 9-73페이지

URL 평판을 기준으로 URL을 텍스트로 대체

평판 서비스에서 점수를 제공할 때 수행해야 할 작업은 다음과 같습니다.

`url-reputation-replace` 작업을 사용합니다.

`url-reputation-replace` 작업을 사용하는 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{url-reputation-replace(<min_score>, <max_score>,'<replace_text>', '<whitelist>',
<Preserve_signed>);}
```

이때 `replace_text`는 URL을 대체할 텍스트입니다.

평판 서비스에서 점수를 제공하지 않을 때 수행해야 할 작업은 다음과 같습니다.

`url-no-reputation-replace` 작업을 사용합니다.

`url-no-reputation-replace` 작업을 사용하는 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{url-no-reputation-replace ('<replace_text>', '<whitelist>', <Preserve_signed>);}
```

이때 `replace_text`는 URL을 대체할 텍스트입니다.

URL 평판을 기준으로 URL 무해화

평판 서비스에서 점수를 제공할 때 수행해야 할 작업은 다음과 같습니다.

`url-reputation-defang` 작업을 사용합니다.

`url-reputation-defang` 작업을 사용하는 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{url-reputation-defang (<min_score>, <max_score>, '<whitelist>', <Preserve_signed>);}
```

평판 서비스에서 점수를 제공하지 않을 때 수행해야 할 작업은 다음과 같습니다.

`url-no-reputation-defang` 작업을 사용합니다.

`url-no-reputation-defang` 작업을 사용하는 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{url-no-reputation-defang ('<whitelist>', <Preserve_signed>);}
```

URL 평판을 기준으로 Cisco 보안 프록시에 URL 리디렉션

평판 서비스에서 점수를 제공할 때 수행해야 할 작업은 다음과 같습니다.

`url-reputation-proxy-redirect` 작업을 사용합니다.

`url-reputation-proxy-redirect` 작업을 사용하는 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{url-reputation-proxy-redirect (<min_score>, <max_score>, '<whitelist>',
<Preserve_signed>);}
```

평판 서비스에서 점수를 제공하지 않을 때 수행해야 할 작업은 다음과 같습니다.

`url-no-reputation-proxy-redirect` 작업을 사용합니다.

`url-no-reputation-proxy-redirect` 작업을 사용하는 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{url-no-reputation-proxy-redirect ('<whitelist>', <Preserve_signed>);}
```

URL 범주 작업

메시지의 URL 범주를 사용하여 URL 또는 동작을 수정합니다. 중요한 정보에 대해서는 필터에서 URL 평판 및 URL 범주 작업을 사용하여 메시지의 URL 수정, 15-8페이지(15 장, "URL 필터링") 항목을 참조하십시오.

이 작업에서는 규칙이 필요하지 않습니다.

모든 URL 범주 작업은 다음과 같습니다.

- `msg_filter_name`은 메시지 필터의 이름입니다.
- `category-name`은 URL 범주입니다. 범주가 여러 개인 경우 쉼표로 구분합니다. 정확한 범주 이름을 가져오기 위해 콘텐츠 필터에서 URL 범주 조건 또는 작업을 확인합니다. 범주에 대한 설명 및 예에 대해서는 URL 범주 정보, 15-13페이지 항목을 참조하십시오.
- `url_white_list`는 정의된 URL 목록(`urllistconfig` 명령 사용)의 이름입니다.
- `unsigned-only`: 0 또는 1을 입력합니다.
  - 1 - 서명되지 않은 메시지에만 이 작업을 적용합니다.
  - 0 - 모든 메시지에 이 작업을 적용합니다.

관련 주제

- URL 범주를 기준으로 URL을 텍스트로 대체, 9-74페이지
- URL 범주를 기준으로 URL 무해화, 9-75페이지
- URL 범주를 기준으로 Cisco 보안 프록시에 URL 리디렉션, 9-75페이지

URL 범주를 기준으로 URL을 텍스트로 대체

`url-category-replace` 작업을 사용하는 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{
url-category-replace(['<category-name1>','<category-name2>',…,
'<category-name3>'],'<replacement-text>', '<url_white_list>', <unsigned-only>);
}
```

이때 `replacement-text`는 URL을 대체하기 위해 사용할 텍스트입니다.

URL 범주를 기준으로 URL 무해화

`url-category-defang` 작업을 사용하는 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{
url-category-defang(['<category-name1>','<category-name2>',…, '<category-name3>'],
'<url_white_list>', <unsigned-only>);
}
```

URL 범주를 기준으로 Cisco 보안 프록시에 URL 리디렉션

`url-category-proxy-redirect` 작업을 사용하는 필터 구문은 다음과 같습니다.

```
<msg_filter_name>:
if <condition>
{
url-category-proxy-redirect(['<category-name1>','<category-name2>',…,
'<category-name3>'], '<url_white_list>', <unsigned-only>);
}
```

작업 없음

작업 없음 작업은 no-op를 수행하거나 작업을 수행하지 않습니다. 알림, 격리 또는 삭제와 같은 다른 동작을 사용하지 않으려는 경우 메시지 필터에서 이 작업을 사용할 수 있습니다. 예를 들어, 생성한 새 메시지 필터의 동작을 이해하려면 작업 없음 작업을 사용할 수 있습니다. 메시지 필터가 동작한 후에 Message Filters(메시지 필터) 보고서 페이지를 사용하여 새 메시지 필터의 동작을 모니터링하고 필터를 요구 사항에 맞게 조정할 수 있습니다.

다음 예는 메시지 필터에서 작업 없음 작업을 사용하는 방법을 보여줍니다.

```
new_filter_test: if header-repeats ('subject', X, 'incoming') {no-op();}
```

첨부 파일 검사

AsyncOS는 메시지에서 회사 정책과 일치하지 않는 첨부 파일은 제거하면서 원본 메시지를 전달할 수 있습니다.

해당하는 특정 파일 유형, 지문 또는 첨부 파일 콘텐츠에 따라 첨부 파일을 필터링할 수 있습니다. 지문을 사용하면 첨부 파일의 정확한 유형을 확인할 수 있습니다. 사용자가 악의적인 첨부 파일 확장명(예: `.exe`)의 이름을 더 일반적인 확장명(예: `.doc`)으로 바꿔 이름이 바뀐 파일이 첨부 파일 필터를 우회하지 못하게 할 수 있습니다.

첨부 파일에서 콘텐츠를 검사할 때 Stellent 첨부 파일 검사 엔진은 정규식을 검색하기 위해 첨부 파일에서 데이터를 추출합니다. 이 엔진은 첨부 파일에서 데이터 및 메타데이터를 모두 검사합니다. Excel 또는 Word 문서를 검사하는 경우, 첨부 파일 검사 엔진은 다음의 내장 파일 유형을 검색할 수 있습니다. .exe , .dll, .bmp, .tiff, .pcx, .gif, .jpeg, .png 및 Photoshop 이미지.

관련 주제

- 첨부 파일 검사를 위한 메시지 필터, 9-76페이지
- 이미지 분석, 9-77페이지

- 이미지 분석 검사 엔진 구성, 9-77페이지
- 이미지 분석 결과에 기반하여 작업을 수행하도록 메시지 필터 구성, 9-81페이지
- 알림, 9-83페이지
- 첨부 파일 검사 메시지 필터 예, 9-83페이지

첨부 파일 검사를 위한 메시지 필터

표 9-8에 설명된 메시지 필터 작업은 *최종 작업 이외의* 작업입니다. (첨부 파일이 삭제되고 메시지 처리가 계속됩니다.)

선택 사항인 주석은 메시지에 추가된 텍스트로 바닥글과 매우 유사하며, 메시지 필터 작업 변수(첨부 파일 검사 메시지 필터 예, 9-83페이지 참조)를 포함할 수 있습니다.

표 9-8 첨부 파일 필터링을 위한 메시지 필터 작업

작업	구문	설명
이름별로 첨부 파일 삭제	`drop-attachments-by-name (<regular expression>[, <optional comment>])`	지정된 정규식과 일치하는 파일 이름을 가진 메시지의 첨부 파일을 모두 삭제합니다. 일치하는 파일이 있는 경우 아카이브 파일 첨부(zip, tar)가 삭제됩니다. 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.
유형별로 첨부 파일 삭제	`drop-attachments-by-type (<MIME type>[, <optional comment>])`	지정된 MIME 유형 또는 파일 확장명에 의해 결정된 MIME 유형이 있는 메시지의 모든 첨부 파일을 삭제합니다. 일치하는 파일이 있는 경우 아카이브 파일 첨부(zip, tar)가 삭제됩니다.
파일 유형별로 첨부 파일 삭제	`drop-attachments-by-filetype (<fingerprint name>[, <optional comment>])`	파일의 지정된 "지문"과 일치하는 메시지의 첨부 파일을 모두 삭제합니다. 일치하는 파일이 있는 경우 아카이브 파일 첨부(zip, tar)가 삭제됩니다. 자세한 내용은 표 9-6첨부 파일 그룹, 9-52페이지 항목을 참조하십시오.
MIME 유형별로 첨부 파일 삭제	`drop-attachments-by-mimetype (<MIME type>[, <optional comment>])`	지정된 MIME 유형을 가진 메시지의 첨부 파일을 모두 삭제합니다. 이 작업에서는 파일 확장명에 따라 MIME 유형을 확인하지 않으므로 아카이브 콘텐츠도 검사하지 않습니다.
크기별로 첨부 파일 삭제	`drop-attachments-by-size (<number>[, <optional comment>])`	원시 인코딩 형식이며 지정된 크기(바이트)보다 크거나 같은 메시지의 첨부 파일을 모두 삭제합니다. 아카이브 파일 또는 압축 파일의 경우 이 작업은 압축되지 않은 크기를 검사하는 대신 실제 첨부 파일 자체의 크기를 검사합니다.

표 9-8 첨부 파일 필터링을 위한 메시지 필터 작업 (계속)

작업	구문	설명
첨부 파일 검사	`drop-attachments-where-contains (<regular expression>[, <optional comment>])`	정규식이 포함된 메시지의 모든 첨부 파일을 삭제합니다. 포함된 파일이 정규식 패턴과 일치하는 경우 아카이브 파일(zip, tar)이 삭제됩니다.
사전 일치별로 첨부 파일 삭제	`drop-attachments-where-dictionary-match(<dictionary name>)`	이 필터 작업은 사전 용어와 일치하는 항목에 따라 첨부 파일을 제거합니다. 첨부 파일로 간주되는 MIME 부분의 용어가 사전 용어와 일치하는 경우(또한 사용자 정의 임계값을 만족하는 경우) 첨부 파일이 이메일에서 제거됩니다. 첨부 파일 검사 메시지 필터 예, 9-83페이지 항목을 참조하십시오.

이미지 분석

일부 메시지에는 부적절한 콘텐츠가 포함되어 있는지 검사해야 하는 이미지가 있습니다. 이미지 분석 엔진을 사용하여 이메일의 부적절한 콘텐츠를 검색할 수 있습니다. 이미지 분석은 안티바이러스 및 안티스팸 검사 엔진을 보완 또는 대체하기 위해 설계되지 않았습니다. 이미지 분석은 이메일에서 부적절한 콘텐츠를 식별하여 사용할 수 있도록 적용합니다. 이미지 분석 검사 엔진을 사용하여 메일을 격리 및 분석하고 트렌드를 파악할 수 있습니다.

이미지 분석을 위해 AsyncOS를 구성한 후에 이미지 분석 필터 규칙을 사용하여 의심스럽거나 부적절한 이메일에서 작업을 수행할 수 있습니다. 이미지 검사를 통해 다음 유형의 첨부 파일을 검사할 수 있습니다. 예: JPEG, BMP, PNG, TIFF, GIF, TGA, ICO 및 PCX. 이미지 분석기는 그래픽에 부적절한 콘텐츠가 포함될 확률을 판단하기 위해 스킨 색상, 본문 크기 및 곡률을 측정하는 알고리즘을 사용합니다. 이미지 첨부 파일을 검사할 때 Cisco 지문을 통해 파일 유형을 판단하고 이미지 분석기는 이미지 콘텐츠를 분석하는 알고리즘을 사용합니다. 이미지가 다른 파일에 내장된 경우, Stellent 검사 엔진은 해당 파일을 추출합니다. Stellent 검사 엔진은 Word, Excel, PowerPoint 문서를 비롯하여 많은 파일 유형으로부터 이미지를 추출할 수 있습니다. 이미지 분석 판정은 메시지에서 전체적으로 계산됩니다. 메시지에 이미지가 포함되지 않은 경우, 메시지는 "0"점을 받아 "clean(정상)" 판정으로 매핑됩니다. 따라서 이미지가 없는 모든 메시지는 "clean(정상)" 판정을 수신합니다.

참고 이미지는 PDF 파일에서 추출할 수 없습니다.

이미지 분석 검사 엔진 구성

GUI에서 이미지 분석을 활성화하려면 다음을 수행합니다.

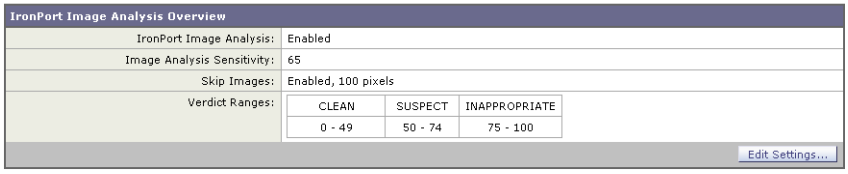
절차

1단계 Security Services(보안 서비스) > IronPort Image Analysis(IronPort 이미지 분석)로 이동합니다.

2단계 Enable(활성화)을 클릭합니다.

성공 메시지가 표시되고 판정 설정이 표시됩니다.

그림 9-3 Cisco 이미지 분석 개요



이미지 분석 필터 규칙을 통해 다음 판정에 따라 취해야 할 조치를 결정할 수 있습니다.

- **Clean(정상)**: 이미지에 부적절한 콘텐츠가 없습니다. 이미지 분석 판정은 메시지에서 전체적으로 계산되므로 이미지가 없는 메시지는 검사되는 경우 "clean(정상)" 판정을 수신합니다.
- **Suspect(의심)**: 이미지에 부적절한 콘텐츠가 포함되어 있을 수 있습니다.
- **Inappropriate(부적절)**: 이미지에 부적절한 콘텐츠가 포함되어 있습니다.

이러한 판정은 부적절한 콘텐츠가 포함될 확률을 판단하는 이미지 분석기 알고리즘에서 할당된 숫자 값을 표시합니다.

다음 값이 권장됩니다.

- 정상: 0~49
- 의심: 50~74
- 부적절: 75~100

민감도 설정을 구성하여 이미지 검사를 조정할 수 있으며 이를 통해 긍정 오류 수를 줄일 수 있습니다. 예를 들어 계속 긍정 오류가 발생하고 있음을 확인한 경우 민감도 설정을 낮출 수 있습니다. 반대로 이미지 검사를 통해 부적절한 콘텐츠가 없음을 발견한 경우 민감도를 더 높게 설정할 수 있습니다. 민감도 설정은 0(민감도 없음)~100(매우 민감)의 값입니다. 기본 민감도 설정은 65가 권장됩니다.

관련 주제

- 이미지 분석 설정 조정, 9-78페이지

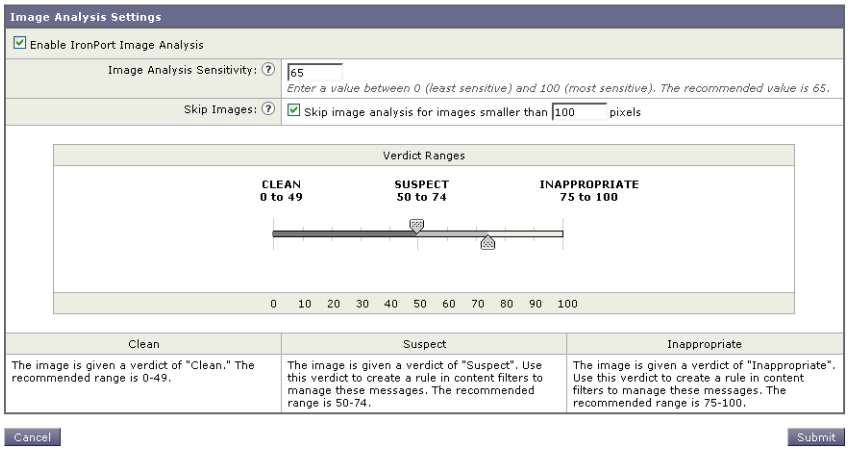
이미지 분석 설정 조정

절차

1단계 **Security Services(보안 서비스) > IronPort Image Analysis(IronPort 이미지 분석)**로 이동합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

그림 9-4 IronPort 이미지 분석 설정 편집



3단계 이미지 분석 민감도 설정을 구성합니다. 기본 민감도 설정은 65가 권장됩니다.

4단계 Clean(정상), Suspect(의심) 및 Inappropriate(부적절)로 설정을 구성합니다.

값 범위를 구성할 때 값이 겹치지 않아야 하며 정수를 사용해야 합니다.

5단계 선택적으로 최소 크기 요구 사항을 만족하지 않는 이미지 검사를 우회하도록 AsyncOS를 구성합니다(권장). 기본적으로 이 설정은 100픽셀에 대해 구성됩니다. 100픽셀보다 작은 이미지를 검사할 때 경우에 따라 긍정 오류가 발생할 수 있습니다.

또한 `imageanalysisconfig` 명령을 사용하여 이미지 분석 설정을 활성화할 수 있습니다.

```
test.com> imageanalysisconfig


IronPort Image Analysis: Enabled

Image Analysis Sensitivity: 65

Verdict Ranges: Clean (0-49), Suspect(50-74), Inappropriate (75+)

Skip small images with size less than 100 pixels (width or height)


Choose the operation you want to perform:

- SETUP - Configure IronPort Image Analysis.

[]> setup


IronPort Image Analysis: Enabled

Would you like to use IronPort Image Analysis? [Y]>


Define the image analysis sensitivity. Enter a value between 0 (least
```

```
sensitive) and 100 (most sensitive). As sensitivity increases, so does the false positive
rate. The default setting of 65 is recommended.

[65]>



Define the range for a CLEAN verdict. Enter the upper bound of the CLEAN range by
entering a value between 0 and 98. The default setting of 49 is recommended.

[49]>



Define the range for a SUSPECT verdict. Enter the upper bound of the SUSPECT range by
entering a value between 50 and 99. The default setting of 74 is recommended.

[74]>



Would you like to skip scanning of images smaller than a specific size? [Y]>



Please enter minimum image size to scan in pixels, representing either height or width of
a given image.

[100]>
```

관련 주제

- 특정 메시지의 판정 점수 보기, 9-80페이지

특정 메시지의 판정 점수 보기

특정 메시지에 대한 판정 점수를 확인하기 위해 메일 로그를 확인할 수 있습니다. 메일 로그는 이미지 이름이나 파일 이름, 특정 메시지 첨부 파일에 대한 점수를 표시합니다. 또한, 로그는 파일의 이미지가 검사 가능한지 여부에 대한 정보를 표시합니다. 로그의 정보는 이미지 대신 각각의 메시지 첨부 파일의 결과를 설명합니다. 예를 들어, 메시지에 JPEG 이미지가 포함된 zip 첨부 파일이 있는 경우, 로그 항목에는 JPEG 이름 대신 zip 파일의 이름이 포함됩니다. 또한 zip 파일에 여러 이미지가 포함된 경우 로그 항목은 모든 이미지의 최대 점수를 포함할 수 있습니다. 검사 불가능 표기법은 모든 이미지를 검사할 수 없음을 표시합니다.

로그에는 점수를 특정 판정(정상, 의심 또는 부적절)으로 변환하는 방법에 대한 정보는 포함하지 않습니다. 그러나, 메일 로그를 사용하여 특정 메시지의 전달을 추적할 수 있으므로 메시지에서 수행한 작업을 통해 메일에 부적절하거나 의심스러운 이미지가 포함되었는지를 판단할 수 있습니다.

예를 들어, 다음 메일 로그는 이미지 분석 검사 결과로 메시지 필터 규칙을 통해 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 결과에 기반하여 작업을 수행하도록 메시지 필터 구성

이미지 분석을 활성화하면 다양한 메시지 판정을 위해 다양한 작업을 수행하도록 메시지 필터를 생성해야 합니다. 예를 들어, 정상 판정을 받은 메시지는 전달하지만 부적절한 콘텐츠를 포함하고 있다고 판단된 메시지는 격리할 수 있습니다.

참고 부적절하거나 의심스러운 판정을 받은 메시지를 삭제하거나 바운스하지 않는 것이 좋습니다. 대신, 나중에 트렌드 분석을 검토하고 이에 대해 잘 이해할 수 있도록 위반사항의 복사본을 격리에 전송합니다.

다음 필터는 콘텐츠가 부적절하거나 의심스러운 경우 태그가 지정된 메시지를 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 판정에 기반하여 첨부 파일을 제거하도록 콘텐츠 필터 생성, 9-82페이지

이미지 분석 판정에 기반하여 첨부 파일을 제거하도록 콘텐츠 필터 생성

이미지 분석을 활성화한 후, 이미지 분석 판정에 기반하여 첨부 파일을 제거하도록 콘텐츠 필터를 생성하거나 다양한 메시지 판정에 대해 다양한 작업을 수행하도록 필터를 구성할 수 있습니다. 예를 들어, 부적절한 콘텐츠가 포함된 메시지를 격리하도록 결정할 수 있습니다.

이미지 분석 판정에 기반하여 첨부 파일을 제거하려면 다음을 수행합니다.

절차

1단계 Mail Policies(메일 정책) > Incoming Content Filter(수신 콘텐츠 필터)를 클릭합니다.

2단계 Add Filter(필터 추가)를 클릭합니다.

3단계 콘텐츠 필터의 이름을 입력합니다.

4단계 Action(작업)에서 **Add Action(작업 추가)**을 클릭합니다.

5단계 Strip Attachment by File Info(파일 정보별 첨부 파일 제거)에서 **Image Analysis Verdict is(이미지 분석 판정 결과)**를 클릭합니다.

6단계 다음 이미지 분석 판정 중에서 선택합니다.

- Suspect
- 부적절함
- 의심 또는 부적절함
- 검색할 수 없음
- 삭제

이미지 분석 판정에 기반하여 작업을 구성하려면 다음을 수행하십시오.

절차

1단계 Mail Policies(메일 정책) > Incoming Content Filter(수신 콘텐츠 필터)를 클릭합니다.

2단계 Add Filter(필터 추가)를 클릭합니다.

3단계 콘텐츠 필터의 이름을 입력합니다.

4단계 Conditions(조건) 아래에서 **Add Condition(조건 추가)**을 클릭합니다.

5단계 Attachment File Info(첨부 파일 정보) 아래에서 **Image Analysis Verdict(이미지 분석 판정)**를 클릭합니다.

6단계 다음 판정 중 하나를 선택합니다.

- 의심
- 부적절함
- 의심 또는 부적절함
- 검색할 수 없음
- 정상

7단계 **Add Action(작업 추가)**을 클릭합니다.

8단계 이미지 분석 판정에 따라 메시지에서 수행할 작업을 선택합니다.

9단계 변경사항을 제출하고 커밋합니다.

알림

사용자 지정 알림 템플릿을 텍스트 리소스로 구성하기 위해 GUI의 Text Resources(텍스트 리소스) 페이지 또는 `textconfig` CLI 명령을 사용하면 첨부 파일 필터링 규칙과 함께 사용할 경우 유용하게 사용할 수 있습니다. 알림 템플릿은 비ASCII 문자를 지원합니다(템플릿을 생성할 때 인코딩을 선택하도록 프롬프트 표시).

다음 예에서 `textconfig` 명령은 알림 메시지의 본문에 삽입될 `strip.mp3`라는 알림 템플릿을 생성하기 위해 처음으로 사용되었습니다. 그런 다음 첨부 파일 필터링 규칙이 생성되어 .mp3 파일이 메시지에서 제거되었을 때 .mp3 파일이 삭제되었음을 알리는 알림 이메일이 원하는 수신자에게 전송됩니다.

```
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 복사본 알림 작업, 9-59페이지 항목을 참조하십시오.

첨부 파일 검사 메시지 필터 예

다음 예는 첨부 파일에서 수행된 작업을 보여줍니다.

- 헤더 삽입, 9-83페이지
- 파일 유형별로 첨부 파일 삭제, 9-84페이지
- 사전 일치별로 첨부 파일 삭제, 9-85페이지
- 보호된 첨부 파일 격리, 9-86페이지
- 보호되지 않는 첨부 파일 탐지, 9-86페이지

헤더 삽입

이 예에서 AsyncOS는 첨부 파일에 지정된 콘텐츠가 포함된 경우 헤더를 삽입합니다.

다음 예에서는 메시지의 모든 첨부 파일에서 키워드가 검사됩니다. 키워드가 모든 첨부 파일에 존재하는 경우 사용자 지정 X-헤더가 삽입됩니다.

```
attach_disclaim:

    if (every-attachment-contains('[dD]isclaimer') ) {
```

```
        insert-header("X-Example-Approval", "AttachOK");

    }
```

다음 예에서 첨부 파일은 이진 데이터의 패턴에 대해 검사됩니다. 필터는 `attachment-binary-contains` 필터 규칙을 사용하여 PDF 문서가 암호화되었음을 알리는 패턴을 검색합니다. 패턴이 이진 데이터로 존재하는 경우 사용자 지정 헤더가 삽입됩니다.

```
match_PDF_Encrypt:

if (attachment-filetype == 'pdf' AND

attachment-binary-contains('/Encrypt')){

strip-header ('Subject');

insert-header ('Subject', '[Encrypted] $Subject');

}
```

파일 유형별로 첨부 파일 삭제

다음 예에서 첨부 파일의 "실행 파일" 그룹(`.exe`, `.dll` 및 `.scr`)이 메시지에서 제거되고 텍스트가 메시지에 추가되었습니다. 이때 `$dropped_filename` 작업 변수를 통해 삭제된 파일의 파일 이름이 나열됩니다. `drop-attachments-by-filetype` 작업은 3글자의 파일 이름 확장명뿐만 아니라 파일의 지문에 기반하여 첨부 파일을 검사하고 제거합니다. 또한 단일 파일 유형("mpeg")을 지정하거나 파일 유형("Media")의 모든 멤버를 참조할 수 있습니다.

```
strip_all_exes: if (true) {

                    drop-attachments-by-filetype ('Executable', "Removed attachment:
$dropped_filename");

                }
```

다음 예에서 첨부 파일의 동일한 "실행 파일" 그룹(`.exe`, `.dll` 및 `.scr`)이 봉투 발신자가 `example.com` 도메인에 속하지 않은 메시지에서 제거되었습니다.

```
strip_inbound_exes: if (mail-from != "@example\\.com$") {

                        drop-attachments-by-filetype ('Executable');

                    }
```

다음 예에서 첨부 파일의 동일한 "실행 파일" 그룹(`.exe`, `.dll` 및 `.scr`)과 파일 유형("wmf")의 특정 멤버가 봉투 발신자가 `example.com` 도메인에 속하지 않은 메시지에서 제거되었습니다.

```
strip_inbound_exes_and_wmf: if (mail-from != "@example\\.com$") {

                        drop-attachments-by-filetype ('Executable');
```

```
                    drop-attachments-by-filetype ('x-wmf');

                }
```

다음 예에서 첨부 파일의 사전 정의된 "실행 파일" 그룹이 더 많은 첨부 파일 이름을 포함하도록 확장되었습니다. (이 작업은 첨부 파일의 파일 유형을 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 비ASCII 문자를 지원합니다.

참고 drop-attachments-by-name 작업은 MIME 헤더에서 캡처한 파일 이름과 정규식의 일치 여부를 확인합니다. MIME 헤더에서 캡처한 파일 이름은 후행 공백을 포함할 수 있습니다.

다음 예에서 첨부 파일이 .exe 실행 파일 유형이 아닌 경우 메시지가 삭제됩니다. 그러나 필터링할 파일 유형의 첨부 파일이 1개 이상이 있는 경우 필터는 메시지에 아무 작업도 수행하지 않습니다. 예를 들어, 다음 필터는 *.exe* 파일이 아닌 첨부 파일의 모든 메시지를 삭제합니다.

```
exe_check: if (attachment-filetype != "exe") {

                drop();

            }
```

메시지에 첨부 파일이 여러 개 있는 경우, Email Security 어플라이언스는 다른 첨부 파일이 .exe 파일이 아니어도 첨부 파일 하나 이상이 .exe 파일인 경우 메시지를 삭제하지 않습니다.

사전 일치별로 첨부 파일 삭제

drop-attachments-where-dictionary-match 작업은 사전 용어와 일치하는 항목에 따라 첨부 파일을 제거합니다. 첨부 파일로 간주되는 MIME 부분의 용어가 사전 용어와 일치하는 경우(또한 사용자 정의 임계값을 만족하는 경우) 첨부 파일이 이메일에서 제거됩니다. 다음 예는 "secret_words" 사전의 단어가 첨부 파일에서 탐지되는 경우 첨부 파일 삭제를 보여줍니다. 일치에 대한 임계값이 1로 설정됩니다.

```
Data_Loss_Prevention: if (true) {

drop-attachments-where-dictionary-match("secret_words", 1);

}
```

보호된 첨부 파일 격리

attachment-protected 필터는 메시지의 모든 첨부 파일이 비밀번호로 암호화되었는지를 테스트합니다. 수신 메일에서 이 필터를 사용하여 첨부 파일이 검사 가능한지 확인할 수 있습니다. 이 정의에 따르면 암호화되지 않은 여러 멤버와 하나의 암호화된 멤버를 포함하는 zip 파일은 보호되는 것으로 간주됩니다. 마찬가지로, 공개 비밀번호가 없는 PDF 파일은 비밀번호가 있는 복사 또는 인쇄로 제한하는 경우에도 보호되는 것으로 간주되지 않습니다. 다음의 예는 정책 격리에 전송된 보호되는 첨부 파일을 보여줍니다.

```
quarantine_protected:

if attachment-protected

{

quarantine("Policy");

}
```

보호되지 않는 첨부 파일 탐지

attachment-unprotected 필터는 메시지의 모든 첨부 파일이 비밀번호로 암호화되지 *않았는지*를 테스트합니다. 이 메시지 필터는 attachment-protected 필터를 보완합니다. 발송 메일에서 이 필터를 사용하여 보호되지 않은 발송 메일을 탐지할 수 있습니다. 다음의 예는 AsyncOS가 발송 리스너에서 보호되지 않는 첨부 파일을 탐지하고 메시지를 격리하는 것을 보여줍니다.

```
quarantine_unprotected:

if attachment-unprotected

{

quarantine("Policy");

}
```

CLI를 사용하여 메시지 필터 관리

CLI를 사용하여 메시지 필터에 대한 로깅 옵션을 추가, 삭제, 활성화 및 비활성화, 가져오기 및 내보내기, 설정할 수 있습니다. 아래 표에는 명령 및 하위 명령이 요약되어 있습니다. 아래 표에는 명령 및 하위 명령이 요약되어 있습니다.

표 9-9 메시지 필터 하위 명령

구문	설명
필터	주요 명령입니다. 이 명령은 대화형으로 이루어지며 자세한 정보를 묻습니다(예: new, delete, import).
new	새 필터를 생성합니다. 위치가 지정되지 않은 경우, 현재 시퀀스에 추가됩니다. 그 밖의 경우 필터는 시퀀스 상 특정한 위치에 삽입됩니다. 자세한 내용은 새 메시지 필터 생성, 9-88페이지 항목을 참조하십시오.

표 9-9 메시지 필터 하위 명령 (계속)

구문	설명
delete	이름 또는 시퀀스 번호별로 필터를 삭제합니다. 자세한 내용은 메시지 필터 삭제, 9-88페이지 항목을 참조하십시오.
move	기존 필터를 다시 정렬합니다. 자세한 내용은 메시지 필터 이동, 9-88페이지 항목을 참조하십시오.
set	필터를 활성 또는 비활성 상태로 설정합니다. 자세한 내용은 메시지 필터 활성화 및 비활성화, 9-89페이지 항목을 참조하십시오.
import	현재 필터 집합을 파일에 저장된 새로운 집합으로 대체합니다(어플라이언스의 /configuration 디렉토리). 자세한 내용은 메시지 필터 가져오기, 9-92페이지 항목을 참조하십시오.
export	현재 필터 집합을 파일로 내보냅니다(어플라이언스의 /configuration 디렉토리). 자세한 내용은 메시지 필터 내보내기, 9-93페이지 항목을 참조하십시오.
이름을	필터 정보를 나열합니다. 자세한 내용은 메시지 필터 목록 표시, 9-93페이지 항목을 참조하십시오.
detail	필터 규칙 자체의 본문을 포함하여 특정 필터에 대한 자세한 정보를 출력합니다. 자세한 내용은 메시지 필터 세부 사항 표시, 9-94페이지 항목을 참조하십시오.
logconfig	필터의 logconfig 하위 메뉴를 입력하면 `archive()` 필터 작업에서 로그 서브스크립션을 편집할 수 있습니다. 자세한 내용은 필터 로그 서브스크립션 구성, 9-94페이지 항목을 참조하십시오.

참고 필터를 적용하려면 `commit` 명령을 실행해야 합니다.

다음 3가지 유형의 매개변수가 있습니다.

표 9-10 필터 관리 매개변수

seqnum	필터 목록에서의 위치에 따라 필터를 나타내는 정수입니다. 예를 들어 *seqnum*이 `2`인 경우 목록에서 두 번째 필터임을 나타냅니다.
filtname	필터의 구어 이름입니다.
range	범위는 1개 이상의 필터를 나타내는 데 사용될 수 있으며 *X-Y* 양식으로 나타나며 이때 X 및 Y는 범위를 식별하는 첫 번째 및 마지막 *seqnums*입니다. 예를 들어, `2-4`는 두 번째, 세 번째, 네 번째 위치의 필터를 나타냅니다. X 또는 Y는 무한 목록을 나타내기 위해 제외될 수 있습니다. 예를 들어, `-4`는 처음 4개의 필터를 나타내며 `2-`는 첫 번째를 제외한 모든 필터를 나타냅니다. 또한 필터 목록의 모든 필터를 나타내기 위해 `all` 키워드를 사용할 수 있습니다.

관련 주제

- 새 메시지 필터 생성, 9-88페이지
- 메시지 필터 삭제, 9-88페이지
- 메시지 필터 이동, 9-88페이지
- 메시지 필터 활성화 및 비활성화, 9-89페이지
- 메시지 필터 가져오기, 9-92페이지
- 메시지 필터 내보내기, 9-93페이지

새 메시지 필터 생성

```
new [seqnum|filtname|last]
```

새 필터를 삽입할 위치를 지정합니다. 키워드 `last`를 생략하거나 지정한 경우, 입력한 필터가 필터 목록에 추가됩니다. 시퀀스 번호에는 간격이 허용되지 않으며 현재 목록의 경계 외부에서 *seqnum*을 입력할 수 없습니다. 알 수 없는 *filtname*을 입력한 경우 프롬프트가 표시되어 유효한 *filtname*, *seqnum* 또는 `last`를 입력할 수 있습니다.

필터를 입력한 후, 수동으로 필터 스크립트를 입력할 수 있습니다. 입력을 완료하려는 경우 줄에 마침표(.)를 입력하여 입력을 종료합니다.

다음 조건에서 오류가 발생할 수 있습니다.

- 시퀀스 번호가 시퀀스 번호의 현재 범위를 초과하는 경우.
- 고유하지 않은 *filtname*을 가진 필터.
- 예약어인 *filtname*을 가진 필터.
- 구문 오류가 있는 필터.
- 인터페이스 등 존재하지 않는 시스템 리소스를 참조하는 작업이 있는 필터.

메시지 필터 삭제

```
delete [seqnum|filtname|range]
```

식별한 필터를 삭제합니다.

다음 조건에서 오류가 발생할 수 있습니다.

- 지정된 필터 이름의 필터가 없는 경우.
- 지정된 시퀀스 번호의 필터가 없는 경우.

메시지 필터 이동

```
move [seqnum|filtname|range seqnum|last]
```

첫 번째 매개변수에서 식별한 필터를 두 번째 매개변수에서 식별한 위치로 이동합니다. 두 번째 매개변수가 `last` 키워드인 경우, 필터는 필터 목록의 끝으로 이동합니다. 하나 이상의 필터가 이동 중이면 다른 필터의 순서는 그대로 유지됩니다.

다음 조건에서 오류가 발생할 수 있습니다.

- 지정된 필터 이름의 필터가 없는 경우.
- 지정된 시퀀스 번호의 필터가 없는 경우.

- 시퀀스 번호가 시퀀스 번호의 현재 범위를 초과하는 경우.
- 이동으로 인해 시퀀스가 변경되지 않는 경우.

메시지 필터 활성화 및 비활성화

지정된 메시지 필터는 *active* 또는 *inactive* 중 하나이며 *valid* 또는 *invalid*도 가능합니다. 메시지 필터가 *active* 및 *valid* 모두에 해당하는 경우 처리를 위해서만 사용됩니다. CLI를 통해 기존 필터를 활성에서 비활성(및 다시 비활성에서 활성으로) 상태로 변경합니다. 필터가 존재하지 않거나 제거된 인터페이스 또는 리스너를 참조하는 경우 유효하지 않습니다.

참고 필터가 구문을 사용하여 비활성화되었는지 여부를 판별할 수 있습니다. AsyncOS는 필터 이름 뒤에 있는 콜론을 비활성 필터의 느낌표로 변경합니다. 필터를 입력하거나 가져올 때 이 구문을 사용하는 경우 AsyncOS는 비활성 상태로 필터를 표시합니다.

예를 들어, 다음의 안전한 필터 이름인 "filterstatus"가 입력됩니다. 그런 다음 `filter -> set` 하위 명령을 사용하여 비활성화됩니다. 필터에 대한 세부 사항이 표시되는 경우 콜론이 느낌표(및 다음 예에서 볼드체)로 변경됩니다.

```
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 및 비활성화, 9-92페이지

메시지 필터 활성화 및 비활성화

```
set [seqnum|filtname|range] active|inactive
```

식별된 필터가 지정된 상태가 되도록 설정합니다. 정상적인 상태는 다음과 같습니다.

- 활성: 선택한 필터의 상태를 활성으로 설정합니다.
- 비활성: 선택한 필터의 상태를 비활성으로 설정합니다.

다음 조건에서 오류가 발생할 수 있습니다.

- 지정된 *filtname*의 필터가 없는 경우.
- 지정된 시퀀스 번호의 필터가 없는 경우.

참고 비활성 상태인 필터가 구문에서 언급되었으며 레이블(필터 이름) 뒤의 콜론이 느낌표(!)로 변경됩니다. 이 구문을 포함하는 CLI에서 수동으로 입력되었거나 가져온 필터는 자동으로 비활성화로 표시됩니다. 예를 들어, `mailfrompm!`이 `mailfrompm:` 대신 표시됩니다.

메시지 필터 가져오기

```
import filename
```

필터를 포함하는 파일 이름이 처리됩니다. 이 파일은 `interfaceconfig` 명령을 사용하여 인터페이스에 대한 FTP/SCP 액세스를 활성화한 경우 어플라이언스의 FTP/SCP 루트 디렉토리의 구성 디렉토리에 있어야 합니다. 이 파일은 수집 및 분석되며 오류는 보고됩니다. 가져온 필터는 현재 필터 집합에 존재하는 모든 필터를 대체합니다. 자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스" 항목을 참조하십시오. 현재 필터 목록을 내보낸 후(메시지 필터 내보내기, 9-93페이지 참조) 가져오기 전에 파일을 편집할 수 있습니다.

메시지 필터를 가져올 때 프롬프트가 표시되어 사용된 인코딩을 선택할 수 있습니다.

다음 조건에서 오류가 발생할 수 있습니다.

- 파일이 없습니다.
- 고유하지 않은 필터 이름을 가진 필터.
- 예약어인 *filtname*을 가진 필터.
- 구문 오류가 있는 필터.
- 인터페이스 등 존재하지 않는 시스템 리소스를 참조하는 작업이 있는 필터.

메시지 필터 내보내기

```
export filename [seqnum|filtname|range]
```

어플라이언스에서 FTP/SCP 루트 디렉토리의 구성 디렉토리에 있는 파일로 설정된 기존 필터 집합의 형식화된 버전을 출력합니다. 자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스" 항목을 참조하십시오.

메시지 필터를 내보낼 때 프롬프트가 표시되어 사용된 인코딩을 선택할 수 있습니다.

다음 조건에서 오류가 발생할 수 있습니다.

- 지정된 필터 이름의 필터가 없는 경우.
- 지정된 시퀀스 번호의 필터가 없는 경우.

비ASCII 문자 집합 보기

CLI에서 UTF-8을 사용하는 비ASCII 문자를 포함하는 필터가 표시됩니다. 터미널/표시 기능이 UTF-8을 지원하지 않는 경우, 필터를 읽을 수 없습니다.

필터의 비ASCII 문자를 관리하는 가장 좋은 방법은 텍스트 파일에서 필터를 편집한 다음 해당 텍스트 파일을 어플라이언스로 가져오는 것입니다(메시지 필터 가져오기, 9-92페이지 참조).

메시지 필터 목록 표시

```
list [seqnum|filtname|range]
```

필터 본문을 출력하기 전에 표 형식으로 식별된 필터에 대한 요약 정보를 보여줍니다. 표시되는 정보는 다음과 같습니다.

- 필터 이름
- 필터 시퀀스 번호
- 필터의 활성/비활성 상태
- 필터의 유효한/유효하지 않은 상태

다음 조건에서 오류가 발생할 수 있습니다.

- 불법적인 범위 형식.

메시지 필터 세부 사항 표시

```
detail [seqnum|filtname|range]
```

필터 본문 및 모든 추가 상태 정보를 비롯해 식별된 필터에 대한 전체 정보를 제공합니다.

필터 로그 서브스크립션 구성

```
logconfig
```

하위 메뉴를 입력하여 `archive()` 작업을 통해 생성된 메일함 파일의 필터 로그 옵션을 구성할 수 있습니다. 이 옵션은 일반적인 `logconfig` 명령에서 사용하는 옵션과 매우 유사하지만 로그는 이 옵션을 참조하는 필터를 추가하거나 제거하여 생성 또는 삭제만 가능합니다.

각 필터 로그 서브스크립션에는 다음의 기본값이 있으며 이 값은 `logconfig` 하위 명령을 사용하여 수정할 수 있습니다.

- 검색 방법 - FTP 설문 조사
- 파일 크기 - 10MB
- 최대 파일 수 - 10개

자세한 내용은 "로깅" 장을 참조하십시오.

```
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

localeconfig 명령을 사용하여 메시지 처리 중에 메시지 머리글 및 바닥글의 인코딩 수정에 관한 AsyncOS의 동작을 설정할 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: Only try encoding from

message body


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]>
```

```
Footers or headings are added in-line with the message body whenever
possible. However, if the footer or heading 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 footer or
heading. If that fails, and if the message body's encoding is US-
ASCII, the system can try to edit the message body to use the footer's
or heading's encoding. Should the system try to impose the footer's
or headings's encoding on the message body? [N]> y


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


Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
```

첫 번째 프롬프트는 헤더가 변경된 경우(예: 필터를 통해) 메시지 본문의 인코딩과 일치하도록 메시지 헤더의 인코딩을 변경해야 하는지를 판단합니다.

두 번째 프롬프트는 헤더가 문자 집합을 사용하여 제대로 태그 지정되지 않는 경우 어플라이언스가 헤더에 메시지 본문 인코딩을 적용해야 하는지 여부를 제어합니다.

세 번째 프롬프트는 메시지 본문의 고지 사항 스탬프(및 여러 인코딩)가 작동하는 방식을 구성하는 데 사용됩니다. 자세한 내용은 "텍스트 리소스" 장의 "고지 사항 스탬프 및 여러 인코딩"을 참조하십시오.

메시지 필터 샘플

다음 예에서 `filter` 명령을 사용하여 새로운 필터 3가지를 생성합니다.

- 첫 번째 필터의 이름은 **`big_messages`**입니다. 이 필터에서는 `body-size` 규칙을 사용하여 10MB보다 큰 메시지를 삭제합니다.
- 두 번째 필터의 이름은 **`no_mp3s`**입니다. 이 필터에서는 `attachment-filename` 규칙을 사용하여 파일 확장명이 `.mp3`인 첨부 파일을 포함하는 메시지를 삭제합니다.

- 세 번째 필터의 이름은 **mailfrompm**입니다. 이 필터에서는 mail-from 규칙을 사용하여 postmaster@example.com의 모든 메일을 검사하고 administrator@example.com으로 BCC(숨은 참조)합니다.

filter -> list 하위 명령을 사용하면 필터가 활성 상태이며 유효한지 확인하기 위해 나열된 다음 move 하위 명령을 사용하여 첫 번째 및 마지막 필터의 위치가 전환됩니다. 마지막으로, 변경사항이 커밋되어 필터가 적용됩니다.

```
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, 9-104페이지
- 정책 시행 필터, 9-104페이지
- 라우팅 및 도메인 스푸핑, 9-108페이지

오픈 릴레이 방지 필터

이 필터는 이메일 주소에 `%`, 추가 `@` 및 `!` 문자를 사용하는 주소가 있는 메시지를 바운스합니다.

- `user%otherdomain@validdomain`
- `user@otherdomain@validdomain:`
- `domain!user@validdomain`

```
sourceRouted:

if (rcpt-to == "(%|@|!)(.*)@") {

  bounce();

}
```

Cisco 어플라이언스는 기존 Sendmail/Qmail 시스템을 활용하기 위해 사용된 타사 릴레이 해킹에 취약하지 않습니다. 이러한 대부분의 기호(예 `%`)는 완전하게 정상적인 이메일 주소에 사용될 수 있기 때문에 Cisco 어플라이언스는 이러한 기호를 유효한 주소로 승인하고 구성된 수신자 목록을 대상으로 확인하며 다음의 내부 서버로 전달합니다. Cisco 어플라이언스는 이러한 메시지를 완전히 릴레이하지 않습니다.

이러한 필터는 해당 유형의 메시지 릴레이가 가능하도록 잘못 구성된 오픈 소스 MTA를 사용할 수 있는 사용자를 보호하기 위해 실행됩니다.

참고 또한 리스너에서 이러한 유형의 주소를 처리하도록 구성할 수 있습니다. 자세한 내용은 GUI를 통해 리스너를 생성하여 연결 요청 수신 대기, 5-6페이지 항목을 참조하십시오.

정책 시행 필터

- 제목 필터에 기반한 알림, 9-105페이지
- 경쟁업체에 전송된 메일 BCC 및 검사, 9-105페이지
- 특정한 사용자 차단 필터, 9-105페이지

제목 필터에 기반한 알림

이 필터는 제목에 특정한 단어가 포함되는지 여부에 기반하여 알림을 전송합니다.

```
search_for_sensitive_content:

if (Subject == "(?i)plaintiff|lawsuit|judge" ) {

    notify ("admin@company.com");

}
```

경쟁업체에 전송된 메일 BCC 및 검사

이 필터는 경쟁업체에 전송된 메시지를 검사하고 숨은 참조를 보냅니다. 사전과 header-dictionary-match() 규칙을 사용하여 더 유연한 방식으로 경쟁업체 목록을 지정할 수 있습니다(사전 규칙, 9-34페이지 참조).

```
competitorFilter:

if (rcpt-to == '@competitor1.com|@competitor2.com') {

    bcc-scan('legal@example.com');

}
```

특정한 사용자 차단 필터

이 필터를 사용하여 특정 주소에서 오는 이메일을 차단합니다.

```
block_harrasing_user:

if (mail-from == "ex-employee@hotmail\\.com") {

    notify ("admin@company.com");

    drop ();

}
```

메시지 아카이브 및 삭제 필터

일치하는 파일 유형이 있는 메시지만 로깅하고 삭제할 수 있습니다.

```
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: $MID");
drop-attachments-by-name("\\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$");

}
```

대형 "To:" 헤더 필터

매우 큰 "To" 헤더가 있는 메시지를 찾습니다.

`archive()`를 사용하여 추가적인 보안을 위해 drop()을 활성화 또는 비활성화하여 올바른 작업을 확인할 수 있습니다.

```
toTooBig:

if(header('To') == "^.{500,}") {

   archive('tooTooBigdropped');

   drop();

}
```

비어 있는 "From:" 필터

비어 있는 "From" 헤더를 식별합니다.

이 필터는 다양한 형태의 비어 있는 "From" 주소를 줄일 수 있습니다.

```
blank_mail_from_stop:

if (recv-listener == "InboundMail" AND header("From") == "^$|<\\s*>") {

  drop ();

}
```

또한 이 필터를 사용하여 비어 있는 Envelope From이 있는 메시지를 삭제할 수 있습니다.

```
blank_mail_from_stop:

if (recv-listener == "InboundMail" AND (mail-from == "^$|<\\s*>" OR header ("From") ==
"^$|<\\s*>"))

{

  drop ();

}
```

SRBS 필터

SenderBase 평판 필터:

```
note_bad_reps:

if (reputation < -2)  {

  strip-header ('Subject');

  insert-header ('Subject', '***BadRep $Reputation *** $Subject');

}
```

SRBS 변경 필터

특정 도메인에 대한 SBRS(SenderBase Reputation 점수) 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 검색합니다 ("readme.zip", "readme.exe", "attach.exe" 등의 파일 이름과 일치함).

```
filename_filter:

if ((body-size >= 9k) AND (body-size <= 20k)) {

   if (body-contains ("(?i)(readme|attach|information)\\.(zip|exe)$")) {

      drop ();
```

```
    }
}
```

헤더에서 SenderBase Reputation 점수 표시 필터

이 필터를 사용하여 헤더를 로깅하면("로깅" 장 참조) 메일 로그에 표시됩니다.

```
Check_SBRS:
if (true) {
  insert-header('X-SBRS', '$Reputation');
}
```

헤더에 정책 삽입 필터

어떤 메일 흐름 정책이 연결을 수락했는지 표시합니다.

```
Policy_Tracker:
if (true) {
  insert-header ('X-HAT', 'Sender Group $Group, Policy $Policy applied.');
}
```

너무 많은 수신자 바운스 필터

2개 이상의 고유한 도메인에서 50명 이상의 수신자가 있는 모든 아웃바운드 이메일 메시지를 바운스합니다.

```
bounce_high_rcpt_count:
if ( (rcpt-count > 49) AND (rcpt-to != "@example\\.com$") ) {
  bounce-profile ("too_many_rcpt_bounce"); bounce ();
}
```

라우팅 및 도메인 스푸핑

- 다른 스푸핑된 도메인 삭제 필터, 9-110페이지
- 루핑 탐지 필터, 9-111페이지

가상 게이트웨이 사용 필터

가상 게이트웨이를 사용하는 트래픽을 분할합니다. 시스템에 'public1'과 'public2'라는 2개의 인터페이스가 있으며 기본 전송 인터페이스가 'public1'인 경우, 두 번째 인터페이스를 통해 아웃바운드 트래픽을 모두 적용하게 되는데 바운스 및 기타 유사한 유형의 메일이 필터를 통과하지 않으므로 public1에서 전송됩니다.

```
virtual_gateways:

if (recv-listener == "OutboundMail") {

    alt-src-host ("public2");

}
```

전달을 위한 동일한 리스너 및 리스너 필터

전달 및 수신을 위해 동일한 리스너를 사용합니다. 이 필터를 사용하면 공용 리스너인 "listener1"에서 수신한 모든 메시지를 인터페이스 "listener1"을 통해 외부로 전송할 수 있습니다(구성된 각 공용 리스너에 대해 고유한 필터를 설정해야 할 수 있음).

```
same_listener:

if (recv-inj == 'listener1') {

  alt-src-host('listener1');

}
```

단일 리스너 필터

단일 리스너에서 필터를 동작시킵니다. 예를 들어, 시스템 전체에서 수행되는 대신 메시지 필터 처리를 위해 특정한 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 도메인이 있는 이메일을 삭제합니다(내부 주소에서 오는 것처럼 가장하고 단일 리스너로 동작함). 아래 IP 주소는 mycompany.com에 대한 가상 도메인을 나타냅니다.

```
DomainSpoofed:

if (mail-from == "mycompany\\.com$") {

  if ((remote-ip != "1.2.") AND (remote-ip != "3.4.")) {

    drop();

  }

}
```

스푸핑된 도메인 삭제 필터(여러 리스너)

위의 필터와 동일하지만 여러 리스너에서 작동합니다.

```
domain_spoof:

if ((recv-listener == "Inbound") and (mail-from == "@mycompany\\.com")) {

archive('domain_spoof');

drop ();

}
```

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");

}
```

루핑 탐지 필터

이 필터는 메일 루프를 유발하는 원인을 탐지, 중지 및 판단하는 데 사용됩니다. 이 필터는 Exchange 서버 또는 기타 서버에서 구성 문제를 판단하는 데 유용합니다.

```
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 100개의 루프 후에 메시지를 삭제합니다.

검사 동작 구성

본문 및 첨부 파일 검사 동작을 제어할 수 있습니다. 예를 들어 검사 매개변수를 구성하여 검사하는 동안 건너뛸 첨부 파일 유형 등을 지정합니다. Scan Behavior(검사 동작) 페이지 또는 `scanconfig` 명령을 사용하여 이 매개변수를 구성합니다. 검사 동작 설정은 전역 설정이므로 모든 검사 동작에 영향을 줄 수 있습니다.

참고 zip 또는 압축 파일에 포함된 MIME 유형을 검사하려는 경우, 검사 목록에 'compressed' 또는 'zip' 또는 'application/zip' 목록을 포함해야 합니다.

절차

1단계 **Security Services(보안 서비스) > Scan Behavior(검사 동작)**를 클릭합니다.

2단계 첨부 파일 유형 매핑을 정의합니다. 다음 중 하나를 수행합니다.

- 새 첨부 파일 유형 매핑을 추가합니다. **Add Mapping(매핑 추가)**을 클릭합니다.
- 구성 파일을 사용하여 첨부 파일 유형 매핑 목록을 가져옵니다. **Import List(목록 가져오기)**를 클릭하고 구성 디렉토리에서 원하는 구성 파일을 가져옵니다.

  참고 이 단계를 수행하려면 구성 파일이 어플라이언스의 구성 디렉토리에 있어야 합니다. 구성 파일 관리, 33-7페이지 항목을 참조하십시오.

- **Edit(편집)**을 클릭하여 기존의 첨부 파일 유형 매핑을 수정합니다.

3단계 전역 설정을 구성합니다. 다음을 수행합니다.

a. Global Settings(전역 설정)에서, **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

b. 원하는 필드를 수정합니다.

표 9-11

필드	설명
위 표에서 MIME 유형/지문이 있는 첨부 파일에 대한 작업	첨부 파일 유형 매핑에 정의된 첨부 파일 유형을 검사할지 또는 건너뛸지를 선택합니다.
검사할 최대 첨부 파일 반복 횟수	검사할 첨부 파일의 최대 반복 횟수를 지정합니다.
검사할 최대 첨부 파일 크기	검사할 첨부 파일의 최대 크기를 지정합니다.
첨부 파일 메타데이터 검사	첨부 파일의 메타데이터를 검사할지 또는 건너뛸지를 지정합니다.
첨부 파일 검사 시간제한	검사 시간제한을 지정합니다.
어떤 이유로든 검사되지 않은 경우 첨부 파일이 패턴과 일치하는 것으로 가정	패턴을 검색하기 위해 검사되지 않은 첨부 파일을 일치하는 것으로 판단할지 여부를 지정합니다.
메시지를 분해하여 지정된 첨부 파일을 제거할 수 없는 경우의 작업	메시지를 분해하여 지정된 첨부 파일을 제거할 수 없을 때 수행할 작업을 지정합니다.
콘텐츠 또는 메시지 필터 오류가 발생할 경우 모든 필터 우회	콘텐츠 또는 메시지 필터 오류가 발생할 경우 모든 필터를 우회할지 여부를 지정합니다.

표 9-11

필드	설명
지정된 인코딩이 없는 경우 사용할 인코딩	인코딩이 지정되지 않은 경우 사용할 인코딩을 지정합니다.
불투명하게 서명된 메시지를 명확하게 서명된 메시지로 변환(S/MIME 압축 해제)	불투명하게 서명된 메시지를 명확하게 서명된 메시지로 변환할지 여부를 지정합니다(S/MIME 압축 해제).

c. **Submit(제출)**을 클릭합니다.

4단계 **Commit Changes(변경사항 커밋)**를 클릭합니다.

관련 주제

- CLI를 사용하여 검사 매개변수 수정, 9-113페이지

CLI를 사용하여 검사 매개변수 수정

`scanconfig` 명령을 사용하여 본문 및 첨부 파일 검사 동작을 구성할 수 있습니다. 다음 예에서 `scanconfig` 명령은 다음 매개변수를 설정합니다.

- `video/*`, `audio/*`, `image/*`의 MIME 유형은 콘텐츠가 검사되지 않습니다.
- 중첩된(반복적인) 아카이브 첨부 파일은 최대 50개까지 검사됩니다.
- 검사할 첨부 파일의 최대 크기는 25MB로, 이보다 큰 파일은 건너뜁니다. (기본값은 5MB입니다.)
- 첨부 파일은 메타데이터 검사가 활성화되어 있습니다. 검사 엔진에서 첨부 파일을 검사할 때 정규식에 대한 메타데이터를 검사합니다. 이는 기본 설정입니다.
- 첨부 파일의 검사 시간제한은 60초로 구성되어 있습니다. 기본값은 30초입니다.
- 검사되지 않은 첨부 파일은 검색 패턴과 일치하지 않는 것으로 가정됩니다. (이것은 기본 동작입니다.)
- 메시지의 `application/(x-)pkcs7-mime`(불투명하게 서명) 부분은 `multipart/signed`(명확하게 서명)로 변환되어 처리를 위한 메시지 콘텐츠를 제공합니다. 기본값은 불투명하게 서명된 메시지로 변환하지 않는 것입니다.

참고 `assume the attachment matches the search pattern`을 Y로 설정하면 검사할 수 없는 메시지로 인해 메시지 필터 규칙이 true로 평가합니다. 이로 인해 사전과 일치하지 않는 메시지 격리와 같이 예기치 않은 동작이 발생하게 되지만 콘텐츠를 올바르게 검사할 수 없기 때문에 격리됩니다.

```
mail3.example.com> scanconfig


There are currently 5 attachment type mappings configured to be SKIPPED.


Choose the operation you want to perform:

- NEW - Add a new entry.
```

```
- DELETE - Remove an entry.

- SETUP - Configure scanning behavior.

- IMPORT - Load mappings from a file.

- EXPORT - Save mappings to a file.

- PRINT - Display the list.

- CLEAR - Remove all entries.

- SMIME - Configure S/MIME unpacking.

[]> setup


1. Scan only attachments with MIME types or fingerprints in the list.

2. Skip attachments with MIME types or fingerprints in the list.

Choose one:

[2]> 2


Enter the maximum depth of attachment recursion to scan:

[5]> 10


Enter the maximum size of attachment to scan:

[5242880]> 10m


Do you want to scan attachment metadata? [Y]> Y


Enter the attachment scanning timeout (in seconds):

[30]> 60


If a message has attachments that were not scanned for any reason (e.g. because of size,
depth limits, or scanning timeout), assume the attachment matches the search pattern?
[N]>
```

```
If a message could not be deconstructed into its component parts in order to remove
specified attachments, the system should:

1. Deliver

2. Bounce

3. Drop

[1]> 1


Configure encoding to use when none is specified for plain body text or anything with
MIME type plain/text or plain/html.

1. US-ASCII

2. Unicode (UTF-8)

3. Unicode (UTF-16)

4. Western European/Latin-1 (ISO 8859-1)

5. Western European/Latin-1 (Windows CP1252)

6. Traditional Chinese (Big 5)

7. Simplified Chinese (GB 2312)

8. Simplified Chinese (HZ GB 2312)

9. Korean (ISO 2022-KR)

10. Korean (KS-C-5601/EUC-KR)

11. Japanese (Shift-JIS (X0123))

12. Japanese (ISO-2022-JP)

13. Japanese (EUC)

[1]>


Scan behavior changed.


There are currently 5 attachment type mappings configured to be SKIPPED.


Choose the operation you want to perform:

- NEW - Add a new entry.
```

```
- DELETE - Remove an entry.

- SETUP - Configure scanning behavior.

- IMPORT - Load mappings from a file.

- EXPORT - Save mappings to a file.

- PRINT - Display the list.

- CLEAR - Remove all entries.

- SMIME - Configure S/MIME unpacking.

[]> SMIME


Do you want to convert opaque-signed messages to clear-signed? This will provide the
clear text content for various blades to process. [N]> Y



There are currently 5 attachment type mappings configured to be SKIPPED.


Choose the operation you want to perform:

- NEW - Add a new entry.

- DELETE - Remove an entry.

- SETUP - Configure scanning behavior.

- IMPORT - Load mappings from a file.

- EXPORT - Save mappings to a file.

- PRINT - Display the list.

- CLEAR - Remove all entries.

- SMIME - Configure S/MIME unpacking.

[]> print


1. Fingerprint   Image

2. Fingerprint   Media

3. MIME Type     audio/*
```

```
4. MIME Type     image/*
5. MIME Type     video/*


There are currently 5 attachment type mappings configured to be SKIPPED.


Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.
[]>
```

10 장

메일 정책

메일 정책 개요

Email Security 어플라이언스는 메일 정책을 통해 사용자에게 전송되는 메시지와 사용자가 전송하는 메시지에 조직의 정책을 적용합니다. 다음은 조직이 네트워크에 유입되거나 네트워크에서 유출하지 않고자 하는 의심스럽고, 민감하거나 악의적인 콘텐츠 유형을 지정하는 규칙입니다. 이 콘텐츠에는 다음이 포함될 수 있습니다.

- 스팸
- 정상적인 마케팅 메시지
- 바이러스
- 피싱 및 기타 대상이 있는 메일 공격
- 회사의 기밀 데이터
- 개인이 식별 가능한 정보

조직 내 다양한 사용자 그룹의 각기 다른 보안 요구 사항을 만족하는 여러 가지 정책을 생성할 수 있습니다. Email Security 어플라이언스는 이러한 정책에 정의되어 있는 규칙을 사용하여 각 메시지를 검사하고 필요시 사용자를 보호하기 위한 작업도 수행합니다. 예를 들어, 정책에서 의심스러운 스팸 메시지가 경영진에게 전달되는 것을 방지하면서 동시에 IT 담당자에게는 전달되도록 허용할 수 있지만 제목이 수정된 경우 콘텐츠에 대해 경고하거나 시스템 관리자 그룹의 사용자를 제외한 모든 사용자를 위해 위험한 실행 첨부 파일을 삭제할 수 있습니다.

사용자 단위로 메일 정책을 적용하는 방법

	수행할 작업	추가 정보
1단계	Email Security 어플라이언스에서 수신 또는 발송 메시지에 사용할 콘텐츠 검사 기능을 활성화합니다.	기능을 활성화하여 다음 중 한 가지 이상을 구성할 수 있습니다. • 안티바이러스 • 파일 평판 필터링 및 파일 분석(수신 메시지만) • 안티스팸 • 신종 바이러스 필터(Outbreak Filter) • 데이터 유출 방지(발송 메시지만) • 콘텐츠 필터
2단계	(선택 사항) 특정 데이터를 포함하는 메시지에 수행해야 하는 작업에 대한 콘텐츠 필터를 생성합니다.	11 장, "콘텐츠 필터" 항목을 참조하십시오.
3단계	(선택 사항) 메일 정책 규칙을 적용할 사용자를 지정하려면 LDAP 그룹 쿼리를 정의합니다.	그룹 LDAP 쿼리를 사용하여 수신자가 그룹 멤버인지 판별, 25-23페이지 항목을 참조하십시오.
4단계	(선택 사항) 수신 또는 발송 메시지의 기본 메일 정책을 정의합니다.	수신 또는 발송 메시지에 대한 기본 메일 정책 구성, 10-7페이지 항목을 참조하십시오.
5단계	사용자별로 메일 정책을 설정할 사용자 그룹을 정의합니다.	수신 또는 발송 메일 정책을 생성합니다. 자세한 내용은 메일 정책 구성, 10-7페이지 항목을 참조하십시오.
6단계	콘텐츠 보안 기능과 어플라이언스가 메시지에 수행하는 콘텐츠 필터 작업을 구성합니다.	메일 정책에 대해 다양한 콘텐츠 보안 기능을 구성합니다. • 콘텐츠 필터: 특정 사용자 그룹의 메시지에 콘텐츠 필터 적용, 11-17페이지 • 안티바이러스: 사용자에 대한 바이러스 검사 작업 구성, 12-7페이지 • 파일 평판 필터링 및 파일 분석: 파일 평판 검사 및 파일 분석을 위한 수신 메일 정책 구성, 16-8페이지 • 안티스팸: 안티스팸 정책 정의, 13-7페이지 • 신종 바이러스 필터(Outbreak Filter): 신종 바이러스 필터(Outbreak Filter) 기능 및 메일 정책, 14-16페이지 • 데이터 유출 방지: 발송 메일 정책을 사용하여 DLP 정책을 발신자 및 수신자에게 할당, 17-21페이지 및 Enterprise Manager 구축 시 발송 메일 정책과 DLP 정책 연결 정보, 17-29페이지

수신 및 발송 메시지를 다양한 방식으로 처리

Email Security 어플라이언스는 메시지 콘텐츠 보안을 위해 2가지 메일 정책 집합을 사용합니다.

- *수신 메일 정책*(메시지용)은 모든 리스너에서 ACCEPT HAT 정책과 일치하는 연결에서 수신되는 메시지입니다.
- *발송 메일 정책*(메시지용)은 모든 리스너에서 RELAY HAT 정책과 일치하는 연결에서 보내는 메시지입니다. 여기에는 SMTP AUTH를 통해 인증된 모든 연결이 포함됩니다.

개별 정책 집합을 사용하면 사용자에게 전송된 메시지와 사용자가 전송한 메시지에 다른 보안 규칙을 정의할 수 있습니다. 이러한 정책은 GUI의 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)** 또는 **Outgoing Mail Policies(발송 메일 정책)** 페이지 또는 CLI의 `policyconfig` 명령을 사용하여 관리합니다.

참고 일부 기능은 수신 또는 발송 메일 정책에만 적용할 수 있습니다. 예를 들어, 데이터 유출 방지 검사는 발송 메시지에만 수행할 수 있습니다. AMP(파일 평판 검사 및 파일 분석)는 수신 메일 정책에만 사용할 수 있습니다.

참고 특정한 설치에서 Cisco 어플라이언스를 통해 라우팅되는 "내부" 메일은 모든 수신자가 내부 주소로 처리된 경우에도 *발송 메일*로 간주될 수 있습니다. 예를 들어, 기본적으로 C170 어플라이언스의 경우, 시스템 설정 마법사는 인바운드 이메일을 수신하고 아웃바운드 이메일을 릴레이하기 위해 단 하나의 물리적 이더넷 포트만 구성합니다.

메일 정책과 사용자 일치

어플라이언스에서 메시지를 수신하면 Email Security 어플라이언스는 수신 또는 발송 메시지인지에 따라 메시지 수신자 및 발신자를 수신 또는 발송 메일 정책 테이블에 있는 메일 정책과 일치시키려고 합니다.

일치 작업은 수신자 주소, 발신자 주소 또는 두 가지 모두를 기반으로 수행됩니다.

- *수신자 주소*는 봉투 수신자 주소와 일치합니다.

  수신자 주소와 일치하는 경우 입력한 수신자 주소는 이메일 파이프라인의 앞부분을 처리한 이후의 최종 주소입니다. 예를 들어 기본 도메인, LDAP 라우팅 또는 마스커레이드, 별칭 테이블, 도메인 맵과 메시지 필터 기능이 활성화된 경우 봉투 수신자 주소를 다시 작성할 수 있으며 메시지가 메일 정책과 일치하는지 여부에 영향을 줄 수 있습니다.
- *발신자 주소*는 다음과 일치합니다.
  - 봉투 발신자(RFC821 MAIL FROM 주소)
  - RFC822 From: 헤더에서 찾은 주소
  - RFC822 Reply-To: 헤더에서 찾은 주소

주소는 전체 이메일 주소, 사용자, 도메인 또는 부분 도메인 중 하나와 일치하거나 LDAP 그룹 멤버십과 일치할 수도 있습니다.

관련 주제

- 첫 번째 일치 항목 적용, 10-4페이지
- 정책 일치의 예, 10-4페이지

첫 번째 일치 항목 적용

각 사용자(발신자 또는 수신자)는 하향식 방식으로 적절한 메일 정책 테이블이 정의된 각 메일 정책에 대해 평가됩니다.

각 사용자의 경우, 첫 번째 일치 정책이 적용됩니다. 사용자가 특정한 정책과 일치하지 않는 경우, 사용자는 테이블의 기본 정책과 자동으로 일치하게 됩니다.

발신자 주소에 기반하여 일치 작업이 수행되는 경우 모든 나머지 메시지 수신자도 해당 정책과 일치하게 됩니다. (이것은 메시지당 한 명의 발신자만 가능하기 때문입니다.)

정책 일치의 예

다음의 예는 정책 테이블이 하향식 방식으로 일치하는 방식을 보여줍니다.

표 10-1의 수신 메일의 이메일 보안 정책 테이블을 참조할 때 수신 메시지는 다른 정책과 일치합니다.

표 10-1 정책 일치 예

주문	정책 이름	사용자	
		발신자	수신자
1	special_people	ANY	joe@example.com ann@example.com
2	from_lawyers	@lawfirm.com	ANY
3	acquired_domains	ANY	@newdomain.com @anotherexample.com
4	engineering	ANY	PublicLDAP.ldapgroup: engineers
5	sales_team	ANY	jim@ john@ larry@
	Default Policy	ANY	ANY

관련 주제

- 예 1, 10-4페이지
- 예 2, 10-4페이지
- 예 3, 10-5페이지

예 1

발신자 bill@lawfirm.com에서 수신자 jim@example.com에게 전송된 메시지는 정책 #2와 일치하는데 이것은 사용자 설명이 발신자(@lawfirm.com) 및 수신자(ANY)와 일치하기 때문입니다.

예 2

발신자 joe@yahoo.com은 다음 3명의 수신자에게 수신 메시지를 전송합니다. john@example.com, jane@newdomain.com 및 bill@example.com

- 수신자 jane@newdomain.com의 메시지는 안티스팸, 안티바이러스, 신종 바이러스 필터(Outbreak Filter) 및 정책 #3에 정의되어 있는 콘텐츠 필터를 수신합니다.

- 수신자 john@example.com의 메시지는 정책 #5에 정의되어 있는 설정을 수신합니다.
- 수신자 bill@example.com이 엔지니어링 LDAP 쿼리와 일치하지 않으므로 메시지는 기본 정책에서 정의한 설정을 수신합니다.

이 예는 수신자가 여러 명인 메시지가 어떻게 *메시지 분리*의 원인이 되는지 보여줍니다. 자세한 내용은 메시지 분리, 10-5페이지 항목을 참조하십시오.

예 3

발신자 bill@lawfirm.com은 수신자 ann@example.com과 larry@example.com에게 메시지를 전송합니다.

- 수신자 ann@example.com은 안티스팸, 안티바이러스, 신종 바이러스 필터(Outbreak Filter) 및 정책 #1에 정의되어 있는 콘텐츠 필터를 수신합니다.
- 수신자 larry@example.com은 안티스팸, 안티바이러스, 신종 바이러스 필터(Outbreak Filter) 및 정책 #2에 정의되어 있는 콘텐츠 필터를 수신하는데 이것은 발신자(@lawfirm.com) 및 수신자(ANY)가 일치하기 때문입니다.

메시지 분리

지능형 메시지 분리는 다양한 수신자 기반 콘텐츠 보안 규칙을 여러 수신자가 있는 메시지와 별개로 적용하는 메커니즘입니다.

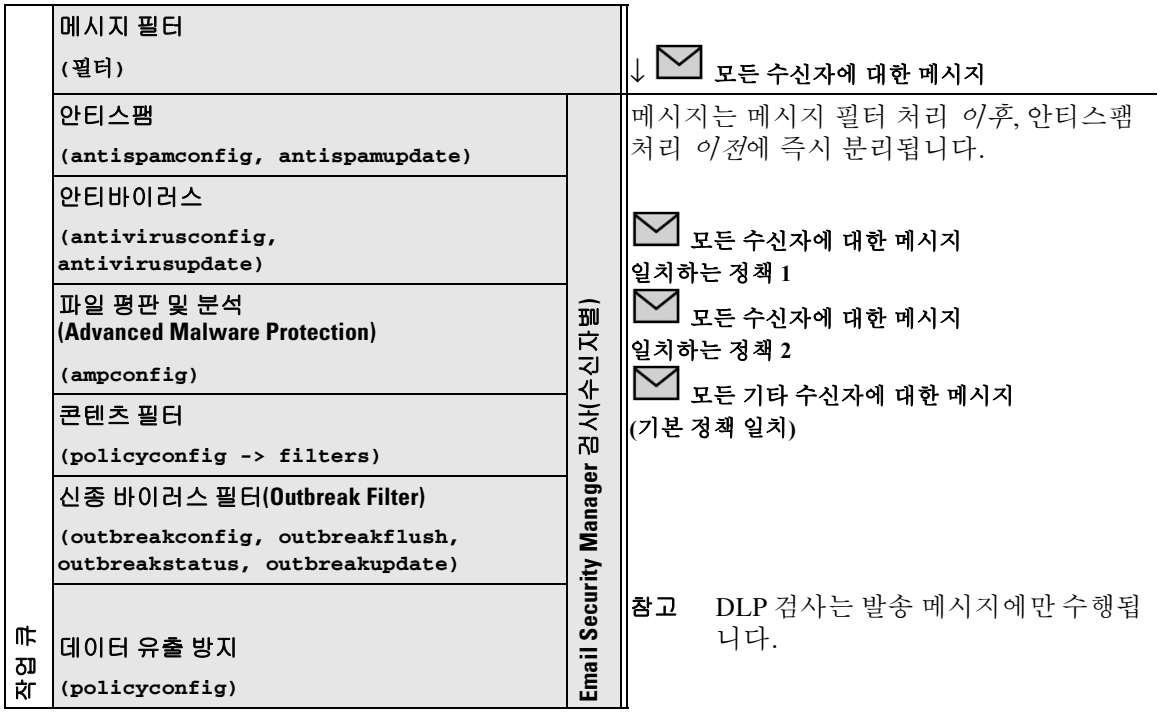
각 수신자는 하향식으로 적절한 메일 정책 테이블(수신 또는 발신)에서 각 정책에 대해 평가됩니다.

메시지와 일치하는 각 정책은 해당 수신자가 있는 새로운 메시지를 생성합니다. 이 프로세스를 *메시지 분리*라고 정의합니다.

- 일부 수신자가 다른 정책과 일치하는 경우 수신자는 일치하는 정책에 따라 그룹화되며 메시지는 일치하는 정책의 수와 동일한 메시지 수로 분리되며 수신자는 각각의 해당 "분리"에 설정됩니다.
- 모든 수신자가 동일한 정책과 일치하는 경우 메시지는 분리되지 않습니다. 반대로, 최대 분리 시나리오는 단일 메시지가 각각의 메시지 수신자에 분리되는 것입니다.
- 그런 다음 각 메시지 분리는 이메일 파이프라인에서 안티스팸, 안티바이러스, Advanced Malware Protection(수신 메시지만), DLP 검사(발송 메시지만), 신종 바이러스 필터(Outbreak Filter) 및 콘텐츠 필터별로 개별적으로 처리됩니다.

표 10-2는 메시지가 이메일 파이프라인에서 분리되는 지점을 설명합니다.

표 10-2 이메일 파이프라인에서의 메시지 분리



참고 새 MID(메시지 ID)는 각 메시지의 분리마다 생성됩니다(예: MID 1은 MID2와 MID3가 됨). 자세한 내용은 "로깅" 장을 참조하십시오. 또한 `trace` 함수는 어떤 정책이 메시지 분리의 원인이 되는지 보여줍니다.

Email Security Manager 정책의 정책 일치 및 메시지 분리는 어플라이언스에서 메시지 처리를 관리하는 방법에 분명하게 영향을 미칩니다.

관련 주제

- 예외 관리, 10-6페이지

예외 관리

각 분리 메시지의 반복 처리가 성능에 영향을 미치기 때문에 *예외 관리* 기준에 따라 콘텐츠 보안 규칙을 구성하는 것이 좋습니다. 즉, 조직의 요구 사항을 평가하고 기능을 구성하여 대부분의 메시지를 기본 메일 정책에 따라 처리하고 소수의 메시지는 몇 가지 추가적인 "예외" 정책에 따라 처리합니다. 이러한 방식에서 메시지 분리가 최소화되고 작업 큐에서 각 분리 메시지를 처리할 때 시스템 성능에 영향을 거의 미치지 않습니다.

메일 정책 구성

메일 정책은 안티스팸 또는 안티바이러스 등의 특정한 보안 설정에 다양한 사용자 그룹을 매핑합니다.

관련 주제

- 수신 또는 발송 메시지에 대한 기본 메일 정책 구성, 10-7페이지
- 발신자 및 수신자 그룹에 대한 메일 정책 생성, 10-7페이지
- 어떤 정책이 발신자 또는 수신자에게 적용되는지 찾기, 10-11페이지

수신 또는 발송 메시지에 대한 기본 메일 정책 구성

기본 메일 정책은 다른 메일 정책에 포함되지 않는 메시지에 적용됩니다. 다른 정책이 구성되지 않은 경우, 기본 정책이 모든 메시지에 적용됩니다.

시작하기 전에

메일 정책에 대해 개인 보안 서비스를 정의하는 방법을 파악합니다. 사용자 단위로 메일 정책을 적용하는 방법, 10-2페이지 항목을 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)**

또는

Mail Policies(메일 정책) > Outgoing Mail Policies(발송 메일 정책)를 클릭합니다.

2단계 기본 메일 정책에 대해 구성할 보안 서비스의 링크를 클릭합니다.

참고 기본 보안 서비스 설정과 관련하여 페이지의 첫 번째 설정에서는 정책에 대해 서비스를 활성화할지 여부를 정의합니다. 서비스를 모두 비활성화하려면 "Disable(비활성화)"을 클릭합니다.

3단계 보안 서비스에 대한 설정을 구성합니다.

4단계 **Submit(제출)**을 클릭합니다.

5단계 변경사항을 제출하고 커밋합니다.

발신자 및 수신자 그룹에 대한 메일 정책 생성

시작하기 전에

- 메일 정책에 대해 개인 보안 서비스를 정의하는 방법을 파악합니다. 사용자 단위로 메일 정책을 적용하는 방법, 10-2페이지 항목을 참조하십시오.
- 각 수신자는 하향식으로 적절한 테이블(수신 또는 발송)의 각 정책에 대해 평가됩니다. 자세한 내용은 첫 번째 일치 항목 적용, 10-4페이지 항목을 참조하십시오.

- (선택 사항) 메일 정책 관리를 책임질 위임 관리자를 정의합니다. 위임 관리자는 정책의 안티스팸, 안티바이러스, Advanced Malware Protection 및 신종 바이러스 필터(Outbreak Filter) 설정을 편집하고 정책에 대한 콘텐츠 필터를 활성화 또는 비활성화할 수 있습니다. 운영자와 관리자만 메일 정책의 이름 또는 메일 정책의 발신자, 수신자 또는 그룹을 수정할 수 있습니다. 메일 정책에 대한 전체 액세스 권한이 있는 사용자 지정 사용자 역할이 메일 정책에 자동으로 할당됩니다.

절차

1단계 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)** 또는 **Mail Policies(메일 정책) > Outgoing Mail Policies(발송 메일 정책)**를 선택합니다.

2단계 **Add Policy(정책 추가)**를 클릭합니다.

3단계 메일 정책 이름을 입력합니다.

4단계 (선택 사항) Editable By (Roles)(편집 가능한 사용자(역할)) 링크를 클릭하고 메일 정책 관리를 담당할 위임 관리자에 대한 사용자 지정 사용자 역할을 선택합니다.

5단계 정책에 대해 사용자를 정의합니다. 사용자 정의에 대한 지침은 메일 정책에 대한 발신자 및 수신자 정의, 10-8페이지 항목을 참조하십시오.

6단계 **Submit(제출)**을 클릭합니다.

7단계 메일 정책에 대해 구성할 콘텐츠 보안 서비스의 링크를 클릭합니다.

8단계 드롭다운 목록에서 기본 설정을 사용하는 대신 정책에 대한 설정을 사용자 지정하는 옵션을 선택합니다.

9단계 보안 서비스 설정을 사용자 지정합니다.

10단계 변경사항을 제출하고 커밋합니다.

관련 주제

- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 13-2페이지
- 메일 정책에 대한 발신자 및 수신자 정의, 10-8페이지

메일 정책에 대한 발신자 및 수신자 정의

다음 방식으로 정책을 적용할 발신자 및 수신자를 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 쿼리와 일치

참고 사용자 항목은 AsyncOS의 GUI 및 CLI에서 모두 대소문자를 구분하지 않습니다. 예를 들어, 사용자에 수신자 `Joe@`를 입력한 경우 `joe@example.com`으로 전송된 메시지와 일치합니다.

메일 정책에 대한 발신자와 수신자를 정의할 때 다음을 유의해야 합니다.

- 하나 이상의 발신자 및 수신자를 지정해야 합니다.
- 다음에 해당하는 경우 정책이 일치하도록 설정할 수 있습니다.
  - 임의의 발신자, 한 명 이상의 지정된 발신자 또는 지정되지 않은 발신자가 보낸 메시지.
  - 임의의 수신자, 한 명 이상의 지정된 수신자 또는 모든 지정된 수신자 및 지정되지 않은 수신자에게 발송된 메시지.

절차

1단계 **Users(사용자)** 섹션에서 **Add User(사용자 추가)**를 클릭합니다.

2단계 정책에 대한 발신자를 정의합니다. 다음 옵션 중 하나를 선택합니다.

- **Any Sender(모든 발신자)**. 메시지가 모든 발신자의 메시지인 경우 정책이 일치합니다.
- **Following Senders(다음 발신자)**. 메시지가 하나 이상의 특정한 발신자의 메시지인 경우 정책이 일치합니다. 이 옵션을 선택하고 텍스트 상자에 발신자 세부 정보를 입력하거나 LDAP 그룹 쿼리를 선택합니다.
- **Following Senders are Not(다음 발신자는 아닙니다)**. 특정한 발신자가 보낸 메시지가 하나도 없는 경우 정책이 일치합니다. 이 옵션을 선택하고 텍스트 상자에 발신자 세부 정보를 입력하거나 LDAP 그룹 쿼리를 선택합니다.

위의 필드를 선택할 때 발신자 조건을 설정하는 방법을 알아보려면 예, 10-10페이지 항목을 참조하십시오.

3단계 정책에 대한 수신자를 정의합니다. 다음 옵션 중 하나를 선택합니다.

- **Any Recipient(모든 수신자)**. 메시지가 모든 수신자에게 전송된 경우 정책이 일치합니다.
- **Following Recipients(다음 수신자)**. 메시지가 특정한 수신자에게 전송된 경우 정책이 일치합니다. 이 옵션을 선택하고 텍스트 상자에 수신자 세부 정보를 입력하거나 LDAP 그룹 쿼리를 선택합니다.

  메시지가 한 명 이상의 지정된 수신자 또는 모든 지정된 수신자에게 전송되는 경우 정책의 일치 여부를 선택할 수 있습니다. 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. **If one more conditions match(하나 이상의 조건이 일치하는 경우)** 또는 **Only if all conditions match(모든 조건이 일치하는 경우에만)**.
- **Following Recipients are Not(다음 수신자는 아닙니다)**. 메시지가 특정한 수신자에게 전송되지 않은 경우 정책이 일치합니다. 이 옵션을 선택하고 텍스트 상자에 수신자 세부 정보를 입력하거나 LDAP 그룹 쿼리를 선택합니다.

  참고 드롭다운 목록에서 **Following Recipients(다음 수신자)**를 선택하고 **Only if all conditions match(모든 조건이 일치하는 경우에만)**를 선택한 경우에만 이 옵션을 구성할 수 있습니다.

위의 필드를 선택할 때 수신자 조건을 설정하는 방법을 알아보려면 예, 10-10페이지 항목을 참조하십시오.

4단계 **Submit(제출)**을 클릭합니다.

5단계 **Users(사용자)** 섹션에서 선택한 조건을 검토합니다.

관련 주제

- 발신자 및 수신자 그룹에 대한 메일 정책 생성, 10-7페이지
- 예, 10-10페이지

예

다음 표는 Add User(사용자 추가) 페이지에서 다양한 옵션을 선택할 때 조건을 설정하는 방법을 설명합니다.

발신자			수신자			조건
모든 발신자	**다음 발신자**	**다음 발신자는 아닙니다.**	**모든 수신자**	**다음 수신자**	**다음 수신자는 아닙니다.**	
선택됨	-	-	-	선택됨 (기본값) **Only if all conditions match(모든 조건이 일치하는 경우에만)** 옵션이 선택되었습니다. 값: `user1@, user2@`	-	**발신자**: 모두 **수신자**: `user1@[AND]user2@`

-	선택됨
	값:
	`u1@a.com, u2@a.com`
		-	-	선택됨
				(기본값) **Only if all conditions match(모든 조건이 일치하는 경우에만)** 옵션이 선택되었습니다.
				값:
				`u1@b.com, u2@b.com`
					선택됨
					값:
					`u3@b.com, u4@b.com`
						발신자:
						`u1@a.com[OR]u2@a.com`
						수신자:
						`[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) 옵션이 선택되었습니다.
				값:
				`u1@b.com, u2@b.com`
					-	**발신자**:
						`[NOT][u1@a.com[OR]u2@a.com]`
						수신자:
						`u1@b.com[OR]u2@b.com`

관련 주제

- 메일 정책에 대한 발신자 및 수신자 정의, 10-8페이지

어떤 정책이 발신자 또는 수신자에게 적용되는지 찾기

Mail Policies(메일 정책) 페이지 상단에 있는 Find Policies(정책 찾기) 섹션을 사용하여 수신 또는 발송 메일 정책에 이미 정의되어 있는 사용자를 찾을 수 있습니다.

예를 들어, bob@example.com을 입력하고 Find Policies(정책 찾기) 버튼을 클릭하면 정의된 사용자를 포함하는 정책과 일치하는 정책이 표시됩니다.

해당 정책에 대해 사용자를 편집하려면 정책의 이름을 클릭합니다.

발신자 또는 수신자가 기타 모든 구성된 정책과 일치하지 않는 경우 이러한 정책은 기본 정책과 *항상* 일치하기 때문에 사용자를 검색할 때 기본 정책이 항상 표시됩니다.

관련 주제

- 예외 관리, 10-11페이지

예외 관리

위의 2가지 예에서 살펴본 단계를 수행하여 *예외 관리* 기준으로 정책 생성 및 구성을 시작할 수 있습니다. 즉 조직의 요구 사항을 평가한 후 메시지 대부분을 기본 정책으로 처리할 수 있도록 정책을 구성할 수 있습니다. 그런 다음 필요 시 다른 정책을 관리하도록 특정 사용자 또는 사용자 그룹을 대상으로 추가 "예외" 정책을 생성할 수 있습니다. 이러한 방식에서 메시지 분리가 최소화되고 작업 큐에서 각 분리 메시지를 처리할 때 시스템 성능에 영향을 거의 미치지 않습니다.

스팸, 바이러스 및 정책 적용을 위한 조직 또는 사용자의 허용 범위를 기준으로 정책을 정의할 수 있습니다. 표 10-3(10-11페이지)에 여러 정책의 예가 설명되어 있습니다. "적극적인" 정책은 최종 사용자 메일함에 도착하는 스팸과 바이러스의 양을 최소화하기 위해 설계되었습니다. "보수적인" 정책은 긍정 오류를 방지하고 정책과 관계없이 누락된 메시지가 없도록 맞춤화되었습니다.

표 10-3 Email Security Manager에 대한 적극적인 설정 및 보수적인 설정

	적극적인 설정	보수적인 설정
안티스팸	스팸으로 확인된 스팸: 삭제 의심스러운 스팸: 격리 마케팅 메일: 전달 및 제목 메시지 앞에 "[마케팅]" 추가	스팸으로 확인된 스팸: 격리 의심스러운 스팸: 전달 및 메시지 제목 앞에 "[의심스러운 스팸]" 추가 마케팅 메일: 비활성화됨
안티바이러스	복구된 메시지: 전달 암호화된 메시지: 삭제 검사할 수 없는 메시지: 삭제 감염된 메시지: 삭제	복구된 메시지: 전달 암호화된 메시지: 격리 검사할 수 없는 메시지: 격리 감염된 메시지: 삭제

표 10-3 Email Security Manager에 대한 적극적인 설정 및 보수적인 설정 (계속)

AMP(Advanced Malware Protection) (파일 평판 필터링 및 파일 분석)	검사하지 않은 첨부 파일: 삭제 악성코드 첨부 파일이 있는 메시지: 삭제 파일 분석을 보류 중인 메시지: 격리	검사하지 않은 첨부 파일: 전달 및 메시지 제목 앞에 "[경고: 첨부 파일 검사 안 함]" 추가 악성코드 첨부 파일이 있는 메시지: 삭제 파일 분석을 보류 중인 메시지: 전달 및 메시지 제목 앞에 "[경고: 첨부 파일에 악성코드가 포함되어 있을 수 있음]" 추가
바이러스 필터	활성화됨, 특정한 파일 이름 확장명 또는 도메인의 우회가 허용되지 않음 모든 메시지의 메시지 수정 활성화	활성화됨, 특정한 파일 이름 확장명 또는 도메인의 우회가 허용됨 서명되지 않은 메시지에 대한 메시지 수정 활성화

11 장

콘텐츠 필터

콘텐츠 필터 개요

Email Security 어플라이언스는 해당 콘텐츠로 인해 가끔 특수한 처리가 필요한 메시지를 수신합니다. 예를 들어 나중에 검사하기 위해 콘텐츠를 격리해야 하거나 기업 정책에 따라 특정 메시지를 전달하기 전 암호화해야 하는 등 여러 가지 이유가 있습니다. 이러한 경우 안티바이러스 검사 또는 DLP와 같은 콘텐츠 보안 기능으로는 메시지를 처리할 수 없습니다. 따라서 Email Security 어플라이언스는 콘텐츠 필터를 사용하여 그러한 콘텐츠를 검사한 다음 메시지에 적절한 조치를 취합니다.

콘텐츠 필터 동작 방식

콘텐츠 필터는 메시지 필터와 유사하지만, 메시지에 메시지 필터 처리와 안티스팸 및 안티바이러스 검사가 완료된 후에 적용됩니다. Email Security 어플라이언스는 콘텐츠 필터를 사용하여 사용자별(발신자 또는 수신자)로 메시지를 검사합니다. 콘텐츠 필터는 이메일 파이프라인의 후반부, 즉 메시지가 일치하는 메일 정책별로 여러 개의 개별 메시지로 "분리"된 후에 적용된다는 점을 제외하고 메시지 필터와 유사합니다. (자세한 내용은 메시지 분리, 10-5페이지 참조.) 콘텐츠 필터의 기능은 메시지에 대해 메시지 필터 처리와 안티스팸 및 안티바이러스 검사가 수행된 후에 적용됩니다.

콘텐츠 필터는 수신 또는 발송 메시지 검사로 제한됩니다. 두 메시지 유형을 모두 검사하는 필터는 정의할 수 없습니다. Email Security 어플라이언스는 메시지 유형마다 별도의 콘텐츠 필터 "마스터 목록"을 갖습니다. 마스터 목록은 또한 어플라이언스에서 콘텐츠 필터가 실행되는 순서를 결정합니다. 그러나 메시지가 정책에 부합할 경우 개별 메일 정책에 따라 실행되는 필터가 결정됩니다.

AsyncOS는 네 가지 기능을 사용하여 콘텐츠 필터를 쉽게 생성할 수 있는 "규칙 빌더" 페이지를 제공합니다.

- *조건*: 어플라이언스가 콘텐츠 필터를 사용하여 메시지를 검사하는 경우 트리거되는 사항(선택 사항)
- *작업*: 어플라이언스가 메시지에 대해 수행하는 작업(필수)
- *작업 변수*: 어플라이언스가 메시지를 수정할 때 메시지에 추가할 수 있는 변수(선택 사항)

관련 주제

- 콘텐츠 필터를 사용하여 메시지 콘텐츠를 검사하는 방법, 11-2페이지
- 콘텐츠 필터 조건, 11-2페이지
- 콘텐츠 필터 작업, 11-9페이지
- 작업 변수, 11-14페이지

콘텐츠 필터를 사용하여 메시지 콘텐츠를 검사하는 방법

	수행할 작업	추가 정보
1단계	(선택 사항) 콘텐츠 필터를 지원하는 기능을 정의합니다.	콘텐츠 필터와 함께 사용할 다음 항목 중 하나를 생성합니다. • 암호화 프로파일 • 고지 사항 템플릿 • 알림 템플릿 • 정책 격리 • URL 화이트리스트
2단계	수신 또는 발송 콘텐츠 필터를 정의합니다.	콘텐츠 필터는 다음 세 부분으로 구성됩니다. • 콘텐츠 필터 조건(선택 사항) • 콘텐츠 필터 작업 • 작업 변수(선택 사항) 콘텐츠 필터 생성, 11-16페이지
3단계	콘텐츠 보안 규칙을 설정하고자 하는 사용자 그룹을 정의합니다.	수신 또는 발송 메일 정책을 생성합니다.
4단계	수신 또는 발송 메시지를 소유하는 사용자 그룹에 사용하고자 하는 콘텐츠 필터를 할당합니다.	10 장, "메일 정책" 항목을 참조하십시오.

콘텐츠 필터 조건

조건이란 Email Security 어플라이언스가 관련된 메일 정책에 부합하는 메시지에 필터를 사용할지 여부를 결정하는 "트리거"를 의미합니다. 콘텐츠 필터에 조건을 지정하는 것은 선택 사항입니다. 조건이 없는 콘텐츠 필터는 관련된 메일 정책에 부합하는 모든 메시지에 적용됩니다.

콘텐츠 필터 조건에서 메시지 본문 또는 첨부 파일의 특정 패턴을 검색하는 필터 규칙을 추가하는 경우 패턴 발견 횟수에 대한 최소 임계값을 지정할 수 있습니다. AsyncOS는 메시지를 검사할 때 메시지 및 첨부 파일에서 확인된 일치 항목의 개수에 해당하는 "점수"를 계산합니다. 최소 임계값을 만족하지 못할 경우 정규식은 true로 평가되지 않습니다. 텍스트, 스마트 식별자 또는 콘텐츠 사전 용어에 대해 이 임계값을 지정할 수 있습니다.

각 필터에 여러 조건을 정의할 수 있습니다. 여러 조건을 정의하는 경우 조건이 논리적 OR("다음 조건 중 하나...") 또는 논리적 AND("다음 조건 모두")로 함께 연결되는지 여부를 선택할 수 있습니다.

표 11-1 콘텐츠 필터 조건

조건	설명
(조건 없음)	콘텐츠 필터에 조건을 지정하는 것은 선택 사항입니다. 조건을 지정하지 않으면 `true` 규칙이 묵시적으로 적용됩니다. `true` 규칙은 모든 메시지와 일치하며 해당 작업은 항상 수행됩니다.
메시지 본문 또는 첨부 파일	**텍스트 포함:** 메시지 본문에 특정 패턴과 일치하는 텍스트 또는 첨부 파일이 포함되어 있습니까? **스마트 식별자 포함:** 메시지 본문 또는 첨부 파일의 콘텐츠가 스마트 식별자와 일치합니까? **콘텐츠 사전의 용어 포함:** 메시지 본문이 정규식이나 <*dictionary name*>이라는 콘텐츠 사전의 용어를 포함하고 있습니까? 이 옵션을 활성화하려면 사전이 이미 생성되어 있어야 합니다. 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **참고** 사전과 관련된 조건은 하나 이상의 사전이 활성화되어 있는 경우에만 사용할 수 있습니다. 콘텐츠 사전 생성에 대한 자세한 내용은 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **필요한 일치 수**. 규칙을 true로 평가하는 데 필요한 일치 수를 지정합니다. 텍스트, 스마트 식별자 또는 콘텐츠 사전 용어에 대해 이 임계값을 지정할 수 있습니다. 여기에는 전송 상태 및 연결된 첨부 파일이 포함됩니다.

표 11-1 콘텐츠 필터 조건 (계속)

조건	설명
메시지 본문	**텍스트 포함:** 메시지 본문에 특정 패턴과 일치하는 텍스트가 포함되어 있습니까? **스마트 식별자 포함:** 메시지 본문의 콘텐츠가 스마트 식별자와 일치합니까? 스마트 식별자는 다음의 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 **콘텐츠 사전의 용어 포함:** 메시지 본문이 정규식이나 <*dictionary name*>이라는 콘텐츠 사전의 용어를 포함하고 있습니까? 이 옵션을 활성화하려면 사전이 이미 생성되어 있어야 합니다. 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **참고** 사전과 관련된 조건은 하나 이상의 사전이 활성화되어 있는 경우에만 사용할 수 있습니다. 콘텐츠 사전 생성에 대한 자세한 내용은 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **필요한 일치 수**. 규칙을 true로 평가하는 데 필요한 일치 수를 지정합니다. 텍스트 또는 스마트 식별자에 대해 이 임계값을 지정할 수 있습니다. 이 규칙은 메시지 본문에만 적용됩니다. 첨부 파일 또는 헤더는 포함되지 않습니다.
URL 평판	메시지에 포함된 URL의 평판 또는 범주에 따라 작업 수행, 15-7페이지 및 URL 필터링 허용 목록 생성, 15-4페이지 항목을 참조하십시오. 평판을 판단할 수 없는 URL에는 "점수 없음"을 사용합니다.
URL 범주	URL 평판 또는 URL 범주를 통한 필터링: 조건 및 규칙, 15-8페이지 및 URL 범주 정보, 15-13페이지 항목을 참조하십시오.
메시지 크기	본문 크기가 지정된 범위 안에 있습니까? 본문 크기는 헤더와 첨부 파일 모두를 포함한 메시지의 크기를 나타냅니다. body-size 규칙은 본문 크기와 지정된 숫자를 지정된 방식으로 비교하는 메시지를 선택합니다.

표 11-1 콘텐츠 필터 조건 (계속)

조건	설명
첨부 파일 콘텐츠	**텍스트 포함.** 메시지에 특정 패턴과 일치하는 텍스트 또는 다른 첨부 파일을 포함하는 첨부 파일이 있습니까? 이 규칙은 `body-contains()` 규칙과 비슷하지만, 메시지의 전체 "본문" 검사를 회피하려고 합니다. 즉, 사용자가 첨부 파일로 보는 부분만 검사하려고 시도합니다. **스마트 식별자 포함.** 메시지 첨부 파일의 콘텐츠가 지정된 스마트 식별자와 일치합니까? **콘텐츠 사전의 용어 포함.** 첨부 파일이 정규식이나 <*dictionary name*>이라는 콘텐츠 사전의 용어를 포함하고 있습니까? 사전 용어를 검색하려면 사전이 이미 생성되어 있어야 합니다. 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **참고** 사전과 관련된 조건은 하나 이상의 사전이 활성화되어 있는 경우에만 사용할 수 있습니다. 콘텐츠 사전 생성에 대한 자세한 내용은 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **필요한 일치 수**. 규칙을 true로 평가하는 데 필요한 일치 수를 지정합니다. 텍스트, 스마트 식별자 또는 콘텐츠 사전 일치에 대해 이 임계값을 지정할 수 있습니다.

표 11-1 콘텐츠 필터 조건 (계속)

조건	설명
첨부 파일 정보	**파일 이름.** 메시지에 특정 패턴과 일치하는 파일 이름을 가진 첨부 파일이 있습니까? **파일 이름에 콘텐츠 사전의 용어 포함.** 메시지의 첨부 파일에 정규식이나 *<dictionary name>*이라는 콘텐츠 사전의 용어를 포함하는 파일 이름이 있습니까? 이 옵션을 활성화하려면 사전이 이미 생성되어 있어야 합니다. 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **참고** 사전과 관련된 조건은 하나 이상의 사전이 활성화되어 있는 경우에만 사용할 수 있습니다. 콘텐츠 사전 생성에 대한 자세한 내용은 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **파일 유형**. 메시지에 해당 지문(UNIX `file` 명령과 유사)을 기준으로 하는 특정 패턴과 일치하는 파일 유형의 첨부 파일이 있습니까? **MIME 유형**. 메시지에 특정 MIME 유형의 첨부 파일이 있습니까? 이 규칙은 MIME 첨부 파일에 지정된 MIME 유형이 평가된다는 것만 제외하고 `attachment-type` 규칙과 유사합니다. (이 어플라이언스는 명시적 유형이 지정되지 않은 경우 파일 유형을 확장명으로 "추측"하지 않습니다.) **이미지 분석.** 메시지에는 지정된 이미지 판정과 일치하는 이미지 첨부 파일이 있습니까? 유효한 이미지 분석 판정에는 *의심*, *부적절*, *의심 또는 부적절*, *검사할 수 없음* 또는 *정상*이 있습니다. **첨부 파일이 손상됨.** 이 메시지에 손상된 첨부 파일이 있습니까? **참고** 손상된 첨부 파일이란 검사 엔진이 검사할 수 없거나 손상된 것으로 식별한 첨부 파일을 의미합니다.
첨부 파일 보호	**비밀번호로 보호되거나 암호화된 첨부 파일 포함.** (예를 들어 검사할 수 없는 첨부 파일을 식별하려면 이 조건을 사용하십시오.) **비밀번호로 보호되거나 암호화되지 않은 첨부 파일 포함.**

표 11-1 콘텐츠 필터 조건 (계속)

조건	설명
제목 헤더	**제목 헤더:** 제목 헤더가 특정 패턴과 일치합니까? **콘텐츠 사전의 용어 포함**: 제목 헤더에 정규식이나 <*dictionary name*>이라는 콘텐츠 사전의 용어를 포함하고 있습니까? 사전 용어를 검색하려면 사전이 이미 생성되어 있어야 합니다. 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **참고** 사전과 관련된 조건은 하나 이상의 사전이 활성화되어 있는 경우에만 사용할 수 있습니다. 콘텐츠 사전 생성에 대한 자세한 내용은 콘텐츠 사전, 21-2페이지 항목을 참조하십시오.
기타 헤더	**헤더 이름**: 메시지에 특정 헤더가 있습니까? **헤더 값:** 헤더 값이 특정 패턴과 일치합니까? **헤더 값에 콘텐츠 사전의 용어 포함.** 지정된 헤더가 정규식이나 <*dictionary name*>이라는 콘텐츠 사전의 용어를 포함하고 있습니까? 사전 용어를 검색하려면 사전이 이미 생성되어 있어야 합니다. 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **참고** 사전과 관련된 조건은 하나 이상의 사전이 활성화되어 있는 경우에만 사용할 수 있습니다. 콘텐츠 사전 생성에 대한 자세한 내용은 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. 이 옵션을 사용할 수 있는 방법을 보여주는 예는 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예, 13-11페이지 항목을 참조하십시오.

표 11-1 콘텐츠 필터 조건 (계속)

조건	설명
봉투 발신자	**봉투 발신자.** 봉투 발신자(예: Envelope From, <MAIL FROM>)가 지정된 패턴과 일치합니까? **LDAP 그룹과 일치**. 봉투 발신자(예: Envelope From, <MAIL FROM>)가 지정된 LDAP 그룹에 있습니까? **콘텐츠 사전의 용어 포함.** 봉투 발신자가 정규식이나 <*dictionary name*>이라는 콘텐츠 사전의 용어를 포함하고 있습니까? 사전 용어를 검색하려면 사전이 이미 생성되어 있어야 합니다. 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **참고** 사전과 관련된 조건은 하나 이상의 사전이 활성화되어 있는 경우에만 사용할 수 있습니다. 콘텐츠 사전 생성에 대한 자세한 내용은 콘텐츠 사전, 21-2페이지 항목을 참조하십시오.
봉투 수신자	**봉투 수신자**. 봉투 수신자(예: Envelope To, <RCPT TO>)가 지정된 패턴과 일치합니까? **LDAP 그룹과 일치**. 봉투 수신자(예: Envelope To, <RCPT TO>)가 지정된 LDAP 그룹에 있습니까? **콘텐츠 사전의 용어 포함.** 봉투 수신자가 <*dictionary name*>이라는 콘텐츠 사전의 정규식이나 용어를 포함하고 있습니까? 사전 용어를 검색하려면 사전이 이미 생성되어 있어야 합니다. 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **참고** 사전과 관련된 조건은 하나 이상의 사전이 활성화되어 있는 경우에만 사용할 수 있습니다. 콘텐츠 사전 생성에 대한 자세한 내용은 콘텐츠 사전, 21-2페이지 항목을 참조하십시오. **참고:** 봉투 수신자 규칙은 메시지를 기반으로 합니다. 메시지에 수신자가 여러 명일 경우 모든 수신자에게 메시지를 적용하려면 지정된 작업에 대해 한 명의 수신자만 있어야 합니다. 봉투 발신자(예: Envelope From, <MAIL FROM>)가 지정된 LDAP 그룹에 있습니까?
수신 리스너	메시지가 명명된 리스너를 통해 도착했습니까? 리스너 이름은 현재 시스템에 구성된 리스너의 이름이어야 합니다.

표 11-1 콘텐츠 필터 조건 (계속)

조건	설명
원격 IP	메시지가 지정된 IP 주소 또는 IP 블록과 일치하는 원격 호스트에서 발송되었습니까? 원격 IP 규칙은 테스트를 통해 해당 메시지를 전송한 호스트의 IP 주소가 특정 패턴과 일치하는지 확인합니다. 이는 인터넷 프로토콜 버전 4(IPv4) 또는 버전 6(IPv6) 주소일 수 있습니다. IP 주소 패턴은 SBO, SBRS, dnslist 표기법 및 특수 키워드 ALL을 제외하고 발신자 그룹 구문, 7-4페이지에 설명된, 허용되는 호스트 표기법을 사용하여 지정됩니다.
Reputation 점수	발신자의 SenderBase Reputation 점수란 무엇입니까? 평판 점수 규칙에서는 다른 값에 대한 SenderBase Reputation 점수를 확인합니다.
DKIM 인증	DKIM 인증을 통과했습니까, 부분적으로 확인되었습니까, 일시적으로 확인 불가능한 결과가 반환되었습니까, 영구적으로 실패했습니까, 아니면 DKIM 결과가 반환되지 않았습니까?
SPF 확인	SPF 확인 상태는 어땠습니까? 이 필터 규칙을 통해 다양한 SPF 확인 결과를 쿼리할 수 있습니다. SPF 확인에 대한 자세한 내용은 "이메일 인증" 장을 참조하십시오.
S/MIME 게이트웨이 메시지	S/MIME 메시지가 서명되었습니까, 암호화되었습니까, 아니면 서명되고 암호화되었습니까? 자세한 내용은 19 장, "S/MIME 보안 서비스" 항목을 참조하십시오.
S/MIME 게이트웨이 확인됨	S/MIME 메시지가 성공적으로 확인되었습니까, 암호가 해독되었습니까, 아니면 암호가 해독되고 확인되었습니까? 자세한 내용은 19 장, "S/MIME 보안 서비스" 항목을 참조하십시오.

콘텐츠 필터 작업

작업이란 Email Security 어플라이언스가 콘텐츠 필터의 조건과 일치하는 메시지에 수행하는 것을 의미합니다. 메시지 수정, 격리 또는 삭제 등 다양한 유형의 작업을 사용할 수 있습니다. 메시지에 수행하는 "최종 작업"(메시지 전달 또는 삭제)에서는 Email Security 어플라이언스가 작업을 즉시 수행하고 신종 바이러스 필터(Outbreak Filter) 또는 DLP 검사와 같은 모든 추가적인 처리를 무시하게 됩니다.

각 콘텐츠 필터마다 적어도 하나의 작업을 정의해야 합니다.

작업은 메시지마다 순서대로 수행되므로 콘텐츠 필터에 여러 작업을 정의할 때는 작업의 순서를 고려해야 합니다.

첨부 파일 콘텐츠 조건, 메시지 본문이나 첨부 파일 조건, 메시지 본문 조건 또는 첨부 파일 콘텐츠 조건과 일치하는 메시지에 대해 격리 작업을 구성하는 경우 격리된 메시지에서 일치하는 콘텐츠를 볼 수 있습니다. 메시지 본문을 표시하면 일치하는 콘텐츠가 노란색으로 강조 표시됩니다. 또한 `$MatchedContent` 작업 변수를 사용하여 메시지 제목에 일치하는 콘텐츠를 포함할 수 있습니다. 자세한 내용은 텍스트 리소스 장을 참조하십시오.

필터별로 하나의 최종 작업만 정의할 수 있으며 최종 작업은 마지막으로 나열된 작업이어야 합니다. 바운스, 전달 및 삭제가 최종 작업입니다. 콘텐츠 필터에 대한 작업을 입력하면 GUI 및 CLI에서 최종 작업이 강제로 마지막에 배치됩니다.

표 11-2 콘텐츠 필터 작업

작업	설명
격리	**격리**. 정책 격리 영역 중 하나에 보관할 메시지에 플래그를 지정합니다. **중복 메시지**: 메시지 복사본을 지정된 격리에 보내고 계속해서 원본 메시지를 처리합니다. 원본 메시지에는 추가 작업이 적용됩니다.
전달 시 암호화	메시지는 계속 다음 처리 단계로 넘어갑니다. 모든 처리가 완료되면 메시지가 암호화되어 전달됩니다. **암호화 규칙**: 메시지를 항상 암호화하거나 TLS 연결을 통해 보내려는 시도가 처음 실패할 경우에만 암호화합니다. 자세한 내용은 암호화 대체 방법으로 TLS 연결 사용하기, 18-9페이지 항목을 참조하십시오. **암호화 프로파일.** 처리가 완료되면 지정된 암호화 프로파일을 사용하여 메시지를 암호화한 다음 메시지를 전달합니다. 이 작업은 Cisco 암호화 어플라이언스 또는 호스팅되는 키 서비스에 사용됩니다. **제목**. 암호화된 메시지의 제목입니다. 기본적으로 값은 `$Subject`입니다.
콘텐츠별 첨부 파일 제거	**첨부 파일 포함.** 정규식이 포함된 메시지의 모든 첨부 파일을 삭제합니다. 포함된 파일이 정규식 패턴과 일치하는 경우 아카이브 파일(zip, tar)이 삭제됩니다. **스마트 식별자 포함.** 지정된 스마트 식별자가 포함된 메시지에서 모든 첨부 파일을 삭제합니다. **첨부 파일에 콘텐츠 사전의 용어 포함.** 첨부 파일이 정규식이나 <*dictionary name*>이라는 콘텐츠 사전의 용어를 포함하고 있습니까? **필요한 일치 수**. 규칙을 true로 평가하는 데 필요한 일치 수를 지정합니다. 텍스트, 스마트 식별자 또는 콘텐츠 사전 일치에 대해 이 임계값을 지정할 수 있습니다. **대체 메시지.** 선택적 주석을 통해 삭제된 첨부 파일을 대체하는 데 사용된 텍스트를 수정할 수 있습니다. 첨부 파일 바닥글은 메시지에 간단하게 추가됩니다.

표 11-2 콘텐츠 필터 작업 (계속)

작업	설명
파일 정보별 첨부 파일 제거	**파일 이름**. 지정된 정규식과 일치하는 파일 이름을 가진 메시지의 첨부 파일을 모두 삭제합니다. 일치하는 파일이 있는 경우 아카이브 파일 첨부(zip, tar)가 삭제됩니다. **파일 크기**. 원시 인코딩 형식이며 지정된 크기(바이트)보다 크거나 같은 메시지의 첨부 파일을 모두 삭제합니다. 아카이브 파일 또는 압축 파일의 경우 이 작업은 압축되지 않은 크기를 검사하는 대신 실제 첨부 파일 자체의 크기를 검사합니다. **파일 유형**. 파일의 지정된 "지문"과 일치하는 메시지의 첨부 파일을 모두 삭제합니다. 일치하는 파일이 있는 경우 아카이브 파일 첨부(zip, tar)가 삭제됩니다. **MIME 유형**. 지정된 MIME 유형을 가진 메시지의 첨부 파일을 모두 삭제합니다. **이미지 분석 판정**. 지정된 이미지 판정과 일치하는 이미지 첨부 파일의 첨부 파일을 삭제합니다. 유효한 이미지 분석 판정에는 *의심*, *부적절*, *의심 또는 부적절*, *검사할 수 없음* 또는 *정상*이 있습니다. **대체 메시지.** 선택적 주석을 통해 삭제된 첨부 파일을 대체하는 데 사용된 텍스트를 수정할 수 있습니다. 첨부 파일 바닥글은 메시지에 간단하게 추가됩니다.
URL 평판	필터에서 URL 평판 및 URL 범주 작업을 사용하여 메시지의 URL 수정, 15-8페이지 및 URL 필터링 허용 목록 생성, 15-4페이지 항목을 참조하십시오. 평판을 판단할 수 없는 URL에 대한 작업을 지정하려면 "점수 없음"을 사용합니다.
URL 범주	필터에서 URL 평판 및 URL 범주 작업을 사용하여 메시지의 URL 수정, 15-8페이지 및 URL 범주 정보, 15-13페이지 항목을 참조하십시오.
경고문 텍스트 추가	**위**. 고지 사항을 메시지 위에 추가합니다(머리글). **아래.** 고지 사항을 메시지 아래에 추가합니다(바닥글). **참고:** 이 콘텐츠 필터 작업을 사용하려면 고지 사항 텍스트가 이미 생성되어 있어야 합니다. 자세한 내용은 고지 사항 템플릿, 21-12페이지 항목을 참조하십시오.
신종 바이러스 필터 (Outbreak Filter) 검사 우회	이 메시지에 대한 신종 바이러스 필터(Outbreak Filter) 검사를 우회합니다.
DKIM 서명 우회	이 메시지에 대해 DKIM 서명 우회합니다.

표 11-2 콘텐츠 필터 작업 (계속)

작업	설명
사본 발송(Bcc:)	**이메일 주소**. 메시지를 익명으로 지정된 수신자에게 복사합니다. **제목**. 복사한 메시지의 제목을 추가합니다. **반환 경로(선택 사항).** 반환 경로를 지정합니다. **대체 메일 호스트(선택 사항).** 대체 메일 호스트를 지정합니다.
알림	**알림.** 지정된 수신자에게 이 메시지를 보고합니다. 선택적으로 발신자 및 수신자에게 알릴 수 있습니다. **제목**. 복사한 메시지의 제목을 추가합니다. **반환 경로(선택 사항).** 반환 경로를 지정합니다. **템플릿 사용**. 생성한 템플릿에서 템플릿을 선택합니다. **원본 메시지를 첨부 파일로 포함**. 원본 메시지를 첨부 파일로 추가합니다.
수신자 변경	**이메일 주소**. 메시지 수신자를 지정된 이메일 주소로 변경합니다.
다른 호스트로 전송	**메일 호스트**. 메시지의 대상 메일 호스트를 지정된 메일 호스트로 변경합니다. **참고** 이 작업은 안티스팸 검사 엔진에서 스팸으로 분류된 메시지가 격리되지 않도록 합니다. 이 작업은 격리를 재정의하여 지정된 메일 호스트로 전송합니다.
IP 인터페이스에서 전달	**IP 인터페이스에서 발송.** 지정된 IP 인터페이스에서 발송. IP 인터페이스에서 전달 작업은 메시지의 소스 호스트를 지정된 소스로 변경합니다. 소스 호스트는 메시지 전달에 사용되는 IP 인터페이스로 구성됩니다.
헤더 제거	**헤더 이름.** 전달 전 메시지에서 지정된 헤더를 제거합니다.

표 11-2 콘텐츠 필터 작업 (계속)

작업	설명
헤더 추가/편집	**새 헤더를 메시지에 삽입하거나 기존 헤더를 수정.** **헤더 이름**. 새 헤더 또는 기존 헤더의 이름입니다. **새 헤더의 값 지정.** 전달 전 메시지에 새 헤더의 값을 삽입합니다. **기존 헤더 값의 앞에 추가.** 전달 전 기존 헤더 앞에 값을 추가합니다. **기존 헤더 값의 뒤에 추가.** 전달 전 기존 헤더 뒤에 값을 추가합니다. **기존 헤더 값으로 검색 및 교체**. 기존 헤더에서 대체할 값을 찾으려면 **Search for(검색)** 필드에 검색어를 입력합니다. 헤더에 삽입할 값을 **Replace with(바꿀 내용)** 필드에 입력합니다. 정규식을 사용하여 값을 검색할 수 있습니다. 헤더에서 값을 삭제하려면 **Replace with(바꿀 내용)** 필드를 비워 두어야 합니다.
메시지 태그 추가	RSA 이메일 DLP 정책 필터링에 사용할 메시지에 사용자 지정 용어를 삽입합니다. 메시지 태그를 포함하는 메시지로 검사를 제한하도록 RSA 이메일 DLP 정책을 구성할 수 있습니다. 수신자에게는 메시지 태그가 보이지 않습니다. DLP 정책에 메시지 태그를 사용하는 방법에 대한 자세한 내용은 DLP 정책(RSA 이메일 DLP용), 17-5페이지 항목을 참조하십시오.
로그 항목 추가	`INFO` 수준의 IronPort 텍스트 메일 로그에 사용자 지정 텍스트를 삽입합니다. 텍스트는 작업 변수를 포함할 수 있습니다. 로그 항목은 메시지 추적에도 표시됩니다.
전달 시 S/MIME 서명/암호화	전달 중에 메시지에 대한 S/MIME 서명 또는 암호화를 수행합니다. 이는 메시지가 다음 처리 단계로 진행되고 모든 처리 작업이 완료되면 메시지가 서명되거나 암호화되어 전달된다는 의미입니다. **S/MIME 전송 프로파일**: 지정된 S/MIME 전송 프로파일을 사용하여 S/MIME 서명 또는 암호화를 수행합니다. S/MIME 전송 프로필 관리, 19-10페이지 항목을 참조하십시오.
암호화 및 지금 전송(최종 작업)	메시지를 암호화하고 전달하여 이후 처리 작업을 건너뜁니다. **암호화 규칙**: 메시지를 항상 암호화하거나 TLS 연결을 통해 보내려는 시도가 처음 실패할 경우에만 암호화합니다. 자세한 내용은 암호화 대체 방법으로 TLS 연결 사용하기, 18-9페이지 항목을 참조하십시오. **암호화 프로파일.** 지정된 암호화 프로파일을 사용하여 메시지를 암호화한 다음 메시지를 전달합니다. 이 작업은 Cisco 암호화 어플라이언스 또는 호스팅되는 키 서비스에 사용됩니다. **제목**. 암호화된 메시지의 제목입니다. 기본적으로 값은 `$Subject`입니다.

표 11-2 콘텐츠 필터 작업 (계속)

작업	설명
S/MIME 서명/암호화(마지막 조치)	S/MIME 서명 또는 암호화를 수행하고 메시지를 전달하여 이후 처리 작업을 건너뜁니다. **S/MIME 전송 프로파일**: 지정된 S/MIME 전송 프로파일을 사용하여 S/MIME 서명 또는 암호화를 수행합니다. S/MIME 전송 프로필 관리, 19-10페이지 항목을 참조하십시오.
바운스(최종 작업)	발신자에게 다시 메시지를 발송합니다.
나머지 콘텐츠 필터 생략(최종 작업)	메시지를 다음 처리 단계로 전달하여 이후 콘텐츠 필터를 건너뜁니다. 구성에 따라서 메시지를 수신자 또는 격리로 전달하거나 신종 바이러스 필터(Outbreak Filter) 검사를 시작합니다.
삭제(최종 작업)	메시지를 삭제하고 버립니다.

작업 변수

콘텐츠 필터로 처리되는 메시지에 추가되는 헤더는 작업이 실행될 때 원본 메시지의 정보로 자동 대체되는 변수를 포함할 수 있습니다. 이 특수 변수를 *작업 변수*라고 합니다. 어플라이언스는 다음과 같은 작업 변수 집합을 지원합니다.

표 11-3 작업 변수

변수	구문	설명
모든 헤더	`$AllHeaders`	메시지 헤더로 대체됩니다.
본문 크기	`$BodySize`	메시지의 크기(바이트)로 대체됩니다.
날짜	`$Date`	YYYY/MM/DD 형식을 사용하여 현재 날짜로 대체됩니다.
삭제된 파일 이름	`$dropped_filename`	최근에 삭제된 파일 이름만 반환합니다.
삭제된 파일 이름	`$dropped_filenames`	`$filenames`와 동일하지만 삭제된 파일 목록을 표시합니다.
삭제된 파일 형식	`$dropped_filetypes`	`$filetypes`와 동일하지만 삭제된 파일 목록 유형을 표시합니다.
봉투 발신자	`$envelopefrom` or `$envelopesender`	메시지의 봉투 발신자(Envelope From, <MAIL FROM>)로 대체됩니다.
봉투 수신자	`$EnvelopeRecipients`	메시지의 모든 봉투 수신자(Envelope To, <RCPT TO>)로 대체됩니다.
파일 이름	`$filenames`	메시지의 첨부 파일 이름이 쉼표로 구분된 목록으로 대체됩니다.
파일 크기	`$filesizes`	메시지의 첨부 파일 크기가 쉼표로 구분된 목록으로 대체됩니다.
파일 형식	`$filetypes`	메시지의 첨부 파일 유형이 쉼표로 구분된 목록으로 대체됩니다.
필터 이름	`$FilterName`	처리 중인 필터의 이름으로 대체됩니다.

표 11-3 작업 변수 (계속)

변수	구문	설명
GMTimeStamp	`$GMTimeStamp`	GMT를 사용하여 이메일 메시지의 Received: 줄에서 확인되는 현재 시간 및 날짜로 대체됩니다.
HAT 그룹 이름	`$Group`	메시지를 삽입할 때 일치하는 발신자가 속한 발신자 그룹의 이름으로 대체됩니다. 발신자 그룹에 이름이 없는 경우 `">Unknown<"` 문자열이 삽입됩니다.
메일 흐름 정책	`$Policy`	메시지를 삽입할 때 발신자에 적용되는 HAT 정책의 이름으로 대체됩니다. 사전 정의된 정책 이름이 사용된 경우 `">Unknown<"` 문자열이 삽입됩니다.
일치하는 콘텐츠	`$MatchedContent`	콘텐츠-검사 필터를 트리거한 값(또는 여러 개의 값)으로 대체됩니다. 일치하는 콘텐츠는 콘텐츠 사전과 일치하거나 스마트 식별자 또는 정규식과 일치할 수 있습니다.
헤더	`$Header['`*string*`']`	원본 메시지에 일치하는 헤더가 있는 경우 작은따옴표가 붙은 헤더 값으로 대체됩니다. 큰따옴표도 사용될 수 있습니다.
호스트 이름	`$Hostname`	Email Security 어플라이언스의 호스트 이름으로 대체됩니다.
내부 메시지 ID	`$MID`	내부에서 메시지를 식별하는 데 사용되는 메시지 ID 또는 "MID"로 대체됩니다. RFC822 "Message-Id" 값과 혼동하지 않도록 주의합니다($Header를 사용하여 해당 항목 검색).
수신 리스너	`$RecvListener`	메시지를 수신한 리스너의 별칭으로 대체됩니다.
수신 인터페이스	`$RecvInt`	메시지를 수신한 인터페이스의 별칭으로 대체됩니다.
원격 IP 주소	`$RemoteIP`	메시지를 Email Security 어플라이언스로 전송한 시스템의 IP 주소로 대체됩니다.
원격 호스트 주소	`$remotehost`	메시지를 어플라이언스로 전송한 시스템의 호스트 이름으로 대체됩니다.
SenderBase Reputation 점수	`$Reputation`	발신자의 SenderBase Reputation 점수로 대체됩니다. 평판 점수가 없는 경우 `"None"`으로 대체됩니다.
제목	`$Subject`	메시지의 제목으로 대체됩니다.
시간	`$Time`	로컬 시간대의 현재 시간으로 대체됩니다.
타임스탬프	`$Timestamp`	로컬 시간대를 사용하여 이메일 메시지의 Received: 줄에서 확인되는 현재 시간 및 날짜로 대체됩니다.

콘텐츠 기준 메시지 필터링

관련 주제

- 콘텐츠 필터 생성, 11-16페이지
- 기본적으로 모든 수신자에 대해 콘텐츠 필터 활성화, 11-17페이지
- 특정 사용자 그룹의 메시지에 콘텐츠 필터 적용, 11-17페이지
- GUI에서 콘텐츠 필터를 구성할 때의 주의 사항, 11-18페이지

콘텐츠 필터 생성

시작하기 전에

- 콘텐츠 필터와 일치하는 메시지를 암호화하려는 경우 암호화 프로파일을 생성하십시오.
- 일치하는 메시지에 고지 사항을 추가하려면 고지 사항을 생성하는 데 사용할 고지 사항 템플릿을 생성합니다.
- 일치하는 메시지가 있어 사용자에게 알림 메시지를 전송하려면 알림을 생성하는 데 사용할 알림 템플릿을 생성합니다.
- 메시지를 격리하려면 이를 위한 새 정책 격리를 생성하거나 기존 정책 격리를 사용합니다.

절차

1단계 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)**를 클릭합니다.

또는

Mail Policies(메일 정책) > Outgoing Mail Policies(발송 메일 정책)를 클릭합니다.

2단계 **Add Filter(필터 추가)**를 클릭합니다.

3단계 필터의 이름과 설명을 입력합니다.

4단계 (X-REF) **Editable By (Roles)(편집 가능한 사용자(역할))** 링크를 클릭하고 Policy Administrator(정책 관리자)를 선택한 다음 **OK(확인)**를 클릭합니다.

정책 관리자 사용자 역할에 속하는 위임 관리자는 이 콘텐츠 필터를 편집하고 메일 정책에 사용할 수 있습니다.

5단계 (선택 사항) 필터를 트리거하기 위한 조건을 추가합니다.

a. **Add Condition(조건 추가)**을 클릭합니다.

b. 조건 유형을 선택합니다.

c. 조건의 규칙을 정의합니다.

d. **OK(확인)를** 클릭합니다.

e. 필터에 추가할 추가적인 조건에 대해 이러한 단계를 반복합니다. 콘텐츠 필터에 대해 하나 이상의 조건을 정의하는 경우 콘텐츠 필터가 일치하는 것으로 간주하려면 정의된 작업 *모두*(즉, 논리적 AND)가 적용되어야 하는지, 아니면 정의된 작업 중 *하나*(논리적 OR)가 적용되어야 하는지 정의할 수 있습니다.

참고 조건을 추가하지 않을 경우 어플라이언스는 필터와 연결된 메일 정책 중 하나와 일치하는 메시지에 대해 콘텐츠 필터 작업을 수행합니다.

6단계 필터 조건과 일치하는 메시지에 대해 어플라이언스가 수행할 작업을 추가합니다.

a. **Add Action(작업 추가)**을 클릭합니다.

b. 작업 유형을 선택합니다.

c. 작업을 정의합니다.

d. **OK(확인)를** 클릭합니다.

e. 어플라이언스에서 수행시킬 추가적인 작업에 대해 이전 단계를 반복합니다.

f. 여러 작업의 경우 어플라이언스에서 메시지에 적용할 작업을 순서대로 정렬합니다. 필터당 하나의 "최종" 작업만 있을 수 있으며 AsyncOS는 최종 작업을 순서 끝으로 자동으로 이동합니다.

7단계 변경사항을 제출하고 커밋합니다.

다음 작업

- 기본 수신 또는 발송 메일 정책에서 콘텐츠 필터를 활성화할 수 있습니다.
- 특정 사용자 그룹의 메일 정책에서 콘텐츠 필터를 활성화할 수 있습니다.

기본적으로 모든 수신자에 대해 콘텐츠 필터 활성화

절차

1단계 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)**를 클릭합니다.

또는

Mail Policies(메일 정책) > Outgoing Mail Policies(발송 메일 정책)를 클릭합니다.

2단계 기본 정책 행에서 콘텐츠 필터 보안 서비스 링크를 클릭합니다.

3단계 Content Filters(콘텐츠 필터) 보안 서비스 페이지에서 기본 정책의 콘텐츠 필터 값을 "Disable Content Filters(콘텐츠 필터 사용 안 함)"에서 "Enable Content Filters (Customize settings)(콘텐츠 필터 사용(설정 사용자 지정))"으로 변경합니다.

마스터 목록에 정의된 콘텐츠 필터(콘텐츠 필터 개요, 11-1페이지에서 생성함)가 이 페이지에 표시됩니다. 값을 "Enable Content Filters (Customize settings)(콘텐츠 필터 사용(설정 사용자 지정))"로 변경하면 각 필터의 확인란이 활성화됩니다.

4단계 활성화할 각 콘텐츠 필터에 대해 **Enable(활성화)** 확인란을 선택합니다.

5단계 변경사항을 제출하고 커밋합니다.

특정 사용자 그룹의 메시지에 콘텐츠 필터 적용

시작하기 전에

- 콘텐츠 필터를 사용할 메시지를 소유하는 사용자 그룹의 수신 또는 발송 메일 정책을 생성합니다. 자세한 내용은 발신자 및 수신자 그룹에 대한 메일 정책 생성, 10-7페이지 항목을 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)**를 클릭합니다.

또는

Mail Policies(메일 정책) > Outgoing Mail Policies(발송 메일 정책)를 클릭합니다.

2단계 콘텐츠 필터를 적용할 메일 정책에 대한 콘텐츠 필터 보안 서비스(콘텐츠 필터 열) 링크를 클릭합니다.

3단계 Content Filters security service(콘텐츠 필터) 보안 서비스 페이지에서 Policy: Engineering(정책: 엔지니어링)의 콘텐츠 필터 값을 "Enable Content Filtering (Inherit default policy settings)(콘텐츠 필터 사용(기본 정책 설정 상속))"에서 "Enable Content Filters (Customize settings)(콘텐츠 필터 사용(설정 사용자 지정))"로 변경합니다.

4단계 사용할 콘텐츠 필터의 확인란을 선택합니다.

5단계 변경사항을 제출하고 커밋합니다.

GUI에서 콘텐츠 필터를 구성할 때의 주의 사항

- 콘텐츠 필터를 생성하는 경우 조건을 지정할 필요가 없습니다. 작업이 정의되지 않은 경우 정의된 작업이 항상 규칙에 적용됩니다. (조건을 지정하지 않는 것은 `true()` 메시지 필터 규칙을 사용하는 것과 같습니다. 콘텐츠 필터가 정책에 적용되는 경우 모든 메시지가 일치됩니다.)
- 콘텐츠 필터에 사용자 지정 사용자 역할을 할당하지 않은 경우 콘텐츠 필터는 공용으로 사용되거나 위임 관리자가 메일 정책에 사용할 수 있습니다. 위임 관리자 및 콘텐츠 필터에 대한 자세한 내용은 "일반 관리 작업" 장을 참조하십시오.
- 콘텐츠 필터가 사용자 지정 사용자 역할에 할당된 경우에도 관리자와 운영자는 어플라이언스에서 모든 콘텐츠 필터를 보거나 편집할 수 있습니다.
- 필터 규칙 및 작업에 대한 텍스트를 입력하는 경우 다음 메타 문자는 정규식 일치에서 특수한 의미가 있습니다. `. ^ $ * + ? { [ ] \ | ( )`

  정규식을 사용하지 않으려는 경우 '\'(백슬래시)를 사용하여 이러한 문자를 이스케이프해야 합니다. 예: "*Warning*"
- "무해한" 콘텐츠 필터를 생성하여 메시지 분리 및 콘텐츠 필터를 테스트할 수 있습니다. 예를 들어 "전달"이 유일한 작업인 콘텐츠 필터를 생성할 수 있습니다. 이 콘텐츠 필터는 메일 처리에 영향을 주지 않지만, 이 필터를 사용하여 Email Security Manager 정책 처리가 시스템의 다른 요소(예: 메일 로그)에 어떤 영향을 미치는지 테스트할 수 있습니다.
- 이와 반대로, 수신 또는 발송 콘텐츠 필터의 "마스터 목록" 개념을 사용하여 어플라이언스에서 취급되는 모든 메일에 대한 메시지 처리에 즉시 영향을 미치는 매우 강력하고 광범위한 콘텐츠 필터를 생성할 수 있습니다. 이를 위한 프로세스는 다음과 같습니다.
  - Incoming or Outgoing Content Filters(수신 또는 발송 콘텐츠 필터) 페이지에서 순서가 1인 새 콘텐츠 필터를 생성합니다.
  - Incoming or Outgoing Mail Policies(수신 또는 발송 메일 정책) 페이지에서 기본 정책에 대한 새 콘텐츠 필터를 활성화합니다.
  - 나머지 모든 정책에 대해 콘텐츠 필터를 활성화합니다.

- 콘텐츠 필터에서 사용할 수 있는 Bcc: 및 격리 작업은 생성한 격리의 보존 설정을 결정하는 데 도움이 될 수 있습니다. (30 장, "정책, 바이러스 및 신종 바이러스 격리" 참조.) 정책 격리 내부 및 외부의 메일 흐름을 시뮬레이션하는 필터를 생성하여 메시지가 시스템에서 너무 빨리 해제(즉, 격리 영역이 할당된 디스크 공간을 지나치게 빠르게 채우지 못함)되지 않도록 할 수 있습니다.
- "전체 메시지" 조건의 경우 Scan Behavior(검사 동작) 페이지 또는 `scanconfig` 명령과 동일한 설정을 사용하므로 메시지 헤더를 검사하지 않습니다. "전체 메시지"를 선택하면 메시지 본문 및 첨부 파일만 검사됩니다. 특정 헤더 정보를 검색하려면 "제목" 또는 "헤더" 조건을 사용하십시오.
- 어플라이언스에 LDAP 서버가 구성된 경우(즉, `ldapconfig` 명령을 사용하여 특정 LDAP 서버에 특정 문자열이 포함된 쿼리를 수행하도록 어플라이언스 구성) LDAP 쿼리로 사용자를 구성하면 GUI에만 나타납니다.
- 리소스가 사전 구성되지 않은 경우 콘텐츠 필터 규칙 빌더의 일부 섹션은 GUI에 표시되지 않습니다. 예를 들어 알림 템플릿 및 메시지 고지 사항이 이전에 Text Resources(텍스트 리소스) 페이지 또는 CLI의 `textconfig` 명령을 사용하여 구성되지 않았다면 옵션으로 표시되지 않습니다.
- 콘텐츠 필터 기능에서는 음 문자 인코딩의 텍스트를 인식, 포함하고 검사할 수 있습니다.
  - 유니코드(UTF-8)
  - 유니코드(UTF-16)
  - 서유럽어/라틴어-1(ISO 8859-1)
  - 서유럽어/라틴어-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 필터에서 여러 문자 집합을 결합하여 사용할 수 있습니다. 여러 문자 인코딩으로 텍스트를 표시하고 입력하기 위한 지원이 필요한 경우 웹 브라우저 설명서를 참조하십시오. 대부분의 브라우저는 여러 문자 집합을 동시에 렌더링할 수 있습니다.
- Incoming or Outgoing Content Filters(수신 또는 발송 콘텐츠 필터) 요약 페이지에서 "Description(설명)", "Rules(규칙)" 및 "Policies(정책)" 링크를 사용하여 콘텐츠 필터에 표시되는 보기를 변경합니다.
  - **Description(설명)** 보기에는 각 콘텐츠 필터의 설명 필드에 입력한 텍스트가 표시됩니다. (이는 기본 보기입니다.)
  - **Rules(규칙)** 보기에는 규칙 빌더 페이지에서 빌드된 규칙 및 정규식이 표시됩니다.
  - **Policies(정책)**에는 각 콘텐츠 필터가 활성화된 정책이 표시됩니다.

그림 11-1 링크를 사용하여 콘텐츠 필터에 대한 설명, 규칙 및 정책 전환

Incoming Content Filters

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	scan_for_confidential	scan_for_confidential: if (body-contains("confidential")) { quarantine ("Policy"); bcc ("hr@example.com", "[message matched confidential filter]"); }		
2	no_mp3s	no_mp3s: if (true) { drop-attachments-by-filetype("mp3", "mp3 deleted"); }		
3	ex_employee	ex_employee: if (rcpt-to == "^doug@") { notify-copy ("$EnvelopeSender", "message bounced for ex-employee of example.com"); bounce(); }		
4	drop_large_attachments	drop_large_attachments: if (true) { drop-attachments-by-size(5242880, "This attachment was too big!"); }		

안티바이러스

안티바이러스 검사 개요

Cisco 어플라이언스에는 타사인 Sophos 및 McAfee의 바이러스 검사 엔진이 통합되어 있습니다. 이러한 바이러스 검사 엔진 중 하나 또는 두 가지 모두를 사용하여 메시지에 바이러스가 있는지 검사할 수 있도록 Cisco 어플라이언스용 라이센스 키를 획득할 수 있습니다. 다음 두 안티바이러스 검사 엔진 중 하나를 사용하여 바이러스를 검사하도록 어플라이언스를 구성할 수 있습니다.

McAfee 및 Sophos 엔진에는 특정 위치의 파일, 프로세스 및 파일에서 발견된 데이터와의 패턴 일치 바이러스 정의를 검사하는 데 필요한 프로그램 로직이 포함되어 있습니다. 이러한 프로그램 로직은 암호를 해독하고, 에뮬레이트된 환경에서 바이러스 코드를 실행하고, 추론 기술을 적용하여 새 바이러스를 인식하고 올바른 파일에서 감염 코드를 제거하는 데에도 사용됩니다.

메시지에서 바이러스를 검사(일치하는 수신 또는 발송 메일 정책 기반)하고, 바이러스가 발견되는 경우 메시지에 대해 서로 다른 작업(바이러스 메시지 "복구", 제목 헤더 수정, 다른 X-헤더 추가, 대체 주소 또는 메일 호스트로 메시지 전송, 메시지 보관 또는 메시지 삭제 포함)을 수행하도록 어플라이언스를 구성할 수 있습니다.

이 기능이 활성화된 경우, 안티스팸 검사 직후에 어플라이언스의 "작업 큐"에서 바이러스 검사를 수행합니다. (이메일 파이프라인 및 보안 서비스, 4-7페이지 참조.)

기본적으로 기본 수신 및 발송 메일 정책에 대해 바이러스 검사가 활성화됩니다.

관련 주제

- 평가 키, 12-2페이지
- 여러 안티바이러스 검사 엔진을 사용한 메시지 검사, 12-2페이지

평가 키

Cisco 어플라이언스에는 30일 평가 키가 함께 제공되며 각 키는 안티바이러스 검사 엔진에서 사용할 수 있습니다. 시스템 설치 마법사 또는 Security Services(보안 서비스) > Sophos/McAfee Anti-Virus(Sophos/McAfee 안티바이러스) 페이지(GUI)에서 라이센스 계약에 액세스하거나 `antivirusconfig` 또는 `systemsetup` 명령(CLI)을 실행하여 평가 키를 활성화합니다. 계약에 동의하면 기본적으로 기본 수신 및 발송 메일 정책에 대해 안티바이러스 검사 엔진이 활성화됩니다. 30일 평가 기간 이후에 이 기능을 사용하는 방법에 대한 자세한 내용은 Cisco 영업 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, 33-5페이지 참조.)

여러 안티바이러스 검사 엔진을 사용한 메시지 검사

AsyncOS에서는 여러 안티바이러스 검사 엔진을 사용하여 메시지를 검사(멀티레이어 안티바이러스 검사)할 수 있습니다. 메일 정책마다 라이센스가 있는 안티바이러스 검사 엔진 중 하나 또는 두 가지 모두를 사용하도록 Cisco 어플라이언스를 구성할 수 있습니다. 예를 들어 경영진을 대상으로 메일 정책을 생성하고 Sophos 및 McAfee 엔진 모두를 사용하여 메일을 검사하도록 해당 정책을 구성할 수 있습니다.

여러 검사 엔진을 사용하여 메시지를 검사하면 Sophos 및 McAfee 안티바이러스 검사 엔진의 이점을 결합하여 "심층 보호"를 구현할 수 있습니다. 각 엔진의 안티바이러스 캡처 속도는 탁월하지만, 각 엔진은 바이러스를 탐지하기 위해 별도의 기술 기반을 활용(McAfee Anti-Virus 필터링, 12-5페이지 및 Sophos Anti-Virus 필터링, 12-2페이지에서 설명됨)하므로 다중 검사는 더욱 효과적인 방식입니다. 여러 검사 엔진을 사용하면 시스템 처리량이 감소할 수 있습니다. 자세한 내용은 Cisco 지원 담당자에게 문의하십시오.

바이러스 검사 순서는 구성할 수 없습니다. 다중 계층 안티바이러스 검사를 사용하는 경우 McAfee 엔진이 먼저 바이러스를 검사하고 Sophos 엔진이 두 번째로 바이러스를 검사합니다. McAfee 엔진에서 메시지에 바이러스가 없다고 확인되면 Sophos 엔진이 메시지를 검사하고 두 번째 보호 계층을 추가합니다. McAfee 엔진에서 메시지에 바이러스가 포함되어 있는 것으로 확인되면 Cisco 어플라이언스는 Sophos 검사를 건너뛰고 사용자가 구성한 설정에 따라 바이러스 메시지에 대한 작업을 수행합니다.

Sophos Anti-Virus 필터링

Cisco 어플라이언스에는 Sophos, Plc.의 바이러스 검사 기술이 통합되어 있습니다. Sophos Anti-Virus는 플랫폼 간 안티바이러스 보호, 탐지 및 치료 기능을 제공합니다.

Sophos Anti-Virus는 파일에서 바이러스, 트로이 목마 및 웜을 검사하는 바이러스 탐지 엔진을 제공합니다. 이러한 프로그램들은 일반적으로 *악성코드*로 분류되며, 이는 "악성 소프트웨어"를 의미합니다. 모든 종류의 악성코드 간 유사성으로 인해 안티바이러스 스캐너가 바이러스뿐 아니라 모든 종류의 악성 소프트웨어를 탐지하고 제거할 수 있습니다.

관련 주제

- 바이러스 탐지 엔진, 12-3페이지
- 바이러스 검사, 12-3페이지
- 탐지 방법, 12-3페이지
- 바이러스 설명, 12-4페이지
- Sophos 경고, 12-4페이지
- 바이러스가 발견된 경우, 12-4페이지

바이러스 탐지 엔진

Sophos 바이러스 탐지 엔진은 Sophos Anti-Virus 기술의 핵심입니다. 이 엔진은 Microsoft의 COM(Component Object Model)과 유사한 독점적 아키텍처를 사용하며, 정의된 인터페이스와 다수의 객체로 구성되어 있습니다. 이 엔진에 사용되는 모듈식 파일 정리 시스템은 별도의 자체 포함 동적 라이브러리를 기반으로 하며, 라이브러리마다 각기 다른 "스토리지 클래스"(예: 파일 유형)를 처리합니다. 이러한 방식을 사용하여 유형과 관계없이 일반 데이터 소스에 바이러스 검사 작업을 적용할 수 있습니다.

데이터를 로드하고 검색할 수 있는 특수 기술 덕분에 엔진의 검사 속도가 매우 빨라집니다. 엔진에 통합된 기능은 다음과 같습니다.

- 다형성 바이러스를 탐지하는 전체 코드 에뮬레이터
- 아카이브 파일 내부를 검사할 수 있는 온라인 압축 해제 프로그램
- 매크로 바이러스를 탐지하고 치료하는 OLE2 엔진

Cisco 어플라이언스에는 SAV 인터페이스를 통한 바이러스 엔진이 통합되었습니다.

바이러스 검사

넓은 의미에서, 분류자에는 찾을 위치가 포함되어 있고 바이러스 데이터베이스에는 찾을 항목이 저장되어 있습니다. 이 두 가지 주요 구성 요소가 강력하게 결합하여 엔진 검색 기능을 관리합니다. 이 엔진은 확장명을 사용하는 대신 유형별로 파일을 분류합니다.

바이러스 엔진은 시스템에 수신된 메시지의 본문 및 첨부 파일에서 바이러스를 검색합니다. 첨부 파일의 파일 유형은 검사를 결정하는 데 도움이 됩니다. 예를 들어 메시지에 첨부된 파일이 실행 파일인 경우 엔진은 실행 파일 코드가 시작된 위치를 알려주는 헤더를 검사하고 찾습니다. 파일이 Word 문서인 경우 엔진은 매크로 스트림을 확인합니다. 메일 메시징에 사용되는 형식인 MIME 파일인 경우에는 첨부 파일이 저장된 위치를 확인합니다.

탐지 방법

바이러스 탐지 방법은 바이러스 유형에 따라 다릅니다. 검사 프로세스 중에 엔진은 각 파일을 분석하고 유형을 식별한 다음 관련 기술을 적용합니다. 모든 방법의 근간이 되는 기본 개념은 특정 유형의 명령 또는 특정 명령 순서를 찾는 것입니다.

관련 주제

- 패턴 일치, 12-3페이지
- 추론, 12-4페이지
- 에뮬레이션, 12-4페이지

패턴 일치

패턴 일치 기술에서 엔진은 특정 코드 시퀀스를 알고 있으며 코드를 바이러스로 식별하는 정확한 일치 항목을 찾습니다. 엔진은 유사한 코드 시퀀스를 찾긴 하지만 알려진 바이러스 코드 시퀀스와 정확히 일치하지 않는 코드 시퀀스를 찾는 경우도 자주 있습니다. 검사 중에 비교 대상 파일에 대한 설명을 생성하는 것과 관련하여 Sophos 바이러스 연구원은 아래 설명된 추론 방식을 통해 엔진이 원본 바이러스는 물론 파생 바이러스도 발견할 수 있도록 식별 코드를 최대한 일반화하였습니다.

추론

바이러스 엔진에는 기본 패턴 일치 기술과 추론(특정 규칙이 아닌 일반 규칙을 사용하는 기법) 기술을 결합되어 있어 Sophos 연구원이 해당 계열에서 한 바이러스만 분석하도록 설계했음에도 불구하고 동일한 계열의 여러 바이러스를 탐지할 수 있습니다. 이러한 기술을 통해 한 바이러스의 여러 변종을 포착하는 단일 설명을 생성할 수 있습니다. Sophos는 다른 방법을 통해 추론을 조정하면서 긍정 오류의 발생을 최소화합니다.

에뮬레이션

에뮬레이션은 바이러스 엔진에서 다형성 바이러스에 적용되는 기술입니다. 다형성 바이러스란 자신을 숨기기 위해 자신을 변환하는 암호화된 바이러스입니다. 일정한 바이러스 코드는 보이지 않으며 바이러스가 전염될 때마다 자신을 다르게 암호화합니다. 실행 시 자동으로 암호 해독됩니다. 바이러스 탐지 엔진의 에뮬레이터는 DOS 및 Windows 실행 파일에 사용되지만, 다형성 매크로 바이러스는 Sophos의 바이러스 기술 언어로 작성된 탐지 코드로 발견됩니다.

이 암호 해독 결과 실제 바이러스 코드가 출력되며, 이 출력 결과는 에뮬레이터에서 실행된 후에 Sophos 바이러스 탐지 엔진으로 탐지됩니다.

검사를 위해 엔진에 전송되는 실행 파일은 에뮬레이터에서 실행되며, 에뮬레이터는 바이러스 본문의 암호 해독을 추적하면서 메모리에 이를 기록합니다. 일반적으로 바이러스 진입 지점은 파일의 시작 부분에 있으며 이 지점이 먼저 실행됩니다. 대부분의 경우 바이러스를 인식하기 위해 약간의 바이러스 본문만 암호 해독하면 됩니다. 바이러스가 없는 실행 파일은 일부 명령 처리 후에 에뮬레이션을 중지하므로 오버헤드가 감소합니다.

에뮬레이터는 제한된 영역에서 실행되므로 코드가 바이러스로 판명되지 않을 경우 바이러스는 어플라이언스를 감염시키지 않습니다.

바이러스 설명

Sophos는 신뢰할 수 있는 다른 안티바이러스 업체와 매달 바이러스 정보를 교환합니다. 또한, 고객은 매달 수천 개에 달하는 의심스러운 파일을 직접 Sophos에 보내고 있으며, 그중 약 30%가 바이러스로 판명됩니다. 각 샘플은 매우 안전한 바이러스 연구소에서 철저하게 분석되어 바이러스 여부가 판정됩니다. 새로 발견된 바이러스 또는 바이러스 그룹의 경우 Sophos는 설명을 작성합니다.

Sophos 경고

Sophos Anti-Virus 검사 기능을 사용하는 고객은 Sophos 사이트 (http://www.sophos.com/virusinfo/notifications/)에서 Sophos 경고 서비스에 가입하는 것이 좋습니다. 서비스에 가입하면 Sophos에서 직접 경고를 수신할 수 있고 최신 신종 바이러스 및 사용 가능한 솔루션에 대한 알림을 받게 됩니다.

바이러스가 발견된 경우

바이러스가 탐지되면 Sophos Anti-Virus는 파일을 복구(치료)할 수 있습니다. Sophos Anti-Virus는 일반적으로 바이러스가 발견된 파일을 복구할 수 있습니다. 파일 복구 후 해당 파일을 위험 없이 사용할 수 있습니다. 수행되는 정확한 조치는 바이러스마다 다릅니다.

감염된 파일을 항상 원래 상태로 복구할 수는 없으므로 감염 치료에 관해서는 제한 사항이 있습니다. 일부 바이러스는 실행 가능한 프로그램 일부를 덮어쓰는데, 이러한 프로그램은 복원되지 않습니다. 이러한 경우 사용자는 복구할 수 없는 첨부 파일이 포함된 메시지를 처리하는 방법을 정의합

니다. 이메일 보안 기능, 즉 Mail Policies(메일 정책) > Incoming or Outgoing Mail Policies(수신 또는 발송 메일 정책) 페이지(GUI)나 `policyconfig -> antivirus` 명령(CLI)을 사용하여 수신자별로 설정을 구성합니다. 이러한 설정 구성에 대한 자세한 내용은 사용자에 대한 바이러스 검사 작업 구성, 12-7페이지 항목을 참조하십시오.

McAfee Anti-Virus 필터링

McAfee® 검사 엔진은 다음을 수행합니다.

- 파일의 데이터와 바이러스 서명의 패턴 일치를 통해 파일을 검사합니다.
- 에뮬레이트된 환경에서 바이러스 코드의 암호를 해독하고 해당 코드를 실행합니다.
- 추론 기술을 적용하여 새 바이러스를 인식합니다.
- 파일에서 감염 코드를 제거합니다.

관련 주제

- 바이러스 시그니처 패턴 일치, 12-5페이지
- 암호화된 다형성 바이러스 탐지, 12-5페이지
- 추론 분석, 12-6페이지
- 바이러스가 발견된 경우, 12-6페이지

바이러스 시그니처 패턴 일치

McAfee는 검사 엔진에 안티바이러스 정의(DAT) 파일을 사용하여 특정 바이러스, 바이러스 유형 또는 사용자 동의 없이 설치된 소프트웨어를 탐지합니다. 또한, 파일의 알려진 위치를 시작으로 바이러스 시그니처를 검색하여 단순 바이러스를 탐지할 수 있습니다. 주로 파일의 일부만 검색하여 파일에 바이러스가 없는지 확인합니다.

암호화된 다형성 바이러스 탐지

복합 바이러스는 널리 통용되는 두 가지 기술을 사용해 서명 검사 바이러스 탐지를 회피합니다.

- **암호화**. 바이러스 내의 데이터는 암호화되어 있으므로 안티바이러스 스캐너는 바이러스의 컴퓨터 코드 또는 메시지를 인식할 수 없습니다. 바이러스가 활성화되면 스스로 동작하는 버전으로 변환한 후 실행됩니다.
- **다형성**. 이 프로세스는 바이러스가 스스로 복제하여 모양을 바꾼다는 점을 제외하면 암호화와 비슷합니다.

이러한 바이러스에 대응하기 위해 엔진은 에뮬레이션 기술을 사용합니다. 엔진이 파일에 바이러스가 있다고 의심하면 인위적 환경을 만들어 바이러스가 스스로 디코딩되고 그 실체가 드러날 때까지 아무런 영향 없이 실행됩니다. 그 다음, 이 엔진은 평소와 같이 바이러스 시그니처를 검사하여 바이러스를 식별할 수 있습니다.

추론 분석

새 바이러스인 경우 해당 바이러스 시그니처가 아직 알려지지 않았기 때문에 엔진에서 바이러스 시그니처를 사용하여 새 바이러스를 탐지할 수 없습니다. 따라서 엔진은 추가로 추론 분석을 사용합니다.

바이러스가 포함된 프로그램, 문서 또는 이메일 메시지에는 고유한 특징이 있는 경우가 많습니다. 프롬프트 없이 파일을 수정하거나 메일 클라이언트를 호출하거나 다른 방법으로 스스로를 복제할 수도 있습니다. 이 엔진은 프로그램 코드를 분석하여 이러한 종류의 컴퓨터 명령을 검색합니다. 바이러스로 보이지 않는 올바른 동작도 검색하고 사용자가 작업하기 전에 확인하게 하여 거짓 경보 발효를 예방합니다.

이러한 기술을 사용하여 다양한 신종 바이러스를 탐지할 수 있습니다.

바이러스가 발견된 경우

바이러스가 탐지되면 McAfee는 파일을 복구(치료)할 수 있습니다. McAfee는 일반적으로 바이러스가 발견된 파일을 복구할 수 있습니다. 파일 복구 후 해당 파일을 위험 없이 사용할 수 있습니다. 수행되는 정확한 조치는 바이러스마다 다릅니다.

가끔 감염된 파일을 원래 상태로 되돌릴 수 없는 경우가 있으므로 감염된 파일 치료에는 제한 사항이 있습니다. 일부 바이러스는 실행 가능한 프로그램 일부를 덮어쓰는데, 이러한 프로그램은 복원되지 않습니다. 이러한 경우 사용자는 복구할 수 없는 첨부 파일이 포함된 메시지를 처리하는 방법을 정의합니다. 이메일 보안 기능, 즉 Mail Policies(메일 정책) > Incoming or Outgoing Mail Policies(수신 또는 발송 메일 정책) 페이지(GUI)나 `policyconfig -> antivirus` 명령(CLI)을 사용하여 수신자별로 설정을 구성합니다. 이러한 설정 구성에 대한 자세한 내용은 사용자에 대한 바이러스 검사 작업 구성, 12-7 페이지 항목을 참조하십시오.

바이러스를 검사하도록 어플라이언스를 구성하는 방법

표 12-1 메시지에서 바이러스를 검사하는 방법

	수행할 작업	추가 정보
1단계	Email Security 어플라이언스의 안티바이러스 검사를 활성화합니다.	바이러스 검사 및 구성 전역 설정 사용, 12-7페이지
2단계	바이러스 검사 대상 메시지를 소유하는 사용자 그룹을 정의합니다.	발신자 및 수신자 그룹에 대한 메일 정책 생성, 10-7페이지
3단계	(선택 사항) 바이러스 격리에서 메시지를 처리하는 방법을 구성합니다.	정책, 바이러스 및 신종 바이러스 격리 구성, 30-5페이지
4단계	어플라이언스에서 바이러스에 감염된 메시지를 처리하는 방법을 결정합니다.	사용자에 대한 바이러스 검사 작업 구성, 12-7페이지
5단계	정의한 사용자 그룹의 안티바이러스 검사 규칙을 구성합니다.	서로 다른 발신자 및 수신자 그룹에 대한 안티바이러스 정책 구성, 12-13페이지
6단계	(선택 사항) 이메일 메시지를 전송하여 구성을 테스트합니다.	어플라이언스에 이메일을 전송하여 안티바이러스 검사 테스트, 12-17페이지

관련 주제

- 바이러스 검사 및 구성 전역 설정 사용, 12-7페이지
- 사용자에 대한 바이러스 검사 작업 구성, 12-7페이지
- 서로 다른 발신자 및 수신자 그룹에 대한 안티바이러스 정책 구성, 12-13페이지
- 안티바이러스 구성에 대한 참고 사항, 12-14페이지
- 안티바이러스 작업 흐름도, 12-16페이지

바이러스 검사 및 구성 전역 설정 사용

시스템 설치 마법사를 실행할 때 바이러스 검사 엔진을 활성화할 가능성이 있습니다. 활성화 여부와 관계없이 다음 절차를 사용하여 설정을 구성할 수 있습니다.

참고 기능 키에 따라 Sophos나 McAfee 또는 두 가지 모두를 활성화할 수 있습니다.

절차

1단계 Security Services(보안 서비스) > McAfee 페이지로 이동합니다.

또는

Security Services(보안 서비스) > Sophos 페이지로 이동합니다.

2단계 **Enable(활성화)**을 클릭합니다.

참고 **Enable(활성화)**을 클릭하면 어플라이언스 전역에서 해당 기능을 사용할 수 있습니다. 그러나 나중에 Mail Policies(메일 정책)에서 수신자별 설정을 활성화해야 합니다.

3단계 라이센스 계약을 읽은 후 페이지 하단으로 스크롤하고 **Accept(동의)**를 클릭하여 계약에 동의합니다.

4단계 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

5단계 바이러스 검사의 최대 시간제한 값을 선택합니다.

시스템에서 메시지의 안티바이러스 검사를 중단하기 전까지의 시간제한 값을 구성합니다. 기본값은 60초입니다.

6단계 변경사항을 제출하고 커밋합니다.

다음 작업

수신자별로 안티바이러스 설정을 구성합니다. 사용자에 대한 바이러스 검사 작업 구성, 12-7페이지 항목을 참조하십시오.

사용자에 대한 바이러스 검사 작업 구성

Cisco 어플라이언스에 통합된 바이러스 검사 엔진은 Email Security Manager 기능을 사용하여 구성한 정책(구성 옵션)을 바탕으로 수신 및 발송 메일 메시지의 바이러스를 처리합니다. 이메일 보안 기능, 즉 Mail Policies(메일 정책) > 수신 또는 발송 메일 정책 페이지(GUI)나 `policyconfig > antivirus` 명령(CLI)으로 수신자별로 안티바이러스 작업을 활성화합니다.

관련 주제

- 메시지 검사 설정, 12-8페이지
- 메시지 처리 설정, 12-8페이지
- 메시지 처리 작업에 대한 설정 구성, 12-9페이지

메시지 검사 설정

- 바이러스만 검사:

  시스템이 처리하는 메시지의 바이러스를 검사합니다. 감염된 첨부 파일에 대한 복구는 시도하지 *않습니다*. 바이러스가 있거나 복구할 수 없는 메시지의 경우 첨부 파일을 삭제하고 메일을 전달할지 여부를 선택할 수 있습니다.

- 바이러스 검사 후 복구:

  시스템이 처리하는 메시지의 바이러스를 검사합니다. 첨부 파일에서 바이러스가 발견되면 시스템은 첨부 파일 "복구"를 시도합니다.

- 첨부 파일 삭제

  감염된 첨부 파일을 삭제하도록 선택할 수 있습니다.

  안티바이러스 검사 엔진이 메시지에서 감염된 첨부 파일을 검사하여 *삭제*한 경우 이 첨부 파일은 "제거된 첨부 파일"이라는 새 첨부 파일로 교체됩니다. 첨부 파일 유형은 text/plain이며 다음 내용이 포함되어 있습니다.

```
This attachment contained a virus and was stripped.

     Filename: filename

 Content-Type: application/filetype
```

  허용되지 않는 첨부 파일에 감염되어 메시지가 어떤 방식으로든 수정된 경우에는 항상 사용자에게 알림이 제공됩니다. 두 번째 알림 작업도 구성할 수 있습니다(알림 전송, 12-11페이지 참조). 감염된 첨부 파일을 삭제하도록 선택한 경우 메시지 수정을 알리는 알림 작업은 필요하지 *않습니다*.

- X-IronPort-AV 헤더

  어플라이언스의 안티바이러스 검사 엔진에서 처리된 모든 메시지에는 `X-IronPort-AV:` 헤더가 추가됩니다. 이 헤더는 안티바이러스 구성 관련 문제를 디버깅할 때 특히 "검사할 수 없음"으로 판명된 메시지의 경우 추가 정보를 제공합니다. 검사되는 메시지에 X-IronPort-AV 헤더를 포함할지 여부를 선택할 수 있습니다. 이 헤더를 포함하는 것이 권장됩니다.

메시지 처리 설정

리스너가 수신하는 4가지 개별 메시지 클래스를 처리하되 메시지마다 별도의 작업이 이루어지도록 바이러스 검사 엔진을 구성할 수 있습니다. 그림 12-1에서는 바이러스 검사 엔진이 활성화된 경우 시스템이 수행하는 작업에 대한 요약 정보를 소개합니다.

다음의 메시지 유형마다 어떤 작업을 수행할지 선택할 수 있습니다. 다음에서 작업에 대해 설명합니다(메시지 처리 작업에 대한 설정 구성, 12-9페이지 참조). 예를 들어 바이러스에 감염된 메시지에 대한 안티바이러스 설정을 구성하여 감염된 첨부 파일을 삭제하고 이메일 제목을 수정하고 사용자 지정 경고를 메시지 수신자에게 전송할 수 있습니다.

관련 주제

- 복구된 메시지 처리, 12-9페이지
- 암호화된 메시지 처리, 12-9페이지
- 검사할 수 없는 메시지 처리, 12-9페이지
- 바이러스에 감염된 메시지 처리, 12-9페이지

복구된 메시지 처리

메시지를 완전히 검사한 후 모든 바이러스가 치료되거나 제거되면 메시지는 *복구*된 것으로 간주됩니다. 이러한 메시지는 있는 그대로 전달됩니다.

암호화된 메시지 처리

메시지의 암호화되었거나 보호된 필드로 인해 엔진에서 검사를 완료할 수 없는 경우 해당 메시지는 *암호화*된 것으로 간주됩니다. 암호화 상태로 표시된 메시지도 복구할 수 있습니다.

암호화 탐지 메시지 필터 규칙(암호화 탐지 규칙, 9-31페이지 참조)과 "암호화된" 메시지에 대한 바이러스 검사 작업에는 차이점이 있습니다. PGP 또는 S/MIME로 암호화된 메시지의 경우 암호화된 메시지 필터 규칙은 "true"로 평가됩니다. 해당 규칙은 PGP 및 S/MIME로 암호화된 데이터만 탐지할 수 있습니다. 비밀번호로 보호된 ZIP 파일 또는 암호화된 콘텐츠가 포함된 Microsoft Word 및 Excel 문서는 탐지하지 않습니다. 바이러스 검사 엔진에서 비밀번호로 보호된 모든 메시지 또는 첨부 파일은 "암호화"된 것으로 간주됩니다.

참고 3.8 이하 버전의 AsyncOS에서 업그레이드하는 경우 Sophos Anti-Virus 검사를 구성했으면 업그레이드 후에 Encrypted Message Handling(암호화된 메시지 처리) 섹션을 구성해야 합니다.

검사할 수 없는 메시지 처리

검사 시간제한 값에 도달했거나 내부 오류로 인해 엔진을 사용할 수 없게 될 경우 메시지는 *검사할 수 없음*으로 간주됩니다. 검사할 수 없는 상태로 표시된 메시지도 복구할 수 있습니다.

바이러스에 감염된 메시지 처리

시스템에서 첨부 파일을 삭제하지 못하거나 메시지를 완전히 복구하지 못하는 경우가 있습니다. 이러한 경우 바이러스에 감염되어 있는 메시지를 시스템이 처리하는 방법을 구성할 수 있습니다.

암호화된 메시지, 검사할 수 없는 메시지 및 바이러스 메시지에 대한 구성 옵션은 모두 동일합니다.

메시지 처리 작업에 대한 설정 구성

관련 주제

- 적용할 작업, 12-10페이지
- 격리 및 안티바이러스 검사, 12-10페이지
- 메시지 제목 헤더 수정, 12-10페이지
- 원본 메시지 보관, 12-11페이지
- 알림 전송, 12-11페이지
- 메시지에 사용자 지정 헤더 추가, 12-12페이지
- 메시지 수신자 수정, 12-12페이지

- 다른 대상 호스트로 메시지 전송, 12-12페이지
- 사용자 지정 경고 알림 전송(수신자에게만), 12-12페이지

적용할 작업

암호화된 메시지, 검사할 수 없는 메시지 또는 바이러스 판정 메시지 등 메시지 유형마다 수행할 전반적인 작업을 선택합니다. 즉, 메시지를 삭제하거나, 새 메시지의 첨부 파일로 메시지를 전달하거나, 메시지를 있는 그대로 전달하거나, 메시지를 안티바이러스 격리 영역(격리 및 안티바이러스 검사, 12-10페이지)으로 보냅니다.

새 메시지의 첨부 파일로 감염된 메시지를 전달하도록 어플라이언스를 구성할 경우 수신자는 감염된 원본 첨부 파일의 처리 방법을 선택할 수 있습니다.

메시지를 전달하거나 새 메시지의 첨부 파일로 메시지를 전달하도록 선택하는 경우 다음 사항을 추가로 수행할 수 있습니다.

- 메시지 제목 수정
- 원본 메시지 보관
- 일반 알림 전송
  GUI의 "Advanced(고급)" 섹션에서 사용할 수 있는 작업은 다음과 같습니다.
- 메시지에 사용자 지정 헤더 추가
- 메시지 수신자 수정
- 다른 대상 호스트로 메시지 전송
- 사용자 지정 경고 알림 전송(수신자에게만)

참고 이러한 작업은 함께 처리될 수 있습니다. 따라서 여러 사용자 그룹의 여러 가지 처리 요구 사항에 따라 여러 수신 또는 발송 정책에서 일부 또는 모두를 다르게 결합하여 사용할 수 있습니다. 이러한 옵션을 사용하여 다양한 검사 정책을 정의하는 방법에 대해서는 다음 섹션 및 안티바이러스 구성에 대한 참고 사항, 12-14페이지 항목을 참조하십시오.

참고 복구된 메시지에 대한 고급 옵션으로는 Add Custom Header(사용자 지정 헤더 추가)와 Send custom alert notification(사용자 지정 경고 알림 전송) 2가지가 있습니다. 기타 모든 메시지 유형의 경우 모든 고급 옵션을 이용할 수 있습니다.

격리 및 안티바이러스 검사

격리를 위해 플래그가 지정된 경우에도 메시지는 이메일 파이프라인의 나머지 작업을 계속 진행합니다. 메시지가 파이프라인 끝에 도달하였고 해당 메시지가 하나 이상의 격리를 위해 플래그가 지정되었다면 해당 큐로 메시지가 들어갑니다. 메시지가 파이프라인 끝에 도달하지 않으면 격리로 이동하지 않습니다.

예를 들어 콘텐츠 필터로 인해 메시지가 삭제되거나 반송될 수 있으며 이 경우 메시지는 격리되지 않습니다.

메시지 제목 헤더 수정

사용자가 보다 쉽게 메시지를 확인하고 확인된 메시지를 정렬할 수 있도록 특정 텍스트 문자열을 앞에 추가하거나 뒤에 추가하여 확인된 메시지 텍스트를 변경할 수 있습니다.

참고 "Modify message subject(메시지 제목 수정)" 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 추가할 경우 일부 후행 공백과 함께 `[WARNING: VIRUS REMOVED]` 텍스트를 추가합니다.

기본 텍스트는 다음과 같습니다.

표 12-2 안티바이러스 제목 줄 수정을 위한 기본 제목 줄 텍스트

판정	제목에 추가할 기본 텍스트
암호화됨	`[WARNING: MESSAGE ENCRYPTED]`
감염됨	`[WARNING: VIRUS DETECTED]`
복구됨	`[WARNING: VIRUS REMOVED]`
검색할 수 없음	`[WARNING: A/V UNSCANNABLE]`

다양한 상태의 메시지는 어플라이언스가 메시지에 어떤 작업을 수행했는지 다중 파트 알림 메시지를 통해 사용자에게 알려줍니다(예: 바이러스로부터 메시지가 복구되었지만 다른 파트가 암호화되었음을 사용자에게 알림).

원본 메시지 보관

시스템에서 바이러스가 있는(또는 포함 가능성이 있는) 것으로 식별된 메시지를 "avarchive" 디렉토리에 보관할 수 있습니다. 형식은 mbox 형식 로그 파일입니다. 바이러스가 포함된 메시지 또는 완벽하게 검사할 수 없는 메시지를 보관하도록 "안티바이러스 보관" 로그 서브스크립션을 *구성*해야 합니다. 자세한 내용은 38 장, "로깅" 항목을 참조하십시오.

참고 GUI에서 "Advanced(고급)" 링크를 클릭하면 "Archive original message(원본 메시지 보관)" 설정이 표시됩니다.

알림 전송

시스템에서 바이러스가 포함된 메시지를 확인한 경우 발신자, 수신자 및/또는 추가 사용자에게 기본 알림을 보낼 수 있습니다. 알림을 위해 추가 사용자를 지정하는 경우 주소가 여러 개이면 쉼표로 구분하십시오(CLI 및 GUI에서 모두). 기본 알림 메시지는 다음과 같습니다.

표 12-3 안티바이러스 알림의 기본 알림

판정	알림
복구됨	메일 메시지에서 다음 바이러스가 탐지되었습니다. <virus name(s)> 수행된 작업: 감염된 첨부 파일이 삭제되었습니다(또는 감염된 첨부 파일이 복구됨).
암호화됨	암호화로 인해 안티바이러스 엔진에서 다음 메시지를 완벽하게 검사할 수 없습니다.
검색할 수 없음	안티바이러스 엔진에서 다음 메시지를 완벽하게 검사할 수 없습니다.
감염	메일 메시지에서 다음과 같이 복구할 수 없는 바이러스가 탐지되었습니다. <virus name(s)>.

메시지에 사용자 지정 헤더 추가

안티바이러스 검사 엔진으로 검사한 모든 메시지에 추가할 다른 사용자 지정 헤더를 정의할 수 있습니다. **Yes(예)**를 클릭하고 헤더 이름 및 텍스트를 정의합니다.

또한, `skip-viruscheck` 작업을 사용하는 필터를 생성하여 특정 메시지에서 바이러스 검사를 우회할 수 있습니다. 안티바이러스 시스템 우회 작업, 9-70페이지 항목을 참조하십시오.

메시지 수신자 수정

메시지가 다른 주소로 전달되도록 메시지 수신자를 수정할 수 있습니다. **Yes(예)**를 클릭하고 새 수신자 주소를 입력합니다.

다른 대상 호스트로 메시지 전송

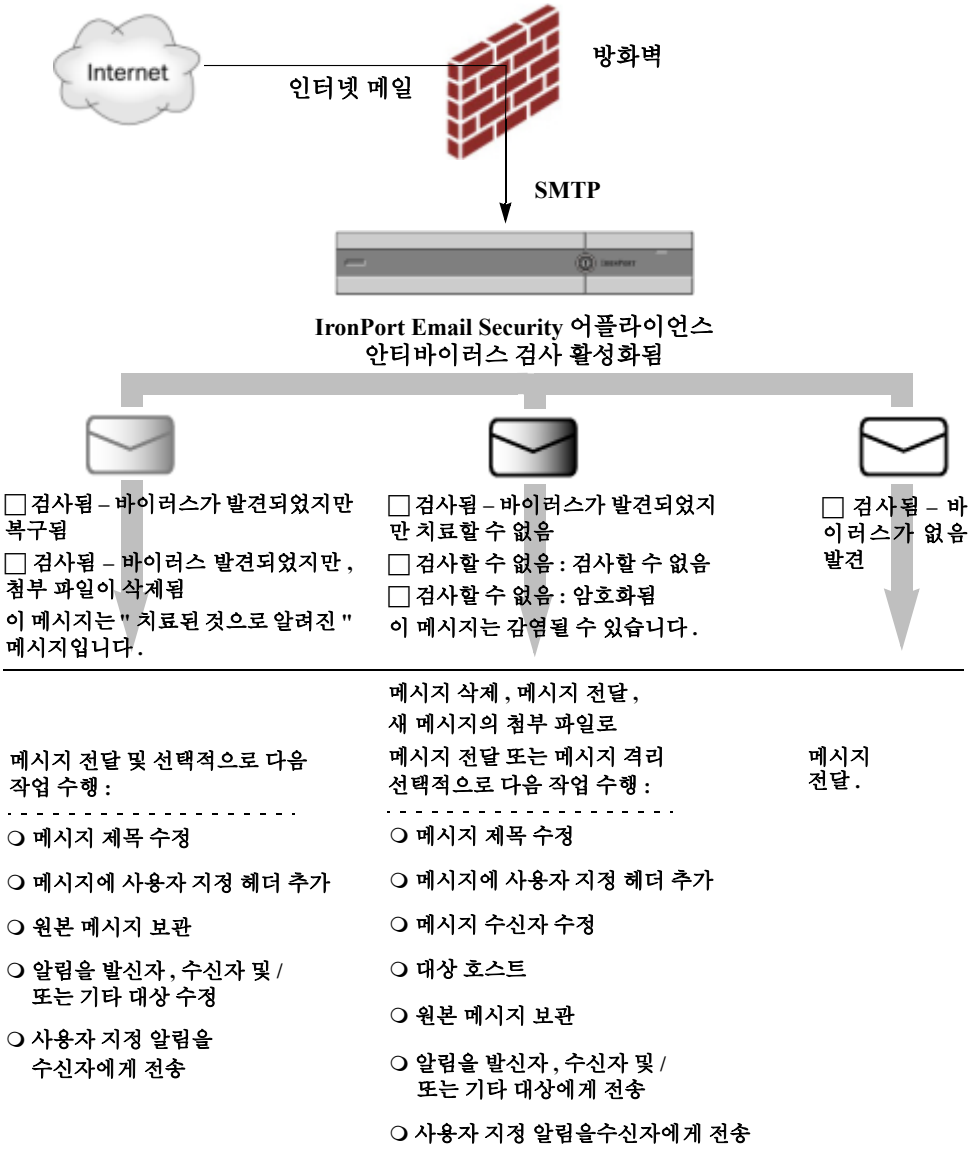
암호화된 메시지, 검사할 수 없는 메시지 또는 바이러스에 감염된 메시지에 대한 알림을 다른 수신자 또는 대상 호스트로 보내도록 선택할 수 있습니다. **Yes(예)**를 클릭하고 대체 주소 또는 호스트를 입력합니다.

예를 들어 후속 검사를 위해 의심스러운 메시지를 관리자의 사서함 또는 특수 메일 서버로 라우팅할 수 있습니다. 다중 수신자 메시지인 경우 단일 복사본만 대체 수신자에게 전송됩니다.

사용자 지정 경고 알림 전송(수신자에게만)

사용자 지정 알림을 수신자에게 전송할 수 있습니다. 이를 위해 설정을 구성하기 전에 먼저 사용자 지정 알림을 생성해야 합니다. 자세한 내용은 텍스트 리소스 이해, 21-8페이지 항목을 참조하십시오.

그림 12-1 바이러스가 검사된 메시지를 처리하기 위한 옵션



참고 기본적으로 안티바이러스 검사는 공용 리스너에 대한 $TRUSTED 메일 흐름 정책에서 활성화됩니다. 이 메일 흐름 정책은 화이트리스트 발신자 그룹에서 참조됩니다. 메일 흐름 정책을 사용하여 이 메일 발신자에 대한 액세스 규칙 정의, 7-8페이지 항목을 참조하십시오.

서로 다른 발신자 및 수신자 그룹에 대한 안티바이러스 정책 구성

메일 정책에 대한 사용자별 안티바이러스 설정을 편집하는 프로세스는 기본적으로 수신 메일 또는 발송 메일에 대해 동일합니다.

개별 정책(기본값 아님)에는 "Use Default(기본값 사용)" 설정에 대한 추가 필드가 있습니다. 기본 메일 정책 설정을 상속하려면 이 설정을 선택합니다.

수신 또는 발송 메일 정책을 사용하여 수신자별로 안티바이러스 작업을 활성화합니다. GUI에서 또는 CLI에서 `policyconfig > antivirus` 명령을 사용하여 메일 정책을 구성할 수 있습니다. 안티바이러스 설정을 전역으로 활성화한 후에 생성한 각 메일 정책에 맞게 이러한 작업을 개별적으로 구성합니다. 메일 정책마다 각기 다른 작업을 구성할 수 있습니다.

절차

1단계 Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책) 또는 Mail Policies(메일 정책) > Outgoing Mail Policies(발송 메일 정책) 페이지로 이동합니다.

2단계 구성하려는 정책에 대한 안티바이러스 보안 서비스 링크를 클릭합니다.

참고 기본 행의 링크를 클릭하여 기본 정책의 설정을 편집합니다.

3단계 **Yes(예)** 또는 **Use Default(기본값 사용)**를 클릭하여 정책에 대한 안티바이러스 검사를 활성화합니다.

페이지의 첫 번째 설정에서는 정책에 대해 서비스를 활성화할지 여부를 정의합니다. **Disable(비활성화)**을 클릭하여 서비스를 모두 비활성화할 수 있습니다.

기본값 이외의 다른 메일 정책에 대해 "Yes(예)"를 선택하면 Repaired(복구됨), Encrypted(암호화됨), Unscannable(검사할 수 없음) 및 Virus Infected Messages(바이러스에 감염된 메시지) 영역의 필드가 활성화됩니다.

4단계 안티바이러스 검사 엔진을 선택합니다. McAfee 또는 Sophos 엔진을 선택할 수 있습니다.

5단계 메시지 검사 설정을 구성합니다.

자세한 내용은 메시지 검사 설정, 12-8페이지 항목을 참조하십시오.

6단계 Repaired(복구됨), Encrypted(암호화됨), Unscannable(검사할 수 없음) 및 Virus Infected Messages(바이러스에 감염된 메시지)에 대한 설정을 구성합니다.

메시지 처리 설정, 12-8페이지 및 메시지 처리 작업에 대한 설정 구성, 12-9페이지 항목을 참조하십시오.

7단계 **Submit(제출)**을 클릭합니다.

8단계 변경사항을 커밋합니다.

안티바이러스 구성에 대한 참고 사항

첨부 파일 삭제 플래그에 따라 안티바이러스 검사 방법에 큰 차이가 발생합니다. 시스템을 "바이러스가 발견되었지만 복구할 수 없는 경우 감염된 첨부 파일 삭제"로 구성한 경우 바이러스에 감염되거나 검사할 수 없는 MIME 파트는 메시지에서 제거됩니다. 그 결과 안티바이러스 검사는 거의 항상 *치료된* 메시지로 출력됩니다. *검사할 수 없는 메시지*에 대해 정의된 작업(GUI 창에 표시됨)은 거의 발생하지 않습니다.

"바이러스만 검사" 환경에서는 허용되지 않는 메시지 부분을 삭제하여 메시지를 "치료"합니다. RFC822 헤더 자체가 공격당하거나 일부 다른 문제가 발생하는 경우에만 검사할 수 없는 작업이 발생하게 됩니다. 그러나 "바이러스만 검사"로 안티바이러스 검사가 구성되고 "바이러스가 발견되었지만 복구할 수 없는 경우 감염된 첨부 파일 삭제"가 선택되지 *않은* 경우에는 검사할 수 없는 작업이 발생할 가능성이 매우 큽니다.

표 12-4에는 일부 공통 안티바이러스 구성 옵션이 나열되어 있습니다.

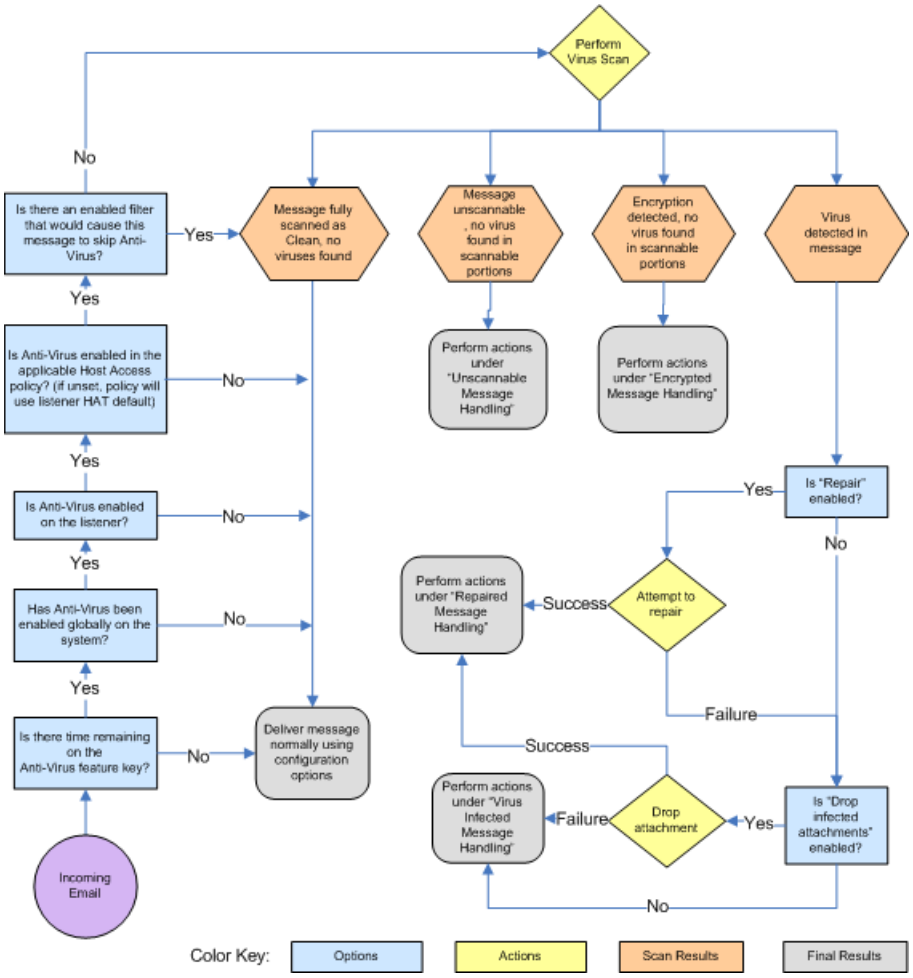
표 12-4 공통 안티바이러스 구성 옵션

상황	안티바이러스 구성
신종 바이러스의 광범위한 유포 바이러스에 감염된 메시지가 시스템에서 삭제되고 다른 프로세스는 거의 실행되지 않습니다.	**첨부 파일 삭제:** NO **검사**: 검사만 **치료된 메시지**: 전달 **검사할 수 없는 메시지**: 메시지 삭제 **암호화된 메시지:** 검토를 위해 관리자 또는 격리에 전송 **바이러스에 감염된 메시지:** 메시지 삭제
관대한 정책 최대한 많은 문서가 전송됩니다.	**첨부 파일 삭제**: YES **검사:** 검사 및 복구 **치료된 메시지:** [바이러스 제거됨] 및 전달 **검사할 수 없는 메시지**: 첨부 파일로 전달 **암호화된 메시지**: 표시 및 전달 **바이러스에 감염된 메시지**: 격리 또는 표시 및 전달
더 보수적인 정책	**첨부 파일 삭제**: YES **검사**: 검사 및 복구 **치료된 메시지:**[바이러스 제거됨] 및 전달 (더 신중한 정책의 경우 치료된 메시지를 보관합니다.) **검사할 수 없는 메시지**: 알림 전송, 격리 또는 삭제 및 보관 **암호화된 메시지:** 표시 및 전달 또는 검사할 수 없는 항목으로 처리 **바이러스에 감염된 메시지:** 보관 및 삭제
보수적 정책과 검토 관리자가 콘텐츠를 검토할 수 있도록 잠재적인 바이러스 메시지가 격리 사서함으로 전송됩니다.	**첨부 파일 삭제:** NO **검사**: 검사만 **치료된 메시지:** 전달(이 작업이 정상적으로 수행되지 않음) **검사할 수 없는 메시지**첨부 파일로 전달, `alt-src-host` 또는 `alt-rcpt-to` 작업으로 전달 **암호화된 메시지:** 검사할 수 없는 항목으로 처리 **바이러스에 감염된 메시지**: 격리 또는 관리자에게 전달

안티바이러스 작업 흐름도

그림 12-2(12-16페이지)에서는 안티바이러스 작업 및 옵션이 어플라이언스에서 처리되는 메시지에 어떤 영향을 미치는지 설명합니다.

그림 12-2 안티바이러스 작업 흐름도



참고 다중 계층 안티바이러스 검사를 구성한 경우 Cisco 어플라이언스는 먼저 McAfee 엔진을 사용하여 바이러스 검사를 수행한 다음 Sophos 엔진을 사용하여 바이러스 검사를 수행합니다. McAfee 엔진에서 바이러스를 탐지하지 못한 경우 두 가지 엔진 모두를 사용하여 메시지를 검사합니다. McAfee 엔진에서 바이러스를 탐지하면 Cisco 어플라이언스가 메일 정책에 대해 정의된 안티바이러스 작업(복구, 격리 등)을 수행합니다.

어플라이언스에 이메일을 전송하여 안티바이러스 검사 테스트

절차

1단계 메일 정책에 대해 바이러스 검사를 활성화합니다.

Security Services(보안 서비스) > Sophos/McAfee Anti-Virus 페이지 또는 `antivirusconfig` 명령을 사용하여 전역 설정을 지정한 다음 Email Security Manager 페이지(GUI) 또는 `policyconfig`의 antivirus 하위 명령을 사용하여 특정 메일 정책에 대한 설정을 구성합니다.

2단계 표준 텍스트 편집기를 열고 다음 문자를 *공백이나 줄 바꿈 없이 한 줄*로 입력합니다.

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

참고 텍스트 편집기 창을 최대화하고 줄 바꿈을 삭제하여 위에 표시된 줄이 텍스트 편집기 창에서 한 줄로 표시되도록 합니다. 또한, 테스트 메시지가 시작되는 "X5O..."에서는 숫자 0이 아니라 문자 O를 입력해야 합니다.

컴퓨터에서 이 설명서를 읽는 경우 PDF 파일 또는 HTML 파일에서 직접 해당 줄을 복사한 후 텍스트 편집기에 붙여넣을 수 있습니다. 이 줄을 복사하는 경우 추가 캐리지 리턴이나 공백을 모두 삭제해야 합니다.

3단계 **`EICAR.COM`** 이름으로 파일을 저장합니다.

파일 크기는 68~70바이트입니다.

참고 이 파일은 바이러스가 *아닙니다*. 이 파일은 퍼지거나 다른 파일을 감염시키거나 컴퓨터에 피해를 주지 않습니다. 그러나 스캐너 테스트를 완료한 후 다른 사용자에게 경보를 보내지 않게 하려면 이 파일을 삭제해야 합니다.

4단계 `EICAR.COM` 파일을 이메일 메시지에 첨부하고 1단계에 구성된 메일 정책과 일치하는 리스너에 전송합니다.

테스트 메시지에 지정한 수신자가 리스너에서 허용되는지 확인합니다 (자세한 내용은 메시지를 수락할 도메인 및 사용자 추가, 8-3페이지 참조).

발송 메일용 바이러스 검사 소프트웨어가 Cisco 이외의 다른 게이트웨이(예: Microsoft Exchange Server)에 설치된 경우 파일을 이메일로 보내기 어려울 수 있습니다.

참고 테스트 파일은 항상 복구할 수 없는 파일로 검사됩니다.

5단계 리스너에서 바이러스 검사를 위해 구성한 작업을 평가하고 해당 작업이 활성화되어 예상대로 동작하고 있는지 확인합니다.

이러한 작업을 쉽게 수행하려면 다음 작업 중 하나를 수행합니다.

- 바이러스 검사 설정을 검사 및 복구 모드로 구성하거나 검사만 모드로 구성하되 첨부 파일을 삭제하지 않습니다.

첨부 파일로 Eicar 테스트 파일을 사용하여 이메일을 전송합니다.

수행되는 작업이 바이러스에 감염된 메시지 처리(바이러스에 감염된 메시지 처리, 12-9페이지의 설정)의 구성과 일치하는지 확인합니다.

- 바이러스 검사 설정을 검사 및 복구 모드로 구성하거나 검사만 모드로 구성하며 첨부 파일을 삭제합니다.

  첨부 파일로 Eicar 테스트 파일을 사용하여 이메일을 전송합니다.

  수행되는 작업이 바이러스에서 복구된 메시지 처리(복구된 메시지 처리, 12-9페이지의 설정)의 구성과 일치하는지 확인합니다.

안티바이러스 검사 테스트를 위한 바이러스 파일을 가져오기에 대한 자세한 내용은 다음을 참조하십시오. `http://www.eicar.org/anti_virus_test_file.htm`이 페이지에서는 다운로드할 수 있는 파일 4개를 제공합니다. 클라이언트측 바이러스 검사 소프트웨어가 설치되어 있는 경우에는 이러한 파일을 다운로드하고 추출하기 어려울 수 있습니다.

바이러스 정의 업데이트

관련 주제

- HTTP를 통한 안티바이러스 업데이트 검색 정보
- 업데이트 서버 설정 구성
- 안티바이러스 업데이트 모니터링 및 수동 확인
- 어플라이언스에서 안티바이러스 파일이 업데이트되었는지 확인

HTTP를 통한 안티바이러스 업데이트 검색 정보

Sophos 및 McAfee는 새로 확인된 바이러스가 포함된 바이러스 정의를 수시로 업데이트합니다. 이러한 업데이트는 사용자 어플라이언스로 전달되어야 합니다.

기본적으로 Cisco 어플라이언스는 5분마다 업데이트를 확인하도록 구성되어 있습니다. Sophos 및 McAfee Anti-Virus 엔진의 경우 서버는 동적 웹 사이트에서 업데이트됩니다.

업데이트가 어플라이언스로 능동적으로 다운로드되면 시스템에서 업데이트 시간이 초과되지 않습니다. 업데이트 다운로드가 오랜 시간 동안 일시 중지될 경우 다운로드 시간이 초과됩니다.

시간 초과가 일어나기 전 시스템에서 업데이트가 완료되기까지 대기하는 최대 시간은 동적이므로 안티바이러스 업데이트 간격보다 짧은 1분으로 정의됩니다(Security Services(보안 서비스) > Service Updates(서비스 업데이트)에 정의됨). 이 구성 값은 완료하는 데 10분 이상 소요될 수 있는 대규모 업데이트를 다운로드하는 동안 연결이 느려지는 어플라이언스에 도움이 됩니다.

업데이트 서버 설정 구성

Security Services(보안 서비스) > Service Updates(서비스 업데이트) 페이지에서 바이러스 업데이트 설정을 구성할 수 있습니다. 예를 들어 시스템에서 안티바이러스 업데이트를 받는 방법 및 업데이트를 확인하는 횟수를 구성할 수 있습니다. 추가 설정에 대한 자세한 내용은 서비스 업데이트, 33-17페이지 항목을 참조하십시오.

안티바이러스 업데이트 모니터링 및 수동 확인

Security Services(보안 서비스) > Sophos 또는 McAfee 페이지나 `antivirusstatus` CLI 명령을 사용하여 어플라이언스에 최신 안티바이러스 엔진 및 ID 파일이 설치되었는지 검사하고 마지막 업데이트가 수행된 시기를 확인할 수 있습니다.

또한 수동으로 업데이트를 수행할 수 있습니다.

관련 주제

- GUI를 사용하여 수동으로 안티바이러스 엔진 업데이트, 12-19페이지
- CLI를 사용하여 수동으로 안티바이러스 엔진 업데이트, 12-19페이지

GUI를 사용하여 수동으로 안티바이러스 엔진 업데이트

절차

1단계 Security Services(보안 서비스) > Sophos 또는 McAfee Anti-Virus 페이지로 이동합니다.

2단계 최신 McAfee/Sophos Anti-Virus 파일 표에서 **Update Now(지금 업데이트)**를 클릭합니다.

어플라이언스에서 최신 업데이트를 확인하여 다운로드합니다.

CLI를 사용하여 수동으로 안티바이러스 엔진 업데이트

`antivirusstatus` CLI 명령을 사용하여 바이러스 파일의 상태를 확인하고, `antivirusupdate` 명령을 사용하여 수동으로 업데이트를 확인합니다.

```
example.com> antivirusstatus

Choose the operation you want to perform:

- MCAFEE - Display McAfee Anti-Virus version information

- SOPHOS - Display Sophos Anti-Virus version information

> sophos

SAV Engine Version        3.2.07.286_4.58
    IDE Serial                0
    Last Engine Update        Base Version
    Last IDE Update           Never updated
```

```
example.com> antivirusupdate

Choose the operation you want to perform:

- MCAFEE - Request updates for McAfee Anti-Virus

- SOPHOS - Request 업데이트s for Sophos Anti-Virus

>sophos

Requesting check for new Sophos Anti-Virus updates

example.com>
```

어플라이언스에서 안티바이러스 파일이 업데이트되었는지 확인

업데이터 로그를 통해 안티바이러스 파일이 성공적으로 다운로드, 추출, 또는 업데이트되었는지 확인할 수 있습니다. `tail` 명령을 사용하여 업데이터 로그 서브스크립션의 최종 항목을 표시하여 바이러스 업데이트가 다운로드되었는지 확인합니다.

안티스팸

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.
  - 스팸 아님
  - 정상적인 출처에서 보낸 원치 않는 마케팅 이메일
  - 의심스러운 스팸
  - 스팸으로 확인된 스팸
- 결과에 따라 작업이 수행됩니다.

  스팸으로 확인된 메시지, 스팸으로 의심되는 메시지 또는 원치 않는 마케팅 메시지로 확인된 메시지에 대한 작업은 함께 수행할 수 있습니다. 따라서 여러 수신 또는 발송 정책에서 사용자 그룹에 대한 여러 가지 처리 요구 사항에 따라 일부 또는 모두를 다르게 결합하여 사용할 수 있습니다. 스팸으로 확인된 스팸을 동일한 정책에서 의심스러운 스팸과 다르게 처리할 수도 있습니다. 예를 들어 스팸으로 확인된 메시지는 삭제하고 의심스러운 스팸 메시지는 격리해야 할 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, 4-7페이지 항목을 참조하십시오.

관련 주제

- 안티스팸 솔루션, 13-2페이지

안티스팸 솔루션

Cisco 어플라이언스는 다음의 안티스팸 솔루션을 제공합니다.

- IronPort Anti-Spam 필터링, 13-3페이지.
- Cisco Intelligent Multi-Scan 필터링, 13-6페이지.

Cisco 어플라이언스에서 이러한 솔루션 모두에 라이센스를 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

	수행할 작업	추가 정보
1단계	Email Security 어플라이언스에서 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, 13-3페이지 • Cisco Intelligent Multi-Scan 필터링, 13-6페이지
2단계	스팸을 로컬 Email Security 어플라이언스에 격리할지, 아니면 보안 관리 어플라이언스의 외부 격리를 사용할지를 구성합니다.	• 로컬 스팸 격리 설정, 31-2페이지 • 외부 스팸 격리 사용, 42-2페이지
3단계	스팸 검사 대상 메시지를 소유하는 사용자 그룹을 정의합니다.	발신자 및 수신자 그룹에 대한 메일 정책 생성, 10-7페이지
4단계	정의한 사용자 그룹의 안티스팸 검사 규칙을 구성합니다.	안티스팸 정책 정의, 13-7페이지
5단계	특정 메시지에서 Cisco Anti-Spam 검사를 건너뛰려면 `skip-spamcheck` 작업을 사용하는 메시지 필터를 생성합니다.	안티스팸 시스템 우회 작업, 9-70페이지

	수행할 작업	추가 정보
6단계	(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 흐름 정책을 사용하여 수신 메시지에 대한 규칙 정의, 7-15페이지 항목을 참조하십시오.
7단계	Email Security 어플라이언스가 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, 13-15페이지
8단계	경고 및 어플라이언스에서 생성된 기타 메시지가 스팸으로 잘못 확인되지 않도록 방지합니다.	스팸 필터로부터 어플라이언스에서 생성된 메시지 보호, 13-14페이지
9단계	(선택 사항) 메시지의 악성 URL에 대한 보호가 강화되도록 URL 필터링을 활성화합니다.	URL 필터링 활성화, 15-2페이지
10단계	구성을 테스트합니다.	안티스팸 테스트, 13-24페이지
11단계	(선택 사항) 서비스 업데이트를 위한 설정(안티스팸 규칙 포함)을 구성합니다.	두 안티스팸 솔루션에 대한 검사 규칙은 모두 기본적으로 Cisco 업데이트 서버에서 검색됩니다. • 서비스 업데이트, 33-17페이지 • 프록시 서버를 통합 업데이트, 33-21페이지 • 업그레이드 및 업데이트를 다운로드하도록 서버 설정 구성, 33-21페이지

IronPort Anti-Spam 필터링

관련 주제

- 평가 키, 13-3페이지
- Cisco Anti-Spam: 개요, 13-4페이지
- IronPort Anti-Spam 검사 구성, 13-5페이지

평가 키

Cisco 어플라이언스에는 Cisco Anti-Spam 소프트웨어를 위한 30일 평가 키가 함께 제공됩니다. 이 키는 시스템 설치 마법사 또는 Security Services(보안 서비스) > IronPort Intelligent Multi-Scan 페이지(GUI), 아니면 `systemsetup` 또는 `antispamconfig` 명령(CLI)으로 라이센스 계약에 동의하기 전까지는 활성화되지 않습니다. 계약에 동의하면 기본적으로 기본 수신 메일 정책에 대해 Cisco Anti-Spam이 활성화됩니다. Cisco 라이센스가 30일 이내에 만료됨을 알리는 경고가 구성한 관리자 주소(시스템 설치 마법사, 2단계: 시스템, 3-15페이지 참조)로 전송됩니다. 경고는 라이센스가 만료되기 30일, 15일, 5일 및 0일 전에 전송됩니다. 30일 평가 기간 이후에 이 기능을 사용하는 방법에 대한 자세한 내용은 Cisco 영업 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, 33-5페이지 참조.)

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 *누구*입니까?
- 메시지 콘텐츠 - 이 메시지에 포함된 콘텐츠는 *무엇*입니까?
- 데이터 구조 - 이 메시지가 구성된 *방식*은 무엇입니까?
- 웹 신뢰도 - 이 작업 지침에 따른 *결과*는 무엇입니까?

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, 13-4페이지
- URL 필터링 개요, 15-1페이지

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, 13-5페이지

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, 13-4페이지 항목을 참조하십시오.

절차

1단계 **Security Services(보안 서비스) > IronPort Anti-Spam**을 선택합니다.

2단계 시스템 설치 마법사에서 IronPort Anti-Spam을 활성화하지 않은 경우 다음을 수행합니다.

a. **Enable(활성화)**을 클릭합니다.

b. 라이센스 계약 페이지 하단으로 스크롤하여 **Accept(동의)**를 클릭하여 계약에 동의합니다.

3단계 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

4단계 **Enable IronPort Anti-Spam Scanning(IronPort Anti-Spam 검사 활성화)** 확인란을 선택합니다.

이 확인란을 선택하면 어플라이언스에 대해 전역으로 기능이 활성화됩니다.

5단계 스패머가 발송한 대용량 메시지를 검사하는 동시에 어플라이언 처리량을 최적화하려면 Cisco Anti-Spam의 메시지 검사에 대한 임계값을 구성합니다.

옵션	설명
메시지 검사 임계값	a. **다음보다 크기가 작은 메시지를 항상 검사**에 대한 값 입력 - 권장 값은 512KB 이하입니다. *항상 검사* 크기보다 작은 메시지는 "조기 종료"를 제외하고 전체적으로 검사됩니다. 해당 크기보다 큰 메시지는 *검사 안 함* 크기보다 작은 경우 부분적으로 검사됩니다. *항상 검사* 메시지 크기로 3MB를 초과하지 않는 것이 좋습니다. 값이 클수록 성능이 저하될 수 있습니다. b. **다음보다 크기가 작은 메시지를 검사 안 함**에 대한 값 입력 - 권장 값은 1,024KB 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. *항상 검사* 크기보다 크거나 *검사 안 함* 크기보다 작은 메시지의 경우 제한적이면서 빠른 속도로 검사가 수행됩니다. **참고** 신종 바이러스 필터(Outbreak Filter) 최대 메시지 크기가 Cisco Anti-Spam의 *항상 검사* 메시지보다 클 경우 신종 바이러스 필터(Outbreak Filter) 최대 크기보다 작은 메시지는 전체적으로 검사됩니다.

옵션	설명
단일 메시지 검사 시간제한	메시지 검사 시의 시간제한 값(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.

6단계 변경사항을 제출하고 커밋합니다.

Cisco Intelligent Multi-Scan 필터링

Cisco Intelligent Multi-Scan은 Cisco Anti-Spam을 비롯한 여러 안티스팸 검사 엔진을 통합하여 다중 계층 안티스팸 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, 13-7페이지

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, 33-5페이지 항목을 참조하십시오. 기능 키를 활성화한 경우에만 IronPort Intelligent Multi-Scan 옵션이 표시됩니다.

절차

1단계 **Security Services(보안 서비스) > IronPort Intelligent Multi-Scan**을 선택합니다.

2단계 시스템 설치 마법사에서 Cisco Intelligent Multi-Scan을 활성화하지 않은 경우 다음을 수행합니다.

a. **Enable(활성화)**을 클릭합니다.

b. 라이센스 계약 페이지 하단으로 스크롤하여 **Accept(동의)**를 클릭하여 계약에 동의합니다.

3단계 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

4단계 **Enable IronPort Intelligent Multi-Scan(IronPort Intelligent Multi-Scan 활성화)** 확인란을 선택합니다.

이 확인란을 선택하면 어플라이언스에 대해 전역으로 기능이 활성화됩니다. 그러나 나중에 Mail Policies(메일 정책)에서 수신자별 설정을 활성화해야 합니다.

5단계 Cisco Intelligent Multi-Scan이 *검사할 최대 메시지 크기*에 해당하는 값을 선택합니다.

기본값은 128KB입니다. Cisco Intelligent Multi-Scan은 이 크기보다 큰 메시지는 검사하지 않습니다.

6단계 메시지 검사 시의 시간제한 값(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.

7단계 변경사항을 제출하고 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, 13-2페이지의 표에 있는 이 지점까지 모든 단계를 완료합니다.

- 다음 사항을 숙지합니다.
  - 스팸 판정 임계값 및 의심스러운 스팸 임계값 이해, 13-10페이지
  - 구성 예: 스팸으로 확인된 스팸과 의심스러운 스팸에 대한 작업, 13-11페이지
  - 정상적인 출처에서 보낸 원치 않는 마케팅 메시지, 13-11페이지
  - 여러 안티스팸 솔루션을 활성화한 경우, 여러 메일 정책에서 서로 다른 안티스팸 검사 엔진 사용: 구성 예, 13-12페이지 항목을 참조하십시오.
  - 안티스팸 검사 중에 추가되는 헤더, 13-14페이지
- 스팸을 "안티스팸 보관소" 로그에 보관하는 경우, 로깅, 38-1페이지 항목을 참조하십시오.
- 메시지를 대체 메일 호스트로 보내는 경우, 전송 호스트 변경 작업, 9-64페이지 항목을 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)** 페이지로 이동합니다.

또는

2단계 **Mail Policies(메일 정책) > Outgoing Mail Policies(발송 메일 정책)** 페이지로 이동합니다.

3단계 메일 정책의 **안티스팸** 열 아래에 있는 링크를 클릭합니다.

4단계 **Enable Anti-Spam Scanning for This Policy(이 정책에 대한 안티스팸 검사 사용)** 섹션에서 정책에 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 안티스팸 검사를 모두 비활성화할 수 있습니다.

5단계 스팸으로 확인된 스팸, 의심스러운 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. 스팸으로 확인된 스팸 검사는 안티스팸 검사가 활성화된 경우 항상 활성화됩니다.
Apply This Action to Message(메시지에 다음 작업 적용)	스팸으로 확인된 스팸, 의심스러운 스팸 또는 원치 않는 마케팅 메시지에 대해 수행할 전반적인 작업을 선택합니다. • 전달 • 삭제 • 바운스 • 격리

옵션	설명
(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. 주요 추가 정보를 확인하려면 전송 호스트 변경 작업, 9-64페이지 항목을 참조하십시오.
제목에 텍스트 추가	사용자가 보다 쉽게 스팸 및 원치 않는 마케팅 메시지를 확인하고 정렬할 수 있도록 특정 텍스트 문자열을 앞에 추가하거나 뒤에 추가하여 확인된 메시지의 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. **참고** "제목에 텍스트 추가"필드에서는 US-ASCII 문자만 허용됩니다.
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, 13-11페이지 항목을 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 "안티스팸 보관소" 로그에 보관할 수 있습니다. 형식은 mbox 형식 로그 파일입니다.
스팸 임계값	기본 임계값을 사용하거나, 스팸으로 확인된 스팸과 의심스러운 스팸에 대한 임계값을 입력합니다.

6단계 변경사항을 제출하고 커밋합니다.

다음 작업

발송 메일에 대해 안티스팸 검사를 활성화한 경우 관련 Host Access Table의 안티스팸 설정, 특히 개인 리스너에 대한 설정을 확인하십시오. 메일 흐름 정책을 사용하여 이메일 발신자에 대한 액세스 규칙 정의, 7-8페이지 항목을 참조하십시오.

관련 주제

- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 13-2페이지
- 스팸 판정 임계값 및 의심스러운 스팸 임계값 이해, 13-10페이지
- 구성 예: 스팸으로 확인된 스팸과 의심스러운 스팸에 대한 작업, 13-11페이지
- 정상적인 출처에서 보낸 원치 않는 마케팅 메시지, 13-11페이지
- 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예, 13-11페이지
- 여러 메일 정책에서 서로 다른 안티스팸 검사 엔진 사용: 구성 예, 13-12페이지

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.

정확도가 높은 경우 스팸으로 확인된 메시지의 임계값은 기본적으로 매우 높습니다. 90~100의 메시지 점수는 스팸으로 간주됩니다. 의심스러운 스팸의 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.

스팸으로 확인된 스팸 임계값을 50~99 값으로 변경할 수 있습니다. 의심스러운 스팸의 임계값은 25와 스팸으로 확인된 스팸에 대해 지정된 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.

스팸으로 확인된 스팸 및 의심스러운 스팸에 대해 수행할 별도의 작업을 정의할 수 있습니다. 예를 들어 "스팸으로 확인된" 스팸은 삭제하되 "의심스러운" 스팸은 격리할 수 있습니다.

관련 주제

- 안티스팸 솔루션, 13-2페이지
- 구성 예: 스팸으로 확인된 스팸과 의심스러운 스팸에 대한 작업, 13-11페이지

구성 예: 스팸으로 확인된 스팸과 의심스러운 스팸에 대한 작업

스팸	샘플 작업 (적극적)	샘플 작업 (보수적)
스팸으로확인된 스팸	삭제	• 메시지 제목에 "[스팸으로 확인된 스팸]"을 추가한 상태로 전달 또는 • 격리
의심스러운스팸	메시지 제목에 "[의심스러운 스팸]"을 추가한 상태로 전달	메시지 제목에 "[의심스러운 스팸]"을 추가한 상태로 전달

적극적인 구성을 한 경우에는 의심스러운 스팸 메시지에만 태그를 지정한 반면 스팸으로 확인된 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.

적극적인 구성을 한 경우에는 스팸으로 확인된 스팸 및 의심스러운 스팸은 변경된 제목으로 전달됩니다. 사용자는 의심스러운 스팸 및 스팸으로 확인된 스팸을 삭제할 수 있습니다. 이 방법은 첫 번째 방법보다 더 보수적인 방법입니다.

메일 정책의 적극적인 정책 및 보수적인 정책에 대한 자세한 설명은 메일 정책 장의 표 10-3(10-11 페이지) 항목을 참조하십시오.

정상적인 출처에서 보낸 원치 않는 마케팅 메시지

두 가지 안티스팸 검사 엔진은 모두 스팸과 정상적인 출처에서 보낸 원치 않는 마케팅 메시지를 구분할 수 있습니다. 마케팅 메시지는 스팸으로 간주되지 않지만, 조직 또는 최종 사용자는 해당 메시지를 받기를 원하지 않을 수 있습니다. 스팸과 마찬가지로 원치 않는 마케팅 메시지도 전달, 삭제, 격리 또는 바운스할 수 있는 옵션이 있습니다. 마케팅 메시지로 식별되도록 메시지 제목에 텍스트를 추가하여 원치 않는 마케팅 메시지에 태그를 지정하는 옵션도 있습니다.

사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 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, 15-2페이지 항목을 참조하십시오.

절차

1단계 의심스러운 스팸 메시지에 사용자 지정 헤더를 적용합니다.

a. **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)**를 선택합니다.

b. 기본 정책 등 해당 정책의 **안티스팸** 열에 있는 링크를 클릭합니다.

c. Suspected Spam Settings(의심스러운 스팸 설정) 섹션에서 의심스러운 스팸 검사를 활성화합니다.
d. **Advanced(고급)**를 클릭하면 Add Custom Header(사용자 지정 헤더 추가) 옵션이 표시됩니다.
e. `url_redirect` 등 사용자 지정 헤더를 추가합니다.
f. 변경사항을 제출하고 커밋합니다.

2단계 사용자 지정 헤더가 있는 메시지의 URL을 리디렉션하도록 다음과 같이 콘텐츠 필터를 생성합니다.

a. **Mail Policies(메일 정책) > Incoming Content Filters(수신 콘텐츠 필터)**를 선택합니다.
b. **Add Filter(필터 추가)**를 클릭합니다.
c. 필터 이름으로 `url_redirect`를 지정합니다.
d. **Add Condition(조건 추가)**을 클릭합니다.
e. **Other Header(기타 헤더)**를 클릭합니다.
f. 헤더 이름으로 `url_redirect`를 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 **Selected Categories(선택한 범주)**에 추가합니다.
l. URL에 대한 작업으로는 **Redirect to Cisco Security Proxy(Cisco Security 프록시로 리디렉션)**를 선택합니다.
m. **OK(확인)**를 클릭합니다.

3단계 메일 정책에 콘텐츠 필터를 추가합니다.

a. **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)**를 선택합니다.
b. 이 절차의 앞부분에서 선택한 정책의 **콘텐츠 필터** 열에서 링크를 클릭합니다.
a. 아직 선택하지 않은 경우 **Enable Content Filters(콘텐츠 필터 사용)**를 선택합니다.
b. **url_filtering** 콘텐츠 필터를 사용하려면 확인란을 선택합니다.
c. 변경사항을 제출하고 커밋합니다.

관련 주제

- URL 리디렉션, 14-5페이지
- 11 장, "콘텐츠 필터"

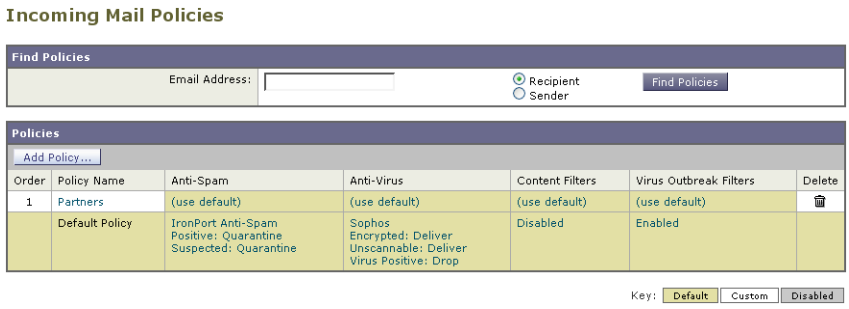
여러 메일 정책에서 서로 다른 안티스팸 검사 엔진 사용: 구성 예

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 안티스팸 검사 솔루션을 구성할 수 있습니다. (발송 메일 정책의 경우 일반적으로 안티스팸 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 13-1 메일 정책 - 수신자별 안티스팸 엔진

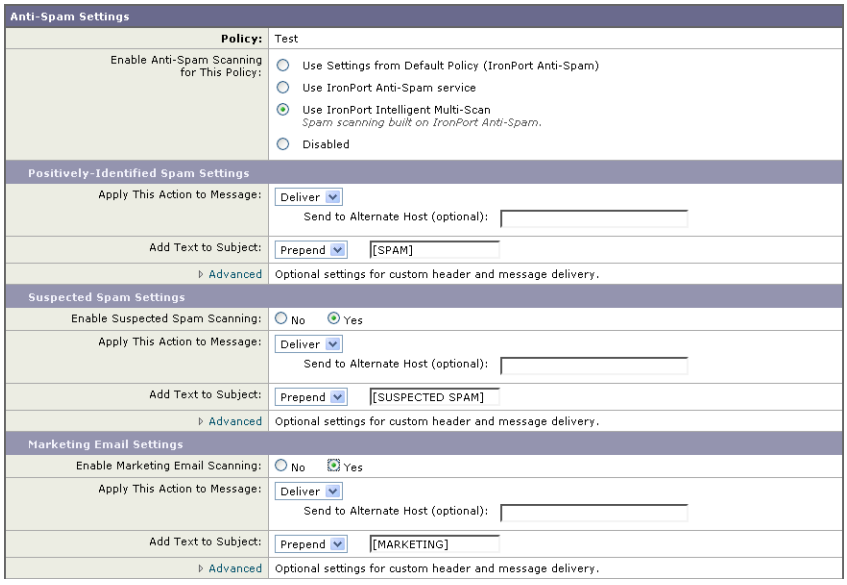


Cisco Intelligent Multi-Scan을 사용하고 원치 않는 마케팅 메시지를 검사하도록 파트너 정책을 변경하려면 파트너 행에 해당하는 안티스팸 열의 항목을 클릭합니다("기본값 사용").

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.

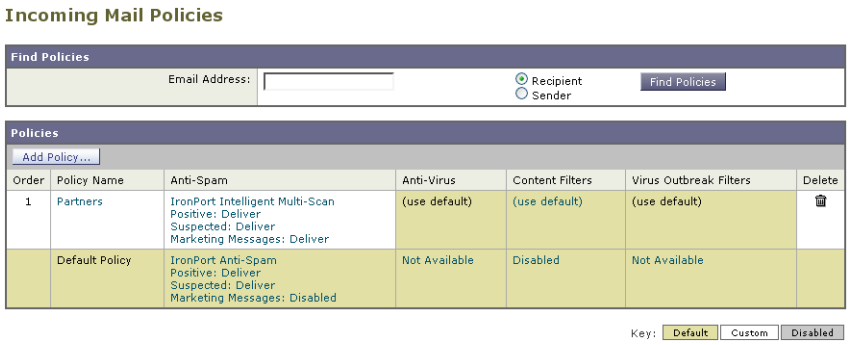
그림 13-2에서는 해당 정책에서 활성화된 Cisco Intelligent Multi-Scan 및 원치 않는 마케팅 메시지 탐지를 보여줍니다.

그림 13-2 Mail Policies(메일 정책) - Cisco Intelligent Multi-Scan 활성화



변경사항을 제출하고 커밋한 후에 메일 정책은 다음과 같습니다.

그림 13-3 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 생성, 10-7페이지 및 안티스팸 시스템 우회 작업, 9-70페이지 항목을 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 안티스팸 검사 엔진에서도 헤더를 추가합니다.
- 지정된 메일 정책과 관련하여 스팸으로 확인되었거나, 스팸으로 의심되거나, 원치 않는 마케팅 메일로 확인된 모든 메시지에 추가할 사용자 지정 헤더를 추가 정의할 수 있습니다. 안티스팸 정책 정의, 13-7페이지 항목을 참조하십시오.

관련 주제

- 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예, 13-11페이지

Cisco Systems에 잘못 분류된 메시지 보고

잘못 분류된 것으로 보이는 메시지는 분석을 위해 Cisco에 보고할 수 있습니다. 각 메시지는 분석가들로 구성된 팀에서 검토되며 제품의 정확성과 효율성을 높이는 데 사용됩니다. 각 메시지는 다음 주소로 RFC 822 첨부 파일로 전달되어야 합니다.

- spam@access.ironport.com - 누락된 스팸 보고
- ham@access.ironport.com - 긍정 오류 보고

제출 볼륨으로 인해 Cisco IronPort는 개별적인 피드백 또는 결과를 고객에게 제공할 수 없습니다.

잘못 분류된 메시지의 보고에 대한 자세한 내용은 Cisco 기술 자료를 참조하거나 Cisco 지원 제공업체에 문의하십시오.

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, 13-15페이지
- 수신 릴레이와 연동되도록 어플라이언스 구성, 13-17페이지
- 수신 릴레이가 기능에 영향을 미치는 방식, 13-21페이지
- 헤더 사용을 지정하는 로그 구성, 13-23페이지

수신 릴레이를 사용하는 예제 환경

그림 13-4는 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 13-4 MX/MTA로 릴레이되는 메일 - 기본

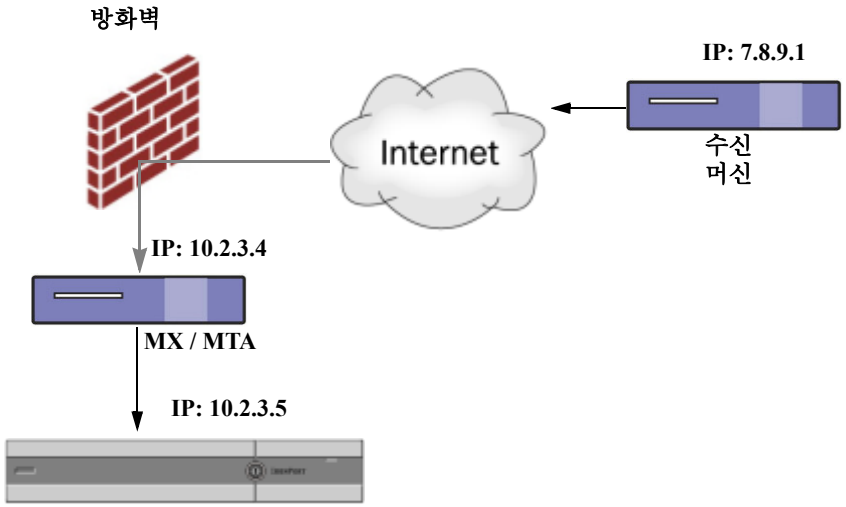
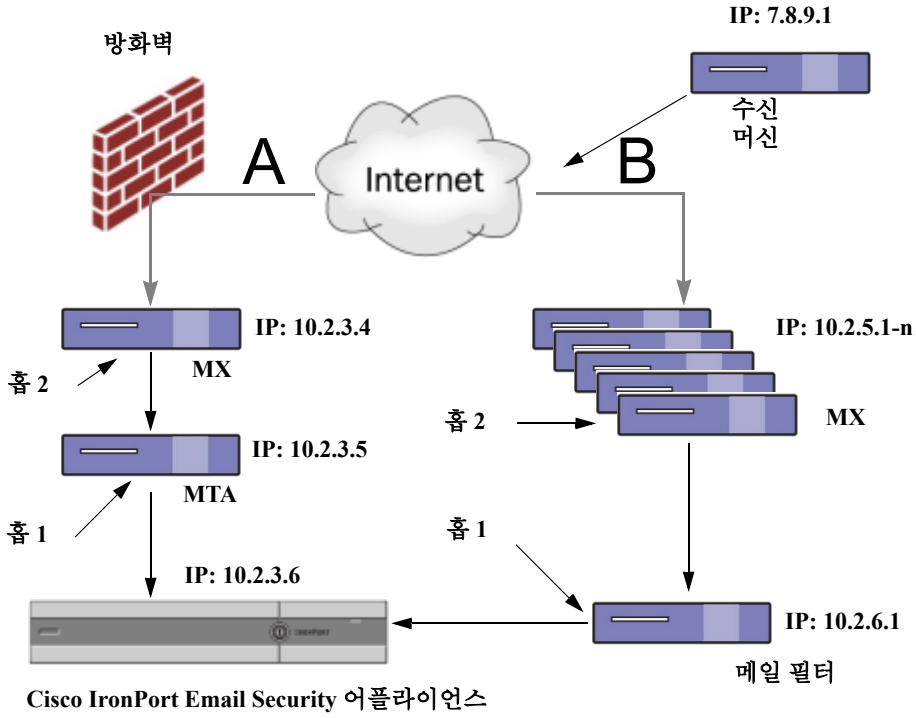


그림 13-5는 메일이 Cisco 어플라이언스에 전달되기 전에 네트워크 내부에서 릴레이되는 방식과 메일이 네트워크 내부의 여러 서버에서 처리되는 방식에 대한 약간 더 복잡한 예를 보여줍니다. 예 A에서 7.8.9.1에서 전송된 메일은 방화벽을 통과하고 Cisco 어플라이언스로 전달되기에 앞서 MX 및 MTA에 의해 처리됩니다. 예 B에서는 7.8.9.1에서 전송된 메일은 부하 분산 장치 또는 다른 유형의 트래픽 셰이핑 어플라이언스로 전송되며 Cisco 어플라이언스에 전달되기에 앞서 MX 주소 중 하나로 전송됩니다.

그림 13-5 MX/MTA로 릴레이되는 메일 - 고급



수신 릴레이와 연동되도록 어플라이언스 구성

관련 주제

- 수신 릴레이 기능 활성화, 13-17페이지
- 수신 릴레이 추가, 13-17페이지
- 릴레이되는 메시지에 대한 메시지 헤더, 13-18페이지

수신 릴레이 기능 활성화

참고 로컬 MX/MTA가 메일을 Cisco 어플라이언스로 릴레이하는 경우에만 수신 릴레이 기능을 활성화해야 합니다.

절차

1단계 **Network(네트워크) > Incoming Relays(수신 릴레이)**를 선택합니다.

2단계 **Enable(활성화)**을 클릭합니다.

3단계 변경사항을 커밋합니다.

수신 릴레이 추가

수신 릴레이를 추가하여 다음을 확인할 수 있습니다.

- 네트워크에서 수신 메시지를 Email Security 어플라이언스로 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, 13-18페이지 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.

절차

1단계 **Network(네트워크) > Incoming Relays(수신 릴레이)**를 선택합니다.

2단계 **Add Relay(릴레이 추가)**를 클릭합니다.

3단계 이 릴레이의 이름을 입력합니다.

4단계 수신 메시지를 릴레이하기 위해 Email Security 어플라이언스에 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 AsyncOS가 지원하는 형식은 다음과 같습니다.

- `2620:101:2004:4202::0-2620:101:2004:4202::ff`
- `2620:101:2004:4202::`
- `2620:101:2004:4202::23`
- `2620:101:2004:4202::/64`

5단계 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.

6단계 변경사항을 제출하고 커밋합니다.

다음 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, 13-22페이지 항목을 참조하십시오.
- 추적 및 문제 해결을 용이하게 하려면 사용되는 헤더를 표시하도록 어플라이언스 로그를 구성합니다. 헤더 사용을 지정하는 로그 구성, 13-23페이지 항목을 참조하십시오.

관련 주제

- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 13-2페이지

릴레이되는 메시지에 대한 메시지 헤더

다음 헤더 유형 중 하나를 사용하여 릴레이되는 메시지의 원래 발신자를 식별하도록 어플라이언스를 구성합니다.

- 사용자 지정 헤더, 13-19페이지
- Received 헤더, 13-19페이지

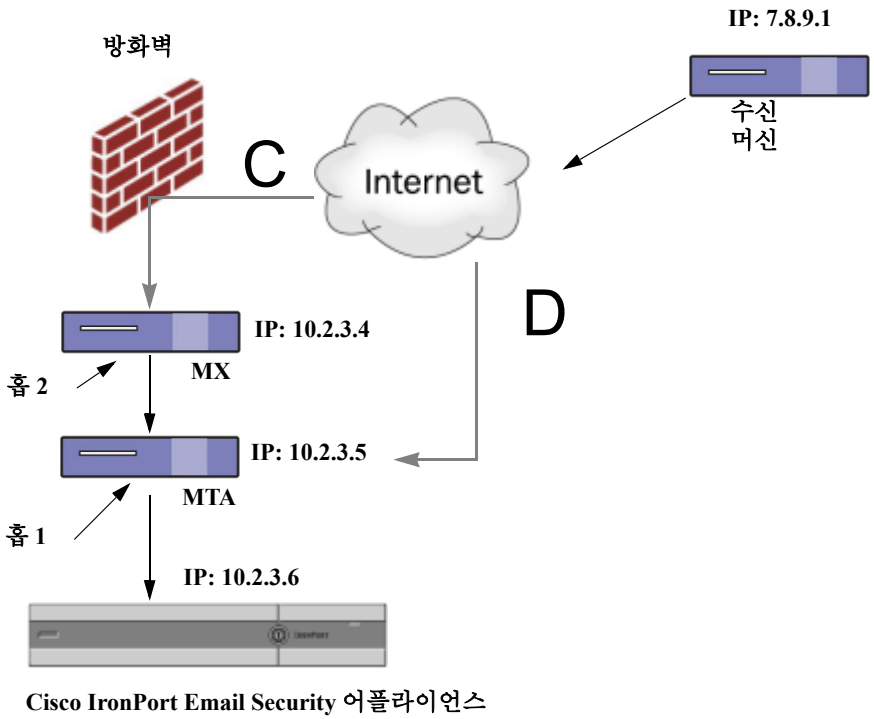
사용자 지정 헤더

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 그림 13-6에서 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 13-6 MX/MTA로 릴레이되는 메일 - 가변적인 홉 수



관련 주제

- 수신 릴레이 추가, 13-17페이지

Received 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 13-5의 10.2.3.5)의 머신은 항상 네트워크 경계에서 벗어난 홉 수와 동일해야 합니다. 수신 메일이(그림 13-6에 설명된 대로 홉 수가 달라짐) Cisco 어플라이언스에 연결된 머신에 대해 서로 다른 경로를 사용하는 경우 사용자 지정 헤더를 사용해야 합니다(사용자 지정 헤더, 13-19페이지 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 헤더 사용을 지정하는 로그 구성, 13-23페이지 참조). 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 13-5에서 수신 릴레이는 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)

표 13-1에서는 그림 13-5에서처럼 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 13-2에서는 잘못된 헤더가 제외된 동일한 이메일 메시지의 헤더를 보여줍니다.

표 13-1 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>`

표 13-1에 대한 참고 사항:

- Cisco 어플라이언스는 이러한 헤더를 무시합니다.
- Cisco 어플라이언스는 메시지(홉으로 계산되지 않음)를 수신합니다.
- 첫 번째 홉(및 수신 릴레이).

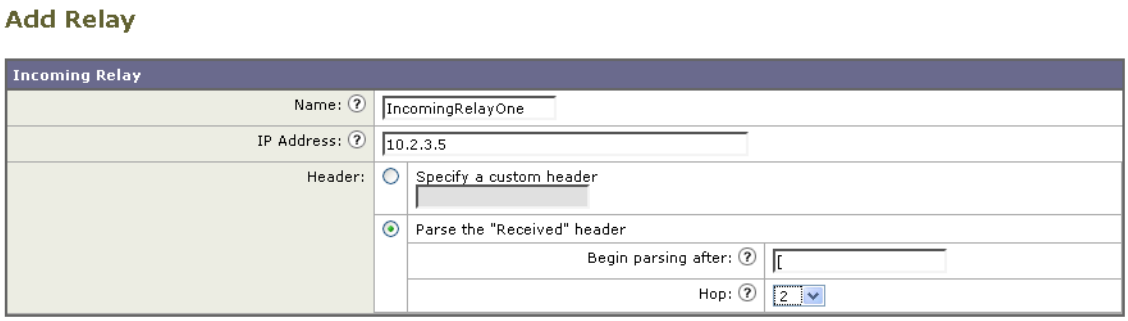
- 두 번째 홉. 이는 전송 MTA입니다. IP 주소는 7.8.9.1입니다.
- Cisco 어플라이언스는 이러한 Microsoft Exchange 헤더를 무시합니다.

표 13-2 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>;`

그림 13-7에서는 GUI의 Add Relay(릴레이 추가) 페이지에 구성된 대로 경로 A(위)에 대한 수신 릴레이를 보여줍니다.

그림 13-7 Received 헤더와 함께 구성된 수신 릴레이



관련 주제

- 수신 릴레이 추가, 13-17페이지

수신 릴레이가 기능에 영향을 미치는 방식

- 수신 릴레이 및 필터, 13-22페이지
- 수신 릴레이, HAT, SBRS 및 발신자 그룹, 13-22페이지
- 수신 릴레이 및 디렉토리 수집 공격 방지, 13-22페이지
- 수신 릴레이 및 추적, 13-22페이지
- 수신 릴레이 및 이메일 보안 모니터(보고), 13-22페이지
- 수신 릴레이 및 메시지 추적, 13-22페이지
- 수신 릴레이 및 로깅, 13-23페이지

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. 이렇게 하면 정상적인 메시지를 비롯한 릴레이의 모든 메시지가 Email Security 어플라이언스에 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
```

헤더 사용을 지정하는 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 구성하려면 로깅을 위한 전역 설정 구성,38-38페이지 항목을 참조하십시오.

규칙 업데이트 모니터링

라이센스 계약에 동의한 경우 가장 최근의 Cisco Anti- Spam 및 Cisco Intelligent Multi-Scan 규칙 업데이트를 볼 수 있습니다.

절차

1단계 Security Services(보안 서비스) > IronPort Anti-Spam을 선택합니다.

또는

2단계 Security Services(보안 서비스) > IronPort Intelligent Multi-Scan을 선택합니다.

3단계 **Rule Updates(규칙 업데이트)** 섹션을 살펴보고 다음을 수행합니다.

변경 후	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.

관련 주제

- 서비스 업데이트, 33-17페이지
- 프록시 서버를 통합 업데이트, 33-21페이지
- 업그레이드 및 업데이트를 다운로드하도록 서버 설정 구성, 33-21페이지

안티스팸 테스트

변경 후	수행할 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, 13-7페이지)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 안티스팸 테스트, 13-25페이지 항목을 참조하십시오. • `trace` 명령을 사용하고 이 헤더를 포함합니다. 테스트 메시지를 사용한 메일 흐름 디버깅: 추적, 40-1페이지 항목을 참조하십시오.
안티스팸 엔진 효율성을 평가합니다.	인터넷에서 직접 라이브 메일 스트림을 사용하여 제품을 평가합니다.	지양해야 할 비효율적인 평가 방법 목록에 대해서는 안티스팸 효율성을 테스트할 때 사용해서는 안 되는 방식, 13-26페이지 항목을 참조하십시오.

관련 주제

- 이메일을 어플라이언스에 전송하여 Cisco 안티스팸 테스트, 13-25페이지
- 안티스팸 효율성을 테스트할 때 사용해서는 안 되는 방식, 13-26페이지

이메일을 어플라이언스에 전송하여 Cisco 안티스팸 테스트

시작하기 전에

- 어플라이언스에 텔넷을 사용하는 방법을 이해합니다. 부록 A, "FTP, SSH, SCP 및 텔넷 액세스" 항목을 참조하십시오.
- 안티스팸 구성 테스트: SMTP 사용 예, 13-25페이지의 예를 검토합니다.

절차

1단계 Cisco 메일 정책에서 안티스팸을 활성화합니다.

2단계 해당 메일 정책에서 다음 헤더를 포함하는 테스트 이메일을 사용자에게 전송합니다.

```
X-Advertisement: spam
```

SMTP 명령과 텔넷을 사용하여 이 메시지를 액세스할 수 있는 주소로 전송합니다.

3단계 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, 13-25페이지

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

데이터

354 go ahead

Subject: Spam Message Test

X-Advertisement: spam



spam test

.

250 Message MID accepted

221 hostname

quit
```

안티스팸 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 안티스팸 벤더에 의해 탐지된 스팸 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.

14 장

신종 바이러스 필터(Outbreak Filter)

신종 바이러스 필터(Outbreak Filter) 개요

신종 바이러스 필터(Outbreak Filter)는 피싱 스캠 및 맬웨어 배포와 같은 대규모 신종 바이러스 공격과 더 규모가 작은 비 바이러스 공격이 발생할 경우 네트워크를 보호해 줍니다. 데이터가 수집되고 소프트웨어 업데이트가 게시될 때까지 새로운 신종 바이러스를 탐지하지 못하는 대부분의 안티맬웨어 보안 소프트웨어와 달리 Cisco는 신종 바이러스가 확산될 때 관련 데이터를 수집해 업데이트된 정보를 사용자의 Email Security 어플라이언스에 실시간으로 전송하여 이러한 메시지가 사용자에게 도달하지 못하게 합니다.

Cisco는 전역 트래픽 패턴을 사용하여 수신 메시지가 안전한지 아니면 신종 바이러스의 일부인지 결정하는 규칙을 개발합니다. 신종 바이러스의 일부일 수 있는 메시지는 Cisco에서 전송한 업데이트된 신종 바이러스 정보 또는 Sophos 및 McAfee에서 게시한 새로운 안티바이러스 정의를 기준으로 해당 메시지가 안전하다고 확인될 때까지 격리됩니다.

소규모 비 바이러스 공격에 사용되는 메시지는 정상적으로 보이는 설계, 수신자의 정보, 단기간 동안만 온라인 상태로 유지되고 웹 보안 서비스에 알려져 있지 않은 피싱 및 맬웨어 웹사이트로 연결되는 사용자 지정 URL을 사용합니다. 신종 바이러스 필터(Outbreak Filter)는 메시지의 내용을 분석하고 URL 링크를 검색하여 이러한 유형의 비 바이러스 공격을 탐지합니다. 신종 바이러스 필터(Outbreak Filter)는 잠재적으로 유해한 웹사이트에 대한 트래픽을 웹 보안 프록시를 통해 리디렉션하도록 URL을 재작성하여 사용자에게 액세스하려는 웹사이트가 악성임을 경고하거나 웹사이트를 완전히 차단할 수 있습니다.

신종 바이러스 필터(Outbreak Filter)의 작동 원리

관련 주제

메시지 표시, 리디렉션 및 수정

신종 바이러스 필터(Outbreak Filter) 기능은 다음과 같은 3가지 전술을 사용하여 신종 바이러스로부터 사용자를 보호합니다.

- **지연.** 신종 바이러스 필터(Outbreak Filter)는 신종 바이러스 또는 비 바이러스 공격의 일부일 수 있는 메시지를 격리합니다. 메시지가 격리되어 있는 동안 어플라이언스가 업데이트된 신종 바이러스 정보를 수신하고 메시지를 다시 검사하여 공격의 일부인지 확인합니다.
- **리디렉션.** 신종 바이러스 필터(Outbreak Filter)는 수신자가 링크된 웹사이트에 액세스하려고 시도할 경우 Cisco Web Security 프록시를 통해 수신자를 리디렉션하도록 비 바이러스 공격 메시지의 URL을 재작성합니다. 프록시에서 웹사이트가 여전히 작동 중인 경우 웹사이트에 맬웨어가 포함되었을 수 있음을 경고하는 스플래시 화면을 표시하고, 웹사이트가 오프라인 상태로 전환된 경우 오류 메시지를 표시합니다. URL 리디렉션에 대한 자세한 내용은 URL 리디렉션, 14-5페이지를 참조하십시오.
- **수정.** 신종 바이러스 필터(Outbreak Filter)는 비 바이러스 위협 메시지의 URL을 재작성할 뿐 아니라 메시지의 제목을 수정하고 메시지 본문 위에 경고문을 추가하여 사용자에게 메시지의 내용에 대해 경고합니다. 자세한 내용은 메시지 수정, 14-6페이지를 참조하십시오.

위협 범주

신종 바이러스 필터(Outbreak Filter) 기능은 두 가지 범주의 메시지 기반 신종 바이러스(첨부 파일에 한 번도 본 적이 없는 바이러스가 있는 메시지인 *신종 바이러스*와 피싱 패턴, 스캠, 링크를 통한 외부 웹사이트로의 맬웨어 배포를 포함하는 *비 바이러스 위협*)로부터 보호합니다.

기본적으로 신종 바이러스 필터(Outbreak Filter) 기능은 신종 바이러스 발생 시 수신 및 발송 메시지에 바이러스가 있는지 검사합니다. 어플라이언스에서 안티스팸 검사를 활성화할 경우 신종 바이러스뿐 아니라 비 바이러스 위협에 대해서 검사를 활성화할 수 있습니다.

참고 신종 바이러스 필터(Outbreak Filter)가 비 바이러스 위협을 검사할 수 있으려면 어플라이언스에 안티스팸 또는 Intelligent Multi-Scan에 대한 기능 키가 있어야 합니다.

관련 주제

- 신종 바이러스, 14-3페이지
- 피싱, 맬웨어 배포 및 기타 비 바이러스 위협, 14-3페이지

신종 바이러스

신종 바이러스 필터(Outbreak Filter) 기능은 신종 바이러스와 싸울 때 유용합니다. 신종 바이러스는 메시지의 첨부 파일에 한 번도 본 적이 없는 바이러스가 포함되어 있거나 기존 바이러스의 변종이 사설 네트워크와 인터넷을 통해 빠르게 확산될 때 발생합니다. 이러한 새로운 바이러스나 변종은 인터넷을 공격하므로 가장 중요한 기간은 바이러스가 릴리스된 시점부터 안티바이러스 공급업체가 업데이트된 바이러스 정의를 릴리스하는 시점까지입니다. 몇 시간 전이라도 사전 알림을 보내는 것이 맬웨어 또는 바이러스의 확산을 억제하는 데 반드시 필요합니다. 이러한 취약성 기간 동안 새로 발견된 바이러스가 전역적으로 전파되어 이메일 인프라가 중지될 수 있습니다.

피싱, 맬웨어 배포 및 기타 비 바이러스 위협

비 바이러스 위협이 포함된 메시지는 정상적인 소스에서 전송된 메시지처럼 보이도록 설계되었으며 종종 소수의 수신자에게 발송됩니다. 이러한 메시지는 신뢰할 수 있는 메시지로 보이기 위해 다음과 같은 특성 중 하나 이상을 가질 수 있습니다.

- 수신자의 연락처 정보
- 소셜 네트워크 또는 온라인 소매업체와 같은 정상적인 소스의 이메일을 모방하도록 설계된 HTML 콘텐츠
- 새로운 IP 주소를 사용하고 단시간 동안만 온라인 상태로 유지되어 이메일 및 웹사이트 보안 서비스가 해당 웹사이트가 악성인지 판단하는 데 필요한 충분한 정보를 얻을 수 없는 웹사이트를 가리키는 URL
- URL 단축 서비스를 가리키는 URL

이 모든 특성으로 인해 이러한 메시지는 스팸으로 탐지하기가 더 어렵습니다. 신종 바이러스 필터(Outbreak Filter) 기능은 사용자가 맬웨어를 다운로드하거나 의심스러운 새 웹사이트에 개인 정보를 제공하지 못하게 하는 다중 계층 방어를 통해 이러한 비 바이러스 위협으로부터 보호합니다.

CASE는 메시지에서 URL을 발견한 경우 메시지와 기존 신종 바이러스 규칙을 비교하여 메시지가 소규모 비 신종 바이러스의 일부인지 결정한 다음 위협 수준을 지정합니다. 위협 수준에 따라 Email Security 어플라이언스는 더 많은 위협 데이터를 수집할 때까지 수신자에게 메시지가 전송되는 것을 지연시키고 수신자가 웹사이트에 액세스하려고 시도할 경우 수신자를 Cisco Web Security 프록시로 리디렉션하도록 메시지의 URL을 재작성합니다. 프록시에서 사용자에게 해당 웹사이트에 맬웨어가 포함되었을 수 있음을 경고하는 스플래시 페이지를 표시합니다.

Cisco Security Intelligence Operations

SIO(Cisco Security Intelligence Operations)는 전역 위협 정보, 평판 기반 서비스, 정교한 분석을 Cisco 보안 어플라이언스에 연결하여 더 빠른 응답 시간과 더 강력한 보호를 제공하는 보안 에코시스템입니다.

SIO는 다음과 같은 3 가지 구성 요소로 이루어져 있습니다.

- SenderBase. 세계 최대의 위협 모니터링 네트워크 및 취약성 데이터베이스
- TOC(Threat Operations Center). 보안 분석가와 SenderBase에서 수집한 실행 가능한 정보를 추출하는 자동 시스템으로 이루어진 글로벌 팀
- 동적 업데이트. 신종 바이러스 발생 시 어플라이언스에 자동으로 전송되는 실시간 업데이트

SIO가 글로벌 SenderBase 네트워크의 실시간 데이터를 일반적인 트래픽 패턴과 비교하여 입증된 신종 바이러스 예측 변수인 이상 현상을 식별합니다. TOC에서 데이터를 검토하고 가능한 신종 바이러스의 위협 수준을 지정합니다. Cisco Email Security 어플라이언스가 업데이트된 위협 수준과 신종 바이러스 규칙을 다운로드하고 이를 사용해 이미 신종 바이러스 격리에 있는 메시지뿐 아니라 수신 및 발송 메시지도 검사합니다.

최신 신종 바이러스에 대한 정보는 아래의 SenderBase 웹사이트에서 찾을 수 있습니다.

`http://www.senderbase.org/`

아래의 SIO 웹사이트는 스팸, 피싱, 맬웨어 배포 시도를 포함한 최신 비 바이러스 위협의 목록을 제공합니다.

`http://tools.cisco.com/security/center/home.x`

컨텍스트 적응형 검사 엔진

신종 바이러스 필터(Outbreak Filter)는 Cisco의 고유한 CASE(컨텍스트 적응형 검사 엔진)를 제공합니다. CASE는 메시징 위협에 대한 실시간 분석을 기반으로 자동으로 조정된 100,000개 이상의 적응형 메시지 특성을 정기적으로 활용합니다.

신종 바이러스의 경우 CASE가 메시지 내용, 컨텍스트 및 구조를 분석하여 적응 규칙이 트리거할 가능성을 정확하게 판단합니다. CASE는 적응 규칙과 SIO에서 게시하는 실시간 신종 바이러스 규칙을 결합하여 모든 메시지를 평가하고 고유한 위협 수준을 지정합니다.

비 바이러스 위협을 탐지하기 위해 CASE는 하나 이상의 URL이 발견될 경우 URL의 메시지를 검사하고 SIO의 신종 바이러스 규칙을 사용하여 메시지의 위협 수준을 평가합니다.

메시지의 위협 수준에 따라 CASE는 신종 바이러스를 차단하기 위해 메시지를 격리할 기간을 권고합니다. 또한 SIO의 업데이트된 신종 바이러스 규칙에 따라 메시지를 다시 평가할 수 있도록 재검사 간격을 결정합니다. 위협 수준이 높을수록 메시지가 격리되어 있는 동안 메시지 재검사 빈도가 더 높아집니다.

CASE는 메시지가 격리에서 릴리스될 때도 메시지를 다시 검사합니다. CASE가 재검사 시 메시지가 스팸이거나 바이러스를 포함하고 있다고 결정할 경우 메시지가 다시 격리될 수 있습니다.

CASE에 대한 자세한 내용은 Cisco Anti-Spam: 개요, 13-4페이지를 참조하십시오.

메시지 지연

신종 바이러스 또는 이메일 공격이 발생한 시점부터 소프트웨어 공급업체가 업데이트된 규칙을 릴리스할 때까지의 기간은 네트워크와 사용자가 가장 취약해질 수 있는 기간입니다. 이 기간 동안 최신 바이러스가 전역으로 전파될 수 있으며 악성 웹사이트가 맬웨어를 전송하거나 사용자의 민감한 정보를 수집할 수 있습니다. 신종 바이러스 필터(Outbreak Filter)는 한시적으로 의심스러운 메시지를 격리하여 Cisco와 기타 공급업체에게 새로운 신종 바이러스를 조사할 시간을 줌으로써 사용자와 네트워크를 보호합니다.

신종 바이러스가 발생하면 업데이트된 신종 바이러스 규칙과 새로운 안티바이러스 서명이 해당 이메일 첨부 파일이 클린인지 아니면 바이러스인지 입증할 때까지 첨부 파일이 포함된 의심스러운 메시지가 격리됩니다.

소규모 비 바이러스 위협에는 신뢰할 수 있는 웹사이트를 가운데에 끼워 넣어 웹 보안을 우회하고 웹 보안 서비스 또는 URL 단축 서비스를 통한 탐지를 피하기 위해 단기간 동안 온라인 상태로 유지될 수 있는 악성 웹사이트에 대한 URL이 포함됩니다. CASE는 위협 수준 임계값을 충족하는 URL이 포함된 메시지를 격리하여 SIO의 업데이트된 신종 바이러스 규칙에 따라 메시지의 내용을 다시 평가할 기회를 얻을 뿐 아니라 링크된 웹사이트가 오프라인으로 전환되거나 웹 보안 솔루션에 의해 차단될 때까지 메시지를 격리 상태로 유지할 수 있습니다.

신종 바이러스 필터(Outbreak Filter)가 의심스러운 메시지를 격리하는 방법에 대한 자세한 내용은 동적 격리, 14-10페이지를 참조하십시오.

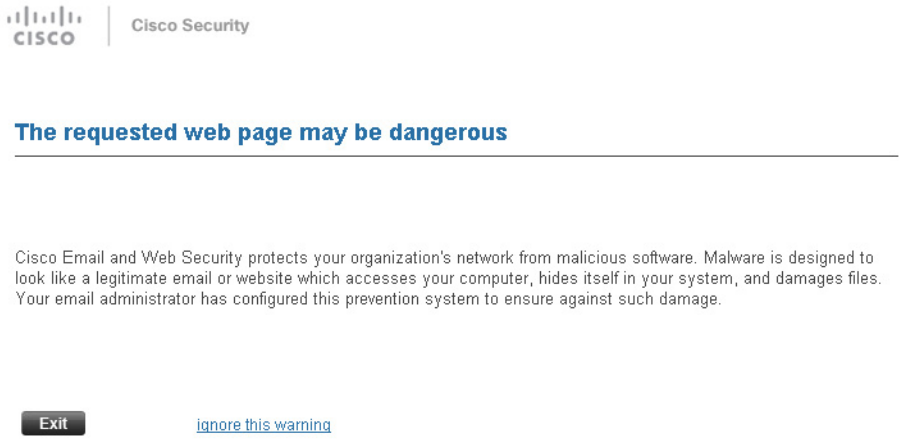
URL 리디렉션

CASE는 신종 바이러스 필터(Outbreak Filter) 단계에서 메시지를 검사할 때 기타 의심스러운 내용 외에 메시지 본문의 URL도 검색합니다. CASE는 게시된 신종 바이러스 규칙을 사용하여 메시지가 위협인지 평가한 다음 해당 위협 수준에 따라 메시지에 점수를 매깁니다. 위협 수준에 따라 신종 바이러스 필터(Outbreak Filter)가 우회된 도메인을 가리키는 URL을 제외하고 수신자를 Cisco Web Security 프록시로 리디렉션하도록 모든 URL을 재작성하고 해당 웹사이트가 더 큰 신종 바이러스의 일부로 판단될 경우 TOC에서 웹사이트에 대한 추가 정보를 수집할 수 있도록 메시지의 전송을 지연시켜 수신자를 보호합니다. 신뢰할 수 잇는 도메인의 URL 우회에 대한 자세한 내용은 URL 재작성 및 도메인 우회, 14-20페이지를 참조하십시오.

Email Security 어플라이언스가 메시지를 릴리스 및 전송한 후에 수신자가 웹사이트에 액세스하려고 시도할 경우 Cisco Web Security 프록시를 통해 리디렉션됩니다. 이는 Cisco에서 호스팅하는 외부 프록시로, 웹사이트가 여전히 작동 중인 경우 사용자에게 해당 웹사이트가 위험할 수 있음을 경고하는 스플래시 화면을 표시합니다. 웹사이트가 오프라인으로 전환된 경우 스플래시 화면에 오류 메시지가 표시됩니다.

수신자가 메시지의 URL을 클릭하기로 결정하면 Cisco Web Security 프록시에서 사용자에게 메시지의 내용에 대해 경고하기 위해 사용자의 웹 브라우저에 스플래시 화면을 표시합니다. 그림 14-1에 스플래시 화면 경고의 예가 나와 있습니다. 수신자가 **Ignore this warning(이 경고 무시)**을 클릭하여 웹사이트 액세스를 진행하거나 **Exit(종료)**를 클릭하여 종료하고 브라우저 창을 안전하게 닫을 수 있습니다.

그림 14-1 Cisco 보안 스플래시 화면 경고



Cisco Web Security 프록시에 액세스할 수 있는 유일한 방법은 메시지의 재작성된 URL을 통하는 것입니다. 웹 브라우저에 URL을 입력하는 방법으로는 프록시에 액세스할 수 없습니다.

참고 이 스플래시 화면의 모양을 사용자 지정하고 회사 로고, 연락처 정보 등과 같은 조직의 브랜딩을 표시할 수 있습니다. 최종 사용자 알림 페이지의 모양 사용자 지정, 15-6페이지를 참조하십시오.

정보 의심스러운 스팸 메시지의 모든 URL을 Cisco Web Security 프록시 서비스로 리디렉션하려면 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예, 13-11페이지를 참조하십시오.

메시지 수정

신종 바이러스 필터(Outbreak Filter) 기능을 통해 비 바이러스 위협 메시지의 메시지 본문을 수정하여 URL를 재작성할 뿐 아니라 사용자에게 해당 메시지가 의심스러운 위협임을 경고할 수 있습니다. 또한 제목 헤더를 수정하고 메시지 본문 위에 메시지의 내용에 대한 경고문을 추가할 수 있습니다. 자세한 내용은 메시지 수정, 14-19페이지를 참조하십시오.

위협 경고문은 Mail Policies(메일 정책) > Text Resources(텍스트 리소스) 페이지의 경고문 템플릿을 사용하여 작성할 수 있습니다. 자세한 내용은 텍스트 리소스 관리의 개요, 21-9페이지를 참조하십시오.

규칙의 유형: 적응 및 신종 바이러스

2가지 유형의 규칙(적응 및 신종 바이러스)은 신종 바이러스 필터(Outbreak Filter)에서 잠재적인 신종 바이러스를 탐지하는 데 사용합니다. 신종 바이러스 필터(Outbreak Filter)는 이러한 2가지 규칙 집합을 사용하여 가장 효율적이고 집중적인 위협 탐지 기준을 제공하여 필터가 특정한 신종 바이러스를 기민하게 포착할 수 있도록 보장합니다. 신종 바이러스 필터(Outbreak Filter) 규칙과 작업은 화면 뒤에 숨겨지지 않고 관리자에게 표시되므로 격리된 메시지와 격리된 이유를 즉각적으로 확인할 수 있습니다.

관련 주제

- 신종 바이러스 규칙, 14-6페이지
- 적응 규칙, 14-7페이지

신종 바이러스 규칙

신종 바이러스 규칙은 Cisco Security Intelligence Operations의 한 부분인 Cisco TOC(Threat Operations Center)에서 생성하며 첨부 파일 유형이 아닌 메시지 전체에 집중합니다. 신종 바이러스 규칙은 SenderBase 데이터(실시간 및 기록 트래픽 데이터)와 첨부 파일 유형, 파일 이름 키워드와 같은 메시지 매개변수의 조합 또는 안티바이러스 엔진 업데이트를 사용하여 신종 바이러스를 실시간으로 인지하고 차단합니다. 신종 바이러스 규칙에는 GUI의 다양한 위치에서 해당 규칙을 참조하는 데 사용되는 고유한 ID가 부여됩니다(신종 바이러스 격리 등).

글로벌 SenderBase 네트워크의 실시간 데이터를 이 기준과 비교하여 입증된 신종 바이러스 예측 변수인 이상 현상을 식별합니다. TOC에서 데이터를 검토하고 위협 표시자 또는 위협 수준을 지정합니다. 위협 수준은 0(위협 없음)과 5(매우 위험) 사이의 숫자값으로, 메시지가 Cisco 고객이 널리 배포한 다른 게이트웨이 방어가 없는 위협일 가능성을 측정합니다(자세한 내용은 위협 수준, 14-7페이지 참조). 위협 수준은 TOC에서 신종 바이러스 규칙으로 게시합니다.

신종 바이러스 규칙에 포함될 수 있는 몇 가지 특성 조합을 예로 들면 다음과 같습니다.

- 파일 유형, 파일 유형 및 크기, 파일 유형 및 파일 이름 키워드 등
- 파일 이름 키워드 및 파일 크기
- 파일 이름 키워드

- 메시지 URL
- 파일 이름 및 Sophos IDE

적응 규칙

적응 규칙은 메시지 특성과 알려진 신종 바이러스 메시지의 특성을 정확하게 비교하는 CASE 내의 규칙 집합입니다. 이러한 규칙은 광범위한 바이러스 데이터 내에서 알려진 위협 메시지와 알려진 양호한 메시지를 연구한 후에 생성되었습니다. 적응 규칙은 데이터 평가 시에 종종 업데이트됩니다. 적응 규칙은 기존 신종 바이러스 규칙을 보완하여 항상 신종 바이러스 메시지를 탐지하도록 도와줍니다. 신종 바이러스 규칙은 가능한 신종 바이러스가 발생할 경우에 적용되는 반면, 적응 규칙은 일단 활성화되면 항상 "활성화된 상태"로 유지되어 전역적으로 완전한 이상 현상이 발생하기 전에 로컬에서 신종 바이러스 메시지를 포착합니다. 또한 적응 규칙은 이메일 트래픽 및 구조의 사소하고 미묘한 변화에 지속적으로 대응하여 고객에게 업데이트된 보호를 제공합니다.

신종 바이러스

신종 바이러스 필터(Outbreak Filter) 규칙은 기본적으로 이메일 메시지 및 첨부 파일의 특성 집합(파일 크기, 파일 유형, 파일 이름, 메시지 내용 등)과 관련된 위협 수준(예: 4)입니다. 예를 들어, Cisco SIO에서 크기가 143킬로바이트인 .exe 첨부 파일을 포함한 의심스러운 이메일 메시지의 발생이 증가하고 있으며 그러한 파일 이름에 특정한 키워드(예: "hello")가 포함되어 있다는 알림을 보낸다고 가정해 보겠습니다. 이 기준에 맞춰 메시지의 위협 수준을 높이는 신종 바이러스 규칙이 게시됩니다. 어플라이언스에서 기본적으로 5분마다 새로 게시된 신종 바이러스 및 적응 규칙을 확인하고 다운로드합니다(신종 바이러스 필터(Outbreak Filter) 규칙 업데이트, 14-15페이지 참조). 적응 규칙은 신종 바이러스 규칙보다 더 낮은 빈도로 업데이트됩니다. 사용자가 어플라이언스에서 의심스러운 메시지 격리에 대한 임계값을 설정합니다. 메시지의 위협 수준이 격리 임계값과 같거나 그보다 높을 경우 메시지가 *신종 바이러스* 격리 영역으로 전송됩니다. 사용자는 또한 비 바이러스 위협 메시지 수정에 대한 임계값을 설정하여 의심스러운 메시지에서 발견된 모든 URL을 재작성하거나 메시지 본문 위에 알림을 추가할 수 있습니다.

위협 수준

표 14-1(14-7페이지)에는 다양한 각 수준에 대한 기본적인 지침 또는 정의 집합이 나와 있습니다.

표 14-1 위협 수준 정의

수준	최소화	의미
0	없음	메시지가 위협일 위험이 없습니다.
1	적음	메시지가 위협일 위험이 낮습니다.
2	낮음/중간	메시지가 위협일 위험이 낮거나 중간입니다. "의심스러운" 위협입니다.
3	중간	메시지가 확인된 신종 바이러스의 일부이거나 메시지 내용이 위협일 위험이 중간에서 높음입니다.
4	높음	메시지가 대규모 신종 바이러스의 일부임이 확인되었거나 메시지 내용이 매우 위험합니다.
5	극히 높음	메시지의 내용이 거대 규모 또는 대규모 신종 바이러스의 일부임이 확인되었으며 극히 위험합니다.

위협 수준과 신종 바이러스 규칙에 대한 자세한 내용은 신종 바이러스 필터(Outbreak Filter) 규칙, 14-15페이지를 참조하십시오.

관련 주제

- 격리 위협 수준 임계값 설정 지침, 14-8페이지
- 컨테이너: 특정 및 항상 규칙, 14-8페이지

격리 위협 수준 임계값 설정 지침

격리 위협 수준 임계값을 통해 관리자가 다소 공격적으로 의심스러운 메시지를 격리할 수 있습니다. 낮은 설정(1 또는 2)은 더 공격적이고 더 많은 메시지를 격리하는 반면 높은 점수(4 또는 5)는 덜 공격적이고 악성일 가능성이 매우 높은 메시지만 격리합니다.

신종 바이러스 위협과 비 신종 바이러스 위협에 모두 동일한 임계값이 적용되지만 사용자가 바이러스 공격 및 기타 위협에 대한 격리 보관 시간을 각기 다르게 지정할 수 있습니다. 자세한 내용은 동적 격리, 14-10페이지를 참조하십시오.

Cisco에서는 기본값으로 3을 설정할 것을 권장합니다.

컨테이너: 특정 및 항상 규칙

컨테이너 파일은 다른 파일을 포함하는 파일입니다(예: 압축된(.zip) 아카이브). TOC에서 아카이브 파일 내의 특정 파일을 처리하는 규칙을 게시할 수 있습니다.

예를 들어, TOC에서 신종 바이러스가 .exe를 포함하는 .zip 파일로 이루어져 있음을 파악한 경우 .zip 파일 내의 .exe 파일(.zip(exe))에 대한 위협 수준을 설정하되, .zip 파일에 포함된 다른 파일 유형(예: .txt 파일)에 대한 구체적인 위협 수준은 설정하지 않는 특정 신종 바이러스 규칙이 게시됩니다. 두 번째 규칙(.zip(*))이 컨테이너 파일 유형 내의 다른 모든 파일에 적용됩니다. 컨테이너에 대한 항상 규칙은 컨테이너에 포함된 파일의 유형에 관계없이 항상 메시지의 위협 수준 계산에 사용됩니다. 항상 규칙은 그러한 모든 컨테이너 유형이 위험하다고 알려진 경우에 SIO에서 게시합니다.

표 14-2 대체 규칙 및 위협 수준 점수

신종 바이러스 규칙	위협 수준	설명
.zip(exe)	4	이 규칙은 .zip 파일에 포함된 .exe 파일의 위협 수준을 4로 설정합니다.
.zip(doc)	0	이 규칙은 .zip 파일에 포함된 .doc 파일의 위협 수준을 0으로 설정합니다.
zip(*)	2	이 규칙은 .zip에 포함된 파일의 유형에 관계없이 모든 .zip 파일의 위협 수준을 2로 설정합니다.

신종 바이러스 필터(Outbreak Filter) 기능의 작동 원리

이메일 메시지는 어플라이언스에서 처리될 때 일련의 단계인 "이메일 파이프라인"을 거칩니다(이메일 파이프라인에 대한 자세한 내용은 이메일 파이프라인 이해, 4-1페이지 참조). 메시지가 이메일 파이프라인을 통과할 때 해당 메일 정책에 안티스팸 및 안티바이러스 검사 엔진이 사용될 경우 그러한 엔진을 통해 메시지가 실행됩니다. 다시 말해서, 알려진 스팸이나 인지된 바이러스가 포함된 메시지는 이미 메일 흐름에서 제거되었으므로(삭제, 격리 등) 안티스팸 및 안티바이러스 설정에 따라 신종 바이러스 필터(Outbreak Filter)에서 검사되지 않습니다. 따라서 신종 바이러스 필터(Outbreak Filter) 기능에 도착하는 메시지는 스팸 또는 바이러스가 없는 메시지로 표시됩니다. 신

종 바이러스 필터(Outbreak Filter)를 통해 격리된 메시지는 격리에서 릴리스되어 CASE를 통해 다시 검사될 때 업데이트된 스팸 규칙 및 바이러스 정의에 따라 스팸 또는 바이러스 포함 메시지로 표시될 수 있습니다.

참고 필터 또는 엔진이 비활성화되어 안티스팸 및 안티바이러스 검사를 건너뛴 메시지는 여전히 신종 바이러스 필터(Outbreak Filter)를 통해 검사됩니다.

관련 주제

- 메시지 점수 매기기, 14-9페이지
- 동적 격리, 14-10페이지

메시지 점수 매기기

새로운 바이러스 공격 또는 비 바이러스 위협이 등장할 경우 그러한 위협을 인식할 수 있는 안티바이러스 또는 안티스팸 소프트웨어가 아직 없으므로 신종 바이러스 필터(Outbreak Filter) 기능이 매우 유용할 수 있습니다. 수신 메시지는 CASE가 게시된 신종 바이러스 및 적응 규칙을 사용하여 검사하고 점수를 매깁니다(규칙의 유형: 적응 및 신종 바이러스, 14-6페이지 참조). 메시지 점수는 메시지의 위협 수준에 해당합니다. 메시지와 일치하는 규칙(있는 경우)에 따라 CASE가 해당 위협 수준을 지정합니다. 관련 위협 수준이 없으면(메시지가 어떤 규칙과도 일치하지 않음) 메시지의 위협 수준이 0으로 지정됩니다.

계산이 완료되면 Email Security 어플라이언스가 해당 메시지의 위협 수준이 격리 또는 메시지 수정 임계값을 충족 또는 초과하는지 확인하고 메시지를 격리하거나 해당 URL을 재작성합니다. 위협 수준이 임계값보다 낮으면 추가 처리를 위해 파이프라인을 따라 진행합니다.

또한 CASE가 최신 규칙을 기준으로 기존의 격리된 메시지를 다시 평가하여 메시지의 최신 위협 수준을 결정합니다. 따라서 위협 수준이 신종 바이러스 메시지와 일치하는 메시지만 격리 내에 남아 있고 더 이상 위협이 아닌 메시지는 자동 재평가 후에 격리에서 빠져나옵니다.

1개의 신종 바이러스 메시지에 여러 개의 점수(적응 규칙의 점수(또는 여러 적응 규칙이 적용된 경우 가장 높은 점수)와 신종 바이러스 규칙의 점수(또는 여러 신종 바이러스 규칙이 적용된 경우 가장 높은 점수))가 매겨진 경우 지능형 알고리즘을 사용하여 최종 위협 수준을 결정합니다.

참고 어플라이언스에서 안티바이러스 검사를 활성화하지 않고도 신종 바이러스 필터(Outbreak Filter)를 사용할 수 있습니다. 이 2개의 보안 서비스는 서로 보완하되 따로 작동하도록 설계되었습니다. 다시 말해서, 어플라이언스에서 안티바이러스 검사를 활성화지 않을 경우 안티바이러스 공급업체의 업데이트를 모니터링하고 신종 바이러스 격리의 일부 메시지를 수동으로 릴리스하거나 재평가해야 합니다. 안티바이러스 검사를 활성화하지 않고 신종 바이러스 필터(Outbreak Filter)를 사용할 경우 다음 사항을 유의하십시오.

- 적응 규칙을 비활성화해야 합니다.
- 메시지가 신종 바이러스 규칙에 의해 격리됩니다.
- 위협 수준이 낮아지거나 시간이 만료되면 메시지가 릴리스됩니다.

다운스트림 안티바이러스 공급업체(데스크탑/그룹웨어)가 릴리스 시 메시지를 포착할 수 있습니다.

참고 신종 바이러스 필터(Outbreak Filter) 기능이 비 바이러스 위협을 검사할 수 있도록 하려면 어플라이언스에서 안티스팸 검사를 전역적으로 활성화해야 합니다.

동적 격리

신종 바이러스 필터(Outbreak Filter) 기능의 신종 바이러스 격리는 메시지가 위협인지 아니면 사용자에게 전송하기에 안전한지 확인될 때까지 메시지를 저장하는 데 사용되는 임시 대기 영역입니다. (자세한 내용은 신종 바이러스 라이프사이클 및 규칙 게시, 14-11페이지를 참조하십시오.) 격리된 메시지는 여러 가지 방법으로 신종 바이러스 격리에서 릴리스될 수 있습니다. 새 규칙이 다운로드되면 신종 바이러스 격리의 메시지가 CASE에서 계산한 권장 재검사 간격에 따라 재평가됩니다. 수정된 메시지 위협 수준이 격리 보관 임계값 범위에 속할 경우 신종 바이러스 격리의 설정에 관계없이 메시지가 자동으로 릴리스되므로 격리 상태로 보내는 시간이 최소화됩니다. 메시지가 재평가되는 도중 새 규칙이 게시되면 재검사가 다시 시작됩니다.

바이러스 공격으로 격리된 메시지는 새 안티바이러스 서명이 제공될 경우에도 신종 바이러스 격리에서 자동으로 릴리스되지 않습니다. 새 규칙이 안티바이러스 서명을 참조하거나 참조하지 않을 수 있지만 신종 바이러스 규칙이 메시지의 위협 수준을 위협 수준 임계값보다 낮은 점수로 변경하지 않는 한 안티바이러스 엔진 업데이트로 인해 메시지가 다시 릴리스되지 않습니다.

CASE의 권장 보관 기간이 경과한 경우에도 메시지가 신종 바이러스 격리에서 릴리스됩니다. CASE가 메시지의 위협 수준을 기준으로 보관 기간을 계산합니다. 신종 바이러스 및 비 바이러스 위협에 대해 별도의 최대 보관 시간을 정의할 수 있습니다. CASE의 권장 보관 시간이 해당 위협 유형의 최대 보관 시간을 초과할 경우 최대 보관 시간이 경과하면 Email Security 어플라이언스가 메시지를 릴리스합니다. 바이러스 메시지의 경우 기본 최대 격리 기간은 1일입니다. 비 바이러스 위협의 기본 격리 기간은 4시간입니다. 수동으로 메시지를 격리에서 릴리스할 수 있습니다.

Email Security 어플라이언스는 격리가 가득 찬 상태에서 더 많은 메시지가 삽입되는 경우(이를 오버플로라고 함)에도 메시지를 릴리스합니다. 오버플로는 신종 바이러스 격리 용량이 100%에 도달한 상태에서 새 메시지가 격리에 추가될 경우에만 발생합니다. 이 때 메시지가 다음과 같은 우선순위로 릴리스됩니다.

- 적응 규칙에 의해 격리된 메시지(가장 빨리 릴리스되도록 예약된 메시지가 첫 번째로 격리됨)
- 신종 바이러스 규칙에 의해 격리된 메시지(가장 빨리 릴리스되도록 예약된 메시지가 첫 번째로 격리됨)

오버플로 릴리스는 신종 바이러스 격리 용량이 100% 아래로 내려가는 시점에 중단됩니다. 격리 오버플로가 처리되는 방법에 대한 자세한 내용은 격리의 메시지 보관 시간, 30-3페이지 및 자동으로 처리된 격리 메시지에 대한 기본 작업, 30-4페이지를 참조하십시오.

신종 바이러스 격리에서 해제된 메시지는 안티바이러스 및 안티스팸 엔진(해당 메일 정책에 사용될 경우)을 통해 검사됩니다. 현재 알려진 바이러스 또는 스팸으로 표시된 경우 사용자의 메일 정책 설정(바이러스 격리 또는 스팸 격리의 가능한 두 번째 격리 포함)에 따라 처리됩니다. 자세한 내용은 신종 바이러스 필터 기능 및 신종 바이러스 격리, 14-21페이지를 참고하십시오.

따라서 메시지의 수명 동안 실제로 두 번 격리될 수 있다는 점에 유의하는 것이 중요합니다. 즉, 신종 바이러스 필터(Outbreak Filter) 기능에 의해 한 번 격리되고, 신종 바이러스 격리에서 릴리스될 때 또 한 번 격리됩니다. 각 검사(신종 바이러스 필터(Outbreak Filter) 검사 전과 신종 바이러스 격리에서 릴리스될 때)의 판정이 일치할 경우 메시지가 두 번째 격리의 적용을 받지 않습니다. 또한 신종 바이러스 필터(Outbreak Filter) 기능이 메시지에 대해 최종 작업을 수행하지 않습니다. 신종 바이러스 필터(Outbreak Filter) 기능은 추가 처리를 위해 메시지를 격리하거나 파이프라인의 다음 단계로 메시지를 이동합니다.

관련 주제

- 신종 바이러스 라이프사이클 및 규칙 게시, 14-11페이지

신종 바이러스 라이프사이클 및 규칙 게시

신종 바이러스 라이프사이클의 초기에는 더 광범위한 규칙을 사용해 메시지를 격리합니다. 더 많은 정보를 사용할 수 있게 됨에 따라 점점 더 집중된 규칙이 게시되고 격리되는 메시지의 정의가 좁혀집니다. 새 규칙이 게시되면 더 이상 가능한 바이러스 메시지로 간주되지 않는 메시지가 격리에서 릴리스됩니다(신종 바이러스 격리의 메시지는 새 규칙이 게시되면 다시 검사됨).

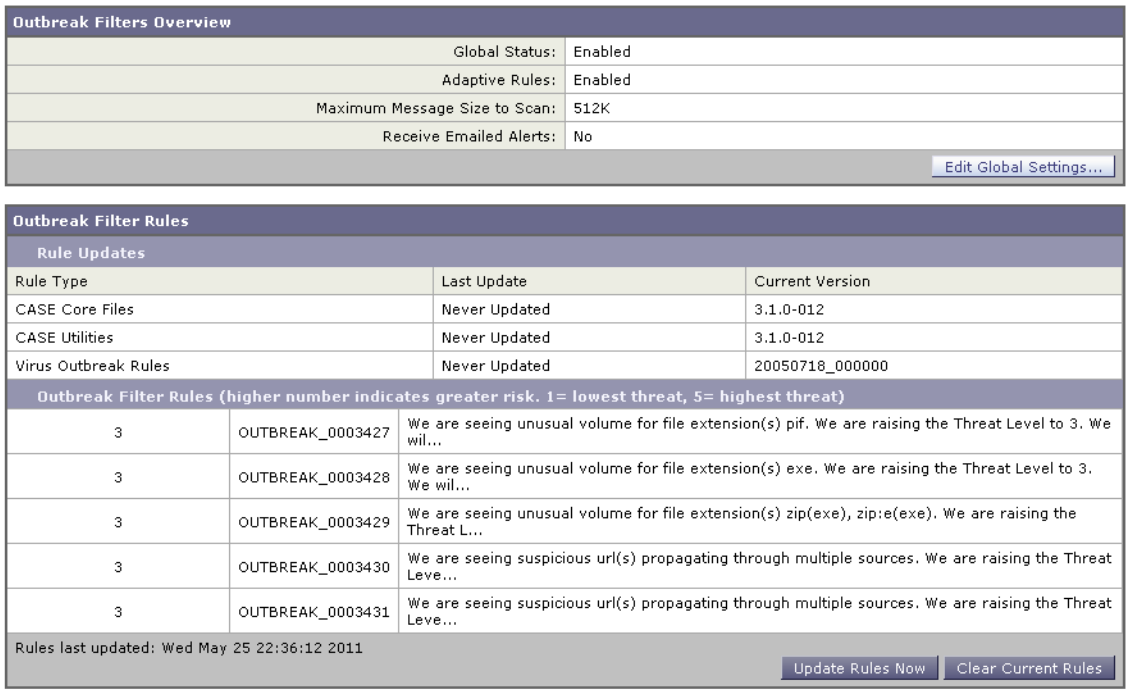
표 14-3 신종 바이러스 라이프사이클의 규칙 예

시간	규칙 유형	규칙 설명	조치
T=0	적응 규칙(과거 신종 바이러스 기반)	100K 이상의 메시지 특성을 기반으로 하는 통합 규칙 집합으로, 메시지 콘텐츠, 컨텍스트 및 구조 분석	적응 규칙과 일치할 경우 메시지가 자동으로 격리됨
T=5분	신종 바이러스 규칙	.zip(exe) 파일이 포함된 신종 바이러스 메시지	.exe가 포함된 .zip인 모든 첨부 파일 격리
T=10분	신종 바이러스 규칙	50KB를 초과하는 .zip(exe) 파일이 포함된 메시지 격리	50KB 미만의 .zip(exe) 파일이 포함된 메시지는 격리에서 릴리스됨
T=20분	신종 바이러스 규칙	50~55KB의 .zip(exe) 파일이 포함되어 있고 파일 이름에 "Price"가 있는 메시지 격리	이 조건과 일치하지 않는 메시지는 격리에서 릴리스됨
T=12시간	신종 바이러스 규칙	새로운 서명을 기준으로 검사	나머지 모든 메시지는 최신 안티바이러스 서명을 기준으로 검사됨

신종 바이러스 필터(Outbreak Filter) 관리

GUI(그래픽 사용자 인터페이스)에 로그인해 메뉴에서 Security Services(보안 서비스)를 선택한 다음 신종 바이러스 필터(Outbreak Filter)를 클릭합니다.

그림 14-2 신종 바이러스 필터(Outbreak Filter) 기본 페이지



신종 바이러스 페이지에는 2개의 섹션(신종 바이러스 필터(Outbreak Filter) 개요 및 최신 신종 바이러스 필터(Outbreak Filter) 규칙 목록(있는 경우))이 표시됩니다.

그림 14-2에서는 신종 바이러스 필터(Outbreak Filter)와 적응형 검사가 활성화되어 있고 최대 메시지가 크기가 512k로 설정되어 있습니다. 이러한 설정을 변경하려면 **Edit Global Settings(전역 설정 편집)**를 클릭합니다. 전역 설정 편집에 대한 자세한 내용은 신종 바이러스 필터(Outbreak Filter) 전역 설정 구성, 14-12페이지를 참조하십시오.

신종 바이러스 필터(Outbreak Filter) 규칙 섹션에는 위협 수준이 포함된 최신 신종 바이러스 필터(Outbreak Filter) 규칙 목록뿐 아니라 다양한 구성 요소(규칙 자체뿐 아니라 규칙 엔진도 포함)의 최신 업데이트의 시간, 날짜 및 버전도 표시됩니다.

신종 바이러스 규칙에 대한 자세한 내용은 신종 바이러스 필터(Outbreak Filter) 규칙, 14-15페이지를 참조하십시오.

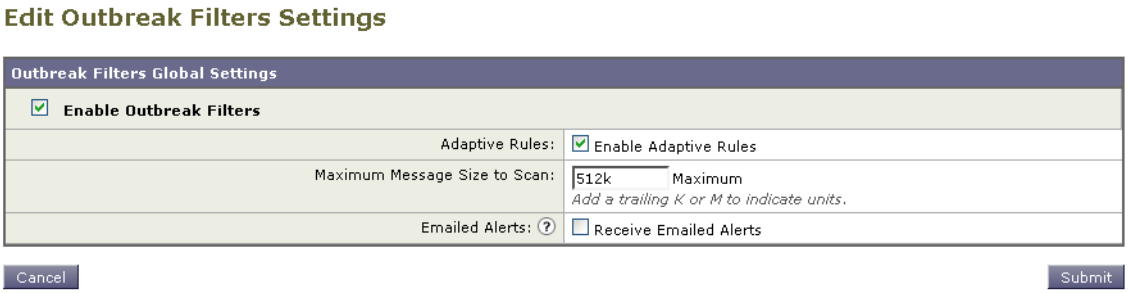
관련 주제

- 신종 바이러스 필터(Outbreak Filter) 전역 설정 구성, 14-12페이지
- 신종 바이러스 필터(Outbreak Filter) 규칙, 14-15페이지
- 신종 바이러스 필터(Outbreak Filter) 기능 및 메일 정책, 14-16페이지
- 신종 바이러스 필터 기능 및 신종 바이러스 격리, 14-21페이지

신종 바이러스 필터(Outbreak Filter) 전역 설정 구성

신종 바이러스 필터(Outbreak Filter)의 전역 설정을 구성하려면 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

그림 14-3 신종 바이러스 필터(Outbreak Filter) 전역 설정 페이지



이 페이지에서 다음을 수행할 수 있습니다.

- 신종 바이러스 필터(Outbreak Filter)를 전역적으로 활성화
- 적응 규칙 검사 활성화
- 검사할 파일의 최대 크기 설정(크기를 *바이트*로 입력)
- 신종 바이러스 필터(Outbreak Filter)에 대한 경고 활성화

경고 및 적응 규칙이 기본적으로 활성화되었는지 확인 이 기능은 `outbreakconfig` CLI 명령(*Cisco AsyncOS CLI 참조 설명서* 참조)을 통해서도 사용할 수 있습니다. 변경한 후 변경 사항을 제출 및 커밋합니다.

참고 웹 인터페이스를 사용하여 URL 로깅을 활성화할 수 없습니다. CLI를 사용하여 URL 로깅을 활성화하는 지침은 URL 로깅 활성화, 14-14페이지를 참조하십시오.

신종 바이러스 필터(Outbreak Filter) 기능 활성화

신종 바이러스 필터 기능을 전역적으로 활성화하려면 신종 바이러스 필터(Outbreak Filter) 전역 설정 페이지의 신종 바이러스 필터(Outbreak Filter) 활성화 옆의 확인란을 선택하고 **Submit(제출)**을 클릭합니다. 먼저 신종 바이러스 필터(Outbreak Filter) 라이센스 계약에 동의해야 합니다.

신종 바이러스 필터(Outbreak Filter) 기능이 전역적으로 활성화되면 기본 정책을 포함하여 각 수신 및 발송 메일 정책에 대해 이를 개별적으로 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 신종 바이러스 필터(Outbreak Filter) 기능 및 메일 정책, 14-16페이지를 참고하십시오.

신종 바이러스 필터(Outbreak Filter) 기능은 안티스팸 검사가 활성화되었는지에 관계없이 CASE(컨텍스트 적응형 검사 엔진)를 사용하여 바이러스 위협을 탐지하지만 비 바이러스 위협을 검사하려면 어플라이언스에서 전역적으로 안티스팸 또는 Intelligent Multi-Scan을 활성화해야 합니다.

참고 시스템 설정 도중 아직 라이센스 계약에 동의하지 않은 경우 (4단계: 보안, 3-21페이지 참조) Security Services(보안 서비스) > Outbreak Filters(신종 바이러스 필터) 페이지에서 **Enable(활성화)**을 클릭한 다음 라이센스 계약을 읽고 동의해야 합니다.

적응 규칙 활성화

적응형 검사는 신종 바이러스 필터(Outbreak Filter)에서 적응 규칙을 사용할 수 있습니다. 요소 또는 특성(파일 크기 등) 집합은 메시지의 콘텐츠와 관련된 바이러스 서명 또는 스팸 조건을 사용할 수 없는 경우 메시지가 신종 바이러스의 일부일 가능성을 결정하는 데 사용됩니다. 적응형 검사를 활성화하려면 신종 바이러스 필터(Outbreak Filter) 전역 설정 페이지에서 적응 규칙 활성화 옆의 상자를 선택하고 **Submit(제출)**을 클릭합니다.

신종 바이러스 필터(Outbreak Filter)에 대한 경고 활성화

"이메일 경고"라는 라벨이 표시된 상자를 선택하여 신종 바이러스 필터(Outbreak Filter) 기능에 대한 경고를 활성화할 수 있습니다. 신종 바이러스 필터(Outbreak Filter)에 대한 이메일 경고를 활성화하면 단지 경고 엔진이 신종 바이러스 필터(Outbreak Filter)에 대한 경고를 전송할 수 있습니다. 시스템 관리 탭의 경고 페이지를 통해 전송할 메시지와 이메일 주소 지정을 구성합니다. 신종 바이러스 필터(Outbreak Filter) 경고 구성에 대한 자세한 내용은 경고, SNMP 트랩 및 신종 바이러스 필터(Outbreak Filter), 14-24페이지를 참조하십시오.

URL 로깅 활성화

URL 관련 로그의 로깅은 기본적으로 비활성화되어 있습니다. 여기에는 다음 이벤트에 대한 로그가 포함됩니다.

- 메시지의 URL 범주가 URL 범주 필터와 일치
- 메시지의 URL 평판 점수가 URL 평판 필터와 일치
- 신종 바이러스 필터(Outbreak Filter)가 메시지의 URL 재작성

CLI에서 `outbreakconfig` 명령을 사용하여 이러한 이벤트의 로깅을 활성화합니다.

관련 주제

- 예, 14-14페이지

예

다음 예제는 `outbreakconfig` 명령을 사용하여 URL 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.
[]>
```

신종 바이러스 필터(Outbreak Filter) 규칙

신종 바이러스 규칙은 Cisco Security Intelligence Operations에서 게시하며 어플라이언스가 5분마다 새로운 신종 바이러스 규칙을 확인하고 다운로드합니다. 이 업데이트 간격을 변경할 수 있습니다. 자세한 내용은 업그레이드 및 업데이트를 다운로드하도록 서버 설정 구성, 33-21페이지를 참조하십시오.

관련 주제

- 신종 바이러스 필터(Outbreak Filter) 규칙 관리, 14-15페이지

신종 바이러스 필터(Outbreak Filter) 규칙 관리

신종 바이러스 필터(Outbreak Filter) 규칙이 자동으로 다운로드되므로 사용자의 입장에서 사실상 관리가 필요하지 않습니다.

그러나 몇 가지 이유로 일정 기간 동안 어플라이언스가 Cisco의 업데이트 서버에 액세스하여 새 규칙을 다운로드할 수 없는 경우 로컬에서 캐시된 점수가 더 이상 유효하지 않을 수 있습니다(즉, 현재 알려진 바이러스 첨부 파일 유형이 안티바이러스 소프트웨어의 업데이트를 포함하거나 더 이상 위협이 아닌 경우). 지금은 이러한 특성이 있는 메시지를 더 이상 격리하려 하지 않을 수 있습니다.

Update Rules Now(지금 규칙 업데이트)를 클릭하여 Cisco의 업데이트 서버에서 업데이트된 신종 바이러스 규칙을 수동으로 다운로드할 수 있습니다.

참고 **Update Rules Now(지금 규칙 업데이트)** 버튼은 어플라이언스의 모든 기존 신종 바이러스 규칙을 "플러싱"하지 않습니다. 단지 업데이트된 신종 바이러스 규칙을 교체합니다. Cisco의 업데이트 서버에 사용할 수 있는 업데이트가 없으면 이 버튼을 클릭해도 어플라이언스가 신종 바이러스 규칙을 다운로드하지 않습니다.

관련 주제

- 신종 바이러스 필터(Outbreak Filter) 규칙 업데이트, 14-15페이지

신종 바이러스 필터(Outbreak Filter) 규칙 업데이트

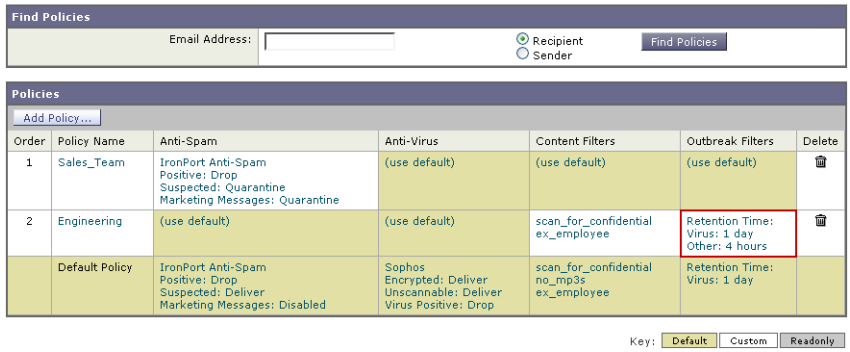
기본적으로 어플라이언스가 5분마다 새로운 신종 바이러스 필터(Outbreak Filter) 규칙 다운로드를 시도합니다. Security Services(보안 서비스) > Service Updates(서비스 업데이트) 페이지를 통해 이 간격을 변경할 수 있습니다. 자세한 내용은 서비스 업데이트, 33-17페이지를 참고하십시오.

신종 바이러스 필터(Outbreak Filter) 기능 및 메일 정책

신종 바이러스 기능은 메일 정책별로 지정할 수 있는 설정이 있습니다. 어플라이언스의 각 메일 정책에 대해 신종 바이러스 필터(Outbreak Filter) 기능을 활성화하거나 비활성화할 수 있습니다. 메일 정책별로 특정 파일 확장자와 도메인을 신종 바이러스 필터(Outbreak Filter) 기능을 통한 처리에서 제외할 수 있습니다. 이 기능은 `policyconfig` CLI 명령(*Cisco AsyncOS CLI 참조 설명서* 참조)을 통해서도 사용할 수 있습니다.

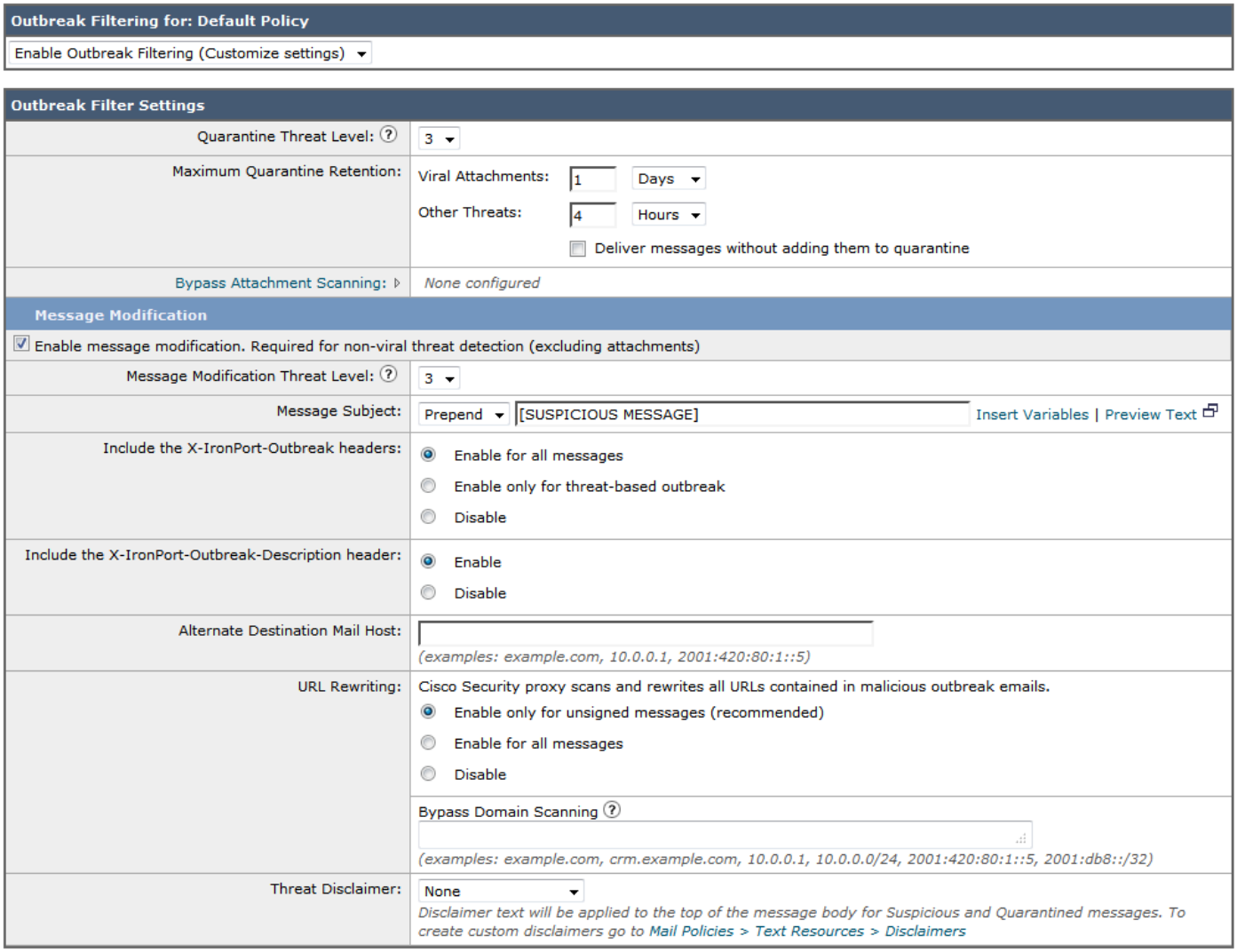
참고 신종 바이러스 필터(Outbreak Filter) 기능이 비 바이러스 위협을 검사할 수 있도록 하려면 어플라이언스에서 안티스팸 또는 Intelligent Multi-Scan 검사를 전역적으로 활성화해야 합니다.

그림 14-4 메일 정책 목록



특정 메일 정책의 신종 바이러스 필터(Outbreak Filter) 기능 설정을 수정하려면 변경할 정책의 신종 바이러스 필터(Outbreak Filter) 열에서 해당 링크를 클릭합니다.

그림 14-5 신종 바이러스 필터(Outbreak Filter) 설정 및 메일 정책



특정 메일 정책에 대해 신종 바이러스 필터(Outbreak Filter) 기능을 활성화하고 사용자 지정하려면 **Enable Outbreak Filtering (Customize Settings)(신종 바이러스 필터링 활성화(사용자 지정 설정))**을 선택합니다.

메일 정책에 대해 다음 신종 바이러스 필터(Outbreak Filter) 설정을 구성할 수 있습니다.

- 격리 위협 수준
- 최대 격리 보관 시간
- 격리에 추가하지 않고 비 바이러스 위협 메시지를 즉시 전송
- 우회할 파일 확장자 유형
- 메시지 수정 임계값
- 사용자 지정 텍스트 및 `$threat_verdict`, `$threat_category`, `$threat_type`, `$threat_description` 및 `$threat_level`과 같은 신종 바이러스 필터(Outbreak Filter) 변수를 사용하여 제목 헤더를 변경합니다.
- 다음 이메일 헤더를 포함합니다.
  - X-IronPort-Outbreak-Status
  - X-IronPort-Outbreak-Description

- Email Security 어플라이언스 또는 교환 서버와 같은 대체 대상으로 메시지를 전송합니다.
- URL 재작성
- 위협 고지 사항

기본 메일 정책에 대해 정의된 신종 바이러스 필터(Outbreak Filter) 설정을 사용하려면 **Enable Outbreak Filtering (Inherit Default mail policy settings)(신종 바이러스 필터링 활성화(기본 메일 정책 설정 상속))**을 선택합니다. 기본 메일 정책에서 신종 바이러스 필터(Outbreak Filter) 기능이 활성화된 경우 기타 모든 메일 정책은 사용자 지정된 경우를 제외하고 동일한 신종 바이러스 필터(Outbreak Filter) 설정을 사용합니다.

변경한 후에는 변경 사항을 커밋합니다.

관련 주제

- 격리 수준 임계값 설정, 14-18페이지
- 최대 격리 보관, 14-18페이지
- 파일 확장자 유형 우회, 14-18페이지
- 메시지 수정, 14-19페이지

격리 수준 임계값 설정

목록에서 신종 바이러스 위협의 신종 바이러스 위협 수준 임계값을 선택합니다. 숫자가 작아질수록 더 많은 메시지가 격리되고, 숫자가 커질수록 더 적은 메시지가 격리됨을 의미합니다. Cisco에서는 기본값으로 3을 설정할 것을 권장합니다.

자세한 내용은 격리 위협 수준 임계값 설정 지침, 14-8페이지를 참고하십시오.

최대 격리 보관

메시지가 신종 바이러스 격리에 유지되는 최대 시간(시간 또는 일)을 지정합니다. 바이러스 첨부 파일이 포함될 수 있는 메시지와 피싱 또는 맬웨어 링크와 같은 다른 위협이 포함될 수 있는 메시지에 대해 서로 다른 보관 시간을 지정할 수 있습니다. 비 바이러스 위협의 경우 **Deliver messages without adding them to quarantine(격리에 추가하지 않고 메시지 전송)** 확인란을 선택하여 격리에 추가하지 않고 메시지를 즉시 전송합니다.

참고 정책의 메시지 수정을 활성화하지 않는 한 비 바이러스 위협을 격리할 수 없습니다.

CASE는 메시지에 위협 수준을 지정할 때 격리 보관 기간을 권장합니다. Email Security 어플라이언스가 CASE에서 권장하는 기간 동안(이 기간이 해당 위협 유형의 최대 격리 보관 시간을 초과하지 않는 경우) 메시지를 격리된 상태로 유지합니다.

파일 확장자 유형 우회

특정 파일 유형을 우회하도록 정책을 수정할 수 있습니다. CASE에서 메시지의 위협 수준을 계산할 때 우회된 파일 확장자가 포함되지 않지만 이메일 보안 파이프라인의 나머지 부분에서 첨부 파일을 여전히 처리합니다.

파일 확장자를 우회하려면 Bypass Attachment Scanning(첨부 파일 검사 우회)을 클릭하고 파일 확장자를 선택하거나 입력한 다음 **Add Extension(확장자 추가)**을 클릭합니다. AsyncOS가 우회할 파일 확장자 목록에 확장자 유형을 표시합니다.

우회된 확장자 목록에서 확장자를 제거하려면 우회할 파일 확장자 목록의 확장자 옆에 있는 휴지통 아이콘을 클릭합니다.

관련 주제

- 파일 확장자 우회: 콘텐츠 필터 유형, 14-19페이지

파일 확장자 우회: 콘텐츠 필터 유형

파일 확장자를 우회할 경우 확장자가 우회할 확장자 목록에 없으면 컨테이너 파일 내의 파일(예: .zip 내의 .doc 파일)이 우회됩니다. 예를 들어, 우회할 확장자 목록에 .doc를 추가할 경우 컨테이너 파일 내의 모든 .doc 파일도 우회됩니다.

메시지 수정

어플라이언스가 피싱 시도 또는 맬웨어 웹사이트 링크와 같은 비 바이러스 위협이 있는지 확인하기 위해 메시지를 검사하려면 메시지 수정을 활성화합니다.

수신자가 메시지의 웹사이트를 열려고 시도할 경우 메시지의 위협 수준에 따라 AsyncOS에서 모든 URL을 재작성하여 Cisco Web Security 프록시를 통해 수신자를 리디렉션하도록 메시지를 수정할 수 있습니다. 어플라이언스가 사용자에게 메시지의 콘텐츠가 의심스럽거나 악성임을 경고하는 고지 사항을 메시지가 추가할 수도 있습니다.

비 바이러스 위협 메시지를 격리하려면 메시지 수정을 활성화해야 합니다.

관련 주제

- 메시지 수정 위협 수준, 14-19페이지
- 메시지 제목, 14-19페이지
- 신종 바이러스 필터(Outbreak Filter) 이메일 헤더, 14-20페이지
- 대체 대상 메일 호스트, 14-20페이지
- URL 재작성 및 도메인 우회, 14-20페이지
- 위협 고지 사항, 14-21페이지

메시지 수정 위협 수준

목록에서 메시지 수정 위협 수준 임계값을 선택합니다. 이 설정은 CASE에서 반환한 위협 수준에 따라 메시지를 수정할지 여부를 결정합니다. 숫자가 작아질수록 더 많은 메시지가 수정되고, 숫자가 커질수록 더 적은 메시지가 수정됨을 의미합니다. Cisco에서는 기본값으로 3을 설정할 것을 권장합니다.

메시지 제목

수정된 링크가 포함된 비 바이러스 위협 메시지의 제목 헤더 텍스트를 변경하여 사용자에게 보호를 위해 메시지가 수정되었음을 알릴 수 있습니다. 사용자 지정 텍스트 또는 `$threat_verdict`, `$threat_category`, `$threat_type`, `$threat_description`, `$threat_level`과 같은 신종 바이러스 필터(Outbreak Filter) 변수 또는 이 둘의 조합을 제목 헤더의 앞 또는 뒤에 추가합니다. 변수를 삽입하려면 **Insert Variables(변수 삽입)**를 클릭하고 변수 목록에서 선택합니다.

메시지 제목 필드의 공백은 무시됩니다. 이 필드에 입력하는 텍스트의 뒤(뒤에 추가될 경우) 또는 앞(앞에 추가될 경우)에 공백을 추가하여 추가한 텍스트를 메시지의 원래 제목과 구분합니다. 예를 들어, 앞에 추가할 경우 몇 개의 후행 공백을 포함한 `[MODIFIED FOR PROTECTION]` 텍스트를 추가합니다.

참고 메시지 제목 필드에는 US-ASCII 문자만 사용할 수 있습니다.

신종 바이러스 필터(Outbreak Filter) 이메일 헤더

메시지에 다음 추가 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`	• 모든메시지에 대해 사용 • 비 바이러스 신종 바이러스에 대해서만 사용 • 사용 안 함
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.`	• 사용 • 사용 안 함

참고 이러한 헤더를 기반으로 메시지를 필터링하려면 대체 대상 메일 호스트를 구성하여 신종 바이러스 필터(Outbreak Filter)에서 처리된 메시지를 Email Security 어플라이언스로 다시 전송해 이러한 헤더와 일치하는 콘텐츠 필터를 사용하여 이러한 메시지를 검사해야 합니다.

대체 대상 메일 호스트

신종 바이러스 필터(Outbreak Filter)에서 처리된 메시지에 대해 콘텐츠 파일 기반 검사를 수행하려면 처리된 메시지를 Email Security 어플라이언스로 다시 보내도록 신종 바이러스 필터(Outbreak Filter)를 구성해야 합니다. 이는 처리 파이프라인에서 콘텐츠 필터 검사 후에 신종 바이러스 필터(Outbreak Filter) 검사가 수행되기 때문입니다.

Alternate Destination Mail Host(대체 대상 메일 호스트) 필드에 추가 검사를 위해 처리된 메시지를 보낼 어플라이언스의 IP 주소(IPv4 또는 IPv6) 또는 FQDN을 입력합니다.

URL 재작성 및 도메인 우회

메시지의 위협 수준이 메시지 수정 임계값을 초과할 경우 사용자가 해당 링크를 클릭할 때 사용자를 Cisco Web Security 프록시의 스플래시 페이지로 리디렉션하도록 신종 바이러스 필터(Outbreak Filter) 기능을 사용하여 메시지의 모든 URL을 재작성합니다. (자세한 내용은 URL 리디렉션, 14-5 페이지를 참조하십시오.) 메시지의 위협 수준이 격리 임계값을 초과할 경우 어플라이언스가 또한 메시지를 격리합니다. 소규모의 비 신종 바이러스가 진행 중인 경우 메시지를 격리하면 가능한 신종 바이러스 메시지에서 링크된 의심스러운 웹사이트를 분석하여 웹사이트가 악성인지 결정하기 위한 TOC 시간이 지정됩니다. CASE는 SIO의 업데이트된 신종 바이러스 규칙을 사용하여 메시지를 검사해 메시지가 신종 바이러스에 해당되는지 확인합니다. 보관 기관이 만료되면 어플라이언스가 메시지를 격리에서 릴리스합니다.

AsyncOS가 우회된 도메인을 가리키는 URL을 제외하고 메시지 안의 모든 URL을 재작성합니다.

다음 옵션을 사용하여 URL을 재작성할 수 있습니다.

- **서명되지 않은 메시지에 대해서만 사용**. 이 옵션을 통해 AsyncOS가 메시지 수정 임계값을 충족하거나 초과하는 서명되지 않은 메시지(서명된 메시지 제외)의 URL을 재작성할 수 있습니다. Cisco에서는 URL 재작성 시 이 설정을 사용할 것을 권장합니다.

참고 Email Security 어플라이언스가 DomainKeys/DKIM 서명 메시지의 URL을 재작성하고 Email Security 어플라이언스가 아닌 네트워크의 서버 또는 어플라이언스에서 DomainKeys/DKIM 서명 확인을 수행할 경우 메시지의 서명을 무효화할 수 있습니다.

- **모든 메시지에 대해 사용.** 이 옵션을 통해 AsyncOS가 메시지 수정 임계값을 충족하거나 초과하는 모든 메시지(서명된 메시지 포함)의 URL을 재작성할 수 있습니다. AsyncOS가 서명된 메시지를 수정하면 서명이 무효화됩니다.
- **사용 안 함.** 이 옵션을 사용하면 신종 바이러스 필터(Outbreak Filter)에 대해 URL 재작성이 비활성화됩니다.

특정 도메인에 대한 URL을 수정에서 제외하도록 정책을 수정할 수 있습니다. 도메인을 우회하려면 도메인 검사 우회 필드에 IPv4 주소, IPv6 주소, CIDR 범위, 호스트 이름, 부분 호스트 이름 또는 도메인을 입력합니다. 항목이 여러 개인 경우 쉼표로 구분합니다.

도메인 검사 우회 기능은 URL 필터링에 사용되는 전역 허용 목록과 유사하지만 이와 무관합니다. 허용 목록에 대한 자세한 내용은 URL 필터링 허용 목록 생성, 15-4페이지를 참조하십시오.

위협 고지 사항

Email Security 어플라이언스가 의심스러운 메시지의 머리글 위에 고지 사항 메시지를 추가하여 사용자에게 메시지의 콘텐츠를 경고합니다. 이 고지 사항은 메시지의 유형에 따라 HTML 또는 일반 텍스트일 수 있습니다.

위협 고지 사항 목록에서 사용할 고지 사항 텍스트를 선택하거나 Mail Policies(메일 정책) > Text Resources(텍스트 리소스) 링크를 클릭하여 고지 사항 템플릿을 사용하여 새 고지 사항을 생성합니다. 고지 사항 템플릿에는 신종 바이러스 위협 정보에 대한 변수가 포함됩니다. 고지 사항 미리보기를 클릭하여 위협 고지 사항의 미리보기를 볼 수 있습니다. 사용자 지정 고지 사항 메시지의 경우 변수를 사용하여 메시지의 위협 수준, 위협 유형, 위협에 대한 설명을 표시할 수 있습니다. 고지 사항 메시지 생성에 대한 내용은 텍스트 리소스 관리의 개요, 21-9페이지를 참조하십시오.

신종 바이러스 필터 기능 및 신종 바이러스 격리

신종 바이러스 필터(Outbreak Filter) 기능을 통해 격리된 메시지는 신종 바이러스 격리로 전송됩니다. 이 격리 기능은 "요약 보기가 있고 메시지를 격리에 배치하는 데 사용된 규칙(신종 바이러스 규칙의 경우 신종 바이러스 ID가 표시되고 적응 규칙의 경우 일반 용어가 표시됨)에 따라 격리에서 모든 메시지를 삭제하거나 릴리스할 때 유용하다는 점을 제외하고 다른 격리(격리 사용에 대한 자세한 내용은 30 장, "정책, 바이러스 및 신종 바이러스 격리" 참조)와 유사합니다. 요약 보기에 대한 자세한 내용은 신종 바이러스 격리 및 규칙 요약에 따름 보기, 14-22페이지를 참조하십시오.

관련 주제

- 신종 바이러스 격리 모니터링, 14-22페이지
- 신종 바이러스 격리 및 규칙 요약에 따름 보기, 14-22페이지

신종 바이러스 격리 모니터링

모니터링 시 올바르게 구성된 격리가 거의 필요하지 않지만 특히 정상적인 메시지가 지연될 수 있는 신종 바이러스 발생 도중 및 후에 신종 바이러스 격리를 지켜보는 것이 좋습니다.

정상적인 메시지가 격리될 경우 신종 바이러스 격리의 설정에 따라 다음 중 하나가 발생합니다.

- 격리의 기본 작업이 릴리스로 설정된 경우 보관 기간이 만료되거나 격리가 오버플로될 경우 메시지가 릴리스됩니다. 오버플로로 인해 메시지가 릴리스되기 전에 메시지에 대해 첨부 파일 제거, 제목 수정 및 X-헤더 추가 등의 작업이 수행되도록 신종 바이러스 격리를 구성할 수 있습니다. 이러한 작업에 대한 자세한 내용은 자동으로 처리된 격리 메시지에 대한 기본 작업, 30-4페이지를 참조하십시오.
- 격리의 기본 작업이 삭제로 설정된 경우 보관 기간이 만료되거나 격리가 오버플로될 경우 메시지가 릴리스됩니다.
- 격리가 꽉 차고 더 많은 메시지가 추가되면 오버플로가 발생합니다. 이 경우 새 메시지를 보관할 충분한 공간이 확보될 때까지 만료일이 가장 가까운 메시지(반드시 가장 오래된 메시지일 필요는 없음)가 먼저 릴리스됩니다. 오버플로로 인해 메시지가 릴리스되기 전에 메시지에 대해 첨부 파일 제거, 제목 수정 및 X-헤더 추가 등의 작업이 수행되도록 신종 바이러스 격리를 구성할 수 있습니다.

새 규칙이 게시될 때마다 격리된 메시지가 재검사되므로 신종 바이러스 격리의 메시지가 만료 시간 전에 릴리스될 가능성이 높습니다.

여전히 기본 작업이 삭제로 설정된 경우 신종 바이러스 격리를 모니터링하는 것이 중요할 수 있습니다. Cisco에서는 대부분의 사용자에게 기본 작업을 삭제로 설정하지 말 것을 권장합니다. 신종 바이러스 격리에서 메시지 릴리스 또는 신종 바이러스 격리의 기본 작업 변경에 대한 자세한 내용은 자동으로 처리된 격리 메시지에 대한 기본 작업, 30-4페이지를 참조하십시오.

반면, 새 규칙 업데이트를 기다리면서 신종 바이러스 격리에 더 오랫동안 보관할 메시지가 있는 경우 그러한 메시지의 만료를 지연시킬 수 있습니다. 메시지의 보관 시간을 높이면 격리의 크기가 확장될 수 있습니다.

참고 메시지가 신종 바이러스 격리에 있는 동안 안티바이러스 검사가 전역적으로 비활성화될 경우(메일 정책을 통하지 않음) 메시지가 격리에서 릴리스되기 전에 안티바이러스 검사가 다시 활성화되어도 메시지가 격리에서 떠날 때 안티바이러스 검사가 수행되지 않습니다.

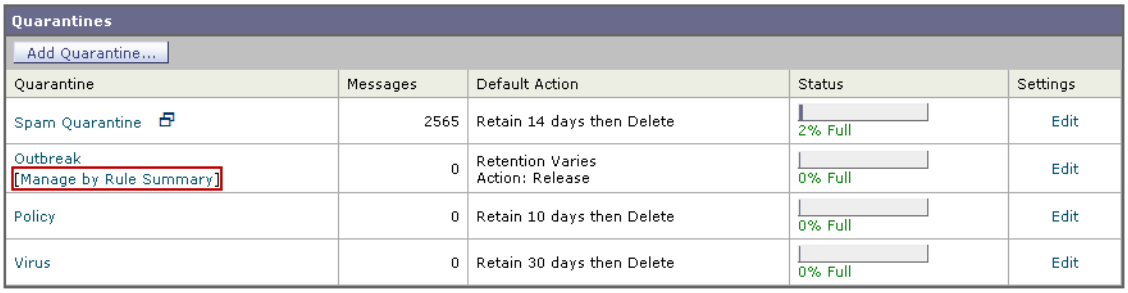
참고 어플라이언스에서 안티바이러스 검사를 활성화하지 않고도 신종 바이러스 필터(Outbreak Filter) 기능을 사용할 수 있습니다. 그러나 어플라이언스에서 안티스팸 검사가 활성화되지 않은 경우 신종 바이러스 필터(Outbreak Filter)가 비 바이러스 위협을 검사할 수 없습니다.

신종 바이러스 격리 및 규칙 요약에 따름 보기

GUI의 모니터 메뉴의 목록에서 격리의 이름을 클릭하여 신종 바이러스 격리의 콘텐츠를 볼 수 있습니다. 신종 바이러스 격리에는 추가 보기인 신종 바이러스 격리 규칙 요약에 따름 링크도 있습니다.

그림 14-6 신종 바이러스 격리 규칙 요약에 따름 링크

Quarantines



관련 주제

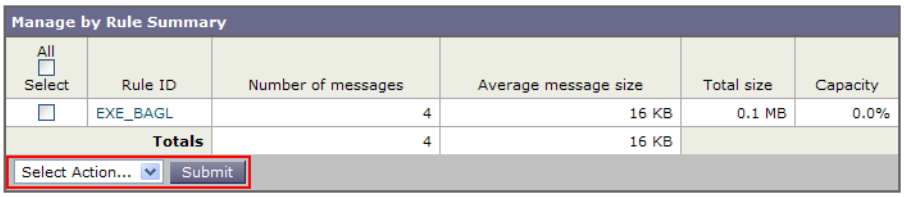
- 요약 보기를 사용하여 규칙 ID를 기반으로 신종 바이러스 격리의 메시지에 대해 메시지 작업 수행., 14-23페이지

요약 보기를 사용하여 규칙 ID를 기반으로 신종 바이러스 격리의 메시지에 대해 메시지 작업 수행.

규칙 요약에 따름 링크를 클릭하여 신종 바이러스 격리의 콘텐츠 목록을 규칙 ID별로 그룹화하여 볼 수 있습니다.

그림 14-7 신종 바이러스 격리 규칙 요약에 따름 보기

Outbreak Quarantine Summary



개별 메시지를 선택하지 않고 이 보기에서 특정 신종 바이러스 또는 적응 규칙에 관한 모든 메시지를 릴리스하거나 삭제하거나 종료를 지연시킬 수 있습니다. 또한 목록을 검색하거나 정렬할 수 있습니다.

이 기능은 `quarantineconfig -> outbreakmanage` CLI 명령을 통해서도 사용할 수 있습니다. 자세한 내용은 *Cisco AsyncOS CLI 참조 설명서*를 참조하십시오.

신종 바이러스 필터(Outbreak Filter) 모니터링

어플라이언스에는 신종 바이러스 필터(Outbreak Filter) 기능의 성능과 활동을 모니터링할 수 있는 여러 툴이 포함되어 있습니다.

관련 주제

- 신종 바이러스 필터(Outbreak Filter) 보고서, 14-24페이지
- 신종 바이러스 필터(Outbreak Filter) 개요 및 규칙 목록, 14-24페이지
- 신종 바이러스 격리, 14-24페이지
- 경고, SNMP 트랩 및 신종 바이러스 필터(Outbreak Filter), 14-24페이지

신종 바이러스 필터(Outbreak Filter) 보고서

신종 바이러스 필터(Outbreak Filter) 보고서에 최근에 신종 바이러스 필터(Outbreak Filter)로 인해 격리된 신종 바이러스 및 메시지에 대한 정보뿐 아니라 어플라이언스의 신종 바이러스 필터(Outbreak Filter)의 현재 상태 및 구성이 표시됩니다. Monitor(모니터링) > Outbreak Filters(신종 바이러스 필터(Outbreak Filter)) 페이지에서 이 정보를 확인합니다. 자세한 내용은 "이메일 보안 모니터링" 장을 참조하십시오.

신종 바이러스 필터(Outbreak Filter) 개요 및 규칙 목록

개요 및 규칙 목록은 신종 바이러스 필터(Outbreak Filter) 기능의 현재 상태에 대한 유용한 정보를 제공합니다. Security Services(보안 서비스) > Outbreak Filters(신종 바이러스 필터(Outbreak Filter)) 페이지를 통해 이 정보를 볼 수 있습니다.

신종 바이러스 격리

신종 바이러스 격리를 사용하여 신종 바이러스 필터(Outbreak Filter) 위협 수준 임계값으로 플래그가 지정되는 메시지의 수를 모니터링할 수 있습니다. 또한 격리된 메시지의 목록을 규칙별로 표시할 수 있습니다. 자세한 내용은 신종 바이러스 격리 및 규칙 요약에 따름 보기, 14-22페이지 및 30장, "정책, 바이러스 및 신종 바이러스 격리"를 참조하십시오.

경고, SNMP 트랩 및 신종 바이러스 필터(Outbreak Filter)

신종 바이러스 필터(Outbreak Filter) 기능은 2가지 유형의 알림(정기적인 AsyncOS 경고 및 SNMP 트랩)을 지원합니다.

SNMP 트랩은 규칙 업데이트가 실패할 때 생성됩니다. AsyncOS의 SNMP 트랩에 대한 자세한 내용은 "CLI를 통한 관리 및 모니터링" 장을 참조하십시오.

AsyncOS에는 2가지 유형의 신종 바이러스 필터(Outbreak Filter) 기능(크기 및 규칙)이 있습니다.

AsyncOS 경고는 신종 바이러스 격리의 크기가 최대 크기의 5, 50, 75, 95%를 초과할 때마다 생성됩니다. 95% 임계값에 대해 생성되는 경고의 심각도는 CRITICAL이고, 나머지 경고 임계값은 WARNING입니다. 격리 크기가 증가할 때 임계값이 교차되면 경고가 생성됩니다. 격리 크기가 감소할 때 임계값이 교차되면 경고가 생성되지 않습니다. 경고에 대한 자세한 내용은 경고, 33-34페이지를 참조하십시오.

AsyncOS는 규칙이 게시되거나, 임계값이 변경되거나, 규칙 또는 CASE 엔진 업데이트 도중 문제가 발생할 경우에도 경고를 생성합니다.

신종 바이러스 필터(Outbreak Filter) 기능 문제 해결

이 섹션에서는 신종 바이러스 필터(Outbreak Filter) 기능에 대한 기본적인 문제 해결 팁을 제공합니다.

관련 주제

- Cisco에 잘못 분류된 메시지 보고, 14-25페이지

- 여러 첨부 파일 및 우회된 파일 유형, 14-25페이지
- 메시지 필터, 콘텐츠 필터 및 이메일 파이프라인, 14-25페이지

Cisco에 잘못 분류된 메시지 보고

신종 바이러스 격리의 격리 관리 페이지의 확인란을 사용하여 Cisco에 메시지가 잘못 분류되었음을 알립니다.

여러 첨부 파일 및 우회된 파일 유형

우회된 파일 유형은 메시지에 해당 유형의 첨부 파일만 있거나, 파일이 여러 개일 때 다른 첨부 파일에 아직 기존 규칙이 없는 경우에만 제외됩니다. 그렇지 않을 경우 메시지가 검사됩니다.

메시지 필터, 콘텐츠 필터 및 이메일 파이프라인

신종 바이러스 필터(Outbreak Filter)에서 검사하기 전에 메시지 및 콘텐츠 필터가 메시지에 적용됩니다. 필터를 사용하면 메시지가 신종 바이러스 필터(Outbreak Filter) 검사를 건너뛰거나 우회할 수 있습니다.

15 장

URL 필터링

URL 필터링 개요

URL 필터링은 메시지에 포함된 URL 링크의 평판과 범주를 사용하여 다음을 수행합니다.

- 메시지의 악성 URL의 보호 효과를 높임

  URL 필터링은 신종 바이러스 필터(Outbreak Filter)에 통합되어 있습니다. 이 강화된 보호는 진입 시점에 위협을 차단하므로 조직에 이미 Cisco Web Security Appliance나 이와 유사한 웹 기반 위협 차단 프로그램이 있는 경우에도 유용합니다.

  또한 콘텐츠 또는 메시지 필터를 사용하여 메시지에 포함된 URL의 WBRS(Web Based Reputation 점수)를 기반으로 작업을 수행할 수 있습니다. 예를 들어, Cisco Web Security 프록시로 리디렉션하여 클릭 시간 평가를 통해 안전성을 확인받도록 의심스럽거나 평판을 알 수 없는 URL을 재작성할 수 있습니다.

- 더 효과적인 스팸 식별

  어플라이언스가 메시지에 포함된 링크의 평판 및 범주와 다른 스팸 확인 알고리즘을 함께 사용해 스팸을 식별할 수 있습니다. 예를 들어, 메시지의 링크가 마케팅 웹사이트에 속한 경우 해당 메시지는 마케팅 메시지일 가능성이 더 높습니다.

- 회사의 제한적 사용 정책 적용 지원

  URL의 범주(예: 성인 콘텐츠 또는 부정 활동)는 콘텐츠 및 메시지 필터와 함께 회사의 제한적 사용 정책을 적용하는 데 사용될 수 있습니다.

URL 필터링은 작업 큐의 안티스팸, 신종 바이러스, 콘텐츠 및 메시지 필터링 프로세스에 통합됩니다.

평가 대상 URL

수신 및 발송 메시지(첨부 파일 제외)의 URL이 평가됩니다. 다음을 포함하는 문자열을 비롯해 URL의 유효한 문자열이 모두 평가됩니다.

- http, https 또는 www
- 도메인 또는 IP 주소
- 앞에 콜론(:)이 표시된 포트 번호
- 대문자 또는 소문자

메시지가 스팸인지 판단하기 위해 URL을 평가할 때 부하 관리에 필요한 경우 시스템이 발송 메시지보다 수신 메시지의 검사를 우선적으로 수행합니다.

URL 필터링 설정

관련 주제

- URL 필터링 요건, 15-2페이지
- URL 필터링 활성화, 15-2페이지
- Cisco Web Security Services에 대한 연결 정보, 15-3페이지
- 클러스터 구성의 URL 필터링, 15-4페이지
- URL 필터링 허용 목록 생성, 15-4페이지

URL 필터링 요건

URL 필터링을 활성화할 뿐 아니라 원하는 기능에 따라 다른 기능도 활성화해야 합니다.

스팸에 대한 보호를 강화하려면 다음을 수행합니다.

- 안티스팸 검사를 전역적으로 활성화하고 해당 메일 정책을 따라야 합니다. IronPort 안티스팸 또는 Intelligent Multi-Scan 기능일 수 있습니다. 안티스팸 장에 대한을 참조하십시오.

맬웨어에 대한 보호를 강화하려면 다음을 수행합니다.

- 신종 바이러스 필터(Outbreak Filter) 기능을 전역적으로 활성화하고 해당 메일 정책을 따라야 합니다. 신종 바이러스 필터(Outbreak Filter)에 대한을 참조하십시오.

URL 평판에 따라 작업을 수행하거나 메시지 및 콘텐츠 필터를 사용하여 해당 사용 정책을 적용하려면 다음을 수행합니다.

- 신종 바이러스 필터(Outbreak Filter) 기능을 전역적으로 활성화해야 합니다. 신종 바이러스 필터(Outbreak Filter)에 대한을 참조하십시오.

URL 필터링 활성화

시작하기 전에

- 사용할 개별 URL 필터링 기능의 요건이 충족되었는지 확인합니다. URL 필터링 요건, 15-2페이지를 참조하십시오.
- (선택 사항) 모든 URL 필터링 기능이 무시할 URL 목록을 만듭니다. URL 필터링 허용 목록 생성, 15-4페이지를 참조하십시오.

절차

1단계 **Security Services(보안 서비스) > URL Filtering(URL 필터링)**을 선택합니다.

2단계 **Enable(활성화)**을 클릭합니다.

3단계 **Enable URL Category and Reputation Filters(URL 범주 및 평판 필터 활성화)** 확인란을 선택합니다.

4단계 (선택 사항) 메시지가 스팸인지 맬웨어인지 평가할 때 URL 검사를 건너뛰고 모든 콘텐츠 및 메시지 필터링에서 제외할 URL의 목록을 만든 경우 해당 목록을 선택합니다.

이 설정을 적용하면 메시지가 일반적으로 안티스팸 또는 신종 바이러스 필터(Outbreak Filter) 처리를 우회하지 않습니다.

5단계 변경 사항을 제출하고 커밋합니다.

해당 요구 사항을 충족하고 신종 바이러스 필터(Outbreak Filter)와 안티스팸 보호를 이미 구성한 경우 강화된 자동 스팸 및 악성 URL 탐지의 이점을 활용하도록 추가로 구성할 필요가 없습니다.

향후 작업

- 메시지에 포함된 URL의 평판에 따라 작업을 수행하려면 메시지에 포함된 URL의 평판 또는 범주에 따라 작업 수행, 15-7페이지를 참조하십시오.
- 콘텐츠 및 메시지 필터에서 URL 범주를 사용하려면(예: 제한적 사용 정책 적용) 메시지에 포함된 URL의 평판 또는 범주에 따라 작업 수행, 15-7페이지를 참조하십시오.
- 의심스러운 스팸 메시지의 모든 URL을 Cisco Web Security 프록시 서비스로 리디렉션하려면 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예, 13-11페이지를 참조하십시오.
- (선택 사항) 최종 사용자 알림 페이지의 모양을 사용자 지정하려면 최종 사용자 알림 페이지의 모양 사용자 지정, 15-6페이지를 참조하십시오.
- 이 기능과 관련된 문제에 대한 경고를 수신하는지 확인합니다. 향후 URL 범주 집합 변경, 15-21페이지의 AsyncOS 릴리스의 릴리스 노트 및 알림 수신자 추가, 33-35페이지를 참조하십시오.

Cisco Web Security Services에 대한 연결 정보

URL 평판 및 범주는 클라우드 기반 Cisco Web Security Services를 통해 제공됩니다.

Email Security 어플라이언스는 부록 D, "방화벽 정보"의 URL 필터링 서비스에 대해 지정된 포트를 사용하여 직접 또는 웹 프록시를 통해 Cisco Web Security Services에 연결합니다. 상호 인증서 인증을 사용해 HTTPS를 통해 통신이 이루어집니다. 인증서가 자동으로 업데이트됩니다(서비스 업데이트, 33-17페이지 참조). 필요한 인증서에 대한 자세한 내용은 URL 필터링 기능 인증서, 15-4페이지에 지정된 위치에 있는 릴리스 노트를 참조하십시오.

Security Services(보안 서비스) > Service Updates(서비스 업데이트) 페이지에서 HTTP 또는 HTTPS 프록시를 구성한 경우 Email Security 어플라이언스가 Cisco Web Security Services와 통신할 때 이를 사용합니다. 프록시 서버 사용에 대한 자세한 내용은 업그레이드 및 업데이트를 다운로드하도록 서버 설정 구성, 33-21페이지를 참조하십시오.

FIPS 모드에서는 Cisco Web Security Services와의 통신이 FIPS 암호를 사용합니다.

참고 인증서는 구성 파일과 함께 저장되지 않습니다.

관련 주제

- URL 필터링 기능 인증서, 15-4페이지
- 경고: SDS: 등록 인증서를 가져오는 도중 오류 발생, 15-11페이지
- 경고: SDS: 인증서가 올바르지 않음, 15-11페이지

URL 필터링 기능 인증서

AsyncOS는 URL 필터링 기능에 사용되는 클라우드 서비스와의 통신에 필요한 인증서를 자동으로 배포 및 업데이트하도록 설계되었습니다. 그러나 어떠한 이유로 시스템이 이러한 인증서를 업데이트할 수 없는 경우 사용자의 작업이 필요하다는 경고를 수신하게 됩니다.

이러한 경고(시스템 유형, 경고 심각도)를 전송하도록 어플라이언스가 구성되었는지 확인합니다. 지침은 경고, 33-34페이지를 참조하십시오.

잘못된 인증서에 대한 경고를 수신한 경우 Cisco TAC에 문의하면 필요한 교체 인증서를 제공해 드릴 수 있습니다. 교체 인증서 사용 지침은 Cisco Web Security Services와의 통신을 위한 인증서를 수동으로 구성, 15-13페이지를 참조하십시오.

클러스터 구성의 URL 필터링

- 머신, 그룹 또는 클러스터 수준에서 URL 필터링을 활성화할 수 있습니다.
- URL 필터링이 머신 수준에서 활성화된 경우 머신, 그룹 또는 클러스터 수준에서 URL 허용 목록을 구성할 수 있습니다.
- URL 필터링이 그룹 수준에서 활성화된 경우 그룹 또는 클러스터 수준에서 URL 허용 목록을 구성해야 합니다.
- URL 필터링이 클러스터 수준에서 활성화된 경우 클러스터 수준에서 URL 허용 목록을 구성해야 합니다.
- 메시지 및 콘텐츠 필터의 클러스터 표준 규칙이 적용됩니다.

URL 필터링 허용 목록 생성

URL 필터링 기능을 구성할 때 전역 허용 목록을 지정하면 허용 목록의 URL에 대해 평판 또는 범주, 안티스팸, 신종 바이러스 필터(Outbreak Filter)링 또는 콘텐츠 및 메시지 필터링 평가가 수행되지 않습니다. 그러나 이러한 URL이 포함된 메시지는 여느 때처럼 안티스팸 검사 및 신종 바이러스 필터(Outbreak Filter)를 통해 평가됩니다. 콘텐츠 및 메시지 필터의 각 URL 필터링 조건(규칙) 및 작업에서 URL 허용 목록을 지정하여 전역 URL 허용 목록을 보완할 수도 있습니다.

신종 바이러스 필터(Outbreak Filter)링의 URL을 일반적으로 허용하려면 메일 정책: 신종 바이러스 필터(Outbreak Filter) 페이지에서 구성하는 도메인 검사 우회를 사용합니다. URL 필터링의 URL 허용 목록은 이와 유사하지만 도메인 검사 우회와 무관합니다. 해당 기능에 대한 자세한 내용은 URL 재작성 및 도메인 우회, 14-20페이지를 참조하십시오.

이 섹션에 설명된 URL 필터링 허용 목록과 SBRS 점수에 따라 평판 필터링을 전송하는 데 사용되는 허용 목록은 서로 관계가 없습니다.

시작하기 전에

웹 인터페이스에서 URL 목록을 생성하지 않고 URL 목록을 가져오는 것이 좋습니다. URL 목록 가져오기, 15-5페이지를 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > URL Lists(URL 목록)**를 선택합니다.

2단계 **Add URL List(URL 목록 추가)**를 선택하거나 편집할 목록을 클릭합니다.

전역적으로 허용할 모든 URL이 단일 목록에 있어야 합니다. URL 필터링의 전역 허용 목록을 하나만 선택할 수 있습니다.

3단계 URL 목록을 생성하고 제출합니다.

지원되는 URL 형식의 목록을 보려면 **URLs** 상자에 세미콜론(;)을 입력하고 **Submit(제출)**을 클릭합니다. 그런 다음 화면에 표시되는 **more...(기타...)** 링크를 클릭합니다.

각 URL, 도메인 또는 IP 주소를 별도의 행에 표시하거나 쉼표로 구분할 수 있습니다.

4단계 변경 사항을 커밋합니다.

향후 작업

- URL 목록을 전역 허용 목록으로 지정하려면 URL 필터링 활성화, 15-2페이지를 참조하십시오.
- URL 목록을 콘텐츠 또는 메시지 필터의 특정 조건(규칙) 또는 작업의 허용 목록으로 지정하려면 메시지에 포함된 URL의 평판 또는 범주에 따라 작업 수행, 15-7페이지 및 콘텐츠 필터 작업, 11-9페이지를 참조하십시오. 메시지 필터의 경우 URL 범주 규칙, 9-46페이지 및 URL 범주 작업, 9-74페이지도 참조하십시오.

관련 주제

- URL 목록 가져오기, 15-5페이지

URL 목록 가져오기

URL 목록을 가져와 URL 필터링의 허용 목록으로 사용할 수 있습니다.

절차

1단계 가져올 텍스트 파일을 생성합니다.

- 첫 번째 행은 URL 목록의 이름이어야 합니다.
- 각 URL은 별도의 행에 표시해야 합니다.

2단계 파일을 어플라이언스의 `/configuration` 디렉토리에 업로드합니다.

3단계 명령줄 인터페이스에서 `urllistconfig > new` 명령을 사용합니다.

Cisco Web Security 프록시 최종 사용자 알림 페이지

최종 사용자가 신종 바이러스 필터(Outbreak Filter) 또는 정책(콘텐츠 또는 메시지 필터 사용)을 통해 재작성된 악성 URL을 클릭하면 Cisco Web Security 프록시가 최종 사용자를 위한 Cisco 브랜드 알림 페이지를 웹 브라우저에 표시합니다. 이 페이지는 해당 사이트가 악성이므로 액세스가 차단되었음을 알립니다. 이 알림 페이지의 모양을 사용자 지정하고 회사 로고, 연락처 정보 등과 같은 조직의 브랜딩을 표시할 수 있습니다. 최종 사용자 알림 페이지의 모양 사용자 지정, 15-6페이지를 참조하십시오.

최종 사용자가 신종 바이러스 필터(Outbreak Filter)를 사용하여 재작성된 URL을 클릭하면 알림 페이지가 10초 동안 표시된 다음 Cisco Web Security 프록시(Cisco 브랜드)로 리디렉션되어 클릭 시간 평가를 거칩니다.

관련 주제

- URL 리디렉션, 14-5페이지
- 메시지에 포함된 URL의 평판 또는 범주에 따라 작업 수행, 15-7페이지

최종 사용자 알림 페이지의 모양 사용자 지정

Cisco Cloud Web Security 프록시 서비스의 평가를 기준으로 사이트가 악성이면 최종 사용자에게 해당 사이트가 악성이므로 액세스가 차단되었다는 알림이 표시됩니다. 이 알림 페이지의 모양을 사용자 지정하고 회사 로고, 연락처 정보 등과 같은 조직의 브랜딩을 표시할 수 있습니다.

참고 알림 페이지를 사용자 지정하지 않으면 최종 사용자에게 Cisco 브랜드 알림 페이지가 표시됩니다.

시작하기 전에

- Cisco Web Security 프록시 최종 사용자 알림 페이지, 15-5페이지의 특성을 검토합니다.
- URL 필터링을 활성화합니다. URL 필터링 활성화, 15-2페이지를 참조하십시오.

절차

1단계 **Security Services(보안 서비스) > Block Page Customization(블록 페이지 사용자 지정)**을 선택합니다.

2단계 **Enable(활성화)**을 클릭합니다.

3단계 **Enable Block Page customization(블록 페이지 사용자 지정 활성화)** 확인란을 선택하고 다음과 같은 세부사항을 입력합니다.

- 조직의 로고 URL. 공개적으로 액세스할 수 있는 서버에서 로고 이미지를 호스팅하는 것이 좋습니다.
- 조직의 이름
- 조직의 연락처 정보

4단계 알림에 사용할 언어를 선택합니다. 웹 인터페이스에서 지원하는 언어 중 하나를 선택할 수 있습니다.

참고 최종 사용자의 브라우저 기본 언어가 여기에서 사용자가 선택한 언어보다 우선합니다. 또한 최종 사용자의 브라우저 기본 언어가 AsyncOS에서 지원되지 않으면 여기에서 선택한 언어로 알림이 표시됩니다.

5단계 (선택 사항) **Preview Block Page Customization(블록 페이지 사용자 지정 미리보기)** 링크를 클릭하여 알림 페이지를 미리 봅니다.

6단계 변경 사항을 제출하고 커밋합니다.

다음 단계

다음 방법 중 하나를 사용하여 URL 재작성을 설정합니다.

- 신종 바이러스 필터(Outbreak Filter) 사용. URL 리디렉션, 14-5페이지를 참조하십시오.
- 콘텐츠 또는 메시지 필터 사용. 메시지에 포함된 URL의 평판 또는 범주에 따라 작업 수행, 15-7페이지를 참조하십시오.

메시지에 포함된 URL의 평판 또는 범주에 따라 작업 수행

수신 및 발송 메일 정책에서 메시지 필터 및 콘텐츠 필터를 사용하여 메시지에 포함된 URL 링크의 평판 또는 범주에 따라 작업을 수행할 수 있습니다.

신종 바이러스 필터(Outbreak Filter)는 메시지가 맬웨어인지 평가할 때 여러 가지 요소를 고려하며 URL 평판을 통해서만 공격적인 메시지 처리가 트리거되는 것은 아니므로 URL 평판에 따라 필터를 생성할 수 있습니다.

예를 들어, URL 평판 필터를 사용하여 다음을 수행할 수 있습니다.

- Cisco Cloud Web Security 프록시로 리디렉션되어 클릭 시간 평가를 거치도록 의심스럽거나 알 수 없는 평판의 URL을 재작성합니다.
- 평판 점수가 악성 범위에 해당하는 URL이 포함된 메시지를 삭제합니다.

URL 범주 필터를 사용하여 다음을 수행할 수 있습니다.

- 예를 들어, 사용자가 사무실에서 성인 또는 도박 사이트를 방문하는 것을 방지하기 위해 URL의 필터 범주를 사용하여 조직의 제한적 사용 정책을 적용할 수 있습니다.
- 분류되기 전에 사라질 수 있는 악성 사이트에 대한 강화된 보호를 제공합니다. 사용자가 링크를 클릭하면 Cisco Cloud Web Security 프록시 서비스로 리디렉션되어 평가를 거치도록 미분류 범주의 모든 URL을 리디렉션합니다.

관련 주제

- URL 관련 조건(규칙) 및 작업 사용, 15-7페이지
- URL 평판 또는 URL 범주를 통한 필터링: 조건 및 규칙, 15-8페이지
- 필터에서 URL 평판 및 URL 범주 작업을 사용하여 메시지의 URL 수정, 15-8페이지
- 리디렉션된 URL: 최종 사용자의 경험, 15-10페이지

URL 관련 조건(규칙) 및 작업 사용

변경 후	예	수행할 작업
메시지 전체에 대해 작업을 수행합니다.	메시지를 삭제하거나 격리합니다.	URL 평판 또는 URL 범주 조건 또는 규칙을 생성한 다음 URL 평판 또는 URL 범주 작업을 제외한 작업과 페어링합니다. 예외: URL 평판 조건 또는 규칙을 바운스 작업과 페어링하지 마십시오.
메시지의 URL을 수정하거나 해당 동작을 수정합니다.	메시지의 URL을 텍스트 메모로 바꾸거나 URL을 클릭할 수 없게 만듭니다.	URL 평판 또는 URL 범주 작업만 생성합니다. 별도의 URL 필터링 조건을 사용하지 마십시오.

늘 그렇듯이 콘텐츠 필터를 사용하려면 메일 정책에서 콘텐츠 필터를 지정해야 합니다.

URL 평판 또는 URL 범주를 통한 필터링: 조건 및 규칙

메시지에 포함된 URL의 평판 또는 범주에 따라 메시지에 대해 작업을 수행할 수 있습니다. URL 또는 해당 동작 수정 이외의 작업을 수행하려면 **URL 평판** 또는 **URL 범주** 조건을 추가하고 작업을 적용할 평판 점수 또는 URL 범주를 선택합니다.

예를 들어, 성인 범주의 URL이 포함된 모든 메시지에 **Drop (Final Action)(삭제(최종 작업))** 작업을 적용하려면 **Adult(성인)** 범주를 선택한 상태에서 **URL Category(URL 범주)** 유형의 조건을 추가합니다.

범주를 지정하지 않으면 선택한 작업이 모든 메시지에 적용됩니다.

클린, 의심 및 악성 URL의 URL 평판 점수 범위는 미리 정의되어 있으며 편집할 수 없습니다. 그러나 대신 사용자 지정 범위를 지정할 수 있습니다. 지정된 엔드포인트는 사용자가 지정하는 범위에 포함됩니다. 예를 들어, -8에서 -10까지의 사용자 지정 범위를 생성하면 -8과 -10이 해당 범위에 포함됩니다. 평판 점수를 결정할 수 없는 URL에는 "점수 없음"을 사용합니다.

선택한 URL 허용 목록 또는 전역 URL 허용 목록에 포함된 URL은 평가되지 않습니다.

이 조건과 페어링한 작업은 메시지의 URL이 평판 점수 또는 조건에 지정된 범주와 일치할 경우에 수행됩니다.

메시지의 URL을 수정하거나 해당 동작을 수정하려면 URL 평판 또는 URL 범주 작업만 구성합니다. 이를 위해 별도의 URL 평판 또는 URL 범주 조건 또는 규칙이 필요하지 않습니다.

참고 URL 평판 조건을 바운스 작업과 페어링하지 마십시오.

정보 특정 URL의 범주를 확인하려면 범주 미지정 및 미분류 URL 보고, 15-21페이지의 링크를 방문하십시오.

관련 주제

- 11 장, "콘텐츠 필터"
- URL 평판 규칙, 9-45페이지
- URL 범주 규칙, 9-46페이지
- URL 필터링 허용 목록 생성, 15-4페이지

필터에서 URL 평판 및 URL 범주 작업을 사용하여 메시지의 URL 수정

URL 평판 또는 URL 범주 작업을 사용하여 URL의 평판 또는 범주에 따라 메시지의 URL 또는 해당 동작을 수정할 수 있습니다.

URL 평판 및 URL 범주 작업은 별도의 조건이 필요하지 않습니다. 그 대신, 선택한 작업이 사용자가 URL 평판 또는 URL 범주 작업에서 선택하는 URL 평판 또는 범주에 따라 적용됩니다.

이 작업은 작업에 지정된 기준을 충족하는 URL에만 적용됩니다. 메시지의 다른 URL은 수정되지 않습니다.

범주를 지정하지 않으면 선택한 작업이 모든 메시지에 적용됩니다.

클린, 의심 및 악성 URL의 URL 평판 점수 범위는 미리 정의되어 있으며 편집할 수 없습니다. 그러나 대신 사용자 지정 범위를 지정할 수 있습니다. 지정된 엔드포인트는 사용자가 지정하는 범위에 포함됩니다. 예를 들어, -8에서 -10까지의 사용자 지정 범위를 생성하면 -8과 -10이 해당 범위에 포함됩니다. 평판 점수를 결정할 수 없는 URL에는 "점수 없음"을 사용합니다.

다음과 같은 URL 관련 작업을 사용할 수 있습니다.

- URL을 클릭할 수 없게 만들어 무해화합니다. 메시지 수신자는 여전히 URL을 보고 복사할 수 있습니다.
- 메시지 수신자가 링크를 클릭하면 트랜잭션이 클라우드의 Cisco Web Security 프록시로 라우팅되어 사이트가 악성인 경우 액세스가 차단되도록 URL을 리디렉션합니다.

  예: 피싱 공격에 사용되는 악성 사이트는 종종 분류되기 전에 사라지므로 **범주 미지정** 범주의 모든 URL을 Cisco Cloud Web Security 프록시 서비스로 리디렉션할 수 있습니다.

  리디렉션된 URL: 최종 사용자의 경험, 15-10페이지도 참조하십시오.

  URL을 다른 프록시로 리디렉션하려면 다음 글머리 기호 목록의 예제를 참조하십시오.

  참고 Cisco Cloud Web Security 프록시 서비스에는 이 릴리스에서 구성 가능한 옵션이 없습니다. 예를 들어, 위협 점수에 따라 조정할 위협 점수 임계값이나 지정할 작업이 없습니다.

- URL을 텍스트로 바꿉니다.

  메시지에 표시되는 텍스트에 원래 URL을 포함하려면 `$URL` 변수를 사용합니다.

  예:

  - **불법 다운로드** 범주의 모든 URL을 메모로 바꿉니다.

    ```
    Message from your system administrator: A link to an illegal downloads web site has been removed from this message.
    ```

  - 경고와 함께 원래 URL을 포함합니다.

    ```
    경고! The following URL may contain malware: $URL
    ```

    이는 WARNING:이 됩니다. 다음 URL에 맬웨어가 포함될 수 있습니다. http://example.com.

  - 사용자 지정 프록시 또는 웹 보안 서비스로 리디렉션합니다.

    ```
    http://custom_proxy/$URL
    ```

    이는 http://custom_proxy/http://example.com이 됩니다.

선택한 URL 허용 목록 또는 전역 URL 허용 목록에 포함된 URL의 평판 및 범주는 평가되지 않습니다.

URL을 무해화하거나 바꿀 경우 서명된 메시지의 URL을 무시하도록 선택할 수 있습니다.

URL 평판 또는 URL 범주 작업과 URL 평판 또는 URL 범주 조건(규칙)을 페어링하는 것은 권장되지 않습니다. 조건(규칙)과 서로 다른 범주가 포함된 작업을 페어링할 경우 일치가 발생하지 않습니다.

정보 특정 URL의 범주를 확인하려면 범주 미지정 및 미분류 URL 보고, 15-21페이지의 링크를 방문하십시오.

관련 주제

- 사용자 지정 헤더를 사용하여 의심스러운 스팸의 URL을 Cisco Web Security 프록시로 리디렉션: 구성 예, 13-11페이지

- 11 장, "콘텐츠 필터"
- URL 평판 작업, 9-72페이지
- URL 범주 작업, 9-74페이지
- URL 필터링 허용 목록 생성, 15-4페이지

리디렉션된 URL: 최종 사용자의 경험

Cisco Cloud Web Security 프록시 서비스의 평가에 따라 다음과 같은 작업이 수행됩니다.

- 사이트가 안전하면 사용자가 대상 웹 사이트로 리디렉션되며 링크가 리디렉션되었다는 것을 알지 못합니다.
- 사이트가 악성이면 사용자에게 해당 사이트가 악성이므로 액세스가 차단되었다는 알림이 표시됩니다.

  최종 사용자 알림 페이지의 모양을 사용자 지정하고 회사 로고, 연락처 정보 등과 같은 조직의 브랜딩을 표시할 수 있습니다. 최종 사용자 알림 페이지의 모양 사용자 지정, 15-6페이지를 참조하십시오.
- Cisco Cloud Web Security 프록시 서비스와의 통신 시간이 초과되면 사용자가 대상 웹 사이트에 액세스할 수 있습니다.
- 다른 오류가 발생할 경우 사용자에게 알림이 표시됩니다.

URL 필터링 경과 모니터링

탐지된 악성 및 의심스러운 URL에 대한 데이터를 보려면 Monitor(모니터) > URL Filtering(URL 필터링)을 선택합니다. 이 페이지의 데이터에 대한 자세한 내용은 URL 필터링 페이지, 28-21페이지를 참조하십시오.

URL 필터링 문제 해결

관련 주제

- 로그 보기, 15-11페이지
- 경고: SDS: 등록 인증서를 가져오는 도중 오류 발생, 15-11페이지
- 경고: SDS: 인증서가 올바르지 않음, 15-11페이지
- Cisco Web Security Services에 연결할 수 없음, 15-11페이지
- websecurityadvancedconfig 명령 사용, 15-12페이지
- 메시지 추적 검색을 통해 지정된 범주의 메시지를 찾을 수 없음, 15-12페이지
- 악성 URL 및 마케팅 메시지가 안티스팸 또는 신종 바이러스 필터(Outbreak Filter)에 포착되지 않음, 15-12페이지
- 필터링된 범주의 URL이 올바르게 처리되지 않음, 15-12페이지
- 최종 사용자가 재작성된 URL을 통해 악성 사이트에 도달함, 15-13페이지
- Cisco Web Security Services와의 통신을 위한 인증서를 수동으로 구성, 15-13페이지

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 시도할 때 발생한 오류, 시간 초과, 네트워크 문제 등과 관련된 정보가 이 로그에 게시됩니다.

대부분의 정보는 정보 또는 디버그 수준의 정보입니다.

로그에는 사용자가 메시지의 리디렉션된 링크를 클릭할 때 발생하는 결과에 대한 정보가 포함되지 않습니다.

로그의 "SDS"는 URL 평판 서비스를 나타냅니다.

경고: SDS: 등록 인증서를 가져오는 도중 오류 발생

문제 등록 클라이언트 인증서를 가져오는 도중 발생한 오류에 대한 정보 수준 경고를 받습니다.

솔루션 URL 평판 및 범주를 얻으려면 이 인증서를 클라우드의 Cisco Web Security Services에 연결해야 합니다. 다음을 시도하십시오.

- 잘못된 프록시 설정 또는 방화벽 문제와 같은 네트워크 문제가 있는지 확인합니다.
- URL 필터링 기능 키가 유효하고 활성화되었는지 확인합니다.
- 문제가 계속되면 Cisco TAC에 문의하십시오.

경고: SDS: 인증서가 올바르지 않음

문제 잘못된 SDS 인증서에 대한 위험 경고를 받습니다.

솔루션 URL 평판 및 범주를 얻으려면 이 인증서를 클라우드의 Cisco Web Security Services에 연결해야 합니다.

인증서를 가져와서 수동으로 설치하려면 Cisco Web Security Services와의 통신을 위한 인증서를 수동으로 구성, 15-13페이지를 참조하십시오.

Cisco Web Security Services에 연결할 수 없음

문제 **Security Services(보안 서비스) > URL Filtering(URL 필터링)** 페이지에 Cisco Web Security Services 연결 문제가 계속해서 표시됩니다.

솔루션

- URL 필터링을 활성화했으나 변경 사항을 아직 커밋하지 않은 경우 변경 사항을 커밋하십시오.
- Cisco Web Security Services와의 연결과 관련한 최근 경고가 있는지 확인하십시오. 최근 경고 보기, 33-37페이지를 참조하십시오. 해당하는 경우 경고: SDS: 등록 인증서를 가져오는 도중 오류 발생, 15-11페이지 및 경고: SDS: 인증서가 올바르지 않음, 15-11페이지를 참조하십시오.
- Security Services(보안 서비스) > Service Updates(서비스 업데이트)에 지정된 프록시를 통해 연결할 경우 올바르게 구성 및 작동되는지 확인하십시오.
- 연결을 방해할 수 있는 다른 네트워크 문제가 있는지 확인하십시오.

- URL 필터링 로그에 SDS 클라이언트에 대한 요청 시간 초과와 관련된 오류가 표시될 경우 명령줄 인터페이스에서 `websecuritydiagnostics` 명령과 `websecurityadvancedconfig` 명령을 사용하여 다음을 조사하고 변경하십시오.
  - 진단에 응답 시간 또는 DNS 조회 시간이 구성된 URL 조회 시간 초과보다 짧다고 표시될 경우 그에 따라 URL 조회 시간 초과 값을 늘리십시오.
  - 진단에 캐시 크기가 고급 구성 설정에 지정된 용량과 같거나 비슷하다고 표시될 경우 캐시 크기를 늘리십시오.
- URL 필터링 로그에 URL 스캐너, Cisco Web Security Services 또는 SDS와의 통신 시 발생한 비시간 초과 오류가 있는지 확인하십시오. 로그의 "SDS"는 Cisco Web Security Services를 나타냅니다. 그러한 로그 메시지가 표시될 경우 TAC에 문의하십시오.

websecurityadvancedconfig 명령 사용

이 문서에 명시적으로 설명된 변경 사항을 제외하고 TAC의 지침 없이 `websecurityadvancedconfig` 명령을 사용하여 다른 변경을 수행하지 마십시오.

메시지 추적 검색을 통해 지정된 범주의 메시지를 찾을 수 없음

문제 특정 범주의 URL이 포함된 메시지가 해당 범주를 기준으로 검색할 경우 발견되지 않습니다.

솔루션 예상 메시지가 검색 결과에서 누락되었음, 29-7페이지를 참조하십시오.

악성 URL 및 마케팅 메시지가 안티스팸 또는 신종 바이러스 필터(Outbreak Filter)에 포착되지 않음

문제 악성 URL과 마케팅 링크가 포함된 메시지가 안티스팸 또는 신종 바이러스 필터(Outbreak Filter)에 포착되지 않습니다.

솔루션

- 이러한 현상은 웹사이트 평판 및 범주가 안티스팸 및 신종 바이러스 필터(Outbreak Filter)를 사용해 감염을 결정하는 여러 기준 중 2개에 불과하기 때문에 발생할 수 있습니다. URL 재작성 또는 URL을 텍스트로 대체, 메시지 격리 또는 삭제와 같은 작업을 수행하는 데 필요한 임계값을 낮춰 이러한 필터의 감도를 높일 수 있습니다. 자세한 내용은 신종 바이러스 필터(Outbreak Filter) 기능 및 메일 정책, 14-16페이지 및 안티스팸 정책 정의, 13-7페이지를 참조하십시오. 또는 URL 평판 점수를 기준으로 콘텐츠 또는 메시지 필터를 생성하십시오.
- 이러한 현상은 Email Security 어플라이언스가 Cisco Web Security Services에 연결할 수 없는 경우에도 발생할 수 있습니다. Cisco Web Security Services에 연결할 수 없음, 15-11페이지를 참조하십시오.

필터링된 범주의 URL이 올바르게 처리되지 않음

문제 URL 범주에 따라 콘텐츠 또는 메시지 필터에 정의된 작업이 적용되지 않습니다.

솔루션

- 추적 기능(문제 해결 장에 설명된)을 사용하여 메시지 처리 경로를 따르십시오.

- 이러한 현상은 Email Security 어플라이언스가 Cisco Web Security Services에 연결할 수 없는 경우에 발생할 수 있습니다. Cisco Web Security Services에 연결할 수 없음, 15-11페이지를 참조하십시오.
- 연결 문제가 없으면 URL의 범주가 아직 지정되지 않았거나 잘못 지정되었을 수 있습니다. 범주 미지정 및 미분류 URL 보고, 15-21페이지를 참조하십시오. 이 사이트를 사용하여 URL의 범주를 결정할 수 있습니다.

최종 사용자가 재작성된 URL을 통해 악성 사이트에 도달함

문제 악성 URL이 Cisco Web Security 프록시로 리디렉션되었으나 최종 사용자가 해당 사이트에 액세스할 수 없었습니다.

솔루션 이러한 현상은 다음과 같은 경우에 발생할 수 있습니다.

- 사이트가 아직 악성 사이트로 확인되지 않았습니다.
- Cisco Web Security Proxy에 대한 연결 시간 초과가 자주 발생해서는 안 됩니다. 네트워크 문제가 연결을 방해하지 않는지 확인하십시오.

Cisco Web Security Services와의 통신을 위한 인증서를 수동으로 구성

어플라이언스가 Cisco Web Security Services와의 통신에 사용할 인증서를 자동으로 가져오지 못할 경우 이 절차를 사용하십시오.

절차

1단계 필요한 인증서를 가져옵니다.

2단계 **Network(네트워크) > Certificates(인증서)**를 사용하거나 명령줄 인터페이스에서 `certconfig` 명령을 사용하여 인증서를 업로드합니다.

3단계 명령줄 인터페이스에 `websecurityconfig` 명령을 입력합니다.

4단계 프롬프트를 따라 Cisco Web Security Services 인증에 사용할 클라이언트 인증서를 설치합니다.

5단계 인증서 설치 프로세스를 완료한 후 `webcacheflush` 명령을 입력합니다.

URL 범주 정보

관련 주제

- URL 범주 설명, 15-14페이지
- URL 범주 결정, 15-21페이지
- 범주 미지정 및 미분류 URL 보고, 15-21페이지
- 향후 URL 범주 집합 변경, 15-21페이지

URL 범주 설명

이러한 URL 범주는 AsyncOS for Web Security 어플라이언스의 최근 릴리스에 사용된 범주와 동일합니다.

표 15-1

URL 범주	약어	코드	설명	URL 예
성인	adlt	1006	성인 콘텐츠를 나타내지만 음란물만을 의미하는 것은 아닙니다. 성인 클럽(스트립 클럽, 스윙어 클럽, 에스코트 서비스, 스트리퍼), 성행위, 특성상 비 음란물, 성기 피어싱, 성인 용품 또는 인사장에 대한 일반 정보, 건강 또는 질병과 관련되지 않은 성행위에 대한 정보가 포함될 수 있습니다.	www.adultentertainmentexpo.com www.adultnetline.com
광고	adv	1027	종종 웹 페이지에 포함되는 배너 및 팝업 광고, 광고 콘텐츠를 제공하는 기타 광고 웹사이트가 해당됩니다. 광고 서비스 및 영업은 "비즈니스 및 산업"으로 분류됩니다.	www.adforce.com www.doubleclick.com
주류	alc	1077	즐겁게 마시는 주류, 맥주 및 와인 제조, 칵테일 제조법, 주류 판매업체, 와이너리, 포도원, 맥주 공장, 주류 유통회사가 해당됩니다. 알코올 중독은 "건강 및 영양"으로 분류됩니다. 바와 레스토랑은 "식당 및 주점"으로 분류됩니다.	www.samueladams.com www.whisky.com
예술	art	1002	갤러리 및 전시회, 예술가 및 예술품, 사진, 문학 및 도서, 공연 예술 및 극장, 뮤지컬, 발레, 박물관, 설계, 건축학이 해당됩니다. 영화 및 TV는 "엔터테인먼트"로 분류됩니다.	www.moma.org www.nga.gov
점성술	astr	1074	점성술. 별점, 점, 숫자점, 심령 상담, 타로가 해당됩니다.	www.astro.com www.astrology.com
경매	auct	1088	온라인 및 오프라인 경매, 경매장 및 항목별 광고가 해당됩니다.	www.craigslist.com www.ebay.com
비즈니스 및 산업	busi	1019	마케팅, 상업, 기업, 비즈니스 관행, 인적 자원, 인사부, 운송, 급여, 보안 및 벤처 자본, 사무용품, 산업 장비(프로세스 장비), 기계 및 기계 시스템, 난방 장비, 냉방 장비, 자재 취급 장비, 포장 장비, 제조, 고체 처리, 금속 가공, 건설 및 건물, 승객 수송, 상업, 산업 디자인, 건설, 건물 자재, 선적 및 화물 운송(화물 운송 서비스, 트럭 수송, 화물 운송업자, 트럭 화물 운송업자, 화물 및 운송 주선인, 급행 서비스, 적재량 및 화물 매칭, 추적 및 조회, 철도 운송, 해상 운송, 복합 물류 시스템, 운반 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

표 15-1

URL 범주	약어	코드	설명	URL 예
부정행위 및 표절	plag	1051	표절을 목적으로 부정행위 및 학기말 리포트와 같은 필기 자료 판매를 조장하는 행위가 해당됩니다.	www.bestessays.com www.superiorpapers.com
아동 학대 콘텐츠	cprn	1064	전 세계의 불법적인 아동 성 학대 콘텐츠가 해당됩니다.	—
컴퓨터 보안	csec	1065	기업 및 가정 사용자를 위한 보안 제품 및 서비스 제공이 해당됩니다.	www.computersecurity.com www.symantec.com
컴퓨터 및 인터넷	comp	1003	하드웨어, 소프트웨어, 소프트웨어와 같은 컴퓨터 및 소프트웨어에 대한 정보, 소프트웨어 엔지니어, 프로그래밍 및 네트워킹, 웹 사이트 설계, 일반적인 웹 및 인터넷, 컴퓨터 공학, 컴퓨터 그래픽 및 클립아트에 대한 정보가 해당됩니다. "프리웨어 및 셰어웨어"는 별도의 범주로 분류됩니다.	www.xml.com www.w3.org
결혼정보업체	date	1055	결혼정보업체, 온라인 데이트 서비스, 결혼상담소가 해당됩니다.	www.eharmony.com www.match.com
디지털 엽서	card	1082	디지털 엽서 및 e-카드를 보낼 수 있습니다.	www.all-yours.net www.delivr.net
식당 및 주점	food	1061	음식점, 레스토랑, 바, 간이 식당, 퍼브, 레스토랑 가이드 및 후기가 해당됩니다.	www.hideawaybrewpub.com www.restaurantrow.com
동적 및 가정용	dyn	1091	일반적으로 사용자가 홈 네트워크에 액세스하려는 시도를 나타내는 광대역 링크의 IP 주소가 해당됩니다(예: 가정용 컴퓨터에 대한 원격 세션).	http://109.60.192.55 http://dynalink.co.jp http://ipadsl.net
교육	edu	1001	학교, 전문대학, 대학교, 교재, 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 세부정보 또는 토론, 음악 및 밴드, TV, 유명인 및 팬 웹사이트, 엔터테인먼트 뉴스, 유명인 가십, 유흥을 즐길 수 있는 장소 등이 해당됩니다. "예술" 범주와 비교해 보십시오.	www.eonline.com www.ew.com
극단	extr	1075	성폭력 또는 범죄성 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
패션	fash	1076	의류 및 패션, 미용실, 화장품, 액세서리, 보석, 향수, 신체 개조와 관련된 사진 및 텍스트, 문신 및 피어싱, 모델 대행사가 해당됩니다. 피부과 제품은 "건강 및 영양"으로 분류됩니다.	www.fashion.net www.findabeautysalon.com

표 15-1

URL 범주	약어	코드	설명	URL 예
파일 전송 서비스	fts	1071	다운로드 서비스 및 호스팅된 파일 공유 제공을 주된 목적으로 하는 파일 전송 서비스입니다.	www.rapidshare.com www.yousendit.com
필터 회피	filt	1025	탐지 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, 은행업, 보험, 투자, 국가 경제, 모든 유형의 보험, 신용카드, 은퇴 및 자산 설계, 대출, 담보 대출을 포함한 개인 금융 등 주로 금융의 특성을 지닌 요소가 해당됩니다. 증권 및 주식은 "온라인 거래"로 분류됩니다.	finance.yahoo.com www.bankofamerica.com
프리웨어 및 쉐어웨어	free	1068	무료 및 쉐어웨어 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 발행 복권은 "복권"으로 분류됩니다.	www.888.com www.gambling.com
게임	game	1007	다양한 카드 게임, 보드 게임, 어휘 게임, 비디오 게임, 전투 게임, 스포츠 게임, 다운로드 가능한 게임, 게임 리뷰, 커닝 페이퍼, 컴퓨터 게임 및 인터넷 게임(예: 롤플레잉 게임)이 해당됩니다.	www.games.com www.shockwave.com
정부 및 법률	gov	1011	정부 웹사이트, 외교 관계, 정부 및 선거에 대한 뉴스와 정보, 변호사, 법률 회사, 법률 출판물, 법적 참조 자료, 법원, 소송사건표 및 법률 협회와 같은 법률 분야에 대한 정보, 입법 및 법원 판결, 시민권 문제, 이민, 특허 및 저작권, 법 집행 및 교정 시스템에 대한 정보, 범죄 보도, 법 집행, 범죄 통계, 군대, 군기지, 군대 제도와 같은 군사, 테러 방지가 해당됩니다.	www.usa.gov www.law.com
해킹	hack	1050	웹사이트, 소프트웨어 및 컴퓨터의 보안을 우회하는 방법을 논의합니다.	www.hackthissite.org www.gohacking.com
혐오 발언	hate	1016	사회 집단, 피부색, 종교, 성적 성향, 장애, 계층, 인종, 국적, 나이, 성별, 성 정체성을 근거로 한 증오, 편협성 또는 차별을 조장하는 웹사이트, 인종 차별, 성차별, 인종 차별 신학, 증오 음악, 신나치주의 단체, 인종 지상주의, 홀로코스트 부정을 조장하는 사이트가 해당됩니다.	www.kkk.com www.nazi.org

표 15-1

URL 범주	약어	코드	설명	URL 예
건강 및 영양	hlth	1009	의료 서비스, 질병 및 장애, 의료, 병원, 의사, 의약품, 정신 건강, 정신 의학, 약리학, 운동 및 신체 단련, 지체장애, 비타민 및 건강 보조제, 건강과 관련된 성행위(질병 및 건강 관리), 흡연, 음주, 약물 사용, 건강과 관련된 도박(질병 및 건강 관리), 일반 식품, 식품 및 음료, 요리 및 조리법, 식품 및 영양, 건강, 식이요법, 조리법 및 요리 웹사이트를 포함한 요리가 해당됩니다.	www.health.com www.webmd.com
유머	lol	1079	농담, 스케치, 만화 및 기타 해학적인 콘텐츠입니다. 모독과 같은 성인 유머는 "성인"으로 분류됩니다.	www.humor.com www.jokes.com
부정 행위	ilac	1022	절도, 사기, 전화 네트워크 불법 액세스와 같은 범죄, 컴퓨터 바이러스, 테러, 폭탄, 무정부 상태, 살인 및 자살을 묘사하고 실행 방법을 설명하는 웹사이트가 해당됩니다.	www.ekran.no www.thedisease.net
불법 다운로드	ildl	1084	소프트웨어 또는 기타 자료, 일련 번호, 키 생성기를 다운로드할 수 있는 기능과 저작권 계약 위반과 관련해서 소프트웨어 보호를 우회하는 툴을 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
인프라 및 콘텐츠 전달 네트워크	infr	1018	콘텐츠 전달 인프라 및 동적으로 생성된 콘텐츠, 보안이 되어 있어 더 구체적으로 분류할 수 없거나 분류하기 어려운 웹사이트가 해당됩니다.	www.akamai.net www.webstat.net
인터넷 전화 통신	voip	1067	인터넷을 사용하는 기술 서비스입니다.	www.evaphone.com www.skype.com
구직	job	1004	직업 관련 자문, 이력서 작성 및 면접 기술, 직업 소개소, 일자리 데이터뱅크, 정규직 및 임시직 직업 소개소, 고용주 웹사이트가 해당됩니다.	www.careerbuilder.com www.monster.com
여성용 속옷 및 수영복	ling	1031	특히 모델용 실내복 및 수영복입니다.	www.swimsuits.com www.victoriassecret.com
복권	lotr	1034	로또, 경연 및 정부에서 후원하는 복권입니다.	www.calottery.com www.flalottery.com
휴대폰	cell	1070	SMS(단문 메시지 서비스), 벨소리 및 휴대폰 다운로드가 해당됩니다. 이동통신 사업자 웹사이트는 "비즈니스 및 산업" 범주에 포함됩니다.	www.cbfsms.com www.zedge.net

표 15-1

URL 범주	약어	코드	설명	URL 예
자연	natr	1013	천연 자원. 생태학 및 보존, 산림, 황무지, 식물, 꽃, 산림 보전, 산림, 황무지 및 임업 관행, 삼림 관리(재조림, 산림 보호, 보전, 수확, 간벌, 불넣기), 농업 경영(농업, 원예, 원예학, 조경, 식재, 잡초 방제, 관개, 가지치기, 수확), 오염 문제(공기 질, 유해 폐기물, 오염 방지, 재활용, 폐기물 관리, 수질, 환경 정화 산업), 동물, 애완동물, 가축, 동물학. 생물학, 식물학이 해당됩니다.	www.enature.com www.nature.org
뉴스	news	1058	뉴스, 헤드라인, 신문, TV 방송국, 잡지, 날씨, 기상 상태에 대한 콘텐츠입니다.	www.cnn.com news.bbc.co.uk
비 정부 단체	ngo	1087	클럽, 로비, 커뮤니티, 비영리 단체 및 노동 조합과 같은 비 정부 단체입니다.	www.panda.org www.unions.org
비 성적인 노출	nsn	1060	나체주의 및 나체, 자연주의, 나체주의자 캠프, 예술적 누드가 해당됩니다.	www.artenuda.com www.naturistsociety.com
온라인 커뮤니티	comm	1024	동호회, 특별 이익 집단, 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 및 호스팅에 사용되는 오프사이트 및 P2P 스토리지입니다.	www.adrive.com www.dropbox.com
온라인 거래	trad	1028	온라인 중개, 사용자가 온라인 주식 거래를 할 수 있는 웹사이트와 주식 시장, 주식, 채권, 뮤추얼 펀드, 중개업자, 주식 분석 및 해석, 주식 선별, 주식 차트, IPO, 주식 분할과 관련된 정보를 다루는 웹사이트입니다. 증권 및 주식에 대한 스프레드 베팅 서비스는 "도박"으로 분류됩니다. 기타 금융 서비스는 "금융"으로 분류됩니다.	www.tdameritrade.com www.scottrade.com
회사 이메일	pem	1085	비즈니스 이메일에 액세스하는 데 사용되는 웹사이트입니다(종종 Outlook Web Access를 통해 액세스).	—
지정 보류된 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. 여기에는 유료 광고 링크를 반환하는 위조 검색 웹사이트도 포함됩니다.	www.domainzaar.com www.parked.com
피어 파일 전송	p2p	1056	P2P 파일 요청 웹사이트입니다. 이러한 사이트에서는 파일 전송을 자체적으로 추적하지 않습니다.	www.bittorrent.com www.limewire.com
개인 사이트	pers	1081	개인이 운영하거나 개인에 대한 웹사이트, 개인 홈 페이지 서버, 개인 콘텐츠가 포함된 웹사이트, 특정한 주제가 없는 개인 블로그가 해당됩니다.	www.karymullis.com www.stallman.org

표 15-1

URL 범주	약어	코드	설명	URL 예
사진 검색 및 이미지	img	1090	이미지, 사진, 클립아트를 쉽게 검색하고 저장할 수 있는 웹사이트입니다.	www.flickr.com www.photobucket.com
정치	pol	1083	정치인, 정당, 정치, 선거, 민주주의, 투표에 대한 정보를 다루는 웹사이트입니다.	www.politics.com www.thisnation.com
음란물	porn	1054	노골적인 성적 표현 또는 묘사가 수반됩니다. 노골적인 일본 애니메이션 및 만화, 기타 페티시 자료, 노골적인 채팅방, 성행위 시뮬레이터, 스트립 포커, 성인 영화, 외설적인 예술, 노골적인 웹 기반 이메일이 포함됩니다.	www.redtube.com www.youporn.com
전문 네트워킹	pnet	1089	경력 또는 전문성 개발을 목적으로 하는 소셜 네트워킹입니다. "소셜 네트워킹 "도 참조하십시오.	www.linkedin.com www.europeanpwn.net
부동산	rest	1045	부동산, 사무실 및 상업용 공간, 부동산 목록(예: 임대 시설, 아파트, 주택, 가옥) 검색을 지원하는 정보입니다.	www.realtor.com www.zillow.com
참조	ref	1017	시/도 가이드, 지도, 역사, 참조자료 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
아동 안전	kids	1057	어린이에게 특별히 액세스가 허용되는 어린이를 대상으로 하는 사이트입니다.	kids.discovery.com www.nickjr.com
과학 및 기술	sci	1012	항공 전자 장치, 엔지니어링, 수학 및 기타 유사 한 주제와 같은 과학 및 기술, 우주 탐험, 기상학. 지리, 환경, 에너지(화석, 핵, 재생), 통신(전화, 전기 통신)이 해당됩니다.	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, 성건강, 피임, 임신에 대해 다루는 사실 기반 웹사이트입니다.	www.avert.org www.scarleteen.com
쇼핑	shop	1005	물물 교환, 온라인 구매, 쿠폰 및 무료 혜택, 일반 사무 용품, 온라인 카탈로그, 온라인 메일이 해당됩니다.	www.amazon.com www.shopping.com
소셜 네트워킹	snet	1069	소셜 네트워킹 사이트입니다. "전문 네트워킹" 도 참조하십시오.	www.facebook.com www.twitter.com
사회 공학	socs	1014	사회와 관련된 과학 및 사학, 고고학, 인류학, 문화 연구, 역사, 언어학, 지리학, 철학, 심리학, 여성학을 다루는 웹사이트입니다.	www.archaeology.org www.anthropology.net

표 15-1

URL 범주	약어	코드	설명	URL 예
사회 및 문화	scty	2010년	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, 전문가 및 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
운송	trns	1044	개인 운송 수단, 자동차 및 오토바이에 대한 정보, 신형 및 중고 자동차/오토바이 구매, 자동차 동호회, 보트/항공기/RV(레크리에이션용 차량) 및 기타 유사 제품이 해당됩니다. 참고: 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 운송, 항공편 예약, 항공료, 렌터카, 별장이 해당됩니다.	www.expedia.com www.lonelyplanet.com
미분류	—	—	Cisco 데이터베이스에 없는 웹사이트는 보고를 위해 미분류로 기록됩니다. 여기에는 잘못 입력된 URL도 포함될 수 있습니다.	—
무기	weap	1036	총포상, 총기 경매, 총기 분류 광고, 총기 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 군 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

표 15-1

URL 범주	약어	코드	설명	URL 예
웹 페이지 번역	tran	1063	웹 페이지를 여러 언어로 번역해 줍니다.	babelfish.yahoo.com translate.google.com
웹 기반 이메일	mail	1038	공개 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

URL 범주 결정

특정 URL의 범주를 조회하려면 범주 미지정 및 미분류 URL 보고, 15-21페이지에 표시된 사이트를 방문하십시오.

범주 미지정 및 미분류 URL 보고

범주가 잘못 지정된 URL과 범주가 지정되지 않았지만 지정해야 하는 URL을 보고하려면 다음 사이트를 방문하십시오.

https://securityhub.cisco.com/web/submit_urls

제출된 URL의 상태를 확인하려면 이 페이지의 **Status on Submitted URLs(제출된 URL의 상태)** 탭을 클릭하십시오.

향후 URL 범주 집합 변경

드물지만, 새롭게 떠오르는 트렌드와 기술로 인해 URL 범주 집합이 변경될 수 있습니다. 예를 들어, 범주가 추가 또는 제거되거나, 이름이 변경되거나, 다른 범주와 병합되거나, 2개의 범주로 분할될 수 있습니다. 이러한 변경은 기존 필터의 결과에 영향을 미칠 수 있으므로 변경이 발생하면 어플라이언스에서 경고(시스템 유형, 경고 심각도)를 보냅니다. 그러한 경고를 수신하면 콘텐츠 및 메시지 필터를 평가하고 경우에 따라 업데이트된 범주와 연동되도록 업데이트해야 합니다. 기존 필터는 자동으로 변경되지 않습니다. 이러한 경고를 받으려면 알림 수신자 추가, 33-35페이지를 참조하십시오.

다음과 같은 변경은 범주 집합 변경이 필요하지 않으므로 경고를 생성하지 않습니다.

- 새로 범주가 지정된 사이트의 일상적인 범주 지정
- 미분류 사이트의 범주 재지정

16 장

파일 평판 필터링 및 파일 분석

파일 평판 필터링 및 파일 분석의 개요

Advanced Malware Protection은 다음을 통해 이메일 첨부 파일의 제로데이 및 표적 파일 기반 위협으로부터 보호합니다.

- 각 파일의 평판 획득
- 아직 평판 서비스에 알려지지 특정 파일의 동작 분석
- 사용자에게 네트워크에 들어온 후 위협으로 확인된 파일에 대해 알림

이러한 기능은 수신 메시지에만 사용할 수 있습니다. 발송 메시지에 첨부된 파일은 평가되지 않습니다.

평판 서비스는 클라우드에 있습니다. 파일 분석 서비스에는 퍼블릭 또는 프라이빗 클라우드(온프레미스)에 대한 옵션이 있습니다.

파일 위협 판정 업데이트

위협 판정은 새 정보가 나타나면 변경될 수 있습니다. 파일이 처음에 알 수 없음 또는 클린으로 평가될 수 있으므로 파일이 수신자에게 릴리스될 수 있습니다. 위협 판정이 변경되면 사용자에게 경고가 전달되고 파일과 파일의 새로운 판정이 AMP 판정 업데이트 보고서에 표시됩니다. 위협의 영향을 해결할 수 있는 시작점으로 진입점 메시지를 조사할 수 있습니다.

판정이 악성에서 클린으로 변경될 수도 있습니다.

어플라이언스가 동일한 파일의 후속 인스턴스를 처리할 경우 업데이트 판정이 즉시 적용됩니다.

관련 주제

- 파일 평판 및 파일 분석 보고 및 추적, 16-13페이지
- 파일 위협 판정 변경 시 작업 수행, 16-15페이지

파일 처리 개요

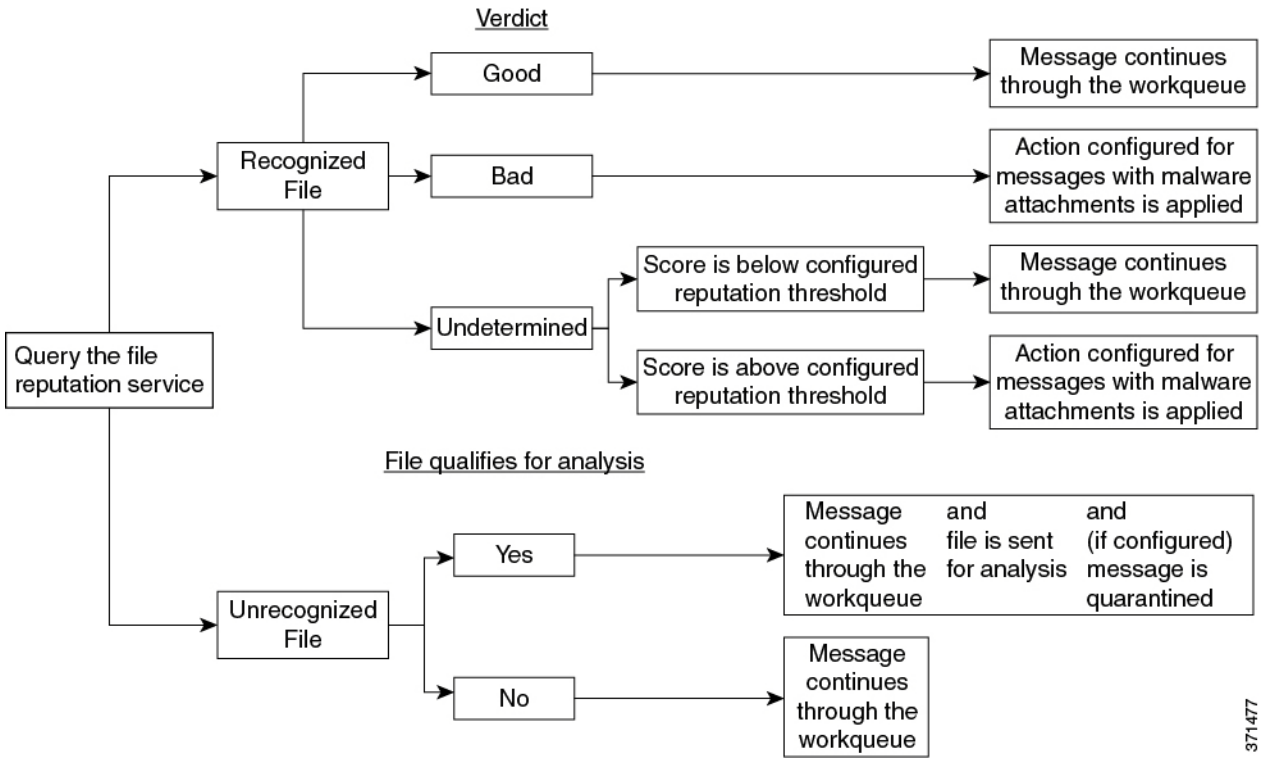
메시지에 대한 최종 작업이 수행되지 않은 경우 파일 판정 평가와 분석을 위한 파일 전송은 이전 검사 엔진의 판정과 관계없이 안티바이러스 검사 직후에 이루어집니다.

어플라이언스와 파일 평판 서비스 간의 통신은 암호화되어 변조로부터 보호됩니다.

파일의 평판이 평가된 후:

- 파일이 파일 평판 서비스에 알려지고 클린으로 확인되면 메시지가 workqueue를 통해 계속됩니다.
- 파일 평판 서비스가 메시지의 첨부 파일에 대해 악성코드 판정을 반환하면 어플라이언스가 사용자가 적용 가능한 메일 정책에서 지정한 작업을 적용합니다.
- 파일 평판이 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 어플라이언스가 사용자가 메일 정책에서 맬웨어가 포함된 파일에 대해 구성한 작업을 적용합니다.
- 평판 서비스에 파일에 대한 정보가 없고 파일이 분석 기준을 충족하지 않을 경우(어떤 파일이 평가 및 분석됩니까?, 16-3페이지 참조) 파일이 클린으로 간주되어 메시지가 workqueue를 통해 계속됩니다.
- 파일 분석 서비스를 활성화하고 평판 서비스에 파일에 대한 정보가 없으며 파일이 분석 가능한 파일에 대한 기준을 충족하면(어떤 파일이 평가 및 분석됩니까?, 16-3페이지 참조) 메시지가 격리되고(분석을 위해 전송된 첨부 파일이 포함된 메시지 격리, 16-9페이지 참조) 파일이 분석을 위해 전송될 수 있습니다. 첨부 파일이 분석을 위해 전송될 경우 메시지를 격리하도록 어플라이언스를 구성하지 않았거나 파일이 분석을 위해 전송되지 않은 경우 메시지가 사용자에게 릴리스됩니다.
- 온프레미스 파일 분석과 함께 배포할 경우 평판 평가와 파일 분석이 동시에 발생합니다. 평판 서비스에는 다양한 소스의 입력이 포함되므로 평판 서비스가 판정을 반환하면 해당 판정이 사용됩니다. 파일이 평판 서비스에 알려지지 않고 해당 파일 분석 판정이 사용됩니다.
- 예를 들어, 파일 평판 또는 파일 분석 판정 정보를 사용할 수 없는 경우 서비스와의 연결 제한 시간이 초과되므로 파일이 클린으로 간주되어 최종 사용자에게 릴리스됩니다. 다른 이유로 인해 판정을 검사할 수 없는 경우 어플라이언스가 사용자가 해당 메일 정책에서 검사할 수 없는 첨부 파일에 대해 지정한 작업을 적용합니다.

그림 16-1 퍼블릭 클라우드 파일 분석 배포를 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.
- 분석을 위해 클라우드로 전송된 그리고 "악성코드" 판정을 받은 모든 파일에 대한 정보가 평판 데이터베이스에 추가됩니다. 온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용하여 분석된 파일에 대한 정보는 평판 서비스와 공유되지 않지만 그 결과가 로컬로 캐시됩니다.

판정 업데이트에 대한 자세한 내용은 파일 위협 판정 업데이트, 16-1페이지를 참조하십시오.

어떤 파일이 평가 및 분석됩니까?

평판 서비스는 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 경우 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.

파일의 평판 평가 및 분석을 위한 파일 전송에 대한 기준은 언제든지 변경될 수 있습니다. 기준은 등록된 Cisco 고객에게만 적용됩니다. 평가 및 분석되는 파일에 대한 내용은 *Cisco 콘텐츠 보안 제품용 Advanced Malware Protection 서비스의 파일 기준* (http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html)을 참조하십시오.

이 문서에 액세스하려면 지원 계약을 통해 제공된 Cisco 고객 계정이 있어야 합니다. 등록하려면 https://tools.cisco.com/RPF/register/register.do를 방문하십시오.

Advanced Malware Protection으로 해결되지 않는 파일의 전송을 차단할 수 있는 정책을 구성합니다.

관련 주제

- 파일 평판 및 분석 서비스 활성화 및 구성, 16-6페이지
- Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 16-13페이지
- 아카이브 또는 압축 파일 처리, 16-4페이지

아카이브 또는 압축 파일 처리

파일이 압축 또는 아카이브될 경우

- 압축 또는 아카이브 파일의 평판이 평가됩니다.
- 압축 또는 아카이브 파일의 압축이 해제되며 추출된 모든 파일의 평판이 평가됩니다.

파일 형식을 포함하여 검사되는 아카이브 및 압축 파일에 대한 내용은 어떤 파일이 평가 및 분석됩니까?, 16-3페이지에서 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).
- 압축 또는 아카이브 파일의 압축을 푸는 동안 파일의 추출이 실패할 경우 파일 평판 서비스가 압축 또는 아카이브 파일에 대해 검사 불가 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 검사 불가 판정보다 우선함).

참고 보안 MIME 유형으로 추출된 파일의 평판은 평가되지 않습니다.

파일 평판 및 분석 구성 기능

- 파일 평판 및 분석 서비스와의 통신을 위한 요건, 16-5페이지
- 온프레미스 파일 분석 서버 구성, 16-5페이지
- 파일 평판 및 분석 서비스 활성화 및 구성, 16-6페이지
- (퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성, 16-7페이지
- 파일 평판 검사 및 파일 분석을 위한 수신 메일 정책 구성, 16-8페이지
- 분석을 위해 전송된 첨부 파일이 포함된 메시지 격리, 16-9페이지
- 파일 분석 격리 사용, 16-10페이지
- 중앙 집중식 파일 분석 격리, 16-12페이지
- 파일 평판 및 분석을 위한 X-헤더, 16-12페이지
- 최종 사용자에게 삭제된 메시지 또는 첨부 파일에 대한 알림 전송, 16-12페이지
- Advanced Malware Protection 및 클러스터, 16-12페이지

- Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 16-13페이지
- Advanced Malware Protection 기능에 대한 중앙 집중식 보고 구성, 16-13페이지

파일 평판 및 분석 서비스와의 통신을 위한 요건

- 이러한 서비스를 사용하는 모든 Email Security 어플라이언스는 인터넷을 통해 직접 서비스에 연결할 수 있어야 합니다(온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용하도록 구성된 파일 분석 서비스 제외).
- 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.
- 열어야 하는 방화벽 포트에 대한 내용은 부록 D, "방화벽 정보"를 참조하십시오.

관련 주제

- TCP/IP 트래픽 경로 구성, 33-55페이지

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 어플라이언스 설명서는 http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html에서 사용할 수 있습니다.

  이 항목에 설명된 작업을 수행하려면 이 설명서를 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 어플라이언스, 에 대한 모든 정보를 검색합니다.
- Cisco AMP Threat Grid 어플라이언스를 설정하고 구성합니다.
- 필요한 경우 Cisco AMP Threat Grid 어플라이언스 소프트웨어를 1.2.1 버전으로 업데이트하여 Cisco Email Security 어플라이언스 와의 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 어플라이언스는 AMP Threat Grid 어플라이언스의 CLEAN 인터페이스에 연결할 수 있어야 합니다.
- 자체 서명 인증서를 배포할 경우: Email Security 어플라이언스에서 사용할 Cisco AMP Threat Grid 어플라이언스에서 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.
- 파일 분석 구성을 제출하면 Email Security 어플라이언스가 Threat Grid 어플라이언스에 자동으로 등록됩니다(파일 평판 및 분석 서비스 활성화 및 구성, 16-6페이지에 설명됨). 그러나 동일한 절차에 설명된 대로 등록을 활성화해야 합니다.

파일 평판 및 분석 서비스 활성화 및 구성

시작하기 전에

- 파일 평판 서비스 및 파일 분석 서비스에 대한 기능 키를 얻습니다.
- 파일 평판 및 분석 서비스와의 통신을 위한 요건, 16-5페이지를 충족해야 합니다.
- 업데이트 페이지에 업데이트 서버에 대한 연결이 구성되었는지 확인합니다. .
- Cisco AMP Threat Grid 어플라이언스를 프라이빗 클라우드 파일 분석 서버로 사용할 경우 온프레미스 파일 분석 서버 구성, 16-5페이지를 참조하십시오.

절차

1단계 **Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)**를 선택합니다.

2단계 Enable(활성화)을 클릭합니다.

3단계 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

4단계 선택 **Enable File Reputation(파일 평판 활성화)**을 선택합니다.

5단계 라이센스 계약이 표시되는 동의합니다.

6단계 파일 분석이 기본적으로 활성화되어 있습니다. **Enable File Analysis(피일 분석 활성화)**를 선택 취소하지 않으면 다음 커밋 후에 파일 분석 기능 키가 활성화됩니다.

7단계 **파일 분석** 섹션에서 분석을 위해 클라우드로 보낼 파일 유형을 선택합니다.

8단계 필요에 따라 다음 파일 평판 **고급 설정**을 조정합니다.

옵션	설명
파일 평판의 SSL 통신	기본 포트 32137이 아닌 포트 443에서 통신하려면 **Use SSL (Port 443)(SSL 사용(포트 443))**을 선택합니다. 이 옵션을 사용하여 파일 평판 서비스와의 통신에 사용할 업스트림 프록시를 구성할 수도 있습니다. **참고** 방화벽에서 포트를 열려면 포트 32137을 통한 SSL 통신이 필요할 수 있습니다.
평판 임계값 • 클라우드 서비스의 값 사용 • 사용자 지정 값 입력	허용되는 파일 평판 점수의 상한. 이 임계값 위의 점수는 해당 파일이 감염되었음을 나타냅니다.

참고 Cisco 지원팀의 지침 없이 이 섹션의 다른 설정을 변경하지 마십시오.

9단계 파일 분석을 위해 클라우드 서비스를 사용할 경우:

a. **Advanced Settings for File Analysis(파일 분석 고급 설정)**를 선택합니다.

b. Email Security 어플라이언스에 물리적으로 가장 가까운 클라우드 서버를 선택합니다.

새로 제공된 서버가 표준 업데이트 프로세스를 사용하여 이 목록에 주기적으로 추가됩니다.

10단계 파일 분석을 위해 온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용할 경우:

Advanced Settings for File Analysis(파일 분석 고급 설정)를 구성합니다.

옵션	설명
파일 분석 서버 URL	**Private cloud(프라이빗 클라우드)**를 선택합니다.
서버	온프레미스로 Cisco AMP Threat Grid 어플라이언스의 URL. 이 값과 인증서에 IP 주소가 아니라 호스트 이름을 사용합니다.
인증서	다음 중 하나를 수행합니다. • Cisco 기본 인증 기관을 선택합니다. • 온프레미스 Cisco AMP Threat Grid 어플라이언스에서 생성한 자체 서명 인증서를 업로드합니다. 가장 최근에 업로드된 자체 서명 인증서가 사용됩니다. 가장 최근 인증서 이전에 업로드된 인증서에 액세스할 수 없습니다. 필요한 경우 원하는 인증서를 다시 업로드합니다.

11단계 변경 사항을 제출하고 커밋합니다.

12단계 온프레미스 Cisco AMP Threat Grid 어플라이언스를 사용할 경우 AMP Threat Grid 어플라이언스에서 이 어플라이언스를 활성화해야 합니다:

활성화 프로세스에 대한 자세한 지침은 AMP Threat Grid 문서에서 확인할 수 있습니다.

a. 페이지 하단에 파일 분석 클라이언트 ID가 나타납니다.

b. AMP Threat Grid 어플라이언스에 로그인합니다.

c. **Welcome...(시작...) > Manage Users(사용자 관리)**를 선택합니다.

d. Email Security 어플라이언스의 파일 분석 클라이언트 ID를 기준으로 "사용자" 계정을 찾습니다.

e. 어플라이언스의 이 "사용자" 계정을 활성화합니다.

(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.

1단계 **Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)**를 선택합니다.

2단계 파일 분석 클라우드 보고 섹션의 어플라이언스 그룹화에 분석 그룹 ID를 입력합니다.

- 그룹 ID를 잘못 입력하거나 어떠한 이유로 인해 이를 변경해야 할 경우 Cisco TAC에서 케이스를 열어야 합니다.
- 이 변경 사항은 즉시 적용되므로 커밋이 필요하지 않습니다.
- 이 값은 분석을 위해 업로드된 파일에 대한 데이터를 공유하는 모든 어플라이언스에서 동일해야 합니다.
- 이 값에 CCOID를 사용하는 것이 좋습니다. 그러나 이 항목의 정확성은 검증되지 않습니다.
- 이 값은 대/소문자를 구분합니다.
- 그룹의 모든 어플라이언스가 클라우드에서 동일한 파일 분석 서버를 사용하도록 구성되어야 합니다.

- 어플라이언스는 한 개의 그룹에만 속할 수 있습니다.
- 언제든지 그룹에 머신을 추가할 수 있지만 한 번만 추가할 수 있습니다.

3단계 **Group Now(지금 그룹화)**를 클릭합니다.

관련 주제

- 분석 그룹에 어떤 어플라이언스가 있습니까?, 16-8페이지

분석 그룹에 어떤 어플라이언스가 있습니까?

1단계 **Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)**를 선택합니다.

2단계 파일 분석 클라우드 보고를 위한 어플라이언스 그룹화 섹션에서 **View Appliances(어플라이언스 보기)** 를 클릭합니다.

3단계 특정 어플라이언스의 **파일 분석 클라이언트 ID**를 보려면 다음 위치에서 찾으십시오.

어플라이언스	파일 분석 클라이언트 ID의 위치
Email Security 어플라이언스	**Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석)** 페이지에서 파일 분석 고급 설정 섹션
웹 보안 어플라이언스	**Security Services(보안 서비스) > Anti-Malware and Reputation(안티맬웨어 및 평판)** 페이지에서 파일 분석 고급 설정 섹션
보안 관리 어플라이언스	**Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Security Appliances(보안 어플라이언스)** 페이지의 하단

관련 주제

- (퍼블릭 클라우드 파일 분석 서비스만 해당) 어플라이언스 그룹 구성, 16-7페이지

파일 평판 검사 및 파일 분석을 위한 수신 메일 정책 구성

절차

1단계 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)**를 선택합니다.

2단계 수정하려면 메일 정책의 **Advanced Malware Protection** 열에 있는 링크를 클릭합니다.

3단계 옵션을 선택합니다.

- 온프레미스 Cisco AMP Threat Grid 어플라이언스가 없고 예를 들어 기밀성의 이유로 클라우드에 파일을 전송하지 않으려면 **Enable File Analysis(파일 분석 활성화)**를 선택 취소합니다.
- 첨부 파일이 검사 불능으로 간주될 경우 AsyncOS에서 수행해야 하는 작업을 선택합니다. 어플라이언스가 어떠한 이유로 인해(예: 연결 시간 초과) 파일 평판 서비스에서 정보를 가져올 수 없는 경우 첨부 파일이 검사 불능으로 간주됩니다.

다음을 선택합니다.

- 메시지를 전송할지 또는 삭제할지 여부
- 원본 메시지를 아카이브할지 여부. 아카이브된 메시지는 mbox 형식의 로그 파일로 어플라이언스의 `amparchive` 디렉토리에 저장됩니다. 사전 구성된 AMP 아카이브(`amparchive`) 로그 가입이 필요합니다.
- 메시지 제목을 수정하여 최종 사용자에게 경고할지 여부(예: [경고: 첨부 파일에 맬웨어가 포함되었을 수 있음])
- 관리자에게 세분화된 제어를 제공하기 위해 사용자 지정 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 아카이브(`amparchive`) 로그 가입이 필요합니다.
  - 맬웨어 첨부 파일을 제거한 후 메시지를 전송할지 여부
  - 메시지 제목을 수정하여 최종 사용자에게 경고할지 여부(예: [경고: 첨부 파일에서 맬웨어가 탐지되었음])
  - 관리자에게 세분화된 제어를 제공하기 위해 사용자 지정 헤더를 추가할지 여부
- 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 아카이브(`amparchive`) 로그 가입이 필요합니다.
  - 메시지 제목을 수정하여 최종 사용자에게 경고할지 여부(예: "`[경고: 첨부 파일에 맬웨어가 포함되었을 수 있음]`")
  - 관리자에게 세분화된 제어를 제공하기 위해 사용자 지정 헤더를 추가할지 여부

4단계 변경 사항을 제출하고 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.

절차

1단계 **Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책)**를 선택합니다.

2단계 수정하려면 메일 정책의 **Advanced Malware Protection** 열에 있는 링크를 클릭합니다.

3단계 파일 분석이 보류 중인 메시지 섹션의 메시지에 적용된 작업 드롭다운에서 **Quarantine(격리)**을 선택합니다.

격리된 메시지는 파일 분석 격리에 저장됩니다. 파일 분석 격리 사용, 16-10페이지를 참조하십시오.

4단계 (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 아카이브(`amparchive`) 로그 가입이 필요합니다.
- 메시지 제목을 수정하여 최종 사용자에게 경고할지 여부(예: "`[경고: 첨부 파일에 맬웨어가 포함되었을 수 있음]`")
- 관리자에게 세분화된 제어를 제공하기 위해 사용자 지정 헤더를 추가할지 여부

5단계 변경 사항을 제출하고 커밋합니다.

관련 주제

- 파일 분석 격리 사용, 16-10페이지
- 정책, 바이러스 및 신종 바이러스 격리, 30-1페이지

파일 분석 격리 사용

파일 분석 격리 설정 편집

절차

1단계 **Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택합니다.

2단계 **File Analysis(파일 분석)** 격리 링크를 클릭합니다.

3단계 보관 기간을 지정합니다.

4단계 거부 기간이 경과된 후 AsyncOS에서 수행해야 할 기본 작업을 지정합니다.

5단계 지정한 보관 기간이 종료되기 전에 이 격리의 메시지를 처리하지 *않으려면* 격리 디스크 공간이 가득 찼더라도 **Free up space by applying default action on messages upon space overflow(공간 오버플로 시 메시지에 기본 작업을 적용하여 공간 확보)**를 선택 취소합니다.

6단계 기본 작업으로 **Release(릴리스)**를 선택한 경우 보관 기간이 경과되기 전에 릴리스되는 메시지에 적용할 추가 작업을 선택적으로 지정합니다.

옵션	정보
제목 수정	추가할 텍스트를 입력하고 이 텍스트를 원래 메시지 제목의 처음에 추가할지 아니면 끝에 추가할지를 지정합니다. 예를 들어, 사용자가 수신자에게 메시지에 맬웨어 첨부 파일이 포함되었을 수 있다고 경고하려 할 수 있습니다. **참고** 비 ASCII 문자가 포함된 제목을 올바르게 표시하려면 RFC 2047에 따라 표시해야 합니다.
X-헤더 추가	X-헤더는 메시지에 대해 수행된 작업의 레코드를 제공할 수 있습니다. 이는 예를 들어 특정 메시지가 전송된 이유에 대한 문의를 처리할 때 유용할 수 있습니다. 이름 및 값을 입력합니다. 예: 이름 =`Inappropriate-release-early` 값 = `True`
첨부 파일 제거	첨부 파일 제거를 통해 메시지의 맬웨어 첨부 파일로부터 보호할 수 있습니다.

7단계 이 격리에 액세스할 수 있는 사용자를 지정합니다.

사용자	정보
로컬 사용자	로컬 사용자 목록에는 격리에 액세스할 수 있는 역할이 있는 사용자만 포함됩니다. 모든 관리자는 격리에 완전히 액세스할 수 있으므로 이 목록에서는 관리자 권한이 있는 사용자가 제외됩니다.
외부에서 인증된 사용자	외부 인증을 구성해야 합니다.
사용자 지정 사용자 역할	이 옵션은 격리 액세스 권한이 있는 사용자 지정 사용자 역할을 최소한 하나 이상 생성한 경우에만 표시됩니다.

8단계 변경 사항을 제출하고 커밋합니다.

파일 분석 격리의 메시지를 수동으로 처리

절차

1단계 **Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택합니다.

2단계 파일 분석 격리 표의 해당 행에서 메시지 열에 있는 파란색 숫자를 클릭합니다.

3단계 요건에 따라 메시지에 대해 다음과 같은 작업을 수행합니다.

- 삭제
- 릴리스
- 예약된 격리에서의 종료 지연
- 지정한 이메일 주소로 메시지의 사본 전송

중앙 집중식 파일 분석 격리

중앙 집중식 파일 분석 격리에 대한 내용은 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리 정보, 30-10페이지를 참조하십시오.

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	삭제 악의적인 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 사용자 지정 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.

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
기능 키 만료	(모든 기능에 기본으로 설정된 대로)	
파일 평판 또는 파일 분석 서비스에 연결할 수 없습니다.	시스템	경고
클라우드 서비스와의 통신이 구성되었습니다.	시스템	정보
평판 및 분석 엔진이 watchdog 서비스에 의해 다시 시작됨	시스템	정보
파일 평판 판정이 변경됩니다.	시스템	정보
분석을 위해 전송할 수 있는 파일 유형이 변경되었습니다. 새 파일 유형의 업로드를 활성화할 수 있습니다.	시스템	정보
일부 파일 유형에 대한 분석을 일시적으로 사용할 수 없습니다.	시스템	경고
지원되는 모든 파일 유형에 대한 분석이 일시적인 중단된 후 복원됩니다.	시스템	정보

관련 주제

- 파일 평판 또는 파일 분석 서버 연결 실패에 대한 여러 경고, 16-16페이지
- 파일 위협 판정 변경 시 작업 수행, 16-15페이지

Advanced Malware Protection 기능에 대한 중앙 집중식 보고 구성

보안 관리 어플라이언스에서 보고를 중앙 집중화할 경우 온라인 도움말의 이메일 보고 장 또는 관리 어플라이언스의 사용 설명서에 있는 Advanced Malware Protection 섹션의 중요한 구성 요건을 참조하십시오.

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)으로 나열됩니다.

파일 평판 및 파일 분석 보고서 페이지

보고서	설명
AMP(Advanced Malware Protection)	구성에 따라 파일 평판 서비스. 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.
파일 분석	분석을 위해 전송된 각 파일의 시간 및 판정(또는 임시 판정)을 표시합니다. Cisco AMP Threat Grid 어플라이언스의 허용 목록에 나열된 파일은 "클린"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 특성을 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.
AMP 판정 업데이트	메시지가 수신된 이후에 판정이 변경되어 이 어플라이언스에서 처리한 파일을 표시합니다. 이 상황에 대한 내용은 파일 위협 판정 업데이트, 16-1 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. 보고서에 대해 선택된 시간 범위와 관계없이 최대 가용 시간 범위 내의 특정 SHA-256의 영향을 받는 모든 메시지을 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. "Advanced Malware Protection에 의해 탐지됨" 열이 해당 보고서에서 기본적으로 숨겨질 수 있습니다. 추가 열을 표시하려면 표 아래의 Columns(열) 링크를 클릭합니다.

메시지 추적 및 Advanced Malware Protection 기능 정보

메시지 추적에서 파일 위협 정보를 검색할 경우 다음 사항에 유의하십시오.

- 파일 평판 서비스에 의해 발견된 악성 파일을 검색하려면 **Advanced Malware Protection Positive(Advanced Malware Protection 판정)**를 Message Event(메시지 이벤트) 옵션(메시지 추적의 고급 섹션)으로 선택합니다.
- 메시지 추적에는 파일 평판 처리와 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
  - 맬웨어가 포함된 것으로 확인된 첨부 파일

    클린 또는 검사 불가 첨부 파일에 대해 제공된 정보가 없습니다.
- 판정 업데이트는 AMP 판정 업데이트 보고서에서만 사용할 수 있습니다. 판정이 변경된 경우 메시지 추적의 원래 메시지 세부사항이 업데이트되지 않습니다. 특정 첨부 파일이 있는 메시지를 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 클라우드에서 사용할 수 있습니다. 파일에 대한 사용 가능한 파일 분석 정보를 보려면 **Monitor(모니터링) > File Analysis(파일 분석)**를 선택하고 SHA-256을 입력하여 해당 파일을 검색합니다. 파일 분석 서비스가 어떤 소스에서 파일을 분석한 경우 세부사항을 볼 수 있습니다. 결과는 분석된 파일에 대해서만 표시됩니다.

  어플라이언스가 분석을 위해 전송된 파일의 후속 인스턴스를 처리한 경우 그러한 인스턴스가 메시지 추적 검색 결과에 표시됩니다.

파일 위협 판정 변경 시 작업 수행

절차

1단계	AMP 판정 업데이트 보고서를 봅니다.
2단계	관련 SHA-256 링크를 클릭하여 최종 사용자에게 제공되었을 수 있는 파일이 포함된 모든 메시지에 대한 메시지 추적 데이터를 봅니다.
3단계	추적 데이터를 사용하여 위협에 포함된 파일 이름 및 파일의 발신자와 같은 정보뿐 아니라 손상되었을 수 있는 사용자를 파악합니다.
4단계	파일 분석 보고서를 검토하여 이 SHA-256이 분석을 위해 전송되었는지 확인하고 파일의 위협 동작을 더 자세히 이해합니다.

관련 주제

- 파일 위협 판정 업데이트, 16-1페이지

파일 평판 및 분석 문제 해결

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 문의에 대해 수신한 응답)"에서 "upload action(업로드 작업)"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.

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, 16-5페이지에서 요건을 충족했는지 확인합니다.
- 어플라이언스가 클라우드 서비스와 통신하는 것을 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 섹션의 고급 설정 영역에 있습니다.

API 키 오류(온프레미스 파일 분석)

문제 파일 분석 보고서 세부사항을 보려고 시도하거나 Email Security 어플라이언스에서 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 어플라이언스에서 새 인증서를 생성합니다.
- 새 인증서를 Email Security 어플라이언스에 업로드합니다.
- AMP Threat Grid 어플라이언스의 API 키를 재설정합니다. 지침은 AMP Threat Grid 어플라이언스에 대한 온라인 도움말을 참조하십시오.

관련 주제

- 파일 평판 및 분석 서비스 활성화 및 구성, 16-6페이지

데이터 유출 방지

데이터 유출 방지 개요

데이터 유출 방지(DLP) 기능은 조직의 독점 정보 및 지적 재산을 보호하고 사용자가 네트워크에서 악성적으로 또는 비고의적으로 민감한 데이터를 이메일로 보내고 받지 못하도록 방지하여 정부 규정을 준수하도록 합니다. 법률 또는 기업 정책을 위반할 수 있는 데이터에 대해 발송 메시지 검사에 사용되는 DLP 정책을 생성하여 직원이 이메일을 보낼 수 없는 데이터 유형을 정의합니다.

관련 주제

- DLP 검사 프로세스 개요, 17-2페이지
- 데이터 유출 방지 작동 방식, 17-2페이지

DLP 검사 프로세스 개요

	작업	추가 정보
1.	조직의 사용자는 조직 외부의 수신자에게 이메일 메시지를 보냅니다.	Email Security 어플라이언스는 네트워크에 진입하거나 빠져나가는 메시지를 처리하는 "게이트웨이" 어플라이언스입니다. 네트워크 내에서 다른 사용자에게 전송된 메시지는 검사되지 않습니다.
2.	Email Security 어플라이언스는 DLP 검사 단계 전에 이메일 "작업 큐" 단계를 거쳐 메시지를 처리합니다.	사전 DLP 검사 프로세스는 예를 들어 메시지에 스팸 또는 악성코드가 포함되어 있는지 확인합니다. 작업 큐에서 DLP 프로세싱이 발생하는 위치를 확인하려면 이메일 파이프라인 흐름, 4-1페이지에서 작업 큐 흐름도를 참조하십시오.
3.	어플라이언스는 DP 정책을 통해 식별한 민감한 콘텐츠에 대해 메시지 본문, 헤더 및 첨부 파일을 검사합니다.	데이터 유출 방지 작동 방식, 17-2페이지 항목을 참조하십시오.
4.	민감한 콘텐츠를 발견한 경우 어플라이언스는 메시지를 격리하거나 삭제하거나 제한적으로 제공하는 등 데이터를 보호하기 위한 작업을 수행합니다. 그렇지 않으면 메시지가 어플라이언스의 작업 큐를 계속 거치게 되고 문제가 발견되지 않는 경우 Email Security 어플라이언스는 이를 수신자에게 전달합니다.	수행할 작업을 정의합니다. 메시지 작업, 17-32페이지 항목을 참조하십시오.

데이터 유출 방지 작동 방식

조직에 속한 사람이 메시지를 조직 외부 수신자에게 보내는 경우 어플라이언스는 정의한 규칙에 따라 해당 메시지의 발신자 또는 수신자에게 적용할 발송 메일 정책을 결정합니다. 어플라이언스는 해당 발송 메일 정책에 지정된 DLP 정책을 사용하여 메시지의 콘텐츠를 평가합니다.

특히 어플라이언스는 해당 DLP 정책에서 민감한 콘텐츠로 식별한 사회 보장 번호 또는 정규식 등 사전 정의된 패턴, 단어, 구문과 일치하는 텍스트의 메시지 콘텐츠(헤더 및 첨부 파일 포함)를 검사합니다.

또한 어플라이언스는 긍정 오류를 최소화하기 위해 허용되지 않는 콘텐츠의 컨텍스트를 평가합니다. 예를 들어 신용 카드 번호 패턴과 일치하는 번호는 만료 날짜, 신용 카드 회사 이름(Visa, AMEX 등) 또는 사람 이름 및 주소가 포함되는 경우에만 위반입니다.

메시지 콘텐츠가 하나 이상의 DLP 정책과 일치하는 경우 목록에서 첫 번째로 일치하는 DLP 정책이 지정한 순서에 따라 적용됩니다. 발송 메일 정책에 콘텐츠가 정책 위반인지 결정하는 데 동일한 기준을 사용하는 여러 DLP 정책이 있는 경우 모든 정책에서 단일 콘텐츠 검사 결과가 사용됩니다.

잠재적으로 민감한 콘텐츠가 메시지에 표시되는 경우 어플라이언스는 위험 계수를 0~100으로 잠재 위반에 할당합니다. 이 점수는 메시지에 DLP 위반이 포함될 가능성을 나타냅니다.

어플라이언스는 해당 위험 계수 점수에 정의한 심각도 수준(심각 또는 낮음 등)을 할당하고 해당 DLP 정책에서 해당 심각도 수준에 지정한 메시지 작업을 수행합니다.

DLP 구축 옵션

RSA 이메일 DLP	RSA Enterprise Manager
모든 DLP 작업은 Email Security 어플라이언스에서 처리합니다.	서버에서 실행되며 Email Security 어플라이언스와 "파트너 장치"로 작동하는 RSA의 타사 DLP 관리 소프트웨어입니다. **참고** RSA Enterprise Manager는 Cisco에서 구입할 수 없습니다.
클러스터 구축을 제외하고 단일 Email Security 어플라이언스에서 DLP 정책을 관리합니다.	중앙 집중식 인터페이스에서 여러 Email Security 어플라이언스를 포함하는 동일한 네트워크의 여러 장치에 대한 DLP 정책을 관리합니다.
Email Security 어플라이언스에서 DLP 정책을 구성합니다.	조직 전반에 일관된 DLP 정책을 위해 정책은 Enterprise Manager에서 구성되며 네트워크의 Email Security 어플라이언스로 푸시됩니다.
사용자가 이메일로 전송할 수 없는 민감한 데이터를 정의하는 데 조직이 사용할 수 있는 RSA로 설계된 100개가 넘는 DLP 정책 템플릿을 포함합니다.	RSA의 DLP 정책 템플릿을 포함하며 RSA의 DLP 데이터센터와 통합하여 특정 DLP 정책에서 소스 코드 및 문서를 검사하는 데 핑거프린팅 탐지 방식을 사용합니다. 핑거프린팅은 핑거프린팅, 17-24페이지에 설명되어 있습니다.
Email Security 어플라이언스 또는 보안 관리 어플라이언스에서 격리된 메시지를 확인하고 관리합니다.	격리된 메시지는 Email Security 어플라이언스 또는 보안 관리 어플라이언스에 보관됩니다. Enterprise Manager Email Security 어플라이언스 또는 보안 관리 어플라이언스에서 격리된 메시지를 볼 수 있습니다. Enterprise Manager를 사용하여 격리된 메시지를 관리(예: 삭제 또는 릴리스)해야 합니다.
Email Security 어플라이언스 또는 보안 관리 어플라이언스에서 보고 및 데이터 추적을 확인하고 검색합니다.	Enterprise Manager Email Security 어플라이언스 또는 보안 관리 어플라이언스에서 보고 및 데이터 추적을 확인하고 검색합니다.
—	기존 DLP 구성을 Email Security 어플라이언스에서 Enterprise Manager로 마이그레이션합니다.
자세한 내용은 RSA 이메일 DLP, 17-4페이지 항목을 참조하십시오.	자세한 내용은 RSA Enterprise Manager, 17-22페이지 항목을 참조하십시오.

참고 다음 작업은 Email Security 어플라이언스에서만 발생합니다.

- 발송 메일 정책 정의
- 메시지 작업 정의
- DLP 검사

데이터 유출 방지의 시스템 요구 사항

데이터 유출 방지는 D-모드 라이센스를 사용하는 어플라이언스를 제외한 지원되는 모든 C-시리즈 및 X-시리즈 어플라이언스에서 지원됩니다.

RSA Enterprise Manager 기능에는 Enterprise Manager 9.0이 필요합니다.

RSA 이메일 DLP

관련 주제

- RSA 이메일 DLP를 사용한 구축에서 데이터 유출 방지를 설정하는 방법, 17-4페이지
- 데이터 유출 방지 활성화(RSA 이메일 DLP), 17-5페이지

RSA 이메일 DLP를 사용한 구축에서 데이터 유출 방지를 설정하는 방법

다음 단계를 순서대로 수행합니다.

	수행할 작업	추가 정보
1단계	DLP 기능을 활성화하고 RSA 이메일 DLP를 구축 옵션으로 선택합니다.	데이터 유출 방지 활성화(RSA 이메일 DLP), 17-5페이지
2단계	위반이 발견되거나 의심되는 메시지에 수행할 수 있는 작업을 정의합니다. 예를 들어 이러한 메시지를 격리할 수 있습니다.	메시지 작업, 17-32페이지
3단계	다음을 수행하는 DLP 정책을 생성합니다. • 조직에서 이메일을 보내거나 받을 수 없는 콘텐츠 식별 • 각 위반에 대해 수행할 작업 지정	방법을 선택합니다. • RSA 이메일 DLP 설정(마법사 사용), 17-7페이지 • 사전 정의된 템플릿을 사용하여 DLP 정책 생성, 17-8페이지 • 사용자 지정 DLP 정책 생성(고급), 17-9페이지
4단계	콘텐츠가 하나 이상의 DLP 정책과 일치할 수 있는 경우 DLP 정책의 순서를 설정하여 DLP를 위반한 메시지를 평가하는 데 사용할 DLP 정책을 결정합니다.	위반 일치에 대한 이메일 DLP 정책 순서 정렬, 17-20페이지
5단계	DLP 위반 검사가 수행될 메시지에 해당하는 발신자 및 수신자의 각 그룹에 발송 메일 정책을 생성했는지 확인합니다.	10 장, "메일 정책" 항목을 참조하십시오. 개별 DLP 정책에서 허용 및 제한된 메시지 발신자 및 수신자를 추가로 조정하려면 DLP 정책에 대한 메시지 필터링, 17-18페이지 항목을 참조하십시오.
6단계	DLP 정책을 발송 메일 정책에 할당하여 발신자 및 수신자에 적용할 DLP 정책을 지정합니다.	DLP 정책을 발송 메일 정책과 연결, 17-20페이지
7단계	민감한 DLP 정보의 저장소 및 액세스에 대한 설정을 구성합니다.	• 메시지 추적 시 민감한 DLP 데이터 표시 또는 숨기기, 17-36페이지 • 메시지 추적 시 중요 정보의 액세스 제어, 32-5페이지

데이터 유출 방지 활성화(RSA 이메일 DLP)

절차

1단계 **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)**를 선택합니다.

2단계 **Enable(활성화)**을 클릭합니다.

3단계 라이센스 계약 페이지 하단으로 스크롤하여 **Accept(동의)**를 클릭하여 계약에 동의합니다.

참고 라이센스 계약에 동의하지 않는 경우 RSA 이메일 DLP는 어플라이언스에서 활성화되지 않습니다.

4단계 **Data Loss Prevention(데이터 유출 방지)**에서 **RSA Email DLP(RSA 이메일 DLP)**를 선택합니다.

5단계 **Enable RSA Email Data Loss Prevention(RSA 이메일 데이터 유출 방지 활성화)** 확인란을 선택합니다.

6단계 (권장) 이 페이지에서 다른 옵션은 선택 해제합니다.

이 장에서 논의된 지침에 따라 이러한 설정은 나중에 변경할 수 있습니다.

7단계 변경사항을 제출하고 커밋합니다.

다음 작업

RSA 이메일 DLP를 사용한 구축에서 데이터 유출 방지를 설정하는 방법, 17-4페이지 항목을 참조하십시오.

관련 주제

- 메시지 추적 시 민감한 DLP 데이터 표시 또는 숨기기, 17-36페이지
- RSA 이메일 DLP 설정(마법사 사용), 17-7페이지
- DLP 엔진 및 콘텐츠 일치 분류자 업데이트 정보, 17-37페이지

DLP 정책(RSA 이메일 DLP용)

관련 주제

- DLP 정책 설명, 17-6페이지
- 사전 정의된 DLP 정책 템플릿, 17-6페이지
- RSA 이메일 DLP 설정(마법사 사용), 17-7페이지
- 사전 정의된 템플릿을 사용하여 DLP 정책 생성, 17-8페이지
- 사용자 지정 DLP 정책 생성(고급), 17-9페이지
- 콘텐츠 일치 분류자를 사용하여 허용되지 않은 콘텐츠 정의에 관한 정보, 17-10페이지
- DLP 정책에 대한 메시지 필터링, 17-18페이지
- 위반 심각도 평가 정보, 17-19페이지
- 위반 일치에 대한 이메일 DLP 정책 순서 정렬, 17-20페이지

- DLP 정책을 발송 메일 정책과 연결, 17-20페이지
- DLP 정책 편집 또는 삭제에 대한 중요 정보, 17-22페이지

DLP 정책 설명

DLP 정책에는 다음이 포함됩니다.

- 발송 메시지가 민감한 데이터를 포함하는지 여부를 결정하는 조건 집합 및
- 메시지가 이러한 데이터를 포함하는 경우 수행해야 할 작업

다음에 따라 메시지 콘텐츠를 평가하는 방법을 지정합니다.

- 허용되지 않는 특정 콘텐츠 또는 정보 패턴. 정책에 따라 정규식을 생성하여 ID 번호를 검색해야 할 수 있습니다. 콘텐츠 일치 분류자를 사용하여 허용되지 않은 콘텐츠 정의에 관한 정보, 17-10페이지 항목을 참조하십시오.
- 필터링 메시지의 특정 발신자 및 수신자 목록. 발신자 및 수신자별 필터링, 17-19페이지 항목을 참조하십시오.
- 필터링 메시지의 첨부 파일 유형 목록. 첨부 파일 유형별 필터링, 17-19페이지 항목을 참조하십시오.
- 위반의 심각도에 따라 수행할 다양한 작업을 허용하는 설정. 위반 심각도 평가 정보, 17-19페이지 항목을 참조하십시오.

DLP 정책을 발송 메일 정책에서 활성화하는 경우 각 정책을 적용할 메시지 발신자 및 수신자를 결정합니다.

사전 정의된 DLP 정책 템플릿

DLP 정책 생성을 간소화하기 위해 어플라이언스에는 RSA, Inc.에서 개발한 사전 정의된 대규모의 정책 템플릿이 포함되어 있습니다.

템플릿 범주에는 다음이 포함됩니다.

- **규정 준수.** 이러한 템플릿은 개인적으로 식별 가능한 정보, 신용 정보 또는 기타 보호 또는 비공개 정보를 포함하는 메시지 및 첨부 파일을 식별합니다.
- **허용 가능한 사용.** 이러한 템플릿은 조직에 관한 민감한 정보가 포함된 경쟁업체 또는 제한된 수신자에게 보낸 메시지를 식별합니다.
- **개인 정보 보호.** 이러한 템플릿은 금융 계정, 세금 기록 또는 국가 ID를 포함하는 메시지 및 첨부 파일을 식별합니다.
- **지적 재산권 보호.** 이러한 템플릿은 조직이 보호하려는 지적 재산권을 포함하거나 많은 사람이 사용하는 발행 및 설계 문서 파일 유형을 식별합니다.
- **회사 기밀.** 이러한 템플릿은 기업 회계 정보 및 향후 합병 및 인수에 관한 정보를 포함하는 문서 및 메시지를 식별합니다.
- **사용자 지정 정책.** 이 "템플릿"은 RSA에서 개발한 콘텐츠 일치 분류자 또는 조직에서 지정한 위반 식별 기준을 사용하여 처음부터 고유한 정책을 생성할 수 있습니다. 이 옵션은 고급 옵션으로 간주되며 사전 정의된 정책 템플릿이 네트워크 환경의 고유한 요구 사항을 만족하지 못하는 비교적 드문 경우에만 사용됩니다.

이러한 템플릿 일부에는 사용자 지정이 필요합니다.

RSA 이메일 DLP 설정(마법사 사용)

DLP 평가 마법사는 일반적으로 사용되는 DLP 정책을 구성하고 이를 어플라이언스의 기본 발송 메일 정책에서 활성화하도록 지원합니다.

참고 기본적으로 DLP 평가 마법사를 사용하여 추가된 DLP 정책은 탐지된 DLP 위반의 심각도와 상관없이 모든 메시지를 전달합니다. 마법사를 사용하여 생성된 정책을 편집해야 합니다.

시작하기 전에

- 어플라이언스에서 기존 DLP 정책을 제거합니다. 어플라이언스에 기존 DLP 정책이 없는 경우 DLP 평가 마법사만 사용할 수 있습니다.
- 신용 카드 번호, 미국 사회 보장 번호 및 미국 운전면허 번호가 아닌 학생 ID 번호 또는 계정 번호를 포함하는 메시지를 탐지해야 하는 경우 이러한 번호를 식별하는 정규식을 생성합니다. 자세한 내용은 ID 번호 식별을 위한 정규식, 17-14페이지 항목을 참조하십시오.

절차

1단계 **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)**를 선택합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 **Enable and configure DLP using the DLP Assessment Wizard(DLP 평가 마법사를 사용하여 DLP 활성화 및 구성)** 확인란을 선택합니다.

4단계 **Submit(제출)**을 클릭합니다.

5단계 마법사를 완료합니다.

다음 사항을 유의해야 합니다.

- 캘리포니아에서 운영되고 실제 위치와는 무관하게 캘리포니아 거주자에 대한 전산화된 개인 식별 정보(PII) 데이터를 소유하거나 라이센스를 부여하는 모든 비즈니스는 **California SB-1386**을 준수해야 합니다. 이 법률은 마법사의 정책 선택 사항 중 하나입니다.
- 자동으로 생성된 예약 DLP 인시던트 요약 보고서를 받을 이메일 주소를 입력하지 않으면 보고서가 생성되지 않습니다.
- 구성된 설정을 검토할 때 변경하는 단계로 돌아가는 경우 검토 페이지에 다시 도달하기 전에 나머지 단계를 거쳐야 합니다. 이전에 입력한 모든 설정이 저장됩니다.
- 마법사를 완료하면 기본 발송 메일 정책에 DLP 정책이 활성화된 상태로 Outgoing Mail Policies(발송 메일 정책) 페이지가 표시됩니다. DLP 정책 구성에 대한 요약이 페이지 상단에 표시됩니다.

6단계 변경사항을 커밋합니다.

다음 작업

- (선택 사항) 이러한 DLP 정책을 편집하고 추가 정책을 생성하고, 메시지의 전체 작업을 변경하거나 심각도 수준 설정을 변경하려면 **Mail Policies(메일 정책) > DLP Policy Manager**를 선택합니다. 자세한 내용은 사전 정의된 템플릿을 사용하여 DLP 정책 생성, 17-8페이지, 사용자 지정 DLP 정책 생성(고급), 17-9페이지 및 심각도 지수 조정, 17-20페이지 항목을 참조하십시오.
- (선택 사항) 기타 발송 메일 정책에 대해 기존 DLP 정책을 활성화하려면 발송 메일 정책을 사용하여 DLP 정책을 발신자 및 수신자에게 할당, 17-21페이지 항목을 참조하십시오.

관련 주제

- 사전 정의된 템플릿을 사용하여 DLP 정책 생성, 17-8페이지
- 사용자 지정 DLP 정책 생성(고급), 17-9페이지

사전 정의된 템플릿을 사용하여 DLP 정책 생성

절차

1단계 **Mail Policies(메일 정책) > DLP Policy Manager**를 선택합니다.

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

3단계 범주 이름을 클릭하면 사용 가능한 RSA 이메일 DLP 정책 템플릿 목록이 표시됩니다.

참고 각 템플릿의 설명을 보려면 **Display Policy Descriptions(정책 설명 표시)**를 클릭합니다.

4단계 **Add(추가)**를 클릭하여 RSA 이메일 DLP 정책 템플릿을 사용합니다.

5단계 (선택 사항) 템플릿에 사전 정의된 이름 및 설명을 변경합니다.

6단계 정책에 하나 이상의 콘텐츠 일치 분류자를 사용자 지정해야 하거나 이러한 사항이 권장되는 경우 정규식을 입력하여 조직의 ID 번호 시스템 패턴 및 ID 번호와 관련된 단어 또는 구문 목록(이러한 방식으로 식별하거나 이와 관련된)을 정의합니다.

자세한 내용은 다음을 참조하십시오.

- 콘텐츠 일치 분류자를 사용하여 허용되지 않은 콘텐츠 정의에 관한 정보, 17-10페이지 및
- ID 번호 식별을 위한 정규식, 17-14페이지

참고 사전 정의된 템플릿을 기반으로 정책에 대한 콘텐츠 일치 분류자를 추가하거나 제거할 수 없습니다.

7단계 (선택 사항) 특정 수신자, 발신자, 첨부 파일 유형 또는 이전에 추가한 메시지 태그가 포함된 메시지에만 DLP 정책을 적용합니다.

자세한 내용은 DLP 정책에 대한 메시지 필터링, 17-18페이지 항목을 참조하십시오.

항목이 여러 개인 경우 줄바꿈 또는 쉼표로 구분할 수 있습니다.

8단계 심각도 설정 섹션에서

- 위반 심각도 수준마다 수행할 작업을 선택합니다.

  자세한 내용은 위반 심각도 평가 정보, 17-19페이지 항목을 참조하십시오.
- (선택 사항) **Edit Scale(지수 편집)**을 클릭하여 정책에 대한 위반 심각도 지수를 조정합니다.

  자세한 내용은 심각도 지수 조정, 17-20페이지 항목을 참조하십시오.

9단계 변경사항을 제출하고 커밋합니다.

관련 주제

- RSA 이메일 DLP 설정(마법사 사용), 17-7페이지
- 사용자 지정 DLP 정책 생성(고급), 17-9페이지

사용자 지정 DLP 정책 생성(고급)

참고 사용자 지정 정책을 생성하는 작업은 매우 복잡합니다. 사전 정의된 DLP 정책 템플릿이 조직의 요구 사항을 만족하지 못하는 경우에만 사용자 지정 정책을 생성합니다.

사용자 지정 정책 템플릿을 사용해서 처음부터 사용자 지정 DLP 정책을 생성하고 사전 정의된 RSA 콘텐츠 일치 분류자 또는 사용자 지정 분류자를 정책에 추가할 수 있습니다.

정책이 정의된 방법에 따라 콘텐츠가 단일 분류자 또는 모든 분류자와 일치하는 경우 사용자 지정 정책이 DLP 위반 결과를 반환할 수 있습니다.

시작하기 전에

제안: 콘텐츠 위반을 식별하는 기준을 정의합니다. 사용자 지정 DLP 정책에 대한 콘텐츠 일치 분류자 생성, 17-13페이지 항목을 참조하십시오. 또한 이 절차 내에서 이러한 기준을 정의할 수 있습니다.

절차

1단계 **Mail Policies(메일 정책) > DLP Policy Manager**를 선택합니다.

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

3단계 사용자 지정 정책 범주의 이름을 클릭합니다.

4단계 사용자 지정 정책 템플릿의 **Add(추가)**를 클릭합니다.

5단계 정책의 이름 및 설명을 입력합니다.

6단계 DLP 위반을 구성하는 콘텐츠 및 컨텍스트를 식별합니다.

a. 콘텐츠 일치 분류자를 선택합니다.

b. **Add(추가)**를 클릭합니다.

- **Create a Classifier(분류자 생성)**를 선택한 경우 사용자 지정 DLP 정책에 대한 콘텐츠 일치 분류자 생성, 17-13페이지 항목을 참조하십시오.
- 그렇지 않으면 선택한 분류자가 표에 추가됩니다.

c. (선택 사항) 추가 분류자를 정책에 추가합니다.

예를 들어 다른 분류자를 추구하고 No(아니요)를 선택하여 알려진 긍정 오류를 제거할 수 있습니다.

d. 여러 분류자를 추가한 경우, 표 제목의 옵션을 선택하여 인스턴스를 위반으로 처리하기 위해 분류자의 **any(일부)** 또는 **all(전부)** 이일치해야 하는지를 지정합니다.

7단계 (선택 사항) 특정 수신자, 발신자, 첨부 파일 유형 또는 이전에 추가한 메시지 태그가 포함된 메시지에만 DLP 정책을 적용합니다.

자세한 내용은 DLP 정책에 대한 메시지 필터링, 17-18페이지 항목을 참조하십시오.

항목이 여러 개인 경우 줄바꿈 또는 쉼표로 구분할 수 있습니다.

8단계 심각도 설정 섹션에서

- 위반 심각도 수준마다 수행할 작업을 선택합니다.

  자세한 내용은 위반 심각도 평가 정보, 17-19페이지 항목을 참조하십시오.

- (선택 사항) **Edit Scale(지수 편집)**을 클릭하여 정책에 대한 위반 심각도 지수를 조정합니다. 자세한 내용은 심각도 지수 조정, 17-20페이지 항목을 참조하십시오.

9단계 변경사항을 제출하고 커밋합니다.

관련 주제

- RSA 이메일 DLP 설정(마법사 사용), 17-7페이지
- 사전 정의된 템플릿을 사용하여 DLP 정책 생성, 17-8페이지
- DLP 정책 복제, 17-12페이지

콘텐츠 일치 분류자를 사용하여 허용되지 않은 콘텐츠 정의에 관한 정보

콘텐츠 일치 분류자는 이메일로 보내거나 받을 수 없는 콘텐츠를 정의하고 데이터 유출 방지 위반으로 간주하기 위해 발생해야 하는 콘텐츠에 대한 컨텍스트를 선택적으로 정의합니다.

조직에서 환자의 ID 번호를 이메일로 보내거나 받지 못하도록 하려고 하는 경우,

어플라이언스에서 이러한 번호를 인식하려면 하나 이상의 정규식을 사용하여 조직에서 사용하는 기록 번호 시스템의 패턴을 지정해야 합니다. 또한 기록 번호가 지원 정보로 함께 제공되는 단어 및 구문 목록을 추가할 수 있습니다. 분류자가 발송 메시지에서 번호 패턴을 탐지하면 지원 정보를 검색하여 해당 패턴이 무작위 번호 문자열이 아닌 ID 번호임을 확인합니다. 컨텍스트 일치 정보를 포함하면 긍정 오류 비율이 감소합니다.

이 예에서는 HIPAA 및 HITECH 템플릿을 사용하는 DLP 정책을 생성할 수 있습니다. 이 템플릿은 환자의 ID 번호를 탐지하도록 사용자 지정할 수 있는 환자 ID 번호 콘텐츠 일치 분류자를 포함합니다. 123-CL456789의 패턴에서 번호를 탐지하려면 분류자에 대해 `[0-9]{3}\-[A-Z]{2}[0-9]{6}` 정규식을 입력합니다. 관련 구문에 "환자 ID"를 입력합니다. 정책 생성을 완료하고 발송 메일 정책에서 활성화합니다. 변경사항을 제출하고 커밋합니다. 이제 정책에서 번호 패턴 가까이에 "환자 ID" 구문이 포함된 발송 메시지에서 번호 패턴을 탐지하면 DLP 정책이 DLP 위반 결과를 반환합니다.

DLP 정책에서 콘텐츠 일치 분류자 사용에 관한 정보

사전 정의된 DLP 정책 템플릿 대부분에는 RSA의 콘텐츠 일치 분류자가 포함됩니다. 이러한 분류자 중 일부는 조직의 데이터에 사용되는 패턴을 식별하기 위해 사용자 지정이 필요합니다.

사용자 지정 DLP 정책을 생성하면 사전 정의된 분류자를 선택하거나 고유 분류자를 생성할 수 있습니다.

관련 주제

- 콘텐츠 일치 분류자 예, 17-11페이지
- 사용자 지정 DLP 정책에 대한 콘텐츠 일치 분류자 생성, 17-13페이지
- 분류자 민감한 콘텐츠 식별에 대한 탐지 규칙(사용자 지정 DLP 정책만 해당), 17-14페이지
- ID 번호 식별을 위한 정규식, 17-14페이지
- 민감한 DLP 용어의 사용자 지정 사전 사용(사용자 지정 DLP 정책만 해당), 17-15페이지
- 의심되는 위반에 대한 위험 계수의 결정자, 17-17페이지
- 사용자 지정 콘텐츠 분류자가 사용되는 정책 보기, 17-18페이지

콘텐츠 일치 분류자 예

다음 예는 분류자와 메시지 콘텐츠가 어떻게 일치하는지 보여줍니다.

신용 카드 번호

여러 DLP 정책 템플릿은 신용 카드 번호 분류자를 포함합니다. 신용 카드 번호 자체는 숫자 및 구두점 패턴, 발급자 특정 접두사 및 최종 검사 숫자 등 다양한 제한의 대상이 됩니다. 분류자는 보조 신용 카드 번호, 만료 날짜 또는 카드 발급자 이름 등 일치시킬 추가 지원 정보가 필요합니다. 이를 통해 긍정 오류가 감소합니다.

예:

- `4999-9999-9999-9996`(지원 정보가 없으므로 일치하지 않음)
- `4999-9999-9999-9996 01/09`(일치)
- `Visa 4999-9999-9999-9996`(일치)
- `4999-9999-9999-9996 4899 9999 9999 9997`(하나 이상의 신용 카드 번호로 인해 일치)

미국 사회 보장 번호

미국 사회 보장 번호 분류자에는 생년월일, 이름 또는 문자열 `SSN` 등의 지원 데이터뿐만 아니라 적절한 형식의 번호가 필요합니다.

예:

- `321-02-3456`(지원 정보가 없으므로 일치하지 않음)
- `321-02-3456 July 4`(일치)
- `321-02-3456 7/4/1980`(일치)
- `321-02-3456 7/4`(일치하지 않음)
- `321-02-3456 321-02-7654`(하나 이상의 SSN으로 인해 일치)
- `SSN: 321-02-3456`(일치)
- `Joe Smith 321-02-3456`(일치)
- `321-02-3456 CA 94066`(일치)

ABA 은행 식별 번호

ABA 은행 식별 번호 분류자는 신용 카드 번호 분류자와 유사합니다.

예:

- `119999992`(지원 정보가 없으므로 일치하지 않음)
- `routing 119999992 account 1234567`(일치)

미국 운전면허증

많은 정책에서 미국 운전면허증 분류자를 사용합니다. 기본적으로 이 분류자는 미국의 50개 주와 컬럼비아 특별구에 대해 운전면허증을 검사합니다. California AB-1298 및 Montana HB-732 등의 미국 주 특정 정책도 모든 51가지 미국 운전면허증 유형을 검색합니다. 따라서 California SB 1386 등 특정 주의 사전 정의된 DLP 정책 템플릿은 모든 주의 탐지 규칙을 사용하며 여전히 개인 정보 위반으로 간주되므로 캘리포니아가 아닌 지역의 운전면허증이 있는 데이터에 대한 DLP 위반 결과를 반환합니다.

긍정 오류 또는 어플라이언스 성능에 관해 우려된다면 **Mail Policies(메일 정책) > DLP Policy Manager**로 이동하여 **Advanced Settings(고급 설정)** 섹션의 **US Drivers Licenses(미국 운전면허증)** 링크를 클릭하여 특정 미국 주 또는 주와 상관없이 검색을 제한할 수 있습니다.

개별 상태 분류자는 해당 주의 패턴과 대조하며 해당 주 이름 또는 약어 및 추가 지원 데이터가 필요합니다.

예:

- `CA DL: C3452362`(번호의 올바른 패턴 및 지원 데이터가 있으므로 일치)
- `California DL: C3452362`(일치)
- `DL: C3452362`(충분한 지원 데이터가 없으므로 일치하지 않음)
- `California C3452362`(충분한 지원 데이터가 없으므로 일치하지 않음)
- `OR DL: C3452362`(오레곤의 잘못된 패턴이므로 일치하지 않음)
- `OR DL: 3452362`(오레곤의 올바른 패턴이므로 일치)
- `WV DL: D654321`(웨스트버지니아의 올바른 패턴이므로 일치)
- `WV DL: G6543`(웨스트버지니아의 잘못된 패턴이므로 일치하지 않음)

미국 NPI

미국 NPI 분류자는 검사 숫자가 포함된 10자리 숫자인 미국 국내 제공업체 식별자(NPI) 번호를 검사합니다.

예:

- `NPI: 3459872347`(NPI와 일치)
- `3459872347`(지원 정보가 없으므로 일치하지 않음)
- `NPI: 3459872342`(잘못된 검사 숫자로 인해 일치하지 않음)

학생 기록

사전 정의된 FERPA(Family Educational Rights and Privacy Act) DLP 정책 템플릿은 학생 기록 분류자를 사용합니다. 이를 사용자 지정된 학생 ID 번호 분류자와 결합하여 더욱 높은 정확도로 특정 학생 ID 패턴을 탐지합니다.

예:

- `Joe Smith, Class Rank: 234, Major: Chemistry Transcript`(일치)

기업 재무

사전 정의된 SOX(Sarbanes-Oxley) 정책 템플릿은 기업 재무 분류자를 사용하여 비공개 기업 재무 정보를 검색합니다.

예:

```
2009 Cisco net sales, net income, depreciation(일치)
FORM 10-Q 2009 I.R.S. Employer Identification No.(일치)
```

사용자 지정 DLP 정책에 대한 콘텐츠 일치 분류자 생성

생성한 사용자 지정 분류자는 사용자 지정 DLP 정책 생성 시 사용할 수 있는 분류자 목록에 추가됩니다.

단계	수행할 작업	정보
1단계	잠재적 DLP 위반을 식별하는 데 콘텐츠 일치 분류자를 사용하는 방법을 숙지합니다.	참조: • 콘텐츠 일치 분류자를 사용하여 허용되지 않은 콘텐츠 정의에 관한 정보, 17-10페이지 • 콘텐츠 일치 분류자 예, 17-11페이지
2단계	**Mail Policies(메일 정책) > DLP Policy Customizations(DLP 정책 사용자 지정)**를 선택한 다음 **Add Custom Classifier(사용자 지정 분류자 추가)**를 클릭합니다. 분류자 이름 및 설명을 입력합니다.	—
3단계	근접 및 최소 총 점수를 입력합니다.	의심되는 위반에 대한 위험 계수의 결정자, 17-17페이지 항목을 참조하십시오.
4단계	다음 탐지 규칙 유형 중 하나를 선택하고 관련된 콘텐츠 일치 기준을 정의합니다. • 단어 또는 구문 • 사전의 텍스트 • 정규식 • 기존 데이터 유출 방지 엔터티	참조: • 분류자 민감한 콘텐츠 식별에 대한 탐지 규칙(사용자 지정 DLP 정책만 해당), 17-14페이지 • 민감한 DLP 용어의 사용자 지정 사전 사용(사용자 지정 DLP 정책만 해당), 17-15페이지 • ID 번호 식별을 위한 정규식, 17-14페이지 중량 및 최대 점수에 대한 자세한 내용은 의심되는 위반에 대한 위험 계수의 결정자, 17-17페이지 항목을 참조하십시오.
5단계	(선택 사항) **Add Rule(규칙 추가)**을 클릭하여 추가 규칙을 추가합니다.	
6단계	여러 규칙을 포함하는 경우 규칙의**All(전부)** 또는 **Any(일부)**가 일치해야 하는지를 지정합니다.	이 설정은 규칙 섹션의 상단에서 확인할 수 있습니다.
7단계	변경사항을 제출하고 커밋합니다.	—

다음 작업

사용자 지정 DLP 정책에서 사용자 지정 콘텐츠 분류자를 사용합니다. 사용자 지정 DLP 정책 생성(고급), 17-9페이지 항목을 참조하십시오.

관련 주제

- 사용자 지정 콘텐츠 분류자가 사용되는 정책 보기, 17-18페이지

분류자 민감한 콘텐츠 식별에 대한 탐지 규칙(사용자 지정 DLP 정책만 해당)

콘텐츠 일치 분류자에는 메시지 또는 문서에서 DLP 위반을 탐지하는 규칙이 필요합니다. 분류자는 다음 중 하나 이상의 탐지 규칙을 사용할 수 있습니다.

- **단어 또는 구문**. 분류자가 살펴보게 되는 단어 및 구문 목록입니다. 쉼표나 줄바꿈으로 여러 항목을 구분합니다.
- **정규식**. 메시지 또는 첨부 파일에 대한 검색 패턴을 정의하는 정규식입니다. 또한 긍정 오류를 방지하기 위해 일치 사항에서 제외할 패턴을 정의할 수 있습니다. 자세한 내용은 ID 번호 식별을 위한 정규식, 17-14페이지 및 ID 번호 식별을 위한 정규식 예, 17-15페이지 항목을 참조하십시오.
- **사전**. 관련 단어 및 구문이 포함된 사전입니다. 어플라이언스는 RSA에서 생성한 사전을 포함하거나 자체 사전을 생성할 수 있습니다. 민감한 DLP 용어의 사용자 지정 사전 사용(사용자 지정 DLP 정책만 해당), 17-15페이지 항목을 참조하십시오.
- **엔터티**. 신용 카드 번호, 주소, 사회 보장 번호 또는 ABA 은행 식별 번호 등 민감한 데이터의 일반 유형을 식별하는 사전 정의된 패턴입니다. 엔터티에 대한 설명을 확인하려면 **Mail Policies(메일 정책) > DLP Policy Manager**로 이동하여 **Add DLP Policy(DLP 정책 추가)**, **Privacy Protection(개인 정보 보호)**, **Display Policy Descriptions(정책 설명 표시)**를 차례로 클릭합니다.

ID 번호 식별을 위한 정규식

일부 정책 템플릿에서는 하나 이상의 콘텐츠 일치 분류자를 사용자 지정해야 합니다. 여기에는 사용자 지정 계정 번호, 환자 ID 번호 또는 학생 ID 등 기밀 정보와 연결될 수 있는 ID 번호를 검색하기 위한 정규식 생성이 포함됩니다. 콘텐츠 일치 분류자에 사용되는 정규식 스타일은 **POSIX 기본 정규식**입니다.

참고 정규식은 대소문자를 구분하여 `[a-zA-Z]` 등의 대문자와 소문자를 포함해야 합니다. 특정 문자만 사용되는 경우 이에 따라 정규식을 정의할 수 있습니다.

8자리 숫자 등 패턴이 덜 구체적이면 실제 고객 번호에서 무작위 8자리 숫자를 구별하도록 추가 단어 및 구문을 검색하는 정책의 필요성이 커집니다.

분류자의 정규식 생성을 위해 다음 표를 가이드로 사용합니다.

요소	설명
정규식(abc)	정규식의 지시문 시퀀스가 문자열의 일부와 일치하는 경우 분류자의 정규식이 문자열과 일치합니다. 예를 들어 `ACC` 정규식은 `ACCOUNT` 문자열과 `ACCT`와 일치합니다.
[ ]	괄호를 사용하여 문자 집합을 표시합니다. 문자는 개별적으로 또는 범위 내에서 정의할 수 있습니다. 예를 들어 `[a-z]`는 `a~z`의 모든 소문자와 일치하고 `[a-zA-Z]`는 `A~Z`의 모든 대문자와 소문자와 일치합니다. `[xyz]`는 `x`, `y` 또는 `z` 문자와만 일치합니다.

요소	설명
백슬래시 특수 문자(\)	백슬래시 문자는 특수 문자를 *이스케이프*합니다. 따라서 `\.` 시퀀스는 오직 리터럴 마침표와 일치하고 `\$` 시퀀스는 오직 리터럴 달러 기호와 일치하며 `\^` 시퀀스는 오직 리터럴 캐럿 기호와 일치합니다. 백슬래시 문자는 또한 `\d` 등의 토큰으로 시작합니다. **참고:** 백슬래시는 구문 분석에 사용되는 특수 이스케이프 문자입니다. 따라서 백슬래시를 정규식에 포함하려면 백슬래시 *두 개*를 사용하여 구문 분석 후 하나의 "실제" 백슬래시만 남아 정규식 시스템에 전달되도록 해야 합니다.
\d	자릿수(0~9)와 일치하는 토큰입니다. 둘 이상의 자릿수와 일치시키려면 `{}`에 정수를 입력하여 숫자의 길이를 정의합니다. 예를 들어 `\d`는 오직 5 등의 단일 자릿수(55가 아님)와 일치합니다. `\d{2}`를 사용하면 55 등의 두 자릿수로 구성된 숫자(5가 아님)와 일치합니다.
반복 횟수{min,max}	이전 토큰의 반복 횟수를 나타내는 정규식 표기법이 지원됩니다. 예를 들어 "`\d{8}`"은 12345678 및 11223344와 일치하지만 8과는 일치하지 않습니다.
Or(|)	대안 또는 "or" 연산자입니다. A 및 B가 정규식인 경우 "`A|B`"는 "A" 또는 "B"와 일치하는 문자열과 일치합니다. 정규식에서 숫자 패턴을 결합하는 데 사용할 수 있습니다. 예를 들어 "`foo|bar`"는 foo 또는 bar와 일치하지만 foobar와는 일치하지 않습니다.

관련 주제

- ID 번호 식별을 위한 정규식 예, 17-15페이지

ID 번호 식별을 위한 정규식 예

ID 또는 계정 번호에 있는 숫자 및 문자의 패턴을 설명하는 단순한 정규식은 다음과 같이 표시될 수 있습니다.

- 8자리 수: `\d{8}`
- 숫자 집합 간에 하이픈이 있는 식별 코드: `\d{3}-\d{4}-\d`
- 대문자 또는 소문자의 단일 문자로 시작하는 식별 코드: `[a-zA-Z]\d{7}`
- 3자릿수로 시작하고 9개의 대문자가 이어지는 식별 코드: `\d{3}[A-Z]{9}`
- `|`를 사용하여 두 가지 다른 패턴을 검색하도록 정의: `\d{3}[A-Z]{9}|\d{2}[A-Z]{9}-\d`

민감한 DLP 용어의 사용자 지정 사전 사용(사용자 지정 DLP 정책만 해당)

AsyncOS에는 RSA Security Inc.가 제공하는 사전 정의한 사전이 제공되지만 사용자 지정 DLP 사전을 생성하여 DLP 검사 기능에 사용할 용어를 지정할 수도 있습니다.

여러 가지 방법으로 사용자 지정 DLP 사전을 생성할 수 있습니다.

- 사용자 지정 DLP 사전 직접 추가

- DLP 사전을 텍스트 파일로 생성 및 DLP 사전 가져오기
- DLP 사전 내보내기(다른 Email Security 어플라이언스에서) 및 DLP 사전 가져오기

사용자 지정 DLP 사전 직접 추가

절차

1단계 **Mail Policies(메일 정책) > DLP Policy Manager**를 선택합니다.

2단계 **Advanced Settings(고급 설정)** 섹션에서 **Custom DLP Dictionaries(사용자 지정 DLP 사전)** 옆의 링크를 클릭합니다.

3단계 **Add Dictionary(사전 추가)**를 클릭합니다.

4단계 사용자 지정 사전의 이름을 입력합니다.

5단계 새 사전 항목(단어 및 구문)을 용어 목록에 입력합니다.

사전 용어는 대소문자를 구분하며 ASCII 문자가 아닌 문자도 포함할 수 있습니다.

여러 항목을 입력하는 경우 줄바꿈을 사용하여 항목을 구분합니다.

6단계 **Add(추가)**를 클릭합니다.

7단계 변경사항을 제출하고 커밋합니다.

DLP 사전을 텍스트 파일로 생성

로컬 머신에 고유 사전을 텍스트 파일로 생성하여 어플라이언스에 가져올 수 있습니다. 사전 텍스트 파일에서 각 용어에 줄바꿈을 사용합니다. 사전 용어는 대소문자를 구분하며 ASCII 문자가 아닌 문자도 포함할 수 있습니다.

DLP 사전 내보내기

참고 사전 정의된 DLP 사전은 내보낼 수 없습니다.

절차

1단계 **Mail Policies(메일 정책) > DLP Policy Manager**를 선택합니다.

2단계 Advanced Settings(고급 설정) 아래에 있는 **Custom DLP Dictionaries(사용자 지정 DLP 사전)** 섹션의 링크를 클릭합니다.

3단계 **Export Dictionary(사전 내보내기)**를 클릭합니다.

4단계 내보내기 할 사전을 선택합니다.

5단계 사전의 파일 이름을 입력합니다.

6단계 로컬 컴퓨터 또는 어플라이언스의 구성 디렉토리에 내보낸 사전을 저장할 위치를 선택합니다.

7단계 파일에 대한 인코딩을 선택합니다.

8단계 **Submit(제출)**을 클릭하고 파일을 저장합니다.

DLP 사전 가져오기

시작하기 전에

Email Security 어플라이언스에서 DLP가 아닌 사전에서 내보낸 파일을 가져오는 경우 텍스트 파일에서 가중치 값을 먼저 삭제하고 정규식을 단어 또는 구문으로 변환해야 합니다.

절차

1단계 **Mail Policies(메일 정책) > DLP Policy Manager**를 선택합니다.

2단계 **Advanced Settings(고급 설정)** 섹션에서 **Custom DLP Dictionaries(사용자 지정 DLP 사전)** 옆의 링크를 클릭합니다.

3단계 **Import Dictionary(사전 가져오기)**를 클릭합니다.

4단계 로컬 컴퓨터 또는 어플라이언스의 구성 디렉토리에서 가져올 파일을 선택합니다.

5단계 인코딩을 선택합니다.

6단계 **Next(다음)**를 클릭합니다.

"성공" 메시지가 나타나며 가져온 사전이 Add Dictionary(사전 추가) 페이지에 표시됩니다. 프로세스가 아직 완료되지 않았습니다.

7단계 사전의 이름을 정하고 편집합니다.

8단계 **Submit(제출)**을 클릭합니다.

의심되는 위반에 대한 위험 계수의 결정자

어플라이언스에서 DLP 위반에 대한 메시지를 검사하면 위험 계수 점수를 메시지에 할당합니다. 이 점수는 메시지에 DLP 위반이 포함될 가능성을 나타냅니다. 점수 0은 메시지에 거의 확실하게 위반이 포함되지 않았음을 의미합니다. 점수 100은 메시지에 거의 확실하게 위반이 포함되어 있음을 의미합니다.

사전 정의된 템플릿을 기반으로 한 DLP 정책의 경우

사전 정의된 템플릿에서 생성된 DLP 정책에 대한 위험 계수 점수 매개변수를 확인하거나 수정할 수 없습니다. 그러나 특정 DLP 정책에 대해 너무 많은 긍정 오류가 있는 경우 해당 정책에 대한 심각도 지수를 조정할 수 있습니다. 위반 심각도 평가 정보, 17-19페이지 항목을 참조하십시오. SOX(Sarbanes-Oxley) 템플릿 등 콘텐츠 일치 분류자가 없는 템플릿을 기반으로 한 정책의 경우 메시지가 정책을 위반할 때 검사 엔진은 항상 위험 계수 값 "75"를 반환합니다.

사용자 지정 DLP 정책의 경우

사용자 지정 DLP 정책에 대해 콘텐츠 일치 분류자를 생성하는 경우 위험 계수 점수를 결정하는 데 사용되는 값을 지정합니다.

- **근접성**. 위반으로 간주하기 위해 메시지 및 첨부 파일에서 얼마나 비슷하게 일치해야 하는지를 지정합니다. 예를 들어 사회 보장 번호와 유사한 숫자 패턴이 긴 메시지 상단에 나타나고 주소가 하단에 있는 발신자의 서명에 나타나는 경우 관련 없는 것으로 간주되고 데이터는 일치하지 않은 것으로 간주됩니다.
- **최소 총 점수**. DLP 위반으로 레이블 지정된 민감한 콘텐츠에 필요한 최소 위험 계수입니다. 메시지의 일치 점수가 최소 총 점수를 만족하지 않는 경우 데이터가 민감하지 않은 데이터로 간주됩니다.

- **가중치**. 사용자 지정 규칙의 경우 규칙의 중요성을 나타내는 "가중치"를 지정합니다. 점수는 규칙의 가중치와 탐지 규칙의 수를 곱하여 얻습니다. 10의 가중치가 있는 규칙의 두 인스턴스는 20점이 반환됩니다. 하나의 규칙에서 다른 규칙보다 분류자가 중요한 경우 더 많은 가중치가 할당되어야 합니다.
- **최대 점수**. 규칙의 최대 점수는 낮은 가중치 규칙이 대량으로 일치하여 해당 검사의 최종 점수가 왜곡되지 않도록 방지합니다.

위험 계수를 계산하기 위해 분류자는 탐지 규칙과 일치하는 횟수에 규칙의 가중치를 곱합니다. 이 값이 탐지 규칙의 최대 점수를 초과하면 분류자는 최대 점수 값을 사용합니다. 분류자에 두 가지 이상의 탐지 규칙이 있는 경우 모든 탐지 규칙에 대한 점수를 단일 값으로 추가합니다. 분류자는 위험 계수를 생성하기 위해 다음 표의 대수 배율을 사용하여 10~100의 배율로 탐지 규칙 점수(10~10,000)를 매핑합니다.

표 17-1 위험 계수 점수를 탐지 규칙 점수로 계산하는 방법

규칙 점수	위험 계수
10	10
20	20
30	30
50	40
100	50
150	60
300	70
500	80
1000	90
10000	100

사용자 지정 콘텐츠 분류자가 사용되는 정책 보기

절차

1단계 **Mail Policies(메일 정책) > DLP Policy Customizations(DLP 정책 사용자 지정)**를 선택합니다.

2단계 **Custom Classifiers(사용자 지정 분류자)** 섹션에서 사용자 지정 분류자 표의 제목에 있는 **Policies(정책)** 링크를 클릭합니다.

관련 주제

- 사용자 지정 DLP 정책에 대한 콘텐츠 일치 분류자 생성, 17-13페이지

DLP 정책에 대한 메시지 필터링

성능 또는 정확성을 높이기 위해 다음 기준에 따라 특정 메시지에만 적용되도록 DLP 정책을 제한할 수 있습니다.

옵션	설명
발신자 및 수신자별 필터링	다음 중 하나를 사용하여 지정한 수신자 또는 발신자를 포함하거나 포함하지 않는 메시지에 적용하도록 DLP 정책을 제한합니다. • 전체 이메일 주소: `user@example.com` • 부분 이메일 주소: `user@` • 도메인의 모든 사용자: `@example.com` • 부분 도메인의 모든 사용자: `@.example.com` 줄바꿈 또는 쉼표를 사용하여 여러 항목을 구분합니다. AsyncOS는 먼저 발송 메시지의 수신자 또는 발신자를 발송 메일 정책과 일치시킨 다음 발신자 또는 수신자를 해당 메일 정책에 대해 활성화된 DLP 정책에 지정된 발신자 및 수신자 필터와 일치시킵니다. 예를 들어 파트너 도메인에 있는 수신자를 제외하고 정보의 특정 유형을 모든 발신자가 보내지 못하도록 할 수 있습니다. 파트너 도메인에서 모든 사용자를 제외하는 필터를 포함하여 해당 정보에 대한 DLP 정책을 설정한 다음 이 DLP 정책을 모든 발신자에게 적용되는 발송 메일 정책에 포함시킵니다.
첨부 파일 유형별 필터링	특정 첨부 파일 유형을 포함하거나 포함하지 않는 메시지만 검사하도록 DLP 정책을 제한할 수 있습니다. 첨부 파일 범주를 선택한 다음 사전 정의된 파일 유형을 선택하거나 목록에 없는 특정 파일 유형을 지정합니다. 사전 정의되지 않은 파일 유형을 지정하는 경우 AsyncOS는 첨부 파일의 확장명에 따라 파일 유형을 검사합니다. 또한 최소 파일 크기가 포함된 첨부 파일에 대한 DLP 검색을 제한할 수 있습니다.
메시지 태그별 필터링	특정 구문을 포함하는 메시지로 DLP 정책을 제한하려는 경우 구문에 대한 발송 메시지를 검색하고 사용자 지정 메시지를 해당 메시지에 삽입하도록 메시지 또는 콘텐츠 필터를 사용할 수 있습니다. 자세한 내용은 콘텐츠 필터 작업, 11-9페이지 및 9 장, "메시지 필터를 사용하여 이메일 정책 적용" 항목을 참조하십시오.

위반 심각도 평가 정보

DLP 검사 엔진에서 잠재적인 DLP 위반을 탐지하는 경우 인스턴스의 실제 DLP 위반 가능성을 나타내는 위험 계수 점수를 계산합니다. 정책은 심각도 수준(예: 낮음 또는 심각)을 결정하기 위해 해당 정책에 정의된 심각도 지수와 위험 계수 점수를 비교합니다. 심각도 수준마다 위반에 대해 수행할 작업을 지정합니다(아무런 작업이 없을 때 무시하는 경우 제외). 각 심각도 수준에 도달하는 데 필요한 위험 계수 점수를 조정할 수 있습니다.

관련 주제

- 심각도 지수 조정, 17-20페이지

심각도 지수 조정

모든 정책마다 기본 심각도 지수가 있습니다. 정책마다 이 지수를 조정할 수 있습니다.

예를 들어 기본적으로 위험 계수 점수가 90~100인 경우 해당 위반은 '심각'이라는 심각도 수준에 해당합니다. 그러나 특정 정책과 일치하는 위반의 경우 잠재적 데이터 유출에 대한 심각도를 높이고자 할 수 있습니다. 이 DLP 정책의 경우 '심각' 심각도 수준을 75~100의 위험 계수 점수를 갖는 위반으로 변경할 수 있습니다.

절차

1단계 **Mail Policies(메일 정책) > DLP Policy Manager**를 선택합니다.

2단계 편집할 정책 이름을 클릭합니다.

3단계 **Severity Settings(심각도 설정)** 섹션에서 **Edit Scale..(지수 편집..)**을 클릭합니다.

4단계 지수의 화살표를 사용하여 심각도 수준의 점수를 조정합니다.

5단계 **Done(완료)**을 클릭합니다.

6단계 심각도 지수 표에서 점수가 원하는 대로 표시되는지 확인합니다.

7단계 **Submit(제출)**을 클릭합니다.

관련 주제

- 위반 심각도 평가 정보, 17-19페이지

위반 일치에 대한 이메일 DLP 정책 순서 정렬

DLP 위반이 발송 메일 정책에서 활성화된 두 가지 이상의 DLP 정책과 일치하는 경우 목록에서 첫 번째로 일치하는 DLP 정책만 사용됩니다.

절차

1단계 DLP Policy Manager 페이지에서 **Edit Policy Order(정책 순서 편집)**를 클릭합니다.

2단계 이동할 정책의 행을 클릭하고 순서대로 새 위치에 끌어놓습니다.

3단계 정책 순서를 다시 정렬했으면 변경사항을 제출하고 커밋합니다.

DLP 정책을 발송 메일 정책과 연결

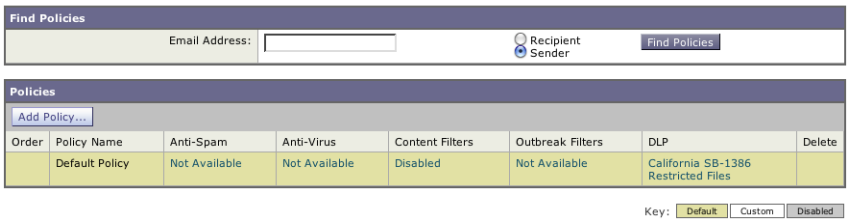
관련 주제

- DLP 정책을 기본 발송 메일 정책과 연결, 17-21페이지
- 발송 메일 정책을 사용하여 DLP 정책을 발신자 및 수신자에게 할당, 17-21페이지

DLP 정책을 기본 발송 메일 정책과 연결

기본 발송 메일 정책은 다른 발송 메일 정책이 발신자 또는 수신자와 일치하지 않는 경우 사용됩니다.

그림 17-1 DLP 정책이 활성화된 기본 발송 메일 정책



시작하기 전에

RSA 이메일 DLP를 사용한 구축에서 데이터 유출 방지를 설정하는 방법, 17-4페이지의 표에 있는 이 지점까지 모든 작업을 완료합니다. 예를 들어 기본 발송 메일 정책에 포함할 DLP 정책을 생성했는지 확인합니다.

절차

1단계 **Mail Policies(메일 정책) > Outgoing Mail Policies(발송 메일 정책)**를 선택합니다.

2단계 표의 **Default Policy(기본 정책)** 행에서 **Disabled(비활성화)** 링크(**DLP** 열)를 클릭합니다.

3단계 **Enable DLP(Customize Settings)(DLP 활성화(사용자 지정))**를 선택합니다.

4단계 기본 발송 메일 정책에 사용할 DLP 정책을 선택합니다.

5단계 변경사항을 제출하고 커밋합니다.

다음 작업

추가 발송 메일 정책에 대한 DLP 정책을 선택합니다. 발송 메일 정책을 사용하여 DLP 정책을 발신자 및 수신자에게 할당, 17-21페이지 항목을 참조하십시오.

발송 메일 정책을 사용하여 DLP 정책을 발신자 및 수신자에게 할당

발송 메일 정책에서 활성화하여 발신자 및 수신자에 적용할 DLP 정책을 지정합니다. 발송 메일 정책에서만 DLP 정책을 사용할 수 있습니다.

시작하기 전에

기본 발송 메일 정책에 사용할 DLP 정책 설정을 구성합니다. DLP 정책을 기본 발송 메일 정책과 연결, 17-21페이지 항목을 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > Outgoing Mail Policies(발송 메일 정책)**를 선택합니다.

2단계 표의 행에서 DLP 열의 링크를 클릭합니다.

3단계 이 발송 메일 정책과 연결할 DLP 정책을 선택합니다.

4단계 변경사항을 제출합니다.

5단계 기타 발송 메일 정책에 필요한 만큼 반복합니다.

6단계 변경사항을 커밋합니다.

다음 작업

RSA 이메일 DLP를 사용한 구축에서 데이터 유출 방지를 설정하는 방법, 17-4페이지 항목을 참조하십시오.

DLP 정책 편집 또는 삭제에 대한 중요 정보

작업	정보
DLP 정책 편집	정책의 이름을 변경하는 경우 발송 메일 정책에서 다시 정책을 활성화해야 합니다.
DLP 정책 삭제	정책을 삭제하는 경우 DLP 정책이 하나 이상의 발송 메일 정책에서 사용되면 알림을 받게 됩니다. DLP 정책을 삭제하면 이러한 메일 정책에서 제거됩니다.

RSA Enterprise Manager

관련 주제

- Enterprise Manager 및 Email Security 어플라이언스 상호 작용 방법, 17-22페이지
- Enterprise Manager 문서, 17-23페이지
- RSA Enterprise Manager로 구축 시 데이터 유출 방지를 설정하는 방법, 17-23페이지
- RSA 이메일 DLP에서 RSA Enterprise Manager로 마이그레이션, 17-29페이지
- Enterprise Manager에서 DLP 정책 업데이트 확인, 17-30페이지
- RSA Enterprise Manager 및 언어 지원, 17-30페이지
- 클러스터된 어플라이언스로 Enterprise Manager 사용, 17-30페이지
- Enterprise Manager 구축 시 정책 삭제 및 비활성화 정보, 17-31페이지
- Email Security 어플라이언스 및 Enterprise Manager 간 연결 해제, 17-31페이지
- Enterprise Manager에서 RSA 이메일 DLP로 전환, 17-31페이지

Enterprise Manager 및 Email Security 어플라이언스 상호 작용 방법

Email Security 어플라이언스에서 RSA Enterprise Manager DLP를 활성화하는 경우 어플라이언스는 Enterprise manager에 구성 정보를 보내며 이로써 자동으로 Email Security 어플라이언스을(를) 파트너 장치로 추가합니다. 다음 번에 Enterprise Manager를 열면 발송 메일 정책의 이름 및 메타데이터와 Email Security 어플라이언스에서 구성한 메시지 작업이 Enterprise Manager에 나타나며 DLP 정책 구성 시 사용할 수 있게 됩니다. (또는 기존 DLP 정책을 Email Security 어플라이언스에서 Enterprise Manager로 내보내기 할 수 있습니다.)

DLP 정책을 Enterprise Manager에서 구성하고 나면 Enterprise Manager는 DLP 정책을 Email Security 어플라이언스에 보냅니다. 기본적으로 Enterprise Manager에서 푸시한 모든 DLP 정책은 Email Security 어플라이언스를 비롯하여 푸시된 모든 장치에서 활성화됩니다.

Email Security 어플라이언스는 Enterprise Manager에서 받은 DLP 정책을 보관하며 발송 메시지의 위반을 검사하는 데 사용하고 발견된 위반에 대한 작업을 수행합니다. Email Security 어플라이언스는 해당하는 경우 메시지 암호화를 포함하여 전달을 위해 릴리스된 메시지를 처리합니다. Email Security 어플라이언스는 확인 및 관리를 위해 위반 정보를 Enterprise Manager에 보냅니다.

관련 주제

- 데이터 유출 방지 작동 방식, 17-2페이지
- DLP 구축 옵션, 17-3페이지

Enterprise Manager 문서

이 구축에는 RSA Inc.의 다음 문서가 필요할 수 있습니다.

- *Enterprise Manager를 활용한 파트너 장치 DLP 관리*(기술 참고). Enterprise Manager 설정 및 이를 사용한 Cisco Email Security 어플라이언스 등 파트너 장치의 DLP 기능 관리 지침.
- *RSA DLP 네트워크 9.0 배포 설명서*. 네트워크에서의 RSA DLP 소프트웨어 배포 지침.
- *RSA DLP 네트워크 9.0 사용 설명서*. Enterprise Manager를 사용하여 Cisco Email Security 어플라이언스 등의 파트너 DLP 장치를 관리하는 방법을 비롯한 RSA DLP 네트워크 소프트웨어 사용 지침.

RSA Enterprise Manager로 구축 시 데이터 유출 방지를 설정하는 방법

다음 단계를 순서대로 수행합니다.

	수행할 작업	추가 정보
1단계	네트워크에 Enterprise Manager를 설치하고 Email Security 어플라이언스와의 파트너 설정을 준비합니다.	온라인 도움말 및 기술 참고 문서 *Enterprise Manager를 활용한 파트너 장치 DLP 관리*를 비롯한 RSA의 DLP 데이터센터 문서를 참조하십시오.
2단계	Email Security 어플라이언스에서 발송 메일 정책을 생성하여 DLP 위반 검사 대상 메시지를 결정합니다. 다양한 정책을 다양한 사용자 또는 사용자 그룹에 할당할 수 있습니다.	10 장, "메일 정책" 항목을 참조하십시오. 참고: 발송 메일 정책에는 발신자를 지정할 수 있는 옵션이 있습니다. 그러나 Enterprise Manager로 구축하는 경우 이 정보는 LDAP에서 사용할 수 없습니다.
3단계	Email Security 어플라이언스에서 DLP 위반이 발견되거나 의심되는 메시지에 수행할 수 있는 작업을 정의합니다. 예를 들어 이러한 메시지를 격리할 수 있습니다.	메시지 작업, 17-32페이지
4단계	Email Security 어플라이언스 및 Enterprise Manager 간에 안전한 통신을 할 수 있도록 인증서를 획득하고 업로드합니다.	(권장) Email Security 어플라이언스 및 Enterprise Manager 간 SSL 연결에 대한 인증서 획득 및 업로드, 17-25페이지 항목을 참조하십시오.
5단계	Email Security 어플라이언스에서 ESA의 DLP 모드로 RSA Enterprise Manager를 선택하고 Email Security 어플라이언스 및 Enterprise Manager 간 연결을 구성합니다.	Enterprise Manager DLP 활성화 및 Email Security 어플라이언스 연결 구성, 17-27페이지 항목을 참조하십시오.

	수행할 작업	추가 정보
6단계	메시지 발신자의 LDAP 구분 이름을 Enterprise Manager에 제공합니다.	LDAP를 사용하여 Enterprise Manager의 메시지 발신자 식별, 17-28페이지
7단계	Email Security 어플라이언스에서 RSA 이메일 DLP 정책을 내보내고 Enterprise Manager로 가져오려면 지금 수행합니다.	Email Security 어플라이언스에서 RSA 이메일 DLP 정책을 내보내려면 Email Security 어플라이언스에서 DLP 정책 내보내기, 17-29페이지 항목을 참조하십시오. 정책을 가져오려면 RSA Enterprise Manager 문서를 참조하십시오.
8단계	Enterprise Manager에서 DLP 정책을 생성하여 다음을 수행합니다. • 위반으로 간주되는 콘텐츠 유형 식별 • 각 위반에 대해 수행할 작업 지정	온라인 도움말 및 기술 참고 문서 *Enterprise Manager를 활용한 파트너 장치 DLP 관리*를 비롯한 RSA의 DLP 데이터센터 문서에서 DLP 정책 생성에 관한 지침을 참조하십시오.
9단계	Enterprise Manager에서 발송 메일 정책을 DLP 정책과 연결하여 발신자 및 수신자에 적용할 DLP 정책을 지정합니다.	Enterprise Manager 구축 시 발송 메일 정책과 DLP 정책 연결 정보, 17-29페이지 항목을 참조하십시오.
10단계	Enterprise Manager에서 DLP 정책 순서를 지정합니다. 어플라이언스가 메시지의 DLP 위반을 평가하는 경우 목록에서 첫 번째로 일치하는 정책만 적용합니다.	Enterprise Manager에서 DLP 정책의 순서를 지정합니다. RSA Enterprise Manager 문서를 참조하십시오.
11단계	Email Security 어플라이언스의 메시지 추적에서 민감한 DLP 정보의 저장소 및 액세스에 대한 설정을 구성합니다.	• 메시지 추적 시 민감한 DLP 데이터 표시 또는 숨기기, 17-36페이지 • 메시지 추적 시 중요 정보의 액세스 제어, 32-5페이지

관련 주제

- 핑거프린팅, 17-24페이지
- (권장) Email Security 어플라이언스 및 Enterprise Manager 간 SSL 연결에 대한 인증서 획득 및 업로드, 17-25페이지
- Enterprise Manager DLP 활성화 및 Email Security 어플라이언스 연결 구성, 17-27페이지
- LDAP를 사용하여 Enterprise Manager의 메시지 발신자 식별, 17-28페이지
- Enterprise Manager 구축 시 발송 메일 정책과 DLP 정책 연결 정보, 17-29페이지

핑거프린팅

Enterprise Manager 구축에 RSA의 DLP 데이터센터가 포함되는 경우 핑거프린팅을 활성화할 수 있습니다.

핑거프린팅은 소스 코드와 다음을 비롯한 민감한 문서 탐지 기능을 향상합니다.

- 데이터베이스
- 전체 또는 일부 텍스트가 문서 텍스트에서 일치
- 파일이 비트별로 정확하게 일치하는 전체 2진 일치

핑거프린팅을 활성화하는 경우 Enterprise Manager에서 핑거프린팅 탐지 정보를 Email Security 어플라이언스에 보내고, Email Security 어플라이언스는 메시지의 데이터 유출 방지에 대해 검사할 때 이 정보를 사용합니다.

핑거프린팅에 관한 자세한 내용은 Enterprise Manager 문서를 참조하십시오.

관련 주제

- Enterprise Manager DLP 활성화 및 Email Security 어플라이언스 연결 구성, 17-27페이지

(권장) Email Security 어플라이언스 및 Enterprise Manager 간 SSL 연결에 대한 인증서 획득 및 업로드

Email Security 어플라이언스 및 Enterprise Manager 간 SSL 연결을 사용하려면 알려진 인증 기관으로부터 하나 이상의 인증서 및 서명 키를사용하여 두 머신 간 상호 인증을 수행할 수 있습니다.

SSL 연결을 구성하는 경우 Enterprise Manager 서버가 서버이며 Email Security 어플라이언스가 클라이언트입니다.

다음 모든 절차를 완료합니다.

- RSA의 인증서 도구를 사용하여 클라이언트 및 서버 인증서 생성, 17-25페이지
- 인증서를 Email Security 어플라이언스에 업로드, 17-26페이지
- 사용자 지정 인증 기관 파일을 Email Security 어플라이언스에 업로드, 17-27페이지
- Email Security 어플라이언스에서 Enterprise Manager에 대한 인증서 생성, 17-27페이지
- SSL 구성 완료, 17-27페이지

RSA의 인증서 도구를 사용하여 클라이언트 및 서버 인증서 생성

RSA는 연결에서 서버 및 클라이언트 인증서로 사용할 수 있는 단일 p.12 파일을 생성하는 데 사용할 수 있는 인증서 생성 도구를 제공합니다. 어플라이언스 및 Enterprise Manager 서버에 다양한 인증서를 사용하려면 다른 소스에서 인증서를 가져와야 합니다.

이 도구는 Enterprise Manager 서버에서 파일 두 개(.p12 인증서 파일 및 .pem 인증서 파일)를 생성하고 보관합니다. .p12 파일을 사용하는 경우에도 Email Security 어플라이언스에 .pem 파일을 인증 기관 목록으로 가져와야 합니다.

자세한 내용은 RSA 문서를 참조하십시오.

절차

1단계 Enterprise Manager 서버에서 명령 프롬프트를 엽니다.

2단계 `C:\Program Files\RSA\Enterprise Manager\etc`로 경로를 변경합니다.

3단계 다음 명령을 실행합니다.

```
"%JAVA_HOME%/bin/java" -cp ./emcerttool.jar
com.rsa.dlp.tem.X509CertGenerator -clientservercasigned -cacn <NAME OF CAPROVIDED DURING INSTALL> -cakeystore catem-keystore -castorepass <PASSWORD FOR CA PROVIDED DURING INSTALL>  -cn <DEVICE_CN> -storepass <DEVICE STORE PASSWORD> -keystore <NAME OF DEVICE STORE>
```

참고 인증서의 공용 이름은 Email Security 어플라이언스의 호스트 이름을 사용해야 합니다.

Enterprise Manager가 그룹 또는 클러스터 수준에서 연결된 Email Security 어플라이언스를 관리하는 경우 각 어플라이언스에는 해당 어플라이언스의 호스트 이름과 일치하는 공용 이름이 포함된 인증서가 필요합니다.

샘플 명령은 다음과 같이 표시될 수 있습니다.

```
"%JAVA_HOME%/bin/java" -cp ./emcerttool.jar
com.rsa.dlp.tem.X509CertGenerator -clientservercasigned -cacn emc-cisco
-cakeystore catem-keystore -castorepass esaem -cn ironport -storepass esaem
-keystore device-store
```

또한 다음 추가 명령줄 스위치를 사용할 수 있습니다.

```
-org <value in double quotes if it contains space>
-orgunit <value in double quotes if it contains space>
-title <value in double quotes if it contains space>
-validity <number of days>
```

이 절차는 <device-store>.p12 파일을 동일한 폴더에 출력합니다.

이 .p12 파일은 Email Security 어플라이언스에 업로드할 인증서입니다.

다음 사항도 필요합니다.

- Email Security 어플라이언스에서 사용자 지정 인증 기관 목록으로 가져올 이 폴더의 .pem 파일.
- 장치 저장소에 비밀번호 입력.

인증서를 Email Security 어플라이언스에 업로드

시작하기 전에

.p12 인증서 파일을 생성합니다. RSA의 인증서 도구를 사용하여 클라이언트 및 서버 인증서 생성, 17-25페이지의 절차를 사용할 수 있습니다.

절차

1단계 **Network(네트워크) > Certificates(인증서)**를 선택합니다.

2단계 **Add Certificate(인증서 추가)**를 클릭합니다.

3단계 **Import Certificate(인증서 가져오기)** 옵션을 선택합니다.

4단계 네트워크 또는 로컬 머신에 있는 인증서 파일에 대한 경로를 입력합니다.

5단계 파일의 비밀번호를 입력합니다.

6단계 **Next(다음)**를 클릭하여 인증서 정보를 확인합니다.

7단계 인증서의 이름을 입력합니다. Email Security 어플라이언스는 기본적으로 공용 이름을 할당합니다.

Enterprise Manager가 그룹 또는 클러스터 수준에서 연결된 Email Security 어플라이언스를 관리하는 경우 각 인증서의 공용 이름이 클러스터의 각 컴퓨터를 대상으로 하더라도 모든 인증서에는 동일한 인증서 이름을 사용해야 합니다.

8단계 변경사항을 제출하고 커밋합니다.

사용자 지정 인증 기관 파일을 Email Security 어플라이언스에 업로드

시작하기 전에

인증 기관 파일을 가져옵니다. RSA의 인증서 도구를 사용하여 클라이언트 및 서버 인증서 생성, 17-25페이지의 절차를 사용하여 인증서를 생성한 경우 이는 .p12 인증서 파일과 동일한 폴더에 있는 .pem 파일입니다.

절차

1단계 **Network(네트워크) > Certificates(인증서)**를 선택합니다.

2단계 Certificate Authorities(인증 기관) 섹션에서 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 Custom List(사용자 지정 목록)의 **Enable(활성화)**을 클릭합니다.

4단계 로컬 또는 네트워크 컴퓨터의 사용자 지정 목록(.pem 파일)의 전체 경로를 입력합니다.

5단계 변경사항을 제출하고 커밋합니다.

Email Security 어플라이언스에서 Enterprise Manager에 대한 인증서 생성

클라이언트 및 서버에 동일한 인증서를 사용하지 않으려면 Email Security 어플라이언스에서 자체 서명된 인증서를 생성하여 Enterprise Manager에 업로드할 수 있습니다. GUI를 사용하여 자체 서명된 인증서 생성, 23-3페이지 항목을 참조하십시오.

SSL 구성 완료

"Enterprise Manager DLP 활성화 및 Email Security 어플라이언스 연결 구성, 17-27페이지"에서와 같이 SSL 구성을 완료합니다.

Enterprise Manager DLP 활성화 및 Email Security 어플라이언스 연결 구성

시작하기 전에

- RSA Enterprise Manager로 구축 시 데이터 유출 방지를 설정하는 방법, 17-23페이지의 표에서와 같이 이 단계 전에 모든 단계를 완료합니다.
- 구축에 RSA의 DLP 데이터센터가 포함되는 경우 핑거프린팅을 활성화할 수 있습니다. 자세한 내용은 핑거프린팅, 17-24페이지 항목을 참조하십시오.

절차

1단계 Email Security 어플라이언스에서 **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)**를 선택합니다.

2단계 이전에 데이터 유출 방지 기능을 활성화한 경우 **Edit Settings(설정 편집)**를 클릭한 다음 5단계로 건너뜁니다.

3단계 **Enable(활성화)**을 클릭합니다.

4단계 라이센스 계약 페이지 하단으로 스크롤하여 **Accept(동의)**를 클릭하여 계약에 동의합니다.

참고 라이센스 계약에 동의하지 않는 경우 데이터 유출 방지 기능은 어플라이언스에서 활성화되지 않습니다.

5단계 Data Loss Prevention(데이터 유출 방지)에서 **RSA Enterprise Manager**를 선택합니다.

6단계 DLP 정책과 포트 번호 20000을 관리하는 데 사용하려는 네트워크에서 Enterprise Manager 서버의 호스트 이름을 입력합니다. 콜론(:)을 사용하여 호스트 이름 및 포트 번호를 구분합니다.

7단계 Email Security 어플라이언스와 Enterprise Manager 간에 SSL 연결을 사용하려면,

a. **Enable SSL Communication(SSL 통신 활성화)** 확인란을 선택합니다.

b. 서버 인증서를 선택합니다. 서버는 Enterprise Manager입니다.

c. 클라이언트 인증서를 선택합니다. 클라이언트는 Email Security 어플라이언스입니다.

클라이언트 및 서버에 동일한 인증서를 사용할 수 있습니다.

8단계 (선택 사항) 구축에 RSA의 DLP 데이터센터가 포함되는 경우 핑거프린팅을 활성화하여 소스 코드, 데이터베이스 및 기타 문서의 탐지 기능을 높일지 여부를 선택합니다.

9단계 (선택 사항) 메시지 추적 기능이 이미 어플라이언스에서 활성화되어 있는 경우 일치된 콘텐츠의 로깅 여부를 선택합니다.

로깅을 선택하는 경우 Email Security 어플라이언스가 DLP 위반 내용을 기록하고 AsyncOS가 신용카드 번호 및 사회 보장 번호 등 민감한 데이터를 비롯하여 메시지 추적에서 얻은 DLP 위반 결과 및 주변 콘텐츠를 표시합니다.

10단계 어플라이언스가 자동으로 업데이트 내용을 DLP 엔진에 다운로드하도록 활성화하지 않도록 합니다.

11단계 변경사항을 제출하고 커밋합니다.

Email Security 어플라이언스는 Enterprise manager에 구성 정보를 보내며 이로써 자동으로 어플라이언스를 파트너 장치로 추가합니다.

LDAP를 사용하여 Enterprise Manager의 메시지 발신자 식별

Email Security 어플라이언스에서 DLP 인시던트 데이터를 Enterprise Manager에 보내는 경우 어플라이언스는 메시지 발신자를 식별하도록 전체 LDAP 고유 이름을 포함해야 합니다. 어플라이언스는 이 정보를 LDAP 서버에서 검색합니다.

시작하기 전에

- RSA Enterprise Manager로 구축 시 데이터 유출 방지를 설정하는 방법, 17-23페이지의 표에 있는 이 지점까지 모든 단계를 완료합니다. 이러한 지침을 따르지 않으면 사용자 고유 이름 쿼리 옵션을 사용할 수 없습니다.
- Email Security 어플라이언스에서 LDAP 서버 프로파일을 생성합니다. 자세한 내용은 25 장, "LDAP 쿼리" 항목을 참조하십시오.
- 기본 쿼리를 사용하지 않는 경우 전체 고유 이름을 검색하기 위해 어플라이언스에서 사용할 쿼리 문자열을 생성합니다. Active Directory 서버의 경우 기본 쿼리 문자열은 `(proxyAddresses=smtp:{a})`입니다. OpenLDAP 서버의 경우 기본 쿼리 문자열은 `(mail={a})`입니다. 쉼표로 구분된 여러 특성을 비롯하여 고유 쿼리 및 이메일 속성을 정의할 수 있습니다.

절차

1단계	Email Security 어플라이언스에서 **System Administration(시스템 관리) > LDAP**를 선택합니다.
2단계	사용하려는 LDAP 서버의 프로파일을 편집합니다.
3단계	**User Distinguished Name Query(사용자 고유 이름 쿼리)**의 확인란을 선택합니다. 이 옵션은 RSA Enterprise manager를 DLP 구축 옵션으로 선택한 경우에만 사용할 수 있습니다.
4단계	쿼리의 이름을 입력합니다.
5단계	사용자 고유 이름을 검색하기 위한 쿼리 문자열을 입력합니다.
6단계	쿼리를 테스트하려면 버튼을 클릭합니다.
7단계	변경사항을 제출하고 커밋합니다.

Enterprise Manager 구축 시 발송 메일 정책과 DLP 정책 연결 정보

발신자 및 수신자에 적용할 DLP 정책을 지정하기 위해 Enterprise Manager를 사용하여 발송 메일 정책을 DLP 정책과 연결합니다. 자세한 내용은 RSA Enterprise Manager 문서를 참조하십시오. Enterprise Manager는 메시지를 검사할 때 사용하기 위해 Email Security 어플라이언스에 이 정보를 보냅니다.

RSA 이메일 DLP와는 달리 발송 메일 정책은 Enterprise Manager가 활성화된 경우 기본 메일 정책의 DLP 설정을 사용할 수 없습니다. 메일 정책이 Enterprise Manager의 DLP 정책에 지정되지 않은 경우 DLP 검사가 메일 정책에 활성화되지 않습니다.

RSA 이메일 DLP에서 RSA Enterprise Manager로 마이그레이션

기존의 RSA 이메일 DLP 구성을 RSA Enterprise Manager로 마이그레이션하려는 경우 어플라이언스를 RSA 이메일 DLP 모드에서 RSA Enterprise Manager 모드로 전환하기 전에 Enterprise Manager에 업로드할 수 있는 .zip 파일로 DLP 구성을 내보낼 수 있습니다.

Email Security 어플라이언스는 Enterprise Manager에서 첫 DLP 정책 패키지를 받을 때까지 기존의 로컬 RSA 이메일 DLP 정책을 사용합니다.

이후에 RSA 이메일 DLP 모드로 전환하는 경우 Email Security 어플라이언스는 기존의 RSA 이메일 DLP 정책을 저장합니다.

관련 주제

- Email Security 어플라이언스에서 DLP 정책 내보내기, 17-29페이지
- RSA Enterprise Manager로 구축 시 데이터 유출 방지를 설정하는 방법, 17-23페이지

Email Security 어플라이언스에서 DLP 정책 내보내기

Email Security 어플라이언스에서 DLP 정책 구성을 .zip 파일로 내보낸 다음 Enterprise Manager로 가져올 수 있습니다.

DLP 구축 모드로 RSA 이메일 DLP 또는 RSA Enterprise Manager 중 어떤 것을 선택하더라도 DLP 정책을 내보낼 수 있습니다.

절차

1단계 **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)**를 선택합니다.

2단계 **Export DLP Configuration(DLP 구성 내보내기)**을 클릭합니다.

3단계 .zip 파일의 이름을 입력하고 **Export(내보내기)**를 클릭합니다.

비활성화된 DLP 정책 및 발송 메일 정책에 할당되지 않은 DLP 정책은 포함되지 않습니다.

참고 Email Security 어플라이언스가 클러스터에 속해 있는 경우 어플라이언스는 가장 낮은 클러스터 수준에서만 정책을 내보냅니다. 예를 들어 클러스터 및 머신 수준 모두에 DLP 정책이 있는 경우 어플라이언스는 머신 수준에서만 DLP 정책을 내보냅니다.

다음 작업

DLP 정책을 Enterprise Manager로 가져오고 관리되는 어플라이언스에 배포하는 방법에 대한 자세한 내용은 Enterprise Manager 문서를 참조하십시오.

Enterprise Manager에서 DLP 정책 업데이트 확인

Enterprise Manager는 주기적으로 Email Security 어플라이언스에서 DLP 정책을 업데이트합니다.

Enterprise Manager에서 최신 DLP 정책 업데이트를 확인하려면 **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)**로 이동합니다.

관련 주제

- Email Security 어플라이언스 및 Enterprise Manager 간 연결 해제, 17-31페이지

RSA Enterprise Manager 및 언어 지원

Email Security 어플라이언스는 Enterprise Manager에서 사용된 언어로 RSA Enterprise Manager에서 받은 모든 데이터를 표시합니다. 어플라이언스는 어플라이언스 인터페이스에서 선택한 언어로 이 정보를 표시하지 않습니다. 이는 DLP 정책, 콘텐츠 일치 분류자, 사전 및 어플라이언스가 데이터 패키지에서 받는 Enterprise Manager에서 생성된 모든 항목에 적용됩니다. 예를 들어 Enterprise Manager의 DLP 정책 및 분류자가 영어로 작성되었지만 Email Security 어플라이언스의 인터페이스가 프랑스어로 표시되는 경우 Email Security 어플라이언스는 Enterprise Manager의 DLP 정책 및 분류자 이름 및 설명을 영어로 표시합니다. 인터페이스의 나머지에서는 프랑스어가 표시됩니다.

클러스터된 어플라이언스로 Enterprise Manager 사용

Enterprise Manager를 사용하여 클러스터된 Email Security 어플라이언스의 DLP 정책을 관리하는 경우 다음 사항에 유의해야 합니다.

- Email Security 어플라이언스는 이러한 설정이 구성된 가장 낮은 클러스터 수준에서 Enterprise Manager에 발송 메일 정책 및 메시지 작업을 보냅니다. 이러한 설정이 클러스터 및 머신 수준에서 다르게 구성되는 경우 Email Security 어플라이언스는 Enterprise Manager에 머신 수준의 설정을 보냅니다. 높은 클러스터 수준에서 구성된 발송 메일 정책 및 메시지 작업을 사용하려는 경우 사용하지 않으려는 낮은 수준에서 지정된 정책 및 작업을 삭제합니다.

- Email Security 어플라이언스에서는 이 설정이 구성된 가장 낮은 클러스터 수준에서 지정된 데이터 유출 방지 모드를 사용합니다. 예를 들어 클러스터된 어플라이언스가 머신 수준에서 로컬 RSA 이메일 DLP 모드를 사용하고 클러스터 수준에서 RSA Enterprise Manager를 사용하도록 구성된 경우 어플라이언스는 데이터 유출 방지에 RSA 이메일 DLP를 사용하고 Enterprise Manager와 통신하지 않습니다.

Enterprise Manager 구축 시 정책 삭제 및 비활성화 정보

DLP 정책 삭제 및 비활성화

- DLP 정책을 삭제하려면 Enterprise Manager를 사용합니다.
- DLP 정책을 비활성화하거나 활성화하려면 Email Security 어플라이언스를 사용합니다. **Mail Policies(메일 정책) > DLP Policy Manager**로 이동합니다.

  비활성화된 DLP 정책과 연결된 모든 발송 메일 정책은 메시지의 DLP 위반을 평가할 때 해당 정책을 건너뜁니다.

발송 메일 정책 삭제

DLP 정책에 연결된 발송 메일 정책을 삭제하려는 경우 Email Security 어플라이언스는 메일 정책이 현재 사용 중이라는 메시지 경고를 표시합니다. 그래도 정책을 삭제하는 경우 Enterprise Manager는 삭제된 발송 메일 정책과 이를 사용하는 DLP 정책의 연결을 자동으로 해제합니다. 삭제된 메일 정책 구성에 따라 메시지를 검사하지 않는 것 외에도 DLP 검사는 예전처럼 계속 작동됩니다. Enterprise Manager에서 Email Security 어플라이언스에 보낸 다음 DLP 정책 패키지는 삭제된 메일 정책과 관련된 항목을 포함하지 않습니다.

Email Security 어플라이언스 및 Enterprise Manager 간 연결 해제

Email Security 어플라이언스와 Enterprise manager 간 연결이 해제된 경우 어플라이언스 및 Enterprise Manager가 보낼 수 없는 모든 데이터가 연결이 복원될 때까지 전달을 위해 큐에 대기됩니다. Email Security 어플라이언스의 경우 DLP 위반 가능성이 있는 메시지의 모든 데이터가 큐 대기 상태임을 의미합니다. Enterprise Manager의 경우 새 DLP 정책 정보가 포함된 데이터 패키지가 큐 대기 상태임을 의미합니다. Email Security 어플라이언스가 Enterprise Manager에서 업데이트된 DLP 정책 데이터를 받지 못하는 경우 어플라이언스는 이전에 Enterprise Manager에서 받은 DLP 정책을 계속 사용합니다.

관련 주제

- Enterprise Manager에서 Email Security 어플라이언스 연결 해제, 17-40페이지

Enterprise Manager에서 RSA 이메일 DLP로 전환

RSA Enterprise Manager를 사용한 후 데이터 유출 방지를 위해 다시 RSA 이메일 DLP를 사용하려는 경우 데이터 유출 방지 활성화(RSA 이메일 DLP), 17-5페이지 항목을 참조하십시오.

Email Security 어플라이언스는 RSA Enterprise Manager 모드를 사용하도록 구성하기 전에 사용된 RSA 이메일 DLP 정책으로 다시 자동 전환됩니다. RSA 이메일 DLP 모드였을 때 어플라이언스가 로컬 DLP 정책을 사용하지 않은 경우 어플라이언스는 로컬 DLP 정책을 생성할 때까지 Enterprise Manager에서 DLP 정책을 계속 사용합니다.

Enterprise Manager의 정책과 유사한 로컬 DLP 정책을 사용하려는 경우 DLP Policy Manager를 사용하여 다시 생성할 수 있습니다. Email Security 어플라이언스는 Enterprise Manager에서 사용한 정책을 기반으로 새 정책을 자동으로 생성하고 Enterprise manager에서는 가져올 수 없습니다.

DLP Policy Manager를 사용하여 DLP 정책을 생성하는 방법에 대한 자세한 내용은 DLP 정책(RSA 이메일 DLP용), 17-5페이지 항목을 참조하십시오.

Enterprise Manager에서 파트너 장치로서의 Email Security 어플라이언스를 제거하는 방법에 대한 자세한 내용은 RSA Enterprise Manager 문서를 참조하십시오.

메시지 작업

발송 메시지에서 가능한 DLP 위반을 탐지하는 경우 Email Security 어플라이언스에서 수행할 1차 및 2차 작업을 지정합니다. 다양한 위반 유형 및 심각도에 다양한 작업을 할당할 수 있습니다.

1차 작업에는 다음이 포함됩니다.

- 전달
- 삭제
- 격리

2차 작업에는 다음이 포함됩니다.

- 메시지 전달을 선택하는 경우 정책 격리에 복사본 전송. 이 복사본은 메시지 ID를 포함한 원본의 완벽한 복제본입니다. 복사본을 격리하면 DLP 위반을 모니터링하는 다른 방법을 제공하는 것 외에도 구축하기 전 RSA 이메일 DLP 시스템을 테스트할 수 있습니다. 격리에서 복사본을 릴리스하면 어플라이언스에서 이미 원본 메시지를 받은 수신자에게 복사본을 전송합니다.
- 메시지 암호화. 어플라이언스는 메시지 본문만 암호화합니다. 메시지 헤더를 암호화하지는 않습니다.
- DLP를 위반한 메시지 제목 헤더 변경.
- 메시지에 고지 사항 텍스트 추가.
- 대체 대상 메일 호스트에 메시지 전송.
- 다른 수신자에게 메시지 사본(Bcc) 전송. (예를 들어 검사를 위해 심각한 DLP 위반이 포함된 메시지를 준수 관리자의 사서함에 복사할 수 있습니다.)
- DLP 위반 알림 메시지를 발신자 또는 관리자나 DLP 준수 관리자 등의 다른 문의처에 전송. DLP 알림 초안 작성, 17-34페이지 항목을 참조하십시오.

참고 이러한 작업은 함께 처리될 수 있습니다. 여러 사용자 그룹의 여러 가지 처리 요구 사항에 따라 여러 DLP 정책에서 일부를 결합하여 사용할 수 있습니다. 또한 동일한 정책에서 다양한 심각도 수준에 따라 다양하게 처리하도록 구성할 수 있습니다. 예를 들어 심각한 DLP 위반이 있는 메시지를 격리하고 알림을 준수 관리자에게 보낼 수 있지만 낮은 심각도 수준의 메시지를 전송하고자 할 수 있습니다.

관련 주제

- DLP 위반 시 수행할 작업 정의(메시지 작업), 17-33페이지
- 메시지 작업 확인 및 편집, 17-34페이지
- DLP 알림 초안 작성, 17-34페이지

DLP 위반 시 수행할 작업 정의(메시지 작업)

시작하기 전에

- 하나 이상의 전용 격리를 생성하여 DLP 정책을 위반하는 메시지(또는 메시지 복사본)를 보관합니다.

  이를 위해 Email Security 어플라이언스의 로컬 격리 또는 보안 관리 어플라이언스의 중앙 집중식 격리를 사용할 수 있습니다.

  Enterprise Manager를 사용한 구축:

  - Enterprise가 작업을 완료할 수 있도록 충분한 시간 제한을 설정합니다.
  - 자동 작업을 신중하게 고려합니다. Enterprise Manager에서 격리된 메시지를 관리해야 하더라도 Email Security 어플라이언스는 격리 작업이 할당된 공간을 초과할 때 격리된 메시지를 계속 릴리스하거나 삭제합니다.

  자세한 내용은 30 장, "정책, 바이러스 및 신종 바이러스 격리" 항목을 참조하십시오.
- 전달하기 전에 메시지를 암호화하려면 암호화 프로파일을 설정했는지 확인합니다. 18 장, "Cisco 이메일 암호화" 항목을 참조하십시오.
- DLP 위반 또는 의심되는 위반이 포함된 메시지를 전달할 때 고지 사항 텍스트를 포함하려면 **Mail Policies(메일 정책) > Text Resources(텍스트 리소스)**에서 고지 사항 텍스트를 지정합니다. 자세한 내용은 고지 사항 템플릿, 21-12페이지 항목을 참조하십시오.
- 알림을 DLP 위반 발신자 또는 준수 관리자 등의 다른 사람에게 보내려면 먼저 DLP 알림 템플릿을 생성합니다. DLP 알림 초안 작성, 17-34페이지 항목을 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > DLP Policy Customizations(DLP 정책 사용자 지정)**를 선택합니다.

2단계 **Message Actions(메시지 작업)** 섹션에서 **Add Message Action(메시지 작업 추가)**을 클릭합니다.

3단계 메시지 작업의 이름을 입력합니다.

4단계 메시지 작업의 설명을 입력합니다.

5단계 DLP를 위반한 메시지를 삭제, 전송 또는 격리할지를 선택합니다.

참고 Deliver(전달)를 선택하면 정책 격리에 보낸 메시지 복사본을 저장하도록 선택할 수 있습니다. 메시지의 복사본은 메시지 ID를 포함한 완벽한 복제본입니다.

6단계 전달 또는 격리에서 릴리스할 때 메시지를 암호화하려는 경우 **Enable Encryption(암호화 활성화)** 확인란을 선택하고 다음 옵션을 선택합니다.

- **Encryption Rule(암호화 규칙)**. 항상 메시지를 암호화하거나 TLS 연결을 통해 보내려는 시도가 처음 실패할 경우에만 암호화합니다.
- **Encryption Profile(암호화 프로파일)**. 지정된 암호화 프로파일을 사용하여 메시지를 암호화하고 Cisco IronPort 암호화 어플라이언스 또는 호스팅 키 서비스를 사용하는 경우 이를 전달합니다.
- **Encrypted Message Subject(암호화된 메시지 제목)**. 암호화된 메시지의 제목입니다. `$Subject` 값을 사용하여 기존 메시지 제목을 유지합니다.

7단계 작업으로 격리를 선택하는 경우 DLP를 위반한 메시지에 사용하려는 정책 격리를 선택합니다.

8단계 다음 옵션 중 하나를 사용하여 메시지를 수정하려면 **Advanced(고급)**를 클릭합니다.

- 사용자 지정 헤더 추가
- 메시지 제목 수정
- 대체 호스트에 전달
- 다른 수신자에게 사본(Bcc) 전송
- DLP 알림 메시지 전송

9단계 변경사항을 제출하고 커밋합니다.

메시지 작업 확인 및 편집

절차

1단계 **Mail Policies(메일 정책) > DLP Policy Customizations(DLP 정책 사용자 지정)**를 선택합니다.

2단계 **Message Actions(메시지 작업)** 섹션에서 작업을 선택합니다.

변경 후	수행할 작업
각 작업이 할당되는 메일 정책 확인	메시지 작업 표의 제목에서 **Policies(정책)** 링크를 클릭합니다.
각 작업마다 입력한 설명 확인	메시지 작업 표의 제목에서 **Description(설명)** 링크를 클릭합니다.
메시지 작업의 세부사항 확인 또는 편집	메시지 작업의 이름을 클릭합니다.
메시지 작업 삭제	삭제하려는 메시지 작업 옆의 휴지통 아이콘을 클릭합니다. 확인 메시지는 메시지 작업이 하나 이상의 DLP 정책에 사용되는지 여부를 알려줍니다.
메시지 작업 복제 변경하기 전에 이 기능을 사용하여 메시지 작업의 백업 복사본을 생성하거나 유사한 새 메시지 작업의 시작 지점으로 사용할 수 있습니다.	복제하려는 메시지 작업 옆의 **Duplicate(복제)** 아이콘을 클릭합니다.

3단계 변경사항을 제출하고 커밋합니다.

DLP 알림 초안 작성

이메일 메시지에 조직의 데이터 유출 방지 정책을 위반하는 정보가 포함되는 경우 이 절차를 사용하여 보낼 알림에 대한 템플릿을 생성합니다. 이 알림을 DLP 정책을 위반한 메시지의 발신자 또는 다른 주소(예: 관리자 또는 DLP 준수 관리자)에 보낼 수 있습니다.

시작하기 전에

- RSA Enterprise Manager를 사용한 구축: Email Security 어플라이언스(메시지 작업 페이지) 또는 Enterprise Manager(DLP 정책)를 구성하여 DLP 위반 알림을 사용자에게 보낼 수 있습니다. 중복 알림을 방지하려면 두 가지 방식 중 하나(둘 모두는 안 됨)를 사용하여 알림을 설정합니다.
- DLP 알림 템플릿 변수 정의, 17-35페이지의 내용을 숙지합니다. 이러한 변수를 사용하여 각 위반에 대한 특정 세부사항을 지정하여 알림을 사용자 지정할 수 있습니다.

절차

1단계 **Mail Policies(메일 정책) > Text Resources(텍스트 리소스)**를 선택합니다.

2단계 **Add Text Resource(텍스트 리소스 추가)**를 클릭합니다.

3단계 **유형**을 위해서는 **DLP Notification Template(DLP 알림 템플릿)**을 선택합니다.

DLP 변수는 일반 알림 템플릿에 사용할 수 없습니다.

4단계 알림 텍스트 및 변수를 입력합니다.

알림을 통해 발송 메시지에 조직의 데이터 유출 방지 정책을 위반하는 민감한 데이터가 포함되어 있음을 수신자에게 알려야 합니다.

다음 작업

이 DLP 알림 템플릿을 DLP Policy Manager의 DLP 정책에 있는 메시지 작업에서 지정합니다.

관련 주제

- DLP 알림 템플릿 변수 정의, 17-35페이지

DLP 알림 템플릿 변수 정의

다음 변수를 사용하여 각 DLP 위반에 대한 특정 정보를 알림에 포함합니다.

변수	다음으로 대체됨
$DLPPolicy	위반된 이메일 DLP 정책의 이름으로 대체됩니다.
$DLPSeverity	위반의 심각도로 대체됩니다. "낮음", "중간", "높음" 또는 "심각"이 사용됩니다.
$DLPRiskFactor	메시지의 민감한 자료에 대한 위험 계수(점수 0~100)로 대체됩니다.
$To	메시지 To: 헤더(봉투 수신자가 아님)로 대체됩니다.
$From	메시지 From: 헤더(봉투 발신자가 아님)로 따라 대체됩니다.
$Subject	원본 메시지의 제목으로 대체됩니다.
$Date	YYYY/MM/DD 형식을 사용하여 현재 날짜로 대체됩니다.
$Time	로컬 시간대의 현재 시간으로 대체됩니다.
$GMTimestamp	GMT를 사용하여 이메일 메시지의 Received: 줄에서 확인되는 현재 시간 및 날짜로 대체됩니다.
$MID	내부에서 메시지를 식별하는 데 사용되는 메시지 ID 또는 "MID"로 대체됩니다. RFC822 "Message-Id" 값과 혼동하지 않도록 주의합니다($Header를 사용하여 해당 항목 검색).

변수	다음으로 대체됨
$Group	메시지를 삽입할 때 일치하는 발신자가 속한 발신자 그룹의 이름으로 대체됩니다. 발신자 그룹에 이름이 없는 경우 ">Unknown<" 문자열이 삽입됩니다.
$Reputation	발신자의 SenderBase Reputation 점수로 대체됩니다. 평판 점수가 없는 경우 "None"으로 대체됩니다.
$filenames	메시지의 첨부 파일 이름이 쉼표로 구분된 목록으로 대체됩니다.
$filetypes	메시지의 첨부 파일 유형이 쉼표로 구분된 목록으로 대체됩니다.
$filesizes	메시지의 첨부 파일 크기가 쉼표로 구분된 목록으로 대체됩니다.
$remotehost	메시지를 Cisco 어플라이언스로 전송한 시스템의 호스트 이름으로 대체됩니다.
$AllHeaders	메시지 헤더로 대체됩니다.
$EnvelopeFrom	메시지의 봉투 발신자(Envelope From, <MAIL FROM>)로 대체됩니다.
$Hostname	Cisco 어플라이언스의 호스트 이름으로 대체됩니다.
$bodysize	메시지의 크기(바이트)로 대체됩니다.
$header['*string*']	원본 메시지에 일치하는 헤더가 있는 경우 작은따옴표가 붙은 헤더 값으로 대체됩니다. 큰따옴표도 사용될 수 있습니다.
$remoteip	메시지를 Cisco 어플라이언스로 전송한 시스템의 IP 주소로 대체됩니다.
$recvlistener	메시지를 수신한 리스너의 별칭으로 대체됩니다.
$dropped_filenames	`$filenames`와 동일하지만 삭제된 파일 목록을 표시합니다.
$dropped_filename	최근에 삭제된 파일 이름만 반환합니다.
$recvint	메시지를 수신한 인터페이스의 별칭으로 대체됩니다.
$timestamp	로컬 시간대를 사용하여 이메일 메시지의 Received: 줄에서 확인되는 현재 시간 및 날짜로 대체됩니다.
$Time	로컬 시간대의 현재 시간으로 대체됩니다.
$orgid	SenderBase 조직 ID(정수 값)로 대체됩니다.
$enveloperecipients	메시지의 모든 봉투 수신자(Envelope To, <RCPT TO>)로 대체됩니다.
$dropped_filetypes	`$filetypes`와 동일하지만 삭제된 파일 목록 유형을 표시합니다.
$dropped_filetype	최근에 삭제한 파일의 파일 유형만 반환합니다.

메시지 추적 시 민감한 DLP 데이터 표시 또는 숨기기

RSA 이메일 DLP 및 RSA Enterprise Manager는 모두 DLP 정책을 위반하고 메시지 추적에서 얻은 콘텐츠와 주변 콘텐츠를 기록할 수 있는 옵션을 제공합니다. 이 콘텐츠는 신용 카드 번호 및 사회 보장 번호 등의 민감한 데이터를 포함할 수 있습니다. 이 콘텐츠를 기록하지 않도록 선택할 수 있습니다.

시작하기 전에

메시지 추적을 활성화합니다. 29 장, "메시지 추적" 항목을 참조하십시오.

절차

1단계 **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)**를 선택합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

변경 후	수행할 작업
메시지 추적에서 민감한 콘텐츠를 포함합니다.	**Enable Matched Content Logging(일치된 콘텐츠 로깅 활성화)** 확인란을 선택합니다.
메시지 추적에서 민감한 콘텐츠를 숨깁니다.	**Enable Matched Content Logging(일치된 콘텐츠 로깅 활성화)** 확인란 선택을 해제합니다.

3단계 변경사항을 제출하고 커밋합니다.

다음 작업

일치된 콘텐츠 로깅을 활성화하는 경우 이 정보를 볼 수 있는 관리자를 지정합니다. 메시지 추적 시 중요 정보의 액세스 제어, 32-5페이지 항목을 참조하십시오.

DLP 엔진 및 콘텐츠 일치 분류자 업데이트 정보

어플라이언스에서 RSA DLP 엔진 및 사전 정의된 콘텐츠 일치 분류자에 대한 업데이트는 다른 보안 서비스 업데이트와 상관없습니다.

관련 주제

- RSA DLP 엔진의 현재 버전 확인, 17-37페이지
- DLP 업데이트에 대한 주의 사항, 17-38페이지
- DLP 엔진 및 콘텐츠 일치 분류자 수동 업데이트, 17-38페이지
- 자동 업데이트 활성화(권장하지 않음), 17-38페이지
- 중앙 집중식(클러스터된) 어플라이언스의 DLP 업데이트, 17-39페이지
- DLP 업데이트 롤백, 17-39페이지

RSA DLP 엔진의 현재 버전 확인

절차

1단계 **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)**를 선택합니다.

2단계 **Current DLP Version Files(현재 DLP 버전 파일)** 섹션을 확인합니다.

DLP 업데이트에 대한 주의 사항

구축 모드	주의 사항
모두	자동 업데이트를 활성화하지 않는 것이 좋습니다. 자동 업데이트 활성화 (권장하지 않음), 17-38페이지 항목을 참조하십시오.
RSA 이메일 DLP	DLP 업데이트를 통해 기존 로컬 DLP 정책에서 사용한 콘텐츠 일치 분류자가 변경될 수 있습니다. DLP 업데이트를 수동으로 실습 환경의 어플라이언스에 다운로드하여 프로덕션에 사용한 어플라이언스를 업데이트하기 전에 DLP 정책을 테스트하는 것이 좋습니다.
RSA Enterprise Manager DLP	DLP 업데이트를 로컬 어플라이언스에 다운로드하면 Enterprise Manager를 사용하여 구성된 DLP 정책에서 사용된 콘텐츠 일치 분류자가 변경되지 않습니다. 그러나 나중에 RSA 이메일 DLP를 사용하도록 어플라이언스를 전환하는 경우 기존의 모든 로컬 DLP 정책은 업데이트된 분류자를 사용합니다.

DLP 엔진 및 콘텐츠 일치 분류자 수동 업데이트

시작하기 전에

다음을 참조하십시오.

- DLP 업데이트에 대한 주의 사항, 17-38페이지
- (해당하는 경우) 중앙 집중식(클러스터된) 어플라이언스의 DLP 업데이트, 17-39페이지

절차

1단계 **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)**를 선택합니다.

2단계 **Current DLP Version Files(현재 DLP 버전 파일)** 섹션에서 **Update Now(지금 업데이트)**를 클릭합니다.

이 버튼은 다운로드할 수 있는 새 업데이트가 있는 경우에만 사용할 수 있습니다.

자동 업데이트 활성화(권장하지 않음)

이 절차를 사용하여 정기적으로 업데이트를 확인하고 다운로드하도록 어플라이언스를 활성화합니다.

참고 자동 업데이트를 활성화하지 않는 것이 좋습니다. 이러한 업데이트를 통해 기존 로컬 DLP 정책에서 사용한 콘텐츠 일치 분류자가 변경될 수 있습니다. 대신 프로덕션에 사용된 어플라이언스를 업데이트하기 전에 DLP 업데이트를 수동으로 다운로드하고 실습 환경에서 테스트합니다.

시작하기 전에

- **Security Settings(보안 설정) > Service Updates(서비스 업데이트)** 페이지에서 모든 서비스 업데이트에 대한 자동 업데이트를 활성화하고 업데이트 간격을 지정했는지 확인합니다.
- 중앙 집중식(클러스터된) 어플라이언스의 DLP 업데이트, 17-39페이지 항목을 참조하십시오.

절차

1단계 **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)**를 선택합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 **Enable automatic updates(자동 업데이트 활성화)** 확인란을 선택합니다.

4단계 변경사항을 제출하고 커밋합니다.

중앙 집중식(클러스터된) 어플라이언스의 DLP 업데이트

다음을 참고하십시오.

- 클러스터된 구축에서는 어플라이언스에 대한 자동 DLP 업데이트를 활성화할 수 없습니다.
- DLP 업데이트는 DLP가 구성된 수준에서 수행됩니다. 예를 들어 DLP가 클러스터 수준에서 구성된 경우 DLP 업데이트도 해당 수준에서 수행되어야 합니다.
- 컴퓨터 수준에서 `dlprollback` CLI 명령을 사용하여 어플라이언스에 대한 업데이트를 롤백할 수 있습니다.
- 머신 수준에서 `dlpstatus` CLI 명령을 사용하여 어플라이언스의 DLP 엔진 상태를 확인할 수 있습니다.

DLP 업데이트 롤백

이 절차는 이전 DLP 엔진 및 콘텐츠 일치 분류자를 사용하는 시스템을 반환합니다.

참고 DLP 업데이트를 롤백하면 메일 정책에 사용된 DLP 정책이 비활성화됩니다.

시작하기 전에

중앙 집중식(클러스터된) 어플라이언스의 DLP 업데이트, 17-39페이지 항목을 참조하십시오.

절차

1단계 CLI에서 `dlprollback` 명령을 사용합니다.

2단계 메일 정책에 사용된 DLP 정책을 다시 활성화합니다.

DLP 인시던트 메시지 및 데이터를 사용하여 작업

참고 구축한 것에 해당하는 경우 Enterprise Manager 및/또는 보안 관리 어플라이언스 문서를 참조하십시오.

변경 후	수행할 작업
DLP 정책 이름, 위반 심각도 및 취한 작업 등의 기준을 사용하여 DLP를 위반하는 메시지를 검색하고 발견된 메시지의 세부사항을 확인합니다.	29 장, "메시지 추적" 항목을 참조하십시오. Enterprise Manager 배포의 경우 Enterprise Manager에서 메시지를 확인할 수도 있습니다. Enterprise Manager 문서를 참조하십시오.
DLP 위반으로 의심되는 격리된 메시지를 확인하거나 관리합니다.	정책, 바이러스 또는 신종 바이러스 격리의 메시지 사용, 30-10페이지 항목을 참조하십시오. Enterprise Manager 구축: Enterprise Manager 또는 Email Security 어플라이언스에서 격리된 메시지를 확인할 수 있지만 Enterprise Manager를 사용하여 격리된 메시지를 릴리스하거나 삭제해야 합니다.
DLP 인시던트 요약 보기	DLP 인시던트 요약 보고서에 관한 자세한 정보는 28 장, "이메일 보안 모니터링 사용" 항목을 참조하십시오.
발송 메일에서 발견된 DLP 위반에 대한 정보를 확인하십시오.	DLP 인시던트 보고서에 관한 자세한 정보는 28 장, "이메일 보안 모니터링 사용" 항목을 참조하십시오. Enterprise Manager 구축의 경우 Enterprise Manager 문서를 참조하십시오.
Enterprise Manager를 사용하여 위반이 의심되는 DLP 인시던트 데이터 및 메시지를 확인하십시오.	Enterprise Manager에 대한 문서를 참조하십시오.

관련 주제

- 메시지 추적 시 민감한 DLP 데이터 표시 또는 숨기기, 17-36페이지
- 메시지 추적 시 중요 정보의 액세스 제어, 32-5페이지

데이터 유출 방지 문제 해결

- Enterprise Manager에서 Email Security 어플라이언스 연결 해제, 17-40페이지
- RSA 이메일 DLP가 이메일 첨부 파일의 위반 탐지 실패, 17-41페이지

Enterprise Manager에서 Email Security 어플라이언스 연결 해제

문제 Enterprise Manager에서 Email Security 어플라이언스 연결을 해제합니다.

솔루션 올바른 인증서가 Email Security 어플라이언스에 설치되어 있지 않습니다. (권장) Email Security 어플라이언스 및 Enterprise Manager 간 SSL 연결에 대한 인증서 획득 및 업로드, 17-25페이지 항목을 참조하십시오.

클러스터 또는 그룹으로 구축된 경우 각 어플라이언스에서 Network(네트워크) > Certificates(인증서) 페이지에서 인증서가 모두 동일한지 확인합니다.

관련 주제

- Email Security 어플라이언스 및 Enterprise Manager 간 연결 해제, 17-31페이지

RSA 이메일 DLP가 이메일 첨부 파일의 위반 탐지 실패

문제 사전 정의된 DLP 정책 사용 시 RSA 이메일 DLP에서 이메일 첨부 파일의 위반을 탐지하지 못합니다. 이 문제는 사전 정의된 DLP 정책에서 근접 매개변수가 작은 값으로 설정되어 발생될 수 있습니다.

참고 사전 정의된 DLP 정책의 근접성을 변경할 수 없습니다.

솔루션 다음 중 하나를 수행합니다.

- 필요한 경우 사용자 지정 정책을 생성하고 근접성을 조정합니다. 사용자 지정 DLP 정책 생성(고급), 17-9페이지 항목을 참조하십시오.
- RSA Enterprise Manager 및 사전 정의된 정책을 사용합니다. RSA Enterprise Manager를 통해 근접성 등의 사전 정의된 정책 구성을 미세 조정할 수 있습니다. RSA Enterprise Manager, 17-22페이지 항목을 참조하십시오.

18 장

Cisco 이메일 암호화

Cisco 이메일 암호화 개요

AsyncOS는 인바운드 및 아웃바운드 메일에 보안을 제공하도록 암호화 사용을 지원합니다. 이 기능을 사용하려면 암호화된 메시지의 특성 및 키 서버에 대한 연결 정보를 지정하는 암호화 프로파일을 생성합니다. 키 서버는 다음 중 하나를 사용할 수 있습니다.

- Cisco Registered Envelope Service(관리형 서비스) 또는
- Cisco 암호화 어플라이언스(로컬 관리형 서버)

다음으로 콘텐츠 필터, 메시지 필터 및 데이터 유출 방지 정책을 생성하여 암호화할 메시지를 결정합니다.

1. 필터 조건을 만족하는 발송 메시지는 암호화 절차를 위해 Email Security 어플라이언스의 큐에 배치됩니다.
2. 메시지가 암호화되면 암호화에 사용된 키가 암호화 프로파일에 지정된 키 서버에 보관되며 암호화된 메시지는 전달을 위해 큐에 대기 됩니다.
3. 큐에 있는 이메일 암호화를 금지하는 임시 조건이 있는 경우(즉, 임시 C-시리즈 busyness 또는 CRES 비가용성) 메시지가 다시 큐 대기 상태가 되며 나중에 다시 시도됩니다.

참고 또한 어플라이언스에서 메시지를 암호화하기 전에 처음에는 TLS 연결을 사용하여 메시지 전송을 시도하도록 설정할 수 있습니다. 자세한 내용은 암호화 대체 방법으로 TLS 연결 사용하기, 18-9페이지 항목을 참조하십시오.

로컬 키 서버로 메시지를 암호화하는 방법

표 18-1 로컬 키 서버로 메시지를 암호화하는 방법

단계	수행할 작업	추가 정보
1단계	네트워크에서 Cisco IronPort 암호화 어플라이언스를 설정합니다.	3 장, "설정 및 설치" 참조.
2단계	메시지 암호화를 활성화합니다.	Email Security 어플라이언스에서 메시지 암호화 활성화하기, 18-4페이지.
3단계	암호화 프로파일을 생성하여 사용할 암호화 키 서버와 암호화된 메시지의 보안 설정을 지정합니다.	키 서비스가 암호화된 메시지를 처리하는 방법 구성, 18-4페이지.
4단계	어플라이언스에서 암호화를 위해 메시지가 만족해야 하는 조건을 정의합니다.	암호화할 메시지 결정하기, 18-8페이지.
5단계	이메일 워크플로에서 메시지를 암호화하는 시기를 결정합니다.	• 콘텐츠 필터를 사용하여 메시지 암호화 및 즉시 전송, 18-9페이지. 또는 • 콘텐츠 필터를 사용하여 전달 시 메시지 암호화하기, 18-10페이지.
6단계	(선택 사항) 추가 보안을 위해 메시지에 플래그를 지정합니다.	메시지에 암호화 헤더를 삽입하기, 18-11페이지.
7단계	메시지를 암호화하려는 사용자 그룹을 정의합니다.	메일 정책을 생성합니다. 10 장, "메일 정책" 참조.
8단계	정의한 사용자 그룹과 정의한 암호화 작업을 연결합니다.	메일 정책과 콘텐츠 필터를 연결합니다. 10 장, "메일 정책" 참조.

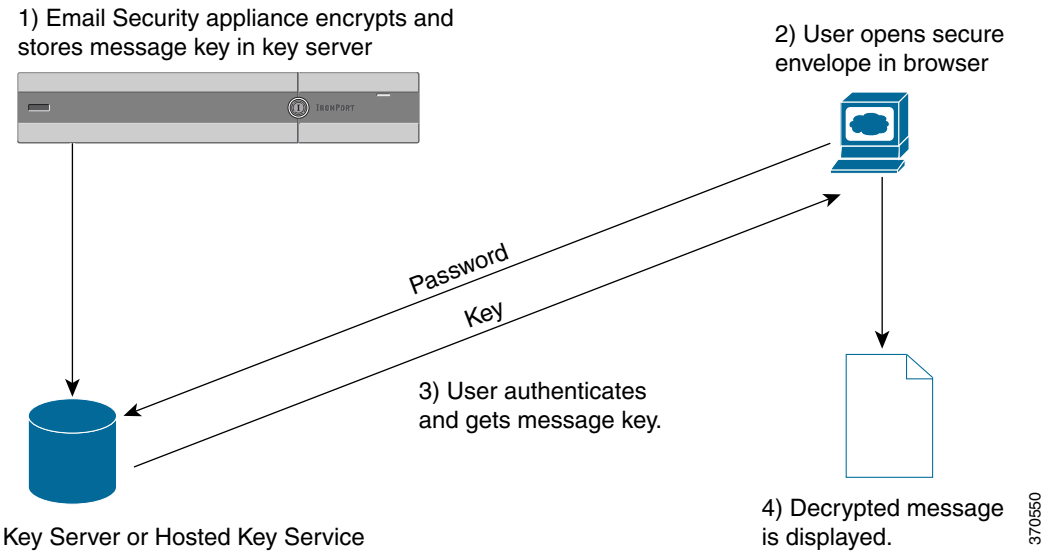
관련 주제

- 암호화 워크플로, 18-2페이지

암호화 워크플로

이메일 암호화를 사용할 때 Cisco Email Security 어플라이언스는 메시지를 암호화하고 로컬 키 서버 또는 호스트 키 서비스에 메시지 키를 보관합니다. 수신자가 암호화된 메시지를 열면 키 서비스로 수신자가 인증되며 암호 해독된 메시지가 표시됩니다.

그림 18-1 암호화 워크플로



암호화된 메시지를 여는 기본 워크플로는 다음과 같습니다.

1. 암호화 프로파일을 구성할 때 메시지 암호화에 대한 매개변수를 지정합니다. 암호화된 메시지의 경우 Email Security 어플라이언스는 로컬 키 서버 또는 호스트 키 서비스(Cisco Registered Envelope Service)에서 메시지 키를 생성하고 보관합니다.
2. 수신자는 브라우저에서 보안 봉투를 엽니다.
3. 수신자가 브라우저에서 암호화된 메시지를 열면 수신자의 ID를 인증하기 위해 비밀번호를 요구합니다. 키 서버는 메시지와 연결된 암호화 키를 반환합니다.

참고 처음으로 암호화된 이메일 메시지를 여는 경우 수신자는 보안 봉투를 열기 위해 키 서비스를 등록해야 합니다. 등록 후 수신자는 암호화 프로파일에 구성된 설정에 따라 인증 없이 암호화된 메시지를 열 수 있습니다. 암호화 프로파일은 비밀번호를 사용하지 않도록 지정할 수 있지만, 특정 기능은 사용할 수 없습니다.

4. 암호 해독된 메시지가 표시됩니다.

Email Security 어플라이언스를 사용하여 메시지 암호화

Email Security 어플라이언스로 암호화를 사용하려면 암호화 프로파일을 구성해야 합니다. `encryptionconfig` CLI 명령을 사용하여 또는 GUI의 Security Services(보안 서비스) > Cisco IronPort Email Encryption(Cisco IronPort 이메일 암호화)을 통해 암호화 프로파일을 활성화하고 구성할 수 있습니다.

참고 PXE 및 S/MIME 암호화가 어플라이언스에서 활성화된 경우 AsyncOS는 S/MIME를 먼저 사용한 다음 PXE를 사용하여 메시지를 암호화합니다.

관련 주제

- Email Security 어플라이언스에서 메시지 암호화 활성화하기, 18-4페이지
- 키 서비스가 암호화된 메시지를 처리하는 방법 구성, 18-4페이지
- 봉투의 기본 로캘 구성, 18-7페이지
- 최신 버전의 PXE 엔진으로 업데이트, 18-8페이지

Email Security 어플라이언스에서 메시지 암호화 활성화하기

절차

1단계 **Security Services(보안 서비스) > Cisco IronPort Email Encryption(Cisco IronPort 이메일 암호화)**을 클릭합니다.

2단계 **Enable(활성화)**을 클릭합니다.

3단계 (선택 사항) **Edit Settings(설정 편집)**를 클릭하여 다음 옵션을 구성합니다.

- 암호화할 최대 메시지 크기. Cisco의 권장 메시지 크기는 10MB입니다. 어플라이언스에서 암호화할 최대 메시지 크기는 25MB입니다.

  참고 권장 크기 10MB보다 큰 메시지를 암호화하면 어플라이언스 성능이 낮아질 수 있습니다. Cisco Registered Envelope Service를 사용 중인 경우 메시지 수신자는 10MB가 넘는 첨부 파일이 있는 암호화된 메시지에 응답할 수 없습니다.

- 암호화 계정 관리자의 이메일 주소. 암호화 프로파일을 프로비저닝하는 경우 이 이메일 주소는 자동으로 암호화 서버에 등록됩니다.
- 프록시 서버를 구성합니다.

키 서비스가 암호화된 메시지를 처리하는 방법 구성

키 서비스를 사용하는 경우 하나 이상의 암호화 프로파일을 생성할 수 있습니다. 다른 그룹의 이메일에 다른 수준의 보안을 사용하려는 경우 다른 암호화 프로파일을 생성할 수 있습니다. 예를 들어 민감한 요소를 포함하는 메시지를 높은 보안 수준으로 전송하거나 기타 메시지를 중간 보안 수준으로 전송할 수 있습니다. 이 경우 높은 수준의 보안 암호화 프로파일을 생성하여 특정 키워드(예: '기밀')를 포함하는 메시지와 연결하고 기타 발송 메시지를 위한 다른 암호화 프로파일을 생성할 수 있습니다.

암호화 프로파일을 사용자 지정 사용자 역할에 할당하여 해당 역할에 할당된 위임 관리자가 DLP 정책 및 콘텐츠 필터로 암호화 프로파일을 사용하도록 허용할 수 있습니다. DLP 정책 및 콘텐츠 필터를 구성할 때 관리자, 운영자 및 위임 사용자만 암호화 프로파일을 사용할 수 있습니다. 사용자 지정 역할에 할당되지 않은 암호화 프로파일은 메일 또는 DLP 정책 권한을 가진 모든 위임 관리자가 사용할 수 있습니다. 자세한 내용은 관리 작업 분배 항목을 참조하십시오.

참고 호스트 키 서비스에 여러 암호화 프로파일을 구성할 수 있습니다. 조직에 여러 브랜드가 있는 경우 이를 통해 PXE 봉투에 해당하는 키 서버에 보관된 여러 로고를 참조할 수 있습니다.

암호화 프로파일은 다음 설정을 보관합니다.

- **키 서버 설정**. 해당 키 서버에 연결하기 위해 키 서버 및 정보를 지정합니다.
- **봉투 설정**. 보안 수준 등의 메시지 봉투 세부사항, 읽음 확인 반환 여부, 시간 초과 전 암호화를 위해 메시지가 큐 대기 되는 시간, 사용할 암호화 알고리즘 유형 및 브라우저에서 실행할 암호 해독 애플릿 활성화 여부를 지정합니다.
- **메시지 설정**. 안전한 메시지 전송 및 안전한 전체 회신 활성화 여부 등의 메시지 세부사항을 지정합니다.
- **알림 설정**. 암호화 실패 알림뿐만 아니라 텍스트 및 HTML 알림을 사용하도록 알림 템플릿을 지정합니다. 암호화 프로파일을 생성할 때 텍스트 리소스에서 템플릿을 생성하고 해당 템플릿을 선택합니다. 또한 봉투를 지역화하고 암호화 실패 알림에 메시지 제목을 지정할 수 있습니다. 알림에 대한 자세한 내용은 암호화 알림 템플릿, 21-24페이지 및 바운스 및 암호화 실패 알림 템플릿, 21-23페이지 항목을 참조하십시오.

절차

1단계 Email Encryption Profiles(이메일 암호화 프로파일) 섹션에서 **Add Encryption Profile(암호화 프로파일 추가)**을 클릭합니다.

2단계 암호화 프로파일의 이름을 입력합니다.

3단계 **Used By (Roles)(사용자(역할))** 링크를 클릭하고 암호화 프로파일에 대한 접근 권한이 필요한 사용자 지정 사용자 역할을 선택한 다음 **OK(확인)**를 클릭합니다.

이 사용자 지정 역할에 할당된 위임 관리자는 자신이 담당하는 모든 DLP 정책 및 콘텐츠 필터에 대해 암호화 프로파일을 사용할 수 있습니다.

4단계 Key Server Settings(키 서버 설정) 섹션에서 다음 키 서버를 선택합니다.

- Cisco 암호화 어플라이언스(네트워크)
- Cisco Registered Envelope Service(호스트 키 서비스)

5단계 Cisco 암호화 어플라이언스(로컬 키 서비스)를 선택한 경우 다음 설정을 입력합니다.

- **내부 URL.** 이 URL은 Cisco Email Security 어플라이언스에서 네트워크 내부의 Cisco 암호화 어플라이언스에 연결할 때 사용됩니다.
- **외부 URL**. 이 URL은 수신자의 메시지가 Cisco 암호화 어플라이언스에서 키 및 다른 서비스에 접근할 때 사용됩니다. 수신자는 이 URL을 사용하여 인바운드 HTTP 또는 HTTPS 요청을 수행합니다.

6단계 Cisco Registered Envelope Service를 선택하는 경우 호스트 키 서비스의 URL을 입력합니다. 키 서비스 URL은 `https://res.cisco.com`입니다.

7단계 Key Server Settings(키 서버 설정) 아래에 있는 **Advanced(고급)**를 클릭하여 수신자가 봉투를 열 때 봉투의 암호화된 페이로드 전송에 HTTP 또는 HTTPS의 사용 여부를 지정합니다. 다음 중 하나를 선택합니다.

- **HTTP로 키 서비스 사용**. 수신자가 봉투를 열 때 HTTP를 사용하여 키 서비스에서 암호화된 페이로드를 전송합니다. Cisco Registered Envelope Service를 사용 중인 경우 이는 6단계에서 지정한 URL입니다. Cisco 암호화 어플라이언스를 사용 중인 경우 이는 5단계에서 지정한 외부 URL입니다.

  페이로드가 이미 암호화되었으므로 HTTP를 통해 전송하는 것이 안전하며 HTTPS를 통해 전송하는 것보다 속도가 빠릅니다. 이는 HTTPS를 통해 이미지 요청을 전송하는 것보다 나은 성능을 제공합니다.

- **HTTPS로 키 서비스 사용**. 수신자가 봉투를 열 때 HTTPS를 사용하여 키 서비스에서 암호화된 페이로드를 전송합니다. Cisco Registered Envelope Service를 사용 중인 경우 이는 6단계에서 지정한 URL입니다. Cisco 암호화 어플라이언스를 사용 중인 경우 이는 5단계에서 지정한 외부 URL입니다.
- **페이로드 전송에 대해 별도의 URL 지정**. 암호화된 페이로드에 키 서버를 사용하지 않는 경우 다른 URL을 사용하고 페이로드 전송에 HTTP 또는 HTTPS를 사용하도록 지정할 수 있습니다.

8단계 Envelope Settings(봉투 설정) 섹션에서 메시지 보안 수준을 선택합니다.

- **높은 보안**. 수신자는 항상 비밀번호를 입력하여 암호화된 메시지를 열어야 합니다.
- **중간 보안**. 수신자 자격 증명이 캐시되는 경우 수신자는 암호화된 메시지를 열기 위해 자격 증명을 입력할 필요가 없습니다.
- **비밀번호 필요 없음**. 가장 낮은 수준의 암호화된 메시지 보안입니다. 수신자는 암호화된 메시지를 열기 위해 비밀번호를 입력할 필요가 없습니다. 비밀번호로 보호되지 않은 봉투에 대해 읽음 확인, 안전한 전체 회신 및 안전한 메시지 전송 기능을 활성화할 수 있습니다.

9단계 로고를 클릭하여 사용자가 조직의 URL을 열도록 활성화하려면 로고의 링크를 추가할 수 있습니다. 다음 옵션 중에서 선택합니다.

- **링크 없음.** 라이브 링크가 메시지 봉투에 추가되지 않습니다.
- **사용자 지정 링크 URL**. URL을 입력하여 메시지 봉투에 라이브 링크를 추가합니다.

10단계 (선택 사항) 읽음 확인을 사용합니다. 이 옵션을 활성화하는 경우 수신자가 안전한 봉투를 열 때 발신자가 확인을 받습니다.

11단계 (선택 사항) Envelope Settings(봉투 설정) 아래에 있는 **Advanced(고급)**를 클릭하여 다음 설정을 구성합니다.

- 시간이 초과되기 전에 메시지가 암호화 큐에 머무를 수 있는 시간(초)을 입력합니다. 메시지 시간이 초과되면 어플라이언스가 메시지를 바운스하고 발신자에게 알림을 보냅니다.
- 암호화 알고리즘을 선택합니다.
  - **ARC4**. ARC4는 가장 일반적인 선택 사항으로 암호 해독 지연 시간을 최소화하여 메시지 수신자에게 강력한 암호화 기능을 제공합니다.
  - **AES**. AES는 강력한 암호화 기능을 제공하지만, 암호 해독에도 시간이 오래 걸려 수신자에게 지연이 발생합니다. AES는 일반적으로 정부 및 은행 애플리케이션에 사용합니다.
- 암호 해독 애플릿을 활성화하거나 비활성화합니다. 이 옵션을 활성화하면 브라우저 환경에서 메시지 첨부 파일이 열립니다. 이 옵션을 비활성화하면 키 서버에서 메시지 첨부 파일이 암호 해독됩니다. 이 옵션을 비활성화하는 경우 메시지가 열리는 데 시간이 오래 걸리지만 브라우저 환경에서는 영향을 받지 않습니다.

12단계 Message Settings(메시지 설정) 섹션에서 다음을 수행합니다.

- 안전한 전체 회신 기능을 활성화하려면 **Enable Secure Reply All(안전한 전체 회신 사용)** 확인란을 선택합니다.
- 안전한 메시지 전송 기능을 활성화하려면 **Enable Secure Message Forwarding(안전한 메시지 전달 사용)** 확인란을 선택합니다.

13단계 (선택 사항) Cisco Registered Envelope Service를 선택하고 이 서비스가 봉투 지역화를 지원하는 경우 봉투 지역화를 활성화합니다. Notification Settings(알림 설정) 섹션에서 **Use Localized Envelope(지역화된 봉투 사용)** 확인란을 선택합니다.

참고 봉투 지역화를 활성화하는 경우 암호화된 메시지 HTML 또는 텍스트 알림을 선택할 수 없습니다.

봉투의 기본 로캘을 설정하려면 봉투의 기본 로캘 구성, 18-7페이지 항목을 참조하십시오.

14단계 HTML 및 텍스트 알림 템플릿을 선택합니다.

참고 키 서버는 수신자의 이메일 애플리케이션을 기반으로 HTML 또는 텍스트 알림을 사용합니다. 두 가지 모두에 알림을 구성해야 합니다.

다음을 수행합니다.

a. HTML 알림 템플릿을 선택합니다. 텍스트 리소스에서 구성한 HTML 알림에서 선택합니다. 템플릿을 구성하지 않은 경우 시스템은 기본 템플릿을 사용합니다.

b. 텍스트 알림 템플릿을 선택합니다. 텍스트 리소스에서 구성한 텍스트 알림에서 선택합니다. 템플릿을 구성하지 않은 경우 시스템은 기본 템플릿을 사용합니다.

참고 지역화된 봉투를 사용하는 경우 이러한 옵션을 사용할 수 없습니다.

15단계 암호화 실패 알림에 제목 헤더를 입력합니다. 암호화 프로세스 시간이 초과되면 어플라이언스에서 알림을 보냅니다.

16단계 메시지 본문에 대한 암호화 실패 알림 템플릿을 선택합니다. 텍스트 리소스에서 구성한 암호화 실패 알림 템플릿에서 선택합니다. 템플릿을 구성하지 않은 경우 시스템은 기본 템플릿을 사용합니다.

17단계 변경사항을 제출하고 커밋합니다.

18단계 Cisco Registered Envelope Service를 사용하는 경우 어플라이언스를 프로비저닝하는 추가 단계를 수행해야 합니다. 어플라이언스를 프로비저닝하면 호스트 키 서비스에 암호화 프로파일을 등록합니다. 어플라이언스를 프로비저닝하려면 등록하려는 암호화 프로파일에 해당하는 **Provision(프로비전)** 버튼을 클릭합니다.

봉투의 기본 로캘 구성

봉투의 기본 로캘은 영어입니다. Cisco Registered Envelope Service를 선택했고 이 서비스가 봉투의 지역화를 지원하는 경우 봉투의 로캘을 다음 중 하나로 변경할 수 있습니다.

- 영어
- 프랑스어
- 독일어
- 일본어
- 포르투갈어
- 스페인어

시작하기 전에

- Cisco Registered Envelope Service를 키 서비스 유형 및 봉투 지역화를 활성화하도록 설정하여 암호화 프로파일을 생성합니다. 키 서비스가 암호화된 메시지를 처리하는 방법 구성, 18-4페이지 항목을 참조하십시오.
- Cisco Registered Envelope Service가 봉투의 지역화를 지원하는지 확인합니다.

절차

1단계 **Security Services(보안 서비스) > Cisco IronPort Email Encryption(Cisco IronPort 이메일 암호화)**을 클릭합니다.

2단계 기존 암호화 프로파일을 엽니다.

3단계 **Notification Settings(알림 설정)** 섹션의 **Localized Envelopes(지역화된 봉투)** 드롭다운 목록에서 해당 로캘을 선택합니다.

4단계 **Submit(제출)**을 클릭합니다.

5단계 **Commit Changes(변경사항 커밋)**를 클릭합니다.

최신 버전의 PXE 엔진으로 업데이트

Cisco Email Encryption Settings(이메일 암호화 설정) 페이지는 PXE 엔진의 현재 버전 및 어플라이언스에서 사용하는 도메인 매핑 파일을 표시합니다. **Security Services(보안 서비스) > Service Updates(서비스 업데이트)** 페이지(또는 CLI의 `updateconfig` 명령)를 사용하여 PXE 엔진을 자동으로 업데이트하도록 Email Security 어플라이언스를 구성할 수 있습니다. 자세한 내용은 서비스 업데이트, 33-17페이지 항목을 참조하십시오.

또한 IronPort Email Encryption Settings(IronPort 이메일 암호화 설정) 페이지의 PXE Engine Updates(PXE 엔진 업데이트) 섹션에 있는 **Update Now(지금 업데이트)** 버튼을 사용하거나 CLI의 `encryptionupdate` 명령을 사용하여 엔진을 수동으로 업데이트할 수 있습니다.

암호화할 메시지 결정하기

암호화 프로파일을 만든 후 암호화해야 하는 이메일 메시지를 결정하는 발송 콘텐츠 필터를 만들어야 합니다. 콘텐츠 필터는 발송 이메일을 스캔하고 메시지가 지정된 조건에 일치하는지 확인합니다. 콘텐츠 필터에서 메시지가 조건과 일치한다고 확인되면 Cisco Email Security 어플라이언스는 메시지를 암호화하고 생성된 키를 키 서버에 보냅니다. 암호화 프로파일에 지정된 설정을 사용하여 사용할 키 서버와 다른 암호화 설정을 확인합니다.

또한 메시지가 데이터 유출 방지 검사 후 릴리스되면 메시지를 암호화할 수 있습니다. 자세한 내용은 DLP 위반 시 수행할 작업 정의(메시지 작업), 17-33페이지 항목을 참조하십시오.

관련 주제

- 암호화 대체 방법으로 TLS 연결 사용하기, 18-9페이지
- 콘텐츠 필터를 사용하여 메시지 암호화 및 즉시 전송, 18-9페이지
- 콘텐츠 필터를 사용하여 전달 시 메시지 암호화하기, 18-10페이지

암호화 대체 방법으로 TLS 연결 사용하기

도메인마다 지정된 대상 제어에 따라 TLS 연결을 사용할 수 있는 경우 Email Security 어플라이언스는 메시지를 암호화하는 대신 TLS 연결을 통해 메시지를 안전하게 릴레이할 수 있습니다. 어플라이언스는 메시지를 암호화하거나 대상 제어의 TLS 설정(필수, 권장 또는 없음) 및 암호화 콘텐츠 필터에 정의된 작업을 기반으로 TLS 연결을 통해 메시지를 보낼지 여부를 결정합니다.

콘텐츠 필터를 생성할 때 항상 메시지를 암호화하거나 가장 먼저 TLS 연결을 통해 전송 시도하거나, TLS 연결을 사용할 수 없는 경우 메시지를 암호화하도록 지정할 수 있습니다. 표 18-2에서는 암호화 제어 필터가 가장 먼저 TLS 연결을 통해 메시지 전송을 시도하는 경우 Email Security 어플라이언스가 대상 제어의 TLS 설정을 기반으로 메시지를 보내는 방법을 보여줍니다.

표 18-2 ESA 어플라이언스에서 TLS 지원

대상 제어 TLS 설정	TLS 연결이 가능한 경우의 작업	TLS 연결이 불가능한 경우의 작업
없음	봉투 암호화 및 전송	봉투 암호화 및 전송
TLS 기본 설정	TLS로 전송	봉투 암호화 및 전송
TLS 필요	TLS로 전송	메시지 재시도/바운스

대상 제어에서 TLS를 활성화하는 방법에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성 항목을 참조하십시오.

콘텐츠 필터를 사용하여 메시지 암호화 및 즉시 전송

시작하기 전에

- 콘텐츠 필터의 조건을 구축하는 개념을 이해하려면 콘텐츠 필터 개요, 11-1페이지 항목을 참조하십시오.
- (선택 사항) 메시지에 암호화 헤더를 삽입하기, 18-11페이지 항목을 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > Outgoing Content Filters(발송 콘텐츠 필터)**로 이동합니다.

2단계 Filters(필터) 섹션에서 **Add Filter(필터 추가)**를 클릭합니다.

3단계 Conditions(조건) 섹션에서 **Add Condition(조건 추가)**을 클릭합니다.

4단계 조건을 추가하여 암호화할 메시지를 필터링합니다. 예를 들어 민감한 요소를 암호화하려면 제목 또는 본문에 "기밀" 등의 특정 단어 또는 구문을 포함하는 메시지를 식별하는 조건을 추가할 수 있습니다.

5단계 **OK(확인)**를 클릭합니다.

6단계 선택적으로 **Add Action(작업 추가)**을 클릭하고 **Add Header(헤더 추가)**를 선택하여 추가 암호화 설정을 지정하도록 메시지에 암호화 헤더를 삽입합니다.

7단계 Actions(작업) 섹션에서 **Add Action(작업 추가)**을 클릭합니다.

8단계 **Add Action(작업 추가)** 목록에서 **Encrypt and Deliver Now(Final Action)(암호화 및 지금 전송(최종 작업))**를 선택합니다.

9단계 조건을 만족하는 메시지를 항상 암호화할지 또는 TLS 연결을 통한 전송 시도가 실패하는 경우에만 메시지를 암호화할지 선택합니다.

10단계 콘텐츠 필터와 연결할 암호화 프로파일을 선택합니다.

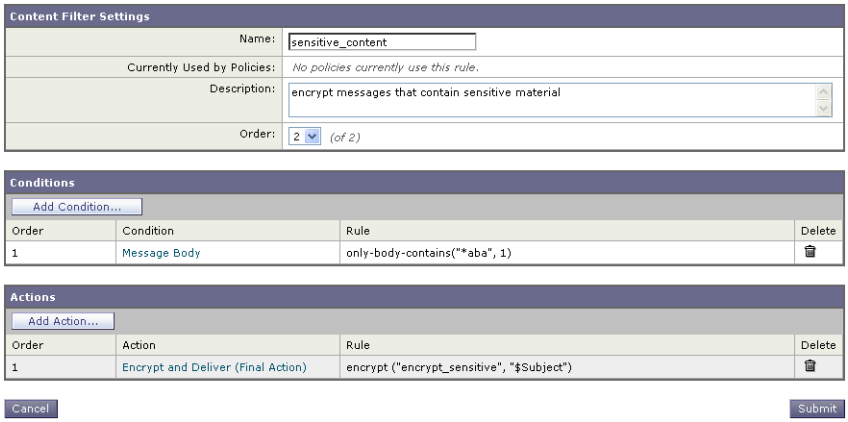
암호화 프로파일에서 사용할 키 서버, 보안 수준, 메시지 봉투의 형식에 관한 설정 및 기타 메시지 설정을 지정합니다. 암호화 프로파일을 콘텐츠 필터와 연결하는 경우 콘텐츠 필터는 이 저장된 설정을 사용하여 메시지를 암호화합니다.

11단계 메세지의 제목을 입력합니다.

12단계 **OK(확인)**를 클릭합니다.

그림 18-2의 콘텐츠 필터는 메시지 본문에서 ABA 콘텐츠를 검색하는 콘텐츠 필터를 보여줍니다. 콘텐츠 필터에 정의된 작업은 이메일이 암호화되고 전송되는지를 지정합니다.

그림 18-2 암호화 콘텐츠 필터



13단계 암호화 작업을 추가한 후 **Submit(제출)**을 클릭합니다.

14단계 변경사항을 커밋합니다.

다음 작업

콘텐츠 필터를 추가한 후 필터를 발송 메일 정책에 추가해야 합니다. 기본 정책에서 콘텐츠 필터를 활성화하거나 조직의 필요에 따라 특정 메일 정책에 필터를 적용하도록 선택할 수 있습니다. 메일 정책 적용에 대한 자세한 내용은 메일 정책 개요, 10-1페이지 항목을 참조하십시오.

콘텐츠 필터를 사용하여 전달 시 메시지 암호화하기

콘텐츠 필터를 생성하여 전달 시 메시지를 암호화합니다. 이는 메시지가 계속 다음 단계로 이동되며 모든 절차가 완료되면 메시지가 암호화되어 전달됨을 의미합니다.

시작하기 전에

- 콘텐츠 필터의 조건을 구축하는 개념을 이해하려면 콘텐츠 필터 개요, 11-1페이지 항목을 참조하십시오.
- (선택 사항) 메시지에 암호화 헤더를 삽입하기, 18-11페이지 항목을 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > Outgoing Content Filters(발송 콘텐츠 필터)**로 이동합니다.

2단계 Filters(필터) 섹션에서 **Add Filter(필터 추가)**를 클릭합니다.

3단계 Conditions(조건) 섹션에서 **Add Condition(조건 추가)**을 클릭합니다.

4단계 조건을 추가하여 암호화할 메시지를 필터링합니다. 예를 들어 민감한 요소를 암호화하려면 제목 또는 본문에 "기밀" 등의 특정 단어 또는 구문을 포함하는 메시지를 식별하는 조건을 추가할 수 있습니다.

5단계 **OK(확인)**를 클릭합니다.

6단계 선택적으로 **Add Action(작업 추가)**을 클릭하고 **Add Header(헤더 추가)**를 선택하여 추가 암호화 설정을 지정하도록 메시지에 암호화 헤더를 삽입합니다.

7단계 Actions(작업) 섹션에서 **Add Action(작업 추가)**을 클릭합니다.

8단계 **Add Action(작업 추가)** 목록에서 **Encrypt on Delivery(전송 시 암호화)**를 선택합니다.

9단계 조건을 만족하는 메시지를 항상 암호화할지 또는 TLS 연결을 통한 전송 시도가 실패하는 경우에만 메시지를 암호화할지 선택합니다.

10단계 콘텐츠 필터와 연결할 암호화 프로파일을 선택합니다.

암호화 프로파일에서 사용할 키 서버, 보안 수준, 메시지 봉투의 형식에 관한 설정 및 기타 메시지 설정을 지정합니다. 암호화 프로파일을 콘텐츠 필터와 연결하는 경우 콘텐츠 필터는 이 저장된 설정을 사용하여 메시지를 암호화합니다.

11단계 메세지의 제목을 입력합니다.

12단계 **OK(확인)**를 클릭합니다.

13단계 암호화 작업을 추가한 후 **Submit(제출)**을 클릭합니다.

14단계 변경사항을 커밋합니다.

다음 작업

콘텐츠 필터를 추가한 후 필터를 발송 메일 정책에 추가해야 합니다. 기본 정책에서 콘텐츠 필터를 활성화하거나 조직의 필요에 따라 특정 메일 정책에 필터를 적용하도록 선택할 수 있습니다. 메일 정책 적용에 대한 자세한 내용은 메일 정책 개요, 10-1페이지 항목을 참조하십시오.

메시지에 암호화 헤더를 삽입하기

AsyncOS에서는 콘텐츠 필터 또는 메시지 필터를 사용하여 SMTP 헤더를 메시지에 삽입하여 메시지에 암호화 설정을 추가할 수 있습니다. 암호화 헤더는 연결된 암호화 프로파일에 정의된 암호화 설정을 재정의할 수 있으며 지정된 암호화 기능을 메시지에 적용할 수 있습니다.

참고 Cisco Ironport 암호화 어플라이언스를 설정하여 플래그가 지정된 메시지를 처리해야 합니다.

절차

1단계 **Mail Policies(메일 정책) > Outgoing Content Filters(발송 콘텐츠 필터)** 또는 **Incoming Content Filters(수신 콘텐츠 필터)**로 이동합니다.

2단계 Filters(필터) 섹션에서 **Add Filter(필터 추가)**를 클릭합니다.

3단계 Actions(작업) 섹션에서 **Add Action(작업 추가)**을 클릭하고 **Add/Edit Header(헤더 추가/편집)**를 선택하여 추가 암호화 설정을 지정하도록 메시지에 암호화 헤더를 삽입합니다.

예를 들어 전송 후 24시간 이내에 만료되는 등록 봉투를 사용하는 경우 헤더 이름으로 `X-PostX-ExpirationDate`를 입력하고 헤더 값으로 `+24:00:00`을 입력합니다.

관련 주제

- 암호화 헤더, 18-12페이지
- 암호화 헤더 예, 18-14페이지
- 암호화 콘텐츠 필터 생성에 대한 자세한 내용은 콘텐츠 필터를 사용하여 메시지 암호화 및 즉시 전송, 18-9페이지 항목을 참조하십시오.
- 메시지 필터를 사용하여 헤더를 삽입하는 방법에 대한 자세한 내용은 메시지 필터를 사용하여 이메일 정책 적용 항목을 참조하십시오.

암호화 헤더

표 18-3에서는 메시지에 추가할 수 있는 암호화 헤더를 표시합니다.

표 18-3 이메일 암호화 헤더

MIME 헤더	설명	값
`X-PostX-Reply-Enabled`	메시지에 대한 안전한 회신을 사용할지 여부를 나타내고 메시지 표시줄에 회신 버튼을 표시합니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.	회신 버튼을 표시할지 여부에 대한 부울 연산자. 버튼을 표시하려면 `true`로 설정합니다. 기본값은 `false`입니다.
`X-PostX-Reply-All-Enabled`	메시지에 대한 안전한 "전체 회신"을 사용할지 여부를 나타내고 메시지 표시줄에 전체 회신 버튼을 표시합니다. 이 헤더는 기본 프로파일 설정을 재정의합니다.	전체 회신 버튼을 표시할지 여부에 대한 부울 연산자. 버튼을 표시하려면 `true`로 설정합니다. 기본값은 `false`입니다.
`X-PostX-Forward-Enabled`	안전한 메시지 전송 기능을 사용할지 여부를 나타내고 메시지 표시줄에 Foward(전송) 버튼을 표시합니다. 이 헤더는 기본 프로파일 설정을 재정의합니다.	전달 버튼을 표시할지 여부에 대한 부울 연산자. 버튼을 표시하려면 `true`로 설정합니다. 기본값은 `false`입니다.
`X-PostX-Send-Return-Receipt`	읽음 확인을 사용할지 여부를 나타냅니다. 수신자가 안전한 봉투를 열 때 발신자가 확인을 받습니다. 이 헤더는 기본 프로파일 설정을 재정의합니다.	읽음 확인을 보낼지 여부에 대한 부울 연산자. 버튼을 표시하려면 `true`로 설정합니다. 기본값은 `false`입니다.

표 18-3 이메일 암호화 헤더

MIME 헤더	설명	값
X-PostX-ExpirationDate	전송하기 전에 등록 봉투의 만료 날짜를 정의합니다. 만료 날짜가 지나고 나면 키 서버는 등록 봉투에 대한 접근을 제한합니다. 등록 봉투는 메시지가 만료되었음을 나타내는 메시지를 표시합니다. 이 헤더는 메시지에 암호화 설정을 추가합니다. Cisco Registered Envelope Service를 사용하는 경우, 웹사이트 (http://res.cisco.com)에서 로그인하여 메시지를 전송한 후 메시지 만료 날짜를 설정, 조정 또는 제거할 수 있습니다.	상대 날짜 또는 시간을 포함하는 문자열 값. 상대 시간, 분 및 초에 +HH:MM:SS 형식을 사용하고 상대 일수에 +D 형식을 사용합니다. 기본적으로 만료 날짜가 없습니다.
X-PostX-ReadNotificationDate	전송하기 전에 등록 봉투의 "읽은 날짜"를 정의합니다. 등록 봉투를 이 날짜까지 읽지 않은 경우 로컬 키 서버는 알림을 생성합니다. 이 헤더가 있는 등록 봉투는 Cisco Registered Envelope Service가 아닌 로컬 키 서버로만 작동합니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.	상대 날짜 또는 시간을 포함하는 문자열 값. 상대 시간, 분 및 초에 +HH:MM:SS 형식을 사용하고 상대 일수에 +D 형식을 사용합니다. 기본적으로 만료 날짜가 없습니다.
X-PostX-Suppress-Applet-For-Open	암호 해독 애플릿을 비활성화할지 여부를 나타냅니다. 암호 해독 애플릿을 통해 메시지 첨부 파일이 브라우저 환경에서 열립니다. 애플릿을 비활성화하면 키 서버에서 메시지 첨부 파일이 암호 해독됩니다. 이 옵션을 비활성화하는 경우 메시지가 열리는 데 시간이 오래 걸리지만 브라우저 환경에서는 영향을 받지 않습니다. 이 헤더는 기본 프로파일 설정을 재정의합니다.	암호 해독 애플릿을 비활성화할지 여부에 대한 부울 연산자. 애플릿을 비활성화하려면 true로 설정합니다. 기본값은 false입니다.

표 18-3 이메일 암호화 헤더

MIME 헤더	설명	값
X-PostX-Use-Script	JavaScript가 없는 봉투를 보낼지 여부를 나타냅니다. JavaScript가 없는 봉투란 수신자의 컴퓨터에서 로컬로 봉투를 여는 데 사용되는 JavaScript를 포함하지 않는 등록 봉투입니다. 수신자는 Open Online(온라인에서 열기) 방법 또는 Open by Forwarding(전송하여 열기) 방법을 사용하여 메시지를 확인해야 합니다. 수신자 도메인의 게이트웨이가 JavaScript를 제거하고 암호화된 메시지를 열 수 없도록 하는 경우 이 헤더를 사용합니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.	JavaScript 애플릿을 포함해야 하는지 여부에 대한 부울 연산자. JavaScript가 없는 봉투를 보내려면 false로 설정합니다. 기본값은 true입니다.
X-PostX-Remember-Envelope-Key-Checkbox	봉투의 오프라인 열기에 대한 봉투 특정 키 캐싱을 허용할지 여부를 나타냅니다. 봉투 키 캐싱을 사용하면 수신자가 올바른 비밀번호를 입력하고 "Remember the password for this envelope(이 봉투에 대한 비밀번호 기억하기)"확인란을 선택할 때 특정 봉투에 대한 암호 해독 키가 수신자의 컴퓨터에 캐시됩니다. 그런 다음에는 수신자는 해당 컴퓨터에서 봉투를 다시 열기 위해 비밀번호를 다시 입력할 필요가 없습니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.	봉투 키 캐싱을 활성화하고 "Remember the password for this envelope(이 봉투에 대한 비밀번호 기억하기)" 확인란을 표시할지 여부에 대한 부울 연산자. 기본값은 false입니다.

암호화 헤더 예

이 절에서는 암호화 헤더의 예를 제공합니다.

관련 주제

- 오프라인에서 열기에 대해 봉투 키 캐싱 활성화하기, 18-14페이지
- JavaScript가 없는 봉투 활성화하기, 18-15페이지
- 메시지 만료 활성화하기, 18-15페이지
- 암호 해독 애플릿 비활성화하기, 18-15페이지

오프라인에서 열기에 대해 봉투 키 캐싱 활성화하기

봉투 키 캐싱이 활성화된 등록 봉투를 보내려면 다음 헤더를 메시지에 삽입합니다.

```
X-PostX-Remember-Envelope-Key-Checkbox: true
```

"Remember the password for this envelope(이 봉투에 대한 비밀번호 기억하기)" 확인란이 등록 봉투에 표시됩니다.

JavaScript가 없는 봉투 활성화하기

JavaScript가 없는 등록 봉투를 보내려면 다음 헤더를 메시지에 삽입합니다.

```
X-PostX-Use-Script: false
```

수신자가 securedoc.html 첨부 파일을 여는 경우 등록 봉투가 Open Online(온라인으로 열기) 링크와 함께 표시되며 Open(열기) 버튼은 비활성화됩니다.

메시지 만료 활성화하기

전송 후 24시간 후 만료하도록 메시지를 구성하려면 다음 헤더를 메시지에 삽입합니다.

```
X-PostX-ExpirationDate: +24:00:00
```

수신자는 전송 후 24시간 동안 암호화된 메시지의 콘텐츠를 열고 볼 수 있습니다. 그런 다음 등록 봉투는 봉투가 만료되었음을 나타내는 메시지를 표시합니다.

암호 해독 애플릿 비활성화하기

암호 해독 애플릿을 비활성화하고 키 서버에서 메시지 첨부 파일을 암호 해독하려면 다음 헤더를 메시지에 삽입합니다.

X-PostX-Suppress-Applet-For-Open: true

참고 암호 해독 애플릿을 비활성화하면 메시지를 여는 데 시간이 오래 걸릴 수 있지만 브라우저 환경에서는 영향을 받지 않습니다.

19 장

S/MIME 보안 서비스

S/MIME 보안 서비스 개요

S/MIME(Secure/Multipurpose Internet Mail Extensions)는 안전하고 확인된 이메일 메시지를 보내거나 받을 수 있는 표준 기반 방법입니다. S/MIME는 공개/개인 키 쌍을 사용하여 메시지를 암호화하거나 메시지에 서명합니다. 그 방법은 다음과 같습니다.

- 메시지가 암호화되어 있으면 메시지 수신자만 암호화된 메시지를 열 수 있습니다.
- 메시지에 서명이 되어 있으면 메시지 수신자가 발신자의 도메인 ID를 검증하여 해당 메시지가 전송 중에 변경되지 않았음을 확인할 수 있습니다.

S/MIME에 대한 자세한 내용을 보려면 다음 RFC를 검토하십시오.

- RFC 5750: S/MIME(Secure/Multipurpose Internet Mail Extensions) 버전 3.2 - 인증서 처리
- RFC 5751: S/MIME(Secure/Multipurpose Internet Mail Extensions) 버전 3.2 - 메시지 사양
- RFC 3369: 암호화 메시지 구문

Email Security 어플라이언스의 S/MIME 보안 서비스

조직은 모든 최종 사용자가 자체 인증서를 처리할 필요 없이 S/MIME를 사용하여 안전하게 통신할 수 있는 방법을 찾고자 할 수 있습니다. 그러한 조직을 위해 Email Security 어플라이언스는 개별 사용자가 아닌 조직을 식별하는 인증서를 사용하여 게이트웨이 수준에서 S/MIME 보안 서비스(서명, 암호화, 확인 및 암호 해독)를 지원합니다.

Email Security 어플라이언스는 B2B(Business-to-Business) 및 B2C(Business-to-Consumer) 시나리오를 위해 다음과 같은 S/MIME 보안 서비스를 제공합니다.

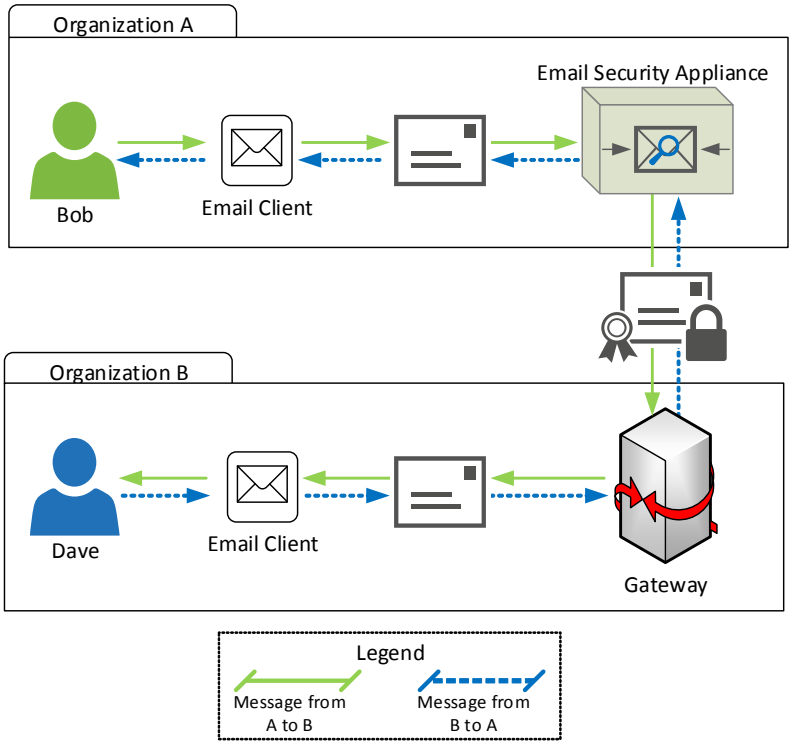
- S/MIME를 사용하여 메시지 서명 또는 암호화 또는 서명 및 암호화하는 서비스. S/MIME를 사용하여 메시지 서명 또는 암호화 또는 서명 및 암호화, 19-4페이지를 참조하십시오.
- S/MIME를 사용하여 메시지 확인 또는 암호 해독 또는 암호 해독 및 확인하는 서비스. S/MIME를 사용하여 수신 메시지 확인 또는 암호 해독 또는 암호 해독 및 확인, 19-13페이지를 참조하십시오.

관련 주제

- S/MIME 보안 서비스의 작동 원리 이해, 19-2페이지

S/MIME 보안 서비스의 작동 원리 이해

시나리오: Business-to-Business



조직 A와 B는 S/MIME를 사용해 서로 주고받는 모든 메시지에 서명하고 메시지를 암호화하고자 합니다. 조직 A는 게이트웨이 수준에서 S/MIME 보안 서비스를 수행하도록 Email Security 어플라이언스를 구성했습니다. 조직 B는 게이트웨이 수준에서 S/MIME 보안 서비스를 수행하도록 타사 어플라이언스를 구성했습니다.

참고 현재 예에서는 조직 B가 타사 어플라이언스를 사용하여 S/MIME 보안 서비스를 수행하고 있다고 가정합니다. 실제 상황에서 이는 게이트웨이 수준에서 S/MIME 보안 서비스를 수행할 수 있는 애플리케이션 또는 어플라이언스(Email Security 어플라이언스 포함)일 수 있습니다.

조직 A에서 조직 B에 메시지를 보내는 경우:

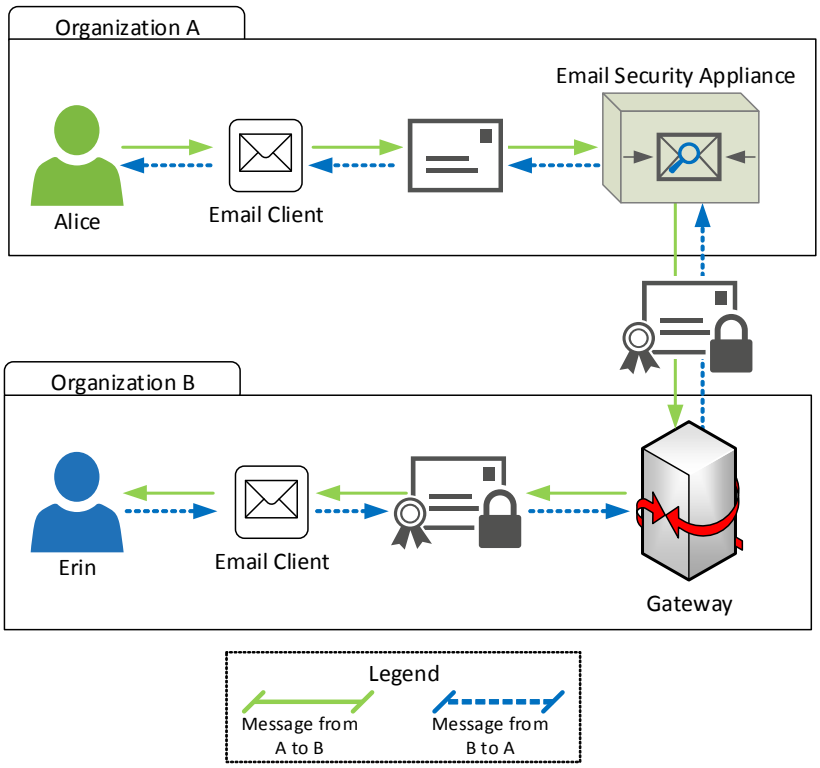
1. Bob(조직 A)이 이메일 클라이언트를 사용하여 서명 및 암호화가 적용되지 않은 메시지를 Dave(조직 B)에게 보냅니다.
2. 조직 A의 Email Security 어플라이언스가 메시지에 서명하고 메시지를 암호화하여 조직 B에 전송합니다.

3. 조직 B의 게이트웨이에서 타사 애플리케이션이 메시지의 암호를 해독하고 메시지를 확인합니다.
4. Dave는 암호가 해독된 서명 없는 메시지를 받습니다.

조직 B에서 조직 A에 메시지를 보내는 경우:

1. Dave(조직 B)가 이메일 클라이언트를 사용하여 서명 및 암호화가 적용되지 않은 메시지를 Bob(조직 A)에게 보냅니다.
2. 조직 B의 게이트웨이에서 타사 애플리케이션이 메시지에 서명하고 메시지를 암호화하여 조직 A에 전송합니다.
3. 조직 A의 Email Security 어플라이언스가 메시지의 암호를 해독하고 메시지를 확인합니다.
4. Bob은 암호가 해독된 서명 없는 메시지를 받습니다.

시나리오: Business-to-Consumer



조직 A와 B는 S/MIME를 사용해 서로 주고받는 모든 메시지에 서명하고 메시지를 암호화하고자 합니다. 조직 A는 게이트웨이 수준에서 S/MIME 보안 서비스를 수행하도록 Email Security 어플라이언스를 구성했습니다. 조직 B는 S/MIME 보안 서비스를 수행하도록 모든 사용자의 이메일 클라이언트를 구성했습니다.

조직 A에서 조직 B에 메시지를 보내는 경우:

1. Alice(조직 A)가 이메일 클라이언트를 사용하여 서명 및 암호화가 적용되지 않은 메시지를 Erin(조직 B)에게 보냅니다.
2. 조직 A의 Email Security 어플라이언스가 메시지에 서명하고 메시지를 암호화하여 조직 B에 전송합니다.

3. 조직 B의 이메일 클라이언트가 메시지의 암호를 해독하고 메시지를 확인하여 Erin에게 표시해 줍니다.

조직 B에서 조직 A에 메시지를 보내는 경우:

1. Erin(조직 B)이 이메일 클라이언트를 사용하여 메시지에 서명과 암호화를 적용하여 Alice(조직 A)에게 보냅니다.
2. 조직 A의 Email Security 어플라이언스가 메시지의 암호를 해독하고 메시지를 확인합니다.
3. Alice는 암호가 해독된 서명 없는 메시지를 받습니다.

S/MIME를 사용하여 메시지 서명 또는 암호화 또는 서명 및 암호화

참고 Email Security 어플라이언스를 사용하여 발송 및 수신 메시지를 서명 또는 암호화하거나 서명 및 암호화할 수 있습니다.

Email Security 어플라이언스의 S/MIME 서명 및 암호화 워크플로

S/MIME 서명 워크플로

다음 프로세스는 Email Security 어플라이언스가 S/MIME 서명을 수행하는 방식에 대해 설명합니다.

1. 메시지에 해시 알고리즘을 적용하여 메시지 다이제스트를 생성합니다.
2. 어플라이언스의 S/MIME 인증서 개인 키를 사용하여 메시지 다이제스트를 암호화합니다.
3. 암호화된 메시지 다이제스트와 어플라이언스의 S/MIME 인증서 공개 키를 사용하여 PKCS7 서명을 만듭니다.
4. PKCS7 서명을 메시지에 첨부하여 메시지에 서명합니다.
5. 수신자에게 서명된 메시지를 보냅니다.

S/MIME 암호화 워크플로

다음 프로세스는 Email Security 어플라이언스가 S/MIME 암호화를 수행하는 방식에 대해 설명합니다.

1. 의사 난수 세션 키를 생성합니다.
2. 세션 키를 사용하여 메시지 본문을 암호화합니다.
3. 수신자(게이트웨이 또는 소비자)의 S/MIME 인증서 공개 키를 사용하여 세션 키를 암호화합니다.
4. 암호화된 세션 키를 메시지에 첨부합니다.
5. 수신자에게 암호화된 메시지를 보냅니다.

참고 어플라이언스에서 PXE 및 S/MIME 암호화를 활성화하면 Email Security 어플라이언스가 먼저 S/MIME를 사용하여 메시지를 암호화한 다음 PXE를 사용합니다.

S/MIME를 사용하여 서명 또는 암호화 또는 서명 및 암호화를 수행하는 방법

단계	수행할 작업	추가 정보
1단계	S/MIME 인증서 요건을 숙지합니다.	S/MIME 인증서 요건, 19-19페이지를 참조하십시오.
2단계	사용자의 요건에 따라 다음 중 하나를 수행합니다. • S/MIME 서명의 경우 S/MIME 서명 인증서를 설정합니다. • S/MIME 암호화의 경우 수신자의 S/MIME 인증서 공개 키를 설정합니다. • S/MIME 서명 및 암호화의 경우 S/MIME 서명 인증서와 수신자의 S/MIME 인증서 공개 키를 각각 설정합니다.	참조: • S/MIME 서명 인증서 설정, 19-6페이지 • S/MIME 암호화에 사용할 공개 키 설정, 19-8페이지
3단계	메시지 서명 또는 암호화 또는 서명 및 암호화에 사용할 프로필을 생성합니다.	메시지 서명 또는 암호화 또는 전송 및 암호화에 사용할 S/MIME 전송 프로필 생성, 19-10페이지를 참조하십시오.
4단계	어플라이언스가 메시지 서명 또는 암호화 또는 서명 및 암호화를 수행할 수 있도록 메시지가 충족해야 하는 조건을 정의합니다.	서명 또는 암호화 또는 서명 및 암호화할 메시지 결정, 19-12페이지를 참조하십시오.
5단계	이메일 워크플로의 어느 단계에서 메시지 서명 또는 암호화 또는 서명 및 암호화를 수행할지 결정합니다.	참조: • 콘텐츠 필터를 사용하여 메시지를 전송한 직후에 메시지 서명 또는 암호화 또는 서명 및 암호화, 19-12페이지 • 콘텐츠 필터를 사용하여 전송할 때 메시지 서명 또는 암호화 또는 서명 및 암호화, 19-13페이지

단계	수행할 작업	추가 정보
6단계	메시지를 서명 또는 암호화할 사용자 그룹을 정의합니다.	메일 정책을 생성합니다. 10 장, "메일 정책" 참조
7단계	정의한 서명 또는 암호화 작업을 정의한 사용자 그룹과 연결합니다.	콘텐츠 필터를 메일 정책과 연결합니다. 10 장, "메일 정책" 참조

참고 CLI를 사용하여 S/MIME 서명 또는 암호화 또는 서명 및 암호화를 수행하려면 `smimeconfig` 명령을 사용합니다. *Cisco AsyncOS for Email CLI 참조 설명서*를 참조하십시오.

S/MIME 서명 인증서 설정

메시지에 서명하려면 S/MIME 인증서를 설정해야 합니다. Email Security 어플라이언스에서 다음 방법 중 하나를 사용하여 S/MIME 서명 인증서를 설정할 수 있습니다.

- 어플라이언스를 사용하여 자체 서명 S/MIME 인증서를 생성합니다. 자체 서명 S/MIME 인증서 생성, 19-6페이지를 참조하십시오.
- 기존 S/MIME 인증서를 어플라이언스로 가져옵니다. S/MIME 서명 인증서 가져오기, 19-7페이지를 참조하십시오.

참고 Cisco에서는 조직 내 또는 테스트 환경의 사용자에게 서명된 메시지를 보낼 경우 자체 서명 S/MIME 인증서를 사용할 것을 권장합니다. 외부 또는 프로덕션 환경의 사용자에게 서명된 메시지를 보낼 경우에는 신뢰할 수 있는 CA에서 발급된 유효한 S/MIME 인증서를 사용하는 것이 좋습니다.

S/MIME의 인증서 요건을 확인하려면 S/MIME 인증서 요건, 19-19페이지를 참조하십시오.

자체 서명 S/MIME 인증서 생성

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 Cisco에서는 조직 내 또는 테스트 환경의 사용자에게 서명된 메시지를 보낼 경우 자체 서명 S/MIME 인증서를 사용할 것을 권장합니다.

절차

1단계 **Network(네트워크) > Certificates(인증서)**를 클릭합니다.

2단계 **Add Certificate(인증서 추가)**를 클릭합니다.

3단계 **Create Self-Signed S/MIME Certificate(자체 서명 S/MIME 인증서 생성)**를 선택합니다.

4단계 다음과 같은 자체 서명 인증서 정보를 입력합니다.

공용 이름	정규화된 도메인 이름입니다.
조직	조직의 정확한 법적 이름입니다.

조직 단위	조직의 부문입니다.
군/구	조직이 법적으로 위치한 시/군/구입니다.
주/도:	조직이 법적으로 위치한 주, 도 또는 지역입니다.
국가	조직이 법적으로 위치한 국가의 ISO 약어(2자)입니다.
만료 전까지 기간	인증서가 만료되기 전 남은 일수입니다.
주체 대체 이름(도메인)	이 필드를 구성하면 지정된 도메인의 사용자가 서명된 메시지를 보낼 수 있습니다. 서명된 메시지를 보낼 도메인의 이름입니다. 예를 들어 `domain.com` 및 `*.domain.net` 등을 지정할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용합니다.
주체 대체 이름(이메일)	이 필드를 구성하면 지정된 사용자만 서명된 메시지를 보낼 수 있습니다. 예를 들어, 서명된 메시지를 보낼 사용자의 이메일 주소로 `user@somedomain.com`을 지정할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용합니다.
개인 키 크기	CSR(인증서 서명 요청)을 생성할 개인 키의 크기입니다.

참고 S/MIME 서명 인증서에는 주체 대체 이름(도메인)과 주체 대체 이름(이메일)이 모두 포함될 수 있습니다.

5단계 **Next(다음)**를 클릭하여 인증서 및 서명 정보를 확인합니다.

6단계 요건에 따라 다음을 수행합니다.

- 인증서의 이름을 입력합니다.
- 자체 서명 인증서의 CSR을 인증 기관에 제출하려면 **Download Certificate Signing Request(인증서 서명 요청 다운로드)**를 클릭하여 CSR을 로컬 또는 네트워크 머신에 PEM 형식으로 저장합니다.

7단계 변경 사항을 제출하고 커밋합니다.

참고 CLI에서 `certconfig` 명령을 사용하여 자체 서명 S/MIME 인증서를 생성합니다.

S/MIME 서명 인증서 가져오기

메시지 서명에 사용할 S/MIME 인증서가 이미 있는 경우 이 인증서를 가져와서 어플라이언스에 추가할 수 있습니다.

시작하기 전에

가져올 S/MIME 인증서가 S/MIME 인증서 요건, 19-19페이지에 설명된 요건을 충족하는지 확인합니다.

절차

1단계 **Network(네트워크)** > **Certificates(인증서)**를 클릭합니다.

2단계 **Add Certificate(인증서 추가)**를 클릭합니다.

3단계 **Import Certificate(인증서 가져오기)**를 선택합니다.

4단계 네트워크 또는 로컬 머신에 있는 인증서 파일에 대한 경로를 입력합니다.

5단계 파일의 비밀번호를 입력합니다.

6단계 **Next(다음)**를 클릭하여 인증서 정보를 확인합니다.

7단계 인증서의 이름을 입력합니다.

8단계 변경사항을 제출하고 커밋합니다.

참고 CLI에서 `certconfig` 명령을 사용하여 S/MIME 인증서를 가져옵니다.

S/MIME 암호화에 사용할 공개 키 설정

메시지를 암호화하려면 수신자의 S/MIME 인증서 공개 키를 어플라이언스에 추가해야 합니다. 조직의 정책과 프로세스에 따라 다음 방법 중 하나를 사용하여 공개 키를 어플라이언스에 추가할 수 있습니다.

- 수신자에게 이메일과 같은 전자 채널을 사용하여 공개 키를 전송하라고 요청합니다. 그런 다음 웹 인터페이스 또는 CLI를 사용하여 공개 키를 추가할 수 있습니다.

  공개 키 추가 지침은 S/MIME 암호화에 사용할 공개 키 추가, 19-8페이지를 참조하십시오.

- 웹 인터페이스 또는 CLI를 사용하여 공개 키 수집을 활성화하고 수신자에게 서명된 메시지를 전송하라고 요청합니다. Email Security 어플라이언스가 서명된 메시지에서 공개 키를 수집할 수 있습니다.

  서명된 수신 이메일에서 공개 키를 수집하는 방법에 대한 지침은 공개 키 수집, 19-9페이지를 참조하십시오.

S/MIME 암호화에 사용할 공개 키 추가

시작하기 전에

- 공개 키가 S/MIME 인증서 요건, 19-19페이지에서 명시된 요구 사항을 만족하는지 합니다.
- 공개 키가 EM 형식인지 확인합니다.

절차

1단계 **Mail Policies(메일 정책) > Public Keys(공개 키)**를 클릭합니다.

2단계 **Add Public Key(공개 키 추가)**를 클릭합니다.

3단계 공개 키의 이름을 입력합니다.

4단계 공개 키를 입력합니다.

5단계 변경사항을 제출하고 커밋합니다.

참고 `smimeconfig` 명령을 사용하여 CLI를 통해 공개 키를 추가할 수 있습니다.

공개 키 수집

수신 S/MIME 서명 메시지에서 공개 키를 검색(수집)하고 이를 사용하여 수집된 키의 소유자(기업 또는 소비자)에게 암호화된 메시지를 보내도록 Email Security 어플라이언스를 구성할 수 있습니다.

참고 기본적으로 만료되었거나 자체 서명된 S/MIME 인증서의 공개 키는 수집되지 않습니다.

시작하기 전에

발신자의 S/MIME 인증서 공개 키가 S/MIME 인증서 요건, 19-19페이지에 설명된 요건을 충족하는지 확인합니다.

절차

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

2단계 새 메일 흐름 정책을 생성하거나 기존 정책을 수정합니다. HAT(Host Access Table)를 사용하여 연결할 수 있는 호스트 정의, 7-1페이지를 참조하십시오.

3단계 아래로 스크롤하여 **Security Features(보안 기능)** 섹션으로 이동합니다.

4단계 S/MIME 공개 키 수집에서 다음을 수행합니다.

- S/MIME 공개 키 수집을 활성화합니다.
- (선택 사항) 서명된 수신 메시지 확인에 실패할 경우 공개 키를 수집할지 선택합니다.
- (선택 사항) 업데이트된 공개 키를 수집할지 선택합니다.

  참고 48시간 이내에 동일한 도메인 또는 메시지에서 2개 이상의 업데이트된 공개 키를 수신할 경우 어플라이언스가 경고 알림을 전송합니다.

5단계 변경 사항을 제출하고 커밋합니다.

참고 어플라이언스의 수집된 공개 키 저장소의 크기는 512MB입니다. 저장소가 꽉 차면 Email Security 어플라이언스가 사용되지 않은 공개 키를 자동으로 제거합니다.

참고 CLI에서 `listenerconfig` 명령을 사용하여 키 수집을 활성화합니다.

다음 단계

수신자에게 서명된 메시지를 Email Security 어플라이언스 관리자에게 전송하라고 요청합니다. Email Security 어플라이언스가 서명된 메시지에서 공개 키를 수집하고 이를 Mail Policies(메일 정책) > Harvested Public Keys(수집된 공개 키) 페이지에 표시합니다.

S/MIME 전송 프로필 관리

S/MIME 전송 프로필을 사용하여 다음과 같은 매개변수를 정의할 수 있습니다.

- 사용할 S/MIME 모드(예: 서명, 암호화 등)
- 서명에 사용할 S/MIME 인증서
- 사용할 S/MIME 서명 모드(예: 불투명 또는 분리됨)
- 어플라이언스에서 수신자의 S/MIME 인증서 공개 키를 사용할 수 없는 경우 수행할 작업

예를 들어, 한 조직은 전송되는 모든 메시지에 서명을 요구하고, 다른 조직은 전송되는 모든 메시지에 서명 및 암호화를 요구합니다. 이 시나리오에서는 2개의 전송 프로필을 생성해야 합니다(서명용 1개와 서명 및 암호화용 1개).

웹 또는 CLI를 사용하여 S/MIME 전송 프로필을 생성, 편집, 삭제, 가져오기, 내보내기 및 검색할 수 있습니다.

메시지 서명 또는 암호화 또는 전송 및 암호화에 사용할 S/MIME 전송 프로필 생성

절차

1단계 **Mail Policies(메일 정책) > Sending Profiles(전송 프로필)**를 클릭합니다.

2단계 **Add Profile(프로필 추가)**을 클릭합니다.

3단계 다음 필드를 구성합니다.

S/MIME 프로필 이름	전송 프로필의 이름을 입력합니다.
S/MIME 모드	S/MIME 모드를 선택합니다. 가능한 값은 다음과 같습니다. • **Sign** • **암호화** • **서명/암호화**. 서명한 다음 암호화합니다. • **3중**. 서명하고 암호화한 다음 다시 서명합니다 **참고** S/MIME 모드(**서명**, **서명/암호화** 또는 **3중**) 중 하나를 사용할 경우 서명에 실패하면 메시지가 발신자에게 바운스됩니다.
서명 인증서	사용할 서명 인증서를 선택합니다. **참고** S/MIME 모드(**서명**, **서명/암호화** 또는 **3중**) 중 하나를 선택할 경우에만 이 필드를 설정해야 합니다.

S/MIME 서명 모드	S/MIME 서명의 모드를 선택합니다. 가능한 값은 다음과 같습니다. • **불투명** 불투명 서명 메시지에는 메시지와 서명이 단일 부분으로 결합되어 있으며 서명을 확인해야만 읽을 수 있습니다. • **분리됨** 서명 정보가 서명할 텍스트에서 분리되어 있습니다. 이 MIME 유형은 멀티파트이거나 애플리케이션/(x-)pkcs7-서명의 MIME 하위 유형이 포함된 두 번째 부분으로 서명됩니다. **참고** S/MIME 모드(**서명**, **서명/암호화** 또는 **3중**) 중 하나를 선택할 경우에만 이 필드를 설정해야 합니다.
S/MIME 작업	수신자의 공개 키를 사용할 수 없을 경우 Email Security 어플라이언스가 수행해야 할 작업을 선택합니다. 가능한 값은 다음과 같습니다. • **바운스**. 수신자의 공개 키를 사용할 수 없는 경우 메시지가 발신자에게 바운스됩니다. • **삭제**. 수신자의 공개 키를 사용할 수 없는 경우 메시지가 삭제됩니다. • **분할**. 메시지가 분할됩니다. 공개 키를 사용할 수 없는 수신자에게는 메시지가 암호화되지 않은 상태로 전송되고, 공개 키를 사용할 수 있는 수신자에게는 메시지가 암호화되어 전송됩니다. **예**: bob@example1.com과 dave@example2.com에 메시지를 전송하고 dave@example2.com의 공개 키를 사용할 수 없다고 가정합니다. 이 시나리오에서 **분할**을 선택하면 Email Security 어플라이언스가 다음 작업을 수행합니다. – 메시지를 암호화한 후 bob@example1.com에 전송합니다. – 메시지를 암호화하지 않고 dave@example2.com에 전송합니다. **참고** S/MIME 모드(**암호화**, **서명/암호화** 또는 **3중**) 중 하나를 선택할 경우에만 이 필드를 설정해야 합니다.

4단계 변경 사항을 제출하고 커밋합니다.

참고 CLI에서 `smimeconfig` 명령을 사용하여 전송 프로필을 생성합니다.

S/MIME 전송 프로필 편집

1단계 **Mail Policies(메일 정책) > Sending Profiles(전송 프로필)**를 클릭합니다.

2단계 수정할 전송 프로필을 클릭합니다.

3단계 메시지 서명 또는 암호화 또는 전송 및 암호화에 사용할 S/MIME 전송 프로필 생성, 19-10페이지에 설명된 대로 필드를 편집합니다.

4단계 변경 사항을 제출하고 커밋합니다.

서명 또는 암호화 또는 서명 및 암호화할 메시지 결정

전송 프로필을 생성한 후 서명 또는 암호화 또는 서명 및 암호화해야 하는 이메일 메시지를 결정하는 발송 콘텐츠 필터를 생성해야 합니다. 콘텐츠 필터가 발송 이메일을 검사하고 메시지가 지정된 조건과 일치하는지 결정합니다. 콘텐츠 필터에서 메시지가 조건과 일치한다고 결정하면 Email Security 어플라이언스가 메시지를 서명 또는 암호화하거나 서명 및 암호화합니다.

관련 주제

- 콘텐츠 기준 메시지 필터링, 11-16페이지

콘텐츠 필터를 사용하여 메시지를 전송한 직후에 메시지 서명 또는 암호화 또는 서명 및 암호화

시작하기 전에

콘텐츠 필터의 구성 조건 개념을 이해합니다. 콘텐츠 필터 동작 방식, 11-1페이지를 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > Outgoing Content Filters(발송 콘텐츠 필터)**로 이동합니다.

2단계 필터 섹션에서 **Add Filter(필터 추가)**를 클릭합니다.

3단계 조건 섹션에서 **Add Condition(조건 추가)**을 클릭합니다.

4단계 서명 또는 암호화하거나 서명 및 암호화할 메시지를 필터링할 조건을 추가합니다. 예를 들어, 민감한 자료를 암호화하려면 제목 또는 본문에 "기밀"과 같은 특정 단어 또는 구문이 포함된 메시지를 식별하는 조건을 추가할 수 있습니다.

5단계 **OK(확인)**를 클릭합니다.

6단계 작업 섹션에서 **Add Action(작업 추가)**을 클릭합니다.

7단계 **Add Action(작업 추가)** 목록에서 **S/MIME Sign/Encrypt (Final Action)(S/MIME 서명/암호화(최종 작업))**를 선택합니다.

8단계 콘텐츠 필터와 연결할 전송 프로필을 선택합니다.

9단계 **OK(확인)**를 클릭합니다.

10단계 변경 사항을 제출하고 커밋합니다.

향후 작업

콘텐츠 필터를 추가한 후 해당 필터를 발송 메일 정책에 추가해야 합니다. 기본 정책에서 콘텐츠 필터를 활성화하거나 조직의 요구 사항에 따라 해당 필터를 특정 메일 정책에 적용하도록 선택할 수 있습니다. 메일 정책 사용에 대한 내용은 메일 정책 개요, 10-1페이지를 참조하십시오.

콘텐츠 필터를 사용하여 전송할 때 메시지 서명 또는 암호화 또는 서명 및 암호화

전송 시 메시지를 서명 또는 암호화 또는 서명 및 암호화할 콘텐츠 필터를 생성합니다. 다시 말해서, 메시지가 처리의 다음 단계를 계속 진행하고 모든 처리가 완료되면 메시지가 서명 또는 암호화 또는 서명 및 암호화되어 전송됩니다.

시작하기 전에

- 콘텐츠 필터의 구성 조건 개념을 이해합니다. 콘텐츠 필터 개요, 11-1페이지를 참조하십시오.

절차

1단계	**Mail Policies(메일 정책) > Outgoing Content Filters(발송 콘텐츠 필터)**로 이동합니다.
2단계	필터 섹션에서 **Add Filter(필터 추가)**를 클릭합니다.
3단계	조건 섹션에서 **Add Condition(조건 추가)**을 클릭합니다.
4단계	서명 또는 암호화하거나 서명 및 암호화할 메시지를 필터링할 조건을 추가합니다. 예를 들어, 민감한 자료를 암호화하려면 제목 또는 본문에 "기밀"과 같은 특정 단어 또는 구문이 포함된 메시지를 식별하는 조건을 추가할 수 있습니다.
5단계	**OK(확인)**를 클릭합니다.
6단계	작업 섹션에서 **Add Action(작업 추가)**을 클릭합니다.
7단계	**Add Action(작업 추가)** 목록에서 **S/MIME Sign/Encrypt on Delivery(전송 시 S/MIME 서명/암호화)**를 선택합니다.
8단계	콘텐츠 필터와 연결할 전송 프로필을 선택합니다.
9단계	**OK(확인)**를 클릭합니다.
10단계	변경 사항을 제출하고 커밋합니다.

향후 작업

콘텐츠 필터를 추가한 후 해당 필터를 발송 메일 정책에 추가해야 합니다. 기본 정책에서 콘텐츠 필터를 활성화하거나 조직의 요구 사항에 따라 해당 필터를 특정 메일 정책에 적용하도록 선택할 수 있습니다. 메일 정책 사용에 대한 내용은 메일 정책 개요, 10-1페이지를 참조하십시오.

S/MIME를 사용하여 수신 메시지 확인 또는 암호 해독 또는 암호 해독 및 확인

참고 Email Security 어플라이언스 S/MIME 보안 서비스를 사용하여 발송 및 수신 메시지를 확인 또는 암호 해독 또는 암호 해독 및 확인할 수 있습니다.

Email Security 어플라이언스의 S/MIME 확인 및 암호 해독 워크플로

S/MIME 확인 워크플로

다음 프로세스는 Email Security 어플라이언스가 S/MIME 확인을 수행하는 방식에 대해 설명합니다.

1. 서명된 메시지에 해시 알고리즘을 적용하여 메시지 다이제스트를 생성합니다.
2. 발신자의 S/MIME 인증서 공개 키를 사용하여 서명된 메시지에 연결된 PKCS7 서명의 암호를 해독하고 메시지 다이제스트를 가져옵니다.
3. 생성된 메시지 다이제스트와 서명된 메시지에서 검색한 메시지 다이제스트를 비교합니다. 메시지 다이제스트가 일치하면 메시지가 확인됩니다.

S/MIME 암호 해독 워크플로

다음 프로세스는 Email Security 어플라이언스가 S/MIME 암호 해독을 수행하는 방식에 대해 설명합니다.

1. 어플라이언스의 S/MIME 인증서 개인 키를 사용하여 세션 키의 암호를 해독합니다.
2. 세션 키를 사용하여 메시지 본문의 암호를 해독합니다.

S/MIME를 사용하여 수신 메시지를 확인 또는 암호 해독 또는 암호 해독 및 확인하는 방법

단계	수행할 작업	추가 정보
1단계	S/MIME 인증서 요건을 숙지합니다.	S/MIME 인증서 요건, 19-19페이지를 참조하십시오.
2단계	사용자의 요건에 따라 다음 중 하나를 수행합니다. • S/MIME 암호 해독의 경우 조직의 S/MIME 인증서(암호 해독을 수행하는 데 필요한 개인 키 포함)를 어플라이언스에 추가합니다. • S/MIME 확인의 경우 확인을 수행하는 데 필요한 발신자의 S/MIME 인증서 공개 키를 어플라이언스에 추가합니다. • S/MIME 암호 해독의 경우 다음 항목을 어플라이언스에 추가합니다. – 조직의 S/MIME 인증서(암호 해독을 수행하는 데 필요한 개인 키 포함)를 어플라이언스에 추가합니다. – 확인을 수행하는 데 필요한 발신자의 S/MIME 인증서 공개 키	참조: • 메시지 암호 해독에 사용할 인증서 설정, 19-15페이지 • 서명된 메시지 확인에 사용할 공개 키 설정, 19-16페이지
3단계	S/MIME를 사용하여 수신 메시지를 확인 또는 암호 해독 또는 암호 해독 및 확인하는 메일 흐름 정책을 구성합니다.	S/MIME 암호 해독 및 확인 활성화, 19-18페이지를 참조하십시오.
4단계	(선택 사항) Email Security 어플라이언스가 암호 해독 또는 확인된 메시지에 대해 수행할 작업을 정의합니다.	S/MIME 암호 해독 또는 확인 메시지에 대한 작업 구성, 19-19페이지를 참조하십시오.

참고 CLI에서 S/MIME 확인 또는 암호 해독 또는 암호 해독 및 확인을 수행하려면 `listenerconfig > hostaccess` 명령을 사용합니다. 자세한 내용은 CLI 인라인 도움말을 참조하십시오.

메시지 암호 해독에 사용할 인증서 설정

조직의 S/MIME 인증서(암호 해독을 수행하는 데 필요한 개인 키 포함)를 어플라이언스에 추가해야 합니다.

시작하기 전에

- 다음 방법 중 하나를 사용하여 어플라이언스의 S/MIME 인증서 공개 키를 발신자(기업 또는 소비자)와 공유합니다.
  - 이메일과 같은 전자 채널을 사용하여 공개 키를 전송합니다.
  - 발신자에게 키 수집을 사용하여 공개 키를 가져오라고 요청합니다.

  발신자가 이 공개 키를 사용하여 암호화된 메시지를 어플라이언스에 전송할 수 있습니다.

참고 B2C 시나리오에서는 조직의 S/MIME 인증서가 도메인 인증서일 경우 일부 이메일 클라이언트(예: Microsoft Outlook)가 조직의 S/MIME 인증서 공개 키를 사용하여 암호화된 메시지를 전송하지 못할 수 있습니다. 이는 이러한 이메일 클라이언트가 도메인 인증서의 공개 키를 사용하는 암호화를 지원하지 않기 때문입니다.

- 가져올 S/MIME 인증서가 S/MIME 인증서 요건, 19-19페이지에 설명된 요건을 충족하는지 확인합니다.

절차

1단계 **Network(네트워크) > Certificates(인증서)**를 클릭합니다.

2단계 **Add Certificate(인증서 추가)**를 클릭합니다.

3단계 **Import Certificate(인증서 가져오기)**를 선택합니다.

4단계 네트워크 또는 로컬 머신에 있는 인증서 파일에 대한 경로를 입력합니다.

5단계 파일의 비밀번호를 입력합니다.

6단계 **Next(다음)**를 클릭하여 인증서 정보를 확인합니다.

7단계 인증서의 이름을 입력합니다.

8단계 변경사항을 제출하고 커밋합니다.

참고 CLI에서 `certconfig` 명령을 사용하여 S/MIME 인증서를 추가합니다.

서명된 메시지 확인에 사용할 공개 키 설정

서명된 메시지를 확인하려면 발신자의 S/MIME 인증서 공개 키를 어플라이언스에 추가해야 합니다. 조직의 정책과 프로세스에 따라 다음 방법 중 하나를 사용하여 공개 키를 어플라이언스에 추가할 수 있습니다.

- 발신자에게 이메일과 같은 전자 채널을 사용하여 공개 키를 전송하라고 요청합니다. 그런 다음 웹 인터페이스 또는 CLI를 사용하여 공개 키를 추가할 수 있습니다.

  공개 키 추가 지침은 S/MIME 확인에 사용할 공개 키 추가, 19-16페이지를 참조하십시오.
- 키 수집을 사용하여 공개 키를 검색합니다. S/MIME 확인에 사용할 공개 키 수집, 19-17페이지를 참조하십시오.

S/MIME 확인에 사용할 공개 키 추가

시작하기 전에

- 공개 키가 S/MIME 인증서 요건, 19-19페이지에서 명시된 요구 사항을 만족하는지 합니다.
- 공개 키가 EM 형식인지 확인합니다.

절차

1단계 **Mail Policies(메일 정책) > Public Keys(공개 키)**를 클릭합니다.

2단계 **Add Public Key(공개 키 추가)**를 클릭합니다.

3단계 공개 키의 이름을 입력합니다.

4단계 공개 키를 입력합니다.

5단계 변경사항을 제출하고 커밋합니다.

참고 `smimeconfig` 명령을 사용하여 CLI를 통해 공개 키를 추가할 수 있습니다.

S/MIME 확인에 사용할 공개 키 수집

수신 S/MIME 서명 메시지에서 공개 키를 검색(수집)하고 이를 사용하여 수집된 키의 소유자(기업 또는 소비자)가 보낸 서명 메시지를 확인하도록 Email Security 어플라이언스를 구성할 수 있습니다.

참고 기본적으로 만료되었거나 자체 서명된 S/MIME 인증서의 공개 키는 수집되지 않습니다.

절차

1. 웹 인터페이스 또는 CLI를 사용하여 공개 키 수집을 활성화합니다. 공개 키 수집 활성화, 19-17 페이지를 참조하십시오.
2. 발신자에게 서명된 메시지를 전송하라고 요청합니다.
3. 수집이 완료된 후 수집된 공개 키를 어플라이언스에 추가합니다. S/MIME 확인에 사용할 수집된 공개 키 추가, 19-18페이지를 참조하십시오.

   이 단계는 메시지가 게이트웨이 수준에서 확인되도록 보장합니다.

공개 키 수집 활성화

절차

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

2단계 새 메일 흐름 정책을 생성하거나 기존 정책을 수정합니다. HAT(Host Access Table)를 사용하여 연결할 수 있는 호스트 정의, 7-1페이지를 참조하십시오.

3단계 아래로 스크롤하여 **Security Features(보안 기능)** 섹션으로 이동합니다.

4단계 S/MIME 공개 키 수집에서 다음을 수행합니다.

- S/MIME 공개 키 수집을 활성화합니다.
- (선택 사항) 서명된 수신 메시지 확인에 실패할 경우 공개 키를 수집할지 선택합니다.
- (선택 사항) 업데이트된 공개 키를 수집할지 선택합니다.

참고 48시간 이내에 동일한 도메인 또는 메시지에서 2개 이상의 업데이트된 공개 키를 수신할 경우 어플라이언스가 경고 알림을 전송합니다.

5단계 변경 사항을 제출하고 커밋합니다.

참고 어플라이언스의 수집된 공개 키 저장소의 크기는 512MB입니다. 저장소가 모두 사용되면 Email Security 어플라이언스가 사용되지 않은 공개 키를 자동으로 제거합니다.

참고 CLI에서 `listenerconfig` 명령을 사용하여 키 수집을 활성화합니다.

S/MIME 확인에 사용할 수집된 공개 키 추가

절차

1단계 **Mail Policies(메일 정책) > Harvested Public Keys(수집된 공개 키)**를 클릭합니다.

2단계 사용할 수집된 공개 키를 클릭하고 이를 복사합니다.

3단계 어플라이언스에 공개 키를 추가합니다. S/MIME 확인에 사용할 공개 키 추가, 19-16페이지를 참조하십시오.

4단계 변경 사항을 제출하고 커밋합니다.

S/MIME 암호 해독 및 확인 활성화

절차

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

2단계 새 메일 흐름 정책을 생성하거나 기존 정책을 수정합니다. HAT(Host Access Table)를 사용하여 연결할 수 있는 호스트 정의, 7-1페이지를 참조하십시오.

3단계 아래로 스크롤하여 **Security Features(보안 기능)** 섹션으로 이동합니다.

4단계 S/MIME 암호 해독/확인에서 다음을 수행합니다.

- S/MIME 암호 해독 및 확인을 활성화합니다.
- S/MIME 확인 후 메시지의 디지털 서명을 유지할지 또는 제거할지 선택합니다. 최종 사용자가 S/MIME 게이트웨이 확인에 대해 아는 것을 원하지 않을 경우 **Remove(제거)**를 선택합니다.

  3중으로 래핑된 메시지의 경우 내부 서명만 유지 또는 제거됩니다.

5단계 변경 사항을 제출하고 커밋합니다.

정보 메일 흐름 정책에서 S/MIME 암호 해독 및 확인이 활성화된 경우 암호 해독 및 확인의 상태와 관계없이 모든 S/MIME 메시지가 전송됩니다. S/MIME 암호 해독 또는 확인 메시지에 대해 수행할 작업을 구성하려면 메시지 필터 규칙 `smime-gateway-verified` 및 `smime-gateway`를 사용할 수 있습니다. 자세한 내용은 S/MIME 암호 해독 또는 확인 메시지에 대한 작업 구성, 19-19페이지를 참고하십시오.

S/MIME 암호 해독 또는 확인 메시지에 대한 작업 구성

Email Security 어플라이언스가 S/MIME 암호 해독, 확인 또는 둘 다를 수행한 후 결과에 따라 다양한 작업을 수행할 수 있습니다. 메시지 필터 규칙 `smime-gateway-verified` 및 `smime-gateway`를 사용하여 암호 해독, 확인 또는 둘 다의 결과에 따라 메시지에 대해 작업을 수행할 수 있습니다. 자세한 내용은 9 장, "메시지 필터를 사용하여 이메일 정책 적용"을 참조하십시오.

참고 콘텐츠 필터 조건 **S/MIME Gateway Message** 및 **S/MIME Gateway Verified**를 사용하여 암호 해독, 확인 또는 둘 다의 결과에 따라 메시지에 대해 작업을 수행할 수 있습니다. 자세한 내용은 11 장, "콘텐츠 필터"를 참조하십시오.

예: 확인, 암호 해독 또는 둘 다에 실패한 S/MIME 메시지 격리

다음 메시지 필터는 메시지가 S/MIME 메시지인지 확인하고 S/MIME를 사용한 확인 또는 암호 해독에 실패할 경우 메시지를 격리합니다.

```
quarantine_smime_messages:if (smime-gateway-message and not smime-gateway-verified) {
quarantine("Policy"); }
```

S/MIME 인증서 요건

서명에 대한 인증서 요건

서명에 사용할 S/MIME 인증서는 다음 정보를 포함해야 합니다.

공용 이름	정규화된 도메인 이름입니다.
조직	조직의 정확한 법적 이름입니다.
조직 단위	조직의 부문입니다.
군/구	조직이 법적으로 위치한 시/군/구입니다.
주/도:	조직이 법적으로 위치한 주, 도 또는 지역입니다.
국가	조직이 법적으로 위치한 국가의 ISO 약어(2자)입니다.
만료 전까지 기간	인증서가 만료되기 전 남은 일수입니다.
주체 대체 이름(도메인)	서명된 메시지를 보낼 도메인의 이름입니다. 예를 들어 `domain.com` 및 `*.domain.net` 등을 지정할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용합니다.

주체 대체 이름(이메일)	예를 들어, 서명된 메시지를 보낼 사용자의 이메일 주소로 user@somedomain.com을 지정할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용합니다.
개인 키 크기	CSR에 대해 생성할 개인 키의 크기입니다.
키 사용	키 사용은 인증서의 용도를 결정하는 제한 방법입니다. 키 사용 확장이 지정된 경우 digitalSignature 및 nonRepudiation 비트를 설정해야 합니다. 키 사용 확장이 지정되지 않은 경우 수신 클라이언트가 digitalSignature 및 nonRepudiation 비트가 설정되었다고 간주해야 합니다.

S/MIME 인증서에 대한 자세한 내용은 RFC 5750: S/MIME(Secure/Multipurpose Internet Mail Extensions) 버전 3.2 - 인증서 처리를 참조하십시오.

암호화에 대한 인증서 요건

암호화에 사용할 S/MIME 인증서는 다음 정보를 포함해야 합니다.

공용 이름	정규화된 도메인 이름입니다.
조직	조직의 정확한 법적 이름입니다.
조직 단위	조직의 부문입니다.
군/구	조직이 법적으로 위치한 시/군/구입니다.
주/도:	조직이 법적으로 위치한 주, 도 또는 지역입니다.
국가	조직이 법적으로 위치한 국가의 ISO 약어(2자)입니다.
만료 전까지 기간	인증서가 만료되기 전 남은 일수입니다.
주체 대체 이름(도메인)	암호화된 메시지를 보낼 도메인의 이름입니다. 예를 들어 domain.com 및 *.domain.net 등을 지정할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용합니다. 도메인의 모든 사용자에게 암호화된 메시지를 보내려면 공개 키에 SAN 도메인이 포함되어야 합니다.
주체 대체 이름(이메일)	예를 들어, 암호화된 메시지를 보낼 사용자의 이메일 주소로 user@somedomain.com을 지정할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분된 목록을 사용합니다.
개인 키 크기	CSR에 대해 생성할 개인 키의 크기입니다.
키 사용	키 사용은 인증서의 용도를 결정하는 제한 방법입니다. 키 사용 확장을 지정하고 keyEncipherment 비트를 설정해야 합니다.

S/MIME 인증서에 대한 자세한 내용은 RFC 5750: S/MIME(Secure/Multipurpose Internet Mail Extensions) 버전 3.2 - 인증서 처리를 참조하십시오.

시작하기 전에

- 공개 키가 S/MIME 인증서 요건, 19-19페이지에서 명시된 요구 사항을 만족하는지 합니다.
- 공개 키가 EM 형식인지 확인합니다.

절차

1단계 **Mail Policies(메일 정책) > Public Keys(공개 키)**를 클릭합니다.

2단계 **Add Public Key(공개 키 추가)**를 클릭합니다.

3단계 공개 키의 이름을 입력합니다.

4단계 공개 키를 입력합니다.

5단계 변경사항을 제출하고 커밋합니다.

참고 `smimeconfig` 명령을 사용하여 CLI를 통해 공개 키를 추가할 수 있습니다.

시작하기 전에

어플라이언스의 `/configuration` 디렉토리에 내보내기 파일을 복사합니다. 내보내기 파일 생성에 관한 지침은 공개 키 내보내기, 19-21페이지 항목을 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > Public Keys(공개 키)**를 클릭합니다.

2단계 **Import Public Keys(공개 키 가져오기)**를 클릭합니다.

3단계 내보내기 파일을 선택하고 **Submit(제출)**을 클릭합니다.

참고 많은 공개 키가 있는 파일을 가져오는 경우 가져오는 시간이 더 오래 걸릴 수 있습니다. 이에 따라 웹 인터페이스 또는 CLI 비활성 시간 제한을 조정합니다.

4단계 변경사항을 커밋합니다.

공개 키 내보내기

어플라이언스의 모든 공개 키는 단일 텍스트 파일로 내보내고 `/configuration` 디렉토리에 저장됩니다.

절차

1단계 **Mail Policies(메일 정책) > Public Keys(공개 키)**를 선택합니다.

2단계 **Export Public Keys(공개 키 내보내기)**를 클릭합니다.

3단계 파일의 이름을 입력하고 **Submit(제출)**을 클릭합니다.

20 장

이메일 인증

이메일 인증 개요

AsyncOS for Email은 이메일 위조를 방지하기 위해 이메일 확인 및 서명을 지원합니다. 수신 메일을 확인하기 위해 AsyncOS는 SPF(Sender Policy Framework), SIDF(Sender ID Framework), DKIM(DomainKeys Identified Mail) 및 DMARC(Domain-based Message Authentication, Reporting and Conformance)를 지원합니다. 아웃바운드 메일을 인증하기 위해 AsyncOS는 DomainKeys 및 DKIM 서명을 지원합니다.

관련 주제

- DomainKeys 및 DKIM 인증, 20-1페이지.
- SPF 및 SIDF 확인 개요, 20-22페이지.
- DMARC 확인, 20-35페이지

DomainKeys 및 DKIM 인증

DomainKeys 또는 DKIM 이메일 인증을 통해 발신자는 공개 키 암호화를 사용하여 이메일에 로그인합니다. 확인된 도메인을 사용하여 이메일의 From:(또는 Sender:) 헤더에서 도메인과 비교하여 위조를 탐지할 수 있습니다.

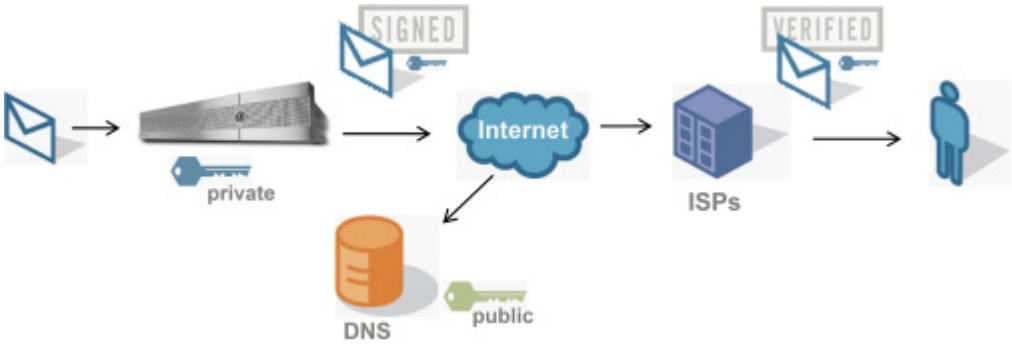
DomainKeys 및 DKIM은 두 가지 주요 파트, 즉 서명 및 확인으로 구성됩니다. AsyncOS는 DomainKeys 절차의 절반에 해당하는 "서명" 기능을 지원하며 DKIM에 대한 서명 및 확인을 모두 지원합니다. 또한 바운스 및 지연 메시지를 활성화하여 DomainKeys 및 DKIM 서명을 사용할 수 있습니다.

관련 주제

- DomainKeys 및 DKIM 인증 워크플로, 20-2페이지
- AsyncOS에서의 DomainKeys 및 DKIM 서명, 20-2페이지

DomainKeys 및 DKIM 인증 워크플로

그림 20-1 인증 워크플로



1. 관리자(도메인 소유자)는 공개 키를 DNS 네임스페이스에 게시합니다.
2. 관리자는 아웃바운드 메일 전송 에이전트(MTA)에 개인 키를 로드합니다.
3. 해당 도메인의 권한 있는 사용자가 제출한 이메일은 해당 개인 키를 사용하여 디지털 서명됩니다. DomainKey 또는 DKIM 서명 헤더로 이메일에 서명이 삽입된 후 이메일이 전송됩니다.
4. MTA를 수신하면 헤더에서 DomainKeys 또는 DKIM 서명을 추출하고 이메일에서 Sender: 또는 From: 헤더를 통해 요청된 전송 도메인을 추출합니다. DomainKeys 또는 DKIM 서명 헤더 필드에서 추출한 요청 서명 도메인에서 공개 키를 검색합니다.
5. 공개 키는 해당 개인 키로 DomainKeys 또는 DKIM 서명이 생성되었는지 여부를 확인하는 데 사용됩니다.

발송 DomainKeys 서명을 테스트하기 위해 Yahoo! 또는 Gmail 주소를 사용할 수 있습니다. 이러한 서비스는 무료이며 DomainKeys로 서명된 수신 메시지에 대한 유효성 검사를 제공합니다.

AsyncOS에서의 DomainKeys 및 DKIM 서명

AsyncOS의 DomainKeys 및 DKIM 서명은 도메인 프로파일을 통해 구현되며 메일 흐름 정책(일반적으로 발송 "릴레이" 정책)을 통해 활성화됩니다. 자세한 내용은 "메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오. 메시지 서명은 메시지를 전송하기 전에 어플라이언스에서 수행하는 마지막 작업입니다.

도메인 프로파일은 도메인을 도메인 키 정보(서명 키 및 관련 정보)와 연결합니다. 어플라이언스에서 메일 흐름 정책을 통해 이메일을 전송하므로 도메인 프로파일과 일치하는 발신자 이메일 주소는 도메인 프로파일에서 지정한 서명 키로 DomainKeys 서명됩니다. DKIM과 DomainKeys 서명 모두를 활성화하는 경우 DKIM 서명이 사용됩니다. `domainkeysconfig` CLI 명령 또는 GUI의 Mail Policies(메일 정책) > Domain Profiles(도메인 프로파일) 및 Mail Policies(메일 정책) > Signing Keys(서명 키) 페이지에서 DomainKeys 및 DKIM 프로파일을 구현합니다.

DomainKeys 및 DKIM 서명은 다음과 같이 작용합니다. 도메인 소유자는 키 두 개, 즉 공용 DNS(해당 도메인과 연결된 DNS TXT 레코드)에 저장된 공개 키와 해당 도메인에서 전송한 메일의 서명에 사용되는 어플라이언스에 저장된 개인 키를 생성합니다.

메시지를 전송(아웃바운드)하는 데 사용된 리스너에서 메시지를 수신하면서 어플라이언스는 도메인 프로파일이 있는지 여부를 확인합니다. 어플라이언스에서 생성되고 메일 흐름 정책에 구현된 도메인 프로파일이 있는 경우 유효한 Sender: 또는 From: 주소에 대한 메시지가 검사됩니다. 모두 있는 경우 Sender:가 DomainKeys에 사용됩니다. From: 주소는 항상 DKIM 서명에 사용됩니다. 또는 첫 번째 From: 주소가 사용됩니다. 유효한 주소가 없으면 메시지가 서명되지 않으며 이벤트가 mail_logs에 기록됩니다.

참고 DomainKey와 DKIM 프로파일을 모두 생성하고 메일 흐름 정책에서 서명을 활성화하는 경우 AsyncOS는 DomainKeys 및 DKIM 서명을 모두 사용하여 발송 메시지에 서명합니다.

유효한 발신 주소가 있으면 발신 주소와 기존의 도메인 프로파일을 대조합니다. 일치하는 항목이 있는 경우 메시지가 서명됩니다. 일치하는 항목이 없는 경우 메시지가 서명 없이 전송됩니다. 메시지에 기존 DomainKeys("DomainKey-Signature:" 헤더)가 있으면, 원본 서명 후 새로운 발신자 주소가 추가된 경우에만 메시지에 서명. 메시지에 기존 DKIM 서명이 있는 경우 새 DKIM 서명이 메시지에 추가됩니다.

AsyncOS는 서명 키를 관리(새로 만들거나 기존 키를 입력)하는 방법과 더불어 도메인을 기반으로 한 이메일 서명 메커니즘을 제공합니다.

이 문서의 구성 설명은 서명 및 확인에 대한 가장 일반적인 사용 방법을 제공합니다. 인바운드 이메일에 대해 메일 흐름 정책에서 DomainKeys 및 DKIM 서명을 활성화하거나 아웃바운드 이메일에 대해 메일 흐름 정책에서 DKIM 확인을 활성화할 수 있습니다.

참고 클러스터된 환경에서 도메인 프로파일 및 서명 키를 구성하는 경우 도메인 키 프로파일 설정 및 서명 키 설정이 연결되어 있으므로 주의해야 합니다. 따라서 서명 키를 복사, 이동 또는 삭제하는 경우 관련된 프로파일에 동일한 작업이 수행됩니다.

DomainKeys 및 DKIM 서명 구성

관련 주제

- 서명 키, 20-4페이지
- 공개 키, 20-4페이지
- 도메인 프로파일, 20-5페이지
- 발송 메일에 서명 활성화, 20-6페이지
- 바운스 및 지연 메시지에 서명 활성화, 20-6페이지
- DomainKeys/DKIM 서명 구성(GUI), 20-7페이지
- 도메인 키 및 로깅, 20-16페이지

서명 키

서명 키는 어플라이언스에 저장된 개인 키입니다. 서명 키를 만들 때 키 크기를 지정합니다. 크기가 큰 키가 안전하지만 이러한 키를 사용하면 성능에 영향을 줄 수 있습니다. 어플라이언스는 512비트에서 최대 2,048비트의 키를 지원합니다. 768~1,024비트 키가 안전하다고 간주되며 현재 대부분의 발신자가 사용합니다. 크기가 큰 키는 성능에 영향을 줄 수 있으며 2,048비트가 넘는 키는 지원되지 않습니다. 서명 키 생성에 대한 자세한 내용은 서명 키 생성 또는 편집, 20-10페이지 항목을 참조하십시오.

기존 키를 입력하는 경우 해당 양식에 붙이기만 하면 됩니다. 기존 서명 키를 사용하는 또 다른 방법은 키를 텍스트 파일로 가져오는 것입니다. 기존 서명 키 추가에 대한 자세한 내용은 기존 서명 키 가져오기 또는 입력하기, 20-11페이지 항목을 참조하십시오.

키가 입력되면 도메인 프로파일에 사용할 수 있으며 도메인 프로파일의 서명 키 드롭다운 목록에 나타납니다.

관련 주제

- 서명 키 내보내기 및 가져오기, 20-4페이지

서명 키 내보내기 및 가져오기

서명 키를 어플라이언스에 텍스트 파일로 내보낼 수 있습니다. 키를 내보낼 때 현재 어플라이언스에 있는 모든 키가 텍스트 파일로 저장됩니다. 키 내보내기에 대한 자세한 내용은 서명 키 내보내기, 20-11페이지 항목을 참조하십시오.

내보낸 키를 가져올 수도 있습니다.

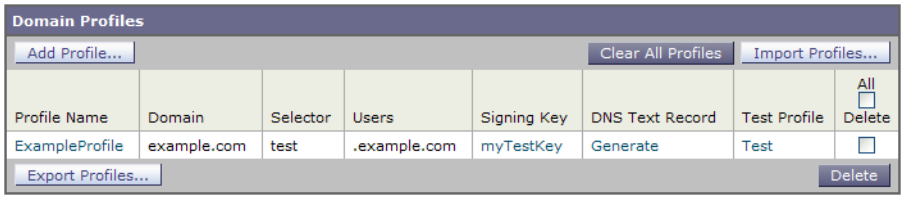
참고 키를 가져오면 현재 어플라이언스에 있는 모든 키가 교체됩니다.

자세한 내용은 기존 서명 키 가져오기 또는 입력하기, 20-11페이지 항목을 참조하십시오.

공개 키

서명 키를 도메인 프로파일과 연결하면 공개 키를 포함하는 DNS Text Record를 생성할 수 있습니다. 도메인 프로파일 목록의 DNS Text 레코드 열에 있는 Generate(생성) 링크를 통해 만들 수 있습니다(또는 CLI의 `domainkeysconfig -> profiles -> dnstxt`).

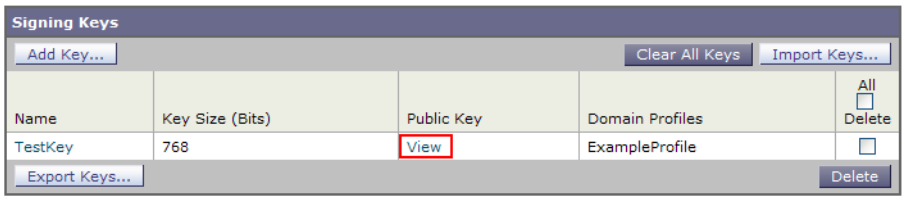
그림 20-2 도메인 프로파일 페이지에서 DNS Text Record 링크 생성



DNS Text Record 생성에 관한 자세한 내용은 DNS Text Record 생성, 20-13페이지 항목을 참조하십시오.

Signing Keys(서명 키) 페이지의 View(보기) 링크를 통해 공개 키를 확인할 수도 있습니다.

그림 20-3 서명 키 페이지에서 공개 키 링크 보기



도메인 프로파일

도메인 프로파일은 서명에 필요한 일부 기타 정보와 더불어 발신자 도메인을 서명 키와 연결합니다.

- 도메인 프로파일의 이름.
- 도메인 이름("d=" 헤더에 포함되는 도메인).
- 선택기(선택기는 공개 키의 쿼리를 구성하는 데 사용됩니다. DNS 쿼리 유형에서는 이 값을 발신 도메인의 "_domainkey." 네임스페이스 앞에 추가합니다).
- 정형화 방법(서명 알고리즘에 대한 헤더 및 콘텐츠의 프레젠테이션을 준비하는 방식). AsyncOS는 Domainkeys에 "simple" 및 "nofws"를 지원하며 DKIM에는 "relaxed" 및 "simple"을 지원합니다.
- 서명 키(자세한 내용은 서명 키, 20-4페이지 참조).
- 헤더 목록 및 서명할 본문 길이(DKIM만 해당).
- 서명 헤더에 포함할 태그 목록(DKIM만 해당). 이러한 태그에는 다음 정보가 저장됩니다.
  - 메시지 서명을 대신하는 사용자 또는 에이전트(예: 메일 목록 관리자)의 ID.
  - 공개 키를 검색하는 데 사용되는 콤마로 구분된 쿼리 방법 목록.
  - 서명이 생성된 시간을 나타내는 타임스탬프.
  - 서명의 만료 시간(초).
  - 메시지가 서명되었을 때 나타나는 세로 막대(예: |)로 구분된 헤더 필드 목록.
- 서명에 포함할 태그(DKIM만 해당).
- 프로파일 사용자 목록(서명에 도메인 프로파일 사용이 허용된 주소).

참고 프로파일 사용자에 지정된 주소의 도메인은 도메인 필드에 지정된 도메인과 일치해야 합니다.

특정 조건으로 기존의 모든 도메인 프로파일을 검색할 수 있습니다. 자세한 내용은 도메인 프로파일 검색, 20-15페이지 항목을 참조하십시오.

시스템에서 생성한 메시지에 DKIM 서명 사용 여부를 선택할 수도 있습니다. 자세한 내용은 시스템에서 생성한 메시지 서명, 20-15페이지 항목을 참조하십시오.

관련 주제

- 도메인 프로파일 내보내기 및 가져오기, 20-6페이지

도메인 프로파일 내보내기 및 가져오기

기존 도메인 프로파일을 어플라이언스에 텍스트 파일로 내보낼 수 있습니다. 도메인 프로파일을 내보낼 때 어플라이언스에 있는 기존의 모든 프로파일이 단일 텍스트 파일로 저장됩니다. 도메인 프로파일 내보내기, 20-14페이지 항목을 참조하십시오.

이전에 내보낸 도메인 프로파일을 가져올 수 있습니다. 도메인 프로파일을 가져오면 현재 머신에 있는 모든 도메인 프로파일이 교체됩니다. 도메인 프로파일 가져오기, 20-14페이지 항목을 참조하십시오.

발송 메일에 서명 활성화

DomainKeys 및 DKIM 서명은 아웃바운드 메일의 메일 흐름 정책에서 활성화됩니다. 자세한 내용은 "메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

절차

1단계 Mail Flow Policies(메일 흐름 정책) 페이지(Mail Policies(메일 정책) 메뉴 아래)에서 RELAYED 메일 흐름 정책(발송)을 클릭합니다.

2단계 Security Features(보안 기능) 섹션에서 On(켜기)을 선택하여 DomainKeys/DKIM 서명을 활성화합니다.

3단계 변경사항을 제출하고 커밋합니다.

바운스 및 지연 메시지에 서명 활성화

아웃바운드 메시지 서명 외에도 바운스 및 지연 메시지에 서명할 수 있습니다. 이를 통해 회사에서 받는 바운스 및 지연 메시지가 정상적인 메시지임을 수신자에게 알릴 수 있습니다. 바운스 및 지연 메시지에 DomainKeys 및 DKIM 서명을 활성화하려면 공용 리스너와 연결된 바운스 프로파일의 DomainKeys/DKIM 서명을 활성화합니다.

절차

1단계 서명된 아웃바운드 메시지를 보낼 공용 리스너와 연결된 바운스 프로파일에서 Hard Bounce and Delay Warning Messages(하드 바운스 및 지연 경고 메시지)로 이동합니다.

2단계 "Use Domain Key Signing for Bounce and Delay Messages(바운스 및 지연 메시지에 Domain Key 서명 사용)"를 활성화합니다.

참고 DomainKeys/DKIM 서명 구성(GUI), 20-7페이지에 나열된 모든 단계를 완료하여 바운스 및 지연 메시지에 서명해야 합니다.

참고 도메인 프로파일의 From: 주소는 바운스 반환 주소에 사용된 주소와 일치해야 합니다. 이러한 주소를 일치시키기 위해 바운스 프로파일에서 반환 주소를 구성(System Administration(시스템 관리) > Return Addresses(반환 주소))한 다음 도메인 프로파일의 Profile Users(프로파일 사용자) 목록에서 동일한 이름을 사용할 수 있습니다. 예를 들어 바운스 반환 주소를 MAILER-DAEMON@example.com으로 구성하고 도메인 프로파일에서 프로파일 사용자로 MAILER-DAEMON@example.com을 추가합니다.

DomainKeys/DKIM 서명 구성(GUI)

절차

1단계 새로운 키를 만들거나 기존의 개인 키를 가져옵니다. 서명 키 생성 또는 가져오기에 대한 자세한 내용은 서명 키, 20-4페이지 항목을 참조하십시오.

2단계 도메인 프로파일을 만들고 키를 도메인 프로파일과 연결합니다. 도메인 프로파일 생성에 대한 자세한 내용은 도메인 프로파일, 20-5페이지 항목을 참조하십시오.

3단계 DNS Text Record를 생성합니다. DNS Text Record 생성에 대한 자세한 내용은 DNS Text Record 생성, 20-13페이지 항목을 참조하십시오.

4단계 이렇게 하지 않은 경우 아웃바운드 메일의 메일 흐름 정책에서 DomainKeys/DKIM 서명을 활성화합니다(발송 메일에 서명 활성화, 20-6페이지 참조).

5단계 선택적으로 바운스 및 지연 메시지에 DomainKeys/DKIM 서명을 활성화합니다. 바운스 및 지연 메시지의 서명 활성화에 대한 자세한 내용은 바운스 및 지연 메시지에 서명 활성화, 20-6페이지 항목을 참조하십시오.

6단계 이메일을 보냅니다. 도메인 프로파일과 일치하는 도메인에서 보낸 메일은 DomainKeys/DKIM으로 서명됩니다. 또한 바운스 및 지연 메시지에 대한 서명을 활성화한 경우 바운스 또는 지연 메시지가 서명됩니다.

참고 DomainKey와 DKIM 프로파일을 모두 생성하고 메일 흐름 정책에서 서명을 활성화하는 경우 AsyncOS는 DomainKeys 및 DKIM 서명을 모두 사용하여 발송 메시지에 서명합니다.

관련 주제

- DomainKeys 서명에 대한 도메인 프로파일 생성, 20-8페이지
- DKIM 서명에 새 도메인 프로파일 생성, 20-8페이지
- 서명 키 생성 또는 편집, 20-10페이지
- 서명 키 내보내기, 20-11페이지
- 기존 서명 키 가져오기 또는 입력하기, 20-11페이지
- 서명 키 삭제, 20-12페이지
- DNS Text Record 생성, 20-13페이지
- 도메인 프로파일 테스트, 20-14페이지
- 도메인 프로파일 내보내기, 20-14페이지

- 도메인 프로파일 가져오기, 20-14페이지
- 도메인 프로파일 삭제, 20-14페이지
- 도메인 프로파일 검색, 20-15페이지
- 시스템에서 생성한 메시지 서명, 20-15페이지

DomainKeys 서명에 대한 도메인 프로파일 생성

절차

1단계 **Mail Policies(메일 정책) > Signing Profile(서명 프로파일)**을 선택합니다.

2단계 **Domain Signing Profiles(도메인 서명 프로파일)** 섹션에서 **Add Profile(프로파일 추가)**을 클릭합니다.

3단계 프로파일의 이름을 입력합니다.

4단계 **Domain Key Type(도메인 키 유형)**에서 **Domain Keys(메인 키)** 선택합니다.

추가 옵션이 페이지에 나타납니다.

5단계 도메인 이름을 입력합니다.

6단계 선택기를 입력합니다. 선택기는 "_domainkey" 네임스페이스 앞에 추가된 임의의 이름이며 각각의 전송 도메인에 다수의 동시 공개 키를 지원합니다. 선택기 값과 길이는 DNS 네임스페이스와 이메일 헤더 조건에 부합해야 하며 세미콜론을 포함할 수 없다는 추가 조건을 만족해야 합니다.

7단계 정형화를 선택합니다(공백 또는 simple 전송 안함).

8단계 이미 서명 키를 생성한 경우 서명 키를 선택합니다. 서명 키가 생성되지 않은 경우 다음 단계로 건너뜁니다. 목록에서 선택할 서명 키가 있으려면 하나 이상의 서명 키를 생성하거나 가져와야 합니다. 서명 키 생성 또는 편집, 20-10페이지 항목을 참조하십시오.

9단계 서명에 도메인 프로파일을 사용할 사용자(이메일 주소, 호스트 등)를 입력합니다.

10단계 변경사항을 제출하고 커밋합니다.

11단계 이 시점에서 이를 수행하지 않은 경우 발송 메일 흐름 정책에서 DomainKeys/DKIM 서명을 활성화해야 합니다(발송 메일에 서명 활성화, 20-6페이지 참조).

참고 DomainKeys 및 DKIM 프로파일을 모두 생성하는 경우 AsyncOS는 발송 메일에 DomainKeys 및 DKIM 서명을 모두 수행합니다.

DKIM 서명에 새 도메인 프로파일 생성

절차

1단계 **Mail Policies(메일 정책) > Signing Profile(서명 프로파일)**을 선택합니다.

2단계 **Domain Signing Profiles(도메인 서명 프로파일)** 섹션에서 **Add Profile(프로파일 추가)**을 클릭합니다.

3단계 프로파일의 이름을 입력합니다.

4단계 **Domain Key Type(도메인 키 유형)**에서 **DKIM**을 선택합니다.

추가 옵션이 페이지에 나타납니다.

5단계 도메인 이름을 입력합니다.

6단계 선택기를 입력합니다. 선택기는 "_domainkey" 네임스페이스 앞에 추가된 임의의 이름이며 각각의 전송 도메인에 다수의 동시 공개 키를 지원합니다. 선택기 값과 길이는 DNS 네임스페이스와 이메일 헤더 조건에 부합해야 하며 세미콜론을 포함할 수 없다는 추가 조건을 만족해야 합니다.

7단계 헤더에 대한 정형화를 선택합니다. 다음 옵션 중에서 선택합니다.

- **Relaxed**. "Relaxed" 헤더 정형화 알고리즘은 다음을 수행합니다. 헤더 이름이 소문자로 변경되고, 헤더가 펼쳐지고, 선형 공백이 단일 공백으로 축소되고, 선행 및 후행 공백이 제거됩니다.
- **Simple**. 헤더가 변경되지 않습니다.

8단계 본문에 대해 정형화를 선택합니다. 다음 옵션 중에서 선택합니다.

- **Relaxed**. "relaxed" 헤더 정형화 알고리즘은 다음을 수행합니다. 비어 있는 줄은 본문 맨 끝에서 제거되며, 공백은 줄 안의 단일 공백으로 축소되고, 후행 공백이 줄에서 제거됩니다.
- **Simple.** 본문 끝의 비어 있는 줄이 제거됩니다.

9단계 이미 서명 키를 생성한 경우 서명 키를 선택합니다. 서명 키가 생성되지 않은 경우 다음 단계로 건너뜁니다. 목록에서 선택할 서명 키가 있으려면 하나 이상의 서명 키를 생성하거나 가져와야 합니다. 서명 키 생성 또는 편집, 20-10페이지 항목을 참조하십시오.

10단계 서명할 헤더 목록을 선택합니다. 다음 헤더에서 선택할 수 있습니다.

- **All**. AsyncOS는 서명 시 표시되는 모든 헤더에 서명합니다. All 헤더에 서명하면 전송 중에 헤더가 추가 또는 제거되지 않습니다.
- **Standard**. Standard 헤더를 선택하면 전송 중에 헤더가 추가 또는 제거될 수도 있습니다. AsyncOS는 다음의 Standard 헤더에만 서명합니다(헤더가 메시지에 표시되지 않는 경우 DKIM 서명이 헤더에 대해 null 값을 표시합니다).
  - 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 선택하면 서명할 추가 헤더를 추가할 수 있습니다.

11단계 메시지 본문이 서명되는 방법을 지정합니다. 메시지 본문이 서명되도록 선택하거나 서명할 크기(바이트)를 선택할 수 있습니다. 다음 옵션 중 하나를 선택합니다.

- **전체 본문 함축**. 본문 길이를 결정하려면 "l=" 태그를 사용하지 않습니다. 전체 메시지가 서명되며 변경되지 않습니다.
- **전체 본문 자동 확인됨**. 전체 메시지 본문이 서명되며 전송 시 본문 끝에 일부 추가 데이터를 첨부하는 것이 허용됩니다.
- **Sign first _ bytes.** 지정된 바이트만큼 메시지 본문이 서명됩니다.

12단계 메시지 서명의 헤더 필드에 포함할 태그를 선택합니다. 이러한 태그에 저장된 정보는 메시지 서명 확인에 사용됩니다. 다음 옵션 중 하나 이상을 선택합니다.

- **"i" 태그**. 이 메시지 서명을 대신하는 사용자 또는 에이전트(예: 메일 목록 관리자)의 ID. @ 기호가 앞에 추가된 도메인 이름(예: @example.com)을 입력합니다.
- **"q" 태그**. 공개 키를 검색하는 데 사용되는 콜론으로 구분된 쿼리 방법 목록. 현재 사용할 수 있는 유일한 값은 dns/txt입니다.
- **"t" 태그**. 서명이 생성된 시간을 나타내는 타임스탬프.
- **"x" 태그**. 서명이 만료되는 절대 날짜 및 시간. 서명에 대한 만료 시간(초)을 지정합니다. 기본값은 31,536,000초입니다.
- **"z" 태그**. 메시지가 서명되었을 때 나타나는 세로 막대(예: |)로 구분된 헤더 필드 목록. 이 태그에는 헤더 필드의 이름 및 그 값을 포함합니다. 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
```

13단계 서명에 도메인 프로파일을 사용할 사용자(이메일 주소, 호스트 등)를 입력합니다.

참고 도메인 프로파일을 생성할 때 특정 사용자와 연결할 프로파일을 결정하는 데 계층 구조가 사용된다는 사실을 유의해야 합니다. 예를 들어 example.com에 하나의 프로파일을 생성하고 joe@example.com에 또 다른 프로파일을 생성합니다. 메일을 joe@example.com에서 보낸 경우 joe@example.com의 프로파일이 사용됩니다. 그러나 메일을 adam@example.com에서 보낸 경우 example.com의 프로파일이 사용됩니다.

14단계 변경사항을 제출하고 커밋합니다.

15단계 이 시점에서 이를 수행하지 않은 경우 발송 메일 흐름 정책에서 DomainKeys/DKIM 서명을 활성화해야 합니다(발송 메일에 서명 활성화, 20-6페이지 참조).

참고 DomainKeys 및 DKIM 프로파일을 모두 생성하는 경우 AsyncOS는 발송 메일에 DomainKeys 및 DKIM 서명을 모두 수행합니다.

서명 키 생성 또는 편집

새 서명 키 생성

서명 키에는 DomainKeys 및 DKIM 서명의 도메인 프로파일에 필요합니다.

절차

1단계 **Mail Policies(메일 정책) > Signing Keys(서명 키)**를 선택합니다.

2단계 **Add Key(키 추가)**를 클릭합니다.

3단계 키의 이름을 입력합니다.

4단계 **Generate(생성)**를 클릭하고 키 크기를 선택합니다.

5단계 변경사항을 제출하고 커밋합니다.

참고 이를 수행하지 않은 경우 도메인 프로파일을 편집하여 키를 할당해야 합니다.

기존 서명 키 편집

절차

1단계 **Mail Policies(메일 정책) > Signing Keys(서명 키)**를 선택합니다.

2단계 원하는 서명 키를 클릭합니다.

3단계 에 설명된 대로 원하는 필드를 편집합니다.

참고 보안 강화를 위해, 어플라이언스의 중요한 데이터의 암호화를 FIPS 모드로 사용하는 경우 개인 키를 확인할 수 없습니다. 개인 키를 편집하기 위해 개인 키를 붙여넣거나 새 개인 키를 생성할 수 있습니다.

4단계 변경사항을 제출하고 커밋합니다.

서명 키 내보내기

어플라이언스에 있는 모든 키를 함께 단일 텍스트 파일로 내보냅니다.

절차

1단계 **Mail Policies(메일 정책) > Signing Keys(서명 키)**를 선택합니다.

2단계 **Export Keys(키 내보내기)**를 클릭합니다.

참고 보안 강화를 위해 어플라이언스의 중요한 데이터 암호화를 FIPS 모드로 사용하는 경우 키를 내보내는 동안 서명 키가 암호화됩니다.

3단계 파일의 이름을 입력하고 **Submit(제출)**을 클릭합니다.

기존 서명 키 가져오기 또는 입력하기

관련 주제

- 키 붙여넣기, 20-12페이지
- 기존의 파일 내보내기로 키 가져오기, 20-12페이지

키 붙여넣기

절차

1단계 **Mail Policies(메일 정책) > Signing Keys(서명 키)**를 선택합니다.
2단계 **Add Key(키 추가)**를 클릭합니다.
3단계 키를 Paste Key(키 붙여넣기) 필드에 붙여넣습니다(PEM 형식이어야 하며 RSA 키여야 함).
4단계 변경사항을 제출하고 커밋합니다.

기존의 파일 내보내기로 키 가져오기

참고 키 파일을 가져오려면 서명 키 내보내기, 20-11페이지 항목을 참조하십시오.

절차

1단계 **Mail Policies(메일 정책) > Signing Keys(서명 키)**를 선택합니다.
2단계 **Import Keys(키 가져오기)**를 클릭합니다.
3단계 내보낸 서명 키를 포함하는 파일을 선택합니다.
4단계 **Submit(제출)**을 클릭합니다. 가져오기를 수행하면 기존의 모든 서명 키가 대체된다는 경고가 표시됩니다. 텍스트 파일에 있는 모든 키를 가져옵니다.
5단계 **Import(가져오기)**를 클릭합니다.

서명 키 삭제

관련 주제

- 선택한 서명 키 삭제, 20-12페이지
- 모든 서명 키 삭제, 20-13페이지

선택한 서명 키 삭제

절차

1단계 **Mail Policies(메일 정책) > Signing Keys(서명 키)**를 선택합니다.
2단계 삭제할 각 서명 키의 오른쪽 확인란을 선택합니다.
3단계 **Delete(삭제)**를 클릭합니다.
4단계 삭제를 확인합니다.

모든 서명 키 삭제

절차

1단계 **Mail Policies(메일 정책) > Signing Keys(서명 키)**를 선택합니다.

2단계 Signing Keys(서명 키) 페이지에서 **Clear All Keys(모든 키 지우기)**를 클릭합니다.

3단계 삭제를 확인합니다.

DNS Text Record 생성

절차

1단계 **Mail Policies(메일 정책) > Signing Profile(서명 프로파일)**을 선택합니다.

2단계 Domain Signing Profiles(도메인 서명 프로파일) 섹션의 DNS Text Record 열에서 해당 도메인 프로파일에 대한 **Generate(생성)** 링크를 클릭합니다.

3단계 DNS Text Record에 포함할 특성에 대한 확인란을 선택합니다.

4단계 **Generate Again(다시 생성)**을 클릭하여 변경 사항을 적용하여 키를 다시 생성합니다.

5단계 DNS Text Record는 창 하단의 텍스트 필드에 표시됩니다(이제 복사 가능). 경우에 따라 다중 문자열 DNS Text Record가 생성됩니다. 다중 문자열 DNS Text Record, 20-13페이지 항목을 참조하십시오.

6단계 **Done(완료)**을 클릭합니다.

관련 주제

- 다중 문자열 DNS Text Record, 20-13페이지

다중 문자열 DNS Text Record

다중 문자열 DNS Text Record는 DNS Text Record를 생성하는 데 사용된 서명 키가 1,024비트보다 큰 경우 생성될 수 있습니다. 이는 DNS Text Record의 단일 문자열은 255자를 초과할 수 없기 때문입니다. DNS 서버 일부에서는 다중 문자열 DNS Text Record를 수락하거나 처리하지 않으므로 DKIM 인증에 실패할 수 있습니다.

이를 피하려면 큰따옴표를 사용하여 다중 문자열 DNS Text Record를 255바이트가 넘지 않는 더 작은 문자열로 나누는 것이 좋습니다. 다음은 예제입니다.

```
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 구현은 처리하기 전 이러한 방식을 통해 전체 원본 단일 문자열로 나눈 DNS Text Record와 유사합니다.

도메인 프로파일 테스트

서명 키를 만들고, 도메인 프로파일과 연결한 후 DNS 텍스트를 생성하여 인증 DNS에 삽입하고 나면, 도메인 프로파일을 테스트할 수 있습니다.

절차

1단계 **Mail Policies(메일 정책) > Signing Profile(서명 프로파일)**을 선택합니다.

2단계 **Domain Signing Profiles(도메인 서명 프로파일)** 섹션의 프로파일 테스트 열에서 도메인 프로파일에 대한 **Test(테스트)** 링크를 클릭합니다.

3단계 성공 또는 실패를 나타내는 메시지가 페이지 상단에 표시됩니다. 테스트가 실패하면 오류 텍스트가 포함된 경고 메시지가 표시됩니다.

도메인 프로파일 내보내기

어플라이언스에 있는 모든 도메인 프로파일을 함께 단일 텍스트 파일로 내보냅니다.

절차

1단계 **Mail Policies(메일 정책) > Signing Profile(서명 프로파일)**을 선택합니다.

2단계 **Export Domain Profiles(도메인 프로파일 내보내기)**를 클릭합니다.

3단계 파일의 이름을 입력하고 **Submit(제출)**을 클릭합니다.

도메인 프로파일 가져오기

절차

1단계 **Mail Policies(메일 정책) > Signing Profile(서명 프로파일)**을 선택합니다.

2단계 **Import Domain Profiles(도메인 프로파일 가져오기)**를 클릭합니다.

3단계 내보낸 도메인 프로파일을 포함하는 파일을 선택합니다.

4단계 **Submit(제출)**을 클릭합니다. 가져오기를 수행하면 기존의 모든 도메인 프로파일이 대체된다는 경고가 표시됩니다. 텍스트 파일에 있는 모든 도메인 프로파일을 가져옵니다.

5단계 **Import(가져오기)**를 클릭합니다.

도메인 프로파일 삭제

관련 주제

- 선택한 도메인 프로파일 제거, 20-15페이지
- 모든 도메인 프로파일 제거, 20-15페이지

선택한 도메인 프로파일 제거

절차

1단계 **Mail Policies(메일 정책) > Signing Profile(서명 프로파일)**을 선택합니다.
2단계 제거할 각 도메인 프로파일의 오른쪽 확인란을 선택합니다.
3단계 **Delete(삭제)**를 클릭합니다.
4단계 삭제를 확인합니다.

모든 도메인 프로파일 제거

절차

1단계 **Mail Policies(메일 정책) > Signing Profile(서명 프로파일)**을 선택합니다.
2단계 **Clear All Profiles(모든 프로파일 지우기)**를 클릭합니다.
3단계 삭제를 확인합니다.

도메인 프로파일 검색

절차

1단계 **Mail Policies(메일 정책) > Signing Profile(서명 프로파일)**을 선택합니다.
2단계 Find Domain Profiles(도메인 프로파일 찾기) 섹션에서 검색 조건을 지정합니다.
3단계 **Find Profiles(프로파일 찾기)**를 클릭합니다.
4단계 각 도메인 프로파일에 대해 이메일, 도메인, 선택기 및 서명 키 이름 필드를 검사합니다.

참고 검색 조건을 입력하지 않으면 검색 엔진은 모든 도메인 프로파일을 반환합니다.

시스템에서 생성한 메시지 서명

시스템에서 생성한 메시지에 DKIM 서명 사용 여부를 선택할 수도 있습니다. 어플라이언스가 다음 메시지에 서명합니다.

- Cisco IronPort Spam Quarantine 알림
- 콘텐츠 필터 생성 알림
- 구성 메시지
- 요청 지원

절차

1단계 **Mail Policies(메일 정책) > Signing Profile(서명 프로파일)**을 선택합니다.

2단계 **DKIM Signing of System Generated Messages(시스템 생성 메시지의 DKIM 서명)** 섹션에서 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 **On(켜기)**을 선택합니다.

4단계 변경사항을 제출하고 커밋합니다.

도메인 키 및 로깅

DomainKeys 서명 시 다음의 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 다음의 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

표 20-1 DKIM을 사용하여 수신 메시지를 확인하는 방법

	수행할 작업	추가 정보
1단계	DKIM을 사용한 메시지 확인에 필요한 프로파일을 생성합니다.	DKIM 확인 프로파일 생성, 20-18페이지.
2단계	(선택 사항) 사용자 지정 메일 흐름 정책을 생성하여 DKIM을 사용한 수신 메시지 확인에 사용합니다.	메일 흐름 정책을 사용하여 수신 메시지에 대한 규칙 정의, 7-15페이지
3단계	메일 흐름 정책을 구성하여 DKIM을 사용한 수신 메시지를 확인합니다.	메일 흐름 정책에서 DKIM 확인 구성, 20-20페이지
4단계	Email Security 어플라이언스가 확인된 메시지에 수행하는 작업을 정의합니다.	DKIM 인증 메일에 대한 작업 구성, 20-21페이지
5단계	특정 발신자 또는 수신자의 그룹과 해당 작업을 연결합니다.	메일 정책 구성, 10-7페이지

관련 주제

- AsyncOS에서 수행하는 DKIM 확인, 20-17페이지
- DKIM 확인 프로파일 관리, 20-17페이지

- 메일 흐름 정책에서 DKIM 확인 구성, 20-20페이지
- DKIM 인증 메일에 대한 작업 구성, 20-21페이지

AsyncOS에서 수행하는 DKIM 확인

AsyncOS 어플라이언스에 DKIM 확인 기능을 구성하는 경우 다음 확인 작업이 수행됩니다.

절차

1단계 AsyncOS는 수신 메일의 DKIM 서명 필드, 즉 서명 헤더 구문, 유효한 태그 값 및 필수 태그를 확인합니다. 이러한 서명 확인에 실패하는 경우 AsyncOS는 *permfail*을 반환합니다.

2단계 서명 확인이 수행된 후 공개 키가 공용 DNS 레코드에서 검색되며 TXT 레코드가 검증됩니다. 이 절차가 진행되는 동안 오류가 발생되면 AsyncOS에서 *permfail*을 반환합니다. *tempfail*은 공개 키의 DNS 쿼리가 응답받지 못하는 경우 발생합니다.

3단계 공개 키를 검색한 후 AsyncOS는 해시 값을 확인하고 서명을 확인합니다. 이 단계 동안 실패가 발생하는 경우 AsyncOS는 *permfail*을 반환합니다.

4단계 모든 검사를 통과하면 AsyncOS는 *pass*를 반환합니다.

참고 메시지 본문이 지정된 길이보다 길면 AsyncOS에서 다음 판정을 반환합니다.

```
dkim = pass (partially verified [x bytes])
```

여기에서 *X*는 인증된 크기(바이트)를 나타냅니다.

최종 확인 결과는 *Authentication-Results* 헤더로 입력됩니다. 예를 들어 다음과 같은 헤더를 받을 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 확인 작업이 첫 번째 유효한 서명에서 중지됩니다. 마지막 서명을 사용하여 확인할 수 없습니다. 이 기능은 향후 릴리스에서 사용할 수 있습니다.

DKIM 확인 프로파일 관리

DKIM 확인 프로파일은 Email Security 어플라이언스의 메일 흐름 정책에서 DKIM 서명 확인에 사용하는 매개변수 목록입니다. 예를 들어 확인 프로파일 두 개, 즉 쿼리가 시간을 초과하기 전에 30초를 허용하는 프로파일과 쿼리가 시간을 초과하기 전 3초만 허용하는 프로파일을 만들 수 있습니다. 두 번째 확인 프로파일을 속도 제한 메일 흐름 정책에 할당하여 DDoS 경우의 연결 기아 상태를 방지할 수 있습니다. 확인 프로파일은 다음의 정보로 구성됩니다.

- 확인 프로파일 이름.
- 최소 및 최대 허용 가능 공개 키 크기. 기본 키 크기는 각각 512와 2,048바이트입니다.

- 확인할 메시지의 최대 서명 수. 메시지에 정의한 최대 크기보다 큰 서명이 있는 경우 어플라이언스는 나머지 서명의 확인을 건너뛰고 계속 메시지를 처리합니다. 기본 서명은 5개입니다.
- 발신자의 시스템 시간과 확인자의 시스템 시간 사이 최대 허용된 시간 차이(초). 예를 들어 메시지 서명이 05:00:00에 만료되고 확인자의 시스템 시간이 05:00:30인 경우 허용된 시간 차이가 60초일 때 메시지 서명이 계속 유효하지만 허용된 차이가 10초인 경우 유효하지 않습니다. 기본값은 60초입니다.
- 본문 길이 매개변수를 사용할지 여부 옵션.
- 임시적인 실패의 경우 수행할 SMTP 작업.
- 영구적인 실패의 경우 수행할 SMTP 작업.

프로파일 이름으로 기존의 모든 확인 프로파일을 검색할 수 있습니다.

DKIM 확인 프로파일을 어플라이언스의 구성 디렉토리에 텍스트 파일로 내보낼 수 있습니다. 확인 프로파일을 내보낼 때 어플라이언스에 있는 기존의 모든 프로파일이 단일 텍스트 파일로 저장됩니다. 자세한 내용은 DKIM 확인 프로파일 내보내기, 20-19페이지 항목을 참조하십시오.

이전에 내보낸 DKIM 확인 프로파일을 가져올 수 있습니다. DKIM 확인 프로파일을 가져오면 현재 머신에 있는 모든 DKIM 확인 프로파일이 교체됩니다. 자세한 내용은 DKIM 확인 프로파일 가져오기, 20-19페이지 항목을 참조하십시오.

관련 주제

- DKIM 확인 프로파일 생성, 20-18페이지
- DKIM 확인 프로파일 내보내기, 20-19페이지
- DKIM 확인 프로파일 가져오기, 20-19페이지
- DKIM 확인 프로파일 삭제, 20-19페이지
- DKIM 확인 프로파일 검색, 20-20페이지

DKIM 확인 프로파일 생성

절차

1단계	**Mail Policies(메일 정책) > Verification Profiles(확인 프로파일)**를 클릭합니다.
2단계	**Add Profile(프로파일 추가)**을 클릭합니다.
3단계	프로파일 이름을 입력합니다.
4단계	어플라이언스에서 수락할 수 있는 서명 키의 최소 키 크기를 선택합니다.
5단계	어플라이언스에서 수락할 수 있는 서명 키의 최대 키 크기를 선택합니다.
6단계	단일 메시지에서 확인할 최대 서명 수를 선택합니다. 기본 서명은 5개입니다.
7단계	키 쿼리가 시간 초과되기 전까지의 시간(초)을 선택합니다. 기본값은 10초입니다.
8단계	발신자의 시스템 시간과 확인자의 시스템 시간 간에 최대 허용된 시간 차이(초)를 선택합니다. 기본값은 60초입니다.
9단계	메시지를 확인하기 위해 서명에서 본문 길이 매개변수를 사용할지 여부를 선택합니다.
10단계	서명을 확인할 때 임시적인 실패가 있는 경우 Email Security 어플라이언스가 메시지를 수락할지 또는 거부할지를 선택합니다. 어플라이언스에서 메시지를 거부하려면 기본 451 SMTP 응답 코드 또는 또 다른 SMTP 응답 코드 및 텍스트를 보내도록 선택할 수 있습니다.

11단계 서명을 확인할 때 영구적인 실패가 있는 경우 Email Security 어플라이언스가 메시지를 수락할지 또는 거부할지를 선택합니다. 어플라이언스에서 메시지를 거부하려면 기본 451 SMTP 응답 코드 또는 또 다른 SMTP 응답 코드 및 텍스트를 보내도록 선택할 수 있습니다.

12단계 변경사항을 제출합니다.

새 프로파일이 DKIM 확인 프로파일 테이블에 나타납니다.

13단계 변경사항을 커밋합니다.

14단계 이때 수신 메일 흐름 정책에서 DKIM 확인을 활성화하고 사용할 확인 프로파일을 선택해야 합니다.

DKIM 확인 프로파일 내보내기

어플라이언스에 있는 모든 DKIM 확인 프로파일은 단일 텍스트 파일로 내보내지며 어플라이언스의 `configuration` 디렉토리에 저장됩니다.

절차

1단계 **Mail Policies(메일 정책) > Verification Profiles(확인 프로파일)**를 선택합니다.

2단계 **Export Profiles(프로파일 내보내기)**를 클릭합니다.

3단계 파일의 이름을 입력하고 **Submit(제출)**을 클릭합니다.

DKIM 확인 프로파일 가져오기

절차

1단계 **Mail Policies(메일 정책) > Verification Profiles(확인 프로파일)**를 선택합니다.

2단계 **Import Profiles(프로파일 가져오기)**를 클릭합니다.

3단계 DKIM 확인 프로파일을 포함하는 파일을 선택합니다.

4단계 **Submit(제출)**을 클릭합니다. 가져오기를 수행하면 기존의 모든 DKIM 확인 프로파일이 대체된다는 경고가 표시됩니다.

5단계 **Import(가져오기)**를 클릭합니다.

DKIM 확인 프로파일 삭제

관련 주제

- 선택한 DKIM 확인 프로파일 제거, 20-20페이지
- 모든 DKIM 확인 프로파일 제거, 20-20페이지

선택한 DKIM 확인 프로파일 제거

절차

1단계 **Mail Policies(메일 정책) > Verification Profiles(확인 프로파일)**를 선택합니다.
2단계 삭제할 각 DKIM 확인 프로파일의 오른쪽 확인란을 선택합니다.
3단계 **Delete(삭제)**를 클릭합니다.
4단계 삭제를 확인합니다.

모든 DKIM 확인 프로파일 제거

절차

1단계 **Mail Policies(메일 정책) > Verification Profiles(확인 프로파일)**를 선택합니다.
2단계 **Clear All Profiles(모든 프로파일 지우기)**를 클릭합니다.
3단계 삭제를 확인합니다.

DKIM 확인 프로파일 검색

프로파일 이름에서 특정 조건으로 모든 DKIM 확인 프로파일을 검색하려면 다음을 수행합니다.

절차

1단계 **Mail Policies(메일 정책) > Verification Profiles(확인 프로파일)**를 선택합니다.
2단계 **Search DKIM Verification Profiles(DKIM 확인 프로파일 검색)** 섹션에서 검색 조건을 지정합니다.
3단계 **Find Profiles(프로파일 찾기)**를 클릭합니다.
각 DKIM 확인 프로파일에 대한 프로파일 이름을 검색합니다.
검색 조건을 입력하지 않으면 검색 엔진은 모든 DKIM 확인 프로파일을 반환합니다.

메일 흐름 정책에서 DKIM 확인 구성

DKIM 확인이 수신 이메일의 메일 흐름 정책에서 활성화됩니다.

절차

1단계 **Mail Policies(메일 정책) > Mail Flow Policies(메일 흐름 정책)**를 선택합니다.
2단계 확인을 수행할 리스너에 해당하는 수신 메일 정책을 클릭합니다.
3단계 메일 흐름 정책의 Security Features(보안 기능) 섹션에서 **On(켜기)**을 선택하여 DKIM 확인을 활성화합니다.

4단계 정책에 사용할 DKIM 확인 프로파일을 선택합니다.

5단계 변경사항을 커밋합니다.

관련 주제

- DKIM 확인 및 로깅, 20-21페이지

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 인증 메일에 대한 작업 구성

DKIM 메일을 확인할 때 *Authentication-Results* 헤더가 메일에 추가되지만, 인증 결과와 상관없이 메일이 수락됩니다. 이러한 인증 결과를 기반으로 작업을 구성하려면 콘텐츠 필터를 생성하여 DKIM 인증 메일에 대한 작업을 수행할 수 있습니다. 예를 들어 DKIM 확인에 실패하는 경우 메일을 전달, 바운스, 삭제 또는 격리하도록 구성할 수 있습니다. 이를 위해 콘텐츠 필터를 사용하여 작업을 구성해야 합니다.

절차

1단계 **Mail Policies(메일 정책) > Incoming Filters(수신 필터)**를 선택합니다.

2단계 **Add Filter(필터 추가)**를 클릭합니다.

3단계 Conditions(조건) 섹션에서 **Add Condition(조건 추가)**을 클릭합니다.

4단계 조건 목록에서 **DKIM Authentication(DKIM 인증)**을 선택합니다.

5단계 DKIM 조건을 선택합니다. 다음 옵션 중 하나를 선택합니다.

- **Pass.** 메시지가 인증 테스트를 통과했습니다.
- **Neutral**. 인증이 수행되지 않았습니다.
- **Temperror**. 복구 가능한 오류가 발생했습니다.
- **Permerror**. 복구할 수 없는 오류가 발생했습니다.
- **Hardfail**. 인증 테스트에 실패했습니다.
- **None**. 메시지가 서명되지 않았습니다.

6단계 조건과 연결할 작업을 선택합니다. 예를 들어 DKIM 확인에 실패하면 수신자에게 알리고 메시지를 바운스할 수 있습니다. 또는 DKIM 확인을 통과하면 추가 프로세스 없이 메시지를 즉시 전송할 수 있습니다.

7단계 새 콘텐츠 필터를 제출합니다.

8단계 적절한 수신 메일 정책에서 콘텐츠 필터를 활성화합니다.

9단계 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 인증을 확인하기 위한 방법입니다. SPF 및 SIDF를 통해 인터넷 도메인의 소유자는 DNS TXT 레코드의 특수 형식을 사용하여 해당 도메인에 이메일을 전송할 수 있는 머신을 지정할 수 있습니다. 정책 준수 메일 수신자는 게시된 SPF 레코드를 사용하여 메일 트랜잭션 과정에서 발신 메일 전송 에이전트의 신원 인증을 테스트합니다.

SPF/SIDF 인증을 사용하는 경우 발신자는 자신의 이름 사용이 허용된 호스트를 표시하는 SPF 레코드를 게시하고, 정책 준수 메일 수신자는 메일 게시된 SPF 레코드를 사용하여 트랜잭션 과정에서 발신 메일 전송 에이전트의 신원 인증을 테스트합니다.

참고 SPF 검사에 구문 분석 및 평가가 필요하므로 AsyncOS 성능에 영향을 줄 수 있습니다. 또한 SPF 검사로 인해 DNS 인프라에 로드가 증가할 수 있습니다.

SPF 및 SIDF를 사용할 때 SIDF가 SPF와 유사하지만 약간 다른 점이 있다는 점을 유의해야 합니다. SIDF와 SPF의 차이점에 대한 모든 설명은 RFC 4406을 참조하십시오. 본 문서의 목적에 따라 한 가지 유형의 확인만 적용되는 경우를 제외하고 두 가지 조건이 함께 논의됩니다.

참고 AsyncOS는 수신 릴레이에 대해 SPF를 지원하지 않습니다.

관련 주제

- 유효한 SPF 레코드에 관한 참고 사항, 20-22페이지

유효한 SPF 레코드에 관한 참고 사항

어플라이언스에 SPF 및 SIDF를 사용하려면 RFC 4406 및 4408에 따라 SPF 레코드를 게시합니다. PRA ID 확인 방법에 대한 정의는 RFC 4407을 검토합니다. SPF 및 SIDF 레코드 생성 시 발생할 수 있는 일반적인 실수를 확인하려면 다음 웹 사이트를 참조할 수 있습니다.

`http://www.openspf.org/FAQ/Common_mistakes`

관련 주제

- 유효한 SPF 레코드, 20-22페이지
- 유효한 SIDF 레코드, 20-23페이지
- SPF 레코드 테스트, 20-23페이지

유효한 SPF 레코드

SPF HELO 검사를 통과하려면 각 발신 MTA마다(도메인과 별도) "v=spf1 a –all" SPF 레코드를 포함하는지 확인합니다. 이 레코드를 포함하지 않으면 HELO 검사가 HELO ID에 대해 None 결과를 반환합니다. 도메인의 SPF 발신자가 많은 None 판정을 반환하는 경우 이러한 발신자는 각 발신 MTA에 대해 "v=spf1 a –all" SPF 레코드를 포함하지 않을 수 있습니다.

유효한 SIDF 레코드

SIDF 프레임워크를 지원하려면 "v=spf1" 및 "spf2.0" 레코드를 모두 게시해야 합니다. 예를 들어 DNS 레코드는 다음과 같이 표시될 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 않으며 따라서 이 경우에는 각 발신 MTA에 대해 SPF v2.0 레코드를 게시할 필요가 없습니다.

참고 SIDF를 지원하지 않도록 선택한 경우 "spf2.0/pra ~all" 레코드를 게시합니다.

SPF 레코드 테스트

RFC 검토 외에도 Email Security 어플라이언스에서 SPF 확인을 구현하기 전에 SPF 레코드를 테스트하는 것도 좋습니다. openspf.org 웹 사이트에는 사용할 수 있는 여러 테스트 도구가 있습니다.

`http://www.openspf.org/Tools`

다음 도구를 사용하여 이메일이 SPF 레코드 검사에 실패한 이유를 확인할 수 있습니다.

`http://www.openspf.org/Why`

또한 테스트 리스너에서 SPF를 활성화하고 Cisco의 `trace` CLI 명령을 사용하거나 GUI에서 추적을 수행하여 SPF 결과를 볼 수 있습니다. 추적 기능을 사용하여 다른 발신 IP를 쉽게 테스트할 수 있습니다.

SPF/SDIF를 사용하여 수신 메시지를 확인하는 방법

표 20-2 SPF/SDIF를 사용하여 수신 메시지를 확인하는 방법

	수행할 작업	추가 정보
1단계	(선택 사항) 사용자 지정 메일 흐름 정책을 생성하여 SPF/SDIF를 사용한 수신 메시지 확인에 사용합니다.	메일 흐름 정책을 사용하여 수신 메시지에 대한 규칙 정의, 7-15페이지
2단계	메일 흐름 정책을 구성하여 SPF/SDIF를 사용한 수신 메시지를 확인합니다.	SPF 및 SIDF 활성화, 20-24페이지
3단계	Email Security 어플라이언스가 확인된 메시지에 수행하는 작업을 정의합니다.	SPF/SIDF 인증 메일에 수행할 작업 확인, 20-31페이지.
4단계	특정 발신자 또는 수신자의 그룹과 해당 작업을 연결합니다.	메일 정책 구성, 10-7페이지
5단계	(선택 사항) 메시지 확인 결과를 테스트합니다.	SPF/SIDF 결과 테스트, 20-34페이지

주의 Cisco에서 이메일 인증을 전역으로 강력하게 보증하지 않지만, 업계에서 채택할 때에는 SPF/SIDF 인증 실패에 대해 신중하게 처리해야 합니다. 더 많은 기관에서 인증된 메일 발신 인프라를 더 많이 제어할 수 있을 때까지 이메일 바운스를 방지하고 대신 SPF/SIDF 확인에 실패한 이메일을 격리하는 것이 좋습니다.

참고 AsyncOS 명령줄 인터페이스(CLI)를 사용하면 SPF 수준에 대해 웹 인터페이스보다 더 많은 제어 설정이 가능합니다. SPF 판정에 따라 어플라이언스는 리스너를 기반으로 SMTP 대화를 통해 메시지를 수락하거나 거부할 수 있습니다. `listenerconfig` 명령을 사용하여 리스너의 Host Access Table에 대한 기본 설정을 편집할 때 SPF 설정을 수정할 수 있습니다. 설정에 대한 자세한 내용은 CLI를 통해 SPF 및 SIDF 활성화, 20-25페이지 항목을 참조하십시오.

SPF 및 SIDF 활성화

SPF/SIDF를 사용하려면 수신 리스너의 메일 흐름 정책에서 SPF/SIDF를 활성화해야 합니다. 기본 메일 흐름 정책을 통해 리스너에 SPF/SIDF를 활성화하거나 특정 수신 메일 흐름 정책에 해당 기능을 활성화할 수 있습니다.

절차

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

2단계 **Default Policy Parameters(기본 정책 매개변수)**를 클릭합니다.

3단계 기본 정책 매개변수에서 Security Features(보안 기능) 섹션을 확인합니다.

4단계 **SPF/SIDF Verification(SPF/SIDF 확인)** 섹션에서 **On(켜기)**을 클릭합니다.

5단계 적합성 수준을 설정합니다(기본값은 SIDF 호환 가능입니다). 이 옵션을 통해 사용할 SPF 또는 SIDF 확인 기준을 결정할 수 있습니다. SIDF 적합성 외에도 SPF와 SIDF가 결합된 SIDF 호환 가능을 선택할 수 있습니다.

표 20-3 SPF/SIDF 적합성 수준

적합성 수준	설명
SPF	SPF/SIDF 확인은 RFC4408에 따라 동작합니다. - PRA(Purported Responsible Address) ID 확인이 수행되지 않습니다. **참고**: 이 적합성 옵션을 선택하여 HELO ID를 테스트합니다.

표 20-3 SPF/SIDF 적합성 수준

적합성 수준	설명
SIDF	SPF/SIDF 확인은 RFC4406에 따라 동작합니다. - PRA ID는 기준의 전체 적합성에 따라 결정됩니다. - SPF v1.0 레코드는 spf2.0/mfrom,pra로 처리됩니다. - 존재하지 않는 도메인이나 잘못된 형식의 ID의 경우 Fail 판정이 반환됩니다.
SIDF 호환 가능	SPF/SIDF 확인은 RFC4406에 따라 동작합니다. 다음의 사항은 *제외*됩니다. - SPF v1.0 레코드는 spf2.0/mfrom으로 처리됩니다. - 존재하지 않는 도메인이나 잘못된 형식의 ID의 경우 None 판정이 반환됩니다. **참고**: 이 적합성 옵션은 OpenSPF 커뮤니티의 요청으로 도입되었습니다(www.openspf.org).

참고 더 많은 설정은 CLI를 통해 사용할 수 있습니다. 자세한 내용은 CLI를 통해 SPF 및 SIDF 활성화, 20-25페이지 항목을 참조하십시오.

6단계 SIDF 호환 가능의 적합성 수준을 선택하는 경우, 메시지에 Resent-Sender: 또는 Resent-From: 헤더가 있는 경우 확인을 통해 PRA ID의 Pass 결과를 None으로 다운그레이드할지 여부를 구성합니다. 보안을 위해 이 옵션을 선택할 수 있습니다.

7단계 SPF의 적합성 수준을 선택하려면 HELO ID에 대해 테스트를 수행할지 여부를 구성합니다. HELO 검사를 비활성화하여 성능을 개선하도록 이 옵션을 사용할 수 있습니다. `spf-passed` 필터 규칙이 PRA 또는 MAIL FROM ID를 먼저 검사하므로 이 옵션이 유용합니다. 어플라이언스는 SPF 적합성 수준에 대해서만 HELO 검사를 수행합니다.

관련 주제

- CLI를 통해 SPF 및 SIDF 활성화, 20-25페이지
- Received-SPF 헤더, 20-30페이지

CLI를 통해 SPF 및 SIDF 활성화

AsyncOS CLI는 각 SPF/SIDF 적합성 수준에 대해 더 많은 제어 설정을 지원합니다. 리스너의 Host Access Table의 기본 설정을 구성하는 경우 SPF/SIDF 확인 결과에 따라 어플라이언스가 수행하는 리스너의 SPF/SIDF 적합성 수준과 SMTP 작업(수락 또는 거부)을 선택할 수 있습니다. 메시지를 거부할 때 어플라이언스에서 보내는 SMTP 응답을 정의할 수도 있습니다.

적합성 수준에 따라 어플라이언스는 HELO ID, MAIL FROM ID 또는 PRA ID 검사를 수행합니다. ID 검사마다 다음 SPF/SIDF 확인 결과에 따라 어플라이언스가 세션을 계속 진행하거나(수락) 세션을 종료할지(거부)를 지정할 수 있습니다.

- **None.** 정보 부족으로 인해 확인을 수행할 수 없습니다.
- **Neutral.** 도메인 소유자가 클라이언트가 해당 ID를 사용하도록 인증되었는지 여부를 어설션하지 않습니다.

- **SoftFail.** 도메인 소유자는 호스트가 해당 ID를 사용하도록 인증되지 않았지만 확정 구문을 만들지 않는다고 판단합니다.
- **Fail.** 클라이언트가 해당 ID로 메일을 보내도록 인증되지 않았습니다.
- **TempError.** 확인하는 동안 일시적인 오류가 발생했습니다.
- **PermError.** 확인하는 동안 영구적인 오류가 발생했습니다.

메시지에 Resent-Sender: 또는 Resent-From: 헤더가 있는 경우 PRA ID의 Pass 결과를 None으로 다운그레이드하도록 SIDF 호환 가능 적합성 수준을 구성하지 않으면 어플라이언스는 Pass 결과를 반환하는 메시지를 수락합니다. 어플라이언스에서 PRA 검사가 None을 반환하는 경우를 대비하여 지정된 SMTP 작업을 수행합니다.

ID 검사에 대해 SMTP 작업을 정의하지 않도록 선택하면 어플라이언스에서 Fail을 포함한 모든 확인 결과를 자동으로 수락합니다.

ID 확인 결과가 활성화된 ID 검사의 거부 작업과 일치하는 경우 어플라이언스는 세션을 종료합니다. 예를 들어 관리자는 모든 HELO ID 검사 결과(Fail을 포함)를 기반으로 메시지를 수락하도록 리스너를 구성하지만 MAIl FROM ID 검사의 Fail 결과를 반환하는 메시지를 거부하도록 구성할 수도 있습니다. 메시지가 HELO ID 검사에 실패하면 어플라이언스가 해당 결과를 수락하므로 세션은 계속 진행됩니다. 메시지가 MAIL FROM ID 검사에 실패하면 리스너는 세션을 종료한 후 거부 작업에 대해 STMP 응답을 반환합니다.

SMTP 응답은 SPF/SIDF 확인 결과에 따라 메시지를 거부하는 경우 어플라이언스가 반환하는 코드 번호 및 메시지입니다. TempError 결과는 나머지 확인 결과로부터 다양한 SMTP 응답을 반환합니다. TempError의 경우 기본 응답 코드는 `451`이며 기본 메시지 텍스트는 `#4.4.3 Temporary error occurred during SPF verification`입니다. 기타 모든 확인 결과의 경우 기본 응답 코드는 `550`이며 기본 메시지 텍스트는 `#5.7.1 SPF unauthorized mail is prohibited`입니다. TempError 및 나머지 확인 결과에 대해 자체 응답 코드 및 메시지 텍스트를 지정할 수 있습니다.

거부 작업이 Neutral, SoftFail 또는 Fail 확인 결과에 대해 수행되는 경우, SPF 게시자 도메인에서 타사 응답을 반환하도록 선택적으로 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 편집합니다. 다음 프롬프트에 `yes`라고 답변하여 SPF 제어를 구성합니다.

```
Would you like to change SPF/SIDF settings?  [N]> yes

Would you like to perform SPF/SIDF Verification?  [Y]> yes
```

다음 SPF 제어 설정은 Host Access Table에 사용할 수 있습니다.

표 20-4 CLI를 통한 SPF 제어 설정

적합성 수준	사용 가능한 SPF 제어 설정
SPF 전용	• HELO ID 검사 수행 여부 • 다음 ID 검사의 결과에 따라 수행되는 SMTP 작업은 다음과 같습니다. – HELO ID(활성화된 경우) – MAIL FROM ID • 거부 작업에 대해 반환된 SMTP 응답 코드 및 텍스트 • 확인 시간제한(초)
SIDF 호환 가능	• HELO ID 검사 수행 여부 • Resent-Sender: 또는 Resent-From: 헤더가 메시지에 있는 경우 확인을 통해 PRA ID의 Pass 결과를 None으로 다운그레이드하는지 여부 • 다음 ID 검사의 결과에 따라 수행되는 SMTP 작업은 다음과 같습니다. – HELO ID(활성화된 경우) – MAIL FROM ID – PRA ID • 거부 작업에 대해 반환된 SMTP 응답 코드 및 텍스트 • 확인 시간제한(초)
SIDF Strict	• 다음 ID 검사의 결과에 따라 수행되는 SMTP 작업은 다음과 같습니다. – MAIL FROM ID – PRA ID • SPF 거부 작업에 대해 반환된 SMTP 응답 코드 및 텍스트 • 확인 시간제한(초)

다음의 예시는 SPF 전용 적합성 수준을 사용하여 SPF/SIDF 확인을 구성하는 사용자를 보여줍니다. 어플라이언스는 HELO ID 검사를 수행하며 None 및 Neutral 확인 결과를 수락하고 나머지는 거부합니다. SMTP 작업에 사용되는 CLI 프롬프트는 모든 ID 유형에 대해 동일하게 사용됩니다. 사용자는 MAIL FROM ID에 대한 SMTP 작업은 정의하지 않습니다. 어플라이언스는 ID에 대한 모든 확인 결과를 자동으로 수락합니다. 어플라이언스는 모든 거부 결과에 대해 기본 거부 코드 및 텍스트를 사용합니다.

```
Would you like to change SPF/SIDF settings?  [N]> yes


Would you like to perform SPF/SIDF Verification?  [N]> yes
```

```
What Conformance Level would you like to use?

1. SPF only

2. SIDF compatible

3. SIDF strict

[2]> 1


Would you like to have the HELO check performed? [Y]> y


Would you like to change SMTP actions taken as result of the SPF verification? [N]> y


Would you like to change SMTP actions taken for the HELO identity? [N]> y


What SMTP action should be taken if HELO check returns None?

1. Accept

2. Reject

[1]> 1


What SMTP action should be taken if HELO check returns Neutral?

1. Accept

2. Reject

[1]> 1


What SMTP action should be taken if HELO check returns SoftFail?

1. Accept

2. Reject

[1]> 2


What SMTP action should be taken if HELO check returns Fail?

1. Accept
```

```
2. Reject

    [1]> 2


    hat SMTP action should be taken if HELO check returns TempError?

    1. Accept

2. Reject

[1]> 2


What SMTP action should be taken if HELO check returns PermError?

1. Accept

2. Reject

[1]> 2


Would you like to change SMTP actions taken for the MAIL FROM identity? [N]> n


Would you like to change SMTP response settings for the REJECT action? [N]> n


Verification timeout (seconds)

[40]>
```

다음은 리스너의 기본 정책 매개변수에 대해 어떻게 SPF/SIDF 설정이 표시되는지를 보여줍니다.

```
SPF/SIDF Verification Enabled: Yes

  Conformance Level: SPF only

  Do HELO test: Yes

  SMTP actions:

    For HELO Identity:

      None, Neutral: Accept

      SoftFail, Fail, TempError, PermError: Reject

    For MAIL FROM Identity: Accept
```

```
SMTP Response Settings:

  Reject code: 550

  Reject text: #5.7.1 SPF unauthorized mail is prohibited.

  Get reject response text from publisher: Yes

  Defer code: 451

  fer text: #4.4.3 Temporary error occurred during SPF verification.

Verification timeout: 40
```

*Cisco AsyncOS CLI 참조 설명서*listenerconfig 명령에 대한 자세한 내용은 항목을 참조하십시오.

Received-SPF 헤더

SPF/SIDF 확인에 대해 AsyncOS를 구성하는 경우 이메일에 SPF/SIDF 확인 헤더(`Received-SPF`)를 배치합니다. `Received-SP` 헤더는 다음의 정보를 포함합니다.

- **확인 결과** - SPF 확인 결과(확인 결과, 20-31페이지 참조).
- **ID** - SPF 확인을 통해 검사한 ID(HELO, MAIL FROM 또는 PRA).
- **수신자** - 검사를 수행하는 확인 호스트 이름.
- **클라이언트 IP 주소** - SMTP 클라이언트의 IP 주소.
- **ENVELOPE FROM** - 봉투 발신자 사서함. (MAIL FROM ID를 비워둘 수 없으므로 MAIL FROM ID와 다를 수 있습니다.)
- **x-sender** - HELO, MAIL FROM 또는 PRA ID의 값.
- **x-conformance** - 적합성 수준(표 20-3SPF/SIDF 적합성 수준, 20-24페이지 참조) 및 PRA 검사의 다운그레이드가 수행되었는지 여부.

다음 예시는 SPF/SIDF 검사를 통과한 메시지에 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 확인 상태를 확인합니다.

SPF/SIDF 인증 메일에 수행할 작업 확인

SPF/SIDF 인증 메일을 받으면 SPF/SIDF 확인 결과에 따라 다른 작업을 수행할 수 있습니다. 다음 메시지 및 콘텐츠 필터 규칙을 사용하여 SPF/SIDF 인증 메일 상태를 확인하고 확인 결과에 따라 메시지에 작업을 수행할 수 있습니다.

- `spf-status`. 이 필터 규칙은 SPF/SIDF 상태에 따른 작업을 결정합니다. 유효한 SPF/SIDF 반환 값마다 다양한 작업을 입력할 수 있습니다.
- `spf-passed`. 이 필터 규칙은 SPF/SIDF 결과를 부울 값으로 일반화합니다.

참고 `spf-passed` 필터 규칙은 메시지 필터에서만 사용할 수 있습니다.

더 세분화된 결과를 처리하려면 `spf-status` 규칙을 사용하고, 단순 부울 값을 생성하려면 `spf-passed` 규칙을 사용할 수 있습니다.

관련 주제

- 확인 결과, 20-31페이지
- CLI의 spf-status 필터 규칙 사용, 20-32페이지
- GUI의 spf-status 콘텐츠 필터 규칙, 20-33페이지
- spf-passed 필터 규칙 사용, 20-33페이지

확인 결과

`spf-status` 필터 규칙을 사용하는 경우 다음 구문을 사용하여 SPF/SIDF 확인 결과를 검사할 수 있습니다.

```
if (spf-status == "Pass")
```

단일 조건으로 여러 상태의 판정을 검사하려면 다음 구문을 사용할 수 있습니다.

```
if (spf-status == "PermError, TempError")
```

다음 구문을 사용하여 HELO, MAIL FROM 및 PRA ID에 대한 확인 결과를 검사할 수도 있습니다.

```
if (spf-status("pra") == "Fail")
```

참고 `spf-status` 메시지 필터 규칙만 사용하여 HELO, MAIL FROM 및 PRA ID에 대한 결과를 검사할 수 있습니다. `spf-status` 콘텐츠 필터 규칙을 사용하여 ID를 검사할 수 없습니다. `spf-status` 콘텐츠 필터는 PRA ID만 검사합니다.

다음 확인 결과를 받을 수 있습니다.

- None - 정보 부족으로 인해 확인을 수행할 수 없습니다.
- Pass - 클라이언트가 해당 ID로 메일을 보내도록 인증되지 않았습니다.

- Neutral - 도메인 소유자가 클라이언트가 해당 ID를 사용하도록 인증되었는지 여부를 어설션하지 않습니다.
- SoftFail - 도메인 소유자는 호스트가 해당 ID를 사용하도록 인증되지 않았지만 확정 구문을 만들지 않는다고 판단합니다.
- Fail - 클라이언트가 주어진 ID로 메일을 보내도록 인증되지 않았습니다.
- TempError - 확인하는 동안 일시적인 오류가 발생했습니다.
- PermError - 확인하는 동안 영구적인 오류가 발생했습니다.

CLI의 spf-status 필터 규칙 사용

다음의 예시는 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

GUI의 콘텐츠 필터에서 `spf-status` 규칙을 활성화할 수도 있습니다. 그러나 `spf-status` 콘텐츠 필터 규칙을 사용하여 HELO, MAIL FROM 및 PRA ID에 대한 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 확인 필터 규칙을 추가합니다. 조건에 대해 하나 이상의 확인 결과를 지정합니다.

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. 다음의 예시는 `spf-passed` 규칙을 사용하여 spf-passed로 표시되지 않은 이메일을 격리하는 것을 보여줍니다.

```
quarantine-spf-unauthorized-mail:

    if (not spf-passed) {

        quarantine("Policy");

    }
```

참고 spf-status 규칙과는 달리 spf-passed 규칙은 SPF/SIDF 확인 값을 단순한 부울 값으로 축소합니다. None, Neutral, Softfail, TempError, PermError 및 Fail 확인 결과는 spf-passed 규칙에서 통과되지 않은 것으로 처리됩니다. 더 세분화된 결과에 따라 메시지에 대한 작업을 수행하려면 spf-status 규칙을 사용합니다.

SPF/SIDF 결과 테스트

SPF/SIDF 확인 결과를 테스트하고 다른 기관에서 다른 방식으로 SPF/SIDF를 구현하므로 이러한 결과를 토대로 SPF/SIDF 실패를 처리하는 방법을 결정합니다. 콘텐츠 필터, 메시지 필터 및 이메일 보안 모니터 - 콘텐츠 필터 보고서를 조합하여 사용하여 SPF/SIDF 확인 결과를 테스트할 수 있습니다.

SPF/SIDF 확인에 대한 종속성 정도는 SPF/SIDF 결과를 테스트할 때의 세분화 수준을 결정합니다.

관련 주제

- SPF/SIDF 결과의 기본 세분화 테스트, 20-34페이지
- SPF/SIDF 결과의 세분화 테스트, 20-34페이지

SPF/SIDF 결과의 기본 세분화 테스트

수신 메일의 SPF/SIDF 확인 결과를 기본 방식으로 얻으려면 콘텐츠 필터를 사용하거나 Email Security Monitor - Content Filters(이메일 보안 모니터 - 콘텐츠 필터) 페이지를 사용할 수 있습니다. 이 테스트는 SPF/SIDF 확인 결과 유형마다 받은 메시지 수를 보여줍니다.

절차

1단계 수신 리스너의 메일 흐름 정책에서 SPF/SIDF 확인을 활성화하고 콘텐츠 필터를 사용하여 수행할 작업을 구성합니다. SPF/SIDF 활성화에 대한 자세한 내용은 SPF 및 SIDF 활성화, 20-24페이지 항목을 참조하십시오.

2단계 SPF/SIDF 확인 유형마다 spf-status 콘텐츠 필터를 생성합니다. 명명 규칙을 사용하여 확인 유형을 나타냅니다. 예를 들어 SPF/SIDF 확인을 통과한 메시지에 "SPF-Passed"를 사용하거나 확인하는 동안 일시적인 오류로 인해 통과되지 못한 메시지에 "SPF-TempErr"을 사용합니다. spf-status 콘텐츠 필터 생성에 대한 자세한 내용은 GUI의 spf-status 콘텐츠 필터 규칙, 20-33페이지 항목을 참조하십시오.

3단계 SPF/SIDF 확인 메시지 여러 개를 처리한 후 Monitor(모니터) > Content Filters(콘텐츠 필터)를 클릭하면 SPF/SIDF 확인 콘텐츠 필터마다 트리거된 메시지의 수를 확인할 수 있습니다.

SPF/SIDF 결과의 세분화 테스트

SPF/SIDF 확인 결과에 대한 더 종합적인 정보를 얻으려면 특정 발신자 그룹에 대해서만 SPF/SIDF 확인을 활성화하고 이에 대한 결과를 검토합니다. 그런 다음 해당 특정 그룹에 대한 메일 정책을 생성하고 메일 정책에서 SPF/SIDF 확인을 활성화합니다. SPF/SIDF 결과의 기본 세분화 테스트, 20-34페이지에서 설명한 대로 콘텐츠 필터를 생성하고 콘텐츠 필터 보고서를 검토합니다. 확인이 유효하다고 판단된 경우, SPF/SIDF 확인을 사용하여 이 지정 발신자 그룹에 대해 이메일을 삭제하거나 바운스할지 결정할 수 있습니다.

절차

1단계 SPF/SIDF 확인에 대해 메일 흐름 정책을 생성합니다. 수신 리스너의 메일 흐름 정책에서 SPF/SIDF 확인을 활성화합니다. SPF/SIDF 활성화에 대한 자세한 내용은 SPF 및 SIDF 활성화, 20-24페이지 항목을 참조하십시오.

2단계 SPF/SIDF 확인에 대한 발신자 그룹을 생성하고 명명 규칙을 사용하여 SPF/SIDF 확인을 나타냅니다. 발신자 그룹 생성에 대한 자세한 내용은 "메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

3단계 SPF/SIDF 확인 유형마다 `spf-status` 콘텐츠 필터를 생성합니다. 명명 규칙을 사용하여 확인 유형을 나타냅니다. 예를 들어 SPF/SIDF 확인을 통과한 메시지에 "SPF-Passed"를 사용하거나 확인하는 동안 일시적인 오류로 인해 통과되지 못한 메시지에 "SPF-TempErr"을 사용합니다. `spf-status` 콘텐츠 필터 생성에 대한 자세한 내용은 GUI의 spf-status 콘텐츠 필터 규칙, 20-33페이지 항목을 참조하십시오.

4단계 SPF/SIDF 확인 메시지 여러 개를 처리한 후 Monitor(모니터) > Content Filters(콘텐츠 필터)를 클릭하면 SPF/SIDF 확인 콘텐츠 필터마다 트리거된 메시지의 수를 확인할 수 있습니다.

DMARC 확인

DMARC(Domain-based Message Authentication, Reporting and Conformance)는 이메일을 기반으로 하는 남용 가능성을 줄이기 위해 생성된 기술입니다. DMARC는 SPF 및 DKIM 메커니즘을 사용하여 이메일 수신자가 이메일을 인증하는 방법을 표준화합니다. DMARC 확인을 통과하려면 이메일은 이러한 인증 메커니즘 하나 이상을 통과해야 하며 인증 식별자는 RFC 5322를 준수해야 합니다.

AsyncOS for Email을 사용하면 다음을 수행할 수 있습니다.

- DMARC를 사용하여 수신 이메일을 확인합니다.
- 도메인 소유자의 정책을 재정의(수락, 격리 또는 거부)하도록 프로파일을 정의합니다.
- 피드백 보고서를 도메인 소유자에게 보내 인증 배포를 강화합니다.
- DMARC 집계 보고서 크기가 10MB를 초과하거나 DMARC 레코드의 RUA 태그에 지정된 크기인 경우 도메인 소유자에게 전송 오류 보고서를 보냅니다.

AsyncOS for Email은 2013년 3월 31일 IETF(Internet Engineering Task Force)에 제출된 대로 DMARC 규격을 준수하는 이메일을 처리할 수 있습니다. 자세한 내용은 http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02를 참조하십시오.

관련 주제

- AsyncOS for Email의 DMARC 확인 워크플로, 20-35페이지
- DMARC를 사용하여 수신 메시지를 확인하는 방법, 20-36페이지

AsyncOS for Email의 DMARC 확인 워크플로

다음은 AsyncOS for Email이 DMARC 확인을 수행하는 방법에 대해 설명합니다.

1. AsyncOS에 구성된 리스너는 SMTP 연결을 수신합니다.
2. AsyncOS는 메시지에 대해 SPF 및 DKIM 확인을 수행합니다.
3. AsyncOS는 DNS에서 발신자 도메인에 대한 DMARC 레코드를 가져옵니다.
   - 레코드가 없으면 AsyncOS는 DMARC 확인을 건너뛰고 프로세스를 계속 진행합니다.

- DNS 조회에 실패하면 AsyncOS는 지정된 DMARC 확인 프로파일을 기반으로 작업을 수행합니다.

4. DKIM 및 SPF 확인 결과에 따라 AsyncOS는 메시지에 대한 DMARC 확인을 수행합니다.

참고 DKIM 및 SPF 확인이 활성화되면 DMARC 확인은 DKIM 및 SPF 확인 결과를 다시 사용합니다.

5. DMARC 확인 결과 및 지정된 DMARC 확인 프로파일에 따라 AsyncOS는 메시지를 수락하고 격리하거나 거부합니다. 메시지가 DMARC 확인 실패로 인해 거부된 경우 AsyncOS는 프로세스를 계속 진행합니다.
6. AsyncOS는 해당 SMTP 응답을 보내고 프로세스를 계속 진행합니다.
7. 집계 보고서 전송이 활성화되는 경우 AsyncOS에서 DMARC 확인 데이터를 수집하고 도메인 소유자에게 보내는 일일 보고서에 그 결과를 포함합니다. DMARC 집계 피드백 보고서에 대한 자세한 내용은 DMARC 집계 보고서, 20-41페이지 항목을 참조하십시오.

참고 집계 보고서 크기가 10MB를 초과하거나 DMARC 레코드의 RUA 태그에 지정된 크기인 경우 AsyncOS는 도메인 소유자에게 전송 오류 보고서를 보냅니다.

DMARC를 사용하여 수신 메시지를 확인하는 방법

표 20-5 DMARC를 사용하여 수신 메시지를 확인하는 방법

	수행할 작업	추가 정보
1단계	새 DMARC 확인 프로파일을 생성하거나 기본 DMARC 확인 프로파일을 수정하여 요구 사항을 준수합니다.	DMARC 확인 프로파일 생성, 20-37페이지 DMARC 확인 프로파일 편집, 20-38페이지
2단계	(선택 사항) 전역 DMARC 설정을 구성하여 요구 사항을 준수합니다.	전체 DMARC 설정 구성, 20-39페이지
3단계	메일 흐름 정책을 구성하여 DMARC를 사용한 수신 메시지를 확인합니다.	메일 흐름 정책에 DMARC 확인 구성, 20-40페이지
4단계	(선택 사항) DMARC 피드백 보고서의 반환 주소를 구성합니다.	DMARC 피드백 보고서에 반환 주소 구성, 20-41페이지
5단계	(선택 사항) 다음을 검토합니다. • DMARC 확인 및 수신 메일 보고서 • 메시지 추적을 통해 DMARC 확인에 실패한 메시지	• DMARC 확인 페이지, 28-18페이지 • 수신 메일 페이지, 28-9페이지 • 메시지 검색, 29-2페이지

관련 주제

- DMARC 확인 프로파일 관리, 20-37페이지
- 전체 DMARC 설정 구성, 20-39페이지
- 메일 흐름 정책에 DMARC 확인 구성, 20-40페이지
- DMARC 피드백 보고서에 반환 주소 구성, 20-41페이지
- DMARC 집계 보고서, 20-41페이지

DMARC 확인 프로파일 관리

DMARC 확인 프로파일은 Email Security 어플라이언스의 메일 흐름 정책에서 DMARC 확인에 사용하는 매개변수 목록입니다. 예를 들어 특정 도메인에서 전달되는 모든 비준수 메시지를 거부하는 엄격한 프로파일과 다른 도메인에서 전달되는 모든 비준수 메시지를 격리하는 덜 엄격한 프로파일을 생성할 수 있습니다.

DMARC 확인 프로파일은 다음의 정보로 구성됩니다.

- 확인 프로파일 이름.
- DMARC 레코드의 정책이 거부인 경우의 메시지 작업.
- DMARC 레코드의 정책이 격리인 경우의 메시지 작업.
- 임시 실패의 경우 메시지 작업.
- 영구 실패의 경우 메시지 작업.

관련 주제

- DMARC 확인 프로파일 생성, 20-37페이지
- DMARC 확인 프로파일 편집, 20-38페이지
- DMARC 확인 프로파일 내보내기, 20-38페이지
- DMARC 확인 프로파일 가져오기, 20-39페이지
- DMARC 확인 프로파일 삭제, 20-39페이지

DMARC 확인 프로파일 생성

이 절차를 사용하여 새 DMARC 확인 프로파일을 생성합니다.

참고 기본적으로 AsyncOS는 기본 DMARC 확인 프로파일을 제공합니다. 새 DMARC 확인 프로파일을 생성하지 않으려면 기본 DMARC 확인 프로파일을 사용할 수 있습니다. 기본 DMARC 확인 프로파일은 **Mail Policies(메일 정책) > DMARC** 페이지에서 사용할 수 있습니다. 기본 DMARC 확인 프로파일의 편집 방법에 대한 지침은 DMARC 확인 프로파일 편집, 20-38페이지 항목을 참조하십시오.

절차

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

2단계 **Add Profile(프로파일 추가)**을 클릭합니다.

3단계 프로파일 이름을 입력합니다.

4단계 DMARC 레코드의 정책이 거부인 경우 AsyncOS에서 수행하는 메시지 작업을 설정합니다. 다음 중 하나를 선택합니다.

- **No Action(작업 없음)**. AsyncOS는 DMARC 확인에 실패한 메시지에 대해 아무런 작업을 수행하지 않습니다.
- **Quarantine(격리)**. AsyncOS는 지정된 격리에 대한 DMARC 확인에 실패한 메시지를 격리합니다.
- **Reject(거부)**. AsyncOS는 DMARC 확인에 실패한 모든 메시지를 거부하고 지정된 SMTP 코드 및 응답을 반환합니다. 기본 값은 각각 `550` 및 `#5.7.1 DMARC unauthenticated mail is prohibited`입니다.

5단계 DMARC 레코드의 정책이 격리인 경우 AsyncOS에서 취하는 메시지 조치를 설정합니다. 다음 중 하나를 선택합니다.

- **No Action(작업 없음)**. AsyncOS는 DMARC 확인에 실패한 메시지에 대해 아무런 작업을 수행하지 않습니다.
- **Quarantine(격리)**. AsyncOS는 지정된 격리에 대한 DMARC 확인에 실패한 메시지를 격리합니다.

6단계 DMARC 확인 중 일시적인 실패가 발생되는 메시지에 대해 AsyncOS가 취하는 메시지 조치를 설정합니다. 다음 중 하나를 선택합니다.

- **Accept(수락)**. AsyncOS가 DMARC 확인 중에 일시적인 실패가 발생되는 메시지를 수락합니다.
- **Reject(거부)**. AsyncOS가 DMARC 확인 중에 일시적인 실패가 발생되는 메시지를 거부하고 지정된 SMTP 코드 및 응답을 반환합니다. 기본값은 각각 `451` 및 `#4.7.1 DMARC 확인을 수행할 수 없음.`입니다.

7단계 DMARC 확인 중 영구적인 실패를 반환하는 메시지에 대해 AsyncOS가 수행하는 메시지 작업을 설정합니다. 다음 중 하나를 선택합니다.

- **Accept(수락)**. AsyncOS는 DMARC 확인 중에 영구적인 실패를 반환하는 메시지를 수락합니다.
- **Reject(거부)**. AsyncOS는 DMARC 확인 중에 영구적인 실패가 반환하는 메시지를 거부하고 지정된 SMTP 코드 및 응답을 반환합니다. 기본값은 각각 `550` 및 `#5.7.1 DMARC DMARC verification failed`입니다.

8단계 변경사항을 제출하고 커밋합니다.

DMARC 확인 프로파일 편집

절차

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

2단계 원하는 확인 프로파일 이름을 클릭합니다.

3단계 DMARC 확인 프로파일 생성, 20-37페이지에 설명된 대로 원하는 필드를 편집합니다.

4단계 변경사항을 제출하고 커밋합니다.

DMARC 확인 프로파일 내보내기

어플라이언스의 모든 DMARC 확인 프로파일을 `configuration` 디렉토리에 단일 텍스트 파일로 내보낼 수 있습니다.

절차

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

2단계 **Export Profiles(프로파일 내보내기)**를 클릭합니다.

3단계 파일의 이름을 입력합니다.

4단계 **Submit(제출)**을 클릭합니다.

DMARC 확인 프로파일 가져오기

절차

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

2단계 **Import Profiles(프로파일 가져오기)**를 클릭합니다.

3단계 DMARC 확인 프로파일을 포함하는 파일을 선택합니다.

4단계 **Submit(제출)**을 클릭합니다. 가져오기를 수행하면 기존의 모든 DMARC 확인 프로파일이 대체된다는 경고가 표시됩니다.

5단계 **Import(가져오기)**를 클릭합니다.

6단계 변경사항을 커밋합니다.

DMARC 확인 프로파일 삭제

절차

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

2단계 삭제할 확인 프로파일을 선택합니다.

3단계 **Delete(삭제)**를 클릭합니다.

4단계 삭제를 확인합니다.

전체 DMARC 설정 구성

절차

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

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

3단계 다음 표에 정의된 설정을 변경합니다.

표 20-6 DMARC 글로벌 설정

전역 설정	설명
특정 발신자 Bypass 주소 목록	특정 발신자의 메시지 DMARC 확인을 건너뜁니다. 드롭다운 목록에서 주소 목록을 선택합니다. **참고** Allow only full Email Addresses(전체 이메일 주소만 허용) 옵션을 선택하여 생성된 주소 목록만 선택할 수 있습니다. 자세한 내용은 수신 연결 규칙에 대해 발신자 주소 목록 사용, 7-21페이지 항목을 참조하십시오.
다음 헤더가 있는 메시지에 대한 Bypass 확인	특정 헤더를 포함하는 메시지의 DMARC 확인을 건너뜁니다. 예를 들어 이 옵션을 사용하여 메일링 목록 및 신뢰할 수 있는 전달자로부터 받은 메시지의 DMARC 확인을 건너뜁니다. 헤더 또는 쉼표로 구분된 여러 헤더를 입력합니다.
보고서 생성 일정	AsyncOS에서 DMARC 집계 보고서를 생성하려는 시간. 예를 들어 메일 흐름에 영향을 주지 않게 집계 보고서를 생성하도록 사용량 감소 시간을 선택할 수 있습니다.
보고서를 생성하는 항목	DMARC 집계 보고서를 생성하는 엔터티. DMARC 집계 보고서를 받는 도메인 소유자가 보고서를 생성한 엔터티를 식별하도록 지원합니다. 유효한 도메인 이름을 입력합니다.
보고서의 추가 연락처 정보	추가 연락처 정보(예: DMARC 집계 보고서를 받는 도메인 소유자가 보고서를 생성한 엔터티를 원하는 경우 기관의 고객 지원 세부 사항).
모든 집계 보고서의 복사본 전송 대상	모든 DMARC 집계 보고서의 복사본을 특정 사용자에게 전송합니다(예: 집계 보고서에 대한 분석을 수행하는 내부 사용자). 이메일 주소 또는 쉼표로 구분된 여러 주소를 입력합니다.
오류 보고서	DMARC 집계 보고서 크기가 10MB를 초과하거나 DMARC 레코드의 RUA 태그에 지정된 크기인 경우 도메인 소유자에게 전송 오류 보고서를 보냅니다. 확인란을 선택합니다.

4단계 변경사항을 제출하고 커밋합니다.

메일 흐름 정책에 DMARC 확인 구성

절차

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

2단계 확인을 수행할 리스너에 해당하는 수신 메일 정책을 클릭합니다.

3단계 메일 흐름 정책의 Security Features(보안 기능) 섹션에서 **On(켜기)**을 선택하여 DMARC 확인을 활성화합니다.

4단계 정책에 사용할 DMARC 확인 프로파일을 선택합니다.

5단계 (선택 사항) 메시지를 수신하는 DMARC가 활성화된 도메인의 RUA 태그에 있는 이메일 주소로 DMARC 집계 피드백 보고서를 전송하도록 활성화합니다.

집계 피드백 보고서는 매일 생성됩니다.

6단계 변경사항을 제출하고 커밋합니다.

관련 주제

DMARC 확인 로그, 20-41페이지

DMARC 확인 로그

다음의 DMARC 확인 단계에 따라 로그 메시지가 메일 로그에 추가됩니다.

- 메시지에 대한 DMARC 확인 시도
- DMARC 확인 완료
- DKIM 및 SPF 조정 결과를 포함한 DMARC 확인 세부사항
- 메시지에 대한 DMARC 확인 건너뛰기
- DMARC 레코드 가져오기 및 구문 분석, 또는 DNS 실패
- 실패한 도메인에 대한 DMARC 집계 보고서 전송
- 도메인에 대해 생성된 오류 보고서
- 성공한 도메인에 대한 오류 보고서 전송
- 실패한 도메인에 대한 오류 보고서 전송

DMARC 피드백 보고서에 반환 주소 구성

절차

1단계 **System Administration(시스템 관리) > Return Addresses(주소 반환)**를 선택합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 DMARC 집계 피드백 보고서의 반환 주소를 제공합니다.

4단계 변경사항을 제출하고 커밋합니다.

DMARC 집계 보고서

DMARC는 피드백 메커니즘을 사용하여 도메인 소유자 정책을 안전하고 확장 가능한 방식으로 적용합니다. 이 피드백 메커니즘은 도메인 소유자가 인증 배포를 강화할 수 있도록 지원합니다.

AsyncOS를 사용하여 DMARC 확인을 수행하고 메일 흐름 정책에서 집계 피드백 보고서의 전송을 활성화한 경우, AsyncOS는 집계 피드백 보고서를 매일 생성하며 도메인 소유자에게 이를 전송합니다. 이러한 보고서는 XML 형식이며 GZip 파일로 보관됩니다.

참고 AsyncOS가 생성하는 모든 DMARC 집계 피드백 보고서는 DMARC를 준수합니다.

DMARC 집계 피드백 보고서는 다음 섹션을 포함합니다.

- 이메일 주소 및 보고서 ID 번호 등의 보고서 발신자 메타데이터.
- 게시된 DMARC 정책의 세부사항.
- 소스 IP 주소 및 처리 요약 등의 DMARC 정책 처리 세부사항.
- 도메인 식별자.
- DMARC 확인 결과 및 인증 요약.

관련 주제

- 샘플 DMARC 집계 피드백 보고서, 20-42페이지

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>
```

21 장

텍스트 리소스

텍스트 리소스 개요

이 장에서는 콘텐츠, 사전, 고지 사항 및 템플릿과 같은 다양한 텍스트 리소스의 생성 및 관리에 대해 설명합니다.

관련 주제

- 콘텐츠 사전, 21-1페이지
- 텍스트 리소스, 21-2페이지
- 메시지 고지 사항 스탬핑, 21-2페이지
- 민감한 DLP 용어의 사용자 지정 사전 사용(사용자 지정 DLP 정책만 해당), 17-15페이지

콘텐츠 사전

회사 정책에 따라 적절한 작업을 수행하기 위해 콘텐츠 사전을 사용하여 메시지 또는 콘텐츠 필터를 통해 메시지를 검사할 수 있습니다. 사전을 생성, 삭제, 확인하거나 사전에서 항목을 추가 및 삭제하거나 전체 사전을 가져오고 내보낼 수 있습니다. 또한 각 사전에 대해 대/소문자 구분 및 단어 경계 탐지를 결정할 수 있습니다. 예를 들어, 비밀어 또는 금기어의 목록을 생성하고 필터 규칙을 사용해 목록에서 단어의 메시지를 검사하여 일치하는 단어가 포함된 메시지를 삭제하거나 아카이브할 수 있습니다. 또한 특정 용어가 필터 작업을 더 쉽게 트리거할 수 있도록 사전에 "가중치" 용어를 추가할 수 있습니다.

사전에 비 ASCII 문자가 포함될 수 있습니다.

텍스트 리소스

텍스트 리소스는 고지 사항, 알림 템플릿 및 안티바이러스 템플릿과 같은 텍스트 개체입니다. AsyncOS의 다양한 구성 요소에 사용할 수 있는 새 개체를 생성할 수 있습니다. 텍스트 리소스를 가져오거나 내보낼 수 있습니다.

메시지 고지 사항 스탬핑

메시지 고지 사항 스탬핑을 사용하여 메시지에 고지 사항 텍스트 리소스를 추가할 수 있습니다. 예를 들어, 회사 내에서 전송된 모든 메시지에 저작권 정보, 홍보 메시지 또는 고지 사항을 추가할 수 있습니다.

콘텐츠 사전

콘텐츠 사전은 어플라이언스의 본문 검사 기능과 함께 사용하는 단어 또는 항목 그룹이며 콘텐츠 및 메시지 필터에 모두 사용할 수 있습니다. 회사 정책에 따라 적절한 작업을 수행할 수 있도록 메시지, 메시지 헤더, 사전에 포함된 용어의 메시지 첨부 파일을 검사하기 위해 사용자가 정의하는 사전을 사용합니다. 예를 들어, 비밀어 또는 금기어의 목록을 생성하고 필터 규칙을 사용해 목록에서 단어를 포함하는 메시지를 검사하여 메시지를 삭제, 아카이브 또는 격리할 수 있습니다.

AsyncOS 운영 체제에는 GUI(Mail Policies(메일 정책) > Dictionaries(사전))를 사용하거나 CLI에서 `dictionaryconfig` 명령을 사용하여 총 100개의 사전을 정의할 수 있는 기능이 있습니다. 사전을 생성, 삭제, 확인하거나 사전에서 항목을 추가 및 삭제하거나 전체 사전을 가져오고 내보낼 수 있습니다.

관련 주제

- 사전 콘텐츠, 21-2페이지
- 사전을 텍스트 파일로 가져오기 및 내보내기, 21-3페이지
- 사전 추가, 21-4페이지
- 사전 삭제, 21-5페이지
- 사전 가져오기, 21-5페이지
- 사전 내보내기, 21-5페이지

사전 콘텐츠

사전의 단어는 줄당 하나의 텍스트 문자열로 생성되며 항목은 일반 텍스트 또는 정규식 형태일 수 있습니다. 사전에 비 ASCII 문자도 포함될 수 있습니다. 정규식 사전을 정의하면 더 유연하게 일치하는 용어를 찾을 수 있지만 그렇게 하려면 단어를 올바르게 구분하는 방법을 이해해야 합니다. Python 스타일 정규식에 대한 자세한 설명은 다음 사이트에서 액세스할 수 있는 Python Regular Expression HOWTO를 참조하십시오.

`http://www.python.org/doc/howto/`

참고 사전 항목의 시작 부분에 특수 문자 #을 사용하려면 주석으로 처리되지 않도록 문자 클래스 [#]를 사용할 수 있습니다.

각 용어에 대해 특정 용어가 필터 조건을 더 쉽게 트리거할 수 있도록 "가중치" 용어를 지정합니다. AsyncOS가 콘텐츠 사전 용어의 메시지를 검사할 때 용어 인스턴스의 수에 용어의 가중치를 곱해서 메시지에 "점수"를 매깁니다. 따라서 가중치가 3인 2개의 용어 인스턴스는 6점이 됩니다. 그런 다음 AsyncOS가 이 점수와 콘텐츠 또는 메시지 필터와 관련된 임계값과 비교하여 메시지가 필터 작업을 트리거해야 하는지 결정합니다.

또한 콘텐츠 사전에 스마트 식별자를 추가할 수 있습니다. 스마트 식별자는 데이터에서 주민등록 번호 및 ABA 라우팅 번호와 같은 일반적인 숫자 패턴에 해당하는 패턴을 검색하는 알고리즘입니다. 이러한 식별자는 정책 적용 시 유용할 수 있습니다. 정규식에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 적용" 장의 "규칙의 정규식"을 참조하십시오. 스마트 식별자에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 적용" 장의 "스마트 식별자"를 참조하십시오.

참고 비 ASCII 문자를 포함하는 사전은 터미널의 CLI에 제대로 표시되거나 표시되지 않을 수 있습니다. 비 ASCII 문자를 포함하는 사전을 보거나 변경할 수 있는 가장 좋은 방법은 사전을 텍스트 파일로 내보내서 편집한 다음 새 파일을 다시 어플라이언스로 가져오는 것입니다. 자세한 내용은 사전을 텍스트 파일로 가져오기 및 내보내기, 21-3페이지를 참고하십시오.

관련 주제

- 단어 경계 및 더블바이트 문자 집합, 21-3페이지

단어 경계 및 더블바이트 문자 집합

일부 언어(더블바이트 문자 집합)에서는 단어 또는 단어 경계의 개념이나 사례가 없습니다. 단어를 구성하는 문자인지 아닌지 구별하는 개념(정규식 구문에서 "\w"로 나타남)에 의존하는 복합한 정규식을 사용하면 로캘을 알 수 없거나 인코딩을 확실히 알지 못할 경우에 문제가 발생할 수 있습니다. 따라서 단어 경계 적용을 비활성화할 수 있습니다.

사전을 텍스트 파일로 가져오기 및 내보내기

콘텐츠 사전 기능에는 기본적으로 어플라이언스의 구성 디렉토리에 위치한 다음 텍스트 파일도 포함됩니다.

- `config.dtd`
- `profanity.txt`
- `proprietary_content.txt`
- `sexual_content.txt`

이러한 텍스트 파일은 콘텐츠 사전 기능과 함께 사용하여 새 사전을 생성할 수 있도록 고안되었습니다. 이러한 콘텐츠 사전은 가중치가 적용되며 스마트 식별자를 사용하여 더 효과적으로 데이터에서 패턴을 탐지하고 해당 패턴이 규제 준수 문제를 나타낼 경우 필터를 트리거합니다.

참고 사전 가져오기 및 내보내기 기능은 전체 단어 일치 및 대/소문자 구분 설정을 유지하지 않습니다. 이 설정은 구성 파일에서만 유지됩니다.

구성 디렉토리에 대한 자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스"를 참조하십시오.

또한 자체 사전 파일을 생성하고 이를 어플라이언스로 가져올 수도 있습니다. 비 ASCII 문자를 사전에 추가하는 가장 좋은 방법은 어플라이언스 외부에서 해당 문자를 텍스트 파일로 사전에 추가하고 해당 파일을 어플라이언스로 옮긴 다음 새 사전으로 가져오는 것입니다. 사전 가져오기에 대한 자세한 내용은 사전 가져오기, 21-5페이지를 참조하십시오. 사전 내보내기에 대한 자세한 내용은 사전 내보내기, 21-5페이지를 참조하십시오.

주의 이러한 텍스트 파일에는 일부 사용자가 불쾌하거나 외설적이거나 모욕적이라고 느낄 수 있는 용어가 포함됩니다. 이러한 파일의 용어를 콘텐츠 사전으로 가져올 경우 나중에 어플라이언스에 구성된 콘텐츠 사전을 볼 때 용어가 표시됩니다.

사전 추가

절차

1단계 **Mail Policies(메일 정책) > Dictionaries page(사전 페이지)**로 이동합니다.

2단계 **Add Dictionary(사전 추가)**를 클릭합니다.

3단계 사전의 이름을 입력합니다.

4단계 (선택 사항) 고급 일치를 구성합니다.

참고 AsyncOS는 사용자가 **전체 단어 일치** 및 **대/소문자 구분** 설정을 구성 파일에 저장하면 이러한 설정을 유지합니다. 사전을 가져오거나 내보낼 경우에는 AsyncOS가 이러한 설정을 유지하지 않습니다.

5단계 (선택 사항) 스마트 식별자를 사전에 추가합니다.

스마트 식별자는 데이터에서 주민등록번호 및 ABA 라우팅 번호와 같은 일반적인 숫자 패턴에 해당하는 패턴을 검색하는 알고리즘입니다. 스마트 식별자에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 적용" 장을 참조하십시오.

6단계 새 사전 항목을 용어 목록에 입력합니다.

여러 개의 새 항목을 추가하고 이러한 항목이 동일하게 필터 작업을 트리거할 수 있게 하려면 각각의 새 항목을 해당 줄에 넣습니다.

참고 정규식을 사용하는 콘텐츠 사전 항목: 시작 부분 또는 끝 부분에 ".*"가 표시되어 있으면 "단어" MIME 부분과 일치하는 용어가 발견될 경우 시스템이 잠깁니다. Cisco Systems에서는 콘텐츠 사전 항목의 시작 부분 또는 앞 부분에 ".*"를 사용하지 말라고 권장합니다.

7단계 용어의 가중치를 지정합니다.

다른 용어보다 필터 작업을 트리거할 가능성이 높아지도록 사전 용어에 "가중치"를 적용할 수 있습니다. 이 가중치를 사용하여 필터 작업을 결정하는 방법에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 적용" 장의 "콘텐츠 사전 점수 임계값"을 참조하십시오.

8단계 **Add(추가)**를 클릭합니다.

9단계 변경 사항을 제출하고 커밋합니다.

관련 주제

- 사전 콘텐츠, 21-2페이지

사전 삭제

시작하기 전에

AsyncOS가 올바르지 않아서 삭제된 사전을 참조하는 메시지 필터에 표시합니다. AsyncOS는 삭제된 사전을 참조하는 콘텐츠 필터를 활성화된 상태로 유지하지만 그러한 필터를 false로 평가합니다.

절차

1단계 **Mail Policies(메일 정책) > Dictionaries page(사전 페이지)**로 이동합니다.

2단계 사전 목록에서 삭제할 사전 옆의 휴지통 아이콘을 클릭합니다.

확인 메시지에 현재 해당 사전을 참조하고 있는 모든 필터가 표시됩니다.

3단계 확인 메시지에서 **Delete(삭제)**를 클릭합니다.

4단계 변경 사항을 커밋합니다.

사전 가져오기

시작하기 전에

가져올 파일이 어플라이언스의 구성 디렉토리에 있는지 확인합니다.

절차

1단계 **Mail Policies(메일 정책) > Dictionaries page(사전 페이지)**로 이동합니다.

2단계 **Import Dictionary(사전 가져오기)**를 클릭합니다.

3단계 가져올 위치를 선택합니다.

4단계 가져올 파일을 선택합니다.

5단계 사전 용어에 사용할 기본 가중치를 선택합니다.

AsyncOS가 가중치가 지정되지 않은 모든 용어에 기본 가중치를 지정합니다. 파일을 가져온 후에 가중치를 편집할 수 있습니다.

6단계 인코딩을 선택합니다.

7단계 **Next(다음)**를 클릭합니다.

8단계 사전에 이름을 지정하고 편집합니다.

9단계 변경 사항을 제출하고 커밋합니다.

사전 내보내기

절차

1단계 **Mail Policies(메일 정책)** > Dictionaries page(사전 페이지)로 이동합니다.

2단계 **Export Dictionary(사전 내보내기)**를 클릭합니다.

3단계 내보낼 사전을 선택합니다.

4단계 내보낸 사전의 파일 이름을 입력합니다.

이는 어플라이언스의 구성 디렉토리에 생성될 파일의 이름입니다.

5단계 내보낼 위치를 선택합니다.

6단계 텍스트 파일의 인코딩을 선택합니다.

7단계 변경 사항을 제출하고 커밋합니다.

콘텐츠 사전 필터 규칙 사용 및 테스트

사전을 다양한 `dictionary-match()` 메시지 필터 규칙 및 콘텐츠 필터와 함께 사용할 수 있습니다.

관련 주제

- 사전 일치 필터 규칙, 21-6페이지

사전 일치 필터 규칙

이름이 `dictionary-match(<`*dictionary_name*`>)`인 메시지 필터 규칙(및 해당 기능)은 메시지 본문에 이름이 *dictionary_name*인 콘텐츠 사전의 정규식이 포함되어 있는지 평가합니다. 사전이 없는 경우 규칙이 false로 평가합니다.

`dictionary-match()` 규칙은 `body-contains()` 본문 검사 규칙과 유사하게 기능하므로 헤더가 아닌 메시지의 본문과 첨부 파일만 검사합니다.

헤더를 검사할 경우 해당 `*-dictionary-match()` 유형 규칙(`subject-dictionary-match()`와 사용자 지정 헤더를 포함한 헤더를 지정할 수 있는 좀 더 일반적인 규칙인 `header-dictionary-match()`와 같은 특정 헤더의 규칙이 있음)을 사용할 수 있습니다. 사전 일치에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 적용" 장의 "사전 규칙"을 참조하십시오.

표 21-1 콘텐츠 사전의 메시지 필터 규칙

규칙	구문	설명
사전 일치	`dictionary-match(<`*dictionary_name*`>)`	명명된 사전에 나열된 모든 정규식과 일치하는 단어가 메시지에 포함되어 있습니까?

다음 예제에서는 어플라이언스가 이전 예제에서 생성된 "secret_words"라는 사전에서 단어가 포함된 메시지를 검사할 경우 참조와 관리자를 바인딩하기 위해 `dictionary-match()` 규칙을 사용하는 새 메시지 필터를 생성합니다. 이 설정 때문에 사례와 정확하게 일치하는 전체 단어 "`codename`"이 포함된 메시지만 이 필터에 대해 true로 평가됩니다.

```
bcc_codenames:

   if (dictionary-match ('secret_words'))

      {
```

```
        bcc('administrator@example.com');
        }
```

이 예제에서는 정책 격리에 메시지를 전송합니다.

```
quarantine_codenames:
   if (dictionary-match ('secret_words'))
        {
        quarantine('Policy');
        }
```

관련 주제

- 사전 항목 예, 21-7페이지
- 콘텐츠 사전 테스트, 21-8페이지

사전 항목 예

표 21-2 사전 항목 예

설명	예
와일드카드	*
앵커	다음으로 끝나는 항목: foo$ 다음으로 시작하는 항목: ^foo
이메일 주소 (기간을 이스케이프하지 마십시오.)	**foo@example.com**, **@example.com** **example.com$**(끝) **@example.***
제목	**An email subject** (이메일 제목에 ^ 앵커를 사용할 경우 종종 제목에 "RE:" 또는 "FW:" 등이 추가됩니다.)

콘텐츠 사전 테스트

trace 기능을 이용하면 dictionary-match() 규칙을 사용하는 메시지 필터에 대한 빠른 피드백을 제공할 수 있습니다. 자세한 내용은 테스트 메시지를 사용한 메일 흐름 디버깅: 추적, 40-1페이지를 참조하십시오. 또한 quarantine() 작업을 사용하여 위의 quarantine_codenames 필터 예에서처럼 필터를 테스트할 수 있습니다.

텍스트 리소스 이해

텍스트 리소스는 메시지에 첨부하거나 메시지로 전송할 수 있는 텍스트 템플릿입니다. 텍스트 리소스는 다음 유형 중 하나일 수 있습니다.

- **메시지 고지 사항 -** 메시지에 추가되는 텍스트입니다. 자세한 내용은 고지 사항 템플릿, 21-12페이지를 참고하십시오.
- **알림 템플릿 -** notify() 및 notify-bcc() 작업에 사용되어 알림으로 전송되는 메시지입니다. 자세한 내용은 알림 템플릿, 21-19페이지를 참고하십시오.
- **안티바이러스 알림 템플릿 -** 메시지에서 바이러스가 발견된 경우에 알림으로 전송되는 메시지입니다. 컨테이너(원본 메시지에 추가됨)에 사용하거나 추가된 메시지 없이 알림으로 전송할 템플릿을 생성할 수 있습니다. 자세한 내용은 안티바이러스 알림 템플릿, 21-20페이지를 참고하십시오.
- **바운스 및 암호화 실패 알림 템플릿 -** 메시지가 바운스되거나 메시지 암호화가 실패할 경우 알림으로 전송되는 메시지입니다. 자세한 내용은 바운스 및 암호화 실패 알림 템플릿, 21-23페이지를 참고하십시오.
- **암호화 알림 템플릿 -** 발송 이메일을 암호화하도록 어플라이언스를 구성할 경우에 전송되는 메시지입니다. 이 메시지는 수신자에게 암호화된 메시지를 수신했음을 알리고 메시지를 읽는 지침을 제공합니다. 자세한 내용은 암호화 알림 템플릿, 21-24페이지를 참고하십시오.

CLI(textconfig) 또는 GUI를 사용하여 추가, 삭제, 편집, 가져오기, 내보내기와 같은 텍스트 리소스 관리를 수행할 수 있습니다. GUI를 사용하여 텍스트 리소스를 관리하는 방법에 대한 내용은 텍스트 리소스 관리의 개요, 21-9페이지를 참조하십시오.

텍스트 리소스에는 비 ASCII 문자가 포함될 수 있습니다.

참고 비 ASCII 문자를 포함하는 텍스트 리소스는 터미널의 CLI에서 제대로 표시되거나 표시되지 않을 수 있습니다. 비 ASCII 문자를 포함하는 텍스트 리소스를 보거나 변경하려면 텍스트 리소스를 텍스트 파일로 내보내서 편집한 다음 새 파일을 다시 어플라이언스로 가져옵니다. 자세한 내용은 텍스트 리소스를 텍스트 파일로 가져오기 및 내보내기, 21-8페이지를 참고하십시오.

관련 주제

- 텍스트 리소스를 텍스트 파일로 가져오기 및 내보내기, 21-8페이지

텍스트 리소스를 텍스트 파일로 가져오기 및 내보내기

어플라이언스의 구성 디렉토리에 액세스할 수 있어야 합니다. 가져온 텍스트 파일은 어플라이언스의 구성 디렉토리에 있어야 합니다. 내보낸 텍스트 파일은 구성 디렉토리에 저장됩니다.

구성 디렉토리에 액세스하는 방법에 대한 자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스"를 참조하십시오.

비 ASCII 문자를 텍스트 리소스에 추가하려면 어플라이언스 외부에서 해당 용어를 텍스트 파일로 텍스트 리소스에 추가하고 해당 파일을 어플라이언스로 옮긴 다음 새 텍스트 리소스로 가져옵니다. 텍스트 리소스 가져오기에 대한 자세한 내용은 텍스트 리소스 가져오기, 21-10페이지를 참조하십시오. 텍스트 리소스 내보내기에 대한 내용은 텍스트 리소스 내보내기, 21-10페이지를 참조하십시오.

텍스트 리소스 관리의 개요

GUI에서 또는 CLI를 사용하여 텍스트 리소스를 관리할 수 있습니다. 이 섹션에서는 GUI를 중점적으로 다룹니다.

`textconfig` 명령을 사용하여 CLI에서 텍스트 리소스를 관리합니다.

텍스트 리소스 관리에는 다음과 같은 작업이 포함됩니다.

- 추가
- 편집 및 삭제
- 내보내기 및 가져오기
- 모든 텍스트 리소스의 일반 텍스트 메시지 정의
- 일부 텍스트 리소스 유형의 HTML 기반 메시지 정의

관련 주제

- 텍스트 리소스 추가, 21-9페이지
- 텍스트 리소스 삭제, 21-10페이지
- 텍스트 리소스 가져오기, 21-10페이지
- 텍스트 리소스 내보내기, 21-10페이지
- HTML 기반 텍스트 리소스의 개요, 21-11페이지

텍스트 리소스 추가

절차

1단계 **Mail Policies(메일 정책)** > **Text Resources(텍스트 리소스)**로 이동합니다.

2단계 **Add Text Resource(텍스트 리소스 추가)**를 클릭합니다.

3단계 **Name(이름)** 필드에 텍스트 리소스의 이름을 입력합니다.

4단계 **Type(유형)** 필드에서 텍스트 리소스의 유형을 선택합니다.

5단계 **Text(텍스트)** 또는 **HTML and Plain Text(HTML 및 일반 텍스트)** 필드에 메시지 텍스트를 입력합니다.

텍스트 리소스에 일반 텍스트 메시지만 사용할 수 있는 경우 **Text(텍스트)** 필드를 사용합니다. 텍스트 리소스에 HTML 및 일반 텍스트 메시지를 모두 사용할 수 있는 경우 **HTML and Plain Text(HTML 및 일반 텍스트)** 필드를 사용합니다.

6단계 변경 사항을 제출하고 커밋합니다.

관련 주제

- HTML 기반 텍스트 리소스의 개요, 21-11페이지

텍스트 리소스 삭제

시작하기 전에

텍스트 리소스 삭제는 다음과 같은 영향을 미칩니다.

- 삭제된 텍스트 리소스를 참조하는 모든 메시지 필터가 잘못된 필터로 표시됩니다.
- 삭제된 텍스트 리소스를 참조하는 콘텐츠 필터는 활성화된 상태로 유지되지만 false로 평가됩니다.

절차

1단계 **Mail Policies(메일 정책) > Text Resources(텍스트 리소스)** 페이지에서 삭제할 텍스트 리소스의 삭제 열 아래에 있는 휴지통 아이콘을 클릭합니다. 확인 메시지가 표시됩니다.

2단계 **Delete(삭제)**를 클릭하여 텍스트 리소스를 삭제합니다.

3단계 변경 사항을 커밋합니다.

텍스트 리소스 가져오기

시작하기 전에

가져올 파일이 어플라이언스의 구성 디렉토리에 있는지 확인합니다.

절차

1단계 **Mail Policies(메일 정책) > Text Resources(텍스트 리소스)** 페이지에서 **Import Text Resource(텍스트 리소스 가져오기)**를 클릭합니다.

2단계 가져올 파일을 선택합니다.

3단계 인코딩을 지정합니다.

4단계 **Next(다음)**를 클릭합니다.

5단계 이름을 선택하고 텍스트 리소스 유형을 선택합니다.

6단계 변경 사항을 제출하고 커밋합니다.

텍스트 리소스 내보내기

시작하기 전에

텍스트 리소스를 내보내면 어플라이언스의 구성 디렉토리에 텍스트 파일이 생성됩니다.

절차

1단계 **Mail Policies(메일 정책) > Text Resources(텍스트 리소스)** 페이지에서 **Export Text Resource(텍스트 리소스 내보내기)**를 클릭합니다.

2단계 내보낼 텍스트 리소스를 선택합니다.

3단계 텍스트 리소스의 파일 이름을 입력합니다.

4단계 텍스트 파일의 인코딩을 선택합니다.

5단계 **Submit(제출)**을 클릭하여 구성 디렉토리의 텍스트 리소스를 포함하는 텍스트 파일을 생성합니다.

HTML 기반 텍스트 리소스의 개요

고지 사항과 같은 일부 텍스트 리소스는 HTML 기반 및 일반 텍스트를 모두 사용해서 생성할 수 있습니다. HTML 기반 및 일반 텍스트 메시지를 모두 포함하는 텍스트 리소스를 이메일 메시지에 적용할 경우 HTML 기반 텍스트 리소스 메시지는 이메일 메시지의 텍스트/html 부분에 적용되고, 일반 텍스트 메시지는 이메일 메시지의 텍스트/일반 부분에 적용됩니다.

HTML 기반 텍스트 리소스를 추가하거나 편집할 경우 수동으로 HTML 코드를 작성하지 않고도 서식 있는 텍스트를 입력할 수 있는 서식 있는 텍스트 편집이 GUI에 포함됩니다.

HTML 기반 텍스트 리소스를 추가 및 편집할 경우 다음 정보를 고려하십시오.

- 메시지의 일반 텍스트 버전이 HTML 버전에 따라 자동으로 생성되게 하거나 일반 텍스트 버전을 개별적으로 정의할 수 있습니다.
- **Code View(코드 보기)** 버튼을 클릭하여 서식 있는 텍스트 편집기와 HTML 코드 사이에서 전환할 수 있습니다.
- 서식 있는 텍스트 편집기에서 지원되지 않는 HTML 코드를 GUI에 입력하려면 코드 보기로 전환하고 HTML 코드를 수동으로 입력합니다. 예를 들어, `<img src>` HTML 태그를 사용하여 외부 서버에 위치한 이미지 파일에 대한 참조를 삽입하여 이 작업을 수행할 수 있습니다.

관련 주제

- HTML 기반 텍스트 리소스 가져오기 및 내보내기, 21-11페이지

HTML 기반 텍스트 리소스 가져오기 및 내보내기

텍스트 파일로 또는 텍스트 파일에서 HTML 기반 텍스트 리소스를 내보내거나 가져올 수 있습니다. HTML 기반 텍스트 리소스를 파일로 내보낼 경우 파일에 다음과 같은 텍스트 리소스의 각 버전 섹션이 포함됩니다.

- `[html_version]`
- `[text_version]`

이러한 섹션의 순서는 중요하지 않습니다.

예를 들어 내보낸 파일에 다음 텍스트가 포함될 수 있습니다.

```
[html_version]
<p>Sample <i>message.</i></p>
[text_version]
Sample message.
```

HTML 기반 텍스트 리소스를 내보내거나 가져올 때 다음 규칙 및 지침을 고려하십시오.

- 일반 텍스트 메시지가 HTML 버전에서 자동으로 생성되는 HTML 기반 텍스트 리소스를 내보낼 경우 내보낸 파일에 `[text_version]` 섹션이 포함되지 않습니다.
- 텍스트 파일에서 가져올 경우 텍스트 리소스 유형이 HTML 메시지를 지원하면 `[html_version]` 섹션의 HTML 코드가 생성된 텍스트 리소스의 HTML 메시지로 변환됩니다. 마찬가지로, `[text_version]` 섹션의 텍스트가 생성된 텍스트 리소스의 일반 텍스트 메시지로 변환됩니다.
- 비어 있거나 없는 `[html_version]` 섹션이 포함된 파일에서 가져와 HTML 기반 텍스트 리소스를 생성할 경우 어플라이언스가 `[text_version]` 섹션의 텍스트를 사용하여 HTML 및 일반 텍스트 메시지를 모두 생성합니다.

텍스트 리소스 사용

모든 유형의 텍스트 리소스는 텍스트 리소스 페이지 또는 `textconfig` CLI 명령을 사용하여 동일한 방식으로 생성됩니다. 일단 생성되면 각 유형이 다른 방식으로 사용됩니다. 고지 사항 및 알림 템플릿은 필터 및 리스너에 사용되고, 안티바이러스 템플릿은 메일 정책 및 안티바이러스 설정에 사용됩니다.

관련 주제

- 고지 사항 템플릿, 21-12페이지
- 고지 사항 스탬핑 및 다중 인코딩, 21-17페이지
- 알림 템플릿, 21-19페이지
- 안티바이러스 알림 템플릿, 21-20페이지
- 바운스 및 암호화 실패 알림 템플릿, 21-23페이지
- 암호화 알림 템플릿, 21-24페이지

고지 사항 템플릿

어플라이언스가 리스너에서 수신하는 일부 또는 모든 메시지에 대해 텍스트 위 또는 아래(머리글 또는 바닥글)에 기본 고지 사항을 추가할 수 있습니다. 다음과 같은 방법을 사용하여 어플라이언스에서 메시지에 고지 사항을 추가할 수 있습니다.

- 리스너를 통해 GUI에서 또는 `listenerconfig` 명령 사용(리스너를 통해 고지 사항 텍스트 추가, 21-13페이지 참조)
- 콘텐츠 필터 작업 `Add Disclaimer Text` 사용(콘텐츠 필터 작업, 11-9페이지 참조).
- 메시지 필터 작업 `add-footer()` 사용("메시지 필터를 사용하여 이메일 정책 적용" 장 참조)
- 데이터 손실 방지 프로필 사용(데이터 유출 방지, 17-1페이지 참조)
- 신종 바이러스 필터(Outbreak Filter)의 메시지 수정을 사용하여 사용자에게 해당 메시지가 피싱 또는 맬웨어 배포 시도일 수 있음을 알림(메시지 수정, 14-6페이지 참조). 이 유형의 알림에 추가되는 고지 사항이 텍스트 위에 추가됩니다.

예를 들어, 회사 내에서 보낸 모든 메시지에 저작권 정보, 홍보 메시지 또는 고지 사항을 추가할 수 있습니다.

고지 사항 텍스트를 사용하기 전에 고지 사항 템플릿을 생성해야 합니다. GUI의 텍스트 리소스 페이지(텍스트 리소스 추가, 21-9페이지 참조) 또는 `textconfig` 명령(*Cisco AsyncOS CLI 참조 설명서* 참조)을 사용하여 사용할 텍스트 문자열 집합을 생성하고 관리할 수 있습니다.

관련 주제

- 리스너를 통해 고지 사항 텍스트 추가, 21-13페이지
- 필터를 통해 고지 사항 추가, 21-13페이지
- 고지 사항 및 필터 작업 변수, 21-14페이지

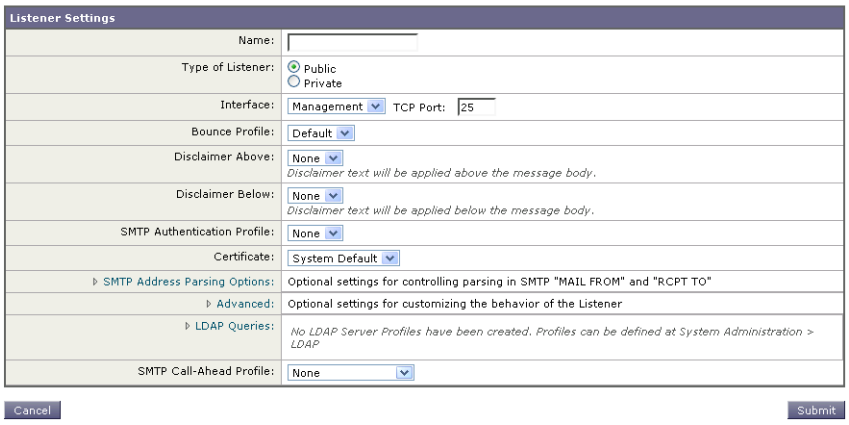
리스너를 통해 고지 사항 텍스트 추가

고지 사항 텍스트 리소스를 생성했으면 리스너에서 수신하는 메시지에 추가할 텍스트 문자열을 선택합니다. 메시지의 위 또는 아래에 고지 사항 텍스트를 추가할 수 있습니다. 이 기능은 공용(인바운드) 및 사설(아웃바운드) 리스너 모두에서 사용할 수 있습니다.

텍스트 및 HTML(Microsoft Outlook에서는 이러한 유형의 메시지를 "다중 파트 대체"라고 함)로 구성된 메시지를 보내면 어플라이언스가 메시지의 두 부분 모두에 고지 사항을 스탬핑합니다. 그러나 메시지에 서명된 콘텐츠가 있을 경우 수정하면 서명이 무효화되기 때문에 콘텐츠가 수정되지 않습니다. 대신 "`Content-Disposition inline attachment`."라는 고지 사항 스탬프가 포함된 새로운 부분이 생성됩니다. 멀티 파트 메시지에 대한 자세한 내용은 "메시지 필터를 사용하여 이메일 정책 적용" 장의 "메시지 본문 및 메시지 첨부 파일"을 참조하십시오.

다음 예에서는 GUI를 통해 리스너의 메시지에 적용할 고지 사항을 선택하는 방법을 보여줍니다.

그림 21-1 고지 사항을 포함하도록 리스너 편집



필터를 통해 고지 사항 추가

또한 필터 작업 `add-footer()` 또는 콘텐츠 필터 작업 "Add Disclaimer Text"를 사용하여 미리 정의된 특정한 텍스트 문자열을 메시지의 고지 사항에 추가할 수 있습니다. 예를 들어, 다음 메시지 필터 규칙은 LDAP 그룹 "Legal:"의 사용자가 보낸 모든 메시지에 `legal.disclaimer`라는 텍스트 문자열을 추가합니다.

```
Add-Disclaimer-For-Legal-Team:

if (mail-from-group == 'Legal')
```

```
{

  add-footer('legal.disclaimer');

}
```

고지 사항 및 필터 작업 변수

또한 메시지 필터 작업 변수를 사용할 수 있습니다(자세한 내용은 "메시지 필터를 사용하여 이메일 정책 적용" 장의 "작업 변수" 참조).

다음과 같은 변수를 고지 사항 템플릿에 사용할 수 있습니다.

표 21-3 안티바이러스 알림 변수

변수	대체 항목
$To	메시지 받는 사람: 헤더(봉투 수신자 아님)로 대체됩니다.
$From	메시지 보내는 사람: 헤더(봉투 발신자 아님)로 대체됩니다.
$Subject	원본 메시지의 제목으로 대체됩니다.
$Date	MM/DD/YYYY 형식을 사용하여 현재 날짜로 대체됩니다.
$Time	지역 표준 시간을 사용하여 현재 날짜로 대체됩니다.
$GMTimestamp	GMT를 사용하여 "수신됨: 이메일 메시지의 줄"에 있는 현재 시간 및 날짜로 대체됩니다.
$MID	메시지 ID 또는 내부에서 메시지를 식별하는 데 사용되는 "MID"로 대체됩니다. RFC822 "Message-Id" 값($Header를 사용하여 검색)과 혼동하지 마십시오.
$Group	메시지를 삽입할 때 발신자가 일치하는 발신자 그룹의 이름으로 대체됩니다. 발신자 그룹에 이름이 없는 경우 문자열 ">Unknown<"이 삽입됩니다.
$Policy	메시지를 삽입할 때 발신자에게 적용되는 HAT 정책의 이름으로 대체됩니다. 미리 정의된 정책 이름이 사용된 경우 문자열 ">Unknown<"이 삽입됩니다.
$Reputation	발신자의 SenderBase Reputation 점수로 대체됩니다. 평판 점수가 없는 경우 "없음"으로 대체됩니다.
$filenames	메시지 첨부 파일의 파일 이름 목록(쉼표로 구분됨)으로 대체됩니다.
$filetypes	메시지 첨부 파일의 파일 유형 목록(쉼표로 구분됨)으로 대체됩니다.
$filesizes	메시지 첨부 파일의 파일 크기 목록(쉼표로 구분됨)으로 대체됩니다.
$remotehost	Email Security 어플라이언스에 메시지를 보낸 시스템의 호스트 이름으로 대체됩니다.
$AllHeaders	메시지 헤더로 대체됩니다.
$EnvelopeFrom	메시지의 봉투 발신자(봉투 보낸 사람, <MAIL FROM>)로 대체됩니다.
$Hostname	Email Security 어플라이언스의 호스트 이름으로 대체됩니다.

표 21-3 안티바이러스 알림 변수 (계속)

변수	대체 항목
$header['*string*']	원본 메시지에 일치하는 헤더가 포함된 경우 따옴표로 묶인 헤더의 값으로 대체됩니다. 큰 따옴표도 사용될 수 있습니다.
$enveloperecipients	메시지의 모든 봉투 수신자(Envelope To, <RCPT TO>)로 대체됩니다.
$bodysize	메시지의 크기(바이트)로 대체됩니다.
$FilterName	처리할 필터의 이름을 반환합니다.
$MatchedContent	검사 필터 규칙(`body-contains` 및 콘텐츠 사전과 같은 필터 규칙 포함)을 트리거한 콘텐츠를 반환합니다.
$DLPPolicy	위반된 이메일 DLP 정책의 이름으로 대체됩니다.
$DLPSeverity	위반의 심각도로 대체됩니다. 심각도는 "낮음", "중간", "높음" 또는 "위험"일 수 있습니다.
$DLPRiskFactor	메시지의 민감한 자료의 위험 계수로 대체됩니다(0~100점).
$threat_category	피싱, 바이러스, 스캠 또는 맬웨어와 같은 신종 바이러스 필터(Outbreak Filter) 위협의 유형으로 대체됩니다.
$threat_type	신종 바이러스 필터(Outbreak Filter) 위협 범주의 하위 범주로 대체됩니다. 예를 들어, 자선 스캠, 금융 피싱 시도, 허위 거래 등이 될 수 있습니다.
$threat_description	신종 바이러스 필터(Outbreak Filter) 위협의 설명으로 대체됩니다.
$threat_level	메시지의 위협 수준(0~5점)으로 대체됩니다.
$threat_verdict	메시지 수정 위협 수준 임계값에 따라 예 또는 아니요로 대체됩니다. 메시지의 바이러스 또는 비 바이러스 위협 수준이 메시지 수정 위협 수준 임계값보다 크거나 같을 경우 이 변수의 값이 예로 설정됩니다.

고지 사항에 메시지 필터 작업 변수를 사용하려면 메시지 고지 사항(GUI의 텍스트 리소스 페이지 또는 **textconfig** 명령을 통해)을 생성하고 변수를 참조합니다.

```
(running textconfig command)


Enter or paste the message disclaimer here. Enter '.' on a blank line to end.
This message processed at: $Timestamp
.


Message disclaimer "legal.disclaimervar" created.


Current Text Resources:
```

```
1. legal.disclaimer (Message Disclaimer)

2. legal.disclaimervar (Message Disclaimer)


Choose the operation you want to perform:

- NEW - Create a new text resource.

- IMPORT - Import a text resource from a file.

- EXPORT - Export text resource to a file.

- PRINT - Display the content of a resource.

- EDIT - Modify a resource.

- DELETE - Remove a resource from the system.

[]>


mail3.example.com>commit
```

이제 필터에서 새 고지 사항을 사용합니다.

```
Add-Timestamp:

if (mail-from-group == 'Legal')

{

  add-footer('legal.disclaimervar');

}
```

`add-footer()` 작업은 바닥글을 따옴표로 묶인 인쇄 가능한 인라인, UTF-8 코딩 첨부로 추가하여 비 ASCII 텍스트를 지원합니다.

고지 사항 스탬핑 및 다중 인코딩

AsyncOS에는 다양한 문자 인코딩 작업으로 고지 사항 스탬핑 방식을 수정하는 데 사용되는 설정이 포함되어 있습니다. 기본적으로 AsyncOS는 이메일 메시지의 본문 부분 내에 고지 사항을 첨부하려고 시도합니다. `localeconfig` 명령 내에서 구성된 설정을 사용하여 본문 부분과 고지 사항의 인코딩이 다를 경우 동작을 구성할 수 있습니다. 이 설정을 이해하려면 이메일 메시지를 여러 부분으로 이루어진 메시지로 바라보는 것이 도움이 됩니다.

To: joe@example.com From: mary@example.com Subject: Hi!	헤더
<blank line>	
Hello!	본문 부분
This message has been scanned...	첫 번째 첨부 부분
Example.zip	두 번째 첨부 부분

첫 번째 빈 줄 뒤에 오는 메시지 부분에 여러 MIME 부분이 포함될 수 있습니다. 두 번째 및 다음 부분은 종종 "첨부"라고 부르며, 첫 번째는 종종 "본문" 또는 "텍스트"라고 부릅니다,

고지 사항은 이메일에 첨부(위) 또는 본문의 일부로 포함될 수 있습니다.

To: joe@example.com From: mary@example.com Subject: Hi!	헤더
<blank line>	
Hello!	본문 부분
This message has been scanned...	이제 고지 사항이 본문 부분에 포함되었음
Example.zip	첫 번째 첨부 부분

일반적으로 메시지 본문과 고지 사항의 인코딩이 일치하지 않을 경우 AsyncOS가 동일한 인코딩의 전체 메시지를 메시지 본문으로 인코딩하려고 시도하므로 고지 사항이 별첨이 아닌 본문("인라인")에 포함됩니다. 다시 말해서, 고지 사항의 인코딩과 본문의 인코딩이 일치하지 않거나 고지 사항의 텍스트에 인라인으로(본문에) 표시될 수 있는 문자가 들어 있는 경우 고지 사항이 인라인으로 포함됩니다. 예를 들어, ISO-8859-1을 통해 US-ASCII 문자만 포함된 고지 사항을 인코딩할 수 있으며 그 결과 고지 사항이 문제 없이 "인라인"으로 표시됩니다.

그러나 고지 사항과 본문을 결합할 수 없는 경우 `localeconfig` 명령을 사용하여 고지 사항이 메시지의 본문에 포함될 수 있게 본문 텍스트를 승격 또는 변환하여 고지 사항의 인코딩과 일치시키도록 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: Only try encoding from

message body


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]>


Footers or headings are added in-line with the message body whenever

possible. However, if the footer or heading 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 footer or
heading. If that fails, and if the message body's encoding is US-
ASCII, the system can try to edit the message body to use the footer's
or heading's encoding. Should the system try to impose the footer's
or headings's encoding on the message body? [N]> y

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

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
```

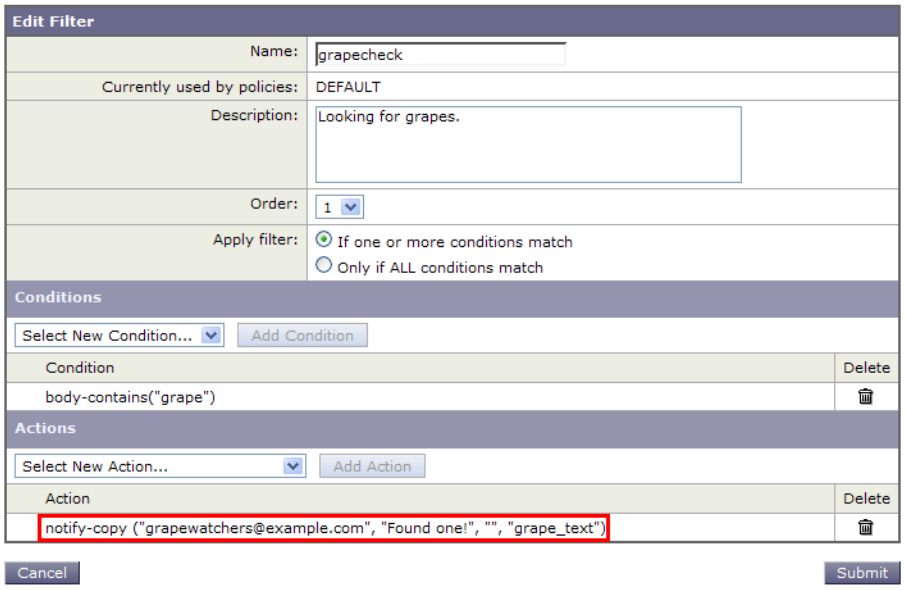
localeconfig 명령에 대한 자세한 내용은 "메일을 수신하도록 어플라이언스 구성" 장을 참조하십시오.

알림 템플릿

알림 템플릿은 `notify()` 및 `notify-copy()` 필터 작업에 사용됩니다. 알림 템플릿에는 안티바이러스 알림에 사용되는 안티바이러스 관련 변수를 포함한 비 ASCII 텍스트 및 작업 변수("메시지 필터를 사용하여 이메일 정책 적용" 장의 "작업 변수" 참조)가 포함될 수 있습니다. 예를 들어, `$Allheaders` 작업 변수를 사용하여 원본 메시지의 헤더를 포함할 수 있습니다. 알림의 보내는 사람: 주소를 구성할 수 있습니다. 관련 내용은 어플라이언스에서 생성된 메시지의 복귀 주소 구성, 33-33페이지를 참조하십시오.

알림 템플릿을 생성하면 콘텐츠 및 메시지 필터에서 참조할 수 있습니다. 그림 21-2에서는 `notify-copy()` 필터 작업이 "grapewatchers@example.com:"에 "grape_text" 알림을 전송하도록 설정된 콘텐츠 필터를 보여줍니다.

그림 21-2 콘텐츠 필터의 알림 예



안티바이러스 알림 템플릿

다음과 같은 2가지 유형의 안티바이러스 알림 템플릿이 있습니다.

- **안티바이러스 알림 템플릿**. 안티바이러스 알림 템플릿은 원본 메시지가 바이러스 알림에 첨부되지 않은 경우에 사용됩니다.
- **안티바이러스 컨테이너 템플릿**. 컨테이너 템플릿은 원본 메시지가 첨부 파일로 전송될 경우에 사용됩니다.

안티바이러스 알림 템플릿은 필터가 아닌 안티바이러스 엔진에 사용된다는 점을 제외하고 기본적으로 알림 템플릿과 동일한 방식으로 사용됩니다. 메일 정책을 편집할 때 전송할 사용자 지정 알림을 지정할 수 있습니다. 안타바이러스 알림의 보내는 사람: 주소를 구성할 수 있습니다. 관련 내용은 어플라이언스에서 생성된 메시지의 복귀 주소 구성, 33-33페이지를 참조하십시오.

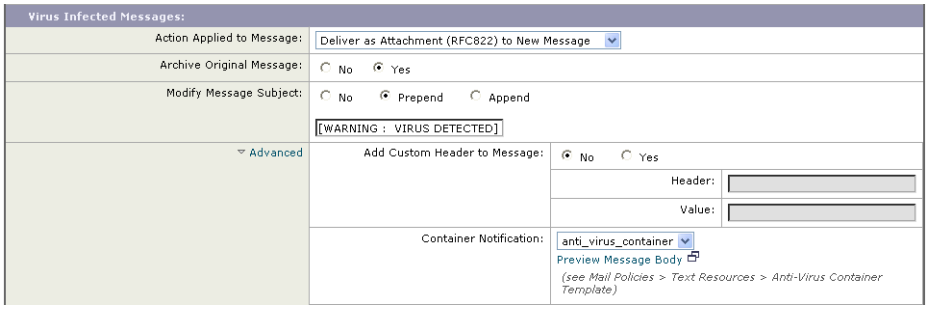
관련 주제

- 사용자 지정 안티바이러스 알림 템플릿, 21-20페이지

사용자 지정 안티바이러스 알림 템플릿

그림 21-3에서는 사용자 지정 안티바이러스 알림이 지정된 메일 정책을 보여줍니다.

그림 21-3 메일 정책의 안티바이러스 컨테이너 템플릿 알림 예



관련 주제

- 안티바이러스 알림 변수, 21-21페이지

안티바이러스 알림 변수

안티바이러스 알림을 생성할 경우 표 21-4에 나열된 알림 변수를 사용할 수 있습니다.

표 21-4 안티바이러스 알림 변수

변수	대체 항목
$To	메시지 받는 사람: 헤더(봉투 수신자 아님)로 대체됩니다.
$From	메시지 보내는 사람: 헤더(봉투 발신자 아님)로 대체됩니다.
$Subject	원본 메시지의 제목으로 대체됩니다.
$AV_VIRUSES	메시지에의 어느 지점에서든 발견되는 모든 바이러스의 목록으로 대체됩니다. "Unix/Apache.Trojan", "W32/Bagel-F"
$AV_VIRUS_TABLE	각 부분의 MIME 부분/첨부 파일 이름 및 바이러스의 표로 대체됩니다. "HELLO.SCR" : "W32/Bagel-F" <unnamed part of the message> : "Unix/Apache.Trojan"
$AV_VERDICT	안티바이러스 판정으로 대체됩니다.
$AV_DROPPED_TABLE	삭제된 첨부 파일의 표로 대체됩니다. 각 행은 한 부분 또는 파일 이름과 그 뒤에 나오는 해당 부분과 관련된 바이러스의 목록으로 구성됩니다. "HELLO.SCR" : "W32/Bagel-f", "W32/Bagel-d" "Love.SCR" : "Netsky-c", "W32/Bagel-d"
$AV_REPAIRED_VIRUSES	발견되어 해결된 모든 바이러스의 목록으로 대체됩니다.
$AV_REPAIRED_TABLE	발견되어 해결된 모든 부분 및 바이러스의 표로 대체됩니다. "HELLO.SCR" : "W32/Bagel-F"
$AV_DROPPED_PARTS	삭제된 파일 이름의 목록으로 대체됩니다. "HELLO.SCR", "CheckThisOut.exe"
$AV_REPAIRED_PARTS	복구된 파일 이름 또는 부분의 목록으로 대체됩니다.
$AV_ENCRYPTED_PARTS	암호화된 파일 이름 또는 부분의 목록으로 대체됩니다.
$AV_INFECTED_PARTS	바이러스가 포함된 파일의 파일 이름 목록(쉼표로 구분됨)으로 대체됩니다.

표 21-4 안티바이러스 알림 변수 (계속)

변수	대체 항목
$AV_UNSCANNABLE_PARTS	검사하지 못한 파일 이름 또는 부분의 목록으로 대체됩니다.
$Date	MM/DD/YYYY 형식을 사용하여 현재 날짜로 대체됩니다.
$Time	지역 표준 시간을 사용하여 현재 날짜로 대체됩니다.
$GMTimestamp	GMT를 사용하여 "수신됨: 이메일 메시지의 줄"에 있는 현재 시간 및 날짜로 대체됩니다.
$MID	메시지 ID 또는 내부에서 메시지를 식별하는 데 사용되는 "MID"로 대체됩니다. RFC822 "Message-Id" 값($Header를 사용하여 검색)과 혼동하지 마십시오.
$Group	메시지를 삽입할 때 발신자가 일치하는 발신자 그룹의 이름으로 대체됩니다. 발신자 그룹에 이름이 없는 경우 문자열 ">Unknown<"이 삽입됩니다.
$Policy	메시지를 삽입할 때 발신자에게 적용되는 HAT 정책의 이름으로 대체됩니다. 미리 정의된 정책 이름이 사용된 경우 문자열 ">Unknown<"이 삽입됩니다.
$Reputation	발신자의 SenderBase Reputation 점수로 대체됩니다. 평판 점수가 없는 경우 "없음"으로 대체됩니다.
$filenames	메시지 첨부 파일의 파일 이름 목록(쉼표로 구분됨)으로 대체됩니다.
$filetypes	메시지 첨부 파일의 파일 유형 목록(쉼표로 구분됨)으로 대체됩니다.
$filesizes	메시지 첨부 파일의 파일 크기 목록(쉼표로 구분됨)으로 대체됩니다.
$remotehost	Email Security 어플라이언스에 메시지를 보낸 시스템의 호스트 이름으로 대체됩니다.
$AllHeaders	메시지 헤더로 대체됩니다.
$EnvelopeFrom	메시지의 봉투 발신자(봉투 보낸 사람, <MAIL FROM>)로 대체됩니다.
$Hostname	Email Security 어플라이언스의 호스트 이름으로 대체됩니다.

참고 변수 이름은 대/소문자를 구분하지 않습니다. 예를 들어, 텍스트 리소스에서 "$to"를 지정할 경우 "$To"를 지정해도 같은 효과가 있습니다. "AV_" 변수가 원본 메시지에서 비어 있을 경우 문자열 `<None>`이 대체됩니다.

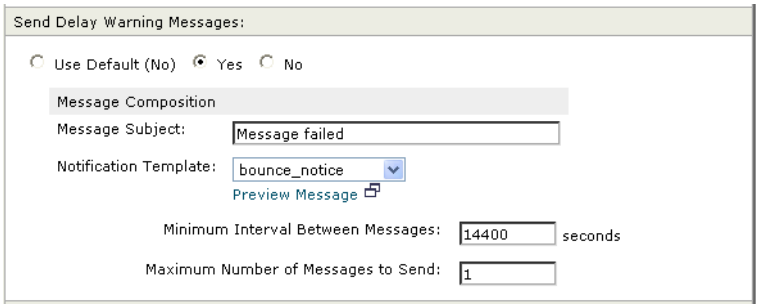
텍스트 리소스가 정의된 후 **Mail Policies(메일 정책) > Incoming/Outgoing Mail Policies(수신/발송 메일 정책) > Edit Anti-Virus Settings(안티바이러스 설정 편집)** 페이지 또는 `policyconfig -> edit -> antivirus` 명령을 사용하여 원본 메시지가 복구되었거나, 검사할 수 없거나, 암호화되었거나, 바이러스에 감염된 메시지의 RFC 822 첨부 파일로 포함되도록 지정합니다. 자세한 내용은 사용자 지정 경고 알림 전송(수신자에게만), 12-12페이지를 참조하십시오.

바운스 및 암호화 실패 알림 템플릿

바운스 및 암호화 실패 알림 템플릿은 바운스 알림 및 메시지 암호화 실패 알림에 사용된다는 점을 제외하고 기본적으로 알림 템플릿과 동일한 방식으로 사용됩니다. 바운스 프로필 편집 시 전송할 사용자 지정 바운스 알림을 지정하고 암호화 프로필 편집 시 사용자 지정 메시지 암호화 실패 알림을 지정할 수 있습니다.

그림 21-4에서는 바운스 프로필에 지정된 바운스 알림 템플릿을 보여줍니다.

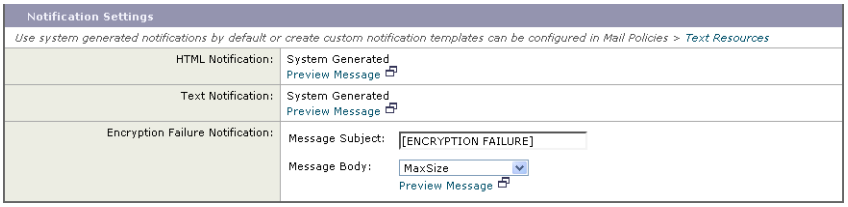
그림 21-4 바운스 프로필의 바운스 알림 예



참고 사용자 지정 템플릿을 사용하려면 RFC-1891 DSN을 사용해야 합니다.

그림 21-5에서는 암호화 프로필에 지정된 암호화 실패 템플릿을 보여줍니다.

그림 21-5 암호화 프로필의 암호화 실패 알림 예



관련 주제

- 바운스 및 암호화 실패 알림 변수, 21-23페이지

바운스 및 암호화 실패 알림 변수

바운스 또는 암호화 실패 알림을 생성할 경우 표 21-5에 나열된 알림 변수를 사용할 수 있습니다.

표 21-5 바운스 알림 변수

변수	대체 항목
$Subject	원본 메시지의 제목입니다.
$Date	MM/DD/YYYY 형식을 사용하여 현재 날짜로 대체됩니다.
$Time	지역 표준 시간을 사용하여 현재 날짜로 대체됩니다.
$GMTimeStamp	GMT를 사용하여 "수신됨: 이메일 메시지의 줄"에 있는 현재 시간 및 날짜로 대체됩니다.

표 21-5 바운스 알림 변수 (계속)

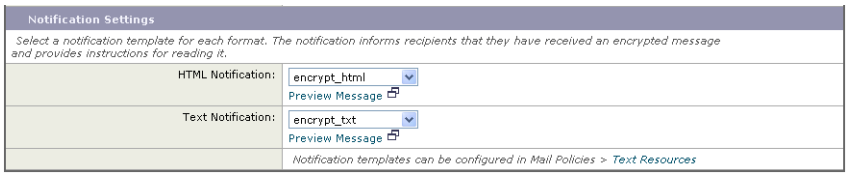
변수	대체 항목
$MID	메시지 ID 또는 내부에서 메시지를 식별하는 데 사용되는 "MID"로 대체됩니다. RFC822 "Message-Id" 값($Header를 사용하여 검색)과 혼동하지 마십시오.
$BouncedRecipient	바운스된 수신자 주소
$BounceReason	이 알림의 이유
$remotehost	Email Security 어플라이언스에 메시지를 보낸 시스템의 호스트 이름으로 대체됩니다.

암호화 알림 템플릿

암호화 알림 템플릿은 아웃바운드 이메일을 암호화하도록 Cisco 이메일 암호화를 구성할 경우에 사용됩니다. 이 알림은 수신자에게 암호화된 메시지를 수신했음을 알리고 메시지를 읽는 지침을 제공합니다. 암호화된 메시지와 함께 전송하도록 사용자 지정 암호화 알림을 지정할 수 있습니다. 암호화 프로필을 생성할 때 HTML 및 텍스트 암호화 알림을 모두 지정합니다. 따라서 사용자 지정 프로필을 생성하려면 텍스트 및 HTML 알림을 모두 생성해야 합니다.

그림 21-6에서는 암호화 프로필에 지정된 암호화 알림을 보여줍니다.

그림 21-6 암호화 프로필에서 활성화된 암호화 알림 템플릿



22 장

SMTP 서버를 사용하여 수신자 검증

SMTP Call-Ahead 수신자 검증 개요

SMTP Call-Ahead 수신자 검증 기능은 수신자의 수신 메일을 수락하기 전에 외부 SMTP 서버를 쿼리합니다. LDAP 수락 또는 RAT(Recipient Access Table)를 사용할 수 없을 때 이 기능을 사용하여 수신자를 검증할 수 있습니다. 예를 들어, 별도의 도메인을 각각 사용하여 여러 사서함의 메일을 호스팅하고 LDAP 인프라에서 LDAP 서버를 쿼리하여 각 수신자를 검증하도록 허용하지 않는다고 가정해 보겠습니다. 이 경우 Email Security 어플라이언스가 SMTP 서버를 쿼리하고 SMTP 대화를 계속하기 전에 수신자를 검증할 수 있습니다.

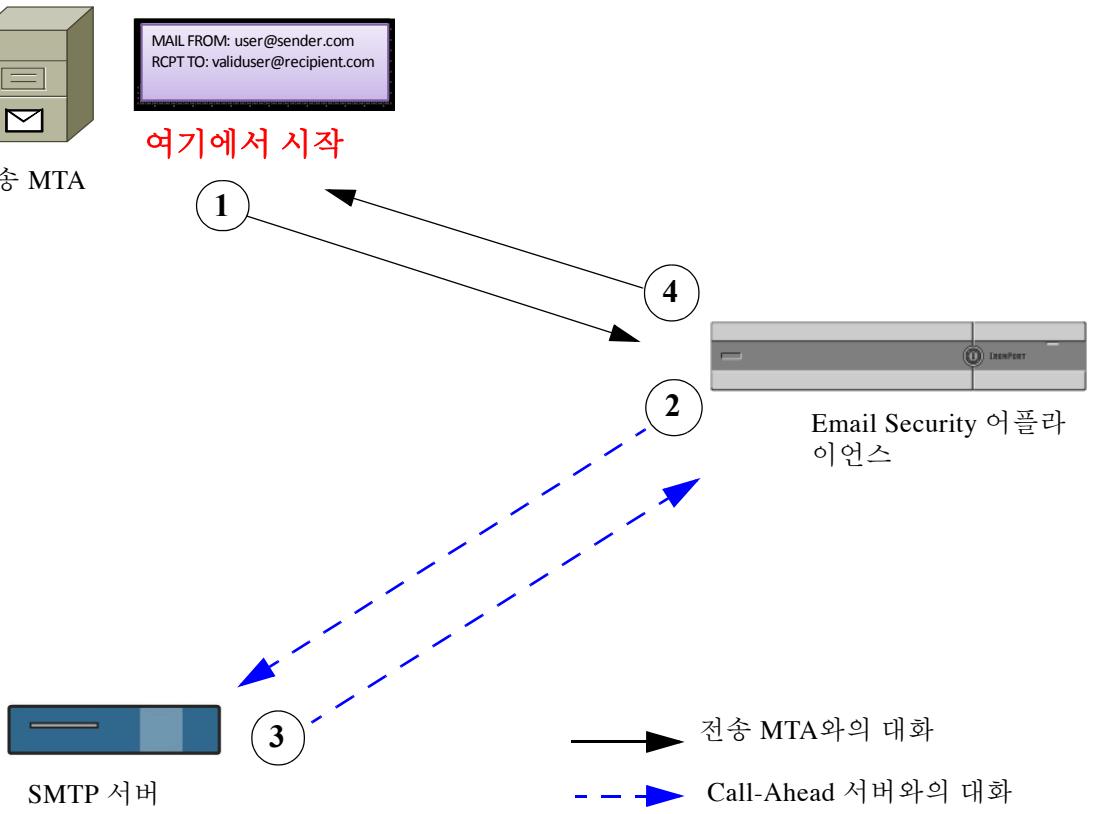
올바르지 않은 수신자의 메시지에 대한 처리를 줄이기 위해 SMTP Call-Ahead 수신자 검증을 사용할 수 있습니다. 일반적으로 올바르지 않은 수신자의 메시지는 작업 큐를 통과한 후에 삭제될 수 있습니다. 그 대신 이메일 파이프라인의 수신/받기 단계에서 추가 처리 요청 없이 잘못된 메시지가 삭제 또는 바운스될 수 있습니다.

SMTP Call-Ahead 수신자 검증 워크플로

SMTP call-ahead 수신자 검증을 수행하도록 Email Security 어플라이언스를 구성할 경우 Email Security 어플라이언스가 수신자를 확인하기 위해 SMTP 서버를 "미리 호출"하는 동안 전송 MTA와의 SMTP 대화를 일시 중지합니다. 어플라이언스가 SMTP 서버를 쿼리할 경우 SMTP 서버의 응답을 Email Security 어플라이언스에 반환하고 구성한 설정에 따라 메일을 수락하거나 코드 및 사용자 지정 응답과의 연결을 삭제할 수 있습니다.

그림 22-1에서는 SMTP Call-Ahead 검증 대화의 기본 워크플로를 보여줍니다.

그림 22-1 SMTP Call Ahead 서버 대화 워크플로



1. 전송 MTA가 SMTP 대화를 시작합니다.
2. Email Security 어플라이언스가 SMTP에 쿼리를 보내 수신자를 확인하는 동안 (*validuser@recipient.com*) SMTP 대화를 일시 중지합니다.

   참고 SMTP 경로 또는 LDAP 라우팅 쿼리가 구성된 경우 이러한 경로가 SMTP 서버를 쿼리하는 데 사용됩니다.

3. SMTP 서버가 Email Security 어플라이언스에 쿼리 응답을 반환합니다.
4. Email Security 어플라이언스가 SMTP 대화를 다시 시작하고 전송 MTA에 응답을 보내므로 SMTP 서버 응답(및 SMTP Call-Ahead 프로필에 구성한 설정)에 따라 대화가 계속되거나 연결이 삭제될 수 있습니다.

이메일 파이프라인의 처리 순서로 인해 지정된 수신자의 메시지가 RAT에서 거부된 경우 SMTP Call-Ahead 수신자 검증이 발생하지 않습니다. 예를 들어, RAT에서 *example.com*의 메일만 수락되도록 지정한 경우 *recipient@domain2.com*의 메일이 거부되어야 SMTP Call-Ahead 수신자 검증이 발생할 수 있습니다.

참고 HAT에서 DHAP(디렉토리 수집 공격 방지)를 구성한 경우 SMTP Call-Ahead 서버 거부는 사용자가 지정한 시간당 최대 수신자 오류에 포함된 거부 수의 일부입니다. 추가 SMTP 서버 거부를 처리하려면 이 수를 조정해야 합니다. DHAP에 대한 자세한 내용은 "메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

외부 SMTP 서버를 사용하여 수신자를 검증하는 방법

표 22-1 외부 SMTP 서버를 사용하여 수신자를 검증하는 방법

	수행할 작업	추가 정보
1단계	어플라이언스가 SMTP 서버에 연결하여 서버의 응답을 해석하는 방법을 결정합니다.	Call-Ahead 서버 프로필 구성, 22-3페이지
2단계	SMTP 서버를 사용하여 수신자를 검증하도록 공용 리스너를 구성합니다.	리스너를 사용하여 SMTP 서버를 통해 수신 메일 검증, 22-6페이지
3단계	(선택 사항) 메일을 다른 호스트로 라우팅할 때 사용할 SMTP 서버를 결정하도록 LDAP 라우팅 쿼리를 업데이트합니다.	LDAP 라우팅 쿼리 설정 구성, 22-6페이지
4단계	(선택 사항) 특정 수신자의 Call-Ahead 검증을 우회하도록 어플라이언스를 구성합니다.	특정 사용자 또는 그룹에 대해 SMTP Call-Ahead 검증 우회, 22-8페이지

관련 주제

- Call-Ahead 서버 프로필 구성, 22-3페이지

Call-Ahead 서버 프로필 구성

SMTP Call-Ahead 서버 프로필을 구성할 경우 Email Security 어플라이언스가 SMTP 서버와 연결하는 방법과 SMTP 서버에서 다시 전송된 응답을 해석하는 방법을 결정하는 설정을 지정합니다.

절차

1단계 **Network(네트워크) > SMTP Call-Ahead**를 클릭합니다.

2단계 **Add Profile(프로필 추가)**을 클릭합니다.

3단계 프로필의 설정을 입력합니다. 자세한 내용은 표 22-2SMTP Call-Ahead 서버 프로필 설정, 22-4페이지를 참고하십시오.

4단계 프로필의 고급 설정을 구성합니다. 자세한 내용은 표 22-3SMTP Call-Ahead 서버 프로필 고급 설정, 22-5페이지를 참고하십시오.

5단계 변경 사항을 제출하고 커밋합니다.

관련 주제

- SMTP Call-Ahead 서버 프로필 설정, 22-4페이지
- Call Ahead 서버 응답, 22-5페이지

SMTP Call-Ahead 서버 프로필 설정

SMTP Call-Ahead 서버 프로필을 구성할 경우 Email Security 어플라이언스가 SMTP 서버와 연결하는 방법을 결정하는 설정을 구성해야 합니다.

표 22-2 SMTP Call-Ahead 서버 프로필 설정

설정	설명
프로필 이름	Call-Ahead 서버 프로필의 이름입니다.
Call-Ahead 서버 유형	다음 방법 중 하나를 선택하여 Call-Ahead 서버에 연결할 수 있습니다. • **전송 호스트 사용**. SMTP Call-Ahead 쿼리에 사용되는 전송 이메일 주소의 호스트를 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 이러한 경로가 쿼리할 SMTP 서버를 결정하는 데 사용됩니다. LDAP 라우팅 쿼리 구성에 대한 자세한 내용은 LDAP 라우팅 쿼리 설정 구성, 22-6페이지를 참조하십시오. • **정적 Call-Ahead 서버**. 쿼리할 Call-Ahead 서버의 정적 목록을 생성하려면 이 옵션을 사용합니다. Call-Ahead 서버의 이름과 위치가 자주 변경되지 않을 경우 이 옵션을 사용할 수 있습니다. 이 옵션을 사용하면 Email Security 어플라이언스가 나열된 정적 Call-Ahead 서버에서 시작하여 라운드 로빈 방식으로 호스트를 쿼리합니다. **참고** 정적 Call-Ahead 서버 유형을 선택하면 SMTP 경로가 쿼리에 적용되지 않습니다. MX 조회를 수행하는 대신 호스트에서 A 조회를 수행하여 정적 서버의 Call-Ahead IP 주소를 가져옵니다.
정적 Call-Ahead 서버	정적 Call-Ahead 서버 유형을 사용하기로 선택할 경우 이 필드에 호스트 및 포트 조합 목록을 입력합니다. 다음 구문을 사용하여 서버와 포트를 나열합니다. `ironport.com:25` 입력 항목이 여럿인 경우에는 쉼표로 구분하십시오.

표 22-3에서는 SMTP Call-Ahead 서버 프로필 고급 설정을 설명합니다.

표 22-3 SMTP Call-Ahead 서버 프로필 고급 설정

설정	설명
인터페이스	SMTP 서버와의 SMTP 대화를 시작하는 데 사용되는 인터페이스입니다. 관리 인터페이스 또는 자동을 사용하도록 선택합니다. 자동을 선택하면 Email Security 어플라이언스가 사용할 인터페이스를 자동으로 탐지하려고 시도합니다. Cisco IronPort 인터페이스가 다음과 같은 방법으로 SMTP 서버에 연결하려고 시도합니다. • Call-Ahead 서버가 구성된 인터페이스 중 하나와 동일한 서브넷에 있는 경우 일치하는 인터페이스가 연결을 시작합니다. • 구성된 SMTP 경로가 쿼리를 라우팅하는 데 사용됩니다. • 그렇지 않으면 기본 게이트웨이와 동일한 서브넷에 있는 인터페이스가 사용됩니다.
MAIL FROM 주소	SMTP 서버와의 SMTP 대화에 사용되는 MAIL FROM: 주소입니다.
검증 요청 시간 초과	SMTP 서버에서 결과를 기다리는 시간(초)입니다. 이 시간 초과 값은 여러 Call-Ahead 서버 연결을 포함할 수 있는 단일 수신자 검증 요청에 적용됩니다. Call Ahead 서버 응답, 22-5페이지를 참조하십시오.
검증 실패 작업	시간 초과, 서버 실패, 네트워크 문제 또는 알 수 없는 응답으로 인해 수신자 검증 요청이 실패할 경우 수행할 작업입니다. Email Security 어플라이언스가 다양한 응답을 처리하는 방식을 구성할 수 있습니다. Call Ahead 서버 응답, 22-5페이지를 참조하십시오.
임시 실패 작업	수신자 검증 요청이 일시적으로 실패하고 4xx 응답이 원격 SMTP 서버에서 반환될 경우 수행할 작업입니다. 이는 사서함이 꽉 찼거나 사서함을 사용할 수 없거나 서비스를 사용할 수 없는 경우에 발생할 수 있습니다. Call Ahead 서버 응답, 22-5페이지를 참조하십시오.
세션당 최대 수신자	단일 SMTP 세션에서 검증할 최대 수신자 수입니다. 1~25,000개의 세션을 지정합니다.
서버당 최대 연결	단일 SMTP Call-Ahead 서버에 대한 최대 연결 수입니다. 1~100개의 연결을 지정합니다.
캐시	SMTP 응답에 대한 캐시 크기입니다. 100~1,000,000개의 항목을 지정합니다.
캐시 TTL	캐시의 항목에 대한 Time-to-live 값입니다. 이 필드는 기본적으로 900초로 설정됩니다. 60~86,400초를 지정합니다.

Call Ahead 서버 응답

SMTP 서버가 다음과 같은 응답을 반환할 수 있습니다.

- **2xx**: Call-Ahead 서버에서 2로 시작하는 SMTP 코드가 수신될 경우 수신자가 수락됩니다. 예를 들어, 응답 250은 메일링 작업이 계속되게 할 수 있습니다.
- **4xx**: 4로 시작하는 SMTP 코드는 SMTP 요청을 처리하는 동안 일시적인 실패가 발생했음을 의미합니다. 재시도가 나중에 성공적으로 처리될 수 있습니다. 예를 들어, 응답 451은 요청된 작업이 취소되었거나 처리 도중 로컬 오류가 발생했음을 의미합니다.

- **5xx**: 5로 시작하는 SMTP 코드는 SMTP 요청을 처리하는 도중 영구적인 실패가 발생했음을 의미합니다. 예를 들어, 응답 550은 요청된 작업이 수행되지 않았거나 사서함을 사용할 수 없었음을 의미합니다.
- **시간 초과.** Call-Ahead 서버에서 응답이 반환되지 않으면 시간 초과가 발생하기 전에 재시도를 시도하는 시간을 구성할 수 있습니다.
- **연결 오류**. Call-Ahead 서버에 대한 연결이 실패할 경우 수신자 주소에 대한 연결을 수락할지 아니면 거부할지 구성할 수 있습니다.

리스너를 사용하여 SMTP 서버를 통해 수신 메일 검증

SMTP Call-Ahead 서버 프로필을 생성한 후에는 리스너가 SMTP 서버를 통해 수신 메일을 검증할 수 있도록 리스너에서 SMTP Call-Ahead 서버 프로필을 활성화해야 합니다. 사설 리스너에는 수신자 검증이 필요하지 않으므로 SMTP Call-Ahead 기능은 공용 리스너에서만 사용할 수 있습니다.

절차

1단계 **Network(네트워크) > Listeners(리스너)**로 이동합니다.

2단계 SMTP Call-Ahead 기능을 활성화할 리스너의 이름을 클릭합니다.

3단계 **SMTP Call Ahead Profile** 필드에서 활성화할 SMTP Call-Ahead 프로필을 선택합니다.

4단계 변경 사항을 제출하고 커밋합니다.

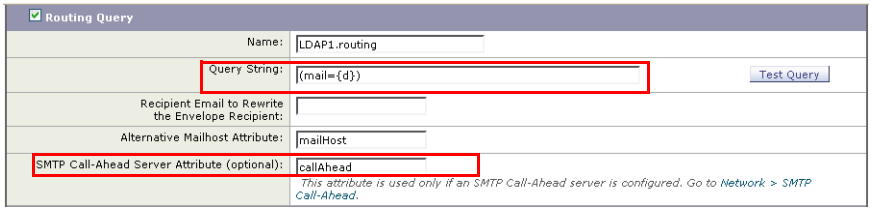
LDAP 라우팅 쿼리 설정 구성

LDAP 라우팅 쿼리를 사용하여 다른 메일 호스트에 메일을 라우팅할 경우 AsyncOS가 대체 메일호스트 특성을 사용하여 쿼리할 SMTP 서버를 결정합니다. 그러나 이렇게 하지 않는 것이 좋은 경우도 있습니다. 예를 들어, 다음 스키마에서는 메일 호스트 특성(`mailHost`)의 SMTP 주소가 Call-Ahead SMTP 서버 특성(`callAhead`)에 나열된 서버와 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 서버에 전달하는 라우팅 쿼리를 생성할 수 있습니다. 예를 들어, 다음 특성으로 라우팅 쿼리를 생성할 수 있습니다.

그림 22-2 SMTP Call-Ahead에 대해 구성된 LDAP 라우팅 쿼리:



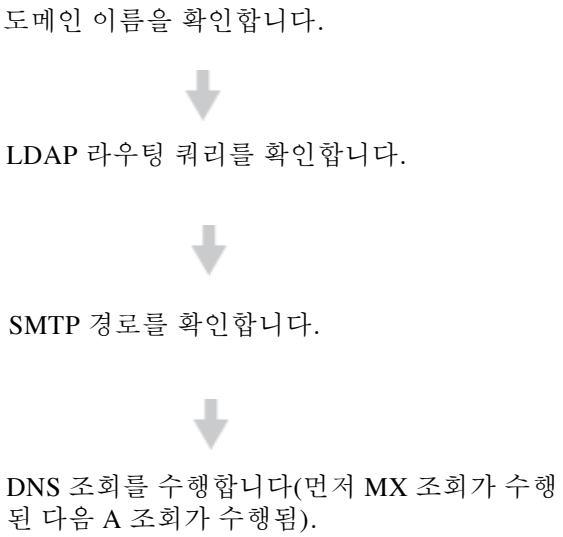
이 쿼리에서 {d}는 수신자 주소의 도메인 부분을 나타내며, SMTP Call-Ahead 서버 특성이 포트 9025에 대한 쿼리: smtp2.mydomain.com, smtp3.mydomain.com에 사용되어야 하는 Call-Ahead 서버 및 포트에 대한 값을 반환합니다.

참고 이 예에서는 LDAP 라우팅 쿼리를 사용하여 SMTP Call-Ahead 쿼리를 올바른 SMTP 서버에 전달할 수 있는 쿼리를 구성하는 한 가지 방법만을 보여줍니다. 이 예에 설명된 쿼리 문자열 또는 특정 LDAP 특성을 사용할 필요가 없습니다.

SMTP Call-Ahead 쿼리 라우팅

SMTP Call-Ahead 쿼리를 라우팅하면 AsyncOS가 다음 순서로 정보를 확인합니다.

그림 22-3 SMTP Call Ahead 쿼리 라우팅 워크플로



LDAP 라우팅 쿼리가 없거나 도메인에 대해 SMTP 경로가 구성되지 않은 경우 이전 상태의 결과가 다음 단계로 전달됩니다. SMTP 경로가 없는 경우 DNS 조회가 수행됩니다.

SMTP Call-Ahead 쿼리에 대해 LDAP 라우팅 쿼리를 사용하고 SMTP 경로도 구성된 경우 라우팅 쿼리에서 반환한 값에 따라 라우팅 동작이 달라집니다.

- LDAP 라우팅 쿼리가 포트 없이 단일 호스트 이름을 반환하면 SMTP Call-Ahead 쿼리가 SMTP 경로를 적용합니다. SMTP 경로에 대상 호스트만 호스트 이름으로 나열될 경우 SMTP 서버의 IP를 가져오기 위해 DNS 조회가 수행됩니다.

- LDAP 라우팅 쿼리가 포트와 함께 단일 호스트 이름을 반환하면 SMTP 경로가 사용되지만 LDAP 쿼리에서 반환한 포트가 SMTP 경로에 지정된 포트 대신 사용됩니다. SMTP 경로에 대상 호스트만 호스트 이름으로 나열될 경우 SMTP 서버의 IP를 가져오기 위해 DNS 조회가 수행됩니다.
- LDAP 라우팅 쿼리가 포트와 함께 또는 포트 없이 여러 호스트를 반환하면 SMTP 경로가 적용되지만 LDAP 라우팅 쿼리에서 반환한 포트가 SMTP 경로에 있는 포트 대신 사용됩니다. SMTP 경로에 대상 호스트만 호스트 이름으로 나열될 경우 SMTP 서버의 IP를 가져오기 위해 DNS 조회가 수행됩니다.

특정 사용자 또는 그룹에 대해 **SMTP Call-Ahead** 검증 우회

리스너에서 SMTP Call-Ahead 검증을 활성화하되 특정 사용자 또는 사용자 그룹에 대해 SMTP Call-Ahead 검증을 건너뛸 수 있습니다.

SMTP Call-Ahead 쿼리 도중 메일이 지연되면 안 되는 수신자에 대해 SMTP Call-Ahead 검증을 건너뛸 수 있습니다. 예를 들어, 사용자가 알고 있는 고객 서비스 별칭이 올바르며 즉각적인 주의가 필요한 경우 RAT 항목을 추가할 수 있습니다.

GUI를 통해 SMTP Call-Ahead 검증 우회를 구성하려면 RAT 항목을 추가하거나 편집할 때 **Bypass SMTP Call-Ahead(SMTP Call-Ahead 우회)**를 선택합니다.

23 장

다른 MTA와의 통신 암호화

다른 MTA와의 통신 암호화에 대한 개요

엔터프라이즈 게이트웨이 또는 MTA(메시지 전송 에이전트)는 일반적으로 인터넷에서 "암호화되지 않은 상태"로 통신합니다. 즉, 통신은 암호화되지 않습니다. 일부 시나리오에서 악성 에이전트는 발신자 또는 수신자의 정보 없이 이 통신을 가로챌 수 있습니다. 통신은 제3자가 모니터링하거나 변경할 수도 있습니다.

TLS(전송 계층 보안)는 SSL(Secure Socket Layer) 기술의 개선된 버전으로, 인터넷에서 SMTP 대화를 암호화하는 데 많이 사용되는 메커니즘입니다. AsyncOS는 SMTP(TLS를 통한 보안 SMTP)의 STARTTLS 확장을 지원하며 이에 대해서는 RFC 3207(RFC 2487은 더 이상 사용되지 않음)에 설명되어 있습니다.

AsyncOS에서 TLS를 구현하면 개인 정보를 암호화를 통해 보호할 수 있습니다. 이를 통해 인증 기관 서비스에서 X.509 인증서 및 개인 키를 가져오거나 자체 서명된 인증서를 만들어 어플라이언스에서 사용할 수 있습니다. AsyncOS는 공용 및 개인 리스너에 대해 별도의 TLS 인증서를 지원합니다. 또한, 인터페이스, LDAP 인터페이스 및 모든 발송 TLS 연결에 대한 보안 HTTP(HTTPS) 관리 액세스에 대해서도 별도의 TLS 인증서를 지원합니다.

관련 주제

- TLS를 사용하여 SMTP 대화를 암호화하는 방법, 23-2페이지

TLS를 사용하여 SMTP 대화를 암호화하는 방법

표 23-1 TLS를 사용하여 SMTP 대화를 암호화하는 방법

	수행할 작업	추가 정보
1단계	공인 인증 기관에서 X.509 인증서 및 개인 키를 얻습니다.	인증서 얻기, 23-2페이지
2단계	Email Security 어플라이언스에 인증서를 설치합니다.	다음 중 하나의 방식으로 인증서를 설치합니다. • GUI를 사용하여 자체 서명된 인증서 생성, 23-3페이지 • GUI를 사용하여 인증서 가져오기, 23-5페이지
3단계	메시지 수신, 메시지 전달 또는 두 가지 모두를 위한 TLS를 활성화합니다.	• 리스너의 HAT에서 TLS 활성화, 23-6페이지 • 전달 시 TLS 및 인증서 확인 활성화, 23-9페이지
4단계	(선택 사항) 신뢰할 수 있는 인증 기관 목록을 사용자 지정하여 어플라이언스가 원격 도메인에서 수신된 인증서를 확인하여 도메인의 자격 증명을 설정하도록 합니다.	인증 기관 목록 관리하기, 23-15페이지
5단계	(선택 사항) TLS 연결이 필요한 도메인에 메시지를 전달할 수 없는 경우 Email Security 어플라이언스를 구성하여 경고를 보냅니다.	필수 TLS 연결이 실패할 경우 경고 보내기, 23-11페이지

인증서 얻기

TLS를 사용하려면 Email Security 어플라이언스에는 X.509 인증서가 있어야 하며 이와 일치하는 수신 및 전달을 위한 개인 키가 있어야 합니다. SMTP 수신 및 전달에 모두 동일한 인증서를 사용하고, 인터페이스, LDAP 인터페이스 및 대상 제어로의 모든 발송 TLS 연결에 대한 HTTPS 서비스마다 서로 다른 인증서를 사용하거나 모두에 하나의 인증서를 사용할 수 있습니다.

공인 인증 기관에서 인증서 및 인증 키를 구매할 수 있습니다. 인증 기관은 ID를 확인하고 공개 키를 배포하는 데 사용하는 디지털 인증서를 발급하는 타사입니다. 이 기관은 인증서가 유효하고 신뢰할 수 있는 ID로 발급되었음을 추가로 보장합니다. Cisco 어플라이언스에서 서비스를 하나씩 사용하지 않는 것이 좋습니다.

Email Security 어플라이언스는 특정 사용자를 위해 자체 서명된 인증서를 만들고, 공용 인증서를 가져오기 위해 인증 기관에 제출할 CSR(인증서 서명 요청)을 생성할 수 있습니다. 인증 기관은 개인 키로 서명한 신뢰할 수 있는 공용 인증서를 반환합니다. GUI의 Network(네트워크) > Certificates(인증서) 페이지 또는 CLI의 `certconfig` 명령을 사용하여 자체 서명된 인증서를 만들고, CSR을 생성하고, 신뢰할 수 있는 공용 인증서를 설치합니다.

처음으로 인증서를 얻거나 생성하는 경우 "인증 기관 서비스 SSL Server Certificates"를 인터넷에서 검색하고 해당 조직의 요구 사항에 가장 맞는 서비스를 선택합니다. 인증서를 얻으려면 서비스 지침을 따릅니다.

GUI의 Network(네트워크) > Certificates(인증서) 페이지 또는 CLI의 `certconfig` 명령을 사용하여 인증서를 구성한 후 `print` 명령을 사용하여 전체 인증서 목록을 볼 수 있습니다. `print` 명령은 중간 인증서를 표시하지 않습니다.

주의 어플라이언스에 데모 인증서가 제공되어 TLS 및 HTTPS 기능을 테스트할 수 있지만, 데모 인증서로 이러한 서비스를 활성화하는 것은 안전하지 않으며 일반적인 사용에는 사용하지 않는 것이 좋습니다. 기본 데모 인증서로 이러한 서비스를 활성화하는 경우 경고 메시지가 CLI에 출력됩니다.

관련 주제

- 중간 인증서, 23-3페이지
- 인증서 및 중앙 집중식 관리, 23-3페이지
- GUI를 사용하여 자체 서명된 인증서 생성, 23-3페이지
- GUI를 사용하여 인증서 가져오기, 23-5페이지
- 자체 서명된 인증서 생성 또는 CLI를 사용하여 인증서 가져오기, 23-5페이지
- GUI를 사용하여 인증서 내보내기, 23-5페이지

중간 인증서

루트 인증서 확인 이외에도 AsyncOS는 중간 인증서 확인 기능을 지원합니다. 중간 인증서는 추가 인증서를 만드는 데 사용되는 신뢰할 수 있는 루트 인증 기관에서 발급하며 효과적으로 신뢰 관계를 구축합니다. 예를 들어 신뢰할 수 있는 루트 인증 기관으로부터 인증서 발급 권한을 받은 godaddy.com은 인증서를 발급할 수 있습니다. godaddy.com에서 발급한 인증서와 관련하여 신뢰할 수 있는 루트 인증 기관에서 얻은 개인 키뿐만 아니라 godaddy.com에서 얻은 개인 키도 검증해야 합니다.

인증서 및 중앙 집중식 관리

인증서는 일반적으로 인증서의 공용 이름으로 로컬 컴퓨터의 호스트 이름을 사용합니다. Email Security 어플라이언스가 클러스터에 연결된 경우 클러스터 수준에서 설치할 수 있는 와일드카드 인증서를 제외하고 머신 수준으로 각 클러스터 멤버에 대한 인증서를 가져와야 합니다. 멤버의 리스너가 다른 머신과 통신할 때 이를 참조할 수 있도록 클러스터 멤버의 인증서는 동일한 인증서 이름을 사용해야 합니다.

GUI를 사용하여 자체 서명된 인증서 생성

다음 이유로 인해 어플라이언스에서 인증서를 만들거나 가져오려고 할 수 있습니다.

- TLS를 사용하여 다른 MTA로 SMTP 대화를 암호화하기 위해(인바운드 및 아웃바운드 대화 모두).
- HTTPS를 사용하여 GUI에 액세스하도록 어플라이언스에서 HTTPS 서비스를 활성화하기 위해.
- LDAP 서버에서 클라이언트 인증서를 요청하는 경우 LDAPS의 클라이언트 인증서로 사용하기 위해.
- 어플라이언스와 DLP용 RSA Enterprise Manager 간 안전한 통신을 하기 위해.

절차

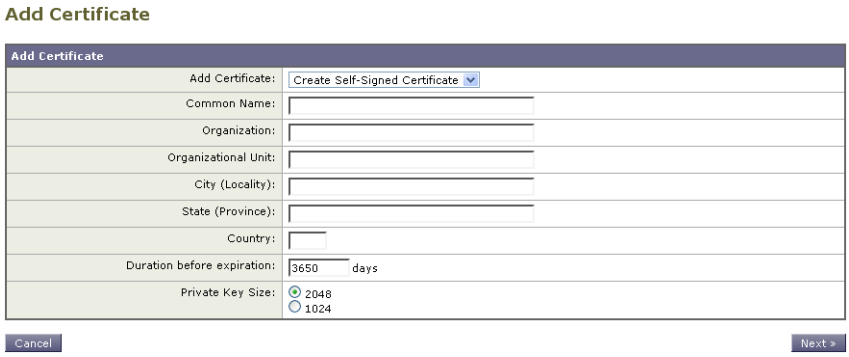
1단계 Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.

2단계 **Add Certificate(인증서 추가)**를 클릭합니다.

3단계 Create Self-Signed Certificate(자체 서명된 인증서 만들기)을 선택합니다.

그림 23-1에서는 Create Self-Signed Certificate(자체 서명된 인증서 만들기) 옵션이 선택된 Add Certificate(인증서 추가) 페이지를 보여줍니다.

그림 23-1 Add Certificate(인증서 추가) 페이지



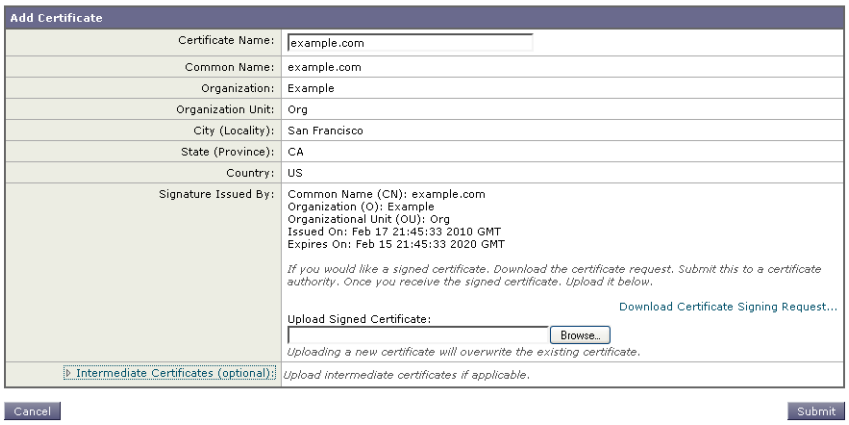
4단계 자체 서명된 인증서에 다음 정보를 입력합니다.

공용 이름	정규화된 도메인 이름.
조직	조직의 정확한 법인명.
조직 단위	조직의 부서.
군/구	조직이 법률상 위치하는 군/구입니다.
시/도	조직이 법률상 위치하는 시/도입니다.
국가	조직이 법률상 위치하는 국가의 두 글자 ISO 약어입니다.
만료 전까지 기간	인증서가 만료되기 전 일수.
개인 키 크기	CSR를 위해 생성할 개인 키 크기. 2048비트 및 1024비트만 지원됩니다.

5단계 **Next(다음)**를 클릭하여 인증서 및 서명 정보를 확인합니다.

그림 23-2에서는 자체 서명된 인증서의 예를 보여줍니다.

그림 23-2 Certificate(인증서) 페이지 보기



6단계 인증서의 이름을 입력합니다. AsyncOS는 기본적으로 이전에 입력한 공용 이름을 할당합니다.

7단계 자체 서명된 인증서의 CSR을 인증 기관에 제출하려면 **Download Certificate Signing Request(인증서 서명 요청 다운로드)**를 클릭하여 CSR을 PEM 형식으로 로컬 또는 네트워크 머신에 저장합니다.

8단계 변경사항을 제출하고 커밋합니다.

인증 기관이 개인 키로 서명한 신뢰할 수 있는 공용 인증서를 반환하는 경우 Certificates(인증서) 페이지에 있는 인증서 이름을 클릭하고 로컬 머신 또는 네트워크에 있는 파일 경로를 입력하여 업로드합니다. 어플라이언스에 업로드하기 전에 받은 신뢰할 수 있는 공용 인증서가 PEM 형식 또는 PEM 형식으로 전환할 수 있는 형식인지 확인합니다. (이 작업을 수행하기 위한 툴은 OpenSSL에 포함되어 있으며 이는 http://www.openssl.org에서 무료로 받을 수 있는 소프트웨어입니다.)

인증 기관에서 받은 인증서를 업로드하면 기존 인증서에 덮어쓰기합니다. 또한, 자체 서명된 인증서와 관련된 중간 인증서를 업로드할 수 있습니다. 공용 또는 개인 리스너, IP 인터페이스의 HTTPS 서비스, LDAP 인터페이스 또는 대상 제어와의 모든 발송 TLS 연결에서 인증서를 사용할 수 있습니다.

GUI를 사용하여 인증서 가져오기

AsyncOS에서는 PKCS #12 형식으로 저장된 인증서를 가져와 어플라이언스에서 사용할 수 있습니다.

절차

1단계 Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.

2단계 **Add Certificate(인증서 추가)**를 클릭합니다.

3단계 **Import Certificate(인증서 가져오기)** 옵션을 선택합니다.

4단계 네트워크 또는 로컬 머신에 있는 인증서 파일에 대한 경로를 입력합니다.

5단계 파일의 비밀번호를 입력합니다.

6단계 **Next(다음)**를 클릭하여 인증서 정보를 확인합니다.

7단계 인증서의 이름을 입력합니다.

AsyncOS는 기본적으로 공용 이름을 할당합니다.

8단계 변경사항을 제출하고 커밋합니다.

자체 서명된 인증서 생성 또는 CLI를 사용하여 인증서 가져오기

CLI로 자체 서명된 인증서를 생성하거나 인증서를 가져오려면 `certconfig` 명령을 사용합니다.

GUI를 사용하여 인증서 내보내기

AsyncOS에서는 PKCS #12 형식으로 인증서를 내보내고 저장할 수 있습니다.

절차

1단계 Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.

2단계 **Export Certificate(인증서 내보내기)**를 클릭합니다.

3단계 내보낼 인증서를 선택합니다.

4단계 인증서의 파일 이름을 입력합니다.

5단계 인증서 파일의 비밀번호를 입력합니다.

6단계 **Export(내보내기)**를 클릭합니다.

7단계 파일을 로컬 또는 네트워크 머신에 저장합니다.

8단계 추가 인증서를 내보내거나 **Cancel(취소)**을 클릭하여 Network(네트워크) > Certificates(인증서) 페이지로 돌아갑니다.

리스너의 HAT에서 TLS 활성화

암호화가 필요한 경우 모든 리스너의 TLS를 활성화해야 합니다. 인터넷에 연결한 리스너(즉, 공용 리스너)에서는 TLS를 활성화하지만 내부 시스템의 리스너(즉, 개인 리스너)에는 TLS를 활성화하지 않도록 설정할 수 있습니다. 또는, 모든 리스너에 암호화를 활성화할 수 있습니다.

리스너에서 TLS에 대해 다음 설정을 지정할 수 있습니다.

표 23-2 리스너에 대한 TLS 설정

TLS 설정	의미
1. No	수신 연결에 TLS가 허용되지 않습니다. 리스너에 연결되지 않은 경우 암호화된 SMTP 대화가 필요합니다. 이는 어플라이언스에서 구성하는 모든 리스너에 대한 기본 설정입니다.
2. Preferred	MTA에서 리스너로의 수신 연결에 TLS가 허용됩니다.
3. Required	MTA에서 리스너로의 수신 연결에 TLS가 허용되면 STARTTLS 명령을 받을 때까지 어플라이언스는 NOOP, EHLO 또는 QUIT이 아닌 모든 명령에 오류 메시지로 응답합니다. 이 동작은 RFC 3207에 명시되어 있으며, TLS에서 보안 SMTP에 대한 SMTP 서비스 확장을 정의합니다. "필수" TLS는 발신자가 TLS로 암호화하지 않으려는 이메일을 보내기 전에 어플라이언스가 이를 거절하여 암호화되지 않은 상태로 이메일이 전송되지 않도록 방지합니다.

기본적으로 개인 또는 공용 리스너 모두 TLS 연결을 허용합니다. 리스너의 HAT에서 TLS를 활성화하여 인바운드(수신) 또는 아웃바운드(발송) 이메일에 TLS를 활성화해야 합니다. 또한, 개인 및 공용 리스너의 모든 기본 메일 흐름 정책 설정에는 tls 설정이 "꺼짐"으로 설정되어 있습니다.

리스너를 생성할 때 개별 공용 리스너에 TLS 연결에 대한 특정 인증서를 할당할 수 있습니다. 자세한 내용은 GUI를 통해 리스너를 생성하여 연결 요청 수신 대기, 5-6페이지 항목을 참조하십시오.

관련 주제

- TLS 연결을 위해 GUI를 사용하여 인증서를 공용 또는 개인 리스너에 할당, 23-7페이지
- TLS 연결을 위해 CLI를 사용하여 인증서를 공용 또는 개인 리스너에 할당, 23-7페이지
- 로깅, 23-7페이지
- GUI 예: 리스너의 HAT에 대한 TLS 설정 변경, 23-7페이지
- CLI 예: 리스너의 HAT에 대한 TLS 설정 변경, 23-8페이지

TLS 연결을 위해 GUI를 사용하여 인증서를 공용 또는 개인 리스너에 할당

절차

1단계 Network(네트워크) > Listeners(리스너) 페이지로 이동합니다.

2단계 편집할 리스너의 이름을 클릭합니다.

3단계 Certificate(인증서) 필드에서 인증서를 선택합니다.

4단계 변경사항을 제출하고 커밋합니다.

TLS 연결을 위해 CLI를 사용하여 인증서를 공용 또는 개인 리스너에 할당

절차

1단계 `listenerconfig -> edit` 명령을 사용하여 구성할 리스너를 선택합니다.

2단계 `certificate` 명령을 사용하여 사용 가능한 인증서를 확인합니다.

3단계 프롬프트가 표시되면 리스너에 할당할 인증서를 선택합니다.

4단계 리스너 구성을 마치면 `commit` 명령을 실행하여 변경사항을 활성화합니다.

로깅

TLS가 필요하지만 리스너에서 TLS를 사용할 수 없는 경우 Email Security 어플라이언스는 메일 로그 인스턴스에 기록합니다. 메일 로그는 다음 조건이 만족되면 업데이트됩니다.

- TLS가 리스너에 대해 "필수"로 설정되어 있는 경우.
- Email Security 어플라이언스에서 "Must issue a STARTTLS command first" 명령을 보낸 경우.
- 성공적인 수신자를 수신하지 않고 연결이 종료된 경우.

TLS 연결 실패 이유에 대한 정보가 메일 로그에 포함됩니다.

GUI 예: 리스너의 HAT에 대한 TLS 설정 변경

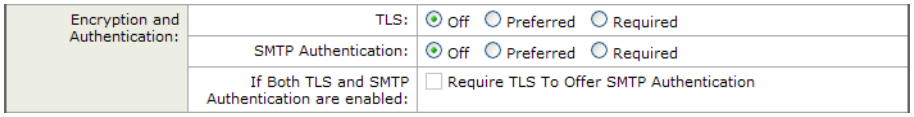
절차

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

2단계 수정하려는 정책이 있는 리스너를 선택한 다음 편집할 정책 이름의 링크를 클릭합니다. 기본 정책 매개 변수도 편집할 수 있습니다.

3단계 "Encryption and Authentication(암호화 및 인증)" 섹션에서 "TLS:" 필드에 대한 리스너의 TLS 수준을 선택합니다.

그림 23-3 리스너의 메일 흐름 정책 매개 변수의 필수 TLS



4단계 변경사항을 제출하고 커밋합니다.

리스너의 메일 흐름 정책은 선택한 TLS 설정으로 업데이트됩니다.

CLI 예: 리스너의 HAT에 대한 TLS 설정 변경

절차

1단계 `listenerconfig -> edit` 명령을 사용하여 구성할 리스너를 선택합니다.

2단계 `hostaccess -> default` 명령을 사용하여 리스너의 기본 HAT 설정을 편집합니다.

3단계 다음 질문이 표시되면 다음 선택 사항 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.
```

이 예는 `certconfig` 명령을 사용하여 리스너와 사용할 수 있는 유효한 인증서가 있는지 확인하도록 요청합니다. 인증서를 생성하지 않은 경우 리스너는 어플라이언스에 사전 설치되어 있는 데모 인증서를 사용합니다. 테스트 목적으로 데모 인증서를 사용하여 TLS를 활성화할 수는 있지만 안전하지 않으며 일반적인 사용에는 사용하지 않는 것이 좋습니다. `listenerconfig -> edit -> certificate` 명령을 사용하여 인증서를 리스너에 할당합니다.

TLS를 구성했으면 CLI의 리스너 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
```

4단계 commit 명령을 실행하여 변경사항을 활성화합니다.

전달 시 TLS 및 인증서 확인 활성화

Destination Controls(대상 제어) 페이지 또는 destconfig 명령을 사용하여 TLS를 특정 도메인에 대한 이메일 전달에 대해 활성화해야 합니다.

TLS 이외에, 도메인의 서버 인증서도 확인해야 합니다. 이러한 도메인 확인은 도메인의 자격 증명을 설정하는 데 사용되는 디지털 인증서를 기반으로 합니다. 확인 절차에서는 다음과 같은 두 가지 사항을 확인해야 합니다.

- SMTP 세션의 발급자 인증서 체인이 신뢰할 수 있는 CA(인증 기관)에서 발급한 인증서로 종료되었는지 여부
- 인증서에 나열된 CN(공용 이름)이 수신 머신의 DNS 이름 또는 메시지의 대상 제어와 일치하는지 여부

  - 또는 -

  메시지의 대상 제어가 RFC 2459에 명시된 대로 인증서의 SAN(Subject Alternative Name, subjectAltName) 확장명에 있는 DNS 이름 중 하나와 일치하는지 여부 일치 항목은 RFC 2818의 3.1절에 명시된 대로 와일드카드를 지원합니다.

신뢰할 수 있는 CA는 ID를 확인하고 공개 키를 배포하는 데 사용하는 디지털 인증서를 발급하는 타사입니다. 이 기관은 인증서가 유효하고 신뢰할 수 있는 ID로 발급되었음을 추가로 보장합니다.

Email Security 어플라이언스에서 봉투 암호화의 대체 방법으로 TLS 연결을 통해 메시지를 도메인으로 보내도록 구성할 수 있습니다. 자세한 내용은 "Cisco 이메일 암호화" 장을 참조하십시오.

어플라이언스에서 모든 발송에 TLS 연결을 사용하도록 인증서를 지정할 수 있습니다. 인증서를 지정하려면 Destination Controls(대상 제어) 페이지에서 **Edit Global Settings(전역 설정 편집)**를 클릭하거나 CLI에서 destconfig -> setup을 사용합니다. 인증서는 도메인 설정이 아닌 전역 설정입니다.

Destination Controls(대상 제어) 페이지 또는 destconfig 명령을 사용하여 도메인을 포함하는 경우 특정 도메인의 TLS에 대해 각기 다른 5가지 다른 설정을 지정할 수 있습니다. 도메인과 교환해야 하는지 여부 또는 도메인과 교환 시 기본으로 TLS 암호화를 설정할지를 지정하는 것 이외에도, 도메인 확인이 필요한지 여부를 지정할 수 있습니다. 설정에 대한 설명은 표 23-3 항목을 참조하십시오.

표 23-3 전달에 대한 TLS 설정

TLS 설정	의미
기본	기본 TLS 설정은 Destination Controls(대상 제어) 페이지 또는 리스너에서 도메인의 MTA로 발송되는 연결에 사용되는 destconfig -> default 하위 명령 사용하여 설정합니다. "Do you wish to apply a specific TLS setting for this domain?(이 도메인에 특정 TLS 설정을 적용하시겠습니까?)"라는 질문에 "No"라고 답한 경우 "기본" 값이 설정됩니다.

표 23-3 전달에 대한 TLS 설정

TLS 설정	의미
1. No	TLS는 인터페이스에서 도메인의 MTA로 발송되는 연결에 대해서는 협상되지 않습니다.
2. Preferred	TLS는 Email Security 어플라이언스 인터페이스에서 도메인의 MTA로 연결되는 경우 협상됩니다. 그러나 TLS 협상에 실패하는 경우(220 응답을 받기 이전에) SMTP 트랜잭션이 "암호화되지 않은 상태로" 계속 진행됩니다. 인증서가 신뢰할 수 있는 인증 기관에서 발급된 경우 확인을 시도하지 않습니다. 220 응답을 받은 후 오류가 발생하면 SMTP 트랜잭션이 일반 텍스트로 돌아가지 않습니다.
3. Required	TLS는 Email Security 어플라이언스 인터페이스에서 도메인의 MTA로 연결되는 경우 협상됩니다. 도메인의 인증서 확인을 시도하지 않습니다. 협상에 실패할 경우 연결을 통해 이메일이 전송되지 않습니다. 수행에 성공할 경우 암호화된 세션을 통해 메일이 전달됩니다.
4. Preferred (Verify)	TLS는 Email Security 어플라이언스에서 도메인의 MTA로 연결되는 경우 협상됩니다. 어플라이언스는 도메인의 인증서 확인을 시도합니다. 다음의 3가지 결과가 가능합니다. • TLS가 협상되며 인증서가 확인됩니다. 암호화된 세션을 통해 메일이 전달됩니다. • TLS가 협상되지만 인증서가 확인되지 않습니다. 암호화된 세션을 통해 메일이 전달됩니다. • TLS 연결이 설정되지 않고 이후에 인증서가 확인되지 않습니다. 이메일 메시지가 일반 텍스트로 전달됩니다.
5. Required (Verify)	TLS는 Email Security 어플라이언스에서 도메인의 MTA로 연결되는 경우 협상됩니다. 도메인의 인증서 확인이 필요합니다. 다음의 3가지 결과가 가능합니다. • TLS 연결이 협상되고 인증서가 확인됩니다. 암호화된 세션을 통해 이메일 메시지가 전달됩니다. • TLS 연결이 협상되지만 인증서가 신뢰할 수 있는 CA에 의해 확인되지 않습니다. 메일이 전달되지 않습니다. • TLS 연결이 협상되지 않습니다. 메일이 전달되지 않습니다.

양호한 인접 테이블에서 주어진 수신자 도메인에 특정 항목이 없거나 특정 항목은 있지만 항목에 대한 특정 TLS 설정이 없는 경우 동작은 Destination Controls(대상 제어) 페이지 또는 `destconfig -> default` 하위 명령("No," "Preferred," "Required," "Preferred (Verify)," or "Required (Verify)")을 사용하여 설정됩니다.

관련 주제

- 필수 TLS 연결이 실패할 경우 경고 보내기, 23-11페이지
- 로깅, 23-11페이지
- CLI 예, 23-12페이지

필수 TLS 연결이 실패할 경우 경고 보내기

TLS 연결이 필요한 도메인에 메시지를 전달할 때 TLS 협상에 실패하는 경우 Email Security 어플라이언스가 경고를 보낼지 여부를 지정할 수 있습니다. 경고 메시지에는 실패한 TLS 협상에 대한 대상 제어의 이름이 포함됩니다. Email Security 어플라이언스는 시스템 경고 유형마다 경고 심각도 수준에 대한 경고를 받도록 설정한 모든 수신자에게 경고 메시지를 보냅니다. GUI의 System Administration(시스템 관리) > Alerts(경고) 페이지 또는 CLI의 `alertconfig` 명령을 통해 경고 수신자를 관리할 수 있습니다.

관련 주제

- GUI를 사용하여 TLS 연결 경고 활성화하기, 23-11페이지
- CLI를 사용하여 TLS 연결 경고 활성화하기, 23-11페이지

GUI를 사용하여 TLS 연결 경고 활성화하기

절차

1단계 메일 정책 Destination Controls(대상 제어) 페이지로 이동합니다.

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

3단계 "Send an alert when a required TLS connection fails(필수 TLS 연결이 실패할 경우 경고 보내기)"에 대해 **Enable(활성화)**을 클릭합니다.

이는 도메인 설정이 아닌 전역 설정입니다. 어플라이언스가 전달을 시도한 메시지에 대한 정보는 Monitor(모니터) > Message Tracking(메시지 추적) 페이지 또는 메일 로그를 사용합니다.

4단계 변경사항을 제출하고 커밋합니다.

CLI를 사용하여 TLS 연결 경고 활성화하기

CLI를 사용하여 TLS 연결 경고를 활성화하려면 `destconfig -> setup` 명령을 사용합니다.

로깅

TLS가 도메인에 필요하지만 사용할 수 없는 경우 Email Security 어플라이언스는 메일 로그 인스턴스에 기록합니다. TLS 연결을 사용할 수 없는 이유에 대한 정보가 포함됩니다. 메일 로그는 다음 조건 중 하나 이상이 만족되면 업데이트됩니다.

- 원격 MTA는 ESMTP를 지원하지 않습니다(예: Email Security 어플라이언스의 EHLO 명령을 이해하지 못함).
- 원격 MTA는 ESMTP를 지원하지만 "STARTTLS"는 EHLO 응답으로 알렸던 확장명 목록에는 없습니다.
- 원격 MTA는 Email Security 어플라이언스가 STARTTLS 명령을 보냈을 때 "STARTTLS" 확장명을 알렸지만 오류를 응답했습니다.

CLI 예

이 예에서 destconfig 명령은 도메인 "partner.com"의 TLS 연결과 암호화된 대화를 요청하기 위해 사용됩니다. 그런 다음 목록이 출력됩니다.

example.com의 인증서는 사전 설치된 데모 인증서 대신 발송 TLS 연결에 사용됩니다. 테스트 목적으로 데모 인증서를 사용하여 TLS를 활성화할 수는 있지만 안전하지 않으며 일반적인 사용에는 사용하지 않는 것이 좋습니다.

```
mail3.example.com> destconfig


There is currently 1 entry configured.


Choose the operation you want to perform:

- SETUP - Change global settings.

- NEW - Create a new entry.

- DELETE - Remove an entry.

- DEFAULT - Change the default.

- LIST - Display a summary list of all entries.

- DETAIL - Display details for one destination or all entries.

- IMPORT - Import tables from a file.

- EXPORT - Export tables to a file.

[]> setup


The "Demo" certificate is currently configured. You may use "Demo", but this will not be
secure.


1. example.com

2. Demo

Please choose the certificate to apply:

[1]> 1


Do you want to send an alert when a required TLS connection fails? [N]>
```

```
There is currently 1 entry configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new

Enter the domain you wish to limit.
[]> partner.com

Do you wish to configure a concurrency limit for partner.com?  [Y]> n

Do you wish to apply a messages-per-connection limit to this domain? [N]> n

Do you wish to apply a recipient limit to this domain?  [N]> n

Do you wish to apply a specific bounce profile to this domain?  [N]> n

Do you wish to apply a specific TLS setting for this domain?  [N]> y

Do you want to use TLS support?
1. No
2. Preferred
```

```
3. Required

4. Preferred (Verify)

5. Required (Verify)

[1]> 3


You have chosen to enable TLS. Please use the 'certconfig' command to ensure that there
is a valid certificate configured.

Do you wish to apply a specific bounce verification address tagging setting for this
domain? [N]> n


Do you wish to apply a specific bounce profile to this domain? [N]> n


There are currently 2 entries configured.


Choose the operation you want to perform:

- SETUP - Change global settings.

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- DEFAULT - Change the default.

- LIST - Display a summary list of all entries.

- DETAIL - Display details for one destination or all entries.

- CLEAR - Remove all entries.

- IMPORT - Import tables from a file.

- EXPORT - Export tables to a file.

[]> list


                    속도                바운스          바운스
Domain              Limiting  TLS       Verification    Profile
==================  ========  ========  ==============  =========
```

```
partner.com  Default   Req      Default       Default
(Default)    On        Off      Off           (Default)

There are currently 2 entries configured.

Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]>
```

인증 기관 목록 관리하기

어플라이언스는 저장된 신뢰할 수 있는 인증 기관을 사용하여 원격 도메인에서 인증서를 확인하여 도메인의 자격 증명을 설정합니다. 어플라이언스가 다음의 신뢰할 수 있는 인증 기관을 사용하도록 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 어플라이언스에 목록을 가져올 수 있습니다.

시스템 목록 또는 사용자 지정한 목록을 사용할 수 있으며 두 가지 목록을 모두 사용하여 원격 도메인에서 인증서를 확인할 수도 있습니다.

GUI의 Network(네트워크) > Certificates(인증서) > Edit Certificate Authorities(인증 기관 편집) 페이지를 사용하거나 CLI의 `certconfig > certauthority` 명령을 사용하여 목록을 관리합니다.

Network(네트워크) > Certificates(인증서) > Edit Certificate Authorities(인증 기관 편집) 페이지에서 다음 작업을 수행할 수 있습니다.

- **인증 기관의 사전 설치된 시스템 목록을 봅니다.** 자세한 내용은 인증 기관의 사전 설치된 목록 보기, 23-16페이지 항목을 참조하십시오.

- **시스템 목록 사용 여부를 선택합니다.** 시스템 목록을 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 시스템 인증 기관 목록 비활성화하기, 23-16페이지 항목을 참조하십시오.
- **사용자 지정 인증 기관 목록 사용 여부를 선택합니다.** 어플라이언스에서 사용자 지정 목록을 사용한 다음 텍스트 파일에서 목록을 가져올 수 있습니다. 자세한 내용은 사용자 지정 인증 기관 목록 가져오기, 23-16페이지 항목을 참조하십시오.
- **인증 기관 목록을 파일로 내보냅니다.** 인증 기관의 시스템 또는 사용자 지정 목록을 텍스트 파일로 내보낼 수 있습니다. 자세한 내용은 인증 기관 목록 내보내기, 23-17페이지 항목을 참조하십시오.

관련 주제

- 인증 기관의 사전 설치된 목록 보기, 23-16페이지
- 시스템 인증 기관 목록 비활성화하기, 23-16페이지
- 사용자 지정 인증 기관 목록 가져오기, 23-16페이지
- 인증 기관 목록 내보내기, 23-17페이지

인증 기관의 사전 설치된 목록 보기

절차

1단계	Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.
2단계	Certificate Authorities(인증 기관) 섹션에서 **Edit Settings(설정 편집)**를 클릭합니다.
3단계	**View System Certificate Authorities(시스템 인증 기관 보기)**를 클릭합니다.

시스템 인증 기관 목록 비활성화하기

사전 설치된 시스템 인증 기관 목록은 어플라이언스에서 제거할 수 없지만 이를 활성화하거나 비활성화할 수 있습니다. 이를 비활성화하여 어플라이언스에서 사용자 지정 목록만 사용하여 원격 호스트로부터의 인증서를 확인할 수 있습니다.

절차

1단계	Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.
2단계	Certificate Authorities(인증 기관) 섹션에서 **Edit Settings(설정 편집)**를 클릭합니다.
3단계	System List(시스템 목록)에 대해 **Disable(비활성화)**을 클릭합니다.
4단계	변경사항을 제출하고 커밋합니다.

사용자 지정 인증 기관 목록 가져오기

신뢰할 수 있는 인증 기관의 사용자 지정 목록을 만들어 어플라이언스에 가져올 수 있습니다. 파일은 PEM 형식이어야 하며 어플라이언스에서 신뢰할 수 있는 인증 기관의 인증서를 포함해야 합니다.

절차

1단계 Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.

2단계 Certificate Authorities(인증 기관) 섹션에서 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 Custom List(사용자 지정 목록)의 **Enable(활성화)**을 클릭합니다.

4단계 로컬 또는 네트워크 머신의 사용자 지정 목록의 전체 경로를 입력합니다.

5단계 변경사항을 제출하고 커밋합니다.

인증 기관 목록 내보내기

시스템에서 신뢰할 수 있는 인증 기관의 하위 집합만 사용하거나 기존 사용자 지정 목록을 편집하려는 경우 목록을 .txt 파일로 내보내고 편집하여 인증 기관을 추가하거나 제거할 수 있습니다. 목록 편집을 마친 후 사용자 지정 목록으로 어플라이언스에 파일을 다시 가져옵니다.

절차

1단계 Network(네트워크) > Certificates(인증서) 페이지로 이동합니다.

2단계 Certificate Authorities(인증 기관) 섹션에서 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 **Export List(목록 내보내기)**를 클릭합니다.

AsyncOS는 Export Certificate Authority List(인증 기관 목록 내보내기) 페이지를 표시합니다.

4단계 내보낼 목록을 선택합니다.

5단계 목록의 파일 이름을 입력합니다.

6단계 **Export(내보내기)**를 클릭합니다.

AsyncOS는 .txt 파일로 목록을 열거나 저장할지를 묻는 대화 상자를 표시합니다.

HTTPS에 대한 인증서 활성화하기

GUI의 Network(네트워크) > IP Interfaces(IP 인터페이스) 페이지를 사용하거나 CLI의 `interfaceconfig` 명령을 사용하여 IP 인터페이스에서 HTTPS 서비스에 대한 인증서를 활성화할 수 있습니다. GUI를 통해 IP 인터페이스를 추가하는 경우 HTTPS 서비스에 사용하려는 인증서를 선택하고 **HTTPS** 확인란을 선택한 다음 포트 번호를 입력합니다.

다음 예에서는 `interfaceconfig` 명령을 사용하여 포트 443(기본 포트)에서 HTTPS 서비스를 활성화하도록 IP 인터페이스 PublicNet을 편집합니다. 해당 인터페이스에 대한 다른 모든 기본값이 수락됩니다. (프롬프트에서 Enter를 입력하면 괄호 안에 표시된 기본값을 수락합니다.)

이 예에서는 어플라이언스에 사전 설치된 데모 인증서 사용을 보여줍니다. 테스트를 목적으로 데모 인증서를 사용하여 HTTPS 서비스를 활성화할 수는 있지만 안전하지 않으며 일반적인 사용에는 사용하지 않는 것이 좋습니다.

참고 GUI에서 시스템 설치 마법사를 사용하여 HTTPS 서비스를 활성화할 수 있습니다. "설정 및 설치" 장의 "기본 라우터(게이트웨이) 정의, DNS 설정 구성 및 보안 웹 액세스 활성화"를 참조하십시오.

이 명령에서 변경 사항이 커밋된 후 사용자는 보안 HTTPS(`https://192.168.2.1`)를 사용하여 GUI(그래픽 사용자 인터페이스)에 접근할 수 있습니다.

```
mail3.example.com> interfaceconfig


Currently configured interfaces:

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)


Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]> edit


Enter the number of the interface you wish to edit.

[]> 3


IP interface name (Ex: "InternalNet"):

[PublicNet]>


Would you like to configure an IPv4 address for this interface (y/n)? [Y]> y


IPv4 Address (Ex: 192.168.1.2):

[192.168.2.1]>
```

```
Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[24]>


Would you like to configure an IPv6 address for this interface (y/n)? [N]>


Ethernet interface:

1. Data 1

2. Data 2

3. Management

[2]>


Hostname:

[mail3.example.com]>


Do you want to enable Telnet on this interface?  [N]>


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?  [Y]>


Which port do you want to use for HTTP?

[80]>


Do you want to enable HTTPS on this interface?  [N]> y


Which port do you want to use for HTTPS?

[443]> 443
```

```
Do you want to enable Spam Quarantine HTTP on this interface? [N]>


Do you want to enable Spam Quarantine HTTPS on this interface? [N]>


The "Demo" certificate is currently configured. You may use "Demo", but this will not be
secure. To assure privacy, run "certconfig" first.


Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the
secure service? [Y]>


Currently configured interfaces:

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)


Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]>
```

24 장

라우팅 및 전달 기능 구성

로컬 도메인의 이메일 라우팅

5 장, "이메일을 수신하도록 게이트웨이 구성"에서는 엔터프라이즈 게이트웨이 구성을 위한 SMTP 연결을 서비스하도록 개인 및 공용 리스너를 사용자 지정했습니다. 이러한 리스너는 특정 연결을 처리(HAT 수정을 통해)하고 특정 도메인에 대한 메일을 수신(공용 리스너의 RAT 수정)하도록 사용자 지정되었습니다.

이 어플라이언스는 Network(네트워크) > SMTP Routes(SMTP 경로) 페이지(또는 `smtproutes` 명령)를 통해 지정된 호스트의 로컬 도메인으로 메일을 라우팅합니다. 이 기능은 sendmail의 `mailertable` 기능과 비슷합니다.

참고 "설정 및 설치" 장에 설명된 대로 GUI의 시스템 설치 마법사(또는 명령줄 인터페이스 `systemsetup` 명령)를 완료하고 변경사항을 커밋하면, 어플라이언스에서 해당 시점에 입력한 각 RAT 항목에 대해 첫 번째 SMTP 경로 항목을 정의한 것입니다.

관련 주제

- SMTP 경로 개요, 24-2페이지
- 기본 SMTP 경로, 24-2페이지
- SMTP 경로 정의, 24-3페이지

SMTP 경로 개요

SMTP 경로를 통해 특정 도메인의 모든 이메일을 다른 메일 교환기(MX) 호스트로 리디렉션할 수 있습니다. 예를 들어 `example.com`에서 `groupware.example.com`으로 매핑할 수 있습니다. 이 매핑을 통해 봉투 수신자 주소에 봉투 수신자 주소에 `@example.com`이 포함된 모든 이메일은 `groupware.example.com`으로 전달됩니다. 시스템은 일반 이메일 전달과 마찬가지로 `groupware.example.com`에서 "MX" 조회를 수행한 후 호스트 에서 "A" 조회를 수행합니다. 이 대체 MX 호스트는 DNS MX 레코드에 나열될 필요가 없으며 심지어 이메일이 리디렉션되는 도메인의 멤버일 필요도 없습니다. AsyncOS 운영 체제에서는 어플라이언스에 대해 최대 40,000개의 SMTP 경로 매핑을 구성할 수 있습니다. (SMTP 경로 제한, 24-3페이지 참조.)

이 기능은 또한 "와일드카드 사용" 호스트도 허용합니다. `.example.com`과 같이 부분 도메인을 지정하는 경우 `example.com`으로 끝나는 모든 도메인은 해당 항목과 일치합니다. 예를 들어 `fred@foo.example.com`과 `wilma@bar.example.com`은 모두 매핑과 일치합니다.

SMTP 경로 테이블에서 호스트를 찾을 수 없으면 DNS를 사용하여 MX 조회를 수행합니다. 이 결과와 SMTP 경로 테이블을 다시 비교하여 확인하지 않습니다. `foo.domain`의 DNS MX 항목이 `bar.domain`인 경우 `foo.domain`으로 전송되는 모든 이메일이 `bar.domain` 호스트로 전달됩니다. 일부 다른 호스트에 대해 `bar.domain`의 매핑을 생성하는 경우 `foo.domain`으로 보낼 이메일에는 영향을 미치지 않습니다.

즉, 재귀 항목 뒤에는 아무것도 오지 않습니다. `b.domain`으로 리디렉션되는 `a.domain`의 항목과 `b.domain`의 이메일을 `a.domain`으로 리디렉션하는 후속 항목이 있는 경우 메일 루프는 생성되지 *않습니다*. 이 경우 `a.domain`으로 보낼 이메일은 `b.domain`에 지정된 MX 호스트로 전달되며, 반대로 `b.domain`으로 보낼 이메일은 `a.domain`에 지정된 MX 호스트로 전달됩니다.

모든 이메일 전달에 대해 SMTP 경로 테이블은 위에서 아래로 참조됩니다. 가장 구체적 항목이 매핑과 일치하면 먼저 참조됩니다. 예를 들어 SMTP 경로 테이블에 `host1.example.com`과 `.example.com`에 대한 매핑이 있는 경우 `host1.example.com` 항목이 더 구체적인 항목이므로 이 항목이 사용됩니다. 해당 항목이 덜 구체적인 `.example.com` 항목 뒤에 있더라도 결과는 동일합니다. 이 밖에 시스템은 봉투 수신자의 도메인에 대해 일반 MX 조회를 수행합니다.

기본 SMTP 경로

특수 키워드 `ALL`을 사용하여 기본 SMTP 경로를 정의할 수 있습니다. 도메인이 SMTP 경로 목록의 이전 매핑과 일치하지 않을 경우 기본적으로 `ALL` 항목에 지정된 MX 호스트로 리디렉션됩니다.

SMTP 경로 항목을 출력하면 기본 SMTP 경로가 `ALL:`로 나열됩니다. 기본 SMTP 경로는 삭제할 수 없으며 입력된 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 구성합니다. 새 경로를 생성하는 경우에는 먼저 영구 경로를 생성할 도메인 또는 부분 도메인을 지정합니다. 그런 다음 대상 호스트를 지정합니다. 대상 호스트는 정규화된 호스트 이름 또는 IP 주소로 입력할 수 있습니다. IP 주소는 인터넷 프로토콜 버전 4(IPv4) 또는 버전 6(IPv6)을 사용할 수 있습니다.

IPv6 주소의 경우 AsyncOS가 지원하는 형식은 다음과 같습니다.

- 2620:101:2004:4202::0-2620:101:2004:4202::ff
- 2620:101:2004:4202::
- 2620:101:2004:4202::23
- 2620:101:2004:4202::/64

또한 특수 대상 호스트 /dev/null을 지정하여 항목과 일치하는 메시지를 삭제할 수 있습니다. (따라서 기본 경로에 대해 /dev/null을 지정하면 어플라이언스에 수신되는 메일이 전달되지 않습니다.)

수신 도메인은 여러 대상 호스트를 가질 수 있으며, MX 레코드와 마찬가지로 각각 우선순위 번호가 할당됩니다. 가장 낮은 번호를 가진 대상 호스트는 수신 도메인의 기본 대상 호스트로 식별됩니다. 나열된 다른 대상 호스트는 백업용으로 사용됩니다.

우선순위가 동일한 대상은 "라운드 로빈" 방식이 적용됩니다. 라운드 로빈 프로세스는 SMTP 연결을 기반으로 하지만 반드시 메시지를 기반으로 하는 것은 아닙니다. 또한 하나 이상의 대상 호스트가 응답하지 않을 경우 메시지는 연결 가능한 호스트 중 하나로 전달됩니다. 구성된 모든 대상 호스트가 응답하지 않을 경우 수신 도메인의 메일은 큐에 저장되고 대상 호스트로의 전달은 나중에 시도됩니다. (MX 레코드를 사용하여 장애 조치되지 않습니다.)

CLI의 smtproutes 명령을 사용하여 경로를 구성하는 경우 호스트 이름 또는 IP 주소 뒤에 /pri=와 0~65535 정수를 차례로 사용하여 우선순위를 할당(0이 최상위 우선순위)하면 각 대상 호스트의 우선순위를 지정할 수 있습니다. 예를 들어 host1.example.com/pri=0의 우선순위는 host2.example.com/pri=10보다 높습니다. 항목이 여러 개인 경우 쉼표로 구분합니다.

SMTP 경로 제한

최대 40,000개의 경로를 정의할 수 있습니다. ALL의 최종 기본 경로는 이 제한과 비교하여 경로가 계산됩니다. 따라서 최대 39,999개의 사용자 지정 경로와 특수 키워드 ALL을 사용하는 하나의 경로를 정의할 수 있습니다.

SMTP 경로 및 DNS

특수 키워드 USEDNS를 사용하여 어플라이언스에서 MX 조회를 수행하여 특정 도메인에 대한 다음 홉을 결정할 수 있습니다. 이는 하위 도메인의 메일을 특정 호스트로 라우팅해야 하는 경우에 유용합니다. 예를 들어 example.com으로 지정된 메일이 회사의 Exchange 서버로 전송되는 경우 경로는 다음 SMTP 경로와 유사할 수 있습니다.

```
example.com exchange.example.com
```

그러나 다양한 하위 도메인(foo.example.com)으로 지정된 메일의 경우 다음과 같은 SMTP 경로를 추가합니다.

```
.example.com USEDNS
```

SMTP 경로 및 경고

어플라이언스에서 System Administration(시스템 관리) > Alerts(경고) 페이지(또는 `alertconfig` 명령)에 지정된 주소로 전송되는 경고는 그러한 대상에 정의된 SMTP 경로를 따릅니다.

SMTP 경로, 메일 전달 및 메시지 분리

수신: 한 메시지의 수신자가 10명이며 수신자가 모두 동일한 Exchange 서버에 있으면 AsyncOS는 TCP 연결 한 개를 열고 개별적인 메시지 10개가 아닌 메시지 하나만 메일 저장소에 제공합니다.

발송: 동작 방식은 비슷하지만 메시지 하나가 서로 다른 도메인 10개에 있는 수신자 10명에게 전달되는 경우 AsyncOS는 MTA 10개에 대한 연결 10개를 열고 각각에 이메일을 하나씩 전달합니다.

분리: 수신 메시지 한 개에 대한 수신자가 10명이며 각 수신자가 별도의 수신 정책 그룹(그룹 10개)에 있는 경우 수신자 10명이 모두 동일한 Exchange 서버에 있더라도 메시지는 분리됩니다. 그러므로 개별 이메일 10개가 단일 TCP 연결을 통해 전달됩니다.

SMTP 경로 및 아웃바운드 SMTP 인증

아웃바운드 SMTP 인증 프로파일이 생성된 경우 SMTP 경로에 적용할 수 있습니다. 이를 통해 어플라이언스가 네트워크 경계에 있는 메일 릴레이 서버 뒤에 배치된 경우 발송 메일에 대한 인증이 가능합니다. 아웃바운드 SMTP 인증에 대한 자세한 내용은 발송 SMTP 인증, 25-39페이지 항목을 참조하십시오.

GUI를 사용하여 아웃바운드 이메일을 전송하도록 SMTP 경로 관리

어플라이언스에서 Network(네트워크) > SMTP Routes(SMTP 경로) 페이지를 사용하여 SMTP 경로를 관리할 수 있습니다. 테이블의 매핑을 추가, 수정 및 삭제할 수 있습니다. SMTP 경로 항목을 내보내거나 가져올 수 있습니다.

관련 주제

- SMTP 경로 추가, 24-4페이지
- SMTP 경로 내보내기, 24-5페이지
- SMTP 경로 가져오기, 24-5페이지

SMTP 경로 추가

절차

1단계 Network(네트워크) > SMTP Routes(SMTP 경로) 페이지에서 **Add Route(경로 추가)**를 클릭합니다.

2단계 수신 도메인을 입력합니다. 호스트 이름, 도메인, IPv4 주소 또는 IPv6 주소를 입력할 수 있습니다.

3단계 대상 호스트를 입력합니다. 호스트 이름, IPv4 주소 또는 IPv6 주소를 입력할 수 있습니다. **Add Row(행 추가)**를 클릭하고 새 행에 다음 대상 호스트를 입력하여 여러 대상 호스트를 추가할 수 있습니다.

참고 대상 호스트에 ":<*포트 번호*>"를 추가하여 포트 번호를 지정할 수 있습니다 (*example.com:25*).

4단계 대상 호스트를 여러 개 추가하는 경우 0~65535 정수를 입력하여 호스트에 우선순위를 할당합니다. 0은 최상위 우선순위입니다. 자세한 내용은 SMTP 경로 정의, 24-3페이지 항목을 참조하십시오.

5단계 변경사항을 제출하고 커밋합니다.

SMTP 경로 내보내기

HAT(Host Access Table) 및 Recipient Access Table(RAT)과 마찬가지로 SMTP 경로 매핑도 파일을 내보내고 가져오는 방식으로 수정할 수 있습니다. SMTP 경로를 내보내려면 다음을 수행합니다.

절차

1단계 SMTP Routes(SMTP 경로) 페이지에서 **Export SMTP Routes(SMTP 경로 내보내기)**를 클릭합니다.

2단계 파일의 이름을 입력하고 **Submit(제출)**을 클릭합니다.

SMTP 경로 가져오기

HAT(Host Access Table) 및 Recipient Access Table(RAT)과 마찬가지로 SMTP 경로 매핑도 파일을 내보내고 가져오는 방식으로 수정할 수 있습니다. SMTP 경로를 가져오려면 다음을 수행합니다.

절차

1단계 SMTP Routes(SMTP 경로) 페이지에서 **Import SMTP Routes(SMTP 경로 가져오기)**를 클릭합니다.

2단계 내보낸 SMTP 경로가 포함된 파일을 선택합니다.

3단계 **Submit(제출)**을 클릭합니다. 가져오기를 수행하면 모든 기존 SMTP 경로가 대체된다는 경고가 표시됩니다. 모든 SMTP 경로를 텍스트 파일로 가져옵니다.

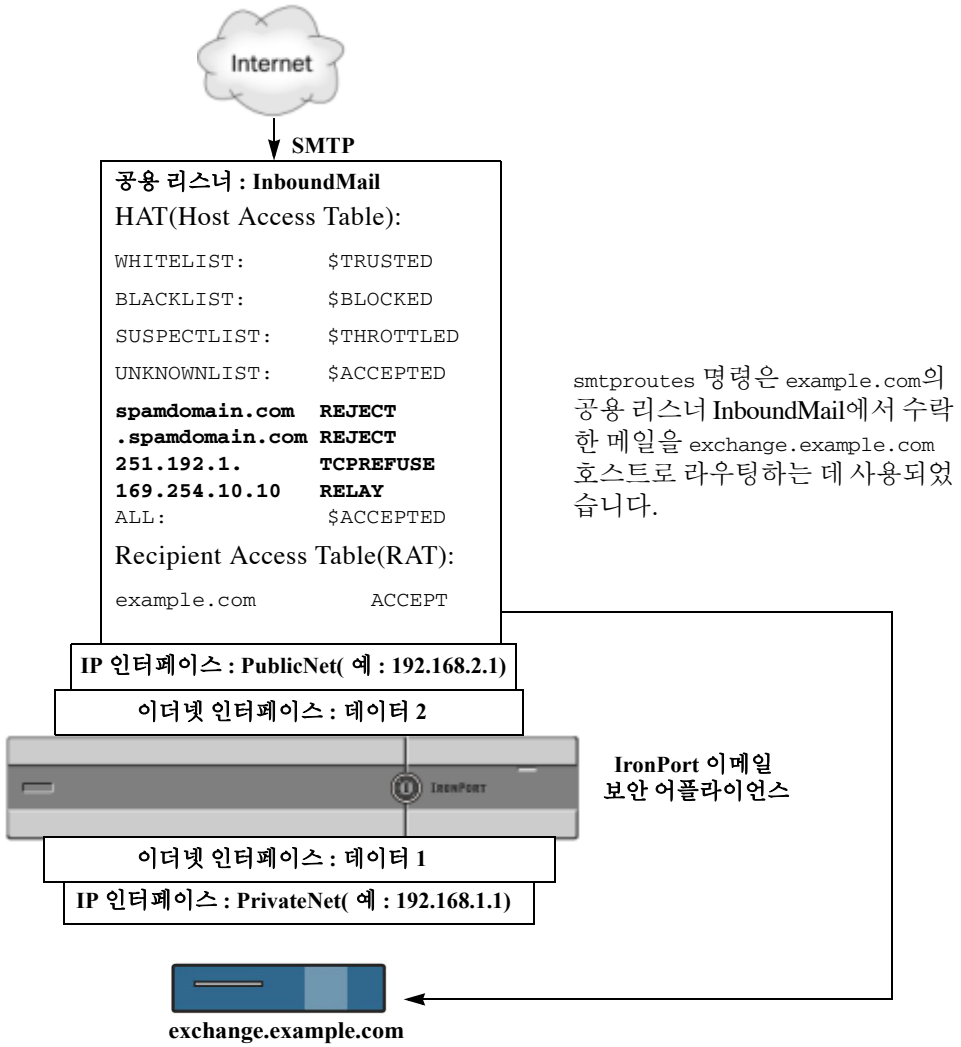
4단계 **Import(가져오기)**를 클릭합니다.

파일에 "주석"을 추가할 수 있습니다. '#' 문자로 시작하는 줄은 주석으로 처리되며 AsyncOS에서 무시됩니다. 예를 들면 다음과 같습니다.

```
# this is a comment, but the next line is not

ALL:
```

이때 이메일 게이트웨이 구성은 다음과 같습니다.

그림 24-1 공용 리스너에 대해 정의된 SMTP 경로



주소 재작성

AsyncOS는 이메일 파이프라인에서 봉투 발신자 및 수신자 주소를 재작성할 수 있는 여러 가지 방법을 제공합니다. 주소 재작성은 예를 들어, 파트너 도메인으로 전송된 메일을 리디렉션하거나 내부 인프라를 숨기기("마스크") 위해 사용할 수 있습니다.

표 24-1에서는 발신자 및 수신자 이메일 주소를 재작성하는 데 사용되는 다양한 기능에 대해 개괄적으로 소개합니다.

표 24-1 주소를 재작성하는 방법

원래 주소	변경 주소	기능	적용 대상
`*@anydomain`	`user@domain`	별칭 테이블(별칭 테이블 생성, 24-7페이지 참조)	• 봉투 수신자만 • 전역으로 적용됨 • 별칭을 이메일 주소 또는 다른 별칭에 매핑
`*@olddomain`	`*@newdomain`	도메인 매핑(도메인 맵 기능, 24-27페이지 참조)	• 봉투 수신자만 • 리스너별로 적용됨
`*@olddomain`	`*@newdomain`	마스커레이드(마스커레이드 구성, 24-15페이지 참조)	• 봉투 발신자 및 To:, From: 및/또는 CC: 헤더 • 리스너별로 적용됨

별칭 테이블 생성

별칭 테이블은 메시지를 하나 이상의 수신자에게 리디렉션하기 위한 메커니즘을 제공합니다. 일부 Unix 시스템에 있는 sendmail 구성의 `/etc/mail/aliases` 기능과 비슷한 방식으로 사용자 이름 및 다른 별칭에 대한 별칭 매핑 테이블을 구성할 수 있습니다.

리스너에서 수락하는 이메일의 봉투 수신자(Envelope To 또는 `RCPT TO`라고도 함)가 별칭 테이블에 정의된 별칭과 일치하는 경우 이메일의 봉투 수신자 주소는 재작성됩니다.

참고 리스너는 별칭 테이블을 확인하고 RAT를 확인한 *후* 메시지 필터를 확인하기 *전* 수신자를 수정합니다. "이메일 파이프라인 이해" 장을 참조하십시오.

참고 별칭 테이블 기능은 사실상 이메일의 봉투 수신자를 재작성합니다. 이는 이메일의 봉투 수신자를 재작성하지 않지만, 대신 이메일을 지정된 도메인으로 다시 라우팅하는 `smtproutes` 명령(바운스된 이메일 전달, 24-34페이지 참조)과는 다릅니다.

관련 주제

- 명령줄에서 별칭 테이블 구성, 24-7페이지
- 별칭 테이블 내보내기 및 가져오기, 24-8페이지
- 별칭 테이블에서 항목 삭제, 24-9페이지

명령줄에서 별칭 테이블 구성

별칭 테이블은 다음과 같이 여러 섹션으로 정의됩니다. 각 섹션 앞에는 섹션과 관련된 도메인 목록에 해당하는 도메인 컨텍스트가 오고 뒤이어 맵 목록이 옵니다.

도메인 컨텍스트는 하나 이상의 도메인 또는 부분 도메인으로 구성된 목록으로, 각 도메인은 쉼표로 구분되고 대괄호('`[`' 및 '`]`')로 묶입니다. 도메인은 RFC 1035, 섹션 2.3.1. "기본 설정 이름 구문"에 정의된 것처럼 문자, 숫자, 하이픈 및 마침표가 포함된 문자열입니다. `.example.com`과 같은 부분 도

메인은 마침표로 시작하는 도메인입니다. 부분 도메인과 일치하는 부분 문자열로 끝나는 모든 도메인은 일치 항목으로 간주됩니다. 예를 들어 도메인 컨텍스트 .example.com은 mars.example.com과 venus.example.com과 일치합니다. 도메인 컨텍스트 아래에는 별칭과 수신자 목록이 차례로 나오는 맵 목록이 있습니다. 맵은 다음과 같이 구성됩니다.

표 24-2 별칭 테이블 구문

LHS(Left-hand Side)	구분 기호	RHS(Right-hand Side)
매칭할 하나 이상의 별칭으로 구성된 목록	콜론 문자(":")	하나 이상의 수신자 주소 또는 별칭으로 구성된 목록

LHS의 별칭에는 다음 형식을 포함할 수 있습니다.

사용자 이름	매칭할 별칭을 지정합니다. 테이블에 지정된 앞에 오는 "domains" 특성이 있어야 합니다. 이 매개변수가 없으면 오류가 발생합니다.
user@domain	매칭할 정확한 이메일 주소를 지정합니다.

LHS의 한 줄에 쉼표로 구분하여 여러 별칭을 입력할 수 있습니다.

RHS의 각 수신자에는 전체 user@domain 이메일 주소 또는 다른 별칭을 사용할 수 있습니다.

별칭 파일에는 묵시적 도메인이 없거나 별칭에 하나 이상의 묵시적 도메인이 포함된 도메인 컨텍스트가 있는 "전역" 별칭(특정 도메인이 아닌 전역으로 적용되는 별칭)이 포함되어 있습니다.

별칭의 "체인"(또는 재귀 항목)을 생성할 수 있지만, 반드시 전체 이메일 주소로 끝나야 합니다.

sendmail 구성 컨텍스트와 호환될 수 있도록 메시지를 삭제하기 위한 특수 대상 /dev/null이 지원됩니다. 메시지가 별칭 테이블을 통해
/dev/null에 매핑된 경우 삭제되는 카운터가 증가합니다. ("CLI를 통한 관리 및 모니터링" 장 참조) 수신자는 수락되지만 큐에 저장되지 않습니다.

관련 주제

- 별칭 테이블 예, 24-9페이지
- aliasconfig 명령 예, 24-11페이지

별칭 테이블 내보내기 및 가져오기

별칭 테이블을 가져오려면 먼저 부록 A, "FTP, SSH, SCP 및 텔넷 액세스" 항목을 참조하여 어플라이언스에 액세스할 수 있는지 확인합니다.

aliasconfig 명령의 export 하위 명령을 사용하여 기존 별칭 테이블을 저장합니다. 파일(사용자가 이름 지정)은 리스너의 /configuration 디렉토리에 기록됩니다. CLI 외부에서 이 파일을 수정한 다음 다시 가져올 수 있습니다. (파일에 잘못된 형식의 항목이 있는 경우 파일을 가져오려고 할 때 오류가 출력됩니다.)

/configuration 디렉토리에 별칭 테이블 파일을 넣고 aliasconfig 명령의 import 하위 명령 을 사용하여 파일을 업로드합니다.

각 줄의 시작 부분에 숫자 기호(#)를 사용하여 테이블의 줄을 주석 처리합니다.

구성 변경사항을 적용하려면 별칭 테이블 파일을 가져온 후에 commit 명령을 실행해야 합니다.

별칭 테이블에서 항목 삭제

명령줄 인터페이스(CLI)를 통해 별칭 테이블의 항목을 삭제하면 먼저 도메인 그룹을 선택하라는 프롬프트가 표시됩니다. "ALL" 항목을 선택하여 모든 도메인에 적용되는 번호가 매겨진 별칭 목록을 확인합니다. 그런 다음 삭제할 별칭 번호를 선택합니다.

별칭 테이블 예

참고 이 예제 테이블의 모든 항목은 주석 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 aliasconfig 명령을 사용하여 별칭 테이블을 구성합니다. 먼저 **example.com**의 도메인 컨텍스트를 지정합니다. 그런 다음 **customercare**의 별칭을 구성하여 customercare@example.com으로 전송되는 모든 이메일이 bob@example.com, frank@example.com 및 sally@example.com으로 리디렉션되도록 합니다. 다음으로 **admin**의 전역 별칭을 구성하여 admin으로 전송되는 이메일이 administrator@example.com으로 리디렉션되도록 합니다. 마지막으로 확인을 위해 별칭 테이블이 출력됩니다.

테이블이 출력될 때 admin의 전역 별칭이 example.com의 첫 번째 도메인 컨텍스트 *앞*에 표시됩니다.

```
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?
```

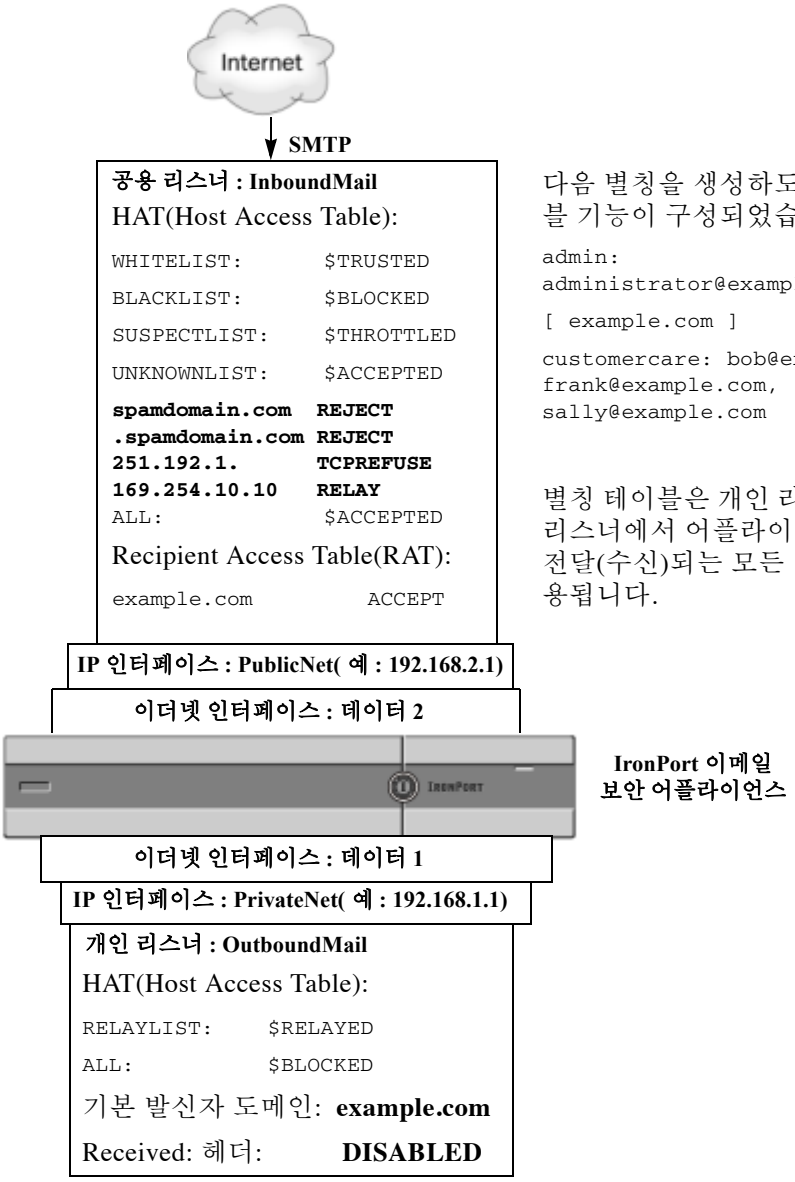
```
1. Globally

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.
[]>
```

이때 이메일 게이트웨이 구성은 다음과 같습니다.

그림 24-2 어플라이언스에 대해 구성된 별칭 테이블



다음 별칭을 생성하도록 별칭 테이블 기능이 구성되었습니다.

```
admin:
administrator@example.com

[ example.com ]

customercare: bob@example.com,
frank@example.com,
sally@example.com
```

별칭 테이블은 개인 리스너와 공용 리스너에서 어플라이언스를 통해 전달(수신)되는 모든 이메일에 적용됩니다.

마스커레이드 구성

마스커레이드는 리스너에서 처리되는 이메일에서 사용자가 구성한 테이블에 따라 봉투 발신자(발신자 또는 MAIL FROM이라고도 함)와 To:, From: 및/또는 CC: 헤더를 재작성하는 기능입니다. 이 기능을 구현하는 일반적인 예로는 단일 사이트에서 여러 도메인을 호스팅할 수 있는 "가상 도메인"이 있습니다. 또 다른 일반적인 구현 방법은 이메일 헤더의 문자열에서 하위 도메인을 "제거"하여 네트워크 인프라를 "숨기기"하는 것입니다. 마스커레이드 기능은 개인 리스너와 공용 리스너에서 모두 사용할 수 있습니다.

참고 마스커레이드 기능은 전체 시스템에 대해 구성되는 별칭 테이블 기능과 달리 리스너별로 구성됩니다.

참고 리스너가 마스커레이드 테이블에서 일치 항목을 확인하고 수신자를 수정할 때 메시지는 작업 큐에서 LDAP 수신자 수락 쿼리 바로 뒤와 LDAP 라우팅 쿼리 바로 앞에 놓입니다. "이메일 파이프라인 이해" 장을 참조하십시오.

마스커레이드 기능은 실제로 봉투 발신자의 주소와 수신된 이메일의 To:, From: 및 CC: 필드를 재작성합니다. 두 가지 중 한 가지 방법을 사용하여 사용자가 생성한 리스너마다 여러 마스커레이드 매개변수를 지정할 수 있습니다.

- 사용자가 생성한 정적 매핑 테이블 사용
- LDAP 쿼리 사용

이 섹션에서는 정적 테이블 메서드에 대해 설명합니다. 테이블 형식은 일부 Unix 시스템에 있는 sendmail 구성의 `/etc/mail/genericstable` 기능과 호환됩니다. LDAP 마스커레이드 쿼리에 대한 자세한 내용은 25 장, "LDAP 쿼리" 항목을 참조하십시오.

관련 주제

- 마스커레이드 및 altsrchost, 24-16페이지

마스커레이드 및 altsrchost

일반적으로 마스커레이드 기능은 봉투 발신자를 재작성하고 메시지에 수행되는 후속 작업은 마스커레이드 주소에서 "트리거"됩니다. 그러나 CLI에서 `altscrchost` 명령을 실행하는 경우 altsrchost 매핑은 수정된 마스커레이드 주소가 아닌 원래 주소에서 트리거됩니다.

자세한 내용은 가상 게이트웨이™ 기술을 사용하여 모든 호스팅된 도메인에 대한 메일 게이트웨이 구성, 24-56페이지 및 검토: 이메일 파이프라인, 24-70페이지 항목을 참조하십시오.

관련 주제

- 정적 마스커레이드 테이블 구성, 24-16페이지
- 개인 리스너에 대한 샘플 마스커레이드 테이블, 24-18페이지
- 마스커레이드 테이블 가져오기, 24-18페이지
- 마스커레이드 예, 24-18페이지

정적 마스커레이드 테이블 구성

`listenerconfig` 명령의 `edit -> masquerade` 하위 명령을 사용하여 정적 마스커레이드 매핑 테이블을 구성합니다. 또는 매핑이 포함된 파일을 가져올 수 있습니다. 마스커레이드 테이블 가져오기, 24-18페이지 항목을 참조하십시오. 하위 명령은 입력 주소, 사용자 이름 및 도메인을 새 주소 및 도메인에 매핑하는 테이블을 생성하고 유지합니다. LDAP 마스커레이드 쿼리에 대한 자세한 내용은 25 장, "LDAP 쿼리" 항목을 참조하십시오.

메시지가 시스템에 삽입되면 테이블이 참조되고 헤더에서 일치하는 항목이 발견되면 메시지가 재작성됩니다.

도메인 마스커레이드 테이블은 다음과 같이 구성됩니다.

표 24-3 마스커레이드 테이블 구문

LHS(Left-hand Side)	구분 기호	RHS(Right-hand Side)
매칭할 하나 이상의 사용자 이름 및/또는 도메인으로 구성된 목록	공백(공백 또는 탭 문자)	재작성된 사용자 이름 및/또는 도메인

다음 표에는 마스커레이드 테이블의 유효한 항목이 나와 있습니다.

LHS(Left-hand Side)	RHS(Right-hand Side)
사용자 이름	username@domain
이 항목은 매칭할 사용자 이름을 지정합니다. LHS의 사용자 이름과 일치하는 수신 이메일 메시지는 RHS에 있는 주소와 일치되며 이 주소로 재작성됩니다. RHS는 전체 주소여야 합니다.	
user@domain	username@domain
이 항목은 매칭할 정확한 주소를 지정합니다. LHS의 전체 주소와 일치하는 수신 메시지는 RHS에 나열된 주소로 재작성됩니다. RHS는 전체 주소여야 합니다.	
@domain	**@domain**
이 항목은 지정된 도메인으로 주소를 지정합니다. LHS의 원래 도메인은 RHS의 도메인으로 대체되며 사용자 이름은 그대로 유지됩니다.	
@.partialdomain	**@domain**
이 항목은 지정된 도메인으로 주소를 지정합니다. LHS의 원래 도메인은 RHS의 도메인으로 대체되며 사용자 이름은 그대로 유지됩니다.	
ALL	**@domain**
ALL 항목은 bare 주소와 일치되며 이 주소는 RHS의 주소로 재작성됩니다. RHS는 "@"가 앞에 오는 도메인이어야 합니다. 이 항목은 테이블에서의 위치와 상관없이 항상 최하위 우선순위를 갖습니다. **참고** 개인 리스너에만 ALL 항목을 사용할 수 있습니다.	

- 마스커레이드 테이블에 나타나는 순서에 따라 규칙이 일치됩니다.
- 기본적으로 수신 시 헤더의 From:, To: 및 CC: 필드에 있는 주소가 일치되고 재작성됩니다. 또한 봉투 발신자와 일치시키고 재작성하도록 옵션을 구성할 수도 있습니다. 봉투 발신자와 config 하위 명령을 사용하여 재작성할 헤더를 활성화 및 비활성화합니다.
- 각 줄의 시작 부분에 숫자 기호(#)를 사용하여 테이블의 줄을 주석 처리할 수 있습니다. # 뒤부터 줄 끝까지 모든 내용은 주석으로 간주하여 무시됩니다.
- 마스커레이드 테이블은 new 하위 명령을 사용하여 생성하든, 아니면 파일에서 가져오든 상관없이 400,000개 항목으로 제한됩니다.

개인 리스너에 대한 샘플 마스커레이드 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
```

마스커레이드 테이블 가져오기

기존의 sendmail `/etc/mail/genericstable` 파일을 가져올 수 있습니다. `genericstable` 파일을 가져오려면 먼저 부록 A, "FTP, SSH, SCP 및 텔넷 액세스"를 항목을 참조하여 어플라이언스에 액세스할 수 있는지 확인합니다.

구성 디렉토리에 `genericstable` 파일을 넣고 `masquerade` 하위 명령의 `import` 하위 명령을 사용하여 파일을 업로드합니다. 다음 순서로 명령을 사용합니다.

`listenerconfig` -> `edit` -> *listener_number* -> `masquerade` -> `import`

또는 `export` 하위 명령을 사용하여 기존 구성을 다운로드할 수 있습니다. 파일(사용자가 이름 지정)은 구성 디렉토리에 기록됩니다. CLI 외부에서 이 파일을 수정한 다음 가져올 수 있습니다.

`import` 하위 명령을 사용할 때 파일에 유효한 항목만 포함되어 있는지 확인합니다. 유효하지 않은 항목(예: RHS가 없는 LHS)이 있는 경우 사용자가 파일을 가져올 때 CLI에서 구문 오류를 보고합니다. 가져오는 동안 구문 오류가 발생하는 경우 전체 파일의 매핑은 가져오지 않습니다.

리스너의 구성 변경사항을 적용하려면 `genericstable` 파일을 가져온 후에 `commit` 명령을 실행해야 합니다.

마스커레이드 예

이 예에서는 `listenerconfig`의 `masquerade` 하위 명령을 사용하여 PrivateNet 인터페이스에서 "OutboundMail"이라는 개인 리스너의 도메인 마스커레이드 테이블을 구성합니다.

먼저 마스커레이드에 LDAP를 사용하는 옵션은 거부됩니다. (LDAP 마스커레이드 쿼리에 대한 자세한 내용은 25 장, "LDAP 쿼리" 항목을 참조하십시오.)

그런 다음 **`@.example.com`**의 부분 도메인 테이블 표기법을 **`@example.com`**에 매핑하여 하위 도메인 `.example.com`에 포함된 모든 머신에서 전송된 이메일이 `example.com`에 매핑되도록 합니다. 다음으로 사용자 이름 **`joe`**를 **`joe@example.com`** 도메인에 매핑합니다. 두 가지 항목을 확인하기 위해 도메인 마스커레이드 테이블이 출력되고 `masquerade.txt`라는 파일로 내보냅니다. `config` 하위 명령을 사용하여 CC: 필드의 주소 재작성을 비활성화하며, 마지막으로 변경사항이 커밋됩니다.

```
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.
```

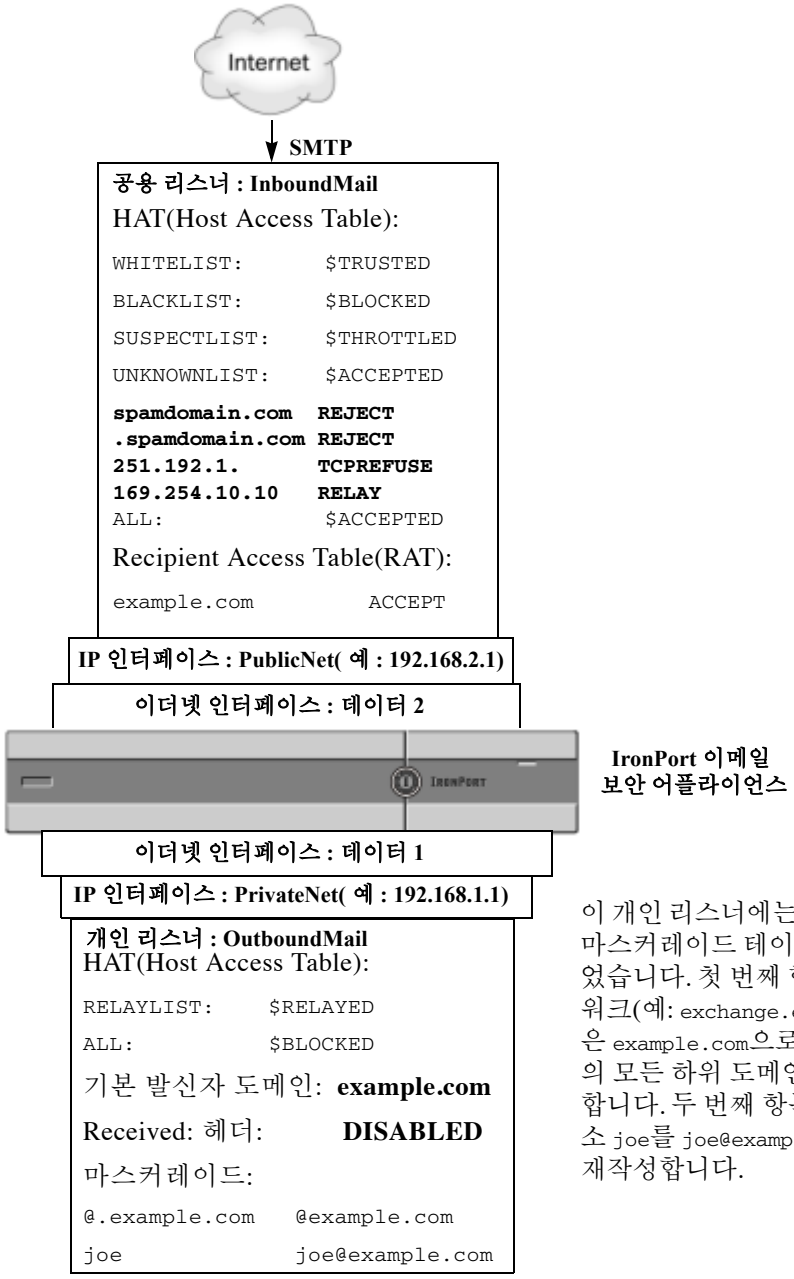
```
- DELETE - Remove an entry.

- 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 구성은 다음과 같습니다.

그림 24-3 개인 리스너에 대해 정의된 마스커레이드



이 개인 리스너에는 2개 항목이 마스커레이드 테이블에 추가되었습니다. 첫 번째 항목은 네트워크(예: `exchange.example.com`은 `example.com`으로 재작성됨)의 모든 하위 도메인을 마스킹합니다. 두 번째 항목은 bare 주소 `joe`를 `joe@example.com`으로 재작성합니다.

도메인 맵 기능

리스너에 대한 "도메인 맵"을 구성할 수 있습니다. 사용자가 구성하는 리스너마다 맵 테이블의 도메인과 일치하는 메시지의 각 수신자의 봉투 수신자를 재작성하는 도메인 맵 테이블을 구성할 수 있습니다. 이 기능은 sendmail "도메인 테이블" 또는 Postfix "가상 테이블" 기능과 비슷합니다. 봉투 수신자만 영향을 받으며 "To:" 헤더는 이 기능을 통해 재작성되지 않습니다.

참고 도메인 맵 기능은 RAT가 평가되기 직전, 그리고 기본 도메인이 평가된 직후에 처리됩니다. "이메일 파이프라인 이해" 장을 참조하십시오.

도메인 맵 기능의 일반적인 구현은 여러 레거시 도메인에 수신 메일을 허용하는 것입니다. 예를 들어 회사가 다른 회사를 인수한 경우 인수한 도메인의 메시지를 수락하고 회사의 현재 도메인의 봉투 수신자를 재작성하도록 어플라이언스에서 도메인 맵을 구성할 수 있습니다.

참고 최대 20,000개의 고유한 개별 도메인 매핑을 구성할 수 있습니다.

표 24-4 도메인 맵 테이블 예제 구문

LS(Left Side)	RS(Right Side)	참고
`username@example.com`	**username2@example.net**	LS의 전체 주소만
`user@.example.com`	**user2@example.net**	
`@example.com`	**user@example.net** *또는* **@example.net**	전체 주소 또는 정규화된 도메인 이름
`@.example.com`	**user@example.net** *또는* **@example.net**	

다음 예에서는 `listenerconfig` 명령의 `domainmap` 하위 명령을 사용하여 공용 리스너 "InboundMail"의 도메인 맵을 생성합니다. `oldcompanyname.com`의 도메인 및 모든 하위 도메인의 메일은 `example.com` 도메인에 매핑됩니다. 그런 다음 확인을 위해 매핑이 출력됩니다. 이 예제를 리스너 RAT에 두 도메인 모두를 배치하는 구성과 비교할 수 있습니다. 도메인 맵 기능은 실제로 `joe@oldcomapanyname.com` 의 봉투 수신자를 `joe@example.com`으로 재작성하지만, `oldcompanyname.com` 도메인을 리스너 RAT에 배치하면 단순히 `joe@oldcompanyname.com`의 메시지를 수락하고 봉투 수신자를 재작성하지 않고도 해당 메시지를 라우팅할 수 있습니다. 이 예제는 별칭 테이블 기능과도 비교할 수 있습니다. 별칭 테이블에서는 *반드시* 명시적 주소를 확인해야 하며 "*모든 username*`@domain`"이
"*동일한 username*`@newdomain`"으로 매핑되도록 구성할 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, 24-33페이지

도메인 맵 테이블 가져오기 및 내보내기

도메인 맵 테이블을 가져오거나 내보내려면 먼저 부록 A, "FTP, SSH, SCP 및 텔넷 액세스"를 항목을 참조하여 어플라이언스에 액세스할 수 있는지 확인합니다.

매핑할 도메인 항목의 텍스트 파일을 생성합니다. 항목끼리는 공백(탭 문자 또는 공백)으로 구분합니다. 각 줄의 시작 부분에 숫자 기호(#)를 사용하여 테이블의 줄을 주석 처리합니다.

구성 디렉토리에 파일을 넣고 `domain` 하위 명령의 `import` 하위 명령을 사용하여 파일을 업로드합니다. 다음 순서로 명령을 사용합니다.

`listenerconfig` -> `edit` -> *inejctor_number* -> `domainmap` -> `import`

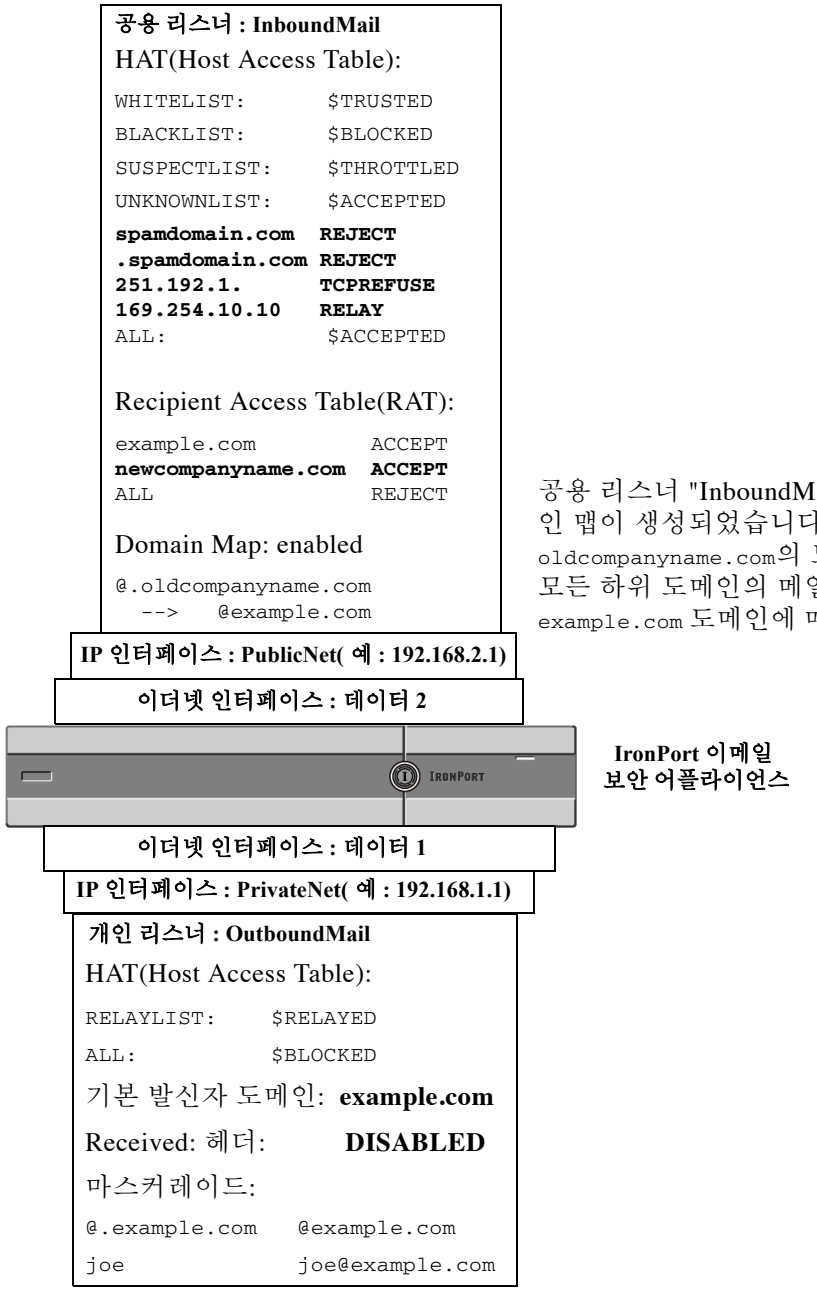
또는 `export` 하위 명령을 사용하여 기존 구성을 다운로드할 수 있습니다. 파일(사용자가 이름 지정)은 구성 디렉토리에 기록됩니다. CLI 외부에서 이 파일을 수정한 다음 가져올 수 있습니다.

`import` 하위 명령을 사용할 때 파일에 유효한 항목만 포함되어 있는지 확인합니다. 유효하지 않은 항목(예: RHS가 없는 LHS)이 있는 경우 사용자가 파일을 가져올 때 CLI에서 구문 오류를 보고합니다. 가져오는 동안 구문 오류가 발생하는 경우 전체 파일의 매핑은 가져오지 않습니다.

리스너의 구성 변경사항을 적용하려면 도메인 맵 테이블 파일을 가져온 후에 `commit` 명령을 실행해야 합니다.

이제 엔터프라이즈 게이트웨이 구성은 다음과 같습니다.

그림 24-4 공용 리스너에 대해 정의된 도메인 맵



바운스된 이메일 전달

이메일 바운스는 모든 이메일 전달에서 불가피하게 발생합니다. 어플라이언스는 여러 가지 구성 가능한 방식으로 바운스된 이메일을 처리할 수 있습니다.

이 섹션에서는 어플라이언스가 발송 바운스(수신 메일 기반)를 생성하는 방식을 제어하는 방법에 대해 설명합니다. 어플라이언스가 수신 바운스(발송 메일 기반)를 제어하는 방식을 제어하려면 바운스 확인을 이용하십시오(바운스 확인, 24-48페이지 참조).

관련 주제

- 전달할 수 없는 이메일 처리, 24-35페이지
- 새 바운스 프로파일 생성, 24-39페이지
- 리스너에 바운스 프로파일 적용, 24-39페이지

전달할 수 없는 이메일 처리

AsyncOS 운영 체제에서는 전달할 수 없는 이메일 또는 "바운스된 메시지"를 다음의 범주로 분류합니다.

"대화식" 바운스: **원격 도메인은 초기 SMTP 대화 중에 메시지를 바운스합니다.**	
소프트 바운스	일시적으로 전달할 수 없는 메시지입니다. 예를 들어 사용자 사서함이 가득 차 있는 경우입니다. 이러한 메시지는 나중에 재시도될 수 있습니다. (예: SMTP 4XX 오류 코드.)
하드 바운스	영구적으로 전송할 수 없는 메시지입니다. 예를 들어 해당 도메인에 더 이상 사용자가 없는 경우입니다. 이러한 메시지는 재시도되지 않습니다. (예: SMTP 5XX 오류 코드.)
"지연된"(또는 "비대화식") 바운스: **원격 도메인은 나중에 바운스하기 위해 전달할 메시지만 수락합니다.**	
소프트 바운스	일시적으로 전달할 수 없는 메시지입니다. 예를 들어 사용자 사서함이 가득 차 있는 경우입니다. 이러한 메시지는 나중에 재시도될 수 있습니다. (예: SMTP 4XX 오류 코드.)
하드 바운스	영구적으로 전송할 수 없는 메시지입니다. 예를 들어 해당 도메인에 더 이상 사용자가 없는 경우입니다. 이러한 메시지는 재시도되지 않습니다. (예: SMTP 5XX 오류 코드.)

GUI에서 Network(네트워크) 메뉴의 Bounce Profiles(바운스 프로파일) 페이지(또는 `bounceconfig` 명령)에서 사용자가 생성한 리스너마다 하드 및 소프트 대화식 바운스를 AsyncOS에서 처리하는 방법을 구성합니다. Network(네트워크) > Listeners(리스너) 페이지(또는 `listenerconfig` 명령)를 통해 바운스 프로파일을 생성한 다음 프로파일을 각 리스너에 적용합니다. 또한 메시지 필터를 사용하여 특정 메시지에 바운스 프로파일을 할당할 수 있습니다. (자세한 내용은 9 장, "메시지 필터를 사용하여 이메일 정책 적용" 참조.)

관련 주제

- 소프트 및 하드 바운스에 대한 참고 사항, 24-36페이지
- 바운스 프로파일 매개변수, 24-36페이지
- 하드 바운스 및 status 명령, 24-37페이지
- 대화식 바운스 및 SMTP 경로 메시지 필터 작업, 24-37페이지
- 바운스 프로파일 예, 24-38페이지
- 전달 상태 알림 형식, 24-38페이지
- 지연 경고 메시지, 24-38페이지
- 지연 경고 메시지 및 하드 바운스, 24-39페이지

소프트 및 하드 바운스에 대한 참고 사항

- 대화식 소프트 바운스의 경우, 소프트 바운스 이벤트는 수신자 전송이 일시적으로 실패할 때마다 항상 정의됩니다. 단일 수신자를 사용하는 경우에도 여러 소프트 바운스 이벤트가 발생할 수 있습니다. Bounce Profiles(바운스 프로파일) 페이지 또는 `bounceconfig` 명령을 사용하여 각 소프트 바운스 이벤트에 대한 매개변수를 구성합니다. (바운스 프로파일 매개변수, 24-36페이지 참조.)
- 기본적으로 시스템은 바운스 메시지를 생성하고 이를 각 하드 바운스 수신자의 원래 발신자에게 전송합니다. (메시지는 메시지 봉투의 봉투 발신자 주소에 정의된 주소로 전송됩니다. Envelope From은 일반적으로 봉투 발신자라고도 합니다.) 이 기능을 비활성화하고 대신 로그 파일을 참조하여 하드 바운스에 대한 정보를 확인할 수 있습니다. ("로깅" 장 참조.)
- 소프트 바운스는 큐에서의 최대 시간이 경과하거나 최대 재시도 횟수를 초과(두 가지 중 먼저 도달한 경우)할 경우 하드 바운스가 됩니다.

바운스 프로파일 매개변수

바운스 프로파일을 구성하는 경우 다음 매개변수는 메시지별로 대화식 바운스가 처리되는 방식을 제어합니다.

표 24-5 바운스 프로파일 매개변수

최대 재시도 횟수	시스템이 소프트 바운스 메시지를 하드 바운스 메시지로 처리하기 전에 수신자 호스트에 다시 연결하여 재전달하려고 시도하는 횟수입니다. 기본 재시도 횟수는 100회입니다.
큐에서의 최대 시간(초)	시스템이 소프트 바운스 메시지를 하드 바운스 메시지로 처리하기 전에 수신자 호스트에 연결하여 재전달하려고 시도하는 시간입니다. 기본값은 259,200초(72시간)입니다.
메시지를 재시도할 때까지 대기하는 초기 시간(초)	시스템이 소프트 바운스 메시지 재전달을 처음 시도하기까지 대기하는 시간입니다. 기본값은 60초입니다. 소프트 바운스가 시도되는 주기를 줄이려면 초기 재시도 시간을 큰 값으로 설정합니다. 반대로, 주기를 늘리려면 작은 값으로 설정합니다.
메시지를 재시도할 때까지 대기하는 최대 시간(초)	시스템이 소프트 바운스 메시지 재전달을 시도하기까지 대기해야 할 최대 시간입니다. 기본값은 3,600초(1시간)입니다. 이는 다음 시도까지 걸리는 시간을 의미하지 않습니다. 그보다 재시도 횟수를 제어하는 데 사용되는 다른 매개변수입니다. 초기 재시도 간격은 최대 재시도 간격에 따른 최대값으로 제한됩니다. 계산된 재시도 간격이 최대 재시도 간격을 초과하는 경우 최대 재시도 간격이 대신 사용됩니다.
하드 바운스 메시지 생성 형식	하드 바운스 메시지 생성을 활성화할지 또는 비활성화할지를 지정합니다. 활성화된 경우 메시지 형식을 선택할 수 있습니다. 기본적으로 생성된 바운스 메시지에는 DSN 형식(RFC 1894)이 사용됩니다. 바운스 메시지에 사용할 사용자 지정 알림 템플릿을 선택할 수 있습니다. 자세한 내용은 "텍스트 리소스" 장을 참조하십시오. 바운스 응답의 DSN 상태 필드를 구문 분석할지 여부를 선택할 수 있습니다. "Yes(예)"를 선택하는 경우 AsyncOS는 바운스 응답에서 DSN 상태 코드(RFC 3436)를 검색하고 전달 상태 알림의 Status(상태) 필드에 있는 코드를 사용합니다.
지연 경고 메시지 전송	지연 경고를 보낼지 여부를 지정합니다. 활성화된 경우, 메시지 간 최소 간격과 더불어 최대 전송 재시도 횟수를 지정합니다. 경고 메시지에 사용할 사용자 지정 알림 템플릿을 선택할 수 있습니다. 자세한 내용은 "텍스트 리소스" 장을 참조하십시오.

표 24-5 바운스 프로파일 매개변수 (계속)

바운스 수신자 지정	메시지를 봉투 발신자 주소 기본값이 아닌 대체 주소로 바운스할 수 있습니다.
바운스 및 지연 메시지에 DomainKeys 서명 사용	바운스 및 지연 메시지 서명에 사용할 DomainKeys 프로파일을 선택할 수 있습니다. DomainKeys에 대한 자세한 내용은 DomainKeys 및 DKIM 인증, 20-1 페이지 항목을 참조하십시오.
전역 설정	
Bounce Profiles(바운스 프로파일) 페이지의 Edit Global Settings(전역 설정 편집) 링크를 통해, 또는 CLI의 `bounceconfig` 명령을 사용하여 기본 바운스 프로파일을 편집하여 이러한 설정을 구성합니다.	
연결할 수 없는 호스트에 재시도할 때까지 대기하는 초기 시간(초)	시스템이 연결할 수 없는 호스트에 재시도할 때까지 대기해야 하는 시간입니다. 기본값은 60초입니다.
연결할 수 없는 호스트에 대한 최대 허용 재시도 간격	시스템이 연결할 수 없는 호스트에 재시도하기까지 대기해야 할 최대 시간입니다. 기본값은 3,600초(1시간)입니다. 호스트 중단으로 인해 초기 전달에 실패할 경우 최소 재시도 시간(초)으로 시작되고, 중단된 호스트에 다음 시도가 이루어질 때마다 시간이 증가하여 최대 시간(초)까지 늘어나게 됩니다.

하드 바운스 및 status 명령

하드 바운스 메시지 생성이 활성화된 경우 어플라이언스가 전달을 위한 하드 바운스 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 참조하십시오. 하드 바운스 메시지 생성을 비활성화한 경우 수신자가 하드 바운스되더라도 카운터는 증가하지 않습니다.

참고 메시지 봉투의 봉투 발신자 주소는 메시지 헤더의 From:과는 다릅니다. 봉투 발신자 주소와 다른 이메일 주소로 하드 바운스 메시지를 보내도록 AsyncOS를 구성할 수 있습니다.

대화식 바운스 및 SMTP 경로 메시지 필터 작업

SMTP 경로 및 메시지 필터 작업에 대한 매핑은 어플라이언스에서 대화식 바운스의 결과로 생성된 SMTP 바운스 메시지 라우팅에는 적용되지 않습니다. 어플라이언스가 대화식 바운스 메시지를 수신하면 원본 메시지의 봉투 발신자에게 다시 전달할 SMTP 바운스 메시지를 생성합니다. 이 경우 어플라이언스는 사실상 메시지를 생성하므로 릴레이를 위해 삽입된 메시지에 적용되는 SMTP 경로는 적용되지 않습니다.

바운스 프로파일 예

서로 다른 바운스 프로파일 매개변수를 사용하는 2가지 예는 다음과 같습니다.

표 24-6 예 1: 바운스 프로파일 매개변수

매개변수	값
최대 재시도 횟수	2
큐에서의 최대 시간(초)	259,200초(72시간)
재시도할 때까지 대기하는 초기 시간(초)	60초
재시도할 때까지 대기하는 최대 시간(초)	60초

예 1에서 첫 번째 수신자 전송 시도는 메시지가 어플라이언스에 삽입된 직후인 t=0에 이루어집니다. 기본 초기 재시도 시간이 60초인 경우 첫 번째 재시도는 약 1분 후인 t=60에 이루어집니다. 재시도 간격이 계산되어 최대 재시도 간격으로 60초가 사용됩니다. 그런 다음 약 t=120에 두 번째 재시도가 이루어집니다. 재시도가 이루어진 직후에 시스템은 최대 재시도 횟수가 2회에 도달했으므로 해당 수신자에 대한 하드 바운스 메시지를 생성합니다.

표 24-7 예 2: 바운스 프로파일 매개변수

매개변수	값
최대 재시도 횟수	100
큐에서의 최대 시간(초)	100초
재시도할 때까지 대기하는 초기 시간(초)	60초
재시도할 때까지 대기하는 최대 시간(초)	120초

예 2에서 첫 번째 전달 시도는 t=0에, 첫 번째 재시도는 t=60에 발생합니다. 시스템은 다음 전달 시도(t=120에 발생하도록 예약됨) 직전에 메시지를 하드 바운스하는데, 이는 큐에서의 최대 시간이 100초를 초과했기 때문입니다.

전달 상태 알림 형식

시스템에서 생성된 바운스 메시지는 기본적으로 하드 바운스와 소프트 바운스 모두 전달 상태 알림(DSN) 형식을 사용합니다. DSN은 RFC 1894(`http://www.faqs.org/rfcs/rfc1894.html` 참조)에서 정의된 형식입니다. RFC 1894는 "메시지 전송 에이전트(MTA) 또는 전자 메일 게이트웨이가 하나 이상의 수신자에게 메시지를 전달하려고 시도한 결과를 보고하기 위해 사용하는 MIME 콘텐츠 유형을 정의"합니다. 기본적으로 전달 상태 알림에는 전달 상태에 대한 설명과 원본 메시지(메시지 크기가 10k 미만인 경우)가 포함됩니다. 메시지 크기가 10k를 초과하는 경우 전달 상태 알림에는 메시지 헤더만 포함됩니다. 메시지 헤더가 10k를 초과하는 경우 전달 상태 알림에서 헤더를 잘라냅니다. 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 생성된 큐의 시간 메시지(지연 알림 메시지)에서도 DSN 형식을 사용합니다. Network(네트워크) 메뉴의 Bounce Profiles(바운스 프로파일) 페이지(또는 `bounceconfig` 명령)에서 기존 항목을 편집하거나 새 바운스 프로파일을 생성하고 다음과 같은 기본값을 변경하는 방식으로 기본 매개변수를 변경할 수 있습니다.

- 지연 경고 메시지 전송 간 최소 시간 간격.

- 수신자마다 전송할 최대 지연 경고 메시지 수.

지연 경고 메시지 및 하드 바운스

"Maximum Time in Queue(큐에서의 최대 시간)" 설정과 "Send Delay Warning Messages(지연 경고 메시지 보내기)"의 최소 시간 간격을 모두 매우 작게 설정한 경우 동일한 메시지에 대해 지연 경고와 하드 바운스를 *동시에* 수신할 수 있습니다. Cisco 시스템에서 지연 경고 메시지 전송을 활성화하는 경우 이러한 설정의 기본값을 최소로 지정하는 것이 좋습니다.

또한 어플라이언스에서 발생한 지연 경고 메시지 및 바운스 메시지는 처리 중에 최대 15분간 지연될 수 있습니다.

새 바운스 프로파일 생성

다음 예에서는 Bounce Profiles(바운스 프로파일) 페이지에서 `bouncepr1`이라는 바운스 프로파일을 생성합니다. 이 프로파일에서 모든 하드 바운스 메시지는 대체 주소 `bounce-mailbox@example.com`으로 전송됩니다. 지연 경고 메시지가 활성화됩니다. 수신자당 경고 메시지 하나가 전송되며 경고 메시지 간 시간 간격으로 기본값인 4시간(14,400초)이 설정됩니다.

관련 주제

- 기본 바운스 프로파일 편집, 24-39페이지
- Minimalist 바운스 프로파일 예, 24-39페이지

기본 바운스 프로파일 편집

바운스 프로파일 목록에서 해당 이름을 클릭하여 바운스 프로파일을 편집할 수 있습니다. 기본 바운스 프로파일을 편집할 수도 있습니다. 이 예에서는 `연결할 수 없는 호스트에 재시도할 때까지 대기해야 하는 최대 시간(초)`을 3,600초(1시간)에서 10,800초(3시간)로 늘리도록 기본 프로파일을 편집합니다.

Minimalist 바운스 프로파일 예

다음 예에서는 `minimalist`라는 바운스 프로파일이 생성됩니다. 이 프로파일에서 바운스되는 메시지는 재시도되지 않으며(최대 재시도 횟수 0) 재시도할 때까지 대기하는 최대 시간이 지정됩니다. 하드 바운스 메시지가 비활성화되며 소프트 바운스 경고는 전송되지 않습니다.

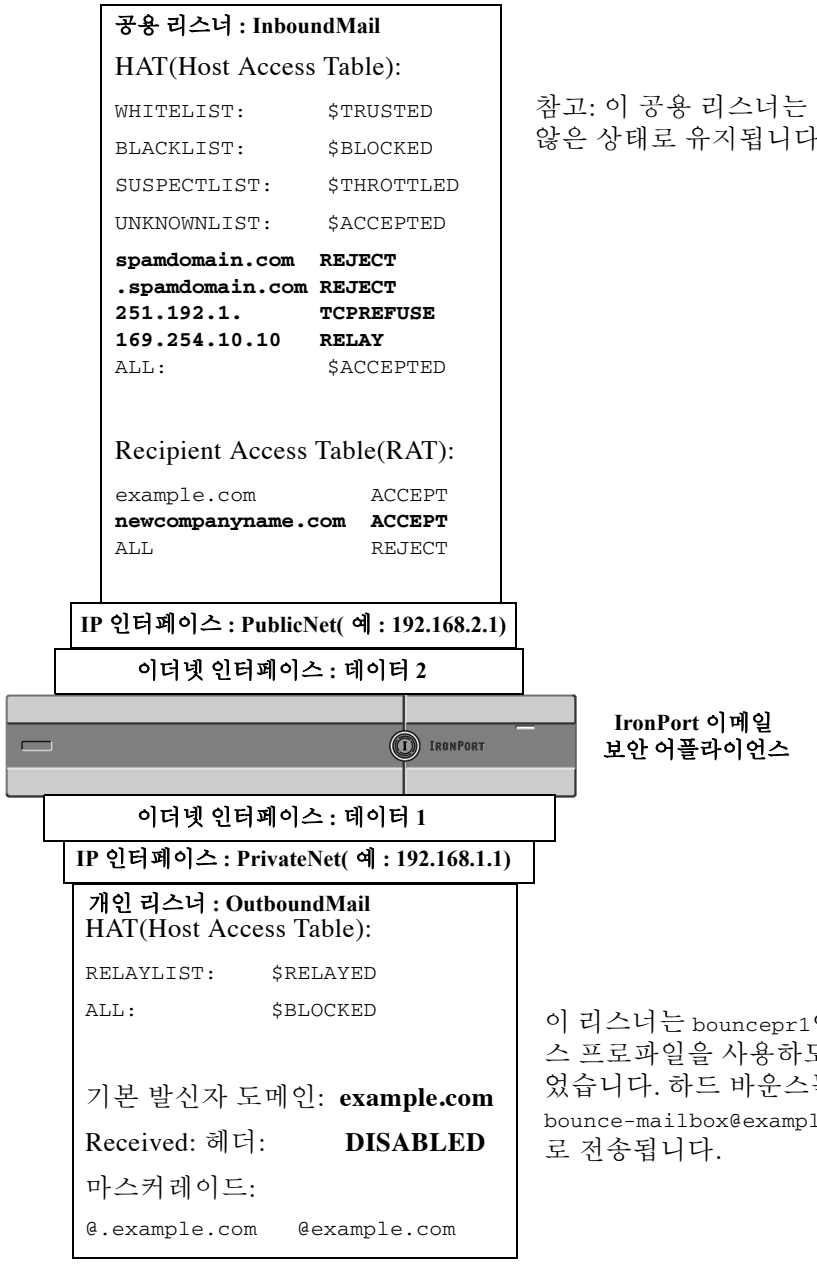
리스너에 바운스 프로파일 적용

바운스 프로파일을 생성한 경우 Network(네트워크) > Listeners(리스너) 페이지 또는 `listenerconfig` 명령을 사용하여 해당 프로파일을 리스너에 적용할 수 있습니다.

다음 예에서는 OutgoingMail 리스너에 `bouncepr1` 프로파일이 적용됩니다.

이때 이메일 게이트웨이 구성은 다음과 같습니다.

그림 24-5 개인 리스너에 바운스 프로파일 적용



참고: 이 공용 리스너는 변경되지 않은 상태로 유지됩니다.

IronPort 이메일 보안 어플라이언스

이 리스너는 `bouncepr1`이라는 바운스 프로파일을 사용하도록 수정되었습니다. 하드 바운스는 `bounce-mailbox@example.com` 주소로 전송됩니다.

대상 제어을 사용하여 이메일 전달 제어

제어되지 않는 대용량 이메일을 전달하는 경우 수신자 도메인에 메시지를 가득 채울 수 있습니다. AsyncOS에서는 어플라이언스가 여는 연결 수 또는 어플라이언스에서 각 대상 제어에 보내는 메시지 수를 정의하여 메시지 전달을 완벽히 제어할 수 있습니다.

대상 제어 기능(GUI의 Mail Policies(메일 정책) > Destination Controls(대상 제어) 또는 CLI의 `destconfig` 명령)을 사용하여 다음 사항을 제어할 수 있습니다.

- 속도 제한, 24-41페이지
- TLS, 24-41페이지

- 바운스 확인, 24-41페이지
- 바운스 프로파일, 24-41페이지

속도 제한

- 동시 연결 수: 어플라이언스가 여는 원격 호스트에 대한 동시 연결 수입니다.
- 연결당 최대 메시지 수: 어플라이언스가 새 연결을 시작하기까지 어플라이언스가 대상 제어에 보내는 메시지 수입니다.
- 수신자 수: 어플라이언스가 지정된 기간에 지정된 원격 호스트로 보내는 수신자 수입니다.
- 제한: 대상별로 또는 MGA 호스트 이름별로 지정한 제한을 적용하는 방법입니다.

TLS

- 원격 호스트에 대한 TLS 연결을 수락할지, 허용할지, 아니면 필수로 할지 선택(TLS 제어, 24-44페이지 참조).
- TLS 연결이 필요한 원격 호스트에 메시지를 전달할 때 TLS 협상에 실패할 경우 경고를 보낼지 여부. 이는 도메인 설정이 아닌 전역 설정입니다.
- 원격 호스트에 대한 모든 아웃바운드 TLS 연결에 사용할 TLS 인증서를 할당합니다.

바운스 확인

- 바운스 확인을 통해 주소 태깅을 수행할지 여부(바운스 확인, 24-48페이지 참조).

바운스 프로파일

- 어플라이언스에서 지정된 원격 호스트에 사용해야 하는 바운스 프로파일(기본 바운스 프로파일은 Network(네트워크) > Bounce Profiles(바운스 프로파일) 페이지에서 설정됨).

지정되지 않은 도메인에 대한 기본 설정도 제어할 수 있습니다.

관련 주제

- 메일 전달에 사용되는 인터페이스 결정, 24-41페이지
- 기본 전달 제한, 24-42페이지
- 대상 제어 작업, 24-42페이지

메일 전달에 사용되는 인터페이스 결정

`deliveryconfig` 명령이나 메시지 필터(`alt-src-host`) 또는 가상 게이트웨이를 사용하여 출력 인터페이스를 지정한 경우를 제외하고 출력 인터페이스는 AsyncOS 라우팅 테이블에서 선택됩니다. 기본적으로 "auto"를 선택하면 AsyncOS에서 자동으로 결정됩니다.

세부적으로 로컬 주소는 인터페이스 넷마스크를 인터페이스 IP 주소에 적용하여 식별됩니다. 이러한 두 항목은 모두 Network(네트워크) > Interfaces(인터페이스) 페이지, 또는 `interfaceconfig` 명령(또는 시스템 설치 중에)으로 설정됩니다. 주소 공간이 겹치는 경우 가장 구체적인 넷마스크가 사용됩니다. 대상이 로컬인 경우 패킷은 해당 로컬 인터페이스를 통해 전송됩니다.

대상이 로컬이 아닌 경우 패킷은 기본 라우터(Network(네트워크) > Routing(라우팅) 페이지, 또는 `setgateway` 명령을 사용하여 설정)로 전송됩니다. 기본 라우터의 IP 주소는 로컬입니다. 출력 인터페이스는 로컬 주소의 출력 인터페이스를 선택하는 규칙에 따라 결정됩니다. 예를 들어 AsyncOS는 기본 라우터의 IP 주소가 포함된 IP 주소 및 넷마스크 중 가장 구체적인 항목을 선택합니다.

라우팅 테이블은 Network(네트워크) > Routing(라우팅) 페이지(또는 `routeconfig` 명령을 사용하여)에서 구성합니다. 라우팅 테이블에서 일치하는 항목이 기본 경로보다 우선합니다. 더 구체적인 경로가 덜 구체적인 경로보다 우선합니다.

기본 전달 제한

각 아웃바운드 대상 제어에는 고유한 아웃바운드 큐가 있습니다. 따라서 각 도메인에는 대상 제어 테이블에 지정된 별도의 동시 연결 제한이 있습니다. 또한 대상 제어 테이블에 특별히 나열되지 않은 고유한 도메인은 테이블에 설정된 다른 "기본" 제한을 사용합니다.

대상 제어 작업

GUI의 Mail Policies(메일 정책) > Destination Controls(대상 제어) 페이지 또는 CLI의 `destconfig` 명령을 사용하여 대상 제어 항목을 생성, 편집 및 삭제할 수 있습니다.

관련 주제

- 인터넷 프로토콜 주소 버전 제어, 24-42페이지
- 도메인에 대한 연결, 메시지 및 수신자 수 제어, 24-42페이지
- TLS 제어, 24-44페이지
- 바운스 확인 태깅 제어, 24-44페이지
- 바운스 제어, 24-44페이지
- 새 대상 제어 항목 추가, 24-44페이지
- 대상 제어 구성 가져오기 및 내보내기, 24-45페이지
- 대상 제어 및 CLI, 24-48페이지

인터넷 프로토콜 주소 버전 제어

도메인 연결에 사용할 인터넷 프로토콜 주소 버전을 구성할 수 있습니다. Email Security 어플라이언스는 인터넷 프로토콜 버전 4(IPv4)와 인터넷 프로토콜 버전 6(IPv6)을 모두 사용합니다. 어플라이언스에서 프로토콜 버전 하나 또는 두 가지 모두를 사용하도록 리스너를 구성할 수 있습니다.

IPv4 또는 IPv6에 대해 "Required(필수)" 설정이 지정된 경우 어플라이언스는 지정된 버전의 주소를 사용하여 도메인에 대한 연결을 협상합니다. 도메인이 해당 IP 주소 버전을 사용하지 않으면 이메일이 전송되지 않습니다. IPv4 또는 IPv6에 대해 "Preferred(기본 설정)" 설정이 지정된 경우 어플라이언스는 먼저 지정된 버전의 주소를 사용하여 도메인에 대한 연결을 협상하며 첫 번째 시도로 연결할 수 없는 경우 다른 버전 주소로 폴백합니다.

도메인에 대한 연결, 메시지 및 수신자 수 제어

원격 호스트 또는 고유의 내부 그룹웨어 서버가 어플라이언스에서 전달되는 이메일로 가득 차지 않도록 어플라이언스에서 이메일을 전달하는 방식을 제한할 수 있습니다.

도메인마다 지정된 기간 동안 시스템에서 초과할 수 없는 최대 연결, 아웃바운드 메시지 및 수신자 수를 할당할 수 있습니다. 이 "양호한 인접" 테이블은 대상 제어 기능(Mail Policies(메일 정책) > Destination Controls(대상 제어) 페이지 또는 `destconfig` 명령(이전의 `setgoodtable` 명령))을 통해 정의됩니다. 다음 구문을 사용하여 도메인 이름을 지정할 수 있습니다.

```
domain.com
```

또는

```
.domain.com
```

이 구문을 사용하면 AsyncOS에서 각각의 전체 하위 도메인 주소를 개별적으로 입력하지 않고 하위 도메인(예: sample.server.domain.com)의 대상 제어을 지정할 수 있습니다.

연결, 메시지 및 수신자에 대해 정의하는 제한이 각 가상 게이트웨이 주소에 적용되는지, 아니면 전체 시스템에 적용되는지 설정합니다. (가상 게이트웨이 주소 제한에서는 IP 인터페이스당 동시 연결 수를 제어합니다. 시스템 전체 제한에서는 어플라이언스에 허용되는 총 연결 수를 제어합니다.)

또한 정의하는 제한이 지정된 도메인의 각 MX 레코드에 적용되는지, 아니면 전체 도메인에 적용되는지 설정합니다. (다수의 도메인에는 이메일을 수락하기 위한 여러 MX 레코드가 정의되어 있습니다.)

참고 현재 시스템 기본값은 도메인당 연결 500개 및 연결당 메시지 50개입니다.

이러한 값은 표 24-8에 설명되어 있습니다.

표 24-8 대상 제어 테이블의 값

필드	설명
동시 연결	어플라이언스가 지정된 호스트를 대상으로 설정하는 최대 아웃바운드 연결 수입니다. (도메인은 내부 그룹웨어 호스트를 포함할 수 있습니다.)
연결당 최대 메시지 수	새 연결을 시작하기 전까지 어플라이언스에서 지정된 호스트로의 단일 아웃바운드 연결에 허용되는 최대 메시지 수입니다.
수신자	지정된 시간 내에 허용되는 최대 수신자 수입니다. "None(없음)"은 지정된 도메인에 대한 수신자 제한이 없음을 의미합니다. 어플라이언스에서 수신자 수를 계산하는 최소 시간(1~60분)입니다. "0"을 지정하면 기능이 비활성화됩니다. **참고** 수신자 제한을 변경하는 경우 AsyncOS는 이미 큐에 있는 모든 메시지에 대해 카운터를 재설정합니다. 어플라이언스는 새 수신자 제한을 바탕으로 메시지를 전달합니다.
제한 적용	제한을 전체 도메인에 적용할지, 아니면 해당 도메인에 지정된 각 메일 교환기 IP 주소에 적용할지 지정합니다. (다수의 도메인에는 여러 MX 레코드가 있습니다.) 이 설정은 연결, 메시지 및 수신자 제한에 적용됩니다. 제한을 시스템 전체에 적용할지, 아니면 각 가상 게이트웨이 주소에 적용할지 지정합니다. **참고** IP 주소 그룹을 구성했지만 가상 게이트웨이는 구성하지 않은 경우 가상 게이트웨이별로 제한을 적용하도록 구성하지 않습니다. 이 설정은 가상 게이트웨이를 사용하도록 구성된 시스템에만 사용됩니다. 가상 게이트웨이 구성에 대한 자세한 내용은 가상 게이트웨이™ 기술을 사용하여 모든 호스팅된 도메인에 대한 메일 게이트웨이 구성, 24-56페이지 항목을 참조하십시오.

참고 가상 게이트웨이 주소별로 제한을 적용하는 경우에도 가능한 게이트웨이 수로 나누어 가상 게이트웨이 제한을 전체 시스템 제한으로 설정하여 시스템 전체 제한을 효율적으로 구현할 수 있습니다. 예를 들어 가상 게이트웨이 주소 4개가 구성되어 있으며 `yahoo.com` 도메인에 대한 동시 연결 수를 100개 이하로 제한하여 열고자 하는 경우 가상 게이트웨이 동시 연결 제한을 25개로 설정합니다.

참고 `delivernow` 명령을 모든 도메인에 적용하는 경우 `destconfig` 명령을 사용하여 추적된 모든 카운터가 재설정됩니다.

TLS 제어

도메인별로 TLS(전송 계층 보안)를 구성할 수 있습니다. "Required(필수)" 설정이 지정된 경우 해당 도메인의 어플라이언스 리스너에서 MTA로의 TLS 연결이 협상됩니다. 협상이 실패할 경우 연결을 통해 이메일이 전송되지 않게 됩니다. 자세한 내용은 전달 시 TLS 및 인증서 확인 활성화, 23-9 페이지 항목을 참조하십시오.

TLS 연결이 필요한 도메인에 메시지를 전달할 때 TLS 협상에 실패하는 경우 어플라이언스가 경고를 보낼지 여부를 지정할 수 있습니다. 경고 메시지에는 실패한 TLS 협상에 대한 대상 제어의 이름이 포함됩니다. 어플라이언스는 시스템 경고 유형마다 경고 심각도 수준에 대한 경고를 받도록 설정한 모든 수신자에게 경고 메시지를 보냅니다. GUI의 System Administration(시스템 관리) > Alerts(경고) 페이지 또는 CLI의 `alertconfig` 명령을 통해 경고 수신자를 관리할 수 있습니다.

TLS 연결 경고를 활성화하려면 Destination Controls(대상 제어) 페이지의 **Edit Global Settings(전역 설정 편집)**를 클릭하거나 `destconfig -> setup` 하위 명령을 사용합니다. 이는 도메인 설정이 아닌 전역 설정입니다. 어플라이언스가 전달을 시도한 메시지에 대한 정보는 Monitor(모니터) > Message Tracking(메시지 추적) 페이지 또는 메일 로그를 사용합니다.

모든 발송 TLS 연결에 사용할 인증서를 지정해야 합니다. Destination Controls(대상 제어) 페이지의 **Edit Global Settings(전역 설정 편집)** 또는 `destconfig -> setup` 하위 명령을 사용하여 인증서를 지정합니다. 인증서 취득에 대한 자세한 내용은 인증서 얻기, 23-2페이지 항목을 참조하십시오.

경고에 대한 자세한 내용은 "시스템 관리" 장을 참조하십시오.

바운스 확인 태깅 제어

전송된 메일에 바운스 확인에 대한 태그를 지정할지 여부를 지정할 수 있습니다. 이는 기본값은 물론 특정 대상에 대해 지정할 수 있습니다. Cisco에서는 기본값에 대해 바운스 확인을 사용하고 특정 제외 항목에 대해 새 대상을 생성하는 것이 좋습니다. 자세한 내용은 바운스 확인, 24-48페이지 항목을 참조하십시오.

바운스 제어

원격 호스트로 전달되는 수신자 및 연결 수를 제어하는 것 외에도, 해당 도메인에 사용할 바운스 프로파일도 지정할 수 있습니다. 바운스 프로파일이 지정된 경우 `destconfig` 명령의 다섯 번째 열에 표시됩니다. 바운스 프로파일을 지정하지 않을 경우 기본 바운스 프로파일이 사용됩니다. 자세한 내용은 새 바운스 프로파일 생성, 24-39페이지 항목을 참조하십시오.

새 대상 제어 항목 추가

절차

1단계 **Add Destination(대상 추가)**을 클릭합니다.

2단계 항목을 구성합니다.

3단계 변경사항을 제출하고 커밋합니다.

대상 제어 구성 가져오기 및 내보내기

여러 도메인을 관리하는 경우 단일 구성 파일을 생성하여 모든 도메인에 대한 대상 제어 항목을 정의하고 어플라이언스로 가져올 수 있습니다. 구성 파일의 형식은 Windows INI 구성 파일과 유사합니다. 도메인 매개변수는 도메인 이름과 같은 섹션에서 그룹화됩니다. 예를 들어 섹션 이름 `[example.com]`을 사용하여 example.com 도메인의 매개변수를 그룹화할 수 있습니다. 정의되지 않은 모든 매개변수는 기본 대상 제어 항목에서 상속됩니다. `[DEFAULT]` 섹션을 구성 파일에 포함하여 기본 대상 제어 항목의 매개변수를 정의할 수 있습니다.

구성 파일에 `[DEFAULT]` 섹션이 포함되어 있지 않은 경우 구성 파일을 가져오면 기본 항목을 제외한 어플라이언스의 모든 대상 제어 항목을 덮어씁니다. 다른 모든 기존 대상 제어 항목이 삭제됩니다.

구성 파일에서 도메인의 다음 매개변수를 정의할 수 있습니다. `[DEFAULT]` 섹션의 경우 `bounce_profile` 매개변수를 제외한 모든 매개변수가 필요합니다.

표 24-9 대상 제어 구성 파일 매개변수

매개 변수 이름	설명
ip_sort_pref	도메인에 대한 인터넷 프로토콜 버전을 지정합니다. 다음 값 중 하나를 입력합니다. • "IPv6 Preferred"의 경우 `PREFER_V6` • "IPv6 Required"의 경우 `PREFER_V6` • "IPv4 Preferred"의 경우 `PREFER_V4` • "IPv4 Required"의 경우 `REQUIRE_v4`
`max_host_concurrency`	어플라이언스가 지정된 호스트를 대상으로 설정하는 최대 아웃바운드 연결 수입니다. 도메인에 이 매개변수를 정의하는 경우 `limit_type` 및 `limit_apply` 매개변수도 정의해야 합니다.
`max_messages_per_connection`	새 연결을 시작하기 전까지 어플라이언스에서 지정된 호스트로의 단일 아웃바운드 연결에 허용되는 최대 메시지 수입니다.
`recipient_minutes`	어플라이언스에서 수신자 수를 계산하는 시간(1~60분)입니다. 수신자 제한이 적용되지 않은 경우 정의되지 않은 상태로 유지합니다.
`recipient_limit`	지정된 시간 내에 허용되는 최대 수신자 수입니다. 수신자 제한이 적용되지 않은 경우 정의되지 않은 상태로 유지합니다. 도메인에 이 매개변수를 정의하는 경우 `recipient_minutes`, `limit_type` 및 `limit_apply` 매개변수도 정의해야 합니다.
`limit_type`	제한을 전체 도메인에 적용할지, 아니면 해당 도메인에 지정된 각 메일 교환기 IP 주소에 적용할지 지정합니다. 다음 값 중 하나를 입력합니다. • 도메인: `0`(또는 `host`) • 메일 교환기 IP 주소: `1`(또는 `MXIP`)

표 24-9 대상 제어 구성 파일 매개변수

매개 변수 이름	설명
limit_apply	제한을 시스템 전체에 적용할지, 아니면 각 가상 게이트웨이 주소에 적용할지 지정합니다. 다음 값 중 하나를 입력합니다. • 시스템 전체: 0(또는 system) • 가상 게이트웨이: 1(또는 VG)
bounce_validation	바운스 검증 주소 태깅을 설정할지 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, 23-9페이지 항목을 참조하십시오. 다음 값 중 하나를 입력합니다. • 0(또는 off) • 1(또는 on) - "Preferred" • "Required": 2(또는 required) • "Preferred (Verify)": 3(또는 on_verify) • "Required (Verify)": 4(또는 require_verify) 문자열은 대소문자를 구분하지 않습니다.
bounce_profile	사용할 바운스 프로파일의 이름입니다. 이는 [DEFAULT] 대상 제어 항목에 사용할 수 없습니다.
send_tls_req_alert	필수 TLS 연결이 실패할 경우 경고를 보낼지 여부를 지정합니다. 다음 값 중 하나를 입력합니다. • 0(또는 off) • 1(또는 on) 이는 전역 설정이며 [DEFAULT] 대상 제어 항목에서만 사용할 수 있습니다.
인증서	발송 TLS 연결에 사용되는 인증서입니다. 이는 전역 설정이며 [DEFAULT] 대상 제어 항목에서만 사용할 수 있습니다. **참고** 인증서를 지정하지 않을 경우 AsyncOS는 데모 인증서를 할당하지만 데모 인증서를 사용하면 안전하지 않으므로 일반적인 사용에는 사용하지 않는 것이 좋습니다.

다음 예에서는 기본 대상 제어 항목과 함께 example1.com 및 example2.com 도메인의 구성 파일을 보여 줍니다.

```
[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 예에서 example1.com 및 example2.com에 대해 생성되는 결과는 다음과 같습니다.

```
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
```

Destination Controls(대상 제어) 페이지의 **Import Table(테이블 가져오기)** 버튼을 클릭하거나 `destconfig -> import` 명령을 사용하여 구성 파일을 가져옵니다. Destination Controls(대상 제어) 페이지의 **Export Table(테이블 내보내기)** 버튼을 클릭하거나 `destconfig -> export` 명령을 사용하여 대상 제어 항목을 INI 파일로 내보낼 수도 있습니다. AsyncOS는 내보낸 INI 파일에 `[Default]` 대상 제어 항목을 포함합니다.

대상 제어 및 CLI

CLI의 `destconfig` 명령을 사용하여 대상 제어 항목을 구성할 수 있습니다. 이 명령은 *Cisco AsyncOS CLI 참조 설명서*에 설명되어 있습니다.

바운스 확인

"바운스" 메시지는 수신 MTA가 원본 이메일의 봉투 발신자를 새 봉투 수신자로 사용하여 전송하는 새 메시지입니다. 이 바운스는 원본 메시지를 전달할 수 없는 경우(일반적으로 존재하지 않는 수신자 주소로 인해) 봉투 발신자(MAIL FROM: < >)가 비워진 상태로 봉투 수신자(대개)로 다시 전송됩니다.

스패머가 미스디렉션 바운스 공격을 통해 이메일 인프라를 공격하는 사례가 점점 더 증가하고 있습니다. 이러한 공격은 알 수 없는 정상적인 메일 서버에서 전송하는 막대한 양의 바운스 메시지로 구성됩니다. 기본적으로 스패머가 사용하는 프로세스는 오픈 릴레이 및 "좀비" 네트워크를 통해 다양한 도메인에 있는 잠재적으로 유효하지 않은 여러 주소(봉투 수신자)로 이메일을 전송하는 것입니다. 이러한 메시지에서는 스팸이 정상적인 도메인에서 온 것처럼 보이도록 봉투 발신자가 위조("Joe job"이라고 함)됩니다.

그러면 올바르지 않은 봉투 수신자를 가진 수신 이메일마다 수신 메일 서버는 새 이메일(바운스 메시지)을 생성하고 해당 도메인(봉투 발신자 주소가 위조된 도메인)의 봉투 발신자와 함께 전송합니다. 결과적으로 이 대상 제어는 막대한 양의 "미스디렉션" 바운스(잠재적으로 수백만 개의 메시지)를 수신합니다. 이러한 종류의 분산 서비스 거부 공격은 이메일 인프라 성능을 저하시키고 대상에서 정상적인 이메일을 주고받을 수 없게 만들 수 있습니다.

이와 같이 미스디렉션 바운스 공격을 차단하기 위해 AsyncOS에서는 바운스 확인이 가능합니다. 바운스 확인이 활성화된 경우, 어플라이언스를 통해 전송된 메시지의 봉투 발신자 주소에 태그를 지정합니다. 그리고 어플라이언스에 수신되는 모든 바운스 메시지의 봉투 수신자에 이 태그가 있는지 확인합니다. 정상적인 바운스(이 태그를 포함해야 함)에는 태그가 지정되지 않은 상태로 전달됩니다. 태그가 포함되지 않은 바운스 메시지는 별도로 처리할 수 있습니다.

바운스 확인을 사용하여 발송 메일을 기반으로 수신 바운스 메시지를 관리할 수 있습니다. 어플라이언스가 발송 바운스를 생성하는 방법(수신 메일 기반)을 제어하려면 바운스된 이메일 전달, 24-34페이지 항목을 참조하십시오.

관련 주제

- 개요: 태깅 및 바운스 확인, 24-49페이지
- 태그가 지정되지 않은 정상적인 바운스 메시지 수락, 24-50페이지
- 바운스 확인을 사용하여 바운스된 메시지 스톰 방지, 24-51페이지

개요: 태깅 및 바운스 확인

바운스 확인을 활성화한 상태에서 이메일을 전송하는 경우 어플라이언스가 메시지의 봉투 발신자 주소를 재작성합니다. 예를 들어 MAIL FROM: `joe@example.com`은 MAIL FROM: `prvs=joe=123ABCDEFG@example.com`이 됩니다. 이 예에서 `123...` 문자열은 어플라이언스에서 전송되면서 봉투 발신자에 추가되는 "바운스 확인 태그"입니다. 이 태그는 바운스 확인 설정에 정의된 키를 사용하여 생성됩니다(키 지정에 대한 자세한 내용은 바운스 확인 주소 태깅 키, 24-50페이지 참조). 이 메시지가 바운스되는 경우 바운스의 봉투 수신자 주소에는 일반적으로 이 바운스 확인 태그가 포함됩니다.

시스템 전체에서 바운스 확인 태깅을 기본값으로 사용하거나 사용하지 않도록 설정할 수 있습니다. 특정 도메인에 대해서도 바운스 확인 태깅을 사용하거나 사용하지 않도록 설정할 수 있습니다. 대부분의 경우 사용자는 바운스 확인 태깅을 기본값으로 사용하며 대상 제어 테이블(대상 제어 작업, 24-42페이지 참조)에서 제외할 특정 도메인을 목록으로 작성합니다.

메시지에 이미 태그가 지정된 주소가 포함되어 있으면 AsyncOS는 다른 태그를 추가하지 않습니다(바운스 메시지를 DMZ 내 어플라이언스로 전달하는 어플라이언스의 경우).

관련 주제

- 수신 바운스 메시지 처리, 24-50페이지
- 바운스 확인 주소 태깅 키, 24-50페이지

수신 바운스 메시지 처리

유효한 태그를 포함하는 바운스는 전달됩니다. 태그가 제거되고 봉투 수신자가 복원됩니다. 이 작업은 이메일 파이프라인의 도메인 맵 단계 직후에 수행됩니다. 어플라이언스에서 태그가 지정되지 않은 바운스 또는 유효하지 않은 태그가 지정된 바운스를 처리하는 방법(해당 바운스를 거부하거나 사용자 지정 헤더 추가)을 정의할 수 있습니다. 자세한 내용은 바운스 확인 설정 구성, 24-52 페이지 항목을 참조하십시오.

바운스 확인 태그가 없거나 태그 생성에 사용된 키가 변경된 경우 또는 메시지가 7일을 경과한 경우 해당 메시지는 바운스 확인에 정의된 설정에 따라 처리됩니다.

예를 들어 다음 메일 로그에서는 어플라이언스에서 거부된 바운스된 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 비바운스 메일을 고유한 내부 메일 서버(Exchange 등)로 전달하는 경우 해당 내부 도메인의 바운스 확인 태깅을 비활성화해야 합니다.

AsyncOS는 바운스를 null Mail From 주소(<>)를 사용하는 메일로 간주합니다. 태그가 지정된 봉투 수신자를 포함할 가능성이 있는 비바운스 메시지의 경우 AsyncOS는 더욱 관대한 정책을 적용합니다. 이 경우 AsyncOS는 7일 키 만료를 무시하고 이전 키와 일치하는 항목 검색을 시도합니다.

바운스 확인 주소 태깅 키

태깅 키는 바운스 확인 태그를 생성할 때 어플라이언스가 사용하는 텍스트 문자열입니다. 원칙적으로 도메인을 빠져나가는 모든 메일에 일관되게 태그가 지정되도록 모든 어플라이언스에서 동일한 키를 사용하는 것이 좋습니다. 따라서 한 어플라이언스에서 발송 메시지의 봉투 발신자에 태그를 지정하면 다른 어플라이언스에서 바운스를 수신하는 경우에도 수신 바운스가 확인되고 전달됩니다.

태그에는 7일간의 유예 기간이 있습니다. 예를 들어 7일 기간 이내에 태깅 키를 여러 번 변경하도록 선택할 수 있습니다. 이 경우 어플라이언스는 7일에 도달하지 않은 모든 이전 키를 사용하여 태그가 지정된 메시지를 확인합니다.

태그가 지정되지 않은 정상적인 바운스 메시지 수락

AsyncOS에서는 태그가 지정되지 않은 바운스가 유효한지 여부를 파악하기 위해 바운스 확인과 관련된 HAT 설정이 가능합니다. 기본 설정은 "No(아니요)"이며, 태그가 지정되지 않은 바운스는 유효하지 않은 것으로 간주됩니다. 어플라이언스는 Mail Policies(메일 정책) > Bounce Verification(바운스 확인) 페이지에서 선택한 작업에 따라 메시지를 거부하거나 사용자 지정 헤더를 적용합니다. "Yes(예)"를 선택할 경우 어플라이언스는 태그가 지정되지 않은 바운스를 유효한 것으로 판단하여 이를 수락합니다. 이는 다음과 같은 경우에 사용될 수 있습니다.

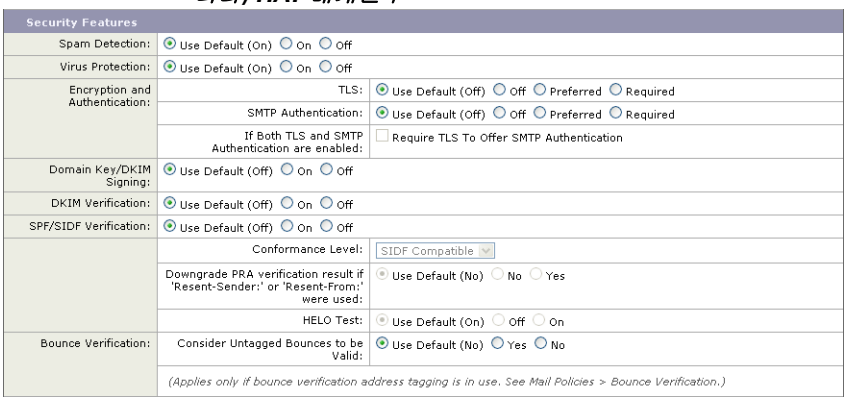
사용자가 메일 목록으로 이메일을 전송하려고 합니다. 그러나 메일 목록은 고정된 봉투 발신자에서 오는 메시지만 수락합니다. 이 경우 사용자가 보낸 태그가 지정된 메시지는 수락되지 않습니다(태그가 정기적으로 변경되므로).

절차

1단계 사용자가 대상 제어 테이블에 메일을 전송하거나 태깅을 비활성화하려는 도메인을 추가합니다. 이 시점에서 사용자는 문제없이 메일을 보낼 수 있습니다.

2단계 그러나 해당 도메인에서의 바운스 수신을 적절히 지원하려면(태그가 지정되지 않으므로) 해당 도메인에 대한 발신자 그룹을 생성하고 "Accept(허용)" 메일 흐름 정책에서 Consider Untagged Bounces to be Valid(다음과 같은 태그 없는 바운스가 유효할 수 있습니다) 매개변수를 활성화합니다.

그림 24-6 Consider Untagged Bounces to be Valid(다음과 같은 태그 없는 바운스가 유효할 수 있습니다) HAT 매개변수



바운스 확인을 사용하여 바운스된 메시지 스톰 방지

절차

1단계 태깅 키를 입력합니다. 자세한 내용은 바운스 확인 주소 태깅 키 구성, 24-52페이지 항목을 참조하십시오.

2단계 바운스 확인 설정을 편집합니다. 자세한 내용은 바운스 확인 설정 구성, 24-52페이지 항목을 참조하십시오.

3단계 Destination Controls(대상 제어)를 통해 바운스 확인을 활성화합니다. 자세한 내용은 대상 제어 작업, 24-42페이지 항목을 참조하십시오.

그림 24-7 IronPort 바운스 확인 페이지

관련 주제

- 바운스 확인 주소 태깅 키 구성, 24-52페이지
- 바운스 확인 설정 구성, 24-52페이지
- CLI를 사용하여 바운스 확인 구성, 24-53페이지
- 바운스 확인 및 클러스터 구성, 24-53페이지

바운스 확인 주소 태깅 키 구성

바운스 확인 주소 태깅 키 목록에는 현재 키와 함께 과거에 사용한 적이 있지만 제거되지 않은 키가 표시됩니다. 새 키를 추가하려면 다음을 수행합니다.

절차

1단계 Mail Policies(메일 정책) > Bounce Verification(바운스 확인) 페이지에서 **New Key(새 키)**를 클릭합니다.

2단계 텍스트 문자열을 입력하고 **Submit(제출)**을 클릭합니다.

3단계 변경사항을 **커밋**합니다.

관련 주제

- 키 제거, 24-52페이지

키 제거

풀다운 메뉴에서 제거 규칙을 선택하고 **Purge(제거)**를 클릭하여 이전 주소 태깅 키를 제거할 수 있습니다.

바운스 확인 설정 구성

바운스 확인 설정을 통해 유효하지 않은 바운스를 수신하는 경우 수행할 작업을 결정합니다.

절차

1단계 Mail Policies(메일 정책) > Bounce Verification(바운스 확인)을 선택합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 유효하지 않은 바운스를 거부할지, 아니면 메시지에 사용자 지정 헤더를 추가할지 선택합니다. 헤더를 추가하려면 헤더 이름 및 값을 입력합니다.

4단계 선택적으로 스마트 예외 사항을 활성화합니다. 이 설정을 사용하면 수신 메일 메시지와 내부 메일 서버에서 생성된 바운스 메시지를 바운스 확인 처리에서 자동으로 제외할 수 있습니다(수신 및 발송 메일에 모두 단일 리스너를 사용하는 경우에도).

5단계 변경사항을 제출하고 커밋합니다.

CLI를 사용하여 바운스 확인 구성

CLI의 `bvconfig` 및 `destconfig` 명령을 사용하여 바운스 확인을 구성할 수 있습니다. 이러한 명령은 *CiscoAsyncOS CLI 참조 설명서*에 설명되어 있습니다.

바운스 확인 및 클러스터 구성

두 어플라이언스가 모두 동일한 "바운스 키"를 사용한다면 클러스터 구성에서 바운스 확인이 동작합니다. 동일한 키를 사용하는 경우 한 시스템에서는 정상적인 바운스를 허용해야 합니다. 수정된 헤더 태그/키는 각 어플라이언스에 국한되지 않습니다.

이메일 전달 매개변수 설정

`deliveryconfig` 명령은 어플라이언스에서 이메일을 전달할 때 사용할 매개변수를 설정합니다.

어플라이언스는 여러 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 섹션에 설명된 여러 기능 또는 명령은 라우팅 우선순위에 영향을 주거나 받지 않습니다. 자세한 내용은 "네트워크 및 IP 주소 할당" 부록을 참조하십시오.

관련 주제

- 기본 전달 IP 인터페이스, 24-54페이지
- 가능한 전달 기능, 24-54페이지
- 기본 최대 동시 연결 수, 24-54페이지
- deliveryconfig 예, 24-54페이지

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 않는 경우 AsyncOS는 수신자 호스트와 통신할 때 SMTP HELO 명령에서 기본 전송 인터페이스와 연결된 호스트 이름을 사용합니다. IP 인터페이스를 구성하려면 interfaceconfig 명령을 사용합니다.

이메일 전달 인터페이스의 자동 선택을 사용하기 위한 규칙입니다.

- 원격 이메일 서버가 구성된 인터페이스 중 하나와 동일한 서브넷에 있는 경우 트래픽은 일치하는 인터페이스에서 발송됩니다.
- auto-select로 설정된 경우 routeconfig를 사용하여 구성한 정적 경로가 적용됩니다.
- 그렇지 않으면, 기본 게이트웨이와 동일한 서브넷에 있는 인터페이스가 사용됩니다. 모든 IP 주소에 대상에 해당하는 경로가 있는 경우 시스템은 사용 가능한 인터페이스 중 가장 효율적인 인터페이스를 사용합니다.

가능한 전달 기능

주의 이 기능을 활성화하는 경우 메시지 전달을 신뢰할 수 없어 메시지가 손실될 수 있습니다. 또한 어플라이언스는 RFC 5321을 준수하지 않게 됩니다. 자세한 내용은 http://tools.ietf.org/html/rfc5321#section-6.1을 참조하십시오.

가능한 전달 기능을 활성화한 경우 AsyncOS는 메시지 본문이 전달된 후에 시간이 초과된 모든 메시지를 처리합니다. 단, 수신자 호스트가 메시지의 수신을 "가능한 전달"로 확인 응답하기 전에 수행합니다. 이 기능은 수신자 호스트의 연속 오류로 인해 수신 확인 응답을 하지 못하는 경우 수신자가 메시지 복사본을 여러 개 수신하지 않도록 합니다. AsyncOS는 이 수신자를 메일 로그에 가능한 전달로 기록하고 메시지를 완료된 메시지로 간주합니다.

기본 최대 동시 연결 수

어플라이언스가 아웃바운드 메시지 전송을 위해 설정하는 기본 최대 동시 연결 수도 지정할 수 있습니다. (시스템 전체 기본값은 개별 도메인에 대해 10,000개입니다.) 이 제한은 아웃바운드 메시지 전달에 대한 리스너별 최대 동시 연결 수(리스너별 기본값은 개인 리스너의 경우 600개이고, 공용 리스너의 경우 1,000개임)와 함께 모니터링됩니다. 값을 기본값보다 낮게 설정하면 게이트웨이가 취약한 네트워크에 큰 영향을 미치는 것을 방지할 수 있습니다. 예를 들어 특정 방화벽이 대량의 연결을 지원하지 않는 경우 그러한 환경에서 DoS(서비스 거부) 경고가 발생할 수 있습니다.

deliveryconfig 예

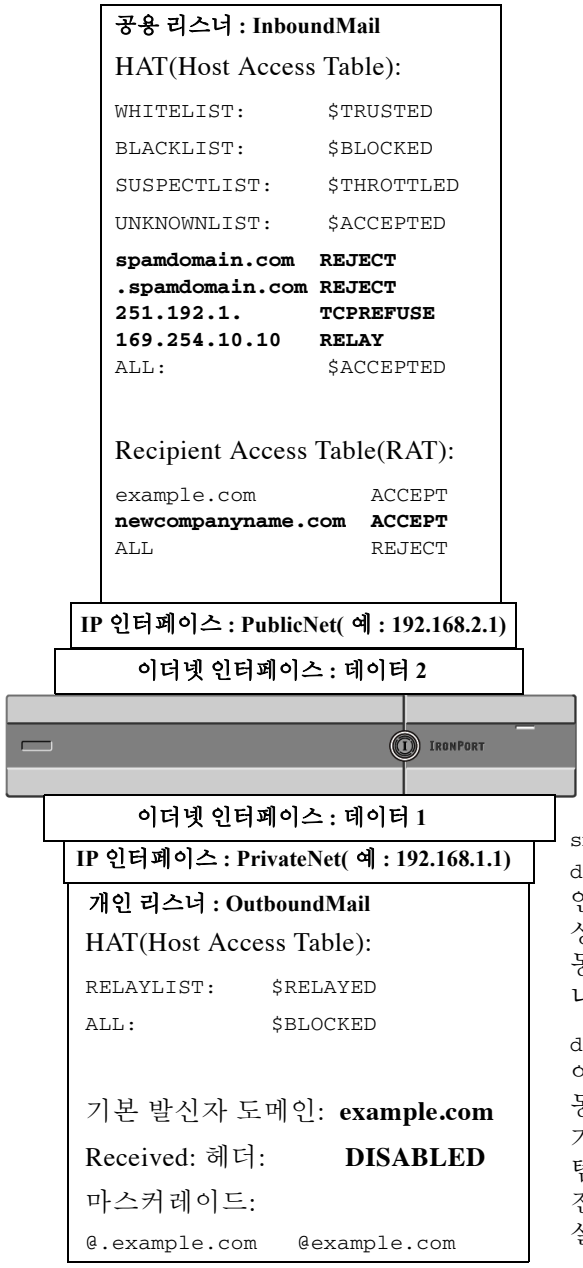
다음 예에서는 "가능한 전달"이 활성화된 상태에서 deliveryconfig 명령을 사용하여 기본 인터페이스가 "Auto(자동)"로 설정되었습니다. 시스템 전체 최대 아웃바운드 메시지 전달은 9,000개로 설정되었습니다.

```
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 구성은 다음과 같습니다.

그림 24-8 대상 및 전달 매개변수 설정



IronPort 이메일 보안 어플라이언스

small-isp.net 호스트에 destconfig 항목을 사용하여 동시 연결 수를 100개로 제한하거나 가상 게이트웨이 주소를 사용하여 동시 연결 수를 10개로 제한했습니다.

deliveryconfig 명령을 사용하여 이메일 전달 시 인터페이스의 자동 선택이 사용되고 가능한 전달 기능이 활성화되었습니다. 시스템 전체 최대 아웃바운드 메시지 전달은 총 동시 연결 수 9,000개로 설정되었습니다.

가상 게이트웨이™ 기술을 사용하여 모든 호스팅된 도메인에 대한 메일 게이트웨이 구성

이 섹션에서는 Cisco 가상 게이트웨이™ 기술과 그 이점, 가상 게이트웨이 주소를 설정하는 방법 및 가상 게이트웨이 주소를 모니터링하고 관리하는 방법에 대해 설명합니다.

Cisco 가상 게이트웨이 기술을 통해 고유한 IP 주소, 호스트 이름 및 도메인 등 호스팅하는 모든 도메인에 엔터프라이즈 메일 게이트웨이를 구성하고 동일한 물리적 어플라이언스 내에서 호스팅하는 동안 이러한 도메인에 대해 기업 이메일 정책 시행하거나 안티스팸 전략을 만들 수 있습니다. 모든 Email Security 어플라이언스 모델에서 사용 가능한 가상 게이트웨이 주소 수는 255개입니다.

관련 주제

- 개요, 24-57페이지
- 가상 게이트웨이 주소 설정, 24-57페이지
- 가상 게이트웨이 주소 모니터링, 24-65페이지
- 가상 게이트웨이 주소별 전송 연결 관리, 24-65페이지

개요

Cisco는 기업이 이메일을 통해 안전하게 고객과 통신할 수 있도록 설계된 독창적인 가상 게이트웨이 기술을 개발했습니다. 가상 게이트웨이 기술을 통해 사용자는 어플라이언스를 이메일을 주고받는 데 사용할 여러 가상 게이트웨이 주소로 구분할 수 있습니다. 각 가상 게이트웨이 주소에는 고유한 IP 주소, 호스트 이름 및 도메인 및 이메일 큐가 지정됩니다.

고유한 IP 주소 및 호스트 이름을 각 가상 게이트웨이 주소에 할당하면 게이트웨이를 통해 전달되는 이메일이 수신자 호스트에 의해 적절히 식별되고 중요한 이메일이 스팸으로 차단되지 않도록 할 수 있습니다. 이 어플라이언스는 SMTP HELO 명령에서 각 가상 게이트웨이 주소마다 올바른 호스트 이름을 지정할 수 있는 인텔리전스를 갖추고 있습니다. 이를 통해 수신 ISP(인터넷 서비스 공급자)가 역방향 DNS 조회를 수행하는 경우 어플라이언스는 해당 가상 게이트웨이 주소를 통해 전송된 이메일의 IP 주소를 일치시킬 수 있습니다. 대부분의 ISP는 역방향 DNS 조회를 사용하여 요청하지 않은 이메일을 검색하기 때문에 이 기능은 매우 유용합니다. 역방향 DNS 조회의 IP 주소가 전송 호스트의 IP 주소와 일치하지 않을 경우 ISP는 발신자가 부적합하다고 간주하여 대부분의 경우 이메일을 무시합니다. Cisco 가상 게이트웨이 기술을 사용하면 역방향 DNS 조회에서 항상 전송 IP 주소를 일치시키므로 메시지가 실수로 차단되는 것을 방지할 수 있습니다.

각 가상 게이트웨이 주소의 메시지는 개별 메시지 큐에도 할당됩니다. 특정 수신자 호스트가 한 가상 게이트웨이 주소의 이메일을 차단하는 경우 해당 호스트를 대상으로 하는 메시지는 큐에 남게 되어 결과적으로 시간 초과가 발생하게 됩니다. 그러나 차단되지 않은 다른 가상 게이트웨이 큐의 동일한 도메인을 대상으로 하는 메시지는 정상적으로 전달됩니다. 이러한 큐는 전달을 목적으로 개별 처리되지만 시스템 관리, 로깅 및 보고 기능에서는 여전히 모든 가상 게이트웨이 큐가 마치 하나인 것처럼 통합되어 보입니다.

가상 게이트웨이 주소 설정

Cisco 가상 게이트웨이 주소를 설정하기에 앞서, 이메일을 전송하는 데 사용할 IP 주소 집합을 할당해야 합니다. (자세한 내용은 "네트워크 및 IP 주소 할당" 부록을 참조하십시오.) 또한 IP 주소가 올바른 호스트 이름으로 확인되도록 DNS 서버가 적절히 구성되었는지 확인해야 합니다. DNS 서버가 적절히 구성되면 수신자 호스트가 역방향 DNS 조회를 수행하는 경우 올바른 IP/호스트 이름 쌍으로 확인됩니다.

관련 주제

- 가상 게이트웨이에 사용할 새 IP 인터페이스 생성, 24-58페이지
- 전달할 메시지를 IP 인터페이스에 매핑, 24-60페이지
- altsrchost 파일 가져오기, 24-61페이지
- altsrchost 제한, 24-61페이지
- altsrchost 명령에 대한 올바른 매핑이 포함된 텍스트 파일 예, 24-62페이지
- CLI를 통해 altsrchost 매핑 추가, 24-62페이지

가상 게이트웨이에 사용할 새 IP 인터페이스 생성

IP 주소 및 호스트 이름을 설정한 후에 가상 게이트웨이 주소를 구성하기 위한 첫 번째 단계는 GUI의 Network(네트워크) > IP Interfaces(IP 인터페이스) 페이지 또는 CLI의 `interfaceconfig` 명령을 사용하여 IP/호스트 이름 쌍을 가진 새 IP 인터페이스를 생성하는 것입니다.

IP 인터페이스가 구성되면 여러 IP 인터페이스를 인터페이스 그룹으로 통합할 수 있습니다. 그런 다음 이러한 그룹을 특정 가상 게이트웨이 주소에 할당하여 시스템이 이메일을 전달할 때 "라운드 로빈" 방식으로 순환되게 할 수 있습니다.

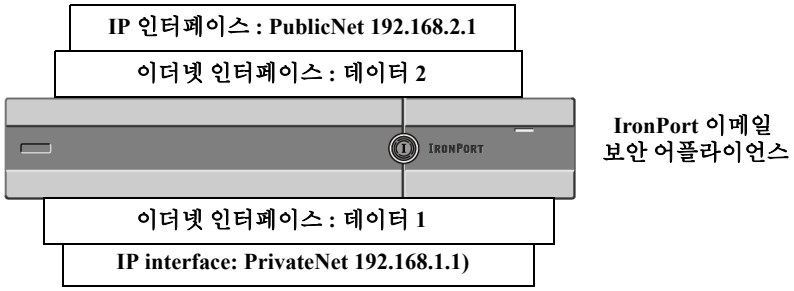
필수 IP 인터페이스를 생성한 후에 가상 게이트웨이 주소를 설정하고 각 IP 인터페이스 또는 인터페이스 그룹에서 보낼 이메일 캠페인을 정의할 수 있는 옵션으로는 2가지 방법이 있습니다.

- `altsrchost` 명령을 사용하여 특정 발신자 IP 주소 또는 봉투 발신자 주소 정보에서 전송을 위한 호스트 IP 인터페이스(가상 게이트웨이 주소) 또는 인터페이스 그룹으로 이메일을 매핑할 수 있습니다.
- 메시지 필터를 통해 특정 호스트 IP 인터페이스(가상 게이트웨이 주소) 또는 인터페이스 그룹을 사용하여 플래그가 지정된 메시지를 전달하도록 특정 필터를 설정할 수 있습니다. 소스 호스트(가상 게이트웨이 주소) 변경 작업, 9-65페이지 항목을 참조하십시오. (이 방법은 위의 방법보다 더 유연하고 강력합니다.)

IP 인터페이스 생성에 대한 자세한 내용은 "어플라이언스 액세스" 부록을 참조하십시오.

지금까지 그림 24-9와 같이 다음 인터페이스를 정의하여 이메일 게이트웨이 구성을 사용했습니다.

그림 24-9 공용 및 개인 인터페이스 예



다음 예의 IP Interfaces(IP 인터페이스) 페이지에서는 관리 인터페이스와 함께 두 가지 인터페이스(PrivateNet 및 PublicNet)가 구성된 것을 확인할 수 있습니다.

그림 24-10 IP 인터페이스 페이지

IP Interfaces

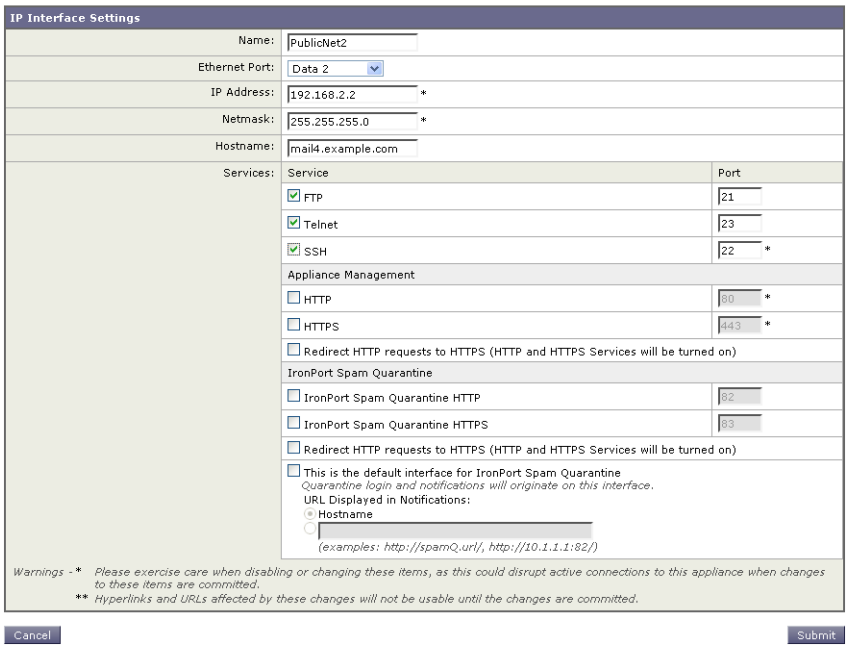
Network Interfaces and IP Addresses

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	

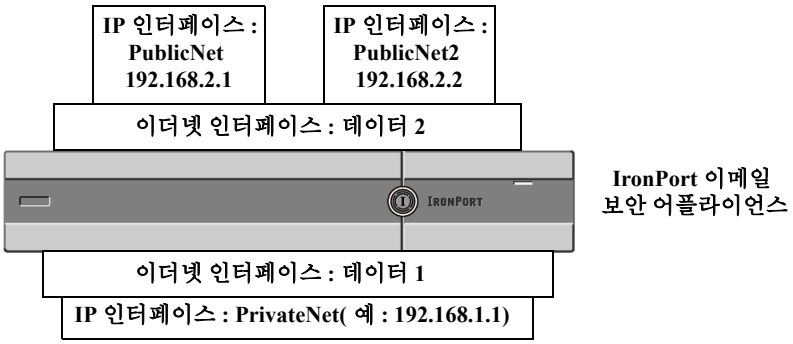
다음으로, Add IP Interface(IP 인터페이스 추가) 페이지를 통해 Data2 이더넷 인터페이스에서 PublicNet2라는 새 인터페이스를 생성합니다. IP 주소로 192.168.2.2가 사용되고 호스트 이름으로 `mail4.example.com`이 지정되었습니다. 그런 다음 FTP(포트 21), 텔넷(포트 23) 및 SSH(포트 22)에 대한 서비스가 활성화되었습니다.

그림 24-11 IP 인터페이스 추가 페이지



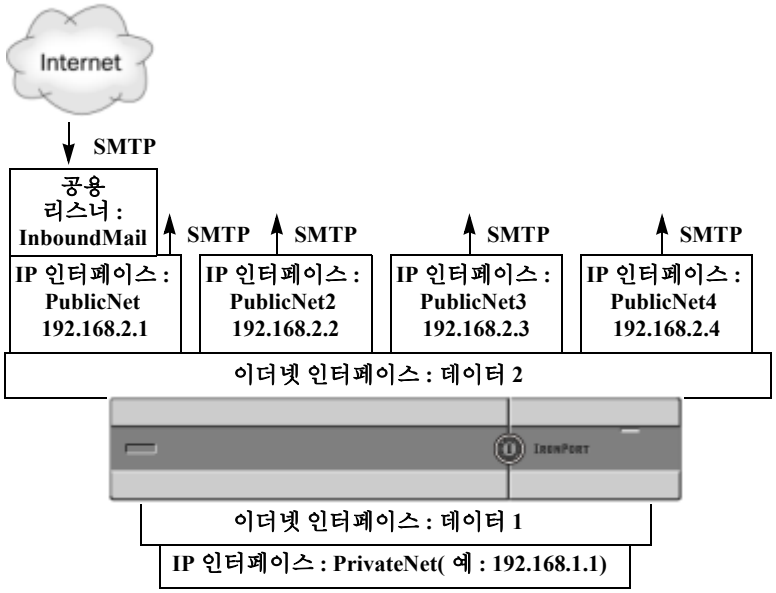
이제 이메일 게이트웨이 구성은 다음과 같습니다.

그림 24-12 다른 공용 인터페이스 추가



가상 게이트웨이 주소를 사용하여 그림 24-13과 같은 구성도 할 수 있습니다.

그림 24-13 한 이더넷 인터페이스의 가상 게이트웨이 주소 4개



개별 IP 인터페이스 4개를 사용하여 메일을 전달할 수 있습니다. 이러한 경우 인터넷의 메시지를 수락하기 위해 하나의 공용 리스너만 구성됩니다.

전달할 메시지를 IP 인터페이스에 매핑

`altsrchost` 명령은 각 어플라이언스를 이메일을 전달하기 위한 여러 IP 인터페이스(가상 게이트웨이 주소)로 분할할 수 있는 가장 단순하고 간편한 방법입니다. 그러나 특정 가상 게이트웨이를 대상으로 메시지를 보다 강력하고 유연하게 매핑해야 하는 사용자는 메시지 필터의 사용을 조사해야 합니다. 자세한 내용은 9 장, "메시지 필터를 사용하여 이메일 정책 적용" 항목을 참조하십시오.

`altsrchost` 명령을 사용하면 이메일 전달 중에 다음 중 한 가지 항목을 기준으로 IP 인터페이스 또는 인터페이스 그룹을 제어할 수 있습니다.

- 발신자의 IP 주소
- 봉투 발신자 주소

시스템에서 이메일을 전달하는 데 사용할 IP 인터페이스 또는 인터페이스 그룹을 지정하려면 발신자의 IP 주소 또는 봉투 발신자 주소를 IP 인터페이스 또는 인터페이스 그룹(인터페이스 이름 또는 그룹 이름으로 지정됨)에 페어링하는 매핑 키를 생성해야 합니다.

AsyncOS는 IP 주소 및 봉투 발신자 주소를 모두 매핑 키와 비교합니다. IP 주소 또는 봉투 발신자 주소가 매핑 키와 일치할 경우 해당 IP 인터페이스가 아웃바운드 전송에 사용됩니다. 일치하는 항목이 없다면 기본 아웃바운드 인터페이스가 사용됩니다.

시스템은 다음 키 중 하나를 일치시키고 다음 순서로 우선순위를 부여합니다.

발신자의 IP 주소	발신자의 IP 주소가 정확히 일치해야 합니다. 예: `192.168.1.5`
적절한 형태의 봉투 발송인	봉투 발신자는 전체 주소가 정확히 일치해야 합니다. 예: `username@example.com`
사용자 이름	시스템은 사용자 이름 구문을 봉투 발신자 주소(`@` 기호까지)와 비교합니다. `@` 기호도 포함되어야 합니다. 예: `username@`
도메인	시스템은 `@` 기호로 시작하는 봉투 발신자 주소와 도메인 이름 구문을 비교합니다. `@` 기호도 포함되어야 합니다. 예: `@example.com`

참고 리스너는 altsrchost 테이블의 정보를 확인하고, 마스커레이드 정보를 확인한 *후* 메시지 필터를 확인하기 *전* 이메일을 특정 인터페이스로 보냅니다.

altsrchost 명령의 다음 하위 명령을 사용하여 가상 게이트웨이의 매핑을 생성합니다.

구문	설명
new	새 매핑을 수동으로 생성합니다.
print	현재 매핑 목록을 표시합니다.
delete	테이블에서 매핑 중 하나를 삭제합니다.

altsrchost 파일 가져오기

HAT, RAT, smtproutes, 마스커레이드 및 별칭 테이블과 마찬가지로, 파일을 내보내고 가져오는 방식으로 altsrchost 항목을 수정할 수 있습니다.

절차

1단계 altsrchost 명령의 export 하위 명령을 사용하여 기존 항목을 파일(이름은 사용자가 지정)로 내보냅니다.

2단계 CLI 외부에서 파일을 가져옵니다. (자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스" 참조.)

3단계 텍스트 편집기를 사용하여 파일에서 새 항목을 생성합니다. altsrchost 테이블에서 규칙이 나타나는 순서는 중요합니다.

4단계 파일을 저장하고, 가져올 수 있도록 인터페이스의 "altsrchost" 디렉토리에 넣습니다. (자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스" 참조.)

5단계 altsrchost의 import 하위 명령을 사용하여 편집된 파일을 가져옵니다.

altsrchost 제한

최대 1,000개의 altsrchost 항목을 정의할 수 있습니다.

altsrchost 명령에 대한 올바른 매핑이 포함된 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 줄 단위로 수행되며 발신자 IP 주소 또는 봉투 발신자 주소줄을 인터페이스 이름에 매핑합니다. 키는 공백이 아닌 문자로 구성된 첫 번째 블록과 이어서 공백이 아닌 문자로 구성된 두 번째 블록(인터페이스 이름)으로 구성됩니다. 이는 쉼표(,) 또는 공백( )으로 구분됩니다. 주석 줄은 숫자 기호(#)로 시작되며 무시됩니다.

CLI를 통해 altsrchost 매핑 추가

다음 예에는 기존 매핑이 없음을 보여 주는 altsrchost 테이블이 출력되어 있습니다. 그런 다음 2개의 항목이 생성됩니다.

- 그룹웨어 서버 호스트 @exchange.example.com의 메일이 PublicNet 인터페이스에 매핑됩니다.
- 발신자 IP 주소 192.168.35.35(예: 마케팅 캠페인 메시징 시스템)의 메일이 PublicNe2t 인터페이스에 매핑됩니다.

마지막으로 확인을 위해 altsrchost 매핑이 출력되고 변경사항이 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
```

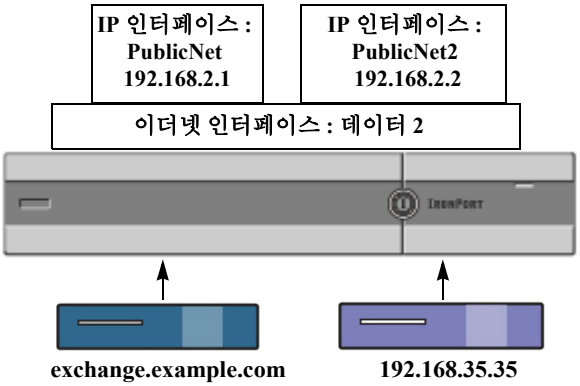
```
Which interface do you want to send messages for @exchange.example.com from?

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 변경을 보여주는 그림을 그림 24-14에서 확인할 수 있습니다.

그림 24-14 예: 사용할 IP 인터페이스 또는 인터페이스 그룹 선택



이러한 매핑을 생성하도록 `altsrchost` 테이블이 수정되었습니다. `@exchange.example.com`의 메시지는 PublicNet 인터페이스를 사용하고, 192.168.35.35의 메시지는 PublicNet2 인터페이스를 사용합니다.

가상 게이트웨이 주소 모니터링

가상 게이트웨이 주소마다 전송을 위한 고유한 이메일 큐를 가지고 있지만 시스템 관리, 로깅 및 보고 기능에서는 여전히 모든 게이트웨이 큐가 마치 하나인 것처럼 통합되어 보입니다. 각 가상 게이트웨이 큐에 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 사용하는 경우 각 가상 게이트웨이 주소에 대한 정보도 표시됩니다. 이 명령을 실행하는 경우 반환될 호스트 정보의 도메인을 입력해야 합니다. AsyncOS 캐시에 저장된 DNS 정보 및 수신자 호스트에서 반환된 마지막 오류도 제공됩니다. 반환되는 데이터는 마지막 `resetcounters` 명령이 실행된 후 계속 누적됩니다.

반환되는 통계는 두 가지 범주(카운터 및 게이지)로 그룹화됩니다. 반환되는 또 다른 데이터로는 마지막 활동, MX 레코드 및 마지막 5XX 오류가 있습니다.

가상 게이트웨이 주소별 전송 연결 관리

특정 시스템 매개변수에는 시스템 및 가상 게이트웨이 수준의 설정이 필요합니다.

예를 들어 일부 수신자 ISP는 각 클라이언트 호스트에 허용되는 연결 수를 제한합니다. 따라서 여러 가상 게이트웨이 주소를 통해 이메일을 전달하는 경우에는 특히 ISP와의 통신을 관리하는 것이 중요합니다.

`destconfig` 명령 및 가상 게이트웨이 주소에 미치는 영향에 대한 자세한 내용은 대상 제어을 사용하여 이메일 전달 제어, 24-40페이지 항목을 참조하십시오.

가상 게이트웨이 주소 "그룹"을 생성하는 경우 이 그룹이 IP 주소 254개로 이루어져 있더라도 가상 게이트웨이의 양호한 인접 테이블 설정이 해당 그룹에 적용됩니다.

예를 들어 "라운드 로빈" 방식으로 순환되는 그룹으로 254개의 아웃바운드 IP 주소 집합 그룹을 생성하거나 `small-isp.com`에 대한 양호한 인접 테이블이 시스템의 경우 동시 연결 100개로 설정되고, 가상 게이트웨이 주소의 경우 연결 10개로 설정되어 있는 경우가 있습니다. 이 구성에서는 해당 그룹의 모든 254개 IP 주소에 대해 총 10개를 초과하는 연결을 열지 *않습니다*. 이 그룹은 하나의 가상 게이트웨이 주소로 처리됩니다.

전역 가입 취소 사용

특정 수신자, 수신자 도메인 또는 IP 주소가 어플라이언스에서 메시지를 수신하지 못하게 하려면 AsyncOS 전역 가입 취소 기능을 사용합니다. `unsubscribe` 명령을 사용하면 전역 가입 취소 목록에 주소를 추가하거나 삭제할 수 있으며 해당 기능을 활성화하거나 비활성화할 수도 있습니다. AsyncOS는 "전역으로 가입 취소된" 사용자, 도메인, 이메일 주소 및 IP 주소 목록과 비교하여 모든 수신자 주소를 확인합니다. 목록의 주소와 일치하는 수신자는 삭제되거나 하드 바운스되고 전역 가입 취소(GUS) 카운터가 증가합니다. (로그 파일에는 일치하는 수신자가 삭제되었는지, 아니면 하드 바운스되었는지 기록합니다.) 이메일을 수신자에게 이메일을 전송하려는 시도가 발생하기 직전에 GUS 확인이 이루어지므로 시스템에서 전송된 모든 메시지가 검사됩니다.

참고 전역 가입 취소는 이름 제거 및 일반적인 메일 목록 유지 관리를 대신하여 사용되지 않습니다. 이 기능은 이메일이 부적절한 엔터티로 전달되지 않도록 하는 유사 시에 사용하는 대기 메커니즘으로 동작하도록 설계되었습니다.

전역 가입 취소 기능은 개인 및 공용 리스너에 적용됩니다.

전역 가입 취소의 최대 주소는 10,000개입니다. 이 제한을 늘리려면 Cisco 영업 담당자에게 문의하십시오. 전역 가입 취소 주소의 형식은 다음 4가지 중 하나를 사용합니다.

표 24-10 전역 가입 취소 구문

username@example.com	적절한 형태의 이메일 주소 이 구문은 특정 도메인의 특정 수신자를 차단하는 데 사용됩니다.
username@	사용자 이름 사용자 이름 구문은 모든 도메인에서 지정된 사용자 이름을 가진 수신자를 모두 차단합니다. 구문은 @ 기호가 뒤에 오는 사용자 이름입니다.
@example.com	도메인 도메인 구문은 특정 도메인을 대상으로 하는 모든 수신자를 차단하는 데 사용됩니다. 구문은 @ 기호가 앞에 오는 특정 도메인입니다.
@.example.com	부분 도메인 부분 도메인 구문은 특정 도메인 및 해당하는 모든 하위 도메인을 대상으로 하는 수신자를 모두 차단하는 데 사용됩니다.
10.1.28.12	IP 주소 IP 주소 구문은 특정 IP 주소를 대상으로 하는 모든 수신자를 차단하는 데 사용됩니다. 이 구문은 단일 IP 주소에서 여러 도메인을 호스팅하는 경우에 유용합니다. 구문은 점으로 구분된 일반 옥텟 IP 주소로 구성됩니다.

관련 주제

- CLI를 사용하여 전역 가입 취소 주소 추가, 24-67페이지
- 전역 가입 취소 파일 내보내기 및 가져오기, 24-69페이지

CLI를 사용하여 전역 가입 취소 주소 추가

이 예에서는 user@example.net 주소가 전역 가입 취소 목록에 추가되고 메시지를 하드 바운스하도록 기능을 구성합니다. 이 주소로 전송된 메시지는 바운스되며 어플라이언스는 전송 전에 즉시 메시지를 바운스합니다.

```
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 가입 취소 파일 내보내기 및 가져오기

HAT, RAT, smtproutes, 정적 마스커레이드 테이블, 별칭 테이블, 도메인 맵 테이블 및 altsrchost 항목과 마찬가지로, 파일을 내보내고 가져오는 방식으로 전역 가입 취소 항목을 수정할 수 있습니다.

절차

1단계 unsubscribe 명령의 export 하위 명령을 사용하여 기존 항목을 파일(이름은 사용자가 지정)로 내보냅니다.

2단계 CLI 외부에서 파일을 가져옵니다. (자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스" 참조.)

3단계 텍스트 편집기를 사용하여 파일에서 새 항목을 생성합니다.

파일의 각 항목은 새 줄로 구분합니다. 모든 표준 운영 체제의 리턴 표시를 사용할 수 있습니다 (<CR>, <LF> 또는 <CR><LF>). 주석 줄은 숫자 기호(#)로 시작되며 무시됩니다. 예를 들어 다음 파일에서는 단일 수신자 이메일 주소(test@example.com), 특정 도메인(@testdomain.com)의 모든 수신자, 여러 도메인에서 이름이 동일한 모든 사용자(testuser@) 및 특정 IP 주소(11.12.13.14)의 수신자를 제외합니다.

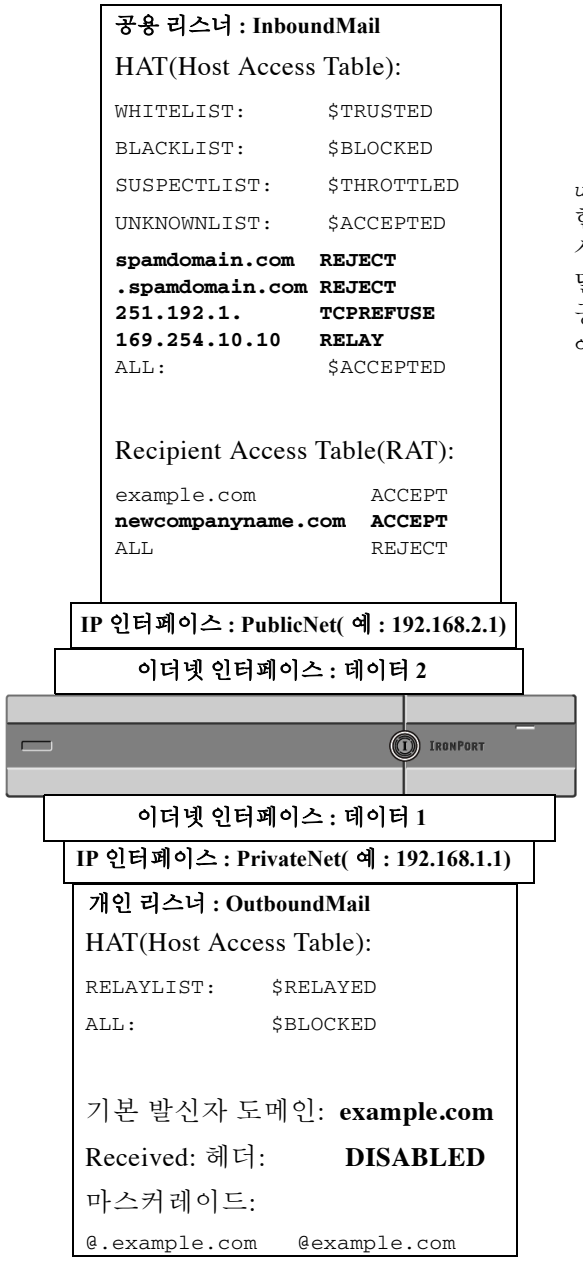
```
# this is an example of the global_unsubscribe.txt file

test@example.com

@testdomain.com

testuser@

11.12.13.14
```

4단계 파일을 저장하고, 가져올 수 있도록 인터페이스의 구성 디렉토리에 넣습니다. (자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스" 참조.)

5단계 unsubscribe의 import 하위 명령을 사용하여 편집된 파일을 가져옵니다.

이제 이메일 게이트웨이 구성은 다음과 같습니다.

그림 24-15 전역 가입 취소 예



user@example.net 주소에 대한 전역 가입 취소 항목이 생성되었습니다. 이 주소로 전달되는 메시지는 개인 또는 공용 리스너가 수락하는 메일에서 바운스됩니다.

IronPort 이메일 보안 어플라이언스

검토: 이메일 파이프라인

표 24-11 및 표 24-12에서는 이메일이 시스템을 통해 라우팅(수신부터 전달에 이르기까지)되는 방식에 대해 개괄적으로 소개합니다. 각 기능은 순서대로(하향식) 처리되며 간략히 요약됩니다. 그림 24-15에서 음영 처리된 영역은 작업 큐에서 발생하는 프로세스를 나타냅니다.

이 파이프라인에서 `trace` 명령을 사용하여 기능의 구성 대부분을 테스트할 수 있습니다. 자세한 내용은 문제 해결 장의 "테스트 메시지를 사용하여 메일 흐름 디버깅: 추적"을 참조하십시오.

참고 발송 메일의 경우 신종 바이러스 필터(Outbreak Filter) 단계 다음에 RSA 이메일 데이터 유출 방지 검사가 이루어집니다.

표 24-11 Email Security 어플라이언스의 이메일 파이프라인: 이메일 수신 기능

기능	설명
호스트 테이블(HAT) **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 메시지당 및 시간당 최대 수신자 TCP 수신 대기 큐 크기 TLS: no/preferred/required SMTP AUTH: no/preferred/required 잘못된 형식의 FROM 헤더가 있는 이메일 삭제 발신자 확인 예외 테이블의 항목의 메일을 항상 수락하거나 거부 SenderBase on/off(IP 프로파일링/흐름 제어)
Received 헤더	수락한 이메일에 Received 헤더를 추가합니다(on/off).
기본 도메인	"bare" 사용자 주소의 기본 도메인을 추가합니다.
바운스 확인	수신 바운스 메시지가 정상적인 메시지인지 확인하는 데 사용됩니다.
도메인 맵	메시지에서 도메인 맵 테이블의 도메인과 일치하는 각 수신자에 대한 봉투 수신자를 재작성합니다.
Recipient Access Table(RAT)	(공용 리스너에만 해당) `RCPT TO` 및 사용자 지정 SMTP 응답에서 수신자를 수락하거나 거부합니다. 특수 수신자가 제한을 우회하도록 허용합니다.
별칭 테이블	봉투 수신자를 재작성합니다. (시스템 전체에서 구성되며, `aliasconfig`는 `listenerconfig`의 하위 명령이 아닙니다.)
LDAP 수신자 수락	SMTP 대화 내에서 수신자 수락에 대한 LDAP 검증이 이루어집니다. 수신자를 LDAP 디렉토리에서 찾을 수 없는 경우 메시지가 삭제되거나 바운스됩니다. 대신 작업 큐 내에서 수행하도록 LDAP 검증을 구성할 수 있습니다.

표 24-12 Email Security 어플라이언스의 이메일 파이프라인: 라우팅 및 전달 기능 구성

작업 큐	**LDAP 수신자 수락**		작업 큐 내에서 수신자 수락에 대한 LDAP 검증이 이루어집니다. 수신자를 LDAP 디렉토리에서 찾을 수 없는 경우 메시지가 삭제되거나 바운스됩니다. 대신 SMTP 대화 내에서 수행하도록 LDAP 검증을 구성할 수 있습니다.
	마스커레이드 또는 **LDAP** 마스커레이드		작업 큐에서 마스커레이드가 수행됩니다. 정적 테이블에서 또는 LDAP 쿼리를 통해 봉투 발신자, To:, From: 및/또는 CC: 헤더를 재작성합니다.
	LDAP 라우팅		메시지 라우팅 또는 주소 재작성을 위한 LDAP 쿼리가 수행됩니다. 그룹 LDAP 쿼리는 메시지 필터 규칙 `mail-from-group` 및 `rcpt-to-group`과 함께 동작합니다.
	메시지 필터*		메시지 필터는 메시지 "분리" 전에 적용됩니다. * 격리할 메시지를 전송할 수 있습니다.
	안티스팸**	수신자 검사 필터	안티스팸 검사 엔진은 메시지를 검사하고 이후의 처리를 위해 판정 결과를 반환합니다.
	안티 바이러스*		안티 바이러스 검사는 메시지에 바이러스가 있는지 점검합니다. 메시지가 검사되고 가능한 경우 선택적으로 복구됩니다. * 격리할 메시지를 전송할 수 있습니다.
	AMP(Advanced Malware Protection)		AMP는 첨부 파일에서 악성코드를 탐지하기 위해 파일 평판 검사 및 파일 분석을 수행합니다.
	콘텐츠 필터*		콘텐츠 필터가 적용됩니다. * 격리할 메시지를 전송할 수 있습니다.
	신종 바이러스 필터(Outbreak Filter)*		신종 바이러스 필터(Outbreak Filter) 기능은 신종 바이러스로부터 보호 기능을 제공합니다. * 격리할 메시지를 전송할 수 있습니다.
	가상 게이트웨이		특정 IP 인터페이스 또는 IP 인터페이스 그룹을 통해 메일을 전송합니다.
	전달 제한		1. 기본 전송 인터페이스를 설정합니다. 2. 최대 전체 아웃바운드 연결 수를 설정합니다.
	도메인 기반 제한		각 가상 게이트웨이 및 전체 시스템에 대한 도메인별 최대 아웃바운드 연결 수, 사용할 바운스 프로파일, 전송에 대한 TLS 환경 설정 (no/preferred/required)을 정의합니다.
	도메인 기반 라우팅		봉투 수신자를 재작성하지 않고 도메인을 기반으로 메일을 라우팅합니다.
	전역 가입 취소		특정 목록에 대한 수신자를 삭제합니다(시스템 전체에서 구성됨).
	바운스 프로파일		전달할 수 없는 메시지 처리. 리스너별로 구성하거나 대상 제어 항목별로 구성하거나 메시지 필터를 통해 구성할 수 있습니다.

* 이러한 기능은 격리라는 특수 큐로 메시지를 보낼 수 있습니다.

25 장

LDAP 쿼리

LDAP 쿼리 개요

네트워크 인프라에서 LDAP 디렉토리(예: Microsoft Active Directory, SunONE Directory 서버 또는 OpenLDAP 디렉토리) 내에 사용자 정보를 저장하는 경우, 메시지를 수락, 라우팅 및 인증하기 위해 LDAP 서버를 쿼리하도록 어플라이언스를 구성할 수 있습니다. 하나 또는 다중 LDAP 서버와 작업하도록 어플라이언스를 구성할 수 있습니다.

다음 섹션에서는 수행할 수 있는 LDAP 쿼리 유형에 대한 개요, 메시지를 인증, 수락 및 라우팅하기 위해 LDAP이 어플라이언스에서 작업하는 방식, LDAP와 작업하도록 어플라이언스를 구성하는 방법을 제공합니다.

관련 주제

- LDAP 쿼리 이해, 25-2페이지
- LDAP가 AsyncOS와 작업하는 방식 이해, 25-3페이지
- LDAP 서버와 작업하도록 Cisco IronPort 어플라이언스 구성, 25-4페이지

- LDAP 서버 정보를 저장하도록 LDAP 서버 프로파일 생성, 25-5페이지
- LDAP 서버 테스트, 25-6페이지
- 특정 리스너에서 실행되도록 LDAP 쿼리 활성화, 25-6페이지
- Microsoft Exchange 5.5에 대한 지원 향상, 25-9페이지

LDAP 쿼리 이해

네트워크 인프라에서 LDAP 디렉토리 내에 사용자 정보를 저장하는 경우, 다음 목적으로 LDAP 서버를 쿼리하도록 어플라이언스를 구성할 수 있습니다.

- **수락 쿼리**. 기존 LDAP 인프라를 사용하여 수신 메시지(공용 리스너에 있음)의 수신자 이메일 주소를 처리하는 방식을 정의할 수 있습니다. 자세한 내용은 수신자 검증에 수락 쿼리 사용, 25-19페이지 항목을 참조하십시오.
- **라우팅(앨리어싱).** 네트워크의 LDAP 디렉토리에서 사용 가능한 정보에 기반하여 적절한 주소 및/또는 메일 호스트에 메시지를 라우팅하도록 어플라이언스를 구성할 수 있습니다. 자세한 내용은 라우팅 쿼리를 사용하여 여러 대상 주소로 메일 전송, 25-20페이지 항목을 참조하십시오.
- **인증서 인증.** 사용자의 메일 클라이언트와 Email Security 어플라이언스 간에 SMTP 세션을 인증하기 위해 클라이언트 인증서의 유효성을 확인하는 쿼리를 만들 수 있습니다. 자세한 내용은 클라이언트 인증서의 유효성 검사, 26-51페이지 항목을 참조하십시오.
- **마스커레이드**. 봉투 발신자(발송 메일) 및 메시지 헤더(수신 메일, 예를 들어 To:, Reply To:, From: 또는 Cc:)를 마스커레이드할 수 있습니다. 마스커레이드에 대한 자세한 내용은 마스커레이드 쿼리를 사용하여 봉투 발신자 재작성, 25-21페이지 항목을 참조하십시오.
- **그룹 쿼리**. LDAP 디렉토리의 그룹을 기준으로 메시지에 대한 동작을 수행하도록 어플라이언스를 구성할 수 있습니다. 이 작업은 그룹 쿼리를 메시지 필터와 연결하여 수행합니다. 정의된 LDAP 그룹과 일치하는 메시지의 메시지 필터에 사용 가능한 모든 메시지 동작을 수행할 수 있습니다. 자세한 내용은 그룹 LDAP 쿼리를 사용하여 수신자가 그룹 멤버인지 판별, 25-23페이지 항목을 참조하십시오.
- **도메인 기반 쿼리**. 어플라이언스가 단일 리스너에서 다양한 도메인에 각각 다른 쿼리를 수행할 수 있도록 도메인 기반 쿼리를 생성할 수 있습니다. Email Security 어플라이언스는 도메인 기반 쿼리를 실행할 때 도메인에 따라 사용할 쿼리를 결정하고 해당 도메인과 연결된 LDAP 서버를 쿼리합니다.
- **체인 쿼리.** 어플라이언스에서 일련의 쿼리를 순서대로 수행하도록 체인 쿼리를 생성할 수 있습니다. 체인 쿼리를 구성할 때 어플라이언스는 LDAP 어플라이언스가 만족하는 결과를 반환할 때까지 각 쿼리를 순서대로 실행합니다.
- **디렉토리 수집 방지**. LDAP 디렉토리를 사용하여 디렉토리 수집 공격을 방지하도록 어플라이언스를 구성할 수 있습니다. SMTP 대화 중 또는 작업 큐 내에서 디렉토리 수집 방지를 구성할 수 있습니다. 수신자가 LDAP 디렉토리에 없는 경우, 지연된 바운스를 수행하거나 메시지를 완전히 삭제하도록 시스템을 구성할 수 있습니다. 따라서, 스패머는 올바른 이메일 주소와 올바르지 않은 이메일 주소를 구분할 수 없습니다. LDAP를 사용하여 디렉토리 수집 공격 방지, 25-29페이지 항목을 참조하십시오.
- **SMTP 인증**. AsyncOS는 SMTP 인증을 지원합니다. SMTP 인증은 SMTP 서버에 연결된 클라이언트를 인증하는 메커니즘입니다. 이 기능을 사용하여 조직에 소속된 사용자가 원격에서 연결하는 경우에도(예: 자택에서 또는 출장 중에) 조직의 메일 서버를 사용하여 메일을 전송하도록 설정할 수 있습니다. 자세한 내용은 SMTP 인증을 위한 AsyncOS 구성, 25-32페이지 항목을 참조하십시오.

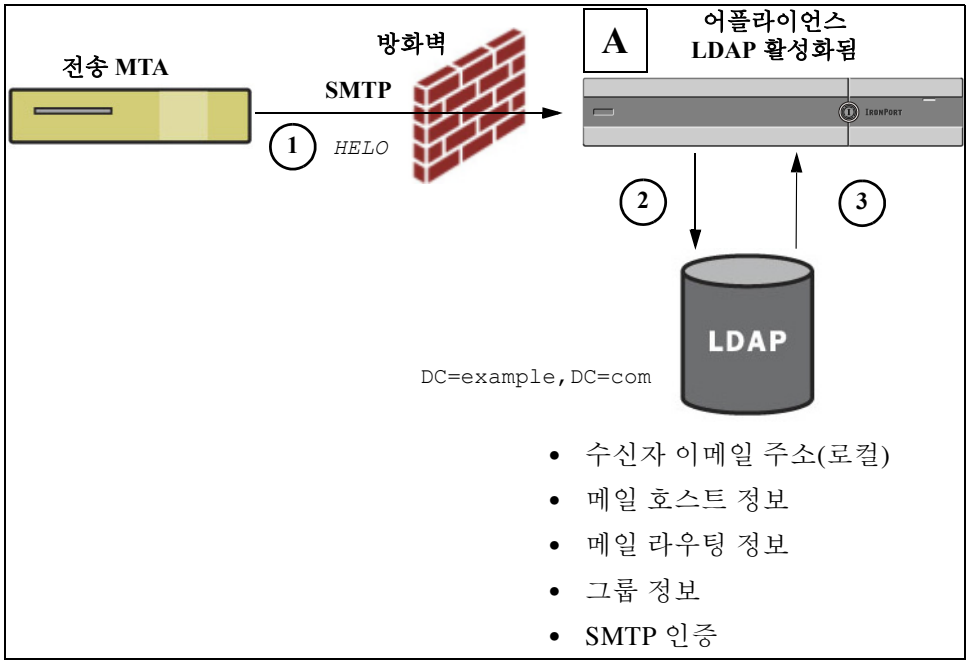
- **외부 인증**. 어플라이언스에서 LDAP 디렉토리를 사용하여 어플라이언스에 로그인하는 사용자를 인증하도록 구성할 수 있습니다. 자세한 내용은 사용자의 외부 LDAP 인증 구성, 25-40페이지 항목을 참조하십시오.
- **스팸 격리의 최종 사용자 인증**. 사용자가 최종 사용자 격리에 로그인할 때 사용자를 검증하도록 어플라이언스를 구성할 수 있습니다. 자세한 내용은 스팸 격리의 최종 사용자 인증, 25-42페이지 항목을 참조하십시오.
- **스팸 격리의 별칭 통합**. 스팸에 대한 이메일 알림을 사용할 경우, 이 쿼리는 최종 사용자가 각각의 별칭 이메일 주소에 대한 격리 통지를 수신하지 않도록 최종 사용자 별칭을 통합합니다. 자세한 내용은 스팸 격리의 별칭 통합 쿼리, 25-44페이지 항목을 참조하십시오.
- **사용자 고유 이름.** DLP(데이터 유출 방지)를 위해 RSA Enterprise Manager를 사용하는 경우, 이 쿼리는 DLP 위반 사항을 포함하는 메시지의 발신자에 대한 고유 이름을 검색합니다. Email Security 어플라이언스는 DLP 인시던트 데이터를 Enterprise Manager에 전송할 때 고유 이름을 포함합니다. 자세한 내용은 RSA Enterprise Manager에 대한 발신자의 사용자 고유 이름 식별, 25-45페이지 항목을 참조하십시오.

LDAP가 AsyncOS와 작업하는 방식 이해

LDAP 디렉토리를 작업할 때 어플라이언스에 LDAP 디렉토리 서버를 사용하여 수신자를 수락하고 메시지를 라우팅하며 헤더를 마스커레이드할 수 있습니다. LDAP 그룹 쿼리를 메시지 필터와 함께 사용하여 어플라이언스에서 메시지를 수신할 때 메시지를 처리하기 위한 규칙을 생성할 수 있습니다.

그림 25-1은 어플라이언스가 LDAP와 작업하는 방식을 보여줍니다.

그림 25-1 LDAP 구성



1. 전송 MTA는 SMTP를 통해 공용 리스너 "A"에 메시지를 전송합니다.
2. 어플라이언스는 System Administration(시스템 관리) > LDAP 페이지(또는 전역 `ldapconfig` 명령)에서 정의한 LDAP 서버를 쿼리합니다.

3. 데이터는 LDAP 디렉토리에서 수신되며 리스너에서 사용되고 System Administration(시스템 관리) > LDAP 페이지(또는 `ldapconfig` 명령)에 정의되어 있는 쿼리에 따라 다릅니다.
   - 메시지는 새로운 수신자 주소로 라우팅되거나 삭제 또는 바운스됨
   - 메시지는 새로운 수신자의 적절한 메일 호스트로 라우팅됨
   - From:, To: 및 CC: 메시지 헤더는 쿼리에 따라 재작성됨
   - `rcpt-to-group` 또는 `mail-from-group` 메시지 필터 규칙에 따라 정의된 추가 작업(구성된 그룹 쿼리와 함께 사용됨)

참고 다중 LDAP 서버에 연결하기 위해 어플라이언스를 구성할 수 있습니다. 이때 부하 균형 또는 장애 조치를 위해 LDAP 프로파일 설정을 구성할 수 있습니다. 다중 LDAP 서버와의 작업에 대한 자세한 정보는 다중 LDAP 서버와 동작하도록 AsyncOS 구성, 25-46페이지 항목을 참조하십시오.

LDAP 서버와 작업하도록 Cisco IronPort 어플라이언스 구성

LDAP 디렉토리와 작업하도록 어플라이언스를 구성하는 경우 다음 단계를 수행하여 수락, 라우팅, 앨리어싱 및 마스커레이드가 가능하도록 AsyncOS 어플라이언스를 구성해야 합니다.

절차

1단계 **LDAP 서버 프로파일을 구성합니다.** 서버 프로파일에는 AsyncOS의 LDAP 서버 연결에 필요한 다음 정보가 포함되어 있습니다.
- 쿼리를 전송하는 서버 및 포트의 이름
- 기본 DN
- 서버에 바인딩하기 위한 인증 요구 사항

서버 프로파일 구성에 대한 자세한 내용은 LDAP 서버 정보를 저장하도록 LDAP 서버 프로파일 생성, 25-5페이지 항목을 참조하십시오.

LDAP 서버 프로파일을 구성할 때, 하나 또는 다중 LDAP 서버에 연결하도록 AsyncOS를 구성할 수 있습니다.

다중 서버에 연결하는 AsyncOS에 대한 자세한 내용은 다중 LDAP 서버와 동작하도록 AsyncOS 구성, 25-46페이지 항목을 참조하십시오.

2단계 **LDAP 쿼리를 구성합니다.** LDAP 서버 프로파일에서 LDAP 쿼리를 구성합니다. 구성된 쿼리는 특정 LDAP 구현 및 스키마에 맞게 맞춤화되어야 합니다.

생성할 수 있는 LDAP 쿼리 유형에 대한 자세한 내용은 LDAP 쿼리 이해, 25-2페이지 항목을 참조하십시오.

쿼리 작성에 대한 자세한 내용은 LDAP 쿼리를 통한 작업, 25-12페이지 항목을 참조하십시오.

3단계 **공용 리스너 또는 개인 리스너에서 LDAP 서버 프로파일을 활성화합니다.** 메시지를 수락, 라우팅 또는 전송할 때 리스너에서 LDAP 쿼리를 실행하도록 지시하려면 리스너에서 LDAP 서버 프로파일을 활성화해야 합니다.

자세한 내용은 특정 리스너에서 실행되도록 LDAP 쿼리 활성화, 25-6페이지 항목을 참조하십시오.

참고 그룹 쿼리를 구성할 때, LDAP 서버와 작업하도록 AsyncOS를 구성하려면 추가 단계를 수행해야 합니다. 그룹 쿼리 구성에 대한 자세한 내용은 그룹 LDAP 쿼리를 사용하여 수신자가 그룹 멤버인지 판별, 25-23페이지 항목을 참조하십시오. 최종 사용자 인증 또는 스팸 알림 통합 쿼리를 구성하는 경우, 스팸 격리에 대한 LDAP 최종 사용자 액세스를 활성화해야 합니다. 스팸 격리에 대한 자세한 내용은 스팸 격리 장을 참조하십시오.

LDAP 서버 정보를 저장하도록 LDAP 서버 프로파일 생성

LDAP 디렉토리를 사용하도록 AsyncOS를 구성할 때 LDAP 서버 정보를 저장하도록 LDAP 서버 프로파일을 생성할 수 있습니다.

절차

1단계 System Administration(시스템 관리) > LDAP 페이지에서 **Add LDAP Server Profile(LDAP 서버 프로파일 추가)**을 클릭합니다.

2단계 서버 프로파일의 이름을 입력합니다.

3단계 LDAP 서버의 호스트 이름을 입력합니다.

다중 호스트 이름을 입력하여 장애 조치 또는 부하 균형이 가능하도록 LDAP 서버를 구성할 수 있습니다. 항목이 여러 개인 경우 쉼표로 구분합니다. 자세한 내용은 다중 LDAP 서버와 동작하도록 AsyncOS 구성, 25-46페이지 항목을 참조하십시오.

4단계 인증 방법을 선택합니다. 익명 인증을 사용하거나 사용자 이름 및 비밀번호를 지정할 수 있습니다.

5단계 LDAP 서버 유형을 Active Directory, OpenLDAP, Unknown 또는 Other 중에서 선택합니다.

6단계 포트 번호를 입력합니다.

기본 포트는 3268입니다. 이 포트는 Active Directory의 기본 포트로서 다중 서버 환경에서 전역 카탈로그에 액세스할 수 있습니다.

7단계 LDAP 서버의 기본 DN(고유 이름)을 입력합니다.

사용자 이름 및 비밀번호를 사용하여 인증하는 경우, 사용자 이름은 비밀번호를 포함하는 항목의 전체 DN을 포함해야 합니다. 예를 들어, 사용자가 joe@example.com 이메일 주소를 사용하는 마케팅 그룹의 멤버라면, 이 사용자의 항목은 다음과 같습니다.

```
uid=joe, ou=marketing, dc=example dc=com
```

8단계 LDAP 서버와 통신할 경우 SSL을 사용할지 여부를 선택합니다.

9단계 Advanced(고급)에서, 캐시 TTL(Time to Live)을 입력합니다. 이 값은 캐시가 보관되는 시간을 나타냅니다.

10단계 보관되는 최대 캐시 항목 수를 입력합니다.

참고 이 캐시는 LDAP 서버를 기준으로 유지됩니다. 하나 이상의 LDAP 서버를 구성하는 경우, 성능 향상을 위해 작은 LDAP 캐시 값을 설정해야 합니다. 또한 어플라이언스에서 다양한 프로세스로 인한 메모리 사용량이 높은 경우, 이 값을 늘리면 시스템 성능이 저하될 수 있습니다.

11단계 최대 동시 연결 수를 입력합니다.

부하 균형에 대한 LDAP 서버 프로파일을 구성하는 경우, 동시 연결은 나열된 LDAP 서버 간에 분배됩니다. 예를 들어, 동시 연결 10개를 구성하고 서버 3개에 대해 연결의 부하 균형을 조정하는 경우, AsyncOS는 각 서버에 연결 10개(총 30개의 연결)를 생성합니다.

참고 최대 동시 연결 수에는 LDAP 쿼리에 사용되는 LDAP 연결이 포함됩니다. 그러나 어플라이언스는 스팸 격리에 대해 LDAP 인증을 사용하는 경우 추가 연결을 열 수 있습니다.

12단계 **Test Server(s)(서버 테스트)** 버튼을 클릭하여 서버에 대한 연결을 테스트합니다. 다중 LDAP 서버를 지정한 경우, 모든 서버가 테스트됩니다. 테스트 결과는 Connection Status(연결 상태) 필드에 나타납니다. 자세한 내용은 LDAP 서버 테스트, 25-6페이지 항목을 참조하십시오.

13단계 확인란을 선택하고 해당 필드를 완료하여 쿼리를 생성합니다. 수락, 라우팅, 마스커레이드, 그룹, SMTP 인증, 외부 인증, 스팸 격리의 최종 사용자 인증 및 스팸 격리의 별칭 통합을 선택할 수 있습니다.

참고 메시지를 수신하거나 전송할 때 어플라이언스가 LDAP 쿼리를 실행하려면 해당 리스너에서 LDAP 쿼리를 활성화합니다. 자세한 내용은 특정 리스너에서 실행되도록 LDAP 쿼리 활성화, 25-6페이지 항목을 참조하십시오.

14단계 **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 변경하는 경우 **Update(업데이트)**를 클릭합니다. 자세한 내용은 LDAP 쿼리 테스트, 25-17페이지 항목을 참조하십시오.

참고 비밀번호가 비어 있는 상태에서 바인딩을 허용하도록 LDAP 서버를 구성한 경우, 쿼리는 비밀번호 필드가 비어 있는 상태로 테스트를 통과할 수 있습니다.

15단계 변경사항을 제출하고 커밋합니다.

참고 서버 구성 횟수에는 제한이 없지만, 서버당 수신자 수락, 라우팅, 마스커레이드 및 그룹 쿼리는 하나씩만 구성할 수 있습니다.

LDAP 서버 테스트

Add LDAP Server Profile(LDAP 서버 프로파일 추가) 또는 Edit LDAP Server Profile(LDAP 서버 프로파일 편집) 페이지에서 **Test Server(s)(서버 테스트)** 버튼(또는 CLI의 `ldapconfig` 명령의 `test` 하위 명령)을 사용하여 LDAP 서버에 대한 연결을 테스트합니다. AsyncOS에는 서버 포트에 대한 연결이 성공 또는 실패되었는지 알리는 메시지가 표시됩니다. 다중 LDAP 서버를 구성한 경우, AsyncOS는 각 서버를 테스트하고 개별 결과를 표시합니다.

특정 리스너에서 실행되도록 LDAP 쿼리 활성화

메시지를 수신하거나 전송할 때 어플라이언스가 LDAP 쿼리를 실행하려면 해당 리스너에서 LDAP 쿼리를 활성화합니다.

관련 주제

- LDAP 쿼리의 전역 설정 구성, 25-7페이지
- LDAP 서버 프로파일 생성 예, 25-7페이지
- 공용 리스너에서 LDAP 쿼리 활성화, 25-8페이지
- 개인 리스너에서 LDAP 쿼리 활성화, 25-9페이지

LDAP 쿼리의 전역 설정 구성

LDAP 전역 설정은 어플라이언스가 모든 LDAP 트래픽을 처리하는 방법을 정의합니다.

절차

1단계 System Administration(시스템 관리) > LDAP 페이지에서 **Edit Settings(설정 편집)**를 클릭합니다.

2단계 LDAP 트래픽에 사용할 IP 인터페이스를 선택합니다. 기본적으로 어플라이언스는 인터페이스를 자동으로 선택합니다.

3단계 LDAP 인터페이스에 사용할 TLS 인증서를 선택합니다(Network(네트워크) > Certificates(인증서) 페이지 또는 CLI의 `certconfig` 명령을 사용하여 추가된 TLS 인증서는 목록에 표시됩니다. 자세한 내용은 다른 MTA와의 통신 암호화에 대한 개요, 23-1페이지 참조).

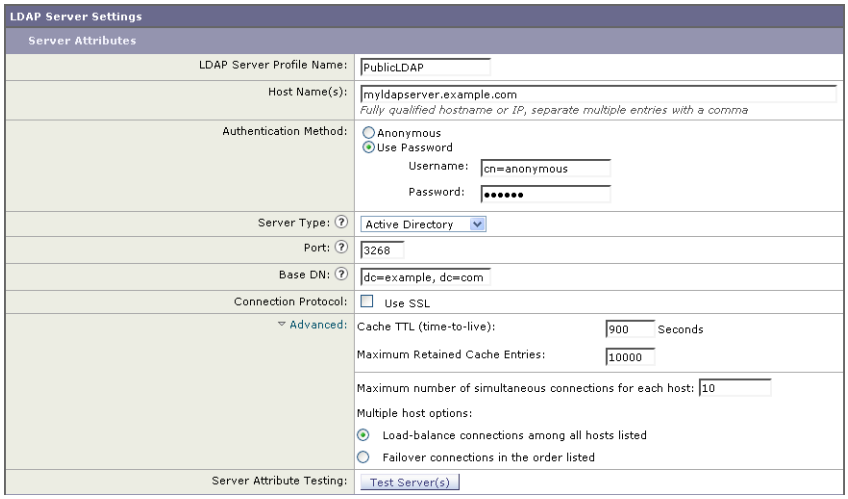
4단계 변경사항을 제출하고 커밋합니다.

LDAP 서버 프로파일 생성 예

다음 예에서는 System Administration(시스템 관리) > LDAP 페이지에서 어플라이언스가 바인드되도록 LDAP 서버를 정의하고 수신자 수락, 라우팅 및 마스커레이드를 수행하도록 쿼리를 구성합니다.

참고 LDAP 연결(DNS 조회, 연결 자체 및 해당되는 경우 어플라이언스 자체에 대한 인증 바인딩 포함)에 대한 60초의 연결 시도 시간제한이 있습니다. 첫 번째 시도에 실패하면 AsyncOS는 바로 동일한 서버에 있는 다른 호스트로 연결을 시도합니다(쉼표로 구분된 목록에 하나 이상의 호스트를 지정한 경우). 서버에 호스트가 하나만 있는 경우 AsyncOS는 계속해서 이 호스트로 연결을 시도합니다.

그림 25-2 LDAP 서버 프로파일 구성(2개중 1개)



먼저, "PublicLDAP"이라는 별칭이 `myldapserver.example.com`의 LDAP 서버에 지정됩니다. 연결 수가 10개(기본값)로 설정되고 다중 LDAP 서버(호스트)의 부하 균형 옵션이 기본값으로 유지됩니다. 이름의 쉼표로 구분된 목록을 제공하여 여러 호스트를 여기에서 지정할 수 있습니다. 쿼리는 포트 3268(기본값)로 디렉션됩니다. SSL은 이 호스트에 대한 연결 프로토콜로 활성화되지 않습니다. `example.com`의 기본 DN이 정의됩니다(`dc=example, dc=com`). 캐시 TTL(Time to Live)은 900초로 설정되며 캐시 항목의 최대 수는 10000개이고 인증 방법은 비밀번호로 설정됩니다.

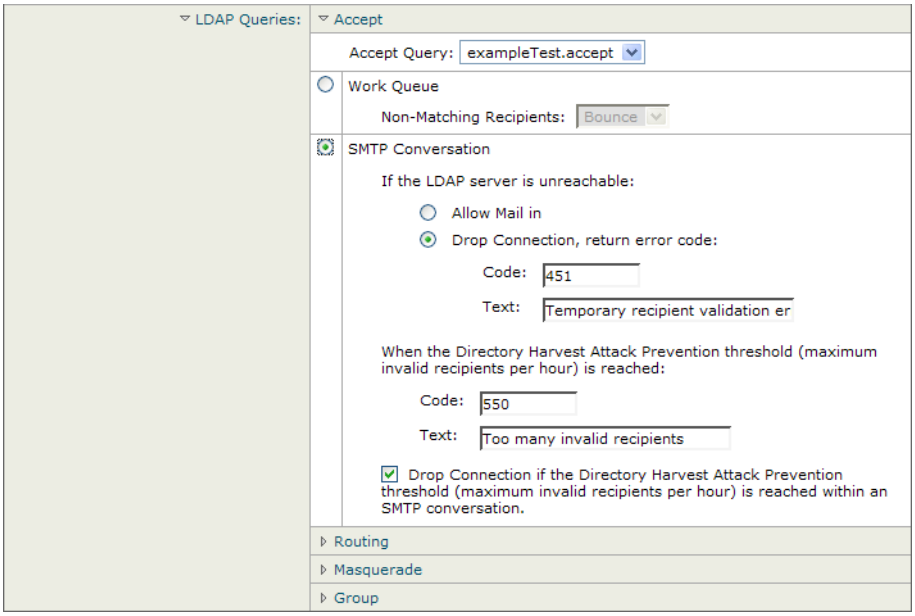
수신자 수락, 메일 라우팅 및 마스커레이드를 위한 쿼리가 정의됩니다. 쿼리 이름은 대소문자를 구분하며 올바른 결과를 반환하려면 정확하게 일치해야 합니다.

그림 25-3 LDAP 서버 프로파일 구성(2개중 2개)

공용 리스너에서 LDAP 쿼리 활성화

이 예에서, 공용 리스너 "InboundMail"이 수신자 수락을 위해 LDAP 쿼리를 사용하도록 업데이트됩니다. 또한, 수신자 수락이 SMTP 대화 중에 발생하도록 구성됩니다(자세한 내용은 수신자 검증에 수락 쿼리 사용, 25-19페이지 항목을 참조).

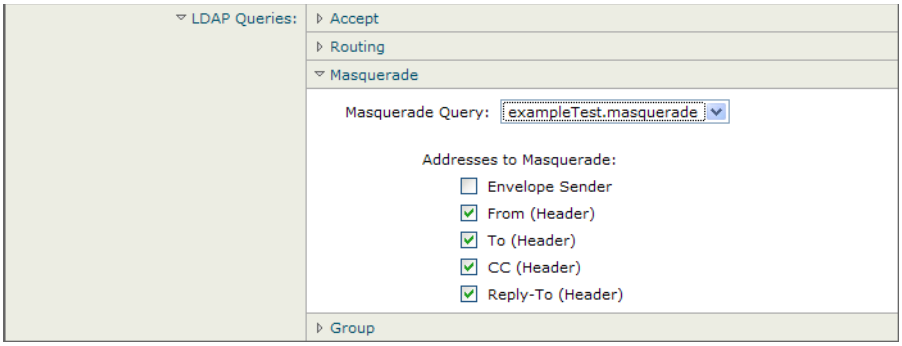
그림 25-4 리스너에서 수락 및 라우팅 쿼리 활성화



개인 리스너에서 LDAP 쿼리 활성화

이 예에서, 개인 리스너 "OutboundMail"이 마스커레이드를 위해 LDAP 쿼리를 사용하도록 업데이트됩니다. 마스커레이드한 필드에는 From, To, CC 및 Reply-To가 포함됩니다.

그림 25-5 리스너에서 마스커레이드 쿼리 활성화



Microsoft Exchange 5.5에 대한 지원 향상

AsyncOS에는 Microsoft Exchange 5.5를 지원하는 구성 옵션이 있습니다. Microsoft Exchange의 최신 버전을 사용 중인 경우 이 옵션을 활성화할 필요가 없습니다. LDAP 서버를 구성할 때 `ldapconfig -> edit -> server -> compatibility` 하위 명령(CLI에서만 사용 가능)에 "y"를 입력하여 Microsoft Exchange 5.5 지원을 활성화할 수 있습니다.

```
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 쿼리를 통한 작업

LDAP 쿼리의 유형별로 LDAP 서버 프로파일에서 항목을 생성합니다. LDAP 쿼리를 생성할 때, LDAP 서버에 대한 쿼리 구문을 입력해야 합니다. 쿼리를 구성할 때, 특히 디렉토리의 고유한 요구 사항에 맞게 새로운 객체 클래스 및 특성이 있는 디렉토리를 확장한 경우 LDAP 디렉토리 서비스의 구현 방식에 따라 쿼리를 맞춤화하고 구체화해야 합니다.

관련 주제

- LDAP 쿼리 유형, 25-12페이지
- 기본 DN(고유 이름), 25-13페이지
- LDAP 쿼리 구문, 25-13페이지
- 보안 LDAP(SSL), 25-14페이지
- 라우팅 쿼리, 25-14페이지
- 클라이언트가 LDAP 서버에 익명으로 바인딩하도록 허용, 25-14페이지
- LDAP 쿼리 테스트, 25-17페이지
- LDAP 서버의 연결 문제 해결, 25-18페이지

LDAP 쿼리 유형

- **수락 쿼리**. 자세한 내용은 수신자 검증에 수락 쿼리 사용, 25-19페이지 항목을 참조하십시오.
- **라우팅 쿼리**. 자세한 내용은 라우팅 쿼리를 사용하여 여러 대상 주소로 메일 전송, 25-20페이지 항목을 참조하십시오.
- **인증서 인증 쿼리.** 자세한 내용은 클라이언트 인증서의 유효성 검사, 26-51페이지 항목을 참조하십시오.
- **마스커레이드 쿼리**. 자세한 내용은 마스커레이드 쿼리를 사용하여 봉투 발신자 재작성, 25-21페이지 항목을 참조하십시오.
- **그룹 쿼리**. 자세한 내용은 그룹 LDAP 쿼리를 사용하여 수신자가 그룹 멤버인지 판별, 25-23페이지 항목을 참조하십시오.
- **도메인 기반 쿼리**. 자세한 내용은 도메인 기반 쿼리를 사용하여 특정 도메인으로 라우팅, 25-26페이지 항목을 참조하십시오.
- **체인 쿼리**. 자세한 내용은 체인 쿼리를 사용하여 일련의 LDAP 쿼리 수행, 25-28페이지 항목을 참조하십시오.

또한 다음 목적을 위해 쿼리를 구성할 수 있습니다.

- **디렉토리 수집 방지**. 자세한 내용은 LDAP 쿼리 이해, 25-2페이지 항목을 참조하십시오.
- **SMTP 인증.** 자세한 내용은 SMTP 인증을 위한 AsyncOS 구성, 25-32페이지 항목을 참조하십시오.

- **외부 인증.** 자세한 내용은 사용자의 외부 LDAP 인증 구성, 25-40페이지 항목을 참조하십시오.
- **스팸 격리의 최종 사용자 인증 쿼리.** 자세한 내용은 스팸 격리의 최종 사용자 인증, 25-42페이지 항목을 참조하십시오.
- **스팸 격리의 별칭 통합 쿼리.** 자세한 내용은 스팸 격리의 별칭 통합 쿼리, 25-44페이지 항목을 참조하십시오.

지정한 검색 쿼리는 시스템에서 구성한 모든 리스너가 사용할 수 있습니다.

기본 DN(고유 이름)

디렉토리의 루트 레벨을 기본이라고 합니다. 기본의 이름은 DN(고유 이름)입니다. Active Directory(및 RFC 2247에 따른 표준)의 기본 DN 형식에는 도메인 구성 요소(dc=)로 변환된 DNS 도메인이 있습니다. 예를 들어, example.com의 기본 DN은 dc=example, dc=com입니다. DNS 이름의 각 부분은 순서대로 표시됩니다. 이 내용은 구성 시 LDAP 설정에 반영되지 않을 수 있습니다.

디렉토리에 여러 도메인이 포함된 경우, 쿼리에 단일 BASE(기본)를 입력하는 것이 불편할 수 있습니다. 이 경우, LDAP 서버 설정을 구성할 때 기본을 NONE으로 설정합니다. 그러나 이렇게 설정하면 검색 시 효율성이 낮아집니다.

LDAP 쿼리 구문

LDAP 경로에는 공백이 허용되며 따옴표를 사용할 필요가 없습니다. CN과 DC 구문은 대소문자를 구분하지 않습니다.

```
Cn=First Last,oU=user,dc=domain,DC=COM
```

쿼리에 입력한 변수 이름은 *대소문자를 구분*하며 제대로 동작하려면 LDAP 구현 방식과 일치해야 합니다. 예를 들어, 프롬프트에 **mailLocalAddress**를 입력하면 **maillocaladdress**와는 다르게 쿼리를 수행합니다.

관련 주제

- 토큰, 25-13페이지

토큰

LDAP 쿼리에서 다음 토큰을 사용할 수 있습니다.

- {a} username@domainname
- {d} 도메인 이름
- {dn} 고유 이름
- {g} 그룹 이름
- {u} 사용자 이름
- {f} MAIL FROM: 주소

참고 {f} 토큰은 수락 쿼리에만 유효합니다.

예를 들어, 다음 쿼리를 사용하여 Active Directory LDAP 서버에 대한 메일을 수락할 수 있습니다.

(|(mail={a})(proxyAddresses=smtp:{a}))

참고 Cisco Systems에서는 LDAP 페이지(또는 `ldapconfig` 명령의 `test` 하위 명령)의 테스트 기능을 통해 구성한 모든 쿼리를 테스트하고 리스너에서 LDAP 기능을 활성화하기 *전*에 예상되는 결과가 반환되는지 확인하는 것이 좋습니다. 자세한 내용은 LDAP 쿼리 테스트, 25-17페이지 항목을 참조하십시오.

보안 LDAP(SSL)

LDAP 서버와 통신할 때 SSL을 사용하도록 AsyncOS에 지시할 수 있습니다. SSL을 사용하도록 LDAP 서버 프로파일을 구성한 경우 다음과 같이 동작합니다.

- AsyncOS는 LDAPS 인증서(CLI의 `certconfig` 명령을 사용하여 구성)를 사용합니다(GUI를 사용하여 자체 서명된 인증서 생성, 23-3페이지 참조).

  LDAPS 인증서 사용을 지원하도록 LDAP 서버를 구성할 수 있습니다.
- LDAPS 인증서가 구성되지 않은 경우, AsyncOS는 데모 인증서를 사용합니다.

라우팅 쿼리

LDAP 라우팅 쿼리에는 반복에 대한 제한이 없습니다. 라우팅은 완벽하게 데이터 기반으로 이루어집니다. 그러나 AsyncOS는 순환 참조 데이터를 확인하여 라우팅이 무한 루핑되지 않도록 합니다.

클라이언트가 LDAP 서버에 익명으로 바인딩하도록 허용

익명 쿼리를 허용하도록 LDAP 디렉토리 서버를 구성할 수 있습니다. (즉 클라이언트가 서버에 익명으로 바인딩되고 쿼리를 수행할 수 있습니다.) 익명 쿼리를 허용하도록 Active Directory를 구성하는 데 대한 자세한 지침은 다음 URL에 있는 "Microsoft 기술 자료 기사 - 320528"을 참조하십시오.

```
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320528
```

또는 임의의 클라이언트에서 익명 쿼리에 대한 LDAP 디렉토리 서버를 여는 대신 오직 쿼리 인증 및 수행을 위해 "사용자" 한 명을 구성할 수 있습니다.

이 단계에 대한 요약은 특히 다음에서 자세히 설명되어 있습니다.

- Microsoft Exchange 2000 서버에서 "익명" 인증을 허용하도록 설정하는 방법.
- Microsoft Exchange 2000 서버에서 "익명 바인딩"을 허용하도록 설정하는 방법.
- AsyncOS가 "익명 바인딩" 및 "익명" 인증을 모두 사용하여 Microsoft Exchange 2000 서버에서 LDAP 데이터를 검색하도록 설정하는 방법.

사용자 이메일 주소를 쿼리하기 위해 "익명" 또는 "익명 바인딩" 인증을 허용하도록 Microsoft Exchange 2000 서버에 특정한 권한을 부여해야 합니다. 이 방법은 LDAP 쿼리를 사용하여 SMTP 게이트웨이에 수신되는 이메일 메시지의 유효성을 판별할 때 매우 유용합니다.

관련 주제

- 익명 인증 설정, 25-15페이지
- Active Directory의 익명 바인딩 설정, 25-16페이지
- Active Directory 구현을 위한 참고 사항, 25-17페이지

익명 인증 설정

다음 설정 지침을 사용하여 Microsoft Windows Active Directory에서 Active Directory 및 Exchange 2000 서버의 인증되지 않은 쿼리에 특정한 데이터를 사용하도록 설정할 수 있습니다. Active Directory에서 "익명 바인딩"을 허용하려면 Active Directory의 익명 바인딩 설정, 25-16페이지 항목을 참조하십시오.

절차

1단계 필요한 Active Directory 권한을 확인합니다.

ADSI 편집 스냅인 또는 LDP 유틸리티를 사용하여 다음 Active Directory 객체의 특성에 대한 권한을 수정해야 합니다.

- 쿼리를 생성할 도메인의 도메인 명명 컨텍스트의 루트.
- 이메일 정보를 쿼리할 사용자를 포함하는 모든 OU 및 CN 객체.

다음 표는 필요한 모든 컨테이너에 적용할 필수 권한을 보여줍니다.

사용자 객체	권한	상속	권한 유형
모든 사람	콘텐츠 나열	컨테이너 객체	객체
모든 사람	콘텐츠 나열	조직 구성 단위	객체
모든 사람	공개 정보 읽기	사용자 객체	속성
모든 사람	전화 및 메일 옵션 읽기	사용자 객체	속성

2단계 Active Directory 권한을 설정합니다.

- ADSI 편집 양식인 Windows 2000 지원 툴을 엽니다.
- **Domain Naming Context(도메인 명명 컨텍스트)** 폴더의 위치를 찾습니다. 이 폴더에는 도메인의 LDAP 경로가 있습니다.
- **Domain Naming Context(도메인 명명 컨텍스트)** 폴더를 마우스 오른쪽 버튼으로 클릭한 다음 **Properties(속성)**를 클릭합니다.
- **Security(보안)**를 클릭합니다.
- **Advanced(고급)**를 클릭합니다.
- **Add(추가)**를 클릭합니다.
- **User Object(사용자 객체)**를 클릭한 다음 **OK(확인)**를 클릭합니다.
- **Permission Type(권한 유형)** 탭을 클릭합니다.
- **Apply onto(적용 대상)** 상자에서**Inheritance(상속)**를 클릭합니다.
- **Permission(권한)**에 대한 Allow(허용) 확인란을 선택합니다.

3단계 CiscoMessaging Gateway(메시지 게이트웨이)를 구성합니다.

CLI(Command Line Interface)에서 `ldapconfig`를 사용하여 다음 정보가 포함된 LDAP 서버 항목을 생성합니다.

- Active Directory 또는 Exchange 서버의 호스트 이름
- 포트 3268
- 도메인의 루트 명명 컨텍스트와 일치하는 기본 DN
- 익명 인증 유형

Active Directory의 익명 바인딩 설정

다음 설정 지침을 사용하여 Microsoft Windows Active Directory에서 Active Directory 및 Exchange 2000 서버의 익명 바인딩 쿼리에 특정한 데이터를 사용하도록 설정할 수 있습니다. Active Directory 서버의 익명 바인딩을 통해 비밀번호가 비어 있는 사용자 이름 `anonymous`를 전송합니다.

참고 익명 바인딩을 시도하는 중에 비밀번호가 Active Directory 서버에 전송되는 경우 인증에 실패할 수 있습니다.

절차

1단계 필요한 Active Directory 권한을 확인합니다.

ADSI 편집 스냅인 또는 LDP 유틸리티를 사용하여 다음 Active Directory 객체의 특성에 대한 권한을 수정해야 합니다.

- 쿼리를 생성할 도메인의 도메인 명명 컨텍스트의 루트.
- 이메일 정보를 쿼리할 사용자를 포함하는 모든 OU 및 CN 객체.

다음 표는 필요한 모든 컨테이너에 적용할 필수 권한을 보여줍니다.

사용자 객체	권한	상속	권한 유형
익명 로그온	콘텐츠 나열	컨테이너 객체	객체
익명 로그온	콘텐츠 나열	조직 구성 단위	객체
익명 로그온	공개 정보 읽기	사용자 객체	속성
익명 로그온	전화 및 메일 옵션 읽기	사용자 객체	속성

2단계 Active Directory 권한을 설정합니다.

- ADSI 편집 양식인 Windows 2000 지원 툴을 엽니다.
- **Domain Naming Context(도메인 명명 컨텍스트)** 폴더의 위치를 찾습니다. 이 폴더에는 도메인의 LDAP 경로가 있습니다.
- **Domain Naming Context(도메인 명명 컨텍스트)** 폴더를 마우스 오른쪽 버튼으로 클릭한 다음 **Properties(속성)**를 클릭합니다.
- **Security(보안)**를 클릭합니다.
- **Advanced(고급)**를 클릭합니다.
- **Add(추가)**를 클릭합니다.
- **User Object(사용자 객체)** 익명 로그온을 클릭한 다음 **OK(확인)**를 클릭합니다.
- **Permission Type(권한 유형)** 탭을 클릭합니다.
- **Apply onto(적용 대상)** 상자에서 **Inheritance(상속)**를 클릭합니다.
- **Permission(권한)**에 대한 **Allow(허용)** 확인란을 선택합니다.

3단계 CiscoMessaging Gateway(메시지 게이트웨이)를 구성합니다.

System Administration(시스템 관리) > LDAP 페이지(또는 CLI의 `ldapconfig` 명령)에서 다음 정보가 포함된 LDAP 서버 항목을 생성합니다.

- Active Directory 또는 Exchange 서버의 호스트 이름
- 포트 3268

  - 도메인의 루트 명명 컨텍스트와 일치하는 기본 DN
  - `cn=anonymous`를 비밀번호가 비어 있는 사용자로 사용하는 인증 유형 비밀번호

Active Directory 구현을 위한 참고 사항

- Active Directory 서버는 포트 3268 및 389에서 LDAP 연결을 수락합니다. 전역 카탈로그 액세스를 위한 기본 포트는 포트 3268입니다.
- Active Directory 서버는 포트 636 및 3269에서 LDAPS 연결을 수락합니다. Microsoft는 Windows Server 2003 이상 버전에서 LDAPS를 지원합니다.
- 동일한 서버를 사용하는 다양한 기반에서 쿼리를 수행할 수 있도록 어플라이언스는 전역 카탈로그인 도메인 컨트롤러에 연결해야 합니다.
- Active Directory 내에서 쿼리에 성공하려면 그룹 "Everyone(모든 사람)"에 대한 읽기 권한을 디렉토리 객체에 부여해야 합니다. 여기에는 도메인 명명 컨텍스트의 루트가 포함됩니다.
- 일반적으로, 대부분의 Active Directory 구현에서 `mail` 특성 항목의 값으로 일치하는 값인 "ProxyAddresses" 특성 항목을 갖습니다.
- 인프라 내에서 서로를 인식하는 Microsoft Exchange 환경은 일반적으로 시작 MTA로 다시 라우팅하지 않고 상호 간에 메일을 라우팅할 수 있습니다.

LDAP 쿼리 테스트

AAdd LDAP Server Profile(LDAP 서버 프로파일 추가) 또는 Edit LDAP Server Profile(LDAP 서버 프로파일 편집) 페이지(또는 CLI의 `test` 하위 명령)의 Test Query(쿼리 테스트) 버튼을 사용하여 구성한 LDAP 서버에 대한 쿼리를 쿼리 유형마다 테스트합니다. AsyncOS는 결과와 함께 쿼리 연결 테스트의 각 단계에 대한 세부 정보도 표시합니다. 각 쿼리 유형에 대해 테스트할 수 있습니다.

`ldaptest` 명령은 배치 명령을 사용하여 사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
ldaptest LDAP.ldapaccept foo@ironport.com
```

LDAP 서버 특성의 Host Name(호스트 이름) 필드에 다중 호스트를 입력한 경우, 어플라이언스는 각 LDAP 서버에 대한 쿼리를 테스트합니다.

표 25-1 LDAP 쿼리 테스트

쿼리 유형	수신자가 일치하는 경우(통과)	수신자가 일치하지 않는 경우(실패)
수신자 수락(수락, `ldapaccept`)	메시지를 수락합니다.	올바르지 않은 수신자: 리스너 설정에 따라 대화 또는 지연된 바운스를 수행하거나 메시지를 삭제. DHAP: 삭제.
라우팅 **(라우팅, `ldaprouting`)**	쿼리 설정에 따라 라우팅합니다.	메시지 처리를 계속합니다.
마스커레이드(마스커레이드, `masquerade`)	쿼리에서 정의한 변수 매핑으로 헤더를 변경합니다.	메시지 처리를 계속합니다.
그룹 멤버십(그룹, `ldapgroup`)	메시지 필터 규칙에 대해 "true"를 반환합니다.	메시지 필터 규칙에 대해 "false"를 반환합니다.

표 25-1 LDAP 쿼리 테스트 (계속)

쿼리 유형	수신자가 일치하는 경우(통과)	수신자가 일치하지 않는 경우(실패)
SMTP 인증 **(SMTP 인증, `smtpauth`)**	비밀번호가 LDAP 서버에서 반환되어 인증에 사용되며 SMTP 인증이 수행됩니다.	비밀번호가 일치하지 않으면 SMTP 인증에 실패합니다.
외부 인증 **(`externalauth`)**	개별적으로 바인딩, 사용자 레코드 및 사용자 그룹 멤버십에 대해 "match positive"를 반환합니다.	개별적으로 바인딩, 사용자 레코드 및 사용자 그룹 멤버십에 대해 "match negative"를 반환합니다.
스팸 격리의 최종 사용자 인증(`isqauth`)	최종 사용자 계정에 대해 "match positive"를 반환합니다.	비밀번호가 일치하지 않으면 최종 사용자 인증에 실패합니다.
스팸 격리의 별칭 통합 **(`isqalias`)**	통합된 스팸 알림을 전송할 대상 이메일 주소를 반환합니다.	스팸 알림은 통합되지 않습니다.

참고 쿼리에 입력한 변수 이름은 *대소문자를 구분*하며 제대로 동작하려면 LDAP 구현 방식과 일치해야 합니다. 예를 들어, 프롬프트에 **`mailLocalAddress`**를 입력하면 **`maillocaladdress`**와는 다르게 쿼리를 수행합니다. Cisco Systems에서 구성한 모든 쿼리 테스트하고 올바른 결과가 반환되도록 보장하기 위해 `ldapconfig` 명령의 `test` 하위 명령을 사용하는 것이 좋습니다.

LDAP 서버의 연결 문제 해결

어플라이언스에서 LDAP 서버에 연결할 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 구성 시 잘못된 포트를 입력했거나 포트가 방화벽에서 열리지 않는 경우 서버에 연결할 수 없습니다. LDAP 서버는 일반적으로 포트 3268 또는 389를 통해 통신합니다. Active Directory는 포트 3268을 사용하여 다중 서버 환경에서 사용되는 전역 카탈로그에 액세스합니다(자세한 내용은 "방화벽 정보" 부록 참조). AsyncOS 4.0에는 SSL을 통해(일반적으로 포트 636을 통해) LDAP 서버와 통신하는 기능이 추가되었습니다. 자세한 내용은 보안 LDAP(SSL), 25-14페이지 항목을 참조하십시오.

입력한 호스트 이름을 확인할 수 없어 서버에 연결할 수 없는 경우도 있습니다.

Add LDAP Server Profile(LDAP 서버 프로파일 추가) 또는 Edit LDAP Server Profile(LDAP 서버 프로파일 편집) 페이지에서 **Test Server(s)(서버 테스트)**(또는 CLI의 `ldapconfig` 명령의 `test` 하위 명령)를 사용하여 LDAP 서버에 대한 연결을 테스트합니다. 자세한 내용은 LDAP 서버 테스트, 25-6페이지 항목을 참조하십시오.

LDAP 서버에 연결할 수 없는 경우,

- LDAP 수락, 마스커레이드 또는 라우팅이 작업 큐에서 활성화되어 있는 경우, 메일이 작업 큐에 남아 있습니다.
- LDAP 수락이 활성화되어 있지 않지만 다른 쿼리(그룹 정책 검사 등)가 필터에서 사용되는 경우 필터가 거짓으로 평가됩니다.

수신자 검증에 수락 쿼리 사용

기존 LDAP 인프라를 사용하여 수신 메시지(공용 리스너에 있음)의 수신자 이메일 주소를 처리하는 방식을 정의할 수 있습니다. 디렉토리에 대한 사용자 데이터의 변경사항은 다음에 어플라이언스가 디렉토리 서버를 쿼리할 때 업데이트됩니다. 어플라이언스가 검색하는 데이터를 저장하는 캐시의 크기 및 시간을 지정할 수 있습니다.

참고 특별한 수신자(예: `administrator@example.com`)에 대한 LDAP 수락 쿼리를 우회할 수 있습니다. RAT(Recipient Access Table)에서 이 설정을 구성할 수 있습니다. 이 설정의 구성에 대한 자세한 내용은 "이메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

관련 주제

- 수락 쿼리 샘플, 25-19페이지
- Lotus Notes에 대한 수락 쿼리 구성, 25-20페이지

수락 쿼리 샘플

표 25-2는 샘플 수락 쿼리를 보여줍니다.

표 25-2 일반적인 LDAP를 구현하는 LDAP 쿼리 문자열의 예: 수락

쿼리 대상:	수신자 검증

OpenLDAP	`(mailLocalAddress={a})`
	`(mail={a})`
	`(mailAlternateAddress={a})`

Microsoft Active Directory 주소록 **Microsoft Exchange**	`(|(mail={a})(proxyAddresses=smtp:{a}))`

SunONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

Lotus Notes **Lotus Domino**	`(|(|(mail={a})(uid={u}))(cn={u}))` `(|(ShortName={u})(InternetAddress={a})(FullName={u}))`

또한 사용자 이름(왼쪽)을 검증할 수 있습니다. 이 방법은 디렉토리에 메일을 수락한 모든 도메인이 포함되지 않는 경우 유용합니다. 수락 쿼리를 (uid={u})로 설정합니다.

Lotus Notes에 대한 수락 쿼리 구성

LDAPACCEPT 및 Lotus Notes와 관련된 잠재적인 문제가 있습니다. Notes LDAP에 다음과 같은 특성을 지닌 사람이 포함되는 경우,

```
mail=juser@example.com

cn=Joe User

uid=juser

cn=123456

location=New Jersey
```

Lotus는 "Joe_User@example.com"과 같이 지정된 이메일 주소가 아닌 LDAP 디렉토리에 없는 다양한 형식의 이메일 주소로 오는 해당 사용자의 이메일을 수락합니다. 따라서 AsyncOS는 해당 사용자에 대한 모든 유효한 사용자 이메일 주소를 찾지 못할 수도 있습니다.

한 가지 가능한 해결책은 다른 형식의 주소를 게시하는 것입니다. 자세한 내용은 Lotus Notes 관리자에게 문의하십시오.

라우팅 쿼리를 사용하여 여러 대상 주소로 메일 전송

AsyncOS는 별칭 확장(여러 대상 주소로 LDAP 라우팅)을 지원합니다. AsyncOS는 원본 이메일 메시지를 별칭 대상마다 새로운 개별 메시지로 대체합니다(예: recipient@yoursite.com은 newrecipient1@hotmail.com 및 recipient2@internal.yourcompany.com으로 보내는 새로운 개별 메시지로 대체 가능). 라우팅 쿼리는 다른 메일 처리 시스템에서는 앨리어싱 쿼리라고도 합니다.

관련 주제

- 라우팅 쿼리 샘플, 25-21페이지

라우팅 쿼리 샘플

표 25-3 일반적인 LDAP를 구현하는 LDAP 쿼리 문자열의 예: 라우팅

쿼리 대상:	다른 메일 호스트로 라우팅
OpenLDAP	`(mailLocalAddress={a})`
Microsoft Active Directory 주소록 **Microsoft Exchange**	적용 불가능할 수 있음[a]

SunONE Directory Server	`(mail={a})`
	`(mailForwardingAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailRoutingAddress={a})`
	`(otherMailbox={a})`
	`(rfc822Mailbox={a})`

a. Active Directory 구현에는 `proxyAddresses` 특성에 여러 항목이 포함될 수 있지만 AD는 이 특성 값을 `smtp:user@domain.com`으로 포맷하기 때문에 해당 데이터를 LDAP 라우팅/별칭 확장에 사용할 수 없습니다. 각 대상 주소는 개별 `attribute:value` 쌍에 포함되어야 합니다. 인프라 내에서 서로를 인식하는 Microsoft Exchange 환경은 일반적으로 시작 MTA로 다시 라우팅하지 않고 상호 간에 메일을 라우팅할 수 있습니다.

관련 주제

라우팅: MAILHOST 및 MAILROUTINGADDRESS, 25-21페이지

라우팅: MAILHOST 및 MAILROUTINGADDRESS

라우팅 쿼리의 경우, MAILHOST의 값으로 IP 주소가 올 수 없으며 반드시 확인 가능한 호스트 이름이 와야 합니다. 일반적으로 내부 DNSconfig를 사용해야 합니다.

MAILHOST는 라우팅 쿼리에 사용되는 선택사항입니다. MAILROUTINGADDRESS는 MAILHOST가 설정되지 않은 경우 필수사항입니다.

마스커레이드 쿼리를 사용하여 봉투 발신자 재작성

마스커레이드는 구성한 쿼리에 따라 봉투 발신자(발신자 또는 MAIL FROM이라고 함)와 To:, From: 및/또는 CC: 헤더를 재작성하는 기능입니다. 이 기능을 구현하는 일반적인 예로는 단일 사이트에서 여러 도메인을 호스팅할 수 있는 "가상 도메인"이 있습니다. 또 다른 일반적인 구현 방법은 이메일 헤더의 문자열에서 하위 도메인을 "제거"하여 네트워크 인프라를 "숨기기"하는 것입니다.

관련 주제

- 마스커레이드 쿼리 샘플, 25-22페이지
- "고유 이름" 마스커레이드, 25-22페이지

마스커레이드 쿼리 샘플

표 25-4 일반적인 LDAP를 구현하는 LDAP 쿼리 문자열의 예: 마스커레이드

쿼리 대상:	마스커레이드
OpenLDAP	`(mailRoutingAddress={a})`
Microsoft Active Directory 주소록	`(proxyaddresses=smtp:{a})`

SunONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

"고유 이름" 마스커레이드

일부 사용자 환경에서는, LDAP 디렉토리 서버 스키마는 메일 라우팅 주소 또는 로컬 메일 주소 외에 "고유 이름"을 저장할 수 있습니다. 고유 주소에 유효한 이메일 주소에 일반적으로 허용되지 않은 특수 문자가 포함되는 경우에도(예: 따옴표, 공백 및 쉼표) AsyncOS에서는 이 "고유 주소"를 사용하여 봉투 발신자(발송 메일) 및 메시지 헤더(수신 메일, 예를 들어 To:, Reply To:, From: 또는 CC:)를 마스커레이드할 수 있습니다.

LDAP 쿼리를 통해 헤더를 마스커레이드하는 경우, 고유 이메일의 전체 문자열을 LDAP 서버의 결과로 대체할지 여부를 구성하는 옵션을 사용할 수 있습니다. 이 동작이 활성화된 경우에도 user@domain 일부만 봉투 발신자(고유 이름은 올바르지 않음)에 사용됩니다.

일반적인 LDAP 마스커레이드와 마찬가지로 LDAP 쿼리를 통해 빈 결과(길이가 0이거나 전체 공백)가 반환되는 경우, 마스커레이드가 발생하지 않습니다.

이 기능을 활성화하려면 리스너에 대한 LDAP 기반 마스커레이드를 구성할 때(LDAP 페이지 또는 `ldapconfig` 명령) 다음 질문에 "y"를 입력합니다.

```
Do you want the results of the returned attribute to replace the entire
friendly portion of the original recipient? [N]
```

예를 들어, 다음 예의 LDAP 항목을 고려합니다.

특성	값
mailRoutingAddress	admin\@example.com
mailLocalAddress	joe.smith\@example.com
mailFriendlyAddress	"example.com 관리자", <joe.smith\@example.com>

이 기능이 활성화된 경우, LDAP 쿼리(mailRoutingAddress={a}) 및 마스커레이드 특성(mailLocalAddress)은 다음으로 대체됩니다.

원래 주소(From, To, CC, Reply-to)	마스커레이드 헤더	마스커레이드 봉투 발신자
admin@example.com	From: "example.com 관리자", <joe.smith@example.com>	MAIL FROM: <joe.smith@example.com>

그룹 LDAP 쿼리를 사용하여 수신자가 그룹 멤버인지 판별

수신자가 LDAP 디렉토리에서 정의한 대로 그룹의 멤버인지 판별하기 위해 LDAP 서버에 대한 쿼리를 정의할 수 있습니다.

절차

1단계 메시지에 적용할 `rcpt-to-group` 또는 `mail-from-group` 규칙을 사용하는 메시지 필터를 생성합니다.

2단계 그런 다음 System Administration(시스템 관리) > LDAP 페이지(또는 `ldapconfig` 명령)에서 어플라이언스가 바인딩할 LDAP 서버를 정의하고 그룹 멤버십에 대한 쿼리를 구성합니다.

3단계 Network(네트워크) > Listeners(리스너) 페이지(또는 `listenerconfig -> edit -> ldapgroup` 하위 명령)에서 리스너에 대한 그룹 쿼리를 활성화합니다.

관련 주제

- 그룹 쿼리 샘플, 25-23페이지
- 그룹 쿼리 구성, 25-23페이지
- 예: 그룹 쿼리를 사용하여 스팸 및 바이러스 검사 건너뛰기, 25-25페이지

그룹 쿼리 샘플

표 25-5 일반적인 LDAP를 구현하는 LDAP 쿼리 문자열의 예: 그룹

쿼리 대상:	그룹
OpenLDAP	OpenLDAP는 `memberOf` 특성을 기본적으로 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 들어, LDAP 디렉토리가 "마케팅" 그룹의 멤버를 `ou=Marketing`으로 분류하는 경우, 이 그룹의 멤버에게 전송된 메시지 또는 이 멤버가 전송한 메시지를 특별한 방식으로 처리할 수 있습니다. 1단계에서는 메시지에 적용할 메시지 필터를 생성하고 2단계 및 3단계에서는 LDAP 조회 메커니즘을 활성화합니다.

그룹 쿼리 구성

다음 예에서는 마케팅 그룹(LDAP 그룹 "마케팅"에서 정의한 대로)의 멤버가 보낸 메일은 대체 전달 호스트인 `marketingfolks.example.com`에 전달됩니다.

절차

1단계 먼저, 그룹 멤버십과 정확하게 일치하는 메시지에 적용할 메시지 필터가 생성됩니다. 이 예에서는 `mail-from-group` 규칙을 사용하는 필터를 생성합니다. 봉투 발신자가 LDAP 그룹 "marketing-group1" 소속인 모든 메시지는 대체 전달 호스트(필터 `alt-mailhost` 작업)를 통해 전달됩니다.

그룹 멤버십 필드 변수(groupName)는 2단계에서 정의됩니다. 그룹 특성인 "groupName"은 `marketing-group1` 값을 사용하여 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.

[]>
```

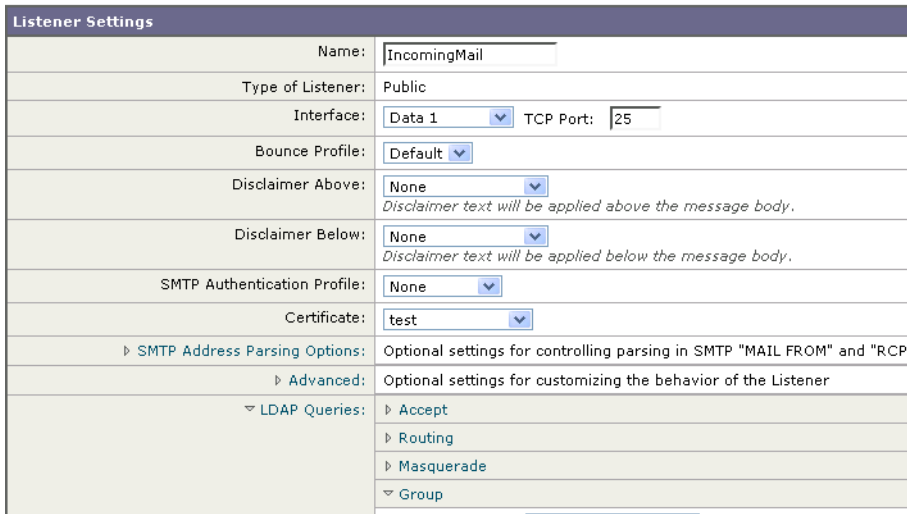
`mail-from-group` 및 `rcpt-to-group` 메시지 필터 규칙에 대한 자세한 내용은 메시지 필터 규칙, 9-2 페이지 항목을 참조하십시오.

2단계 다음으로, Add LDAP Server Profile(LDAP 서버 프로파일 추가) 페이지에서 어플라이언스가 바인딩할 LDAP 서버가 정의되고 그룹 멤버십을 위한 첫 번째 쿼리가 구성됩니다.

3단계 다음으로, 공용 리스너 "InboundMail"이 그룹 라우팅을 위해 LDAP 쿼리를 사용하도록 업데이트됩니다. Edit Listener(리스너 편집) 페이지를 사용하여 위에서 지정한 LDAP 쿼리를 활성화합니다.

이 쿼리의 결과로, 리스너에서 수락한 메시지는 그룹 멤버십을 판별하기 위해 LDAP 서버에 대한 쿼리를 트리거합니다. PublicLDAP2.group 쿼리는 System Administration(시스템 관리) > LDAP 페이지에서 이미 정의되었습니다.

그림 25-6 리스너에서 그룹 쿼리 지정



이 예에서 변경사항을 적용하기 위해 커밋해야 합니다.

예: 그룹 쿼리를 사용하여 스팸 및 바이러스 검사 건너뛰기

메시지 필터링은 파이프라인 초기에 발생하기 때문에 그룹 쿼리를 사용하여 지정된 그룹에 대한 바이러스 및 스팸 검사를 건너뛸 수 있습니다. 예를 들어, IT 그룹에서 모든 메시지를 수신하고 스팸 및 바이러스 검사를 건너뛸 수 있습니다. LDAP 레코드에서 DN을 그룹 이름으로 사용하는 그룹 항목을 생성합니다. 그룹 이름은 다음 DN 항목으로 구성됩니다.

cn=IT, ou=groups, o=sample.com

다음 그룹 쿼리를 통해 LDAP 서버 프로파일을 생성합니다.

(&(memberOf={g})(proxyAddresses=smtp:{a}))

그런 다음 리스너에서 이 쿼리를 활성화하면 리스너에서 메시지를 수신하는 경우 그룹 쿼리가 트리거됩니다.

IT 그룹의 멤버에 대한 바이러스 및 스팸 필터링을 건너뛰려면, LDAP 그룹을 대상으로 수신 메시지를 검사하는 다음 메시지 필터를 생성합니다.

```
- 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 입력한 DN(cn=IT, ou=groups, o=sample.com)을 반영합니다. 필터가 LDAP 디렉토리에 있는 이름과 일치하도록 메시지 필터에서 올바른 그룹 이름을 사용하는지 확인합니다.

리스너에서 수락한 메시지는 그룹 멤버십을 판별하기 위해 LDAP 서버에 대한 쿼리를 트리거합니다. 메시지 수신자가 IT 그룹의 멤버인 경우, 메시지 필터는 바이러스 및 스팸 검사를 모두 건너뛰고 메시지를 수신자에게 전달합니다. LDAP 쿼리 결과를 검사하도록 필터를 활성화하려면, LDAP 서버에서 LDAP 쿼리를 생성하고 리스너에서 LDAP 쿼리를 활성화해야 합니다.

도메인 기반 쿼리를 사용하여 특정 도메인으로 라우팅

도메인 기반 쿼리는 유형별로 그룹화된 LDAP 쿼리로, 도메인에 연결되고 특정 리스너에 할당됩니다. 다른 도메인에 연결된 다른 LDAP 서버가 있지만 동일한 리스너에서 모든 LDAP 서버에 대한 쿼리를 실행하려는 경우 도메인 기반 쿼리를 사용할 수 있습니다. 예를 들어, 회사 "MyCompany"는 "HisCompany" 및 "HerCompany"를 구매합니다. MyCompany는 해당 도메인인 MyCompany.example.com과 HisCompany.example.com 및 HerCompany.example.com 도메인을 유지하고 각 도메인과 연결된 직원을 위해 다른 LDAP 서버를 유지합니다. 이러한 도메인 3개가 모두 메일을 수락하기 위해 MyCompany가 도메인 기반 쿼리를 생성합니다. 이렇게 하면 MyCompany.example.com은 동일한 리스너에서 Mycompany.example.com, HisCompany.example.com 및 HerCompany.example.com에 대한 이메일을 수락할 수 있습니다.

절차

1단계 도메인 기반 쿼리에서 사용할 도메인마다 서버 프로파일을 생성합니다. 서버 프로파일마다 이 도메인 기반 쿼리(수락, 라우팅 등)에 사용할 쿼리를 구성합니다. 자세한 내용은 LDAP 서버 정보를 저장하도록 LDAP 서버 프로파일 생성, 25-5페이지 항목을 참조하십시오.

2단계 도메인 기반 쿼리를 생성합니다. 도메인 기반 쿼리를 생성할 때, 각 서버 프로파일에서 쿼리를 선택하고 어플라이언스가 Envelope To 필드에서 도메인에 기반하여 실행할 쿼리를 결정하도록 설정합니다. 쿼리 생성에 대한 자세한 내용은 도메인 기반 쿼리 생성, 25-27페이지 항목을 참조하십시오.

3단계 공용 또는 개인 리스너에서 도메인 기반 쿼리를 활성화합니다. 리스너 구성에 대한 자세한 내용은 "메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

참고 또한 LDAP 최종 사용자 액세스에 대한 도메인 기반 쿼리 또는 스팸 격리를 위한 스팸 알림을 활성화할 수 있습니다. 자세한 내용은 스팸 격리 장을 참조하십시오.

관련 주제

- 도메인 기반 쿼리 생성, 25-27페이지

도메인 기반 쿼리 생성

System Administration(시스템 관리) > LDAP > LDAP Server Profiles(LDAP 서버 프로파일) 페이지에서 도메인 기반 쿼리를 생성합니다.

절차

1단계 LDAP Server Profiles(LDAP 서버 프로파일) 페이지에서 **Advanced(고급)**를 클릭합니다.

2단계 **Add Domain Assignments(도메인 지정 추가)**를 클릭합니다.

3단계 도메인 기반 쿼리의 이름을 입력합니다.

4단계 쿼리 유형을 선택합니다.

참고 도메인 기반 쿼리를 생성할 때 쿼리의 다른 형식의 쿼리를 선택할 수 없습니다. 일단 한 가지 쿼리 유형을 선택하면 어플라이언스는 쿼리 필드를 사용 가능한 서버 프로파일에서 확인된 해당 유형의 쿼리로 채웁니다.

5단계 Domain Assignment(도메인 지정) 필드에서 도메인을 입력합니다.

6단계 도메인과 연결할 쿼리를 선택합니다.

7단계 쿼리에 모든 도메인을 추가할 때까지 행을 계속 추가합니다.

8단계 다른 모든 쿼리에 실패한 경우 실행할 기본 쿼리를 입력할 수 있습니다. 기본 쿼리를 입력하지 않으려면 **None(없음)**을 선택합니다.

9단계 **Test Query(쿼리 테스트)** 버튼을 클릭하고 Test Parameters(테스트 매개 변수) 필드에 테스트할 이메일 주소 또는 사용자 로그인 ID 및 비밀번호를 입력하여 쿼리를 테스트합니다. 테스트 결과는 Connection Status(연결 상태 필드)에 나타납니다.

10단계 선택적으로, 수락 쿼리에서 {f} 토큰을 사용하는 경우 테스트하는 쿼리에 봉투 발신자 주소를 추가할 수 있습니다.

참고 도메인 기반 쿼리를 생성한 후, 개인 또는 공용 리스너에 연결해야 합니다.

11단계 변경사항을 제출하고 커밋합니다.

체인 쿼리를 사용하여 일련의 LDAP 쿼리 수행

체인 쿼리는 어플라이언스가 연속으로 실행하려고 하는 일련의 LDAP 쿼리입니다. 어플라이언스는 LDAP 서버가 긍정적인 응답을 반환(또는 "체인"의 마지막 쿼리가 부정적인 응답을 반환하거나 실패)할 때까지 "체인"에서 각 쿼리를 실행합니다. 체인 쿼리는 LDAP 디렉토리의 항목에서 다양한 특성을 사용하여 유사한(또는 동일한) 값을 저장하는 경우 유용합니다. 예를 들어, `maillocaladdress` 및 `mail` 특성을 사용하여 사용자 이메일 주소를 저장한 경우, 이러한 특성 모두에 대해 쿼리를 실행하기 위해 체인 쿼리를 사용할 수 있습니다.

절차

1단계 체인 쿼리에서 사용할 쿼리에 대해 서버 프로파일을 생성합니다. 각 서버 프로파일에 체인 쿼리에 사용할 쿼리를 구성합니다. 자세한 내용은 LDAP 서버 정보를 저장하도록 LDAP 서버 프로파일 생성, 25-5페이지 항목을 참조하십시오.

2단계 체인 쿼리를 생성합니다. 자세한 내용은 체인 쿼리 생성, 25-28페이지 항목을 참조하십시오.

3단계 공용 또는 개인 리스너에서 체인 쿼리를 활성화합니다. 리스너 구성에 대한 자세한 내용은 "메일을 수신하도록 게이트웨이 구성" 장을 참조하십시오.

참고 또한 LDAP 최종 사용자 액세스에 대한 도메인 기반 쿼리 또는 스팸 격리를 위한 스팸 알림을 활성화할 수 있습니다. 자세한 내용은 스팸 격리 장을 참조하십시오.

관련 주제

- 체인 쿼리 생성, 25-28페이지

체인 쿼리 생성

System Administration(시스템 관리) > LDAP > LDAP Server Profiles(LDAP 서버 프로파일) 페이지에서 체인 쿼리를 생성합니다.

절차

1단계 LDAP Server Profiles(LDAP 서버 프로파일) 페이지에서 **Advanced(고급)**를 클릭합니다.

2단계 **Add Chain Query(체인 쿼리 추가)**를 클릭합니다.

3단계 체인 쿼리 이름을 추가합니다.

4단계 쿼리 유형을 선택합니다.

체인 쿼리를 생성할 때 쿼리의 다른 형식의 쿼리를 선택할 수 없습니다. 일단 한 가지 쿼리 유형을 선택하면 어플라이언스는 쿼리 필드를 사용 가능한 서버 프로파일에서 확인된 해당 유형의 쿼리로 채웁니다.

5단계 체인 쿼리에 추가할 쿼리를 선택합니다.

어플라이언스는 쿼리를 구성한 순서에 따라 쿼리를 실행합니다. 따라서 체인 쿼리에 여러 쿼리를 추가한 경우, 구체적인 쿼리 다음에 일반적인 쿼리가 나오도록 쿼리 순서를 지정할 수 있습니다.

6단계 **Test Query(쿼리 테스트)** 버튼을 클릭하고 Test Parameters(테스트 매개 변수) 필드에 테스트할 이메일 주소 또는 사용자 로그인 ID 및 비밀번호를 입력하여 쿼리를 테스트합니다. 테스트 결과는 Connection Status(연결 상태 필드)에 나타납니다.

7단계 선택적으로, 수락 쿼리에서 {f} 토큰을 사용하는 경우 테스트하는 쿼리에 봉투 발신자 주소를 추가할 수 있습니다.

참고 체인 쿼리를 생성한 후, 개인 또는 공용 리스너에 연결해야 합니다.

8단계 변경사항을 제출하고 커밋합니다.

LDAP를 사용하여 디렉토리 수집 공격 방지

디렉토리 수집 공격은 악의적인 발신자가 일반적인 이름의 수신자에게 메시지를 전송하려고 시도하고 이메일 게이트웨이에서 수신자가 해당 위치에 유효한 메일함이 있는지를 확인하여 응답할 때 발생합니다. 공격이 대규모로 실행될 때 악의적인 발신자는 스팸 발송을 위해 이러한 유효한 주소를 "수집"하여 메일을 전송할 대상자를 판별할 수 있습니다.

Email Security 어플라이언스는 LDAP 수락 검증 쿼리를 사용할 때 DHA(디렉토리 수집 공격)를 탐지하고 방지할 수 있습니다. SMTP 대화 중 또는 작업 큐 내에서 디렉토리 수집 공격을 방지하기 위해 LDAP 수락을 구성할 수 있습니다.

관련 주제

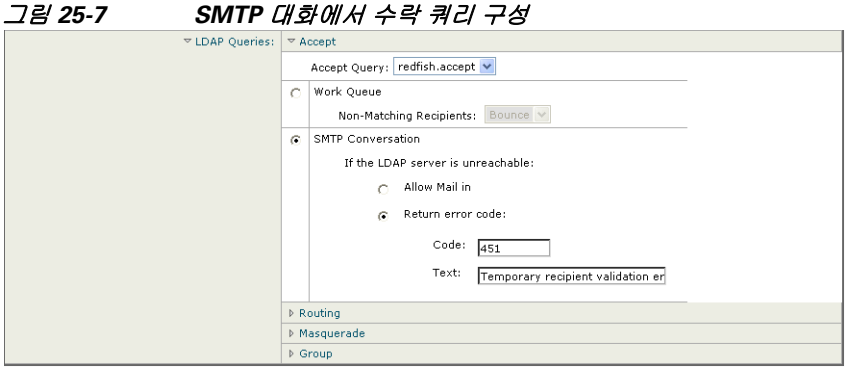
- SMTP 대화 중 디렉토리 수집 공격 방지, 25-29페이지
- 작업 큐 내에서 디렉토리 수집 공격 방지, 25-31페이지

SMTP 대화 중 디렉토리 수집 공격 방지

RTA(Recipient Access Table)에 도메인만 입력하고 SMTP 대화에서 LDAP 수락 검증을 수행하여 DHA를 방지할 수 있습니다.

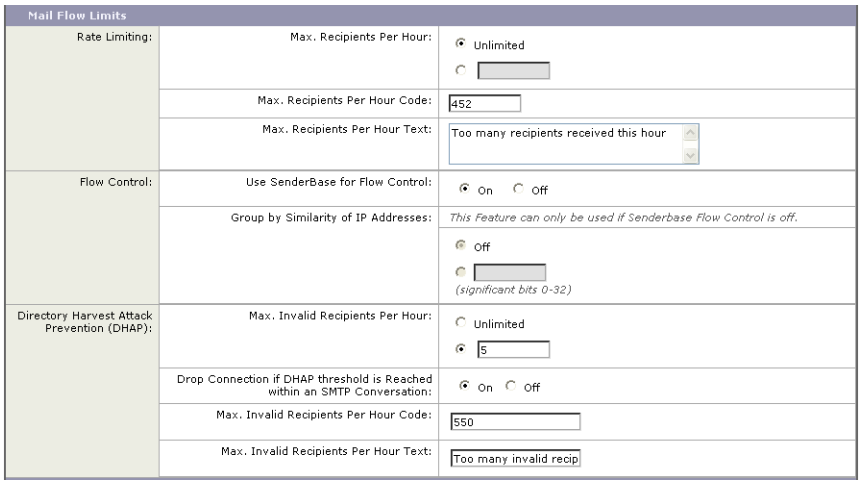
SMTP 대화 중에 메시지를 삭제하려면 LDAP 수락을 위한 LDAP 서버 프로파일을 구성합니다. 그런 다음 SMTP 대화 중에 LDAP 수락 쿼리를 수행하도록 리스너를 구성합니다.

그림 25-7 SMTP 대화에서 수락 쿼리 구성



리스너에 대한 LDAP 수락 쿼리를 구성한 후 리스너와 연결된 메일 흐름 정책에서 DHAP 설정을 구성해야 합니다.

그림 25-8 SMTP 대화에서 연결을 삭제하기 위해 메일 흐름 정책 구성



리스너와 연결된 메일 흐름 정책에서 다음 디렉토리 수집 공격 방지 설정을 구성합니다.

- **시간당 올바르지 않은 최대 수신자 수**. 이 리스너가 원격 호스트로부터 수신할 때의 시간당 올바르지 않은 최대 수신자 수입니다. 이 임계값은 SMTP 대화에서 삭제되었거나 작업 큐에서 바운스된 올바르지 않은 LDAP 수신자에 대한 총 메시지 수와 RAT 거부의 총 수를 나타냅니다. 예를 들어, 임계값을 5로 구성하고 카운터에서 올바르지 않은 LDAP 수신자로 보내는 RAT 거부 2개와 삭제된 메시지 3개를 탐지합니다. 이때 어플라이언스는 임계값에 도달했는지, 연결이 삭제되었는지 확인합니다. 기본적으로, 공용 리스너의 시간당 최대 수신자 수는 25명입니다. 개인 리스너의 경우, 시간당 최대 수신자 수는 기본적으로 무제한입니다. "무제한"으로 설정하면 DHAP가 해당 메일 흐름 정책에서 활성화되지 않은 것입니다.
- **SMTP 대화 도중에 DHAP 임계값에 도달하면 연결 삭제**. 디렉토리 수집 공격 방지 임계값에 도달하면 연결을 삭제하도록 어플라이언스를 구성합니다.
- **시간당 최대 수신자 수 코드**. 연결을 삭제할 때 사용할 코드를 지정합니다. 기본 코드는 550입니다.
- **시간당 최대 수신자 수 텍스트**. 삭제된 연결에 사용할 텍스트를 지정합니다. 기본 텍스트는 "Too many invalid recipients."입니다.

임계값에 도달하면 메시지의 봉투 발신자는 올바르지 않은 수신자의 경우 바운스 메시지를 수신하지 않습니다.

작업 큐 내에서 디렉토리 수집 공격 방지

RTA(Recipient Access Table)에 도메인만 입력하고 작업 큐 내에서 LDAP 수락 검증을 수행하여 대부분의 DHA를 방지할 수 있습니다. 이 기술은 악의적인 발신자가 SMTP 대화 도중에 수신자가 유효한지 여부를 파악하는 것을 방지합니다. (수락 쿼리가 구성된 경우, 시스템은 메시지를 수락한 다음 작업 큐 내에서 LDAP 수락 검증을 수행합니다.) 그러나 메시지의 봉투 발신자는 수신자가 유효하지 않은 경우에도 바운스 메시지를 여전히 수신합니다.

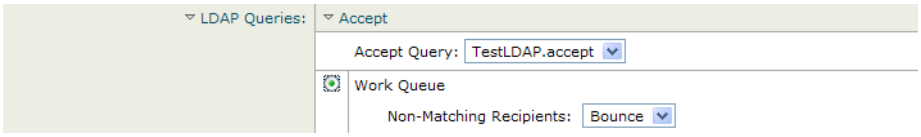
관련 주제

- 작업 큐에서 디렉토리 수집 방지 구성, 25-31페이지

작업 큐에서 디렉토리 수집 방지 구성

디렉토리 수집 공격을 방지하려면 먼저, LDAP 서버 프로파일을 구성하고 LDAP 수락을 활성화해야 합니다. LDAP 수락 쿼리를 활성화한 후 리스너에서 수락 쿼리를 사용하고 일치하지 않는 수신자에 대한 메일을 바운스하도록 구성합니다.

그림 25-9 일치하지 않는 수신자에 대한 메시지를 바운스하도록 수락 쿼리 구성



다음으로, 시스템이 특정 기간 동안 IP 주소를 전송할 때마다 허용할 올바르지 않은 수신자 주소의 수를 지정하도록 메일 흐름 정책을 구성합니다. 이 수를 초과하는 경우, 시스템은 이 상태를 DHA로 식별하고 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 흐름 정책에 지정한 임계값까지 메시지를 바운스한 다음 나머지를 자동으로 수락하고 삭제합니다. 이를 통해 올바른 발신자에게 해당 주소가 불량하다고 알리고 악의적인 발신자가 어떤 메시지가 수락되었는지 판별하는 것을 방지할 수 있습니다.

이러한 유효하지 않은 수신자를 카운터하는 기능은 AsyncOS에서 현재 사용 가능한 속도 제한과 유사한 방식입니다. 이 기능을 활성화하고 공용 리스너의 HAT(HAT에 대한 기본 메일 흐름 정책 포함)에서 메일 흐름 정책을 설정하는 방법의 하나로서 한계값을 지정합니다.

예를 들어 공용 리스너의 HAT에서 메일 흐름 정책 생성 또는 편집 시 CLI(`listenerconfig -> edit -> hostaccess -> default | new` 명령)에서 다음 질문이 포함된 프롬프트가 표시됩니다.

```
Do you want to enable Directory Harvest Attack Prevention per host?   [Y]> y


Enter the maximum number of invalid recipients per hour from a remote host.

[25]>
```

이 기능은 GUI에서 메일 흐름 정책을 편집할 때 표시되며 LDAP 쿼리가 해당 리스너에서 구성되었음을 알려줍니다.

그림 25-10 GUI에서의 DHAP 방지 기능

시간당 올바르지 않은 수신자를 여러 명 입력하면 해당 메일 흐름 정책에 대한 DHAP가 활성화됩니다. 기본적으로, 시간당 올바르지 않은 수신자 25명이 공용 리스너에서 허용됩니다. 개인 리스너의 경우, 시간당 올바르지 않은 최대 수신자 수는 기본적으로 무제한입니다. "무제한"으로 설정하면 DHAP가 해당 메일 흐름 정책에서 활성화되지 않은 것입니다.

SMTP 인증을 위한 AsyncOS 구성

AsyncOS는 SMTP 인증을 지원합니다. SMTP 인증은 SMTP 서버에 연결된 클라이언트를 인증하는 메커니즘입니다.

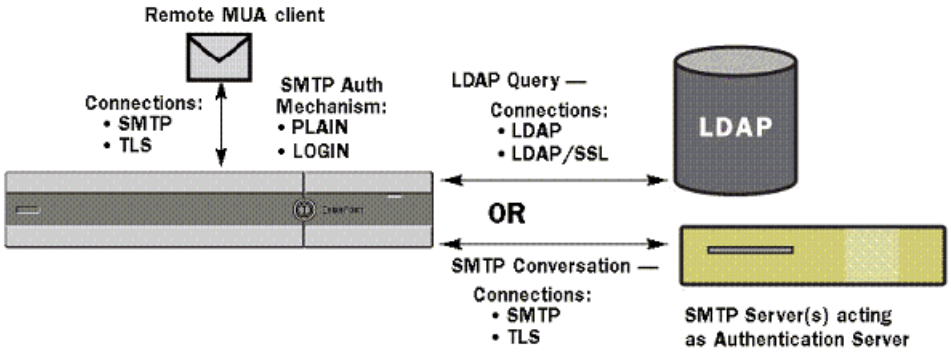
이 메커니즘을 사용하여 조직에 소속된 사용자가 원격에서 연결하는 경우에도(예: 자택에서 또는 출장 중에) 엔터티의 메일 서버를 사용하여 메일을 전송하도록 설정할 수 있습니다. MUA(메일 사용자 에이전트)는 메일을 전송하려고 시도할 때 인증 요청(챌린지/응답)을 실행할 수 있습니다.

또한 사용자는 발송 메일 릴레이에 대한 SMTP 인증을 사용할 수 있습니다. 이렇게 하면 어플라이언스가 네트워크 경계에 없는 구성에서 어플라이언스가 릴레이 서버에 보안 연결을 설정할 수 있습니다.

AsyncOS는 사용자 자격 증명을 인증하기 위해 다음의 2가지 방법을 지원합니다.

- LDAP 디렉토리를 사용할 수 있습니다.
- 다른 SMTP 서버를 사용할 수 있습니다(SMTP 인증 포워딩 및 SMTP 인증 발신).

그림 25-11 SMTP 인증 지원: LDAP 디렉토리 저장소 또는 SMTP 서버



구성된 SMTP 인증 방법은 HAT 메일 흐름 정책에서 사용할 `smtpauthconfig` 명령을 사용하여 SMTP 인증 프로파일을 생성하는 데 사용됩니다(리스너에서 SMTP 인증 활성화, 25-36페이지 참조).

관련 주제

- SMTP 인증 구성, 25-33페이지
- SMTP 인증 쿼리 구성, 25-34페이지
- 두 번째 SMTP 서버를 통한 SMTP 인증(포워딩을 통한 SMTP 인증), 25-35페이지
- LDAP을 통한 SMTP 인증, 25-35페이지

- 클라이언트 인증서를 사용하여 SMTP 세션 인증, 25-39페이지
- 발송 SMTP 인증, 25-39페이지
- 로깅 및 SMTP 인증, 25-39페이지

SMTP 인증 구성

LDAP 서버를 인증하려는 경우 Add LDAP Server Profile(LDAP 서버 프로파일 추가) 또는 Edit LDAP Server Profile(LDAP 서버 프로파일 편집) 페이지에서 SMTPAUTH 쿼리 유형을 선택하거나 `ldapconfig` 명령을 사용하여 SMTP 인증 쿼리를 생성합니다. 구성한 LDAP 서버마다 SMTP 인증 프로파일로 사용할 SMTPAUTH 쿼리를 구성할 수 있습니다.

SMTP 인증 쿼리는 LDAP 바인딩과 특성으로 비밀번호 사용하는 방식을 사용합니다. 특성으로 비밀번호를 사용하는 경우 어플라이언스는 LDAP 디렉토리에서 비밀번호 필드를 가져옵니다. 비밀번호는 일반 텍스트로 저장되고 암호화되거나 해시될 수 있습니다. LDAP 바인딩을 사용할 때 어플라이언스는 클라이언트가 제공한 자격 증명을 사용하여 LDAP 서버에 로그인합니다.

관련 주제

- 비밀번호를 특성으로 지정, 25-33페이지

비밀번호를 특성으로 지정

OpenLDAP에서 규칙은 RFC 2307을 따르며 인코딩된 비밀번호에 중괄호로 묶인 코딩 유형이 앞에 추가되는 방식입니다(예: "{SHA}5en6G6MezRroT3XKqkdPOmY/BfQ="). 이 예에서 비밀번호 부분은 SHA를 적용한 이후에 일반 텍스트 비밀번호를 base64 인코딩했습니다.

어플라이언스는 비밀번호를 얻기 전에 SASL 메커니즘과 MUA와 협상하고 어플라이언스와 MUA는 사용 방법을 결정합니다(LOGIN, PLAIN, MD5, SHA, SSHA 및 CRYPT SASL 메커니즘이 지원됨). 그런 다음 어플라이언스는 비밀번호를 가져오기 위해 LDAP 데이터베이스를 쿼리합니다. LDAP에서 비밀번호에는 중괄호로 묶인 접두사가 포함될 수 있습니다.

- 접두사가 없는 경우, 어플라이언스는 비밀번호가 일반 텍스트로 LDAP에 저장되어 있다고 가정합니다.
- 접두사가 있는 경우, 어플라이언스는 해시된 비밀번호를 가져오고 MUA가 제공한 사용자 이름 및/또는 비밀번호에 해시를 수행하고 해시된 버전을 비교합니다. 어플라이언스는 비밀번호 필드에서 해시된 비밀번호 앞에 해시 메커니즘 유형을 추가하는 RFC 2307 규칙에 따라 SHA1 및 MD5 해시 유형을 지원합니다.
- 일부 LDAP 서버(예: OpenWave LDAP 서버)는 암호화된 비밀번호 앞에 암호화 유형을 붙이지 않습니다. 대신, 암호화 유형을 별도의 LDAP 특성으로 저장합니다. 이러한 경우, 비밀번호를 SMTP 대화에서 얻은 비밀번호와 비교할 때 어플라이언스가 가정할 기본 SMTP AUTH 암호화 방법을 지정할 수 있습니다.

어플라이언스는 SMTP 인증 Exchange에서 임의의 사용자 이름을 가져와 지워졌거나 해시된 비밀번호 필드를 가져오는 LDAP 쿼리로 변환합니다. 그런 다음 SMTP 인증 자격 증명에서 제공된 비밀번호에 필요한 해시를 수행하고 이 결과를 LDAP에서 검색한 결과와 비교합니다(해시 유형 태그 포함, 가능한 경우 제거됨). 결과가 일치하는 경우 SMTP 인증 대화가 계속 진행됩니다. 결과가 일치하지 않으면 오류 코드가 발생합니다.

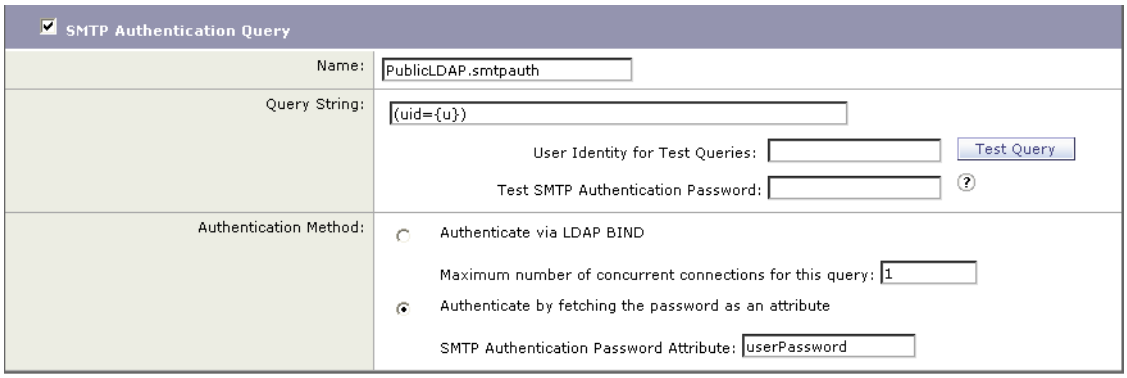
SMTP 인증 쿼리 구성

표 25-6 SMTP 인증 LDAP 쿼리 필드

이름	쿼리의 이름입니다.
쿼리 문자열	LDAP 바인딩 또는 비밀번호를 특성으로 가져오는 방법 중에서 인증 방법을 선택할 수 있습니다. **바인딩**: 클라이언트가 제공한 자격 증명을 사용하여 LDAP 서버에 로그인을 시도합니다(LDAP 바인딩이라고 함). SMTP 인증 쿼리에서 사용할 최대 동시 연결 수를 지정합니다. 이 숫자는 위의 LDAP 서버 특성에 지정된 수를 초과할 수 없습니다. 바인딩 인증을 위해 세션 시간 초과가 많이 발생하는 것을 방지하려면 최대 동시 연결 수를 늘립니다(일반적으로 거의 모든 연결이 SMTP 인증에 할당 가능). 새로운 연결이 각 바인딩 인증에 사용됩니다. 나머지 연결은 기타 LDAP 쿼리 유형에서 공유합니다. **특성으로 비밀번호 사용**: 비밀번호를 가져와 인증하려면 아래의 SMTP 인증 비밀번호 특성 필드에 비밀번호를 지정합니다. 인증 유형에 사용할 LDAP 쿼리를 지정합니다. Active Directory 쿼리 예: `(&(samaccountname={u})(objectCategory=person)(objectClass=user))`
SMTP 인증 비밀번호 특성	"비밀번호를 특성으로 가져와 인증"을 선택한 경우 비밀번호 특성을 여기에 지정할 수 있습니다.

다음 예에서는 System Administration(시스템 관리) > LDAP 페이지에서 SMTPAUTH 쿼리를 포함하도록 "PublicLDAP"라는 LDAP 구성을 편집합니다. 쿼리 문자열(`uid={u}`)은 userPassword 특성과 일치하도록 구성되었습니다.

그림 25-12 SMTP 인증 쿼리



SMTPAUTH 프로파일이 구성된 경우 리스너가 SMTP 인증에 대한 쿼리를 사용하도록 지정할 수 있습니다.

두 번째 SMTP 서버를 통한 SMTP 인증(포워딩을 통한 SMTP 인증)

다른 SMTP 서버를 통해 다른 SMTP 인증 대화에 제공된 사용자 이름과 비밀번호를 확인하도록 어플라이언스를 구성할 수 있습니다.

인증 서버는 메일을 전송하는 서버가 아니며 SMTP 인증 요청에만 응답합니다. 인증이 성공한 경우 전용 메일 서버를 사용하여 SMTP를 통한 메일 전송을 계속할 수 있습니다. 이 기능은 경우에 따라 "포워딩을 통한 SMTP 인증"이라고 하는데 그 이유는 인증을 위해 자격 증명만 다른 SMTP 서버에 포워딩(또는 "프록시")되기 때문입니다.

절차

1단계 Network(네트워크) > SMTP Authentication(SMTP 인증)을 선택합니다.

2단계 **Add Profile(프로파일 추가)**을 클릭합니다.

3단계 SMTP 인증 프로파일에 고유한 이름을 입력합니다.

4단계 **Profile Type(프로파일 유형)**에서 **Forward(포워드)**를 선택합니다.

5단계 **Next(다음)**를 클릭합니다.

6단계 포워딩 서버의 호스트 이름/IP 주소 및 포트를 입력합니다. 포워딩 인증 요청에 사용할 포워딩 인터페이스를 선택합니다. 최대 동시 연결 수를 지정합니다. 그런 다음 어플라이언스에서 포워딩 서버에 연결할 때 TLS를 사용할지 여부를 구성할 수 있습니다. 또한 가능한 경우 사용할 SASL 방법(PLAIN 또는 LOGIN)을 선택할 수 있습니다. 이 선택사항은 각 포워딩 서버에 구성됩니다.

7단계 변경사항을 제출하고 커밋합니다.

8단계 인증 프로파일을 생성한 후, 리스너에서 프로파일을 활성화할 수 있습니다. 자세한 내용은 리스너에서 SMTP 인증 활성화, 25-36페이지 항목을 참조하십시오.

LDAP을 통한 SMTP 인증

LDAP 기반 SMTP 인증 프로파일을 생성하려면 System Administration(시스템 관리) > LDAP 페이지에서 LDAP 서버 프로파일과 함께 SMTP 인증 쿼리를 생성한 상태여야 합니다. 그런 다음 이 프로파일을 사용하여 SMTP 인증 프로파일을 생성할 수 있습니다. LDAP 프로파일 생성에 대한 자세한 내용은 LDAP 쿼리 이해, 25-2페이지 항목을 참조하십시오.

절차

1단계 Network(네트워크) > SMTP Authentication(SMTP 인증)을 선택합니다.

2단계 **Add Profile(프로파일 추가)**을 클릭합니다.

3단계 SMTP 인증 프로파일에 고유한 이름을 입력합니다.

4단계 Profile Type(프로파일 유형)에서 **LDAP**를 선택합니다.

5단계 **Next(다음)**를 클릭합니다.

6단계 이 인증 프로파일에 사용할 LDAP 쿼리를 선택합니다.

7단계 드롭다운 메뉴에서 기본 암호화 방법을 선택합니다. SHA, Salted SHA, Crypt, Plain 또는 MD5를 선택할 수 있습니다. LDAP 서버가 암호화된 비밀번호 앞에 암호화 유형을 붙이는 경우, 'None'을 선택합니다. LDAP 서버가 개별 엔터티(예: OpenWave LDAP 서버)로 암호화 유형을 저장하는 경우 메뉴에서 암호화 방법을 선택합니다. 기본 암호화 설정은 LDAP 쿼리에서 바인딩을 사용하는 경우 사용되지 않습니다.

8단계 **Finish(마침)**를 클릭합니다.

9단계 변경사항을 제출하고 커밋합니다.

10단계 인증 프로파일을 생성한 후, 리스너에서 프로파일을 활성화할 수 있습니다. 자세한 내용은 리스너에서 SMTP 인증 활성화, 25-36페이지 항목을 참조하십시오.

관련 주제

- 리스너에서 SMTP 인증 활성화, 25-36페이지

리스너에서 SMTP 인증 활성화

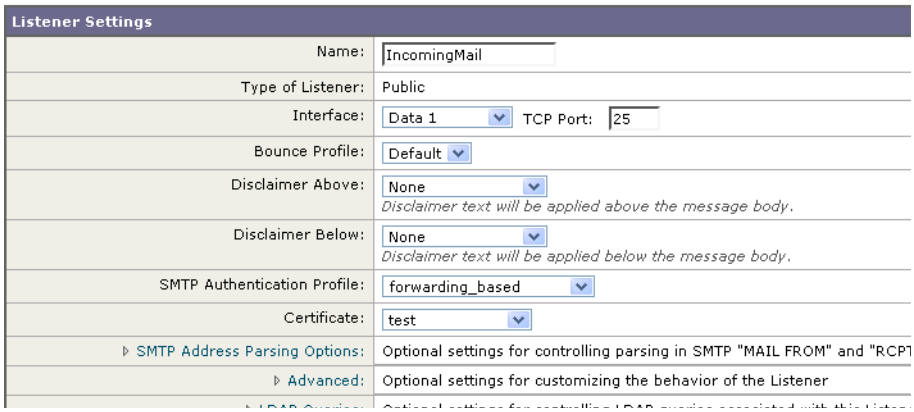
Network(네트워크) > SMTP Authentication(SMTP 인증) 페이지에서 SMTP 인증 유형을 지정하는(LDAP 기반 또는 SMTP 포워딩 기반) SMTP 인증 "프로파일"을 생성한 후, Network(네트워크) > Listeners(리스너) 페이지(또는 `listenerconfig` 명령)에서 리스너와 해당 프로파일을 연결해야 합니다.

참고 인증된 사용자는 자신의 현재 메일 흐름 정책 내의 RELAY 연결 동작에 대한 권한을 부여받습니다.

참고 하나의 프로파일에 포워딩 서버를 두 개 이상 지정할 수 있습니다. SASL 메커니즘인 CRAM-MD5 및 DIGEST-MD5는 어플라이언스 및 포워딩 서버 연결에 지원되지 않습니다.

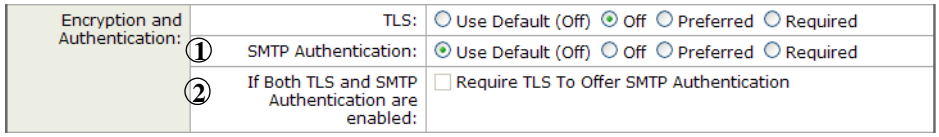
다음 예에서는 Edit Listener(리스너 편집) 페이지를 통해 구성된 SMTPAUTH 프로파일을 사용하도록 리스너 "InboundMail"을 편집합니다.

그림 25-13 리스너 편집 페이지를 통해 SMTP 인증 프로파일 선택



리스너가 프로파일을 사용하도록 구성되면 Host Access Table의 기본 설정을 리스너에서 SMTP 인증을 허용, 허용 안 함 또는 필수로 지정할 수 있습니다.

그림 25-14 메일 흐름 정책에서 SMTP 인증 활성화



번호	설명
1.	SMTP 인증 필드는 SMTP 인증을 위해 리스너 수준의 제어를 제공합니다. "No"를 선택한 경우 다른 SMTP 설정 구성과 관계없이 리스너에서 인증이 활성화되지 않습니다.
2.	두 번째 프롬프트에서 "Required"를 선택한 경우(SMTP 인증), TLS를 협상할 때까지(클라이언트가 두 번째 EHLO 명령을 실행한 후) AUTH 키워드가 실행되지 않습니다.

관련 주제

- SMTP 인증 및 HAT 정책 설정, 25-37페이지
- HAT 지연 거부, 25-37페이지

SMTP 인증 및 HAT 정책 설정

SMTP 인증 협상을 시작하기 전에 발신자는 적절한 발신자 그룹으로 분류되어 있으므로 HAT(Host Access Table) 설정에는 영향을 주지 않습니다. 원격 메일 호스트에 연결하면 어플라이언스는 먼저 어떤 발신자 그룹에 적용할지를 결정하고 해당 발신자 그룹에 메일 정책을 실행합니다. 예를 들어, 원격 MTA "suspicious.com"이 SUSPECTLIST 발신자 그룹에 있는 경우, THROTTLE 정책은 "suspicious.com"의 SMTPAUTH 협상 결과와 관계없이 적용됩니다.

그러나, SMTPAUTH로 인증하는 발신자는 "일반" 발신자와 다르게 처리됩니다. 성공적인 SMTPAUTH 세션을 위한 연결 동작은 "릴레이"로 변경되며 RAT(Recipient Access Table) 및 LDAPACCEPT를 효과적으로 우회합니다. 이렇게 하면 발신자가 어플라이언스를 통해 메시지를 릴레이할 수 있습니다. 언급한 것처럼, 속도 제한이나 적용되는 제한이 계속 영향을 미칩니다.

HAT 지연 거부

HAT 지연 거부가 구성된 경우, HAT 발신자 그룹과 메일 흐름 정책 구성에 기반하여 삭제되는 연결은 인증에 성공하며 RELAY 메일 흐름 정책을 부여받습니다.

`listenerconfig --> setup` CLI 명령을 사용하여 지연 거부를 구성할 수 있습니다. 이 동작은 기본적으로 비활성화되어 있습니다.

다음 테이블은 HAT에 대해 지연 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

이 Email Security 어플라이언스는 Email Security 어플라이언스와 사용자 메일 클라이언트 간 SMTP 세션을 인증하기 위해 클라이언트 인증서의 사용을 지원합니다.

SMTP 인증 프로파일을 생성하는 경우, 인증서 확인하는 데 사용할 인증서 인증 LDAP 쿼리를 선택합니다. 클라이언트 인증서를 사용할 수 없는 경우 사용자 인증을 위해 Email Security 어플라이언스에서 SMTP AUTH 명령을 사용하여 변경할 것인지 여부도 지정할 수 있습니다.

조직에서 클라이언트 인증서를 사용하여 사용자를 인증하는 경우, 클라이언트 인증서가 없는 사용자가 레코드에 메일 전송이 허용된다고 지정되어 있으면 메일을 전송할 수 있는지 여부를 확인하기 위해 SMTP 인증 쿼리를 사용하는 옵션이 있습니다.

자세한 내용은 클라이언트 인증서를 사용하여 SMTP 세션 인증 항목을 참조하십시오.

발송 SMTP 인증

SMTP 인증은 사용자 이름 및 비밀번호를 사용하여 아웃바운드 메일 릴레이를 검증하는 데 사용할 수 있습니다. '발송' SMTP 인증 프로파일을 생성한 다음 이 프로파일을 모든 도메인에 대한 SMTP 경로에 추가합니다. 메일 전달을 시도할 때 어플라이언스는 필요한 자격 증명을 통해 업스트림 메일 릴레이에 로그온합니다. SMTP 인증은 권한 부여 프로토콜인 PLAIN과 LOGIN을 지원합니다.

절차

1단계 **Network(네트워크) > SMTP Authentication(SMTP 인증)**을 선택합니다.

2단계 **Add Profile(프로파일 추가)**을 클릭합니다.

3단계 SMTP 인증 프로파일에 고유한 이름을 입력합니다.

4단계 Profile Type(프로파일 유형)의 경우 **Outgoing(발송)**을 선택합니다.

5단계 **Next(다음)**를 클릭합니다.

6단계 인증 프로파일에 대한 인증 사용자 이름 및 비밀번호를 입력합니다.

7단계 **Finish(마침)**를 클릭합니다.

8단계 **Network(네트워크) > SMTP Routes(SMTP 경로)**를 선택합니다.

9단계 테이블의 **Receiving Domain(수신 도메인)** 열에서 **All Other Domains(다른 모든 도메인)** 링크를 클릭합니다.

10단계 SMTP 경로에 대한 대상 호스트 이름을 입력합니다. 이것은 발송 메일을 전달하는 데 사용된 외부 메일 릴레이의 호스트 이름입니다.

11단계 드롭다운 메뉴에서 발송 SMTP 인증 프로파일을 선택합니다.

12단계 변경사항을 제출하고 커밋합니다.

로깅 및 SMTP 인증

SMTP 인증 메커니즘(LDAP 기반, SMTP 포워딩 서버 기반 또는 SMTP 발송)이 어플라이언스에 구성된 경우 다음 이벤트가 메일 로그에 로깅됩니다.

- [정보] SMTP 인증 시도 성공 — 인증된 사용자 및 사용된 메커니즘 포함 (일반 텍스트 비밀번호는 로깅되지 않음.)

- [정보] SMTP 인증 시도 실패 — 인증된 사용자 및 사용된 메커니즘 포함
- [경고] 인증 서버에 연결할 수 없음 — 서버 이름 및 메커니즘 포함
- [경고] 인증 요청을 대기하는 동안 포워딩 서버(업스트림과 대화 중, 어플라이언스 삽입 중) 시간이 초과된 경우 시간 초과 이벤트

사용자의 외부 LDAP 인증 구성

사용자가 LDAP 사용자 이름 및 비밀번호를 통해 로그인하도록 허용함으로써 네트워크에서 LDAP 디렉토리를 사용하여 사용자를 인증하도록 어플라이언스를 구성할 수 있습니다. LDAP 서버에 대한 인증 쿼리를 구성한 후, GUI의 System Administration(시스템 관리) > Users(사용자) 페이지에서 어플라이언스가 외부 인증을 사용하도록 설정합니다(또는 CLI에서 `userconfig` 명령).

절차

1단계 **사용자 계정을 찾는 쿼리를 생성합니다.** LDAP 서버 프로파일에서, LDAP 디렉토리에 있는 사용자 계정을 검색하는 쿼리를 생성합니다.

2단계 **그룹 멤버십 쿼리를 생성합니다.** 사용자가 디렉토리 그룹의 멤버인지를 확인하는 쿼리를 생성합니다.

3단계 **LDAP 서버를 사용하려면 외부 인증을 설정합니다.** 어플라이언스에서 사용자 인증에 LDAP 서버를 사용하도록 설정하고 LDAP 디렉토리의 그룹에 사용자 역할을 지정합니다. 자세한 내용은 "관리 작업 분배" 장의 "사용자 추가"를 참조하십시오.

참고 쿼리가 예상 결과를 반환하는지 확인하려면 LDAP 페이지에서 Test Query(쿼리 테스트) 버튼을 사용합니다(또는 `ldaptest` 명령). 자세한 내용은 LDAP 쿼리 테스트, 25-17페이지 항목을 참조하십시오.

관련 주제

- 사용자 계정 쿼리, 25-40페이지
- 그룹 멤버십 쿼리, 25-41페이지

사용자 계정 쿼리

외부 사용자를 인증하기 위해 AsyncOS는 쿼리를 사용하여 LDAP 디렉토리에서 사용자 레코드를 검색하고 사용자의 전체 이름을 포함하는 특성을 사용합니다. 선택한 서버 유형에 따라 AsyncOS는 기본 쿼리 및 기본 특성을 입력합니다. RFC 2307에 정의된 특성이 LDAP 사용자 레코드(`shadowLastChange`, `shadowMax` 및 `shadowExpire`)에 있는 경우 어플라이언스가 만료된 계정을 가진 사용자를 거부하도록 선택할 수 있습니다. 기본 DN은 사용자 레코드가 있는 도메인 수준에 필요합니다.

표 25-7은 Active Directory 서버에서 사용자 계정을 검색할 때 AsyncOS가 사용하는 기본 쿼리 문자열과 전체 사용자 이름 특성을 보여줍니다.

표 25-7 기본 사용자 계정 쿼리 문자열 및 특성: Active Directory

서버 유형	Active Directory
기본 DN	[공백] (사용자 레코드를 찾으려면 특정한 기본 DN을 사용해야 합니다.)
쿼리 문자열	`(&(objectClass=user)(sAMAccountName={u}))`
사용자의 전체 이름을 포함하는 특성	`displayName`

표 25-8은 OpenLDAP 서버에서 사용자 계정을 검색할 때 AsyncOS가 사용하는 기본 쿼리 문자열과 전체 사용자 이름 특성을 보여줍니다.

표 25-8 기본 사용자 계정 쿼리 문자열 및 특성: OpenLDAP

서버 유형	OpenLDAP
기본 DN	[공백] (사용자 레코드를 찾으려면 특정한 기본 DN을 사용해야 합니다.)
쿼리 문자열	`(&(objectClass=posixAccount)(uid={u}))`
사용자의 전체 이름을 포함하는 특성	`gecos`

그룹 멤버십 쿼리

AsyncOS는 사용자가 디렉토리 그룹의 멤버인지를 판별하는 쿼리를 생성합니다. 디렉토리 그룹 멤버십은 시스템 내에서의 사용자의 권한을 결정합니다. GUI의 System Administration(시스템 관리) > Users(사용자) 페이지에서(또는 CLI에서 `userconfig`) 외부 인증을 활성화한 경우, LDAP 디렉토리에 있는 그룹에 사용자 역할을 지정합니다. 사용자 역할은 사용자의 시스템 내 권한에 따라 결정되며, 외부에서 인증된 사용자의 경우 사용자 역할은 개별 사용자 대신 디렉토리 그룹에 지정됩니다. 예를 들어, IT 디렉토리 그룹의 사용자에게 관리자 역할을 할당할 수 있으며 지원 디렉토리 그룹의 사용자에게는 헬프 데스크 사용자 역할을 할당할 수 있습니다.

사용자가 다양한 사용자 역할이 있는 여러 LDAP 그룹에 속하는 경우, AsyncOS는 사용자에게 가장 제한이 많은 역할에 해당하는 권한을 부여합니다. 예를 들어 사용자가 작업자 권한을 가진 그룹과 헬프 데스크 사용자 권한을 가진 그룹에 속하는 경우, AsyncOS는 사용자에게 헬프 데스크 사용자 역할에 대한 권한을 부여합니다.

그룹 멤버십을 쿼리하도록 LDAP 프로파일을 구성하는 경우, 그룹 레코드를 찾을 수 있는 디렉토리 수준에 대한 기본 DN, 그룹 멤버의 사용자 이름을 포함하는 특성, 그룹 이름을 포함하는 특성을 입력합니다. LDAP 서버 프로파일에 대한 서버 유형을 선택하면, AysncOS는 이에 따라 사용자 이름 및 그룹 이름 특성에 대한 기본 값과 기본 쿼리 문자열을 입력합니다.

참고 Active Directory 서버의 경우, 사용자가 그룹의 멤버인지를 판별하는 기본 쿼리 문자열은 `(&(objectClass=group)(member={u}))` 입니다. 그러나, LDAP 스키마가 사용자 이름 대신 "memberof" 목록에 있는 고유 이름을 사용하는 경우, `{u}` 대신 `{dn}`을 사용할 수 있습니다.

표 25-9는 Active Directory 서버에서 그룹 멤버십 정보를 검색할 때 AsyncOS가 사용하는 기본 쿼리 문자열과 특성을 보여줍니다.

표 25-9 기본 그룹 멤버십 쿼리 문자열 및 특성: Active Directory

서버 유형	Active Directory
기본 DN	[공백] (그룹 레코드를 찾으려면 특정한 기본 DN을 사용해야 합니다.)
사용자가 그룹 멤버인지 판단하는 쿼리 문자열	`(&(objectClass=group)(member={u}))` **참고** LDAP 스키마가 사용자 이름 대신 `memberOf` 목록에 있는 고유 이름을 사용하는 경우, `{u}`를 `{dn}`으로 대체할 수 있습니다.
각 멤버의 사용자 이름을 가진 특성(또는 사용자 레코드에 대한 DN)	`member`
그룹 이름을 포함하는 특성	`cn`

표 25-10은 OpenLDAP 서버에서 그룹 멤버십 정보를 검색할 때 AsyncOS가 사용하는 기본 쿼리 문자열과 특성을 보여줍니다.

표 25-10 기본 그룹 멤버십 쿼리 문자열 및 특성: OpenLDAP

서버 유형	OpenLDAP
기본 DN	[공백] (그룹 레코드를 찾으려면 특정한 기본 DN을 사용해야 합니다.)
사용자가 그룹 멤버인지 판단하는 쿼리 문자열	`(&(objectClass=posixGroup)(memberUid={u}))`
각 멤버의 사용자 이름을 가진 특성(또는 사용자 레코드에 대한 DN)	`memberUid`
그룹 이름을 포함하는 특성	`cn`

스팸 격리의 최종 사용자 인증

스팸 격리의 최종 사용자 인증 쿼리는 사용자가 스팸 격리에 로그인할 때 사용자를 검증합니다. 토큰 {u}는 사용자(사용자 로그인 이름을 나타냄)를 지정합니다. 토큰 {a}는 사용자의 이메일 주소를 지정합니다. LDAP 쿼리는 이메일 주소에서 "SMTP:"를 제거하지 않습니다. AsyncOS는 주소의 해당 부분을 제거합니다.

스팸 격리에서 최종 사용자 액세스를 위해 LDAP 쿼리를 사용하려면 "Designate as the active query(활성 쿼리로 지정)" 확인란을 선택합니다. 기존 활성 쿼리가 있는 경우 이 쿼리는 비활성화됩니다. System Administration(시스템 관리) > LDAP 페이지를 열면 별표(*)가 활성 쿼리 옆에 표시됩니다.

서버 유형에 따라 AsyncOS는 최종 사용자 인증 쿼리를 위해 다음 기본 쿼리 문자열을 사용합니다.

- **Active Directory:** `(sAMAccountName={u})`
- **OpenLDAP:** `(uid={u})`
- **알 수 없음 또는 기타:** [공백]

기본적으로, 기본 이메일 특성은 Active Directory 서버의 경우 `proxyAddresses`이고 OpenLDAP 서버의 경우 `mail`입니다. 고유한 쿼리와 이메일 특성을 입력할 수 있습니다. CLI에서 쿼리를 생성하려면 `ldapconfig` 명령의 `isqauth` 하위 명령을 사용합니다.

참고 사용자가 전체 이메일 주소를 사용하여 로그인하도록 설정하려면 쿼리 문자열 `(mail=smtp:{a})`를 사용합니다.

관련 주제

- Active Directory 최종 사용자 인증 설정 샘플, 25-43페이지
- OpenLDAP 최종 사용자 인증 설정 샘플, 25-43페이지
- 스팸 격리에 대한 최종 사용자 액세스 구성, 31-16페이지
- 스팸 격리에 대한 최종 사용자 액세스 구성, 31-16페이지

Active Directory 최종 사용자 인증 설정 샘플

이 섹션은 Active Directory 서버 및 최종 사용자 인증 쿼리에 대한 샘플 설정을 보여줍니다. 이 예에서는 Active Directory 서버에 대한 최종 사용자 인증을 위해 비밀번호 인증, 이메일 특성 `mail` 및 `proxyAddresses`, 기본 쿼리 문자열을 사용합니다.

표 25-11 LDAP 서버 및 스팸 격리 최종 사용자 인증 설정 예: Active Directory

인증 방법	비밀번호 사용(검색을 위해 바인딩할 낮은 권한의 사용자를 생성하거나 익명 검색을 구성해야 함)
서버 유형	Active Directory
포트	3268
기본 DN	[공백]
연결 프로토콜	[공백]
쿼리 문자열	`(sAMAccountName={u})`
이메일 특성	`mail,proxyAddresses`

OpenLDAP 최종 사용자 인증 설정 샘플

이 섹션은 OpenLDAP 서버 및 최종 사용자 인증 쿼리에 대한 샘플 설정을 보여줍니다. 이 예에서는 OpenLDAP 서버에 대한 최종 사용자 인증을 위해 익명 인증, 이메일 특성 `mail` 및 `mailLocalAddress`, 기본 쿼리 문자열을 사용합니다.

표 25-12 LDAP 서버 및 스팸 격리의 최종 사용자 인증 설정 예: OpenLDAP

인증 방법	익명
서버 유형	OpenLDAP
포트	389
기본 DN	[공백] (일부 이전 스키마에서 특정 기본 DN 사용 가능)
연결 프로토콜	[공백]
쿼리 문자열	`(uid={u})`
이메일 특성	`mail,mailLocalAddress`

스팸 격리의 별칭 통합 쿼리

스팸 알림을 사용하는 경우, 스팸 격리의 별칭 통합 쿼리가 이메일 별칭을 통합하므로 수신자가 각 별칭에 대한 격리 통지를 수신하지 않습니다. 예를 들어, 수신자는 다음 이메일 주소에 대한 메일을 수신할 수 있습니다. john@example.com, jsmith@example.com 및 john.smith@example.com. 별칭 통합을 사용할 경우, 수신자는 사용자의 모든 별칭에 전송된 메시지에 대해 선택한 기본 이메일 주소로 단일한 스팸 통지를 수신합니다.

기본 이메일 주소로 메시지를 통합하려면 수신자의 대체 이메일 별칭을 검색하는 쿼리를 생성한 다음 Email Attribute(이메일 특성) 필드에 해당 수신자의 기본 이메일 주소의 특성을 입력합니다.

스팸 격리에서 스팸 알림을 위해 LDAP 쿼리를 사용하려면 "Designate as the active query(활성 쿼리로 지정)" 확인란을 선택합니다. 기존 활성 쿼리가 있는 경우 이 쿼리는 비활성화됩니다. System Administration(시스템 관리) > LDAP 페이지를 열면 별표(*)가 활성 쿼리 옆에 표시됩니다.

Active Directory 서버의 경우, 기본 쿼리 문자열은 `(|(proxyAddresses={a})(proxyAddresses=smtp:{a}))`이고 기본 이메일 특성은 `mail`입니다. OpenLDAP 서버의 경우, 기본 쿼리 문자열은 `(mail={a})`이고 기본 이메일 특성은 `mail`입니다. 쉼표로 구분된 여러 특성을 비롯하여 고유 쿼리 및 이메일 속성을 정의할 수 있습니다. 이메일 특성을 2개 이상 입력한 경우, Cisco에는 단일한 값을 사용하는 고유한 특성을 입력하는 것이 좋습니다. 예를 들어 첫 번째 이메일 특성으로 `proxyAddresses`와 같이 여러 값을 지닌 특성 대신 `mail`을 입력합니다.

CLI에서 쿼리를 생성하려면 `ldapconfig` 명령의 `isqalias` 하위 명령을 사용합니다.

관련 주제

- Active Directory의 별칭 통합 설정 샘플, 25-44페이지
- OpenLDAP의 별칭 통합 설정 샘플, 25-45페이지

Active Directory의 별칭 통합 설정 샘플

이 섹션은 Active Directory 서버 및 별칭 통합 쿼리에 대한 샘플 설정을 보여줍니다. 이 예에서는 Active Directory 서버에 대한 익명 인증, Active Directory 서버의 별칭 통합에 사용되는 쿼리 문자열, `mail` 이메일 특성을 사용합니다.

표 25-13 LDAP 서버 및 스팸 격리의 별칭 통합 설정 예: Active Directory

인증 방법	익명
서버 유형	Active Directory
포트	3268
기본 DN	[공백]
연결 프로토콜	SSL 사용
쿼리 문자열	`(|(mail={a})(mail=smtp:{a}))`
이메일 특성	`mail`

OpenLDAP의 별칭 통합 설정 샘플

이 섹션은 OpenLDAP 서버 및 별칭 통합 쿼리에 대한 샘플 설정을 보여줍니다. 이 예에서는 OpenLDAP 서버에 대한 익명 인증, OpenLDAP 서버의 별칭 통합에 사용되는 쿼리 문자열, `mail` 이메일 특성을 사용합니다.

표 25-14 LDAP 서버 및 스팸 격리의 별칭 통합 설정 예: OpenLDAP

인증 방법	익명
서버 유형	OpenLDAP
포트	389
기본 DN	[공백] (일부 이전 스키마에서 특정 기본 DN 사용 가능)
연결 프로토콜	SSL 사용
쿼리 문자열	`(mail={a})`
이메일 특성	`mail`

RSA Enterprise Manager에 대한 발신자의 사용자 고유 이름 식별

Email Security 어플라이언스는 Enterprise Manager에 DLP 인시던트 데이터를 전송할 때 메시지 발신자의 고유 이름 전체를 포함해야 합니다. Enterprise Manager에 대한 발신자 이름을 얻으려면 LDAP 서버에 대한 사용자 고유 이름 쿼리를 생성하고 이 쿼리를 Email Security 어플라이언스에서 발송 메시지를 전송하는 리스너에 추가합니다. Email Security 어플라이언스는 RSA Enterprise Manager가 DLP에 대해 활성화된 경우에만 이 쿼리를 사용합니다. 그렇지 않으면, 서버 프로파일에 대한 옵션이 표시되지 않습니다.

관련 주제

- 사용자 고유 이름 설정 샘플, 25-45페이지
- 다중 LDAP 서버와 동작하도록 AsyncOS 구성, 25-46페이지
- 서버 및 쿼리 테스트, 25-46페이지
- 장애 조치, 25-46페이지
- 부하 균형, 25-47페이지

사용자 고유 이름 설정 샘플

이 섹션은 Active Directory 서버 및 사용자 고유 이름 쿼리에 대한 샘플 설정을 보여줍니다. 이 예에서는 Active Directory 서버에 대한 익명 인증과 사용자 고유 이름 검색에 쿼리 문자열을 사용합니다.

표 25-15 LDAP 서버 및 스팸 격리의 별칭 통합 설정 예: Active Directory

인증 방법	익명
서버 유형	Active Directory
포트	3268
기본 DN	[공백]

표 25-15 LDAP 서버 및 스팸 격리의 별칭 통합 설정 예: Active Directory

연결 프로토콜	SSL 사용
쿼리 문자열	`(proxyAddresses=smtp:{a})`

다중 LDAP 서버와 동작하도록 AsyncOS 구성

LDAP 프로파일을 구성할 때, 다중 LDAP 서버 목록에 연결하도록 어플라이언스를 구성할 수 있습니다. 다중 LDAP 서버를 사용하려면 LDAP 서버가 동일한 서버를 포함하고 동일한 구조를 사용하며 동일한 인증 정보를 사용하도록 구성해야 합니다. (레코드를 통합할 수 있는 타사 제품이 있음.)

중복 LDAP 서버에 연결하도록 어플라이언스를 구성할 때 장애 조치 또는 부하 균형이 가능하도록 LDAP를 구성할 수 있습니다.

다중 LDAP 서버를 사용하여 다음 결과를 얻을 수 있습니다.

- **장애 조치**. 장애 조치를 위해 LDAP 프로파일을 구성하는 경우, 어플라이언스는 첫 번째 LDAP 서버에 연결할 수 없는 경우 목록의 다음 LDAP 서버로 장애 조치를 보냅니다.
- **부하 균형**. 부하 균형을 위해 LDAP 프로파일을 구성하는 경우 어플라이언스는 LDAP 쿼리를 수행할 때 LDAP 서버 목록 전체에 연결을 분배합니다.

System Administration(시스템 관리) > LDAP 페이지(또는 CLI의 `ldapconfig` 명령)에서 중복 LDAP 서버를 구성할 수 있습니다.

서버 및 쿼리 테스트

Add LDAP Server Profile(LDAP 서버 프로파일 추가) 또는 Edit LDAP Server Profile(LDAP 서버 프로파일 편집) 페이지에서 **Test Server(s)(서버 테스트)** 버튼(또는 CLI의 `test` 하위 명령)을 사용하여 LDAP 서버에 대한 연결을 테스트합니다. 다중 LDAP 서버를 사용한 경우, AsyncOS는 각 서버를 테스트하고 각 서버에 대해 개별적으로 결과를 표시합니다. AsyncOS는 각 LDAP 서버에서 쿼리를 테스트하고 개별 결과를 표시합니다.

장애 조치

LDAP 쿼리를 확인할 수 있도록 장애 조치에 대한 LDAP 프로파일을 구성할 수 있습니다.

어플라이언스는 지정된 시간 동안 LDAP 서버 목록에 있는 첫 번째 서버에 연결을 시도합니다. 어플라이언스가 목록의 첫 번째 LDAP 서버에 연결할 수 없는 경우, 어플라이언스는 목록의 다음 LDAP 서버에 연결을 시도합니다. 기본적으로, 어플라이언스는 항상 목록의 첫 번째 서버에 연결을 시도하고 서버가 나열된 순서대로 다음 서버로 연결을 시도합니다. 기본적으로 어플라이언스가 기본 LDAP 서버로 연결하려면 LDAP 서버의 목록에 해당 서버를 첫 번째 서버로 입력해야 합니다.

어플라이언스가 두 번째 또는 다음 LDAP 서버로 연결하는 경우, 시간제한에 도달할 때까지 해당 서버와의 연결 상태를 유지합니다. 이 시간제한에 도달한 후, 목록에서 첫 번째 서버에 다시 연결을 시도합니다.

관련 주제

- LDAP 장애 조치를 위한 어플라이언스 구성, 25-47페이지

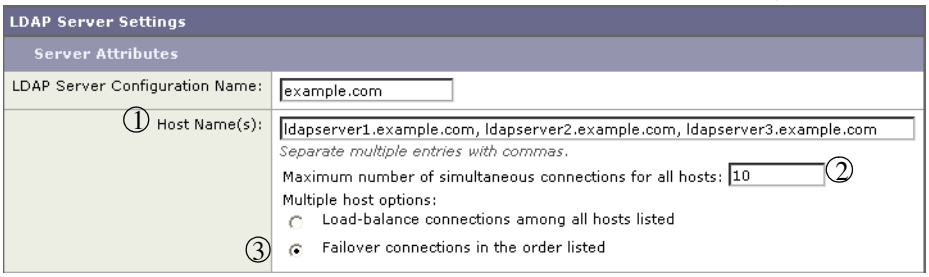
LDAP 장애 조치를 위한 어플라이언스 구성

LDAP 장애 조치를 위해 어플라이언스를 구성하려면 GUI에서 다음 단계를 완료합니다.

절차

1단계 System Administration(시스템 관리) > LDAP 페이지에서 편집할 LDAP 서버 프로파일을 선택합니다.

2단계 LDAP 서버 프로파일에서 다음 설정을 구성합니다.



번호	설명
1	LDAP 서버를 나열합니다.
2	최대 연결 수를 구성합니다.
3	장애 조치 모드를 선택합니다.

3단계 LDAP 설정을 구성하고 변경사항을 커밋합니다.

부하 균형

LDAP 서버 그룹에 LDAP 연결을 분배하도록 부하 균형을 위한 LDAP 프로파일을 구성할 수 있습니다.

부하 균형을 위해 LDAP 프로파일을 구성하는 경우 어플라이언스는 목록에 있는 LDAP 서버 간에 연결을 분배합니다. 연결이 실패하거나 시간을 초과한 경우 어플라이언스는 어떤 LDAP 서버가 사용 가능한지 확인하고 사용 가능한 서버에 다시 연결합니다. 어플라이언스는 구성한 최대 연결 수에 따라 설정할 동시 연결 수를 결정합니다.

나열된 LDAP 서버 중 하나가 응답하지 않는 경우, 어플라이언스는 나머지 LDAP 서버 간에 연결 부하를 분배합니다.

신뢰 항목

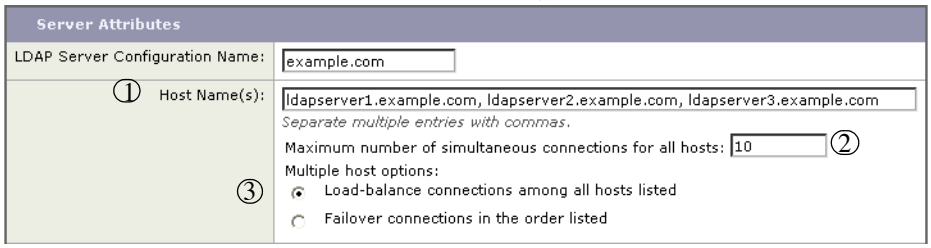
- 부하 균형을 위한 어플라이언스 구성, 25-47페이지

부하 균형을 위한 어플라이언스 구성

절차

1단계 System Administration(시스템 관리) > LDAP 페이지에서 편집할 LDAP 서버 프로파일을 선택합니다.

2단계 LDAP 서버 프로파일에서 다음 설정을 구성합니다.



번호	설명
1	LDAP 서버를 나열합니다.
2	최대 연결 수를 구성합니다.
3	부하 균형 모드를 선택합니다.

3단계 LDAP 설정을 구성하고 변경사항을 커밋합니다.

26 장

클라이언트 인증서를 사용하여 SMTP 세션 인증

인증서 및 SMTP 인증 개요

이 Email Security 어플라이언스는 Email Security 어플라이언스와 사용자 메일 클라이언트 간 SMTP 세션을 인증하기 위해 클라이언트 인증서의 사용을 지원합니다. Email Security 어플라이언스는 애플리케이션이 메시지를 보내기 위해 어플라이언스 연결을 시도할 때 사용자 메일 클라이언트로부터 클라이언트 인증서를 요청할 수 있습니다. 어플라이언스가 클라이언트 인증서를 받으면, 인증서가 유효하고 만료되었거나 해지되지 않았는지 확인합니다. 인증서가 유효한 경우 Email Security 어플라이언스는 TLS를 통해 메일 애플리케이션에서의 SMTP 연결을 허용합니다.

사용자가 메일 클라이언트에서 CAC(Common Access Card)를 사용하도록 설정하는 조직은 이 기능을 사용하여 CAC 및 ActivClient 미들웨어 애플리케이션이 어플라이언스에 제공하는 인증서를 요청하도록 Email Security 어플라이언스를 구성할 수 있습니다.

사용자가 메일을 보낼 때 인증서를 제공해야 하지만, 특정 사용자의 경우 예외를 허용하도록 Email Security 어플라이언스를 구성할 수 있습니다. 그러한 사용자의 경우 SMTP 인증 LDAP 쿼리를 사용하여 사용자를 인증하도록 어플라이언스를 구성할 수 있습니다.

사용자는 보안 연결(TLS)을 통해 메시지를 보내고 어플라이언스에서 서버 인증서를 허용하도록 메일 클라이언트를 구성해야 합니다.

관련 주제

- 클라이언트 인증서를 사용하여 사용자를 인증하는 방법, 26-50페이지
- SMTP 인증 LDAP 쿼리를 사용하여 사용자를 인증하는 방법, 26-50페이지
- 클라이언트 인증서가 유효하지 않은 경우 LDAP SMTP 인증 쿼리를 사용하여 사용자를 인증하는 방법, 26-50페이지

클라이언트 인증서를 사용하여 사용자를 인증하는 방법

표 26-1 클라이언트 인증서를 사용하여 사용자를 인증하는 방법

	수행할 작업	추가 정보
1단계	LDAP 서버에 대한 인증서 쿼리를 정의합니다.	클라이언트 인증서의 유효성 검사, 26-51페이지
2단계	인증서 기반 SMTP 인증 프로파일을 생성합니다.	클라이언트 인증서를 사용하여 TLS를 통해 SMTP 연결 인증, 26-52페이지
3단계	인증서 SMTP 인증 프로파일을 사용하도록 리스너를 구성합니다.	GUI를 통해 리스너를 생성하여 연결 요청 수신 대기, 5-6페이지
4단계	TLS, 클라이언트 인증서 및 SMTP 인증을 요구하도록 RELAYED 메일 흐름 정책을 수정합니다.	어플라이언스에서 TLS 연결 설정, 26-53페이지

SMTP 인증 LDAP 쿼리를 사용하여 사용자를 인증하는 방법

표 26-2 SMTP 인증 LDAP 쿼리를 사용하여 사용자를 인증하는 방법

	수행할 작업	추가 정보
1단계	인증 방법으로 허용 쿼리 문자열과 Bind를 사용하는 서버에 대한 SMTP 인증 쿼리를 정의합니다.	LDAP Directory를 사용하여 사용자 인증, 26-51페이지
2단계	LDAP 기반 SMTP 인증 프로파일을 생성합니다.	SMTP 인증을 위한 AsyncOS 구성, 25-32페이지
3단계	LDAP SMTP 인증 프로파일을 사용하도록 리스너를 구성합니다.	사용자가 연결 시 LDAP 기반 SMTP 인증을 사용하도록 허용되지 않은 경우 어플라이언스가 연결을 거부할지, 아니면 모든 활동을 기록하는 동안 임시로 연결을 허용할지 선택할 수 있습니다.
4단계	TLS 및 SMTP 인증을 요구하도록 RELAYED 메일 흐름 정책을 수정합니다.	어플라이언스에서 TLS 연결 설정, 26-53페이지

클라이언트 인증서가 유효하지 않은 경우 LDAP SMTP 인증 쿼리를 사용하여 사용자를 인증하는 방법

표 26-3 클라이언트 인증서 또는 LDAP SMTP 인증 쿼리를 사용하여 사용자를 인증하는 방법

	수행할 작업	추가 정보
1단계	인증 방법으로 허용 쿼리 문자열과 Bind를 사용하는 서버에 대한 SMTP 인증 쿼리를 정의합니다.	LDAP Directory를 사용하여 사용자 인증, 26-51페이지
2단계	LDAP 서버에 대한 인증서 기반 쿼리를 정의합니다.	클라이언트 인증서의 유효성 검사, 26-51페이지
3단계	인증서 기반 SMTP 인증 프로파일을 생성합니다.	클라이언트 인증서를 사용하여 TLS를 통해 SMTP 연결 인증, 26-52페이지

표 26-3 클라이언트 인증서 또는 LDAP SMTP 인증 쿼리를 사용하여 사용자를 인증하는 방법

	수행할 작업	추가 정보
4단계	LDAP SMTP 인증 프로파일을 생성합니다.	SMTP 인증을 위한 AsyncOS 구성, 25-32페이지
5단계	인증서 SMTP 인증 프로파일을 사용하도록 리스너를 구성합니다.	GUI를 통해 리스너를 생성하여 연결 요청 수신 대기, 5-6페이지
6단계	1. 다음 설정을 사용하도록 RELAYED 메일 흐름 정책을 수정합니다. • TLS 기본 설정 • SMTP 인증 필요 • SMTP 인증에 TLS 필요	어플라이언스에서 TLS 연결 설정, 26-53페이지

클라이언트 인증서의 유효성 검사

인증서 인증 LDAP 쿼리에서는 사용자 메일 클라이언트와 Email Security 어플라이언스 간 SMTP 세션을 인증하기 위해 클라이언트 인증서의 유효성을 검사합니다. 이 쿼리를 생성하는 경우 인증에 대한 인증서 필드 목록을 선택하고 사용자 ID 특성(기본값은 `uid`임)을 지정하고 쿼리 문자열을 입력합니다.

예를 들어 인증서의 일반 이름 및 일련 번호를 검색하는 쿼리 문자열은 다음과 같이 입력할 수 있습니다. `(&(objectClass-posixAccount)(caccn={cn})(cacserial={sn})` 쿼리를 생성하고 나면 인증서 SMTP 인증 프로파일에서 사용할 수 있습니다. 이 LDAP 쿼리는 OpenLDAP, Active Directory 및 Oracle Directory를 지원합니다.

LDAP 서버 구성에 대한 자세한 내용은 25 장, "LDAP 쿼리" 항목을 참조하십시오.

절차

1단계 **System Administration(시스템 관리) > LDAP**를 선택합니다.

2단계 새 LDAP 프로파일을 생성합니다. 자세한 내용은 LDAP 서버 정보를 저장하도록 LDAP 서버 프로파일 생성, 25-5페이지 항목을 참조하십시오.

3단계 **Certificate Authentication Query(인증서 인증 쿼리)** 확인란을 선택합니다.

4단계 쿼리 이름을 입력합니다.

5단계 사용자 인증서를 인증하기 위한 쿼리 문자열을 입력합니다. 예: `(&(objectClass=user)(cn={cn}))`

6단계 `sAMAccountName`과 같은 사용자 ID 특성을 입력합니다.

7단계 변경사항을 제출하고 커밋합니다.

LDAP Directory를 사용하여 사용자 인증

SMTP 인증 LDAP 쿼리에는 Email Security 어플라이언스가 사용자 메일 클라이언트가 LDAP 디렉토리의 사용자 레코드를 기반으로 어플라이언스를 통해 메일을 보낼 수 있는지 여부를 검사하도록 허용하는 허용 쿼리 문자열이 있습니다. 이를 통해 클라이언트 인증서가 없는 사용자도 레코드에 허용되도록 지정되어 있다면 메일을 보낼 수 있습니다.

또한 다른 특성을 기준으로 결과를 필터링할 수 있습니다. 예를 들어 `(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))` 쿼리 문자열은 사용자에 대해 다음 조건이 참인지 확인합니다.

- CAC가 사용자에게 발급되지 않음(`caccn=*`)
- CAC가 예외임(`cacexempt=*`)
- 사용자가 일시적으로 CAC 없이 메일을 보낼 수 있는 기간이 나중에 만료됨 (`cacemergency>={t}`)

SMTP 인증 쿼리 사용에 대한 자세한 내용은 SMTP 인증을 위한 AsyncOS 구성, 25-32페이지 항목을 참조하십시오.

절차

1단계 **System Administration(시스템 관리) > LDAP**를 선택합니다.

2단계 LDAP 프로파일을 정의합니다. 자세한 내용은 LDAP 서버 정보를 저장하도록 LDAP 서버 프로파일 생성, 25-5페이지 항목을 참조하십시오.

3단계 LDAP 프로파일에 대한 SMTP 인증 쿼리를 정의합니다.

4단계 SMTP Authentication Query(SMTP 인증 쿼리) 확인란을 선택합니다.

5단계 쿼리 이름을 입력합니다.

6단계 사용자 ID를 쿼리할 문자열을 입력합니다. 예: `(uid={u})`

7단계 인증 방법으로 LDAP BIND를 선택합니다.

8단계 허용 쿼리 문자열을 입력합니다. 예:
`(&(uid={u})(|(!(caccn=*))(cacexempt=*)(cacemergency>={t})))`

9단계 변경사항을 제출하고 커밋합니다.

클라이언트 인증서를 사용하여 TLS를 통해 SMTP 연결 인증

인증서 기반 SMTP 인증 프로파일을 사용하면 Email Security 어플라이언스가 클라이언트 인증서를 사용하여 TLS를 통해 SMTP 연결을 인증할 수 있습니다. 프로파일을 생성하는 경우 인증서를 확인하는 데 사용할 인증서 인증 LDAP 쿼리를 선택합니다. 클라이언트 인증서를 사용할 수 없는 경우 사용자 인증을 위해 Email Security 어플라이언스에서 SMTP AUTH 명령을 사용하여 변경할 것인지 여부도 지정할 수 있습니다.

LDAP를 사용한 SMTP 연결 인증에 대한 자세한 내용은 SMTP 인증을 위한 AsyncOS 구성, 25-32 페이지 항목을 참조하십시오.

절차

1단계 **Network(네트워크) > SMTP Authentication(SMTP 인증)**을 선택합니다.

2단계 **Add Profile(프로파일 추가)**을 클릭합니다.

3단계 SMTP 인증 프로파일의 이름을 입력합니다.

4단계 프로파일 유형으로 **Certificate(인증서)**를 선택합니다.

5단계 **Next(다음)**를 클릭합니다.

6단계 프로파일 이름을 입력합니다.

7단계 이 SMTP 인증 프로파일에 사용할 인증서 LDAP 쿼리를 선택합니다.

참고 클라이언트 인증서를 사용할 수 없는 경우 SMTP AUTH 명령을 허용하는 옵션을 선택하면 안 됩니다.

8단계 **Finish(마침)**를 클릭합니다.

9단계 변경사항을 제출하고 커밋합니다.

어플라이언스에서 TLS 연결 설정

RELAYED 메일 흐름 정책의 Verify Client Certificate(클라이언트 인증서 확인) 옵션을 사용하면 클라이언트 인증서가 유효한 경우 Email Security 어플라이언스가 사용자 메일 애플리케이션에 대한 TLS 연결을 설정합니다. TLS Preferred(TLS 기본 설정) 옵션을 선택하면, 사용자에게 인증서가 없더라도 어플라이언스는 계속 비TLS 연결을 허용하지만 사용자의 인증서가 유효하지 않은 경우에는 연결을 거부합니다. TLS Required(TLS 필수) 옵션을 선택하면, 어플라이언스가 연결을 허용하기 위해서는 사용자에게 유효한 인증서가 있어야 합니다.

클라이언트 인증서를 사용하여 사용자의 SMTP 세션을 인증하려면 다음 설정을 선택합니다.

- TLS - 필수
- 클라이언트 인증서 확인
- SMTP 인증 필수

참고 SMTP 인증이 필요한 경우에도 Email Security 어플라이언스는 인증서 인증을 사용하기 때문에 SMTP 인증 LDAP 쿼리를 사용하지 않습니다.

클라이언트 인증서 대신 SMTP 인증 쿼리를 사용하여 사용자 SMTP 세션을 인증하려면 RELAYED 메일 흐름 정책에서 다음 설정을 선택합니다.

- TLS - 필수
- SMTP 인증 필수

Email Security 어플라이언스가 특정 사용자로부터 클라이언트 인증서를 요구하는 반면 다른 사용자에게는 LDAP 기반 SMTP 인증을 허용해야 할 경우 RELAYED 메일 흐름 정책에서 다음 설정을 선택하십시오.

- TLS - 기본 설정
- SMTP 인증 필수
- SMTP 인증을 위한 TLS 필수

해지된 인증서 목록 업데이트

Email Security 어플라이언스는 인증서 확인 과정에서 해지된 인증서 목록(인증서 해지 목록이라고 함)을 검사하여 사용자 인증서가 해지되지 않았는지 확인합니다. 서버에 이 목록의 최신 버전을 유지할 수 있으며 Email Security 어플라이언스가 사용자가 만든 일정에 따라 해당 목록을 다운로드합니다.

절차

1단계 **Network(네트워크) > CRL Sources(CRL 소스)**로 이동합니다.

2단계 SMTP TLS 연결에 대해 CRL 검사를 활성화합니다.

- **a.** Global Settings(전역 설정)에서 Edit Settings(설정 편집)를 클릭합니다.
- **b.** **CRL check for inbound SMTP TLS(인바운드 SMTP TLS에 대한 CRL 검사)** 확인란을 선택합니다.
- **c.** (선택 사항) **CRL check for inbound SMTP TLS(인바운드 SMTP TLS에 대한 CRL 검사)** 확인란을 선택합니다.
- **d.** 변경사항을 제출합니다.

3단계 **Add CRL Source(CRL 소스 추가)**를 클릭합니다.

4단계 CRL 소스의 이름을 입력합니다.

5단계 파일 유형을 선택합니다. ASN.1 또는 PEM이 될 수 있습니다.

6단계 파일 이름을 포함하여 파일의 기본 소스에 대한 URL을 입력합니다. 예:
`https://crl.example.com/certs.crl`

7단계 어플라이언스가 기본 소스에 연결할 수 없는 경우에 대비하여 선택적으로 보조 소스의 URL을 입력합니다.

8단계 CRL 소스를 다운로드하기 위한 일정을 지정합니다.

9단계 CRL 소스를 활성화합니다.

10단계 변경사항을 제출하고 커밋합니다.

27 장

FIPS 관리

FIPS 관리 개요

FIPS(Federal Information Processing Standard) 140은 미국 및 캐나다 연방 정부가 공동 개발하여 공식적으로 발표한 표준으로, 민감하지만 기밀사항으로 분류되지 않은 정보를 보호하기 위해 정부 기관에서 사용하는 암호화 모듈에 대한 요구 사항을 명시한 표준입니다. Cisco IronPort Email Security 어플라이언스는 Cisco SSL Cryptographic Toolkit을 사용하여 FIPS 140-2 레벨 1 규정을 준수합니다.

Cisco SSL Cryptographic Toolkit은 OpenSSL의 FIPS 지원 고급 버전인 Cisco SSL과 FIPS 규격 Cisco Common Cryptography Module을 포함합니다. Cisco Common Cryptography Module은 Email Security 어플라이언스에서 SSH 등의 프로토콜에 대한 FIPS 검증 암호화 알고리즘으로 사용하는 소프트웨어 라이브러리입니다.

FIPS 모드의 구성 변경사항

Email Security 어플라이언스는 통신을 위해 어플라이언스가 FIPS 모드일 때 Cisco SSL 및 FIPS 규격 인증서를 사용합니다. 자세한 내용은 FIPS 모드로 어플라이언스 전환, 27-2페이지 항목을 참조하십시오.

참고 FIPS 규정 준수 일환으로, AsyncOS for Email은 SSH 버전 1을 지원하지 않습니다.

FIPS 레벨 1 규격을 위해 Email Security 어플라이언스의 구성을 다음과 같이 변경합니다.

- **SMTP 수신 및 전달.** Email Security 어플라이언스와 원격 호스트의 공용 리스너 간 TLS로 이뤄지는 수신 및 발송 SMTP 대화는 TLS 버전 1 및 FIPS 암호 그룹을 사용합니다. FIPS 모드에서 `sslconfig`를 사용하여 암호 그룹을 수정할 수 있습니다. TLS v1은 FIPS 모드에서 지원되는 유일한 TLS 버전입니다.
- **웹 인터페이스.** TLS 버전 1 및 FIPS 암호 그룹을 사용하는 Email Security 어플라이언스 웹 인터페이스의 HTTPS 세션입니다. IronPort Spam Quarantine 및 기타 IP 인터페이스에 대한 HTTP 세션도 포함합니다. FIPS 모드에서 `sslconfig`를 사용하여 암호 그룹을 수정할 수 있습니다.
- **인증서.** FIPS 모드에서는 어플라이언스에서 사용하는 인증서 종류가 제한됩니다. 인증서는 SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 및 2,048비트 크기의 RSA 키와 같은 서명 알고리즘을 사용해야 합니다. 어플라이언스는 이 알고리즘을 사용하지 않는 인증서는 가져오지 않습니다. 어플라이언스가 비규격 인증서를 사용 중인 경우 FIPS 모드로 전환될 수 없습니다. 대신 오류 메시지를 표시합니다. 자세한 내용은 인증서 및 키 관리, 27-4페이지 항목을 참조하십시오.
- **DKIM 서명 및 확인.** DKIM 서명 및 확인에 사용되는 RSA 키는 길이가 2,048비트여야 합니다. 어플라이언스가 비규격 RSA 키를 사용 중인 경우 FIPS 모드로 전환될 수 없습니다. 대신 오류 메시지를 표시합니다. DKIM 서명을 확인하는 중에 서명이 FIPS 규격 키를 사용하지 않는 경우 어플라이언스는 영구 실패를 반환합니다. 27 장, "DKIM 서명 및 확인을 위한 키 관리" 항목을 참조하십시오.
- **LDAPS.** 외부 인증을 위한 LDAP 서버 사용을 포함해 Email Security 어플라이언스 및 LDAP 서버 간 TLS 트랜잭션은 TLS 버전 1 및 FIPS 암호 그룹을 사용합니다. 비밀번호를 저장하기 위해 LDAP 서버에서 MD5 해시를 사용하는 경우, MD5가 FIPS 규격이 아니므로 SMTP 인증 쿼리에 실패합니다.
- **로그.** SSH2는 SCP를 통해 로그를 푸쉬하기 위해 유일하게 허용되는 프로토콜입니다. FIPS 관리와 관련된 오류 메시지의 경우, INFO의 FIPS 로그를 확인합니다.
- **중앙 집중식 관리.** 클러스터된 어플라이언스에서, FIPS 모드는 클러스터 수준에서만 활성화될 수 있습니다.
- **SSL 암호.** FIPS 모드에서는 SSL 암호 중 AES256-SHA:AES128-SHA:DES-CBC3-SHA만 지원됩니다.

FIPS 모드로 어플라이언스 전환

`fipsconfig` CLI 명령을 사용하여 어플라이언스를 FIPS 모드로 전환합니다.

참고 관리자만 이 명령을 사용할 수 있습니다. 어플라이언스를 비FIPS 모드에서 FIPS 모드로 전환한 후에는 재부팅해야 합니다.

시작하기 전에

어플라이언스에 비FIPS 규격 객체(예: 키 크기가 512비트인 DKIM 확인 프로파일)가 없는지 확인합니다. FIPS 모드를 활성화하려면 FIPS 요구 사항을 만족하도록 모든 비FIPS 규격 객체를 변경해야 합니다. FIPS 모드의 구성 변경사항, 27-1페이지 항목을 참조하십시오. 어플라이언스에 비FIPS 규격 객체가 있는지 확인하기 위한 명령은 FIPS 모드 규정 준수 검사, 27-4페이지 항목을 참조하십시오.

절차

```
mail.example.com> fipsconfig

FIPS mode is currently disabled.

Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> setup

To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.

Are you sure you want to enable FIPS mode and reboot now ? [N]> y

Do you want to enable encryption of sensitive data in configuration file when FIPS mode is
enabled? Changing the value will result in system reboot [N]> n

Enter the number of seconds to wait before forcibly closing connections.
[30]>

System rebooting.  Please wait while the queue is being closed...

Closing CLI connection.
Rebooting the system...
```

FIPS 모드에서 민감한 데이터 암호화

어플라이언스에서 `fipsconfig` 명령을 사용하여 비밀번호 및 키 등의 민감한 데이터를 암호화합니다. 이 옵션을 사용하는 경우,

- 어플라이언스에서 다음의 주요 보안 매개변수가 암호화되고 저장됩니다.
  - 인증서 개인 키
  - RADIUS 비밀번호
  - LDAP 바인딩 비밀번호
  - 로컬 사용자 비밀번호 해시
  - SNMP 비밀번호
  - DK/DKIM 서명 키
  - 발송 SMTP 인증 비밀번호
  - PostX 암호화 키
  - PostX 암호화 프록시 비밀번호
  - FTP 푸쉬 로그 구독 비밀번호
  - IPMI LAN 비밀번호
  - 업데이터 서버 URL

  참고 관리자를 비롯한 모든 사용자는 구성 파일에 있는 민감한 정보를 볼 수 없습니다.

- 어플라이언스의 스왑 공간은 어플라이언스의 물리적 보안이 손상되는 경우 무단 액세스 또는 포렌식 공격을 방지하기 위해 암호화되어 있습니다.

절차

```
mail.example.com> fipsconfig

FIPS mode is currently enabled.

Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> setup

To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.

Are you sure you want to disable FIPS mode and reboot now ? [N]> n

Do you want to enable encryption of sensitive data in configuration file when FIPS mode is
enabled? Changing the value will result in system reboot [N]> y

Enter the number of seconds to wait before forcibly closing connections.
[30]>

System rebooting.  Please wait while the queue is being closed...

Closing CLI connection.
Rebooting the system...
```

FIPS 모드 규정 준수 검사

`fipsconfig` 명령을 사용하여 어플라이언스에 비FIPS 규격 객체가 포함되어 있는지 확인합니다.

절차

```
mail.example.com> fipsconfig

FIPS mode is currently disabled.

Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> fipscheck

All objects in the current configuration are FIPS compliant.

FIPS mode is currently disabled.
```

인증서 및 키 관리

AsyncOS에서는 인증서 및 개인 키 쌍을 사용하여 어플라이언스와 외부 머신 간의 통신을 암호화할 수 있습니다. 기존 인증서 및 키 쌍을 업로드하거나 자체 서명 인증서를 생성하거나 CRS(Certificate Signing Request)를 생성하여 인증 기관에 제출하고 공용 인증서를 획득할 수 있습니다. 인증 기관에서는 개인 키로 서명한 신뢰할 수 있는 공용 인증서를 반환하며 이는 어플라이언스에 업로드할 수 있습니다.

어플라이언스가 FIPS 모드인 경우 다음을 진행할 수 있습니다.

어플라이언스의 FIPS 모드에서는 어플라이언스의 FIPS 규격 준수를 위해 어플라이언스에서 사용하는 인증서에 여러 제한사항을 추가합니다. 인증서는 SHA-1, SHA-224, SHA-256, SHA-384 및 SHA-512와 같은 서명 알고리즘을 사용해야 합니다.

어플라이언스는 이 알고리즘을 사용하지 않는 인증서는 가져오지 않습니다. 또한 리스너에서 비규격 인증서를 사용 중인 경우 FIPS 모드로 전환될 수 없습니다. 대신 오류 메시지를 표시합니다.

인증서의 `Non-FIPS` 상태는 어플라이언스가 FIPS 모드인 경우 CLI 및 GUI 모두에 표시됩니다. 리스너 또는 대상 제어 등의 기능에 사용할 인증서를 선택하는 경우 어플라이언스는 비규격 인증서를 옵션으로 표시하지 않습니다.

어플라이언스에서의 인증서 사용에 대한 자세한 내용은 인증서 얻기, 23-2페이지 항목을 참조하십시오.

다음의 모든 서비스에서 FIPS 규격 인증서를 사용할 수 있습니다.

- **SMTP 수신 및 전달. Network(네트워크) > Listener(리스너)** 페이지(또는 `listenerconfig -> edit -> certificate` CLI 명령)에서 TLS를 사용하는 암호화가 필요한 모든 리스너에 인증서를 할당합니다. 인터넷을 연결한 리스너(즉 공용 리스너)에서는 TLS를 활성화하지만 내부 시스템(즉, 개인 리스너)을 포함하는 모든 리스너에서는 암호화를 사용하도록 설정할 수 있습니다.
- **대상 제어 Mail Policies(메일 정책) > Destination Controls(대상 제어)** 페이지(또는 `destconfig` CLI 명령)에서 이메일 전달을 위한 모든 발송 TLS 연결에 대해 전역 설정으로 인증서를 할당합니다.
- **인터페이스. Network(네트워크) > IP Interfaces(IP 인터페이스)** 페이지(또는 `interfaceconfig` CLI 명령)에서 관리 인터페이스 등의 인터페이스에 사용되는 HTTPS 서비스에 대해 인증서를 사용합니다.
- **LDAP. System Administration(시스템 관리) > LDAP** 페이지에서 TLS 연결이 필요한 모든 LDAP 트래픽에 대해 인증서를 할당합니다. 어플라이언스는 사용자의 외부 인증을 위해 LDAP를 사용할 수도 있습니다.

DKIM 서명 및 확인을 위한 키 관리

Email Security 어플라이언스에서 DomainKeys 및 DKIM이 작동하는 방법에 대한 개요는 20 장, "이메일 인증" 항목을 참조하십시오.

관련 주제

- DKIM 서명, 27-5페이지
- DKIM 확인, 27-6페이지

DKIM 서명

DKIM 서명 키를 만들 때 키 크기를 지정합니다. FIPS 모드의 Email Security 어플라이언스는 2,048비트 키만 지원합니다. 크기가 큰 키가 안전하지만 이러한 키를 사용하면 성능에 영향을 줄 수 있습니다.

어플라이언스가 비규격 RSA 키를 사용 중인 경우 FIPS 모드로 전환될 수 없습니다. 대신 오류 메시지를 표시합니다.

FIPS 규격 서명 키는 도메인 프로파일에서 사용할 수 있으며 **Mail Policies(메일 정책) > Domain Profiles(도메인 프로파일)** 페이지에서 도메인 프로파일을 만들거나 편집하는 경우 서명 키 목록에 나타납니다. 서명 키를 도메인 프로파일과 연결하면 공개 키를 포함하는 DNS 텍스트 기록을 생성할 수 있습니다. 도메인 프로파일 목록의 DNS Text Record 열에 있는 Generate(생성) 링크를 통해 만들 수 있습니다(또는 CLI의 `domainkeysconfig -> profiles -> dnstxt`).

DKIM 확인

어플라이언스에서 DKIM 서명을 확인하려면 메시지가 FIPS 규격 키를 사용해야 합니다. 서명에서 FIPS 규격 키를 사용하지 않는 경우, 어플라이언스는 영구 실패를 반환합니다.

28 장

이메일 보안 모니터링 사용

이메일 보안 모니터링 개요

이메일 보안 모니터링 기능은 이메일 전송 프로세스의 각 단계에서 데이터를 수집합니다. 데이터베이스가 실시간 ID 정보를 얻기 위해 SenderBase Reputation Service와 상호 작용하면서 각 이메일 발신자를 IP 주소로 식별하여 기록합니다. 모든 이메일 발신자의 로컬 메일 흐름 기록을 즉시 보고하고 발신자의 글로벌 기록을 포함하는 프로필을 인터넷에 표시할 수 있습니다. 이메일 보안 모니터링 기능을 사용하면 보안 팀이 사용자에게 메일을 보내는 사람, 사용자가 보내거나 받은 메일의 양, 보안 정책의 효율성에 대한 "결함을 보완할" 수 있습니다.

이 장에서는 다음을 수행하는 방법을 설명합니다.

- 이메일 보안 모니터링 기능에 액세스하여 인바운드 및 아웃바운드 메시지 흐름을 모니터링하는 방법
- 발신자의 SBRS(SenderBase Reputation 점수)를 쿼리하여 메일 흐름 정책에 대한 결정(업데이트 허용 목록, 차단 목록 및 유보 목록)을 내리는 방법. 네트워크 소유자, 도메인, 심지어 개별 IP 주소에 대해서도 쿼리할 수 있습니다.
- 메일 흐름, 시스템 상태 및 네트워크에서 주고받은 메일을 보고하는 방법

수신 메일에 이메일 발신자가 지정되어 있으면 이메일 보안 모니터링 데이터베이스가 다음과 같은 중요한 매개변수를 캡처합니다.

- 메시지 볼륨
- 연결 기록
- 수락 및 거부된 연결
- 수락률 및 스로틀 제한
- 발신자 평판 필터 일치
- 의심스러운 스팸과 스팸으로 확인된 스팸에 대한 안티스팸 메시지 수
- 안티바이러스 검사를 통해 탐지된 바이러스에 감염된 메시지 수

안티스팸 검사에 대한 자세한 내용은 13 장, "안티스팸"을, 안티바이러스 검사에 대한 자세한 내용은 12 장, "안티바이러스"를 참조하십시오.

이메일 보안 모니터링 기능은 메시지를 받거나 보낸 내부 사용자(이메일 수신자)를 포함하여 특정 메시지가 트리거하는 콘텐츠 필터에 대한 정보도 캡처합니다.

이메일 보안 모니터링 기능은 GUI에서만 사용할 수 있으며, 이메일 트래픽과 어플라이언스의 상태에 대한 보기를 제공합니다(격리, 작업 큐, 신종 바이러스 등). 어플라이언스는 발신자가 정상적인 트래픽 프로필 외부에 있는지 확인합니다. 그러한 발신자는 인터페이스에서 강조 표시되므로 해당 발신자를 발신자 그룹에 할당하거나 발신자의 액세스 프로필을 조정하여 정정 작업을 수행할 수 있습니다. 또는 AsyncOS의 보안 서비스가 계속해서 대응하도록 설정할 수 있습니다. 아웃바운드 메일에는 메일 큐의 상위 도메인과 수신 호스트의 상태를 볼 수 있는 유사한 모니터링 기능이 있습니다(전송 상태 세부사항 페이지, 28-15페이지 참조).

참고 어플라이언스가 재부팅될 때 작업 큐에 있는 메시지에 대한 정보는 이메일 보안 모니터링 기능을 통해 보고되지 않습니다.

관련 주제

- 이메일 보안 모니터링 및 중앙 집중식 관리, 28-2페이지

이메일 보안 모니터링 및 중앙 집중식 관리

집계된 보고서 데이터를 보려면 Content Security Management Appliance를 배포합니다.

클러스터링 어플라이언스의 이메일 보안 모니터링 보고서를 집계할 수 없습니다. 모든 보고서는 머신 수준으로 제한됩니다. 이는 해당 그룹 또는 클러스터 수준이 아닌 개별 머신에서만 보고서를 실행할 수 있음을 의미합니다.

아카이브된 보고서 페이지에서도 마찬가지입니다. 즉, 적용되는 머신마다 자체 아카이브가 있으므로 "보고서 생성" 기능이 선택한 머신에서 실행됩니다.

예약 보고서 페이지는 머신 수준으로 제한되지 않으므로 여러 머신에서 설정을 공유할 수 있습니다. 개별 예약 보고서는 인터랙티브 보고서와 마찬가지로 머신 수준에서 실행되므로 클러스터 수준에서 예약 보고서를 구성할 경우 해당 클러스터의 모든 머신이 자체 보고서를 보냅니다.

"Preview This Report(이 보고서 미리보기)" 버튼이 로그인 호스트에 대해 항상 실행됩니다.

이메일 보안 모니터링 페이지

이메일 보안 모니터링 기능은 격리 페이지를 제외하고 모니터링 메뉴에서 사용할 수 있는 모든 페이지로 구성됩니다.

GUI에서 이러한 페이지를 사용하여 어플라이언스의 리스너에 연결되는 도메인을 모니터링할 수 있습니다. 어플라이언스의 "메일 흐름"을 모니터링, 정렬, 분석 및 분류하고 정상적인 메일을 대량으로 보내는 발신자와 잠재적인 "스패머"(원치 않는 상업용 이메일을 대량으로 보내는 발신자) 또는 바이러스 발신자를 구분할 수 있습니다. 이러한 페이지를 사용해 시스템에 대한 인바운드 연결 문제를 해결하거나 SBRS 점수 및 도메인의 가장 최근 발신자 그룹 일치 등의 중요한 정보를 확인할 수도 있습니다.

이러한 페이지를 통해 어플라이언스와 관련된 메일뿐 아니라 SenderBase Reputation Service, 안티스팸 검사 서비스, 안티바이러스 검사 보안 서비스, 콘텐츠 필터, 신종 바이러스 필터(Outbreak Filter)와 같은 게이트웨이의 범위를 벗어나 있는 서비스와 관련된 메일도 분류할 수 있습니다.

페이지의 오른쪽 상단에서 Printable PDF(인쇄 가능 PDF) 링크를 클릭하여 이메일 보안 모니터링 페이지의 인쇄용 .PDF 버전을 생성할 수 있습니다. 영어가 아닌 다른 언어로 PDF를 생성하는 방법에 대한 내용은 "보고서에 대한 참고사항" 섹션, 28-34페이지를 참조하십시오.

Export(내보내기) 링크를 통해 그래프와 기타 데이터를 CSV(쉼표로 구분된 값) 형식으로 내보낼 수 있습니다.

내보낸 CSV 데이터에는 Email Security 어플라이언스의 설정에 관계없이 GMT의 모든 메시지 추적 및 보고 데이터가 표시됩니다. GMT 시간 변환의 목적은 어플라이언스에서 독립적으로 데이터를 사용하거나 여러 표준 시간대에 있는 어플라이언스의 데이터를 참조할 수 있도록 하기 위한 것입니다.

참고 지역화된 CSV 데이터를 내보낼 경우 일부 브라우저에서는 머리글이 제대로 표시되지 않을 수 있습니다. 이러한 현상은 일부 브라우저가 지역화된 텍스트에 올바른 문자 집합을 사용하지 않기 때문에 발생할 수 있습니다. 이 문제를 해결하려면, 디스크에 파일을 저장하고 File(파일) > Open(열기)을 사용하여 파일을 열면 됩니다. 파일을 열 때 해당 문자 집합을 선택하면 지역화된 텍스트가 표시됩니다.

보고서 데이터의 내보내기 자동화에 대한 자세한 내용은 CSV 데이터 검색, 28-31페이지를 참조하십시오.

관련 주제

- 검색 및 이메일 보안 모니터링, 28-4페이지
- 보고서에 포함된 메시지의 세부사항 보기, 28-4페이지
- 내 보고서 페이지, 28-5페이지
- 개요 페이지, 28-5페이지
- 수신 메일 페이지, 28-9페이지
- 발송 대상, 28-14페이지
- 발송 발신자, 28-14페이지
- 전송 상태 페이지, 28-15페이지
- 내부 사용자 페이지, 28-16페이지
- DLP 사고 페이지, 28-17페이지
- 콘텐츠 필터 페이지, 28-18페이지
- DMARC 확인 페이지, 28-18페이지
- 신종 바이러스 필터(Outbreak Filter) 페이지, 28-19페이지
- 바이러스 유형 페이지, 28-20페이지
- URL 필터링 페이지, 28-21페이지
- 파일 평판 및 파일 분석 보고서, 28-21페이지
- TLS 연결 페이지, 28-21페이지
- 인바운드 SMTP 인증 페이지, 28-22페이지
- 속도 제한 페이지, 28-22페이지
- 시스템 용량 페이지, 28-23페이지
- 시스템 상태 페이지, 28-28페이지
- 대량 메일 페이지, 28-30페이지

- 메시지 필터 페이지, 28-30페이지
- CSV 데이터 검색, 28-31페이지

검색 및 이메일 보안 모니터링

상당수의 이메일 보안 모니터링 페이지에는 검색 양식이 포함되어 있습니다. 다음과 같은 다양한 유형의 항목을 검색할 수 있습니다.

- IP 주소(IPv4 및 IPv6)
- 도메인
- 네트워크 소유자
- 내부 사용자
- 대상 제어
- 내부 발신자 도메인
- 내부 발신자 IP 주소
- 발송 도메인 전송 상태

도메인, 네트워크 소유자 및 내부 사용자를 검색할 경우 검색 텍스트와 정확하게 일치하는 결과를 표시할지, 아니면 입력한 텍스트로 시작하는 항목을 찾을지 선택합니다(예를 들어, "ex"는 "example.com"과 일치).

IPv4 주소를 검색할 경우 입력한 텍스트가 항상 점으로 구분되는 10진수 형식으로 표시되는 최대 4개의 IP 옥텟의 시작 부분으로 해석됩니다. 예를 들어, "17"을 입력하면 17.0.0.0~17.255.255.255 범위의 항목이 검색되므로 172.0.0.1이 아닌 17.0.0.1과 일치합니다. 정확하게 일치하는 항목을 검색할 경우에는 4개의 옥텟을 입력하면 됩니다. IP 주소 검색은 CIDR 형식(17.16.0.0/12)도 지원합니다.

IPv6 주소 검색의 경우 AsyncOS는 다음과 같은 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 해당 페이지에서 현재 선택된 시간 범위로 제한됩니다.

보고서에 포함된 메시지의 세부사항 보기

절차

1단계 보고서 페이지의 표에서 파란색 번호를 클릭합니다.

(모든 표에 이러한 링크가 있는 것은 아닙니다.)

해당 번호에 포함된 메시지가 메시지 추적에 표시됩니다.

2단계 목록을 보려면 아래로 스크롤합니다.

관련 주제

- 메시지 추적 검색 결과 사용, 29-4페이지

내 보고서 페이지

기존 보고서 페이지에서 차트(그래프)와 표를 조합하여 사용자 지정 보고서 페이지와 를 생성할 수 있습니다.

변경 후	수행할 작업
사용자 지정 보고서 페이지에 모듈 추가	1. **Monitor(모니터링) > My Reports(내 보고서)**로 이동해 모듈의 오른쪽 상단에 있는 **[X]**를 클릭하여 필요하지 않은 샘플 모듈을 삭제합니다. 2. 다음 중 하나를 수행합니다. – 보고서 페이지에서 모듈의 **[+]** 버튼을 클릭(모니터링 메뉴)하여 사용자 지정 보고서에 모듈을 추가합니다. – **Monitor(모니터링) > My Reports(내 보고서)로 이동해** [+] 버튼을 클릭(섹션 중 하나에서)한 다음 추가할 보고서 모듈을 선택합니다. 원하는 보고서를 찾으려면 각 섹션의 **+ Report Module(+ 보고서 모듈)**을 선택해야 할 수 있습니다. 3. 모듈은 기본 설정으로 추가됩니다. 사용자 지정한(예: 열을 추가, 삭제 또는 재정렬하거나) 모듈을 추가할 경우 추가한 후에 모듈을 다시 사용자 지정합니다. 원래 모듈의 시간 범위가 유지되지 않습니다. 4. 개별 범례(예: 개요 페이지의 그래프)가 포함된 차트를 추가하려면 범례를 따로 추가합니다. 필요한 경우 범례가 설명하는 데이터 옆에 범례를 끌어 놓습니다. 참고: • 몇몇 보고서 페이지의 일부 모듈은 위의 방법 중 하나를 통해서만 사용할 수 있습니다. 한 가지 방법으로 모듈을 추가할 수 없는 경우 다른 방법을 시도하십시오. • 사용자 지정 보고서에 다음과 같은 보고 모듈은 추가할 수 없습니다. – 신종 바이러스 필터(Outbreak Filter) 보고서 페이지의 **이전 연도 신종 바이러스 요약** 차트 및 **이전 연도 신종 바이러스** 표 – 모든 보고서에 대한 검색 결과 • 각 모듈을 한 번만 추가할 수 있습니다. 보고서에 이미 특정 모듈을 추가한 경우 해당 모듈을 추가하는 옵션을 사용할 수 없습니다.
사용자 지정 보고서 페이지 보기	1. **Monitor(모니터링) > My Reports(내 보고서)**를 선택합니다. 2. 시간 범위 섹션의 보고서: 모든 보고서 페이지에 대해 선택한 시간 범위가 내 보고서 페이지의 모든 모듈에 적용됩니다. 보려는 시간 범위를 선택합니다. 새로 추가된 모듈이 관련 섹션의 상단에 표시됩니다.
사용자 지정 보고서 페이지에서 모듈 다시 정렬	원하는 위치로 모듈을 끌어서 놓습니다.
사용자 지정 보고서 페이지에서 모듈을 삭제합니다.	모듈의 오른쪽 상단에서 [X]를 클릭합니다.

개요 페이지

개요 페이지는 사용자의 격리 및 신종 바이러스 필터(Outbreak Filter) 상태에 대한 개요를 포함하여 어플라이언스의 메시지 활동 개요를 제공합니다. 개요 페이지에는 수신 및 발송 메시지의 그래프와 자세한 메시지 수도 나와 있습니다. 이 페이지를 사용하여 게이트웨이로 들어오거나 게이트웨이에서 나가는 모든 메일의 흐름을 모니터링할 수 있습니다.

개요 페이지에서는 어플라이언스가 수신 메일(예: 평판 필터링에 의해 중지된 메시지)의 SenderBase Reputation Service와 통합되는 방식을 중점적으로 보여줍니다. **개요** 페이지에서 다음을 수행할 수 있습니다.

- 게이트웨이로 들어가거나 게이트웨이에서 나가는 모든 메일 "흐름"의 메일 트렌드 그래프를 볼 수 있습니다.
- 시도된 메시지, SBRS(발신자 평판 필터링)에 의해 중지된 메시지, 수신자가 올바르지 않은 메시지, 스팸으로 표시된 메시지, 바이러스 감염으로 표시된 메시지 및 클린 메시지의 수를 시간 경과에 따라 보여주는 그래프를 볼 수 있습니다.
- 시스템 상태 및 로컬 격리의 요약을 볼 수 있습니다.
- TOC(Threat Operations Center)에 제공된 정보를 기반으로 하는 현재 바이러스 및 비 신종 바이러스 정보를 참조할 수 있습니다.

개요 페이지는 2개의 섹션(시스템 개요, 수신/발송 메일 그래프 및 요약)으로 나누어져 있습니다.

관련 주제

- 시스템 개요, 28-6페이지
- 수신 및 발송 요약 및 그래프, 28-7페이지
- 이메일 분류, 28-8페이지
- 메시지를 분류하는 방법, 28-8페이지

시스템 개요

개요 페이지의 시스템 개요 섹션은 시스템 및 작업 큐 상태, 격리 상태, 신종 바이러스 활동을 포함한 어플라이언스에 대한 세부사항을 제공하는 시스템 대시보드의 역할을 합니다.

관련 주제

- 상태, 28-6페이지
- 시스템 격리, 28-7페이지
- 바이러스 위협 수준, 28-7페이지

상태

이 섹션에서는 어플라이언스 및 인바운드 메일 처리에 대한 현재 상태 개요를 제공합니다.

시스템 상태: 다음 상태 중 하나를 표시합니다.

- 온라인
- 리소스 보존(conservation)
- 전송 일시 중단
- 수신 일시 중단
- 작업 대기열 일시 중지
- 오프라인

자세한 내용은 34 장, "CLI를 통한 관리 및 모니터링"을 참조하십시오.

수신 메시지: 시간당 수신 메일의 평균 속도입니다.

작업 큐: 작업 큐에서 처리 대기 중인 메시지의 수입니다.

시스템 상태 페이지로 이동하려면 System Status Details(시스템 상태 정보) 링크를 클릭합니다.

시스템 격리

이 섹션에는 격리의 이름, 현재 격리 사용 용량(디스크 공간), 격리의 현재 메시지 수를 포함하여 어플라이언스의 디스크 사용량에 따라 상위 3개의 격리에 대한 정보가 표시됩니다.

로컬 격리 페이지로 이동하려면 Local Quarantines(로컬 격리) 링크를 클릭합니다.

바이러스 위협 수준

이 섹션에는 TOC(Threat Operations Center)에서 보고된 대로 신종 바이러스 상태가 표시됩니다. 또한 현재 사용 용량(디스크 공간) 및 격리의 메시지 수를 포함하여 신종 바이러스 격리의 상태도 표시됩니다. 신종 바이러스 격리는 어플라이언스에서 신종 바이러스 필터(Outbreak Filter) 기능을 활성화한 경우에만 표시됩니다.

참고 위협 수준 표시기가 작동하려면 방화벽의 개방형 포트 80을 "downloads.ironport.com"에 연결해야 합니다. 또는 로컬 업데이트 서버를 지정한 경우 위협 수준 표시기가 해당 주소를 사용하려고 시도합니다. 서비스 업데이트 페이지를 통해 운로드에 대한 프록시를 구성한 경우에도 위협 수준 표시기가 올바르게 업데이트됩니다. 자세한 내용은 서비스 업데이트, 33-17페이지를 참고하십시오.

외부 Threat Operations Center 웹사이트를 보려면 Outbreak Details(신종 바이러스 세부사항) 링크를 클릭합니다. 사용 중인 어플라이언스에서 인터넷에 액세스할 수 있어야 이 링크가 작동합니다. 별도의 창 아이콘( )은 클릭하면 링크가 별도의 창에 열림을 나타냅니다. 이러한 창을 허용하려면 브라우저의 팝업 차단기 설정을 구성해야 할 수 있습니다.

수신 및 발송 요약 및 그래프

수신 및 발송 요약 섹션은 시스템의 모든 실시간 메일 활동에 대한 액세스를 제공하며 수신 및 발송 메일 그래프 및 메일 요약으로 구성되어 있습니다. 시간 범위 메뉴를 통해 보고할 기간을 선택할 수 있습니다. 선택하는 시간 범위는 모든 이메일 보안 모니터링 페이지에서 사용됩니다. 각 메시지 유형 또는 범주에 대한 설명이 아래에 나와 있습니다(이메일 분류, 28-8페이지 참조).

메일 트렌드 그래프에 메일 흐름이 시각적으로 표시되지만 요약 표에는 동일한 그래프의 숫자 분석이 표시됩니다. 요약 표에는 시도한 메시지, 위협 메시지 및 클린 메시지의 총 수를 포함한 각 메시지 유형의 비율 및 실제 수가 포함되어 있습니다.

발송 그래프 및 요약은 발송 메일에 대한 유사한 정보를 표시합니다.

관련 주제

- 이메일 보안 모니터링 메시지 계산 관련 참고 사항, 28-7페이지

이메일 보안 모니터링 메시지 계산 관련 참고 사항

수신 메일을 계산하기 위한 이메일 보안 모니터링 방법 사용은 메시지당 수신자의 수에 따라 달라집니다. 예를 들어, example.com에서 3명의 수신자에게 보낸 수신 메시지는 해당 발신자에게서 오는 3개의 메시지로 계산됩니다.

발신자 평판 필터링에 의해 차단된 메시지는 실제로 작업 큐에 들어가지 않으므로 어플라이언스가 수신 메시지의 발신자 목록에 액세스할 수 없습니다. 이 경우, 승수는 수신자의 수를 추정하는 데 사용됩니다. 이 승수는 Cisco에서 기존 고객 데이터의 대규모 샘플링 연구를 기반으로 결정합니다.

이메일 분류

개요 및 수신 메일 페이지에 보고된 메시지는 다음과 같이 분류됩니다.

평판 필터링에 의해 중지됨: HAT 정책에 의해 차단된 모든 연결에 고정된 숫수를 곱한 값(이메일 보안 모니터링 메시지 계산 관련 참고 사항, 28-7페이지 참조)에 수신자 제한에 의해 차단된 모든 수신자를 더한 값입니다.

올바르지 않은 수신자: 대화식 LDAP 거부에 의해 거부된 모든 수신자에 모든 RAT 거부를 더한 값입니다.

탐지된 스팸 메시지: 안티스팸 검사 엔진에서 스팸으로 확인된 스팸 또는 의심스러운 스팸으로 탐지한 총 메시지 수와 스팸 및 바이러스에 감염된 총 메시지 수입니다.

탐지된 바이러스 메시지: 바이러스 감염으로 탐지되었으나 스팸은 아닌 메시지의 총 수 및 비율입니다.

참고 검색할 수 없거나 암호화된 메시지를 전달하도록 안티바이러스 설정을 구성한 경우 이러한 메시지가 바이러스 감염 메시지가 아닌 클린 메시지로 계산됩니다. 그렇지 않은 경우 메시지는 바이러스 감염 메시지로 계산됩니다.

Advanced Malware Protection에 의해 탐지됨: 파일 평판 필터링에 의해 악성으로 발견된 메시지 첨부 파일입니다. 이 값은 파일 분석에 의해 악성으로 발견된 판정 업데이트 또는 파일을 포함하지 않습니다.

악성 URL을 포함한 메시지: URL 필터링에 의해 메시지에서 악성 URL이 하나 이상 발견되었습니다.

콘텐츠 필터에 의해 중지됨: 콘텐츠 필터에 의해 중지된 총 메시지 수입니다.

DMARC에 의해 중지됨: DMARC 확인 후에 중지된 총 메시지 수입니다.

S/MIME 확인/암호 해독 실패: S/MIME 확인이나 암호 해독 또는 둘 다 실패한 총 메시지 수입니다.

마케팅 메시지: 안티스팸 검사에 의해 정상적인 소스에서 수신된 것으로 확인된 총 마케팅 메시지 수입니다. 이 항목은 마케팅 데이터가 시스템에 있는 경우에만 나타납니다.

S/MIME 확인/암호 해독 성공: 성공적으로 확인 또는 암호 해독되었거나 S/MIME를 사용하여 암호 해독 및 확인된 총 메시지 수입니다.

승인된 클린: 승인되었으며 바이러스 및 스팸이 없는 것으로 간주되는 메일로, 수신자당 검사 작업을 고려할 때 승인된 클린 메시지의 가장 정확한 표현입니다(별도의 메일 정책에 의해 처리되는 분할된 메시지 등). 그러나 스팸 또는 바이러스 감염으로 표시되었으나 여전히 전달되는 메시지는 계산되지 않으므로 전달되는 실제 메시지 수가 클린 메시지 수와 다를 수 있습니다.

참고 *메시지* 필터와 일치하지 않으며 필터에 의해 삭제 또는 바운스되지 않은 메시지는 클린 메시지로 처리됩니다. 메시지 필터에 의해 삭제 또는 바운스된 메시지는 합계에서 계산되지 않습니다.

메시지를 분류하는 방법

메시지가 이메일 파이프라인을 따라 진행할 때 여러 범주에 적용할 수 있습니다. 예를 들어, 메시지가 스팸 또는 바이러스 감염으로 표시될 수 있으며 콘텐츠 필터와 일치할 수도 있습니다. 다양한 판정은 다음과 같은 우선 규칙을 따릅니다. 즉, 신종 바이러스 필터(Outbreak Filter) 격리(이 경우 메시지는 격리에서 해제되고 작업 큐를 통해 다시 처리될 때까지 계산되지 않음) 후에 스팸 감염, 바이러스 감염, 콘텐츠 필터 일치로 표시됩니다.

예를 들어, 메시지가 스팸 감염으로 표시되고 안티스팸 설정이 스팸 감염 메시지 삭제로 지정되면 메시지가 삭제되고 스팸 카운터가 증분됩니다. 뿐만 아니라 안티스팸 설정이 파이프라인에서 스팸 감염 메시지 계속 진행되도록 지정되고 후속 콘텐츠 필터가 메시지를 삭제, 바운스 또는 격리할 경우에도 스팸 카운트가 증분됩니다. 콘텐츠 필터 카운트는 메시지가 스팸 또는 바이러스 감염이 아닌 경우에만 증분됩니다.

수신 메일 페이지

수신 메일 페이지는 이메일 보안 모니터링 기능이 어플라이언스에 연결된 모든 원격 호스트에 대해 수집하는 실시간 정보를 보고하는 메커니즘을 제공합니다. 따라서 사용자에게 메일을 보내는 IP 주소, 도메인 및 조직(네트워크 소유자)에 대한 자세한 정보를 수집할 수 있습니다. 사용자에게 메일을 보낸 IP 주소, 도메인 또는 조직에 대한 발신자 프로필 검색을 수행할 수 있습니다.

수신 메일 페이지는 도메인, IP 주소, 네트워크 소유자의 3가지 보기로 구성되며 선택된 보기의 컨텍스트에서 시스템에 연결된 원격 호스트의 스냅샷을 제공합니다.

이 페이지는 어플라이언스에서 구성된 모든 공용 리스너에 메일을 보낸 상위 도메인(또는 보기에 따라 IP 주소나 네트워크 소유자)의 표(수신 메일 세부사항)를 표시합니다. 게이트웨이로 들어가는 모든 메일의 흐름을 모니터링할 수 있습니다. 발신자 프로필 페이지(클릭한 도메인/IP/네트워크 소유자에 해당하는 수신 메일 페이지)에서 도메인/IP/네트워크 소유자를 클릭하여 이 발신자에 대한 액세스 세부사항을 드릴다운할 수 있습니다.

사용 가능한 모든 열이 기본적으로 표시되는 것은 아닙니다. 표 아래에 있는 Columns(열) 링크를 클릭하여 다른 정보 집합을 표시할 수 있습니다. 예를 들어, 기본적으로 숨겨져 있는 "Advanced Malware Protection에 의해 탐지됨" 열을 표시할 수 있습니다.

수신 메일 페이지는 페이지 그룹(수신 메일, 발신자 프로필, 발신자 그룹 보고서)을 포함하도록 확장됩니다. **수신 메일** 페이지에서 다음을 수행할 수 있습니다.

- 사용자에게 메일을 보낸 IP 주소, 도메인 또는 조직(네트워크 소유자)에 대한 검색을 수행합니다.
- 발신자 그룹 보고서를 확인하여 특정 발신자 그룹 및 메일 흐름 정책 작업을 통한 연결을 봅니다. 자세한 내용은 발신자 그룹 보고서, 28-13페이지를 참조하십시오.
- 보안 서비스(발신자 평판 필터링, 안티스팸, 안티바이러스 등)가 분석을 시도한 메시지의 수를 포함하여 사용자에게 메일을 보낸 발신자에 대한 세부 통계를 봅니다.
- 안티스팸 또는 안티바이러스 보안 서비스를 통해 분석한 결과 대량의 스팸 또는 바이러스 이메일을 보낸 것으로 확인된 발신자를 기준으로 정렬합니다.
- SenderBase Reputation Service를 사용하여 특정 IP 주소, 도메인 및 조직 간의 관계를 드릴다운하고 검사해 발신자에 대한 자세한 정보를 얻을 수 있습니다.
- 특정 발신자를 드릴다운하여 SenderBase Reputation Service에서 발신자의 SenderBase Reputation 점수 및 가장 최근에 도메인과 일치한 발신자 그룹 등 발신자에 대한 자세한 정보를 얻을 수 있습니다. 발신자 그룹에 발신자를 추가합니다.
- 안티스팸 또는 안티바이러스 보안 서비스를 통해 분석한 결과 대량의 스팸 또는 바이러스 이메일을 보낸 것으로 확인된 특정 발신자를 드릴다운합니다.
- 일단 도메인에 대한 정보를 수집하면 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, 5-1페이지를 참조하십시오.

관련 주제

- 수신 메일, 28-10페이지
- 수신 메일 세부사항 목록, 28-10페이지

- 데이터로 채워진 보고 페이지: 발신자 프로필 페이지, 28-12페이지
- 발신자 그룹 보고서, 28-13페이지

수신 메일

수신 메일 페이지는 시스템에 구성된 모든 공용 리스너의 실시간 활동에 대한 액세스를 제공하며 수신된 상위 도메인을 요약하는 메일 트렌드 그래프(총 위협 메시지 및 총 클린 메시지별)와 수신 메일 세부사항 목록의 2가지 주요 섹션으로 구성됩니다.

수신 메일 세부사항 목록에 포함된 데이터의 설명은 수신 메일 세부사항 목록, 28-10페이지를 참조하십시오.

관련 주제

메일 트렌드 그래프의 시간 범위 관련 참고 사항, 28-10페이지

메일 트렌드 그래프의 시간 범위 관련 참고 사항

이메일 보안 모니터링 기능이 게이트웨이로 들어가는 메일에 대한 데이터를 지속적으로 기록합니다. 데이터는 60초마다 업데이트되지만, 나타나는 표시는 현재 시스템 시간보다 120초 지연됩니다. 표시되는 결과에 포함할 시간 범위를 지정할 수 있습니다. 데이터가 실시간으로 모니터링되므로 정보가 데이터베이스에서 정기적으로 업데이트 및 요약됩니다.

표 28-1에서 시간 범위 옵션을 선택합니다.

표 28-1 이메일 보안 모니터링 기능에서 사용할 수 있는 시간 범위

GUI에서 선택된 이 시간 범위	...다음으로 정의됨:
시	지난 60분 + 최대 5분
교육일	지난 24시간 + 지난 60분
주	지난 7일 + 현재 날짜의 경과된 시간
30일	지난 30일 + 현재 날짜의 경과된 시간
90일	지난 90일 + 현재 날짜의 경과된 시간
과거	00:00~23:59(자정~11:59 PM)
이전 달	해당 월의 첫날의 00:00~해당 월의 마지막 날의 23:59
사용자 지정 범위	시작 날짜 및 시간에서 사용자가 지정한 종료 날짜 및 시간까지의 범위

표시되는 시간 범위 옵션은 중앙 집중식 보고를 활성화한 경우 달라집니다. 자세한 내용은 42 장, "Cisco Content Security Management Appliance에서 서비스 중앙 집중화"의 중앙 집중식 보고 모드에 대한 정보를 참조하십시오.

수신 메일 세부사항 목록

어플라이언스의 공용 리스너에 연결된 상위 발신자는 선택한 보기에 따라 수신 메일 페이지 하단의 수신된 외부 도메인 목록 표에 나열됩니다. 데이터를 정렬하려면 열 머리글을 클릭합니다. 다양한 범주에 대한 설명은 이메일 분류, 28-8페이지를 참조하십시오.

시스템에서 *이중 DNS 조회*를 수행하여 원격 호스트의 IP 주소(즉, 도메인)를 얻고 그 유효성을 검사합니다. 이중 DNS 조회 및 발신자 확인에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 5-1페이지를 참조하십시오.

발신자 세부사항 목록은 요약 보기와 모두 보기의 2가지 보기로 표시할 수 있습니다.

기본 발신자 세부사항 보기는 각 발신자가 시도한 총 메시지 수를 표시하며 범주(개요 페이지의 수신 메일 요약 그래프와 동일한 범주)별 분석을 포함합니다.

평판 필터링에 의해 중지됨의 값은 다음과 같은 여러 요소에 따라 계산됩니다.

- 이 발신자가 보낸 "제한된" 메시지의 수

- 거부된 연결 또는 거부된 TCP 연결 수(부분적으로 계산될 수 있음)

- 연결당 메시지 수에 대한 보수적인 승수

어플라이언스의 작업량이 너무 많을 경우 거부된 정확한 연결 수가 발신자 기준으로 유지되지 않습니다. 그 대신 거부된 연결 수는 각 시간 간격에서 가장 중요한 발신자에 대해서만 유지됩니다. 이 경우 표시된 값이 "바닥"으로 해석될 수 있습니다. 다시 말해서, 최소한 이 많은 메시지가 중단되었습니다.

참고 개요 페이지의 평판 필터링에 의해 중지된 총 메시지 수는 항상 거부된 모든 연결의 전체 수를 기준으로 합니다. 발신자당 연결 수만 로드로 인해 제한됩니다.

표시할 수 있는 추가 열은 다음과 같습니다.

거부된 연결: HAT 정책에 의해 차단된 모든 연결. 어플라이언스의 작업량이 너무 많을 경우 거부된 정확한 연결 수가 발신자 기준으로 유지되지 않습니다. 그 대신 거부된 연결 수는 각 시간 간격에서 가장 중요한 발신자에 대해서만 유지됩니다.

수락된 연결: 수락된 모든 연결

수신자 제한에 의해 중지됨: 이는 평판 필터링에 의해 중지됨의 구성 요소입니다. 다음과 같은 HAT 제한 즉, 시간당 최대 수신자, 메시지당 최대 수신자 또는 연결당 최대 메시지 중 하나가 초과되었으므로 이는 중지된 수신자 메시지 수를 나타냅니다. 이는 평판 필터링에 의해 중지됨을 얻기 위해 거부된 연결 또는 거부된 TCP 연결과 관련된 수신자 메시지 추정치를 합한 값입니다.

Advanced Malware Protection에 의해 탐지됨: 파일 평판 필터링에 의해 악성으로 발견된 첨부 파일이 있는 메시지입니다. 이 값은 파일 분석에 의해 악성으로 발견된 판정 업데이트 또는 파일을 포함하지 않습니다.

총 위협: 총 위협 메시지(발신자 평판에 의해 중지됨 또는 잘못된 수신자, 스팸, 바이러스로 중지됨).

표 하단의 Columns(열) 링크를 클릭하여 열을 표시하거나 숨깁니다.

열 헤더 링크를 클릭하여 목록을 정렬합니다. 열 헤더 옆에 있는 작은 삼각형은 데이터가 현재 정렬되어 있음을 나타냅니다.

관련 주제

- "도메인 정보 없음", 28-11페이지
- 추가 정보 쿼리, 28-12페이지

"도메인 정보 없음"

어플라이언스에 연결되었으나 이중 DNS 조회로 확인할 수 없는 도메인은 자동으로 특수 도메인 "도메인 정보 없음"으로 그룹화됩니다. 이러한 유형의 확인되지 않은 호스트가 발신자 확인을 통해 관리되는 방식을 제어할 수 있습니다. 이메일을 수신하도록 게이트웨이 구성, 5-1페이지를 참조하십시오.

표시된 항목 메뉴를 통해 목록에 표시할 발신자의 수를 선택할 수 있습니다.

추가 정보 쿼리

이메일 보안 모니터링 표에 나열된 발신자의 경우 발신자(또는 "No Domain Information(도메인 정보 없음)" 링크)를 클릭하여 특정 발신자에 대한 자세한 정보를 드릴다운할 수 있습니다. 결과는 SenderBase Reputation Service의 실시간 정보를 포함하는 발신자 프로필 페이지에 표시됩니다. 발신자 프로필 페이지에서 특정 IP 주소 또는 네트워크 소유자에 대한 자세한 정보를 드릴다운할 수 있습니다(데이터로 채워진 보고 페이지: 발신자 프로필 페이지, 28-12페이지 참조).

또한 수신 메일 페이지의 하단에 있는 발신자 그룹 보고서를 클릭하여 다른 보고서인 발신자 그룹 보고서를 볼 수 있습니다. 발신자 그룹 보고서에 대한 자세한 내용은 발신자 그룹 보고서, 28-13페이지를 참조하십시오.

데이터로 채워진 보고 페이지: 발신자 프로필 페이지

수신 메일 페이지의 수신 메일 세부사항 표에서 발신자를 클릭하면 특정 IP 주소, 도메인 또는 조직(네트워크 소유자)에 대한 데이터가 포함된 *발신자 프로필 페이지*가 표시됩니다. 발신자 프로필 페이지에는 발신자에 대한 자세한 정보가 표시됩니다. 수신 메일 또는 기타 발신자 프로필 페이지에서 지정된 항목을 클릭하여 모든 네트워크 소유자, 도메인 또는 IP 주소에 대한 발신자 프로필 페이지에 액세스할 수 있습니다. 네트워크 소유자는 도메인을 포함하는 엔터티이고, 도메인은 IP 주소를 포함하는 엔터티입니다. 이 관계와 SenderBase Reputation Service와의 연관성에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 5-1페이지를 참조하십시오.

IP 주소, 네트워크 소유자 및 도메인에 대해 표시되는 발신자 프로필 페이지는 약간 다릅니다. 각 항목의 페이지에는 이 발신자에게서 수신되는 메일에 대한 그래프 및 요약 표가 포함되어 있습니다. 그래프 아래에는 발신자와 연결된 도메인 또는 IP 주소가 나열된 표(개별 IP의 발신자 프로필 페이지에는 자세한 목록이 포함되지 않음)와 현재 SenderBase, 발신자 그룹, 발신자의 네트워크 정보가 포함된 정보 섹션이 있습니다.

- 네트워크 소유자 프로필 페이지에는 해당 네트워크 소유자와 연결된 도메인 및 IP 주소뿐 아니라 해당 네트워크 소유자에 대한 정보가 포함됩니다.
- 도메인 프로필 페이지에는 해당 도메인과 연계된 도메인 및 IP 주소에 대한 정보가 포함됩니다.
- IP 주소 프로필 페이지에는 IP 주소에 대한 정보만 포함됩니다.

각 발신자 프로필 페이지는 페이지 하단의 현재 정보 표에 다음과 같은 정보를 포함합니다.

- 다음을 포함한 SenderBase Reputation Service의 **전체** 정보:
  - IP 주소, 도메인 이름 및/또는 네트워크 소유자
  - 네트워크 소유자 범주(네트워크 소유자만 해당)
  - CIDR 범위(IP 주소만 해당)
  - IP 주소, 도메인 및/또는 네트워크 소유자에 대한 일일 발송 규모 및 월간 발송 규모
  - 이 발신자에게서 첫 번째 메시지가 수신된 이후에 경과한 일수
  - 마지막 발신자 그룹 및 DNS 확인 여부(IP 주소 발신자 프로필 페이지만 해당)

  일일 발송 규모는 지난 24시간 동안 도메인에서 보낸 메시지 수의 척도입니다. 지진을 측정하는 리히터 척도와 유사하게 SenderBase 발송 규모는 10 단위의 로그 눈금을 사용하여 계산된 메시지 볼륨의 척도입니다. 눈금의 최대 이론값은 전 세계 이메일 메시지 볼륨(약 100억 개 메시지/일)의 100%에 해당하는 10으로 설정됩니다. 로그 눈금을 사용할 경우 발송 규모에서 1점 증가는 실제 볼륨에서 10배 증가한 것과 동일합니다.

  월간 발송 규모는 지난 30일 동안 전송된 이메일의 볼륨을 기준으로 비율이 계산되는 것을 제외하고 일일 발송 규모와 동일한 접근 방식을 사용하여 계산됩니다.

  - 평균 발송 규모(IP 주소만 해당)
  - 수명 볼륨/30일 볼륨(IP 주소 프로필 페이지만 해당)

  - 결합된 발신자 상태(IP 주소 프로필 페이지만 해당)
  - SenderBase Reputation 점수(IP 주소 프로필 페이지만 해당)
  - 첫 번째 메시지 이후에 경과한 일수(네트워크 소유자 및 도메인 프로필 페이지만 해당)
  - 이 네트워크 소유자와 연결된 도메인 수(네트워크 소유자 및 도메인 프로필 페이지만 해당)
  - 이 네트워크 소유자의 IP 주소 수(네트워크 소유자 및 도메인 프로필 페이지만 해당)
  - 이메일 전송에 사용되는 IP 주소 수(네트워크 소유자 페이지만 해당)

  SenderBase Reputation Service에서 제공된 모든 정보가 있는 페이지를 보려면 "More from SenderBase(SenderBase의 정보 더 보기)" 링크를 클릭합니다.

- 사용자가 지정한 시간 범위를 초과하는 발신자에 대해 수집된 이메일 보안 모니터링 정보를 포함한 **메일 흐름 통계**.
- 이 네트워크 소유자가 제어하는 도메인과 IP 주소에 대한 **세부사항**이 네트워크 소유자 프로필 페이지에 표시됩니다. 도메인의 IP 주소에 대한 세부사항이 도메인 페이지에 표시됩니다.

도메인 프로필 페이지에서 특정 IP 주소를 드릴다운하거나 드릴업하여 조직 프로필 페이지를 볼 수 있습니다. 또한 해당 표 하단의 Columns(열) 링크를 클릭하여 DNS 확인 상태, SBRS(SenderBase Reputation 점수), IP 주소 표의 각 발신자 주소의 마지막 발신자 그룹을 표시할 수 있습니다. 뿐만 아니라 해당 표의 열을 숨길 수 있습니다.

네트워크 소유자 프로필 페이지에서 해당 표 하단의 Columns(열) 링크를 클릭하여 도메인 표에 있는 각 도메인의 연결 거부, 연결 승인, 수신자 제한의 의해 중지됨, Advanced Malware Protection에 의해 탐지됨과 같은 정보를 표시할 수 있습니다. 뿐만 아니라 해당 표의 열을 숨길 수 있습니다.

시스템 관리자인 경우 이러한 각 페이지에서 해당 엔터티의 확인란(필요한 경우)을 클릭한 다음 Add to Sender Group(발신자 그룹에 추가)을 클릭하여 발신자 그룹에 네트워크 소유자, 도메인 또는 IP 주소를 추가할 수 있습니다.

또한 발신자의 현재 정보 표에 있는 발신자 그룹 정보 아래의 **Add to Sender Group(발신자 그룹에 추가)** 링크를 클릭한 다음 Add to Sender Group(발신자 그룹에 추가)을 클릭하여 발신자 그룹에 발신자를 추가할 수 있습니다. 발신자 그룹에 발신자를 추가하는 방법에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 5-1페이지를 참조하십시오. 물론 보안 서비스로 수신 메일을 처리할 수 있으므로 사용자가 따로 변경할 필요가 없습니다.

관련 주제

- 발신자 프로필 검색, 28-13페이지

발신자 프로필 검색

특정 발신자를 검색하려면 빠른 검색 상자에 IP 주소, 도메인 또는 조직 이름을 입력합니다.

발신자 프로필 페이지에는 발신자에 대한 정보가 표시됩니다. 데이터로 채워진 보고 페이지: 발신자 프로필 페이지, 28-12페이지를 참조하십시오.

발신자 그룹 보고서

발신자 그룹 보고서는 발신자 그룹과 메일 흐름 정책 작업별로 연결의 요약을 제공하므로 SMTP 연결 및 메일 흐름 정책 트렌드를 검토할 수 있습니다. 발신자 그룹별 메일 흐름 목록에는 각 발신자 그룹에 대한 연결의 비율과 수가 표시됩니다. 메일 흐름 정책 작업별 연결 차트에는 각 메일 흐름 정책 작업에 대한 연결의 비율이 표시됩니다. 이 페이지에서는 HAT(Host Access Table) 정책의 효율성에 대한 개요를 제공합니다. HAT에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성, 5-1페이지를 참조하십시오.

발송 대상

발송 대상 페이지에서는 귀사에서 메일을 보내는 도메인에 대한 정보를 제공합니다. 이 페이지는 2개의 섹션으로 구성됩니다. 페이지의 상단은 위협 메시지 발송별 상위 대상과 클린 메시지 발송별 상위 대상을 보여주는 그래프로 구성됩니다. 페이지의 하단에는 총 수신자를 기준으로 정렬된 모든 열을 보여주는 차트가 표시됩니다(기본 설정).

시간, 주 또는 사용자 지정 범위 등 보고할 시간 범위를 선택할 수 있습니다. 모든 보고서와 마찬가지로 **Export(내보내기)** 링크를 통해 그래프 또는 세부사항 목록의 데이터를 CSV 형식으로 내보낼 수 있습니다.

발송 대상 페이지는 다음과 같은 유형의 질문에 답변하는 데 사용할 수 있습니다.

- 어플라이언스가 어떤 도메인에 메일을 보냅니까?
- 각 도메인에 얼마나 많은 메일이 전송됩니까?
- 그러한 메일 중 클린 메일, 스팸 감염 메일, 바이러스 감염 메일 또는 콘텐츠 필터에 의해 중지된 메일은 얼마입니까?
- 전송되는 메시지와 대상 서버에 의해 하드 바운스되는 메시지는 얼마입니까?

발송 발신자

발송 발신자 페이지에서는 사용자 네트워크의 IP 주소와 도메인에서 전송되는 메일의 수량과 유형에 대한 정보를 제공합니다. 이 페이지를 볼 때 도메인 또는 IP 주소별로 결과를 볼 수 있습니다. 각 도메인에서 보내는 메일의 볼륨을 보려는 경우 도메인별로 결과를 볼 수 있으며, 어떤 IP 주소에서 가장 많은 바이러스 메시지를 보내거나 콘텐츠 필터를 트리거하는지 확인하려는 경우 IP 주소별로 결과를 볼 수 있습니다.

이 페이지는 2개의 섹션으로 구성됩니다. 페이지의 왼쪽에는 총 위협 메시지별 상위 발신자를 보여주는 그래프가 있습니다. 총 위협 메시지에는 스팸 또는 바이러스에 감염되었거나 콘텐츠 필터를 트리거한 메시지가 포함됩니다. 페이지의 오른쪽에는 페이지 상단에 클린 메시지별 상위 발신자를 표시하는 그래프가 있습니다. 페이지의 하단에는 총 메시지를 기준으로 정렬된 모든 열을 표시하는 차트가 표시됩니다.

참고 이 페이지에서는 메시지 전송에 대한 정보를 표시하지 않습니다. 전송 상태 페이지를 사용하여 특정 도메인의 메시지가 바운스된 수와 같은 전송 정보를 추적할 수 있습니다.

시간, 주 또는 사용자 지정 범위 등 보고할 시간 범위를 선택할 수 있습니다. 모든 보고서와 마찬가지로 **Export(내보내기)** 링크를 통해 그래프 또는 세부사항 목록의 데이터를 CSV 형식으로 내보낼 수 있습니다.

발송 발신자 페이지를 사용해 다음과 같은 유형의 질문에 답변할 수 있습니다.

- 어떤 IP 주소에서 가장 많은 바이러스 또는 스팸 감염 이메일을 전송합니까?
- 어떤 IP 주소가 콘텐츠 필터를 가장 자주 트리거합니까?
- 어떤 도메인에서 가장 많은 메일을 전송합니까?

전송 상태 페이지

특정 수신자 도메인에 전송 문제가 있다고 의심되거나 가상 게이트웨이에 대한 정보를 수집하려는 경우 Monitor(모니터링) > Delivery Status(전송 상태) 페이지에서 특정 수신자 도메인과 관련된 이메일 작업에 대한 모니터링 정보를 제공합니다.

전송 상태 페이지에는 CLI 내의 `tophosts` 명령과 동일한 정보가 표시됩니다. (자세한 내용은 34 장, "CLI를 통한 관리 및 모니터링"의 '이메일 큐 구성 결정' 참조)

이 페이지에는 지난 3시간 이내에 시스템에서 전송한 메시지의 상위 20, 50 또는 100개의 수신자 도메인 목록이 표시됩니다. 각 통계의 열 머리글에 있는 링크를 클릭하여 최신 호스트 상태, 활성 수신자(기본값), 연결, 전송된 수신자, 소프트 바운스된 이벤트 및 하드 바운스된 수신자를 기준으로 정렬할 수 있습니다.

- 특정 도메인을 검색하려면 도메인 이름: 필드에 해당 도메인의 이름을 입력하고 **Search(검색)**를 클릭합니다.
- 표시된 도메인을 드릴다운하려면 도메인 이름 링크를 클릭합니다

결과가 전송 상태 세부사항 페이지에 표시됩니다.

참고 수신자 도메인의 모든 활동으로 인해 해당 도메인이 "활성" 상태가 되므로 개요 페이지에 표시됩니다. 예를 들어, 메일이 전송 문제로 인해 아웃바운드 큐에 남아 있는 경우 해당 수신자 도메인이 발송 메일 개요에 계속 표시됩니다.

관련 주제

- 전송 다시 시도, 28-15페이지
- 전송 상태 세부사항 페이지, 28-15페이지

전송 다시 시도

Retry All Delivery(모든 전송 다시 시도)를 클릭하여 나중에 전송되도록 예약된 메시지가 즉시 다시 시도되도록 할 수 있습니다. Retry All Delivery(모든 전송 다시 시도)를 사용하여 즉시 전송되도록 큐의 메시지를 다시 예약할 수 있습니다. "다운"으로 표시된 모든 도메인과 예약되거나 소프트 바운스된 메시지가 즉시 전송 대기 상태로 전환됩니다.

특정 대상 제어로 다시 전송을 시도하려면 도메인 이름 링크를 클릭합니다. 전송 상태 세부사항 페이지에서 **Retry Delivery(전송 다시 시도)**를 클릭합니다.

또한 CLI에서 `delivernow` 명령을 사용하여 즉시 전송되도록 메시지를 다시 예약할 수 있습니다. 자세한 내용은 즉시 전달을 위한 이메일 예약, 34-31페이지를 참고하십시오.

전송 상태 세부사항 페이지

전송 상태 세부사항 페이지를 사용하여 특정 수신자 도메인에 대한 통계를 조회할 수 있습니다. 이 페이지에는 CLI 내의 `hoststatus` 명령과 동일한 정보인 메일 상태, 카운터 및 게이지가 표시됩니다. (자세한 내용은 "메일 호스트 상태 모니터링"(34 장, "CLI를 통한 관리 및 모니터링") 참조) 특정 도메인을 검색하려면 도메인 이름: 필드에 도메인의 이름을 입력하고 **Search(검색)**를 클릭합니다. `altsrchost` 기능을 사용하는 경우 가상 게이트웨이 주소 정보가 나타납니다.

내부 사용자 페이지

내부 사용자 페이지에서는 내부 사용자가 보내거나 받은 메일에 대한 정보를 *이메일 주소별로* 제공합니다(단일 사용자가 여러 개의 이메일 주소를 표시할 수 있으며 이러한 이메일 주소는 보고서에 통합되지 않음).

이 페이지는 클린 수신 및 발송 메시지별 상위 사용자를 보여주는 그래프와 사용자 메일 흐름 세부사항의 2가지 섹션으로 구성됩니다. 보고할 시간 범위(시간, 일, 주 또는 월)를 선택할 수 있습니다. 모든 보고서와 마찬가지로 **Export(내보내기)** 링크를 통해 그래프 또는 세부사항 목록의 데이터를 CSV 형식으로 내보낼 수 있습니다. 또한 표 아래의 Columns(열) 링크를 클릭하여 숨겨진 표 열을 표시하거나 기본 열을 숨길 수 있습니다.

사용자 메일 흐름 세부사항 목록은 각 메일 주소에서 수신 및 전송된 메일을 클린 메일, 스팸으로 탐지된 메일(수신만 해당), 바이러스로 탐지된 메일, 콘텐츠 필터 일치 메일로 분류합니다. 열 헤더를 클릭하여 목록을 정렬할 수 있습니다.

내부 사용자 보고서를 사용하여 다음과 같은 종류의 질문에 답변할 수 있습니다.

- 누가 가장 많은 외부 이메일을 보냅니까?
- 누가 가장 많은 클린 이메일을 받습니까?
- 누가 가장 많은 스팸을 받습니까?
- 누가 어떤 콘텐츠 필터를 트리거합니까?
- 누구의 이메일이 콘텐츠 필터에 걸립니까?

인바운드 내부 사용자는 받는 사람: 주소를 기반으로 사용자가 이메일을 받은 사용자입니다. 아웃바운드 내부 사용자는 보낸 사람: 주소를 기반으로 하며 내부 네트워크의 발신자가 보내는 이메일의 유형을 추적할 때 유용합니다.

일부 아웃바운드 메일에는 null 발신자가 있습니다. 이러한 발신자는 아웃바운드 및 "알 수 없는" 발신자로 계산됩니다.

해당 사용자의 내부 사용자 세부사항 페이지를 보려면 내부 사용자를 클릭합니다.

Advanced Malware Protection에 의해 탐지된 수신 메시지 열과 같은 기본적으로 숨겨진 열을 표시하려면 표 아래의 Columns(열) 링크를 클릭합니다.

관련 주제

- 내부 사용자 세부사항, 28-16페이지
- 특정 내부 사용자 검색, 28-17페이지

내부 사용자 세부사항

내부 사용자 세부사항 페이지에는 각 범주(스팸으로 탐지된 메시지, 바이러스로 탐지된 메시지, 콘텐츠 필터에 의해 중지된 메시지, 클린 메시지)의 메시지 수를 보여주는 수신 및 발송 메시지 분석을 포함하여 지정된 사용자에 대한 자세한 정보가 표시됩니다. 또는 수신 메시지의 경우 표 아래의 Columns(열) 링크를 클릭하여 Advanced Malware Protection에 의해 탐지된 수신 메시지 열을 표시할 수 있습니다. 이 값은 파일 평판 필터링에 의해 악성으로 확인된 첨부 파일을 포함한 메시지의 수를 반영합니다. 파일 분석에 의해 악성으로 발견된 판정 업데이트 또는 파일은 포함하지 않습니다. 수신 및 발송 콘텐츠 필터와 DLP 정책도 표시됩니다.

해당 콘텐츠 필터 정보 페이지에서 해당 필터의 자세한 정보를 보려면 콘텐츠 필터 이름을 클릭합니다(콘텐츠 필터 페이지, 28-18페이지 참조). 이 방법을 사용하여 특정 콘텐츠 필터와 일치하는 메일을 보내거나 받은 사용자의 목록을 가져올 수도 있습니다.

특정 내부 사용자 검색

내부 사용자 페이지와 내부 사용자 세부사항 페이지의 하단에 있는 검색 양식을 통해 특정 내부 사용자(이메일 주소)를 검색할 수 있습니다. 검색 텍스트와 정확하게 일치하는지 여부를 선택하거나 입력한 텍스트로 시작하는 항목(예를 들어, "ex"로 시작하는 항목은 "example.com"과 일치함)을 검색합니다.

DLP 사고 페이지

DLP 사고 페이지에는 발송 메일에서 발생하는 DLP(데이터 유출 방지) 정책 위반에 대한 정보가 표시됩니다. 이 어플라이언스는 발송 메일 정책 표에서 활성화된 DLP 이메일 정책을 사용하여 사용자가 보낸 민감한 데이터를 탐지합니다. DLP 정책을 위반하는 발송 메시지의 발생은 모두 사고로 보고됩니다.

DLP 시건 보고서를 사용하여 다음과 같은 종류의 질문에 답변할 수 있습니다.

- 사용자가 어떤 유형의 민감한 데이터를 보냅니까?
- 이러한 DLP 사고가 얼마나 심각합니까?
- 이러한 메시지 중 몇 개가 전송됩니까?
- 이러한 메시지 중 몇 개가 삭제됩니까?
- 누가 이러한 메시지를 보냅니까?

DLP 사고 페이지는 다음 2개의 섹션으로 구성됩니다.

- 심각도(낮음, 중간, 높음, 위험) 및 정책 일치를 기준으로 상위 DLP 사고를 요약하는 DLP 사고 트렌드 그래프
- DLP 사고 세부사항 목록

시간, 주 또는 사용자 지정 범위 등 보고할 시간 범위를 선택할 수 있습니다. 모든 보고서와 마찬가지로 **Export(내보내기)** 링크를 통해 그래프 또는 세부사항 목록의 데이터를 CSV 형식으로 내보내거나 **Printable (PDF)(인쇄 가능(PDF))** 링크를 클릭하여 PDF 형식으로 내보낼 수 있습니다. 영어가 아닌 다른 언어로 PDF를 생성하는 방법에 대한 내용은 "보고서에 대한 참고사항" 섹션, 28-34페이지를 참조하십시오.

정책에서 탐지된 DLP 사고에 대한 자세한 정보를 보려면 DLP 정책의 이름을 클릭합니다. 이 방법을 사용하여 정책에서 탐지된 민감한 데이터가 포함된 메일을 보낸 사용자의 목록을 가져올 수 있습니다.

관련 주제

- DLP 사고 세부사항, 28-17페이지
- DLP 정책 세부사항 페이지, 28-18페이지

DLP 사고 세부사항

현재 어플라이언스의 발송 메일 정책에서 활성화된 DLP 정책은 DLP 사고 페이지의 하단에 있는 DLP 사고 세부사항 표에 나열됩니다. 보다 자세한 정보를 보려면 DLP 정책의 이름을 클릭합니다.

DLP 사고 세부사항 표에는 심각도 수준에 따라 분류된 정책당 총 DLP 사고 수와 암호화되지 않은 상태로 전송되거나, 암호화되어 전송되거나, 삭제된 메시지 수가 표시됩니다. 데이터를 정렬하려면 열 머리글을 클릭합니다.

DLP 정책 세부사항 페이지

DLP 사고 세부사항 표에서 DLP 정책의 이름을 클릭하면 DLP 정책 세부사항 페이지에 해당 정책의 DLP 사고 데이터가 표시됩니다. 이 페이지에는 심각도에 따라 DLP 사고를 보여주는 그래프가 표시됩니다.

이 페이지의 하단에는 DLP 정책을 위반한 메시지를 보낸 각 내부 사용자를 나열하는 발신자별 사고 목록도 포함되어 있습니다. 이 목록에서는 심각도 수준과 메시지가 암호화되지 않은 상태로 전송되었는지, 암호화된 상태로 전송되었는지 또는 삭제되었는지 여부를 기준으로 메시지를 분류하며 사용자당 이 정책의 총 DLP 사고 수도 표시합니다. 발신자별 사고 목록을 사용하여 네트워크 외부의 사람들에게 조직의 민감한 데이터를 보낼 가능성이 있는 사람을 찾아낼 수 있습니다.

발신자 이름을 클릭하면 내부 사용자 페이지가 열립니다. 자세한 내용은 내부 사용자 페이지, 28-16 페이지를 참조하십시오.

콘텐츠 필터 페이지

콘텐츠 필터 페이지에는 상위 수신 및 발송 센터 필터 일치(가장 일치하는 메시지가 있는 콘텐츠 필터)에 대한 정보가 막대 그래프와 목록의 2가지 형식으로 표시됩니다. 콘텐츠 필터 페이지를 사용하여 콘텐츠 필터 또는 사용자 단위로 기업 정책을 검토하고 다음과 같은 질문에 답변할 수 있습니다.

- 수신 또는 발송 메일로 인해 가장 많이 트리거되는 콘텐츠 필터는 무엇입니까?
- 특정 콘텐츠 필터를 트리거하는 메일을 보내거나 받는 상위 사용자는 누구입니까?

콘텐츠 필터 세부사항 페이지에서 필터에 대한 자세한 정보를 보려면 목록에서 해당 콘텐츠 필터의 이름을 클릭하면 됩니다.

관련 주제

- 콘텐츠 필터 세부사항, 28-18페이지

콘텐츠 필터 세부사항

콘텐츠 필터 세부사항 페이지에는 내부 사용자별 일치뿐 아니라 시간 경과에 따른 해당 필터의 일치가 표시됩니다.

내부 사용자별 일치 섹션에서 사용자 이름을 클릭하면 해당 내부 사용자의 (이메일 주소) 내부 사용자 세부사항 페이지를 볼 수 있습니다(내부 사용자 세부사항, 28-16페이지 참조).

DMARC 확인 페이지

DMARC 확인 페이지에는 DMARC 확인이 실패한 상위 도메인과 DMARC 확인이 실패한 메시지에 대해 수행된 AsyncOS 작업에 대한 세부사항이 표시됩니다. 이 보고서를 사용하여 DMARC 설정을 세부적으로 조정하고 다음과 같은 종류의 질문에 답변할 수 있습니다.

- DMARC에 부합하지 않는 메시지를 가장 많이 보낸 도메인은 무엇입니까?
- 각 도메인의 경우 DMARC 확인이 실패한 메시지에 대해 어떤 AsyncOS 작업이 수행되었습니까?

DMARC 확인 페이지에는 다음과 같은 내용이 포함됩니다.

- DMARC 확인 실패를 기준으로 상위 도메인을 보여주는 막대 그래프
- 각 도메인에 대해 다음과 같은 내용을 표시한 표
  - 작업 없이 거부, 격리 또는 수락된 메시지 수 선택한 범주의 메시지 목록을 보려면 숫자를 클릭합니다.

- DMARC 확인을 통과한 메시지 수
- 총 DMARC 확인 시도 횟수

시간, 주 또는 사용자 지정 범위 등 보고할 시간 범위를 선택할 수 있습니다. 모든 보고서와 마찬가지로 **Export(내보내기)** 링크를 통해 그래프 또는 세부사항 목록의 데이터를 CSV 형식으로 내보내거나 **Printable (PDF)(인쇄 가능(PDF))** 링크를 클릭하여 PDF 형식으로 내보낼 수 있습니다.

신종 바이러스 필터(Outbreak Filter) 페이지

신종 바이러스 필터(Outbreak Filter) 페이지에서는 최근에 신종 바이러스 필터(Outbreak Filter)로 인해 격리된 신종 바이러스 및 메시지에 대한 정보뿐 아니라 어플라이언스의 신종 바이러스 필터(Outbreak Filter)의 현재 상태 및 구성도 보여줍니다. 이 페이지를 사용하여 표적 바이러스, 스캠 및 피싱 공격에 대한 방어를 모니터링할 수 있습니다.

유형별 위협 섹션에는 어플라이언스에서 수신한 다양한 유형의 위협 메시지가 표시됩니다.

위협 요약 섹션에는 맬웨어, 피싱, 스캠, 바이러스별로 분류된 위협 메시지가 표시됩니다. 메시지 추적을 사용하여 해당 숫자에 포함된 모든 메시지의 목록을 보려면 숫자를 클릭합니다.

이전 연도 신종 바이러스 요약에는 지난 해의 로컬 신종 바이러스뿐 아니라 전역 신종 바이러스도 표시되므로 로컬 네트워크 트렌드와 전역 트렌드를 비교할 수 있습니다. 전역 신종 바이러스 목록은 바이러스와 비 바이러스를 포함한 모든 신종 바이러스의 상위 집합인 반면, 로컬 신종 바이러스는 사용자의 어플라이언스에 영향을 미친 신종 바이러스로 제한됩니다. 로컬 신종 바이러스 데이터에는 비 바이러스 위협이 포함되지 않습니다. 전역 신종 바이러스 데이터는 Threat Operations Center에서 탐지한, 현재 구성된 신종 바이러스 격리 임계값을 초과한 모든 신종 바이러스를 나타냅니다. 로컬 신종 바이러스 데이터는 이 어플라이언스에서 탐지된, 현재 구성된 신종 바이러스 격리 임계값을 초과한 모든 신종 바이러스를 나타냅니다. 총 로컬 보호 시간은 항상 Threat Operations Center에서 각 신종 바이러스를 탐지한 시간과 주요 공급업체에서 안티바이러스 서명을 한 시간 사이의 차이를 기반으로 합니다. 모든 전역 신종 바이러스가 어플라이언스에 영향을 미치는 것은 아닙니다. "--" 값은 보호 시간이 존재하지 않거나 안티바이러스 공급업체에서 서명 시간을 사용할 수 없었음을 나타냅니다(일부 공급업체가 서명 시간을 보고하지 않을 수 있음). 이는 보호 시간이 0이라는 의미보다는 보호 시간을 계산하는 데 필요한 정보를 사용할 수 없다는 의미입니다.

격리된 메시지 섹션은 신종 바이러스 필터(Outbreak Filter) 격리를 요약하며 신종 바이러스 격리 필터에 포착되는 잠재적인 위협 메시지의 수를 알 수 있는 유용한 게이지입니다. 격리된 메시지는 릴리스 시에 계산됩니다. 일반적으로 메시지는 안티바이러스 및 안티스팸 규칙이 사용되기 전에 격리됩니다. 메시지가 릴리스되면 안티바이러스 및 안티스팸 소프트웨어에서 이를 검사하여 감염인지 클린인지 결정합니다. 신종 바이러스 추적의 동적인 특성으로 인해 메시지와 심지어 관련 신종 바이러스가 격리되는 규칙이 변경될 수 있습니다. 격리에 들어가는 시점이 아닌 릴리스 시점에 메시지를 계산함으로써 카운트를 늘리거나 줄이는 혼동을 피할 수 있습니다.

위협 세부사항 목록에는 위협 범주(바이러스, 스캠 또는 피싱), 위협 이름, 위협에 대한 설명, 확인된 메시지 수를 포함한 특정 신종 바이러스에 대한 정보가 표시됩니다. 신종 바이러스의 경우 이전 연도 신종 바이러스에 신종 바이러스 이름 및 ID, 신종 바이러스가 전역에서 처음으로 발견된 날짜 및 시간, 신종 바이러스 필터(Outbreak Filter)에서 제공한 보호 시간, 격리된 메시지 수가 포함됩니다. 왼쪽의 메뉴를 통해 표시할 메시지의 수뿐 아니라 전역 또는 로컬 신종 바이러스도 선택할 수 있습니다. 열 헤더를 클릭하여 목록을 정렬할 수 있습니다. 메시지 추적을 사용하여 해당 숫자에 포함된 모든 메시지의 목록을 보려면 숫자를 클릭합니다.

전역에서 처음으로 발견된 시간은 세계에서 가장 큰 이메일 및 웹 트래픽 모니터링 네트워크인 Threat Operations Center에서 결정합니다. 보호 시간은 Threat Operations Center에서 각 위협을 탐지한 시간과 주요 공급업체에서 안티바이러스 서명을 한 시간 사이의 차이를 기반으로 합니다.

"--" 값은 보호 시간이 존재하지 않거나 안티바이러스 공급업체에서 서명 시간을 사용할 수 없었음을 나타냅니다(일부 공급업체가 서명 시간을 보고하지 않을 수 있음). 이는 보호 시간이 0이라는 의미가 아닙니다. 그보다는 보호 시간을 계산하는 데 필요한 정보를 사용할 수 없다는 의미입니다.

수신 메시지의 적중 메시지 섹션에는 바이러스 첨부 파일, 기타 위협(비 바이러스), 클린 수신 메시지의 수와 비율이 표시됩니다.

위협 수준별 적중 메시지 섹션에는 위협 수준(수준 1~5)에 따른 수신 위협 메시지(바이러스 및 비 바이러스)의 수와 비율이 표시됩니다.

신종 바이러스 격리에 상주하는 메시지 섹션에는 해당 기간을 기준으로 신종 바이러스 위협에 상주하는 위협 메시지의 수가 표시됩니다.

상위 URL의 재작성 섹션에는 발생 수를 기준으로 재작성된 상위 10개 URL의 목록이 표시됩니다. 항목 사용 드롭다운을 사용하여 재작성된 추가 URL을 볼 수 있습니다. 메시지 추적 페이지에서 선택한 재작성된 URL을 포함하는 모든 메시지의 목록을 보려면 숫자를 클릭합니다.

신종 바이러스 필터(Outbreak Filter) 페이지를 사용하여 다음과 같은 질문에 답변할 수 있습니다.

- 얼마나 많은 메시지가 격리되며 그러한 메시지의 위협 유형은 무엇이었습니까?
- 신종 바이러스 필터(Outbreak Filter) 기능이 신종 바이러스에 대해 제공한 리드 타임은 얼마였습니까?
- 내 로컬 신종 바이러스와 전역 신종 바이러스를 비교하려면 어떻게 해야 합니까?

바이러스 유형 페이지

바이러스 유형 페이지에서는 네트워크에서 입력 및 전송되는 바이러스에 대한 개요를 제공합니다. 바이러스 유형 페이지에는 어플라이언스에서 실행되는 바이러스 검사 엔진이 탐지한 바이러스가 표시됩니다. 이 보고서를 사용하여 특정 바이러스에 대해 특정 작업을 수행할 수 있습니다. 예를 들어, PDF 파일에 내장된다고 알려진 대량의 바이러스를 수신하고 있는지 확인하려면 PDF 첨부 파일이 포함된 메시지를 격리하는 필터 작업을 생성할 수 있습니다.

여러 바이러스 검사 엔진을 실행하는 경우 바이러스 유형 페이지에 활성화된 모든 바이러스 검사 엔진의 결과가 포함됩니다. 이 페이지에 표시된 바이러스의 이름은 바이러스 검사 엔진에서 정한 이름입니다. 2개 이상의 검사 엔진에서 바이러스를 탐지한 경우 동일한 바이러스에 대한 항목이 2개 이상 있을 수 있습니다.

바이러스 유형 페이지에서는 네트워크에서 입력하거나 전송 또는 수신하는 바이러스의 개요를 제공합니다. 탐지된 상위 수신 바이러스 섹션에는 네트워크에 전송된 바이러스의 차트 보기가 내림차순으로 표시됩니다. 탐지된 상위 발송 바이러스 섹션에는 네트워크에서 전송한 바이러스의 차트 보기가 내림차순으로 표시됩니다.

참고 바이러스에 감염된 메시지를 네트워크에 보낸 호스트를 보려면 수신 메일 페이지로 이동하여 동일한 보고 기간을 지정하고 바이러스 감염을 기준으로 정렬하면 됩니다. 마찬가지로, 네트워크 내에서 바이러스 감염 이메일을 보낸 IP 주소를 보려면 발송 발신자 페이지를 확인하고 바이러스 감염 메시지를 기준으로 정렬하면 됩니다.

VirusTypes 세부사항 목록에는 감염된 수신 및 발송 메시지와 감염된 총 메시지를 포함한 특정 바이러스에 대한 정보가 표시됩니다. 감염된 수신 메시지 세부사항 목록에는 해당 바이러스의 이름과 이 바이러스에 감염된 수신 메시지의 수가 표시됩니다. 마찬가지로, 발송 메시지에는 해당 바이러스의 이름과 이 바이러스에 감염된 발송 메시지의 수가 표시됩니다. 수신 메시지, 발송 메시지 또는 감염된 총 메시지를 기준으로 바이러스 유형을 정렬할 수 있습니다.

URL 필터링 페이지

- URL 필터링 보고서 모듈은 URL 필터링이 활성화된 경우에만 채워집니다.
- URL 필터링 보고서는 수신 및 발신 메시지에 사용할 수 있습니다.
- URL 필터링 엔진에서 안티스팸/신종 바이러스 필터(Outbreak Filter) 검사의 일부로 또는 메시지/콘텐츠 필터를 통해 검사한 메시지만 이러한 모듈에 포함됩니다. 그러나 모든 결과가 반드시 명확하게 URL 필터링에서 기인해야 하는 것은 아닙니다.
- 상위 URL 범주 모듈에는 콘텐츠와 일치하든, 메시지 필터와 일치하든 관계없이 검사된 메시지에서 발견된 모든 범주가 포함됩니다.
- 각 메시지는 1개의 URL 평판 수준과만 연계될 수 있습니다. URL이 여러 개인 메시지의 경우 해당 메시지에서 가장 낮은 URL 평판이 통계에 반영됩니다.
- Security Services(보안 서비스) > URL Filtering(URL 필터링)에서 구성된 전역 허용 목록의 URL은 보고서에 포함되지 않습니다.

  개별 필터에 사용된 허용 목록의 URL은 보고서에 포함됩니다.
- 악성 URL은 신종 바이러스 필터(Outbreak Filter)에서 평판이 좋지 않다고 결정한 URL입니다. 의심스러운 URL은 신종 바이러스 필터(Outbreak Filter)에서 클릭 시간 보호가 필요하다고 결정한 URL입니다. 따라서 의심스러운 URL은 Cisco Web Security 프록시에 리디렉션되도록 재작성되었습니다.
- URL 범주 기반 필터의 결과는 콘텐츠 및 메시지 필터 보고서에 반영됩니다.
- Cisco Web Security 프록시의 클릭 시간 URL 평가 결과는 보고서에 반영되지 않습니다.

파일 평판 및 파일 분석 보고서

다음 보고서는 파일 평판 및 파일 분석 보고 및 추적, 16-13페이지를 참조하십시오.

- AMP(Advanced Malware Protection)
- 파일 분석
- AMP 판정 업데이트

TLS 연결 페이지

TLS 연결 페이지에는 전송 및 수신된 메일에 대한 TLS 연결의 전체 사용량이 표시됩니다. 이 보고서에서는 TLS 연결을 사용하여 메일을 전송하는 각 도메인에 대한 세부사항도 보여줍니다.

TLS 연결 페이지를 사용하여 다음 정보를 확인할 수 있습니다.

- 전반적으로 수신 및 발송 연결의 어느 부분이 TLS를 사용합니까?
- 내가 어떤 파트너와의 TLS 연결에 성공했습니까?
- 내가 어떤 파트너와의 TLS 연결에 실패했습니까?
- TLS 인증서에 문제가 있는 파트너는 어디입니까?
- 파트너와의 전체 메일이 사용하는 TLS의 비율은 얼마입니까?

TLS 연결 페이지는 수신 연결에 대한 섹션과 발송 연결에 대한 섹션으로 나누어집니다. 각 섹션에는 그래프, 요약 및 세부사항이 표시된 표가 포함됩니다.

그래프는 사용자가 지정한 시간 범위 동안의 수신 또는 발송 TLS 암호화된 연결 및 암호화되지 않은 연결의 보기를 표시합니다. 이 그래프는 메시지의 총 볼륨, 암호화된 메시지와 암호화되지 않은 메시지의 볼륨, 성공 및 실패한 TLS 암호화된 메시지의 볼륨을 표시합니다. 이 그래프는 TLS가 필요한 연결과 TLS가 단순히 선호되는 연결을 구별합니다.

이 표에는 암호화된 메시지를 전송하거나 수신하는 도메인에 대한 세부사항이 표시됩니다. 각 도메인의 경우 성공했거나 실패한 필요 및 선호 TLS 연결의 수, 시도된 총 TLS 연결 수(성공 또는 실패 여부와 무관), 암호화되지 않은 연결의 총 수를 볼 수 있습니다. 또한 TLS가 시도된 모든 연결의 비율과 TLS 선호 또는 필요 여부와 관계없이 성공적으로 전송된 암호화된 메시지의 총 수를 볼 수 있습니다. 이 표 하단의 Columns(열) 링크를 클릭하여 열을 표시하거나 숨길 수 있습니다.

인바운드 **SMTP** 인증 페이지

인바운드 SMTP 인증 페이지에서는 클라이언트 인증서와 SMTP AUTH 명령을 사용하여 Email Security 어플라이언스와 사용자의 메일 클라이언트 간 SMTP 세션을 인증하는 방법을 보여줍니다. 어플라이언스가 인증서 또는 SMTP AUTH 명령을 수락하면 클라이언트가 메시지를 보내는 데 사용할 메일 클라이언트에 대한 TLS 연결을 구성합니다. 어플라이언스가 사용자 단위로 이러한 시도를 추적할 수 없으므로 보고서에서 도메인 이름과 도메인 IP 주소를 기반으로 SMTP 인증에 대한 세부사항을 보여줍니다.

이 보고서를 사용하여 다음 정보를 확인할 수 있습니다.

- 전반적으로 SMTP 인증을 사용하는 수신 연결은 몇 개입니까?
- 클라이언트 인증서를 사용하는 연결은 몇 개입니까?
- SMTP AUTH를 사용하는 연결은 몇 개입니까?
- SMTP 인증을 사용하려고 시도할 때 연결에 실패하는 도메인은 무엇입니까?
- SMTP 인증이 실패한 경우 대안을 성공적으로 사용하는 연결은 몇 개입니까?

인바운드 SMTP 인증 페이지에는 수신된 연결에 대한 그래프, SMTP 인증 연결을 시도한 메일 수신자에 대한 그래프, 연결 인증 시도에 대한 세부사항이 표시된 표가 포함됩니다.

수신된 연결 그래프에서는 사용자가 지정한 시간 범위 동안 SMTP 인증을 사용하여 연결 인증을 시도하는 메일 클라이언트의 수신 연결을 보여줍니다. 이 그래프에는 어플라이언스가 수신한 총 연결 수, SMTP 인증을 사용하여 인증을 시도하지 않은 횟수, 클라이언트 인증서를 사용하여 연결을 인증하는 데 실패 및 성공한 횟수, SMTP AUTH 명령을 사용하여 인증하는 데 실패 및 성공한 횟수가 표시됩니다.

수신된 수신자 그래프에는 메일 클라이언트가 SMTP 인증을 사용하여 메시지를 전송하기 위해 Email Security 어플라이언스에 대한 연결을 인증하려고 시도한 수신자의 수가 표시됩니다. 이 그래프에는 연결이 인증된 수신자의 수와 연결이 인증되지 않은 수신자의 수도 표시됩니다.

SMTP 인증 세부사항 표에는 사용자가 메시지를 보내기 위해 Email Security 어플라이언스에 대한 연결을 인증하려고 시도한 도메인에 대한 세부사항이 표시됩니다. 각 도메인의 경우 클라이언트 인증서를 사용한 성공 또는 실패한 연결 시도 횟수, SMTP AUTH 명령을 사용한 성공 또는 실패한 연결 시도 횟수, 클라이언트 인증서 연결 시도가 실패한 후 SMTP AUTH로 대체된 횟수를 볼 수 있습니다. 페이지 상단의 링크를 사용하여 도메인 이름 또는 도메인 IP 주소별로 이 정보를 표시할 수 있습니다.

속도 제한 페이지

봉투 발신자별 속도 제한을 통해 메일 받는 사람 주소를 기반으로 개별 발신자의 시간 간격당 이메일 메시지 수신자의 수를 제한할 수 있습니다. 속도 제한 보고서에서는 이 제한을 가장 심하게 초과하는 발신자를 보여줍니다.

이 보고서를 사용하여 다음 정보를 확인할 수 있습니다.

- 스팸을 대량으로 보내는 데 사용될 수 있는 손상된 사용자 계정
- 조직에서 알림, 경고, 자동 문 등에 이메일을 사용하는 통제 불능 애플리케이션
- 조직 내에서 내부 청구 또는 리소스 관리 목적으로 이루어지는 많은 이메일 활동의 소스
- 다른 경우에는 스팸으로 간주되지 않았을 수 있는 대용량 인바운드 이메일 트래픽의 소스

내부 발신자(내부 사용자 또는 발송 발신자)에 대한 통계를 포함하는 다른 보고서는 전송된 메시지 수만 측정하며 많은 수신자에게 몇 개의 메시지를 보내는 발신자는 식별하지 않습니다.

사고별 상위 위반자 차트에서는 구성된 제한보다 더 많은 수신자에게 메시지를 보내려고 가장 자주 시도한 봉투 발신자를 보여줍니다. 각 시도가 하나의 사고로 간주됩니다. 이 차트는 모든 리스너의 사고 수를 집계합니다.

거부된 수신자별 상위 위반자 차트에서는 구성된 제한을 초과해 가장 많은 수신자에게 메시지를 보낸 봉투 발신자를 보여줍니다. 이 차트는 모든 리스너의 수신자 수를 집계합니다.

봉투 발신자별 속도 제한을 구성하거나 기존 속도 제한을 수정하려면 메일 흐름 정책을 사용하여 수신 메시지에 대한 규칙 정의, 7-15페이지를 참조하십시오.

시스템 용량 페이지

시스템 용량 페이지에서는 작업 큐의 메시지, 작업 큐에서 소요된 평균 시간, 수신 및 발송 메시지(볼륨, 크기 및 수), 전체 CPU 사용량, 기능별 CPU 사용량, 메모리 페이지 스와핑 정보를 포함한 자세한 시스템 로드 표현을 제공합니다.

시스템 용량 페이지를 사용해 다음 정보를 확인할 수 있습니다.

- 어플라이언스가 권장 용량을 초과하거나 구성 최적화 또는 추가 어플라이언스가 필요한 경우를 식별합니다.
- 차후에 용량 문제가 발생할 수 있음을 나타내는 시스템 동작의 내역 트렌드를 식별합니다.
- 시스템의 어느 부분에서 문제 해결을 지원하기 위해 가장 많은 리소스를 사용하는지 식별합니다.

어플라이언스를 모니터링하여 현재 용량이 메시지 볼륨에 적합한지 확인하는 것이 중요합니다. 시간이 지남에 따라 볼륨이 필연적으로 증가하게 되므로 적절한 모니터링을 통해 추가 용량 또는 구성 변경 사항을 사전에 적용할 수 있는지 확인합니다. 시스템 용량을 모니터링하는 가장 효과적인 방법은 전체 볼륨, 작업 큐의 메시지, 리소스 보존 모드의 사고를 추적하는 것입니다.

- **볼륨**: 해당 환경의 "일반적인" 메시지 볼륨과 "평소의" 사용량 급증을 이해하는 것이 중요합니다. 시간 경과에 따라 이 데이터를 추적하여 볼륨 증가를 측정합니다. 수신 메일 및 발송 메일 페이지를 사용하여 시간 경과에 따른 볼륨을 추적할 수 있습니다. 자세한 내용은 시스템 용량-수신 메일, 28-25페이지 및 시스템 용량-발송 메일, 28-26페이지를 참조하십시오.
- **작업 큐**: 작업 큐는 스팸 공격을 흡수 및 필터링하고 햄 메시지의 비정상적인 증가를 처리하는 "완충기"로 작동하도록 설계 되었습니다. 그러나 작업 큐는 로드가 높은 시스템을 가장 잘 나타내는 지표이기도 하므로 장시간의 빈번한 작업 큐 백업은 용량 문제가 있음을 나타낼 수 있습니다. WorkQueue 페이지를 사용하여 작업 큐에서 메시지가 소비한 평균 시간과 작업 큐의 활동을 추적할 수 있습니다. 자세한 내용은 시스템 용량-Workqueue, 28-24페이지를 참고하십시오.
- **리소스 보존 모드**: 어플라이언스가 오버로드되면 "RCM(리소스 보존 모드)"으로 전환되어 CRITICAL 시스템 경고를 보냅니다. 이 모드는 디바이스를 보호하고 디바이스가 메시지 백로그를 처리할 수 있도록 고안되었습니다. 어플라이언스는 메일 볼륨이 대량으로 또는 비정상적으로 증가할 경우에만 RCM으로 전환되어야 하며, RCM으로 전환되는 빈도가 드물어야 합니다. 빈번한 RCM 경고는 시스템이 오버로드되고 있음을 나타낼 수 있습니다. 리소스 보존 모드는 시스템 용량 페이지에서 추적되지 않습니다.

관련 주제

- 시스템 용량-Workqueue, 28-24페이지
- 시스템 용량-수신 메일, 28-25페이지
- 시스템 용량-발송 메일, 28-26페이지
- 시스템 용량-시스템 로드, 28-27페이지
- 메모리 페이지 스와핑에 대한 참고사항, 28-28페이지
- 시스템 용량-모두, 28-28페이지

시스템 용량-Workqueue

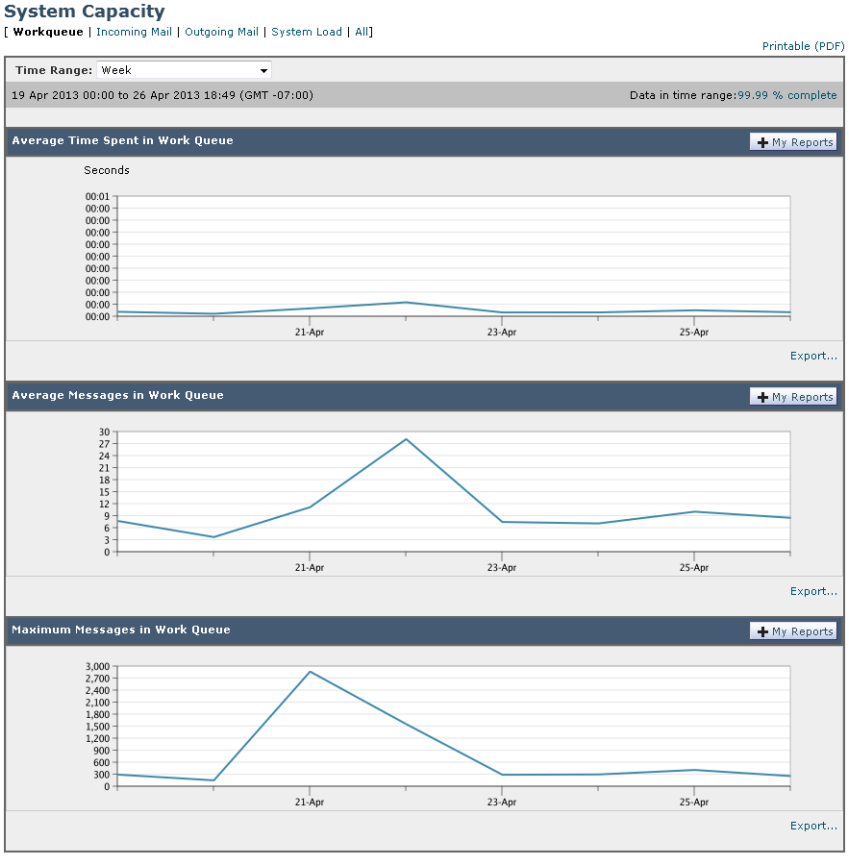
Workqueue 페이지에는 스팸 격리 또는 정책, 바이러스 또는 신종 바이러스 격리에서 소요된 시간을 제외하고 작업 큐에서 메시지가 소비한 평균 시간이 표시됩니다. 1시간에서 최대 1개월까지의 기간을 볼 수 있습니다. 이 평균으로 메일 전송을 연기하는 단기 이벤트와 시스템 워크로드의 장기 트렌드를 모두 식별할 수 있습니다.

참고 메시지가 격리에서 작업 큐로 릴리스되면 "작업 큐의 평균 시간" 메트릭이 이 시간을 무시합니다. 따라서 격리에서 소요된 시간이 연장되어 이중 계산과 왜곡된 통계가 발생하는 것을 방지할 수 있습니다.

이 보고서에서는 지정된 기간 동안의 작업 큐의 메시지 볼륨과 같은 기간 동안의 작업 큐의 최대 메시지도 보여줍니다.

Workqueue 그래프에서 가끔 나타나는 사용량 급증은 정상적이며 예상된 것입니다. 사용량 급증이 발생하는 빈도가 증가하고 장기간 유지될 경우 용량 문제가 있음을 나타낼 수 있습니다. 작업 큐 페이지를 검토할 때 작업 큐 백업의 빈도를 측정하고 10,000개의 메시지를 초과하는 작업 큐 백업을 적어 둘 수 있습니다.

그림 28-1 시스템 용량 - Workqueue



시스템 용량-수신 메일

수신 메일 페이지에는 수신 연결, 총 수신 메시지 수, 평균 메시지 크기, 총 수신 메시지 크기가 표시됩니다. 결과를 지정한 시간 범위로 제한할 수 있습니다. 해당 환경의 일반적인 메시지 볼륨 트렌드와 사용량 급증을 이해하는 것이 중요합니다. 수신 메일 페이지를 사용하여 시간 경과에 따른 볼륨 증가를 추적하고 시스템 용량 계획을 세울 수 있습니다. 또한 수신 메일 데이터를 발신자 프로필 데이터와 비교하여 특정 도메인에서 네트워크로 전송되는 이메일 볼륨의 트렌드를 볼 수 있습니다.

참고 수신 연결 수 증가가 반드시 시스템 로드에 영향을 미치는 것은 아닙니다.

그림 28-2 시스템 용량 - 수신 메일(1/2페이지)

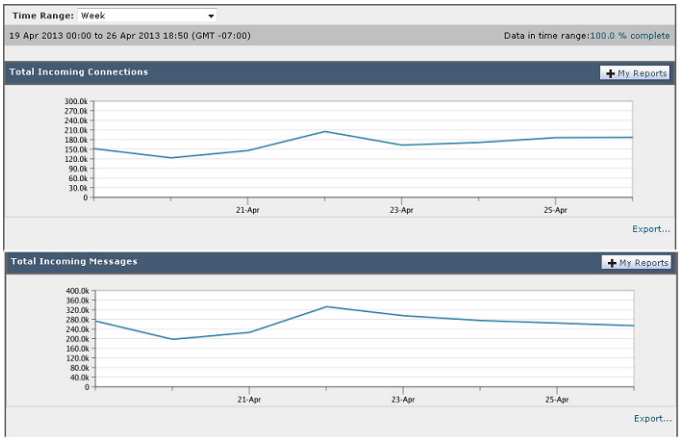
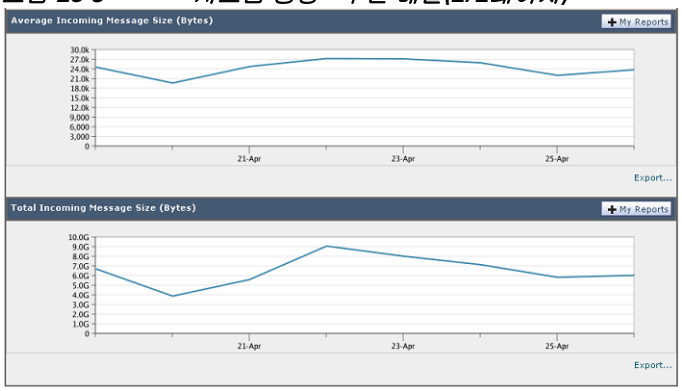


그림 28-3 시스템 용량 - 수신 메일(2/2페이지)



시스템 용량-발송 메일

발송 메일 페이지에는 발송 연결, 총 발송 메시지 수, 평균 메시지 크기, 총 발송 메시지 크기가 표시됩니다. 결과를 지정한 시간 범위로 제한할 수 있습니다. 해당 환경의 일반적인 메시지 볼륨 트렌드와 사용량 급증을 이해하는 것이 중요합니다. 발송 메일 페이지를 사용하여 시간 경과에 따른 볼륨 증가를 추적하고 시스템 용량 계획을 세울 수 있습니다. 또한 발송 메일 데이터를 발송 대상 데이터와 비교하여 특정 도메인 또는 IP 주소에서 전송되는 이메일 볼륨의 트렌드를 볼 수 있습니다.

그림 28-4 시스템 용량 - 발송 메일(1/2페이지)

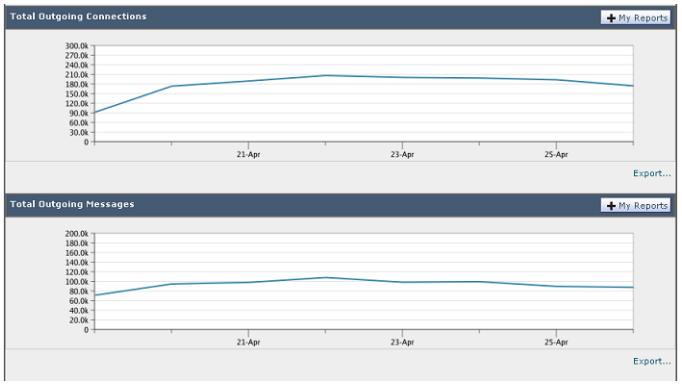
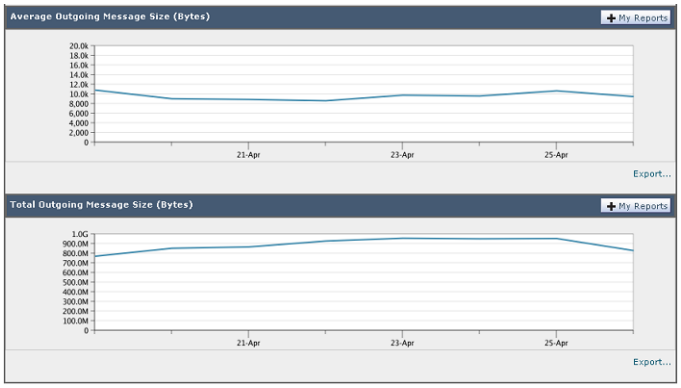


그림 28-5 시스템 용량 - 발송 메일(2/2페이지)

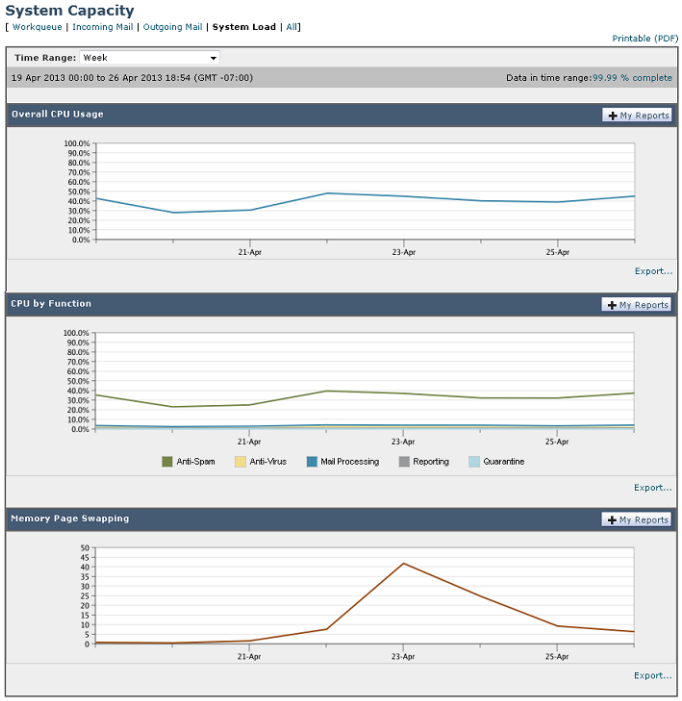


시스템 용량-시스템 로드

시스템 로드 보고서에서는 어플라이언스의 전체 CPU 사용량을 보여줍니다. AsyncOS는 유휴 CPU 리소스를 사용하여 메시지 처리량을 개선할 수 있도록 최적화되었습니다. 높은 CPU 사용량은 시스템 용량 문제를 나타낼 수 있습니다. 높은 CPU 사용량과 일관된 고용량 메모리 페이지 스와핑이 함께 나타날 경우 용량 문제가 있을 수 있습니다. 이 페이지에서는 메일 처리, 스팸 및 바이러스 엔진, 보고, 격리를 포함한 다른 기능에서 사용되는 CPU의 양을 표시하는 그래프도 보여줍니다. 기능별 CPU 그래프는 시스템에서 가장 많은 리소스를 사용하는 제품 영역을 잘 보여줍니다. 어플라이언스를 최적화해야 하는 경우 이 그래프를 이용해 조정하거나 비활성화해야 하는 기능을 결정할 수 있습니다.

메모리 페이지 스와핑 그래프에서는 시스템이 디스크로 페이징해야 하는 빈도를 보여줍니다.

그림 28-6 시스템 용량 - 시스템 로드



메모리 페이지 스와핑에 대한 참고사항

이 시스템은 정기적으로 메모리를 서로 바꿀 수 있도록 설계되었으므로 일부 메모리 스와핑이 예상되며 이는 어플라이언스에 문제가 있음을 나타내지 않습니다. 시스템이 *일관되게* 대량의 메모리를 서로 바꾸지 않는 한 메모리 스와핑은 정상이며 예상된 동작입니다(특히 C160 어플라이언스에서). 예를 들어, 그림 28-7은 일관되게 대량의 메모리를 서로 바꾸는 시스템을 보여줍니다. 성능을 향상시키려면 네트워크에 어플라이언스를 추가하거나 최대 처리량을 얻을 수 있도록 구성을 조정해야 할 수 있습니다.

그림 28-7 시스템 용량 - 시스템 로드(로드가 높은 시스템)

시스템 용량-모두

모든 페이지는 이전의 모든 시스템 용량 보고서를 단일 페이지로 통합하므로 서로 다른 보고서 간의 관계를 볼 수 있습니다. 예를 들어, 과도한 메모리 스와핑이 발생함과 동시에 메시지 큐가 높아지는 것을 볼 수 있습니다. 이는 용량 문제가 있음을 나타낼 수 있습니다. 나중에 참조하거나 지원 인력을 공유할 수 있도록 이 페이지를 PDF로 저장하여 시스템 성능의 스냅샷을 보존할 수 있습니다. 영어가 아닌 다른 언어로 PDF를 생성하는 방법에 대한 내용은 "보고서에 대한 참고사항" 섹션, 28-34페이지를 참조하십시오.

시스템 상태 페이지

시스템 상태 페이지에서는 모든 실시간 메일과 시스템의 DNS 활동을 자세히 표현합니다. 표시되는 정보는 CLI에서 `status detail` 및 `dnsstatus` 명령을 사용하여 이용할 수 있는 정보와 동일합니다. 자세한 내용은 상태 세부사항의 명령의 경우는 "자세한 이메일 상태 모니터링"을, `dnsstatus` 명령(34 장, "CLI를 통한 관리 및 모니터링")의 경우는 "DNS 상태 확인"을 각각 참조하십시오.

시스템 상태 페이지는 시스템 상태, 게이지, 속도 및 카운터의 4개 섹션으로 구성됩니다.

관련 주제

- 시스템 상태, 28-29페이지
- 게이지, 28-29페이지
- 속도, 28-29페이지
- 카운터, 28-30페이지

시스템 상태

시스템 상태 섹션에서는 메일 시스템 상태와 버전 정보를 보여줍니다.

관련 주제

- 메일 시스템 상태, 28-29페이지
- 버전 정보, 28-29페이지

메일 시스템 상태

메일 시스템 상태 섹션에는 다음 정보가 포함됩니다.

- 시스템 상태(시스템 상태에 대한 자세한 내용은 상태, 28-6페이지 참조)
- 마지막으로 상태가 보고된 시간
- 어플라이언스의 가동 시간
- 아직 전송 대기 중이 아닌 메시지를 포함하여 시스템에서 가장 오래된 메시지

버전 정보

버전 정보 섹션에는 다음 정보가 포함됩니다.

- 어플라이언스 모델 이름
- 설치된 AsyncOS 운영 체제의 버전 및 빌드 날짜
- AsyncOS 운영 체제의 설치 날짜
- 사용자가 연결된 시스템의 일련 번호

이 정보는 시스코 고객 지원에 문의할 경우에 유용합니다. (기술 지원 이용, 40-25페이지 참조.)

게이지

게이지 섹션에서는 큐와 리소스 사용률을 보여줍니다.

- 메일 처리 대기열
- 큐에 있는 활성 수신자
- 대기열 공간
- CPU 사용률

  메일 게이트웨이 어플라이언스는 AsyncOS 프로세스가 사용하는 CPU의 비율을 나타냅니다. CASE는 안티스팸 검사 엔진과 신종 바이러스 필터(Outbreak Filter) 프로세스를 포함한 여러 항목을 나타냅니다.
- 일반 리소스 사용률
- 로깅 디스크 사용률

속도

속도 섹션에서는 수신자 처리 속도를 보여줍니다.

- 메일 처리율
- 완료 비율

카운터

시스템 통계에 대한 누적 이메일 모니터링 카운터를 재설정하고 카운터가 마지막으로 재설정된 시간을 볼 수 있습니다. 재설정은 도메인별 카운터뿐 아니라 시스템 카운터에도 영향을 미칩니다. 재설정은 재시도 일정과 관련된 전송 큐에 있는 메시지의 카운터에는 영향을 미치지 않습니다.

참고 관리자 또는 운영자 그룹에 있는 사용자 계정만 카운터에 액세스하여 재설정할 수 있습니다. 게스트 그룹에서 생성한 사용자 계정은 카운터를 재설정할 수 없습니다. 자세한 내용은 사용자 계정 작업, 32-1페이지를 참조하십시오.

카운터를 재설정하려면 Reset Counters(카운터 재설정)를 클릭합니다. 이 버튼은 CLI의 `resetcounters` 명령과 동일한 기능을 제공합니다. 자세한 내용은 이메일 모니터링 카운터 재설정, 34-21페이지를 참조하십시오.

- 메일 처리 이벤트
- 완료 이벤트
- 도메인 키 이벤트
- DNS 상태

대량 메일 페이지

참고 대량 메일 페이지에서는 헤더 반복 규칙을 사용하는 메시지 필터의 데이터만 보여줍니다.

대량 메일 페이지에는 다음과 같은 보고서가 막대 그래프 형태로 포함되어 있습니다.

- **상위 제목**. 이 차트를 사용하여 AsyncOS가 받은 메시지의 상위 제목을 이해할 수 있습니다.
- **상위 봉투 발신자**. 이 차트를 사용하여 AsyncOS가 받은 메시지의 상위 봉투 발신자를 이해할 수 있습니다.
- **일치 항목 수별 상위 메시지 필터**. 이 차트를 사용하여 상위 메시지 필터(헤더 반복 규칙 사용) 일치 항목을 이해할 수 있습니다.

대량 메일 페이지에서는 상위 메시지 필터와 해당 메시지 필터의 일치 항목 수를 표 형식으로 표현합니다. 메시지 추적을 사용하여 해당 숫자에 포함된 모든 메시지의 목록을 보려면 숫자를 클릭합니다.

시간, 주 또는 사용자 지정 범위 등 보고할 시간 범위를 선택할 수 있습니다. 모든 보고서와 마찬가지로 **Export(내보내기)** 링크를 통해 그래프 또는 세부사항 목록의 데이터를 CSV 형식으로 내보내거나 **Printable (PDF)(인쇄 가능(PDF))** 링크를 클릭하여 PDF 형식으로 내보낼 수 있습니다.

메시지 필터 페이지

메시지 필터 페이지에서는 상위 메시지 필터 일치 항목(가장 일치하는 메시지가 있는 메시지 필터)에 대한 정보를 막대 그래프와 표 형식 표현의 두 가지 형태로 보여줍니다.

막대 그래프를 사용하여 수신 및 발송 메시지에 의해 가장 많이 트리거되는 메시지 필터를 찾을 수 있습니다. 표 형식 표현은 상위 메시지 필터와 해당 메시지 필터의 일치 항목 수를 보여줍니다. 메시지 추적을 사용하여 해당 숫자에 포함된 모든 메시지의 목록을 보려면 숫자를 클릭합니다.

시간, 주 또는 사용자 지정 범위 등 보고할 시간 범위를 선택할 수 있습니다. 모든 보고서와 마찬가지로 **Export(내보내기)** 링크를 통해 그래프 또는 세부사항 목록의 데이터를 CSV 형식으로 내보내거나 **Printable (PDF)(인쇄 가능(PDF))** 링크를 클릭하여 PDF 형식으로 내보낼 수 있습니다.

CSV 데이터 검색

이메일 보안 모니터링에서 차트와 그래프를 구성하는 데 사용된 데이터를 CSV 형식으로 검색할 수 있습니다. CSV 데이터는 다음 2가지 방법으로 액세스할 수 있습니다.

- **이메일을 통해 제공된 CSV 보고서**. CSV 보고서를 생성하여 이메일을 통해 제공하거나 아카이브할 수 있습니다. 이 제공 방법은 이메일 보안 모니터링 페이지에 표시된 각 표에 대한 별도의 보고서를 전달하거나 내부 네트워크에 액세스할 수 없는 사용자에게 CSV 데이터를 전송하려는 경우에 유용합니다.

  CSV(쉼표로 구분된 값) 보고서 유형은 예약된 보고서의 표 형식 데이터가 들어 있는 ASCII 텍스트 파일입니다. 각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 보고서에 두 가지 이상의 표 유형이 포함된 경우 각 표에 대해 별도의 CSV 파일을 생성합니다. 단일 보고서에 대한 여러 CSV 파일은 아카이브된 파일 저장 옵션의 경우 단일 .zip 파일로 압축되고, 이메일 전송의 경우 별도의 이메일 메시지로 모두 첨부됩니다.

  예약된 보고서 또는 온디맨드 보고서 구성에 대한 자세한 내용은 보고 개요, 28-33페이지를 참조하십시오.

- **HTTP를 통해 검색한 CSV 파일**. HTTP를 통해 이메일 보안 모니터링 기능의 차트와 그래프를 구성하는 데 사용된 데이터를 검색할 수 있습니다. 이 제공 방법은 다른 툴을 통해 데이터에 대한 추가 분석을 수행하려는 경우에 유용합니다. 예를 들어, 원시 데이터를 다운로드하고 처리한 다음 그 결과를 몇 개의 다른 시스템에 표시하는 자동 스크립트로 이 데이터의 검색을 자동화할 수 있습니다.

관련 주제

- 자동 프로세스를 통한 CSV 데이터 검색, 28-31페이지

자동 프로세스를 통한 CSV 데이터 검색

HTTP 쿼리를 가져오는 가장 쉬운 방법은 이메일 보안 모니터링 페이지 중 하나를 원하는 데이터의 유형을 표시하도록 구성하는 것입니다. 그러면 **Export(내보내기)** 링크를 복사할 수 있습니다. 이는 다운로드 URL입니다. 이와 같이 데이터 검색을 자동화할 경우 다운로드 URL에서 고정해야 하는 매개변수와 변경해야 하는 매개변수를 적어 두는 것이 중요합니다(아래 참조).

다운로드 URL은 동일한 쿼리를 실행(적절한 HTTP 인증 사용)하고 유사한 데이터 집합을 가져올 수 있는 외부 스크립트에 복사할 수 있는 방식으로 인코딩됩니다. 이 스크립트는 기본 HTTP 인증 또는 쿠키 인증을 사용할 수 있습니다. 자동 프로세스를 통해 CSV 데이터를 검색할 때 다음에 유의하십시오.

- URL이 다시 사용될 때와 관련한 시간 범위 선택(과거 시간, 일, 주, 등). URL을 복사해 "과거 날짜"에 대한 CSV 데이터 집합을 검색하려면 URL을 다시 전송한 시간에서부터 "과거 날짜"를 포함하는 새로운 데이터 세트를 가져옵니다. 데이터 범위 선택이 유지되고 CSV 쿼리 문자열(예: `date_range=current_day`)에 나타납니다.
- 데이터 집합의 환경 설정 필터링 및 그룹화. 필터가 유지되고 쿼리 문자열에 나타납니다. 보고서의 필터는 드뭅니다. 보고서 필터의 한 가지 예는 신종 바이러스 보고서의 "전역/로컬" 신종 바이러스 선택기입니다.
- CVS 다운로드는 선택한 시간 범위의 표에 있는 모든 데이터 행을 반환합니다.

- CSV 다운로드는 타임스탬프 및 키에 따라 정렬된 표의 데이터 행을 반환합니다. 스프레드시트 애플리케이션을 사용하는 등 별도의 단계로 추가 정렬을 수행할 수 있습니다.
- 첫 번째 행에는 보고서에 표시된 표시 이름과 일치하는 열 헤더가 포함됩니다. 타임스탬프(타임스탬프, 28-32페이지 참조)와 키(키, 28-32페이지 참조)도 나타납니다.

관련 주제

- 샘플 URL, 28-32페이지
- 기본 HTTP 인증 자격 증명 추가, 28-32페이지
- 파일 형식, 28-32페이지
- 타임스탬프, 28-32페이지
- 키, 28-32페이지
- 스트리밍, 28-33페이지

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 기본 HTTP 인증 자격 증명을 지정하려면 다음을 수행합니다.

```
http://example.com/monitor/
```

결과:

```
http://username:password@example.com/monitor/
```

파일 형식

다운로드한 파일은 CSV 형식이며 파일 확장자는 .csv입니다. 파일 헤더에 보고서의 이름으로 시작하고 그 다음에 보고서의 섹션이 나오는 기본 파일 이름이 있습니다.

타임스탬프

각 시간 원시 "간격"의 스트림 데이터 표시 시작 및 종료 타임스탬프를 내보냅니다. 시작 타임스탬프와 종료 타임스탬프가 각각 2개씩 제공됩니다. 하나는 숫자 형식이고 다른 하나는 사람이 읽을 수 있는 문자열 형식입니다. 타임스탬프는 GMT 시간을 사용하므로 어플라이언스가 여러 표준 시간대에 있는 경우 로그 집계가 더 쉽습니다.

드물긴 하지만 데이터가 다른 소스의 데이터와 병합된 경우 내보내기 파일에 타임스탬프가 포함되지 않습니다. 예를 들어, 신종 바이러스 세부사항 내보내기는 보고서 데이터와 TOC(Threat Operations Center) 데이터를 병합하므로 간격이 없어 타임스탬프와 무관합니다.

키

보고서에 키가 표시되지 않더라도 내보내기에 보고서 표 키도 포함됩니다. 키가 표시된 경우 보고서에 표시된 표시 이름이 열 헤더로 사용됩니다. 그렇지 않은 경우 "key0", "key1" 등과 같은 열 헤더가 표시됩니다.

스트리밍

데이터의 양이 잠재적으로 매우 크기 때문에 대부분의 내보내기가 데이터를 클라이언트로 다시 스트리밍합니다. 그러나 일부 내보내기는 데이터를 스트리밍하지 않고 전체 결과 집합을 반환합니다. 이는 보고서 데이터가 비 보고서 데이터와 함께 집계된 경우에 일반적입니다.

보고 개요

AsyncOS에서의 보고는 3가지 기본 작업을 포함합니다.

- 매일, 매주 또는 매월 실행되는 예약 보고서를 생성할 수 있습니다.
- 보고서를 즉시 생성할 수 있습니다("온디맨드" 보고서).
- 이전에 실행된 보고서(예약 및 온디맨드 보고서 모두)의 아카이브된 버전을 볼 수 있습니다.

Monitor(모니터링) > Scheduled Reports(예약 보고서) 페이지를 통해 예약 및 온디맨드 보고서를 구성합니다. Monitor(모니터링) > Archived Reports(아카이브된 보고서) 페이지를 통해 보관된 보고서를 봅니다.

어플라이언스가 가장 최근에 생성한 보고서를 유지합니다(모든 보고서에 대해 최대 총 1,000개의 버전). 원하는 경우 제로 수신자를 포함해 보고서의 수신자를 필요한 수만큼 정의할 수 있습니다. 이메일 수신자를 지정하지 않으면 시스템에서 보고서를 계속 보관합니다. 그러나 여러 주소로 보고서를 보내야 할 경우 수신자를 개별적으로 나열하는 것보다 메일 목록을 만드는 것이 더 쉬울 수 있습니다.

기본적으로 어플라이언스는 예약된 각 보고서의 가장 최근 보고서 12개를 보관합니다. 보고서는 어플라이언스의 `/saved_reports` 디렉토리에 저장됩니다. 자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스" 를 참조하십시오.

관련 주제

- 예약 보고서 유형, 28-33페이지
- 보고서의 반환 주소 설정, 28-34페이지

예약 보고서 유형

다음과 같은 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
- 발송 발신자: 도메인
- 그룹
- 시스템 용량

- TLS 연결
- Outbreak 필터
- 바이러스 유형

각 보고서는 해당 이메일 보안 모니터링 페이지의 요약으로 구성됩니다. 따라서 예를 들어 콘텐츠 필터 보고서에서는 Monitor(모니터링) > Content Filters(콘텐츠 필터) 페이지에 표시된 정보의 요약을 제공합니다. 개요 요약 보고서는 Monitor(모니터링) > Overview(개요) 페이지를 기반으로 합니다.

관련 주제

- 보고서에 대한 참고사항, 28-34페이지

보고서에 대한 참고사항

PDF 형식의 콘텐츠 필터 보고서는 최대 40개의 콘텐츠 필터로 제한됩니다. CSV 형식의 보고서를 통해 전체 목록을 얻을 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

보고서의 반환 주소를 설정하려면 어플라이언스에서 생성된 메시지의 복귀 주소 구성, 33-33페이지를 참조하십시오. CLI에서 `addressconfig` 명령을 사용합니다.

보고서 관리

아카이브된 예약 보고서를 생성, 편집, 삭제하거나 볼 수 있습니다. 또한 보고서를 즉시 실행할 수 있습니다(온디맨드 보고서). 콘텐츠 필터, DLP 사고 요약, 개요 요약, 수신 메일 요약, 내부 사용자 요약, 발송 메일 요약, 발신자 그룹, 신종 바이러스 필터(Outbreak Filter) 등의 보고서 유형을 사용할 수 있습니다. 이러한 보고서는 관리하고 보는 방법은 아래에서 설명합니다.

참고 클러스터 모드에서는 보고서를 볼 수 없습니다. 머신 모드에서는 보고서를 볼 수 있습니다.

Monitor(모니터링) > Scheduled Reports(예약 보고서) 페이지에서는 어플라이언스에서 이미 생성된 예약 보고서의 목록을 보여줍니다.

관련 주제

- 예약 보고서, 28-35페이지
- 아카이브된 보고서, 28-36페이지

예약 보고서

예약 보고서는 매일, 매주 또는 매월 실행되도록 예약할 수 있습니다. 보고서를 실행할 시간을 선택할 수 있습니다. 보고서 실행 시간에 관계없이 사용자가 지정한 기간의 데이터만 포함합니다(예: 지난 3일 또는 이전 달). 오전 1시에 실행되도록 예약된 일일 보고서에는 전날 자정부터 자정까지의 데이터가 포함됩니다.

어플라이언스에 기본 예약 보고서 집합이 내장되어 있으며 이러한 보고서를 사용, 수정 또는 삭제할 수 있습니다.

관련 주제

- 보고서가 자동으로 생성되도록 예약, 28-35페이지
- 예약 보고서 편집, 28-36페이지
- 예약 보고서 삭제, 28-36페이지

보고서가 자동으로 생성되도록 예약

절차

1단계 Monitor(모니터링) > Scheduled Reports(예약 보고서) 페이지에서 **Add Scheduled Report(예약 보고서 추가)**를 클릭합니다.

2단계 보고서 유형을 선택합니다. 선택한 보고서 유형에 따라 각기 다른 옵션을 사용할 수 있습니다.

사용 가능한 예약 보고서 유형에 대한 자세한 내용은 예약 보고서 유형, 28-33페이지를 참조하십시오.

3단계 보고서 제목을 알기 쉽게 입력합니다. AsyncOS는 보고서 이름이 고유한지 확인하지 않습니다. 혼동을 피하려면 이름이 같은 보고서를 여러 개 생성하지 마십시오.

4단계 보고서 데이터의 시간 범위를 선택합니다. (이 옵션은 신종 바이러스 필터(Outbreak Filter) 보고서에 사용할 수 없습니다.)

5단계 보고서의 형식을 선택합니다.

- **PDF**. 전송, 아카이브 또는 이 두 가지 목적으로 사용할 PDF 형식의 문서를 생성합니다. Preview PDF Report(PDF 보고서 미리보기)를 클릭하여 보고서를 즉시 PDF 파일로 볼 수 있습니다.

  영어가 아닌 다른 언어로 PDF를 생성하는 방법에 대한 내용은 "보고서에 대한 참고사항" 섹션, 28-34페이지를 참조하십시오.
- **CSV**. 쉼표로 구분된 값의 표 형식 데이터를 포함하는 ASCII 텍스트 파일을 생성합니다. 각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 보고서에 두 가지 이상의 표 유형이 포함된 경우 각 표에 대해 별도의 CSV 파일을 생성합니다.

6단계 보고서 옵션을 지정합니다(사용 가능한 경우). 일부 보고서에는 보고서 옵션이 없습니다.

7단계 예약 및 전송 옵션을 지정합니다. 이메일 주소를 지정하지 않으면 보고서가 아카이브되지만 수신자에게 전송되지 않습니다.

참고 외부 계정(Yahoo 또는 Gmail 등)으로 보고서를 보내려면 보고서 이메일이 스팸으로 잘못 분류되는 것을 방지하기 위해 외부 계정의 허용 목록에 보고 반환 주소를 추가해야 할 수 있습니다.

8단계 **Submit**을 클릭합니다. 변경 사항을 커밋합니다.

예약 보고서 편집

절차

1단계 Services(서비스) > Centralized Reporting(중앙 집중식 보고) 페이지의 목록에서 보고서 제목을 클릭합니다.

2단계 변경 사항을 적용합니다.

3단계 변경 사항을 제출하고 커밋합니다.

예약 보고서 삭제

절차

1단계 Services(서비스) > Centralized Reporting(중앙 집중식 보고) 페이지에서 삭제할 보고서에 해당하는 확인란을 선택합니다.

참고 예약 보고서를 모두 제거하려면 모두 확인란을 선택합니다.

2단계 **삭제**를 클릭합니다.

3단계 삭제를 확인한 다음 변경 사항을 커밋합니다.

삭제된 보고서의 아카이브된 버전은 자동으로 삭제되지 *않습니다*.

아카이브된 보고서

Monitor(모니터링) > Archived Reports(아카이브된 보고서) 페이지에 사용 가능한 보관된 보고서가 나열됩니다. 보고서 제목 열에서 해당 이름을 클릭하여 보고서를 볼 수 있습니다. **Generate Report Now(지금 보고서 생성)**를 클릭하여 즉시 보고서를 생성할 수 있습니다.

표시 메뉴를 사용하여 나열할 보고서의 유형을 필터링할 수 있습니다. 목록을 정렬하려면 열 머리글을 클릭합니다.

아카이브된 보고서가 자동으로 삭제됩니다. 각 예약 보고서(최대 1,000개의 보고서)의 인스턴스가 최대 30까지 보관되고 새 보고서가 추가되므로 보고서 수를 1,000개로 유지하기 위해 오래된 보고서가 삭제됩니다. 30개의 인스턴스 제한은 보고서 유형이 아닌 각 개별 예약 보고서에 적용됩니다.

관련 주제

- 온디맨드 보고서 생성, 28-36페이지

온디맨드 보고서 생성

예약하기 않고 보고서를 생성할 수 있습니다. 이러한 온디맨드 보고서는 여전히 지정된 기간을 기반으로 하지만 즉시 생성됩니다.

절차

1단계 아카이브된 보고서 페이지에서 **Generate Report Now(지금 보고서 생성)**를 클릭합니다.

2단계 보고서 유형을 선택하고 원하는 경우 제목을 편집합니다. AsyncOS는 보고서 이름이 고유한지 확인하지 않습니다. 혼동을 피하려면 이름이 같은 보고서를 여러 개 생성하지 마십시오.

사용 가능한 예약 보고서 유형에 대한 자세한 내용은 예약 보고서 유형,28-33페이지를 참조하십시오.

3단계 보고서 데이터의 시간 범위를 선택합니다. (이 옵션은 신종 바이러스 보고서에 사용할 수 없습니다.)

사용자 지정 범위를 생성할 경우 범위가 링크로 나타납니다. 범위를 수정하려면 링크를 클릭합니다.

4단계 보고서의 형식을 선택합니다.

- **PDF**. 전송, 아카이브 또는 이 두 가지 목적으로 사용할 PDF 형식의 문서를 생성합니다. Preview PDF Report(PDF 보고서 미리보기)를 클릭하여 보고서를 즉시 PDF 파일로 볼 수 있습니다.

  영어가 아닌 다른 언어로 PDF를 생성하는 방법에 대한 내용은 "보고서에 대한 참고사항" 섹션, 28-34페이지를 참조하십시오.

- **CSV**. 쉼표로 구분된 값의 표 형식 데이터를 포함하는 ASCII 텍스트 파일을 생성합니다. 각 CSV 파일은 최대 100개의 행을 포함할 수 있습니다. 보고서에 두 가지 이상의 표 유형이 포함된 경우 각 표에 대해 별도의 CSV 파일을 생성합니다. 보고서 옵션을 지정합니다.

5단계 보고서를 아카이브할지 여부를 선택합니다(아카이브하기로 선택하면 보고서가 아카이브된 보고서 페이지에 표시됩니다).

6단계 보고서를 이메일로 전송할지 여부와 보고서를 전송할 이메일 주소를 지정합니다.

7단계 보고서를 생성하고 수신자에게 전송하거나 보관하려면 **Deliver this Report(이 보고서 전송)**를 클릭합니다.

8단계 변경 사항을 커밋합니다.

이메일 보고서 문제 해결

문제 보고서에서 드릴다운하여 메시지 추적의 세부사항을 볼 경우 예기치 않은 결과가 발생합니다.

솔루션 이러한 현상은 보고 및 메시지 추적이 동시에 활성화되지 않았거나, 올바르게 작동하지 않거나, 로컬로 데이터를 저장(보안 관리 어플라이언스에 중앙 집중식으로 저장하는 것과 반대)한 경우에 발생할 수 있습니다. 각 기능(보고 및 메시지 추적)의 데이터는 다른 기능(보고 또는 메시지 추적)의 활성화 및 작동 여부와 관계없이 어플라이언스에서 해당 기능이 활성화되고 작동하는 경우에만 저장됩니다. 따라서 보고서에 메시지 추적에서 사용할 수 없는 데이터가 포함될 수 있으며 그 반대의 경우도 마찬가지입니다.

29 장

메시지 추적

메시지 추적 개요

메시지 추적을 통해 메시지 흐름에 대한 자세한 보기를 제공하여 Help Desk 통화를 확인할 수 있습니다. 예를 들어, 메시지가 예상대로 전송되지 않은 경우 해당 메시지에 바이러스가 있는지, 스팸 격리에 보관되었는지 또는 메일 스트림의 어딘가에 있는지 확인할 수 있습니다.

특정 이메일 메시지 또는 사용자에게 지정하는 기준과 일치하는 메시지 그룹을 검색할 수 있습니다.

참고 메시지 추적을 사용하여 메시지의 내용을 읽을 수 없습니다.

메시지 추적 활성화

참고 메시지 추적 데이터는 이 기능을 활성화한 후에 처리되는 메시지에 대해서만 유지됩니다.

시작하기 전에

- 메시지 추적에서 첨부 파일 이름을 검색하고 표시하고 로그 파일에서 첨부 파일 이름을 보려면 메시지 필터 또는 콘텐츠 필터와 같은 본문 검사 프로세스를 최소한 하나 이상 구성하고 활성화해야 합니다.
- 제목별 검색을 지원하려면 제목 헤더를 기록하도록 로그 파일을 구성해야 합니다. 자세한 내용은 38 장, "로깅"을 참조하십시오.
- 중앙 집중식 추적을 설정할 경우:
  이 Email Security 어플라이언스의 중앙 집중식 메시지 추적을 지원하도록 보안 관리 어플라이언스를 설정합니다. *Cisco Content Security Management Appliance 사용 설명서*를 참조하십시오.

절차

1단계 **Services(서비스) > Centralized Services(중앙 집중식 서비스) > Message Tracking(메시지 추적)**을 클릭합니다.

이 서비스를 중앙 집중화할 계획이 없는 경우에도 이 경로를 사용합니다.

2단계 **Enable Message Tracking Service(메시지 추적 서비스 활성화)**를 선택합니다.

3단계 시스템 설정 마법사를 실행한 후에 메시지 추적을 처음으로 활성화할 경우 최종 사용자 라이센스 계약을 검토하고 **Accept(동의)**를 클릭합니다.

4단계 메시지 추적 서비스를 선택합니다.

Option	설명
로컬 추적	이 어플라이언스에서 메시지 추적을 사용합니다.
중앙 추적	보안 관리 어플라이언스를 사용하여 이를 포함한 여러 Email Security 어플라이언스의 메시지를 추적할 수 있습니다.

5단계 (선택 사항) 해당 확인란을 선택하여 거부된 연결의 정보를 저장할 수 있습니다.

최고의 성능을 얻으려면 이 설정을 선택하지 마십시오.

6단계 변경 사항을 제출하고 커밋합니다.

향후 작업

로컬 추적을 선택한 경우:

- DLP 위반과 관련된 콘텐츠에 액세스할 수 있는 사람을 선택합니다. 메시지 추적 시 중요 정보의 액세스 제어, 32-5페이지를 참조하십시오.
- (선택 사항) 메시지 저장을 위한 디스크 공간 할당을 조정합니다. 디스크 공간 관리, 33-15페이지를 참조하십시오.

메시지 검색

절차

1단계 **Monitor(모니터링) > Message Tracking(메시지 추적)을 선택합니다.**

2단계 검색 조건을 입력합니다.

- 모든 옵션을 보려면 **Advanced(고급)** 링크를 클릭합니다.
- 추적은 와일드카드 문자 또는 정규식을 지원하지 않습니다.
- 검색 추적은 대/소문자를 구분하지 않습니다.
- 달리 명시되지 않는 한 쿼리는 "AND" 검색입니다. 즉, 쿼리가 검색 필드에 지정된 *모든* 조건과 일치하는 메시지를 반환합니다. 예를 들어, 봉투 수신자와 제목 줄 매개변수에 대한 텍스트 문자열을 지정하면 쿼리가 지정된 봉투 수신자*와* 제목 줄이 *모두* 일치하는 메시지만 반환됩니다.
- 검색 조건은 다음과 같습니다.

Option	설명
봉투 발신자	**Begins With**, **Is** 또는 **Contains**를 선택한 다음 찾을 이메일 주소, 사용자 이름 또는 메시지 발신자의 도메인을 입력합니다. 모든 문자를 입력할 수 있습니다. 항목 검증이 수행되지 않습니다.
봉투 수신자	**Begins With**, **Is** 또는 **Contains**를 선택하고 찾을 이메일 주소, 사용자 이름 또는 메시지 수신자의 도메인을 입력합니다. 모든 문자를 입력할 수 있습니다. 항목 검증이 수행되지 않습니다.
제목	**Begins With**, **Is** 또는 **Contains**를 선택하고 메시지 제목 줄에 검색할 텍스트 문자열을 입력합니다. **경고**: 규정에서 그러한 검색을 금지하는 환경에서는 이 유형의 검색을 사용하지 마십시오.
메시지 수신됨	날짜 및 시간 범위를 지정합니다. 날짜를 지정하지 않으면 쿼리가 모든 날짜의 데이터를 반환합니다. 시간 범위만 지정하면 쿼리가 사용 가능한 모든 날짜 전체에서 해당 시간 범위의 데이터를 반환합니다. Email Security 어플라이언스가 수신한 메시지의 로컬 날짜와 시간을 사용합니다.
고급 옵션:	
발신자 IP 주소/도메인/네트워크 소유자	원격 호스트의 IP 주소, 도메인 또는 네트워크 소유자를 지정합니다. 거부된 연결 내에서만 검색하거나 모든 메시지를 검색할 수 있습니다.
첨부 파일	**Begins With**, **Is** 또는 **Contains**를 선택하고 찾을 첨부 파일의 ASCII 또는 유니코드 텍스트 문자열을 입력합니다. 선행 및 후행 공백은 입력한 텍스트에서 제거되지 *않습니다*. 다음을 수행한 경우에만 첨부 파일의 파일 이름별로 메시지를 검색할 수 있습니다. • 메시지 필터를 사용한 본문 검사 • 콘텐츠 필터를 사용한 본문 검사 • AMP(Advanced Malware Protection) 검사 SHA-256 해시를 기반으로 파일을 식별하는 방법에 대한 자세한 내용은 SHA-256 해시로 파일 식별, 16-13페이지를 참조하십시오.
메시지 이벤트	하나 이상의 메시지 처리 이벤트를 선택합니다. 예를 들어, 전송, 격리 또는 하드 바운스된 메시지를 검색할 수 있습니다. 메시지 이벤트가 "OR" 연산자를 통해 추가됨: 여러 이벤트를 선택하면 사용자가 지정하는 *모든* 조건과 일치하는 메시지를 검색합니다.
메시지 ID 헤더	SMTP 메시지 ID 헤더의 텍스트 문자열을 입력합니다. 이 RFC 822 메시지 헤더가 각 이메일 메시지를 고유하게 식별합니다. 메시지 ID 헤더는 메시지가 처음으로 생성될 때 메시지에 삽입됩니다.
Cisco IronPort MID	검색할 메시지 수를 입력합니다. IronPort MID가 Email Security 어플라이언스에서 각 이메일 메시지를 고유하게 식별합니다.
쿼리 설정	기본 쿼리 시간 초과와 반환할 최대 결과 수를 변경합니다.

3단계 **Search(검색)**를 클릭하여 쿼리를 제출합니다.

쿼리 결과가 페이지의 하단에 표시됩니다.

관련 주제

- 메시지 추적 검색 결과 사용, 29-4페이지

메시지 추적 검색 결과 사용

다음 사항을 기억하십시오.

- 검색 결과는 구성에 따라 다릅니다. 예를 들어, 사용자가 필터링하지 않은 URL 범주에서 메시지를 검색할 경우 결과를 찾을 수 없습니다.
- Advanced Malware Protection(파일 평판 검사 및 파일 분석)을 포함한 검색에 대한 내용은 메시지 추적 및 Advanced Malware Protection 기능 정보, 16-15페이지를 참조하십시오.

검색 결과를 사용할 때 수행할 수 있는 작업:

- 검색 결과를 검색 조건으로 반환하고, 고급을 클릭하고, 쿼리 설정으로 스크롤한 다음 최대 결과 수를 1,000으로 설정하여 250개 이상의 검색 결과를 표시합니다.
- 검색 결과 섹션의 오른쪽 상단에서 옵션을 선택하여 페이지당 더 많은 결과를 표시합니다.
- 검색 결과 섹션의 오른쪽 상단에서 여러 검색 결과 페이지를 탐색합니다.
- 조건으로 추가할 검색 결과의 값에 커서를 올려 검색 결과를 좁힙니다. 주황색 강조 표시가 나타나면 값을 클릭하여 해당 조건으로 검색을 좁힙니다. 그러면 추가 조건이 검색 조건에 추가됩니다. 예를 들어, 특정 수신자에게 전송된 메시지를 검색할 경우 검색 결과에서 발신자 이름을 클릭하여 사용자가 처음에 지정한 시간 범위 내에 해당 발신자가 수신자에게 보낸 모든 메시지(다른 조건을 충족하는 메시지 포함)를 찾습니다.
- 검색 조건과 일치하는 메시지가 1,000개 이상인 경우 검색 결과 섹션의 오른쪽 상단에 있는 링크인 Export All(모두 내보내기)을 클릭하고 최대 50,000개의 검색 결과를 쉼표로 구분된 값 파일로 내보내고 다른 애플리케이션의 데이터를 사용할 수 있습니다.
- 해당 메시지의 행에서 Show Details(세부사항 표시)를 클릭하여 메시지에 대한 자세한 내용을 볼 수 있습니다. 메시지 세부사항이 포함된 새로운 브라우저 창이 열립니다.
- 격리된 메시지의 경우 메시지 추적 검색 결과의 링크를 클릭하여 메시지가 격리된 이유와 같은 세부사항을 볼 수 있습니다.

참고 보고서 페이지의 링크를 클릭하여 메시지 추적에서 메시지 세부사항을 확인했으나 결과 집합이 예상과 다른 경우, 이는 사용자가 검토하는 기간 동안 보고와 추적이 동시에, 연속해서 활성화되지 않았을 때 발생할 수 있습니다.

관련 주제

- 메시지 세부사항, 29-5페이지

메시지 세부사항

항목	설명
봉투 및 헤더 요약 섹션:	
수신 시간	Email Security 어플라이언스가 메시지를 수신한 시간입니다. 날짜 및 시간이 Email Security 어플라이언스에 구성된 로컬 시간을 사용해 표시됩니다.
MID	고유한 IronPort 메시지 ID입니다.
메시지 크기	메시지 크기입니다.
제목	메시지의 제목 줄입니다. 메시지에 제목이 없거나 로그 파일이 제목 헤더를 기록하도록 구성되지 않은 경우 추적 결과의 제목 줄에 "(제목 없음)" 값이 포함될 수 있습니다. 자세한 내용은 38 장, "로깅"을 참조하십시오.
봉투 발신자	SMTP 봉투의 발신자 주소입니다.
봉투 수신자	배포에서 별칭 확장에 별칭 테이블을 사용할 경우, 검색을 통해 원래 봉투 주소가 아닌 확장된 수신자 주소를 찾을 수 있습니다. 별칭 테이블에 대한 자세한 내용은 "라우팅 및 전송 기능 구성" 장의 "별칭 테이블 생성"을 참조하십시오. 그 밖의 모든 경우에 메시지 추적 쿼리를 통해 원래 봉투 수신자 주소를 찾을 수 있습니다.
메시지 ID 헤더	RFC 822 메시지 헤더입니다.
SMTP 인증 사용자 ID	발신자가 SMTP 인증을 사용하여 메시지를 전송한 경우 발신자의 SMTP 인증 사용자 이름입니다. 그렇지 않을 경우 이 값은 "N/A"입니다.
첨부 파일	메시지에 첨부된 파일의 이름입니다. 쿼리한 이름의 첨부 파일이 최소한 하나 이상 포함된 메시지가 검색 결과에 나타납니다. 일부 첨부 파일은 추적할 수 없습니다. 성능 상의 이유로 인해 첨부 파일 이름 검사는 다른 검사 작업(예: 메시지 또는 콘텐츠 필터, DLP 또는 고지 사항 스탬핑)의 일부로 발생합니다. 첨부 파일 이름은 첨부 파일이 여전히 첨부된 상태에서 본문 검사를 통과하는 메시지에만 사용할 수 있습니다. 다음과 같은 경우(단, 이에 국한되지 않음)에는 첨부 파일 이름이 검색 결과에 나타나지 않습니다. • 시스템이 콘텐츠 필터만 사용하고 메시지가 삭제되거나 첨부 파일이 안티스팸 또는 안티스팸 필터를 통해 제거된 경우 • 메시지 분할 정책이 본문 검사가 진행되기 전에 일부 메시지에서 첨부 파일을 제거하는 경우 성능 상의 이유로 OLE 개체 또는 .ZIP 파일 등의 아카이브와 같은 첨부 파일 내의 파일 이름이 검색되지 않습니다.
발신 호스트 요약 섹션	
역방향 DNS 호스트 이름	역방향 DNS(PTR) 조회를 통해 확인된 전송 호스트의 이름입니다.
IP 주소	전송 호스트의 IP 주소입니다.

항목	설명
SBRS 점수	SenderBase Reputation 점수입니다. 범위는 10(신뢰할 수 있는 발신자일 수 있음)~-10(명백한 스패머)입니다. "없음" 점수는 메시지가 처리되었을 때 이 호스트에 대한 정보가 없었음을 나타냅니다. SBRS에 대한 자세한 내용은 6 장, "발신자 평판 필터링"을 참조하십시오.
처리 세부사항 섹션	
요약 정보 (요약 탭은 DLP 일치 콘텐츠 탭도 있는 경우에만 표시됩니다. 요약 정보는 항상 표시됩니다.)	요약 섹션에는 메시지 처리 도중 기록된 상태 이벤트가 표시됩니다. 항목에는 안티스팸 및 안티바이러스 검사와 같은 메일 정책 처리와 메시지 분할 및 콘텐츠 필터 또는 메시지 필터를 통해 추가된 사용자 지정 로그 항목과 같은 기타 이벤트에 대한 정보가 포함됩니다. 메시지가 전송되면 전송 세부정보가 여기에 표시됩니다. 마지막으로 기록된 이벤트가 처리 세부사항에서 강조 표시됩니다.
DLP 일치 콘텐츠 탭	이 탭은 DLP 정책에 걸린 메시지에 대해서만 표시됩니다. 여기에는 DLP 정책 일치를 트리거한 민감한 콘텐츠뿐 아니라 일치에 대한 정보도 포함됩니다. 이 정보에 액세스할 수 있는 사람을 제어할 수 있습니다. 메시지 추적 시 중요 정보의 액세스 제어, 32-5페이지를 참조하십시오.

관련 주제

- 메시지 검색, 29-2페이지

메시지 추적 데이터 가용성 확인

데이터에서 누락 간격을 식별할 뿐 아니라 메시지 추적 데이터가 포함되는 날짜 범위를 결정할 수 있습니다.

절차

1단계 **Email(이메일) > Message Tracking(메시지 추적) > Message Tracking Data Availability(메시지 추적 데이터 가용성) 선택Monitor(모니터링) > Message Tracking(메시지 추적)**을 선택합니다.

2단계 검색 상자의 오른쪽 상단에서 **Data in time range:(시간 범위의 데이터:)**를 조회합니다.

3단계 **Data in time range:(시간 범위의 데이터:)**에 대해 표시된 값을 클릭합니다.

관련 주제

- 메시지 추적 및 업그레이드 정보, 29-6페이지

메시지 추적 및 업그레이드 정보

새 메시지 추적 기능이 업그레이드 전에 처리된 메시지에 적용되지 않을 수 있습니다. 그러한 메시지의 경우는 필수 데이터가 유지되지 않기 때문입니다. 메시지 추적 데이터 및 업그레이드와 관련된 가능한 제한은 릴리스의 릴리스 노트를 참조하십시오.

메시지 추적 문제 해결

관련 주제

- 첨부 파일이 검색 결과에 나타나지 않음, 29-7페이지
- 예상 메시지가 검색 결과에서 누락되었음, 29-7페이지

첨부 파일이 검색 결과에 나타나지 않음

문제 첨부 파일 이름이 없고 검색 결과에 표시되지 않습니다.

솔루션 메시지 추적 활성화, 29-1페이지의 구성 요건을 참조하십시오. 메시지 세부사항, 29-5페이지의 첨부 파일 이름 검색 제한도 참조하십시오.

예상 메시지가 검색 결과에서 누락되었음

문제 검색 결과에 조건을 충족해야 하는 메시지가 포함되지 않았습니다.

솔루션

- 어플라이언스 구성에 따라 여러 검색, 특히 메시지 이벤트가 포함된 검색의 결과가 표시됩니다. 예를 들어, 필터링하지 않은 URL 범주를 검색할 경우 메시지에 해당 범주의 URL이 포함되어 있어도 결과를 찾을 수 없습니다. 예상한 동작을 수행하도록 Email Security 어플라이언스가 올바르게 구성되었는지 확인하십시오. 예를 들어, 메일 정책, 콘텐츠 및 메시지 필터, 격리 설정을 확인하십시오.
- 보고서의 링크를 클릭한 후 예상한 정보가 누락된 경우 이메일 보고서 문제 해결, 28-37페이지를 참조하십시오.

30 장

정책, 바이러스 및 신종 바이러스 격리

정책, 바이러스 및 신종 바이러스 격리의 개요

"정책, 바이러스 및 신종 바이러스 격리"에는 파일 분석 격리를 포함해 모든 비 스팸 격리가 포함됩니다.

Email Security 어플라이언스가 수신 또는 발송 메시지에서 조직에서 허용하지 않는 가능한 맬웨어 또는 콘텐츠를 탐지한 경우 그러한 메시지를 즉시 삭제하지 않고 격리로 보낼 수 있습니다. 격리가 이러한 메시지를 Email Security 어플라이언스 또는 Cisco Content 보안 관리 어플라이언스에 일정 기간 동안 안전하게 보관하므로 메시지를 검토하거나 메시지의 안전을 더 잘 평가하는 업데이트를 기다릴 수 있습니다.

조직에서 비 스팸 격리를 사용할 수 있는 방법을 보여주는 예:

- **정책 시행.** 인사부 담당자 또는 법무부서에서 모욕적이거나 기밀로 처리해야 하거나 허용되지 않는 정보가 포함될 수 있는지 검토하게 합니다.
- **바이러스 격리.** 바이러스가 사용자에게 확산되는 것을 방지하기 위해 감염된 메시지 또는 암호화된 메시지로 표시되거나 안티바이러스 검사로 검사할 수 없는 메시지를 저장합니다.
- **신종 바이러스 방지.** 신종 바이러스 필터(Outbreak Filter)에 의해 플래그가 지정된 메시지는 신종 바이러스 또는 소규모 맬웨어 공격의 일부일 수 있으므로 안티바이러스 또는 안티스팸 업데이트가 릴리스될 때까지 보관합니다.
- **파일 분석 격리.** 맬웨어가 포함되었을 수 있는 첨부 파일이 있고 분석을 위해 전송된 메시지는 판정에 도달할 때까지 저장합니다.

관련 항목

- 격리 유형, 30-2페이지
- 31 장, "스팸 격리"

격리 유형

쿼런틴 유형	쿼런틴 이름	시스템에서 기본적으로 생성됩니까?	설명	추가 정보
AMP(Advanced Malware Protection)	파일 분석	예	판정에 도달할 때까지 파일 분석을 위해 전송된 메시지를 보관합니다. 특수 문자의 경우 다음을 참조하십시오. • 분석을 위해 전송된 첨부 파일이 포함된 메시지 격리, 16-9페이지	• 정책,바이러스 및 신종 바이러스 격리 관리, 30-3페이지 • 정책,바이러스 또는 신종 바이러스 격리의 메시지 사용, 30-10페이지
바이러스	바이러스	예	안티바이러스 엔진에서 맬웨어를 전송할 수 있는 메시지로 판단한 메시지를 보관합니다.	
신종 바이러스	신종 바이러스	예	스팸 또는 맬웨어로 의심되어 신종 바이러스 필터(Outbreak Filter)에 걸린 메시지를 보관합니다.	
정책	정책	예	메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업에 걸린 메시지를 보관합니다. 기본 정책 격리가 생성되었습니다.	
	미분류	예	메시지 필터, 콘텐츠 필터 또는 DLP 메시지 작업에 지정된 격리가 삭제된 경우에만 메시지를 보관합니다. 이 격리를 필터 또는 메시지 작업에 할당할 수 없습니다.	
	(사용자가 만든 정책 격리)	아니요	메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업에 사용하기 위해 만든 정책 격리.	
스팸	스팸	예	메시지의 수신자 또는 관리자가 검토 후에 스팸 또는 의심스러운 스팸으로 판단한 메시지를 보관합니다. 스팸 격리는 정책, 바이러스 및 신종 바이러스 격리 그룹에 포함되지 않으며 다른 모든 격리와 별개로 관리됩니다.	31 장, "스팸 격리"

정책, 바이러스 및 신종 바이러스 격리 관리

정책, 바이러스 및 신종 바이러스 격리에 사용할 디스크 공간 할당

정책, 바이러스 및 신종 바이러스 격리에 사용되는 디스크 공간 정보는 디스크 공간 관리, 33-15페이지를 참조하십시오.

격리가 중앙 집중화된 경우에도 정책, 바이러스 및 신종 바이러스 격리가 Email Security 어플라이언스의 일부 디스크 공간을 사용합니다.

여러 격리의 메시지가 단일 격리의 메시지와 동일한 디스크 공간을 사용합니다.

관련 주제

- 격리 상태, 용량 및 활동 모니터링, 30-7페이지
- 격리 디스크 공간 사용에 대한 경고, 30-8페이지
- 격리의 메시지 보관 시간, 30-3페이지

격리의 메시지 보관 시간

다음과 같은 상황에서는 메시지가 격리에서 자동으로 제거됩니다.

- 정상 만료 - 격리의 메시지에 대해 구성된 보관 시간이 충족됩니다. 각 격리에 있는 메시지의 보관 시간을 지정합니다. 각 메시지에 특정 자체 만료 시간이 지정되어 있으며 격리 목록에 표시됩니다. 이 주제에 설명된 다른 상황이 발생하지 않는 하 메시지가 지정된 시간 동안 저장됩니다.

참고 신종 바이러스 필터(Outbreak Filter) 격리에 있는 메시지의 일반 보관 시간은 신종 바이러스 격리가 아닌 각 메일 정책의 신종 바이러스 필터(Outbreak Filter) 섹션에 구성됩니다. 관련 내용은 14 장, "신종 바이러스 필터(Outbreak Filter)"를 참조하십시오.

- 조기 만료 - 구성된 보관 시간에 도달하기 전에 격리에서 메시지가 강제됩니다. 이는 다음 경우에 발생할 수 있습니다.
  - 정책, 바이러스 및 신종 바이러스 격리에 사용할 디스크 공간 할당, 30-3페이지에 정의된 대로 모든 격리의 제한 시간에 도달했습니다.

    크기 제한에 도달한 경우 격리와 관계없이 모든 격리의 크기가 다시 제한 크기 미만이 될 때까지 가장 오래된 메시지가 처리되고 각 메시지에 대해 기본 작업이 수행됩니다. 이 정책은 FIFO(선입 선출) 방식입니다. 여러 격리의 메시지는 가장 최근의 만료 시간에 따라 만료됩니다.

    (선택 사항) 디스크 공간이 부족하므로 릴리스 또는 삭제에서 제외할 개별 격리를 구성할 수 있습니다. 제외할 모든 격리를 구성하고 디스크 공간이 용량에 도달한 경우 새 메시지를 위한 공간을 확보하기 위해 격리의 메시지가 전송됩니다.

    디스크 공간 중요 시점에 경고를 수신하게 됩니다. 격리 디스크 공간 사용에 대한 경고, 30-8페이지를 참조하십시오.
  - 여전히 메시지를 보유하고 있는 격리를 삭제합니다.

메시지가 격리에서 자동으로 제거되면 해당 메시지에 대해 기본 작업이 수행됩니다. 자동으로 처리된 격리 메시지에 대한 기본 작업, 30-4페이지를 참조하십시오.

참고 위 시나리오 외에도 검사 작업(신종 바이러스 필터(Outbreak Filter) 또는 파일 분석)의 결과에 따라 메시지가 격리에서 자동으로 제거될 수 있습니다.

시간 조정이 보관 시간에 미치는 영향

- 일광 절약 시간과 어플라이언스 표준 시간대 변경은 보관 기간에 영향을 주지 않습니다.
- 격리의 보관 시간을 변경하면 새 메시지에만 새 만료 시간이 적용됩니다.
- 시스템 클럭이 변경되면 과거에 만료되었어야 하는 메시지가 다음에 가장 적절한 시간에 만료됩니다.
- 시스템 클럭 변경은 만료 프로세스에 있는 메시지에는 적용되지 않습니다.

자동으로 처리된 격리 메시지에 대한 기본 작업

격리의 메시지 보관 시간, 30-3페이지에 설명된 상황이 발생할 경우 정책, 바이러스 또는 신종 바이러스 격리의 메시지에 대해 기본 작업이 수행됩니다.

다음 2개의 기본 작업이 있습니다.

- 삭제 - 메시지가 삭제됩니다.
- 릴리스 - 메시지가 전송을 위해 릴리스됩니다.

  릴리스 시 메시지가 위협인지 확인하기 위한 재검사가 수행됩니다. 자세한 내용은 격리된 메시지 재검사 정보, 30-17페이지를 참고하십시오.

  또한 예상된 보관 시간이 경과하기 전에 릴리스된 메시지는 X-헤더 추가와 같은 추가 작업이 수행될 수 있습니다. 자세한 내용은 정책, 바이러스 및 신종 바이러스 격리 구성, 30-5페이지를 참고하십시오.

시스템에서 생성한 격리의 설정 확인

격리를 사용하기 전에 미분류 격리를 포함한 기본 격리의 설정을 사용자 지정합니다.

관련 주제

- 정책, 바이러스 및 신종 바이러스 격리 구성, 30-5페이지

정책, 바이러스 및 신종 바이러스 격리 구성

시작하기 전에

- 기존 격리를 편집하려면 정책, 바이러스 및 신종 바이러스 격리 설정 정보, 30-6페이지를 참조하십시오.
- 보관 시간 및 기본 작업을 포함하여 격리의 메시지가 자동으로 관리되는 방식을 이해합니다. 격리의 메시지 보관 시간, 30-3페이지 및 자동으로 처리된 격리 메시지에 대한 기본 작업, 30-4페이지를 참조하십시오.
- 각 격리에 액세스할 수 있는 사용자를 결정하고 그에 따라 사용자 및 사용자 지정 역할을 생성합니다. 자세한 내용은 정책, 바이러스 및 신종 바이러스 격리에 액세스할 수 있는 사용자 그룹, 30-9페이지를 참조하십시오.

절차

1단계 **Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택합니다.

2단계 다음 중 하나를 수행합니다.

- **Add Policy Quarantine(정책 격리 추가)**을 클릭합니다.
- 편집할 격리를 클릭합니다.

3단계 정보를 입력합니다.

다음 사항을 기억하십시오.

- 지정한 보관 기간이 종료되기 전에 이 격리의 메시지를 처리하지 *않으려면* 격리 디스크 공간이 가득 찼더라도 **Free up space by applying default action on messages upon space overflow(공간 오버플로 시 메시지에 기본 작업을 적용하여 공간 확보)**를 선택 취소합니다.

  모든 격리에 이 옵션을 선택하지 마십시오. 시스템이 최소한 하나 이상의 격리에서 메시지를 삭제하여 공간을 확보할 수 있어야 합니다.
- 기본 작업으로 **Release(릴리스)**를 선택한 경우 보관 기간이 경과되기 전에 릴리스되는 메시지에 적용할 추가 작업을 지정할 수 있습니다.

옵션	정보
제목 수정	추가할 텍스트를 입력하고 이 텍스트를 원래 메시지 제목의 처음에 추가할지 아니면 끝에 추가할지를 지정합니다. 예를 들어, 사용자가 수신자에게 메시지에 적절하지 않은 내용이 포함되었을 수 있다고 경고하려 할 수 있습니다. **참고** 비 ASCII 문자가 포함된 제목을 올바르게 표시하려면 RFC 2047에 따라 표시해야 합니다.
X-헤더 추가	X-헤더는 메시지에 대해 수행된 작업의 레코드를 제공할 수 있습니다. 이는 예를 들어 특정 메시지가 전송된 이유에 대한 문의를 처리할 때 유용할 수 있습니다. 이름 및 값을 입력합니다. 예: 이름 =`Inappropriate-release-early` 값 = `True`
첨부 파일 제거	첨부 파일을 제거하면 그러한 파일에 있을 수 있는 바이러스로부터 보호할 수 있습니다.

4단계 이 격리에 액세스할 수 있는 사용자를 지정합니다.

사용자	정보
로컬 사용자	로컬 사용자 목록에는 격리에 액세스할 수 있는 역할이 있는 사용자만 포함됩니다. 모든 관리자는 격리에 완전히 액세스할 수 있으므로 이 목록에서는 관리자 권한이 있는 사용자가 제외됩니다.
외부에서 인증된 사용자	외부 인증을 구성해야 합니다.
사용자 지정 사용자 역할	이 옵션은 격리 액세스 권한이 있는 사용자 지정 사용자 역할을 최소한 하나 이상 생성한 경우에만 표시됩니다.

5단계 변경 사항을 제출하고 커밋합니다.

향후 작업

메시지를 격리로 옮길 메시지 필터, 콘텐츠 필터 및 DLP 메시지 작업을 생성합니다. 9 장, "메시지 필터를 사용하여 이메일 정책 적용", 11 장, "콘텐츠 필터" 및 메시지 작업, 17-32페이지를 참조하십시오.

정책, 바이러스 및 신종 바이러스 격리 설정 정보

참고

- 격리의 이름을 변경할 수 없습니다.

- 시간 조정이 보관 시간에 미치는 영향, 30-4페이지도 참조하십시오.

격리 설정을 변경하려면 Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)를 선택한 다음 격리의 이름을 클릭합니다.

정책 격리를 할당할 필터 및 메시지 작업 결정

메시지 필터, 콘텐츠 필터, DLP(데이터 손실 방지) 메시지 작업 및 정책 격리와 연결된 DMARC 검증 프로필을 볼 수 있습니다.

절차

1단계 **Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 클릭합니다.

2단계 확인할 정책 격리의 이름을 클릭합니다.

3단계 페이지 하단으로 스크롤해서 **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 확인합니다. 정책 격리를 할당할 필터 및 메시지 작업 결정, 30-7페이지를 참조하십시오.
- 필터 또는 메시지 작업에 할당되어 있는 경우에도 정책 격리를 삭제할 수 있습니다.
- 비어 있지 않은 격리를 삭제하면 디스크가 꽉 찼을 때 메시지를 삭제하지 않는 옵션을 선택했어도 격리에 정의된 기본 작업이 모든 메시지에 적용됩니다. 자동으로 처리된 격리 메시지에 대한 기본 작업, 30-4페이지를 참조하십시오.
- 필터 또는 메시지 작업과 연결된 격리를 삭제하면 이후에 해당 필터 또는 메시지 작업에 의해 격리된 메시지가 미분류 격리로 전송됩니다. 격리를 삭제하기 전에 미분류 격리의 기본 설정을 사용자 지정해야 합니다.
- 미분류 격리를 삭제할 수 없습니다.

격리 상태, 용량 및 활동 모니터링

모니터링할 항목	수행할 작업
현재 모든 비 스팸 격리에 사용할 수 있는 공간	**Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택하고 테이블 바로 아래를 봅니다.
현재 모든 격리에서 사용하는 총 공간	**Monitor(모니터링) > System Status(시스템 상태)**를 선택하고 **Queue Space Used by Quarantine(격리에서 사용하는 큐 공간)**을 찾습니다.

모니터링할 항목	수행할 작업
현재 각 격리에서 사용하는 공간	**Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택하고 격리 이름을 클릭한 다음 격리 이름 바로 아래의 테이블 행에서 이 정보를 찾습니다.
현재 모든 격리의 총 메시지 수	**Monitor(모니터링) > System Status(시스템 상태)**를 클릭하고 **Active Messages in Quarantine(격리의 활성 메시지)**을 찾습니다.
현재 각 격리의 메시지 수	**Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택하고 격리의 테이블 행을 봅니다.
모든 격리의 총 CPU 사용량	**Monitor(모니터링) > System Status(시스템 상태)**를 선택하고 **CPU Utilization(CPU 사용률)** 섹션을 봅니다.
마지막 메시지가 각 격리에 들어간 날짜 및 시간(정책 격리 사이의 이동 제외)	**Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택하고 격리의 테이블 행을 봅니다.
정책 격리가 생성된 날짜 정책 격리 생성자의 이름	**Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택하고 격리 이름을 클릭한 다음 격리 이름 바로 아래의 테이블 행에서 이 정보를 찾습니다. 시스템에서 생성한 격리에 생성 날짜 및 생성자 이름을 사용할 수 없습니다.
정책 격리와 연결된 필터 및 메시지 작업	정책 격리를 할당할 필터 및 메시지 작업 결정, 30-7페이지를 참조하십시오.

정책 격리 성능

정책 격리에 저장된 메시지는 하드 드라이브 공간 외에도 시스템 메모리를 사용합니다. 단일 어플라이언스의 정책 격리에 수십만 개의 메시지를 저장하면 과도한 메모리 사용으로 인해 어플라이언스의 성능이 저하될 수 있습니다. 어플라이언스가 메시지를 격리, 삭제 및 릴리스하는 데 시간이 더 오래 소요되므로 메시지 처리가 느려지고 이메일 파이프라인이 백업됩니다.

Cisco에서는 Email Security 어플라이언스가 정상적인 속도로 이메일을 처리할 수 있도록 정책 격리에 평균 20,000개 미만의 메시지를 저장할 것을 권장합니다.

격리의 메시지 수를 확인하려면 격리 상태, 용량 및 활동 모니터링, 30-7페이지를 참조하십시오.

격리 디스크 공간 사용에 대한 경고

정책, 바이러스 및 신종 바이러스 격리의 총 크기가 용량의 75%, 85% 및 95%에 도달하거나 이를 초과할 때마다 경고가 전송됩니다. 메시지가 격리에 보관되면 확인이 수행됩니다. 예를 들어, 격리에 메시지를 추가하여 크기가 총 용량의 75%에 도달하거나 이를 초과하면 경고가 전송됩니다. 경고, SNMP 트랩 및 신종 바이러스 필터(Outbreak Filter), 14-24페이지도 참조하십시오.

경고에 대한 자세한 내용은 경고, 33-34페이지를 참조하십시오.

정책 격리 및 로깅

AsyncOS가 격리된 모든 메시지를 개별적으로 기록합니다.

```
Info: MID 482 quarantined to "Policy" (message filter:policy_violation)
```

메시지를 격리한 메시지 필터 또는 신종 바이러스 필터(Outbreak Filter)는 괄호 안에 표시됩니다. 개별 로그 항목이 메시지가 보관된 각 격리에 대해 생성됩니다.

AsyncOS가 격리에서 제거된 메시지도 개별적으로 기록합니다.

```
Info: MID 483 released from quarantine "Policy" (queue full)
```

```
Info: MID 484 deleted from quarantine "Anti-Virus" (expired)
```

예를 들어, 메시지가 모든 격리에서 제거되고 영구적으로 삭제되거나 전송 예약된 후에 시스템에서 개별적으로 메시지를 기록합니다.

```
Info: MID 483 released from all quarantines
```

```
Info: MID 484 deleted from all quarantines
```

메시지가 다시 삽입되면 시스템에서 새로운 MID(메시지 ID)로 새 메시지 개체를 생성합니다. 이는 예를 들어 새 그러면 MID "줄별"로 기존 로그 메시지를 사용하여 기록됩니다.

```
Info: MID 483 rewritten to 513 by Policy Quarantine
```

다른 사용자에게 메시지 처리 작업 분배 정보

다른 관리자에게 메시지 검토 및 처리 작업을 분배할 수 있습니다. 예를 들면 다음과 같습니다.

- 인사 팀은 정책 격리를 검토 및 관리할 수 있습니다.
- 법무 팀은 기밀 자료 격리를 관리할 수 있습니다.

격리에 대한 설정을 지정할 때 이러한 사용자에게 액세스 권한을 할당합니다. 격리에 사용자를 추가하려면 사용자가 이미 있어야 합니다.

각 사용자는 격리의 모든 부분 또는 일부에 액세스할 수 있거나 격리의 어떤 부분에도 액세스할 수 없습니다. 격리를 볼 권한이 없는 사용자에게는 GUI에서 또는 CLI 격리 목록의 어디에도 격리의 존재가 표시되지 않습니다.

관련 주제

- 정책, 바이러스 및 신종 바이러스 격리에 액세스할 수 있는 사용자 그룹, 30-9페이지
- 사용자 계정 작업, 32-1페이지
- 외부 인증, 32-21페이지
- 위임 관리를 위한 사용자 지정 사용자 역할 관리, 32-7페이지

정책, 바이러스 및 신종 바이러스 격리에 액세스할 수 있는 사용자 그룹

관리자가 격리에 액세스하도록 허용할 경우 사용자 그룹에 따라 다음 작업을 수행할 수 있습니다.

- 관리자 그룹격리를 생성, 구성, 삭제 및 중앙 집중화하고 격리된 메시지를 관리할 수 있습니다.
- 격리 관리 권한이 있는 사용자 지정 사용자 역할뿐 아니라 작업자, 게스트, 읽기 전용 작업자 및 헬프 데스크 사용자 그룹의 사용자는 격리에서 메시지를 검색하거나 보거나 처리할 수 있지만 격리의 설정을 변경하거나 격리를 생성, 삭제 또는 중앙 집중화할 수 없습니다. 이러한 사용자 중 각 격리에서 해당 격리에 액세스할 수 있는 사용자를 지정합니다.
- 기술자 그룹의 사용자는 격리에 액세스할 수 없습니다.

메시지 추적 및 데이터 손실 방지와 같은 관련 기능에 대한 액세스 권한도 관리자가 격리 페이지에서 볼 수 있는 옵션 및 정보에 영향을 미칩니다. 예를 들어, 사용자가 메시지 추적에 액세스할 수 없는 경우 해당 사용자에게는 격리된 메시지의 메시지 추적 링크 및 정보가 표시되지 않습니다.

최종 사용자는 정책, 바이러스 및 신종 바이러스 격리를 보거나 액세스할 수 없습니다.

클러스터 구성의 정책, 바이러스 및 신종 바이러스 격리 정보

정책, 바이러스 및 신종 바이러스 격리는 중앙 집중식 관리를 포함한 배포에서 머신 수준에서만 구성할 수 있습니다.

중앙 집중식 정책, 바이러스 및 신종 바이러스 격리 정보

Cisco Content 보안 관리 어플라이언스의 정책, 바이러스 및 신종 바이러스 격리를 중앙 집중화할 수 있습니다. 자세한 내용은 정책, 바이러스 및 신종 바이러스 격리 중앙 집중화 정보, 42-5페이지와 보안 관리 어플라이언스의 사용 설명서를 참조하십시오.

정책, 바이러스 또는 신종 바이러스 격리의 메시지 사용

관련 주제

- 격리의 메시지 보기, 30-11페이지
- 정책, 바이러스 및 신종 바이러스 격리의 메시지 찾기, 30-11페이지
- 격리의 메시지를 수동으로 처리, 30-12페이지
- 여러 격리의 메시지, 30-13페이지
- 메시지 세부사항 및 메시지 콘텐츠 보기, 30-14페이지
- 격리된 메시지 재검사 정보, 30-17페이지
- 신종 바이러스 격리, 30-17페이지

격리의 메시지 보기

변경 후	수행할 작업
격리의 모든 메시지 보기	**Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택합니다. 관련 격리 표의 해당 행에서 **메시지** 열에 있는 파란색 숫자를 클릭합니다.
신종 바이러스 격리의 메시지 보기	• **Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택합니다. 관련 격리 표의 해당 행에서 **메시지** 열에 있는 파란색 숫자를 클릭합니다. • 규칙 요약에 따름 링크, 30-18페이지를 참조하십시오.
격리의 메시지 목록 탐색	이전, 다음, 페이지 번호 또는 이중 화살표를 클릭합니다. 이중 화살표를 클릭하면 목록의 첫 번째 페이지(<<) 또는 마지막(>>) 페이지가 표시됩니다.
격리의 메시지 목록 정렬	열 머리글을 클릭합니다(여러 항목을 포함할 수 있는 열 또는 "다른 격리에 있음" 열 제외).
표 크기 조정	구분선을 열 머리글 사이에서 끕니다.
메시지를 격리한 콘텐츠 보기	일치 콘텐츠 보기, 30-15페이지를 참조하십시오.

관련 주제

- 격리된 메시지 및 국제 문자 집합, 30-11페이지

격리된 메시지 및 국제 문자 집합

제목에 국제 문자 집합의 문자(이중 바이트, 변수 길이 및 비 ASCII 인코딩)가 포함된 메시지의 경우 정책 격리 페이지에 제목 줄이 디코딩된 형식의 비 ASCII 문자로 표시됩니다.

정책, 바이러스 및 신종 바이러스 격리의 메시지 찾기

참고

- 정책, 바이러스 및 신종 바이러스 격리에서 검색을 수행하면 스팸 격리의 메시지를 찾을 수 없습니다.
- 사용자는 액세스 권한이 있는 격리의 메시지만 찾아서 볼 수 있습니다.

절차

1단계 **Monitor(모니터링) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택합니다.

2단계 **Search Across Quarantines(격리 검색)** 버튼을 클릭합니다.

정보 신종 바이러스 격리의 경우 각 신종 바이러스 규칙에 의해 격리된 모든 메시지도 찾을 수 있습니다. 격리 표 행에서 **Manage by Rule Summary(규칙 요약에 따름)** 링크를 클릭한 다음 관련 규칙을 클릭합니다.

3단계 검색할 격리를 선택합니다.

4단계 (선택 사항) 다른 검색 조건을 입력합니다.

- 봉투 발신자와 봉투 수신자의 경우 원하는 문자를 입력할 수 있습니다. 입력 검증이 수행되지 않습니다.
- 검색 결과에는 지정한 *모든* 조건과 일치하는 메시지만 포함됩니다. 예를 들어, 봉투 수신자와 제목을 지정한 경우 봉투 수신자 *및* 제목에 지정된 용어와 일치하는 메시지만 반환됩니다.

향후 작업

격리 목록을 사용하는 것과 동일한 방식으로 검색 결과를 사용할 수 있습니다. 자세한 내용은 격리의 메시지를 수동으로 처리, 30-12페이지를 참고하십시오.

격리의 메시지를 수동으로 처리

수동으로 메시지를 처리한다는 것은 메시지 작업 페이지에서 메시지에 해당하는 메시지 작업을 수동으로 선택함을 의미합니다.

참고 RSA Enterprise Manager를 사용하는 배포의 경우 Email Security 어플라이언스 또는 Enterprise Manager에서 격리된 메시지를 볼 수 있지만 Enterprise Manager를 사용하여 메시지에 대한 작업을 수행해야 합니다. Enterprise Manager에 대한 내용은 17 장, "데이터 유출 방지"를 참조하십시오.

메시지에 대해 다음 작업을 수행할 수 있습니다.

- 삭제
- 릴리스
- 예약된 격리에서의 종료 지연
- 지정한 이메일 주소로 메시지의 사본 전송
- 한 격리에서 다른 격리로 메시지 이동

일반적으로 다음을 수행할 때 표시되는 목록의 메시지에 대해 작업을 수행할 수 있습니다. 그러나 모든 상황에서 모든 작업을 사용할 수 있는 것은 아닙니다.

- Monitor(모니터) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리) 페이지의 격리 목록에서 격리의 메시지 수를 클릭합니다.
- Search Across Quarantines(격리 검색)를 클릭합니다.
- 격리 이름을 클릭하고 격리 내에서 검색합니다.

다음과 같은 방법으로 한 번에 여러 메시지에 대해 이러한 작업을 수행할 수 있습니다.

- 메시지 목록의 상단에 있는 선택 목록에서 옵션을 선택합니다.
- 페이지에 나열된 각 메시지 옆의 확인란을 선택합니다.
- 메시지 목록의 상단에 있는 표 머리글의 확인란을 선택합니다. 그러면 화면에 표시되는 모든 메시지에 작업이 적용됩니다. 다른 페이지의 메시지는 영향을 받지 않습니다.

신종 바이러스 격리의 메시지에 추가 옵션을 사용할 수 있습니다. 신종 바이러스 격리 및 규칙 요약에 따름 보기, 14-22페이지를 참조하십시오.

관련 주제

- 메시지 사본 전송, 30-13페이지
- 정책 격리 간 메시지 이동 정보, 30-13페이지
- 여러 격리의 메시지, 30-13페이지
- 자동으로 처리된 격리 메시지에 대한 기본 작업, 30-4페이지

메시지 사본 전송

관리자 그룹에 속한 사용자만 메시지의 사본을 보낼 수 있습니다.

메시지의 사본을 보내려면 사본 받는 사람: 필드에 이메일 주소를 입력하고 **Submit(제출)**을 클릭합니다. 메시지의 사본을 전송하면 메시지에 대해 다른 작업이 수행되지 않습니다.

정책 격리 간 메시지 이동 정보

단일 어플라이언스에서 수동으로 한 정책 격리에서 다른 정책 격리로 메시지를 이동할 수 있습니다.

다른 격리로 메시지를 이동할 경우:

- 만료 시간이 변경되지 않습니다. 메시지의 원래 격리 보관 시간이 유지됩니다.
- 일치 콘텐츠 및 다른 관련 세부사항을 포함하여 메시지가 격리된 이유가 변경되지 않습니다.
- 메시지가 여러 격리에 있고 이미 해당 메시지의 사본이 있는 대상으로 메시지를 이동할 경우 이동된 메시지 사본의 만료 시간 및 격리 이유가 대상 격리에 원래 있던 메시지 사본의 만료 시간 및 격리 이유를 덮어씁니다.

여러 격리의 메시지

메시지가 하나 이상의 다른 격리에 있는 경우 사용자에게 그러한 다른 격리에 대한 액세스 권한이 있는지에 관계없이 격리 메시지 목록의 "다른 격리에 있음" 열에 "예"가 표시됩니다.

하나의 메시지가 여러 격리에 있는 경우:

- 메시지가 상주하는 모든 격리에서 릴리스되지 않는 한 전송되지 않습니다. 격리에서 삭제되면 전송되지 않습니다.
- 메시지가 상주하는 모든 격리에서 삭제 또는 릴리스될 때까지 격리에서 삭제되지 않습니다.

메시지를 릴리스하려는 사용자에게 메시지가 상주하는 모든 격리에 액세스할 수 있는 권한이 없으므로 다음 규칙이 적용됩니다.

- 메시지가 상주하는 모든 격리에서 릴리스될 때까지 격리에서 릴리스되지 않습니다.

- 메시지가 격리에 삭제됨으로 표시된 경우 메시지가 상주하는 다른 격리에서 전송할 수 없습니다. (여전히 릴리스될 수는 있습니다.)

메시지가 여러 격리에서 큐에 대기 중이고 사용자에게 하나 이상의 다른 격리에 액세스할 수 있는 권한이 없는 경우:

- 사용자는 액세스 권한이 있는 각각의 격리에 메시지가 있는지 알려주는 알림을 받게 됩니다.
- GUI에 사용자가 액세스할 수 있는 격리의 예약된 종료 시간만 표시됩니다. (지정된 메시지의 경우 각 격리에 별도의 종료 시간이 있습니다.)
- 사용자에게 메시지가 보관된 다른 격리의 이름이 표시되지 않습니다.
- 사용자는 액세스 권한이 없는 격리로 메시지를 옮긴 일치 콘텐츠가 표시되지 않습니다.
- 메시지를 릴리스하면 사용자가 액세스할 수 있는 큐만 영향을 받습니다.
- 사용자가 액세스할 수 없는 다른 격리에서도 메시지가 큐에 대기 중인 경우 나머지 격리에 대한 필수 액세스 권한이 있는 사용자가 작업을 수행할 때까지(또는 조기 또는 정상 만료를 통해 메시지가 "정상적으로" 릴리스될 때까지) 메시지가 격리에 변경되지 않은 상태로 남게 됩니다.

메시지 세부사항 및 메시지 콘텐츠 보기

메시지의 콘텐츠를 보고 격리된 메시지 페이지에 액세스할 메시지의 제목 줄을 클릭합니다.

격리된 메시지 페이지는 2개의 섹션(격리 세부사항 및 메시지 세부사항)으로 이루어져 있습니다.

격리된 메시지 페이지에서 메시지를 읽거나, 메시지 작업을 선택하거나, 메시지의 사본을 보내거나, 바이러스를 테스트할 수 있습니다. 또한 메시지가 전송 시 암호화 필터 작업으로 인해 격리에서 릴리스될 때 암호화되는지 확인할 수 있습니다.

메시지 세부사항 섹션에는 메시지 본문, 메시지 헤더 및 첨부 파일이 표시됩니다. 메시지 본문의 처음 100K만 표시됩니다. 메시지가 더 긴 경우 처음 100K가 표시된 다음 줄임표(...)가 표시됩니다. 실제 메시지는 잘리지 않습니다. 이는 표시 목적으로만 사용됩니다. 메시지 세부사항의 하단에 있는 메시지 부분 섹션에서 `[message body]`를 클릭하여 메시지 본문을 다운로드할 수 있습니다. 또한 첨부 파일의 파일 이름을 클릭하여 메시지의 첨부 파일을 다운로드할 수 있습니다.

바이러스가 포함된 메시지를 보고 컴퓨터에 데스크탑 안티바이러스 소프트웨어가 설치된 경우 안티바이러스 소프트웨어가 바이러스 발견 시 알림을 표시할 수 있습니다. 이는 컴퓨터에 위협이 되지 않으며 안전하게 무시할 수 있습니다.

메시지에 대한 자세한 내용을 보려면 **Message Tracking(메시지 추적)** 링크를 클릭합니다.

참고 특별 신종 바이러스 격리의 경우 추가 기능이 제공됩니다. 신종 바이러스 격리, 30-17페이지를 참조하십시오.

관련 주제

- 일치 콘텐츠 보기, 30-15페이지
- 첨부 파일 다운로드, 30-16페이지
- 바이러스 테스트, 30-16페이지

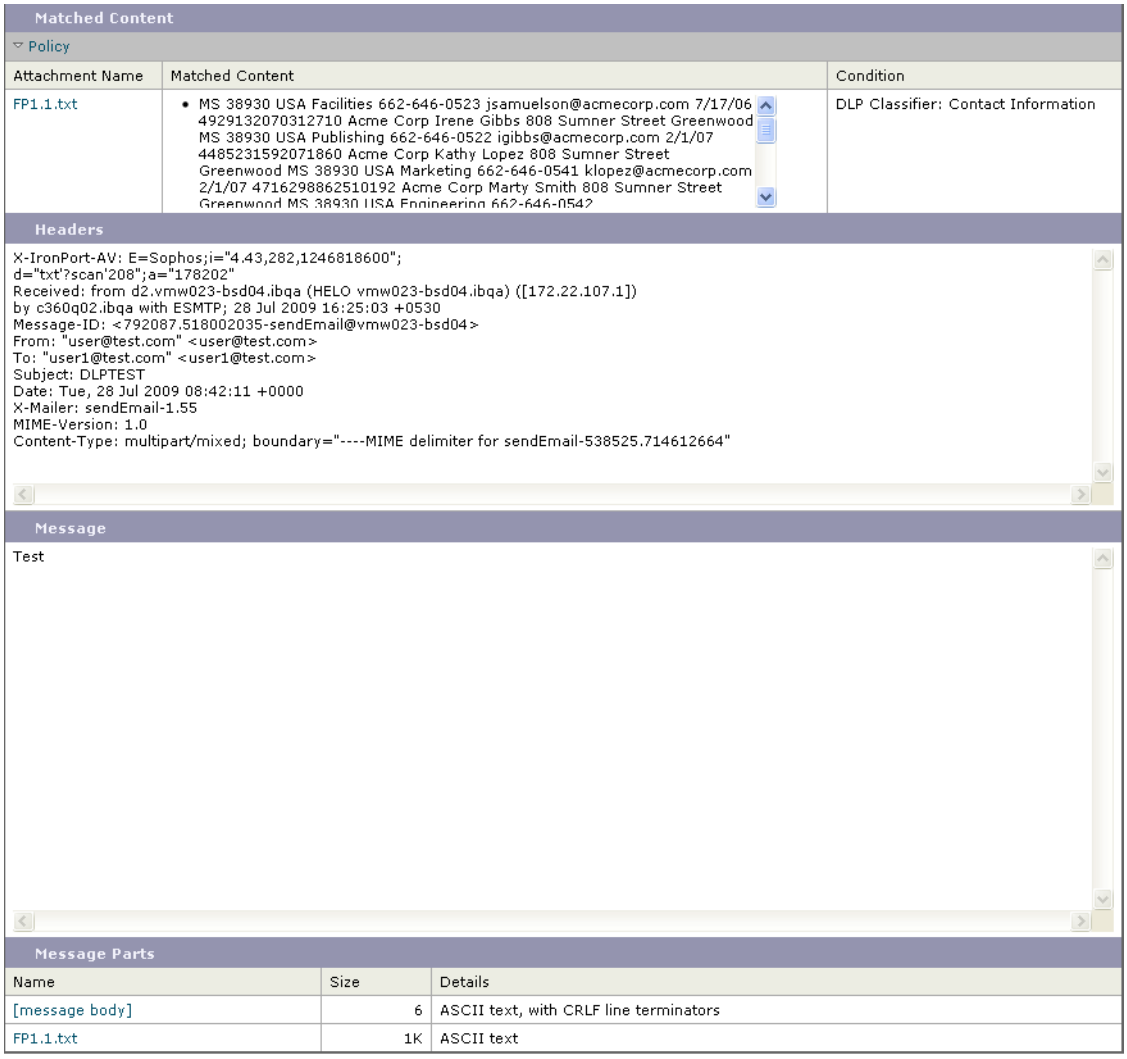
일치 콘텐츠 보기

첨부 파일 콘텐츠 조건, 메시지 본문 또는 첨부 파일 조건, 메시지 본문 조건 또는 첨부 파일 콘텐츠 조건과 일치하는 메시지에 대해 격리 작업을 구성할 경우 격리된 메시지에서 일치 콘텐츠를 볼 수 있습니다. 메시지 본문을 표시하면 DLP 정책 위반 일치를 제외하고 일치 콘텐츠가 노란색으로 강조 표시됩니다. 또한 `$MatchedContent` 작업 변수를 사용하여 메시지 또는 콘텐츠 필터 일치의 일치 콘텐츠를 메시지 제목에 포함할 수 있습니다.

첨부 파일에 일치 콘텐츠가 포함된 경우 DLP 정책 위반, 콘텐츠 필터 조건, 메시지 필터 조건 또는 이미지 분석 판정 등 격리된 이유뿐 아니라 첨부 파일의 콘텐츠도 표시됩니다.

메시지 또는 콘텐츠 필터 규칙을 트리거한 로컬 격리에서 메시지를 볼 경우 GUI에 필터 작업을 트리거한 콘텐츠와 함께 실제로 필터 작업을 트리거하지 않는 콘텐츠가 표시될 수 있습니다. GUI 표시는 콘텐츠 일치를 찾는 지침으로 사용해야 하지만 반드시 정확한 콘텐츠 일치 목록을 반영해야 하는 것은 아닙니다. 이는 GUI가 필터에 사용되는 것보다 덜 엄격한 콘텐츠 일치 논리를 사용하기 때문에 발생합니다. 이 문제는 메시지 본문에서 강조 표시된 부분에만 적용됩니다. 관련 필터 규칙과 함께 메시지의 각 부분의 일치 문자열을 나열하는 표가 올바릅니다.

그림 30-1 정책 격리에 표시되는 일치 콘텐츠



첨부 파일 다운로드

메시지 부분 또는 일치 콘텐츠 섹션에서 첨부 파일의 파일 이름을 클릭하여 메시지 첨부 파일을 다운로드할 수 있습니다. AsyncOS가 알 수 없는 소스의 첨부 파일에 바이러스가 포함되었을 수 있음을 알리고 계속할 것인지 묻는 경고를 표시합니다. 바이러스가 포함되었을 수 있는 첨부 파일을 다운로드할 경우 그에 따른 위험은 사용자가 부담합니다. 메시지 부분 섹션에서 `[message body]`를 클릭하여 메시지 본문을 다운로드할 수도 있습니다.

바이러스 테스트

메시지에 바이러스가 있는지 테스트하려면 **Start Test(테스트 시작)**를 클릭합니다. 격리를 사용해 안티바이러스 서명이 업데이트될 때까지 메시지를 보관합니다.

바이러스 테스트를 수행하면 메시지 자체가 아닌 메시지의 사본이 안티바이러스 엔진에 전송됩니다. 안티바이러스 엔진의 판정이 반환되어 격리 영역 위에 표시됩니다.

격리된 메시지 재검사 정보

메시지가 격리된 모든 큐에서 메시지가 릴리스될 경우 어플라이언스에서 활성화된 기능과 처음에 메시지를 격리한 메일 정책에 따라 다음 재검사가 발생합니다.

- 정책 및 바이러스 격리에서 릴리스된 메시지는 안티바이러스 엔진을 통해 검사됩니다.
- 신종 바이러스 격리에서 릴리스된 메시지는 안티스팸 및 안티바이러스 엔진을 통해 검사됩니다. (신종 바이러스 격리의 메시지 재검사에 대한 내용은 14 장, "신종 바이러스 필터(Outbreak Filter)"를 참조하십시오.)
- 파일 분석 격리에서 릴리스된 메시지는 위협이 있는지 재검사됩니다.
- 첨부 파일이 있는 메시지는 정책, 바이러스 및 신종 바이러스 격리에서 릴리스될 때 파일 평판 서비스를 통해 재검사됩니다.

재검사 시 나온 판정이 이전에 메시지가 처리되었을 때 나온 판정과 일치할 경우 메시지가 다시 격리되지 않습니다. 반대로 판정이 다를 경우에는 메시지가 다른 격리로 보내질 수 있습니다.

이는 메시지가 무한정 격리로 되돌아가는 것을 방지하기 위한 것입니다. 예를 들어, 메시지가 암호화되어 바이러스 격리로 전송되었다고 가정해 보겠습니다. 관리자가 메시지를 릴리스하면 안티바이러스 엔진은 여전히 메시지의 암호를 해독할 수 없지만 메시지가 다시 격리되거나 루프가 생성되어야 하므로 메시지가 격리에서 릴리스되지 않습니다. 2개의 판정이 동일하므로 시스템이 두 번째에는 바이러스 격리를 우회합니다.

신종 바이러스 격리

신종 바이러스 격리는 유효한 신종 바이러스 필터(Outbreak Filter) 기능 라이센스 키를 입력한 경우에 나타납니다. 신종 바이러스 필터(Outbreak Filter) 기능은 설정된 임계값에 따라 메시지를 신종 바이러스 격리로 보냅니다. 자세한 내용은 14 장, "신종 바이러스 필터(Outbreak Filter)"를 참조하십시오.

신종 바이러스 격리 기능은 다른 격리와 비슷합니다. 즉, 메시지를 검색하거나, 릴리스 또는 삭제하는 등의 작업을 수행할 수 있습니다.

신종 바이러스 격리에는 규칙 요약에 따름 링크, 메시지 세부사항을 볼 때 선택할 수 있는 Cisco로 전송 기능, 검색 결과의 메시지를 예약된 종료 시간별로 정렬할 수 있는 옵션 등 다른 격리에서 사용할 수 없는 몇 가지 추가 기능이 있습니다.

신종 바이러스 필터(Outbreak Filter) 기능의 라이센스가 만료되면 신종 바이러스 격리에 메시지를 추가할 수 없게 됩니다. 현재 격리에 있는 메시지가 만료되어 신종 바이러스 격리가 비게 되면 GUI의 격리 목록에 더 이상 표시되지 않습니다.

관련 주제

- 신종 바이러스 격리의 메시지 재검사, 30-17페이지
- 규칙 요약에 따름 링크, 30-18페이지
- Cisco Systems에 잘못된 긍정 또는 의심스러운 메시지 보고, 30-18페이지

신종 바이러스 격리의 메시지 재검사

신종 바이러스 격리에 보관된 메시지는 새로 게시된 규칙이 격리된 메시지를 더 이상 위협으로 간주하지 않을 경우에 자동으로 릴리스됩니다.

어플라이언스에서 안티스팸 및 안티바이러스가 활성화된 경우 검사 엔진이 메시지에 적용된 메일 흐름 정책에 따라 신종 바이러스 격리에서 릴리스된 모든 메시지를 검사합니다.

규칙 요약에 따름 링크

격리 목록에서 신종 바이러스 격리 옆의 규칙 요약에 따름 링크를 클릭하여 규칙 요약에 따름 페이지를 볼 수 있습니다. 메시지를 격리한 신종 바이러스 규칙에 따라 격리에 있는 모든 메시지에 대해 메시지 작업(릴리스, 삭제, 종료 지연)을 수행할 수 있습니다. 이는 신종 바이러스 격리에서 많은 메시지를 지우는 경우에 유용합니다. 자세한 내용은 신종 바이러스 격리 및 규칙 요약에 따름 보기, 14-22페이지 아래의 항목을 참조하십시오

Cisco Systems에 잘못된 긍정 또는 의심스러운 메시지 보고

신종 바이러스 격리의 메시지에 대한 메시지 세부사항을 볼 경우 해당 메시지를 Cisco로 보내 잘못된 긍정 또는 의심스러운 메시지를 보고할 수 있습니다.

절차

1단계 신종 바이러스 격리의 메시지로 이동합니다.

2단계 메시지 세부사항 섹션에서 **Send a Copy to Cisco Systems(Cisco Systems에 사본 전송)** 확인란을 선택합니다.

3단계 **Send(보내기)**를 클릭합니다.

31 장

스팸 격리

스팸 격리 개요

스팸 격리(일명 ISQ, 최종 사용자 격리 및 EUQ)는 "잘못된 긍정" 즉, 어플라이언스가 스팸으로 간주한 정상적인 이메일 메시지가 우려되는 조직을 위한 보호 메커니즘을 제공합니다. 어플라이언스에서 메시지를 스팸 또는 의심스러운 스팸으로 결정한 경우 수신자 또는 관리자가 메시지를 검토한 후 전송하거나 삭제하게 할 수 있습니다. 스팸 격리는 이러한 목적으로 메시지를 저장합니다.

Email Security 어플라이언스의 관리자는 스팸 격리의 모든 메시지를 볼 수 있습니다. 일반적으로 메시지 수신자인 최종 사용자는 직접 격리한 메시지를 약간 다른 웹 인터페이스에서 볼 수 있습니다.

스팸 격리는 정책, 바이러스 및 신종 바이러스 격리와 구분됩니다.

관련 주제

- 13장, "안티스팸"
- 30장, "정책, 바이러스 및 신종 바이러스 격리"

로컬 바이러스 외부 스팸 격리

로컬 스팸 격리는 스팸과 의심스러운 스팸을 Email Security 어플라이언스에 저장합니다. 외부 스팸 격리는 이러한 메시지를 별도의 Cisco Content 보안 관리 어플라이언스에 저장할 수 있습니다.

다음과 같은 경우 외부 스팸 격리 사용을 고려하십시오.

- 여러 Email Security 어플라이언스에서 스팸을 저장하고 관리할 수 있는 중앙 집중식 위치를 원하는 경우

- Email Security 어플라이언스보다 더 많은 스팸을 저장하려는 경우
- 동일한 격리와 해당 메시지를 정기적으로 백업하려는 경우

관련 주제

- 스팸 격리를 위한 디스크 공간, 31-23페이지
- 외부 스팸 격리 사용, 42-2페이지

로컬 스팸 격리 설정

표 31-1 스팸 격리에 메시지를 보내는 방법

	수행할 작업	추가 정보
1단계	안티스팸 기능을 활성화합니다(아직 활성화하지 않은 경우).	13장, "안티스팸"
2단계	격리 설정을 활성화하고 구성합니다.	스팸 격리 활성화 및 구성, 31-2페이지
3단계	스팸 격리에 할당된 디스크 공간을 조정합니다.	디스크 공간 관리, 33-15페이지
4단계	브라우저가 격리에 액세스할 수 있도록 설정합니다.	스팸 격리에 대한 브라우저 액세스를 위한 IP 인터페이스 구성, 31-4페이지
5단계	Email Security 어플라이언스에서 격리에 스팸을 보내도록 구성합니다.	• 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 13-2페이지 • 스팸을 격리할 메일 정책 구성, 31-5페이지 • 메일 격리 수신자 제한, 31-5페이지
6단계	머리글에서 이 정보가 없는 메시지에 기본 문자 인코딩을 지정합니다.	메시지 텍스트를 올바르게 표시, 31-6페이지

관련 주제

- 스팸 격리 활성화 및 구성, 31-2페이지
- 스팸 격리에 대한 브라우저 액세스를 위한 IP 인터페이스 구성, 31-4페이지
- 스팸 격리에 대한 관리자 액세스 구성, 31-4페이지
- 스팸을 격리할 메일 정책 구성, 31-5페이지
- 메일 격리 수신자 제한, 31-5페이지
- 메시지 텍스트를 올바르게 표시, 31-6페이지
- 스팸 격리 언어, 31-6페이지

스팸 격리 활성화 및 구성

참고 외부 스팸 격리를 사용할 경우 보안 관리 어플라이언스에서 이 섹션에 설명된 설정을 구성합니다.

절차

1단계 **Monitor(모니터링) > Spam Quarantine(스팸 격리)**을 선택합니다.

2단계 이전에 스팸 격리를 활성화하지 않은 경우 **Enable Spam Quarantine(스팸 격리 활성화)**을 선택합니다.

스팸 격리 설정을 편집하려면 스팸 격리 섹션의 격리 이름 열에 있는 **Spam Quarantine(스팸 격리)** 링크를 클릭합니다.

3단계 옵션을 지정합니다.

Option	설명
쿼런틴 크기	**When storage space is full, automatically delete oldest messages first(저장 공간이 가득 차면 가장 오래된 메시지부터 자동으로 삭제)**를 선택 취소하면 최신 메시지가 전체 격리에 추가되지 않습니다. Cisco에서는 전체 격리가 어플라이언스의 큐로 메시지를 보내지(백업) 않도록 이 옵션을 활성화할 것을 권장합니다. 격리에 사용되는 디스크 공간을 관리하려면 디스크 공간 관리, 33-15페이지를 참조하십시오.
삭제 기준 일정	메시지를 삭제하기 전에 보류할 기간(일)을 지정합니다. Cisco에서는 격리 용량이 가득 차는 것을 방지하기 위해 오래된 메시지를 삭제하도록 격리를 구성할 것을 권장하지만 자동 삭제를 예약하지 않을 수도 있습니다.
메시지 릴리스 시 Cisco에 알림	—
스팸 격리 모양	**로고** 기본적으로 Cisco 로고는 사용자가 격리된 메시지를 보기 위해 로그인할 때 스팸 격리 페이지의 상단에 표시됩니다. 사용자 지정 로그를 대신 사용하려면 해당 로고를 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 최종 사용자 및 관리자가 격리를 보기 위해 로그인할 때 표시됩니다. 메시지를 지정하지 않으면 다음 메시지가 나타납니다. 아래에 로그인 정보를 입력합니다. 잘 모를 경우 관리자에게 문의하십시오.
관리자	스팸 격리에 대한 관리자 액세스 구성, 31-4페이지를 참조하십시오.

4단계 변경 사항을 제출하고 커밋합니다.

향후 작업

- 로컬 스팸 격리 설정, 31-2페이지로 돌아갑니다.

스팸 격리에 대한 브라우저 액세스를 위한 IP 인터페이스 구성

관리자와 최종 사용자가 스팸 격리에 액세스할 때 별도의 브라우저 창이 열립니다.

절차

1단계 **Network(네트워크) > IP Interfaces(IP 인터페이스)**를 선택합니다.

2단계 인터페이스 이름을 클릭합니다(이 예의 경우 관리 인터페이스를 사용합니다).

3단계 스팸 격리 섹션에서 스팸 격리에 대한 액세스 설정을 구성합니다.

- 기본적으로 HTTP는 포트 82를 사용하고 HTTPS는 포트 83을 사용합니다.
- 알림 및 스팸 격리 브라우저 창에 표시되는 URL을 지정합니다.

  보안 관리 어플라이언스의 호스트 이름을 최종 사용자에게 노출시키지 않으려면 대체 호스트 이름을 지정할 수 있습니다.

4단계 변경 사항을 제출하고 커밋합니다.

향후 작업

DNS 서버가 사용자가 스팸 격리 액세스에 대해 지정한 호스트 이름을 확인할 수 있는지 확인합니다.

스팸 격리에 대한 관리자 액세스 구성

관리자 권한이 있는 모든 사용자는 스팸 격리 설정을 변경하고 스팸 격리에서 메시지를 보거나 관리할 수 있습니다. 따라서 관리자에 대한 스팸 격리 액세스를 구성할 필요가 없습니다.

다음과 같은 역할이 있는 사용자에 대해 스팸 격리 액세스를 구성하면 해당 사용자가 스팸 격리에서 메시지를 보거나, 릴리스하거나, 삭제할 수 있습니다.

- 운영자
- 읽기 전용 작업자
- Help Desk 사용자
- 게스트
- 스팸 격리 권한이 있는 사용자 지정 사용자 역할

이러한 사용자는 스팸 격리 설정에 액세스할 수 없습니다.

시작하기 전에

스팸 격리에 액세스할 수 있는 사용자를 생성하거나 사용자 지정합니다. 자세한 내용은 32 장, "관리 작업 분배" 를 참조하십시오.

절차

1단계 아직 스팸 격리 설정 페이지를 편집하지 않은 경우:

a. **Monitor(모니터링) > Spam Quarantine(스팸 격리)**을 선택합니다.

b. 스팸 격리 섹션의 격리 이름 열에 있는 **Spam Quarantine(스팸 격리)** 링크를 클릭합니다.

2단계 추가할 사용자(로컬 사용자, 외부에서 인증된 사용자 또는 사용자 지정 역할)의 사용자 유형에 대한 링크를 클릭합니다.

이미 사용자 또는 역할을 추가한 경우 사용자 이름 또는 역할을 클릭하여 자격이 있는 모든 사용자 또는 역할을 봅니다.

3단계 추가할 사용자 또는 역할을 선택합니다.

관리자 권한이 있는 사용자는 자동으로 스팸 격리에 완전히 액세스할 수 있으므로 표시되지 않습니다.

4단계 **OK**를 클릭합니다.

5단계 변경 사항을 제출하고 커밋합니다.

관련 주제

- 스팸 격리에 대한 최종 사용자 액세스 구성, 31-16페이지

스팸을 격리할 메일 정책 구성

스팸 격리를 활성화하면 해당 격리에 스팸 또는 의심스러운 스팸을 보내기 위한 메일 정책을 구성할 수 있습니다. 스팸 격리에 메일을 보내려면 메일 정책에서 안티스팸 검사를 활성화해야 합니다.

스팸을 격리할 메일 정책을 구성하는 방법에 대한 자세한 내용은 안티스팸 정책 정의, 13-7페이지를 참조하십시오.

절차

1단계 Mail Policies(메일 정책) > Incoming Mail Policies(수신 메일 정책) 페이지에서 해당 메일 정책의 Anti-Spam(안티스팸) 열에 있는 링크를 클릭합니다.

2단계 안티스팸 설정 섹션에서 **Use IronPort Anti-Spam service(IronPort Anti-Spam 서비스 사용)**를 선택합니다.

3단계 스팸으로 확인된 스팸 설정 섹션에서 **Apply This Action to Message(메시지에 이 작업 적용)** 옵션으로 **Spam Quarantine(스팸 격리)**을 선택합니다.

4단계 의심스러운 스팸 및 마케팅 이메일에 대한 설정을 구성합니다.

5단계 변경 사항을 제출하고 커밋합니다.

메일 격리 수신자 제한

여러 메일 정책을 사용하여(Mail Policies(메일 정책) > Incoming Mail Policy(수신 메일 정책)) 메일을 격리하지 않을 수신자 주소의 목록을 지정합니다. 메일 정책에 대해 안티스팸 설정을 구성할 때 격리 대신 '전송' 또는 '삭제'를 선택합니다.

메시지 텍스트를 올바르게 표시

AsyncOS는 메시지 헤더에 지정된 인코딩을 기반으로 메시지의 문자 집합을 결정하려고 시도합니다. 그러나 헤더에 지정된 인코딩이 실제 텍스트의 인코딩과 일치하지 않을 경우 스팸 격리에서 메시지를 볼 때 메시지가 제대로 표시되지 않습니다. 이 상황은 스팸 메시지에서 발생할 가능성이 더 높습니다.

이러한 메시지의 메시지 텍스트를 올바르게 표시하려면 기본 인코딩 지정, 31-6페이지를 참조하십시오.

관련 주제

- 기본 인코딩 지정, 31-6페이지

기본 인코딩 지정

수신 메시지의 헤더에 문자 집합 인코딩이 지정되지 않은 경우 기본 인코딩을 지정하도록 어플라이언스를 구성할 수 있습니다.

이렇게 하면 스팸 격리에서 이러한 유형의 메시지를 올바르게 표시할 수 있습니다. 그러나 기본 인코딩을 지정하면 다른 문자 집합의 메시지가 잘못 표시될 수 있습니다. 이 설정은 메시지 헤더에 인코딩을 지정하지 않은 메시지에만 적용됩니다. 일반적으로 대다수의 메일이 특정 인코딩으로 분류된 이 범주에 해당한다고 예상할 경우에만 기본 인코딩을 지정합니다.

예를 들어, 대부분의 격리된 메시지가 메시지 헤더에 문자 집합 인코딩이 지정되지 않았고 일본어(ISO-2022-JP)로 된 경우 검사 동작 페이지에서 인코딩을 **일본어(ISO-2022-JP)**로 설정할 수 있습니다.

절차

1단계 **Security Services(보안 서비스) > Scan Behavior(검사 동작)**를 클릭합니다.

2단계 Global Settings(전역 설정)에서, **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

3단계 **지정된 인코딩이 없는 경우 사용할 인코딩** 드롭다운 목록에서 원하는 인코딩 유형을 선택합니다.

4단계 **Submit(제출)**을 클릭합니다.

5단계 **Commit Changes(변경 사항 커밋)**를 클릭합니다.

스팸 격리 언어

각 사용자는 창 오른쪽 상단의 옵션 메뉴에서 스팸 격리 언어를 선택합니다.

발신자를 기준으로 이메일 전송을 제어하는 허용 목록 및 차단 목록 사용

관리자와 최종 사용자가 허용 목록과 차단 목록을 사용하여 어떤 메시지가 스팸인지 판단할 수 있습니다. 허용 목록은 어떤 경우에도 스팸으로 처리되지 않는 발신자와 도메인을 지정합니다. 차단 목록은 항상 스팸으로 처리되는 발신자와 도메인을 지정합니다.

최종 사용자(이메일 사용자)가 본인의 이메일 계정의 허용 목록과 차단 목록을 관리하도록 허용할 수 있습니다. 예를 들어, 최종 사용자가 더 이상 관심이 없는 메일 목록의 이메일을 수신할 수 있습니다. 따라서 해당 메일 목록의 이메일이 받은 편지함으로 전송되지 않도록 이 발신자를 차단 목록에 추가하기로 결정할 수 있습니다. 반면, 최종 사용자가 스팸으로 처리하고 싶지 않은 특정 발신자의 이메일이 스팸 격리로 전송된다는 사실을 알게 될 수 있습니다. 따라서 최종 사용자가 이러한 발신자의 메시지가 격리되지 않도록 해당 발신자를 허용 목록에 추가할 수 있습니다.

최종 사용자와 관리자가 변경한 내용이 표시되고 최종 사용자나 관리자가 이를 변경할 수 있습니다.

관련 주제

- 허용 목록 및 차단 목록의 메시지 처리, 31-7페이지
- 허용 목록 및 차단 목록 활성화, 31-8페이지
- 외부 스팸 격리 및 허용 목록/차단 목록, 31-8페이지
- 허용 목록 및 차단 목록에 발신자 및 도메인 추가(관리자), 31-8페이지
- 허용 목록 및 차단 목록에 대한 최종 사용자 액세스 정보, 31-10페이지
- 여러 이메일 보안 어플라이언스에서 허용 목록/차단 목록 동기화(보안 관리 어플라이언스 없이 배포), 31-12페이지
- 허용 목록/차단 목록 백업 및 복원, 31-12페이지
- 허용 목록 및 차단 목록 문제 해결, 31-13페이지

허용 목록 및 차단 목록의 메시지 처리

발신자를 허용 목록 또는 차단 목록에 추가한다고 해서 어플라이언스가 메시지를 검사해 바이러스가 있는지 확인하거나 메시지가 콘텐츠 관련 메일 정책의 기준을 충족하는지 판단하는 작업이 차단되지 않습니다. 메시지의 발신자가 수신자의 허용 목록에 있더라도 다른 검사 설정 및 결과에 따라 메시지가 최종 사용자에게 전송되지 않을 수 있습니다.

허용 목록 및 차단 목록을 활성화하면 어플라이언스가 안티스팸 검사 직전에 허용 목록/차단 목록 데이터베이스를 기준으로 메시지를 검사합니다. 어플라이언스가 허용 목록 또는 차단 목록 항목과 일치하는 발신자 또는 도메인을 탐지한 경우 수신자가 여러 명이면 메시지가 분할됩니다(수신자마다 허용 목록/차단 목록 설정이 다름). 예를 들어, 메시지가 수신자 A와 수신자 B에게 모두 전송됩니다. 수신자 A는 해당 발신자가 허용 목록에 있지만 수신자 B는 허용 목록 또는 차단 목록에 해당 발신자에 대한 항목이 없습니다. 이 경우 메시지가 메시지 ID가 서로 다른 2개의 메시지로 분할될 수 있습니다. 수신자 A에게 전송된 메시지는 *X-SLBL-Result-Safelist* 헤더를 통해 허용 메시지로 표시되므로 안티스팸 검사를 건너뛰지만 수신자 B의 메시지 바운스는 안티스팸 검사 엔진에서 검사합니다. 그런 다음 두 메시지가 모두 계속해서 파이프라인(안티바이러스 검사, 콘텐츠 정책 등)을 따라가며 구성된 설정에 따라 처리됩니다.

메시지 발신자 또는 도메인이 차단 목록에 있는 경우 사용자가 허용 목록/차단 목록 기능을 활성화할 때 지정한 차단 목록 작업에 따라 전송 동작이 달라집니다. 허용 목록 전송과 마찬가지로 허용 목록/차단 목록 설정이 다른 여러 수신자가 있는 경우 메시지가 분할됩니다. 그런 다음 차단 목록 작업 설정에 따라 차단된 메시지 조각이 격리 또는 삭제됩니다. 차단 목록 작업이 메시지를 격리하도록 구성된 경우 메시지가 검사되어 결국 격리됩니다. 차단 목록 작업이 메시지를 삭제하도록 구성된 경우 허용 목록/차단 목록 검사 후에 메시지가 즉시 삭제됩니다.

허용 목록과 차단 목록은 스팸 격리에 유지되므로 전송 동작도 다른 안티스팸 설정에 따라 결정됩니다. 예를 들어, 안티스팸 검사를 건너뛰도록 HAT(Host Access Table)의 "수락" 메일 흐름 정책을 구성한 경우 해당 리스너에서 메일을 수신하는 사용자의 허용 목록 및 차단 목록 설정이 해당 리스너에서 수신된 메일에 적용되지 않습니다. 마찬가지로 특정 메시지 수신자에 대한 안티스팸 검사를 건너뛰는 메일 흐름 정책을 생성할 경우 이러한 수신자의 허용 목록 및 차단 목록 설정이 적용되지 않습니다.

관련 주제

- 허용 목록 및 차단 목록 활성화, 31-8페이지
- 외부 스팸 격리 및 허용 목록/차단 목록, 31-8페이지

허용 목록 및 차단 목록 활성화

시작하기 전에

- 스팸 격리를 활성화해야 합니다. 로컬 스팸 격리 설정, 31-2페이지를 참조하십시오.

절차

1단계 **Monitor(모니터링) > Spam Quarantine(스팸 격리)**을 선택합니다.

2단계 **최종 사용자 허용 목록/차단 목록(스팸 격리)** 섹션에서 **Enable(활성화)**을 선택합니다.

3단계 **Enable End User Safelist/Blocklist Feature(최종 사용자 허용 목록/차단 목록 기능 사용)**를 선택합니다.

4단계 차단 목록 작업으로 **Quarantine(격리)** 또는 **Delete(삭제)**를 선택합니다.

5단계 **Maximum List Items Per User(사용자당 최대 목록 항목)**를 지정합니다.

이는 각 수신자의 각 목록의 최대 주소 또는 도메인 수입니다. 사용자당 많은 수의 목록 항목을 허용할 경우 시스템 성능이 부정적인 영향을 줄 수 있습니다.

6단계 변경 사항을 제출하고 커밋합니다.

외부 스팸 격리 및 허용 목록/차단 목록

보안 관리 어플라이언스에서 외부 스팸 격리를 사용할 경우 허용 목록/차단 목록이 관리 어플라이언스에 저장됩니다. 따라서 모든 어플라이언스의 안전한 발신자와 차단된 발신자를 단일 위치에서 관리할 수 있습니다.

Email Security 어플라이언스가 수신 메일 처리 시 허용 목록 및 차단 목록의 발신자를 평가하므로 수신 메일에 적용되도록 하려면 보안 관리 어플라이언스에 저장된 허용 목록 및 차단 목록을 Email Security 어플라이언스로 보내야 합니다. 보안 관리 어플라이언스에서 허용 목록/차단 목록 기능을 구성할 경우 이러한 업데이트의 간격을 구성합니다.

보안 관리 어플라이언스에서 외부 허용 목록 및 차단 목록을 사용하는 방법에 대한 자세한 내용은 외부 스팸 격리 사용, 42-2페이지의 해당 항목과 *Cisco Content Security Management Appliance 사용 설명서*를 참조하십시오.

허용 목록 및 차단 목록에 발신자 및 도메인 추가(관리자)

스팸 격리 인터페이스를 통해 허용 목록 및 차단 목록을 관리합니다.

또한 여러 수신자(조직의 최종 사용자)가 특정 발신자 또는 도메인을 허용하는지 아니면 차단하는지 파악할 수 있습니다.

관리자는 각 최종 사용자가 보고 사용하는 것과 동일한 항목의 상위 집합을 보고 사용할 수 있습니다.

시작하기 전에

- 스팸 격리에 액세스할 수 있는지 확인합니다. 스팸 격리 액세스(관리자), 31-21페이지를 참조하십시오.
- 허용 목록/차단 목록에 대한 액세스를 사용합니다. 허용 목록 및 차단 목록 활성화, 31-8페이지를 참조하십시오.
- (선택 사항) 이 섹션의 절차를 사용하여 이러한 목록을 구성하는 대신 허용 목록/차단 목록을 가져오려면 허용 목록/차단 목록 백업 및 복원, 31-12페이지에 설명된 프로세스를 사용합니다.
- 허용 목록 및 차단 목록 항목의 필수 형식을 이해합니다. 허용 목록 및 차단 목록 항목의 구문, 31-10페이지를 참조하십시오.

절차

1단계 브라우저를 사용하여 스팸 격리에 액세스합니다.

2단계 로그인합니다.

3단계 페이지의 오른쪽 상단에서 **옵션** 드롭다운 메뉴를 선택합니다.

4단계 **Safelist(허용 목록)** 또는 **Blocklist(차단 목록)**를 선택합니다.

5단계 (선택 사항) 발신자 또는 수신자를 검색합니다.

6단계 다음 중 하나 이상을 수행합니다.

To	수행할 작업
한 명의 수신자에 대해 여러 발신자를 추가합니다.	1. **View by: Recipient(보기 기준: 수신자)**를 선택합니다. 2. 수신자에 대해 **Add(추가)** 또는 **Edit(편집)**를 클릭합니다. 3. 수신자 이메일 주소를 입력하거나 편집합니다. 4. 발신자 이메일 주소 및 도메인을 입력합니다. 각 항목을 별도의 행에 표시하거나 각 항목을 쉼표로 구분합니다. 5. **Submit(제출)**을 클릭합니다.
한 명의 발신자에 대해 여러 수신자를 추가합니다.	1. **View by: Sender(보기 기준: 발신자)**를 선택합니다. 2. 발신자에 대해 **Add(추가)** 또는 **Edit(편집)**를 클릭합니다. 3. 발신자 주소 또는 도메인을 입력하거나 편집합니다. 4. 수신자 이메일 주소를 입력합니다. 각 항목을 별도의 행에 표시하거나 각 항목을 쉼표로 구분합니다. 5. **Submit(제출)**을 클릭합니다.
수신자와 연결된 모든 발신자를 삭제합니다. 발신자와 연결된 모든 수신자를 삭제합니다.	1. **View by(보기 기준)** 옵션을 선택합니다. 2. 전체 표 행을 삭제하려면 휴지통 아이콘을 클릭합니다.

To	수행할 작업
한 명의 수신자에 대해 개별 발신자를 삭제합니다. 한 명의 발신자에 대해 개별 수신자를 삭제합니다.	1. View by(보기 기준) 옵션을 선택합니다. 2. 개별 수신자 또는 발신자에 대해 **Edit(편집)**를 클릭합니다. 3. 텍스트 상자에서 항목을 추가하거나 제거합니다. 최소 한 하나 이상의 항목을 남겨 둬야 합니다. 4. **Submit(제출)**을 클릭합니다.

관련 주제

- 허용 목록 및 차단 목록 항목의 구문, 31-10페이지
- 모든 허용 목록 및 차단 목록 지우기, 31-10페이지

허용 목록 및 차단 목록 항목의 구문

다음과 같은 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]

허용 목록과 차단 목록이 동시에 동일한 항목(예: 발신자 주소 또는 도메인)을 포함할 수 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 넣을 수 있습니다. 그러면 어플라이언스는 *example.com*에서 보낸 모든 메일을 스팸 검사 없이 전송합니다. 단, *george@example.com*에서 보낸 메일은 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 할 경우 허용 목록/차단 목록 백업 및 복원, 31-12페이지의 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 웹 브라우저를 통해 스팸 격리에 대한 최종 사용자 액세스 설정, 31-16페이지를 참조하십시오.

해당하는 경우 최종 사용자에게 스팸 격리 및 아래 명령의 URL을 제공할 수 있습니다.

관련 주제

- 허용 목록에 항목 추가(최종 사용자), 31-11페이지
- 차단 목록에 발신자 추가(최종 사용자), 31-11페이지

허용 목록에 항목 추가(최종 사용자)

참고 허용 목록에 있는 발신자의 메시지 전송은 시스템에 구성된 기타 설정에 따라 다릅니다. 허용 목록 및 차단 목록의 메시지 처리, 31-7페이지를 참조하십시오.

다음 두 가지 방법으로 허용 목록에 최종 사용자를 추가할 수 있습니다.

- 허용 목록에 격리된 메시지의 발신자 추가, 31-11페이지
- 격리된 메시지 없이 허용 목록에 발신자 추가, 31-11페이지

허용 목록에 격리된 메시지의 발신자 추가

메시지가 스팸 격리로 전송된 경우 최종 사용자는 허용 목록에 발신자를 추가할 수 있습니다.

절차

1단계 스팸 격리에서 메시지 옆의 확인란을 선택합니다.

2단계 드롭다운 메뉴에서 **Release and Add to Safelist(해제한 후 허용 목록에 추가)**를 선택합니다.

봉투 발신자와 지정된 메일의 보낸 사람 헤더가 모두 허용 목록에 추가되고 릴리스된 메시지가 이메일 파이프라인의 추가 작업 큐 처리를 건너뛰고 대상 큐로 바로 진행합니다.

격리된 메시지 없이 허용 목록에 발신자 추가

절차

1단계 브라우저를 통해 스팸 격리에 액세스합니다.

2단계 페이지의 오른쪽 상단에서 **옵션** 드롭다운 메뉴를 선택합니다.

3단계 **Safelist(허용 목록)**를 선택합니다.

4단계 허용 목록 대화 상자에서 이메일 주소 또는 도메인을 입력합니다. 여러 도메인과 이메일 주소를 쉼표로 구분해서 입력할 수 있습니다.

5단계 **Add to List(목록에 추가)**를 클릭합니다.

차단 목록에 발신자 추가(최종 사용자)

차단된 발신자의 메시지는 관리자가 정의한 허용 목록/차단 목록 작업 설정에 따라 거부되거나 격리될 수 있습니다.

참고 이 절차를 사용해서만 차단 목록 항목을 추가할 수 있습니다.

절차

1단계 스팸 격리에 로그인합니다.

2단계 페이지의 오른쪽 상단에서 **옵션** 드롭다운 메뉴를 선택합니다.

3단계 차단할 도메인 또는 이메일 주소를 입력합니다. 여러 도메인과 이메일 주소를 쉼표로 구분해서 입력할 수 있습니다.

4단계 **Add to List(목록에 추가)**를 클릭합니다.

여러 이메일 보안 어플라이언스에서 허용 목록/차단 목록 동기화(보안 관리 어플라이언스 없이 배포)

여러 개의 Email Security 어플라이언스를 보안 관리 어플라이언스 없이 사용할 경우 여러 Email Security 어플라이언스 전체에서 허용 목록/차단 목록과 해당 구성 설정을 수동으로 동기화해야 할 수 있습니다.

허용 목록/차단 목록 백업 및 복원, 31-12페이지에 설명된 절차를 사용하여 .csv 파일을 내보내거나 가져온 다음 FTP를 사용하여 파일을 업로드하거나 다운로드할 수 있습니다. 자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스"를 참조하십시오.

허용 목록/차단 목록 백업 및 복원

어플라이언스를 업그레이드하거나 설치 마법사를 실행하기 전에 허용 목록/차단 목록 데이터베이스를 백업해야 합니다. 허용 목록/차단 목록 정보가 어플라이언스 구성 설정을 포함하는 기본 구성 XML 파일에 들어 있지 않습니다.

이 절차를 사용하여 허용 목록/차단 목록의 사본을 저장해 여러 Email Security 어플라이언스를 동기화할 수도 있습니다.

절차

1단계 **System Administration(시스템 관리) > Configuration File(구성 파일)**을 선택합니다.

2단계 **최종 사용자 허용 목록/차단 목록 데이터베이스(스팸 격리)** 섹션으로 스크롤합니다.

To	수행할 작업
허용 목록/차단 목록을 내보냅니다.	.csv 파일의 경로와 파일 이름을 기록해 두고 필요에 따라 수정합니다. **Backup Now(지금 백업)**를 클릭합니다. 어플라이언스가 다음 명명 규칙을 사용하여 어플라이언스의 `/configuration` 디렉토리에 .csv 파일을 저장합니다. *slbl<serial number><timestamp>.csv*
허용 목록/차단 목록을 가져옵니다.	⚠ **주의** 이 프로세스는 모든 사용자의 허용 목록 및 차단 목록에 있는 모든 기존 항목을 덮어씁니다. **Select File to Restore(복원할 파일 선택)**를 클릭합니다. 구성 디렉토리의 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 경고를 확인하면 됩니다.

허용 목록/차단 목록 설정으로 인해 이메일이 차단된 경우 해당 작업이 ISQ_log 파일 또는 안티스팸 로그 파일에 기록됩니다. 허용 목록에 있는 이메일은 *X-SLBL-Result-Safelist* 헤더를 통해 허용 이메일로 표시됩니다. 차단 목록에 있는 이메일은 *X-SLBL-Result-Blocklist* 헤더를 통해 차단 이메일로 표시됩니다.

데이터베이스가 생성 또는 업데이트되거나 데이터베이스 수정 또는 허용 목록/차단 목록 실행 프로세스에 오류가 있는 경우 경고가 발송됩니다.

경고에 대한 자세한 내용은 33 장, "경고"

로그 파일에 대한 자세한 내용은 38 장, "로깅"을 참조하십시오.

관련 주제

- 허용된 발신자의 메시지가 전송되지 않았음, 31-13페이지

허용된 발신자의 메시지가 전송되지 않았음

문제 허용된 발신자의 메시지가 전송되지 않았습니다.

솔루션 가능한 원인:

- 메시지가 맬웨어 또는 콘텐츠 위반으로 인해 삭제되었습니다. 허용 목록 및 차단 목록의 메시지 처리, 31-7페이지를 참조하십시오.
- 여러 어플라이언스를 사용하고 해당 발신자가 최근에 허용 목록에 추가된 경우 허용 목록/차단 목록이 메시지가 처리되었을 때 동기화되지 않았을 수 있습니다. 외부 스팸 격리 및 허용 목록/차단 목록, 31-8페이지 및 여러 이메일 보안 어플라이언스에서 허용 목록/차단 목록 동기화(보안 관리 어플라이언스 없이 배포), 31-12페이지를 참조하십시오.

최종 사용자를 위한 스팸 관리 기능 구성

To	참조:
스팸 관리 기능에 대한 최종 사용자 액세스를 위한 다양한 인증 방법의 이점과 한계를 이해합니다.	스팸 격리에 대한 최종 사용자 액세스 구성, 31-16페이지 및 하위 섹션
최종 사용자가 브라우저를 통해 스팸 격리에 직접 액세스할 수 있도록 허용합니다.	스팸 관리 기능에 액세스하는 최종 사용자의 인증 옵션, 31-14페이지
전송된 메시지가 스팸 격리로 라우팅되면 사용자에게 알림을 전송합니다. 알림에는 스팸 격리에 대한 액세스 링크가 포함될 수 있습니다.	최종 사용자에게 격리된 메시지에 대해 알림, 31-18페이지
사용자가 안전하다고 알려진 발신자와 스팸 또는 기타 원하지 않는 메일을 보내는 것으로 알려진 발신자의 이메일 주소와 도메인을 지정할 수 있도록 허용합니다.	발신자를 기준으로 이메일 전송을 제어하는 허용 목록 및 차단 목록 사용, 31-6페이지

관련 주제

- 스팸 관리 기능에 액세스하는 최종 사용자의 인증 옵션, 31-14페이지
- 웹 브라우저를 통해 스팸 격리에 대한 최종 사용자 액세스 설정, 31-16페이지
- 최종 사용자에게 격리된 메시지에 대해 알림, 31-18페이지

스팸 관리 기능에 액세스하는 최종 사용자의 인증 옵션

참고 사서함 인증을 사용하면 사용자가 이메일 별칭으로 전송된 메시지를 볼 수 없습니다.

최종 사용자 스팸 격리 액세스의 경우	수행할 작업
웹 브라우저를 통해 직접(인증 필요) 및 알림의 링크를 통해(인증 필요)	1. 최종 사용자 격리 액세스 설정에서 **LDAP** 또는 **Mailbox (IMAP/POP)(사서함 (IMAP/POP))**를 선택합니다. 2. 스팸 알림 설정에서 **Enable login without credentials for quarantine access(격리 액세스 자격 증명 없이 로그인 사용)**를 선택 취소합니다.
웹 브라우저를 통해 직접(인증 필요) 및 알림의 링크를 통해(인증 불필요)	1. 최종 사용자 격리 액세스 설정에서 **LDAP** 또는 **Mailbox (IMAP/POP)(사서함 (IMAP/POP))**를 선택합니다. 2. 스팸 알림 설정에서 **Enable login without credentials for quarantine access(격리 액세스 자격 증명 없이 로그인 사용)**를 선택합니다.

최종 사용자 스팸 격리 액세스의 경우	수행할 작업
알림의 링크를 통해서만(인증 불필요)	최종 사용자 격리 액세스 설정에서 인증 방법으로 **None(없음)**을 선택합니다.
액세스 없음	최종 사용자 격리 액세스 설정에서 **Enable End-User Quarantine Access(최종 사용자 격리 액세스 사용)**를 선택 취소합니다.

관련 주제

- LDAP 인증 프로세스, 31-15페이지
- IMAP/POP 인증 프로세스, 31-15페이지
- 스팸 격리에 대한 최종 사용자 액세스 구성, 31-16페이지
- 최종 사용자에게 격리된 메시지에 대해 알림, 31-18페이지
- 스팸 격리의 최종 사용자 인증, 25-42페이지
- 허용 목록 및 차단 목록에 대한 최종 사용자 액세스 정보, 31-10페이지

LDAP 인증 프로세스

1. 사용자가 웹 UI 로그인 페이지에 사용자 이름과 비밀번호를 입력합니다.
2. 스팸 격리가 지정된 LDAP 서버에 연결하여 익명으로 또는 "서버 로그인" DN 및 비밀번호가 지정된 인증된 사용자로 검색을 수행할 수 있습니다. Active Directory의 경우 일반적으로 "전역 카탈로그 포트"(6000s에 있음)에 서버를 연결해야 하며 검색을 실행하기 위해 스팸 격리를 바인딩할 수 있는 권한이 낮은 LDAP 사용자를 생성해야 합니다.
3. 그러면 스팸 격리가 지정된 BaseDN 및 쿼리 문자열을 사용하여 사용자를 검색할 수 있습니다. 사용자의 LDAP 기록이 발견되면 스팸 격리가 해당 기록의 DN을 추출하고 처음에 입력한 사용자 기록의 DN 및 비밀번호를 사용하여 디렉토리에 직접 바인딩을 시도합니다. 이 비밀번호 확인이 성공하면 사용자가 올바르게 인증되지만 스팸 격리는 여전히 해당 사용자에 대해 표시할 사서함의 내용을 결정해야 합니다.
4. 메시지는 수신자의 봉투 주소를 사용하여 스팸 격리에 저장됩니다. 사용자 비밀번호가 LDAP에 대해 검증되면 스팸 격리가 LDAP 기록에서 "기본 이메일 특성"을 검색하여 격리된 메시지에 표시할 봉투 주소를 결정합니다. "기본 이메일 특성"에는 여러 이메일 주소가 포함될 수 있으므로 이를 사용하여 격리에서 인증된 사용자에 대해 표시해야 하는 봉투 주소를 결정합니다.

관련 주제

- 스팸 격리의 최종 사용자 인증, 25-42페이지

IMAP/POP 인증 프로세스

1. 메일 서버 구성에 따라 사용자가 웹 UI 로그인 페이지에 사용자 이름(`joe`) 또는 이메일 주소(`joe@example.com`)와 비밀번호를 입력합니다. 로그인 페이지 메시지를 수정하여 사용자에게 전체 이메일 주소를 입력해야 하는지 아니면 사용자 이름만 입력하면 되는지 알려줄 수 있습니다(스팸 격리에 대한 최종 사용자 액세스 구성, 31-16페이지 참조).
2. 스팸 격리가 IMAP 또는 POP 서버에 연결하여 입력된 로그인(사용자 이름 또는 이메일 주소)과 비밀번호를 사용하여 MAP/POP 서버에 대한 로그인을 시도합니다. 비밀번호가 수락되면 해당 사용자는 인증된 사용자로 간주되어 스팸 격리가 즉시 IMAP/POP 서버에서 로그아웃합니다.

3. 사용자가 인증되면 스팸 격리가 이메일 주소를 기반으로 해당 사용자의 이메일을 나열합니다.
   - 기본 사용자 이름(joe 등)에 추가할 도메인을 지정하도록 스팸 격리를 구성한 경우 이 도메인이 추가되고 정규화된 이메일 주소를 사용해 격리에서 일치하는 봉투를 검색합니다.
   - 그렇지 않은 경우 스팸 격리가 입력한 이메일 주소를 사용하여 일치하는 봉투를 검색합니다.

IMAP에 대한 자세한 내용은 워싱턴대학교 웹사이트를 참조하십시오.

http://www.washington.edu/imap/

웹 브라우저를 통해 스팸 격리에 대한 최종 사용자 액세스 설정

	수행할 작업	추가 정보
1단계	스팸 관리 기능에 대한 최종 사용자 액세스를 위한 다양한 인증 방법의 이점과 한계를 이해합니다.	스팸 관리 기능에 액세스하는 최종 사용자의 인증 옵션, 31-14페이지
2단계	LDAP를 사용하여 최종 사용자를 인증하려면 **System Administration(시스템 관리) > LDAP > LDAP Server Profile(LDAP 서버 프로필)** 페이지의 **Spam Quarantine End-User Authentication Query(스팸 격리 최종 사용자 인증 쿼리)** 설정을 포함하여 LDAP 서버 프로필을 구성합니다.	스팸 격리의 최종 사용자 인증, 25-42페이지 및 하위 섹션
3단계	스팸 격리에 대한 최종 사용자 액세스를 구성합니다.	스팸 격리에 대한 최종 사용자 액세스 구성, 31-16페이지
4단계	스팸 격리에 대한 최종 사용자 액세스의 URL을 결정합니다.	스팸 격리에 대한 최종 사용자 액세스의 URL 결정, 31-17페이지

관련 주제

- 스팸 격리에 대한 최종 사용자 액세스 구성, 31-16페이지
- 스팸 격리에 대한 최종 사용자 액세스의 URL 결정, 31-17페이지
- 최종 사용자가 볼 수 있는 메시지, 31-17페이지

스팸 격리에 대한 최종 사용자 액세스 구성

관리자는 최종 사용자 액세스가 사용되든 아니든 스팸 격리에 액세스할 수 있습니다.

시작하기 전에

스팸 관리 기능에 액세스하는 최종 사용자의 인증 옵션, 31-14페이지의 요건을 참조하십시오.

절차

1단계 Select **Monitor > Spam Quarantine**.

2단계 스팸 격리 섹션의 격리 이름 열에 있는 **Spam Quarantine(스팸 격리)** 링크를 클릭합니다.

3단계 아래로 스크롤하여 **최종 사용자 격리 액세스** 섹션으로 이동합니다.

4단계 **Enable End-User Quarantine Access(최종 사용자 격리 액세스 사용)**를 선택합니다.

5단계 격리된 메시지를 보려고 시도할 때 최종 사용자를 인증하는 데 사용할 방법을 지정합니다.

이 옵션 선택	추가 정보
None	—
Mailbox(IMAP/POP)	인증에 사용할 LDAP 디렉토리가 없는 사이트의 경우 격리가 사서함이 있는 표준 기반 IMAP 또는 POP 서버를 기준으로 사용자 이메일 주소와 비밀번호를 검증할 수 있습니다. 스팸 격리에 로그인할 때 최종 사용자가 전체 이메일 주소와 사서함 비밀번호를 입력합니다. POP 서버가 배너에서 APOP 지원을 광고할 경우 보안상의 이유로(즉, 암호화되지 않은 상태로 비밀번호가 전송되는 것을 방지) Cisco 어플라이언스가 APOP만 사용합니다. APOP가 일부 또는 모든 사용자에 대해 지원되지 않을 경우 APOP를 광고하지 않도록 POP 서버를 다시 구성해야 합니다. SSL을 사용하도록 서버를 구성한 경우 SSL을 선택합니다. 사용자가 사용자 이름만 입력한 경우 이메일 주소를 자동으로 완성하기 위해 추가할 도메인을 지정할 수 있습니다. "Append Domain to Unqualified Usernames(부적격한 사용자 이름에 도메인 추가)"에 로그인하는 사용자의 봉투의 도메인을 입력합니다.
LDAP	이 항목의 시작하기 전에 섹션에서 언급된 섹션에 설명된 대로 LDAP 설정을 구성합니다.

6단계 메시지가 릴리스되기 전에 메시지 본문을 표시할지를 지정합니다.

이 상자를 선택하면 사용자가 스팸 격리 페이지를 통해 메시지 본문을 볼 수 없습니다. 그 대신 격리된 메시지의 본문을 보려면 사용자가 메시지를 릴리스하여 메일 애플리케이션(Microsoft Outlook 등)에서 봐야 합니다. 이 기능을 사용하여 정책 및 규정을 준수할 수 있습니다(예: 규정에서 사용자가 본 모든 이메일을 아카이브하도록 요구할 경우).

7단계 변경 사항을 제출하고 커밋합니다.

향후 작업

(선택 사항) 사용자가 스팸 격리에 액세스할 때 표시되는 페이지를 사용자 지정합니다(아직 지정하지 않은 경우). 스팸 격리 활성화 및 구성, 31-2페이지의 설정 설명을 참조하십시오.

스팸 격리에 대한 최종 사용자 액세스의 URL 결정

최종 사용자가 스팸 격리에 직접 액세스하는 데 사용할 수 있는 URL은 머신의 호스트 이름과 격리가 활성화된 IP 인터페이스에 구성된 설정(HTTP/S 및 포트 번호)에서 형성됩니다. 예를 들면, `HTTP://mail3.example.com:82`와 같습니다.

최종 사용자가 볼 수 있는 메시지

일반 적으로 최종 사용자는 스팸 격리에서 자신의 메시지만 볼 수 있습니다.

액세스 방법(알림을 통해 또는 웹 브라우저를 통해 직접)과 인증 방법(LDAP 또는 IMAP/POP)에 따라 사용자가 스팸 격리에서 여러 이메일 주소의 메일을 볼 수 있습니다.

LDAP 인증을 사용할 경우 기본 이메일 특성의 LDAP 디렉토리에 여러 값이 있으면 그러한 값이 모두 사용자와 연결됩니다. 따라서 LDAP 디렉토리에서 최종 사용자와 연결된 모든 이메일 주소로 전송된 격리된 메시지가 격리에 나타납니다.

인증 방법이 IMAP/POP이거나 사용자가 알림을 통해 직접 격리에 액세스하면 격리가 해당 사용자의 이메일 주소(또는 알림이 전송된 주소)의 메시지만 표시합니다.

사용자가 멤버인 별칭으로 전송된 메시지에 대한 내용은 수신자 이메일 메일 목록 별칭 및 스팸 알림, 31-19페이지를 참조하십시오.

관련 주제

- 스팸 격리에 대한 최종 사용자 액세스 구성, 31-16페이지
- 수신자 이메일 메일 목록 별칭 및 스팸 알림, 31-19페이지

최종 사용자에게 격리된 메시지에 대해 알림

스팸 격리에 스팸 또는 의심스러운 스팸 메시지가 있는 경우 일부 또는 모든 사용자에게 알림 이메일을 보내도록 시스템을 구성할 수 있습니다.

기본적으로 스팸 알림에는 사용자의 격리된 메시지가 표시됩니다. 알림에는 사용자가 스팸 격리에서 격리된 메시지를 보기 위해 클릭할 수 있는 링크도 포함될 수 있습니다. 이러한 링크는 만료되지 않습니다. 사용자가 격리된 메시지를 보고 받은 편지함으로 전송할지 아니면 삭제할지를 결정할 수 있습니다.

참고 클러스터 구성에서 머신 수준에서만 알림을 받을 사용자를 선택할 수 있습니다.

시작하기 전에

- 최종 사용자가 알림에 표시된 메시지를 관리하려면 스팸 격리에 액세스할 수 있어야 합니다. 스팸 격리에 대한 최종 사용자 액세스 구성, 31-16페이지를 참조하십시오.
- 알림을 사용하여 스팸을 관리하는 인증 옵션을 이해합니다. 스팸 관리 기능에 액세스하는 최종 사용자의 인증 옵션, 31-14페이지를 참조하십시오.
- 최종 사용자가 여러 별칭으로 이메일을 수신할 경우 수신자 이메일 메일 목록 별칭 및 스팸 알림, 31-19페이지를 참조하십시오.

절차

1단계 **Monitor(모니터링) > Spam Quarantine(스팸 격리)**을 선택합니다.

2단계 스팸 격리 섹션의 격리 이름 열에 있는 **Spam Quarantine(스팸 격리)** 링크를 클릭합니다.

3단계 아래로 스크롤하여 **스팸 알림** 섹션으로 이동합니다.

4단계 **Enable Spam Notification(스팸 알림 사용)**을 선택합니다.

5단계 옵션을 지정합니다.

메시지 본문을 사용자 지정하려면 다음을 수행합니다.

a. (선택 사항) 기본 텍스트 및 변수를 사용자 지정합니다.

다음과 같은 메시지 변수가 특정 최종 사용자의 실제 값으로 확장됩니다.

- **새 메시지 수**(`%new_message_count%`) - 사용자가 마지막으로 로그인한 이후의 새 메시지 수입니다.

- **총 메시지 수**(`%total_message_count%`) - 스팸 격리의 사용자의 메시지 수입니다.
- **메시지 만료 기한(일)**(`%days_until_expire%`)
- **격리 URL**(`%quarantine_url%`) - 격리에 로그인하여 메시지를 볼 수 있는 URL입니다.
- **사용자 이름**(`%username%`)
- **새 메시지 표**(`%new_quarantine_messages%`) - 격리에서 사용자의 새 메시지를 표시하는 목록입니다.

변수를 삽입하려면 변수를 삽입할 위치에 커서를 놓은 다음 오른쪽의 메시지 변수 목록에서 해당 변수의 이름을 클릭합니다. 또는 변수를 입력합니다.

b. 이 페이지의 최종 사용자 격리 액세스 섹션에서 인증 방법을 활성화한 경우:

- 사용자가 알림의 링크를 클릭하여 스팸 격리에 액세스할 경우 자동으로 로그인되게 하려면 **Enable login without credentials for quarantine access(격리 액세스 자격 증명 없이 로그인 사용)**를 선택합니다. 최종 사용자가 알림의 "Release(릴리스)" 링크만 클릭하면 메시지를 릴리스할 수 있습니다.
- 사용자가 알림의 링크를 클릭하여 스팸 격리에 액세스할 경우 스팸 격리에 로그인하도록 요구하려면 이 옵션을 선택 취소합니다. 최종 사용자가 알림의 "Release(릴리스)" 링크만 클릭해서 메시지를 릴리스할 수 없습니다.

c. **Preview Message(메시지 미리보기)**를 클릭하여 메시지가 원하는 대로 표시되는지 확인할 수 있습니다.

6단계 변경 사항을 제출하고 커밋합니다.

향후 작업

최종 사용자가 이러한 알림을 받게 하려면 스팸 격리 알림 이메일의 보낸 사람: 주소를 메일 애플리케이션(Microsoft Outlook 또는 Mozilla Thunderbird 등)의 정크 메일 설정에 있는 "허용 목록"에 추가할 것을 권장하십시오.

관련 주제

- 수신자 이메일 메일 목록 별칭 및 스팸 알림, 31-19페이지
- 알림 테스트, 31-20페이지
- 스팸 알림 문제 해결, 31-20페이지

수신자 이메일 메일 목록 별칭 및 스팸 알림

알림은 메일 목록과 기타 별칭을 포함하여 격리된 이메일이 있는 각 봉투 수신자에게 전송될 수 있습니다. 각 메일 목록이 단일 다이제스트를 수신합니다. 메일 목록에 알림을 전송하면 목록의 모든 가입자가 알림을 받게 됩니다. 여러 이메일 별칭 또는 알림을 수신하는 LDAP 그룹에 속해 있거나 여러 이메일 주소를 사용하는 사용자는 여러 개의 스팸 알림을 받을 수 있습니다. 다음 표에는 사용자가 여러 개의 알림을 받을 수 있는 상황의 예가 나와 있습니다.

표 31-2 주소/별칭별 알림

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 사용할 경우 메일 목록 별칭에 알림을 보내지 않도록 선택할 수 있습니다. 또는 메일 목록 별칭에 스팸 알림을 보내도록 선택하면 여러 개의 알림이 발생할 수 있는 상황을 어느 정도 방지할 수 있습니다. 스팸 격리의 별칭 통합 쿼리, 25-44페이지를 참조하십시오.

알림의 링크를 클릭하여 스팸 격리에 액세스하는 사용자는 어플라이언스가 스팸 격리 별칭 통합 쿼리를 사용하여 이메일 알림을 보내지 않는 한 최종 사용자가 갖고 있을 수 있는 다른 별칭의 격리된 메시지를 볼 수 없습니다. 어플라이언스에서 처리한 후 확장된 배포 목록에 알림이 전송되면 여러 수신자가 해당 목록의 동일한 격리에 액세스할 수 있습니다.

이는 모든 메일 목록 가입자가 알림을 받게 되며 격리에 로그인하여 메시지를 릴리스하거나 삭제할 수 있음을 의미합니다. 이 경우 알림에 언급된 메시지를 보기 위해 격리를 방문하는 최종 사용자는 다른 사용자가 이미 그러한 메시지를 삭제했음을 알게 될 수 있습니다.

참고 LDAP를 사용하지 않으며 최종 사용자가 여러 개의 이메일 알림을 받지 않게 하려면 알림을 비활성화하고 그 대신 최종 사용자가 직접 격리에 액세스하여 LDAP 또는 POP/IMAP를 통해 인증하도록 허용하는 방법을 고려하십시오.

알림 테스트

테스트 메일 정책을 구성하고 단일 사용자에 대해서만 스팸이 격리되게 하여 알림을 테스트할 수 있습니다. 그런 다음 스팸 격리 알림 설정을 구성합니다. **Enable Spam Notification(스팸 알림 사용)** 확인란을 선택하고 **Enable End-User Quarantine Access(최종 사용자 격리 액세스 사용)**는 선택하지 않습니다. 그러면 **바운스 메시지 전송 대상** 필드에 구성된 관리자만 격리의 새 스팸에 대한 알림을 받습니다.

스팸 알림 문제 해결

관련 주제

- 사용자가 여러 알림을 수신함, 31-20페이지
- 수신자가 알림을 받지 않음, 31-21페이지

사용자가 여러 알림을 수신함

문제 한 명의 사용자가 단일 메시지에 대해 여러 개의 스팸 알림을 받습니다.

솔루션 가능한 원인:

- 사용자가 여러 개의 이메일 주소를 사용하고 있으며 스팸 메시지가 그러한 주소 중 2개 이상에 전송되었습니다.

- 스팸 메시지를 받은 이메일 별칭 중 사용자가 멤버인 이메일 별칭이 하나 이상입니다. 중복을 최소화하고 자세한 내용을 보려면 수신자 이메일 메일 목록 별칭 및 스팸 알림, 31-19페이지를 참조하십시오.

수신자가 알림을 받지 않음

문제 수신자가 스팸 알림을 받지 않습니다.

솔루션

- 알림이 스팸 수신자가 아닌 "바운스 메시지 전송 대상:" 주소로 전송될 경우 스팸 알림이 활성화되었지만 스팸 격리 액세스가 활성화되지 않았음을 의미합니다. 스팸 관리 기능에 액세스하는 최종 사용자의 인증 옵션, 31-14페이지를 참조하십시오.
- 사용자에게 이메일 클라이언트의 정크 메일 설정을 확인해 보라고 요청하십시오.

스팸 격리에서 메시지 관리

이 섹션에서는 로컬 또는 외부 스팸 격리에서 메시지를 처리하는 방법을 설명합니다.

관리자는 스팸 격리의 모든 메시지를 보거나 관리할 수 있습니다.

관련 주제

- 스팸 격리 액세스(관리자), 31-21페이지
- 스팸 격리에서 메시지 검색, 31-21페이지
- 스팸 격리에서 메시지 보기, 31-22페이지
- 스팸 격리에서 메시지 전송, 31-22페이지
- 스팸 격리에서 메시지 삭제, 31-23페이지

스팸 격리 액세스(관리자)

1단계 **Monitor(모니터링) > Spam Quarantine(스팸 격리)**을 선택한 다음 메시지 열의 숫자를 클릭합니다.

스팸 격리가 별도의 브라우저 창에서 열립니다.

스팸 격리에서 메시지 검색

절차

1단계 봉투 수신자를 지정합니다.

참고 부분 주소를 입력할 수 있습니다.

2단계 검색 결과가 입력한 수신자와 정확히 일치해야 하는지 여부를 선택하거나 검색 결과가 입력한 항목을 포함하거나 입력한 항목으로 시작하거나 끝나야 하는지 여부를 선택합니다.

3단계 검색할 날짜 범위를 입력합니다. 달력 아이콘을 클릭하여 날짜를 선택합니다.

4단계 받는 사람: 주소를 지정하고 검색 결과가 입력한 값을 포함하거나 입력한 값과 정확히 일치하거나 입력한 값으로 시작하거나 끝나야 하는지 여부를 선택합니다.

5단계 **Search(검색)**를 클릭합니다. 검색 조건과 일치하는 메시지가 페이지의 검색 섹션 아래에 표시됩니다.

관련 주제

- 매우 큰 메시지 컬렉션 검색, 31-22페이지

매우 큰 메시지 컬렉션 검색

스팸 격리에 매우 큰 메시지 컬렉션이 있고 검색어가 구체적으로 정의되지 않은 경우 쿼리 후에 정보가 반환될 때까지 매우 오래 걸리거나 시간이 초과될 수 있습니다.

검색을 다시 제출할지 확인하는 메시지가 나타납니다. 여러 개의 큰 검색을 동시에 실행할 경우 성능에 영향을 미칠 수 있다는 점에 유의하십시오.

스팸 격리에서 메시지 보기

메시지 목록에는 스팸 격리에 있는 메시지가 표시됩니다. 한 번에 표시되는 메시지 수를 선택할 수 있습니다. 열 머리글을 클릭하여 표시를 정렬할 수 있습니다. 정렬 순서를 반대로 하려면 동일한 열을 다시 클릭하십시오.

본문 및 헤더를 포함하여 메시지를 보려면 메시지의 제목을 클릭하십시오. 메시지가 메시지 세부사항 페이지에 표시됩니다. 메시지의 처음 20K가 표시됩니다. 메시지가 더 긴 경우 20K에서 잘리며 메시지 하단의 링크를 통해 메시지를 다운로드할 수 있습니다.

메시지 세부사항 페이지에서 메시지를 삭제(**Delete(삭제)** 선택)하거나 **Release(릴리스)**를 선택하여 메시지를 릴리스할 수 있습니다. 메시지를 릴리스하면 메시지가 전송됩니다.

메시지에 대한 자세한 내용을 보려면 **Message Tracking(메시지 추적)** 링크를 클릭합니다.

다음을 참고하십시오.

- **첨부 파일이 포함된 메시지 보기**

  첨부 파일이 포함된 메시지를 볼 때 메시지의 본문이 표시된 다음 첨부 파일의 목록이 표시됩니다.

- **HTML 메시지 보기**

  스팸 격리가 HTML 기반 메시지를 최대한 비슷하게 표시하려고 시도합니다. 이미지가 표시되지 않습니다.

- **인코딩된 메시지 보기**

  Base64 인코딩 메시지는 디코딩된 후에 표시됩니다.

스팸 격리에서 메시지 전송

메시지를 전송하기 위해 릴리스하려면 릴리스할 메시지 옆의 확인란을 클릭하고 드롭다운 메뉴에서 **Release(릴리스)**를 선택합니다. 그런 후 **Submit(제출)**을 클릭합니다.

현재 페이지에 표시된 모든 메시지를 자동으로 선택하려면 머리글 행의 확인란을 클릭합니다.

릴리스된 메시지는 이메일 파이프라인의 추가 작업 큐 처리를 건너뛰고 바로 대상 큐로 진행합니다.

스팸 격리에서 메시지 삭제

일정 시간이 지나면 메시지를 자동으로 삭제하도록 스팸 격리를 구성할 수 있습니다. 또한 격리가 최대 크기에 도달하면 가장 오래된 메시지를 자동으로 삭제하도록 스팸 격리를 구성할 수 있습니다. 스팸 격리에서 수동으로 메시지를 삭제할 수도 있습니다.

특정 메시지를 삭제하려면 삭제할 메시지 옆의 확인란을 클릭하고 드롭다운 메뉴에서 **Delete(삭제)**를 선택합니다. 그런 후 **Submit(제출)**을 클릭합니다. 현재 페이지에 표시된 모든 메시지를 자동으로 선택하려면 머리글 행의 확인란을 클릭합니다.

스팸 격리의 모든 메시지를 삭제하려면 격리를 비활성화(스팸 격리 비활성화 정보, 31-23페이지 참조)한 다음 **Delete All Messages(모든 메시지 삭제)** 링크를 클릭합니다. 링크 끝의 괄호 안에 있는 숫자는 스팸 격리의 메시지 수입니다.

스팸 격리를 위한 디스크 공간

기본적으로 스팸 격리의 메시지는 정해진 시간이 지나면 자동으로 삭제됩니다. 격리가 가득 차면 오래된 스팸이 삭제됩니다. 이 설정을 변경하려면 스팸 격리 활성화 및 구성, 31-2페이지를 참조하십시오.

관련 주제

- 디스크 공간 관리, 33-15페이지

스팸 격리 비활성화 정보

스팸 격리를 비활성화한 경우:

- 비활성화할 때 스팸 격리에 메시지가 표시되면 모든 메시지를 삭제하도록 선택할 수 있습니다.
- 격리 스팸 또는 의심스러운 스팸으로 설정된 메일 정책이 메시지를 전송하도록 설정됩니다. 메일 정책을 조정해야 할 수 있습니다.
- 외부 스팸 격리를 완전히 비활성화하려면 Email Security 어플라이언스와 보안 관리 어플라이언스에서 모두 비활성화하십시오.

  Email Security 어플라이언스에서만 외부 스팸 격리를 비활성화하면 외부 격리 또는 해당 메시지 및 데이터가 삭제되지 않습니다.

스팸 격리 기능 문제 해결

- 허용 목록 및 차단 목록 문제 해결, 31-13페이지
- 스팸 알림 문제 해결, 31-20페이지
- 메시지 텍스트를 올바르게 표시, 31-6페이지

32 장

관리 작업 분배

사용자 계정 작업

Cisco 어플라이언스는 사용자 계정을 추가하는 두 가지 방법을 제공합니다. 첫 번째는 Cisco 어플라이언스 자체에서 사용자 계정을 생성하는 것이고, 두 번째는 고유한 중앙 집중식 인증 시스템(LDAP 또는 RADIUS 디렉토리)을 사용하여 사용자 인증을 활성화하는 것입니다. GUI의 System Administration(시스템 관리) > Users(사용자) 페이지(또는 CLI의 `userconfig` 명령)에서 사용자 및 외부 인증 소스에 대한 연결을 관리할 수 있습니다. 외부 디렉토리를 사용한 사용자 인증에 대한 자세한 내용은 외부 인증, 32-21페이지 항목을 참조하십시오.

시스템의 기본 사용자 계정인 admin은 모든 관리 권한을 갖습니다. admin 사용자 계정은 삭제할 수 없지만, 비밀번호를 변경하거나 계정 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 32-1 사용자 역할 목록

사용자 역할	설명
admin	admin 사용자는 시스템의 기본 사용자 계정으로 모든 관리 권한을 갖습니다. 여기에 편의상 나와 있는 admin 사용자 계정은 사용자 역할을 통해 할당할 수 없으며, 비밀번호 변경을 제외하고 편집하거나 삭제할 수 없습니다. admin 사용자만 resetconfig 및 revert 명령을 실행할 수 있습니다.
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 동시에 GUI로 Email Security 어플라이언스를 구성하는 기능을 지원하지 않습니다.
기사	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.
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 비밀번호를 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.

표 32-1 사용자 역할 목록

사용자 역할	설명
읽기 전용 작업자	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, 편집 삭제 또는 중앙 집중식 처리를 위한 설정.
Help Desk 사용자	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 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, 32-7페이지 항목을 참조하십시오. **참고** 사용자 지정 역할에 할당된 사용자는 CLI에 액세스할 수 없습니다.

GUI에만 액세스할 수 있는 Help Desk User 역할 및 사용자 지정 사용자 역할을 제외하고, 표 32-1에 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, 32-21페이지 항목을 참조하십시오.

관련 주제

- 사용자 관리, 32-3페이지

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, 32-4페이지 항목을 참조하십시오.
- 사용자를 삭제합니다. 자세한 내용은 사용자 삭제, 32-5페이지 항목을 참조하십시오.
- 사용자 비밀번호 변경, 사용자 계정 잠금 및 잠금 해제 등 사용자를 편집합니다. 자세한 내용은 사용자 편집, 32-4페이지 항목을 참조하십시오.

- 사용자가 비밀번호를 변경하도록 강제 실행합니다. 사용자가 비밀번호를 변경하도록 강제 실행, 32-5페이지 항목을 참조하십시오.
- 로컬 계정에 대한 사용자 계정 및 비밀번호 설정을 구성합니다. 자세한 내용은 제한적인 사용자 계정 및 비밀번호 설정 구성, 32-17페이지 항목을 참조하십시오.
- 어플라이언스에서 LDAP 또는 RADIUS 디렉토리를 사용하여 사용자를 인증할 수 있습니다. 자세한 내용은 외부 인증, 32-21페이지 항목을 참조하십시오.
- 비관리자가 메시지 추적의 DLP 일치 콘텐츠에 액세스할 수 있습니다. 자세한 내용은 메시지 추적 시 중요 정보의 액세스 제어, 32-5페이지 항목을 참조하십시오.

관련 주제

- 여러 사용자를 지원하는 추가 명령: who, whoami 및 last, 32-6페이지

사용자 추가

시작하기 전에

- 사용하고자 하는 사용자 역할을 확인합니다.
  - 사전 정의된 사용자 역할에 대한 설명은 사용자 역할, 32-2페이지 항목을 참조하십시오.
  - 사용자 지정 역할을 생성하려면 위임 관리를 위한 사용자 지정 사용자 역할 관리, 32-7페이지 항목을 참조하십시오.
- 비밀번호 요구 사항을 지정합니다. 제한적인 사용자 계정 및 비밀번호 설정 구성, 32-17페이지 항목을 참조하십시오.

절차

1단계 **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.

2단계 **Add User(사용자 추가)**를 클릭합니다.

3단계 사용자의 로그인 이름을 입력합니다. 일부 이름은 예약되어 있습니다(예: "operator" 또는 "root").

4단계 사용자의 전체 이름을 입력합니다.

5단계 사전 정의된 사용자 역할 또는 사용자 지정 사용자 역할을 선택합니다.

6단계 비밀번호를 생성하거나 입력합니다.

7단계 변경사항을 제출하고 커밋합니다.

사용자 편집

비밀번호 등을 변경하려면 다음 절차를 수행합니다.

절차

1단계 **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.

2단계 사용자 목록에서 사용자 이름을 클릭합니다.

3단계 사용자를 변경합니다.

4단계 변경사항을 제출하고 커밋합니다.

사용자가 비밀번호를 변경하도록 강제 실행

절차

1단계 **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.

2단계 사용자 목록에서 사용자를 선택합니다.

3단계 **Enforce Password Change(강제로 비밀번호 변경)**를 클릭합니다.

4단계 사용자가 비밀번호를 다음 로그인 시에 변경해야 할지, 또는 지정된 기간(일)이 지난 후에 변경해야 할지를 선택합니다.

5단계 (선택 사항) 지정된 기간 후에 강제로 비밀번호를 변경하도록 하는 경우 비밀번호가 만료된 후 비밀번호를 재설정하도록 유예 기간(일)을 설정합니다.

6단계 **OK(확인)**를 클릭합니다.

7단계 변경사항을 제출하고 커밋합니다.

사용자 삭제

절차

1단계 사용자 목록의 사용자 이름에 해당하는 휴지통 아이콘을 클릭합니다.

2단계 나타나는 경고 대화 상자에서 **Delete(삭제)**를 클릭하여 삭제를 확인합니다.

3단계 변경사항을 커밋합니다.

메시지 추적 시 중요 정보의 액세스 제어

DLP(데이터 유출 방지) 정책을 위반하는 메시지에는 일반적으로 회사 기밀 정보 또는 개인 정보(신용 카드 번호 및 건강 기록 등)와 같은 민감한 정보가 포함됩니다. 기본적으로 이러한 콘텐츠는 Message Details(메시지 정보) 페이지의 DLP Matched Content(DLP 일치 콘텐츠) 탭에 메시지 추적 결과 목록에 메시지로 나타납니다.

관리자 사용자는 항상 이 콘텐츠를 볼 수 있습니다. 그러나 메시지 추적에 액세스할 수 있는 사용자가 어떤 사전 정의된 역할 또는 사용자 지정 역할로 할당되었는지에 따라 이 탭 및 탭의 내용을 숨기도록 선택할 수 있습니다.

시작하기 전에

일치 콘텐츠 로깅을 활성화했는지 여부를 확인합니다. 활성화 여부에 따라 민감한 DLP 데이터를 메시지 추적에 표시할지 여부를 결정합니다. 메시지 추적 시 민감한 DLP 데이터 표시 또는 숨기기, 17-36페이지 항목을 참조하십시오.

절차

1단계 **System Administration(시스템 관리) > Users(사용자)** 페이지로 이동합니다.

2단계 **DLP Tracking Privileges(DLP 추적 권한)**에서 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 메시지 추적 시 DLP 데이터 액세스 권한을 부여할 역할을 선택합니다.

메시지 추적에 액세스할 수 없는 사용자 지정 역할은 이 정보를 볼 수 없으므로 해당 정보 목록이 표시되지 않습니다.

4단계 변경사항을 제출하고 커밋합니다.

이 설정을 적용하려면 보안 서비스에서 다음 기능을 활성화해야 합니다.

- 메시지 추적
- RSA 이메일 DLP
- RSA Email DLP(RSA 이메일 DLP) > Matched Content Logging(일치 콘텐츠 로깅)

여러 사용자를 지원하는 추가 명령: who, whoami 및 last

다음 명령은 어플라이언스에 대한 여러 사용자 액세스를 지원합니다.

- Who 명령은 CLI로 시스템에 로그인한 모든 사용자, 로그인 시간, 유휴 시간 및 사용자가 로그인에 사용한 원격 호스트 목록을 표시합니다.

```
mail3.example.com> who


Username  Login Time  Idle Time  Remote Host  What

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

admin     03:27PM     0s         10.1.3.201   cli
```

- Whoami 명령은 현재 로그인한 사용자의 사용자 이름 및 전체 이름 및 사용자가 속해 있는 그룹을 표시합니다.

```
mail3.example.com> whoami


Username: admin

Full Name: Administrator

Groups: admin, operators, config, log, guest
```

- last 명령은 최근에 어플라이언스에 로그인한 사용자를 표시합니다. 원격 호스트의 IP 주소, 로그인 시간, 로그아웃 시간 및 총 시간도 표시됩니다.

```
mail3.example.com> last


Username  Remote Host  Login Time        Logout Time       Total Time
========  ===========  ================  ================  ==========
admin     10.1.3.67    Sat May 15 23:42  still logged in   15m
admin     10.1.3.67    Sat May 15 22:52  Sat May 15 23:42  50m
admin     10.1.3.67    Sat May 15 11:02  Sat May 15 14:14  3h 12m
admin     10.1.3.67    Fri May 14 16:29  Fri May 14 17:43  1h 13m
shutdown                                 Fri May 14 16:22
shutdown                                 Fri May 14 16:15
admin     10.1.3.67    Fri May 14 16:05  Fri May 14 16:15  9m
admin     10.1.3.103   Fri May 14 16:12  Fri May 14 16:15  2m
admin     10.1.3.103   Thu May 13 09:31  Fri May 14 14:11  1d 4h 39m
admin     10.1.3.135   Fri May 14 10:57  Fri May 14 10:58  0m
admin     10.1.3.67    Thu May 13 17:00  Thu May 13 19:24  2h 24m
```

위임 관리를 위한 사용자 지정 사용자 역할 관리

사용자 지정 사용자 역할을 설계하고 조직 내 사용자 역할에 따라 사용자에게 특정 책임을 위임할 수 있습니다. *위임 관리자*는 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 어플라이언스의 특정 도메인에 대한 메일 정책을 관리하는 사용자가 시스템 관리 및 보안 서비스 구성 기능에는 액세스하지 못하도록 해야 하는 경우, 이러한 액세스 권한은 사전 정의된 관리자 및 운영자 역할에서 부여합니다. 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.

GUI의 System Administration(시스템 관리) > User Roles(사용자 역할) 페이지(또는 CLI의 `userconfig -> role` 명령)에서 사용자 지정 사용자 역할을 정의하고 이 역할이 담당하는 이메일 보안 기능(예: 메일 정책, RSA 이메일 DLP 정책, 이메일 보고서 및 격리)을 관리할 수 있습니다. 위임 관리자가 관리할 수 있는 이메일 보안 기능의 전체 목록은 액세스 권한 할당, 32-9페이지 항목을 참조하십시오. System Administration(시스템 관리) > Users(사용자) 페이지에서 로컬 사용자 계정을 추가하거나 편집할 때 사용자 지정 역할을 생성할 수 있습니다. 자세한 내용은 사용자 계정 추가 시 사용자 지정 사용자 역할 정의, 32-14페이지 항목을 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, 32-1페이지 항목을 참조하십시오. 사용자 지정 역할에 할당된 사용자는 CLI에 액세스할 수 없습니다.

그림 32-1에서는 역할에 할당된 액세스 권한을 포함하여 Email Security 어플라이언스에 정의된 사용자 지정 사용자 역할 목록을 보여줍니다.

그림 32-1 사용자 지정 사용자 역할 목록

User Roles

Custom User Roles for Delegated Administration

Add User Role...

Role Name	Privileges							Assigned Users	Duplicate	Delete
	Email Policies	Data Loss Prevention	Reporting	Message Tracking	Trace	Quarantines	Encryption Profiles			
DLP Administrator	No Access	DLP Policies: 3	Relevant Reports*	Available	No Access	No Access	*Feature Disabled*	susan1		
Policy Administrator	**Incoming** Policies: 1 Content Filters: 0 **Outgoing** Policies: 1 Content Filters: 0	No Access	Relevant Reports*	Available	No Access	Quarantines: 1	*Feature Disabled*	grace1		
Quarantine Manager	No Access	No Access	No Access	No Access	No Access	Quarantines: 3	*Feature Disabled*	jessie1		

** Report access for this role is controlled by the Mail Policy and DLP privileges.*

Key: View restricted to editable items

관련 주제

- 계정 권한 페이지, 32-8페이지
- 액세스 권한 할당, 32-9페이지
- 사용자 지정 사용자 역할 정의, 32-13페이지
- 사용자 계정 추가 시 사용자 지정 사용자 역할 정의, 32-14페이지
- 사용자 지정 사용자 역할에 대한 책임 업데이트, 32-14페이지
- 사용자 지정 사용자 역할 편집, 32-15페이지
- 사용자 지정 사용자 역할 복제, 32-15페이지
- 사용자 지정 사용자 역할 삭제, 32-16페이지

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.

그림 32-2에서는 메일 정책, 이메일 보고, 메시지 추적 및 격리에 액세스 권한이 있는 위임 관리자의 Account Privileges(계정 권한) 페이지를 보여줍니다.

그림 32-2 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 RSA 이메일 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. 위임 관리자는 메시지 추적을 사용할 때 자신이 관리하는 정책과 관련된 DLP 위반 사항을 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, 32-14페이지 항목을 참조하십시오.

관련 주제

- 메일 정책 및 콘텐츠 필터, 32-10페이지
- DLP 정책, 32-11페이지

메일 정책 및 콘텐츠 필터

메일 정책 및 콘텐츠 필터 액세스 권한에서는 Email Security 어플라이언스의 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 *공용*입니다. 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 어플라이언스의 메일 정책 및 콘텐츠 필터를 보거나 편집할 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, 32-14페이지 항목을 참조하십시오.

DLP 정책

DLP 정책 액세스 권한에서는 Email Security 어플라이언스의 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. 관리자 및 운영자만 사용되는 DLP 모드를 RSA 이메일 DLP에서 RSA Enterprise Manager로 변경하거나 그 반대로 변경할 수 있습니다.

위임 관리자가 메일 정책 권한도 보유하고 있는 경우 RSA 이메일 DLP 정책을 사용자 지정할 수 있습니다. 위임 관리자는 RSA 이메일 DLP 정책에 사용자 지정 DLP 사전을 사용할 수 있지만, 사용자 지정 DLP 사전을 보거나 수정할 수는 없습니다.

사용자 지정 사용자 역할에 RSA 이메일 DLP 정책과 관련하여 다음의 액세스 수준을 할당할 수 있습니다.

- **액세스 없음**: 위임 관리자는 Email Security 어플라이언스에 대한 RSA 이메일 DLP 정책을 보거나 편집할 수 없습니다.
- **할당된 항목 보기, 할당된 항목 편집**: 위임 관리자는 DLP 정책 관리자를 사용하여 사용자 지정 사용자 역할에 할당된 RSA 이메일 DLP 정책을 보거나 편집할 수 있습니다. 위임 관리자는 DLP 정책 관리자의 DLP 정책의 이름을 바꾸거나 순서를 바꿀 수 없습니다. 위임 관리자는 DLP 구성을 내보낼 수 있습니다.
- **모든 항목 보기, 할당된 항목 편집**: 위임 관리자는 사용자 지정 사용자 역할에 할당된 RSA 이메일 DLP 정책을 보거나 편집할 수 있습니다. DLP 구성을 내보낼 수 있습니다. 또한, 사용자 지정 사용자 역할에 할당되지 않은 모든 RSA 이메일 DLP 정책도 볼 수 있으나 편집할 수는 없습니다. 위임 관리자는 DLP 정책 관리자에서 DLP 정책 순서를 바꾸거나 정책의 이름을 바꿀 수 없습니다.
- **모든 항목 보기, 모든 항목 편집(전체 액세스)**: 위임 관리자는 새 정책 생성 기능을 포함하여 어플라이언스의 모든 RSA 이메일 DLP 정책에 대한 전체 액세스 권한을 갖습니다. 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 사용자 지정 사용자 역할 테이블을 사용하여 사용자 지정 사용자 역할에 개별 RSA 이메일 DLP 정책을 할당할 수 있습니다.

RSA 이메일 DLP 정책 및 DLP 정책 관리자에 대한 자세한 내용은 17 장, "데이터 유출 방지" 항목을 참조하십시오.

위임 관리를 위한 사용자 지정 사용자 역할 목록을 사용한 RSA 이메일 DLP 정책 할당에 대한 자세한 내용은 사용자 지정 사용자 역할에 대한 책임 업데이트, 32-14페이지 항목을 참조하십시오.

이메일 보고

이메일 보고 액세스 권한에서는 메일 정책, 콘텐츠 필터 및 RSA 이메일 DLP 정책에 대한 사용자 지정 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.

- **액세스 없음**: 위임 관리자는 Email Security 어플라이언스에 대한 보고서를 볼 수 없습니다.
- **관련 보고서 보기**: 위임 관리자는 Email Security Monitor(이메일 보안 모니터) 페이지에서 메일 정책 및 콘텐츠 필터 및 DLP 정책 액세스 권한과 관련된 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.
  - 개요
  - 수신 메일
  - 발송 대상
  - 발송 발신인
  - 내부 사용자
  - 콘텐츠 필터
  - 바이러스 침해
  - 바이러스 유형
  - 보관된 보고서

  DLP 정책 액세스 권한을 가진 위임 관리자는 다음 Email Security Monitor(이메일 보안 모니터) 페이지를 볼 수 있습니다.
  - 개요
  - DLP 사고
  - 보관된 보고서
- **모든 보고서 보기**: 위임 관리자는 Email Security 어플라이언스에서 모든 보고서 및 Email Security Monitor(이메일 보안 모니터) 페이지를 볼 수 있습니다.

이메일 보고 및 이메일 보안 모니터에 대한 자세한 내용은 28장, “이메일 보안 모니터링 사용” (1페이지) 장을 참조하십시오.

메시지 추적

메시지 추적 액세스 권한에서는 System Administration(시스템 관리) > Users(사용자) 페이지에서 DLP Tracking Policies(DLP 추적 정책) 옵션이 활성화되어 있고 사용자 지정 사용자 역할에 DLP 정책 액세스 권한도 있는 경우, 사용자 지정 사용자 역할에 할당된 위임 관리자가 조직의 DLP 정책을 위반할 가능성이 있는 메시지 콘텐츠를 비롯하여 메시지 추적에 액세스할지 여부를 정의합니다.

위임 관리자는 자신에게 할당된 RSA 이메일 DLP 정책에 대한 DLP 위반 사항만 검색할 수 있습니다.

메시지 추적에 대한 자세한 내용은 29장, “메시지 추적” (1페이지) 항목을 참조하십시오.

위임 관리자가 메시지 추적에서 일치하는 DLP 콘텐츠를 볼 수 있도록 허용하는 정보에 대해서는 메시지 추적 시 중요 정보의 액세스 제어, 32-5페이지 항목을 참조하십시오.

추적

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 사용한 메일 흐름 디버깅: 추적, 40-1페이지 항목을 참조하십시오.

격리

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 위임 관리를 위한 사용자 지정 사용자 역할 테이블을 사용하여 사용자 지정 사용자 역할에 격리를 할당할 수 있습니다.

격리 관리 작업을 관리자에게 할당하는 방법에 대한 자세한 내용은 다른 사용자에게 메시지 처리 작업 분배 정보, 30-9페이지 및 스팸 격리에 대한 관리자 액세스 구성, 31-4페이지 항목을 참조하십시오.

위임 관리를 위한 사용자 지정 사용자 역할 목록을 사용한 격리 할당에 대한 자세한 내용은 사용자 지정 사용자 역할에 대한 책임 업데이트, 32-14페이지 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(IronPort 이메일 암호화) 페이지에서 암호화 프로파일을 생성하거나 편집할 때 암호화 프로파일을 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.

절차

1단계 **System Administration(시스템 관리) > User Roles(사용자 역할)**를 선택합니다.

2단계 **Add User Role(사용자 역할 추가)**을 클릭합니다.

3단계 사용자 역할의 이름을 입력합니다.

4단계 사용자 역할 및 해당 권한에 대한 설명을 입력합니다.

5단계 사용자 역할의 액세스 권한을 선택합니다. (각 액세스 권한 유형에 대한 자세한 내용은 액세스 권한 할당, 32-9페이지 항목을 참조하십시오.)

6단계 변경사항을 제출하고 커밋합니다.

사용자 계정 추가 시 사용자 지정 사용자 역할 정의

Email Security 어플라이언스에서 로컬 사용자 계정을 추가하거나 편집할 때 새 사용자 지정 사용자 역할을 생성할 수 있습니다.

사용자 계정 추가에 대한 자세한 내용은 사용자 관리, 32-3페이지 항목을 참조하십시오.

절차

1단계 **System Administration(시스템 관리) > Users(사용자)** 페이지로 이동합니다.

2단계 **Add User(사용자 추가)**를 클릭합니다.

3단계 사용자 계정을 생성할 때 사용자 지정 역할을 선택합니다.

4단계 **Add Role(역할 추가)**을 선택합니다.

5단계 새 역할의 이름을 입력합니다.

6단계 새 사용자 계정을 제출합니다.

AsyncOS는 새 사용자 계정 및 사용자 지정 사용자 역할이 추가되었음을 알리는 알림을 표시합니다.

7단계 **System Administration(시스템 관리) > User Roles(사용자 역할)** 페이지로 이동합니다.

8단계 위임 관리를 위한 사용자 지정 사용자 역할 표에서 사용자 지정 사용자 역할의 이름을 클릭합니다.

9단계 사용자 역할 및 해당 권한에 대한 설명을 입력합니다.

10단계 사용자 역할의 액세스 권한을 선택합니다. (각 액세스 권한 유형에 대한 자세한 내용은 액세스 권한 할당, 32-9페이지 항목을 참조하십시오.)

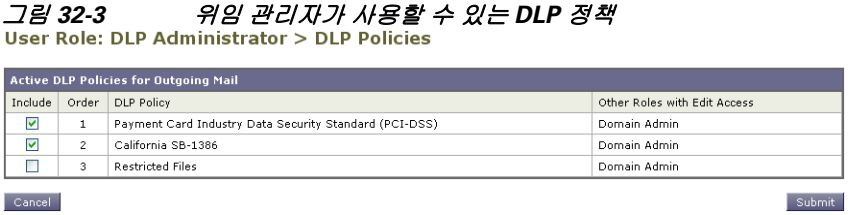
11단계 변경사항을 제출하고 커밋합니다.

사용자 지정 사용자 역할에 대한 책임 업데이트

GUI 상단에 있는 메뉴에서 개별 보안 기능을 검색하여 사용자 지정 사용자 역할에 책임을 할당할 수 있습니다. 또한, User Roles(사용자 역할) 페이지의 위임 관리를 위한 사용자 지정 사용자 역할 테이블에는 위임 관리자가 한 곳에서 관리할 수 있는 모든 보안 기능(암호화 프로파일 제외)에 대한 링크가 통합되어 있습니다. 이 표에서 사용자 지정 사용자 그룹의 액세스 권한 이름을 클릭하면 어플라이언스의 모든 메일 정책, 콘텐츠 필터, 활성 RSA 이메일 DLP 정책 또는 격리 목록이 표시되고, 액세스할 수 있는 다른 사용자 지정 사용자 역할의 이름이 표시됩니다.

예를 들어 그림 32-3에서는 Email Security 어플라이언스에서 사용할 수 있는 활성 RSA 이메일 DLP 정책 목록을 표시합니다. DLP 정책에 액세스할 수 있는 다른 사용자 지정 사용자 그룹도 나열됩니다. 관리자는 DLP 정책 관리자를 사용하여 이 목록에서 위임 관리자에게 할당할 DLP 정책을 선택할 수 있습니다.

그림 32-3 위임 관리자가 사용할 수 있는 DLP 정책



절차

1단계 **System Administration(시스템 관리) > User Roles(사용자 역할)** 페이지로 이동합니다.

2단계 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.

3단계 위임 관리자에게 할당하려는 메일 정책, 콘텐츠 필터, DLP 정책 또는 격리를 선택합니다.

4단계 변경사항을 제출하고 커밋합니다.

사용자 지정 사용자 역할 편집

절차

1단계 **System Administration(시스템 관리) > User Roles(사용자 역할)** 페이지로 이동합니다.

2단계 위임 관리를 위한 사용자 지정 사용자 역할 목록에서 사용자 역할의 이름을 클릭합니다.

3단계 사용자 역할을 변경합니다.

4단계 변경사항을 제출하고 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 어플라이언스가 여러 도메인의 메시지를 처리하는 경우, 유사한 액세스 권한을 가진 사용자 지정 사용자 역할을 생성하되 도메인에 따라 메일 정책을 각기 다르게 적용할 수 있습니다. 이렇게 하면 위임 관리자가 다른 위임 관리자의 책임에 영향을 주지 않으면서 도메인에 대한 메일 정책을 관리할 수 있습니다.

절차

1단계 **System Administration(시스템 관리) > User Roles(사용자 역할)** 페이지로 이동합니다.

2단계 위임 관리를 위한 사용자 지정 사용자 역할 목록에서 복제할 사용자 역할의 복제 아이콘을 클릭합니다.

3단계 사용자 지정 사용자 역할의 이름을 변경합니다.

4단계 새 사용자 지정 사용자 역할에 맞게 액세스 권한을 변경합니다.

5단계 변경사항을 제출하고 커밋합니다.

사용자 지정 사용자 역할 삭제

사용자 지정 역할을 삭제하면 사용자는 할당 해제 상태가 되고 어플라이언스에 액세스할 수 없습니다. 사용자 한 명 이상에게 할당된 사용자 지정 사용자 역할을 삭제하더라도 경고 메시지가 발송되지 않습니다. 삭제한 사용자 지정 사용자 역할에 할당된 사용자를 다시 할당해야 합니다.

절차

1단계 **System Administration(시스템 관리) > User Roles(사용자 역할)** 페이지로 이동합니다.

2단계 위임 관리를 위한 사용자 지정 사용자 역할 목록에서 삭제할 사용자 역할의 휴지통 아이콘을 클릭합니다.

3단계 나타나는 경고 대화 상자에서 **Delete(삭제)**를 클릭하여 삭제를 확인합니다.

4단계 변경사항을 커밋합니다.

비밀번호

비밀번호 변경

관리자는 GUI 상단에 있는 Options(옵션) > Change Password(비밀번호 변경) 링크를 통해 자신의 비밀번호를 변경할 수 있습니다.

새 비밀번호를 제출하는 즉시 로그아웃되고 로그인 화면으로 연결됩니다.

CLI에서는 `password` 또는 `passwd` 명령을 사용하여 비밀번호를 변경합니다. admin 사용자 계정의 비밀번호를 잊은 경우 비밀번호를 재설정하려면 고객 지원 업체에 문의하십시오.

`password` 명령에서는 보안을 위해 이전 비밀번호를 입력해야 합니다.

참고 비밀번호 변경사항은 즉시 적용되므로 변경사항을 커밋할 필요가 없습니다.

사용자 계정 잠금 및 잠금 해제

사용자 계정을 잠그면 로컬 사용자가 어플라이언스에 로그인할 수 없습니다. 다음 중 한 가지 방법으로 사용자 계정을 잠글 수 있습니다.

- AsyncOS는 사용자가 Local User Account & Password Settings(로컬 사용자 계정 및 비밀번호 설정) 섹션에 정의된 최대 로그인 실패 횟수를 초과한 경우 사용자 계정을 잠급니다.
- 관리자는 System Administration(시스템 관리) > Users(사용자) 페이지에서 보안을 위해 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 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 계정 및 비밀번호 설정 구성, 32-17페이지 항목을 참조하십시오.

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 사용한 어플라이언스 액세스에 대한 자세한 내용은 어플라이언스에 연결, 3-9페이지 항목을 참조하십시오.

제한적인 사용자 계정 및 비밀번호 설정 구성

조직의 비밀번호 정책을 적용하기 위한 사용자 계정 및 비밀번호에 대한 제한 사항을 정의할 수 있습니다. 사용자 계정 및 비밀번호 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
- **비밀번호 수명 규칙.** 사용자가 로그인한 후 비밀번호를 변경해야 하기 전까지 비밀번호를 유지할 수 있는 기간을 정의할 수 있습니다.
- **비밀번호 규칙.** 사용자가 선택할 수 있는 비밀번호의 종류(예: 선택 문자 또는 필수 문자)를 정의할 수 있습니다.

System Administration(시스템 관리) > Users(사용자) 페이지의 Local User Account and Password Settings(로컬 사용자 계정 및 비밀번호 설정) 섹션에서 사용자 계정 및 비밀번호 제한 사항을 정의합니다.

절차

1단계 **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.

2단계 **Local User Account and Password Settings(로컬 사용자 계정 및 비밀번호 설정)** 섹션으로 스크롤합니다.

3단계 **Edit Settings(설정 편집)**를 클릭합니다.

4단계 아래 설명된 대로 설정을 구성합니다.

설정	설명
사용자 계정 잠금	사용자가 로그인에 실패한 후 사용자 계정을 잠글지 여부를 선택합니다. 사용자 계정을 잠그기 위한 로그인 실패 횟수를 지정합니다. 1~ 60의 숫자를 입력할 수 있습니다. 기본값은 5입니다. 계정 잠금을 구성할 때 로그인을 시도하는 사용자에게 표시할 메시지를 입력합니다. 7비트 ASCII 문자를 사용하여 텍스트를 입력합니다. 사용자가 관리자가 잠근 계정에 대한 올바른 비밀번호를 입력하는 경우에만 이 메시지가 표시됩니다. 로그인 실패로 인해 계정이 잠긴 경우에는 이 메시지가 표시되지 않습니다. 사용자 계정이 잠긴 경우 관리자는 GUI의 Edit User(사용자 편집) 페이지 또는 `userconfig` CLI 명령을 사용하여 해당 계정을 잠금 해제할 수 있습니다. 로그인 실패는 사용자가 연결된 머신 또는 연결 유형(예: SSH 또는 HTTP)에 관계없이 사용자에 의해 추적됩니다. 사용자가 성공적으로 로그인하면 로그인 실패 횟수는 0으로 재설정됩니다. 최대 로그인 실패 횟수에 도달하여 사용자 계정이 잠긴 경우 관리자에게 경고를 보냅니다. 이 경고는 "Info" 심각도 수준으로 설정됩니다. **참고** 개별 사용자 계정은 수동으로 잠글 수 있습니다. 자세한 내용은 사용자 계정 잠금 및 잠금 해제, 32-17페이지 항목을 참조하십시오.
비밀번호 재설정	다음을 선택할 수 있습니다. • 관리자가 사용자의 비밀번호를 변경하면 사용자는 비밀번호를 강제로 변경해야 하는지 여부. • 사용자는 지정된 기간이 지난 후에 비밀번호를 변경해야 하는지 여부. 사용자가 비밀번호를 변경하기 전까지 비밀번호가 유지되는 기간(일)을 입력합니다. 1~366의 숫자를 입력할 수 있습니다. 기본값은 90입니다. 이 경우 선택적으로 다음을 선택할 수 있습니다. – 예정된 비밀번호 만료에 대한 알림 표시. 비밀번호가 만료되기 며칠 전부터 사용자에게 알릴지 그 기간(일)을 입력합니다. – 비밀번호 만료 후에 비밀번호를 재설정하는 유예 기간(일)을 허용합니다. 기간(일)을 입력합니다. 유예 기간을 설정하는 경우 지정된 기간 안에 비밀번호가 변경되지 않으면 사용자 계정이 잠깁니다. 유예 기간을 설정하지 않은 경우 사용자는 비밀번호가 만료된 후 언제든지 비밀번호를 변경할 수 있습니다. **참고** 사용자 계정에서 비밀번호 챌린지 대신 SSH 키를 사용하는 경우에도 계속 비밀번호 재설정 규칙이 적용됩니다. SSH 키를 사용하는 사용자 계정이 만료되면, 사용자는 이전 비밀번호를 입력하거나 관리자에게 수동으로 비밀번호를 변경하여 계정과 관련된 키를 변경하도록 요청해야 합니다. 자세한 내용은 SSH(Secure Shell) 키 관리, 32-28페이지 항목을 참조하십시오.

설정	설명
비밀번호 규칙: 최소 <number>자가 필요합니다.	비밀번호에 포함될 수 있는 최소 문자 수를 입력합니다. 0~128의 숫자를 입력합니다. CSCuh96198 기본값은 8자입니다. 비밀번호는 여기에 지정한 숫자보다 더 많은 문자로 구성할 수 있습니다.
비밀번호 규칙: 적어도 하나의 숫자(0~9)가 필요합니다.	비밀번호에 적어도 하나의 숫자가 포함되어야 하는지 여부를 선택합니다.
비밀번호 규칙: 적어도 하나의 특수 문자가 필요합니다.	비밀번호에 적어도 하나의 특수 문자가 포함되어야 하는지 여부를 선택합니다. 비밀번호에는 다음과 같은 특수 문자가 포함될 수 있습니다. ~ ? ! @ # $ % ^ & * - _ + = \ | / [ ] ( ) < > { } ` ' " ; : , .
비밀번호 규칙: 사용자 이름이나 사용자 이름을 변형한 비밀번호를 사용할 수 없습니다.	비밀번호가 사용자 이름 또는 사용자 이름을 변형한 비밀번호와 동일해도 되는지 여부를 선택합니다. 사용자 이름 변형이 금지되는 경우 다음 규칙이 비밀번호에 적용됩니다. • 비밀번호는 대소문자에 상관없이 사용자 이름과 동일할 수 없습니다. • 비밀번호는 대소문자에 상관없이 사용자 이름의 역순과 동일할 수 없습니다. • 비밀번호는 다음의 대체 문자가 있는 사용자 이름 또는 사용자 이름의 역순과 동일할 수 없습니다. – "a": "@" 또는 "4" – "e": "3" – "i": "|", "!" 또는 "1" – "o": "0" – "s": "$" 또는 "5" – "t"" "+" 또는 "7"
비밀번호 규칙: 지난 비밀번호 <number>개를 재사용할 수 없도록 설정합니다.	사용자가 비밀번호를 강제로 변경해야 하는 경우 최근에 사용한 비밀번호를 사용하도록 허용할지 여부를 선택합니다. 최근 비밀번호를 재사용하는 것을 허용하지 않을 경우 지난 비밀번호 몇 개를 사용할 수 없는지 그 숫자를 입력합니다. 1~15의 숫자를 입력할 수 있습니다. 기본값은 3입니다.

설정	설명
비밀번호 규칙:	비밀번호에 사용할 수 없는 단어 목록을 생성할 수 있습니다.
비밀번호에 사용할 수 없는 단어 목록	금지된 단어를 별도의 행에 표시하여 이 파일을 텍스트 파일로 만듭니다. `forbidden_password_words.txt` 이름으로 파일을 저장하고 SCP 또는 FTP를 사용하여 파일을 어플라이언스의 에 업로드합니다. 이 제한 사항을 선택된 상태에서 단어 목록을 업로드하지 않으면 제한 사항이 무시됩니다.
비밀번호 강도	관리자 또는 사용자가 새 비밀번호를 입력하는 경우 비밀번호 강도 표시기를 표시할 수 있습니다. 이 설정은 강력한 비밀번호를 생성하도록 강제하는 것은 아니며 단순히 입력한 비밀번호가 얼마나 쉽게 추측될 수 있는지를 나타낼 뿐입니다. 표시기를 표시할 역할을 선택합니다. 선택한 역할에 0보다 큰 숫자를 입력합니다. 숫자가 클수록 강력한 비밀번호 등록이 까다로워집니다. 이 설정에는 최대값이 없습니다. 예: • `30`을 입력하면 하나 이상의 대문자, 소문자, 숫자 및 특수 문자를 포함하는 8자리 비밀번호가 강력한 비밀번호로 등록됩니다. • `18`을 입력하면 모두 소문자이고 숫자 또는 특수 문자가 없는 8자리 비밀번호가 강력한 비밀번호로 등록됩니다. 비밀번호 강도는 로그 스케일로 측정됩니다. 평가는 NIST SP 800-63, 부록 A에 정의된 미국 NIST(National Institute of Standards and Technology) 엔트로피 규칙을 기반으로 합니다. 일반적으로 강력한 비밀번호의 특성은 다음과 같습니다. • 긴 길이 • 대문자, 소문자, 숫자 및 특수 문자 포함 • 모든 언어의 사전에 있는 단어를 포함하지 않음 이러한 특성을 가진 비밀번호 생성을 강제하려면 이 페이지의 나머지 설정을 사용합니다.

5단계 변경사항을 제출하고 커밋합니다.

다음 작업

비밀번호에 사용할 수 없는 단어 목록을 선택한 경우 설명되어 있는 텍스트 파일을 생성 및 업로드합니다.

외부 인증

네트워크의 LDAP 또는 RADIUS 디렉토리에 사용자 정보를 저장하는 경우 외부 디렉토리를 사용하여 어플라이언스에 로그인한 사용자를 인증하도록 Cisco 어플라이언스를 구성할 수 있습니다. 인증에 외부 디렉토리를 사용하도록 어플라이언스를 설정하려면 GUI의 System Administration(시스템 관리) > Users(사용자) 페이지 또는 CLI의 `userconfig` 명령과 `external` 하위 명령을 사용합니다.

외부 인증이 활성화된 경우 사용자가 Email Security 어플라이언스에 로그인하면 어플라이언스는 먼저 사용자가 시스템에서 정의한 "admin" 계정인지 여부를 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 서버에 대한 사용자 인증에 실패하면 어플라이언스는 이 사용자를 Email Security 어플라이언스에 정의된 로컬 사용자로 인증하려고 시도합니다. 사용자가 외부 서버 또는 어플라이언스에 없는 경우 또는 사용자가 잘못된 비밀번호를 입력하는 경우 어플라이언스에 대한 액세스가 거부됩니다.

외부 RADIUS 서버에 연결할 수 없는 경우 목록의 다음 서버를 시도합니다. 모든 서버에 연결할 수 없는 경우 어플라이언스는 사용자를 사용자 Email Security 어플라이언스에 정의된 로컬 사용자로 인증하려고 시도합니다. 그러나 외부 RADIUS 서버에서 어떤 이유(예: 잘못된 비밀번호 또는 사용자 부재)로든 사용자를 거부하는 경우 어플라이언스에 대한 액세스가 거부됩니다.

관련 주제

- LDAP 인증 사용, 32-21페이지
- RADIUS 인증 활성화, 32-22페이지

LDAP 인증 사용

LDAP 디렉토리를 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. 사용자가 다양한 사용자 역할이 있는 여러 LDAP 그룹에 속하는 경우, AsyncOS는 사용자에게 가장 제한이 많은 역할에 해당하는 권한을 부여합니다. 예를 들어 사용자가 작업자 권한을 가진 그룹과 헬프 데스크 사용자 권한을 가진 그룹에 속하는 경우, AsyncOS는 사용자에게 헬프 데스크 사용자 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 25 장, "LDAP 쿼리" 항목을 참조하십시오.

절차

1단계 **System Administration(시스템 관리) > Users(사용자)**를 선택합니다.

2단계 아래로 스크롤하여 **External Authentication(외부 인증)** 섹션으로 이동합니다.

3단계 **Enable(활성화)**을 클릭합니다.

4단계 **Enable External Authentication(외부 인증 활성화)** 확인란을 선택합니다.

5단계 인증 유형으로 **LDAP**를 선택합니다.

6단계 웹 사용자 인터페이스에서 외부 인증 자격 증명을 저장할 시간을 입력합니다.

7단계 사용자를 인증하는 LDAP 외부 인증 쿼리를 선택합니다.

8단계 어플라이언스가 시간 초과되기 전까지 서버의 응답을 기다리는 시간(초)을 입력합니다

9단계 어플라이언스에서 인증할 LDAP 디렉토리 그룹의 이름을 입력하고 그룹의 사용자 역할을 선택합니다.

10단계 선택적으로 **Add Row(행 추가)**를 클릭하여 다른 디렉토리 그룹을 추가합니다. 어플라이언스에서 인증할 각 디렉토리 그룹에 대해 9단계 및 10단계단계를 반복합니다.

11단계 변경사항을 제출하고 커밋합니다.

RADIUS 인증 활성화

또한 RADIUS 디렉토리를 사용하여 사용자를 인증하고 사용자 그룹을 Cisco 역할에 할당할 수 있습니다. RADIUS 서버는 AsyncOS가 RADIUS 디렉토리의 사용자를 Cisco 사용자 역할에 할당하는 데 사용하는 CLASS 특성을 지원합니다. 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.

절차

1단계 System Administration(시스템 관리) > Users(사용자) 페이지에서 **Enable(활성화)**을 클릭합니다.

2단계 활성화되어 있지 않은 경우에는 **Enable External Authentication(외부 인증 활성화)** 옵션을 선택합니다.

3단계 RADIUS 서버의 호스트 이름을 입력합니다.

4단계 RADIUS 서버의 포트 번호를 입력합니다. 기본 포트 번호는 1812입니다.

5단계 RADIUS 서버의 공유 암호를 입력합니다.

6단계 어플라이언스가 시간 초과되기 전까지 서버의 응답을 기다리는 시간(초)을 입력합니다.

7단계 (선택 사항) **Add Row(행 추가)**를 클릭하여 다른 RADIUS 서버를 추가합니다. 각 RADIUS 서버에 대해 3단계~6단계를 반복합니다.

참고 최대 10개의 RADIUS 서버를 추가할 수 있습니다.

8단계 "External Authentication Cache Timeout(외부 인증 캐시 시간제한)" 필드에는 재인증을 위해 RADIUS 서버에 다시 연결하기 전까지 AsyncOS가 외부 인증 자격 증명을 저장하는 시간(초)을 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.

9단계 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 • 관리자 • 기사 • 운영자 • 읽기 전용 작업자 • Help Desk 사용자 • 게스트
외부에서 인증된 모든 사용자를 관리자 역할에 매핑합니다.	AsyncOS는 RADIUS 사용자를 관리자 역할에 할당합니다.

10단계 외부에서 인증된 모든 사용자를 관리자 역할에 매핑할지, 아니면 각기 다른 어플라이언스 사용자 역할 유형에 매핑할지 선택합니다.

11단계 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, 32-1페이지 항목을 참조하십시오.

12단계 변경사항을 제출하고 커밋합니다.

Email Security 어플라이언스에 대한 액세스 구성

AsyncOS는 Email Security 어플라이언스에 대한 사용자 액세스를 관리하는 관리자 제어 기능을 제공합니다. 여기에는 웹 UI 세션에 대한 시간제한과 사용자 및 조직의 프록시 서버에서 어플라이언스에 액세스할 때 사용하는 IP 주소가 표시된 액세스 목록이 포함됩니다.

관련 주제

- IP 기반 네트워크 액세스 구성, 32-24페이지
- 세션 시간제한 구성, 32-26페이지
- 관리자에게 메시지 표시, 32-27페이지
- 로그인 후 메시지 표시, 32-27페이지

IP 기반 네트워크 액세스 구성

어플라이언스에 직접 연결된 사용자 및 역방향 프록시를 통해 연결된 사용자(조직에서 원격 사용자에 대해 역방향 프록시를 사용하는 경우)에 대한 액세스 목록을 생성하여 사용자가 Email Security 어플라이언스에 액세스하는 데 사용하는 IP 주소를 제어할 수 있습니다.

관련 주제

- 직접 연결, 32-24페이지
- 프록시를 통한 연결, 32-24페이지
- 액세스 목록 생성, 32-25페이지

직접 연결

Email Security 어플라이언스에 연결할 수 있는 머신의 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

조직 네트워크에서 원격 사용자 머신과 Email Security 어플라이언스 간에 역방향 프록시 서버를 사용하는 경우, AsyncOS에서는 어플라이언스에 연결할 수 있는 프록시의 IP 주소를 포함하는 액세스 목록을 생성할 수 있습니다.

역방향 프록시를 사용하는 경우에도 AsyncOS는 사용자 연결을 허용하는 IP 주소 목록과 비교하여 원격 사용자 머신의 IP 주소 유효성을 검사합니다. 프록시가 원격 사용자 IP 주소를 Email Security 어플라이언스로 전송하기 위해서는 어플라이언스로의 연결 요청에 `x-forwarded-for` HTTP 헤더를 포함해야 합니다.

`x-forwarded-for` 헤더는 비RFC 표준 HTTP 헤더로 다음과 같은 형식을 사용합니다.

```
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 어플라이언스는 허용되는 사용자 및 액세스 목록의 프록시 IP 주소와 비교하여 헤더의 원격 사용자 IP 주소 및 연결 프록시의 IP 주소가 일치하는지 확인합니다.

참고 AsyncOS는 `x-forwarded-for` 헤더에서 IPv4 주소만 지원합니다.

액세스 목록 생성

GUI의 Network Access(네트워크 액세스) 페이지 또는 `adminaccessconfig > ipaccess` CLI 명령을 사용하여 네트워크 액세스 목록을 생성할 수 있습니다.

AsyncOS는 액세스 목록에 대해 다음 4가지 제어 모드를 제공합니다.

- **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 사용자 IP 주소가 `x-forwarded-header`에 포함되어 있으며 액세스 목록에 있는 사용자에 대해 정의된 IP 주소, IP 범위 또는 CIDR 범위와 일치합니다.
- **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.

다음 조건 중 하나가 참인 경우 변경사항을 제출하고 커밋한 후에는 어플라이언스에 대한 액세스를 잃게 됩니다.

- **특정 연결만 허용**을 선택했지만 목록에 현재 머신의 IP 주소가 포함되어 있지 않음.
- **프록시를 통한 특정 연결만 허용**을 선택하고 현재 어플라이언스에 연결되어 있는 프록시의 IP 주소가 프록시 목록에 포함되어 있지 않으며 원본 IP 헤더의 값이 허용되는 IP 주소 목록에 없음.
- **직접 또는 프록시를 통한 특정 연결만 허용**을 선택하고
  - 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.

절차

1단계 **System Administration(시스템 관리) > Network Access(네트워크 액세스)**를 선택합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 액세스 목록에 대한 제어 모드를 선택합니다.

4단계 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.

5단계 프록시를 통한 연결이 허용되는 경우 다음 정보를 입력합니다.

- 어플라이언스에 연결할 수 있는 프록시의 IP 주소 여러 항목을 구분하려면 쉼표를 사용합니다.
- 프록시가 어플라이언스에 전송하는 원래 IP 헤더의 이름. 원격 사용자 머신 및 요청을 전달한 프록시 서버의 IP 주소를 포함합니다. 기본적으로 헤더의 이름은 `x-forwarded-for`입니다.

6단계 변경사항을 제출하고 커밋합니다.

세션 시간제한 구성

- 웹 UI 세션 시간제한 구성, 32-26페이지
- CLI 세션 시간제한 구성, 32-27페이지

웹 UI 세션 시간제한 구성

비활성화로 인해 AsyncOS에서 사용자가 로그아웃하기 전에 Email Security 어플라이언스의 웹 UI에 로그인할 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.

절차

1단계 **System Administration(시스템 관리) > Network Access(네트워크 액세스)**를 선택합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 **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.

4단계 변경사항을 제출하고 커밋합니다.

또한 CLI의 `adminaccessconfig` 명령을 사용하여 웹 UI 세션 시간제한을 구성할 수 있습니다. *Cisco AsyncOS for Email CLI 참조 설명서*를 참조하십시오.

CLI 세션 시간제한 구성

비활성화로 인해 AsyncOS에서 사용자가 로그아웃하기 전에 Email Security 어플라이언스의 CLI에 로그인할 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.

절차

1단계 **System Administration(시스템 관리) > Network Access(네트워크 액세스)**를 선택합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 **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.

4단계 변경사항을 제출하고 커밋합니다.

또한 CLI의 `adminaccessconfig` 명령을 사용하여 CLI 시간제한을 구성할 수 있습니다. *Cisco AsyncOS for Email CLI 참조 설명서*를 참조하십시오.

관리자에게 메시지 표시

로그인 전 메시지 표시

사용자가 SSH, 텔넷, FTP 또는 웹 UI를 통해 어플라이언스에 로그인하려고 시도하기 전에 Email Security 어플라이언스를 구성하여 메시지를 표시할 수 있습니다. 로그인 배너는 로그인 프롬프트 위에 표시되는 사용자 지정 가능한 텍스트입니다. 로그인 배너를 사용하여 어플라이언스에 대한 내부 보안 정보 또는 모범 사례 지침을 표시할 수 있습니다. 예를 들어 어플라이언스의 무단 사용을 금지한다는 내용의 간단한 메모나 사용자가 어플라이언스에 대해 변경한 내용을 검토할 수 있는 조직의 권리에 대해 명시하는 상세 경고를 생성할 수 있습니다.

CLI의 `adminaccessconfig > banner` 명령을 사용하여 로그인 배너를 생성합니다. 로그인 배너의 최대 길이는 2,000자입니다(80x25 콘솔에 적합). 로그인 배너는 어플라이언스의 `/data/pub/configuration` 디렉토리에 있는 파일에서 가져올 수 있습니다. 배너를 생성한 후에는 변경사항을 커밋합니다.

로그인 후 메시지 표시

사용자가 SSH, 텔넷, FTP 또는 웹 UI를 통해 어플라이언스에 성공적으로 로그인한 후 시작 배너를 표시하도록 Cisco AsyncOS for Email을 구성할 수 있습니다. 시작 배너를 사용하여 어플라이언스에 대한 내부 보안 정보 또는 모범 사례 지침을 표시할 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 생성한 후에는 변경사항을 커밋합니다.

자세한 내용은 *Cisco AsyncOS for Email CLI 참조 설명서*를 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 비밀번호 챌린지가 아닌 SSH 키를 사용하여 사용자 계정을 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 머신으로 로그 파일을 SCP 푸시할 때 사용할 호스트 키를 구성하려면 logconfig -> hostkeyconfig를 사용합니다. 자세한 내용은 38 장, "로깅" 항목을 참조하십시오.

참고 sshconfig 명령을 사용한 후에 변경사항을 적용하려면 재부팅해야 합니다.

hostkeyconfig를 사용하여 원격 호스트 키를 검색하고 이를 Cisco 어플라이언스에 추가할 수 있습니다.

관련 주제

- 예: 새 공개 키 설치, 32-28페이지
- 예: SSH 서버 구성 편집, 32-29페이지

예: 새 공개 키 설치

다음 예에서는 관리자 계정에 대한 새 공개 키를 설치합니다.

```
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 예에서는 SSH 서버 구성을 편집하는 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,c
ast128-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-sha
1-96,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-gr
oup14-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. 명령 목록은 부록 A, "AsyncOS 빠른 참조 설명서" 항목을 참조하십시오. 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]
```

활성 관리자 세션 보기

어플라이언스에 현재 로그인되어 있는 모든 관리자 및 세션에 대한 정보를 보려면 페이지 상단의 **Options(옵션) > Active Sessions(활성 세션)**를 클릭합니다.

33 장

시스템 관리

참고 이 섹션에 설명된 여러 기능 또는 명령이 영향을 미치거나 라우팅 우선순위의 영향을 받습니다. 자세한 내용은 IP 주소, 인터페이스 및 라우팅, B-3페이지를 참조하십시오.

어플라이언스 관리

다음과 같은 작업을 통해 어플라이언스 내에서 공통 기능을 손쉽게 관리할 수 있습니다. 다음 작업과 명령을 설명합니다.

- `shutdown`
- `reboot`
- `suspend`
- 오프라인
- `resume`

- resetconfig
- version
- updateconfig
- upgrade

어플라이언스 종료 또는 재부팅

종료하거나 재부팅한 후 전송 큐의 메시지를 잃지 않고 나중에 어플라이언스를 다시 시작할 수 있습니다.

CLI에서 shutdown 또는 reboot 명령을 사용하거나 다음과 같은 GUI를 사용할 수 있습니다.

절차

1단계 **System Administration(시스템 관리) > Shutdown/Suspend(종료/일시 중단)**를 선택합니다.

2단계 **시스템 작업** 섹션의 **작업** 드롭다운 목록에서 **Shutdown(종료)** 또는 **Reboot(재부팅)**를 선택합니다.

3단계 열려 있는 연결이 종료되어 강제로 닫히기 전까지 대기할 시간(초)을 입력합니다.

기본 지연 시간은 30초입니다.

4단계 **Commit(커밋)**을 클릭합니다.

이메일 수신 및 전송 일시 중단

AsyncOS를 이용해 이메일의 수신 및 전송을 일시 중단할 수 있습니다. 다음을 일시 중단할 수 있습니다.

- 특정 리스너 또는 여러 리스너에서 이메일 수신
- 특정 도메인 또는 여러 도메인에 모든 이메일 또는 여러 이메일 전송

CLI에서 suspend 명령을 사용하거나 GUI를 사용합니다.

절차

1단계 **System Administration(시스템 관리) > Shutdown/Suspend(종료/일시 중단)**를 선택합니다.

2단계 특정 리스너 또는 여러 리스너의 이메일 수신 일시 중단

메일 작업 섹션에서 해당 기능 및/또는 일시 중단할 리스너를 선택합니다. 어플라이언스에 여러 리스너가 있는 경우 개별 리스너의 이메일 수신을 일시 중단할 수 있습니다.

3단계 특정 도메인 또는 여러 도메인에 모든 이메일 또는 여러 이메일 전송을 일시 중단합니다. 사용자의 요건에 따라 다음 중 하나를 수행합니다.

- 모든 이메일의 전송을 일시 중단하려면 **도메인/하위 도메인 지정** 필드에 ALL을 입력하고 **Enter**를 누릅니다.
- 특정 도메인 또는 하위 도메인에 이메일 전송을 일시 중단하려면 **도메인/하위 도메인 지정** 필드에 해당 도메인 또는 하위 도메인의 이름이나 IP 주소를 입력하고 **Enter**를 누릅니다. 여러 항목을 추가하려면 쉼표로 구분된 텍스트를 사용합니다.

4단계 열려 있는 연결이 종료되어 강제로 닫히기 전까지 대기할 시간(초)을 입력합니다.

열려 있는 연결이 없으면 시스템이 즉시 오프라인으로 전환됩니다.

기본 지연 시간은 30초입니다.

5단계 **Commit(커밋)**을 클릭합니다.

향후 작업

일시 중단된 서비스를 다시 시작할 준비가 된 경우 일시 중단된 이메일 수신 및 전송 다시 시작, 33-3 페이지를 참조하십시오.

일시 중단된 이메일 수신 및 전송 다시 시작

종료/일시 중단 페이지 또는 `resume` 명령을 사용하여 일시 중단된 이메일 수신 및 전송을 다시 시작할 수 있습니다.

절차

1단계 **System Administration(시스템 관리) > Shutdown/Suspend(종료/일시 중단)**를 선택합니다.

2단계 **메일 작업** 섹션에서 해당 기능 및/또는 다시 시작할 리스너를 선택합니다.

어플라이언스에 리스너가 여러 개인 경우 개별 리스너에서 이메일 수신을 다시 시작할 수 있습니다.

3단계 특정 도메인 또는 여러 도메인에 모든 이메일 또는 여러 이메일 전송을 다시 시작합니다.

도메인/하위 도메인 지정 필드에서 원하는 항목의 닫기 아이콘을 클릭합니다.

4단계 **Commit(커밋)**을 클릭합니다.

CLI를 사용하여 어플라이언스를 오프라인으로 전환

Cisco 지원팀에서 요구할 경우 Cisco IronPort AsyncOS를 오프라인 상태로 전환합니다.

시스템이 오프라인 상태인 경우:

- 인바운드 이메일 연결이 허용되지 않습니다.
- 아웃바운드 이메일 전송이 중단됩니다.
- 로그 전송이 중단됩니다.
- CLI에는 여전히 액세스할 수 있습니다.

절차

1단계 `offline` 명령을 사용합니다.

2단계 열려 있는 연결이 강제로 닫히기 전까지 대기할 시간(초)을 지정합니다.

공장 기본값으로 리셋

어플라이언스를 물리적으로 이동할 때 공장 기본값으로 시작할 수 있습니다. System Administration(시스템 관리) > Configuration File(구성 파일) 페이지의 구성 리셋 섹션에서 또는 resetconfig 명령을 사용하여 *모든* AsyncOS 구성 값을 공장 기본값으로 리셋합니다. 이 명령은 매우 파괴적이므로 장치를 운반하거나 마지막 수단으로 구성 문제를 해결할 때만 사용해야 합니다. 구성을 리셋한 후에 시스템 설정 마법사 또는 systemsetup 명령을 실행하는 것이 좋습니다.

참고 resetconfig 명령은 어플라이언스가 오프라인 상태일 경우에만 작동합니다. resetconfig 명령이 완료되면 systemsetup 명령을 다시 실행하기도 전에 어플라이언스가 온라인 상태로 돌아갑니다. 그러나 메일 전송이 다시 시작되지 않으므로 메일 전송을 다시 켜야 합니다.

주의 resetconfig 명령을 실행하면 모든 네트워크 설정이 공장 기본값으로 돌아가므로 잠재적으로 CLI에서 분리되고 어플라이언스에 연결하는 데 사용한 서비스(FTP, Telnet, SSH, HTTP, HTTPS)가 비활성화되며 심지어 userconfig 명령을 사용하여 생성한 추가 사용자 계정이 제거됩니다. 직렬 인터페이스를 사용하거나 기본 관리자 계정을 통해 관리 포트에서 기본 설정을 사용하여 CLI에 다시 연결할 수 없는 경우 이 명령을 사용하지 마십시오.

resetconfig 명령

```
mail3.example.com> offline


Delay (seconds, minimum 30):

[30]> 45


Waiting for listeners to exit...

Receiving suspended.

Waiting for outgoing deliveries to finish...

Mail delivery suspended.


mail3.example.com> resetconfig


Are you sure you want to reset all configuration values? [N]> Y


All settings have been restored to the factory default.
```

AsyncOS의 버전 정보 표시

어플라이언스에 현재 설치되어 있는 AsyncOS 버전을 확인하려면 GUI의 모니터 메뉴에 있는 시스템 개요 페이지(시스템 상태, 28-29페이지 참조)를 사용하거나 CLI에서 `version` 명령을 사용하십시오.

기능 키

기능 키 추가 및 관리

물리적 어플라이언스의 경우 기능 키는 어플라이언스의 일련 번호와 활성화할 기능에 고유합니다(한 시스템의 키를 다른 시스템에서 다시 사용할 수 없음).

CLI에서 기능 키를 사용하려면 `featurekey` 명령을 사용하십시오.

절차

1단계 **System Administration(시스템 관리) > Feature Keys(기능 키)**를 선택합니다.

2단계 다음 작업을 수행합니다.

변경 후	수행할 작업
활성 기능 키 상태 보기	**<serial number>의 기능 키** 섹션을 봅니다.
사용 중인 어플라이언스에 발급되었으나 아직 활성화되지 않은 기능 키 보기	**활성화 보류 중** 섹션을 봅니다. 자동 다운로드 및 활성화를 활성화한 경우 기능 키가 이 목록에 나타나지 않습니다.
최근에 발급된 기능 키 확인	활성화 보류 중 섹션의 **Check for New Keys(새 키 확인)** 버튼을 클릭합니다. 이 기능은 기능 키 자동 다운로드 및 활성화를 활성화하지 않았거나 다음 자동 확인 전에 기능 키를 다운로드해야 하는 경우에 유용합니다.
발급된 기능 키 활성화	**활성화 보류 중** 목록에서 키를 선택하고 **Activate Selected Keys(선택한 키 활성화)**를 클릭합니다.
새 기능 키 추가	**기능 활성화** 섹션을 사용합니다.

관련 주제

- 기능 키 다운로드 및 활성화 자동화, 33-6페이지
- Cisco Email Security Virtual Appliance 라이센스, 33-6페이지

기능 키 다운로드 및 활성화 자동화

이 어플라이언스에 발급된 기능 키를 자동으로 확인, 다운로드 및 활성화하도록 어플라이언스를 설정할 수 있습니다.

절차

1단계 **System Administration(시스템 관리) > Feature Key Settings(기능 키 설정)**를 선택합니다.

2단계 **Edit Feature Key Settings(기능 키 설정 편집)**를 클릭합니다.

3단계 새 기능 키의 확인 빈도를 보려면 (?) 도움말 버튼을 클릭합니다.

4단계 설정을 지정합니다.

5단계 변경 사항을 제출하고 커밋합니다.

관련 주제

- 기능 키 추가 및 관리, 33-5페이지

만료된 기능 키

GUI를 통해 액세스하려는 기능의 기능 키가 만료된 경우 Cisco 담당자 또는 지원 조직에 문의하십시오.

Cisco Email Security Virtual Appliance 라이센스

이메일 보안 가상 어플라이언스를 설정하고 라이센스를 취득하려면 *Cisco Content Security Virtual Appliance 설치 설명서*를 참조하십시오. 이 문서는 문서, 1-7페이지에 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 후에도 180일 동안은 보안 서비스 없이 어플라이언스가 계속해서 메일을 전송합니다. 이 기간에는 보안 서비스 업데이트가 수행되지 않습니다.

경고는 라이센스가 만료되기 180일, 150일, 120일, 90일, 60일, 30일, 15일, 5일, 1일 및 0초 전에 그리고 유예 기간 종료 전과 동일한 간격으로 전송됩니다. 이러한 경고의 유형은 "시스템"이며 심각도는 "위험"입니다. 이러한 경고를 받으려면 알림 수신자 추가, 33-35페이지를 참조하십시오.

이러한 경고는 시스템 로그에도 기록됩니다.

개별 기능 키가 가상 어플라이언스 라이센스보다 먼저 만료될 수 있습니다. 이러한 기능 키의 만료일이 다가오는 경우에도 경고를 수신하게 됩니다.

관련 주제

- 가상 어플라이언스에서 AsyncOS를 되돌리면 라이센스에 영향을 미칠 수 있음, 33-30페이지

구성 파일 관리

어플라이언스 내의 모든 구성 설정은 단일 구성 파일을 통해 관리할 수 있습니다. 파일은 XML(Extensible Markup Language) 형식으로 유지됩니다.

다음과 같은 여러 방법으로 이 파일을 사용할 수 있습니다.

- 구성 파일을 다른 시스템에 저장하여 중요한 구성 파일을 백업하고 유지할 수 있습니다. 어플라이언스 구성 도중 실수한 경우 가장 최근에 저장된 구성 파일로 "롤백"할 수 있습니다.
- 기존 구성 파일을 다운로드하여 어플라이언스의 전체 구성을 빠르게 볼 수 있습니다. (많은 최신 브라우저에는 XML 파일을 직접 렌더링할 수 있는 기능이 포함되어 있습니다.) 이 기능은 현재 구성에 있을 수 있는 사소한 오류(오타 등)를 해결할 수 있습니다.
- 기존 구성 파일을 다운로드하고 내용을 변경하고 동일한 어플라이언스에 업로드할 수 있습니다. 이 기능은 구성을 변경할 수 있도록 사실상 CLI와 GUI를 모두 "우회"합니다.
- FTP 액세스를 통해 전체 구성 파일을 업로드하거나 구성 파일의 일부 또는 전부를 CLI에 직접 붙여 넣을 수 있습니다.
- 파일이 XML 형식이므로 구성 파일의 모든 XML 엔터티를 설명하는 관련 DTD(문서 형식 정의)도 제공됩니다. DTD를 다운로드하려 XML 구성 파일을 업로드하기 전에 검증할 수 있습니다. (XML 검증 툴은 인터넷에서 바로 사용할 수 있습니다.)

XML 구성 파일로 여러 어플라이언스 관리

- 한 어플라이언스에서 기존 구성 파일을 다운로드해서 변경한 후 다른 어플라이언스에 업로드할 수 있습니다. 따라서 여러 어플라이언스의 설치를 더 쉽게 관리할 수 있습니다. 현재 C/X-Series 어플라이언스에서 M-Series 어플라이언스로 구성 파일을 로드할 수 없습니다.
- 어플라이언스에서 다운로드한 기존 구성 파일을 여러 개의 하위 섹션으로 나눌 수 있습니다. 모든 어플라이언스에서 공통인 그러한 섹션을 수정하고(여러 어플라이언스 환경에서) 하위 섹션을 업데이트할 때 다른 어플라이언스에 로드할 수 있습니다.

  예를 들어, 테스트 환경에서 어플라이언스를 사용하여 Global Unsubscribe 명령을 테스트할 수 있습니다. 전역 구독 취소 목록을 적절하게 구성했다고 생각할 경우 테스트 어플라이언스에서 모든 프로덕션 어플라이언스에 전역 구독 취소 구성을 로드할 수 있습니다.

GUI를 사용하여 구성 파일 관리

GUI를 사용하여 어플라이언스에서 구성 파일을 관리하려면 System Administration(시스템 관리) 탭의 Configuration File(구성 파일) 링크를 클릭합니다.

구성 파일 페이지에는 다음과 같은 섹션이 포함되어 있습니다.

- **현재 구성** - 현재 구성 파일을 저장하고 내보내는 데 사용됩니다.
- **구성 로드** - 전체 또는 부분 구성 파일을 로드하는 데 사용됩니다.
- **최종 사용자 허용 목록/차단 목록 데이터베이스(스팸 격리)** - 관련 내용은 발신자를 기준으로 이메일 전송을 제어하는 허용 목록 및 차단 목록 사용, 31-6페이지 및 허용 목록/차단 목록 백업 및 복원, 31-12페이지를 참조하십시오.
- **구성 리셋** - 현재 구성을 공장 기본값으로 리셋하는 데 사용됩니다(리셋하기 전에 구성을 저장해야 함).

현재 구성 파일 저장 및 내보내기

System Administratio(시스템 관리) > Configuration File(구성 파일) 페이지의 **현재 구성** 섹션을 사용하여 현재 구성 파일을 로컬 머신과 어플라이언스(FTP/SCP 루트의 `configuration` 디렉토리에 있음)에 저장하거나 지정된 이메일 주소로 보낼 수 있습니다.

다음 정보는 구성 파일과 함께 저장되지 않습니다.

- URL 필터링 기능에 사용되는 서비스와의 보안 통신에 사용되는 인증서
- 연락처 기술 지원 페이지에 저장된 CCO 사용자 ID 및 계약 ID

Mask passwords in the Configuration Files(구성 파일의 비밀번호 마스크 처리) 확인란을 클릭하여 사용자의 비밀번호를 마스크 처리할 수 있습니다. 비밀번호를 마스크 처리하면 내보내거나 저장한 파일의 암호화된 원래 비밀번호가 "*****"로 바뀝니다. 그러나 비밀번호가 마스크 처리된 구성 파일을 AsyncOS로 다시 로드할 수 없습니다.

Encrypt passwords in the Configuration Files(구성 파일의 비밀번호 암호화) 확인란을 클릭하여 사용자의 비밀번호를 암호화할 수 있습니다. 다음은 암호화할 구성 파일의 중요한 보안 매개변수입니다.

- 인증서 개인 키
- RADIUS 비밀번호
- LDAP 바인딩 비밀번호
- 로컬 사용자의 비밀번호 해시
- SNMP 비밀번호
- DK/DKIM 서명 키
- 발송 SMTP 인증 비밀번호
- PostX 암호화 키
- PostX 암호화 프록시 비밀번호
- FTP 푸시 로그 구독 비밀번호
- IPMI LAN 비밀번호
- 업데이트 프로그램 서버 URL

참고 보안이 강화되면 어플라이언스의 민감한 데이터의 암호화가 FIPS 모드에서 활성화된 경우 **Plain passwords in the Configuration Files(구성 파일의 일반 비밀번호)** 옵션이 웹 인터페이스에 표시되지 않습니다.

구성 파일 로드

System Administration(시스템 관리) > Configuration File(구성 파일) 페이지의 구성 로드 섹션을 사용하여 새 구성 정보를 어플라이언스에 로드할 수 있습니다. 다음 세 가지 방법 중 하나를 사용하여 정보를 로드할 수 있습니다.

- `configuration` 디렉토리에 정보를 배치해서 업로드
- 로컬 머신에서 직접 구성 파일 업로드
- GUI에 직접 구성 정보 붙여 넣기

비밀번호가 마스크 처리된 구성 파일은 로드할 수 없습니다.

참고 클러스터 모드에서는 클러스터 또는 어플라이언스의 구성을 로드할 수 있습니다. 클러스터 구성 로드에 대한 지침은 클러스터된 어플라이언스에 구성 로드, 39-23페이지를 참조하십시오.

방법에 관계없이 구성 상단에 다음과 같은 태그를 포함해야 합니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

 ... your configuration information in valid XML

</config>
```

닫는 `</config>` 태그는 구성 정보를 따라야 합니다. XML 구문의 값은 DTD(문서 형식 정의)(어플라이언스의 `configuration` 디렉토리에 위치)를 기준으로 구문 분석 및 검증됩니다. DTD 파일 이름이 `config.dtd`로 지정됩니다. `loadconfig` 명령을 사용할 때 명령줄에서 검증 오류가 보고되면 변경 사항이 로드되지 않습니다. 구성 파일을 업로드하기 전에 DTD를 다운로드하여 어플라이언스 밖의 구성 파일을 검증할 수 있습니다.

어떤 방법을 사용하든 전체 구성 파일(최상위 태그인 `<config></config>` 사이에 정의된 정보) 또는 구성 파일의 *완료* 및 *고유* 하위 섹션을 가져올 수 있습니다. 단, 선언 태그(위)를 포함하고 `<config></config>` 태그 안에 포함되어야 합니다.

"완료"란 DTD에서 정의된 대로 주어진 하위 섹션의 전체 시작 및 끝 태그가 포함되어 있음을 의미합니다. 예를 들어,

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

  <autosupport_enabled>0</autosu

</config>
```

태그를 업로드하거나 붙여 넣으면 업로드할 때 검증 오류가 발생합니다. 그러나

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

  <autosupport_enabled>0</autosupport_enabled>

</config>
```

태그는 검증 오류를 유발하지 않습니다.

"고유"는 업로드하거나 붙여 넣을 구성 파일의 하위 섹션이 구성에 대해 모호하지 않음을 의미합니다. 예를 들어, 시스템에 하나의 호스트 이름만 있어야 하므로 다음 태그(선언 및 `<config></config>` 태그 포함)

```
<hostname>mail4.example.com</hostname>
```

이 허용됩니다. 그러나 시스템에서 Recipient Access Table을 각기 다르게 정의하여 여러 개의 리스너를 정의할 수 있으므로

```
<rat>
   <rat_entry>
     <rat_address>ALL</rat_address>
     <access>RELAY</access>
   </rat_entry>
 </rat>
```

태그는 "완전한" 구문이라 해도 모호하다고 간주되어 허용되지 않습니다.

주의 구성 파일 또는 구성 파일의 하위 섹션을 업로드하거나 붙여 넣으면 보류될 수 있는 커밋되지 않은 변경 사항이 지워질 수 있습니다.

주의 구성 파일의 디스크 공간 할당이 현재 어플라이언스에 저장된 데이터의 양보다 작은 경우 구성 파일에 지정된 할당량을 충족하기 위해 가장 오래된 데이터가 삭제됩니다.

빈 태그 및 생략된 태그

구성 파일의 섹션을 업로드하거나 붙여 넣을 때 주의를 기울이십시오. 태그를 포함하지 않은 경우 구성 파일을 로드할 때 구성의 해당 값이 수정되지 않습니다. 그러나 빈 태그를 포함할 경우 해당 구성 설정이 지워집니다.

예를 들어,

```
<listeners></listeners>
```

태그를 업로드하면 시스템의 모든 리스너가 제거됩니다!

주의 구성 파일의 하위 섹션을 업로드하거나 붙여 넣을 때 GUI에서 또는 CLI에서 분리되고 대량의 구성 데이터가 삭제될 수 있습니다. 다른 프로토콜, 직렬 인터페이스 또는 관리 포트의 기본 설정을 사용하여 어플라이언스에 연결할 수 없는 경우 이 명령을 사용하여 서비스를 비활성화하지 마십시오. 또한 DTD에 정의된 정확한 구성 구문을 잘 모를 경우 이 명령을 사용하지 마십시오. 새 구성 파일을 로드하기 전에 항상 구성 데이터 파일을 백업하십시오.

로그 구독을 위한 비밀번호 로드에 대한 참고사항

비밀번호가 필요한 로그 구독(예: FTP 푸시 사용)이 포함된 구성 파일을 로드하려고 시도할 경우 `loadconfig` 명령이 비밀번호 누락에 대해 경고하지 않습니다. FTP 푸시가 실패하고 `logconfig` 명령을 사용하여 올바른 비밀번호를 구성할 때까지 경고가 생성됩니다.

문자 집합 인코딩에 대한 참고사항

오프라인으로 파일을 조작하는 데 사용할 수 있는 문자 집합에 관계없이 XML 구성 파일의 "인코딩" 특성이 "`ISO-8859-1`"이어야 합니다. `showconfig`, `saveconfig` 또는 `mailconfig` 명령을 실행할 때마다 파일에 다음 인코딩 특성이 지정되어 있는지 확인해야 합니다.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

현재 이 인코딩이 있는 구성 파일만 로드할 수 있습니다.

현재 구성 리셋

현재 구성을 리셋하면 어플라이언스가 원래 공장 기본값으로 되돌아갑니다. 리셋하기 전에 구성을 저장해야 합니다. GUI의 이 버튼을 통해 구성을 리셋하는 기능은 클러스터링 환경에서 지원되지 않습니다.

공장 기본값으로 리셋, 33-4페이지를 참조하십시오.

구성 파일에 대한 CLI 명령

다음과 같은 명령을 사용하여 구성 파일을 조작할 수 있습니다.

- `showconfig`
- `mailconfig`
- `saveconfig`
- `loadconfig`
- `resetconfig`(공장 기본값으로 리셋, 33-4페이지 참조)

showconfig, mailconfig 및 saveconfig 명령

구성 파일 명령 `showconfig`, `mailconfig` 및 `saveconfig`의 경우 메일로 보내거나 표시할 파일에 비밀번호를 포함할지 선택하라는 메시지가 표시됩니다. 비밀번호를 포함하지 않기로 선택할 경우 비밀번호 필드를 비워 둡니다. 보안 위협이 염려된다면 비밀번호를 포함하지 않기로 선택할 수 있습니다. 그러나 비밀번호가 없는 구성 파일은 `loadconfig` 명령을 사용하여 로드할 때 실패하게 됩니다. 로그 구독을 위한 비밀번호 로드에 대한 참고사항, 33-11페이지를 참조하십시오.

참고 비밀번호를 포함하기로 선택할 경우("Do you want to include passwords?"에 예라고 답함) 구성 파일을 저장하거나 표시하거나 메일로 보낼 때 비밀번호가 암호화됩니다. 그러나 개인 키와 인증서는 암호화되지 않은 PEM 형식으로 포함됩니다.

showconfig 명령을 실행하면 현재 구성이 화면에 인쇄됩니다.

```
mail3.example.com> showconfig


Do you want to include passwords? Please be aware that a configuration without passwords
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.]
```

mailconfig 명령을 사용하여 현재 구성을 사용자에게 이메일로 전송합니다. XML 형식의 구성 파일(이름 config.xml)이 메시지에 첨부됩니다.

```
mail3.example.com> mailconfig


Please enter the email address to which you want to send

the configuration file.

[]> administrator@example.com


Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.  [N]> y


The configuration file has been sent to administrator@example.com.
```

Saveconfig 명령을 실행하면 구성 파일을 고유한 파일 이름으로 어플라이언스의 configuration 디렉토리에 저장할 수 있습니다.

```
mail3.example.com> saveconfig


Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.  [N]> y


File written on machine "mail3.example.com" to the location
"/configuration/C360-420E874BB4B3C41C5C71-1419B58528A0-20120105T214041.xml".
Configuration saved.


mail3.example.com>
```

loadconfig 명령

loadconfig를 사용하여 새 구성 정보를 어플라이언스에 로드할 수 있습니다. 다음 두 가지 방법 중 하나를 사용하여 정보를 로드할 수 있습니다.

- configuration 디렉토리에 정보를 배치해서 업로드
- CLI에 직접 구성 정보 붙여 넣기

자세한 내용은 구성 파일 로드, 33-8페이지를 참조하십시오.

CLI를 사용하여 구성 변경 사항 업로드

절차

1단계 CLI 외부에서 어플라이언스의 configuration 디렉토리에 액세스할 수 있는지 확인합니다. 자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스"를 참조하십시오.

2단계 어플라이언스의 configuration 디렉토리에 전체 구성 파일 또는 구성 파일의 하위 섹션을 배치하거나 saveconfig 명령을 사용하여 생성한 기존 구성을 편집합니다.

3단계 CLI 내에서 loadconfig 명령을 사용하여 2단계에서 디렉토리에 배치한 구성 파일을 로드하거나 텍스트(XML 구문)를 CLI에 직접 붙여 넣습니다.

이 예제에서는 이름이 changed.config.xml인 파일을 업로드하고 변경 사항을 커밋합니다.

```
mail3.example.com> loadconfig


1. Paste via CLI

2. Load from file

[1]> 2
```

```
Enter the name of the file to import:

[]> changed.config.xml


Values have been loaded.

Be sure to run "commit" to make these settings active.
```

이 예제에서는 새 구성 파일을 명령줄에 직접 붙여 넣습니다. (붙여 넣기 명령을 종료하려면 빈 행에 Control-D를 입력해야 합니다.) 그런 다음 시스템 설정 마법사를 사용하여 기본 호스트 이름, IP 주소, 기본 게이트웨이 정보를 변경합니다. (자세한 내용은 시스템 설정 마법사 사용, 3-13페이지를 참조하십시오.) 마지막으로 변경 사항을 커밋합니다.

```
mail3.example.com> loadconfig


1. Paste via CLI

2. Load from file

[1]> 1


Paste the configuration file now. Press CTRL-D on a blank line when done.


[The configuration file is pasted until the end tag </config>. Control-D is entered on a
separate line.]


Values have been loaded.

Be sure to run "commit" to make these settings active.

mail3.example.com> systemsetup


[The system setup wizard is run.]


mail3.example.com> commit


Please enter some comments describing your changes:
```

```
[]> pasted new configuration file and changed default settings via
systemsetup


Do you want to save the current configuration for rollback? [Y]> n

Changes committed: Fri May 23 11:42:12 2014 GMT
```

디스크 공간 관리

(가상 어플라이언스만 해당) 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 2TB로 제한됩니다.

가상 어플라이언스 인스턴스에 디스크 공간을 추가하려면 다음을 수행합니다.

참고 ESX는 디스크 공간 줄이기를 지원하지 않습니다. 관련 내용은 VMWare 설명서를 참조하십시오.

시작하기 전에

늘려야 할 디스크 공간을 신중하게 결정합니다.

1단계 인스턴스를Email Security 어플라이언스 종료합니다.

2단계 VMWare에서 제공하는 관리 툴 또는 유틸리티를 사용하여 디스크 공간을 늘립니다.

VMWare 설명서의 가상 디스크 구성 변경에 대한 정보를 참조하십시오. 릴리스 시 ESXi 5.5에 대한 이 정보가 여기에서 제공되었습니다.
http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html.

3단계 **System Administration(시스템 관리) > Disk Management(디스크 관리)**로 이동하여 변경 사항이 적용되었는지 확인합니다.

디스크 공간 할당량 할당

배포 시 사용하는 기능 중 하나로 어플라이언스에 디스크 공간을 할당하여 디스크 공간을 최적화할 수 있습니다.

변경 후	수행할 작업
• 디스크 공간 할당량과 각 서비스의 현재 사용량 보기 • 언제든지 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 신종 바이러스 격리의 경우 격리에 구성된 기본 작업이 수행됩니다. 자동으로 처리된 격리 메시지에 대한 기본 작업, 30-4페이지를 참조하십시오. • 기타 할당량의 경우 먼저 데이터를 수동으로 삭제하여 사용량을 설정할 새 할당량 아래로 줄여야 합니다. 기타 할당량의 디스크 공간 관리, 33-16페이지를 참조하십시오.

기타 할당량의 디스크 공간 관리

기타 할당량에는 시스템 데이터와 사용자 데이터가 포함됩니다. 시스템 데이터는 삭제할 수 없습니다. 관리할 수 있는 사용자 데이터에는 다음과 같은 유형의 파일이 포함됩니다.

관리 하려면	수행할 작업
로그 파일	**System Administration(시스템 관리) > Log Subscriptions(로그 구독)**로 이동하여 다음을 수행합니다. • 가장 많은 디스크 공간을 사용하는 로그 디렉토리를 확인합니다. • 생성할 모든 로그 구독이 필요한지 확인합니다. • 로그 수준이 필요한 것보다 더 높지 않은지 확인합니다. • 실행 가능한 경우 롤오버 파일 크기를 줄입니다.
패킷 캡처	**Help and Support(도움말 및 지원)**(화면의 오른쪽 위 근처) > **Packet Capture(패킷 캡처)**로 이동합니다.
구성 파일 (이러한 파일은 디스크 공간을 많이 사용할 가능성이 없습니다.)	어플라이언스의 `/data/pub` 디렉토리에 대한 FTP 액세스. 어플라이언스에 대한 FTP 액세스를 구성하려면 부록 A, "FTP, SSH, SCP 및 텔넷 액세스"를 참조하십시오.
할당량 크기	**System Administration(시스템 관리) > Disk Management(디스크 관리)**로 이동합니다.

디스크 공간에 대한 경고 수신 확인

기타 디스크 사용량이 할당량의 75%에 도달하면 경고 수준에서 시스템 경고 수신을 시작하게 됩니다. 이러한 경고를 수신하면 작업을 수행해야 합니다.

이러한 경고를 받으려면 알림 수신자 추가, 33-35페이지를 참조하십시오.

디스크 공간 및 중앙 집중식 관리

디스크 공간 관리는 그룹 또는 클러스터 모드가 아닌 머신 모드에서만 사용할 수 있습니다.

서비스 업데이트

다음과 같은 서비스를 최대한 효과적으로 사용하려면 업데이트가 필요합니다.

- 기능 키
- McAfee Anti-Virus 정의
- PXE 엔진
- Sophos Anti-Virus 정의
- IronPort 안티스팸 규칙
- 신종 바이러스 필터(Outbreak Filter) 규칙
- 표준 시간대 규칙
- URL 범주(URL 필터링 기능에 사용됩니다. 자세한 내용은 향후 URL 범주 집합 변경, 15-21페이지)를 참조하십시오
- 등록 클라이언트(URL 필터링 기능에 사용된 클라우드 기반 서비스와의 통신에 필요한 인증서를 업데이트하는 데 사용됩니다. 관련 내용은 Cisco Web Security Services에 대한 연결 정보, 15-3페이지를 참조하십시오.)

참고 RSA 이메일 DLP 엔진 및 콘텐츠 일치 분류자의 설정은 **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)** 페이지에서 처리됩니다. 자세한 내용은 DLP 엔진 및 콘텐츠 일치 분류자 업데이트 정보, 17-37페이지를 참조하십시오.

서비스 업데이트 설정은 DLP 업데이트를 제외한 업데이트를 수신하는 모든 서비스에 사용됩니다. DLP 업데이트를 제외한 모든 개별 서비스에 고유한 설정을 지정할 수 없습니다.

이러한 중요한 업데이트를 가져오도록 네트워크와 어플라이언스를 설정하려면 업그레이드 및 업데이트를 가져오도록 설정, 33-17페이지를 참조하십시오.

업그레이드 및 업데이트를 가져오도록 설정

- 업데이트 서버 인증서의 유효성을 확인하도록 어플라이언스 구성, 33-23페이지
- 신뢰할 수 있는 프록시 서버 통신을 수행하도록 어플라이언스 구성, 33-24페이지

업그레이드 및 업데이트 배포 옵션

다음은 AsyncOS 업그레이드 및 업데이트 파일을 어플라이언스에 배포하는 몇 가지 방법입니다.

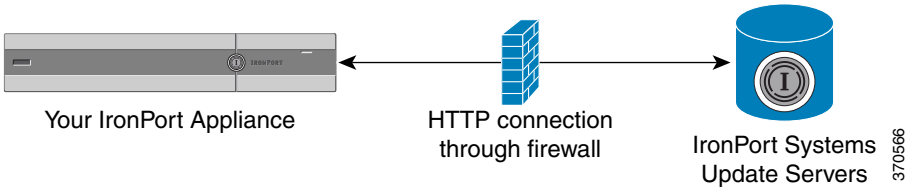
- 각 어플라이언스가 Cisco 업데이트 서버에서 직접 파일을 다운로드할 수 있습니다. 이는 기본적으로 사용되는 방법입니다.
- Cisco에서 파일을 다운로드한 다음 네트워크 내의 서버에서 어플라이언스에 배포할 수 있습니다. 로컬 서버에서 업그레이드 및 업데이트, 33-19페이지를 참조하십시오.

방법을 선택하고 구성하려면 업그레이드 및 업데이트를 다운로드하도록 서버 설정 구성, 33-21페이지를 참조하십시오.

Cisco 서버에서 업그레이드 및 업데이트를 다운로드하도록 네트워크 구성

어플라이언스가 Cisco 업데이트 서버에 직접 연결하여 업그레이드 및 업데이트를 찾아서 다운로드합니다.

그림 33-1 스트리밍 업데이트 방법



Cisco 업데이트 서버는 동적 IP 주소를 사용합니다. 엄격한 방화벽 정책이 있는 경우 그 대신 정적 위치를 구성해야 할 수 있습니다. 자세한 내용은 엄격한 방화벽 환경에서 업그레이드 및 업데이트를 다운로드하도록 어플라이언스 구성, 33-18페이지를 참고하십시오.

Cisco 포트 80과 443의 업데이트 서버에서 업그레이드를 다운로드할 수 있도록 허용하는 방화벽 규칙을 생성합니다.

엄격한 방화벽 환경에서 업그레이드 및 업데이트를 다운로드하도록 어플라이언스 구성

Cisco IronPort 업그레이드 및 업데이트 서버는 동적 IP 주소를 사용합니다. 엄격한 방화벽 정책이 있는 경우 업데이트 및 AsyncOS 업그레이드를 위한 정적 위치를 구성해야 할 수 있습니다.

절차

1단계 정적 URL 주소를 가져오려면 Cisco 고객 지원팀에 문의하십시오.

2단계 포트 80의 정적 IP 주소에서 업그레이드 및 업데이트를 다운로드할 수 있도록 허용하는 방화벽 규칙을 생성합니다.

3단계 **Security Services(보안 서비스) > Service Updates(서비스 업데이트)**를 선택합니다.

4단계 **Edit Update Settings(업데이트 설정 편집)**를 클릭합니다.

5단계 업데이트 설정 편집 페이지의 "업데이트 서버(이미지)" 섹션에서 Local Update Servers(로컬 업데이트 서버)를 선택하고 AsyncOS 업그레이드 및 McAfee 안티바이러스 정의의 기본 URL 필드에 1단계에서 수신한 정적 URL을 입력합니다.

6단계 "업데이트 서버(목록)" 섹션에 대해 IronPort Update Servers가 선택되었는지 확인합니다.

7단계 변경 사항을 제출하고 커밋합니다.

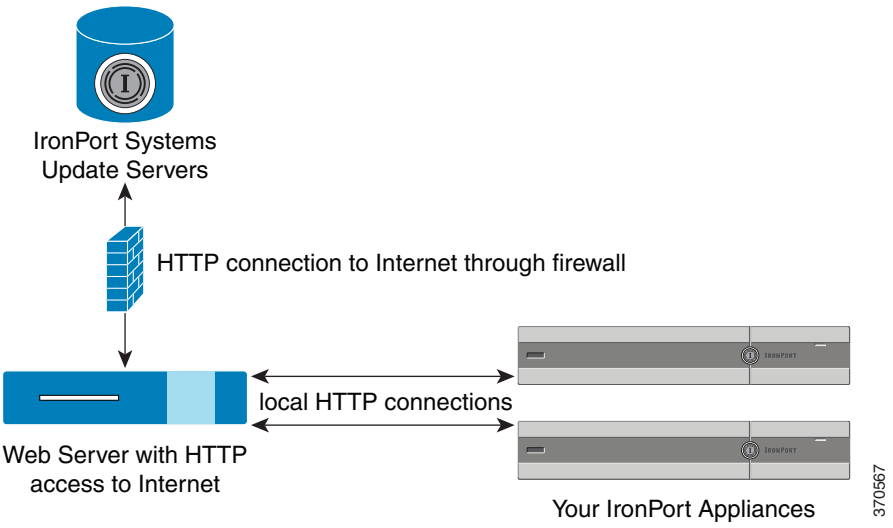
로컬 서버에서 업그레이드 및 업데이트

Cisco의 업데이트 서버에서 직접 업그레이드를 가져오지 않고 AsyncOS 업그레이드 이미지를 로컬 서버에 다운로드하고 자체 네트워크 내에서 업그레이드를 호스팅할 수 있습니다. 이 기능을 사용하여 HTTP를 통해 업그레이드 이미지를 인터넷에 액세스한 네트워크의 서버에 다운로드할 수 있습니다. 업그레이드 이미지 다운로드를 선택한 경우 AsyncOS 이미지를 어플라이언스에 호스팅하도록 내부 HTTP 서버("업데이트 관리자")를 구성할 수 있습니다.

어플라이언스에 인터넷 액세스 권한이 없거나 조직에서 다운로드에 사용되는 사이트를 미러링하기 위한 액세스를 제한할 경우 로컬 서버를 사용하십시오. 로컬 서버에서 각 어플라이언스로 AsyncOS 업그레이드를 다운로드하는 것은 일반적으로 Cisco IronPort 서버에서 다운로드하는 것보다 빠릅니다.

참고 Cisco에서는 AsyncOS 업그레이드에만 로컬 서버를 사용할 것을 권장합니다. 보안 업데이트 이미지에 로컬 업데이트 서버를 사용할 경우 로컬 서버가 Cisco IronPort에서 자동으로 보안 업데이트를 수신하지 않으므로 네트워크의 어플라이언스가 항상 최신 보안 서비스를 사용하지 못할 수 있습니다.

그림 33-2 원격 업데이트 방법



절차

1단계 업그레이드 파일을 검색해서 서비스하도록 로컬 서버를 구성합니다.

2단계 업그레이드 파일을 다운로드합니다.

3단계 GUI의 Security Services(보안 서비스) > Service Updates(서비스 업데이트) 페이지를 사용하거나 CLI에서 `updateconfig` 명령을 사용하여 로컬 서버를 사용하도록 어플라이언스를 구성합니다.

4단계 System Administration(시스템 관리) > System Upgrade(시스템 업그레이드) 페이지를 사용하거나 CLI에서 `upgrade` 명령을 사용하여 어플라이언스를 업그레이드합니다.

로컬 서버에서 업그레이드 및 업데이트하기 위한 하드웨어 및 소프트웨어 요건

AsyncOS 업그레이드 및 업데이트 파일을 *다운로드*하려면 내부 네트워크에 다음을 가진 시스템이 있어야 합니다.

- Cisco Systems 업데이트 서버에 대한 인터넷 액세스 권한
- 웹 브라우저(브라우저 요구 사항, 2-1페이지 참조)

참고 이 릴리스의 경우 이 주소에 대한 HTTP 액세스를 허용하도록 방화벽 설정을 구성해야 한다면 특정 IP 주소가 아닌 DNS 이름을 사용하여 구성해야 합니다.

AsyncOS 업데이트 파일을 *호스팅*하려면 내부 네트워크에 다음을 가진 서버가 있어야 합니다.

- 다음 조건을 충족하는 웹 서버(예: Microsoft IIS(Internet Information Services) 또는 Apache 오픈 소스 서버):
  - 24자를 초과하는 파일 이름 또는 디렉토리 표시 지원
  - 디렉토리 탐색이 활성화됨
  - 익명(인증 없음) 또는 기본("단순") 인증으로 구성됨
  - 각 AsyncOS 업데이트 이미지에 대해 최소한 350MB의 여유 디스크 공간을 포함함

로컬 서버에서 업그레이드 이미지 호스팅

로컬 서버를 설정한 후 `http://updates.ironport.com/fetch_manifest.html`로 이동하여 업그레이드 이미지의 ZIP 파일을 다운로드합니다. 이미지를 다운로드하려면 일련 번호(물리적 어플라이언스의 경우) 또는 VLN(가상 어플라이언스의 경우)과 어플라이언스의 버전 번호를 입력합니다. 그러면 사용 가능한 업그레이드 목록이 표시됩니다. 다운로드할 업그레이드 버전을 클릭하고 디렉토리 구조를 그대로 유지하고 로컬 서버의 루트 디렉토리에 ZIP 파일의 압축을 풉니다. 업그레이드 이미지를 사용하려면 업데이트 설정 페이지에서(또는 CLI에서 `updateconfig` 사용) 로컬 서버를 사용하도록 어플라이언스를 구성합니다.

또한 로컬 서버는 네트워크의 어플라이언스에 사용 가능한 AsyncOS 업그레이드를 다운로드된 업그레이드 이미지로 제한하는 XML 파일을 호스팅합니다. 이 파일을 "매니페스트"라고 합니다. 매니페스트는 업그레이드 이미지 ZIP 파일의 `asyncos` 디렉토리에 있습니다. 로컬 서버의 루트 디렉토리에 ZIP 파일의 압축을 푼 후에 업데이트 설정 편집 페이지에(또는 CLI에서 `updateconfig` 사용) 파일 이름을 포함한 XML 파일의 전체 URL을 입력합니다.

원격 업그레이드에 대한 자세한 내용은 가술 자료를 참조하거나 Cisco 지원 공급자에게 문의하십시오.

프록시 서버를 통합 업데이트

어플라이언스가 Cisco의 업데이트 서버에 직접 연결하여 업데이트를 수신하도록 구성됩니다(기본 구성). 이 연결은 포트 80의 HTTP를 통해 구성되며 콘텐츠가 암호화됩니다. 방화벽에서 이 포트를 열지 않으려면 프록시 서버와 어플라이언스가 업데이트된 규칙을 수신할 수 있는 특정 포트를 정의합니다.

프록시 서버를 사용하도록 선택할 경우 옵션 인증 및 포트를 지정할 수 있습니다.

참고 프록시 서버를 정의하면 프록시 서버를 사용하도록 구성된 모든 서비스 업데이트에 *자동으로* 사용됩니다. 개별 서비스의 업데이트에 프록시 서버를 사용하지 않게 할 수 있는 방법은 없습니다.

업그레이드 및 업데이트를 다운로드하도록 서버 설정 구성

어플라이언스에 업그레이드 및 업데이트를 다운로드하는 데 필요한 서버 및 연결 정보를 지정합니다.

AsyncOS 업그레이드와 서비스 업데이트에 동일하거나 다른 설정을 사용할 수 있습니다.

시작하기 전에

어플라이언스가 Cisco에서 직접 업그레이드 및 업데이트를 다운로드할지, 아니면 네트워크의 로컬 서버에서 이러한 이미지를 호스팅할지 결정합니다. 그런 다음 선택한 방법을 지원하도록 네트워크를 설정합니다. 업그레이드 및 업데이트를 가져오도록 설정, 33-17페이지의 모든 항목을 참조하십시오.

절차

1단계 **Security Services(보안 서비스) > Service Updates(서비스 업데이트)**를 선택합니다.

2단계 **Edit Update Settings(업데이트 설정 편집)**를 클릭합니다.

3단계 옵션을 입력합니다.

설정	설명
업데이트 서버(이미지)	Cisco IronPort AsyncOS 업그레이드 이미지 및 서비스 업데이트를 Cisco IronPort 업데이트 서버에서 다운로드할지 아니면 네트워크의 로컬 서버에서 다운로드할지 선택합니다. 업그레이드 및 업데이트 기본 서버는 Cisco IronPort 업데이트 서버입니다. 업그레이드 및 업데이트에 동일한 설정을 사용하려면 표시 필드에 정보를 입력합니다. 로컬 업데이트 서버를 선택할 경우 업그레이드 및 업데이트를 다운로드하는 데 사용할 서버의 기본 URL과 포트 번호를 입력합니다. 서버에 인증이 필요한 경우 올바른 사용자 이름과 비밀번호도 입력할 수 있습니다. AsyncOS 업그레이드 및 McAfee 안티바이러스 정의에 고유한 별도의 설정을 입력하려면 **Click to use different settings for AsyncOS(다른 AsyncOS 설정을 사용하려면 클릭)** 링크를 클릭합니다. **참고** Cisco Intelligent Multi-Scan은 두 번째 로컬 서버가 있어야만 타사 안티스팸 규칙을 다운로드할 수 있습니다.
업데이트 서버(목록)	각 어플라이언스가 해당 배포에만 적합한 업그레이드 및 업데이트를 사용할 수 있도록 Cisco IronPort는 관련 파일의 매니페스트 목록을 생성합니다. 사용 가능한 업그레이드 및 서비스 업데이트(매니페스트 XML 파일)의 목록을 Cisco IronPort 업데이트 서버에서 다운로드할지 아니면 네트워크의 로컬 서버에서 다운로드할지 선택합니다. 업데이트 및 AsyncOS 업그레이드용 서버를 지정하는 별도의 섹션이 있습니다. 업그레이드 및 업데이트 기본 서버는 Cisco IronPort 업데이트 서버입니다. 로컬 업데이트 서버를 선택할 경우 서버의 HTTP 포트 번호 및 파일 이름을 포함하여 각 목록의 매니페이스트 XML 파일에 대한 전체 경로를 입력합니다. 포트 필드를 비워 두면 AsyncOS가 포트 80을 사용합니다. 서버에 인증이 필요한 경우에 올바른 사용자 이름과 비밀번호를 입력합니다.
자동 업데이트	자동 업데이트 및 업데이트 간격(어플라이언스가 업데이틀 확인하는 빈도)을 Sophos 및 McAfee Anti-Virus 정의, Cisco 안티스팸 규칙, Cisco Intelligent Multi-Scan 규칙, PXE Engine 업데이트, 신종 바이러스 필터(Outbreak Filter) 규칙, 표준 시간대 규칙에 대해 활성화합니다. 초, 분 또는 시간을 나타내는 후행 s, m 또는 h를 포함합니다. 자동 업데이트를 비활성화하려면 0을 입력합니다. **참고** **Security Services(보안 서비스) > RSA Email DLP(RSA 이메일 DLP)** 페이지를 사용해야만 DLP에 대한 자동 업데이트를 켤 수 있습니다. 그러나 먼저 모든 서비스에 대해 자동 업데이트를 활성화해야 합니다. 자세한 내용은 DLP 엔진 및 콘텐츠 일치 분류자 업데이트 정보, 17-37페이지를 참조하십시오.
인터페이스	나열된 보안 구성 요소 업데이트의 업데이트 서버에 연결하는 데 사용할 네트워크 인터페이스를 선택합니다. 사용 가능한 프록시 데이터 인터페이스가 표시됩니다. 기본적으로 어플라이언스가 사용할 인터페이스를 선택합니다.

설정	설명
HTTP 프록시 서버	GUI에 나열된 서비스에 사용되는 옵션 프록시 서버입니다. 프록시 서버를 지정하면 해당 서버가 모든 서비스를 업데이트하는 데 사용됩니다.
HTTPS 프록시 서버	HTTPS를 사용하는 옵션 프록시 서버입니다. HTTPS 프록시 서버를 정의하면 해당 서버가 GUI에 나열된 서비스를 업데이트하는 데 사용됩니다.

4단계 변경 사항을 제출하고 커밋합니다.

자동 업데이트 구성

절차

1단계 Security Services(보안 서비스) > Service Updates(서비스 업데이트) 페이지로 이동하여 **Edit Update Settings(업데이트 설정 편집)**를 클릭합니다.

2단계 확인란을 선택하여 자동 업데이트를 활성화합니다.

3단계 업데이트 간격(업데이트 확인 사이의 대기 시간)을 입력합니다. 분의 경우 후행 **m**을 추가하고 시간의 경우 **h**를 추가합니다. 최대 업데이트 간격은 1시간입니다.

업데이트 서버 인증서의 유효성을 확인하도록 어플라이언스 구성

Email Security 어플라이언스는 어플라이언스가 업데이트 서버와 통신할 때마다 Cisco 업데이트 서버 인증서의 유효성을 확인할 수 있습니다. 이 옵션을 구성하고 확인에 실패한 경우 업데이트가 다운로드되지 않으며 세부정보가 업데이트 프로그램 로그에 기록됩니다.

이 옵션을 구성하려면 `updateconfig` 명령을 사용합니다. 다음 예제는 이 옵션을 구성하는 방법을 보여줍니다.

```
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
[]>
```

신뢰할 수 있는 프록시 서버 통신을 수행하도록 어플라이언스 구성

투명하지 않은 프록시 서버를 사용할 경우 프록시 인증서에 서명하는 데 사용할 CA 인증서를 어플라이언스에 추가할 수 있습니다. 이렇게 하면 어플라이언스가 프록시 서버 통신을 신뢰합니다.

이 옵션을 구성하려면 `updateconfig` 명령을 사용합니다. 다음 예제는 이 옵션을 구성하는 방법을 보여줍니다.

```
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

	수행할 작업	참조:
1단계	모든 업데이트 및 업그레이드 다운로드에 적용한 설정을 구성하고 이러한 다운로드를 지원하고 선택적으로 배포하도록 네트워크를 설정합니다(아직 이러한 구성 및 설정을 수행하지 않은 경우).	업그레이드 및 업데이트를 가져오도록 설정, 33-17페이지
2단계	언제 업그레이드를 사용할 수 있는지 파악하고 설치할지 여부를 결정합니다.	사용 가능한 업그레이드 알림, 33-26페이지
3단계	각 업그레이드 전에 필수 및 권장 작업을 수행합니다.	AsyncOS 업그레이드 준비, 33-26페이지
4단계	업그레이드를 수행합니다.	업그레이드 다운로드 및 설치, 33-27페이지

클러스터 시스템 업그레이드 정보

클러스터 머신을 업그레이드할 경우 클러스터의 머신 업그레이드, 39-12페이지를 참조하십시오.

업그레이드 절차의 배치 명령 정보

업그레이드 절차의 배치 명령은 *Cisco AsyncOS CLI 참조 설명서* (http://www.cisco.com/en/US/products/ps10154/prod_command_reference_list.html)에 문서화되어 있습니다.

사용 가능한 업그레이드 알림

기본적으로 관리자 및 기술자 권한이 있는 사용자는 어플라이언스에 AsyncOS 업그레이드를 사용할 수 있는 경우 웹 인터페이스의 상단에 알림이 표시됩니다.

클러스터 머신에서는 사용자가 로그인한 머신에만 작업이 적용됩니다.

변경 후	수행할 작업
최신 업그레이드에 대한 자세한 정보 보기	업그레이드 알림 위에 마우스 커서를 놓습니다.
사용 가능한 모든 업그레이드 목록 보기	알림에서 아래로 화살표를 클릭합니다.
현재 알림을 해제합니다. 새 업그레이드를 사용할 수 있을 때까지 어플라이언스가 다른 알림을 표시하지 않습니다.	아래로 화살표를 클릭한 다음 **Clear the notification(알림 지우기)**을 선택하고 **Close(닫기)**를 클릭합니다.
더 이상 알림을 표시하지 않음(관리자 권한이 있는 사용자만 해당)	**System Administration(시스템 관리) > System Upgrade(시스템 업그레이드)**로 이동합니다.

사용 가능한 업그레이드 알림

기본적으로 관리자 및 기술자 권한이 있는 사용자는 어플라이언스에 AsyncOS 업그레이드를 사용할 수 있는 경우 웹 인터페이스의 상단에 알림이 표시됩니다.

클러스터 머신에서는 사용자가 로그인한 머신에만 작업이 적용됩니다.

변경 후	수행할 작업
최신 업그레이드에 대한 자세한 정보 보기	업그레이드 알림 위에 마우스 커서를 놓습니다.
사용 가능한 모든 업그레이드 목록 보기	알림에서 아래로 화살표를 클릭합니다.
현재 알림을 해제합니다. 새 업그레이드를 사용할 수 있을 때까지 어플라이언스가 다른 알림을 표시하지 않습니다.	아래로 화살표를 클릭한 다음 **Clear the notification(알림 지우기)**을 선택하고 **Close(닫기)**를 클릭합니다.
더 이상 알림을 표시하지 않음(관리자 권한이 있는 사용자만 해당)	**System Administration(시스템 관리) > System Upgrade(시스템 업그레이드)**로 이동합니다.

AsyncOS 업그레이드 준비

모범 사례로서, Cisco에서는 다음과 같은 단계를 수행하여 업그레이드를 준비할 것을 권장합니다.

절차

1단계 XML 구성 파일 오프 박스를 저장합니다. 어떠한 이유로 업그레이드 전 릴리스로 되돌아가야 할 경우 이 파일이 필요합니다.

2단계 허용 목록/차단 목록 기능을 사용할 경우 목록 오프 박스를 내보냅니다.

3단계 모든 리스너를 일시 중단합니다. CLI에서 업그레이드를 수행할 경우 `suspendlistener` 명령을 사용합니다. GUI에서 업그레이드를 수행할 경우 리스너 일시 중단이 자동으로 수행됩니다.

4단계 큐가 빌 때까지 기다립니다. `workqueue` 명령을 사용하여 작업 큐의 메시지 수를 보거나 CLI에서 `rate` 명령을 사용하여 어플라이언스의 메시지 처리량을 모니터링할 수 있습니다.

참고 업그레이드 후에 리스너를 다시 활성화합니다.

업그레이드 다운로드 및 설치

단일 작업으로 다운로드 및 설치하거나 백그라운드에서 다운로드하여 나중에 설치할 수 있습니다.

참고 Cisco IronPort 서버가 아닌 로컬 서버에서 단일 작업으로 AsyncOS를 다운로드 및 설치하면 *다운로드 즉시 업그레이드*가 설치됩니다.
업그레이드 프로세스 시작 시 10초 동안 배너가 표시됩니다. 이 배너가 표시되어 있는 동안 Control-C를 입력하여 다운로드가 시작되기 전에 업그레이드 프로세스를 종료할 수 있는 옵션을 사용할 수 있습니다.

시작하기 전에

- Cisco에서 직접 업그레이드를 다운로드할지 또는 네트워크의 서버에서 업그레이드 이미지를 호스팅할지 선택합니다. 그런 다음 선택한 방법을 지원하도록 네트워크를 설정합니다. 그런 후에 선택한 소스에서 업그레이드를 가져오도록 어플라이언스를 구성합니다. 업그레이드 및 업데이트를 가져오도록 설정, 33-17페이지 및 업그레이드 및 업데이트를 다운로드하도록 서버 설정 구성, 33-21페이지를 참조하십시오.
- 지금 업그레이드를 설치하려면 AsyncOS 업그레이드 준비, 33-26페이지의 지침을 따르십시오.
- 클러스터 시스템에 업그레이드를 설치할 경우 클러스터의 머신 업그레이드, 39-12페이지를 참조하십시오.
- 업그레이드를 다운로드만 할 경우 설치할 준비가 될 때까지 특별한 요구 사항이 없습니다.

절차

1단계 **System Administration(시스템 관리) > System Upgrade(시스템 업그레이드)**를 선택합니다.

2단계 **Upgrade Options(업그레이드 옵션)**를 클릭합니다.

3단계 다음 옵션을 선택합니다.

변경 후	수행할 작업
단일 작업으로 업그레이드 다운로드 및 설치	**Download and Install(다운로드 및 설치)**을 클릭합니다. 이미 설치 프로그램을 다운로드한 경우 기존 다운로드를 덮어쓸 것인지 묻는 메시지가 표시됩니다.

변경 후	수행할 작업
설치 프로그램 다운로드 및 업그레이드	**Download only(다운로드만)**를 클릭합니다. 이미 설치 프로그램을 다운로드한 경우 기존 다운로드를 덮어쓸 것인지 묻는 메시지가 표시됩니다. 서비스 중단 없이 설치 프로그램이 백그라운드에서 다운로드됩니다.
다운로드한 업그레이드 설치 프로그램 설치	**Install(설치)**을 클릭합니다. 이 옵션은 설치 프로그램이 다운로드된 경우에만 나타납니다. 설치할 AsyncOS 버전이 설치 옵션 아래에 표시됩니다.

4단계 이전에 다운로드한 설치 프로그램을 설치하지 않을 경우 사용 가능한 업그레이드 목록에서 AsyncOS 버전을 선택합니다.

5단계 설치할 경우 다음을 수행합니다.

a. 현재 구성을 어플라이언스의 `configuration` 디렉토리에 저장할지 선택합니다.

b. 구성 파일의 비밀번호를 마스크 처리할지 선택합니다.

참고 비밀번호가 마스크 처리된 구성 파일은 GUI의 구성 파일 페이지를 사용하거나 CLI에서 `loadconfig` 명령을 사용하여 로드할 수 없습니다.

c. 구성 파일의 사본을 이메일로 보내려면 이메일로 파일을 보낼 이메일 주소를 입력합니다. 여러 개의 이메일 주소를 구분하려면 쉼표를 사용합니다.

6단계 **진행**을 클릭합니다.

7단계 설치할 경우 다음을 수행합니다.

a. 프로세스 도중 표시되는 프롬프트에 응답할 준비를 합니다.

응답할 때까지 프로세스가 일시 중지됩니다.

진행률 표시줄이 페이지 상단 근처에 나타납니다.

b. 프롬프트에서 **Reboot Now(지금 재부팅)**를 클릭합니다.

c. 약 10분 후에 어플라이언스에 다시 액세스하여 로그인합니다.

업그레이드 문제를 해결하기 위해 어플라이언스의 전원을 껐다가 켜야 할 경우 재부팅한 후 최소한 20분이 경과할 때까지 기다리십시오.

향후 작업

- 프로세스가 중단된 경우 해당 프로세스를 다시 시작해야 합니다.
- 업그레이드를 다운로드했으나 설치하지 않은 경우 다음을 수행합니다.

  업그레이드를 설치할 준비가 되면 시작하기 전에 섹션의 요구 사항을 포함해 처음부터 이러한 지침을 따르되 설치 옵션을 선택합니다.
- 업그레이드를 설치한 경우 다음을 수행합니다.
  - 리스너를 다시 활성화(다시 시작)합니다.
  - 새 시스템의 구성 파일을 저장합니다. 관련 내용은 구성 파일 관리, 33-7페이지를 참조하십시오.
- 업그레이드가 완료된 후 리스너를 다시 활성화합니다.

백그라운드 다운로드 상태 보기, 취소 또는 삭제

절차

1단계 **System Administration(시스템 관리) > System Upgrade(시스템 업그레이드)**를 선택합니다.

2단계 **Upgrade Options(업그레이드 옵션)**를 클릭합니다.

3단계 다음 옵션을 선택합니다.

변경 후	수행할 작업
다운로드 상태 보기	페이지의 가운데 부분을 봅니다. 진행 중인 다운로드가 없고 설치 대기 중인 완료된 다운로드가 없는 경우 다운로드 상태 정보가 표시되지 않습니다.
다운로드 취소	페이지의 가운데에 있는 **Cancel Download(다운로드 취소)** 버튼을 클릭합니다. 이 옵션은 다운로드가 진행 중인 경우에만 나타납니다.
다운로드한 설치 프로그램 삭제	페이지의 가운데에 있는 **Delete File(파일 삭제)** 버튼을 클릭합니다. 이 옵션은 설치 프로그램이 다운로드된 경우에만 나타납니다.

4단계 (선택 사항) 업그레이드 로그를 확인합니다.

원격 전력 관리 활성화

어플라이언스 섀시의 전력을 원격으로 리셋할 수 있는 기능은 하드웨어 C380 및 C680에서만 사용할 수 있습니다.

어플라이언스 전력을 원격으로 리셋할 수 있으려면 이 섹션에 설명된 절차를 사용하여 이 기능을 미리 구성하고 활성화해야 합니다.

시작하기 전에

- 전용 원격 전력 관리 포트를 보안 네트워크에 직접 연결합니다. 관련 내용은 하드웨어 설치 설명서를 참조하십시오.
- 어플라이언스가 원격으로 액세스할 수 있는지 확인합니다. 예를 들어, 방화벽을 통해 필수 포트를 엽니다.
- 이 기능을 사용하려면 전용 원격 전력 관리 인터페이스에 고유한 IPv4 주소가 필요합니다. 이 인터페이스는 이 섹션에 설명된 절차를 통해서만 구성할 수 있으며, `ipconfig` 명령을 사용해서 구성할 수 없습니다.
- 어플라이언스 전원을 제어하려면 IPMI(Intelligent Platform Management Interface) 버전 2.0을 지원하는 디바이스를 관리할 수 있는 타사 툴이 필요합니다. 그러한 툴을 사용할 준비가 되었는지 확인합니다.
- 명령줄 인터페이스에 액세스하는 방법에 대한 자세한 내용은 CLI 참조 설명서를 참조하십시오.

절차

1단계 SSH, 텔넷 또는 직렬 콘솔 포트를 사용하여 명령줄 인터페이스에 액세스합니다.

2단계 관리자 액세스 권한이 있는 계정을 사용하여 로그인합니다.

3단계 다음과 같은 명령을 입력합니다.

```
remotepower
setup
```

4단계 프롬프트에 따라 다음을 지정합니다.

- 이 기능의 전용 IP 주소와 넷마스크 및 게이트웨이.
- 전원 사이클 명령을 실행하는 데 필요한 사용자 이름 및 비밀번호.

  이러한 자격 증명은 어플라이언스에 액세스하는 데 사용되는 다른 인증서와 무관합니다.

5단계 `commit`을 입력하여 변경 사항을 저장합니다.

6단계 구성을 테스트하여 원격으로 어플라이언스 전력을 관리할 수 있는지 확인합니다.

7단계 입력한 자격 증명을 이후에 필요할 때에 사용할 수 있는지 확인합니다. 예를 들어, 이 정보를 안전한 곳에 저장하고 이 작업을 수행해야 할 수 있는 관리자가 필요한 자격 증명에 액세스할 수 있는지 확인합니다.

관련 주제

- 원격으로 어플라이언스 전력 리셋, 40-24페이지

이전 버전의 AsyncOS로 되돌리기

AsyncOS에는 비상 시에 AsyncOS 운영 체제를 이전의 적격한 빌드로 되돌릴 수 있는 기능이 포함되어 있습니다.

되돌리기의 영향

어플라이언스에서 `revert` 명령을 사용하는 것은 매우 파괴적인 작업입니다. 이 명령은 모든 구성 로그와 데이터베이스를 제거합니다. 관리 인터페이스의 네트워크 정보만 유지되고 그 밖의 모든 네트워크 구성은 삭제됩니다. 또한 되돌리기를 실행하면 어플라이언스가 재구성될 때까지 메일 처리가 중단됩니다. 이 명령을 실행하면 네트워크 구성이 제거되므로 `revert` 명령을 실행하려는 경우 로컬에서 물리적으로 어플라이언스에 액세스해야 할 수 있습니다.

주의 되돌리려는 버전의 구성 파일이 있어야 합니다. 구성 파일은 역호환성을 지원하지 *않습니다*.

가상 어플라이언스에서 AsyncOS를 되돌리면 라이센스에 영향을 미칠 수 있음

AsyncOS 9.0 for Email에서 AsyncOS 8.5 for Email로 되돌릴 경우 라이센스는 변경되지 않습니다.

AsyncOS 9.0 for Email에서 AsyncOS 8.0 for Email로 되돌릴 경우 보안 기능 없이 어플라이언스가 메일을 전송할 수 있는 180일의 유예 기간이 더 이상 주어지지 않습니다.

어느 경우든 기능 키 만료일은 변경되지 않습니다.

관련 주제

- 가상 어플라이언스 라이센스 만료, 33-6페이지

AsyncOS 되돌리기

절차

1단계 되돌리려는 버전의 구성 파일이 있는지 확인합니다. 구성 파일은 역호환성을 지원하지 않습니다. 이렇게 하려면 이메일로 파일을 본인에게 보내거나 FTP를 사용하여 파일을 보낼 수 있습니다. 이 작업을 수행할 수 있는 간단한 방법은 `mailconfig` CLI 명령을 실행하는 것입니다.

2단계 어플라이언스의 현재 구성의 백업 사본(비밀번호 마스크 해제)을 다른 머신에 저장합니다.

참고 이 파일은 되돌리기 후에 로드할 구성 파일이 아닙니다.

3단계 허용 목록/차단 목록 기능을 사용할 경우 허용 목록/차단 목록 데이터베이스를 다른 머신으로 내보냅니다.

4단계 메일 큐가 빌 때까지 기다립니다.

5단계 되돌릴 어플라이언스의 CLI에 로그인합니다.

`revert` 명령을 실행하면 여러 개의 경고 프롬프트가 표시됩니다. 이러한 경고 프롬프트가 수락된 직후에 되돌리기 작업이 수행됩니다. 따라서 되돌리기 전 단계를 완료할 때까지 되돌리기 프로세스를 시작하지 마십시오.

6단계 CLI에서 `revert` 명령을 실행합니다.

참고 되돌리기 프로세스는 시간이 소요됩니다. 되돌리기가 완료되고 어플라이언스에 대한 콘솔 액세스를 다시 사용할 수 있을 때까지 15분~20분이 소요될 수 있습니다.

다음 예제는 `revert` 명령을 보여줍니다.

```
mail.mydomain.com> revert


This command will revert the appliance to a previous version of AsyncOS.


WARNING: Reverting the appliance is extremely destructive.

The following data will be destroyed in the process:

- all configuration settings (including listeners)

- all log files

- all databases (including messages in Virus Outbreak and Policy

quarantines)

- all reporting data (including saved scheduled reports)

- all message tracking data
```

```
- all IronPort Spam Quarantine message and end-user safelist/blocklist data


Only the network settings will be preserved.


Before running this command, be sure you have:

- saved the configuration file of this appliance (with passwords

unmasked)

- exported the IronPort Spam Quarantine safelist/blocklist database

   to another machine (if applicable)

- waited for the mail queue to empty


Reverting the device causes an immediate reboot to take place.

After rebooting, the appliance reinitializes itself and reboots again to the desired
version.


계속하시겠습니까?

Are you *really* sure you want to continue? yes


 Available version               Install date

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

 Available version               Install date

1. 5.5.0-236                       Tue Aug 28 11:03:44 PDT 2007

2. 5.5.0-330                       Tue Aug 28 13:06:05 PDT 2007

3. 5.5.0-418                       Wed Sep  5 11:17:08 PDT 2007


Please select an AsyncOS version: 2

You have selected "5.5.0-330".

The system will now reboot to perform the revert operation.
```

7단계 어플라이언스가 두 번 재부팅될 때까지 기다립니다.

8단계 머신이 두 번 재부팅되면 직렬 콘솔을 사용하여 `interfaceconfig` 명령을 실행해 액세스 가능한 IP 주소로 인터페이스를 구성합니다.

9단계 구성된 인터페이스 중 하나에서 FTP 또는 HTTP를 활성화합니다.

10단계 생성한 XML 구성 파일을 FTP를 사용해 전송하거나 GUI 인터페이스에 붙여 넣습니다.

11단계 되돌릴 버전의 XML 구성 파일을 로드합니다.

12단계 허용 목록/차단 목록 기능을 사용할 경우 허용 목록/차단 목록 데이터베이스를 가져와서 복원합니다.

13단계 변경 사항을 커밋합니다.

이제 선택한 AsyncOS 버전을 사용하여 되돌린 어플라이언스를 실행해야 합니다.

어플라이언스에서 생성된 메시지의 복귀 주소 구성

다음과 같은 경우 AsyncOS에서 생성한 메일의 봉투 발신자를 구성할 수 있습니다.

- 안티바이러스 알림
- 바운스
- DMARC 피드백
- 알림(`notify()` 및 `notify-copy()` 필터 작업)
- 격리 알림(및 격리 관리의 "Send Copy(사본 전송)")
- 보고서
- 기타 모든 메시지

복귀 주소의 표시, 사용자 및 도메인 이름을 지정할 수 있습니다. 또한 도메인 이름에 가상 게이트웨이 도메인을 사용하도록 선택할 수 있습니다.

GUI에서 또는 CLI에서 `addressconfig` 명령을 사용하여 시스템에서 생성한 이메일 메시지의 복귀 주소를 수정할 수 있습니다.

절차

1단계 System Administration(시스템 관리) > Return Addresses(복귀 주소) 페이지로 이동합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 수정할 주소를 변경합니다.

4단계 변경 사항을 제출하고 커밋합니다.

경고

경고 메시지는 어플라이언스에서 발생한 이벤트에 대한 정보를 포함하는 자동으로 생성된 표준 이메일 메시지입니다. 이러한 이벤트는 중요도(또는 심각도)가 보통에서 중요에 이르기까지 다양할 수 있으며 일반적으로 어플라이언스의 특정 구성 요소 또는 기능과 관련이 있을 수 있습니다. 경고는 어플라이언스에서 생성됩니다. 전송할 경고 메시지, 경고 메시지를 받을 사용자, 경고 전송 시 이벤트의 심각도를 훨씬 더 세부적으로 지정할 수 있습니다. GUI의 System Administration(시스템 관리) > Alerts(경고) 페이지를 통해(또는 CLI에서 `alertconfig` 명령을 통해) 경고를 관리합니다.

경고 심각도

다음과 같은 심각도로 경고를 보낼 수 있습니다.

- 위험: 즉각적인 대처가 필요
- 경고: 추가 모니터링 및 잠재적으로 즉각적인 대처가 필요한 문제 또는 오류
- 정보: 이 디바이스의 일상적인 작동 과정에서 생성된 정보

AutoSupport

Cisco가 더 나은 지원을 제공하고 향후 시스템 변경 사항을 설계할 수 있도록 Cisco Systems에 시스템에서 생성된 모든 경고 메시지의 사본을 보내도록 어플라이언스를 구성할 수 있습니다. AutoSupport라는 이 기능은 Cisco 팀이 사용자의 요구를 능동적으로 지원할 수 있는 유용한 방법입니다. 또한 AutoSupport는 시스템의 가동 시간, `status` 명령의 출력, 사용된 AsyncOS 버전이 표시된 보고서를 매주 전송합니다.

기본적으로 시스템 경고 유형의 정보 심각도 경고를 수신하도록 설정된 경고 수신자는 Cisco에 전송된 모든 메시지의 사본을 받게 됩니다. 매주 내부에서 경고 메시지를 전송하지 않으려면 이 기능을 비활성화할 수 있습니다. 이 기능을 활성화하거나 비활성화하려면 경고 설정 구성, 33-36페이지를 참조하십시오.

경고 전송

어플라이언스에서 경고 수신자에 지정된 주소로 전송된 경고는 그러한 대상에 대해 정의된 SMTP 경로를 따릅니다.

경고 메시지는 사용자에게 어플라이언스 내의 문제를 알리는 데 사용될 수 있으므로 AsyncOS의 일반적인 메일 전송 시스템을 사용하여 전송되지 않습니다. 그 대신, 경고 메시지는 AsyncOS에서 중대한 시스템 장애가 발생한 경우에도 작동하도록 설계된 별도의 병렬 이메일 시스템을 통해 전달됩니다.

경고 메일 시스템은 AsyncOS와 동일한 구성을 공유하지 않으며, 이는 경고 메시지가 다른 메일 전송과 약간 다르게 동작할 수 있음을 의미합니다.

- 경고 메시지는 표준 DNS MX 및 A 레코드 조회를 사용하여 전송됩니다.
  - AsyncOS 5.X 이전 버전에서는 `smtproutes`를 사용하지 않습니다.
  - 30분 동안 DNS 항목을 캐시하고 캐시가 30분마다 새로 고쳐지므로 DNS 실패 시에도 경고가 전송됩니다.
- 경고 메시지는 작업 큐를 통과하지 않으므로 바이러스 또는 스팸 검사를 받지 않습니다. 또한 메시지 필터 또는 콘텐츠 필터가 적용되지 않습니다.
- 경고 메시지는 전송 큐를 통과하지 않으므로 바운스 프로필 또는 대상 제어 제한의 영향을 받지 않습니다.

경고 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

경고 엔진은 전송할 경고와 경고를 받을 수신자를 더 세부적으로 제어할 수 있습니다. 예를 들어, 시스템(경고 유형)에 대한 위험(심각도) 정보를 전송할 경우에만 알림을 수신하도록 경고 수신자를 구성하여 경고 수신자에게 특정한 경고만 보내도록 시스템을 구성할 수 있습니다.

참고 시스템 설정 도중 AutoSupport를 활성화한 경우 지정된 이메일 주소가 기본적으로 모든 심각도 및 등급의 경고를 수신합니다. 언제든지 이 구성을 변경할 수 있습니다.

절차

1단계 **System Administration(시스템 관리) > Alerts(경고)**를 선택합니다.

2단계 **Add Recipient(수신자 추가)**를 클릭합니다.

3단계 수신자의 이메일 주소를 입력합니다. 여러 주소를 쉼표로 구분하여 입력할 수 있습니다.

4단계 (선택 사항) Cisco 지원에서 소프트웨어 릴리스와 중요한 지원 알림 경고를 수신하려면 **Release and Support Notifications(릴리스 및 지원 알림)** 확인란을 선택합니다.

5단계 이 수신자가 받을 경고 유형과 심각도를 선택합니다.

6단계 변경 사항을 제출하고 커밋합니다.

경고 설정 구성

다음과 같은 설정이 모든 경고에 적용됩니다.

참고 `alertconfig` CLI 명령을 사용하여 어플라이언스에 저장해서 나중에 볼 경고의 수를 정의할 수 있습니다.

절차

1단계 경고 페이지에서 **Edit Settings(설정 편집)**를 클릭합니다.

2단계 경고를 보낼 때 사용할 헤더 전송 주소를 입력하거나 자동으로 생성된 주소("경고@<호스트 이름>")를 선택합니다.

3단계 중복 경고 전송 사이의 대기 시간(초)을 지정하려면 해당 확인란을 선택합니다. 자세한 내용은 중복 경고 전송, 33-37페이지를 참고하십시오.

- 중복 경고를 보내기 전에 대기할 초기 시간(초)을 지정합니다.
- 중복 경고를 보내기 전에 대기할 최대 시간(초)을 지정합니다.

4단계 IronPort AutoSupport 옵션을 선택하여 AutoSupport를 활성화할 수 있습니다. AutoSupport에 대한 자세한 내용은 AutoSupport, 33-34페이지를 참조하십시오.

- AutoSupport가 활성화되면 정보 수준에서 시스템 경고를 받도록 설정된 경고 수신자에게 주별 AutoSupport 보고서가 전송됩니다. 해당 확인란을 통해 이 옵션을 비활성화할 수 있습니다.

5단계 변경 사항을 제출하고 커밋합니다.

경고 설정

경고 설정은 다음을 포함한 일반적인 경고 동작 및 구성을 제어합니다.

- RFC 2822 헤더 전송 주소: 경고 전송 시(주소를 입력하거나 기본 "경고@<호스트 이름>" 사용). CLI에서 `alertconfig -> from` 명령을 사용하여 이를 설정할 수도 있습니다.
- 중복 경고를 보내기 전에 대기할 초기 시간(초)
- 중복 경고를 보내기 전에 대기할 최대 시간(초)
- AutoSupport의 상태(활성화 또는 비활성화)
- 정보 수준에서 시스템 경고를 받도록 설정된 경고 수신자에게 AutoSupport의 주별 보고서 전송

중복 경고 전송

AsyncOS가 중복 경고를 보내기 전에 대기할 초기 시간(초)을 지정할 수 있습니다. 이 값을 0으로 설정하면 중복 경고 요약이 전송되지 않고 그 대신 모든 중복 경고가 즉시 전송됩니다(이로 인해 단시간에 대량의 이메일이 전송될 수 있음). 각 경고가 전송된 후 중복 경고 전송 사이의 대기 시간(초, 경고 간격)이 증가합니다. 증가 값은 대기 시간(초)에 마지막 간격의 2배에 해당하는 간격을 더한 값입니다. 따라서 대기 시간이 5초라면 5초, 15초, 35초, 75초, 155초, 315초 등의 간격으로 경고가 전송되었음을 의미합니다.

경국 간격이 상당히 커질 수 있습니다. 중복 경고를 보내기 전에 대기할 최대 시간(초) 필드를 통해 간격 사이의 최대 대기 시간(초)을 설정할 수 있습니다. 예를 들어, 초기 값을 5초로 설정하고 최대 값을 60초로 설정하면 5초, 15초, 35초, 60초, 120초 등의 간격으로 경고가 전송됩니다.

최근 경고 보기

Email Security 어플라이언스는 최신 경고를 저장하므로 경고 메시지를 잃거나 삭제한 경우 GUI와 CLI 모두에서 경고를 볼 수 있습니다. 이러한 경고는 어플라이언스에서 다운로드할 수 없습니다.

최신 경고 목록을 보려면 경고 페이지의 **View Top Alerts(상위 경고 보기)** 버튼을 클릭하거나 CLI에서 `displayalerts` 명령을 사용합니다. GUI에서 날짜, 수준, 등급, 텍스트, 수신자별로 경고를 정렬할 수 있습니다.

기본적으로 어플라이언스는 최대 50개의 경고를 저장하여 **Top Alerts(상위 경고)** 창에 표시합니다. CLI에서 `alertconfig -> setup` 명령을 사용하여 어플라이언스가 저장할 경고의 수를 편집합니다. 이 기능을 비활성화하려면 경고의 수를 0으로 변경합니다.

경고 설명

다음과 같은 표에는 경고 이름(Cisco에 사용되는 내부 설명자), 경고의 실제 텍스트, 설명, 심각도(위험, 정보 또는 경고), 메시지의 텍스트에 포함된 매개변수(있는 경우)를 포함하여 경고가 분류별로 나열되어 있습니다. 매개변수의 값은 경고의 실제 텍스트에서 바뀝니다. 예를 들어, 아래의 경고 메시지가 메시지 텍스트에서 "$ip"를 언급할 수 있습니다. "$ip"는 경고가 생성될 때 실제 IP 주소로 바뀝니다.

안티스팸 경고

표 33-1에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 안티스팸 경고의 목록이 포함되어 있습니다.

표 33-1 가능한 안티스팸 경고 목록

경고 이름	메시지 및 설명	매개변수
AS.SERVER.ALERT	$engine anti-spam - $message $tb 위험. 안티스팸 엔진이 실패했을 때 전송됩니다.	'**engine**' - 안티스팸 엔진의 유형입니다. '**message**' - 로그 메시지입니다. '**tb**' - 이벤트의 역추적입니다.
AS.TOOL.INFO_ALERT	업데이트 - $engine - $message 정보. 안티스팸 엔진에 문제가 있을 때 전송됩니다.	'**engine**' - 안티스팸 엔진 이름입니다. '**message**' - 메시지입니다.

표 33-1 가능한 안티스팸 경고 목록 (계속)

경고 이름	메시지 및 설명	매개변수
AS.TOOL.ALERT	업데이트 - $engine - $message 위험. 안티스팸 엔진을 관리하는 데 사용된 툴 중 하나에 문제가 있어 업데이트가 중단되었을 때 전송됩니다.	'**engine**' - 안티스팸 엔진 이름입니다. '**message**' - 메시지입니다.

안티바이러스 경고

표 33-2에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 안티바이러스 경고의 목록이 포함되어 있습니다.

표 33-2 가능한 안티바이러스 경고 목록

경고 이름	메시지 및 설명	매개변수
AV.SERVER.ALERT / AV.SERVER.CRITICAL	$engine antivirus - $message $tb 위험. 안티바이러스 검사 엔진에 중요한 문제가 있을 때 전송됩니다.	'**engine**' - 안티바이러스 엔진의 유형입니다. '**message**' - 로그 메시지입니다. '**tb**' - 이벤트의 역추적입니다.
AV.SERVER.ALERT.INFO	$engine antivirus - $message $tb 정보. 안티바이러스 검사 엔진에 정보성 이벤트가 발생했을 때 전송됩니다.	'**engine**' - 안티바이러스 엔진의 유형입니다. '**message**' - 로그 메시지입니다. '**tb**' - 이벤트의 역추적입니다.
AV.SERVER.ALERT.WARN	$engine antivirus - $message $tb 경고. 안티바이러스 검사 엔진에 문제가 있을 때 전송됩니다.	'**engine**' - 안티바이러스 엔진의 유형입니다. '**message**' - 로그 메시지입니다. '**tb**' - 이벤트의 역추적입니다.
MAIL.ANTIVIRUS. ERROR_MESSAGE	MID $mid antivirus $what error $tag 위험. 메시지를 검사하는 도중 안티바이러스 검사로 인해 오류가 발생했을 때 전송됩니다.	'**mid**' - MID '**what**' - 발생한 오류입니다. '**tag**' - 신종 바이러스 이름입니다(설정된 경우).
MAIL.SCANNER. PROTOCOL_MAX_RETRY	MID $mid is malformed and cannot be scanned by $engine. 위험. 메시지 형식이 잘못되어 검사 엔진의 메시지 검사 시도가 실패했습니다. 최대 재시도 횟수가 초과되어 이 엔진이 검사하지 않고 메시지가 처리됩니다.	'**mid**' - MID '**engine**' - 사용되는 엔진입니다.

디렉토리 수집 공격 방지(DHAP) 경고

표 33-3에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 DHAP 경고의 목록이 포함되어 있습니다.

표 33-3 가능한 디렉토리 수집 공격 방지 경고 목록

경고 이름	메시지 및 설명	매개변수
LDAP.DHAP_ALERT	LDAP: 잠재적인 디렉토리 수집 공격이 탐지되었습니다. 이 공격에 대한 자세한 내용은 시스템 메일 로그를 참조하십시오.	
	경고. 가능한 디렉토리 수집 공격이 탐지되었을 때 전송됩니다.	

하드웨어 경고

표 33-4에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 하드웨어 경고의 목록이 포함되어 있습니다.

표 33-4 가능한 하드웨어 경고 목록

경고 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.	'**port**' - 인터페이스 이름입니다. '**in_err**' - 마지막 메시지 이후에 발생한 입력 오류의 수입니다. '**out_err**' - 마지막 메시지 이후에 발생한 출력 오류의 수입니다. '**col**' - 마지막 메시지 이후에 발생한 패킷 충돌 횟수입니다.
	경고. 인터페이스 오류가 탐지되었을 때 전송됩니다.	
MAIL.MEASUREMENTS_ FILESYSTEM	The $file_system partition is at $capacity% capacity	'**file_system**' - 파일 시스템의 이름입니다. '**capacity**' - 파일 시스템이 현재 사용 용량을 백분율로 표시한 값입니다.
	경고. 디스크 파티션이 용량(75%)에 근접했을 때 전송됩니다.	
MAIL.MEASUREMENTS_ FILESYSTEM.CRITICAL	The $file_system partition is at $capacity% capacity	'**file_system**' - 파일 시스템의 이름입니다. '**capacity**' - 파일 시스템이 현재 사용 용량을 백분율로 표시한 값입니다.
	위험. 디스크 파티션이 90% 용량(95%, 96%, 97% 등)에 도달했을 때 전송됩니다.	
SYSTEM.RAID_EVENT_ ALERT	A RAID-event has occurred: $error	'**error**' - RAID 오류의 텍스트입니다.
	경고. 중요한 RAID 이벤트가 발생했을 때 전송됩니다.	
SYSTEM.RAID_EVENT_ ALERT_INFO	A RAID-event has occurred: $error	'**error**' - RAID 오류의 텍스트입니다.
	정보. RAID 이벤트가 발생했을 때 전송됩니다.	

스팸 격리 경고

표 33-5에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 스팸 격리 경고의 목록이 포함되어 있습니다.

표 33-5 가능한 스팸 격리 경고 목록

경고 이름	메시지 및 설명	매개변수
ISQ.CANNOT_CONNECT_OFF_BOX	ISQ: Could not connect to off-box quarantine at $host:$port 정보. AsyncOS가 (오프 박스) IP 주소에 연결하지 못했을 때 전송됩니다.	'**host**' - 오프 박스 격리의 주소입니다. '**port**' - 오프 박스 격리에 연결할 포트입니다.
ISQ.CRITICAL	ISQ: $msg 위험. 중요한 스팸 격리 오류가 발생했을 때 전송됩니다.	'**msg**' - 표시할 메시지입니다.
ISQ.DB_APPROACHING_FULL	ISQ: Database over $threshold% full 경고. 스팸 격리 데이터베이스가 거의 다 찼을 때 전송됩니다.	'**threshold**' - 경고가 시작되는 임계값에 도달한 비율입니다.
ISQ.DB_FULL	ISQ: database is full 위험. 스팸 격리 데이터베이스가 꽉 찼을 때 전송됩니다.	
ISQ.MSG_DEL_FAILED	ISQ: Failed to delete MID $mid for $rcpt: $reason 경고. 이메일이 스팸 격리에서 성공적으로 삭제되지 않았을 때 전송됩니다.	'**mid**' - MID '**rcpt**' - 수신자 또는 "모두"입니다. '**reason**' - 메시지가 삭제되지 않은 이유입니다.
ISQ.MSG_NOTIFICATION_FAILED	ISQ: Failed to send notification message: $reason 경고. 알림 메시지가 성공적으로 전송되지 않았을 때 전송됩니다.	'**reason**' - 알림이 전송되지 않은 이유입니다.
ISQ.MSG_QUAR_FAILED	 경고. 메시지가 성공적으로 격리되지 않았을 때 전송됩니다.	
ISQ.MSG_RLS_FAILED	ISQ: Failed to release MID $mid to $rcpt: $reason 경고. 메시지가 성공적으로 릴리스되지 않았을 때 전송됩니다.	'**mid**' - MID '**rcpt**' - 수신자 또는 "모두"입니다. '**reason**' - 메시지가 릴리스되지 않은 이유입니다.
ISQ.MSG_RLS_FAILED_UNK_RCPTS	ISQ: Failed to release MID $mid: $reason 경고. 수신자를 알 수 없어 메시지가 성공적으로 릴리스되지 않았을 때 전송됩니다.	'**mid**' - MID '**reason**' - 메시지가 릴리스되지 않은 이유입니다.
ISQ.NO_EU_PROPS	ISQ: Could not retrieve $user's properties. Setting defaults 정보. AsyncOS가 사용자에 대한 정보를 검색할 수 없을 때 전송됩니다.	'**user**' - 최종 사용자 이름입니다.
ISQ.NO_OFF_BOX_HOST_SET	ISQ: Setting up off-box ISQ without setting host 정보. 외부 격리를 참조하도록 AsyncOS가 구성되었으나 외부 격리가 정의되지 않았을 때 전송됩니다.	

허용 목록/차단 목록 경고

경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 허용 목록/차단 목록 경고의 목록이 포함되어 있습니다.

표 33-6 가능한 허용 목록/차단 목록 경고 목록

경고 이름	메시지 및 설명	매개변수
SLBL.DB.RECOVERY_FAILED	SLBL: Failed to recover End-User Safelist/Blocklist database: '$error'.	'**error**' - 오류가 발생한 이유입니다.
	위험. 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**' - 현재 사용된 용량입니다(MB).
	위험. 허용 목록/차단 목록 데이터베이스가 허용된 디스크 공간을 초과했습니다.	'**limit**' - 구성된 제한입니다(MB).

시스템 경고

표 33-7에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 시스템 경고의 목록이 포함되어 있습니다.

표 33-7 가능한 시스템 경고 목록

구성 요소/경고 이름	메시지 및 설명	매개변수
AMP.ENGINE.ALERT	Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인, 16-13페이지(16 장, "Advanced Malware Protection 문제에 대한 경고를 수신하는지 확인")를 참조하십시오.	-
AsyncOS API 경고	"경고" 섹션(Cisco AsyncOS API for Email - 시작 설명서)을 참조하십시오.	-
COMMON.APP_FAILURE	An application fault occurred: $error	'**error**' - 오류(일반적으로 역추적)의 텍스트입니다.
	경고. 알 수 없는 애플리케이션 오류가 있을 때 전송됩니다.	
COMMON.KEY_EXPIRED_ALERT	Your "$feature" key has expired. Please contact your authorized Cisco sales representative.	'**feature**' - 만료될 기능의 이름입니다.
	경고. 기능 키가 만료되었을 때 전송됩니다.	
COMMON.KEY_EXPIRING_ALERT	Your "$feature" key will expire in under $days day(s). Please contact your authorized Cisco sales representative.	'**feature**' - 만료될 기능의 이름입니다.
	경고. 기능 키가 만료되려고 할 때 전송됩니다.	'**days**' - 만료될 때까지 남은 일 수입니다.
COMMON.KEY_FINAL_EXPIRING_ALERT	This is a final notice. Your "$feature" key will expire in under $days day(s). Please contact your authorized Cisco sales representative.	'**feature**' - 만료될 기능의 이름입니다.
	경고. 기능 키가 곧 만료된다는 최종 알림으로 전송됩니다.	'**days**' - 만료될 때까지 남은 일 수입니다.

표 33-7 가능한 시스템 경고 목록 (계속)

구성 요소/경고 이름	메시지 및 설명	매개변수
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. 위험. 가상 어플라이언스 라이센스 만료의 유예 기간이 시작되는 시점부터 정기적으로 전송됩니다.	'**days**' - 경고가 전송되었을 때 남은 유예 기간의 일 수입니다. 유예 기간에 대한 자세한 내용은 가상 어플라이언스 라이센스 만료, 33-6페이지를 참조하십시오.
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. 위험. 가상 어플라이언스 라이센스가 만료되기 하루 전에 전송됩니다.	유예 기간에 대한 자세한 내용은 가상 어플라이언스 라이센스 만료, 33-6페이지를 참조하십시오.
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. 위험. 가상 어플라이언스의 유예 기간이 만료되면 전송됩니다.	유예 기간에 대한 자세한 내용은 가상 어플라이언스 라이센스 만료, 33-6페이지를 참조하십시오.
DNS.BOOTSTRAP_FAILED	Failed to bootstrap the DNS resolver. Unable to contact root servers. 경고. 어플라이언스가 루트 DNS 서버에 연결할 수 없을 때 전송됩니다.	
INTERFACE. FAILOVER.FAILURE_ BACKUP_DETECTED	Standby port $port on $pair_name failure 경고. 백업 NIC 페어링 인터페이스가 실패했을 때 전송됩니다.	'**port**' - 탐지된 포트입니다. '**pair_name**' - 대체작동 쌍 이름입니다.
INTERFACE. FAILOVER.FAILURE_ BACKUP_RECOVERED	Standby port $port on $pair_name okay 정보. NIC 쌍 대체작동이 복구되면 전송됩니다.	'**port**' - 실패한 포트입니다. '**pair_name**' - 대체작동 쌍 이름입니다.
INTERFACE.FAILOVER. FAILURE_DETECTED	Port $port failure on $pair_name, switching to $port_other 위험. 인터페이스 오류로 인해 NIC 페어링 대체작동이 탐지되었을 때 전송됩니다.	'**port**' - 실패한 포트입니다. '**port_other**' - 새 포트입니다. '**pair_name**' - 대체작동 쌍 이름입니다.
INTERFACE.FAILOVER. FAILURE_DETECTED_NO_ BACKUP	Port $port_other on $pair_name is down, can't switch to $port_other 위험. 인터페이스 오류로 인해 NIC 페어링 대체작동이 탐지되었으나 백업 인터페이스를 사용할 수 없을 때 전송됩니다.	'**port**' - 실패한 포트입니다. '**port_other**' - 새 포트입니다. '**pair_name**' - 대체작동 쌍 이름입니다.

표 33-7 가능한 시스템 경고 목록 (계속)

구성 요소/경고 이름	메시지 및 설명	매개변수
INTERFACE.FAILOVER. FAILURE_RECOVERED	Recovered network on $pair_name using port $port 정보. NIC 쌍 대체작동이 복구되면 전송됩니다.	'**port**' - 실패한 포트입니다. '**pair_name**' - 대체작동 쌍 이름입니다.
INTERFACE.FAILOVER. MANUAL	Manual failover to port $port on $pair_name 정보. 다른 NIC 쌍에 대한 수동 대체작동이 탐지되었을 때 전송됩니다.	'**port**' - 새 활성 포트입니다. '**pair_name**' - 대체작동 쌍 이름입니다.
COMMON.INVALID_FILTER	Invalid $class: $error 경고. 올바르지 않은 필터가 발견되었을 때 전송됩니다.	'**class**' - "Filter", "SimpleFilter" 등입니다. '**error**' - 필터가 올바르지 않은 이유에 대한 추가 정보입니다.
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 경고. SSH를 통해 어플라이언스에 연결하려고 시도하지만 올바른 자격 증명을 제공하지 않는 IP 주소는 2분 내에 시도 실패 횟수가 10번을 넘을 경우 SSH 차단 목록에 추가됩니다. 사용자가 동일한 IP 주소에서 성공적으로 로그인하면 해당 IP 주소가 허용 목록에 추가됩니다. 허용 목록의 주소는 차단 목록에도 포함되어 있더라도 액세스가 허용됩니다. 약 하루 뒤에 항목이 차단 목록에서 자동으로 제거됩니다.	'**ip**' - 로그인 시도가 발생한 IP 주소입니다.
LDAP.GROUP_QUERY_ FAILED_ALERT	LDAP: Failed group query $name, comparison in filter will evaluate as false 위험. LDAP 그룹 쿼리가 실패했을 때 전송됩니다.	'**name**' - 쿼리의 이름입니다.
LDAP.HARD_ERROR	LDAP: work queue processing error in $name reason $why 위험. 모든 서버를 시도한 후에 LDAP 쿼리가 완전히 실패했을 때 전송됩니다.	'**name**' - 쿼리의 이름입니다. '**why**' - 오류가 발생한 이유입니다.
LOG.ERROR.*	위험. 다양한 기록 오류입니다.	
MAIL.FILTER.RULE_MATCH_ALERT	MID $mid matched the $rule_name rule. \n Details: $details 정보. 헤더 반복 규칙이 `true`로 평가할 때마다 전송됩니다.	'**mid**' - 메시지의 고유한 식별 번호 수입니다. '**rule_name**' - 일치하는 규칙의 이름입니다. '**details**' - 메시지 또는 규칙에 대한 자세한 정보입니다.

표 33-7 가능한 시스템 경고 목록 (계속)

구성 요소/경고 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. 위험. 수신자별 검사 도중 LDAP 그룹 쿼리가 실패했을 때 전송됩니다.	
MAIL.QUEUE.ERROR.*	위험. 다양한 메일 큐 중요 오류입니다.	
MAIL.RES_CON_START_ ALERT.MEMORY	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%. 위험. RAM 사용률이 시스템 리소스 보존 임계값을 초과했을 때 전송됩니다.	'**hostname**' - 호스트의 이름입니다. '**memory_threshold_start**' - 메모리 타피팅이 시작되는 백분율 임계값입니다. '**memory_threshold_halt**' - 메모리가 꽉 차서 시스템이 중단되는 백분율 임계값입니다.
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. 위험. 메일 큐가 오버로드되고 시스템 리소스 보존이 활성화된 경우에 전송됩니다.	'**hostname**' - 호스트의 이름입니다.
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%. 위험. 큐 사용률이 시스템 리소스 보존 임계값을 초과했을 때 전송됩니다.	'**hostname**' - 호스트의 이름입니다. '**queue_threshold_start**' - 큐 타피팅이 시작되는 백분율 임계값입니다. '**queue_threshold_halt**' - 큐가 꽉 차서 시스템이 중단되는 백분율 임계값입니다.
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. 정보. 작업 큐 크기가 너무 커서 리스너가 일시 중지되었을 때 전송됩니다.	'**hostname**' - 호스트의 이름입니다. '**suspend_threshold**' - 작업 큐 크기가 리스너가 일시 중단되는 크기보다 큽니다. '**resume_threshold**' - 작업 큐 크기가 리스너가 다시 시작되는 크기보다 작습니다.
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. 위험. 어플라이언스가 "리소스 보존" 모드로 들어가면 전송됩니다.	'**hostname**' - 호스트의 이름입니다.

표 33-7 가능한 시스템 경고 목록 (계속)

구성 요소/경고 이름	메시지 및 설명	매개변수
MAIL.RES_CON_STOP_ALERT	This system (hostname: $hostname) has exited 'resource conservation' mode as resource utilization has dropped below the conservation threshold. 정보. 어플라이언스가 '리소스 보존' 모드에서 나오면 전송됩니다.	'**hostname**' - 호스트의 이름입니다.
MAIL.SDS.CATEGORY_CHANGE **MAIL.SDS.CERTIFICATE_INVALID** **MAIL.SDS.ERROR_FETCHING_CERTIFICATE**	향후 URL 범주 집합 변경, 15-21페이지를 참조하십시오. URL 필터링 문제 해결, 15-10페이지를 참조하십시오.	—
MAIL.WORK_QUEUE_PAUSED_NATURAL	work queue paused, $num msgs, $reason 위험. 작업 큐가 일시 중지되면 전송됩니다.	'**num**' - 작업 큐의 메시지 수입니다. '**reason**' - 작업 큐가 일시 중지된 이유입니다.
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	work queue resumed, $num msgs 위험. 작업 큐가 다시 시작되면 전송됩니다.	'**num**' - 작업 큐의 메시지 수입니다.
NTP.NOT_ROOT	Not running as root, unable to adjust system time 경고. NTP가 루트로 실행되지 않아서 어플라이언스가 시간을 조정할 수 없을 때 전송됩니다.	
QUARANTINE.ADD_DB_ERROR	Unable to quarantine MID $mid - quarantine system unavailable 위험. 메시지를 격리로 보낼 수 없을 때 전송됩니다.	'**mid**' - MID
QUARANTINE.DB_UPDATE_FAILED	Unable to update quarantine database (current version: $version; target $target_version) 위험. 격리 데이터베이스를 업데이트할 수 없을 때 전송됩니다.	'**version**' - 탐지된 스키마 버전입니다. '**target_version**' - 대상 스키마 버전입니다.
QUARANTINE.DISK_SPACE_LOW	The quarantine system is unavailable due to a lack of space on the $file_system partition. 위험. 격리에 사용되는 디스크 공간이 꽉 찼을 때 전송됩니다.	'**file_system**' - 파일 시스템의 이름입니다.
QUARANTINE.THRESHOLD_ALERT	Quarantine "$quarantine" is $full% full 경고. 격리가 용량의 5%, 50% 또는 75%에 도달했을 때 전송됩니다.	'**quarantine**' - 격리의 이름입니다. '**full**' - 격리의 현재 사용 용량을 백분율로 표시한 값입니다.
QUARANTINE.THRESHOLD_ALERT.SERIOUS	Quarantine "$quarantine" is $full% full 위험. 격리가 용량의 95%에 도달했을 때 전송됩니다.	'**quarantine**' - 격리의 이름입니다. '**full**' - 격리의 현재 사용 용량을 백분율로 표시한 값입니다.

표 33-7 가능한 시스템 경고 목록 (계속)

구성 요소/경고 이름	메시지 및 설명	매개변수
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**' - 발생한 오류 메시지입니다.
	위험. 보고 엔진이 데이터베이스를 열 수 없을 때 전송됩니다.	
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 $threshold percent, full processing of reporting data will be restarted automatically.	'**threshold**' - 임계값입니다.
	경고. 시스템의 디스크 공간이 부족할 경우에 전송됩니다. 로그 항목의 디스크 사용량이 로그 사용량 임계값을 초과할 경우 reportd를 실행하면 집계 보고 기능이 비활성화되고 경고가 전송됩니다.	
REPORTING.CLIENT. UPDATE_FAILED_ALERT	Reporting Client: The reporting system has not responded for an extended period of time ($duration).	'**duration**' - 클라이언트가 보고 데몬에 연결하려고 시도한 기간입니다. 이는 사람이 읽을 수 있는 형식입니다('1시간 3분 27초').
	경고. 보고 엔진이 보고 데이터를 저장하지 못했을 때 전송됩니다.	
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.	
	위험. 보고 엔진이 새 데이터를 저장할 수 없는 경우에 전송됩니다.	
REPORTING.CLIENT. JOURNAL.FREE	Reporting Client: The reporting system is now able to handle new data.	
	정보. 보고 엔진이 새 데이터를 다시 저장할 수 있을 때 전송됩니다.	
PERIODIC_REPORTS. REPORT_TASK.BUILD_ FAILURE	A failure occurred while building periodic report '$report_title'. This subscription has been removed from the scheduler.	'**report_title**' - 보고서 제목입니다.
	위험. 보고 엔진이 보고서를 작성할 수 없을 때 전송됩니다.	
PERIODIC_REPORTS. REPORT_TASK.EMAIL_ FAILURE	A failure occurred while emailing periodic report '$report_title'. This subscription has been removed from the scheduler.	'**report_title**' - 보고서 제목입니다.
	위험. 보고서를 이메일로 전송할 수 없을 때 전송됩니다.	
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 제목입니다.
	위험. 보고서를 아카이브할 수 없을 때 전송됩니다.	

표 33-7 가능한 시스템 경고 목록 (계속)

구성 요소/경고 이름	메시지 및 설명	매개변수
SENDERBASE.ERROR	Error processing response to query $query: response was $response	'**query**' - 쿼리 주소입니다. '**response**' - 수신된 응답의 원시 데이터입니다.
	정보. SenderBase에서 수신한 응답을 처리하는 도중 오류가 발생했을 때 전송됩니다.	
SMTPAUTH.FWD_SERVER_FAILED_ALERT	SMTP Auth: could not reach forwarding server $ip with reason: $why	'**ip**' - 원격 서버의 IP입니다. '**why**' - 오류가 발생한 이유입니다.
	경고. SMTP 인증 전달 서버에 연결할 수 없을 때 전송됩니다.	
SMTPAUTH.LDAP_QUERY_FAILED	SMTP Auth: LDAP query failed, see LDAP debug logs for details.	
	경고. LDAP 쿼리가 실패했을 때 전송됩니다.	
SYSTEM.HERMES_SHUTDOWN_FAILURE.REBOOT	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=reboot	'**error**' - 발생한 오류입니다.
	경고. 재부팅 시 시스템이 중단되는 문제가 발생했을 때 전송됩니다.	
SYSTEM.HERMES_SHUTDOWN_FAILURE.SHUTDOWN	While preparing to ${what}, failed to stop mail server gracefully: ${error}$what:=shut down	'**error**' - 발생한 오류입니다.
	경고. 시스템이 중단되는 문제가 발생했을 때 전송됩니다.	
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	Error updating recipient validation data: $why	'why' - The error message.
	위험. 수신자 검증 업데이트가 실패했을 때 전송됩니다.	
SYSTEM.SERVICE_TUNNEL.DISABLED	Tech support: Service tunnel has been disabled	
	정보. Cisco Support Services에 대해 생성된 터널이 비활성화되었을 때 전송됩니다.	
SYSTEM.SERVICE_TUNNEL.ENABLED	Tech support: Service tunnel has been enabled, port $port	'**port**' - 서비스 터널에 사용된 포트입니다.
	정보. Cisco Support Services에 대해 생성된 터널이 활성화되었을 때 전송됩니다.	
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 주소입니다.
	경고. SSH를 통해 어플라이언스에 연결하려고 시도하지만 올바른 자격 증명을 제공하지 않는 IP 주소는 2분 내에 시도 실패 횟수가 10번을 넘을 경우 SSH 차단 목록에 추가됩니다. 사용자가 동일한 IP 주소에서 성공적으로 로그인하면 해당 IP 주소가 허용 목록에 추가됩니다. 허용 목록의 주소는 차단 목록에도 포함되어 있더라도 액세스가 허용됩니다. 약 하루 뒤에 항목이 차단 목록에서 자동으로 제거됩니다.	

업데이트 프로그램 경고

표 33-8에는 AsyncOS에서 생성할 수 있는 다양한 업데이트 프로그램 경고의 목록이 포함되어 있습니다.

표 33-8 가능한 업데이트 프로그램 경고 목록

경고 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 이름입니다. '**attempts**' - 시도한 횟수입니다.
	경고. 애플리케이션이 업데이트를 중단하고 있습니다.	
UPDATER.UPDATERD.MANIFEST_FAILED_ALERT	The updater has been unable to communicate with the update server for at least $threshold.	'**threshold**' - 사람이 읽을 수 있는 임계값 문자열입니다.
	경고. 서버 매니페스트를 가져오지 못했습니다.	
UPDATER.UPDATERD.RELEASE_NOTIFICATION	$mail_text	'**mail_text**' - 알림 텍스트입니다. '**notification_subject**' - 알림 텍스트입니다.
	경고. 릴리스 알림입니다.	
UPDATER.UPDATERD.UPDATE_FAILED	Unknown error occured: $traceback	'**traceback**' - 역추적입니다.
	위험. 업데이트를 실행하지 못했습니다.	

신종 바이러스 필터(Outbreak Filter) 경고

표 33-9에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 신종 바이러스 필터(Outbreak Filter) 경고의 목록이 포함되어 있습니다. 격리(특히 신종 바이러스 격리)를 위해 시스템 경고에 신종 바이러스 필터(Outbreak Filter)도 표시될 수 있습니다.

표 33-9 가능한 신종 바이러스 필터(Outbreak Filter) 경고 목록

경고 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 경고 텍스트입니다. '**time**' - 마지막 업데이트의 시간입니다. '**date**' - 마지막 업데이트의 날짜입니다.
	정보. 신종 바이러스 필터(Outbreak Filter) 임계값이 변경되었을 때 전송됩니다.	
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 엔진입니다. '**error**' - 발생한 오류입니다.
	경고. 안티스팸 엔진 또는 CASE 규칙을 업데이트하지 못했을 때 전송됩니다.	

클러스터링 경고

표 33-10에는 경고에 대한 설명과 경고 심각도를 포함하여 AsyncOS에서 생성될 수 있는 다양한 클러스터링 경고의 목록이 포함되어 있습니다.

표 33-10 가능한 클러스터링 경고 목록

경고 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 위험. 인증 오류가 발생했을 때 전송됩니다. 이 오류는 머신이 클러스터의 멤버가 아닌 경우에 발생할 수 있습니다.	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다. '**ip**' - 원격 호스트의 IP입니다. '**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR.DROPPED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Existing connection dropped 경고. 클러스터에 대한 연결이 삭제되었을 때 전송됩니다.	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다. '**ip**' - 원격 호스트의 IP입니다. '**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR.FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Connection failure 경고. 클러스터 연결이 실패했을 때 전송됩니다.	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다. '**ip**' - 원격 호스트의 IP입니다. '**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR.FORWARD_FAILED	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Message forward failed, no upstream connection 위험. 어플라이언스가 클러스터의 머신에 데이터를 전달할 수 없을 때 전송됩니다.	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다. '**ip**' - 원격 호스트의 IP입니다. '**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR.NOROUTE	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=No route found 위험. 머신이 클러스터의 다른 머신에 대한 경로를 가져오지 못했을 때 전송됩니다.	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다. '**ip**' - 원격 호스트의 IP입니다. '**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR.SSH_KEY	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Invalid host key 위험. 잘못된 SSH 호스트 키가 있을 때 전송됩니다.	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다. '**ip**' - 원격 호스트의 IP입니다. '**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR.TIMEOUT	Error connecting to cluster machine $name at IP $ip - $error - whyerror:=Operation timed out 경고. 지정된 작업 시간이 초과되었을 때 전송됩니다.	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다. '**ip**' - 원격 호스트의 IP입니다. '**why**' - 오류에 대한 자세한 텍스트입니다.

표 33-10 가능한 클러스터링 경고 목록 (계속)

경고 이름	메시지 및 설명	매개변수
CLUSTER.CC_ERROR_NOIP	Error connecting to cluster machine $name - $error - $why	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다.
	위험. 어플라이언스가 클러스터에 있는 다른 머신의 올바른 IP 주소를 가져오지 못했을 때 전송됩니다.	'**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR_NOIP.AUTH_ERROR	Error connecting to cluster machine $name - $error - whyerror:=Machine does not appear to be in the cluster	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다.
	위험. 클러스터의 머신에 연결하는 도중 인증 오류가 발생했을 때 전송됩니다. 이 오류는 머신이 클러스터의 멤버가 아닌 경우에 발생할 수 있습니다.	'**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR_NOIP.DROPPED	Error connecting to cluster machine $name - $error - whyerror:=Existing connection dropped	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다.
	경고. 머신이 클러스터에 있는 다른 머신의 올바른 IP 주소를 가져오지 못하고 클러스터에 대한 연결이 삭제되었을 때 전송됩니다.	'**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR_NOIP.FAILED	Error connecting to cluster machine $name - $error - whyerror:=Connection failure	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다.
	경고. 알 수 없는 연결 오류가 발생하고 머신이 클러스터에 있는 다른 머신의 올바른 IP 주소를 가져올 수 없을 때 전송됩니다.	'**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR_NOIP.FORWARD_FAILED	Error connecting to cluster machine $name - $error - whyerror:=Message forward failed, no upstream connection	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다.
	위험. 머신이 클러스터에 있는 다른 머신의 올바른 IP 주소를 가져오지 못하고 어플라이언스가 머신에 데이터를 전달할 수 없을 때 전송됩니다.	'**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR_NOIP.NOROUTE	Error connecting to cluster machine $name - $error - whyerror:=No route found	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다.
	위험. 머신이 클러스터에 있는 다른 머신의 올바른 IP 주소와 머신에 대한 경로를 가져오지 못했을 때 전송됩니다.	'**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR_NOIP.SSH_KEY	Error connecting to cluster machine $name - $error - whyerror:=Invalid host key	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다.
	위험. 머신이 클러스터에 있는 다른 머신의 올바른 IP 주소와 올바른 SSH 호스트 키를 가져오지 못했을 때 전송됩니다.	'**why**' - 오류에 대한 자세한 텍스트입니다.
CLUSTER.CC_ERROR_NOIP.TIMEOUT	Error connecting to cluster machine $name - $error - whyerror:=Operation timed out	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다.
	경고. 머신이 클러스터에 있는 다른 머신의 올바른 IP 주소를 가져오지 못하고 지정된 작업 시간이 초과되었을 때 전송됩니다.	'**why**' - 오류에 대한 자세한 텍스트입니다.

표 33-10 가능한 클러스터링 경고 목록 (계속)

경고 이름	메시지 및 설명	매개변수
CLUSTER.SYNC.PUSH_ALERT	Overwriting $sections on machine $name 위험. 구성 데이터가 동기화되지 않았으며 원격 호스트로 전송되었을 때 전송됩니다.	'**name**' - 머신의 호스트 이름 및/또는 일련 번호입니다. '**sections**' - 전송할 클러스터 섹션의 목록입니다.

네트워크 설정 변경

이 섹션에서는 어플라이언스의 네트워크 작업을 구성하는 데 사용되는 기능을 설명합니다. 이러한 기능을 사용하면 시스템 설정 마법사 또는 `systemsetup` 명령(시스템 설정 마법사 사용, 3-13페이지)을 통해 구성한 호스트 이름, DNS 및 라우팅 설정에 직접 액세스할 수 있습니다.

다음과 같은 기능을 설명합니다.

- `sethostname`
- DNS 구성(GUI와 `dnsconfig` 명령을 통해)
- 라우팅 구성(GUI와 `routeconfig` 및 `setgateway` 명령을 통해)
- `dnsflush`
- 비밀번호
- 네트워크 액세스
- 로그인 배너

시스템 호스트 이름 변경

호스트 이름은 CLI 프롬프트에서 시스템을 식별하는 데 사용됩니다. 정규화된 호스트 이름을 입력해야 합니다. `sethostname` 명령은 어플라이언스의 이름을 설정합니다. 새 호스트 이름은 `commit` 명령을 실행할 때까지 적용되지 않습니다.

sethostname 명령

```
oldname.example.com> sethostname


[oldname.example.com]> mail3.example.com


oldname.example.com>
```

호스트 이름 변경을 적용하려면 commit 명령을 입력해야 합니다. 호스트 이름 변경을 성공적으로 커밋하면 새 이름이 CLI 프롬프트에 나타납니다.

```
oldname.example.com> commit


Please enter some comments describing your changes:

[]> Changed System Hostname


Do you want to save the current configuration for rollback? [Y]> n

Changes committed: Fri May 23 11:42:12 2014 GMT
```

새 호스트 이름이 다음과 같이 프롬프트에 나타납니다. mail3.example.com>

DNS(Domain Name System) 설정 구성

GUI의 네트워크 메뉴에 있는 DNS 페이지 또는 dnsconfig 명령을 통해 어플라이언스의 DNS 설정을 구성할 수 있습니다.

다음과 같은 설정을 구성할 수 있습니다.

- 인터넷의 DNS 서버, 자체 서버 또는 특정 서버를 사용할지 여부
- DNS 트래픽에 사용할 인터페이스
- 역방향 DNS 조회 시간이 초과되기 전에 대기할 시간(초)
- DSN 캐시 지우기

DNS 서버 지정

AsyncOS는 인터넷 루트 DNS 서버, 자체 DNS 서버 또는 사용자가 지정한 인터넷 루트 DNS 서버 및 권한 있는 DNS 서버를 사용할 수 있습니다. 인터넷 루트 서버를 사용할 경우 특정 도메인에 사용할 대체 서버를 지정할 수 있습니다. 대체 DNS 서버는 단일 도메인에 적용되므로 해당 도메인에 대한 권한이 있어야 합니다(확정적인 DNS 레코드 제공).

AsyncOS는 인터넷의 DNS 서버를 사용하지 않을 경우 DNS 서버 "분할"을 지원합니다. 자체 내부 서버를 사용할 경우 예외 도메인 및 관련 DNS 서버도 지정할 수 있습니다.

"스플릿 DNS"를 설정할 때 in-addr.arpa(PTR) 항목도 설정해야 합니다. 따라서 예를 들어, ".eng" 쿼리를 네임서버 1.2.3.4에 리디렉션하려 하고 모든 .eng 항목이 172.16 네트워크에 있는 경우 스플릿 DNS 구성의 도메인으로 "eng,16.172.in-addr.arpa"를 지정해야 합니다.

여러 항목 및 우선순위

입력하는 각 DNS 서버에 대해 숫자 우선순위를 지정할 수 있습니다. AsyncOS가 우선순위가 0에 가장 가까운 DNS 서버를 사용하려고 시도합니다. 해당 DNS 서버가 응답하지 않을 경우 AsyncOS가 다음 우선순위의 서버를 사용하려고 시도합니다. 동일한 우선순위에 여러 DNS 서버 항목을 지정할 경우 시스템이 쿼리를 수행할 때마다 해당 우선순위의 DNS 서버 목록을 임의로 지정합니다. 그러면 시스템이 첫 번째 쿼리가 만료되거나 "시간 초과"될 때까지 잠시 기다린 다음 두 번째 쿼리가 만료될 때까지 조금 더 오래 기다립니다. 대기 시간은 정확한 DNS 서버 총 수와 구성된 우선순위에 따라 다릅니다. 시간 초과 길이는 특정 우선순위의 모든 IP 주소에 대해 동일합니다. 첫 번째 우선순위의 시간 초과 값이 가장 짧고 각 후속 우선순위의 시간 초과 값은 더 깁니다. 또한 시간 초과 기간이 대략 60초입니다. 우선순위가 1개인 경우 해당 우선순위의 각 서버의 시간 초과 값은 60초입니다. 우선순위가 2개인 경우 첫 번째 우선순위의 각 서버의 시간 초과 값은 15초이며 두 번째 우선순위의 각 서버의 시간 초과 값은 45초입니다. 우선순위가 3개인 경우 시간 초과 값은 5, 10, 45초입니다.

예를 들어, 4개의 DNS 서버를 구성하고 그 중 2개의 우선순위를 0으로 지정하고 나머지 서버의 우선순위를 각각 1과 2로 지정한다고 가정해 보겠습니다.

표 33-11 DNS 서버, 우선순위 및 시간 초과 간격의 예

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

AsyncOS가 우선순위가 0인 2개의 서버 중 하나를 임의로 선택합니다. 우선순위 0 서버 중 하나가 다운되면 다른 서버가 사용됩니다. 우선순위 0 서버가 모두 다운되면 우선순위 1 서버(1.2.3.6)가 사용된 다음 마지막으로 우선순위 2 서버(1.2.3.7)가 사용됩니다.

시간 초과 기간은 우선순위 0 서버에 대해 모두 동일하며 우선순위 1 서버의 경우 더 길고 우선순위 2 서버의 경우도 더 깁니다.

인터넷 루트 서버 사용

AsyncOS DNS 확인자는 고성능 이메일 전송에 필요한 대량의 동시 DNS 연결을 수용할 수 있도록 설계되었습니다.

참고 기본 DNS 서버를 인터넷 루트 서버 이외의 서버로 설정하면 해당 서버가 권한 있는 서버가 아닌 도메인의 쿼리를 재귀적으로 해결할 수 있어야 합니다.

역방향 DNS 조회 시간 초과

어플라이언스가 이메일을 보내거나 받기 위해 리스너에 연결된 모든 원격 호스트에서 "이중 DNS 조회"를 수행하려고 시도합니다. [즉, 시스템에서 이중 DNS 조회를 수행하여 원격 호스트의 IP 주소를 얻고 그 유효성을 검사합니다. 이중 DNS 조회는 연결 호스트의 IP 주소에 대한 역방향 DNS(PTR) 조회와 그 이후의 PTR 조회 결과에 대한 전달 DNS(A) 조회로 구성됩니다. 그런 다음 시스템이 A 조회 결과가 PTR 조회 결과와 일치하는지 확인합니다. 결과가 일치하지 않거나 A 레코드가 없는 경우 시스템에서 IP 주소만 사용하여 HAT(Host Access Table)의 항목을 일치시킵니다.] 이 특정 시간 초과 기간은 이 조회에만 적용되며 여러 항목 및 우선순위, 33-53페이지에 설명된 일반 DNS 시간 초과와 관련이 없습니다.

기본값은 20초입니다. 시간(초)으로 '0'을 입력하여 모든 리스너 전체에서 전역적으로 역방향 DNS 조회 시간 초과를 비활성화할 수 있습니다.

값이 0초로 설정되면 역방향 DNS 조회가 시도되지 않고 그 대신 표준 시간 초과 응답이 즉시 반환됩니다. 따라서 수신 호스트의 인증서에 호스트의 IP 조회에 매핑되는 공통 이름(CN)이 지정된 경우 어플라이언스가 TLS 확인 연결이 필요한 도메인에 메일을 전송하는 것도 방지됩니다.

DNS 경고

때때로 어플라이언스가 재부팅될 때 "Failed to bootstrap the DNS cache"라는 메시지와 함께 경고가 생성될 수 있습니다. 이 메시지는 시스템이 1차 DNS 서버에 연결하지 못했음을 의미하며, 이러한 오류는 네트워크 연결이 구성되기 전에 DNS 하위 시스템이 온라인 상태가 된 경우 부팅 시에 발생할 수 있습니다. 이 메시지가 다른 시점에 나타나는 경우 네트워크 문제 또는 DNS 구성이 올바른 서버를 가리키지 않음을 나타낼 수 있습니다.

DNS 캐시 지우기

GUI의 Clear Cache(캐시 지우기) 버튼 또는 `dnsflush` 명령(`dnsflush` 명령에 대한 자세한 내용은 *Cisco AsyncOS CLI 참조 설명서* 참조)은 DNS 캐시의 모든 정보를 지웁니다. 로컬 DNS 시스템에 변경이 있는 경우 이 기능을 사용할 수 있습니다. 이 명령은 즉시 실행되며 캐시가 다시 채워지는 동안 일시적인 성능 저하를 유발할 수 있습니다.

그래픽 사용자 인터페이스를 통해 DNS 설정 구성

절차

1단계 **Network(네트워크) > DNS**를 선택합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 인터넷의 루트 DNS 서버, 자체 내부 DNS 서버 또는 인터넷의 루트 DNS를 사용할지 아니면 대체 DNS 서버를 지정할지 선택합니다

4단계 자체 DNS 서버를 사용하려면 서버 ID를 입력하고 **Add Row(행 추가)**를 클릭합니다. 각 서버에 대해 이 작업을 반복합니다. 자체 DNS 서버를 입력할 경우 우선순위도 지정합니다. 자세한 내용은 DNS 서버 지정, 33-52페이지를 참고하십시오.

5단계 특정 도메인에 대해 대체 DNS 서버를 지정하려면 도메인과 대체 DNS 서버 IP 주소를 입력합니다. 추가 도메인을 추가하려면 **Add Row(행 추가)**를 클릭합니다.

참고 쉼표를 사용해 도메인 이름을 구분하여 단일 DNS 서버에 대해 여러 도메인을 입력할 수 있습니다. 또한 쉼표를 사용해 IP 주소를 구분하여 여러 DNS 서버를 입력할 수 있습니다.

6단계 DNS 트래픽에 사용할 인터페이스를 선택합니다.

7단계 역방향 DNS 조회를 취소하기 전에 대기할 시간(초)을 입력합니다.

8단계 또한 **Clear Cache(캐시 지우기)**를 클릭하여 DNS 캐시를 지울 수 있습니다.

9단계 변경 사항을 제출하고 커밋합니다.

TCP/IP 트래픽 경로 구성

일부 네트워크 환경에서는 표준 기본 게이트웨이가 아닌 트래픽 경로를 사용해야 합니다.

Email Security 어플라이언스는 인터넷 프로토콜 버전 4(IPv4) 및 인터넷 프로토콜 버전 6(IPv6) 정적 경로를 모두 사용할 수 있습니다.

CLI에서 `routeconfig` 명령을 사용하거나 다음 절차를 사용하여 정적 경로를 관리할 수 있습니다.

절차

1단계 **Network(네트워크) > Routing(라우팅)**을 선택합니다.

2단계 생성할 정적 경로의 유형(IPv4 또는 IPv6)에 대해 **Add Route(경로 추가)**를 클릭합니다.

3단계 경로의 이름을 입력합니다.

4단계 대상 IP 주소를 입력합니다.

5단계 게이트웨이 IP 주소를 입력합니다.

6단계 변경 사항을 제출하고 커밋합니다.

기본 게이트웨이 구성

CLI에서 `setgateway` 명령을 사용하거나 다음 절차를 사용하여 기본 게이트웨이를 구성할 수 있습니다.

절차

1단계 **Network(네트워크) > Routing(라우팅)**을 선택합니다.

2단계 수정할 인터넷 프로토콜 버전의 경로 목록에서 **Default Route(기본 경로)**를 클릭합니다.

3단계 게이트웨이 IP 주소를 변경합니다.

4단계 변경 사항을 제출하고 커밋합니다.

SSL 설정 구성

SSL 구성 설정 페이지 또는 `sslconfig` 명령을 사용하여 어플라이언스의 SSL 설정을 구성할 수 있습니다.

절차

1단계 **System Administration(시스템 관리) > SSL Configuration Settings(SSL 구성 설정)**를 클릭합니다.

2단계 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 요건에 따라 다음을 수행합니다.

- GUI HTTPS SSL 설정을 지정합니다. GUI HTTPS에서 사용할 SSL 방법과 암호를 지정합니다.
- 인바운드 SMTP SSL 설정을 지정합니다. 인바운드 SMTP에서 사용할 SSL 방법과 암호를 지정합니다.
- 아웃바운드 SMTP SSL 설정을 지정합니다. 아웃바운드 SMTP에서 사용할 SSL 방법과 암호를 지정합니다.

참고 SSL v2 및 TLS v1 방법을 동시에 사용할 수 없습니다. 그러나 SSL v3 방법과 함께 이러한 방법을 사용할 수 있습니다.

4단계 **Submit(제출)**을 클릭합니다.

5단계 **Commit Changes(변경 사항 커밋)**를 클릭합니다.

보안 강화를 위해 SSLv3 비활성화

보안 강화를 위해 다음과 같은 서비스에 대해 SSLv3를 비활성화할 수 있습니다.

- 업데이터
- URL 필터링
- 최종 사용자 격리
- LDAP

CLI에서 `sslv3config` 명령을 사용하여 위의 서비스에 대해 SSLv3를 활성화하거나 비활성화할 수 있습니다. 다음 예에서는 최종 사용자 격리에 대해 SSLv3를 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 선택하거나, GUI의 시스템 관리 메뉴의 표준 시간대 또는 시간 설정 페이지를 사용하거나, CLI에서 `ntpconfig`, `settime` 및 `settz` 명령을 사용합니다.

또한 **System Administration(시스템 관리) > Time Settings(시간 설정)** 페이지에서 또는 `tzupdate` CLI 명령을 사용하여 AsyncOS가 사용하는 표준 시간대 파일을 확인할 수 있습니다.

표준 시간대 선택

표준 시간대 페이지(GUI의 시스템 관리 메뉴를 통해 사용 가능)에 어플라이언스의 표준 시간대가 표시됩니다. 특정 표준 시간대 또는 GMT 오프셋을 선택할 수 있습니다.

절차

1단계 **System Administration(시스템 관리) > Time Zone(표준 시간대)** 페이지에서 **Edit Settings(설정 편집)**를 클릭합니다.

2단계 풀다운 메뉴에서 지역, 국가, 표준 시간대를 선택합니다.

3단계 변경 사항을 제출하고 커밋합니다.

GMT 오프셋 선택

절차

1단계 **System Administration(시스템 관리) > Time Zone(표준 시간대)** 페이지에서 **Edit Settings(설정 편집)**를 클릭합니다.

2단계 지역 목록에서 GMT 오프셋을 선택합니다.

3단계 표준 시간대 목록에서 오프셋을 선택합니다. 오프셋은 GMT(본초 자오선)에 도달하기 위해 더하거나 빼야 하는 시간을 나타냅니다. 앞에 뺄셈 기호("-")가 표시된 시간은 본초 자오선의 동쪽입니다. 덧셈 기호("+")는 본초 자오선의 서쪽을 나타냅니다.

4단계 변경 사항을 제출하고 커밋합니다.

시간 설정 편집

다음과 같은 방법 중 하나를 사용하여 어플라이언스의 시간 설정을 편집할 수 있습니다.

- NTP(Networking Time Protocol) 사용
- 수동으로

NTP(Network Time Protocol)를 사용하여 어플라이언스 시스템 시간 설정

절차

1단계	System Administration(시스템 관리) > Time Settings(시간 설정) 페이지로 이동합니다.
2단계	**Edit Settings(설정 편집)**를 클릭합니다.
3단계	시간 유지 방법 섹션에서 Use Network Time Protocol(Network Time Protocol 사용)을 선택합니다.
4단계	NTP 서버 주소를 입력하고 **Add Row(행 추가)**를 클릭합니다. 여러 NTP 서버를 추가할 수 있습니다.
5단계	목록에서 NTP 서버를 삭제하려면 해당 서버의 휴지통 아이콘을 클릭합니다.
6단계	NTP 쿼리에 사용할 인터페이스를 선택합니다. 이는 NTP 쿼리를 시작해야 하는 IP 주소입니다.
7단계	변경 사항을 제출하고 커밋합니다.

수동으로 어플라이언스 시스템 시간 설정

절차

1단계	System Administration(시스템 관리) > Time Settings(시간 설정) 페이지로 이동합니다.
2단계	**Edit Settings(설정 편집)**를 클릭합니다.
3단계	시간 유지 방법 섹션에서 Set Time Manually(수동으로 시간 설정)를 선택합니다.
4단계	월, 일, 연도, 시, 분, 초를 입력합니다.
5단계	A.M 또는 P.M을 선택합니다.
6단계	변경 사항을 제출하고 커밋합니다.

보기 사용자 지정

- 즐겨 찾는 페이지 사용, 33-59페이지
- 사용자 환경 설정 지정, 33-59페이지

즐겨 찾는 페이지 사용

(로컬에서 인증된 관리자만) 가장 많이 사용하는 페이지의 빠른 액세스 목록을 생성할 수 있습니다.

변경 후	수행할 작업
즐겨찾기 목록에 페이지 추가	추가할 페이지로 이동한 다음 창의 오른쪽 상단 근처에 있는 내 즐겨찾기 메뉴에서 **Add This Page To My Favorites(이 페이지를 내 즐겨찾기에 추가)**를 선택합니다. 내 즐겨찾기를 변경할 경우에는 커밋이 필요하지 않습니다.
즐겨찾기 재정렬	**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.
즐겨 찾는 페이지로 이동	창의 오른쪽 상단 근처에 있는 **내 즐겨찾기** 메뉴에서 페이지를 선택합니다.
사용자 지정 보고 페이지 보기 또는 구성	내 보고서 페이지, 28-5페이지를 참조하십시오.

사용자 환경 설정 지정

로컬 사용자는 언어 등의 환경 설정을 각 계정에 고유하게 정의할 수 있습니다. 이러한 설정은 사용자가 어플라이언스에 처음으로 로그인할 때 기본적으로 적용됩니다. 환경 설정은 각 사용자에 대해 저장되며 사용자가 어플라이언스에 로그인하는 클라이언트 머신에 관계없이 동일합니다.

사용자가 이러한 설정을 변경하되 변경 사항을 커밋하지 않을 경우 다시 로그인하면 설정이 기본값으로 되돌아갑니다.

참고 외부에서 인증된 사용자는 이 기능을 사용할 수 없습니다. 이러한 사용자는 옵션 메뉴에서 직접 언어를 선택할 수 있습니다.

절차

1단계 환경 설정을 정의할 사용자 계정으로 어플라이언스에 로그인합니다.

2단계 **Options(옵션) > Preferences(환경 설정)**를 선택합니다. 이 옵션 메뉴는 창의 오른쪽 상단에 있습니다.

3단계 **Edit Preferences(환경 설정 편집)**를 클릭합니다.

4단계 설정을 구성합니다.

환경 설정	설명
표시 언어	AsyncOS for Web이 웹 인터페이스와 CLI에서 사용하는 언어입니다.
Landing Page	사용자가 어플라이언스에 로그인하면 표시되는 페이지입니다.

환경 설정	설명
표시되는 보고 시간 범위(기본값)	Reporting(보고) 탭의 보고서에 대해 표시되는 기본 시간 범위입니다.
표시되는 보고 행 수	각 보고서에 대해 기본적으로 표시되는 데이터의 행 수입니다.

5단계 변경 사항을 제출하고 커밋합니다.

6단계 페이지 하단에서 **Return to previous page(이전 페이지로 돌아가기)** 링크를 클릭합니다.

Internet Explorer 호환성 모드 재정의

더 나은 웹 인터페이스 렌더링을 위해 Cisco에서는 Internet Explorer Compatibility Mode Override(Internet Explorer 호환성 모드 재정의)를 활성화할 것을 권장합니다.

참고 이 기능을 활성화하는 것이 조직의 정책에 어긋날 경우 이 기능을 비활성화할 수 있습니다.

절차

1단계 System **Administration(시스템 관리) > General Settings(일반 설정)**를 클릭합니다.

2단계 **Override IE Compatibility Mode(IE 호환성 모드 재정의)** 확인란을 선택합니다.

3단계 변경 사항을 제출하고 커밋합니다.

34 장

CLI를 통한 관리 및 모니터링

CLI를 통한 관리 및 모니터링 개요

CLI를 통한 Email Security 어플라이언스를 관리 및 모니터링하는 데에는 다음 유형의 작업이 포함됩니다.

- 메시지 작업 모니터링.
  - 어플라이언스가 이메일 파이프라인에서 처리하는 메시지, 수신자 및 바운스 수신자의 실제 수
  - 최근 1분, 5분 또는 15분 간격으로 메시지를 전달하고 메시지를 바운스하는 시간당 비율
- 시스템 리소스 모니터링. 예:
  - 메모리 사용량
  - 디스크 공간
  - 연결 수
- SNMP(Simple Network Management Protocol)를 사용하여 확인할 수 있는 시스템 기능 장애 모니터링. 예:
  - 팬 고장
  - 업데이트 실패
  - 비정상적으로 높은 어플라이언스 온도
- 파이프라인에 있는 이메일 관리. 예:
  - 큐에 있는 수신자 삭제
  - 다른 호스트로 메시지 리디렉션
  - 수신자를 삭제하거나 메시지를 리디렉션하여 큐 지우기
  - 이메일 수신, 전달 또는 작업 큐 처리를 일시 중단 또는 다시 시작
  - 특정 메시지 찾기

모니터링 가능한 구성 요소 읽기

이벤트 카운터 읽기

카운터는 시스템에서 실행 중인 총 이벤트 수를 제공합니다. 각 카운터에서는 카운터가 재설정된 이후, 마지막 시스템 재부팅 이후, 시스템 수명 주기 동안 발생한 총 이벤트 수를 확인할 수 있습니다.

카운터는 이벤트가 발생할 때마다 증가하며 다음의 3가지 버전으로 표시됩니다.

초기화	`resetcounters` 명령을 사용하여 마지막 카운터가 재설정된 이후
실행 시간	마지막 시스템 재부팅 이후
수명 주기	Cisco 어플라이언스의 수명 주기 동안 발생한 총 이벤트 수

표 34-1은 Cisco 어플라이언스를 모니터링할 때 사용할 수 있는 카운터와 이에 대한 설명을 나열한 것입니다.

참고 이것은 전체 목록입니다. 선택한 표시 옵션 또는 명령에 따라 표시되는 카운터가 달라집니다. 이 목록은 참조용으로만 사용합니다.

표 34-1 카운터

통계	설명
수신	
수신 메시지	전송 큐로 수신되는 메시지입니다.
수신된 수신자	모든 수신된 메시지의 수신자입니다.
생성된 바운스 수신자	시스템에서 생성되어 전송 큐에 삽입된 바운스의 수신자입니다.

표 34-1 카운터 (계속)

통계	설명
거부	
거부된 수신자	RAT(Recipient Access Table) 또는 예상치 않은 프로토콜 협상(중간에 연결이 종료된 경우 포함)으로 인해 전송 큐로의 수신이 거부된 수신자입니다.
삭제(drop)된 메시지	필터 삭제 작업과 일치하여 전송 큐로의 수신이 거부되었거나 Black Hole 큐잉 리스너에서 수신된 메시지입니다. 별칭 테이블에서 `/dev/null` 항목으로 전달된 메시지도 삭제된 메시지로 간주됩니다. 안티스팸 필터링(시스템에서 활성화된 경우)을 통해 메시지가 삭제되는 경우 카운터가 증가합니다.
큐	
소프트 바운스 이벤트	소프트 바운스 이벤트 수를 나타내며 여러 번 소프트 바운스된 메시지는 여러 소프트 바운스 이벤트를 가집니다.
완료	
완료된 수신자	하드 바운스된 모든 수신자, 전달된 수신자 및 삭제된 수신자의 총 수를 나타냅니다. 전송 큐에서 제거된 모든 수신자입니다.
하드 바운스 수신자	모든 DNS 하드 바운스, 5XX 하드 바운스, 필터 하드 바운스, 만료된 하드 바운스 및 기타 하드 바운스의 총 수를 나타냅니다. 수신자로의 메시지 전달에 실패한 것으로, 해당 메시지 전달이 즉시 종료됩니다.
DNS 하드 바운스	수신자에게 메시지 전달을 시도하는 중에 DNS 오류가 발생했습니다.
5XX 하드 바운스	수신자에게 메시지 전달을 시도하는 중에 대상 메일 서버에서 "5XX" 응답 코드를 반환했습니다.
만료된 하드 바운스	전송 큐에서 허용되는 최대 시간 또는 최대 연결 시도 수를 초과한 메시지 수신자입니다.
필터 하드 바운스	일치하는 필터의 `bounce` 작업을 통해 수신자 전달을 선취했습니다. 안티스팸 필터링(시스템에서 활성화된 경우)을 통해 메시지가 삭제되는 경우 카운터가 증가합니다.
기타 하드 바운스	메시지 전송 중 예기치 않은 오류가 발생했거나 메시지 수신자가 `bouncerecipients` 명령을 통해 명시적으로 바운스되었습니다.
전달된 수신자	메시지가 수신자에게 성공적으로 전달되었습니다.
삭제된 수신자	`deleterecipients` 명령을 통해 명시적으로 삭제된 총 메시지 수신자 수 또는 전역 가입 취소 횟수입니다.
전역 가입 취소 횟수	일치하는 전역 가입 취소 설정으로 메시지 수신자가 삭제되었습니다.
현재 ID	
메시지 ID(MID)	마지막 메시지 ID가 전송 큐에 삽입된 메시지에 할당되었습니다. MID는 Cisco 어플라이언스에서 수신한 모든 메시지와 연결되며 메일 로그에서 추적할 수 있습니다. MID는 2^{31}에서 0으로 재설정됩니다.

표 34-1 카운터 (계속)

통계	설명
수신 연결 ID(ICID)	리스너 인터페이스에 대한 연결에 할당된 마지막 수신 연결 ID입니다. ICID는 2^{31}에서 롤오버됩니다(0으로 재설정).
전송 연결 ID(DCID)	대상 메일 서버에 대한 연결에 할당된 마지막 전송 연결 ID입니다. DCID는 2^{31}에서 롤오버됩니다(0으로 재설정).

시스템 게이지 읽기

게이지는 메모리, 디스크 공간 또는 활성 연결과 같은 시스템 리소스의 현재 사용률을 보여줍니다.

표 34-2는 Cisco 어플라이언스를 모니터링할 때 사용할 수 있는 게이지와 이에 대한 설명을 나열한 것입니다.

참고 이것은 전체 목록입니다. 선택하는 표시 옵션 또는 명령에 따라 표시되는 게이지가 달라집니다. 이 목록은 참조용으로만 사용합니다.

표 34-2 게이지

통계	설명
시스템 게이지	
RAM 사용률	시스템에서 사용되는 물리적인 RAM(Random Access Memory)의 백분율입니다.
CPU 사용률	CPU 사용량의 백분율입니다.
디스크 I/O 사용률	사용 중인 디스크 I/O의 백분율입니다. **참고** 디스크 I/O 사용률 게이지는 알려진 값의 범위에 대한 측정값을 표시하지 않습니다. 대신, 지금까지 시스템이 보여준 I/O 사용률과 마지막 재부팅 이후 최대 값의 범위를 표시합니다. 게이지가 100%를 표시하는 경우, 시스템은 재부팅 이후 최고 수준의 I/O 사용률을 기록하고 있다는 의미입니다(전체 시스템의 물리적 디스크 I/O가 100%임을 나타내는 것은 아님).
리소스 보존(conservation)	`0~60` 또는 `999`입니다. `0~60`은 중요한 시스템 리소스가 빠르게 소모되는 것을 방지하기 위해 시스템에서 메시지 수락을 감소시키는 정도를 나타냅니다. 숫자가 높을수록 메시지 수락 감소 수준이 높습니다. 0은 메시지 수락이 감소하지 않음을 나타냅니다. 이 게이지가 `999`를 표시하면 시스템에서 "리소스 보존 모드"가 시작되어 메시지를 수락하지 않습니다. 알림 메시지는 시스템의 리소스 보존 모드 시작 또는 종료와 관계 없이 언제든지 전송됩니다.
디스크 사용률: 로그	로그에 사용 중인 디스크의 백분율로, 상태 로그에서는 `LogUsd`로 표시되고 XML 상태에서는 `log_used`로 표시됩니다.

표 34-2 게이지 (계속)

통계	설명
연결 게이지	
현재 인바운드 연결	리스너 인터페이스에 대한 현재 인바운드 연결입니다.
현재 아웃바운드 연결	대상 메일 서버에 대한 현재 아웃바운드 연결입니다.
큐 게이지	
활성 수신자	전송 큐의 메시지 수신자입니다. 전달을 시도하지 않은 수신자와 전달을 시도했던 수신자의 총 수입니다.
전달을 시도하지 않은 수신자	활성 수신자의 하위 범주입니다. 전달을 아직 시도하지 않은 큐에 있는 메시지 수신자입니다.
전달을 시도했던 수신자	활성 수신자의 하위 범주입니다. 전달을 시도했지만 소프트 바운스 이벤트 때문에 실패한 큐에 있는 메시지 수신자입니다.
작업 큐에 있는 메시지	별칭 테이블 확장, 마스커레이드, 안티스팸, 안티바이러스 검사, 메시지 필터 및 큐에 저장되기 전의 LDAP 쿼리로 처리되기 위해 대기 중인 메시지 수입니다.
격리에 있는 메시지	격리에 있는 메시지의 수를 나타내며, 릴리스되었거나 삭제되었지만 아직 적용되지 않은 메시지의 수를 나타냅니다. 예를 들어, 신종 바이러스로부터 격리된 모든 메시지를 릴리스하는 경우 신종 바이러스에 대한 총 메시지 수는 즉시 0이 되지만 해당 메시지가 모두 전달될 때까지 이 필드에는 격리된 메시지가 반영됩니다.
메모리에 있는 대상	메모리에 있는 대상 제어의 수입니다. 전달해야 하는 메시지가 있는 도메인마다 대상 객체가 메모리에 생성됩니다. 해당 도메인으로 보내는 모든 메일이 전달된 후 대상 객체는 추가로 3시간 더 보관됩니다. 3시간 후에 새 메시지가 해당 도메인으로 바인딩되지 않으면, 객체는 만료되어 대상에 대해 더 이상 보고하지 않습니다 (예: `tophosts` 명령). 단일 도메인에만 메일을 전달하는 경우, 이 카운터는 "1"이 됩니다. 메시지를 수신하거나 전송하지 않은 경우 (또는 오랜 시간 동안 어플라이언스에서 메시지를 처리하지 않은 경우), 카운터는 "0"이 됩니다. 가상 게이트웨이를 사용하는 경우 각 가상 게이트웨이의 대상 제어는 개별 대상 객체를 갖습니다. 예를 들어, 각기 다른 3가지 가상 게이트웨이에서 yahoo.com으로 전달 중인 경우 yahoo.com은 대상 객체 3개로 카운트합니다.
사용된 킬로바이트	사용된 큐 스토리지(킬로바이트)입니다.
격리 상태의 킬로바이트	격리된 메시지에 사용된 큐 스토리지입니다. 이 값은 메시지 크기에 각 수신자별로 30바이트를 더하여 계산되며 위에서 계산한 것과 마찬가지로 "격리 상태의 메시지"에 대해 총계가 계산됩니다. 일반적으로 사용된 공간보다 *더 크게 계산됩니다.*
사용 가능한 킬로바이트	나머지 큐 스토리지(킬로바이트)입니다.

전달 및 바운스된 메시지 비율 읽기

모든 비율은 쿼리가 생성되는 시점에 평균적인 시간당 이벤트 발생 비율로 표시됩니다. 비율은 3가지 시간 간격을 통해 계산되며 시간당 평균 비율은 지난 1분, 지난 5분 및 지난 15분을 기준으로 계산됩니다.

예를 들어 Cisco 어플라이언스가 1분에 100명의 수신자를 수신하는 경우 1분간의 비율은 시간당 6,000이 됩니다. 5분간의 비율은 시간당 1,200이고 15분 간의 비율은 시간당 400이 됩니다. 1분간의 비율이 계속되는 경우 시간당 평균 비율이 얼마인지를 알기 위해 비율이 계산됩니다. 따라서, 1분 동안 메시지 100개를 수신하는 것이 15분 동안 메시지 100개를 수신하는 것보다 비율이 높습니다.

표 34-3은 Cisco 어플라이언스를 모니터링할 때 사용할 수 있는 비율과 이에 대한 설명을 나열한 것입니다.

참고 이것은 전체 목록입니다. 선택하는 표시 옵션 또는 명령에 따라 표시되는 비율이 달라집니다. 이 목록은 참조용으로만 사용합니다.

표 34-3 비율

통계	설명
수신 메시지	시간당 전송 큐에 삽입되는 메시지 비율입니다.
수신된 수신자	시간당 전송 큐에 삽입되는 모든 메시지에 대한 수신자 수를 나타내는 비율입니다.
소프트 바운스 이벤트	시간당 소프트 바운스 이벤트 수를 나타내는 비율입니다. (여러 번 소프트 바운스된 메시지는 여러 소프트 바운스 이벤트를 가집니다.)
완료된 수신자	하드 바운스된 모든 수신자, 전달된 수신자 및 삭제된 수신자의 총 수를 나타내는 비율입니다. 전송 큐에서 제거된 모든 수신자는 완료된 것으로 간주됩니다.
하드 바운스 수신자	모든 DNS 하드 바운스, 5XX 하드 바운스, 필터 하드 바운스, 만료된 하드 바운스 및 기타 하드 바운스의 총 수를 나타내는 비율입니다. 수신자로의 메시지 전달에 실패한 것으로 해당 메시지 전달이 즉시 종료되고 하드 바운스됩니다.
전달된 수신자	시간당 수신자에게 성공적으로 전달되는 메시지의 비율입니다.

CLI를 사용한 모니터링

이메일 상태 모니터링

Cisco 어플라이언스에서 이메일 작업 상태를 모니터링할 수 있습니다. status 명령은 이메일 작업에 대해 모니터링된 정보의 하위 집합을 반환합니다. 반환된 통계는 두 가지 유형(카운터와 게이지)으로 표시됩니다. 카운터는 시스템에서 실행 중인 총 이벤트 수를 제공합니다. 각 카운터에서는 카운터가 재설정된 이후, 마지막 시스템 재부팅 이후, 시스템 수명 주기 동안 발생한 총 이벤트 수를 확인할 수 있습니다. 게이지는 메모리, 디스크 공간 또는 활성 연결과 같은 시스템 리소스의 현재 사용률을 보여줍니다.

각 항목에 대한 자세한 설명은 CLI를 통한 관리 및 모니터링 개요, 34-1페이지 항목을 참조하십시오.

표 34-4 메일 상태

통계	설명
현재 시간	현재 시스템 시간과 날짜를 표시합니다.
마지막 카운터 재설정	카운터가 재설정된 마지막 시간을 표시합니다.
시스템 상태	온라인, 오프라인, 수신 일시 중단됨 또는 전달 일시 중단됨 상태를 표시합니다. *모든 리스너가* 일시 중단된 경우에만 "수신 일시 중단됨" 상태가 됩니다. *모든 리스너에 대해* 수신 및 전달이 일시 중단된 경우 "오프라인" 상태가 됩니다.
가장 오래된 메시지	시스템에서 전달되기 위해 대기 중인 가장 오래된 메시지를 표시합니다.
기능	featurekey 명령을 사용하여 시스템에 설치되어 있는 모든 특수한 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>
```

상세한 이메일 상태 모니터링

`status detail` 명령은 이메일 작업에 대해 모니터링된 전체 정보를 반환합니다. 반환된 통계는 세 가지 범주(카운터, 비율 및 게이지)로 표시됩니다. 카운터는 시스템에서 실행 중인 총 이벤트 수를 제공합니다. 각 카운터에서는 카운터가 재설정된 이후, 마지막 시스템 재부팅 이후, 시스템 수명 주기 동안 발생한 총 이벤트 수를 확인할 수 있습니다. 게이지는 메모리, 디스크 공간 또는 활성 연결과 같은 시스템 리소스의 현재 사용률을 보여줍니다. 모든 비율은 쿼리가 생성되는 시점에 평균적인 시간당 이벤트 발생 비율로 표시됩니다. 비율은 3가지 시간 간격을 통해 계산되며 시간당 평균 비율은 지난 1분, 지난 5분 및 지난 15분을 기준으로 계산됩니다. 각 항목에 대한 자세한 설명은 CLI를 통한 관리 및 모니터링 개요, 34-1페이지 항목을 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 새롭게 설치된 어플라이언스에는 가장 오래된 메시지 카운터에서 메시지를 보여주는 경우도 있지만 실제로는 카운터에 수신자가 표시되지 않습니다. 원격 호스트가 연결 중이며 메시지를 매우 느리게 수신하고 있는 경우(즉 메시지를 수신하는 데 몇 분이 소요됨) 수신된 수신자의 카운터는 "0"을 표시하지만 가장 오래된 메시지 카운터는 "1"을 표시할 수 있습니다. 이는 가장 오래된 메시지 카운터가 진행 중인 메시지를 표시하기 때문입니다. 카운터는 연결이 최종적으로 삭제되는 경우 재설정됩니다.

메일 호스트 상태 모니터링

특정 수신자 호스트에 전달 문제가 있다고 의심되거나 가상 게이트웨이 주소에 대한 정보를 수집하려는 경우, `hoststatus` 명령을 사용합니다. `hoststatus` 명령은 특정 수신자 호스트와 관련된 이메일 작업에 대한 모니터링 정보를 반환합니다. 이 명령을 실행하는 경우 반환될 호스트 정보의 도메인을 입력해야 합니다. AsyncOS 캐시에 저장된 DNS 정보 및 수신자 호스트에서 반환된 마지막 오류도 제공됩니다. 반환되는 데이터는 마지막 `resetcounters` 명령이 실행된 후 계속 누적됩니다. 반환되는 통계는 두 가지 범주(카운터 및 게이지)로 표시됩니다. 각 항목에 대한 자세한 설명은 CLI를 통한 관리 및 모니터링 개요, 34-1페이지 항목을 참조하십시오.

또한 `hoststatus` 명령에 관련된 기타 데이터가 반환됩니다.

표 34-5 hoststatus 명령의 추가 데이터

통계	설명
보류 중인 아웃바운드 연결	열린 연결 및 작업 중인 연결과는 다른, 대상 메일 호스트에 대한 보류 중인 연결 또는 "원시" 연결입니다. 보류 중인 아웃바운드 연결은 프로토콜 시작 단계에 아직 도달하지 않은 연결입니다.
가장 오래된 메시지	이 도메인의 전송 큐에서 가장 오래된 활성 수신자의 사용 기간입니다. 이 카운터는 소프트 바운스 이벤트 및/또는 다운된 호스트로 인해 전달될 수 없는 큐에 있는 메시지의 사용 기간을 판별하는 데 유용합니다.
최근 활동	이 필드는 해당 호스트로 메시지 전달이 시도될 때마다 업데이트됩니다.
정렬된 IP 주소	이 필드에는 IP 주소에 대한 TTL(Time to Live), MX 코드에 따른 기본 설정 및 실제 주소가 포함됩니다. MX 레코드는 도메인의 메일 서버 IP 주소를 지정합니다. 도메인에는 여러 MX 레코드를 가질 수 있습니다. 각 MX 레코드 메일 서버에는 우선순위가 지정되어 있습니다. 가장 우선순위가 낮은 MX 레코드에는 기본 설정이 지정됩니다.
최근 5XX 오류	이 필드에는 호스트가 반환한 가장 최근의 "5XX" 상태 코드 및 설명이 포함됩니다. 이 필드는 5XX 오류가 있는 경우에만 표시됩니다.
MX 레코드	MX 레코드는 도메인의 메일 서버 IP 주소를 지정합니다. 도메인에는 여러 MX 레코드를 가질 수 있습니다. 각 MX 레코드 메일 서버에는 우선순위가 지정되어 있습니다. 가장 우선순위가 낮은 MX 레코드에는 기본 설정이 지정됩니다.
이 호스트의 SMTP 경로	이 도메인의 SMTP 경로가 정의된 경우 해당 경로가 여기에 나열됩니다.
최근 TLS 오류	이 필드에는 어플라이언스가 설정하려고 시도한 TLS 연결 유형과 가장 최근의 발송 TLS 연결 오류에 대한 설명이 포함됩니다. 이 필드는 TLS 오류가 있는 경우에만 표시됩니다.

가상 게이트웨이

다음의 가상 게이트웨이 정보는 가상 게이트웨이 주소(이메일을 수신하도록 게이트웨이 구성 참조)를 설정한 경우에만 표시됩니다.

표 34-6 hoststatus 명령의 추가 가상 게이트웨이 데이터

통계	설명
호스트 up/down	가상 게이트웨이 주소별로 추적되는 동일한 이름의 전역 `hoststatus` 필드와 동일하게 정의됩니다.
최근 활동	가상 게이트웨이 주소별로 추적되는 동일한 이름의 전역 `hoststatus` 필드와 동일하게 정의됩니다.
수신자	이 필드는 전역 `hoststatus` 명령과 동일하게 정의됩니다. 활성 수신자 필드는 가상 게이트웨이 주소별로 추적됩니다.
최근 5XX 오류	이 필드에는 호스트가 반환한 가장 최근의 5XX 상태 코드 및 설명이 포함됩니다. 이 필드는 5XX 오류가 있는 경우에만 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 가상 게이트웨이 주소 정보는 `altsrchost` 기능을 사용하는 경우에만 나타납니다.

이메일 큐의 구성 확인

이메일 큐에 대한 실시간 정보를 얻고 특정한 수신자 호스트에 전달 문제(예: 큐 생성)가 있는지 확인하려면 `tophosts` 명령을 사용합니다. `tophosts` 명령은 큐에 있는 상위 20개의 수신자 호스트 목록을 반환합니다. 이 목록은 활성 수신자, 발송 연결, 전달된 수신자, 소프트 바운스 이벤트 및 하드 바운스 수신자 등 다양한 통계를 사용하여 정렬할 수 있습니다. 각 항목에 대한 자세한 설명은 CLI를 통한 관리 및 모니터링 개요, 34-1페이지 항목을 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 시스템에서 이메일 작업의 진행 상태를 확인할 수 있도록 실시간 모니터링 기능을 제공합니다. `rate` 명령은 이메일 작업에 대한 실시간 모니터링 정보를 반환합니다. 이 정보는 지정한 주기적인 간격으로 업데이트됩니다. `rate` 명령을 중지하려면 Control-C를 사용합니다.

표시된 데이터는 표 34-7에 나열되어 있습니다.

표 34-7 rate 명령의 데이터

통계	설명
인바운드 연결	인바운드 연결 수입니다.
아웃바운드 연결	아웃바운드 연결 수입니다.
수신된 수신자	시스템에 수신된 총 수신자 수입니다.
완료된 수신자	완료된 총 수신자 수입니다.
델타	마지막 데이터 업데이트 이후 수신된 수신자와 완료된 수신자의 차이 변화입니다.
사용된 큐	메시지 큐의 크기(킬로바이트)입니다.

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. (상세한 이메일 상태 모니터링, 34-8페이지 참조.)

표 34-8 hostrate 명령의 데이터

통계	설명
호스트 상태	특정 호스트의 현재 상태로 up, down 또는 unknown으로 표시됩니다.
현재 아웃바운드 연결	호스트에 대한 현재 아웃바운드 연결 수입니다.
큐에 있는 활성 수신자	큐에 있는 특정 호스트에 대한 총 활성 수신자 수입니다.
큐에 있는 활성 수신자 델타	마지막 호스트 상태 이후 큐에 있는 특정 호스트에 대한 총 활성 수신자 수의 차이입니다.
전달된 수신자 델타	마지막 호스트 상태 이후 큐에 있는 특정 호스트에 대한 총 전달된 수신자 수의 차이입니다.

표 34-8 hostrate 명령의 데이터 (계속)

통계	설명
하드 바운스 수신자 델타	마지막 호스트 상태 이후 큐에 있는 특정 호스트에 대한 총 하드 바운스된 수신자 수의 차이입니다.
소프트 바운스 이벤트 델타	마지막 호스트 상태 이후 큐에 있는 특정 호스트에 대한 총 소프트 바운스된 수신자 수의 차이입니다.

hostrate 명령을 중지하려면 Control-C를 사용합니다.

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

대량 발신자를 확인하거나 시스템의 인바운드 연결 문제를 해결하기 위해 Cisco 어플라이언스에 연결되어 있는 호스트를 모니터링할 수 있습니다. `topin` 명령은 시스템에 연결된 원격 호스트의 스냅샷을 제공합니다. 스냅샷은 특정 리스너에 연결된 각 원격 IP 주소가 포함된 행이 하나 있는 테이블을 표시합니다. 동일한 IP 주소에서 각기 다른 리스너로 2가지 연결을 하는 경우 테이블에 행 2개가 생성됩니다. 표 34-9는 `topin` 명령을 사용할 때 표시되는 필드에 대한 설명입니다.

표 34-9 topin 명령의 데이터

통계	설명
원격 호스트 이름	역방향 DNS 조회로 얻은 원격 호스트의 호스트 이름입니다.
원격 IP 주소	원격 호스트의 IP 주소입니다.
리스너	연결을 수신 중인 Cisco 어플라이언스에 있는 리스너의 별칭입니다.
인바운드 연결	명령 실행 시 지정된 IP 주소가 열려 있는 원격 호스트의 동시 연결 수입니다.

시스템은 역방향 DNS 조회를 수행하여 원격 호스트 이름을 찾은 다음 포워드 DNS 조회를 수행하여 이름을 검증합니다. 포워드 조회 결과 원래 IP 주소가 조회되지 않거나 역방향 DNS 조회에 실패할 경우 테이블의 호스트 이름 열에 IP 주소가 표시됩니다. 발신자 확인 프로세스에 대한 자세한 정보는 발신자 확인, 7-27페이지 항목을 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 카운터 표시 통계를 반환합니다. 각 카운터에서 카운터가 마지막으로 재설정된 이후, 마지막 시스템 재부팅 이후 그리고 시스템 수명 전체 동안의 총 이벤트 수를 확인할 수 있습니다.

표 34-10은 사용 가능한 카운터를 나열합니다.

표 34-10 dnsstatus 명령의 데이터

통계	설명
DNS 요청	도메인 이름을 해석하기 위해 시스템 DNS 캐시에 보내는 반복되지 않는 최상위 요청입니다.
네트워크 요청	DNS 정보를 검색하기 위해 네트워크(비로컬)에 보내는 요청입니다.
캐시 성공률	레코드가 발견 및 반환되는 DNS 캐시에 보내는 요청입니다.
캐시 실패	레코드가 발견되지 않은 DNS 캐시에 보내는 요청입니다.

표 34-10 dnsstatus 명령의 데이터 (계속)

통계	설명
캐시 예외 사항	레코드는 발견되었지만 도메인을 알 수 없는 DNS 캐시에 보내는 요청입니다.
캐시 만료	레코드가 발견되어 사용하려고 했지만 너무 오래되어 삭제된 DNS에 캐시에 보내는 요청입니다. 여러 항목이 TTL(Time to Live)을 초과한 경우에도 캐시에 존재할 수 있습니다. 이 항목을 사용하지 않는 한, 만료 카운터에 포함되지 않습니다. 캐시가 플러시되는 경우 유효한 항목과 유효하지 않은 항목(너무 오래됨)이 모두 삭제됩니다. 플러시 작업으로 인해 만료 카운터가 변경되지 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 누적 이메일 모니터링 카운터를 재설정합니다. 재설정은 호스트 카운터뿐만 아니라 전역 카운터에도 영향을 줍니다. 재설정은 재시도 일정과 관련하여 전송 큐에 있는 메시지의 카운터에는 영향을 주지 않습니다.

참고 또한 GUI에서 카운터를 재설정할 수 있습니다. 시스템 상태 페이지, 28-28페이지 항목을 참조하십시오.

예

```
mail3.example.com> resetcounters


Counters reset: Mon Jan 01 12:00:01 2003
```

활성 TCP/IP 서비스 확인

Email Security 어플라이언스에서 사용되는 활성 TCP/IP 서비스를 확인하려면 CLI의 `tcpservices` 명령을 사용합니다.

이메일 큐 관리

Cisco AsyncOS에서는 이메일 큐에 있는 메시지에 작업을 수행할 수 있습니다. 이메일 큐에 있는 메시지를 삭제, 바운스, 일시 중단 또는 리디렉션할 수 있습니다. 또한 큐에 있는 이전 메시지를 찾고 제거하고 보관할 수 있습니다.

큐에 있는 수신자 삭제

특정 수신자가 전달 중이 아니거나 이메일 큐를 지우려면 `deleterecipients` 명령을 사용합니다. `deleterecipients` 명령을 사용하면 전달 대기 중인 특정한 수신자를 삭제하여 이메일 전송 큐를 관리할 수 있습니다. 삭제할 수신자는 수신자가 향하는 수신자 호스트 또는 메시지 봉투의 Envelope From에 지정된 특정한 주소로 식별되는 메시지 발신자를 통해 식별됩니다. 또는 전송 큐(모든 활성 수신자)에 있는 모든 메시지를 한 번에 삭제할 수도 있습니다.

참고 `deleterecipients` 기능을 수행하려면 Cisco 어플라이언스를 오프라인 상태로 전환하거나 전달을 일시 중단하는 것이 좋습니다(CLI를 사용하여 어플라이언스를 오프라인으로 전환, 33-3페이지 또는 이메일 수신 및 전송 일시 중단, 33-2페이지 참조).

참고 이 기능은 모든 상태에서 지원되지만 기능이 수행되는 동안 특정한 메시지가 전달될 수 있습니다.

수신자 호스트 및 발신자 일치 항목은 동일한 문자열로 일치되어야 합니다. 와일드카드는 사용할 수 없습니다. `deleterecipients` 명령은 총 삭제된 메시지 수를 반환합니다. 또한 메일 로그 서브스크립션(IronPort 텍스트 형식만)이 구성된 경우, 메시지 삭제는 개별 행으로 로깅됩니다.

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 삭제하는 다양한 옵션을 제공합니다. 다음 예는 수신자 호스트를 사용한 수신자 삭제, Envelope From 주소를 사용한 삭제 및 큐에 있는 모든 수신자 삭제를 보여줍니다.

수신자 도메인을 통한 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.
```

봉투 발신자 주소를 통한 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.
```

큐에 있는 수신자 바운스

deleterecipients 명령과 유사하게 bouncerecipients 명령을 사용하면 전달 대기 중인 특정한 수신자를 하드 바운스하여 이메일 전송 큐를 관리할 수 있습니다. 메시지 바운스는 bounceconfig 명령에 지정된 일반적인 메시지 바운스 구성을 따릅니다.

참고 bouncerecipients 기능을 수행하려면 Cisco 어플라이언스를 오프라인 상태로 전환하거나 전달을 일시 중단하는 것이 좋습니다(CLI를 사용하여 어플라이언스를 오프라인으로 전환, 33-3페이지 또는 이메일 수신 및 전송 일시 중단, 33-2페이지 참조).

참고 이 기능은 모든 상태에서 지원되지만 기능이 수행되는 동안 특정한 메시지가 전달될 수 있습니다.

수신자 호스트 및 발신자 일치 항목은 동일한 문자열로 일치되어야 합니다. 와일드카드는 사용할 수 없습니다. bouncerecipients 명령은 총 바운스된 메시지 수를 반환합니다.

참고 bouncerecipients 기능은 리소스를 많이 사용하며 완료하는 데 몇 분이 걸릴 수 있습니다. 오프라인 또는 전달이 일시 중단된 상태인 경우, 바운스 메시지의 실제 전송(하드 바운스 생성이 설정된 경우)은 Cisco AsyncOS가 resume 명령을 통해 다시 온라인 상태로 전환된 이후에만 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 대상 수신자 호스트 또는 메시지 봉투의 Envelope From에 지정된 특정한 주소로 식별되는 메시지 발신자를 통해 식별됩니다. 또는 전송 큐에 있는 모든 메시지는 한 번에 바운스할 수 있습니다.

수신자 호스트를 통한 바운스

```
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.
```

봉투 발신자 주소를 통한 바운스

```
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 바운스

```
Are you sure you want to bounce all messages in the queue? [N]> Y


Bouncing messages, please wait.

1000 messages bounced.
```

큐에 있는 메시지 리디렉션

redirectrecipients 명령을 사용하면 이메일 전송 큐에 있는 모든 메시지를 다른 릴레이 호스트로 리디렉션할 수 있습니다. 이 호스트에서 대량의 SMTP 메일을 수락할 준비가 되어 있지 않은 IP 주소 또는 호스트에 수신자를 리디렉션하면 메시지가 바운스되어 메일이 손실될 가능성이 있습니다.

주의 대상이 /dev/null인 수신 도메인으로 메시지를 리디렉션하면 메시지가 손실됩니다. CLI는 이러한 도메인에 메일을 리디렉션하는 경우 경고를 표시하지 않습니다. 메시지를 리디렉션하기 전에 수신 도메인의 SMTP 경로를 확인합니다.

예

다음 예에서는 example2.com 호스트에 모든 메일을 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.
```

큐에 있는 수신자 기반 메시지 표시

showrecipients 명령을 사용하여 수신자 호스트 또는 Envelope From 주소별로 이메일 전송 큐의 메시지를 확인할 수 있습니다. 큐에 있는 모든 메시지도 확인할 수 있습니다.

예

다음 예는 모든 수신자 호스트의 큐에 있는 메시지를 보여줍니다.

```
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
```

이메일 전달 일시 중단

유지 보수 또는 문제 해결을 위해 이메일 전달을 일시적으로 일시 중단하려면 suspenddel 명령을 사용합니다. suspenddel 명령은 Cisco AsyncOS를 일시 중단된 전송 상태로 전환합니다. 이 상태는 다음과 같은 특징이 있습니다.

- 아웃바운드 이메일 전달이 중지됩니다.
- 인바운드 이메일 연결은 허용됩니다.
- 로그 전송이 계속됩니다.
- CLI에 액세스할 수 있습니다.

suspenddel 명령을 사용하면 열려 있는 아웃바운드 연결이 종료되고 새로운 연결이 열리는 것이 중지됩니다. suspenddel 명령은 즉시 시작되며 모든 설정된 연결을 성공적으로 종료합니다. resumedel 명령을 사용하면 전달이 일시 중단된 상태에서 일반 작업 상태로 돌아갑니다.

참고 "전달 일시 중단" 상태는 시스템이 재부팅되는 동안에 유지됩니다. suspenddel 명령을 사용한 다음 어플라이언스를 재부팅하는 경우, resumedel 명령을 사용하여 재부팅한 후에 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

resumedel 명령은 Cisco AsyncOS를 suspenddel 명령을 사용한 이후에 일반 동작 상태로 되돌립니다.

구문

```
resumedel
```

```
mail3.example.com> resumedel


Mail delivery resumed.
```

이메일 수신 일시 중단

수신 이메일의 모든 리스너를 일시적으로 일시 중단하려면 suspendlistener 명령을 사용합니다. 수신이 일시 중단되는 동안에는 시스템은 리스너의 특정 포트에 대한 연결을 수락하지 않습니다.

이 동작은 AsyncOS의 이번 릴리스에서 변경되었습니다. 이전 릴리스에서는 시스템이 연결을 수락하고 다음과 같이 응답하며 연결을 해제했습니다.

- SMTP: `421` *hostname* `Service not available, closing transaction channel`
- QMQP: `ZService not available`

참고 "수신 일시 중단" 상태는 시스템이 재부팅되는 동안에 유지됩니다. suspendlistener 명령을 사용한 다음 어플라이언스를 재부팅하는 경우, 리스너에서 메시지 수신을 다시 시작하기 전 resumelistener 명령을 사용해야 합니다.

구문

```
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

resumelistener 명령은 Cisco AsyncOS를 suspendlistener 명령을 사용한 이후에 일반 동작 상태로 되돌립니다.

구문

```
       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>
```

이메일 전달 및 수신 다시 시작

resume 명령은 전달 및 수신을 모두 다시 시작합니다.

구문

```
        resume

mail3.example.com> resume


Receiving resumed.

Mail delivery resumed.

mail3.example.com>
```

즉시 전달을 위한 이메일 예약

나중에 전달하도록 예약된 수신자 및 호스트는 delivernow 명령을 사용하여 즉시 재시도될 수 있습니다. delivernow 명령을 사용하면 큐에 있는 이메일을 즉시 전달하기 위해 일정을 재조정할 수 있습니다. 표시되어 있는 모든 도메인과 모든 예약 또는 소프트 바운스된 메시지는 즉시 전송되기 위해 큐에 대기합니다.

delivernow 명령은 큐에 있는 모든 수신자 또는 특정 수신자를 대상으로 호출될 수 있습니다(예약 및 활성 수신자). 특정 수신자를 선택할 경우, 즉시 전달하기 위해 예약하려면 수신자의 도메인 이름을 입력해야 합니다. 시스템은 전체 문자열의 문자 및 길이가 일치하는지 확인합니다.

구문

```
        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 큐 일시 중지

LDAP 수신자 액세스, 마스커레이드, LDAP 재라우팅, 메시지 필터, 안티스팸 및 안티바이러스 검사 엔진의 처리는 모두 "작업 큐"에서 수행됩니다. 처리 흐름에 대해서는 라우팅 및 전달 기능 구성, 24-1 페이지 항목을 조하고 "작업 큐에 있는 메시지"의 게이지에 대한 설명은 표 34-2(34-4페이지) 항목을 참조하십시오. `workqueue` 명령을 사용하여 메시지를 처리하는 작업 큐 일부를 수동으로 일시 중지할 수 있습니다.

예를 들어 많은 메시지가 작업 큐에 있을 때 LDAP 서버 구성을 변경하려고 하는 경우, LDAP 수신자 액세스 쿼리에 기반하여 메시지 바운스 작업을 메시지 삭제 작업으로 전환할 수 있습니다. 또는 최신 안티바이러스 검사 엔진의 정의 파일(`antivirusupdate` 명령 사용)을 수동으로 검사하면서 큐를 일시 중지할 수도 있습니다. `workqueue` 명령을 사용하면 처리를 중지하기 위해 작업 큐를 일시 중지하고 다시 시작할 수 있으며 기타 구성을 변경할 수 있습니다.

작업 큐를 일시 중지 및 다시 시작할 때 이벤트가 로깅됩니다. 예를 들면 다음과 같습니다.

```
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 예에서 작업 큐가 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 않는 경우, 시스템은 이유를 "Manually paused by user"로 기록합니다.

이 예에서 작업 큐가 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
```

이전 메시지 찾기 및 보관

이전 메시지가 전달될 수 없어 큐에 남아 있는 경우도 있습니다. 이러한 메시지를 제거하고 보관할 수 있습니다. 이 작업을 수행하려면 showmessage 명령을 사용하여 지정된 메시지 ID에 해당하는 메시지를 표시합니다. oldmessage 명령을 사용하여 시스템에서 가장 오래된 비격리 메시지를 표시합니다. 그런 다음 선택적으로 removemessage를 사용하여 지정된 메시지 ID에 해당하는 메시지를 안전하게 제거할 수 있습니다. 이 명령을 통해 작업 큐, 재시도 큐 또는 대상 큐에 있는 메시지만 제거할 수 있습니다. 메시지가 해당 모든 큐에 없는 경우 메시지를 거할 수 없습니다.

또한 archivemessage[mid] 명령을 사용하여 지정된 메시지 ID에 해당하는 메시지를 구성 디렉토리의 mbox 파일에 보관할 수 있습니다.

oldmessage 명령을 사용하여 격리 상태의 메시지의 메시지 ID를 얻을 수 없습니다. 그러나 메시지 ID를 아는 경우, 지정된 메시지를 표시하거나 보관할 수 있습니다. 메시지가 작업 큐, 재시도 큐 또는 대상 큐에 없으므로 removemessage 명령을 사용하여 메시지를 제거할 수 없습니다.

참고 Cisco 스팸 격리에 있는 메시지에는 이러한 큐 관리 명령을 수행할 수 없습니다.

구문

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>
```

구문

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>
```

시스템에서의 메시지 추적

findevent 명령은 onbox 메일 로그 파일을 사용하여 시스템에서의 메시지 추적 프로세스를 간소화합니다. findevent 명령을 사용하면 메시지 ID 또는 제목 헤더, 봉투 발신자 또는 봉투 수신자에 대한 정규식 일치를 검색하여 메일 로그를 통해 특정 메시지를 검색할 수 있습니다. 현재 로그 파일, 모든 로그 파일에 대한 결과를 표시하거나 날짜별로 로그 파일을 표시할 수 있습니다. 날짜별로 로그 파일을 확인하는 경우 날짜 또는 날짜 범위를 지정할 수 있습니다.

로그를 확인할 메시지를 확인한 다음 findevent 명령을 사용하면 분리 정보(로그 메시지, 바운스 및 시스템에서 생성된 메시지 분리)를 비롯하여 해당 메시지 ID에 해당하는 로그 정보를 표시합니다. 다음 예는 제목 헤더에 "기밀"이 있는 메시지의 수신 및 전달을 추적하는 findevent 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
```

SNMP 모니터링

Cisco AsyncOS 운영 체제는 SNMP(Simple Network Management Protocol)를 통해 시스템 상태 모니터링을 지원합니다. 여기에는 Cisco의 엔터프라이즈 MIB, ASYNCOS-MAIL-MIB가 있습니다. ASYNCOS-MAIL-MIB를 활용하면 관리자가 시스템 상태를 보다 효율적으로 모니터링할 수 있습니다. 또한 이 릴리스는 RFC 1213 및 1907의 정의에 따라 MIB II의 읽기 전용 하위 집합을 구현합니다. (SNMP에 대한 자세한 내용은 RFC 1065, 1066 및 1067을 참조하십시오.) 참고:

- SNMP는 기본적으로 **비활성화**되어 있습니다.
- SNMP SET 연산(구성)은 구현되지 않았습니다.
- AsyncOS는 SNMPv1, v2 및 v3를 지원합니다.
- SNMPv3를 활성화할 때 메시지 인증 및 암호화는 필수사항입니다. 인증과 암호화를 위한 비밀번호는 서로 달라야 합니다. 암호화 알고리즘은 AES(권장) 또는 DES를 사용할 수 있습니다. 인증 알고리즘은 SHA-1(권장) 또는 MD5를 사용할 수 있습니다. `snmpconfig` 명령은 다음에 명령을 실행할 때 비밀번호를 "기억"합니다.
- SNMPv3 사용자 이름: v3get.

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 ironport mail.example.com
```

- SNMPv1 또는 SNMPv2만 사용하는 경우, 커뮤니티 문자열을 설정해야 합니다. 커뮤니티 문자열은 기본값이 `public`으로 설정되어 있지 않습니다.
- SNMPv1 및 SNMPv2의 경우, SNMP GET 요청을 수락한 네트워크를 지정해야 합니다.

- 트랩을 사용하려면 SNMP 관리자(AsyncOS에 포함되지 않음)가 실행 중이어야 하며 IP 주소가 트랩 대상으로 입력되어야 합니다. (호스트 이름을 사용할 수 있지만, 이러한 경우 DNS가 동작할 때만 트랩이 동작합니다.)

`snmpconfig` 명령을 사용하여 어플라이언스에 SNMP 시스템 상태를 구성할 수 있습니다 인터페이스에 대한 값을 선택하고 구성하면 어플라이언스가 SNMPv3 GET 요청에 응답합니다. 이러한 버전 3 요청은 일치하는 비밀번호를 포함해야 합니다. 기본적으로, 버전 1 및 버전 2 요청이 거부됩니다. 활성화된 경우, 버전 1 및 버전 2 요청에는 일치하는 커뮤니티 문자열을 포함해야 합니다.

MIB 파일

Cisco 시스템은 "엔터프라이즈" MIB와 "관리 정보 구조"(SMI) 파일을 제공합니다.

- ASYNCOS-MAIL-MIB.txt — Cisco 어플라이언스에 대한 엔터프라이즈 MIB의 SNMPv2 호환성 설명입니다.
- IRONPORT-SMI.txt — IronPort의 SNMP 관리 제품의 ASYNCOS-MAIL-MIB 역할을 정의합니다.

해당 파일은 Cisco 어플라이언스에 함께 포함된 문서 CD에서 사용할 수 있습니다. Cisco 고객 지원을 통해 이 파일을 요청할 수 있습니다.

하드웨어 객체

IPMI(Intelligent Platform Management Interface) 사양을 준수하는 하드웨어 센서는 온도, 팬 속도 및 전원 공급 장치 상태를 보고합니다.

표 34-11은 각 모델을 모니터링하는 데 어떤 하드웨어 파생 객체를 사용할 수 있는지 보여줍니다. 표시된 번호는 모니터링 가능한 객체의 인스턴스 수입니다. 예를 들어, C160/170 어플라이언스에서 팬 3개에 대해 RPM을 쿼리하고 C300/C600/X1000 어플라이언스에서 팬 6개에 대해 쿼리할 수 있습니다.

표 34-11 Cisco 어플라이언스당 하드웨어 객체 수

모델	CPU 온도	주변 온도	백플레인 온도	라이저 온도	팬	전원 공급 장치 상태	디스크 상태	NIC 링크
C160/170	1	1	0	0	3	0	2	2
C30/C60	0	0	0	0	0	0	2(C60은 4개)	3
C300/C600/ X1000	2	1	1	1	6	2	4(C300은 2개)	3(*파이버 인터페이스를 갖는 C600 및 X1000의 경우 5개*)
C350/C650/ X1050	2	1	0	0	4	2	4(C350은 2개)	3(*파이버 인터페이스를 갖는 C650 및 X1050의 경우 5개*)

모든 모델은 SNMP를 사용하여 네트워크 인터페이스의 디스크 드라이브 상태와 연결 상태를 모니터링할 수 있습니다.

하드웨어 트랩

표 34-12는 하드웨어 트랩이 전송되는 온도 및 하드웨어 상태를 나열합니다.

표 34-12 하드웨어 트랩: 온도 및 하드웨어 상태

모델	최고 온도(CPU)	최고 온도(주변)	최고 온도(백플레인)	최고 온도(라이저)	팬 고장	전력 공급 장치	RAID	링크
C160/ C170	90C	47C	NA	NA	0RPM	상태 변경	상태 변경	상태 변경
C30/ C60	NA	NA	NA	NA	NA	NA	상태 변경	상태 변경
C300/ C600/ X1000	90C	47C	72C	62C	0RPM	상태 변경	상태 변경	상태 변경
C350/ C650/ X1050	90C	47C	NA	NA	0RPM	상태 변경	상태 변경	상태 변경

상태 변경 시 상태 변경 트랩이 전송됩니다. 팬 고장 및 최고 온도 트랩이 5초마다 전송됩니다. 나머지 트랩은 오류 상태 알람 트랩으로, 상태 변경 시(정상 상태에서 고장 상태로) 한 번만 전송됩니다. 하드웨어 상태 테이블에 대해 폴링하고 심각한 상태가 되기 전에 가능한 하드웨어 오류를 식별하는 것이 좋습니다. 임계값 10% 이내의 온도는 문제가 될 수 있습니다.

오류 상태 알람 트랩은 개별 구성 요소의 심각한 오류를 나타내지만 전체 시스템 오류를 야기하지는 않습니다. 예를 들어, 단일 팬이나 전원 공급 장치는 C600 어플라이언스에서 오류를 일으킬 수 있지만 어플라이언스는 계속해서 동작합니다.

SNMP 트랩

SNMP는 하나 이상의 조건을 만족하는 경우 관리 애플리케이션(일반적으로, SNMP 관리 콘솔)에 알리기 위해 트랩 또는 알림을 전송하는 기능을 제공합니다. 트랩은 트랩을 전송하는 시스템 구성 요소와 관련된 데이터를 포함하는 네트워크 패킷입니다. 트랩은 SNMP 에이전트(여기서는 Cisco 어플라이언스)에서 조건이 만족되는 경우 생성됩니다. 조건이 만족되면 SNMP 에이전트가 SNMP 패킷을 형성하고 이를 포트 162, 표준 SNMP 트랩 포트를 통해 전송합니다. 아래 예에는 `snmp-monitor.example.com`의 트랩 대상과 트랩 커뮤니티 문자열이 입력됩니다. 이것은 Cisco 어플라이언스에서 SNMP 트랩을 수신하는 SNMP 관리 콘솔 소프트웨어를 실행 중인 호스트입니다.

인터페이스에 SNMP를 활성화하는 경우 SNMP 트랩(특정 트랩 활성화 또는 비활성화)을 구성할 수 있습니다. 여러 트랩 대상을 지정하려면 트랩 대상을 묻는 프롬프트에 IP 주소를 쉼표로 구분하여 최대 10개를 입력할 수 있습니다.

CLI 예

다음 예에서는 포트 161의 "PublicNet" 인터페이스에 SNMP를 활성화하기 위해 `snmpconfig` 명령을 사용합니다. 버전 3에 대한 암호를 입력하고 확인 암호를 다시 입력합니다. 시스템이 버전 1과 버전 2 요청을 처리하도록 구성되고 버전 1과 버전 2의 GET 요청을 위해 커뮤니티 문자열 `public`이 입력됩니다. `snmp-monitor.example.com`의 트랩 대상이 입력됩니다. 마지막으로, 시스템 위치와 연락처 정보가 입력됩니다.

```
mail3.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? [N]> y


Please choose an IP interface for SNMP requests.

1. Data 1 (192.168.1.1/24: mail3.example.com)

2. Data 2 (192.168.2.1/24: mail3.example.com)

3. Management (192.168.44.44/24: mail3.example.com)

[1]>


Enter the SNMPv3 passphrase.

>

Please enter the SNMPv3 passphrase again to confirm.

>

Which port shall the SNMP daemon listen on?

[161]>


Service SNMP V1/V2c requests? [N]> y


Enter the SNMP V1/V2c community string.

[]> public


From which network shall SNMP V1/V2c requests be allowed?

[192.168.2.0/24]>
```

```
Enter the Trap target (IP address recommended). Enter "None" to disable traps.
[None]> 10.1.1.29

Enter the Trap Community string.
[]> tcomm

Enterprise Trap Status
1. RAIDStatusChange             Enabled
2. fanFailure                   Enabled
3. highTemperature              Enabled
4. keyExpiration                Enabled
5. linkDown                     Enabled
6. linkUp                       Enabled
7. powerSupplyStatusChange      Enabled
8. resourceConservationMode     Enabled
9. updateFailure                Enabled
Do you want to change any of these settings? [N]> y

Do you want to disable any of these traps? [Y]>

Enter number or numbers of traps to disable. Separate multiple numbers with commas.
[]> 1,8

Enterprise Trap Status
1. RAIDStatusChange             Disabled
2. fanFailure                   Enabled
3. highTemperature              Enabled
4. keyExpiration                Enabled
```

```
5. linkDown                     Enabled

6. linkUp                       Enabled

7. powerSupplyStatusChange      Enabled

8. resourceConservationMode     Disabled

9. updateFailure                Enabled

Do you want to change any of these settings? [N]>


Enter the System Location string.

[Unknown: Not Yet Configured]> Network Operations Center - west; rack #31, position 2


Enter the System Contact string.

[snmp@localhost]> Joe Administrator, x8888


Current SNMP settings:

Listening on interface "Data 1" 192.168.2.1/24 port 161.

SNMP v3: Enabled.

SNMP v1/v2: Enabled, accepting requests from subnet 192.168.2.0/24.

SNMP v1/v2 Community String: public

Trap target: 10.1.1.29

Location: Network Operations Center - west; rack #31, position 2

System Contact: Joe Administrator, x8888


mail3.example.com>
```

35 장

SenderBase 네트워크 참여

SenderBase 네트워크 참여 개요

SenderBase는 이메일 관리자가 발신자를 조사하고 이메일의 정상적인 소스를 파악하고 스패머를 차단할 수 있도록 설계된 이메일 평판 서비스입니다.

SenderBase 네트워크에 참여하는 고객은 Cisco에 조직에 대한 집계된 이메일 트래픽 통계를 수집하여 모든 사용자를 위해 서비스 유틸리티를 늘릴 수 있는 권한을 부여합니다. 참여는 자발적입니다. Cisco는 메시지 특성에 대한 요약 데이터와 Cisco 어플라이언스에서 처리한 메시지 유형에 대한 정보만 수집합니다. 예를 들어, Cisco는 메시지 본문 또는 메시지 제목을 수집하지 않습니다. 개인 식별 정보 또는 조직을 식별할 수 있는 정보는 기밀로 유지됩니다.

SenderBase와 통계 공유

절차

1단계 **Security Services(보안 서비스) > SenderBase**로 이동합니다.

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

3단계 SenderBase Information Service와 통계 데이터를 공유할 수 있도록 해당 상자를 선택합니다.

이 상자를 선택하면 어플라이언스에서 이 기능을 전역적으로 활성화할 수 있습니다. 이 기능이 활성화되면 CASE(컨텍스트 적응형 검사 엔진)를 사용하여 데이터를 수집 및 보고합니다(Cisco 안티스팸 검사 활성화 여부와 무관).

4단계 (선택 사항) SenderBase Information Service와 통계 데이터를 공유하기 위해 프록시 서버를 활성화합니다.

규칙 업데이트를 검색할 프록시 서버를 정의할 경우 프록시 서버에 연결할 때 제공된 추가 필드에서 인증된 사용자 이름, 비밀번호 및 특정 포트도 구성할 수 있습니다. 이러한 설정을 편집하려면 시스템 시간, 33-57페이지를 참조하십시오. CLI에서 `senderbaseconfig` 명령을 사용할 때와 동일한 설정을 구성할 수 있습니다.

FAQ(자주 묻는 질문)

Cisco는 사용자에게 개인정보 보호가 중요하다는 사실을 인지하고 있으므로 사용자의 개인정보 보호를 염두에 두고 서비스를 설계 및 운영합니다. SenderBase 네트워크 참여에 등록하면 Cisco에서 사용자의 조직의 이메일 트래픽에 대한 집계된 통계를 수집하지만 개인 식별 정보는 수집하거나 사용하지 않습니다. Cisco에서 수집하는 정보 중 사용자 또는 사용자의 조직을 식별할 수 있는 정보는 기밀로 처리됩니다.

참여해야 하는 이유는 무엇입니까?

SenderBase 네트워크에 참여하면 Cisco에서 사용자를 지원할 수 있습니다. 당사와 데이터를 공유하는 것은 스팸, 바이러스 및 디렉토리 수집 공격과 같은 이메일 기반 위협이 사용자의 조직에 영향을 미치는 것을 차단하는 데 중요합니다. 참여가 특히 중요한 이유를 예로 들면 다음과 같습니다.

- 특히 사용자의 조직을 대상으로 한 이메일 공격의 경우(사용자가 제공한 데이터가 사용자를 보호할 수 있는 정보의 기본 소스 제공).
- 사용자의 조직이 새로운 전역 이메일 공격을 받는 첫 번째 대상 중 하나인 경우(당사와 공유하는 데이터가 새로운 위협에 대응할 수 있는 속도를 크게 높여줌).

어떤 데이터를 공유합니까?

공유하는 데이터에는 메시지 특성에 대한 요약 정보와 Cisco 어플라이언스에서 처리한 메시지 유형에 대한 정보가 포함됩니다. 당사는 메시지의 전체 본문을 수집하지 않습니다. 다시 한 번 설명하지만, Cisco에 제공된 정보 중 사용자 또는 사용자의 조직을 식별할 수 있는 정보는 기밀로 처리됩니다. (아래의 내가 공유하는 데이터를 안전하게 유지하기 위해 Cisco에서 어떤 작업을 수행합니까?, 35-4페이지를 참조하십시오.)

표 35-1 및 표 35-2에서는 "사용자에게 익숙한" 형식의 샘플 로그 항목을 설명합니다.

표 35-1 어플라이언스별로 Cisco 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
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
격리 시작 및 종료 이유, 안티바이러스 결과와의 상관 관계별로 분석된 신종 바이러스 격리 메시지 수	.exe 규칙에 의해 30개의 메시지 격리 시작 수동 릴리스로 인해 30개의 메시지가 격리에서 릴리스되고 30개 모두 바이러스에 감염되었음

표 35-1 어플라이언스별로 Cisco 공유되는 통계 (계속)

항목	샘플 데이터
격리 종료 시 수행된 작업별로 분석된 신종 바이러스 격리 메시지 수	쿼런틴을 종료한 후 10개 메시지의 첨부파일이 제거됨
메시지가 쿼런틴된 시간 합계	20시간

표 35-2 IP 주소별로 공유되는 통계

항목	샘플 데이터
어플라이언스 내 다양한 단계에서의 메시지 수	안티바이러스 엔진을 통해 발견된 메시지 수: 100 안티스팸 엔진을 통해 발견된 메시지 수: 80
안티스팸 및 안티바이러스 점수 및 판정 합계	2,000(발견된 모든 메시지에 대한 안티스팸 점수 합계)
다른 안티스팸 및 안티바이러스 규칙 조합에 적중하는 메시지 수	100 메시지 적중 규칙 A 및 B 50 메시지 적중 규칙 A만
연결 수	20 SMTP 연결
전체 수 및 올바르지 않은 수신인	50 총 수신자 10 잘못된 수신자
해시된 파일 이름: (a)	이름이 <one-way-hash>.zip인 첨부 파일에서 <one-way-hash>.pif 파일이 발견되었습니다.
난독 처리된 파일 이름: **(b)**	aaaaaaa.zip 파일에서 aaaaaaa0.aaa.pif 파일이 발견되었습니다.
URL 호스트 이름: (c)	메시지 안에 www.domain.com에 대한 링크가 있습니다.
난독 처리된 **URL** 경로: (d)	호스트 이름에 대한 메시지 안에 www.domain.com에 대한 링크와 aaa000aa/aa00aaa 경로가 있습니다.
스팸 및 바이러스 검사 결과에 의한 메시지 수	10 - 스팸 감염 10 - 스팸 음성 5 - 의심스러운 스팸 4 - 바이러스 감염 16 - 바이러스 음성 5 - 바이러스 검사 불가능
다른 안티스팸 및 안티바이러스 판정을 받은 메시지 수	500 스팸, 300 햄
크기 범위의 메시지 수	30K-35K 범위에서 125개
다른 확장명 유형 수	300 - '.exe' 첨부 파일

표 35-2 IP 주소별로 공유되는 통계

항목	샘플 데이터 (계속)
첨부파일 유형의 상관 관계, 참 파일 유형 및 컨테이너 유형	100 - 확장자가 ".doc"이지만 실제로는 ".exe"인 첨부 파일 50 - zip 내에서 확장자가 ".exe"인 첨부 파일
확장명 및 참 파일 유형과 첨부파일 크기의 상관 관계	30 - 50-55K 범위 내에서 ".exe"인 첨부 파일

(a) 파일 이름이 1방향 해시(MD5)로 인코딩됩니다.

(b) 파일 이름이 난독 처리된 형식으로 전송됩니다. 이 형식에서 모든 소문자 ASCII 문자([a-z])는 "a"로 대체되고, 모든 대문자 ASCII 문자([A-Z])는 "A"로 대체되고, 모든 멀티바이트 UTF-8 문자는 "x"(다른 문자 집합에 대한 개인정보 보호 제공)로 대체되며, 모든 ASCII 숫자([0-9])는 "0"으로 대체되고, 다른 모든 싱글바이트 문자(공백, 구두점 등)는 유지됩니다. 예를 들어, 파일 Britney1.txt .pif는 Aaaaaaa0.aaa.pif로 표시됩니다.

(c) URL 호스트 이름은 IP 주소와 마찬가지로 콘텐츠를 제공하는 웹 서버를 가리킵니다. 사용자 이름 및 비밀번호와 같은 기밀 정보는 포함되지 않습니다.

(d) 사용자의 개인 정보가 노출되지 않도록 호스트 이름 다음에 나오는 URL 정보는 난독 처리되어 있습니다.

AsyncOS 8.5 for Email 이상에서 IronPort Anti-Spam 또는 Intelligent Multi-Scan 기능 키와 SenderBase 네트워크 참여가 활성화된 경우 AsyncOS가 다음 작업을 수행하여 제품의 효율성을 높입니다.

- 메시지의 특정 헤더 반복에 대한 정보를 수집하고, 수집한 정보를 암호화하며, 암호화된 정보를 해당 메시지에 헤더로 추가합니다.

  분석을 위해 이러한 처리된 메시지를 Cisco에 전송할 수 있습니다. 각 메시지는 분석가로 구성된 팀에서 검토되며 제품의 효율성을 높이는 데 사용됩니다. 분석을 위해 Cisco에 메시지를 전송하는 지침은 Cisco Systems에 잘못 분류된 메시지 보고, 13-15페이지를 참조하십시오.

- 해당 발신자의 SBRS에 관계없이 안티스팸 검사를 위해 임의의 메시지 샘플을 CASE에 보냅니다. CASE가 이러한 메시지를 검사하고 검사 결과를 사용하여 제품의 효율성을 높입니다. AsyncOS는 유휴 상태일 때만 이 작업을 수행합니다. 따라서 이 피드백 메커니즘은 메시지 처리에 중대한 영향을 미치지 않습니다.

내가 공유하는 데이터를 안전하게 유지하기 위해 Cisco에서 어떤 작업을 수행합니까?

SenderBase 네트워크 참여에 동의할 경우:

- Cisco 어플라이언스에서 보낸 데이터는 보안 프로토콜 HTTPS를 사용하여 Cisco SenderBase 네트워크 서버에 전송됩니다.
- 모든 고객 데이터는 Cisco에서 신중하게 처리됩니다. 이 데이터는 안전한 위치에 저장되며, 회사의 이메일 보안 제품 및 서비스를 개선하거나 고객 지원을 제공하기 위해 데이터 액세스가 필요한 Cisco 직원 및 계약업체만 이 데이터에 액세스할 수 있습니다.
- 데이터를 기반으로 보고서 또는 통계를 생성할 경우 이메일 수신자 또는 고객의 회사를 식별할 수 있는 정보는 Cisco Systems 외부에서 공유되지 않습니다.

데이터 공유가 내 Cisco 어플라이언스의 성능에 영향을 미칩니까?

Cisco는 대부분의 고객에게 최소한의 성능 영향이 있을 것으로 확신합니다. Cisco는 메일 전송 프로세스의 일환으로 이미 존재하는 데이터를 기록합니다. 그리고 고객 데이터는 어플라이언스에 집계되어 보통 5분마다 SenderBase 서버로 일괄 전송됩니다. Cisco는 HTTPS를 통해 전송되는 데이터의 총 크기가 일반적인 회사의 이메일 트래픽 대역폭의 1% 미만이 될 것으로 예상합니다.

이 기능이 활성화되면 CASE(컨텍스트 적응형 검사 엔진)를 사용하여 데이터를 수집 및 보고합니다(Cisco 안티스팸 검사 활성화 여부와 무관).

참고 SenderBase 네트워크에 참여하기로 선택한 경우 각 메시지에 대해 "본문 검사"가 수행됩니다. 이 검사는 메시지에 적용된 필터 또는 다른 작업이 본문 검사를 트리거하는지 여부에 관계없이 수행됩니다. 본문 검사에 대한 자세한 내용은 "본문 검사 규칙, 9-30페이지"를 참조하십시오.

그 밖에 궁금한 점이 있으면 Cisco 고객 지원팀에 문의하십시오. Cisco 지원 커뮤니티, 1-8페이지를 참조하십시오.

데이터를 공유할 수 있는 다른 방법이 있습니까?

Cisco가 최고 품질의 보안 서비스를 제공할 수 있도록 더 적극적으로 도우려는 고객을 위해 추가 데이터를 공유할 수 있는 명령이 있습니다. 이처럼 데이터 공유 수준이 높을 경우 메시지에 포함된 URL의 호스트 이름뿐 아니라 해시되지 않은 일반 텍스트의 첨부 파일 이름도 공유합니다. 이 기능에 대해 더 자세히 알고 싶으시면 시스템 엔지니어에게 문의하거나 Cisco 고객 지원팀에 문의하십시오.

36 장

GUI 기타 작업

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.

이 장에는 다음 섹션이 포함되어 있습니다.

그래픽 사용자 인터페이스(GUI)

인터페이스에 HTTP 및/또는 HTTPS 서비스를 활성화한 후에 GUI에 액세스하고 로그인할 수 있습니다. 자세한 내용은 "어플라이언스 액세스" 장을 참조하십시오.

인터페이스의 GUI 활성화

기본적으로, 시스템은 관리 인터페이스에 HTTP가 활성화된 상태로 제공됩니다.

GUI를 활성화하려면 명령줄 인터페이스에서 `interfaceconfig` 명령을 실행하고 연결하려는 인터페이스를 편집한 다음 HTTP 서비스 또는 보안 HTTP 서비스 모두를 활성화합니다.

참고 다른 인터페이스에서 GUI를 활성화한 경우 Network(네트워크) > IP Interfaces(IP 인터페이스) 페이지를 사용하여 인터페이스의 GUI를 활성화 또는 비활성화할 수 있습니다. 자세한 내용은 IP 인터페이스, A-1페이지 항목을 참조하십시오.

참고 인터페이스에 보안 HTTP를 활성화하려면 인증서를 설치해야 합니다. 자세한 내용은 "HTTPS에 대한 인증서 활성화하기"를 참조하십시오.

두 가지 서비스를 활성화할 포트를 지정합니다. 기본적으로, HTTP는 포트 80에서 활성화되고 HTTPS는 포트 443에서 활성화됩니다. 인터페이스에 두 가지 서비스를 모두 활성화한 경우, 자동으로 보안 서비스에 HTTP 요청을 리디렉션할 수 있습니다.

또한, 이 인터페이스에서 GUI에 액세스를 시도하는 모든 사용자(사용자 계정 작업, 32-1페이지 참조, HTTP 또는 HTTPS를 통해)는 표준 사용자 이름 및 비밀번호 로그인 페이지를 통해 인증을 받아야 합니다.

참고 GUI에 액세스하려면 먼저 commit 명령을 사용하여 변경 사항을 저장해야 합니다.

다음 예에서 GUI는 데이터 1 인터페이스에서 활성화됩니다. interfaceconfig 명령을 사용하여 포트 80에서 HTTP를 활성화하고 포트 443에서 HTTPS를 활성화합니다. (데모 인증서는 certconfig 명령을 실행할 수 있을 때까지 HTTP에 임시로 사용됩니다.) 자세한 내용은 "Cisco 어플라이언스에 인증서 설치하기"를 참조하십시오. 포트 80에 대한 HTTP 요청은 자동으로 데이터 1 인터페이스의 포트 443으로 리디렉션되도록 구성되어 있습니다.

예

```
mail3.example.com> interfaceconfig

Currently configured interfaces:
1. Data 1 (192.168.1.1/24 on Data1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: mail3.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.
[]> edit

Enter the number of the interface you wish to edit.
[]> 1

IP interface name (Ex: "InternalNet"):
[Data 1]>
```

```
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>

IPv4 Address (Ex: 192.168.1.2):
[192.168.1.1]>

Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[24]>

Would you like to configure an IPv6 address for this interface (y/n)? [N]>

Ethernet interface:
1. Data 1
2. Data 2
3. Management
[1]>

Hostname:
[mail3.example.com]>

Do you want to enable Telnet on this interface?  [N]>

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]> y

Which port do you want to use for HTTP?
[80]> 80
```

```
Do you want to enable HTTPS on this interface?  [N]> y

Which port do you want to use for HTTPS?
[443]> 443

You have not entered a certificate. To assure privacy, run
'certconfig' first.  You may use the demo certificate
to test HTTPS, but this will not be secure.
Do you really wish to use a demo certificate?  [N]> y

Both HTTP and HTTPS are enabled for this interface, should HTTP requests
redirect to the secure service?  [Y]> y

Currently configured interfaces:
1. Data 1 (192.168.1.1/24 on Data 1: mail3.example.com)
2. Data 2 (192.168.2.1/24 on Data 2: mail3.example.com)
3. Management (192.168.42.42/24 on Management: mail3.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.
[]>
mail3.example.com> commit

Please enter some comments describing your changes:
[]> enabled HTTP, HTTPS for Data 1
```

```
Do you want to save the current configuration for rollback? [Y]> n

Changes committed: Fri May 23 11:42:12 2014 GMT
```

GUI의 시스템 정보

- **System Overview(시스템 요약)** 페이지에서 다음을 수행할 수 있습니다.
  - 주요 시스템 상태 및 성능 정보의 일부를 보여주는 기록 그래프 및 표 보기.
  - 어플라이언스에 설치된 AsyncOS 운영 체제의 버전 보기.
  - 주요 통계의 하위 집합 보기.
- **System Status(시스템 상태)** 페이지는 모든 실시간 메일 및 시스템의 DNS 활동을 자세히 보여줍니다. 또한 시스템 통계의 카운터를 재설정하고 카운터가 재설정된 마지막 시간을 확인할 수 있습니다.

GUI에서 XML 상태 수집

- XML 페이지를 통해 상태를 보거나 프로그램을 통해 XML 상태 정보에 액세스합니다.

XML 상태 기능은 프로그래밍 방식을 통해 이메일 모니터링 통계에 액세스하도록 합니다. 일부 최신 브라우저에서는 XML 데이터를 직접 렌더링할 수 있습니다.

다음 표에 있는 GUI의 페이지 정보는 해당 URL에 액세스하여 동적 XML 출력으로 사용할 수 있습니다.

GUI 페이지 이름	해당 XML 상태 URL
메일 상태	`http://`*호스트 이름*`/xml/status`
지정된 호스트의 호스트 메일 상태	`http://`*호스트 이름*`/xml/hoststatus?hostname=`*호스트*
DNS 상태	`http://`*호스트 이름*`/xml/dnsstatus`
상위 수신 도메인	`http://`*호스트 이름*`/xml/topin`
상위 발송 도메인[a]	`http://`*호스트 이름*`/xml/tophosts`

[a] 이 페이지의 기본 정렬 순서는 활성 수신자 번호 기준입니다. "?sort=***order***"를 URL에 추가하여 이 순서를 변경할 수 있습니다. 이때 ***order***는 **`conn_out`**, **`deliv_recip`**, **`soft_bounced`** 또는 **`hard_bounced`**로 설정합니다.

37 장

고급 네트워크 구성

이 장은 NIC 페어링, VLAN, Direct Server Return 등 `etherconfig` 명령을 사용하여 일반적으로 사용할 수 있는 고급 네트워크 구성에 대한 정보를 포함하고 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, 37-2페이지 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.

참고 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, 37-3페이지 항목을 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.

[]> 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. 자동 선택

2. 10baseT/UTP 반이중

3. 10baseT/UTP 전이중

4. 100baseTX 반이중

5. 100baseTX 전이중
```

```
6. 1000baseTX 반이중

7. 1000baseTX 전이중

[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.

[]>
```

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 인터페이스가 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), 37-6페이지 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 이메일 보안 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.

[]> pairing
```

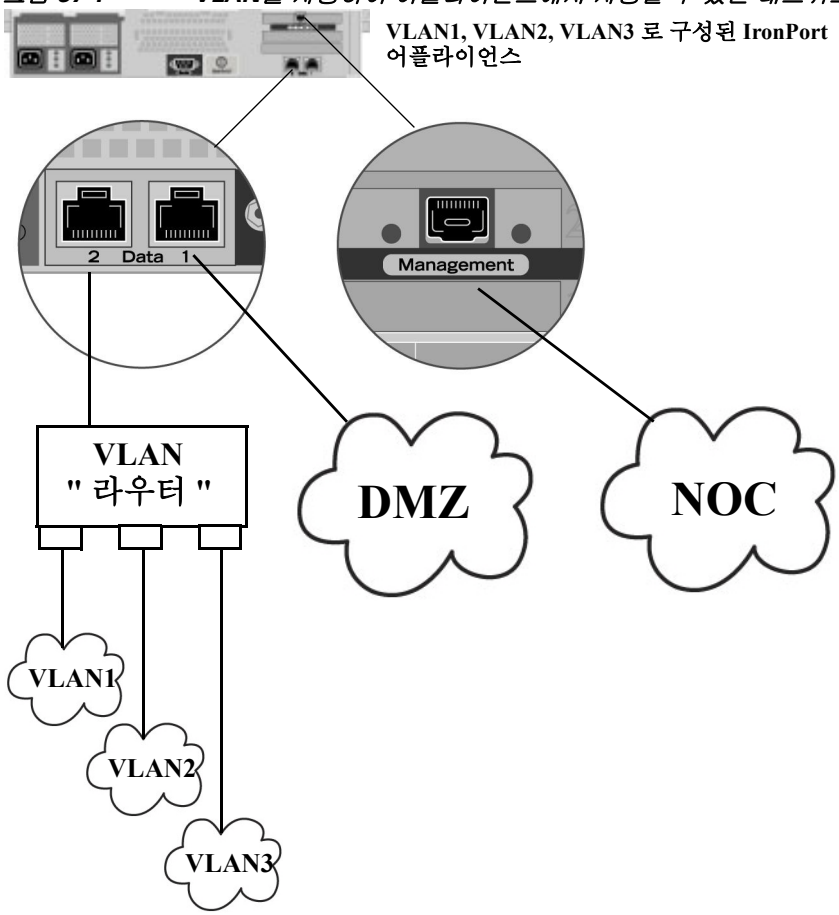
```
Paired interfaces:


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.

계속하시겠습니까? [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)

VLAN은 물리적 데이터 포트에 바인딩된 가상 로컬 영역 네트워크입니다. 어플라이언스에서 연결할 수 있는 네트워크 수가 포함된 물리적 인터페이스 수를 초과하도록 VLAN을 구성할 수 있습니다. 예를 들어 일부 어플라이언스 모델에는 인터페이스가 3개(데이터 1, 데이터 2 및 관리 인터페이스)가 있습니다. VLAN을 사용하면 기존 리스너에서 별도의 "포트"에 추가 네트워크를 정의할 수 있습니다. (자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스" 참조.) 물리적 네트워크 포트에 여러 VLAN을 구성할 수 있습니다. 그림 37-1에서는 데이터 2 인터페이스에서 여러 VLAN을 구성하는 방법에 대한 예를 보여줍니다.

그림 37-1 VLAN을 사용하여 어플라이언스에서 사용할 수 있는 네트워크 수 늘리기



VLAN을 사용하여 보안을 강화하거나 관리 효율성을 높이거나 대역폭을 증가시키기 위해 네트워크를 분할할 수 있습니다. VLAN은 "VLAN DDDD" 형식의 동적 "데이터 포트"로 표시됩니다. 여기서 "DDDD"는 ID이고 최대 4자리 정수입니다(예: VLAN 2 또는 VLAN 4094). AsyncOS는 최대 30개의 VLAN을 지원합니다. 어플라이언스에서 중복 VLAN ID는 허용되지 않습니다.

VLAN 및 물리적 포트

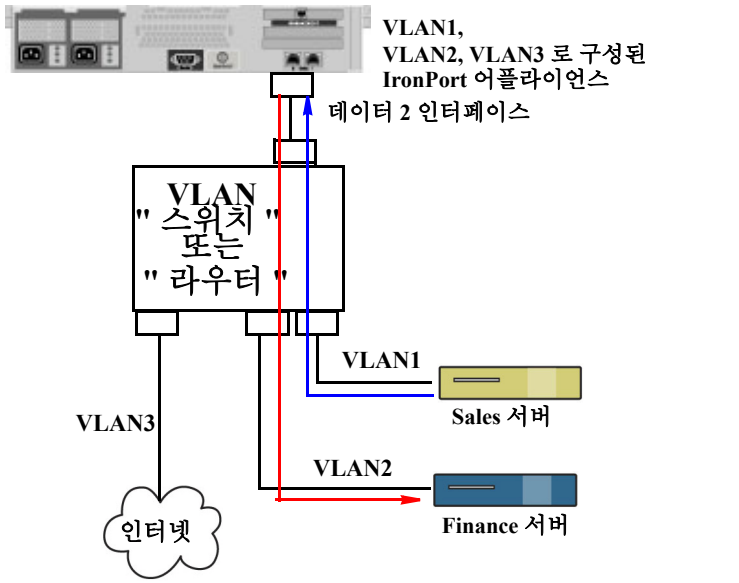
VLAN에 물리적 포트를 포함하기 위해 IP 주소를 구성할 필요는 없습니다. VLAN이 생성된 물리적 포트에는 비VLAN 트래픽을 수신하는 IP가 있으므로 VLAN 트래픽과 비VLAN 트래픽 모두 동일한 인터페이스에서 처리할 수 있습니다.

VLAN은 일부 어플라이언스 모델에서 사용할 수 있는 광섬유 데이터 포트를 비롯하여 모든 "데이터" 및 "관리" 포트에서 생성할 수 있습니다.

VLAN은 NIC 페어링(페어링된 NIC에서 사용 가능) 및 DSR(Direct Server Return)에 사용될 수 있습니다.

그림 37-2에서는 VLAN 제한으로 인해 직접 통신할 수 없는 두 메일 서버가 Email Security 어플라이언스를 통해 메일을 전송하는 방법을 보여주는 활용 사례를 확인할 수 있습니다. 파란색 줄은 Sales 네트워크(VLAN1)에서 어플라이언스로 전송되는 메일을 나타냅니다. 이 어플라이언스는 해당 메일을 정상으로 처리하며, 메일 전달 시 VLAN 정보(빨간색 줄)를 사용하여 패킷에 태그를 지정합니다.

그림 37-2 VLAN을 사용하여 어플라이언스 간 통신 효율 증대



VLAN 관리

`etherconfig` 명령을 사용하여 VLAN을 생성, 편집 및 삭제할 수 있습니다. VLAN이 생성되면, VLAN은 Network(네트워크) -> Interfaces(인터페이스) 페이지 또는 CLI에서 `interfaceconfig`명령을 사용하여 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.
[]> 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.
[]>
```

interfaceconfig 명령을 통해 VLAN에서 IP 인터페이스 생성

이 예에서는 VLAN 31 이더넷 인터페이스에서 새 IP 인터페이스를 생성합니다.

참고 인터페이스를 변경하면 어플라이언스와의 연결이 종료될 수 있습니다.

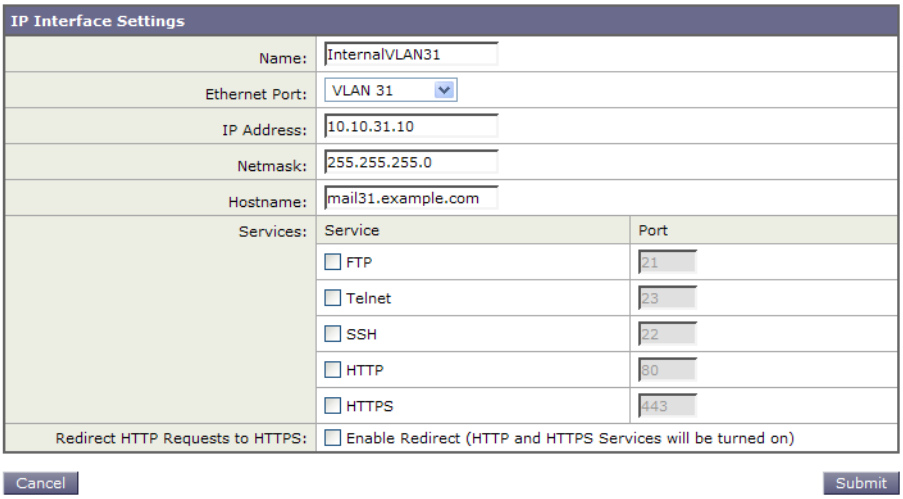
```
mail3.example.com> interfaceconfig


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 Telnet on this interface? [N]>


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.

[]>
```

Network(네트워크) -> Listeners(리스너) 페이지에서도 VLAN을 구성할 수 있습니다.

그림 37-3 GUI를 통해 새 IP 인터페이스를 생성할 때 VLAN 사용



Direct Server Return

DSR(Direct Server Return)은 동일한 VIP(가상 IP)를 공유하는 여러 Email Security 어플라이언스 간에 로드를 분산하는 경량의 로드 밸런싱 메커니즘을 지원하는 방법입니다.

DSR은 어플라이언스의 "루프백" 이더넷 인터페이스에서 생성된 IP 인터페이스를 통해 구현됩니다.

참고 Email Security 어플라이언스에 대한 로드 밸런싱을 구성하는 것은 이 문서의 범위에 포함되지 않습니다.

DSR(Direct Server Return) 활성화

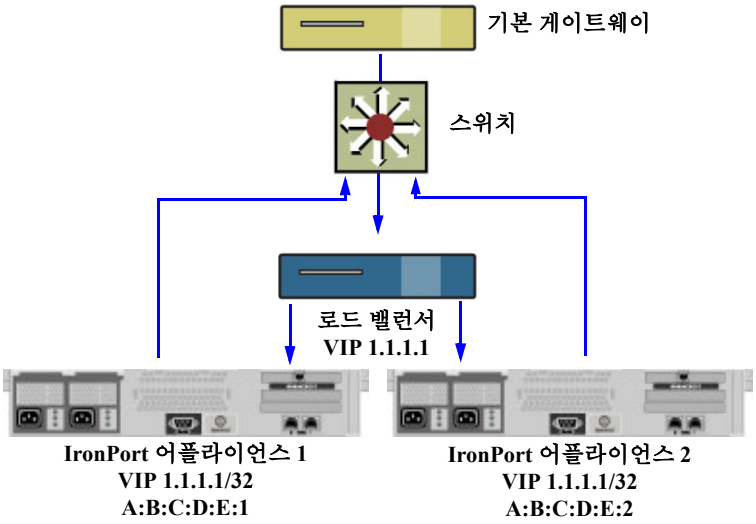
참여하는 각 어플라이언스에서 "루프백" 이더넷 인터페이스를 활성화하여 DSR을 사용할 수 있습니다. 다음으로, CLI의 `interfaceconfig` 명령, 또는 GUI의 Network(네트워크) -> Interfaces(인터페이스) 페이지에서 VIP(가상 IP)를 사용하는 루프백 인터페이스의 IP 인터페이스를 생성합니다. 마지막으로, CLI의 `listenerconfig` 명령, 또는 GUI의 Network(네트워크) -> Listeners(리스너) 페이지에서 새 IP 인터페이스의 리스너를 생성합니다. 모든 변경사항을 커밋해야 합니다.

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 37-4 DSR을 사용하여 스위치의 여러 Email Security 어플라이언스 간에 로드 밸런싱



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.

[]> 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.

[]>
```

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)
```

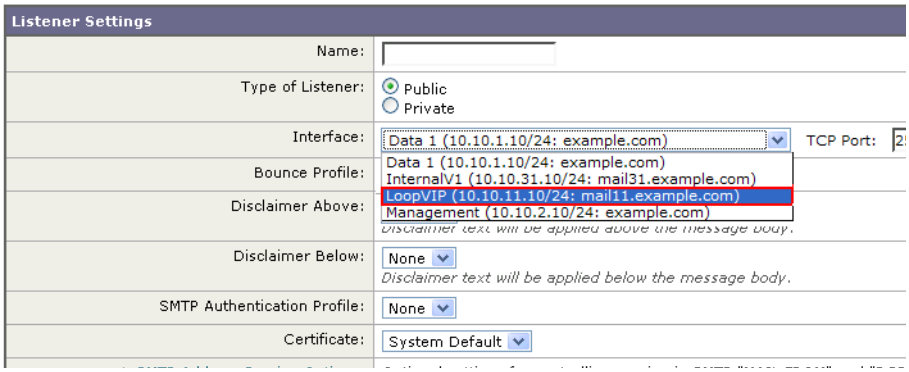
```
Choose the operation you want to perform:

- 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 Telnet on this interface? [N]>


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 그림 37-5에서는 GUI의 Add Listener(리스너 추가) 페이지에서 생성할 수 있는 새로 생성된 IP 인터페이스를 보여줍니다.

그림 37-5 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.

[]> 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.

[]>
```

38 장

로깅

개요

로그 파일과 로그 서브스크립션 이해

로그는 AsyncOS의 이메일 작업에 대한 중요 정보를 수집하는 간단하고 효율적인 방법입니다. 로그는 어플라이언스에서의 활동에 대한 정보를 기록합니다. 이 정보는 확인할 수 있는 로그(예: 바운스 로그 또는 전송 로그)에 따라 다릅니다.

대부분의 로그는 일반 텍스트(ASCII) 형식으로 기록됩니다. 그러나 전송 로그는 리소스 효율성을 위해 이진 형식으로 구성됩니다. ASCII 텍스트 정보는 모든 텍스트 편집기에서 읽을 수 있습니다.

Cisco는 여러 Email Security 어플라이언스의 로그에 대한 중앙 집중식 보고와 추적 기능을 제공하는 M-Series Content Security Management Appliance를 제공합니다. 자세한 내용은 Cisco 담당자에게 문의하십시오.

로그 서브스크립션은 로그 유형을 이름, 로깅 수준 및 다른 제약 조건(예: 크기 및 대상 정보)과 연결합니다. 동일한 로그 유형에 대해 여러 서브스크립션이 허용됩니다.

로그 유형

로그 유형은 생성된 로그 안에 어떤 정보가 기록되는지 나타냅니다(예: 메시지 데이터, 시스템 통계, 이진 또는 텍스트 데이터 등). 로그 서브스크립션을 생성할 때 로그 유형을 선택합니다. 자세한 내용은 로그 서브스크립션, 38-36페이지 항목을 참조하십시오.

AsyncOS for Email은 다음 로그 유형을 생성합니다.

표 38-1 로그 유형

로그	설명
텍스트 메일 로그	텍스트 메일 로그는 이메일 시스템의 작업에 대한 정보를 기록합니다. 예를 들어, 메시지 수신, 메시지 전송 시도, 열린 연결 및 종료된 연결, 바운스, TLS 연결 및 기타 정보를 기록합니다.
qmail 형식 메일 로그	qmail 형식 전송 로그는 이메일 시스템 작업에 대해 전송 로그와 동일한 정보를 기록하지만 qmail 형식으로 저장됩니다.
전송 로그	전송 로그는 Email Security 어플라이언스의 이메일 전달 작업에 대한 중요 정보(예: 각 수신자 전달 및 전달 시도 시의 바운스에 대한 정보)를 기록합니다. 로그 메시지는 "무상태(stateless)"인데 이것은 모든 관련 정보가 각 로그 메시지에 기록되며 사용자가 현재 전송 시도에 대한 정보를 얻기 위해 이전 로그 메시지를 참조할 필요가 없음을 의미합니다. 전송 로그는 리소스 효율성을 위해 이진 형식으로 기록됩니다. 전송 로그 파일은 XML 또는 CSV(Comma-Separated Values) 형식으로 변환하기 위해 제공된 유틸리티를 사용하여 사후 처리해야 합니다. 변환 툴은 다음에서 확인할 수 있습니다. `http://support.ironport.com`
바운스 로그	바운스 로그는 바운스된 수신자에 대한 정보를 기록합니다. 바운스된 수신자에 대해 기록된 정보에는 메시지 ID, 수신자 ID, Envelope From 주소, Envelope To 주소, 수신자 바운스 이유 및 수신자 호스트의 응답 코드가 포함되어 있습니다. 또한 바운스된 각 수신자 메시지의 고정된 크기를 로그하도록 선택할 수 있습니다. 이 크기는 바이트로 정의되며 기본값은 0입니다.
상태 로그	이 로그 파일은 `status detail` 및 `dnsstatus` 등의 CLI 상태 명령을 사용하여 확인된 시스템 통계를 기록합니다. 기록 기간은 `logconfig`의 `setup` 하위 명령을 사용하여 설정됩니다. 상태 로그에서 보고된 각 카운터 또는 속도는 카운터가 마지막으로 재설정된 이후의 값입니다.
도메인 디버그 로그	도메인 디버그 로그는 Email Security 어플라이언스 및 지정된 수신자 호스트 간의 SMTP 대화 중에 클라이언트 및 서버 통신을 기록합니다. 이러한 로그 유형은 특정한 수신자 호스트의 문제를 디버깅합니다. 로그 파일에 기록할 총 SMTP 세션 수를 지정해야 합니다. 세션이 기록되면 이 숫자가 감소합니다. 로그 서브스크립션을 삭제하거나 편집하여 모든 세션을 기록하기 전에 도메인 디버깅을 중지할 수 있습니다.
수신 디버그 로그	수신 디버그 로그는 Email Security 어플라이언스와 시스템에 연결 중인 지정된 호스트 간의 SMTP 대화를 기록합니다. 수신 디버그 로그는 Email Security 어플라이언스와 인터넷 호스트 간의 통신 문제를 해결하는 데 유용합니다.
시스템 로그	시스템 로그에는 부팅 정보, 가상 어플라이언스 라이센스 만료 알림, DNS 상태 정보 및 `commit` 명령을 사용하여 사용자가 입력한 설명이 기록됩니다. 시스템 로그는 어플라이언스의 기본 상태의 문제를 해결하는 데 유용합니다.
CLI 감사 로그	CLI 감사 로그는 시스템의 모든 CLI 활동을 기록합니다.
FTP 서버 로그	FTP 로그는 인터페이스에서 활성화된 FTP 서비스에 대한 정보를 기록합니다. 연결 세부 정보 및 사용자 활동이 기록됩니다.
GUI 로그	HTTP 로그를 참조합니다.

표 38-1 로그 유형 (계속)

로그	설명
HTTP 로그	HTTP 로그는 인터페이스에서 활성화된 HTTP 및/또는 보안 HTTP 서비스에 대한 정보를 기록합니다. 그래픽 사용자 인터페이스(GUI)는 HTTP를 통해 액세스되기 때문에 HTTP 로그는 표면상 CLI 감사 로그의 GUI입니다. GUI에서 액세스한 세션 데이터(새 세션, 만료 세션) 및 페이지가 기록됩니다. 이 로그에는 어플라이언스에서 이메일로 전송된 예약된 보고서의 정보 등 SMTP 트랜잭션에 대한 정보가 포함됩니다.
NTP 로그	NTP 로그는 구성된 모든 NTP(Network Time Protocol) 서버와 어플라이언스 간의 대화를 기록합니다. 자세한 내용은 "시스템 관리" 장의 "NTP(Network Time Protocol) 구성 수정(시간 유지 방법)"을 참조하십시오.
LDAP 디버그 로그	LDAP 디버그 로그는 LDAP 설치 디버깅 정보를 기록합니다. ("LDAP 쿼리" 장 참조.) Email Security 어플라이언스가 LDAP 서버에 전송 중인 쿼리에 대한 유용한 정보가 여기에 기록됩니다.
안티스팸 로그	안티스팸 로그는 최신 안티스팸 규칙의 업데이트 수신에 관한 상태를 포함하여 시스템의 안티스팸 검사 기능의 상태를 기록합니다. 또한 Context Adaptive Scanning Engine과 관련된 모든 로그가 여기에 로깅됩니다.
안티스팸 아카이브	안티스팸 검사 기능을 활성화한 경우, "아카이브 메시지" 작업과 관련하여 검사된 메시지가 여기에 보관됩니다. 형식은 mbox 형식 로그 파일입니다. 안티스팸 엔진에 대한 자세한 내용은 "안티스팸" 장을 참조하십시오.
안티바이러스 로그	안티바이러스 로그는 최신 안티바이러스 ID 파일의 업데이트 수신에 관한 상태를 포함하여 시스템의 안티바이러스 검사 기능의 상태를 기록합니다.
안티바이러스 아카이브	안티바이러스 엔진을 활성화한 경우, "아카이브 메시지" 작업과 관련하여 검사된 메시지가 여기에 보관됩니다. 형식은 mbox 형식 로그 파일입니다. 자세한 내용은 "안티바이러스" 장을 참조하십시오.
AMP 엔진 로그	AMP(Advanced Malware Protection) 기능의 상태에 대한 로깅입니다.
AMP 아카이브	AMP(Advanced Malware Protection)가 검사할 수 없는 첨부 파일이 있거나 악성코드를 포함한 것으로 확인된 메시지를 보관하도록 메일 정책을 구성한 경우 해당 메시지가 여기에 보관됩니다. 형식은 mbox 형식 로그 파일입니다.
검사 로그	검사 로그에는 검사 엔진의 모든 LOG 및 COMMON 메시지가 포함됩니다(경고, 33-34페이지 참조). 일반적으로 애플리케이션 오류, 전송된 알림, 실패한 알림 및 로그 오류 메시지입니다. 이 로그는 시스템 전체 알림에는 적용되지 않습니다.
스팸 격리 로그	스팸 격리 로그는 스팸 격리 프로세스와 관련된 작업을 기록합니다.
스팸 격리 GUI 로그	스팸 격리 로그는 GUI, 최종 사용자 인증 및 최종 사용자 작업(예: 이메일 릴리스)을 통한 구성을 비롯해 스팸 격리와 관련된 동작을 기록합니다.
SMTP 대화 로그	SMTP 대화 로그는 수신 및 발송 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.

표 38-1 로그 유형 (계속)

로그	설명
쿼리 보고 로그	쿼리 보고 로그는 어플라이언스에서 실행되는 보고 쿼리와 관련된 작업을 기록합니다.
업데이터 로그	업데이터 로그는 McAfee 안티바이러스 정의 업데이트와 같은 시스템 서비스 업데이트와 관련된 이벤트를 기록합니다.
추적 로그	추적 로그는 추적 서비스의 프로세스와 관련된 작업을 기록합니다. 추적 로그는 메일 로그의 하위 집합입니다.
인증 로그	인증 로그는 성공적인 사용자 로그인과 실패한 로그인 시도를 기록합니다.
구성 기록 로그	구성 기록 로그는 Email Security 어플라이언스의 변경 사항 및 변경 사항 적용 시기에 대한 정보를 기록합니다. 새 구성 기록 로그는 사용자가 변경사항을 커밋할 때마다 생성됩니다.
업그레이드 로그	업그레이드 다운로드 및 설치에 대한 상태 정보입니다.
API 로그	API 로그는 Cisco AsyncOS API for Email과 관련된 다양한 이벤트를 기록합니다. 예는 다음과 같습니다. • API 시작 또는 중지 • 실패 또는 종료된 API에 대한 연결(응답을 제공한 후) • 인증 성공 또는 실패 • 오류가 있는 요청 • AsyncOS API와 네트워크 구성 변경 사항을 통신하는 동안의 오류

로그 유형 특성

표 38-2는 각 로그 유형의 다양한 특성을 요약합니다.

표 38-2 로그 유형 비교

						포함								
	트랜잭션	무상태(stateless)	텍스트로 기록됨	mbox 파일로 기록됨	이진으로 기록됨	정기적인 상태 정보	메시지 수신 정보	제공 정보	개별 하드 바운스	개별 소프트 바운스	수신 SMTP 대화	헤더 로깅	전송 SMTP 대화	구성 정보
메일 로그	•		•			•	•	•	•	•		•		
qmail 형식 전송 로그		•			•		•	•	•			•		
전송 로그		•			•		•	•	•			•		
바운스 로그	•		•						•	•		•		
상태 로그		•	•			•								
도메인 디버그 로그	•		•					•	•	•			•	

표 38-2 로그 유형 비교 (계속)

						포함								
	트랜잭션	무상태(stateless)	텍스트로 기록됨	mbox 파일로 기록됨	이진으로 기록됨	정기적인 상태 정보	메시지 수신 정보	제공 정보	개별 하드 바운스	개별 소프트 바운스	수신 SMTP 대화	헤더 로깅	전송 SMTP 대화	구성 정보
수신 디버그 로그	•		•				•				•			
시스템 로그	•		•			•								
CLI 감사 로그	•		•			•								
FTP 서버 로그	•		•			•								
HTTP 로그	•		•			•								
NTP 로그	•		•			•								
LDAP 로그	•		•											
안티스팸 로그	•		•			•								
안티스팸 아카이브 로그				•										
안티바이러스 로그	•		•			•								
안티바이러스 아카이브				•										
검사 로그	•		•			•								•
스팸 격리	•		•			•								
스팸 격리 **GUI**	•		•			•								
허용 목록/차단 목록 로그	•		•			•								
보고 로그	•		•		•									
쿼리 보고 로그	•		•		•									
업데이터 로그			•											
추적 로그	•				•	•	•	•	•	•		•		
인증 로그	•		•											
구성 기록 로그	•		•											•
API 로그	•		•											

로그 검색 방법

로그 파일은 다음의 파일 전송 프로토콜에 따라 검색할 수 있습니다. 로그 서브스크립션 프로세스 동안 GUI에서 또는 `logconfig` 명령을 사용하여 로그 서브스크립션을 생성하거나 편집하면서 프로토콜을 설정합니다.

표 38-3 로그 전송 프로토콜

수동 다운로드	이 방법을 사용하면 Log Subscriptions(로그 서브스크립션) 페이지에 있는 로그 디렉토리에 대한 링크를 클릭한 다음 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 프로토콜을 사용하며 기본 검색 방법입니다. **참고** 이 방법을 사용하는 경우, CLI로 이 방법을 지정한다 할지라도, 머신, 그룹 또는 클러스터 수준과 관계없이 클러스터에 있는 어떠한 컴퓨터의 로그도 검색할 수 없습니다.
FTP 푸시	이 방법을 사용하면 원격 컴퓨터에 있는 FTP 서버에 로그 파일을 정기적으로 푸시할 수 있습니다. 서브스크립션에는 원격 컴퓨터의 사용자 이름, 비밀번호 및 대상 디렉토리가 필요합니다. 로그 파일은 설정된 롤오버 일정에 따라 전송됩니다.
SCP 푸시	이 방법을 사용하면 원격 컴퓨터에 있는 SCP 서버에 로그 파일을 정기적으로 푸시할 수 있습니다. 이 방법을 사용하려면 SSH1 또는 SSH2 프로토콜을 사용하는 원격 컴퓨터에 SSH SCP 서버가 필요합니다. 서브스크립션에는 원격 컴퓨터의 사용자 이름, SSH 키 및 대상 디렉토리가 필요합니다. 로그 파일은 설정된 롤오버 일정에 따라 전송됩니다.
Syslog 푸시	이 방법은 원격 syslog 서버에 로그 메시지를 전송합니다. 이 방법은 RFC 3164를 준수합니다. syslog 서버의 호스트 이름을 제출하고 로그 전송을 위해 UDP 또는 TCP를 선택해야 합니다. 사용되는 포트는 514입니다. 기능은 로그에 따라 선택할 수 있지만 로그 유형의 기본값은 드롭다운 메뉴에 사전 선택되어 있습니다. 텍스트 기반 로그만 syslog 푸시를 사용하여 전송할 수 있습니다.

로그 파일 이름 및 디렉토리 구조

AsyncOS는 로그 서브스크립션 이름에 따라 각 로그 서브스크립션에 대한 디렉토리를 생성합니다. 디렉토리에 있는 로그 파일의 실제 이름은 사용자가 지정한 로그 파일 이름, 로그 파일이 시작된 타임스탬프와 단일 문자 상태 코드로 구성되어 있습니다. 로그의 파일 이름은 다음 수식을 사용하여 생성됩니다.

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

상태 코드는 `.current` 또는 `.s`(저장됨을 의미)입니다. 저장된 상태의 로그 파일만 전송하거나 삭제해야 합니다.

로그 롤오버 및 전송 일정

로그 파일은 로그 서브스크립션을 통해 생성되며 첫 번째로 사용자가 지정한 조건(최대 파일 크기 또는 예정된 롤오버)을 만족하면 롤오버(및 푸시 기반 검색 옵션이 선택된 경우에는 전송됨)됩니다. 최대 파일 크기 및 예약된 롤오버의 시간 간격을 모두 구성하려면 CLI의 `logconfig` 명령 또는 GUI의 Log Subscriptions(로그 서브스크립션) 페이지를 사용합니다. 또한 선택한 로그 서브스크립션을 롤오버하려면 GUI의 **Rollover Now(지금 롤오버)** 버튼을 사용하거나 CLI의 `rollovernow` 명령을 사용합니다. 롤오버 일정에 대한 자세한 내용은 로그 서브스크립션 롤오버, 38-41페이지 항목을 참조하십시오.

수동 다운로드를 사용하여 검색된 로그는 지정한 최대 수(기본값은 파일 10개)에 도달할 때까지 또는 시스템에서 로그 파일 공간이 추가로 필요할 때까지 저장됩니다.

기본적으로 활성화된 로그

Email Security 어플라이언스는 기본적으로 활성화된 많은 로그 서브스크립션을 통해 사전 구성됩니다 (다른 로그는 적용한 라이센스 키에 따라 구성될 수 있음). 기본적으로 검색 방법은 "수동 다운로드"입니다.

모든 사전 구성된 로그 서브스크립션은 로그 레벨이 3입니다. (레벨이 1로 설정된 `error_logs`는 예외이므로 오류만 포함함) 자세한 내용은 로그 레벨, 38-37페이지 항목을 참조하십시오. 새 로그 서브스크립션 생성 또는 기존 로그 서브스크립션 수정에 대한 자세한 내용은 로그 서브스크립션, 38-36페이지 항목을 참조하십시오.

로그 유형

로그 파일의 타임스탬프

다음 로그 파일에는 로그의 시작 및 종료 날짜, AsyncOS 버전 및 GMT 오프셋(초 단위이며 로그 시작 시에만 제공)이 포함됩니다.

- 안티바이러스 로그
- LDAP 로그
- 시스템 로그
- 메일 로그

텍스트 메일 로그 사용

이메일 수신, 이메일 전송 및 바운스에 대한 세부 정보를 포함합니다. 상태 정보도 1분 단위로 메일 로그에 기록됩니다. 이 로그는 특정 메시지의 전달을 이해하고 시스템 성능을 분석하는 데 유용하게 사용됩니다.

이 로그에는 특별한 구성이 필요하지 않습니다. 그러나 첨부 파일 이름을 보려면 시스템을 제대로 구성해야 하며 첨부 파일 이름은 경우에 따라 로깅되지 않을 수 있습니다. 자세한 내용은, 메시지 추적 활성화, 29-1페이지 및 메시지 추적 개요, 29-1페이지 항목을 참조하십시오.

텍스트 메일 로그에 표시된 정보는 표 38-4에서 확인할 수 있습니다.

표 38-4 텍스트 메일 로그 통계

통계	설명
ICID	수신 연결 ID입니다. 이것은 시스템에 대한 개별 SMTP 연결에 해당하는 숫자 ID로 이를 통해 한 개에서 수천 개에 이르는 개별 메시지가 전송될 수 있습니다.
DCID	전송 연결 ID입니다. 이것은 다른 서버에 대한 개별 SMTP 연결에 해당하는 숫자 ID로, 한 개에서 수천 개에 이르는 메시지를 전송하는 데 사용되며 각각에는 단일 메시지 전송 시 전달되는 RID가 일부 또는 모두 포함되어 있습니다.
RCID	RPC 연결 ID입니다. 이것은 스팸 격리에 대한 개별 RPC 연결에 해당하는 숫자 ID입니다. 또한 스팸 격리로 전송되는 메시지와 스팸 격리에서 전송되는 메시지를 추적하는 데 사용됩니다.
MID	메시지 ID: 로그를 통해 유입되는 메시지를 추적하는 데 사용됩니다.
RID	수신자 ID: 각 메시지 수신자에게 할당되는 ID입니다.
신규	새 연결이 시작되었습니다.
처음	새 메시지가 시작되었습니다.

텍스트 메일 로그 해석

다음 샘플을 가이드로 사용하여 로그 파일을 해석할 수 있습니다.

참고 로그 파일의 개별 행마다 번호가 지정되어 있지는 않습니다. 다음의 예에서는 샘플을 보여주기 위해 번호가 지정되었습니다.

표 38-5 텍스트 메일 로그 세부 정보

```
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
```

표 38-6을 가이드로 사용하여 앞에 나온 로그 파일을 읽을 수 있습니다.

표 38-6 텍스트 메일 로그 세부 정보의 예

라인 번호	설명
1.	시스템에 대한 새로운 연결이 시작되고 수신 ID(ICID) "5"가 할당되었습니다. 관리 IP 인터페이스에서 연결이 수신되고 이 연결은 10.1.1.209의 원격 호스트에서 시작되었습니다.
2.	클라이언트에서 `MAIL FROM` 명령이 실행된 이후에 메시지에 메시지 ID(MID) "6"이 할당되었습니다.
3.	발신자 주소가 식별되고 수락되었습니다.
4.	수신자가 식별되고 수신자 ID(RID) "0"이 할당되었습니다.
5.	MID 5가 수락되었으며 디스크에 기록되고 확인 응답을 받았습니다.
6.	성공적으로 수신되었고 수신 연결이 종료되었습니다.
7.	다음 메시지 전달 프로세스가 시작됩니다. 192.168.42.42에서 10.5.3.25로 전송 연결 ID(DCID) "8"이 할당되었습니다.
8.	RID "0"으로의 메시지 전달이 시작됩니다.
9.	MID 6에서 RID "0"으로의 전달에 성공합니다.
10.	전송 연결이 종료됩니다.

텍스트 메일 로그 항목의 예

다음은 다양한 상황에 따른 몇 가지 샘플 로그 항목입니다.

메시지 수신 및 전달

메시지는 단일 수신자의 Email Security 어플라이언스에 수신됩니다. 메시지가 성공적으로 전달되었습니다.

```
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
```

성공적인 메시지 전달

```
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
```

실패한 메시지 전달(하드 바운스)

수신자가 2명이 있는 메시지가 Email Security 어플라이언스에 수신됩니다. 전달되는 즉시 대상 호스트에서 5*XX* 메시지를 반환하는데, 이 오류는 메시지를 수신자 모두에게 전송할 수 없음을 의미합니다. 어플라이언스는 발신자에게 알리고 큐에서 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 바운스 이후 성공적인 전달

Email Security 어플라이언스에 메시지가 수신됩니다. 첫 번째 전달 시도 시 메시지가 소프트 바운스되고 다음에 전달하기 위해 큐에 남습니다. 두 번째 시도 시 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

(첨부 파일을 제거할 때) 메시지를 구성 요소 부분으로 나눠 분석할 수 없는 경우 scanconfig 명령을 사용하여 시스템 동작을 판단할 수 있습니다. 옵션은 Deliver, Bounce 또는 Drop입니다.

다음의 예는 scanconfig가 deliver로 설정된 텍스트 메일 로그입니다.

```
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
```

다음의 예는 scanconfig가 drop으로 설정된 텍스트 메일 로그입니다.

```
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 포함된 메시지

이 예에서는 "메시지 본문 포함" 조건이 있는 콘텐츠 필터를 구성하여 첨부 파일 이름 식별 기능을 활성화 합니다.

```
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
```

첨부 파일 3개 중 두 번째 파일은 Unicode입니다. Unicode를 표시할 수 없는 터미널에서 이러한 첨부 파일은 quoted-printable 형식으로 표시됩니다.

생성 또는 재작성된 메시지의 로그 항목

재작성/리디렉션 작업(`alt-rcpt-to` 필터, 안티스팸 rcpt 재작성, `bcc()` 작업, 안티바이러스 리디렉션 등)과 같은 작업에서 새로운 메시지를 생성합니다. 로그를 확인할 때 결과를 확인하고 MID 및 경우에 따라 DCID를 추가해야 할 수 있습니다. 다음과 같은 항목이 가능합니다.

```
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'
```

"재작성" 항목에 대한 흥미로운 점은 재작성 항목은 새로운 MID의 사용을 나타내는 로그의 행 이후에 나타날 수 있다는 점입니다.

스팸 격리로 전송된 메시지

메시지를 격리로 전송할 때 메일 로그는 RCID(RPC 연결 ID)를 사용하여 격리 안팎으로의 이동을 추적하여 RPC 연결을 식별합니다. 다음 메일 로그에서 메시지는 스팸으로 태그가 지정되고 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
```

전송 로그 사용

전송 로그는 AsyncOS의 이메일 전달 작업에 대한 중요 정보를 기록합니다. 로그 메시지는 "무상태(stateless)"인데 이것은 모든 관련 정보가 각 로그 메시지에 기록되며 사용자가 현재 전송 시도에 대한 정보를 얻기 위해 이전 로그 메시지를 참조할 필요가 없음을 의미합니다.

전송 로그는 각 수신자의 이메일 전달 작업에 포함되는 모든 정보를 기록합니다. 모든 정보는 논리적인 방식으로 배치되며 Cisco에서 제공하는 유틸리티를 사용하여 변환한 후에 사용자가 읽을 수 있습니다. 변환 툴은 다음에서 확인할 수 있습니다.
`http://support.ironport.com`

전송 로그는 리소스 효율성을 위해 이진 형식으로 기록되고 전송됩니다. 전송 로그에 기록된 정보는 다음 표에서 확인할 수 있습니다.

표 38-7 전송 로그 통계

통계	설명
전달 상태	성공(메시지가 성공적으로 전달) 또는 바운스(메시지가 하드 바운스됨)
Del_time	전달 시간
Inj_time	수신 시간. `del_time - inj_time` = 수신자 메시지가 큐에서 대기한 시간
Bytes	메시지 크기
Mid	메시지 ID
Ip	수신자 호스트 IP. 수신자 메시지를 수신하거나 바운스한 호스트의 IP 주소
From	Envelope From(봉투 발신자 또는 MAIL FROM이라고도 함)
Source_ip	소스 호스트 IP. 수신 메시지의 호스트 IP 주소
코드	수신자 호스트의 SMTP 응답 코드
답글	수신자 호스트의 SMTP 응답 메시지
Rcpt Rid	수신자 ID. <0>으로 시작되는 수신자 ID. 여러 수신자가 있는 메시지에는 여러 수신자 ID가 있습니다.
To	Envelope To
시도	전달 시도 수

전달 상태가 바운스된 경우 다음의 추가 정보가 전송 로그에 나타납니다.

표 38-8 전송 로그 바운스 정보

통계	설명
사유	전달하는 동안 SMTP 응답에 대한 RFC 1893의 Enhanced Mail Status Code 해석
코드	수신자 호스트의 SMTP 응답 코드
오류	수신자 호스트의 SMTP 응답 메시지

logheaders(메시지 헤더 로깅, 38-40페이지 참조)를 설정하는 경우 다음과 같이 전달 정보 다음에 헤더 정보가 나타납니다.

표 38-9 전송 로그 헤더 정보

통계	설명
Customer_data	로그된 헤더의 시작을 표시하는 XML 태그
헤더 이름	헤더의 이름
값	로그된 헤더의 콘텐츠

전송 로그 항목 예

이 섹션의 예는 다양한 전송 로그 항목을 보여줍니다.

성공적인 메시지 전달

```
<success del_time="Fri Jan 09 15:34:20.234 2004" inj_time="Fri Jan 09 15:33:38.623 2004"
bytes="202" mid="45949" ip="10.1.1.1" from="campaign1@yourdomain.com"
source_ip="192.168.102.1" code="250" reply="sent">

<rcpt rid="0" to="alsdfj.ajsdfl@alsdfj.d2.qa25.qa" attempts="1" />

</success>
```

전달 상태 정보

```
<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 전송 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>
```

바운스 로그 사용

바운스 로그는 각 바운스된 수신자에 대한 모든 정보를 기록합니다. 바운스 로그에 기록된 정보는 표 38-10에서 확인할 수 있습니다.

표 38-10 바운스 로그 통계

통계	설명
타임스탬프	바운스 이벤트 시간
로그 레벨	이 바운스 로그의 상세 설정 레벨
바운스 유형	바운스됨 또는 지연됨(예: 하드 또는 소프트 바운스)
MID/RID	메시지 ID 및 수신자 ID
From	Envelope From
To	Envelope To
사유	전달하는 동안 SMTP 응답에 대한 RFC 1893의 Enhanced Mail Status Code 해석
응답	수신자 호스트의 SMTP 응답 코드 및 메시지

또한 logheaders를 로깅하거나 설정하기 위해 메시지 크기를 지정한 경우(메시지 헤더 로깅, 38-40 페이지 참조), 메시지 및 헤더 정보가 바운스 정보 다음에 나타납니다.

표 38-11 바운스 로그 헤더 정보

헤더	헤더 이름 및 헤더 콘텐츠
메시지	로깅된 메시지 콘텐츠

바운스 로그 항목 예

소프트 바운스 수신자(바운스 유형 = 지연됨)

```
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'])"
```

하드 바운스 수신자(바운스 유형 = 바운스됨)

```
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.'])"
```

메시지 본문 및 Logheaders가 있는 바운스 로그

```
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 `status`, `status detail` 및 `dnsstatus` 등의 CLI 상태 명령을 사용하여 확인된 시스템 통계를 기록합니다. 기록 기간은 `logconfig`의 `setup` 하위 명령을 사용하여 설정됩니다. 상태 로그에서 보고된 각 카운터 또는 속도는 카운터가 마지막으로 재설정된 이후의 값입니다.

상태 로그 읽기

표 38-12의 테이블은 상태 로그 레이블과 일치하는 시스템 통계를 보여줍니다.

표 38-12 상태 로그 통계

통계	설명
CPULd	CPU 사용률
DskIO	디스크 I/O 사용률
RAMUtil	RAM 사용률
QKUsd	사용된 큐(킬로바이트)
QKFre	사용 가능한 큐(킬로바이트)
CrtMID	메시지 ID(MID)
CrtICID	수신 연결 ID(ICID)
CRTDCID	전송 연결 ID(DCID)
InjBytes	수신되는 총 메시지 크기(바이트)
InjMsg	수신된 메시지
InjRcp	수신된 수신자
GenBncRcp	생성된 바운스 수신자
RejRcp	거부된 수신자
DrpMsg	삭제(drop)된 메시지
SftBncEvnt	소프트 바운스 이벤트
CmpRcp	완료된 수신자

표 38-12 상태 로그 통계 (계속)

통계	설명
HrdBncRcp	하드 바운스 수신자
DnsHrdBnc	DNS 하드 바운스
5XXHrdBnc	5XX 하드 바운스
FltrHrdBnc	필터 하드 바운스
ExpHrdBnc	만료된 하드 바운스
OtrHrdBnc	기타 하드 바운스
DlvRcp	전달된 수신자
DelRcp	삭제된 수신자
GlbUnsbHt	전역 가입 취소 횟수
ActvRcp	활성 수신자
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 사용된 총 CPU 시간
CPUETm	애플리케이션이 시작된 이후 경과한 시간
MaxIO	메일 프로세스의 초당 최대 디스크 I/O 작업
RamUsd	할당된 메모리(바이트)
SwIn	스왑인 메모리
SwOut	스왑 아웃된 메모리
SwPgIn	페이지인 메모리
SwPgOut	페이지 아웃된 메모리
MMLen	시스템에 있는 총 메시지 수
DstInMem	메모리에 있는 대상 객체 수
ResCon	리소스 보존 tarpit 값. 과도한 시스템 부하로 인해 이 시간(초) 동안 수신 메일 수락이 지연됩니다.
WorkQ	이 작업 큐에 있는 현재 메시지 수
QuarMsgs	정책, 바이러스 또는 신종 바이러스 격리(여러 격리에 존재하는 메시지는 한 번만 계산됨)에 있는 개별 메시지 수
QuarQKUsd	정책, 바이러스 및 신종 바이러스 격리 메시지에서 사용된 킬로바이트
LogUsd	사용된 로그 파티션 백분율

표 38-12 상태 로그 통계 (계속)

통계	설명
AVLd	안티바이러스 검사에서 사용된 CPU 백분율
CmrkLd	Cloudmark 안티스팸 검사에서 사용된 CPU 백분율
SophLd	Sophos 안티스팸 검사에서 사용된 CPU 백분율
McafLd	McAfee 안티바이러스 검사에서 사용된 CPU 백분율
CASELd	CASE 검사에서 사용된 CPU 백분율
TotalLd	총 CPU 소비
LogAvail	로그 파일에 사용 가능한 디스크 공간
EuQ	스팸 격리에 있는 예상 메시지 수
EuqRls	스팸 격리 릴리스 큐에 있는 예상 메시지 수

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 어플라이언스 및 지정된 수신자 호스트 간의 SMTP 대화 중에 클라이언트 및 서버 통신을 기록합니다. 이러한 로그 유형은 특정한 수신자 호스트의 문제를 디버깅하는 데 주로 사용됩니다.

표 38-13 도메인 디버그 로그 통계

통계	설명
타임스탬프	바운스 이벤트 시간
로그 레벨	이 바운스 로그의 상세 설정 레벨
From	Envelope From
To	Envelope To
사유	전달하는 동안 SMTP 응답에 대한 RFC 1893의 Enhanced Mail Status Code 해석
응답	수신자 호스트의 SMTP 응답 코드 및 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'
```

수신 디버그 로그 사용

수신 디버그 로그는 Email Security 어플라이언스와 시스템에 연결 중인 지정된 호스트 간에 SMTP 대화를 기록합니다. 수신 디버그 로그는 인터넷에서 연결을 시작하는 클라이언트와 Email Security 어플라이언스 간의 통신 문제를 해결하는 데 유용합니다. 로그는 두 시스템 간에 전송된 모든 바이트를 기록하며 해당 바이트를 연결 호스트의 "Sent to" 또는 연결 호스트의 "Received from"으로 분류합니다.

IP 주소, IP 범위, 호스트 이름 또는 부분 호스트 이름을 지정하여 기록할 호스트 대화를 지정해야 합니다. IP 범위 내의 모든 연결 IP 주소가 기록됩니다. 부분 도메인 내의 모든 호스트가 기록됩니다. 시스템은 호스트 이름으로 변환하기 위해 연결 IP 주소에 역방향 DNS 조회를 수행합니다. DNS에 일치하는 PTR 레코드가 없는 IP 주소는 호스트 이름과 일치하지 않습니다.

기록할 세션 수도 지정해야 합니다.

수신 디버그 로그의 각 행에는 표 38-14의 다음 정보가 포함되어 있습니다.

표 38-14 수신 디버그 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
ICID	수신 연결 ID는 다른 로그 서브스크립션의 동일한 연결에 연결될 수 있는 고유한 식별자입니다.
전송됨/수신됨	"Sent to"로 표시된 행은 연결 호스트에 전송된 실제 바이트입니다. "Received from"으로 표시된 행은 연결 호스트에서 수신된 실제 바이트입니다.
IP 주소	연결 호스트의 IP 주소

수신 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 38-15 시스템 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	로깅된 이벤트

시스템 로그 예

이 예에서 시스템 로그는 일부 커밋된 항목을 보여줍니다. (커밋을 실행 중인 사용자의 이름 및 입력한 주석 포함)

```
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 38-16 CLI 감사 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
PID	명령어가 입력된 특정한 CLI 세션의 프로세스 ID
메시지	메시지는 입력된 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 38-17 FTP 서버 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
ID	연결 ID. 각 FTP 연결에 대한 별도의 ID
메시지	로그 항목의 메시지 섹션에는 로그 파일 상태 정보 또는 FTP 연결 정보(로그인, 업로드, 다운로드, 로그아웃 등)가 올 수 있습니다.

FTP 서버 로그 예

이 예에서 FTP 서버 로그는 연결(ID:1)을 기록합니다. 수신 연결의 IP 주소, 작업(파일 업로드 및 다운로드) 및 로그아웃 정보가 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 38-18 HTTP 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
ID	세션 ID
req	연결 중인 머신의 IP 주소
user	연결 중인 사용자의 사용자 이름
메시지	수행된 작업에 대한 정보. GET 또는 POST 명령 또는 시스템 상태 등을 포함할 수 있습니다.

HTTP 로그 예

이 예에서 HTTP 로그는 admin 사용자의 GUI와의 상호 작용을 보여줍니다. (시스템 설치 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 38-19 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 NTP 호스트를 두 번 폴링하는 어플라이언스를 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 엔진의 모든 LOG 및 COMMON 메시지가 포함됩니다. 사용 가능한 COMMON 및 LOG 알림 메시지 목록은 "시스템 관리" 장의 알림 섹션을 참조하십시오.

표 38-20 검사 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 애플리케이션 오류, 전송된 알림, 실패한 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...".
```

안티스팸 로그 사용

표 38-21 안티스팸 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 안티스팸 업데이트에 대한 검사 및 결과(엔진 또는 안티스팸 규칙에 대한 업데이트의 필요 여부 등)로 구성됩니다.

안티스팸 로그 예

이 예에서 안티스팸 로그는 스팸 정의에 대한 업데이트 및 CASE 업데이트에 대한 안티스팸 엔진 검사를 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
```

안티바이러스 로그 사용

표 38-22 안티바이러스 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 안티바이러스 업데이트에 대한 검사 및 결과(엔진 또는 바이러스 정의에 대한 업데이트의 필요 여부 등)로 구성됩니다.

안티바이러스 로그 예

이 예에서 안티바이러스 로그는 바이러스 정의(IDE) 및 엔진 자체 업데이트에 대한 Sophos 안티바이러스 엔진 검사를 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 진단하기 위해 이 로그를 일시적으로 DEBUG 수준으로 설정할 수 있습니다. DEBUG 로깅 정보는 자세한 정보를 표시하므로 주의해서 사용해야 합니다.

스팸 격리 로그 사용

표 38-23 스팸 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 수행한 작업(격리된 메시지 또는 격리에서 릴리스된 메시지 등)으로 구성됩니다.

스팸 격리 로그 예

이 예에서 로그는 격리에서 admin@example.com으로 릴리스되고 있는 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 38-24 스팸 GUI 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 사용자 인증 등 수행한 작업으로 구성됩니다.

스팸 격리 GUI 로그 예

이 예에서 로그는 성공한 인증, 로그인 및 로그아웃 정보를 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 38-25 LDAP 디버그 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	LDAP 디버그 메시지

LDAP 디버그 로그 예

참고 로그 파일의 개별 행마다 번호가 지정되어 있지는 않습니다. 다음의 예에서는 샘플을 보여주기 위해 번호가 지정되었습니다.

```
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.r
      oute.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.ro
      ute.local.add00002.qa)) returned 1 results

11    Thu Sep  9 13:00:09 2004 LDAP: returning: [<LDAP:>]
```

가이드로 사용하여 앞에 나온 로그 파일을 읽을 수 있습니다.

표 38-26 LDAP 디버그 로그 세부 정보의 예

라인 번호	설명
1.	로그 파일이 초기화됩니다.
2. 3. 4.	리스너는 LDAP을 사용하여 마스커레이드하도록 구성됩니다. (특히 "sun.masquerade"라는 LDAP 쿼리 사용) LDAP 서버에서 주소 employee@routing.qa를 조회하고 일치 항목을 찾습니다. 조회된 마스커레이드 주소는 employee@mail.qa이며 이 주소는 마스커레이드 구성에 따라 메시지 헤더 및/또는 Envelope From에 기록됩니다.
5.	사용자는 수동으로 `ldapflush`를 실행합니다.
6.	쿼리는 sun.qa, 포트 389로 전송됩니다. 쿼리 템플릿은 (&(ObjectClass={g})(mailLocalAddress={a}))입니다. {g}는 호출 필터에 지정된 그룹 이름(rcpt-to-group 또는 mail-from-group 규칙)으로 대체됩니다. {a}는 문제의 주소로 대체됩니다.
7. 8.	이전에 설명한 대체 작업이 지금 수행되고 쿼리가 LDAP 서버에 전송되기 이전의 내용입니다.
9.	서버에 대한 연결이 아직 설정되지 않았으므로 연결을 설정합니다.
10.	서버로 전송된 데이터입니다.
11.	결과는 empty positive입니다. 이것은 레코드 1개가 반환되었지만 쿼리에서 필드를 요청하지 않았으므로 보고할 데이터가 없음을 의미합니다. 이것은 두 그룹 모두에 사용되며 쿼리가 데이터베이스에서 일치하는 항목이 있는지 확인하기 위해 검사할 때 쿼리를 수락합니다.

허용 목록/차단 목록 로그 사용

표 38-27은 허용 목록/차단 목록 로그에 기록된 통계를 보여줍니다.

표 38-27 허용 목록/차단 목록 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 사용자 인증 등 수행한 작업으로 구성됩니다.

허용 목록/차단 목록 로그 예

이 예에서 허용 목록/차단 목록 로그는 2시간 마다 데이터베이스 스냅샷을 생성하는 어플라이언스를 보여줍니다. 또한 발신자가 데이터베이스에 추가된 시간도 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

표 38-28은 보고 로그에 기록된 통계를 보여줍니다.

표 38-28 보고 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 사용자 인증 등 수행한 작업으로 구성됩니다.

보고 로그 예

이 예에서 보고 로그는 정보 로그 레벨로 설정된 어플라이언스를 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
```

쿼리 보고 로그 사용

표 38-29는 쿼리 보고 로그에 기록된 통계를 보여줍니다.

표 38-29 쿼리 보고 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 사용자 인증 등 수행한 작업으로 구성됩니다.

쿼리 보고 로그 예

이 예에서 쿼리 보고 로그는 2007년 8월 29일부터 10월 10일 사이에 일일 발송 이메일 트래픽 쿼리를 실행 중인 어플라이언스를 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_CONTEN

T_FILTER', 'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_CLEAN_RECIPIENTS',
'MAIL_OUTGOING_TRAFFIC_SUMMARY.TOTAL_RECI
```

```
PIENTS_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_ascendin

g=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_SUMM

ARY.TOTAL_RECIPIENTS'] for rollup period "day" with interval range 2007-08-29 to
2007-10-01 with key constra

ints 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.
```

업데이터 로그 사용

표 38-30 업데이터 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 시스템 서비스 업데이트 정보와 업데이트 및 다음 업데이트의 예정 날짜 및 시간을 검사하는 AsyncOS 작업으로 구성됩니다.

업데이터 로그 예

이 예에서 로그는 새로운 McAfee 안티바이러스 정의로 업데이트 중인 어플라이언스를 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
```

추적 로그 이해

추적 로그는 AsyncOS의 이메일 작업에 대한 중요 정보를 기록합니다. 로그 메시지는 메일 로그에 기록된 메시지의 하위 집합입니다.

추적 로그는 메시지 추적 데이터베이스를 구축하기 위해 어플라이언스의 메시지 추적 구성 요소에서 사용됩니다. 로그 파일이 데이터베이스 구축 프로세스에서 사용되기 때문에 추적 로그는 일시적입니다. 추적 로그의 정보는 사용자가 읽거나 분석할 수 없습니다.

Cisco Security Management 어플라이언스를 사용하여 여러 Email Security 어플라이언스의 추적 정보를 확인할 수 있습니다.

인증 로그 사용

인증 로그는 성공적인 사용자 로그인과 실패한 로그인 시도를 기록합니다.

표 38-31 인증 로그 통계

통계	설명
타임스탬프	바이트가 전송된 시간
메시지	메시지는 어플라이언스에 로그인하려고 시도하는 사용자의 사용자 이름 및 이 사용자가 성공적으로 인증되었는지에 대한 정보로 구성됩니다.

인증 로그 예

이 예에서 로그는 사용자 "admin," "joe," 그리고 "dan"이 수행하는 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.
```

구성 기록 로그 사용

구성 기록 로그는 사용자 이름, 사용자가 변경한 구성에 대한 설명과 변경 사항을 커밋할 때 사용자가 입력한 설명을 나열하는 추가 섹션이 있는 구성 파일로 구성됩니다. 사용자가 변경 사항을 커밋할 때마다 변경 후의 구성 파일이 포함된 새 로그가 생성됩니다.

구성 기록 로그 예

이 예에서 구성 기록 로그는 사용자(관리자)가 시스템에 로그인할 수 있는 로컬 사용자를 정의하는 테이블에 게스트 사용자가 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>
```

로그 서브스크립션

로그 서브스크립션 구성

System Administration(시스템 관리) 메뉴의 Log Subscriptions(로그 서브스크립션) 페이지(또는 CLI의 `logconfig` 명령)에서 로그 서브스크립션을 구성합니다. 로그 서브스크립션은 AsyncOS 활동(오류 포함)에 대한 정보를 저장하는 로그 파일을 생성합니다. 로그 서브스크립션을 검색하거나 다른 컴퓨터로 전달(푸시)할 수 있습니다. 일반적으로 로그 서브스크립션에는 다음의 특성이 있습니다.

표 38-32 로그 파일 특성

특성	설명
로그 유형	기록된 정보 유형 및 로그 서브스크립션의 형식을 정의합니다. 자세한 내용은 표 38-1, "로그 유형" (2페이지) 항목을 참조하십시오.
이름	이후 참조에 사용하는 로그 서브스크립션에 대한 별칭입니다.
파일 크기별 롤오버	롤오버 이전에 도달할 수 있는 파일의 최대 크기입니다.
시간별 롤오버	파일 롤오버의 시간 간격을 설정합니다.
로그 레벨	각 로그 서브스크립션에 대한 상세 설정 레벨을 설정합니다.
검색 방법	Email Security 어플라이언스에서 로그 서브스크립션을 얻는 방법을 정의합니다.
로그 파일 이름	디스크에 기록할 때 파일의 물리적 이름으로 사용됩니다. 여러 Email Security 어플라이언스를 사용 중인 경우 로그 파일 이름은 로그 파일을 생성한 시스템을 식별하기 위해 고유해야 합니다.

로그 레벨

로그 레벨은 로그에서 전달되는 정보의 크기를 결정합니다. 로그는 5가지 상세 설정 레벨로 구성할 수 있습니다. 더 상세하게 로그를 설정하면 더 큰 로그 파일을 생성되어 시스템 성능이 저하됩니다. 상위 단계 설정에는 하위 단계에 포함되어 있는 모든 메시지와 추가 메시지가 포함되어 있습니다. 상세 설정 레벨이 높을수록 시스템 성능이 저하됩니다.

참고 모든 메일 로그 유형에 대해 로그 레벨을 선택할 수 있습니다.

표 38-33 로그 레벨

로그 레벨	설명
중요	가장 상세하지 않은 설정입니다. 오류만 로깅됩니다. 이 설정을 사용하면 성능 및 기타 중요한 작업을 모니터링할 수 없습니다. 단, 로그 파일이 금방 최대 크기에 도달하지 않습니다. 이 로그 레벨은 syslog 수준의 "알림"과 같습니다.
경고	시스템에서 발생한 모든 오류 및 경고입니다. 이 설정을 사용하면 성능 및 기타 중요한 작업을 모니터링할 수 없습니다. 이 로그 레벨은 syslog 수준의 "경고"와 같습니다.
정보	정보 설정은 시스템 작업을 초단위로 캡처합니다. 예를 들어, 연결이 열리거나 전달이 시도되는 것을 기록합니다. 이 레벨은 로그에 권장되는 설정입니다. 이 로그 레벨은 syslog 수준의 "정보"와 같습니다.

표 38-33 로그 레벨 (계속)

로그 레벨	설명
디버그	오류의 원인을 확인하려고 시도할 때 디버그 로그 레벨을 사용합니다. 이 설정을 일시적으로 사용한 다음 기본 레벨로 돌아갑니다. 이 로그 레벨은 syslog 수준의 "디버그"와 같습니다.
추적	추적 로그 레벨은 개발자용으로만 권장됩니다. 이 레벨을 사용하면 시스템 성능이 심각하게 저하되므로 권장되지 않습니다. 이 로그 레벨은 syslog 수준의 "디버그"와 같습니다.

GUI에서 로그 서브스크립션 생성

절차

1단계 **System Administration(시스템 관리) > Log Subscription(로그 서브스크립션)**을 선택합니다.

2단계 **Add Log Subscription(로그 서브스크립션 추가)**을 클릭합니다.

3단계 로그 유형을 선택하고 로그 이름(로그 디렉토리용)과 로그 파일의 이름을 입력합니다.

4단계 AsyncOS가 로그 파일을 롤오버 하기 전의 최대 파일 크기와 롤오버 시간 간격을 지정합니다. 로그 파일 롤오버에 대한 자세한 내용은 로그 서브스크립션 롤오버, 38-41페이지 항목을 참조하십시오.

5단계 로그 레벨을 선택합니다. 사용 가능한 옵션은 중요, 경고, 정보, 디버그, 추적입니다.

6단계 로그 검색 방법을 구성합니다.

7단계 변경사항을 제출하고 커밋합니다.

로그 서브스크립션 편집

절차

1단계 **System Administration(시스템 관리) > Log Subscription(로그 서브스크립션)**을 선택합니다.

2단계 Log Settings(로그 설정) 열에서 로그 이름을 클릭합니다.

3단계 로그 서브스크립션을 변경합니다.

4단계 변경사항을 제출하고 커밋합니다.

로깅을 위한 전역 설정 구성

시스템은 정기적으로 텍스트 메일 로그 및 상태 로그의 시스템 측정치를 기록합니다. 다음을 구성하려면 System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션) 페이지의 Global Settings(전역 설정) 섹션에서 **Edit Settings(설정 편집)** 버튼을 클릭합니다. (또는 CLI의 `logconfig -> setup` 명령)

- 시스템 측정 빈도. 시스템이 측정치를 기록하는 동안 대기하는 시간(초)입니다.
- 메시지 ID 헤더의 기록 여부.

- 원격 응답 상태 코드의 기록 여부.
- 원본 메시지의 제목 헤더의 기록 여부.
- 각 메시지에 대해 로깅해야 할 헤더 목록.

모든 로그에는 선택적으로 다음의 3가지 데이터가 포함됩니다.

1. 메시지 ID

   이 옵션이 구성되어 있고 사용 가능한 경우 모든 메시지에 로깅된 메시지 ID 헤더가 포함됩니다. 이 메시지 ID는 수신된 메시지에서 가져오거나 AsyncOS 자체에서 생성될 수 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 구성되어 있고 사용 가능한 경우 모든 메시지에 로깅된 원격 응답 상태 코드가 포함됩니다. 예를 들면 다음과 같습니다.

```
Tue Apr 6 14:38:34 2004 Info: MID 1 RID [0] Response 'queued as 9C8B425DA7'
```

   원격 응답 문자열은 전송 SMTP 대화 중에 DATA 명령에 응답한 이후에 수신한 사용자가 읽을 수 있는 텍스트입니다. 이 예에서 연결 호스트가 데이터 명령을 실행한 이후의 원격 응답은 "queued as 9C8B425DA7"입니다.

```
[...]

250 ok hostname

250 Ok: queued as 9C8B425DA7
```

   공백, 구두점(및 250 응답의 경우 OK 문자)은 문자열 시작 부분에서 제거됩니다. 공백만 문자열 끝에서 제거됩니다. 예를 들어, Email Security 어플라이언스는 기본적으로 250 Ok: Message MID accepted 문자열이 있는 DATA 명령에 응답합니다. 따라서 원격 호스트가 다른 Email Security 어플라이언스인 경우 "Message MID accepted" 문자열이 로깅됩니다.

3. 원본 제목 헤더

   이 옵션이 활성화된 경우 각 메시지의 원본 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 메시지 헤더가 시스템을 통과할 때 메시지 헤더의 상태 및 콘텐츠를 기록해야 합니다. Log Subscriptions Global Settings(로그 서브스크립션 전역 설정) 페이지(또는 CLI의 `logconfig` -> `logheaders` 하위 명령)에서 기록할 헤더를 지정합니다. Email Security 어플라이언스는 텍스트 메일 로그, 전송 로그 및 바운스 로그에 지정된 메시지 헤더를 기록합니다. 헤더가 있는 경우 시스템은 헤더 이름 및 값을 기록합니다. 헤더가 없는 경우 로그에 아무 내용도 기록되지 않습니다.

참고 시스템은 로깅을 위해 지정된 헤더와 관계없이 기록을 위해 메시지를 처리하는 동안 언제든지 메시지에 있는 모든 헤더를 평가합니다.

참고 SMTP 프로토콜에 대한 RFC는 `http://www.faqs.org/rfcs/rfc2821.html`에서 확인할 수 있으며 사용자 정의 헤더를 정의합니다.

참고 `logheaders` 명령을 통해 로깅할 헤더를 구성한 경우 헤더 정보는 다음과 같이 전달 정보 이후에 나타납니다.

표 38-34 로그 헤더

헤더 이름	헤더의 이름
값	로그된 헤더의 콘텐츠

예를 들어 로깅할 헤더로 "date, x-subject"를 지정하면 다음 행이 메일 로그에 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 로깅을 위한 전역 설정 구성

절차

1단계 **System Administration(시스템 관리) > Log Subscription(로그 서브스크립션)**을 선택합니다.

2단계 아래로 스크롤하여 **Global Settings(전역 설정)** 섹션으로 이동합니다.

3단계 **Edit Settings(설정 편집)**를 클릭합니다.

4단계 시스템 측정 빈도, 메일 로그에 메시지 ID 헤더를 포함할지, 원격 응답을 포함할지 및 메시지마다 원본 제목 헤더를 포함할지 등의 정보를 지정합니다.

5단계 로그에 포함할 다른 헤더를 입력합니다.

6단계 변경사항을 제출하고 커밋합니다.

로그 서브스크립션 롤오버

어플라이언스에서 로그 파일이 지나치게 커지는 것을 방지하기 위해 AsyncOS는 로그 파일이 사용자가 지정한 최대 파일 크기 또는 시간 간격에 도달할 경우 로그 파일을 "롤오버" 및 아카이브하고 수신 로그 데이터에 대해 새 파일을 생성합니다. 로그 서브스크립션을 위해 정의한 검색 방법에 따라 기존 로그 파일은 검색을 위해 어플라이언스에 저장되거나 외부 컴퓨터에 전송됩니다. 어플라이언스에서 로그 파일을 검색하는 방법에 대한 자세한 내용은 로그 검색 방법, 38-6페이지 항목을 참조하십시오.

AsyncOS는 로그 파일을 롤오버할 때 다음 작업을 수행합니다.

- 현재 로그 파일의 이름을 롤오버 타임스탬프와 저장된 상태를 의미하는 "**s**" 확장명으로 변경합니다.
- 새 로그 파일을 생성하고 이 파일을 "**current**" 확장명을 사용하여 최신 파일로 지정합니다.
- 새로 저장한 로그 파일을 원격 호스트에 전송합니다. (푸시 기반 검색 방법을 사용하는 경우)
- 동일한 서브스크립션에서 이전에 성공하지 못한 모든 로그 파일을 전송합니다. (푸시 기반 검색 방법을 사용하는 경우)
- 보관 가능 총 파일 수가 초과된 경우로그 서브스크립션에서 가장 오래된 파일을 삭제합니다 (폴 기반 검색 방법을 사용하는 경우).

GUI의 System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션) 페이지 또는 CLI의 `logconfig` 명령을 사용하여 서브스크립션을 생성 또는 편집 시 로그 서브스크립션의 롤오버 설정을 정의합니다. 로그 파일 롤오버를 트리거하기 위해 다음의 2가지 설정을 사용할 수 있습니다.

- 최대 파일 크기.
- 시간 간격.

파일 크기별 롤오버

AsyncOS는 로그 파일이 디스크 공간을 너무 많이 사용하는 것을 방지하기 위해 로그가 최대 파일 크기에 도달하면 로그 파일을 롤오버합니다. 롤오버를 위한 최대 파일 크기를 정의할 때 메가바이트의 경우 접미사 `m`을 사용하고 킬로바이트의 경우 접미사 `k`를 사용합니다. 예를 들어 AsyncOS가 로그 파일이 10메가바이트에 도달할 때 로그 파일을 롤오버 하려면 `10m`을 입력합니다.

시간별 롤오버

정기적으로 롤오버가 발생하도록 일정을 예약하려면, 다음의 시간 간격을 선택할 수 있습니다.

- **없음.** AsyncOS는 로그 파일이 최대 파일 크기에 도달하면 롤오버를 수행합니다.
- **사용자 지정 시간 간격.** AsyncOS는 이전 롤오버 후 지정한 시간이 경과하면 롤오버를 수행합니다. 예약된 롤오버를 수행하기 위해 사용자 지정 시간 간격을 생성하려면 `d`, `h` 및 `m`을 접미사로 사용하여 롤오버 간격을 일, 시간 및 분 단위로 입력합니다.
- **일별 롤오버.** AsyncOS는 지정된 시간에 매일 롤오버를 수행합니다. 일별 롤오버를 선택하는 경우, 24시간 형식(HH:MM)을 사용하여 AsyncOS가 롤오버를 수행하는 시간을 입력합니다.

  Daily Rollover(일별 롤오버) 옵션은 GUI에서만 제공됩니다. CLI의 `logconfig` 명령을 사용하여 일별 롤오버를 구성하려는 경우, Weekly Rollover(주별 롤오버) 옵션을 선택하고 별표(*)를 사용하여 AsyncOS가 일주일 내내 롤오버를 수행하도록 지정합니다.
- **주별 롤오버.** AsyncOS는 일주일에 하루 이상 지정된 시간에 롤오버를 수행합니다. 예를 들어, 수요일과 금요일 자정마다 로그 파일을 롤오버하도록 AsyncOS를 설정할 수 있습니다. 주별 롤오버를 구성하려면 롤오버를 수행할 요일과 24시간 형식(HH:MM)의 시간을 선택합니다.

CLI를 사용할 경우, 대시(-)를 사용하여 요일 범위를 지정하고 별표(*)를 사용하여 주의 모든 요일을 지정하거나 쉼표(,)를 사용하여 여러 요일과 시간을 구분할 수 있습니다.

표 38-35는 CLI를 사용하여 수요일과 금요일 자정(00:00)마다 로그 서브스크립션의 파일을 롤오버하는 방법을 보여줍니다.

표 38-35 CLI에서 주별 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. 월

2. 2015년 2월 3일

3. 수

4. 목

5. 금

6. 토

7. 일요일

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
```

요청 시 로그 서브스크립션 롤오버

GUI를 사용하여 즉시 로그 서브스크립션을 롤오버하려면 다음을 수행합니다.

절차

1단계 System Administration(시스템 관리) > Log Subscriptions(로그 서브스크립션) 페이지에서 롤오버할 로그 오른쪽에 있는 확인란을 체크합니다.

2단계 또는 모든 확인란을 체크하여 모든 로그를 롤오버하도록 선택할 수 있습니다.

3단계 롤오버할 로그가 하나 이상 선택된 경우 **Rollover Now(지금 롤오버)** 버튼이 활성화됩니다. **Rollover Now(지금 롤오버)** 버튼을 클릭하여 선택한 로그를 롤오버합니다.

GUI에서 최근 로그 항목 보기

시작하기 전에

GUI를 통해 로그를 확인하려면 Management(관리) 인터페이스에서 HTTP 또는 HTTPS 서비스를 활성화해야 합니다.

절차

1단계 **System Administration(시스템 관리) > Log Subscription(로그 서브스크립션)**을 선택합니다.

2단계 테이블의 **Log Files(로그 파일)** 열에서 로그 서브스크립션을 선택합니다.

3단계 로그인합니다.

4단계 브라우저에서 확인하거나 디스크로 저장하려면 로그 파일을 선택합니다.

CLI에서 최근 로그 항목 보기(tail 명령)

AsyncOS는 어플라이언스에서 구성한 로그의 최근 항목을 보여주는 `tail` 명령을 지원합니다. `tail` 명령을 실행하고 최근에 구성한 로그를 선택하여 확인합니다. `tail` 명령을 종료하려면 Ctrl-C를 사용합니다.

예

다음 예에서는 시스템 로그를 확인하기 위해 `tail` 명령을 사용합니다. (이 로그는 `commit` 명령에서 사용자 주석을 추적합니다.) 또한 tail 명령은 매개변수로 간주할 로그의 이름을 수락합니다. (예: `tail mail_logs`)

```
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

`logconfig -> hostkeyconfig` 하위 명령을 사용하여 Email Security 어플라이언스에서 다른 서버로 로그를 푸시할 경우 SSH에 사용할 호스트 키를 관리할 수 있습니다. SSH 서버에는 개인 키 1개와 공용 키 1개로 이루어진 호스트 키 쌍이 필요합니다. 개인 호스트 키는 SSH 서버에 있으며 원격 머신에서는 읽을 수 없습니다. 공개 호스트 키는 SSH 서버와 상호작용해야 하는 모든 클라이언트 머신에 분배됩니다.

참고 사용자 키를 관리하려면 SSH(Secure Shell) 키 관리, 32-28페이지 항목을 참조하십시오.

`hostkeyconfig` 하위 명령은 다음 기능을 수행합니다.

표 38-36 호스트 키 관리 - 하위 명령 목록

명령어	설명
신규	새 키를 추가합니다.
수정	기존 키를 수정합니다.
삭제	기존 키를 삭제합니다.
검사	자동으로 호스트 키를 다운로드합니다.
인쇄	키를 표시합니다.
호스트	시스템 호스트 키를 표시합니다. 이것은 원격 시스템의 'known_hosts' 파일에 있는 값입니다.
지문	시스템 호스트 키 지문을 표시합니다.
사용자	원격 머신에 로그를 푸시하는 시스템 계정의 공개 키를 표시합니다. 이것은 SCP 푸시 서브스크립션을 설정할 때 표시되는 키와 동일한 키입니다. 이것은 원격 시스템의 'authorized_keys' 파일에 있는 값입니다.

다음 예에서 AsyncOS는 호스트 키를 검사하고 이 키를 호스트로 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.

[]>
```

39 장

클러스터를 사용한 중앙 집중식 관리

클러스터를 사용한 중앙 집중식 관리 개요

Cisco의 중앙 집중식 관리 기능을 사용하면 여러 어플라이언스를 동시에 관리 및 구성하여 관리 시간을 줄이고 네트워크 전체에서 일관된 구성을 유지할 수 있습니다. 여러 어플라이언스를 관리하기 위해 추가 하드웨어를 구입할 필요가 없습니다. 중앙 집중식 관리 기능은 네트워크의 안정성, 유연성 및 확장성을 개선하며 로컬 정책을 준수하면서 전역으로 관리할 수 있도록 해 줍니다.

*클러스터*는 구성 정보를 공유하는 일련의 머신으로 정의됩니다. 클러스터 내 머신(Cisco 어플라이언스)은 여러 *그룹*으로 나뉘며 각 클러스터에는 적어도 하나의 그룹을 포함됩니다. 지정된 머신은 유일하게 존재하는 하나의 그룹에 속한 멤버입니다. 관리자 사용자는 클러스터 전체나 그룹 전체 또는 머신별로 서로 다른 시스템 요소를 구성하여 네트워크, 지리적 위치, 사업 부서 또는 기타 논리적 관계에 따라 Cisco 어플라이언스를 분할할 수 있습니다.

클러스터는 *P2P(peer-to-peer)* 아키텍처로 구현되며 클러스터 내에는 마스터/슬레이브 관계가 없습니다. 머신에 로그인하여 클러스터를 제어 및 관리할 수 있습니다. (그러나 일부 구성 명령은 제한됩니다. 제한된 명령, 39-14페이지 참조.)

사용자 데이터베이스는 클러스터 내 모든 머신에서 공유됩니다. 따라서 전체 클러스터에는 단 하나의 사용자 집합과 한 명의 관리자 사용자(연결된 비밀번호 사용)만 존재합니다. 클러스터에 조인한 모든 머신은 클러스터의 *관리자 비밀번호*라고 하는 단일 관리자 비밀번호를 공유합니다.

클러스터 요구 사항

- 클러스터의 머신에는 DNS에서 확인이 가능한 호스트 이름이 있어야 합니다. 아니면 IP 주소를 대신 사용할 수 있지만 두 가지를 모두 사용할 수는 없습니다.

  DNS 및 호스트 이름 확인, 39-18페이지 항목을 참조하십시오. 클러스터 통신은 일반적으로 머신의 DNS 호스트 이름을 사용하여 시작됩니다.

- 클러스터는 모두 동일한 AsyncOS 버전을 실행하는 머신으로 구성되어야 합니다.

  클러스터 멤버를 업그레이드하는 방법은 클러스터의 머신 업그레이드, 39-12페이지 항목을 참조하십시오.

- 머신은 SSH(일반적으로 포트 22) *또는* 클러스터 통신 서비스(CCS)를 통해 클러스터에 조인할 수 있습니다.

  클러스터 통신, 39-18페이지 항목을 참조하십시오.

- 머신이 클러스터에 조인한 경우 SSH 또는 클러스터 통신 서비스를 통해 통신할 수 있습니다. 사용되는 포트를 구성할 수 있습니다. SSH는 일반적으로 포트 22에서 사용되고 CCS는 기본적으로 포트 2222에서 사용되지만, 이러한 서비스를 다른 포트에서도 구성할 수 있습니다.

  어플라이언스를 위해 열리는 표준 방화벽 포트 외에, CCS를 통해 통신하는 클러스터된 머신은 CCS 포트를 통해 서로 연결할 수 있어야 합니다. 클러스터 통신, 39-18페이지 항목을 참조하십시오.

- 머신 클러스터를 생성, 조인 또는 구성하려면 명령줄 인터페이스(CLI) 명령 `clusterconfig`를 사용해야 합니다.

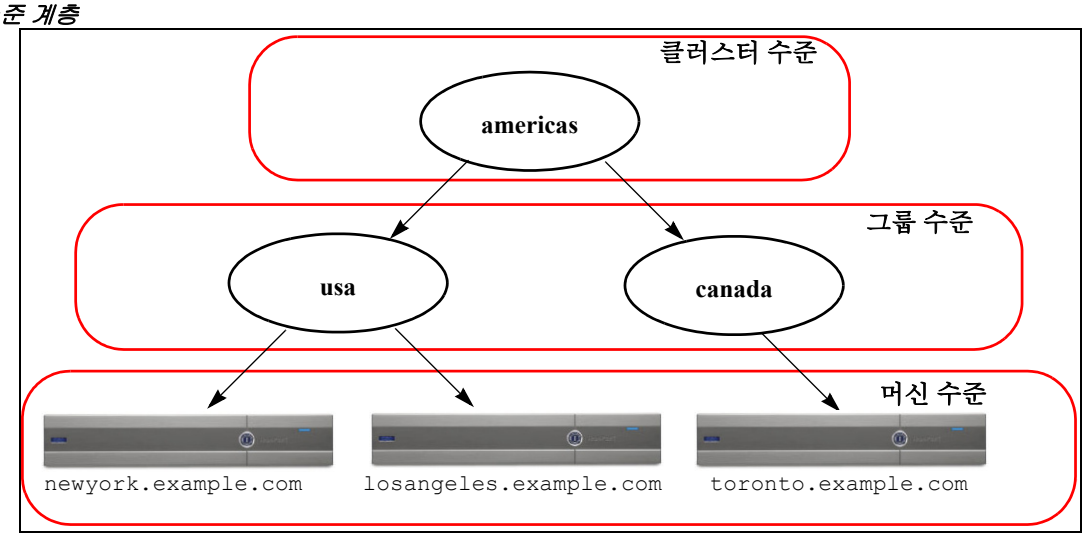
  클러스터를 생성한 경우 GUI에서 또는 CLI에서 비클러스터 구성 설정을 관리할 수 있습니다.

  클러스터 생성 및 클러스트에 조인, 39-4페이지 및 GUI에서 클러스터 관리, 39-15페이지 항목을 참조하십시오.

클러스터 조직

클러스터 내의 구성 정보는 3개의 그룹 또는 *수준*으로 나뉩니다. 최상위 수준에서는 클러스터 설정을 설명하고, 중간 수준에서는 그룹 설정을, 최하위 수준에서는 머신별 설정을 설명합니다.

그림 39-1 클러스터 수준 계층



각 수준에는 하나 이상의 특정 멤버가 있으며 멤버마다 설정을 구성할 수 있습니다. 이를 *모드*라고 합니다. 모드는 지정된 수준에서 명명된 멤버를 가리킵니다. 예를 들어 "usa" 그룹은 다이어그램의 두 그룹 모드 중 하나를 나타냅니다. 수준은 일반적인 용어지만 모드는 특정하며 항상 이름으로 나타냅니다. 그림 39-1에 나와 있는 클러스터에는 6개 모드가 있습니다.

설정은 지정된 수준에서 구성되지만 항상 특정 모드에 **맞게** 구성됩니다. 한 수준의 모든 모드에 대한 설정을 구성할 필요는 없습니다. 클러스터 모드는 특수한 경우입니다. 하나의 클러스터만 존재할 수 있으므로 클러스터 모드에 대해 구성된 모든 설정은 클러스터 수준에서 구성될 수 있습니다.

일반적으로 대부분의 설정은 클러스터 수준에서 구성해야 합니다. 그러나 특별히 하위 수준에서 구성된 설정은 상위 수준에서 구성된 설정을 *재정의*합니다. 따라서 클러스터-모드 설정은 그룹-모드 또는 머신-모드 설정으로 재정의할 수 있습니다.

예를 들어 먼저 클러스터 모드에서 양호한 인접 테이블을 구성하면 클러스터의 모든 머신은 해당 구성을 사용합니다. 그런 다음 머신 모드에서 `newyork` 머신에 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 머신에 대한 클러스터 설정을 재정의하는 기능은 높은 유연성을 제공합니다. 그러나 사용자가 머신 모드에서 많은 설정을 개별적으로 직접 구성하는 경우 클러스터가 제공하는 관리 편의성을 대부분 상실하게 됩니다.

초기 구성 설정

대부분의 기능에 대해 새 모드의 설정을 구성할 경우 그러한 설정은 초기에는 기본적으로 비어 있습니다. 모드에서 빈 설정과 설정이 없는 것에는 차이가 있습니다. 하나의 그룹과 하나의 머신으로 구성된 간단한 클러스터를 예로 들어보겠습니다. 클러스터 수준에서 구성된 LDAP 쿼리가 있다고 가정해 봅시다. 그리고 그룹 또는 머신 수준에서 구성된 설정은 없습니다.

`Cluster`	`(ldap queries: a, b, c)`
`Group`	
`Machine`	

이제 그룹에 대한 LDAP 쿼리 설정을 새로 생성한다고 가정해 봅시다. 결과는 다음과 같을 수 있습니다.

Cluster	(ldap queries: a, b, c)
Group	(ldap queries: None)
Machine	

그룹 수준 설정은 클러스터 수준 설정을 재정의하지만 새 그룹 설정은 초기에는 비어 있습니다. 그룹 모드에는 사실상 자체적으로 LDAP 쿼리가 구성되어 있지 않습니다. 이 그룹 내의 머신은 그룹에서 이와 같이 "비어 있는" LDAP 쿼리 집합을 상속받습니다.

다음으로 LDAP 쿼리를 그룹에 추가할 수 있습니다. 예를 들면 다음과 같습니다.

Cluster	(ldap queries: a, b, c)
Group	(ldap queries: d)
Machine	

클러스터 수준에는 하나의 쿼리 집합이 구성되어 있는 반면, 그룹에는 다른 쿼리 집합이 구성되어 있습니다. 머신은 그룹에서 해당 쿼리를 상속받습니다.

클러스터 생성 및 클러스트에 조인

그래픽 사용자 인터페이스(GUI)에서는 클러스터를 생성하거나 클러스트에 조인할 수 없습니다. 머신 클러스터를 생성, 조인 또는 구성하려면 명령줄 인터페이스(CLI)를 사용해야 합니다. 클러스터를 생성한 경우에는 GUI에서 또는 CLI에서 클러스터 구성 설정을 변경할 수 있습니다.

clusterconfig 명령

머신에서는 `clusterconfig` 명령을 통해서만 클러스터를 생성하거나 클러스트에 조인할 수 있습니다.

- 새 클러스터를 *생성*한 경우 클러스터를 생성한 머신에서 해당 클러스터의 모든 초기 설정을 상속받습니다. 이전에 "독립형" 모드에서 머신을 구성한 경우 클러스터를 생성할 때 독립형 설정이 사용됩니다.
- 머신이 클러스터에 *조인*할 때 해당 머신에서 클러스터로 구성할 수 있는 모든 설정은 클러스터 수준에서 상속됩니다. 즉, 특정 머신별 설정(IP 주소 등)을 제외한 모든 설정은 손실되고 해당 머신이 조인하기 위해 선택한 클러스터 및/또는 그룹의 설정으로 바뀝니다. 이전에 "독립형" 모드에서 머신을 구성한 경우 클러스터를 생성할 때 독립형 설정이 사용되며 머신 수준에서의 설정은 유지되지 않습니다.

현재 머신이 클러스터에 속해 있지 않을 경우 `clusterconfig` 명령을 실행하면 기존 클러스터에 조인하거나 새 클러스터를 생성할 수 있는 옵션이 제공됩니다.

```
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.

[]>
```

이때 머신을 새 클러스터에 추가할 수 있습니다. 이러한 머신은 SSH 또는 CCS를 통해 통신할 수 있습니다.

기존 클러스터에 조인

클러스터에 추가할 호스트에서 clusterconfig 명령을 실행하여 기존 클러스터에 조인합니다. SSH 또는 CCS(클러스터 통신 서비스)를 통해 클러스터에 조인하도록 선택할 수 있습니다.

기존 클러스터에 호스트를 조인시키기 위한 요구 사항은 다음과 같습니다.

- 클러스터에 있는 머신의 SSH 호스트 키를 검증해야 합니다.
- 클러스터에 있는 머신의 IP 주소를 알고 있어야 하며 클러스터 내의 해당 머신에 연결할 수 있어야 합니다(예: SSH 또는 CCS).
- 클러스터 내 머신의 관리자 사용자에 대한 관리자 비밀번호를 알고 있어야 합니다.

SSH를 통해 기존 클러스터에 조인

다음 표에서는 SSH 옵션을 사용하여 머신 losangeles.example.com을 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 password for the cluster.
The administrator password 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 조인

SSH를 사용할 수 없는 경우 대신 CCS를 사용하십시오. CCS의 유일한 이점은 클러스터 통신이 사용자 로그인, SCP 등 없이 포트를 통해서만 발생한다는 것입니다. CCS를 통해 다른 머신을 기존 클러스터에 추가하려면 `clusterconfig`의 하위 명령인 `prepjoin`을 사용하여 머신을 클러스터에 추가합니다. 이 예에서는 `newyork` 머신에서 `prepjoin` 명령을 실행하여 `losangeles` 머신을 클러스터에 추가합니다.

`prepjoin` 명령을 실행하면 클러스터에 추가하고자 하는 호스트의 사용자 키를 획득할 수 있습니다. 이를 위해 CLI에서 `clusterconfig prepjoin print`를 입력한 후 현재 클러스터에 있는 호스트의 명령줄에 해당 키를 복사합니다.

```
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.

[]>
```

머신이 이미 클러스터에 속해 있는 경우 `clusterconfig` 명령을 통해 클러스터에 다양한 설정을 구성할 수 있습니다.

```
(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.

[]>
```

그룹 추가

모든 클러스터에는 하나 이상의 그룹이 포함되어야 합니다. 새 클러스터를 생성하는 경우 Main_Group이라는 기본 그룹이 자동으로 생성됩니다. 그러나 클러스터 내에서 추가 그룹을 생성해야 할 수 있습니다. 이 예에서는 기존 클러스터에 추가 그룹을 생성하고 머신을 새 그룹에 할당하는 방법을 보여줍니다.

절차

1단계 `clusterconfig` 명령을 실행합니다.

2단계 `addgroup` 하위 명령을 선택하고 새 그룹의 이름을 입력합니다.

3단계 `setgroup` 하위 명령을 사용하여 새 그룹에 할당할 머신을 선택합니다.

클러스터 관리

CLI에서 클러스터 관리

클러스터에 속해 있는 머신의 경우 CLI를 다른 *모드*로 전환할 수 있습니다. 모드란 일정 수준에서 명명된 특정 멤버를 나타냅니다.

CLI 모드에 따라 구성 설정이 수정되는 위치가 결정됩니다. 기본값은 사용자가 로그인한 머신의 "머신" 모드, 즉 "로그인 호스트"입니다.

clustermode 명령을 사용하여 모드를 전환합니다.

표 39-1 클러스터 관리

명령 예제	설명
clustermode	클러스터 모드를 전환하기 위한 프롬프트
clustermode group northamerica	"northamerica" 그룹의 그룹 모드로 전환
clustermode machine losangeles.example.com	"losangeles" 머신의 머신 모드로 전환

CLI 프롬프트가 현재 모드를 나타내도록 변경됩니다.

```
(Cluster Americas)>
```

또는

```
(Machine losangeles.example.com)>
```

머신 모드에서 프롬프트에는 머신의 정규화된 도메인 이름이 포함됩니다.

설정 복사 및 이동

제한되지 않은(제한된 명령, 39-14페이지 참조) 모든 명령에는 새로운 작업인 CLUSTERSHOW와 CLUSTERSET가 있습니다. CLUSTERSHOW는 명령이 구성된 모드(새 작업 추가됨, 39-14페이지 참조)를 표시합니다. CLUSTERSET 작업을 사용하면 한 모드에서 다른 모드로, 또는 서로 다른 수준 간에(예: 머신에서 그룹으로) 현재 설정(현재 명령을 사용하여 구성 가능)을 이동하거나 복사할 수 있습니다.

*복사*를 사용하면 현재 모드의 설정이 유지됩니다. *이동*을 사용하면 현재 모드의 구성이 재설정(지우기)됩니다. 즉, 이동 후에는 현재 모드에 대한 설정이 구성되지 않습니다.

예를 들어 northamerica 그룹에 대해 양호한 인접 테이블 설정(destconfig 명령)을 구성한 경우, 전체 클러스터에 이러한 설정을 적용하려면 destconfig 명령에서 clusterset 작업을 실행하여 현재 설정을 클러스터 모드로 복사(또는 이동)할 수 있습니다. (새 구성으로 실험, 39-11페이지 참조.)

주의 구성 설정을 이동하거나 복사하는 경우 일관성 없는 종속성이 발생하지 않도록 주의해야 합니다. 예를 들어 고지 사항 스탬프가 구성되어 있는 리스너를 다른 머신으로 이동하거나 복사하는 경우 새 머신에 동일한 고지 사항이 구성되어 있지 않으면 고지 사항 스탬프는 새 머신에서 활성화되지 않습니다.

새 구성으로 실험

클러스터를 사용하는 방법 중 가장 유용한 방법은 새 구성 설정을 사용하여 실험하는 것입니다. 먼저 분리된 환경에서 머신 모드에서 발생한 변경사항을 적용합니다. 그런 다음 구성이 만족스러운 경우, 해당 구성 변경사항을 클러스터 모드로 이동시키면 모든 머신에서 사용할 수 있습니다.

다음 예에서는 하나의 머신에서 리스너 설정을 변경한 후 준비되면 클러스터의 나머지 부분에 설정을 게시하는 단계를 보여줍니다. 리스너는 클러스터 수준에서 일반적으로 구성되어 있으므로 예제에서는 변경사항을 적용하고 테스트하기에 앞서 해당 구성을 머신 모드로 이동시키는 것으로 시작합니다. 한 머신에서 클러스터의 다른 머신에 변경사항을 적용하기 전에 이러한 유형의 실험적 변경사항을 테스트해야 합니다.

절차

1단계 `clustermode cluster` 명령을 사용하여 클러스터 모드로 변경합니다.

중요: `clustermode` 명령은 클러스터, 그룹 및 머신 수준으로 모드를 변경할 때 사용하는 CLI 명령입니다.

2단계 `listenerconfig`를 입력하여 클러스터에 구성된 리스너 설정을 확인합니다.

3단계 실험하기 위한 머신을 선택한 다음 `clusterset` 명령을 사용하여 클러스터에서 머신 모드로 설정을 복사합니다.

4단계 `clustermode` 명령을 사용하여 실험적 머신의 머신 모드로 이동합니다. 예를 들면 다음과 같습니다.

```
clustermode machine newyork.example.com
```

5단계 실험적 머신의 머신 모드에서 `listenerconfig` 명령을 실행하여 해당 실험적 머신에 맞는 변경사항을 적용합니다.

6단계 변경 사항을 커밋합니다.

7단계 실험적 머신에서 구성 변경사항을 사용하여 실험을 계속하되 변경사항을 커밋해야 합니다.

8단계 새 설정을 다른 모든 머신에 적용할 준비가 되었다면 `clusterset` 명령을 사용하여 해당 설정을 클러스터 모드로 이동시킵니다.

9단계 변경 사항을 커밋합니다.

클러스터에서 영구히 나가기(제거)

`clusterconfig`의 `REMOVEMACHINE` 작업으로 클러스터에서 머신을 영구히 제거합니다. 클러스터에서 머신을 영구히 제거할 경우 해당 구성은 "평면화"되고 클러스터에 속해 있었을 때와 동일하게 동작합니다. 예를 들어 클러스터-모드 전역 구독 취소 테이블만 있는 경우 머신이 클러스터에서 제거되면 전역 구독 취소 테이블 데이터가 머신의 로컬 구성으로 복사됩니다.

클러스터의 머신 업그레이드

클러스터에 연결된 머신들은 같은 AsyncOS 버전을 사용해야 합니다.

AsyncOS 업그레이드를 설치하기 전에 먼저 `clusterconfig` 명령을 사용하여 클러스터에 있는 개별 머신의 연결을 끊어야 합니다. 모든 머신을 업그레이드한 후에는 `clusterconfig` 명령을 사용하여 클러스터를 다시 연결할 수 있습니다. 머신을 동일한 버전으로 업그레이드하는 동안 2개의 개별 클러스터를 실행할 수 있습니다. GUI Upgrades(GUI 업그레이드) 페이지에서 클러스터된 머신을 업그레이드할 수 있습니다.

백그라운드에서 업그레이드를 다운로드할 수 있으므로 업그레이드 설치 준비가 완료될 때까지 클러스터 머신의 연결을 끊을 필요가 없습니다.

참고 클러스터에서 개별 머신의 연결을 끊기 전에 업그레이드 명령을 사용할 경우 AsyncOS는 클러스터의 모든 머신 연결을 끊습니다. 업그레이드하기 전에 클러스터의 개별 머신 연결을 끊는 것이 좋습니다. 그러면 각 머신의 연결이 끊기고 업그레이드될 때까지 다른 머신이 클러스터로 계속 동작할 수 있습니다.

절차

1단계 클러스터의 한 머신에서 `clusterconfig` 명령의 `disconnect` 작업을 실행합니다. 예를 들어 `losangeles.example.com` 머신의 연결을 끊으려면 `clusterconfig disconnect losangeles.example.com`을 입력합니다. `commit`을 사용하지 않아도 됩니다.

2단계 `suspendlistener` 명령을 사용하여 선택적으로 업그레이드 프로세스 중에 새 연결 및 메시지의 수락을 중지합니다.

3단계 `upgrade` 명령을 실행하여 AsyncOS를 신규 버전으로 업그레이드합니다.

참고 클러스터의 모든 머신 연결 끊기에 대한 경고 또는 확인 프롬프트는 무시합니다. 머신의 연결을 끊었으므로 AsyncOS는 현재 클러스터에 있는 다른 머신의 연결을 끊지 않습니다.

4단계 머신의 AsyncOS 버전을 선택합니다. 업그레이드가 완료되면 머신은 재부팅됩니다.

5단계 업그레이드된 머신에서 새 메시지를 수락하도록 `resume` 명령을 실행합니다.

6단계 클러스터의 머신마다 1~5단계를 반복합니다.

참고 클러스터에서 머신 연결이 끊어진 후에는 해당 머신을 사용하여 다른 머신의 구성을 변경할 수 없습니다. 클러스터 구성을 수정할 수는 있지만, 머신 연결이 끊어진 상태에서는 변경하지 마십시오. 이 경우 설정이 동기화되지 않습니다.

7단계 머신을 모두 업그레이드한 후에는 clusterconfig의 reconnect 작업을 실행하여 업그레이드된 각 머신을 다시 연결합니다. 예를 들어 `losangeles.example.com` 머신을 다시 연결하려면 `clusterconfig reconnect losangeles.example.com`을 입력합니다. 동일한 AsyncOS 버전을 실행하는 클러스터에만 머신을 연결할 수 있습니다.

CLI 명령 지원

클러스터를 인식하는 모든 명령

AsyncOS의 모든 CLI 명령은 이제 클러스터를 인식합니다. 클러스터 모드에서 실행할 경우 일부 명령의 동작은 약간 변경됩니다. 예를 들어 클러스터에 속해 있는 머신에서 실행할 경우 다음 명령의 동작은 변경됩니다.

commit 및 clearchanges 명령

commit

commit 명령은 현재 모드에 상관없이 클러스터의 모든 세 가지 수준에서 모든 변경사항을 커밋합니다.

commitdetail

commitdetail 명령은 구성 변경사항이 클러스터 내 모든 머신으로 전파되면 그에 대한 세부사항을 제공합니다.

clearchanges

clearchanges(clear) 명령은 현재 모드에 상관없이 클러스터의 세 가지 수준에서 모두 변경사항을 지웁니다.

새 작업 추가됨

CLUSTERSHOW

이제 각 명령에는 명령이 구성된 모드를 확인할 수 있는 CLUSTERSHOW 작업이 추가되었습니다.

CLI 명령을 사용하여 하위 수준에서 기존 설정으로 재정의되는 작업을 수행하는 경우 알림이 제공됩니다. 예를 들어 클러스터 모드에 있는 경우 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 모드의 설정을 편집하는 경우에도 유사한 메시지가 출력됩니다.

제한된 명령

대부분의 CLI 명령 및 이에 해당하는 GUI 페이지는 모든 모드(클러스터, 그룹 또는 머신)에서 실행될 수 있습니다. 그러나 일부 명령 및 페이지는 한 모드로만 제한됩니다.

시스템 인터페이스(GUI 및 CLI)에서는 명령이 제한되고 명령이 제한되는 방식을 항상 명확하게 표시합니다. 따라서 명령을 구성하기 위한 적절한 모드로 쉽게 전환할 수 있습니다.

- GUI에서 "Change Mode(모드 변경)" 메뉴 또는 "Settings for this features are currently defined at(이 기능에 대한 설정이 현재 다음 위치에서 정의됨):" 링크를 사용하여 모드를 전환합니다.
- CLI에서는 clustermode 명령을 사용하여 모드를 전환합니다.

표 39-2 클러스터 모드로 제한된 명령

clusterconfig	**sshconfig**

표 39-2 클러스터 모드로 제한된 명령

clustercheck	**userconfig**
passwd	

그룹 또는 머신 모드에서 이러한 명령 중 하나를 실행하는 경우 경고 메시지가 표시되며 적절한 모드로 전환할 수 있습니다.

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 사용자는 위에 기록된 동작(다른 제한된 구성 명령과 일치)을 받습니다.

다음 명령은 *머신 모드*로 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 실행하는 경우 경고 메시지가 표시되며 적절한 모드로 전환할 수 있습니다.

다음 명령은 *로그인 호스트*(즉, 사용자가 로그인한 특정 머신)로 추가로 제한됩니다. 이러한 명령을 사용하려면 로컬 파일 시스템에 대한 액세스 권한이 필요합니다.

표 39-3 로그인 호스트 모드로 제한되는 명령

last	resetconfig	tail	upgrade
ping	supportrequest	telnet	who

GUI에서 클러스터 관리

GUI에서는 클러스터를 생성하거나 클러스트에 조인할 수 없으며, 또한 클러스터별 설정을 관리(clusterconfig 명령에 해당)할 수 없지만, 클러스터에서 머신을 찾아 설정을 생성 또는 삭제하거나 클러스터, 그룹 및 머신 간에 복사 또는 이동(즉, clustermode 및 clusterset 명령에 해당하는 명령 실행)할 수는 있습니다.

현재 보고 있는 메일 플로우 모니터링 데이터는 로컬 머신에 저장되기 때문에 Incoming Mail Overview(수신 메일 요약) 페이지는 로그인 호스트로 제한된 명령의 예를 보여줍니다. 다른 머신의 Incoming Mail Overview(수신 메일 요약) 보고서를 보려면 해당 머신의 GUI에 로그인해야 합니다.

어플라이언스에서 클러스터링이 활성화된 경우 브라우저의 주소 필드에 있는 URL을 확인합니다. 이 URL에는 machine, group 또는 cluster라는 단어가 적절하게 포함되어 있습니다. 예를 들어 처음 로그인하는 경우 Incoming Mail Overview(수신 메일 요약) 페이지의 URL은 다음과 같이 표시됩니다.

```
https://hostname/machine/serial_number/monitor/incoming_mail_overview
```

참고 Monitor(모니터) 메뉴의 Incoming Mail Overview(수신 메일 요약) 및 Incoming Mail Details(수신 메일 정보) 페이지는 로그인 머신으로 제한됩니다.

Mail Policies(메일 정책), Security Services(보안 서비스), Network(네트워크) 및 System Administration(시스템 관리) 탭에는 로컬 머신으로 제한되지 않은 페이지를 확인할 수 있습니다. Mail Policies(메일 정책) 탭을 클릭하면 GUI의 중앙 집중식 관리 정보가 변경됩니다.

그림 39-2 GUI의 중앙 집중식 관리 기능: 설정이 정의되지 않음

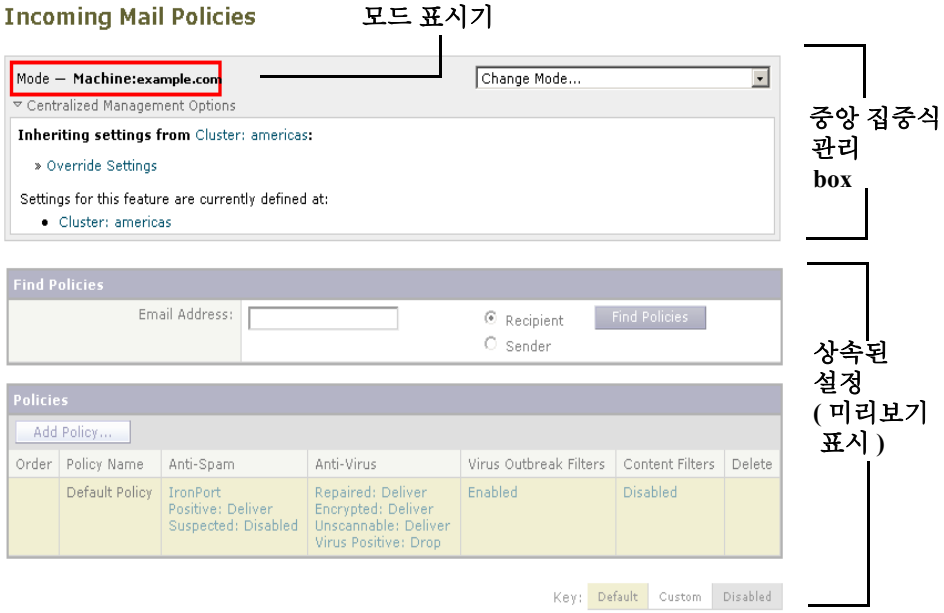


그림 39-2에서 머신은 클러스터 모드로부터 현재 기능의 모든 구성 설정을 상속받습니다. 연한 회색(미리보기)으로 표시된 설정이 상속됩니다. 이러한 설정을 유지하거나 변경하거나, 이 머신의 클러스터 수준 설정을 재정의할 수 있습니다.

참고 상속된 설정(미리보기 표시)에서는 항상 클러스터로부터 상속된 설정을 표시합니다. 그룹 및 클러스터 수준 간에 종속 서비스를 활성화하거나 비활성화할 때는 주의해야 합니다. 자세한 내용은 설정 복사 및 이동, 39-11페이지 항목을 참조하십시오.

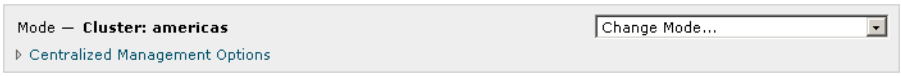
Override Settings(설정 재정의) 링크를 클릭하면 해당 기능의 새 페이지로 연결됩니다. 이 페이지에서는 머신 모드의 새 구성 설정을 생성할 수 있습니다. 기본 설정으로 시작하거나 다른 모드에서 이미 설정을 구성한 경우에는 해당 설정을 이 머신에 복사할 수도 있습니다.

그림 39-3 GUI의 중앙 집중식 관리 기능: 새 설정 생성

또한 그림 39-2에 표시된 것처럼, 이 구성 설정이 이미 정의되어 있는 모드로 이동할 수 있습니다. 이러한 모드는 중앙 집중식 관리 상자 하단의 "Settings for this features are currently defined at(이 기능에 대한 설정이 현재 다음 위치에서 정의됨)" 아래에 나열되어 있습니다. 설정이 실제로 정의되어 있는 모드만 여기에 나열됩니다. 다른 모드에서 정의된(및 상속된) 설정에 해당하는 페이지를 보는 경우 페이지에 자동으로 해당 설정이 표시됩니다.

나열된 모드(예: 그림 39-2에 표시된 클러스터 Americas 링크) 중 하나를 클릭하면 해당 모드의 설정을 보고 관리할 수 있는 새 페이지로 연결됩니다.

그림 39-4 GUI의 중앙 집중식 관리 기능: 설정 정의됨



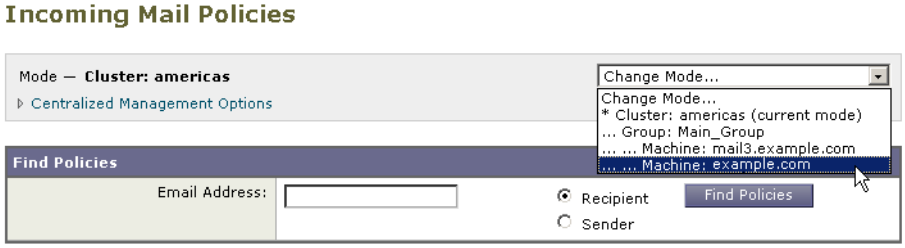
지정된 모드의 설정이 정의된 경우 모든 페이지에서 중앙 집중식 관리 상자가 최소화된 상태로 표시됩니다. "Centralized Management Options(중앙 집중식 관리 옵션)" 링크를 클릭하면 상자가 확장되고 현재 페이지와 관련하여 현재 모드에서 사용 가능한 옵션 목록을 표시됩니다. "Manage Settings(설정 관리)" 버튼을 클릭하면 현재 설정을 다른 모드로 복사 또는 이동시키거나 해당 설정을 완전히 삭제할 수 있습니다.

예를 들어 그림 39-5에서는 Centralized Management Options(중앙 집중식 관리 옵션) 링크를 클릭하여 사용 가능한 옵션이 표시되었습니다.

그림 39-5 GUI의 중앙 집중식 관리 기능: 설정 관리

상자 오른쪽에는 "Change Mode(모드 변경)" 메뉴가 있습니다. 이 메뉴에는 현재 모드가 표시되며 언제든지 다른 모드(클러스터, 그룹 또는 머신)로 이동할 수 있는 기능이 제공됩니다.

그림 39-6 Change Mode(모드 변경) 메뉴



다른 모드를 나타내는 페이지로 이동하는 경우, 중앙 집중식 관리 상자의 왼쪽에 "Mode —" 텍스트가 노란색으로 깜박이고 모드가 변경되었다는 알림이 잠시 나타납니다.

특정 탭의 일부 페이지는 머신 모드로 제한됩니다. 그러나 Incoming Mail Overview(수신 메일 요약) 페이지(현재 로그인 호스트로 제한됨)와는 다르게 이러한 페이지는 클러스터의 모든 머신에서 사용할 수 있습니다.

그림 39-7 중앙 집중식 관리 기능: 머신 제한됨

Change Mode(모드 변경) 메뉴에서 관리할 머신을 선택합니다. 모드를 변경했음을 알리는 텍스트가 잠시 깜박입니다.

클러스터 통신

클러스터 내 머신은 *메시 네트워크*를 사용하여 서로 통신합니다. 기본적으로 모든 머신은 다른 모든 머신과 연결되어 있습니다. 한 링크가 중단되더라도 다른 머신에서 정상적으로 업데이트를 수신할 수 있습니다.

기본적으로 모든 클러스터 내 통신은 SSH로 보호됩니다. 각 머신은 경로 테이블의 메모리 내 복사본을 유지하고 링크가 중단되거나 다시 동작할 경우 필요에 따라 메모리 내 변경사항을 적용합니다. 각 머신은 또한 클러스터의 다른 모든 머신에 주기적으로 "ping"(1분마다)을 수행합니다. 이를 통해 라우터 또는 NAT의 시간이 초과할 경우를 대비하여 최신 링크 상태 및 연결 상태를 유지할 수 있습니다.

참고 클러스터된 두 어플라이언스 간 연결은 어플라이언스 중 하나가 허용되는 최대 SSH 연결 수를 초과하여 연결을 시도할 경우 끊어질 수 있습니다. 어플라이언스는 몇 초 이내에 자동으로 클러스터에 다시 조인하므로 수동 구성이 필요하지 않습니다.

DNS 및 호스트 이름 확인

DNS는 머신을 클러스터에 연결하는 데 필요합니다. 클러스터 통신은 일반적으로 머신의 인터페이스 호스트 이름이 아니라 머신의 DNS 호스트 이름을 사용하여 시작됩니다. 확인할 수 없는 호스트 이름을 가진 머신은 기술적으로 클러스터에 속해 있더라도 사실상 클러스터의 다른 머신과 통신할 수 없습니다.

SSH 또는 CCS를 사용하는 어플라이언스에서 호스트 이름이 올바른 IP 인터페이스를 가리키도록 DNS를 구성해야 합니다. 이는 매우 중요합니다. DNS가 SSH 또는 CCS를 사용하지 않는 다른 IP 주소를 가리킬 경우 호스트를 찾지 못합니다. 중앙 집중식 관리에서는 인터페이스별 호스트 이름이 아니라, `sethostname` 명령을 사용하여 설정된 "기본 호스트 이름"을 사용합니다.

IP 주소를 사용하여 클러스터의 다른 머신에 연결하는 경우 연결된 머신은 연결 IP 주소에 대한 역방향 조회를 수행할 수 있어야 합니다. IP 주소가 DNS에 없어 역방향 조회 시간이 초과할 경우 머신은 클러스터에 연결되지 않습니다.

클러스터링, 정규화된 도메인 이름 및 업그레이드

DNS 변경사항으로 인해 AsyncOS 업그레이드 후 연결이 끊어질 수 있습니다. 클러스터 내 머신의 정규화된 도메인 이름(클러스터 내 머신의 인터페이스 호스트 이름 아님)을 변경해야 할 경우, `sethostname`을 통해 호스트 이름 설정을 변경하고 AsyncOS를 업그레이드하기 *전*에 해당 머신의 DNS 레코드를 업데이트해야 합니다.

클러스터 통신 보안

클러스터 통신 보안(CCS)은 일반적인 SSH 서비스와 비슷한 보안 셸 서비스입니다. Cisco는 클러스터 통신에 일반 SSH를 사용하는 것과 관련된 우려 사항에 대응하여 CCS를 구현했습니다. 두 머신 간의 SSH 통신을 수행할 때는 동일한 포트에서 일반 로그인(관리자 등)을 열어줍니다. 클러스터된 머신에서 일반 로그인을 열고자 하는 관리자는 많지 않습니다.

팁: 클러스터된 일부 머신에 포트 22를 차단하는 방화벽이 있는 경우를 제외하고 클러스터 통신 서비스가 기본값을 사용해도 이 서비스를 활성화하면 안 됩니다. 클러스터링할 때는 모든 머신 간에 SSH 터널(포트 22)의 풀 메시를 사용합니다. 머신에서 CCS 활성화를 묻는 질문에 이미 '예'로 답변한 경우에는 클러스터에서 모든 머신을 제거하고 다시 시작합니다. 클러스터에서 마지막 머신을 제거하면 클러스터가 제거됩니다.

CCS는 관리자가 CLI 로그인이 아닌 클러스터 통신을 열 수 있도록 하는 개선된 기능을 제공합니다. 기본적으로 서비스는 비활성화되어 있습니다. 다른 서비스를 활성화할지 묻는 프롬프트가 표시되면 `interfaceconfig` 명령을 사용하여 CCS를 활성화할지 묻는 메시지가 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]>
```

CCS의 기본 포트 번호는 2222입니다. 원하는 경우 다른 미사용 포트 번호를 열도록 변경할 수 있습니다. 조인이 완료되고 조인하는 머신이 클러스터의 모든 구성 데이터를 가진 경우 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 머신은 클러스터 내 다른 머신과의 네트워크 연결을 지속적으로 확인합니다. 이는 클러스터의 다른 머신으로 주기적으로 전송되는 "ping"을 통해 확인됩니다.

특정 머신과의 모든 통신 시도에 실패할 경우 통신을 시도한 머신에서 원격 호스트 연결이 끊어졌다는 메시지를 기록합니다. 그러면 시스템에서 관리자에게 원격 호스트가 다운되었다는 경고를 보냅니다.

머신이 다운된 경우에도 확인 ping을 계속 받습니다. 머신이 클러스터 네트워크에 다시 조인하면 동기화 명령이 실행되어 이전의 오프라인 머신에서 업데이트를 다운로드할 수 있습니다. 동기화 명령은 변경사항이 한쪽에서만 적용되고 다른 쪽에서는 적용되지 않았는지도 확인합니다. 만일 그렇다면 이전에 다운된 머신에서 자동으로 업데이트를 다운로드합니다.

연결 끊기/다시 연결

클러스트로부터 머신 연결이 끊어질 수 있습니다. 가끔 머신 업그레이드와 같은 이유로 인해 의도적으로 머신 연결을 끊는 경우도 있습니다. 정전 또는 다른 소프트웨어 또는 하드웨어 오류 등과 같은 사고로 인해 연결이 끊어질 수도 있습니다. 또한, 한 어플라이언스에서 세션에서 허용되는 최대 SSH 연결 수를 초과하여 연결을 시도할 경우에도 연결이 끊어질 수 있습니다. 클러스터와의 연결이 끊어진 머신은 바로 액세스하여 구성할 수 있지만, 연결이 끊어진 머신이 다시 연결될 때까지 변경된 사항은 클러스터 내 다른 머신에 전파되지 않습니다.

한 머신이 클러스터에 다시 연결되는 경우 모든 머신에 한꺼번에 다시 연결하려고 시도합니다.

이론상, 클러스트 내의 연결이 끊어진 두 머신은 로컬 데이터베이스의 유사한 변경사항을 동시에 커밋할 수 있습니다. 머신이 클러스터에 다시 연결되면 이러한 변경사항에 대한 동기화를 시도합니다. 충돌이 있는 경우 가장 최근의 변경사항이 기록됩니다(다른 변경사항을 대체).

커밋 과정에서 어플라이언스는 변경되고 있는 모든 변수를 확인합니다. 커밋 데이터에는 비교할 수 있는 버전 정보, 시퀀스 식별 번호 및 기타 정보가 포함됩니다. 변경하려는 데이터가 이전 변경사항과 충돌하는 경우 변경사항을 무시하는 옵션이 제공됩니다. 예를 들어 다음과 같은 메지시가 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]>
```

변경사항을 무시하지 않기로 선택하는 경우 변경사항을 그대로 유지합니다(그러나 커밋되지 않음). 현재 설정을 기준으로 변경사항을 검토하고 어떻게 처리할지 결정할 수 있습니다.

언제든지 `clustercheck` 명령을 사용하여 클러스터가 올바르게 동작하는지 확인할 수도 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 종속적 설정

중앙 집중식 관리 환경에서는 일부 상호 종속적 설정이 서로 다른 모드로 구성됩니다. 구성 모델의 유연성 덕분에 여러 모드에서 설정을 구성할 수 있으며 상속 법칙에 따라 머신별로 사용되는 설정이 결정됩니다. 그러나 일부 설정은 다른 설정에 종속성을 가지며 종속 설정 구성의 가용성은 동일한 모드에서의 설정으로 제한되지 않습니다. 따라서 한 수준에서 다른 수준의 특정 머신용으로 구성된 설정을 참조하는 설정을 구성할 수 있습니다.

상호 종속적 설정의 가장 일반적인 예는 한 페이지에서 다른 클러스터 섹션에서 데이터를 가져오는 필드를 선택하는 것입니다. 예를 들어 서로 다른 모드로 구성할 수 있는 기능은 다음과 같습니다.

- LDAP 쿼리 사용
- 사전 또는 텍스트 리소스 사용
- 바운스 또는 SMTP 인증 프로파일 사용

중앙 집중식 관리에는 제한된 명령 및 제한되지 않은 명령이 있습니다. (제한된 명령, 39-14페이지 참조.) 제한되지 않은 명령은 일반적으로 클러스터 전체에서 공유할 수 있는 구성 명령입니다.

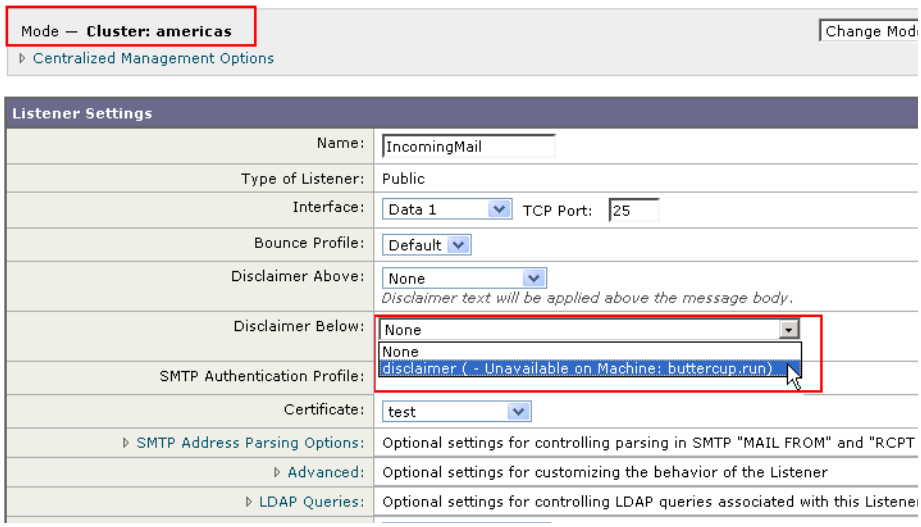
`listenerconfig` 명령은 클러스터의 모든 머신에 대해 구성할 수 있는 대표적인 명령입니다. 제한되지 않은 명령은 클러스터의 모든 머신에 미러링될 수 있으며 머신별 데이터를 수정할 필요가 없는 명령을 나타냅니다.

반면, 제한된 명령은 특정 모드에만 적용되는 명령입니다. 예를 들어 특정 머신에 대한 사용자를 구성할 수 없습니다. 즉, 전체 클러스터에서 하나의 사용자 집합만 존재할 수 있습니다. (그렇지 않으면 동일한 로그인을 사용하여 원격 머신에 로그인할 수 없습니다.) 마찬가지로, Mail Flow Monitor(메일 플로우 모니터) 데이터, System Overview(시스템 개요) 카운터 및 로그 파일은 머신별로 유지되므로 이러한 명령 및 페이지는 머신으로 제한되어야 합니다.

예약 보고서는 전체 클러스터에서 동일하게 구성될 수 있지만 보고서 보기는 머신별로 적용됩니다. 따라서 GUI의 단일 예약 보고서 페이지 내에서의 구성은 클러스터 모드에서 수행되지만 보고서 보기는 머신 모드에서 수행되어야 합니다.

System Time(시스템 시간) 페이지에는 `settz`, `ntpconfig` 및 `settime` 명령이 포함되어 있어 제한된 명령과 제한되지 않은 명령이 혼합되어 있습니다. 이 경우 `settime`은 머신 전용 모드로 제한되어야 하지만(시간 설정은 머신의 고유 정보이므로), `settz` 및 `ntpconfig`는 클러스터 또는 그룹 모드에서 구성할 수 있습니다.

그림 39-8 상호 종속적 설정 예



여기에서 "IncomingMail" 리스너는 머신 수준에서만 구성되는 "고지 사항"이라는 바닥글을 참조합니다. 사용 가능한 바닥글 리소스의 드롭다운 목록에는 바닥글을 "buttercup.run" 머신에서는 사용할 수 없지만 클러스터에서는 사용할 수 있다고 표시됩니다. 이러한 상충 문제에 대한 2가지 해결 방법은 다음과 같습니다.

- "고지 사항" 바닥글을 머신 수준에서 클러스터 수준으로 올립니다.
- 리스너를 머신 수준으로 내려 상호 종속성을 제거합니다.

중앙 집중식 관리 시스템의 기능을 최대한 활용하려면 첫 번째 해결 방법을 사용하는 것이 좋습니다. 클러스터된 머신의 구성을 맞춤식으로 조정하는 경우 설정 간 상호 종속이 발생할 수 있습니다.

클러스터된 어플라이언스에 구성 로드

AsyncOS for Email을 사용하면 클러스터된 어플라이언스에 클러스터 구성을 로드할 수 있습니다. 다음 시나리오의 클러스터 구성을 로드할 수 있습니다.

- 온프레미스 환경에서 호스팅된 환경으로 마이그레이션하고 온프레미스 클러스터 구성을 호스팅된 환경으로 마이그레이션하려는 경우.
- 클러스터의 어플라이언스가 다운되었거나 사용 중지해야 하며 이 어플라이언스에서 클러스터에 추가할 새 어플라이언스로 구성을 로드하려는 경우.
- 클러스터에 어플라이언스를 더 추가하고 클러스터의 기존 어플라이언스 중 하나에서 새로 추가된 어플라이언스로 구성을 로드하려는 경우.
- 백업된 구성을 클러스터로 로드하려는 경우.

사용자 요구 사항에 따라 유효한 클러스터 구성 파일에서 클러스터 구성 또는 어플라이언스 구성을 로드할 수 있습니다.

참고 클러스터된 어플라이언스에서는 독립형 어플라이언스의 구성을 로드할 수 없습니다.

시작하기 전에

- 완전하고 올바른 XML 구성이 있는지 확인합니다. 구성 파일 로드, 33-8페이지 항목을 참조하십시오.
- 구성을 로드하려는 어플라이언스의 현재 구성 백업을 생성합니다. 현재 구성 파일 저장 및 내보내기, 33-8페이지 항목을 참조하십시오.
- 사용자 설치에 적용하려는 모든 어플라이언스에 대한 클러스터 설정을 생성합니다. 클러스터 생성 및 클러스트에 조인, 39-4페이지 항목을 참조하십시오.

참고 한 그룹에 포함된 모든 어플라이언스를 포함시킬 수 있습니다. 사용자 설치의 클러스터 통신용 인터페이스는 이름과 SSH 및 CCS 설정이 XML 구성과 동일해야 합니다.

절차

1단계 **System Administration(시스템 관리) > Configuration File(구성 파일)**을 클릭합니다.

2단계 **Mode(모드)** 드롭다운 메뉴에서 클러스터를 선택합니다.

3단계 클러스터를 로드할지, 어플라이언스 구성을 로드할지에 따라 다음 중 하나를 수행하십시오.

- **클러스터 구성 로드**
  a. Load Configuration(로드 구성) 섹션의 드롭다운 목록에서 **Cluster(클러스터)**를 선택합니다.
  b. 클러스터 구성을 로드하고 **Load(로드)**를 클릭합니다. 구성 파일 로드, 33-8페이지 항목을 참조하십시오.
  c. 로드된 구성의 그룹을 클러스터의 어플라이언스에 할당하고 선택한 그룹의 어플라이언스에서 해당 어플라이언스로 어플라이언스 구성을 복사합니다. **Group Configuration(그룹 구성)** 및 **Appliance Configuration(어플라이언스 구성)** 드롭다운 목록을 사용합니다.

  어플라이언스 구성을 복사하지 않으려면 Appliance Configuration(어플라이언스 구성) 드롭다운 목록에서 **Don't Copy** from the **Appliance Configuration(어플라이언스 구성에서 복사하지 않음)**을 선택합니다.

d. 구성을 검토합니다. **Review(검토)**를 클릭합니다.

e. **Confirm(확인)**을 클릭합니다.

f. **Continue(계속)**를 클릭합니다.

- **어플라이언스 구성 로드**

a. Load Configuration(로드 구성) 섹션의 드롭다운 목록에서 **Appliance in cluster(클러스터의 어플라이언스)**를 선택합니다.

b. 구성을 로드하고 **Load(로드)**를 클릭합니다. 구성 파일 로드, 33-8페이지 항목을 참조하십시오. 독립형 어플라이언스 구성은 클러스터된 어플라이언스에 로드할 수 없습니다.

c. 로드된 구성에서 어플라이언스 구성을 선택하고 클러스터에서 구성을 로드하려는 어플라이언스를 선택합니다. 드롭다운 목록을 사용합니다.

d. **OK(확인)**를 클릭합니다.

e. **Continue(계속)**를 클릭합니다.

f. 어플라이언스 구성을 더 많은 어플라이언스에 로드하려면 a단계부터 e단계까지 반복합니다.

4단계 클러스터된 어플라이언스의 네트워크 설정을 검토하고 변경사항을 커밋합니다.

모범 사례 및 자주 묻는 질문

모범 사례

클러스터를 생성하는 경우 로그인하는 머신이 첫 번째 머신으로 클러스터에 자동으로 추가되며 Main_Group에도 추가됩니다. 머신 수준 설정은 클러스터 수준으로 최대한 많이 효과적으로 이동합니다. 그룹 수준의 설정은 없으며 머신 수준에서 유지되는 유일한 설정은 클러스터 수준에서는 의미가 없는 설정으로 따라서 클러스터될 수 없습니다. 예로는 IP 주소, 기능 키 등이 있습니다.

가능하면 많은 설정을 클러스터 수준으로 유지해야 합니다. 클러스터에서 하나의 머신에만 다른 설정이 필요한 경우 클러스터 설정을 해당 머신의 머신 수준으로 복사합니다. 해당 설정은 이동하면 안 됩니다. 공장 기본값(예: HAT 테이블, SMTPROUTES 테이블, LDAP 서버 프로필 등)이 없는 설정을 이동하는 경우, 클러스터 설정을 상속받는 시스템은 빈 테이블을 가지며 프로세스 이메일을 처리하지 않을 수 있습니다.

머신에서 클러스터 설정을 다시 상속받게 하려면 CM 설정을 관리하고 머신 설정을 삭제합니다. 다음 화면이 표시될 때 머신이 클러스터 설정을 재정의하는지 여부만 파악할 수 있습니다.

```
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 화면이 표시되는 경우:

```
Delete settings from:
    Cluster: xxx
    Machine: yyyy.domain.com
```

복사와 이동 비교

복사하는 경우: 클러스터에 설정을 포함하고 그룹 또는 머신에는 설정을 포함하지 않거나 다른 설정을 포함하고자 할 때

이동하는 경우: 클러스터에 설정을 전혀 포함하지 않지만 그룹 또는 머신에는 설정을 포함하고자 할 때

적절한 CM 설계 사례

LIST로 CM 머신을 나열하는 경우 다음과 같이 표시될 수 있습니다.

```
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)
```

변경사항을 적용하는 수준의 추적 경로를 잃지 않도록 주의하십시오. 예를 들어 Main_Group의 이름(RENAMEGROUP 사용)을 London으로 변경한 경우 다음과 같은 형식이 표시됩니다.

```
cluster = CompanyName
Group London:
    Machine lab1.cable.nu (Serial #: 000F1FF7B3F0-CF2SX51)
    ...
```

그러나 이 구성은 그룹 수준에서 London 시스템을 변경하여 많은 관리자에게 혼동을 주므로 관리자들은 기본 설정의 표준 구성 수준으로 클러스터 수준을 사용하지 않습니다.

팁: 클러스터와 동일한 이름의 그룹(예: London 클러스터, London 그룹)은 사용하지 않는 것이 좋습니다. 그룹 이름에 사이트 이름을 사용하는 경우 위치를 나타내는 클러스터 이름은 사용하지 않는 것이 좋습니다.

올바른 방법은 위에 설명된 것처럼 가능하면 많은 설정을 클러스터 수준으로 유지하는 것입니다. 대부분의 경우 기본 사이트 또는 기본 머신 집합은 Main_Group에서 유지하고 추가 사이트에는 그룹을 사용해야 합니다. 이는 두 사이트가 모두 "동일"한 것으로 간주되는 경우에도 마찬가지입니다. CM에 기본/보조 또는 마스터/슬레이브 서버가 없는 경우 모든 클러스터된 머신은 피어입니다.

팁: 추가 그룹을 사용하는 경우 추가 머신이 클러스터에 조인하기 전에 쉽게 그룹을 준비할 수 있습니다.

클러스터 설정에서 스팸 격리에 액세스하기 위한 모범 사례

로그인한 어플라이언스에서 클러스터에 있는 다른 어플라이언스의 스팸 격리에 액세스하면 로그인한 어플라이언스의 과도한 CPU 사용을 유발할 수 있습니다. 이러한 상황을 방지하기 위해 해당 어플라이언스에 로그인하여 스팸 격리에 액세스할 수 있습니다.

절차: 예제 클러스터 구성

이 예제 클러스터를 구성하려면 clusterconfig를 실행하기 전에 전체 머신의 모든 GUI에서 로그아웃합니다. 기본 사이트 머신 중 한 곳에서 clusterconfig를 실행합니다. 그런 다음 가능한 최대 공유 설정(IP 주소와 같은 머신 전용 설정 허용)이 필요한 다른 로컬 및 원격 머신만 이 클러스터에 조인시킵니다. 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. 동일한 요구 사항을 갖춘 머신은 하나만 있으므로 lab2에 로그인하고 saveconfig를 실행하여 기존 구성(대부분의 lab1 설정을 상속할 때 크게 변경됨)을 저장합니다. 그런 다음 lab2에서 clusterconfig를 사용하여 기존 클러스터에 조인할 수 있습니다. 이 사이트에서 유사한 정책 및 설정이 필요한 추가 머신이 있는 경우 위 단계를 반복합니다.

CONNSTATUS를 실행하고 DNS가 올바르게 확인되는지 검사합니다. 머신이 클러스터에 조인하면서 새 머신은 lab1에서 거의 모든 설정을 상속받고 이전 설정은 손실됩니다. 프로덕션 머신의 경우 메일이 이전 구성이 아니라 새 구성을 사용하여 계속 처리되는지 예측할 수 있어야 합니다. 클러스터에서 구성을 제거할 경우 이전의 개인 구성으로 되돌릴 수 없습니다.

다음으로 예외 머신 수를 계산합니다. 예외 머신이 하나만 있는 경우에는 추가 머신 수준의 몇 가지 설정만 수신하므로 그에 대한 추가 그룹을 생성할 필요가 없습니다. 클러스터에 조인시키고 설정을 머신 수준으로 복사합니다. 이 머신이 기존 프로덕션 머신인 경우 구성을 백업하고 위와 같이 메일 프로세스를 변경할 것을 고려해야 합니다.

머신이 2개 이상인 경우 여기의 예제에서처럼 클러스터 내에서 두 머신이 공유하지 않는 설정을 공유하게 할지 결정합니다. 이 경우 하나 이상의 그룹을 생성합니다. 그렇지 않으면 각 머신에 대해 머신 수준 설정을 적용하게 되므로 추가 그룹이 필요하지 않습니다.

여기에서는 이미 클러스터에 속해 있는 머신의 CLI에서 clusterconfig를 실행하고 ADDGROUP을 선택합니다. 이 과정은 두 번, 즉 Paris와 Rome에 한 번씩 수행합니다.

이제 그룹에 아직 머신이 없는 경우에도 GUI 및 CLI를 사용하여 클러스터 및 모든 그룹에 대해 구성 설정을 생성할 수 있습니다. 머신이 클러스터에 조인한 *이후*에만 머신별 설정을 생성할 수 있습니다.

재정의 또는 예외 설정을 생성하는 가장 효과적인 방법은 설정을 상위(예: 클러스터) 수준에서 하위(예: 그룹) 수준으로 복사하는 것입니다.

예를 들어 클러스터를 생성한 후 처음 dnsconfig 설정은 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 수준의 DNS 설정을 편집할 수 있으며 Paris 그룹의 다른 머신은 해당 설정을 상속합니다. Paris에 속하지 않은 머신은 머신별 설정이 없다면 클러스터 설정을 상속합니다. DNS 설정 외에도, 일반적으로 SMTPROUTES에 대한 그룹 수준 설정을 생성합니다.

팁: 다양한 메뉴에서 CLI CLUSTERSET 기능을 사용하는 경우 특수 옵션을 사용하여 설정을 모든 그룹에 복사합니다. 이 기능은 GUI로는 사용할 수 없습니다.

팁: 전체 리스너는 그룹 또는 클러스터에서 자동으로 상속되며 일반적으로 클러스터의 첫 번째 시스템에서만 해당 리스너를 생성합니다. 이렇게 하여 관리 작업을 크게 줄일 수 있습니다. 그러나 이를 위해서는 *그룹 또는 클러스터 전체에서 인터페이스 이름을 동일하게 지정해야 합니다.*

설정이 그룹 수준에서 올바르게 정의된 경우 머신을 클러스터에 조인시키고 이 그룹에 포함시킵니다. 이 경우 다음 두 단계를 수행해야 합니다.

먼저, 나머지 4개 시스템을 클러스터에 조인시키려면 각 시스템에서 `clusterconfig`를 실행합니다. 클러스터가 크고 복잡할수록 참가 시간이 더 많이 걸립니다. 이 작업은 몇 분 정도 걸릴 수 있습니다. LIST 및 CONNSTATUS 하위 명령을 사용하여 조인 진행 상황을 모니터링할 수 있습니다. 조인이 완료되면 SETGROUP을 사용하여 머신을 Main_Group에서 Paris 및 Rome으로 이동할 수 있습니다. 클러스터에 추가된 모든 머신은 처음에 Paris 및 Rome 설정이 아니라 Main_Group 설정을 상속합니다. 따라서 새 시스템이 이미 프로덕션 환경에 있는 경우에는 메일 흐름 트래픽에 영향을 미칠 수 있습니다.

팁: 랩 머신을 프로덕션 머신과 동일한 클러스터로 포함시키면 안 됩니다. 랩 시스템에 새 클러스터 이름을 사용합니다. 이는 예기치 못한 변경사항(예: 누군가 랩 시스템을 변경하여 실수로 프로덕션 메일이 손실됨)으로부터 추가적인 보호 계층을 제공합니다.

클러스터 기본값 외 다른 CM 설정을 사용하기 위한 GUI 옵션에 대한 요약

설정을 재정의하고 기본 설정으로 시작합니다. 예를 들어 SMTPROUTES 구성의 기본 설정은 빈 테이블이며 이는 처음부터 만들 수 있습니다.

설정을 재정의하되, 클러스터 xxx 또는 그룹 yyy로부터 현재 상속받은 설정 복사본으로 시작합니다. 예를 들어 그룹 수준에서 처음에는 클러스터 테이블과 동일한 SMTPROUTES 테이블 복사본을 새로 작성할 수 있습니다. 동일한 그룹(SETGROUP)에 포함되어 있는 모든 Cisco 어플라이언스는 이 테이블을 가져옵니다. 그룹에 포함되지 않은 머신은 계속 클러스터 수준 설정을 사용합니다. 이 독립적인 테이블 복사본에서 SMTPROUTES를 변경해도 다른 그룹 및 클러스터 설정을 상속하는 머신 또는 개별 머신 수준에서 설정이 정의된 머신에는 영향을 미치지 않습니다. 이것이 가장 일반적인 선택입니다.

Centralized Management Options(중앙 집중식 관리 옵션)의 하위 메뉴에 있는 설정을 관리합니다. 이 메뉴에서 위와 같이 복사할 수 있지만 설정을 이동하거나 삭제할 수도 있습니다. SMTPROUTES를 그룹 또는 머신 수준으로 이동하는 경우 경로 테이블은 클러스터 수준에서는 비어 있지만 더 세부적인 수준에서는 존재합니다.

설정을 관리합니다. SMTPROUTES 예를 계속 살펴보면, 삭제 옵션을 사용해도 클러스터의 SMTPROUTES 테이블이 공백이 됩니다. 이전에 그룹 수준 또는 머신 수준에서 SMTPROUTES에 대한 정의를 구성했다면 아무런 문제가 없습니다. 클러스터 수준 설정을 삭제하고 그룹 또는 머신 설정만 사용하는 것은 권장되지 않습니다. 클러스터 전체 설정은 새로 추가된 머신의 기본값으로 유용하며 이 설정을 유지하면 유지 관리해야 하는 그룹 또는 사이트 설정 수를 하나로 줄일 수 있습니다.

설정 및 구성 질문

Q. 이전에 구성된 독립형 머신이 있고 기존 클러스터에 조인하는 경우, 내 설정은 어떻게 됩니까?

A. 머신이 클러스터에 조인할 때 해당 머신의 클러스터로 구성할 수 있는 모든 설정은 클러스터 수준에서 상속됩니다. 클러스터에 조인하면 로컬로 구성된 비네트워크 설정은 클러스터 및 연결된 그룹의 설정으로 덮어쓰기 되어 모두 손실됩니다. (여기에는 사용자/비밀번호 테이블이 포함됩니다. 비밀번호 및 사용자는 클러스터에서 공유됩니다.)

Q. 클러스터된 머신이 있는 경우 이를 클러스터에서 영구히 제거하면 내 설정은 어떻게 됩니까?

A. 머신을 클러스터에서 영구히 제거하면 해당 구성 계층은 "평면화"되고 머신은 클러스터에 속해 있었을 때와 동일하게 동작합니다. 머신이 상속하는 모든 설정은 독립형 설정의 머신에 적용됩니다.

예를 들어 클러스터-모드 전역 구독 취소 테이블만 있는 경우 머신이 클러스터에서 제거되면 전역 구독 취소 테이블 데이터가 머신의 로컬 구성으로 복사됩니다.

일반 질문

Q. 로그 파일은 중앙에서 관리되는 머신에 취합됩니까?

A. 로그 파일은 계속 개별 머신별로 유지됩니다. Security Management 어플라이언스는 추적 및 보고를 위해 여러 머신에서 메일 로그를 취합하는 데 사용할 수 있습니다.

Q. 사용자 액세스는 어떤 식으로 동작합니까?

A. Cisco 어플라이언스는 전체 클러스터에서 하나의 데이터베이스를 공유합니다. 특히 전체 클러스터에는 관리자 계정(및 비밀번호)만 있습니다.

Q. 데이터 센터를 클러스터링하려면 어떻게 해야 합니까?

A. 데이터 센터는 클러스터 자체로 만들기보다 클러스터 내 "그룹"으로 만드는 것이 좋습니다. 그러나 데이터 센터가 공유하는 부분이 많지 않다면 데이터 센터마다 별도의 클러스터를 사용하면 더 좋은 결과를 얻을 수 있습니다.

Q. 시스템이 오프라인이 되었다가 다시 연결되면 어떻게 됩니까?

A. 시스템이 클러스터에 다시 연결되면 동기화를 시도합니다.

네트워크 질문

Q. 중앙 집중식 관리 기능은 "P2P(peer-to-peer)" 아키텍처 또는 "마스터/슬레이브" 아키텍처 중 어떤 것에 해당합니까?

A. 각 머신은 모든 머신의 전체 데이터(사용하지 않는 모든 머신별 설정 포함)를 가지므로 중앙 집중식 관리 기능은 P2P(peer-to-peer) 아키텍처로 간주될 수 있습니다.

Q. 머신을 설정할 때 피어가 아닌 "슬레이브" 시스템으로 설정하려면 어떻게 해야 합니까?

A. 이 아키텍처에서는 진정한 "슬레이브" 머신을 생성하는 것이 불가능합니다. 그러나 머신 수준에서 HTTP(GUI) 및 SSH/텔넷(CLI) 액세스를 비활성화할 수는 있습니다. 이 방식에서 GUI에서 또는 CLI 액세스 권한이 없는 머신은 clusterconfig 명령을 통해서 *만* 구성할 수 있습니다(즉, 로그인 호스트가 될 수 없음). 이는 슬레이브를 갖는 것과 유사하지만, 로그인 액세스를 다시 설정하면 구성을 해지할 수 있습니다.

Q. 여러 개로 분할된 클러스터를 생성할 수 있습니까?

A. 분리된 클러스터 "그룹"을 만들 수 있습니다. 실제로 분리된 클러스터를 생성하면 성능상의 이유로 도움이 되는 경우가 있습니다.

Q. 클러스터된 어플라이언스 중 하나에 IP 주소 및 호스트 이름을 다시 구성하고자 합니다. 이를 수행하는 경우 재부팅 명령을 실행하기에 앞서 GUI/CLI 세션이 손실됩니까?

다음 단계를 수행합니다.

a. 새 IP 주소를 추가합니다.
b. 리스너를 새 주소로 이동합니다.
c. 클러스터를 벗어납니다.
d. 호스트 이름 변경을 변경합니다.
e. 한 머신에서 볼 때 oldmachinename이 `clusterconfig` 연결 목록에 표시되지 않는지 확인합니다.
f. 모든 GUI 세션이 로그아웃되었는지 확인합니다.
g. CCS가 인터페이스에서 활성화되지 않았는지 확인합니다(`interfaceconfig` 또는 Network(네트워크) > Listeners(리스너) 통해 확인).
h. 머신을 다시 클러스터에 추가합니다.

Q. 대상 제어 기능을 클러스터 수준에서 적용할 수 있습니까? 아니면 로컬 머신 수준에서만 적용할 수 있습니까?

클러스터 수준에서 설정할 수 있지만 머신별로 제한이 적용됩니다. 50개 연결로 제한하는 경우 클러스터의 각 머신에 해당 제한이 설정됩니다.

계획 및 구성

Q. 클러스터를 설정할 때 효율성을 극대화하고 문제를 최소화하려면 어떻게 해야 합니까?

1. 초기 계획
   - 클러스터 수준에서 가능한 한 많은 설정을 구성합니다.
   - 예외인 경우에만 머신별로 관리합니다.
   - 예를 들어 데이터 센터가 여러 개인 경우 그룹을 사용하여 클러스터 전체 특성도, 머신별 특성도 아닌 특성을 공유합니다.
   - 각 어플라이언스에서 인터페이스와 리스너에 동일한 이름을 사용합니다.
2. 제한된 명령에 유의해야 합니다.
3. 설정 간 상호 종속성에 주의해야 합니다.

   예를 들어 `listenerconfig` 명령(클러스터 수준에서도)은 머신 수준에서만 존재하는 인터페이스에 따라 다릅니다. 클러스터 내 모든 머신의 머신 수준에 인터페이스가 없는 경우 해당 리스너는 비활성화됩니다.

   인터페이스를 삭제해도 `listenerconfig`에 영향을 미치게 됩니다.
4. 설정에 주의해야 합니다.

   클러스터에 조인하면 이전에 구성한 머신의 독립 설정이 손실됩니다. 이전에 구성한 설정 중 일부를 머신 수준에서 다시 적용하려면 클러스터에 조인하기 전에 모든 설정을 기록해 두십시오.

   "연결이 끊긴" 머신은 여전히 클러스터에 남아 있습니다. 다시 연결되면 오프라인일 때 변경한 모든 사항은 클러스터의 나머지 부분과 동기화됩니다.

머신을 클러스터에서 영구히 제거하더라도 해당 클러스터에 속해있으면서 가졌던 모든 설정이 유지됩니다. 그러나 클러스터에 다시 조인할 경우 머신의 모든 독립형 설정은 손실됩니다.

`saveconfig` 명령을 사용하여 설정 레코드를 유지합니다.

40 장

테스트 및 문제 해결

참고 이 섹션에 설명된 여러 기능 또는 명령이 영향을 미치거나 라우팅 우선순위의 영향을 받습니다. 자세한 내용은 네트워크 및 IP 주소 할당을 참조하십시오.

테스트 메시지를 사용한 메일 흐름 디버깅: 추적

System Administration(시스템 관리) > Trace(추적) 페이지(CLI에서 `trace` 명령을 사용해도 됨)를 사용하여 테스트 메시지 전송을 에뮬레이션해 시스템의 메시지 흐름을 디버깅합니다. 추적 페이지(및 `trace` CLI 명령)는 리스너가 수락할 때 메시지를 에뮬레이션하고 시스템의 현재 구성에 의해 "트리거"되었거나 영향을 받은 기능의 요약(*커밋되지 않은 변경 사항 포함*)을 출력합니다. 테스트 메시지는 실제로 전송되지 않습니다. 추적 페이지(및 `trace` CLI 명령)는 특히 Cisco 어플라이언스에서 제공되는 여러 고급 기능을 결합한 경우 강력한 문제 해결 또는 디버깅 툴이 될 수 있습니다.

참고 추적은 파일 평판 검사 테스트에 효과적이지 않습니다.

추적 페이지(및 trace CLI 명령)에 표 40-1에 나열된 입력 매개변수를 입력하라는 메시지가 표시됩니다.

표 40-1 추적 페이지의 입력

값	설명	예
소스 IP 주소	원격 도메인의 소스를 모방하는 원격 클라이언트의 IP 주소를 입력합니다. 이 IP 주소는 IPv4(인터넷 프로토콜 버전 4) 또는 IPv6(인터넷 프로토콜 버전 6) 주소일 수 있습니다. **참고:** trace 명령을 실행하면 IP 주소와 정규화된 도메인 이름을 입력하라는 메시지가 표시됩니다. IP 주소가 정규화된 도메인 이름과 일치할 경우 IP 주소 되돌리기를 시도하지 *않습니다*. trace 명령을 사용할 경우 정규화된 도메인 이름 필드를 비워 둬서는 안 되므로 DNS가 일치하는 이름을 올바르게 되돌리는 시나리오를 테스트할 수 없습니다.	**203.45.98.109** **2001:0db8:85a3::8a2e:0370:7334**
소스 IP의 정규화된 도메인 이름	모방할 정규화된 원격 도메인 이름을 입력합니다. Null로 남겨 둘 경우 소스 IP 주소에 대해 역방향 DNS 조회가 수행됩니다.	**smtp.example.com**
동작을 추적할 리스너:	시스템에 구성된 리스너 목록에서 수신 리스너를 선택해 테스트 메시지 전송을 에뮬레이션합니다.	**InboundMail**
SenderBase 네트워크 소유자 조직 ID	SenderBase 네트워크 소유자의 고유한 식별 번호를 입력하거나 시스템이 소스 IP 주소와 관련된 네트워크 소유자 ID를 조회하도록 허용합니다. GUI를 통해 네트워크 소유자를 발신자 그룹에 추가한 경우 이 정보를 볼 수 있습니다.	**34**
SBRS(SenderBase Reputation 점수)	스푸핑된 도메인에 지정할 SBRS 점수를 입력하거나 시스템이 소스 IP 주소와 관련된 SBRS 점수를 조회하도록 허용합니다. 이는 SBRS 점수를 사용하는 정책을 테스트 할 때 유용할 수 있습니다. 수동으로 입력한 SBRS 점수는 CASE(컨텍스트 적응형 검사 엔진)로 전달됩니다. 자세한 내용은 리스너의 발신자 평판 필터링 점수 임계값 편집, 6-5페이지를 참조하십시오.	**-7.5**
봉투 발신자	테스트 메시지의 봉투 발신자를 입력합니다.	**admin@example.net**
봉투 수신자	테스트 메시지의 수신자 목록을 입력합니다. 쉼표로 여러 항목을 구분합니다.	**joe** **frank@example.com**
메시지 본문	헤더를 포함해 테스트 메시지의 메시지 본문을 입력합니다. 별도의 행에 마침표를 입력해 메시지 본문 입력을 마칩니다. "헤더"는 메시지 본문의 일부로 간주되므로(빈 행으로 구분) 헤더를 생략하거나 형식이 잘못 지정된 헤더를 포함하면 예기치 않은 추적 결과를 초래할 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 구성된 기능 중 메시지에 영향을 미치는 모든 기능의 요약이 출력됩니다.

로컬 파일 시스템에서 메시지 본문을 업로드할 수 있습니다. (CLI에서 `/configuration` 디렉토리에 업로드한 메시지 본문을 테스트할 수 있습니다. FTP, SSH, SCP 및 텔넷 액세스에서 가져올 파일을 Cisco 어플라이언스에 배치하는 방법에 대한 자세한 내용을 확인할 수 있습니다.)

요약이 출력된 후 결과 메시지를 보고 테스트 메시지를 다시 실행하라는 메시지가 표시됩니다. 다른 테스트 메시지를 입력하면 추적 페이지와 `trace` 명령이 표 40-1에서 사용자가 입력한 이전 값을 사용합니다.

참고 `trace` 명령을 사용하여 테스트한 구성의 섹션(표 40-2에 있음)이 *순서대로* 수행됩니다. 이는 기능의 구성이 다른 기능에 어떤 영향을 미치는지 이해하는 데 매우 유용합니다. 예를 들어, 도메인 맵 기능으로 변환된 수신자 주소는 RAT에 의해 평가되므로 주소에 영향을 미칩니다. RAT의 영향을 받는 수신자는 별칭 테이블 등에 의해 평가되므로 주소에 영향을 미칩니다.

표 40-2 추적 수행 시 출력 보기

trace 명령 섹션	산출물
HAT(Host Access Table)와 메일 흐름 정책 처리	사용자가 지정한 리스너의 Host Access Table이 처리됩니다. 시스템이 사용자가 입력한 원격 IP 주소와 원격 도메인 이름에서 일치한 HAT의 항목을 보고합니다. 기본 메일 흐름 정책 및 발신자 그룹과 지정된 입력과 일치하는 항목을 볼 수 있습니다. Cisco 어플라이언스가 연결을 거부(REJECT 또는 TCPREFUSE 액세스 규칙을 통해)하도록 구성된 경우 `trace` 명령이 처리 시 해당 시점에서 종료됩니다. HAT 매개변수 설정에 대한 자세한 내용은 사전 정의 발신자 그룹 및 메일 흐름 정책 이해, 7-11페이지를 참조하십시오.
봉투 발신자 주소 처리	
이러한 섹션에는 어플라이언스 구성이 사용자가 입력한 봉투 발신자에게 미치는 영향이 요약되어 있습니다. (다시 말해서, 어플라이언스의 구성에서 MAIL FROM 명령을 어떻게 해석하는지에 대한 요약이 나와 있습니다.) `trace` 명령이 이 섹션 앞에 `"Processing MAIL FROM:"`을 출력합니다.	
기본 도메인	리스너가 수신하는 메시지의 기본 발신자 도메인을 변경하도록 지정한 경우 봉투 발신자에 대한 변경 사항이 이 섹션에 출력됩니다. 자세한 내용은 이메일을 수신하도록 게이트웨이 구성을 참고하십시오.
마스커레이드	메시지의 봉투 발신자가 변환되도록 지정한 경우 변경 사항이 여기에 표시됩니다. `listenerconfig -> edit -> masquerade -> config` 하위 명령을 사용하여 사설 리스너에서 봉투 발신자에 대해 마스커레이드를 활성화합니다. 자세한 내용은 라우팅 및 전달 기능 구성을 참고하십시오.
봉투 수신인 처리	
이러한 섹션에는 어플라이언스가 사용자가 입력한 봉투 수신자에게 미치는 영향이 요약되어 있습니다. (다시 말해서, 어플라이언스의 구성에서 MAIL RCPT TO 명령을 어떻게 해석하는지에 대한 요약이 나와 있습니다.) `trace` 명령이 이 섹션 앞에 `"Processing Recipient List:"`를 출력합니다.	

표 40-2 추적 수행 시 출력 보기 (계속)

trace 명령 섹션	산출물
기본 도메인	리스너가 수신하는 메시지의 기본 발신자 도메인을 변경하도록 지정한 경우 봉투 수신자에 대한 변경 사항이 이 섹션에 출력됩니다. 자세한 내용은 이메일을 수신하도록 게이트웨이 구성을 참고하십시오.
도메인 맵 변환	도메인 맵 기능이 수신자 주소를 대체 주소로 변환합니다. 도메인 맵 변경 사항을 지정하고 지정한 수신자 주소가 일치하면 변환이 이 섹션에 출력됩니다. 자세한 내용은 라우팅 및 전달 기능 구성을 참고하십시오.
RAT(Recipient Access Table)	정책 및 매개변수 외에도 RAT의 항목과 일치하는 각 봉투 수신자가 이 섹션에 출력됩니다. (예를 들어, 수신자가 리스너의 RAT의 제한을 우회하도록 지정된 경우) 수락할 수신자 지정에 대한 자세한 내용은 이메일을 수신하도록 게이트웨이 구성을 참조하십시오.
별칭 테이블	어플라이언스에 구성된 별칭 테이블의 항목과 일치하는 각 봉투 수신자(및 하나 이상의 주신자 주소로의 후속 변환)가 이 섹션에 출력됩니다. 자세한 내용은 라우팅 및 전달 기능 구성을 참고하십시오.
큐 대기 전 메시지 작업	
이러한 섹션에는 메시지 내용이 수신된 후, 그러나 메시지가 작업 큐에서 대기하기 전에 어플라이언스가 각 메시지에 미치는 영향이 요약되어 있습니다. 이 처리는 마지막 `250 ok` 명령이 원격 MTA로 반환되기 전에 발생합니다. `trace` 명령은 이 섹션 앞에 "Message Processing:"을 출력합니다.	
가상 게이트웨이	`altsrchost` 명령은 봉투 발신자의 전체 주소, 도메인, 이름 또는 IP 주소의 일치를 기반으로 메시지를 특정 인터페이스에 할당합니다. 봉투 발신자가 `altsrchost` 명령의 항목과 일치할 경우 해당 정보가 이 섹션에 출력됩니다. 이 시점에 지정된 가상 게이트웨이 주소가 아래의 메시지 필터에 의해 재정의될 수 있습니다. 자세한 내용은 라우팅 및 전달 기능 구성을 참고하십시오.
바운스 프로필	바운스 프로필은 처리 시 3개의 시점에서 적용됩니다. 이는 첫 번째 발생입니다. 리스너에 바운스 프로필이 할당된 경우 프로세스의 이 시점에서 할당됩니다. 해당 정보가 이 섹션에 출력됩니다. 자세한 내용은 라우팅 및 전달 기능 구성을 참고하십시오.

표 40-2 추적 수행 시 출력 보기 (계속)

trace 명령 섹션	산출물
작업 큐 작업	
다음 기능 그룹은 작업 큐의 메시지에 대해 수행됩니다. 이는 클라이언트에서 메시지를 수락한 후, 그러나 메시지가 대상 큐로 전송되기 위해 대기하기 전에 발생합니다. "작업 큐의 메시지"는 `status` 및 `status detail` 명령을 통해 보고됩니다.	
마스커레이드	메시지의 To:, From:, CC: 헤더가 리스너에서 또는 LDAP 쿼리를 통해 입력된 정적 테이블에서 마스크 처리되도록 지정한 경우 변경 사항이 여기에 표시됩니다. `listenerconfig -> edit -> masquerade -> config` 하위 명령을 사용하여 사설 리스너에서 메시지 헤더에 대해 마스커레이드를 활성화할 수 있습니다. 자세한 내용은 라우팅 및 전달 기능 구성을 참고하십시오.
LDAP 라우팅	LDAP 쿼리가 리스너에서 활성화된 경우 LDAP 수락, 재라우팅, 마스커레이드, 그룹 쿼리의 결과가 이 섹션에 출력됩니다. 자세한 내용은 LDAP 쿼리를 참고하십시오.
메시지 필터 처리	시스템에서 활성화된 모든 메시지 필터가 이 시점에서 테스트 메시지를 통해 평가됩니다. 각 필터에 대해 규칙이 평가되며 최종 결과가 "true"이면 해당 필터의 각 작업이 순서대로 수행됩니다. 필터에는 다른 필터가 하나의 작업으로 포함될 수 있으며 필터 중첩은 제한이 없습니다. 규칙의 평가 결과가 "false"이고 작업 목록이 `else` 절과 관련된 경우 그러한 작업이 대신 평가됩니다. 순서대로 처리된 메시지 필터의 결과가 이 섹션에 출력됩니다. 메시지 필터를 사용하여 이메일 정책 적용을 참조하십시오.
메일 정책 처리	
메일 정책 처리 섹션에는 안티스팸, 안티바이러스, 신종 바이러스 필터(Outbreak Filter) 기능, 사용자가 입력한 모든 수신자에 대한 경고문 스탬핑이 표시됩니다. 여러 수신자가 Email Security Manager의 여러 정책과 일치할 경우 일치하는 각 정책에 대해 다음 섹션이 반복됩니다. 문자열 "Message Going to"가 어떤 수신자가 어떤 정책과 일치하는지 정의합니다.	
안티스팸	이 섹션에는 안티스팸 검사를 통해 처리되도록 플래그가 지정되지 않은 메시지가 표시됩니다. 메시지가 리스너의 안티스팸 검사를 통해 처리될 경우 메시지가 처리되고 반환된 판정이 출력됩니다. Cisco 어플라이언스가 판정에 따라 메시지를 바운스하거나 삭제하도록 구성된 경우 해당 정보가 출력되고 `trace` 명령 처리가 중지됩니다. 참고: 시스템에서 안티스팸 검사를 사용할 수 없는 경우에는 이 단계를 건너뜁니다. 안티스팸 검사를 사용할 수 있으나 기능 키를 통해 활성화되지 않은 경우 해당 정보도 이 섹션에 출력됩니다. 안티스팸을 참조하십시오.

표 40-2 추적 수행 시 출력 보기 (계속)

trace 명령 섹션	산출물
안티바이러스	이 섹션에는 안티바이러스 검사를 통해 처리되도록 플래그가 지정되지 않은 메시지가 표시됩니다. 메시지가 리스너의 안티바이러스 검사를 통해 처리될 경우 메시지가 처리되고 반환된 판정이 출력됩니다. Cisco 어플라이언스가 감염된 메시지를 "치료"하도록 구성된 경우 해당 정보가 표시됩니다. 판정에 따라 메시지를 바운스하거나 삭제하도록 구성된 경우 해당 정보가 출력되고 `trace` 명령 처리가 중지됩니다. 참고: 시스템에서 안티바이러스 검사를 사용할 수 없는 경우에는 이 단계를 건너뜁니다. 안티바이러스 검사를 사용할 수 있으나 기능 키를 통해 활성화되지 않은 경우 해당 정보도 이 섹션에 출력됩니다. 안티바이러스를 참조하십시오.
필터 처리	시스템에서 활성화된 모든 콘텐츠 필터가 이 시점에서 테스트 메시지를 통해 평가됩니다. 각 필터에 대해 규칙이 평가되며 최종 결과가 "true"이면 해당 필터의 각 작업이 순서대로 수행됩니다. 필터에는 다른 필터가 하나의 작업으로 포함될 수 있으며 필터 중첩은 제한이 없습니다. 순서대로 처리된 콘텐츠 필터의 결과가 이 섹션에 출력됩니다. 콘텐츠 필터를 참조하십시오.
신종 바이러스 필터(Outbreak Filter) 처리	이 섹션에는 신종 바이러스 필터(Outbreak Filter) 기능을 우회하는 첨부 파일이 포함된 메시지가 표시됩니다. 메시지가 수신자의 신종 바이러스 필터(Outbreak Filter)를 통해 처리될 경우 메시지가 처리되고 평가 결과가 표시됩니다. 어플라이언스가 판정에 따라 메시지를 격리, 바운스 또는 삭제하도록 구성된 경우 해당 정보가 출력되고 처리가 중지됩니다. 신종 바이러스 필터(Outbreak Filter)를 참조하십시오.
Footer 스탬프	이 섹션에는 바닥글 텍스트 리소스가 메시지에 추가되었는지 표시됩니다. 텍스트 리소스의 이름이 표시됩니다. 메시지 고지 사항 스탬핑, 21-2페이지를 참조하십시오(텍스트 리소스).

표 40-2 추적 수행 시 출력 보기 (계속)

trace 명령 섹션	산출물
전송 옵션	
다음 섹션에는 메시지가 전송될 때 발생하는 작업이 표시됩니다. `trace` 명령은 이 섹션 앞에 "`Message Enqueued for Delivery`"를 출력합니다.	
도메인 및 사용자당 전역 구독 취소	`trace` 명령에 대한 입력으로 지정한 수신자가 전역 구독 취소 기능에 표시된 수신자, 수신자 도메인 또는 IP 주소와 일치할 경우 구독 취소된 수신자 주소가 이 섹션에 출력됩니다. 라우팅 및 전달 기능 구성을 참조하십시오.
최종 결과	
모든 처리가 출력되면 최종 결과가 표시됩니다. CLI에서 "Would you like to see the resulting message?"라는 질문에 대해 **y**를 선택하면 결과 메시지가 표시됩니다.	

추적 페이지의 GUI 예

그림 40-1 추적 페이지의 입력

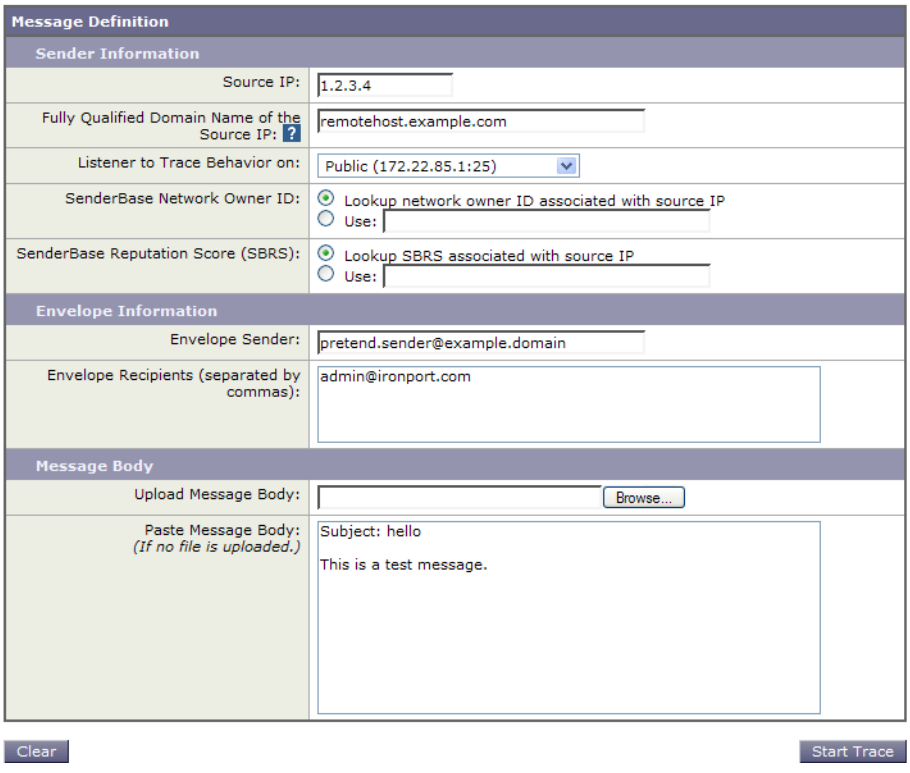


그림 40-2 추적 페이지(1/2페이지)의 출력

Trace

Trace Results			
Host Access Table Processing (Listener: Public)			
Matched On:	ALL Sender Group		
Named Policy:	ACCEPTED		
Connection Behavior:	ACCEPT		
Fully Qualified Domain Name:			
SenderBase Network Owner ID:	N/A		
SenderBase Reputation Score:	N/A		
Policy Parameters:	Max. Messages Per Connection:	1,000	Default
	Max. Recipients Per Message:	1,000	Default
	Max. Message Size:	100M	Default
	Max. Concurrent Connection From a Single IP:	1,000	Default
	Use TLS:	No	Default
	Max. Recipients Per Hour:	1000	
	Use SenderBase:	Yes	
	Use Spam Detection:	Yes	
	Use Virus Detection:	Yes	Default
Envelope Sender Processing			
Envelope Sender: pretend.sender@example.domain			
Default Domain Processing:	No Change		
Envelope Recipient Processing			
Envelope Recipient: admin@ironport.com			
Default Domain Processing:	No Change		
Domain Map Processing:	No Change		
Recipient Access Table Processing:	Behavior: ACCEPT Matched On: admin@ironport.com		
Alias Expansion:	No Change		
Message Processing			
Assigned Virtual Gateway:	None		
Assigned Bounce Profile:	None		

그림 40-3 추적 페이지(2/2페이지)의 출력

Domain Masquerading	
	No changes
Filter Processing	
skipper	Skipped (Inactive)
always_deliver	Rule: rcpt-to == "@mail.qa": False Rule: rcpt-to == "ironport.com": True Rule: OR: True Action: deliver()
Mail Policy Processing: Inbound (matched on policy Public Upgrade)	
Message going to:	admin@ironport.com
Anti-Spam Processing	
Evaluation:	Not Spam
Anti-Virus Processing	
Evaluation:	No Viruses Detected Elapsed Time: 0.000 sec
Actions Taken:	Delivered
VOF Processing	
Evaluation:	No threat detected
Footer Stamping	
Appended Text Resource:	footer
DomainKey Signing	
Result of DomainKeys processing:	DomainKeys signing not enabled in this listener's HAT
Message Delivery (matched on policy Public Upgrade)	
Final Envelope Sender:	pretend.sender@example.domain
Final Recipients:	admin@ironport.com
Final Message:	Received: from remotehost.example.com (HELO TEST) ([1.2.3.4]) by mail3.example.com with TEST; 21 Jul 2005 14:40:05 -0700 Message-Id: <48q06k$@Public> X-Brightmail-Tracker: AAAAAA== X-BrightmailFiltered: true X-IronPort-Anti-Spam-Filtered: true X-IronPort-AV: i="3.95,134,1120460400"; d="scan'"; a="0:sNHT0" Subject: hello Content-Transfer-Encoding: base64 Content-Type: text/plain; charset="utf-8" VGhpcyBpcyBhIHRlc3QgbWVzc2FnZS4KPT09PT09PT09CuODleODg+OCv+ODvOOBp+OBmeOA guOCj+OBhOOCj+OBhOOAggpUaGlzIGlzIGEgSmFwYW5lc2UgZm9vdGVyCj09PT09PT09PQo=

Done

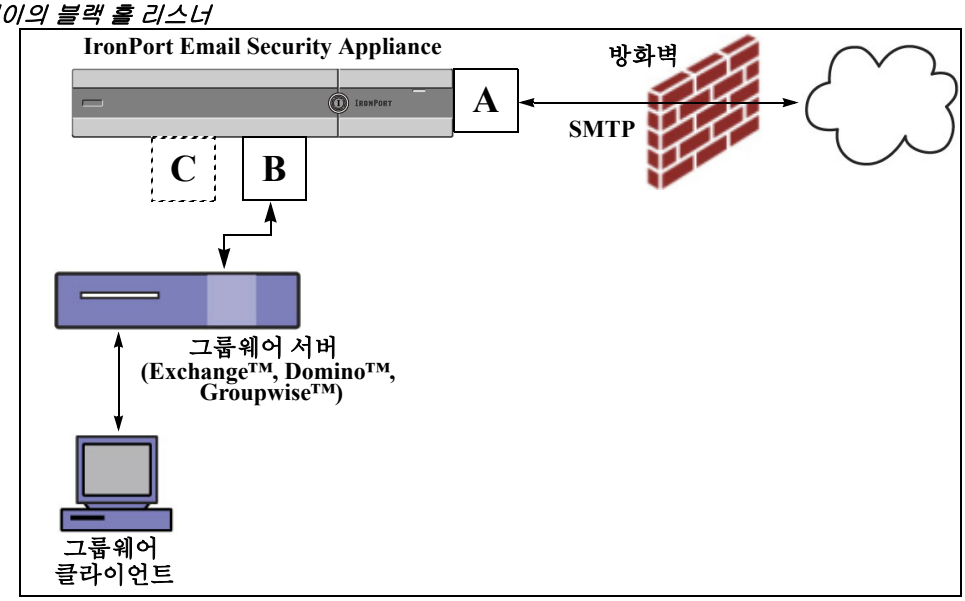
리스너를 사용해 어플라이언스 테스트

"블랙 홀" 리스너를 사용하여 메시지 생성 시스템을 테스트할 뿐 아니라 수신 성능을 대략적으로 측정할 수도 있습니다. 두 가지 유형의 블랙 홀 리스너(*대기* 및 *비 대기*)가 있습니다.

- 대기 리스너는 메시지를 큐에 저장하지만 즉시 삭제합니다. 메시지 생성 시스템의 전체 삽입 부분의 성능을 측정하는 데 관심이 있는 경우 대기 리스너를 사용하십시오.
- 비 대기 리스너는 메시지를 수락한 다음 저장하지 않고 즉시 삭제합니다. 메시지 생성 시스템과 어플라이언스의 연결 문제를 해결하려면 비 대기 리스너를 사용하십시오.

예를 들어, 그림 40-4에서 "B"라는 레이블이 지정된 사설 리스너를 미러링하는 블랙 홀 리스너 "C"를 생성할 수 있습니다. 대기 버전이 그룹웨어 클라이언트에서 그룹웨어 서버 및 어플라이언스에 이르기까지 시스템의 성능을 테스트합니다. 대기 버전이 동일한 경로*와* 어플라이언스가 메시지를 큐에 넣고 SMTP를 통해 전송할 준비를 할 수 있는 능력을 테스트합니다.

그림 40-4 엔터프라이즈 게이트웨이의 블랙 홀 리스너



다음 예제에서는 관리 인터페이스에서 `listenerconfig` 명령을 사용해 `BlackHole_1`이라는 이름의 블랙 홀 대기 리스너를 생성합니다. 그런 다음 다음과 같은 호스트에서 연결을 수락하도록 리스너의 이 HAT(Host Access Table)를 편집합니다.

- `yoursystem.example.com`
- `10.1.2.29`
- `badmail.tst`
- `.tst`

참고 마지막 항목인 `.tst`는 `.tst` 도메인의 모든 호스트가 `BlackHole_1`이라는 이름의 리스너에 이메일을 전송할 수 있도록 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. 사설
2. 공개
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

프로토콜을 선택합니다.
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.

".example.com"과 같은 부분 호스트 네임을 허용합니다.

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


기본 정책 설정

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

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

바이러스 감지 활성화:  예

TLS 연결 허용: 아니요

SMTP 인증 허용: 아니요

SMTP 인증을 위해 TLS 필요: 아니요

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 한다는 점을 기억하십시오.

블랙 홀 대기 리스너를 구성하고 삽입 시스템에서 연결을 수락하도록 HAT를 수정한 후에 삽입 시스템을 사용하여 어플라이언스에 이메일을 전송합니다. `status`, `status detail` 및 `rate` 명령을 사용하여 시스템 성능을 모니터링합니다. GUI(그래픽 사용자 인터페이스)를 통해서도 시스템을 모니터링할 수 있습니다. 자세한 내용은 다음 링크를 참고하십시오.

- CLI를 사용한 모니터링, 34-6페이지
- GUI 기타 작업, 36-7페이지

네트워크 문제 해결

어플라이언스에 네트워크 연결 문제가 있다고 의심될 경우 먼저 어플라이언스가 올바르게 작동하고 있는지 확인하십시오.

어플라이언스의 네트워크 연결 테스트

절차

1단계 시스템에 연결하고 관리자로 로그인합니다. 성공적으로 로그인하면 다음과 같은 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)
```

2단계 status 또는 status detail 명령을 사용합니다.

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

또는

```
mail3.example.com> status detail
```

status 명령은 이메일 작업에 대해 모니터링된 정보의 하위 집합을 반환합니다. 반환된 통계는 2개의 범주(카운터 및 게이지)로 그룹화됩니다. 속도를 포함하여 이메일 작업에 대한 전체 모니터링 정보를 보려면 status detail 명령을 사용합니다. 카운터는 시스템의 다양한 이벤트의 총 실행 합계를 제공합니다. 각 카운터의 경우 카운터가 리셋된 이후와 마지막 시스템 재부팅 이후 그리고 시스템의 수명 동안 발생한 총 이벤트 수를 볼 수 있습니다. (자세한 내용은 CLI를 사용한 모니터링, 34-6페이지를 참조하십시오.)

3단계 mailconfig 명령을 사용하여 알려진 작업 주소로 메일을 전송할 수 있습니다.

mailconfig 명령은 어플라이언스에 사용할 수 있는 모든 구성 설정을 포함하는 사람이 읽을 수 있는 파일을 생성합니다. 어플라이언스에서 알려진 작업 이메일 주소로 파일을 전송하여 어플라이언스가 네트워크를 통해 이메일을 전송할 수 있는지 확인합니다.

```
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 passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig.  [N]> y


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

mail3.example.com>
```

문제 해결

어플라이언스가 네트워크에서 활성화되어 있는지 확인한 후 다음 명령을 사용하여 네트워크 문제를 찾아냅니다.

- `netstat` 명령을 사용하여 다음 정보를 포함한 네트워크 연결(수신 및 발송 모두), 라우팅 테이블, 네트워크 인터페이스 수 통계를 표시할 수 있습니다.
  - 활성 소켓 목록
  - 네트워크 인터페이스의 상태
  - 라우팅 테이블의 목차
  - 대기 큐의 크기
  - 패킷 트래픽 정보
- `diagnostic -> network -> flush` 명령을 사용하여 캐시와 관련된 모든 네트워크를 플러싱할 수 있습니다.
- `diagnostic -> network -> arpshow` 명령을 사용하여 시스템 ARP 캐시를 표시할 수 있습니다.
- `packetcapture` 명령을 사용하여 컴퓨터에 연결된 네트워크를 통해 전송 또는 수신되는 TCP/IP 및 기타 패킷을 가로채서 표시할 수 있습니다.

  `packetcapture`를 사용하려면 네트워크 인터페이스와 필터를 설정합니다. 필터가 UNIX `tcpdump` 명령과 동일한 형식을 사용합니다. `start`를 사용하여 패킷 캡처를 시작하고 `stop`을 사용하여 중단합니다. 캡처를 중단한 후 SCP 또는 FTP를 사용하여 `/pub/captures` 디렉토리에서 파일을 다운로드해야 합니다. 자세한 내용은 패킷 캡처 다시 실행, 40-28페이지를 참고하십시오.
- `ping` 명령을 사용하여 알려진 작동 호스트가 어플라이언스에 네트워크의 활성 연결이 있으며 네트워크의 특정 세그먼트에 도달할 수 있는지 확인하게 할 수 있습니다.

  `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 호스트에 대한 연결을 테스트하고 네트워크 홉의 라우팅 문제를 디버깅할 수 있습니다.

```
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 테스트할 수 있습니다.
- nslookup 명령을 사용하여 DNS 기능을 확인합니다.

  nslookup 명령을 통해 어플라이언스가 DNS(domain name service) 서버 작업에서 호스트 이름과 IP 주소에 도달하고 이를 확인할 수 있는 것을 알 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 40-3 DNS 확인 기능: 쿼리 유형

Query Type	설명
A	호스트의 인터넷 주소
CNAME	별칭(alias)에 대한 정규 이름(canonical name)
MX	메일 수신 장비
NS	해당 zone의 네임 서버
PTR	쿼리가 인터넷 주소인 경우에는 호스트 이름, 그렇지 않은 경우는 기타 정보에 대한 포인터
SOA	도메인의 "start-of-authority" 정보
TXT	텍스트 정보

- CLI 또는 GUI에서 tophosts 명령을 사용하여 활성 수신자별로 정렬할 수 있습니다.

tophosts 명령을 실행하면 큐의 상위 20개의 수신자 호스트 목록이 반환됩니다. 이 명령을 사용하여 네트워크 연결 문제가 사용자가 이메일을 전송하려는 단일 호스트 또는 호스트 그룹으로 격리되는지 확인할 수 있습니다. (자세한 내용은 49페이지의 "메일 큐 구성 결정"을 참조하십시오.)

```
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 결과에서 나열된 상위 도메인의 hoststatus 명령을 사용하여 "드릴다운"합니다.

  hoststatus 명령을 실행하면 특정 수신자 호스트와 관련된 이메일 작업에 대한 모니터링 정보가 반환됩니다. AsyncOS 캐시에 저장된 DNS 정보와 수신 호스트에서 반환된 최신 오류도 제공됩니다. 반환된 데이터가 마지막 resetcounters 명령 후에 누적됩니다. (자세한 내용은 메일 호스트 상태 모니터링, 34-11페이지를 참조하십시오.)

  상위 도메인의 hoststatus 명령을 사용하여 DNS 확인의 성능 문제를 어플라이언스 또는 인터넷으로 격리할 수 있습니다. 예를 들어, 상위 활성 수신 호스트의 hoststatus 명령은 보류 중인 아웃바운드 연결을 표시한 다음 특정 호스트가 다운되었는지 연결할 수 없는지 또는 어플라이언스가 모든 호스트 또는 대다수의 호스트에 연결할 수 없는지 확인할 수 있습니다.

- 방화벽 권한을 확인합니다.

  어플라이언스가 제대로 작동하려면 포트 20, 21, 22, 23, 25, 53, 80, 123, 443 및 628이 모두 열려 있어야 합니다. (*방화벽 정보* 참조)

- 네트워크의 어플라이언스에서 dnscheck@ironport.com으로 이메일을 전송합니다.

  네트워크 내에서 dnscheck@ironport.com으로 이메일을 전송하여 시스템에서 기본 DNS 확인을 수행합니다. 또한 자동 응답 이메일이 다음 4가지 테스트의 결과 및 세부사항에 응답합니다.

  DNS PTR 레코드 - 봉투 보낸 사람의 IP 주소가 도메인의 PTR 레코드와 일치합니까?

  DNS A 레코드 - 도메인의 PTR 레코드가 봉투 보낸 사람의 IP 주소와 일치합니까?

  HELO 일치 - SMTP HELO 명령에 나열된 도메인이 봉투 보낸 사람의 DNS 호스트 이름과 일치합니까?

  지연된 바운스 메시지를 수락하는 메일 서버 - SMTP HELO 명령에 나열된 도메인에 도메인의 IP 주소를 확인하는 MX 레코드가 있습니까?

리스너 문제 해결

이메일 삽입 시 의심스러운 문제가 있는 경우 다음 전략을 사용합니다.

- 이메일을 삽입하는 IP 주소를 확인한 다음 listenerconfig 명령을 사용하여 허용된 호스트인지 확인합니다.

  이 IP 주소를 사용자가 생성한 리스너에 연결할 수 있습니까? listenerconfig 명령을 사용하여 리스너의 HAT(Host Access Table)를 검사합니다. 이러한 명령을 사용하여 리스너의 HAT를 출력할 수 있습니다.

  listenerconfig -> edit -> *listener_number* -> hostaccess -> print

  IP 주소, IP 주소 블록, 호스트 이름 또는 도메인을 통한 연결을 거부하도록 HAT를 구성할 수 있습니다. 자세한 내용은 107페이지의 "연결이 허용되는 호스트 지정"을 참조하십시오.

  또한 limits 하위 명령을 사용하여 리스너에 허용된 최대 연결 수를 확인할 수 있습니다.

  listenerconfig -> edit -> *listener_number* -> limits

- 사용자가 삽입하는 머신에서 텔넷 또는 FTP를 사용하여 어플라이언스에 수동으로 연결할 수 있습니다. 예를 들면 다음과 같습니다.

```
injection_machine% telnet appliance_name
```

  또한 어플라이언스 자체 내에서 telnet 명령을 사용하여 리스너에서 실제 어플라이언스에 연결할 수 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 인터페이스에 연결할 수 없는 경우 어플라이언스의 관리 및 Data1 및 Data2 인터페이스가 네트워크에 연결된 방식에 문제가 있을 수 있습니다. 텔넷을 사용하여 연결을 시도할 경우 대상 인터페이스에서 텔넷 서비스가 활성화되었는지 확인합니다. 자세한 내용은 부록 A, "FTP, SSH, SCP 및 텔넷 액세스"를 참조하십시오. 또한 텔넷을 사용하여 리스너의 포트 25에 연결하고 SMTP 명령을 수동으로 입력할 수 있습니다(해당 프로토콜을 잘 알고 있는 경우).

- IronPort 텍스트 메일 로그 및 삽입 디버그 로그를 검사하여 수신 오류가 있는지 확인합니다.

  삽입 디버그 로그는 어플라이언스와 시스템에 연결하는 지정된 호스트 사이의 SMTP 대화를 기록합니다. 삽입 디버그 로그는 어플라이언스와 인터넷에서 연결을 시작하는 클라이언트 사이의 통신 문제를 해결하려는 경우에 유용합니다. 이 로그는 두 시스템 사이에서 전송된 모든 바이트를 기록하고 이를 연결 호스트로 "전송" 또는 연결 호스트에서 "수신"으로 분류합니다.

  자세한 내용은 텍스트 메일 로그 사용, 38-8페이지 및 수신 디버그 로그 사용, 38-21페이지를 참조하십시오.

어플라이언스에서 이메일 전송 문제 해결

어플라이언스에서 이메일을 전송할 때 의심스러운 문제가 있는 경우 다음 전략을 시도합니다.

- 문제가 도메인과 관련이 있는지 파악합니다.

  `tophosts` 명령을 사용하여 이메일 큐에 대한 정보를 즉시 가져오고 특정 수신 도메인에 전송 문제가 있는지 확인합니다.

  "활성 수신자"별로 정렬할 때 문제 도메인이 반환됩니까?

  연결 중단을 기준으로 정렬할 경우 도메인이 리스너에 지정된 최대 연결에 도달합니까? 리스너의 기본 최대 연결 수는 600입니다. 시스템 전체의 기본 최대 연결 수가 10,000인 경우 (`deliveryconfig` 명령을 사용하여 설정). 다음 명령을 사용하여 리스너의 최대 연결 수를 검사할 수 있습니다.

`listenerconfig` -> `edit` -> *listener_number* -> `limits`

리스너의 연결 수가 `destconfig` 명령을 통해 추가로 제한됩니까(시스템 최대 또는 가상 게이트웨이 주소별)? 이 명령을 사용하여 `destconfig` 연결 제한을 검사합니다.

`destconfig` -> `list`

- `hoststatus` 명령을 사용합니다.

  `tophosts` 명령을 통해 나열된 결과에 표시된 상위 도메인의 `hoststatus` 명령을 사용하여 "드릴다운"합니다.

  호스트를 사용할 수 있으며 연결을 수락합니까?

  지정된 호스트의 특정 MX 레코드 메일 서버에 문제가 있습니까?

  `hoststatus` 명령을 실행하면 지정된 호스트에 5XX 오류(영구 부정적 완료 응답)가 있는 경우 호스트에서 반환한 마지막 "5XX" 상태 코드와 설명이 반환됩니다. 호스트에 대한 마지막 발송 TLS 연결이 실패하면 `hoststatus` 명령이 실패한 이유를 표시합니다.

- 도메인 디버그, 바운스 및 텍스트 메일 로그를 구성 및 검사하여 수신 호스트를 사용할 수 있는지 확인합니다.

  도메인 디버그 로그는 어플라이언스와 지정된 수신 호스트 사이의 SMTP 대화 도중 클라이언트 및 서버 통신을 기록합니다. 이 로그 파일 유형을 사용하여 특정 수신 호스트의 문제를 디버깅할 수 있습니다.

  자세한 내용은 도메인 디버그 로그 사용, 38-20페이지를 참고하십시오.

  바운스 로그는 바운스된 각 수신자에 대한 모든 정보를 기록합니다.

  자세한 내용은 바운스 로그 사용, 38-17페이지를 참고하십시오.

  텍스트 메일 로그는 이메일 수신, 이메일 전송 및 바운스의 세부사항이 포함됩니다. 상태 정보도 1분마다 메일 로그에 작성됩니다. 이러한 로그는 특정 메시지의 전송을 이해하고 시스템 성능을 분석할 수 있는 유용한 정보 소스입니다.

  자세한 내용은 텍스트 메일 로그 사용, 38-8페이지를 참고하십시오.

- `telnet` 명령을 사용하여 어플라이언스에서 문제 도메인에 연결할 수 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]> 1


Enter the remote hostname or IP.

[]> problemdomain.net
```

```
Enter the remote port.

[25]> 25
```

- `tlsverify` 명령을 사용하여 요청 시 아웃바운드 TLS 연결을 구성하고 대상 제어에 대한 TLS 연결 문제를 디버깅할 수 있습니다. 연결을 생성하기 위해, 확인할 도메인과 대상 호스트를 지정합니다. AsyncOS가 필수 (확인) TLS 설정에 따라 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 문제 해결

어플라이언스에 성능 문제가 있는 경우 다음 전략을 활용합니다.

- `rate` 및 `hostrate` 명령을 사용하여 현재 시스템 활동을 확인합니다.

  `rate` 명령은 이메일 작업에 대한 실시간 모니터링 정보를 반환합니다. 자세한 내용은 실시간 활동 표시, 34-16페이지를 참고하십시오.

  `hostrate` 명령은 특정 호스트에 대한 실시간 모니터링 정보를 반환합니다.

- `status` 명령을 사용하여 속도 기록을 교차 참조하여 성능 저하가 있는지 확인합니다.

- `status detail` 명령을 사용하여 RAM 사용률을 확인합니다.

  `status detail` 명령을 사용하여 시스템의 RAM, CPU 및 Disk I/O 사용률을 빠르게 확인할 수 있습니다.

참고 RAM 사용률은 항상 45% 미만이어야 합니다. RAM 사용률이 45%를 초과하면 어플라이언스가 "리소스 대화 모드"로 전환되어 리소스 과도 구독을 방지하는 "백오프" 알고리즘을 시작하고 다음 이메일 경고를 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%.
```

이 상황은 전송 가능성이 낮은 시설에서 공격적인 삽입을 할 경우에만 발생합니다. RAM 사용률이 45%를 초과할 경우 큐의 메시지 수를 확인하고 특정 도메인이 다운되었는지 또는 전송할 수 없는지 확인합니다(`hoststatus` 또는 `hostrate` 명령을 통해). 또한 시스템의 상태를 확인하고 전송이 중단되지 않도록 합니다. 삽입을 중단한 후에도 계속해서 높은 RAM 사용률을 경험하려면 Cisco 고객 지원팀에 문의하십시오. Cisco 고객 지원, 1-8페이지를 참조하십시오.

- 문제가 1개의 도메인과 관련이 있습니까?

  `tophosts` 명령을 사용하여 이메일 큐에 대한 정보를 즉시 가져오고 특정 수신 도메인에 전송 문제가 있는지 확인합니다.

  큐의 크기를 확인합니다. 이메일 큐의 메시지를 삭제, 바운스, 일시 중지 또는 리디렉션하여 크기를 관리하거나 문제가 있는 특정 도메인의 수신자를 처리할 수 있습니다. 자세한 내용은 이메일 큐 관리, 34-22페이지를 참고하십시오. 다음과 같은 명령을 사용합니다.

  - `deleterecipients`
  - `bouncerecipients`
  - `redirectrecipients`
  - `suspenddel` / `resumedel`
  - `suspendlistener` / `resumelistener`

  `tophosts` 명령을 사용하여 소프트 및 하드 바운스의 수를 확인합니다. "소프트 바운스된 이벤트"(옵션 4) 또는 "하드 바운스된 수신자"(옵션 5)를 기준으로 정렬합니다. 특정 도메인의 성능에 문제가 있는 경우 위의 명령을 사용하여 해당 도메인의 전송을 관리합니다.

경고에 응답

경고: C380 또는 C680 하드웨어의 배터리 재충전 시간 초과(RAID 이벤트)

문제 C380 또는 C680 하드웨어를 사용하고 있으며 "배터리 재충전 시간 초과"(RAID 이벤트) 경고를 수신합니다.

솔루션 이 경고는 문제를 나타내거나 그렇지 않을 수 있습니다. 배터리 재충전 시간 초과는 그 자체로 RAID 컨트롤러에 문제가 있음을 의미하지 않습니다. 컨트롤러를 통해 후속 재충전을 복구할 수 있습니다. 다음 48시간 동안 다른 RAID 경고가 있는지 이메일을 모니터링하여 이것이 다른 문제의 부작용이 아님을 확인하십시오. 시스템에서 다른 RAID 관련 경고가 표시되지 않으면 이 경고를 안전하게 무시할 수 있습니다.

기타 디스크 사용량이 할당량에 근접하고 있음을 알리는 경고 문제 해결

문제 기타 디스크 사용량이 할당량에 근접하고 있음을 알리는 경고를 수신합니다.

솔루션 이 경우 할당량을 늘리거나 파일을 삭제할 수 있습니다. 기타 할당량의 디스크 공간 관리, 33-16페이지를 참조하십시오.

원격으로 어플라이언스 전력 리셋

어플라이언스에 하드 리셋이 필요한 경우 타사 IPMI(Intelligent Platform Management Interface) 툴을 사용하여 어플라이언스 섀시를 원격으로 재부팅할 수 있습니다.

제한 사항

- 원격 전력 관리는 특정 하드웨어에서만 사용할 수 있습니다.

  자세한 내용은 원격 전력 관리 활성화, 33-29페이지를 참조하십시오.
- 이 기능을 사용할 수 있으려면 먼저 이 기능을 활성화해야 합니다.

  자세한 내용은 원격 전력 관리 활성화, 33-29페이지를 참조하십시오.
- 다음 IPMI 명령만 지원됩니다.

  `status, on, off, cycle, reset, diag, soft`

  지원되지 않는 명령을 실행하면 "권한 부족" 오류가 발생합니다.

시작하기 전에

- IPMI 버전 2.0을 사용하여 디바이스를 관리할 수 있는 유틸리티를 구매해서 설치합니다.
- 지원되는 IPMI 명령을 사용하는 방법을 이해합니다. IPMI 툴의 설명서를 참조하십시오.

절차

1단계 IPMI를 사용하여 필요한 자격 증명과 함께 초기에 구성된 원격 전력 관리 포트에 할당된 IP 주소에 대해 지원되는 전원 사이클 명령을 실행합니다.

예를 들어, IPMI 지원을 통해 UNIX 유형의 머신에서 다음 명령을 실행할 수 있습니다.

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

여기에서 `192.0.2.1`은 원격 전력 관리 포트에 할당된 IP 주소이고 `remoteresetuser` 및 `password`는 이 기능을 활성화하는 도중 입력한 자격 증명입니다.

2단계 어플라이언스가 재부팅될 때까지 최소한 5분 이상 기다리십시오.

기술 지원 이용

가상 어플라이언스에 대한 기술 지원

가상 어플라이언스에 대한 기술 지원을 받기 위한 요건은 *Cisco Content Security Virtual Appliance 설치 설명서* (http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html)에 설명되어 있습니다.

어플라이언스에서 지원 사례 열기 또는 업데이트

시작하기 전에

- 문제가 긴급한 경우 이 방법을 사용하지 마십시오. 그 대신 Cisco 고객 지원, 1-8페이지에 나열된 다른 방법 중 하나를 사용하여 지원팀에 연락하십시오.

  다음 절차는 정보에 대한 요청 또는 해결책이 있지만 대체 해결책을 찾으려는 문제와 같은 문제에만 사용할 수 있습니다.
- 도움을 받을 수 있는 다른 옵션을 고려하십시오.
  - 기술 자료, 1-8페이지
  - Cisco 지원 커뮤니티, 1-8페이지
- 해당 어플라이언스에서 직접 Cisco 기술 지원에 액세스하려면 Cisco.com 사용자 ID가 해당 어플라이언스의 서비스 협정 계약에 연결되어 있어야 합니다. 현재 Cisco.com 프로필과 연결된 서비스 연락처 목록을 보려면 Cisco.com Profile Manager(https://tools.cisco.com/RPFA/profile/profile_management.do)를 방문하십시오. Cisco.com 사용자 ID가 없는 경우 ID를 등록하십시오. Cisco 계정 등록, 1-9페이지를 참조하십시오.

  Cisco.com 사용자 ID와 지원 연락처 ID를 안전한 곳에 보관하십시오.
- 이 절차를 사용하여 지원 사례를 열 경우 어플라이언스 구성 파일이 Cisco 고객 지원팀에 전송됩니다. 어플라이언스 구성을 전송하지 않으려면 다른 방법을 사용하여 고객 지원팀에 연락할 수 있습니다.
- 클러스터 구성에서 지원 요청과 저장된 값은 머신에만 적용됩니다.

- 어플라이언스가 인터넷에 연결되어 있고 이메일을 전송할 수 있어야 합니다.
- 기존 사례에 대한 정보를 전송할 경우 사례 번호가 있는지 확인합니다.

절차

1단계 어플라이언스에 서명합니다.

2단계 **Help and Support(도움말 및 지원) > Contact Technical Support(기술 지원팀에 문의)**를 선택합니다.

3단계 양식을 작성합니다.

4단계 **Send(보내기)**를 클릭합니다.

참고 CCO 사용자 ID와 마지막에 입력된 연락처 ID가 나중에 사용할 수 있도록 어플라이언스에 저장됩니다.

Cisco 기술 지원 담당자에 대한 원격 액세스 활성화

Cisco 고객 지원팀만 이러한 방법을 사용하여 어플라이언스에 액세스할 수 있습니다.

- 인터넷 연결을 사용하여 어플라이언스에 대한 원격 액세스 활성화, 40-26페이지
- 직접 인터넷 연결 없이 어플라이언스에 대한 원격 액세스 활성화, 40-27페이지
- 기술 지원 터널 비활성화, 40-27페이지
- 원격 액세스 비활성화, 40-28페이지
- 지원 연결의 상태 확인, 40-28페이지

인터넷 연결을 사용하여 어플라이언스에 대한 원격 액세스 활성화

지원팀은 이 절차를 통해 어플라이언스와 `upgrades.ironport.com` 서버 사이에서 생성되는 SSH 터널을 통해 어플라이언스에 액세스합니다.

시작하기 전에

인터넷에서 연결할 수 있는 포트를 식별합니다. 기본 포트는 포트 25입니다. 이메일 메시지를 전송하려면 시스템에 해당 포트를 통한 일반 액세스가 필요하므로 이 포트는 대부분의 환경에서 작동됩니다. 이 포트를 통한 연결은 대부분의 방화벽 구성에서 허용됩니다.

절차

1단계 어플라이언스에 로그인합니다.

2단계 GUI 창의 오른쪽 상단에서 **Help and Support(도움말 및 지원) > Remote Access(원격 액세스)**를 선택합니다.

3단계 **Enable(활성화)**을 클릭합니다.

4단계 정보를 입력합니다.

Option	설명
고객 지원 비밀번호	이 임시 비밀번호와 어플라이언스 일련 번호(물리적 어플라이언스의 경우) 또는 VLN(가상 어플라이언스의 경우)은 지원 액세스의 비밀번호를 생성하는 데 사용됩니다.
보안 터널	원격 액세스 연결에 보안 터널을 사용하려면 해당 확인란을 선택합니다. 연결의 포트를 입력합니다. 기본 포트는 대부분의 환경에서 작동되는 25입니다.

5단계 **Submit**을 클릭합니다.

향후 작업

지원 담당자의 원격 액세스가 더 이상 필요하지 않으면 기술 지원 터널 비활성화, 40-27페이지를 참조하십시오.

직접 인터넷 연결 없이 어플라이언스에 대한 원격 액세스 활성화

직접 인터넷 연결이 없는 어플라이언스의 경우 인터넷에 연결된 두 번째 어플라이언스를 통해 액세스가 이루어집니다.

시작하기 전에

- 어플라이언스가 포트 22를 통해 인터넷에 연결된 두 번째 어플라이언스에 연결할 수 있어야 합니다.
- 인터넷 연결이 있는 어플라이언스에서 인터넷 연결을 사용하여 어플라이언스에 대한 원격 액세스 활성화, 40-26페이지의 절차에 따라 해당 어플라이언스에 대한 지원 터널을 생성합니다.

절차

1단계 지원이 필요한 어플라이언스의 명령줄 인터페이스에서 `techsupport` 명령을 입력합니다.

2단계 `sshaccess`를 입력합니다.

3단계 프롬프트를 따릅니다.

향후 작업

지원 담당자에 대한 원격 액세스가 더 이상 필요하지 않으면 다음을 참조하십시오.

- 원격 액세스 비활성화, 40-28페이지
- 기술 지원 터널 비활성화, 40-27페이지

기술 지원 터널 비활성화

활성화된 기술 지원 터널은 7일 동안 `upgrades.ironport.com`에 연결되어 있습니다. 그 후에는 구성된 연결이 분리되지 않지만 한 번 분리된 후에는 터널에 다시 연결할 수 없습니다.

터널을 수동으로 비활성화하려면 다음을 수행합니다.

절차

1단계 어플라이언스에 로그인합니다.

2단계 GUI 창의 오른쪽 상단에서 **Help and Support(도움말 및 지원) > Remote Access(원격 액세스)**를 선택합니다.

3단계 **Disable(비활성화)**을 클릭합니다.

원격 액세스 비활성화

techsupport 명령을 사용하여 생성하는 원격 액세스 계정은 사용자가 비활성화할 때까지 활성화된 상태로 유지됩니다.

절차

1단계 명령줄 인터페이스에서 techsupport 명령을 입력합니다.

2단계 sshaccess를 입력합니다.

3단계 disable을 입력합니다.

지원 연결의 상태 확인

절차

1단계 명령줄 인터페이스에서 techsupport 명령을 입력합니다.

2단계 status를 입력합니다.

패킷 캡처 다시 실행

패킷 캡처를 통해 지원 담당자가 TCP/IP 데이터와 어플라이언스에서 들어오고 나가는 기타 패킷을 볼 수 있습니다. 따라서 지원 담당자가 네트워크 설정을 디버깅하고 어플라이언스에 도달하거나 어플라이언스에서 나가는 네트워크 트래픽을 찾을 수 있습니다.

절차

1단계 **Help and Support(도움말 및 지원) > Packet Capture(패킷 캡처)**를 선택합니다.

2단계 패킷 캡처 설정을 지정합니다.

a. **패킷 캡처 설정** 섹션에서 **Edit Settings(설정 편집)**를 클릭합니다.

b. (선택 사항) 패킷 캡처의 기간, 제한 및 필터를 입력합니다.

지원 담당자가 이러한 설정에 대한 지침을 제공할 수 있습니다.

시간 단위를 지정하지 않고 캡처 기간을 입력하면 AsyncOS가 기본적으로 초 단위를 사용합니다.

필터 섹션에서 다음 작업이 수행됩니다.

- 사용자 지정 필터는 UNIX `tcpdump` 명령에서 지원하는 모든 구문을 사용할 수 있습니다 (`host 10.10.10.10 && port 80` 등).
- 클라이언트 IP는 어플라이언스에 연결되는 머신(Email Security 어플라이언스를 통해 메시지를 전송하는 메일 클라이언트 등)의 IP 주소입니다.
- 서버 IP는 어플라이언스가 연결되는 머신(어플라이언스가 메시지를 전송하는 교환 서버 등)의 IP 주소입니다.

  클라이언트 및 서버 IP 주소를 사용하여 특정 클라이언트와 특정 서버 사이의 트래픽(중간에 Email Security 어플라이언스가 있음)을 추적할 수 있습니다.

c. **Submit**을 클릭합니다.

3단계 **Start Capture(캡처 시작)**를 클릭합니다.

- 한 번에 하나의 캡처만 실행할 수 있습니다.
- 패킷 캡처가 실행 중일 때 패킷 캡처 페이지에 진행 중인 캡처의 상태가 표시되어 파일 크기 및 경과된 시간과 같은 현재 통계를 보여줍니다.
- GUI에는 CLI가 아닌 GUI에서 시작된 패킷 캡처만 표시됩니다. 마찬가지로 CLI에는 CLI에서 시작된 현재 패킷 캡처 실행의 상태만 표시됩니다.
- 패킷 캡처 파일은 10개로 분할됩니다. 패킷 캡처가 종료되기 전에 파일이 최대 크기 제한에 도달할 경우 파일의 가장 오래된 부분이 삭제되고(데이터가 삭제됨) 새로운 부분이 현재 패킷 캡처 데이터와 함께 시작됩니다. 한 번에 패킷 캡처 파일의 1/10만 삭제됩니다.
- GUI에서 시작된 실행 캡처는 세션 사이에서 유지됩니다. (CLI에서 시작된 실행 캡처는 세션이 종료되면 중지됩니다.)

4단계 캡처가 지정된 기간 동안 실행되도록 허용하거나 캡처가 무한정 실행되도록 지정한 경우 **Stop Capture(캡처 중지)**를 클릭하여 캡처를 중지합니다.

5단계 패킷 캡처 파일에 액세스합니다.

- **패킷 캡처 파일 관리** 목록의 파일을 클릭하고 **Download File(파일 다운로드)**을 클릭합니다.
- FTP 또는 SCP를 사용하여 어플라이언스의 `captures` 하위 디렉토리에 있는 파일에 액세스합니다.

향후 작업

지원팀이 파일을 사용할 수 있게 합니다.

- 어플라이언스에 원격으로 액세스하도록 허용할 경우 기술자가 FTP 또는 SCP를 사용하여 패킷 캡처 파일에 액세스할 수 있습니다. Cisco 기술 지원 담당자에 대한 원격 액세스 활성화, 40-26페이지를 참조하십시오.
- 파일을 지원팀에 이메일로 보냅니다.

41 장

D-모드를 사용하여 아웃바운드 메일 전달 시 어플라이언스 최적화

기능 요약: 최적화된 아웃바운드 전송을 위한 D-모드

D-모드는 아웃바운드 이메일 전달에 특정 Email Security 어플라이언스를 최적화하는 기능으로 키를 사용합니다. 인바운드 메일 처리에 해당하는 기능은 D-모드에서 비활성화됩니다.

D-모드를 사용하는 어플라이언스의 고유 기능

- 256개의 가상 게이트웨이 주소 - Cisco 가상 게이트웨이 기술을 통해 고유한 IP 주소, 호스트 이름 및 도메인 등 호스팅하는 모든 도메인에 엔터프라이즈 메일 게이트웨이를 구성하고 동일한 물리적 어플라이언스 내에서 호스팅하는 동안 이러한 도메인에 대해 기업 이메일 정책 시행하거나 안티스팸 전략을 만들 수 있습니다. 자세한 내용은 5 장, "이메일을 수신하도록 게이트웨이 구성"의 "리스너 사용자 지정"을 참조하십시오.
- IPMM(IronPort Mail Merge) - IPMM(IronPort Mail Merge)은 고객 시스템에서 개인화된 개별 메시지를 생성하는 부담을 덜어줍니다. 수천 개의 개별 메시지를 생성하여 메시지 생성 시스템과 이메일 게이트웨이 간에 메시지를 전송할 필요성을 없애 사용자는 시스템 부하 감소와 이메일 전달 처리량 증가라는 이점을 얻을 수 있습니다. 자세한 내용은 IPMM(IronPort Mail Merge)을 사용하여 대량 메일 전송, 41-4페이지 항목을 참조하십시오.
- 리소스 보존 바운스 설정 - D-모드를 사용하는 어플라이언스에서 잠재적으로 차단된 대상을 탐지하고 해당 대상에 대한 모든 메시지를 바운스하도록 구성할 수 있습니다. 자세한 내용은 리소스 보존 바운스 설정 구성, 41-3페이지 항목을 참조하십시오.
- 아웃바운드 전송의 성능 향상

D-모드를 사용하는 어플라이언스에서 비활성화된 표준 기능

- IronPort Anti-Spam 검사 및 On/Off box 스팸 격리 — 안티스팸 검사는 대부분 수신 메일과 관련이 있으므로 IronPort Anti-Spam 검사 엔진이 비활성화됩니다. 따라서 안티스팸 장은 해당하지 않습니다.
- 신종 바이러스 필터(Outbreak Filter) — 신종 바이러스 필터(Outbreak Filter) 기능은 수신 메일을 격리하는 데 사용되므로 이 기능은 D-모드를 사용하는 어플라이언스에서 비활성화됩니다. 따라서 신종 바이러스 필터(Outbreak Filter) 장의 정보는 해당하지 않습니다.
- SenderBase 네트워크 참여 기능 — SenderBase 네트워크 참여 기능은 수신 메일에 관한 정보를 보고하므로 이 기능은 D-모드를 사용하는 어플라이언스에서 비활성화됩니다. 따라서 SenderBase 네트워크 참여 즉, 에 있는 정보는 해당하지 않습니다.
- 보고 — 보고가 제한됩니다. 일부 보고서는 사용할 수 없으며 발생한 보고는 성능 문제로 인해 매우 제한적인 수준에서 실행되도록 설정됩니다.

참고 D-모드를 사용하는 어플라이언스의 이메일 보안 모니터 개요 보고서에 표시된 총수는 해당 기능이 D-모드를 사용하는 어플라이언스에서 비활성화된 경우에도 스팸 및 의심스러운 스팸 횟수를 잘못 포함할 수 있습니다.

- RSA 데이터 유출 방지 — 발송 메시지의 RSA DLP 검사는 D-모드를 사용하는 어플라이언스에서 비활성화됩니다.

D-모드를 사용하는 어플라이언스에 해당하는 표준 기능

표 41-1 D-모드를 사용하는 어플라이언스에 포함된 AsyncOS 기능

기능	추가 정보
안티바이러스 검사	12 장, "안티바이러스" 항목을 참조하십시오.
도메인 키 서명	DKIM/Domain 키는 발신자가 사용하는 서명 키에 따라 이메일의 신뢰성을 확인하는 방법입니다. 20 장, "이메일 인증" 항목을 참조하십시오.
중앙 집중식 관리	39 장, "클러스터를 사용한 중앙 집중식 관리" 항목을 참조하십시오.
전송 제한	도메인 마다 지정된 기간 동안 시스템에서 초과할 수 없는 최대 연결 및 수신자 수를 할당할 수 있습니다. 이 "양호한 인접" 테이블은 `destconfig` 명령을 통해 정의됩니다. 자세한 내용은 대상 제어을 사용하여 이메일 전달 제어, 24-40페이지 항목을 참조하십시오.
바운스 확인	바운스 메시지의 신뢰성을 확인합니다. 바운스 확인, 24-48페이지 항목을 참조하십시오.
위임 관리	32 장, "관리 작업 분배" 항목을 참조하십시오.
추적(디버그)	테스트 메시지를 사용한 메일 흐름 디버깅: 추적, 40-1페이지 항목을 참조하십시오.

표 41-1 D-모드를 사용하는 어플라이언스에 포함된 AsyncOS 기능 (계속)

기능	추가 정보
VLAN의 NIC 페어링	37 장, "고급 네트워크 구성" 항목을 참조하십시오.
선택적 안티바이러스 엔진	아웃바운드 메시지의 무결성을 확인하기 위해 선택적 안티바이러스 검사를 추가할 수 있습니다. 안티바이러스 검사 개요, 12-1 페이지 항목을 참조하십시오.

최적화된 아웃바운드 메일 전달을 위한 어플라이언스 설정

절차

1단계 제공된 기능 키를 적용합니다. Cisco Email Security 어플라이언스에서 *시스템 설치 마법사를 실행하기 전에*(어플라이언스를 구성하기 전에) 키를 적용해야 합니다. System Administration(시스템 관리) > Feature Key(기능 키) 페이지 또는 CLI의 `featurekey` 명령을 사용하여 키를 적용합니다.

참고 앞에 있는 기능 키에는 아웃바운드 메일의 안티바이러스 검사에 사용할 수 있는 30일 Sophos 또는 McAfee Anti-Virus 라이센스가 포함됩니다.

2단계 어플라이언스를 재부팅합니다.

3단계 시스템 설치 마법사(GUI에서 또는 CLI)를 실행하고 어플라이언스를 구성합니다.

아웃바운드 전송에 최적화된 어플라이언스에는 안티스팸 검사 또는 신종 바이러스 필터(Outbreak Filter) 기능이 포함되지 않습니다. (이러한 장은 무시하십시오.)

참고 클러스터된 환경에서는 D-모드 기능 키로 구성된 어플라이언스를 전송 성능 패키지로 구성되지 않은 AsyncOS 어플라이언스와 결합할 수 없습니다.

리소스 보존 바운스 설정 구성

어플라이언스가 최적화된 아웃바운드 메일 전달으로 구성되면, 시스템이 잠재적인 전송 문제를 탐지하고 대상에 관련된 모든 메시지를 바운스할 수 있도록 구성할 수 있습니다.

참고 이 설정을 사용하면 전송할 수 없다고 간주되는 대상 제어에 대한 큐에서 모든 메시지를 바운스합니다. 전송 문제가 해결되고 나면 메시지를 다시 전송해야 합니다.

리소스 보존 바운스 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 10번의 연속 연결 시도가 실패한 후 호스트가 "다운"되었다고 간주합니다. AsyncOS는 15분마다 다운된 호스트를 검색하므로 큐가 지워지기 전에 10번이 넘는 시도가 수행되었을 가능성이 있습니다.

IPMM(IronPort Mail Merge)을 사용하여 대량 메일 전송

참고 IronPort Mail Merge는 D-모드를 사용하는 어플라이언스에서만 사용할 수 있습니다.

IronPort Mail Merge 개요

IPMM(IronPort Mail Merge)은 고객 시스템에서 개인화된 개별 메시지를 생성하는 부담을 덜어줍니다. 수천 개의 개별 메시지를 생성하여 메시지 생성 시스템과 이메일 게이트웨이 간에 메시지를 전송할 필요성을 없애 시스템 부하는 감소하고 이메일 전달 처리량은 증가합니다.

IPMM을 통해 개인화를 위해 대체될 메시지에 위치를 표시하는 변수를 사용하여 단일 메시지 본문이 생성됩니다. 개별 메시지 수신자마다 이메일 게이트웨이에 수신자 이메일 주소와 변수 대체만 전송되어야 합니다. 또한, IPMM은 기타 수신자로부터 특정 파트를 제외하면서 특정 수신자에게 메시지 본문의 특정 "파트"를 전송하는 데 사용할 수 있습니다. (예를 들어 다른 두 국가에 있는 수신자에게 메시지의 마지막에 다른 저작권 정보를 포함해야 한다고 가정해 보겠습니다.)

메일 병합 기능의 이점

- 메일 관리자의 편의성. IPMM에서 많은 공통 언어로 된 변수 대체 및 추상적인 인터페이스를 제공하므로 각 수신자에 대한 개인화된 메시지를 생성할 때의 복잡성이 없어집니다.

- 메시지 생성 시스템의 부하 감소. 메시지 본문과 필수 대체 테이블을 한 번 복사하므로 메시지 생성 시스템에서 대부분의 메시지 생성 "작업"의 부하를 줄이고 최적화된 아웃바운드 메일 전달으로 구성된 어플라이언스로 이동합니다.
- 전송 처리량 증가. 수천 개의 수신 메시지를 수락 및 큐에 넣는 데 필요한 리소스를 줄여 어플라이언스는 아웃바운드 전송 성능을 크게 향상할 수 있습니다.
- 큐 저장소 효율성. 메시지 수신자마다 적은 정보를 저장하여 사용자는 D-모드를 사용하는 어플라이언스에서 작업량 및 큐 저장소 사용을 더 효율적으로 달성할 수 있습니다.

메일 병합 사용

SMTP 삽입

IPMM은 전송 프로토콜로 SMTP를 확장합니다. 어플라이언스에 설정해야 하는 특별 구성은 없습니다. (기본적으로 IPMM은 D-모드를 사용하는 어플라이언스의 개인 리스너에서는 활성화되고 공용 리스너에서는 비활성화될 수 있습니다.) 그러나 현재 수신 프로토콜로 SMTP를 사용하고 있지 않으면 D-모드를 사용하는 어플라이언스 인터페이스를 통해 SMTP를 사용하는 새 개인 리스너를 만들어야 합니다.

`listenerconfig`의 하위 명령 `setipmm`을 사용하여 리스너에서 IPMM을 활성화합니다. 자세한 내용은 5 장, "이메일을 수신하도록 게이트웨이 구성" 항목을 참조하십시오.

IPMM은 2가지 명령, 즉 `MAIL FROM` 및 `DATA`를 변경하고 `XDFN`을 추가하여 SMTP를 수정합니다. `MAIL FROM` 명령은 `XMRG FROM`으로 대체되고 `DATA` 명령은 `XPRT`로 대체됩니다.

Mail Merge 메시지를 생성하려면 메시지를 생성하는 데 사용한 명령이 특정 시퀀스에서 실행되어야 합니다.

1. 전송 호스트를 식별하는 초기 EHLO 문입니다.
2. 각 메시지는 발신자 주소를 나타내는 XMRG FROM: 문으로 시작합니다.
3. 그러면 각 수신자가 다음과 같이 정의됩니다.
   - 파트(XDFN *파트=1,2,3...) 정의 및 기타 수신자별 변수를 포함하는 하나 이상의 XDFN 변수 할당문이 만들어집니다.
   - 수신자 이메일 주소는 RCPT TO: 문으로 정의됩니다. RCPT TO: 앞과 XMRG FROM 또는 RCPT TO 명령 뒤의 모든 변수 할당은 해당 수신자 이메일 주소로 매핑됩니다.
4. 각 파트는 XPRT n 명령을 사용하여 정의되며 DATA 명령과 유사한 마침표(.) 문자로 종료됩니다. 마지막 파트는 XPRT n LAST 명령을 사용하여 정의됩니다.

변수 대체

메시지 헤더가 포함된 메시지 본문의 모든 파트는 대체용 변수를 포함할 수 있습니다. 변수는 HTML 메시지로 표시될 수도 있습니다. 변수는 사용자가 정의하며, 앰퍼샌드(&) 문자로 시작하고 세미콜론 문자(;)로 끝나야 합니다. 별표(*)로 시작하는 변수 이름은 예약되어 있어 사용할 수 없습니다.

예약 변수

IPMM은 사전 정의된 5개의 특수 "예약 변수"가 있습니다.

표 41-2 IPMM: 예약 변수

*FROM	예약 변수 *FROM? "Envelope From" 매개변수에서 파생됩니다. "Envelope From" 매개변수는 "XMRG FROM:" 명령을 사용하여 설정됩니다.
*TO	예약 변수 *TO는 "RCPT TO:" 명령을 사용하여 설정된 대로 봉투 수신자 값에서 파생됩니다.
*PARTS	예약 변수 *PARTS는 쉼표로 구분된 파트 목록을 보유합니다. 이는 "RCPT TO:"로 수신자를 정의하기 전에 설정되며 특정 사용자가 수신하는 "XPRT n" 메시지 본문 중 어떤 부분을 차단할지를 결정합니다.
*DATE	예약 변수 *DATE는 현재 날짜 스탬프로 대체됩니다.
*DK	예약 변수 *DK는 DomainKeys Signing 프로파일(이 프로파일은 반드시 AsyncOS에 이미 있어야 함)을 지정하는 데 사용됩니다. DomainKeys Signing 프로파일 생성에 대한 자세한 내용은 20 장, "이메일 인증" 항목을 참조하십시오.

예제 메시지 #1

다음의 예제 메시지 본문(헤더 포함)에는 4개의 고유 변수와 최종 메시지에서 대체될 5개의 대체 위치가 있습니다. 동일한 변수가 메시지 본문에 두 번 이상 사용될 수 있습니다. 또한, 예약 변수 &*TO;가 사용되며 이는 수신자 이메일 주소로 대체됩니다. 이 예약 변수는 별도의 변수로 전달할 필요가 없습니다. 예제에 있는 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.
```

이 메시지는 어플라이언스에 한 번만 삽입해야 합니다. 각 수신자의 경우 다음 추가 정보가 필요합니다.

- 수신자 이메일 주소
- 변수 대체용 이름 값 쌍

파트 어셈블리

SMTP가 각 메시지 본문에 단일 DATA 명령을 사용하는 경우 IPMM은 하나 이상의 XPRT 명령을 사용하여 메시지를 구성합니다. 파트는 주문별로 수신자에 따라 조합됩니다. 각 수신자는 메시지 파트를 일부 또는 모두 수신할 수 있습니다. 파트는 어떤 순서로도 조합 가능합니다.

특수 변수 *PARTS는 쉼표로 구분된 파트 목록을 보유합니다.

예를 들어 다음의 예제 메시지에는 두 개의 파트가 포함됩니다.

첫 번째 파트에는 메시지 헤더와 메시지 본문 일부가 포함됩니다. 두 번째 파트에는 특정 고객을 위해 가변적으로 포함할 수 있는 제안 사항이 포함됩니다.

예제 메시지 #2, 파트 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.
```

예제 메시지 #2, 파트 2

```
Please accept our offer for 10% off your next sprocket purchase.
```

해당 메시지 파트는 어플라이언스에 한 번만 삽입해야 합니다. 이 경우 각 수신자는 다음의 추가 정보가 필요합니다.

- 최종 메시지에 포함할 파트의 순서 목록
- 수신자 이메일 주소
- 변수 대체용 이름 값 쌍

IPMM 및 DomainKeys Signing

IPMM은 DomainKeys Signing을 지원하지 않습니다. *DK 예약 변수를 사용하여 DomainKeys 프로파일을 지정합니다. 예를 들면 다음과 같습니다.

```
XDFN first_name="Jane" last_name="User" color="red" *PARTS=1,2 *DK=mass_mailing_1
```

이 예제에서 "mail_mailing_1"은 이전에 구성한 DomainKeys 프로파일의 이름입니다.

명령 설명

클라이언트가 IPMM 메시지를 리스너에 삽입하는 경우 다음 키 명령을 사용하여 확장된 SMTP를 사용합니다.

XMRG FROM

구문:

```
XMRG FROM: <sender email address>
```

이 명령은 SMTP MAIL FROM: 명령을 대체하고 다음에 IPMM 메시지가 표시됨을 나타냅니다. IPMM 작업은 XMRG FROM: 명령을 사용하여 초기화됩니다.

XDFN

구문:

```
XDFN <KEY=VALUE> [KEY=VALUE]
```

XDFN 명령은 수신자별 메타데이터를 설정합니다. 키-값 쌍은 선택적으로 꺾쇠괄호 또는 대괄호로 묶을 수 있습니다.

*PARTS는 XPRT 명령(아래 설명)으로 정의된 대로 인덱스 번호를 나타내는 특수 예약 변수입니다. *PARTS 변수는 쉼표로 구분된 정수 목록으로 나누어집니다. 정수는 XPRT 명령을 사용하여 정의된 대로 전송할 본문 파트와 일치합니다. 다른 예약 변수는 *FROM, *TO 및 *DATE입니다.

XPRT

구문:

```
XPRT index_number LAST

Message

.
```

XPRT 명령은 SMTP DATA 명령을 대체합니다. 해당 명령은 명령이 실행된 후 메시지 파트의 전송을 수락합니다. 명령은 특정 줄에서 하나의 마침표 완료되며 바로 뒤에 반환 문자가 삽입됩니다 (SMTP DATA 명령 완료 방식과 동일).

특수 키워드 **LAST**는 메일 병합 작업의 끝을 나타내며 삽입할 최종 파트를 지정하는 데 사용해야 합니다.

LAST 키워드가 사용된 후 메시지는 큐에 대기 되며 전송이 시작됩니다.

변수 정의에 대한 참고 사항

- XDFN 명령을 사용하여 변수를 정의하는 경우 실제 명령줄은 시스템의 실제 제한 크기를 초과할 수 없습니다. D-모드를 사용하는 어플라이언스의 경우 이 제한 크기는 줄당 4KB입니다. 다른 호스트 시스템에는 더 낮은 임계값이 사용될 수 있습니다. 매우 큰 줄에서 여러 변수를 정의하는 경우 주의해야 합니다.
- 변수 키-값 쌍을 정의할 때 슬래시"/" 문자를 사용하여 특수 문자를 이스케이프할 수 있습니다. 메시지 본문에 변수 정의로 잘못 대체된 HTML 문자 엔티티가 포함된 경우에 유용합니다. 예를 들면 문자 엔티티 ™가 상표 문자의 HTML 문자를 정의합니다. 명령 XDFN trade=foo를 만든 후 HTML 문자 엔티티 "™"를 포함하는 IPMM 메시지를 만든 경우 조합된 메시지에는 상표 문자 대신 변수 대체 ("foo")가 포함됩니다. GET 명령을 포함하는 URL에 사용되기도 하는 앰퍼샌드 문자 "&"에도 동일한 개념이 적용됩니다.

IPMM 대화 예제

다음은 예제 메시지 #2(위에 표시)의 IPMM 대화 예제입니다. 이 예제에서 메시지는 두 명의 수신자("Jane User" 및 "Joe User")에게 전송됩니다.

이 예제에서 **굵게** 입력된 내용은 D-모드를 사용하는 어플라이언스에서 수동 SMTP 대화로 입력된 내용이며 monospaced type으로 입력된 내용은 SMTP 서버의 응답을 나타내고 *기울임꼴*은 주석 또는 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
```

변수 및 파트는 수신자마다 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
```

다음으로 파트 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 파트 2가 전송됩니다. LAST 키워드는 조합할 최종 파트로서 파트 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 예제에 따라 수신자 Jane User는 다음 메시지를 받게 됩니다.

```
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 User는 다음 메시지를 받게 됩니다.

```
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.
```

예제 코드

Cisco에서 공통 프로그래밍 언어로 라이브러리를 만들어 IPMM이 활성화된 어플라이언스 리스너에 IPMM 메시지를 삽입하는 작업을 추상화했습니다. IPMM 라이브러리 사용 방법에 대한 예제는 Cisco 고객 지원팀에 문의하십시오. 코드는 구문을 설명하기 위해 광범위하게 사용됩니다.

42 장

Cisco Content Security Management Appliance 에서 서비스 중앙 집중화

Content Security Management Appliance 서비스의 개요

Cisco Content 보안 관리 어플라이언스(M-Series 어플라이언스)는 외부 또는 "오프 박스" 위치로, 여러 Email Security 어플라이언스의 특정 서비스에 단일 인터페이스를 제공합니다.

보안 관리 어플라이언스에서 제공하는 기능은 다음과 같습니다.

- 외부 스팸 격리. 최종 사용자에 대한 스팸 및 의심스러운 스팸을 보류하므로 최종 사용자와 관리자가 최종 결정을 내리기 전에 스팸으로 플래그가 지정된 메시지를 검토할 수 있습니다.
- 중앙 집중 식 정책, 바이러스 및 신종 바이러스 격리. 방화벽 뒤에 안티바이러스 검사, 신종 바이러스 필터(Outbreak Filter) 및 정책을 통해 격리된 메시지를 저장하고 관리하는 단일 위치를 제공합니다.
- 중앙 집중식 보고. 여러 Email Security 어플라이언스에서 집계된 데이터에 대한 보고서를 실행합니다.
- 중앙 집중식 추적. 여러 Email Security 어플라이언스를 이동하는 이메일 메시지를 추적합니다.

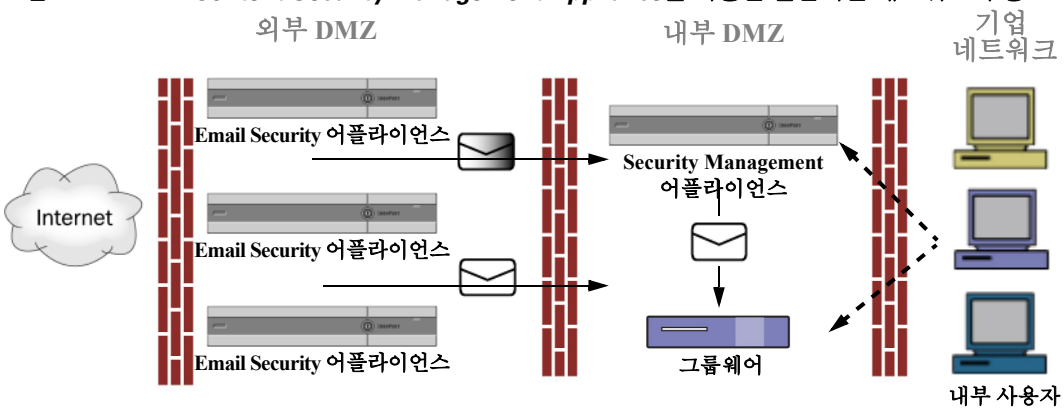
Cisco Content 보안 관리 어플라이언스 구성 및 사용에 대한 자세한 내용은 *Cisco Content Security Management Appliance 사용 설명서*를 참조하십시오.

네트워킹 계획

Cisco Content 보안 관리 어플라이언스를 사용하여 다양한 DMZ에 상주하는 더 안전한 게이트웨이 시스템에서 최종 사용자 인터페이스(메일 애플리케이션 등)를 분리할 수 있습니다. 2계층 방화벽을 사용하면 최종 사용자가 외부 DMZ에 직접 연결하지 못하도록 네트워킹 계획 시 유연성을 발휘할 수 있습니다.

그림 42-1에서는 보안 관리 어플라이언스와 여러 DMZ를 통합하는 일반적인 네트워크 구성을 보여줍니다.

그림 42-1 Content Security Management Appliance를 사용한 일반적인 네트워크 구성



대기업 데이터 센터에서는 하나의 보안 관리 어플라이언스(하나 이상의 Email Security 어플라이언스에 대한 외부 스팸 격리로 사용됨)를 공유합니다. 한편 원격 사무소는 로컬 사용을 위해 Email Security 어플라이언스에 로컬 스팸 격리를 유지할 수 있습니다.

외부 스팸 격리 사용

메일 흐름 및 외부 스팸 격리

그림 42-1에 설명된 대로 네트워크를 구성한 경우 외부 DMZ의 어플라이언스에서 인터넷의 수신 메일을 수신합니다. 클린 메일은 내부 DMZ의 MTA(mail transfer agent)(그룹웨어)로 전송되어 결국에는 회사 네트워크 내의 최종 사용자에게 전달됩니다.

스팸 및 의심스러운 스팸(사용자의 메일 흐름 정책 설정에 따라 결정됨)은 보안 관리 어플라이언스의 스팸 격리로 전송됩니다. 그러면 최종 사용자가 격리를 평가하고 스팸을 삭제하고 받으려는 메시지를 릴리스할 수 있습니다. 스팸 격리에 남아 있는 메시지는 구성 가능한 시간이 지나면 자동으로 삭제됩니다.

보안 관리 어플라이언스의 외부 격리에서 릴리스된 메시지는 전송을 위해 원래 Email Security 어플라이언스로 반환됩니다. 이러한 메시지는 일반적으로 전송 전에 HAT 및 기타 정책 또는 검사 설정, RAT, 도메인 예외, 앨리어싱, 수신 필터, 마스커레이드, 바운스 확인, 작업 큐와 같은 프로세스를 거치지 않습니다.

Email Security 어플라이언스는 보안 관리 어플라이언스로 메일을 전송하도록 구성된 경우 보안 관리 어플라이언스에서 릴리스된 메시지를 자동으로 수신할 것으로 예상하므로 해당 메시지가 다시 수신될 경우 재처리하지 않습니다. 이를 위해서는 보안 관리 어플라이언스의 IP 주소를 변경하지 말아야 합니다. 보안 관리 어플라이언스의 IP 주소가 변경될 경우 수신 Email Security 어플라이언스가 해당 메시지를 다른 수신 메시지와 동일하게 처리합니다. 따라서 사용자는 항상 보안 관리 어플라이언스의 수신 및 전송에 동일한 IP 주소를 사용해야 합니다.

보안 관리 어플라이언스는 스팸 격리 설정에 지정된 IP 주소에서 수신되는 메일을 수락하여 격리합니다. 보안 관리 어플라이언스에서 스팸 격리를 구성하려면 *Cisco Content Security Management Appliance 사용 설명서*를 참조하십시오.

보안 관리 어플라이언스에서 릴리스된 메일은 스팸 격리 설정(*Cisco Content Security Management Appliance 사용 설명서* 참조)에 정의된 대로 주 호스트와 보조 호스트(콘텐츠 보안 어플라이언스 또는 기타 그룹웨어 호스트)로 전송됩니다. 따라서 Email Security 어플라이언스에서 보안 관리 어플라이언스에 전송하는 메일의 수와 관계없이 릴리스된 모든 메일, 알림, 경고가 단일 호스트(그룹웨어 또는 콘텐츠 보안 어플라이언스)로 전송됩니다. 보안 관리 어플라이언스에서 메일을 전송하기 위해 주 호스트에 과도한 부담을 주지 않도록 주의하십시오.

로컬 스팸 격리에서 외부 격리로 마이그레이션

현재 Email Security 어플라이언스의 로컬 스팸 격리를 사용하고 있지만 로컬 격리의 메시지에 대한 액세스는 유지하면서 보안 관리 어플라이언스에서 호스팅된 외부 스팸 격리로 마이그레이션하려면 새 메시지가 전환 도중 로컬 격리로 들어가는 것을 방지해야 합니다.

아래의 가능한 전략을 고려하십시오.

- 안티스팸 설정 구성 - 메일 정책에서 보안 관리 어플라이언스를 대체 호스트로 지정하는 안티스팸 설정을 구성합니다. 이 작업은 새 스팸을 외부 격리로 보내는 한편 로컬 격리에 대한 액세스를 여전히 허용합니다.
- 더 짧은 만료 시간 설정 - 로컬 격리의 삭제 기준 일정을 더 짧은 기간으로 구성합니다.
- 남은 메시지 모두 삭제 - 로컬 격리에 남아 있는 모든 메시지를 삭제하려면 격리를 비활성화하고 로컬 격리 페이지의 "Delete All(모두 삭제)" 링크를 클릭합니다(스팸 격리에서 메시지 삭제, 31-23 페이지 참조). 이 링크는 여전히 메시지를 포함한 로컬 스팸 격리가 비활성화되었을 경우에만 사용할 수 있습니다.

현재 외부 격리를 활성화하고 로컬 격리를 비활성화할 준비가 되어 있어야 합니다.

참고 로컬 격리와 외부 격리가 모두 활성화된 경우에는 로컬 격리가 사용됩니다.

외부 스팸 격리 및 외부 허용 목록/차단 목록 활성화

Email Security 어플라이언스에서 1개의 외부 스팸 격리만 활성화할 수 있습니다.

시작하기 전에

- 메일 흐름 및 외부 스팸 격리, 42-2페이지의 정보를 검토합니다.

- 로컬 스팸 격리에서 외부 격리로 마이그레이션, 42-3페이지의 정보를 검토하고 해당 정보에 대한 작업을 수행합니다.
- 중앙 집중식 스팸 격리와 허용 목록/차단 목록 기능을 지원하도록 보안 관리 어플라이언스를 구성합니다. 보안 관리 어플라이언스의 설명서를 참조하십시오.
- 다른 외부 스팸 격리가 이전에 Email Security 어플라이언스에 대해 구성된 경우 먼저 외부 스팸 격리 설정을 비활성화합니다.

각 Email Security 어플라이언스에서 다음 절차를 완료합니다.

절차

1단계 **Security Services(보안 서비스) > Centralized Services(중앙 집중식 서비스) > Spam Quarantine(스팸 격리)**을 선택합니다.

2단계 **Configure(구성)**를 클릭합니다.

3단계 **Enable External Spam Quarantine(외부 스팸 격리 활성화)**을 선택합니다.

4단계 이름 필드에 보안 관리 어플라이언스의 이름을 입력합니다.

이 이름은 중요하지 않으며 참조 목적으로만 사용됩니다. 예를 들어, 보안 관리 어플라이언스의 호스트 이름을 입력합니다.

5단계 IP 주소와 포트 번호를 입력합니다.

이 IP 주소와 포트 번호는 스팸 격리 설정 페이지에서 보안 관리 어플라이언스에 대해 지정된 IP 주소와 포트 번호와 일치해야 합니다(**Management Appliance(관리 어플라이언스) > Centralized Services(중앙 집중식 서비스) > Spam Quarantine(스팸 격리)**).

6단계 (선택 사항) **외부 허용 목록/차단 목록** 기능을 활성화할 확인란을 선택하고 해당 차단 목록 작업을 지정합니다.

7단계 변경 사항을 제출하고 커밋합니다.

8단계 각 Email Security 어플라이언스에 대해 이 절차를 반복합니다.

향후 작업

로컬 격리를 사용하고 있는 경우 외부 격리를 활성화하기 위해 로컬 스팸 격리 비활성화, 42-4페이지를 참조하십시오.

관련 주제

- 로컬 바이러스 외부 스팸 격리, 31-1페이지
- 31 장, "스팸 격리"
- 13 장, "안티스팸"
- 메시지에서 스팸을 검사하도록 어플라이언스를 구성하는 방법, 13-2페이지

외부 격리를 활성화하기 위해 로컬 스팸 격리 비활성화

외부 스팸 격리를 활성화하기 전에 로컬 스팸 격리를 사용한 경우 외부 격리로 메시지를 전송하려면 로컬 격리를 비활성화해야 합니다.

시작하기 전에

시작하기 전에 섹션의 정보를 포함하여 외부 스팸 격리 및 외부 허용 목록/차단 목록 활성화, 42-3 페이지의 모든 지침을 따릅니다.

절차

1단계 **Monitor(모니터링) > Spam Quarantine(스팸 격리)**을 선택합니다.

2단계 스팸 격리 섹션에서 **Spam Quarantine(스팸 격리)** 링크를 클릭합니다.

3단계 **Enable Spam Quarantine(스팸 격리 사용)**을 선택 취소합니다.

이 변경의 결과로 메일 정책을 조정하라는 메시지를 무시합니다. 외부 격리 설정을 구성한 경우 메일 정책이 메시지를 외부 스팸 격리로 자동 전송합니다.

4단계 변경 사항을 제출하고 커밋합니다.

외부 스팸 격리 문제 해결

Email Security 어플라이언스가 외부 격리에서 릴리스된 메시지 재처리

문제 보안 관리 어플라이언스에서 릴리스된 메시지는 Email Security 어플라이언스에서 불필요하게 재처리되지 않습니다.

솔루션 이는 보안 관리 어플라이언스의 IP 주소가 변경된 경우에 발생할 수 있습니다. 메일 흐름 및 외부 스팸 격리, 42-2페이지를 참조하십시오.

정책, 바이러스 및 신종 바이러스 격리 중앙 집중화 정보

중앙 집중식 정책, 바이러스 및 신종 바이러스 격리

보안 관리 어플라이언스의 정책, 바이러스 및 신종 바이러스 격리를 중앙 집중화할 수 있습니다. 메시지는 Email Security 어플라이언스에서 처리되지만 보안 관리 어플라이언스의 격리에 저장됩니다.

정책, 바이러스 및 신종 바이러스 격리를 중앙 집중화하면 다음과 같은 이점을 얻을 수 있습니다.

- 관리자가 하나의 위치에서 여러 Email Security 어플라이언스의 격리된 메시지를 관리할 수 있습니다.
- 격리된 메시지가 DMZ가 아닌 방화벽 뒤에 저장되므로 보안 위험이 감소합니다.
- 보안 관리 어플라이언스의 표준 백업 기능을 사용하여 중앙 집중식 격리를 백업할 수 있습니다.

자세한 내용은 보안 관리 어플라이언스의 사용 설명서 또는 온라인 도움말을 참조하십시오.

중앙 집중식 정책, 바이러스 및 신종 바이러스 격리의 제한 사항

- 각 Email Security 어플라이언스에서 모든 정책, 바이러스 및 신종 바이러스 격리를 중앙 집중화하거나 로컬에 저장해야 합니다.
- 보안 관리 어플라이언스에서 검사 엔진을 사용할 수 없으므로 정책, 바이러스 또는 신종 바이러스 격리의 메시지를 수동으로 테스트하여 바이러스가 있는지 확인할 수 없습니다.

클러스터 구성의 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리 요건

클러스터 어플라이언스에 대해 모든 수준에서 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리를 활성화할 수 있습니다.

요건:

- 특정 수준(머신, 그룹 또는 클러스터)에서 Email Security 어플라이언스의 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리를 활성화하기 전에 동일한 수준에 속한 모든 어플라이언스를 먼저 보안 관리 어플라이언스에 추가해야 합니다.
- 콘텐츠 및 메시지 필터와 DLP 메시지 작업은 동일한 수준에서 구성해야 하며 해당 수준 아래의 수준에서 재정의되지 않습니다.
- 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리 설정은 동일한 수준에서 구성해야 하며 구성된 수준보다 낮은 수준에서 재정의되지 않습니다.
- 보안 관리 어플라이언스와의 통신에 사용할 인터페이스가 해당 그룹 또는 클러스터의 모든 어플라이언스에서 이름이 같은지 확인합니다.

예:

클러스터 또는 그룹 수준에서 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리를 활성화하려 하지만 해당 클러스터에 연결된 Email Security 어플라이언스에서 이러한 설정이 머신 수준에서 정의된 경우 머신 수준에서 구성된 중앙 집중식 격리 설정을 먼저 제거해야만 클러스터 또는 그룹 수준에서 해당 기능을 활성화할 수 있습니다.

정책, 바이러스 및 신종 바이러스 격리 마이그레이션 정보

정책, 바이러스 및 신종 바이러스 격리를 중앙 집중화하면 Email Security 어플라이언스의 기존 정책, 바이러스 및 신종 바이러스 격리가 보안 관리 어플라이언스로 마이그레이션됩니다.

보안 관리 어플라이언스에서 마이그레이션을 구성하지만 Email Security 어플라이언스의 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리를 활성화하는 변경 사항을 커밋할 때 마이그레이션이 발생합니다.

이 변경 사항을 커밋하면 다음과 같은 결과가 발 발생 합니다:

- Email Security 어플라이언스의 로컬 정책, 바이러스 및 신종 바이러스 격리가 비활성화됩니다. 이 격리로 들어가는 모든 새 메시지가 보안 관리 어플라이언스에서 격리됩니다.
- 기존의 비 스팸 격리가 보안 관리 어플라이언스로 마이그레이션되기 시작합니다.
- 모든 로컬 정책, 바이러스 및 신종 바이러스 격리가 삭제됩니다. 사용자 지정 마이그레이션을 구성한 경우 마이그레이션하지 않기로 선택한 로컬 정책 격리도 삭제됩니다. 정책 격리를 삭제할 경우 미치는 영향은 정책 격리 삭제 정보, 30-7페이지를 참조하십시오.
- 마이그레이션 전에 여러 격리에 있던 메시지는 마이그레이션 후에 해당 중앙 집중식 격리로 옮겨집니다.

- 마이그레이션은 백그라운드에서 진행됩니다. 소요되는 시간은 격리의 크기와 네트워크에 따라 다릅니다. Email Security 어플라이언스에서 중앙 집중식 격리를 활성화할 경우 마이그레이션 완료 시 알림을 받을 이메일 주소를 하나 이상 입력할 수 있습니다.
- 시작 로컬 격리의 설정이 아닌 중앙 집중식 격리의 설정이 메시지에 적용됩니다. 그러나 원래 만료 시간이 여전히 각 메시지에 적용됩니다.

참고 마이그레이션 도중 자동으로 생성된 모든 중앙 집중식 격리에는 기본 격리 설정이 지정됩니다.

정책, 바이러스 및 신종 바이러스 격리 중앙 집중화

참고 유지 관리 도중 또는 사용량이 적은 시간에 이 절차를 수행합니다.

시작하기 전에

- 먼저 정책, 바이러스 및 신종 바이러스 격리를 중앙 집중화하도록 보안 관리 어플라이언스를 구성해야 합니다. 보안 관리 어플라이언스의 온라인 도움말 또는 사용 설명서의 "중앙 집중식 정책, 바이러스 및 신종 바이러스 격리" 장에 있는 "정책, 바이러스 및 신종 바이러스 격리 중앙 집중화" 섹션의 표를 참조하십시오.
- 보안 관리 어플라이언스의 중앙 집중식 격리에 할당된 공간이 기존 로컬 격리가 전체적으로 사용하는 공간보다 작을 경우 보안 관리 어플라이언스의 격리 설정에 따라 메시지가 조기에 만료됩니다. 마이그레이션 전에 수동 작업을 수행하여 격리 크기를 줄이는 것을 고려하십시오. 조기 만료에 대한 자세한 내용은 자동으로 처리된 격리 메시지에 대한 기본 작업, 30-4페이지를 참조하십시오.
- 지동 마이그레이션을 선택했거나 마이그레이션 도중 중앙 집중식 격리를 생성하도록 사용자 지정 마이그레이션을 구성한 경우 중앙 집중식 격리 구성의 지침으로 사용할 수 있도록 Email Security 어플라이언스의 현재 격리 설정을 기록해 두는 것이 좋습니다.
- Email Security 어플라이언스가 클러스터 구성으로 배포될 경우 클러스터 구성의 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리 요건, 42-6페이지를 참조하십시오.
- 이 절차에서 변경 사항을 커밋하는 즉시 변경이 발생한다는 점에 유의하십시오. 정책, 바이러스 및 신종 바이러스 격리 마이그레이션 정보, 42-6페이지를 참조하십시오.

절차

1단계 **Security Services(보안 서비스) > Centralized Services(중앙 집중식 서비스) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택합니다.

2단계 **Enable(활성화)**을 클릭합니다.

3단계 보안 관리 어플라이언스와의 통신에 사용할 인터페이스와 포트를 입력합니다.

보안 관리 어플라이언스에서 인터페이스와 포트에 연결할 수 있는지 확인합니다.

Email Security 어플라이언스가 클러스터링된 경우 선택한 인터페이스를 클러스터의 모든 머신에서 사용할 수 있어야 합니다.

4단계 마이그레이션 완료 시 알림을 받으려면 이메일 주소를 하나 이상 입력합니다.

5단계 격리가 원하는 대로 마이그레이션되도록 해당 격리에 대한 정보를 확인합니다.

6단계 사용자 지정 마이그레이션을 완료할 경우 이 절차의 변경 사항을 커밋할 때 삭제될 격리를 기록해 둡니다.

7단계 콘텐츠 및 메시지 필터와 DLP 메시지 작업이 기대한 대로 업데이트되도록 해당 정보를 확인합니다.

참고 클러스터 구성의 경우 필터 및 메시지 작업이 특정 수준에서 정의된 경우에만 필터 및 메시지 작업이 해당 수준에서 자동으로 업데이트되고 해당 수준보다 낮은 수준에서 재정의되지 않을 수 있습니다. 마이그레이션 후, 중앙 집중식 격리 이름을 사용하여 필터와 메시지 작업을 수동으로 재구성해야 합니다.

8단계 마이그레이션 매핑을 재구성해야 하는 경우:

a. 보안 관리 어플라이언스로 돌아갑니다.

b. 마이그레이션 매핑을 재구성합니다.

관리 어플라이언스에서 다시 매핑할 격리를 선택한 다음 **Remove from Centralized Quarantine(중앙 집중식 격리에서 제거)**을 클릭합니다. 그러면 격리를 다시 매핑할 수 있습니다.

c. 보안 관리 어플라이언스에서 새로운 마이그레이션 구성을 커밋합니다.

d. 이 절차를 처음부터 시작합니다.

중요! Security Services(보안 서비스) > Centralized Services(중앙 집중식 서비스) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리) 페이지를 다시 로드하십시오.

9단계 **Submit(제출)**을 클릭합니다.

10단계 마이그레이션 매핑을 재구성해야 할 경우 8단계의 절차를 따르십시오.

11단계 변경 사항을 커밋합니다.

참고 마이그레이션이 진행 중인 상태에서는 Email Security 어플라이언스 또는 보안 관리 어플라이언스에서 구성을 변경하지 마십시오.

12단계 페이지의 상단에서 마이그레이션 상태를 모니터링하거나 마이그레이션 구성 시 이메일 주소를 입력한 경우 마이그레이션이 완료되었음을 알리는 이메일을 기다립니다.

향후 작업

보안 관리 어플라이언스의 온라인 도움말 또는 사용 설명서의 "정책, 바이러스 및 신종 바이러스 격리 중앙 집중화" 항목의 표에 설명된 나머지 작업을 수행합니다.

관련 주제

- 정책, 바이러스 및 신종 바이러스 격리에 액세스할 수 있는 사용자 그룹, 30-9페이지

중앙 집중식 정책, 바이러스 및 신종 바이러스 격리 비활성화 정보

Email Security 어플라이언스에서 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리를 비활성화할 경우:

- 로컬 격리가 Email Security 어플라이언스에서 자동으로 활성화됩니다.
- 시스템에서 생성한 격리 및 메시지 필터, 콘텐츠 필터에서 참조하는 격리와 DLP 메시지 작업이 Email Security 어플라이언스에서 자동으로 생성됩니다. 바이러스, 신종 바이러스 및 미분류 격리는 할당된 사용자 역할을 포함해 격리가 중앙 집중화되기 전에 사용했던 것과 동일한 설정으로 생성됩니다. 기타 모든 격리는 기본 설정으로 생성됩니다.

- 새로 격리된 메시지가 즉시 로컬 격리로 이동합니다.
- 중앙 집중식 격리가 비활성화될 때 격리 안의 메시지는 다음 중 하나가 발생할 때까지 남아 있습니다.
  - 메시지가 만료되면 수동으로 삭제되거나 자동으로 삭제됩니다.
  - 다음 중 하나가 참일 때에도 메시지가 수동으로 또는 자동으로 릴리스됩니다.

    * 대체 릴리스 어플라이언스가 보안 관리 어플라이언스에서 구성됩니다. 보안 관리 어플라이언스의 온라인 도움말 또는 설명서를 참조하십시오.

    * 중앙 집중식 격리가 Email Security 어플라이언스에서 다시 활성화됩니다.

중앙 집중식 정책, 바이러스 및 신종 바이러스 격리 비활성화

시작하기 전에

- 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리의 영향을 이해합니다를 참조하십시오.
- 다음 중 하나를 수행합니다.
  - 현재 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리에 있는 모든 메시지를 처리합니다.
  - 중앙 집중식 격리를 비활성화한 후 여기에서 릴리스된 메시지를 처리할 대체 릴리스 어플라이언스를 지정했는지 확인합니다. 자세한 내용은 보안 관리 어플라이언스의 온라인 도움말 또는 사용 설명서를 참조하십시오.

절차

1단계 Email Security 어플라이언스에서 **Security Services(보안 서비스) > Centralized Services(중앙 집중식 서비스) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 신종 바이러스 격리)**를 선택합니다.

2단계 중앙 집중식 정책, 바이러스 및 신종 바이러스 격리를 비활성화합니다.

3단계 변경 사항을 제출하고 커밋합니다.

4단계 새로 생성된 로컬 격리의 설정을 사용자 지정합니다.

중앙 집중식 정책, 바이러스 및 신종 바이러스 격리 문제 해결

Content Security Management Appliance가 고장 난 경우

정책, 바이러스 및 신종 바이러스 격리가 고장 난 보안 관리 어플라이언스에서 중앙 집중화된 경우 Email Security 어플라이언스에서 이러한 중앙 집중식 격리를 비활성화해야 합니다.

교체 보안 관리 어플라이언스를 배포할 경우 보안 관리 어플라이언스와 각 Email Security 어플라이언스에서 격리 마이그레이션을 재구성해야 합니다. 보안 관리 어플라이언스의 온라인 도움말 또는 사용 설명서의 "중앙 집중식 정책, 바이러스 및 신종 바이러스 격리" 장에 있는 "정책, 바이러스 및 신종 바이러스 격리 중앙 집중화" 섹션의 표를 참조하십시오.

중앙 집중식 보고 구성

시작하기 전에

- 보안 관리 어플라이언스에서 중앙 집중식 보고를 활성화하고 구성합니다. *Cisco Content Security Management Appliance 사용 설명서*의 요구 사항과 지침을 참조하십시오.
- 보안 관리 어플라이언스의 보고 서비스에 충분한 공간이 할당되었는지 확인합니다.

절차

1단계	**Security Services(보안 서비스) > Reporting(보고)**을 클릭합니다.
2단계	보고 서비스 섹션에서 중앙 집중식 보고 옵션을 선택합니다.
3단계	변경 사항을 제출하고 커밋합니다.

Advanced Malware Protection의 요건

보안 관리 어플라이언스의 Advanced Malware Protection(파일 평판 및 파일 분석)에 대한 전체 보고의 필수 구성은 보안 관리 어플라이언스 소프트웨어 버전의 온라인 도움말 또는 사용 설명서의 이메일 보고 장에 있는 Advanced Malware Protection 보고서에 대한 정보를 참조하십시오.

중앙 집중식 보고 변경 후 보고 정보의 가용성

Email Security 어플라이언스에서 중앙 집중식 보고를 활성화한 경우:

- 월간 보고서의 Email Security 어플라이언스의 기존 데이터가 보안 관리 어플라이언스로 전송되지 않습니다.
- Email Security 어플라이언스에 아카이브된 보고서를 사용할 수 없습니다.
- Email Security 어플라이언스가 일주일 분량의 데이터만 저장합니다.
- 월간 및 연간 보고서의 새 데이터가 보안 관리 어플라이언스에 저장됩니다.
- Email Security 어플라이언스에 예약된 보고서가 일시 중지됩니다.
- Email Security 어플라이언스의 예약된 보고서 구성 페이지에 더 이상 액세스할 수 없습니다.

중앙 집중식 보고 비활성화 정보

Email Security 어플라이언스에서 중앙 집중식 보고를 비활성화하면 Email Security 어플라이언스가 새 월간 보고서 데이터, 예약된 보고서 이력서 저장을 시작하므로 아카이브된 보고서에 액세스할 수 있습니다. 중앙 집중식 보고를 비활성화한 후 어플라이언스에 지난 시간 및 요일의 데이터만 표시되지만 지난 주 또는 달의 데이터는 표시되지 않습니다. 이는 일시적입니다. 어플라이언스에 충분한 데이터가 누적된 후 지난 주 및 지난 달의 보고서가 표시됩니다. Email Security 어플라이언스가 다시 중앙 집중식 보고 모드로 돌아가면 인터랙티브 보고서에 지난 주의 데이터가 표시됩니다.

중앙 집중식 메시지 추적 구성

참고 Email Security 어플라이언스에서 중앙 집중식 및 로컬 추적을 모두 활성화할 수 없습니다.

절차

1단계 **Security Services(보안 서비스) > Message Tracking(메시지 추적)**을 클릭합니다.

2단계 메시지 추적 서비스 섹션에서 **Edit Settings(설정 편집)**를 클릭합니다.

3단계 **Enable Message Tracking Service(메시지 추적 서비스 활성화)** 확인란을 선택합니다.

4단계 중앙 집중식 추적 옵션을 선택합니다.

5단계 (선택 사항) 해당 확인란을 선택하여 거부된 연결의 정보를 저장할 수 있습니다.

참고 거부된 연결의 추적 정보를 저장하면 보안 관리 어플라이언스의 성능에 부정적인 영향을 줄 수 있습니다.

6단계 변경 사항을 제출하고 커밋합니다.

향후 작업

중앙 집중식 추적을 사용하려면 Email Security 어플라이언스 *및* 보안 관리 어플라이언스에서 해당 기능을 활성화해야 합니다. 보안 관리 어플라이언스에서 중앙 집중식 추적을 활성화하려면 *Cisco Content Security Management Appliance 사용 설명서*를 참조하십시오.

중앙 집중식 서비스 사용

중앙 집중식 서비스 사용에 대한 지침은 *Cisco Content Security Management Appliance 사용 설명서*를 참조하십시오.

FTP, SSH, SCP 및 텔넷 액세스

다양한 서비스를 통해 어플라이언스에 생성한 모든 인터페이스에 액세스할 수 있습니다.

IP 인터페이스

IP 인터페이스에는 네트워크에 대한 개별 연결에 필요한 네트워크 구성 데이터가 포함됩니다. 물리적인 이더넷 인터페이스에 여러 IP 인터페이스를 구성할 수 있습니다. IP 인터페이스에 인터넷 프로토콜 버전 4(IPv4) 또는 버전 6(IPv6)을 할당하거나 두 가지 모두를 할당할 수 있습니다.

표 A-1 인터페이스에서 기본적으로 사용 가능한 서비스

		기본적인 사용 가능 여부	
서비스	기본 포트	관리 인터페이스[a]	직접 구성한 새로운 인터페이스
FTP	21	아니요	아니요
Telnet	23	예	아니요
SSH	22	예	아니요
HTTP	80	예	아니요
HTTPS	443	예	아니요

a. 여기에 표시된 "관리 인터페이스" 설정은 C170 어플라이언스의 데이터 1 인터페이스에 대한 기본 설정입니다.

- 그래픽 사용자 인터페이스(GUI)를 통해 어플라이언스에 액세스해야 하는 경우, 인터페이스에서 HTTP 및/또는 HTTPS를 활성화해야 합니다.
- 구성 파일을 업로드 또는 다운로드하기 위해 어플라이언스에 액세스해야 하는 경우, 인터페이스에서 FTP 또는 텔넷을 활성화해야 합니다.
- 또한 Secure Copy(scp)를 사용하여 파일을 업로드 또는 다운로드할 수 있습니다.

IP 인터페이스를 통해 스팸 격리에 대한 HTTP 또는 HTTPS 액세스를 구성할 수 있습니다.

이메일 전송 및 가상 게이트웨이의 경우, 각 IP 인터페이스는 특정 IP 주소 및 호스트 이름이 포함된 단일 가상 게이트웨이 주소 역할을 합니다. 또한 인터페이스를 고유한 그룹(CLI를 통해)으로 "조인"할 수 있으며 이메일 전송 시 시스템이 이 그룹 전체를 순환합니다.

가상 게이트웨이에 조인하거나 이를 그룹화하는 방법은 여러 인터페이스에서 대량 이메일 캠페인에 부하 균형을 실행할 때 유용합니다. 또한 VLAN을 생성하고 다른 인터페이스(CLI를 통해)와 동일하게 구성할 수 있습니다. 자세한 내용은 37 장, "고급 네트워크 구성" 항목을 참조하십시오.

AsyncOS에서 기본 IP 인터페이스를 선택하는 방법

AsyncOS는 IP 인터페이스가 **Network(네트워크) > IP Interfaces(IP 인터페이스)** 페이지 또는 `ifconfig` CLI 명령에 따라 나타나는 순서대로 기본 IP 인터페이스를 선택합니다. 해당 서브넷에 있는 목록의 첫 번째 IP 인터페이스가 사용됩니다.

기본 게이트웨이와 동일한 서브넷에 여러 개의 IP 주소가 구성되어 있는 경우 낮은 숫자의 IP 주소가 사용됩니다. 예를 들어, 다음 IP 주소가 동일한 서브넷에 구성되어 있는 경우,

- 10.10.10.2/24
- 10.10.10.30/24
- 10.10.10.100/24
- 10.10.10.105/24

AsyncOS는 기본 IP 인터페이스로 10.10.10.2/24를 선택합니다.

이메일 보안 어플라이언스에 대한 FTP 액세스 구성

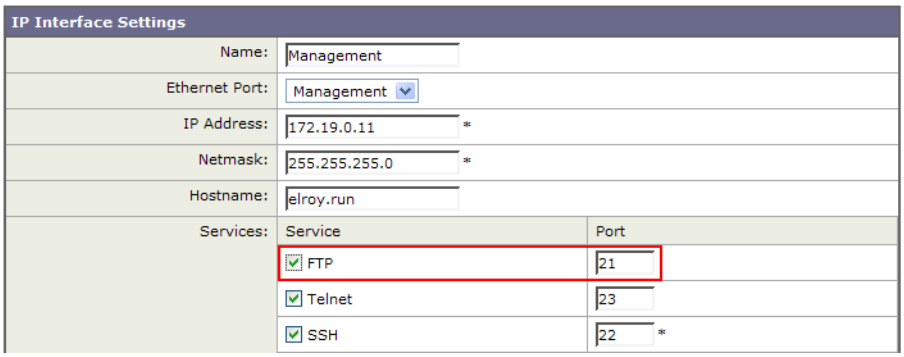
절차

단계 1 Network(네트워크) > IP Interfaces(IP 인터페이스) 페이지 또는 `interfaceconfig` 명령을 사용하여 인터페이스에 대한 FTP 액세스를 활성화합니다.

> 경고: `interfaceconfig` 명령을 통해 서비스를 비활성화하는 경우 어플라이언스에 연결되어 있는 방식에 따라 CLI 연결이 끊어질 수 있습니다. 다른 프로토콜, 직렬 인터페이스 또는 관리 포트의 기본 설정을 사용하여 어플라이언스에 다시 연결할 수 없는 경우 이 명령을 사용하여 서비스를 비활성화하지 마십시오.

이 예제에서, 관리 인터페이스는 포트 21(기본 포트)에서 FTP 액세스를 활성화하기 위해 수정되었습니다.

그림 A-1 IP 인터페이스 편집 페이지



참고 다음 단계로 이동하기 전에 변경사항을 커밋해야 합니다.

단계 2 FTP를 통해 인터페이스에 액세스합니다. 인터페이스에 올바른 IP 주소를 사용하고 있는지 확인합니다. 예를 들면 다음과 같습니다.

```
$ ftp 192.168.42.42
```

참고 여러 브라우저를 사용하는 경우에도 FTP를 통해 인터페이스에 액세스할 수 있습니다.

단계 3 특정 작업을 수행할 디렉토리를 찾습니다. FTP를 통해 인터페이스에 액세스한 후, 다음 디렉토리를 찾아 파일을 복사하고 추가("GET" 및 "PUT")할 수 있습니다. 다음 표를 참조하십시오.

디렉토리 이름	설명
/configuration	다음 명령을 사용하여 데이터가 내보내기 되는 대상 디렉토리 및/또는 가져오기(저장) 되는 원본 디렉토리입니다. • 가상 게이트웨이 매핑(altsrchost) • XML 형식의 구성 데이터 (saveconfig, loadconfig) • HAT(Host Access Table)(hostaccess) • Recipient Access Table(RAT)(rcptaccess) • SMTP 라우팅 항목(smtproutes) • 별칭 테이블(aliasconfig) • 마스커레이드 테이블(masquerade) • 메시지 **필터**(filters) • 전역 구독 취소 데이터(unsubscribe) • trace 명령에 대한 테스트 메시지 • 허용 목록/차단 목록 백업 파일은 다음 형식으로 저장됨: *slbl<timestamp><serial number>.csv*
/antivirus	안티바이러스 엔진 로그 파일이 저장된 디렉토리입니다. 바이러스 정의 파일(scan.dat)에서 마지막으로 성공한 다운로드를 수동으로 확인하기 위해 이 디렉토리의 로그 파일을 검사할 수 있습니다.
/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	**로깅**을 위해 자동으로 생성된 디렉토리입니다(logconfig 및 rollovernow 명령을 통해). 각 로그에 대한 자세한 설명은 로깅 항목을 참조하십시오. 로그 파일 유형의 차이점에 대해서는 "로그 파일 유형 비교"를 참조하십시오.

단계 4 적절한 디렉토리로 파일을 업로드하거나 다운로드하려면 FTP 프로그램을 사용하십시오.

Secure Copy(scp) 액세스

클라이언트 운영 체제에서 Secure Copy(scp) 명령을 지원하는 경우, 이전 표에 나열된 디렉토리에 또는 디렉토리로부터 파일을 복사할 수 있습니다. 예를 들어, 다음 예에서 /tmp/test.txt 파일은 클라이언트 머신에서 호스트 이름이 mail3.example.com인 어플라이언스의 구성 디렉토리로 복사됩니다.

사용자(admin) 비밀번호를 입력하도록 프롬프트가 표시됩니다. 이 예는 참조용으로만 표시되며 특정 운영 체제의 Secure Copy 구현에 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 password: (type the password)

test.txt             100% |***************************|  1007       00:00

%
```

이 예에서 동일한 파일이 어플라이언스에서 클라이언트 머신으로 복사됩니다.

```
% scp admin@mail3.example.com:configuration/text.txt .

admin@mail3.example.com's password: (type the password)

test.txt             100% |***************************|  1007       00:00

%
```

FTP 대신 Secure Copy(scp)를 사용하여 Cisco 어플라이언스에서 파일을 전송할 수 있습니다.

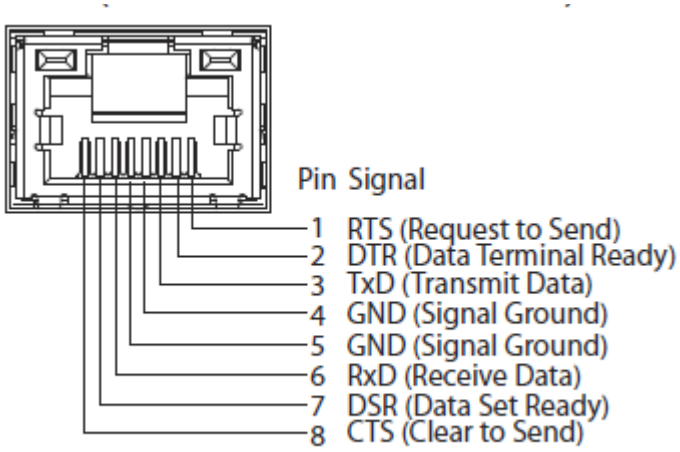
참고 운영자 및 관리자 그룹에 속하는 사용자만 Secure Copy(scp)를 사용하여 어플라이언스에 액세스할 수 있습니다. 자세한 내용은 사용자 추가, 32-4페이지 항목을 참조하십시오.

직렬 연결을 통한 Email Security 어플라이언스 액세스

직렬 연결을 통해 어플라이언스에 연결하는 경우, 콘솔 포트에 다음 정보를 사용하십시오.

이 포트에 대한 전체 내용은 해당 어플라이언스에 대한 하드웨어 설치 가이드에서 확인할 수 있습니다.

80-시리즈 하드웨어의 직렬 포트에 대한 핀아웃 상세정보



70-시리즈 하드웨어의 직렬 포트에 대한 핀아웃 상세정보

그림 A-2는 직렬 포트 커넥터의 핀 번호를 보여주며 표 A-2는 직렬 포트 커넥터의 핀 배열 및 인터페이스 신호를 정의한 것입니다.

그림 A-2 직렬 포트용 핀 번호

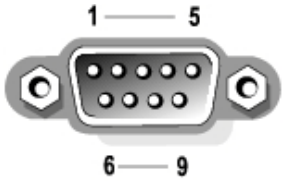


표 A-2 직렬 포트 핀 배열

PIN	신호	I/O	정의
1	DCD	I	데이터 캐리어 탐지
2	SIN	I	직렬 입력
3	SOUT	O	직렬 출력
4	DTR	O	데이터 터미널 대기
5	GND	해당 없음	신호 접지
6	DSR	I	데이터 세트 대기
7	RTS	I	전송 요청
8	CTS	O	전송 가능
9	RI	I	링 표시기
셸	해당 없음	해당 없음	섀시 접지

네트워크 및 IP 주소 할당

이 부록에서는 네트워크 및 IP 주소 할당에 대한 일반적인 규칙에 관해 설명하고, Cisco 어플라이언스를 네트워크에 연결하기 위한 몇 가지 전략을 제시합니다.

이더넷 인터페이스

Cisco X1070, C670 및 C370 어플라이언스에는 이더넷 인터페이스 4개가 장착되어 있으며, 구성(선택 사항인 옵티컬 네트워크 인터페이스 사용 여부)에 따라 시스템의 후면 패널에서 확인할 수 있습니다. 다음과 같은 레이블이 지정됩니다.

- Management
- Data1
- Data2
- Data3
- Data4

Cisco C170 어플라이언스에는 시스템의 후면 패널에 이더넷 인터페이스 2개가 장착되어 있습니다. 다음과 같은 레이블이 지정됩니다.

- Data1
- Data2

IP 주소 및 넷마스크 선택

네트워크를 구성하는 경우 Cisco 어플라이언스는 발송 패킷을 전송하기 위해 인터페이스를 고유한 방식으로 선택해야 합니다. 이러한 요구 사항으로 인해 이더넷 인터페이스에 대한 IP 주소 및 넷마스크를 선택할 때 영향을 받습니다. 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. 4옥텟 주소에서 상위 비트 수는 CIDR(Classless Inter-Domain Routing) 스타일로 표현되기도 합니다. 이 경우 슬래시 다음에 비트 수(1~32)가 옵니다.

넷마스크는 이진법으로 계산하여 이와 같이 표현될 수 있으므로 `255.255.255.0`은 "`/24`"가 되고 `255.255.240.0`은 "`/20`"이 됩니다.

인터페이스 구성 샘플

이 섹션에서는 일부 일반 네트워크를 기반으로 한 샘플 인터페이스 구성을 보여줍니다. 이 예에서는 Int1과 Int2라는 2개의 인터페이스를 사용합니다. Cisco 어플라이언스의 경우 이 인터페이스 이름은 3개의 Cisco 인터페이스(Management, Data1, Data2) 중 2개 인터페이스를 나타낼 수 있습니다.

네트워크 1:

각 인터페이스는 별도의 네트워크에 있는 것으로 표시되어야 합니다.

인터페이스	IP 주소	넷마스크	네트워크 주소
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`

`192.168.1.x`로 지정된 데이터(여기서 X는 사용자 고유의 주소를 제외한 1~255 숫자이며 이 경우에는 10임)는 Int1에서 전송됩니다. `192.168.0.x`로 지정된 데이터는 Int2에서 전송됩니다. 이러한 형식이 아닌 다른 주소로 지정된 패킷(대부분 WAN 또는 인터넷에서 발생)은 그 자체가 이러한 네트워크 중 하나에 있어야 하는 기본 게이트웨이로 전송됩니다. 그러면 기본 게이트웨이에서 패킷을 전달합니다.

네트워크 2:

다른 두 인터페이스의 네트워크 주소(IP 주소의 네트워크 부분)는 동일할 수 없습니다.

이더넷 인터페이스	IP 주소	넷마스크	네트워크 주소
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. Cisco 어플라이언스의 패킷이 `192.168.1.11`로 전송되는 경우 패킷을 전달에 어떤 이더넷 인터페이스를 사용해야 하는지는 결정할 수 없습니다. 두 이더넷 인터페이스가 두 개의 개별 물리적 네트워크에 연결된 경우 패킷이 잘못된 네트워크로 전달되어 대상을 찾지 못할 수 있습니다. Cisco 어플라이언스에서는 충돌이 있는 네트워크를 구성할 수 없습니다.

두 이더넷 인터페이스를 동일한 물리적 네트워크에 연결할 수 있지만 Cisco 어플라이언스에서 고유한 전송 인터페이스를 선택하도록 IP 주소 및 넷마스크를 구성해야 합니다.

IP 주소, 인터페이스 및 라우팅

인터페이스를 선택하여 GUI에서 또는 CLI에서 인터페이스를 선택할 수 있는 명령 또는 함수(예: AsyncOS 업그레이드 또는 DNS 구성 등)를 실행하는 경우 라우팅(기본 게이트웨이)이 선택한 인터페이스보다 우선합니다.

예를 들어 Cisco 어플라이언스에 다음과 같이 네트워크 인터페이스 3개가 구성되어 있으며 이는 각각 다른 네트워크 세그먼트(모두 /24라고 가정)에 있습니다.

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 인터페이스를 선택할 수 있는 다른 명령 또는 함수)를 수행하면서 data1(192.19.1.100)에 있는 IP를 선택하면 모든 TCP 트래픽은 data1 이더넷 인터페이스를 통해 발생할 것입니다. 그러나 트래픽이 기본 게이트웨이(이 경우 Management)로 설정된 인터페이스에서 전송되지만 data1의 IP 소스 주소로 스탬프가 지정됩니다.

요약

Cisco 어플라이언스는 항상 패킷이 전달되는 고유 인터페이스를 식별할 수 있어야 합니다. 이를 결정하기 위해 Cisco 어플라이언스는 패킷의 대상 IP 주소와 해당 이더넷 인터페이스의 네트워크 및 IP 주소 설정을 조합하여 사용합니다. 다음 표에는 위의 예제가 요약되어 있습니다.

	동일한 네트워크	다른 네트워크
동일한 물리적 인터페이스	허용됨	허용됨
다른 물리적 인터페이스	허용되지 않음	허용됨

Cisco 어플라이언스를 연결하기 위한 전략

Cisco 어플라이언스를 연결하는 경우 다음 사항을 확인해야 합니다.

- 관리 트래픽(CLI, 웹 인터페이스, 로그 전송)은 일반적으로 이메일 트래픽에 비해 양이 적습니다.
- 두 가지 이더넷 인터페이스를 동일한 네트워크 스위치에 연결하되 다른 호스트 다운스트림의 단일 인터페이스와 통신하게 되거나 모든 데이터가 모든 포트에 에코되는 네트워크 허브에 연결될 경우, 두 인터페이스를 사용하여 얻을 수 있는 이점은 없습니다.
- 1000Base-T로 동작하는 인터페이스를 사용하는 SMTP 대화는 100Base-T로 동작하는 같은 인터페이스를 사용하는 대화보다 약간 더 빠르지만 이는 이상적인 조건에서만 가능합니다.
- 전송 네트워크의 다른 부분에 병목 현상이 있는 경우 네트워크 연결을 최적화하는 의미가 없습니다. 병목 현상은 인터넷 연결 및 연결 공급자의 업스트림에서 가장 빈번하게 발생합니다.

연결하도록 선택하는 Cisco 어플라이언스 인터페이스 수와 인터페이스를 지정하는 방법은 기본 네트워크의 복잡성에 따라 결정됩니다. 네트워크 토폴로지 또는 데이터 볼륨에 맞지 않을 경우 여러 인터페이스를 연결할 필요가 없습니다. 처음에는 연결을 단순하게 유지하다가 게이트웨이에 익숙해지면 볼륨 및 네트워크 토폴로지에 필요한 만큼 연결을 늘릴 수도 있습니다.

메일 정책 및 콘텐츠 필터 예

수신 메일 정책 개요

다음 예에서는 다음 작업에 대한 설명을 통해 메일 정책의 기능을 보여줍니다.

1. 기본 수신 메일 정책에 대한 안티스팸, 안티바이러스, 신종 바이러스 필터(Outbreak Filter) 및 콘텐츠 필터 편집.
2. 영업 조직 및 엔지니어링 조직 등 서로 다른 사용자 집합을 위한 새로운 정책 2가지 추가한 후 각각에 대해 다른 이메일 보안 설정을 구성.
3. 수신 메일 개요 정책 테이블에 사용할 새로운 콘텐츠 필터 3가지 생성.
4. 일부 그룹(다른 그룹은 해당되지 않음)에 대한 콘텐츠 필터를 활성화하기 위해 정책 다시 편집.

이 예는 안티스팸, 안티바이러스, 신종 바이러스 필터(Outbreak Filter) 및 메일 정책용 콘텐츠 필터의 다양한 수신자 기반 설정을 관리하기 위한 권한과 유연성을 보여줍니다. 이 예에서는 메일 정책 및 콘텐츠 필터 액세스 권한이 있는 "정책 관리자"라고 하는 사용자 지정 사용자 역할을 할당합니다. 안티스팸, 안티바이러스, 신종 바이러스 필터(Outbreak Filter) 및 위임 관리 작업 방식에 대한 자세한 내용은 다음에 이어지는 장을 참조하십시오.

- 안티스팸, 13-1페이지
- 안티바이러스, 12-1페이지
- 신종 바이러스 필터(Outbreak Filter), 14-1페이지
- 관리 작업 분배, 32-1페이지

메일 정책 액세스

Mail Policies(메일 정책) 메뉴를 사용하여 수신 및 발송 메일 정책에 액세스할 수 있습니다.

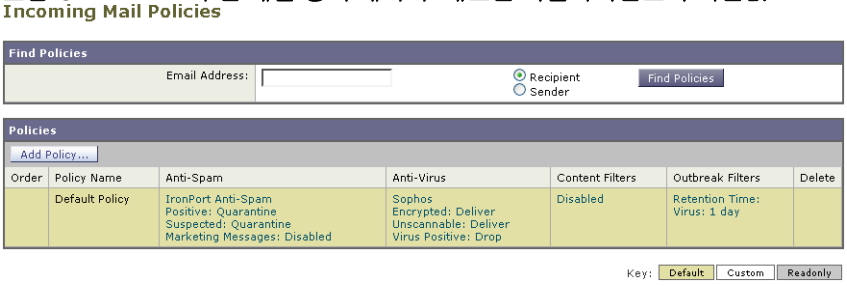
새로운 시스템에서 시스템 설치 마법사의 모든 단계를 완료하고 안티스팸, Sophos 또는 McAfee 안티바이러스, 신종 바이러스 필터(Outbreak Filter)를 활성화하도록 선택한 경우, Incoming Mail Policies(수신 메일 정책) 페이지가 그림 C-1과 같이 구성할 수 있습니다.

기본적으로 이러한 설정은 기본 수신 메일 정책에서 활성화됩니다.

- 안티스팸(스팸 격리가 활성화된 상태): 활성화됨
  - 스팸으로 확인된 스팸: 격리, 메시지 제목 앞에 추가
  - 의심스러운 스팸: 격리, 메시지 제목 앞에 추가
  - 마케팅 이메일: 검사가 활성화되지 않음

- 안티스팸(스팸 격리가 활성화되지 않은 상태): 활성화됨
  - 스팸으로 확인된 스팸: 전달, 메시지 제목 앞에 추가
  - 의심스러운 스팸: 전달, 메시지 제목 앞에 추가
  - 마케팅 이메일: 검사가 활성화되지 않음
- 안티바이러스: 활성화됨, 바이러스 검사 후 복구, 안티바이러스 검사 결과를 포함하는 X-헤더 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
- 신종 바이러스 필터(Outbreak Filter): 활성화됨
  - 파일 확장명이 제외되지 않음
  - 바이러스에 감염이 의심되는 첨부 파일이 있는 메시지의 보존 기간: 1일
  - 메시지 수정이 활성화되지 않음
- 콘텐츠 필터: 비활성화됨

그림 C-1 수신 메일 정책 페이지: 새로운 어플라이언스의 기본값



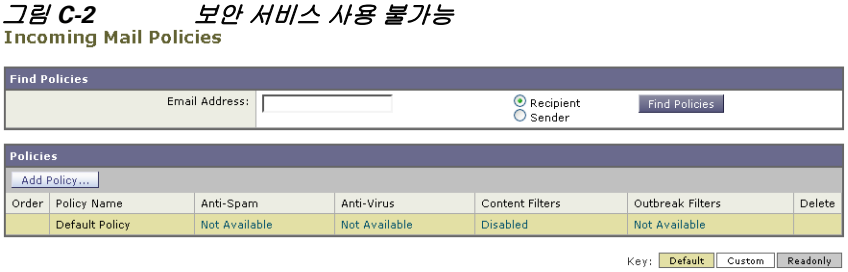
참고 이 예에서 수신 메일 정책은 스팸 격리가 활성화된 경우 기본 안티스팸 설정을 사용합니다.

활성화됨, 비활성화됨 및 "사용 불가능"

메일 정책 테이블(수신 또는 발송)의 열은 정책의 이름마다 보안 서비스 상태에 대한 링크를 표시합니다. 서비스가 활성화된 경우, "활성화됨" 또는 구성 요약이 표시됩니다. 마찬가지로, 서비스가 비활성화된 경우 "비활성화됨"이 표시됩니다.

서비스에 대한 라이센스 계약이 아직 수락되지 않았거나 서비스가 만료된 경우 "사용 불가능"이 링크로 표시됩니다. "사용 불가능" 링크를 클릭하면 서비스에 대한 정책별 설정을 구성할 수 있는 페이지 대신 Security Services(보안 서비스) 탭에 있는 전역 페이지가 표시됩니다. 페이지가 다른 탭으로 변경되었음을 알려주는 알림 메시지가 표시됩니다. 그림 C-2를 참조하십시오.

그림 C-2 보안 서비스 사용 불가능



수신 메시지에 대한 기본 안티스팸 정책 구성

메일 정책 테이블의 각 행은 다른 정책을 나타냅니다. 각 열은 다른 보안 서비스를 나타냅니다.

- 기본 정책을 수정하려면 수신 또는 발송 메일 정책 테이블의 가장 아래 행에서 보안 서비스 링크를 클릭합니다.

이 예에서 수신 메일 기본 정책의 안티스팸 설정을 더 적극적으로 변경할 수 있습니다. 기본값은 마케팅 이메일 검사가 비활성화된 경우 스팸으로 확인된 스팸과 의심스러운 스팸 메시지를 격리하는 것입니다. 이 예는 스팸으로 확인된 스팸을 삭제하도록 설정을 변경하는 방법을 보여줍니다. 의심스러운 스팸은 계속 격리됩니다. 마케팅 이메일 검사는 마케팅 메시지가 원하는 수신자에게 전송된 상태에서 활성화됩니다. 마케팅 메시지 제목 앞에는 [마케팅] 텍스트가 추가됩니다.

절차

1단계 안티스팸 보안 서비스에 대한 링크를 클릭합니다.

참고 기본 보안 서비스 설정과 관련하여 페이지의 첫 번째 설정에서는 정책에 대해 서비스를 활성화할지 여부를 정의합니다. 서비스를 모두 비활성화하려면 "Disable(비활성화)"을 클릭합니다.

2단계 "Positively Identified Spam Settings(스팸으로 확인된 스팸 설정)" 섹션에서 "Action to apply to this message(메시지에 적용할 작업)"를 Drop(삭제)으로 변경합니다.

3단계 "Marketing Email Settings(마케팅 이메일 설정)" 섹션에서 마케팅 이메일 검사를 활성화하려면 **Yes(예)**를 클릭합니다.

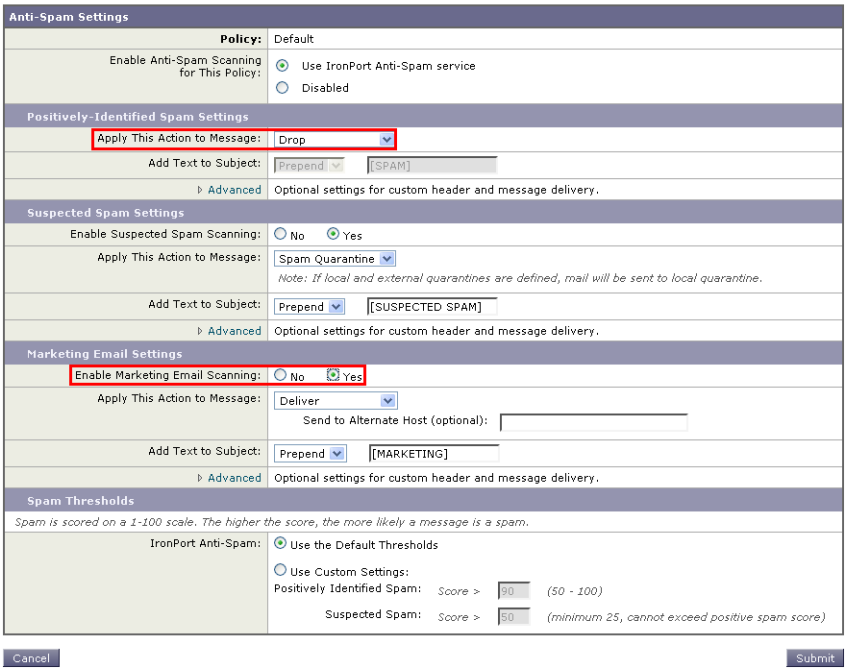
이 검사를 활성화한 경우, 기본 작업은 제목 앞에 [마케팅] 텍스트를 추가하여 정상적인 마케팅 메시지를 전송하는 것입니다.

"Add text to message(메시지에 텍스트 추가)" 필드에서만 US-ASCII 문자를 사용할 수 있습니다.

4단계 **Submit(제출)**을 클릭합니다. 수신 메일 정책 테이블의 안티스팸 보안 서비스에 대한 요약 링크가 새 값을 반영하도록 변경되었습니다.

위의 단계와 유사한 방식으로 기본 정책의 기본 안티바이러스 및 신종 바이러스 필터(Outbreak Filter) 설정을 변경할 수 있습니다.

그림 C-3 안티스팸 설정 페이지



발신자 및 수신자 그룹에 대한 메일 정책 생성

이 예에서는 새로운 정책 2가지를 생성할 수 있습니다. 한 가지는 영업 조직(멤버가 LDAP 수락 쿼리에서 정의됨)에 대한 정책이며 다른 하나는 엔지니어링 조직에 대한 정책입니다. 두 가지 정책에 사용자 지정 사용자 역할인 정책 관리자를 할당하여 위임 관리자가 이러한 정책을 담당하는 해당 역할에 속하도록 합니다. 그런 다음 각각에 대해 다른 이메일 보안 설정을 구성합니다.

절차

1단계 **Add Policy(정책 추가)** 버튼을 클릭하여 새로운 정책 생성을 시작합니다.

2단계 고유한 이름을 정의하고 정책 순서를 조정합니다(필요한 경우).

정책 이름은 정책이 정의된 메일 정책 테이블에서 고유한 이름이어야 합니다(수신 또는 발신 모두 해당됨).

각 수신자는 하향식으로 적절한 테이블(수신 또는 발송)의 각 정책에 대해 평가됩니다.

3단계 Editable By (Roles)(편집 가능한 사용자(역할)) 링크를 클릭하고 메일 정책 관리를 담당할 위임 관리자에 대한 사용자 지정 사용자 역할을 선택합니다.

링크를 클릭하면 AsyncOS는 메일 정책에 대한 편집 권한이 있는 위임 관리자의 사용자 지정 역할을 표시합니다. 위임 관리자는 정책의 안티스팸, 안티바이러스 및 신종 바이러스 필터(Outbreak Filter) 설정을 편집하고 정책의 콘텐츠 필터를 활성화 또는 비활성화할 수 있습니다. 운영자와 관리자만 메일 정책의 이름 또는 메일 정책의 발신자, 수신자 또는 그룹을 수정할 수 있습니다. 메일 정책에 대한 전체 액세스 권한이 있는 사용자 지정 사용자 역할이 메일 정책에 자동으로 할당됩니다.

위임 관리자에 대한 자세한 내용은 관리 작업 분배 항목을 참조하십시오.

4단계 정책에 대해 사용자를 정의합니다.

사용자가 발신자 또는 수신자인지를 정의합니다. 자세한 내용은 정책 일치의 예, 10-4페이지 항목을 참조하십시오. 그림 C-4의 양식은 수신 메일 정책의 수신자와 발송 메일 정책의 발신자에 대한 기본값입니다.

해당 정책에 대한 사용자는 다음 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 쿼리와 일치

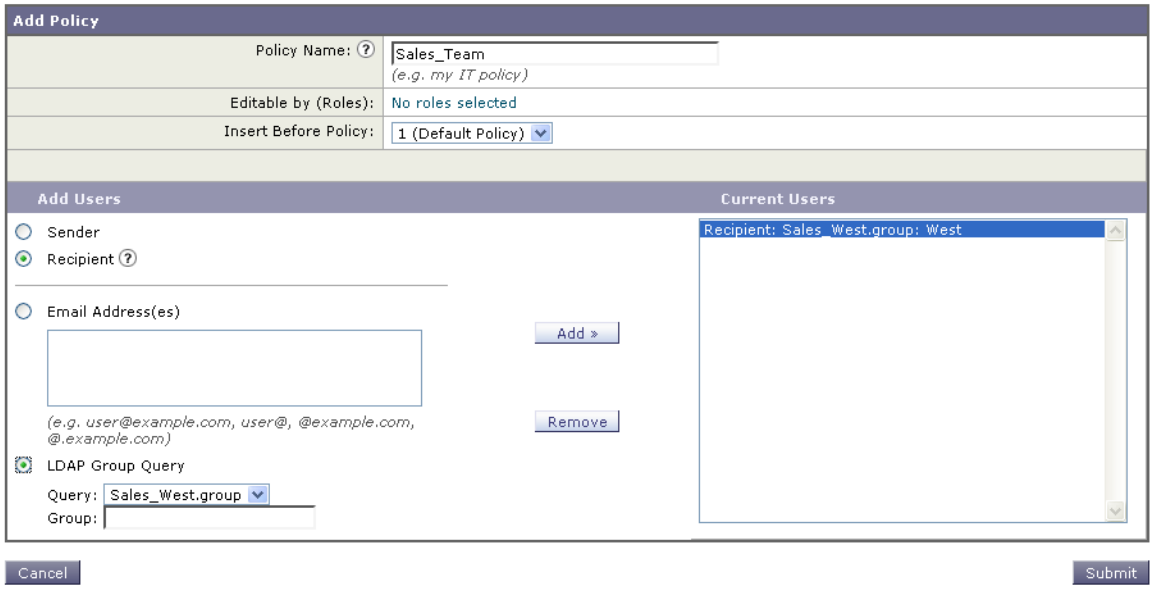
참고 사용자 항목은 AsyncOS의 GUI 및 CLI에서 모두 대소문자를 구분하지 않습니다. 예를 들어, 사용자에 수신자 `Joe@`를 입력한 경우 `joe@example.com`으로 전송된 메시지와 일치합니다.

네트워크 인프라에서 LDAP 디렉토리(예: Microsoft Active Directory, SunONE Directory Server(이전 명칭 "iPlanet Directory Server") 또는 Open LDAP 디렉토리) 내부에 사용자 정보를 저장하는 경우, LDAP 서버에 쿼리하도록 어플라이언스를 구성하여 수신자 주소를 수락하고 메시지를 대체 주소 및/또는 메일 호스트에 다시 라우팅하고, 헤더를 마스커레이드하며 메시지에 특정 그룹의 발신자 또는 수신자가 있는지 확인할 수 있습니다.

LDAP 서버에 쿼리하도록 어플라이언스를 구성한 경우, 구성한 쿼리를 사용하여 메일 정책에 대해 사용자를 정의할 수 있습니다.

자세한 내용은 LDAP 쿼리 항목을 참조하십시오.

그림 C-4 정책에 대한 사용자 정의



5단계 **Add(추가)** 버튼을 클릭하여 현재 사용자 목록에 사용자를 추가합니다.

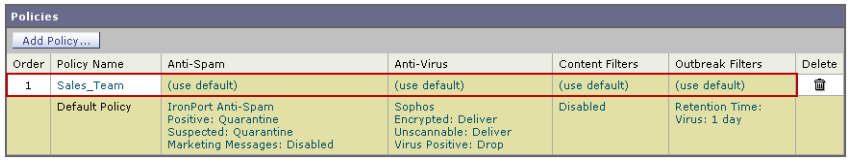
정책에는 발신자, 수신자 및 LDAP 쿼리가 결합되어 포함됩니다.

Remove(제거) 버튼을 사용하여 현재 사용자 목록에서 정의된 사용자를 제거합니다.

6단계 사용자 추가를 완료하면 **Submit(제출)**을 클릭합니다.

처음으로 정책을 추가하는 경우 기본값을 사용하도록 모든 보안 서비스 설정이 설정됩니다.

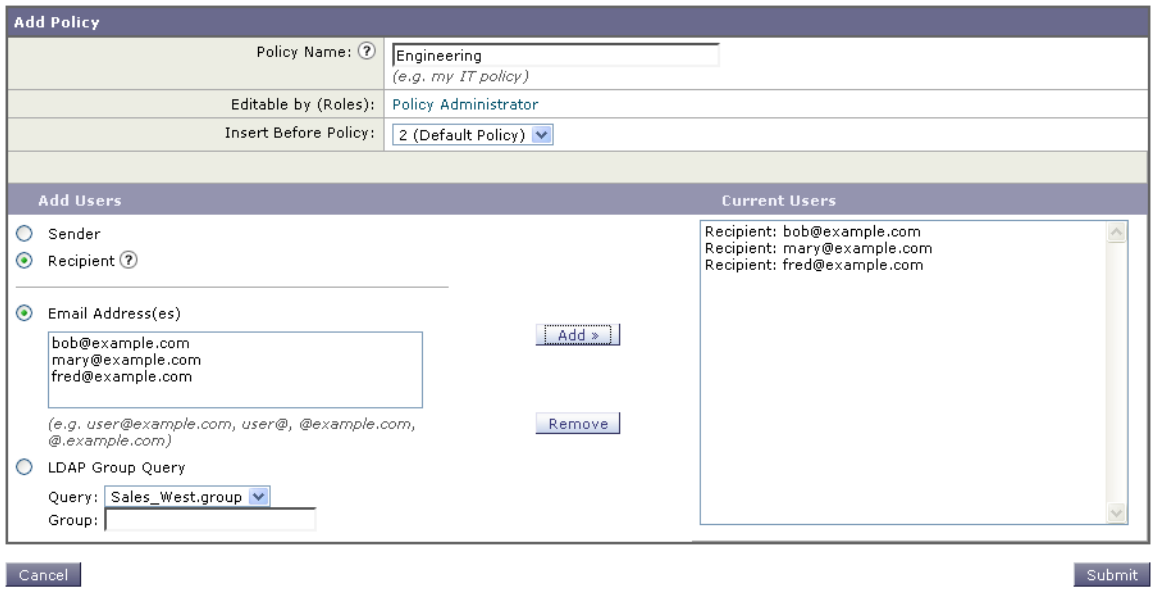
그림 C-5 새로 추가된 정책 — 영업 그룹



7단계 **Add Policy(정책 추가)** 버튼을 다시 클릭하여 다른 새로운 정책을 추가합니다.

이 정책에서 엔지니어링팀 멤버의 개별 이메일 주소가 다음과 같이 정의됩니다.

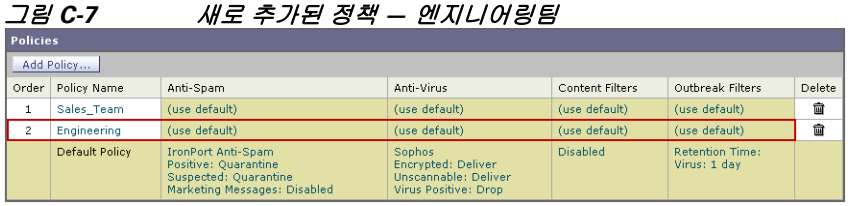
그림 C-6 엔지니어링팀을 위한 정책 생성



8단계 엔지니어링 정책에 대한 사용자 추가를 완료하면 **Submit(제출)**을 클릭합니다.

9단계 변경사항을 커밋합니다.

그림 C-7 새로 추가된 정책 — 엔지니어링팀



참고 이때 새로 생성된 2가지 정책에는 기본 정책에 적용된 것과 동일한 설정이 적용되어 있습니다. 한 가지 정책의 사용자에 대한 메시지는 일치하지만 메일 처리 설정은 기본 정책과 다르지 않습니다. 따라서, "Sales_Group" 또는 "Engineering" 정책의 사용자와 일치하는 메시지는 기본 정책과 동일하게 처리됩니다.

기본값, 사용자 지정 및 비활성화됨

테이블의 가장 아래에 있는 키는 특정 정책에 대한 셀의 색상 코딩이 기본 행에 정의된 정책과 어떤 관련이 있는지 보여줍니다.

Key: Default Custom Disabled

- 노란색 음영은 정책이 기본 정책과 동일한 설정을 사용하고 있음을 보여줍니다.
- 음영이 없는 부분(흰색)은 정책이 기본 정책과 다른 설정을 사용하고 있음을 보여줍니다.
- 회색 음영은 정책의 보안 서비스가 비활성화되어 있음을 보여줍니다.

다양한 그룹의 발신자 및 수신자에 대한 메일 정책 생성

이 예에서는 이전 섹션에서 생성한 정책 2가지를 편집합니다.

- 영업 그룹에 대해서는 안티스팸 설정을 기본 정책보다 더 적극적으로 변경합니다. (수신 메시지에 대한 기본 안티스팸 정책 구성, C-3페이지 참조.) 스팸으로 확인된 스팸 메시지 삭제에 대한 기본 정책이 그대로 적용됩니다. 그러나 이 예에서는 마케팅 메시지를 스팸 격리에 전송하기 위해 마케팅 메시지의 설정을 변경합니다.

  이러한 적극적인 정책은 영업팀의 받은 편지함에 원치 않는 메시지가 전송되는 것을 최소화합니다.

  안티스팸 설정에 대한 자세한 내용은 안티스팸, 13-1페이지 항목을 참조하십시오.
- 엔지니어링팀에 대해서는 의심스러운 메시지의 URL을 수정하도록(example.com 링크 제외) 신종 바이러스 필터(Outbreak Filter) 기능 설정을 사용자 지정합니다. 확장명 "dwg"가 있는 첨부 파일은 신종 바이러스 필터(Outbreak Filter) 검사를 통해 우회됩니다.

  신종 바이러스 필터(Outbreak Filter) 구성에 대한 자세한 내용은 신종 바이러스 필터(Outbreak Filter), 14-1페이지 항목을 참조하십시오.

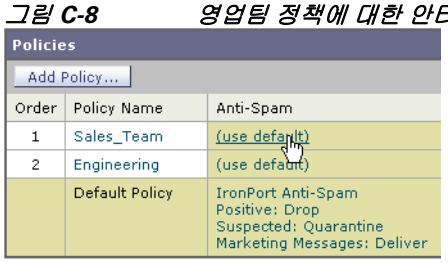
영업팀 정책에 대한 안티스팸 설정을 편집하려면 다음을 수행합니다.

절차

1단계 영업 정책 행에서 안티스팸 보안 서비스(안티스팸) 열의 링크를 클릭합니다.

정책을 방금 추가했으므로 링크 이름은 `(use default)`입니다.

그림 C-8 영업팀 정책에 대한 안티스팸 설정 수정



2단계 Anti-spam(안티스팸) 보안 서비스 페이지에서 "Enable Anti-Spam Scanning for this Policy(이 정책에 대한 안티스팸 검사 사용)"의 값을 "Use Default Settings(기본 설정 사용)"에서 "Use Anti-Spam service(안티스팸 서비스 사용)"로 변경합니다.

여기에서 "Use Anti-Spam service(안티스팸 서비스 사용)"를 선택하면 기본 정책에 정의된 설정을 재정의할 수 있습니다.

3단계 "Positively-Identified Spam Settings(스팸으로 확인된 스팸 설정)" 섹션에서 "Apply This Action to Message(메시지에 다음 작업 적용)"를 Drop(삭제)으로 변경합니다.

4단계 "Suspected Spam Settings(의심스러운 스팸 설정)" 섹션에서 의심스러운 스팸 검사를 활성화하려면 **Yes(예)**를 클릭합니다.

5단계 "Suspected Spam Settings(의심스러운 스팸 설정)" 섹션에서 "Apply This Action to Message(메시지에 다음 작업 적용)"를 "Spam Quarantine(스팸 격리)"으로 변경합니다.

참고 스팸 격리를 선택하면 스팸 격리 장에 정의된 설정에 따라 메일이 전달됩니다.

6단계 "Add text to subject(제목에 텍스트 추가)" 필드에서 **None(없음)**을 클릭합니다.

스팸 격리에 전달된 메시지에 추가로 제목 태그가 지정되지 않습니다.

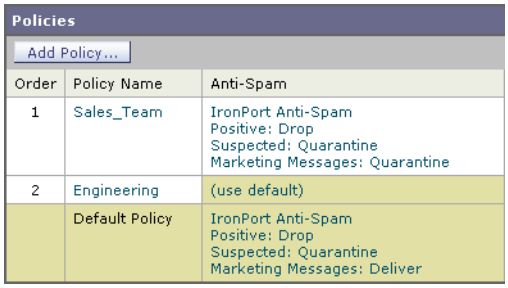
7단계 "Marketing Email Settings(마케팅 이메일 설정)" 섹션에서 정상적인 출처에서 보낸 마케팅 메일 검사를 활성화하려면 **Yes(예)**를 클릭합니다.

8단계 "Apply This Action to Message(메시지에 다음 작업 적용)" 섹션에서 "Spam Quarantine(스팸 격리)"을 선택합니다.

9단계 변경사항을 제출하고 커밋합니다.

음영은 정책이 기본 정책과 다른 설정을 사용하고 있음을 보여줍니다.

그림 C-9 변경된 영업 그룹 정책에 대한 안티스팸 설정



이제 의심스러운 스팸에 해당하며 수신자가 영업팀 정책에 정의된 LDAP 쿼리와 일치하는 메시지는 스팸 격리로 전달됩니다.

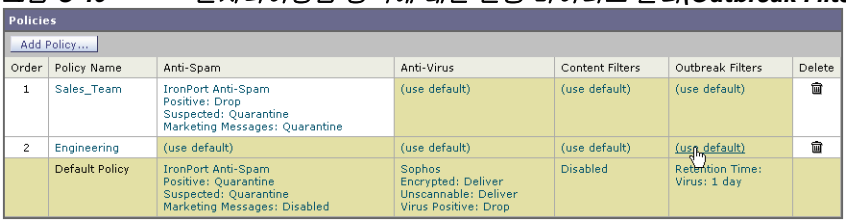
엔지니어링팀 정책에 대한 신종 바이러스 필터(Outbreak Filter) 설정을 편집하려면 다음을 수행합니다.

절차

1단계 엔지니어링 정책 행에서 신종 바이러스 필터(Outbreak Filter) 기능 보안 서비스(신종 바이러스 필터(Outbreak Filter) 열)의 링크를 클릭합니다.

정책을 방금 추가했으므로 링크 이름은 `(use default)`입니다.

그림 C-10 엔지니어링팀 정책에 대한 신종 바이러스 필터(Outbreak Filter) 기능 설정 수정



2단계 Outbreak Filters(신종 바이러스 필터(Outbreak Filter)) 보안 서비스 페이지에서 정책에 대한 검사 설정을 "Enable Outbreak Filtering(Customize settings)(신종 바이러스 필터(Outbreak Filter)링 활성화(사용자 지정 설정))"으로 변경합니다.

여기에서 "(Customize settings)((사용자 지정 설정))"를 선택하면 기본 정책에 정의된 설정을 재정의할 수 있습니다.

이렇게 하면 페이지의 나머지 콘텐츠에서 다른 설정을 선택하도록 설정할 수 있습니다.

3단계 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 3자로 된 파일 이름 확장명 앞에 마침표(.)를 입력할 필요가 없습니다.

4단계 **Add Extension(확장명 추가)**을 클릭하여 `.dwg` 파일을 신종 바이러스 필터(Outbreak Filter) 기능 검사를 우회하는 파일 확장명 목록에 추가합니다.

5단계 **Enable Message Modification(메시지 수정 사용)**을 클릭합니다.

메시지 수정을 사용하면 어플라이언스가 목표 위협(예: 피싱 및 스캠)과 의심스럽거나 악의적인 웹 사이트에 대한 URL을 검사할 수 있습니다. 어플라이언스는 메시지의 링크를 다시 작성하여 이 링크에서 웹 사이트에 액세스하려고 시도하는 경우 Cisco 보안 프록시를 통해 사용자를 리디렉션할 수 있습니다.

참고 신종 바이러스 필터(Outbreak Filter)가 바이러스가 아닌 목표 위협을 검사하도록 메일 정책의 안티스팸 검사가 활성화되어야 합니다.

6단계 **Enable for Unsigned Messages(서명되지 않은 메시지에 대해 사용)**를 선택합니다.

이렇게 하면 어플라이언스가 서명된 메시지의 URL을 다시 작성할 수 있습니다. 기타 메시지 수정 설정을 구성하고 메시지가 해제되기 전에 바이러스가 아닌 위협으로 판정될 때까지 격리에서 머문 시간을 구성하려면 URL 재작성 기능을 사용해야 합니다. 이 예에서는 기본값 4시간을 사용합니다.

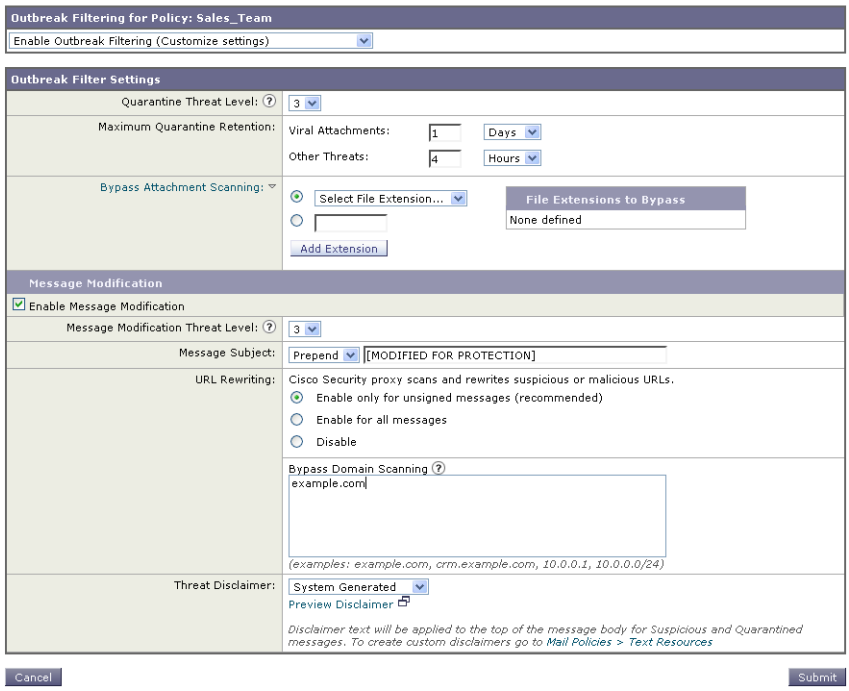
7단계 **Bypass Domain Scanning(도메인 검사 우회)** 필드에 example.com을 입력합니다.

어플라이언스는 example.com에 대한 링크를 수정하지 않습니다.

8단계 **Threat Disclaimer(위협 책임 부인 공지)**에 대한 System Generated(생성된 시스템)를 선택합니다.

어플라이언스는 사용자에게 메시지 콘텐츠에 대해 경고하기 위해 메시지 본문 위에 책임 부인 공지를 삽입할 수 있습니다. 이 예에서는 시스템에서 생성한 위협 책임 부인 공지를 사용합니다.

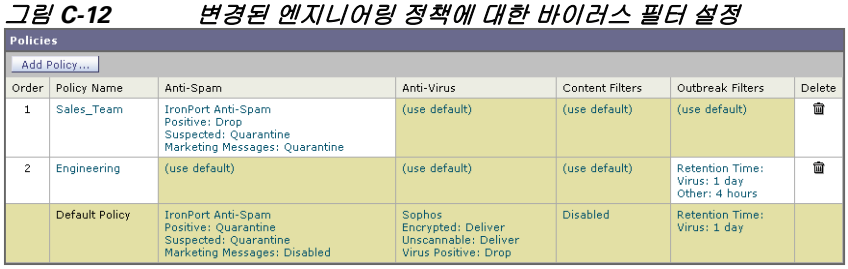
그림 C-11 신종 바이러스 필터(Outbreak Filter) 설정



9단계 변경사항을 제출하고 커밋합니다.

음영은 정책이 기본 정책과 다른 설정을 사용하고 있음을 보여줍니다.

그림 C-12 변경된 엔지니어링 정책에 대한 바이러스 필터 설정



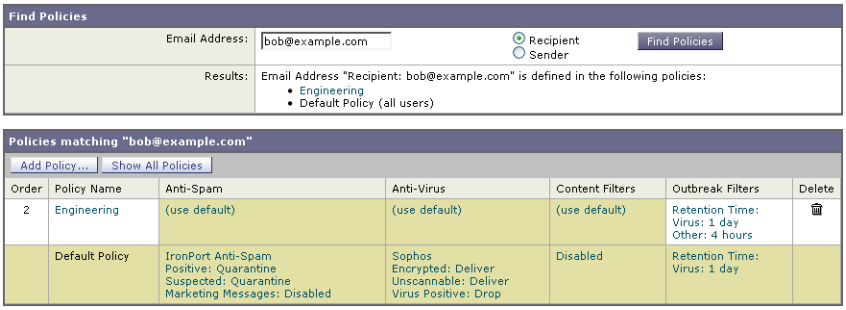
이때 파일 확장명이 `dwg`이고 수신자가 엔지니어링팀 정책에 정의된 수신자와 일치하는 첨부 파일을 포함하는 모든 메시지는 신종 바이러스 필터(Outbreak Filter) 검사를 우회하고 처리를 계속합니다. example.com 도메인에 대한 링크를 포함하는 메시지는 Cisco 보안 프록시를 통해 리디렉션하기 위해 링크를 수정하지 않으며 의심스러운 링크로 간주되지 않습니다.

메일 정책에서 발신자 또는 수신자 찾기

"Find Policies(정책 찾기)" 버튼을 사용하여 Incoming or Outgoing Mail Policies(수신 또는 발송 메일 정책) 페이지에 정의되어 있는 정책에 이미 정의된 사용자를 검색합니다.

예를 들어, `joe@example.com`을 입력하고 Find Policies(정책 찾기) 버튼을 클릭하면 정의된 사용자를 포함하는 정책과 일치하는 정책이 표시됩니다.

그림 C-13 정책에서 사용자 찾기



해당 정책에 대한 사용자를 편집하려면 정책 이름을 클릭하여 Edit Policy(정책 편집) 페이지로 이동합니다.

발신자 또는 수신자가 기타 모든 구성된 정책과 일치하지 않는 경우 이러한 정책은 기본 정책과 *항상* 일치하기 때문에 사용자를 검색할 때 기본 정책이 항상 표시됩니다.

예외 관리

위의 2가지 예에서 살펴본 단계를 수행하여 *예외 관리* 기준으로 정책 생성 및 구성을 시작할 수 있습니다. 즉 조직의 요구 사항을 평가한 후 메시지 대부분을 기본 정책으로 처리할 수 있도록 정책을 구성할 수 있습니다. 그런 다음 필요 시 다른 정책을 관리하도록 특정 사용자 또는 사용자 그룹을 대상으로 추가 "예외" 정책을 생성할 수 있습니다. 이러한 방식에서 메시지 분리가 최소화되고 작업 큐에서 각 분리 메시지를 처리할 때 시스템 성능에 영향을 거의 미치지 않습니다.

스팸, 바이러스 및 정책 적용을 위한 조직 또는 사용자의 허용 범위를 기준으로 정책을 정의할 수 있습니다. 표 C-1(C-11페이지)에 여러 정책의 예가 설명되어 있습니다. "적극적인" 정책은 최종 사용자 메일함에 도착하는 스팸과 바이러스의 양을 최소화하기 위해 설계되었습니다. "보수적인" 정책은 긍정 오류를 방지하고 정책과 관계없이 누락된 메시지가 없도록 맞춤화되었습니다.

표 C-1 적극적, 보수적 메일 정책 설정

	적극적인 설정	보수적인 설정
안티스팸	스팸으로 확인된 스팸: 삭제 의심스러운 스팸: 격리 마케팅 메일: 전달 및 제목 메시지 앞에 "[마케팅]" 추가	스팸으로 확인된 스팸: 격리 의심스러운 스팸: 전달 및 메시지 제목 앞에 "[의심스러운 스팸]" 추가 마케팅 메일: 비활성화됨

표 C-1 적극적, 보수적 메일 정책 설정 (계속)

안티바이러스	복구된 메시지: 전달 암호화된 메시지: 삭제 검사할 수 없는 메시지: 삭제 감염된 메시지: 삭제	복구된 메시지: 전달 암호화된 메시지: 격리 검사할 수 없는 메시지: 격리 감염된 메시지: 삭제
바이러스 필터	활성화됨, 특정한 파일 이름 확장명 또는 도메인의 우회가 허용되지 않음 모든 메시지의 메시지 수정 활성화	활성화됨, 특정한 파일 이름 확장명 또는 도메인의 우회가 허용됨 서명되지 않은 메시지에 대한 메시지 수정 활성화

콘텐츠 기준 메시지 필터링

이 예에서는 수신 메일 정책 테이블에서 사용할 새로운 콘텐츠 필터 3가지를 생성합니다. 이러한 콘텐츠 필터는 모두 사용자 지정 사용자 역할인 정책 관리에 속하는 위임 관리자가 편집할 수 있습니다. 다음을 생성합니다.

1. "scan_for_confidential"

   이 필터는 문자열 "confidential"이 있는지 메시지를 검사합니다. 이 문자열이 발견되면 메시지 복사본이 이메일 별칭 `hr@example.com`에 전송되며 메시지는 정책 격리 영역에 전송됩니다.

2. "no_mp3s"

   이 필터는 MP3 첨부 파일을 제거하며 수신자에게 MP3 파일이 제거되었음을 알립니다.

3. "ex_employee"

   이 콘텐츠 필터는 특정한 봉투 수신자 주소(이전 직원)에 전송된 메시지를 검사합니다. 메시지가 일치하면 메시지 발신자에게 특정한 알림 메시지가 전송된 다음 메시지가 바운스됩니다.

콘텐츠 필터를 생성한 후, 각각의 정책을 구성하여 다양한 조합으로 구성된 특정 콘텐츠 필터를 활성화합니다.

제목에 "기밀"이 포함된 메시지 격리

첫 번째 예의 콘텐츠 필터에는 조건 1개와 작업 2개가 있습니다.

절차

1단계 Mail Policies(메일 정책) 탭을 클릭합니다.

2단계 Incoming Content Filters(수신 콘텐츠 필터)를 클릭합니다.

3단계 **Add Filter(필터 추가)** 버튼을 클릭합니다.

4단계 Name(이름) 필드에 새로운 필터 이름으로 `scan_for_confidential`을 입력합니다.

필터 이름에는 ASCII 문자, 숫자, 밑줄 또는 대시가 포함될 수 있습니다. 콘텐츠 필터 이름의 첫 번째 문자는 숫자 또는 밑줄이어야 합니다.

5단계 **Editable By(Roles)(편집 가능(역할))** 링크를 클릭하고 Policy Administrator(정책 관리자)를 선택한 다음 **OK(확인)**를 클릭합니다.

정책 관리자 사용자 역할에 속하는 위임 관리자는 이 콘텐츠 필터를 편집하고 메일 정책에 사용할 수 있습니다.

6단계 Description(설명) 필드에 설명을 입력합니다. 예: `scan all incoming mail for the string 'confidential'.`

7단계 **Add Condition(조건 추가)**을 클릭합니다.

8단계 메시지 본문을 선택합니다.

9단계 Contains text:(텍스트 포함:) 필드에 `confidential`을 입력하고 **OK(확인)**를 클릭합니다.

Add Content Filter(콘텐츠 필터 추가) 페이지에 추가된 조건이 표시됩니다.

10단계 **Add Action(작업 추가)**을 클릭합니다.

11단계 복사본 전달(Bcc:)을 선택합니다.

12단계 Email Addresses(이메일 주소) 필드에 `hr@example.com`을 입력합니다.

13단계 Subject(제목) 필드에 `[message matched confidential filter]`를 입력합니다.

14단계 **OK(확인)를** 클릭합니다.

Add Content Filter(콘텐츠 필터 추가) 페이지에 추가된 작업이 표시됩니다.

15단계 **Add Action(작업 추가)**을 클릭합니다.

16단계 격리를 선택합니다.

17단계 드롭다운 메뉴에서 정책 격리 영역을 선택합니다.

18단계 **OK(확인)**를 클릭합니다.

Add Content Filter(콘텐츠 필터 추가) 페이지에 추가된 두 번째 작업이 표시됩니다.

19단계 변경사항을 제출하고 커밋합니다.

이때 콘텐츠 필터는 수신 메일 정책에 대해 활성화되지 않습니다. 이 예에서는 마스터 목록에만 새 콘텐츠 필터를 추가합니다. 이 필터를 모든 정책에 적용하지는 않았기 때문에 어플라이언스에서 수행하는 이메일 처리는 이 필터의 영향을 받지 않습니다.

메시지에서 MP3 첨부 파일 제거

두 번째 예의 콘텐츠 필터에는 조건은 없으며 작업 1개가 있습니다.

절차

1단계 **Add Filter(필터 추가)** 버튼을 클릭합니다.

2단계 Name(이름) 필드에 새로운 필터 이름으로 `no_mp3s`를 입력합니다.

3단계 **Editable By(Roles)(편집 가능(역할))** 링크를 클릭하고 Policy Administrator(정책 관리자)를 선택한 다음 **OK(확인)**를 클릭합니다.

4단계 Description(설명) 필드에 설명을 입력합니다. 예: `strip all MP3 attachments.`

5단계 **Add Action(작업 추가)**을 클릭합니다.

6단계 파일 정보별 첨부 파일 제거를 선택합니다.

7단계 `File type is`를 선택합니다.

8단계 드롭다운 필드에서 `-- mp3`를 선택합니다.

9단계 필요한 경우 대체 메시지를 입력합니다.

10단계 **OK(확인)**를 클릭합니다.

11단계 변경사항을 제출하고 커밋합니다.

참고 콘텐츠 필터를 생성하는 경우 조건을 지정할 필요가 없습니다. 조건을 정의하지 않은 경우 정의된 작업이 항상 규칙에 적용됩니다. (조건을 지정하지 않는 것은 `true()` 메시지 필터 규칙을 사용하는 것과 같습니다. 콘텐츠 필터가 정책에 적용되는 경우 모든 메시지가 일치됩니다.)

이전 직원에게 전송된 메시지 바운스

세 번째 예의 콘텐츠 필터에는 조건 1개와 작업 2개가 있습니다.

절차

1단계 **Add Filter(필터 추가)** 버튼을 클릭합니다.

2단계 Name:(이름:) 필드에 새로운 필터 이름으로 `ex_employee`를 입력합니다.

3단계 **Editable By(Roles)(편집 가능(역할))** 링크를 클릭하고 Policy Administrator(정책 관리자)를 선택한 다음 **OK(확인)**를 클릭합니다.

4단계 Description:(설명:) 필드에 설명을 입력합니다. 예: `bounce messages intended for Doug.`

5단계 **Add Condition(조건 추가)**을 클릭합니다.

6단계 봉투 수신자를 선택합니다.

7단계 봉투 수신자의 경우 `Begins with`를 선택하고 `doug@`를 입력합니다.

8단계 **OK(확인)**를 클릭합니다.

Content Filters(콘텐츠 필터) 페이지가 새로 고침 되고 추가된 조건이 표시됩니다. 이전 직원의 이메일 주소를 포함하는 LDAP 디렉토리를 생성할 수 있습니다. 이전 직원이 해당 디렉토리에 추가되었으므로 이 콘텐츠 필터가 동적으로 업데이트됩니다.

9단계 **Add Action(작업 추가)**을 클릭합니다.

10단계 알림을 선택합니다.

11단계 발신자 확인란을 선택하고 Subject(제목) 필드에 `message bounced for ex-employee of example.com`을 입력합니다.

12단계 Use template(템플릿 사용) 섹션에서 알림 템플릿을 선택합니다.

참고 리소스가 사전 구성되지 않은 경우 콘텐츠 필터 규칙 빌더의 일부 섹션은 사용자 인터페이스에 나타나지 않습니다. 예를 들어 콘텐츠 사전, 알림 템플릿 및 메시지 책임 부인 공지는 Mail Policies(메일 정책) > Dictionaries(사전) 페이지(또는 CLI에서 `dictionaryconfig` 명령)에서 사전에 구성하지 않은 경우 옵션으로 나타나지 않습니다. 사전 생성에 대한 자세한 내용은 콘텐츠 사전, 21-2페이지 항목을 참조하십시오.

13단계 **OK(확인)**를 클릭합니다.

Add Content Filter(콘텐츠 필터 추가) 페이지에 추가된 작업이 표시됩니다.

14단계 **Add Action(작업 추가)**을 클릭합니다.

15단계 바운스(최종 작업)를 선택하고 **OK(확인)**를 클릭합니다.

콘텐츠 필터에 하나의 최종 작업만 지정할 수 있습니다. 최종 작업 1개 이상을 추가하려고 시도하는 경우, GUI에 오류가 표시됩니다.

이 작업을 추가하면 이전 직원에게 전송하는 메시지의 발신자가 잠재적으로 메시지 2개를 수신하게 됩니다. 하나는 알림 템플릿이고 나머지 하나는 바운스 알림 템플릿입니다.

16단계 변경사항을 제출하고 커밋합니다.

다양한 수신자 그룹에게 게별 콘텐츠 필터 적용

위의 예에서는 Incoming Content Filters(수신 콘텐츠 필터) 페이지를 사용하여 콘텐츠 필터 3개를 생성했습니다. Incoming Content Filters(수신 콘텐츠 필터) 및 Outgoing Content filters(발송 콘텐츠 필터) 페이지는 정책에 적용될 수 있는 모든 콘텐츠 필터의 "마스터 목록"을 보관합니다.

그림 C-14 수신 콘텐츠 필터: 필터 3개가 생성됨

Incoming Content Filters

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	scan_for_confidential	scan all incoming mail for the string 'confidential'		
2	no_mp3s	strip all MP3 attachments		
3	ex_employee	bounce messages intended for Doug		

이 예에서는 수신 메일 정책 테이블에서 사용할 새로운 콘텐츠 필터 3가지를 적용할 수 있습니다.

- 기본 정책은 콘텐츠 필터 3개를 모두 수신합니다.
- 엔지니어링 그룹은 no_mp3s 필터를 수신하지 *않습니다*.
- 영업 그룹은 기본 수신 메일 정책으로 콘텐츠 필터를 수신합니다.

기본적으로 모든 수신자에 대해 콘텐츠 필터 활성화

링크를 클릭하여 개별 정책마다 콘텐츠 필터를 활성화하고 선택합니다.

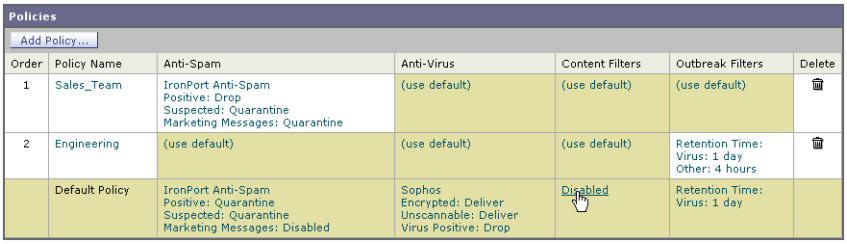
절차

1단계 수신 메일 정책을 클릭하여 수신 메일 정책 테이블로 돌아갑니다.

이 페이지가 새로 고침 되고 기본 정책과 발신자 및 수신자 그룹에 대한 메일 정책 생성, C-4페이지에서 추가한 정책 2개가 표시됩니다. 콘텐츠 필터는 기본적으로 모든 정책에 대해 비활성화되어 있습니다.

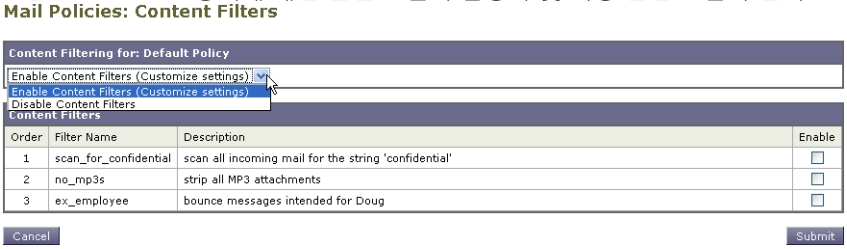
2단계 기본 정책 행에서 콘텐츠 필터 보안 서비스(콘텐츠 필터 열)의 링크를 클릭합니다. 그림 C-15를 참조하십시오.

그림 C-15 기본 수신 메일 정책에 대한 콘텐츠 필터 설정 편집



3단계 Content Filters(콘텐츠 필터) 보안 서비스 페이지에서 기본 정책의 콘텐츠 필터 값을 "Disable Content Filters(콘텐츠 필터 사용 안 함)"에서 "Enable Content Filters (Customize settings)(콘텐츠 필터 사용(설정 사용자 지정))"로 변경합니다.

그림 C-16 정책에 대한 콘텐츠 필터 활성화 및 특정 콘텐츠 필터 선택



마스터 목록(콘텐츠 필터 개요, 11-1페이지에서처럼 Incoming Content Filters(수신 콘텐츠 필터) 페이지를 사용하여 생성됨)에 정의된 콘텐츠 필터가 이 페이지에 표시됩니다. 값을 "Enable Content Filters (Customize settings)(콘텐츠 필터 활성화(설정 사용자 지정))"로 변경하면 각 필터의 확인란이 비활성화(회색) 상태에서 활성화 상태로 변경됩니다.

4단계 각 콘텐츠 필터에 대해 **Enable(활성화)** 확인란을 선택합니다.

5단계 **Submit(제출)**을 클릭합니다.

Incoming Mail Policies(수신 메일 정책) 페이지의 테이블은 기본 정책에 활성화된 필터의 이름을 보여줍니다.

그림 C-17 기본 수신 메일 정책에 대한 활성화된 콘텐츠 필터 3개

엔지니어링의 수신자에게 MP3 첨부 파일 허용

"엔지니어링" 정책의 "no_mp3s" 콘텐츠 필터를 비활성화하려면 다음을 수행합니다.

절차

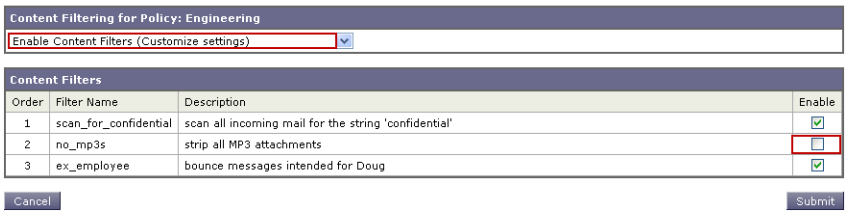
1단계 엔지니어링 정책 행에서 콘텐츠 필터 보안 서비스(콘텐츠 필터 열)의 링크를 클릭합니다.

2단계 Content Filters security service(콘텐츠 필터) 보안 서비스 페이지에서 Policy: Engineering(정책: 엔지니어링)의 콘텐츠 필터 값을 "Enable Content Filtering (Inherit default policy settings)(콘텐츠 필터 사용(기본 정책 설정 상속))"에서 "Enable Content Filters (Customize settings)(콘텐츠 필터 사용(설정 사용자 지정))"로 변경합니다.

이 정책은 기본값을 사용하기 때문에 "Use Default Settings(기본 설정 사용)"의 값을 "Yes(예)"로 변경하는 경우, 각 필터의 확인란이 비활성화(회색) 상태에서 활성화 상태로 변경됩니다.

3단계 "no_mp3s" 필터의 확인란을 선택 취소합니다.

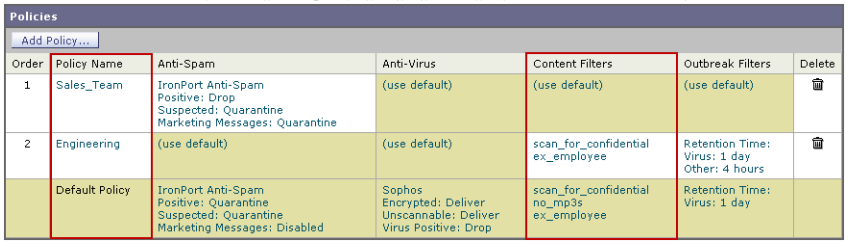
그림 C-18 콘텐츠 필터 선택 취소



4단계 **Submit(제출)**을 클릭합니다.

Incoming Mail Policies(수신 메일 정책) 페이지의 테이블은 엔지니어링 정책에 활성화된 필터의 이름을 보여줍니다.

그림 C-19 수신 메일 정책에 대해 업데이트된 콘텐츠 필터



5단계 변경사항을 커밋합니다.

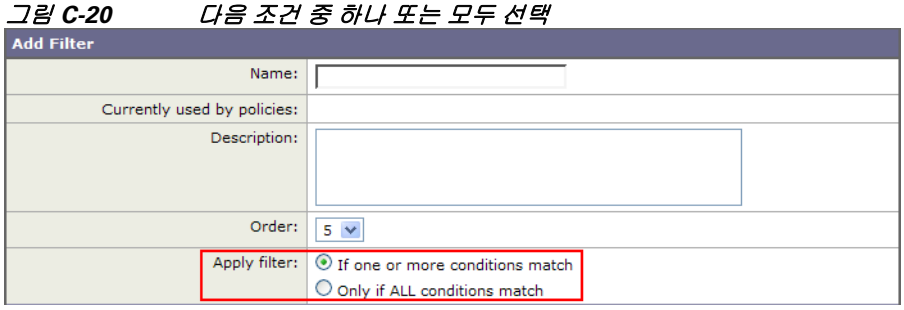
이때 엔지니어링 정책에 대한 사용자 목록과 일치하는 수신 메시지에서는 MP3 첨부 파일이 제거되지 않지만 기타 모든 수신 메시지의 MP3 첨부 파일은 제거됩니다.

GUI에서 콘텐츠 필터를 구성할 때의 주의 사항

- 콘텐츠 필터를 생성하는 경우 조건을 지정할 필요가 없습니다. 작업이 정의되지 않은 경우 정의된 작업이 항상 규칙에 적용됩니다. (작업을 지정하지 않는 것은 `true()` 메시지 필터 규칙을 사용하는 것과 같습니다. 콘텐츠 필터가 정책에 적용되는 경우 모든 메시지가 일치됩니다.)
- 콘텐츠 필터에 사용자 지정 사용자 역할을 할당하지 않은 경우 콘텐츠 필터는 공용으로 사용되거나 위임 관리자가 메일 정책에 사용할 수 있습니다. 위임 관리자 및 콘텐츠 필터에 대한 자세한 내용은 관리 작업 분배 항목을 참조하십시오.
- 콘텐츠 필터가 사용자 지정 사용자 역할에 할당된 경우에도 관리자와 운영자는 어플라이언스에서 모든 콘텐츠 필터를 보거나 편집할 수 있습니다.
- 필터 규칙 및 작업에 대한 텍스트를 입력하는 경우 다음 메타 문자는 정규식 일치에서 특수한 의미가 있습니다. `. ^ $ * + ? { [ ] \ | ( )`

  정규식을 사용하지 않으려는 경우 '\'(백슬래시)를 사용하여 이러한 문자를 이스케이프해야 합니다. 예: "*Warning*"
- 콘텐츠 필터에 대해 하나 이상의 조건을 정의하는 경우 콘텐츠 필터가 일치하는 것으로 간주하려면 정의된 작업 *모두*(즉, 논리적 AND)가 적용되어야 하는지, 아니면 정의된 작업 중 하나(논리적 OR)가 적용되어야 하는지 정의할 수 있습니다.

그림 C-20 다음 조건 중 하나 또는 모두 선택



- "무해한" 콘텐츠 필터를 생성하여 메시지 분리 및 콘텐츠 필터를 테스트할 수 있습니다. 예를 들어 "전달"이 유일한 작업인 콘텐츠 필터를 생성할 수 있습니다. 이 콘텐츠 필터는 메일 처리에 영향을 주지 않지만, 이 필터를 사용하여 이메일 정책 처리가 시스템의 다른 요소(예: 메일 로그)에 어떤 영향을 미치는지 테스트할 수 있습니다.
- 이와 반대로, 수신 또는 발송 콘텐츠 필터의 "마스터 목록" 개념을 사용하여 어플라이언스에서 취급되는 모든 메일에 대한 메시지 처리에 즉시 영향을 미치는 매우 강력하고 광범위한 콘텐츠 필터를 생성할 수 있습니다. 이를 위한 프로세스는 다음과 같습니다.
  - Incoming or Outgoing Content Filters(수신 또는 발송 콘텐츠 필터) 페이지에서 순서가 1인 새 콘텐츠 필터를 생성합니다.
  - Incoming or Outgoing Mail Policies(수신 또는 발송 메일 정책) 페이지에서 기본 정책에 대한 새 콘텐츠 필터를 활성화합니다.
  - 나머지 모든 정책에 대해 콘텐츠 필터를 활성화합니다.
- 콘텐츠 필터에서 사용할 수 있는 Bcc: 및 격리 작업은 생성한 격리의 보존 설정을 결정하는 데 도움이 될 수 있습니다. (30 장, "정책, 바이러스 및 신종 바이러스 격리" 참조.) 정책 격리 내부 및 외부의 메일 흐름을 시뮬레이션하는 필터를 생성하여 메시지가 시스템에서 너무 빨리 해제(즉, 격리 영역이 할당된 디스크 공간을 지나치게 빠르게 채우지 못함)되지 않도록 할 수 있습니다.
- "전체 메시지" 조건의 경우 Scan Behavior(검사 동작) 페이지 또는 `scanconfig` 명령과 동일한 설정을 사용하므로 메시지 헤더를 검사하지 않습니다. "전체 메시지"를 선택하면 메시지 본문 및 첨부 파일만 검사됩니다. 특정 헤더 정보를 검색하려면 "제목" 또는 "헤더" 조건을 사용하십시오.
- 어플라이언스에 LDAP 서버가 구성된 경우(즉, `ldapconfig` 명령을 사용하여 특정 LDAP 서버에 특정 문자열이 포함된 쿼리를 수행하도록 어플라이언스 구성) LDAP 쿼리로 사용자를 구성하면 GUI에만 나타납니다.
- 리소스가 사전 구성되지 않은 경우 콘텐츠 필터 규칙 빌더의 일부 섹션은 GUI에 표시되지 않습니다. 예를 들어 알림 템플릿 및 메시지 고지 사항이 이전에 Text Resources(텍스트 리소스) 페이지 또는 CLI의 `textconfig` 명령을 사용하여 구성되지 않았다면 옵션으로 표시되지 않습니다.
- 콘텐츠 필터 기능에서는 음 문자 인코딩의 텍스트를 인식, 포함하고 검사할 수 있습니다.
  - 유니코드(UTF-8)
  - 유니코드(UTF-16)
  - 서유럽/라틴어-1(ISO 8859-1)
  - 서유럽/라틴어-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 필터에서 여러 문자 집합을 결합하여 사용할 수 있습니다. 여러 문자 인코딩으로 텍스트를 표시하고 입력하기 위한 지원이 필요한 경우 웹 브라우저 설명서를 참조하십시오. 대부분의 브라우저는 여러 문자 집합을 동시에 렌더링할 수 있습니다.

그림 C-21 콘텐츠 필터의 여러 문자 집합

- Incoming or Outgoing Content Filters(수신 또는 발송 콘텐츠 필터) 요약 페이지에서 "Description(설명)", "Rules(규칙)" 및 "Policies(정책)" 링크를 사용하여 콘텐츠 필터에 표시되는 보기를 변경합니다.
  - **Description(설명)** 보기에는 각 콘텐츠 필터의 설명 필드에 입력한 텍스트가 표시됩니다. (이는 기본 보기입니다.)
  - **Rules(규칙)** 보기에는 규칙 빌더 페이지에서 빌드된 규칙 및 정규식이 표시됩니다.
  - **Policies(정책)**에는 각 콘텐츠 필터가 활성화된 정책이 표시됩니다.

그림 C-22 링크를 사용하여 콘텐츠 필터에 대한 설명, 규칙 및 정책 전환

Incoming Content Filters

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	scan_for_confidential	scan_for_confidential: if (body-contains("confidential")) { quarantine ("Policy"); bcc ("hr@example.com", "[message matched confidential filter]"); }		
2	no_mp3s	no_mp3s: if (true) { drop-attachments-by-filetype("mp3", "mp3 deleted"); }		
3	ex_employee	ex_employee: if (rcpt-to == "^doug@") { notify-copy ("$EnvelopeSender", "message bounced for ex-employee of example.com"); bounce(); }		
4	drop_large_attachments	drop_large_attachments: if (true) { drop-attachments-by-size(5242880, "This attachment was too big!"); }		

방화벽 정보

다음 표에는 가능한 포트가 나와 있으며 Cisco 어플라이언스(기본값임)가 올바르게 작동하려면 이 포트를 열어 두어야 합니다.

표 D-1 방화벽 포트

포트	프로토콜	인/아웃	호스트 이름	설명
20/21	TCP	인 또는 아웃	AsyncOS IP, FTP 서버	로그 파일 집계를 위한 FTP입니다. 데이터 포트 TCP 1024 이상은 모두 열려 있어야 합니다. 자세한 내용은 기술 자료의 FTP 포트 정보를 검색하십시오. 기술 자료(1-8 페이지) 항목을 참조하십시오.
22	TCP	인	AsyncOS IP	CLI에 대한 SSH 액세스, 로그 파일의 집계입니다.
22	TCP	아웃	SSH 서버	로그 파일의 SSH 집계입니다.
22	TCP	아웃	SCP 서버	로그 서버로 SCP 푸쉬
23	텔넷	인	AsyncOS IP	CLI에 대한 텔넷 액세스, 로그 파일의 집계입니다.
23	텔넷	아웃	텔넷 서버	텔넷 업그레이드, 로그 파일의 집계(권장되지 않음)입니다.
25	TCP	아웃	모두	이메일을 전송하기 위한 SMTP입니다.
25	TCP	인	AsyncOS IP	바운스된 이메일을 수신하기 위한 SMTP 또는 외부 방화벽에서 이메일을 삽입하는 경우입니다.
53	UDP/TCP	인 및 아웃	DNS 서버	인터넷 루트 서버 또는 방화벽 외부의 기타 DNS 서버를 사용하도록 구성된 경우의 DNS입니다. 또한 SenderBase 쿼리에 사용됩니다.
80	HTTP	인	AsyncOS IP	시스템 모니터링을 위한 GUI에 대한 HTTP 액세스입니다.
80	HTTP	아웃	downloads.ironport.com	AsyncOS 업그레이드 및 McAfee 정의를 제외한 서비스 업데이트입니다.
80	HTTP	아웃	updates.ironport.com	AsyncOS 업그레이드 및 McAfee 안티바이러스 정의입니다.

표 D-1 방화벽 포트 (계속)

80	HTTP	아웃	cdn-microupdates.cloudmark.com	Intelligent MultiScan에서 타사 스팸 구성 요소로의 업데이트에 사용됩니다. 어플라이언스는 타사 전화 홈 업데이트를 위해 CIDR 범위 208.83.136.0/22에 연결돼야 합니다.
82	HTTP	인	AsyncOS IP	Cisco 안티 스팸 격리 보기에 사용됩니다.
83	HTTPS	인	AsyncOS IP	Cisco 안티 스팸 격리 보기에 사용됩니다.
110	TCP	아웃	POP 서버	Cisco 스팸 격리를 위한 최종 사용자에 대한 POP 인증
123	UDP	인 및 아웃	NTP 서버	시간 서버가 외부 방화벽인 경우 NTP입니다.
143	TCP	아웃	IMAP 서버	Cisco 스팸 격리를 위한 최종 사용자에 대한 IMAP 인증
161	UDP	인	AsyncOS IP	SNMP 쿼리
162	UDP	아웃	관리 스테이션	SNMP 트랩
389 3268	LDAP	아웃	LDAP 서버	LDAP 디렉토리 서버가 외부 방화벽인 경우 LDAP입니다. Cisco 스팸 격리를 위한 LDAP 인증
636 3269	LDAPS	아웃	LDAPS	LDAPS — ActiveDirectory의 전역 카탈로그 서버(SSL 사용)
443	TCP	인	AsyncOS IP	시스템 모니터링을 위한 GUI에 대한 보안 HTTP(`https`) 액세스입니다.
443	TCP	아웃	res.cisco.com	Cisco Registered Envelope Service
443	TCP	아웃	update-manifests.ironport.com	업데이트 서버에 대한 최신 파일을 확인합니다.
443	TCP	아웃	phonehome.senderbase.org	신종 바이러스 필터(Outbreak Filter) 수신/전송
443	TCP	아웃	명령줄 인터페이스에서 `websecurityadvancedconfig` 명령을 실행하고 모든 기본값을 수락합니다. 웹 보안 서비스 호스트 이름이 표시됩니다.	URL 필터링을 위해 URL 평판 및 카테고리 정보를 얻기 위한 클라우드 서비스입니다.
443	TCP	아웃	Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석), Advanced(고급) 섹션에 구성된 대로 클라우드 서버 풀 매개변수입니다.	구성된 경우 파일 평판을 얻기 위해 클라우드 서비스에 액세스하는 데 사용되는 포트입니다. 기본 포트는 32137입니다. 파일 분석 서비스의 경우 포트 443을 참조하십시오.

표 D-1 방화벽 포트 (계속)

443	TCP	아웃	Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석), Advanced(고급) 섹션에 구성된 대로 사용합니다.	파일 분석을 위해 클라우드 서비스에 액세스합니다. 파일 평판 서비스의 경우 포트 443 또는 32137을 참조하십시오.
514	UDP/TCP	아웃	Syslog 서버	Syslog 로깅
628	TCP	인	AsyncOS IP	외부 방화벽에서 이메일을 삽입하는 경우 QMQP입니다.
1024 이상	—	—	—	포트 21(FTP)에 대해서는 위의 정보를 참조하십시오.
2222	CCS	인 및 아웃	AsyncOS IP	클러스터 통신 서비스(중앙 집중식 관리용)
6025	TCP	아웃	AsyncOS IP	Cisco 스팸 격리
7025	TCP	인 및 아웃	AsyncOS IP	이 기능이 중앙 집중식인 경우 Email Security 어플라이언스와 Cisco Content Security Management Appliance 간에 정책, 바이러스 및 신종 바이러스 격리 데이터를 전달합니다.
32137	TCP	아웃	Security Services(보안 서비스) > File Reputation and Analysis(파일 평판 및 분석), Advanced(고급) 섹션에 구성된 대로 클라우드 서버 풀 매개변수입니다.	파일 평판을 얻기 위해 클라우드 서비스에 액세스하는 데 사용되는 기본 포트입니다. 포트 443도 참조하십시오. 파일 분석 서비스의 경우 포트 443을 참조하십시오.

최종 사용자 라이센스 계약

Cisco 시스템 최종 사용자 라이센스 계약

중요: 본 최종 사용자 라이센스 계약을 신중하게 읽어 주십시오. 승인된 제공원에서 Cisco 소프트웨어 또는 장비를 구입하였으며 귀하 또는 귀하가 대표하는 실체(통칭하여, "고객")가 본 Cisco 최종 사용자 라이센스 계약의 목적에 따라 최종 사용자로 등록되어 있는지 확인하는 것이 매우 중요합니다. 귀하가 최종 사용자로 등록되어 있지 않은 경우 소프트웨어를 사용할 수 있는 라이센스가 없으며 본 최종 사용자 라이센스 계약의 제한 보증이 적용되지 않습니다. 승인된 제공원에서 구입하였다고 가정하고, Cisco 또는 Cisco에서 제공한 소프트웨어를 다운로드하여 설치 또는 사용하였다면 이는 본 계약을 수락하였다고 해석됩니다.

Cisco Systems, Inc. 또는 Cisco System, Inc.를 대신하여 소프트웨어의 라이센스를 제공하는 Cisco 자회사. ("CISCO")는 귀하가 승인된 제공원에서 소프트웨어를 구입했으며 본 최종 사용자 라이센스 계약과 더불어 제품에 함께 제공되거나 주문 시 이용 가능한 추가 라이센스 계약에 명시된 라이센스의 추가 제한(통칭하여 "계약")에 포함된 모든 조건을 수락하는 경우에만 본 소프트웨어에 대한 라이센스를 제공합니다. 본 최종 사용자 라이센스 계약과 모든 추가 라이센스 계약의 조건 간에 충돌이 발생하는 경우 추가 라이센스 계약이 적용됩니다. 소프트웨어를 다운로드하고 설치하거나 사용하는 것은 귀하가 승인된 제공원에서 소프트웨어를 구입했으며 계약에 대한 의무가 있음을 나타냅니다. 계약의 모든 조건에 동의하지 않는 경우 Cisco는 소프트웨어에 대한 라이센스를 제공하지 않으며 (A) 귀하는 소프트웨어를 다운로드, 설치 또는 사용할 수 없고, (B) 전액 환불을 위해 개봉하지 않은 CD 패키지와 서면 자료를 포함한 소프트웨어를 반환할 수 있으며 또한 소프트웨어 및 서면 자료가 다른 제품의 일부로 제공된 경우 전액 환불을 위해 전 제품을 반환할 수 있습니다. 귀하의 반환 및 환불 권한은 승인된 제공원에서 구입 후 30일 후에 만료되며 귀하가 원래 및 등록 최종 사용자 구매자인 경우에만 이 사항이 적용됩니다. 본 최종 사용자 라이센스 계약에서 "승인된 제공원"이란 (A) Cisco 또는 (B) Ciso 장비, 소프트웨어 및 서비스를 해당 지역 내에서 최종 사용자에게 배포 및 판매할 수 있는 Cisco가 승인한 공인 배포업체 또는 시스템 통합업체 또는 (C) Cisco 장비, 소프트웨어 및 서비스를 해당 지역 내에서 최종 사용자에게 배포 및 판매할 수 있는 배포업체의 Cisco 계약 약관에 따라 이러한 배포업체 또는 시스템 통합업체가 승인한 공인 리셀러를 의미합니다.

다음 계약 약관은 다음의 해당 범위를 제외하고 고객의 소프트웨어 사용에 적용됩니다. (A) 고객의 소프트웨어 사용에 적용되는 고객과 Cisco 간 별도의 서명 계약이 있습니다. 또한, (B) 소프트웨어는 고객의 소프트웨어 사용에 적용되는 설치 또는 다운로드 절차의 일부로서 별도의 "클릭 동의" 라이센스 계약 또는 타사 라이센스 계약을 포함합니다. 위 문서의 조항 간에 충돌이 발생하는 경우, (1) 서명한 계약 (2) 클릭 동의 계약 또는 타사 라이센스 계약, (3) 본 계약이 순서대로 우선합니다. 계약의 목적에 따라 "소프트웨어"는 승인된 제공원에서 고객에게 제공된 대로 Cisco 장비에 내장된 펌웨어 및 컴퓨터 프로그램을 포함하는 컴퓨터 프로그램, 모든 업그레이드, 업데이트, 버그 수정 또는 수정된 버전(통칭하여, "업그레이드"), Cisco 소프트웨어 양도 및 재라이센싱 정책(Cisco에서 언제든지 수정할 수 있음)에 따라 재라이센스된 동일한 항목 또는 앞서 언급한 항목의 백업 복사본을 의미합니다.

라이센스. 본 계약의 사용 약관 준수에 따라 Cisco는 고객이 승인된 제공원에게 필요한 라이센스 요금을 지불한 소프트웨어 및 문서에 대해 고객의 내부 비즈니스 목적으로 사용할 비독점적이고 양도 불가능한 라이센스를 고객에게 제공합니다. "문서"는 소프트웨어와 관련된 서면 정보(사용자 또는 기술 설명서, 교육 자료, 사양 등)를 의미하며 승인된 제공원에 의해 소프트웨어와 어떤 방식으로든 사용할 수 있습니다(CD-ROM 또는 온라인 포함). 소프트웨어를 사용하기 위해 고객은 등록 번호 또는 제품 인증 키를 입력하고 필요 라이센스 키 또는 라이센스 파일을 가져오기 위해 Cisco 웹 사이트에서 온라인으로 고객 소프트웨어의 복사본을 등록해야 합니다.

소프트웨어 사용을 위한 고객의 라이센스는 해당 추가 라이센스 계약 또는 승인된 제공원에서 수락하고 고객이 승인된 제공원에게 필요한 라이센스 요금을 지불한 해당 구매 주문서("구매 주문서")에 명시된 단일 하드웨어 섀시나 카드 또는 이러한 기타 제한 사항으로 제한되며 고객은 이 범위를 초과하여 소프트웨어를 사용할 수 없습니다.

문서 또는 해당 추가 라이센스 계약에 명시되어 있지 않는 한 고객은 실행을 위해 내장된 대로만 소프트웨어를 사용하거나, 해당 문서가 Cisco가 아닌 장비에 설치를 허용하는 경우 고객이 소유하거나 임대한 Cisco 장비와의 통신을 위해 또는 고객의 내부 비즈니스 목적을 위해서만 사용됩니다. 기타 라이센스는 묵시적으로, 금반언의 원칙에 의하여 또는 기타 어떠한 방식에 의해서 제공되지 않습니다.

Cisco가 라이센스 요금을 부과하지 않는 평가 또는 베타 복사본의 경우 라이센스 요금을 지급하는 위의 요구 사항이 적용되지 않습니다.

일반적인 제한사항. 이는 소프트웨어 및 문서에 대한 라이센스이며 소유권 양도가 아닙니다. Cisco는 소프트웨어와 문서의 모든 복사본에 대한 소유권을 보유합니다. 고객은 소프트웨어와 문서에 개별 프로그램의 특정 내부 설계 및 구조와 관련 인터페이스 정보를 비롯한(이에 국한되지 않음) Cisco 또는 공급업체 또는 라이센스 허가자의 영업 기밀을 포함되어 있다는 것을 인정합니다. 본 계약 하에 명시적으로 제공되지 않는 한 고객은 승인된 제공원으로부터 구입한 Cisco 장비 사용과 관련된 소프트웨어만 사용해야 합니다. 또한, 고객에게는 다음 사항에 대한 권한이 없으며 고객은 특별히 다음 사항을 수행하지 않을 것에 동의합니다.

(i) 다른 사람 또는 실체에게 라이센스 권한 양도, 할당 또는 2차 라이센스 부여(Cisco 현행 재라이센싱/양도 정책을 준수하는 것 외) 또는 고객이 승인된 제공원으로부터 구입하지 않은 Cisco 장비에서 또는 중고 Cisco 장비에서 소프트웨어를 사용하는 행위. 고객은 이러한 양도, 할당, 2차 라이센스 부여 또는 사용을 시도한 경우 무효임을 인정합니다.

(ii) 소프트웨어에 대한 오류 수정, 또는 소프트웨어를 수정하거나 변경, 또는 소프트웨어를 기반으로 한 파생물 생성 또는 타사가 동일한 작업을 수행하도록 허용하는 행위.

(iii) 본 제한 사항에도 불구하고 해당 법에서 명시적으로 허용하거나 Cisco가 법적으로 해당 오픈 소스 라이센스와 관련된 특정 활동을 허용해야 하는 경우를 제외하고 리버스 엔지니어링 또는 디컴파일, 암호 해독, 디스어셈블 또는 소프트웨어를 사람이 읽을 수 있는 형식으로 변경하는 행위.

(iv) 소프트웨어에서 실행하는 벤치마크 테스트 결과를 게시하는 행위.

(v) 출력소에서 또는 시간 공유 기반으로, 또는 어떤 형태로든 Cisco의 명시적인 서면 승인 없이 타사 서비스를 수행하는 데 소프트웨어를 사용하거나 사용하도록 허용하는 행위.

(vi) Cisco의 사전 서면 승인 없이 타사에 어떤 형식으로든 소프트웨어 및 문서에 포함된 거래 기밀을 공개 및 제공하거나 사용을 허용하는 행위. 고객은 이러한 영업 기밀을 보호하기 위해 적절한 보안 조치를 실행합니다.

해당 법률 및 고객의 서면 요청에 의해 필요한 경우 Cisco의 해당 요금이 지불되면 소프트웨어와 다른 독립 생성 프로그램 간 상호 운용성을 위해 필요한 인터페이스 정보를 고객에게 제공합니다. 고객은 이러한 정보에 대한 기밀성의 엄격한 의무를 준수하고 모든 해당 사용 약관을 준수하여 이러한 정보를 사용합니다.

소프트웨어, 업그레이드 및 추가 복사본. 본 계약의 그 밖의 조항에도 불구하고 (1) 고객에게는 복사본이나 업그레이드를 생성하거나 획득하는 시점에 원래 소프트웨어에 대한 유효한 라이센스를 보유하지 않거나 승인된 제공원에게 업그레이드 또는 추가 복사본에 대한 해당 요금을 지불하지 않은 경우, 추가 복사본 또는 업그레이드를 생성하거나 사용할 라이센스 또는 권한이 없습니다. (2)

업그레이드 사용은 고객이 원래 최종 사용자 구매자이거나 임차인이거나 업그레이드하는 소프트웨어를 사용할 유효 라이센스를 보유하는 경우에 승인된 제공원에서 제공한 Cisco 장비로 제한됩니다. (3) 추가 복사본 생성 및 사용은 필수 백업 목적으로만 제한됩니다.

소유권 통지. 고객은 소프트웨어의 모든 복사본에 대한 모든 저작권 및 기타 소유권 통지가 소프트웨어에 포함되는 동일한 형식 및 방식으로 그러한 저작권, 소유권 및 기타 통지를 어떠한 형태로든 유지하고 복제한다는 것에 동의합니다. 본 계약에 명시되어 있지 않은 한 고객은 Cisco의 사전 서면 허가 없이 어떠한 소프트웨어의 복사본도 만들거나 복제하지 않습니다.

기간 및 종료. 본 계약에서 부여된 계약 및 라이센스는 계약이 종료될 때까지 유효합니다. 고객은 소프트웨어 및 모든 문서의 모든 복사본을 파기함으로써 언제든지 본 계약 및 라이센스를 종료할 수 있습니다. 고객이 본 계약의 어떤 조항이라도 준수하지 않는 경우 Cisco의 통지 없이 본 계약에 따른 고객의 권한이 즉시 종료됩니다. 계약 종료 시 고객은 소유하거나 관리하고 있는 소프트웨어 및 문서의 모든 복사본을 파기합니다. 고객의 모든 비밀유지의무, "일반 제한 사항" 섹션에 따라 고객에게 부과된 모든 규제 및 제한 사항, 보증의 모든 책임 제한, 보증 부인 및 규제는 본 계약 종료에도 유지됩니다. 또한 "미국 정부 최종 사용자 구매자" 및 "제한 보증서 및 최종 사용자 라이센스 계약에 해당하는 일반 조건" 섹션의 조항은 계약 종료에도 유지됩니다.

고객 기록. 고객의 본 계약 준수 여부를 확인하기 위해 고객의 일반적인 업무 시간 동안 고객의 예약, 기록 및 계정을 검토할 수 있는 권한을 Cisco 및 독립 회계사에게 부여합니다. 이러한 감사를 통해 고객이 본 계약을 준수하지 못했다는 사실이 밝혀지는 경우 고객은 Cisco에 해당하는 라이센스 비용과 감사 진행에 대한 적절한 비용을 즉각 지불해야 합니다.

수출, 재수출, 양도 및 규제 사용. 본 계약에 따라 Cisco에서 공급하는 소프트웨어, 문서 및 기술 또는 직접 제품(이후 소프트웨어 및 기술이라고 함)은 미국의 법률 및 규정과 기타 해당 국가의 법률 및 규정에 따른 수출 규제를 따릅니다. 고객은 Cisco 소프트웨어 및 기술의 수출, 재수출, 양도 및 사용에 적용되는 이러한 법률 및 규정을 준수하고 필요한 모든 미국 및 현지 인증서, 허가권 또는 라이센스를 획득해야 합니다. Cisco와 고객은 상대 당사자에게 인증서 또는 라이센스 획득과 관련하여 필요한 정보, 보충 문서 및 지원을 제공한다는 것에 동의합니다. 수출, 재수출, 양도 및 사용을 준수하는 것과 관련된 정보는 다음 URL에서 확인할 수 있습니다.

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html.

미국 정부 최종 사용자 구매자. 소프트웨어 및 문서는 연방조달규정("FAR") 12.212에 사용되는 "상업용 컴퓨터 소프트웨어" 및 "상업용 컴퓨터 소프트웨어 문서"로 구성된 FAR(48 C.F.R.) 2.101에 정의된 대로 "상업용 제품"으로 허용됩니다. 이는 FAR 12.212 및 DoD FAR Supp.과 일치합니다. 227.7202-1부터 227.7202-4까지 및 기타 FAR 또는 본 계약이 통합될 수 있는 모든 계약과 반대되는 기타 계약 조항에도 불구하고, 고객은 정부 최종 사용자에게 본 계약에 명시된 그러한 권한만이 포함된 소프트웨어 및 문서를 제공할 수 있고 본 계약이 직접적인 경우 정부 최종 사용자가 이러한 소프트웨어 및 문서를 획득할 수 있습니다. 소프트웨어나 문서를 사용하거나 두 가지 모두를 사용하는 것은 소프트웨어 및 문서가 "상업용 컴퓨터 소프트웨어" 및 "상업용 컴퓨터 소프트웨어 문서"라는 정부의 계약을 구성하며 본 계약의 권한 및 제한을 수락한 것으로 해석됩니다.

식별된 구성 요소, 추가 조건. 소프트웨어는 본 계약에 명시된 사항 이외에도 다른 라이센스 계약 약관, 보증 부인, 제한 보증 또는 기타 사용 약관(통칭하여, "추가 조건")을 따르며 문서, Readme.txt 파일, 타사 클릭 동의 또는 기타 위치(예: www.cisco.com)에서 Cisco가 식별한 타사 구성 요소("식별된 구성 요소")를 포함하는 하나 이상의 구성 요소를 포함하거나 이를 포함하여 제공될 수 있습니다. 귀하는 이러한 식별된 구성 요소에 해당하는 추가 조건에 동의합니다."

제한 보증

본 계약에 명시된 제한 및 조건에 따라 Cisco는 고객에게 배송 날짜로부터 개시하며(Cisco외의 승인된 제공원의 재판매 경우 Cisco의 원래 배송 후 90일 이상 개시하지 않음) 및 (a) 90일 또는 (b) 소프트웨어가 일부인 제품("제품")을 제공하는 보증 카드의 소프트웨어에 특히 해당한다고 명시되어 있는 보증 기간 동안 지속하여 (a) 일반적인 사용 시 소프트웨어가 공급된 미디어에 재료 및 기술에 결함이 없고 (b) 소프트웨어가 문서를 준수한다는 것을 보증합니다. Cisco의 제품 배송 날짜는 제품이 배송되는 포장재에 표시되어 있습니다. 앞서 언급한 사항을 제외하고 소프트웨어는 "있

는 그대로" 제공됩니다. 이 제한 보증은 첫 번째로 등록된 최종 사용자인 고객이 승인된 제공원으로부터 구입한 소프트웨어에만 제공됩니다. 이 제한 보증에 따른 고객의 단독적이고 독점적인 해결 방안 및 Cisco와 공급업체의 전체 법적 책임은 (i) 결함이 있는 미디어의 교체 및/또는 (ii) Cisco의 옵션, 수리, 교체 또는 소프트웨어 구매 금액 환불에 해당하며, 두 가지 경우 모두 이 제한 보증을 위반한 것으로 해석되는 모든 오류 또는 결함이 보증 기간 내에 소프트웨어를 고객에게 공급하는 승인된 제공원에게 보고되어야 한다는 조건을 따라야 합니다. 소프트웨어를 고객에게 공급하는 Cisco 또는 승인된 제공원은 옵션으로 소프트웨어 및/또는 문서의 반환을 해결 방안으로 요구할 수 있습니다. Cisco는 소프트웨어에 오류가 없거나 고객이 문제 또는 중단 없이 소프트웨어를 작동할 수 있다는 것을 보장하지는 않습니다. 또한 네트워크 침입 및 공격에 대한 새로운 기술이 계속 발전하고 있으므로 Cisco는 소프트웨어 또는 소프트웨어가 사용되는 모든 장비, 시스템 또는 네트워크가 침입 또는 공격에 대한 취약성이 없다고 보장하지 않습니다.

제한 사항. 이 보증은 소프트웨어, 제품 또는 소프트웨어가 인증되어 사용할 수 있는 기타 모든 장비가 (a) Cisco 또는 공인 대리인을 제외한 다른 실체에 의해 변경되고 (b) Cisco에서 제공한 지침에 따라 설치, 작동, 수리 또는 유지되지 않고 (c) 비정상적인 물리적 또는 전기적 응력, 비정상적인 환경 조건, 오용, 과실 또는 사고를 거쳤거나 (d) 베타, 평가, 테스트 또는 데모 목적으로 라이센스가 제공된 경우에는 적용되지 않습니다. 소프트웨어 보증 역시 (e) 임시 소프트웨어 모듈, (f) Cisco의 소프트웨어 센터에 게시되지 않은 모든 소프트웨어, (g) Cisco가 Cisco의 소프트웨어 센터에 "있는 그대로" 명시적으로 제공하는 모든 소프트웨어, (h) 승인된 제공원이 라이센스 요금을 받지 않은 모든 소프트웨어 및 (i) 승인된 제공원이 아닌 모든 타사에서 제공한 소프트웨어에는 적용되지 않습니다.

보증 부인

이 보증 섹션에 지정된 사항을 제외하고 명시적 또는 묵시적 조건, 진술 및 상업성, 특정 목적에의 적합성, 비침해성, 만족할 만한 품질, 비간섭, 정보 컨텐츠의 정확성 또는 거래 과정으로 인해 발생한 사항, 법률, 사용 또는 거래 관습의 묵시적 보증 또는 조건을 비롯한(이에 국한되지 않음) 보증은 해당 법률에서 허용된 범위에서 제외되며 Cisco, 공급업체 및 라이센스 허가자는 이를 명시적으로 부인합니다. 동일한 사항이 제외되지 않는 경우 이러한 묵시적 조건, 진술 및/또는 보증은 위의 "제한 보증" 섹션에 언급된 명시적 보증 기간으로 제한됩니다. 일부 주 또는 관할 지역에서는 묵시적 보증이 지속되는 기간에 대한 제한을 허용하지 않으므로 위의 제한은 일부 주에서 적용되지 않을 수 있습니다. 이 보증은 고객에게 특정 법적 권한을 제공하며 고객은 관할 지역별로 다양한 기타 권한을 보유할 수 있습니다. 이 보증 및 제한 사항은 위에 명시된 명시적 보증이 핵심 목적을 이루지 못한 경우에도 적용됩니다.

책임 부인 - 책임 제한. 미국, 라틴 아메리카, 캐나다, 일본 또는 카리브해 지역에서 소프트웨어를 획득한 경우, 본 계약의 다른 모든 사항과 반대되는 내용에도 불구하고 계약, 불법 행위(과실 포함), 보증 위반 또는 기타 경우로 인한 고객에게 져야할 Cisco, 해당 계열사, 관리자, 책임자, 직원, 에이전트, 공급업체 및 라이센스 허가자의 모든 책임은 클레임이 발생한 소프트웨어에 대해 고객이 승인된 제공원에게 지불한 가격을 초과하지 않으며 소프트웨어가 다른 제품의 일부를 구성하는 경우에는 해당 제품을 위해 지불된 가격을 초과하지 않습니다. 소프트웨어에 대한 이 책임 제한은 누적되며 사건별로 적용되지 않습니다(즉, 두 개 이상의 클레임이 있더라도 이 제한이 확대되지 않습니다).

유럽, 중동, 아프리카, 아시아 또는 오세아니아에서 소프트웨어를 획득한 경우, 본 계약의 다른 모든 사항과 반대되는 내용에도 불구하고 계약, 불법 행위(과실 포함), 보증 위반 또는 기타 경우로 인한 고객에게 져야할 Cisco, 해당 계열사, 관리자, 책임자, 직원, 에이전트, 공급업체 및 라이센스 허가자의 모든 책임은 클레임이 발생한 소프트웨어에 대해 고객이 Cisco에게 지불한 가격을 초과하지 않으며 소프트웨어가 다른 제품의 일부를 구성하는 경우에는 해당 제품을 위해 지불된 가격을 초과하지 않습니다. 소프트웨어에 대한 이 책임 제한은 누적되며 사건별로 적용되지 않습니다(즉, 두 개 이상의 클레임이 있더라도 이 제한이 확대되지 않습니다). 본 계약의 어떤 조항도 (I) 고객의 과실에 기인한 개인적인 상해 또는 사망에 대한 Cisco, 해당 계열사, 담당자, 책임자, 직원, 에이전트, 공급업체 및 라이센스 허가자의 책임, (II) Cisco의 사기 허위 진술에 대한 책임 또는 (III) 해당 법률에 따라 제외할 수 없는 Cisco의 모든 책임을 제한할 수 없습니다.

책임 부인 - 결과적 손해 및 기타 손실의 권리 포기. 미국, 라틴 아메리카, 캐나다, 일본 또는 카리브해 지역에서 소프트웨어를 획득한 경우, 본 계약에 명시된 해결 방안이 핵심 목적 또는 기타 사항을 이루었는지 여부를 불문하고 어떠한 경우라도 Cisco 또는 해당 공급업체는 손실 소득, 수익 또는 손실되거나 손상된 데이터, 업무 중단, 자본 손실 또는 특별, 간접적, 결과적, 부수적 또는 처벌적 손해에 대해 발생 방법과 책임 이론과 무관하게 또는 소프트웨어 또는 기타 사항을 사용 또는 사용하지 못함으로 인하여 발생하고 Cisco 또는 해당 공급업체 또는 라이센스 허가자가 이러한 손해의 가능성에 대해 언급을 받더라도 책임을 지지 않습니다. 일부 주 또는 관할 지역에서는 결과적 또는 부수적 손해의 제한 또는 제외를 허용하지 않으므로 위의 제한은 귀하에게 적용되지 않을 수 있습니다.

일본에서 소프트웨어를 획득한 경우, 사망 또는 개인적 상해, 사기 허위 진술로 인한 책임을 제외하고, 본 계약에 명시된 해결 방안이 핵심 목적 또는 기타 사항을 이루었는지 여부를 불문하고 어떠한 경우라도 Cisco, 해당 계열사, 담당자, 책임자, 직원, 에이전트, 공급업체 및 라이센스 허가자는 손실 소득, 수익 또는 손실되거나 손상된 데이터, 업무 중단, 자본 손실 또는 특별, 간접적, 결과적, 부수적 또는 처벌적 손해에 대해 발생 방법과 책임 이론과 무관하게 또는 소프트웨어 또는 기타 사항을 사용 또는 사용하지 못함으로 인하여 발생하고 Cisco 또는 모든 승인된 제공원, 또는 해당 공급업체 또는 라이센스 허가자가 이러한 손해의 가능성에 대해 언급을 받더라도 책임을 지지 않습니다.

유럽, 중동, 아프리카, 아시아 또는 오세아니아에서 소프트웨어를 획득한 경우 어떠한 경우라도 Cisco, 해당 계열사, 담당자, 책임자, 직원, 에이전트, 공급업체 및 라이센스 허가자는 모든 손실 소득, 손실 수익 또는 손실되거나 손상된 데이터, 업무 중단, 자본 손실 또는 특별, 간접적, 결과적, 부수적 또는 처벌적 손해에 대해 계약, 불법 행위(과실 포함)에서의 제한을 비롯한(이에 국한되지 않음) 발생 방법과 상관없이 또는 소프트웨어를 사용 또는 사용하지 못함으로 인하여 발생하고 각각의 경우에 Cisco, 해당 계열사, 담당자, 책임자, 직원, 에이전트, 공급업체 및 라이센스 허가자가 이러한 손해의 가능성에 대해 언급을 받더라도 책임을 지지 않습니다. 일부 주 또는 관할지에서는 결과적 또는 부수적 손해의 제한 또는 제외를 허용하지 않으므로 위의 제한은 귀하에게 완전히 적용되지 않을 수 있습니다. 위의 제외 사항은 (I) 사망 또는 개인 상해, (II) 사기 허위 진술 또는 (III) 해당 법에 따라 제외할 수 없는 모든 조건과 관련된 Cisco의 책임으로 인해 발생하거나 이와 관련된 모든 책임에 적용되지 않습니다.

고객은 Cisco가 본 계약에 명시된 보증 부인 및 책임의 제한에 따라 가격을 설정하고 계약을 체결했으며, 동일한 사항이 당사자 간 위험 할당(계약 해결 방안이 핵심 목적을 이루지 못하고 결과적 손실을 야기할 수 있는 위험 포함)을 반영하고, 동일한 사항이 당사자 간 협상의 핵심적 기반을 이룬다는 것을 인정하고 이에 동의합니다.

규제 법률, 관할 지역. 승인된 제공원에서 수락한 구매 주문서의 주소를 참조하여 미국, 라틴 아메리카 또는 카리브해 지역에서 소프트웨어를 획득한 경우 본 계약 및 보증("보증")은 법률 조항이 충돌하더라도 미국 캘리포니아 주의 법률이 적용되어 해석되며, 캘리포니아 주 및 연방 법원은 본 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 독점적인 관할권을 갖습니다. 캐나다에서 소프트웨어를 획득한 경우 현지 법률에 의해 명시적으로 금지되지 않는 한 본 계약 및 보증은 법률 조항이 충돌하더라도 캐나다 온타리오 지역의 법률이 적용되어 해석되며 온타리오 지역 법원은 본 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 독점적인 관할권을 갖습니다. 유럽, 중동, 아프리카, 아시아 또는 오세아니아(호주 제외)에서 소프트웨어를 획득한 경우 현지 법률에 의해 명시적으로 금지되지 않는 한 본 계약 및 보증은 법률 조항이 충돌하더라도 영국의 법률이 적용되어 해석되며 영국 법원은 본 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 독점적인 관할권을 갖습니다. 또한 계약에 영국의 법률이 적용되는 경우 본 계약의 당사자가 아닌 사람은 1999년 계약(제3자의 권리) 법에 따른 약관의 혜택을 집행하거나 이용할 수 있는 자격이 없습니다. 일본에서 소프트웨어를 획득한 경우 현지 법률에 의해 명시적으로 금지되지 않는 한 본 계약 및 보증은 법률 조항이 충돌하더라도 일본의 법률이 적용되어 해석되며 일본의 도쿄 법원은 본 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 독점적인 관할권을 갖습니다. 호주에서 소프트웨어를 획득한 경우 현지 법률에 의해 명시적으로 금지되지 않는 한 본 계약 및 보증은 법률 조항이 충돌하더라도 호주 뉴사우스웨일스의 법률이 적용되어 해석되며 뉴사우스웨일스의 주 및 연방 법원은 본 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 독점적인 관할권을 갖습니다. 기타 국가에서 소프트

웨어를 획득한 경우 현지 법률에 의해 명시적으로금지되지 않는 한 본 계약 및 보증은 법률 조항이 충돌하더라도 미국 캘리포니아 주의 법률이 적용되어 해석되며 캘리포니아 주 및 연방 법원은 본 계약 또는 보증에 따라 발생하는 모든 클레임에 대해 독점적인 관할권을 갖습니다.

위에서 언급된 모든 국가의 경우 당사자는 특히 국제물품매매계약에 관한 국제연합협약(UN Convention on Contracts for the International Sale of Goods)의 적용을 부인합니다. 앞서 언급한 사항에도 불구하고 당사자는 이러한 당사자의 지적 재산권 또는 소유권의 혐의 위반과 관련하여 해당 관할 지역 법원에서 잠정적인 금지명령 구제를 구할 수 있습니다. 본 계약의 일부가 무효가 되거나 집행할 수 없다고 확인되는 경우 본 계약 및 보증의 나머지 조항은 완전한 효력을 갖습니다. 본 계약에 명시적으로 제공된 사항을 제외하고 본 계약은 소프트웨어 및 문서의 라이센스와 관련된 당사자 간 전체 계약을 구성하며 모든 구매 주문서 또는 모든 조건이 제외된 다른 항목에 포함된 충돌하거나 추가된 조건을 대체합니다. 본 계약은 영어로 작성되었으며 당사자는 영어 버전이 적용되는 것에 동의합니다.

Cisco 제품에 적용되는 제품 보증 조항 및 기타 정보는 다음 URL에서 확인할 수 있습니다.

http://www.cisco.com/go/warranty

Cisco 시스템 콘텐츠 보안 소프트웨어의 추가 최종 사용자 라이센스 계약

중요: 신중하게 읽어보십시오.

이 추가 최종 사용자 라이센스 계약("SEULA")은 귀하(여기서 "귀하"란 귀하 또는 귀하가 대표하는 기업 실체, 또는 "회사"를 의미)와 Cisco 간 최종 사용자 라이센스 계약("EULA")에 따라 라이센스가 제공된 소프트웨어 제품에 대한 추가 사용 약관을 포함합니다(통칭하여, "계약"). 본 SEULA에 사용되지만 정의되지 않은 대문자로 된 약관은 EULA에서 지정한 의미를 갖습니다. EULA 및 본 SEULA의 사용 약관 사이에 충돌이 발생하는 경우 본 SEULA의 약관이 우선합니다.

소프트웨어 액세스 및 사용에 관해 EULA에 명시된 제한 사항 외에도 귀하는 본 SEULA에 제공된 사용 약관을 항상 준수한다는 데 동의합니다.

소프트웨어 다운로드, 설치 또는 사용은 본 계약에 대한 동의로 해석되며 귀하와 귀하가 대표하는 비즈니스 실체는 본 계약에 구속됩니다. 계약의 모든 조건에 동의하지 않는 경우 Cisco는 소프트웨어에 대한 라이센스를 제공하지 않으며 (A) 귀하는 소프트웨어를 다운로드, 설치 또는 사용할 수 없고, (B) 전액 환불을 위해 개봉하지 않은 CD 패키지와 서면 자료를 포함한 소프트웨어를 반환할 수 있으며 또한 소프트웨어 및 서면 자료가 다른 제품의 일부로 제공된 경우 전액 환불을 위해 전 제품을 반환할 수 있습니다. 귀하의 반환 및 환불 권한은 Cisco 또는 공인 Cisco 리셀러로에서 구입 후 30일 후에 만료되며 귀하가 원래 최종 사용자 구매자인 경우에만 이 사항이 적용됩니다.

본 SEULA의 목적에 따라, 귀하가 주문한 제품 이름 및 제품 설명은 다음 Cisco 시스템 Email Security 어플라이언스("ESA"), Cisco 시스템 웹 보안 어플라이언스("WSA") 및 Cisco 시스템 보안 관리 애플리케이션("SMA")(통칭하여, "콘텐츠 보안") 및 이에 해당하는 가상 어플라이언스("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 RSA Data Loss Prevention

Cisco Email Encryption

Cisco Email Delivery Mode

Cisco Web Usage Controls

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 SEULA의 목적에 따라 다음 용어 정의가 적용됩니다.

"회사 서비스"는 회사의 내부 비즈니스 수행을 목적으로 최종 사용자에게 제공되는 회사의 이메일, 인터넷, 보안 관리 서비스를 의미합니다.

"최종 사용자"는 (1) WSA 및 SMA의 경우, 회사 서비스를 통해 인터넷 및 SMA에 액세스하도록 회사에서 인증한 직원, 계약자 또는 기타 에이전트이며 (2) ESA의 경우, 회사 서비스를 통해 이메일 서비스를 접근 또는 사용하도록 회사에서 인증한 직원, 계약자 또는 기타 에이전트의 이메일 상자입니다.

"주문 문서"는 회사와 Cisco 또는 회사와 Cisco 리셀러 간의 구매 계약, 평가 계약, 베타, 사전 출시 계약 또는 유사한 계약 또는 본 계약에서 부여한 소프트웨어 라이센스의 구매 약관을 포함하는 Cisco에서 수락한 구매 주문서의 유효한 약관을 의미합니다.

"개인적으로 식별 가능한 정보"는 개인 이름, 사용자 이름, 이메일 주소 및 개별적으로 식별 가능한 기타 정보를 비롯하여(이에 국한되지 않음) 개인을 식별하는 데 사용할 수 있는 모든 정보를 의미합니다.

"서버"는 여러 사용자를 위해 네트워크 리소스를 관리하거나 제공하는 네트워크의 단일 물리적 컴퓨터 또는 장치를 의미합니다.

"서비스"는 Cisco 소프트웨어 구독 서비스를 의미합니다.

"서비스 설명"은 http://www.cisco.com/web/about/doing_business/legal/service_descriptions/index.html에서 확인할 수 있는 소프트웨어 구독 지원 서비스의 설명을 의미합니다.

"원격 분석 데이터"는 이메일 메시지와 웹 요청 속성에 있는 데이터 및 회사의 Cisco 하드웨어 제품이 처리한 이메일 메시지와 웹 요청의 다양한 유형에 대한 정보를 비롯한 회사의 이메일 및 웹 트래픽 샘플을 의미합니다. 원격 분석 데이터에 포함된 이메일 메시지 메타데이터 및 웹 요청은 개인적으로 식별 가능한 정보를 제거하도록 익명화되거나 난독 처리되었습니다.

"기간"은 주문 문서에 표시된 대로 귀하가 구매한 소프트웨어 구독 기간을 의미합니다.

"가상 어플라이언스"는 Cisco의 Email Security 어플라이언스, 웹 보안 어플라이언스 및 보안 관리 어플라이언스의 가상 버전을 의미합니다.

"가상 머신"은 자체 운영 체제를 실행하고 서버와 같은 애플리케이션을 실행할 수 있는 소프트웨어 컨테이너를 의미합니다.

추가 라이센스 사용 약관

라이센스 부여 및 데이터 수집에 동의

소프트웨어 라이센스.

소프트웨어 및 문서를 사용함으로써 회사는 본 계약의 약관에 동의하는 것으로 간주되며 회사가 본 계약을 준수하는 한 Cisco는 이 기간 동안 Cisco의 하드웨어 제품에서만 또는 최종 사용자에게 회사 서비스의 조항과 관련된 가상 컴퓨터의 가상 어플라이언스에서 소프트웨어를 사용할 수 있는 비독점적이고 2차 라이센스를 제공할 수 없고 양도할 수 없는 라이센스를 회사에 제공합니다. 소프트웨어 사용 라이센스를 부여받은 최종 사용자 수는 주문 문서에 지정된 최종 사용자의 수로 제한됩니다. 회사 서비스의 제공과 관련된 최종 사용자 수가 주문 문서에 지정된 최종 사용자 수를 초과하는 경우 회사는 승인된 제공원에 소프트웨어의 추가 라이센스 구매를 문의해야 합니다. 이 라이센스의 기간 및 범위는 주문 문서에 추가로 정의됩니다. 주문 문서는 소프트웨어 라이센스의 약관과 관련하여 EULA를 대체합니다. 본 계약에서 부여된 라이센스 권한을 제외한 모든 소프트웨어의 권한, 소유권 또는 이익은 Cisco, Cisco의 리셀러 또는 별도의 라이센스 허가자가 회사에 부여하지 않습니다. 소프트웨어 업그레이드 권한은 서비스 설명을 따릅니다. 본 계약 및 서비스는 함께 종료됩니다.

데이터 사용에 대한 동의 및 라이센스.

http://www.cisco.com/web/siteassets/legal/privacy.html에서 확인할 수 있는 Cisco 개인정보 보호정책에 따라 회사는 회사로부터 원격 분석 데이터를 수집하고 사용할 권한에 동의하고 이를 Cisco에 부여합니다. Cisco는 원격 분석 데이터에서 개인적으로 식별 가능한 정보를 수집하거나 사용하지 않습니다. Cisco는 타사와 집계된 익명 원격 분석 데이터를 공유하여 사용자 환경과 소프트웨어 및 기타 Cisco 보안 제품 및 서비스 개선을 지원할 수 있습니다. 회사는 소프트웨어에서 SenderBase 네트워크 참여 기능을 비활성화하여 원격 분석 데이터를 수집할 Cisco의 권한을 언제든지 종료할 수 있습니다. SenderBase 네트워크 참여 기능 활성화 또는 비활성화에 대한 지침은 소프트웨어 구성 설명서에서 확인할 수 있습니다.

기타 권한 및 의무 설명

Cisco Systems, Inc. 최종 사용자 라이센스 계약, 개인정보 보호정책 및 소프트웨어 구독 지원 서비스의 서비스 설명을 참조하십시오.

용 어 집

A

AMP(Advanced Malware Protection) 파일 평판 및 파일 분석 서비스입니다.

C

CIDR 표기법 CIDR(Classless Inter-Domain Routing)입니다. 임의 크기의 비트를 사용하여 네트워크 컨텍스트 내에서 IP 주소 범위를 설명하기 위한 편리한 표기법입니다. 이 표기법을 사용하여 슬래시(/) 뒤의 네트워크 부분에 사용되는 비트 수를 추가하여 주소의 네트워크 접두사 부분을 확인할 수 있습니다. 따라서 클래스 C 네트워크는 192.168.0.1/24와 같은 접두사 표기법으로 설명할 수 있습니다. 206.13.1.48/25의 CIDR 사양에는 주소의 첫 번째 25비트가 206.13.1.48의 첫 번째 25비트와 일치하는 모든 주소가 포함됩니다.

D

DLP 데이터 유출 방지입니다. RSA 보안 DLP 검사 엔진은 조직의 정보 및 지적 재산권을 보호하고 사용자가 민감한 데이터를 의도치 않게 이메일로 보내는 것을 방지하여 규제 및 조직의 규정 준수를 적용합니다.

DLP 사고 데이터 유출 방지 사고는 DLP 정책이 발송 메시지에서 주의해야 할 하나 이상의 DLP 위반을 탐지하는 경우 발생합니다.

DLP 정책 데이터 유출 방지 정책은 발송 메시지에 민감한 데이터가 포함되는지 여부와 AsyncOS가 이러한 데이터를 포함하는 메시지에서 수행하는 조치를 결정하는 데 사용되는 조건 집합입니다.

DLP 위험 계수 발송 메시지에서 탐지된 DLP 위반의 보안 위험을 나타내는 0부터 100까지의 점수입니다. 위험 계수에 따라 DLP 정책은 메시지에 수행할 조치를 결정합니다.

DLP 위반 조직의 DLP 규칙을 위반하는 메시지에서 발견되는 데이터의 인스턴스입니다.

DNS Domain Name System입니다. RFC 1045 및 RFC 1035를 참조하십시오. 네트워크의 DNS 서버는 IP 주소를 호스트 이름으로 확인하고 반대로 호스트 이름을 IP 주소로 확인합니다.

DoS 공격 서비스 거부 공격은 DDos(분산 서비스 거부 공격) 형태로도 가능합니다. 네트워크 또는 컴퓨터에 대한 공격의 주요 목표는 지정된 서비스에 대한 액세스를 방해하는 것입니다.

DSN 바운스된 메시지의 전송 상태 알림입니다.

E

Email Security Manager IronPort 어플라이언스에서 모든 이메일 보안 서비스 및 애플리케이션을 관리하기 위한 포괄적인 단일 대시보드입니다. Email Security Manager를 사용하면 고유의 인바운드 및 아웃바운드 정책을 통해 수신자별 또는 발신자별 기준에 따라 신종 바이러스 필터(Outbreak Filter), 안티스팸, 안티바이러스 및 이메일 콘텐츠 정책을 관리할 수 있습니다. *콘텐츠 필터*도 참조하십시오.

H

HAT Host Access Table입니다. HAT는 리스너에 대한 원격 호스트에서의 수신 연결을 제어하는 일련의 규칙을 유지 관리합니다. 각 *리스너*는 고유한 HAT를 보유합니다. HAT는 공용 및 개인 리스너마다 정의되며 *메일 흐름 정책*및 *발신자 그룹*을 포함합니다.

I

IDE 파일 바이러스 정의 파일입니다. IDE 파일에는 안티바이러스 소프트웨어가 바이러스를 탐지하기 위해 사용하는 서명 또는 정의가 들어 있습니다.

L

LDAP Lightweight Directory Access Protocol입니다. 개인(이메일 주소 등), 조직 및 인터넷 디렉토리 또는 인트라넷 디렉토리의 기타 리소스에 대한 정보에 액세스하는 데 사용되는 프로토콜입니다.

M

MAIL FROM *봉투 발신자*를 참조하십시오.

MTA 메일 전송 에이전트 또는 메시징 전송 에이전트입니다. 이메일 메시지를 수락, 라우팅 및 전송하는 프로그램입니다. 메일 사용자 에이전트(Mail User Agent, MTA) 또는 다른 MTA에서 메시지를 수신하는 즉시 MTA는 메시지를 일시적으로 로컬에 저장하고 수신자를 분석하며 다른 MTA에 라우트합니다(라우팅). 메시지 헤더를 수정 및/또는 추가할 수 있습니다. Cisco 어플라이언스는 엔터프라이즈 메시징 전용으로 특수한 랙마운트 서버 어플라이언스를 생성하기 위해 하드웨어, 강화된 운영 체제, 애플리케이션 및 지원 서비스를 통합하는 MTA입니다.

MUA 메일 사용자 에이전트(Mail User Agent)입니다. 사용자가 이메일 메시지를 작성하고 읽을 수 있도록 지원하는 프로그램입니다. MUA는 사용자 및 메시지 전송 에이전트간 인터페이스를 제공합니다. 발신 메일은 전송을 위해 최종적으로 MTA에 전달됩니다.

MX 레코드 지정한 도메인에 대한 메일 수락을 담당하는 인터넷상의 MTA를 지정합니다. 메일 교환 레코드는 도메인 이름에 대한 메일 경로를 만듭니다. 도메인 이름에는 우선순위 번호가 할당된 여러 메일 경로가 있을 수 있습니다. 가장 낮은 번호의 메일 경로는 도메인용 기본 서버를 식별합니다. 나열된 다른 메일 서버는 백업용으로 사용됩니다.

N

NTP Network Time Protocol입니다. `ntpconfig` 명령을 이용해 다른 컴퓨터와 시스템 시계를 동기화하기 위해 NTP(Network Time Protocol)를 사용하도록 IronPort AsyncOS를 구성합니다.

R

RAT Recipient Access Table입니다. Recipient Access Table은 어떤 수신자가 공용 리스너에서 수락되는지를 정의합니다. 이 테이블은 주소(일부 주소 또는 호스트 이름 가능)와 이 주소를 수락 또는 거부할지 여부를 지정합니다. 해당 수신자에 대한 RCPT TO 명령의 SMTP 응답을 선택적으로 포함할 수 있습니다. RAT는 일반적으로 로컬 도메인을 포함합니다.

RCPT TO *봉투 수신자*를 참조하십시오.

S

STARTTLS TLS(전송 계층 보안)는 SSL(Secure Socket Layer) 기술의 개선된 버전으로, 인터넷에서 SMTP 대화를 암호화하는 데 많이 사용되는 메커니즘입니다. IronPort AsyncOS 운영 체제는 RFC 2487에서 설명된 SMTP에 대한 STARTTLS 확장(TLS를 통한 보안 SMTP)을 지원합니다.

T

TOC 위협 운영 센터입니다. 바이러스 침투를 탐지하고 이에 대응하는 모든 인력, 툴, 데이터 및 기능을 의미합니다.

W

ㄱ

긍정 오류 스팸 또는 바이러스나 DLP 위반을 포함하는 것으로 잘못 분류된 메시지입니다.

ㄷ

대화식 바운스 SMTP 대화에서 발생하는 바운스입니다. 대화식 바운스의 두 가지 유형은 *하드 바운스*와 소프트 바운스입니다.

디바운스 시간 제한 시스템에서 동일한 경고를 사용자에게 전송하지 않는 시간(초)입니다.

ㄹ

로그 서브스크립션 Cisco 어플라이언스의 성능을 모니터링하는 로그 파일을 생성합니다. 로그 파일은 로컬 디스크에 저장되며 원격 시스템에서도 전송 및 저장 가능합니다. 로그 설정의 일반적인 특성에는 이름, 모니터링할 구성 요소(이메일 운영, 서버), 형식 및 전송 방법이 포함됩니다.

리스너 리스너는 특정 IP 인터페이스에 구성할 이메일 처리 서비스를 설명합니다. 리스너는 사용자 네트워크 내부의 내부 시스템 또는 인터넷에서 Cisco 어플라이언스로 수신되는 이메일에만 적용됩니다. IronPort AsyncOS는 리스너를 사용하여 메시지가 승인되고 수신자 호스트로 릴레이되기 위해 만족해야 하는 기준을 지정합니다. 리스너는 "이메일 인젝터" 또는 사용자가 지정한 각 IP 주소에 대해 실행되는 "SMTP 데몬"으로도 생각할 수 있습니다.

IronPort AsyncOS는 기본적으로 인터넷에서 이메일을 수신하기 위한 특성을 지니고 있는 *공용* 리스너와 내부(그룹 웨어, POP/IMAP 및 기타 메시지 생성) 시스템에서만 이메일을 수락하는 *개인* 리스너 간의 차이점을 구분합니다.

ㅁ

메일 흐름 정책 메일 흐름 정책은 *리스너*에 대한 *HAT*(Host Access Table) 매개변수(뒤에 *속도 제한* 매개변수 및 사용자 지정 SMTP 코드 및 응답이 오는 액세스 규칙)의 그룹을 표현하는 방식입니다. 이와 함께 *발신자 그룹* 및 메일 흐름 정책이 리스너의 HAT에 정의되어 있습니다. Cisco 어플라이언스는 리스너에 대한 사전 정의된 메일 흐름 정책 및 발신자 그룹과 함께 제공됩니다.

문자 집합(더블바이트) 더블바이트 문자 집합은 각 문자를 표현하기 위해 1바이트를 초과하는 정보가 필요한 외국어 문자 집합입니다.

ㅂ

발신자 그룹 발신자 그룹은 간단하게 말해 해당 발신자의 이메일을 동일한 방식으로 처리하기 위해(즉, 발신자 그룹에 메일 흐름 정책 적용) 수집한 발신자 목록입니다. 발신자 그룹은 리스너의 HAT(Host Access Table)에서 쉼표로 구분되는 발신자 목록(IP 주소, IP 범위, 호스트/도메인, SenderBase Reputation Service 분류, SenderBase Reputation 점수 범위 또는 DNS 목록 쿼리 응답으로 식별됨)입니다. 발신자 그룹의 이름과 *메일 흐름 정책*을 할당할 수 있습니다.

봉투 발신자 MAIL FROM: SMTP 명령에 정의되어 있는 이메일 메시지의 발신자입니다. 경우에 따라 "Mail From" 또는 "Envelope From" 주소라고도 합니다.

봉투 수신자 RCPT TO: SMTP 명령에 정의되어 있는 이메일 메시지의 수신자입니다. 경우에 따라 "Recipient To" 또는 "Envelope To" 주소라고도 합니다.

부정 오류 스팸 메시지 또는 바이러스나 탐지되지 않은 DLP 위반을 포함하는 메시지입니다.

블랙리스트 알려진 악의적인 발신자 목록입니다. 기본적으로, 공용 리스너의 블랙리스트 발신자 그룹에 속하는 발신자는 $BLOCKED *메일 흐름 정책*에 설정된 매개변수에 따라 거부됩니다.

비대화식 바운스 수신자 호스트가 전송을 위해 메시지를 수락한 이후 메시지가 반환되어 발생하는 바운스입니다. 소프트 바운스(4XX) 또는 하드 바운스(5XX)가 가능합니다. 수신자 메시지로 수행해야 할 작업(예: 소프트 바운스 수신자 메시지 재전송 및 데이터베이스에서 하드 바운스 수신자 제거)을 결정하기 위해 바운스 응답을 분석할 수 있습니다.

ㅅ

소프트 바운스 메시지 구성된 *최대 재시도 횟수*또는 *최대 큐 시간*에 기반하여 이후에 메시지 전송이 재시도됩니다.

속도 제한 속도 제한은 세션당 최대 메시지 수, 메시지당 최대 수신자 수, 최대 메시지 크기, 시간당 최대 수신자 및 원격 호스트에서 수락할 최대 동시 연결 수를 제한합니다.

수신 IP 인터페이스에 구성된 특정 리스너에서 이메일 메시지를 수신하는 작업입니다. Cisco 어플라이언스는 이메일 메시지를 수신할 리스너를 인터넷의 인바운드 또는 내부 시스템의 아웃바운드 중에서 구성합니다.

스팸 원치 않는 상업용 대량 이메일(UCE/UBE)입니다. 안티스팸 검사에서 필터링 규칙에 따라 스팸으로 의심되는 이메일 메시지를 확인합니다.

신종 바이러스 필터 (Outbreak Filter) IronPort의 신종 바이러스 필터(Outbreak Filter) 기능은 바이러스로부터 추가적인 보호 레이어를 제공합니다. 신종 바이러스 필터(Outbreak Filter) 기능은 업데이트된 바이러스 IDE를 사용할 수 있거나 메시지가 위협이 아니라고 판단될 때까지 메시지를 보류하여 의심스러운 이메일 메시지를 격리합니다.

ㅇ

안티바이러스 Sophos 및 McAfee 안티바이러스 검사 엔진은 플랫폼 간 안티바이러스 보호, 탐지 및 치료 기능을 제공합니다. 바이러스 탐지 엔진을 통해 파일에 바이러스, 트로이 목마 및 웜이 있는지 검사합니다. 이러한 프로그램들은 일반적으로 *악성코드*로 분류되며, 이는 "악성 소프트웨어"를 의미합니다. 모든 종류의 악성코드 간 유사성으로 인해 안티바이러스 스캐너가 바이러스뿐 아니라 모든 종류의 악성 소프트웨어를 탐지하고 제거할 수 있습니다.

오픈 릴레이 오픈 릴레이(종종 "안전하지 않은 릴레이" 또는 "타사" 릴레이라고도 함)는 이메일 메시지의 확인되지 않은 타사 릴레이를 허용하는 SMTP 이메일 서버입니다. 로컬 사용자에게 보내지 않은 이메일 또는 로컬 사용자가 보내지 않은 이메일을 처리함으로써 오픈 릴레이는 알 수 없는 발신자가 *게이트웨이*를 통해 대량의 이메일(일반적으로 *스팸*)을 라우팅하도록 할 수 있습니다. `listenerconfig` 및 `systemsetup` 명령을 사용하여 시스템이 의도치 않게 오픈 릴레이로 구성되는 것을 방지합니다.

ㅈ

전달 특정 IP 인터페이스에서 Cisco 어플라이언스의 내부 메일 호스트 또는 수신자 도메인에 이메일 메시지를 전달하는 동작입니다. Cisco 어플라이언스는 가상 게이트웨이 기술을 사용하여 동일한 물리적 시스템 내의 여러 IP 인터페이스에서 메시지를 전달할 수 있습니다. 각 가상 게이트웨이에는 고유한 IP 주소, 호스트 이름 및 도메인, 이메일 큐가 포함되어 있으며 가상 게이트웨이별로 다양한 메일 흐름 정책 및 검사 전략을 구성할 수 있습니다.

원격 호스트에 대한 최대 동시 연결, 호스트에 대한 최대 동시 연결의 가상 게이트웨이별 제한사항, 원격 호스트에 대한 대화의 암호화 여부를 포함하여 Cisco 어플라이언스가 수행하는 메시지 전달 작업 구성을 맞춤 조정할 수 있습니다.

정규화된 도메인 이름 (FQDN) 최상위 도메인 이름을 비롯해 모든 상위 수준의 도메인 이름을 포함하는 도메인 이름입니다. 예를 들어 `mail3.example.com`은 192.168.42.42의 *호스트*에 대한 정규화된 도메인 이름이며 `example.com`은 example.com *도메인*의 정규화된 도메인 이름입니다. 정규화된 도메인 이름은 인터넷에서 고유해야 합니다.

지연된 바운스 SMTP 대화에서 발생하는 바운스입니다. 수신자 호스트는 전송할 메시지를 수락하며 이후에 바운스를 수행합니다.

ㅊ

최대 재시도 횟수 *하드 바운스*되기 전 *소프트 바운스* 메시지가 재전송 시도되는 최대 횟수입니다.

최대 큐 시간 *소프트 바운스* 메시지가 *하드 바운스*되기 전에 *전송*되기 위해 이메일 큐에서 대기하는 최대 시간입니다.

ㅋ

콘텐츠 일치 분류자 RSA 데이터 유출 방지 검사 엔진의 탐지 구성 요소입니다. 분류자에는 지원 데이터를 검색하는 컨텍스트 규칙과 함께 민감한 데이터를 탐지하기 위한 여러 가지 규칙이 포함됩니다. 예를 들어, 신용 카드 분류자는 신용 카드 번호와 일치하는 문자열을 포함하는 메시지 뿐만 아니라 만료일, 신용 카드 회사명 또는 주소 등의 지원 정보를 포함하는 메시지가 필요합니다.

콘텐츠 필터 콘텐츠 기반 필터는 이메일 파이프라인에서 작업 큐의 수신자 별 검사 단계 동안 메시지를 처리하기 위해 사용됩니다. 콘텐츠 필터는 메시지 필터링 이후 호출되고 분리된 개별 메시지에 적용됩니다.

큐 Cisco 어플라이언스에서 이메일 큐에 있는 메시지를 삭제, 바운스, 일시 중단 또는 리디렉션할 수 있습니다. 대상 제어에 대한 메시지의 이메일 큐를 *전송 큐*라고도 합니다. IronPort Anti-Spam 또는 메시지 필터 작업에서 처리되기 위해 대기 중인 메시지 큐를 *작업 큐*라고도 합니다. `status detail` 명령을 사용하여 두 가지 큐의 상태를 볼 수 있습니다.

ㅍ

평판 필터 평판을 기준으로 의심스러운 발신자를 필터링하는 방법입니다. SenderBase Reputation Service는 원격 호스트의 연결 IP 주소에 기반하여 의심스러운 *스팸*을 거부하거나 "스로틀"할 수 있도록 정확하고 유연한 방식을 제공합니다.

ㅎ

하드 바운스 메시지 영구적으로 전송할 수 없는 메시지입니다. 이것은 SMTP 대화 도중 또는 이후에 발생할 수 있습니다.

허용된 호스트 개인 리스너를 통해 Cisco 어플라이언스를 사용하는 이메일 릴레이가 허용되는 컴퓨터입니다. 허용된 호스트는 호스트 이름 또는 IP 주소로 정의됩니다.

화이트리스트 알려진 선의의 발신자 목록입니다. 신뢰하는 발신자를 화이트리스트 *발신자 그룹*에 추가합니다. $TRUSTED 메일 흐름 정책은 신뢰하는 발신자의 이메일에 *속도 제한*을 사용하지 않고 해당 발신자의 콘텐츠를 안티스팸 검사 대상에 포함하지 않도록 구성됩니다.

인 덱 스

기호

숫자

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

기호 / 버튼

T

U

V

W

X

ㄱ

ㄴ

ㄷ

ㄹ

ㅂ

ㅅ

O

ㅈ

ㅊ

ㅋ

ㅌ

ㅍ

ㅎ