ASA FirePOWER 모듈 사용 설명서

버전 5.4.1
2015년 1월 22일

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.

동봉된 제품의 소프트웨어 라이센스 및 제한 보증은 제품과 함께 제공되는 정보 패킷에 설명되어 있으며 본 참조 문서에 통합되어 있습니다. 소프트웨어 라이센스 또는 제한 보증을 찾을 수 없는 경우 CISCO 담당자에게 사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 University of California, Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 언급된 기타 모든 보증에도 불구하고 이러한 공급자의 모든 문서 및 소프트웨어는 모든 결함이 포함된 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

Cisco 또는 해당 공급업체는 피해의 가능성에 대해 언급한 경우라도 이 설명서의 사용 또는 사용 불능으로 인해 발생하는 이익 손실, 데이터 손실 또는 손상을 포함하여(단, 이에 한하지 않음) 간접, 특별, 중대 또는 부수적 손해에 대해 어떠한 경우라도 책임을 지지 않습니다.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 보려면 다음 URL로 이동하십시오. www.cisco.com/go/trademarks 여기에 언급된 서드파티 상표는 해당 소유권자의 자산입니다. 파트너라는 용어의 사용이 Cisco와 다른 업체 사이의 제휴 관계를 의미하는 것은 아닙니다. (1110R)

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

목 차

CiscoASA FirePOWER 모듈 소개

CiscoASA FirePOWER 모듈®은 Cisco ASA5506-X 디바이스에 구축할 수 있는 모듈입니다. 이 모듈은 사용자 조직의 보안 정책-네트워크 보호를 위한 지침을 준수하는 방식으로 네트워크 트래픽 처리를 도울 수 있도록 설계되었습니다. 보안 정책에는 직원의 조직 시스템 이용 지침을 제공하는 AUP(Acceptable Use Policy)도 포함됩니다.

이 설명서는 기능의 onbox 구성 및 ASDM를 통해 액세스 가능한 ASA FirePOWER 모듈기능에 대한 정보를 제공합니다. 각 장의 설명 텍스트, 다이어그램 및 절차는 사용자 인터페이스를 탐색하고, 시스템 성능을 최대화하고, 복잡한 문제를 해결하는 데 도움이 되는 자세한 정보를 제공합니다.

참고 ASA FirePOWER 모듈을 호스팅하는 ASA에서 명령 권한을 활성화할 경우, ASA FirePOWER 홈, 구성 및 모니터링 페이지를 볼 수 있는 권한 레벨 15의 사용자 이름으로 로그인해야 합니다. 상태 페이지를 제외하고 ASA FirePOWER 페이지에 대한 읽기 전용 또는 모니터링 전용 액세스는 지원되지 않습니다.

다음 항목은 ASA FirePOWER 모듈을 소개하고, 주요 구성 요소에 대해 설명하며 이 가이드의 사용 방법을 이해하도록 도와줍니다.

ASA FirePOWER 모듈 소개

ASA FirePOWER 모듈은 분석을 위한 트래픽 모니터링 네트워크 세그먼트에 설치된 ASA 디바이스에서 실행됩니다.

인라인으로 구축된 시스템은 네트워크에서 트래픽이 들어오고 나가고 통과하는 방법을 세부적으로 지정할 수 있는 *액세스 제어*를 사용하여 트래픽의 흐름에 영향을 미칠 수 있습니다. 네트워크 트래픽에 대해 수집하는 데이터 및 여기에서 가져오는 모든 정보를 사용하여 다음을 기반으로 트래픽을 필터링 및 제어할 수 있습니다.

- 소스와 목적지, 포트, 프로토콜 등 간단하고 쉽게 결정되는 전송 및 네트워크 레이어 특성
- 평판, 위험, 사업 타당성, 사용된 애플리케이션 또는 방문한 URL 등의 특성을 비롯하여 트래픽에 대한 최신 상황 정보
- 조직의 Microsoft Active Directory LDAP 사용자(서로 다른 사용자에게 여러 액세스 레벨 허용 가능)

각 유형의 트래픽 검사와 제어는 유연성과 성능을 최대화할 수 있는 방식으로 발생합니다. 예를 들어 평판 기반의 블랙리스트 추가는 단순한 소스 및 목적지 데이터를 사용하므로 프로세스 초기에 금지된 트래픽을 차단할 수 있는 반면, 침입과 익스플로잇의 탐지 및 차단은 최후의 방어 수단입니다.

ASA FirePOWER 모듈 구성 요소

다음 항목은 조직의 보안, 허용되는 사용 정책 및 트래픽 관리 전략에 기여하는 ASA FirePOWER 모듈의 주요 기능에 대해 설명합니다.

액세스 제어

*액세스 제어*는 네트워크를 통과할 수 있는 트래픽을 지정하고, 검사하고 로깅할 수 있는 정책 기반 기능입니다. *액세스 제어 정책*에 따라 시스템이 네트워크의 트래픽을 처리하는 방식이 결정됩니다.

가장 간단한 액세스 제어 정책은 *기본 작업*을 사용하여 모든 트래픽을 처리합니다. 이 기본 작업을 설정하여 모든 트래픽을 차단하거나 추가 검사 없이 신뢰할 수 있고, 트래픽을 검사하여 침입을 탐지할 수 있습니다.

액세스 제어 정책이 보다 복잡할 경우 트래픽이 보안 인텔리전스 데이터에 근거하여 차단 목록에 추가되고 *액세스 제어 규칙*을 통해 네트워크 트래픽 로깅 및 처리가 세부적으로 제어될 수도 있습니다. 이러한 규칙은 간단하거나 복잡할 수 있으며, 여러 기준을 사용하여 트래픽과 일치시키고 검사합니다. 사용자는 보안 영역, 네트워크 또는 지리적 위치, 포트, 애플리케이션, 요청된 URL 및 사용자별로 트래픽을 제어할 수 있습니다. 고급 액세스 제어 옵션은 전처리 및 성능을 포함합니다.

각 액세스 제어 규칙에는 일치하는 트래픽의 모니터링, 신뢰, 차단 또는 허용 여부를 결정하는 *작업*이 있습니다. 트래픽을 허용할 때, 익스플로잇, 악성코드 또는 금지 파일이 자산에 도달하거나 네트워크를 빠져나가기 전에 이를 차단할 수 있도록 침입 또는 파일 정책으로 시스템이 먼저 검사하도록 지정할 수 있습니다.

침입 탐지 및 방지

침입 탐지와 방지는 트래픽이 목적지로 들어가기 전 시스템의 최후의 방어선입니다. *침입 정책*은 액세스 제어 정책에 의해 호출되는 침입 탐지 및 방지 구성의 정의된 세트입니다. 침입 정책은 *침입 규칙* 및 기타 설정을 사용하여 트래픽에서 보안 위반을 검사하고, 인라인 구축 시 악성 트래픽을 차단 또는 변경할 수 있습니다.

시스템 제공 정책이 조직의 보안 요구를 충분히 충족하지 못하는 경우, 사용자 지정 정책을 사용하면 사용자 환경에서 시스템 성능을 개선할 수 있으며 네트워크에서 발생하는 악성 트래픽과 정책 위반을 집중적으로 관찰할 수 있습니다. 사용자 지정 정책을 생성 및 조정함으로써, 시스템이 네트워크의 트래픽에서 침입을 처리하고 검사하는 방법을 매우 세밀하게 구성할 수 있습니다.

Advanced Malware Protection 및 파일 제어

악성코드의 효과를 식별 및 완화할 수 있도록 ASA FirePOWER 모듈의 파일 제어 및 Advanced Malware Protection 구성 요소는 네트워크 트래픽의 파일(악성코드 파일 및 보관 파일 내 중첩된 파일 포함) 전송을 탐지, 추적, 캡처, 분석하고 선택적으로 차단할 수 있습니다.

파일 제어

*파일 제어*를 사용하면 사용자가 특정 애플리케이션 프로토콜에서 특정 유형의 파일을 업로드(전송) 또는 다운로드(수신)하는 것을 디바이스가 탐지하고 차단할 수 있습니다. 파일 제어를 전반적 액세스 제어 구성의 일부로 구성하고, 액세스 제어 규칙과 연결된 파일 정책이 규칙 조건을 충족하는 네트워크 트래픽을 검사합니다.

네트워크 기반 AMP(Advanced Malware Protection)

네트워크 기반 *AMP(Advanced Malware Protection)*를 사용하면 몇 가지 유형의 파일로 된 악성코드의 네트워크 트래픽을 검사할 수 있습니다.

탐지된 파일의 저장 여부와 상관없이, 파일을 종합적 보안 인텔리전스 클라우드에 제출하여 파일의 SHA-256 해시값으로 알려진 속성 조회를 간단히 수행할 수 있습니다. 이 컨텍스트 정보를 바탕으로 시스템을 구성하여 특정 파일을 차단 또는 허용할 수 있습니다.

악성코드 차단을 전반적 액세스 제어 구성의 일부로 구성하면 액세스 제어 규칙과 연결된 파일 정책이 규칙 조건을 충족하는 네트워크 트래픽을 검사합니다.

애플리케이션 프로그래밍 인터페이스

API(애플리케이션 프로그래밍 인터페이스)를 사용하여 시스템과 상호 작용하는 몇 가지 방법이 있습니다. 자세한 내용은 다음 Support Sites(지원 사이트) 중 하나에서 추가 문서를 다운로드할 수 있습니다.

- **Sourcefire:** (https://support.sourcefire.com/)
- **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

라이센스 규칙

섹션 시작 시 License(라이센스) 문서는 다음과 같이 섹션에 설명된 기능을 사용하기 위해 필요한 라이센스를 나타냅니다.

보호

보호 라이센스를 사용하면 디바이스가 침입 탐지 및 방지, 파일 제어, Security Intelligence(보안 인텔리전스) 필터링을 수행할 수 있습니다.

제어

제어 라이센스를 통해 디바이스가 사용자 및 애플리케이션 제어를 수행할 수 있습니다. 제어 라이센스에는 보호 라이센스가 필요합니다.

URL 필터링

URL 필터링 라이센스는 디바이스가 정기적으로 업데이트되는 클라우드 기반 카테고리 및 평판 데이터를 사용하여 모니터링되는 호스트에서 요청한 URL을 기준으로 네트워크를 이동할 수 있는 트래픽을 결정하도록 허용합니다. URL 필터링 라이센스에는 보호 라이센스가 필요합니다.

악성코드

악성코드 라이센스는 디바이스가 네트워크 기반 AMP를 수행하도록 허용합니다. 네트워크 기반 AMP란 네트워크에 전송된 파일에서 악성코드를 탐지 및 차단하는 것입니다. 또한 네트워크에서 전송된 파일을 추적하는 전파 흔적 분석을 볼 수 있습니다. 악성코드 라이센스에는 보호 라이센스가 필요합니다.

허용된 기능은 대개 추가된 것이기 때문에, 이 문서는 각 기능을 위해 가장 필요한 라이센스만을 제공합니다. 예를 들어 기능에 보호 및 제어 라이센스가 필요한 경우 제어만 나열됩니다. 그러나, 추가된 것이 아닌 라이센스가 기능에 필요한 경우, 문서는 이들을 더하기(+) 문자를 넣어서 나열합니다.

License(라이센스) 문서 내 "또는" 문장은 섹션에 설명된 기능을 사용하기 위해 특정 라이센스가 필요하지만 추가 라이센스는 기능을 추가할 수 있습니다. 예를 들어, 파일 정책 내 일부 파일 규칙 작업에는 보호 라이센스가 필요한 반면, 일부에는 악성코드 라이센스가 필요합니다. 따라서, 파일 규칙 상 문서에 대한 License(라이센스) 문서는 “보호 또는 악성코드”를 나열합니다.

IP 주소 규칙

IPv4 클래스리스 도메인 간 라우팅(CIDR) 표기법 및 유사한 IPv6 접두사 길이 표기법을 사용하여 ASA FirePOWER 모듈의 여러 위치에서 주소 블록을 정의할 수 있습니다.

CIDR 표기법은 비트 마스크에 통합된 네트워크 IP 주소를 사용하여 지정된 주소 블록에서 IP 주소를 정의합니다. 예를 들어, 다음 표는 CIDR 표기법의 개인 IPv4 주소 공간을 나열합니다.

표 1-1 CIDR 표기법 구문 예

CIDR 블록	CIDR 블록 내 IP 주소	서브넷 마스크	IP 주소의 수
10.0.0.0/8	10.0.0.0 - 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0/12	172.16.0.0 - 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 - 192.168.255.255	255.255.0.0	65,536

마찬가지로, IPv6은 접두사 길이에 통합된 네트워크 IP 주소를 사용하여 지정된 주소 블록 안에서 IP 주소를 정의합니다. 예를 들어, 2001:db8::/32는 2001:db8:: 네트워크에서 32비트의 접두사 길이로 IPv6 주소를 지정하는데, 이는, 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff를 통한 2001:db8::입니다.

CIDR 또는 접두사 길이 표기법을 사용하여 IP 주소 블록을 지정하려는 경우, ASA FirePOWER 모듈은 마스크 또는 접두사 길이에 의해 지정된 네트워크 IP 주소의 일부**만** 사용합니다. 예를 들어, 10.1.2.3/8을 입력한 경우, ASA FirePOWER 모듈은 10.0.0.0/8을 사용합니다.

즉 Cisco는 CIDR 또는 접두사 길이 표기법을 사용하는 경우 비트 경계에 있는 네트워크 IP 주소를 사용하는 표준 방식을 권장하지만 ASA FirePOWER 모듈은 이를 요구하지 않습니다.

2 장

재사용 가능한 개체 관리

향상된 유연성 및 사용 편의성을 위해, ASA FirePOWER 모듈에서는 사용자가 명명된 *개체*를 생성할 수 있는데, 이는 해당 값을 사용하고자 할 때 명명된 개체를 대신 사용할 수 있도록 이름을 값과 연결하는 재사용 가능한 구성입니다.

다음과 같은 유형의 개체를 만들 수 있습니다.

- IP 주소 및 네트워크, 포트/프로토콜 쌍, 보안 영역 및 원래/대상 국가(위치 정보)를 나타내는 네트워크 기반 개체
- Security Intelligence(보안 인텔리전스) 피드와 목록, 애플리케이션 필터, URL, 파일 목록 및 침입 정책 변수 집합을 포함하여 트래픽 처리를 지원하는 개체

ASA FirePOWER 모듈의 다양한 위치에서 이 개체를 사용할 수 있습니다. 여기에는 액세스 제어 정책, 네트워크 분석 정책, 침입 정책 및 규칙 보고서, 대시보드 등이 포함됩니다.

개체 그룹화는 단일 구성으로 여러 개체를 참조하도록 허용합니다. 네트워크, 포트, 그리고 URL 개체를 정렬할 수 있습니다.

참고 대부분의 경우, 정책에서 사용되는 개체를 수정하려면 변경 사항을 적용하기 위해 정책을 재적용해야 합니다. 보안 영역을 수정하는 경우에도 적절한 디바이스 구성을 재적용해야 합니다.

자세한 내용은 다음 섹션을 참고하십시오.

개체 관리자 사용

라이센스: 모두

개체 관리자(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 사용하여 애플리케이션 필터, 변수 집합 및 보안 영역을 포함하는 개체를 만들고 관리합니다. 네트워크, 포트 및 URL 개체를 그룹화할 수 있습니다. 또한 개체 및 개체 그룹 목록을 정렬하고, 필터링하고, 검색할 수 있습니다.

자세한 내용은 다음을 참고하십시오.

- 2-2페이지의 개체 내 그룹
- 2-3페이지의 개체 검색, 정렬, 필터링

개체 내 그룹

라이센스: 모두

네트워크, 포트 및 URL 개체를 그룹화할 수 있습니다. 시스템을 통해 개체 및 개체 그룹을 같은 의미로 사용할 수 있습니다. 예를 들어, 포트 개체를 사용하는 모든 곳에서 포트 개체 그룹을 사용할 수 있습니다. 유형이 동일한 개체 및 개체 그룹이 동일한 이름을 가질 수 없습니다.

정책에서 사용되는 개체 그룹(예: 액세스 제어 정책에서 사용되는 네트워크 개체 그룹)을 수정할 때, 변경 사항을 적용하려면 정책을 재적용해야 합니다.

그룹을 삭제해도 그룹 내 개체는 삭제되지 않으며, 개체 간 연결만 삭제됩니다. 또한, 사용 중인 그룹을 삭제할 수 없습니다. 예를 들어 저장한 액세스 제어 정책의 URL 조건에서 사용 중인 URL 그룹을 삭제할 수 없습니다.

재사용 가능한 개체를 그룹화하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 그룹화하려는 **Network(네트워크)**, **Port(포트)** 또는 **URL** 개체의 유형에서, **Object Groups(개체 그룹)**를 선택합니다.

그룹화하는 개체 유형의 페이지가 나타납니다.

단계 3 그룹화할 개체에 해당하는 **Add(추가)** 버튼을 클릭합니다.

그룹을 만들 수 있는 팝업 창이 나타납니다.

단계 4 그룹의 **Name(이름)**을 입력합니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 모두 사용할 수 있습니다.

단계 5 하나 이상의 개체를 선택하고 **Add(추가)**를 클릭합니다.

- 여러 개체를 선택하려면, Shift와 Ctrl 키를 사용하거나, 마우스 오른쪽 단추를 클릭한 후 **Select All(모두 선택)**을 선택합니다.
- 기존 개체를 포함하여 검색하려면 필터 필드( )를 사용합니다. 이는 일치하는 항목을 표시하기 위해 입력 시 업데이트됩니다. 검색 필드 위에 있는 다시 로드 아이콘( )을 클릭하거나 검색 필드에서 지우기 아이콘( )을 클릭하여 검색 문자열을 지웁니다.
- 어떤 기존 개체도 요구 사항을 충족하지 않는 경우 추가 아이콘( )을 클릭하여 상황에 따라 개체를 생성합니다.

단계 6 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

그룹이 생성됩니다.

개체 검색, 정렬, 필터링

라이센스: 모두

개체 관리자는 페이지당 20개의 개체 또는 그룹을 표시합니다. 모든 유형의 개체 또는 그룹이 20개 이상 있는 경우, 추가 페이지를 보려면 페이지 하단의 탐색 링크를 사용합니다. 또한 특정 페이지로 이동하거나 새로 고침 아이콘( )을 클릭하여 보기를 새로 고칠 수 있습니다.

기본적으로, 페이지는 개체 및 그룹을 이름의 알파벳 순으로 나열합니다. 그러나, 표시되는 모든 열에 따라 각 유형의 개체 또는 그룹을 정렬할 수 있습니다. 열 제목 옆에 있는 위쪽(▲) 또는 아래쪽(▼) 화살표는 페이지가 해당 방향에서 해당 열을 기준으로 정렬된다는 것을 나타냅니다. 또한 페이지의 개체를 이름 또는 값으로 필터링할 수 있습니다.

개체 또는 그룹을 정렬하려면 다음을 수행합니다.

단계 1 열 제목을 클릭합니다. 반대 방향으로 정렬하려면, 제목을 다시 클릭합니다.

개체 또는 그룹을 필터링하려면 다음을 수행합니다.

단계 1 **Filter(필터)** 필드에 필터 기준을 입력합니다.

일치하는 항목을 입력하여 표시하면 페이지가 업데이트됩니다. 필드는 하나 이상의 별표(*)를 와일드 카드로 수용합니다.

네트워크 개체 작업

라이센스: 모두

네트워크 개체는 개별적으로 또는 주소 블록으로 지정할 수 있는 하나 이상의 IP 주소를 나타냅니다. 네트워크 개체 및 그룹(2-2페이지의 개체 내 그룹 참고)을 ASA FirePOWER 모듈 내 여러 위치에서 사용할 수 있습니다. 여기에는 액세스 제어 정책, 네트워크 변수, 침입 규칙, 보고서 등이 포함됩니다.

사용 중인 네트워크 개체를 삭제할 수 없습니다. 또한, 액세스 제어 또는 침입 정책에서 사용되는 네트워크 개체를 수정한 후 변경 사항을 적용하려면 정책을 재적용해야 합니다.

네트워크 개체를 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 **Network(네트워크)**에서, **Individual Objects(개별 개체)**를 선택합니다.

단계 3 **Add Network(네트워크 추가)**를 클릭합니다.

Network Objects(네트워크 개체) 팝업 창이 나타납니다.

단계 4 네트워크 개체의 **Name(이름)**을 입력합니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 모두 사용할 수 있습니다.

단계 5 네트워크 개체에 추가하고자 하는 각 IP 주소 또는 주소 블록에 대해 해당 값을 입력하고 **Add(추가)**를 클릭합니다.

단계 6 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

네트워크 개체가 추가됩니다.

보안 인텔리전스 목록 및 피드 작업

라이센스: 보호

액세스 제어 정책에 따라 보안 인텔리전스 기능을 사용하면 소스 또는 대상 IP 주소를 기준으로 네트워크를 통과시킬 트래픽을 지정할 수 있습니다. 이는 액세스 제어 규칙에 의해 트래픽이 분석되기 전에 특정 IP 주소를 오가는 트래픽을 거부하거나 차단 목록에 추가하려는 경우에 특히 유용합니다. 이와 마찬가지로, IP 주소를 허용 목록에 추가하여 시스템이 액세스 제어를 사용하여 연결을 강제로 처리하도록 할 수 있습니다.

특정 IP 주소를 차단 목록에 추가하기를 원하는지 확신할 수 없는 경우 시스템이 액세스 제어를 사용하여 연결을 처리하도록 허용하는 "모니터링 한정" 설정을 사용할 수 있으며, 차단 목록에 연결의 일치 항목을 로깅할 수도 있습니다.

모든 액세스 제어 정책에는 *전역 허용 목록* 및 *전역 차단 목록*이 기본적으로 포함되어 있으며, 모든 영역에 적용됩니다. 또한 각 액세스 제어 정책 내에서 네트워크 개체와 그룹, Security Intelligence(보안 인텔리전스) 목록 및 피드를 조합하여 별도의 허용 목록 및 차단 목록을 생성할 수 있으며, 이러한 모든 항목은 보안 영역으로 제한할 수 있습니다.

피드 및 목록 비교

보안 인텔리전스 *피드*는 사용자가 구성한 간격에서 시스템이 HTTP 또는 HTTPS 서버로부터 다운로드하는 IP 주소의 동적 컬렉션입니다. 피드는 정기적으로 업데이트되므로 시스템은 최신 정보를 사용하여 네트워크 트래픽을 필터링할 수 있습니다. 차단 목록 작성을 지원하기 위해 ASA FirePOWER 모듈은 *인텔리전스 피드*를 제공하며, 여기에는 VRT가 평판이 좋지 않은 것으로 판단한 IP 주소가 나와 있습니다.

피드 업데이트가 적용되는 데는 몇 분이 걸릴 수 있지만, 피드를 만들거나 변경한 다음 또는 예약된 피드 업데이트 후에 액세스 제어 정책을 재적용할 필요가 없습니다.

참고 시스템이 인터넷에서 피드를 다운로드할 때 엄격한 제어를 원할 경우, 해당 피드에 대한 자동 업데이트를 비활성화할 수 있습니다. 그러나 Cisco는 자동 업데이트를 허용할 것을 권장합니다. 온디맨드 업데이트를 수동으로 수행할 수 있지만, 시스템이 정기적으로 피드를 다운로드할 수 있도록 하면 관련된 최신 데이터를 제공받을 수 있습니다.

Security Intelligence(보안 인텔리전스) *목록*은 피드와 대조적으로, 사용자가 시스템에 수동으로 업로드하는 IP 주소에 대한 간단한 정적 목록입니다. 사용자 지정 목록을 사용하여 피드와 전역 허용 목록 및 차단 목록을 늘리고 미세 조정합니다. (네트워크 개체를 수정하고 전역 허용 또는 차단 목록에서 IP 주소를 제거할 뿐만 아니라) 사용자 지정 목록을 수정하려면 액세스 제어 정책을 재적용해야 변경 사항이 적용된다는 점에 유의하십시오.

서식 설정 및 손상된 피드 데이터

피드 및 목록 소스는 회선 당 1개의 IP 주소 또는 주소 블록을 가진, 500MB 미만의 간단한 텍스트 파일이어야 합니다. 코멘트 행은 반드시 # 문자로 시작해야 합니다. 목록 소스 파일은 반드시 .txt 확장자를 사용해야 합니다.

시스템이 손상된 피드 또는 인식할 수 있는 IP 주소가 없는 피드를 다운로드하는 경우, (처음 다운로드가 아니라면) 시스템은 오래된 피드 데이터를 계속해서 사용합니다. 그러나, 시스템이 피드에서 IP 주소를 하나라도 인식할 수 있는 경우, 인식할 수 있는 주소를 업데이트합니다.

인터넷 액세스 및 고가용성

시스템은 포트 443/HTTPS를 사용하여 인텔리전스 피드를 다운로드하고 443/HTTP 또는 80/HTTP를 사용하여 사용자 지정 피드 또는 서드파티 피드를 다운로드합니다. 피드를 업데이트하려면 디바이스에서 인바운드 및 아웃바운드 모두로 해당 포트를 열어야 합니다. 시스템에 피드 사이트에 대한 직접 액세스 기능이 없는 경우 프록시 서버를 사용할 수 있습니다.

참고 시스템은 사용자 지정 피드를 다운로드할 때 P2P SSL 인증서 확인을 수행하지 **않습니다**. 또한 시스템은 원격 피어를 확인하는 인증서 번들 또는 자체 서명된 인증서를 사용하도록 지원하지 않습니다.

피드 및 목록 관리

개체 관리자의 Security Intelligence(보안 인텔리전스) 페이지를 사용하여 Security Intelligence(보안 인텔리전스) 개체로 총괄하여 명명된 Security Intelligence(보안 인텔리전스) 목록 및 피드를 작성 및 관리합니다. (네트워크 개체 및 그룹 생성 및 관리에 대한 자세한 내용은 2-3페이지의 네트워크 개체 작업을 참고하십시오.)

저장 또는 적용된 액세스 제어 정책에서 현재 사용되고 있는 사용자 지정 목록 또는 피드를 삭제할 수 없습니다. 또한 개별 IP 주소를 제거할 수 있지만, 전역 목록을 삭제할 수는 없습니다. 마찬가지로, 인텔리전스 피드를 삭제할 수 없지만, 이를 수정하면 해당 업데이트의 빈도를 비활성화하거나 변경할 수 있습니다.

보안 인텔리전스 개체 빠른 참조

다음 표에서는 보안 인텔리전스 필터링을 수행하는 데 사용할 수 있는 개체에 대한 빠른 참조를 제공합니다.

표 2-1 보안 인텔리전스 개체 기능

기능	전역 허용 목록 또는 차단 목록	인텔리전스 피드	사용자 지정 피드	사용자 지정 목록	네트워크 개체
사용 방법	액세스 제어 정책에서 기본값으로 사용	액세스 제어 정책에서 허용 목록 또는 차단 목록 개체로 사용			
보안 영역에 의한 제한 가능 여부	아니요	예	예	예	예
삭제 가능 여부	아니요	아니요	예(저장 또는 적용된 액세스 제어 정책에서 현재 사용되지 않는 경우에만 해당)		
개체 관리자 수정 기능	IP 주소만 삭제	비활성화 또는 업데이트 빈도 변경	전체 변경	수정된 목록만 업로드	전체 변경
수정할 경우 액세스 정책 제어 재적용 필요 여부	삭제할 경우 필요(IP 주소 추가 시에는 재적용이 필요하지 않음)	아니요	아니요	예	예

Security Intelligence(보안 인텔리전스) 목록 및 피드의 생성, 관리, 사용에 대한 자세한 내용은 다음을 참고하십시오.

- 2-6페이지의 전역 허용 목록 및 차단 목록 작업
- 2-6페이지의 인텔리전스 피드 작업
- 2-7페이지의 사용자 지정 보안 인텔리전스 피드 작업
- 2-8페이지의 보안 인텔리전스 피드 수동 업데이트
- 2-8페이지의 사용자 지정 보안 인텔리전스 목록 작업
- 5-1페이지의 보안 인텔리전스 IP 주소 평판을 사용한 차단 목록 추가

전역 허용 목록 및 차단 목록 작업

라이센스: 보호

시스템의 전역 허용 목록 및 차단 목록은 각각의 액세스 제어 정책에 기본적으로 포함되어 있으며 모든 영역에 적용됩니다. 정책별로 전역 목록을 사용하지 않도록 선택할 수 있습니다.

전역 목록에 IP 주소를 추가한 후 액세스 제어 정책을 재적용할 필요는 없습니다. 반대로, 전역 허용 또는 차단 목록에서 IP 주소를 삭제한 후 액세스 제어 정책을 적용해야 변경 사항이 적용됩니다.

허용 목록 또는 차단 목록에 /0의 넷마스크를 가진 네트워크 개체를 추가할 수 있지만, 해당 개체 내 `/0` 넷마스크를 사용한 주소 블록은 무시되며 허용 목록 및 차단 목록 필터링은 해당 주소에 기반하여 발생하지 않는다는 점을 참고하십시오. 보안 인텔리전스 피드에서 `/0` 넷마스크를 가진 주소 블록 또한 무시됩니다. 정책이 대상으로 하는 모든 트래픽을 모니터링하거나 차단하려는 경우, **Monitor(모니터링)** 또는 **Block(차단)** 규칙 작업과 함께 각각의 액세스 제어 정책을 사용하거나, **any**(기본값)를 사용하여 보안 인텔리전스 필터링 대신에 **Source Networks(소스 네트워크)** 및 **Destination Networks(대상 네트워크)**를 사용합니다.

전역 허용 목록 또는 차단 목록에서 IP 주소를 제거하려면 다음을 수행합니다.

단계 1 개체 관리자의 Security Intelligence(보안 인텔리전스) 페이지에서 전역 허용 목록 및 차단 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

Global Whitelist(전역 허용 목록) 또는 Global Blacklist(전역 차단 목록) 팝업 창이 나타납니다.

단계 2 이 목록에서 제거할 IP 주소 옆에 있는 삭제 아이콘( )을 클릭합니다.

여러 IP 주소를 한 번에 삭제하려면, Shift와 Ctrl 키를 사용하여 선택한 후 마우스 오른쪽 단추를 클릭하고 **Delete(삭제)**를 선택합니다.

단계 3 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

변경 사항이 저장되지만 액세스 제어 정책을 적용해야 변경 사항이 적용됩니다.

인텔리전스 피드 작업

라이센스: 보호

차단 목록 작성을 지원하기 위해 ASA FirePOWER 모듈은 인텔리전스 피드를 제공하며, 이는 VRT가 평판이 좋지 않은 것으로 판단한 IP 주소가 정기적으로 업데이트된 여러 목록으로 구성되어 있습니다. 피드의 각 목록은 특정 카테고리, 즉, 오픈 릴레이, 알려진 공격, bogon(bogus IP 주소) 등을 나타냅니다. 액세스 제어 정책에서 카테고리 중 하나 또는 전체를 차단 목록에 추가할 수 있습니다.

인텔리전스 피드는 정기적으로 업데이트되므로, 시스템은 최신 정보를 사용하여 네트워크 트래픽을 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 IP 주소는 새로운 정책을 업데이트하고 적용하는 것보다 빠르게 나타났다가 사라질 수 있습니다.

Intelligence Feed(인텔리전스 피드)를 삭제할 수 없지만, 이를 수정하면 해당 업데이트의 빈도를 변경할 수 있습니다. 기본적으로, 피드는 매 2시간마다 업데이트됩니다.

인텔리전스 피드의 업데이트 빈도를 수정하려면 다음을 수행합니다.

단계 1 개체 관리자의 Security Intelligence(보안 인텔리전스) 페이지에서 인텔리전스 피드 옆에 있는 수정 아이콘( )을 클릭합니다.

Security Intelligence(보안 인텔리전스) 팝업 창이 나타납니다.

단계 2 **Update Frequency(업데이트 빈도)**를 수정합니다.

2시간부터 1주까지 다양한 간격을 선택할 수 있습니다. 또한 피드 업데이트를 비활성화할 수 있습니다.

단계 3 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

변경 내용이 저장됩니다.

사용자 지정 보안 인텔리전스 피드 작업

라이센스: 보호

사용자 지정 또는 서드파티 보안 인텔리전스 피드를 사용하면 인터넷에서 정기적으로 업데이트되며, 평판이 좋은 다른 허용 목록 및 차단 목록으로 인텔리전스 피드를 늘릴 수 있습니다. 또한 내부 피드를 설정할 수 있습니다.

피드를 구성할 때, URL을 사용하여 해당 위치를 지정합니다. URL은 Punycode로 인코딩된 것이 아니어야 합니다. 기본적으로, 시스템은 사용자가 구성한 간격에서 전체 피드 소스를 다운로드합니다.

또는, 시스템이 md5 체크섬을 사용하도록 구성하여 업데이트된 피드를 다운로드할지 결정할 수 있습니다. 모듈이 피드를 마지막으로 다운로드한 이후로 체크섬이 변경되지 않는 경우, 시스템이 이를 다시 다운로드할 필요는 없습니다. 특히 내부 피드가 클 경우 md5 체크섬을 사용할 수 있습니다. md5 체크섬은 오직 체크섬으로만 간편한 텍스트 파일로 저장해야 합니다. 코멘트가 지원되지 않습니다.

보안 인텔리전스 피드를 구성하려면 다음을 수행합니다.

단계 1 개체 관리자의 Security Intelligence(보안 인텔리전스) 페이지에서 **Add Security Intelligence(보안 인텔리전스 추가)**를 클릭합니다.

Security Intelligence(보안 인텔리전스) 팝업 창이 나타납니다.

단계 2 피드의 **Name(이름)**을 입력합니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 모두 사용할 수 있습니다.

단계 3 **Type(유형)** 드롭다운 목록에서 **Feed(피드)**를 구성할 것인지 지정합니다.

새 옵션으로 팝업 창이 업데이트됩니다.

단계 4 **Feed URL(피드 URL)**을 지정하고, 선택적으로, **MD5 URL**을 지정합니다.

단계 5 **Update Frequency(업데이트 빈도)**를 선택합니다.

2시간부터 1주까지 다양한 간격을 선택할 수 있습니다. 또한 피드 업데이트를 비활성화할 수 있습니다.

단계 6 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

보안 인텔리전스 피드 개체가 생성됩니다. 피드 업데이트를 비활성화하지 않는 한, 시스템은 피드를 다운로드하고 확인하려고 시도합니다. 이제 액세스 제어 정책에서 피드 개체를 사용할 수 있습니다.

보안 인텔리전스 피드 수동 업데이트

라이센스: 보호

수동으로 보안 인텔리전스 피드를 업데이트하면 인텔리전스 피드를 포함하는 모든 피드가 업데이트됩니다.

모든 보안 인텔리전스 피드를 업데이트하려면 다음을 수행합니다.

단계 1 개체 관리자의 Security Intelligence(보안 인텔리전스) 페이지에서 **Update Feeds(피드 업데이트)**를 클릭합니다.

단계 2 모든 피드를 업데이트할 것인지 확인합니다.

확인 대화 상자가 나타나고 업데이트를 적용하는 데 몇 분 정도 걸릴 수 있음을 경고하는 메시지가 나타납니다.

단계 3 **OK(확인)**를 클릭합니다.

시스템이 피드 업데이트를 다운로드하고 확인한 후, 업데이트된 피드를 사용하여 트래픽 필터링을 시작합니다.

사용자 지정 보안 인텔리전스 목록 작업

라이센스: 보호

Security Intelligence(보안 인텔리전스) 목록은 사용자가 수동으로 업로드하는 IP 주소와 주소 블록에 대한 간단한 정적 목록입니다. 사용자 지정 목록은 피드 또는 전역 목록 중 하나를 보완하고 미세 조정할 경우에 유용합니다.

주소 블록에 대한 넷마스크는 IPv4 및 IPv6의 경우 각각 `0~32` 또는 `0~128`의 정수일 수 있다는 점에 유의하십시오.

예를 들어, 평판이 좋은 피드가 중요한 리소스에 액세스하는 것을 잘못 차단하고 있지만 사용자 조직에 전반적으로 유용한 경우, Security Intelligence(보안 인텔리전스) 피드 개체를 액세스 제어 정책의 차단 목록에서 제거하는 대신 잘못 분류된 IP 주소만 포함하는 사용자 지정 허용 목록을 생성할 수 있습니다.

Security Intelligence(보안 인텔리전스) 목록을 수정하려면 소스 파일을 변경하고 새 복사본을 업로드해야 한다는 점에 유의하십시오. 자세한 내용은 2-9페이지의 보안 인텔리전스 목록 업데이트를 참고하십시오.

새 Security Intelligence(보안 인텔리전스) 목록을 업로드하려면 다음을 수행합니다.

단계 1 개체 관리자의 Security Intelligence(보안 인텔리전스) 페이지에서 **Add Security Intelligence(보안 인텔리전스 추가)**를 클릭합니다.

Security Intelligence(보안 인텔리전스) 팝업 창이 나타납니다.

단계 2 목록의 **Name(이름)**을 입력합니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 모두 사용할 수 있습니다.

단계 3 **Type(유형)** 드롭다운 목록에서 **List(목록)**를 업로드할 것인지 지정합니다.

새 옵션으로 팝업 창이 업데이트됩니다.

단계 4 **Browse(찾아보기)**를 클릭하여 목록에서 `.txt` 파일을 탐색한 후 **Upload(업로드)**를 클릭합니다.

목록이 업로드됩니다. 팝업 창은 시스템이 목록에서 발견한 IP 주소 및 주소 블록의 총 수를 표시합니다.

예상한 숫자가 아닌 경우, 파일의 형식을 확인하고 다시 시도하십시오.

단계 5 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

Security Intelligence(보안 인텔리전스) 목록 개체가 저장됩니다. 이제 액세스 제어 정책에서 사용할 수 있습니다.

보안 인텔리전스 목록 업데이트

라이센스: 보호

Security Intelligence(보안 인텔리전스) 목록을 수정하려면 소스 파일을 변경하고 새 복사본을 업로드해야 합니다. ASDM를 사용하여 파일의 내용을 수정할 수 없습니다. 소스 파일에 액세스할 수 없는 경우, ASDM 인터페이스를 사용하여 복사본을 다운로드할 수 있습니다.

Security Intelligence(보안 인텔리전스) 목록을 수정하려면 다음을 수행합니다,

단계 1 개체 관리자의 Security Intelligence(보안 인텔리전스) 페이지에서 업데이트할 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

Security Intelligence(보안 인텔리전스) 팝업 창이 나타납니다.

단계 2 목록의 복사본을 수정해야 하는 경우, 텍스트 파일로 목록을 저장하려면 **Download(다운로드)**를 클릭한 후, 프롬프트를 따라야 합니다.

단계 3 필요에 따라 목록을 변경합니다.

단계 4 Security Intelligence(보안 인텔리전스) 팝업 창에서 **Browse(찾아보기)**를 클릭하여 수정된 목록을 탐색한 후 **Upload(업로드)**를 클릭합니다.

목록이 업로드됩니다.

단계 5 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

변경 내용이 저장됩니다. 목록이 활성 액세스 제어 정책에서 사용되고 있는 경우 변경 사항을 적용하려면 정책을 적용해야 합니다.

포트 개체 작업

라이센스: 모두

포트 개체는 여러 프로토콜을 조금씩 다른 방법으로 나타냅니다.

- TCP와 UDP의 경우, 포트 개체는 연결된 포트 또는 포트 범위(선택 사항)와 함께 괄호 안에 프로토콜 번호로 전송 레이어 프로토콜을 나타냅니다. 예: `TCP(6)/22`
- ICMP 및 ICMPv6(IPv6-ICMP)의 경우, 포트 개체는 유형 및 코드(선택 사항)와 함께 인터넷 레이어 프로토콜을 나타냅니다. 예: `ICMP(1):3:3`
- 포트 개체는 또한 포트를 사용하지 않는 다른 프로토콜을 나타낼 수 있습니다.

시스템은 잘 알려진 포트에 기본 포트 개체를 제공한다는 점에 유의하십시오. 이 개체를 수정 또는 삭제할 수 있지만, Cisco는 사용자 지정 포트 개체를 만들 것을 권장합니다.

포트 개체 및 그룹(2-2페이지의 개체 내 그룹 참고)을 ASA FirePOWER 모듈의 다양한 위치에서 사용할 수 있습니다. 여기에는 액세스 제어 정책, 그리고 포트 변수, 및 이벤트 검색이 포함됩니다.

사용 중인 포트 개체를 삭제할 수 없습니다. 또한, 액세스 제어에서 사용되는 포트 개체를 수정한 후, 변경 사항을 적용하려면 정책을 재적용해야 합니다.

액세스 제어 규칙에서 소스 포트 조건의 TCP 또는 UDP 이외의 다른 프로토콜을 추가할 수 없습니다. 또한, 규칙에서 소스 및 대상 포트 조건을 모두 설정할 때 전송 프로토콜을 조합할 수 없습니다.

소스 포트 상태에서 사용되는 포트 개체 그룹에 지원되지 않는 프로토콜을 추가한 경우, 사용되는 규칙은 정책 적용 시 반영되지 않습니다. 또한, TCP와 UDP 포트를 모두 포함하는 포트 개체를 만들고 이를 규칙의 소스 포트 조건으로 추가하는 경우 대상 포트를 추가할 수 없으며, 그 반대도 마찬가지입니다.

포트 개체를 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 **Port(포트)**에서, **Individual Objects(개별 개체)**를 선택합니다.

단계 3 **Add Port(포트 추가)**를 클릭합니다.

Port Objects(포트 개체) 팝업 창이 나타납니다.

단계 4 포트 개체의 **Name(이름)**을 입력합니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 모두 사용할 수 있습니다.

단계 5 **Protocol(프로토콜)**을 선택합니다.

TCP, **UDP**, **IP**, **ICMP** 또는 **IPv6-ICMP**를 신속하게 선택하거나 **기타** 드롭다운 목록을 사용하여 다른 프로토콜 또는 **모든** 프로토콜을 선택할 수 있습니다.

단계 6 또는, **Port(포트)** 또는 포트 범위를 사용하여 TCP 또는 UDP 포트 개체를 제한합니다.

1에서 65535까지 포트를 지정하거나 모든 포트에 일치하도록 `any`를 지정할 수 있습니다. 포트 범위를 지정하려면 하이픈을 사용합니다.

단계 7 또는, **Type(유형)**를 사용하여 ICMP 또는 IPv6-ICMP 포트 개체를 제한하고 해당하는 경우 관련 **Code(코드)**를 사용합니다.

ICMP 또는 IPv6-ICMP 개체를 생성할 때, 유형을 지정할 수 있고 해당하는 경우 코드도 지정할 수 있습니다. ICMP 유형과 코드에 관한 자세한 정보는 http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml 및 http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml을 참고하십시오. 유형을 any로 설정하여 모든 유형에 일치하도록 하거나 코드를 any로 설정하여 특정 유형의 모든 코드에 일치하도록 할 수 있습니다.

단계 8 또는, 드롭다운 목록에서 **Other(기타)** 및 프로토콜을 선택합니다. **All(모든)** 프로토콜을 선택한 경우, **Port(포트)** 필드에 포트 번호를 입력합니다.

단계 9 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

포트 개체가 추가됩니다.

URL 개체 작업

라이센스: 모두

사용자가 구성한 각 URL 개체는 단일 URL 또는 IP 주소를 나타냅니다. URL 개체 및 그룹(2-2페이지의 개체 내 그룹 참고)을 액세스 제어 정책에서 사용할 수 있습니다. 예를 들어, 특정 URL을 차단하는 액세스 제어 규칙을 작성할 수 있습니다.

HTTPS 트래픽을 차단하기 위해 해당 트래픽에 대해 SSL(Secure Sockets Layer) 인증서의 URL을 입력할 수 있다는 점에 유의하십시오. 인증서의 URL을 입력할 경우, 도메인 이름을 입력하고 하위 도메인 정보를 생략합니다. (예를 들어, `www.example.com` 대신 `example.com`을 입력합니다.) 인증서 URL에 따라 트래픽을 차단하는 경우, 해당 웹 사이트로 연결된 HTTP 및 HTTPS 트래픽 모두 차단됩니다.

사용 중인 URL 개체를 삭제할 수 없습니다. 또한, 액세스 제어에서 사용되는 URL 개체를 수정한 후 , 변경 사항을 적용하려면 정책을 재적용해야 합니다.

URL 개체를 추가하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 **URL**에서, **Individual Objects(개별 개체)**를 선택합니다.

단계 3 **Add URL(URL 추가)**을 클릭합니다.

URL Objects(URL 개체) 팝업 창이 나타납니다.

단계 4 URL 개체의 **Name(이름)**을 입력합니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 모두 사용할 수 있습니다.

단계 5 URL 개체에 대한 **URL** 또는 IP 주소를 입력합니다.

단계 6 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

URL 개체가 추가됩니다.

애플리케이션 필터 작업

라이센스: 모두

ASA FirePOWER 모듈이 IP 트래픽을 분석할 경우, 네트워크에서 일반적으로 사용되는 애플리케이션을 식별하려고 시도합니다. 애플리케이션 인식은 애플리케이션 기반 액세스 제어를 수행하기 위한 중요한 요소입니다. 시스템은 여러 애플리케이션에 대한 탐지기를 제공하며, Cisco는 자주 업데이트되어 시스템 및 취약점 데이터베이스(VDB) 업데이트를 통해 추가 탐지기를 추가합니다.

애플리케이션은 애플리케이션의 위험, 사업 타당성, 유형, 카테고리 및 태그와 관련된 기준에 따라 그룹 애플리케이션을 필터링합니다. 애플리케이션 필터를 사용하면 애플리케이션을 개별적으로 검색하고 추가할 필요가 없기 때문에 액세스 제어 규칙의 애플리케이션 조건을 신속하게 생성할 수 있습니다. 자세한 내용은 8-3페이지의 애플리케이션 필터를 통한 트래픽 일치를 참고하십시오.

애플리케이션 필터 사용의 또 다른 장점은 새로운 애플리케이션을 변경하거나 추가할 때 필터를 사용한 액세스 제어 규칙을 업데이트하지 않아도 된다는 것입니다. 예를 들어 모든 소셜 네트워킹 애플리케이션을 차단하기 위해 액세스 제어 정책을 설정하고 VDB 업데이트에 새 소셜 네트워킹 애플리케이션 탐지기가 포함되어 있는 경우 VDB를 업데이트할 때 정책이 업데이트됩니다. 시스템에서 새 애플리케이션을 차단하기 전에 정책을 재적용해야 하지만, 애플리케이션을 차단하는 액세스 제어 규칙을 업데이트할 필요가 없습니다.

Cisco가 제공한 애플리케이션 필터가 필요에 따라 애플리케이션을 정렬하지 않는 경우, 사용자 고유의 필터를 만들 수 있습니다, 사용자가 정의한 필터는 ASA FirePOWER 모듈이 제공한 필터를 정렬 및 결합할 수 있습니다. 예를 들어, 위험도가 높고 사업 관련성이 낮은 모든 애플리케이션을 차단하도록 허용하는 필터를 만들 수 있습니다. 모듈 소프트웨어 또는 VDB를 업데이트할 때 해당 필터가 자동으로 업데이트되지 **않는다**는 점을 숙지해야 하지만 개별 애플리케이션을 수동으로 지정하여 필터를 생성할 수도 있습니다.

ASA FirePOWER 모듈이 제공한 애플리케이션 필터와 마찬가지로 액세스 제어 규칙에서 사용자가 정의한 애플리케이션 필터를 사용할 수 있습니다.

개체 관리자(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**)를 사용하여 애플리케이션 필터를 생성하고 관리할 수 있습니다. 또한 애플리케이션 조건을 액세스 제어 규칙에 추가하면서 애플리케이션 필터를 생성할 수 있다는 점을 참고하십시오.

애플리케이션 필터 목록에는 ASA FirePOWER 모듈이 제공한 애플리케이션 필터가 포함되어 있는데 사용자가 이를 선택하여 자체 필터를 구축할 수 있습니다. 검색 문자열을 사용하여 나타나는 필터를 제한할 수 있습니다. 이는 카테고리 및 태그에 특히 유용합니다.

Available Applications(가용 애플리케이션) 목록에는 선택한 필터의 개별 애플리케이션이 포함되어 있습니다. 또한 검색 문자열을 사용하여 표시되는 애플리케이션을 제한할 수 있습니다.

시스템은 동일한 필터 유형의 여러 필터를 OR 연산자와 연결합니다. 중간 위험도 필터에 100개의 애플리케이션이 포함되어 있고 고위험도 필터에 50개의 애플리케이션이 포함되어 있는 시나리오를 고려하십시오. 두 필터를 모두 선택하는 경우, 시스템은 150개의 가용 애플리케이션을 표시합니다.

시스템은 서로 다른 유형의 필터를 AND 작업과 연결합니다. 예를 들어, 중간 위험도 및 고위험도 필터와 중간 수준 및 높은 수준의 사업 타당성 필터를 선택하는 경우, 시스템은 중간 또는 높은 위험을 가진 애플리케이션과 중간 또는 높은 사업 타당성을 가진 애플리케이션을 표시합니다.

팁 관련 애플리케이션에 대한 자세한 내용을 보려면 정보 아이콘( )을 클릭합니다. 추가 정보를 표시하려면, 표시되는 팝업의 인터넷 검색 링크를 클릭합니다.

필터에 추가할 애플리케이션을 결정한 후 이들을 개별적으로 추가할 수 있으며, 애플리케이션 필터를 선택한 경우, **필터와 일치하는 모든 앱**을 추가할 수도 있습니다. 선택한 애플리케이션 및 필터 목록의 총 항목 수가 50을 초과하지 않는 한, 여러 필터 및 여러 애플리케이션을 어떤 조합으로나 추가할 수 있습니다.

애플리케이션 필터를 만든 후에는, 개체 관리자의 Application Filters(애플리케이션 필터) 페이지에 나열됩니다. 페이지는 각 필터를 구성하는 조건의 총 수를 표시합니다.

표시되는 애플리케이션 필터를 분류하고 필터링하는 것에 관한 자세한 내용은 2-2페이지의 개체 관리자 사용을 참고하십시오. 사용 중인 애플리케이션 필터를 삭제할 수 없습니다. 또한, 액세스 제어 정책에서 사용된 애플리케이션 필터를 수정한 후 변경 사항을 적용하려면 정책을 재적용해야 합니다.

애플리케이션 필터를 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 **Application Filters(애플리케이션 필터)**를 클릭합니다.

Application Filters(애플리케이션 필터) 섹션이 나타납니다.

단계 3 **Add Application Filter(애플리케이션 필터 추가)**를 클릭합니다.

Application Filter(애플리케이션 필터) 팝업 창이 나타납니다.

단계 4 필터에 **Name(이름)**을 입력합니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 모두 사용할 수 있습니다.

단계 5 또는, ASA FirePOWER 모듈이 제공한 필터를 **Application Filters(애플리케이션 필터)** 목록에서 사용하여 필터에 추가할 애플리케이션 목록을 축소합니다.

- 목록을 확장 및 축소하려면 각 필터 유형 옆에 있는 화살표를 클릭합니다.
- 필터 유형을 마우스 오른쪽 단추로 클릭하고 **Check All(모두 선택)** 또는 **Uncheck All(모두 선택 취소)**을 클릭합니다. 목록은 각 유형의 필터를 얼마나 많이 선택했는지를 나타낸다는 점에 유의하십시오.
- 나타나는 필터를 축소하려면, **Search by name(이름으로 검색)** 필드에 검색 문자열을 입력합니다. 이는 카테고리 및 태그에 특히 유용합니다. 검색을 지우려면, 지우기 아이콘( )을 클릭합니다.
- 필터 목록을 새로 고침하고 선택한 모든 필터를 지우려면 다시 로드 아이콘( )을 클릭합니다.
- 모든 필터 및 검색 필드를 지우려면, **Clear All Filters(모든 필터 지우기)**를 클릭합니다.

선택한 필터와 일치하는 애플리케이션이 Available Applications(가용 애플리케이션) 목록에 나타납니다. 목록은 한 번에 100개의 애플리케이션을 표시합니다.

단계 6 **Available Applications(가용 애플리케이션)** 목록에서 필터에 추가하려는 애플리케이션을 선택합니다.

- 이전 단계에서 지정한 제약 조건을 충족하는 모든 애플리케이션을 추가하려면 **All apps matching the filter(필터와 일치하는 모든 앱)**을 선택합니다.
- 표시되는 개별 애플리케이션을 축소하려면, **Search by name(이름으로 검색)** 필드에 검색 문자열을 입력합니다. 검색을 지우려면, 지우기 아이콘( )을 클릭합니다.
- 개별 가용 애플리케이션 목록을 조회하려면 목록 하단의 페이징 아이콘을 사용합니다.
- 여러 개별 애플리케이션을 선택하려면 Ctrl 및 Shift 키를 사용합니다. 현재 표시된 개별 애플리케이션을 **Select All(모두 선택)**하려면 마우스 오른쪽 단추를 클릭합니다.
- 애플리케이션을 새로 고침하고 선택한 모든 애플리케이션을 지우려면 다시 로드 아이콘( )을 클릭합니다.

개별 애플리케이션과 **All apps matching the filter(필터와 일치하는 모든 앱)**를 동시에 선택할 수는 없습니다.

단계 7 선택한 애플리케이션을 필터에 추가합니다. 클릭하여 드래그하거나 **Add to Rule(규칙에 추가)**을 클릭할 수 있습니다.

결과는 다음의 조합과 같습니다.

- 선택한 Application Filters(애플리케이션 필터)
- 선택한 개별 Available Applications(가용 애플리케이션), 또는 **All apps matching the filter(필터와 일치하는 모든 앱)**

필터에 최대 50개의 애플리케이션과 필터를 추가할 수 있습니다. 선택한 애플리케이션에서 애플리케이션 또는 필터를 삭제하려면, 해당 삭제 아이콘( )을 클릭합니다. 하나 이상의 애플리케이션 및 필터를 선택하거나 마우스 오른쪽 단추를 클릭하여 **모두 선택**한 후 마우스 오른쪽 단추를 클릭하여 **선택한 항목을 삭제**할 수 있습니다.

단계 8 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

애플리케이션 필터가 저장됩니다.

변수 집합 작업

라이센스: 보호

변수는 소스 및 대상 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 또한 침입 정책 내 변수를 사용하여 규칙 삭제, 적응형 프로파일 및 동적 규칙 상태의 IP 주소를 나타낼 수 있습니다.

팁 전처리기 규칙은 침입 규칙에서 사용되는 네트워크 변수에 의해 정의된 호스트에 관계없이 이벤트를 트리거할 수 있습니다.

변수 집합을 사용하여 변수를 관리하고, 사용자 정의하며, 정렬합니다. ASA FirePOWER 모듈에서 제공하는 기본 변수 집합을 사용하거나 사용자 고유의 집합을 생성할 수 있습니다. 모든 설정에서 미리 정의된 기본 변수를 수정하고 사용자가 정의한 변수를 추가 및 수정할 수 있습니다.

대부분의 공유 객체 규칙 및 표준 텍스트 규칙은 ASA FirePOWER 모듈에서 제공하는 것으로 미리 정의된 기본 변수를 사용하여 네트워크와 포트 번호를 정의합니다. 예를 들어, 대부분의 규칙은 `$HOME_NET` 변수를 사용하여 보호된 네트워크를 지정하고 `$EXTERNAL_NET` 변수를 사용하여 보호되지 않은(또는 외부) 네트워크를 지정합니다. 또한, 전문 규칙은 종종 미리 정의된 다른 변수를 사용합니다. 예를 들어, 웹 서버에 대한 익스플로잇을 탐지하는 규칙은 `$HTTP_SERVERS` 및 `$HTTP_PORTS` 변수를 사용합니다.

규칙은 변수가 더 정확하게 네트워크 환경을 반영할 때 더욱 효과적입니다. 최소한, 2-15페이지의 미리 정의된 기본 변수 최적화에 설명된 대로 기본값 집합의 기본 변수를 변경해야 합니다. `$HOME_NET`과 같은 변수가 올바르게 네트워크를 정의하고 `$HTTP_SERVERS`가 네트워크에서 모든 웹 서버를 포함한다는 것을 확인함으로써 프로세스가 최적화되고 모든 관련 시스템에서 의심스러운 활동이 감시됩니다.

변수를 사용하려면, 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업과 관련된 침입 정책에 변수 집합을 연결합니다. 기본적으로, 기본 변수 집합은 액세스 제어 정책에 의해 사용된 모든 침입 정책에 연결됩니다.

자세한 내용은 다음 섹션을 참고하십시오.

미리 정의된 기본 변수 최적화

라이센스: 보호

기본적으로, ASA FirePOWER 모듈은 단일 기본 변수 집합을 제공하는데, 이는 미리 정의된 기본 변수로 구성되어 있습니다. VRT(취약성 연구단)는 규칙 업데이트를 사용하여 기본 변수를 포함하는 새롭고 업데이트된 침입 규칙 및 다른 침입 정책 요소를 제공합니다. 자세한 내용은 35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기를 참고하십시오.

ASA FirePOWER 모듈을 통해 제공되는 대부분의 침입 규칙이 미리 정의된 기본 변수를 사용하기 때문에, 이러한 변수에 적절한 값을 설정해야 합니다. 네트워크의 트래픽을 확인하기 위해 변수 집합을 사용하는 방법에 따라 일부 또는 전체 변수 집합에서 이 기본 변수의 값을 수정할 수 있습니다. 자세한 내용은 2-21페이지의 변수 추가 및 수정을 참고하십시오.

주의 액세스 제어 정책 또는 침입 정책을 가져오는 경우, 기본 변수 집합의 기존 기본 변수를 가져온 기본 변수로 덮어씁니다. 기존 기본 변수 값 집합이 가져온 기본 변수 값 집합에 없는 사용자 지정 변수를 포함하는 경우, 고유 변수는 유지됩니다. 자세한 내용은 B-3페이지의 구성 가져오기를 참고하십시오.

다음 표는 ASA FirePOWER 모듈이 제공한 변수를 설명하고 어떤 변수를 일반적으로 수정하는지를 나타냅니다. 네트워크에 맞게 변수를 조정하는 방법을 확인하는 데 대한 지원을 받으려면 Professional Services(전문 서비스) 또는 Support(지원부)에 문의하십시오.

표 2-2 ASA FirePOWER 모듈에서 제공하는 변수

변수 이름	설명	수정 여부
$AIM_SERVERS	알려진 AIM(AOL Instant Messenger) 서버에 대해 정의하며, 채팅 기반 규칙 및 AIM 익스플로잇을 검색하는 규칙에서 사용됩니다.	필요하지 않음
$DNS_SERVERS	DNS(Domain Name Service) 서버에 대해 정의합니다. 특히 DNS 서버에 영향을 미치는 규칙을 작성하는 경우, $DNS_SERVERS 변수를 대상 또는 소스 IP 주소로 사용할 수 있습니다.	현재 규칙 집합에서 필요하지 않습니다.
$EXTERNAL_NET	ASA FirePOWER 모듈이 보호되지 않은 네트워크로 간주하는 네트워크에 대해 정의하며, 외부 네트워크에 대해 정의하는 여러 규칙에서 사용됩니다.	예, $HOME_NET을 적절하게 정의한 후 $EXTERNAL_NET에 대한 값에서 $HOME_NET을 제외해야 합니다.

표 2-2 ASA FirePOWER 모듈에서 제공하는 변수 (계속)

변수 이름	설명	수정 여부
$FILE_DATA_PORTS	네트워크 스트림에서 파일을 탐지하는 침입 규칙에 사용되는 암호화되지 않은 포트에 대해 정의합니다.	필요하지 않음
$FTP_PORTS	네트워크에서 FTP 서버의 포트에 대해 정의하고, FTP 서버 익스플로잇 규칙에 사용됩니다.	예(FTP 서버가 기본 포트 이외의 포트를 사용할 경우), 모듈 인터페이스에서 기본 포트를 확인할 수 있습니다.
$GTP_PORTS	패킷 디코더가 GTP(GPRS[General Radio Packet Service] 터널링 프로토콜) PDU 내의 페이로드를 추출하는 데이터 채널 포트에 대해 정의합니다.	필요하지 않음
$HOME_NET	관련된 침입 정책이 모니터링하는 네트워크에 대해 정의하며, 내부 네트워크를 정의하는 많은 규칙에서 사용됩니다.	예(내부 네트워크에 대한 IP 주소를 포함할 경우)
$HTTP_PORTS	네트워크에서 웹 서버의 포트에 대해 정의하고, 웹 서버 익스플로잇 규칙에 사용됩니다.	예(웹 서버가 기본 포트 이외에 포트를 사용할 경우), 모듈 인터페이스에서 기본 포트를 확인할 수 있습니다.
$HTTP_SERVERS	네트워크에서 웹 서버에 대해 정의합니다. 웹 서버 익스플로잇 규칙에 사용합니다.	예(HTTP 서버를 실행하는 경우)
$ORACLE_PORTS	네트워크에서 Oracle(오라클) 데이터베이스 서버 포트에 대해 정의하고, Oracle(오라클) 데이터베이스 공격을 검색하는 규칙에서 사용됩니다.	예(Oracle(오라클) 서버를 실행하는 경우)
$SHELLCODE_PORTS	시스템이 셸 코드 코드 익스플로잇을 검색하기를 원하는 포트에 대해 정의하고, 셸 코드를 사용하는 익스플로잇을 탐지하는 규칙에서 사용됩니다.	필요하지 않음
$SIP_PORTS	네트워크에서 SIP 서버 포트에 대해 정의하고, SIP 익스플로잇 규칙에 사용됩니다.	필요하지 않음
$SIP_SERVERS	네트워크에서 SIP 서버에 대해 정의하고, SIP를 표적으로 삼은 익스플로잇을 해결하는 규칙에서 사용됩니다.	예(SIP 서버를 실행하는 경우), $HOME_NET을 적절하게 정의한 후 $HOME_NET을 $SIP_SERVERS에 대한 값으로 포함해야 합니다.
$SMTP_SERVERS	네트워크에서 SMTP 서버에 대해 정의하고, 메일 서버를 대상으로 하는 익스플로잇을 해결하는 규칙에서 사용됩니다.	예(SMTP 서버를 실행하는 경우)
$SNMP_SERVERS	네트워크에서 SNMP 서버에 대해 정의하고, SNMP 서버에서 공격을 검색하는 규칙에 사용됩니다.	예(SNMP 서버를 실행하는 경우)
$SNORT_BPF	버전 5.3.0 이상으로 순차적으로 업그레이드한 버전 5.3.0 이전의 ASA FirePOWER 모듈 소프트웨어 릴리스에서 시스템에 존재한 경우에만 표시되는 레거시 고급 변수를 식별합니다. 2-28페이지의 고급 변수의 이해를 참고하십시오.	아니요, 이 변수를 보거나 삭제하는 것만 가능합니다. 삭제한 다음 수정하거나 복원할 수 없습니다.
$SQL_SERVERS	네트워크에서 데이터베이스 서버에 대해 정의하고, 데이터베이스를 표적으로 삼은 익스플로잇을 해결하는 규칙에서 사용됩니다.	예(SQL Server를 실행하는 경우)
$SSH_PORTS	네트워크에서 SSH 서버의 포트에 대해 정의하고, SSH 서버 익스플로잇 규칙에 사용됩니다.	예(SSH 서버가 기본 포트 이외에 포트를 사용할 경우), 모듈 인터페이스에서 기본 포트를 확인할 수 있습니다.

표 2-2 ASA FirePOWER 모듈에서 제공하는 변수 (계속)

변수 이름	설명	수정 여부
$SSH_SERVERS	네트워크에서 SSH 서버에 대해 정의하고, SSH를 표적으로 삼은 익스플로잇을 해결하는 규칙에서 사용됩니다.	예(SSH 서버를 실행하는 경우), $HOME_NET을 적절하게 정의한 후 $HOME_NET을 $SSH_SERVERS에 대한 값으로 포함해야 합니다.
$TELNET_SERVERS	네트워크에서 알려진 텔넷 서버에 대해 정의하고, 텔넷 서버를 표적으로 삼은 익스플로잇을 해결하는 규칙에 사용됩니다.	예(텔넷 서버를 실행하는 경우)
$USER_CONF	원래는 모듈 인터페이스를 통해 사용이 불가능한 하나 이상의 기능을 구성할 수 있는 일반 도구를 제공합니다. 2-28페이지의 고급 변수의 이해를 참고하십시오. ⚠ **주의** 충돌 또는 중복 $USER_CONF 구성은 시스템을 중단시킵니다. 2-28페이지의 고급 변수의 이해를 참고하십시오.	아니요(기능 설명의 지침에 따른 경우 또는 Support(지원부)의 안내에 따른 경우에만 해당)

변수 집합의 이해

라이센스: 보호

어느 집합이든 변수를 추가하면 모든 집합에 변수가 추가됩니다. 즉 각 변수 집합은 시스템에서 현재 구성된 모든 변수의 집합입니다. 모든 변수 집합에서 사용자 정의한 변수를 추가하고 모든 변수의 값을 사용자 정의할 수 있습니다.

먼저, ASA FirePOWER 모듈은 단일 기본 변수 집합을 제공하는데, 이는 미리 정의된 기본값으로 구성되어 있습니다. 기본 집합의 각 변수는 초기 기본값으로 설정되는데, 이는 사전 정의된 변수의 경우 VRT가 설정하고 규칙 업데이트에서 제공되는 값입니다.

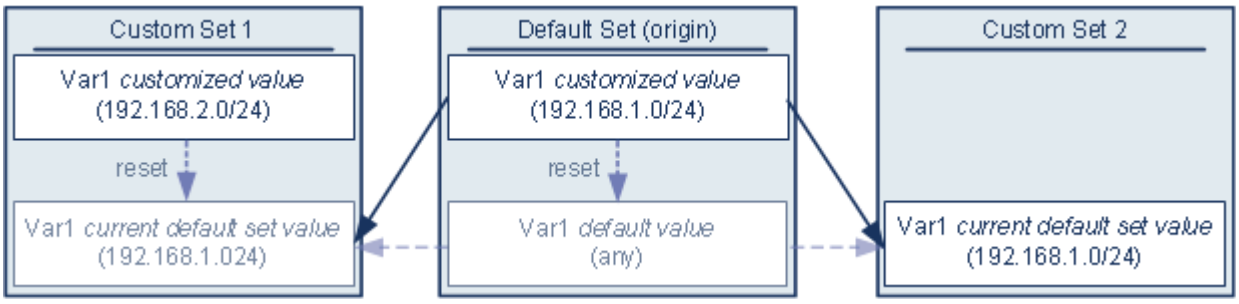
미리 정의된 기본 변수가 해당 기본값으로 구성된 상태로 둘 수도 있지만, Cisco는 사용자가 2-15페이지의 미리 정의된 기본 변수 최적화에 설명된 대로 미리 정의된 변수의 하위 집합을 변경할 것을 권장합니다.

기본 집합에서만 변수를 사용할 수 있지만 대부분의 경우 하나 이상의 사용자 지정 집합을 추가하고, 다양한 집합에서 여러 변수 값을 구성하며, 새로운 변수를 추가하는 것이 유용할 수 있습니다.

여러 집합을 사용할 때, 기본 집합 내 모든 변수의 *현재 값*이 다른 모든 집합 내 변수의 *기본값*을 결정한다는 점을 기억하는 것이 중요합니다.

예: 기본 집합에 사용자 정의 변수 추가

다음 다이어그램은 사용자 정의 변수 Var1을 192.168.1.0/24 값과 함께 기본 집합에 추가하는 경우 집합 상호 작용에 대해 설명합니다.



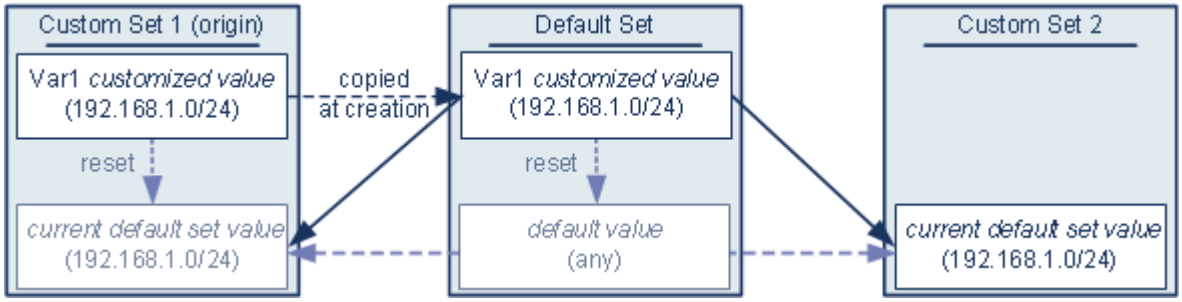
또는, 모든 설정에서 Var1의 값을 사용자 정의할 수 있습니다. Var1이 사용자 정의되지 않은 사용자 지정 집합 2에서 해당 값은 192.168.1.0/24입니다. 사용자 지정 집합 1에서 사용자 정의 값 192.168.2.0/24는 Var1이며, 이는 기본값을 재정의합니다. 기본 설정의 사용자 정의 변수를 재설정하면 모든 집합에서 기본값을 any로 재설정합니다.

이 예에서 특히 주의해야 할 점은, 사용자가 Var1을 사용자 지정 집합 2에서 업데이트하지 않는 경우, 기본 집합에서 Var1을 사용자 지정하거나 재설정하면 결과적으로 사용자 지정 집합 2의 현재 Var1 기본값이 업데이트되며, 따라서 변수 집합에 연결된 모든 침입 규칙에 영향을 준다는 점입니다.

예에 나타나 있지 않지만, 기본 집합에서 기본 변수를 재설정하면 현재 규칙 업데이트에서 시스템이 구성한 값에 이를 재설정하는 경우를 제외하면, 집합 간의 상호작용은 사용자 정의 변수와 기본 변수의 경우 동일하다는 점에 유의하십시오.

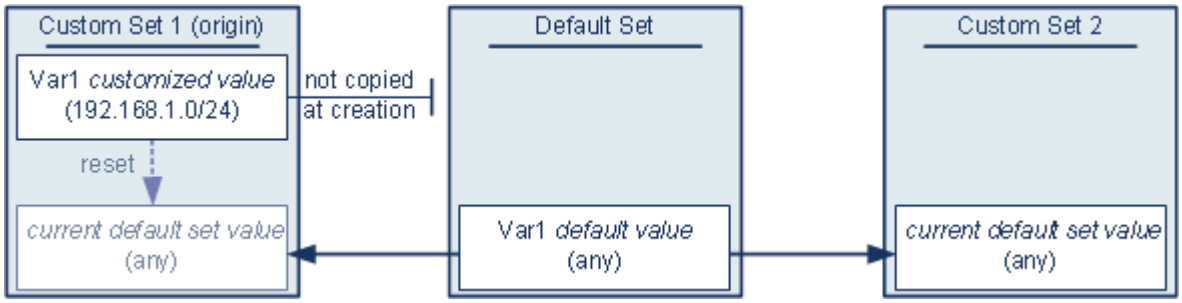
예: 사용자 지정 집합에 사용자 정의 변수 추가

다음 2가지 예는 사용자 지정 집합에 사용자 정의 변수를 추가할 때 변수 집합 상호 작용에 대해 설명합니다. 새로운 변수를 저장할 때, 다른 집합에 대해 구성된 값을 기본값으로 사용하도록 설정할지 묻는 메시지가 표시됩니다. 다음 예에서, 구성된 값을 **사용**하도록 선택합니다.



사용자 지정 집합 1에서 Var1의 출처를 제외하고 이 예는 사용자가 기본 집합에 Var1을 추가한 위 예와 동일합니다. Var1에 대한 사용자 지정 값 192.168.1.0/24를 사용자 지정 집합 1에 추가하면 해당 값을 기본값 any와 함께 사용자 지정 값으로 기본 집합에 복사합니다. 따라서, Var1 값과 상호 작용은 사용자가 Var1을 기본 집합에 추가한 경우와 동일합니다. 이전 예와 마찬가지로, 기본 집합에서 Var1을 사용자 지정하거나 재설정하면 결과적으로 사용자 지정 집합 2의 현재 Var1 기본값이 업데이트되며, 따라서 변수 집합에 연결된 모든 침입 정책에 영향을 준다는 점에 유의하십시오.

다음 예에서는 이전 예처럼 Var1을 값 192.168.1.0/24와 함께 사용자 지정 집합 1에 추가하지만 Var1의 구성된 값은 다른 집합의 기본값으로 **사용하지 않기**로 선택합니다.



이 접근 방식은 Var1을 기본값 any를 가진 모든 집합에 추가합니다. Var1을 추가한 후, 모든 설정에서 해당 값을 사용자 정의할 수 있습니다. 이 접근 방식의 이점은 기본 집합에서 Var1을 초기에 사용자 정의하지 않음으로써 기본 집합에서 값을 사용자 정의하여 Var1을 사용자 정의하지 않은 사용자 지정 집합 2와 같은 집합에서 현재 값을 부주의하게 변경하는 것의 위험을 줄일 수 있다는 것입니다.

변수 집합 관리

라이센스: 보호

Object Manager(개체 관리자) 페이지에서 **Variable Sets(변수 집합)**(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**)를 선택하면 개체 관리자는 사용자가 만든 모든 사용자 지정 집합 및 기본 변수 집합을 나열합니다.

새롭게 설치된 시스템에서, 기본 변수 집합은 ASA FirePOWER 모듈에 의해 사전 정의된 기본 변수만으로 구성됩니다.

각 변수 집합은 Cisco에서 제공된 기본 변수와 사용자가 모든 변수 집합에서 추가한 모든 사용자 변수를 포함합니다. 기본 집합을 수정할 수 있지만, 기본 집합을 변경하거나 삭제할 수 없다는 점을 참고하십시오.

다음 표는 변수 집합을 관리하기 위해 수행할 수 있는 작업에 대해 요약합니다.

표 2-3 변수 집합 관리 작업

목적	방법
변수 집합 표시하기	**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택한 후 **Variable Set(변수 집합)**를 선택합니다.
변수 집합을 이름별로 필터링하기	이름 입력합니다. 사용자가 입력하면 해당 페이지는 새로 고침되어 일치하는 이름을 표시합니다.
이름 필터링 지우기	필터 필드에서 지우기 아이콘( )을 클릭합니다.
사용자 지정 변수 집합 추가하기	**Add Variable Set(변수 집합 추가)**를 클릭합니다. 사용자 편의를 위해, 새로운 변수 집합은 모든 현재 정의된 기본값 및 사용자 정의된 변수를 포함합니다.
변수 집합 수정하기	수정하려는 변수 집합 옆에 있는 수정 아이콘( ) 클릭합니다. **팁** 변수 집합에 대한 행에서 오른쪽 단추를 클릭한 후 **Edit(수정)**를 선택해도 됩니다.
사용자 지정 변수 집합 삭제하기	변수 집합 옆에 있는 삭제 아이콘( )을 클릭한 후 **Yes(예)**를 클릭합니다. 기본 변수 집합을 삭제할 수 없습니다. 삭제할 변수 집합에서 생성한 변수는 삭제되거나 다른 집합에서 영향을 받지 않는다는 점에 유의하십시오. **팁** 또한 변수 집합에 대한 행에서 마우스 오른쪽 단추를 클릭하여 **Delete(삭제)**를 선택한 후 **Yes(예)**를 클릭합니다. Ctrl 및 Shift 키를 사용하여 여러 집합을 선택합니다.

변수 집합을 구성한 후, 침입 정책에 애플리케이션을 연결할 수 있습니다.

변수 집합을 만들거나 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 **Variable Set(변수 집합)**를 선택합니다.

단계 3 변수 집합을 추가하거나 기존 집합을 수정하려면 다음을 수행합니다.

- 변수 집합을 추가하려면, **Add Variable Set(변수 집합 추가)**를 클릭합니다.
- 변수 집합을 수정하려면, 변수 집합 옆에 수정 아이콘( )을 클릭합니다.

새로운 변수 집합 페이지 또는 변수 집합 수정 페이지가 나타납니다. 변수 집합 내 변수 추가 및 수정에 대한 내용은 2-21페이지의 변수 추가 및 수정을 참고하십시오.

변수 관리

라이센스: 보호

변수 집합의 새로운 변수 페이지 또는 변수 수정 페이지에서 변수를 관리합니다. 모든 변수 집합에 대한 변수 페이지가 변수를 Customized Variables(사용자 지정 변수)와 Default Variables(기본 변수) 페이지 영역으로 분리합니다.

*기본 변수*는 ASA FirePOWER 모듈이 제공한 변수입니다. 기본 변수 값을 사용자 정의할 수 있습니다. 기본 변수의 이름을 변경하거나 삭제할 수 없으며, 해당 기본값을 변경할 수 없습니다.

*사용자 지정 변수*는 다음 중 하나입니다.

- 사용자 지정 기본 변수

  기본 변수 값을 수정할 때, 시스템은 변수를 Default Variables(기본 변수) 영역에서 Customized Variables(사용자 지정 변수) 영역으로 옮깁니다. 기본 집합의 변수 값이 사용자 지정 집합 내 변수의 기본값을 결정하기 때문에, 기본 집합의 기본 변수를 사용자 지정하면 다른 모든 집합 내 변수의 기본값을 수정합니다.

- 사용자 정의 변수

  사용자 고유의 변수를 추가 및 삭제할 수 있으며, 그 값을 다른 변수 집합 내에서 사용자 정의하고, 기본값에 사용자 지정 변수를 재설정할 수 있습니다. 사용자 정의된 변수를 재설정할 때, 사용자 지정 변수 영역에 남아 있습니다.

다음 표는 변수를 만들거나 수정하기 위해 수행할 수 있는 작업에 대해 요약합니다.

표 2-4 변수 관리 작업

목적	방법
변수 페이지 표시하기	변수 집합 페이지에서 **Add Variable Set(변수 집합 추가)**를 클릭하여 새로운 변수 집합을 만들거나, 수정할 변수 집합 옆에 있는 수정 아이콘( )을 클릭합니다.
변수 집합의 이름을 지정하고 선택적으로 설명하기	**Name(이름)** 및 **Description(설명)** 필드에 스페이스 및 특수 문자를 포함하여 스트링 영숫자를 입력합니다.
변수 추가하기	**Add(추가)**를 클릭합니다. 자세한 내용은 2-21페이지의 변수 추가 및 수정을 참고하십시오.
변수 수정하기	수정하려는 변수 옆에 있는 수정 아이콘( )을 클릭합니다. 자세한 내용은 2-21페이지의 변수 추가 및 수정을 참고하십시오.
수정된 변수를 기본값으로 재설정하기	**팁** 수정된 변수 옆에 있는 재설정 아이콘( )을 클릭합니다. 음영으로 처리한 재설정 아이콘은 현재 값이 이미 기본값임을 나타냅니다.
사용자 정의한 사용자 지정 변수 삭제하기	변수 집합 옆에 있는 삭제 아이콘( )을 클릭합니다. 변수를 추가한 이후 변수 집합을 저장할 경우, **Yes(예)**를 클릭하여 변수를 삭제할 것인지 확인합니다. 기본 변수 및 침입 규칙 또는 여러 변수에 사용된 사용자 정의 변수를 삭제할 수 없습니다.
변수 집합에 변경 사항 저장하기	액세스 제어 정책에서 변수 집합을 사용 중인 경우 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭한 후 **Yes(예)**를 클릭하여 변경 사항을 저장할 것인지 확인합니다. 기본 집합의 현재 값이 다른 모든 집합의 기본값을 결정하기 때문에 기본 집합의 변수를 수정하거나 재설정하면 기본값을 사용자 정의하지 않은 집합에서 현재 값이 변경됩니다.

변수 집합의 변수를 보려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 **Variable Set(변수 집합)**를 선택합니다.

단계 3 변수 집합을 추가하거나 기존 집합을 수정하려면 다음을 수행합니다.

- 변수 집합을 추가하려면, **Add Variable Set(변수 집합 추가)**를 클릭합니다.
- 변수 집합을 수정하려면, 변수 집합 옆에 수정 아이콘()을 클릭합니다.

새로운 변수 집합 페이지 또는 변수 집합 수정 페이지가 나타납니다.

단계 4 변수를 추가하거나 기존 변수를 수정하려면 다음을 수행합니다.

- 변수를 추가하려면 **Add(추가)**를 클릭합니다.
- 변수를 수정하려면, 변수 옆에 있는 수정 아이콘()을 클릭합니다.

새로운 변수 페이지 또는 변수 수정 페이지가 나타납니다.

변수 집합 내 변수 추가 및 수정에 대한 내용은 2-21페이지의 변수 추가 및 수정을 참고하십시오.

변수 추가 및 수정

라이센스: 보호

모든 사용자 지정 집합 내에서 변수를 수정할 수 있습니다.

사용자 지정 표준 텍스트 규칙을 만든 경우, 트래픽을 더욱 정확하게 반영하기 위해 사용자 정의된 변수를 추가하거나 규칙 생성 프로세스를 간소화하는 바로가기로 추가하기를 원할 수 있습니다. 예를 들어, "비무장 지대"(또는 DMZ)의 트래픽만 검사할 규칙을 작성하는 경우, 해당 값이 노출된 서버 IP 주소를 나열하는 `$DMZ`라는 이름의 변수를 만들 수 있습니다. 그러면 이 영역에 작성된 모든 규칙에서 `$DMZ` 변수를 사용할 수 있습니다.

변수 집합에 변수를 추가하면 다른 모든 집합에 추가됩니다. 아래에 설명된 대로 한 가지 예외를 제외하고는, 변수는 기본값으로 다른 집합에 추가되며, 이후 사용자가 사용자 정의할 수 있습니다.

사용자 지정 집합의 변수를 추가할 때, 구성된 값을 기본 집합의 사용자 지정 값으로 사용할지 선택해야 합니다.

- 구성된 값(예를 들어, 192.168.0.0/16)을 사용하지 **않는** 경우, 변수는 구성된 값을 기본값 `any`와 함께 사용자 지정 값으로 사용하는 기본 집합에 추가됩니다. 기본 집합의 현재 값이 다른 집합의 기본값을 결정하기 때문에, 다른 사용자 지정 집합의 초기 기본값은 구성된 값(예에서는 192.168.0.0/16)입니다.
- 구성된 값을 사용하지 **않는** 경우, 변수는 기본값 `any`만 사용하는 기본 집합에 추가되며, 결과적으로, 다른 사용자 지정 집합의 초기 기본값은 `any`입니다.

자세한 내용은 2-17페이지의 변수 집합의 이해를 참고하십시오.

New Variable(새로운 변수) 페이지에서 변수 집합 내 변수를 추가하고 Edit Variable(변수 수정) 페이지에서 기존 변수를 수정합니다. 기존 변수를 수정하면 변수 이름 또는 변수 유형을 변경할 수 없다는 점을 제외하면 두 페이지는 동일하게 사용됩니다.

각 페이지는 주로 3개의 창으로 이루어져 있습니다.

- 기존 네트워크 또는 포트 변수, 개체 및 네트워크 개체 그룹을 포함하여 사용 가능한 항목
- 변수 정의에 포함할 네트워크 또는 포트
- 변수 정의에서 제외할 네트워크 또는 포트

2가지 변수 유형을 만들거나 수정할 수 있습니다.

- *network* 변수는 네트워크 트래픽에서 호스트 IP 주소를 지정합니다. 2-24페이지의 네트워크 변수 작업을 참고하십시오.
- *port* 변수는 각 유형에 대한 any 값을 포함하여 네트워크 트래픽에서 TCP 또는 UDP 포트를 지정합니다. 2-26페이지의 포트 변수 작업을 참고하십시오.

네트워크 또는 포트 변수 유형을 추가할지 지정할 때, 페이지는 새로 고침되어 사용 가능한 항목을 나열합니다. 목록 위의 검색 필드를 통해 목록을 제한할 수 있으며 이는 입력 시 업데이트됩니다.

항목 목록을 포함하거나 제외하기 위해 가용 항목을 선택하고 드래그할 수 있습니다. 또한 항목을 선택하고 **Include(포함하기)** 또는 **Exclude(제외하기)** 버튼을 클릭할 수 있습니다. 여러 항목을 선택하려면 Ctrl 및 Shift 키를 사용합니다. 포함되거나 제외된 항목의 목록 아래의 구성 필드를 사용하여 네트워크 변수에 대한 리터럴 IP 주소 및 주소 블록과 포트 변수에 대한 포트 및 포트 범위를 지정할 수 있습니다.

포함하거나 제외할 항목 목록은 리터럴 문자열 및 기존 변수, 개체, 그리고 네트워크 변수의 경우 네트워크 개체 그룹의 모든 조합으로 구성될 수 있습니다.

다음 표는 사용자 변수를 만들거나 수정하기 위해 수행할 수 있는 작업에 대해 요약합니다.

표 2-5 변수 수정 작업

목적	방법
변수 페이지 표시하기	변수 집합 페이지에서 **Add(추가)**를 클릭하여 새로운 변수를 추가하거나, 기존 변수 옆에 있는 수정 아이콘( )을 클릭합니다.
변수 이름 지정하기	**Name(이름)** 필드에 밑줄 문자(_) 이외의 특수 문자를 포함하지 않으며 대소문자를 구분하는 고유한 영숫자 문자열을 입력합니다. 변수 이름은 대소문자를 구분한다는 점에 유의하십시오. 예를 들어,var와 Var은 각각 다른 이름입니다.
네트워크 또는 포트 변수 지정하기	**Network(네트워크)** 또는 **Port(포트)**를 **Type(유형)** 드롭다운 목록에서 선택합니다. 네트워크 및 포트 변수를 사용하고 구성하는 방법에 관한 자세한 내용은 2-24페이지의 네트워크 변수 작업 및 2-26페이지의 포트 변수 작업을 참고하십시오.
가용 네트워크 목록에서 선택할 수 있도록 개별 네트워크 개체 추가하기	**Network(네트워크)**를 **Type(유형)** 드롭다운 목록에서 선택한 다음, 추가 아이콘( )을 클릭합니다. 개체 관리자를 사용하여 네트워크 개체를 추가하는 데 대한 내용은 2-3페이지의 네트워크 개체 작업을 참고하십시오.
가용 포트 목록에서 선택할 수 있도록 개별 포트 개체 추가하기	**Port(포트)**를 **Type(유형)** 드롭다운 목록에서 선택한 다음, 추가 아이콘( )을 클릭합니다. 모든 포트 유형을 추가할 수 있지만, 각 유형에 대한 any 값을 포함하여 TCP와 UDP 포트만이 유효한 변수 값이며, 가용 포트 목록은 이 값 유형을 사용하는 변수만 표시합니다. 개체 관리자를 사용하여 포트 개체를 추가하는 데 대한 내용은 2-10페이지의 포트 개체 작업을 참고하십시오.
사용 가능한 포트 또는 네트워크 항목을 이름별로 검색하기	사용 가능한 항목의 목록 위에 있는 검색 필드에 이름을 입력합니다. 입력하면 페이지가 새로 고침되어 일치하는 이름을 표시합니다.
이름 검색 지우기	검색 필드 위에 있는 다시 로드 아이콘( ) 또는 검색 필드의 지우기 아이콘(✖)을 클릭합니다.

표 2-5 변수 수정 작업 (계속)

목적	방법
사용 가능한 항목 구별하기	변수 아이콘( ), 네트워크 개체 아이콘( ), 포트 아이콘( ), 및 개체 그룹 아이콘( ) 옆에 있는 항목을 검색합니다. 포트 그룹이 아닌 네트워크 그룹만 사용 가능하다는 점에 유의하십시오.
변수 정의에 포함하거나 제외할 개체 선택하기	사용 가능한 네트워크 또는 포트 목록에서 개체를 클릭합니다. 여러 개체를 선택하려면 Ctrl 및 Shift 키를 사용합니다.
포함되거나 제외된 네트워크 또는 포트 목록에 선택한 항목 추가하기	선택한 항목을 드래그합니다. 또는 **Include(포함하기)** 또는 **Exclude(제외하기)**를 클릭합니다. 네트워크 및 포트 변수, 그리고 가용 항목 목록의 개체를 추가할 수 있습니다. 네트워크 개체 그룹을 추가할 수도 있습니다.
네트워크 또는 포트 목록에 리터럴 네트워크 또는 포트를 추가하여 포함하거나 제외하기	리터럴 **Network(네트워크)** 또는 **Port(포트)** 필드에서 프롬프트를 클릭하여 제거하고, 네트워크 변수에 대한 리터럴 IP 주소 또는 주소 블록 또는 포트 변수에 대한 리터럴 포트 또는 포트 범위를 입력한 후 **Add(추가)**를 클릭합니다. 도메인 이름 또는 목록을 입력할 수 없다는 점에 유의하십시오. 여러 항목을 추가하려면, 각각을 개별적으로 추가합니다.
모든 값으로 변수 추가하기	변수 이름을 지정하고 변수 유형을 선택한 다음, 값을 구성하지 않고 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.
포함되거나 제외된 목록에서 변수 또는 개체 삭제하기	변수 옆에 있는 삭제 아이콘( )을 클릭합니다.
새로운 변수 또는 수정된 변수 저장하기	**Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다. 사용자 지정 집합의 변수를 추가할 경우, **Yes(예)**를 클릭하여 구성된 값을 다른 집합에서 기본값으로 사용하거나, **No(아니오)**를 클릭하여 기본값 any를 사용합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 2-24페이지의 네트워크 변수 작업
- 2-26페이지의 포트 변수 작업

변수를 추가하거나 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 **Variable Set(변수 집합)**를 선택합니다.

단계 3 변수 집합을 추가하거나 기존 집합을 수정하려면 다음을 수행합니다.

- 변수 집합을 추가하려면, **Add Variable Set(변수 집합 추가)**를 클릭합니다.
- 기존 변수 집합을 수정하려면, 변수 집합 옆에 있는 수정 아이콘( )을 클릭합니다.

새로운 변수 집합 페이지 또는 변수 집합 수정 페이지가 나타납니다.

단계 4 새로운 변수를 추가하거나 기존 변수를 수정하려면 다음을 수행합니다.

- 새로운 변수를 추가하려면 **Add(추가)**를 클릭합니다.
- 기존 변수를 수정하려면, 변수 옆에 있는 수정 아이콘( )을 클릭합니다.

새로운 변수 페이지 또는 변수 수정 페이지가 나타납니다.

단계 5 새로운 변수를 추가하는 경우 다음을 수행합니다.

- 고유한 변수 **Name(이름)**을 입력합니다.

  영숫자 및 밑줄(_) 문자를 사용할 수 있습니다.

- 드롭다운 목록에서 **Network(네트워크)** 또는 **Port(포트)** 변수 **Type(유형)**를 선택합니다.

단계 6 또는, 사용 가능한 네트워크 또는 포트 목록에서 포함되거나 제외된 항목의 목록으로 항목을 이동합니다.

항목을 하나 이상 선택한 다음 끌어 놓거나 **Include(포함하기)** 또는 **Exclude(제외하기)**를 클릭할 수 있습니다. 여러 항목을 선택하려면 Ctrl 및 Shift 키를 사용합니다.

팁 네트워크 또는 포트 변수에 대해 포함되거나 제외된 목록에서 주소 또는 포트가 중복되는 경우, 제외된 주소 또는 포트가 우선합니다.

단계 7 또는, 단일 리터럴 값을 입력한 다음, **Add(추가)**를 클릭합니다.

네트워크 변수에 대해, 단일 IP 주소 또는 주소 블록을 입력할 수 있습니다. 포트 변수의 경우 단일 포트 또는 포트 범위를 추가할 수 있는데, 하이픈(-)으로 높은 값과 낮은 값을 나눕니다.

여러 문자 값을 입력하기 위해 필요한 만큼 이 단계를 반복합니다.

단계 8 변수를 저장하려면 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다. 사용자 지정 집합에서 새로운 변수를 추가하는 경우 다음과 같은 옵션을 사용할 수 있습니다.

- 구성된 값을 기본 집합에서 사용자 지정 값으로 사용하여 변수를 추가하여 다른 사용자 지정 집합의 기본값으로 사용하려면 **Yes(예)**를 클릭합니다.
- **No(아니오)**를 클릭하면 기본 집합에서 기본값 any로 변수를 추가하여 다른 사용자 지정 집합의 기본값으로 사용할 수 있습니다.

단계 9 변경 작업을 마친 후 변수 집합을 저장하려면 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭한 후 **Yes(예)**를 클릭합니다.

변경 사항이 저장되며 변수 집합이 연결된 모든 액세스 제어 정책이 오래된 상태로 표시됩니다. 변경 사항을 적용하려면 변수 집합이 침입 정책에 연결된 액세스 제어 정책을 적용해야 합니다(4-10 페이지의 액세스 제어 정책 적용 참고).

네트워크 변수 작업

라이센스: 보호

네트워크 변수는 사용자가 침입 정책과 침입 정책 규칙 삭제, 동적 규칙 상태 및 적응형 프로파일에서 활성화한 침입 규칙에서 사용할 수 있는 IP 주소를 나타냅니다. 네트워크 변수는 네트워크 개체 및 네트워크 개체 그룹과 차이와 달리 침입 정책 및 침입 규칙에 특정됩니다. 반면 사용자는 네트워크 개체 및 그룹을 사용하여 ASA FirePOWER 모듈의 다양한 위치에 있는 IP 주소를 나타낼 수 있습니다. 여기에는 액세스 제어 정책, 네트워크 변수, 침입 규칙, 보고서 등이 포함됩니다. 자세한 내용은 2-3페이지의 네트워크 개체 작업을 참고하십시오.

다음 구성의 네트워크 변수를 사용하여 네트워크에 호스트의 IP 주소를 지정할 수 있습니다.

- 침입 규칙

  침입 규칙 **Source IPs(소스 IP)** 및 **Destination IPs(대상 IP)** 헤더 필드를 통해 패킷 검사를 특정 IP 주소에서 시작되었거나 특정 IP 주소로 향하는 패킷으로 제한할 수 있습니다. 23-5페이지의 침입 규칙 내 IP 주소 지정을 참고하십시오.

- 삭제

  소스 또는 대상 침입 규칙 삭제 내 **Network(네트워크)** 필드를 통해 특정 IP 주소 또는 특정 범위의 IP 주소가 침입 규칙 또는 전처리기를 트리거할 때 침입 이벤트 알림을 삭제할 수 있습니다. 20-26페이지의 침입 정책에 따른 삭제 구성을 참고하십시오.

- 동적 규칙 상태

  소스 또는 대상 동적 규칙 상태 내 **Network(네트워크)** 필드를 통해 지정된 기간 동안 침입 규칙 또는 전처리기 규칙에 대해 너무 많은 일치 항목이 발생할 때 사용자가 이를 탐지할 수 있습니다. 20-28페이지의 동적 규칙 상태 추가를 참고하십시오.

- 적응형 프로파일

  적응형 프로파일 **Network(네트워크)** 필드는 수동 배포에서 패킷 단편화 및 TCP 스트림 리어셈블리를 향상시키고자 하는 네트워크에서 호스트를 식별합니다. 18-1페이지의 수동 배포 시 전처리 조정을 참고하십시오.

이 섹션에서 식별된 필드에 변수를 사용할 때, 사용자가 침입 정책에 연결하는 변수 집합은 침입 정책을 사용하는 액세스 제어 정책에 의해 처리된 네트워크 트래픽에서 변수 값을 결정합니다.

변수에 다음 네트워크 구성의 모든 조합을 추가할 수 있습니다:

- 네트워크 변수, 네트워크 개체 및 사용 가능한 네트워크 목록에서 선택하는 네트워크 개체 그룹의 조합

  개체 관리자를 사용하여 개별 및 그룹 네트워크 개체를 생성하는 데 대한 내용은 2-3페이지의 네트워크 개체 작업을 참고하십시오.

- New Variable(새 변수) 페이지 또는 Edit Variable(변수 수정) 페이지에서 추가한 후 사용자 변수 및 기타 기존 및 이후 변수에 추가할 수 있는 개별 네트워크 개체

- 리터럴, 단일 IP 주소 또는 주소 블록

  여러 리터럴 IP 주소 및 주소 블록 각각을 개별적으로 추가하여 나열할 수 있습니다. IPv4 및 IPv6 주소와 주소 블록을 단독으로 또는 조합하여 나열할 수 있습니다. IPv6 주소를 지정할 때, RFC 4291에 정의된 주소 지정 규칙을 사용할 수 있습니다.

추가한 모든 변수의 네트워크에 포함된 기본값은 `any`이며, 이는 모든 IPv4 또는 IPv6 주소를 나타냅니다. 제외된 네트워크의 기본값은 없으며, 이는 아무 네트워크도 없음을 나타냅니다. 또한 포함된 네트워크 목록에서 모든 IPv6 주소를 나타내는 리터럴 값으로, 또는 제외 목록에서 IPv6 주소 없음으로 주소 `::`를 지정할 수 있습니다.

제외한 목록에 네트워크를 추가하면 지정된 주소 및 주소 블록을 무효화합니다. 즉 제외된 IP 주소 또는 주소 블록을 제외한 모든 IP 주소와 일치시킬 수 있습니다.

예를 들어, 리터럴 주소 `192.168.1.1`을 제외하면 192.168.1.1을 제외한 모든 IP 주소가 지정되며, `2001:db8:ca2e::fa4c`를 제외하면 2001:db8:ca2e::fa4c를 제외한 모든 IP 주소가 지정됩니다.

리터럴 또는 가용 네트워크를 사용하여 모든 네트워크의 조합을 제외할 수 있습니다. 예를 들어, 리터럴 값 `192.168.1.1` 및 `192.168.1.5`를 제외하면 192.168.1.1 또는 192.168.1.5를 제외한 모든 IP 주소가 *포함됩니다*. 즉 시스템은 이를 "192.168.1.1이 **아니고** 192.168.1.5도 **아닌 것**"으로 해석하며, 이는 괄호 사이에 나열된 IP 주소를 제외한 모든 IP 주소에 일치하는 것입니다.

네트워크 변수를 추가하거나 수정할 때는 다음 사항에 유의하십시오.

- 논리적으로 `any` 값을 제외할 수 없습니다. 제외할 경우, 이는 어떤 주소도 나타내지 않습니다. 예를 들어, 제외한 네트워크 목록에 `any` 값을 가진 변수를 추가할 수 없습니다.
- 네트워크 변수는 지정된 침입 규칙 및 침입 정책 기능의 트래픽을 식별합니다. 전처리기 규칙은 침입 규칙에서 사용되는 네트워크 변수에 의해 정의된 호스트에 관계없이 이벤트를 트리거할 수 있습니다.

- 제외된 값은 포함된 값의 하위 집합을 확인해야 합니다. 예를 들어, 192.168.5.0/24 주소 블록을 포함하거나 192.168.6.0/24를 제외할 수 없습니다. 오류 메시지는 사용자에게 경고하고 문제가 되는 변수를 식별하며, 사용자는 포함된 값의 범위 밖의 값을 제외할 때 변수 집합을 저장할 수 없습니다.

네트워크 변수 추가 및 수정에 대한 자세한 내용은 2-21페이지의 변수 추가 및 수정을 참고하십시오.

포트 변수 작업

라이센스: 보호

포트 변수는 사용자가 침입 정책에서 활성화한 침입 규칙 내 **Source Port(소스 포트)** 및 **Destination Port(대상 포트)** 헤더 필드에서 사용할 수 있는 TCP 및 UDP 포트를 나타냅니다. 포트 변수는 포트 개체 및 포트 개체 그룹과 달리 침입 규칙에 특정적입니다. TCP 및 UDP 이외의 프로토콜에 대한 포트 개체를 생성할 수 있고, 포트 개체를 사용할 수 있는데, 여기에는 포트 변수 그리고 액세스 제어 정책이 포함됩니다. 자세한 내용은 2-10페이지의 포트 개체 작업을 참고하십시오.

침입 규칙 **Source Port(소스 포트)** 및 **Destination Port(대상 포트)** 헤더 필드에서 포트 변수를 사용하여 패킷 검사를 특정 TCP 및 UDP 포트에서 시작되었거나 특정 TCP 및 UDP 포트로 향하는 패킷에 제한할 수 있습니다.

이 필드에 변수를 사용할 때, 액세스 제어 규칙 또는 정책과 관련된 침입 정책에 연결한 변수 집합은 액세스 제어 정책을 적용하는 네트워크 트래픽에서 해당 변수의 값을 결정합니다.

변수에 다음 포트 구성의 모든 조합을 추가할 수 있습니다

- 사용 가능한 포트 목록에서 선택하는 포트 변수 및 포트 개체의 모든 조합

  사용 가능한 포트 목록이 포트 개체 그룹을 표시하지 않는다는 점과 변수에 이를 추가할 수 없다는 점에 주의하십시오. 개체 관리자를 사용하여 포트 개체를 만드는 것에 대한 내용은 2-10페이지의 포트 개체 작업을 참고하십시오.

- New Variable(새 변수) 페이지 또는 Edit Variable(변수 수정) 페이지에서 추가한 후 사용자 변수 및 기타 기존 및 이후 변수에 추가할 수 있는 개별 포트 개체

  각 유형의 any 값을 포함하여 TCP 및 UDP 포트만이 유효한 변수 값입니다. 유효한 변수 값이 아닌 유효한 포트 개체를 추가하기 위해 새 변수 페이지 또는 변수 수정 페이지를 사용할 경우, 개체는 시스템에 추가되지만 가용 개체 목록에 표시되지 않습니다. 개체 관리자를 사용하여 변수에 사용되는 포트 개체를 수정할 때, 유효한 변수 값에 대해 값을 변경하기만 할 수 있습니다.

- 단일, 리터럴 포트 값 및 포트 범위

  대시(-)로 포트 범위를 구분해야 합니다. 콜론(:)으로 표시된 포트 범위는 이전 버전 호환성을 위해 지원되지만 사용자가 생성하는 포트 변수에 콜론을 사용할 수 없습니다.

  여러 리터럴 포트 값 및 범위를 어떤 조합에서나 각각 개별적으로 추가하여 나열할 수 있습니다.

포트 변수를 추가하거나 수정할 때는 다음 사항에 유의하십시오.

- 추가한 모든 변수의 포트에 포함된 기본값은 any이며, 이는 모든 포트 또는 포트 범위를 나타냅니다. 제외한 포트에 대한 기본값은 none이며, 이는 아무 포트도 없음을 나타냅니다.

팁 any 값으로 변수를 생성하려면, 특정 값을 추가하지 않고 변수의 이름을 지정하고 저장합니다.

- 논리적으로 any 값을 제외할 수 없습니다. 제외할 경우, 이는 어떤 포트도 나타내지 않습니다. 예를 들어 제외된 포트 목록에 any 값을 가진 변수를 추가할 때 변수 집합을 저장할 수 없습니다.
- 제외한 목록에 포트를 추가하면 지정된 포트 및 포트 범위가 무효화됩니다. 즉 제외된 포트 또는 포트 범위를 제외한 모든 포트와 일치시킬 수 있습니다.

- 제외된 값은 포함된 값의 하위 집합을 확인해야 합니다. 예를 들어, 포트 범위 10-50을 포함하거나 포트 60를 제외할 수 없습니다. 오류 메시지는 사용자에게 경고하고 문제가 되는 변수를 식별하며, 사용자는 포함된 값의 범위 밖의 값을 제외할 때 변수 집합을 저장할 수 없습니다.

포트 변수 추가 및 수정에 대한 자세한 내용은 2-21페이지의 변수 추가 및 수정을 참고하십시오.

변수 재설정

라이센스: 보호

새 변수 페이지 또는 변수 수정 페이지에서 변수 집합의 기본값에 변수를 재설정할 수 있습니다. 다음 표는 변수 재설정의 기본 원칙에 대해 요약합니다.

표 2-6 변수 재설정 값

재설정할 변수 유형	집합 유형	재설정
기본값	기본값	규칙 업데이트 값
사용자 정의됨	기본값	any
기본 또는 사용자 정의됨	사용자 지정	현재 기본 설정값(변경되거나 변경되지 않은)

사용자 지정 집합의 변수를 재설정하면 기본 집합에서 해당 변수의 현재 값으로 재설정되기만 합니다.

반대로, 기본 집합의 변수 값을 재설정하거나 변경하면 모든 사용자 지정 집합에서 해당 변수의 기본값이 항상 업데이트됩니다. 재설정 아이콘이 회색으로 비활성화된 경우, 이는 변수를 재설정할 수 없음을 나타내므로, 이는 해당 설정에서 변수에 사용자 정의된 값이 없음을 의미합니다. 사용자 지정 집합의 변수 값을 사용자 정의하지 않는 한, 기본 집합의 변수를 수정하면 변수 집합에 연결한 침입 정책에서 사용되는 값이 업데이트됩니다.

참고 변경 사항이 연결된 사용자 지정 집합의 변수를 사용하는 침입 정책에 영향을 미치는 방식을 평가하기 위해 기본 집합의 변수를 변경해 보는 것이 좋습니다. 사용자 지정 집합의 변수 값을 사용자 지정하지 않은 경우 특히 그렇습니다.

사용자 지정 값과 재설정 값이 동일한 경우, 이는 다음 중 하나를 나타냅니다.

- any 값을 가진 변수를 추가한 사용자 지정 집합 또는 기본 집합에 있는 것입니다
- 고유한 값을 가진 변수를 추가하고 기본값으로 구성된 값을 사용하도록 선택한 사용자 지정 집합에 있는 것입니다

침입 정책에 변수 집합 연결

라이센스: 제어

기본적으로, ASA FirePOWER 모듈은 액세스 제어 정책에서 사용되는 모든 침입 정책에 기본 변수 집합을 연결합니다. 침입 정책을 사용하는 액세스 제어 정책을 적용하면, 침입 정책에서 활성화한 침입 규칙이 연결된 변수 집합의 변수 값을 사용합니다.

액세스 제어 정책의 침입 정책에서 사용하는 사용자 지정 변수 집합을 변경할 때, 시스템은 Access Control(액세스 제어) 페이지에서 해당 정책의 상태를 오래된 것으로 반영합니다. 사용자 변수 집합의 변경을 수행하도록 액세스 제어 정책을 재적용해야 합니다. 기본 집합을 변경할 때, 시스템은 침입 정책을 사용하는 모든 액세스 제어 정책 상태를 오래된 것으로 반영하며, 사용자는 변경 사항을 수행하도록 모든 액세스 제어 정책을 재적용해야 합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 액세스 제어 규칙에 기본 집합이 아닌 변수 집합을 연결하려면, 10-4페이지의 침입 방지 수행을 위한 액세스 제어 규칙 구성의 절차를 참고하십시오.
- 액세스 제어 정책의 기본 작업에 기본 집합이 아닌 변수 집합을 연결하려면, 4-4페이지의 네트워크 트래픽에 대한 기본 처리와 검사 설정을 참고하십시오.
- 침입 정책에 변수 집합을 연결하는 정책을 비롯한 액세스 제어 정책을 적용하려면 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

고급 변수의 이해

라이센스: 보호

고급 변수를 사용하여 모듈 인터페이스를 통해 구성할 수 없는 기능을 구성할 수 있습니다. ASA FirePOWER 모듈은 현재 단 2개의 고급 변수만 제공하며, 사용자는 USER_CONF 고급 변수만 수정할 수 있습니다.

USER_CONF

USER_CONF는 모듈 인터페이스를 통해 원래는 사용이 불가능한 하나 이상의 기능을 구성할 수 있는 일반 도구를 제공합니다.

주의 기능 설명에서 또는 Support(지원부)를 통해 침입 정책 기능을 구성하라는 안내를 받지 않은 한 침입 정책 기능을 구성하기 위해 USER_CONF 고급 변수를 사용하지 **마십시오**. 충돌이나 이중 설정은 시스템을 중단시킵니다.

USER_CONF를 수정할 때, 단일 회선에 총 최대 4096개의 문자를 입력할 수 있습니다. 회선은 자동으로 래핑됩니다. 디스크 공간과 같은 변수 또는 물리적 제한을 위한 8192개의 최대 문자 길이에 도달할 때까지 유효한 지침 또는 회선을 원하는 만큼 포함할 수 있습니다. 명령 지시어의 모든 전체 인수 뒤에 백슬래시(\) 줄 연속 문자를 사용합니다.

USER_CONF를 재설정하면 빈 상태로 남게 됩니다.

파일 목록 작업

라이센스: 악성코드

네트워크 기반 AMP(지능형 악성코드 차단)를 사용하고 종합적 보안 인텔리전스 클라우드가 파일 속성을 잘못 식별한 경우, 향후 파일을 더 잘 탐지하기 위해 SHA-256 해시 값을 사용하여 *파일 목록*에 파일을 추가할 수 있습니다. 파일 목록 유형에 따라, 다음을 수행할 수 있습니다.

- 클라우드가 안전 속성으로 할당한 것처럼 파일을 처리하려면 파일을 *안전 목록*에 추가합니다.
- 클라우드가 악성코드 속성으로 할당한 것처럼 파일을 처리하려면 파일을 *사용자 지정 탐지 목록*에 추가합니다.

사용자가 이 파일에 대한 차단 작업을 수동으로 지정하므로 해당 파일이 클라우드에서 악성코드로 식별되는 경우에도 시스템은 악성코드 클라우드 검색을 수행하지 않습니다. 반드시 **Malware Cloud Lookup(악성코드 클라우드 조회)** 또는 **Block Malware(악성코드 차단)** 작업 중 하나 및 파일의 SHA 값을 계산하는 일치 파일 유형과 함께 파일 정책 내 규칙을 구성해야 한다는 점에 유의하십시오. 자세한 내용은 24-10페이지의 파일 규칙 작업을 참고하십시오.

시스템의 정상 목록 및 사용자 지정 탐지 목록은 각 파일 정책의 기본값에 포함됩니다. 정책별 기반으로 하나의 목록 또는 두 목록 모두를 사용하지 않도록 선택할 수 있습니다.

주의 이 목록에 실제 악성 프로그램인 파일을 포함하지 **마십시오**. 클라우드가 파일에 Malware(악성 프로그램) 속성이 있음을 지정한 경우 또는 사용자 지정 탐지 목록에 파일을 추가한 경우에도 시스템은 이들을 차단하지 않습니다.

각 파일 목록은 최대 10000개의 고유한 SHA-256 값을 포함할 수 있습니다. 파일 목록에 파일을 추가하려면 다음을 수행할 수 있습니다.

- 시스템이 파일의 SHA 256 값을 계산하고 추가할 수 있도록 파일을 업로드합니다.
- 파일의 SHA-256 값을 직접 입력합니다.
- 여러 SHA-256 값을 포함하는 쉼표로 구분된 값(CSV) 소스 파일을 생성하고 업로드합니다. 모든 비복제 SHA-256 값이 파일 목록에 추가됩니다.

파일 목록에 파일을 추가하거나, 파일 목록에서 SHA-256 값을 수정하거나, 또는 파일 목록에서 SHA-256 값을 삭제하면, 목록을 사용하는 파일 정책을 가진 모든 액세스 제어 정책을 재적용해야 변경 사항이 적용됩니다.

파일 목록 사용에 대한 자세한 내용은 다음 주제를 참고하십시오.

- 2-29페이지의 파일 목록에 여러 SHA-256 값 업로드
- 2-31페이지의 파일 목록에 개별 파일 업로드
- 2-31페이지의 파일 목록에 SHA-256 값 추가
- 2-32페이지의 파일 목록에서 파일 수정
- 2-32페이지의 파일 목록에서 소스 파일 다운로드

파일 목록에 여러 SHA-256 값 업로드

라이센스: 악성코드

SHA-256 값 목록 및 설명을 포함하는 쉼표로 구분된 값(CSV) 소스 파일을 업로드하여 파일 목록에 여러 SHA-256 값을 추가할 수 있습니다. 시스템은 컨텐츠를 확인하고 유효한 SHA-256 값으로 파일 목록을 입력합니다.

소스 파일은 .csv 파일 이름 확장자를 가진 간편한 텍스트 파일이어야 합니다. 모든 헤더는 파운드 기호(#)로 시작해야 합니다. 이는 코멘트로 처리되어 업로드되지 않습니다. 각 항목은 최대 256개의 영숫자 또는 특수 문자의 설명이 뒤따르는 단일 SHA-256 값을 포함해야 하고, LF 또는 CR+LF 줄바꿈 문자로 끝나야 합니다. 시스템은 항목의 추가 정보는 모두 무시합니다.

다음 사항을 참고하십시오.

- 파일 목록에서 소스 파일을 삭제하면 이는 또한 파일 목록에서 모든 관련 SHA-256 해시를 제거합니다.
- 성공적인 소스 파일 업로드의 결과 파일 목록이 10000개 이상의 명시적 SHA-256 값을 포함하는 경우 파일 목록에 여러 파일을 업로드할 수 없습니다.

- 시스템은 업로드 시 256개의 문자를 초과하는 설명이 있으면 이를 줄여서 처음 256개 문자만 남깁니다. 설명에 쉼표가 포함되어 있는 경우, 이스케이프 문자(\,)를 사용해야 합니다. 어떤 설명도 포함되지 않은 경우, 소스 파일 이름을 대신 사용합니다.
- 파일 목록이 SHA-256 값을 포함하고, 해당 값이 포함된 소스 파일을 업로드할 경우, 새로 업로드한 값은 기존 SHA-256 값을 변경하지 않습니다. 캡처 파일, 파일 이벤트 또는 SHA-256 값과 관련된 악성코드 이벤트를 볼 때, 모든 위협 이름 또는 설명은 개별 SHA-256 값에서 파생됩니다.
- 시스템은 소스 파일에 유효하지 않은 SHA-256 값을 업로드하지 않습니다.
- 업로드된 여러 소스 파일이 동일한 SHA-256 값에 대한 항목을 포함할 경우, 시스템은 가장 최근 값을 사용합니다.
- 소스 파일이 동일한 SHA-256 값에 대한 여러 항목을 포함할 경우, 시스템은 가장 최근 값을 사용합니다.
- 개체 관리자 내 소스 파일을 직접 수정할 수 없습니다. 변경하려면, 먼저 소스 파일을 직접 수정하고, 시스템에서 복사본을 삭제한 후, 수정된 소스 파일을 업로드해야 합니다. 자세한 내용은 2-32페이지의 파일 목록에서 소스 파일 다운로드를 참고하십시오.

파일 목록에 소스 파일을 업로드하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 **File List(파일 목록)**를 클릭합니다.

File List(파일 목록) 섹션이 나타납니다.

단계 3 소스 파일의 값을 추가할 파일 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

File List(파일 목록) 팝업 창이 나타납니다.

단계 4 `List of SHAs(SHA 목록)`을 **Add by(추가 기준)** 필드에서 선택합니다.

팝업 창이 업데이트되어 새 필드를 포함합니다.

단계 5 또는, **Description(설명)** 필드에 소스 파일에 대한 설명을 입력합니다.

설명을 입력하지 않을 경우, 시스템은 파일 이름을 사용합니다.

단계 6 **Browse(찾아보기)**를 클릭하여 소스 파일을 탐색한 후 **Upload and Add List(목록 업로드 및 추가)**를 클릭하여 목록을 추가합니다.

소스 파일이 파일 목록에 추가됩니다. SHA- 256열은 파일이 얼마나 많은 SHA-256 값을 포함하는지 나열합니다.

단계 7 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

단계 8 파일 목록을 사용하는 파일 정책을 가진 모든 액세스 제어 정책을 재적용합니다.

정책을 적용한 후, 시스템은 더 이상 파일 목록의 파일에서 악성코드 클라우드 검색을 수행하지 않습니다.

파일 목록에 개별 파일 업로드

라이센스: 악성코드

파일 목록에 추가할 파일 복사본이 있는 경우, 분석을 위해 시스템에 파일을 업로드할 수 있습니다. 시스템은 파일의 SHA-256 값을 계산하고 목록에 파일을 추가합니다. 시스템은 SHA-256 계산을 위한 파일 크기에 대해 제한을 실시하지 않습니다.

시스템이 SHA-256 값을 계산하도록 하여 파일을 추가하려면 다음을 수행합니다.

단계 1 개체 관리자의 File List(파일 목록) 페이지에서 정상 목록 또는 파일을 추가할 사용자 지정 탐지 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

File List(파일 목록) 팝업 창이 나타납니다.

단계 2 **Calculate SHA(SHA 계산)**을 **Add by(추가 기준)** 필드에서 선택합니다.

팝업 창이 업데이트되어 새 필드를 포함합니다.

단계 3 또는, **Description(설명)** 필드에 파일에 대한 설명을 입력합니다.

설명을 입력하지 않은 경우, 업로드 시 설명에 파일 이름이 사용됩니다.

단계 4 **Browse(찾아보기)**를 클릭하여 소스 파일을 탐색한 후 **Calculate and Add SHA(SHA 계산 및 추가)**를 클릭하여 목록을 추가합니다.

파일이 파일 목록에 추가됩니다.

단계 5 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

단계 6 파일 목록을 사용하는 파일 정책을 가진 모든 액세스 제어 정책을 재적용합니다.

정책을 적용한 후, 시스템은 더 이상 파일 목록의 파일에서 악성코드 클라우드 검색을 수행하지 않습니다.

파일 목록에 SHA-256 값 추가

라이센스: 악성코드

파일의 SHA-256 값을 제출하여 파일 목록에 추가할 수 있습니다. 이중 SHA-256 값을 추가할 수 없습니다.

파일의 SHA-256 값을 수동으로 입력하여 파일을 추가하려면 다음을 수행합니다.

단계 1 개체 관리자의 File List(파일 목록) 페이지에서 정상 목록 또는 파일을 추가할 사용자 지정 탐지 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

File List(파일 목록) 팝업 창이 나타납니다.

단계 2 `Enter SHA Value(SHA 값 입력)`을 **Add by(추가 기준)** 필드에서 선택합니다.

팝업 창이 업데이트되어 새 필드를 포함합니다.

단계 3 **Description(설명)** 필드에 소스 파일에 대한 설명을 입력합니다.

단계 4 파일의 전체 **SHA-256** 값을 입력하거나 붙여 넣습니다. 시스템은 일치하는 부분 값을 지원하지 않습니다.

단계 5 파일을 추가하려면 **Add(추가)**를 클릭합니다.

파일이 파일 목록에 추가됩니다.

단계 6 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

단계 7 파일 목록을 사용하는 파일 정책을 가진 모든 액세스 제어 정책을 재적용합니다.

정책을 적용한 후, 시스템은 더 이상 파일 목록의 파일에서 악성코드 클라우드 검색을 수행하지 않습니다.

파일 목록에서 파일 수정

라이센스: 악성코드

파일 목록에서 개별 SHA-256 값을 수정하거나 삭제할 수 있습니다. 개체 관리자 내 소스 파일을 직접 수정할 수 없다는 점에 유의하십시오. 변경하려면, 먼저 소스 파일을 직접 수정하고, 시스템에서 복사본을 삭제한 후, 수정된 소스 파일을 업로드해야 합니다. 자세한 내용은 2-32페이지의 파일 목록에서 소스 파일 다운로드를 참고하십시오. 파일 목록에서 파일을 수정하려면 다음을 수행합니다.

단계 1 개체 관리자의 File List(파일 목록) 페이지에서 파일을 수정할 사용자 지정 탐지 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

File List(파일 목록) 팝업 창이 나타납니다.

단계 2 수정할 SHA-256 값 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit SHA-256(SHA-256 수정) 팝업 창이 나타납니다.

팁 또한 목록에서 파일을 삭제할 수 있습니다. 삭제할 파일 옆에 있는 삭제 아이콘( )을 클릭합니다.

단계 3 **SHA-256** 값 또는 **Description(설명)**을 업데이트합니다.

단계 4 **Save(저장)**를 클릭합니다.

File List(파일 목록) 팝업 창이 나타납니다. 시스템이 목록에서 파일 항목을 업데이트합니다.

단계 5 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

단계 6 파일 목록을 사용하는 파일 정책을 가진 모든 액세스 제어 정책을 재적용합니다.

정책을 적용한 후, 시스템은 더 이상 파일 목록의 파일에서 악성코드 클라우드 검색을 수행하지 않습니다.

파일 목록에서 소스 파일 다운로드

라이센스: 악성코드

파일 목록에서 기존 소스 파일 항목을 보고, 다운로드하거나, 삭제할 수 있습니다. 한 번 업로드된 소스 파일은 수정할 수 없다는 점에 유의하십시오. 먼저 파일 목록에서 소스 파일을 삭제한 후, 수정된 파일을 업로드합니다. 소스 파일 업로드에 대한 자세한 내용은 2-29페이지의 파일 목록에 여러 SHA-256 값 업로드를 참고하십시오.

소스 파일과 관련된 항목 수는 명시적 SHA-256 값의 수를 나타납니다. 파일 목록에서 소스 파일을 삭제하는 경우, 파일 목록이 포함하는 SHA-256 항목의 총 수는 소스 파일 내 유효한 항목 수에 따라 감소합니다.

소스 파일을 다운로드하려면 다음을 수행합니다.

단계 1 개체 관리자의 File List(파일 목록) 페이지에서 소스 파일을 다운로드할 사용자 지정 탐지 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

File List(파일 목록) 팝업 창이 나타납니다.

단계 2 다운로드할 소스 파일 옆에 있는 보기 아이콘( )을 클릭합니다.

목록 팝업 창에 View SHA-256's(SHA-256 보기)가 나타납니다.

단계 3 **Download SHA List(SHA 목록 다운로드)**를 클릭하고 프롬프트에 따라 소스 파일을 저장합니다.

단계 4 **Close(닫기)**를 클릭합니다.

File List(파일 목록) 팝업 창이 나타납니다.

보안 영역 작업

라이센스: 모두

지원되는 디바이스: 모두

*보안 영역*은 다양한 정책과 구성에서 트래픽 흐름을 관리하고 분류하기 위해 사용할 수 있는 하나 이상의 ASA 인터페이스입니다. 사용자는 단일 디바이스에 여러 영역을 구성할 수 있습니다. 이를 통해 다양한 정책을 적용할 수 있는 세그먼트로 네트워크를 분할할 수 있습니다. 최소 1개의 인터페이스를 보안 영역에 할당하여 해당 보안 영역과 트래픽을 맞추어 볼 수 있도록 해야 하며, 각 인터페이스는 단 하나의 영역에 속할 수 있습니다.

인터페이스를 정렬하기 위해 보안 영역을 사용하는 것 외에도, 영역을 사용할 수 있는 곳은 액세스 제어 정책입니다. 예를 들어, 특정 소스 또는 대상 영역에만 적용된 액세스 제어 규칙을 작성할 수 있습니다.

개체 관리자의 Security Zones(보안 영역)은 ASA FirePOWER 모듈에 구성된 영역을 나열합니다.

사용 중인 보안 영역을 삭제할 수 없습니다. 영역에서 인터페이스를 추가하거나 제거한 후, 디바이스 구성을 재적용해야 합니다. 또한 해당 영역을 사용하는 액세스 제어 정책을 재적용해야 합니다.

보안 영역을 추가하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 **Security Zones(보안 영역)**를 선택합니다.

단계 3 **Add Security Zone(보안 영역 추가)**을 클릭합니다.

Security Zones(보안 영역) 팝업 창이 나타납니다.

단계 4 영역의 **Name(이름)**을 입력합니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자 및 파운드 기호(#)를 모두 사용할 수 있습니다.

단계 5 영역을 위한 인터페이스 **Type(유형)**을 선택합니다.

보안 영역을 만든 다음, 해당 유형을 변경할 수 없습니다.

단계 6 하나 이상의 인터페이스를 선택합니다.

여러 개체를 선택하려면 Ctrl(컨트롤) 및 Shift(쉬프트) 키를 사용합니다. 아직 인터페이스를 설정하지 않은 경우, 빈 영역을 만들고 인터페이스를 나중에 추가할 수 있습니다. 단계 9로 건너뜁니다.

단계 7 **Add(추가)**를 클릭합니다.

선택한 인터페이스는 디바이스가 그룹화한 영역에 추가됩니다.

단계 8 영역에 다른 디바이스의 인터페이스를 추가하려면 단계 6에서 8을 반복합니다.

단계 9 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

보안 영역이 추가됩니다.

위치 정보 개체로 작업하기

라이센스: 모두

사용자가 구성한 각 위치 정보 개체는 시스템이 사용자의 모니터링된 네트워크에서 트래픽의 소스 또는 대상으로 파악한 하나 이상의 국가 또는 대륙을 나타냅니다. 위치 정보 개체를 사용할 수 있는 곳은 액세스 제어 정책입니다. 예를 들어, 특정 국가를 오가는 트래픽을 차단하는 액세스 제어 규칙을 작성할 수 있습니다. 지리적 위치로 트래픽을 필터링하는 것에 대한 정보는 7-3페이지의 네트워크 또는 지리적 위치별 트래픽 제어를 참고하십시오.

사용자 네트워크 트래픽을 필터링하기 위해 최신 정보를 사용하고 있음을 확인하기 위해 Cisco는 사용자가 위치 정보 데이터베이스(GeoDB)를 정기적으로 업데이트할 것을 강력하게 권장합니다. GeoDB 업데이트를 다운로드하고 설치하는 것에 대한 정보는 35-20페이지의 위치 정보 데이터베이스 업데이트를 참고하십시오.

사용 중인 위치 정보 개체를 삭제할 수 없습니다. 또한, 액세스 제어 정책에서 사용되는 위치 정보 개체를 수정한 후, 변경을 적용하려면 액세스 제어 정책을 재적용해야 합니다.

위치 정보 개체를 추가하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Object Management(개체 관리)**를 선택합니다.

Object Management(개체 관리) 페이지가 나타납니다.

단계 2 **Geolocation(위치 정보)**을 선택합니다.

Geolocation Objects(위치 정보 개체) 페이지가 나타납니다.

단계 3 **Add Geolocation(위치 정보 추가)**을 클릭합니다.

Geolocation Objects(위치 정보 개체) 팝업 창이 나타납니다.

단계 4 위치 정보 개체의 **Name(이름)**을 입력합니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 모두 사용할 수 있습니다.

단계 5 위치 정보 개체에 포함할 대륙 및 국가에 대한 확인 상자를 선택합니다.

대륙을 선택하면 해당 대륙 내의 모든 국가, 그리고 GeoDB 업데이트가 향후 해당 대륙에 추가할 수 있는 모든 국가를 선택합니다. 대륙에 속한 모든 국가를 선택 취소하면 대륙을 선택 취소합니다. 국가 및 대륙의 모든 조합을 선택할 수 있습니다.

단계 6 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

위치 정보 개체가 추가됩니다.

3 장

디바이스 구성 관리

Device Management(디바이스 관리) 페이지를 통해 ASA FirePOWER 모듈에 대한 디바이스 및 인터페이스 구성을 관리할 수 있습니다.

주의 ASA를 장애 조치 페어로 구성할 경우, ASA FirePOWER 구성은 보조 디바이스의 ASA FirePOWER 모듈과 자동으로 동기화되지 않습니다. 따라서 변경할 때마다 직접 기본 디바이스에서 ASA FirePOWER 구성을 내보내고 보조 디바이스로 이를 가져와야 합니다. 장애 조치의 경우, 모듈은 또한 실패한 디바이스의 모든 구성을 손실합니다.

자세한 내용은 다음 섹션을 참고하십시오.

디바이스 구성 수정

Device Management(디바이스 관리) 페이지의 Device(디바이스) 탭은 ASA FirePOWER 모듈에 적용될 때, 디바이스 상세 구성 및 정보를 표시합니다. 또한 이를 통해 표시된 모듈 이름의 변경 및 관리 설정 수정과 같이 디바이스 구성의 일부를 변경할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

일반 디바이스 구성 수정

라이센스: 모두

Device(디바이스) 탭의 General(일반) 섹션에는 변경 가능한 모듈 이름이 표시됩니다. 여기에서, 디바이스가 패킷을 ASA FirePOWER 모듈에 전송할 수 있는지 여부를 지정할 수 있습니다.

일반 디바이스 구성을 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Device Management(디바이스 관리) > Device(디바이스)**를 선택합니다.

Device(디바이스) 페이지가 나타납니다.

단계 2 **General(일반)** 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

General(일반) 팝업 창이 나타납니다.

단계 3 **Name(이름)** 필드에 모듈에 할당된 새 이름을 입력합니다. +, (,), {, }, #, &, \, <, >, ?, ‘, 및 “와 같은 유효하지 않은 문자를 제외하고 영숫자 문자 및 특수 문자를 입력할 수 있습니다.

단계 4 **Transfer Packets(패킷 전송)** 확인 상자를 선택하여 패킷 데이터가 이벤트와 함께 ASA FirePOWER 모듈에 저장되도록 합니다. 디바이스가 이벤트로 패킷 데이터를 전송하는 것을 방지하려면 확인 상자을 비워둡니다.

단계 5 **Save(저장)**를 클릭합니다.

변경 내용이 저장됩니다. 디바이스 구성을 적용할 때까지 변경 사항이 적용되지 않는다는 점에 유의하십시오. 자세한 내용은 3-4페이지의 디바이스 구성에 변경 사항 적용을 참고하십시오.

디바이스 시스템 설정 보기

라이센스: 모두

Device(디바이스) 탭의 System(시스템) 섹션은 다음 표에 설명된 대로 시스템 정보의 읽기 전용 표를 표시합니다.

표 3-1 시스템 섹션 표 필드

필드	설명
모델	디바이스의 모델 이름 및 번호입니다.
일련 번호	디바이스의 섀시의 일련 번호입니다.
시간	디바이스의 현재 시스템 시간입니다.
버전	ASA FirePOWER 모듈에 현재 설치된 소프트웨어 버전입니다.
정책	시스템 정책으로 연결되는 링크는 ASA FirePOWER 모듈에 적용됩니다.

고급 디바이스 설정의 이해

Device(디바이스) 탭의 Advanced(고급) 섹션은 다음 표에 설명된 대로 고급 구성 설정을 표시합니다.

표 3-2 고급 섹션 표 필드

필드	설명
Application Bypass(애플리케이션 우회)	모듈에서 Automatic Application Bypass(자동 애플리케이션 우회)의 상태입니다.
Bypass Threshold(우회 임계값)	밀리초로 나타낸 Automatic Application Bypass(자동 애플리케이션 우회) 임계값입니다.

Advanced(고급) 섹션을 사용하여 이 설정을 수정할 수 있습니다. 자세한 내용은 다음 섹션을 참고하십시오.

- 3-3페이지의 자동 애플리케이션 우회
- 3-3페이지의 고급 디바이스 설정 수정

자동 애플리케이션 우회

라이센스: 모두

Automatic Application Bypass(자동 애플리케이션 우회, AAB) 기능은 인터페이스를 통해 패킷을 처리하는 데 허용된 시간을 제한하고 이 기능을 사용하면 시간이 초과되는 경우 패킷이 탐지를 우회할 수 있습니다. 이 기능은 모든 배포에서 기능하지만, 인라인 배포에서 특히 유용합니다.

패킷 처리 지연을 패킷 대기 시간을 위한 네트워크의 허용 오차와 균형을 맞춥니다. Snort 내의 오류 또는 디바이스 구성 오류로 인해 트래픽 처리 시간이 지정된 임계값을 초과하는 경우 AAB는 Snort가 실패 후 10분 내에 재시작하도록 하고, 과도한 처리 시간의 원인을 조사하기 위한 분석 가능한 문제 데이터를 생성합니다.

옵션을 선택한 경우 우회 임계값을 변경할 수 있습니다. 기본 설정은 3000밀리초(ms)입니다. 유효한 범위는 250~60,000ms입니다.

참고 AAB는 단일 패킷을 처리하는 데 과도한 시간이 소요될 때만 활성화됩니다. AAB를 사용하면, 시스템은 모든 Snort 프로세스를 중단합니다.

Automatic Application Bypass(자동 애플리케이션 우회)의 활성화와 우회 임계값 설정에 대한 자세한 내용은 3-3페이지의 고급 디바이스 설정 수정을 참고하십시오.

고급 디바이스 설정 수정

Device(디바이스) 탭의 Advanced(고급) 섹션을 사용하여 Automatic Application Bypass(자동 애플리케이션 우회)를 변경할 수 있습니다.

고급 디바이스 설정을 변경하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Device Management(디바이스 관리) > Device(디바이스)**를 선택합니다.

Device(디바이스) 페이지가 나타납니다.

단계 2 **Advanced(고급))** 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

Advanced(고급) 팝업 창이 나타납니다.

단계 3 선택적으로, 네트워크가 대기 시간에 민감한 경우 **Automatic Application Bypass(자동 애플리케이션 우회)**를 선택합니다. Automatic Application Bypass(자동 애플리케이션 우회)는 인라인 배포에서 가장 유용합니다. 자세한 내용은 3-3페이지의 자동 애플리케이션 우회를 참고하십시오.

단계 4 Automatic Application Bypass(자동 애플리케이션 우회) 옵션을 선택하면, 밀리초(ms) 단위로 **Bypass Threshold(우회 임계값)**를 입력할 수 있습니다. 기본 설정은 3000밀리초이고 유효한 범위는 250~60,000ms입니다.

단계 5 **Save(저장)**를 클릭합니다.

변경 내용이 저장됩니다. 디바이스 구성을 적용할 때까지 변경 사항이 적용되지 않는다는 점에 유의하십시오. 자세한 내용은 3-4페이지의 디바이스 구성에 변경 사항 적용을 참고하십시오.

ASA FirePOWER 모듈 인터페이스 관리

라이센스: 제어, 보호

ASA FirePOWER 인터페이스를 수정할 때, ASA FirePOWER 모듈에서 인터페이스의 보안 영역만 구성할 수 있습니다. 자세한 내용은 2-33페이지의 보안 영역 작업을 참고하십시오.

ASDM 및 CLI를 사용하여 인터페이스를 구성합니다.

ASA FirePOWER 인터페이스를 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Device Management(디바이스 관리) > Interfaces(인터페이스)**를 선택합니다.

Interfaces(인터페이스) 페이지가 나타납니다.

단계 2 수정하려는 인터페이스 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Interfaces(인터페이스 수정) 팝업 창이 나타납니다.

단계 3 **Security Zone(보안 영역)** 드롭다운 목록에서 기존 보안 영역을 선택하거나, 새 보안 영역을 추가하려면 **New(신규)**를 선택합니다.

단계 4 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

보안 영역이 구성됩니다. 디바이스 구성을 적용할 때까지 변경 사항이 적용되지 않는다는 점에 유의하십시오. 자세한 내용은 3-4페이지의 디바이스 구성에 변경 사항 적용을 참고하십시오.

디바이스 구성에 변경 사항 적용

라이센스: 모두

디바이스의 ASA FirePOWER 구성을 변경한 후 적용해야 모듈 전반에 걸쳐 효과가 나타납니다. 디바이스에는 적용되지 않은 변경 사항이 있거나 이 옵션이 비활성화되어 있다는 점에 유의하십시오.

인터페이스를 수정하고 디바이스 정책을 재적용하는 경우, Snort는 사용자가 수정한 것 외에도 디바이스의 모든 인터페이스 인스턴스에 대해 재시작한다는 점에 유의하십시오.

디바이스에 변경 내용을 적용하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Device Management(디바이스 관리) > Device(디바이스)** 또는 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Device Management(디바이스 관리) > Interfaces(인터페이스)**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

단계 2 **Apply ASA FirePOWER Changes(ASA FirePOWER 변경 사항 적용)**를 클릭합니다.

단계 3 메시지가 표시되면 **Apply(적용)**를 클릭합니다.

디바이스 변경 사항이 적용됩니다.

팁 또는, Apply Device Changes(디바이스 변경 사항 적용) 대화 상자에서 **View Changes(변경 사항 보기)**를 클릭합니다. Device Management Revision Comparison Report(디바이스 관리 수정 비교 보고서) 페이지가 새 창에 나타납니다. 자세한 내용은 3-5페이지의 디바이스 관리 수정 비교 보고서 사용을 참고하십시오.

단계 4 **OK(확인)**를 클릭합니다.

Device Management(디바이스 관리) 페이지로 돌아갑니다.

디바이스 관리 수정 비교 보고서 사용

라이센스: 모두

디바이스 관리 비교 보고서에서는 어플라이언스에 대해 변경한 내용을 적용 전에 볼 수 있습니다. 보고서는 현재 어플라이언스 구성과 제안된 어플라이언스 구성의 모든 차이점을 표시합니다. 따라서 잠재적 구성 오류가 있으면 찾아낼 수 있습니다.

어플라이언스 변경 사항을 적용하기 전에 비교하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Device Management(디바이스 관리) > Device(디바이스)** 또는 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Device Management(디바이스 관리) > Interfaces(인터페이스)**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

단계 2 **Apply Changes(변경 사항 적용)**를 클릭합니다.

Apply Device Changes(디바이스 변경 사항 적용) 팝업 창이 나타납니다. 어플라이언스에 적용되지 않은 변경 사항이 있어야 합니다. 그렇지 않으면 Apply Changes(변경 사항 적용) 버튼이 비활성 상태로 표시됩니다.

단계 3 **View Changes(변경 사항 보기)**를 클릭합니다.

Device Management Revision Comparison Report(디바이스 관리 수정 비교 보고서) 페이지가 새 창에 나타납니다.

단계 4 **Previous(이전)** 및 **Next(다음)**를 클릭하여 제안된 어플라이언스 구성 및 현재 어플라이언스 구성 간의 차이를 스크롤하여 볼 수 있습니다.

단계 5 또는 **Comparison Report(비교 보고서)**를 클릭하여 보고서의 PDF 버전을 만듭니다.

원격 관리 구성

라이센스: 모두

한 FireSIGHT 시스템 어플라이언스를 다른 어플라이언스로 관리하려면 두 어플라이언스 사이에 양방향 SSL 암호화 통신 채널을 설정해야 합니다. 어플라이언스는 채널을 사용하여 구성 및 이벤트 정보를 공유합니다. 고가용성 피어도 채널을 사용하며, 기본 포트는 8305/tcp입니다.

관리할 어플라이언스, 즉 방어 센터로 관리하려는 디바이스에 원격 관리를 구성해야 합니다. 원격 관리를 구성한 후, 어플라이언스의 웹 인터페이스 관리를 사용하여 사용자 배포에 관리 어플라이언스를 추가할 수 있습니다.

참고 원격 관리를 구축하고 Cisco ASA with FirePOWER Services를 방어 센터에 등록한 후, ASA FirePOWER 모듈을 ASDM이 아닌 방어 센터에서 관리해야 합니다.

두 어플라이언스 간 커뮤니케이션을 활성화하려면 어플라이언스가 서로 인식할 수 있는 방법을 제공해야 합니다. 커뮤니케이션을 허용할 때 FireSIGHT 시스템이 사용하는 3가지 기준이 있습니다.

- 호스트 이름 또는 사용자가 커뮤니케이션을 설정하려는 어플라이언스의 IP 주소

  NAT 환경에서 다른 어플라이언스는 라우팅할 수 있는 주소가 없는 경우에도 원격 관리를 구성할 때 또는 관리 어플라이언스를 추가할 때 IP 주소 또는 호스트 이름을 제공해야 합니다.
- 연결을 식별하는 최대 37자의 자체 생성 영숫자 등록 키
- NAT 환경에서 FireSIGHT 시스템이 커뮤니케이션을 설정하는 데 도움이 될 수 있는 선택적인 고유한 영숫자 NAT ID

  NAT ID는 **반드시** 관리되는 어플라이언스 등록에 사용되는 모든 NAT ID 중에서 고유한 것이어야 합니다.

방어 센터에 매니지드 디바이스를 등록하는 경우, 선택한 액세스 제어 정책이 디바이스에 적용됩니다. 그러나, 사용자가 선택한 액세스 제어 정책에서 사용되는 기능에 필요한 디바이스에 대한 라이센스를 활성화하지 않은 경우, 액세스 제어 정책은 적용되지 않습니다.

로컬 어플라이언스의 원격 관리를 구성하려면 다음을 수행합니다.

액세스: Admin(관리)

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성) > Registration(등록)**을 선택합니다.

Remote Management(원격 관리) 페이지가 나타납니다.

단계 2 **Add Manager(관리자 추가)**를 클릭합니다.

Add Remote Management(원격 관리 추가) 페이지가 나타납니다.

단계 3 **Management Host(관리 호스트)** 필드에서 어플라이언스를 관리하는 데 사용할 어플라이언스의 IP 주소 또는 호스트 이름을 입력합니다.

호스트 이름은 완전히 자격을 갖춘 도메인 이름 또는 유효한 IP 주소에 로컬 DNS를 통해 확인하는 이름입니다.

NAT 환경에서 관리되는 어플라이언스를 추가할 때 IP 주소 또는 호스트 이름을 지정하려는 경우 이를 지정할 필요가 없습니다. 이 경우, FireSIGHT 시스템은 추후 제공할 NAT ID를 사용하여 관리되는 ASA FirePOWER 모듈 인터페이스에서 원격 관리자를 확인합니다.

주의 사용자 네트워크가 IP 주소를 할당하기 위해 DHCP를 사용하는 경우 IP 주소 대신 호스트 이름을 사용합니다.

단계 4 **Registration Key(등록 키)** 필드에 어플라이언스 간 커뮤니케이션을 설정하는 데 사용할 등록 키를 입력합니다.

단계 5 NAT 환경의 경우, **Unique NAT ID(고유 NAT ID)** 필드에 어플라이언스 간 커뮤니케이션을 설정하는 데 사용할 **고유한** 영숫자 NAT ID를 입력합니다.

단계 6 **Save(저장)**를 클릭합니다.

어플라이언스가 서로 커뮤니케이션할 수 있는지 확인하면 Pending Registration(보류 중인 등록) 상태가 표시됩니다.

단계 7 이 어플라이언스를 배포에 추가하려면 관리 어플라이언스의 웹 사용자 인터페이스를 사용합니다.

참고 NAT를 사용하는 일부 고가용성 배포에서 디바이스의 원격 관리를 활성화하면 부차적인 방어 센터를 관리자로 추가해야 할 수도 있습니다. 자세한 내용은 Support(지원부)에 문의하십시오.

원격 관리 수정

라이센스: 모두

관리하는 어플라이언스의 호스트 이름 또는 IP 주소를 수정하려면 다음 절차를 사용하십시오. FireSIGHT 시스템의 컨텍스트 내에서만 사용되는 이름인 관리하는 어플라이언스의 표시 이름도 변경할 수 있습니다. 어플라이언스의 표시 이름으로 호스트 이름을 사용할 수 있지만 다른 표시 이름을 입력하면 호스트 이름이 변경되지 않습니다.

원격 관리를 수정하려면 다음을 수행합니다.

액세스: Admin(관리)

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성) > Registration(등록)**을 선택합니다.

Remote Management(원격 관리) 페이지가 나타납니다.

단계 2 원격 관리 설정을 수정하려면 관리자 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Remote Management(원격 관리 수정) 페이지가 나타납니다.

단계 3 관리하는 어플라이언스의 표시 이름을 **Name(이름)** 필드에서 변경합니다.

단계 4 관리하는 어플라이언스의 IP 주소 또는 호스트 이름을 **Host(호스트)** 필드에서 변경합니다.

호스트 이름은 완전히 자격을 갖춘 도메인 이름 또는 유효한 IP 주소에 로컬 DNS를 통해 확인하는 이름입니다.

단계 5 **Save(저장)**를 클릭합니다.

변경 내용이 저장됩니다.

서버에서 **eStreamer eStreamer**구성

라이센스: FireSIGHT + 보호

eStreamer 서버로 사용할 어플라이언스가 외부 클라이언트에 eStreamer 이벤트를 스트리밍하기 전에, 이벤트를 클라이언트에게 보내는 eStreamer 서버를 구성하고, 클라이언트에 대한 정보를 제공하며, 커뮤니케이션을 설정할 경우 사용하려는 인증 자격 증명 집합을 생성하도록 해야 합니다.

eStreamer 이벤트 유형 구성

eStreamer 서버가 이벤트를 요청하는 클라이언트에 전송할 수 있는 이벤트 유형을 제어할 수 있습니다.

매니지드 디바이스 또는 방어 센터에서 사용 가능한 이벤트 유형은 다음과 같습니다.

- 침입 이벤트
- 침입 이벤트 패킷 데이터
- 침입 이벤트 추가 데이터

eStreamer에서 전송된 이벤트 유형을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성) > Registration(등록)**을 선택합니다.

Registration(등록) 페이지가 나타납니다.

단계 2 **eStreamer** 탭을 선택합니다.

eStreamer 페이지가 나타납니다.

단계 3 **eStreamer Event Configuration(이벤트 구성)**에서, eStreamer가 요청 클라이언트로 전달하도록 할 이벤트 유형 옆에 있는 확인란을 선택합니다.

방어 센터 또는 매니지드 디바이스에서 다음 중 하나 또는 전체를 선택할 수 있습니다.

- 침입 이벤트를 전송하는 **Intrusion Events(침입 이벤트)**
- 침입 이벤트와 관련된 패킷을 전송하는 **Intrusion Event Packet Data(침입 이벤트 패킷 데이터)**
- HTTP 프록시 또는 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소와 같은 침입 이벤트와 관련된 추가 데이터를 전송하는 **Intrusion Event Extra Data(침입 이벤트 추가 데이터)**

참고 이렇게 하면 eStreamer 서버에서 전송할 수 있는 이벤트를 제어할 수 있습니다. 클라이언트에서는 여전히 eStreamer 서버로 전송하는 요청 메시지에서 수신하고자 하는 이벤트 유형을 구체적으로 요청해야 합니다. 자세한 내용은 *FireSIGHT 시스템 eStreamerIntegration Guide(통합 가이드)*를 참고하십시오.

단계 4 **Save(저장)**를 클릭합니다.

설정이 저장되고 선택한 이벤트는 요청 시 eStreamer클라이언트에 전달됩니다.

eStreamer 클라이언트에 대한 인증 추가

eStreamer가 eStreamer 이벤트를 클라이언트로 전송하려면, eStreamer 페이지에서 클라이언트를 eStreamer 서버의 피어 데이터베이스에 추가해야 합니다. 또한 eStreamer 서버에서 생성된 인증 인증서를 클라이언트에 복사해야 합니다.

eStreamer 클라이언트를 추가하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성) > Registration(등록)**을 선택합니다.

Registration(등록) 페이지가 나타납니다.

단계 2 **eStreamer** 탭을 선택합니다.

eStreamer 페이지가 나타납니다.

단계 3 **Create Client(클라이언트 생성)**를 클릭합니다.

Create Client(클라이언트 생성) 페이지가 나타납니다.

단계 4 **Hostname(호스트 이름)** 필드에 eStreamer 클라이언트를 실행하는 호스트의 IP 주소 또는 호스트 이름을 입력합니다.

참고 호스트 이름을 사용하는 경우, eStreamer 서버는 **반드시** 호스트를 IP 주소로 확인할 수 있어야 합니다. DNS 확인을 설정하지 않은 경우, 이를 먼저 구성하거나 IP 주소를 사용해야 합니다.

단계 5 인증서 파일을 암호화하려면, **Password(비밀번호)** 필드에 비밀번호를 입력합니다.

단계 6 **Save(저장)**를 클릭합니다.

eStreamer 서버는 이제 호스트가 eStreamer 서버의 포트 8302에 액세스하는 것을 허용하고 클라이언트 서버 인증 중에 사용할 인증 인증서를 만듭니다. eStreamer 페이지가 **Hostname(호스트 이름)** 아래에 나열된 새 클라이언트와 함께 다시 표시됩니다.

단계 7 인증서 파일을 다운로드하려면 클라이언트 호스트 이름 옆에 있는 다운로드 아이콘( )을 클릭합니다.

단계 8 SSL 인증을 위해 클라이언트가 사용한 적절한 디렉터리에 인증서 파일을 저장합니다.

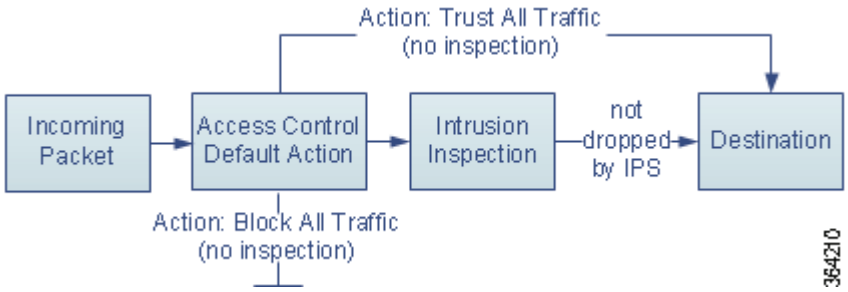
클라이언트는 이제 eStreamer 서버에 연결할 수 있습니다. eStreamer 서비스를 다시 시작할 필요가 없습니다.

팁 클라이언트에 대한 액세스를 취소하려면, 제거할 호스트 옆에 있는 삭제 아이콘( )을 클릭합니다. eStreamer 서비스를 다시 시작할 필요가 없으며, 액세스는 즉시 취소됩니다.

액세스 제어 정책 시작하기

*액세스 제어 정책*에 따라 시스템에서 네트워크의 트래픽이 처리되는 방식이 달라집니다. 각 ASA FirePOWER 모듈에는 하나의 정책만 적용할 수 있습니다.

가장 간단한 액세스 제어 정책은 *기본 작업*을 사용하여 모든 트래픽을 처리합니다. 이 기본 작업을 설정하여 모든 트래픽을 차단하거나 추가 검사 없이 신뢰할 수 있고, 트래픽을 검사하여 침입을 탐지할 수 있습니다.



인라인 배포된 ASA FirePOWER 모듈만이 트래픽의 흐름에 영향을 줄 수 있다는 점에 유의하십시오. 트래픽을 차단 또는 변경하도록 구성된 액세스 제어 정책을 수동으로 배포된 디바이스에 적용하면 예기치 않은 결과가 발생할 수 있습니다. 경우에 따라서는 시스템에서 수동으로 배포된 ASA FirePOWER 모듈에 인라인 구성을 적용하지 못할 수 있습니다.

이 장에서는 간단한 액세스 제어 정책을 생성하고 적용하는 방법을 설명합니다. 이 장에는 또한 수정, 업데이트, 비교 등 액세스 제어 정책을 관리하는 데 필요한 기본 정보가 포함되어 있습니다. 자세한 내용은 다음을 참고하십시오.

액세스 제어 정책이 보다 복잡할 경우 트래픽이 보안 인텔리전스 데이터에 근거하여 차단 목록에 추가되고 *액세스 제어 규칙*을 통해 네트워크 트래픽 로깅 및 처리가 세부적으로 제어될 수도 있습니다. 이러한 규칙은 간단하거나 복잡할 수 있으며, 다양한 기준을 사용하여 트래픽을 일치시키거나 검사할 수 있습니다. 고급 액세스 제어 정책 옵션으로 전처리, 성능 및 기타 일반 환경 설정을 제어할 수 있습니다.

기본 액세스 제어 정책을 생성한 후 배포에 맞게 조정하는 방법에 대한 자세한 내용은 다음 장을 참고하십시오.

- 5-1페이지의 보안 인텔리전스 IP 주소 평판을 사용한 차단 목록 추가에서는 최신 신뢰도 인텔리전스에 따라 연결을 즉각 차단 목록에 추가하거나 차단하는 방법에 대해 설명합니다.
- 11-1페이지의 네트워크 분석 및 침입 정책의 이해에서는 네트워크 분석 및 침입 정책이 시스템의 침입 탐지 및 방지 기능의 일부로 패킷을 전처리하고 검사하는 방식에 대해 설명합니다.
- 6-1페이지의 액세스 제어 규칙을 사용한 트래픽 흐름 조정에서는 액세스 제어 규칙이 여러 ASA FirePOWER 모듈에서 네트워크 트래픽을 처리하는 세분화된 방법을 제공합니다.
- 10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어에서는 트래픽이 대상에 대해 허용되기 전에 침입 정책 및 파일 정책이 침입, 차단된 파일 및 악성코드를 탐지하고 선택적으로 차단하여 최후의 보호 수단을 제공하는 방법에 대해 설명합니다.

액세스 제어 라이센스 및 역할 요건

ASA FirePOWER 모듈의 라이센스에 관계없이 액세스 제어 정책을 생성할 수 있지만, 대부분의 기능을 사용하려면 정책을 적용하기 전에 적절한 라이센스를 활성화해야 합니다.

자세한 내용은 4-2페이지의 액세스 제어를 위한 라이센스 요건을 참고하십시오.

액세스 제어를 위한 라이센스 요건

ASA FirePOWER 모듈의 라이센스에 관계없이 액세스 제어 정책을 생성할 수 있지만, 액세스 제어의 특정 기능을 사용하려면 정책을 적용하기 전에 라이센스가 허가된 특정 기능을 활성화해야 합니다.

경고 아이콘 및 확인 대화 상자를 사용하여 지원되는 배포 기능을 지정할 수 있습니다. 자세한 내용은 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

다음 표에는 액세스 제어 정책을 적용하는 데 필요한 라이센스 및 요건이 나와 있습니다.

표 4-1 액세스 제어를 위한 라이센스 요건

다음과 같은 액세스 제어 정책을 적용하려면...	라이센스
영역, 네트워크 또는 포트 기반의 액세스 제어를 수행하는 액세스 제어 정책 리터럴 URL 및 URL 개체를 사용하여 URL 필터링을 수행하는 액세스 제어 정책	모두
지리적 위치 데이터(소스 또는 대상 국가 또는 대륙)를 사용하여 액세스 제어를 수행하는 액세스 제어 정책	모두
침입 탐지 및 방지, 파일 제어 또는 보안 인텔리전스 필터링을 수행하는 액세스 제어 정책	보호
고급 악성코드 방지, 즉, 네트워크 기반 악성코드 탐지 및 차단을 수행하는 액세스 제어 정책	악성코드

표 4-1 액세스 제어를 위한 라이센스 요건 (계속)

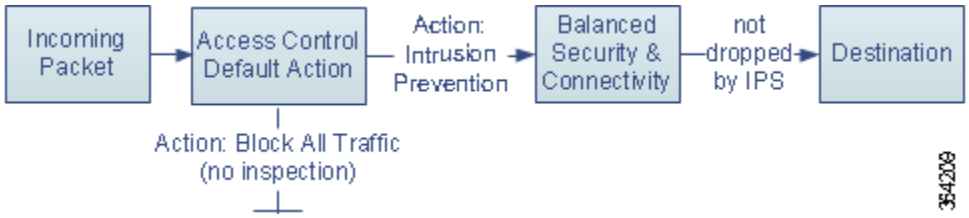
다음과 같은 액세스 제어 정책을 적용하려면...	라이센스
사용자 또는 애플리케이션 제어를 수행하는 액세스 제어 정책	제어
카테고리 및 신뢰도 데이터를 사용하여 URL 필터링을 수행하는 액세스 제어 정책	URL 필터링

기본 액세스 제어 정책 만들기

라이센스: 모두

새로운 액세스 제어 정책을 만들 때 사용자는 고유한 이름 및 기본 작업을 지정해야 합니다. 여기서, 기본 작업은 ASA FirePOWER 모듈이 모든 트래픽을 처리하는 방법을 결정하며 사용자는 추후 트래픽 흐름에 영향을 주는 기타 구성을 추가할 것입니다.

사용자는 새로운 정책을 만들 때 모든 트래픽을 추가 검사 없이 차단하는 기본 작업을 설정할 수 있습니다. 또는 다음 그림에서 보여진 것처럼 침입에 대한 트래픽을 검사하는 기본 작업을 설정할 수 있습니다.



팁 사용자가 처음 액세스 제어 정책을 만들 때, 트래픽을 신뢰하는 것을 기본 작업으로 선택할 수 없습니다. 모든 트래픽을 신뢰하는 것을 기본값으로 할 경우, 정책을 생성한 후 기본 작업을 변경합니다.

새로운 액세스 제어 정책을 만들고 기존의 액세스 제어 정책을 관리하려면 액세스 제어 정책 페이지(**Policies(정책) > Access Control(액세스 제어)**)를 사용합니다.

또는 사용자가 Default Trust All Traffic(기본값 신뢰 전체 트래픽)이라는 이름의 초기 시스템이 제공한 정책을 사용하고 수정할 수 있습니다.

액세스 제어 정책을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

팁 사용자는 또한 이 ASA FirePOWER 모듈의 기존 정책을 복사하거나 다른 ASA FirePOWER 모듈에서 정책을 가져올 수 있습니다. 정책을 복사하려면, 복사 아이콘( )을 클릭합니다. 정책을 가져오려면, B-1페이지의 구성 가져오기 및 내보내기를 참고하십시오.

단계 2 **New Policy(새로운 정책)**를 클릭합니다.

New Access Control Policy(새로운 액세스 제어 정책) 팝업 창이 나타납니다.

단계 3 정책에 고유한 **Name(이름)** 또는 **Description(설명)**을 지정합니다.

파운드 기호(#), 세미콜론(;) 또는 중괄호({})를 제외한 모든 인쇄할 문자를 스페이스 및 특수 문자를 포함하여 사용할 수 있습니다. 이름은 1개 이상의 여백이 없는 문자를 포함해야 합니다.

단계 4 초기 **Default Action(기본 작업)**을 지정합니다.

- **Block all traffic(모든 트래픽을 차단)**은 **Access Control: Block All Traffic(액세스 제어: 모든 트래픽을 차단)** 기본 작업을 통해 정책을 생성합니다.
- **Intrusion Prevention(침입 방지)**은 **Intrusion Prevention: Balanced Security and Connectivity(침입 방지: 균형 잡힌 보안 및 연결성)** 기본 작업을 통해 정책을 생성합니다.

초기 기본 작업을 선택하는 것 뿐 아니라 추후 수정 방법에 대한 참조 자료를 보려면, 4-4페이지의 네트워크 트래픽에 대한 기본 처리와 검사 설정을 참고하십시오.

단계 5 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 저장)**를 클릭합니다.

액세스 제어 정책 편집기가 나타납니다. 새 정책 구성에 관한 정보는 4-7페이지의 액세스 제어 정책 수정을 참고하십시오. 반드시 해당 정책을 적용해야 효력이 발생합니다(4-10페이지의 액세스 제어 정책 적용 참고).

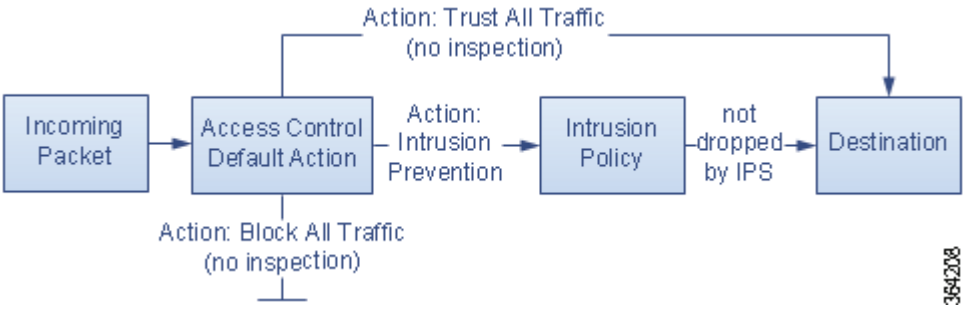
네트워크 트래픽에 대한 기본 처리와 검사 설정

라이센스: 모두

액세스 제어 정책을 만들 때, 반드시 기본 작업을 선택해야 합니다. 액세스 제어 정책에 대한 기본 작업은 시스템이 트래픽을 처리하는 방식을 결정합니다.

- 이 트래픽은 보안 인텔리전스에 의해 차단 목록에 추가된 것이 아니며
- 정책 내 규칙 중 어느 것과도 일치하지 않는 것입니다(트래픽에 일치시키거나 트래픽을 로깅하지만 처리하거나 검사하지는 않는 모니터링 규칙은 제외).

따라서, 사용자가 모든 액세스 제어 규칙 또는 보안 인텔리전스 구성을 포함하지 않고 액세스 제어 정책을 적용할 때, 사용자 네트워크의 *모든* 트래픽을 처리하는 방법을 결정하는 것은 기본 작업입니다. 사용자는 추가 검사 없이 모든 트래픽을 차단하거나 신뢰할 수 있고, 침입 및 트래픽을 검사할 수 있습니다. 다음 다이어그램에는 사용자 옵션이 표시되어 있습니다.

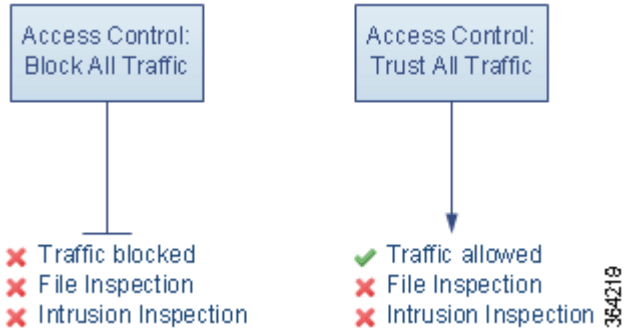


다음 표는 서로 다른 기본 작업이 트래픽을 처리하는 방법을 설명하고 각 기본 작업에 의해 처리된 트래픽에서 수행할 수 있는 검사 유형을 나열합니다. 기본 작업에 의해 처리된 트래픽에서 파일 또는 악성코드 검사를 수행할 수 **없다**는 점을 참고하십시오. 자세한 내용은 10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어를 참고하십시오.

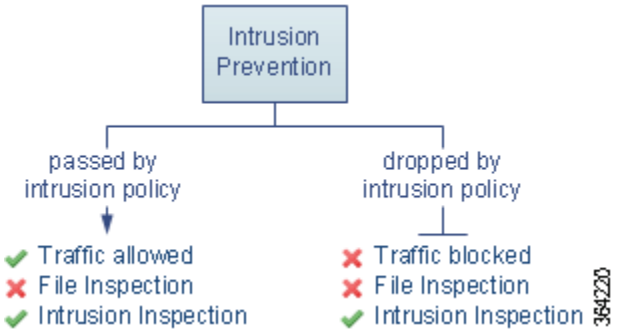
표 4-2 액세스 제어 정책 기본 작업

기본 작업	트래픽에 미치는 영향	검사 유형 및 정책
액세스 제어: 모든 트래픽 차단	추가 검사 없이 차단	없음
액세스 제어: 모든 트래픽 신뢰	신뢰(추가 검사 없이 최종 대상에서 허용)	없음
침입 방지	허용. 사용자가 지정한 침입 정책에 의해 통과된 경우(보호 라이센스 필요)	지정된 침입 정책 및 관련 변수 집합을 사용한 침입

아래의 다이어그램은 **Block All Traffic(모든 트래픽 차단)** 및 **Trust All Traffic(모든 트래픽 신뢰)** 기본 작업을 설명합니다.



아래의 다이어그램은 **Intrusion Prevention(침입 방지)** 기본 작업을 설명합니다.



사용자가 액세스 제어 정책을 처음 만들 때, 기본 작업에 의해 처리된 로깅 연결은 기본값으로 비활성화됩니다. 사용자가 침입 검사를 수행하는 기본 작업을 선택하면, 시스템은 기본값 침입 변수 집합을 선택하는 침입 정책과 함께 자동으로 연결합니다. 사용자는 정책을 생성한 후, 다음 옵션 중 하나뿐 아니라, 기본 작업 자체를 변경할 수 있습니다.

액세스 제어 정책의 기본 작업 및 관련 옵션을 변경하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 구성하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Default Action(기본 작업)**을 선택합니다.

- 모든 트래픽을 차단하려면, **Access Control: Block All Traffic(액세스 제어: 모든 트래픽 차단)**을 선택합니다.
- 모든 트래픽을 신뢰하려면, **Access Control: Trust All Traffic(액세스 제어: 모든 트래픽 신뢰)**을 선택합니다.
- 침입 정책과 함께 모든 트래픽을 검사하려면 침입 정책을 선택합니다. 이들 모두는 **Intrusion Prevention(침입 방지)** 레이블로 시작합니다. 침입 정책이 트래픽을 차단할 수 있다는 점에 유의하십시오.

주의 **반드시** `Experimental Policy 1(실험 정책 1)`을 Cisco 관계자의 지시 없이는 사용하지 마십시오. Cisco는 이 정책을 테스트용으로 사용합니다.

단계 4 사용자가 **Intrusion Prevention(침입 방지)** 기본 작업을 선택한 경우, 선택한 침입 정책과 관련된 변수 집합을 변경하려면 변수 아이콘( )을 클릭합니다.

이때 나타나는 팝업 창에서 새로운 변수 집합을 선택하고 **OK(확인)**를 클릭합니다. 사용자는 또한 수정 아이콘( )을 클릭하여 선택한 변수 집합을 새 창에서 수정할 수 있습니다. 사용자가 변수 집합을 변경하지 않는 경우, 시스템은 기본 집합을 사용합니다. 자세한 내용은 2-14페이지의 변수 집합 작업을 참고하십시오.

단계 5 기본 작업에 의해 처리된 연결에 대한 로깅 옵션을 변경하려면 로깅 아이콘( )을 클릭합니다.

일치하는 연결의 시작 및 종료 시 이를 로깅할 수 있습니다. 시스템은 차단된 트래픽의 종료를 로깅할 수 없다는 점에 유의하십시오. ASA FirePOWER 모듈 이벤트 뷰어 및 외부 시스템 로그(syslog) 또는 SNMP 트랩 서버 연결을 로깅할 수 있습니다. 자세한 내용은 25-11페이지의 액세스 제어 정책 기본 작업이 처리하는 연결 로깅을 참고하십시오.

액세스 제어 정책 관리

라이센스: 모두

Access Control Policy(액세스 제어 정책) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**)에서 정책의 적용 여부에 관한 정보와 함께 현재 사용자 지정 액세스 제어 정책을 확인할 수 있습니다.

사용자가 생성하는 사용자 지정 정책에 덧붙여, 시스템은 사용자가 수정하여 사용할 수 있는 Default Allow All Traffic(모든 트래픽 허용 기본값) 사용자 지정 정책을 제공합니다.

Access Control Policy(액세스 제어 정책) 페이지의 옵션을 통해 다음 표에 있는 조치를 취할 수 있습니다.

표 4-3 액세스 제어 정책 관리 작업

목적	방법	참고 사항
새로운 액세스 제어 정책 생성하기	**New Policy(새로운 정책)**를 클릭합니다.	4-3페이지의 기본 액세스 제어 정책 만들기
기존 액세스 제어 정책 수정하기	수정 아이콘( )을 클릭합니다.	4-7페이지의 액세스 제어 정책 수정
액세스 제어 정책 재적용하기	적용 아이콘( )을 클릭합니다.	4-10페이지의 액세스 제어 정책 적용

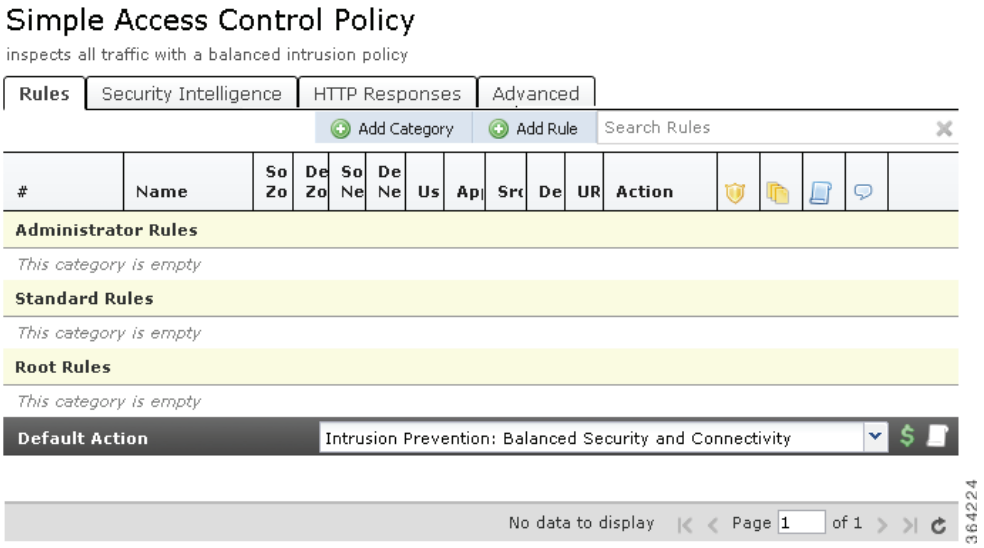
표 4-3 액세스 제어 정책 관리 작업 (계속)

목적	방법	참고 사항
액세스 제어 정책을 다른 곳에 가져오기 위해 내보내기 ASA FirePOWER 모듈	내보내기 아이콘( )을 클릭합니다.	B-1페이지의 구성 내보내기
액세스 제어 정책의 현재 구성 설정을 표시하는 PDF 보고서 보기	보고서 아이콘( )을 클릭합니다.	4-17페이지의 현재 액세스 제어 설정에 관한 보고서 생성
액세스 제어 정책 비교하기	**Compare Policies(정책 비교)**를 클릭합니다.	4-18페이지의 액세스 제어 정책 비교
액세스 제어 정책 삭제하기	삭제 아이콘( )을 클릭한 다음 정책을 삭제할 것인지 확인합니다. 적용된 액세스 제어 정책 또는 현재 적용 중인 액세스 제어 정책을 삭제할 수 없습니다.	

액세스 제어 정책 수정

라이센스: 모두

새로운 액세스 제어 정책을 처음 생성할 때, 액세스 제어 정책 편집기가 Rules(규칙) 탭에 집중되어 나타납니다. 다음 그래픽은 새로 생성된 정책을 보여줍니다. 새 정책에는 아직 규칙 또는 다른 구성이 없기 때문에, 기본 작업은 모든 트래픽을 처리합니다. 이 경우, 기본 작업은 최종 대상에서 트래픽을 허용하기 전에 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책과 함께 트래픽을 검사합니다.



액세스 제어 정책 편집기를 사용하여 규칙을 추가하고 구성하는 등의 작업을 수행합니다. 다음 목록은 사용자가 변경할 수 있는 정책 구성에 관한 정보를 제공합니다.

이름 및 설명

정책의 이름 및 설명을 변경하려면, 해당 필드를 클릭하고 새 이름 또는 설명을 입력합니다.

보안 인텔리전스

보안 인텔리전스는 악성 인터넷 콘텐츠에 대한 1차 방어선입니다. 이 기능을 사용하여 최신 평판 정보에 따라 연결을 즉각 차단 목록에 추가(차단)할 수 있습니다. 중요 리소스로 지속적으로 액세스할 수 있도록 사용자 지정 허용 목록으로 차단 목록을 무시할 수 있습니다. 이 트래픽 필터링은 규칙 및 기본 작업을 포함하여 다른 모든 정책 기반 검사, 분석, 트래픽 관리 **이전에** 발생합니다. 자세한 내용은 5-1페이지의 보안 인텔리전스 IP 주소 평판을 사용한 차단 목록 추가를 참고하십시오.

규칙

규칙은 네트워크 트래픽 처리에 대한 세분화된 방법을 제공합니다. 액세스 제어 정책 내 규칙은 1부터 시작하여 번호가 매겨집니다. 시스템은 규칙의 수를 늘리면서 하향 순서로 액세스 제어 규칙에 트래픽을 일치시킵니다.

대부분의 경우, 시스템은 *모든* 규칙의 조건이 트래픽과 일치하는 *첫 번째* 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 이 조건은 보안 영역, 네트워크 또는 지리적 위치, 포트, 애플리케이션, 요청된 URL 또는 사용자를 포함합니다. 조건은 간단하거나 복잡할 수 있습니다. 조건을 사용하는 것은 특정 라이센스에 따라 종종 다릅니다.

Rules(규칙) 탭을 사용하여 규칙을 추가하거나 분류하고, 활성화, 비활성화하며, 필터링하거나, 관리합니다. 자세한 내용은 6-1페이지의 액세스 제어 규칙을 사용한 트래픽 흐름 조정을 참고하십시오.

기본 작업

기본 작업은 보안 인텔리전스에 의해 차단 목록에 추가된 트래픽을 시스템이 처리하는 방식을 결정하며, 어떤 액세스 제어 규칙과도 일치하지 않습니다. 기본 작업을 사용하여 추가 검사 없이 모든 트래픽을 차단하거나 신뢰할 수 있고, 침입 트래픽을 검사할 수 있습니다. 또한 기본 작업이 처리한 연결의 로깅을 활성화하거나 비활성화할 수 있습니다.

자세한 내용은 4-4페이지의 네트워크 트래픽에 대한 기본 처리와 검사 설정 및 25-9페이지의 액세스 제어 처리에 기반한 연결 로깅을 참고하십시오.

HTTP 응답

시스템이 사용자의 웹 사이트 요청을 차단할 때 브라우저에서 사용자에게 표시되는 내용을 지정할 수 있습니다. 바로 시스템이 제공하는 일반 응답 페이지를 보여주거나 사용자 지정 HTML을 입력하는 것 중 하나입니다. 또한 사용자에게 경고하는 페이지를 표시할 수도 있지만 버튼을 클릭하여 계속 진행하거나 페이지를 새로 고쳐 원래 요청한 사이트를 로드하도록 할 수 있습니다. 자세한 내용은 8-14페이지의 차단된 URL을 위한 사용자 지정 웹페이지 표시를 참고하십시오.

고급 액세스 제어 옵션

고급 액세스 제어 정책 설정은 일반적으로 약간의 변경이 필요하거나 변경이 필요하지 않습니다. 기본 설정은 대부분의 배포에 적합합니다. 변경할 수 있는 고급 설정은 다음과 같습니다.

- 사용자가 요청한 각 URL에 대해 ASA FirePOWER 모듈 데이터베이스 안에 저장하는 문자의 수(25-13페이지의 연결에서 탐지된 URL 로깅 참고).
- 사용자가 최초 차단을 건너뛴 후 웹사이트를 다시 차단할 때까지 소요된 시간(8-13페이지의 차단된 웹 사이트의 사용자 우회 시간 제한 설정 참고).
- 네트워크에 여러 전처리 옵션을 맞춰 넣을 수 있도록 하는 네트워크 분석 및 침입 정책 구성 및 영역, 그리고 집합 기본값 침입 검사 작업(13-1페이지의 트래픽 전처리 사용자 정의 참고).
- 액세스 제어 정책을 적용한 경우 모든 네트워크 및 영역에 전반적으로 적용되는 고급 전송 및 네트워크 전처리 설정(17-1페이지의 고급 전송/네트워크 설정 구성 참고).

- 수동 배포에서 사용자 네트워크의 호스트 운영 체제에 기반한 패킷 단편화 및 TCP 스트림의 리어셈블리를 개선하는 적응형 프로파일(18-1페이지의 수동 배포 시 전처리 조정 참고).
- 침입 검사, 파일 제어, 파일 저장, , Advanced Malware Protection를 위한 성능 옵션(10-6페이지의 침입 방지 성능 조정 및 10-16페이지의 파일 및 악성코드 탐지 성능 및 저장 조정 참고).

액세스 제어 정책을 수정할 때, 저장되지 않은 변경 사항이 있음을 나타내는 메시지가 표시됩니다. 변경 내용을 유지하려면, 정책 편집기를 종료하기 전에 정책을 저장해야 합니다. 변경 사항을 저장하지 않고 정책 편집기를 종료하려고 할 경우, 저장되지 않은 변경 사항이 있음을 경고하는 메시지가 나타납니다. 그리고 나면 변경을 삭제하고 정책을 종료하거나 정책 편집기로 돌아갈 수 있습니다.

정책 편집기에서 60분 동안 비활성 상태가 유지된 후에는, 세션의 개인 정보를 보호하기 위해 정책 변경 사항이 삭제되고 액세스 제어 정책 페이지로 돌아갑니다. 처음 30분 동안 비활성 상태가 지속된 후, 변경 사항이 삭제되기 전에 남아있는 시간이 얼마나 되는지를 보여주는 메시지가 정기적으로 나타나 업데이트됩니다. 페이지의 모든 작업이 타이머를 취소합니다.

액세스 제어 정책을 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 구성하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 정책을 수정합니다. 상기 요약된 모든 작업을 수행합니다.

단계 4 구성을 저장하거나 새로 고칩니다.

- 변경 사항을 저장하고 수정을 계속하려면, **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)를 클릭합니다.**
- 변경 사항을 저장하고 정책을 적용하려면, **Apply ASA FirePOWER Changes(ASA FirePOWER 변경 사항 적용)**를 클릭합니다. 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.
- 변경을 삭제하려면 **Cancel(취소)**을 클릭하고, 확인 메시지가 표시되면 **OK(확인)**를 클릭합니다.

이전 정책 경고의 이해

라이센스: 모두

Access Control Policy(액세스 제어 정책) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**)에서 이전 정책은 빨간색 상태 텍스트로 나타납니다.

대부분의 경우, 액세스 제어 정책을 변경할 때마다 변경 사항을 재적용해야 효력이 발생합니다. 액세스 제어 정책이 다른 정책을 호출하거나 다른 구성을 사용할 경우, 이를 변경하려면 또한 액세스 제어 정책을 재적용해야 합니다. 또는, 침입 정책 변경을 위한 경우라면 침입 정책만 재적용할 수 있습니다.

정책 재적용이 필요한 구성 변경은 다음과 같습니다.

- 액세스 제어 정책 자체 변경: 액세스 제어 규칙에 대한 모든 변경, 기본 작업, 보안 인텔리전스 필터링, NAP 규칙을 포함하는 고급 옵션 등

- 액세스 제어 정책이 호출하는 모든 침입 정책 및 파일 정책의 변경: 네트워크 분석 정책, 침입 정책 및 파일 정책
- 액세스 제어 정책 또는 액세스 제어 정책이 호출한 정책에서 사용된 재사용 가능 개체 또는 구성의 변경: 네트워크, 포트, URL 및 위치 정보 개체. 보안 인텔리전스 목록 및 피드. 애플리케이션 필터 또는 탐지기. 침입 정책 변수 집합. 파일 목록. 보안 영역 등
- 시스템 소프트웨어, 침입 규칙 또는 취약성 데이터베이스(VDB)의 업데이트

ASA FirePOWER 모듈 인터페이스 내 여러 위치에서 이러한 구성 중 일부를 변경할 수 있다는 점에 주의하십시오. 예를 들어, 개체 관리자(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) >Object Management(개체 관리)**)를 사용하여 보안 영역을 변경할 수 있습니다.

다음 업데이트에는 정책 재적용이 필요하지 **않는다**는 점을 참고하십시오.

- URL 필터링 데이터에 대한 자동 업데이트
- 예약된 위치 정보 데이터베이스(GeoDB) 업데이트

액세스 제어 또는 침입 정책이 오래된 버전인지 확인하려면, 비교 뷰어를 사용합니다.

액세스 제어 정책이 오래된 버전인 이유를 확인하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다. 오래된 버전의 정책은 빨간색 상태 텍스트로 표시되며, ASA FirePOWER 모듈정책 업데이트가 필요한 디바이스의 수를 나타냅니다.

단계 2 오래된 버전의 정책에 대한 정책 상태를 클릭합니다.

상세한 Apply Access Control Policy(액세스 제어 정책 적용) 팝업 창이 나타납니다.

단계 3 관심 있는 변경 구성 요소 옆의 **Out-of-date(오래된 버전)** 버튼을 클릭합니다.

새 창에 정책 비교 보고서가 표시됩니다. 자세한 내용은 4-18페이지의 액세스 제어 정책 비교 및 19-9페이지의 두 침입 정책 또는 수정 버전 비교를 참고하십시오.

단계 4 또는 정책을 재적용합니다.

다음 액세스 제어 정책 적용 섹션을 참고하십시오.

액세스 제어 정책 적용

라이센스: 모두

액세스 제어 정책을 변경한 후, 사용자는 반드시 정책을 에 적용해야 합니다. 이는 ASA FirePOWER 모듈에서 모니터링 되는 네트워크에 변경을 실행하기 위함입니다. 액세스 제어 정책 및 연결된 침입 정책의 조합을 적용할 수 있지만, 액세스 제어 정책을 적용하면 자동으로 모든 관련 , 네트워크 분석 파일 정책이 적용됩니다. 이러한 정책은 독립적으로 적용할 수 없습니다.

주의 특별한 경우, 액세스 제어 정책을 적용하면 트래픽 흐름 및 처리 내에서 짧은 휴지기를 야기할 수 있으며, 또한 일부 패킷을 검사하지 않고 통과시킬 수 있습니다.액세스 제어 정책을 적용하면 최장 5분 정도 걸릴 수 있습니다. 불편을 최소화하려면, 수정 창에서 액세스 제어 정책을 적용합니다.

Snort® 프로세스를 다시 시작할 때 트래픽 중단이 발생합니다. 예를 들어, 새로운 버전의 Snort를 포함하는 액세스 제어 정책을 ASA FirePOWER 모듈을 업그레이드한 후 적용할 때, 공유 객체 규칙을 포함하는 규칙을 가져온 후 처음으로 정책을 적용할 때, 그리고 일부의 경우 VDB 업데이트를 설치할 때 프로세스가 다시 시작됩니다.

인라인 배포된 디바이스만이 트래픽 흐름에 영향을 줄 수 있음을 참고하시기 바랍니다. 수동으로 배포된 디바이스에 트래픽을 차단하거나 변경하기 위해 구성된 액세스 제어 정책을 적용하면 예측하지 못한 결과가 발생할 수 있습니다. 예를 들어, 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에 시스템은 각 차단된 연결에 대한 여러 초기 연결 이벤트를 보고할 수 있습니다.

액세스 제어 정책을 적용할 경우 다음 부가 포인트를 숙지하십시오.

- 일부 기능에는 특정 라이센스 또는 최소 버전의 시스템이 필요합니다. 자세한 내용은 4-2페이지의 액세스 제어를 위한 라이센스 요건을 참고하십시오. 또한 실행 중인 시스템 버전에 대해서는 릴리스 정보를 참고하십시오. 액세스 제어 정책이 최근에 적용된 디바이스 구성을 통해 사용 가능한 라이센스를 필요로 하는 경우, 시스템은 디바이스 구성의 마지막 부분을 적용할 때까지 액세스 제어 정책을 대기시킵니다.
- 액세스 제어 정책을 적용하면 시스템은 모든 규칙을 함께 평가하고 네트워크 트래픽을 평가하기 위해 확장된 기준 집합을 만듭니다. 지원되는 액세스 제어 정책 규칙 또는 침입 정책이 최대 수를 초과했음을 나타내는 팝업 창이 표시될 수 있습니다.. 사용자는 전체 액세스 제어 정책을 통틀어 3개 정도의 침입 정책을 선택할 수 있습니다. 자세한 내용은 4-15페이지의 성능 개선을 위한 규칙 간소화를 참고하십시오.
- 침입 규칙 업데이트를 가져올 때, 가져오기가 완료된 후 자동으로 액세스 제어 및 침입 정책을 재적용할 수 있습니다. 이를 통해 사용자는 최신 침입 규칙 및 고급 설정을 사용할 수 있을 뿐만 아니라 전처리기 규칙 및 전처리기 설정을 사용할 수 있습니다. 이는 시스템이 제공하는 기본 정책을 수정할 수 있도록 하는 업데이트를 허용하는 경우에 특히 유용합니다. 규칙 업데이트도 액세스 제어 정책의 고급 전처리 및 성능 옵션에 대한 기본값을 변경할 수 있음을 참고하십시오. 자세한 내용은 35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기를 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 4-11페이지의 전체 정책 적용은 모든 관련 네트워크 분석, 침입 및 파일 정책과 함께 액세스 제어 정책을 적용하는 빠른 적용 옵션을 사용하는 방법에 대해 설명합니다.
- 4-12페이지의 선택한 정책 구성 적용은 개별 침입 정책을 포함 하여 특정 액세스 제어 정책 구성을 적용하는 방법을 설명합니다.

전체 정책 적용

라이센스: 모두

언제든지 액세스 제어 정책을 적용할 수 있습니다. 액세스 제어 정책을 적용하면 지금 실행되고 있는 정책과 다른 관련 정책도 모두 적용됩니다.

- 네트워크 분석 정책
- 침입 정책
- 파일 정책

팝업 창을 사용하면 이 모두를 하나의 빠른 적용 작업처럼 함께 적용할 수 있습니다. 빠른 적용 옵션을 사용할 때 변경되지 않은 정책은 적용되지 않습니다.

전체 액세스 제어 정책을 빠르게 적용하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 적용하려는 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

Apply Access Control Policy(액세스 제어 정책 적용) 팝업 창이 표시됩니다.

또는 정책을 수정하는 동안 **Apply ASA FirePOWER Changes(ASA FirePOWER 변경 적용)**를 클릭하면 됩니다(4-7페이지의 액세스 제어 정책 수정 참고).

단계 3 **Apply All(모두 적용)**을 클릭합니다.

정책 적용 작업이 대기열에 추가됩니다. **OK(확인)**를 클릭하여 Access Control Policy(액세스 제어 정책) 페이지로 돌아갑니다. Task Status(작업 상태) 페이지(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 정책 적용 작업의 진행 상황을 살펴볼 수 있습니다.

선택한 정책 구성 적용

라이센스: 모두

상세 정책 적용 페이지를 사용하여 액세스 제어 정책 및 모든 관련 침입 정책에 변경 사항을 적용할 수 있습니다. 상세 페이지는 액세스 제어 정책 열 및 관련 침입 정책 열을 제공합니다. 변경 사항을 액세스 제어 정책과 관련 침입 정책에 개별적으로 적용할지 아니면 결합해서 적용할지, 아니면 둘 다 할지를 지정할 수 있습니다.

다음 경우 중 하나에서는 액세스 제어 정책 및 관련 침입 정책을 반드시 모두 적용해야 합니다.

- 액세스 제어 정책이 처음 적용되는 경우
- 침입 정책이 액세스 제어 정책에 새로 추가된 경우

두 경우 모두 액세스 제어 정책 및 침입 정책의 상태가 연결되어 있습니다. 즉 사용자는 둘 다 또는 둘 중 하나를 적용해야 합니다.

사용자가 적용하는 침입 정책에 상관 없이, 액세스 제어 정책을 적용하면 관련된 모든 네트워크 분석 현재 실행되고 있는 것과는 다른 파일 정책이 자동으로 적용된다는 점에 유의하시기 바랍니다. 이러한 정책은 독립적으로 적용할 수 없습니다.

액세스 제어 정책 목록

액세스 제어 정책 목록은 액세스 제어 정책 적용 여부를 나타내는 확인란을 제공합니다.

팁 사용자는 정책이 작업 큐에 있는 동안, 즉, 적용 작업이 완료되지 않은 동안에는 정책을 재적용할 수 있지만, 이렇게 하는 것에는 이점이 없습니다.

상태 메시지는 정책이 현재 최신인지 오래된 버전인지 여부를 표시합니다. 정책이 오래된 버전인 경우, 사용자는 해당 정책과 현재 실행 중인 정책을 편리하게 비교할 수 있습니다. 이 비교에는 액세스 제어 정책과 관련된 침입 정책에서의 차이점은 포함되지 않습니다.

침입 정책 목록

침입 정책 목록은 액세스 제어 정책과 관련된 침입 정책을 적용할 것인지 여부를 표시하는 하나 이상의 확인란을 제공합니다. 단일 회색 확인란은 모든 관련 침입 정책이 현재 실행 중인 정책과 동일함을 나타내며, 이런 경우 확인란이 지워져 선택할 수 없습니다. 변경되지 않은 침입 정책을 적용할 수 없습니다. 변경된 침입 정책만 나열되며, 개별적으로 선택할 수 있습니다. 동일한 침입 정책이 정책 내 여러 규칙과 관련된 경우, 침입 정책은 한 번씩만 나열됩니다.

다음의 경우 침입 정책에 대한 확인란을 선택했는데 액세스 제어 정책 및 침입 정책을 함께 적용해야 한다면 위에서 설명한 대로 확인란은 회색으로 표시되며 변경할 수 없습니다.

- 액세스 제어 정책이 처음 적용되는 경우
- 침입 정책이 액세스 제어 정책에 새로 추가된 경우

상태 메시지는 침입 정책이 현재 최신인지 오래된 버전인지를 표시합니다. 침입 정책이 디바이스에서 현재 실행 중인 침입 정책과 동일하지 않은 경우 오래된 버전입니다. 디바이스에 있는 것과 동일한 침입 정책은 최신 버전입니다. 정책이 오래된 버전인 경우, 사용자는 해당 정책과 현재 실행 중인 정책을 편리하게 비교할 수 있습니다.

선택한 액세스 제어 정책 구성을 적용하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 적용하려는 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

Apply Access Control Policy(액세스 제어 정책 적용) 팝업 창이 표시됩니다.

또는 정책을 수정하는 동안 **Apply ASA FirePOWER Changes(ASA FirePOWER 변경 적용)**를 클릭하면 됩니다(4-7페이지의 액세스 제어 정책 수정 참고).

단계 3 **Details(상세)**를 클릭합니다.

상세한 Apply Access Control Policy(액세스 제어 정책 적용) 팝업 창이 나타납니다. Access Control Policy(액세스 제어 정책) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어) Policy(정책)**)에서 정책의 **Status(상태)** 열에 있는 오래된 메시지를 클릭하여 팝업 창을 열 수도 있다는 점을 참고하시기 바랍니다.

단계 4 액세스 제어 정책을 적용하도록 지정하려면 액세스 제어 정책 확인란을 선택하거나 지웁니다.

단계 5 침입 정책을 적용하도록 지정하려면 침입 정책 확인란을 선택하거나 지웁니다.

단계 6 **Apply Selected Configurations(선택한 설정 적용)**를 클릭합니다.

정책 적용 작업이 대기열에 추가됩니다. **OK(확인)**를 클릭하여 Access Control Policy(액세스 제어 정책) 페이지로 돌아갑니다.

지원되는 액세스 제어 정책 규칙 또는 침입 정책이 최대 수를 초과했음을 팝업 창이 표시할 수 있음을 참고하십시오. 사용자는 반드시 액세스 제어 정책을 재평가하고 침입 정책을 통합해야 합니다. 연결된 침입 정책의 수가 (기본 작업을 포함하여) 최대치의 범위에 들어갈 때까지 액세스 제어 정책을 적용할 수 없습니다.

Task Status(작업 상태) 페이지(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 정책 적용 작업의 진행 상황을 살펴볼 수 있습니다.

액세스 제어 정책과 규칙 문제 해결

라이센스: 모두

액세스 제어 정책을 올바르게 구성하는 것, 특히 액세스 제어 규칙을 만들고 지시하는 것은 복잡한 작업입니다. 그러나, 이 작업은 효율적인 배포를 구축하는 데 필수적입니다. 정책을 주의 깊게 계획하지 않은 경우, 규칙이 다른 규칙을 사전에 대응하거나 유효하지 않은 구성을 포함할 수 있습니다. 두 규칙 모두 및 기타 정책 설정에는 추가 라이센스가 필요할 수 있습니다.

사용자의 예상대로 시스템이 트래픽을 처리할 수 있도록 액세스 제어 정책 인터페이스에는 강력한 피드백 시스템이 있습니다. 액세스 제어 정책 및 규칙 편집기의 아이콘은 액세스 제어 오류 아이콘 표에 설명된 대로 경고 및 오류를 표시합니다.

팁 액세스 제어 정책 편집기에서, **Show Warnings(경고 보기)**를 클릭하여 정책에 대한 모든 경고를 나열하는 팝업 창을 표시합니다.

또한, 시스템은 트래픽 분석과 흐름에 영향을 미칠 수 있는 모든 문제가 적용되는 순간 사용자에게 경고합니다.

표 4-4 액세스 제어 오류 아이콘

아이콘	설명	세부 사항
	오류	규칙 또는 구성에 오류가 있는 경우, 오류의 영향을 받는 모든 규칙을 비활성화하더라도 문제가 해결될 때까지 정책을 적용할 수 없습니다.
	경고	규칙 또는 다른 경고를 표시하는 액세스 제어 정책은 적용할 수 있습니다. 그러나, 경고가 표시된 오류 구성은 적용되지 않습니다. 예를 들어, 사용자는 사전 대응된 규칙 또는 비어 있는 객체 그룹, 클라우드 커뮤니케이션을 활성화하지 않은 URL 상태 구성 등 구성 오류로 인해 트래픽과 일치시킬 수 없는 규칙을 포함하는 정책을 적용할 수 있습니다. 이러한 규칙은 트래픽을 평가하지 않습니다. 경고가 표시된 규칙을 비활성화하는 경우, 경고 아이콘이 사라집니다. 경고 아이콘은 근본적인 문제를 해결하지 않고 규칙을 활성화하는 경우 다시 나타납니다. 다른 예로, 여러 기능에는 특정 라이센스 가 필요합니다. 액세스 제어 정책은 자격이 있는 디바이스에서만 성공적으로 적용됩니다.
	정보	정보 아이콘은 트래픽의 흐름에 영향을 줄 수 있는 구성에 대한 유용한 정보를 제공합니다. 이 문제는 사용자가 정책을 적용할 수 없도록 합니다. 예를 들어, 애플리케이션 제어 또는 URL 필터링을 수행하는 경우, 시스템은 해당 연결에서 애플리케이션 또는 웹 트래픽을 식별할 때까지 일부의 액세스 제어 규칙에 대해 연결의 처음 일부 패킷에 일치시키는 작업을 건너뛸 수 있습니다. 이는 애플리케이션 및 HTTP 요청을 확인할 수 있도록 연결을 설정할 수 있게 합니다. 자세한 내용은 8-6페이지의 애플리케이션 제어의 한계 및 8-11페이지의 URL 탐지 및 차단에 대한 제한을 참고하십시오.

액세스 제어 정책 및 규칙을 올바르게 구성하면 네트워크 트래픽을 처리하는 데 필요한 리소스를 줄일 수도 있습니다. 복잡한 규칙을 생성하는 것과 여러 다양한 침입 정책을 호출하는 것, 그리고 규칙을 잘못 지시하는 것은 모두 성능에 영향을 미칠 수 있습니다.

자세한 내용은 다음을 참고하십시오.

- 4-2페이지의 액세스 제어 라이센스 및 역할 요건
- 4-15페이지의 성능 개선을 위한 규칙 간소화
- 4-16페이지의 규칙 사전 대응 및 유효하지 않은 구성 경고에 대한 이해
- 4-16페이지의 성능을 개선하고 사전 대응을 방지하기 위한 규칙 지시

성능 개선을 위한 규칙 간소화

복잡한 액세스 제어 정책 및 규칙은 중요한 리소스를 명령할 수 있습니다. 액세스 제어 정책을 적용하면, 시스템은 모든 규칙을 함께 평가하고 ASA FirePOWER 모듈이 네트워크 트래픽을 평가하는 데 사용하는 확장된 기준 집합을 생성합니다. 지원되는 액세스 제어 정책 규칙 또는 침입 정책이 최대 수를 초과했음을 나타내는 팝업 창이 표시될 수 있습니다.

액세스 제어 규칙 간소화

다음 지침은 액세스 제어 규칙을 단순화하고 성능을 향상시키는 데 도움을 줄 수 있습니다.

- 규칙을 설정할 때, 사용자의 조건에서 가능한 적은 개별 요소를 사용합니다. 예를 들어, 네트워크 조건에서 개별 IP 주소 대신 IP 주소 블록을 사용합니다. 포트 조건에서 포트 범위를 사용합니다. 애플리케이션 필터, URL 카테고리 및 평판을 사용하여 애플리케이션 제어 및 URL 필터링을 수행하고, LDAP 사용자 그룹을 사용하여 사용자 제어를 수행합니다.

  구성 요소를 개체에 결합하여 액세스 제어 규칙 조건을 사용하는 것이 성능을 향상시키지는 못한다는 점에 유의하시기 바랍니다. 예를 들어, 50개의 개별적인 IP 주소를 포함하는 네트워크 개체를 사용하면 사용자가 얻을 수 있는 이점은 성능에 관한 것이 아닌 구성적인 것에 한정되며, 조건에 해당 IP 주소를 개별적으로 포함하는 것입니다.
- 가능하다면 언제든 보안 영역으로 규칙을 제한하십시오. 디바이스의 인터페이스가 영역이 제한된 규칙 안에서 영역 중 하나에 있지 않은 경우, 규칙은 해당 디바이스에서의 성능에 영향을 주지 않습니다.
- 규칙을 과잉 구성하지 않도록 하십시오. 하나의 조건이 처리하려는 트래픽과 일치시키는 데 충분하다면 두 조건을 사용하지 마십시오.

침입 정책 및 변수 집합 확산 방지

액세스 제어 정책에서 트래픽을 검사하기 위해 사용할 수 있는 고유한 침입 정책의 수는 사용자 정책의 복잡성에 따라 다릅니다. 하나의 침입 정책을 각 Allow and Interactive Block(허용 및 인터랙티브 차단) 규칙뿐 아니라 기본 작업과 연결할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 **쌍**은 하나의 정책으로 계산됩니다. 사용자는 전체 액세스 제어 정책을 통틀어 3개 정도의 침입 정책을 선택할 수 있습니다.

지원하는 침입 정책 수를 초과할 경우, 액세스 제어 정책을 재평가합니다. 침입 정책 또는 변수 집합을 결합할 수 있습니다.

얼마나 많은 정책을 선택하는지, 그리고 액세스 제어 정책의 다음 위치 중 각각에 대해 해당 정책이 얼마나 많은 변수 집합을 사용하는지 확인합니다. 고급 액세스 제어 정책 설정 내 **Intrusion Policy used before Access Control rule is determined(액세스 제어 규칙이 결정되기 전에 사용되는 침입 정책)** 옵션, 액세스 제어 정책의 기본 작업, 정책의 액세스 제어 규칙에 대한 검사 설정.

규칙 사전 대응 및 유효하지 않은 구성 경고에 대한 이해

라이센스: 모두

액세스 제어 규칙을 올바르게 구성하고 지시하는 것(그리고, 고급 배포, 네트워크 분석 규칙)은 효율적인 배포 구축에 필수적입니다. 액세스 제어 정책 안에서, 액세스 제어 규칙은 다른 규칙에 사전에 대응하거나 유효하지 않은 구성을 포함할 수 있습니다. 마찬가지로, 사용자가 액세스 제어 정책의 고급 설정을 사용하여 구성한 네트워크 분석 규칙에도 동일한 문제가 있을 수 있습니다. 시스템은 경고 및 오류 아이콘을 사용하여 이를 표시합니다.

규칙 사전 대응 경고 이해

액세스 제어 규칙의 조건은 일치하는 트래픽으로부터의 연속 규칙을 사전 대응할 수 있습니다. 예를 들면 다음과 같습니다.

```
규칙 1: 하용 관리 사용자
규칙 2: 차단 관리 사용자
```

첫 번째 규칙이 트래픽을 허용할 것이므로 위의 두 번째 규칙은 트래픽을 차단하지 않습니다.

다음 사항을 참고하십시오.

- 모든 유형의 규칙 조건은 후속 규칙에 사전 대응할 수 있습니다.
- 규칙은 또한 구성된 모든 조건이 동일한 똑같은 후속 규칙에 사전 대응합니다.
- 후속 규칙은 어느 조건이든 다른 경우 사전 대응되지 않습니다.

유효하지 않은 구성 경고 이해

액세스 제어 정책이 의존하는 외부 설정은 변경될 수 있으므로, 유효한 액세스 제어 정책 설정이 무효화될 수 있습니다. 다음 예를 참고하십시오.

- 규칙 내 소스 포트에 포트 그룹을 추가하여 ICMP 포트를 포함하기 위해 포트 그룹을 변경하는 경우 규칙은 유효하지 않게 되며, 그 옆에 경고 아이콘이 나타납니다. 사용자는 여전히 정책을 적용할 수 있지만, 규칙은 네트워크 트래픽에 아무런 영향을 끼치지 않습니다.
- 규칙에 사용자를 추가하면 해당 사용자를 제외하기 위해 LDAP 사용자 인식 설정을 변경하며, 해당 사용자는 더 이상 액세스에 의해 제어되는 사용자가 아니므로 아무런 영향을 끼치지 않습니다.

성능을 개선하고 사전 대응을 방지하기 위한 규칙 지시

라이센스: 모두

액세스 제어 정책 내 규칙은 1부터 시작하여 번호가 매겨집니다. 시스템은 규칙의 수를 늘리면서 하향 순서로 규칙에 트래픽을 일치시킵니다. 모니터링 규칙을 제외하면, 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

적절한 액세스 제어 규칙 순서는 네트워크 트래픽을 처리하는 데 필요한 리소스를 줄이고 규칙의 사전 대응을 방지합니다. 사용자가 생성한 규칙이 모든 조직과 배포에 고유하더라도 사용자의 필요를 처리하는 동안 성능을 최적화할 수 있는 규칙을 언제 지시할 지에 대해 몇 가지 따라야 할 지침이 있습니다.

가장 중요한 것에서 중요도가 낮은 순서로 규칙 지시하기

먼저, 조직의 필요에 맞게 규칙을 지시해야 합니다. 정책 상단에서 모든 트래픽에 적용되어야 하는 규칙에 우선 순위를 둡니다. 예를 들어, (허용 규칙을 사용하여) 침입 여부를 알기 위해 단일 사용자의 트래픽을 검사하고자 하지만 (신뢰 규칙을 사용하여) 부서의 다른 모든 사용자를 신뢰할 경우, 해당 지시 안에 두 가지 액세스 제어 규칙을 배치합니다.

특정한 것에서 일반적인 순서로 규칙 지시하기

특정 규칙을 먼저 배치하여 성능을 향상시킬 수 있습니다. 이는 바로 사용자가 처리하는 트래픽 범위를 좁혀 정의하는 규칙입니다. 이것은 또한 폭넓은 조건을 가진 규칙이 다양한 트래픽 유형과 일치할 수 있기 때문에, 그리고 추후 더 많은 특정 규칙에 사전 대응할 수 있기 때문에 중요합니다.

대부분의 소셜 네트워킹 사이트의 차단하되 특정 사이트에는 액세스 허용을 원하는 시나리오를 고려해 보십시오. 예를 들어, 사용자는 자신이 고용한 그래픽 디자이너가 Creative Commons Flickr(크리에이티브 커먼즈 플리커) 및 deviantART(데비앙 아트)의 콘텐츠에는 액세스할 수 있지만, Facebook(페이스북)이나 Google+(구글플러스) 등 다른 사이트에는 액세스할 수 없도록 하는 것을 원할 수도 있습니다. 사용자는 다음과 같이 사용자 규칙을 지시해야 합니다.

```
규칙 1: "Design" LDAP 사용자 그룹에 플리커, 데비앙 아트 허용
규칙 2: 소셜 네트워킹 차단
```

다음과 같이 규칙을 반대로 하는 경우

```
규칙 1: 소셜 네트워킹 차단
규칙 2: "Design" LDAP 사용자 그룹에 플리커, 데비앙 아트 허용
```

첫 번째 규칙은 플리커 및 데비앙 아트를 포함한 모든 소셜 네트워킹 트래픽을 차단합니다. 어떤 트래픽도 두 번째 규칙에 일치하지 않게 되므로 사용자가 고용한 디자이너는 사용자가 사용 가능하도록 원한 콘텐츠에도 액세스할 수 없습니다.

추후 트래픽을 검사할 규칙 배치하기

침입, 파일 및 악성코드 검사에는 리소스 처리가 필요하므로, 트래픽을 검사하는 규칙(Allow(허용), Interactive Block(인터랙티브 차단))을 적용하기 전에 트래픽을 검사하지 않는 규칙(Trust(신뢰), Block(차단))을 적용하여 성능을 높일 수 있습니다. 이것은 시스템이 검사했을 수 있는 트래픽을 Trust and Block(신뢰 및 차단) 규칙이 전환할 수 있기 때문입니다. 다른 모든 요소가 동일한, 즉, 사전 대응이 문제가 되지 않고 중요도가 동일한 일련의 규칙이 제공되는 경우, 다음과 같은 순서에 따라 배치하는 것을 고려하십시오.

- 일치하는 연결을 로깅하지만, 트래픽에 다른 작업을 수행하지 않는 Monitor(모니터링) 규칙
- 추가 검사 없이 트래픽을 처리하는 Trust and Block(신뢰 및 차단) 규칙
- 트래픽을 자세히 조사하지 않는 Allow and Interactive Block(허용 및 인터랙티브 차단) 규칙
- 악성코드, 침입 또는 둘 다에 대한 트래픽을 선택적으로 검사하는 Allow and Interactive Block(허용 및 인터랙티브 차단) 규칙

현재 액세스 제어 설정에 관한 보고서 생성

라이센스: 모두

액세스 제어 정책 보고서는 특정 시점의 정책 및 규칙 구성에 대한 레코드입니다. 사용자는 감사 목적으로나 현재 구성을 검사하기 위해 다음 정보를 포함하는 보고서를 사용할 수 있습니다.

표 4-5 액세스 제어 정책 보고서 섹션

섹션	설명
정책 정보	정책의 이름 및 설명, 정책을 최종 수정한 사용자의 이름, 정책이 마지막으로 수정된 날짜 및 시간을 제공합니다.
HTTP 차단 응답 HTTP 인터랙티브 차단 응답	정책을 사용하여 웹 사이트를 차단한 경우 사용자에게 표시하는 페이지에 세부 정보를 제공합니다.

표 4-5 액세스 제어 정책 보고서 섹션 (계속)

섹션	설명
보안 인텔리전스	정책의 보안 인텔리전스 허용 목록 및 차단 목록에 대한 세부 정보를 제공합니다.
기본 작업	기본 작업 및 관련 변수 집합을 나열합니다(있는 경우).
규칙	정책에서 각 액세스 제어 규칙을 나열하고, 해당 구성에 대한 세부 정보를 제공합니다.
고급 설정	다음을 포함하는 정책의 고급 설정에 대한 자세한 정보. • 액세스 제어 정책 및 전역 전처리 옵션을 위해 트래픽을 전처리하는 데 사용되는 네트워크 분석 정책 • 수동 배포에 대한 적응형 프로파일 설정 • 파일, 악성코드 및 침입 탐지를 위한 성능 설정 • 기타 정책 전반의 설정
참조된 개체	침입 정책 변수 집합과 SSL 정책에서 사용된 개체를 포함하여, 액세스 제어 정책에 따라.

사용자는 또한 정책을 최근 적용된 정책 또는 다른 정책과 비교하는 액세스 제어 비교 보고서를 생성할 수 있습니다. 자세한 내용은 4-18페이지의 액세스 제어 정책 비교를 참고하십시오.

액세스 제어 정책 보고서를 보려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 보고서를 생성하려는 정책 옆에 있는 보고서 아이콘( )을 클릭합니다. 액세스 제어 정책 보고서를 생성하기 전에 모든 변경 사항을 저장해야 합니다. 보고서에는 저장된 변경 사항만 표시됩니다.

시스템이 보고서를 생성합니다. 사용자에게 보고서를 컴퓨터에 저장하라는 메시지가 표시됩니다.

액세스 제어 정책 비교

라이센스: 모두

조직의 표준 준수를 위한 정책 변경 사항을 검토하거나 시스템 성능을 최적화하려면, 두 액세스 제어 정책의 차이점을 검토할 수 있습니다. 어느 것이든 두 개 의 정책을 비교하거나 현재 적용된 정책을 다른 정책과 비교할 수 있습니다. 선택적으로, 비교 후 두 정책의 차이점을 기록하는 PDF 보고서를 생성할 수 있습니다.

정책을 비교하는 데 사용할 수 있는 두 가지 도구가 있습니다.

- 비교 보기는 나란한 형식으로 두 정책 간 차이점만을 표시합니다. 각 정책의 이름은 비교 보기의 왼쪽과 오른쪽의 제목 표시줄에 표시되는데, 사용자가 **Running Configuration(실행 중인 구성)**을 선택한 경우는 제외됩니다. 이때는 빈 막대에 현재 실행 중인 정책이 표시됩니다.

  이를 사용하여 모듈 인터페이스에서 두 정책 모두를 살펴보고 탐색할 수 있습니다. 이때 각각의 차이가 강조 표시됩니다.

- 비교 보고서는 정책 보고서와 유사한 형식으로 된 두 정책 사이의 차이점만 한정적으로 다루는 레코드를 PDF 형식으로 생성합니다.

  추가 검사를 위한 정책 비교를 저장, 복사, 인쇄, 공유하는 데 이 보고서를 사용할 수 있습니다.

정책 비교 도구를 이해하고 사용하는 데 대한 자세한 내용은 다음을 참고하십시오.

- 4-19페이지의 액세스 제어 정책 비교 보기 사용
- 4-19페이지의 액세스 제어 정책 비교 보고서 사용

액세스 제어 정책 비교 보기 사용

라이센스: 모두

비교 보기는 두 정책을 나란한 형식으로 표시하는데, 각 정책은 비교 보기의 왼쪽과 오른쪽에 있는 제목 표시 줄에서 이름으로 식별됩니다. 실행 중인 구성이 아닌 두 정책을 비교하는 경우, 정책 이름과 함께 마지막 수정 시간 및 최종 수정한 사용자가 표시됩니다.

두 정책 간 차이점은 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책 사이에서 다름을 나타내고, 그러한 차이점은 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 한 정책에서는 나타나지만 다른 정책에서는 나타나지 않음을 표시합니다.

다음 표에서 모든 작업을 수행할 수 있습니다.

표 4-6 액세스 제어 정책 비교 보기 작업

목적	방법
수정 사항을 개별적으로 탐색하기	제목 표시줄 상단의 **Previous(이전)** 또는 **Next(다음)**를 클릭합니다. 좌우 측면 사이에 있는 이중 화살표 아이콘()을 움직여 **Difference(차이)** 수를 조정하여 표시되는 차이점이 무엇인지 확인합니다.
새로운 정책 비교 보기 생성하기	**New Comparison(새로 비교)을 클릭합니다.** **Select Comparison(비교 선택)** 창이 나타납니다. 자세한 내용은 4-19페이지의 액세스 제어 정책 비교 보고서 사용을 참고하십시오.
정책 비교 보고서 생성하기	**Comparison Report(비교 보고서)**를 클릭합니다. 정책 비교 보고서가 두 정책 사이의 차이점만 나열한 PDF 문서를 생성합니다.

액세스 제어 정책 비교 보고서 사용

라이센스: 모두

액세스 제어 정책 비교 보고서는 두 액세스 제어 정책 사이의 모든 차이점 또는 정책 비교 보기에서 파악한 대로, 하나의 정책을 최근에 적용된 정책과 비교한 모든 차이점에 대한 레코드로서, PDF 형식으로 표시됩니다. 이 보고서를 사용하여 두 정책 구성 사이의 차이점을 더욱 자세히 살펴보고 발견한 점을 저장하여 전달할 수 있습니다.

비교 보기에서 액세스할 수 있는 모든 정책에 대한 액세스 제어 정책 비교 보고서를 생성할 수 있습니다. 정책 보고서를 생성하기 전에 모든 변경 사항을 저장해야 합니다. 보고서에는 저장된 변경 사항만 표시됩니다.

정책 비교 보고서의 형식은 한 가지를 제외하면 정책 보고서와 동일합니다. 정책 보고서는 정책의 모든 구성을 포함하는데, 정책 비교 보고서에는 정책 간 상이한 구성만 포함됩니다. 액세스 제어 정책 비교 보고서에는 4-17페이지의 표 4-5에서 설명한 섹션이 포함됩니다.

팁 유사한 절차를 사용하여 네트워크 분석, 침입, 파일, 또는 시스템 정책을 비교할 수 있습니다.

두 개의 액세스 제어 정책을 비교하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 **Compare Policies(정책 비교)**를 클릭합니다.

Select Comparison(비교 선택) 창이 나타납니다.

단계 3 **Compare Against(비교 대상)** 드롭다운 목록에서 비교를 원하는 유형을 선택합니다.

- 두 가지의 서로 다른 정책을 비교하려면, **Other Policy(다른 정책)**를 선택합니다.

  페이지가 새로 고침되어 Policy A(정책 A) 및 Policy B(정책 B) 드롭다운 목록이 나타납니다.
- 현재 활성화된 정책과 다른 정책을 비교하려면, **Running Configuration(실행 중인 구성)**을 선택합니다.

  페이지가 새로 고쳐져 Target(대상)/Running Configuration A(실행 중인 구성 A) 및 Policy B(정책 B) 드롭다운 목록이 나타납니다.

단계 4 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 가지의 서로 다른 정책을 비교할 경우, Policy A(정책 A)와 Policy B(정책 B) 드롭다운 목록에서 비교하려는 정책을 선택합니다.
- 실행 중인 구성을 다른 정책과 비교할 경우, Policy B(정책 B) 드롭다운 목록에서 두 번째 정책을 선택합니다.

단계 5 정책 비교 보기를 표시하려면 **OK(확인)**를 클릭합니다.

비교 보기가 나타납니다.

단계 6 또는, **Comparison Report(비교 보고서)**를 클릭하여 액세스 제어 정책 비교 보고서를 생성합니다.

액세스 제어 정책 비교 보고서가 나타납니다. 사용자에게 보고서를 컴퓨터에 저장하라는 메시지가 표시됩니다.

5 장

보안 인텔리전스 IP 주소 평판을 사용한 차단 목록 추가

ASA FirePOWER 모듈은 악성 인터넷 콘텐츠에 대한 1차 방어선으로서, 사용자가 최신 평판 정보에 근거하여 연결을 즉시 차단 목록에 추가(차단)할 수 있도록 하는 보안 인텔리전스 기능을 포함하며, 동시에 더욱 리소스 집약적이고 심도 깊은 분석을 수행해야 한다는 부담을 덜어줍니다. 보안 인텔리전스 필터링에는 보호 라이센스가 필요합니다.

보안 인텔리전스는 평판이 좋지 않은 IP 주소를 오가는 트래픽을 차단함으로써 작동합니다. 이 트래픽 필터링은 여타의 정책 기반 검사, 분석 또는 트래픽 관리 **이전에** 수행됩니다.

IP 주소로 트래픽을 수동 제한하여 필터링하는 보안 인텔리전스와 유사한 기능을 수행하는 액세스 제어 규칙을 만들 수 있다는 점을 참고하십시오. 그러나, 액세스 제어 규칙은 범위가 더 넓고, 구성이 더 복잡하며, 동적 피드를 사용하여 자동으로 업데이트할 수 없습니다.

보안 인텔리전스가 차단 목록에 추가한 트래픽은 즉시 차단되므로 침입, 익스플로잇, 악성코드 등에 대한 어떤 추가적인 검사의 대상이 되지 않습니다. 또는, 수동 배포에서 권장되는 대로, 보안 인텔리전스 필터링을 위한 모니터링 전용 설정을 사용할 수 있습니다. 이는 시스템으로 하여금 차단 목록에 추가되었을 수도 있는 연결을 분석하도록 허용할 뿐 아니라 차단 목록에 대한 일치를 로깅하고 연결 종료 보안 인텔리전스 이벤트를 생성합니다.

사용자의 편의를 위해 Cisco는 *인텔리전스 피드*(*Sourcefire 인텔리전스 피드*라고도 함)를 제공합니다. 이는 평판이 좋지 않은 VRT가 결정하는 여러 IP 주소를 모아 정기적으로 업데이트하여 이뤄집니다. 인텔리전스 피드는 오픈 릴레이, 알려진 공격자, 위조된 IP 주소(bogon) 등을 추적합니다. 또한 조직의 고유한 필요에 맞게 기능을 사용자 정의할 수 있습니다. 예는 다음과 같습니다.

- **서드파티 피드** — Cisco 피드를 처리한 대로 시스템이 자동으로 업데이트할 수 있는 서드파티 평판 피드로 인텔리전스 피드를 보완할 수 있습니다
- **사용자 지정 차단 목록** — 시스템에서 필요에 따라 여러 방법으로 특정 IP 주소를 차단 목록에 수동으로 올릴 수 있습니다.
- **보안 영역에 의한 차단 목록 추가 시행** — 성능 향상을 위해 이메일 트래픽을 처리하는 영역에 스팸 차단 목록 추가를 제한하는 등 대상 시행을 원할 수 있습니다.
- **차단 목록 추가 대신 모니터링**— 특히 수동 배포와 시행 전 피드 테스팅에 유용합니다. 위반 세션을 차단하지 않고 모니터링만 수행하여 연결 종료 이벤트를 생성할 수 있습니다.
- **잘못된 긍정 제거를 위한 허용 목록** —차단 목록의 범위가 너무 넓거나 허용을 원하는 트래픽(예를 들어, 중요한 리소스)을 잘못 차단한 경우, 사용자 지정 허용 목록으로 차단 목록을 대체할 수 있습니다.

이 필터링이 만들어내는 이벤트 데이터를 필터링하고 살펴보는 보안 인텔리전스 수행을 위한 액세스 제어 정책 구성에 대한 자세한 정보는 다음 섹션을 참고하십시오.

- 5-2페이지의 보안 인텔리전스 전략 선택
- 5-3페이지의 보안 인텔리전스 허용 목록 및 차단 목록 작업
- 25-8페이지의 보안 인텔리전스(차단 목록 추가) 결정 로깅

보안 인텔리전스 전략 선택

라이센스: 보호

차단 목록을 구성하는 가장 쉬운 방법은 인텔리전스 피드를 사용하여 오픈 릴레이로 알려진 IP 주소, 알려진 공격자, 위조된 IP 주소(bogon) 등을 추적하는 것입니다. 인텔리전스 피드는 정기적으로 업데이트되므로, 이를 사용하면 시스템이 네트워크 트래픽을 필터링하는 최신 정보를 사용할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 IP 주소는 새로운 정책을 업데이트하고 적용하는 것보다 빠르게 나타났다가 사라질 수 있습니다.

인텔리전스 피드 증가를 위해 다음과 같은 경우 사용자 지정 또는 서드파티 IP 주소 목록 및 피드를 사용하여 보안 인텔리전스를 수행할 수 있습니다.

- *목록*이 업로드할 IP 주소의 정적 목록인 경우 ASA FirePOWER 모듈
- *피드*가 ASA FirePOWER 모듈이 인터넷에서 정기적으로 다운로드하는 IP 주소의 동적 목록인 경우. 인텔리전스 피드는 특수한 종류의 피드입니다.

인터넷 액세스 요구 사항을 포함하여 보안 인텔리전스 목록 및 피드 구성에 대한 자세한 정보는 2-4페이지의 보안 인텔리전스 목록 및 피드 작업을 참고하십시오.

보안 인텔리전스 전역 차단 목록 사용

분석 과정 중에 *전역 차단 목록*을 구성할 수 있습니다. 예를 들어, 공격 시도와 관련된 침입 이벤트에서 라우팅 가능한 IP 주소의 집합을 포착하는 경우, 해당 IP 주소를 차단 목록에 추가할 수 있습니다. ASA FirePOWER 모듈은 이 차단 목록(및 관련 *전역 허용 목록*)을 사용하여 모든 액세스 제어 정책에서 보안 인텔리전스를 수행합니다. 전역 목록 관리에 관한 정보는 2-6페이지의 전역 허용 목록 및 차단 목록 작업을 참고하십시오.

참고 글로벌 차단 목록(또는 글로벌 허용 목록, 아래 참고)에 대한 피드 업데이트 및 추가는 배포를 통해 자동으로 변경을 수행하지만, 보안 인텔리전스 개체에 대한 다른 변경은 액세스 제어 정책을 재적용해야 할 수 있습니다. 자세한 내용은 2-5페이지의 표 2-1을 참고하십시오.

네트워크 개체 사용

마지막으로, 차단 목록을 구성하는 간단한 방법은 IP 주소, IP 주소 블록 또는 IP 주소의 무리를 나타내는 *네트워크 개체 그룹 또는 네트워크 개체*를 사용하는 것입니다. 네트워크 개체 생성 및 변경에 대한 자세한 내용은 2-3페이지의 네트워크 개체 작업을 참고하십시오.

보안 인텔리전스 허용 목록 사용

각 액세스 제어 정책은 차단 목록 외에도 관련 허용 목록이 있는데, 이는 보안 인텔리전스 개체로 채울 수 있습니다. 한 정책의 허용 목록은 차단 목록을 대체합니다. 즉 시스템은 액세스 제어 규칙을 사용하여 허용 목록에 있는 소스 또는 대상 IP로 트래픽을 평가합니다. 해당 IP 주소가 차단 목록에 있는 경우라고 해도 마찬가지입니다. 일반적으로 차단 목록이 여전히 유용한 경우라고 해도 범위가 너무 넓고 검사를 원하는 트래픽을 오류로 차단하는 경우 허용 목록을 사용합니다.

예를 들어, 평판이 좋은 피드가 중요한 리소스에 액세스하는 것을 잘못 차단하고 있지만 사용자 조직에 전반적으로 유용한 경우, 모든 피드를 차단 목록에서 제거하는 대신 잘못 분류된 IP 주소만 허용 목록에 추가할 수 있습니다.

보안 영역에 의한 보안 인텔리전스 필터링 시행

추가 세분화를 위해 연결 내 소스 또는 대상 IP 주소가 특정 보안 영역에 위치하는지를 기반으로 한 보안 인텔리전스 필터링을 수행할 수 있습니다.

상기 허용 목록 예를 확장하기 위해 잘못 분류된 IP 주소를 허용 목록에 추가할 수 있지만 한편으로 해당 IP 주소에 액세스해야 할 사용자 조직에 의해 사용된 보안 영역을 사용하여 허용 목록 개체를 제한할 수 있습니다. 이렇게 해서, 사업적 필요가 있는 이들만 해당 허용 목록에 있는 IP 주소에 액세스할 수 있습니다. 다른 예로, 서드파티 스팸 피드를 사용하여 이메일 서버 보안 영역에서 트래픽을 차단 목록에 추가할 수 있습니다.

차단 목록 추가 대신 연결 모니터링

특정 IP 주소 또는 주소의 집합을 차단 목록에 추가하기를 원하는지 확신할 수 없는 경우, 시스템이 액세스 제어 규칙에 일치하는 연결을 통과시킬 수 있도록 하는 "모니터링 한정" 설정을 사용할 수 있으며 차단 목록에 대한 일치를 로깅하고 연결 종료 보안 인텔리전스 이벤트를 생성할 수도 있습니다. 전역 차단 목록을 모니터링 한정으로 설정할 수 없다는 점에 유의하십시오.

서드파티 피드 사용에 대한 차단을 실행하기 전에 해당 피드 테스트를 원하는 시나리오를 고려해 보십시오. 피드를 모니터링 한정으로 설정하면, 시스템은 시스템이 추가 분석을 위해 차단할 수도 있었던 연결을 허용하며, 사용자 평가를 위해 각 연결의 레코드를 로깅합니다.

수동 배포에서 성능 최적화를 위해 Cisco는 항상 모니터링 한정 설정을 사용하는 것을 권장합니다. 디바이스는 수동 배포된 것으로 트래픽 흐름에 영향을 줄 수 없습니다. 트래픽을 차단하도록 시스템을 구성하는 데는 어떤 이점도 없습니다. 또한, 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에 시스템은 각 차단된 연결에 대한 여러 초기 연결 이벤트를 보고할 수 있습니다.

보안 인텔리전스 허용 목록 및 차단 목록 작성

라이센스: 보호

허용 목록 및 차단 목록을 작성하려면, 목록을 네트워크 개체 및 그룹의 모든 조합뿐 아니라 보안 인텔리전스 피드 및 목록, 보안 영역으로 제한할 수 있는 모든 목록을 사용하여 채웁니다.

기본적으로, 액세스 제어 정책은 ASA FirePOWER 모듈의 전역 허용 목록 및 차단 목록을 사용하는데, 이는 모든 영역에 적용됩니다. 이 목록은 분석가가 채웁니다. 정책별 기반으로 전역 목록을 사용하도록 선택하지 않을 수 있습니다.

참고 채워진 전역 허용 목록 또는 차단 목록을 사용하는 액세스 제어 정책을 자격이 주어지지 않은 디바이스 보호에 적용할 수 없습니다. IP 주소를 전역 목록 둘 중 하나에 추가한 경우, **반드시** 정책을 적용하기 전에 먼저 정책의 보안 인텔리전스 구성에서 비어 있지 않은 목록을 제거해야 합니다. 자세한 내용은 2-6페이지의 전역 허용 목록 및 차단 목록 작업을 참고하십시오.

허용 목록 및 차단 목록을 작성한 후, 차단 목록에 올린 연결을 로깅할 수 있습니다. 또한 피드 및 목록을 포함하는 차단 목록에 추가한 개체를 모니터링 한정으로 설정할 수 있습니다. 이를 통해 시스템에서 액세스 제어를 사용하여 차단 목록에 올린 IP 주소를 포함하는 연결을 처리할 수 있으며 차단 목록에 대한 연결의 일치 항목을 로깅할 수도 있습니다.

허용 목록, 차단 목록 및 로깅 옵션을 구성하려면 액세스 제어 정책에서 보안 인텔리전스 탭을 사용합니다. 해당 페이지에서는 허용 목록 또는 차단 목록에서 사용할 수 있는 Available Objects(가용 개체)뿐 아니라, 허용 또는 차단 목록에 올린 개체를 제한하는 데 사용할 수 있는 Available Zones(가용 영역)를 나열합니다. 개체 또는 영역의 각 유형은 다른 아이콘으로 구분됩니다. Cisco아이콘( )으로 표시된 개체는 인텔리전스 피드에서 다른 카테고리를 나타냅니다.

차단 목록에서 차단으로 설정된 개체는 차단 아이콘( )으로 표시되는 반면 모니터링 한정 개체는 모니터링 아이콘( )으로 표시됩니다. 허용 목록이 차단 목록을 대체하므로, 두 목록에 모두 동일한 개체를 추가하는 경우, 시스템은 차단 목록에 추가한 개체를 취소선으로 표시합니다.

허용 목록 및 차단 목록에 총 255개의 개체를 추가할 수 있습니다. 즉 허용 목록의 개체 수와 차단 목록의 개체 수를 합하여 255를 초과할 수 없습니다.

허용 목록 또는 차단 목록에 `/0`의 넷마스크를 가진 네트워크 개체를 추가할 수 있지만, 해당 개체 내 `/0` 넷마스크를 사용한 주소 블록은 무시되며 허용 목록 및 차단 목록 필터링은 해당 주소에 기반하여 발생하지 않는다는 점을 참고하십시오. 보안 인텔리전스 피드에서 `/0` 넷마스크가 있는 주소 블록 또한 무시됩니다. 정책이 대상으로 하는 모든 트래픽을 모니터링하거나 차단하려는 경우, **Monitor(모니터링)** 또는 **Block(차단)** 규칙 작업과 함께 각각의 액세스 제어 정책을 사용하거나, **any**(기본값)를 사용하여 보안 인텔리전스 필터링 대신에 **Source Networks(소스 네트워크)** 및 **Destination Networks(대상 네트워크)**를 사용합니다.

액세스 제어 정책에 대한 보안 인텔리전스 허용 목록 및 차단 목록을 구축하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 구성하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Security Intelligence(보안 인텔리전스)** 탭을 선택합니다.

액세스 제어 정책에 대한 보안 인텔리전스 설정이 나타납니다.

단계 4 또는, 로깅 아이콘( )을 클릭하여 차단 목록에 올린 연결을 로깅합니다.

차단 목록에 있는 개체를 모니터링 한정으로 설정하려면 반드시 먼저 로깅을 활성화해야 합니다. 자세한 내용은 25-8페이지의 보안 인텔리전스(차단 목록 추가) 결정 로깅을 참고하십시오.

단계 5 하나 이상의 **Available Objects(가용 개체)**를 선택하여 허용 목록 및 차단 목록 구성을 시작합니다.

여러 개체를 선택하려면, Shift와 Ctrl 키를 사용하거나, 마우스 오른쪽 단추를 클릭한 후 **Select All(모두 선택)**을 선택합니다.

팁 사용자 조직의 요구를 충족하는 기존 개체가 없는 경우 포함할 기존 개체를 검색하거나, 상황에 따라 개체를 생성할 수 있습니다. 자세한 내용은 5-5페이지의 허용 목록 또는 차단 목록에 추가할 개체 검색을 참고하십시오.

단계 6 또는, **Available Zone(가용 영역)**을 선택하여 영역별 선택 개체를 제한합니다.

기본적으로 개체는 제한되지 않습니다. 즉, `Any(모든)` 영역을 가지고 있습니다. **Any(모든)**를 사용하지 않더라도 단 하나의 영역으로 제한할 수 있음을 참고하십시오. 여러 영역에서 하나의 개체를 위한 보안 인텔리전스 필터링을 수행하려면, 개체를 각 영역에 대해 별도로 허용 목록 또는 차단 목록에 추가해야 합니다. 또한, 전역 허용 목록 또는 차단 목록은 영역에 의해 제한할 수 없습니다.

단계 7 **Add to Whitelist(허용 목록에 추가)** 또는 **Add to Blacklist(차단 목록에 추가)**를 클릭합니다.

둘 중 하나의 목록에서 선택된 개체를 클릭하여 끌어 놓을 수 있습니다.

선택한 개체는 허용 목록 또는 차단 목록에 추가됩니다.

팁 목록에서 개체를 제거하려면, 삭제 아이콘( )을 클릭합니다. 여러 개체를 선택하려면, Shift(쉬프트)와 Ctrl(컨트롤) 키를 사용하거나, 마우스 오른쪽 단추로 클릭한 후 **Select All(모두 선택)**을 선택하거나 마우스 오른쪽 단추로 클릭한 후 **Delete Selected(선택된 항목 삭제)**를 선택합니다. 전역 목록을 삭제할 경우, 반드시 선택을 확인해야 합니다. 허용 목록 또는 차단 목록에서 개체를 제거하는 것은 ASA FirePOWER 모듈에서 해당 개체를 제거하지 않습니다.

단계 8 허용 목록 및 차단 목록에 개체 추가를 완료할 때까지 5-7단계를 반복합니다.

단계 9 선택적으로, **Blacklist(차단 목록)** 아래의 개체를 마우스 오른쪽 단추로 클릭한 후 **Monitor-only(모니터링 한정; 차단 안 함)**를 선택하여 차단 목록에 있는 개체를 모니터링 한정으로 설정합니다.

수동 배포에서 Cisco는 차단 목록에 있는 모든 개체를 모니터링 한정으로 설정할 것을 권장합니다. 하지만 전역 차단 목록을 모니터링 한정으로 설정할 수 없다는 점에 유의하십시오.

단계 10 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 저장)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

허용 목록 또는 차단 목록에 추가할 개체 검색

라이센스: 보호

여러 네트워크 개체, 그룹, 피드 및 목록이 있는 경우, 탐색 기능을 사용하여 허용 목록 또는 차단 목록에 추가하려는 개체를 검색합니다.

허용 목록 또는 차단 목록에 추가할 개체를 검색하려면

단계 1 **Search by name or value(이름 또는 값으로 검색)** 필드에 쿼리를 입력합니다.

일치하는 항목을 입력하여 표시하면 Available Objects(가용 개체) 목록이 업데이트됩니다. 검색 문자열을 지우려면 검색 필드 위에 있는 다시 로드 아이콘( )을 클릭하거나 검색 필드에서 지우기 아이콘( )을 클릭합니다.

해당 개체에 대해 구성된 네트워크 개체 이름값을 검색할 수 있습니다. 예를 들어, `Texas Office`(텍사스 사무소)라는 이름의 개별 네트워크 개체가 구성값 `192.168.3.0/24`를 가지고 있는 경우 그리고 해당 개체가 `US Offices`(미국 사무소) 그룹 개체에 속해 있는 경우, `Tex`와 같은 부분 검색 문자열 또는 완전한 검색 문자열을 입력하거나 `3`과 같은 값을 입력하여 두 개체 모두를 표시할 수 있습니다.

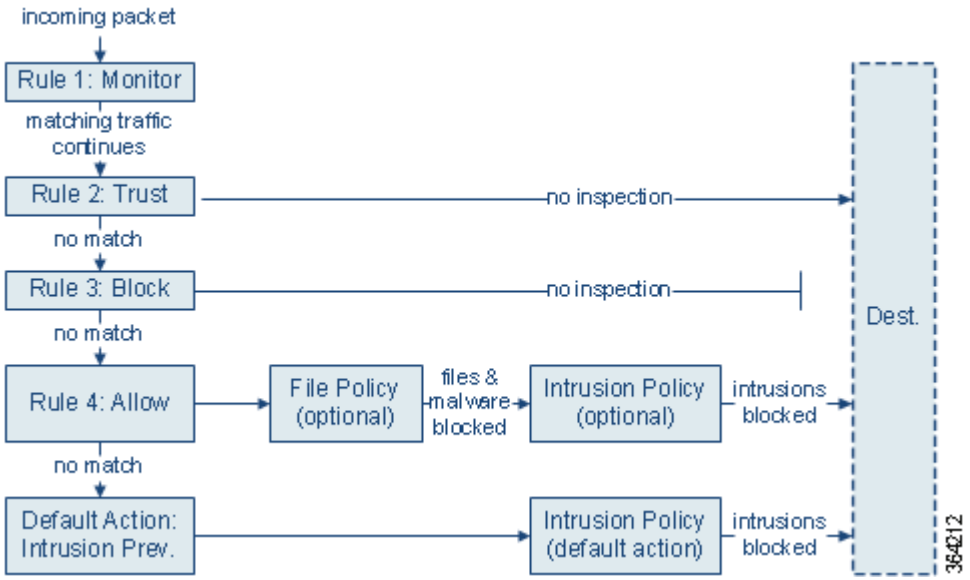
액세스 제어 규칙을 사용한 트래픽 흐름 조정

액세스 제어 정책 내, *액세스 제어 규칙*은 네트워크 트래픽을 처리하는 세분화된 방법을 제공합니다.

보안 인텔리전스 기반의 트래픽 필터링, 그리고 일부 디코딩 및 전처리 과정은 네트워크 트래픽이 액세스 제어 규칙으로 평가되기 **전에** 이루어집니다.시스템은 사용자가 지정하는 순서로 액세스 제어 규칙에 트래픽을 일치시킵니다. 대부분의 경우, 시스템은 *모든* 규칙의 조건이 트래픽과 일치하는 *첫 번째* 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 조건은 간단하거나 복잡할 수 있습니다. 사용자는 보안 영역, 네트워크 또는 지리적 위치, 포트,애플리케이션, 요청된 URL 및 사용자로 트래픽을 제어할 수 있습니다.

각 규칙에는 일치하는 트래픽의 모니터링, 신뢰, 차단 또는 허용 여부를 결정하는 *작업*이 있습니다. 트래픽을 허용하는 경우, 트래픽이 자산에 도달하거나 네트워크에서 빠져나가기 전에 시스템에서 먼저 침입 또는 파일 정책으로 트래픽을 검사하여 익스플로잇, 악성코드 또는 금지된 파일을 차단하도록 지정할 수 있습니다. 그러나, 시스템에서 트래픽을 신뢰하거나 차단한 후에는 추가 검사를 수행하지 **않습니다**.

다음 시나리오에서는 트래픽이 인라인 침입 방지 배포에서 액세스 제어 규칙에 의해 평가될 수 있는 방법을 요약합니다.



이 시나리오에서, 트래픽은 다음과 같이 평가됩니다.

- **규칙 1: 모니터링**은 가장 먼저 트래픽을 평가합니다. 모니터링 규칙은 네트워크 트래픽을 추적하고 로깅하지만 트래픽 흐름에 영향을 주지 않습니다. 시스템은 허용할지 아니면 거부할지 여부를 결정하기 위해 계속해서 트래픽을 추가 규칙에 일치시킵니다.
- **규칙 2: 신뢰**는 두 번째로 트래픽을 평가합니다. 일치하는 트래픽은 추가 검사 없이 목적지로 전달될 수 있습니다. 일치하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- **규칙 3: 차단**은 세 번째로 트래픽을 평가합니다. 일치하는 트래픽은 추가 검사 없이 차단됩니다. 일치하는 않는 트래픽은 마지막 규칙으로 계속 진행됩니다.
- **규칙 4: 허용**은 마지막 규칙입니다. 이 규칙에서, 일치하는 트래픽은 허용되지만 해당 트래픽 내 금지된 파일, 악성코드, 침입 및 익스플로잇은 탐지 및 차단됩니다. 나머지 금지되지 않은 비악성 트래픽은 목적지로 허용됩니다. 파일 검사나 침입 검사 중 하나만 수행하거나 둘 다 수행하지 않는 추가 Allow(허용) 규칙을 사용할 수도 있습니다.
- **기본 작업**은 어느 규칙과도 일치하지 않는 모든 트래픽을 처리합니다. 이 시나리오에서 기본 작업은 비악성 트래픽의 통과를 허용하기 전에 침입 방지를 수행하는 것입니다. 다른 배포에서는 추가 검사 없이 모든 트래픽을 신뢰하거나 차단하는 기본 작업이 있을 수 있습니다. (기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다.)

액세스 제어 규칙에 대한 자세한 내용은 다음을 참고하십시오.

- 6-2페이지의 액세스 제어 규칙 생성 및 수정
- 6-10페이지의 정책에서 액세스 제어 규칙 관리
- 4-14페이지의 액세스 제어 정책과 규칙 문제 해결

액세스 제어 규칙 생성 및 수정

라이센스: 모두

액세스 제어 정책 내, 액세스 제어 규칙은 네트워크 트래픽을 처리하는 세분화된 방법을 제공합니다. 각 액세스 제어 규칙에는 고유한 이름 외에도, 다음과 같은 기본 구성 요소가 있습니다.

상태

기본적으로 규칙이 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다.

위치

액세스 제어 정책 내 규칙은 1부터 시작하여 번호가 매겨집니다. 시스템은 규칙의 수를 늘리면서 하향 순서로 규칙에 트래픽을 일치시킵니다. 모니터링 규칙을 제외하면, 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 조건은 보안 영역, 네트워크 또는 지오로케이션, 포트, 애플리케이션, 요청된 URL 또는 사용자 기준으로 트래픽의 일치 여부를 확인할 수 있습니다. 조건은 간단하거나 복잡할 수 있습니다. 조건을 사용하는 것은 라이센스에 따라 종종 다릅니다.

작업

규칙의 작업은 시스템이 일치하는 트래픽을 처리하는 방법을 결정합니다. 일치하는 트래픽을 모니터링, 신뢰, 차단 또는 허용(추가 검사 실행 또는 실행 안 함)할 수 있습니다. 시스템은 신뢰받는 트래픽 또는 차단된 트래픽에 대해 검사를 수행하지 **않습니다**.

검사

액세스 제어 규칙에 대한 검사 옵션은, 사용자가 허용할 수도 있는 악성 트래픽을 시스템이 검사 및 차단하는 방법을 제어합니다. 규칙으로 트래픽을 허용하는 경우 트래픽이 자산에 도달하거나 네트워크에서 빠져나가기 전에, 시스템에서 먼저 침입 또는 파일 정책으로 트래픽을 검사하여 익스플로잇, 악성코드 또는 금지된 파일을 차단하도록 지정할 수 있습니다.

로깅

규칙의 로깅 설정은, 처리하는 트래픽에 대해 시스템에서 유지하는 레코드를 관리합니다. 규칙과 일치하는 트래픽을 기록할 수 있습니다. 일반적으로, 연결의 시작 및 끝에 세션을 로깅할 수 있습니다. ASA FirePOWER 모듈 및 시스템 로그(syslog) 또는 SNMP 트랩 서버에 대한 연결을 로깅할 수 있습니다.

코멘트

액세스 제어 규칙에 대한 변경 사항을 저장할 때마다 코멘트를 추가할 수 있습니다.

액세스 제어 규칙을 추가 및 수정하려면 액세스 제어 규칙 편집기를 사용하십시오. 액세스 제어 정책 편집기의 Rules(규칙) 탭에서 규칙 편집기에 액세스할 수 있습니다. 규칙 편집기에서는 다음과 같은 작업을 할 수 있습니다.

- 편집기의 상단에서 규칙의 이름, 상태, 위치 및 작업과 같은 기본 속성을 구성합니다.
- 편집기 하단의 왼쪽 탭을 사용하여 조건을 추가합니다.
- 편집기 하단의 오른쪽 탭을 사용하여 검사 및 로깅 옵션을 구성하고 규칙에 코멘트를 추가합니다. 편의를 위해, 사용자가 어떤 탭에 있든 편집기에는 규칙의 검사 및 로깅 옵션이 나열됩니다.

참고 액세스 제어 규칙을 올바르게 생성하고 지시하는 것은 복잡한 과제이지만 효율적인 배포 구축에 필수적입니다. 정책을 신중하게 계획하지 않으면 규칙이 다른 규칙을 선점하거나, 추가 라이센스를 요구하거나, 잘못된 구성을 포함할 수 있습니다. 시스템이 트래픽을 예상대로 처리하도록 보장하기 위해, 액세스 제어 정책 인터페이스에는 규칙에 대한 강력한 경고 및 오류 피드백 시스템이 있습니다. 자세한 내용은 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

액세스 제어 규칙을 만들거나 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 규칙을 추가하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

Rules(규칙) 탭을 중점적으로 다루는 정책 페이지가 나타납니다.

단계 3 다음 옵션을 이용할 수 있습니다.

- 새 규칙을 추가하려면 **Add Rule(규칙 추가)**을 클릭합니다.
- 기존 규칙을 수정하려면 수정하려는 규칙 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 규칙 편집기가 나타납니다.

단계 4 규칙의 **Name(이름)**을 입력합니다.

각 규칙에는 고유한 이름이 있어야 합니다. 콜론(:)을 제외한 특수 문자 및 공백을 포함하여 최대 30개의 인쇄 가능한 문자를 사용할 수 있습니다.

단계 5 위에 요약된 대로 규칙 구성 요소를 구성합니다. 다음을 구성하거나 기본값을 수락할 수 있습니다.

- 규칙이 **Enabled(활성화)** 상태인지 여부를 지정합니다.
- 규칙 위치를 지정합니다(6-4페이지의 규칙의 평가 순서 지정 참고).
- 규칙 **Action(작업)**을 선택합니다(6-6페이지의 규칙 작업을 사용하여 트래픽 관리 및 검사 결정 참고).
- 규칙의 조건을 구성합니다(6-5페이지의 조건을 사용하여 규칙이 처리하는 트래픽 지정 참고).
- Allow and Interactive Block(허용 및 인터랙티브 차단) 규칙의 경우, 규칙의 **Inspection(검사)** 옵션을 구성합니다(10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어 참고).
- **Logging(로깅)** 옵션을 지정합니다(25-1페이지의 네트워크 트래픽의 연결 로깅 참고).
- **Comments(코멘트)**를 추가합니다(6-10페이지의 규칙에 코멘트 추가 참고).

단계 6 **Store FirePOWER Changes(FirePOWER 변경 사항 저장)**를 클릭하여 규칙을 저장합니다.

사용자의 규칙이 저장됩니다. 삭제 아이콘( )을 클릭하여 규칙을 삭제할 수 있습니다. 변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

규칙의 평가 순서 지정

라이센스: 모두

처음으로 액세스 제어 규칙을 만드는 경우 규칙 편집기에서 **Insert(삽입)** 드롭다운 목록을 사용하여 해당 위치를 지정합니다. 액세스 제어 정책 내 규칙은 1부터 시작하여 번호가 매겨집니다. 시스템은 규칙의 수를 늘리면서 하향 순서로 액세스 제어 규칙에 트래픽을 일치시킵니다.

대부분의 경우, 시스템은 *모든* 규칙의 조건이 트래픽과 일치하는 *첫 번째* 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. Monitor(모니터링) 규칙(트래픽을 로깅하지만 트래픽 흐름에 영향을 주지 않음)의 경우를 제외하고 트래픽이 규칙과 일치하면 시스템은 추가적이고 우선 순위가 낮은 규칙에 대해 계속해서 트래픽을 평가하지 **않습니다**.

팁 적절한 액세스 제어 규칙 순서는 네트워크 트래픽을 처리하는 데 필요한 리소스를 줄이고 규칙의 사전 대응을 방지합니다. 사용자가 생성한 규칙이 모든 조직과 배포에 고유하더라도 사용자의 필요를 처리하는 동안 성능을 최적화할 수 있는 규칙을 언제 지시할 지에 대해 몇 가지 따라야 할 지침이 있습니다. 자세한 내용은 4-16페이지의 성능을 개선하고 사전 대응을 방지하기 위한 규칙 지시를 참고하십시오.

번호로 규칙의 순서를 지정하는 것 외에도 카테고리로 규칙을 그룹화할 수 있습니다. 기본적으로 시스템에서는 Administrator(관리자), Standard(표준) 그리고 Root(루트)의 3가지 카테고리를 제공합니다. 사용자 지정 카테고리를 추가할 수는 있지만, Cisco에서 제공하는 카테고리를 삭제하거나 순서를 변경할 수는 없습니다. 기존 규칙의 위치나 카테고리를 변경하는 방법에 대한 자세한 내용은 6-12페이지의 규칙의 위치 또는 카테고리 변경을 참고하십시오.

규칙을 수정 또는 생성하는 동안 카테고리에 추가하려면 다음을 수행합니다.

단계 1 액세스 제어 규칙 편집기의 **Insert(삽입)** 드롭다운 목록에서 **Into Category(도입 카테고리)**를 선택한 후 사용하려는 카테고리를 선택하십시오.

규칙을 저장하면 최종적으로 해당 카테고리에 위치합니다.

규칙을 생성하거나 수정하는 중에 숫자로 위치를 지정하려면 다음을 수행합니다.

단계 1 액세스 제어 규칙 편집기의 **Insert(삽입)** 드롭다운 목록에서 **above rule(규칙 위)** 또는 **below rule(규칙 아래)**을 선택한 후 적절한 규칙 번호를 입력합니다.

규칙을 저장하면 지정한 위치에 배치됩니다.

조건을 사용하여 규칙이 처리하는 트래픽 지정

라이센스: 기능에 따라 다름

액세스 제어 규칙의 조건은 규칙이 처리하는 트래픽의 유형을 식별합니다. 조건은 간단하거나 복잡할 수 있습니다. 사용자는 보안 영역, 네트워크 또는 지리적 위치, 포트,애플리케이션, 요청된 URL 및 사용자로 트래픽을 제어할 수 있습니다.

조건을 액세스 제어 규칙에 추가할 경우 다음 사항에 유의합니다.

- 규칙마다 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용할 수 있으려면 트래픽이 규칙의 **모든** 조건과 일치해야 합니다. 예를 들어, 특정 호스트(영역 또는 네트워크 상태)에 대해 URL 필터링(URL 조건)을 수행하는 단일 규칙을 사용할 수 있습니다.
- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. 조건의 기준 중 **어느** 것이든 모두 일치하는 트래픽은 조건을 만족합니다. 예를 들어, 최대 50명의 사용자와 그룹에 대한 사용자 제어를 수행하는 단일 규칙을 사용할 수 있습니다.

  최대 50개의 소스 및 최대 50개의 대상 기준을 사용하여 소스 및 대상으로 영역 및 네트워크 조건을 제한할 수 있다는 점에 유의하십시오. 영역 및 네트워크 조건에 소스와 대상 기준을 모두 추가한 경우 일치하는 트래픽은 지정된 소스 영역/네트워크 중 하나에서 발생해야 **하며** 대상 영역/네트워크 중 하나를 통해 전송되어야 합니다. 다시 말하면 시스템은 동일한 유형의 여러 조건 기준을 OR 연산자로 연결하고, 여러 조건 유형을 AND 연산자로 연결합니다. 예를 들어, 규칙 조건이 다음과 같은 경우:

```
Source Networks: 10.0.0.0/8, 192.168.0.0/16
Application Category: peer to peer
```

규칙은 사용자의 개인 IPv4 네트워크 중 하나의 호스트에서 P2P 애플리케이션 트래픽을 일치시킵니다. 패킷은 반드시 하나의 소스 네트워크 **또는** 다른 소스 네트워크에서 발생해야 **하며** P2P 애플리케이션 트래픽을 나타내야 합니다. 다음 연결은 둘 다 규칙을 트리거합니다.

```
10.42.0.105 to anywhere, using LimeWire
192.168.42.105 to anywhere, using Kazaa
```

규칙의 특정 조건을 구성하지 않은 경우, 시스템은 해당 기준에 따라 트래픽을 일치시키지 않습니다. 예를 들어, 네트워크 조건이 있지만 애플리케이션 조건이 없는 규칙은 세션에서 사용되는 애플리케이션에 관계 없이 해당 소스 또는 대상에 근거하여 트래픽을 평가합니다.

참고 액세스 제어 정책을 적용하면 시스템은 모든 규칙을 평가하며 확장된 기준 집합을 생성하여 ASA FirePOWER 모듈네트워크 트래픽을 평가하는 데 사용합니다. 복잡한 액세스 제어 정책 및 규칙은 중요한 리소스를 명령할 수 있습니다. 성능 향상을 위한 액세스 제어 규칙 간소화 방법 및 기타 방법에 대한 팁은 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

액세스 제어 규칙을 추가하거나 수정할 때 규칙 편집기 하단의 왼쪽에 있는 탭을 사용하여 규칙 조건을 추가 및 수정합니다. 다음 표에는 추가할 수 있는 조건 유형이 요약되어 있습니다.

표 6-1 액세스 제어 규칙 조건 유형

조건 유형...	트래픽 일치 대상...	세부 사항
영역	특정 보안 영역의 인터페이스를 통해 디바이스에 들어오거나 디바이스에서 나감	보안 영역은 배포 및 보안 정책에 따라 하나 이상의 인터페이스를 논리적으로 그룹화한 것입니다. 영역 조건을 구축하려면, 7-1페이지의 보안 영역을 통한 트래픽 제어를 참고하십시오.
네트워크	해당 소스 또는 대상 IP 주소, 국가 또는 대륙	IP 주소 또는 주소 블록을 명시적으로 지정할 수 있습니다. 위치 정보 기능을 사용하여 해당 소스 또는 대상 국가나 대륙에 근거하여 트래픽을 제어할 수도 있습니다. 네트워크 조건을 구축하려면, 7-3페이지의 네트워크 또는 지리적 위치별 트래픽 제어를 참고하십시오.
포트	해당 소스 또는 대상 포트	TCP와 UDP의 경우 전송 레이어 프로토콜에 따라 트래픽을 제어할 수 있습니다. ICMP 및 ICMPv6(IPv6-ICMP)의 경우 해당 인터넷 레이어 프로토콜과 선택적 유형 및 코드에 따라 트래픽을 제어할 수 있습니다. 포트 조건을 사용하면 포트를 사용하지 않는 다른 프로토콜을 사용하여 트래픽을 제어할 수도 있습니다. 포트 조건을 작성하려면 7-4페이지의 포트 및 ICMP 코드로 트래픽 제어를 참고하십시오.
애플리케이션	세션에서 탐지되는 애플리케이션별	개별 애플리케이션에 대한 액세스를 제어하거나 유형, 위험, 사업 타당성, 카테고리 및 태그 등 기본 특성에 따라 액세스를 필터링할 수 있습니다. 애플리케이션 조건을 구축하려면 8-2페이지의 애플리케이션 트래픽 제어를 참고하십시오.
URL	세션에서 요청된 URL별	네트워크의 사용자가 개별적으로 또는 URL의 일반 분류 및 위험 레벨을 기반으로 액세스할 수 있는 웹사이트를 제한할 수 있습니다. URL 조건을 구축하려면 8-7페이지의 URL 차단을 참고하십시오.
사용자	세션에 개입된 사용자별	모니터링된 세션에 개입된 호스트에 로그인한 LDAP 사용자를 기반으로 트래픽을 제어할 수 있습니다. Microsoft Active Directory 서버에서 검색된 개별 사용자 또는 그룹을 기준으로 트래픽을 제어할 수 있습니다. 사용자 조건을 구축하려면 9-1페이지의 사용자 기반 트래픽 제어를 참고하십시오.

어떤 라이센스로든 액세스 제어 규칙을 생성할 수 있지만, 특정 규칙 조건에서는 정책을 적용하려면 우선 특정 라이센스 기능을 활성화해야 합니다. 자세한 내용은 4-2페이지의 액세스 제어를 위한 라이센스 요건을 참고하십시오.

규칙 작업을 사용하여 트래픽 관리 및 검사 결정

라이센스: 모두

각 액세스 제어 규칙에는 일치하는 트래픽에 대해 다음을 결정하는 *작업*이 있습니다.

- 처리-시스템이 규칙의 조건과 일치하는 트래픽을 모니터링, 신뢰, 차단, 또는 허용하는 데 있어 그 여부를 제어하는 가장 중요한 규칙 작업
- 검사-적절하게 자격이 부여되었을 때, 일치하는 트래픽의 통과를 허용하기 전에 추가 검사를 허용하는 특정 규칙 작업
- 로깅-일치하는 트래픽에 관한 세부 사항을 로깅하는 시기와 방법을 결정하는 규칙 작업

액세스 제어 정책의 *기본 작업*은 모든 비 모니터링 액세스 제어 규칙의 조건을 충족하지 않는 트래픽을 처리합니다(4-4페이지의 네트워크 트래픽에 대한 기본 처리와 검사 설정 참고).

인라인으로 배포된 디바이스에서만 트래픽을 차단하거나 수정할 수 있다는 점에 유의하십시오. 수동 배포된 디바이스 분석하고 로깅할 수는 있지만 트래픽 흐름에 영향을 줄 수 없습니다. 규칙 작업 및 규칙 작업이 트래픽 처리, 검사 및 로깅에 미치는 영향에 대해 자세히 알아보려면 다음 섹션을 참고하십시오.

- 6-7페이지의 모니터링 작업: 작업 연기 및 로깅 보장
- 6-7페이지의 신뢰 작업: 검사 없이 트래픽 전달
- 6-8페이지의 작업 차단: 검사 없이 트래픽 차단
- 6-8페이지의 인터랙티브 차단 작업: 사용자가 웹 사이트 차단을 우회하도록 허용
- 6-9페이지의 허용 작업: 트래픽 허용 및 검사
- 10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어
- 25-9페이지의 액세스 제어 처리에 기반한 연결 로깅

모니터링 작업: 작업 연기 및 로깅 보장

라이센스: 모두

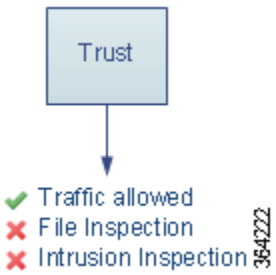
모니터링 작업은 트래픽 흐름에 영향을 주지 않습니다. 일치하는 트래픽은 즉시 허용되지도, 거부되지도 않습니다. 대신, 트래픽이 허용할지 아니면 거부할지 여부를 결정하기 위해 추가 규칙에 일치됩니다. 일치하는 첫 번째 비 모니터링 규칙은 트래픽 흐름과 추가 검사를 결정합니다. 추가로 일치하는 규칙이 없는 경우, 시스템은 기본 작업을 사용합니다.

모니터링 규칙의 주요 목적이 네트워크 트래픽을 추적하는 것이므로, 시스템은 모니터링된 트래픽에 대한 연결 이벤트의 종료를 자동으로 로깅합니다. 즉, 트래픽과 일치하는 다른 규칙이 없고 기본 작업에서 로깅을 활성화하지 않은 경우에도 연결이 로깅됩니다. 자세한 내용은 25-5페이지의 모니터링된 연결 로깅에 대한 이해를 참고하십시오.

신뢰 작업: 검사 없이 트래픽 전달

라이센스: 모두

Trust(신뢰) 작업은 어떤 종류든 추가 검사 없이 트래픽이 통과하도록 허용합니다.

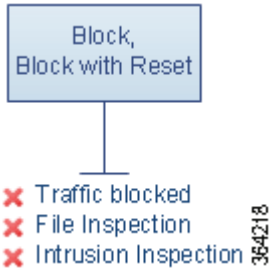


연결의 시작과 끝에서 모두 신뢰할 수 있는 네트워크 트래픽을 로깅할 수 있습니다. 자세한 내용은 25-5페이지의 신뢰할 수 있는 연결에 대한 로깅 이해를 참고하십시오.

작업 차단: 검사 없이 트래픽 차단

라이센스: 모두

Block(차단) 및 **Block with reset(차단 후 초기화)** 작업은 어떤 종류의 추가 검사도 없이 트래픽을 거부합니다. Block with reset(차단 후 초기화) 규칙은 연결을 재설정합니다.



HTTP 트래픽의 경우, 시스템이 웹 요청을 차단하면, 연결이 거부되었음을 설명하는 사용자 지정 페이지와 함께 서버 페이지 또는 기본 브라우저를 우회할 수 있습니다. 시스템은 이 사용자 지정 페이지를 *HTTP 응답 페이지*라고 명명합니다(8-14페이지의 차단된 URL을 위한 사용자 지정 웹페이지 표시 참고).

연결의 시작에서만 차단된 네트워크 트래픽을 로깅할 수 있습니다. 인라인으로 구축된 디바이스만이 트래픽을 차단할 수 있음을 참고하기 바랍니다. 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에, 시스템은 각 차단된 연결에 대한 여러 연결 시작 이벤트를 보고할 수 있습니다. 자세한 내용은 25-5페이지의 차단된 연결 및 인터랙티브 차단된 연결 로깅에 대한 이해를 참고하십시오.

주의 서비스 거부(DoS) 공격 중 차단된 TCP 연결을 로깅하는 경우 시스템 성능에 영향을 미칠 수 있으며 유사한 다수의 이벤트로 수 있습니다. Block(차단) 규칙에 대한 로깅을 활성화하기 전에, 해당 규칙이 인터넷에 연결된 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스의 트래픽을 모니터링하고 있는지 여부를 고려하시기 바랍니다.

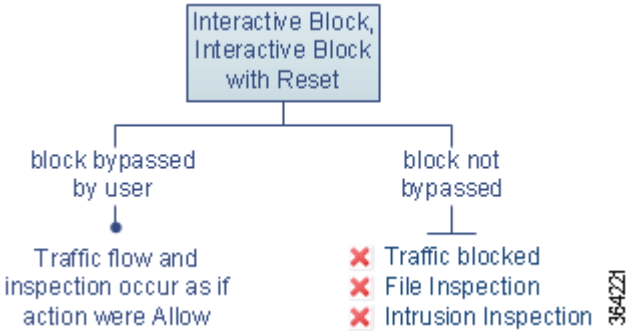
인터랙티브 차단 작업: 사용자가 웹 사이트 차단을 우회하도록 허용

라이센스: 모두

HTTP 트래픽의 경우, **Interactive Block(인터랙티브 차단)** 및 **Interactive Block with reset(인터랙티브 차단 후 초기화)** 작업은 사용자에게 *HTTP 응답 페이지*라는 사용자 지정 가능한 경고 페이지를 통해 클릭함으로써 웹 사이트 차단을 우회할 수 있는 기회를 제공합니다. Interactive Block with reset(인터랙티브 차단 후 초기화) 규칙은 연결을 재설정합니다.

인터랙티브 방식으로 차단된 모든 트래픽에서 시스템의 처리, 검사 및 로깅은 사용자가 차단을 우회하는지 여부에 따라 달라집니다.

- 사용자가 차단을 우회하지 않거나 우회할 수 없는 경우, 규칙은 Block(차단) 규칙을 모방합니다. 일치하는 트래픽이 추가 검사 없이 거부되며 사용자는 연결의 시작 부분만 로깅할 수 있습니다. 이 연결 시작 이벤트에는 `Interactive Block(인터랙티브 차단)` 또는 `Interactive Block with Reset(인터랙티브 차단 후 초기화)` 작업이 있습니다.
- 사용자가 차단을 우회하는 경우, 규칙은 Allow(허용) 규칙을 모방합니다. 따라서, Interactive Block(인터랙티브 차단) 규칙 중 한 유형을 파일 및 침입 정책과 연결하여 이 사용자 허용 트래픽을 검사할 수 있습니다. 시스템은 또한 연결 시작 이벤트와 종료 이벤트를 모두 로깅할 수 있습니다. 이 연결 이벤트에는 `Allow(허용)` 작업이 있습니다.



허용 작업: 트래픽 허용 및 검사

라이센스: 모두

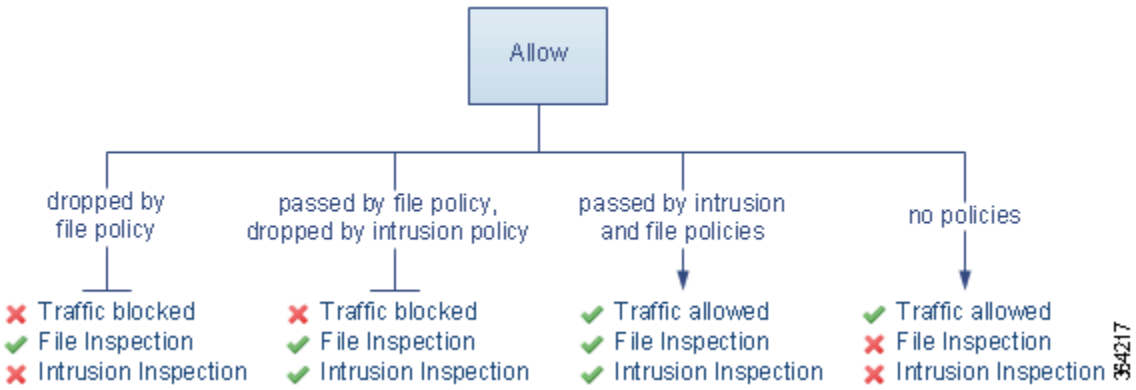
Allow(허용) 작업은 일치하는 트래픽이 통과하도록 허용합니다. 트래픽을 허용할 때, 결합된 침입 또는 파일 정책(또는 둘 다)을 사용하여 네트워크 트래픽을 자세히 검사하고 차단할 수 있습니다.

- 보호 라이센스가 있으면 침입 탐지 및 보호 구성에 따라 침입 정책을 사용하여 네트워크 트래픽을 분석할 수 있고 선택적으로 문제가 되는 패킷을 중단할 수 있습니다.
- 또한 보호라이센스가 있으면 파일 정책을 사용하여 파일 제어를 수행할 수 있습니다. 파일 제어를 수행하면, 사용자가 특정 애플리케이션 프로토콜에서 특정 유형의 파일을 업로드(전송) 또는 다운로드(수신)하는 행동을 탐지하고 차단할 수 있습니다.
- 악성코드 라이센스가 있으면 파일 정책을 사용하여 네트워크 기반 AMP(advanced malware protection)를 수행할 수 있습니다. 네트워크 기반 AMP는 파일에서 악성코드를 검색할 수 있으며, 선택적으로 탐지된 악성코드를 차단할 수 있습니다.

침입 또는 파일 정책을 액세스 제어 규칙과 연결하는 방법에 대한 자세한 내용은 10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어를 참고하십시오.

아래 다이어그램은 허용 규칙 또는 사용자가 우회한 인터랙티브 차단 규칙의 조건을 충족하는 트래픽에 실행되는 검사의 유형을 보여줍니다(6-8페이지의 인터랙티브 차단 작업: 사용자가 웹 사이트 차단을 우회하도록 허용 참고). 파일 검사는 침입 검사 전에 발생합니다. 차단된 파일에 대해서는 침입 관련 익스플로잇을 검사하지 않습니다.

간소화를 위해, 다이어그램은 액세스 제어 규칙과 침입 정책 및 파일 정책 둘 다 연관되어 있는 또는 둘 다 연관되어 있지 않은 상황을 위한 트래픽 흐름을 표시합니다. 그러나 하나가 없더라도 다른 하나를 구성할 수 있습니다. 파일 정책이 없으면 트래픽 흐름은 침입 정책에 의해 결정되고, 침입 정책이 없으면 트래픽 흐름은 파일 정책에 의해 결정됩니다.



연결의 시작 및 종료 모두에서 허용된 네트워크 트래픽을 로깅할 수 있습니다.

규칙에 코멘트 추가

라이센스: 모두

액세스 제어 규칙을 만들거나 수정할 때 코멘트를 추가할 수 있습니다. 예를 들어, 다른 사용자를 위해 전체 구성을 요약할 수 있습니다. 규칙을 변경할 때와 변경 이유를 로깅할 수 있습니다. 각 코멘트 및 코멘트가 추가된 각 날짜를 추가한 사용자와 마찬가지로 규칙을 위한 모든 코멘트의 목록을 표시할 수 있습니다.

규칙을 저장할 때, 마지막 저장 이후 만들어진 모든 코멘트는 읽기 전용이 됩니다.

규칙에 코멘트를 추가하려면 다음을 수행합니다.

단계 1 액세스 제어 규칙 편집기에서, **Comments(코멘트)** 탭을 선택합니다.

Comments(코멘트) 페이지가 나타납니다.

단계 2 **New Comment(새 코멘트)**를 클릭합니다.

New Comment(새 코멘트) 팝업 창이 열립니다.

단계 3 코멘트를 입력하고 **OK(확인)**를 클릭합니다.

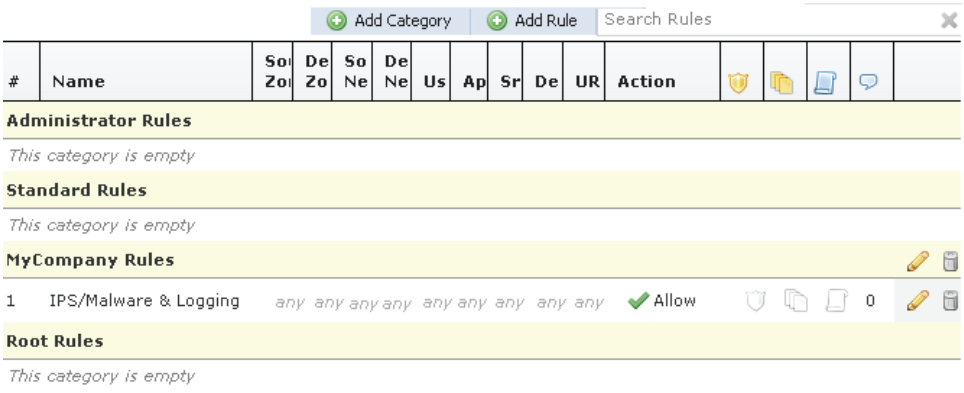
코멘트가 저장됩니다. 규칙을 저장할 때까지 이 코멘트를 수정하거나 삭제할 수 있습니다.

단계 4 규칙을 저장하거나 계속 수정합니다.

정책에서 액세스 제어 규칙 관리

라이센스: 모두

다음 그래픽에 보여지는 액세스 제어 정책 편집기의 Rules(규칙) 탭은 사용자가 추가, 수정, 검색, 이동, 활성화, 비활성화, 삭제할 수 있도록 하거나 사용자의 정책 내 액세스 제어 정책을 관리합니다.



각 규칙에서 정책 편집기는 해당 이름, 해당 조건에 대한 요약, 규칙 작업에 덧붙여 규칙의 검사 및 로깅 옵션을 전달하는 아이콘을 보여줍니다. 다른 아이콘은 다음 표에서 설명된 대로 코멘트, 경고, 오류 및 기타 중요한 정보를 나타냅니다. 비활성화된 규칙은 회색이며, 규칙 이름 아래에 (비활성화) 표시가 되어 있습니다.

표 6-2 액세스 제어 정책 편집기의 이해

아이콘	설명	방법
	침입 검사	규칙 검사 옵션을 수정하려면 활성화된(노란색) 검사 아이콘을 클릭하십시오(10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어 참고). 아이콘이 비활성화되면(흰색), 해당 규칙을 위해 그 유형의 어느 정책도 선택되지 않습니다.
	파일 및 악성코드 검사	
	로깅	규칙에 대한 로깅 옵션을 수정하려면 활성화된(파란색) 로깅 아이콘을 클릭하십시오(25-9페이지의 액세스 제어 처리에 기반한 연결 로깅 참고). 아이콘이 비활성화되면(흰색), 해당 규칙을 위한 연결 로깅은 비활성화됩니다.
	코멘트	규칙에 코멘트를 추가하려면 코멘트 열의 번호를 클릭하십시오(6-10페이지의 규칙에 코멘트 추가 참고). 번호는 규칙에 이미 포함된 코멘트의 수를 나타냅니다.
	경고	액세스 제어 정책 편집기에서 **Show Warnings(경고 보기)**를 클릭하여 해당 정책에 대한 모든 경고를 나열하는 팝업 창을 표시합니다(4-14페이지의 액세스 제어 정책과 규칙 문제 해결 참고).
	오류	
	정보	

액세스 제어 규칙 관리에 대한 자세한 내용은 다음을 참고하십시오.

- 6-2페이지의 액세스 제어 규칙 생성 및 수정
- 6-11페이지의 액세스 제어 규칙 검색
- 6-12페이지의 활성화 및 비활성화 규칙
- 6-12페이지의 규칙의 위치 또는 카테고리 변경

액세스 제어 규칙 검색

라이센스: 모두

스페이스 및 출력 가능한 특수 문자를 포함하는 영숫자 스트링을 사용하여 일치 값을 위해 액세스 제어 규칙의 목록을 검색할 수 있습니다. 검색은 규칙에 추가한 규칙 조건 및 규칙 이름을 검사합니다. 규칙 조건을 위해 검색은 각 조건 유형(영역, 네트워크, 애플리케이션, 등)에 추가할 수 있는 모든 이름 또는 값에 일치합니다. 여기에는 개별 개체 이름 또는 값, 그룹 개체 이름, 그룹 내 개별 개체 이름 또는 값, 그리고 문자 값이 포함됩니다.

완전한 또는 부분 검색 문자열을 사용할 수 있습니다. 일치 값을 위한 열은 각 일치하는 규칙에 강조 표시됩니다. 예를 들어, 스트링 `100Bao`의 전체 또는 일부를 최소한도로 검색하는 경우, 애플리케이션 열은 100Bao 애플리케이션을 추가한 각 규칙에 강조 표시됩니다. 또한 100Bao라는 이름의 규칙이 있는 경우, 이름 및 애플리케이션 열이 모두 강조 표시됩니다.

이전에 일치하는 규칙 또는 다음에 일치하는 규칙 각각으로 이동할 수 있습니다. 상태 메시지는 현재 일치하는 규칙과 일치하는 총 수를 나타냅니다.

일치는 여러 페이지가 있는 규칙 목록의 어느 페이지에서나 발생할 수 있습니다. 첫 번째 일치가 첫 번째 페이지에 없는 경우, 첫 번째 일치가 발생한 페이지가 표시됩니다. 마지막 일치 중일 때 다음 일치를 선택하면 첫 번째 일치로 이동하며, 첫 번째 일치 중일 때 이전 일치를 선택하면 마지막 일치로 이동합니다.

규칙을 검색하려면 다음을 수행합니다.

단계 1 검색을 원하는 정책에 대한 액세스 제어 정책 편집기에서, **Search Rules(검색 규칙)** 프롬프트를 클릭하고 문자열을 입력한 후 Enter(엔터) 키를 누릅니다. 또한 Tab(탭) 키를 사용하거나 빈 페이지 영역을 클릭하여 검색을 시작할 수 있습니다.

일치하는 값을 가진 규칙의 열이 강조 표시되며, 이는 명시된 (첫 번째) 일치를 위한 강조 표시와는 차별화됩니다.

단계 2 관심이 가는 규칙을 찾으십시오.

- 일치하는 규칙을 탐색하려면 다음 일치(▼) 또는 이전 일치(▲) 아이콘을 클릭합니다.
- 페이지를 새로 고침하고 검색 문자열 및 강조 표시를 지우려면, 지우기 아이콘(✖)을 클릭합니다.

활성화 및 비활성화 규칙

라이센스: 모두

액세스 제어 규칙을 만드는 경우, 이는 기본적으로 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다. 액세스 제어 정책에서 규칙 목록을 볼 때, 비활성화된 규칙은 계속 수정할 수 있지만 회색으로 표시됩니다. 또한 규칙 편집기를 사용하여 액세스 제어 규칙을 활성화 또는 비활성화할 수 있다는 점에 유의하십시오(6-2페이지의 액세스 제어 규칙 생성 및 수정 참고).

액세스 제어 규칙 상태를 변경하려면 다음을 수행합니다.

단계 1 활성화 또는 비활성화하려는 규칙이 포함된 정책에 대한 액세스 제어 정책 편집기에서 규칙을 마우스 오른쪽 단추로 클릭하여 규칙 상태를 선택합니다.

- 비활성 규칙을 활성화하려면, **State(상태) > Enable(활성화)**을 선택합니다.
- 활성 규칙을 비활성화하려면, **State(상태) > Disable(비활성화)**을 선택합니다.

단계 2 **Store FirePOWER Changes(FirePOWER 변경 사항 저장)** 를 클릭하여 정책을 저장합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

규칙의 위치 또는 카테고리 변경

라이센스: 모두

액세스 제어 규칙을 구성할 수 있도록 하려면, 각 액세스 제어 정책에 Administrator Rules(관리자 규칙), Standard Rules(표준 규칙) 및 Root Rules(루트 규칙) 3개의 시스템 제공 규칙 카테고리가 있어야 합니다. 사용자 지정 카테고리를 만들 수는 있지만 카테고리를 이동하거나, 삭제하거나, 이름을 변경할 수는 없습니다.

자세한 내용은 다음을 참고하십시오.

- 6-13페이지의 규칙 이동
- 6-13페이지의 새 규칙 카테고리 추가

규칙 이동

라이센스: 모두

적절한 액세스 제어 규칙 순서는 네트워크 트래픽을 처리하는 데 필요한 리소스를 줄이고 규칙의 사전 대응을 방지합니다.

다음 절차는 액세스 제어 정책 편집기를 사용하여 하나 이상의 규칙을 이동하는 방법을 설명합니다. 또한 규칙 편집기를 사용하여 개별 액세스 제어 규칙을 이동할 수 있습니다(6-2페이지의 액세스 제어 규칙 생성 및 수정 참고).

규칙을 이동하려면 다음을 수행합니다.

단계 1 이동하려는 규칙이 포함된 정책에 대한 액세스 제어 정책 편집기에서, 각 규칙의 빈 영역을 클릭하여 규칙을 선택합니다. Ctrl 및 Shift 키를 사용하여 여러 규칙을 선택합니다.

선택한 규칙은 강조 표시됩니다.

단계 2 규칙을 이동합니다. 잘라서 붙이거나 끌어다 놓을 수 있습니다.

새 위치로 규칙을 잘라내고 붙여넣으려면, 선택한 규칙을 마우스 오른쪽 단추로 클릭하고 **Cut(자르기)**를 선택합니다. 다음으로, 규칙을 잘라서 붙이기를 원하는 곳의 옆에 있는 규칙의 빈 영역을 마우스 오른쪽 단추로 클릭하고 **Paste above(위 붙여넣기)** 또는 **Paste below(아래 붙여넣기)**를 선택합니다. 두 가지 다른 액세스 제어 정책 간의 액세스 제어 규칙은 복사하여 붙여 넣을 수 없다는 점에 주의하십시오.

단계 3 **Store FirePOWER Changes(FirePOWER 변경 사항 저장)**를 클릭하여 정책을 저장합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

새 규칙 카테고리 추가

라이센스: 모두

액세스 제어 규칙을 구성할 수 있도록 하려면, 각 액세스 제어 정책에 Administrator Rules(관리자 규칙), Standard Rules(표준 규칙) 및 Root Rules(루트 규칙) 3개의 시스템 제공 규칙 카테고리가 있어야 합니다. 표준 규칙 및 루트 규칙 사이에 사용자 지정 카테고리를 만들 수는 있지만 카테고리를 이동하거나, 삭제하거나, 이름을 변경할 수는 없습니다.

사용자 지정 카테고리를 추가하면 추가 정책을 생성할 필요없이 규칙을 추가로 구성할 수 있습니다. 추가한 카테고리의 이름을 변경하고 삭제할 수 있습니다. 이 카테고리를 이동할 수는 없지만 이 카테고리 안으로, 이 카테고리 안에서, 이 카테고리 밖으로 규칙을 이동할 수는 있습니다.

새 카테고리를 추가하려면 다음을 수행합니다.

단계 1 규칙 카테고리를 추가하려는 정책에 대한 액세스 제어 정책 편집기에서 Add Category(카테고리 추가)를 클릭합니다.

팁 정책에 이미 규칙이 포함된 경우, 새로운 규칙을 추가하기 전에 기존 규칙에 대한 행의 빈 영역을 클릭하여 새로운 카테고리의 위치를 지정합니다. 기존 규칙을 마우스 오른쪽 단추로 클릭하고 **Insert new category(새 카테고리 삽입)**를 선택합니다.

Add Category(카테고리 추가) 팝업 창이 열립니다.

단계 2 고유한 카테고리 **Name(이름)**을 입력합니다.

스페이스 및 출력 가능한 특수 문자를 포함하는 영숫자 이름을 최대 30자로 입력할 수 있습니다.

단계 3 다음 옵션을 이용할 수 있습니다.

- 기존 카테고리 바로 위에 새 카테고리를 위치시키려면, 첫 번째 **Insert(삽입)** 드롭다운 목록에서 **above Category(상위 카테고리)**를 선택한 후, 두 번째 드롭다운 목록에서 규칙을 위치시키고자 하는 상위 카테고리를 선택합니다.
- 기존 규칙 아래에 새 카테고리 규칙을 위치시키려면, 드롭다운 목록에서 **below rule(하위 규칙)**을 선택한 후 기존의 규칙 번호를 입력합니다. 이 옵션은 최소 하나의 규칙이 정책에 존재할 경우에만 유효합니다.
- 기존 규칙 위에 새 카테고리 규칙을 위치시키려면, 드롭다운 목록에서 **above rule(상위 규칙)**을 선택한 후 기존의 규칙 번호를 입력합니다. 이 옵션은 최소 하나의 규칙이 정책에 존재할 경우에만 유효합니다.

단계 4 **OK(확인)**를 클릭합니다.

카테고리가 추가됩니다. 사용자 지정 카테고리 옆의 수정 아이콘( )을 클릭하여 이름을 수정하거나, 삭제 아이콘( )을 클릭하여 카테고리를 삭제할 수 있습니다. 삭제한 카테고리의 규칙은 상위 카테고리에 추가됩니다.

단계 5 **Store FirePOWER Changes(FirePOWER 변경 사항 저장)** 를 클릭하여 정책을 저장합니다.

네트워크 기반 규칙으로 트래픽 제어

액세스 제어 정책 내에서 *액세스 제어 규칙*은 네트워크 트래픽 로깅 및 처리에 세분화된 제어를 제공합니다. 네트워크 기반 조건을 통해 다음 중 하나 이상의 기준을 사용하여 트래픽이 네트워크를 통과하도록 관리할 수 있습니다.

- 소스 및 대상 보안 영역
- 소스 및 수신 IP 주소 또는 지리적 위치
- 소스 및 목적지 포트 - 전송 레이어 프로토콜 및 ICMP 코드 옵션도 포함

네트워크 기반의 조건을 서로 결합하거나 다른 유형의 조건과 결합하여 액세스 제어 규칙을 만들 수 있습니다. 이러한 액세스 제어 규칙은 간단하거나 복잡할 수 있으며, 다양한 조건을 사용하여 트래픽에 일치시키거나 트래픽을 검사합니다. 액세스 제어 규칙에 대한 자세한 내용은 6-1페이지의 액세스 제어 규칙을 사용한 트래픽 흐름 조정을 참고하십시오.

참고 보안 인텔리전스 기반의 트래픽 필터링, 그리고 일부 디코딩 및 전처리 과정은 네트워크 트래픽이 액세스 제어 규칙으로 평가되기 **전에** 이루어집니다.

표 7-1 네트워크 기반 액세스 제어 규칙의 라이센스 요건

요건	지오로케이션 제어	다른 모든 네트워크 기반 제어
라이센스	모두	모두

네트워크 기반 액세스 제어 규칙의 구축에 대한 자세한 정보는 다음을 참고하십시오.

- 7-1페이지의 보안 영역을 통한 트래픽 제어
- 7-3페이지의 네트워크 또는 지리적 위치별 트래픽 제어
- 7-4페이지의 포트 및 ICMP 코드로 트래픽 제어

보안 영역을 통한 트래픽 제어

라이센스: 모두

액세스 제어 규칙의 영역 조건을 통해 소스 및 대상 보안 영역으로 트래픽을 제어할 수 있습니다. *보안 영역*은 하나 이상의 인터페이스를 그룹화하는 것입니다. .

간단한 예로,내부와 외부, 두 영역을 만들 수 있습니다. 이는 해당 영역에 디바이스 상 인터페이스의 첫 번째 쌍을 할당합니다. 내부에서 네트워크에 연결된 호스트는 보호된 자산을 나타냅니다.

이 시나리오를 확장하려면, 동일하게 구성된 디바이스를 추가로 배치하여 여러 다른 장소에서 유사한 리소스를 보호할 수 있습니다. 각 디바이스는 내부 보안 영역의 자산을 보호합니다.

팁 모든 내부 (또는 외부) 인터페이스를 단일 영역으로 그룹화할 필요는 없습니다. 구축 및 보안 정책에 알맞은 그룹화를 선택합니다. 영역 생성에 대한 자세한 내용은 2-33페이지의 보안 영역 작업을 참고하십시오.

이 구축에서는 호스트에 인터넷에 대한 무제한 액세스를 허용하더라도 수신 트래픽에서 침입 및 악성코드 검사를 수행하여 보호하도록 결정할 수 있습니다.

액세스 제어를 통해 이를 실현하려면 영역 조건이 있는 액세스 제어 규칙을 구성합니다. 여기서 **Destination Zone(대상 영역)**은 **Internal(내부)**로 설정됩니다. 이 단순한 액세스 제어 규칙은 내부 영역 내 모든 인터페이스로부터 디바이스를 나가는 트래픽에 일치됩니다.

일치하는 트래픽에 대해 침입 및 악성코드 검사를 수행하려면 **Allow(허용)** 규칙 작업을 선택한 다음 이 규칙을 침입 및 파일 정책과 연결합니다. 자세한 내용은 6-6페이지의 규칙 작업을 사용하여 트래픽 관리 및 검사 결정 및 10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어를 참고하십시오.

좀 더 복합적인 규칙을 만들려는 경우 단일 영역 조건에서 각 **Source Zones(소스 영역)** 및 **Destination Zones(대상 영역)**에 최대 50개의 영역을 추가할 수 있습니다:

- 영역 내 인터페이스의 디바이스에서 *나가는* 트래픽에 일치시키기 위해서는 **Destination Zones(대상 영역)**에 해당 영역을 추가합니다.

  패시브 구축된 디바이스는 트래픽을 전송하지 않으므로, **Destination Zone(대상 영역)** 조건에서 패시브 인터페이스로 구성된 영역을 사용할 수 없습니다.
- 영역 내 인터페이스를 통해 디바이스로 *들어오는* 트래픽에 일치시키기 위해서는 **Source Zones(소스 영역)**에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가하는 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 시작해야 하고 **또한** 대상 영역 중 하나를 통해 나가야 합니다.

영역 조건을 구축할 때, 경고 아이콘은 잘못된 구성을 나타냅니다. 자세한 내용을 보려면

영역별 트래픽을 제어하려면 다음을 수행합니다.

단계 1 영역별로 트래픽을 제어할 액세스 제어 정책에서 새로운 액세스 제어 규칙을 만들거나 기존 규칙을 수정합니다.

자세한 내용은 6-2페이지의 액세스 제어 규칙 생성 및 수정을 참고하십시오.

단계 2 규칙 편집기에서, Zones(영역) 탭을 선택합니다.

Zones(영역) 탭이 나타납니다.

단계 3 **Available Zones(사용 가능한 영역)**에서 추가하려는 영역을 찾아 선택합니다.

영역을 찾아 추가하려면, **Available Zones(사용 가능한 영역)** 목록 위에 있는 **Search by name(이름으로 검색)** 프롬프트를 클릭한 후, 영역 이름을 입력합니다. 일치하는 영역을 입력하여 표시하면 목록이 업데이트됩니다.

영역을 선택하려면 클릭하십시오. 여러 영역을 선택하려면, Shift와 Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 후 **Select All(모두 선택)**을 선택합니다.

단계 4 **Add to Source(소스에 추가)** 또는 **Add to Destination(대상에 추가)**을 클릭하여 적절한 목록에 선택한 영역을 추가합니다.

사용자는 또한 선택한 영역을 끌어 놓을 수 있습니다.

단계 5 규칙을 저장하거나 계속 수정합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

네트워크 또는 지리적 위치별 트래픽 제어

라이센스: 기능에 따라 다름

액세스 제어 규칙의 네트워크 조건을 통해 소스 및 수신 IP 주소로 트래픽을 제어할 수 있습니다. 다음 중 하나를 수행할 수 있습니다.

- 제어를 원하는 트래픽에 대해 소스 및 수신 IP 주소를 명시적으로 지정
- 지리적 위치와 IP 주소를 결합하는 지오로케이션 기능을 사용하여 해당 소스 또는 대상 국가/대륙을 기반으로 트래픽 제어

네트워크 기반 액세스 제어 규칙 조건을 구축할 때, IP 주소 및 지리적 위치를 수동으로 지정할 수 있습니다. 또는, 네트워크 및 지오로케이션 *객체*를 사용하여 네트워크 조건을 구성할 수 있습니다. 이 객체는 재사용가능하며 이름을 하나 이상의 IP 주소, 주소 블록, 국가, 대륙 등과 연결합니다.

팁 네트워크 또는 지오로케이션 객체를 만든 후에는 액세스 제어 규칙을 작성하는 데 뿐만 아니라 시스템의 모듈 인터페이스 내 다양한 장소에서 IP 주소를 나타나는 데에도 사용할 수 있습니다. 객체 관리자를 사용하여 이 객체를 생성할 수 있습니다. 액세스 제어 규칙을 구성하는 동안 즉석에서 네트워크 객체를 만들 수도 있습니다. 자세한 내용은 2-1페이지의 재사용 가능한 개체 관리를 참고하십시오.

지리적 위치로 트래픽을 제어하는 규칙을 작성하려는 경우 최신 지오로케이션 데이터를 사용하여 트래픽을 필터링할 수 있도록 Cisco는 **강력히** ASA FirePOWER 모듈의 지오로케이션 데이터베이스(GeoDB)를 정기적으로 업데이트할 것을 권장합니다(35-20페이지의 위치 정보 데이터베이스 업데이트 참고).

표 7-2 네트워크 조건의 라이센스 요건

요건	지오로케이션 제어	IP 주소 제어
라이센스	모두	모두

단일 네트워크 조건에서 각 **Source Networks(소스 네트워크)** 및 **Destination Networks(대상 네트워크)**에 최대 50개의 항목을 추가할 수 있으며, 네트워크 구성 및 지오로케이션 기반 구성을 결합할 수 있습니다.

- IP 주소*로부터 나오는* 트래픽 또는 지리적 위치를 일치시키려면 **Source Networks(소스 네트워크)**를 구성합니다.
- IP 주소 또는 지리적 위치*로 향하는* 트래픽을 일치시키려면 **Destination Networks(대상 네트워크)**를 구성합니다.

규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 시작하고 **또한** 그 목적지가 수신 IP 주소 중 하나여야 합니다.

네트워크 조건을 구축할 때, 경고 아이콘은 잘못된 구성을 나타냅니다. 자세한 내용을 보려면 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

네트워크 또는 지리적 위치별로 트래픽을 제어하려면 다음을 수행합니다.

단계 1 네트워크별로 트래픽을 제어할 액세스 제어 정책에서 새로운 액세스 제어 규칙을 만들거나 기존 규칙을 수정합니다.

자세한 내용은 6-2페이지의 액세스 제어 규칙 생성 및 수정을 참고하십시오.

단계 2 규칙 편집기에서, Networks(네트워크) 탭을 선택합니다.

Networks(네트워크) 탭이 나타납니다.

단계 3 다음과 같이, **Available Networks(사용 가능한 네트워크)**로부터 추가하려는 네트워크를 찾아 선택합니다.

- Networks(네트워크) 탭을 클릭하여 추가할 네트워크 객체 및 그룹을 표시합니다. 위치 정보 개체를 표시하려면 Geolocation(지오로케이션) 탭을 클릭합니다.
- 네트워크 객체를 즉시 추가한 다음 조건에 추가하려면, **Available Networks(사용가능한 네트워크)** 목록 위의 추가 아이콘( )을 클릭합니다(2-3페이지의 네트워크 개체 작업 참고).
- 추가할 네트워크 또는 지오로케이션 객체를 검색하려면, 알맞은 탭을 선택하여 **Available Networks(사용 가능한 네트워크)** 목록 위에 있는 **Search by name or value(이름 또는 값으로 검색)** 프롬프트를 클릭한 후 개체 이름이나 개체의 구성 요소 중 하나의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 일치하는 객체를 표시합니다.

개체를 선택하려면 이를 클릭합니다. 여러 객체를 선택하려면, Shift와 Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 후 **Select All(모두 선택)**을 선택합니다.

단계 4 **Add to Source(소스에 추가)** 또는 **Add to Destination(대상에 추가)**을 클릭하여 적절한 목록에 선택한 개체를 추가합니다.

선택한 영역을 끌어서 놓을 수도 있습니다.

단계 5 수동으로 지정하려는 주소 블록, 대상 IP 주소 또는 모든 소스를 추가합니다.

Source Networks(소스 네트워크) 또는 **Destination Networks(대상 네트워크)** 목록 아래에 있는 **Enter an IP address(IP 주소 입력)** 프롬프트를 클릭한 후 IP 주소 또는 주소 블록을 입력하고 **Add(추가)**를 클릭합니다.

단계 6 규칙을 저장하거나 계속 수정합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

포트 및 ICMP 코드로 트래픽 제어

라이센스: 모두

액세스 제어 규칙의 네트워크 조건을 통해 소스 및 대상 포트로 트래픽을 제어할 수 있습니다. 이 컨텍스트에서 "포트"란 다음 중 하나를 말합니다.

- TCP와 UDP의 경우 전송 레이어 프로토콜에 따라 트래픽을 제어할 수 있습니다. 시스템은 괄호 내 프로토콜 번호와 선택적으로 결합된 포트 또는 포트 범위를 사용하여 이 구성을 나타냅니다. 예: TCP(6)/22
- ICMP 및 ICMPv6(IPv6-ICMP)의 경우 해당 인터넷 레이어 프로토콜과 선택적 유형 및 코드에 따라 트래픽을 제어할 수 있습니다. 예: ICMP(1):3:3
- 포트를 사용하지 않는 다른 프로토콜을 사용하여 트래픽을 제어할 수 있습니다.

포트 기반 액세스 제어 규칙 조건을 구축할 때, 수동으로 포트를 지정할 수 있습니다. 대안으로, 재사용이 가능하며 하나 이상의 포트와 이름을 연결하는 포트 *개체*로 포트 조건을 구성할 수 있습니다.

팁 포트 개체를 만든 후에는 액세스 제어 규칙을 작성하는 데 뿐만 아니라 시스템의 모듈 인터페이스 내 다양한 장소에서 포트를 나타나는 데에도 사용할 수 있습니다. 개체 관리자를 사용하거나 액세스 제어 규칙을 구성하는 동안 상황에 따라 포트 개체를 만들 수 있습니다. 자세한 내용은 2-10페이지의 포트 개체 작업을 참고하십시오.

단일 네트워크 조건에서 각 **Selected Source Ports(선택된 소스 포트)** 및 **Selected Destination Ports(선택된 대상 포트)** 목록에 최대 50개의 항목을 추가할 수 있습니다.

- 포트*로부터 나오는* 트래픽을 일치시키려면 **Selected Source Ports(선택된 소스 포트)**를 구성합니다.

  조건에 소스 포트만 추가할 경우, 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. 예를 들어, DNS over TCP 및 DNS over UDP 모두를 단일 액세스 제어 규칙의 소스 포트 조건으로 추가할 수 있습니다.

- 포트*로 향하는* 트래픽을 일치시키려면 **Selected Destination Ports(선택된 대상 포트)**를 구성합니다.

  조건에 대상 포트만 추가할 경우, 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다.

- 특정 **Selected Source Ports(선택된 소스 포트)**에서 발생한 트래픽 *및* 특정 **Selected Destination Ports(선택된 대상 포트)**로 향하는 트래픽을 일치시키기 위해서는 둘 다 구성합니다.

  조건에 소스 및 대상 포트를 모두 추가한 경우, 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다 . 예를 들어, 소스 포트로 DNS over TCP를 추가한 경우, 대상 포트에 Yahoo 메신저 음성 채팅(TCP)을 추가할 수 있지만 Yahoo 메신저 음성 채팅(UDP)은 해당되지 않습니다.

포트 상태를 구축할 때는 다음 사항에 유의하십시오.

- 0으로 설정된 유형의 대상 ICMP 포트 또는 129로 설정된 유형의 대상 ICMPv6 포트를 추가하면, 액세스 제어 규칙은 요청하지 않은 에코 응답에만 일치됩니다. ICMP 에코 요청에 대한 응답으로 전송된 ICMP 에코 응답은 무시됩니다. 모든 ICMP 에코에 일치하는 규칙의 경우, ICMP 유형 8 또는 ICMPv6 유형 128을 사용합니다.
- 대상 포트 조건으로 GRE(47) 프로토콜을 사용할 경우, 액세스 제어 규칙에 다른 네트워크 기반 조건(즉, 영역 및 네트워크 조건)만 추가할 수 있습니다. 평판 또는 사용자 기반 조건을 추가하는 경우 규칙을 저장할 수 없습니다.

포트 조건을 구축할 때, 경고 아이콘은 유효하지 않은 구성을 나타냅니다. 예를 들어 해당 객체 그룹을 사용하는 규칙이 무효화될 수 있도록, 개체 관리자를 사용하여 사용 중인 포트 개체를 수정할 수 있습니다. 자세한 내용을 보려면 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

포트별 트래픽을 제어하려면 다음을 수행합니다.

단계 1 포트별 트래픽 제어를 원하는 액세스 제어 정책에서 새로운 액세스 제어 규칙을 만들거나 기존 규칙을 수정합니다.

자세한 내용은 6-2페이지의 액세스 제어 규칙 생성 및 수정을 참고하십시오.

단계 2 규칙 편집기에서, Ports(포트) 탭을 선택합니다.

Ports(포트) 탭이 나타납니다.

단계 3 다음과 같이, **Available Ports(사용 가능한 포트)**로부터 추가하려는 포트를 찾아 선택합니다.

- 상황에 따라 포트 개체를 추가하여 조건에 추가하려면, Available Ports(사용 가능한 포트) 목록 위에 있는 추가 아이콘( )을 클릭합니다(2-10페이지의 포트 개체 작업 참고).

- 추가할 포트 개체 및 그룹을 검색하려면, **Available Ports(사용 가능한 포트)** 목록 위에 있는 **Search by name or value(이름 또는 값으로 검색)** 프롬프트를 클릭한 후 개체 이름 또는 개체의 포트 값을 입력합니다. 일치하는 개체를 입력하여 표시하면 목록이 업데이트됩니다. 예를 들어, 80을 입력하면, ASA FirePOWER 모듈은 Cisco가 제공한 HTTP 포트 개체를 표시합니다.

  개체를 선택하려면 이를 클릭합니다. 여러 개체를 선택하려면, Shift와 Ctrl 키를 사용하거나, 마우스 오른쪽 단추를 클릭한 후 **Select All(모두 선택)**을 선택합니다.

단계 4 **Add to Source(소스에 추가)** 또는 **Add to Destination(대상에 추가)**을 클릭하여 적절한 목록에 선택한 개체를 추가합니다.

선택한 영역을 끌어서 놓을 수도 있습니다.

단계 5 수동으로 지정하려는 대상 포트 또는 모든 소스를 추가합니다.

- 소스 포트의 경우 **Selected Source Ports(선택된 소스 포트)** 목록 아래의 **Protocol(프로토콜)** 드롭다운 목록에서 **TCP** 또는 **UDP**를 선택합니다. 그런 다음, **Port(포트)**를 입력합니다. 0-65535 값으로 단일 포트를 지정할 수 있습니다.
- 대상 포트의 경우, **Selected Source Ports(선택된 소스 포트)** 목록 아래의 **Protocol(프로토콜)** 드롭다운 목록에서 프로토콜을 선택합니다(모든 프로토콜의 경우 **All(모든)** 선택). 목록에 나타나지 않는 할당되지 않은 프로토콜 또한 입력할 수 있습니다.

  ICMP 또는 **IPv6-ICMP**를 선택한 경우 유형 및 관련 코드를 선택할 수 있는 팝업 창이 나타납니다. ICMP 유형과 코드에 관한 자세한 정보는 http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml 및 http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml을 참고하십시오.

  프로토콜을 지정하지 않으려는 경우 또는 선택적으로 TCP 또는 UDP를 지정한 경우, **Port(포트)**를 입력합니다. 0-65535 값으로 단일 포트를 지정할 수 있습니다.

ADD(추가)를 클릭합니다. ASA FirePOWER 모듈은 유효하지 않은 구성으로 귀결되는 규칙 조건에는 포트를 추가하지 않습니다.

단계 6 규칙을 저장하거나 계속 수정합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

8 장

평판 기반 규칙으로 트래픽 제어

액세스 제어 정책 내 *액세스 제어 규칙*은 네트워크 트래픽 로깅 및 처리를 세부적으로 제어합니다. 액세스 제어 규칙의 평판 기반 조건을 통해 사용자는 네트워크 트래픽의 컨텍스트를 파악하고 적절한 경우 이를 제한하여 네트워크를 통과시킬 트래픽을 관리할 수 있습니다. 액세스 제어 규칙은 다음 유형의 평판 기반 제어를 관장합니다.

- 애플리케이션 조건을 통해 사용자는 *애플리케이션 제어*를 수행할 수 있습니다. 이는 개별 애플리케이션뿐 아니라 유형, 위험, 사업 타당성, 카테고리 및 태그 등 애플리케이션의 기본 특성을 기반으로 애플리케이션 트래픽을 제어합니다.
- URL 조건에서는 *URL 필터링*을 수행할 수 있습니다. 즉 개별 웹 사이트뿐 아니라 웹 사이트의 시스템 할당 카테고리 및 평판을 기반으로 웹 트래픽을 제어합니다.

평판 기반 조건끼리 또는 다른 조건 유형과 조합하여 액세스 제어 규칙을 생성할 수 있습니다. 이러한 액세스 제어 규칙은 간단하거나 복잡할 수 있으며, 다양한 조건을 사용하여 트래픽에 일치시키거나 트래픽을 검사합니다. 액세스 제어 규칙에 대한 자세한 내용은 6-1페이지의 액세스 제어 규칙을 사용한 트래픽 흐름 조정을 참고하십시오.

보안 인텔리전스 기반의 트래픽 필터링, 그리고 일부 디코딩 및 전처리는 네트워크 트래픽이 액세스 제어 규칙으로 평가되기 **전에** 이루어집니다. 평판 기반 액세스 제어를 이용하려면 다음 라이센스 가 필요합니다.

표 8-1 평판 기반 액세스 제어 규칙의 라이센스 요건

요건	애플리케이션 제어	URL 필터링(카테고리 및 평판)	URL 필터링(수동)
라이센스	제어	URL 필터링	모두

액세스 제어 규칙에 평판 기반 조건을 추가하는 것에 대한 자세한 내용은 다음을 참고하십시오.

- 8-2페이지의 애플리케이션 트래픽 제어
- 8-7페이지의 URL 차단

ASA FirePOWER 모듈에서는 다른 유형의 평판 기반 제어를 수행할 수 있지만, 이러한 제어는 액세스 제어 규칙으로 구성하지 않습니다. 자세한 내용은 다음을 참고하십시오.

- 5-1페이지의 보안 인텔리전스 IP 주소 평판을 사용한 차단 목록 추가는 1차 방어선으로 연결의 기점과 종점의 평판을 기준으로 트래픽을 제한하는 방법을 설명합니다.
- 10-6페이지의 침입 방지 성능 조정에서는 악성코드 및 기타 금지된 파일 유형을 탐지, 추적, 저장, 분석하고 차단하는 방법에 대해 설명합니다.

애플리케이션 트래픽 제어

라이센스: 제어

ASA FirePOWER 모듈에서 IP 트래픽을 분석할 때, 사용자의 네트워크에서 자주 사용되는 애플리케이션을 식별하여 분류할 수 있습니다.

애플리케이션 제어의 이해

액세스 제어 규칙의 애플리케이션 조건을 통해 이러한 *애플리케이션 제어*를 수행할 수 있습니다. 단일 액세스 제어 규칙 내에서 트래픽을 제어할 애플리케이션을 몇 가지 방법으로 지정할 수 있습니다.

- 사용자 지정 애플리케이션을 포함하여 개별 애플리케이션을 선택할 수 있습니다.
- 시스템에서 제공한 *애플리케이션 필터*를 사용할 수 있습니다. 이는 이름이 지정된 애플리케이션 집합으로 애플리케이션의 기본 특성, 즉 유형, 위험, 사업 타당성, 카테고리, 태그에 따라 구성됩니다.
- 사용자 지정 애플리케이션 필터를 생성하고 사용할 수 있으며, 이는 선택하는 모든 방식을 통해 애플리케이션(사용자 지정 애플리케이션 포함)을 그룹화합니다.

애플리케이션 필터를 사용하여 액세스 제어 규칙에 대한 애플리케이션 조건을 신속하게 생성할 수 있습니다. 이러한 필터는 정책 생성 및 관리를 간소화하며, 시스템에서 웹 트래픽을 예상대로 제어한다는 확신을 가질 수 있습니다. 예를 들어, 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

이와 더불어 Cisco에서는 VDB(System and Vulnerability Database: 취약점 데이터베이스)를 통해 추가 탐지기를 자주 업데이트하고 추가합니다. 애플리케이션 특징을 기준으로 한 필터를 사용하면 시스템에서는 최신 탐지기를 사용하여 애플리케이션 트래픽을 모니터링할 수 있습니다.

애플리케이션 조건 작성

트래픽이 애플리케이션 조건이 있는 액세스 제어 규칙과 일치하려면 **Selected Applications and Filters(선택한 애플리케이션 및 필터)** 목록에 추가된 필터 또는 애플리케이션 중 하나와 일치해야 합니다.

단일 애플리케이션 조건의 경우, **Selected Applications and Filters(선택한 애플리케이션 및 필터)** 목록에 최대 50개의 항목을 추가할 수 있습니다. 다음 각각의 경우는 하나의 항목으로 간주됩니다.

- 개별적으로 조합하거나 맞춤형으로 조합한 **Application Filters(애플리케이션 필터)** 목록의 하나 이상의 필터. 이 항목은 특성을 기준으로 그룹화된 애플리케이션 집합을 나타냅니다.
- **Available Applications(사용가능한 애플리케이션)** 목록에 애플리케이션 검색을 저장하여 생성하는 필터. 이 항목은 부분 문자열 일치를 기준으로 그룹화된 애플리케이션 집합을 나타냅니다.
- **Available Applications(사용 가능한 애플리케이션)** 목록의 개별 애플리케이션.

모듈 인터페이스의 경우, 조건에 추가된 필터는 위에 나열되며, 개별적으로 추가된 애플리케이션과는 따로 구분됩니다.

액세스 제어 정책을 적용하는 경우 시스템은 애플리케이션 조건이 있는 각 규칙에 대해 일치하는 고유한 애플리케이션 목록을 생성합니다. 즉, 겹치는 필터 및 개별적으로 지정된 애플리케이션을 사용하여 전체 범위를 포괄할 수 있습니다.

참고 암호화된 트래픽의 경우, 시스템은 **SSL Protocol(SSL 프로토콜)** 태그가 지정된 애플리케이션만 사용하여 트래픽을 식별하고 필터링할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽에서만 탐지될 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

애플리케이션 필터를 통한 트래픽 일치

라이센스: 제어

액세스 제어 규칙에서 애플리케이션 조건을 작성할 경우, **Application Filters(애플리케이션 필터)** 목록을 사용하여 특성에 따라 그룹화된 애플리케이션(트래픽을 매칭할 애플리케이션) 집합을 생성합니다.

액세스 제어 규칙 내에서 애플리케이션을 필터링하는 메커니즘은 객체 관리자를 사용하여 재사용 가능한 사용자 지정 애플리케이션 필터를 생성하는 메커니즘과 동일합니다(2-12페이지의 애플리케이션 필터 작업 참고). 액세스 제어 규칙에서 즉시 생성하는 많은 필터를 새로운 재사용 가능한 필터로 저장할 수도 있습니다. 사용자 생성 필터는 중첩될 수 없으므로 다른 사용자 생성 필터를 포함하는 필터를 저장할 수 없습니다.

필터를 조합하는 방법 이해

필터를 단독으로 또는 조합하여 선택할 경우, 해당 기준에 맞는 애플리케이션만 표시하도록 **Available Applications(사용가능한 애플리케이션)** 목록이 업데이트됩니다. 시스템에서 제공된 필터를 조합하여 선택할 수 있으나, 사용자 지정 필터는 그렇지 않습니다.

동일한 필터 유형의 여러 필터는 OR 연산자로 연결됩니다. 예를 들어, Risks(위험도) 유형에서 Medium(중간) 및 High(높음) 필터를 선택할 경우, 결과 필터는 다음과 같습니다.

Risk(위험도): Medium OR High(중간 또는 높음)

Medium(중간) 필터가 110개의 애플리케이션을 포함하고 High(높음) 필터가 82개의 애플리케이션을 포함하는 경우, 총 192개의 애플리케이션이 **Available Applications(사용 가능한 애플리케이션)** 목록에 표시됩니다.

서로 다른 유형의 필터는 AND 연산자로 연결됩니다. 예를 들어, Risks(위험도) 유형에서 Medium(중간) 및 High(높음) 필터를, 그리고 Business Relevance(사업 타당성) 유형에서 Medium(중간) 및 High(높음) 필터를 선택한 경우, 결과 필터는 다음과 같습니다:

Risk(위험도): Medium OR High(중간 또는 높음)
및
Business Relevance(사업 타당성): Medium OR High(중간 또는 높음)

이 경우, 시스템은 Medium(중간) 또는 High Risk(위험도 높음) 유형과 Medium(중간) 또는 High Business Relevance(사업 타당성 높음) 유형이 모두 포함된 애플리케이션만 표시됩니다.

필터 찾기 및 선택

필터를 선택하려면 필터 옆의 화살표를 클릭하여 확장한 다음, 표시하거나 숨기려는 애플리케이션의 각 필터 옆에 있는 확인란을 선택하거나 선택을 취소합니다. 또한 시스템에서 제공한 필터 유형을 마우스 오른쪽 단추로 클릭하여(**Risks(위험도)**, **Business Relevance(사업 타당성)**, **Types(유형)**, **Categories(카테고리)** 또는 **Tags(태그)**) **Check All(모두 선택)** 또는 **Uncheck All(모두 선택 취소)**을 선택합니다.

필터를 검색하려면, **Available Filters(사용 가능한 필터)** 목록 위에 있는 **Search by name(이름으로 검색)** 프롬프트를 클릭한 후, 이름을 입력합니다. 입력을 수행하면 목록이 업데이트되어 일치하는 필터를 표시합니다.

필터 선택을 완료한 후, **Available Applications(사용 가능한 애플리케이션)** 목록을 사용하여 규칙에 필터를 추가합니다(8-4페이지의 개별 애플리케이션에서 나가는 트래픽 일치 참고).

개별 애플리케이션에서 나가는 트래픽 일치

라이센스: 제어

액세스 제어 규칙에서 애플리케이션 조건을 작성할 경우, **Available Applications(사용 가능한 애플리케이션)** 목록을 사용하여 트래픽을 일치시킬 애플리케이션을 선택합니다.

애플리케이션 목록 탐색

조건 만들기를 처음 시작할 경우 목록은 제한되지 않은 상태이며, 시스템에서 탐지되는 모든 애플리케이션이 한 번에 100개씩 표시됩니다.

- 애플리케이션 페이지를 넘기려면 목록 아래의 화살표를 클릭합니다.
- 팝업 창에 애플리케이션 특징에 대한 요약 정보뿐 아니라 찾아갈 수 있는 인터넷 검색 링크를 표시하려면, 애플리케이션 옆에 있는 정보 아이콘( )을 클릭합니다.

일치시킬 애플리케이션 찾기

일치시키려는 애플리케이션을 찾으려면, 다음과 같은 방법으로 **Available Applications(사용 가능한 애플리케이션)** 목록을 제한할 수 있습니다.

- 애플리케이션을 검색하려면, 목록 위에 있는 **Search by name(이름으로 검색)** 프롬프트를 클릭한 후, 이름을 입력합니다. 입력을 수행하면 목록이 업데이트되어 일치하는 애플리케이션을 표시합니다.
- 필터를 적용하여 애플리케이션을 제한하려면, **Application Filters(애플리케이션 필터)** 목록을 사용합니다(8-3페이지의 애플리케이션 필터를 통한 트래픽 일치 참고). 필터를 적용하면 **Available Applications(사용 가능한 애플리케이션)** 목록이 업데이트됩니다.

제한이 이루어지면, **Available Applications(사용 가능한 애플리케이션)** 목록 상단에 **All apps matching the filter(필터와 일치하는 모든 앱)** 옵션이 표시됩니다. 이 옵션을 사용하면 제한된 목록의 모든 애플리케이션을 **Selected Applications and Filters(선택한 애플리케이션 및 필터)** 목록에 한번에 추가할 수 있습니다.

참고 애플리케이션 필터 목록에서 하나 이상의 필터를 선택하고 **Available Applications(사용 가능한 애플리케이션)** 목록을 검색하는 경우, 선택한 항목 및 검색-필터링을 거친 **Available Applications(사용 가능한 애플리케이션)** 목록이 AND 연산을 사용하여 조합됩니다. 즉, **All apps matching the filter(필터와 일치하는 모든 앱)** 조건에는 **Available Applications(사용 가능한 애플리케이션)** 목록에 현재 표시된 모든 개별 조건뿐 아니라 **Available Applications(사용 가능한 애플리케이션)** 목록 위에 입력된 검색 문자열이 포함됩니다.

조건에서 일치하는 단일 애플리케이션 선택

일치시키려는 애플리케이션을 찾은 다음 클릭하여 선택합니다. 여러 애플리케이션을 선택하려면, Shift(쉬프트)와 Ctrl(컨트롤) 키를 사용하거나 마우스 오른쪽 단추로 클릭 후 **Select All(모두 선택)**을 선택하여 현재 제한된 뷰에서 모든 애플리케이션을 선택합니다.

단일 애플리케이션 조건의 경우, 최대 50개의 애플리케이션을 개별적으로 선택하여 일치시킬 수 있습니다. 50개 이상을 추가하려면 반드시 여러 액세스 제어 규칙을 생성하거나 필터를 사용하여 애플리케이션을 그룹화해야 합니다.

조건에 대한 필터와 일치하는 모든 애플리케이션 선택

Application Filters(애플리케이션 필터) 목록에서 필터를 검색하거나 사용하여 제한이 이루어진 경우, **Available Applications(사용 가능한 애플리케이션)** 목록 상단에 **All apps matching the filter(필터와 일치하는 모든 앱)** 옵션이 표시됩니다.

이 옵션을 사용하면 제한된 **Available Applications(사용 가능한 애플리케이션)** 목록에서 전체 애플리케이션 집합을 **Selected Applications and Filters(선택한 애플리케이션 및 필터)** 목록에 한번에 추가할 수 있습니다. 애플리케이션을 개별적으로 추가하는 것과는 달리, 이렇게 애플리케이션 집합을 추가하면 구성하는 개별 애플리케이션의 수에 관계 없이 최대 50개까지 한 개의 항목으로 계산됩니다.

애플리케이션 조건을 이러한 방식으로 만들 경우, **Selected Applications and Filters(선택한 애플리케이션 및 필터)** 목록에 추가하는 필터의 이름은 필터에 표시된 필터 유형과 각 유형의 세 가지 필터의 이름을 최대 세 개까지 더하여 연결됩니다. 동일한 유형의 필터가 3개 이상 나오면 뒤에 생략 부호(...)가 표시됩니다. 예를 들어, 다음 필터 이름은 Risks(위험도) 유형에서 두 개의 필터, Business Relevance(사업 타당성)에서 네 개의 필터를 포함합니다.

```
Risks(위험도): Medium, High(중간, 높음) Business Relevance(사업 타당성): Low, Medium,
High,...(낮음, 중간, 높음,....)
```

All apps matching the filter(필터와 일치하는 모든 앱)를 사용하여 추가하는 필터에 나타나지 않은 필터 유형은 추가하는 필터의 이름에 포함되지 않습니다. 이 필터 유형은 *모든*으로 설정되어 있습니다. 즉, 이 필터 유형은 필터를 제한하지 않으며, 따라서 이를 위해서는 모든 값이 허용됩니다.

애플리케이션 조건에 **Selected Applications and Filters(선택한 애플리케이션 및 필터)** 목록에 있는 개별 항목으로서 각 경우와 함께 **All apps matching the filter(필터와 일치하는 모든 앱)**의 여러 예를 추가할 수 있습니다. 예를 들어, 모든 고위험도 애플리케이션을 하나의 항목으로 추가할 수 있으며, 선택을 취소한 후 모든 낮은 사업 타당성 애플리케이션을 다른 하나의 항목으로 추가할 수 있습니다. 이 애플리케이션 조건은 고위험도이거나 사업 타당성이 낮은 애플리케이션과 일치합니다.

액세스 제어 규칙에 애플리케이션 조건 추가

라이센스: 제어

액세스 제어 규칙을 애플리케이션 조건과 맞춘 트래픽의 경우, 해당 트래픽은 반드시 **Selected Applications and Filters(선택한 애플리케이션 및 필터)** 목록에 추가한 애플리케이션 또는 필터 중 하나와 일치해야 합니다.

조건 당 최대 50개 항목을 추가할 수 있으며, 조건에 추가된 필터는 개별적으로 추가한 애플리케이션으로부터 분리하여 위쪽에 별도로 나열됩니다. 애플리케이션 조건을 구축할 때, 경고 아이콘은 유효하지 않은 구성을 나타냅니다. 자세한 내용을 보려면 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

애플리케이션 트래픽을 제어하려면 다음을 수행합니다.

단계 1 애플리케이션별 트래픽 제어를 원하는 지점의 액세스 제어 정책에서 새로운 액세스 제어 규칙을 만들거나 기존 규칙을 수정합니다.

자세한 내용은 6-2페이지의 액세스 제어 규칙 생성 및 수정을 참고하십시오.

단계 2 규칙 편집기에서, Applications(애플리케이션) 탭을 선택합니다.

Applications(애플리케이션) 탭이 나타납니다.

단계 3 또는, 필터를 사용하여 **Available Applications(사용 가능한 애플리케이션)** 목록에 표시되는 애플리케이션의 목록을 제한합니다.

Application Filters(애플리케이션 필터) 목록에서 하나 이상의 필터를 선택합니다. 자세한 내용은 8-3페이지의 애플리케이션 필터를 통한 트래픽 일치를 참고하십시오.

단계 4 **Available Applications(사용 가능한 애플리케이션)** 목록에서 추가하려는 애플리케이션을 찾아 선택합니다.

개별 애플리케이션을 검색하여 선택하거나 목록이 제한된 경우 **All apps matching the filter(필터와 일치하는 모든 앱)**를 검색하여 선택할 수 있습니다. 자세한 내용은 8-4페이지의 개별 애플리케이션에서 나가는 트래픽 일치를 참고하십시오.

단계 5 **Add to Rule(규칙에 추가)**을 클릭하여 **Selected Applications and Filters(선택한 애플리케이션 및 필터)** 목록에 선택한 애플리케이션을 추가합니다.

또한 선택한 애플리케이션 및 필터를 끌어다 놓을 수 있습니다. 필터는 표제 *Filters(필터)* 아래에 표시되고, 애플리케이션은 표제 *Applications(애플리케이션)* 아래에 표시됩니다.

팁 이 애플리케이션 조건에 다른 필터를 추가하기 전에, **Clear All Filters(모든 필터 선택 해제)**를 클릭하여 기존의 선택을 취소합니다.

단계 6 또는, 추가 아이콘( )(**Selected Applications and Filters(선택한 애플리케이션 및 필터)** 목록 상단)을 클릭하여 현재 목록에 있는 필터 및 모든 개별 애플리케이션으로 구성된 사용자 정의 필터를 저장합니다.

개체 관리자를 사용하여 상황에 따라 생성된 필터를 관리하십시오(2-12페이지의 애플리케이션 필터 작업 참고). 다른 사용자 생성 필터를 포함하는 필터를 저장할 수 없고, 사용자 생성 필터는 중첩될 수 없다는 점에 유의하십시오.

단계 7 규칙을 저장하거나 계속 수정합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

애플리케이션 제어의 한계

라이센스: 제어

애플리케이션 제어를 수행할 때 다음 사항에 유의하십시오.

애플리케이션 식별 속도

시스템에서 다음을 작업한 후 애플리케이션 제어를 수행할 수 있습니다.

- 클라이언트와 서버 간에 모니터링된 연결 설정
- 시스템이 세션에서 애플리케이션 식별

이 식별은 3-5 패킷 내에 이루어져야 합니다. 애플리케이션 조건을 포함하는 액세스 제어 규칙에서 다른 모든 조건이 첫 번째 패킷 중 하나에 일치하지만 식별이 완료되지 않은 경우, 액세스 제어 정책은 해당 패킷을 전달할 수 있습니다. 이 작업은 애플리케이션이 식별될 수 있도록 연결 설정을 허용합니다. 사용자 편의를 위해 영향을 받는 규칙은 정보 아이콘( )으로 표시됩니다.

허용되는 패킷은 액세스 제어 정책의 *기본* 침입 정책(*기본 작업* 침입 정책도 아니고 거의 일치하는 규칙의 침입 정책도 아님)에 의해 검사됩니다. 자세한 내용은 13-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을 참고하십시오.

시스템은 해당 식별을 마친 후, 액세스 제어 규칙 작업뿐 아니라 모든 관련 침입 및 파일 정책을 애플리케이션 상태와 일치하는 나머지 세션 트래픽에 적용합니다.

암호화된 트래픽 처리

시스템은 비암호화 애플리케이션 트래픽을 식별하고 필터링할 수 있습니다. 이는 SMTPS, POPS, FTPS, TelnetS 및 IMAPS와 같은 StartTLS를 사용하여 암호화됩니다. 또한, 시스템은 TLS client hello 메시지 내 서버 이름 지표 또는 서버 인증서 주체로 구별되는 이름값에 따라 암호화된 특정 애플리케이션을 식별할 수 있습니다.

이 애플리케이션은 **SSL 프로토콜**로 태그됩니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽에서만 탐지될 수 있습니다.

페이로드 없이 애플리케이션 트래픽 패킷 처리

시스템은 애플리케이션이 식별된 연결에서 페이로드가 없는 패킷에 기본 정책 작업을 적용합니다.

참조된 트래픽 처리

광고물 트래픽과 같이, 웹 서버에서 참조된 트래픽에서 작동하는 규칙을 생성하기 위해서는, 참조하는 애플리케이션이 아닌 참조되는 애플리케이션을 위한 조건을 추가합니다.

다중 프로토콜을 사용하는 애플리케이션 트래픽 제어(Skype)

시스템은 Skype 애플리케이션 트래픽의 여러 유형을 탐지할 수 있습니다. Skype 트래픽을 제어하기 위한 애플리케이션 조건을 구축하는 경우, 개별 애플리케이션을 선택하지 말고 **Application Filters(애플리케이션 필터)** 목록에서 **Skype** 태그를 선택합니다. 이렇게 하면 시스템이 동일한 방법으로 모든 Skype 트래픽을 탐지하고 제어할 수 있도록 할 수 있습니다. 자세한 내용은 8-3페이지의 애플리케이션 필터를 통한 트래픽 일치를 참고하십시오.

URL 차단

라이센스: 기능에 따라 다름

액세스 제어 규칙 내 URL 조건을 통해 네트워크에 있는 사용자가 액세스할 수 있는 웹 사이트를 제한할 수 있습니다. 이 기능을 *URL 필터링*이라고 합니다. 액세스 제어를 사용하여 차단(또는 반대로 허용)하려는 URL을 지정하는 방법에는 두 가지가 있습니다.

- 어떤 것이든 라이센스가 있으면 수동으로 개별 URL 또는 그룹 URL을 지정하여 웹 트래픽에 대한 사용자 지정 제어를 세분화할 수 있습니다.
- URL 필터링 라이센스로는 또한 URL의 공통 분류나 *카테고리* 및 위험 수준 또는 *평판*에 따라 웹 사이트에 대한 액세스를 제어할 수 있습니다. 시스템은 이 카테고리와 평판 데이터를 연결 로그, 침입 이벤트 및 애플리케이션 세부 정보에서 표시합니다.

참고 이벤트의 URL 카테고리 및 평판 정보를 보려면, URL 상태와 더불어 1개 이상의 액세스 제어 규칙을 만들어야 합니다.

웹 사이트를 차단하면 사용자의 브라우저에 기본 작업을 허용하거나 시스템 제공 또는 사용자 지정 일반 페이지를 표시할 수 있습니다. 또한 사용자에게 경고 페이지를 통해 클릭하여 웹 사이트 차단을 우회하도록 할 수도 있습니다.

표 8-2 URL 필터링의 라이센스 요건

요건	카테고리 및 평판 기반	수동
라이센스	URL 필터링	모두

자세한 내용은 다음을 참고하십시오.

- 8-8페이지의 평판 기반 URL 차단 수행
- 8-10페이지의 수동 URL 차단 실행
- 8-11페이지의 URL 탐지 및 차단에 대한 제한
- 8-12페이지의 사용자의 URL 차단 우회 허용
- 8-14페이지의 차단된 URL을 위한 사용자 지정 웹페이지 표시

평판 기반 URL 차단 수행

라이센스: URL 필터링

URL 필터링 라이센스가 있으면, 요청된 URL의 평판과 카테고리에 기반하여 사용자가 웹사이트에 액세스하는 것을 제어할 수 있으며, 이들은 ASA FirePOWER 모듈이 Cisco 클라우드에서 얻을 수 있습니다.

- URL *카테고리*는 URL에 대한 일반 분류입니다. 예를 들어, ebay.com은 **Auctions(경매)** 카테고리에, monster.com은 **Job Search(구직)** 카테고리에 속합니다. 하나의 URL이 여러 카테고리에 속할 수 있습니다.
- URL *평판*은 URL이 사용자가 속한 조직의 보안 정책에 어긋나는 용도로 사용될 수 있는 가능성을 나타냅니다. URL의 위험도는 **High Risk(고위험)**(레벨 1)부터 **Well Known(잘 알려진)**(레벨 5)으로 나타냅니다.

참고 카테고리 및 평판 기반 URL 조건과 더불어 액세스 제어 규칙이 효과를 나타내기 전에 **반드시** Cisco 클라우드와의 통신을 활성화해야 합니다. 이는 ASA FirePOWER 모듈이 URL 데이터를 검색하도록 허용합니다. 자세한 내용은 33-6페이지의 클라우드 커뮤니케이션 활성화를 참고하십시오.

평판 기반 URL 차단의 이점

URL 카테고리 및 평판을 통해 액세스 제어 규칙의 URL 조건을 신속하게 만들 수 있습니다. 예를 들어, **Abused Drugs(남용 약물)** 카테고리 안에 있는 모든 **High Risk(고위험)** URL을 식별하고 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL 검색을 시도하는 모든 경우, 세션이 차단됩니다.

Cisco클라우드에서 카테고리 및 평판 데이터를 사용하면 정책 생성 및 관리도 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 예상대로 제어할 수 있습니다. 마지막으로, 클라우드는 계속해서 새 URL 및 기존 URL을 위한 새로운 카테고리와 위험 요소로 업데이트되기 때문에, 시스템이 최신 정보를 사용하여 요청된 URL를 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 사이트는 새로운 정책을 업데이트하고 적용하는 것보다 빠르게 나타났다 사라질 수 있습니다.

몇 가지 예를 들면 다음과 같습니다.

- 규칙이 모든 게임 사이트를 차단하는 경우, 새로운 도메인이 **Gaming(게임)**으로 등록되고 분류되는 순간 시스템은 해당 사이트를 자동으로 차단할 수 있습니다.
- 규칙이 모든 악성코드 사이트를 차단하는 경우, 블로그 페이지 하나가 악성코드에 감염되면 클라우드는 해당 URL의 카테고리를 **Blog(블로그)**에서 **Malware(악성코드)**로 재조정하고 시스템은 해당 사이트를 차단할 수 있습니다.
- 규칙이 고위험군의 소셜 네트워킹 사이트를 차단하는 경우, 누군가 자신의 프로파일 페이지에 악성코드 페이로드로 연결될 수 있는 링크가 포함된 링크를 게시하면 클라우드는 해당 페이지의 평판을 **Benign sites(안전한 사이트)**에서 **High Risk(고위험)**로 변경하여 시스템이 해당 페이지를 차단할 수 있습니다.

클라우드가 URL의 카테고리 또는 평판을 알지 못하거나, ASA FirePOWER 모듈이 클라우드에 접속할 수 없는 경우, 해당 URL은 카테고리 또는 평판 기반의 URL 조건을 가진 액세스 제어 규칙을 이끌어내지 **않습니다**. URL에 카테고리 또는 평판을 수동으로 할당할 수 없습니다.

URL 조건 구성

단일 URL 조건에서 일치하는 **Selected URLs(선택한 URL)**에 최대 50개의 항목을 추가할 수 있습니다. 각 URL 카테고리는 평판에 따라 선택적으로 자격을 부여받으며, 단일 항목으로 계산됩니다. URL 조건에서 문자 URL 및 URL 개체를 사용할 수는 있지만, 이 항목을 평판으로 분류할 수 없다는 점에 유의하십시오. 자세한 내용은 8-10페이지의 수동 URL 차단 실행을 참고하십시오.

문자 URL 또는 URL 개체에 평판을 가지고 자격을 부여할 수 없다는 점에 유의하십시오.

URL 조건을 구축할 때, 경고 아이콘은 유효하지 않은 구성을 나타냅니다. 자세한 내용을 보려면 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

카테고리 및 평판 데이터를 사용하여 요청된 URL로 트래픽을 제어하려면 다음을 수행합니다.

단계 1 URL별 트래픽 제어를 원하는 지점의 액세스 제어 정책에서 새로운 액세스 제어 규칙을 만들거나 기존 규칙을 수정합니다.

자세한 내용은 6-2페이지의 액세스 제어 규칙 생성 및 수정을 참고하십시오.

단계 2 규칙 편집기에서, URL 탭을 선택합니다.

URL 탭이 나타납니다.

단계 3 **Categories and URLs(카테고리 및 URL)** 목록에서 추가를 원하는 URL의 카테고리를 찾아 선택합니다. 카테고리에 관계 없이 웹 트래픽과 일치시키려면, **Any(모든)** 카테고리를 선택합니다.

카테고리를 찾아 선택하려면, **Categories and URLs(카테고리 및 URL)** 목록 위에 있는 **Search by name or value(이름 또는 값으로 검색)** 프롬프트를 클릭한 후 카테고리 이름을 입력합니다. 일치하는 카테고리를 입력하여 표시하면 목록이 업데이트됩니다.

카테고리를 선택하려면, 이를 클릭합니다. 여러 카테고리를 선택하려면, Shift(쉬프트)와 Ctrl(컨트롤) 키를 사용합니다.

팁 마우스 오른쪽 단추를 클릭하여 카테고리를 **Select All(모두 선택)**할 수도 있지만, 이런 방식으로 모든 카테고리를 추가하는 것은 액세스 제어 규칙에 대한 50개의 최대 항목을 초과합니다. 이보다는 **Any(모두)**를 사용하십시오.

단계 4 또는, **Reputations(평판)** 목록에서 평판 수준을 클릭하여 선택한 카테고리에 자격을 부여합니다. 평판 수준을 지정하지 않은 경우, 시스템은 **Any(모두)**를 기본값으로 하며, 이는 모든 수준임을 의미합니다.

오직 하나의 평판 수준만 선택할 수 있습니다. 평판 수준을 선택할 경우, 액세스 제어 규칙은 목적에 따라 다르게 작동합니다.

- 규칙이 웹 액세스를 모니터링하거나 차단하는 경우(규칙 작업은 **Block(차단)**, **Block with reset(차단 후 초기화)**, **Interactive Block(인터랙티브 차단)**, **Interactive Block with reset(인터랙티브 차단 후 초기화)** 또는 **Monitor(모니터링)**), 하나의 평판 수준을 선택하는 것은 또한 해당 수준보다 더욱 엄격한 모든 평판을 선택하는 것입니다. 예를 들어, **Suspicious sites(의심스러운 사이트)**(레벨 2)를 모니터링하거나 차단하는 규칙을 구성하는 경우, 이는 또한 **High risk(고위험)**(레벨 1) 사이트를 자동으로 모니터링하거나 차단합니다.
- 규칙이 웹 액세스를 허용하는 경우, 해당 웹 액세스를 신뢰하든 또는 추가 조사하든 상관 없이(규칙 작업은 **Allow(허용)** 또는 **Trust(신뢰)**), 하나의 평판 수준을 선택하면 해당 수준보다 덜 엄격한 모든 평판도 선택됩니다. 예를 들어, **Benign sites(안전한 사이트)**(레벨 4)를 허용하는 규칙을 구성하는 경우, 이는 또한 **Well known(잘 알려진)**(레벨 5) 사이트를 자동으로 허용합니다.

규칙 작업을 변경한 경우, 시스템은 상기 요점에 따라 자동으로 URL 조건의 평판 수준을 변경합니다.

단계 5 이를 **Selected URLs(선택한 URL)** 목록에 추가하려면 **Add to Rule(규칙에 추가)**을 클릭하거나 선택 항목을 끌어다 놓습니다.

단계 6 규칙을 저장하거나 계속 수정합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

수동 URL 차단 실행

라이센스: 모두

카테고리와 평판으로 URL 필터링을 보완 또는 선택적으로 재설정하려면 수동으로 개별 URL 또는 URL 그룹을 지정하여 웹 트래픽을 제어하면 됩니다. 이를 통해 허용되거나 차단된 웹 트래픽에 대해 사용자 지정 제어를 세분화할 수 있습니다. 또한 이러한 유형의 URL 필터링을 실행하는 데는 특별한 라이센스가 필요하지 않습니다.

액세스 제어 규칙에서 허용하거나 차단하도록 URL을 수동으로 지정하려면 단일 문자 URL에서 입력할 수 있습니다. 또는, URL 개체를 사용하여 URL 조건을 구성할 수 있는데, 이는 재사용이 가능하며 URL 또는 IP 주소와 이름을 결합합니다.

팁 URL 개체를 만든 후에는 액세스 제어 규칙을 작성하는 데 뿐만 아니라 시스템의 모듈 인터페이스 내 다양한 장소에서 URL을 나타나는 데에도 사용할 수 있습니다. 개체 관리자를 사용하여 이 개체를 만들 수 있습니다. 액세스 제어 규칙을 구성하는 동안 상황에 따라 URL 개체를 만들 수도 있습니다. 자세한 내용은 2-11페이지의 URL 개체 작업을 참고하십시오.

URL 조건에서 URL 수동 지정

수동 입력은 허용된 웹 트래픽 및 차단된 웹 트래픽에 대한 정확한 제어를 가능하게 하지만, 평판으로 수동 지정된 URL에 자격을 부여할 수는 없습니다. 또한, 사용자는 규칙에 의도하지 않은 결과가 없도록 해야 합니다. URL 조건이 네트워크 트래픽과 일치하는지 확인하기 위해 시스템은 간단한 부분 문자열 일치를 실행합니다. URL 개체 또는 수동으로 입력한 URL의 값이 모니터링된 호스트가 요청한 URL의 일부와 일치하는 경우 액세스 제어 규칙의 URL 조건을 충족합니다.

따라서, URL 개체에 포함되는 것을 비롯하여, URL 조건에서 수동으로 URL를 지정할 때 영향을 받을 수 있는 다른 트래픽을 신중하게 고려합니다. 예를 들어, example.com의 모든 트래픽을 허용하는 경우, 사용자는 다음을 포함하는 URL을 찾아볼 수 있습니다.

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

다른 예로, ign.com(게임 사이트)의 차단을 명시적으로 원하는 경우의 차단 시나리오를 생각해 보십시오. 부분 문자열 일치가 의미하는 바는 *ign.com*을 차단하면 의도치 않게 veris*ign.com* 또한 차단한다는 것입니다.

암호화된 웹 트래픽 수동 차단

액세스 제어 규칙 내 URL 조건:

- 웹 트래픽(HTTP 또는 HTTPS)의 암호화 프로토콜 무시

  예를 들어, 액세스 제어 규칙은 https://example.com/ 트래픽을 http://example.com/ 트래픽과 동일하게 처리합니다. HTTP 또는 HTTPS 트래픽에만 일치하는 액세스 제어 규칙을 구성하려면 규칙에 애플리케이션 조건을 추가합니다. 자세한 내용은 8-7페이지의 URL 차단을 참고하십시오.

- 트래픽을 암호화하는 데 사용되는 공개 키 인증에서 제목 일반 이름에 근거한 HTTPS 트래픽 일치, 그리고 제목 일반 이름 내의 하위 도메인 무시

  수동으로 HTTPS 트래픽을 필터링할 경우 하위 도메인 정보를 포함하지 마십시오.

URL 조건을 구축할 때, 경고 아이콘은 유효하지 않은 구성을 나타냅니다. 자세한 내용을 보려면 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

허용하거나 차단할 URL를 수동으로 지정하여 웹 트래픽을 제어하려면 다음을 수행합니다.

단계 1 URL별 트래픽 제어를 원하는 지점의 액세스 제어 정책에서 새로운 액세스 제어 규칙을 만들거나 기존 규칙을 수정합니다.

자세한 내용은 6-2페이지의 액세스 제어 규칙 생성 및 수정을 참고하십시오.

단계 2 규칙 편집기에서, URL 탭을 선택합니다.

URL 탭이 나타납니다.

단계 3 **Categories and URLs(카테고리 및 URL)** 목록에서 추가를 원하는 URL 개체와 그룹을 찾아 선택합니다.

- 상황에 따라 URL 개체를 추가하여 조건에 추가하려면, 추가 아이콘( )(**Categories and URLs(카테고리 및 URL)** 위)을 클릭합니다(2-11페이지의 URL 개체 작업 참고).
- 추가할 URL 개체 및 그룹을 검색하려면, **Categories and URLs(카테고리 및 URL)** 목록 위에 있는 **Search by name or value(이름 또는 값으로 검색)** 프롬프트를 클릭한 후 개체 이름 또는 개체의 URL이나 IP 주소 중 하나의 값을 입력합니다. 일치하는 개체를 입력하여 표시하면 목록이 업데이트됩니다.

개체를 선택하려면 이를 클릭합니다. 여러 개체를 선택하려면, Shift(쉬프트)와 Ctrl(컨트롤) 키를 사용합니다. 마우스 오른쪽 단추를 클릭하여 URL 개체 및 카테고리를 **Select All(모두 선택)**할 수도 있지만, 이런 방식으로 URL을 추가하는 것은 액세스 제어 규칙에 대한 50개의 최대 항목을 초과합니다.

단계 4 **Add to Rule(규칙에 추가)**을 클릭하여 **Selected URLs(선택한 URL)** 목록에 선택한 항목을 추가합니다.

또한 선택한 항목을 끌어다 놓을 수 있습니다.

단계 5 수동 지정을 원하는 모든 문자 URL를 추가합니다. 이 필드에는 다음과 같은 와일드카드를 사용할 수 **없습니다**. *

Selected URLs(선택한 URL) 목록 아래의 **Enter URL(URL 입력)** 프롬프트를 클릭한 후, URL 또는 IP 주소를 입력하고 **Add(추가)**를 클릭합니다.

단계 6 규칙을 저장하거나 계속 수정합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

URL 탐지 및 차단에 대한 제한

라이센스: 모두

URL 탐지 및 차단을 수행할 때는 다음 사항에 유의하십시오.

URL 식별 속도

시스템은 다음 작업을 수행한 후 URL을 필터링할 수 있습니다.

- 클라이언트와 서버 간에 모니터링된 연결 설정
- 시스템이 세션에서 HTTP 또는 HTTPS 애플리케이션 식별
- 시스템이 요청된 URL 식별(암호화된 세션의 경우, client hello 메시지 또는 서버 인증서로부터)

이 식별은 3-5 패킷 내에 이루어져야 합니다. URL 조건을 포함하는 액세스 제어 규칙에서 다른 모든 조건이 첫 번째 패킷 중 하나에 일치하지만 식별이 완료되지 않은 경우, 액세스 제어 정책은 해당 패킷을 전달할 수 있습니다. 이 작업은 URL이 식별될 수 있도록 연결 설정을 허용합니다. 사용자 편의를 위해 영향을 받는 규칙은 정보 아이콘( )으로 표시됩니다.

허용되는 패킷은 액세스 제어 정책의 *기본* 침입 정책(*기본 작업* 침입 정책도 아니고 거의 일치하는 규칙의 침입 정책도 아님)에 의해 검사됩니다. 자세한 내용은 13-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을 참고하십시오.

시스템은 해당 식별을 마친 후, 액세스 제어 규칙 작업뿐 아니라 모든 관련 침입 및 파일 정책을 URL 상태와 일치하는 나머지 세션 트래픽에 적용합니다.

암호화된 웹 트래픽 처리

액세스 제어 규칙과 URL 조건을 사용하여 암호화된 웹 트래픽을 평가할 때, 시스템이 하는 일은 다음과 같습니다.

- 암호화 프로토콜 무시. 규칙에 URL 정보가 있지만 프로토콜을 지정하는 애플리케이션 조건이 없는 경우 HTTPS 및 HTTP 트래픽 모두에 일치하는 액세스 제어 규칙
- 트래픽을 암호화하는 데 사용되는 공개 키 인증에서 제목 일반 이름에 근거한 HTTPS 트래픽 일치, 그리고 제목 일반 이름 내의 하위 도메인 무시
- 하나를 구성했다 하더라도 HTTP 응답 페이지를 표시하지 않음

URL 내 검색 쿼리 매개변수

시스템은 URL 조건과 일치하도록 URL에서 검색 쿼리 매개변수를 사용하지 않습니다. 예를 들어, 모든 쇼핑 트래픽을 차단하는 시나리오를 생각해 보십시오. 이 경우, amazon.com을 검색하기 위해 웹 검색을 사용하는 것은 차단되지 않지만 amazon.com 브라우징은 차단됩니다.

사용자의 URL 차단 우회 허용

라이센스: 모두

액세스 제어 규칙을 사용하여 사용자의 HTTP 웹 요청을 차단하는 경우, 규칙 작업을 **Interactive Block(인터랙티브 차단)** 또는 **Interactive Block with reset(인터랙티브 차단 후 초기화)**으로 설정해 두면 사용자는 경고 *HTTP 응답 페이지*를 통해 클릭함으로써 차단을 우회할 수 있습니다. 시스템이 제공하는 일반 응답 페이지를 표시하거나 사용자 지정 HTML을 입력할 수 있습니다.

기본적으로 시스템에서는 사용자가 10분(600초) 동안 후속 방문에서 경고 페이지 표시 없이 연결을 우회할 수 있습니다. 이 기간은 최대 1년까지 설정할 수 있으며, 사용자가 매번 차단을 강제로 우회하도록 할 수도 있습니다.

사용자가 차단을 우회하지 않는 경우, 일치하는 트래픽은 추가 검사 없이 거부되며 연결을 초기화할 수 있습니다. 반면, 사용자가 차단을 우회하는 경우, 시스템은 트래픽을 허용합니다. 이 트래픽을 허용하는 것은 침입, 악성코드 그리고 금지 파일에 대한 암호화되지 않은 페이로드를 계속해서 검사할 수 있다는 의미입니다. 로드하지 않은 페이지 요소를 로드하기 위해 사용자는 차단을 우회한 후 새로 고침해야 할 수 있다는 점에 유의하십시오.

차단 규칙을 구성하는 응답 페이지와 별도로 인터랙티브 HTTP 응답 페이지를 구성할 수 있습니다. 예를 들어, 세션이 상호 작용 없이 차단된 사용자에게 시스템이 제공한 페이지를 표시할 수는 있지만 계속을 클릭한 사용자에게는 사용자 지정 페이지를 표시할 수 있습니다. 자세한 내용은 8-14페이지의 차단된 URL을 위한 사용자 지정 웹페이지 표시를 참고하십시오.

팁 신속하게 액세스 제어 정책의 모든 규칙에 인터랙티브 차단을 비활성화하려면, 시스템 제공 페이지와 사용자 지정 페이지를 모두 표시하지 마십시오. 이렇게 되면 시스템은 상호 작용 없는 Interactive Block(인터랙티브 차단) 규칙과 일치하는 모든 연결을 차단합니다.

사용자가 웹 사이트 차단을 우회하도록 허용하려면 다음을 수행합니다.

단계 1 URL 조건과 더불어 웹 트래픽에 일치하는 액세스 제어 규칙을 만듭니다.

8-8페이지의 평판 기반 URL 차단 수행 및 8-10페이지의 수동 URL 차단 실행을 참고하십시오.

단계 2 액세스 제어 규칙 작업이 **Interactive Block(인터랙티브 차단)** 또는 **Interactive Block with reset(인터랙티브 차단 후 초기화)**인지 확인합니다.

6-6페이지의 규칙 작업을 사용하여 트래픽 관리 및 검사 결정을 참고하십시오.

단계 3 사용자가 차단을 우회하고 그에 따라 규칙을 위한 검사 및 로깅 옵션을 선택할 것으로 가정합니다. Allow(허용) 규칙에서처럼

- Interactive Block(인터랙티브 차단) 규칙의 유형을 파일 및 침입 정책과 결합할 수 있습니다. 자세한 내용은 10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어를 참고하십시오.
- 인터랙티브 차단된 트래픽에 대한 로깅 옵션은 허용된 트래픽의 옵션과 동일하지만, 사용자가 인터랙티브 차단을 우회하지 않는 경우, 시스템은 연결 시작 이벤트만 로깅할 수 있다는 점에 유의하십시오.

  시스템이 사용자에게 최초 경고할 때, Interactive Block(인터랙티브 차단) 또는 Interactive Block with reset(인터랙티브 차단 후 초기화) 작업과 함께 로깅된 모든 연결 시작 이벤트를 표시합니다. 사용자가 차단을 우회하는 경우, 세션에 로깅된 추가 연결 이벤트에는 Allow(허용) 작업이 있습니다. 자세한 내용은 25-9페이지의 액세스 제어 처리에 기반한 연결 로깅을 참고하십시오.

단계 4 선택적으로, 사용자가 차단을 우회한 후 시스템이 경고 페이지를 다시 표시하기 전까지의 경과 시간을 설정합니다.

8-13페이지의 차단된 웹 사이트의 사용자 우회 시간 제한 설정을 참고하십시오.

단계 5 선택적으로, 사용자가 차단을 우회할 수 있도록 표시하는 사용자 지정 페이지를 만들어 사용합니다.

8-14페이지의 차단된 URL을 위한 사용자 지정 웹페이지 표시를 참고하십시오.

차단된 웹 사이트의 사용자 우회 시간 제한 설정

라이센스: 모두

기본적으로 시스템은 사용자가 10분(600초) 동안 후속 방문에서 경고 페이지 표시 없이 인터랙티브 차단을 우회하도록 허용합니다. 이 기간은 최대 1년까지 설정할 수 있으며 0으로 설정하여 사용자가 매번 차단을 우회하도록 할 수도 있습니다. 이러한 제한은 정책에서 모든 Interactive Block(인터랙티브 차단) 규칙을 적용합니다. 규칙별 제한은 설정할 수 없습니다.

사용자 우회가 만료되기 전에 시간의 길이를 사용자 지정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 구성하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책에 대한 고급 설정이 나타납니다.

단계 4 General Settings(일반 설정) 옆에 있는 수정 아이콘( )을 클릭합니다.

General Settings(일반 설정) 팝업 창이 나타납니다.

단계 5 **Allow an Interactive Block to bypass blocking for (seconds)((초)동안 차단 우회를 위한 인터랙티브 차단 허용)** 필드에 사용자 우회가 만료되기 전에 경과해야 하는 시간(초)을 입력합니다.

0-31536000초(1년)의 시간(초)을 지정할 수 있습니다. 0를 지정하면 사용자가 매번 차단을 강제로 우회하도록 합니다.

단계 6 **OK(확인)**를 클릭합니다.

액세스 제어 정책에 대한 고급 설정이 나타납니다.

단계 7 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 저장)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다. 자세한 내용은 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

차단된 URL을 위한 사용자 지정 웹페이지 표시

라이센스: 모두

시스템이 액세스 제어 규칙의 작업을 사용하여 사용자의 HTTP 웹 요청을 차단하는 경우, 사용자가 브라우저에서 보는 내용은 세션을 차단하는 방식에 따라 다릅니다. 선택해야 하는 사항은 다음과 같습니다.

- **Block(차단)** 또는 **Block with reset(차단 후 초기화)**을 선택하여 연결을 거부합니다. 차단된 세션의 시간이 초과되며, 시스템에서 차단 후 초기화 연결을 초기화합니다. 그러나, 두 가지 차단 작업 모두 연결이 거부되었음을 설명하는 맞춤형 페이지로 기본 브라우저 또는 서버 페이지를 변경할 수 있습니다. 시스템은 이 사용자 지정 페이지를 *HTTP 응답 페이지*라고 명명합니다.
- **Interactive Block(인터랙티브 차단)** 또는 **Interactive Block with reset(인터랙티브 차단 후 초기화)**은 사용자에게 경고를 나타내는 *인터랙티브 HTTP 응답 페이지*를 표시하기를 원하는 경우입니다. 이를 사용하면 또한 사용자가 버튼을 클릭하여 페이지를 계속하거나 새로 고침하여 원래 요청한 사이트를 로드할 수 있습니다. 사용자는 로드하지 않은 페이지 요소를 로드하기 위해 응답 페이지를 우회한 후 새로 고침해야 할 수 있습니다.

시스템이 제공하는 일반 응답 페이지를 표시하거나 사용자 지정 HTML을 입력할 수 있습니다. 사용자 지정 텍스트를 입력하면 계수기에서 몇 개의 철자를 사용했는지 보여줍니다.

각 액세스 제어 정책에서 상호 작용 없이 트래픽 차단을 위해 사용하는 응답 페이지와 별도로 인터랙티브 HTTP 응답 페이지를 구성할 수 있습니다. 즉, Block(차단) 규칙을 사용하는 것입니다. 예를 들어, 세션이 상호 작용 없이 차단된 사용자에게 시스템이 제공한 페이지를 표시할 수는 있지만 계속을 클릭한 사용자에게는 사용자 지정 페이지를 표시할 수 있습니다.

사용자에게 신뢰할 수 있는 HTTP 응답 페이지를 보여주는 것은 네트워크 구성, 트래픽 로드, 페이지 크기에 따라 다릅니다. 사용자 지정 응답 페이지를 구축할 경우, 소규모 페이지가 성공적으로 표시될 가능성이 더욱 높다는 점에 유의하십시오.

HTTP 응답 페이지를 구성하려면 다음을 수행합니다.

단계 1 웹 트래픽을 모니터링하는 액세스 제어 정책을 수정합니다.

자세한 내용은 4-7페이지의 액세스 제어 정책 수정을 참고하십시오.

단계 2 HTTP Responses(HTTP 응답) 탭을 선택합니다.

액세스 제어 정책을 위한 HTTP 응답 설정 페이지가 나타납니다.

단계 3 **Block Response Page(응답 페이지 차단)** 및 **Interactive Block Response Page(응답 페이지 인터랙티브 차단)**의 경우 드롭다운 목록에서 응답을 선택합니다. 각 페이지에서 다음을 선택할 수 있습니다.

- 일반적인 답변을 사용하려면, **System-provided(시스템 제공)**를 선택합니다. 이 페이지에 대한 HTML 코드를 보려면 보기 아이콘( )을 클릭합니다.
- 사용자 지정 응답을 생성하려면, **Custom(사용자 지정)**을 선택합니다.

  수정 또는 교체할 수 있는 시스템 제공 코드가 미리 채워진 팝업 창이 열립니다. 완료했으면 변경 사항을 저장합니다. 수정 아이콘( )을 클릭하여 사용자 지정 페이지를 수정할 수 있음을 참고하십시오.
- 시스템이 HTTP 응답 표시 페이지를 표시하지 못하도록 하려면, **None(없음)**을 선택합니다. 인터랙티브 차단된 세션을 위해 이 옵션을 선택하면 사용자가 클릭하여 계속할 수 없다는 점에 유의하십시오. 세션은 상호 작용 없이 차단됩니다.

단계 4 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 저장)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다. 자세한 내용은 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

9 장

사용자 기반 트래픽 제어

액세스 제어 정책 내에서 *액세스 제어 규칙*은 네트워크 트래픽 로깅 및 처리에 세분화된 제어를 제공합니다. 액세스 제어 규칙에서 사용자 조건을 통해 *사용자 제어*를 수행하여 호스트에 로그인한 LDAP 사용자에 근거하여 트래픽을 제한함으로써 어느 트래픽이 네트워크를 통과할지를 관리할 수 있습니다.

사용자 제어는 IP 주소와 *액세스 제어 사용자*를 결합함으로써 작동합니다.시스템이 모니터링하는 대상은 지정된 사용자들로, 이들이 호스트에 로그인하거나 호스트에서 로그아웃하는 경우 또는 다른 이유로 Active Directory 자격 증명을 인증하는 경우 이를 모니터링합니다. 예를 들어, 사용자 조직은 중앙 집중식 인증을 위해 Active Directory를 이용하는 애플리케이션 또는 서비스를 사용할 수 있습니다.

사용자 조건과 함께 액세스 제어 규칙에 일치하는 트래픽의 경우, 모니터링된 세션의 소스 또는 대상 호스트의 IP 주소는 로그인된 액세스 제어 사용자와 연결되어야 합니다. 개별 사용자에 기반한 트래픽이나 해당 사용자들이 속한 그룹은 제어 가능합니다.

사용자 조건을 서로 결합하거나 다른 유형의 조건과 결합하여 액세스 제어 규칙을 만들 수 있습니다. 이러한 액세스 제어 규칙은 간단하거나 복잡할 수 있으며, 다양한 조건을 사용하여 트래픽에 일치시키거나 트래픽을 검사합니다. 액세스 제어 규칙에 대한 자세한 내용은 6-1페이지의 액세스 제어 규칙을 사용한 트래픽 흐름 조정을 참고하십시오.

참고 보안 인텔리전스 기반의 트래픽 필터링, 그리고 일부 디코딩 및 전처리 과정은 네트워크 트래픽이 액세스 제어 규칙으로 평가되기 **전에** 이루어집니다.

사용자 제어에는 제어 라이센스가 필요하며 이는 LDAP 사용자 및 그룹(액세스 제어 사용자)에 한해 지원됩니다.

사용자 인식을 통해 모든 형식의 배포에서 "행위"의 "대상"을 확인할 수 있습니다. 예를 들어, 다음을 확인할 수 있습니다.

- 높은 호스트 임계를 가진 서버의 무단 액세스를 시도하는 대상
- 지나치게 많은 양의 대역폭을 소비하는 대상
- 주요 운영 체제 업데이트를 적용하지 않은 대상
- 회사 IT 정책을 위반하는 인스턴트 메시징 소프트웨어 또는 P2P 파일 공유 애플리케이션을 사용하는 대상
- 침입 이벤트가 대상으로 하는 호스트를 보유하는 대상
- 내부 공격 또는 포트 스캔을 시작한 대상(보호필요)

이 정보로 무장하면 위험을 완화하는 표적 접근법을 사용할 수 있고, 다른 이들을 혼란으로부터 보호하는 조치를 취할 수 있습니다. 사용자 제어는 LDAP 사용자 및 사용자 활동을 차단하는 기능을 추가합니다. 사용자 인식과 제어 기능은 감사 통제를 확연히 향상시키고 규정 준수를 개선합니다.

다음 표는 사용자 인식 및 제어를 위한 요건을 나열합니다.

표 9-1 사용자 인식 및 제어 요건

요건	사용자 인식	사용자 제어
라이센스	모두	제어
사용자 메타데이터 복원을 위한 LDAP 서버	Windows Server 2003 및 Windows Server 2008의 Microsoft Active Directory(사용자 제어에 필요)	

자세한 내용은 다음을 참고하십시오.

- 9-2페이지의 액세스 제어 규칙에 사용자 조건 추가
- 9-3페이지의 액세스 제어 사용자 및 LDAP 사용자 메타데이터 검색

액세스 제어 규칙에 사용자 조건 추가

라이센스: 제어

ASA FirePOWER 모듈의 사용자 제어 기능은 호스트 IP 주소와 액세스 제어 사용자를 결합함으로써 작동합니다. 사용자 조건과 함께 액세스 제어 규칙에 일치하는 트래픽의 경우, 모니터링된 세션의 소스 또는 대상 호스트의 IP 주소는 로그인된 액세스 제어 사용자와 연결되어야 합니다.

사용자 제어를 수행하기 전에 ASA FirePOWER 모듈과 Microsoft Active Directory 서버 간 연결을 구성해야 합니다(9-3페이지의 액세스 제어 사용자 및 LDAP 사용자 메타데이터 검색 참고).

주의 모니터링할 많은 수의 사용자 그룹을 구성하는 경우 또는 네트워크 호스트에 매핑된 매우 많은 수의 사용자가 있는 경우, 시스템은 메모리 제한으로 인해 그룹을 기준으로 사용자 매핑을 삭제할 수 있습니다. 그 결과, 사용자 그룹 기반 액세스 제어 규칙은 예상대로 작동하지 않을 수도 있습니다.

단일 사용자 조건에서 **Selected Users(선택된 사용자)**에 최대 50명의 사용자 및 그룹을 추가할 수 있습니다. 사용자 그룹의 조건은 개별적으로 제외된 사용자 및 제외된 하위 그룹의 구성원을 예외로 한 모든 하위 그룹의 구성원을 포함하여 모든 그룹의 구성원으로부터의, 또는 구성원을 향한 트래픽에 일치됩니다.

참고 그룹 기준을 사용하는 사용자 제어를 수행하려면 먼저 시스템이 해당 그룹 내 최소 1명의 사용자로부터 활동을 탐지해야 합니다. 이 초기 연결은 일치되는 액세스 제어 규칙에 따라 처리되지 **않고** 대신 일치되는 다음 규칙 또는 액세스 제어 정책 기본 작업에 따라 처리됩니다.

사용자 조건을 구축할 때, 경고 아이콘은 유효하지 않은 구성을 나타냅니다. 자세한 내용을 보려면 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

사용자 트래픽을 제어하려면 다음을 수행합니다.

단계 1 LDAP 사용자 또는 그룹별 트래픽 제어를 원하는 액세스 제어 정책에서 새로운 액세스 제어 규칙을 만들거나 기존 규칙을 수정합니다.

자세한 내용은 6-2페이지의 액세스 제어 규칙 생성 및 수정을 참고하십시오.

단계 2 규칙 편집기에서, Users(사용자) 탭을 선택합니다.

Users(사용자) 탭이 나타납니다.

단계 3 **Available Users(사용 가능한 사용자)** 목록으로부터 추가를 원하는 사용자 및 그룹을 찾아 선택합니다.

사용자와 그룹은 다른 아이콘으로 표시됩니다. 추가할 사용자 및 그룹을 검색하려면, **Available Users(사용 가능한 사용자)** 목록 위에 있는 **Search by name or value(이름 또는 값으로 검색)** 프롬프트를 클릭한 후 사용자 또는 그룹의 이름을 입력합니다. 일치하는 항목을 입력하여 표시하면 목록이 업데이트됩니다.

항목을 선택하려면 이를 클릭합니다. 여러 항목을 선택하려면 Shift(쉬프트)와 Ctrl(컨트롤) 키를 사용하거나 마우스 오른쪽 단추를 클릭한 후 **Select All(모두 선택)**을 선택합니다.

단계 4 **Add to Rule(규칙에 추가)**를 클릭하여 **Selected Users(선택된 사용자)** 목록에 선택한 사용자 및 그룹을 추가합니다.

또한 선택한 사용자 및 그룹을 끌어다 놓을 수 있습니다.

단계 5 규칙을 저장하거나 계속 수정합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

액세스 제어 사용자 및 LDAP 사용자 메타데이터 검색

라이센스: 기능에 따라 다름

사용자 제어를 수행하기 전에(즉 사용자 조건으로 액세스 제어 규칙 작성), ASA FirePOWER 모듈과 사용자 조직의 Microsoft Active Directory 서버 중 최소 하나 간에 연결을 구성해야 합니다. ASA FirePOWER 모듈은 액세스 제어 사용자를 위한 메타데이터를 업데이트하기 위해 정기적이고 자동적으로 LDAP 서버를 쿼리합니다. 이 사용자 및 그룹은 트래픽 제한 시기의 기준으로 사용할 수 있습니다.

자세한 내용은 다음을 참고하십시오.

- 9-3페이지의 사용자 인식 및 제어를 위해 LDAP 서버에 연결
- 9-7페이지의 온디맨드 사용자 제어 매개 변수 업데이트
- 9-7페이지의 LDAP 서버와의 통신 일시 중지
- 9-8페이지의 Active Directory 로그인을 보고하도록 사용자 에이전트 사용

사용자 인식 및 제어를 위해 LDAP 서버에 연결

라이센스: FireSIGHT 또는 제어

ASA FirePOWER 모듈과 사용자 조직의 LDAP 서버 간의 연결을 통해 다음을 수행할 수 있습니다.

- 액세스 제어 규칙으로 트래픽을 제한할 때 기준으로 사용하기를 원하는 활동의 주체인 액세스 제어 사용자 및 그룹을 지정할 수 있습니다.
- 액세스 제어 사용자에 대한 메타데이터를 서버에 쿼리할 수 있습니다.

이 연결 또는 *사용자 인식 개체*는 LDAP 서버를 위한 연결 설정 및 인증 필터 설정을 지정합니다.

사용자 제어를 수행하려면, Microsoft Active Directory LDAP 서버에 연결**해야 합니다**. 단순히 LDAP 사용자 메타데이터 검색만 원할 경우, 시스템은 다른 유형의 LDAP 서버에 대한 연결을 지원합니다(9-2페이지의 표 9-1 참고).

시스템이 사용자 활동을 탐지하면,ASA FirePOWER 모듈 사용자에 해당 사용자의 레코드를 추가할 수 있습니다. ASA FirePOWER 모듈은 마지막 쿼리 이후 활동이 탐지된 새로운 사용자 및 업데이트된 사용자에 대한 메타데이터를 얻기 위해 정기적으로 LDAP 서버에 쿼리합니다. 사용자가 데이터베이스에 이미 존재할 경우, 시스템이 마지막 12시간 동안 업데이트되지 않은 경우 시스템은 메타데이터를 업데이트합니다. 시스템이 새로운 사용자 로그인을 탐지한 후 ASA FirePOWER 모듈이 사용자 메타데이터로 업데이트하는 데는 몇 분 정도 걸릴 수 있습니다.

참고 LDAP 서버에서 시스템이 탐지한 사용자를 제거할 경우, ASA FirePOWER 모듈은 **절대** 해당 사용자를 제거하지 않습니다. 반드시 수동으로 삭제해야 합니다. 그러나, ASA FirePOWER 모듈이 액세스 제어 사용자 목록을 다음에 업데이트할 때 LDAP 변경 사항은 액세스 제어 규칙에 반영됩니다.

다음 표는 모니터링된 사용자와 연결할 수 있는 LDAP 메타데이터를 나열합니다. LDAP 서버에서 사용자 메타데이터를 성공적으로 검색하려면, 서버가 **반드시** 표에 나열된 LDAP 필드 이름을 사용해야 한다는 점에 유의하십시오. LDAP 서버에서 필드 이름을 바꾸는 경우, ASA FirePOWER 모듈은 해당 필드에 있는 정보로 사용자 목록을 채울 수 없습니다.

표 9-2 Cisco 필드에 LDAP 필드 매핑

메타데이터	ASA FirePOWER 모듈	Active Directory
LDAP 사용자 이름	사용자 이름	samaccountname
이름	이름	givenname
성	성	sn
이메일 주소	이메일	mail userprincipalname(메일에 값이 없는 경우)
department	부서	department distinguishedname(부서에 값이 없는 경우)
전화번호	전화번호	telephonenumber

LDAP 서버가 정확하게 구성되어 있도록, 그리고 확실히 연결될 수 있도록 하기 위해, 그리고 LDAP 연결 생성 시 제공해야 하는 정보를 얻기 위해 LDAP 관리자와 긴밀히 협력하십시오.

서버 유형, IP 주소 및 포트

IP 주소 또는 호스트 이름, 기본 백업 및 선택적인 백업을 위한 포트 및 LDAP 서버를 지정해야 합니다. 사용자는 **반드시** Microsoft Active Directory 서버를 사용해야 합니다.

LDAP-특정 매개 변수

ASA FirePOWER 모듈이 인증 서버에서 사용자 정보를 검색하기 위해 LDAP 서버를 검색할 때, 검색을 위한 시작점이 필요합니다. *명칭 공간*, 또는 디렉토리 트리를 지정하여 구분된 기본 이름 또는 *기본 DN*을 제공함으로써 검색할 수 있습니다. 일반적으로, 기본 DN은 회사 도메인 및 운영 단위를 나타내는 기본 구조를 가지고 있습니다. 예를 들어, 예시 회사의 보안 조직은 `ou=security,dc=example,dc=com`의 기본 DN을 가질 수 있습니다. 기본 서버를 파악한 다음, 서버에서 사용 가능한 기본 DN 목록을 자동으로 검색하고 적절한 기준 DN를 선택할 수 있다는 점을 참고하십시오.

검색을 원하는 사용자 정보에 대한 적절한 권한과 더불어 사용자를 위한 사용자 자격 증명을 제공해야 합니다. 지정한 사용자의 고유 이름은 디렉터리 서버에 대한 디렉터리 정보 트리에서 고유해야 합니다.

또한 LDAP 연결을 위해 암호화 방법을 지정할 수 있습니다. 인증을 위해 인증서를 사용하는 경우, 인증서에 LDAP 서버 이름은 **반드시** ASA FirePOWER 모듈인터페이스에 지정한 호스트 이름과 일치해야 한다는 점에 유의하십시오. 예를 들어, LDAP 연결을 설정할 때 `10.10.10.250`을 사용하지만 인증서에는 `computer1.example.com`을 사용한다면 연결은 실패합니다.

마지막으로, 응답하지 않는 LDAP 서버에 대한 접속 시도가 백업 연결에 롤오버되면 시간 제한을 지정해야 합니다.

사용자 및 그룹 액세스 제어 매개 변수

사용자 제어를 수행하려면, 사용자가 액세스 제어 규칙의 기준으로 사용하기를 원하는 그룹을 지정합니다.

그룹을 자동으로 포함시키는 것은 해당 그룹의 모든 구성원을 포함하는 것이며, 모든 하위 그룹의 구성원도 포함됩니다. 그러나, 액세스 제어 규칙의 하위 그룹을 사용하려는 경우, 명시적으로 하위 그룹을 포함해야 합니다. 또한 그룹 및 개별 사용자를 제외할 수도 있습니다. 그룹을 제외하는 것은 해당 사용자가 포함된 그룹의 구성원이라고 해도 해당 그룹의 구성원 모두를 제외하는 것입니다.

액세스 제어 매개 변수가 너무 광범위한 경우, ASA FirePOWER 모듈은 사용자에 관해 가능한 많은 정보를 얻고, 작업 큐에서 검색에 실패한 사용자 수를 보고합니다.

참고 포함할 어떤 그룹도 지정하지 않은 경우, 시스템은 제공된 LDAP 매개 변수에 일치하는 모든 그룹에 대한 사용자 데이터를 검색합니다. 성능을 이유로 Cisco는 액세스 제어에서 사용을 원하는 사용자를 나타내는 그룹만 배타적으로 포함할 것을 권장합니다. 사용자 또는 도메인 사용자 그룹을 포함**할 수 없다**는 점에 유의하십시오.

또한 액세스 제어에 사용할 새로운 사용자를 포함하기 위해 ASA FirePOWER 모듈이 LDAP 서버를 얼마나 자주 쿼리할지 지정해야 합니다.

LDAP 연결을 생성한 후 삭제 아이콘( )을 클릭하고 선택을 확인하여 이를 삭제할 수 있습니다. LDAP 연결을 변경하려면, 수정 아이콘( )을 클릭합니다. 연결이 활성화된 경우, ASA FirePOWER 모듈이 다음에 LDAP 서버를 쿼리하면 저장된 변경 사항이 적용됩니다.

사용자 인식 또는 사용자 제어를 위해 LDAP 연결을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Users(사용자)**를 선택합니다.

Users Policy(사용자 정책) 페이지가 나타납니다.

단계 2 **Add LDAP Connection(LDAP 연결 추가)**을 클릭합니다.

Create User Awareness Authentication Object(사용자 인식 인증 개체 생성) 페이지가 나타납니다.

단계 3 개체의 **Name(이름)** 및 **Description(설명)**을 입력합니다.

단계 4 사용자는 **반드시** Microsoft Active Directory LDAP **Server Type(서버 유형)**을 사용해야 합니다.

단계 5 기본 LDAP 서버 및 선택적으로 백업 LDAP 서버를 위한 **IP Address(IP 주소)** 또는 **Host Name(호스트 이름)**을 지정합니다.

단계 6 LDAP 서버가 트래픽 인증을 위해 사용하는 **Port(포트)**를 지정합니다.

단계 7 액세스를 원하는 LDAP 디렉터리에 대해 **Base DNs(기본 DN)**를 지정합니다.

예를 들어, 예시 회사의 보안 조직 내 이름을 인증하려면 `ou=security,dc=example,dc=com`을 입력합니다.

팁 사용 가능한 모든 도메인 목록을 가져오려면, **Fetch DN(DN 가져오기)**을 클릭하고 드롭다운 목록에서 적절한 기본 고유 이름을 선택합니다.

단계 8 LDAP 디렉터리에 액세스 인증을 위해 사용하고자 하는 고유한 **User Name(사용자 이름)** 및 **Password(비밀번호)**를 지정합니다. 비밀번호를 확인합니다.

단계 9 **Encryption(암호화)** 방법을 선택합니다. 암호화를 사용할 경우, **SSL Certificate(SSL 인증서)**를 추가할 수 있습니다.

인증서의 호스트 이름은 **반드시** 4단계에서 지정한 LDAP 서버의 호스트 이름과 일치해야 합니다.

단계 10 응답하지 않는 기본 LDAP 서버에 대한 접속 시도가 백업 연결에 롤오버된 후에 **Timeout(시간 제한)**(초)을 지정합니다.

단계 11 선택적으로, 개체에 대한 사용자 인식 설정을 지정하기 전에, **Test(테스트)**를 클릭하여 연결을 테스트합니다.

단계 12 선택적으로, **User/Group Access Control Parameters(사용자/그룹 액세스 제어 매개 변수)**를 활성화하여 액세스 제어에서 사용하는 사용자를 지정합니다.

단계 13 **Fetch Groups(그룹 가져오기)**를 클릭하여 사용자가 제공한 LDAP 매개 변수를 사용하는 사용 가능한 그룹 목록을 채웁니다.

단계 14 그룹을 포함하거나 제외하기 위해 왼쪽 및 오른쪽 화살표 단추를 사용하여 액세스 제어에서 사용할 사용자를 지정합니다.

그룹을 자동으로 포함시키는 것은 해당 그룹의 모든 구성원을 포함하는 것이며, 모든 하위 그룹의 구성원도 포함됩니다. 그러나, 액세스 제어 규칙의 하위 그룹을 사용하려는 경우, 명시적으로 하위 그룹을 포함해야 합니다. 그룹을 제외하는 것은 해당 사용자가 포함된 그룹의 구성원이라고 해도 해당 그룹의 구성원 모두를 제외하는 것입니다.

단계 15 특정 **User Exclusions(사용자 제외)**를 지정합니다.

사용자를 제외하면 해당 사용자를 조건으로 사용하여 액세스 제어 규칙을 작성할 수 없습니다. 사용자가 여러 명인 경우 쉼표로 구분하십시오. 또한 이 필드에서 와일드카드 문자로 별표(*)를 사용할 수 있습니다.

단계 16 새로운 사용자 및 그룹 정보를 얻기 위해 얼마나 자주 LDAP 서버 쿼리를 원하는지 지정합니다.

기본적으로, ASA FirePOWER 모듈은 하루에 한 번 자정에 서버를 쿼리합니다.

- **Start At(시작 지점)** 드롭다운 목록을 사용하여 언제 쿼리 발생을 원하는지 지정합니다. **0**은 자정을, **1**은 오전 1시를 나타냅니다.
- **Update Interval(업데이트 간격)** 드롭다운 목록을 사용하여 얼마나 자주 서버 쿼리를 원하는지 시간을 지정합니다.

단계 17 **Save(저장)**를 클릭합니다.

사용자 및 그룹 액세스 제어 매개 변수를 추가하거나 변경한 경우, 변경 수행을 원하는지 여부를 확인합니다. 개체는 저장되고 Users Policy(사용자 정책) 페이지가 다시 표시됩니다.

단계 18 방금 생성한 연결 옆에 있는 슬라이더를 클릭하여 연결을 활성화합니다.

연결을 활성화하여 연결에 사용자 및 그룹 액세스 제어 매개 변수가 있는 경우, 사용자 및 그룹 정보를 얻기 위해 즉시 LDAP 서버를 쿼리하기를 원하는지 여부를 선택합니다. 즉시 LDAP 서버 쿼리를 원하지 않는 경우, 쿼리는 예약된 시간에 발생한다는 점을 참고하십시오. 작업 큐(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 쿼리 진행 상황을 모니터링할 수 있습니다.

온디맨드 사용자 제어 매개 변수 업데이트

라이센스: 제어

LDAP 연결의 사용자 및 그룹 액세스 제어 매개 변수를 변경하는 경우, 또는 LDAP 서버의 사용자 또는 그룹을 변경하고 사용자 제어를 위해 변경 사항을 바로 사용할 수 있기를 원하는 경우 ASA FirePOWER 모듈이 Active Directory 서버에서 온 디맨드 사용자 데이터 검색을 강제로 수행하도록 할 수 있습니다.

LDAP 연결에서 액세스 제어 매개 변수가 너무 광범위한 경우, ASA FirePOWER 모듈은 사용자에 관해 가능한 많은 정보를 얻고, 작업 큐에서 검색에 실패한 사용자 수를 보고합니다.

온디맨드 사용자 데이터 검색을 수행하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Users(사용자)**를 선택합니다.

Users Policy(사용자 정책) 페이지가 나타납니다.

단계 2 LDAP 서버 쿼리에 사용하려는 LDAP 연결 옆의 다운로드 아이콘( )을 클릭합니다.

쿼리가 시작됩니다. 작업 큐(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 진행 상황을 모니터링할 수 있습니다.

LDAP 서버와의 통신 일시 중지

라이센스: 기능에 따라 다름

활성화된 LDAP 연결만이 ASA FirePOWER 모듈이 LDAP 서버를 쿼리하도록 허용합니다. 쿼리를 중지하려면, LDAP 연결을 삭제하기 보다는 일시적으로 비활성화할 수 있습니다.

액세스 제어에 사용되는 LDAP 연결을 재활성화하는 경우, ASA FirePOWER 모듈이 업데이트된 사용자 및 그룹 정보에 대해 즉시 서버를 쿼리하도록 강제할 수도 있고, 또는 먼저 일정이 잡힌 쿼리가 발생할 때까지 기다릴 수도 있습니다.

LDAP 연결을 비활성화하거나 재활성화하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Users(사용자)**를 선택합니다.

Users Policy(사용자 정책) 페이지가 나타납니다.

단계 2 방금 생성한 연결 옆에 있는 슬라이더를 클릭하여 연결을 일시 중지하거나 재활성화합니다.

연결을 다시 활성화하여 연결에 사용자 및 그룹 액세스 제어 매개 변수가 있는 경우, 사용자 및 그룹 정보를 얻기 위해 즉시 LDAP 서버를 쿼리하기를 원하는지 여부를 선택합니다. 즉시 LDAP 서버 쿼리를 원하지 않는 경우, 쿼리는 예약된 시간에 발생합니다. 작업 큐(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 쿼리 진행 상황을 모니터링할 수 있습니다.

Active Directory 로그인을 보고하도록 사용자 에이전트 사용

라이센스: 제어

Microsoft Windows 컴퓨터에 배포된 사용자 에이전트는 Microsoft Active Directory 서버를 모니터링할 수 있으며, 다음으로 사용자 조직 내 LDAP 사용자가 호스트에 로그인하거나 로그아웃할 때 ASA FirePOWER 모듈에 알릴 수 있으며, 또는 다른 이유로 Active Directory 자격 증명을 인증할 수 있습니다. 예를 들어, 사용자 조직은 중앙 집중식 인증을 위해 Active Directory를 이용하는 애플리케이션 또는 서비스를 사용할 수 있습니다.

에이전트가 보고한 이 정보는 사용자 제어의 근간이 됩니다. 사용자 조건과 함께 액세스 제어 규칙에 일치하는 트래픽의 경우, 모니터링된 세션의 소스 또는 대상 호스트의 IP 주소는 로그인된 액세스 제어 사용자와 연결되어야 합니다. 개별 사용자에 기반한 트래픽이나 해당 사용자들이 속한 그룹은 제어 가능합니다.

참고 사용자 제어를 수행하려는 경우 **반드시** 사용자 에이전트를 설치하고 사용해야 합니다. 그러나, 사용자 에이전트는 Active Directory 인증에 관련된 사용자 활동만 보고합니다. 사용자 인식을 통해 에이전트가 보고한 사용자 활동뿐만 아니라 허용된 네트워크 트래픽에서 탐지된 추가 활동을 살펴볼 수 있습니다.

사용자 인식 또는 제어를 위해 사용자 에이전트와 더불어 LDAP 사용자 인증 레코드를 검색하려면, 먼저 각 ASA FirePOWER 모듈을 구성하여 에이전트의 연결을 허용합니다. 고가용성 배포에서는 기본 ASA FirePOWER 모듈 및 2차 ASA FirePOWER 모듈 둘 다에 대해 에이전트 통신을 활성화합니다. ASA FirePOWER 모듈에서 사용자 에이전트 통신을 활성화한 후, Windows 컴퓨터에 에이전트를 설치할 수 있습니다.

마지막으로, 사용자 에이전트를 구성하여 Microsoft Active Directory 서버로부터 데이터를 수신하고 ASA FirePOWER 모듈에 정보를 보고합니다. 또한 에이전트를 구성하여 보고서에서 특정 사용자 이름 및 IP 주소를 제외할 수 있고, 로컬 이벤트 로그 또는 Windows 애플리케이션 로그에 상태 메시지를 로깅합니다.

사용자 에이전트에 연결하기 위해 ASA FirePOWER 모듈을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Users(사용자)**를 선택합니다.

Users Policy(사용자 정책) 페이지가 나타납니다.

단계 2 **Add User Agent(사용자 에이전트 추가)**를 클릭합니다.

Add User Agent(사용자 에이전트 추가) 팝업 창이 열립니다.

단계 3 에이전트의 **Name(이름)**을 입력합니다.

단계 4 에이전트 설치를 계획하고 있는 컴퓨터의 **Hostname or Address(호스트 이름 또는 주소)**를 입력합니다. **반드시** IPv4 주소를 사용해야 합니다. IPv6 주소를 사용하여 사용자 에이전트에 연결하기 위해 ASA FirePOWER 모듈을 구성할 수 없습니다.

단계 5 **Add User Agent(사용자 에이전트 추가)**를 클릭합니다.

ASA FirePOWER 모듈은 이제 사용자가 지정한 컴퓨터에서 사용자 에이전트에 연결합니다. 연결을 삭제하려면, 삭제 아이콘( )을 클릭하고 삭제할지 여부를 확인합니다.

단계 6 지정한 컴퓨터에 사용자 에이전트를 설치합니다. 사용자 에이전트를 구성하여 Microsoft Active Directory 서버로부터 데이터를 수신하고 ASA FirePOWER 모듈에 정보를 보고합니다.

세부적인 최신 정보는 *User Agent Configuration Guide(사용자 에이전트 구성 설명서)*를 참고하십시오. 사용자 에이전트를 구성할 때 ASA FirePOWER 모듈이 방어 센터와 동일한 역할을 한다는 점을 참고하십시오. 예를 들면, ASA FirePOWER 모듈에 연결을 구성할 수 있으며, 방어 센터에 연결을 생성함으로써 수행할 수 있습니다. ASA FirePOWER 모듈에 정보를 제공할 수 있으며 이는 방어 센터에서와 동일하게 할 수 있습니다.

침입 정책 및 파일 정책을 사용하여 트래픽 제어

침입 정책 및 파일 정책은 의 일부로서, 그리고 트래픽이 원하는 대상에 도달하도록 허용하기 전에 최종 방어선으로서의 역할을 함께 수행합니다.

- **침입 정책**은 시스템의 침입 방지 기능을 제어합니다(11-1페이지의 네트워크 분석 및 침입 정책의 이해 참고).
- **파일 정책**은 시스템의 네트워크 기반 파일 제어 및 AMP(Advanced Malware Protection) 기능을 제어합니다(24-4페이지의 파일 정책 이해 및 생성 참고).

보안 인텔리전스 기반의 트래픽 필터링(차단 목록 추가) 그리고 트래픽 해독 및 전처리는 네트워크 트래픽에 대한 침입, 금지 파일, 그리고 악성코드 점검이 이루어지기 **전에** 발생합니다. 액세스 제어 규칙 및 액세스 제어 기본 작업은 침입 정책 및 파일 정책으로 어떤 트래픽을 검사할지를 결정합니다.

침입 또는 파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽이 통과하기 전에 침입 정책이나 파일 정책 또는 두 정책을 모두 사용하여 우선 트래픽을 검사하도록 할 수 있습니다.

침입 방지 및 AMP를 사용하려면 다음 표에 설명된 대로 특정 라이센스 기능을 활성화해야 합니다.

표 10-1 침입 및 파일 검사를 위한 라이센스 요건

기능	설명	라이센스
침입 방지	침입 및 익스플로잇을 탐지하고 선택적으로 차단	보호
파일 제어	파일 유형의 전송을 탐지하고 선택적으로 차단	보호
AMP(Advanced Malware Protection)	악성코드의 전송을 탐지,추적하고 선택적으로 차단	악성코드

침입, 금지된 파일, 악성코드에 대해 트래픽을 검사하는 방법에 대한 자세한 내용은 다음을 참고하십시오.

- 10-2페이지의 침입 및 악성코드에 대해 허용된 트래픽 검사
- 10-6페이지의 침입 방지 성능 조정
- 10-16페이지의 파일 및 악성코드 탐지 성능 및 저장 조정

침입 및 악성코드에 대해 허용된 트래픽 검사

라이센스: 보호 또는 악성코드

침입 정책 및 파일 정책은 트래픽이 원하는 대상에 도달할 수 있게 되기 전에 최종 방어선으로서 시스템의 침입, 파일 제어, AMP 기능을 제어합니다. 보안 인텔리전스 기반의 트래픽 필터링, 디코딩 및 전처리, 액세스 제어 규칙 선택은 침입 및 파일 검사 **전에** 수행됩니다.

침입 또는 파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽이 통과하기 전에 침입 정책이나 파일 정책 또는 두 정책을 모두 사용하여 우선 트래픽을 검사하도록 할 수 있습니다. 액세스 제어 규칙 조건은 간단할 수도 있고 복잡할 수도 있습니다. 보안 영역, 네트워크 또는 지리적 위치, 포트,애플리케이션, 요청된 URL 및 사용자로 트래픽을 제어할 수 있습니다.

시스템은 사용자가 지정하는 순서대로 액세스 제어 규칙에 트래픽을 일치시킵니다. 대부분의 경우, 시스템은 *모든* 규칙의 조건이 트래픽과 일치하는 *첫 번째* 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 액세스 제어 규칙의 *작업*은 시스템에서 일치하는 트래픽을 처리하는 방법을 결정합니다. 일치하는 트래픽을 모니터링, 신뢰, 차단, 허용(추가 검사 실행 또는 실행 안 함)할 수 있습니다(6-6페이지의 규칙 작업을 사용하여 트래픽 관리 및 검사 결정 참고).

Interactive Block(인터랙티브 차단) 규칙은 Allow(허용) 규칙과 동일한 검사 옵션이 있습니다. 이를 사용하면 사용자가 경고 페이지를 클릭하여 차단된 웹 페이지를 우회할 경우 악의적인 콘텐츠에 대해 트래픽을 검사할 수 있습니다. 자세한 내용은 6-8페이지의 인터랙티브 차단 작업: 사용자가 웹 사이트 차단을 우회하도록 허용을 참고하십시오.

내 어느 비모니터링 액세스 제어 규칙과도 일치하지 않는 트래픽은 기본 작업에 의해 처리됩니다. 시스템은 기본 작업에서 허용하는 트래픽에 대해 침입 여부를 검사할 수 있으나, 금지된 파일 또는 악성코드 여부는 검사할 수 없습니다. 파일 정책을 액세스 제어 기본 작업과 연결할 수 **없습니다**.

참고 액세스 제어 정책으로 연결을 분석할 경우, 시스템에서는 어떤 액세스 제어 규칙(있는 경우)으로 트래픽을 처리할 것인지 결정하기 전에 해당 연결의 처음 몇 가지 패킷을 처리하여, **통과되도록 허용**해야 합니다. 그러나 이러한 패킷은 검사하지 않은 대상에는 도달할 수 없으며, 기본 침입 정책이라고 하는 침입 정책을 사용하여 이러한 패킷을 검사하고 침입 이벤트를 생성할 수 있습니다. 자세한 내용은 13-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을 참고하십시오.

위의 시나리오에 대한 자세한 내용 및 파일과 침입 정책을 액세스 제어 규칙 및 액세스 제어 기본 작업과 연결하는 방법에 대한 지침을 보려면 다음을 참고하십시오.

- 10-2페이지의 파일 및 침입 검사 순서 이해
- 10-3페이지의 액세스 제어 규칙을 구성하여 AMP 또는 파일 제어 수행
- 10-4페이지의 침입 방지 수행을 위한 액세스 제어 규칙 구성
- 4-4페이지의 네트워크 트래픽에 대한 기본 처리와 검사 설정

파일 및 침입 검사 순서 이해

라이센스: 보호 또는 악성코드

참고 트래픽이 침입 방지 기본 작업에 의해 허용된 경우 침입은 검사할 수 있지만, 금지된 파일 또는 악성코드는 검사할 수 없습니다. 파일 정책을 액세스 제어 기본 작업과 연결할 수 **없습니다**.

동일한 규칙에서 파일 및 침입 검사를 모두 수행할 필요는 없습니다. Allow or Interactive Block(허용 또는 인터랙티브 차단) 규칙과 일치하는 연결의 경우:

- 파일 정책이 없는 경우, 트래픽 흐름은 침입 정책에 의해 결정됨
- 침입 정책이 없는 경우, 트래픽 흐름은 파일 정책에 의해 결정됨

팁 시스템은 신뢰할 수 있는 트래픽에는 검사를 수행하지 않습니다.

액세스 제어 규칙으로 처리되는 단일한 연결의 경우, 침입 검사 전에 파일 검사가 이루어집니다. 즉, 시스템에서는 파일 정책 또는 침입에 의해 차단된 파일은 검사하지 않습니다. 파일 검사 내에서 유형을 기준으로 한 간단한 차단은 악성코드 검사 및 차단보다 우선합니다.

참고 세션에서 파일이 탐지되고 차단될 때까지, 세션의 패킷은 침입 검사 대상이 될 수 있습니다.

예를 들어, 액세스 제어 규칙에 정의된 대로 특정 네트워크 트래픽을 일반적으로 허용하고자 하는 시나리오를 가정해보겠습니다. 그러나 일종의 예방 조치로서 실행 파일의 다운로드를 차단하고, 다운로드된 PDF의 악성코드 여부를 검사하고 검색된 모든 인스턴스를 차단하며, 트래픽에 침입 검사를 수행하고자 합니다.

일시적으로 허용하고자 하는 트래픽의 특성과 일치하는 규칙으로 액세스 제어 정책을 생성하고 이를 침입 정책과 파일 정책에 모두 연결합니다. 파일 정책은 모든 실행 파일의 다운로드를 차단하며, 검사를 수행하고 악성코드가 포함된 PDF를 차단합니다.

- 우선 시스템에서는 파일 정책에 지정된 것과 일치하는 간단한 유형을 기준으로 모든 실행 파일의 다운로드를 차단합니다. 해당 파일은 즉시 차단되므로, 이러한 파일은 악성코드 클라우드 조회 또는 침입 검사 대상에서 제외됩니다.
- 그다음, 시스템에서는 네트워크의 호스트에 다운로드된 PDF에 악성코드 클라우드 조회를 수행합니다. 악성코드 파일 속성이 포함된 모든 PDF 파일은 차단되며, 침입 검사 대상에서 제외됩니다.
- 마지막으로, 시스템에서는 액세스 제어 규칙과 연결된 침입 정책을 사용하여 모든 나머지 트래픽을 검사하며 여기에는 파일 정책으로 차단되지 않은 파일이 포함됩니다.

액세스 제어 규칙을 구성하여 AMP 또는 파일 제어 수행

라이센스: 보호 또는 악성코드

액세스 제어 정책에는 파일 정책과 연결된 여러 액세스 제어 규칙이 포함될 수 있습니다. 모든 Allow or Interactive Block (허용 또는 인터랙티브 차단) 액세스 제어 규칙에 대해 파일 검사를 구성할 수 있습니다. 이를 통해 트래픽이 최종 대상에 도달하기 전에 네트워크 상에 있는 다양한 유형의 트래픽에 대해 다양한 파일 및 악성코드 검사 프로파일과 맞춰볼 수 있습니다.

시스템이 파일 정책의 설정에 따라 (악성코드 등) 금지된 파일을 탐지하면, 자동으로 에 이벤트가 로깅됩니다. 파일 또는 악성코드 이벤트를 로깅하지 않으려는 경우, 액세스 제어 규칙마다 이러한 로깅을 비활성화할 수 있습니다. 액세스 제어 규칙과 파일 정책을 결합한 후에는, 액세스 제어 규칙 편집기의 Logging(로깅) 탭에서 **Log Files(로그 파일)** 확인 상자을 비워두십시오. 자세한 내용은 25-7페이지의 허용된 연결에 대한 파일 및 악성코드 이벤트 로깅 비활성화를 참고하십시오.

시스템은 또한 액세스 제어 규칙 호출의 로깅 구성에 관계없이 결합된 연결의 말단을 로깅합니다(25-3페이지의 파일 및 악성 프로그램 이벤트와 결합된 연결(자동) 참고).

파일 정책을 액세스 제어 규칙과 연결하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**을 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 액세스 제어 규칙을 사용하여 AMP 또는 파일 제어를 구성하려면 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

단계 3 새 규칙을 생성하거나 기존 규칙을 수정합니다(6-2페이지의 액세스 제어 규칙 생성 및 수정 참고).

액세스 제어 규칙 편집기가 나타납니다.

단계 4 규칙 작업이 **Allow(허용)**, **Interactive Block(인터랙티브 차단)** 또는 **Interactive Block with reset(인터랙티브 차단 후 초기화)**로 설정되어 있는지 확인합니다.

단계 5 Inspection(검사) 탭을 선택합니다.

Inspection(검사) 탭이 나타납니다.

단계 6 액세스 제어 규칙에 일치하는 트래픽 검증을 위해서는 **File Policy(파일 정책)**을, 트래픽에 일치하는 파일 검사를 비활성화하기 위해서는 **None(없음)**을 선택합니다.

사용자는 이때 표시되는 수정 아이콘( )을 클릭하여 정책을 수정할 수 있습니다(24-9페이지의 파일 정책 생성 참고).

단계 7 **Add(추가)**를 클릭하여 규칙을 저장하십시오.

사용자의 규칙이 저장됩니다. 변경 사항을 반영하려면 액세스 제어 정책을 저장하고 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

침입 방지 수행을 위한 액세스 제어 규칙 구성

라이센스: 보호

액세스 제어 정책에는 침입 정책과 관련된 여러 액세스 제어 규칙이 포함될 수 있습니다. 모든 Allow or Interactive Block(허용 또는 인터랙티브 차단) 액세스 제어 규칙에 대해 침입 검사를 구성할 수 있습니다. 이를 통해 트래픽이 최종 대상에 도달하기 전에 네트워크 상에 있는 다양한 유형의 트래픽에 대해 다양한 침입 검사 프로파일과 맞춰볼 수 있습니다.

시스템이 트래픽 평가를 위해 침입 정책을 사용할 때마다, 결합된 *변수 집합*을 사용합니다. 집합의 변수는 소스 및 대상 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 또한 침입 정책 내 변수를 사용하여 규칙 삭제 및 동적 규칙 상태의 IP 주소를 나타낼 수 있습니다.

팁 시스템에서 제공한 침입 정책을 사용하고 있는 경우에도, Cisco는 사용자가 자신의 네트워크 환경을 정확하게 반영할 수 있도록 시스템의 침입 변수를 구성할 것을 **강력히** 권장합니다. 최소한, 기본값 집합의 기본값 변수라도 수정하시기 바랍니다(2-15페이지의 미리 정의된 기본 변수 최적화 참고).

다양한 침입 정책-변수 집합 쌍을 Allow or Interactive Block(허용 또는 인터랙티브 차단) 규칙 (및 기본 작업)과 결합할 수 있다 해도, 대상 디바이스가 구성한 대로 검사를 수행할 수 있는 리소스가 충분하지 않은 경우 액세스 제어 정책을 적용할 수 없습니다. 자세한 내용은 4-15페이지의 성능 개선을 위한 규칙 간소화를 참고하십시오.

시스템이 제공하는 침입 정책 및 사용자 정의 침입 정책의 이해

Cisco는 ASA FirePOWER 모듈과 더불어 여러 침입 정책을 제공합니다. 시스템이 제공하는 침입 정책을 사용하여 Cisco VRT(취약성 연구단)의 경험을 활용할 수 있습니다. VRT는 이 정책에 대해, 침입 및 전처리 연결 규칙 상태를 설정할 뿐만 아니라, 고급 설정에 대한 초기 구성을 제공합니다. 사용자는 시스템이 제공하는 정책을 있는 그대로 사용할 수도 있고, 이를 맞춤형 정책을 위한 기반으로 사용할 수도 있습니다. 맞춤형 정책을 구축하면 사용자 환경에서 시스템의 성능을 개선할 수 있으며, 사용자 네트워크에서 발생하는 악의적인 트래픽 및 정책 위반을 집중적으로 확인할 수 있습니다.

사용자가 생성하는 맞춤형 정책 이외에도 시스템은 두 개의 맞춤형 정책인, Initial Inline Policy(초기 인라인 정책)과 Initial Passive Policy(초기 수동 정책)를 제공합니다. 이 두 침입 정책은 자체 정책을 토대로 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 정책을 사용합니다. 이 둘 사이의 유일한 차이는 **Drop When Inline(인라인 시 삭제)** 설정인데, 인라인 정책에서는 삭제 작업을 활성화하고 수동 정책에서는 비활성화하는 것입니다. 자세한 내용은 11-6페이지의 시스템 제공 정책과 사용자 지정 정책 비교를 참고하십시오.

연결 및 침입 이벤트 로깅

액세스 제어 규칙에 의해 호출된 침입 정책이 침입을 탐지할 경우, 침입 정책은 침입 이벤트를 생성합니다. 시스템은 또한 액세스 제어 규칙의 로깅 구성에 관계없이 침입이 발생한 연결의 종료를 로깅합니다(25-2페이지의 침입과 결합된 연결(자동) 참고).

침입 정책을 액세스 제어 규칙과 결합하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**을 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 액세스 제어 규칙을 사용하여 침입 검사를 구성하려면 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

단계 3 새 규칙을 생성하거나 기존 규칙을 수정합니다(6-2페이지의 액세스 제어 규칙 생성 및 수정 참고).

액세스 제어 규칙 편집기가 나타납니다.

단계 4 규칙 작업이 **Allow(허용)**, **Interactive Block(인터랙티브 차단)** 또는 **Interactive Block with reset(인터랙티브 차단 후 초기화)**로 설정되어 있는지 확인합니다.

단계 5 Inspection(검사) 탭을 선택합니다.

Inspection(검사) 탭이 나타납니다.

단계 6 시스템이 제공하는 정책 또는 사용자 정의**Intrusion Policy(침입 정책)**를 선택하거나 **None(없음)**을 선택하여 액세스 제어 규칙과 일치하는 트래픽에 대한 침입 검사를 비활성화합니다.

사용자 정의 침입 정책을 선택하는 경우, 사용자는 이때 표시되는 수정 아이콘()을 클릭하여 정책을 수정할 수 있습니다(19-4페이지의 침입 정책 수정 참고).

주의 **반드시** `Experimental Policy 1(실험 정책 1)`을 Cisco 관계자의 지시 없이는 사용하지 마십시오. Cisco는 이 정책을 테스트용으로 사용합니다.

단계 7 선택적으로, 침입 정책과 결합된 **Variable Set(변수 집합)**를 변경할 수 있습니다.

사용자는 이때 표시되는 수정 아이콘()을 클릭하여 변수 집합을 수정할 수 있습니다(2-14페이지의 변수 집합 작업 참고).

단계 8 **Save(저장)**를 클릭하여 규칙을 저장하십시오.

사용자의 규칙이 저장됩니다. 변경 사항을 반영하려면 액세스 제어 정책을 저장하고 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

침입 방지 성능 조정

라이센스: 보호

Cisco는 시스템이 시도된 침입의 트래픽을 분석할 때 시스템의 성능을 향상시키는 기능을 제공합니다. 사용자는 액세스 제어 정책을 기반으로 한 성능 설정을 구성하고, 해당 상위 액세스 제어 정책에 의해 호출된 모든 침입 정책에 적용합니다.

자세한 내용은 다음을 참고하십시오.

- 10-6페이지의 침입에 대한 패턴 일치 제한은 사용자가 이벤트 큐에 허용된 패킷 수를 지정할 수 있는 방법과 대형 스트림으로 재구축되는 패킷에 대한 검사를 활성화 또는 비활성화하는 방법을 설명합니다.
- 10-7페이지의 침입 규칙을 위한 정규식 재정의는 사용자가 기본값 일치 및 PCRE(펄 호환 정규 표현식)의 반복 한계를 재정의할 수 있는 방법을 설명합니다.
- 10-8페이지의 패킷당 생성되는 침입 이벤트 제한은 사용자가 규칙 처리 이벤트 큐 설정을 구성하는 방법을 설명합니다.
- 10-9페이지의 패킷 및 침입 규칙 레이턴시 임계값 구성은 사용자가 패킷 및 규칙 레이턴시 임계값으로 보안과 디바이스 레이턴시 유지 필요성 사이의 균형을 적절한 수준으로 유지할 수 있는 방법을 설명합니다.
- 10-15페이지의 침입 성능 통계 로깅 구성은 사용자가 기본 성능 모니터링 및 매개 변수 보고를 구성하는 방법을 설명합니다.

침입에 대한 패턴 일치 제한

라이센스: 보호

이벤트 큐에서 허용되는 패킷 수를 지정할 수 있습니다. 또한, 스트림 리어셈블리 전후에, 대형 스트림으로 재구축되는 패킷에 대한 검사를 활성화 또는 비활성화할 수 있습니다.

이벤트 큐 설정을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**을 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 Advanced(고급) 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Performance Settings(성능 설정)** 옆에 있음)을 클릭한 후 나타나는 팝업 창에서 **Pattern Matching Limits(패턴 일치 제한)** 탭을 선택합니다.

단계 5 사용자는 다음 옵션을 변경할 수 있습니다.

- **Maximum Pattern States to Analyze Per Packet(패킷 당 분석할 최대 패턴 상태)** 필드에 대기할 이벤트의 최대 수 값을 입력합니다.
- 스트림 리어셈블리 전후에 대형 데이터 스트림으로 재구축되는 패킷을 검사하려면, **Disable Content Checks on Traffic Subject to Future Reassembly(향후 리어셈블리 대상이 되는 트래픽에 대해 콘텐츠 확인 비활성화)**를 선택합니다. 리어셈블리 전후의 검사에는 추가 프로세싱 오버헤드가 필요하므로 성능이 저하될 수 있습니다.
- 스트림 리어셈블리 전후에 대형 데이터 스트림으로 재구축되는 패킷을 비활성화하려면 **Disable Content Checks on Traffic Subject to Future Reassembly(향후 리어셈블리 대상이 되는 트래픽에 대해 콘텐츠 확인 비활성화)**를 지웁니다. 검사 비활성화로 스트림 삽입 검사를 위한 프로세싱 오버헤드를 줄이고 성능을 개선할 수 있습니다.

단계 6 **OK(확인)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 저장하고 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

침입 규칙을 위한 정규식 재정의

라이센스: 보호

사용자는 패킷 페이로드 콘텐츠 검토를 위해 침입 규칙에서 사용되는 PCRE에서 기본 일치 값과 반복 한계를 무시할 수 있습니다. 23-35페이지의 PCRE를 사용한 콘텐츠 검색에서 침입 규칙 내 `pcre` 키워드 사용에 대한 자세한 내용을 참고하십시오. 기본 제한값은 최소 수준의 성능을 보장합니다. 이러한 제한을 재정의하면 보안을 강화할 수 있지만, 비효율 정규식에 대한 패킷 평가를 허용함으로써 성능에 중대한 영향을 미칠 수 있습니다.

주의 손상 패턴의 영향에 대한 지식이 있는 숙련된 침입 규칙 작성가가 아닌 이상 기본 PCRE 제한값을 재정의하지 마십시오.

다음 표에서는 사용자가 기본 제한값을 재정의하여 구성할 수 있는 옵션을 설명합니다.

표 10-2 정규식 제약 조건 옵션

옵션	설명
일치 제한 상태	**Match Limit(일치 제한)** 재정의 여부를 지정합니다. 다음 옵션을 이용할 수 있습니다. • **Match Limit(일치 제한)**에 대해 구성된 값을 사용하려면 **Default(기본값)**를 선택합니다. • 무제한 시도를 허용하려면 **Unlimited(무제한)**를 선택합니다. • **Match Limit(일치 제한)**를 위해 1 이상의 제한값을 지정하거나, PCRE 일치 평가를 완전히 비활성화하는 0을 지정하려면 **Custom(사용자 정의)**을 선택합니다.
일치 제한	PCRE 정규식에 정의된 패턴에 일치시키려는 시도의 횟수를 지정합니다.

표 10-2 정규식 제약 조건 옵션 (계속)

옵션	설명
일치 반복 제한 상태	**Match Recursion Limit(일치 반복 제한)** 재정의 여부를 지정합니다. 다음 옵션을 이용할 수 있습니다. • **Match Recursion Limit(일치 반복 제한)**에 대해 구성된 값을 사용하려면 **Default(기본값)**를 선택합니다. • 무제한 반복을 허용하려면 **Unlimited(무제한)**를 선택합니다. • **Match Recursion Limit(일치 반복 제한)**에 대해 1 이상의 제한값을 지정하거나, PCRE 반복을 완전히 비활성화하는 0을 지정하려면 **Custom(사용자 정의)**을 선택합니다. **Match Recursion Limit(일치 반복 제한)**가 작동하려면 반드시 **Match Limit(일치 제한)**보다 작아야 함을 참고하시기 바랍니다.
일치 반복 제한	패킷 페이로드에 대한 PCRE 정규식을 평가할 때 반복 수를 지정합니다.

PCRE 재정의를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**을 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 Advanced(고급) 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘()(**Performance Settings(성능 설정)** 옆에 있음)을 클릭한 후, 표시되는 팝업 창에서 Regular Expression Limits(일반 표현 한계) 탭을 선택합니다.

단계 5 정규식 제약 조건 옵션에서 모든 옵션을 변경할 수 있습니다.

단계 6 **OK(확인)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 저장하고 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

패킷당 생성되는 침입 이벤트 제한

라이센스: 보호

규칙 엔진이 규칙에 대한 트래픽을 평가할 때, 주어진 패킷 또는 이벤트 큐의 패킷 스트림에 대해 생성된 이벤트를 배치하고, 큐의 상위 이벤트를 사용자 인터페이스에 보고합니다. 여러 이벤트가 생성될 때 규칙 엔진이 패킷당 하나의 이벤트 또는 패킷 스트림보다 더 많이 로깅하도록 할 수 있습니다. 이 이벤트를 로깅하면 보고된 이벤트를 넘어서는 정보를 수집할 수 있습니다. 이 옵션을 설정할 때, 큐에 얼마나 많은 이벤트가 지정될 수 있는지, 그리고 얼마나 많은 이벤트가 로깅되는지를 지정하고, 해당 큐 내 이벤트 순서를 결정하기 위한 기준을 선택할 수 있습니다.

다음 표는 패킷 또는 스트림 당 얼마나 많은 이벤트를 로깅할지 결정하기 위해 사용자가 구성할 수 있는 옵션을 설명합니다.

표 10-3 침입 이벤트 로깅 제한 옵션

옵션	설명
패킷 당 저장된 최대 이벤트	주어진 패킷 또는 패킷 스트림에 대해 저장될 수 있는 최대 이벤트 수
패킷 당 로깅된 최대 이벤트	주어진 패킷 또는 패킷 스트림에 대해 로깅될 수 있는 최대 이벤트 수. 이는 **Maximum Events Stored Per Packet(패킷 당 저장된 최대 이벤트)** 값을 초과할 수 없습니다.
이벤트 로깅 우선 순위 지정 기준	이벤트 큐 내 이벤트 순서를 결정하는 데 사용되는 값. 최고 순위 이벤트는 사용자 인터페이스를 통해 보고됩니다. 사용자는 다음에서 선택할 수 있습니다. • `priority`. 이벤트 우선 순위에 따라 해당 큐에서 이벤트 순서를 결정하는 것 • `content_length`. 가장 긴 것으로 확인된 콘텐츠 일치에 따라 이벤트 순서를 결정하는 것. 이벤트가 콘텐츠 길이에 의해 순서가 정해질 때, 규칙 이벤트는 항상 디코더 및 전처리기 이벤트에 우선합니다.

패킷 또는 스트림 당 로깅되는 이벤트 수를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**을 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 Advanced(고급) 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Performance Settings(성능 설정)** 옆에 있음)을 클릭한 후 표시되는 팝업 창에서 **Intrusion Event Logging Limits(침입 이벤트 로깅 제한)** 탭을 선택합니다.

단계 5 침입 이벤트 로깅 제한 옵션에서 모든 옵션을 변경할 수 있습니다.

단계 6 **OK(확인)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 저장하고 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

패킷 및 침입 규칙 레이턴시 임계값 구성

라이센스: 보호

사용자는 패킷 및 규칙 레이턴시 임계값으로 보안과 디바이스 레이턴시 유지 필요성 사이의 균형을 적절한 수준으로 유지할 수 있는 방법을 설명합니다. 자세한 내용은 다음을 참고하십시오.

- 10-10페이지의 패킷 레이턴시 임계값의 이해
- 10-11페이지의 패킷 레이턴시 임계값 구성
- 10-12페이지의 규칙 레이턴시 임계값의 이해
- 10-14페이지의 규칙 레이턴시 임계값 구성

패킷 레이턴시 임계값의 이해

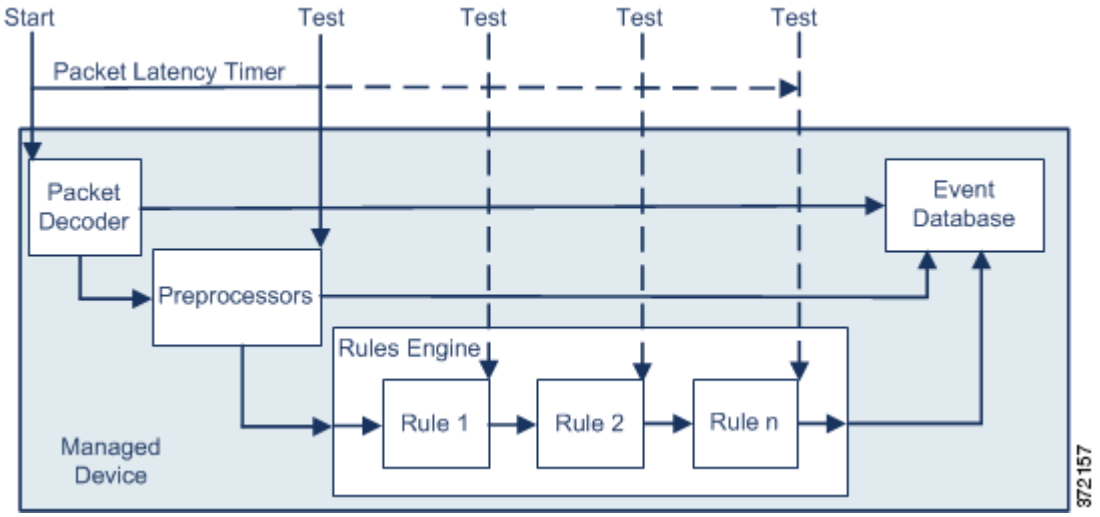
라이센스: 보호

패킷 레이턴시 임계값을 활성화하면 보안과 레이턴시 유지 필요성 사이의 균형을 적절한 수준으로 유지할 수 있습니다. 패킷 레이턴시 임계값은 처리 시간이 구성 가능한 임계값을 초과하는 경우 적용 가능한 디코더, 전처리기 및 규칙에 의해 패킷을 처리하는 데 드는 총 소요 시간을 측정합니다.

패킷 레이턴시 임계값은 처리 시간뿐만 아니라 소요된 시간까지 측정하여 패킷을 처리하는 규칙에 필요한 실제 시간을 더욱 정확하게 반영합니다. 그러나 레이턴시 임계값은 엄격한 타이밍을 시행하지 않는 소프트웨어 기반의 레이턴시 구현입니다.

레이턴시 임계값에서 파생된 레이턴시 이점과 성능의 반대 급부는 검사하지 않은 패킷에 공격이 포함되어 있을 수 있다는 점입니다. 그러나, 패킷 레이턴시 임계값은 사용자가 보안과 연결성 사이의 균형을 잡는 데 사용할 수 있는 도구를 제공합니다.

디코더가 프로세스를 시작할 때 각 패킷의 타이머가 시작됩니다. 타이밍은 패킷의 모든 처리가 종료되거나, 처리 시간이 타이밍 테스트 지점의 임계값을 초과할 때까지 계속됩니다.



위 그림에 표시된 것처럼, 패킷 레이턴시 타이밍은 다음과 같은 테스트 지점에서 테스트됩니다.

- 모든 디코더 및 전처리기의 처리가 완료된 이후 및 규칙 처리가 시작되기 이전
- 각 규칙에 따라 처리된 이후

처리 시간이 테스트 지점의 임계값을 초과할 경우, 패킷 검사가 중단됩니다.

팁 루틴 TCP 스트림 또는 IP 조각 리어셈블리 시간은 총 패킷 처리 시간에 포함되지 않습니다.

패킷 레이턴시 임계값은 디코더, 전처리기 또는 패킷 처리 규칙에 의해 시작된 이벤트에 대해서는 영향을 미치지 않습니다. 적용 가능한 디코더, 전처리기 또는 규칙은 보통 패킷이 완전히 처리될 때까지, 또는 레이턴시 임계값이 초과하여 패킷 처리가 끝날 때까지, 어느 쪽이든 먼저 될 때까지 작동합니다. 삭제 규칙이 인라인 배포에서 침입을 탐지하는 경우, 삭제 규칙은 이벤트를 시작하며 패킷은 삭제됩니다.

참고 패킷 레이턴시 임계값 위반으로 인해 해당 패킷 처리가 끝난 후 규칙에 반하여 평가되는 패킷은 없습니다. 이벤트를 시작했을 수도 있는 규칙은 해당 이벤트를 시작할 수 없으며, 삭제 규칙을 위해 패킷을 삭제할 수 없습니다.

삭제 규칙에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

패킷 레이턴시 임계값을 사용하면 과도한 처리 시간이 요구되는 패킷 검사를 중단함으로써 패시브 및 인라인 구축 시 시스템 성능을 향상하고, 인라인 구축 시 레이턴시를 줄일 수 있습니다. 다음과 같은 경우 이러한 성능 이점을 누릴 수 있습니다.

- 패시브 및 인라인 배포에서 과도한 시간을 들여 여러 규칙별 패킷 검사를 순차적으로 수행하는 경우
- 인라인 배포에서 네트워크 성능이 저하된 경우(예: 누군가 대용량 파일을 다운로드하여 패킷 처리 속도가 느려짐)

수동 배포에서 패킷의 처리를 중지하면 처리는 다음 패킷으로 간단하게 옮겨가므로 네트워크 성능 복구에 도움이 되지 않을 수도 있습니다.

패킷 레이턴시 임계값 구성

라이센스: 보호

다음 표에서는 사용자가 패킷 레이턴시 임계값 구성을 설정할 수 있는 옵션을 설명합니다.

표 10-4 패킷 레이턴시 임계값 옵션

옵션	설명
임계값(마이크로초)	패킷의 검사가 중지될 때, 마이크로초로 시간을 지정합니다. 권장되는 최소 임계값 설정은 최소 패킷 레이턴시 임계값 설정 표를 참고하십시오.

패킷 레이턴시 임계값이 초과하므로 사용자는 시스템이 패킷 검사를 중지할 때 규칙 134:3을 활성화하여 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

여러 요소가 CPU 속도, 통신 속도, 패킷 크기 및 프로토콜 유형과 같은 시스템 성능 및 패킷 레이턴시 측정에 영향을 줍니다. 이러한 이유로, Cisco는 사용자 고유의 계산 결과가 사용자의 네트워크 환경에 맞춤식 설정을 제공할 때까지 사용자가 다음 표에서 임계값 설정을 사용할 것을 권장합니다.

표 10-5 최소 패킷 레이턴시 임계값 설정

데이터 속도	임계값 마이크로초 설정 최솟값
1Gbps	100
100Mbps	250
5Mbps	1000

설정을 계산할 때 다음을 결정하십시오.

- 초당 평균 패킷 수
- 패킷 당 평균 마이크로초

불필요하게 패킷 검사를 중단하지 않도록 하려면 사용자 네트워크를 위해 주요 보안 요인을 감안하여 패킷 당 평균 마이크로초를 증대하십시오.

예를 들어, 최소 패킷 레이턴시 임계값 설정 표는 1기가비트 환경에서 100마이크로초의 최소 패킷 레이턴시 임계값을 권장합니다. 이 최소 권장 사항은 테스트 데이터를 기반으로 하며, 초당 평균 250,000 패킷을 보입니다. 이는 마이크로초 당 0.25 패킷으로, 패킷 당 4마이크로초입니다. 스물 다섯 가지 요인으로 증대한 결과는 100마이크로초의 권장 최소 임계값입니다.

패킷 레이턴시 임계값 설정을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**을 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 Advanced(고급) 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Latency-Based Performance Settings(레이턴시 기반 성능 설정)** 옆에 있음)을 클릭한 후 표시되는 팝업 창에서 Packet Handling(패킷 처리) 탭을 선택합니다.

단계 5 최소 패킷 레이턴시 임계값 설정 표에서 권장되는 최소 **Threshold(임계값)** 설정을 참고하십시오.

단계 6 **OK(확인)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 저장하고 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

규칙 레이턴시 임계값의 이해

라이센스: 보호

규칙 레이턴시 임계값을 활성화하면 보안과 레이턴시 유지 필요성 사이의 균형을 적절한 수준으로 유지할 수 있습니다. 규칙 레이턴시 임계값은 각 규칙에서 개별 패킷을 처리하는 데 걸리는 시간을 측정하고, 처리 시간이 규칙 레이턴시 임계값(구성 가능한 연속 횟수)을 넘을 경우 위반 규칙 및 지정된 시간에 대한 관련 규칙 그룹을 동시에 중단하며, 일시 중단이 만료되면 해당 규칙을 복원합니다.

규칙 레이턴시 임계값은 처리 시간뿐만 아니라 소요된 시간까지 측정하여 패킷을 처리하는 규칙에 필요한 실제 시간을 더욱 정확하게 반영합니다. 그러나 레이턴시 임계값은 엄격한 타이밍을 시행하지 않는 소프트웨어 기반의 레이턴시 구현입니다.

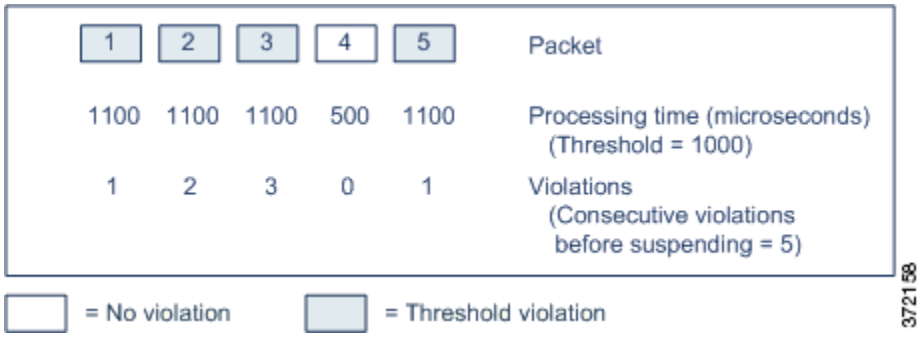
레이턴시 임계값에서 파생된 레이턴시 이점과 성능의 반대 급부는 검사하지 않은 패킷에 공격이 포함되어 있을 수 있다는 점입니다. 그러나, 규칙 레이턴시 임계값은 사용자가 보안과 연결성 사이의 균형을 잡는 데 사용할 수 있는 도구를 제공합니다.

타이머는 패킷이 규칙 그룹에 대해 처리될 때마다 처리 시간을 측정합니다. 규칙 처리 시간이 지정된 규칙 레이턴시 임계값을 초과하는 모든 경우, 시스템은 계수기를 증대합니다. 후속 임계값 위반 수가 지정된 수에 도달하는 경우, 시스템은 다음 작업을 수행합니다.

- 지정된 기간 동안 규칙을 중지합니다.
- 규칙이 중지되었음을 나타내는 이벤트를 시작합니다.
- 중지가 만료되면 규칙을 재활성화합니다.
- 규칙이 재활성화되었음을 나타내는 이벤트를 시작합니다.

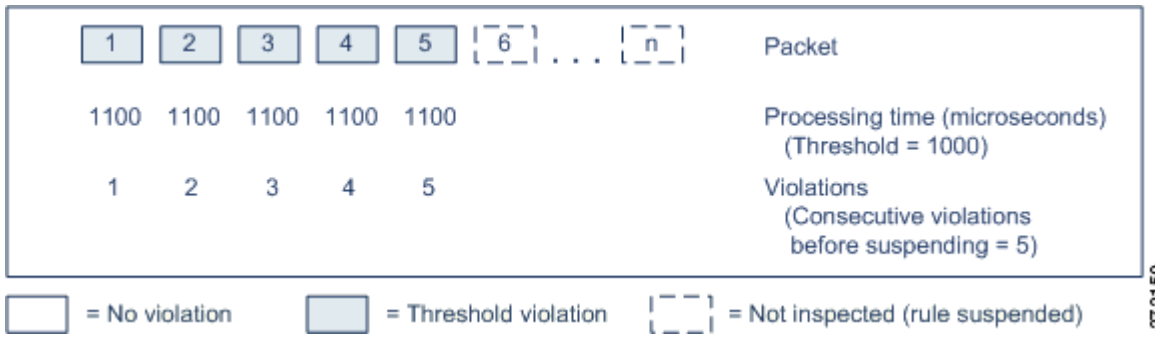
그룹 규칙이 중지되거나 규칙 위반이 연속적이지 않은 경우 시스템은 계수기를 0에 맞춥니다. 규칙을 중지하기 전에 여러 개의 연속되는 위반을 허용하면 사용자는 가끔 일어나는 규칙 위반, 즉 성능에 미치는 영향이 무시할 만한 수준인 위반을 무시해버리고 사용자는 규칙 레이턴시 임계값을 반복적으로 초과하는 규칙에 미치는 더욱 중대한 영향력에 집중하게 됩니다.

다음의 예시는 규칙 중단으로 귀결되지 않는 다섯 가지의 연속 규칙 처리 시간을 보여줍니다.



위 예시에서, 처음 3개 패킷의 각각을 처리하는 데 필요한 시간은 1000마이크로초의 규칙 레이턴시 임계값을 위반하며, 각 위반과 함께 위반 계수기도 증대됩니다. 네 번째 패킷 처리는 임계값을 위반하지 않으며, 위반 계수기는 0으로 재설정됩니다. 다섯 번째 패킷은 임계값을 위반하며, 위반 계수기는 1에서 다시 시작합니다.

다음의 예시는 규칙 중단으로 귀결되는 다섯 가지의 연속 규칙 처리 시간을 보여줍니다.



두 번째 예에서, 다섯 개의 패킷 중 각각을 처리하는 데 필요한 시간은 1000마이크로초의 규칙 레이턴시 임계값을 위반합니다. 규칙 그룹은 각 패킷에 대한 1100마이크로초의 규칙 처리 시간이 명시된 5회 연속 위반 기간 동안 1000마이크로초의 임계값을 초과하므로 중지됩니다. 패킷 6 또는 그보다 큰 수(n)로 표시된 모든 후속 패킷은 중지가 만료될 때까지 중지된 규칙에 반해 검토되지 않습니다. 규칙이 재활성화된 후에 추가 패킷이 발생하는 경우, 위반 계수기는 0에서 다시 시작됩니다.

규칙 레이턴시 임계값은 패킷을 처리하는 규칙에 의해 시작된 침입 이벤트에는 어떤 영향도 미치지 않습니다. 규칙은 규칙 처리 시간이 임계값을 초과하는지 여부에 상관 없이 패킷에서 탐지된 모든 침입에 대한 이벤트를 시작합니다. 침입을 탐지하는 규칙이 인라인 배포에서 삭제 규칙인 경우, 패킷은 삭제됩니다. 삭제 규칙이 패킷에서 규칙 중단으로 귀결되는 침입을 탐지하는 경우, 삭제 규칙은 침입 이벤트를 시작하고, 패킷은 삭제되며, 해당 규칙 및 모든 관련 규칙은 중지됩니다. 삭제 규칙에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

참고 패킷은 중단된 규칙에 반해 평가되지 않습니다. 이벤트를 시작했을 수도 있는 중지된 규칙은 해당 이벤트를 시작할 수 없으며, 삭제 규칙을 위해 패킷을 삭제할 수 없습니다.

규칙 레이턴시 임계값을 사용하면 대부분의 패킷 처리 시간을 관장하는 규칙을 중지함으로써 수동 배포 및 인라인 배포에 있어 시스템 성능을 향상하고, 인라인 배포 시 레이턴시를 줄일 수 있습니다. 패킷은 과부하된 디바이스에 복원할 수 있는 시간을 제공하면서 구성 가능한 시간이 만료될 때까지 중지된 규칙에 반해 다시 평가되지 않습니다. 다음과 같은 경우 이러한 성능 이점을 누릴 수 있습니다.

- 급히 쓰여진, 대개 테스트되지 않는 규칙에 과도한 양의 처리 시간이 필요한 경우
- 네트워크 성능이 저하된 경우(예: 누군가 대용량 파일을 다운로드하여 패킷 검사 속도가 느려짐)

규칙 레이턴시 임계값 구성

라이센스: 보호

규칙 레이턴시 임계값, 중단 규칙의 중단 시간, 그리고 연속된 임계값 위반 수를 수정할 수 있습니다. 이 위반은 규칙을 중단하기 전에 발생한 것이어야 합니다.

규칙 레이턴시 임계값은 시간 규칙이 **Consecutive Threshold Violations Before Suspending Rule(규칙 중지 전 연속 임계값 위반)**에 지정된 연속된 횟수 동안 **Threshold(임계값)**를 초과하는 패킷을 처리하기 시작할 때 **Suspension Time(중지 시간)**에 지정된 시간 동안 규칙을 중지합니다.

규칙이 중지되었을 때 규칙 134:1을 활성화하여 이벤트를 생성할 수 있고, 중지된 규칙이 활성화되었을 때는 규칙 134:2를 활성화하여 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

다음 표는 규칙 레이턴시 임계값 구성을 위해 설정할 수 있는 옵션을 자세히 설명합니다.

표 10-6 규칙 레이턴시 임계값 옵션

옵션	설명
임계값	패킷을 검토할 때 규칙이 초과해서는 안 되는 시간을 마이크로초로 지정합니다. 권장되는 최소 임계값 설정은 최소 규칙 레이턴시 임계값 설정 표를 참고하십시오.
규칙 중지 전 연속 임계값 위반	규칙이 중단되기 전에 패킷을 검사하려면 규칙이 **Threshold(임계값)**에 설정된 시간보다 더 오래 걸릴 수 있는 연속 횟수를 지정합니다.
중단 시간	규칙 그룹을 중지하려면 초 단위 시간을 지정합니다.

여러 요소가 CPU 속도, 통신 속도, 패킷 크기 및 프로토콜 유형과 같은 시스템 성능 측정에 영향을 줍니다. 이러한 이유로, Cisco는 사용자 고유의 계산 결과가 사용자의 네트워크 환경에 맞춤식 설정을 제공할 때까지 사용자가 다음 표에서 임계값 설정을 사용할 것을 권장합니다.

표 10-7 최소 규칙 레이턴시 임계값 설정

데이터 속도	임계값 마이크로초 설정 최솟값
1Gbps	500
100Mbps	1250
5Mbps	5000

설정을 계산할 때 다음을 결정하십시오.

- 초당 평균 패킷 수
- 패킷 당 평균 마이크로초

불필요하게 규칙을 중단하지 않도록 하려면 네트워크를 위해 주요 보안 요인을 감안하여 패킷 당 평균 마이크로초를 증대하십시오.

규칙 레이턴시 임계값 설정을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**을 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 Advanced(고급) 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Latency-Based Performance Settings(레이턴시 기반 성능 설정)** 옆에 있음)을 클릭한 후, 표시되는 팝업 창에서 Rule Handling(규칙 처리) 탭을 선택합니다.

단계 5 규칙 레이턴시 임계값 옵션 표에서 모든 옵션을 구성할 수 있습니다.

최소 규칙 레이턴시 임계값 설정 표에서 권장되는 최소 **Threshold(임계값)** 설정을 참고하십시오.

단계 6 **OK(확인)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 저장하고 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

침입 성능 통계 로깅 구성

라이센스: 보호

디바이스가 자체 기능을 모니터링하고 보고하는 방법에 대한 기본 매개변수를 구성할 수 있습니다. 이를 통해 시스템이 다음 옵션을 설정하여 디바이스의 성능 통계량을 업데이트하는 간격을 지정할 수 있습니다.

시간(초) 샘플링 및 패킷 수 최소화

성능 통계량 업데이트 사이에 지정된 시간(초)이 소요된 경우, 시스템은 패킷의 지정된 수를 분석했는지 확인합니다. 확인된 경우, 시스템은 성능 통계량을 업데이트합니다. 그렇지 않은 경우, 시스템은 패킷의 지정된 수를 분석할 때까지 기다립니다.

문제 해결 옵션: 로그 세션/프로토콜 배포

지원팀은 문제 해결 통화 중 사용자에게 프로토콜 배포, 패킷 길이 및 포트 통계량을 로깅할 것을 요청할 수 있습니다.

주의 이 문제 해결 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

문제 해결 옵션: 요약

지원팀은 문제 해결 통화 중 사용자에게 성능 통계량을 계산하는 시스템을 구성하도록 요청할 수 있습니다. 이는 Snort® 프로세스가 종료되었거나 다시 시작할 때에만 해당합니다. 이 옵션을 활성화하려면, 또한 반드시 **Log Session/Protocol Distribution(로그 세션/프로토콜 배포)** 옵션을 선택합니다.

주의 이 문제 해결 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

기본 성능 통계량 매개변수를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**을 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 Advanced(고급) 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘()(**Performance Settings(성능 설정)** 옆에 있음)을 클릭한 후, 표시되는 팝업 창에서 Performance Statistics(성능 통계) 탭을 선택합니다.

단계 5 위에 설명된 대로 **Sample time(샘플 시간)** 또는 **Minimum number of packets(패킷 최소 수)**를 수정합니다.

단계 6 지원팀의 요청이 있는 경우에만 선택적으로, **Troubleshoot Options(문제 해결 옵션)** 섹션을 확장하고 해당 옵션을 수정합니다.

단계 7 **OK(확인)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 저장하고 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

파일 및 악성코드 탐지 성능 및 저장 조정

라이센스: 보호 또는 악성코드

파일 제어, 악성코드 탐지 또는 차단 작업을 수행하는 파일 정책을 사용할 경우, 다음 표에 나열된 옵션을 설정할 수 있습니다. 파일 크기를 늘리면 시스템의 성능에 영향을 줄 수 있다는 점에 유의하십시오.

표 10-8 고급 액세스 제어 파일 및 악성 프로그램 탐지 옵션

필드	설명	기본값	범위	참고
파일 유형 탐지 중에 검사되는 바이트 수 제한	파일 유형 탐지를 수행할 때 검사되는 바이트 수를 지정합니다.	1460 바이트 또는 TCP 패킷의 최대 세그먼트 크기	0-4294967295 (4GB)	제한을 없애려면 0으로 설정합니다. 대부분의 경우 시스템은 첫 번째 패킷을 사용하여 공용 파일 유형을 확인할 수 있습니다.
다음보다 더 큰 파일의 SHA - 256 해시 값은 계산하지 않음(바이트)	사용자 탐지 목록에 추가된 경우 시스템이 특정 크기보다 큰 파일을 저장하지 않도록 하고, 해당 파일에 대한 종합적 보안 인텔리전스 클라우드 조회를 하거나, 해당 파일을 차단하지 않도록 합니다.	10485760 (10MB)	0-4294967295 (4GB)	제한을 없애려면 0으로 설정합니다.
악성 프로그램 차단을 위한 클라우드 조회가 다음보다 오래 걸리는 경우 파일 허용(초)	악성코드 클라우드 조회가 이루어지는 동안 **Block Malware(악성 프로그램 차단)** 규칙과 일치하고 캐시된 속성이 없는 파일의 최종 바이트가 시스템에 유지되는 기간을 지정합니다. 시스템이 속성을 보유하지 못하고 시간이 경과하면, 파일은 통과됩니다. 사용할 수 없는 속성은 캐시되지 않습니다.	2초	0-30초	이 옵션이 최대 30초의 값을 승인하더라도 Cisco는 사용자가 기본값을 사용하여 연결 실패로 인한 트래픽 차단을 예방할 것을 권장합니다. **반드시** 지원팀과 접촉 없이 이 옵션을 0으로 설정하지 마십시오.

파일 및 악성코드 검사 성능과 저장을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control(액세스 제어)**을 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 Advanced(고급) 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘()(**Files and Malware Settings(파일 및 악성코드 설정)**옆에 있음)을 클릭합니다.

Files and Malware Settings(파일 및 악성코드 설정) 팝업 창이 표시됩니다.

단계 5 고급 액세스 제어 파일 및 악성 프로그램 탐지 옵션 표에서 모든 옵션을 설정할 수 있습니다.

단계 6 **OK(확인)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 저장하고 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

네트워크 분석 및 침입 정책의 이해

네트워크 분석 및 침입 정책은 ASA FirePOWER 모듈 침입 탐지 및 방지 기능의 일환으로 함께 작동합니다. *침입 탐지*란 용어는 일반적으로 네트워크 트래픽에서 잠재적인 침입을 수동적으로 분석하고 보안 분석을 위한 공격 데이터를 저장하는 프로세스를 말합니다. *침입 방지*란 용어에는 침입 탐지의 개념이 포함되지만, 악성 트래픽이 네트워크를 통과할 때 이를 차단 또는 변경하는 기능이 추가됩니다.

침입 방지 구축에서 시스템이 패킷을 검토할 때:

- **네트워크 분석 정책**은 트래픽을 *디코딩하고 전처리하는*방법을 제어합니다. 이 정책의 목적은 향후 평가를 위함이며, 특히 침입 시도의 신호가 될 수 있는 변칙 트래픽의 경우 유효합니다.
- **침입 정책**은 *침입 및 전처리 규칙*(집합적으로 *침입 규칙*이라고도 함)을 사용하여 패턴 기반의 공격에 대한 디코딩된 패킷을 검사합니다. 침입 정책은 *변수 집합*과 페어링되는데, 이를 통해 네트워크 환경을 올바르게 반영하는 지정된 값을 사용할 수 있습니다.

네트워크 분석과 침입 정책 모두 상위 액세스 제어 정책에 의해 호출되지만 그 시점은 다릅니다. 시스템이 트래픽을 분석하기 때문에, 네트워크 분석(디코딩 및 전처리) 단계는 침입 방지(추가 전처리 및 침입 규칙) 단계보다 이전에 또는 별도로 발생합니다. 네트워크 분석 및 침입 정책은 폭넓고 심층적인 패킷 검사를 제공합니다. 이 둘을 함께 사용하면 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성을 위협할 수 있는 네트워크 트래픽을 탐지하고 알리고 방지할 수 있습니다.

ASA FirePOWER 모듈에서는 상호 보완하고 함께 작동하는 비슷한 이름의 여러 네트워크 분석 및 침입 정책(예: Balanced Security and Connectivity)을 제공합니다. 시스템에서 제공하는 정책을 사용하여 Cisco VRT(Vulnerability Research Team)의 경험을 활용할 수 있습니다. VRT는 이 정책에 대해, 침입 및 전처리기 규칙 상태를 설정할 뿐만 아니라, 전처리기 및 다른 고급 설정에 대한 초기 구성을 제공합니다.

또한 사용자 지정 네트워크 분석 및 침입 정책을 만들 수 있습니다. 사용자 지정 정책의 설정을 조정하여 가장 중요하다고 생각되는 방식으로 트래픽을 검사할 수 있습니다. 유사한 정책 편집기를 사용하여 네트워크 분석 및 침입 정책을 생성, 수정, 저장 및 관리합니다. 정책 유형 중 하나를 수정할 때, 탐색 패널은 사용자 인터페이스의 왼쪽에 표시되며, 오른쪽에는 다양한 구성 페이지를 표시합니다.

이 장에서는 네트워크 분석 및 침입 정책에서 제어하는 구성의 유형에 대해 간략하게 살펴보고, 트래픽을 검토하고 정책 위반 레코드를 생성하기 위해 정책이 함께 작동하는 방법에 대해 설명하고, 정책 편집기 탐색에 대한 기본적인 정보를 제공합니다. 이 장에서는 또한 시스템이 제공하는 정책과 사용자 지정 정책을 사용하는 것의 이점과 한계를 비교하여 설명합니다. 자세한 내용은 다음 섹션을 참고하십시오.

침입 배포를 사용자 정의하려면 다음 단계를 위해 다음을 참고하십시오.

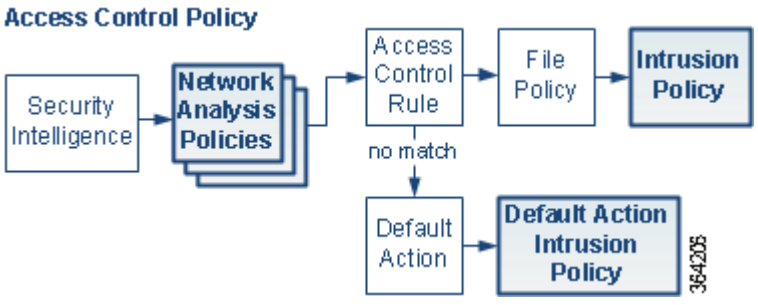
- 2-14페이지의 변수 집합 작업은 네트워크 환경을 정확하게 반영하도록 시스템의 침입 변수를 설정하는 방법을 설명합니다. 사용자 지정 정책을 사용하지 않는 경우에도 Cisco는 기본 변수 집합의 기본 변수를 수정할 것을 **강력하게** 권장합니다. 고급 사용자는 하나 이상의 사용자 지정 침입 정책으로 페어링을 위한 사용자 지정 변수 집합을 만들고 사용할 수 있습니다.
- 19-1페이지의 침입 정책 시작하기는 간단한 사용자 지정 침입 정책을 만들고 수정하는 방법을 설명합니다.
- 10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어는 침입 정책과 상위 액세스 제어 정책을 연결함으로써 관심이 있는 트래픽만 검토하도록 침입 정책을 사용하여 시스템을 구성하는 방법에 대해 설명합니다. 또한 고급 침입 정책 성능 옵션을 구성하는 방법에 대해서도 설명합니다.
- 17-1페이지의 고급 전송/네트워크 설정 구성은 모든 트래픽에 전역으로 적용하는 고급 전송 및 네트워크 전처리기 설정을 구성하는 방법에 대해 설명합니다. 이러한 고급 설정은 네트워크 분석 또는 침입 정책보다는 액세스 제어 정책에서 구성합니다.
- 14-1페이지의 네트워크 분석 정책 시작하기는 간단한 사용자 지정 네트워크 분석 정책을 만들고 수정하는 방법을 설명합니다.
- 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의는 기본 네트워크 분석 정책을 변경하는 방법에 대해 설명합니다. 고급 사용자의 경우, 이 섹션은 또한 일치하는 트래픽을 전처리하는 사용자 지정 네트워크 분석 정책을 할당하여 특정 보안 영역 및 네트워크에 따라 전처리를 조정하는 방법을 설명합니다.
- 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용은 대규모 조직 또는 복잡한 배포에서 여러 네트워크 분석 또는 침입 정책을 더욱 효율적으로 관리하기 위해 정책 *레이어*이라는 구성 요소를 사용하는 방법을 설명합니다.

정책이 트래픽에서 침입을 검토하는 방법 이해

라이센스: 보호

시스템이 액세스 제어 배포의 일부로 트래픽을 분석할 때, 네트워크 분석(디코딩 및 전처리) 단계는 침입 방지(침입 규칙 및 고급 설정) 단계보다 이전에 또는 별도로 발생합니다.

다음 다이어그램은 인라인, 침입 방지 및 AMP(Advanced Malware Protection) 배포에서 트래픽 분석의 순서를 간소화된 형식으로 보여줍니다. 또한 액세스 제어 정책이 다른 정책을 호출하여 트래픽을 검토하는 방법 및 그러한 정책이 호출되는 순서를 보여줍니다. 네트워크 분석 및 침입 정책 선택 단계는 강조 표시됩니다.



인라인 배포에서 시스템은 설명된 절차의 거의 모든 단계에서 추가 검사 없이 트래픽을 차단할 수 있습니다. 보안 인텔리전스, 네트워크 분석 정책, 파일 정책 및 침입 정책은 모든 트래픽을 수정 또는 삭제할 수 있습니다.

마찬가지로 프로세스의 각 단계에서 패킷은 시스템이 이벤트를 생성하도록 할 수 있습니다. 침입 및 전처리기 이벤트(집합적으로 *침입 이벤트*라고도 함)는 패킷 또는 패킷의 콘텐츠가 보안 위험을 나타낼 수 있음을 표시합니다.

단일 연결의 경우, 다이어그램에 나타난 것처럼 시스템은 액세스 제어 규칙에 앞서 네트워크 분석 정책을 선택하지만, 일부 전처리(특히 애플리케이션 레이어 전처리)는 액세스 제어 규칙 선택 이후에 발생한다는 점에 유의하십시오. 이는 사용자 지정 네트워크 분석 정책에서 전처리를 구성하는 방식에 영향을 주지 **않습니다**.

자세한 내용은 다음을 참고하십시오.

- 11-3페이지의 디코딩, 정규화 및 전처리: 네트워크 분석 정책
- 11-4페이지의 액세스 제어 규칙: 침입 정책 선택
- 11-5페이지의 침입 검사: 침입 정책, 규칙 및 변수 집합
- 11-6페이지의 침입 이벤트 생성

디코딩, 정규화 및 전처리: 네트워크 분석 정책

라이센스: 보호

프로토콜 차이가 패턴 일치를 불가능하게 할 수 있으므로 디코딩과 전처리가 없으면 시스템은 침입 탐지를 위해 트래픽을 제대로 평가할 수 없습니다. 11-2페이지의 정책이 트래픽에서 침입을 검토하는 방법 이해의 다이어그램에서 볼 수 있듯이, 네트워크 분석 정책이 이러한 트래픽 처리 작업을 제어합니다.

- **이후** 트래픽은 보안 인텔리전스에서 필터링됩니다.
- **이전** 트래픽은 파일 또는 침입 정책에 의해 검사될 수 있습니다.

네트워크 분석 정책은 처리 단계에서 패킷을 제어합니다. 먼저 시스템이 첫 세 개 TCP/IP 레이어를 통해 패킷을 디코딩한 다음, 프로토콜 이상 징후를 표준화하고, 전처리하며, 계속해서 탐지합니다.

- 패킷 디코더는 패킷 헤더 및 페이로드를 전처리기에서 쉽게 사용할 수 있는 형식으로, 그리고 추후 침입 규칙에서 쉽게 사용할 수 있는 형식으로 변환합니다. TCP/IP 스택의 각 레이어는 데이터 링크 레이어로 시작하여 계속해서 네트워크 및 전송 레이어를 통해 차례로 디코딩됩니다. 패킷 디코더는 또한 패킷 헤더의 다양하고 변칙적인 작업을 탐지합니다. 자세한 내용은 17-16페이지의 패킷 디코딩 이해를 참고하십시오.
- 인라인 배포에서, 인라인 표준화 전처리기는 공격자가 탐지를 우회하는 가능성을 최소화하기 위해 트래픽을 새로 포맷합니다(표준화합니다). 이는 다른 전처리기 및 침입 규칙에 따라 패킷이 검사될 수 있도록 준비하고, 시스템이 처리하는 패킷이 사용자 네트워크 호스트에서 수신된 패킷과 동일한지 확인할 수 있도록 지원합니다. 자세한 내용은 17-6페이지의 인라인 트래픽 표준화를 참고하십시오.
- 다양한 네트워크 및 전송 레이어 전처리기는 IP 조각을 이용한 익스플로잇을 탐지하고 체크섬 유효성 검증을 수행하며, TCP와 UDP 세션 전처리를 수행합니다(17-1페이지의 전송 및 네트워크 레이어 전처리 구성 참고).

  일부 고급 전송 및 네트워크 전처리기 설정은 액세스 제어 정책에서 처리된 모든 트래픽에 전역으로 적용된다는 점에 유의하십시오. 이러한 설정은 네트워크 분석 정책보다는 액세스 제어 정책에서 구성합니다(17-1페이지의 고급 전송/네트워크 설정 구성 참고).
- 다양한 애플리케이션 레이어 프로토콜 디코더는 특정 패킷 데이터 유형을 침입 규칙 엔진이 분석할 수 있는 형식으로 표준화합니다. 애플리케이션 레이어 프로토콜 인코딩을 정규화함으로써 시스템에서는 데이터가 다르게 표현된 패킷에 동일한 콘텐츠 관련 침입 규칙을 효과적으로 적용하고 의미 있는 결과를 얻을 수 있습니다. 자세한 내용은 15-1페이지의 애플리케이션 레이어 전처리기 사용을 참고하십시오.

- Modbus(모드버스), DNP3 및 SCADA 전처리기는 트래픽의 비정상적인 상태를 탐지하고 침입 규칙에 데이터를 제공합니다. Supervisory Control(감시 제어) 및 Data Acquisition(데이터 획득. SCADA) 프로토콜은 제조, 생산, 정수 처리, 배전, 공항 및 배송 시스템 등과 같은 산업, 인프라 및 설비의 데이터를 모니터링하고, 제어하며, 획득합니다. 자세한 내용은 16-1페이지의 SCADA 전처리 구성을 참고하십시오.
- 여러 전처리기는 사용자가 Back Orifice, portscans, SYN floods 및 기타 속도 기반 공격과 같은 특정 위협을 탐지하도록 합니다(21-1페이지의 특정 위협 탐지 참고).

  침입 정책 내에서 신용 카드 번호 및 ASCII 문자로 표시된 주민등록번호와 같은 중요한 데이터를 탐지하는 민감한 데이터 전처리기를 구성한다는 점에 유의하십시오(21-20페이지의 민감한 데이터 검색 참고).

새로 만든 액세스 제어 정책에서 하나의 기본 네트워크 분석 정책은 동일한 상위 액세스 제어 정책에 의해 호출된 *모든* 침입 정책에 대한 *모든* 트래픽에 대해 전처리를 제어합니다. 먼저, 시스템은 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책을 기본값으로 사용하지만, 기타 시스템이 제공하는 네트워크 분석 정책 또는 사용자 지정 네트워크 분석 정책으로 변경할 수 있습니다. 더 복잡한 배포에서, 고급 사용자는 일치하는 트래픽을 전처리하는 다양한 사용자 정의 네트워크 분석 정책을 부과하여 특정 보안 영역 및 네트워크에 트래픽 전처리 옵션을 맞출 수 있습니다. 자세한 내용은 11-6페이지의 시스템 제공 정책과 사용자 지정 정책 비교를 참고하십시오.

액세스 제어 규칙: 침입 정책 선택

라이센스: 보호

초기 전처리 후, (있는 경우) 액세스 제어 규칙이 트래픽을 평가합니다. 대부분의 경우 패킷과 일치하는 첫 번째 액세스 제어 규칙이 트래픽을 처리하는 규칙입니다. 일치하는 트래픽을 모니터링, 신뢰, 차단 또는 허용할 수 있습니다.

액세스 제어 규칙을 통해 트래픽을 허용할 경우, 시스템은 트래픽에서 악성코드, 금지 파일 및 침입을 순서대로 검사할 수 있습니다. 액세스 제어 규칙과 일치하지 않는 트래픽은 침입을 검사할 수 있는 액세스 제어 정책의 기본 작업에 의해 처리됩니다.

참고 어느 네트워크 분석 정책이 패킷을 전처리하는지에 **상관없이** 모든 패킷은 구성된 액세스 제어 규칙에 일치되며 따라서 하향식 순서로 침입 정책에 의한 잠재적 검사의 대상이 됩니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

11-2페이지의 정책이 트래픽에서 침입을 검토하는 방법 이해의 다이어그램은 다음과 같이 인라인, 침입 방지 및 AMP 배포에서 디바이스를 통해 트래픽의 흐름을 보여줍니다.

- 액세스 제어 규칙을 사용하면 트래픽 일치를 진행할 수 있습니다. 이후 트래픽은 탐지되며, 금지 파일 및 악성코드 검색을 위해 파일 정책으로 탐지되며, 이후 침입 탐지를 위해 침입 정책으로 탐지됩니다.
- 이 시나리오에서 액세스 제어 정책의 기본 작업은 일치하는 트래픽을 허용하는 것입니다. 다음으로 트래픽은 침입 정책의 검사를 받습니다. 침입 정책을 액세스 제어 규칙 또는 기본 작업과 연결할 때 다른 침입 정책을 사용할 수 있습니다(그러나 반드시 그렇게 해야 할 필요는 없음).

시스템은 차단된 트래픽 또는 신뢰할 수 있는 트래픽은 검사하지 않으므로 다이어그램의 예에는 차단 또는 신뢰 규칙이 포함되어 있지 않습니다. 자세한 내용은 6-6페이지의 규칙 작업을 사용하여 트래픽 관리 및 검사 결정 및 4-4페이지의 네트워크 트래픽에 대한 기본 처리와 검사 설정을 참고하십시오.

침입 검사: 침입 정책, 규칙 및 변수 집합

라이센스: 보호

침입 방지는 트래픽이 목적지로 들어가기 전 시스템의 최후의 방어선으로 사용할 수 있습니다. 침입 정책은 보안 위반 확인을 위해 시스템이 인라인 배포에서 트래픽을 검사하는 방식을 제어하며, 악성 트래픽을 차단하거나 변경할 수 있습니다. 침입 정책의 주요 기능은 어느 침입 및 전처리기 규칙이 활성화되는지와 이들이 구성되는 방식을 관리하는 것입니다.

침입 및 전처리기 규칙

침입 규칙은 네트워크의 취약성을 이용하려는 시도를 탐지하는 키워드 및 논쟁의 지정된 집합이며, 시스템은 침입 규칙을 사용하여 네트워크 트래픽을 분석하고, 규칙의 기준과 일치하는지를 확인합니다. 시스템은 패킷을 각 규칙에 지정된 조건과 비교하며, 패킷 데이터가 규칙에 지정된 모든 조건에 일치하는 경우 규칙이 트리거됩니다.

시스템은 VRT에서 만든 다음 유형의 규칙을 포함합니다.

- *공유 개체 침입 규칙*. 이는 컴파일된 것이며 수정할 수 없습니다(소스 및 대상 포트, IP 주소와 같은 규칙 헤더 정보 제외)
- *표준 텍스트 침입 규칙*. 이는 규칙의 새 사용자 지정 인스턴스로 저장되며 수정할 수 있습니다.
- *전처리기 규칙*. 이는 네트워크 분석 정책에서 전처리기 및 패킷 디코더 탐지 옵션과 관련된 규칙입니다. 전처리기 규칙을 복사하거나 수정할 수 없습니다. 대부분의 전처리기 규칙은 기본적으로 비활성화됩니다. 이벤트를 생성하고, 인라인 배포에서, 문제가 되는 패킷을 중단하기 위해 전처리기를 사용하려면 이들을 활성화해야 합니다.

시스템이 침입 정책에 따라 패킷을 처리할 때, 먼저 규칙 최적화기가 다음과 같은 기준에 근거하여 하위 집합 내 모든 활성화된 규칙을 분류합니다. 전송 레이어, 애플리케이션 프로토콜, 보호된 네트워크로 오가는 방향 등. 다음으로, 침입 규칙 엔진은 각 패킷에 적용하기 위해 적절한 규칙 하위 집합을 선택합니다. 마지막으로, 다중 규칙 검색 엔진은 트래픽이 규칙과 일치하는지 확인하기 위해 서로 다른 세 가지 유형의 검색을 수행합니다.

- 프로토콜 필드 검색은 애플리케이션 프로토콜 내 특정 필드에서 일치 항목을 검색합니다.
- 일반적인 콘텐츠 검색은 패킷 페이로드의 ASCII 또는 이진 바이트 일치 항목을 검색합니다.
- 패킷 이상 징후 검색은 특정 내용을 포함하기보다는 안정된 프로토콜을 위반하는 패킷 헤더 및 페이로드를 검색합니다.

사용자 지정 침입 정책에서 규칙을 활성화 및 비활성화고 사용자 고유의 표준 텍스트 규칙을 작성 및 추가하여 탐지를 설정할 수 있습니다.

변수 집합

시스템이 트래픽 평가를 위해 침입 정책을 사용할 때마다, 연결된 *변수 집합*을 사용합니다. 집합 내 대부분의 변수는 소스 및 목적지 IP 주소와 포트 확인을 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 또한 침입 정책 내 변수를 사용하여 규칙 삭제 및 동적 규칙 상태의 IP 주소를 나타낼 수 있습니다.

시스템은 단일 기본 변수 집합을 제공하는데, 이는 미리 정의된 기본 변수로 구성되어 있습니다. 대부분의 시스템이 제공하는 공유 객체 규칙과 표준 텍스트 규칙은 미리 정의된 기본 변수를 사용하여 네트워크와 포트 번호를 정의합니다. 예를 들어, 대부분의 규칙은 `$HOME_NET` 변수를 사용하여 보호된 네트워크를 지정하고 `$EXTERNAL_NET` 변수를 사용하여 보호되지 않은(또는 외부) 네트워크를 지정합니다. 또한 특수한 규칙은 종종 다른 사전 정의된 변수를 사용합니다. 예를 들어, 웹 서버에 대한 익스플로잇을 탐지하는 규칙은 `$HTTP_SERVERS` 및 `$HTTP_PORTS` 변수를 사용합니다.

팁 시스템에서 제공한 침입 정책을 사용하는 경우에도 Cisco는 기본 변수 집합의 주요 기본 변수를 수정할 것을 **강력하게** 권장합니다. 올바르게 네트워크 환경을 반영하는 변수를 사용할 때, 처리는 최적화되고 시스템은 의심스러운 활동에 대해 관련 시스템을 모니터링할 수 있습니다. 고급 사용자는 하나 이상의 사용자 지정 침입 정책으로 페어링을 위한 사용자 지정 변수 집합을 만들고 사용할 수 있습니다. 자세한 내용은 2-15페이지의 미리 정의된 기본 변수 최적화를 참고하십시오.

침입 이벤트 생성

라이센스: 보호

시스템이 가능한 침입을 식별할 때, (집합적으로 *침입 이벤트*라고도 함) *침입*또는 *전처리기 이벤트*를 생성합니다. 네트워크 자산에 대한 공격을 더욱 잘 이해하기 위해서 해당 데이터를 볼 수 있습니다. 인라인 배포에서, 시스템은 또한 유해한 것으로 알려진 패킷을 삭제하거나 교체할 수 있습니다.

각 침입 이벤트는 이벤트 헤더를 포함하며, 이벤트 이름 및 분류에 관한 정보를 포함합니다. 여기에는 소스 및 대상 IP 주소, 포트, 이벤트를 생성한 프로세스, 이벤트의 날짜 및 시간, 그리고 공격의 출처 및 공격 대상에 대한 컨텍스트 관련 정보 등이 있습니다. 패킷 기반 이벤트의 경우, 시스템은 또한 디코딩된 패킷 헤더 및 패킷의 페이로드 또는 이벤트를 시작한 패킷의 복사본을 로깅합니다.

패킷 디코더, 전처리기 및 침입 규칙 엔진은 모두 시스템이 이벤트를 생성하도록 할 수 있습니다. 예를 들면 다음과 같습니다.

- (네트워크 분석 정책에서 구성된) 패킷 디코더가 어떤 옵션 또는 페이로드도 없는 IP 데이터그램의 크기인 20바이트 보다 작은 IP 패킷을 수신한 경우, 디코더는 이를 이상 트래픽으로 해석합니다. 나중에, 패킷을 검토하는 침입 정책에서 관련 디코더 규칙이 활성화된 경우, 시스템은 전처리기 이벤트를 생성합니다.
- IP 조각 모음 전처리기에 중복되는 일련의 IP 조각이 발생할 경우, 전처리기는 이를 잠재적인 공격으로 해석하며, 관련 전처리기 규칙이 활성화된 경우 시스템은 전처리기 이벤트를 생성합니다.
- 패킷이 시작되면 침입 이벤트를 생성할 수 있도록 침입 규칙 엔진에서 대부분의 표준 텍스트 규칙 및 공유 객체 규칙은 로깅됩니다.

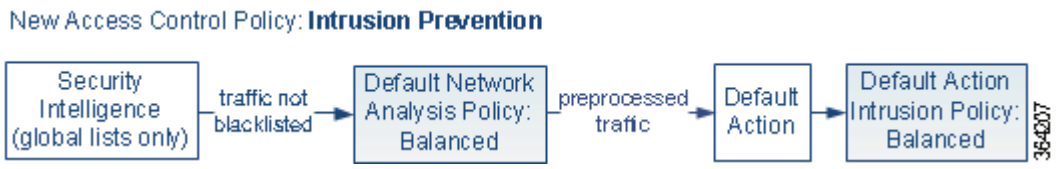
디바이스가 침입 이벤트를 누적하므로, 잠재적인 공격에 대한 분석을 시작할 수 있습니다. 시스템은 침입 이벤트를 검토하고 네트워크 환경 및 보안 정책의 컨텍스트에서 중요성을 띠는지 여부를 평가하는 데 필요한 툴을 제공합니다.

시스템 제공 정책과 사용자 지정 정책 비교

라이센스: 보호

새 액세스 제어 정책을 만드는 것은 ASA FirePOWER 모듈을 사용하여 트래픽 흐름을 관리하는 첫 단계 중 하나입니다. 기본적으로, 새로 만든 액세스 제어 정책은 트래픽을 검토하기 위해 시스템 제공 네트워크 분석 및 침입 정책을 호출합니다.

다음 다이어그램은 인라인 침입 방지 배포에서 새로 만든 액세스 제어 정책이 트래픽을 초반에 처리하는 방식을 보여줍니다. 전처리 및 침입 방지 단계는 강조 표시됩니다.



다음 방식을 참고하십시오.

- 기본 네트워크 분석 정책이 액세스 제어 정책에서 처리된 *모든* 트래픽의 전처리를 제어하는 방식. 초기에는 시스템이 제공한 *Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책*이 기본값입니다.
- 액세스 제어 정책의 기본 작업은 시스템이 제공한 *Balanced Security and Connectivity(균형 잡힌 보안 및 연결성)*에 의해 결정된 대로 모든 비 악성 트래픽을 허용합니다.
- 정책은 기본 Security Intelligence(보안 인텔리전스) 옵션(전역 허용 목록 및 차단 목록 한정)을 사용하고 액세스 제어 규칙을 사용하여 네트워크 트래픽을 특수한 방식으로 처리하거나 검사하지 않습니다.

침입 방지 배포를 조정하기 위해 취할 수 있는 간단한 조치는 시스템 제공 네트워크 분석 및 침입 정책의 서로 다른 집합을 기본값으로 사용하는 것입니다. Cisco는 ASA FirePOWER 모듈과 더불어 여러 쌍의 침입 정책을 제공합니다.

또는, 사용자 지정 정책을 생성하고 사용하여 침입 방지 배포를 맞춤화할 수 있습니다. 전처리기 옵션, 침입 규칙 및 이 정책에 구성된 기타 고급 설정이 네트워크의 보안 요구를 충족하지 않음을 알게 될 수도 있습니다. 네트워크 분석 및 침입 정책을 설정하여 시스템이 침입 탐지를 위해 네트워크에서 트래픽을 처리하고 검사하는 방식을 매우 세부적으로 구성할 수 있습니다.

자세한 내용은 다음을 참고하십시오.

- 11-7페이지의 시스템 제공 정책의 이해
- 11-8페이지의 사용자 지정 정책의 이점
- 11-11페이지의 사용자 지정 정책의 한계

시스템 제공 정책의 이해

라이센스: 보호

Cisco는 ASA FirePOWER 모듈과 함께 여러 쌍의 네트워크 분석 및 침입 정책을 제공합니다. 시스템이 제공하는 네트워크 분석 및 침입 정책을 사용하여 Cisco VRT(취약성 연구단)의 경험을 활용할 수 있습니다. VRT는 이 정책에 대해, 침입 및 전처리기 규칙 상태를 설정할 뿐만 아니라, 전처리기 및 다른 고급 설정에 대한 초기 구성을 제공합니다. 사용자는 시스템이 제공하는 정책을 있는 그대로 사용할 수도 있고, 이를 맞춤형 정책을 위한 기반으로 사용할 수도 있습니다.

팁 시스템에서 제공한 네트워크 분석 및 침입 정책을 사용하고 있는 경우에도 자신의 네트워크 환경을 정확하게 반영할 수 있도록 시스템의 침입 변수를 구성해야 합니다. 최소한, 기본값 집합의 주요 기본 변수라도 수정하시기 바랍니다(2-15페이지의 미리 정의된 기본 변수 최적화 참고).

새로운 취약성이 알려지면 VRT에서 침입 규칙 업데이트를 릴리스합니다. 이 규칙 업데이트는 모든 시스템 제공 네트워크 분석 또는 침입 정책을 수정할 수 있고 새롭게 업데이트된 침입 규칙 및 전처리기 규칙, 기존 규칙을 위한 수정된 상태, 그리고 수정된 기본 정책 설정을 제공할 수 있습니다. 규칙 업데이트는 또한 시스템 제공 정책에서 규칙을 삭제할 수 있고, 새로운 규칙 카테고리를 제공할 수 있으며, 기본 변수 집합을 수정할 수 있습니다.

규칙 업데이트가 배포에 영향을 미치는 경우, 시스템은 영향을 받는 침입 및 네트워크 분석 정책 뿐만 아니라 상위 액세스 제어 정책을 오래된 것으로 표시합니다. 변경 사항을 반영하려면 업데이트된 정책을 다시 적용해야 합니다.

사용자의 편의를 위해 규칙 업데이트를 구성하여 영향을 받는 침입 정책을 단독으로 또는 영향을 받는 액세스 제어 정책과 조합하여 자동으로 다시 적용할 수 있습니다. 이를 통해 쉽고 자동적으로 사용자 배포를 최신 상태로 유지하여 최근 발견된 침입 및 익스플로잇으로부터 보호할 수 있습니다.

최신 전처리 설정을 확보하려면 **반드시** 액세스 제어 정책을 다시 적용해야 하는데, 이는 또한 현재 실행 중인 것과는 다른 모든 관련 네트워크 분석 및 파일 정책을 다시 적용하며, 또한 고급 전처리 및 성능 옵션의 기본값을 업데이트할 수 있습니다. 자세한 내용은 35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기를 참고하십시오.

Cisco는 ASA FirePOWER 모듈과 함께 다음 네트워크 분석 및 침입 정책을 제공합니다.

Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 및 침입 정책

이 정책은 속도 및 탐지 모두에 구축됩니다. 이들은 함께 사용되며, 대다수 조직을 위해 좋은 시작점의 역할을 합니다. 시스템은 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 정책 및 설정을 대부분의 경우 기본값으로 사용합니다.

Connectivity Over Security(보안에 우선하는 연결성) 보안 네트워크 분석 및 침입 정책

이 정책은 (모든 리소스에 접근할 수 있는) 연결성이 네트워크 인프라 보안에 우선하는 조직을 위해 구축됩니다. 침입 정책은 Security Over Connectivity(연결성에 우선하는 보안)에서 활성화된 것보다 훨씬 더 적은 규칙을 활성화합니다. 트래픽을 차단하는 가장 중요한 규칙만 활성화됩니다.

Security Over Connectivity(연결성에 우선하는 보안) 네트워크 분석 및 침입 정책

이 정책은 네트워크 인프라 보안이 사용자 편의에 우선하는 조직을 위해 구축됩니다. 침입 정책은 적합한 트래픽에 대해 경계하거나 중단할 수 있는 다양한 네트워크 이상 침입 규칙을 활성화합니다.

No Rules Active(활성 규칙 불가) 침입 정책

No Rules Active(활성 규칙 불가) 침입 정책에서, 모든 침입 규칙 및 고급 설정이 비활성화됩니다. 이 정책은 다른 시스템 제공 정책 중 하나에서 활성화된 규칙에 근거를 두는 것을 대신하여 사용자 고유의 침입 정책 생성을 원할 경우 시작점이 됩니다.

주의 Cisco는 다른 정책, 즉 Experimental Policy 1(실험 정책 1)을 테스트용으로 사용합니다. Cisco 관계자의 지시 없이는 Experimental Policy 1(실험 정책 1)을 사용하지 마십시오.

사용자 지정 정책의 이점

라이센스: 보호

전처리기 옵션, 침입 규칙 및 시스템 제공 네트워크 분석 또는 침입 정책에 구성된 기타 고급 설정이 조직의 보안 요구를 완전히 충족하지 않음을 확인할 수도 있습니다.

사용자 지정 정책을 구축하는 것은 사용자 환경에서 시스템의 성능을 개선할 수 있으며, 사용자 네트워크에서 일어나는 악의적인 트래픽 및 정책 위반을 집중적으로 살펴볼 수 있도록 할 수 있습니다. 사용자 지정 정책을 생성하고 설정함에 따라 사용자는 시스템이 침입 탐지를 위해 네트워크에서 트래픽을 처리 하고 검사하는 방식을 매우 세부적으로 구성할 수 있습니다.

모든 사용자 정책에는 기본 정책이 있으며, 이는 기본 레이어라고도 하는데, 정책의 모든 구성에 대한 기본 설정을 정의합니다. 레이어는 여러 네트워크 분석 또는 침입 정책을 효율적으로 관리하는 데 사용할 수 있는 구성 요소입니다(12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용 참고).

대부분의 경우, 사용자 지정 정책은 시스템 제공 정책을 기반으로 하지만, 다른 사용자 지정 정책을 사용할 수 있습니다. 하지만, 사용자 지정 정책은 시스템 제공 정책을 정책 체인의 궁극적인 기반으로 둡니다. 사용자 지정 정책을 사용자 기반으로 사용하는 경우 규칙 업데이트는 시스템 제공 정책을 변경할 수 있으며, 규칙 업데이트를 가져오는 것이 사용자에게 영향을 미칠 수 있습니다. 규

칙 업데이트가 정책에 영향을 미치는 경우, 모듈 인터페이스는 영향을 받은 정책을 오래된 것으로 표시합니다. 자세한 내용은 12-4페이지의 규칙 업데이트를 통해 시스템이 제공하는 기본 정책 수정 허용을 참고하십시오.

자세한 내용은 다음을 참고하십시오.

- 11-9페이지의 사용자 지정 네트워크 분석 정책의 이점
- 11-10페이지의 사용자 지정 침입 정책의 이점

사용자 지정 네트워크 분석 정책의 이점

라이센스: 보호

기본적으로 하나의 네트워크 분석 정책은 액세스 제어 정책에서 처리된 모든 트래픽을 전처리합니다. 이는 모든 패킷이 나중에 이들을 검토하는 침입 정책(따라서 침입 규칙 집합)에 관계없이 동일한 설정에 따라 디코딩 및 전처리된다는 것을 의미합니다.

초기에는 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책이 기본값입니다. 전처리를 조정하는 간단한 방법은 기본값으로 사용자 네트워크 분석 정책을 생성하고 사용하는 것입니다(13-4페이지의 액세스 제어를 위한 기본 네트워크 분석 정책 설정 참고).

사용 가능한 옵션 조정은 전처리기에 따라 다르지만, 전처리기 및 디코더를 조정할 수 있는 일부 방법은 다음을 포함합니다:

- 모니터링하는 트래픽에 적용하지 않는 전처리를 비활성화할 수 있습니다. 예를 들어, HTTP Inspect(HTTP 검사) 전처리기는 HTTP 트래픽을 표준화합니다. 사용자가 네트워크에 Microsoft IIS(Internet Information Services)를 사용하는 웹 서버는 어느 것도 포함되어 있지 않음을 확신할 경우, IIS 특정 트래픽을 검색하는 전처리기 옵션을 비활성화하고 이에 따라 오버헤드를 처리하는 시스템을 줄일 수 있습니다.

  참고 사용자 지정 네트워크 분석 정책에서 전처리기를 비활성화했지만 활성화된 침입 또는 전처리기 규칙에 대해 패킷을 차후에 평가하기 위해 시스템이 해당 전처리기를 사용해야 하는 경우, 네트워크 분석 정책 사용자 인터페이스에서는 전처리기가 여전히 비활성화 상태인 경우에도 시스템은 전처리기를 자동으로 활성화하여 사용합니다.

- 적절하다고 판단되는 경우, 포트를 지정하여 특정 전처리기 활동에 집중합니다. 예를 들어, DNS 서버 응답을 모니터링할 추가 포트를 식별할 수 있습니다.

복합적인 배포를 사용하는 고급 사용자의 경우, 다수의 네트워크 분석 정책을 생성할 수 있는데, 각각은 트래픽을 다르게 전처리하기 위해 조정된 것입니다. 그런 다음, 사용자는 다양한 보안 영역, 또는 네트워크를 사용하여 트래픽의 전처리를 제어하는 정책을 사용하는 시스템을 구성할 수 있습니다.

참고 사용자 지정 네트워크 분석 정책, 특히 다중 네트워크 분석 정책을 사용하여 전처리를 조작하는 것은 고급 작업입니다. 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 사용자는 **반드시** 주의하여 서로 보완하는 단일 패킷을 검토하는 네트워크 분석 및 침입 정책을 허용해야 합니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

사용자 지정 침입 정책의 이점

라이센스: 보호

처음에 침입 방지를 수행하도록 구성된 새로 만든 액세스 제어 정책에서 기본 작업은 모든 트래픽을 허용하지만, 먼저 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책으로 이를 검사합니다. 액세스 제어 규칙을 추가하거나 기본 작업을 변경하지 않는 한, 모든 트래픽은 침입 정책에 의해 검사됩니다. 11-6페이지의 시스템 제공 정책과 사용자 지정 정책 비교의 다이어그램을 참고하십시오.

침입 방지 배포를 사용자 정의하려면 여러 침입 정책을 만들 수 있는데, 각각은 트래픽을 검사하기 위해 서로 다르게 지정됩니다. 다음으로 어떤 정책이 어떤 트래픽을 검사하는지를 지정하는 규칙으로 액세스 제어 정책을 구성합니다. 액세스 제어 규칙은 간단하거나 복잡할 수 있으며, 보안 영역, 네트워크 또는 지리적 위치, 포트, 애플리케이션, 요청된 URL 및 사용자를 포함하는 여러 기준을 사용하여 트래픽과 일치시키고 검사합니다. 11-2페이지의 정책이 트래픽에서 침입을 검토하는 방법 이해에 있는 시나리오는 트래픽이 하나 또는 두 개의 침입 정책에 의해 검사되는 배포를 보여줍니다.

침입 정책의 주요 기능은 어느 침입 및 전처리기 규칙이 활성화되는지와 다음과 같이 이들이 구성되는 방식을 관리하는 것입니다.

- 각 침입 정책 내에서 사용자의 환경에 적용 가능한 모든 규칙이 활성화되어 있음을 확인해야 하며, 환경에 적용할 수 없는 규칙은 비활성화하여 성능을 향상시켜야 합니다. 인라인 배포에서, 악성 패킷을 삭제하거나 수정할 규칙을 지정할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.
- 새로운 익스플로잇을 탐지하거나 보안 정책을 강화하는 데 필요하다면 기존 규칙을 수정하고 새 표준 텍스트 규칙을 작성할 수 있습니다(23-1페이지의 침입 규칙의 이해와 작성 참고).

침입 정책에 만들 수 있는 다른 사용자 지정은 다음을 포함합니다.

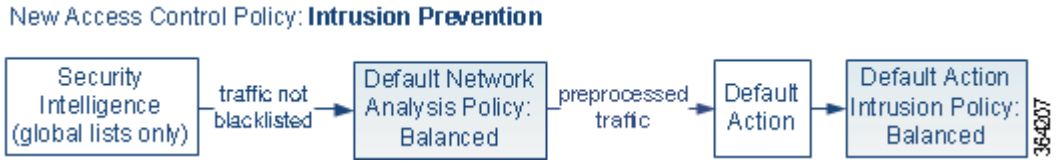
- 중요한 데이터 전처리기는 신용 카드 번호 및 ASCII 문자로 표시된 Social Security numbers(사회 보장 번호)와 같은 중요한 데이터를 탐지합니다. 특정 위협(Back Orifice 공격, 여러 포트스캔 유형 및 과도한 트래픽으로 네트워크를 마비시키려고 하는 속도 기반 공격)을 탐지하는 다른 전처리기는 네트워크 분석 정책 내에 구성됩니다. 자세한 내용은 21-1페이지의 특정 위협 탐지를 참고하십시오.
- 전역 임계값은 침입 규칙과 일치하는 트래픽이 얼마나 많이 지정된 기간 내 특정 주소 또는 주소 범위를 대상으로 하거나 특정 주소 또는 주소 범위로부터 발생하는지에 근거하여 시스템이 이벤트를 생성하도록 합니다. 이를 통해 많은 수의 이벤트로 인해 시스템이 마비되는 것을 방지할 수 있습니다. 자세한 내용은 22-1페이지의 침입 이벤트 로깅의 전역적 제한을 참고하십시오.
- 침입 이벤트 알림을 차단하고 개별 규칙 또는 전체 침입 정책에 대한 임계값을 설정하여 많은 수의 이벤트로 인해 시스템이 마비되는 것을 방지할 수 있습니다. 자세한 내용은 20-21페이지의 정책에 따른 침입 이벤트 알림 필터링을 참고하십시오.
- 침입 이벤트 이외에도, syslog 기능에 로깅을 활성화하거나 SNMP 트랩 서버에 이벤트 데이터를 보낼 수 있습니다. 정책별로 침입 이벤트 알림 제한을 지정하고, 외부 로깅 기능에 침입 이벤트 알림을 설정하며, 침입 이벤트에 외부 응답을 구성할 수 있습니다. 자세한 내용은 28-1페이지의 침입 규칙을 위한 외부 경고 구성을 참고하십시오.

사용자 지정 정책의 한계

라이센스: 보호

전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 사용자는 **반드시** 주의하여 구성이 서로 보완하는 단일 패킷을 처리하고 검토하는 네트워크 분석 및 침입 정책을 허용할 수 있도록 해야 합니다.

기본적으로, 시스템은 모든 트래픽을 전처리하도록 하나의 네트워크 분석 정책을 사용합니다. 다음 다이어그램은 인라인 침입 방지 배포에서 새로 만든 액세스 제어 정책이 트래픽을 초반에 처리하는 방식을 보여줍니다. 전처리 및 침입 방지 단계는 강조 표시됩니다.



기본 네트워크 분석 정책이 액세스 제어 정책에서 처리된 모든 트래픽의 전처리를 제어하는 방식에 유의하십시오. 초기에는 시스템이 제공한 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책이 기본값입니다.

전처리를 설정하는 간단한 방법은 기본값으로 사용자 네트워크 분석 정책을 생성하고 사용하는 것이며, 이는 11-9페이지의 사용자 지정 네트워크 분석 정책의 이점에 잘 요약되어 있습니다. 단, 사용자 지정 네트워크 분석 정책에서 전처리기를 비활성화했지만 시스템이 활성화된 침입 또는 전처리기 규칙에 대해 전처리된 패킷을 평가해야 하는 경우, 시스템이 자동으로 네트워크 분석 정책 사용자 인터페이스에서는 전처리기가 비활성화되어 있지만 시스템이 자동으로 전처리기를 활성화하여 사용합니다.

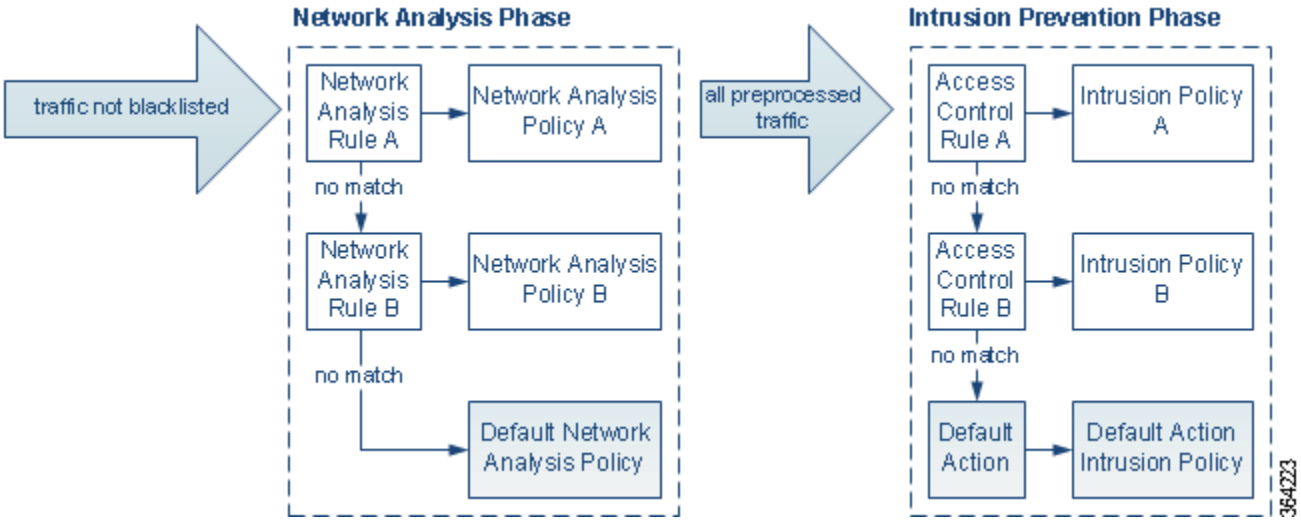
참고 전처리기를 비활성화하는 성능 이점을 가져오려면, **반드시** 전처리기를 요구하는 규칙을 활성화한 침입 정책이 없음을 확인해야 합니다.

여러 사용자 지정 네트워크 분석 정책을 사용하는 경우 추가 문제가 발생합니다. 복잡한 배포를 가진 고급 사용자의 경우, 일치하는 트래픽을 전처리하는 사용자 지정 네트워크 분석 정책을 할당하여 특정 보안 영역및 네트워크에 따라 전처리를 조정할 수 있습니다. 이를 수행하려면, 액세스 제어 정책에 사용자 지정 *네트워크 분석 규칙*을 추가합니다. 각 규칙에 규칙과 일치하는 트래픽의 전처리를 관리하는 연결된 네트워크 정책 분석이 있습니다.

팁 액세스 제어 정책의 고급 설정으로 네트워크 분석 규칙을 구성합니다. ASA FirePOWER 모듈 내 다른 유형 규칙과는 달리, 네트워크 분석 규칙은 네트워크 분석 정책에 포함되지 않고 네트워크 분석 정책을 호출합니다.

시스템은 규칙 번호로 하향식 순서로 구성된 모든 네트워크 분석 규칙에 패킷을 일치시킵니다. 어떤 네트워크 분석 규칙과도 일치하지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다. 이는 사용자에게 트래픽을 전처리하는 데 있어 많은 유연성을 제공하지만, 어느 네트워크 분석 정책이 패킷을 전처리했는지에 **상관 없이** 모든 패킷은 고유의 프로세스에서 순차적으로 액세스 제어 규칙에 일치되므로 침입 정책에 의해 잠재적인 검사에도 일치된다는 점에 유의하십시오. 즉, 특정 네트워크 분석 정책을 통해 패킷을 전처리하면 해당 패킷이 특정 침입 정책으로 검토된다고 보장되지 **않습니다**. **반드시** 신중하게 액세스 제어 정책을 구성하여 특정 패킷을 평가하는 올바른 네트워크 분석 및 침입 정책을 호출하도록 해야 합니다.

다음 다이어그램은 네트워크 분석 정책 (전처리) 선택 단계가 어떻게 해서 침입 방지 (규칙) 단계 전에 또는 별도로 발생하는지를 집중적으로 자세히 보여줍니다. 간소화를 위해 다이어그램은 파일/악성코드 검사 단계를 포함하지 않습니다. 이는 또한 기본 네트워크 분석 및 기본 작업 침입 정책을 강조 표시합니다.



이 시나리오에서 액세스 제어 정책은 두 개의 네트워크 분석 규칙 및 기본 네트워크 분석 정책으로 구성됩니다.

- Network Analysis Rule A(네트워크 분석 규칙 A)는 Network Analysis Policy A(네트워크 분석 규칙 A)로 일치하는 트래픽을 전처리합니다. 나중에 이 트래픽을 Intrusion Policy A(침입 정책 A)로 검사할 수 있습니다.
- Network Analysis Rule B(네트워크 분석 규칙 B)는 Network Analysis Policy B(네트워크 분석 규칙 B)로 일치하는 트래픽을 전처리합니다. 나중에 이 트래픽을 Intrusion Policy B(침입 정책 B)로 검사할 수 있습니다.
- 나머지 모든 트래픽은 기본 네트워크 분석 정책으로 전처리됩니다. 나중에, 이 트래픽을 액세스 제어 정책의 기본 작업과 관련된 침입 정책에 따라 검사할 수 있습니다.

시스템은 트래픽을 전처리한 후, 침입 탐지를 위해 트래픽을 검토할 수 있습니다. 다이어그램은 두 개의 액세스 제어 규칙 및 기본 작업으로 액세스 제어 정책을 보여 줍니다.

- Access Control Rule A(액세스 제어 규칙 A)가 일치하는 트래픽을 허용합니다. 다음으로 트래픽은 Intrusion Policy A(침입 정책 A)로 검사됩니다.
- Access Control Rule B(액세스 제어 규칙 B)가 일치하는 트래픽을 허용합니다. 다음으로 트래픽은 Intrusion Policy B(침입 정책 B)로 검사됩니다.
- 액세스 제어 정책의 기본 작업이 일치하는 트래픽을 허용합니다. 다음으로 트래픽은 기본 작업의 침입 정책에 의해 검사됩니다.

각 패킷의 처리는 네트워크 분석 정책과 침입 정책 쌍에 의해 제어되지만, 시스템이 사용자를 대신하여 쌍을 조정하는 것은 **아닙니다**. Network Analysis Rule A(네트워크 분석 규칙 A) 및 Access Control Rule A(액세스 제어 규칙 A)가 동일한 트래픽을 처리하지 않도록 액세스 제어 정책을 잘못 설정한 시나리오를 고려하십시오. 예를 들어, 특정 보안 영역에서 트래픽 처리를 제어하기 위해 페어링된 정책을 의도할 수 있지만 두 규칙의 조건에서 서로 다른 영역을 잘못 사용하는 것입니다. 그러면 트래픽이 잘못 전처리될 수 있습니다. 따라서, 네트워크 분석 규칙 및 사용자 지정 정책을 사용하여 전처리를 조작하는 것은 **고급** 작업입니다.

단일 연결의 경우, 시스템은 액세스 제어 규칙에 앞서 네트워크 분석 정책을 선택하지만, 일부 전처리(특히 애플리케이션 레이어 전처리)는 액세스 제어 규칙 선택 이후에 발생한다는 점에 유의하십시오. 이는 사용자 지정 네트워크 분석 정책에서 전처리를 구성하는 방식에 영향을 주지 **않습니다**.

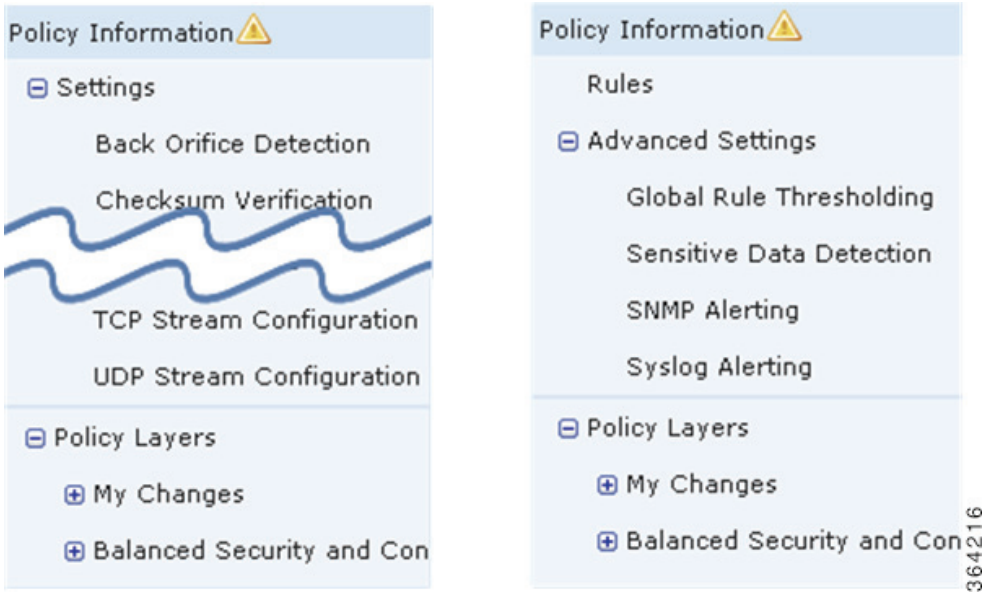
탐색 패널 사용

라이센스: 보호

네트워크 분석 및 침입 정책은 유사한 사용자 인터페이스를 사용하여 구성을 변경하고 그 내용을 저장합니다. 다음을 참고하십시오.

- 14-4페이지의 네트워크 분석 정책 수정
- 19-4페이지의 침입 정책 수정

탐색 패널은 정책 유형 중 하나를 수정할 때 사용자 인터페이스의 왼쪽에 나타납니다. 다음 그래픽은 네트워크 분석 정책(왼쪽) 및 침입 정책(오른쪽) 탐색 패널을 표시합니다.



분계선이 정책 설정으로 연결되는 링크로 탐색 패널을 분리합니다. 정책 설정은 정책 레이어와의 직접 상호 작용이 있는 것(아래) 또는 해당 상호 작용이 없는 것(위)으로 구성할 수 있습니다. 모든 설정 페이지로 이동하려면 탐색 패널에서 해당 이름을 클릭합니다. 탐색 패널에서 항목을 어둡게 하는 것은 현재 설정 페이지를 강조 표시합니다. 예를 들어, Policy Information(정책 정보) 위에 있는 그림에서 페이지는 탐색 패널의 오른쪽에 표시됩니다.

정책 정보

Policy Information(정책 정보) 페이지는 일반적으로 사용되는 설정을 위한 구성 옵션을 제공합니다. 위에 표시된 네트워크 분석 정책 패널의 그림과 같이, 정책이 저장되지 않은 변경 사항을 포함할 때 정책 변경 아이콘(⚠)이 탐색 패널의 **Policy Information(정책 정보)** 옆에 나타납니다. 변경 사항을 저장하면 아이콘은 사라집니다.

규칙(침입 정책만)

침입 정책에서 Rules(규칙) 페이지를 통해 공유 객체 규칙, 표준 텍스트 규칙, 그리고 전처리기 규칙의 규칙 상태 및 기타 설정을 구성할 수 있습니다. 자세한 내용은 20-1페이지의 규칙을 사용한 침입 정책 조정을 참고하십시오.

설정(네트워크 분석 정책) 및 고급 설정(침입 정책)

네트워크 분석 정책에서 Settings(설정) 페이지를 통해 전처리기를 활성화하거나 비활성화하고 전처리기 구성 페이지에 액세스할 수 있습니다. **Settings(설정)** 링크를 확장하여 정책의 모든 활성화된 전처리기를 위한 개별 구성 페이지로 연결되는 하위 링크를 표시합니다. 자세한 내용은 14-6페이지의 네트워크 분석 정책에서 전처리기 구성을 참고하십시오.

침입 정책에서 Advanced Settings(고급 설정) 페이지를 통해 고급 설정 및 해당 고급 설정을 위한 액세스 구성 페이지를 활성화하거나 비활성화할 수 있습니다. **Advanced Settings(고급 설정)** 링크를 확장하여 정책에서 활성화된 모든 고급 설정을 위한 개별 구성 페이지로 연결되는 하위 링크를 표시합니다. 자세한 내용은 19-7페이지의 침입 정책 내 고급 설정 구성을 참고하십시오.

정책 레이어

Policy Layers(정책 레이어) 페이지는 네트워크 분석 또는 침입 정책을 구성하는 레이어에 대한 요약을 표시합니다. Policy Layers(정책 레이어) 페이지를 확장하여 정책의 레이어를 위한 요약 페이지로 연결되는 하위 링크를 표시합니다. 각 레이어 하위 링크를 확장하면 레이어에서 활성화된 모든 규칙, 전처리기 또는 고급 설정에 대한 구성 페이지로 연결되는 하위 링크를 표시합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

문제 해결 및 정책 변경 사항 커밋

라이센스: 보호

네트워크 분석 또는 침입 정책을 수정할 때, 시스템이 이들을 인식하기 전에 변경 사항을 저장(또는 *커밋*)해야 합니다.

참고 저장한 후, 변경 사항을 반영하려면 네트워크 분석 또는 침입 정책을 적용해야 합니다. 저장하지 않고 정책을 적용하면, 시스템은 가장 최근에 저장된 구성을 사용합니다. 침입 정책은 개별적으로 다시 적용할 수 있지만, 네트워크 분석 정책은 상위 액세스 제어 정책과 함께 적용됩니다.

수정 문제 해결

Network Analysis Policy(네트워크 분석 정책) 페이지 및 Intrusion Policy(침입 정책) 페이지는 각 정책에 저장되지 않은 변경 사항이 있는지 표시합니다. 14-4페이지의 네트워크 분석 정책 수정 및 19-4페이지의 침입 정책 수정을 참고하십시오.

Cisco는 한 사람이 한 번에 하나의 정책을 수정할 것을 권장합니다. 여러 사용자 인터페이스 인스턴스를 통해 동일한 사용자로 동일한 네트워크 분석 또는 침입 정책을 수정하는 경우, 하나의 인스턴스에 대한 변경 사항을 저장하면, 다른 인스턴스에 대한 변경 사항을 저장할 수 없습니다.

구성 종속성 해결

특정 분석을 수행하기 위해, 많은 전처리기와 침입 규칙은 트래픽이 특정 방법으로 먼저 디코딩되거나 전처리되도록, 또는 다른 종속성을 갖도록 요청합니다. 네트워크 분석 또는 침입 정책을 저장하면, 시스템은 자동으로 필수 설정을 활성화하거나 다음과 같이 비활성화된 설정은 트래픽에 영향을 미치지 못함을 경고합니다.

- SNMP 알림 규칙을 추가했지만 SNMP 경고를 구성하지 않은 경우 침입 정책을 저장할 수 없습니다. SNMP 경고를 설정하거나 규칙 경고를 비활성화한 후 다시 저장해야 합니다.

- 침입 정책이 활성화된 중요한 데이터를 포함하지만 중요한 데이터 전처리를 활성화하지 않은 경우 침입 정책을 저장할 수 없습니다. 시스템이 전처리를 활성화하고 정책을 저장할 수 있도록 하거나, 규칙을 비활성화하고 다시 저장할 수 있도록 해야 합니다.
- 네트워크 분석 정책에 필요한 전처리기를 비활성화한 경우에도, 여전히 정책을 저장할 수 있습니다. 그러나, 전처리기가 사용자 인터페이스에서 비활성화되어 있는 경우에도 시스템은 자동으로 현재의 설정으로 비활성화된 전처리기를 사용합니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.
- 네트워크 분석 정책에서 인라인 모드를 비활성화하지만 Inline Normalization(인라인 표준화) 전처리기를 활성화한 경우, 여전히 정책을 저장할 수 있습니다. 그러나 시스템은 표준화 설정이 무시될 것임을 경고합니다. 인라인 모드를 비활성화해도 전처리기가 트래픽을 수정하거나 차단할 수 있는 다른 설정을 시스템이 무시하는 결과를 야기하며, 여기에는 체크섬 유효성 검증 및 속도 기반 공격 방지가 포함됩니다. 자세한 내용은 14-5페이지의 전처리기의 영향을 받도록 트래픽 설정 및 17-6페이지의 인라인 트래픽 표준화를 참고하십시오.

정책 변경 커밋, 삭제 및 캐싱

네트워크 분석 또는 침입 정책을 수정할 때 변경 사항을 저장하지 않고 정책 편집기를 종료할 경우, 시스템은 해당 변경 사항을 캐시합니다. 변경 사항은 시스템에서 로그아웃하거나 시스템 충돌이 발생할 때도 캐시됩니다. 시스템 캐시는 네트워크 분석 하나와 침입 정책 하나에 대한 저장되지 않은 변경 사항을 저장할 수 있습니다. 동일한 유형의 다른 정책을 수정하려면 먼저 변경 사항을 커밋하거나 삭제해야 합니다. 시스템은 변경 내용을 처음 정책에 저장하지 않고 다른 정책을 수정할 때 또는 침입 규칙 업데이트를 가져올 때 캐시된 변경 사항을 삭제합니다.

네트워크 분석 또는 침입 정책 편집기의 Policy Information(정책 정보) 페이지에서 정책 변경 사항을 커밋하거나 폐기할 수 있습니다(14-4페이지의 네트워크 분석 정책 수정 및 19-4페이지의 침입 정책 수정 참고).

다음 표에서는 네트워크 분석 침입 정책에 변경 내용을 저장하는 방법 또는 폐기하는 방법에 대해 요약합니다.

표 11-1 네트워크 분석 또는 침입 정책에 변경 사항 커밋

목적	Policy Information(정책 정보) 페이지에서 수행할 수 있는 작업
정책에 변경 사항 저장하기	**Commit Changes(변경 사항 커밋)**를 클릭하면 됩니다. 또는, 코멘트를 입력합니다. **OK(확인)**를 클릭하여 계속 커밋합니다.
저장되지 않은 모든 변경 사항 삭제하기	**Discard Changes(변경 사항 삭제)**를 클릭한 다음, **OK(확인)**를 클릭하여 변경 사항을 삭제하고 Intrusion Policy(침입 정책) 페이지로 이동하면 됩니다. 변경 사항을 삭제하지 않으려면, **Cancel(취소)**을 클릭하여 Policy Information(정책 정보) 페이지로 돌아갑니다.
정책 종료 및 변경 사항 캐싱하기	모든 메뉴를 선택하거나 다른 페이지로 이동하는 다른 경로를 선택하면 됩니다. 종료 시 프롬프트가 표시되면 **Leave page(페이지에서 나가기)**를 클릭하거나, 고급 편집기에 남으려면 **Stay on page(페이지에 남기)**를 클릭합니다.

12장 네트워크 분석 또는 침입 정책에서 레이어 사용

ASA FirePOWER 모듈이 많은 대규모 조직은 다양한 부서, 사업부 또는 경우에 따라서는 다양한 기업의 고유한 요구사항을 지원하기 위해 다수의 침입 정책 및 네트워크 분석 정책을 보유할 수 있습니다. 두 정책 유형의 구성은 여러 정책을 효율적으로 관리하기 위해 사용할 수 있는 *레이어*라는 구성 요소에 포함됩니다.

침입 및 네트워크 분석 정책의 레이어는 기본적으로 동일한 방식으로 작동합니다. 의식적으로 레이어를 사용하지 않고 각 정책 유형을 만들고 수정할 수 있습니다. 정책 구성을 수정할 수 있으며, 정책에 사용자 레이어를 추가하지 않은 경우 시스템은 초기 이름이 *My Changes(내 변경 사항)*인 구성 가능한 단일 레이어에 변경 사항을 자동으로 포함합니다. 선택적으로, 최대 200개의 레이어를 추가할 수 있으며 여기에서 설정의 조합을 구성할 수 있습니다. 사용자 레이어를 복사, 병합, 이동 및 삭제할 수 있으며 가장 중요한 기능으로는 개별 사용자 레이어를 동일한 유형의 다른 정책과 공유할 수 있다는 점입니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 12-1페이지의 레이어 스택의 이해는 기본 정책을 이루는 사용자 구성 가능한 내장 레이어에 대해 설명합니다.
- 12-5페이지의 레이어 관리는 정책에서 레이어를 사용하는 방법에 대해 설명합니다.

레이어 스택의 이해

라이센스: 보호

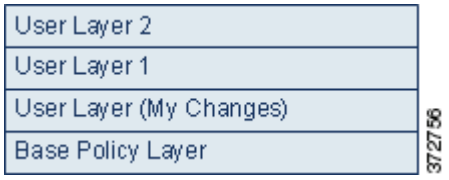
레이어를 추가하지 않은 네트워크 분석 또는 침입 정책에는 내장된 읽기 전용 기반 정책 레이어 및 초기 이름이 My Changes(내 변경 사항)인 사용자 구성 가능한 단일 레이어가 포함되어 있습니다. 사용자 구성 가능한 레이어를 복사, 병합, 이동 또는 삭제할 수 있으며, 사용자 구성 가능한 모든 레이어를 동일한 유형의 다른 정책과 공유할 수 있습니다.

각 정책 레이어에는 네트워크 분석 정책의 모든 프리프로세서에 대한 또는 침입 정책의 모든 침입 규칙 및 고급 설정에 대한 완전한 구성이 포함되어 있습니다. 최하위 기반 정책 레이어에는 정책 생성 시 선택한 기반 정책의 모든 설정이 포함되어 있습니다. 상위 레이어의 설정이 하위 레이어의 동일한 설정에 비해 우선권을 갖습니다. 레이어에 명시적으로 설정되지 않은 기능은 명시적으로 설정된 다음 최상위 레이어에서 설정을 *상속*합니다.

시스템은 레이어를 *병합*합니다. 즉, 네트워크 트래픽을 처리할 때 모든 설정의 누적된 효과만 적용합니다.

팁 기반 정책의 기본 설정에만 전적으로 기반하는 침입 또는 네트워크 분석 정책을 생성할 수 있.

다음 그림에서는 레이어 스택의 예를 보여줍니다. 여기에는 기반 정책 레이어 및 초기 My Changes(내 변경 사항) 레이어 외에 두 개의 사용자 구성 가능한 레이어인 *User Layer 1* 및 *User Layer 2*가 포함되어 있습니다. 이 그림에서, 추가하는 사용자 구성 가능한 각 레이어는 처음에 스택의 최상위 레이어에 배치됩니다. 따라서 그림의 User Layer 2는 스택에서 가장 마지막에 추가된 것이며 최상위 레이어입니다.



여러 레이어로 작업할 경우 다음 사항에 유의해야 합니다.

- 정책에서 최상위 레이어가 읽기 전용 레이어이거나 12-9페이지의 정책 간 레이어 공유에 설명된 대로 공유 레이어인 경우, 사용자가 다음 중 하나를 수행하면 시스템은 사용자 구성 가능한 레이어를 침입 정책에서 최상위 레이어로 자동으로 추가합니다.
  - 침입 정책 Rules(규칙) 페이지에서 규칙 작업(즉, 규칙 상태, 이벤트 필터링, 동적 상태 또는 알림) 수정. 자세한 내용은 20-1페이지의 규칙을 사용한 침입 정책 조정을 참고하십시오.
  - 프리프로세서, 침입 규칙 또는 고급 설정의 활성화, 비활성화 또는 수정

  시스템에서 추가한 레이어의 모든 설정은 상속됩니다. 단, 변경 사항이 새 레이어가 되는 경우는 예외입니다.
- 최상위 레이어가 공유 레이어인 경우 시스템은 사용자가 다음 작업 중 하나를 수행할 때 레이어를 추가합니다.
  - 최상위 레이어를 다른 정책과 공유
  - 공유 레이어를 정책에 추가
- 규칙 업데이트가 정책을 수정하도록 허용하는지와 상관없이, 규칙 업데이트의 변경 사항은 레이어에서 사용자가 수행한 변경 사항을 재정의하지 않습니다. 이는 규칙 업데이트의 변경 사항이 기반 정책에서 이루어지며, 이것이 기반 정책 레이어의 기본 설정을 결정하기 때문입니다. 사용자 변경 사항은 항상 상위 레이어에서 이루어지므로, 규칙 업데이트가 기반 정책에 대해 수행하는 모든 변경 사항을 재정의합니다. 자세한 내용은 35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기를 참고하십시오.

자세한 내용은 12-2페이지의 기본 레이어의 이해를 참고하십시오.

기본 레이어의 이해

라이센스: 보호

침입 또는 네트워크 분석 정책의 기반 레이어(기반 정책이라고도 함)는 정책의 모든 구성에 대한 기본 설정을 정의하며 정책에서 최하위 레이어입니다. 새 정책을 생성할 때 새 레이어를 추가하지 않은 채 설정을 변경하면 변경 사항은 My Changes(내 변경 사항) 레이어에 저장되며 기반 정책의 설정을 재정의합니다(그러나 변경하지는 않음).

자세한 내용은 다음 섹션을 참고하십시오.

- 12-3페이지의 시스템 제공 기반 정책의 이해
- 12-3페이지의 사용자 지정 기본 정책의 이해
- 12-4페이지의 기본 정책 변경
- 12-4페이지의 규칙 업데이트를 통해 시스템이 제공하는 기본 정책 수정 허용

시스템 제공 기반 정책의 이해

라이센스: 보호

Cisco에서는 ASA FirePOWER 모듈과 함께 여러 쌍의 네트워크 분석 및 침입 정책을 제공합니다. 시스템이 제공하는 네트워크 분석 및 침입 정책을 사용하여 Cisco VRT(취약성 연구단)의 경험을 활용할 수 있습니다. VRT는 이 정책에 대해, 침입 및 전처리기 규칙 상태를 설정할 뿐만 아니라, 전처리기 및 다른 고급 설정에 대한 초기 구성을 제공합니다. 시스템이 제공하는 정책을 있는 그대로 사용할 수도 있고, 이를 맞춤형 정책을 위한 기반으로 사용할 수도 있습니다.

시스템이 제공하는 정책을 기반으로 사용할 경우, 규칙 업데이트를 가져오면 기반 정책의 설정을 수정할 수 있습니다. 그러나, 사용자 지정 정책을 구성하여 시스템 제공 기본 정책을 자동으로 변경하지 않도록 할 수도 있습니다. 이를 통해 규칙 업데이트를 가져오는 것과 별개로 시스템 제공 기본 정책을 수동으로 업데이트할 수 있습니다. 어떤 경우든, 규칙 업데이트가 기반 정책에 대해 수행하는 변경 사항은 My Changes(내 변경 사항) 또는 다른 레이어의 설정을 변경하거나 재정의하지 않습니다. 자세한 내용은 12-4페이지의 규칙 업데이트를 통해 시스템이 제공하는 기본 정책 수정 허용을 참고하십시오.

시스템이 제공하는 침입 및 네트워크 분석 정책은 이름은 유사하지만 다른 구성을 포함합니다. 예를 들어, Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트될 수 있습니다. 자세한 내용은 11-7페이지의 시스템 제공 정책의 이해를 참고하십시오.

사용자 지정 기본 정책의 이해

라이센스: 보호

네트워크 분석 또는 침입 정책 내 기본 정책으로 시스템 제공 정책을 사용하지 않으려는 경우, 사용자 지정 정책을 기본으로 사용할 수 있습니다. 사용자 지정 정책의 설정을 조정하여 가장 중요하다고 생각되는 방식으로 트래픽을 검사할 수 있으며, 이에 따라 디바이스의 성능과 디바이스가 생성하는 이벤트에 효과적으로 대응하는 능력 모두를 향상시킬 수 있습니다.

최대 다섯 개의 사용자 지정 정책을 묶을 수 있는데, 다섯 중 넷은 이전에 만들어진 다른 넷 중 하나를 기본 정책으로 사용하는 것이며, 다섯 번째는 반드시 시스템이 제공하는 정책을 기본 정책으로 사용해야 합니다.

다른 정책에 대한 기본으로 사용하는 사용자 지정 정책을 변경하면 해당 변경 사항은 자동적으로 기본 정책을 사용하는 정책의 기본 설정으로 사용됩니다. 또한 모든 정책은 정책 체인 내 궁극적인 기본으로 시스템이 제공하는 정책을 보유하기 때문에 사용자 지정 기본 정책을 사용하는 경우에도 규칙 업데이트를 가져오는 것은 사용자 정책에 영향을 줄 수 있습니다. 체인 내 첫 번째 사용자 지정 정책(시스템이 제공하는 정책을 기본으로 사용하는 것)은 규칙 업데이트가 해당 기본 정책을 수정하는 것을 허용하며, 사용자 정책에도 영향을 줄 수 있습니다. 이 설정 변경에 대한 자세한 내용은 12-4페이지의 규칙 업데이트를 통해 시스템이 제공하는 기본 정책 수정 허용을 참조하십시오.

수행 방식에 상관 없이 사용자 기본 정책을 변경하면 해당 변경 사항은 규칙 업데이트에 의한 것이든 또는 기본 정책으로 사용하는 사용자 지정 정책을 수정하는 경우에 의해서든 사용자의 My Changes(내 변경 사항) 또는 다른 모든 레이어 내 설정을 변경하거나 대체하지 않습니다.

기본 정책 변경

라이센스: 보호

네트워크 분석 또는 침입 정책에 대해 다른 기반 정책을 선택할 수 있으며, 선택적으로 상위 레이어의 수정에 영향을 주지 않은 채 규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 허용할 수 있습니다.

기반 정책을 변경하려면 다음을 수행합니다.

단계 1 정책을 수정하는 동안 탐색 패널에서 **Policy Information(정책 정보)**을 클릭합니다.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 2 **Base Policy(기반 정책)** 드롭다운 목록에서 기반 정책을 선택합니다.

단계 3 선택적으로 시스템 제공 기반 정책을 선택하는 경우, **Manage Base Policy(기반 정책 관리)**를 클릭하여 침입 규칙 업데이트가 기반 정책을 자동으로 수정할 수 있는지 여부를 지정합니다.

자세한 내용은 12-4페이지의 규칙 업데이트를 통해 시스템이 제공하는 기본 정책 수정 허용을 참고하십시오.

단계 4 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

규칙 업데이트를 통해 시스템이 제공하는 기본 정책 수정 허용

라이센스: 보호

가져온 규칙 업데이트는 시스템 제공 정책에 수정된 네트워크 분석 프리프로세서 설정, 수정된 침입 정책 고급 설정, 새로운/업데이트된 침입 규칙, 기존 규칙의 수정된 상태 등을 제공합니다. 또한 규칙 업데이트는 규칙을 삭제하고 새로운 규칙 카테고리와 기본 변수를 제공할 수 있습니다. 자세한 내용은 35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기를 참고하십시오.

규칙 업데이트는 항상 프리프로세서, 고급 설정 및 규칙에 대한 변경 사항으로 시스템 제공 정책을 수정합니다. 기본 변수 및 규칙 카테고리를 변경하면 시스템 수준에서 처리됩니다. 자세한 내용은 12-3페이지의 시스템 제공 기반 정책의 이해를 참고하십시오.

시스템 제공 정책을 기반 정책으로 사용하는 경우 규칙 업데이트(이 경우 시스템 제공 정책의 복사본)가 기반 정책을 수정하도록 허용할 수 있습니다. 규칙 업데이트가 기반 정책을 업데이트하는 것을 허용할 경우, 새로운 규칙 업데이트는 기반 정책으로 사용하는 시스템 제공 정책에 대한 변경 사항과 동일하게 기반 정책을 변경합니다. 해당 설정을 수정하지 않은 경우 기반 정책의 설정이 현재 정책의 설정을 결정합니다. 그러나 규칙 업데이트는 현재 정책에서 수행하는 변경 사항을 재정의하지 않습니다.

규칙 업데이트를 통해 기반 정책을 업데이트할 수 없는 경우, 하나 이상의 규칙 업데이트를 가져온 후 수동으로 기반 정책을 업데이트할 수 있습니다.

침입 정책의 규칙 상태와 상관없이 또는 규칙 업데이트가 기반 침입 정책을 업데이트하도록 허용하는지 여부와 상관없이, 규칙 업데이트는 항상 VRT가 삭제하는 침입 규칙을 삭제합니다. 변경 사항을 네트워크 트래픽에 다시 적용할 때까지, 현재 적용된 침입 정책의 규칙은 다음과 같이 작동합니다.

- 비활성화된 규칙은 비활성화 상태를 유지합니다.
- Generate Events(이벤트 생성)로 설정된 규칙은 트리거되었을 때 계속해서 이벤트를 생성합니다.
- Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙은 트리거되었을 때 계속해서 이벤트를 생성하고 위반 패킷을 삭제합니다.

규칙 업데이트는 다음 조건이 모두 충족되지 않으면 사용자 지정 기본 정책을 수정하지 않습니다.

- 규칙 업데이트를 통해 상위 정책의 시스템이 제공하는 기본 정책, 즉 사용자 지정 기본 정책을 생성한 정책을 수정할 수 있습니다.
- 상위 기본 정책 내 해당 설정을 대체하는 상위 정책을 변경하지 않았습니다.

두 조건이 충족된 경우, 상위 정책을 저장하면 규칙 업데이트 내 변경 사항이 하위 정책, 즉, 사용자 지정 기본 정책을 사용하는 정책에 전달됩니다.

예를 들어 규칙 업데이트가 이전에 비활성화된 침입 규칙을 활성화하여 상위 침입 정책의 규칙 상태를 수정하지 않은 경우, 상위 정책을 저장하면 수정된 규칙 상태가 기반 정책에 전달됩니다.

마찬가지로, 규칙 업데이트가 기본 프리프로세서 설정을 수정하고 상위 네트워크 분석 정책에서 설정을 수정하지 않은 경우, 상위 정책을 저장하면 수정된 설정이 기반 정책에 전달됩니다.

자세한 내용은 12-4페이지의 기본 정책 변경을 참고하십시오.

규칙 업데이트를 통해 시스템 제공 기반 정책을 수정하려면 다음을 수행합니다.

단계 1 시스템 제공 정책을 기반 정책으로 사용하는 정책을 수정하는 동안, 탐색 패널에서 **Policy Information(정책 정보)**을 클릭합니다.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 2 **Manage Base Policy(기반 정책 관리)**를 클릭합니다.

Base Policy(기반 정책) 요약 페이지가 나타납니다.

단계 3 **Update when a new Rule Update is installed(새 규칙 업데이트가 설치된 경우 업데이트)** 확인란을 선택하거나 선택 취소합니다.

확인란을 취소하고 정책을 저장한 다음 규칙 업데이트를 가져오면 Base Policy(기반 정책) 요약 페이지에 **Update Now(지금 업데이트)** 버튼이 나타나고, 페이지의 상태 메시지가 업데이트되어 정책이 최신 상태가 아님을 알립니다. 선택적으로, **Update Now(지금 업데이트)**를 클릭하여 가장 최근에 가져온 규칙 업데이트의 변경 사항으로 기반 정책을 업데이트할 수 있습니다.

단계 4 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

레이어 관리

라이센스: 보호

Policy Layers(정책 레이어) 페이지는 네트워크 분석 또는 침입 정책에 대한 완전한 레이어 스택을 요약하는 단일 페이지를 제공합니다. 이 페이지에서 공유 및 비공유 레이어를 추가하고, 레이어를 복사, 병합, 이동 및 삭제하고, 각 레이어의 요약 페이지에 액세스하고, 각 레이어 내에서 활성화, 비활성화 및 재정의된 구성에 대한 구성 페이지에 액세스할 수 있습니다.

각 레이어에 대해 다음 정보를 볼 수 있습니다.

- 레이어가 내장 레이어인지, 공유된 사용자 레이어인지, 공유되지 않은 사용자 레이어인지 여부
- 가장 높은(효과적인) 프리프로세서 또는 고급 설정 구성이 포함되어 있는 레이어(기능 이름별)
- 침입 정책에서, 상태가 레이어에 설정되어 있고 각 규칙 상태에 대해 규칙 수가 설정된 침입 규칙의 수

각 레이어의 요약에 있는 기능 이름은 어떤 구성이 레이어에서 활성화, 비활성화, 재정의 또는 상속되었는지를 다음과 같이 나타냅니다.

기능 상태	기능 이름
레이어에서 활성화됨	일반 텍스트로 작성됨
레이어에서 비활성화됨	삭제됨
상위 레이어에서 구성에 의해 대체됨	기울임 꼴 텍스트로 작성됨
하위 레이어에서 상속됨	없음

이 페이지는 또한 활성화된 모든 프리프로세서(네트워크 분석) 또는 고급 설정(침입), 침입 정책, 침입 규칙의 최종 효과에 대한 요약을 제공합니다.

다음 표에는 Policy Layers(정책 레이어) 페이지에서 사용할 수 있는 작업이 나열되어 있습니다.

표 12-1 네트워크 분석 및 침입 정책 레이어 구성 작업

목적	방법
Policy Information(정책 정보) 페이지 표시	**Policy Summary(정책 요약)**를 클릭합니다. Policy Information(정책 정보) 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 20-1페이지의 규칙을 사용한 침입 정책 조정, 14-1페이지의 네트워크 분석 정책 시작하기, 및 19-1페이지의 침입 정책 시작하기를 참조하십시오.
레이어의 요약 페이지 표시	레이어에 대한 행에서 레이어 이름을 클릭하거나, 사용자 레이어 옆에 있는 수정 아이콘( )을 클릭합니다. 공유 레이어에 대한 읽기 전용 요약 페이지에 액세스하려면 보기 아이콘( )을 클릭할 수도 있습니다. 레이어에 대한 요약 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 12-9페이지의 정책 간 레이어 공유, 12-14페이지의 레이어 내 전처리기 및 고급 설정 구성 및 12-11페이지의 레이어 내 침입 규칙 구성을 참조하십시오.
레이어 레벨 프리프로세서 또는 고급 설정 구성 페이지에 액세스	레이어에 대한 행에서 기능 이름을 클릭합니다. 구성 페이지는 기반 정책 및 공유 레이어에 있는 읽기 전용 페이지입니다. 자세한 내용은 12-14페이지의 레이어 내 전처리기 및 고급 설정 구성을 참고하십시오.
규칙 상태 유형으로 필터링된 레이어 레벨 규칙 구성 페이지에 액세스	레이어에 대한 요약에서 이벤트 삭제 및 생성 아이콘( ),이벤트 생성 아이콘( ) 또는 비활성화에 대한 아이콘( )을 클릭합니다. 선택한 규칙 상태로 설정된 규칙이 레이어에 포함되지 않는 경우 규칙이 표시되지 않습니다.
레이어를 정책에 추가	12-7페이지의 레이어 추가를 참조하십시오.
다른 정책에서 공유 레이어 추가	12-9페이지의 정책 간 레이어 공유를 참고하십시오.
레이어의 이름 또는 설명 변경	12-7페이지의 레이어의 이름 및 설명 변경을 참고하십시오.
레이어 이동, 복사 또는 삭제	12-8페이지의 레이어의 이동, 복사 및 삭제를 참고하십시오.
레이어를 그 아래에 있는 다음 레이어로 병합	12-9페이지의 레이어 병합을 참고하십시오.

Policy Layers(정책 레이어) 페이지를 사용하려면 다음을 수행합니다.

단계 1 정책을 수정하는 동안 탐색 패널에서 **Policy Layers(정책 레이어)**를 클릭합니다.

Policy Layers(정책 레이어) 요약 페이지가 나타납니다.

단계 2 네트워크 분석 및 침입 정책 레이어 구성 작업 표의 작업을 수행할 수 있습니다.

단계 3 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

레이어 추가

라이센스: 보호

네트워크 분석 또는 침입 정책에 최대 200개의 레이어를 추가할 수 있습니다. 레이어를 추가하면 정책에서 최상위 레이어로 나타납니다. 초기 상태는 모든 기능에 대한 Inherit(상속) 상태이며, 침입 정책에 이벤트 필터링, 동적 상태 또는 알림 규칙 작업이 설정되어 있지 않습니다.

네트워크 분석 또는 침입 정책에 레이어를 추가하려면 다음을 수행합니다.

단계 1 정책을 수정하는 동안 탐색 패널에서 **Policy Layers(정책 레이어)**를 클릭합니다.

Policy Layers(정책 레이어) 페이지가 나타납니다.

단계 2 User Layers(사용자 레이어) 옆에 있는 레이어 추가 아이콘( )을 클릭합니다.

Add Layer(레이어 추가) 팝업 창이 나타납니다.

단계 3 고유한 레이어 **Name(이름)**을 입력하고 **OK(확인)**를 클릭합니다.

새 레이어는 User Layers(사용자 레이어) 아래의 맨 위 레이어로 나타납니다.

단계 4 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

레이어의 이름 및 설명 변경

라이센스: 보호

네트워크 분석 또는 침입 정책에서 사용자 구성 가능한 레이어의 이름을 변경할 수 있으며, 선택적으로 레이어를 수정할 때 표시되는 설명을 추가 또는 수정할 수 있습니다.

레이어의 이름을 변경하고 설명을 추가 또는 수정하려면 다음을 수행합니다.

단계 1 정책을 수정하는 동안 탐색 패널에서 **Policy Layers(정책 레이어)**를 클릭합니다.

Policy Layers(정책 레이어) 페이지가 나타납니다.

단계 2 수정하려는 사용자 레이어 옆에 있는 수정 아이콘( )을 클릭합니다.

레이어에 대한 요약 페이지가 나타납니다.

단계 3 다음과 같은 작업을 수행할 수 있습니다.

- 레이어 **Name(이름)**을 수정합니다.
- 레이어 **Description(설명)**을 추가하거나 수정합니다.

단계 4 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

레이어의 이동, 복사 및 삭제

라이센스: 보호

네트워크 분석 또는 침입 정책에서, 초기 My Changes(내 변경 사항) 레이어를 포함하여 사용자 레이어를 복사, 이동 또는 삭제할 수 있습니다. 다음과 같은 고려 사항을 참고하십시오,

- 레이어를 복사하면 복사본이 최상위 레이어로 나타납니다.
- 공유 레이어를 복사하면 비공유 복사본이 생성되며, 선택적으로 이를 다른 정책과 공유할 수 있습니다.
- 공유 레이어는 삭제할 수 없습니다. 공유가 활성화되었지만 다른 정책과 공유되지 않은 레이어는 공유 레이어가 아닙니다.

레이어를 복사, 이동 또는 삭제하려면 다음을 수행합니다.

단계 1 정책을 수정하는 동안 탐색 패널에서 **Policy Layers(정책 레이어)**를 클릭합니다.

Policy Layers(정책 레이어) 페이지가 나타납니다.

단계 2 다음과 같은 작업을 수행할 수 있습니다.

- 레이어를 복사하려면 복사할 레이어에 대한 복사 아이콘( )을 클릭합니다.

  페이지가 새로 고쳐지고 레이어의 복사본이 최상위 레이어로 나타납니다.
- User Layers(사용자 레이어) 페이지 영역 내에서 레이어를 위나 아래로 이동하려면, 레이어 요약에서 열린 영역을 클릭하고 위치 화살표( )가 이동하려는 레이어의 위나 아래에 있는 선을 가리킬 때까지 끕니다.

  화면이 새로 고쳐지고 레이어가 새 위치에 나타납니다.
- 레이어를 삭제하려면 삭제할 레이어에 대한 삭제 아이콘( )을 클릭하고 **OK(확인)**를 클릭합니다.

  페이지가 새로 고쳐지고 레이어가 삭제됩니다.

단계 3 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

레이어 병합

라이센스: 보호

네트워크 분석 또는 침입 정책의 사용자 구성 가능한 레이어를 아래에 있는 다음 사용자 레이어와 병합할 수 있습니다. 병합된 레이어는 각 레이어의 고유한 설정을 모두 보유하며, 두 레이어 모두 동일한 프리프로세서에 대한 설정, 침입 규칙 또는 고급 설정을 포함한 경우 상위 레이어의 설정을 수용합니다. 병합된 레이어는 하위 레이어의 이름을 유지합니다.

다른 정책에 추가한 공유 레이어를 생성하는 정책에서, 공유 레이어 바로 위의 비공유 레이어는 공유 레이어와 병합할 수 있지만, 아래에 있는 비공유 레이어는 공유 레이어와 병합할 수 없습니다.

또 다른 정책에서 생성한 공유 레이어를 추가하는 정책에서는 공유 레이어를 바로 아래에 있는 비공유 레이어와 병합할 수 있으며 이 경우 그 결과 레이어는 더 이상 공유되지 않습니다. 비공유 레이어는 그 아래에 있는 공유 레이어와 병합할 수 없습니다.

사용자 레이어를 그 아래의 사용자 레이어와 병합하려면 다음을 수행합니다.

단계 1 정책을 수정하는 동안 탐색 패널에서 **Policy Layers(정책 레이어)**를 클릭합니다.

Policy Layers(정책 레이어) 페이지가 나타납니다.

단계 2 두 레이어 중 위의 레이어에 있는 병합 아이콘( )을 클릭하고 **OK(확인)**를 클릭합니다.

페이지가 새로 고쳐지고 레이어가 그 아래에 있는 레이어와 병합됩니다.

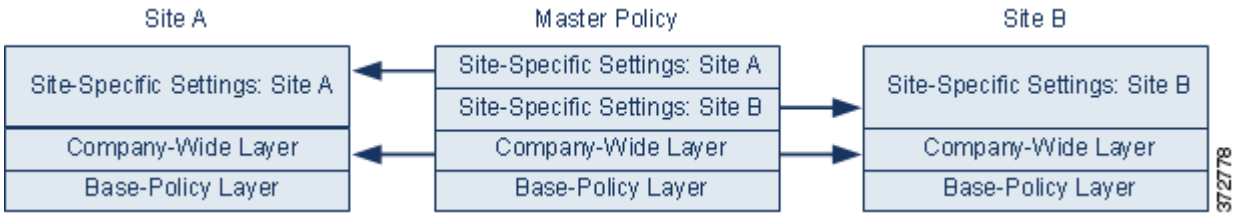
단계 3 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

정책 간 레이어 공유

라이센스: 보호

사용자 공유 가능한 레이어를 동일한 유형(침입 또는 네트워크 분석)의 다른 정책과 공유할 수 있습니다. 공유 레이어 내에서 구성을 수정하고 변경 사항을 커밋하면, 시스템은 공유 레이어를 사용하는 모든 정책을 업데이트하고 영향받는 모든 정책의 목록을 제공합니다. 레이어를 생성한 정책에 있는 공유 레이어 기능 구성만 수정할 수 있습니다.

다음 그림은 사이트별 정책에 대한 소스로 사용되는 마스터 정책의 예입니다.



그림의 마스터 정책은 Site A(사이트 A)와 Site B(사이트 B)에 있는 정책에 적용 가능한 설정을 가진 전사적 레이어를 포함합니다. 이는 또한 각 정책에 대한 사이트별 레이어를 포함합니다. 예를 들어 네트워크 분석 정책의 경우 Site A(사이트 A)에는 모니터링되는 네트워크에 웹 서버가 없을 수 있으며 HTTP Inspect 프리프로세서의 보호 또는 처리 오버헤드가 필요하지 않을 수 있지만, 두 사이트에 모두 TCP 스트림 전처리가 필요할 수 있습니다. 두 사이트 모두와 공유하는 전사적 레이어에서 TCP 스트림 프로세싱을 활성화할 수 있고, Site A(사이트 A)와 공유하는 사이트별 레이어에

서 HTTP Inspect 프리프로세서를 비활성화할 수도 있으며, Site B(사이트 B)와 공유하는 사이트별 레이어에서 HTTP Inspect 프리프로세서를 활성화할 수도 있습니다. 또한 구성 조정에 필요한 경우 사이트별 정책의 상위 레이어에서 구성을 수정하여 각 사이트에 대한 정책을 추가적으로 조정할 수도 있습니다.

마스터 정책 예에서 합병된 최종 설정이 트래픽 모니터링에 유용할 것이라고 말할 수는 없지만, 사이트별 정책의 구성 및 업데이트에서 절약되는 시간을 고려하면 정책 레이어를 유용하게 응용하는 예라고 할 수 있습니다.

다른 많은 레이어 구성도 가능합니다. 예를 들어, 기업별, 부서별, 또는 네트워크별 정책 레이어를 정의할 수 있습니다. 침입 정책의 경우 한 레이어에는 고급 설정을 포함하고 다른 레이어에는 규칙 설정을 포함할 수도 있습니다.

팁 공유하고자 하는 레이어가 생성된 사용자 지정 정책이 기본 정책인 경우 정책에 공유 레이어를 추가할 수 없습니다. 변경 사항을 저장하려고 시도하면 정책에 순환 종속성이 포함되어 있다는 오류 메시지가 표시됩니다. 자세한 내용은 12-3페이지의 사용자 지정 기본 정책의 이해를 참고하십시오.

레이어를 다른 정책과 공유하려면 다음을 수행해야 합니다.

- 공유할 레이어의 레이어 요약 페이지에서 공유를 활성화합니다.
- 공유하려는 정책의 Policy Layers(정책 레이어) 페이지에서 공유 레이어를 추가합니다.

다른 정책에서 사용되고 있는 레이어에 대한 공유를 비활성화할 수 없습니다. 먼저 다른 정책에서 레이어를 삭제하거나 다른 정책을 삭제해야 합니다.

다른 정책과의 레이어 공유를 활성화 또는 비활성화하려면 다음을 수행합니다.

단계 1 정책을 수정하는 동안 탐색 패널에서 **Policy Layers(정책 레이어)**를 클릭합니다.

Policy Layers(정책 레이어) 페이지가 나타납니다.

단계 2 다른 정책과 공유하려는 레이어 옆에 있는 수정 아이콘( )을 클릭합니다.

레이어에 대한 요약 페이지가 표시됩니다.

단계 3 **Sharing(공유)** 확인란을 선택(활성화) 또는 선택 취소(비활성화)합니다.

단계 4 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

공유 레이어를 정책에 추가하려면 다음을 수행합니다.

단계 1 정책을 수정하는 동안 탐색 패널에서 **Policy Layers(정책 레이어)**를 클릭합니다.

Policy Layers(정책 레이어) 페이지가 나타납니다.

단계 2 User Layers(사용자 레이어) 옆에 있는 공유 레이어 추가 아이콘( )을 클릭합니다.

Add Shared Layer(공유 레이어 추가) 팝업 창이 나타탑니다.

단계 3 Add Shared Layer(공유 레이어 추가) 드롭다운 목록에서 추가하려는 공유 레이어를 선택한 후 **OK(확인)**를 클릭합니다.

Policy Layers(정책 레이어) 요약 페이지가 나타나고 선택한 공유 레이어는 정책에서 최상위 레이어로 나타납니다.

다른 정책에 공유 레이어가 없으면 드롭다운 목록이 나타나지 않습니다. 팝업 창에서 **OK(확인)**를 클릭하거나, Policy Layers(정책 레이어) 요약 페이지로 돌아가려면 **Cancel(취소)**을 클릭합니다.

단계 4 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

레이어 내 침입 규칙 구성

라이센스: 보호

침입 정책에서 사용자 구성 가능한 레이어의 규칙에 대해 규칙 상태, 이벤트 필터링, 동적 상태, 알림, 규칙 코멘트를 설정할 수 있습니다. 변경하려는 레이어에 액세스한 후 침입 정책 Rules(규칙) 페이지에서 하듯 레이어에 대한 Rules(규칙) 페이지에서 설정을 추가합니다(20-1페이지의 규칙을 사용한 침입 정책 조정 참고).

레이어에 대한 Rules(규칙) 페이지에서 개별 레이어 설정을 볼 수도 있고, Rules(규칙) 페이지의 정책 보기에서 모든 설정의 최종 효과를 볼 수도 있습니다. Rules(규칙) 페이지의 정책 보기에서 규칙 설정을 수정할 경우 정책에서 사용자 구성 가능한 최상위 레이어를 수정하게 됩니다. Rules(규칙) 페이지의 레이어 드롭다운 목록을 사용하여 다른 레이어로 전환할 수 있습니다.

다음 표에서는 여러 레이어에서 동일한 설정 유형을 구성하는 효과에 대해 설명합니다.

표 12-2 레이어 규칙 설정

설정 수	설정 유형	목적
하나	규칙 상태	하단 레이어의 규칙에 설정된 규칙 상태를 무시하고, 하단 레이어에서 구성한 규칙에 대한 모든 임계값, 삭제, 속도 기반 규칙 상태 및 경고를 무시합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오. 규칙이 기반 정책 또는 하위 레이어에서 상태를 상속하도록 하려면 규칙 상태를 Inherit(상속)로 설정합니다. 침입 정책 Rules(규칙) 페이지에서 작업할 때는 규칙 상태를 Inherit(상속)로 설정할 수 없습니다. 또한 특정 레이어의 Rules(규칙) 페이지에서 규칙 상태 설정을 볼 때 규칙 상태 설정은 색으로 지정된다는 점을 참고하십시오. 유효한 상태가 하단 레이어으로 설정된 규칙은 노란색으로 강조 표시되고, 유효한 상태가 상단 레이어으로 설정된 규칙은 빨간색으로 강조 표시되며, 유효한 상태가 현재 레이어으로 설정된 규칙은 강조 표시되지 않습니다. 침입 정책 Rules(규칙) 페이지는 모든 규칙 설정의 기본 효과에 대한 중첩 보기이므로, 규칙 상태는 이 페이지에서 색으로 지정되지 않습니다.
하나	임계값 SNMP 경고	하단 레이어의 규칙에 대해 동일한 유형의 설정을 무시합니다. 임계값을 설정하여 레이어에서 규칙에 대한 기존 임계값을 모두 덮어쓴다는 점을 참고하십시오. 자세한 내용은 20-22페이지의 이벤트 임계값 설정 구성 및 20-32페이지의 SNMP 알림 추가를 참고하십시오.
하나 이상	삭제 속도 기반 규칙 상태	규칙 상태가 설정되어 있는 첫 번째 레이어까지 각각의 선택한 규칙에 대한 동일한 유형의 설정을 중첩적으로 결합합니다. 규칙 상태가 설정되어 있는 레이어 아래의 설정은 무시됩니다. 자세한 내용은 20-26페이지의 침입 정책에 따른 삭제 구성 및 20-28페이지의 동적 규칙 상태 추가를 참고하십시오.
하나 이상	코멘트	규칙에 코멘트를 추가합니다. 코멘트은 정책 또는 레이어가 아닌 규칙에 해당하는 것입니다. 모든 레이어의 규칙에 하나 이상의 코멘트를 추가할 수 있습니다. 자세한 내용은 20-9페이지의 규칙에 대해 규칙 코멘트 추가를 참고하십시오.

예를 들어, 규칙 상태를 한 레이어에서는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정하고 상위 레이어에서는 Disabled(비활성화)로 설정할 경우, 침입 정책 Rules(규칙) 페이지는 규칙이 비활성화되었음을 나타냅니다.

다른 예로, 한 레이어에서는 규칙에 대한 소스 기반 삭제를 192.168.1.1로 설정하고, 다른 레이어에서는 규칙에 대한 대상 기반 삭제를 192.168.1.2로 설정하는 경우, Rules(규칙) 페이지는 소스 주소 192.168.1.1 및 대상 주소 192.168.1.2에 대한 이벤트를 삭제하는 것이 중첩 효과임을 보여줍니다. 삭제와 속도 기반 규칙 상태 설정이 규칙 상태가 설정되어 있는 첫 번째 레이어까지 각각의 선택한 규칙에 대한 동일한 유형의 설정을 중첩적으로 결합한다는 점을 참고하십시오. 규칙 상태가 설정되어 있는 레이어 아래의 설정은 무시됩니다.

레이어에서 규칙을 수정하려면 다음을 수행합니다.

단계 1 침입 정책을 수정할 때, 탐색 패널에서 **Policy Layers(정책 레이어)**를 확장하여 수정할 정책 레이어를 확장합니다.

단계 2 수정할 정책 레이어 바로 아래에 있는 **Rules(규칙)**를 클릭합니다.

레이어의 Rules(규칙) 페이지가 나타납니다.

레이어 규칙 설정 표에서 모든 설정을 변경할 수 있습니다. 침입 규칙 구성에 대한 자세한 내용은 20-1페이지의 규칙을 사용한 침입 정책 조정을 참고하십시오.

수정 가능한 레이어에서 개인 설정을 삭제하려면 Rules(규칙) 페이지에서 규칙 세부 정보를 표시하는 레이어에 대한 규칙 메시지를 두 번 클릭합니다. 삭제하려는 설정 옆에 있는 **Delete(삭제)**를 클릭한 후 **OK(확인)**를 두 번 클릭합니다.

단계 3 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

다층 레이어 규칙 설정 제거

라이센스: 보호

침입 정책 Rules(규칙) 페이지에서 하나 이상의 규칙을 선택하고 침입 정책의 여러 레이어에서 특정 유형의 이벤트 필터, 동적 상태 또는 경고를 동시에 제거할 수 있습니다.

시스템은 모든 설정을 제거하거나 규칙 상태가 설정되어 있는 레이어를 발견할 때까지 설정된 각 레이어를 통해 설정 유형을 아래로 제거합니다. 규칙 상태가 설정된 레이어를 발견할 경우, 해당 레이어에서 설정을 제거하고 설정 유형 제거를 중단합니다.

시스템이 기본 정책 또는 공유 레이어에서 설정 유형을 발견할 때, 그리고 정책 내 최고 레이어가 수정 가능한 경우, 시스템은 규칙에 대한 나머지 설정 및 규칙 상태를 수정 가능한 해당 레이어에 복사합니다. 또는 정책 내 최고 레이어가 공유 레이어인 경우, 시스템은 공유 레이어 위에 수정 가능한 새 레이어를 만들고 나머지 설정 및 규칙 상태를 수정 가능한 해당 레이어에 복사합니다.

참고 공유 레이어 또는 기본 정책에서 파생된 규칙 설정을 제거하면 하단 레이어 또는 기본 정책에서 이 규칙에 대한 모든 변경이 무시됩니다. 하단 레이어 또는 기본 정책에서 변경 사항 무시를 중지하려면, 최상위 레이어의 요약 페이지에서 규칙 상태를 **Inherit(상속)**로 설정합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

여러 레이어에서 규칙 설정을 제거하려면 다음을 수행합니다.

단계 1 침입 정책을 수정하는 동안, 탐색 패널에서 Policy Information(정책 정보) 바로 아래에 있는 **Rules(규칙)**를 클릭합니다.

팁 또한 모든 레이어에 대한 Rules(규칙) 페이지의 레이어 드롭다운 목록에서 **Policy(정책)**를 선택하거나, Policy Information(정책 정보) 페이지에서 **Manage Rules(규칙 관리)**를 선택할 수 있습니다.

침입 정책 Rules(규칙) 페이지가 나타납니다.

단계 2 여러 설정을 제거하고자 하는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록에서 모든 규칙을 선택하려면 열 맨 위의 확인 상자를 선택합니다.

규칙 찾기에 관한 정보는 20-10페이지의 침입 정책 내 규칙 필터링의 이해 및 20-18페이지의 침입 정책에서 규칙 필터 설정을 참고하십시오.

단계 3 다음 옵션을 이용할 수 있습니다.

- 규칙에 대한 모든 임계값을 제거하려면, **Event Filtering(이벤트 필터링) > Remove Thresholds(임계값 제거)**를 선택합니다.
- 규칙에 대한 모든 삭제를 제거하려면, **Event Filtering(이벤트 필터링) > Suppressions(삭제)**를 선택합니다.
- 규칙에 대한 모든 속도 기반의 규칙 상태를 제거하려면, **Dynamic State(동적 상태) > Remove Rate-Based Rule States(속도 기반의 규칙 상태 제거)**를 선택합니다.
- 규칙에 대한 모든 SNMP 경고 설정을 제거하려면, **Alerting(경고) > Remove SNMP(SNMP 제거)**를 선택합니다.

확인 팝업 창이 나타납니다.

참고 공유 레이어 또는 기본 정책에서 파생된 규칙 설정을 제거하면 하단 레이어 또는 기본 정책에서 이 규칙에 대한 모든 변경이 무시됩니다. 하단 레이어 또는 기본 정책에서 변경 사항 무시를 중지하려면, 최상위 레이어의 요약 페이지에서 규칙 상태를 **Inherit(상속)**로 설정합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

단계 4 **OK(확인)**를 클릭합니다.

시스템은 선택한 설정을 제거하고 정책에서 수정 가능한 최고 레이어에 규칙에 대한 나머지 설정을 복사합니다. 시스템이 나머지 설정을 복사하는 방식에 영향을 미치는 조건을 보려면 본 절차에 대한 소개를 참고하십시오.

단계 5 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

사용자 지정 기본 정책에서 규칙 변경 허용하기

라이센스: 보호

레이어를 추가하지 않은 사용자 지정 네트워크 분석 또는 침입 정책이 다른 사용자 지정 정책을 기본 정책으로 사용할 때, 다음과 같은 경우 해당 규칙 상태를 상속할 규칙을 설정해야 합니다.

- 기본 정책에서 규칙에 설정된 이벤트 필터, 동적 상태 또는 SNMP 경고를 삭제하는 경우
- 해당 규칙이 기본 정책으로 사용하는 다른 사용자 지정 정책에서 사용자가 차후에 변경하는 사항을 허용하기를 원하는 경우

다음 절차는 이를 수행하는 방법을 설명합니다. 레이어를 추가한 정책에서 이러한 규칙에 대한 설정을 승인하려면 12-12페이지의 다층 레이어 규칙 설정 제거를 참고하십시오.

레이어를 추가하지 않은 정책에서 규칙 변경을 승인하려면 다음을 수행합니다.

단계 1 침입 정책을 수정할 때, 탐색 패널 내 **Policy Layers(정책 레이어)** 링크를 확장한 후, **My Changes(내 변경 사항)** 링크를 확장합니다.

단계 2 My Changes(내 변경 사항) 바로 아래에 있는 **Rules(규칙)** 링크를 클릭합니다.

My Changes(내 변경 사항) 레이어의 Rules(규칙) 페이지가 나타납니다.

단계 3 수락하려는 설정의 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록에서 모든 규칙을 선택하려면 열 맨 위의 확인 상자를 선택합니다.

규칙 찾기에 관한 정보는 20-10페이지의 침입 정책 내 규칙 필터링의 이해 및 20-18페이지의 침입 정책에서 규칙 필터 설정을 참고하십시오.

단계 4 **Rule State(규칙 상태)** 드롭다운 목록에서 **Inherit(상속)**를 선택합니다.

단계 5 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

레이어 내 전처리기 및 고급 설정 구성

라이센스: 보호

침입 정책의 네트워크 분석 및 고급 설정에서 전처리기를 구성하기 위해 유사한 메커니즘을 사용합니다. 네트워크 분석 Settings(설정) 페이지에서 전처리기 및 침입 정책 Advanced Settings(고급 설정) 페이지에서 침입 정책 고급 설정을 활성화 및 비활성화할 수 있습니다. 이 페이지는 또한 모든 관련 기능에 대한 효과적인 상태의 개요를 제공합니다. 예를 들어, 네트워크 분석 SSL 전처리기가 한 레이어에서 비활성화되고 상위 레이어에서 활성화된 경우 Settings(설정) 페이지에서는 활성화된 것으로 보여줍니다. 이 페이지에서 변경된 사항은 정책의 상단 레이어에 나타납니다.

또한 사용자가 구성할 수 있는 레이어에 대한 요약 페이지에서 전처리기 또는 고급 설정을 활성화하거나 비활성화하고 해당 구성 페이지에 액세스할 수 있습니다. 이 페이지에서 레이어 이름 및 설명을 변경할 수 있고, 동일한 유형의 다른 정책과 레이어를 공유할지 여부를 설정할 수 있습니다. 자세한 내용은 12-9페이지의 정책 간 레이어 공유를 참고하십시오. 탐색 패널에서 **Policy Layers(정책 레이어)** 아래 레이어 이름을 선택하여 다른 레이어에 대한 요약 페이지로 전환할 수 있습니다.

전처리기 또는 고급 설정을 활성화하면 탐색 패널에서 레이어 이름 아래에 해당 기능에 대한 구성 페이지에 하위 링크가 나타나고, 레이어에 대한 요약 페이지의 기능 옆에 수정 아이콘( )이 나타납니다. 이는 레이어의 기능을 비활성화하거나 Inherit(상속)로 설정하면 사라집니다.

전처리기 또는 고급 설정의 상태(활성화 또는 비활성화)를 설정하면 하단 레이어에서 해당 기능의 상태 및 구성 설정을 무시합니다. 기본 정책 또는 하단 레이어에서 전처리기 또는 고급 설정이 상태와 구성을 상속하는 것을 원하는 경우, 규칙 상태를 **Inherit(상속)**로 설정합니다. Settings(설정) 또는 Advanced Settings(고급 설정) 페이지에서 작업하는 경우 Inherit(상속)을 선택할 수 없다는 점에 유의하십시오.

각 레이어 요약 페이지에서 색상 구분은 다음과 같이 효과적인 구성이 상위 레이어, 하단 레이어 또는 현재 레이어 중 어디에 있는지 나타냅니다.

- 빨간색 - 효과적인 구성은 상위 레이어에 있습니다.
- 황색 - 효과적인 구성은 하단 레이어에 있습니다.
- 비음영 - 효과적인 구성은 현재 레이어에 있습니다.

Settings(설정) 및 Advanced Settings(고급 설정) 페이지는 관련된 모든 설정의 복합적인 보기이므로, 이 페이지는 효과적인 구성의 위치를 나타내는 색상 구분을 사용하지 않습니다.

시스템은 기능이 활성화된 가장 높은 레이어에서 구성을 사용합니다. 명시적으로 구성을 수정하지 않은 경우, 시스템은 기본 구성을 사용합니다. 예를 들어, 한 레이어에서 네트워크 분석 DCE/RPC 전처리기를 활성화하고 수정하는 경우, 그리고 상위 레이어에서는 그것을 활성화하지만 변경하지 않는 경우, 시스템은 상위 레이어의 기본 구성을 사용합니다.

다음 표는 사용자가 구성할 수 있는 레이어에 대한 요약 페이지에서 사용 가능한 작업을 설명합니다.

표 12-3 레이어 요약 페이지 작업

목적	방법
레이어 이름 또는 설명을 수정하려면	**Name(이름)** 또는 **Description(설명)**에 대한 새 값을 입력합니다.
다른 침입 정책과 레이어를 공유하려면	**Allow this layer to be used by other policies(이 레이어를 다른 정책과 공유할 수 있도록 수락)**를 선택합니다. 자세한 내용은 12-9페이지의 정책 간 레이어 공유를 참고하십시오.
현재 레이어에서 전처리기/고급 설정을 활성화하거나 비활성화하려면	기능 옆에 있는 **Enabled(활성화)** 또는 **Disabled(비활성화)**를 클릭합니다. 활성화하면 탐색 패널에서 레이어 이름 아래에 구성 페이지 하위 링크가 나타나고, 기능 옆 요약 페이지에 수정 아이콘( )이 나타납니다. 비활성화하면 하위 링크 및 수정 아이콘이 삭제됩니다.
현재 레이어 아래 최상위 레이어의 설정에서 전처리기/고급 설정 상태 및 구성을 상속하려면	**Inherit(상속)**를 클릭합니다. 페이지는 새로 고침되며, 기능을 활성화한 경우 탐색 패널의 기능 하위 링크 및 수정 아이콘은 더 이상 나타나지 않습니다.
활성화된 전처리기/고급 설정을 위해 구성 페이지에 액세스하기	현재 구성을 수정하려면 수정 아이콘( ) 또는 기능 하위 링크를 클릭합니다. Back Orifice 전처리기에는 사용자가 구성할 수 있는 옵션이 없다는 점에 유의하십시오.

사용자 레이어에서 전처리기/고급 설정을 수정하려면 다음을 수행합니다.

단계 1 정책을 수정할 때, 탐색 패널에서 **Policy Layers(정책 레이어)**를 확장한 후 수정할 레이어 이름을 클릭합니다.

레이어에 대한 요약 페이지가 표시됩니다.

단계 2 레이어 요약 페이지 작업 표에서 모든 조치를 취할 수 있습니다.

단계 3 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

트래픽 전처리 사용자 정의

액세스 제어 정책의 고급 설정 대부분은 구성을 위한 특정 전문성을 요구하는 침입 탐지 및 방지 구성을 제어합니다. 고급 설정은 일반적으로 거의 또는 전혀 수정할 필요가 없으며 모든 배포에 공통적으로 적용하지는 않습니다.

이 장에서는 다음 기본 설정을 설정하는 방법을 설명합니다.

- 13-1페이지의 액세스 제어에 대한 기본 침입 정책 설정에서는 시스템에서 트래픽을 검사하는 방법을 결정하기 전에 트래픽을 초기에 검사하는 데 사용되는 액세스 제어 정책의 기본 침입 정책을 변경하는 방법에 대해 설명합니다.
- 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의는 일치하는 트래픽을 전처리하는 사용자 정의 네트워크 분석 정책을 할당하여 특정 보안 영역 및 네트워크에 특정 트래픽 전처리 옵션을 맞추는 방법을 설명합니다.

다른 장에서는 액세스 제어 정책에 대한 정책 전반의 전처리 및 성능 옵션을 설명합니다. 자세한 내용은 다음을 참고하십시오.

- 17-1페이지의 고급 전송/네트워크 설정 구성
- 18-1페이지의 수동 배포 시 전처리 조정
- 10-6페이지의 침입 방지 성능 조정
- 10-16페이지의 파일 및 악성코드 탐지 성능 및 저장 조정

액세스 제어에 대한 기본 침입 정책 설정

라이센스: 모두

각 액세스 제어 정책은 *기본 침입 정책*을 사용하여 시스템에서 트래픽을 검사하는 방법을 결정하기 전에 트래픽을 초기에 검사합니다. 이렇게 해야 하는 이유는 시스템에서 어떤 액세스 제어 규칙(규칙이 있는 경우)으로 트래픽을 처리할 수 있는지 결정하기 전에, 연결의 처음 몇 가지 패킷을 처리하여 **해당 패킷의 통과를 허용**해야 하는 경우가 있기 때문입니다. 그러나 이러한 패킷은 검사하지 않은 대상에는 도달할 수 없으며, 기본 침입 정책이라고 하는 침입 정책을 사용하여 이러한 패킷을 검사하고 침입 이벤트를 생성할 수 있습니다.

기본 침입 정책은 애플리케이션 제어 및 URL 필터링을 수행할 때 특히 유용합니다. 시스템은 클라이언트와 서버 간의 연결이 완전히 설정되기 전에는 애플리케이션 또는 필터 URL을 확인할 수 없기 때문입니다. 예를 들어, 어떤 패킷이 애플리케이션 또는 URL 조건이 포함된 액세스 제어 규칙의 다른 모든 조건과 일치할 경우, 해당 패킷과 후속 패킷은 연결이 설정되고 애플리케이션 또는 URL 확인이 완료될 때까지 통과될 수 있으며 일반적으로 3~5개의 패킷이 허용됩니다.

시스템에서는 기본 침입 정책으로 이러한 허용된 패킷을 검사합니다. 해당 정책은 이벤트를 생성할 수 있으며, 인라인으로 배치된 경우 악성 트래픽을 차단할 수 있습니다. 시스템이 액세스 제어 규칙 또는 연결을 처리해야 하는 기본 작업을 확인하면, 연결의 나머지 패킷이 처리되고 그에 따라 검사됩니다.

액세스 제어 정책을 생성할 경우, 기본 침입 정책은 **처음** 선택한 기본 작업에 따라 달라집니다. 액세스 제어를 위한 최초 기본 침입 정책은 다음과 같습니다.

- 균형 잡힌 보안 및 연결(시스템 제공 정책)은 액세스 제어 정책에 대한 기본 침입 정책이며, 이는 사용자가 **Intrusion Prevention(침입 방지)** 기본 작업을 처음 선택하는 지점입니다.
- No Rules Active(활성 규칙 불가)는 액세스 제어 정책의 기본 침입 정책입니다. 이는 사용자가 **Block all traffic(모든 트래픽 차단)** 기본 작업을 가장 먼저 선택하는 것입니다. 이 옵션을 선택하면 위에서 설명한 허용된 패킷에 대한 침입 검사를 비활성화할 수 있지만 사용자가 침입 데이터에 관심이 없는 경우 성능을 향상시킬 수 있습니다.

참고 사용자가 침입 선택을 수행하지 않은 경우, No Rules Active(활성 규칙 불가) 정책을 기본 침입 정책으로 유지하십시오. 자세한 내용은 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

액세스 제어 정책을 생성한 후 기본 작업을 변경할 경우, 기본 침입 정책은 자동으로 변경되지 **않습니다**. 이를 수동으로 변경하려면 액세스 제어 정책의 고급 옵션을 사용하십시오.

액세스 제어 정책의 기본 침입 정책을 변경하려면 다음을 수행합니다.

단계 1 기본 침입 정책을 변경하려는 액세스 제어 정책에서 **Advanced(고급)** 탭을 선택한 후 Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

Network and Analysis Policies(네트워크 분석 정책) 대화 상자가 나타납니다.

단계 2 **Intrusion Policy used before Access Control rule is determined(액세스 제어 규칙이 결정되기 전에 사용된 침입 정책)** 드롭다운 목록에서 기본 침입 정책을 선택합니다. 시스템에서 생성된 정책 또는 사용자가 생성한 정책을 선택할 수 있습니다.

사용자가 생성한 정책을 선택할 경우, 수정 아이콘( )을 클릭하여 새 창에서 정책을 수정할 수 있습니다. 시스템에서 제공된 정책은 수정할 수 없습니다.

주의 **반드시** `Experimental Policy 1(실험 정책 1)`을 Cisco 관계자의 지시 없이는 사용하지 마십시오. Cisco는 이 정책을 테스트용으로 사용합니다.

단계 3 **OK(확인)**를 클릭하여 변경 사항을 저장합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다.

네트워크 분석 정책으로 전처리 사용자 정의

라이센스: 모두

*네트워크 분석 정책*은 특히 침입 시도의 신호가 될 수 있는 변칙 트래픽을 향후에 평가할 수 있도록 트래픽을 해독하고 전처리하는 방법을 제어합니다. 이 트래픽 전처리는 Security Intelligence(보안 인텔리전스) 차단 목록 추가 이후, 침입 정책이 패킷을 상세히 검사하기 전에 이루어집니다. 기본적으로, 시스템이 제공하는 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책은 액세스 제어 정책이 처리하는 *모든* 트래픽에 적용됩니다.

팁 시스템이 제공하는 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트할 수 있습니다. 하지만, 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다.

전처리를 조정하는 간단한 방법은 기본값으로 사용자 네트워크 분석 정책을 생성하고 사용하는 것입니다(14-2페이지의 사용자 지정 네트워크 분석 정책 만들기 참고). 사용 가능한 옵션 조정은 전처리기에 따라 다릅니다.

복합적인 배포를 사용하는 고급 사용자의 경우, 다수의 네트워크 분석 정책을 생성할 수 있는데, 각각은 트래픽을 다르게 전처리하기 위해 조정된 것입니다. 그런 다음, 사용자는 다양한 보안 영역 또는 네트워크를 사용하여 트래픽의 전처리를 제어하는 정책을 사용하는 시스템을 구성할 수 있습니다.

이를 수행하려면, 액세스 제어 정책에 사용자 지정 *네트워크 분석 규칙*을 추가합니다. 각 규칙에는 다음이 포함되어 있습니다.

- 전처리하려는 특정 트래픽을 확인하는 일련의 규칙 조건
- 모든 규칙의 조건을 충족하는 트래픽을 전처리하는 데 사용하려는 결합된 네트워크 분석 정책

시스템이 트래픽을 전처리할 시간이 되면, 큰 규칙 번호에서 작은 번호 순서로 패킷을 네트워크 분석 규칙에 일치시킵니다. 어떤 네트워크 분석 규칙과도 일치하지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다.

참고 전처리기를 비활성화했지만 시스템이 활성화된 침입 또는 전처리기 규칙에 대해 전처리한 패킷을 평가해야 하는 경우, 네트워크 분석 정책 인터페이스에서는 비활성화 상태로 남아 있는 상태라 해도 시스템은 전처리기를 자동으로 활성화하여 사용합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 사용자는 **반드시** 주의하여 서로 보완하는 단일 패킷을 검토하는 네트워크 분석 및 침입 정책을 허용해야 합니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 13-4페이지의 액세스 제어를 위한 기본 네트워크 분석 정책 설정
- 13-4페이지의 네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정
- 13-8페이지의 네트워크 분석 규칙 관리

액세스 제어를 위한 기본 네트워크 분석 정책 설정

라이센스: 모두

기본적으로, 시스템이 제공하는 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책은 액세스 제어 정책이 처리하는 모든 트래픽에 적용됩니다. 트래픽 전처리 옵션을 맞춤화하기 위해 네트워크 분석 규칙을 추가하는 경우, 기본 네트워크 분석 정책은 해당 규칙에 의해 처리되는 모든 트래픽을 전처리합니다.

액세스 제어 정책의 고급 설정을 통해 기본 정책을 변경할 수 있습니다.

액세스 제어 정책의 기본 네트워크 분석 정책을 변경하려면 다음을 수행합니다.

단계 1 기본 네트워크 분석 정책을 변경하려는 액세스 제어 정책에서 **Advanced(고급)** 탭을 선택한 후 Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

Network and Analysis Policies(네트워크 분석 정책) 대화 상자가 나타납니다.

단계 2 **Default Network Analysis Policy(기본 네트워크 분석 정책)** 드롭다운 목록에서 기본 네트워크 분석 정책을 선택합니다. 시스템에서 생성된 정책 또는 사용자가 생성한 정책을 선택할 수 있습니다.

사용자가 생성한 정책을 선택할 경우, 수정 아이콘( )을 클릭하여 새 창에서 정책을 수정할 수 있습니다. 시스템이 제공하는 정책은 수정할 수 없습니다.

주의 **반드시** `Experimental Policy 1(실험 정책 1)`을 Cisco 관계자의 지시 없이는 사용하지 마십시오. Cisco는 이 정책을 테스트용으로 사용합니다.

단계 3 **OK(확인)**를 클릭하여 변경 사항을 저장합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다.

네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정

라이센스: 모두

액세스 제어 정책의 고급 설정에서, 네트워크 분석 규칙을 사용하여 네트워크 트래픽에 대한 전처리 구성을 맞춤화할 수 있습니다. 액세스 제어 규칙과 마찬가지로, 네트워크 분석 규칙도 1번을 시작으로 번호가 지정됩니다.

시스템이 트래픽을 전처리할 시간이 되면, 오름차순 규칙 번호가 적어지는 순서로 패킷을 네트워크 분석 규칙에 일치시키며, 모든 규칙의 조건이 일치하는 첫 번째 규칙에 따라 트래픽을 전처리합니다. 규칙에 추가할 수 있는 조건은 아래 표에 설명되어 있습니다.

표 13-1 네트워크 분석 규칙 조건 유형

조건	트래픽 일치 방법	세부 사항
영역	특정 보안 영역에서 인터페이스를 통해 디바이스로 들어가거나 디바이스에서 나옴	보안 영역은 구축 및 보안 정책에 따라 하나 이상의 인터페이스를 논리적으로 그룹화한 것입니다. 영역 조건을 작성하려면 13-6페이지의 영역 당 트래픽 전처리를 참고하십시오.
네트워크	해당 소스 또는 대상 IP 주소를 이용함	명시적으로 IP 주소를 지정할 수 있습니다. 네트워크 조건을 작성하려면 13-7페이지의 네트워크 당 트래픽 전처리를 참고하십시오.

규칙에 대해 특별한 조건을 구성하지 않으면 시스템에서는 해당 기준을 기반으로 트래픽의 일치를 확인하지 않습니다. 예를 들어, 네트워크 조건은 있지만 영역 조건이 없는 규칙의 경우 인그레스 또는 이그레스 인터페이스에 상관없이 소스 또는 대상 IP 주소에 따라 트래픽을 평가합니다. 어떤 네트워크 분석 규칙과도 일치하지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다.

사용자 정의 네트워크 분석 규칙을 추가하려면 다음을 수행합니다.

단계 1 사용자 정의 전처리 구성을 생성하려는 액세스 제어 정책에서 **Advanced(고급)** 탭을 선택한 후 Intrusion and Network Analysis Policies(침입 및 네트워크 분석 정책) 섹션 옆에 있는 수정 아이콘(✎)을 클릭합니다.

Network and Analysis Policies(네트워크 분석 정책) 대화 상자가 나타납니다. 사용자 지정 네트워크 분석 규칙을 추가하지 않은 경우, 모듈 인터페이스는 **No Custom Rules(사용자 지정 규칙이 없음)**이라고 표시하며, 그렇지 않은 경우 구성한 지정 네트워크 분석 규칙 수를 표시 합니다.

팁 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭하여 새 창에서 Network Analysis Policy(네트워크 분석 정책) 페이지를 표시합니다. 이 페이지를 사용하여 사용자 정의 네트워크 분석 정책을 살펴보고 수정합니다(14-3페이지의 네트워크 분석 정책 관리 참고).

단계 2 **Network Analysis Rules(네트워크 분석 규칙)** 옆에 있는 보유하고 있는 사용자 지정 규칙의 수를 표시하는 문장을 클릭합니다.

사용자 정의 규칙이 있는 경우 대화 상자가 확장되어 표시됩니다.

단계 3 **Add Rule(규칙 추가)**을 클릭합니다.

네트워크 분석 규칙 편집기가 나타납니다.

단계 4 규칙 조건을 작성합니다. 다음 기준을 사용하여 NAP 전처리를 제한할 수 있습니다.

- 13-6페이지의 영역 당 트래픽 전처리
- 13-7페이지의 네트워크 당 트래픽 전처리

단계 5 **Network Analysis(네트워크 분석)** 탭을 클릭하고 **Network Analysis Policy(네트워크 분석 정책)** 드롭다운 목록에서 정책을 선택하여 네트워크 분석 정책을 규칙과 결합합니다.

시스템은 모든 규칙의 조건을 충족하는 트래픽을 전처리하기 위해 선택한 네트워크 분석 정책을 사용합니다. 사용자가 생성한 정책을 선택할 경우, 수정 아이콘(✎)을 클릭하여 새 창에서 정책을 수정할 수 있습니다. 시스템이 제공하는 정책은 수정할 수 없습니다.

주의 **반드시** `Experimental Policy 1(실험 정책 1)`을 Cisco 관계자의 지시 없이는 사용하지 마십시오. Cisco는 이 정책을 테스트용으로 사용합니다.

단계 6 **Add(추가)**를 클릭합니다.

규칙은 다른 규칙 뒤에 추가됩니다. 규칙의 평가 순서를 변경하려면 13-8페이지의 네트워크 분석 규칙 관리를 참고하십시오.

영역 당 트래픽 전처리

라이센스: 모두

네트워크 분석 규칙의 영역 조건을 통해 소스 및 대상 보안 영역으로 트래픽을 전처리할 수 있습니다. 보안 영역은 하나 이상의 인터페이스를 그룹화한 것입니다. 영역 생성에 대한 자세한 내용은 2-33페이지의 보안 영역 작업을 참고하십시오.

단일 영역 조건에서 각 **Source Zones(소스 영역)** 및 **Destination Zones(대상 영역)**에 최대 50개의 영역을 추가할 수 있습니다.

- 영역 내 인터페이스의 디바이스에서 *나가는* 트래픽에 일치시키기 위해서는 **Destination Zones(대상 영역)**에 해당 영역을 추가합니다. 수동적으로 배포된 디바이스는 트래픽을 전송하지 않으므로, **Destination Zone(대상 영역)** 조건에서 수동 인터페이스로 구성된 영역을 사용할 수 없습니다.
- 영역 내 인터페이스의 디바이스에서 *들어가는* 트래픽에 일치시키기 위해서는 **Source Zones(소스 영역)**에 해당 영역을 추가합니다.

규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

경고 아이콘(⚠)은 어느 인터페이스도 포함하지 않는 영역과 같이 유효하지 않은 구성을 나타냅니다. 자세한 내용을 보려면, 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

영역별 트래픽을 전처리하려면 다음을 수행합니다.

단계 1 영역별 트래픽 전처리를 원하는 지점의 액세스 제어 정책에서 새로운 네트워크 분석 규칙을 만들거나 기존 규칙을 수정합니다.

자세한 지침은 13-4페이지의 네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정을 참고하십시오.

단계 2 네트워크 분석 규칙 편집기에서, **Zones(영역)** 탭을 선택합니다.

Zones(영역) 탭이 나타납니다.

단계 3 **Available Zones(사용 가능한 영역)**에서 추가하려는 영역을 찾아 선택합니다.

영역을 찾아 추가하려면, **Available Zones(사용 가능한 영역)** 목록 위에 있는 **Search by name(이름으로 검색)** 프롬프트를 클릭한 후, 영역 이름을 입력합니다. 일치하는 영역을 입력하여 표시하면 목록이 업데이트됩니다.

영역을 선택하려면 클릭하십시오. 여러 영역을 선택하려면, **Shift**와 **Ctrl** 키를 사용하거나, 마우스 오른쪽 단추를 클릭한 후 **Select All(모두 선택)**을 선택합니다.

단계 4 **Add to Source(소스에 추가)** 또는 **Add to Destination(대상에 추가)**을 클릭하여 적절한 목록에 선택한 영역을 추가합니다.

선택한 영역을 끌어서 놓을 수도 있습니다.

단계 5 규칙을 저장하거나 계속 수정합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

네트워크 당 트래픽 전처리

라이센스: 모두

네트워크 분석 규칙의 네트워크 조건을 통해 소스 및 대상 IP 주소로 트래픽을 전처리할 수 있습니다. 전처리를 원하는 트래픽에 수동으로 소스 및 대상 IP 주소를 지정할 수 있으며, 하나 이상의 IP 주소 및 주소 블록을 이름과 결합하여 재사용이 가능한 네트워크 개체로 네트워크 상태를 구성할 수 있습니다.

팁 네트워크 개체를 생성한 후에는 네트워크 분석 규칙을 작성하는 데 뿐만 아니라 시스템의 모듈 인터페이스 내 다양한 장소에서 IP 주소를 나타나는 데에도 사용할 수 있습니다. 개체 관리자를 사용하여 이 개체를 만들 수 있습니다. 네트워크 분석 규칙을 구성하는 동안 상황에 따라 네트워크 개체를 만들 수도 있습니다. 자세한 내용은 2-3페이지의 네트워크 개체 작업을 참고하십시오.

사용자는 단일 영역 조건에서 각 **Source Networks(소스 네트워크)** 및 **Destination Networks(대상 네트워크)**에 최대 50개의 영역을 추가할 수 있습니다.

- IP 주소의 트래픽과 일치시키려면, **Source Networks(소스 네트워크)**를 구성합니다.
- IP 주소에 트래픽을 일치시키려면, **Destination Networks(대상 네트워크)**를 구성합니다.

규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

네트워크 상태를 구축할 때, 경고 아이콘( )은 유효하지 않은 구성을 나타냅니다. 자세한 내용을 보려면, 4-14페이지의 액세스 제어 정책과 규칙 문제 해결을 참고하십시오.

네트워크별 트래픽을 전처리하려면 다음을 수행합니다.

단계 1 네트워크별 트래픽 전처리를 원하는 지점의 액세스 제어 정책에서 새로운 네트워크 분석 규칙을 만들거나 기존 규칙을 수정합니다.

자세한 내용은 13-4페이지의 네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정을 참고하십시오.

단계 2 네트워크 분석 규칙 편집기에서, **Networks(네트워크)** 탭을 선택합니다.

Networks(네트워크) 탭이 나타납니다.

단계 3 다음과 같이, **Available Networks(사용 가능한 네트워크)**로부터 추가하려는 네트워크를 찾아 선택합니다.

- 상황에 따라 네트워크 개체를 추가한 다음 조건에 추가하려면, 추가 아이콘( )(**Available Networks(사용 가능한 네트워크)** 목록 위에 있음)을 클릭합니다(2-3페이지의 네트워크 개체 작업 참고).
- 추가할 네트워크를 검색하려면, **Available Networks(사용 가능한 네트워크)** 목록 위에 있는 **Search by name or value(이름 또는 값으로 검색)** 프롬프트를 클릭한 후 개체 이름이나 개체의 구성 요소 중 하나의 값을 입력합니다. 일치하는 개체를 입력하여 표시하면 목록이 업데이트됩니다.

개체를 선택하려면 이를 클릭합니다. 여러 개체를 선택하려면, Shift와 Ctrl 키를 사용하거나, 마우스 오른쪽 단추를 클릭한 후 **Select All(모두 선택)**을 선택합니다.

단계 4 **Add to Source(소스에 추가)** 또는 **Add to Destination(대상에 추가)**을 클릭하여 적절한 목록에 선택한 개체를 추가합니다.

선택한 영역을 끌어서 놓을 수도 있습니다.

단계 5 수동으로 지정하려는 주소 블록, 대상 IP 주소 또는 모든 소스를 추가합니다.

Source Networks(소스 네트워크) 또는 **Destination Networks(대상 네트워크)** 목록 아래에 있는 **Enter an IP address(IP 주소 입력)** 프롬프트를 클릭한 후 IP 주소 또는 주소 블록을 입력하고 **Add(추가)**를 클릭합니다.

단계 6 규칙을 저장하거나 계속 수정합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

네트워크 분석 규칙 관리

라이센스: 모두

네트워크 분석 규칙은 해당 자격과 일치하는 트래픽을 어떻게 전처리할지 단순히 지정한 일련의 구성과 조건입니다. 사용자는 기존의 액세스 제어 정책의 고급 옵션에서 네트워크 분석 규칙을 만들고 수정합니다. 각 규칙은 하나의 정책에만 속합니다.

사용자 정의 네트워크 분석 규칙을 수정하려면 다음을 수행합니다.

단계 1 사용자 정의 전처리 구성을 변경하려는 액세스 제어 정책에서 **Advanced(고급)** 탭을 선택한 후 Intrusion and Network Analysis Policies(침입 및 네트워크 분석 정책) 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

Network and Analysis Policies(네트워크 분석 정책) 대화 상자가 나타납니다. 사용자 지정 네트워크 분석 규칙을 추가하지 않은 경우, 모듈 인터페이스는 **No Custom Rules(사용자 지정 규칙이 없음)**라고 표시하며, 그렇지 않은 경우 구성한 지정 네트워크 분석 규칙 수를 표시합니다.

단계 2 **Network Analysis Rules(네트워크 분석 규칙)** 옆에 있는 보유하고 있는 사용자 지정 규칙의 수를 표시하는 문장을 클릭합니다.

사용자 정의 규칙이 있는 경우 대화 상자가 확장되어 표시됩니다.

단계 3 사용자 지정 규칙을 수정합니다. 다음 옵션을 이용할 수 있습니다.

- 규칙 조건을 수정하거나, 규칙에 의해 호출된 네트워크 분석 정책을 변경하기 위해서는, 규칙 옆에 있는 수정 아이콘( )을 클릭합니다.
- 규칙의 평가 순서를 변경하려면, 정확한 위치에 규칙을 클릭하여 끌어옵니다. 여러 규칙을 선택하려면 Shift와 Ctrl 키를 사용합니다.
- 규칙을 삭제하려면, 규칙 옆에 있는 삭제 아이콘( )을 클릭합니다.

단계 4 **OK(확인)**를 클릭하여 변경 사항을 저장합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

14장

네트워크 분석 정책 시작하기

*네트워크 분석 정책*은 많은 트래픽 전처리 옵션을 관리하며, 액세스 제어 정책의 고급 설정에 의해 호출됩니다. 네트워크 분석 관련 전처리는 Security Intelligence(보안 인텔리전스) 차단 목록 추가 후에 발생하지만 액세스 제어 규칙이 패킷을 자세히 조사하기 전과 모든 침입 또는 파일 검사가 시작되기 전에 발생합니다.

기본적으로, 시스템은 *Balanced Security and Connectivity(균형 잡힌 보안 및 연결성)* 네트워크 분석 정책을 사용하여 액세스 제어 정책에서 처리된 모든 트래픽을 전처리합니다. 그러나, 사용자는 이 전처리를 수행하는 기타 기본 네트워크 분석 정책을 선택할 수 있습니다 사용자 편의를 위해, 시스템은 VRT(취약성 연구단)가 보안 및 연결의 특정 균형을 위해 조정한 변경할 수 없는 여러 네트워크 분석 정책 선택권을 제공합니다. 또한 이 기본 정책을 사용자 지정 전처리 설정이 있는 사용자 지정 네트워크 분석 정책으로 변경할 수 있습니다.

팁 시스템이 제공하는 침입 및 네트워크 분석 정책은 이름은 유사하지만 다른 구성을 포함합니다. 예를 들어, Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트될 수 있습니다. 하지만, 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다. 11-1페이지의 네트워크 분석 및 침입 정책의 이해는 사용자의 트래픽을 검토하기 위해 네트워크 분석과 침입 정책이 함께 작동하는 방식에 대한 개요뿐 아니라 탐색 패널을 사용하고, 문제를 해결하며, 변경 사항을 커밋하는 것에 대한 일부 기반을 제공합니다.

또한 여러 사용자 지정 네트워크 분석 정책을 작성한 다음, 다른 트래픽을 전처리하도록 할당하여 특정 보안 영역, 네트워크 에 맞추어 트래픽 전처리 옵션을 조정할 수 있습니다.

참고 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 서로 보완해야 합니다. 시스템이 사용자를 위해 정책을 조정하지 **않으며**, 구성이 잘못된 경우에는 기본 옵션을 사용합니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

이 장에서는 간단한 사용자 지정 네트워크 분석 정책을 작성하는 방법에 대해 설명합니다. 이 장에는 또한 수정, 비교 등의 네트워크 분석 정책 관리에 대한 기본 정보가 포함되어 있습니다. 자세한 내용은 다음을 참고하십시오.

사용자 지정 네트워크 분석 정책 만들기

라이센스: 모두

새로운 네트워크 분석 정책을 생성하는 경우 고유한 이름 및 기본 정책을 지정하고 *인라인 모드*를 선택해야 합니다.

기본 정책은 네트워크 분석 정책의 기본 설정을 정의합니다. 새로운 정책에서 구성을 변경하면 기본 정책 설정을 대체하지만 변경하지는 않습니다. 기본 정책으로 시스템 제공 정책 또는 사용자 지정 정책을 사용할 수 있습니다. 자세한 내용은 12-2페이지의 기본 레이어의 이해를 참고하십시오.

네트워크 분석 정책의 인라인 모드에서는 전처리기가 트래픽을 수정(표준화)하고 삭제하여 공격자가 탐지를 회피할 가능성을 최소화할 수 있습니다. 수동 배포에서는 시스템이 인라인 모드와 관계없이 트래픽 흐름에 영향을 줄 수 없다는 점에 유의하십시오. 자세한 내용은 14-5페이지의 전처리기의 영향을 받도록 트래픽 설정을 참고하십시오.

네트워크 분석 정책을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 **Create Policy(정책 생성)**를 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, Network Analysis Policy(네트워크 분석 정책) 페이지로 돌아가라는 메시지가 나타나면**Cancel(취소)**을 클릭합니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Create Network Analysis Policy(네트워크 분석 정책 생성) 팝업 창이 나타납니다.

단계 7 정책에 고유한 **Name(이름)** 또는 **Description(설명)**을 지정합니다.

단계 8 초기 **Base Policy(기본 정책)**를 지정합니다.

시스템 제공 정책 또는 사용자 지정 정책을 기본 정책으로 사용할 수 있습니다.

⚠ **주의** **반드시** `Experimental Policy 1(실험 정책 1)`을 Cisco 관계자의 지시 없이는 사용하지 마십시오. Cisco는 이 정책을 테스트용으로 사용합니다.

단계 9 인라인 배포에서 트래픽을 전처리기의 영향을 받도록 설정할지 여부를 지정합니다.

- 트래픽을 전처리기의 영향을 받도록 설정하려면, **Inline Mode(인라인 모드)**를 활성화합니다.
- 트래픽을 전처리기의 영향을 받지 않도록 설정하려면 **Inline Mode(인라인 모드)**를 비활성화합니다.

단계 10 다음과 같이 정책을 생성합니다.

- 새로운 정책을 만들고 Network Analysis Policy(네트워크 분석 정책)로 돌아가려면 **Create Policy(정책 생성)**를 클릭합니다. 새로운 정책의 설정은 기본 정책의 설정과 같습니다.
- **Create and Edit Policy(정책 생성 및 수정)**를 클릭하여 정책을 만들고 고급 네트워크 분석 정책 편집기에서 이를 열어 수정합니다(14-4페이지의 네트워크 분석 정책 수정 참고).

네트워크 분석 정책 관리

라이센스: 모두

Network Analysis Policy(네트워크 분석 정책) 페이지에서 다음 정보와 함께 현재 사용자 지정 네트워크 분석 정책을 볼 수 있습니다.

- 정책이 최종 수정된 시간과 날짜(로컬 시간) 및 정책을 수정한 사용자
- 트래픽을 전처리기의 영향을 받도록 설정하는 **Inline Mode(인라인 모드)** 활성화 여부
- 트래픽을 전처리하는 데 네트워크 분석 정책을 사용하는 액세스 제어 정책
- 정책에 저장되지 않은 변경 사항이 있는지 여부 및 현재 정책을 수정하고 있는 사람에 관한 정보

Network Analysis Policy(네트워크 분석 정책) 페이지의 옵션을 통해 다음 표에 있는 조치를 취할 수 있습니다.

표 14-1 네트워크 분석 정책 관리 작업

목적	방법	참고 사항
새로운 네트워크 분석 정책 생성	**Create Policy(정책 생성)**를 클릭합니다.	14-2페이지의 사용자 지정 네트워크 분석 정책 만들기.
기존 네트워크 분석 정책 수정하기	수정 아이콘( )을 클릭합니다.	14-4페이지의 네트워크 분석 정책 수정.
네트워크 분석 정책의 현재 구성 설정을 나열하는 PDF 보고서 보기	보고서 아이콘( )을 클릭합니다.	14-8페이지의 현재 네트워크 분석 설정 보고서 생성
두 가지 네트워크 분석 정책의 설정을 비교하거나 동일한 정책의 두 가지 수정 버전 비교하기	**Compare Policies(정책 비교)**를 클릭합니다.	14-9페이지의 두 네트워크 분석 정책 또는 수정 버전 비교.
새로운 네트워크 분석 정책 삭제하기	삭제 아이콘( )을 클릭한 다음 정책을 삭제할 것인지 확인합니다. 액세스 제어 정책이 네트워크 분석 정책을 참조하는 경우 이를 삭제할 수 없습니다.	

네트워크 분석 정책 수정

라이센스: 모두

새로운 네트워크 분석 정책을 생성하는 경우 해당 기본 정책의 설정과 동일합니다. 다음 표는 새로운 정책을 사용자의 요구에 맞추기 위해 취할 수 있는 가장 일반적인 작업에 대해 나열합니다.

표 14-2 네트워크 분석 정책 수정 작업

목적	방법	참고 사항
전처리기가 트래픽을 수정하거나 삭제할 수 있도록 하기	Policy Information(정책 정보) 페이지에서 **Inline Mode(인라인 모드)** 확인 상자를 선택합니다.	14-5페이지의 전처리기의 영향을 받도록 트래픽 설정
기본 정책 변경하기	Policy Information(정책 정보) 페이지의 **Base Policy(기본 정책)** 드롭다운 목록에서 기본 정책을 선택합니다.	12-4페이지의 기본 정책 변경
기본 정책 설정 보기	Policy Information(정책 정보) 페이지에서 **Manage Base Policy(기본 정책 관리)**를 클릭합니다.	12-2페이지의 기본 레이어의 이해
전처리기에 대한 설정을 활성화 또는 비활성화로 설정하거나 수정하기	탐색 패널에서 **Settings(설정)**를 클릭합니다.	14-6페이지의 네트워크 분석 정책에서 전처리기 구성
정책 레이어 관리하기	탐색 패널에서 **Policy Layers(정책 레이어)**를 클릭합니다.	12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용

네트워크 분석 정책을 조정할 경우, 특히 전처리기를 비활성화할 경우, 일부 전처리기 및 침입 규칙은 트래픽이 먼저 특정 방법으로 디코딩되거나 전처리되어야 한다는 점에 유의하십시오. 필수 전처리기를 비활성화한 경우, 전처리기가 네트워크 분석 정책 모듈 인터페이스에서 비활성화 상태로 남아 있더라도 시스템은 자동으로 전처리기를 현재의 설정으로 사용합니다.

참고 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 서로 보완해야 합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

시스템은 사용자당 1개의 네트워크 분석 정책을 캐시합니다. 네트워크 분석 정책을 수정하는 동안 모든 메뉴 또는 다른 페이지로 이동하는 다른 경로를 선택하는 경우, 해당 페이지를 벗어난다고 해도 변경 사항은 시스템 캐시에 유지됩니다. 위 표에서 수행할 수 있는 작업 외에도, 11-1페이지의 네트워크 분석 및 침입 정책의 이해는 탐색 패널 사용, 문제 해결, 및 변경 사항 커밋에 관한 정보를 제공합니다.

네트워크 분석 정책을 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 구성하려는 네트워크 분석 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

네트워크 분석 정책 편집기가 Policy Information(정책 정보) 페이지 및 왼쪽 탐색 패널에 집중적으로 나타납니다.

단계 7 정책을 수정합니다. 상기 요약된 모든 작업을 수행합니다.

단계 8 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

전처리기의 영향을 받도록 트래픽 설정

라이센스: 모두

인라인 배포에서 일부 전처리기는 트래픽을 수정하고 차단할 수 있습니다. 예를 들면 다음과 같습니다.

- 인라인 표준화 전처리기는 패킷을 정규화하여 다른 전처리기와 침입 규칙 엔진에 의한 분석을 위해 준비합니다. 또한 전처리기의 **Block Unrecoverable TCP Header Anomalies(복구 불능 TCP 헤더 이상 징후 차단)** 및 **Allow These TCP Options(이러한 TCP 옵션 허용)** 옵션을 사용하여 특정 패킷을 차단할 수 있습니다. 자세한 내용은 17-6페이지의 인라인 트래픽 표준화를 참고하십시오.
- 시스템은 잘못된 체크섬이 포함된 패킷을 삭제할 수 있습니다(17-5페이지의 체크섬 확인 참고).
- 시스템은 속도 기반 공격 방지 설정과 일치하는 패킷을 삭제할 수 있습니다(21-10페이지의 속도 기반 공격 방지 참고).

네트워크 분석 정책에서 트래픽에 영향을 주도록 구성된 전처리기의 경우, 전처리기를 활성화하고 올바르게 구성해야 하며, 또한 디바이스 인라인을 올바르게 구축해야 합니다. 마지막으로, 네트워크 분석 정책의 **Inline Mode(인라인 모드)** 설정을 활성화해야 합니다.

구성이 인라인 배포에서 실제로는 트래픽을 수정하지 않으면서 어떻게 작동하는지 평가하려는 경우 인라인 모드를 비활성화하면 됩니다. 수동 배포에서 시스템은 인라인 모드에 관계없이 트래픽에 영향을 줄 수 없다는 점에 유의하십시오.

팁 인라인 배포에서 Cisco는 인라인 모드를 활성화하고 **Normalize TCP Payload(TCP 페이로드 표준화)** 옵션이 활성화된 인라인 표준화 전처리기를 구성할 것을 권장합니다. 수동 배포에서 Cisco는 적응형 프로파일을 구성할 것을 권장합니다.

인라인 배포에서 트래픽을 전처리기의 영향을 받도록 설정할지 여부를 지정하려면 다음을 수행합니다

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘()(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 트래픽을 전처리기의 영향을 받도록 설정할지 여부를 지정합니다.

- 트래픽을 전처리기의 영향을 받도록 설정하려면, **Inline Mode(인라인 모드)**를 활성화합니다.
- 트래픽을 전처리기의 영향을 받지 않도록 설정하려면 **Inline Mode(인라인 모드)**를 비활성화합니다.

단계 8 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

네트워크 분석 정책에서 전처리기 구성

라이센스: 모두

*전처리기*는 트래픽을 정규화하고 프로토콜 이상 징후를 확인하여 트래픽의 추가 검사를 준비합니다. 전처리기는 패킷에서 구성한 전처리기 옵션을 트리거하는 경우 전처리기 이벤트를 생성합니다. 네트워크 분석 정책에 대한 기본 정책은 기본적으로 활성화되는 전처리기 및 각각에 대한 기본 구성을 결정합니다.

네트워크 분석 정책의 탐색 패널에 있는 **Settings(설정)**를 선택하는 경우, 정책은 유형 별 전처리기를 나열합니다. Settings(설정) 페이지에서 네트워크 분석 정책의 전처리기를 활성화 또는 비활성화할 수 있으며, 전처리기 구성 페이지에 액세스할 수도 있습니다.

이를 구성하려면 전처리기를 활성화해야 합니다. 전처리기를 활성화하면, 전처리기 구성 페이지로 연결되는 하위 링크가 탐색 패널의 **Settings(설정)** 링크 아래에 나타나고, Settings(설정) 페이지의 전처리기 옆에 구성 페이지로 연결되는 **Edit(수정)** 링크가 나타납니다.

팁 전처리기의 구성을 기본 정책의 설정으로 되돌리려면, 전처리기 구성 페이지에서 **Revert to Defaults(기본값으로 되돌리기)**를 클릭합니다. 메시지가 표시되면 복원할 것인지 확인합니다.

전처리기를 비활성화하면, 하위 링크 및 **Edit(수정)** 링크는 더 이상 표시되지 않지만, 구성은 유지됩니다. 특정 분석을 수행하려면 많은 전처리기와 침입 규칙에서 트래픽이 특정 방법으로 먼저 디코딩되거나 전처리되어야 한다는 점에 유의하십시오. 필수 전처리기를 비활성화한 경우, 전처리기가 네트워크 분석 정책 모듈 인터페이스에서 비활성화 상태로 남아 있더라도 시스템은 자동으로 전처리기를 현재의 설정으로 사용합니다.

참고 대부분의 경우, 전처리기는 특정 전문가가 구성해야 하며 거의 수정이 필요하지 않습니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 서로 보완해야 합니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

전처리 구성을 수정하려면 구성 및 네트워크에 미치는 잠재적 영향에 대한 이해가 필요합니다. 다음 섹션에서는 각 전처리기에 대한 특정 구성의 세부 사항으로 연결되는 링크를 제공합니다.

애플리케이션 레이어 프리프로세서

애플리케이션 레이어 프로토콜 디코더는 특정 패킷 데이터 유형을 침입 규칙 엔진이 분석할 수 있는 형식으로 표준화합니다.

표 14-3 애플리케이션 레이어 프리프로세서 설정

정보	참고 사항
DCE/RPC 구성	15-2페이지의 DCE/RPC 트래픽 디코딩
DNS 구성	15-14페이지의 DNS 이름 서버 응답에서 익스플로잇 탐지
FTP 및 텔넷 구성	15-18페이지의 FTP 및 텔넷 트래픽 디코딩
HTTP 구성	15-32페이지의 HTTP 트래픽 디코딩
Sun RPC 구성	15-47페이지의 Sun RPC 전처리기의 사용
SIP 구성	15-49페이지의 세션 시작 프로토콜 디코딩
GTP 명령 채널 구성	15-54페이지의 GTP 명령 채널 구성
IMAP 구성	15-55페이지의 IMAP 트래픽 디코딩
POP 구성	15-58페이지의 POP 트래픽 디코딩
SMTP 구성	15-61페이지의 SMTP 트래픽 디코딩
SSH 구성	15-69페이지의 SSH 전처리기를 사용한 익스플로잇 탐지
SSL 구성	15-73페이지의 SSL 전처리기 사용

SCADA 프리프로세서

Modbus 및 DNP3 프리프로세서는 트래픽 변칙을 탐지하고 침입 규칙 엔진에 검사를 위한 데이터를 제공합니다.

표 14-4 SCADA 프리프로세서 설정

정보	참고 사항
Modbus 구성	16-1페이지의 Modbus 전처리기 구성
DNP3 구성	16-3페이지의 DNP3 전처리기 구성

전송/네트워크 레이어 프리프로세서

네트워크 및 전송 레이어 프리프로세서는 네트워크 및 전송 레이어에서 익스플로잇을 탐지합니다. 패킷이 프리프로세서로 전송되기 전, 패킷 디코더는 프리프로세서 및 침입 규칙 엔진이 쉽게 사용할 수 있는 형식으로 패킷 헤더 및 페이로드를 변환하고 패킷 헤더에서 비정상적인 각종 작업을 탐지합니다.

표 14-5 전송 및 네트워크 레이어 프리프로세서 설정

정보	참고 사항
체크섬 확인	17-5페이지의 체크섬 확인
인라인 표준화	17-6페이지의 인라인 트래픽 표준화
IP 조각 모음	17-12페이지의 IP 패킷 조각 모음
패킷 디코딩	17-16페이지의 패킷 디코딩 이해
TCP 스트림 구성	17-20페이지의 TCP 스트림 전처리 사용
UDP 스트림 구성	17-32페이지의 UDP 스트림 전처리 사용

일부 고급 전송 및 네트워크 프리프로세서 설정은 액세스 제어 정책을 적용하는 모든 네트워크, 영역에 전역적으로 적용됩니다. 이러한 고급 설정은 네트워크 분석 정책보다는 액세스 제어 정책에서 구성합니다(17-1페이지의 고급 전송/네트워크 설정 구성 참고).

특정 위협 탐지

Back Orifice 전처리기는 Back Orifice 매직 쿠키에 대한 UDP 트래픽을 분석합니다. 스캔 활동을 보고하도록 포트스캔 탐지기를 구성할 수 있습니다. 속도 기반 공격 방지는 네트워크를 마비시키도록 설계된 굉장히 많은 수의 동시 연결 및 SYN 플러드로부터 네트워크를 보호하는 데 도움이 될 수 있습니다.

표 14-6 특정 위협 탐지 설정

정보	참고 사항
Back Orifice 탐지	21-1페이지의 Back Orifice 탐지
포트 스캔 탐지	21-3페이지의 포트 스캔 탐지
속도 기반 공격 방지	21-10페이지의 속도 기반 공격 방지

침입 정책에서 ASCII 텍스트의 신용카드 번호 및 주민등록번호/사회보장번호 같은 민감한 데이터를 탐지하는 민감한 데이터 프리프로세서를 구성할 수 있습니다. 자세한 내용은 21-20페이지의 민감한 데이터 검색을 참고하십시오.

현재 네트워크 분석 설정 보고서 생성

라이센스: 모두

네트워크 분석 정책 보고서는 특정 시점의 정책 구성에 대한 기록입니다. 시스템은 기본 정책의 설정과 정책 레이어의 설정을 결합하며, 어느 설정이 기본 정책 또는 정책 레이어에서 시작된 것인지 구별하지 않습니다.

사용자는 감사 목적으로나 현재 구성을 검사하기 위해 다음 정보를 포함하는 보고서를 사용할 수 있습니다.

표 14-7 네트워크 분석 정책 보고서 섹션

섹션	설명
정책 정보	정책의 이름과 설명, 정책을 최종 수정한 사용자의 이름, 정책이 최종 수정된 날짜와 시간을 제공합니다. 또한 인라인 표준화의 활성화 가능 여부, 현재 규칙 업데이트 버전, 기반 정책이 현재 규칙 업데이트로 잠겼는지 여부도 나타납니다.
설정	활성화된 모든 프리프로세서 설정 및 해당 구성을 나열합니다.

두 가지 네트워크 분석 정책 또는 동일한 정책의 두 개정을 비교하는 비교 보고서를 생성할 수도 있습니다. 자세한 내용은 14-9페이지의 두 네트워크 분석 정책 또는 수정 버전 비교를 참고하십시오.

네트워크 분석 정책 보고서를 보려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 보고서를 생성하려는 정책 옆에 있는 보고서 아이콘( )을 클릭합니다. 네트워크 분석 정책 보고서를 생성하기 전에 모든 변경 사항을 커밋해야 합니다. 커밋된 변경 사항만 보고서에 나타납니다.

시스템이 보고서를 생성합니다. 보고서를 컴퓨터에 저장하라는 메시지가 표시됩니다.

두 네트워크 분석 정책 또는 수정 버전 비교

라이센스: 모두

조직의 표준을 준수하거나 시스템 성능을 최적화하기 위해 정책 변경 사항을 검토할 경우 두 네트워크 분석 정책 간의 차이를 확인할 수 있습니다. 두 네트워크 분석 정책 또는 동일한 네트워크 분석 정책의 두 개정을 비교할 수 있습니다. 비교한 후 선택적으로 두 정책 또는 정책 수정 버전의 차이를 기록하는 PDF 보고서를 생성할 수 있습니다.

네트워크 분석 정책 또는 정책 개정의 비교에 사용할 수 있는 두 가지 툴이 있습니다.

- 비교 보기에는 두 네트워크 분석 정책 또는 네트워크 분석 정책 개정 간의 차이점만 나란히 표시됩니다. 각 정책 또는 정책 개정의 이름은 비교 보기 왼쪽과 오른쪽의 제목 표시줄에 나타납니다.

  이를 사용하여 웹 인터페이스에서 차이점이 강조 표시된 상태로 모듈 인터페이스에서 두 정책 개정 버전을 모두 살펴보고 탐색할 수 있습니다.

- 비교 보고서는 두 네트워크 분석 정책 또는 네트워크 분석 정책 개정의 차이점에 대해서만 기록을 생성하는데, 그 형식은 네트워크 분석 정책 보고서와 비슷하지만 PDF 형식입니다.

  이를 사용하여 향후 점검을 위해 정책 비교를 저장, 복사, 인쇄, 공유할 수 있습니다.

정책 비교 도구를 이해하고 사용하는 데 대한 자세한 내용은 다음을 참고하십시오.

- 14-10페이지의 네트워크 분석 정책의 비교 보기 사용
- 14-10페이지의 네트워크 분석 정책 비교 보고서 사용

네트워크 분석 정책의 비교 보기 사용

라이센스: 모두

비교 보기에서는 두 정책 또는 정책 개정을 나란히 표시하며, 각 정책 또는 정책 개정은 비교 보기의 좌우 제목 표시줄에 있는 이름으로 식별됩니다. 최종 수정 시간 및 수정한 최종 사용자는 정책 이름과 함께 표시됩니다.

두 정책 간 차이점은 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책 사이에서 다름을 나타내고, 그러한 차이점은 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 한 정책에서는 나타나지만 다른 정책에서는 나타나지 않음을 표시합니다.

다음 표에서 모든 작업을 수행할 수 있습니다.

표 14-8 네트워크 분석 정책 비교 보기 작업

목적	방법
개별 변경 사항 탐색	제목 표시줄 상단의 **Previous(이전)** 또는 **Next(다음)**를 클릭합니다. 좌우 측면 사이에 있는 이중 화살표 아이콘()을 움직여 **Difference(차이)** 수를 조정하여 표시되는 차이점이 무엇인지 확인합니다.
새로운 정책 비교 보기 생성하기	**New Comparison(새로 비교)**을 클릭합니다. **Select Comparison(비교 선택)** 창이 나타납니다. 자세한 내용은 14-10페이지의 네트워크 분석 정책 비교 보고서 사용을 참고하십시오.
정책 비교 보고서 생성하기	**Comparison Report(비교 보고서)**를 클릭합니다. 정책 비교 보고서에서는 두 정책 또는 정책 개정의 차이점만 나열하는 PDF 문서를 생성합니다.

네트워크 분석 정책 비교 보고서 사용

라이센스: 모두

네트워크 분석 정책 비교 보고서는 두 네트워크 분석 정책 또는 동일한 네트워크 분석 정책의 두 개정 간 모든 차이점을 PDF에서 네트워크 분석 정책 비교 보기 형태로 기록한 것입니다. 두 네트워크 분석 정책 구성의 차이점을 더 자세히 살펴보고 조사 결과를 저장하여 배포하는 데 이 보고서를 사용할 수 있습니다.

액세스 권한이 있는 모든 네트워크 분석 정책에 대해 비교 보기에서 정책 비교 보고서를 생성할 수 있습니다. 정책 보고서를 생성하기 전에 모든 변경 사항을 저장해야 합니다. 보고서에는 저장된 변경 사항만 표시됩니다.

정책 비교 보고서의 형식은 한 가지를 제외하면 정책 보고서와 동일합니다. 정책 보고서는 정책의 모든 구성을 포함하는데, 정책 비교 보고서에는 정책 간 상이한 구성만 포함됩니다. 네트워크 분석 정책 비교 보고서는 14-9페이지의 표 14-7에 설명된 섹션을 포함합니다.

팁 액세스 제어, 침입, 파일 정책을 비교하는 데에도 비슷한 절차를 사용할 수 있습니다.

두 네트워크 분석 정책 또는 정책 개정을 비교하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 **Compare Policies(정책 비교)**를 클릭합니다.

Select Comparison(비교 선택) 창이 나타납니다.

단계 7 **Compare Against(비교 대상)** 드롭다운 목록에서 비교를 원하는 유형을 선택합니다.

- 두 가지의 서로 다른 정책을 비교하려면, **Other Policy(다른 정책)**를 선택합니다.

  페이지가 새로 고쳐지고 Policy A(정책 A) 및 Policy B(정책 B) 드롭다운 목록이 나타납니다.
- 동일한 정책의 두 개정을 비교하려면 **Other Revision(다른 개정 버전)**을 선택합니다.

  페이지가 새로 고쳐지고 Policy(정책), Revision A(개정 버전 A) 및 Revision B(개정 버전 B) 드롭다운 목록이 나타납니다.

단계 8 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 가지의 서로 다른 정책을 비교할 경우, Policy A(정책 A)와 Policy B(정책 B) 드롭다운 목록에서 비교하려는 정책을 선택합니다.
- 동일한 정책의 두 개정을 비교하는 경우 Policy(정책)를 선택한 다음, Revision A(개정 버전 A) 및 Revision B(개정 버전 B) 드롭다운 목록에서 비교할 타임스탬프된 개정을 선택합니다.

단계 9 정책 비교 보기를 표시하려면 **OK(확인)**를 클릭합니다.

비교 보기가 나타납니다.

단계 10 또는 **Comparison Report(비교 보고서)**를 클릭하여 네트워크 분석 정책 비교 보고서를 생성합니다.

네트워크 분석 정책 비교 보고서가 나타납니다. 보고서를 컴퓨터에 저장하라는 메시지가 표시됩니다.

애플리케이션 레이어 전처리기 사용

네트워크 분석 정책에서 애플리케이션 레이어 전처리기를 구성하는데, 이는 침입 정책에서 활성화된 규칙을 사용하여 트래픽이 검사될 수 있도록 준비합니다. 자세한 내용은 11-1페이지의 네트워크 분석 및 침입 정책의 이해를 참고하십시오.

애플리케이션 레이어 프로토콜은 다양한 방법으로 동일한 데이터를 나타낼 수 있습니다. Cisco 패킷 데이터의 특정 유형을 침입 규칙 엔진이 분석할 수 있는 형식으로 표준화하는 애플리케이션 레이어 프로토콜 디코더를 제공합니다. 애플리케이션 레이어 프로토콜 인코딩을 표준화하면 규칙 엔진이 동일한 콘텐츠 관련 규칙을 해당 데이터가 다르게 표시되는 패킷에 보다 효율적으로 적용할 수 있으며, 유익한 결과를 얻을 수 있습니다.

침입 정책에서 동반되는 전처리기 규칙을 활성화하지 않는 경우 대부분의 경우 전처리기는 이벤트를 생성하지 않는다는 점에 유의하십시오. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 15-2페이지의 DCE/RPC 트래픽 디코딩에서는 DCE/RPC 전처리기에 대해 설명하고, 회피 시도를 방지하고 DCE/RPC 트래픽에서 이상 징후를 탐지하기 위해 이를 구성하는 방법에 대해 설명합니다.
- 15-14페이지의 DNS 이름 서버 응답에서 익스플로잇 탐지에서는 DNS 전처리기를 설명하고 DNS 이름 서버 응답의 3가지 특정 익스플로잇을 탐지하기 위해 이를 구성하는 방법에 대해 설명합니다.
- 15-18페이지의 FTP 및 텔넷 트래픽 디코딩에서는 FTP/Telnet 디코더에 대해 설명하고 FTP 및 Telnet 트래픽을 표준화하고 디코딩하기 위해 이를 구성하는 방법에 대해 설명합니다.
- 15-32페이지의 HTTP 트래픽 디코딩에서는 HTTP 디코더에 대해 설명하고 HTTP 트래픽을 표준화하도록 이를 구성하는 방법에 대해 설명합니다.
- 15-47페이지의 Sun RPC 전처리기의 사용에서는 RPC 디코더에 대해 설명하고 RPC 트래픽을 표준화하도록 이를 구성하는 방법에 대해 설명합니다.
- 15-49페이지의 세션 시작 프로토콜 디코딩에서는 SIP 전처리기를 사용하여 SIP 트래픽에서 이상 징후를 탐지하고 디코딩하는 방법에 대해 설명합니다.
- 15-54페이지의 GTP 명령 채널 구성에서는 GTP 전처리기를 사용하여 패킷 디코더에 의해 추출된 GTP 명령 채널 메시지로 규칙 엔진을 제공하는 방법에 대해 설명합니다.
- 15-55페이지의 IMAP 트래픽 디코딩에서는 IMAP 전처리기를 사용하여 IMAP 트래픽에서 이상 징후를 탐지하고 디코딩하는 방법에 대해 설명합니다.
- 15-58페이지의 POP 트래픽 디코딩에서는 POP 전처리기를 사용하여 POP 트래픽에서 이상 징후를 탐지하고 디코딩하는 방법에 대해 설명합니다.
- 15-61페이지의 SMTP 트래픽 디코딩에서는 SMTP 디코더에 대해 설명하고 SMTP 트래픽을 디코딩하고 표준화하도록 이를 구성하는 방법에 대해 설명합니다.

- 15-69페이지의 SSH 전처리기를 사용한 익스플로잇 탐지에서는 SSH로 암호화된 트래픽에서 익스플로잇을 확인하고 처리하는 방법에 대해 설명합니다.
- 15-73페이지의 SSL 전처리기 사용에서는 SSL 전처리기를 사용하여 암호화된 트래픽을 식별하고 해당 트래픽에 대한 검사를 중단함으로써 잘못된 긍정을 삭제하는 방법에 대해 설명합니다.
- 16-1페이지의 SCADA 전처리 구성에서는 Modbus 및 DNP3 전처리기를 사용하여 해당 트래픽에서 이상 징후를 탐지하고 특정 프로토콜 필드를 검사하기 위해 침입 규칙 엔진에 데이터를 제공하는 방법에 대해 설명합니다.

DCE/RPC 트래픽 디코딩

라이센스: 보호

DCE/RPC 프로토콜을 사용하면 개별 네트워크 호스트에 있는 프로세스가 동일한 호스트에 있는 것처럼 통신할 수 있습니다. 이 프로세스 간 통신은 일반적으로 TCP 및 UDP 기반의 호스트 간에 전송됩니다. TCP 전송 내에서, DCE/RPC는 또한 Windows 및 UNIX 또는 Linux와 유사한 운영 체제로 구성되어 있는 혼합된 환경에서 프로세스 간 통신에 사용되는 오픈 소스 SMB 구현인 Windows 서버 메시지 블록(SMB) 프로토콜 또는 Samba에서 캡슐화될 수 있습니다. 또한, 네트워크의 Windows IIS 웹 서버는 IIS RPC over HTTP를 사용할 수 있는데, 이는 분산된 통신을 방화벽을 통해 프록시 TCP에서 전송되는 DCE/RPC 트래픽에 제공합니다.

DCE/RPC 전처리기 옵션 및 기능의 설명에는 MSRPC로 알려진 DCE/RPC의 Microsoft 구현이 포함됩니다. SMB 옵션 및 기능에 대한 설명은 SMB 및 Samba를 모두 나타냅니다.

대부분의 DCE/RPC 익스플로잇이 실제로 Windows 또는 Samba를 실행하는 네트워크의 모든 호스트가 될 수 있는 DCE/RPC 서버를 대상으로 하는 DCE/RPC 클라이언트 요청에서 발생하더라도, 익스플로잇은 서버 응답에서도 발생할 수 있습니다. DCE/RPC 전처리기는 RPC over HTTP 버전 1을 사용하는 TCP에서 전송되는 DCE/RPC를 포함하여 TCP, UDP 및 SMB 전송에서 캡슐화된 DCE/RPC 요청 및 응답을 탐지합니다. 전처리기는 DCE/RPC 데이터 스트림을 분석하고 이상 징후를 보이는 작업과 DCE/RPC 트래픽 내 회피 기술을 탐지합니다. 또한 SMB 데이터 스트림을 분석하고 SMB 이상 작업 및 회피 기술을 탐지합니다.

DCE/RPC 전처리기는 또한 IP 조각 모음 전처리기가 제공하는 IP 조각 모음 및 TCP 스트림 전처리기가 제공하는 TCP 스트림 리어셈블리에 더해 SMB의 분할을 해제하고 DCE/RPC 조각을 모읍니다. 17-20페이지의 TCP 스트림 전처리 사용 및 17-12페이지의 IP 패킷 조각 모음을 참고하십시오.

마지막으로, DCE/RPC 전처리기는 규칙 엔진에 의한 처리를 위해 DCE/RPC 트래픽을 표준화합니다. 특정 DCE/RPC 규칙 키워드를 사용하여 DCE/RPC를 탐지하는 데 대한 내용은 23-58페이지의 DCE/RPC 키워드를 참고하십시오. 서비스, 운영 및 스텁 데이터.

전처리기 작동 방식을 제어하는 모든 전역 옵션을 수정함으로써, 그리고 사용자 네트워크의 DCE/RPC 서버를 그 위에서 운영되는 IP 주소 및 Windows 또는 Samba 버전 중 하나로 식별하는 하나 이상의 대상 기반 서버 정책을 지정함으로써 DCE/RPC 전처리기를 구성합니다.

132 또는 133의 생성기 ID(GID)가 있는 DCE/RPC 전처리기 규칙에서 이벤트를 생성하려는 경우 이 규칙을 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 15-3페이지의 전역 DCE/RPC 옵션 선택
- 15-4페이지의 대상 기반 DCE/RPC 서버 정책의 이해
- 15-5페이지의 DCE/RPC 전송의 이해
- 15-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택
- 15-11페이지의 DCE/RPC 전처리기 구성

전역 DCE/RPC 옵션 선택

라이센스: 보호

전역 DCE/RPC 전처리기 옵션은 전처리기가 작용하는 방법을 제어합니다. **Memory Cap Reached(메모리 용량 도달)** 옵션을 제외한 경우, 이 옵션을 변경하면 성능 또는 탐지 기능에 부정적인 영향을 미칠 수 있습니다. 전처리기 및 전처리기와 활성화된 DCE/RPC 규칙 간의 상호 작용을 완벽하게 파악하지 않은 경우 이들을 변경할 수 없습니다. 특히, **Maximum Fragment Size(최대 조각 크기)** 옵션 및 **Reassembly Threshold(리어셈블리 임계값)** 옵션이 규칙이 탐지해야 하는 수준보다 크거나 동일한지 확인합니다. 자세한 내용은 23-17페이지의 콘텐츠 일치 제한 및 23-30페이지의 Byte_Jump 및 Byte_Test 사용을 참고하십시오.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

최대 조각 크기

Enable Defragmentation(조각 모음 활성화)을 선택하면 1514에서 65535바이트까지 허용된 최대 DCE/RPC 조각 길이를 지정합니다. 전처리기는 조각 모음 전에 처리를 위해 지정된 크기에 큰 조각을 자르지만 실제 패킷을 변경하지 않습니다. 빈 필드는 이 옵션을 비활성화합니다.

리어셈블리 임계값

Enable Defragmentation(조각 모음 활성화)을 선택하면, 0은 이 옵션을 비활성화하고 1에서 65535 바이트는 조각화된 DCE/RPC 바이트의 최소 수와, 해당되는 경우, 리어셈블된 패킷을 규칙 엔진에 전송하기 전에 대기할 세분화된 SMB 바이트의 최소 수를 지정합니다. 낮은 값은 조기 검색 가능성을 증가시키지만 성능에 부정적인 영향을 미칠 수 있습니다. 이 옵션을 활성화하면 성능 영향을 테스트해야 합니다.

조각 모음 활성화

조각화된 DCE/RPC 트래픽을 조각 모음할지 여부를 지정합니다. 비활성화할 경우, 전처리기는 계속해서 이상 징후를 탐지하고 규칙 엔진에 DCE/RPC 데이터를 전송하지만, 조각화된 DCE/RPC 데이터에서 유실된 익스플로잇의 위험에 노출됩니다.

이 옵션을 사용하면 DCE/RPC 트래픽을 조각 모음하지 않는 유연성이 제공되지만, 대부분의 DCE/RPC 익스플로잇은 익스플로잇을 숨기기 위해 조각화를 이용하려고 시도합니다. 이 옵션을 비활성화하면 대부분의 알려진 익스플로잇을 우회하여 많은 수의 잘못된 부정이 야기됩니다.

메모리 용량 도달

전처리기에 할당된 최대 메모리 한도에 도달하거나 초과할 경우 이를 탐지합니다. 최대 메모리 용량에 도달하거나 초과할 경우, 전처리기는 메모리 용량 이벤트를 야기하고 해당 세션의 나머지 부분을 무시하는 세션과 관련된 보류 중인 모든 데이터를 비웁니다.

규칙 133:1을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

SMB 세션의 정책 자동 탐지

SMB `Session Setup AndX` 요청 및 응답에서 확인된 Windows 또는 Samba 버전을 탐지합니다. 탐지된 버전이 **Policy(정책)** 구성 옵션에 대해 구성된 Windows 또는 Samba 버전과 다른 경우, 탐지된 버전은 해당 세션만을 위해 구성된 버전을 대체합니다. 자세한 내용은 15-4페이지의 대상 기반 DCE/RPC 서버 정책의 이해를 참고하십시오.

예를 들어, 사용자가 Windows XP에 **Policy(정책)**를 설정하고 전처리기가 Windows Vista를 탐지하는 경우, 전처리기는 해당 세션에 대한 Windows Vista 정책을 사용합니다. 다른 설정은 계속 적용됩니다.

DCE/RPC 전송이 SMB(즉, 전송이 TCP 또는 UDP인 경우)가 아닐 때는 버전을 탐지하고 정책을 자동으로 구성할 수 없습니다.

이 옵션을 활성화하려면 드롭다운 목록에서 다음 중 하나를 선택하십시오.

- **Client(클라이언트)**를 선택하여 정책 유형에 대한 서버-클라이언트 트래픽을 검사합니다.
- **Server(서버)**를 선택하여 정책 유형에 대한 클라이언트-서버 트래픽을 검사합니다.
- **Both(모두)**를 선택하여 정책 유형에 대한 서버-클라이언트 트래픽 및 클라이언트-서버 트래픽을 검사합니다.

대상 기반 DCE/RPC 서버 정책의 이해

라이센스: 보호

하나 이상의 대상 기반 서버 정책을 생성하여 DCE/RPC 전처리기가 지정된 유형의 서버가 처리하는 것과 동일한 DCE/RPC 트래픽을 검사하도록 구성할 수 있습니다. 대상 기반 정책 구성에는 사용자 네트워크에서 식별된 호스트에서 운영되는 Windows 또는 Samba 버전 확인, 전송 프로토콜 활성화, DCE/RPC 트래픽을 해당 호스트로 전송하는 포트 지정 및 다른 서버에 특정적인 문자 옵션 설정이 포함되어 있습니다.

Windows 및 Samba DCE/RPC 구현은 매우 다릅니다. 예를 들어, DCE/RPC 트래픽을 조각 모음할 때 Windows의 모든 버전은 첫 번째 조각에서 DCE/RPC 컨텍스트 ID를 사용하고, Samba의 모든 버전은 마지막 조각에서 컨텍스트 ID를 사용합니다. 다른 예로, 특정 함수 호출을 식별하기 위해 Windows Vista는 첫 번째 조각의 opnum(작업 번호) 헤더 필드를 사용하고, Samba 및 다른 모든 Windows 버전은 마지막 조각의 opnum 필드를 사용합니다.

또한 Windows 및 Samba SMB 구현에도 상당한 차이점이 있습니다. 예를 들어, 명명된 파이프로 작업할 때 Windows는 SMB OPEN 및 READ 명령을 인식하지만 Samba는 이러한 명령을 인식하지 않습니다.

DCE/RPC 전처리기를 활성화할 때, 기본 대상 기반 정책을 자동으로 활성화합니다. 또는, **Policy(정책)** 드롭다운 목록에서 올바른 버전을 선택하여 다른 Windows 또는 Samba 버전을 실행하는 다른 호스트를 대상으로 하는 대상 기반 정책을 추가할 수 있습니다. 기본 대상 기반 정책은 다른 대상 기반 정책에 포함되지 않는 모든 호스트에 적용됩니다.

각 대상 기반 정책에서, 하나 이상의 전송을 활성화하고 각각에 대해 *탐지 포트*를 지정할 수 있습니다. 또한 *자동 탐지 포트*를 활성화하고 지정할 수 있습니다. 자세한 내용은 15-5페이지의 DCE/RPC 전송의 이해를 참고하십시오.

다른 대상 기반 정책 옵션을 구성할 수도 있습니다. 사용자가 식별하는 하나 이상의 공유 SMB 리소스에 연결하려는 시도가 있는 경우 이를 탐지하도록 전처리기를 설정할 수 있습니다. SMB 트래픽의 파일을 탐지하고, 탐지한 파일에서 지정한 바이트 수를 검사하도록 전처리기를 구성할 수 있습니다. 또한 SMB 프로토콜 전문성을 가진 사용자만 변경할 수 있는 고급 옵션을 변경할 수 있습니다. 이 옵션을 통해 연속된 많은 SMB AndX 명령이 지정된 최대치를 초과하는 경우 이를 탐지하도록 전처리기를 설정할 수 있습니다.

각 대상 기반 정책에서 다음을 수행할 수 있습니다,

- 하나 이상의 전송을 활성화하고 각각에 대해 *탐지 포트*를 지정합니다.
- *자동 탐지 포트*를 활성화하고 지정합니다. 자세한 내용은 15-5페이지의 DCE/RPC 전송의 이해를 참고하십시오.
- 사용자가 식별하는 하나 이상의 공유 SMB 리소스에 연결하려는 시도가 있는 경우 이를 탐지하도록 전처리기를 설정할 수 있습니다.
- SMB 트래픽의 파일을 탐지하고, 탐지한 파일에서 지정한 바이트 수를 검사하도록 전처리기를 구성할 수 있습니다.

- 또한 SMB 프로토콜 전문성을 가진 사용자만 변경할 수 있는 고급 옵션을 변경할 수 있습니다. 이 옵션을 통해 연속된 많은 SMB AndX 명령이 지정된 최대치를 초과하는 경우 이를 탐지하도록 전처리기를 설정할 수 있습니다.

Auto-Detect Policy on SMB Session(SMB 세션에서 정책 자동 탐지) 전역 옵션을 활성화하여 SMB가 DCE/RPC 전송일 때 세션별로 대상이 되는 정책에 대해 구성된 정책 유형을 자동으로 대체할 수 있다는 점에 유의하십시오. 15-3페이지의 SMB 세션의 정책 자동 탐지를 참고하십시오.

DCE/RPC 전처리기 내 SMB 트래픽 파일 탐지를 활성화하는 것 외에도, 파일 정책을 구성하여 해당 파일을 선택적으로 수집 및 차단할 수 있습니다. 자세한 내용은 24-9페이지의 파일 정책 생성 및 24-10페이지의 파일 규칙 작업을 참고하십시오.

DCE/RPC 전송의 이해

라이센스: 보호

각 대상 기반 정책에서 TCP, UDP, SMB 및 RPC over HTTP 전송 중 하나 이상을 활성화할 수 있습니다. 전송을 활성화할 때, 하나 이상의 *탐지 포트*, 즉, DCE/RPC 트래픽을 전달하는 것으로 알려진 포트를 지정해야 합니다. 또는, *자동 탐지 포트*, 즉, 전처리기가 DCE/RPC 트래픽을 탐지하는 경우에만 포트가 DCE/RPC 트래픽을 전송하고 처리를 계속할지 결정하기 위해 전처리기가 처음 테스트하는 포트를 활성화하고 지정할 수도 있습니다.

Cisco는 기본 탐지 포트를 사용할 것을 권장합니다. 이는 잘 알려진 포트이거나 그 외 각 프로토콜을 위해 일반적으로 사용되는 포트입니다. 기본이 아닌 포트에서 DCE/RPC 트래픽을 탐지한 경우에만 탐지 포트를 추가합니다.

자동 탐지 포트를 활성화할 때, 자동 탐지 포트가 전체 사용 후 삭제 포트 범위를 포함하기 위해 1024에서 65535까지의 포트 범위에 설정되어 있는지 확인합니다. RPC over HTTP Proxy Auto-Detect Ports(프록시 자동 탐지 포트) 옵션 또는 SMB Auto-Detect Ports(자동 탐지 포트) 옵션에 대한 자동 탐지 포트를 활성화하거나 지정할 가능성이 낮다는 점에 유의하십시오. 이는 지정된 기본 탐지 포트를 제외하고는 이 둘을 위한 트래픽이 발생하거나 잠재력이 있을 가능성이 거의 없기 때문입니다. 또한 자동 탐지는 전송 탐지 포트에서 아직 식별되지 않은 포트에만 발생한다는 점에 유의하십시오. 각 전송에 대한 자동 탐지 포트를 활성화하거나 비활성화하는 것에 대한 권장 사항은 15-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택을 참고하십시오.

Windows 대상 기반 정책에서는 네트워크 트래픽에 맞게 어떤 조합에서나 하나 이상의 전송에 대해 포트를 지정할 수 있지만, Samba 대상 기반 정책에서는 SMB 전송에만 포트를 지정할 수 있습니다.

최소 하나의 전송이 활성화된 DCE/RPC 대상 기반 정책을 추가하는 경우를 제외하면 기본 대상 기반 정책에서 최소 하나의 DCE/RPC 전송을 활성화해야 한다는 점에 유의하십시오. 예를 들어, 모든 DCE/RPC 구현을 위해 호스트를 지정하지만 기본 대상 기반 정책을 지정되지 않은 호스트에 적용하지는 않으려는 경우 기본 대상 기반 정책에 대한 전송을 활성화하지 않습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 15-5페이지의 연결 없는 DCE/RPC 트래픽 및 연결 지향 DCE/RPC 트래픽의 이해
- 15-7페이지의 HTTP 전송 기반의 RPC 이해

연결 없는 DCE/RPC 트래픽 및 연결 지향 DCE/RPC 트래픽의 이해

라이센스: 보호

DCE/RPC 메시지는 DCE/RPC Protocol Data Units(프로토콜 데이터 단위, PDU)의 두 가지 명시적인 프로토콜 중 하나를 준수합니다.

- 연결 지향 DCE/RPC PDU 프로토콜

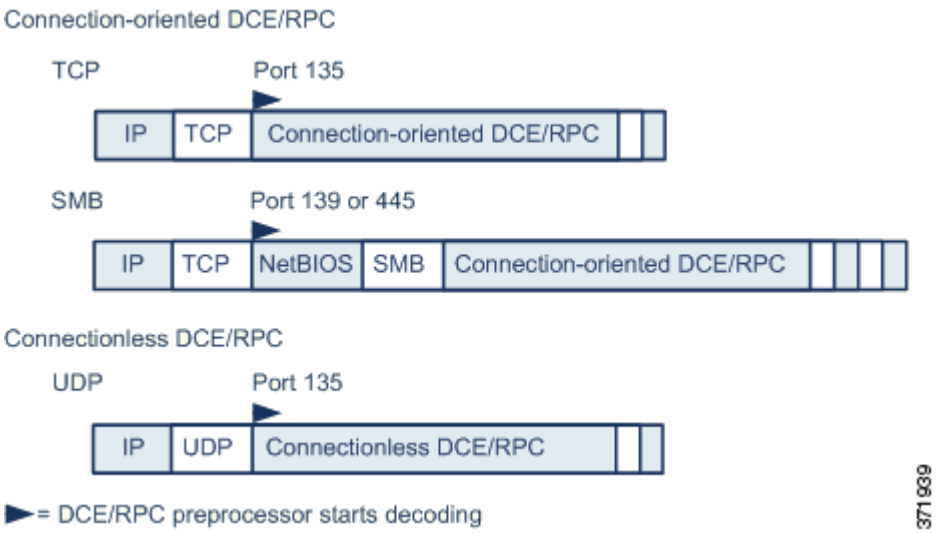
  DCE/RPC 전처리기는 TCP, SMB 및 RPC over HTTP에서 연결 지향 DCE/RPC를 탐지합니다.

- 연결 없는 DCE/RPC PDU 프로토콜

  DCE/RPC 전처리기는 UDP 전송에서 연결 없는 DCE/RPC를 탐지합니다.

2개의 DCE/RPC PDU 프로토콜은 자체 고유한 헤더와 데이터 특성이 있습니다. 예를 들어, 연결 지향 DCE/RPC 헤더 길이는 일반적으로 24바이트이며 연결 없는 DCE/RPC 헤더 길이는 80바이트로 고정됩니다. 또한, 조각화된 연결 없는 DCE/RPC의 정확한 조각 순서는 연결 없는 전송으로 처리할 수 없으며, 연결 없는 DCE/RPC 헤더 값이어야 합니다. 반면, 전송 프로토콜은 연결 지향 DCE/RPC의 정확한 조각 순서를 보장합니다. DCE/RPC 전처리기는 이와 그외 기타 프로토콜 특정 특성을 이용하여 이상 징후 및 다른 회피 기술에 대한 프로토콜 모두를 모니터링하고, 트래픽을 규칙 엔진에 전달하기 전에 디코딩하고 조각 모음합니다.

다음 다이어그램은 DCE/RPC 전처리기가 여러 전송을 위해 DCE/RPC 트래픽을 처리하기 시작하는 시점에 대해 설명합니다.



그림에서 다음에 유의하십시오.

- 잘 알려진 TCP 또는 UDP 포트 135는 TCP와 UDP 전송에서 DCE/RPC 트래픽을 식별합니다.
- 그림은 RPC over HTTP를 포함하지 않습니다.

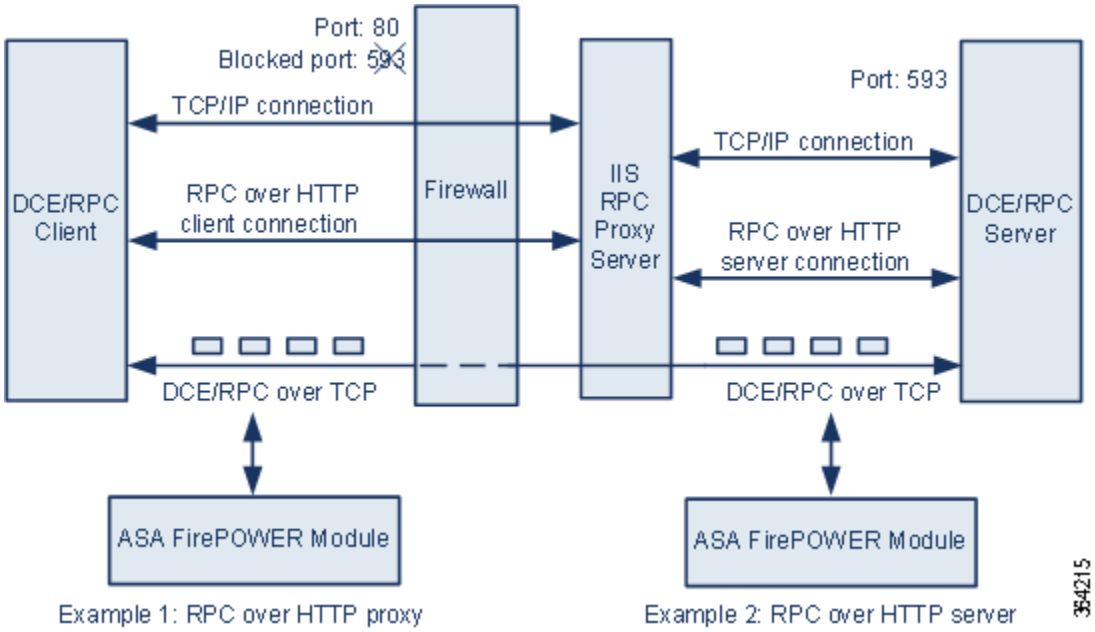
  RPC over HTTP의 경우, 연결 지향 DCE/RPC는 그림에서처럼 HTTP를 통한 초기 구성 시퀀스 후 TCP에 직접 전송됩니다. 자세한 내용은 15-7페이지의 HTTP 전송 기반의 RPC 이해를 참고하십시오.
- DCE/RPC 전처리기는 일반적으로 NetBIOS 세션 서비스의 잘 알려진 TCP 포트 139 또는 이와 유사하게 구현된 잘 알려진 Windows 포트 445에서 SMB 트래픽을 수신합니다.

  SMB에는 DCE/RPC 전송 외에도 많은 기능이 있으므로, 전처리기는 먼저 SMB 트래픽이 DCE/RPC 트래픽을 전달하고 있는지 여부를 테스트하고 전달하고 있는 경우 처리를 계속하며 그렇지 않은 경우 처리를 중지합니다.
- IP는 모든 DCE/RPC 전송을 캡슐화합니다.
- TCP는 모든 연결 지향 DCE/RPC를 전송합니다.
- UDP는 연결 없는 DCE/RPC를 전송합니다.

HTTP 전송 기반의 RPC 이해

라이센스: 보호

HTTP 기반의 Microsoft RPC가 있으면 다음 다이어그램에서처럼 방화벽을 통해 DCE/RPC 트래픽을 터널링할 수 있습니다. DCE/RPC 전처리기는 HTTP 기반의 Microsoft RPC 버전 1을 탐지합니다.



Microsoft IIS 프록시 서버 및 DCE/RPC 서버는 동일한 호스트 또는 다른 호스트에 있을 수 있습니다. 개별 프록시와 서버 옵션은 두 경우 모두를 제공합니다. 그림에서 다음에 유의하십시오.

- DCE/RPC 서버는 DCE/RPC 클라이언트 트래픽에 대한 포트 593을 모니터링하지만, 방화벽은 포트 593을 차단합니다.

  방화벽은 일반적으로 포트 593을 기본값으로 차단합니다.

- RPC over HTTP는 방화벽이 허용할 가능성이 높은 잘 알려진 HTTP 포트 80을 사용하여 DCE/RPC over HTTP를 전송합니다.
- 예 1은 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 간 트래픽을 모니터링하기 위해 **RPC over HTTP proxy(RPC over HTTP 프록시)** 옵션을 선택하는 것에 대해 보여줍니다.
- 예 2는 Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링할 때 **RPC over HTTP server(RPC over HTTP 서버)** 옵션을 선택하는 것에 대해 보여줍니다.
- 트래픽은 RPC over HTTP가 DCE/RPC 클라이언트와 서버 간의 프록시 설정을 완료한 후 연결 지향 DCE/RPC over TCP로만 구성됩니다.

DCE/RPC 대상 기반 정책 옵션 선택

라이센스: 보호

각 대상 기반 정책을 통해 아래의 다양한 옵션을 지정할 수 있습니다. **Memory Cap Reached(메모리 용량 도달)** 및 **Auto-Detect Policy on SMB Session(SMB 세션에서 자동 탐지 정책)** 옵션을 제외한 경우, 이 옵션을 변경하면 성능 또는 탐지 기능에 부정적인 영향을 미칠 수 있다는 점에 유의하십시오. 전처리기 및 전처리기와 활성화된 DCE/RPC 규칙 간의 상호 작용을 완벽하게 파악하지 않은 경우 이들을 변경할 수 없습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

DCE/RPC 대상 기반 서버 정책을 적용할 호스트 IP 주소

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 기본 정책을 비롯한 255개의 총 프로파일을 지정할 수 있습니다. ASA FirePOWER 모듈에서 IPv4 및 IPv6 주소 블록을 지정하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역 의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

정책

모니터링된 네트워크 세그먼트에서 대상 호스트가 사용하는 Windows 또는 Samba DCE/RPC 구현 이 정책에 대한 자세한 내용은 15-4페이지의 대상 기반 DCE/RPC 서버 정책의 이해를 참고하십시오.

Auto-Detect Policy on SMB Session(SMB 세션에서 정책 자동 탐지) 전역 옵션을 활성화하여 SMB가 DCE/RPC 전송일 때 세션별로 이 옵션의 설정을 자동으로 대체할 수 있다는 점에 유의하십시오. 15-3페이지의 SMB 세션의 정책 자동 탐지를 참고하십시오.

SMB 유효하지 않은 공유

하나 이상의 SMB 공유 리소스를 식별하는, 대소문자를 구분하지 않는 영숫자 문자열. 전처리기는 사용자가 지정하는 공유 리소스에 연결하려는 시도가 있는 경우 이를 탐지합니다. 사용자는 쉼표로 구분된 목록에서 여러 공유를 지정할 수 있고, 선택적으로, 공유를 인용구로 묶을 수 있는데, 이는 이전 소프트웨어 버전에서는 필요했지만 더 이상 필요하지 않습니다. 예를 들면 다음과 같습니다.

```
"C$", D$, "admin", private
```

전처리기는 SMB 포트와 SMB 트래픽 탐지를 모두 활성화할 때 SMB 트래픽에서 유효하지 않은 공유를 탐지합니다.

대부분의 경우 Windows에서 명명되었고, 유효하지 않은 공유로 식별된 드라이브에 달러 표시를 추가해야 한다는 점에 유의하십시오. 예를 들어, C$ 또는 "C$"로 드라이브 C를 식별합니다.

규칙 133:26을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

SMB 최대 AndX 체인

연속된 SMB AndX 명령의 0과 255 사이에서 허용할 최대 값. 일반적으로, 연속된 여러 AndX 명령이 이상 작업을 나타내며 회피 시도를 나타낼 수 있습니다. 1을 지정하여 연속된 명령을 허용하지 않거나 0을 지정하여 연속된 명령의 수 탐지를 비활성화합니다.

동반되는 SMB 전처리기 규칙이 활성화되고 연속된 명령의 수가 구성한 값과 동일하거나 초과할 경우 전처리기는 먼저 연속된 명령의 수를 세고 이벤트를 생성한다는 점에 유의하십시오. 그런 다음 처리를 계속 진행합니다.

참고 SMB 프로토콜의 전문가만이 이 옵션의 기본 설정을 변경해야 합니다.

규칙 133:20을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

RPC 프록시 트래픽 전용

RPC over HTTP Proxy Ports(RPC over HTTP 프록시 포트)를 활성화할 경우, 탐지된 클라이언트 측 RPC over HTTP가 프록시 트래픽 전용인지 또는 다른 웹 서버 트래픽을 포함하는지 여부를 나타냅니다. 예를 들어, 포트 80은 프록시와 다른 웹 서버 트래픽을 모두 전달할 수 있습니다.

이 옵션을 비활성화하면, 프록시 및 다른 웹 서버 트래픽 모두 예상됩니다. 예를 들어, 서버가 전용 프록시 서버인 경우, 이 옵션을 활성화합니다. 활성화되었을 때, 전처리기는 트래픽이 DCE/RPC를 전달하고 있는지 확인하기 위해 트래픽을 테스트하고, 전달하고 있는 경우 처리를 계속 진행하고 그렇지 않은 경우 트래픽을 무시합니다. **RPC over HTTP Proxy Ports(RPC over HTTP 프록시 포트)** 확인 상자 또한 활성화된 경우에만 이 옵션을 활성화하는 것이 기능을 추가한다는 점에 유의하십시오.

RPC over HTTP 프록시 포트

디바이스가 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 사이에 있는 경우 각 지정된 포트의 RPC over HTTP에서 터널링된 DCE/RPC 트래픽의 탐지를 활성화합니다. 15-7페이지의 HTTP 전송 기반의 RPC 이해를 참고하십시오.

활성화하면, 웹 서버에서 일반적으로 DCE/RPC와 기타 트래픽 모두에 기본 포트를 사용하기 때문에 트래픽이 필요한 가능성이 낮더라도, DCE/RPC 트래픽을 볼 수 있는 모든 포트를 추가할 수 있습니다. 활성화하면, **RPC over HTTP Proxy Auto-Detect Ports(RPC over HTTP 프록시 자동 탐지 포트)**를 활성화하지 않지만, 탐지된 클라이언트 측 HTTP 트래픽 기반의 RPC가 프록시 트래픽 전용일 경우에만 **RPC Proxy Traffic Only(RPC 프록시 트래픽 전용)**를 활성화하며, 다른 웹 서버 트래픽을 포함하지 않습니다.

RPC over HTTP 서버 포트

Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링할 때 각 지정된 포트에서 RPC over HTTP에 의해 터널링된 DCE/RPC 트래픽의 탐지를 활성화합니다. 15-7페이지의 HTTP 전송 기반의 RPC 이해를 참고하십시오.

일반적으로, 이 옵션을 활성화하는 경우 네트워크에서 어떤 프록시 웹 서버도 인식하지 않더라도 해당 옵션에 대해 1025에서 최대 65535 포트 범위를 가진 **RPC over HTTP Server Auto-Detect Ports(RPC over HTTP 서버 자동 탐지 포트)**도 활성화해야 합니다. HTTP 서버 포트 기반의 RPC가 경우에 따라 재구성되는데, 이 경우 사용자는 이 옵션의 포트 목록에 재설정된 서버 포트를 추가해야 합니다.

TCP 포트

각 지정된 포트의 TCP에서 DCE/RPC 트래픽의 탐지를 활성화합니다.

적정 DCE/RPC 트래픽 및 익스플로잇은 다양한 포트를 사용하고, 포트 1024 이상의 다른 포트는 일반적입니다. 일반적으로, 이 옵션을 활성화하면 해당 옵션에 대해 1025에서 최대 65535 포트 범위의 **TCP Auto-Detect Ports(TCP 자동 탐지 포트)**도 활성화해야 합니다.

UDP 포트

각 지정된 포트에서 UDP 내 DCE/RPC 트래픽의 탐지를 활성화합니다.

적정 DCE/RPC 트래픽 및 익스플로잇은 다양한 포트를 사용하고, 포트 1024 이상의 다른 포트는 일반적입니다. 일반적으로, 이 옵션을 활성화하면 또한 해당 옵션에 대해 1025에서 최대 65535 포트 범위의 **UDP Auto-Detect Ports(UDP 자동 탐지 포트)**도 활성화해야 합니다.

SMB 포트

각 지정된 포트에서 SMB 내 DCE/RPC 트래픽의 탐지를 활성화합니다.

기본 탐지 포트를 사용하면 SMB 트래픽이 발생할 수 있습니다. 다른 포트를 사용할 경우 발생 가능성은 매우 낮습니다. 일반적으로, 기본 설정을 사용합니다.

RPC over HTTP 프록시 자동 탐지 포트

디바이스가 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 사이에 있는 경우 지정된 포트에서 RPC over HTTP에서 터널링된 DCE/RPC 트래픽의 자동 탐지를 활성화합니다. 15-7 페이지의 HTTP 전송 기반의 RPC 이해를 참고하십시오.

활성화하면, 일반적으로 1025에서 65535까지 포트 범위를 지정하여 사용 후 삭제 포트의 전체 범위를 지원할 수 있습니다.

RPC over HTTP 서버 자동 탐지 포트

Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링할 때 지정된 포트에서 RPC over HTTP에 의해 터널링된 DCE/RPC 트래픽의 자동 탐지를 활성화합니다. 15-7페이지의 HTTP 전송 기반의 RPC 이해를 참고하십시오.

TCP 자동 탐지 포트

지정된 포트의 TCP에서 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

UDP 자동 탐지 포트

각 지정된 포트에서 UDP 내 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

SMB 자동 탐지 포트

SMB 내 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

SMB 파일 검사

파일 검색을 위한 SMB 트래픽의 검사를 활성화합니다. 다음 옵션을 이용할 수 있습니다.

- 파일 선택을 비활성화하려면 **Off(끄기)**를 선택합니다.
- SMB의 DCE/RPC 트래픽 검사 없이 파일 데이터를 검사하려면 **Only(전용)**를 선택합니다. 이 옵션을 선택하면 파일 및 DCE/RPC 트래픽 모두의 검사 성능을 높일 수 있습니다.
- SMB에서 파일 및 DCE/RPC 트래픽을 모두 검사하려면 **On(켜기)**을 선택합니다. 이 옵션을 선택하면 성능에 영향을 줄 수 있습니다.

다음에 대한 SMB 트래픽의 검사는 지원되지 않습니다.

- SMB 2.x 및 SMB 3.x에서 전송된 파일
- 이 옵션이 활성화되고 정책이 적용되기 전에 설정된 TCP 또는 SMB 세션에서 전송된 파일
- 단일 TCP 또는 SMB 세션에서 동시에 전송된 파일
- 여러 TCP 또는 SMB 세션을 통해 전송된 파일
- 메시지 서명이 협상될 때와 같이 비인접 데이터로 전송된 파일
- 데이터를 중첩하여 동일한 오프셋에 서로 다른 데이터로 전송된 파일
- 클라이언트가 파일 서버에 저장한 수정 사항에 대해 원격 클라이언트에 열린 파일

SMB 파일 검사 수준

SMB File Inspection(SMB 파일 검사)가 **Only(전용)** 또는 **On(켜기)**으로 설정된 경우, 파일이 SMB 트래픽에서 탐지될 때 바이트 수를 검사합니다. 다음 중 하나를 지정하십시오.

- 1부터 2147483647 사이의 정수(약 2GB)
- 전체 파일을 검사하려면 0
- 파일 검사를 비활성화하려면 -1

이 필드에 액세스 제어 정책에 정의된 것과 동일하거나 보다 작은 값을 입력합니다. 이 옵션에 **파일 유형 탐지 시 검사할 바이트 수 제한**에 정의된 것보다 큰 값을 설정한 경우, 시스템은 액세스 제어 정책 설정의 기능을 최대로 사용합니다. 자세한 내용은 10-16페이지의 파일 및 악성코드 탐지 성능 및 저장 조정을 참고하십시오.

SMB File Inspection(SMB 파일 검사)를 **Off(해제)**로 설정한 경우, 이 필드는 비활성화됩니다.

DCE/RPC 전처리기 구성

라이센스: 보호

DCE/RPC 전처리기 전역 옵션 및 하나 이상의 대상 기반 서버 정책을 구성할 수 있습니다.

전처리기는 사용자가 생성기 ID(GID) 133 규칙을 활성화하지 않는 한 이벤트를 생성하지 않습니다. 특정 탐지 옵션과 관련된 규칙은 15-3페이지의 전역 DCE/RPC 옵션 선택 및 15-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택을 참고하십시오(20-19페이지의 규칙 상태 설정도 참고).

또한, 대부분의 DCE/RPC 전처리기 규칙은 SMB, 연결 지향 DCE/RPC 또는 연결 없는 DCE/RPC 트래픽에서 탐지된 이상 징후 및 회피 기술에 대해 이벤트를 생성합니다. 다음 표는 각 유형의 트래픽을 위해 활성화할 수 있는 규칙을 식별합니다.

표 15-1 트래픽 관련 DCE/RPC 규칙

트래픽	전처리기 규칙 GID:SID
SMB	133:26을 통한 133:2, 133:57을 통한 133:48
연결 지향 DCE/RPC	133:39를 통한 133:27
연결 없는 DCE/RPC를 탐지	133:43을 통한 133:40

DCE/RPC 전처리기를 설정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **DCE/RPC Configuration(DCE/RPC 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

DCE/RPC Configuration(DCE/RPC 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 15-3페이지의 전역 DCE/RPC 옵션 선택에서 설명한 모든 옵션을 수정할 수 있습니다.

단계 10 다음 2가지 옵션을 사용할 수 있습니다.

- 새 대상 기반 정책을 추가합니다. 추가 아이콘( )을 클릭합니다. 이 아이콘은 페이지 왼쪽의 **Servers(서버)** 옆에 있습니다. Add Target(대상 추가) 팝업 창이 나타납니다. **서버 주소(Server Address)** 필드에 하나 이상의 IP 주소를 지정하고 **OK(확인)**를 클릭합니다.

  단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. ASA FirePOWER 모듈에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

  기본 정책을 비롯한 최대 255개 정책을 구성할 수 있습니다.

  트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

  새 항목은 페이지 왼쪽의 서버 목록에 나타나는데, 선택되었음을 나타내도록 강조 표시됩니다. 그리고 Configuration(구성) 섹션은 추가한 프로파일에 대한 현재 구성을 반영하도록 업데이트됩니다.

- 기존 대상 기반 정책의 설정을 수정합니다. 페이지 왼쪽의 **Servers(서버)**에 추가한 정책에 대해 구성된 주소를 클릭하거나 **default(기본값)**를 클릭합니다.

  선택한 부분이 강조 표시되고, Configuration(구성) 섹션이 선택한 정책에 대한 현재 구성을 표시하도록 업데이트됩니다. 기존 정책을 삭제하려면, 제거할 정책 옆에 있는 삭제 아이콘( )을 클릭합니다.

단계 11 다음 대상 기반 정책 옵션을 변경할 수 있습니다.

- DCE/RPC 대상 기반 서버 정책을 적용할 호스트를 지정하려면 **Networks(네트워크)** 필드에 단일 IP 주소 또는 주소 블록을 입력하거나 하나 또는 둘 다의 쉼표로 구분된 목록을 입력합니다.

  기본 정책을 비롯한 255개의 총 프로파일을 지정할 수 있습니다. 기본 정책에서 **Networks(네트워크)**에 대한 설정을 변경할 수 없다는 점에 유의하십시오. 기본 정책은 다른 정책에 인증되지 않은 네트워크의 모든 서버에 적용됩니다.

- 사용자 네트워크 세그먼트 상의 지정된 호스트에 적용할 정책 유형을 지정하려면 **Policy(정책)** 드롭다운 목록에서 Windows 또는 Samba 정책 유형 중 하나를 선택합니다.

  Auto-Detect Policy on SMB Session(SMB 세션에서 정책 자동 탐지) 전역 옵션을 활성화하여 SMB가 DCE/RPC 전송일 때 세션별로 이 옵션의 설정을 자동으로 대체할 수 있다는 점에 유의하십시오. 15-3페이지의 SMB 세션의 정책 자동 탐지를 참고하십시오.

- 지정된 공유 SMB 리소스에 연결하려는 시도가 있는 경우 전처리기가 이를 탐지하도록 설정하려면, **SMB Invalid Shares(SMB 유효하지 않은 공유)** 필드에서 공유 리소스를 식별하는 대소문자를 구분하지 않는 문자열의 단일 목록 또는 쉼표로 구분된 목록을 입력합니다. 또는, 개별 문자열을 인용구로 묶습니다. 이는 이전 소프트웨어 버전에서는 필요했지만 더 이상 필요하지 않습니다.

  예를 들어, C$, D$, admin 및 private으로 명명된 공유 리소스를 탐지하려면 다음을 입력할 수 있습니다.

  ```
  "C$", D$, "admin", private
  ```

  SMB 유효하지 않은 공유를 탐지하려면 또한 **SMB Ports(SMB 포트)** 또는 **SMB Auto-Detect Ports(SMB 자동 탐지 포트)**를 활성화해야 하고, **SMB Traffics(SMB 트래픽)** 옵션을 활성화해야 한다는 점에 유의하십시오.

  또한 대부분의 경우 Windows에서 명명되었고, 유효하지 않은 공유로 식별된 드라이브에 달러 표시를 추가해야 한다는 점에 유의하십시오. 예를 들어, `C$` 또는 `"C$"`를 입력하여 드라이브 C를 식별합니다.

- DCE/RPC 트래픽의 분석 없이 SMB의 DCE/RPC 트래픽에서 탐지된 파일을 검사하려면, **SMB File Inspection(SMB 파일 검사)** 드롭다운 목록에서 **Only(전용)**를 선택합니다. DCE/RPC 트래픽뿐만 아니라 SMB의 DCE/RPC 트래픽에서 탐지된 파일을 검사하려면, **SMB File Inspection(SMB 파일 검사)** 드롭다운 목록에서 **On(켜기)**을 선택합니다. **SMB File Inspection Depth(SMB 파일 검사 수준)** 필드의 탐지된 파일에서 검사할 바이트 수를 입력합니다. 전체에서 탐지된 파일을 검사하려면 `0`을 입력합니다.

- 허용할 연결된 SMB AndX 명령의 최대 수를 지정하려면, **SMB Maximum AndX Chains(SMB 최대 AndX 체인)** 필드에 0-255를 입력합니다. 연속된 명령을 허용하지 않으려면 `1`을 지정합니다. 이 기능을 비활성화하려면 `0`을 지정하거나 이 옵션을 비워 둡니다.

  참고 SMB 프로토콜의 전문가만이 **SMB Maximum AndX Chains(SMB 최대 AndX 체인)** 옵션의 기본 설정을 변경해야 합니다.

- Windows 정책을 전송하기 위해 DCE/RPC 트래픽을 전달하는 것으로 알려진 포트를 통한 DCE/RPC 트래픽 처리를 활성화하려면 전송 탐지 옆에 있는 확인 상자를 선택하거나 비워두며 선택적으로 전송을 위한 포트를 추가 또는 삭제합니다.

Windows 정책에 대해 **RPC over HTTP Proxy Ports(RPC over HTTP 프록시 포트)**, **RPC over HTTP Server Ports(RPC over HTTP 서버 포트)**, **TCP Ports(TCP 포트)** 및 **UDP Ports(UDP 포트)** 중 하나 또는 모든 형태의 조합을 선택합니다. **RPC over HTTP Proxy(RPC over HTTP 프록시)**가 활성화되고 클라이언트 측 RPC over HTTP 트래픽이 프록시 트래픽 전용임을 탐지한 경우, 즉, 다른 웹 서버 트래픽을 포함하지 않는 경우 **RPC Proxy Traffic Only(RPC 프록시 트래픽 전용)**를 선택합니다.

Samba 정책에 대해 **SMB Ports(SMB 포트)**를 선택합니다.

대부분의 경우, 기본 설정을 사용합니다. 자세한 내용은 15-5페이지의 DCE/RPC 전송의 이해, 15-7페이지의 HTTP 전송 기반의 RPC 이해 및 15-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택을 참고하십시오.

단일 포트, 대시(-)로 구분된 포트 번호의 범위 또는 포트 번호와 범위의 쉼표로 구분된 목록을 입력할 수 있습니다.

- 지정된 포트가 DCE/RPC 트래픽을 전달하는지 여부를 테스트하고 전달하는 경우 처리를 계속 진행하려면 자동 탐지 전송 옆에 있는 확인 상자를 선택하거나 비워두고 선택적으로 전송을 위한 포트를 추가하거나 삭제합니다.

  Windows 정책에 대해 **RPC over HTTP Server Auto-Detect Ports(RPC over HTTP 서버 자동 탐지 포트)**, **TCP Auto-Detect Ports(TCP 자동 탐지 포트)** 및 **UDP Auto-Detect Ports(UDP 자동 탐지 포트)** 중 하나 또는 모든 형태의 조합을 선택합니다.

  RPC over HTTP Proxy Auto-Detect Ports(RPC over HTTP 프록시 자동 탐지 포트) 또는 **SMB Auto-Detect Ports(SMB 자동 탐지 포트)**를 선택할 수도 있다는 점에 유의하십시오.

  일반적으로, 선택 후 삭제 포트의 전체 범위를 포함하도록 활성화하는 자동 탐지 포트에 1025에서 65535까지의 포트 범위를 지정합니다. 자세한 내용은 15-5페이지의 DCE/RPC 전송의 이해, 15-7페이지의 HTTP 전송 기반의 RPC 이해 및 15-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택을 참고하십시오.

자세한 내용은 15-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택을 참고하십시오.

단계 12 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

DNS 이름 서버 응답에서 익스플로잇 탐지

라이센스: 보호

DNS 전처리기는 다음 특정 익스플로잇에 대해 DNS 이름 서버 응답을 검사합니다.

- RData 텍스트 필드에서 오버플로 시도
- 사용하지 않는 DNS 리소스 레코드 유형
- 실험적 DNS 리소스 레코드 유형

자세한 내용은 다음 섹션을 참고하십시오.

- 15-15페이지의 DNS 전처리기 리소스 레코드 검사의 이해
- 15-16페이지의 RData 텍스트 필드의 오버플로 시도 탐지
- 15-16페이지의 사용하지 않는 DNS 리소스 레코드 유형 탐지
- 15-16페이지의 실험적 DNS 리소스 레코드 유형 탐지
- 15-17페이지의 DNS 전처리기 구성

DNS 전처리기 리소스 레코드 검사의 이해

라이센스: 보호

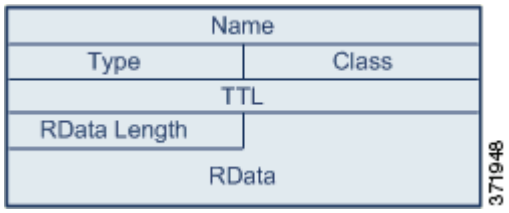
DNS 이름 서버 응답의 가장 일반적인 유형은 응답을 표시한 쿼리에서 도메인 이름에 해당하는 하나 이상의 IP 주소를 제공합니다. 예를 들면, 서버 응답의 다른 유형은 원래 쿼리된 서버에서 사용 가능한 정보를 제공하는 이름 서버의 전자 메일 메시지 또는 위치를 위한 대상을 제공합니다.

DNS 응답은 메시지 헤더, 하나 이상의 요청을 포함하는 Question(질문) 섹션 및 Question(질문) 섹션(Answer(응답), Authority(권한) 및 Additional Information(추가 정보))에서 요청에 응답하는 3가지 섹션으로 구성됩니다. 이 3가지 섹션에서 응답은 이름 서버에 유지되는 *리소스 레코드*(RR)의 정보를 반영합니다. 다음 표는 이러한 3가지 섹션에 대해 설명합니다.

표 15-2 DNS 이름 서버 RR 응답

섹션	포함 내용	예시
답변	선택 사항. 쿼리에 특정 응답을 제공하는 하나 이상의 리소스 레코드	도메인 이름에 해당하는 IP 주소
권한	선택 사항. 권위 있는 이름 서버를 가리키는 하나 이상의 리소스 레코드	응답에 대한 권위 있는 이름 서버의 이름
추가 정보	선택 사항. Answer(응답) 섹션에 관련된 추가 정보를 제공한 하나 이상의 리소스 레코드	쿼리할 다른 서버의 IP 주소

많은 유형의 리소스 레코드가 있으며, 이는 모두 다음 구조를 준수합니다.



이론적으로, 모든 종류의 리소스 레코드는 이름 서버 응답 메시지의 Answer(답변), Authority(권한), 또는 Additional Information(추가 정보) 섹션에 사용될 수 있습니다. DNS 전처리기는 탐지하는 익스플로잇을 위해 3개의 응답 섹션 각각의 리소스 레코드를 검사합니다.

Type(유형) 및 RData 리소스 레코드 필드는 DNS 전처리기에 특히 중요합니다. Type(유형) 필드는 리소스 레코드 유형을 식별합니다. RData(리소스 데이터) 필드는 응답 콘텐츠를 제공합니다. RData 필드의 크기 및 내용은 리소스 레코드 유형에 따라 다릅니다.

DNS 메시지는 일반적으로 UDP 전송 프로토콜을 사용하지만 메시지 유형이 신뢰할 수 있는 전송을 요청하거나 메시지 크기가 UDP 기능을 초과할 경우 TCP도 사용합니다. DNS 전처리기는 UDP 및 TCP 트래픽 모두에서 DNS 서버 응답을 검사합니다.

세션이 삭제된 패킷 때문에 상태를 상실할 경우 DNS 전처리기는 중간에 선택된 TCP 세션을 검사하지 않으며, 검사를 중지합니다.

DNS 전처리기에 대해 구성할 일반적인 포트는 잘 알려진 포트 53인데, 이는 DNS 이름 서버가 UDP 및 TCP 모두에서 DNS 메시지에 사용하는 것입니다.

RData 텍스트 필드의 오버플로 시도 탐지

라이센스: 보호

리소스 레코드 유형이 TXT(텍스트)일 때, RData 필드는 변수 길이의 ASCII 텍스트 필드입니다.

DNS 전처리기의 **RData 텍스트 필드의 오버플로 시도 탐지** 옵션이 선택된 경우 MITRE’ s Current Vulnerabilities and Exposures(MITRE의 현재 취약성 및 노출) 데이터베이스에서 식별된 특정 취약성을 탐지합니다. 이는 Microsoft Windows 2000 서비스 팩 4, Windows XP 서비스 팩 1 및 서비스 팩 2, 그리고 Windows Server 2003 서비스 팩 1에서 잘 알려진 취약점입니다. 공격자는 이러한 취약성을 악용하고 호스트를 전송하거나 호스트가 RData 텍스트 필드의 길이에서 계산착오를 일으키도록 하는 악의적으로 조작된 이름 서버 응답을 수신하도록 하여 버퍼 오버플로를 일으킴으로써 호스트를 완전히 제어할 수 있습니다.

네트워크가 이 취약성을 해결하기 위해 업그레이드된 적이 없는 운영 체제를 실행하는 호스트를 포함하는 경우 사용자는 이 기능을 활성화해야 합니다.

규칙 131:3을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

사용하지 않는 DNS 리소스 레코드 유형 탐지

라이센스: 보호

RFC 1035는 여러 리소스 레코드 유형을 사용하지 않는 것으로 식별합니다. 이는 사용하지 않는 레코드 유형이기 때문에, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다. 네트워크에 이들을 포함하도록 의도적으로 구성하지 않는 이상 일반 DNS 응답에서 이러한 레코드 유형이 발생하지 않습니다.

시스템을 구성하여 사용하지 않는 알려진 리소스 레코드 유형을 검색할 수 있습니다. 다음 표는 이러한 레코드 유형에 대해 나열하고 설명합니다.

표 15-3 사용하지 않는 DNS 리소스 레코드 유형

RR 유형	코드	설명
3	MD	메일 대상
4	MF	메일 발송자

규칙 131:1을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

실험적 DNS 리소스 레코드 유형 탐지

라이센스: 보호

RFC 1035는 여러 리소스 레코드 유형을 실험적인 것으로 식별합니다. 다음은 실험적 레코드 유형이기 때문에, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다. 네트워크에 이들을 포함하도록 의도적으로 구성하지 않는 이상 일반 DNS 응답에서 이러한 레코드 유형이 발생하지 않습니다.

시스템을 구성하여 알려진 실험적 리소스 레코드 유형을 검색할 수 있습니다. 다음 표는 이러한 레코드 유형에 대해 나열하고 설명합니다.

표 15-4 실험적 DNS 리소스 레코드 유형

RR 유형	코드	설명
7	MB	메일함 도메인 이름
8	MG	메일 그룹 멤버
9	MR	메일 이름 변경 도메인 이름
10	NUL	null 리소스 레코드

규칙 131:2를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

DNS 전처리기 구성

라이센스: 보호

DNS 전처리기를 설정하려면 다음 절차를 수행합니다. 이 페이지에서 옵션을 구성하는 데 대한 자세한 내용은 15-16페이지의 RData 텍스트 필드의 오버플로 시도 탐지,15-16페이지의 사용하지 않는 DNS 리소스 레코드 유형 탐지 및 15-16페이지의 실험적 DNS 리소스 레코드 유형 탐지를 참고하십시오.

DNS 전처리기를 설정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **DNS Configuration(DNS 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

DNS Configuration(DNS 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어을 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용를 참고하십시오.

단계 9 또는, Settings(설정) 영역에서 다음 중 하나를 수정할 수 있습니다.

- DNS 전처리기가 **Ports(포트)** 필드에서 DNS 서버 응답에 대해 모니터링해야 하는 소스 포트 또는 포트를 지정하십시오. 포트가 여러 개인 경우 쉼표로 구분하십시오.
- **Detect Overflow Attempts on RData(RData의 오버플로 시도 탐지) Text(텍스트) fields(필드)** 확인 상자를 선택하여 RData 텍스트 필드 내 버퍼 오버플로 시도에 대한 탐지를 활성화합니다.
- **Detect Obsolete DNS RR Types(사용하지 않는 DNS RR 유형 탐지)** 확인 상자를 선택하여 사용하지 않는 리소스 레코드 유형의 탐지를 활성화합니다.
- **Detect Experimental DNS RR Types(실험적 DNS RR 유형 탐지)** 확인 상자를 선택하여 실험적 리소스 레코드 유형을 탐지합니다.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

FTP 및 텔넷 트래픽 디코딩

라이센스: 보호

FTP/텔넷 디코더는 FTP 및 텔넷 데이터 스트림을 분석하고, 규칙 엔진으로 처리하기 전에 FTP 및 텔넷 명령을 표준화합니다.

125 및 126의 생성기 ID(GID)가 있는 FTP 및 텔넷 전처리기 규칙에서 이벤트를 생성하려는 경우 이 규칙을 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

자세한 내용은 다음 주제를 참고하십시오.

전역 FTP 및 텔넷 옵션의 이해

라이센스: 보호

전역 옵션을 설정하여 FTP/텔넷 디코더가 패킷의 상태 저장 또는 상태 비저장 검사를 수행할지 여부, 디코더가 암호화된 FTP 또는 텔넷 세션을 탐지할지 여부, 그리고 암호화된 데이터가 발생한 후 디코더가 데이터 스트림 확인을 계속할지 여부를 결정할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

상태 저장 검사

이를 선택하면, FTP/텔넷 디코더가 상태를 저장하고 개별 패킷을 위한 세션 컨텍스트를 제공하며, 리어셈블한 세션만 검사할 수 있습니다. 이를 취소하면, 세션 컨텍스트 없이 각 개별 패킷을 분석합니다.

FTP 데이터 전송을 확인하려면, 이 옵션을 선택해야 합니다.

암호화된 트래픽 탐지

암호화된 텔넷 및 FTP 세션을 탐지합니다.

규칙 125:7 및 126:2을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

암호화된 데이터 검사 계속 진행

데이터 스트림이 암호화된 후 전처리기가 계속해서 이를 확인하여 마지막으로 암호 해독된 데이터를 찾도록 합니다.

전역 FTP/텔넷 옵션의 구성

라이센스: 보호

상태 저장 또는 상태 비저장 검사가 수행되는지, 암호화된 트래픽이 탐지되는지 여부 및 암호화된 것으로 식별된 데이터 스트림에서 디코더가 계속해서 암호 해독된 데이터를 확인해야 하는지 여부를 제어하려면 FTP/텔넷 디코더에 대한 전역 옵션을 구성해야 합니다. 전역 설정에 대한 자세한 내용은 15-19페이지의 전역 FTP 및 텔넷 옵션의 이해를 참고하십시오.

전역 옵션을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

Advanced Settings(고급 설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **FTP and Telnet Configuration(FTP 및 텔넷 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

FTP and Telnet Configuration(FTP 및 텔넷 구성) 페이지가 나타납니다.

페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

팁 이 페이지에서 다른 옵션을 구성하는 데 대한 자세한 내용은 15-21페이지의 텔넷 옵션의 구성, 15-26페이지의 서버 수준 FTP 옵션 구성 및 15-29페이지의 클라이언트 수준 FTP 옵션 구성을 참고하십시오.

단계 9 또는, Global Settings(전역 설정) 페이지 영역에서 다음 중 하나를 수정할 수 있습니다.

- FTP 패킷을 포함하는 리어셈블된 TCP 스트림을 검토하려면 **Stateful Inspection(상태 저장 검사)**을 선택합니다. 리어셈블되지 않은 패킷만 검사하려면 **Stateful Inspection(상태 저장 검사)**를 비워둡니다.
- 암호화된 트래픽을 탐지하려면 **Detect Encrypted Traffic(암호화된 트래픽 탐지)**을 선택합니다. 암호화된 트래픽을 무시하려면 **Detect Encrypted Traffic(암호화된 트래픽 탐지)**을 비워둡니다.
- 필요한 경우 **Continue to Inspect Encrypted Data(계속해서 암호화된 데이터 검사)**를 선택하여 스트림이 다시 암호 해독되어 처리될 수 있는 경우 암호화된 후에도 스트림을 계속해서 검사합니다.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

텔넷 옵션의 이해

라이센스: 보호

FTP/텔넷 디코더에 의한 텔넷 명령의 표준화를 활성화 또는 비활성화할 수 있으며, 특정 이상 징후의 경우를 활성화 또는 비활성화할 수 있고 허용할 AYT(Are You There) 공격의 임계값 수를 설정할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

텔넷 트래픽을 표준화할 포트를 나타냅니다. 인터페이스에서, 쉼표로 구분하여 여러 개의 포트를 나열합니다.

표준화

지정된 포트로 향하는 텔넷 트래픽을 표준화합니다.

이상 징후 탐지

해당 SE(subnegotiation 종료) 없이 텔넷 SB(subnegotiation 시작)의 탐지를 활성화합니다.

텔넷은 SB(subnegotiation 시작)로 시작하고 SE(subnegotiation 종료)로 끝나는 subnegotiation를 지원합니다. 그러나, 텔넷 서버의 특정 구현은 해당 SE가 없는 SB를 무시합니다. 이는 우회하는 경우일 수 있는 이상 작업입니다. FTP가 제어 연결에서 텔넷 프로토콜을 사용하므로, 또한 이러한 작업에 취약합니다.

규칙 126:3을 활성화하여 텔넷 트래픽에서 이 이상 징후가 탐지될 때 이벤트를 생성할 수 있으며, 규칙 125:9를 활성화하여 FTP 명령 계통에서 이 이상 징후가 탐지될 때 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

AYT(Are You There) 공격 임계값 수

연속적인 AYT 명령의 수가 지정된 임계값을 초과하는 경우 이를 탐지합니다. Cisco는 임계값으로 20을 넘지 않는 값을 설정할 것을 권장합니다.

규칙 126:1을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

텔넷 옵션의 구성

라이센스: 보호

표준화를 활성화 또는 비활성화할 수 있으며, 특정 이상 징후의 경우를 활성화 및 비활성화할 수 있고 허용할 AYT(Are You There) 공격의 임계값 수를 제어할 수 있습니다. 텔넷 옵션에 대한 자세한 내용은 15-20페이지의 텔넷 옵션의 이해를 참고하십시오.

텔넷 옵션을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘()(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **FTP and Telnet Configuration(FTP 및 텔넷 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

FTP and Telnet Configuration(FTP 및 텔넷 구성) 페이지가 나타납니다.

페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

팁 이 페이지에서 다른 옵션을 구성하는 데 대한 자세한 내용은 15-19페이지의 전역 FTP/텔넷 옵션의 구성, 15-26페이지의 서버 수준 FTP 옵션 구성 및 15-29페이지의 클라이언트 수준 FTP 옵션 구성을 참고하십시오.

단계 9 또는, Telnet Settings(텔넷 설정) 페이지 영역에서 다음 중 하나를 수정할 수 있습니다.

- 텔넷 트래픽이 **Ports(포트)** 필드에서 디코딩되어야 하는 포트를 지정합니다. 텔넷은 일반적으로 TCP 포트 23에 연결됩니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

주의 암호화된 트래픽(SSL)은 디코딩될 수 없으므로, 포트 22(SSH)를 추가하면 예측되지 않은 결과를 얻을 수 있습니다.

- Telnet Protocol Options(텔넷 프로토콜 옵션) **Normalize(표준화)** 확인 상자를 선택하거나 비워두어 텔넷 표준화를 활성화하거나 비활성화합니다.
- Telnet Protocol Options(텔넷 프로토콜 옵션) **Detect Anomalies(이상 징후 탐지)** 확인 상자를 선택하거나 비워두어 이상 징후 탐지를 활성화하거나 비활성화합니다.
- 허용할 연속된 AYT 명령의 **Are You There Attack Threshold Number(AYT(Are You There) 공격 임계값 수)**를 지정합니다.

팁 Cisco는 임계값으로 기본값을 초과하지 않는 값을 설정할 것을 권장합니다.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

서버 수준 FTP 옵션의 이해

라이센스: 보호

여러 FTP 서버에서 디코딩을 위한 옵션을 설정할 수 있습니다. 생성한 각 서버 프로파일은 서버 IP 주소 및 트래픽이 모니터링되어야 할 서버의 포트를 포함합니다. 특정 서버에 대해 어느 FTP 명령을 인증할지, 그리고 어느 FTP 명령을 무시할지 지정하고 명령에 대한 최대 매개변수 길이를 설정할 수 있습니다. 또한 디코더가 특정 명령을 위해 인증해야 할 특정 명령어 구문을 설정하고, 대안이 되는 최대 명령 매개변수 길이를 지정할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

FTP 서버에서 하나 이상의 IP 주소를 지정하려면 이 옵션을 사용합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 하나 또는 둘 다로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다. 최대 1024개의 문자를 구성할 수 있고, 기본 프로파일을 포함하여 최대 255개 프로파일을 지정할 수 있습니다. ASA FirePOWER 모듈에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 주소 블록을 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역 의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

포트

디바이스가 트래픽을 모니터링해야 하는 FTP 서버에서 포트를 지정하려면 이 옵션을 사용합니다. 인터페이스에서, 쉼표로 구분하여 여러 개의 포트를 나열합니다.

File Get 명령

이 옵션을 사용하여 서버에서 클라이언트로 파일을 전송하는 데 사용되는 FTP 명령을 정의합니다. Support(지원팀)의 지시가 있는 경우가 아니면 이 값을 변경하지 마십시오.

File Put 명령

이 옵션을 사용하여 클라이언트에서 서버로 파일을 전송하는 데 사용되는 FTP 명령을 정의합니다. Support(지원팀)의 지시가 있는 경우가 아니면 이 값을 변경하지 마십시오.

추가 FTP 명령

이 문구를 사용하여 디코더가 탐지해야 하는 추가 명령을 지정합니다. 스페이스로 추가 명령을 구분합니다.

기본 최대 매개변수 길이

이 옵션을 사용하여 대체 매개변수 최대 길이가 설정되지 않은 명령에 대해 매개변수 최대 길이를 감지합니다.

규칙 125:3을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

대체 매개변수 최대 길이

이 옵션을 사용하여 다른 매개변수 최대 길이를 탐지할 명령을 지정하고, 해당 명령에 대한 최대 매개변수 길이를 지정합니다. **Add(추가)**를 클릭하여 특정 명령을 위해 탐지할 다른 매개변수 최대 길이를 지정할 수 있는 회선을 추가합니다.

문자열 형식 공격에 대한 명령 확인

이 옵션을 사용하여 문자열 형식 공격에 대해 지정된 명령을 확인합니다.

규칙 125:5을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

명령의 유효성

이 옵션을 사용하여 특정 명령의 유효한 형식을 입력합니다. FTP 커뮤니케이션의 일부로 수신된 매개변수의 문구를 인증하는 FTP 명령 매개변수 유효성 입증 명령문을 생성하는 데 대한 내용은 15-25페이지의 FTP 명령 매개변수 유효성 입증 명령문 생성을 참고하십시오. **Add(추가)**를 클릭하여 명령 유효성 검사 회선을 추가합니다.

규칙 125:2 및 125:4을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

FTP 전송 무시

이 옵션을 사용하여 데이터 전송 채널의 상태 확인 이외의 모든 검사를 비활성화하여 FTP 데이터 전송의 성능을 개선합니다.

FTP 명령 내 텔넷 이스케이프 코드 탐지

이 옵션을 사용하여 텔넷 명령이 FTP 명령 계통에서 사용되는 경우를 탐지합니다.

규칙 125:1을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

표준화 진행 중 삭제 명령 무시

Detect Telnet Escape Codes within FTP Commands(FTP 명령 내 텔넷 이스케이프 코드 탐지)를 선택한 경우 이 옵션을 사용하여 FTP 트래픽을 표준화할 때 텔넷 특성과 회선 삭제 명령을 무시합니다. 설정은 FTP 서버 처리가 텔넷 삭제 명령을 처리하는 방식에 일치해야 합니다. 이전 서버는 일반적으로 이를 처리하지만 새로운 FTP 서버는 일반적으로 텔넷 삭제 명령을 무시한다는 점에 유의하십시오.

문제 해결 옵션: FTP 명령 유효성 검사 구성 로그

Support(지원팀)은 문제 해결 통화 중에 사용자에게 시스템을 구성하여 서버에 나열된 각 FTP 명령에 대한 구성 정보를 인쇄하도록 요청할 수 있습니다.

주의 이 문제 해결 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

FTP 명령 매개변수 유효성 입증 명령문 생성

라이센스: 보호

FTP 명령을 위한 유효성 입증 명령문을 설정할 때, 스페이스로 매개변수를 분리하여 대체 매개변수 그룹을 지정할 수 있습니다. 또한 유효성 입증 명령문에서 파이프 문자(|)로 이들을 분리하여 두 매개변수 간 이진 또는 관계를 생성할 수 있습니다. 매개변수를 대괄호([])로 묶는 것은 해당 매개변수가 선택 사항임을 나타냅니다. 매개변수를 중괄호{}로 묶는 것은 해당 매개변수가 요청된 것임을 나타냅니다.

FTP 커뮤니케이션의 일부로 수신된 매개변수의 문구를 인증하는 FTP 명령 매개변수 유효성 입증 명령문을 생성할 수 있습니다. 자세한 내용은 15-23페이지의 서버 수준 FTP 옵션의 이해를 참고하십시오.

다음 표에 나열된 모든 매개변수는 FTP 명령 매개변수 유효성 입증 명령문에 사용할 수 있습니다.

표 15-5 FTP 명령 매개변수

사용 대상	발생하는 유효성 검사
int	표시된 매개변수는 정수여야 합니다.
number	표시된 매개변수는 1과 255 사이의 정수여야 합니다.
char _chars	표시된 매개변수는 _chars 인수에 지정된 특성 중 하나인 단일 특성이거나 그 구성원이어야 합니다. 예를 들어, MODE의 명령 유효성을 유효성 입증 명령문 char로 정의하면 SBC는 MODE 명령을 위한 매개변수가 (Stream(스트림) 모드를 표시하는) S자와 (Block(차단 모드를 표시하는) B자, (Compressed(압축된) 모드를 표시하는) C자로 이루어짐을 확인합니다.
date _datefmt	_datefmt가 #를 포함하는 경우, 표시된 매개변수는 숫자여야 합니다. _datefmt가 C를 포함하는 경우, 표시된 매개변수는 문자여야 합니다. _datefmt가 리터럴 문자열을 포함하는 경우, 표시된 매개변수는 리터럴 문자열에 일치해야 합니다.
string	표시된 매개변수는 문자열이어야 합니다.
host_port	표시된 매개변수는 RFC 959에 의해 정의된 대로 유효한 호스트 포트 지정자여야 하며, File Transfer Protocol 사양은 네트워크 작업 그룹에 의해 정의된 대로 유효한 호스트 포트 지정자여야 합니다.

필요한 경우 위 표의 문구를 조합하여 트래픽의 유효성을 입증해야 할 필요가 있는 각 FTP 명령을 정확하게 입증하는 매개변수 유효성 입증 명령문을 생성할 수 있습니다.

참고 TYPE 명령에서 복잡한 표현을 포함할 때, 스페이스로 이를 묶습니다. 또한, 표현 안의 각 피연산자를 스페이스로 묶습니다. 예를 들어, char A | B 를 입력합니다. char A|B는 올바르지 않습니다.

서버 수준 FTP 옵션 구성

라이센스: 보호

서버 수준에서 여러 옵션을 구성할 수 있습니다. 추가하는 각 FTP 서버에 대해 모니터링할 포트, 유효성을 입증할 명령, 명령을 위한 기본 매개변수 최대 길이, 특정 명령에 대한 대체 매개변수 길이, 특정 명령에 대한 유효성 입증 문구를 지정할 수 있습니다. 또한 FTP 채널에서 문자열 형식 공격 및 텔넷 명령을 확인할지 그리고 각 명령을 사용하여 구성 정보를 인쇄하도록 할지 선택할 수 있습니다. 서버 수준 FTP 옵션에 대한 자세한 내용은 15-23페이지의 서버 수준 FTP 옵션의 이해를 참고하십시오.

서버 수준 FTP 옵션을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **FTP and Telnet Configuration(FTP 및 텔넷 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

FTP and Telnet Configuration(FTP 및 텔넷 구성) 페이지가 나타납니다.

페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

팁 이 페이지에서 다른 옵션을 구성하는 데 대한 자세한 내용은 15-19페이지의 전역 FTP/텔넷 옵션의 구성, 15-21페이지의 텔넷 옵션의 구성 및 15-29페이지의 클라이언트 수준 FTP 옵션 구성을 참고하십시오.

단계 9 다음 2가지 옵션을 사용할 수 있습니다.

- 새로운 서버 프로파일을 추가합니다. 추가 아이콘( )을 클릭합니다. 이 아이콘은 페이지 왼쪽의 **FTP Server(FTP 서버)** 옆에 있습니다. Add Target(대상 추가) 팝업 창이 나타납니다. **Server Address(서버 주소)** 필드에 하나 이상의 IP 주소를 지정하고 **OK(확인)**를 클릭합니다.

  단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 최대 1024개의 문자를 구성할 수 있고, 기본 정책을 포함하여 최대 255개의 정책을 구성할 수 있습니다. ASA FirePOWER 모듈에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

  트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

  새 항목은 페이지 왼쪽의 FTP 서버 목록에 나타나는데, 선택되었음을 나타내도록 강조 표시됩니다. 그리고 Configuration(구성) 섹션은 추가한 프로파일에 대한 현재 구성을 반영하도록 업데이트됩니다.

- 기존 서버 프로파일의 설정을 수정합니다. 페이지 왼쪽의 **FTP Server(FTP 서버)**에 추가한 프로파일에 대해 구성된 주소를 클릭하거나 **default(기본값)**를 클릭합니다.

  선택한 부분이 강조 표시되고, Configuration(구성) 섹션이 선택한 프로파일에 대한 현재 구성을 표시하도록 업데이트됩니다. 기존 프로파일을 삭제하려면, 제거할 프로파일 옆에 있는 삭제 아이콘( )을 클릭합니다.

단계 10 또는, Configuration(구성) 페이지 영역에서 다음 중 하나를 수정할 수 있습니다.

- **Networks(네트워크)** 필드에 나열된 주소를 수정하고 페이지의 다른 영역을 클릭합니다.

  페이지 왼쪽에 강조 표시된 주소가 업데이트됩니다.

  기본 프로파일에서 **Networks(네트워크)** 설정을 변경할 수 없다는 점에 유의하십시오. 기본 프로파일은 다른 프로파일에서 인증되지 않은 네트워크의 모든 서버에 적용됩니다.

- FTP 트래픽에 대해 모니터링되어야 하는 모든 **Ports(포트)**를 지정합니다. 포트 21은 FTP 트래픽의 잘 알려진 포트입니다.

- **File Get Commands(File Get 명령)** 필드에서 서버로부터 클라이언트로 파일을 전송하는 데 사용하는 FTP 명령을 업데이트합니다.

- **File Put Commands(File Put 명령)** 필드에서 클라이언트로부터 서버로 파일을 전송하는 데 사용하는 FTP 명령을 업데이트합니다.

참고 Support(지원팀)의 지시가 있는 경우가 아니면 **File Get Commands(File Get 명령)** 및 **File Put Commands(File Put 명령)** 필드의 값을 변경하지 마십시오.

- FTP/텔넷 전처리기에 의해 기본적으로 확인되는 FTP 명령 외의 추가 FTP 명령을 탐지하려면 **Additional FTP Commands(추가 FTP 명령)** 필드에 스페이스로 구분된 명령어를 입력합니다.

  추가 FTP 명령을 필요한 만큼 많이 추가할 수 있습니다.

참고 사용자가 추가할 수 있는 추가 명령에는 `XPWD`, `XCWD`, `XCUP`, `XMKD`, 그리고 `XRMD`가 포함되어 있습니다. 이 명령에 대한 자세한 내용은 네트워크 작업 그룹에 의한 디렉토리 지향 FTP 명령 사양인 RFC 775를 참고하십시오.

- **Default Max Parameter Length(기본 최대 매개변수 길이)** 필드에 명령 매개변수의 기본 최대 바이트 수를 지정합니다.

- 특정 명령에 대해 다른 최대 매개변수 길이를 검색하려면 **Add(추가)(Alternate Max Parameter Length(대체 매개변수 최대 길이)** 옆에 있음)를 클릭합니다. 나타나는 열의 첫 번째 텍스트 상자에서 최대 매개변수 길이를 지정합니다. 두 번째 텍스트 상자에서, 스페이스로 구분하여 명령을 지정합니다. 여기에서 대체 매개변수 최대 길이를 적용해야 합니다.

  대체 매개변수 최대 길이를 필요한 만큼 추가할 수 있습니다.
- 특정 명령에서 문자열 형식 공격을 확인하려면, **Check Commands for String Format Attacks(문자열 형식 공격에 대한 명령 확인)** 텍스트 상자에서 스페이스로 구분하여 명령을 지정합니다.
- 명령을 위해 유효한 형식을 지정하려면 **Add(추가)(Command Validity(명령 유효성)** 옆에 있음)를 클릭합니다. 사용자가 검증할 명령을 지정한 다음, 명령 매개변수를 위한 유효성 입증 명령문을 입력합니다. 유효성 입증 명령문의 구문에 대한 자세한 내용은 15-23페이지의 서버 수준 FTP 옵션의 이해를 참고하십시오.
- 데이터 전송 채널의 상태 확인 이외의 모든 조사를 비활성화하여 FTP 데이터 전송 성능을 개선하려면, **Ignore FTP Transfers(FTP 전송 무시)**를 활성화합니다.

참고 데이터 전송을 검사하려면, 전역 FTP/텔넷 **Stateful Inspection(상태 저장 검사)** 옵션을 선택해야 합니다. 전역 옵션 설정에 대한 자세한 내용은 15-19페이지의 전역 FTP 및 텔넷 옵션의 이해를 참고하십시오.

- 텔넷 명령이 FTP 명령 계통에서 사용되는 경우 이를 탐지하려면 **Detect Telnet Escape Codes within FTP Commands(FTP 명령 내 텔넷 이스케이프 코드 탐지)**를 선택합니다.
- FTP 트래픽을 표준화할 때 텔넷 특성과 회선 삭제 명령을 무시하려면 **Ignore Erase Commands during Normalization(표준화 진행 중 삭제 명령 무시)**을 활성화합니다.

단계 11 선택적으로, Support(지원팀)의 지시가 있는 경우에만 **+** 기호를 클릭하여 관련된 문제 해결 옵션을 수정하십시오. **Troubleshooting Options(문제 해결 옵션)** 옆에 있는 이 기호를 클릭하면 문제 해결 옵션 섹션이 확장됩니다.

단계 12 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

클라이언트 수준 FTP 옵션의 이해

라이센스: 보호

FTP 클라이언트의 프로파일을 생성할 수 있습니다. 각 프로파일에서, 클라이언트로부터 온 FTP 응답에 대해 최대 응답 길이를 지정할 수 있습니다. 또한 특정 클라이언트에 대한 FTP 명령 계통에서 디코더가 바운스 공격 및 텔넷 명령의 사용을 탐지하는지 여부를 설정할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

FTP 클라이언트의 하나 이상의 IP 주소를 지정하려면 이 옵션을 사용합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 하나 또는 둘 다로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다. 최대 1024개의 문자를 지정할 수 있고, 기본 프로파일을 포함하여 최대 255개 프로파일을 지정할 수 있습니다. ASA FirePOWER 모듈에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

기본 정책의 default 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 주소 블록을 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 any(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역 의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

최대 응답 길이

FTP 클라이언트로부터 온 응답 문자열의 최대 길이를 지정하려면 이 옵션을 사용합니다.

규칙 125:6을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

FTP 바운스 공격 탐지

FTP 바운스 공격을 탐지하려면 이 옵션을 사용합니다.

규칙 125:8을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

FTP 바운스 허용

FTP PORT 명령이 FTP 바운스 공격으로 처리되어서는 안되는 호스트에서 추가 호스트 및 포트 목록을 구성하려면 이 옵션을 사용합니다.

FTP 명령 내 텔넷 이스케이프 코드 탐지

이 옵션을 사용하여 텔넷 명령이 FTP 명령 계통에서 사용되는 경우를 탐지합니다.

규칙 125:1을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

표준화 진행 중 삭제 명령 무시

Detect Telnet Escape Codes within FTP Commands(FTP 명령 내 텔넷 이스케이프 코드 탐지)를 선택한 경우 이 옵션을 사용하여 FTP 트래픽을 표준화할 때 텔넷 특성과 회선 삭제 명령을 무시합니다. 이 설정은 FTP 클라이언트가 텔넷 삭제 명령을 처리하는 방식에 일치해야 합니다. 이전 클라이언트는 일반적으로 이를 처리하지만 새로운 FTP 클라이언트는 일반적으로 텔넷 삭제 명령을 무시한다는 점에 유의하십시오.

클라이언트 수준 FTP 옵션 구성

라이센스: 보호

FTP 클라이언트에 대한 클라이언트 프로파일을 구성하여 클라이언트에서 FTP 트래픽을 모니터링할 수 있습니다. 사용자가 클라이언트 모니터링을 위해 설정할 수 있는 옵션에 대한 내용은 15-28 페이지의 클라이언트 수준 FTP 옵션의 이해를 참고하십시오. 텔넷 옵션에 대한 자세한 내용은 15-20페이지의 텔넷 옵션의 이해를 참고하십시오. FTP 추가 옵션에 대한 추가 정보에 대한 자세한 내용은 15-23페이지의 서버 수준 FTP 옵션의 이해 및 15-19페이지의 전역 FTP 및 텔넷 옵션의 이해를 참고하십시오.

클라이언트 수준 FTP 옵션을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **FTP and Telnet Configuration(FTP 및 텔넷 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

FTP and Telnet Configuration(FTP 및 텔넷 구성) 페이지가 나타납니다.

단계 9 다음 2가지 옵션을 사용할 수 있습니다.

- 새 클라이언트 프로파일을 추가합니다. 추가 아이콘( )을 클릭합니다. 이 아이콘은 페이지 왼쪽의 **FTP Client(FTP 클라이언트)** 옆에 있습니다. Add Target(대상 추가) 팝업 창이 나타납니다. **Client Address(클라이언트 주소)** 필드에 하나 이상의 클라이언트 IP 주소를 지정하고 **OK(확인)**를 클릭합니다.

  단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 최대 1024개의 문자를 구성할 수 있고, 기본 정책을 포함하여 최대 255개의 정책을 구성할 수 있습니다. ASA FirePOWER 모듈에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

  트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

  새 항목은 페이지 왼쪽의 FTP 클라이언트 목록에 나타나는데, 선택되었음을 나타내도록 강조 표시됩니다. 그리고 Configuration(구성) 섹션은 추가한 프로파일에 대한 현재 구성을 반영하도록 업데이트됩니다.

- 기존 클라이언트 프로파일의 설정을 수정합니다. 페이지 왼쪽의 **FTP Client(FTP 클라이언트)**에 추가한 프로파일에 대해 구성된 주소를 클릭하거나 **default(기본값)**를 클릭합니다.

  선택한 부분이 강조 표시되고, Configuration(구성) 섹션이 선택한 프로파일에 대한 현재 구성을 표시하도록 업데이트됩니다. 기존 프로파일을 삭제하려면, 제거할 프로파일 옆에 있는 삭제 아이콘( )을 클릭합니다.

단계 10 또는, Configuration(구성) 페이지 영역에서 다음 중 하나를 수정할 수 있습니다.

- 또는, **Networks(네트워크)** 필드에 나열된 주소를 수정하고 페이지의 다른 영역을 클릭합니다.

  페이지 왼쪽에 강조 표시된 주소가 업데이트됩니다.

  기본 프로파일에서 **Networks(네트워크)** 설정을 변경할 수 없다는 점에 유의하십시오. 기본 프로파일은 다른 프로파일에서 식별되지 않은 네트워크의 모든 클라이언트 호스트에 적용됩니다.

- **Max Response Length(최대 응답 길이)** 필드에서 FTP 클라이언트의 최대 응답 길이를 바이트 단위로 지정합니다.

- FTP 바운스 공격을 탐지하려면 **Detect FTP Bounce attempts(FTP 바운스 공격 탐지)**를 선택합니다.

  FTP/텔넷 디코더는 FTP PORT 명령이 발행되고 지정된 호스트가 클라이언트의 지정된 호스트에 일치하지 경우 이를 탐지합니다.

- FTP PORT 명령이 FTP 바운스 공격으로 처리되어서는 안되는 추가 호스트 및 포트 목록을 구성하려면, 콜론(:) 앞에 오는 각 호스트(또는 CIDR 형식의 네트워크)를 지정하거나 **Allow FTP Bounce to(FTP 바운스 허용)** 필드의 포트 또는 포트 범위를 지정합니다. 호스트에 대한 포트 범위를 입력하려면, 범위 내 최초 포트 및 범위 내 최종 포트를 대시(-)로 구분합니다. 호스트에 대한 항목을 쉼표로 구분하여 여러 호스트를 입력할 수 있습니다.

  예를 들어, 포트 21에서 호스트 192.168.1.1로 전송된 FTP PORT 명령과 22에서 1024까지의 모든 포트에서 호스트 192.168.1.2로 전송된 명령을 허용하려면 다음을 입력합니다.

  ```
  192.168.1.1:21, 192.168.1.2:22-1024
  ```

  ASA FirePOWER 모듈에서 CIDR 표기법 및 접두사 길이를 사용하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

참고 호스트에 대한 여러 개별 포트를 지정하려면, 각 포트 정의에 대한 호스트 IP 주소를 반복해야 합니다. 예를 들어, 192.168.1.1에서 포트 22 및 25를 지정하려면 `192.168.1.1:22, 192.168.1.1:25`를 입력합니다.

- 텔넷 명령이 FTP 명령 계통에서 사용되는 경우 이를 탐지하려면 **Detect Telnet Escape Codes within FTP Commands(FTP 명령 내 텔넷 이스케이프 코드 탐지)**를 선택합니다.
- FTP 트래픽을 표준화할 때 텔넷 특성과 회선 삭제 명령을 무시하려면 **Ignore Erase Commands during Normalization(표준화 진행 중 삭제 명령 무시)**을 선택합니다.

단계 11 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

HTTP 트래픽 디코딩

라이센스: 보호

HTTP Inspect(HTTP 검사) 전처리기는 다음 작업을 담당합니다.

- 사용자 네트워크 웹 서버로 전송된 HTTP 요청 및 사용자 네트워크 웹 서버에서 수신된 HTTP 응답 디코딩 및 표준화
- HTTP 관련 침입 규칙의 성능을 개선하기 위해 웹 서버로 전송된 메시지를 URI, 비 쿠키 헤더, 쿠키 헤더, 메서드 및 메시지 본문 구성 요소로 분리
- HTTP 관련 침입 규칙의 성능을 개선하기 위해 웹 서버에서 수신된 메시지를 상태 코드, 상태 메시지, 비 집합 쿠키 헤더, 쿠키 헤더 및 응답 본문 구성 요소로 분리
- 가능한 URI 인코딩 공격 탐지
- 추가 규칙을 처리하는 데 표준화된 데이터를 사용 가능하도록 하기

HTTP 트래픽은 여러 형식으로 인코딩될 수 있기 때문에 규칙의 적절한 검사를 어렵게 합니다. HTTP Inspect(HTTP 검사)는 14가지 유형의 인코딩을 디코딩하여 사용자의 HTTP 트래픽이 가능한 최상의 검사를 받을 수 있도록 합니다.

HTTP Inspect(HTTP 검사) 옵션을 전역으로, 단일 서버에서 또는 서버 목록에 대해 구성할 수 있습니다.

HTTP Inspect(HTTP 검사) 전처리기를 사용할 때 다음 사항에 유의하십시오

- 전처리기 엔진은 HTTP 표준화를 *상태 비저장으로* 수행합니다. 즉, 전처리기 엔진은 HTTP 문자열을 패킷별 기반으로 표준화하고, TCP 스트림 전처리기에 의해 리어셈블된 HTTP 문자열만 처리할 수 있습니다.
- 119의 생성기 ID(GID)가 있는 HTTP 전처리기 규칙에서 이벤트를 생성하려는 경우 이 규칙을 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 15-32페이지의 전역 HTTP 표준화 옵션 선택
- 15-33페이지의 전역 HTTP 구성 옵션 구성
- 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택
- 15-42페이지의 서버 수준 HTTP 표준화 인코딩 옵션 선택
- 15-45페이지의 HTTP 서버 옵션 구성
- 15-47페이지의 추가 HTTP 검사 전처리기 규칙 활성화

전역 HTTP 표준화 옵션 선택

라이센스: 보호

HTTP Inspect(HTTP 검사) 전처리기에 제공되는 전역 HTTP 옵션은 전처리기가 작동하는 방식을 제어합니다. 이 옵션을 사용하여 웹 서버 포트로 지정되지 않은 포트가 HTTP 트래픽을 수신할 때 HTTP 표준화를 활성화하거나 비활성화합니다.

다음 사항을 참고하십시오.

- **Unlimited Decompression(무제한 압축 해제)**을 활성화하는 경우, 변경 사항을 커밋하면 **Maximum Compressed Data Depth(압축 데이터 최대 수준)** 및 **Maximum Decompressed Data Depth(압축 해제된 데이터 최대 수준)** 옵션이 자동으로 65535로 설정됩니다. 자세한 내용은 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택을 참고하십시오.

- **Maximum Compressed Data Depth(압축 데이터 최대 수준)** 및 **Maximum Decompressed Data Depth(압축 해제된 데이터 최대 수준)** 옵션이 액세스 제어 규칙과 관련된 침입 정책 및 액세스 제어 정책의 기본 작업과 관련된 침입 정책에서 다른 경우, 가장 높은 값이 사용됩니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

이상 HTTP 서버 탐지

웹 서버 포트로 지정되지 않은 포트로 전송되거나 해당 포트에서 수신되는 HTTP 트래픽을 탐지합니다.

참고 이 옵션을 설정하는 경우, HTTP 구성 페이지의 서버 프로파일에서 HTTP 트래픽을 수신하는 모든 포트를 나열합니다. 이 옵션을 설정하지 않는 경우, 그리고 이 옵션 및 관련 전처리기 규칙을 활성화하는 경우, 서버를 오가는 일반 트래픽이 이벤트를 생성합니다. 기본 서버 프로파일은 보통 HTTP 트래픽에 사용되는 모든 포트를 포함하지만, 해당 프로파일을 수정한 경우, 이벤트가 생성되는 것을 방지하기 위해 다른 프로파일에 포트를 추가해야 할 수 있습니다.

규칙 120:1을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

HTTP 프록시 서버 탐지

Allow HTTP Proxy Use(HTTP 프록시 사용 허용) 옵션으로 정의되지 않은 프록시 서버를 사용하여 HTTP 트래픽을 탐지합니다.

규칙 119:17을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

압축 데이터 최대 수준

Inspect Compressed Data(압축 데이터 검사)(및, 선택적으로, **Decompress SWF File(SWF 파일 압축 해제, LZMA)**, **Decompress SWF File(SWF 파일 압축 해제, Deflate)** 또는 **Decompress PDF File(PDF 파일 압축 해제, Deflate)**)가 활성화되어 있는 경우 압축 해제할 압축 데이터의 최대 크기를 설정합니다. 1부터 65535 바이트까지 지정할 수 있습니다.

압축 해제된 데이터 최대 수준

Inspect Compressed Data(압축 데이터 검사)(및, 선택적으로, **Decompress SWF File(SWF 파일 압축 해제, LZMA)**, **Decompress SWF File(SWF 파일 압축 해제, Deflate)** 또는 **Decompress PDF File(PDF 파일 압축 해제, Deflate)**)가 활성화되어 있는 경우 압축 해제된 표준화 데이터의 최대 크기를 설정합니다. 1부터 65535 바이트까지 지정할 수 있습니다.

전역 HTTP 구성 옵션 구성

라이센스: 보호

비표준 포트로 향하는 HTTP 트래픽과 프록시 서버를 사용하는 HTTP 트래픽에 대한 탐지를 구성할 수 있습니다. 전역 HTTP 구성 옵션에 대한 자세한 내용은 15-32페이지의 전역 HTTP 표준화 옵션 선택을 참고하십시오.

전역 HTTP 구성 옵션을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **HTTP Configuration(HTTP 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

HTTP Configuration(HTTP 구성) 페이지가 나타납니다.

단계 9 15-32페이지의 전역 HTTP 표준화 옵션 선택에 설명된 전역 옵션을 수정할 수 있습니다.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

서버 수준 HTTP 표준화 옵션 선택

라이센스: 보호

모니터링하는 각 서버에 대한 서버 수준 옵션을 모든 서버 또는 서버 목록에 대해 전역으로 설정할 수 있습니다. 또한, 미리 정의된 서버 프로파일을 사용하여 이 옵션을 설정하거나, 사용자 환경의 요구를 충족하도록 이들을 개별적으로 설정할 수 있습니다. 이 옵션 또는 이 옵션을 설정하는 기본 프로파일 중 하나를 사용하여 트래픽을 표준화할 HTTP 서버 포트와 표준화할 서버 응답 페이로드의 양, 그리고 표준화할 인코딩 유형을 지정합니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

하나 이상 서버의 IP 주소를 지정하려면 이 옵션을 사용합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 하나 또는 둘 다로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다.

최대 255개의 총 프로파일의 제한 외에도, 기본 프로파일을 포함하여 최대 496개의 문자 또는 약 26개의 항목을 하나의 HTTP 서버 목록에 포함할 수 있으며 모든 서버 프로파일에 대해 총 256개의 주소 항목을 지정할 수 있습니다. ASA FirePOWER 모듈에서 IPv4 CIDR 표기법 및 IPv6 접두사 길이를 사용하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역 의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

포트

HTTP 트래픽을 전처리기 엔진이 표준화하는 포트. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

오버사이즈 디렉토리 길이

지정한 값보다 긴 URL 디렉토리를 탐지합니다.

규칙 119:15를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

클라이언트 흐름 수준

Ports(포트)에 정의된 클라이언트 측 HTTP 트래픽의 헤더 및 페이로드 데이터를 포함하여 원시 HTTP 패킷에서 규칙이 검사하는 바이트 수를 지정합니다. 규칙 내 HTTP 콘텐츠 규칙 옵션이 요청 메시지의 특정 부분을 검사할 때 클라이언트 흐름 수준은 적용되지 않습니다. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오.

-1에서 1460까지의 값을 지정할 수 있습니다. Cisco는 클라이언트 흐름 수준를 해당 최대값으로 설정할 것을 권장합니다. 다음 중 하나를 지정합니다.

- 1 - 1460은 첫 번째 패킷에서 지정한 바이트 수를 검사합니다. 첫 번째 패킷이 지정된 것보다 작은 바이트를 포함하는 경우, 전체 패킷을 검사합니다. 지정된 값이 세그먼트 및 리어셈블된 패킷 모두에 적용된다는 점에 유의하십시오.

  또한 300 값은 여러 클라이언트 요청 헤더의 끝에 나타나는 큰 HTTP 쿠키의 검사를 일반적으로 수행하지 않는다는 점에 유의하십시오.
- 0은 클라이언트 측의 모든 트래픽을 검사하는데, 세션의 여러 패킷을 포함하며, 필요한 경우 1460바이트 제한을 초과합니다. 이 값이 성능에 영향을 줄 수 있다는 점에 유의하십시오.
- -1은 클라이언트 측 트래픽을 모두 무시합니다.

서버 흐름 수준

Ports(포트)에 지정된 서버 측 HTTP 트래픽의 원시 HTTP 패킷에서 규칙이 검사하는 바이트 수를 지정합니다. **Inspect HTTP Response(HTTP 응답 검사)**가 비활성화되어 있는 경우 원시 헤더와 페이로드가 검사에 포함되고 **Inspect HTTP Response(HTTP 응답 검사)**가 활성화되어 있는 경우에는 원시 응답 본문만 검사에 포함됩니다.

서버 흐름 수준은 **Ports(포트)**에 정의된 서버 측 HTTP 트래픽에서 규칙이 검사하는 세션의 원시 서버 응답 데이터의 바이트 수를 지정합니다. 이 옵션을 사용하여 HTTP 서버 응답 데이터의 조사 수준 및 성능의 균형을 맞출 수 있습니다. 규칙 내 HTTP 콘텐츠 규칙 옵션이 응답 메시지의 특정 부분을 검사할 때 서버 흐름 수준은 적용되지 않습니다. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오.

클라이언트 흐름 수준과 달리, 서버 흐름 수준은 검사하는 규칙에 대해 HTTP 요청 패킷이 아닌 HTTP 응답별로 바이트 수를 지정합니다.

-1에서 65535까지 값을 지정할 수 있습니다. Cisco는 서버 흐름 수준을 해당 최대값으로 설정할 것을 권장합니다. 다음 값 중 하나를 지정할 수 있습니다.

- 1 ~ 65535:

  Inspect HTTP Response(HTTP 응답 검사)가 **활성화**된 경우 원시 HTTP 헤더가 아닌 원시 HTTP 응답 본문만을 검사합니다. 또한 **Inspect Compressed Data(압축 데이터 검사)**가 활성화된 경우 압축 해제된 데이터를 검사합니다.

  Inspect HTTP Response(HTTP 응답 검사)가 **비활성화**된 경우 원시 패킷 헤더 및 페이로드를 검사합니다.

  세션이 지정된 것보다 작은 응답 바이트를 포함하는 경우, 규칙은 주어진 세션의 모든 응답 패킷을 완전히 검사하며, 필요에 따라 여러 패킷에 걸쳐 검사합니다. 세션이 지정된 것보다 많은 응답 바이트를 포함하는 경우, 규칙은 해당 세션에 대해 지정된 수의 바이트만 검사하며, 필요에 따라 여러 패킷에 걸쳐 검사합니다.

  소규모 흐름 수준 값이 **Ports(포트)**에 정의된 서버 측 트래픽을 대상으로 하는 규칙에서 잘못된 부정을 야기할 수 있다는 점에 유의하십시오. 이러한 규칙의 대부분은 비 헤더 데이터의 처음 백여 바이트에 있을 가능성이 높은 HTTP 헤더 또는 컨텐츠를 대상으로 합니다. 헤더 길이는 일반적으로 300바이트보다 작지만, 헤더 크기는 다양할 수 있습니다.

  또한 지정된 값이 세그먼트 및 리어셈블된 패킷 모두에 적용된다는 점에 유의하십시오.

- 0은 **Ports(포트)**에 정의된 모든 서버 측 HTTP 트래픽에 대한 전체 패킷을 검사하는데, 65535 바이트를 초과하는 세션에서 응답 데이터를 포함합니다.

  이 값이 성능에 영향을 줄 수 있다는 점에 유의하십시오.

- -1:

  Inspect HTTP Response(HTTP 응답 검사)가 **활성화**된 경우 원시 HTTP 응답 본문이 아닌 원시 HTTP 헤더만 검사합니다.

  Inspect HTTP Response(HTTP 응답 검사)가 **비활성화**된 경우 **Ports(포트)**에 정의된 모든 서버 측 트래픽을 무시합니다.

최대 헤더 길이

HTTP 요청에서 지정된 최대 바이트 수보다 긴 헤더 필드를 탐지합니다. **Inspect HTTP Response(HTTP 응답 검사)**가 활성화된 경우 HTTP 응답에도 해당됩니다. 0 값은 이 옵션을 비활성화합니다. 1에서 65535 사이의 값을 지정하여 이 옵션을 활성화합니다.

규칙 119:19를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

최대 헤더 수

HTTP 요청에서 헤더 수가 이 설정을 초과하는 경우 이를 탐지합니다. 1에서 1024 사이의 값을 지정하여 이 옵션을 활성화합니다.

규칙 119:20을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

최대 스페이스 수

접혀진 회선에서 공백의 수가 HTTP 요청에서 이 설정과 동일하거나 초과하는 경우 이를 탐지합니다. 0 값은 이 옵션을 비활성화합니다. 1에서 65535 사이의 값을 지정하여 이 옵션을 활성화합니다.

규칙 119:26을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

HTTP 클라이언트 본문 추출 수준

HTTP 클라이언트 요청의 메시지 본문에서 추출할 바이트 수를 지정합니다. 침입 규칙을 사용하여 `content` 또는 `protected_content` 키워드 **HTTP Client Body(HTTP 클라이언트 본문)** 옵션을 선택하여 추출된 데이터를 검사할 수 있습니다. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오.

-1에서 65495 사이의 값을 지정합니다. 클라이언트 본문을 무시하려면 -1을 지정합니다. 전체 클라이언트 본문을 추출하려면 0을 지정합니다. 추출할 특정 바이트를 확인하면 시스템 성능을 개선할 수 있다는 점에 유의하십시오. **HTTP Client Body(HTTP 클라이언트 본문)** 옵션이 침입 규칙에서 작동하도록 하려면 0에서 65495 사이의 값을 지정해야 한다는 점에 유의하십시오.

소규모 청크 크기

하나의 청크가 작은 것으로 고려되는 최대 바이트 수를 지정합니다. 0에서 255 사이의 값을 지정합니다. 0 값은 이상 징후를 보이는 연속된 소규모 세그먼트의 탐지를 비활성화합니다. 자세한 내용은 **Consecutive Small Chunks(연속된 소규모 청크)** 옵션을 참고하십시오.

연속된 소규모 청크

얼마나 많은 연속된 작은 청크가 청크화된 이동 인코딩을 사용하는 클라이언트 또는 서버 트래픽에서 비정상적으로 큰 수를 나타내는지 지정합니다. **Small Chunk Size(소규모 청크 크기)** 옵션은 작은 청크의 최대 크기를 지정합니다.

예를 들어, **Small Chunk Size(소규모 청크 크기)**를 10으로 설정하고 **Consecutive Small Chunks(연속된 소규모 청크)**를 5로 설정하여 10바이트 이하의 연속된 5개의 청크를 탐지합니다.

전처리기 규칙 119:27을 활성화하여 클라이언트 트래픽의 과도한 소규모 청크에서 이벤트를 트리거할 수 있고, 전처리기 규칙 120:7을 활성화하여 서버 트래픽의 과도한 소규모 청크에서 이벤트를 트리거할 수 있습니다. **Small Chunk Size(소규모 청크 크기)**가 활성화되고 이 옵션이 0 또는 1에 설정될 때, 이 규칙을 활성화하면 지정된 크기 또는 그보다 작은 모든 청크에서 이벤트가 트리거됩니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

HTTP 메서드

시스템의 트래픽에 발생할 것으로 예상되는 GET 및 POST 외에 HTTP 요청 메서드를 지정합니다. 여러 개의 값을 구분하려면 쉼표를 사용하십시오.

침입 규칙은 `content` 또는 `protected_content` 키워드를 **HTTP Method(HTTP 메서드)** 인수와 함께 사용하여 HTTP 메서드 내 콘텐츠를 검색합니다. 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오. 규칙 119:31을 활성화하여 GET 및 POST 이외의 메서드 또는 이 옵션에 구성된 메서드가 트래픽에 발생할 경우 이벤트를 생성할 수 있습니다.

경고 없음

동반되는 전처리기 규칙이 활성화된 경우 침입 이벤트를 비활성화합니다.

참고 이 옵션은 **절대** HTTP 표준 텍스트 규칙 및 공유 객체 규칙을 비활성화하지 않습니다.

HTTP 헤더 표준화

Inspect HTTP Response(HTTP 응답 검사)가 활성화된 경우 요청 및 응답 헤더에서 비쿠키 데이터의 표준화를 활성화합니다. **Inspect HTTP Response(HTTP 응답 검사)**가 활성화되지 **않은** 경우 요청 및 응답 헤더에서 쿠키를 포함하여 전체 HTTP 헤더의 표준화를 활성화합니다.

HTTP 쿠키 검사

HTTP 요청 헤더에서 쿠키 추출을 활성화합니다. 또한 **Inspect HTTP Responses(HTTP 응답 검사)**가 활성화된 경우 응답 헤더에서 set-cookie 데이터 추출을 활성화합니다. 쿠키 추출이 필요하지 않은 경우 이 옵션을 비활성화하면 성능을 높일 수 있습니다.

`Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스, 그리고 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않는다는 점에 유의하십시오.

HTTP 헤더 내 쿠키 표준화

HTTP 요청 헤더에서 쿠키의 표준화를 활성화합니다. **Inspect HTTP Responses(HTTP 응답 검사)**가 활성화된 경우 응답 헤더 내 set-cookie 데이터의 표준화 또한 활성화합니다. 이 옵션을 선택하기 전에 **Inspect HTTP Cookies(HTTP 쿠키 검사)**를 선택해야 합니다.

HTTP 프록시 사용 허용

모니터링된 웹 서버가 HTTP 프록시로 사용되는 것을 허용합니다. 이 옵션은 HTTP 요청 검사에서만 사용됩니다.

URI만 검사

표준화된 HTTP 요청 패킷의 URI 부분만 검사합니다.

HTTP 응답 검사

HTTP 요청 메시지를 디코딩하고 표준화하는 것 외에도 HTTP 응답의 확장된 검사를 활성화하여 전처리기가 규칙 엔진에 의한 검사를 위해 응답 필드를 추출하도록 합니다. 이 옵션을 활성화하면 시스템이 응답 헤더, 본문, 상태 코드 등을 추출하며 **Inspect HTTP Cookies(HTTP 쿠키 검사)**가 활성화된 경우 set-cookie 데이터도 추출합니다. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션, 23-94페이지의 HTTP 인코딩 유형 및 위치에서 이벤트 생성 및 23-97페이지의 특정 페이로드 유형 나타내기를 참고하십시오.

규칙 120:2 및 120:3을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

UTF 인코딩을 UTF-8로 표준화

Inspect HTTP Response(HTTP 응답 검사)가 활성화된 경우 HTTP 응답에서 UTF-16LE, UTF-16BE, UTF-32LE 및 그리고 UTF32-BE 인코딩을 탐지하고 이들을 UTF-8로 표준화합니다.

규칙 120:4를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

압축 데이터 검사

Inspect HTTP Response(HTTP 응답 검사)가 활성화된 경우 HTTP 응답 본문 내 gzip 및 deflate 호환 가능 압축 데이터의 압축 해제와 압축 해제된 표준화 데이터의 검사를 활성화합니다. 시스템이 청크화된 HTTP 응답 데이터 및 비청크화된 HTTP 응답 데이터를 검사합니다. 시스템은 필요에 따라 여러 패킷에 걸쳐 패킷 별로 압축 해제된 데이터 패킷을 검사합니다. 즉 시스템이 검사를 위해 서로 다른 패킷의 압축 해제된 데이터를 결합하지 않습니다. **Maximum Compressed Data Depth(압축 데이터 최대 수준)**, **Maximum Decompressed Data Depth(압축 해제된 데이터 최대 수준)** 또는 압축 해제된 데이터의 끝부분에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression(무제한 압축 해제)**를 선택하지 않은 경우 **Server Flow Depth(서버 흐름 수준)**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. `file_data` 규칙 키워드를 사용하여 압축 해제된 데이터를 검사할 수 있습니다. 자세한 내용은 23-97페이지의 특정 페이로드 유형 나타내기를 참고하십시오.

무제한 압축 해제

Inspect Compressed Data(압축 데이터 검사)(및, 선택적으로, **Decompress SWF File(SWF 파일 압축 해제, LZMA)**, **Decompress SWF File(SWF 파일 압축 해제, Deflate)** 또는 **Decompress PDF File(PDF 파일 압축 해제, Deflate)**)가 활성화되어 있는 경우 여러 패킷에 걸친 **Maximum Decompressed Data Depth(압축 해제된 데이터 최대 수준)**를 재정의합니다. 즉, 이 옵션은 여러 패킷에 걸친 무제한 압축 해제를 활성화합니다. 이 옵션을 활성화해도 단일 패킷 내 **Maximum Compressed Data Depth(압축 데이터 최대 수준)** 또는 **Maximum Decompressed Data Depth(압축 해제된 데이터 최대 수준)**에 영향을 주지 않는다는 점에 유의하십시오. 또한 이 옵션을 활성화하는 경우 변경을 커밋하면 **Maximum Compressed Data Depth(압축 데이터 최대 수준)** 및 **Maximum Decompressed Data Depth(압축 해제된 데이터 최대 수준)**를 65535로 설정한다는 점에 유의하십시오. 15-32페이지의 전역 HTTP 표준화 옵션 선택을 참고하십시오.

JavaScript 표준화

Inspect HTTP Response(HTTP 응답 검사)가 활성화된 경우 HTTP 응답 본문 내 JavaScript의 탐지 및 표준화를 활성화합니다. 전처리기는 unescape 및 decodeURI 함수 및 String.fromCharCode 메서드와 같이 난독 처리된 JavaScript 데이터를 표준화합니다. 전처리기는 unescape, decodeURI 및 decodeURIComponent 함수에서 다음 인코딩을 표준화합니다.

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

전처리기는 연속적인 여백을 탐지하고 이를 단일 스페이스로 표준화합니다. 이 옵션을 활성화할 경우, 구성 필드를 사용하여 사용자가 난독 처리된 JavaScript 데이터에서 허용할 연속적인 여백의 최대 수를 지정할 수 있습니다. 1에서 65535까지의 값을 입력할 수 있습니다. 이 필드와 연결된 전처리기 규칙(120:10)이 활성화되는지 여부에 관계 없이 0 값은 이벤트 생성을 비활성화합니다.

전처리기는 또한 JavaScript의 더하기(+) 연산자를 표준화하고 연산자를 사용하여 문자열을 연결합니다.

`file_data` 키워드를 사용하여 표준화된 JavaScript 데이터에 침입 규칙을 연결할 수 있습니다. 자세한 내용은 23-97페이지의 특정 페이로드 유형 나타내기를 참고하십시오.

다음과 같이, 규칙 120:9, 120:10 및 120:11을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다.

표 15-6 JavaScript 옵션 규칙 표준화

규칙	다음과 같은 경우 이벤트가 트리거됩니다...
120:9	전처리기 내 난독 처리 수준은 2와 같거나 큽니다.
120:10	JavaScript 난독 처리된 데이터에서 연속적인 여백의 수는 허용된 연속적인 여백의 최대 수에 구성된 값과 같거나 큽니다.
120:11	이스케이프 또는 인코딩된 데이터는 하나 이상의 인코딩 유형을 포함합니다.

자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

SWF 파일 압축 해제(LZMA) 및 SWF 파일 압축 해제(Deflate)

HTTP Inspect Responses(HTTP 응답 검사)가 활성화된 경우 이러한 옵션은 HTTP 요청의 HTTP 응답 본문 내에 있는 파일의 압축된 부분을 압축 해제합니다.

참고 HTTP GET 응답에서 찾은 파일의 압축된 부분**만** 압축 해제할 수 있습니다.

- **Decompress SWF File(SWF 파일 압축 해제, LZMA)**은 Adobe ShockWave Flash(`.swf`) 파일의 LZMA 호환 가능 압축된 부분을 압축 해제합니다.
- **Decompress SWF File(SWF 파일 압축 해제, Deflate)**은 Adobe ShockWave Flash(`.swf`) 파일의 deflate 호환 가능 압축된 부분을 압축 해제합니다.

Maximum Compressed Data Depth(압축 데이터 최대 수준), **Maximum Decompressed Data Depth(압축 해제된 데이터 최대 수준)** 또는 압축 해제된 데이터의 끝부분에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression(무제한 압축 해제)**를 선택하지 않은 경우 **Server Flow Depth(서버 흐름 수준)**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. `file_data` 규칙 키워드를 사용하여 압축 해제된 데이터를 검사할 수 있습니다. 자세한 내용은 23-97페이지의 특정 페이로드 유형 나타내기를 참고하십시오.

다음과 같이, 규칙 120:12 및 120:13을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다.

표 15-7 SWF 파일 압축 해제 옵션 규칙

규칙	다음과 같은 경우 이벤트가 트리거됩니다...
120:12	deflate 파일 압축 풀기에 실패합니다.
120:13	LZMA 파일 압축 풀기에 실패합니다.

PDF 파일 압축 해제(Deflate)

HTTP Inspect Responses(HTTP 응답 검사)가 활성화된 경우, **Decompress PDF File(PDF 파일 압축 해제, Deflate)**은 HTTP 요청의 HTTP 응답 본문 내에 있는 Portable Document Format(`.pdf`) 파일의 deflate 호환 가능 압축된 부분을 압축 해제합니다. 시스템은 `/FlateDecode` 스트림 필터를 사용하는 PDF 파일의 압축만 해제할 수 있습니다. 다른 스트림 필터(`/FlateDecode /FlateDecode` 포함)는 지원되지 않습니다.

참고 HTTP GET 응답에서 찾은 파일의 압축된 부분**만** 압축 해제할 수 있습니다.

Maximum Compressed Data Depth(압축 데이터 최대 수준), **Maximum Decompressed Data Depth(압축 해제된 데이터 최대 수준)** 또는 압축 해제된 데이터의 끝부분에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression(무제한 압축 해제)**를 선택하지 않은 경우 **Server Flow Depth(서버 흐름 수준)**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. `file_data` 규칙 키워드를 사용하여 압축 해제된 데이터를 검사할 수 있습니다. 자세한 내용은 23-97페이지의 특정 페이로드 유형 나타내기를 참고하십시오.

다음과 같이, 규칙 120:14, 120:15, 120:16 및 120:17을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다.

표 15-8 PDF 파일 압축 해제(Deflate) 옵션 규칙

규칙	다음과 같은 경우 이벤트가 트리거됩니다...
120:14	파일 압축 풀기에 실패합니다.
120:15	지원되지 않는 압축 유형 때문에 파일 압축 풀기에 실패합니다.
120:16	지원되지 않는 PDF 스트림 필터로 인해 파일 압축 풀기에 실패합니다.
120:17	파일 구문 분석에 실패합니다.

원래 클라이언트 IP 주소 추출

X-Forwarded-For(XFF), True-Client-IP 또는 사용자가 정의한 HTTP 헤더에서 원래 클라이언트 IP 주소의 추출을 활성화합니다. 추출된 원래 클라이언트 IP 주소를 침입 이벤트 보기에서 표시할 수 있습니다. 자세한 내용은 26-1페이지의 이벤트 보기를 참고하십시오.

규칙 119:23, 119:29 및 119:30을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

XFF 헤더 우선 순위

Extract Original Client IP Address(원래 클라이언트 IP 주소 추출)가 활성화된 경우 시스템이 원래 클라이언트 IP HTTP 헤더를 처리할 순서를 지정합니다. 모니터링된 네트워크에서 X-Forwarded-For(XFF) 또는 True-Client-IP가 아닌 원래 클라이언트 IP 헤더가 발생할 것으로 예상하는 경우, **Add(추가)**를 클릭하여 우선 순위에 추가 헤더 이름을 추가할 수 있습니다. 그러면 각 헤더 유형 옆에 있는 위로 및 아래로 화살표 아이콘을 사용하여 해당 우선 순위를 설정할 수 있습니다. 여러 XFF 헤더가 하나의 HTTP 요청에 표시되는 경우, 시스템은 가장 높은 우선 순위를 가진 헤더만 처리한다는 점에 유의하십시오.

URI 로그

HTTP 요청 패킷의 원시 URI 추출(있는 경우)을 활성화하고 세션에 대해 생성된 모든 침입 이벤트와 해당 URI를 연결합니다.

이 옵션을 활성화할 경우, 침입 이벤트 표 보기의 HTTP URI 열에서 추출한 URI의 첫 50자를 표시할 수 있습니다. 패킷 보기에서 전체 URI를 최대 2048바이트까지 표시할 수 있습니다. 자세한 내용은 26-1페이지의 이벤트 보기를 참고하십시오.

호스트 이름 로그

HTTP 요청 호스트 헤더의 호스트 이름 추출(있는 경우)을 활성화하고 세션에 대해 생성된 모든 침입 이벤트와 해당 호스트 이름을 연결합니다. 여러 호스트 헤더가 있을 경우, 첫 번째 헤더에서 호스트 이름을 추출합니다.

이 옵션을 활성화할 경우, 침입 이벤트 표 보기의 HTTP Hostname(호스트 이름) 열에서 추출한 호스트 이름의 첫 50자를 표시할 수 있습니다. 패킷 보기에서 전체 호스트 이름을 최대 2048바이트까지 표시할 수 있습니다. 자세한 내용은 26-1페이지의 이벤트 보기를 참고하십시오.

규칙 119:25를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

전처리기 및 규칙 119:24를 활성화할 경우, 이 옵션의 설정에 상관없이, 전처리기가 HTTP 요청에서 여러 Host(호스트) 헤더를 탐지하면 침입 이벤트를 생성한다는 점에 유의하십시오. 자세한 내용은 15-47페이지의 추가 HTTP 검사 전처리기 규칙 활성화를 참고하십시오.

프로파일

HTTP 트래픽에 표준화된 인코딩 유형을 지정합니다. 시스템은 대부분의 서버에 적절한 기본 프로파일을 제공하고, Apache 서버 및 IIS 서버에 대한 기본 프로파일과 모니터링되는 트래픽의 요구 사항을 충족하도록 조정할 수 있는 사용자 지정 기본 설정을 제공합니다. 자세한 내용은 15-42페이지의 서버 수준 HTTP 표준화 인코딩 옵션 선택을 참고하십시오.

서버 수준 HTTP 표준화 인코딩 옵션 선택

라이센스: 보호

서버 수준 HTTP 표준화 옵션을 선택하여 HTTP 트래픽에 표준화된 인코딩 유형을 지정하고, 시스템이 이 인코딩 유형을 포함하는 트래픽에 대해 이벤트를 생성하도록 할 수 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

ASCII 인코딩

인코딩된 ASCII 문자를 디코딩하고 규칙 엔진이 ASCII 기반으로 인코딩된 URI에서 이벤트를 생성할지 여부를 지정합니다.

규칙 119:1을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

UTF-8 인코딩

URI에서 UTF-8 유니코드 표준 시퀀스를 디코딩합니다.

규칙 119:6을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

Microsoft %U 인코딩

4개 문자가 IIS 유니코드 코드 포인트와 관련이 있는 16진수로 인코딩된 값인 4개 문자가 뒤에 오는 %u를 사용하는 IIS %u 인코딩 체계를 디코딩합니다.

팁 적법한 클라이언트는 %u 인코딩을 거의 사용하지 않으며, 따라서 Cisco는 %u 인코딩으로 인코딩된 HTTP 트래픽을 디코딩할 것을 권장합니다.

규칙 119:3을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

베어 바이트 UTF-8 인코딩

UTF-8 값 디코딩 시 비ASCII 문자를 유효한 값으로 사용하는 베어 바이트 인코딩을 디코딩합니다.

팁 베어 바이트 인코딩을 통해 사용자가 IIS 서버를 에뮬레이션하고 비표준 인코딩을 올바르게 해석할 수 있습니다. 적법한 어떤 클라이언트도 UTF-8을 이러한 방식으로 인코딩하지 않으므로 Cisco는 이 옵션을 활성화할 것을 권장합니다.

규칙 119:4를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

Microsoft IIS 인코딩

유니코드 코드 포인트 매핑을 사용하여 디코딩합니다.

팁 이는 주로 공격 및 우회 시도에서 발견되므로 Cisco는 이 옵션을 활성화할 것을 권장합니다.

규칙 119:7을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

이중 인코딩

각각에서 디코딩을 수행하는 요청 URI를 통해 두 개 회선을 만들어 IIS 이중 인코딩된 트래픽을 디코딩합니다. 이는 주로 공격 시나리오에서 발견되므로 Cisco는 이 옵션을 활성화할 것을 권장합니다.

규칙 119:2를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

다중 슬래시 난독 처리

연속된 다중 슬래시를 단일 슬래시로 표준화합니다.

규칙 119:8을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

IIS 백슬래시 난독 처리

백슬래시를 사선으로 표준화합니다.

규칙 119:9를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

디렉토리 접근 공격

디렉토리 접근 공격 및 자기 참조 디렉토리를 표준화합니다. 이 트래픽 유형에 대한 이벤트를 생성하기 위해 해당 전처리기 규칙을 활성화하는 경우, 일부 웹 사이트에서 디렉토리 접근 공격을 사용하는 파일을 참조하므로 잘못된 긍정이 생성될 수 있습니다.

규칙 119:10 및 119:11을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

탭 난독 처리

스페이스 구분 기호에 탭을 사용하는 비 RFC 표준을 표준화합니다. Apache 및 기타 비 IIS 웹 서버는 URL의 구분 기호로 탭 문자(0x09)를 사용합니다.

참고 이 옵션의 구성에 관계 없이, 공백 문자(0x20)가 이 앞에 오는 경우 HTTP Inspect(HTTP 검사) 전처리기는 탭을 공백으로 처리합니다.

규칙 119:12를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

유효하지 않은 RFC 구분 기호

URI 데이터 내 행 바꿈(\n)을 표준화합니다.

규칙 119:13을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

Webroot 디렉토리 접근 공격

URL에서 초기 디렉토리를 가로질러 통과하는 디렉토리 접근 공격을 탐지합니다.

규칙 119:18을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

탭 URI 구분 기호

URI의 구분 기호로 탭 문자(0x09) 사용을 설정합니다. IIS의 Apache, 새 버전, 다른 웹 서버는 URL의 탭으로 구분 문자를 사용합니다.

참고 이 옵션의 구성에 관계 없이, 공백 문자(0x20)가 이 앞에 오는 경우 HTTP Inspect(HTTP 검사) 전처리기는 탭을 공백으로 처리합니다.

비 RFC 문자

사용자가 추가한 비 RFC 문자 목록이 수신 및 발신 URI 데이터에 나타날 때 해당 필드에서 이를 탐지합니다. 이 필드를 수정할 경우, 바이트 문자를 나타내는 16진수 형식을 사용합니다. 이 옵션을 구성할 경우 값을 신중하게 설정합니다. 매우 일반적인 문자를 사용하면 이벤트가 과하게 생성될 수 있습니다.

규칙 119:14를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

최대 청크 인코딩 크기

URI 데이터에서 비정상적으로 큰 청크 크기를 탐지합니다.

규칙 119:16 및 119:22를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

파이프라인 디코딩 비활성화

파이프라인 요청에 대한 HTTP 디코딩을 비활성화합니다. 이 옵션을 비활성화하면, 파이프라인에 대기 중인 HTTP 요청이 디코딩되거나 분석되지 않고, 일반 패턴 일치만 사용하여 검사되기 때문에 성능이 향상됩니다.

엄격하지 않은 URI 구문 분석

엄격하지 않은 URI 구문 분석을 활성화합니다. "GET /index.html abc xo qr \n" 형식에서 비표준 URI를 수용하는 서버에서만 이 옵션을 사용합니다. 이 옵션을 사용하면, 두 번째 스페이스 뒤에 유효한 HTTP 식별자가 없는 경우에도 디코더는 URI가 첫 번째와 두 번째 스페이스 사이에 있다고 가정합니다.

확장된 ASCII 인코딩

HTTP 요청 URI 내 확장된 ASCII 문자의 구문 분석을 활성화합니다. 이 옵션은 사용자 지정 서버 프로파일에서만 사용 가능하며, Apache, IIS 또는 모든 서버에 제공된 기본 프로파일에서는 그렇지 않다는 점에 유의하십시오.

HTTP 서버 옵션 구성

라이센스: 보호

HTTP 서버 옵션을 구성하려면 다음 절차를 수행합니다. HTTP 서버 옵션에 대한 자세한 내용은 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택 및 15-42페이지의 서버 수준 HTTP 표준화 인코딩 옵션 선택을 참고하십시오.

서버 수준 HTTP 구성 옵션을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **HTTP Configuration(HTTP 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

HTTP Configuration(HTTP 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 다음 2가지 옵션을 사용할 수 있습니다.

- 새로운 서버 프로파일을 추가합니다. 추가 아이콘( )을 클릭합니다. 이 아이콘은 페이지 왼쪽의 **Servers(서버)** 옆에 있습니다. Add Target(대상 추가) 팝업 창이 나타납니다. **Server Address(서버 주소)** 필드에 하나 이상의 IP 주소를 지정하고 **OK(확인)**를 클릭합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 목록에 최대 496개의 문자를 포함할 수 있고, 모든 서버 프로파일에 대해 총 256개의 주소 항목을 지정할 수 있으며, 기본 프로파일을 포함하여 총 255개의 프로파일을 생성할 수 있습니다. ASA FirePOWER 모듈에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

새 항목은 페이지 왼쪽의 서버 목록에 나타나는데, 선택되었음을 나타내도록 강조 표시됩니다. 그리고 Configuration(구성) 섹션은 추가한 프로파일에 대한 현재 구성을 반영하도록 업데이트됩니다.

- 기존 프로파일에 대한 설정을 수정합니다. 페이지 왼쪽의 **Servers(서버)**에 추가한 프로파일에 대해 구성된 주소를 클릭하거나 **default(기본값)**를 클릭합니다.

  선택한 부분이 강조 표시되고, Configuration(구성) 섹션이 선택한 프로파일에 대한 현재 구성을 표시하도록 업데이트됩니다. 기존 프로파일을 삭제하려면, 제거할 프로파일 옆에 있는 삭제 아이콘( )을 클릭합니다.

단계 10 또는, **Networks(네트워크)** 필드에 나열된 주소를 수정하고 페이지의 다른 영역을 클릭합니다.

페이지 왼쪽에 강조 표시된 주소가 업데이트됩니다.

기본 프로파일에서 **Networks(네트워크)**에 대한 설정을 수정할 수 없다는 점에 유의하십시오. 기본 프로파일은 다른 프로파일에서 인증되지 않은 네트워크의 모든 서버에 적용됩니다.

단계 11 **Ports(포트)** 필드에, 트래픽을 HTTP Inspect(HTTP 검사)로 검사할 포트를 나열합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

단계 12 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택에 설명된 다른 옵션을 변경할 수 있습니다.

단계 13 다음과 같이 서버 프로파일을 선택합니다:

- 자체 서버 프로파일을 만들려면 **Custom(사용자 지정)**을 선택합니다(자세한 내용은 15-42페이지의 서버 수준 HTTP 표준화 인코딩 옵션 선택 참조).
- 모든 서버에 대해 적절한 표준 기본 프로파일을 사용하려면 **All(모두)**을 선택합니다.
- 기본 IIS 프로파일을 사용하려면 **IIS**를 선택합니다.
- 기본 Apache 프로파일을 사용하려면 **Apache**를 선택합니다.

단계 14 **Custom(사용자 지정)**을 선택한 경우, 사용자 지정 옵션이 나타납니다.

단계 15 사용자 프로파일에서 원하는 HTTP 디코딩 옵션을 구성합니다.

사용 가능한 표준화 옵션에 대한 자세한 내용은 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택을 참고하십시오.

단계 16 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

추가 HTTP 검사 전처리기 규칙 활성화

라이센스: 보호

다음 표의 **Preprocessor Rule GID:SID(전처리기 규칙 GID:SID)** 열에서 규칙을 활성화하여 특정 구성 옵션과 관련이 없는 HTTP Inspect(HTTP 검사) 전처리기 규칙에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

표 15-9 추가 HTTP 검사 전처리기 규칙

전처리기 규칙 GID:SID	설명
120:5	HTTP 응답 트래픽에서 UTF-7 인코딩이 발생할 때 이벤트를 생성합니다. UTF-7은 SMTP 트래픽에서와 같이 7비트 패리티가 필요한 경우에만 표시되어야 합니다.
119:21	HTTP 요청 헤더에 하나 이상의 `content-length` 필드가 있는 경우 이벤트를 생성합니다.
119:24	HTTP 요청에 하나 이상의 Host(호스트) 헤더가 있는 경우 이벤트를 생성합니다.
119:28 120:8	활성화된 경우, 이러한 규칙은 이벤트를 생성하지 않습니다.
119:32	트래픽에서 HTTP 버전 0.9가 발생할 때 이벤트를 생성합니다. TCP 스트림 구성 역시 활성화되어야 한다는 점에 유의하십시오. 17-20페이지의 TCP 스트림 전처리 사용을 참고하십시오.
119:33	HTTP URL가 이스케이프되지 않은 스페이스를 포함할 때 이벤트를 생성합니다.
119:34	TCP 연결이 24 또는 그 이상의 파이프라인 처리된 HTTP 요청을 포함할 때 이벤트를 생성합니다.

Sun RPC 전처리기의 사용

라이센스: 보호

RPC(원격 절차 호출) 표준화가 조각화된 RPC 레코드를 가져와 단일 레코드로 표준화하므로 규칙 엔진이 전체 레코드를 검사할 수 있습니다. 예를 들어, 공격자는 RPC `admind`가 실행되는 포트를 검색하려고 시도할 수 있습니다. 일부 UNIX 호스트는 RPC `admind`를 사용하여 원격 분산 시스템 작업을 수행합니다. 호스트가 보안성이 낮은 인증을 수행할 경우, 악의적인 사용자가 원격 관리를 적용할 수 있습니다. Snort ID(SID) 575가 포함된 표준 텍스트 규칙(생성기 ID: 1)은 특정 위치의 콘텐츠를 검색함으로써 이 공격을 탐지하여 부적절한 `portmap GETPORT` 요청을 식별합니다.

포트

트래픽을 표준화할 포트를 지정합니다. 인터페이스에서, 쉼표로 구분하여 여러 개의 포트를 나열합니다. 일반적인 RPC 포트는 111 및 32771입니다. 네트워크가 다른 포트에 RPC 트래픽을 전송할 경우 이들의 추가를 고려하십시오.

조각화된 RPC 레코드 탐지

조각화된 RPC 레코드를 탐지합니다.

규칙 106:1 및 106:5을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

1개의 패킷에서 여러 레코드 탐지

패킷 (또는 리어셈블된 패킷) 당 1개 이상의 RPC 요청을 탐지합니다.

규칙 106:2를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

단일 조각을 초과하는 조각화된 레코드 총합 탐지

현재 패킷 길이를 초과하는 리어셈블된 조각 레코드 길이를 탐지합니다.

규칙 106:3을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

1개의 패킷 크기를 초과하는 단일 조각 레코드 탐지

일부 레코드를 탐지합니다.

규칙 106:4를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

Sun RPC 전처리기 구성

라이센스: 보호

다음 절차를 사용하여 Sun RPC 전처리기를 구성할 수 있습니다. Sun RPC 전처리기 구성 옵션에 대한 자세한 내용은 15-47페이지의 Sun RPC 전처리기의 사용을 참고하십시오.

Sun RPC 전처리기를 설정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **Sun RPC Configuration(Sun RPC 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Sun RPC Configuration(Sun RPC 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 **Ports(포트)** 필드에, RPC 트래픽을 디코딩할 포트 번호를 입력합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

단계 10 Sun RPC Configuration(Sun RPC 구성) 페이지에서 다음 탐지 옵션을 선택하거나 지울 수 있습니다.

- **조각화된 RPC 레코드 탐지**
- **1개의 패킷에서 여러 레코드 탐지**
- **1개의 패킷을 초과하는 단편화된 레코드 총합 탐지**
- **1개의 패킷 크기를 초과하는 단일 조각 레코드 탐지**

단계 11 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

세션 시작 프로토콜 디코딩

라이센스: 보호

SIP(세션 시작 프로토콜)는 인터넷 텔레포니, 멀티미디어 컨퍼런싱, 인스턴트 메시징, 온라인 게임 및 파일 전송과 같은 클라이언트 애플리케이션의 한 명 이상의 사용자를 위한 하나 이상의 세션을 가진 통화 설정, 수정 및 세분화를 제공합니다. 각 SIP 요청의 *method(메서드)* 필드는 요청의 목적을 확인하고, Request-URI는 요청을 전송할 위치를 지정합니다. 각 SIP 응답의 상태 코드는 요청된 작업의 결과를 나타냅니다.

통화가 SIP를 사용하여 설치되면 RTP(실시간 전송 프로토콜)가 이후의 오디오 및 비디오 커뮤니케이션을 담당합니다. 세션의 이 부분은 경우에 따라 통화 채널, 데이터 채널 또는 오디오/비디오 데이터 채널로 지칭됩니다. RTP는 데이터 채널 매개변수 협상, 세션 공지 및 세션 초대를 위한 SIP 메시지 본문 내에서 SDP(세션 설명 프로토콜)를 사용합니다.

SIP 전처리기는 다음과 같은 작업을 담당합니다.

- SIP 2.0 트래픽 디코딩 및 분석
- SDP 데이터가 있는 경우 이를 포함하여 SIP 헤더 및 메시지 본문 추출, 추가 검사를 위해 규칙 엔진에 추출된 데이터 전달
- 다음 조건이 탐지되고 해당 전처리기 규칙이 활성화된 경우 이벤트 생성: SIP 패킷의 이상 징후 및 알려진 취약성, 비순차적이고 유효하지 않은 통화 시퀀스
- 또는 통화 채널 무시

전처리기는 SIP 메시지 본문에 내장된 SDP 메시지에서 식별된 포트에 따라 RTP 채널을 식별하지만, 전처리기는 RTP 프로토콜 검사를 제공하지 않습니다.

SIP 전처리기를 사용하는 경우 다음 사항에 유의하십시오.

- UDP는 일반적으로 SIP에서 지원되는 미디어 세션을 전송합니다. UDP 스트림 전처리는 SIP 전처리기에 SIP 세션 추적을 제공합니다.

- SIP 규칙 키워드를 통해 SIP 패킷 헤더 또는 메시지 본문으로 이동하고 특정 SIP 메서드 또는 상태 코드의 패킷에 대한 탐지를 제한할 수 있습니다. 자세한 내용은 23-61페이지의 SIP 키워드를 참고하십시오.
- 전처리기가 활성화되면, 생성기 ID(GID) 140에 동반되는 규칙 또한 활성화하지 않는 한 전처리기는 추출한 데이터를 규칙 엔진에 전송하기 전에는 어떤 이벤트도 생성하지 않습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 15-50페이지의 SIP 전처리기 옵션 선택
- 15-52페이지의 SIP 전처리기 구성
- 15-53페이지의 추가 SIP 전처리기 규칙 활성화

SIP 전처리기 옵션 선택

라이센스: 보호

다음 목록은 사용자가 수정할 수 있는 SIP 전처리기 옵션에 대해 설명합니다.

Maximum Request URI Length(요청 URI 최대 길이), **Maximum Call ID Length(통화 ID 최대 길이)**, **Maximum Request Name Length(요청 이름 최대 길이)**, **Maximum From Length(발신지 최대 길이)**, **Maximum To Length(수신지 최대 길이)**, **Maximum Via Length(경유지 최대 길이)**, **Maximum Contact Length(접촉 최대 길이)** 및 **Maximum Content Length(콘텐츠 최대 길이)** 옵션의 경우 1에서 65535바이트까지 지정할 수 있으며, 0을 지정하여 연결된 규칙이 활성화되는지 여부에 관계 없이 해당 옵션에 대한 이벤트 생성을 비활성화할 수도 있습니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

SIP 트래픽을 위해 검사할 포트를 지정합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

점검할 메서드

탐지할 SIP 메서드를 지정합니다. 다음 중 하나로 현재 정의된 SIP 메서드를 지정할 수 있습니다.

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

메서드는 대소문자를 구분하지 않습니다. 메서드 이름은 알파벳 문자, 숫자 및 밑줄 문자를 포함할 수 있습니다. 다른 특수 문자는 허용되지 않습니다. 메서드가 여러 개인 경우 쉼표로 구분하십시오.

향후 새 SIP 메서드가 정의될 수도 있기 때문에, 사용자의 구성은 현재 정의되지 않은 영문자열을 포함할 수 있습니다. 시스템은 최대 32개의 메서드까지 지원하는데, 최근 정의된 메서드 21개에 메서드 11개를 추가한 것입니다. 시스템은 사용자가 구성할 수 있는 정의되지 않은 모든 메서드를 무시합니다.

이 옵션에 지정한 메서드 외에도 총 32개의 메서드에는 침입 규칙에서 `sip_method` 키워드를 사용하여 지정된 메서드가 포함된다는 점에 유의하십시오. 자세한 내용은 23-62페이지의 sip_method를 참고하십시오.

세션 내 최대 대화 상자

스트림 세션 내에서 허용되는 최대 대화 상자 수를 지정합니다. 이 숫자보다 많은 대화 상자가 생성되는 경우 대화 상자 수가 지정된 최대 수를 초과하지 않을 때까지 가장 오래된 통화가 삭제됩니다. 규칙 140:27이 활성화된 경우 이벤트도 트리거됩니다.

1에서 4194303까지의 정수를 지정할 수 있습니다.

요청 URI 최대 길이

Request-URI 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:3이 활성화된 경우 더 긴 URI가 이벤트를 트리거합니다. 요청 URI 필드는 요청에 대한 대상 경로 또는 페이지를 나타냅니다.

통화 ID 최대 길이

요청 또는 응답 Call-ID 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:5가 활성화된 경우 더 긴 Call-ID가 이벤트를 트리거합니다. Call-ID 필드는 특별히 요청 및 응답의 SIP 세션을 식별합니다.

요청 이름 최대 길이

CSeq 트랜잭션 식별자에 지정된 메서드의 이름인 요청 이름에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:7이 활성화된 경우 더 긴 요청 이름이 이벤트를 트리거합니다.

발신지 최대 길이

요청 또는 응답 From 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:9가 활성화된 경우 더 긴 From 필드에서 이벤트를 트리거합니다. From 필드는 메시지 초기자를 식별합니다.

수신지 최대 길이

요청 또는 응답 To 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:11이 활성화된 경우 더 긴 To 필드에서 이벤트를 트리거합니다. To 필드는 메시지 수신자를 식별합니다.

경유지 최대 길이

요청 또는 응답 Via 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:13이 활성화된 경우 더 긴 Via 필드가 이벤트를 트리거합니다. Via 필드는 요청이 뒤따르는 경로를 제공하며, 응답에서는 수신 정보를 제공합니다.

접촉 최대 길이

요청 또는 응답 Contact 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:15가 활성화된 경우 더 긴 Contact 필드에서 이벤트를 트리거합니다. Contact 필드는 이후의 메시지와 접촉할 위치를 지정하는 URI를 제공합니다.

콘텐츠 최대 길이

요청 또는 응답 메시지 본문의 콘텐츠에서 허용할 최대 바이트 수를 지정합니다. 규칙 140:16이 활성화된 경우 더 긴 콘텐츠가 이벤트를 트리거합니다.

오디오/비디오 데이터 채널 무시

데이터 채널 트래픽에 대한 검사를 활성화 및 비활성화합니다. 이 옵션을 활성화하면 전처리기는 비 데이터 채널 SIP 트래픽에 대한 검사를 계속한다는 점에 유의하십시오.

SIP 전처리기 구성

라이센스: 보호

SIP 전처리기를 구성하려면 다음 절차를 수행합니다.

SIP 전처리기를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **SIP Configuration(SIP 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

SIP Configuration(SIP 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 15-50페이지의 SIP 전처리기 옵션 선택에서 설명한 모든 옵션을 수정할 수 있습니다.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

추가 SIP 전처리기 규칙 활성화

라이센스: 보호

다음 표의 SIP 전처리기 규칙은 특정 구성 옵션과 관련이 없습니다. 다른 SIP 전처리기 규칙에서와 마찬가지로 SIP 전처리기 규칙에서 이벤트를 생성하려는 경우, 이러한 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

표 15-10 추가 SIP 전처리기 규칙

전처리기 규칙 GID:SID	설명
140:1	전처리기가 시스템에서 허용되는 SIP 세션의 최대 수를 모니터링할 때 이벤트를 생성합니다.
140:2	요청된 Request_URI 필드가 SIP 요청에서 비어 있는 경우 이벤트를 생성합니다.
140:4	Call-ID 헤더 필드가 SIP 요청 또는 응답에서 비어 있는 경우 이벤트를 생성합니다.
140:6	SIP 요청 또는 응답 CSeq 필드의 시퀀스 번호의 값이 231보다 작은 32비트 무부호 정수가 아닌 경우 이벤트를 생성합니다.
140:8	From 헤더 필드가 SIP 요청 또는 응답에서 비어 있는 경우 이벤트를 생성합니다.
140:10	To 헤더 필드가 SIP 요청 또는 응답에서 비어 있는 경우 이벤트를 생성합니다.
140:12	Via 헤더 필드가 SIP 요청 또는 응답에서 비어 있는 경우 이벤트를 생성합니다.
140:14	요청된 Contact 헤더 필드가 SIP 요청 또는 응답에서 비어 있는 경우 이벤트를 생성합니다.
140:17	UDP 트래픽의 단일 SIP 요청 또는 응답 패킷이 여러 메시지를 포함할 때 이벤트를 생성합니다. 이전 버전의 SIP는 여러 메시지를 지원했지만 SIP 2.0은 패킷당 1개의 메시지만 지원한다는 점에 유의하십시오.
140:18	UDP 트래픽의 SIP 요청 또는 응답에서 메시지 본문의 실제 길이가 SIP 요청 또는 응답 내 Content-Length 헤더 필드에 지정된 값에 일치하지 않을 경우 이벤트를 생성합니다.
140:19	전처리기가 SIP 응답의 CSeq 필드에서 메서드 이름을 인식하지 않을 경우 이벤트를 생성합니다.
140:20	SIP 서버가 입증된 초대 메시지에 이의를 제기하지 않을 경우 이벤트를 생성합니다. 이는 InviteReplay 청구 공격의 경우 발생한다는 점에 유의하십시오.
140:21	통화가 설정되기 전에 세션 정보가 바뀌는 경우 이벤트를 생성합니다. 이는 FakeBusy 청구 공격의 경우 발생한다는 점에 유의하십시오.
140:22	응답 상태 코드가 3자리 수인 경우 이벤트를 생성합니다.
140:23	Content-Type(콘텐츠 유형) 헤더 필드가 콘텐츠 형식을 지정하지 않고 메시지 텍스트가 데이터를 포함하는 경우 이벤트를 생성합니다.
140:24	SIP 버전이 1, 1.1, 또는 2.0인 경우 이벤트를 생성합니다.
140:25	CSeq 헤더 및 메서드 필드에 지정된 메서드가 SIP 요청에 일치하지 않는 경우 이벤트를 생성합니다.
140:26	전처리기가 SIP 요청 방법 필드에서 명명된 메서드를 인식하지 않을 경우 이벤트를 생성합니다.

GTP 명령 채널 구성

라이센스: 보호

GTP(GPRS[General Service Packet Radio] 터널링 프로토콜)는 GTP 코어 네트워크를 통한 통신을 제공합니다. GTP 전처리기는 GTP 트래픽 내 이상 징후를 탐지하고 검사를 위해 규칙 엔진에 명령 채널 신호 메시지를 전달합니다. `gtp_version`, `gtp_type` 및 `gtp_info` 규칙 키워드를 사용하여 익스플로잇 탐지를 위해 GTP 명령 채널 트래픽을 검사할 수 있습니다.

단일 구성 옵션을 사용하면 전처리기가 GTP 명령 채널 메시지를 검사하는 포트의 기본 설정을 변경할 수 있습니다.

GTP 전처리기 규칙이 이벤트를 생성하기를 원할 경우 다음 표에서 이를 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

표 15-11 GTP 전처리기 규칙

전처리기 규칙 GID:SID	설명
143:1	전처리기가 유효하지 않은 메시지 길이를 탐지하면 이벤트를 생성합니다.
143:2	전처리기가 유효하지 않은 정보 요소 길이를 탐지하면 이벤트를 생성합니다.
143:3	전처리기가 비순차적 정보 요소를 탐지하면 이벤트를 생성합니다.

다음 절차를 수행하여 GTP 전처리기가 GTP 명령 메시지를 모니터링하는 포트를 수정할 수 있습니다.

GTP 명령 채널을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘()(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **GTP Command Channel Configuration(GTP 명령 채널 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

GTP Command Channel Configuration(GTP 명령 채널 구성) 페이지가 나타납니다.

단계 9 또는, 전처리기가 GTP 명령 메시지를 검사하는 포트를 수정합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 여러 포트를 구분하려면 쉼표를 사용하십시오.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

IMAP 트래픽 디코딩

라이센스: 보호

Internet Message Application Protocol(인터넷 메시지 애플리케이션 프로토콜, IMAP)을 사용하여 원격 IMAP 서버의 이메일을 검색합니다. IMAP 전처리기는 서버-클라이언트 IMAP4 트래픽을 검사하고 관련 전처리기 규칙이 활성화되면 변칙 트래픽에 이벤트를 생성합니다. 전처리기는 또한 클라이언트-서버 IMAP4 트래픽의 이메일 첨부 파일을 추출하여 디코딩하고 규칙 엔진에 첨부 파일 데이터를 보낼 수 있습니다. 첨부 파일 데이터를 지정할 때 침입 규칙에서 `file_data` 키워드를 사용할 수 있습니다. 자세한 내용은 23-97페이지의 특정 페이로드 유형 나타내기를 참고하십시오.

여러 첨부 파일이 있는 경우 추출 및 디코딩에 포함되며, 여러 패킷을 포괄하는 큰 첨부 파일도 포함됩니다.

IMAP 전처리기 규칙에서 이벤트를 생성하려는 경우 규칙을 활성화해야 합니다. IMAP 전처리기 규칙에는 생성기 ID(GID) 141이 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 15-55페이지의 IMAP 전처리기 옵션 선택
- 15-57페이지의 IMAP 전처리기 구성
- 15-58페이지의 추가 IMAP 전처리기 규칙 활성화

IMAP 전처리기 옵션 선택

라이센스: 보호

다음 목록은 사용자가 수정할 수 있는 IMAP 전처리기 옵션에 대해 설명합니다.

MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 디코딩 또는 추출에는 여러 첨부 파일(있는 경우) 및 여러 패킷을 포괄하는 큰 첨부 파일이 포함된다는 점에 유의하십시오.

또한 다음 상황에서 **Base64 Decoding Depth(Base64 디코딩 수준)**, **7-Bit/8-Bit/Binary Decoding Depth(7비트/8비트/이진 디코딩 수준)**, **Quoted-Printable Decoding Depth(따옴표로 묶인 인쇄 가능한 디코딩 수준)** 또는 **Unix-to-Unix Decoding Depth(Unix-to-Unix 디코딩 수준)** 옵션의 값이 서로 다를 때 가장 높은 값이 사용된다는 점에 유의하십시오.

- 기본 네트워크 분석 정책
- 동일한 액세스 제어 정책의 네트워크 분석 규칙에서 호출된 기타 사용자 지정 네트워크 분석 정책

자세한 내용은 13-4페이지의 액세스 제어를 위한 기본 네트워크 분석 정책 설정 및 13-4페이지의 네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정을 참고하십시오.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

IMAP 트래픽을 검사할 포트를 지정합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

Base64 디코딩 수준

Base64로 인코딩된 각 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트를 지정할 수 있으며, 0을 지정하여 모든 Base64 데이터를 디코딩할 수도 있습니다. Base64 데이터를 무시하려면 -1을 지정합니다.

4로 나누어지지 않는 양수는 다음 4의 배수로 올림 처리된다는 점에 유의하십시오. 이때 65533, 65534, 및 65535 값은 제외되는데, 이들은 65532로 내림 처리됩니다.

Base64 디코딩이 활성화된 경우, 규칙 141:4를 활성화하여 디코딩이 실패할 경우 이벤트를 생성할 수 있습니다. 예를 들어, 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

7비트/8비트/이진 디코딩 수준

디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 데이터의 최대 바이트를 지정합니다. 이 첨부 파일 형식에는 평문, jpeg 이미지, mp3 파일 등과 같이 7비트, 8비트, 이진 및 다양한 다중 부분 콘텐츠 형식 등이 있습니다. 1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출할 수도 있습니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다.

따옴표로 묶인 인쇄 가능한 디코딩 수준

QP(Quoted-Printable)로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 QP로 인코딩된 모든 데이터를 디코딩할 수도 있습니다. QP로 인코딩된 데이터를 무시하려면 -1을 지정합니다.

QP(Quoted-Printable) 디코딩이 활성화된 경우, 규칙 141:6을 활성화하여 디코딩이 실패할 경우 이벤트를 생성할 수 있습니다. 예를 들어, 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

Unix-to-Unix 디코딩 수준

Unix-to-Unix로 인코딩된(uuencoded) 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 1~65535 바이트를 지정할 수 있으며, 0을 지정하여 패킷의 모든 uuencoded 데이터를 디코딩할 수도 있습니다. uuencoded 데이터를 무시하려면 -1을 지정합니다.

Unix-to-Unix 디코딩이 활성화된 경우, 규칙 141:7을 활성화하여 디코딩이 실패할 경우 이벤트를 생성할 수 있습니다. 예를 들어, 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다.

IMAP 전처리기 구성

라이센스: 보호

IMAP 전처리기를 구성하려면 다음 절차를 수행합니다. IMAP 전처리기 구성 옵션에 대한 자세한 내용은 15-55페이지의 IMAP 전처리기 옵션 선택을 참고하십시오.

IMAP 전처리기를 설정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘()(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **IMAP Configuration(IMAP 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

IMAP Configuration(IMAP 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 IMAP 트래픽이 디코딩되어야 할 **Ports(포트)**를 지정합니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

단계 10 다음 이메일 첨부 파일 유형의 조합에서 추출하고 디코딩할 데이터의 최대 바이트 수를 지정합니다.

- **Base64 디코딩 수준**
- **7-Bit/8-Bit/Binary Decoding Depth(7비트/8비트/이진 디코딩 수준)**(평문, jpeg 이미지, mp3 파일 등과 같이 다양한 다중 부분 콘텐츠 형식 포함)
- **따옴표로 묶인 인쇄 가능한 디코딩 수준**
- **Unix-to-Unix 디코딩 수준**

각 유형의 경우, 1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출하고 필요한 경우 디코딩할 수도 있습니다. 첨부 파일 유형의 데이터를 무시하려면 -1을 지정합니다.

침입 규칙에서 `file_data` 규칙 키워드를 사용하여 첨부 파일 데이터를 검사할 수 있습니다. 자세한 내용은 23-97페이지의 특정 페이로드 유형 나타내기를 참고하십시오.

단계 11 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

추가 IMAP 전처리기 규칙 활성화

라이센스: 보호

다음 표의 IMAP 전처리기 규칙은 특정 구성 옵션과 관련이 없습니다. 다른 IMAP 전처리기 규칙에서와 마찬가지로 IMAP 전처리기 규칙에서 이벤트를 생성하려는 경우, 이러한 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

표 15-12 추가 IMAP 전처리기 규칙

전처리기 규칙 GID:SID	설명
141:1	전처리기가 RFC 3501에 정의되지 않은 클라이언트 명령을 탐지하면 이벤트를 생성합니다.
141:2	전처리기가 RFC 3501에 정의되지 않은 서버 응답을 탐지하면 이벤트를 생성합니다.
141:3	전처리기가 시스템에서 허용되는 최대 메모리 양을 사용하는 경우 이벤트를 생성합니다. 여기서, 전처리기는 메모리를 사용할 수 있을 때까지 디코딩을 중지합니다.

POP 트래픽 디코딩

라이센스: 보호

Post Office Protocol(포스트 오피스 프로토콜, POP)을 사용하여 원격 POP 서버의 이메일을 검색합니다. POP 전처리기는 서버-클라이언트 POP3 트래픽을 검사하고 관련 전처리기 규칙이 활성화되면 변칙 트래픽에 이벤트를 생성합니다. 전처리기는 또한 클라이언트-서버 POP3 트래픽의 이메일 첨부 파일을 추출 및 디코딩하고 규칙 엔진에 첨부 파일 데이터를 보낼 수 있습니다. 첨부 파일 데이터를 지정할 때 침입 규칙에서 `file_data` 키워드를 사용할 수 있습니다. 자세한 내용은 23-97페이지의 특정 페이로드 유형 나타내기를 참고하십시오.

여러 첨부 파일이 있는 경우 추출 및 디코딩에 포함되며, 여러 패킷을 포괄하는 큰 첨부 파일도 포함됩니다.

POP 전처리기에서 이벤트를 생성하려는 경우 규칙을 활성화해야 합니다. POP 전처리기 규칙에는 생성기 ID(GID) 142가 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 15-59페이지의 POP 전처리기 옵션 선택
- 15-60페이지의 POP 전처리기 구성
- 15-61페이지의 추가 POP 전처리기 규칙 활성화

POP 전처리기 옵션 선택

라이센스: 보호

다음 목록은 수정할 수 있는 POP 전처리기 옵션에 대해 설명합니다.

MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 디코딩 또는 추출에는 여러 첨부 파일(있는 경우) 및 여러 패킷을 포괄하는 큰 첨부 파일이 포함된다는 점에 유의하십시오.

또한 **Base64 Decoding Depth(Base64 디코딩 수준)**, **7-Bit/8-Bit/Binary Decoding Depth(7비트/8비트/이진 디코딩 수준)**, **Quoted-Printable Decoding Depth(따옴표로 묶인 인쇄 가능한 디코딩 수준)** 또는 **Unix-to-Unix Decoding Depth(Unix-to-Unix 디코딩 수준)** 옵션의 값이 액세스 제어 규칙과 관련된 침입 정책 및 액세스 제어 정책의 기본 작업과 관련된 침입 정책에서 서로 다른 경우, 가장 높은 값이 사용된다는 점에 유의하십시오.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

POP 트래픽을 검사할 포트를 지정합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

Base64 디코딩 수준

Base64로 인코딩된 각 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트를 지정할 수 있으며, 0을 지정하여 모든 Base64 데이터를 디코딩할 수도 있습니다. Base64 데이터를 무시하려면 -1을 지정합니다.

4로 나누어지지 않는 양수는 다음 4의 배수로 올림 처리된다는 점에 유의하십시오. 이때 65533, 65534, 및 65535 값은 제외되는데, 이들은 65532로 내림 처리됩니다.

Base64 디코딩이 활성화된 경우, 규칙 142:4를 활성화하여 디코딩이 실패할 경우 이벤트를 생성할 수 있습니다. 예를 들어, 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

7비트/8비트/이진 디코딩 수준

디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 데이터의 최대 바이트를 지정합니다. 이 첨부 파일 형식에는 평문, jpeg 이미지, mp3 파일 등과 같이 7비트, 8비트, 이진 및 다양한 다중 부분 콘텐츠 형식 등이 있습니다. 1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출할 수도 있습니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다.

따옴표로 묶인 인쇄 가능한 디코딩 수준

QP(Quoted-Printable)로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 QP로 인코딩된 모든 데이터를 디코딩할 수도 있습니다. QP로 인코딩된 데이터를 무시하려면 -1을 지정합니다.

QP(Quoted-Printable) 디코딩이 활성화된 경우, 규칙 142:6을 활성화하여 디코딩이 실패할 경우 이벤트를 생성할 수 있습니다. 예를 들어, 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

Unix-to-Unix 디코딩 수준

Unix-to-Unix로 인코딩된(uuencoded) 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 1~65535 바이트를 지정할 수 있으며, 0을 지정하여 패킷의 모든 uuencoded 데이터를 디코딩할 수도 있습니다. uuencoded 데이터를 무시하려면 -1을 지정합니다.

Unix-to-Unix 디코딩이 활성화된 경우, 규칙 142:7을 활성화하여 디코딩이 실패할 경우 이벤트를 생성할 수 있습니다. 예를 들어, 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

POP 전처리기 구성

라이센스: 보호

POP 전처리기를 구성하려면 다음 절차를 수행합니다. POP 전처리기 구성 옵션에 대한 자세한 내용은 15-59페이지의 POP 전처리기 옵션 선택을 참고하십시오.

POP 전처리기를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **POP Configuration(POP 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

POP Configuration(POP 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 IMAP 트래픽이 디코딩되어야 할 **Ports(포트)**를 지정합니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

단계 10 다음 이메일 첨부 파일 유형의 조합에서 추출하고 디코딩할 데이터의 최대 바이트 수를 지정합니다.

- **Base64 디코딩 수준**
- **7-Bit/8-Bit/Binary Decoding Depth(7비트/8비트/이진 디코딩 수준)**(평문, jpeg 이미지, mp3 파일 등과 같이 다양한 다중 부분 콘텐츠 형식 포함)
- **따옴표로 묶인 인쇄 가능한 디코딩 수준**
- **Unix-to-Unix 디코딩 수준**

각 유형의 경우, 1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출하고 필요한 경우 디코딩할 수도 있습니다. 첨부 파일 유형의 데이터를 무시하려면 -1을 지정합니다.

침입 규칙에서 `file_data` 규칙 키워드를 사용하여 첨부 파일 데이터를 검사할 수 있습니다. 자세한 내용은 23-97페이지의 특정 페이로드 유형 나타내기를 참고하십시오.

단계 11 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

추가 POP 전처리기 규칙 활성화

라이센스: 보호

다음 표의 POP 전처리기 규칙은 특정 구성 옵션과 관련이 없습니다. 다른 POP 전처리기 규칙에서와 마찬가지로 POP 전처리기 규칙에서 이벤트를 생성하려는 경우, 이러한 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

표 15-13 추가 POP 전처리기 규칙

전처리기 규칙 GID:SID	설명
142:1	전처리기가 RFC 1939에 정의되지 않은 클라이언트 명령을 탐지하면 이벤트를 생성합니다.
142:2	전처리기가 RFC 1939에 정의되지 않은 서버 응답을 탐지하면 이벤트를 생성합니다.
142:3	전처리기가 시스템에서 허용되는 최대 메모리 양을 사용하는 경우 이벤트를 생성합니다. 여기서, 전처리기는 메모리를 사용할 수 있을 때까지 디코딩을 중지합니다.

SMTP 트래픽 디코딩

라이센스: 보호

SMTP 전처리기는 규칙 엔진이 SMTP 명령을 표준화하도록 지시합니다. 전처리기는 또한 클라이언트-서버 트래픽의 이메일 첨부 파일을 추출하고 디코딩할 수 있습니다. 그리고, SMTP 트래픽에서 트리거된 침입 이벤트를 표시할 경우 이메일 파일 이름, 주소 및 헤더 데이터를 소프트웨어 버전에 따라 추출하여 컨텍스트를 제공할 수 있습니다.

SMTP 전처리기를 사용하는 경우 다음 사항에 유의하십시오.

- 124의 생성기 ID(GID)가 있는 SMTP 전처리기 규칙에서 이벤트를 생성하려는 경우, 이 규칙을 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 15-62페이지의 SMTP 디코딩 이해
- 15-66페이지의 SMTP 디코딩 구성
- 15-69페이지의 SMTP 디코딩 최대 메모리 경고 활성화

SMTP 디코딩 이해

라이센스: 보호

표준화를 활성화하거나 비활성화하고, SMTP 디코더가 탐지하는 변칙 트래픽 유형을 제어하는 옵션을 구성할 수 있습니다.

MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 디코딩 또는 추출에는 여러 첨부 파일(있는 경우) 및 여러 패킷을 포괄하는 큰 첨부 파일이 포함된다는 점에 유의하십시오.

또한 **Base64 Decoding Depth(Base64 디코딩 수준)**, **7-Bit/8-Bit/Binary Decoding Depth(7비트/8비트/이진 디코딩 수준)**, **Quoted-Printable Decoding Depth(따옴표로 묶인 인쇄 가능한 디코딩 수준)** 또는 **Unix-to-Unix Decoding Depth(Unix-to-Unix 디코딩 수준)** 옵션의 값이 액세스 제어 규칙과 관련된 침입 정책 및 액세스 제어 정책의 기본 작업과 관련된 침입 정책에서 서로 다른 경우, 가장 높은 값이 사용된다는 점에 유의하십시오.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

포트

SMTP 트래픽을 표준화할 포트를 지정합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

상태 저장 검사

이를 선택하면, SMTP 디코더가 상태를 저장하고 개별 패킷을 위한 세션 컨텍스트를 제공하며, 리어셈블한 세션만 검사할 수 있습니다. 이를 취소하면, 세션 컨텍스트 없이 각 개별 패킷을 분석합니다.

표준화

All(모두)로 설정된 경우, 모든 명령을 표준화합니다. 명령 다음에 나오는 하나 이상의 공백 문자를 확인합니다.

None(없음)으로 설정된 경우, 어떤 명령도 표준화하지 않습니다.

Cmds로 설정된 경우, **Custom Commands(사용자 지정 명령)**에 나열된 명령을 표준화합니다.

사용자 지정 명령

Normalize(표준화)가 Cmds로 설정된 경우, 나열된 명령을 표준화합니다.

텍스트 상자에서 표준화되어야 하는 명령을 지정합니다. 명령 다음에 나오는 하나 이상의 공백 문자를 확인합니다.

스페이스(ASCII 0x20) 및 탭(ASCII 0x09) 문자는 표준화를 위한 공백 문자로 간주됩니다.

데이터 무시

메일 데이터를 처리하지 않습니다. MIME 메일 헤더 데이터만 처리합니다.

TLS 데이터 무시

Transport Layer Security(전송 레이어 보안) 프로토콜의 암호화된 데이터를 처리하지 않습니다.

경고 없음

동반되는 전처리기 규칙이 활성화된 경우 침입 이벤트를 비활성화합니다.

알 수 없는 명령 탐지

SMTP 트래픽에서 알 수 없는 명령을 탐지합니다.

규칙 124:5 및 124:6이 이 옵션을 위해 이벤트를 생성하도록 활성화할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

명령줄 최대 길이

SMTP 명령줄이 이 값보다 길 경우 이를 탐지합니다. 명령줄 길이를 탐지하지 않으려면 0을 지정합니다.

간단한 메일 전송 프로토콜의 네트워크 작업 그룹 사양인 RFC 2821은 명령줄 최대 길이로 512를 권장합니다.

규칙 124:1을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

헤더 행 최대 길이

SMTP 데이터 헤더 행이 이 값보다 길 경우 이를 탐지합니다. 데이터 헤더 행 길이를 탐지하지 않으려면 0을 지정합니다.

규칙 124:2 및 124:7을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

응답 회선 최대 길이

SMTP 응답 회선이 이 값보다 길 경우 이를 탐지합니다. 응답 회선 길이를 탐지하지 않으려면 0을 지정합니다.

RFC 2821는 응답 회선 최대 길이로 512를 권장합니다.

규칙 124:3을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

대안적 명령줄 최대 길이

지정된 모든 명령에 대한 SMTP 명령줄이 이 값보다 길 경우 이를 탐지합니다. 지정된 명령에 대한 명령줄 길이를 탐지하지 않으려면 0을 지정합니다. 여러 명령에 대해 다양한 기본 회선 길이가 설정됩니다.

이 설정은 지정된 명령에 대한 Max Command Line Len(명령줄 최대 길이) 설정을 무시합니다.

규칙 124:3을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

유효하지 않은 명령

이 명령어가 클라이언트 측에서 전송되는지 여부를 탐지합니다.

규칙 124:5 및 124:6이 이 옵션을 위해 이벤트를 생성하도록 활성화할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

유효한 명령

이 목록에 있는 명령을 허용합니다.

이 목록이 비어있더라도, 전처리기는 다음 유효한 명령을 허용합니다. ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

참고 RCPT TO 및 MAIL FROM은 SMTP 명령입니다. 전처리기 구성은 RCPT와 MAIL의 명령 이름을 각각 사용합니다. 해당 코드 안에서, 전처리기는 RCPT와 MAIL을 정확한 명령 이름에 매핑합니다.

규칙 124:4를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

데이터 명령

SMTP DATA 명령이 RFC 5321당 데이터를 전송하는 것과 동일한 방식으로 데이터 전송을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

이진 데이터 명령

BDAT 명령이 RFC 3030당 데이터를 전송하는 것과 유사한 방식으로 데이터 전송을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

인증 명령

클라이언트와 서버 간의 인증 교환을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

xlink2state 탐지

X-Link2State Microsoft Exchange 버퍼 데이터 오버플로 공격의 일부인 패킷을 탐지합니다. 인라인 배포에서, 시스템은 해당 패킷을 삭제할 수 있습니다.

규칙 124:8을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

Base64 디코딩 수준

Ignore Data(데이터 무시)가 비활성화된 경우, Base64로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트를 지정할 수 있으며, 0을 지정하여 모든 Base64 데이터를 디코딩할 수도 있습니다. Base64 데이터를 무시하려면- 1을 지정합니다. **Ignore Data(데이터 무시)**를 선택한 경우 전처리기는 데이터를 디코딩하지 않습니다.

4로 나누어지지 않는 양수는 다음 4의 배수로 올림 처리된다는 점에 유의하십시오. 이때 65533, 65534, 및 65535 값은 제외되는데, 이들은 65532로 내림 처리됩니다.

Base64 디코딩이 활성화된 경우, 규칙 124:10을 활성화하여 디코딩이 실패할 경우 이벤트를 생성할 수 있습니다. 예를 들어, 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

이 옵션은 **Enable MIME Decoding(MIME 디코딩 활성화)** 및 **Maximum MIME Decoding Depth(MIME 디코딩 최대 수준)**와 같이 더 이상 사용되지 않는 옵션을 대체한다는 점에 유의하십시오. 이 옵션은 이전 버전과의 호환성을 위해 기존 침입 정책에서 계속 지원됩니다.

7비트/8비트/이진 디코딩 수준

Ignore Data(데이터 무시)가 비활성화된 경우, 디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 데이터의 최대 바이트를 지정합니다. 이 첨부 파일 형식에는 평문, jpeg 이미지, mp3 파일 등과 같이 7비트, 8비트, 이진 및 다양한 다중 부분 콘텐츠 형식 등이 있습니다. 1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 모든 데이터를 추출할 수도 있습니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다. **Ignore Data(데이터 무시)**가를 선택한 경우 전처리기는 데이터를 추출하지 않습니다.

따옴표로 묶인 인쇄 가능한 디코딩 수준

Ignore Data(데이터 무시)가 비활성화된 경우, QP(Quoted-Printable)로 인코딩된 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다.

1~65535바이트를 지정할 수 있으며, 0을 지정하여 패킷의 QP로 인코딩된 모든 데이터를 디코딩할 수도 있습니다. QP로 인코딩된 데이터를 무시하려면 -1을 지정합니다. **Ignore Data(데이터 무시)**를 선택한 경우 전처리기는 데이터를 디코딩하지 않습니다.

QP(Quoted-Printable) 디코딩이 활성화된 경우, 규칙 124:11을 활성화하여 디코딩이 실패할 경우 이벤트를 생성할 수 있습니다. 예를 들어, 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

Unix-to-Unix 디코딩 수준

Ignore Data(데이터 무시)가 비활성화된 경우, Unix-to-Unix로 인코딩된(uuencoded) 각 MIME 이메일 첨부 파일에서 추출 및 디코딩할 최대 바이트 수를 지정합니다. 1~65535 바이트를 지정할 수 있으며, 0을 지정하여 패킷의 모든 uuencoded 데이터를 디코딩할 수도 있습니다. uuencoded 데이터를 무시하려면 -1을 지정합니다. **Ignore Data(데이터 무시)**를 선택한 경우 전처리기는 데이터를 디코딩하지 않습니다.

Unix-to-Unix 디코딩이 활성화된 경우, 규칙 124:13을 활성화하여 디코딩이 실패할 경우 이벤트를 생성할 수 있습니다. 예를 들어, 유효하지 않은 인코딩 또는 손상된 데이터로 인해 디코딩이 실패할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

MIME 첨부 파일 이름 로그

MIME Content-Disposition 헤더에서 MIME 첨부 파일 이름의 추출을 활성화하고 파일 이름을 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 파일 이름이 지원됩니다.

이 옵션을 사용할 경우, 침입 이벤트 표 보기의 Email Attachment(이메일 첨부 파일) 열에서 이벤트와 관련된 파일 이름을 볼 수 있습니다. 자세한 내용은 26-1페이지의 이벤트 보기를 참고하십시오.

수신지 주소 로그

SMTP RCPT TO 명령에서 수신자 전자 메일 주소의 추출을 활성화하고 수신자 주소를 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 수신자가 지원됩니다.

이 옵션을 사용할 경우, 침입 이벤트 표 보기의 Email Recipient(전자 메일 수신자) 열에서 이벤트와 관련된 수신자를 볼 수 있습니다. 자세한 내용은 26-1페이지의 이벤트 보기를 참고하십시오.

발신지 주소 로그

SMTP MAIL FROM 명령에서 발신자 전자 메일 주소의 추출을 활성화하고 발신자 주소를 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 발신자 주소가 지원됩니다.

이 옵션을 사용할 경우, 침입 이벤트 표 보기의 Email Sender(이메일 발신자) 열에서 이벤트와 관련된 발신자를 볼 수 있습니다. 자세한 내용은 26-1페이지의 이벤트 보기를 참고하십시오.

헤더 로그

전자 메일 헤더의 추출을 활성화합니다. 추출할 바이트 수는 **Header Log Depth(헤더 로그 수준)**에 지정된 값에 따라 결정됩니다.

`content` 또는 `protected_content` 키워드를 사용하여 이메일 헤더 데이터를 패턴으로 사용하는 침입 규칙을 작성할 수 있습니다. 또한 침입 이벤트 패킷 보기에서 추출한 전자 메일 헤더를 볼 수 있습니다. 자세한 내용은 26-1페이지의 이벤트 보기를 참고하십시오.

헤더 로그 수준

Log Headers(헤더 로그)가 활성화된 경우 추출할 전자 메일 헤더의 바이트 수를 지정합니다. 0~20480바이트를 지정할 수 있습니다. 값을 0으로 지정하면 **Log Headers(헤더 로그)**가 비활성화됩니다.

SMTP 디코딩 구성

라이센스: 보호

침입 정책의 SMTP Configuration(SMTP 구성) 페이지를 사용하여 SMTP 표준화를 구성할 수 있습니다. SMTP 전처리기 구성 옵션에 대한 자세한 내용은 15-62페이지의 SMTP 디코딩 이해를 참고하십시오.

SMTP 디코딩 옵션을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘()(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **SMTP Configuration(SMTP 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

SMTP Configuration(SMTP 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 SMTP 트래픽을 디코딩해야 하는 **Ports(포트)**를 쉼표로 구분하여 지정합니다.

단계 10 SMTP 패킷을 포함하는 리어셈블된 TCP 스트림을 검토하려면 **Stateful Inspection(상태 저장 검사)**을 선택합니다. 리어셈블되지 않은 SMTP 패킷만 검사하려면 **Stateful Inspection(상태 저장 검사)**을 비워둡니다.

단계 11 다음 표준화 옵션을 구성합니다.

- 모든 명령을 표준화하려면 **All(모두)**을 선택합니다.
- **Custom Commands(사용자 지정 명령)**에 지정된 명령만 표준화하려면, **Cmds**를 선택하고 표준화할 명령을 지정합니다. 스페이스로 명령을 구분합니다.
- 어떤 명령도 표준화하지 않으려면, **None(없음)**을 선택합니다.
- MIME 메일 헤더 데이터를 제외한 메일 데이터를 무시하려면, **Ignore Data(데이터 무시)**를 선택합니다.
- Transport Security Layer(전송 보안 레이어) 프로토콜에서 암호화된 데이터를 무시하려면 **Ignore TLS Data(TLS 데이터 무시)**를 선택합니다.
- 동반되는 전처리기 규칙이 활성화된 경우 이벤트 생성을 비활성화하려면 **No Alerts(경고 없음)**를 선택합니다.
- SMTP 데이터에서 알 수 없는 명령을 탐지하려면 **Detect Unknown Commands(알 수 없는 명령 탐지)**를 선택합니다.

단계 12 **Max Command Line Len(명령줄 최대 길이)** 필드에 명령줄 최대 길이를 지정합니다.

단계 13 **Max Header Line Len(헤더 행 최대 길이)** 필드에 데이터 헤더 행 최대 길이를 지정합니다.

단계 14 **Max Response Line Len(응답 회선 최대 길이)** 필드에 응답 회선 최대 길이를 지정합니다.

참고 RCPT TO 및 MAIL FROM은 SMTP 명령입니다. 전처리기 구성은 RCPT와 MAIL의 명령 이름을 각각 사용합니다. 해당 코드 안에서, 전처리기는 RCPT와 MAIL을 정확한 명령 이름에 매핑합니다.

단계 15 필요한 경우 **Alt Max Command Line Len(대안적 명령줄 최대 길이)** 옆에 있는 **Add(추가)**를 클릭하여 대안적 명령줄 최대 길이를 지정할 명령을 추가한 후 해당 길이를 적용할 회선 길이 및 명령을 스페이스로 구분하여 지정합니다.

단계 16 **Invalid Commands(유효하지 않은 명령)** 필드에 유효하지 않은 것으로 처리하고 탐지할 모든 명령을 지정합니다. 스페이스로 명령을 구분합니다.

단계 17 **Valid Commands(유효한 명령)** 필드에 유효한 것으로 처리할 모든 명령을 지정합니다. 스페이스로 명령을 구분합니다.

참고 **Valid Commands(유효한 명령)** 목록이 비어있더라도, 전처리기는 다음 명령을 유효한 것으로 처리합니다. ATRN, AUTH, BDAT, DATA, DEBUG, EHLO, EMAL, ESAM, ESND, ESOM, ETRN, EVFY, EXPN, HELO, HELP, IDENT, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SOML, SEND, ONEX, QUEU, STARTTLS, TICK, TIME, TURN, TURNME, VERB, VRFY, X-EXPS, X-LINK2STATE, XADR, XAUTH, XCIR, XEXCH50, XGEN, XLICENSE, XQUE, XSTA, XTRN 또는 XUSR.

단계 18 **Data Commands(데이터 명령)** 필드에 SMTP DATA 명령이 RFC 5321당 데이터를 전송하는 것과 동일한 방식으로 데이터 전송을 시작할 모든 명령을 지정합니다. 스페이스로 명령을 구분합니다.

단계 19 **Binary Data Commands(이진 데이터 명령)** 필드에 BDAT 명령이 RFC 3030당 데이터를 전송하는 것과 유사한 방식으로 데이터 전송을 시작할 모든 명령을 지정합니다. 스페이스로 명령을 구분합니다.

단계 20 **Authentication Commands(인증 명령)** 필드에 클라이언트와 서버 사이의 인증 교환을 시작하는 모든 명령을 지정합니다. 스페이스로 명령을 구분합니다.

단계 21 X-Link2State Microsoft Exchange 버퍼 데이터 오버플로 공격의 일부인 패킷을 탐지하려면 **Detect xlink2state(xlink2state 탐지)**를 선택합니다.

단계 22 다양한 유형의 이메일 첨부 파일에 대해 추출 및 디코딩할 데이터의 최대 바이트를 지정하려면, 다음과 같은 첨부 파일 유형의 값을 지정합니다.

- **Base64 디코딩 수준**
- **7-Bit/8-Bit/Binary Decoding Depth(7비트/8비트/이진 디코딩 수준)**(평문, jpeg 이미지, mp3 파일 등과 같이 다양한 다중 부분 콘텐츠 형식 포함)
- **따옴표로 묶인 인쇄 가능한 디코딩 수준**
- **Unix-to-Unix 디코딩 수준**

1~65535 바이트를 지정할 수 있으며, 0을 지정하여 해당 유형에 대한 패킷의 모든 데이터를 추출하고 필요한 경우 디코딩할 수도 있습니다. 첨부 파일 유형의 데이터를 무시하려면 -1을 지정합니다.

침입 규칙에서 `file_data` 규칙 키워드를 사용하여 추출된 데이터를 검사할 수 있습니다. 자세한 내용은 23-97페이지의 특정 페이로드 유형 나타내기를 참고하십시오.

또한 교차 패킷 데이터 또는 여러 TCP 세그먼트를 교차하는 데이터를 추출하고 디코딩하려면 SMTP **Stateful Inspection(상태 저장 검사)** 옵션을 선택해야 합니다.

단계 23 SMTP 트래픽에 의해 트리거된 침입 이벤트와 컨텍스트 정보를 연결할 옵션을 구성합니다.

- 침입 이벤트에 연결할 MIME 첨부 파일 이름의 추출을 활성화하려면, **Log MIME Attachment Names(MIME 첨부 파일 이름 로그)**를 선택합니다.
- 수신자 이메일 주소의 추출을 활성화하려면 **Log To Addresses(수신지 주소 로그)**를 선택합니다.
- 침입 이벤트에 연결할 발신자 이메일 주소의 추출을 활성화하려면, **Log From Addresses(발신지 주소 로그)**를 선택합니다.
- 침입 이벤트에 연결할 이메일 헤더의 추출을 활성화하고 이메일 헤더를 검사하는 규칙을 작성하려면 **Log Headers(헤더 로그)**를 선택합니다.

  헤더 정보가 침입 이벤트 패킷 보기에 표시된다는 점에 유의하십시오. 또한 `content` 또는 `protected_content` 키워드를 이메일 헤더 데이터와 함께 패턴으로 사용하는 침입 규칙을 작성할 수 있다는 점에 유의하십시오. 자세한 내용은 26-1페이지의 이벤트 보기를 참고하십시오.

  또는, 추출할 이메일 헤더의 **Header Log Depth(헤더 로그 수준)**을 0~20480바이트로 지정할 수 있습니다. 값을 0으로 지정하면 **Log Headers(헤더 로그)**가 비활성화됩니다.

단계 24 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

SMTP 디코딩 최대 메모리 경고 활성화

라이센스: 보호

SMTP 전처리기 규칙 124:9를 활성화하여 다음 유형의 인코딩된 데이터의 디코딩을 위해 활성화된 전처리기가 시스템에서 허용되는 최대 메모리 양을 사용하는 경우 이벤트를 생성할 수 있습니다.

- Base64
- 7비트/8비트/이진
- QP(Quoted-Printable)
- Unix-to-Unix

최대 디코딩 메모리를 초과할 경우, 전처리기는 메모리를 사용할 수 있을 때까지 인코딩된 데이터 유형의 디코딩을 중지합니다. 이 전처리기 규칙은 단일 특정 구성 옵션과 관련이 없습니다. 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

SSH 전처리기를 사용한 익스플로잇 탐지

라이센스: 보호

SSH 전처리기는 시도-응답 버퍼 오버플로 익스플로잇, CRC-32 익스플로잇, SecureCRT SSH 클라이언트 버퍼 오버플로 익스플로잇, 프로토콜 불일치 및 잘못된 SSH 메시지 방향을 탐지합니다. 전처리기는 또한 버전 1 또는 2 이외의 다른 버전 문자열을 탐지합니다.

시도 응답 버퍼 오버플로 및 CRC-32 공격은 키 교환 이후에 발생하므로 암호화됩니다. 두 공격 모두 인증 시도 직후 서버에 20KB가 넘는 터무니없이 큰 페이로드를 보냅니다. CRC-32 공격은 SSH 버전 1에만 적용되고, 시도 응답 버퍼 오버플로 익스플로잇은 SSH 버전 2에만 적용됩니다. 버전 문자열은 세션 시작 시 읽혀집니다. 버전 문자열의 차이를 제외하면, 두 공격 모두 동일하게 취급됩니다.

SecureCRT SSH 익스플로잇 및 프로토콜 불일치 공격은 키 교환 전에, 보안 연결을 하려고 할 때 발생합니다. SecureCRT 익스플로잇은 버퍼 오버플로를 야기하는 클라이언트에 과도하게 긴 프로토콜 식별자 문자열을 보냅니다. 프로토콜 불일치는 비SSH 클라이언트 애플리케이션이 보안 SSH 서버에 연결을 시도하거나 서버와 클라이언트 버전 번호가 일치하지 않는 경우 발생합니다.

전처리기가 지정된 포트 또는 포트 목록의 트래픽을 검사하거나 자동으로 SSH 트래픽을 탐지하도록 설정할 수 있습니다. 전처리기는 지정된 수의 암호화된 패킷이 지정된 수의 바이트 내부를 통과할 때까지 또는 지정된 최대 수의 바이트가 지정된 수의 패킷 내부에서 초과될 때까지 계속해서 SSH 트래픽을 검사합니다. 최대 수의 바이트가 초과된 경우, CRC-32(SSH 버전 1) 또는 시도-응답 버퍼 오버플로(SSH 버전 2) 공격이 발생한 것으로 가정합니다. 또한, SecureCRT 익스플로잇, 프로토콜 불일치 및 오류 메시지 방향을 탐지할 수 있습니다. 전처리기가 설정 없이도 버전 1 또는 2 이외의 다른 모든 버전의 문자열 값을 탐지한다는 점에 유의하십시오.

SSH 전처리기를 사용하는 경우 다음 사항에 유의하십시오.

- 128의 생성기 ID(GID)가 있는 SSH 전처리기 규칙에서 이벤트를 생성하려는 경우, 이 규칙을 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.
- SSH 전처리기는 무차별 암호 대입 공격을 처리하지 않습니다. 무차별 암호 대입 공격에 대한 내용은 20-28페이지의 동적 규칙 상태 추가를 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 15-70페이지의 SSH 전처리기 옵션 선택
- 15-72페이지의 SSH 전처리기 구성

SSH 전처리기 옵션 선택

라이센스: 보호

이 섹션에서는 SSH 전처리기를 구성하는 데 사용할 수 있는 옵션에 대해 설명합니다.

전처리기는 다음 사항 중 하나가 발생할 경우 세션에 대한 트래픽 검사를 중지합니다.

- 서버와 클라이언트 간 유효한 교환이 이 암호화된 패킷의 수만큼 발생하며 연결은 지속됩니다.
- **Number of Bytes Sent Without Server Response(서버 응답 없이 전송된 바이트 수)**에 도달한 후에 검사할 암호화된 패킷 수에 도달하며 공격이 있는 것으로 간주됩니다.

Number of Encrypted Packets to Inspect(검사할 암호화된 패킷 수)가 경과되는 동안 유효한 각 서버 응답은 **Number of Bytes Sent Without Server Response(서버 응답 없이 전송된 바이트 수)**를 재설정하며 패킷 카운트가 계속됩니다.

다음의 예시 SSH 전처리기 구성을 고려하십시오.

- **Server Ports(서버 포트)**: 22
- **Autodetect Ports(자동 탐지된 포트)**: 꺼짐
- **Maximum Length of Protocol Version String(프로토콜 버전 문자열의 최대 길이)**: 80
- **Number of Encrypted Packets to Inspect(검사할 암호화된 패킷 수)**: 25
- **Number of Bytes Sent Without Server Response(서버 응답 없이 전송된 바이트 수)**: 19,600
- 모든 탐지 옵션이 활성화됩니다.

예제에서, 전처리기는 포트 22에서만 트래픽을 검사합니다. 즉, 연결 자동 탐지가 비활성화되므로, 지정된 포트에서만 검사합니다.

또한, 다음 사항 중 하나가 발생할 경우 예제의 전처리기는 트래픽 검사를 중지합니다.

- 클라이언트는 누적해서 19,600 미만의 바이트를 포함하는 25개의 암호화된 패킷을 전송합니다. 공격이 전혀 없는 것으로 가정합니다.
- 클라이언트는 25개의 암호화된 패킷으로 19,600 이상의 바이트를 전송합니다. 이 경우, 예제의 세션이 SSH 버전 2 세션이므로 전처리기는 해당 공격이 시도 응답 버퍼 오버플로 익스플로잇인 것으로 간주합니다.

예제에서 전처리기는 트래픽을 처리하는 동안 발생하는 다음과 같은 모든 징후를 탐지합니다.

- 80바이트보다 큰 버전 문자열에서 트리거되었고 SecureCRT 익스플로잇을 나타내는 서버 오버플로
- 프로토콜 불일치
- 잘못된 방향으로 흐르는 패킷

마지막으로, 전처리기는 버전 1 또는 버전 2 외에도 자동으로 모든 버전 문자열을 탐지합니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

서버 포트

SSH 전처리기가 트래픽을 검사할 포트를 지정합니다.

단일 포트 또는 쉼표로 구분된 포트 목록을 구성할 수 있습니다.

자동 탐지된 포트

전처리기는 자동으로 SSH 트래픽을 탐지할 수 있습니다.

이 옵션을 선택하면, 전처리기는 SSH 버전 번호에 대한 모든 트래픽을 검사합니다. 이는 클라이언트와 서버 패킷 모두가 버전 번호를 포함하지 않을 때 처리를 중지합니다. 이를 비활성화하면, 전처리기는 **Server Ports(서버 포트)** 옵션에서 확인된 트래픽만 검사합니다.

검사할 암호화된 패킷 수

세션당 검토할 암호화된 패킷 수를 지정합니다.

이 옵션을 0으로 설정하면 모든 트래픽이 통과할 수 있습니다.

검사할 암호화된 패킷 수를 줄이면 일부 공격이 탐지를 이스케이프할 수 있습니다. 검사할 암호화된 패킷 수를 늘리면 성능에 부정적인 영향을 줄 수 있습니다.

서버 응답 없이 전송된 바이트 수

시도 응답 버퍼 오버플로 공격 또는 CRC-32 공격이 있는 것으로 가정하기 전에 SSH 클라이언트가 응답 없이 서버에 보낼 수 있는 최대 바이트 수를 지정합니다.

전처리기가 시도 응답 버퍼 오버플로 또는 CRC-32 익스플로잇에 대해 잘못된 긍정을 생성할 경우 이 옵션의 값이 증가합니다.

프로토콜 버전 문자열의 최대 길이

문자열을 SecureCRT 익스플로잇으로 간주하기 전에 서버의 버전 문자열에 허용할 최대 바이트 수를 지정합니다.

시도 응답 버퍼 오버플로 공격 탐지

시도 응답 버퍼 오버플로 익스플로잇에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:1을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

SSH1 CRC-32 공격 탐지

CRC-32 익스플로잇에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:2를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

서버 오버플로 탐지

SecureCRT SSH 클라이언트 버퍼 오버플로 익스플로잇에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:3을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

프로토콜 불일치 탐지

프로토콜 불일치에 대한 탐지를 활성화 또는 비활성화합니다.

규칙 128:4를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

오류 메시지 방향 탐지

트래픽이 잘못된 방향으로 흐르는 경우(즉, 가정한 서버가 클라이언트 트래픽을 생성하거나, 클라이언트가 서버 트래픽을 생성한 경우) 탐지를 활성화 또는 비활성화합니다.

규칙 128:5을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

지정된 페이로드에 대해 유효하지 않은 페이로드 크기 탐지

SSH 패킷에서 지정한 길이가 IP 헤더에 지정된 총 길이와 일관되지 않고 메시지 끝이 잘렸을 때, 즉, 전체 SSH 헤더에 충분한 데이터가 있지 않은 경우에 유효하지 않은 페이로드 크기를 가진 패킷 탐지를 활성화 또는 비활성화합니다.

규칙 128:6을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

유효하지 않은 버전 문자열 탐지

이를 활성화할 경우, 전처리기가 설정 없이도 버전 1 또는 2 이외의 다른 모든 버전의 문자열을 탐지한다는 점에 유의하십시오.

규칙 128:7을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

SSH 전처리기 구성

라이센스: 보호

이 섹션에서는 SSH 전처리기를 구성하는 방법에 대해 설명합니다.

SSH 전처리기를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 이 변경 사항을 삭제하고 계속합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 데 대한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **SSH Configuration(SSH 구성)**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

SSH Configuration(SSH 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어을 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용를 참고하십시오.

단계 9 SSH Configuration(SSH 구성) 전처리기 페이지에서 옵션을 수정할 수 있습니다. 자세한 내용은 15-70페이지의 SSH 전처리기 옵션 선택을 참고하십시오.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

SSL 전처리기 사용

라이센스: 보호

시스템이 암호화된 트래픽의 콘텐츠를 분석할 수 없더라도, SSL 전처리기 옵션을 설정하여 간헐적으로 잘못된 긍정을 생성하고 탐지 리소스를 낭비하는 트래픽을 계속해서 검사하려고 시도할 수 있습니다. 하지만, SSL 전처리기를 사용하면 시스템이 SSL 세션 시작 시 교환되는 핸드쉐이크 및 키 교환 메시지의 콘텐츠를 분석하여 세션이 암호화되는 경우를 파악할 수 있습니다. SSL 전처리가 활성화되면, 세션이 암호화되는 즉시 시스템의 세션 검사를 중단할 수 있습니다. SSL 전처리기를 사용하려면 반드시 TCP 스트림 전처리가 활성화되어야 합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 15-73페이지의 SSL 전처리 이해
- 15-74페이지의 SSL 전처리기 규칙 활성화
- 15-75페이지의 SSL 전처리기 구성

SSL 전처리 이해

라이센스: 보호

SSL 전처리기는 잘못된 긍정을 제거할 수 있는 암호화된 데이터의 검사를 중지합니다. SSL 전처리기는 SSL 핸드쉐이크를 검사할 때 상태 정보를 유지하며, 해당 세션에 대한 상태 및 SSL 버전을 모두 추적합니다. 세션 상태가 암호화되었음을 전처리기가 탐지하면 시스템은 해당 세션의 트래픽이 암호화되었음을 표시합니다. 암호화가 설정된 경우 암호화된 세션의 모든 패킷 처리를 중지하도록 시스템을 구성할 수 있습니다.

SSL 전처리기는 각 패킷에 대해 트래픽이 IP 헤더, TCP 헤더 및 TCP 페이로드를 포함하며 SSL 전처리를 위해 지정된 포트에서 발생한다는 것을 확인합니다. 다음 시나리오는 트래픽 검증을 위해 트래픽이 암호화되었는지 여부를 확인합니다.

- 시스템은 세션 내 모든 패킷을 관찰하고, **Server side data is trusted(서버 측 데이터가 신뢰됨)** 기능은 활성화되지 않으며, 서버와 클라이언트 모두로부터 수신된 완료됨 메시지와 애플리케이션 레코드가 있지만 경고 레코드는 없는 각 측면으로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.
- 시스템은 트래픽 일부를 유실하고, **Server side data is trusted(서버 측 데이터가 신뢰됨)** 기능은 활성화되지 않으며, 경고 레코드로 응답되지 않은 애플리케이션 레코드를 가진 각 측면으로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.
- 시스템은 세션 내 모든 패킷을 관찰하고, **Server side data is trusted(서버 측 데이터가 신뢰됨)** 기능이 활성화되며, 클라이언트로부터 수신된 완료됨 메시지 및 애플리케이션 레코드가 있지만 경고 레코드는 없는 각 클라이언트로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.
- 시스템은 트래픽 일부를 유실하고, **Server side data is trusted(서버 측 데이터가 신뢰됨)** 기능이 활성화되며, 경고 레코드로 응답되지 않은 애플리케이션 레코드를 가진 각 클라이언트로부터 수신된 최소 하나의 패킷이 세션에 포함됩니다.

암호화된 트래픽 처리를 중단하도록 선택할 경우, 시스템은 세션이 암호화된 것으로 표시한 후에는 세션의 이후 패킷을 무시합니다.

참고 `ssl_state` 및 `ssl_version` 키워드를 규칙에 추가하여 SSL 상태 또는 버전 정보를 규칙과 함께 사용할 수 있습니다. 자세한 내용은 23-54페이지의 세션에서 SSL 정보 추출을 참고하십시오.

SSL 전처리기 규칙 활성화

라이센스: 보호

SSL 전처리기 규칙을 활성화면 전처리기는 SSL 세션 시작 시 교환되는 핸드쉐이크 및 키 교환 메시지 콘텐츠를 검사합니다.

137의 생성기 ID(GID)가 있는 SSH 전처리기 규칙에서 이벤트를 생성하려는 경우, 이 규칙을 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

다음 표는 사용자가 활성화할 수 있는 SSL 전처리기 규칙에 대해 설명합니다.

표 15-14 SSL 전처리기 규칙

전처리기 규칙 GID:SID	설명
137:1	서버 Hello 메시지 후에 나타나는 클라이언트 Hello 메시지를 탐지합니다. 이는 유효하지 않으며 이상 작업으로 간주됩니다.
137:2	**Server side data is trusted(서버 측 데이터가 신뢰됨)** 기능이 비활성화되면 클라이언트 Hello 없는 서버 Hello를 탐지합니다. 이는 유효하지 않으며 이상 작업으로 간주됩니다. 자세한 내용은 15-75페이지의 SSL 전처리기 구성을 참고하십시오.

SSL 전처리기 구성

라이센스: 보호

기본적으로, 시스템은 암호화된 트래픽을 검사하려고 시도합니다. SSL 전처리기를 활성화하면, 세션이 암호화되는 경우를 탐지합니다. SSL 전처리기를 활성화한 후, 규칙 엔진은 전처리기를 호출하여 SSL 상태 및 버전 정보를 얻을 수 있습니다. 침입 정책에서 `ssl_statessl_state` 및 `ssl_version` 키워드를 사용하여 규칙을 활성화하는 경우, 해당 정책에서 SSL 전처리기도 활성화해야 합니다.

또한, **Stop inspecting encrypted traffic(암호화된 트래픽 검사 중지)** 옵션을 활성화하여 암호화된 세션에 대한 검사와 리어셈블리를 비활성화할 수 있습니다. SSL 전처리기가 이 세션에 대한 상태를 유지하므로 세션의 모든 트래픽의 검사를 비활성화할 수 있습니다. SSL 전처리기를 활성화하고 **Stop inspecting encrypted traffic(암호화된 트래픽 검사 중지)** 옵션을 선택한 경우 시스템은 암호화된 세션의 트래픽 검사만 중지합니다.

서버 트래픽에만 암호화된 트래픽의 ID를 기반으로 하려면 **Server side data is trusted(서버 측 데이터가 신뢰됨)** 옵션을 활성화할 수 있습니다. 즉, 트래픽이 암호화되었음을 나타내기 위해 서버 측 데이터가 신뢰됩니다. 세션이 암호화되어 있는지 확인하기 위해 SSL 전처리기는 일반적으로 클라이언트 트래픽 및 해당 트래픽에 대한 서버 응답 모두를 검사합니다. 하지만 세션의 양쪽 모두를 탐지할 수 없는 경우 시스템이 암호화된 대로 트랜잭션을 표시하지 않을 수 있으므로, SSL 서버를 이용하여 세션이 암호화되었음을 나타낼 수 있습니다. **Server side data is trusted(서버 측 데이터가 신뢰됨)** 옵션을 활성화하는 경우 **Stop inspecting encrypted traffic(암호화된 트래픽 검사 중지)** 옵션 또한 활성화해야 한다는 점에 유의하십시오. 그렇지 않으면 시스템이 암호화된 세션의 트래픽 검사를 계속 진행합니다.

전처리기가 암호화된 세션에 대한 트래픽을 모니터링하는 포트를 지정할 수 있습니다.

참고 SSL 전처리기가 SSL 모니터링을 위해 지정된 포트를 통해 비 SSL 트래픽을 탐지하는 경우, 해당 트래픽을 SSL 트래픽으로 디코딩하려고 시도한 다음 이를 손상된 것으로 표시합니다.

SSL 전처리기를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘()(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Application Layer Preprocessors(애플리케이션 레이어 전처리기)에서 **SSL Configuration(SSL 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

SSL Configuration(SSL 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 SSL 전처리기가 암호화된 세션의 트래픽을 모니터링할 포트를 쉼표로 구분하여 입력합니다. **Ports(포트)** 필드에 포함된 포트만 암호화된 트래픽에 대해 검사됩니다.

단계 10 세션이 암호화된 것으로 표시되면 **Stop inspecting encrypted traffic(암호화된 트래픽 검사 중지)** 확인 상자를 클릭하여 세션의 트래픽에 대한 검사를 활성화하거나 비활성화합니다.

단계 11 **Server side data is trusted(서버 측 데이터가 신뢰됨)** 확인 상자를 클릭하여 클라이언트 측 트래픽에만 기반하는 암호화된 트래픽의 ID를 활성화하거나 비활성화합니다.

단계 12 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

SCADA 전처리 구성

네트워크 분석 정책에서 SCADA(Supervisory Control and Data Acquisition System) 전처리기를 구성하는데, 이는 침입 정책에서 활성화된 규칙을 사용하여 트래픽이 검사될 수 있도록 준비합니다. 자세한 내용은 11-1페이지의 네트워크 분석 및 침입 정책의 이해를 참고하십시오.

SCADA 프로토콜은 제조, 생산, 정수 처리, 배전, 공항 및 배송 시스템 등과 같은 산업, 인프라 및 설비의 데이터를 모니터링하고, 제어하며, 획득합니다. ASA FirePOWER 모듈은 네트워크 분석 정책의 일부로 구성할 수 있는 Modbus 및 DNP3 SCADA 프로토콜을 위한 전처리기를 제공합니다.

해당 침입 정책에서 Modbus 또는 DNP3 키워드를 포함하는 규칙을 활성화하는 경우, 전처리기는 네트워크 분석 정책 모듈 인터페이스에서 비활성화되어 있는 상태로 남아 있지만, 시스템은 현재의 구성과 함께 각각 Modbus 또는 DNP3 프로세서를 자동으로 사용합니다. 자세한 내용은 23-73페이지의 Modbus 키워드 및 23-75페이지의 DNP3 키워드를 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

Modbus 전처리기 구성

라이센스: 보호

Modbus 프로토콜은 1979년 Modicon에 의해 처음 게시되어 널리 사용되는 SCADA 프로토콜입니다. Modbus 전처리기는 Modbus 트래픽 내 이상 징후를 탐지하고 규칙 엔진에 의한 처리를 위해 Modbus 프로토콜을 디코딩하는데, 특정 프로토콜 필드에 액세스하기 위해 Modbus 키워드를 사용합니다. 자세한 내용은 23-73페이지의 Modbus 키워드를 참고하십시오.

단일 구성 옵션을 사용하면 전처리기가 Modbus 트래픽을 검사할 포트에 대한 기본 설정을 변경할 수 있습니다.

이러한 규칙에서 이벤트를 생성하려는 경우 다음 표에서 Modbus 전처리기 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오

표 16-1 Modbus 전처리기 규칙

전처리기 규칙 GID:SID	설명
144:1	Modbus 헤더 내 길이가 Modbus 기능 코드가 요청하는 길이에 일치하지 않을 경우 이벤트를 생성합니다. 각 Modbus 기능에는 요청과 응답에 대한 예상된 형식이 있습니다. 메시지 길이가 예상된 형식과 일치하지 않는 경우 이 이벤트가 생성됩니다.
144:2	Modbus 프로토콜 ID가 0이 아닐 때 이벤트를 생성합니다. 프로토콜 ID 필드는 Modbus로 다른 프로토콜을 다중화하는 데 사용됩니다. 전처리기가 다른 프로토콜을 처리하지 않으므로, 이 이벤트가 대신 생성됩니다.
144:3	전처리기가 예약된 Modbus 기능 코드를 탐지하면 이벤트를 생성합니다.

Modbus 전처리기 사용과 관련하여, Modbus가 활성화된 디바이스가 네트워크에 포함되지 않는 경우 트래픽에 적용한 네트워크 분석 정책에서 이 전처리기를 활성화하지 않아야 한다는 점에 유의하십시오.

다음 절차를 사용하여 Modbus 전처리기가 모니터링하는 포트를 변경할 수 있습니다.

Modbus 전처리기를 설정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 **SCADA Preprocessors(SCADA 전처리기)**에서 **Modbus Configuration(Modbus 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Modbus Configuration(Modbus 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 또는, 전처리기가 Modbus 트래픽을 검사하는 **Ports(포트)**를 변경합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 여러 포트를 구분하려면 쉼표를 사용하십시오.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

DNP3 전처리기 구성

라이센스: 보호

Distributed Network Protocol(DNP3)는 원래 전력발전소 간 일관된 커뮤니케이션을 제공하기 위해 개발된 SCADA 프로토콜입니다. DNP3는 또한 상수도산업, 산업 폐기물 처리업, 운송 산업 및 많은 기타 업계에서 널리 사용되고 있습니다.

DNP3 전처리기는 DNP3 트래픽 내 이상 징후를 탐지하고 규칙 엔진에 의한 처리를 위해 DNP3 프로토콜을 디코딩하는데, 특정 프로토콜 필드에 액세스하기 위해 DNP3 키워드를 사용합니다. 자세한 내용은 23-75페이지의 DNP3 키워드를 참고하십시오.

이러한 규칙에서 이벤트를 생성하려는 경우 다음 표에서 DNP3 전처리기 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

표 16-2 DNP3 전처리기 규칙

전처리기 규칙 GID:SID	설명
145:1	**Log bad CRC(잘못된 CRC 로깅)**를 활성화한 경우 전처리기가 유효하지 않은 체크섬을 통해 연결 레이어 프레임을 탐지하면 이벤트를 생성합니다.
145:2	전처리기가 유효하지 않은 길이로 DNP3 연결 레이어 프레임을 탐지하면 이벤트를 생성하고 패킷을 차단합니다.
145:3	전처리기가 유효하지 않은 시퀀스 번호로 전송 레이어 세그먼트를 탐지하면 이벤트를 생성하고 리어셈블리 중에 패킷을 차단합니다.
145:4	완전한 조각이 리어셈블되기 전에 DNP3 리어셈블리 버퍼가 지워지면 이벤트를 생성합니다. 이는 다른 세그먼트가 대기된 후 FIR 플래그를 전송하는 세그먼트가 나타날 때 발생합니다.
145:5	전처리기가 예약된 주소를 사용하는 DNP3 연결 레이어 프레임을 탐지하면 이벤트를 생성합니다.
145:6	전처리기가 예약된 기능 코드를 사용하는 DNP3 요청 또는 응답을 탐지하면 이벤트를 생성합니다.

DNP3 전처리기 사용과 관련하여, DNP3가 활성화된 디바이스가 네트워크에 포함되지 않는 경우 트래픽에 적용한 네트워크 분석 정책에서 이 전처리기를 활성화하지 않아야 한다는 점에 유의하십시오. 자세한 내용은 17-29페이지의 TCP 스트림 전처리 구성을 참고하십시오.

다음 목록은 사용자가 구성할 수 있는 DNP3 전처리기 옵션에 대해 설명합니다.

포트

각 지정된 포트의 DNP3 트래픽 검사를 활성화합니다. 단일 포트 또는 쉼표로 구분된 포트 목록을 지정할 수 있습니다. 각 포트에 대해 0에서 65535 사이의 값을 지정할 수 있습니다.

잘못된 CRC 로깅

이를 활성화할 경우, DNP3 연결 레이어 프레임에 포함된 체크섬을 인증합니다. 유효하지 않은 체크섬을 가진 프레임은 무시됩니다.

규칙 145:1을 활성화하여 유효하지 않은 체크섬이 탐지된 경우 이벤트를 생성할 수 있습니다.

DNP3 전처리기를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 **SCADA Preprocessors(SCADA 전처리기)**에서 **DNP3 Configuration(DNP3 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

DNP3 Configuration(DNP3 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 또는, 전처리기가 DNP3 트래픽을 검사하는 **Ports(포트)**를 변경합니다. 0부터 65535까지의 정수를 지정할 수 있습니다. 여러 포트를 구분하려면 쉼표를 사용하십시오.

단계 10 또는, **Log bad CRCs(잘못된 CRC 로깅)** 확인 상자를 선택하거나 비워 두어 DNP3 연결 레이어 프레임에 포함된 체크섬을 검증할지 여부 및 유효하지 않은 체크섬을 가진 프레임을 무시할지 여부를 지정합니다.

단계 11 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 네트워크 분석 정책 수정 작업 표를 참고하십시오.

전송 및 네트워크 레이어 전처리 구성

네트워크 분석 정책에서 네트워크 레이어 전처리기의 대부분의 전송을 구성하는데, 이는 침입 정책에서 활성화된 규칙을 사용하여 트래픽이 검사될 수 있도록 준비합니다. 자세한 내용은 11-1페이지의 네트워크 분석 및 침입 정책의 이해를 참고하십시오.

전송 및 네트워크 레이어 전처리기는 IP 조각을 이용한 공격을 탐지하고 체크섬 유효성 검증을 수행하며, TCP와 UDP 세션 전처리를 수행합니다. 패킷이 전처리기로 전달되기 전에, 패킷 디코더는 전처리기 및 침입 규칙 엔진에서 쉽게 사용할 수 있는 형식으로 패킷 헤더와 페이로드를 변환하고 패킷 헤더에서 다양한 이상 작업을 탐지합니다. 패킷을 디코딩한 후 다른 전처리기에 전송하기 전에 인라인 표준화 전처리기는 인라인 배포를 위해 트래픽을 표준화합니다.

네트워크 분석 정책에서 영역 또는 네트워크로 구성하는 전송 및 네트워크 레이어 전처리기 설정을 조정할 수 있습니다. 일부 전송 및 네트워크 레이어 설정은 모든 트래픽에 전역으로 적용되며 이들을 액세스 제어 정책에서 구성할 수 있습니다.

고급 전송/네트워크 설정 구성

라이센스: 보호

고급 전송 및 네트워크 전처리기 설정은 액세스 제어 정책을 적용하는 모든 네트워크와 영역에 전역으로 적용됩니다. 네트워크 분석 정책이 아닌 액세스 제어 정책에서 이 고급 설정을 구성합니다.

다음 섹션에서는 이러한 설정에 대해 설명합니다.

침입 드롭 규칙으로 활성 응답 시작

라이센스: 보호

드롭 규칙은 규칙 상태가 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 침입 규칙 또는 전처리기 규칙입니다. 인라인 배포에서 시스템은 트리거 패킷을 삭제하고 패킷이 시작된 세션을 차단하여 TCP 또는 UDP 드롭 규칙에 응답합니다. 수동 배포에서 시스템은 패킷을 삭제할 수 없고, 활성 응답의 사용을 제외하고는 세션을 차단하지 않습니다.

팁 UDP 데이터 스트림은 일반적으로 *세션*의 측면에서 평가되지 않으므로, 스트림 전처리기가 흐름의 방향을 결정하고 UDP 세션을 식별하기 위해 캡슐화하는 IP 데이터그램 헤더 내 소스 및 대상 IP 주소 필드와 UDP 헤더 내 포트 필드를 사용하는 방식에 대한 자세한 설명은 17-32페이지의 UDP 스트림 전처리 사용을 참고하십시오.

Maximum Active Responses(최대 활성 응답) 옵션을 구성하여 문제를 일으키는 패킷이 TCP 또는 UDP 드롭 규칙을 트리거할 때 TCP 연결 또는 UDP 세션이 더욱 정확하고 분명하게 닫히도록 하나 이상의 *활성 응답*을 시작할 수 있습니다.

활성 응답이 인라인 배포에서 활성화될 경우, 시스템은 트리거 패킷을 삭제하고 클라이언트와 서버 트래픽 모두에 TCP 재설정(RST) 패킷을 삽입하여 TCP 드롭 규칙에 응답합니다. 시스템은 수동 배포에서 패킷을 삭제할 수 없습니다. 활성 응답이 수동 배포에서 활성화되면, 시스템은 TCP 연결의 클라이언트와 서버 끝 모두에 TCP 재설정을 전송하여 TCP 드롭 규칙에 응답합니다. 활성 응답이 인라인 또는 수동 배포에서 활성화될 경우, 시스템은 ICMP에 도달할 수 없는 패킷을 세션의 양쪽 끝에 보내 UDP 세션을 닫습니다. 재설정이 연결 또는 세션에 영향을 줄 수 있는 시간에 맞게 도착할 가능성이 크기 때문에 활성 응답은 인라인 배포에서 가장 효과적입니다.

Maximum Active Responses(최대 활성 응답) 옵션을 구성하는 방식에 따라 시스템이 연결 또는 세션의 한쪽 끝에서 전송되는 추가 트래픽을 발견하는 경우 추가 활성 응답을 시작할 수도 있습니다. 시스템은 이전 응답으로부터 지정된 시간(단위: 초)이 경과한 후, 지정된 최대 수까지 각 추가 활성 응답을 시작합니다.

활성 응답의 최대 수 설정에 대한 내용은 17-21페이지의 TCP 전역 옵션 선택을 참고하십시오.

트리거된 **응답** 또는 **반응** 규칙이 **Maximum Active Responses(최대 활성 응답)**의 구성에 상관 없이 활성 응답도 시작한다는 점에 유의하십시오. 하지만, **Maximum Active Responses(최대 활성 응답)**는 시스템이 드롭 규칙에 대한 활성 응답의 최대 수를 제어하는 것과 같은 방식으로 **응답** 및 **반응** 규칙에 대한 추가 활성 응답을 시작할지 여부를 제어합니다. 자세한 내용은 23-83페이지의 규칙 키워드로 활성 응답 시작을 참고하십시오.

`config response` 명령을 사용하여 수동 배포에서 시도할 TCP 재설정 수 및 수동 배포에서 사용할 활성 응답 인터페이스를 구성할 수 있습니다. 자세한 내용은 23-86페이지의 활성 응답 재설정 시도 및 인터페이스 설정을 참고하십시오.

어떤 전처리기 규칙도 다음 옵션과 연결되어 있지 않습니다.

최대 활성 응답

TCP 연결당 1개에서 최대 25개의 활성 응답을 지정합니다. 추가 트래픽은 활성 응답이 시작된 연결에서 발생하고, 이전 활성 응답 이후 **Minimum Response Seconds(최소 응답 시간(단위: 초))**보다 트래픽이 더 많이 발생한 경우, 지정된 최대값에 도달하지 않는 한 시스템은 다른 활성 응답을 보냅니다. 0 값을 설정하면 드롭 규칙으로 트리거된 활성 응답이 비활성화되고 **resp** 또는 **react** 규칙으로 트리거된 추가 활성 응답이 비활성화됩니다. 자세한 내용은 17-2페이지의 침입 드롭 규칙으로 활성 응답 시작 및 23-83페이지의 규칙 키워드로 활성 응답 시작을 참고하십시오.

최소 응답 시간(단위: 초)

Maximum Active Responses(최대 활성 응답)가 발생할 때까지 시스템이 이후의 활성 응답 내 활성 응답 결과를 시작한 연결에서 추가 트래픽이 발생하기 전에 1에서 300초의 대기 시간을 지정합니다.

드롭 규칙으로 활성 응답을 시작하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 7 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 8 수정 아이콘( )을 클릭합니다. 이 아이콘은 **Transport/Network Layer Preprocessor Settings(전송/네트워크 레이어 전처리기 설정)** 옆에 있습니다.

Transport/Network Layer Preprocessor Settings(전송/네트워크 레이어 전처리기 설정) 팝업 창이 표시됩니다.

단계 9 다음 옵션을 이용할 수 있습니다.

- TCP 연결당 **Maximum Active Responses(최대 활성 응답)**의 값을 1부터 25까지 지정합니다. 0 값을 설정하면 드롭 규칙으로 트리거된 활성 응답이 비활성화되고 **resp** 또는 **react** 규칙으로 트리거된 추가 활성 응답이 비활성화됩니다.
- **Minimum Response Seconds(최소 응답 시간(단위: 초))** 값을 1부터 300까지 지정하여 **Maximum Active Responses(최대 활성 응답)**가 발생하거나 시스템이 활성 응답을 시작한 연결에서 추가 트래픽이 발생하여 이후의 활성 응답이 나타날 때까지 기다립니다.

단계 10 **OK(확인)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다. 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

문제 해결: 세션 종료 메시지 로깅

라이센스: 보호

Support(지원팀)은 문제 해결 통화 중에 시스템을 구성하여 개별 연결이 지정된 임계값을 초과하면 메시지를 로깅하도록 요청할 수 있습니다. 이 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

세션 종료 메시지를 로깅하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 7 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 8 수정 아이콘( )을 클릭합니다. 이 아이콘은 **Transport/Network Layer Preprocessor Settings(전송/네트워크 레이어 전처리기 설정)** 옆에 있습니다.

Transport/Network Layer Preprocessor Settings(전송/네트워크 레이어 전처리기 설정) 팝업 창이 표시됩니다.

단계 9 **Troubleshooting Options(문제 해결 옵션)**를 확장합니다.

단계 10 세션이 종료되고 지정된 수가 초과된 경우 **Session Termination Logging Threshold(세션 종료 로깅 임계값)**을 로깅된 메시지의 바이트 수로 지정합니다.

1GB의 상한 값은 또한 스트림 처리에 할당된 디바이스의 메모리 양에 의해 제한됩니다.

단계 11 **OK(확인)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다. 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

체크섬 확인

라이센스: 보호

시스템은 프로토콜 수준 체크섬을 모두 검증하여 전체 IP, TCP, UDP 및 ICMP 전송이 수신되고 기본 수준에서 패킷이 전송 중에 함부로 조작되거나 실수로 변경되지 않았는지 확인할 수 있습니다. 체크섬은 알고리즘을 사용하여 패킷 내 프로토콜의 무결성을 확인합니다. 종단 호스트가 패킷 내에 작성한 것과 동일한 값을 시스템이 산출할 경우 패킷은 변경되지 않은 것으로 간주됩니다.

체크섬 확인을 비활성화한 경우 네트워크는 삽입 공격의 영향을 받기 쉽습니다. 시스템은 체크섬 확인 이벤트를 생성하지 않는다는 점에 유의하십시오. 인라인 배포에서 시스템을 구성하여 유효하지 않은 체크섬을 가진 패킷을 삭제할 수 있습니다.

체크섬 확인을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Edit Policy(정책 수정) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Transport/Network Layer Preprocessors(전송/네트워크 레이어 전처리기)에서 **Checksum Verification(체크섬 확인)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Checksum Verification(체크섬 확인) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 수동 또는 인라인 배포에서 Checksum Verification(체크섬 확인) 섹션의 모든 옵션을 **Enabled(활성화)** 또는 **Disabled(비활성화)**, 또는 인라인 배포에서 **Drop(삭제)**으로 설정할 수 있습니다.

- **ICMP 체크섬**
- **IP 체크섬**
- **TCP 체크섬**
- **UDP 체크섬**

문제를 일으키는 패킷을 삭제하려면 옵션을 **Drop(삭제)**으로 설정하고 연결된 네트워크 분석 정책에서 **Inline Mode(인라인 모드)**도 활성화해야 한다는 점에 유의하십시오. 자세한 내용은 14-5페이지의 전처리기의 영향을 받도록 트래픽 설정을 참고하십시오. 또한 이러한 옵션을 수동 배포에서 **Drop(삭제)**으로 설정하는 것은 이들을 **Enabled(활성화)**로 설정하는 것과 동일하다는 점에 유의하십시오.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

인라인 트래픽 표준화

라이센스: 보호

인라인 표준화 전처리기는 인라인 배포에서 공격자가 탐지를 우회하는 가능성을 최소화하기 위해 트래픽을 표준화합니다. 네트워크 분석 정책에서 인라인 표준화 전처리기를 활성화하는 경우, 시스템은 사용자가 인라인 배포를 사용하고 있는지 확인하기 위해 다음 2가지 조건을 테스트합니다.

- 정책 내 **Inline Mode(인라인 모드)**가 활성화되어 있습니다. 14-5페이지의 전처리기의 영향을 받도록 트래픽 설정을 참고하십시오.
- 인라인 표준화가 활성화된 액세스 제어 정책이 인라인으로 구축되어 있는 디바이스에 적용되어 있습니다.

두 조건이 모두 충족되는 경우에만 전처리기가 지정된 트래픽을 표준화합니다.

IPv4, IPv6, ICMPv4, ICMPv6 및 TCP 트래픽의 모든 조합에 대해 표준화를 지정할 수 있습니다. 대부분의 표준화는 패킷별 기반이며 인라인 표준화 전처리기에서 수행됩니다. 그러나, TCP 스트림 전처리기는 TCP 페이로드 표준화를 포함하여 대부분의 상태 관련 패킷 및 스트림 표준화를 처리합니다.

인라인 표준화는 패킷 디코더의 디코딩 직후 및 다른 전처리기의 처리 직전에 발생합니다. 표준화는 패킷 레이어의 내부에서 외부로 진행됩니다.

인라인 표준화 전처리기는 이벤트를 생성하지 않고 인라인 배포에서 다른 전처리기 및 규칙 엔진에 의한 사용을 위해 패킷을 준비합니다. 또한 전처리기를 통해 시스템이 처리하는 패킷이 네트워크 호스트에서 수신된 패킷과 동일한지 확인할 수 있습니다.

팁 인라인 배포의 경우 Cisco는 **Normalize TCP Payload(TCP 페이로드 정규화)** 옵션이 활성화된 인라인 정규화 전처리기를 구성할 것을 권장합니다. Cisco는 수동 배포 시 적응형 프로파일을 구성할 것을 권장합니다. 자세한 내용은 18-1페이지의 수동 배포 시 전처리 조정을 참고하십시오.

최소 TTL

Reset TTL(TTL 재설정)이 이 옵션에 설정된 1~255 값보다 크거나 같을 때 다음을 지정합니다.

- **Normalize IPv4(IPv4 표준화)**를 활성화할 때 시스템에서 IPv4 TTL(Time to Live) 필드에 허용할 최소값. 값이 더 낮은 경우 TTL의 패킷 값이 **Reset TTL(재설정 TTL)**에 설정된 값으로 표준화됩니다.

- **Normalize IPv6(IPv6 표준화)**를 활성화할 때 시스템에서 IPv6 Hop Limit(홉 제한) 필드에 허용할 최소값. 값이 더 낮은 경우 Hop Limit(홉 제한)의 패킷 값이 **Reset TTL(재설정 TTL)**에 설정된 값으로 표준화됩니다.

  필드가 비어 있는 경우 시스템은 값을 1로 가정합니다.

  디코더 규칙 카테고리에서 다음 규칙을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있다는 점을 참고하십시오.

- 규칙 116:428을 활성화하여 시스템이 지정된 최소 값보다 작은 TTL 값이 포함된 IPv4 패킷을 탐지하는 경우 이벤트를 생성할 수 있습니다.
- 규칙 116:270을 활성화하여 시스템이 지정된 최소 값보다 작은 홉 제한 값이 포함된 IPv6 패킷을 탐지하는 경우 이벤트를 생성할 수 있습니다.

  자세한 내용은 패킷 디코더 **Detect Protocol Header Anomalies(프로토콜 헤더 이상 징후 탐지)** 옵션을 참고하십시오. 이 옵션은 17-19페이지의 패킷 디코딩 구성에서 확인할 수 있습니다.

TTL 재설정

Minimum TTL(최소 TTL)보다 크거나 같은 1~255 값을 설정할 때, 다음을 표준화합니다.

- **Normalize IPv4(IPv4 표준화)**를 활성화하는 경우 IPv4 TTL 필드
- **Normalize IPv6(IPv6 표준화)**를 활성화하는 경우 IPv6 Hop Limit(홉 제한) 필드

패킷 값이 **Minimum TTL(최소 TTL)**보다 작을 때 시스템은 해당 TTL 또는 Hop Limit(홉 제한) 값을 이 옵션에 설정된 값으로 변경하여 패킷을 표준화합니다. 이 옵션을 0 값 또는 **Minimum TTL(최소 TTL)**보다 작은 값으로 설정하면 옵션이 비활성화됩니다. 필드가 비어 있는 경우 시스템은 값을 0으로 가정합니다.

IPv4 표준화

IPv4 트래픽의 표준화를 활성화합니다. 이 옵션이 활성화되고 **Reset TTL(TTL 재설정)**에 설정된 값이 TTL 표준화를 활성화하는 경우 시스템에서도 필요에 따라 TTL 필드를 표준화합니다. 이 옵션이 활성화되면 **Normalize Don't Fragment Bits(조각화 금지 비트 표준화)** 및 **Normalize Reserved Bits(예약 비트 표준화)** 또한 활성화할 수 있습니다.

이 옵션을 활성화하면, 시스템은 다음 기본 IPv4 표준화를 수행합니다.

- 과도한 페이로드를 가진 패킷을 IP 헤더에 지정된 데이터그램 길이로 줄입니다.
- 예전에는 Type of Service(서비스 유형, ToS)로 알려졌던 Differentiated Services(차별화된 서비스, DS) 필드의 내용을 지웁니다.
- 모든 옵션 옥텟을 1(무연산)로 설정합니다.

조각화 금지 비트 표준화

IPv4 Flags(플래그) 헤더 필드의 단일 비트 Don't Fragment(조각화 금지) 하위 필드의 내용을 지웁니다. 이 옵션을 활성화하면 필요한 경우 다운스트림 라우터가 패킷을 삭제하는 대신 조각화할 수 있습니다. 또한 삭제할 조작된 패킷에 기반하여 회피를 방지할 수 있습니다. 이 옵션을 선택하려면 **Normalize IPv4(IPv4 표준화)**를 활성화해야 합니다.

예약 비트 표준화

IPv4 Flags(플래그) 헤더 필드의 단일 비트 Reserved(예약) 하위 필드의 내용을 지웁니다. 일반적으로 이 옵션을 활성화합니다. 이 옵션을 선택하려면 **Normalize IPv4(IPv4 표준화)**를 활성화해야 합니다.

TOS 비트 표준화

예전에는 Type of Service(서비스 유형, ToS)로 알려졌던 1 바이트 Differentiated Services(차별화된 서비스, DS) 필드의 내용을 지웁니다. 이 옵션을 선택하려면 **Normalize IPv4(IPv4 표준화)**를 활성화해야 합니다.

초과 페이로드 표준화

페이로드가 과도한 패킷을 IP 헤더 및 Layer(레이어) 2(예를 들어, Ethernet(이더넷)) 헤더에 지정된 데이터그램 길이로 줄이지만 최소 프레임 길이 이하로 줄이지는 않습니다. 이 옵션을 선택하려면 **Normalize IPv4(IPv4 표준화)**를 활성화해야 합니다.

IPv6 표준화

Hop-by-Hop Options(홉 바이 홉 옵션) 및 Destination Options(대상 옵션) 확장 헤더의 모든 Option Type(옵션 유형) 필드를 00(건너뛰기 및 처리 계속)으로 설정합니다. 이 옵션이 활성화되고 **Reset TTL(TTL 재설정)**에 설정된 값이 홉 제한 표준화를 활성화하는 경우 시스템에서도 필요에 따라 Hop Limit(홉 제한) 필드를 표준화합니다.

ICMPv4 표준화

ICMPv4 트래픽 내 Echo(Request)(에코(요청)) 및 Echo Reply(에코 응답) 메시지에서 8비트 Code(코드) 필드의 내용을 지웁니다.

ICMPv6 표준화

ICMPv6 트래픽 내 Echo(Request)(에코(요청)) 및 Echo Reply(에코 응답) 메시지에서 8비트 Code(코드) 필드의 내용을 지웁니다.

예약 비트 표준화/지우기

TCP 헤더에 있는 Reserved(예약) 비트를 지웁니다.

옵션 패딩 바이트 표준화/지우기

모든 TCP 옵션 패딩 바이트를 지웁니다.

URG=0인 경우 긴급 포인터 지우기

긴급(URG) 제어 비트가 설정되지 않은 경우 16비트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드의 내용을 지웁니다.

빈 페이로드의 긴급 포인터/URG 지우기

페이로드가 없는 경우 TCP 헤더 Urgent Pointer(긴급 포인터) 필드의 내용 및 URG 제어 비트를 비웁니다.

긴급 포인터가 설정되지 않은 경우 URG 지우기

긴급 포인터가 설정되지 않은 경우 TCP 헤더 URG 제어 비트를 지웁니다.

긴급 포인터 표준화

포인터가 페이로드 길이보다 긴 경우 2바이트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드를 페이로드 길이로 설정합니다.

TCP 페이로드 표준화

TCP Data(데이터) 필드의 표준화를 활성화하여 재전송된 데이터의 일관성을 유지합니다. 제대로 리어셈블될 수 없는 모든 세그먼트는 삭제됩니다.

SYN 데이터 제거

TCP 운영 체제 정책이 Mac OS가 **아닌** 경우 동기화(SYN) 패킷의 데이터를 제거합니다.

이 옵션은 또한 규칙 129:2의 이벤트 생성을 비활성화합니다.

RST 데이터 제거

TCP 재설정(RST) 패킷에서 모든 데이터를 제거합니다.

Window로 데이터 절감

TCP Data(데이터) 필드를 Window 필드에 지정된 크기로 줄입니다.

MSS로 데이터 절감

페이로드가 Maximum Segment Size(최대 세그먼트 크기, MSS)보다 긴 경우 TCP Data(데이터) 필드를 MSS로 줄입니다.

복구 불능 TCP 헤더 이상 징후 차단

이 옵션을 활성화하면 표준화된 경우 시스템은 유효하지 않고 수신 호스트가 차단할 가능성이 높은 변칙적 TCP 패킷을 차단합니다. 예를 들어, 시스템은 설정된 세션에 차후에 전송된 모든 SYN 패킷을 차단합니다.

시스템은 또한 규칙이 활성화되어 있는지 여부에 관계없이 다음 TCP 스트림 전처리기 규칙에 하나라도 일치하는 모든 패킷을 삭제합니다.

- 129:1
- 129:3
- 129:4
- 129:6
- 129:8
- 129:11
- 129:14~129:19

Total Blocked Packets(전체 차단된 패킷) 성능 표는 인라인 배포와 수동 배포에서 차단된 패킷 수 및 인라인 배포에서 차단되었을 수도 있는 수를 추적합니다.

명시적 정체 알림

Explicit Congestion Notification(명시적 정체 알림, ECN) 플래그의 패킷별 또는 스트림별 표준화를 다음과 같이 활성화합니다.

- 협상에 관계없이 패킷별로 ECN 플래그를 지우려면 **Packet(패킷)**을 선택합니다
- ECN 사용이 협상되지 않은 경우 스트림별로 ECN 플래그를 지우려면 **Stream(스트림)**을 선택합니다

Stream(스트림)을 선택한 경우, 이 표준화가 실행되기 위해서는 반드시 TCP 스트림 전처리기 **Require TCP 3-Way Handshake(TCP 3방향 핸드셰이크 요청)** 옵션을 활성화해야 합니다. 자세한 내용은 17-23페이지의 TCP 정책 옵션 선택을 참고하십시오.

이러한 TCP 옵션 허용

사용자가 트래픽에서 허용하는 특정 TCP 옵션의 표준화를 비활성화합니다.

시스템은 사용자가 명시적으로 허용하는 옵션을 표준화하지 않습니다. 이는 옵션을 No Operation(무연산, TCP 옵션 1)으로 설정함으로써 사용자가 명시적으로 허용하지 않는 옵션을 표준화합니다.

시스템은 Maximum Segment Size(최대 세그먼트 크기, MSS), Window Scale(Window 크기), Time Stamp(타임 스탬프) TCP 옵션을 항상 허용하는데, 이러한 옵션은 주로 최적의 TCP 성능을 위해 사용되기 때문입니다. 시스템은 **Allow These TCP Options(이러한 TCP 옵션 허용)**의 구성에 관계없이 주로 사용되는 이러한 옵션을 표준화합니다. 시스템은 드물게 사용되는 다른 옵션은 자동으로 허용하지 않습니다.

다음의 예시에서처럼 옵션 키워드, 옵션 번호, 또는 둘 다로 이루어진 쉼표로 구분된 목록을 작성하여 특정 옵션을 허용할 수 있습니다.

```
sack, echo, 19
```

옵션 키워드를 지정하는 것은 키워드와 관련된 하나 이상의 TCP 옵션을 지정하는 것과 같습니다. 예를 들어, `sack`를 지정하는 것은 TCP 옵션 4(Selective Acknowledgment Permitted(허용된 선택적 수신 확인)) 및 5(Selective Acknowledgment(선택적 수신 확인))를 지정하는 것과 같습니다. 옵션 키워드는 대소문자를 구분하지 않습니다.

또한 모든 TCP 옵션을 허용하고 모든 TCP 옵션의 표준화를 효과적으로 비활성화하는 `any`를 지정할 수 있습니다.

다음 표는 허용할 TCP 옵션을 지정하는 방법에 대해 요약합니다. 필드를 비워 둘 경우, 시스템은 MSS, Window Scale(Window 크기), Time Stamp(타임 스탬프) 옵션만 허용합니다.

지정 대상	허용 대상
sack	TCP 옵션 4(Selective Acknowledgment Permitted(허용된 선택적 수신 확인)) 및 5(Selective Acknowledgment(선택적 수신 확인))
echo	TCP 옵션 6(Echo Request(에코 요청)) 및 7(Echo Reply(에코 응답))
partial_order	TCP 옵션 9(Partial Order Connection Permitted(허용된 부분 순서 연결)) 및 10(Partial Order Service Profile(부분 순서 서비스 프로파일))
conn_count	TCP Connection Count(연결 집계) 옵션 11(CC), 12(CC.New(새로운)), 그리고 13(CC.Echo(에코))
alt_checksum	TCP 옵션 14(Alternate Checksum Request(대체 체크섬 요청)) 및 15(Alternate Checksum(대체 체크섬))
md5	TCP 옵션 19(MD5 서명)
옵션 번호. 2~255.	키워드가 없는 옵션을 비롯한 특정 옵션
any	모든 TCP 옵션. 이 설정은 TCP 옵션 표준화를 효과적으로 비활성화합니다

이 옵션에 `any`를 지정하지 않은 경우, 표준화에는 다음이 포함됩니다.

- MSS, Window Scale(Window 크기), Time Stamp(타임 스탬프) 및 모든 명시적으로 허용된 옵션을 제외하고, 모든 옵션 바이트를 No Operation(무연산, TCP 옵션 1)으로 설정합니다.
- Time Stamp(타임 스탬프)가 존재하지만 유효하지 않은 경우, 또는 유효하지만 협상되지 않은 경우, Time Stamp(타임 스탬프) 옥텟을 No Operation(무연산)으로 설정합니다.
- Time Stamp(타임 스탬프)가 협상되었지만 존재하지 않는 경우 패킷을 차단합니다.
- Acknowledgment(수신 확인, ACK) 제어 비트가 설정되지 않은 경우 Time Stamp Echo Reply(타임 스탬프 에코 응답, TSecr) 옵션 필드를 비웁니다.
- SYN 제어 비트가 설정되지 않은 경우 MSS 및 Window Scale(Window 크기) 옵션을 No Operation(무연산, TCP 옵션 1)으로 설정합니다

인라인 표준화 전처리기를 설정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Edit Policy(정책 수정) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Transport/Network Layer Preprocessors(전송/네트워크 레이어 전처리기)에서 **Inline Normalization(인라인 표준화)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Inline Normalization(인라인 표준화) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 17-6페이지의 인라인 트래픽 표준화에 설명된 옵션을 설정할 수 있습니다.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

IP 패킷 조각 모음

라이센스: 보호

IP 데이터그램이 최대 전송 단위(MTU)보다 커서 2개 이상의 소규모 IP 데이터그램으로 쪼개진 경우 *조각화*됩니다. 단일 IP 데이터그램 조각에는 숨겨진 공격을 식별하기에 충분한 정보가 포함되어 있지 않을 수 있습니다. 공격자는 조각화된 패킷 내에 공격 데이터를 전송하여 탐지 우회를 시도할 수 있습니다. IP 조각 모음 전처리기는 규칙 엔진이 조각화된 IP 데이터그램에 대해 규칙을 실행하기 전에 이를 리어셈블하므로 규칙이 해당 패킷에서 공격을 더욱 적절히 식별할 수 있습니다. 조각화된 데이터그램이 리어셈블되지 않는 경우 데이터그램에 대해 규칙이 실행되지 않습니다.

123의 생성기 ID(GID)가 있는 IP 조각 모음 전처리기 규칙에서 이벤트를 생성하려는 경우, 이 규칙을 활성화해야 한다는 점에 유의하십시오. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 17-12페이지의 IP 조각화 익스플로잇 이해
- 17-13페이지의 대상 기반 조각 모음 정책
- 17-13페이지의 조각 모음 옵션 선택
- 17-15페이지의 IP 조각 모음 구성

IP 조각화 익스플로잇 이해

라이센스: 보호

IP 조각 모음을 활성화하면 티어드롭 공격과 같은 네트워크 호스트에 대한 공격 및 Jolt2 공격과 같은 시스템 자체에 대한 리소스 소모 공격을 탐지할 수 있습니다.

티어드롭 공격은 특정 운영 체제에서 버그를 공격하는데, 중첩되는 IP 조각을 리어셈블하려고 시도할 때 충돌을 야기합니다. IP 조각 모음 전처리기가 중첩되는 조각을 식별하도록 활성화 및 구성된 경우 이를 수행합니다. IP 조각 모음 전처리기는 티어드롭과 같은 중첩되는 조각화 공격의 첫 번째 패킷을 탐지하지만 동일한 공격의 후속 패킷은 탐지하지 않습니다.

Jolt2 공격은 IP 조각 모음기를 혹사시키기 위한 시도로 동일한 조각화된 IP 패킷을 엄청난 수로 복제하여 전송해서 서비스 거부 공격을 야기합니다. 메모리 사용량 한도는 IP 조각 모음 전처리기에서 이것 및 이와 유사한 공격을 차단하고, 철저한 검사를 기반으로 시스템 자체 보호를 유지합니다. 시스템은 공격에 의해 마비되지 않고 운영 상태를 유지하며 계속해서 네트워크 트래픽을 검사합니다.

다양한 운영 체제는 조각화된 패킷을 다양한 방법으로 리어셈블합니다. 호스트가 실행 중인 운영 체제를 결정할 수 있는 공격자는 또한 악성 패킷을 조각화하여 대상 호스트가 특정 방식으로 이를 리어셈블하도록 할 수 있습니다.제 모니터링한 네트워크 상의 호스트가 어떤 운영 체제를 실행 중인지 시스템에서 알 수 없기 때문에 전처리기가 패킷을 부정확하게 검사하고 리어셈블할 수 있으므로 익스플로잇이 탐지되지 않고 통과될 수 있습니다. 이러한 유형의 공격을 줄이기 위해 조각 모음 전처리기를 네트워크의 각 호스트에 대한 패킷을 조각 모음하는 적절한 방법을 사용하도록 구성할 수 있습니다. 자세한 내용은 17-13페이지의 대상 기반 조각 모음 정책을 참고하십시오.

또한 적응형 프로파일을 사용하여 패킷의 대상 호스트에 대한 호스트 운영 체제 정보를 통해 IP 조각 모음 전처리기의 대상 기반 정책을 동적으로 선택할 수도 있다는 점에 유의하십시오. 자세한 내용은 18-1페이지의 수동 배포 시 전처리 조정을 참고하십시오.

대상 기반 조각 모음 정책

라이센스: 보호

호스트의 운영 체제는 패킷을 리어셈블할 때 지원할 패킷 조각을 결정하는 세 가지 기준인, 조각이 운영 체제에서 수신되는 순서, 해당 조각의 오프셋(패킷의 시작 부분으로부터 조각의 거리(단위: 바이트)), 그리고 중첩 조각과 비교했을 때 해당 조각의 시작 및 종료 위치를 사용합니다. 모든 운영 체제가 이러한 기준을 사용하지만, 조각화된 패킷을 리어셈블할 때 서로 다른 운영 체제는 서로 다른 조각을 지원합니다. 따라서, 네트워크에서 서로 다른 운영 체제를 사용 중인 두 호스트는 중첩되는 동일한 조각을 완전히 다른 방법으로 리어셈블할 수 있습니다.

사용 중인 호스트 중 하나의 운영 체제를 알고 있는 공격자는 중첩되는 패킷 조각에 숨겨진 악성 콘텐츠를 전송하여 탐지 우회를 시도하고 해당 호스트를 공격할 수 있습니다. 이 패킷은 리어셈블되고 검사될 때는 무해하게 보일 수 있지만 대상 호스트에 의해 리어셈블될 경우에는 악성 익스플로잇이 포함됩니다. 그러나, 모니터링된 네트워크 세그먼트에서 실행되는 운영 체제를 식별하기 위해 IP 조각 모음 전처리기를 구성한 경우, 이는 대상 호스트가 하는 것과 동일한 방법으로 조각을 리어셈블하여 공격을 식별할 수 있습니다.

대상 호스트의 운영 체제에 따라 7개의 조각 모음 정책 중 하나를 사용하는 IP 조각 모음 전처리기를 구성할 수 있습니다. 다음 표는 7개의 정책 및 각각을 사용하는 운영 체제를 나열합니다. First 및 Last 정책 이름은 해당 정책이 원래의 중첩 패킷을 지원하는지, 아니면 후속 중첩 패킷을 지원하는지 여부를 반영합니다.

표 17-1 대상 기반 조각 모음 정책

정책	운영 체제
BSD	AIX
	FreeBSD
	IRIX
	VAX/VMS
BSD-right	HP JetDirect
First	Mac OS
	HP-UX
Linux	Linux
	OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

조각 모음 옵션 선택

라이센스: 보호

단순히 IP 조각 모음을 활성화하거나 비활성화하도록 선택할 수도 있습니다. 그러나 Cisco는 IP 조각 모음 전처리기의 활성화된 작업을 더욱 세밀한 수준으로 지정할 것을 권장합니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

전역 **Preallocated Fragments(미리 할당된 조각)** 옵션을 구성할 수 있습니다.

Preallocated Fragments(미리 할당된 조각)

전처리기가 한 번에 처리할 수 있는 개별 조각의 최대 수입니다. 미리 할당할 조각 노드의 수를 지정하면 정적 메모리 할당이 활성화됩니다.

주의 개별 조각을 처리하면 메모리 중 약 1550바이트가 사용됩니다. 전처리기가 개별 조각을 처리하는 데 디바이스에 미리 정해진 허용 가능한 메모리 제한보다 더 많은 메모리가 필요한 경우 해당 디바이스의 메모리 제한이 우선합니다.

각 IP 조각 모음 정책에 다음 옵션을 구성할 수 있습니다,

네트워크

조각 모음 정책을 적용할 호스트의 IP 주소입니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 기본 정책을 비롯한 총 255개의 프로파일을 지정할 수 있습니다. ASA FirePOWER 모듈에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역 의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

정책

모니터링된 네트워크 세그먼트의 호스트 집합에 사용할 조각 모음 정책입니다. 일곱 개의 정책인 BSD, BSD-Right, First, Linux, Last, Solaris, Windows 중에서 선택할 수 있습니다. 이 정책에 대한 자세한 내용은 17-13페이지의 대상 기반 조각 모음 정책을 참고하십시오.

시간 제한

조각화된 패킷을 리어셈블할 때 전처리기 엔진이 사용할 수 있는 최대 시간(단위: 초)을 지정합니다. 패킷이 지정된 기간 내에 리어셈블될 수 없는 경우, 전처리기 엔진은 패킷 리어셈블 시도를 중지하고 수신한 조각을 삭제합니다.

최소 TTL

패킷이 가질 수 있는 허용 가능한 최소 TTL 값을 지정합니다. 이 옵션은 TTL 기반 삽입 공격을 탐지합니다.

규칙 123:1을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

이상 징후 탐지

중첩되는 조각과 같은 조각화 문제를 식별합니다.

다음 규칙을 활성화하여 옵션에 대한 이벤트를 생성할 수 있습니다.

- 123:1~123:4
- 123:5(BSD 정책)
- 123:6~123:8

중첩 제한

한 세션에서 중첩되는 세그먼트에 대해 0(무제한)과 255 사이의 구성된 수가 탐지된 경우 해당 세션에 대한 조각 모음이 중단됨을 명시합니다. 이 옵션을 구성하려면 **Detect Anomalies(이상 징후 탐지)**를 활성화해야 합니다. 빈 필드 값이 이 옵션을 비활성화합니다.

규칙 123:12를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

최소 조각 크기

0(무제한)과 255 사이의 구성된 수보다 작은, 마지막이 아닌 조각이 탐지된 경우 패킷이 악성으로 간주됨을 명시합니다. 이 옵션을 구성하려면 **Detect Anomalies(이상 징후 탐지)**를 활성화해야 합니다. 빈 필드 값이 이 옵션을 비활성화합니다.

규칙 123:13을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

IP 조각 모음 구성

라이센스: 보호

다음 절차를 사용하여 IP 조각 모음 전처리기를 구성할 수 있습니다. IP 조각 모음 전처리기 구성 옵션에 대한 자세한 내용은 17-13페이지의 조각 모음 옵션 선택을 참고하십시오.

IP 조각 모음을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Edit Policy(정책 수정) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Transport/Network Layer Preprocessors(전송/네트워크 레이어 전처리기)에서 **IP Defragmentation(IP 조각 모음)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

IP Defragmentation(IP 조각 모음) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 또는, Global Settings(전역 설정) 페이지 영역에서 **Preallocated Fragments(미리 할당된 조각)** 설정을 수정할 수 있습니다.

단계 10 다음 2가지 옵션을 사용할 수 있습니다.

- 새 대상 기반 정책을 추가합니다. 추가 아이콘( )을 클릭합니다. 이 아이콘은 페이지 왼쪽의 **Servers(서버)** 옆에 있습니다. Add Target(대상 추가) 팝업 창이 나타납니다. **Host Address(호스트 주소)** 필드에 하나 이상의 IP 주소를 지정하고 **OK(확인)**를 클릭합니다.

  단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 기본 정책을 비롯한 총 255가지 대상 기반 정책을 생성할 수 있습니다. ASA FirePOWER 모듈에서 IP 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

  트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

  새 항목은 페이지 왼쪽의 대상 목록에 나타나는데, 선택되었음을 나타내도록 강조 표시됩니다. 그리고 Configuration(구성) 섹션은 추가한 정책에 대한 현재 구성을 반영하도록 업데이트됩니다.

- 기존 대상 기반 정책의 설정을 수정합니다. 페이지 왼쪽의 **Hosts(호스트)**에 추가한 정책에 대해 구성된 주소를 클릭하거나 **default(기본값)**를 클릭합니다.

  선택한 부분이 강조 표시되고, Configuration(구성) 섹션이 선택한 정책에 대한 현재 구성을 표시하도록 업데이트됩니다. 기존 대상 기반 정책을 삭제하려면, 제거할 정책 옆에 있는 삭제 아이콘( )을 클릭합니다.

단계 11 또는, Configuration(구성) 페이지 영역에서 옵션 중 하나를 수정할 수 있습니다.

단계 12 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

패킷 디코딩 이해

라이센스: 보호

시스템은 전처리기에 캡처된 패킷을 보내기 전에 먼저 패킷 디코더에 패킷을 보냅니다. 패킷 디코더는 패킷 헤더와 페이로드를 전처리기 및 규칙 엔진이 쉽게 사용할 수 있는 형식으로 변환합니다. 각 스택 레이어는 데이터 링크 레이어에서 시작해서 네트워크 및 전송 레이어에 이르기까지 계속해서 차례로 디코딩됩니다.

116의 생성기 ID(GID)가 있는 패킷 디코더 규칙에서 이벤트를 생성하려는 경우, 이 규칙을 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

GTP 데이터 채널 디코딩

캡슐화된 GTP(GPRS[General Packet Radio Service] 터널링 프로토콜) 데이터 채널을 디코딩합니다. 기본적으로, 디코더는 포트 3386의 버전 0 데이터 및 포트 2152의 버전 1 데이터를 디코딩합니다. `GTP_PORTS` 기본 변수를 사용하여 캡슐화된 GTP 트래픽을 식별하는 포트를 수정할 수 있습니다. 자세한 내용은 2-15페이지의 미리 정의된 기본 변수 최적화를 참고하십시오.

규칙 116:297 및 116:298을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다.

비표준 포트에서 Teredo 탐지

포트 3544 이외의 UDP 포트에서 확인된 IPv6 트래픽의 Teredo 터널링을 검사합니다.

IPv6 트래픽이 있으면 항상 시스템에서 검사합니다. 기본적으로, IPv6 검사에는 4in6, 6in4, 6to4 및 6in6 터널링 체계가 포함되며, UDP 헤더가 포트 3544를 지정하는 경우에는 Teredo 터널링도 포함됩니다.

IPv4 네트워크에서 IPv4 호스트는 Teredo 프로토콜을 사용하여 IPv4 NAT(Network Address Translation) 디바이스를 통해 IPv6 트래픽을 터널링할 수 있습니다. Teredo는 IPv4 NAT 디바이스의 배후에 있는 IPv6 연결을 허용하기 위해 IPv4 UDP 데이터그램 안에서 IPv6 패킷을 캡슐화합니다. 시스템은 일반적으로 UDP 포트 3544를 사용하여 Teredo 트래픽을 식별합니다. 그러나, 공격자는 탐지를 피하기 위해 비표준 포트를 사용할 수 있습니다. **Detect Teredo on Non-Standard Ports(비표준 포트에서 Teredo 탐지)**를 활성화하여 시스템이 Teredo 터널링의 모든 UDP 페이로드를 검사하도록 할 수 있습니다.

Teredo 디코딩은 첫 번째 UDP 헤더에서만, 그리고 IPv4가 외부 네트워크 레이어에 사용될 때만 수행됩니다. IPv6 데이터에서 캡슐화된 UDP 데이터로 인해 Teredo IPv6 레이어 다음에 두 번째 UDP 레이어가 나타나는 경우 규칙 엔진은 UDP 침입 규칙을 사용하여 내부 및 외부 UDP 레이어를 분석합니다.

정책- 기타 규칙 카테고리의 침입 규칙 12065, 12066, 12067, 및 12068은 Teredo 트래픽을 탐지하지만 디코딩하지는 않는다는 점에 유의하십시오. 또는, 이 규칙을 사용하여 인라인 배포에서 Teredo 트래픽을 삭제할 수 있는데, **Detect Teredo on Non-Standard Ports(비표준 포트에서 Teredo 탐지)**를 활성화한 경우 반드시 이 규칙을 비활성화하거나 트래픽 삭제 없이 이벤트를 생성하도록 설정해야 합니다. 자세한 내용은 20-9페이지의 침입 정책에서 규칙 필터링 및 20-19페이지의 규칙 상태 설정을 참고하십시오.

과도한 길이 값 탐지

패킷 헤더가 실제 패킷 길이보다 큰 패킷 길이를 지정할 때를 탐지합니다.

규칙 116:6, 116:47, 116:97 및 116:275를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다.

유효하지 않은 IP 옵션 탐지

유효하지 않은 IP 옵션을 사용하는 익스플로잇을 식별하기 위해 유효하지 않은 IP 헤더 옵션을 탐지합니다. 예를 들어, 시스템을 마비시키는 방화벽에 대한 서비스 거부(DoS) 공격이 존재합니다. 방화벽은 유효하지 않은 Timestamp(타임 스탬프) 및 Security IP(보안 IP) 옵션의 분석을 시도하고 제로 길이를 점검하는 데 실패하는데, 이는 복구할 수 없는 무한 루프를 야기합니다. 규칙 엔진은 제로 길이 옵션을 식별하고, 방화벽에서 공격을 완화하는 데 사용할 수 있는 정보를 제공합니다.

규칙 116:4 및 116:5를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

실험적 TCP 옵션 탐지

실험적 TCP 옵션이 포함된 TCP 헤더를 탐지합니다. 다음 표는 이러한 옵션에 대해 설명합니다.

TCP 옵션	설명
9	허용된 부분 순서 연결
10	부분 순서 서비스 프로파일
14	대체 체크섬 요청
15	대체 체크섬 데이터
18	트레일러 체크섬
20	우주 통신 프로토콜 표준(SCPS)
21	선택적 부정적 수신 확인(SCPS)
22	레코드 경계(SCPS)
23	손상(SPCS)
24	SNAP
26	TCP 압축 필터

이는 실험적 옵션이므로, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다.

참고 위 표에 나열된 실험적 옵션 외에도, 시스템은 26보다 큰 옵션 번호를 가진 모든 TCP 옵션을 실험적인 것으로 고려합니다.

규칙 116:58을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

사용하지 않는 TCP 옵션 탐지

사용하지 않는 TCP 옵션이 포함된 TCP 헤더를 탐지합니다. 이는 사용하지 않는 옵션이므로, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다. 다음 표는 이러한 옵션에 대해 설명합니다.

TCP 옵션	설명
6	에코
7	에코 응답
16	Skeeter
17	Bubba
19	MD5 서명
25	할당되지 않음

규칙 116:57을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

T/TCP 탐지

CC.ECHO 옵션이 포함된 TCP 헤더를 탐지합니다. CC.ECHO 옵션은 TCP for Transactions(트랜잭션용 TCP, T/TCP)가 사용되고 있음을 확인합니다. T/TCP 헤더 옵션은 널리 사용되지 않기 때문에, 일부 시스템은 이를 처리하지 않고 익스플로잇에 노출될 수 있습니다.

규칙 116:56을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19 페이지의 규칙 상태 설정을 참고하십시오.

기타 TCP 옵션 탐지

다른 TCP 디코딩 이벤트 옵션으로 탐지되지 않는 유효하지 않은 TCP 옵션을 통해 TCP 헤더를 탐지합니다. 예를 들어, 이 옵션은 정확하지 않은 길이 또는 옵션 데이터를 TCP 헤더 외부에 배치하는 길이를 가진 TCP 옵션을 탐지합니다.

규칙 116:54, 116:55 및 116:59를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

프로토콜 헤더 이상 징후 탐지

더 많은 특정 IP 및 TCP 디코더 옵션으로 탐지되지 않는 다른 디코딩 오류를 탐지합니다. 예를 들어, 디코더는 잘못된 형식의 데이터 연결 프로토콜 헤더를 탐지할 수 있습니다.

이 옵션의 이벤트를 생성하려면, 특히 다른 패킷 디코더 옵션과 연결된 규칙 이외의 모든 패킷 디코더 규칙을 활성화하면 됩니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

다음 규칙이 이상 IPv6 트래픽에 의해 트리거된 이벤트를 생성한다는 점에 유의하십시오. 116:270에서 116:274, 116:275에서 116:283, 116:291, 116:292, 116:295, 116:296, 116:406, 116:458, 116:460, 116:461.

또한 인라인 표준화 전처리기 **Minimum TTL(최소 TTL)** 옵션과 연결된 다음 규칙에 유의하십시오.

- 규칙 116:428을 활성화하여 시스템이 지정된 최소 값보다 작은 TTL 값이 포함된 IPv4 패킷을 탐지하는 경우 이벤트를 생성할 수 있습니다.
- 규칙 116:270을 활성화하여 시스템이 지정된 최소 값보다 작은 홉 제한 값이 포함된 IPv6 패킷을 탐지하는 경우 이벤트를 생성할 수 있습니다.

자세한 내용은 인라인 표준화 **Minimum TTL(최소 TTL)** 옵션을 참고하십시오. 이는 17-6페이지의 인라인 트래픽 표준화에서 확인할 수 있습니다.

패킷 디코딩 구성

라이센스: 보호

Packet Decoding(패킷 디코딩) 구성 페이지에서 디코딩하는 패킷을 구성할 수 있습니다. 패킷 디코딩 구성 옵션에 대한 자세한 내용은 17-16페이지의 패킷 디코딩 이해를 참고하십시오.

패킷 암호를 설정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Edit Policy(정책 수정) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Transport/Network Layer Preprocessors(전송/네트워크 레이어 전처리기)에서 **Packet Decoding(패킷 디코딩)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Packet Decoding(패킷 디코딩) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 정책 레이어를 식별합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

단계 9 Packet Decoding(패킷 디코딩) 페이지에서 모든 탐지 옵션을 활성화하거나 비활성화할 수 있습니다. 자세한 내용은 17-16페이지의 패킷 디코딩 이해를 참고하십시오.

단계 10 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

TCP 스트림 전처리 사용

라이센스: 보호

TCP 프로토콜은 연결이 존재할 수 있는 다양한 상태를 정의합니다. 각 TCP 연결은 소스 및 대상 IP 주소와 소스 및 대상 포트에 의해 식별됩니다. TCP는 동일한 연결 매개 변수 값을 가진 연결이 한 번에 하나만 존재하도록 허용합니다.

129의 생성기 ID(GID)가 있는 TCP 스트림 전처리기 규칙에서 이벤트를 생성하려는 경우, 이 규칙을 활성화해야 한다는 점에 유의하십시오. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

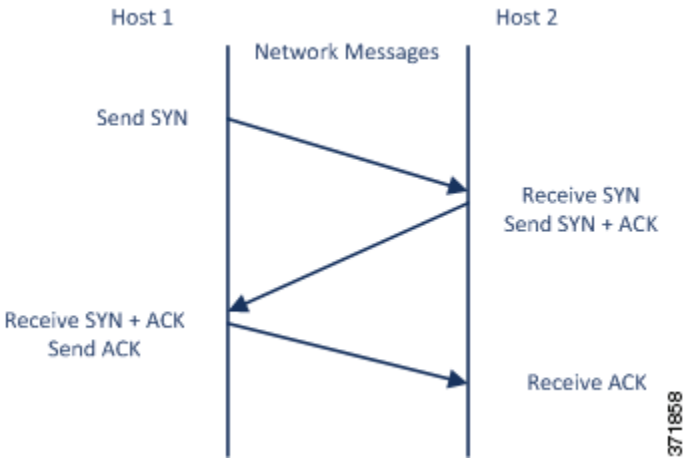
자세한 내용은 다음 섹션을 참고하십시오.

- 17-21페이지의 상태 관련 TCP 익스플로잇 이해
- 17-2페이지의 침입 드롭 규칙으로 활성 응답 시작
- 17-21페이지의 TCP 전역 옵션 선택
- 17-22페이지의 대상 기반 TCP 정책 이해

상태 관련 TCP 익스플로잇 이해

라이센스: 보호

침입 규칙에 `established` 인수로 `flow` 키워드를 추가한 경우, 침입 규칙 엔진은 상태 저장 모드에서 규칙 및 지시와 일치하는 패킷을 검사합니다. 상태 저장 모드는 클라이언트와 서버 사이의 적정 3방향 핸드셰이크로 설정된 TCP 세션의 일부인 트래픽만 평가합니다. 다음 다이어그램은 3방향 핸드셰이크를 설명합니다.



전처리기가 설정된 TCP 세션의 일부로 식별할 수 없는 모든 TCP 트래픽을 검색하도록 시스템을 구성할 수 있습니다. 그러나 이벤트가 시스템의 빠른 과부하를 야기하고 의미 있는 데이터를 제공하지 않으므로 일반적인 사용에는 권장되지 않습니다.

stick 및 snot과 같은 공격은 시스템의 광범위한 규칙 집합 및 자체 패킷 검사를 사용합니다. 이 툴은 Snort 기반 침입 규칙의 패턴에 따라 패킷을 생성하고, 네트워크를 통해 전송합니다. 사용자 규칙이 상태 저장 검사를 위한 규칙 구성을 위해 `flow` 또는 `flowbits` 키워드를 포함하지 않은 경우, 각 패킷은 규칙을 트리거하여 시스템을 마비시킵니다. 이러한 패킷은 설정된 TCP 세션의 일부가 아니며 의미 있는 정보를 제공하지 않으므로 상태 저장 검사를 통해 패킷을 무시할 수 있습니다. 상태 저장 검사를 수행하는 경우, 규칙 엔진은 설정된 TCP 세션의 일부인 해당 공격만 탐지하므로 분석가가 stick 또는 snot로 인해 발생하는 이벤트 볼륨이 아닌 해당 공격에 집중할 수 있습니다.

TCP 전역 옵션 선택

라이센스: 보호

TCP 스트림 전처리기에는 TCP 스트림 전처리기의 작동 방식을 제어하는 하나의 전역 옵션이 있습니다.

어떤 전처리기 규칙도 이 옵션과 연결되어 있지 않습니다.

패킷 유형 성능 증대

활성화된 침입 규칙에서 지정되지 않은 모든 포트 및 애플리케이션 프로토콜에 대한 TCP 트래픽을 무시하도록 활성화합니다. `any`로 설정된 소스 및 대상 포트 둘 다를 지닌 TCP 규칙에 `flow` 또는 `flowbits` 옵션이 있는 경우는 제외됩니다. 이러한 성능 향상으로 공격이 누락될 수 있습니다.

대상 기반 TCP 정책 이해

라이센스: 보호

서로 다른 운영 체제는 TCP를 서로 다른 방식으로 구현합니다. 예를 들어, Windows 및 일부의 다른 운영 체제에서 세션을 재설정하려면 정확한 TCP 시퀀스 번호를 지닌 TCP 재설정 세그먼트가 필요한 반면, Linux 및 기타 운영 체제에서는 다양한 시퀀스 번호를 허용합니다. 이 예제에서, 스트림 전처리기는 대상 호스트가 시퀀스 번호에 근거한 재설정에 대응하는 방식을 정확하게 이해해야 합니다. 스트림 전처리기는 대상 호스트가 재설정을 유효한 것으로 간주하는 경우에 한해 세션 추적을 중지하므로, 전처리기가 스트림 검사를 중지한 후 공격이 패킷을 전송하여 탐지를 우회할 수 없습니다. TCP 구현의 다른 변경 사항에는 운영 체제가 TCP 타임 스탬프 옵션을 채택하는지 여부 등이 포함되 있으며, 이를 포함할 경우 타임 스탬프를 처리하는 방식 및 운영 체제가 SYN 패킷의 데이터를 수락하거나 무시하는지 여부를 포함합니다.

다양한 운영 체제는 또한 중첩되는 TCP 세그먼트를 다양한 방법으로 리어셈블합니다. 중첩되는 TCP 세그먼트는 접수되지 않은 일반 재전송을 반영할 수 있습니다. 세그먼트는 또한 호스트 중 하나의 운영 체제를 알고 있는 공격자가 중첩되는 세그먼트에 숨겨진 악성 콘텐츠를 전송하여 탐지를 우회하고 해당 호스트를 공격하는 시도를 나타낼 수 있습니다. 그러나, 스트림 전처리기를 구성하여 모니터링된 네트워크 세그먼트에서 실행되는 운영 체제를 인식할 수 있으며, 따라서 이는 대상 호스트가 하는 것과 동일한 방법으로 세그먼트를 리어셈블하여 공격을 식별하도록 허용합니다.

하나 이상의 TCP 정책을 만들어서 TCP 스트림 검사 및 리어셈블리를 모니터링된 네트워크 세그먼트에서 다른 운영 체제로 조정할 수 있습니다. 각 정책에 대해 13개 운영 체제 정책 중 하나를 확인합니다. 다른 운영 체제를 사용하는 호스트의 일부 또는 전체를 식별하기 위해 필요한 만큼 많은 TCP 정책을 사용하여 각 TCP 정책을 특정 IP 주소 또는 주소 블록에 바인딩합니다. 기본 TCP 정책은 다른 TCP 정책에서 식별하지 않는 모니터링된 네트워크의 모든 호스트에 적용되므로 기본 TCP 정책에 대한 IP 주소, CIDR 블록 또는 접두사 길이를 지정할 필요가 없습니다.

또한 적응형 프로파일을 사용하여 패킷의 대상 호스트에 대한 호스트 운영 체제 정보를 통해 TCP 스트림 전처리기의 대상 기반 정책을 동적으로 선택할 수도 있다는 점에 유의하십시오. 자세한 내용은 18-1페이지의 수동 배포 시 전처리 조정을 참고하십시오.

다음 표는 각각을 사용하는 호스트 운영 체제 및 운영 체제 정책을 식별합니다.

표 17-2 TCP 운영 체제 정책

정책	운영 체제
First	알 수 없는 OS
Last	Cisco IOS
BSD	AIX FreeBSD OpenBSD
Linux	Linux 2.4 커널 Linux 2.6 커널
이전 Linux	Linux 2.2 및 이전 커널

표 17-2 TCP 운영 체제 정책 (계속)

정책	운영 체제
Windows	Windows 98
	Windows NT
	Windows 2000
	Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS
	SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 이상 버전
HPUX 10	HP-UX 10.2 이하 버전
Mac OS	Mac OS 10(Mac OS X)

팁 First 운영 체제 정책에서는 호스트 운영 체제를 알 수 없는 경우 일부 보호를 제공할 수 있습니다. 하지만, 이로 인해 공격이 누락될 수 있습니다. 알고 있는 경우 정확한 운영 체제를 지정하는 정책을 수정해야 합니다.

TCP 정책 옵션 선택

라이센스: 보호

다음 목록은 스트림 전처리기가 검사하는 TCP 트래픽을 식별하고 제어하기 위해 설정할 수 있는 옵션에 대해 설명합니다.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

네트워크

사용자가 TCP 스트림 리어셈블리 정책을 적용할 호스트 IP 주소를 지정합니다.

단일 IP 주소 또는 주소 블록을 지정할 수 있습니다. 기본 정책을 비롯한 255개의 총 프로파일을 지정할 수 있습니다. ASA FirePOWER 모듈에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책으로는 처리되지 않는 모니터링된 네트워크 세그먼트에 모든 IP 주소를 지정한다는 점에 유의하십시오. 따라서, 기본 정책에 대한 IP 주소 또는 CIDR 차단/접두사 길이를 지정할 수가 없으며, 지정할 필요도 없습니다. 그리고 다른 정책에서 이 설정을 공백으로 비워둘 수 없으며 `any`(예를 들어, 0.0.0.0/0 또는 ::/0)를 나타내는 주소 표기법을 사용할 수도 없습니다.

트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역 의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

정책

대상 호스트의 TCP 정책 운영 체제를 식별합니다. **Mac OS** 이외의 정책을 선택하는 경우, 시스템은 동기화(SYN) 패킷에서 데이터를 제거하고 규칙 129:2의 이벤트 생성을 비활성화합니다.

자세한 내용은 17-22페이지의 대상 기반 TCP 정책 이해를 참고하십시오.

시간 제한

1에서 86400 사이의 시간(단위: 초)으로, 침입 규칙 엔진이 이 시간 동안 상태 표에서 비활성 스트림을 유지합니다. 스트림이 지정된 시간에 리어셈블되지 않는 경우, 침입 규칙 엔진은 이를 상태 표에서 삭제합니다.

참고 디바이스가 네트워크 트래픽이 디바이스의 대역폭 제한에 도달할 가능성이 높은 세그먼트에 구축된 경우, 처리 오버헤드의 양을 낮추기 위해 이 값을 더 높게(예: 600초) 설정할 것을 고려해야 합니다.

최대 TCP 창

수신 호스트가 지정한 대로 허용된 1에서 1073725440 바이트 사이의 최대 TCP 창 크기를 지정합니다. 값을 0으로 설정하면 TCP 창 크기 확인이 비활성화됩니다.

주의 상한 값은 RFC가 허용하는 최대 창 크기로, 공격자가 탐지를 회피하는 것을 방지하는 것이 목적이지만, 훨씬 큰 최대 창 크기를 설정하면 스스로 자초한 서비스 거부(DoS) 공격이 발생할 수 있습니다.

규칙 129:6을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

중첩 제한

세션에서 중첩되는 세그먼트에 대해 0(무제한)과 255 사이의 구성된 번호가 탐지된 경우 해당 세션을 위한 세그먼트 리어셈블리가 중단되며, **Stateful Inspection Anomalies(상태 저장 검사 이상 징후)**가 활성화되고 동반되는 전처리기 규칙이 활성화된 경우 이벤트가 생성된다는 것을 지정합니다.

규칙 129:7을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

플러시 팩터

인라인 배포에서, 줄어들지 않는 크기의 세그먼트에 대해 1에서 2048 사이의 구성된 번호 이후에 줄어든 크기의 세그먼트가 탐지된 경우, 시스템은 탐지를 위해 누적된 세그먼트 데이터를 삭제함을 지정합니다. 값을 0으로 설정하면 이러한 세그먼트 패턴의 탐지가 비활성화되며, 이는 요청 또는 응답의 종료를 나타낼 수 있습니다. 이 옵션을 적용하려면 Inline Normalization(인라인 표준화) **Normalize TCP Payload(TCP 페이로드 표준화)** 옵션이 활성화되어야 한다는 점에 유의하십시오. 자세한 내용은 17-6페이지의 인라인 트래픽 표준화를 참고하십시오.

상태 저장 검사 이상 징후

TCP 스택에서 비정상적 상태를 탐지합니다. TCP/IP 스택이 잘못 로깅된 경우 동반되는 전처리기 규칙이 활성화되면 이로 인해 많은 이벤트가 생성될 수 있습니다.

다음 규칙을 활성화하여 옵션에 대한 이벤트를 생성할 수 있습니다.

- 129:1~129:5
- 129:6(Mac OS만 해당)

- 129:8~129:11
- 129:13~129:19

자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

TCP 세션 가로채기

세션에서 수신된 후속 패킷에 대한 3방향 핸드셰이크 동안 TCP 연결의 양쪽에서 탐지된 하드웨어(MAC) 주소를 검증하여 TCP 세션 가로채기를 탐지합니다. **Stateful Inspection Anomalies(상태 저장 검사 이상 징후)**가 활성화되고 하나 또는 두 개의 해당 전처리기 규칙이 활성화된 경우, 한 쪽의 MAC 주소가 다른 쪽의 주소와 일치하지 않으면 이벤트가 생성됩니다.

규칙 129:9 및 129:10을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

연속된 소규모 세그먼트

Stateful Inspection Anomalies(상태 저장 검사 이상 징후)가 활성화된 경우, 허용된 소규모 연속 TCP 세그먼트의 최대 수를 1부터 2048까지의 범위에서 지정합니다. 값을 0으로 설정하면 소규모 연속 세그먼트 확인이 비활성화됩니다.

이 옵션을 **Small Segment Size(소규모 세그먼트 크기)** 옵션과 함께 설정해야 하는데, 둘 다 비활성화하거나 둘 모두에 대해 0이 아닌 값을 설정합니다. 각 세그먼트의 길이가 1바이트라고 해도 개입 ACK 없이 최대 2000개의 연속 세그먼트를 수신하는 경우 일반적으로 예상하는 것보다 훨씬 많은 연속 세그먼트일 수 있음에 유의하십시오.

규칙 129:12를 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

소규모 세그먼트 크기

Stateful Inspection Anomalies(상태 저장 검사 이상 징후)가 활성화된 경우, 소규모로 간주되는 TCP 세그먼트 크기를 1에서 2048바이트 사이의 범위에서 지정합니다. 값을 0으로 설정하면 소규모 세그먼트의 크기기 비활성화됩니다.

이 옵션을 **Consecutive Small Segment Size(연속된 소규모 세그먼트)** 옵션과 함께 설정해야 하는데, 둘 다 비활성화하거나 둘 모두에 대해 0이 아닌 값을 설정합니다. 2048 바이트 TCP 세그먼트는 일반적인 1500 바이트 이더넷 프레임보다 크다는 점에 유의하십시오.

Ports Ignoring Small Segments(소규모 세그먼트를 무시하는 포트)

Stateful Inspection Anomalies(상태 저장 검사 이상 징후), **Consecutive Small Segment Size(연속된 소규모 세그먼트)** 및 **Small Segment Size(소규모 세그먼트 크기)**가 활성화된 경우, 소규모 세그먼트 탐지를 무시하는 쉼표로 구분된 하나 이상의 포트 목록을 선택적으로 지정합니다. 이 옵션을 비워 두면 어떤 포트도 무시되지 않습니다.

어느 포트든 목록에 추가할 수 있지만, 목록은 TCP 정책 내 **Perform Stream Reassembly on(스트림 리어셈블리 수행)** 포트 목록 중 하나에서 지정된 포트에만 영향을 미칩니다.

TCP 3방향 핸드셰이크 요청

TCP 3방향 핸드셰이크가 완료되는 경우에만 세션이 설정된 것으로 처리됨을 지정합니다. 성능을 향상시키고, SYN 플러드 공격으로부터 보호하며, 부분 비동기 환경에서 작업을 허용하려면 이 옵션을 비활성합니다. 설정된 TCP 세션의 일부가 아닌 정보를 전송하여 잘못된 긍정을 생성하려고 시도하는 공격을 차단하려면 이 옵션을 활성화합니다.

규칙 129:20을 활성화하여 이 옵션에 대한 이벤트를 생성할 수 있습니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

3방향 핸드셰이크 시간 제한

Require TCP 3-Way Handshake(TCP 3방향 핸드셰이크 요청)가 활성화된 경우 핸드셰이크 완료 기한이 되는 시간(단위: 초)을 0(무제한)에서 86400(24시간)까지의 범위에서 지정합니다. 이 옵션의 값을 수정하려면 **Require TCP 3-Way Handshake(TCP 3방향 핸드셰이크 요청)**를 활성화해야 합니다.

패킷 크기 성능 증대

전처리기가 리어셈블리 버퍼에서 대규모 패킷을 대기열에 넣지 않도록 설정합니다. 이러한 성능 향상으로 공격이 누락될 수 있습니다. 1~20 바이트의 소규모 패킷을 사용하여 회피 시도를 차단하려면 이 옵션을 비활성화합니다. 모든 트래픽이 매우 큰 패킷으로 구성되어 있어서 그러한 공격이 없을 것임을 확신하는 경우 이 옵션을 활성화합니다.

레거시 리어셈블리

패킷을 리어셈블할 때 스트림 전처리기가 더 이상 사용되지 않는 Stream 4(스트림 4) 전처리기를 모방하도록 설정하여 스트림 전처리기가 리어셈블한 이벤트를 Stream 4(스트림 4) 전처리기가 리어셈블한 동일 데이터 스트림에 기반한 이벤트와 비교할 수 있습니다.

비동기 네트워크

모니터링된 네트워크가 비동기 네트워크, 즉, 시스템이 트래픽의 절반만 표시하는 네트워크인지 여부를 지정합니다. 이 옵션을 활성화할 경우, 시스템은 성능을 높이기 위해 TCP 스트림을 리어셈블하지 않습니다.

클라이언트 포트, 서버 포트, 두 포트 모두에서 스트림 리어셈블리 수행

클라이언트 포트, 서버 포트, 또는 두 포트 모두에 대해 스트림 전처리기가 리어셈블할 트래픽을 식별하는, 쉼표로 구분된 포트 목록을 지정합니다. 17-27페이지의 스트림 리어셈블리 옵션 선택을 참고하십시오.

클라이언트 서비스, 서버 서비스, 두 서비스 모두에서 스트림 리어셈블리 수행

클라이언트 서비스, 서버 서비스, 또는 두 서비스 모두에 대해 스트림 전처리기가 리어셈블하려는 트래픽에서 식별할 서비스를 지정합니다. 17-27페이지의 스트림 리어셈블리 옵션 선택을 참고하십시오.

문제 해결 옵션: 최대 대기 바이트

Support(지원팀)은 문제 해결 통화 중 사용자에게 TCP 연결의 한 쪽에 대기될 수 있는 데이터의 양을 지정하도록 요청할 수 있습니다. 0 값은 무제한 바이트 수를 지정합니다.

주의 이 문제 해결 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

문제 해결 옵션: 최대 대기 세그먼트

Support(지원팀)은 문제 해결 통화 중 사용자에게 TCP 연결의 한 쪽에 대기될 수 있는 세그먼트의 최대 바이트 수를 지정하도록 요청할 수 있습니다. 0 값은 무제한 데이터 세그먼트 바이트 수를 지정합니다.

주의 이 문제 해결 옵션에 대한 설정을 변경하면 성능에 영향을 미치므로 지원 안내서를 통해서만 변경해야 합니다.

TCP 스트림 리어셈블

라이센스: 보호

스트림 전처리기는 TCP 세션의 서버의 서버-클라이언트 통신 스트림, 클라이언트-서버 통신 스트림, 또는 둘 다에 속하는 모든 패킷을 수집하고 리어셈블합니다. 이를 통해 규칙 엔진은 주어진 스트림에 속하는 개별 패킷만 검사하는 것이 아니라 단일, 리어셈블된 엔터티로서의 스트림을 검사할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 17-27페이지의 스트림 기반 공격 이해
- 17-27페이지의 스트림 리어셈블리 옵션 선택

스트림 기반 공격 이해

라이센스: 보호

규칙 엔진은 스트림 리어셈블리를 통해 개별 패킷 검사에서는 탐지하지 못할 수 있는 스트림 기반 공격을 식별할 수 있습니다. 규칙 엔진이 네트워크의 필요에 따라 리어셈블할 통신 스트림을 지정할 수 있습니다. 예를 들어, 사용자 웹 서버에서 트래픽을 모니터링하는 경우에는 본인의 웹 서버로부터 악성 트래픽을 수신할 가능성이 거의 없으므로 클라이언트 트래픽만 검사하기를 원할 수 있습니다.

스트림 리어셈블리 옵션 선택

라이센스: 보호

각 TCP 정책에서 스트림 전처리기가 리어셈블할 트래픽을 식별하는, 쉼표로 구분된 포트 목록을 지정할 수 있습니다. 적응형 프로파일을 활성화하는 경우, 포트에 대한 대안으로 또는 포트와 조합하여 리어셈블할 트래픽을 식별하는 서비스를 나열할 수 있습니다. 적응형 프로파일의 활성화 및 사용에 대한 자세한 내용은 18-1페이지의 수동 배포 시 전처리 조정을 참고하십시오.

포트, 서비스, 또는 둘 다를 지정할 수 있습니다. 클라이언트 포트, 서버 포트 및 둘 다의 모든 조합에 대해 포트의 개별 목록을 지정할 수 있습니다. 또한 클라이언트 서비스, 서버 서비스 및 둘 다의 모든 조합에 대해 서비스의 개별 목록을 지정할 수 있습니다. 예를 들어 다음을 리어셈블하기를 원하는 것으로 가정합니다.

- 클라이언트로부터의 SMTP(포트 25) 트래픽
- FTP 서버 응답(포트 21)
- 두 방향 모두에서의 텔넷(포트 23) 트래픽

다음을 구성할 수 있습니다.

- 클라이언트 포트에 대해, `23, 25`를 지정합니다.
- 서버 포트에 대해, `21, 23`을 지정합니다.

또는, 그 대신, 다음을 설정할 수 있습니다.

- 클라이언트 포트에 대해, `25`을 지정합니다.
- 서버 포트에 대해, `21`을 지정합니다.
- 두 포트 모두에 대해, `23`을 지정합니다.

또한, 포트 및 서비스를 결합하고 적응형 프로파일을 활성화하는 경우 유효하게 될 다음 예를 고려하십시오.

- 클라이언트 포트에 대해, `23`을 지정합니다.
- 클라이언트 서비스에 대해, `smtp`를 지정합니다.
- 서버 포트에 대해, `21`을 지정합니다.
- 서버 서비스에 대해, `telnet`을 지정합니다.

모든 포트에 리어셈블리를 제공하기 위해 `all`을 인수로 지정할 수도 있지만, Cisco가 권장하는 바는 **아닙니다**. 이렇게 하면 이 전처리기가 검사한 트래픽 볼륨을 높여 불필요하게 성능을 느리게 할 수 있으므로 포트를 `all`로 설정하는 것은 권장하지 않습니다.

TCP 리어셈블리는 다른 전처리기에 추가한 포트를 자동으로 포함합니다. 그러나, 다른 전처리기 구성에 추가한 TCP 리어셈블리 목록에 포트를 명확하게 추가한 경우, 이러한 추가 포트는 정상적으로 처리됩니다. 여기에는 다음 전처리기를 위한 포트 목록이 포함됩니다.

- FTP/Telnet(서버 수준 FTP)
- DCE/RPC
- HTTP 검사
- SMTP
- 세션 시작 프로토콜
- POP
- IMAP
- SSL

포트를 무효화(예: !77)하면 TCP 스트림 전처리기가 해당 포트에 대한 트래픽 처리를 차단하여 성능을 높일 수 있습니다.

추가 트래픽 유형(클라이언트, 서버, 둘 다)을 리어셈블하면 리소스 요구가 증대된다는 점에 유의하십시오.

어떤 전처리기 규칙도 다음 설명에 언급되지 않은 경우, 이 옵션은 전처리기 규칙과 연결되지 않습니다.

클라이언트 포트에서 스트림 리어셈블리 수행

연결의 클라이언트 측 포트에 기반한 스트림 리어셈블리를 활성화합니다. 다시 말해, 일반적으로 $HOME_NET에 지정된 IP 주소에 의해 정의되는 웹 서버, 메일 서버, 또는 다른 IP 주소로 전송되는 스트림을 리어셈블합니다. 악성 트래픽이 클라이언트에서 시작될 것으로 예상되는 경우 이 옵션을 사용하십시오.

클라이언트 서비스에서 스트림 리어셈블리 수행

연결의 클라이언트 측을 위한 서비스에 기반한 스트림 리어셈블리를 활성화합니다. 악성 트래픽이 클라이언트에서 시작될 것으로 예상되는 경우 이 옵션을 사용하십시오.

이 기능을 사용하려면 보호 및 제어 라이센스가 필요합니다.

서버 포트에서 스트림 리어셈블리 수행

연결의 서버 측만을 위한 포트에 기반한 스트림 리어셈블리를 활성화합니다. 다시 말해, 일반적으로 $EXTERNAL_NET에 지정된 IP 주소에 의해 정의되는 웹 서버, 메일 서버, 또는 다른 IP 주소에서 시작되는 스트림을 리어셈블합니다. 서버 측 공격을 경계하고자 하는 경우 이 옵션을 사용합니다. 포트를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

서버 서비스에서 스트림 리어셈블리 수행

연결의 서버 측만을 위한 서비스에 기반한 스트림 리어셈블리를 활성화합니다. 서버 측 공격을 경계하고자 하는 경우 이 옵션을 사용합니다. 서비스를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

이 기능을 사용하려면 보호 및 제어 라이센스가 필요합니다.

두 포트 모두에서 스트림 리어셈블리 수행

연결의 클라이언트 및 서버 측 모두를 위한 포트에 기반한 스트림 리어셈블리를 활성화합니다. 동일한 포트의 악성 트래픽이 클라이언트와 서버 사이에서 어느 방향에서나 이동할 수 있을 것으로 예상되는 경우 이 옵션을 사용하십시오. 포트를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

두 서비스 모두에서 스트림 리어셈블리 수행

연결의 클라이언트 및 서버 측 모두를 위한 서비스에 기반한 스트림 리어셈블리를 활성화합니다. 동일한 서비스의 악성 트래픽이 클라이언트와 서버 사이에서 어느 방향에서나 이동할 수 있을 것으로 예상되는 경우 이 옵션을 사용하십시오. 서비스를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

이 기능을 사용하려면 보호 및 제어 라이센스가 필요합니다.

TCP 스트림 전처리 구성

라이센스: 보호

TCP 정책을 포함하여 TCP 스트림 전처리를 구성할 수 있습니다. TCP 스트림 전처리기 구성 옵션에 대한 자세한 내용은 17-23페이지의 TCP 정책 옵션 선택을 참고하십시오.

TCP 세션을 추적하기 위해 스트림 전처리기를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Edit Policy(정책 수정) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Transport/Network Layer Preprocessors(전송/네트워크 레이어 전처리기)에서 **TCP Stream Configuration(TCP 스트림 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

TCP Stream Configuration(TCP 스트림 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 또는, Global Settings(전역 설정)에서 **Packet Type Performance Boost(패킷 유형 성능 증대)**을 수정합니다. 자세한 내용은 17-21페이지의 TCP 전역 옵션 선택을 참고하십시오.

단계 10 다음 2가지 옵션을 사용할 수 있습니다.

- 새 대상 기반 정책을 추가합니다. 추가 아이콘( )을 클릭합니다. 이 아이콘은 페이지 왼쪽의 **Hosts(호스트)** 옆에 있습니다. Add Target(대상 추가) 팝업 창이 나타납니다. **Host Address(호스트 주소)** 필드에 하나 이상의 IP 주소를 지정하고 **OK(확인)**를 클릭합니다.

  단일 IP 주소 또는 주소 블록을 지정할 수 있습니다. 기본 정책을 비롯한 총 255가지 대상 기반 정책을 생성할 수 있습니다. ASA FirePOWER 모듈에서 IP 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

  트래픽을 처리하는 대상 기반 정책의 경우, 사용자가 파악하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책이 처리하는 네트워크와 영역의 하위 집합에 일치하거나 동일해야 합니다. 자세한 내용은 13-3페이지의 네트워크 분석 정책으로 전처리 사용자 정의를 참고하십시오.

  새 항목은 페이지 왼쪽의 대상 목록에 나타나는데, 선택되었음을 나타내도록 강조 표시됩니다. 그리고 Configuration(구성) 섹션은 추가한 정책에 대한 현재 구성을 반영하도록 업데이트됩니다.

- 기존 대상 기반 정책의 설정을 수정합니다. 페이지 왼쪽의 **Hosts(호스트)**에 추가한 정책에 대해 구성된 주소를 클릭하거나 **default(기본값)**를 클릭합니다.

  선택한 부분이 강조 표시되고, Configuration(구성) 섹션이 선택한 정책에 대한 현재 구성을 표시하도록 업데이트됩니다. 기존 대상 기반 정책을 삭제하려면, 제거할 정책 옆에 있는 삭제 아이콘( )을 클릭합니다.

단계 11 또는, Configuration(구성)의 모든 TCP 정책 옵션을 수정합니다.

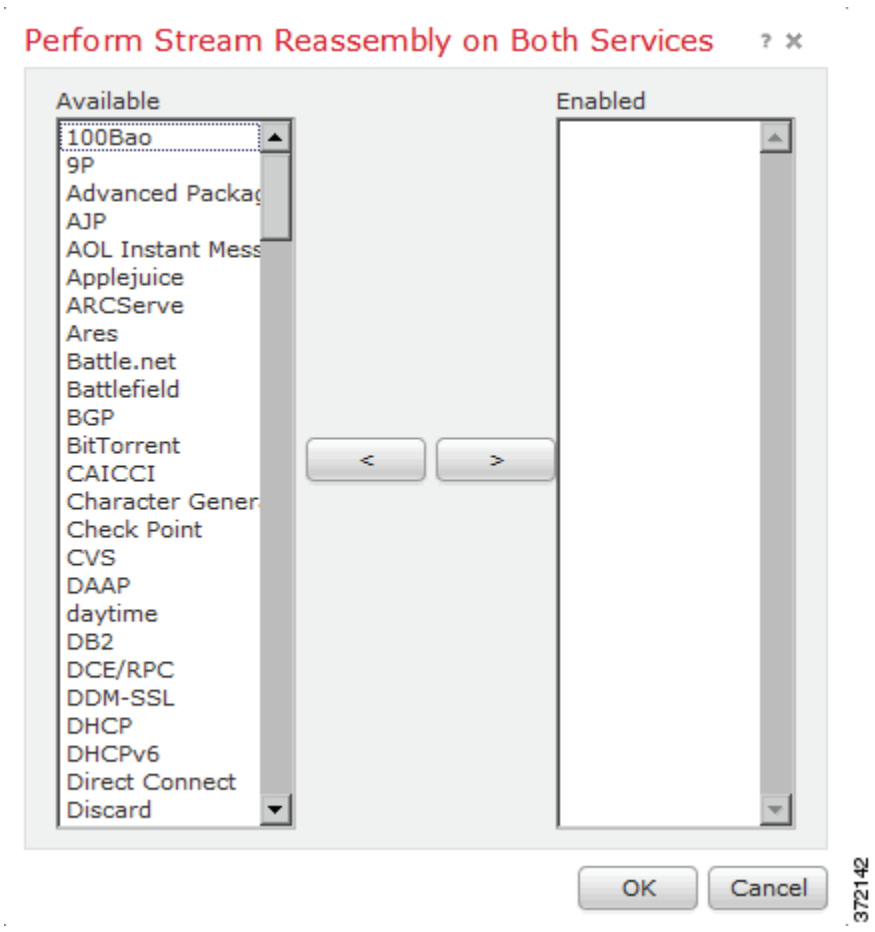
클라이언트 서비스, 서버 서비스, 또는 둘 다에 기반한 스트림 리어셈블리에 대한 설정 변경에 대한 구체적인 지침을 보려면 12단계로, 그렇지 않으면, 15단계로 이동합니다.

자세한 내용은 17-23페이지의 TCP 정책 옵션 선택 및 17-27페이지의 스트림 리어셈블리 옵션 선택을 참고하십시오.

단계 12 클라이언트, 서버, 또는 두 서비스 모두에 기반한 스트림 리어셈블리에 대한 설정을 변경하려면 수정하려는 필드 내부를 클릭하거나 필드 옆에 있는 **Edit(수정)**를 클릭합니다.

선택한 필드의 팝업 창이 표시됩니다.

예를 들어, 다음 그래픽은 Both Services(두 서비스 모두) 팝업 창에서의 Perform Stream Reassembly(스트림 리어셈블리 수행)를 표시합니다.



적응형 프로파일을 활성화하여 네트워크에서 검색된 서비스에 따라 리어셈블하는 스트림 전처리기의 트래픽을 모니터링할 수 있다는 점을 참고하십시오. 자세한 내용은 18-1페이지의 수동 배포 시 전처리 조정을 참고하십시오.

단계 13 다음 2가지 옵션을 사용할 수 있습니다.

- 모니터링할 서비스를 추가하려면, 왼쪽에 있는 **Available(사용 가능한)** 목록에서 하나 이상의 서비스를 선택한 다음, 오른쪽 화살표(**>**) 단추를 클릭합니다.
- 서비스를 제거하려면, 오른쪽에 있는 **Enabled(활성화된)** 목록에서 이를 선택한 다음, 왼쪽 화살표(**<**) 단추를 클릭합니다.

클릭과 함께 Ctrl 및 Shift 키를 사용하여 다중 서비스 탐지기를 선택합니다. 또한 인접한 여러 서비스 탐지기를 선택하려면 클릭하고 드래그할 수 있습니다.

단계 14 **OK(확인)**를 클릭하여 선택 항목을 추가합니다.

TCP Stream Configuration(TCP 스트림 구성) 페이지가 표시되고 서비스가 업데이트됩니다.

단계 15 Support(지원팀)의 지시가 있는 경우에만 선택적으로 **Troubleshooting Options(문제 해결 옵션)**를 확장하고 TCP 스트림 전처리 정책 설정 중 하나를 수정합니다. 자세한 내용은 17-23페이지의 TCP 정책 옵션 선택을 참고하십시오.

단계 16 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

UDP 스트림 전처리 사용

라이센스: 보호

규칙 엔진이 다음 인수를 사용하는 `flow` 키워드(23-51페이지의 TCP 또는 UDP 클라이언트 또는 서버 흐름에 규칙 적용 참고)를 포함하는 UDP 규칙에 대한 패킷을 처리할 때 UDP 스트림 전처리가 발생합니다.

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDP는 커뮤니케이션 채널을 설정하고, 데이터를 교환하며, 채널을 종료하는 두 엔드포인트를 위한 수단을 제공하지 않는 비연결형 프로토콜입니다. UDP 데이터 스트림은 *세션*의 측면에서는 일반적으로 고려되지 않습니다. 그러나, 스트림 전처리기는 흐름의 방향을 결정하고 세션을 확인하기 위해 캡슐화하는 IP 데이터그램 헤더의 소스 및 대상 IP 주소 필드, 그리고 UDP 헤더의 포트 필드를 사용합니다. 구성 가능한 타이머가 초과되는 경우, 또는 둘 중 한 쪽의 엔드포인트가 다른 엔드포인트에 도달할 수 없거나 요청된 서비스가 사용할 수 없다는 ICMP 메시지를 수신한 경우 세션이 종료됩니다.

시스템이 UDP 스트림 전처리와 관련된 이벤트를 생성하지 않는다는 점에 유의하십시오. 하지만, 관련된 패킷 디코더 규칙을 활성화하여 UDP 프로토콜 헤더 이상 징후를 탐지할 수 있습니다. 패킷 디코더에서 생성된 이벤트에 대한 자세한 내용은 17-16페이지의 패킷 디코딩 이해를 참고하십시오.

UDP 스트림 전처리 구성

라이센스: 보호

UDP 스트림 전처리를 구성할 수 있습니다.

UDP 세션을 추적하기 위해 스트림 전처리기를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘()(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Edit Policy(정책 수정) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 Transport/Network Layer Preprocessors(전송/네트워크 레이어 전처리기)에서 **UDP Stream Configuration(UDP 스트림 구성)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

UDP Stream Configuration(UDP 스트림 구성) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 또는, **Timeout(시간 제한)** 값을 구성하여 1에서 86400까지의 범위에서 시간(단위: 초)을 지정합니다. 이 시간 동안 전처리기가 상태 표에서 비활성화 스트림을 유지합니다. 추가 데이터그램이 지정된 시간 안에 표시되지 않으면, 전처리기는 상태 표에서 스트림을 삭제합니다.

단계 10 또는, **Packet Type Performance Boost(패킷 유형 성능 증대)**를 선택하여 활성화된 규칙에서 지정되지 않은 모든 포트 및 애플리케이션 프로토콜에 대한 TCP 트래픽을 무시합니다. `any`로 설정된 소스 및 대상 포트 둘 다를 가진 UDP 규칙에 `flow` 또는 `flowbits` 옵션이 있는 경우는 제외됩니다. 이러한 성능 향상으로 공격이 누락될 수 있습니다.

단계 11 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

수동 배포 시 전처리 조정

일반적으로, 시스템은 트래픽을 전처리하고 분석하기 위해 네트워크 분석 정책의 정적 설정을 사용합니다. 하지만 적응형 프로파일 기능을 사용하면 트래픽을 호스트 정보에 연결하고 그에 따라 트래픽을 처리하여 네트워크 트래픽에 맞추어 조정할 수 있습니다.

호스트가 트래픽을 받을 때 호스트에서 실행되는 운영 체제가 IP 조각을 리어셈블합니다. 리어셈블리에 사용되는 순서는 운영 체제에 따라 다릅니다. 이와 마찬가지로, 각 운영 체제에서 여러 가지 방법으로 TCP를 구현할 수 있습니다. 따라서 TCP 스트림이 다양한 방식으로 리어셈블됩니다. 전처리기가 대상 호스트의 운영 체제에서 사용하지 않는 형식을 사용하여 데이터를 리어셈블하는 경우 악의적일 수 있는 콘텐츠가 수신 호스트에 리어셈블될 때 시스템에서 이를 놓칠 수 있습니다.

팁

Cisco는 수동 배포 시 적응형 프로파일을 구성할 것을 권장합니다. 인라인 배포의 경우 Cisco는 **Normalize TCP Payload(TCP 페이로드 정규화)** 옵션이 활성화된 인라인 정규화 전처리기를 구성할 것을 권장합니다. 자세한 내용은 17-6페이지의 인라인 트래픽 표준화를 참고하십시오.

적응형 프로파일을 사용하여 패킷 조각 및 TCP 스트림 리어셈블리를 개선하는 방법에 대한 자세한 내용은 다음 주제를 참고하십시오.

적응형 프로파일 이해

라이센스: 보호

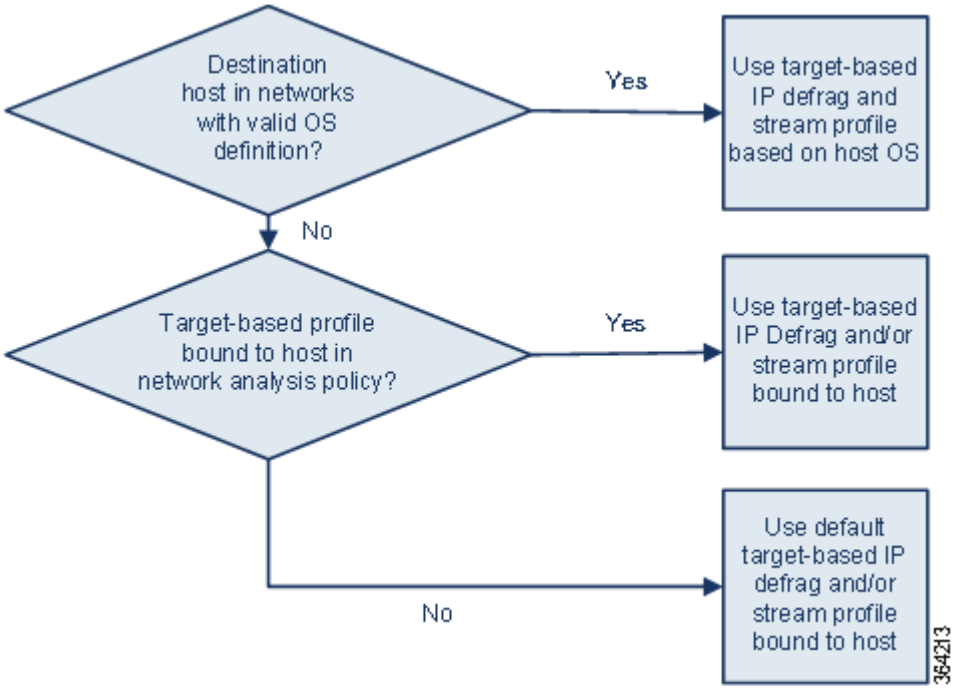
적응형 프로파일은 IP 조각 모음과 TCP 스트림 전처리에 가장 적절한 운영 체제 프로파일을 사용할 수 있도록 해 줍니다. 적응형 프로파일의 영향을 받는 네트워크 분석 정책의 측면에 대한 자세한 내용은 17-12페이지의 IP 패킷 조각 모음 및 17-20페이지의 TCP 스트림 전처리 사용을 참고하십시오.

전처리기에서 적응형 프로파일 사용

라이센스: 보호

적응형 프로파일은 대상 호스트의 운영 체제와 같은 방식으로 IP 패킷을 조각 모음하고 스트림을 리어셈블하는 데 도움이 됩니다. 침입은 엔진을 통제한 다음 대상 호스트에서 사용하는 것과 동일한 형식으로 데이터를 분석합니다.

적응형 프로파일은 다음 다이어그램에 설명된 대로, 대상 호스트를 위한 호스트 프로파일의 운영 체제에 따라 적절한 운영 체제 프로파일로 전환됩니다.



예를 들어, 10.6.0.0/16 서브넷에 적응형 프로파일을 구성하고 기본 IP 조각 모음 대상 기반 정책을 Linux로 설정합니다. 설정을 구성하는 ASA FirePOWER 모듈에는 10.6.0.0/16 서브넷을 포함하는 이 있습니다.

디바이스에서 10.6.0.0/16 서브넷에 없는 호스트 A의 트래픽을 탐지하면 디바이스는 Linux 대상 기반 정책을 사용하여 IP 조각을 리어셈블합니다. 그러나 디바이스에서 10.6.0.0/16 서브넷에 있는 호스트 B의 트래픽을 탐지하면 디바이스는 호스트 B에서 Microsoft Windows XP Professional이 실행되는 것으로 호스트 B의 운영 체제 데이터를 검색합니다. 시스템은 Windows 대상 기반 프로파일을 사용하여 호스트 B로 전송되는 트래픽을 위한 IP 조각 모음을 수행합니다.

IP 조각 모음 전처리기에 대한 자세한 내용은 17-12페이지의 IP 패킷 조각 모음을 참고하십시오. 스트림 전처리기에 대한 자세한 내용은 17-20페이지의 TCP 스트림 전처리 사용을 참고하십시오.

적응형 프로파일 구성

라이센스: 보호

호스트 정보를 통해 IP 조각 모음 및 TCP 스트림 전처리에 사용할 대상 기반 프로파일을 결정하기 위해 적응형 프로파일을 구성할 수 있습니다.

적응형 프로파일을 구성할 때 적응형 프로파일 설정을 특정 네트워크에 바인딩해야 합니다. 성공적으로 적응형 프로파일을 사용하려면 해당 네트워크가 디바이스에 의해 모니터링되는 세그먼트 내에 있어야 합니다.

네트워크에 호스트를 표시할 수 있습니다. 이 네트워크 맵은 액세스 제어 정책을 위해 IP 주소, 주소 블록 또는 네트워크 변수를 기본 침입 정책에 연결된 변수 집합에 구성된 원하는 값으로 지정하여 트래픽을 처리하는 데 적응형 프로파일을 사용해야 하는 맵입니다. 자세한 내용은 13-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을 참고하십시오.

이러한 주소 지정 방법은 단독으로 사용하거나 다음의 예에서처럼 쉼표로 구분된 IP 주소, 주소 블록 또는 변수 목록을 결합하여 사용할 수 있습니다.

```
192.168.1.101, 192.168.4.0/24, $HOME_NET
```

주소 블록을 지정하는 방법에 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

팁 네트워크의 모든 호스트에 변수의 값으로 `any`를 사용하거나 네트워크 값으로 `0.0.0.0/0`을 지정하여 적응형 프로파일을 적용할 수 있습니다.

적응형 프로파일을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)를 선택합니다.**

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 Detection Enhancement Settings(탐지 향상 설정) 옆에 있는 수정 아이콘( )을 클릭합니다.

Detection Enhancement Settings(탐지 향상 설정) 팝업 창이 나타납니다.

단계 5 **Adaptive Profiles(적응형 프로파일) - Enabled(활성화)**를 선택하여 적응형 프로파일을 활성화합니다.

단계 6 또는 **Adaptive Profiles(적응형 프로파일) - Attribute Update Interval(속성 업데이트 간격)** 필드에 데이터를 동기화하는 데 걸리는 시간(단위: 분)을 입력합니다.

참고 이 옵션 값을 높이면 대규모 네트워크의 성능을 개선할 수 있습니다.

단계 7 **Adaptive Profiles(적응형 프로파일) - Networks(네트워크)** 필드에 특정 IP 주소, 주소 블록, 변수 또는 쉼표로 구분된 주소 지정 방법을 모두 포함하는 목록을 입력합니다. 그러면 적응형 프로파일을 사용하려는 네트워크에 있는 모든 호스트를 확인할 수 있습니다.

변수 구성에 대한 자세한 내용은 2-14페이지의 변수 집합 작업을 참고하십시오.

단계 8 **OK(확인)**를 클릭하여 설정을 저장합니다.

19장

침입 정책 시작하기

*침입 정책*은 보안 위반 탐지를 위해 트래픽을 검사하는 침입 탐지 및 방지 구성의 집합으로 정의되며, 인라인 배포에서 악성 트래픽을 차단하거나 변경할 수 있습니다. 침입 정책은 액세스 제어 정책에 따라 호출되며, 트래픽이 목적지에 허가되기 전 시스템의 마지막 방어선입니다.

Cisco는 ASA FirePOWER 모듈과 더불어 여러 침입 정책을 제공합니다. 사용자는 시스템이 제공하는 정책을 사용하여 Cisco VRT(취약성 연구단)의 경험을 활용할 수 있습니다. VRT는 이 정책에 대해, 침입 및 전처리기 규칙 상태를 설정(활성화 또는 비활성화)할 뿐만 아니라, 다른 고급 설정에 대한 초기 구성을 제공합니다. 활성화된 규칙은 시스템이 규칙과 일치하는 트래픽의 침입 이벤트를 생성하도록 (하거나 선택적으로 차단하도록) 합니다. 규칙을 비활성화하면 규칙 처리가 중지됩니다.

팁

시스템이 제공하는 침입 및 네트워크 분석 정책은 이름은 유사하지만 다른 구성을 포함합니다. 예를 들어, Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 네트워크 분석 정책 및 Balanced Security and Connectivity(균형 잡힌 보안 및 연결성) 침입 정책은 함께 작동하며 침입 규칙 업데이트에서 모두 업데이트될 수 있습니다. 하지만, 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다. 11-1페이지의 네트워크 분석 및 침입 정책의 이해는 사용자의 트래픽을 검토하기 위해 네트워크 분석과 침입 정책이 함께 작동하는 방식에 대한 개요뿐 아니라 탐색 패널을 사용하고, 문제를 해결하며, 변경 사항을 커밋하는 것에 대한 일부 기반을 제공합니다.

사용자 지정 침입 정책을 생성하는 경우, 다음을 수행할 수 있습니다.

- 규칙 활성화/비활성화 및 고유의 규칙 작성과 추가를 통해 탐지 기능을 조정할 수 있습니다.
- 외부 경고, 민감한 데이터 전처리 및 전역 규칙 임계값과 같은 다양한 고급 설정을 구성합니다.
- 효율적으로 여러 침입 정책을 관리하기 위해 레이어를 구성 요소로 사용합니다.

침입 정책을 조정할 경우, 특히 규칙을 활성화하고 추가할 경우, 일부 침입 규칙에서는 트래픽이 먼저 특정 방법으로 디코딩되거나 전처리되어야 합니다. 침입 정책이 패킷을 검토하기 전에, 패킷은 네트워크 분석 정책 내 구성에 따라 전처리됩니다. 전처리기를 비활성화한 경우, 전처리기가 네트워크 분석 정책 사용자 인터페이스에서 비활성화된 상태로 남아 있다고 해도, 시스템은 자동으로 전처리기를 현재의 설정으로 사용합니다.

참고

전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 서로 보완해야 합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

사용자 지정 침입 정책을 구성한 후, 하나 이상의 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업과 침입 정책을 연결함으로써 액세스 제어 구성의 일부로 사용할 수 있습니다. 이는 트래픽이 최종 목적지로 전달되기 전에 허용되는 특정 트래픽을 검토하기 위해 시스템이 침입 정책을 강제로 사용하도록 합니다. 침입 정책과 페어링된 변수 집합을 통해 홈 네트워크 및 외부 네트워크와 사용자 네트워크의 서버를 적절하게 반영할 수 있습니다. 자세한 내용은 10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어를 참고하십시오.

이 장에서는 간단한 사용자 지정 침입 정책을 만들고 적용하는 방법을 설명합니다. 또한 이 장에는 수정, 비교 등 침입 정책을 관리하는 데 대한 기본 정보가 포함되어 있습니다. 자세한 내용은 다음을 참고하십시오.

사용자 지정 침입 정책 생성

라이센스: 보호

새로운 침입 정책을 만드는 경우, 사용자는 반드시 고유한 이름을 제공하고, 기본 정책을 지정하며, 삭제 작업을 지정해야 합니다.

기본 정책은 침입 정책의 기본 설정을 정의합니다. 새로운 정책에서 구성을 변경하면 기본 정책 설정을 대체하지만 변경하지는 않습니다. 기본 정책으로 시스템 제공 정책 또는 사용자 지정 정책을 사용할 수 있습니다. 자세한 내용은 12-2페이지의 기본 레이어의 이해를 참고하십시오.

침입 정책의 삭제 작업 또는 **Drop When Inline(인라인 시 삭제)** 설정은 시스템이 삭제 규칙(규칙 상태가 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되어 있는 침입 또는 전처리 규칙) 및 트래픽에 영향을 미치는 다른 침입 정책 구성을 처리하는 방식을 결정합니다. 악성 패킷을 삭제하거나 교체하기를 원할 때 인라인 배포에서 삭제 작업을 활성화해야 합니다. 수동 배포에서, 시스템은 삭제 작업에 관계없이 트래픽 흐름에 영향을 줄 수 없습니다. 자세한 내용은 19-5페이지의 인라인 배포에서 삭제 작업 설정하기를 참고하십시오.

침입 정책을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**를 선택합니다.

Intrusion Policy(침입 정책) 페이지가 나타납니다.

팁 또한 다른 ASA FirePOWER 모듈에서 정책을 가져올 수 있습니다(B-1페이지의 구성 가져오기 및 내보내기 참고).

단계 2 **Create Policy(정책 생성)**를 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, Intrusion Policy(침입 정책) 페이지로 돌아가라는 메시지가 나타나면 **Cancel(취소)**을 클릭합니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Create Intrusion Policy(침입 정책 생성) 팝업 창이 표시됩니다.

단계 3 정책에 고유한 **Name(이름)** 또는 **Description(설명)**을 지정합니다.

단계 4 초기 **Base Policy(기본 정책)**를 지정합니다.

기본 정책으로 시스템 제공 정책 또는 사용자 지정 정책을 사용할 수 있습니다.

주의 **반드시** `Experimental Policy 1(실험 정책 1)`을 Cisco 관계자의 지시 없이는 사용하지 마십시오. Cisco는 이 정책을 테스트용으로 사용합니다.

단계 5 인라인 배포에서 시스템의 삭제 작업을 설정합니다.

- 침입 정책이 트래픽에 영향을 미치고 이벤트를 생성할 수 있게 하려면, **Drop When Inline(인라인 시 삭제)**을 활성화합니다.
- 침입 정책이 트래픽에 영향을 미치지 못하지만 이벤트는 계속해서 생성할 수 있게 하려면, **Drop When Inline(인라인 시 삭제)**을 비활성화합니다.

단계 6 다음과 같이 정책을 생성합니다.

- 새로운 정책을 만들고 Intrusion Policy(침입 정책)로 돌아가려면 **Create Policy(정책 생성)**를 클릭합니다. 새로운 정책의 설정은 기본 정책의 설정과 같습니다.
- **Create and Edit Policy(정책 생성 및 수정)**를 클릭하여 정책을 만들고 고급 침입 정책 편집기에서 이를 열어 수정합니다(19-4페이지의 침입 정책 수정 참고).

침입 정책 관리

라이센스: 보호

침입 정책 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**)에서 다음 정보와 함께 현재 사용자 지정 침입 정책을 볼 수 있습니다.

- 정책이 최종 수정된 시간과 날짜(로컬 시간)
- **Drop When Inline(인라인 시 삭제)** 설정의 활성화 여부. 이는 인라인 배포에서 트래픽을 삭제하고 수정할 수 있도록 합니다
- 트래픽을 검사하기 위해 침입 정책을 사용하는 액세스 제어 정책 의 유형
- 정책에 저장되지 않은 변경 사항이 있는지 여부

Intrusion Policy(침입 정책) 페이지의 옵션을 통해 다음 표에 있는 조치를 취할 수 있습니다.

표 19-1 침입 정책 관리 작업

목적	방법	참고 사항
새로운 침입 정책 생성하기	**Create Policy(정책 생성)**를 클릭합니다.	19-2페이지의 사용자 지정 침입 정책 생성
기존 침입 정책 수정하기	수정 아이콘( )을 클릭합니다.	19-4페이지의 침입 정책 수정
침입 정책 재적용하기	적용 아이콘( )을 클릭합니다.	19-8페이지의 침입 정책 적용

표 19-1 침입 정책 관리 작업 (계속)

목적	방법	참고 사항
다른 ASA FirePOWER 모듈에 가져오기 위해 침입 정책 내보내기	내보내기 아이콘( )을 클릭합니다.	B-1페이지의 구성 내보내기
침입 정책의 현재 구성 설정을 표시하는 PDF 보고서 보기	보고서 아이콘( )을 클릭합니다.	19-8페이지의 현재 침입 설정 보고서 생성
두 가지 침입 정책의 설정을 비교하거나 동일한 정책의 두 가지 수정 버전 비교하기	**Compare Policies(정책 비교)**를 클릭합니다.	19-9페이지의 두 침입 정책 또는 수정 버전 비교
침입 정책 삭제하기	삭제 아이콘( )을 클릭한 다음 정책을 삭제할 것인지 확인합니다. 액세스 제어 정책이 침입 정책을 참조하는 경우 이를 삭제할 수 없습니다.	

침입 정책 수정

라이센스: 보호

새 침입 정책을 생성할 때, 기본 정책과 동일한 침입 규칙 및 고급 설정을 갖습니다. 다음 표는 침입 정책을 수정할 때 취할 수 있는 가장 일반적인 작업을 설명합니다.

표 19-2 침입 정책 수정 작업

목적	방법	참고 사항
인라인 배포에서 삭제 작업 지정하기	Policy Information(정책 정보) 페이지에서 **Drop when Inline(인라인 시 삭제)** 확인 상자를 선택하거나 선택 해제합니다.	19-5페이지의 인라인 배포에서 삭제 작업 설정하기
기본 정책 변경하기	Policy Information(정책 정보) 페이지의 **Base Policy(기본 정책)** 드롭다운 목록에서 기본 정책을 선택합니다.	12-4페이지의 기본 정책 변경
기본 정책 설정 보기	Policy Information(정책 정보) 페이지에서 **Manage Base Policy(기본 정책 관리)**를 클릭합니다.	12-2페이지의 기본 레이어의 이해
침입 규칙 표시 또는 구성하기	Policy Information(정책 정보) 페이지에서 **Manage Rules(규칙 관리)**를 클릭합니다.	20-3페이지의 침입 정책에서 규칙 보기
침입 규칙의 필터링된 보기를 현재 규칙 상태로 표시하고, 선택적으로 해당 규칙 설정하기	Policy Information(정책 정보) 페이지에서 **View(보기)**를 클릭합니다. 이는 **Manage Rules(규칙 관리)** 아래의 규칙 수 옆에 있으며, Generate Events(이벤트 생성) 또는 Drop and Generate Events(이벤트 삭제 및 생성)를 위해 설정되어 있습니다.	20-9페이지의 침입 정책에서 규칙 필터링
고급 설정을 활성화, 비활성화 또는 수정하기	탐색 패널에 있는 **Advanced Settings(고급 설정)**를 클릭합니다.	19-7페이지의 침입 정책 내 고급 설정 구성
정책 레이어 관리하기	탐색 패널에 있는 **Policy Layers(정책 레이어)**를 클릭합니다.	12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용

침입 정책을 조정할 경우, 특히 규칙을 활성화하고 추가할 경우, 일부 침입 규칙에서는 트래픽이 먼저 특정 방법으로 디코딩되거나 전처리되어야 합니다. 침입 정책이 패킷을 검토하기 전에, 패킷은 네트워크 분석 정책 내 구성에 따라 전처리됩니다. 전처리기를 비활성화한 경우, 전처리기가 네트워크 분석 정책 사용자 인터페이스에서 비활성화된 상태로 남아 있다고 해도, 시스템은 자동으로 전처리기를 현재의 설정으로 사용합니다.

참고 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 서로 보완해야 합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

시스템은 하나의 침입 정책을 캐시합니다. 침입 정책을 수정하는 동안 모든 메뉴 또는 다른 페이지로 이동하는 다른 경로를 선택하는 경우, 해당 페이지를 벗어난다고 해도 변경 사항은 시스템 캐시에 유지됩니다. 위 표에서 수행할 수 있는 작업 외에도, 11-1페이지의 네트워크 분석 및 침입 정책의 이해는 문제 해결 및 변경 사항 커밋에 관한 정보를 제공합니다.

침입 정책을 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**를 선택합니다.

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 구성하려는 침입 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

침입 정책 편집기가 Policy Information(정책 정보) 페이지 및 왼쪽 탐색 패널에 집중적으로 나타납니다.

단계 3 정책을 수정합니다. 상기 요약된 모든 작업을 수행합니다.

단계 4 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

인라인 배포에서 삭제 작업 설정하기

라이센스: 보호

인라인 배포에서 침입 정책은 트래픽을 차단하고 수정할 수 있습니다.

- *삭제 규칙*은 일치하는 패킷을 삭제하고 침입 이벤트를 생성할 수 있습니다. 침입 또는 전처리기 삭제 규칙을 구성하려면, 해당 상태를 Drop and Generate Events(이벤트 삭제 및 생성)로 설정합니다(20-19페이지의 규칙 상태 설정 참고).
- 침입 규칙은 악성 콘텐츠를 대체하기 위해 `replace` 키워드를 사용할 수 있습니다(23-29페이지의 인라인 배포에서 콘텐츠 대체 참고).

트래픽에 영향을 미치는 침입 규칙의 경우, 콘텐츠를 대체하는 규칙 및 삭제 규칙을 올바르게 구성해야 하며 시스템 인라인을 올바르게 구축해야 합니다. 마지막으로, 침입 정책의 *삭제 작업*을 활성화하거나 **Drop when Inline(인라인 시 삭제)** 설정을 활성화해야 합니다.

참고 FTP를 통한 악성코드 파일 전송을 차단하려면, 네트워크 기반의 지능형 악성코드 차단(AMP)을 올바르게 구성해야 할뿐만 아니라 액세스 제어 정책의 기본 침입 정책에서 **Drop when Inline(인라인 시 삭제)**을 활성화해야 합니다. 기본 침입 정책을 결정하거나 변경하려면, 13-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을 참고하십시오.

구성이 인라인 배포에서 실제로는 트래픽에 영향을 주지 않으면서 어떻게 작동하는지 평가하려는 경우 삭제 작업을 비활성화하면 됩니다. 이 경우, 시스템은 침입 이벤트를 생성하지만 삭제 규칙을 트리거하는 패킷을 삭제하지는 않습니다. 결과에 만족하는 경우, 삭제 작업을 활성화할 수 있습니다.

수동 배포에서 시스템은 삭제 작업에 관계없이 트래픽에 영향을 줄 수 없습니다. 즉 수동 배포에서 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙은 Generate Events(이벤트 생성)로 설정된 규칙과 동일하게 작동합니다. 말하자면 시스템은 침입 이벤트를 생성하지만 패킷을 삭제하지는 않습니다.

침입 이벤트를 볼 때, 워크플로는 *인라인 결과*를 포함할 수 있는데, 이는 트래픽이 실제로 삭제되었는지 여부 또는 단지 트래픽이 삭제되었을 가능성이 있는지 여부를 나타냅니다. 패킷이 삭제 규칙에 일치하는 경우, 인라인 결과는 다음과 같습니다.

- `Dropped(삭제)`. 삭제 작업이 활성화되었을 때 올바르게 구성된 인라인 배포에서 삭제된 패킷의 경우
- `Would have dropped(삭제되었을 가능성)`. 사용자의 디바이스가 수동으로 구축되었거나 삭제 작업이 비활성화되었기 때문에 삭제되지 않은 패킷의 경우 배포에 관계없이 시스템이 잘라내는 동안 표시된 패킷의 경우 인라인 결과는 항상 `Would have dropped`로 표시됩니다.

인라인 배포에서 침입 정책의 삭제 작업을 설정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**를 선택합니다.

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 정책의 삭제 작업을 설정합니다.

- 침입 규칙이 트래픽에 영향을 미치고 이벤트를 생성할 수 있게 하려면, **Drop When Inline(인라인 시 삭제)**을 활성화합니다.
- 침입 규칙이 트래픽에 영향을 미치지 못하지만 이벤트는 계속해서 생성할 수 있게 하려면, **Drop When Inline(인라인 시 삭제)**을 비활성화합니다.

단계 4 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

침입 정책 내 고급 설정 구성

라이센스: 보호

침입 정책의 *고급 설정*을 구성하려면 특정한 전문성이 필요합니다. 침입 정책에 대한 기본 정책은 기본적으로 활성화되는 고급 설정 및 각각에 대한 기본 구성을 결정합니다.

침입 정책의 탐색 패널에 있는 **Advanced Settings(고급 설정)**를 선택하는 경우, 정책은 유형별 고급 설정을 나열합니다. Advanced Settings(고급 설정) 페이지에서 침입 정책의 고급 설정을 활성화하거나 비활성화할 수 있으며, 고급 설정 구성 페이지에 액세스할 수도 있습니다.

고급 설정은 구성할 수 있도록 활성화되어 있어야 합니다. 고급 설정을 활성화하면, 고급 설정을 위한 구성 페이지로 연결되는 하위 링크가 탐색 패널의 **Advanced Settings(고급 설정)** 링크 아래에 나타나고, Advanced Settings(고급 설정) 페이지의 고급 설정 옆에 구성 페이지로 연결되는 **Edit(수정)** 링크가 나타납니다.

팁 기본 정책의 설정에 고급 설정의 구성을 되돌리려면, 고급 설정을 위한 구성 페이지에서 **Revert to Defaults(기본값으로 되돌리기)**를 클릭합니다. 메시지가 표시되면 복원할 것인지 확인합니다.

고급 설정을 비활성화하면 하위 링크 및 **Edit(수정)** 링크는 더 이상 표시되지 않지만, 구성은 유지됩니다. 일부 침입 정책 구성(침입 규칙에 대한 중요한 데이터 규칙, SNMP 경고)은 활성화되고 고급 설정을 정확하게 구성해야 합니다. 이런 방식으로 잘못 구성된 침입 정책은 저장할 수 없습니다 (11-14페이지의 문제 해결 및 정책 변경 사항 커밋 참고).

고급 설정에서 구성을 수정하는 데는 수정하고 있는 구성과 네트워크에 미칠 잠재적 영향에 대한 이해가 필요합니다. 다음 섹션에서는 각 고급 설정을 위한 특정 구성의 세부 사항으로 연결되는 링크를 제공합니다.

특정 위협 탐지

중요한 데이터 전처리기는 신용 카드 번호 및 ASCII 문자로 표시된 Social Security numbers(사회 보장 번호)와 같은 중요한 데이터를 탐지합니다. 전처리기 구성에 관한 정보는 21-20페이지의 민감한 데이터 검색을 참고하십시오.

특정 위협(Back Orifice 공격, 여러 포트스캔 유형 및 과도한 트래픽으로 네트워크를 마비시키려고 하는 속도 기반 공격)을 탐지하는 다른 전처리기는 네트워크 분석 정책 내에 구성됩니다. 자세한 내용은 21-1페이지의 특정 위협 탐지를 참고하십시오.

침입 규칙 임계값

전역 규칙 임계값은 임계값을 사용하여 시스템이 로깅하고 침입 이벤트를 표시하는 횟수를 제한할 수 있도록 하여 많은 이벤트로 인해 시스템이 마비되는 것을 방지합니다. 자세한 내용은 22-1페이지의 침입 이벤트 로깅의 전역적 제한을 참고하십시오.

외부 응답

사용자 인터페이스에서 침입 이벤트의 다양한 보기 외에도, 시스템 로그(syslog) 기능에 로깅을 활성화하거나 SNMP 트랩 서버에 이벤트 데이터를 보낼 수 있습니다. 정책별로 침입 이벤트 알림 제한을 지정하고, 외부 로깅 기능에 침입 이벤트 알림을 설정하며, 침입 이벤트에 외부 응답을 구성할 수 있습니다. 자세한 내용은 다음을 참고하십시오.

- 28-3페이지의 SNMP 응답 구성
- 28-6페이지의 Syslog 응답 구성

침입 정책 적용

라이센스: 보호

침입 정책(액세스 제어(4-10페이지의 액세스 제어 정책 적용 참고) 사용)을 적용한 후 언제든지 침입 정책을 다시 적용할 수 있습니다. 이를 통해 액세스 제어 정책의 재적용 없이 모니터링된 네트워크에서 침입 정책을 변경할 수 있습니다. 재적용하는 동안 침입 정책이 마지막으로 적용된 이후 변경된 사항을 검토하기 위해 비교 보고서를 볼 수도 있습니다.

침입 정책 재적용 시 다음에 유의하십시오.

- 침입 정책 재적용 작업이 정기적으로 되풀이될 수 있도록 일정을 잡을 수 있습니다(31-5페이지의 침입 정책 적용의 자동화 참고).
- 규칙 업데이트를 가져올 때, 가져오기가 완료된 후 자동으로 침입 정책을 적용할 수 있습니다. 이 옵션을 활성화하지 않은 경우, 규칙 업데이트에 의해 수정된 정책을 수동으로 재적용해야 합니다. 자세한 내용은 35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기를 참고하십시오.

침입 정책을 재적용하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**를 선택합니다.

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 재적용하려는 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

Reapply Intrusion Policy(침입 정책 재적용) 창이 나타납니다.

단계 3 **Reapply(재적용)**를 클릭합니다.

정책이 재적용됩니다. 작업 큐(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)을 사용하여 적용 상태를 모니터링할 수 있습니다. 자세한 내용은 C-1페이지의 작업 큐 보기를 참고하십시오.

현재 침입 설정 보고서 생성

라이센스: 보호

침입 정책 보고서는 특정 시점의 정책 구성에 대한 레코드입니다. 시스템은 기본 정책의 설정과 정책 레이어의 설정을 결합하며, 어느 설정이 기본 정책 또는 정책 레이어에서 시작된 것인지 구별하지 않습니다.

사용자는 감사 목적으로나 현재 구성을 검사하기 위해 다음 정보를 포함하는 보고서를 사용할 수 있습니다.

표 19-3 침입 정책 보고서 섹션

섹션	설명
정책 정보	침입 정책의 이름 및 설명, 정책을 최종 수정한 사용자의 이름, 정책이 마지막으로 수정된 날짜 및 시간을 제공합니다. 또한 인라인 배포에서 패킷 삭제의 활성화 또는 비활성화 여부, 현재 규칙 업데이트 버전, 기본 정책이 현재 규칙 업데이트에 대해 잠겨 있는지 여부를 나타냅니다.
고급 설정	모든 활성화된 침입 정책의 고급 설정 및 구성을 나열합니다.
규칙	모든 활성화된 규칙 및 해당 작업의 목록을 제공합니다.

또한 두 개의 침입 정책 또는 동일한 정책의 두 가지 수정 버전을 비교하는 비교 보고서를 생성할 수 있습니다. 자세한 내용은 19-9페이지의 두 침입 정책 또는 수정 버전 비교를 참고하십시오.

침입 정책 보고서를 보려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**를 선택합니다.

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 보고서를 생성하려는 침입 정책 옆에 있는 보고서 아이콘( )을 클릭합니다. 침입 정책 보고서를 생성하기 전에 모든 잠재적인 변경 사항을 커밋하십시오. 확인된 변경 사항만 보고서에 표시됩니다.

시스템은 침입 정책 보고서를 생성합니다. 사용자에게 보고서를 컴퓨터에 저장하라는 메시지가 표시됩니다.

두 침입 정책 또는 수정 버전 비교

라이센스: 보호

사용자 조직의 표준 준수를 위한 정책 변경 사항을 검토하거나 시스템 성능을 최적화하기 위해 두 침입 정책 간 차이를 검토할 수 있습니다. 사용자가 액세스할 수 있는 침입 정책의 경우, 두 개의 침입 정책 또는 동일한 정책의 두 가지 수정 버전을 비교할 수 있습니다. 비교한 후 선택적으로 두 정책 또는 정책 수정 버전의 차이를 기록하는 PDF 보고서를 생성할 수 있습니다.

침입 정책을 비교하는 데 사용할 수 있는 두 가지 툴이 있습니다.

- 비교 보기는 두 개의 침입 정책 또는 두 가지 침입 정책 수정 버전 간 차이점을 나란한 형식으로 표시합니다. 각 정책의 이름은 비교 보기의 왼쪽 끝에 있는 제목 표시줄에 표시됩니다.

  이를 사용하여 사용자 인터페이스에서 두 가지 정책 수정 버전을 모두 보고 탐색할 수 있습니다. 차이점은 강조 표시됩니다.

- 비교 보고서는 두 개의 침입 정책 또는 두 가지 침입 정책 수정 버전 간 차이점에 대한 레코드만 침입 정책 보고서와 유사한 형식으로 생성하는데, PDF 형식으로 생성합니다.

  정책 비교를 저장, 복사, 인쇄, 공유하는 데 이 보고서를 사용하여 추가 검사를 수행할 수 있습니다.

침입 정책 비교 도구의 이해와 사용에 관한 자세한 내용은 다음을 참고하십시오.

- 19-10페이지의 침입 정책 비교 보기 사용
- 19-10페이지의 침입 정책 비교 보고서 사용

침입 정책 비교 보기 사용

라이센스: 보호

비교 보기는 두 개의 침입 정책 모두 또는 두 가지 침입 정책 수정 버전 간 차이점을 나란한 형식으로 표시합니다. 각 정책 또는 정책 수정 버전의 이름은 비교 보기의 왼쪽 끝에 있는 제목 표시줄에 표시됩니다. 마지막 수정 시간 및 수정한 최종 사용자는 정책 이름 오른쪽에 표시됩니다. Intrusion Policy(침입 정책) 페이지는 정책이 최종 수정된 시간을 로컬 시간으로 표시하지만 침입 정책 보고서는 해당 시간을 UTC로 표시한다는 점에 유의하십시오. 두 개의 침입 정책 또는 두 가지 침입 정책 수정 버전 간 차이점은 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책 또는 정책 수정 버전 사이에서 다름을 나타내고, 그러한 차이점은 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 한 정책 또는 정책 수정 버전에서는 나타나지만 다른 곳에서는 나타나지 않음을 표시합니다.

다음 표에서 설명된 모든 작업을 수행할 수 있습니다.

표 19-4 침입 정책 비교 보기 작업

목적	방법
수정 사항을 개별적으로 탐색하기	제목 표시줄 상단의 **Previous(이전)** 또는 **Next(다음)**를 클릭합니다. 좌우 측면 사이에 있는 이중 화살표 아이콘()을 움직여 **Difference(차이)** 수를 조정하여 표시되는 차이점이 무엇인지 확인합니다.
새 침입 정책 비교 보기 생성하기	**New Comparison(새로 비교)을 클릭합니다.** **Select Comparison(비교 선택)** 창이 나타납니다. 자세한 내용은 침입 정책 비교 보고서 사용을 참고하십시오.
침입 정책 비교 보고서 생성하기	**Comparison Report(비교 보고서)를 클릭합니다.** 정책 비교 보고서는 두 정책 또는 정책 수정 버전 사이의 차이만을 표시하는 PDF를 만듭니다.

침입 정책 비교 보고서 사용

라이센스: 보호

침입 정책 비교 보고서는 두 개의 침입 정책 또는 동일한 침입 정책의 두 가지 수정 버전 간 차이에 대한 레코드입니다. 이 차이는 침입 정책 비교 보기로 식별되며, PDF로 표시됩니다. 이 보고서를 사용하여 두 침입 정책 구성 간 차이를 자세히 검토하고 결과를 저장하거나 전달할 수 있습니다.

사용자가 액세스한 모든 침입 정책에 대해 비교 보기에서 침입 정책 비교 보고서를 생성할 수 있습니다. 침입 정책 보고서를 생성하기 전에 모든 잠재적인 변경 사항을 커밋하십시오. 확인된 변경 사항만 보고서에 표시됩니다.

침입 정책 비교 보고서의 형식은 침입 정책 보고서와 동일한데, 한 가지 예외가 있습니다. 침입 정책 보고서는 침입 정책의 모든 구성을 포함하며, 침입 정책 비교 보고서는 정책 간 차이가 나는 설정만 나열합니다.

구성에 따라, 침입 정책 비교 보고서는 침입 정책 보고서 섹션 표에 설명된 대로 하나 이상의 섹션을 포함할 수 있습니다.

팁 액세스 제어, 네트워크 분석, 파일, 또는 시스템 정책을 비교하기 위해 유사한 절차를 사용할 수 있습니다.

두 가지 침입 정책 또는 동일한 정책의 두 가지 수정 버전을 비교하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**를 선택합니다.

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 **Compare Policies(정책 비교)**를 클릭합니다.

Select Comparison(비교 선택) 창이 나타납니다.

단계 3 **Compare Against(비교 대상)** 드롭다운 목록에서 비교를 원하는 유형을 선택합니다.

- 두 가지의 서로 다른 정책을 비교하려면, **Other Policy(다른 정책)**를 선택합니다.
- 동일한 정책의 두 가지 수정 버전을 비교하려면, **Other Revision(다른 수정 버전)**을 선택합니다.

침입 정책 보고서를 생성하기 전에 모든 잠재적인 변경 사항을 커밋하십시오. 확인된 변경 사항만 보고서에 표시됩니다.

단계 4 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 가지의 서로 다른 정책을 비교할 경우, **Policy A(정책 A)**와 **Policy B(정책 B)** 드롭다운 목록에서 비교하려는 정책을 선택합니다.
- 동일한 정책의 두 가지 수정 버전을 비교하는 경우, **Policy(정책)** 드롭다운 목록에서 정책을 선택한 다음 **Revision A(수정 버전 A)** 및 **Revision B(수정 버전 B)** 드롭다운 목록에서 비교하려는 수정 버전을 선택합니다.

단계 5 침입 정책 비교 보기를 표시하려면 **OK(확인)**를 클릭합니다.

비교 보기가 나타납니다.

단계 6 침입 정책 비교 보고서를 생성하려면 **Comparison Report(비교 보고서)**를 클릭합니다.

단계 7 침입 정책 보고서가 표시됩니다. 사용자에게 보고서를 컴퓨터에 저장하라는 메시지가 표시됩니다.

규칙을 사용한 침입 정책 조정

침입 정책에서 Rules(규칙) 페이지에서는 공유 객체 규칙, 표준 텍스트 규칙, 그리고 프리프로세서 규칙의 규칙 상태 및 기타 설정을 구성할 수 있습니다.

규칙 상태를 Generate Events(이벤트 생성) 또는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정하여 규칙을 활성화합니다. 규칙을 활성화하면 시스템은 규칙과 일치하는 트래픽에 대해 이벤트를 생성합니다. 규칙을 비활성화하면 규칙 처리가 중지됩니다. 선택적으로, 침입 정책을 설정하여 인라인 배포에서 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙이 이벤트를 생성하고 삭제하며 트래픽과 일치하도록 할 수 있습니다. 자세한 내용은 19-5페이지의 인라인 배포에서 삭제 작업 설정하기를 참고하십시오. 수동 배포에서, Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙은 일치 트래픽에만 이벤트를 생성합니다.

하위 집합을 표시하도록 규칙을 필터링하면 규칙 상태 또는 규칙 설정을 변경하고자 하는 정확한 규칙 집합을 선택할 수 있습니다.

침입 규칙 또는 규칙 인수를 사용하려면 비활성화된 전처리기가 필요한 경우 네트워크 분석 정책 사용자 인터페이스에서 비활성화 상태로 남아 있다고 해도, 시스템은 자동으로 전처리기를 현재 구성으로 사용한다는 점에 유의하십시오. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 20-2페이지의 침입 방지 규칙 유형의 이해에서는 사용자가 침입 정책에서 확인하고 구성할 수 있는 침입 규칙 및 전처리기 규칙에 대해 설명합니다.
- 20-3페이지의 침입 정책에서 규칙 보기에서는 Rules(규칙) 페이지에서 규칙의 순서를 변경하고, 페이지에서 아이콘을 해석하고, 규칙 세부사항에 집중하는 방법에 대해 설명합니다.
- 20-9페이지의 침입 정책에서 규칙 필터링에서는 규칙 필터를 사용하여 규칙 설정을 적용할 규칙을 검색하는 방법에 대해 설명합니다.
- 20-19페이지의 규칙 상태 설정에서는 Rules(규칙) 페이지에서 규칙을 활성화 및 비활성화하는 방법에 대해 설명합니다.
- 20-21페이지의 정책에 따른 침입 이벤트 알림 필터링에서는 특정 규칙에 대한 이벤트 필터링 임계값을 설정하고 특정 규칙에서 억제를 설정하는 방법에 대해 설명합니다.
- 20-28페이지의 동적 규칙 상태 추가에서는 일치하는 트래픽에서 규칙 변칙이 탐지될 때 동적으로 트리거되는 규칙 상태를 설정하는 방법에 대해 설명합니다.
- 20-32페이지의 SNMP 알림 추가에서는 SNMP 경고를 특정 규칙과 연결하는 방법에 대해 설명합니다.
- 20-33페이지의 규칙 코멘트 추가에서는 침입 정책에서 규칙에 코멘트를 추가하는 방법에 대해 설명합니다.

침입 방지 규칙 유형의 이해

라이센스: 보호

침입 정책의 규칙에는 침입 규칙과 전처리기 규칙과 같이 두 가지 유형이 있습니다.

침입 규칙은 네트워크에서 취약성 악용 시도를 탐지하는 키워드와 인수의 지정된 집합이며, 네트워크 트래픽을 분석하여 규칙의 기준과 일치하는지를 확인합니다. 시스템은 패킷을 각 규칙에 지정된 조건과 비교하며, 패킷 데이터가 규칙에 지정된 모든 조건에 일치하는 경우 규칙이 트리거됩니다. 시스템에는 CiscoVRT(취약성 연구단)에서 만든 두 가지 유형의 침입 규칙이 포함되어 있습니다. 첫 번째 유형은 컴파일되어 있고 수정할 수 없는 공유 객체 규칙(소스, 대상 포트 및 IP 주소와 같은 규칙 헤더 정보 제외)이고 두 번째 유형은 규칙의 새로운 사용자 지정 인스턴스로 저장되어 있고 수정할 수 있는 표준 텍스트 규칙입니다.

시스템에는 전처리기 및 패킷 디코더 탐지 옵션과 관련된 규칙인 전처리기 규칙도 포함되어 있습니다. 전처리기 규칙을 복사하거나 수정할 수 없습니다. 대부분의 전처리기 규칙은 기본적으로 비활성화되어 있으며, 시스템에서 전처리기 규칙을 위한 이벤트를 생성하고 인라인 배포에서 문제가 되는 패킷을 삭제하고자 할 경우 활성화(즉, Generate Events(이벤트 생성) 또는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정)해야 합니다.

VRT는 시스템에 포함된 각 기본 침입 정책에 대해 Cisco의 공유 객체 규칙, 표준 텍스트 규칙 및 프리프로세서 규칙에 대한 기본 규칙 상태를 결정합니다.

다음 표는 ASA FirePOWER 모듈에 포함된 규칙의 각 유형에 대해 설명합니다.

표 20-1 규칙 유형

유형	설명
공유 객체 규칙	C 소스 코드에서 컴파일되어 이진 모듈로 제공되는 CiscoVRT(취약성 연구단)가 생성한 침입 규칙. 공유 객체 규칙을 사용하여 표준 텍스트 규칙이 수행할 수 없는 방식으로 공격을 탐지할 수 있습니다. 공유 객체 규칙에서 규칙 키워드 및 인수를 수정할 수 없습니다. 수행 가능한 작업은 규칙에서 사용되는 변수의 변경, 또는 소스, 대상 포트 및 IP 주소와 같은 부분의 변경, 그리고 규칙의 새로운 인스턴스를 사용자 지정 공유 객체 규칙으로 저장하는 것으로 제한됩니다. 공유 객체 규칙은 GID(생성기 ID) 3을 갖습니다. 자세한 내용은 23-103페이지의 기존 규칙 변경을 참고하십시오.
표준 텍스트 규칙	VRT에 의해 생성되거나, 새로운 사용자 정의 규칙으로 복사 및 저장되거나, 규칙 편집기를 사용하여 생성되거나 로컬 컴퓨터에서 생성하여 가져오는 로컬 규칙으로 가져온 침입 규칙. VRT에 의해 생성된 표준 규칙에서 규칙 키워드 및 인수를 수정할 수 없습니다. 수행할 수 있는 작업은 규칙에서 사용되는 변수의 변경, 또는 소스, 대상 포트 및 IP 주소와 같은 부분의 변경, 그리고 규칙의 새로운 인스턴스를 사용자 지정 표준 텍스트 규칙으로 저장하는 것으로 제한됩니다. 자세한 내용은 23-103페이지의 기존 규칙 변경, 23-1페이지의 침입 규칙의 이해와 작성 및 35-15페이지의 로컬 규칙 파일 가져오기를 참고하십시오. VRT에 의해 생성된 표준 텍스트 규칙은 GID(생성기 ID) 1을 갖습니다. 규칙 편집기를 사용하여 생성하거나 로컬 규칙으로서 가져오는 사용자 지정 표준 텍스트 규칙에는 SID(Signature ID) 1000000 이상이 있습니다.
전처리기 규칙	패킷 디코더의 탐지 옵션 또는 ASA FirePOWER 모듈에 포함된 전처리기 중 하나와 연결된 규칙. 전처리기 규칙이 이벤트를 생성하기를 원할 경우 전처리기 규칙을 활성화해야 합니다. 이 규칙에는 해독기 특정 또는 전처리기 특정 GID(생성기 ID)가 있습니다.

침입 정책에서 규칙 보기

라이센스: 보호

침입 정책에서 규칙이 표시되는 방법을 조정할 수 있으며, 여러 기준으로 규칙을 정렬할 수 있습니다. 또한 규칙 설정, 규칙 문서 및 기타 규칙 사양을 보려면 특정 규칙에 대한 세부사항을 표시할 수 있습니다.

Rules(규칙) 페이지에는 다음과 같은 4가지 주요 기능 영역이 있습니다.

- 필터링 기능 - 자세한 내용은 20-9페이지의 침입 정책에서 규칙 필터링을 참고하십시오.
- 규칙 특성 메뉴 - 자세한 내용은 20-19페이지의 규칙 상태 설정, 20-21페이지의 정책에 따른 침입 이벤트 알림 필터링, 20-28페이지의 동적 규칙 상태 추가, 20-32페이지의 SNMP 알림 추가 및 20-33페이지의 규칙 코멘트 추가 참조
- 규칙 목록 - 자세한 내용은 규칙 페이지 열 표 참조
- 규칙 세부사항 - 자세한 내용은 20-5페이지의 규칙 세부 정보 보기 참조

또한 서로 다른 기준으로 규칙을 정렬할 수 있습니다. 자세한 내용은 20-4페이지의 규칙표시 분류를 참조하십시오.

열 헤더로 사용되는 아이콘은 메뉴 모음의 메뉴에 해당하며, 이 메뉴를 통해 구성 항목에 액세스할 수 있습니다. 예를 들어, Rule State(규칙 상태) 메뉴는 Rule State(규칙 상태) 열과 동일한 아이콘(➡)으로 표시됩니다.

다음 표는 Rules(규칙) 페이지의 열에 대해 설명합니다.

표 20-2 규칙 페이지 열

제목	설명	자세한 내용은 다음을 참고하십시오.
GID	규칙의 GID(Generator ID)를 나타내는 정수.	26-1페이지의 이벤트 보기
SID	규칙에 대한 고유 식별자 역할을 하는, Snort ID(SID)를 나타내는 정수.	26-1페이지의 이벤트 보기
메시지	규칙 이름으로도 작동하는 이 규칙에서 생성된 이벤트에 포함된 메시지.	23-11페이지의 이벤트 메시지 정의
➡	규칙의 규칙 상태로, 다음 세 가지 상태 중 하나일 수 있습니다. • 이벤트 삭제 및 생성(❌) • 이벤트 생성(➡) • 비활성화(➡) 해당 규칙 상태 아이콘을 클릭하여 규칙을 위한 Set(집합) 규칙 상태 대화 상자에 액세스할 수 있다는 점에 유의하십시오.	20-19페이지의 규칙 상태 설정
	규칙에 적용된 이벤트 임계값 및 이벤트 삭제를 포함하는 이벤트 필터.	20-21페이지의 정책에 따른 침입 이벤트 알림 필터링
	특정 속도 이상이 발생한 경우 효과를 나타내는 규칙을 위한 동적 상태 규칙.	20-28페이지의 동적 규칙 상태 추가
	규칙에 구성된 경고(현재 SNMP 경고 한정).	20-32페이지의 SNMP 알림 추가
	규칙에 추가된 코멘트.	20-33페이지의 규칙 코멘트 추가

또한 레이어 드롭다운 목록을 사용하여 침입 정책의 다른 레이어를 위해 Rules(규칙) 페이지로 전환할 수 있습니다. 정책에 레이어를 추가하지 않는 한, 드롭다운 목록에 나열된 유일한 수정 가능한 보기는 정책 Rules(규칙) 페이지이며 원래 `My Changes(내 변경 사항)`라는 이름의 정책 레이어에 대한 Rules(규칙) 페이지입니다. 이 보기 중 하나에서 내용을 변경하는 것은 다른 보기에서 내용을 변경하는 것과 같다는 점에 유의하십시오. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오. 드롭다운 목록은 또한 읽기 전용 기본 정책을 위한 Rules(규칙) 페이지를 나열합니다. 기본 정책에 대한 내용은 12-2페이지의 기본 레이어의 이해를 참고하십시오.

침입 정책에서 규칙을 보려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 Policy Information(정책 정보) 페이지에서 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다. 기본적으로, 페이지는 메시지를 기준으로 규칙을 알파벳 순으로 나열합니다.

탐색 패널에서 분계선 위의 **Rules(규칙)**를 선택하여 동일한 규칙 나열을 확인할 수 있다는 점에 유의하십시오. 이 보기에서 정책의 모든 규칙 속성을 보고 설정할 수 있습니다.

규칙표시 분류

라이센스: 보호

주요 제목 또는 아이콘을 클릭하여 Rules(규칙) 페이지의 모든 열로 규칙을 정렬할 수 있습니다.

제목 또는 아이콘의 위(▲) 또는 아래(▼) 화살표로 정렬이 해당 방향의 해당 열에 있음을 나타낼 수 있다는 점에 유의하십시오.

침입 정책에서 규칙을 정렬하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다. 기본적으로, 페이지는 메시지를 기준으로 규칙을 알파벳 순으로 나열합니다.

단계 4 정렬하려는 열의 상단에서 제목 또는 아이콘을 클릭합니다.

열 머리글에 나타나는 화살표의 방향으로 규칙이 열에서 정렬됩니다. 반대 방향으로 정렬하려면 머리글을 다시 클릭합니다. 정렬 순서 및 화살표가 반대 방향으로 됩니다.

규칙 세부 정보 보기

라이센스: 보호

Rule Detail(규칙 세부 정보) 보기에서 규칙 문서 및 규칙 오버헤드를 볼 수 있습니다. 또한 규칙 특정 기능을 보고 추가할 수 있습니다.

취약성에 매핑되지 않는 한 로컬 규칙에는 오버헤드가 없습니다.

표 20-3 규칙 세부사항

항목	설명	자세한 내용은 다음을 참고하십시오.
요약	규칙 요약. 규칙 기반 이벤트의 경우, 규칙 문서에 요약 정보가 포함되어 있으면 이 행이 나타납니다.	26-1페이지의 이벤트 보기
규칙 상태	해당 규칙에 대한 현재 규칙 상태. 규칙 상태가 설정된 레이어를 나타내기도 합니다.	20-19페이지의 규칙 상태 설정. 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용
임계값	현재 이 규칙에 설정된 임계값이자 해당 규칙에 대해 임계값을 추가하는 기능	20-6페이지의 규칙에 대한 임계값 설정
삭제	현재 이 규칙에 설정된 삭제 설정이자 해당 규칙에 대해 삭제를 추가하는 기능	20-7페이지의 규칙에 대한 삭제 설정
동적 상태	현재 이 규칙에 설정된 속도 기반 규칙 상태이자 해당 규칙에 대해 동적 규칙 상태를 추가하는 기능	20-7페이지의 규칙에 대한 동적 규칙 상태 설정
알림	현재 이 규칙에 설정된 알림이자 해당 규칙에 대해 알림을 추가하는 기능. 현재, SNMP 알림만 지원됩니다.	20-8페이지의 규칙에 대한 SNMP 경고 설정
코멘트	이 규칙에 추가된 코멘트이자 해당 규칙에 대해 코멘트를 추가하는 기능	20-9페이지의 규칙에 대해 규칙 코멘트 추가
설명서	Cisco VRT(취약성 연구단)가 제공한 현재 규칙의 규칙 문서	26-1페이지의 이벤트 보기

규칙 세부 사항을 보려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다. 기본적으로, 페이지는 메시지를 기준으로 규칙을 알파벳 순으로 나열합니다.

단계 4 세부사항을 보려는 규칙을 강조 표시합니다.

단계 5 **Show details(세부 사항 표시)**를 클릭합니다.

Rule Detail(규칙 세부 사항) 보기가 나타납니다. 세부 사항을 다시 숨기려면 **Hide details(세부사항 숨기기)**를 클릭합니다.

팁 또한 Rules(규칙) 보기에서 규칙을 더블클릭하여 Rule Detail(규칙 세부 사항)을 열 수 있습니다.

규칙에 대한 임계값 설정

라이센스: 보호

Rule Detail(규칙 세부 사항) 페이지에서 규칙에 대한 단일 임계값을 설정할 수 있습니다. 임계값을 추가하여 규칙에 대한 기존 임계값을 덮어씁니다. 임계값 설정에 대한 자세한 내용은 20-22페이지의 이벤트 임계값 설정 구성을 참고하십시오.

잘못된 값을 입력하면 되돌리기 아이콘( )이 필드에 나타납니다. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워둡니다.

규칙 세부 사항에서 임계값을 설정하려면 다음을 수행합니다.

단계 1 **Thresholds(임계값)** 옆에 있는 **Add(추가)**를 클릭합니다.

Set Threshold(임계값 설정) 대화 상자가 나타납니다.

단계 2 **Type(유형)** 드롭다운 목록에서 설정하려는 임계값 유형을 선택합니다.

- **Limit(제한)**을 선택하여 기간당 이벤트 인스턴스의 지정된 수로 알림을 제한합니다.
- **Threshold(임계값)**를 선택하여 기간당 이벤트 인스턴스의 각 지정된 수에 대해 알림을 제공합니다.
- **Both(모두)**를 선택하여 지정된 횟수의 이벤트 인스턴스 후 기간당 알림을 한 번만 제공합니다.

단계 3 **Track By(추적 기준)** 드롭다운 목록에서 **Source(소스)** 또는 **Destination(대상)**을 선택하여 이벤트 인스턴스가 소스 또는 대상 IP 주소로 추적되기를 원하는지 나타냅니다.

단계 4 임계값으로 사용할 이벤트 인스턴스의 수를 **Count(카운트)** 필드에 입력합니다.

단계 5 이벤트 인스턴스를 추적할 기간(초 단위)을 지정하는 0~2147483647의 숫자를 **Seconds(초)** 필드에 입력합니다.

단계 6 **OK(확인)**를 클릭합니다.

시스템은 임계값을 추가하여 Event Filtering(이벤트 필터링) 열의 규칙 옆에 이벤트 필터 아이콘( )을 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우 이벤트 필터 개수가 아이콘 위에 표시됩니다.

규칙에 대한 삭제 설정

라이센스: 보호

Rule Detail(규칙 세부 사항) 페이지에서 규칙에 대해 하나 이상의 삭제를 설정할 수 있습니다. 삭제에 대한 자세한 내용은 20-26페이지의 침입 정책에 따른 삭제 구성을 참고하십시오.

유효하지 않은 값을 입력하면 되돌리기 아이콘( )이 필드에 나타난다는 점에 유의하십시오. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워 둡니다.

규칙 세부 정보에서 삭제를 설정하려면 다음을 수행합니다.

단계 1 **Suppressions(삭제)** 옆에 있는 **Add(추가)**를 클릭합니다.

Add Suppression(삭제 추가) 대화 상자가 나타납니다.

단계 2 **Suppression Type(삭제 유형)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Rule(규칙)**을 선택하여 선택한 규칙에 대한 이벤트를 완전히 삭제합니다.
- **Source(소스)**를 선택하여 지정된 소스 IP 주소로 시작되는 패킷에서 생성된 이벤트를 삭제합니다.
- **Destination(대상)**을 선택하여 지정된 대상 IP 주소로 이동하는 패킷에서 생성된 이벤트를 삭제합니다.

단계 3 삭제 유형으로 **Source(소스)** 또는 **Destination(대상)**을 선택한 경우, Network (네트워크) 필드가 나타납니다. **Network (네트워크)** 필드에 IP 주소, 주소 블록 또는 이들의 조합으로 구성되고 쉼표로 구분된 목록을 입력합니다. 침입 정책이 액세스 제어 정책의 기본 작업과 연결된 경우 기본 작업 변수 집합의 네트워크 변수를 지정하거나 나열할 수도 있습니다.

IPv4 CIDR 및 IPv6 접두사 길이 주소 블록을 사용하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

단계 4 **OK(확인)**를 클릭합니다.

시스템은 삭제 조건을 추가하여 삭제된 규칙 옆의 Event Filtering(이벤트 필터링) 열에서 해당 규칙 옆에 이벤트 필터 아이콘( )을 표시합니다. 규칙에 여러 이벤트 필터를 추가한 경우, 아이콘 위의 숫자는 필터 수를 나타냅니다.

규칙에 대한 동적 규칙 상태 설정

라이센스: 보호

Rule Detail(규칙 세부 사항) 페이지에서 규칙에 대한 하나 이상의 동적 규칙 상태를 설정할 수 있습니다. 나열된 첫 번째 동적 규칙 상태의 우선 순위가 가장 높습니다. 2개의 동적 규칙 상태가 충돌할 때, 첫 번째 작업이 수행됩니다. 동적 규칙 상태에 대한 자세한 내용은 20-29페이지의 동적 규칙 상태의 이해를 참고하십시오.

유효하지 않은 값을 입력하면 되돌리기 아이콘( )이 필드에 나타난다는 점에 유의하십시오. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워 둡니다.

규칙 세부 사항에서 동적 규칙 상태를 설정하려면 다음을 수행합니다.

단계 1 **Dynamic State(동적 상태)** 옆에 있는 **Add(추가)**를 클릭합니다.

Add Rate-Based Rule State(속도 기반 규칙 상태 추가) 대화 상자가 표시됩니다.

단계 2 **Track By(추적 기준)** 드롭다운 목록에서 규칙 일치를 추적할 방법을 나타내는 옵션을 선택합니다.

- **Source(소스)**를 선택하여 특정 소스 또는 소스 집합으로부터 규칙에 대한 적중 수를 추적합니다.
- **Destination(대상)**을 선택하여 특정 대상 또는 대상 집합에 대한 규칙의 적중 수를 추적합니다.
- **Rule(규칙)**을 선택하여 해당 규칙에 대한 모든 일치 항목을 추적합니다.

단계 3 선택적으로, **Track By(추적 기준)**를 **Source(소스)** 또는 **Destination(대상)**으로 설정하는 경우, **Network (네트워크)** 필드에서 추적하려는 각 호스트의 IP 주소를 입력합니다.

IPv4 CIDR 및 IPv6 접두사 길이 코멘트를 사용하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

단계 4 공격 속도를 설정하려면 **Rate(속도)** 옆에 기간당 규칙 일치 수를 지정합니다.

- 0~2147483647의 정수를 사용하여 임계값으로 사용할 규칙 일치의 수를 **Count(카운트)** 필드에 지정합니다.
- 0~2147483647의 정수를 사용하여 공격이 추적되는 기간의 값(초 단위)을 **Seconds(초)** 필드에 입력합니다.

단계 5 조건이 일치할 때 수행할 새 작업을 **New State(새로운 상태)** 드롭다운 목록에서 선택합니다.

- **Generate Events(이벤트 생성)**을 선택하여 이벤트를 생성합니다.
- **Drop and Generate Events(이벤트 삭제 및 생성)**을 선택하여 인라인 배포에서 이벤트를 시작한 패킷을 삭제하고 이벤트를 생성하거나 수동 배포에서 이벤트를 생성합니다.
- 작업을 수행하지 않으려면 **Disabled(비활성화)**를 선택합니다.

단계 6 **Timeout(시간 제한)** 필드에 1과 2147483647 사이의 정수를 사용하여(약 68년), 새로운 작업의 효과를 지속하려는 시간(초)을 입력합니다. 시간 제한이 발생한 후, 규칙은 원래 상태로 돌아갑니다. 0을 지정하여 새로운 작업이 시간 초과되는 것을 방지합니다.

단계 7 **OK(확인)**를 클릭합니다.

시스템은 동적 규칙 상태를 추가하여 Dynamic State(동적 상태) 열의 규칙 옆에 동적 상태 아이콘( )을 표시합니다. 규칙에 여러 동적 규칙 상태 필터를 추가한 경우, 아이콘 위의 숫자는 필터 수를 나타냅니다.

필수 필드 중 비어 있는 것이 있으면 필드를 작성해야 한다는 오류 메시지가 표시됩니다.

규칙에 대한 SNMP 경고 설정

라이센스: 보호

Rule Detail(규칙 세부 사항) 페이지에서 규칙에 대한 SNMP 알림을 설정할 수 있습니다. SNMP 알림에 대한 자세한 내용은 20-32페이지의 SNMP 알림 추가를 참고하십시오.

규칙 세부 사항에서 SNMP 알림을 추가하려면 다음을 수행합니다.

단계 1 **Alerts(알림)** 옆에 있는 **Add SNMP Alert(SNMP 알림 추가)**를 클릭합니다.

시스템은 알림을 추가하여 Alerting(알림) 열의 규칙 옆에 알림 아이콘( )을 표시합니다. 규칙에 여러 알림을 추가하는 경우 알림 개수가 아이콘 위에 표시됩니다.

규칙에 대해 규칙 코멘트 추가

라이센스: 보호

Rule Detail(규칙 세부 사항) 페이지에서 규칙에 대한 규칙 코멘트를 추가할 수 있습니다. 규칙 코멘트에 대한 자세한 내용은 20-33페이지의 규칙 코멘트 추가를 참조하십시오.

규칙 세부사항에서 코멘트를 추가하려면 다음을 수행합니다.

단계 1 **Comments(코멘트)** 옆에 있는 **Add(추가)**를 클릭합니다.

Add Comments(코멘트 추가) 대화 상자가 나타납니다.

단계 2 **Comments(코멘트)** 필드에 규칙 코멘트를 입력합니다.

단계 3 **OK(확인)**를 클릭합니다.

시스템은 코멘트를 추가하고 Comments(코멘트) 열의 규칙 옆에 코멘트 아이콘( )을 표시합니다. 규칙에 여러 코멘트를 추가하는 경우 아이콘 위의 숫자는 코멘트의 수를 나타냅니다.

팁 규칙 코멘트를 삭제하려면 규칙 코멘트 섹션에서 **Delete(삭제)**를 클릭합니다. 커밋되지 않은 침입 정책 변경 사항과 함께 코멘트가 캐시된 경우에만 코멘트를 삭제할 수 있습니다. 침입 정책 변경 사항이 커밋되면 규칙 코멘트는 영구적인 상태가 됩니다.

침입 정책에서 규칙 필터링

라이센스: 보호

Rules(규칙) 페이지에 표시된 규칙을 단일 기준 또는 여러 기준의 조합으로 필터링할 수 있습니다.

구성한 필터가 Filter(필터) 텍스트 상자에 표시됩니다. 필터 패널에서 키워드 및 키워드 인수를 클릭하여 필터를 구성할 수 있습니다. 여러 키워드를 선택하면 시스템에서는 AND 논리를 사용하여 결합한 다음 복합 검색 필터를 생성합니다. 예를 들어, **Category(카테고리)** 아래에서 **preprocessor(전처리기)**를 선택한 다음 **Rule Content(규칙 콘텐츠) > GID**를 선택하고 `116`을 입력하면 `Category: "preprocessor" GID:"116"` 필터가 생성됩니다. 이 필터는 GID가 116**이며** 전처리기 규칙인 규칙을 모두 검색합니다.

Category(카테고리), Microsoft Vulnerabilities(Microsoft 취약성), Microsoft Worms(Microsoft 웜), Platform Specific(플랫폼 특징), Preprocessor(전처리기) 및 Priority(우선 순위) 필터 그룹을 통해 키워드를 위한 1개 이상의 인수를 쉼표로 구분하여 제출할 수 있습니다. 예를 들어, Shift를 누른 채 **Category(카테고리)**에서 **os-linux** 및 **os-windows**를 선택하여 `Category:"os-windows,os-linux"` 필터를 생성할 수 있습니다. 이 필터는 `os-linux` 카테고리 또는 `os-windows` 카테고리에 속하는 모든 규칙을 검색합니다.

필터 패널을 표시하려면 표시 아이콘( )을 클릭합니다.

필터 패널을 숨기려면, 숨기기 아이콘( )을 클릭합니다.

자세한 내용은 다음 주제를 참고하십시오.

- 20-10페이지의 침입 정책 내 규칙 필터링의 이해
- 20-18페이지의 침입 정책에서 규칙 필터 설정

침입 정책 내 규칙 필터링의 이해

라이센스: 보호

규칙 필터 키워드를 사용하면 규칙 설정(예: 규칙 상태 또는 이벤트 필터)을 적용할 규칙을 쉽게 찾을 수 있습니다. 키워드로 필터링하고 동시에 Rules(규칙) 페이지 필터 패널에서 원하는 인수를 선택하여 키워드에 대한 인수를 선택할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

침입 정책 규칙 필터 구성을 위한 지침

라이센스: 보호

필터를 구축하면 대부분의 경우, 침입 정책의 Rules(규칙) 페이지 왼쪽에 있는 필터 패널을 사용하여 사용하려는 인수/키워드를 선택할 수 있습니다.

Rule(규칙) 필터는 필터 패널의 규칙 필터 그룹으로 그룹화됩니다. 많은 규칙 필터 그룹에 하위 기준이 포함되어 있어서 원하는 특정 규칙을 손쉽게 찾을 수 있습니다. 일부 규칙 필터에는 개별 규칙으로 드릴다운하기 위해 확장할 수 있는 여러 레벨이 있습니다.

필터 패널의 항목은 때로는 필터 유형 그룹, 때로는 키워드, 그리고 때로는 키워드에 대한 인수를 나타냅니다. 필터를 구축할 수 있도록 다음과 같은 대략적인 규칙을 사용합니다.

- 키워드(Rule Configuration(규칙 구성), Rule Content(규칙 콘텐츠), Platform Specific(플랫폼 특징) 및 Priority(우선 순위))가 아닌 필터 유형 그룹 제목을 선택하면 확장되어 사용 가능한 키워드가 나열됩니다.

  기준 목록에서 노드를 클릭하여 키워드를 선택하면 필터링할 인수를 입력하라는 팝업 창이 나타납니다.

  해당 키워드가 필터에서 이미 사용되고 있는 경우 해당 키워드의 기존 인수가 사용자가 입력하는 인수로 대체됩니다.

- 키워드(Category(카테고리), Classifications(분류), Microsoft Vulnerabilities(Microsoft 취약성), Microsoft Worms(Microsoft 웜), Priority(우선 순위) 및 Rule Update(규칙 업데이트))인 필터 유형 그룹 제목을 선택하면 사용 가능한 인수가 나열됩니다.

  이 그룹 유형에서 항목을 선택하면, 적용하는 인수와 키워드가 필터에 즉시 추가됩니다. 키워드가 필터에 이미 있는 경우, 그룹에 해당하는 키워드에 대한 기존 인수를 교체합니다.

  예를 들어, 필터 패널에서 **Category(카테고리)** 아래의 **os Linux**를 클릭할 경우,필터 텍스트 상자에 `카테고리:"os-linux"`가 추가됩니다. **Category(카테고리)** 아래 **os-windows**를 클릭할 경우, 필터는 `카테고리:"os-windows"`로 변경됩니다.

- Rule Content(규칙 콘텐츠) 아래의 참조는 키워드이며, 그 아래에 나열된 참조 ID 유형도 마찬가지입니다. 참조 키워드를 선택하면 팝업 창이 나타납니다. 여기서 인수를 제공하면 기존 필터에 키워드가 추가됩니다. 해당 키워드가 필터에서 이미 사용되고 있는 경우, 새로 제공하는 인수가 기존 인수를 교체합니다.

예를 들어, 필터 패널에서 **Rule Content(규칙 내용) > Reference(참조) > CVE ID**를 클릭하면 팝업 창에 CVE ID를 제공하라는 메시지가 표시됩니다. 2007을 입력한 경우, 다음 `CVE: "2007"`이 필터 텍스트 상자에 추가됩니다. 다른 예를 들어, 필터 패널에서 **Rule Content(규칙 내용) > Reference(참조)**를 클릭하면 팝업 창에 참고 자료를 제공하라는 메시지가 표시됩니다. 2007을 입력한 경우, `Reference:"2007"`이 필터 텍스트 상자에 추가됩니다.

- 서로 다른 그룹에서 규칙 필터 키워드를 선택하면 각 필터 키워드가 필터에 추가되며 기존 키워드는 유지됩니다(동일한 키워드의 새 값으로 덮어쓰지 않는 한).

  예를 들어, 필터 패널에서 **Category(카테고리)** 아래의 **os Linux**를 클릭할 경우,필터 텍스트 상자에 `카테고리:"os-linux"`가 추가됩니다. **Microsoft Vulnerabilities(Microsoft 취약성)** 아래의 **MS00-006**을 클릭할 경우, 필터는 `카테고리:"os-linux" MicrosoftVulnerabilities:"MS00-006"`으로 변경됩니다.

- 여러 키워드를 선택하면 시스템에서 AND 논리로 키워드를 통합하여 복합 검색 필터를 생성합니다. 예를 들어, **Category(카테고리)** 아래에서 **preprocessor(전처리기)**를 선택한 다음 **Rule Content(규칙 콘텐츠) > GID**를 선택하고 116을 입력하면 `Category: "preprocessor" GID:"116"` 필터가 생성됩니다. 이 필터는 GID가 116**이며** 전처리기 규칙인 규칙을 모두 검색합니다.

- Category(카테고리), Microsoft Vulnerabilities(Microsoft 취약성), Microsoft Worms(Microsoft 웜), Platform Specific(플랫폼 특징) 및 Priority(우선 순위) 필터 그룹을 통해 키워드를 위한 하나 이상의 인수를 쉼표로 구분하여 제출할 수 있습니다. 예를 들어, Shift를 누른 채 **Category(카테고리)**에서 **os-linux** 및 **os-windows**를 선택하여 `카테고리:"os-windows,app-detect"` 필터를 생성할 수 있습니다. 이 필터는 `os-linux` 카테고리 또는 `os-windows` 카테고리에 속하는 모든 규칙을 검색합니다.

둘 이상의 필터 키워드/인수 쌍으로 동일한 규칙을 검색할 수 있습니다. 예를 들어, 규칙이 **dos** 카테고리에서 필터링될 경우, 그리고 **High(높은)** 우선 순위로 필터링할 경우 DOS Cisco 시도 규칙(SID 1545)이 나타납니다.

참고 Cisco VRT는 규칙 업데이트 메커니즘을 사용하여 규칙 필터를 추가 및 제거할 수 있습니다.

Rules(규칙) 페이지의 규칙은 공유 객체 규칙(생성기 ID 3) 또는 표준 텍스트 규칙(생성기 ID 1)일 수 있다는 점에 유의하십시오. 다음 표는 다양한 규칙 필터에 대해 설명합니다.

표 20-4 규칙 필터 그룹

필터 그룹	설명	다중인수 지원 여부	제목	목록 내 항목
규칙 구성	규칙의 구성에 따라 규칙을 찾습니다. 20-12페이지의 규칙 구성 필터 이해를 참고하십시오.	아니요	그룹화	키워드
규칙 콘텐츠	규칙의 내용에 따라 규칙을 찾습니다. 20-14페이지의 규칙 콘텐츠 필터의 이해를 참고하십시오.	아니요	그룹화	키워드
카테고리	규칙 편집기에 사용되는 규칙 카테고리에 따라 규칙을 찾습니다. 로컬 규칙은 로컬 하위 그룹에 나타납니다. 20-16페이지의 규칙 카테고리의 이해를 참고하십시오.	예	키워드	인수
분류	규칙에 의해 생성된 이벤트의 패킷 표시에 나타나는 공격 분류에 따라 규칙을 찾습니다. 23-12페이지의 침입 이벤트 분류 정의를 참고하십시오.	아니요	키워드	인수
Microsoft 취약성	Microsoft 게시판 번호에 따라 규칙을 찾습니다.	예	키워드	인수
Microsoft 웜	Microsoft Windows 호스트에 영향을 미치는 특정 웜에 따라 규칙을 찾습니다.	예	키워드	인수

표 20-4 규칙 필터 그룹 (계속)

필터 그룹	설명	다중인수 지원 여부	제목	목록 내 항목
플랫폼별	특정 운영 체제 버전에 대한 연관성에 따라 규칙을 찾습니다. 규칙 하나가 둘 이상의 운영 체제 또는 둘 이상의 운영 체제 버전에 영향을 미칠 수 있습니다. 예를 들어, SID 2260을 활성화하면 Mac OS X, IBM AIX 및 기타 운영 체제의 모든 버전에 영향을 줍니다.	예	키워드	인수 하위 목록의 항목 중 하나를 선택한 경우, 인수에 수정자가 추가됩니다.
전처리기	개별 전처리기에 대한 규칙을 찾습니다. 전처리기를 활성화하면 옵션의 이벤트를 생성하는 전처리기 옵션과 관련된 전처리기 규칙을 활성화해야 한다는 점에 유의하십시오(20-19페이지의 규칙 상태 설정 참고).	예	그룹화	하위 그룹화
우선순위	높음, 중간, 낮음 우선순위에 따라 규칙을 찾습니다. 규칙에 할당된 분류가 우선순위를 결정합니다. 이 그룹은 규칙 카테고리로 심화 그룹화됩니다. 로컬 규칙(즉, 사용자가 생성하는 규칙)은 우선순위 그룹에 나타나지 않습니다.	예	키워드	인수 하위 목록의 항목 중 하나를 선택한 경우, 인수에 수정자를 추가한다는 점에 유의하십시오.
규칙 업데이트	특정 규칙 업데이트를 통해 추가 또는 수정된 규칙을 찾습니다. 각 규칙 업데이트에 대해 모든 규칙을 보거나, 가져온 규칙만 보거나, 업데이트에 의해 변경된 기존 규칙만 볼 수 있습니다.	아니요	키워드	인수

규칙 구성 필터 이해

라이센스: 보호

Rules(규칙) 페이지에 나열되는 규칙을 여러 규칙 구성 설정으로 필터링할 수 있습니다.

기준 목록에서 노드를 클릭하여 키워드를 선택하면 필터링할 인수를 입력하라는 팝업 창이 나타납니다.

해당 키워드가 필터에서 이미 사용되고 있는 경우 해당 키워드의 기존 인수가 사용자가 입력하는 인수로 대체됩니다.

필터링하기 위해 사용할 수 있는 규칙 구성 설정에 대한 자세한 내용은 다음 절차를 참조하십시오.

Rule State(규칙 상태) 필터를 사용하려면 다음을 수행합니다.

단계 1 **Rule State(규칙 상태)**에서 **Rule Configuration(규칙 구성)**을 클릭합니다.

단계 2 **Rule State(규칙 상태)** 드롭다운 목록에서 필터링할 규칙 상태를 선택합니다.

- 이벤트를 생성하기만 하는 규칙을 찾으려면 **Generate Events(이벤트 생성)**를 선택하고 **OK(확인)**를 클릭합니다.
- 이벤트를 생성하고 일치하는 패킷을 삭제하도록 설정되어 있는 규칙을 찾으려면 **Drop and Generate Events(이벤트 삭제 및 생성)**를 선택한 다음, **OK(확인)**를 클릭합니다.
- 비활성화된 규칙을 찾으려면 **Disabled(비활성화)**를 선택한 다음, **OK(확인)**를 클릭합니다.

현재 규칙 상태에 따라 규칙을 표시하도록 Rules(규칙) 페이지가 업데이트됩니다.

Threshold(임계값) 필터를 사용하려면 다음을 수행합니다.

단계 1 **Rule Configuration(규칙 구성)**에서 **Threshold(임계값)**를 클릭합니다.

단계 2 **Threshold(임계값)** 드롭다운 목록에서 필터링할 임계값 설정을 선택합니다.

- `limit(한계)`라는 임계값 유형으로 규칙을 찾으려면, **Limit(한계)**를 선택한 후 **OK(확인)**를 클릭합니다.
- `threshold(임계값)`라는 임계값 유형으로 규칙을 찾으려면, **Threshold(임계값)**를 선택한 후 **OK(확인)**를 클릭합니다.
- `both(모두)`라는 임계값 유형으로 규칙을 찾으려면, **Both(모두)**를 선택한 후 **OK(확인)**를 클릭합니다.
- `source(소스)`로 추적된 임계값으로 규칙을 찾으려면, **Source(소스)**를 선택한 후 **OK(확인)**를 클릭합니다.
- `destination(대상)`으로 추적된 임계값으로 규칙을 찾으려면, **Destination(대상)**을 선택한 후 **OK(확인)**를 클릭합니다.
- 임계값 집합을 가진 모든 규칙을 찾으려면, **All(모두)**을 선택한 다음 **OK(확인)**를 클릭합니다.

Rules(규칙) 페이지가 업데이트되면서 필터에 나타난 임계값 유형이 적용된 규칙이 표시됩니다.

삭제 필터를 사용하려면 다음을 수행합니다.

단계 1 **Rule Configuration(규칙 구성)**에서 **Suppression(삭제)**을 클릭합니다.

단계 2 **Suppression(삭제)** 드롭다운 목록에서 필터링의 기준이 될 삭제 설정을 선택합니다.

- 해당 규칙에 따라 검사된 패킷에 대해 이벤트가 삭제된 규칙을 찾으려면 **By Rule(규칙별로)**을 선택한 후 **OK(확인)**를 클릭합니다.
- 트래픽 소스에 따라 이벤트가 삭제된 규칙을 찾으려면 **By Source(소스별로)**를 선택한 후 **OK(확인)**를 클릭합니다.
- 트래픽 대상에 따라 이벤트가 삭제된 규칙을 찾으려면 **By Destination(대상별로)**을 선택한 후 **OK(확인)**를 클릭합니다.
- 삭제 집합을 가진 모든 규칙을 찾으려면, **All(모두)**을 선택한 다음 **OK(확인)**를 클릭합니다.

Rules(규칙) 페이지가 필터에 표시된 삭제 유형이 규칙에 적용된 규칙을 표시하도록 업데이트됩니다.

Dynamic State(동적 상태) 필터를 사용하려면 다음을 수행합니다.

단계 1 **Rule Configuration(규칙 구성)**에서 **Dynamic State(동적 상태)**를 클릭합니다.

단계 2 **Dynamic State(동적 상태)** 드롭다운 목록에서 필터링의 기준이 될 삭제 설정을 선택합니다.

- 해당 규칙에 따라 검사된 패킷에 대해 동적 상태가 구성된 규칙을 찾으려면 **By Rule(규칙별로)**을 선택한 후 **OK(확인)**를 클릭합니다.
- 트래픽 소스에 따라 패킷에 대해 동적 상태가 구성된 규칙을 찾으려면 **By Source(소스별로)**를 선택한 후 **OK(확인)**를 클릭합니다.

- 트래픽 대상에 따라 동적 상태가 구성된 규칙을 찾으려면 **By Destination(대상별로)**을 선택한 후 **OK(확인)**를 클릭합니다.
- Generate Events(이벤트 생성)의 동적 상태가 구성된 규칙을 찾으려면, **Generate Events(이벤트 생성)**를 선택한 후 **OK(확인)**를 클릭합니다.
- Drop and Generate Events(이벤트 삭제 및 생성)의 동적 상태가 구성된 규칙을 찾으려면, **Drop and Generate Events(이벤트 삭제 및 생성)**를 선택한 후 **OK(확인)**를 클릭합니다.
- Disabled(비활성화)의 동적 상태가 구성된 규칙을 찾으려면, **Disabled(비활성화)**를 선택한 후 **OK(확인)**를 클릭합니다.
- 삭제 집합을 가진 모든 규칙을 찾으려면, **All(모두)**을 선택한 다음 **OK(확인)**를 클릭합니다.

Rules(규칙) 페이지가 필터에 표시된 동적 규칙 상태가 규칙에 적용된 규칙을 표시하도록 업데이트됩니다.

경고 필터를 사용하려면 다음을 수행합니다.

단계 1 **Rule Configuration(규칙 구성)**에서 **Alert(경고)**를 클릭합니다.

단계 2 **Alert(경고)** 드롭다운 목록에서 필터링의 기준이 될 삭제 설정을 **SNMP**로 선택합니다.

단계 3 **OK(확인)**를 클릭합니다.

Rules(규칙) 페이지가 경고 필터를 적용한 규칙을 표시하도록 업데이트됩니다.

코멘트 필터를 사용하려면 다음을 수행합니다.

단계 1 **Rule Configuration(규칙 구성)**에서 **Comment(코멘트)**를 클릭합니다.

단계 2 **Comment(코멘트)** 필드에서, 필터링의 기준이 될 코멘트 텍스트 문자열을 입력한 후 **OK(확인)**를 클릭합니다.

Rules(규칙) 페이지가 규칙에 적용된 코멘트가 필터에 표시된 문자열을 포함하는 규칙을 표시하도록 업데이트됩니다.

규칙 콘텐츠 필터의 이해

라이센스: 보호

Rules(규칙) 페이지에 나열되는 규칙을 여러 규칙 콘텐츠 항목별로 필터링할 수 있습니다. 예를 들어, 규칙의 SID를 검색하여 규칙을 빠르게 검색할 수 있습니다. 또한 특정 목적지 포트로 가는 트래픽을 검사하는 모든 규칙을 찾을 수 있습니다.

기준 목록에서 노드를 클릭하여 키워드를 선택하면 필터링할 인수를 입력하라는 팝업 창이 나타납니다.

해당 키워드가 필터에서 이미 사용되고 있는 경우 해당 키워드의 기존 인수가 사용자가 입력하는 인수로 대체됩니다.

예를 들어, 필터 패널의 **Rule Content(규칙 콘텐츠)**에서 **SID**를 클릭하면 SID를 입력하라는 팝업 창이 나타납니다. 1045를 입력하면 SID:"1045"가 필터 텍스트 상자에 추가됩니다. 그런 다음 **SID**를 다시 클릭하여 SID 필터를 1044로 변경하면 필터가 SID:"1044"로 바뀝니다.

필터링에 사용할 수 있는 규칙 내용에 대해 자세히 알아보려면 다음 표를 참조하십시오.

표 20-5 규칙 콘텐츠 필터

필터 사용을 위해 클릭할 콘텐츠	콘텐츠 클릭 후 수행 작업	결과
메시지	필터링할 기준이 되는 메시지 문자열을 입력한 다음, **OK(확인)**를 클릭합니다.	메시지 필드에 제공된 문자열을 포함하는 규칙을 찾습니다.
SID	필터링할 기준이 되는 SID 번호를 입력한 다음, **OK(확인)**를 클릭합니다.	지정된 SID가 있는 규칙을 찾습니다.
GID	필터링할 기준이 되는 GID 번호를 입력한 다음, **OK(확인)**를 클릭합니다.	지정된 GID가 있는 규칙을 찾습니다.
참조	필터링할 기준이 되는 참조 문자열을 입력한 다음, **OK(확인)**를 클릭합니다. 필터링할 기준이 되는 특정 유형의 참조 문자열을 입력하려면, **CVE ID**, **URL**, **Bugtraq ID**, **Nessus ID**, **Arachnids ID** 또는 **Mcafee ID**를 선택하고, 문자열을 입력한 다음, **OK(확인)**를 클릭합니다.	참조 필드에 제공된 문자열을 포함하는 규칙을 찾습니다.
작업	필터링할 기준이 되는 작업을 선택합니다. • 경고 규칙을 찾으려면 **Alert(경고)**를 선택한 다음, **OK(확인)**를 클릭합니다. • 통과 규칙을 찾으려면 **Pass(통과)**를 선택한 다음, **OK(확인)**를 클릭합니다.	경고 또는 통과로 시작하는 규칙을 찾습니다.
프로토콜	필터링할 기준이 되는 프로토콜을 선택합니다. **ICMP**, **IP**, **TCP** 또는 **UDP**를 선택한 다음, **OK(확인)**를 클릭합니다.	선택한 프로토콜을 포함하는 규칙을 찾습니다.
방향	필터링할 기준이 되는 방향 설정을 선택합니다. • 특정 방향으로 이동하는 트래픽을 검사할 규칙을 찾으려면, **Directional(방향)**을 선택한 다음, **OK(확인)**를 클릭합니다. • 소스 및 대상 간에 어느 방향에서나 이동하는 트래픽을 검사할 규칙을 찾으려면, **Bidirectional(양방향)**을 선택한 다음, **OK(확인)**를 클릭합니다.	표시된 방향 설정이 규칙에 포함되어 있는지 여부에 따라 규칙을 찾습니다.
소스 IP	필터링할 기준이 되는 소스 IP 주소를 입력한 다음, **OK(확인)**를 클릭합니다. 유효한 IP 주소, CIDR 블록/접두사 길이, $HOME_NET 또는 $EXTERNAL_NET과 같은 변수를 사용하여 필터링할 수 있다는 점을 참고하십시오.	지정된 주소 또는 규칙에서 소스 IP 주소 지정을 위한 변수를 사용하는 규칙을 찾습니다.

표 20-5 규칙 콘텐츠 필터 (계속)

필터 사용을 위해 클릭할 콘텐츠	콘텐츠 클릭 후 수행 작업	결과
대상 IP	필터링할 기준이 되는 대상 IP 주소를 입력한 다음, **OK(확인)**를 클릭합니다. 유효한 IP 주소, CIDR 블록/접두사 길이, `$HOME_NET` 또는 `$EXTERNAL_NET`과 같은 변수를 사용하여 필터링할 수 있다는 점을 참고하십시오.	지정된 주소 또는 규칙에서 소스 IP 주소 지정을 위한 변수를 사용하는 규칙을 찾습니다.
소스 포트	필터링할 기준이 되는 소스 포트를 입력한 다음, **OK(확인)**를 클릭합니다. 포트 값은 1과 65535 사이의 정수이거나 포트 변수여야 합니다.	지정된 소스 포트를 포함하는 규칙을 찾습니다.
대상 포트	필터링할 기준이 되는 대상 포트를 필터 기준을 입력한 다음, **OK(확인)**를 클릭합니다. 포트 값은 1과 65535 사이의 정수이거나 포트 변수여야 합니다.	지정된 대상 포트를 포함하는 규칙을 찾습니다.
규칙 오버헤드	필터링할 기준이 되는 규칙 오버헤드 볼륨을 선택합니다. **Low(낮음)**, **Medium(중간)**, **High(높음)** 또는 **Very High(매우 높음)**를 선택한 다음, **OK(확인)**를 클릭합니다.	선택한 규칙 오버헤드를 가진 규칙을 찾습니다.
메타데이터	필터링할 기준이 되는 메타데이터 키-값 쌍을 공백으로 구분하여 입력한 다음, **OK(확인)**를 클릭합니다. 예를 들어, HTTP 애플리케이션 프로토콜과 관련된 메타데이터로 규칙을 찾으려면 `metadata:"service http"`를 입력합니다.	일치하는 키-값 쌍을 포함하는 메타데이터로 규칙을 찾습니다.

규칙 카테고리의 이해

라이센스: 보호

ASA FirePOWER 모듈은 규칙을 탐지하는 트래픽 유형에 따라 카테고리에 규칙을 배치합니다. Rules(규칙) 페이지에서 규칙 카테고리로 필터링하여, 한 카테고리의 모든 규칙에 대해 규칙 속성을 설정할 수 있습니다. 예를 들어, 네트워크에 Linux 호스트가 없는 경우, **os-linux** 카테고리로 필터링할 수 있으며, **os-linux** 카테고리 전체를 비활성화하기 위해 모든 규칙 보기를 비활성화할 수 있습니다.

참고 Cisco VRT에서는 규칙 카테고리를 추가 및 제거하기 위해 규칙 업데이트 메커니즘을 사용할 수 있습니다.

규칙 필터 직접 수정

라이센스: 보호

필터 패널에서 필터를 클릭할 때 제공되는 특수 키워드 및 해당 인수를 변경하려면 필터를 수정할 수 있습니다. Rules(규칙) 페이지의 사용자 지정 필터 규칙은 규칙 편집기에서 사용되는 것처럼 기능하지만 필터 패널을 통해 필터를 선택할 때 표시되는 구문을 사용하여 Rules(규칙) 페이지 필터에 제공된 모든 키워드를 사용할 수 있습니다. 나중에 사용할 키워드를 결정하려면 필터 패널 오른쪽에서 적절한 인수를 클릭합니다. 필터 텍스트 상자에 필터 키워드와 인수 구문이 나타납니다.

특정 값만 지원하는 키워드의 인수 목록을 보려면 20-12페이지의 규칙 구성 필터 이해, 20-14페이지의 규칙 콘텐츠 필터의 이해 및 20-16페이지의 규칙 카테고리의 이해를 참조하십시오. 키워드에 대한 쉼표로 구분된 여러 인수는 Category(카테고리) 및 Priority(우선 순위) 필터 유형에만 지원된다는 점을 기억하십시오.

키워드와 인수, 문자 문자열, 따옴표의 리터럴 문자 문자열을 사용할 수 있으며 여러 필터 조건을 공백으로 구분할 수 있습니다. 필터에는 정규 표현식, 와일드카드 문자 또는 부정 문자(!), 보다 큼 기호(>), 보다 작음 기호(<)와 같은 특별 연산자를 포함할 수 없습니다. 키워드 없이, 키워드의 첫 글자 대문자 없이 또는 인수 앞뒤의 따옴표 없이 검색할 용어를 입력하면 검색은 문자열 검색으로 처리되며, 지정된 용어가 카테고리, 메시지 및 SID 필드에서 검색됩니다.

모든 키워드, 키워드 인수 및 문자열은 대/소문자 구분이 없습니다. `gid` 및 `sid` 키워드를 제외한, 모든 인수 및 문자열은 부분 문자열로 처리됩니다. `gid` 및 `sid`의 인수는 정확히 일치하는 것만 반환합니다.

각 규칙 필터의 형식에는 하나 이상의 키워드를 포함할 수 있습니다.

키워드:*"인수"*

*키워드*가 규칙 유형 표에 설명된 필터 그룹의 키워드 중 하나인 경우 및 *인수*가 큰 따옴표로 둘러싸인, 특정 필드 또는 키워드 관련 필드에서 검색할 단일 대소문자 구분 영숫자 문자열인 경우입니다. 키워드의 첫 글자는 대문자로 입력해야 합니다.

`gid` 및 `sid`를 제외한 모든 키워드에 대한 인수는 부분 문자열로 처리됩니다. 예를 들어, 인수 `123`은 `"12345"`, `"41235"`, `"45123"` 등을 반환합니다. `gid` 및 `sid`의 인수는 정확하게 일치하는 경우에만 반환됩니다. 예를 들어, `sid:3080`은 `SID 3080`만 반환합니다.

각 규칙 필터는 또한 하나 이상의 영숫자 문자 문자열을 포함할 수 있습니다. 문자열은 규칙 Message(메시지) 필드, 서명 ID 및 생성자 ID를 검색합니다. 예를 들어, 문자열 `123`은 규칙 메시지에서 문자열 `"Lotus123"`, `"123mania"` 등을 반환하며, 또한 `SID 6123`, `SID 12375` 등을 반환합니다. 규칙 Message(메시지) 필드에 대한 자세한 내용은 23-11페이지의 이벤트 메시지 정의를 참고하십시오. 하나 이상의 문자열로 필터링하여 부분 SID를 검색할 수 있습니다.

모든 문자열은 대소문자를 구분하지 않으며 부분 문자열로 처리됩니다. 예를 들어, 문자열 `ADMIN`, `admin` 또는 `Admin`은 모두 `"admin"`, `"CFADMIN"`, `"Administrator"` 등을 반환합니다.

정확히 일치하는 항목을 반환하기 위해 인용구에서 문자열을 묶을 수 있습니다. 예를 들어, 인용구 내 문자열 `"overflow attempt"`는 정확한 문자열만 반환하지만, 인용구가 없는 두 개의 문자열 `overflow` 및 `attempt`로 구성된 필터는 `"overflow attempt"`, `"overflow multipacket attempt"`, `"overflow with evasion attempt"` 등을 반환합니다.

키워드, 문자 문자열 또는 둘 모두의 임의의 조합을 공백으로 구분하여 입력함으로써 필터링 결과의 범위를 좁힐 수 있습니다. 결과는 필터링 조건과 일치하는 모든 규칙을 포함합니다.

순서에 상관없이 여러 필터 상태를 입력할 수 있습니다. 예를 들어, 다음 필터 각각은 동일한 규칙을 반환합니다.

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

침입 정책에서 규칙 필터 설정

라이센스: 보호

규칙의 하위 집합을 표시하려면 Rule(규칙) 페이지에서 규칙을 필터링할 수 있습니다. 그러면 모든 페이지 기능을 사용할 수 있습니다. 이 기능은 예를 들어 특정 카테고리의 모든 규칙에 대해 임계값을 설정하고자 할 때 유용할 수 있습니다. 필터링된 목록이나 필터링되지 않은 목록의 규칙과 같은 기능을 사용할 수 있습니다. 예를 들어 필터링된 목록 또는 필터링되지 않은 목록에서 규칙에 새 규칙 상태를 적용할 수 있습니다.

침입 정책의 Rules(규칙) 페이지 왼쪽에 있는 필터 패널에서 사전 정의된 필터 키워드를 선택할 수 있습니다. 필터를 선택하면 페이지에 모든 일치하는 규칙이 표시되거나 일치하는 규칙이 없음이 표시됩니다.

사용할 수 있는 모든 키워드와 인수 및 필터 패널에서 필터를 구성하는 방법에 대한 자세한 내용은 20-10페이지의 침입 정책 내 규칙 필터링의 이해를 참조하십시오.

추가로 제한하려면 필터에 키워드를 추가할 수 있습니다. 입력한 모든 필터는 전체 규칙 데이터베이스를 검색하고 일치하는 규칙을 모두 반환합니다. 페이지가 계속 이전 검색 결과를 표시하고 있는데 필터를 입력하는 경우, 페이지는 이를 지우고 새 필터의 결과로 돌아갑니다.

필터를 선택할 때 제공된 동일한 키워드 및 인수 구문을 사용하여 필터를 입력할 수도 있고, 선택한 후 필터에서 인수 값을 수정할 수도 있습니다. 키워드 없이, 키워드의 첫 대문자 없이 또는 인수를 둘러싼 따옴표 없이 검색 용어를 입력하면, 검색은 문자열 검색으로 간주되며, 지정된 용어 탐색을위해 메시지 및 SID 필드가 검색됩니다.

침입 정책에서 특정 규칙을 필터링하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다. 기본적으로, 페이지는 메시지를 기준으로 규칙을 알파벳 순으로 나열합니다.

단계 4 왼쪽에 있는 필터 패널에서 키워드나 인수를 클릭하여 필터를 구성합니다. 필터에 이미 있는 키워드에 대한 인수를 클릭하면 기존 인수가 교체됩니다. 자세한 내용은 다음 링크를 참고하십시오.

- 20-10페이지의 침입 정책 규칙 필터 구성을 위한 지침
- 20-12페이지의 규칙 구성 필터 이해
- 20-14페이지의 규칙 콘텐츠 필터의 이해
- 20-16페이지의 규칙 카테고리의 이해
- 20-17페이지의 규칙 필터 직접 수정

페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시되며, 필터와 일치하는 규칙의 수가 필터 텍스트 상자 위에 표시됩니다.

단계 5 새로운 설정을 적용하고자 하는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록에서 모든 규칙을 선택하려면 열 맨 위의 확인 상자를 선택합니다.

단계 6 선택적으로, 페이지에서 일반적으로 수행하는 모든 변경 사항은 규칙에 적용할 수 있습니다. 자세한 내용은 다음 섹션을 참고하십시오.

- Rules(규칙) 페이지에서 규칙을 활성화 및 비활성화하는 방법에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참조하십시오.
- 규칙에 임계값과 억제를 추가하는 방법에 대한 자세한 내용은 20-21페이지의 정책에 따른 침입 이벤트 알림 필터링을 참조하십시오.
- 일치하는 트래픽에서 속도 변칙이 발생할 때 트리거되는 동적 규칙 상태 설정에 대한 자세한 내용은 20-28페이지의 동적 규칙 상태 추가를 참조하십시오.
- 20-32페이지의 SNMP 알림 추가에서 SNMP 경고를 특정 규칙에 추가하는 데 대한 자세한 내용을 참고하십시오.
- 규칙 코멘트를 규칙에 추가하는 방법에 대한 자세한 내용은 20-33페이지의 규칙 코멘트 추가를 참조하십시오.

단계 7 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다.

자세한 내용은 19-3페이지의 침입 정책 관리 및 19-4페이지의 침입 정책 수정을 참고하십시오.

규칙 상태 설정

라이센스: 보호

Cisco VRT(취약성 연구단)는 각 정책에서 각 침입 및 전처리기 규칙의 기본 상태를 설정합니다. 예를 들어, 규칙은 Security Over Connectivity(연결성에 우선하는 보안) 기본 정책에서 활성화되며 Connectivity Over Security(보안에 우선하는 연결성) 기본 정책에서는 비활성화됩니다. 생성하는 침입 정책 규칙은 정책을 생성하기 위해 사용하는 기본 정책에 있는 규칙의 기본 상태를 상속합니다.

Generate Events(이벤트 생성), Drop and Generate Events(이벤트 삭제 및 생성) 또는 Disable(비활성화)로 규칙을 개별적으로 설정할 수 있으며 다양한 요소로 규칙을 필터링하여 상태를 수정하려는 규칙을 선택할 수 있습니다. 인라인 배포에서, 인라인 침입 배포의 Drop and Generate Events(이벤트 삭제 및 생성) 규칙 상태를 사용하여 악성 패킷을 삭제할 수 있습니다. Drop and Generate Events(이벤트 삭제 및 생성) 규칙 상태를 가진 규칙은 이벤트를 생성하지만 수동 배포에서 패킷을 삭제하지 않습니다. Generate Events(이벤트 생성) 또는 Drop and Generate Events(이벤트 삭제 및 생성)로 규칙을 설정하면 규칙이 활성화됩니다. 규칙을 Disable(비활성화)로 설정하면 규칙이 비활성화됩니다.

두 가지 시나리오를 생각해볼 수 있습니다. 첫 번째 시나리오에서, 특정 규칙에 대한 규칙 상태는 Generate Events(이벤트 생성)로 설정되어 있습니다. 악의적인 패킷이 네트워크를 이동하여 규칙을 트리거하면 규칙이 목적지로 전송되고 시스템이 침입 이벤트를 생성합니다. 두 번째 시나리오에서는, 동일한 규칙의 규칙 상태가 인라인 배포에서 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 것으로 가정합니다. 이 경우 악의적인 패킷이 네트워크를 이동하면 시스템은 이를 삭제하고 침입 이벤트를 생성합니다. 패킷은 대상에 도달하지 못합니다.

침입 정책에서 규칙의 상태를 다음 중 하나로 설정할 수 있습니다.

- 시스템이 일치하는 트래픽을 찾을 때 특정 침입 시도를 탐지하고 침입 이벤트를 생성하기를 원하는 경우 규칙 상태를 **Generate Events(이벤트 생성)**로 설정합니다.

- 시스템이 인라인 배포에서 일치하는 트래픽을 찾을 때 특정 침입 시도를 탐지하고 공격을 포함하는 패킷을 삭제한 후 침입 이벤트를 생성하기를 원하는 경우, 또는 시스템이 수동 배포에서 일치하는 트래픽을 찾을 때 침입 이벤트를 생성하기를 원하는 경우 규칙 상태를 Drop and Generate Events(이벤트 삭제 및 생성)로 설정합니다.

  패킷을 삭제하는 시스템의 경우, 인라인 배포에서 침입 정책을 규칙 삭제로 설정해야 한다는 점에 유의하십시오. 자세한 내용은 19-5페이지의 인라인 배포에서 삭제 작업 설정하기를 참고하십시오.

- 시스템이 일치하는 트래픽을 평가하지 않도록 하려면 규칙 상태를 **Disable(비활성화)**로 설정합니다.

삭제 규칙을 사용하려면 다음을 수행해야 합니다.

- 침입 정책의 **Drop when Inline(인라인 시 삭제)** 옵션을 활성화합니다.
- 규칙과 일치하는 모든 패킷을 삭제해야 하는 규칙의 경우 규칙 상태를 **Drop and Generate Events(이벤트 삭제 및 생성)**로 설정합니다.
- 침입 정책과 연결된 액세스 제어 규칙이 포함된 액세스 제어 정책을 인라인 배포에서 적용합니다.

Rules(규칙) 페이지에서 규칙을 필터링하면 삭제 규칙으로 설정할 규칙을 찾는 데 도움이 될 수 있습니다. 자세한 내용은 20-9페이지의 침입 정책에서 규칙 필터링을 참고하십시오.

규칙 구조, 규칙 키워드와 옵션, 규칙 작성 구문에 대한 자세한 내용은 23-1페이지의 침입 규칙의 이해와 작성을 참조하십시오.

VRT에서는 때때로 규칙 업데이트를 사용하여 기본 정책에 있는 하나 이상의 규칙의 기본 상태를 변경합니다. 규칙 업데이트가 기반 정책을 업데이트하도록 허용하면, 정책을 생성하기 위해 사용한 기본 정책(또는 기반으로 하는 기본 정책)에서 기본 상태가 변경될 때 정책에 있는 규칙의 기본 상태를 변경하는 것도 허용됩니다. 그러나 규칙 상태를 변경한 경우 규칙 업데이트가 변경 사항을 재정의하지 않습니다.

하나 이상의 규칙의 상태를 변경하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

이 페이지가 나타내는 것은 활성화된 규칙의 총 수, Generate Events(이벤트 생성)로 설정된 활성화된 규칙의 총 수, Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 총 수라는 점에 유의하십시오. 또한 수동 배포에서는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정된 규칙만 이벤트를 생성한다는 점에 유의하십시오.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다. 기본적으로, 페이지는 메시지를 기준으로 규칙을 알파벳 순으로 나열합니다.

단계 4 규칙 상태를 설정할 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 머리글이나 아이콘을 클릭합니다. 정렬 순서를 반대로 하려면 다시 클릭합니다.

- 왼쪽 필터 패널의 키워드 또는 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 20-10페이지의 침입 정책 내 규칙 필터링의 이해 및 20-18페이지의 침입 정책에서 규칙 필터 설정 항목을 참조하십시오.

  페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시됩니다.

단계 5 규칙 상태를 설정할 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록에서 모든 규칙을 선택하려면 열 맨 위의 확인 상자를 선택합니다.

단계 6 다음 옵션을 이용할 수 있습니다.

- 선택한 규칙이 트래픽과 일치할 때 이벤트를 생성하려면, **Rule State(규칙 상태) > Generate Events(이벤트 생성)**를 선택합니다.
- 선택한 규칙이 트래픽과 일치할 때 인라인 배포에서 트래픽을 삭제하고 이벤트를 생성하려면, **Rule State(규칙 상태) > Drop and Generate Events(이벤트 삭제 및 생성)**를 선택합니다.
- 선택한 규칙과 일치하는 트래픽을 검사하지 않으려면 **Rule State(규칙 상태) > Disable(비활성화)**을 선택합니다.

참고 Cisco는 침입 정책 내 모든 침입 규칙을 활성화하지 **않을 것을 강력히** 권장합니다. 모든 규칙이 활성화될 경우 디바이스의 성능이 저하될 수 있습니다. 대신 네트워크 환경과 가능한 한 일치하도록 규칙 설정을 조정하십시오.

단계 7 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 19-3페이지의 침입 정책 관리 및 19-4페이지의 침입 정책 수정을 참고하십시오.

정책에 따른 침입 이벤트 알림 필터링

라이센스: 보호

침입 이벤트의 중요성은 발생 빈도 또는 소스/대상 IP 주소를 기준으로 결정될 수 있습니다. 어떤 경우에는 특정 횟수가 발생할 때까지 이벤트에 대해 신경 쓰지 않아도 됩니다. 예를 들어, 어떤 사용자가 서버에 로그인을 시도하는 경우 특정 횟수만큼 실패할 때까지는 염려하지 않아도 됩니다. 다른 경우에는 소수의 발생 상황만 확인해도 광범위한 문제의 존재 여부를 파악할 수 있습니다. 예를 들어 웹 서버에 대해 DoS 공격이 시작된 경우, 상황을 해결해야 하는지를 파악하려면 침입 이벤트의 발생 상황을 몇 번만 확인해보면 됩니다. 동일한 이벤트를 수백 번 확인하면 시스템에 부담을 줄 뿐입니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 20-22페이지의 이벤트 임계값 설정 구성에서는 발생 횟수를 기반으로, 이벤트가 표시되는 빈도를 나타내는 임계값을 설정하는 방법에 대해 설명합니다. 이벤트 및 정책당 임계값 설정을 구성할 수 있습니다.
- 20-26페이지의 침입 정책에 따른 삭제 구성에서는 정책에 따라 소스 또는 대상 IP 주소당 지정된 이벤트 알림을 삭제하는 방법에 대해 설명합니다.

이벤트 임계값 설정 구성

라이센스: 보호

지정된 기간 내 이벤트 생성 횟수를 기반으로 시스템이 침입 이벤트를 로깅 및 표시하는 횟수를 제한하도록 침입 정책당 개별 규칙에 대한 임계값을 설정할 수 있습니다. 이를 통해 많은 수의 동일한 이벤트로 인해 마비되는 것을 방지할 수 있습니다. 공유 객체 규칙, 표준 텍스트 규칙 또는 전처리기 규칙당 임계값을 설정할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 20-22페이지의 이벤트 임계값 설정의 이해
- 20-23페이지의 침입 이벤트 임계값 추가 및 수정
- 20-25페이지의 침입 이벤트 임계값 보기 및 삭제
- 20-6페이지의 규칙에 대한 임계값 설정

이벤트 임계값 설정의 이해

라이센스: 보호

먼저, 임계값 설정 유형을 지정해야 합니다. 다음 표에 설명된 옵션 중에서 선택할 수 있습니다.

표 20-6 임계값 설정 옵션

옵션	설명
Limit(제한)	지정된 기간 중 규칙을 트리거하는 지정된 패킷 수(count 인수로 지정)에 대한 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Limit(제한)**로, **Count(카운트)**는 10으로, 그리고 **Seconds(초)**는 60으로 설정하고 14개의 패킷이 규칙을 트리거하는 경우, 시스템은 동일한 시간(분) 내 발생한 첫 10개의 패킷을 표시한 후 규칙의 이벤트 로깅을 중단합니다.
Threshold(임계값)	지정된 기간 중 지정된 패킷 수(count 인수로 지정)가 규칙을 트리거하면 단일 이벤트를 로깅하고 표시합니다. 이벤트의 임계값 카운트에 도달하고 시스템이 해당 이벤트를 로깅한 후 시간 카운터가 다시 시작된다는 점에 유의하십시오. 예를 들어, 유형은 **Threshold(임계값)**로, **Count(카운트)**는 10으로, 그리고 **Seconds(초)**는 60으로 설정하면 규칙은 33초에 10번 트리거됩니다. 시스템은 이벤트를 한 번 생성한 다음 Seconds(초) 및 Count(카운트) 카운터를 0으로 재설정합니다. 그런 다음 규칙은 다음 25초 안에 다시 10번 트리거됩니다. 33초에 카운터가 0으로 재설정되므로 시스템은 또 다른 이벤트를 로깅합니다.
Both(모두)	지정된 수(카운트)의 패킷이 규칙을 트리거한 후 특정 시기 동안 한 번에 하나의 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Both(모두)**로, **Count(카운트)**는 2로, 그리고 **Seconds(초)**는 10으로 설정하면, 다음과 같이 이벤트가 계산됩니다. • 규칙이 10초 안에 한 번 트리거되는 경우, 시스템은 어떤 이벤트도 생성하지 않습니다(임계값이 충족되지 않음). • 규칙이 10초 안에 두 번 트리거되는 경우, 시스템은 하나의 이벤트를 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족됨). • 규칙이 10초에 네 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족되고 이후 이벤트는 무시됨).

다음으로 이벤트 임계값이 소스 또는 대상 IP 주소별로 계산되는지 확인하는 추적을 지정해야 합니다. 시스템이 이벤트 인스턴스를 추적하는 방법을 지정하려면 다음 표의 옵션 중 하나를 선택합니다.

표 20-7 임계값 설정 IP 옵션

옵션	설명
소스	소스 IP 주소당 이벤트 인스턴스 수를 계산합니다.
대상	대상 IP 주소당 인스턴스 이벤트 수를 계산합니다.

마지막으로, 임계값을 정의하는 인스턴스 수 및 기간을 지정해야 합니다.

표 20-8 임계값 설정 인스턴스/시간 옵션

옵션	설명
개수	임계값 충족에 필요한 추적 IP 주소당 지정된 기간의 이벤트 인스턴스 수.
시간(초)	카운트가 재설정되기 전에 경과된 시간(초). 임계값 유형을 **limit(제한)**로, 추적을 **Source IP(소스 IP)**로, **count(카운트)**를 10으로, 그리고 **seconds(초)**를 10으로 설정한 경우, 시스템은 주어진 소스 포트에서 10초 안에 발생한 첫 10개의 이벤트를 로깅하고 표시합니다. 첫 10초 안에 7개의 이벤트만 발생한 경우, 시스템은 이를 모두 로깅하고 표시하며, 첫 10초 안에 40개의 이벤트가 발생한 경우, 시스템은 10개를 로깅하고 표시한 후 10초의 시간이 경과한 시점에서 다시 카운팅을 시작합니다.

침입 이벤트 임계값 설정을 단독으로 사용할 수도 있고, 속도 기반 공격 방지, `detection_filter` 키워드 및 침입 이벤트 삭제와 조합하여 사용할 수도 있다는 점을 참고하십시오. 자세한 내용은 20-28페이지의 동적 규칙 상태 추가, 23-87페이지의 필터링 이벤트 및 20-26페이지의 침입 정책에 따른 삭제 구성을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 20-23페이지의 침입 이벤트 임계값 추가 및 수정
- 20-6페이지의 규칙에 대한 임계값 설정
- 20-25페이지의 침입 이벤트 임계값 보기 및 삭제

침입 이벤트 임계값 추가 및 수정

라이센스: 보호

하나 이상의 특정 규칙에 대한 임계값을 설정할 수 있습니다. 별도로 또는 동시에 기존 임계값 설정을 수정할 수도 있습니다. 각각에 대한 단일 임계값을 설정할 수 있습니다. 임계값을 추가하여 규칙에 대한 기존 임계값을 덮어씁니다.

임계값 구성을 보고 삭제하는 방법에 대한 자세한 내용은 20-25페이지의 침입 이벤트 임계값 보기 및 삭제를 참조하십시오.

또한 모든 규칙 및 전처리기가 생성한 이벤트에 기본적으로 적용되는 전역 임계값을 수정할 수 있습니다. 자세한 내용은 22-1페이지의 침입 이벤트 로깅의 전역적 제한을 참고하십시오.

유효하지 않은 값을 입력하면 되돌리기 아이콘( )이 필드에 나타난다는 점에 유의하십시오. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워둡니다.

이벤트 임계값을 추가하거나 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다. 기본적으로, 페이지는 메시지를 기준으로 규칙을 알파벳 순으로 나열합니다.

단계 4 임계값을 설정할 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 제목 또는 아이콘을 클릭합니다. 분류를 되돌리려면, 다시 클릭합니다.
- 왼쪽 필터 패널의 키워드 또는 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 20-10페이지의 침입 정책 내 규칙 필터링의 이해 및 20-18페이지의 침입 정책에서 규칙 필터 설정 주제를 참고하십시오.

페이지는 새로 고침되어 일치하는 모든 규칙을 표시합니다.

단계 5 임계값을 설정할 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록에서 모든 규칙을 선택하려면 열 맨 위의 확인 상자를 선택합니다.

단계 6 **Event Filtering(이벤트 필터링) > Threshold(임계값)**를 선택합니다.

임계값 설정 팝업 창이 나타납니다.

단계 7 **Type(유형)** 드롭다운 목록에서 설정하려는 임계값 유형을 선택합니다.

- **Limit(제한)**을 선택하여 시간당 이벤트 인스턴스의 지정된 수로 알림을 제한합니다.
- **Threshold(임계값)**를 선택하여 시간당 이벤트 인스턴스의 각 지정된 수에 대해 알림을 제공합니다.
- **Both(모두)**를 선택하여 지정된 횟수의 이벤트 인스턴스 후 기간별 알림을 한 번만 제공합니다.

단계 8 **Track By(추적 기준)** 드롭다운 목록에서 **Source(소스)** 또는 **Destination(대상)** IP 주소로 추적되기를 원하는지 여부를 선택합니다.

단계 9 임계값으로 사용할 이벤트 인스턴스의 수를 **Count(카운트)** 필드에 지정합니다.

단계 10 **Seconds(초)** 필드에서, 이벤트 인스턴스를 추적할 기간을 구성하는 시간(초)를 지정합니다.

단계 11 **OK(확인)**를 클릭합니다.

시스템은 임계값을 추가하여 Event Filtering(이벤트 필터링) 열의 규칙 옆에 이벤트 필터 아이콘( )을 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우 아이콘 위의 숫자는 이벤트 필터의 수를 나타냅니다.

단계 12 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다.

자세한 내용은 19-3페이지의 침입 정책 관리 및 19-4페이지의 침입 정책 수정을 참고하십시오.

침입 이벤트 임계값 보기 및 삭제

라이센스: 보호

기존 임계값 설정을 보거나 삭제하고자 할 수 있습니다. 임계값에 대해 구성된 설정을 표시하여 시스템에 적절한지 확인하려면 Rules Details(규칙 세부 사항) 보기를 사용할 수 있습니다. 적절하지 않은 경우 새 임계값을 추가하여 기존 값을 덮어쓸 수 있습니다.

또한 모든 규칙 및 전처리기가 생성한 이벤트에 기본적으로 적용되는 전역 임계값을 수정할 수 있다는 점을 참고하십시오. 자세한 내용은 22-1페이지의 침입 이벤트 로깅의 전역적 제한을 참고하십시오.

임계값을 보거나 삭제하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다. 기본적으로, 페이지는 메시지를 기준으로 규칙을 알파벳 순으로 나열합니다.

단계 4 보거나 삭제할 구성된 임계값이 있는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 제목 또는 아이콘을 클릭합니다. 분류를 되돌리려면, 다시 클릭합니다.
- 왼쪽 필터 패널의 키워드 또는 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 20-10페이지의 침입 정책 내 규칙 필터링의 이해 및 20-18페이지의 침입 정책에서 규칙 필터 설정 주제를 참고하십시오.

  페이지는 새로 고침되어 일치하는 모든 규칙을 표시합니다.

단계 5 보거나 삭제할 구성된 임계값이 있는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록에서 모든 규칙을 선택하려면 열 맨 위의 확인 상자를 선택합니다.

단계 6 선택한 각 규칙에 대한 임계값을 제거하려면, **Event Filtering(이벤트 필터링) > Remove Thresholds(임계값 제거)**를 선택합니다. 표시되는 확인 팝업 창에서 **OK(확인)**를 클릭합니다.

팁 특정 임계값을 제거하려면, 규칙을 강조 표시하고 **Show details(세부 정보 보기)**를 클릭합니다. 임계값 설정을 확장한 다음, 제거할 임계값 설정 옆에 있는 **Delete(삭제)**를 클릭합니다. **OK(확인)**를 클릭하여 구성을 삭제할 것임을 확인합니다.

페이지가 새로 고쳐지고 임계값이 삭제됩니다.

단계 7 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 19-3페이지의 침입 정책 관리 및 19-4페이지의 침입 정책 수정을 참고하십시오.

침입 정책에 따른 삭제 구성

라이센스: 보호

특정 IP 주소 또는 특정 범위의 IP 주소가 특정 규칙 또는 전처리기를 트리거하면 침입 이벤트 알림을 삭제할 수 있습니다. 이렇게 하면 오탐을 없애는 데 도움이 됩니다. 예를 들어 특정 익스플로잇처럼 보이는 패킷을 전송하는 메일 서버가 있는 경우, 메일 서버에 의해 이벤트가 트리거될 때 해당 이벤트에 대한 이벤트 알림을 억제할 수 있습니다. 규칙은 모든 패킷에 대해 트리거되지만, 기준에 맞는 공격에 대한 이벤트만 표시됩니다.

침입 이벤트 삭제를 단독으로 사용할 수도 있고, 속도 기반 공격 방지, `detection_filter` 키워드 및 침입 이벤트 임계값 설정과 조합하여 사용할 수도 있다는 점을 참고하십시오. 자세한 내용은 20-28페이지의 동적 규칙 상태 추가, 23-87페이지의 필터링 이벤트 및 20-22페이지의 이벤트 임계값 설정 구성을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 20-26페이지의 침입 이벤트 삭제
- 20-27페이지의 삭제 조건 보기 및 삭제

침입 이벤트 삭제

라이센스: 보호

규칙에 대한 침입 이벤트 알림을 삭제할 수 있습니다. 규칙에 대한 알림이 삭제되면, 규칙은 트리거되지만 이벤트는 생성되지 않습니다. 규칙에 하나 이상의 삭제를 설정할 수 있습니다. 나열된 첫 번째 삭제가 가장 높은 우선 순위를 갖습니다. 2개의 삭제가 충돌할 때, 첫 번째 작업이 수행된다는 점에 유의하십시오.

유효하지 않은 값을 입력하면 되돌리기 아이콘()이 필드에 나타난다는 점에 유의하십시오. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워둡니다.

이벤트 표시를 삭제하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다. 기본적으로, 페이지는 메시지를 기준으로 규칙을 알파벳 순으로 나열합니다.

단계 4 삭제를 설정할 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 제목 또는 아이콘을 클릭합니다. 분류를 되돌리려면, 다시 클릭합니다.
- 왼쪽 필터 패널의 키워드 또는 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 20-10페이지의 침입 정책 내 규칙 필터링의 이해 및 20-18페이지의 침입 정책에서 규칙 필터 설정 주제를 참고하십시오.

  페이지는 새로 고침되어 일치하는 모든 규칙을 표시합니다.

단계 5 삭제 조건을 구성하려는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란를 선택합니다.

단계 6 **Event Filtering(이벤트 필터링) > Suppression(삭제)**을 선택합니다.

삭제 팝업 창이 나타납니다.

단계 7 다음 **Suppression Type(삭제 유형)** 옵션 중 하나를 선택합니다.

- **Rule(규칙)**을 선택하여 선택한 규칙에 대한 이벤트를 완전히 삭제합니다.
- **Source(소스)**를 선택하여 지정된 소스 IP 주소로 시작되는 패킷에서 생성된 이벤트를 삭제합니다.
- **Destination(대상)**을 선택하여 지정된 대상 IP 주소로 이동하는 패킷에서 생성된 이벤트를 삭제합니다.

단계 8 **Network (네트워크)** 필드에서 삭제 유형의 **Source(소스)** 또는 **Destination(대상)**을 선택하여, IP 주소, 주소 블록, 소스 또는 대상 IP 주소로 지정할 변수 또는 이들의 조합으로 구성되고 쉼표로 구분된 목록을 입력합니다.

IPv4 CIDR 및 IPv6 접두사 길이 주소 블록을 사용하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

단계 9 **OK(확인)**를 클릭합니다.

시스템은 삭제 조건을 추가하여 삭제된 규칙 옆의 Event Filtering(이벤트 필터링) 열에서 해당 규칙 옆에 이벤트 필터 아이콘( )을 표시합니다. 규칙에 여러 이벤트 필터를 추가한 경우, 아이콘 위의 숫자는 이벤트 필터 수를 나타냅니다.

단계 10 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다.

자세한 내용은 19-3페이지의 침입 정책 관리 및 19-4페이지의 침입 정책 수정을 참고하십시오.

삭제 조건 보기 및 삭제

라이센스: 보호

기존 삭제 조건을 보거나 삭제하려고 할 수 있습니다. 예를 들어, 메일 서버는 일반적으로 익스플로잇처럼 보이는 패킷을 전송하므로 메일 서버 IP 주소에서 시작되는 패킷에 대한 이벤트 알림을 억제할 수 있습니다. 그리고 해당 메일 서버를 폐쇄하고 다른 호스트에 IP 주소를 다시 할당할 경우, 해당 소스 IP 주소에 대한 삭제 조건을 삭제해야 합니다.

정의된 삭제 조건을 보거나 삭제하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다. 기본적으로 페이지에는 규칙이 메시지별 알파벳순으로 나열됩니다.

단계 4 삭제를 보거나 삭제할 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 제목 또는 아이콘을 클릭합니다. 분류를 되돌리려면, 다시 클릭합니다.
- 왼쪽 필터 패널의 키워드 또는 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 20-10페이지의 침입 정책 내 규칙 필터링의 이해 및 20-18페이지의 침입 정책에서 규칙 필터 설정 주제를 참고하십시오.

  페이지는 새로 고침되어 일치하는 모든 규칙을 표시합니다.

단계 5 삭제를 보거나 삭제할 규칙 또는 규칙들을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록에서 모든 규칙을 선택하려면 열 맨 위의 확인 상자를 선택합니다.

단계 6 다음 2가지 옵션을 사용할 수 있습니다.

- 규칙에 대한 모든 삭제를 제거하려면, **Event Filtering(이벤트 필터링) > Suppressions(삭제)**를 선택합니다. 표시되는 확인 팝업 창에서 **OK(확인)**를 클릭합니다.
- 특정 삭제 설정을 제거하려면, 규칙을 강조 표시하고 **Show details(세부 정보 보기)**를 클릭합니다. 삭제 설정을 확장하고 제거할 삭제 설정 옆에 있는 **Delete(삭제)**를 클릭합니다. **OK(확인)**를 클릭하여 선택한 설정을 삭제할 것인지 확인합니다.

페이지는 새로 고침되며 삭제 설정이 삭제됩니다.

단계 7 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 19-3페이지의 침입 정책 관리 및 19-4페이지의 침입 정책 수정을 참고하십시오.

동적 규칙 상태 추가

라이센스: 보호

속도 기반 공격은 네트워크 또는 호스트에 과도한 트래픽을 전송하여 네트워크 또는 호스트를 마비시켜 느려지게 하거나 적법한 요청을 거부하도록 시도하는 것입니다. 속도 기반 차단을 사용하여 특정 규칙에 대한 과도한 규칙 일치에 대응하여 규칙 작업을 변경할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 20-29페이지의 동적 규칙 상태의 이해
- 20-30페이지의 동적 규칙 상태 설정

동적 규칙 상태의 이해

라이센스: 보호

지정된 기간에 규칙에 대해 너무 많은 일치가 발생할 때 이를 탐지하는 속도 기반 필터를 포함하도록 침입 정책을 구성할 수 있습니다. 인라인으로 배포된 디바이스에서 이 기능을 사용하여 지정된 시간 동안 속도 기반 공격을 차단한 후 규칙 일치를 통해 이벤트만 생성하고 트래픽을 삭제하지는 않는 규칙 상태로 돌아갈 수 있습니다.

속도 기반 공격 방지는 잘못된 트래픽 패턴을 식별하고 정당한 요청에 대한 해당 트래픽의 영향을 최소화하려고 합니다. 특정 대상 IP 주소로 이동하거나 특정 소스 IP 주소에서 오는 트래픽에서의 과도한 규칙 일치를 식별할 수 있습니다. 탐지된 모든 트래픽에서 특정 규칙에 대해 발생하는 과도한 일치에 대응할 수도 있습니다.

침입 정책에서, 모든 침입 또는 전처리기 규칙에 대해 속도 기반 필터를 구성할 수 있습니다. 속도 기반 필터에는 다음과 같은 3개의 구성 요소가 포함되어 있습니다.

- 특정 초 이내 규칙 일치의 계수로 구성한 규칙 일치 비율
- 속도를 초과할 경우 다음 3개의 사용 가능한 작업과 함께 취할 새로운 작업: Generate Events(이벤트 생성), Drop and Generate Events(이벤트 삭제 및 생성), Disable(비활성화)
- 시간 제한 값으로 설정한 작업 기간

시작한 경우, 속도가 해당 기간 동안 구성된 속도까지 떨어지더라도 시간 제한에 도달할 때까지 새로운 작업이 발생한다는 점에 유의하십시오. 시간 제한에 도달하면, 속도가 임계값 아래로 떨어진 경우, 규칙 작업은 규칙에 처음 설정된 작업으로 돌아갑니다.

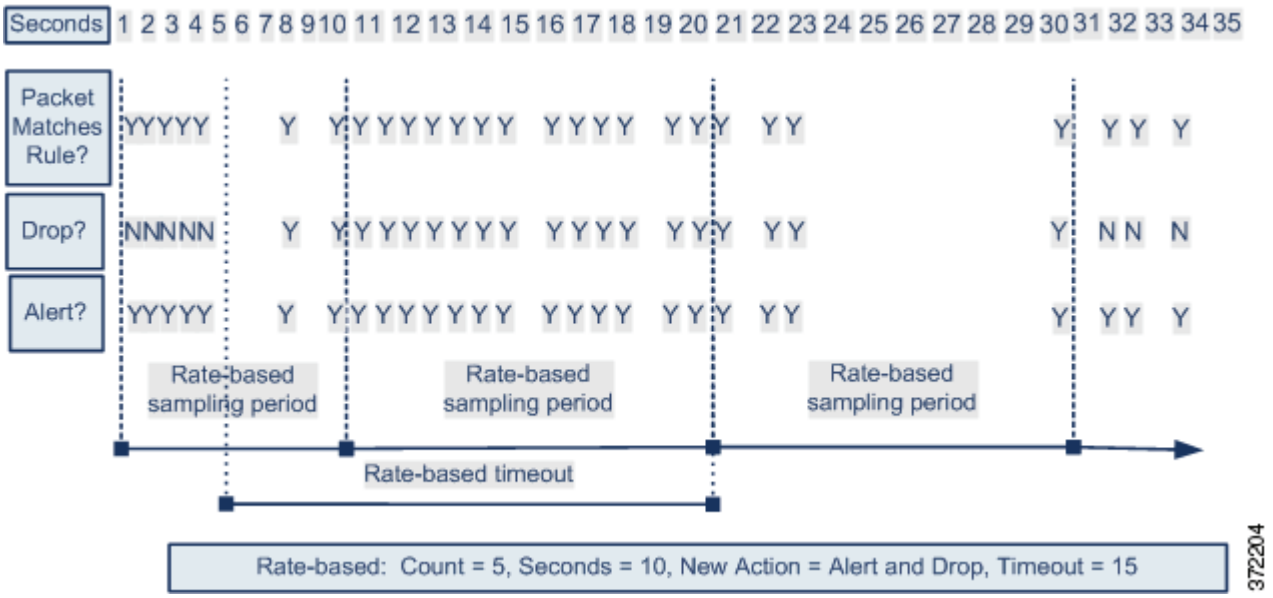
인라인 배포에서 속도 기반 공격 차단을 구성하여 일시적으로 또는 영구적으로 공격을 차단할 수 있습니다. 속도 기반 구성 없이, Generate Events(이벤트 생성)로 설정된 규칙은 이벤트를 생성하지만 시스템은 해당 규칙에 대한 패킷을 삭제하지 않습니다. 그러나, 속도 기반 기준이 구성되어 있는 규칙이 공격 트래픽과 일치하는 경우, 해당 규칙이 처음에는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되어 있지 않더라도 속도 작업은 속도 작업이 활성화된 기간 동안 패킷이 삭제되도록 할 수 있습니다.

참고 속도 기반 작업은 비활성화된 규칙을 활성화하거나 비활성화된 규칙에 일치하는 트래픽을 삭제할 수 없습니다.

동일한 규칙에서 다중 속도 기반 필터를 정의할 수 있습니다. 침입 정책에 나열된 첫 번째 필터의 우선 순위가 가장 높습니다. 2개의 속도 기반 필터링 작업이 충돌할 때, 첫 번째 속도 기반 필터가 수행된다는 점에 유의하십시오.

다음 다이어그램은 공격자가 호스트에 액세스하기 위해 시도하는 예를 보여줍니다. 비밀번호를 찾으려는 반복된 시도는 속도 기반 공격 방지를 구성한 규칙을 트리거합니다. 속도 기반 설정은 10초 범위 안에 규칙 일치가 다섯 번 발생하면 규칙 속성을 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다. 새로운 규칙 속성은 15초 후 시간 초과됩니다.

시간 제한 후에도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값 속도보다 높을 경우, 새로운 작업은 계속됩니다. 새로운 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 Generate Events(이벤트 생성)로 돌아갑니다.



동적 규칙 상태 설정

라이센스: 보호

규칙과 일치하는 모든 패킷을 삭제하지는 않을 것이지만 지정된 시간에 특정 일치 속도가 발생하면 규칙과 일치하는 패킷을 삭제하려는 경우, 규칙을 Drop and Generate Events(이벤트 삭제 및 생성) 상태로 설정하지 않을 수 있습니다. 동적 규칙 상태를 사용하면 규칙에 대한 작업에서 변경을 트리거하는 속도, 속도가 충족될 때 작업에서 변경해야 할 내용, 새 작업의 지속 시간 등을 구성할 수 있습니다.

카운트와 초(작업 변경을 트리거하기 위해 히트 수가 발생해야 하는 시간)를 지정하여 규칙에 대한 히트 수를 설정할 수 있습니다. 또한, 시간 제한이 만료되면 규칙에 대한 이전 상태에 되돌리는 작업을 야기할 시간 제한을 설정할 수 있습니다.

동일한 규칙에서 여러 동적 규칙 상태 필터를 정의할 수 있습니다. 침입 정책의 규칙 세부사항에 첫 번째로 나열되는 필터의 우선순위가 가장 높습니다. 2개의 속도 기반 필터링 작업이 충돌할 때, 첫 번째 속도 기반 필터가 수행된다는 점에 유의하십시오.

유효하지 않은 값을 입력하면 되돌리기 아이콘( )이 필드에 나타난다는 점에 유의하십시오. 아이콘을 클릭하여 해당 필드의 마지막 유효한 값으로 되돌리거나 이전 값이 없을 경우 필드를 비워둡니다.

참고 동적 규칙 상태는 비활성화된 규칙을 활성화하거나, 비활성화된 규칙과 일치하는 트래픽을 삭제할 수 없습니다.

동적 규칙 상태를 추가하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다.

단계 4 동적 규칙 상태를 추가하고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 제목 또는 아이콘을 클릭합니다. 분류를 되돌리려면, 다시 클릭합니다.
- 왼쪽 필터 패널의 키워드 또는 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 20-10페이지의 침입 정책 내 규칙 필터링의 이해 및 20-18페이지의 침입 정책에서 규칙 필터 설정 주제를 참고하십시오.

  페이지는 새로 고침되어 일치하는 모든 규칙을 표시합니다.

단계 5 동적 규칙 상태를 추가하고자 하는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록에서 모든 규칙을 선택하려면 열 맨 위의 확인 상자를 선택합니다.

단계 6 **Dynamic State(동적 상태) > Add Rate-Based Rule State(속도 기반 규칙 상태 추가)**를 선택합니다.

Add Rate-Based Rule State(속도 기반 규칙 상태 추가) 대화 상자가 표시됩니다.

단계 7 **Track By(추적 기준)** 드롭다운 목록에서 규칙 일치가 추적되기를 원하는 방법을 선택합니다.

- **Source(소스)**를 선택하여 특정 소스 또는 소스 집합으로부터 규칙에 대한 적중 수를 추적합니다.
- **Destination(대상)**을 선택하여 특정 대상 또는 대상 집합에 대한 규칙의 적중 수를 추적합니다.
- **Rule(규칙)**을 선택하여 해당 규칙에 대한 모든 일치 항목을 추적합니다.

단계 8 **Track By(추적 기준)**를 **Source(소스)** 또는 **Destination(대상)**으로 설정하는 경우, **Network (네트워크)** 필드에서 추적하려는 각 호스트의 주소를 입력합니다.

단일 IP 주소, 주소 블록, 변수 또는 이들 조합으로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다. IPv4 CIDR 및 IPv6 접두사 길이 주소 블록을 사용하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

단계 9 공격 속도를 설정하려면 **Rate(속도)** 옆에 기간별 규칙 일치 수를 지정합니다.

- 1~2147483647의 정수를 사용하여 임계값으로 사용할 규칙 일치의 수를 **Count(카운트)** 필드에 지정합니다.
- 1~2147483647의 정수를 사용하여 공격이 추적되는 기간의 값(초 단위)을 **Seconds(초)** 필드에 지정합니다.

단계 10 **New State(새로운 상태)** 드롭다운 목록에서 조건이 충족되면 취할 새로운 작업을 지정합니다.

- **Generate Events(이벤트 생성)**을 선택하여 이벤트를 생성합니다.
- **Drop and Generate Events(이벤트 삭제 및 생성)**를 선택하여 이벤트를 생성하고 인라인 배포에서 이벤트를 트리거한 패킷을 삭제하거나 수동 배포에서 이벤트를 생성합니다.
- 아무런 조치도 취하지 않으려면 **Disabled(비활성화)**를 선택합니다.

단계 11 **Timeout(시간 제한)** 필드에 새로운 작업이 계속 적용되기를 원하는 시간(초)를 입력합니다. 시간 제한이 발생한 후, 규칙은 원래 상태로 돌아갑니다. 0을 지정하거나, 새로운 작업이 시간 초과되는 것을 방지하기 위해 **Timeout(시간 제한)** 필드를 비워 둡니다.

단계 12 **OK(확인)**를 클릭합니다.

시스템은 동적 규칙 상태를 추가하여 Dynamic State(동적 상태) 열의 규칙 옆에 동적 상태 아이콘()을 표시합니다. 규칙에 여러 동적 규칙 상태 필터를 추가한 경우, 아이콘 위의 숫자는 필터 수를 나타냅니다.

필수 필드가 비어 있는 모든 경우, 어느 필드를 채워야하는지 나타내는 오류 메시지를 받습니다.

팁 규칙 집합에 대한 모든 동적 규칙 설정을 삭제하려면 Rules(규칙) 페이지에서 규칙을 선택한 후 **Dynamic State(동적 상태) > Remove Rate-Based States(속도 기반 상태 제거)**를 선택합니다. 또한 규칙을 선택하고, **Show details(세부 정보 보기)**를 클릭한 후 제거할 속도 기반 필터로 **Delete(삭제)**를 클릭하여 규칙에 대한 규칙 세부 정보에서 개별 속도 기반 규칙 상태 필터를 삭제할 수 있습니다.

단계 13 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다.

자세한 내용은 19-3페이지의 침입 정책 관리 및 19-4페이지의 침입 정책 수정을 참고하십시오.

SNMP 알림 추가

라이센스: 보호

ASA FirePOWER 모듈에 대해 SNMP 알림을 구성하는 경우, 규칙이 이벤트를 생성할 때 SNMP 알림을 제공하는 특정 규칙을 구성할 수 있습니다. 자세한 내용은 28-1페이지의 SNMP 응답 사용을 참고하십시오.

SNMP 알림을 설정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다.

단계 4 SNMP 알림을 설정하고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 제목 또는 아이콘을 클릭합니다. 분류를 되돌리려면, 다시 클릭합니다.
- 왼쪽 필터 패널의 키워드 또는 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 20-10페이지의 침입 정책 내 규칙 필터링의 이해 및 20-18페이지의 침입 정책에서 규칙 필터 설정 주제를 참고하십시오.

  페이지는 새로 고침되어 일치하는 모든 규칙을 표시합니다.

단계 5 SNMP 알림을 설정하고자 하는 규칙을 선택합니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록에서 모든 규칙을 선택하려면 열 맨 위의 확인 상자를 선택합니다.

단계 6 **Alerting(알림) > Add SNMP Alert(SNMP 알림 추가)**를 선택합니다.

시스템은 경고를 추가하여 Alerting(경고) 열의 규칙 옆에 경고 아이콘( )을 표시합니다. 규칙에 여러 알림 유형을 추가하는 경우 아이콘 위의 숫자는 알림 유형의 수를 나타냅니다.

팁 규칙에서 SNMP 알림을 제거하려면, 규칙 옆 확인 상자를 클릭하고 **Alerting(알림) > Remove SNMP Alerts(SNMP 알림 제거)**를 선택한 다음, **OK(확인)**를 클릭하여 삭제를 확인합니다.

단계 7 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 19-3페이지의 침입 정책 관리 및 19-4페이지의 침입 정책 수정을 참고하십시오.

규칙 코멘트 추가

라이센스: 보호

규칙에 코멘트를 추가할 수 있습니다. 추가하는 코멘트는 Rules(규칙) 페이지의 Rule Details(규칙 세부 사항) 보기에서 볼 수 있습니다.

코멘트가 포함된 침입 정책 변경 사항을 커밋한 후에는 또한 규칙 Edit(수정) 페이지에서 **Rule Comment(규칙 코멘트)**를 클릭하여 코멘트를 볼 수 있습니다. 규칙 수정에 대한 자세한 내용은 23-103페이지의 기존 규칙 변경을 참조하십시오.

규칙에 코멘트를 추가하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 **Rules(규칙)**를 클릭합니다.

Rules(규칙) 페이지가 나타납니다.

단계 4 코멘트를 추가하고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 제목 또는 아이콘을 클릭합니다. 분류를 되돌리려면, 다시 클릭합니다.
- 왼쪽 필터 패널의 키워드 또는 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 20-10페이지의 침입 정책 내 규칙 필터링의 이해 및 20-18페이지의 침입 정책에서 규칙 필터 설정 주제를 참고하십시오.

  페이지는 새로 고침되어 일치하는 모든 규칙을 표시합니다.

단계 5 코멘트를 추가하고자 하는 규칙을 선택합니다.

- 특정 규칙을 선택하려면, 규칙 옆의 확인 상자를 선택합니다.
- 현재 목록에서 모든 규칙을 선택하려면 열 맨 위의 확인 상자를 선택합니다.

단계 6 **Comments(코멘트) > Add Rule Comment(규칙 코멘트 추가)**를 선택합니다.

Add Comments(코멘트 추가) 대화 상자가 나타납니다.

단계 7 **Comments(코멘트)** 필드에 규칙 코멘트를 입력합니다.

단계 8 **OK(확인)**를 클릭합니다.

시스템은 코멘트를 추가하여 Comments(코멘트) 열의 규칙 옆에 코멘트 아이콘( )을 표시합니다. 규칙에 여러 코멘트를 추가한 경우, 아이콘 위의 숫자는 코멘트 수를 나타냅니다.

팁 규칙 코멘트를 삭제하려면 규칙을 강조 표시하고 **Show Details(세부 사항 보기)**를 클릭한 다음, **Comments(코멘트)** 섹션에서 **Delete(삭제)**를 클릭합니다. 코멘트가 커밋되지 않은 침입 정책 변경 사항으로 캐시된 경우 코멘트 삭제만 할 수 있다는 점에 유의하십시오. 침입 정책 변경 사항이 커밋되면 규칙 코멘트는 영구적입니다.

단계 9 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다.

자세한 내용은 19-3페이지의 침입 정책 관리 및 19-4페이지의 침입 정책 수정을 참고하십시오.

21장 특정 위협 탐지

네트워크 분석 정책에서 여러 프리프로세서를 사용하여 Back Orifice 공격, 여러 포트 스캔 유형, 그리고 과도한 트래픽으로 네트워크를 무력화하려는 속도 기반 공격과 같은 사용자의 모니터링된 네트워크에 대한 특정 위협을 탐지할 수 있습니다. 침입 규칙 또는 규칙 인수에서 비활성화된 프리프로세서를 요구하면, 네트워크 분석 정책 사용자 인터페이스에 비활성 상태로 남아 있더라도 시스템에서는 자동으로 현재의 구성과 함께 해당 프리프로세서를 사용합니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

보안없이 전송되는 민감한 수치 데이터를 탐지하려면 침입 정책에서 구성하는 민감한 데이터 탐지 기능을 사용할 수도 있습니다.

특정 위협 탐지에 대한 자세한 내용은 다음 섹션을 참고하십시오.

- 21-1페이지의 Back Orifice 탐지에서는 Back Orifice 공격의 탐지에 대해 설명합니다.
- 21-3페이지의 포트 스캔 탐지에서는 다양한 유형의 포트 스캔을 설명하고 포트 스캔 탐지를 사용하여 네트워크 위협이 공격으로 발전하기 전에 식별하는 방법에 대해 설명합니다.
- 21-10페이지의 속도 기반 공격 방지에서는 서비스 거부(DoS) 및 SYN 플러드 공격을 제한하는 방법에 대해 설명합니다.
- 21-20페이지의 민감한 데이터 검색에서는 신용 카드 번호 및 ASCII 문자로 표시된 주민등록번호/사회보장번호와 같은 민감한 데이터를 탐지하고 이벤트를 생성하는 방법에 대해 설명합니다.

Back Orifice 탐지

라이센스: 보호

ASA FirePOWER 모듈은 다음 Back Orifice 프로그램의 존재를 탐지하는 프리프로세서를 제공합니다. 이 프로그램은 Windows 호스트에 대한 관리자 액세스 권한을 얻는 데 사용할 수 있습니다. Back Orifice 프리프로세서는 Back Orifice 매직 쿠키인 "*! *QWTY?"(패킷의 처음 8바이트에 있으며 XOR로 암호화됨)에 대한 UDP 트래픽을 분석합니다.

Back Orifice 프리프로세서는 구성 페이지가 있지만, 구성 옵션은 없습니다. Back Orifice가 활성화된 경우, 프리프로세서가 해당 이벤트를 생성하도록 하려면 다음 표의 프리프로세서 규칙도 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

표 21-1 Back Orifice GID:SID

프리프로세서 규칙 GID:SID	설명
105:1	Back Orifice 트래픽이 탐지됨
105:2	Back Orifice 클라이언트 트래픽이 탐지됨
105:3	Back Orifice 서버 트래픽이 탐지됨
105:4	Back Orifice snort 버퍼 공격이 탐지됨

Back Orifice Detection(Back Orifice 탐지) 페이지를 보려면

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 **Specific Threat Detection(특정 위협 탐지)** 아래의 **Back Orifice Detection(Back Orifice 탐지)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 프리프로세서가 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 프리프로세서가 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Back Orifice Detection(Back Orifice 탐지) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

포트 스캔 탐지

라이센스: 보호

포트스캔은 공격에 앞서 공격자가 종종 사용하는 네트워크 정찰의 형태입니다. 포트스캔에서 공격자는 특별히 고안된 패킷을 대상 호스트로 전송합니다. 호스트가 응답하는 패킷을 검사하여 공격자는 종종 호스트에서 어떤 포트가 열려 있는지, 그리고 직접적으로 또는 추론에 의해 이러한 포트에서 어떤 애플리케이션 프로토콜이 실행 중인지 확인할 수 있습니다.

포트스캔 탐지가 활성화된 경우 포트스캔 탐지기의 활성화된 포트스캔 유형이 포트스캔 이벤트를 생성하도록 하려면 침입 정책 Rules(규칙) 페이지에서 GID(generator ID) 122로 규칙을 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정 및 21-8페이지의 표 21-5를 참고하십시오.

포트스캔 자체는 공격의 증거가 되지 못합니다. 실제로, 공격자가 사용하는 포트스캔 기법 중 일부는 네트워크의 합법적인 사용자들도 사용할 수 있습니다. Cisco의 포트스캔 탐지기는 활동의 패턴을 탐지하여 어떤 포트스캔이 악의적일 수 있는지를 확인하도록 설계되었습니다.

공격자들은 네트워크에 대한 프로브를 위해 여러 방법을 사용할 것입니다. 이들은 종종, 하나의 프로토콜 유형이 차단되면 다른 것을 사용할 수 있도록 대상 호스트에서 서로 다른 응답을 이끌어내기 위해 여러 프로토콜을 사용합니다. 다음 표에서는 포트스캔 탐지기에서 활성화할 수 있는 프로토콜에 대해 설명합니다.

표 21-2 프로토콜 유형

프로토콜	설명
TCP	SYN 스캔, ACK 스캔, TCP connect() 스캔, 그리고 Xmas tree, FIN, NULL 등 특이한 플래그 조합의 스캔과 같은 TCP 프로브를 탐지합니다.
UDP	제로바이트 UDP 패킷과 같은 UDP 프로브를 탐지합니다.
ICMP	ICMP 에코 요청(ping)을 탐지합니다.
IP	IP 프로토콜 스캔을 탐지합니다. 이 스캔은 TCP 및 UDP 스캔과 다릅니다. 공격자가 열린 포트를 찾는 대신 대상 호스트에서 어떤 IP 프로토콜이 지원되는지를 알아보려고 하기 때문입니다.

참고 포트스캔 연결 탐지기가 생성하는 이벤트의 경우 프로토콜 번호는 255로 설정됩니다. 포트스캔에는 기본적으로 연결된 특정 프로토콜이 없기 때문에 IANA(Internet Assigned Numbers Authority)에서는 프로토콜 번호를 할당하지 않습니다. IANA에서는 255를 예약 번호로 지정하므로, 이벤트에 대해 연결된 프로토콜이 없음을 나타내기 위해 프로토콜 이벤트에 해당 번호가 사용됩니다.

포트스캔은 일반적으로 대상 호스트의 수, 스캔하는 호스트의 수, 스캔되는 포트의 수를 기반으로 네 가지 유형으로 구분됩니다. 다음 표에서는 탐지할 수 있는 포트스캔 활동 유형에 대해 설명합니다.

표 21-3 포트 스캔 유형

유형	설명
포트 스캔 탐지	공격자가 단일 대상 호스트에서 여러 포트를 스캔하기 위해 하나 또는 소수의 호스트를 사용하는 일대일 포트스캔. 일대일 포트 스캔의 특성: • 스캔하는 호스트 수가 적음 • 단일 호스트가 스캔됨 • 스캔되는 포트 수가 많음 이 옵션은 TCP, UDP 및 IP 포트스캔을 탐지합니다.
포트 스윕	공격자가 하나 또는 여러 호스트를 사용하여 여러 대상 호스트에서 단일 포트를 스캔하는 일 대 다 포트 스윕. 포트 스윕에는 다음과 같은 특징이 있습니다. • 적은 수의 스캐닝 호스트 • 많은 수의 스캐닝된 호스트 • 적은 수의 스캐닝된 고유 포트 이 옵션은 TCP, UDP, ICMP 및 IP 포트 스윕을 탐지합니다.
Decoy 포트 스캔	공격자가 실제 스캐닝 IP 주소와 스푸핑된 소스 IP 주소를 혼합하는 일 대 일 포트 스캔. Decoy 포트 스캔에는 다음과 같은 특징이 있습니다. • 많은 수의 스캐닝 호스트 • 한 번만 스캐닝된 적은 수의 포트 • 스캐닝된 단일 (또는 적은 수의) 호스트 Decoy 포트 스캔 옵션은 TCP, UDP 및 IP 프로토콜 포트 스캔을 탐지합니다.
분산형 포트 스캔	여러 호스트가 개방형 포트를 위해 단일 호스트를 쿼리하는 다 대 일 포트 스캔 분산형 포트 스캔에는 다음과 같은 특징이 있습니다. • 많은 수의 스캐닝 호스트 • 한 번만 스캐닝된 많은 수의 포트 • 스캐닝된 단일 (또는 적은 수의) 호스트 분산형 포트 스캔 옵션은 TCP, UDP 및 IP 프로토콜 포트 스캔을 탐지합니다.

포트 스캔 탐지기가 프로브에 대해 알게 되는 정보는 대개 검토된 호스트에서 음수 응답이 표시되는 것을 기반으로 합니다. 예를 들어, 웹 클라이언트가 웹 서버에 연결을 시도할 때, 클라이언트는 포트 80/tcp를 사용하며 서버는 해당 포트가 열려 있도록 하는 역할을 수행할 수 있습니다. 그러나, 공격자가 서버를 검토할 때 웹 서비스가 제공되는지 여부를 미리 알 수 없습니다. 포트 스캔 탐지기에 음수 응답(즉 ICMP에 연결할 수 없는 패킷 또는 TCP RST 패킷)이 표시되면 해당 응답을 잠재적 포트 스캔으로 기록합니다. 이러한 프로세스는 대상 호스트가 음수 응답을 필터링하는 방화벽 또는 라우터와 같은 디바이스의 다른 편에 있는 경우 더욱 복잡합니다. 이 경우 포트스캔은 사용자가 선택한 민감도 레벨을 기반으로 *필터링된* 포트스캔 이벤트를 생성할 수 있습니다.

다음 표에서는 사용자가 선택할 수 있는 세 가지 민감도 레벨에 대해 설명합니다.

표 21-4 민감도 레벨

수준	설명
낮음	대상 호스트에서 부정적인 응답만 탐지합니다. 이 민감도 레벨을 선택하면 오탐을 억제할 수 있지만, 일부 포트스캔 유형(느린 스캔, 필터링된 스캔)을 놓칠 수 있습니다. 이 레벨은 포트스캔 탐지에 가장 짧은 시간 창을 사용합니다.
중간	호스트에 대한 연결 수를 기반으로 포트스캔을 탐지합니다. 즉, 필터링된 포트스캔을 탐지할 수 있습니다. 그러나 네트워크 주소 변환기와 프록시 등 매우 활동적인 호스트는 오탐을 생성할 수 있습니다. 이 유형의 오탐을 완화하려면 이러한 활동적인 호스트의 IP 주소를 **Ignore Scanned(스캔을 탐지하지 않음)** 필드에 추가할 수 있습니다. 이 레벨은 포트스캔 탐지에 좀 더 긴 시간 창을 사용합니다.
높음	시간 창을 기반으로 포트스캔을 탐지합니다. 즉, 시간 기반 포트스캔을 탐지할 수 있습니다. 그러나 이 옵션을 사용할 경우 **Ignore Scanned(스캔을 탐지하지 않음)** 및 **Ignore Scanner(스캐너를 탐지하지 않음)** 필드에 IP 주소를 지정하여 시간에 따라 탐지기를 신중하게 조정해야 합니다. 이 레벨은 포트스캔 탐지에 훨씬 긴 시간 창을 사용합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 21-5페이지의 포트 스캔 탐지 구성
- 21-7페이지의 포트 스캔 이벤트의 이해

포트 스캔 탐지 구성

라이센스: 보호

포트스캔 탐지 구성 옵션을 사용하면 포트스캔 탐지기가 스캔 활동을 보고하는 방식을 세부적으로 조정할 수 있습니다.

포트스캔 탐지가 활성화된 경우 포트스캔 탐지기의 활성화된 포트스캔 유형이 포트스캔 이벤트를 생성하도록 하려면 침입 정책 Rules(규칙) 페이지에서 GID(generator ID) 122로 규칙을 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정 및 포트 스캔 탐지 SID (GID: 122) 표를 참조하십시오.

포트 스캔 탐지를 구성하려면 다음을 수행합니다.

Admin(관리)/Intrusion Admin(침입 관리)

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에 있는 저장하지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 [was Committing Intrusion Policy Changes; update xref]을/를 참조하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 **Specific Threat Detection(특정 위협 탐지)** 아래의 **Portscan Detection(포트 스캔 탐지)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

  Portscan Detection(포트 스캔 탐지) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 다음 중 활성화할 프로토콜을 **Protocol(프로토콜)** 필드에서 지정합니다.

- TCP
- UDP
- ICMP
- IP

여러 프로토콜을 선택하거나 개별 프로토콜을 지우려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다. 자세한 내용은 프로토콜 유형 표를 참고하십시오.

TCP를 통해 스캔을 탐지할 수 있도록 TCP 스트림 프로세싱이 활성화되었는지, 그리고 UDP를 통해 스캔을 탐지할 수 있도록 UDP 스트림 프로세싱이 활성화되었는지 확인해야 합니다.

단계 10 다음 중 탐지할 포트스캔을 **Scan Type(스캔 유형)** 필드에서 지정합니다.

- 포트 스캔 탐지
- 포트 스윕
- Decoy 포트 스캔
- 분산형 포트 스캔

여러 프로토콜을 선택하거나 선택 취소하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다. 자세한 내용은 포트 스캔 유형 표를 참고하십시오.

단계 11 사용할 레벨을 **Sensitivity Level(민감도 레벨)** 목록에서 선택합니다(low, medium, high).

자세한 내용은 민감도 레벨 표를 참고하십시오.

단계 12 선택적으로, 포트스캔 활동의 징후를 관찰할 호스트를 **Watch IP(IP 감시)** 필드에서 지정합니다. 모든 네트워크 트래픽을 관찰하려면 이 필드를 비워둡니다.

단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록(둘 중 하나 또는 모두)을 지정할 수 있습니다. IPv4 및 IPv6 주소 블록을 사용하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

단계 13 또는, **Ignore Scanner(스캐너를 탐지하지 않음)** 필드에서 스캐너로 건너뛸 호스트를 지정합니다. 특별히 활성화된 네트워크에서 호스트를 지정하려면 이 필드를 사용합니다. 시간이 지남에 따라 호스트 목록을 변경해야 합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. IPv4 및 IPv6 주소 블록을 사용하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

단계 14 또는, **Ignore Scanned(스캔을 탐지하지 않음)** 필드에서 스캔의 대상으로 건너뛸 호스트를 지정합니다. 특별히 활성화된 네트워크에서 호스트를 지정하려면 이 필드를 사용합니다. 시간이 지남에 따라 호스트 목록을 변경해야 합니다.

단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. IPv4 및 IPv6 주소 블록을 사용하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

단계 15 또는, **Detect Ack Scans(Ack 스캔 탐지)** 확인 상자를 비워 중앙 스트림에서 선택된 세션의 모니터링을 중지합니다.

참고 중앙 스트림 세션의 탐지는 ACK 스캔을 확인하는 데 도움이 되지만 특히 트래픽 과부하로 패킷을 삭제한 네트워크에 잘못된 이벤트를 발생시킬 수 있습니다.

단계 16 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

포트 스캔 이벤트의 이해

라이센스: 보호

포트 스캔 탐지가 활성화되면, 활성화된 각 포트 스캔 유형에 대한 이벤트를 생성하기 위해 생성기 ID(GID) 122 및 SID 1에서 27 사이의 Snort® ID(SID)로 규칙을 활성화해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오. 다음 표의 **Preprocessor Rule SID(전처리기 규칙 SID)** 열은 각 포트 스캔 유형에 대해 활성화해야 할 전처리기 규칙에 대한 SID를 나열합니다.

표 21-5 포트 스캔 탐지 SID (GID: 122)

포트 스캔 유형	프로토콜:	민감도 수준	전처리기 규칙 SID
포트 스캔 탐지	TCP	낮음	1
		중간 또는 높음	5
	UDP	낮음	17
		중간 또는 높음	21
	ICMP	낮음	이벤트를 생성하지 않습니다.
		중간 또는 높음	이벤트를 생성하지 않습니다.
	IP	낮음	9
		중간 또는 높음	13
포트 스윕	TCP	낮음	3, 27
		중간 또는 높음	7
	UDP	낮음	19
		중간 또는 높음	23
	ICMP	낮음	25
		중간 또는 높음	26
	IP	낮음	11
		중간 또는 높음	15
Decoy 포트 스캔	TCP	낮음	2
		중간 또는 높음	6
	UDP	낮음	18
		중간 또는 높음	22
	ICMP	낮음	이벤트를 생성하지 않습니다.
		중간 또는 높음	이벤트를 생성하지 않습니다.
	IP	낮음	10
		중간 또는 높음	14
분산형 포트 스캔	TCP	낮음	4
		중간 또는 높음	8
	UDP	낮음	20
		중간 또는 높음	24
	ICMP	낮음	이벤트를 생성하지 않습니다.
		중간 또는 높음	이벤트를 생성하지 않습니다.
	IP	낮음	12
		중간 또는 높음	16

관련 전처리기 규칙을 활성화하면, 포트 스캔 탐지기는 다른 모든 침입 이벤트를 수행할 때 표시될 수 있는 침입 이벤트를 생성합니다. 그러나, 패킷 보기에 표시되는 정보는 다른 유형의 침입 이벤트와는 다릅니다. 이 섹션에서는 네트워크에 발생한 프로브 유형을 이해하기 위해 해당 정보를 사용할 수 있는 방법과 포트 스캔 이벤트에 대한 패킷 보기에 나타나는 필드에 대해 설명합니다.

포트 스캔 이벤트에 대한 패킷 보기로 드릴 다운하는 침입 이벤트 보기를 사용하는 것으로 시작합니다.

단일 포트 스캔 이벤트가 여러 패킷에 기반하므로 포트 스캔 패킷을 다운로드할 수 없습니다. 그러나, 포트 스캔 패킷 보기는 모든 가용 패킷 정보를 제공합니다.

참고 포트 스캔 연결 탐지기에서 생성된 이벤트의 경우, 프로토콜 번호는 255로 설정됩니다. 포트 스캔은 기본적으로 연결할 특정 프로토콜이 없기 때문에, IANA(Internet Assigned Numbers Authority, 인터넷 할당 번호 관리기관)에는 그에 할당된 프로토콜 번호가 없습니다. IANA는 255를 예약된 번호로 지정하여 해당 번호가 포트 스캔 이벤트에서 사용되는 경우 해당 이벤트에 대해 연결된 프로토콜이 없음을 나타냅니다.

다음 표는 포트 스캔 이벤트를 위한 패킷 보기에서 제공되는 정보에 대해 설명합니다.

표 21-6 포트 스캔 패킷 보기

정보	설명
디바이스	이벤트를 탐지한 디바이스입니다.
시간	이벤트가 발생한 시간입니다.
메시지	전처리기에서 생성된 이벤트 메시지입니다.
소스 IP	스캐닝하는 호스트의 IP 주소입니다.
대상 IP	스캐닝된 호스트의 IP 주소입니다.
우선 순위 집계	스캐닝된 호스트로부터의 음수 응답 수(예를 들어, TCP RSTs 및 ICMP에 도달할 수 없는)입니다. 음수 응답 수가 많을수록 우선 순위가 높습니다.
연결 집계	호스트에 연결된 활성 연결 수입니다. 이 값은 TCP 및 IP와 같은 연결 기반 스캔의 경우 더 정확합니다.
IP 집계	스캐닝된 호스트에 연결된 IP 주소가 변경된 횟수입니다. 예를 들어, 첫 번째 IP 주소가 10.1.1.1인 경우, 두 번째 IP는 10.1.1.2이며, 3 번째 IP는 10.1.1.1이며, 다음으로 IP 수는 3입니다. 이 번호는 프록시 및 DNS 서버 등 활성 호스트의 경우 덜 정확합니다.
스캐너/스캐닝된 IP 범위	스캔 유형에 따른 스캐닝된 호스트 또는 스캐닝하는 호스트의 IP 주소 범위입니다. 포트 스윕의 경우, 이 필드는 스캐닝된 호스트의 IP 범위를 보여줍니다. 포트 스캔의 경우, 이는 스캐닝하는 호스트의 IP 범위를 보여줍니다.
포트/프로토콜 집계	TCP와 UDP 포트 스캔의 경우, 스캐닝되고 있는 포트가 변경된 횟수입니다. 예를 들어, 스캐닝된 첫 번째 포트가 80인 경우, 스캐닝된 두 번째 포트는 8080이고, 스캐닝된 세 번째 포트는 다시 80이며, 다음 포트 수는 3입니다. IP 프로토콜 포트 스캔의 경우, 스캐닝된 호스트에 연결하기 위해 사용되고 있는 프로토콜의 변경 횟수입니다.
포트/프로토콜 범위	TCP와 UDP 포트 스캔의 경우, 스캐닝된 포트 범위입니다. IP 프로토콜 포트 스캔의 경우, 스캐닝된 호스트에 연결하려고 시도하는 데 사용되는 IP 프로토콜 수의 범위입니다.
개방 포트	스캐닝된 호스트에 개방된 TCP 포트입니다. 이 필드는 포트 스캔이 하나 이상의 개방형 포트를 탐지하는 경우에만 나타납니다.

속도 기반 공격 방지

라이센스: 보호

속도 기반 공격은 공격을 저지르는 연결 또는 반복된 시도의 빈도에 따른 공격입니다. 속도 기반 탐지 기준을 사용하여 속도 기반 공격이 발생한 경우 이를 탐지하고 공격이 발생하는 경우 이에 반응한 후 공격이 중단되면 일반 탐지 설정으로 돌아옵니다. 속도 기반 탐지 구성에 대한 자세한 내용은 다음 주제를 참고하십시오.

- 21-10페이지의 속도 기반 공격 방지의 이해
- 21-13페이지의 속도 기반 공격 차단 및 다른 필터
- 21-18페이지의 속도 기반 공격 차단 구성
- 20-29페이지의 동적 규칙 상태의 이해
- 20-30페이지의 동적 규칙 상태 설정

속도 기반 공격 방지의 이해

라이센스: 보호

네트워크의 호스트로 향하는 과도한 활동을 탐지하는 속도 기반 필터를 포함하도록 네트워크 분석 정책을 구성할 수 있습니다. 인라인 모드로 배포된 디바이스에서 이 기능을 사용하여 지정된 시간 동안 속도 기반 공격을 차단한 후 이벤트 생성으로만 되돌아가며 트래픽을 삭제하지는 않습니다.

속도 기반 공격 방지는 잘못된 트래픽 패턴을 식별하고 정당한 요청에 대한 해당 트래픽의 영향을 최소화하려고 합니다. 속도 기반 공격은 일반적으로 다음 중 하나의 특성을 갖습니다.

- 네트워크의 호스트로 향하는 불완전한 연결을 포함하는, SYN 플러드 공격을 나타내는 모든 트래픽

  SYN 공격 탐지를 구성하려면 21-12페이지의 SYN 공격 방지를 참고하십시오.
- 네트워크의 호스트로 향하는 과도하고 완전한 연결을 포함하는, TCP/IP 연결 플러드 공격을 나타내는 모든 트래픽

  동시 연결 탐지를 구성하려면 21-12페이지의 동시 연결 조정을 참고하십시오.
- 특정 대상 IP 주소 또는 주소로 이동하거나 특정 소스 IP 주소 또는 주소에서 오는 트래픽에서의 과도한 규칙 일치.

  소스 또는 대상 기반 동적 규칙 상태를 구성하려면 20-30페이지의 동적 규칙 상태 설정을 참고하십시오.
- 모든 트래픽을 가로지르는 특정 규칙에 대한 과도한 일치 항목.

  규칙 기반 동적 규칙 상태를 구성하려면 20-30페이지의 동적 규칙 상태 설정을 참고하십시오.

네트워크 분석 정책에서 전체 정책에 대한 SYN flood 또는 TCP/IP 연결 flood 탐지를 구성할 수 있습니다. 침입 정책에서 개별적인 침입 또는 전처리기 규칙을 위한 속도 기반 필터를 설정할 수 있습니다. 규칙 135:1과 135:2에 수동으로 속도 기반 필터를 추가하는 것은 아무 효과가 없다는 점에 유의하십시오. GID:135가 포함된 규칙은 해당 클라이언트를 소스 값으로 사용하고 해당 서버를 대상 값으로 사용합니다. 자세한 내용은 21-12페이지의 SYN 공격 방지 및 21-12페이지의 동시 연결 조정을 참고하십시오.

각 속도 기반 필터에는 여러 구성 요소가 포함되어 있습니다.

- 전정책적 또는 규칙 기반의 소스 또는 대상 설정의 경우, 네트워크 주소 할당
- 특정 초 이내 규칙 일치의 계수로 구성한 규칙 일치 비율

- 속도를 초과할 경우 취해야 할 새로운 작업

  전체 정책에 대한 속도 기반 설정을 설정한 경우, 시스템이 속도 기반 공격을 탐지하면 이벤트를 생성하고, 선택적으로 인라인 배포에서 트래픽을 삭제할 수 있습니다. 개별 규칙에 대한 속도 기반 작업을 설정할 때, 사용 가능한 작업에는 3가지의 Generate Events(이벤트 생성), Drop and Generate Events(이벤트 삭제 및 생성), Disable(비활성화)이 있습니다.

- 시간 제한 값으로 설정한 작업 기간

시작한 경우, 속도가 해당 기간 동안 구성된 속도까지 떨어지더라도 시간 제한에 도달할 때까지 새로운 작업이 발생한다는 점에 유의하십시오. 시간 제한이 만료되면, 속도가 임계값 아래로 떨어진 경우, 규칙 작업은 규칙에 처음 설정된 작업으로 돌아갑니다. 전정책적 설정에 대해, 작업은 트래픽이 일치하는 각 규칙의 작업으로 돌아가거나 어느 규칙과도 일치하지 않는 경우 중단됩니다.

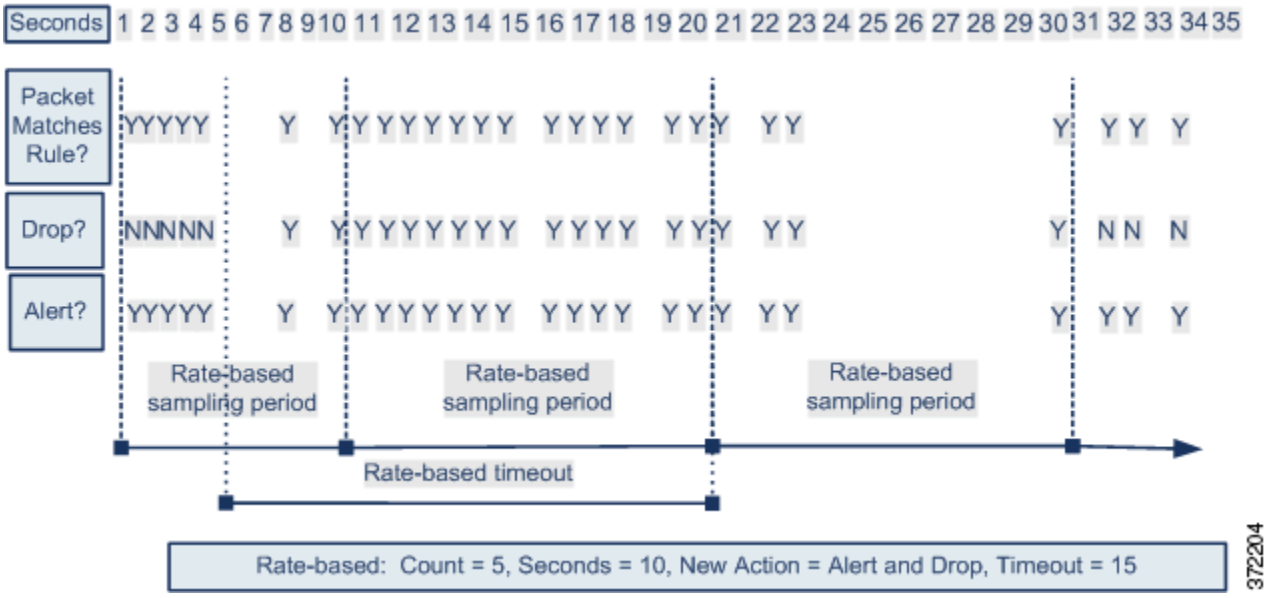
인라인 배포에서 속도 기반 공격 차단을 구성하여 일시적으로 또는 영구적으로 공격을 차단할 수 있습니다. 속도 기반 구성 없이, Generate Events(이벤트 생성)로 설정된 규칙은 이벤트를 생성하지만 시스템은 해당 규칙에 대한 패킷을 삭제하지 않습니다. 그러나, 속도 기반 기준이 구성되어 있는 규칙이 공격 트래픽과 일치하는 경우, 해당 규칙이 처음에는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되어 있지 않더라도 속도 작업은 속도 작업이 활성화된 기간 동안 패킷이 삭제되도록 할 수 있습니다.

참고 속도 기반 작업은 비활성화된 규칙을 활성화하거나 비활성화된 규칙에 일치하는 트래픽을 삭제할 수 없습니다. 그러나, 정책 수준에서 속도 기반 필터를 설정하는 경우, 지정된 기간 이내에 SYN 패킷 또는 SYN/ACK 상호작용의 과도한 수를 포함하는 트래픽에 이벤트를 생성하거나 트래픽에 이벤트를 생성하고 삭제할 수 있습니다.

동일한 규칙에서 다중 속도 기반 필터를 정의할 수 있습니다. 침입 정책에 나열된 첫 번째 필터의 우선 순위가 가장 높습니다. 두 개의 속도 기반 필터 작업이 충돌할 때 시스템은 첫 번째 속도 기반 필터의 작업을 시행합니다. 마찬가지로, 필터가 충돌하는 경우 전정책적 속도 기반 필터는 개별 규칙에 설정된 속도 기반 필터를 재정의합니다.

다음 다이어그램은 공격자가 호스트에 액세스하기 위해 시도하는 예를 보여줍니다. 비밀번호를 찾으려는 반복된 시도는 속도 기반 공격 방지를 구성한 규칙을 트리거합니다. 속도 기반 설정은 10초 범위 안에 규칙 일치가 다섯 번 발생하면 규칙 속성을 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다. 새로운 규칙 속성은 15초 후 시간 초과됩니다.

시간 제한 후에도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값 속도보다 높을 경우, 새로운 작업은 계속됩니다. 새로운 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 이벤트 생성으로 돌아갑니다.



SYN 공격 방지

라이센스: 보호

SYN 공격 방지 옵션을 통해 SYN 플러드 공격에 대해 네트워크 호스트를 보호할 수 있습니다. 일정 기간 동안 발견된 패킷 수에 따라 개별 호스트 또는 전체 네트워크를 보호할 수 있습니다. 디바이스가 수동으로 구축된 경우, 이벤트를 생성할 수 있습니다. 디바이스가 인라인에 위치한 경우, 악성 패킷 또한 삭제할 수 있습니다. 시간 제한이 경과한 후 속도 상태가 중단될 경우, 이벤트 생성 및 패킷 삭제가 중지됩니다.

예를 들어, 어느 것이든 하나의 IP 주소에서 최대 10개의 SYN 패킷을 허용하도록 설정을 구성할 수 있으며, 60초 동안 해당 IP 주소에서 추가 연결을 차단할 수 있습니다.

이 옵션을 활성화하면 규칙 135:1을 활성화합니다. 이 규칙을 수동으로 활성화하면 효과가 없습니다. 규칙 상태는 항상 Disabled(비활성화)로 표시되며 변경되지 않습니다. 이 옵션이 활성화되고 정의된 속도 조건을 초과할 경우 규칙에서 이벤트를 생성합니다.

동시 연결 조정

라이센스: 보호

또한 네트워크에서 호스트를 오가는 TCP/IP 연결을 제한하여 서비스 거부 공격(DoS) 또는 사용자의 과도한 활동을 방지할 수 있습니다. 시스템이 특정 IP 주소 또는 주소 범위를 오가는 성공적인 연결의 구성된 수를 탐지하는 경우, 추가 연결에서 이벤트를 생성합니다. 속도 기반 이벤트 생성은 속도 조건의 발생 없이 시간 제한이 경과할 때까지 계속됩니다. 인라인 배포에서 속도 조건이 시간 초과될 때까지 패킷을 삭제하도록 선택할 수 있습니다.

예를 들어, 어느 것이든 하나의 IP 주소에서 최대 10개의 동시 연결이 성공할 수 있도록 설정을 구성할 수 있으며, 60초 동안 해당 IP 주소에서 추가 연결을 차단할 수 있습니다.

이 옵션을 활성화하면 규칙 135:2를 활성화합니다. 이 규칙을 수동으로 활성화하면 효과가 없습니다. 규칙 상태는 항상 Disabled(비활성화)로 표시되며 변경되지 않습니다. 이 옵션이 활성화되고 정의된 속도 조건을 초과할 경우 규칙에서 이벤트를 생성합니다.

속도 기반 공격 차단 및 다른 필터

라이센스: 보호

detection_filter 키워드 및 임계값 설정 그리고 삭제 기능은 트래픽 자체 또는 시스템에서 생성된 이벤트를 필터링할 다른 방법을 제공합니다. 속도 기반 공격 차단을 단독으로 사용하거나 임계값 설정, 삭제, 또는 detection_filter 키워드를 조합하여 사용할 수 있습니다.

자세한 내용은 다음 예를 참고하십시오.

- 21-13페이지의 속도 기반 공격 방지 및 탐지 필터링
- 21-14페이지의 동적 규칙 상태 및 임계값 설정 또는 삭제
- 21-16페이지의 전정책적 속도 기반 탐지 및 임계값 설정 또는 삭제
- 21-17페이지의 여러 필터링 방법으로 속도 기반 탐지

속도 기반 공격 방지 및 탐지 필터링

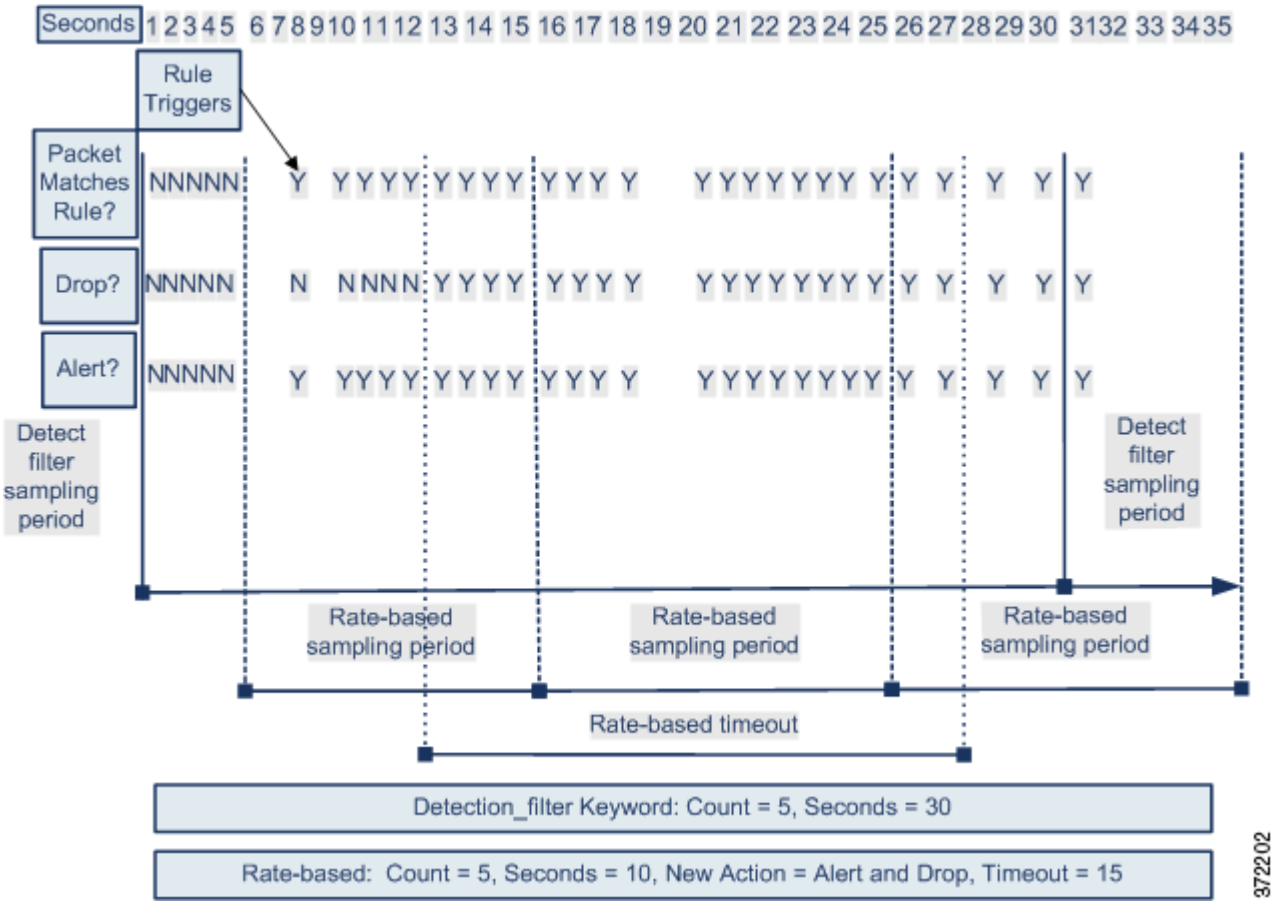
라이센스: 보호

detection_filter 키워드는 지정된 시간 내에 규칙 일치의 임계값 수가 나올 때까지 규칙이 트리거되지 않도록 합니다. 규칙이 detection_filter 키워드를 포함할 경우, 시스템은 시간 제한별 규칙에서 패턴 일치한 수신 패킷 수를 추적할 수 있습니다. 시스템은 특정 소스 또는 대상 IP 주소에서 해당 규칙 적중 횟수를 카운트할 수 있습니다. 속도가 규칙의 속도를 초과한 후, 해당 규칙에 대한 이벤트 알림이 시작됩니다.

다음의 예시는 무작위 대입 로그인을 시도한 공격자를 보여줍니다. 비밀번호를 찾는 반복된 시도는 또한 5로 설정된 계수와 함께 detection_filter 키워드를 포함하는 규칙을 트리거합니다. 이 규칙은 속도 기반 공격 방지가 구성되도록 합니다. 속도 기반 설정은 10초 범위 안에 규칙을 다섯 번 적중할 경우 규칙 속성을 20초 동안 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다.

다이어그램에 보여진 것과 같이, 속도가 detection_filter 키워드에 표시된 속도를 초과할 때까지 규칙이 트리거되지 않으므로 규칙과 일치하는 첫 5개의 패킷은 이벤트를 생성하지 않습니다. 규칙이 트리거되면 이벤트 알림이 시작되지만, 속도 기반 기준은 5개의 추가 패킷이 통과할 때까지 Drop and Generate Events(이벤트 삭제 및 생성)의 새로운 작업을 트리거하지 않습니다.

속도 기반 기준이 충족되면, 이벤트가 생성되고, 속도 기반 시간 제한이 만료되고 속도가 임계값 아래로 떨어질 때까지 패킷은 삭제됩니다. 20초 경과 후, 속도 기반 작업은 시간 초과됩니다. 시간 제한 후에도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 시간 제한이 발생할 때 샘플링된 속도는 이전 샘플링 기간의 임계값 속도보다 높으므로, 속도 기반 작업이 계속됩니다.



예제는 이를 표시하지 않지만, Drop and Generate Events(이벤트 삭제 및 생성) 규칙 상태를 `detection_filter` 키워드와 조합하여 사용하면 규칙에 대한 적중 수가 지정된 속도에 도달했을 때 트래픽 삭제를 시작할 수 있다는 점에 유의하십시오. 속도 기반 설정을 구성할 것인지 여부를 결정할 때, 규칙을 Drop and Generate Events(이벤트 삭제 및 생성)로 설정할지 여부와 `detection_filter` 키워드를 포함할지 여부가 같은 결과를 초래한다는 점을 고려하십시오. 침입 정책의 속도 및 시간 제한 설정을 관리할 것인지 여부도 마찬가지입니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

동적 규칙 상태 및 임계값 설정 또는 삭제

라이센스: 보호

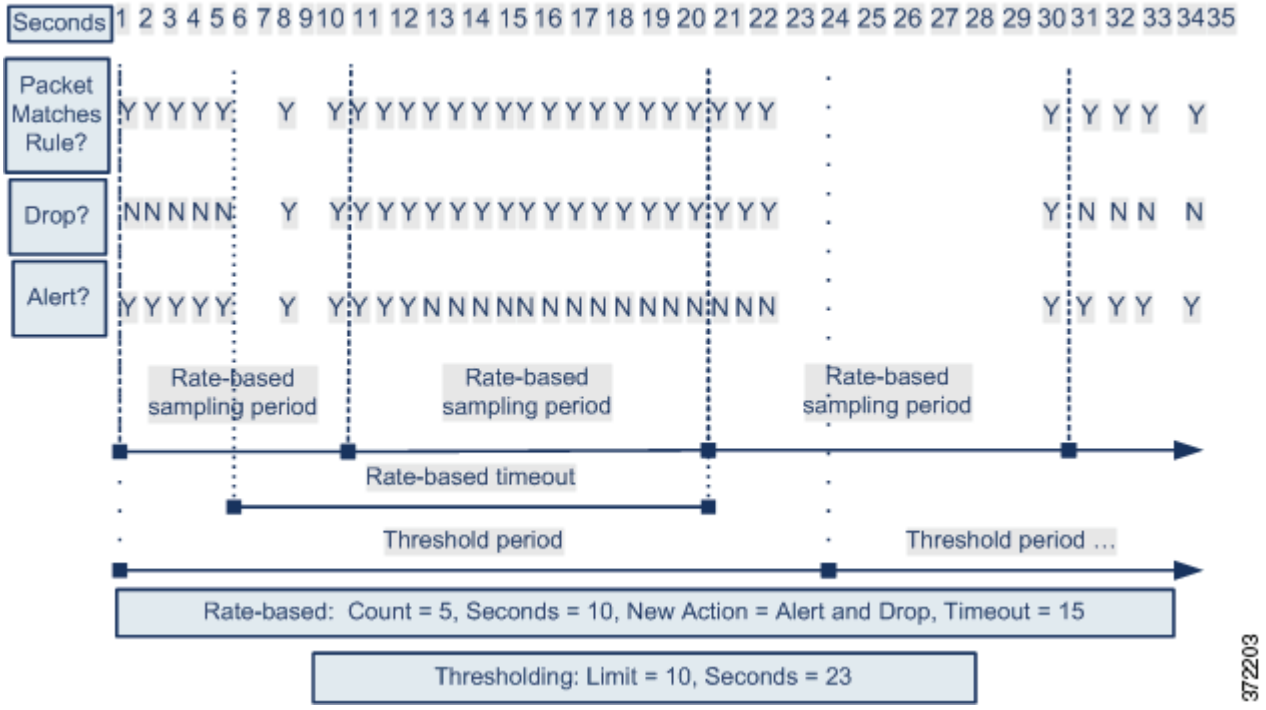
임계값 설정 및 삭제를 사용하여 규칙에 대한 이벤트 알림 수를 제한함으로써 또는 해당 규칙에 대한 알림을 모두 삭제함으로써 과도한 이벤트를 삭제할 수 있습니다. 임계값 설정 및 삭제를 위한 사용 가능한 옵션에 대한 추가 정보는 20-22페이지의 이벤트 임계값 설정 구성 및 20-26페이지의 침입 정책에 따른 삭제 구성을 참고하십시오.

규칙에 삭제를 적용할 경우, 속도 기반 작업 변화가 발생한 경우에도 시스템은 모든 사용 가능한 IP 주소에 대한 해당 규칙을 위한 이벤트 알림을 삭제합니다. 그러나, 임계값 설정 및 속도 기반 기준 간 상호 작용은 더 복잡합니다.

다음의 예시는 무작위 대입 로그인을 시도한 공격자를 보여줍니다. 비밀번호를 찾으려는 반복된 시도는 속도 기반 공격 방지를 구성한 규칙을 트리거합니다. 속도 기반 설정은 10초 안에 규칙을 다섯 번 적중할 경우 규칙 속성을 15초 동안 Drop and Generate Events(이벤트 삭제 및 생성)로 변경합니다. 또한, 제한 임계값은 규칙이 23초 안에 10개의 이벤트를 생성할 수 있도록 이벤트 수를 제한합니다.

다이어그램에 보여진 것과 같이, 규칙은 처음 5개의 일치 패킷의 이벤트를 생성합니다. 속도 기반 기준은 5개의 패킷 후 Drop and Generate Events(이벤트 삭제 및 생성)의 새로운 작업을 트리거하며, 다음 5개의 패킷 중에 규칙은 이벤트를 생성하고 시스템은 패킷을 삭제합니다. 10개의 패킷 후, 제한 임계값에 도달하므로, 나머지 패킷에 대해 시스템은 이벤트를 생성하지 않지만 패킷을 삭제합니다.

시간 제한 후에도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값 속도보다 높을 경우, 새로운 작업은 계속됩니다. 새로운 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 Generate Events(이벤트 생성)로 돌아갑니다.



예제는 이를 표시하지 않지만, 임계값에 도달 *후* 속도 기반 기준으로 인해 새로운 작업이 트리거되는 경우, 시스템은 작업 변화를 나타내는 단일 이벤트를 생성합니다. 따라서, 예를 들면, 제한 임계값인 10에 도달하고 시스템이 이벤트 생성을 중단하며 작업이 14번째 패킷에서 Drop and Generate Events(이벤트 삭제 및 생성)에서 Generate Events(이벤트 생성)으로 변경되었을 때, 시스템은 작업 변화를 나타내는 11번째 이벤트를 생성합니다.

전정책적 속도 기반 탐지 및 임계값 설정 또는 삭제

라이센스: 보호

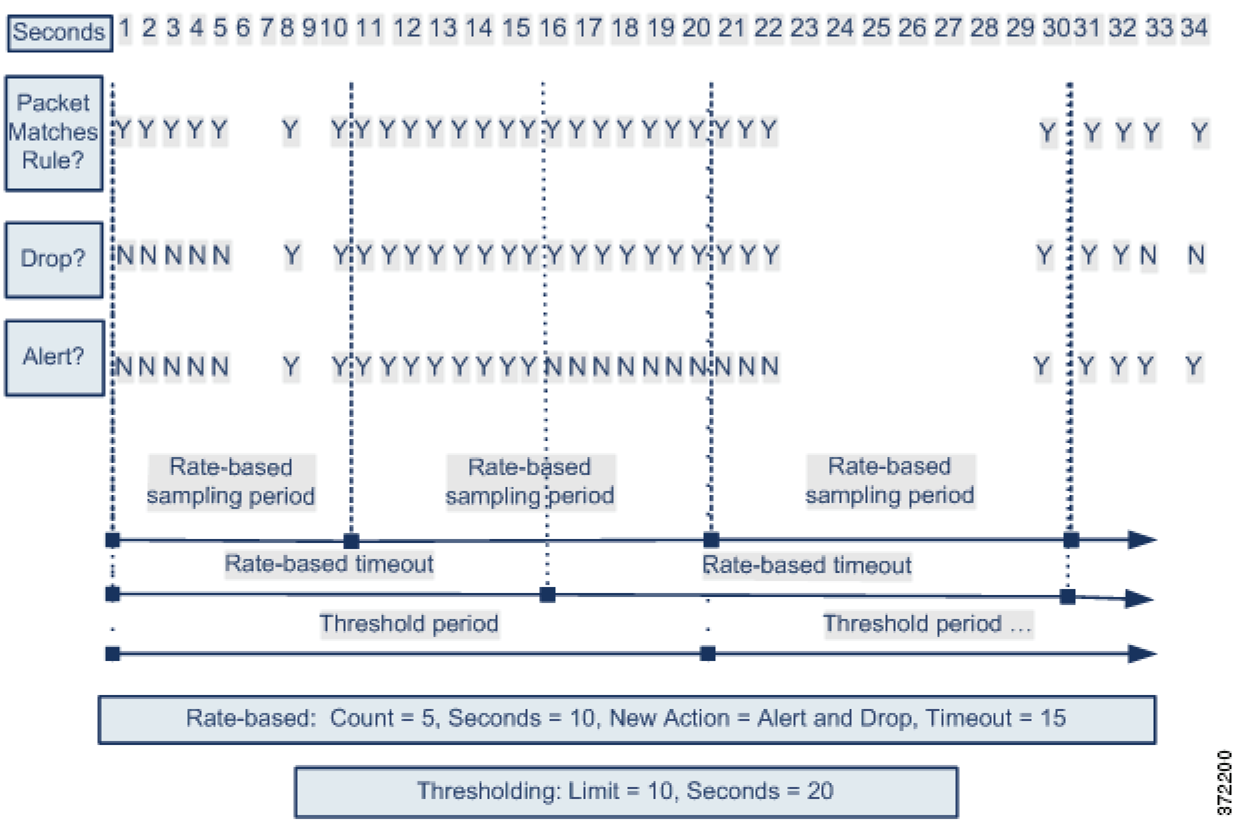
임계값 설정 및 삭제를 사용하여 소스 또는 대상에 대한 이벤트 알림 수를 제한함으로써 또는 해당 규칙에 대한 알림을 모두 삭제함으로써 과도한 이벤트를 줄일 수 있습니다. 임계값 설정 및 삭제를 위한 사용 가능한 옵션에 대한 자세한 내용은 22-3페이지의 전역 임계값 구성, 20-22페이지의 이벤트 임계값 설정 구성 및 20-26페이지의 침입 정책에 따른 삭제 구성을 참고하십시오.

삭제가 규칙에 적용된 경우, 전정책적 또는 특정 규칙 속도 기반 설정으로 인해 속도 기반 작업 변화가 발생하는 경우에도 적용 가능한 모든 IP 주소의 규칙에 대한 이벤트 알림은 삭제됩니다. 그러나, 임계값 설정 및 속도 기반 기준 간 상호 작용은 더 복잡합니다.

다음의 예시는 네트워크에서 호스트에 서비스 거부 공격(DoS) 공격을 시도한 공격자를 보여줍니다. 동일한 소스로부터 호스트로 향하는 많은 동시 연결은 전정책적 Control Simultaneous Connections(제어 동시 연결) 설정을 시작합니다. 설정은 10초 안에 한 개의 소스로부터 5개의 연결이 있을 때 이벤트를 생성하고 악성 트래픽을 삭제합니다. 또한, 전역 제한 임계값은 모든 규칙 또는 설정이 20초 안에 10개의 이벤트를 생성할 수 있도록 이벤트 수를 제한합니다.

다이어그램에 표시된 대로 전정책적 설정은 처음 10개의 일치 패킷의 이벤트를 생성하며 트래픽을 삭제합니다. 10개의 패킷 후, 제한 임계값에 도달되므로, 나머지 패킷에 대한 어떤 이벤트도 생성되지 않지만 패킷이 삭제됩니다.

시간 제한 후에도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값 속도보다 높을 경우, 이벤트를 생성하고 트래픽을 삭제하는 속도 기반 작업은 계속됩니다. 속도 기반 작업은 샘플링된 속도가 임계값 속도보다 낮은 샘플링 기간을 완료한 후에만 중지됩니다.



예제는 이를 표시하지 않지만, 임계값에 도달 *후* 속도 기반 기준으로 인해 새로운 작업이 트리거되는 경우, 시스템은 작업 변화를 나타내는 단일 이벤트를 생성합니다. 따라서, 예를 들면, 제한 임계값인 10에 도달하고 시스템이 이벤트 생성을 중단하며 작업이 14번째 패킷에서 Drop and Generate Events(이벤트 삭제 및 생성)로 변경되었을 때, 시스템은 작업 변화를 나타내는 11번째 이벤트를 생성합니다.

여러 필터링 방법으로 속도 기반 탐지

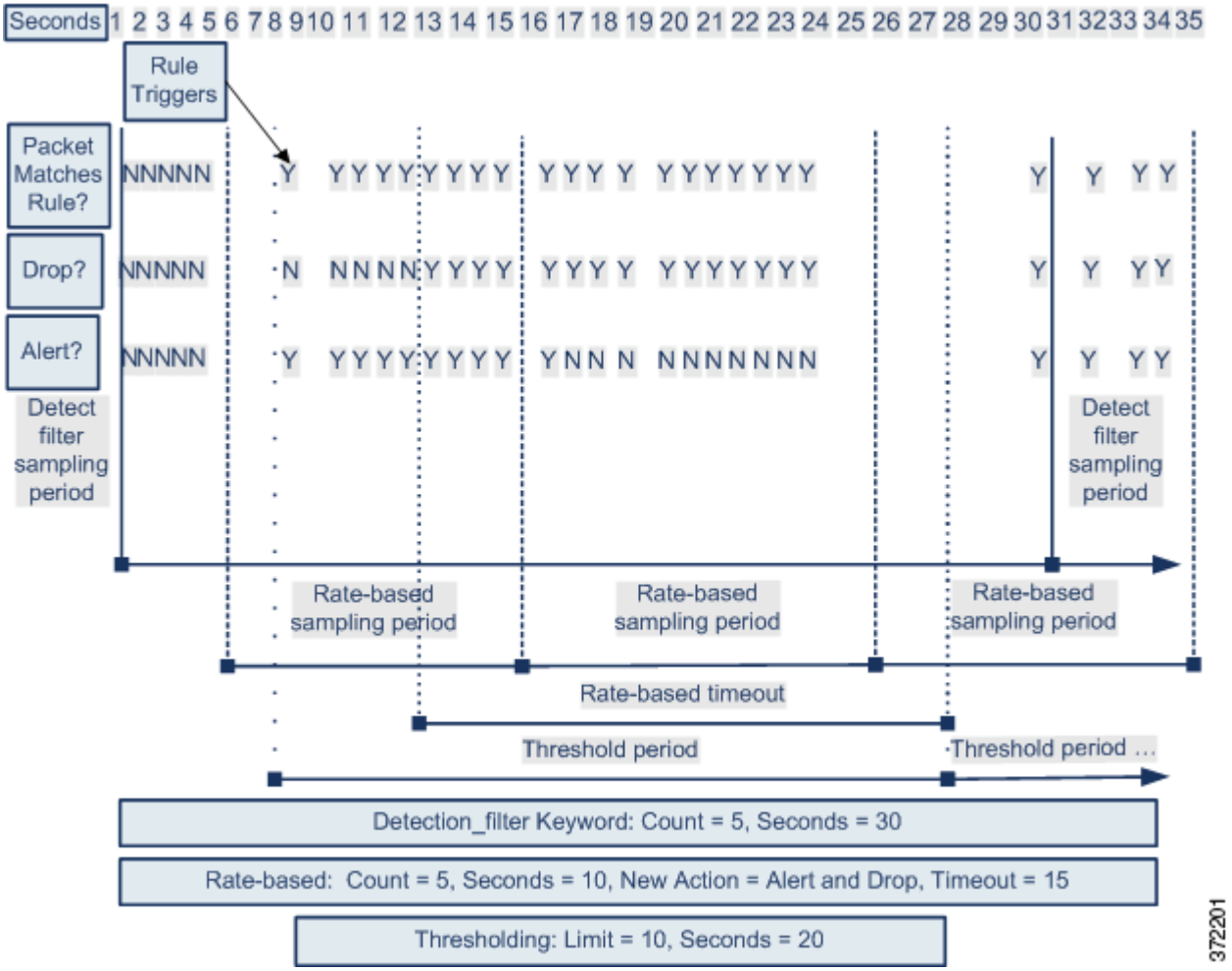
라이센스: 보호

`detection_filter` 키워드, 임계값 설정 또는 삭제 및 속도 기반 기준이 모두 동일한 트래픽에 적용되는 상황이 발생할 수 있습니다. 규칙에 대한 삭제를 활성화하면, 속도 기반 변경이 발생한 경우에도 이벤트는 지정된 IP 주소에 대해 삭제됩니다.

다음의 예시는 무작위 대입 로그인을 시도한 공격자를 표시하고, `detection_filter` 키워드, 속도 기반 필터링, 임계값 설정이 상호 작용하는 경우에 대해 설명합니다. 비밀번호를 찾는 반복된 시도는 또한 5로 설정된 계수와 함께 `detection_filter` 키워드를 포함하는 규칙을 트리거합니다. 이 규칙에는 또한 15초 안에 다섯 번의 적중이 있을 경우 규칙 속성을 30초 동안 Drop and Generate Events(이벤트 삭제 및 생성)로 변경하는 속도 기반 공격 방지 설정이 있습니다. 또한, 제한 임계값은 규칙이 30초 안에 10개의 이벤트를 생성할 수 있도록 규칙을 제한합니다.

다이어그램에 표시된 대로 속도가 `detection_filter` 키워드에 표시된 속도를 초과할 때까지 규칙이 트리거되지 않으므로 규칙과 일치하는 첫 5개의 패킷은 이벤트 알림을 야기하지 않습니다. 규칙이 트리거되면 이벤트 알림이 시작되지만, 속도 기반 기준은 5개의 추가 패킷이 통과할 때까지 Drop and Generate Events(이벤트 삭제 및 생성)의 새로운 작업을 트리거하지 않습니다. 속도 기반 기준이 충족되면, 시스템은 패킷 11-15를 위한 이벤트를 생성하고 패킷을 삭제합니다. 15개의 패킷 후 제한 임계값에 도달하므로, 나머지 패킷에 대해 시스템은 이벤트를 생성하지 않지만 패킷을 중단합니다.

속도 기반 시간 제한 후에도 패킷은 뒤따르는 속도 기반 샘플링 기간 안에 여전히 삭제된다는 점에 유의하십시오. 샘플링된 속도가 이전 샘플링 기간의 임계값 속도보다 높으므로 새로운 작업이 계속됩니다.



속도 기반 공격 차단 구성

라이센스: 보호

정책 수준에서 속도 기반 공격 차단을 구성하여 SYN 플러드 공격을 차단할 수 있습니다. 또한 특정 소스로부터 또는 특정 대상을 향한 과도한 연결을 중지할 수 있습니다.

속도 기반 공격 방지를 구성하려면 다음을 수행합니다.

Admin(관리)/Intrusion Admin(침입 관리)

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

액세스 제어 정책의 고급 설정 페이지가 나타납니다.

단계 4 수정 아이콘( )(**Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책)** 옆에 있음)을 클릭합니다.

Network Analysis and Intrusion Policies(네트워크 분석 및 침입 정책) 팝업 창이 나타납니다.

단계 5 **Network Analysis Policy List(네트워크 분석 정책 목록)**를 클릭합니다.

Network Analysis Policy List(네트워크 분석 정책 목록) 팝업 창이 나타납니다.

단계 6 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 7 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 8 **Specific Threat Detection(특정 위협 탐지)** 아래의 **Rate-Based Attack Prevention(속도 기반 공격 방지)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Rate-Based Attack Prevention(속도 기반 공격 방지) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 9 다음 2가지 옵션을 사용할 수 있습니다.

- 호스트를 초과하도록 고안된 불완전 연결을 차단하려면 **SYN Attack Prevention(SYN 공격 방지)** 아래의 **Add(추가)**를 클릭합니다.

  SYN Attack Prevention(SYN 공격 방지) 대화 상자가 나타납니다.

- 과도한 수의 연결을 방지하려면, **Control Simultaneous Connections(제어 동시 연결)** 아래의 **Add(추가)**를 클릭합니다.

  Control Simultaneous Connections(제어 동시 연결) 대화 상자가 나타납니다.

단계 10 트래픽을 추적할 방법을 선택합니다.

- 특정 소스 또는 소스의 범위로부터의 모든 트래픽을 추적하려면 **Track By(추적 기준)** 드롭다운 목록에서 **Source(소스)**를 선택하고 **Network(네트워크)** 필드에 단일 IP 주소 또는 주소 블록을 입력합니다.
- 특정 대상 또는 대상의 범위로 향하는 모든 트래픽을 추적하려면 **Track By(추적 기준)** 드롭다운 목록에서 **Destination(대상)**을 선택하고 **Network(네트워크)** 필드에 IP 주소 또는 주소 블록을 입력합니다.

시스템이 Network(네트워크) 필드에 포함된 각 IP 주소에 대한 개별 트래픽을 추적한다는 점에 유의하십시오. 구성한 속도 결과를 초과하는 단일 IP 주소로부터의 트래픽은 해당 IP 주소만을 위해 생성된 이벤트로 귀결됩니다. 한 예를 들어, 네트워크 구성에 `10.1.0.0/16`의 소스 CIDR 차단을 설정하고 10개의 동시 연결이 개방되어 있을 때 이벤트를 생성하도록 시스템을 구성할 수 있습니다. 10.1.4.21에서 8개의 연결이 열리고 10.1.5.10에서 6개의 연결이 열리는 경우, 어느 소스도 트리거하는 수의 연결을 갖고 있지 않으므로 시스템이 이벤트를 생성하지 않습니다. 그러나, 10.1.4.21에서 11개의 동시 연결이 열리는 경우, 시스템은 10.1.4.21으로부터의 연결에 해당하는 이벤트만 생성합니다.

CIDR 표기법 및 접두사 길이를 사용하는 것에 관한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

단계 11 설정을 추적하는 속도에 대해 시작 속도를 지정합니다.

- SYN 공격 구성에 대해, **Rate(속도)** 필드에 초당 SYN 패킷 수를 지정합니다.
- 동시 연결을 구성하려면, **Count(계수)** 필드에서 연결 수를 지정합니다.

단계 12 속도 기반 공격 방지 구성에 일치하는 패킷을 삭제하려면 **Drop(삭제)**을 선택합니다.

단계 13 **Timeout(시간 제한)** 필드에서, 일정 기간 이후에 이벤트 생성을 중지하려면 기간을 지정합니다. 그리고 해당되는 경우, SYN의 일치 패턴 또는 동시 연결을 가진 트래픽의 경우 이벤트를 삭제하는 기간을 지정합니다.

주의 시간 제한 값은 0에서 1,000,000 사이의 정수일 수 있습니다. 하지만, 높은 시간 제한 값을 설정하면 인라인 배포에서 호스트로 향하는 연결을 완전히 차단할 수 있습니다.

단계 14 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

민감한 데이터 검색

라이센스: 보호

사회 보장 번호, 신용카드 번호, 운전면허증 번호 같은 민감한 정보가 인터넷에 고의적으로 또는 실수로 유출될 수 있습니다. 이 시스템에서는 ASCII 텍스트로 된 민감한 데이터에 대한 이벤트를 탐지하고 생성할 수 있는 민감한 데이터 전처리기를 제공하며, 이는 실수로 인한 데이터 유출을 탐지할 때 특히 유용합니다.

시스템에서는 암호화되거나 위장된 형태의 민감한 데이터나 압축 또는 인코딩된 형식(예: Base64 인코딩 이메일 첨부 파일)의 민감한 데이터를 탐지하지 않습니다. 예를 들어, 시스템은 전화 번호 (555)123 - 4567을 탐지하지만, 각 번호가 스페이스로 구분되어 일부러 혼란스럽게 구성된 버전(5 5 5) 1 2 3 - 4 5 6 7, 또는 (555)-123-4567처럼 개입 HTML 코드)은 탐지하지 않습니다. 그러나, 시스템은, 개입 코드가 번호 패턴을 방해하지 않는 경우, 예를 들어, HTML 코드화된 번호 (555) - 123 - 4567와 같은 경우는 탐지합니다.

팁 민감한 데이터 전처리기는 FTP 또는 HTTP를 사용하여 업로드되고 다운로드된 암호화되지 않은 Microsoft 에서 민감한 데이터를 탐지할 수 있습니다. Word 파일이 ASCII 텍스트 및 서식 설정 명령을 별도로 분류하는 방식 때문에 이것이 가능합니다.

시스템에서는 개별 데이터 유형을 트래픽과 일치시켜 TCP 세션당 민감한 데이터를 탐지합니다. 사용자 침입 정책에서 모든 데이터 유형에 적용되는 전역 옵션 및 각 데이터 유형에 대한 기본 설정을 수정할 수 있습니다. Cisco는 미리 정의된, 일반적으로 사용되는 데이터 유형을 제공합니다. 또한 사용자 지정 데이터 유형을 만들 수 있습니다.

민감한 데이터 전처리기 규칙은 각 데이터 유형과 연결됩니다. 각 데이터 유형의 전처리기 규칙을 활성화하여 각 데이터 유형에 대한 민감한 데이터 탐지 및 이벤트 생성을 활성화할 수 있습니다. 구성 페이지 링크를 통해 Rules(규칙) 페이지에서 민감한 데이터를 필터링하여 볼 수 있는데, 여기서 규칙을 활성화/비활성화하고 다른 규칙 속성을 구성할 수 있습니다.

데이터 유형과 관련된 규칙이 활성화되고 민감한 데이터 탐지가 비활성화된 경우, 침입 정책에 변경 사항을 저장하면, 자동으로 민감한 데이터 전처리기를 활성화하는 옵션이 제공됩니다.

자세한 내용은 다음 섹션을 참고하십시오.

민감한 데이터 탐지 구축

라이센스: 보호

민감한 데이터 탐지는 시스템 성능에 상당한 영향을 줄 수 있으므로, Cisco는 다음 지침을 준수할 것을 권장합니다.

- 기본 침입 정책으로 No Rules Active(활성 규칙 불가) 기본 정책을 선택합니다. 자세한 내용은 12-3페이지의 시스템 제공 기반 정책의 이해를 참고하십시오.
- 해당 네트워크 분석 정책에서 다음 구성이 활성화되어 있는지 확인하십시오.
  - **Application Layer Preprocessors(애플리케이션 레이어 전처리기)** 아래의 **FTP and Telnet Configuration(FTP 및 텔넷 구성)**
  - **Transport/Network Layer Preprocessors(전송/네트워크 레이어 전처리기)** 아래의 **IP Defragmentation(IP 조각 모음)** 및 **TCP Stream Configuration(TCP 스트림 구성)**.
- 민감한 데이터 탐지에 대해 예약된 디바이스에 민감한 데이터 구성을 비롯한 침입 정책을 포함하는 액세스 제어 정책을 적용합니다. 자세한 내용은 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

전역 민감한 데이터 탐지 옵션 선택

라이센스: 보호

전역 민감한 데이터 전처리기 옵션은 전처리기가 작용하는 방법을 제어합니다. 다음을 지정하는 전역 옵션을 변경할 수 있습니다.

- 시작하는 패킷에서 전처리기가 신용 카드 번호 또는 사회 보장 번호의 마지막 네 자리를 제외한 모든 것을 대체하는지 여부
- 네트워크에서 민감한 데이터에 대해 모니터링하는 대상 호스트의 종류
- 단일 세션에서 단일 이벤트로 귀결되는 모든 데이터 유형의 총 발생 횟수

전역 민감한 데이터 옵션은 특정 정책을 기반으로 하며 모든 데이터 유형에 적용된다는 점에 유의하십시오.

다음의 전역 데이터 탐지 옵션을 구성할 수 있습니다.

마스크

시작하는 패킷에서 신용 카드 번호 또는 사회 보장 번호의 마지막 네 자리를 제외한 모든 것을 X로 대체합니다. 감춰진 번호는 사용자 인터페이스 및 다운로드한 패킷의 침입 이벤트 패킷 보기에 표시됩니다.

네트워크

민감한 데이터를 위해 모니터링할 대상 호스트를 지정합니다. 단일 IP 주소 또는 주소 블록을 지정하거나, 쉼표로 구분된 하나 또는 둘 다의 목록을 지정할 수 있습니다. 시스템은 비어 있는 필드를 모든으로 해석하며, 모든 대상 IP 주소를 의미합니다. IPv4 및 IPv6 주소 블록을 사용하는 데 대한 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.

전역 임계값

전처리기가 전역 임계값 이벤트를 생성하기 전에 모든 조합에서 탐지해야 하는 단일 세션 동안 모든 데이터 유형의 모든 항목 수를 지정합니다. 1부터 65535까지 지정할 수 있습니다.

Cisco는 이 옵션 값을 사용자 정책에서 활성화한 모든 개별 데이터 유형에 대한 가장 높은 임계값 보다 높게 설정할 것을 권장합니다. 자세한 내용은 21-22페이지의 개별 데이터 유형 옵션 선택을 참고하십시오.

전역 임계값에 관해 다음 사항에 유의하십시오.

- 전처리기 규칙 139:1을 활성화하여 결합된 데이터 유형 발생에서 이벤트를 탐지하고 생성할 수 있어야 합니다. 침입 정책에서 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.
- 전처리기는 세션 당 하나의 전역 임계값 이벤트를 생성합니다.
- 전역 이벤트 임계값은 개별 데이터 유형 이벤트와 상관없습니다. 즉 전처리기는 모든 개별 데이터 유형에 대한 이벤트 임계값에 도달했는지에 관계없이, 그리고 그 반대의 경우에도 그에 관계없이, 전역 임계값에 도달했을 때 이벤트를 생성합니다.

개별 데이터 유형 옵션 선택

라이센스: 보호

개별 데이터 유형은 지정된 대상 네트워크에서 이벤트를 탐지하고 생성할 수 있는 민감한 데이터를 식별합니다. 다음을 지정하는 데이터 유형 옵션에 대한 기본 설정을 변경할 수 있습니다.

- 세션 당 단일 이벤트를 생성하는 탐지된 데이터 유형을 위해 충족해야 하는 임계값
- 각 데이터 유형을 모니터링할 대상 포트
- 각 데이터 유형을 모니터링할 애플리케이션 프로토콜

최소한, 각 데이터 유형은 모니터링할 하나의 이벤트 임계값 및 최소 1개의 포트 또는 애플리케이션 프로토콜을 지정해야 합니다.

Cisco가 제공한 각각의 미리 정의된 데이터는 다른 경우에는 액세스할 수 없는 `sd_pattern` 키워드를 사용하여 트래픽에서 탐지할 내장된 데이터 패턴을 정의합니다. 미리 정의된 데이터 유형의 목록은 21-24페이지의 표 21-8을 참고하십시오. 또한 간단한 정규 표현식을 사용하여 사용자 고유의 데이터 패턴을 지정할 수 있는 사용자 지정 데이터 유형을 생성할 수도 있습니다. 자세한 내용은 21-28페이지의 사용자 지정 데이터 유형 사용을 참고하십시오.

데이터 유형 이름과 패턴은 시스템 전체에 적용되며, 다른 모든 데이터 유형 옵션은 정책에만 적용됩니다.

다음 표는 구성할 수 있는 데이터 유형 옵션에 대해 설명합니다.

표 21-7 개별 데이터 유형 옵션

옵션	설명
데이터 유형	데이터 유형의 고유한 이름을 표시합니다.
임계값	시스템이 이벤트를 생성할 때 데이터 유형 발생 수를 지정합니다. 활성화된 데이터 유형에 대한 임계값을 설정하지 않을 경우 정책을 저장하면 오류 메시지를 받게 됩니다. 1부터 255까지 지정할 수 있습니다. 전처리기는 세션 당 탐지한 데이터 유형에 대한 1가지 이벤트를 생성한다는 점에 유의하십시오. 전역 이벤트 임계값은 개별 데이터 유형 이벤트와 상관없습니다. 즉 전처리기는 전역 이벤트 임계값에 도달했는지 여부와 그 반대의 경우에도 관계없이, 데이터 유형 이벤트 임계값에 도달했을 때 이벤트를 생성합니다.
대상 포트	각 데이터 유형을 모니터링할 대상 포트를 지정합니다. 단일 포트, 포트의 쉼표로 구분된 목록, 또는 모든을 지정할 수 있습니다. 말하자면 모든 대상 포트를 의미합니다. 데이터 유형에 대한 최소 1개의 포트 또는 애플리케이션 프로토콜을 설정하지 않고 데이터 유형에 대한 규칙을 활성화한 경우 정책을 저장하면 오류 메시지를 받게 됩니다.
애플리케이션 프로토콜 이 기능은 제어 라이센스가 필요하다는 점에 유의하십시오.	데이터 유형에 대해 모니터링하기 위해 최대 8개의 애플리케이션 프로토콜을 지정합니다. 데이터 유형에 대한 최소 1개의 포트 또는 애플리케이션 프로토콜을 설정하지 않고 데이터 유형에 대한 규칙을 활성화한 경우 정책을 저장하면 오류 메시지를 받게 됩니다. 데이터 유형의 애플리케이션 프로토콜을 선택하는 데 대한 자세한 내용은 21-26페이지의 모니터링할 애플리케이션 프로토콜 선택을 참고하십시오.
패턴	사용자 지정 데이터 유형의 경우, 탐지할 지정된 패턴(Cisco가 제공하는 데이터 유형에 대한 데이터 패턴은 미리 정의됨)입니다. 자세한 내용은 21-28페이지의 사용자 지정 데이터 유형 사용을 참고하십시오. 사용자 인터페이스는 미리 정의된 데이터 유형에 대한 내장된 패턴을 표시하지 않습니다. 사용자 지정 및 미리 정의된 데이터 패턴은 시스템 전체에 적용된다는 점에 유의하십시오.

미리 정의된 데이터 유형 사용

라이센스: 보호

각 침입 정책은 대시가 있거나 없는 신용 카드 번호, 전자 메일 주소, 미국 전화 번호 및 미국 사회 보장 번호와 같은 일반적으로 사용되는 데이터 패턴 탐지를 위한 사전 정의된 데이터 유형을 포함합니다. 각각의 미리 정의된 데이터 유형은 생성기 ID(GID) 138을 가진 단일 민감한 데이터 전처리기 규칙과 연결됩니다. 침입 정책에서 관련된 민감한 데이터를 활성화하여 사용자 정책에서 사용할 각 데이터 유형에 대한 탐지 및 이벤트 발생을 활성화해야 합니다. 침입 정책에서 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

민감한 데이터 규칙을 활성화할 수 있도록 하기 위해, 구성 페이지 링크를 통해 모든 미리 정의한 민감한 데이터 규칙 및 사용자 지정 민감한 데이터 규칙을 표시하는 Rules(규칙) 페이지의 필터링된 보기로 이동합니다. 또한 Rules(규칙) 페이지에서 민감한 데이터 규칙 필터링 카테고리를 선택하여 미리 정의된 민감한 데이터만 표시할 수 있습니다. 자세한 내용은 20-9페이지의 침입 정책에서 규칙 필터링을 참고하십시오. 미리 정의된 민감한 데이터 규칙은 또한 Rule Editor(규칙 편집기) 페이지 (**Policies(정책) > Intrusion(침입) > Rule Editor(규칙 편집기)**)에 나열되는데, 여기서 규칙을 볼 수는 있지만 민감한 데이터 규칙 카테고리에서 수정할 수는 없습니다.

다음 표는 데이터 유형에 대한 탐지 및 이벤트 발생을 활성화해야 하는 해당 전처리기 연결 규칙을 나열하고 각 데이터 유형을 설명합니다.

표 21-8 민감한 데이터 유형

데이터 유형	설명	전처리기 규칙 GID:SID
신용 카드 번호	Visa®, MasterCard®, Discover® 및 American Express®의 15-16자리 신용카드 번호에 일치합니다. 일반적으로 분리하는 대시 또는 스페이스는 있거나 없을 수도 있으며, 또한 신용 카드 검사 숫자 확인을 위해 Luhn 알고리즘을 사용합니다.	138:2
이메일 주소	이메일 주소에 일치합니다.	138:5
미국 전화 번호	패턴 `(\d{3}) ?\d{3}-\d{4}`을 준수하는 미국 전화 번호에 일치합니다.	138:6
대시 없는 미국 사회 보장 번호	유효한 3자리 지역번호, 유효한 2자리 그룹 번호가 있으며 대시를 포함하지 않는 9자리 미국 Social Security(사회 보장 번호)에 일치합니다.	138:4
대시 있는 미국 사회 보장 번호	유효한 3자리 지역 번호, 유효한 2자리 그룹 번호가 있으며 대시를 포함하는 9자리 미국 사회 보장 번호 번호에 일치합니다.	138:3
사용자 지정	지정된 트래픽의 사용자 지정된 데이터 패턴에 일치합니다. 자세한 내용은 21-28페이지의 사용자 지정 데이터 유형 사용을 참고하십시오.	138:>999999

사회 보장 번호가 아닌 9자리 번호에서 잘못된 긍정을 삭제하기 위해 전처리기는 각 사회 보장 번호에서 4자리 일련 번호의 앞에 있는 3자리 지역 번호와 2자리 그룹 번호를 승인하는 알고리즘을 사용합니다. 전처리기는 2009년11월까지 사회 보장 그룹 번호를 승인합니다.

민감한 데이터 구성

라이센스: 보호

개별 데이터 유형에 대한 기본 전역 설정 및 구성을 수정할 수 있습니다. 또한 탐지할 각 데이터 유형에 대한 전처리기 규칙을 활성화해야 합니다.

민감한 데이터 탐지를 활성화하지 않고 정책에서 민감한 데이터 전처리기 규칙을 활성화한 경우, 정책에 변경 사항을 저장하면 민감한 데이터 탐지를 활성화하라는 메시지가 표시됩니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

다음 표는 Sensitive Data Detection(민감한 데이터 탐지) 페이지에서 수행할 수 있는 작업을 설명합니다.

표 21-9 민감한 데이터 구성 작업

목적	방법
전역 설정 수정하기	사용자가 수정할 수 있는 전역 설정에 대한 내용은 21-9페이지의 표 21-6을 참고하십시오.
데이터 유형 옵션 수정하기	Targets(대상) 페이지 영역에서 데이터 유형 이름을 클릭합니다. Configuration(구성) 페이지 영역이 데이터 유형에 대한 현재 설정을 표시하기 위해 업데이트됩니다. 사용자가 변경할 수 있는 옵션에 대한 자세한 내용은 개별 데이터 유형 옵션 표를 참고하십시오.

표 21-9 민감한 데이터 구성 작업 (계속)

목적	방법
데이터 유형에 대한 모니터링을 위해 애플리케이션 프로토콜을 추가 또는 제거하기 이 기능은 제어 라이센스가 필요하다는 점에 유의하십시오.	**Application Protocols(애플리케이션 프로토콜)** 필드 안을 클릭하거나, 필드 옆의 **Edit(수정)**를 클릭합니다. Application Protocols(애플리케이션 프로토콜) 팝업 창이 나타납니다. • 모니터링할 8개의 애플리케이션 프로토콜을 추가하려면 왼쪽에 있는 **Available(사용 가능)** 목록에서 하나 이상의 애플리케이션 프로토콜을 선택한 다음 오른쪽 화살표(**>**) 단추를 클릭합니다. • 애플리케이션 프로토콜을 제거하려면 오른쪽에 있는 **Enabled(사용)** 목록에서 이를 선택한 다음 왼쪽 화살표(**<**) 단추를 클릭합니다. Ctrl 또는 Shift 클릭하여 다중 애플리케이션 프로토콜을 선택합니다. 또한 인접한 여러 애플리케이션 프로토콜을 선택하려면 클릭하고 드래그할 수 있습니다. **참고** FTP 트래픽에서 민감한 데이터를 탐지하려면 `Ftp data` 애플리케이션 프로토콜을 추가해야 합니다.. 자세한 내용은 21-27페이지의 특별 케이스: FTP 트래픽의 민감한 데이터 검색을 참고하십시오.
사용자 지정 데이터 유형 만들기	페이지 왼쪽에 있는 **Data Types(데이터 유형)** 옆의 **+** 기호를 클릭합니다. Add Data Type(데이터 유형 추가) 팝업 창이 열립니다. 이 데이터 유형으로 탐지할 고유한 데이터 유형 이름 및 패턴을 지정하려면 **OK(확인)**를 클릭하거나 **Cancel(취소)**을 클릭하여 수정을 취소합니다. 자세한 내용은 21-28페이지의 사용자 지정 데이터 유형 사용을 참고하십시오.
민감한 데이터 전처리기 규칙을 표시합니다	Global Settings(전역 설정) 페이지 영역 위에 있는 **Configure Rules for Sensitive Data Detection(민감한 데이터 탐지를 위한 규칙 구성)** 링크를 클릭합니다. Rules(규칙) 페이지의 필터링된 표시에 모든 민감한 데이터 전처리기 규칙의 목록이 나타납니다. 또는, 나열된 모든 규칙을 활성화하거나 비활성화할 수 있습니다. 사용자 침입 정책에서 사용할 각 데이터 유형에 대한 민감한 데이터 전처리기 규칙을 활성화해야 한다는 점에 유의하십시오. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오. 또한 Rules(규칙) 페이지에서 규칙 삭제, 속도 기반 공격 방지와 같은 사용 가능한 다른 작업에 대한 민감한 데이터 규칙을 구성할 수 있습니다. 자세한 내용은 20-1페이지의 규칙을 사용한 침입 정책 조정을 참고하십시오. **Back(뒤로)**을 클릭하여 Sensitive Data Detection(민감한 데이터 탐지) 페이지로 돌아갑니다.

민감한 데이터 탐지를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 왼쪽 탐색 패널에서 **Advanced Settings(고급 설정)**를 클릭합니다.

Advanced Settings(고급 설정) 페이지가 나타납니다.

단계 4 **Specific Threat Detection(특정 위협 탐지)** 아래의 **Sensitive Data Detection(민감한 데이터 탐지)**이 활성화되어 있는지에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Sensitive Data Detection(민감한 데이터 탐지) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 5 민감한 데이터 구성 작업 표에서 설명된 모든 조치를 취할 수 있습니다.

단계 6 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

모니터링할 애플리케이션 프로토콜 선택

라이센스: 제어

각 데이터 유형에 대해 모니터링하기 위해 최대 8개의 애플리케이션 프로토콜을 지정할 수 있습니다.

각 데이터 유형에 대해 모니터링하기 위해 최소 1개의 애플리케이션 프로토콜 또는 포트를 지정해야 합니다. 그러나, FTP 트래픽에서 민감한 데이터 탐지를 원하는 경우를 제외하고, Cisco는 완벽한 적용을 위해 애플리케이션 프로토콜을 지정하는 경우 해당 포트를 지정할 것을 권장합니다. 예를 들어, HTTP를 지정한 경우 잘 알려진 HTTP 포트 80 또한 구성할 수 있습니다. 네트워크에서 새로운 호스트가 HTTP를 구현할 경우, 시스템이 새로운 HTTP 애플리케이션 프로토콜을 발견하면 간격 동안 포트 80을 모니터링합니다.

FTP 트래픽에서 민감한 데이터 탐지를 원하는 경우, `Ftp data` 애플리케이션 프로토콜을 추가해야 합니다. 포트 번호 지정에는 이점이 없습니다. 자세한 내용은 21-27페이지의 특별 케이스: FTP 트래픽의 민감한 데이터 검색을 참고하십시오.

민감한 데이터 탐지를 위해 애플리케이션 프로토콜을 수정하려면 다음을 수행합니다.

Admin(관리)/Intrusion Admin(침입 관리)

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 왼쪽 탐색 패널에서 **Advanced Settings(고급 설정)**를 클릭합니다.

Advanced Settings(고급 설정) 페이지가 나타납니다.

단계 4 **Specific Threat Detection(특정 위협 탐지)** 아래의 **Sensitive Data Detection(민감한 데이터 탐지)**이 활성화되어 있는지에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Sensitive Data Detection(민감한 데이터 탐지) 페이지가 나타납니다.

페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 5 수정할 데이터 유형을 선택하려면 **Data Types(데이터 유형)**에서 데이터 유형 이름을 클릭합니다.

Configuration(구성) 영역이 선택된 데이터 유형에 대한 현재 설정을 표시하도록 업데이트됩니다.

단계 6 **Application Protocols(애플리케이션 프로토콜)** 필드 안을 클릭하거나, 필드 옆의 **Edit(수정)**를 클릭합니다.

Application Protocols(애플리케이션 프로토콜) 팝업 창이 나타납니다.

단계 7 다음 2가지 옵션을 사용할 수 있습니다.

- 모니터링할 8개의 애플리케이션 프로토콜을 추가하려면 왼쪽에 있는 **Available(사용 가능)** 목록에서 하나 이상의 애플리케이션 프로토콜을 선택한 다음 오른쪽 화살표(**>**) 단추를 클릭합니다.
- 애플리케이션 프로토콜을 제거하려면 오른쪽에 있는 **Enabled(사용)** 목록에서 이를 선택한 다음 왼쪽 화살표(**<**) 단추를 클릭합니다.

Ctrl 또는 Shift 클릭하여 다중 애플리케이션 프로토콜을 선택합니다. 또한 인접한 여러 애플리케이션 프로토콜을 선택하려면 클릭하고 드래그할 수 있습니다.

참고 FTP 트래픽에서 민감한 데이터를 탐지하려면 `FTP data` 애플리케이션 프로토콜을 추가해야 합니다. 자세한 내용은 21-27페이지의 특별 케이스: FTP 트래픽의 민감한 데이터 검색을 참고하십시오.

단계 8 애플리케이션 프로토콜을 추가하려면 **OK(확인)**를 클릭합니다.

Sensitive Data Detection(민감한 데이터 탐지) 페이지가 표시되고 애플리케이션 프로토콜을 업데이트합니다.

특별 케이스: FTP 트래픽의 민감한 데이터 검색

라이센스: 제어

민감한 데이터를 모니터링할 트래픽은 보통 모니터링할 포트를 지정하거나, 선택적으로 배포 내 애플리케이션 프로토콜을 지정하여 결정합니다. 그러나, 포트 또는 애플리케이션 프로토콜을 지정하는 것은 FTP 트래픽의 민감한 데이터를 탐지하는 데 충분하지 않습니다. FTP 트래픽 내 민감한 데이터가 FTP 애플리케이션 프로토콜의 트래픽에서 발견되는 일이 간헐적으로 발생하는데, 일시적 포트 번호를 사용하여 탐지하는 것을 어렵게 만듭니다. FTP 트래픽에서 민감한 데이터를 검색하려면 **반드시** 구성에 다음을 포함해야 합니다.

- `FTP data` 애플리케이션 프로토콜을 지정합니다.

  `FTP data` 애플리케이션 프로토콜을 지정하면 FTP 트래픽 내 민감한 데이터의 탐지가 활성화됩니다. 자세한 내용은 21-26페이지의 모니터링할 애플리케이션 프로토콜 선택을 참고하십시오.

  FTP 트래픽에서 민감한 데이터를 탐지하는 특정 케이스의 경우 `FTP data` 애플리케이션 프로토콜을 지정해도 탐지되지 않습니다. 대신, 이는 FTP/텔넷 처리기의 신속한 처리를 통해 FTP 트래픽에서 민감한 데이터를 탐지하도록 합니다. 자세한 내용은 15-18페이지의 FTP 및 텔넷 트래픽 디코딩을 참고하십시오.

- 민감한 데이터에 대해 모니터링하는 최소 1개의 포트가 구성에 포함되어 있는지 확인합니다.

  FTP 트래픽에서 민감한 데이터에 대해 탐지만 원하는 가능성이 낮은 경우를 제외하면 FTP 포트를 지정할 필요가 없다는 점에 유의하십시오. 대부분의 민감한 데이터 구성은 HTTP 또는 이메일 포트와 같은 다른 포트를 포함합니다. 모니터링을 위해 1개의 FTP 포트만 지정하고 다른 포트는 지정하지 않을 경우 Cisco는 FTP 명령 포트 23을 지정할 것을 권장합니다. 자세한 내용은 21-24페이지의 민감한 데이터 구성을 참고하십시오.

사용자 지정 데이터 유형 사용

라이센스: 보호

사용자 지정 데이터 유형을 만들고 수정하여 지정하려는 데이터 패턴을 탐지할 수 있습니다. 예를 들어, 병원이 환자 번호를 보호하기 위해 데이터 유형을 만들 수 있으며 대학이 고유 번호 패턴이 있는 학생 수를 탐지하기 위해 데이터 유형을 만들 수도 있습니다.

사용자가 만든 각 사용자 지정 날짜 형식은 생성기 ID(GID) 138과 1000000 이상의 Snort ID, 즉 로컬 규칙에 대한 SID를 갖는 민감한 단일 데이터 전처리기 규칙을 생성합니다. 관련된 민감한 데이터 규칙을 활성화하여 사용자 정책에서 사용할 각 사용자 지정 데이터 유형에 대한 탐지 및 이벤트 발생을 활성화해야 합니다. 침입 정책에서 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

민감한 데이터 규칙을 활성화할 수 있도록 하기 위해, 구성 페이지 링크를 통해 모든 미리 정의한 민감한 데이터 규칙 및 사용자 지정 민감한 데이터 규칙을 표시하는 Rules(규칙) 페이지의 필터링된 보기로 이동합니다. 또한 Rules(규칙) 페이지에서 로컬 규칙 필터링 카테고리를 선택하여 모든 로컬 사용자 지정 규칙과 함께 사용자 지정 민감한 데이터 규칙을 표시할 수 있습니다. 자세한 내용은 20-9페이지의 침입 정책에서 규칙 필터링을 참고하십시오. 사용자 지정 민감한 데이터 규칙은 Rule Editor(규칙 편집기) 페이지에 표시되지 않는다는 점에 유의하십시오.

사용자가 만든 사용자 지정 데이터 유형은 모든 침입 정책에 추가됩니다. 특정 사용자 지정 데이터 유형에 대한 이벤트를 탐지하고 생성하기 위해 사용할 모든 정책에서 관련된 민감한 데이터 규칙을 활성화해야 합니다.

데이터 유형 및 관련 규칙을 만들려면 Sensitive Data Detection(민감한 데이터 탐지) 구성 페이지를 사용해야 한다는 점에 유의하십시오. 민감한 데이터 규칙을 만들기 위해 규칙 편집기를 사용할 수 없습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 21-28페이지의 사용자 지정 데이터 유형에서 데이터 패턴 정의
- 21-30페이지의 사용자 지정 데이터 유형 구성
- 21-31페이지의 사용자 지정 데이터 유형 이름 및 탐지 패턴 수정

사용자 지정 데이터 유형에서 데이터 패턴 정의

라이센스: 보호

다음으로 구성된 정규식 단순 집합을 사용하여 사용자 지정 데이터 유형에 대한 데이터 패턴을 정의합니다.

- 3개의 메타 문자
- 메타 문자를 문자로 사용할 수 있도록 하는 이스케이프된 문자
- 6개의 문자 클래스

메타 문자는 정규 표현식에서 특정 의미가 있는 리터럴 문자입니다. 다음 표는 사용자 지정 데이터 패턴을 정의할 때 사용할 수 있는 메타 문자에 대해 설명합니다.

표 21-10 민감한 데이터 패턴 메타 문자

메타 문자	설명	예
?	앞선 문자 또는 이스케이프 시퀀스에 0회 또는 1회 발생에 일치합니다. 즉, 앞선 문자 또는 이스케이프 시퀀스는 선택 사항입니다.	colou?r는 color 또는 colour에 일치합니다.
{*n*}	앞선 문자 또는 이스케이프 시퀀스에 *n*회 일치합니다.	예를 들어, \d{2}는 55, 12 등에 일치합니다. \l{3}는 AbC, www 등에 일치합니다. \w{3}는 a1B, 25C 등에 일치합니다. x{5}는 xxxxx에 일치합니다.
\	메타 문자를 실제 문자로 사용할 수 있으며, 미리 정의된 문자 클래스를 지정하는 데 사용할 수도 있습니다. 사용자가 민감한 데이터 패턴에서 사용할 수 있는 문자 클래스에 대한 설명은 21-29페이지의 표 21-12를 참고하십시오.	\?는 물음표와 일치하고, \\는 백슬래시에 일치하며 \는 숫자 등에 일치합니다.

민감한 데이터 전처리기가 이들을 문자로 정확하게 해석하도록 하려면 다음 표에서 백슬래시를 사용하여 문자를 이스케이프해야 합니다.

표 21-11 이스케이프된 민감한 데이터 패턴 문자

사용할 이스케이프된 문자	나타낼 문자
\?	?
\{	{
\}	}
\\	\

다음 표는 민감한 데이터 패턴을 정의할 때 사용할 수 있는 문자 클래스를 설명합니다.

표 21-12 민감한 데이터 패턴 문자 클래스

문자 클래스	설명	문자 클래스 정의
\d	모든 숫자 ASCII 문자 0-9와 일치합니다.	0-9
\D	숫자 ASCII 문자가 아닌 모든 바이트와 일치합니다.	0-9 아님
\l(소문자 "ell")	모든 ASCII 문자와 일치합니다.	a-zA-Z
\L	ASCII 문자가 아닌 모든 바이트와 일치합니다.	a-zA-Z 아님
\w	모든 ASCII 영숫자 문자와 일치합니다. PCRE 정규식과는 달리, 이는 밑줄(_)을 포함하지 않는다는 점에 유의하십시오.	a-zA-Z0-9
\W	ASCII 영숫자 문자가 아닌 모든 바이트와 일치합니다.	a-zA-Z0-9 아님

전처리기는 직접 입력한 문자를 정규식의 일부 대신 문자로 처리합니다. 예를 들어, 데이터 패턴 1234는 1234에 일치합니다.

다음 데이터 패턴 예제는 미리 정의된 민감한 데이터 규칙 138:4에서 사용되는데, 미국 전화 번호를 검색하기 위해 이스케이프된 디지트 문자 클래스, 승수 및 옵션 지정자 메타 문자, 그리고 문자 대시(-) 및 좌우 괄호() 문자를 사용합니다.

```
(\d{3}) ?\d{3}-\d{4}
```

사용자 지정 데이터 패턴을 만들 때 주의를 기울이십시오. 올바른 구문을 사용하지만 많은 잘못된 긍정을 야기할 수도 있는 전화 번호 탐지를 위해 다음 데이터 패턴을 고려하십시오.

```
(?\d{3})? ?\d{3}-?\d{4}
```

두 번째 예제는 괄호(선택 사항), 스페이스(선택 사항) 및 대시(선택 사항)를 조합하므로 다음과 같은 원하는 패턴의 전화 번호를 탐지합니다.

- `(555)123-4567`
- `555123-4567`
- `5551234567`

그러나, 두 번째 예제 패턴은 또한 잘못된 긍정을 야기하는 다음과 같은 유효하지 않은 잠재적인 패턴을 탐지합니다.

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

마지막으로 이해를 돕기 위해 소규모 회사 네트워크에서 모든 대상 트래픽의 낮은 이벤트 임계값을 사용하여 소문자 a를 탐지하는 데이터 패턴을 생성하는 극단적인 예를 고려하십시오. 이러한 데이터 패턴은 단지 몇 분 만에 사용자 시스템을 수 백 만개의 이벤트로 마비시킬 수 있습니다.

사용자 지정 데이터 유형 구성

라이센스: 보호

미리 정의된 데이터 유형에 대해 구성한 사용자 지정 데이터 유형에 대해 기본적으로 동일한 데이터 유형 옵션을 구성합니다. 모든 데이터 유형에 일반적인 설정 옵션에 대한 자세한 내용은 21-22페이지의 개별 데이터 유형 옵션 선택을 참고하십시오. 또한, 사용자 지정 데이터 유형에 대한 이름 및 데이터 패턴을 지정해야 합니다.

사용자 지정 데이터 유형을 생성하면 규칙을 전처리하는 관련 사용자 지정 민감한 데이터도 생성되는데, 이는 해당 데이터 유형을 사용하려는 각 정책에서 활성화해야 한다는 점에 유의하십시오. 침입 정책에서 규칙 활성화에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

사용자 지정 데이터 유형을 생성하거나 수정하려면 다음을 수행합니다.

Admin(관리)/Intrusion Admin(침입 관리)

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 왼쪽 탐색 패널에서 **Advanced Settings(고급 설정)**를 클릭합니다.

Advanced Settings(고급 설정) 페이지가 나타납니다.

단계 4 **Specific Threat Detection(특정 위협 탐지)** 아래의 **Sensitive Data Detection(민감한 데이터 탐지)**이 활성화되어 있는지에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Sensitive Data Detection(민감한 데이터 탐지) 페이지가 나타납니다.

페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 5 다음 옵션을 이용할 수 있습니다.

- 사용자 지정 데이터 유형을 생성하려면 페이지 왼쪽에 있는 **Data Types(데이터 유형)** 옆의 **+** 기호를 클릭합니다. Add Data Type(데이터 유형 추가) 팝업 창이 열립니다.

  이 데이터 유형으로 탐지할 고유한 데이터 유형 이름 및 패턴을 지정하려면 **OK(확인)**를 클릭하거나 **Cancel(취소)**을 클릭하여 수정을 취소합니다. 자세한 내용은 21-31페이지의 사용자 지정 데이터 유형 이름 및 탐지 패턴 수정을 참고하십시오.

  Sensitive Data Detection(민감한 데이터 탐지) 페이지가 나타납니다. **OK(확인)**를 클릭한 경우, 변경 내용을 표시하도록 페이지를 업데이트합니다.

- 미리 정의한 데이터 유형 및 사용자 지정 데이터 유형에 일반적인 모든 옵션을 변경하려면, **Targets(대상)** 페이지 영역에서 데이터 유형 이름을 클릭합니다.

  Configuration(구성) 페이지 영역이 데이터 유형에 대한 현재 설정을 표시하기 위해 업데이트됩니다. 자세한 내용은 21-24페이지의 민감한 데이터 구성을 참고하십시오.

- 사용자 지정 데이터 유형에 대한 시스템 전체의 이름 및 데이터 패턴을 수정하려면 21-31페이지의 사용자 지정 데이터 유형 이름 및 탐지 패턴 수정을 참고하십시오.

- 사용자 지정 데이터 유형을 삭제하려면, 삭제하려는 데이터 유형 옆에 있는 삭제 아이콘( )을 클릭한 후 **OK(확인)**를 클릭하거나 **Cancel(취소)**을 클릭하여 데이터 유형의 삭제를 취소합니다.

  해당 데이터 유형에 대한 민감한 데이터 규칙이 모든 침입 정책에서 활성화된 경우 데이터 유형을 삭제할 수 없다는 점에 유의하십시오. 사용자 지정 데이터 유형을 삭제하면 모든 침입 정책에서 삭제됩니다.

사용자 지정 데이터 유형 이름 및 탐지 패턴 수정

라이센스: 보호

사용자 지정 민감한 데이터 규칙을 위해 시스템 전체의 이름 및 탐지 패턴을 수정할 수 있습니다. 이 설정을 변경하면 시스템의 다른 모든 정책에서도 변경된다는 점에 유의하십시오. 또한 사용자가 변경한 사용자 지정 데이터 유형을 사용하는 침입 정책을 포함하는 적용된 액세스 제어 정책을 모두 재적용해야 한다는 점에 유의하십시오

사용자 지정 데이터 유형 이름 및 데이터 패턴을 제외한, 모든 데이터 유형 옵션은 사용자 및 미리 정의된 데이터 유형 모두를 위한 특정 정책에 해당합니다. 사용자 지정 데이터 유형에서 이름 및 데이터 패턴이 아닌 옵션 변경에 대한 내용은 21-22페이지의 개별 데이터 유형 옵션 선택을 참고하십시오.

사용자 지정 데이터 유형 이름 및 데이터 패턴을 수정하려면 다음을 수행합니다.

Admin(관리)/Intrusion Admin(침입 관리)

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)를 선택합니다.**

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 왼쪽 탐색 패널에서 **Advanced Settings(고급 설정)**를 클릭합니다.

Advanced Settings(고급 설정) 페이지가 나타납니다.

단계 4 **Specific Threat Detection(특정 위협 탐지)** 아래의 **Sensitive Data Detection(민감한 데이터 탐지)**이 활성화되어 있는지에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Sensitive Data Detection(민감한 데이터 탐지) 페이지가 나타납니다.

페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 5 **Targets(대상)** 페이지 영역에서 수정할 사용자 지정 데이터 유형의 이름을 클릭합니다.

페이지가 업데이트되어 데이터 유형에 대한 현재 설정을 보여주며, Configuration(구성) 페이지의 오른쪽 상단에 **Edit Data Type Name and Pattern(데이터 이름 및 패턴 수정)** 링크가 나타납니다.

단계 6 **Edit Data Type Name and Pattern(데이터 이름 및 패턴 수정)** 링크를 클릭합니다.

Edit Data Type(데이터 유형 수정) 팝업 창이 나타납니다.

단계 7 데이터 유형 이름, 패턴, 또는 둘 다를 수정하고 **OK(확인)**를 클릭하거나 **Cancel(취소)**를 클릭하여 수정을 취소합니다. 데이터 패턴 지정에 대한 내용은 21-28페이지의 사용자 지정 데이터 유형에서 데이터 패턴 정의를 참고하십시오.

Sensitive Data Detection(민감한 데이터 탐지) 페이지가 나타납니다. **OK(확인)**를 클릭한 경우, 페이지에서 변경 내용을 표시합니다.

침입 이벤트 로깅의 전역적 제한

시스템이 침입 이벤트를 로깅하고 표시하는 횟수를 제한하기 위해 임계값을 사용할 수 있습니다. 침입 정책의 일부로 구성되는 임계값을 지정하면, 규칙과 일치하는 트래픽이 지정된 기간 내에 특정 주소나 주소 범위에서 발생하거나 그러한 주소나 주소 범위로 이동하는 횟수를 기반으로 시스템이 이벤트를 생성하도록 합니다. 이를 통해 많은 수의 이벤트로 인해 마비되는 것을 방지할 수 있습니다. 이 기능을 사용하려면 보호 라이센스가 필요합니다.

이벤트 알림 임계값은 두 가지 방법으로 설정할 수 있습니다.

- 모든 트래픽에 해당되는 전역 임계값을 설정하여 지정된 기간 당 특정 소스 또는 대상에서 이벤트가 얼마나 자주 로깅되고 표시되는지 제한할 수 있습니다. 자세한 내용은 22-1페이지의 임계값 설정의 이해 및 22-3페이지의 전역 임계값 구성을 참고하십시오.
- 20-22페이지의 이벤트 임계값 설정 구성에 설명된 대로 침입 정책 구성에서 공유 객체 규칙, 표준 텍스트 규칙 또는 프리프로세서 규칙당 임계값을 설정할 수 있습니다.

임계값 설정의 이해

라이센스: 보호

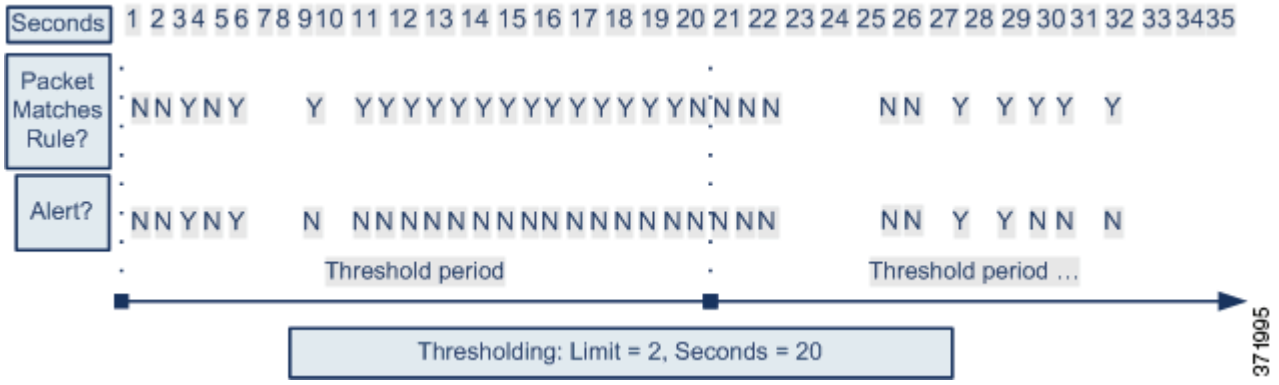
기본적으로 모든 침입 정책에는 전역 규칙 임계값이 포함되어 있습니다. 기본 임계값은 각 규칙에 대한 이벤트 생성을 동일한 대상으로 향하는 트래픽에서 매 60초 당 하나의 이벤트로 제한합니다. 이 전역 임계값은 기본적으로 모든 침입 규칙 및 프리프로세서 규칙에 적용됩니다. 침입 정책의 Advanced Settings(고급 설정) 페이지에서 임계값을 비활성화할 수 있습니다.

특정 규칙에 대해 개별 임계값을 설정하여 이 임계값을 재정의할 수도 있습니다. 예를 들어 전역 제한 임계값은 60초당 이벤트 5회이지만, SID 1315에 대해서는 60초당 이벤트 10회의 특정 임계값을 설정할 수 있습니다. 다른 모든 규칙은 60초당 생성되는 이벤트가 5회를 넘지 않지만, SID 1315의 경우 시스템은 60초당 이벤트를 최대 10회 생성합니다.

규칙 기반 임계값 설정에 대한 자세한 내용은 20-22페이지의 이벤트 임계값 설정 구성을 참조하십시오.

다음 다이어그램은 특정 규칙에 대해 진행되는 공격의 예를 보여줍니다. 전역 제한 임계값은 각 규칙에 대한 이벤트 생성을 20초당 이벤트 2회로 제한합니다.

기간은 1초에 시작하여 21초에 끝납니다. 기간이 끝나면 주기가 다시 시작되고 다음 두 규칙 일치가 이벤트를 생성하며, 시스템은 해당 기간 중에 더 이상 이벤트를 생성하지 않습니다.



임계값 설정 옵션의 이해

라이센스: 보호

임계값을 사용하면 특정 기간에 특정 수의 이벤트만을 생성하여 또는 이벤트 집합에 대해 하나의 이벤트만 생성하여 침입 이벤트 생성을 제한할 수 있습니다. 전역 임계값 설정을 구성할 때에는 다음 표에 설명된 대로 먼저 임계값 설정 유형을 지정해야 합니다.

표 22-1 임계값 설정 옵션

옵션	설명
Limit(제한)	지정된 기간 중 규칙을 트리거하는 지정된 패킷 수(count 인수로 지정)에 대한 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Limit(제한)**로, **Count(카운트)**는 10으로, 그리고 **Seconds(초)**는 60으로 설정하고 14개의 패킷이 규칙을 트리거하는 경우, 시스템은 동일한 시간(분) 내 발생한 첫 10개를 표시한 후 규칙에 대한 이벤트 로깅을 중지합니다.
Threshold (임계값)	지정된 기간 중 지정된 패킷 수(count 인수로 지정)가 규칙을 트리거하면 단일 이벤트를 로깅 및 표시합니다. 이벤트의 임계값 카운트에 도달하고 시스템이 해당 이벤트를 로깅하면 시간에 대한 카운터가 다시 시작됩니다. 예를 들어, 유형은 **Threshold(임계값)**로, **Count(카운트)**는 10으로, 그리고 **Seconds(초)**는 60으로 설정하면 규칙은 33초에 10번 트리거됩니다. 시스템은 하나의 이벤트를 생성한 다음, Seconds(초) Count(카운트) 카운터를 0으로 재설정합니다. 그런 다음 규칙은 다음 25초 안에 다시 10번 트리거됩니다. 카운터가 33초에 0으로 재설정되어 있기 때문에 시스템은 다른 이벤트를 로깅합니다.
Both(모두)	지정된 수(카운트)의 패킷이 규칙을 트리거한 후 특정 시기 동안 한 번에 하나의 이벤트를 로깅하고 표시합니다. 예를 들어, 유형은 **Both(모두)**로, **Count(카운트)**는 2로, 그리고 **Seconds(초)**는 10으로 설정하면, 다음 이벤트가 결과를 카운트합니다. • 10초에 한 번 규칙이 트리거되면 시스템은 이벤트를 생성하지 않습니다(임계값이 충족되지 않음). • 규칙이 10초에 두 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족됨). • 규칙이 10초에 네 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족되고 이후 이벤트는 무시됨).

다음으로 이벤트 인스턴스 카운트가 소스 또는 대상 IP 주소 별로 계산되는지 확인하는 추적을 지정합니다. 마지막으로, 임계값을 정의하는 기간 및 인스턴스 수를 지정합니다.

표 22-2 임계값 설정 인스턴스/시간 옵션

옵션	설명
Count(개수)	추적 IP 주소 또는 임계값을 충족시키는 데 필요한 주소 범위 당 지정된 기간에 해당하는 이벤트 인스턴스의 수
Seconds(초)	카운트가 재설정되기 전에 경과된 시간(초). 임계값 유형을 **Limit(제한)**로, 추적을 **Source(소스)**로, **Count(카운트)**를 10으로, 그리고 **Seconds(초)**를 10으로 설정한 경우, 시스템은 주어진 소스 포트에서 10초 안에 발생한 첫 10개의 이벤트를 로깅하고 표시합니다. 첫 10초 안에 일곱 개의 이벤트만 발생한 경우, 시스템은 이를 모두 로깅하고 표시하며, 첫 10초 안에 40개의 이벤트가 발생한 경우, 시스템은 10개를 로깅하고 표시한 후, 10초의 시간이 경과한 시점에서 다시 카운팅을 시작합니다.

전역 임계값 구성

라이센스: 보호

전역 임계값을 설정하여 일정 기간 동안 각 규칙에 의해 생성되는 이벤트 수를 관리할 수 있습니다. 전역 임계값을 설정하면 해당 임계값은 특정 임계값을 재정의하지 않는 각 규칙에 적용됩니다. 임계값 구성에 대한 자세한 내용은 22-1페이지의 임계값 설정의 이해를 참조하십시오.

전역 임계값은 시스템에서 기본적으로 구성됩니다. 기본값은 다음과 같습니다.

- **Type(유형)** — 제한
- **Track By(추적 방법)** — 대상
- **Count(카운트)** — 1
- **Seconds(초)** — 60

전역 임계값 설정을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**를 선택합니다.

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 왼쪽 탐색 패널에서 **Advanced Settings(고급 설정)**를 클릭합니다.

Advanced Settings(고급 설정) 페이지가 나타납니다.

단계 4 **Intrusion Rule Thresholds(침입 규칙 임계값)** 아래의 **Global Rule Thresholding(전역 규칙 임계값 설정)**이 활성화되었는지 여부에 따라 두 가지 선택이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Global Rule Thresholding(전역 규칙 임계값 설정) 페이지가 나타납니다. 페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 5 **Type(유형)** 라디오 단추에서 초 인수로 지정된 시간 동안 적용할 임계값 유형을 선택합니다. 자세한 내용은 임계값 설정 옵션 표를 참고하십시오.

- **Limit(제한)**를 선택하여 count 인수로 지정된 제한이 초과될 때까지 규칙을 트리거하는 각 패킷에 대한 이벤트를 로깅하고 표시합니다.
- **Threshold(임계값)**를 선택하여 규칙을 트리거하고 count 인수에 의해 설정된 임계값에 일치하는 인스턴스 또는 임계값의 배수에 해당하는 인스턴스 중 하나를 나타내는 각 패킷에 대한 단일 이벤트를 로깅하고 표시합니다.
- **Both(모두)**를 선택하여 count 인수로 지정된 패킷의 수가 규칙을 트리거한 후 단일 이벤트를 로깅하고 표시합니다.

단계 6 **Track By(추적 방법)** 라디오 단추에서 추적 방법을 선택합니다.

- **Source(소스)**를 선택하여 특정 소스 IP 주소 또는 주소에서 유입되는 트래픽 내에서 일치하는 규칙을 확인합니다.
- **Destination(대상)**을 선택하여 특정 대상 IP 주소로 가는 트래픽 내에서 일치하는 규칙을 확인합니다.

단계 7 **Count(카운트)** 필드에서:

- **Limit(제한)** 임계값의 경우, 임계값을 충족시키는 데 필요한 추적 IP 주소 당 지정된 기간별 이벤트 인스턴스의 수를 지정합니다.
- **Threshold(임계값)** 임계값의 경우, 사용자 임계값으로 사용할 규칙 일치의 수를 지정합니다.

단계 8 **Seconds(초)** 필드에서:

- **Limit(제한)** 임계값의 경우, 공격을 추적할 시간(초)을 지정합니다.
- **Threshold(임계값)** 임계값의 경우, 카운트가 재설정되기 전에 경과된 시간(초)을 지정합니다. 표시된 시간(초)이 경과하기 전에 **Count(카운트)** 필드에 표시된 규칙 일치의 수가 발생한 경우 카운트는 재설정된다는 점에 유의하십시오.

단계 9 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

전역 임계값 비활성화

라이센스: 보호

기본적으로, 전역 제한 임계값은 대상에 방문하는 트래픽의 이벤트 수를 60초 당 하나로 제한합니다. 특정 규칙에 대한 이벤트 임계값을 설정하기를 원하지만 각 규칙에 기본적으로 임계값을 적용하기를 원하지 않는 경우 가장 높은 정책 레이어에 있는 전역 임계값 설정을 비활성화할 수 있습니다.

전역 임계값 설정을 비활성화하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**를 선택합니다.

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 왼쪽 탐색 패널에서 **Settings(설정)**를 클릭합니다.

Settings(설정) 페이지가 나타납니다.

단계 4 **Intrusion Rule Thresholds(침입 규칙 임계값)** 아래의 **Global Rule Thresholding(전역 규칙 임계값 설정)**을 비활성화합니다.

단계 5 변경 사항을 시스템 캐시에서 유지한 상태에서 정책을 저장하고, 수정을 계속하며, 변경 사항을 삭제하거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

침입 규칙의 이해와 작성

*침입 규칙*은 규칙의 기준과 일치하는지 확인하기 위해 네트워크 트래픽을 분석함으로써 사용자 네트워크의 취약성을 이용하려는 시도를 탐지하는 키워드 및 인수의 지정된 집합입니다. 시스템은 패킷을 각 규칙에 지정된 조건과 비교하며, 패킷 데이터가 규칙에 지정된 모든 조건에 일치하는 경우 규칙이 트리거됩니다. 규칙이 *알림 규칙*인 경우, 침입 이벤트를 생성합니다. 규칙이 *전달 규칙*인 경우, 트래픽을 무시합니다. ASA FirePOWER 모듈 인터페이스에서 침입 이벤트를 보고 평가할 수 있습니다.

주의 제어 네트워크 환경을 사용하여 프로덕션 환경에서 규칙을 사용하기 전에 작성하는 모든 침입 규칙을 테스트하도록 하십시오. 잘못 작성한 침입 규칙은 시스템의 성능에 심각한 영향을 줄 수 있습니다.

다음 사항을 참고하십시오.

- 인라인 배포에서 *삭제* 규칙의 경우, 시스템은 패킷을 삭제하고 이벤트를 생성합니다. 삭제 규칙에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.
- Cisco는 두 가지 유형의 침입 규칙을 제공하는데, 바로 공유 객체 규칙과 표준 텍스트 규칙입니다. Cisco VRT(취약성 연구단)는 공유 객체 규칙을 사용하여 기존의 표준 텍스트 규칙이 수행할 수 없는 방식으로 취약성에 대해 공격을 탐지합니다. 사용자가 공유 객체 규칙을 생성할 수는 없습니다. 침입 규칙을 작성할 때 사용자는 표준 텍스트 규칙을 생성합니다.

사용자가 볼 가능성이 큰 이벤트 유형을 설정할 수 있도록 사용자 지정 표준 텍스트 규칙을 작성할 수 있습니다. 이 설명서는 특정 익스플로잇 탐지를 목표로 하는 규칙을 설명하고 있지만, 가장 성공적인 규칙은 알려진 특정 익스플로잇보다는 알려진 취약성을 공격하려고 시도하는 트래픽을 대상으로 합니다. 규칙을 작성하고 규칙의 이벤트 메시지를 지정하여, 공격 및 정책 회피를 나타내는 트래픽을 더욱 쉽게 확인할 수 있습니다. 이벤트 평가에 관한 자세한 정보는 26-1페이지의 이벤트 보기를 참고하십시오.

사용자 지정 침입 정책에서 사용자 지정 표준 텍스트 규칙을 활성화하는 경우, 트래픽이 특정 방법으로 먼저 디코딩 또는 전처리되는 것을 일부 규칙 키워드 및 인수가 요구한다는 점에 유의하십시오. 이 챕터에서는 전처리를 제어하는 네트워크 분석 정책에서 구성해야 하는 옵션을 설명합니다. 필요한 전처리기를 비활성화한 경우, 전처리기가 네트워크 분석 정책 사용자 인터페이스에서 비활성화된 상태로 남아 있더라도 시스템은 자동으로 전처리기를 현재의 설정으로 사용한다는 점에 유의하십시오.

참고 전처리 및 침입 탐지는 매우 밀접하게 연관되어 있기 때문에, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 서로 보완해야 합니다. 전처리 과정을 맞춤화하는 것, 특히 다양한 사용자 정의 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 자세한 내용은 11-11페이지의 사용자 지정 정책의 한계를 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-2페이지의 규칙 구조의 이해는 규칙 헤더 및 규칙 옵션을 포함하여 구성 요소를 설명하는데, 이는 유효한 표준 텍스트 규칙을 구성하는 것입니다.
- 23-3페이지의 규칙 헤더의 이해는 규칙 헤더의 일부에 대한 상세한 지침을 제공합니다.
- 23-9페이지의 규칙 내 키워드 및 인수의 이해는 ASA FirePOWER 모듈에서 사용 가능한 침입 규칙 키워드의 사용과 구문을 설명합니다.
- 23-100페이지의 규칙 구성은 규칙 편집기를 사용하여 새 규칙을 작성하는 방법을 설명합니다.
- 23-105페이지의 규칙 편집기 페이지의 규칙 필터링은 특정 규칙을 찾을 수 있도록 규칙의 하위 집합을 표시하는 방법을 설명합니다.

규칙 구조의 이해

라이센스: 보호

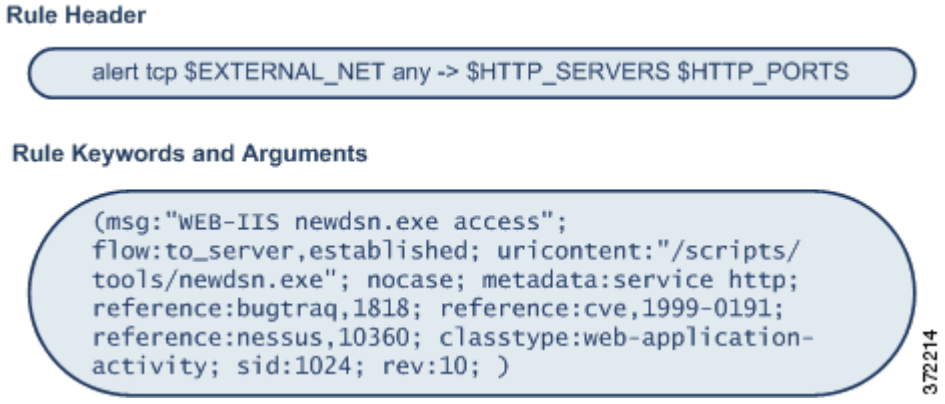
모든 표준 텍스트 규칙은 두 개의 논리적 섹션인 규칙 헤더 및 규칙 옵션을 포함합니다. 규칙 헤더에는 다음이 포함됩니다.

- 규칙의 상태 또는 유형
- 프로토콜
- 소스와 대상 IP 주소 및 넷마스크
- 소스에서 대상에 이르는 트래픽의 흐름을 보여 주는 방향 표시기
- 소스 및 대상 포트

규칙 옵션 섹션에는 다음이 포함됩니다.

- 이벤트 메시지
- 키워드와 매개 변수 및 인수
- 규칙을 트리거하기 위해 패킷 페이로드가 일치해야 하는 패턴
- 규칙 엔진이 패킷의 어느 부분을 검사해야 하는지에 관한 설명서

다음 다이어그램은 규칙의 일부를 설명합니다.

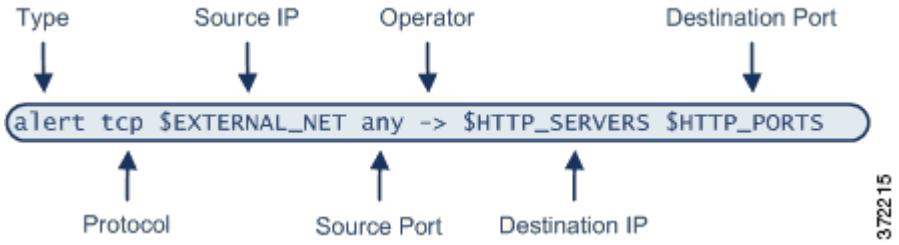


규칙의 옵션 섹션은 괄호로 둘러싸인 섹션이라는 점에 유의하십시오. 규칙 편집기는 표준 텍스트 규칙을 구축할 수 있도록 사용하기 쉬운 인터페이스를 제공합니다.

규칙 헤더의 이해

라이센스: 보호

각 표준 텍스트 규칙 및 공유 객체 규칙에는 매개 변수 및 인수가 포함된 규칙 헤더가 있습니다. 다음은 규칙 헤더의 일부를 설명합니다.



다음 표는 위에 표시된 규칙 헤더의 각 부분을 나타냅니다.

표 23-1 규칙 헤더 값

규칙 헤더 구성 요소	예제 값	값
작업	`경고`	침입 이벤트가 트리거되면 이를 생성합니다.
프로토콜	`tcp`	TCP 트래픽만 테스트합니다.
소스 IP 주소	`$EXTERNAL_NET`	내부 네트워크에 없는 모든 호스트에서 나오는 트래픽을 테스트합니다.
소스 포트	`any`	시작 호스트의 모든 포트에서 나오는 트래픽을 테스트합니다.
연산자	`->`	(네트워크 웹 서버로 가는) 외부 트래픽을 테스트합니다.
대상 IP 주소	`$HTTP_SERVERS`	내부 네트워크에서 웹 서버로 지정된 모든 호스트에 인도되는 트래픽을 테스트합니다.
대상 포트	`$HTTP_PORTS`	내부 네트워크에서 HTTP 포트에 인도되는 트래픽을 테스트합니다.

참고 이전 예제는 대부분의 침입 규칙과 같이 기본 변수를 사용합니다. 변수와, 변수가 의미하는 바, 그리고 이들을 구성하는 방법에 대한 자세한 내용은 2-14페이지의 변수 집합 작업을 참고하십시오.

규칙 헤더 매개 변수에 대한 자세한 내용은 다음 섹션을 참고하십시오.

- 23-4페이지의 규칙 작업 지정은 규칙 유형을 보여주고 규칙을 트리거할 때 발생하는 작업을 지정하는 방법에 대해 설명합니다.
- 23-4페이지의 프로토콜 지정은 규칙이 테스트해야 하는 트래픽의 프로토콜을 정의하는 방법에 대해 설명합니다.
- 23-5페이지의 침입 규칙 내 IP 주소 지정은 규칙 헤더의 개별 IP 주소 및 IP 주소 블록을 정의하는 방법에 대해 설명합니다.
- 23-8페이지의 침입 규칙 내 포트 정의는 헤더 규칙에서 개별 포트 및 포트 범위를 정의하는 정의하는 방법에 대해 설명합니다.
- 23-9페이지의 방향 지정은 사용 가능한 연산자를 보여주고 트래픽이 규칙으로 테스트될 수 있도록 순회되어야 하는 방향을 지정하는 방식을 설명합니다.

규칙 작업 지정

라이센스: 보호

각 규칙 헤더는 패킷이 규칙을 트리거할 때 시스템이 취할 작업을 지정하는 매개 변수를 포함합니다. *경고*로 설정된 작업을 가진 규칙은 규칙을 트리거한 패킷에 대해 침입 이벤트를 생성하고 해당 패킷의 세부 사항을 로깅합니다. *통과*로 설정된 작업을 가진 규칙은 규칙을 트리거한 패킷에 대해 이벤트를 생성하거나 해당 패킷의 세부 사항을 로깅하지 않습니다.

참고 인라인 배포에서 *Drop and Generate Events(이벤트 삭제 및 생성)*로 설정된 상태의 규칙은 규칙을 트리거한 패킷에 대해 침입 이벤트를 생성합니다. 또한 수동 배포에서 삭제 규칙을 적용할 경우, 규칙은 알림 규칙으로 작동합니다. 삭제 규칙에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

기본적으로, 통과 규칙은 경고 규칙을 대체합니다. 특정 상황에서 경고 규칙을 비활성화하는 대신 알림 규칙을 트리거하여 전달 규칙에 정의된 기준을 충족하는 패킷을 방지하는 전달 규칙을 만들 수 있습니다. 예를 들어, "익명" 사용자로 FTP 서버에 로그인을 시도하는 규칙이 활성 상태로 유지되기를 원할 수 있습니다. 하지만, 네트워크에 하나 이상의 적정 익명 FTP 서버가 있는 경우, 특정 서버의 경우, 익명 사용자는 원래 규칙을 트리거하지 않도록 지정하는 규칙을 작성하고 활성화할 수 있습니다.

규칙 편집기 내 **Action(작업)** 목록에서 규칙 유형을 선택합니다. 규칙 편집기를 사용하여 규칙 헤더를 구축하는 데 사용할 절차에 대한 자세한 내용은 23-100페이지의 규칙 구성을 참고하십시오.

프로토콜 지정

라이센스: 보호

각 규칙 헤더에서, 규칙이 검사하는 트래픽의 프로토콜을 지정해야 합니다. 분석을 위해 다음 네트워크 프로토콜을 지정할 수 있습니다.

- ICMP(Internet Control Message Protocol)
- IP(인터넷 프로토콜)

참고 프로토콜이 `ip`로 설정되면 시스템은 침입 규칙 헤더의 포트 정의를 무시합니다. 자세한 내용은 23-8페이지의 침입 규칙 내 포트 정의를 참고하십시오.

- TCP(전송 제어 프로토콜)
- UDP(사용자 데이터그램 프로토콜)

IP를 프로토콜 유형으로 사용하여 TCP, UDP, ICMP, IGMP 및 더 많은 수를 포함하는 IANA에 의해 할당된 모든 프로토콜을 검토합니다. IANA가 할당한 프로토콜의 전체 목록은 http://www.iana.org/assignments/protocol-numbers를 참고하십시오.

참고 지금은 IP 페이로드에서 다음 헤더(예를 들어, TCP 헤더)의 패턴과 일치하는 규칙을 작성할 수 없습니다. 대신, 일치하는 콘텐츠는 마지막 디코딩된 프로토콜과 함께 시작됩니다. 해결 방법으로, 규칙 옵션을 사용하여 TCP 헤더에서 패턴을 일치시킬 수 있습니다.

규칙 편집기 내 **Protocol(프로토콜)** 목록에서 프로토콜 유형을 선택합니다. 규칙 편집기를 사용하여 규칙 헤더를 구축하는 데 사용할 절차에 대한 자세한 내용은 23-100페이지의 규칙 구성을 참고하십시오.

침입 규칙 내 IP 주소 지정

라이센스: 보호

특정 IP 주소에서 시작하거나 특정 IP 주소를 대상으로 한 패킷 검사를 제한하면 시스템이 실행해야 하는 패킷 검사량이 줄어듭니다. 이는 또한 규칙을 보다 구체적으로 만들고 소스와 대상 IP 주소가 의심스러운 작업을 표시하지 않는 패킷에 대해 트리거된 규칙 가능성을 제거하여 잘못된 긍정을 줄입니다.

팁 시스템은 IP 주소만 인식하고 소스 또는 대상 IP 주소의 호스트 이름을 수락하지 않습니다.

규칙 편집기에서, **Source IPs(소스 IP)** 및 **Destination IPs(대상 IP)** 필드에 소스 및 대상 IP 주소를 지정합니다. 규칙 편집기를 사용하여 규칙 헤더를 구축하는 데 사용할 절차에 대한 자세한 내용은 23-100페이지의 규칙 구성을 참고하십시오.

표준 텍스트 규칙을 작성할 때, 필요에 따라 다양한 방법으로 IPv4 및 IPv6 주소를 지정할 수 있습니다. 단일 IP 주소, `any`(모두), IP 주소 목록, CIDR 코멘트, 접두사 길이, 네트워크 변수 또는 네트워크 개체나 네트워크 객체 그룹을 지정할 수 있습니다. 또한, 특정 IP 주소 또는 IP 주소의 집합을 제외할지 여부를 나타낼 수 있습니다. IPv6 주소를 지정할 때, RFC 4291에 정의된 주소 지정 규칙을 사용할 수 있습니다.

다음 표에서는 소스 및 대상 IP 주소를 지정할 수 있는 다양한 방법을 요약합니다.

표 23-2 소스/대상 IP 주소 구문

지정 대상	사용 환경	예
모든 IP 주소	`any`	`any`
특정 IP 주소	해당 IP 주소 동일한 규칙에서 IPv4 및 IPv6 소스와 대상 주소를 혼용하지 않는다는 점에 유의하십시오.	`192.168.1.1` `2001:db8::abcd`
IP 주소 목록	IP 주소를 둘러싸는 괄호(`[]`) 및 IP 주소를 구분하는 쉼표	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`
IP 주소 블록	IPv4 CIDR 블록 또는 IPv6 주소 접두사 코멘트	`192.168.1.0/24` `2001:db8::/32`
특정 IP 주소 또는 주소 집합을 제외한 모든 주소	IP 주소 또는 무효화를 원하는 주소 앞에 있는 `!` 문자	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
하나 이상의 특정 IP 주소를 제외한 IP 주소의 블록 내 모든 주소	무효화된 주소 또는 블록 목록이 뒤따르는 주소 블록	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
네트워크 변수에 정의된 IP 주소	`$`로 시작하는 대문자로 된 변수 이름 전처리기 규칙은 침입 규칙에서 사용되는 네트워크 변수에 의해 정의된 호스트에 관계없이 이벤트를 트리거할 수 있습니다. 자세한 내용은 2-14페이지의 변수 집합 작업을 참고하십시오.	`$HOME_NET`

표 23-2 소스/대상 IP 주소 구문 (계속)

지정 대상	사용 환경	예
IP 주소 변수에 의해 정의된 주소를 제외한 모든 IP 주소	`!$`로 시작하는 대문자로 된 변수 이름 자세한 내용은 23-7페이지의 침입 규칙에서 IP 주소 제외를 참고하십시오.	`!$HOME_NET`
네트워크 개체 또는 네트워크 객체 그룹에 의해 정의된 IP 주소	`!{object_name}`형식을 사용하는 개체 또는 그룹 이름 자세한 내용은 2-3페이지의 네트워크 개체 작업을 참고하십시오.	`${192.168sub16}`
네트워크 개체 또는 네트워크 객체 그룹에 의해 정의된 주소를 제외한 모든 IP 주소	`!$`로 시작하며 중괄호(`{}`) 안에 있는 개체 또는 그룹 이름 자세한 내용은 2-3페이지의 네트워크 개체 작업을 참고하십시오.	`!${192.168sub16}`

소스 및 대상 IP 주소를 지정하는 데 사용할 수 있는 구문에 대한 자세한 내용과 변수를 사용한 IP 주소 지정에 대한 자세한 내용은

- 1-4페이지의 IP 주소 규칙.
- 2-14페이지의 변수 집합 작업
- 23-6페이지의 모든 IP 주소 지정
- 23-6페이지의 여러 IP 주소 지정
- 23-7페이지의 네트워크 개체 지정
- 23-7페이지의 침입 규칙에서 IP 주소 제외

모든 IP 주소 지정

라이센스: 보호

모든 IPv4 또는 IPv6 주소를 나타내는 규칙 소스 또는 대상 IP 주소로 `any`라는 단어를 지정할 수 있습니다.

예를 들어, 다음 규칙은 **Source IPs(소스 IP)** 및 **Destination IPs(대상 IP)** 필드의 인수 **any**를 사용하며 모든 IPv4 또는 IPv6 소스와 대상 주소로 패킷을 평가합니다.

```
alert tcp any any -> any any
```

또한 `::`을 지정하여 모든 IPv6 주소를 나타낼 수 있습니다.

여러 IP 주소 지정

라이센스: 보호

쉼표로 IP 주소를 구분하고 선택적으로, 다음의 예시에서와 같이 무효화되지 않은 목록을 괄호로 묶어 개별 IP 주소를 나열할 수 있습니다.

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

IPv4와 IPv6는 다음의 예시에서처럼 개별적으로 또는 조합하여 나열할 수 있습니다.

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

이전 소프트웨어 릴리스에서는 괄호로 IP 주소 목록을 포함하는 것이 필요하지만 여기서는 필요하지 않다는 점에 유의하십시오. 선택 사항으로, 각 쉼표 앞이나 뒤에 스페이스로 목록을 입력할 수 있다는 점도 참고하십시오.

참고 무효화된 목록을 괄호로 묶어야 합니다. 자세한 내용은 23-7페이지의 침입 규칙에서 IP 주소 제외를 참고하십시오.

또한 IPv4 CIDR(Classless Inter-Domain Routing: 클래스리스 도메인 간 라우팅) 표시법 또는 IPv6 접두사 길이를 사용하여 주소 블록을 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- 192.168.1.0/24는 서브넷 마스크 255.255.255.0, 즉, 192.168.1.255를 통한 192.168.1.0으로 192.168.1.0 네트워크에서 IPv4 주소를 지정합니다. 자세한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.
- 2001:db8::/32는 2001:db8:: 네트워크에서 32비트의 접두사 길이로 IPv6 주소를 지정하는데, 이는, 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff를 통한 2001:db8::입니다.

팁 IP 주소 블록을 지정해야 하지만 CIDR 또는 접두사 길이 표기를 사용하여 이를 표시할 수 없는 경우, CIDR 블록 및 IP 주소 내 접두사 길이를 사용할 수 있습니다.

네트워크 개체 지정

라이센스: 보호

구문을 사용하여 네트워크 개체 또는 네트워크 객체 그룹을 지정할 수 있습니다.

```
${object_name | group_name}
```

여기에서 각 항목은 다음을 나타냅니다.

- *object_name*은 네트워크 개체의 이름입니다.
- *group_name*은 네트워크 객체 그룹의 이름입니다.

네트워크 개체 및 네트워크 객체 그룹 생성에 대한 내용은 2-3페이지의 네트워크 개체 작업을 참고하십시오.

`192.168sub16`으로 명명된 네트워크 개체 및 `all_subnets`로 명명된 네트워크 객체 그룹을 생성한 경우를 고려하십시오. 네트워크 개체를 사용하여 IP 주소를 확인하려면 다음과 같이 지정할 수 있습니다.

```
${192.168sub16}
```

네트워크 객체 그룹을 사용하려면 다음과 같이 지정할 수 있습니다.

```
${all_subnets}
```

또한 네트워크 개체 및 네트워크 객체 그룹과 함께 무효화를 사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
!${192.168sub16}
```

자세한 내용은 23-7페이지의 침입 규칙에서 IP 주소 제외를 참고하십시오.

침입 규칙에서 IP 주소 제외

라이센스: 보호

느낌표(!)를 사용하여 지정된 IP 주소를 무효화할 수 있습니다. 즉, 지정된 IP 주소 또는 주소를 제외한 모든 IP 주소와 일치할 수 있습니다. 예를 들어, `! 192.168.1.1`은 192.168.1.1 이외의 모든 IP 주소를 지정하고, `! 2001: db8: ca2e:: fa4c`는 2001: db8: ca2e:: fa4c. 이외의 모든 IP 주소를 지정합니다.

IP 주소 목록을 무효화하려면 괄호로 묶은 IP 주소의 목록 앞에 !를 표시하십시오. 예를 들어, `![192.168.1.1,192.168.1.5]`는 192.168.1.1 또는 192.168.1.5. 이외의 모든 IP 주소를 정의합니다.

참고 IP 주소 목록을 무효화하기 위해서는 괄호를 사용해야 합니다.

IP 주소 목록과 함께 무효화 문자를 사용할 때는 주의하십시오. 예를 들어, 192.168.1.1 또는 192.168.1.5가 아닌 모든 주소를 일치시키기 위해 `[!192.168.1.1,!192.168.1.5]`를 사용하는 경우, 시스템은 이 구문을 "192.168.1.1이 아닌 모든 주소, **또는** 192.168.1.5가 아닌 모든 주소"로 해석합니다.

192.168.1.5는 192.168.1.1이 아니고 192.168.1.1은 192.168.1.5가 아니므로, 두 IP 주소 모두 IP 주소 `[!192.168.1.1,!192.168.1.5]` 값에 일치하며, 이는 본질적으로 "`any(모두)`"를 사용하는 것과 동일합니다.

이보다는 `![192.168.1.1,192.168.1.5]`를 사용하십시오. 시스템은 이를 "192.168.1.1이 **아니며** 192.168.1.5도 **아닌** 주소"로 해석하며, 이는 괄호 사이에 나열된 IP 주소를 제외한 모든 IP 주소에 일치하는 것입니다.

논리적으로 `any(모두)`와 무효화를 함께 사용할 수 없다는 점에 유의하십시오. 함께 사용하는 경우 무효화되면 어떤 주소도 나타내지 못하게 됩니다.

침입 규칙 내 포트 정의

라이센스: 보호

규칙 편집기에서, **Source Port(소스 포트)**와 **Destination Port(대상 포트)** 필드에 소스 및 대상 포트를 지정합니다. 규칙 편집기를 사용하여 규칙 헤더를 구축하는 데 사용할 절차에 대한 자세한 내용은 23-100페이지의 규칙 구성을 참고하십시오.

ASA FirePOWER 모듈은 규칙 헤더에 사용되는 포트 번호를 정의하기 위해 특정 유형의 구문을 사용합니다.

참고 프로토콜이 `ip`로 설정되면 시스템은 침입 규칙 헤더의 포트 정의를 무시합니다. 자세한 내용은 23-4페이지의 프로토콜 지정을 참고하십시오.

다음의 예시에서와 같이 쉼표로 포트를 구분하여 나열할 수 있습니다.

```
80, 8080, 8138, 8600-9000, !8650-8675
```

또는, 다음의 예시는 괄호로 포트 목록을 묶는 방법을 보여주는데, 이는 이전의 소프트웨어 버전에서는 필요했지만 더 이상 필요하지 않습니다.

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

다음의 예시에서처럼 무효화된 포트 목록을 **반드시** 괄호로 묶어야 한다는 점에 유의하십시오.

```
![20, 22, 23]
```

침입 규칙 내 소스 또는 대상 포트의 목록은 최대 64개의 문자를 포함할 수 있다는 점에 유의하십시오.

다음 표는 사용 가능한 구문을 요약한 것입니다.

표 23-3 소스/대상 포트 구문

지정 대상	사용 환경	예
모든 포트	`any`	`any`
특정 포트	포트 번호	`80`
포트 범위	범위 내 첫 번째 및 마지막 포트 번호 사이의 대시	`80-443`

표 23-3 소스/대상 포트 구문 (계속)

지정 대상	사용 환경	예
특정 포트보다 작거나 같은 모든 포트	포트 번호 앞의 대시	-21
특정 포트보다 같거나 큰 모든 포트	포트 번호 다음의 대시	80-
특정 포트 또는 특정 범위의 포트를 제외한 모든 포트	무효화를 원하는 포트, 포트 목록 또는 범위의 포트 앞의 !문자 논리적으로는 *any (모두)*를 제외한 모든 포트 대상과 무효화를 함께 사용할 수 있다는 점에 유의하십시오. 이 경우 무효화되면 *no port (포트 없음)*로 표시됩니다.	!20
포트 변수에 의해 정의된 모든 포트	$로 시작하는 대문자로 된 변수 이름 자세한 내용은 2-26페이지의 포트 변수 작업을 참고하십시오.	$HTTP_PORTS
포트 변수에 의해 정의된 포트를 제외한 모든 포트	!$로 시작하는 대문자로 된 변수 이름	!$HTTP_PORTS

방향 지정

라이센스: 보호

규칙 헤더 내에서, 규칙이 패킷을 검사할 수 있도록 패킷이 이동해야 하는 방향을 지정할 수 있습니다. 다음 표는 이러한 옵션에 대해 설명합니다.

표 23-4 규칙 헤더의 방향 옵션

사용 환경	테스트 대상
방향	특정 소스 IP 주소에서 특정 대상 IP 주소로 이동하는 트래픽에 한정
양방향	특정 소스 및 대상 IP 주소 간에 이동하는 모든 트래픽

규칙 편집기를 사용하여 규칙 헤더를 구축하는 데 사용할 절차에 대한 자세한 내용은 23-100페이지의 규칙 구성을 참고하십시오.

규칙 내 키워드 및 인수의 이해

라이센스: 보호

규칙 언어를 사용하여 키워드를 결합함으로써 규칙 작업을 지정할 수 있습니다. 키워드 및 관련 값(일명 *인수*)은 규칙 엔진이 테스트하는 패킷 및 패킷 관련 값을 시스템이 평가하는 방법을 지시합니다. ASA FirePOWER 모듈은 현재 콘텐츠 일치, 특정 프로토콜에 한정된 패턴 일치, 특성 상태에 한정된 일치와 같은 검사 기능을 수행할 수 있도록 하는 키워드를 지원합니다. 키워드 당 최대 100개의 인수를 정의할 수 있고, 매우 특정한 규칙을 만들기 위해 호환성 키워드를 얼마든지 통합할 수 있습니다. 이는 잘못된 긍정 및 잘못된 부정의 가능성을 줄이고 사용자가 수신하는 침입 정보에 집중하는 데 도움을 줍니다.

또한 적응형 프로파일을 사용하여 규칙 메타데이터와 호스트 정보에 따라 특정 패킷에 대한 활성 규칙 처리를 동적으로 조정할 수 있습니다. 자세한 내용은 18-1페이지의 수동 배포 시 전처리 조정을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-11페이지의 침입 이벤트 세부사항 정의는 구문을 설명하고 이벤트 메시지, 우선 순위 정보 및 규칙이 탐지하는 공격에 대한 외부 정보 참고 사항을 정의할 수 있는 키워드를 사용합니다.
- 23-15페이지의 콘텐츠 일치 검색은 `content` 또는 `protected_content` 키워드를 사용하여 패킷 페이로드의 내용을 테스트하는 방법을 설명합니다.
- 23-17페이지의 콘텐츠 일치 제한은 `content` 또는 `protected_content` 키워드에 대해 수정 키워드를 사용하는 방법을 설명합니다.
- 23-29페이지의 인라인 배포에서 콘텐츠 대체는 인라인 배포에서 `replace` 키워드를 사용하여 동일한 길이의 지정된 내용을 대체하는 방법을 설명합니다.
- 23-30페이지의 Byte_Jump 및 Byte_Test 사용은 `byte_jump` 및 `byte_test` 키워드를 사용하여 규칙 엔진이 콘텐츠 일치에 대한 테스트를 패킷의 어디에서 시작해야 할지와 어느 바이트를 평가해야 할지 계산하는 방법을 설명합니다.
- 23-35페이지의 PCRE를 사용한 콘텐츠 검색은 `pcre` 키워드를 사용하여 규칙에서 펄 호환 정규 표현식을 사용하는 방법을 설명합니다.
- 23-41페이지의 규칙에 메타데이터 추가는 `metadata` 키워드를 사용하여 규칙에 정보를 추가하는 방법을 설명합니다.
- 23-45페이지의 IP 헤더 값 검사는 패킷의 IP 헤더 값을 테스트할 키워드의 구문 및 사용을 설명합니다.
- 23-47페이지의 ICMP 헤더 값 검사는 패킷의 ICMP 헤더 값을 테스트할 키워드의 구문 및 사용을 설명합니다.
- 23-49페이지의 TCP 헤더 값과 스트림 크기 검사는 패킷의 TCP 헤더 값을 테스트할 키워드의 구문 및 사용을 설명합니다.
- 23-53페이지의 TCP 스트림 리어셈블리 활성화 및 비활성화는 규칙의 조건이 연결에서 검사된 트래픽과 일치할 때 단일 연결에 대한 스트림 리어셈블리를 활성화 및 비활성화하는 방법을 설명합니다.
- 23-54페이지의 세션에서 SSL 정보 추출은 암호화된 트래픽에서 버전 및 상태 정보를 추출할 키워드 사용 및 구문을 설명합니다.
- 23-81페이지의 패킷 데이터를 키워드 인수로 읽어들이기는 다른 특정 키워드에서 인수에 대한 값을 지정하기 위해 패킷으로부터 값을 읽어 동일한 규칙에서 나중에 사용할 수 있는 변수로 해석하는 방법을 설명합니다.
- 23-56페이지의 애플리케이션 레이어 프로토콜 값 검사는 애플리케이션 레이어 프로토콜 속성을 테스트하는 키워드 사용 및 구문을 설명합니다.
- 23-78페이지의 패킷 특성 검사는 `dsize`, `sameIP`, `isdataat`, `fragoffset` 및 `cvs` 키워드의 사용 및 구문을 설명합니다.
- 23-83페이지의 규칙 키워드로 활성 응답 시작은 `resp` 키워드를 사용하여 TCP 연결 또는 UDP 세션을 적극적으로 닫는 방법, `react` 키워드를 사용하여 HTML 페이지를 전송한 후 TCP 연결을 적극적으로 닫는 방법, 그리고 `config response` 명령을 사용하여 활성 응답 인터페이스와 수동 배포에서 시도하도록 재설정된 TCP 수를 지정하는 방법을 설명합니다.
- 23-87페이지의 필터링 이벤트은 지정된 패킷 수가 지정된 시간 내 규칙의 탐지 기준을 충족하지 않는 한 규칙이 이벤트를 트리거하지 못하도록 차단하는 방법을 설명합니다.
- 23-88페이지의 공격 후 트래픽 평가는 호스트 또는 세션에 대한 추가 트래픽을 로깅하는 방법을 설명합니다.
- 23-89페이지의 다중 패킷을 포함하는 공격 탐지는 단일 세션에서 여러 패킷에 걸친 공격에서 패킷에 상태 이름을 지정한 후 상태에 따라 패킷을 분석하고 경고하는 방법에 대해 설명합니다.

- 23-94페이지의 HTTP 인코딩 유형 및 위치에서 이벤트 생성은 표준화하기 전의 HTTP 요청 또는 응답 URI, 헤더 또는 set-cookie를 포함하는 쿠키에서 인코딩 유형에 이벤트를 생성하는 방법을 설명합니다.
- 23-95페이지의 파일 유형 및 버전 탐지는 `file_type` 또는 `file_group` 키워드를 사용하여 특정 파일 유형 또는 파일 버전을 가리키도록 하는 방법을 설명합니다.
- 23-97페이지의 특정 페이로드 유형 나타내기는 HTTP 응답 엔터티 텍스트, SMTP 페이로드 또는 인코딩된 이메일 첨부 파일의 초기를 가리키도록 하는 방법을 설명합니다.
- 23-98페이지의 패킷 페이로드의 시작 나타내기는 패킷 페이로드의 시작을 가리키도록 하는 방법을 설명합니다.
- 23-99페이지의 Base64 데이터 디코딩 및 검사는 특히 HTTP 요청에서 `base64_decode` 및 `base64_data` 키워드를 사용하여 Base64 데이터를 디코딩하고 검사하는 방법을 설명합니다.

침입 이벤트 세부사항 정의

라이센스: 보호

표준 텍스트 규칙을 구성할 때, 규칙이 공격 시도를 탐지하게 되는 취약점을 설명하는 컨텍스트 정보를 포함할 수 있습니다. 또한 취약점 데이터베이스에 외부 참조를 포함하고 사용자 조직에서 이벤트가 가지고 있는 우선 순위를 정의할 수 있습니다. 분석가가 이벤트를 볼 때, 그들은 우선 순위, 공격, 즉시 사용 가능한 알려진 위협 완화에 대한 정보를 가지게 됩니다.

이벤트 관련 키워드에 대한 자세한 내용은 다음 섹션을 참고하십시오.

- 23-11페이지의 이벤트 메시지 정의
- 23-12페이지의 이벤트 우선 순위 정의
- 23-12페이지의 침입 이벤트 분류 정의
- 23-14페이지의 이벤트 참조 정의

이벤트 메시지 정의

라이센스: 보호

규칙이 트리거될 때 메시지로 표시되는 의미 있는 텍스트를 지정할 수 있습니다. 메시지는 규칙이 공격 시도를 탐지하게 되는 취약점의 속성에 대한 즉각적인 통찰력을 제공해 줍니다. 중괄호(`{}`)를 제외한 인쇄 가능한 표준 ASCII 문자를 모두 사용할 수 있습니다. 시스템은 메시지를 완전히 묶고 있는 따옴표를 떼어버립니다.

팁 규칙 메시지를 지정해야 합니다. 또한, 공백, 하나 이상의 따옴표, 하나 이상의 아포스트로피 또는 공백, 따옴표, 아포스트로피로의 조합만으로는 메시지를 구성할 수 없습니다.

규칙 편집기에서 이벤트 메시지를 정의하려면, **Message(메시지)** 필드에 이벤트 메시지를 입력합니다. 규칙을 구축하는 규칙 편집기 사용에 대한 자세한 내용은 23-100페이지의 규칙 구성을 참고하십시오.

이벤트 우선 순위 정의

라이센스: 보호

기본적으로, 규칙의 우선 순위는 규칙에 대한 이벤트 분류에서 파생됩니다. 그러나, 규칙에 `priority` 키워드를 추가하여 규칙에 대한 분류 우선 순위를 무시할 수 있습니다.

규칙 편집기를 사용하여 우선 순위를 지정하려면, **Detection Options(탐지 옵션)** 목록에서 **priority(우선 순위)**를 선택하고, 드롭다운 목록에서 **high(높음)**, **medium(중간)** 또는 **low(낮음)**를 선택합니다. 예를 들어, 웹 애플리케이션 공격을 탐지하는 규칙에 **high(높음)** 우선 순위를 할당하기 위해서는, `priority` 키워드를 규칙에 추가하고 우선 순위로 **high(높음)**를 선택합니다. 규칙을 구축하는 규칙 편집기 사용에 대한 자세한 내용은 23-100페이지의 규칙 구성을 참고하십시오.

침입 이벤트 분류 정의

라이센스: 보호

각 규칙에, 이벤트의 패킷 표시에 나타나는 공격 분류를 지정할 수 있습니다. 다음 표에서는 각 분류의 이름과 번호를 나열합니다.

표 23-5 규칙 분류

번호	분류 이름	설명
1	not-suspicious	의심스럽지 않은 트래픽
2	unknown	알 수 없는 트래픽
3	bad-unknown	잠재적인 악성 트래픽
4	attempted-recon	정보 유출 시도
5	successful-recon-limited	정보 유출
6	successful-recon-largescale	대규모 정보 유출
7	attempted-dos	서비스 거부 시도
8	successful-dos	서비스 거부
9	attempted-user	사용자 권한 획득 시도
10	unsuccessful-user	사용자 권한 획득 실패
11	successful-user	사용자 권한 획득 성공
12	attempted-admin	관리자 권한 획득 시도
13	successful-admin	관리자 권한 획득 성공
14	rpc-portmap-decode	RPC 쿼리 디코드
15	shellcode-detect	실행 가능한 코드가 탐지됨
16	string-detect	의심스러운 문자열이 탐지됨
17	suspicious-filename-detect	의심스러운 파일 이름이 탐지됨
18	suspicious-login	의심스러운 사용자 이름을 사용한 로그인 시도가 탐지됨
19	system-call-detect	시스템 호출이 탐지됨
20	tcp-connection	TCP 연결이 탐지됨
21	trojan-activity	네트워크 트로이 목마가 탐지됨
22	unusual-client-port-connection	클라이언트가 비정상적인 포트를 사용하고 있음

표 23-5 규칙 분류 (계속)

번호	분류 이름	설명
23	network-scan	네트워크 스캔이 탐지됨
24	denial-of-service	서비스 거부 공격(DoS)이 탐지됨
25	non-standard-protocol	비표준 프로토콜 또는 이벤트가 탐지됨
26	protocol-command-decode	일반적인 프로토콜 명령 디코드
27	web-application-activity	잠재적으로 취약한 웹 애플리케이션에 액세스
28	web-application-attack	웹 애플리케이션 공격
29	misc-activity	기타 활동
30	misc-attack	기타 공격
31	icmp-event	일반 ICMP 이벤트
32	inappropriate-content	부적절한 콘텐츠가 발견됨
33	policy-violation	잠재적인 기업 개인 정보 보호 위반
34	default-login-attempt	기본 사용자 이름 및 비밀번호로 로그인 시도
35	sdf	중요한 데이터
36	malware-cnc	알려진 악성코드 명령 및 제어 트래픽
37	client-side-exploit	알려진 클라이언트 측 공격 시도
38	file-format	알려진 악성 파일 또는 파일 기반 공격

규칙 편집기의 분류를 지정하려면, **Classification(분류)** 목록에서 분류를 선택합니다. 규칙 편집기에 대한 자세한 내용은 23-101페이지의 새규칙 작성을 참고하십시오.

사용자 지정 분류 추가

라이센스: 보호

사용자가 정의하는 규칙에서 생성된 이벤트의 패킷 표시 설명을 위한 더 많은 맞춤형 콘텐츠를 원할 경우, 사용자 지정 그룹을 만듭니다.

분류를 정렬 목록에 추가하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책) > Rule Editor(규칙 편집기)**.를 선택합니다.

Rule Editor(규칙 편집기) 페이지가 나타납니다.

단계 2 **Create Rule(규칙 생성)**을 클릭합니다.

Create Rule(규칙 생성) 페이지가 나타납니다.

단계 3 **Classification(분류)** 드롭다운 목록 아래에서 **Edit Classifications(분류 수정)**를 클릭합니다.

팝업 창이 나타납니다.

단계 4 **Classification Name(분류 이름)** 필드에 분류 이름을 입력합니다.

최대 255개의 영숫자를 사용할 수 있지만, 페이지에 40개 이상의 문자를 사용하면 가독성이 떨어집니다. 다음 문자는 지원되지 않습니다: `<> () \ ' " & $ ;` 및 공백 문자.

단계 5 **Classification Description(분류 설명)** 필드에 분류 설명을 입력합니다.

최대 255자의 영숫자 및 공백을 사용할 수 있습니다. <> () \ ' " & $; 문자는 지원되지 않습니다.

단계 6 **Priority(우선 순위)** 목록에서 우선 순위를 선택하십시오.

high(높음), **medium(중간)** 또는 **low(낮음)**를 선택할 수 있습니다.

단계 7 **Add(추가)**를 클릭합니다.

새 분류가 목록에 추가되고 규칙 편집기에 사용할 수 있게 됩니다.

단계 8 **Done(완료)**을 클릭합니다.

이벤트 참조 정의

라이센스: 보호

`reference` 키워드를 사용하여 외부 웹 사이트에 참조를 추가하고 이벤트에 대한 자세한 내용을 추가할 수 있습니다. 참조를 추가하면 패킷이 규칙을 트리거한 이유에 대한 확인을 돕기 위해 분석가에게 즉시 사용 가능한 리소스를 제공합니다. 다음 표는 알려진 악성 공격에 관한 데이터를 제공하는 몇 가지 외부 시스템 나열합니다.

표 23-6 외부 공격 식별 시스템

시스템 ID	설명	예시 ID
`bugtraq`	Bugtraq 페이지	`8550`
`cve`	일반 취약성 및 노출 페이지	`CAN-2003-0702`
`mcafee`	McAfee 페이지	`98574`
`url`	웹사이트 참조	`www.example.com?exploit=14`
`msb`	Microsoft 보안 공지	`MS11-082`
`nessus`	Nessus 페이지	`10039`
`secure-url`	보안 웹 사이트 참조 (https://...)	`intranet/exploits/exploit=14` 모든 보안 웹 사이트로 `secure-url`을 함께 사용할 수 있다는 점을 참고하십시오.

규칙 편집기를 사용하여 참조 사항을 지정하려면, **Detection Options(탐지 옵션)** 목록에서 **reference(참조)**를 선택하고, 다음과 같이 해당되는 필드에 값을 입력합니다.

`id_system``,`*`id`*

*`id_system`*이 접두사로 사용되고 있는 시스템인 경우, 그리고 *`id`*가 Bugtraq ID, CVE 번호, Arachnids ID 또는 URL인 경우(`http://` 제외)

예를 들어, Bugtraq ID 17134에 문서화된 Microsoft Commerce Server 2002 서버에 인증 우회 취약성을 지정하려면, **reference(참조)** 필드에서 다음을 입력합니다.

```
bugtraq,17134
```

규칙에 참조 사항을 추가할 때 다음에 유의하십시오.

- 쉼표 뒤에 스페이스를 사용하지 마십시오.
- 시스템 ID에 대문자를 사용하지 마십시오.

규칙을 구축하는 규칙 편집기 사용에 대한 자세한 내용은 23-100페이지의 규칙 구성을 참고하십시오.

콘텐츠 일치 검색

라이센스: 보호

이 패킷에서 탐지할 내용을 지정하려면 `content` 또는 `protected_content` 키워드를 사용합니다. 자세한 내용은 다음 섹션을 참고하십시오.

- 23-15페이지의 콘텐츠 키워드 사용
- 23-15페이지의 protected_content 키워드 사용
- 23-16페이지의 콘텐츠 일치 구성

콘텐츠 키워드 사용

`content` 키워드를 사용하면, 규칙 엔진이 해당 문자열에 대한 패킷 페이로드 또는 스트림을 검색합니다. 예를 들어, `content` 키워드 중 하나의 값으로 `/bin/sh`를 입력하면, 규칙 엔진은 문자열 `/bin/sh`에 대한 패킷 페이로드를 검색합니다.

ASCII 문자열, 16진수 콘텐츠(이진 바이트 코드) 또는 이 둘의 조합 중 하나를 사용하여 콘텐츠에 일치시킵니다. 키워드 값에서 파이프 문자(|)로 16진수 콘텐츠를 묶습니다. 예를 들어, `|90C8 C0FF FFFF|/bin/sh`와 같은 형태를 사용하여 16진수 콘텐츠 및 ASCII 콘텐츠를 섞을 수 있습니다.

단일 규칙에서 여러 콘텐츠 일치를 지정할 수 있습니다. 이를 위해, `content` 키워드의 추가 인스턴스를 사용합니다. 각 콘텐츠 일치의 경우, 규칙이 트리거되려면 패킷 페이로드 또는 스트림에서 콘텐츠 일치를 찾아야 한다는 것을 나타낼 수 있습니다.

protected_content 키워드 사용

`protected_content` 키워드를 사용하면 규칙 인수를 구성하기 전에 검색 내용 문자열을 인코딩할 수 있습니다. 원래 규칙 작성자는 키워드를 구성하기 전에 문자열을 인코딩하기 위해 해시 함수(SHA-512, SHA-256 또는 MD5)를 사용합니다.

`content` 키워드 대신 `protected_content` 키워드를 사용하면, 규칙 엔진이 해당 문자열 및 예상한 대로 대부분 키워드 옵션에 대해 패킷 페이로드 또는 스트림을 검색하는 방법은 변경되지 않습니다. 다음 표에서는 `protected_content` 키워드 옵션이 `content` 키워드 옵션과 구별되는 예외를 요약합니다.

표 23-7 protected_content 옵션 예외

옵션	설명
해시 유형	`protected_content` 규칙 키워드에 대한 새로운 옵션. 자세한 내용은 23-18페이지의 해시 유형을 참고하십시오.
대소문자 구분 안 함	지원되지 않음
내부	지원되지 않음
수준	지원되지 않음
길이	`protected_content` 규칙 키워드에 대한 새로운 옵션. 자세한 내용은 23-21페이지의 길이를 참고하십시오.
빠른 패턴 매처 사용	지원되지 않음
빠른 패턴 매처 한정	지원되지 않음
빠른 패턴 매처 오프셋 및 길이	지원되지 않음

Cisco는 protected_content 키워드를 포함하는 규칙에 최소 하나의 content 키워드를 포함할 것을 권장합니다. 이렇게 하면 규칙 엔진이 빠른 패턴 매처를 사용하여 처리 속도를 높이고 성능을 향상시킬 수 있습니다. 규칙에서 protected_content 키워드 앞에 콘텐츠 keyword를 배치합니다. 규칙에 최소 하나의 content 키워드가 포함될 때, content 키워드 Use Fast Pattern Matcher(빠른 패턴 매처 사용) 인수를 활성화했는지 여부에 상관 없이 규칙 엔진이 빠른 패턴 매처를 사용한다는 점에 유의하십시오.

콘텐츠 일치 구성

사용자는 거의 항상 content 또는 protected_content 키워드를 따라야 합니다. 이 키워드는 콘텐츠를 어디에서 검색해야 할지, 검색에 있어 대소문자 구분이 필요한지 여부, 그리고 다른 옵션을 나타내는 수식어 옆에 있습니다. content 및 protected_content 키워드에 대한 수식어에 관한 자세한 내용은 콘텐츠 일치 제한을 참고하십시오.

모든 콘텐츠 일치는 이벤트를 트리거하는 규칙에 대해 참이어야 한다는 점, 즉, 각 콘텐츠 일치는 다른 항목과 AND 관계를 가지고 있다는 점에 유의하십시오.

또한, 인라인 배포에서 악성 콘텐츠와 일치하고 이를 동일한 길이의 자체 문자열로 대체하는 규칙을 설정할 수 있다는 점에 유의하십시오. 자세한 내용은 23-29페이지의 인라인 배포에서 콘텐츠 대체를 참고하십시오.

일치하는 내용을 입력하려면 다음을 수행합니다.

단계 1 content 필드에, 찾고 싶은 내용(예를 들어, |90C8 C0FF FFFF|/bin/sh)을 입력합니다.

지정된 내용이 **아닌** 모든 콘텐츠를 검색하고자 하는 경우, **Not(아님)** 확인 상자를 선택합니다.

주의 단 한 개의 content 키워드만 포함하는데 해당 키워드가 **Not(아님)** 옵션을 선택한 규칙을 생성하는 경우, 침입 정책을 무효화할 수 있습니다. 자세한 내용은 23-19페이지의 아님을 참고하십시오.

단계 2 또는, content 키워드를 수정하거나 키워드에 대한 제한 조건을 추가하는 추가 키워드를 추가합니다.

다른 키워드에 대한 자세한 내용은 23-9페이지의 규칙 내 키워드 및 인수의 이해를 참고하십시오. content 키워드 제한에 대한 자세한 내용은 23-17페이지의 콘텐츠 일치 제한을 참고하십시오.

단계 3 규칙 만들기 또는 수정을 계속합니다.

자세한 내용은 23-101페이지의 새규칙 작성 또는 23-103페이지의 기존 규칙 변경을 참고하십시오.

일치하는 보호된 콘텐츠를 입력하려면 다음을 수행합니다.

단계 1 SHA-512, SHA-256, 또는 MD5 해시 생성기를 사용하여 찾고자 하는 콘텐츠를 인코딩합니다(예를 들어, SHA-512 해시 생성기를 통해 Sample1 문자열을 실행합니다).

생성기가 문자열에 대한 해시를 출력합니다.

단계 2 protected_content 필드에 1단계에서 생성한 해시(예를 들어, B20AABAF59605118593404BD42FE69BD8D6506EE7F1A71CE6BB470B1DF848C814BC5DBEC2081999F15691A71FAECA5FBA4A3F8B8AB56B7F04585DA6D73E5DD15)를 입력합니다.

지정된 내용이 **아닌** 모든 콘텐츠를 검색하고자 하는 경우, **Not(아님)** 확인 상자를 선택합니다.

주의 단 한 개의 `protected_content` 키워드만 포함하는데 해당 키워드가 **Not(아님)** 옵션을 선택한 규칙을 생성하는 경우, 침입 정책을 무효화할 수 있습니다. 자세한 내용은 23-19페이지의 아님을 참고하십시오.

단계 3 **Hash Type(해시 유형)** 드롭다운 목록에서 1단계에서 사용한 해시 함수(예를 들어, **SHA-512**)를 선택합니다. 2단계에 입력된 해시의 비트 수는 **반드시** 해시 유형에 일치해야 하며, 그렇지 않을 경우 시스템이 규칙을 저장하지 않는다는 점에 유의하십시오. 자세한 내용은 23-18페이지의 해시 유형을 참고하십시오.

팁 Cisco가 설정한 **Default(기본값)**를 선택할 경우, 시스템은 SHA-512를 해시 함수로 가정합니다.

단계 4 필요한 **Length(길이)** 필드에 값을 입력합니다. 이 값은 **반드시** 사용자가 찾고자 하는 원래의 해시되지 않은 문자열의 길이에 일치해야 합니다(예를 들어, 2단계의 문자열 `Sample1`은 `7`의 길이를 갖고 있습니다).

자세한 내용은 23-21페이지의 길이를 참고하십시오.

단계 5 **Offset(오프셋)** 또는 **Distance(영역)** 필드에 값을 입력합니다. 단일 키워드 구성에서 **Offset(오프셋)**과 **Distance(영역)** 옵션을 함께 사용할 수 없습니다.

자세한 내용은 23-22페이지의 protected_content 키워드에서 검색 위치 옵션 사용을 참고하십시오.

단계 6 또는, `protected_content` 키워드를 수정하는 추가 제한 옵션을 추가합니다.

자세한 내용은 23-17페이지의 콘텐츠 일치 제한을 참고하십시오.

단계 7 또는, `protected_content` 키워드를 수정하는 추가 키워드를 추가합니다.

자세한 내용은 23-9페이지의 규칙 내 키워드 및 인수의 이해를 참고하십시오.

단계 8 규칙 만들기 또는 수정을 계속합니다.

자세한 내용은 23-101페이지의 새규칙 작성 또는 23-103페이지의 기존 규칙 변경을 참고하십시오.

콘텐츠 일치 제한

라이센스: 보호

`content` 또는 `protected_content` 키워드를 수정할 매개 변수로 콘텐츠 검색 위치 및 대문자와 소문자가 구별 민감도를 제한할 수 있습니다. 검색할 내용을 지정하기 위해 `content` 또는 `protected_content` 키워드를 수정하는 옵션을 구성합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-18페이지의 대소문자 구분 안 함
- 23-18페이지의 해시 유형
- 23-19페이지의 원시 데이터
- 23-19페이지의 아님
- 23-20페이지의 위치 검색 옵션
- 23-23페이지의 HTTP 콘텐츠 옵션
- 23-26페이지의 빠른 패턴 매처 사용

대소문자 구분 안 함

라이센스: 보호

참고 protected_content 키워드를 구성할 때 이 옵션은 지원되지 **않습니다**. 자세한 내용은 23-15페이지의 protected_content 키워드 사용을 참고하십시오.

ASCII 문자열의 콘텐츠 일치를 검색할 때 대소문자 구분을 무시하기 위해 규칙 엔진을 검사할 수 있습니다. 콘텐츠 검색을 지정할 때 검색에 대소문자 구분이 없게 하려면 **Case Insensitive(대소문자 구분 안 함)**를 선택합니다.

콘텐츠 검색을 할 때 대소문자 구분 안 함을 지정하려면 다음을 수행합니다.

단계 1 추가하려는 content 키워드에 대해 **Case Insensitive(대소문자 구분 안 함)**를 선택합니다.

단계 2 규칙 만들기 또는 수정을 계속합니다.

자세한 내용은 콘텐츠 일치 제한, 23-15페이지의 콘텐츠 일치 검색, 23-101페이지의 새규칙 작성 또는 23-103페이지의 기존 규칙 변경을 참고하십시오.

해시 유형

라이센스: 보호

참고 이 옵션은 protected_content 키워드에 **한정하여** 구성 가능합니다. 자세한 내용은 23-15페이지의 protected_content 키워드 사용을 참고하십시오.

Hash Type(해시 유형) 드롭다운을 사용하여 검색 문자열을 인코딩하는 데 사용한 해시 함수를 확인합니다. 시스템은 protected_content 검색 문자열에 대해 SHA-512, SHA-256 및 MD5 해싱을 지원합니다. 선택한 해시 유형이 해시된 콘텐츠의 길이와 일치하지 않을 경우, 시스템은 규칙을 저장하지 **않습니다**.

시스템은 자동으로 Cisco가 지정한 기본값 집합을 선택합니다. **Default(기본값)**를 선택할 때, 어떤 특정 해시 함수도 규칙에 로깅되지 않으며 시스템은 해시 함수에 대해 SHA-512를 가정합니다.

보호된 콘텐츠 검색을 할 때 해시 함수를 지정하려면 다음을 수행합니다.

단계 1 **Hash Type(해시 유형)** 드롭다운 목록에서 **Default(기본값)**를 선택하고, 추가하는 protected_content 키워드에 대한 해시로서 **SHA-512**, **SHA-256** 또는 **MD5**를 선택합니다.

팁 Cisco가 설정한 **Default(기본값)**를 선택할 경우, 시스템은 SHA-512를 해시 함수로 가정합니다. 자세한 내용은 23-18페이지의 해시 유형을 참고하십시오.

단계 2 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 콘텐츠 일치 제한, 23-15페이지의 콘텐츠 일치 검색, 23-101페이지의 새규칙 작성 또는 23-103페이지의 기존 규칙 변경을 참고하십시오.

원시 데이터

라이센스: 보호

Raw Data(원시 데이터) 옵션은 (네트워크 분석 정책에서 디코딩된) 표준화된 페이로드 데이터를 분석하기 전에 원래 패킷 페이로드를 규칙 엔진이 분석하도록 지시하며, 인수 값을 사용하지 않습니다. 텔넷 트래픽을 분석할 때 이 키워드를 사용하여 표준화 전 페이로드에서 텔넷 협상 옵션을 선택할 수 있습니다.

Raw Data(원시 데이터) 옵션을 모든 HTTP 콘텐츠 옵션과 더불어 동일한 `content` 또는 `protected_content` 키워드 안에서 함께 사용할 수 없습니다. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오.

팁 HTTP 검사 전처리기 **Client Flow Depth(클라이언트 흐름 수준)** 및 **Server Flow Depth(서버 흐름 수준)** 옵션을 구성하여 원시 데이터가 HTTP 트래픽에서 검사되는지 여부 및 검사할 원시 데이터의 양을 결정할 수 있습니다. 자세한 내용은 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택을 참고하십시오.

원시 데이터를 분석하려면 다음을 수행합니다.

단계 1 추가하는 `content` 또는 `protected_content` 키워드를 위해 **Raw Data(원시 데이터)** 확인 상자를 선택합니다.

단계 2 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 콘텐츠 일치 제한, 23-15페이지의 콘텐츠 일치 검색, 23-101페이지의 새규칙 작성 또는 23-103페이지의 기존 규칙 변경을 참고하십시오.

아님

라이센스: 보호

지정된 내용과 일치하지 않는 콘텐츠를 검색하려면 **Not(아님)** 옵션을 선택합니다. **Not(아님)**옵션을 선택하여 `content` 또는 `protected_content` 키워드를 포함하는 규칙을 생성하는 경우, 반드시 규칙 안에 **Not(아님)** 옵션을 선택하지 않는 다른 `content` 또는 `protected_content` 키워드를 최소한 하나 포함해야 합니다.

주의 해당 키워드가 **Not(아님)**옵션을 선택하지 않은 경우 오직 하나의 `content` 또는 `protected_content` 키워드를 포함하는 규칙을 생성하지 않습니다. 침입 정책을 무효화할 수 있습니다.

예를 들어, SMTP 규칙 1:2541: 9는 3개의 `content` 키워드를 포함하며, 이 중 하나는 **Not(아님)** 옵션을 선택했습니다. **Not(아님)** 옵션을 선택한 키워드를 제외한 모든 `content` 키워드를 제거할 경우 이 규칙에 기반한 사용자 지정 규칙은 무효화될 것입니다. 침입 정책에 이러한 규칙을 추가하면 정책을 무효화할 수 있습니다.

지정된 콘텐츠와 일치하지 않는 콘텐츠를 검색하려면 다음을 수행합니다.

단계 1 추가하는 `content` 또는 `protected_content` 키워드에 대해 **Not(아님)** 확인 상자를 선택합니다.

팁 동일한 `content` 키워드와 함께 **Use Fast Pattern Matcher(빠른 패턴 확인 매처 사용)** 확인 상자와 **Not(아님)** 확인 상자를 선택할 수 없습니다.

단계 2 규칙에 **Not(아님)** 옵션을 선택하지 않은 다른 `content` 또는 `protected_content` 키워드를 최소한 하나 포함합니다.

단계 3 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 콘텐츠 일치 제한, 23-15페이지의 콘텐츠 일치 검색, 23-101페이지의 새규칙 작성 또는 23-103페이지의 기존 규칙 변경을 참고하십시오.

위치 검색 옵션

라이센스: 보호

위치 검색 옵션을 사용하여 지정된 콘텐츠 검색을 시작할 위치 및 검색 범위를 지정할 수 있습니다. 각 옵션에 대한 자세한 내용은 다음을 참고하십시오,

- 23-20페이지의 수준
- 23-20페이지의 영역
- 23-21페이지의 길이
- 23-21페이지의 오프셋
- 23-21페이지의 내부

`content` 또는 `protected_content` 키워드 내의 위치 검색 옵션을 사용하는 방법에 관한 자세한 내용은 다음을 참고하십시오.

- 23-21페이지의 콘텐츠 키워드 내 검색 위치 옵션 사용
- 23-22페이지의 protected_content 키워드에서 검색 위치 옵션 사용

수준

참고 이 옵션은 `content` 키워드를 구성할 때**만** 지원됩니다. 자세한 내용은 23-15페이지의 콘텐츠 키워드 사용을 참고하십시오.

최대 콘텐츠 검색 수준을 오프셋 값의 시작부터 바이트 단위로 지정하거나 오프셋이 구성되어 있지 않은 경우 패킷 페이로드의 시작부터 지정합니다.

예를 들어, 콘텐츠 값 `cgi-bin/phf`와 `offset(오프셋)` 값 `3`, 그리고 `depth(수준)` 값 `22`를 가진 규칙에서, 해당 규칙은 3바이트에서 `cgi-bin/phf` 문자열 일치 검색을 시작하며, 규칙 헤더가 지정한 매개 변수를 충족하는 패킷에서 22바이트(25바이트)를 처리한 후 중지합니다.

최대 65535바이트의 지정된 콘텐츠의 길이와 같거나 큰 값을 지정해야 합니다. 값으로 0을 지정할 수 없습니다.

기본 수준은 패킷 끝까지 검색하는 것입니다.

영역

이전의 성공적인 콘텐츠 일치 후에 지정한 바이트 수가 나타나는 다음 콘텐츠 일치를 규칙 엔진이 확인하도록 지시합니다.

영역 카운터가 0바이트에서 시작하므로, 마지막 성공적인 콘텐츠 일치보다 앞으로 이동하기를 원하는 바이트 수보다 하나 적은 수를 지정합니다. 예를 들어, 4를 지정한 경우, 검색은 다섯 번째 바이트에서 시작됩니다.

-65535에서 65535까지 바이트 값을 지정할 수 있습니다. 마이너스 `Distance(영역)` 값을 지정한 경우, 사용자가 찾기 시작한 바이트가 패킷의 초기에 범위 밖으로 밀려날 수 있습니다. 검색은 패킷의 첫번째 바이트에서 시작하지만, 패킷 외부 바이트를 모두 고려합니다. 예를 들어 패킷

의 현재 위치가 다섯 번째 바이트인 경우, 그리고 다음 콘텐츠 규칙 옵션이 `Distance(영역)` 값 -10과 `Within(내부)` 값 20을 지정한 경우, 검색은 페이로드 초반에 시작하며 `Within(내부)` 옵션은 15로 조정됩니다.

기본값이 0인 것은 마지막 콘텐츠 일치 다음의 패킷 내 현재 위치를 의미합니다.

길이

참고 이 옵션은 `protected_content` 키워드를 구성할 때**만** 지원됩니다. 자세한 내용은 23-15페이지의 protected_content 키워드 사용을 참고하십시오.

Length(길이) `protected_content` 키워드 옵션은 해시되지 않은 검색 문자열의 길이를 바이트 단위로 나타냅니다.

예를 들어 보안 해시를 생성하기 위해 콘텐츠 `Sample1`을 사용한 경우, **Length(길이)** 값으로 `7`을 사용합니다. **반드시** 이 필드에 값을 입력해야 합니다.

오프셋

패킷 페이로드의 어느 위치에서 패킷 페이로드의 시작과 관련된 콘텐츠 검색을 시작할지 바이트 단위로 지정합니다. -65535에서 65535까지 값을 지정할 수 있습니다.

오프셋 카운터가 0바이트에서 시작하므로, 패킷 페이로드의 시작에서 앞으로 이동하기를 원하는 바이트 수보다 하나 적은 수를 지정합니다. 예를 들어, 7을 지정한 경우, 검색은 여덟 번째 바이트에서 시작됩니다.

기본 오프셋은 0으로, 패킷의 시작을 의미합니다.

내부

참고 이 옵션은 `content` 키워드를 구성할 때**만** 지원됩니다. 자세한 내용은 23-15페이지의 콘텐츠 키워드 사용을 참고하십시오.

Within(내부) 옵션은 규칙을 트리거하려면 다음 콘텐츠 일치가 마지막 콘텐츠 일치 종료 후 지정한 바이트 수 안에 발생해야 한다는 것을 나타냅니다. 예를 들어, **Within(내부)** 값 `8`을 지정한 경우, 다음 콘텐츠 일치는 패킷 페이로드의 다음 8바이트 안에서 발생하거나 규칙을 트리거하는 기준을 충족하지 않습니다.

최대 65535바이트의 지정된 콘텐츠의 길이와 같거나 큰 값을 지정할 수 있습니다.

Within(내부) 기본값은 패킷 끝까지 검색하는 것입니다.

콘텐츠 키워드 내 검색 위치 옵션 사용

두 개의 `content` 위치 쌍 중 하나를 사용하여 지정된 콘텐츠 검색을 시작할 위치 및 검색 범위를 다음과 같이 지정할 수 있습니다.

- **Offset(오프셋)** 및 **Depth(수준)**를 함께 사용하여 패킷 페이로드의 시작과 관련된 항목을 검색합니다.
- **Distance(영역)** 및 **Within(내부)**을 함께 사용하여 현재 검색 위치와 관련된 항목을 검색합니다.

한 쌍만 지정할 때, 쌍에서 다른 옵션의 기본값이 가정됩니다.

Offset(오프셋) 및 **Depth(수준)** 옵션을 **Distance(영역)** 및 **Within(내부)** 옵션과 함께 사용할 수 없습니다. 예를 들어, **Offset(오프셋)**과 **Within(내부)**을 페어링할 수 없습니다. 규칙에서 위치 옵션을 얼마든지 사용할 수 있습니다.

어떤 위치도 지정하지 않은 경우, **Offset(오프셋)** 및 **Depth(수준)**의 기본값이 가정됩니다. 즉, 패킷 페이로드가 시작될 때 콘텐츠 검색이 시작되며, 패킷이 종료될 때까지 계속됩니다.

기존의 byte_extract 변수를 사용하여 위치 옵션에 대한 값을 지정할 수 있습니다. 자세한 내용은 23-81페이지의 패킷 데이터를 키워드 인수로 읽어들이기를 참고하십시오.

콘텐츠 키워드에 검색 위치 값을 지정하려면 다음을 수행합니다.

단계 1 추가하려는 content 키워드 필드에 값을 입력합니다. 다음 옵션을 이용할 수 있습니다.

- **오프셋**
- **수준**
- **영역**
- **내부**

규칙에서 위치 옵션을 얼마든지 사용할 수 있습니다.

단계 2 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 23-17페이지의 콘텐츠 일치 제한, 23-15페이지의 콘텐츠 일치 검색, 23-101페이지의 새규칙 작성 또는 23-103페이지의 기존 규칙 변경을 참고하십시오.

protected_content 키워드에서 검색 위치 옵션 사용

다음과 같이 요구되는 **Length(길이)** protected_content 위치 옵션을 **Offset(오프셋)** 또는 **Distance(영역)** 위치 옵션과 함께 사용하여 지정된 콘텐츠 검색을 시작할 위치 및 검색 범위를 지정합니다.

- **Length(길이)**와 **Offset(오프셋)**을 함께 사용하여 패킷 페이로드의 시작과 관련된 보호된 문자열을 검색합니다.
- **Length(길이)**와 **Distance(영역)**를 함께 사용하여 현재 검색 위치와 관련된 보호된 문자열을 검색합니다.

팁 단일 키워드 구성에서 **Offset(오프셋)**과 **Distance(영역)** 옵션을 함께 사용할 수 없지만, 규칙에서 위치 옵션은 얼마든지 사용할 수 있습니다.

어떤 위치도 지정하지 않은 경우, 기본값이 가정됩니다. 즉, 패킷 페이로드가 시작될 때 콘텐츠 검색이 시작되며, 패킷이 종료될 때까지 계속됩니다.

기존의 byte_extract 변수를 사용하여 위치 옵션에 대한 값을 지정할 수 있습니다. 자세한 내용은 23-81페이지의 패킷 데이터를 키워드 인수로 읽어들이기를 참고하십시오.

보호된 콘텐츠 키워드에 검색 위치 값을 지정하려면 다음을 수행합니다.

단계 1 추가하려는 protected_content 키워드 필드에 값을 입력합니다. 다음 옵션을 이용할 수 있습니다.

- **길이**(필수)
- **오프셋**
- **영역**

단일 protected_content 키워드에서 **Offset(오프셋)**과 **Distance(영역)** 옵션을 함께 사용할 수 없지만, 규칙에서 위치 옵션은 얼마든지 사용할 수 있습니다.

단계 2 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 23-17페이지의 콘텐츠 일치 제한, 23-15페이지의 콘텐츠 일치 검색, 23-101페이지의 새규칙 작성 또는 23-103페이지의 기존 규칙 변경을 참고하십시오.

HTTP 콘텐츠 옵션

라이센스: 보호

HTTP `content` 또는 `protected_content` 키워드 옵션으로 인해 HTTP 검사 전처리기에서 디코딩된 HTTP 메시지 안에서 콘텐츠 일치를 검색할 위치를 지정할 수 있습니다.

두 가지 옵션은 HTTP 응답의 상태 필드를 검색합니다.

- **HTTP 상태 코드**
- **HTTP 상태 메시지**

규칙 엔진이 원시, 비정규 상태 필드를 검색하더라도 다른 원시 HTTP 필드 및 표준화된 HTTP 필드가 결합되면 이 옵션은 고려해야 할 제한 조건 하에서 설명을 간소화하기 위해 여기에 별도로 나열된다는 점에 유의하십시오.

다섯 가지 옵션은 적절한 수준에서 HTTP 요청, 응답, 또는 둘 다에서 표준화된 필드를 검색합니다(자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오).

- **HTTP URI**
- **HTTP 메서드**
- **HTTP 헤더**
- **HTTP 쿠키**
- **HTTP 클라이언트 본문**

세 가지 옵션은 적절한 수준에서 HTTP 요청, 응답, 또는 둘 다에서 원시(표준화되지 않은) 비상태 필드를 검색합니다(자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오).

- **HTTP 원시 URI**
- **HTTP 원시 헤더**
- **HTTP 원시 쿠키**

HTTP `content` 옵션을 선택할 때 다음 지침을 사용하십시오.

- HTTP `content` 옵션은 TCP 트래픽에만 적용됩니다.
- 성능에 부정적인 영향을 방지하려면, 지정된 내용이 표시될 수 있는 메시지의 해당 부분만 선택합니다.

  예를 들어, 쇼핑 카트 메시지에서처럼 트래픽이 규모가 큰 쿠키를 포함할 가능성이 높을 경우, HTTP 헤더에서 지정된 콘텐츠를 검색할 수 있지만 HTTP 쿠키에서는 검색할 수 없습니다.
- HTTP 검사 전처리기 표준화를 이용하고 성능을 향상시키려면, 사용자가 생성한 모든 HTTP 관련 규칙에 **HTTP URI**, **HTTP Method(HTTP 메서드)**, **HTTP Header(HTTP 헤더)** 또는 **HTTP Client Body(HTTP 클라이언트 본문)** 옵션이 선택된 최소한 하나의 `content` 또는 `protected_content` 키워드가 포함되어야 합니다.
- `replace` 키워드를 HTTP `content` 또는 `protected_content` 키워드 옵션과 함께 사용할 수 없습니다.

단일 표준화된 HTTP 옵션 또는 상태 필드를 지정하거나, 표준화된 HTTP 옵션 및 상태 필드를 어떤 조합에서나 사용하여 일치하는 콘텐츠 영역을 대상으로 할 수 있습니다. 그러나 HTTP 필드 옵션을 사용할 경우, 다음 제한 사항을 참고하십시오.

- **Raw Data(원시 데이터)** 옵션을 모든 HTTP 콘텐츠 옵션과 더불어 동일한 `content` 또는 `protected_content` 키워드 안에서 함께 사용할 수 없습니다.
- 동일한 `content` 또는 `protected_content` 키워드 내의 원시 HTTP 필드 옵션(**HTTP Raw URI(HTTP 원시 URI)**, **HTTP Raw Header(HTTP 원시 헤더)** 또는 **HTTP Raw Cookie(HTTP 원시 쿠키)**)을 표준화된 옵션(**HTTP URI**, **HTTP Header(HTTP 헤더)** 또는 **HTTP Cookie(HTTP 쿠키)** 순서대로)과 함께 사용할 수 없습니다.
- **Use Fast Pattern Matcher(빠른 패턴 매처 사용)**를 다음 HTTP 필드 옵션 중 하나 이상과 조합하여 선택할 수 없습니다.

  HTTP Raw URI(HTTP 원시 URI), **HTTP Raw Header(HTTP 원시 헤더)**, **HTTP Raw Cookie(HTTP 원시 쿠키)**, **HTTP Cookie(HTTP 쿠키)**, **HTTP Method(HTTP 메서드)**, **HTTP Status Message(HTTP 상태 메시지)** 또는 **HTTP Status Code(HTTP 상태 코드)**

  그러나, 빠른 패턴 매처 또한 사용하는 `content` 또는 `protected_content` 키워드에 상기 옵션을 포함하여 다음 표준화된 필드 중 하나를 검색할 수 있습니다.

  HTTP URI, **HTTP Header(HTTP 헤더)** 또는 **HTTP Client Body(HTTP 클라이언트 본문)**

  예를 들어, **HTTP Cookie(HTTP 쿠키)**, **HTTP 헤더(HTTP Header)**, 및 **Use Fast Pattern Matcher(빠른 패턴 매처 사용)**를 선택한 경우, 규칙 엔진은 HTTP 쿠키 및 HTTP 헤더 모두에서 콘텐츠를 검색하지만 빠른 패턴 매처는 HTTP 헤더에만 적용되고 HTTP 쿠키에는 적용되지 않습니다.
- 제한 옵션과 무제한 옵션을 결합할 때, 빠른 패턴 매처는 사용자가 지정하는 무제한 필드만을 검색하여 제한된 필드의 평가를 포함하는 전체 평가를 위한 규칙 편집기로 규칙을 전달할지 여부를 테스트합니다. 자세한 내용은 23-26페이지의 빠른 패턴 매처 사용을 참고하십시오.

위 제한 사항은 HTTP `content` 또는 `protected_content` 키워드 옵션을 설명하는 다음 목록에서 각 옵션의 설명에 반영됩니다.

HTTP URI

이 옵션을 선택하여 표준화된 요청 URI 필드에서 콘텐츠 일치를 검색합니다.

같은 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP URI (U) 옵션과 조합하여 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 Snort 특정 게시물 정규 표현식 수식자 표를 참고하십시오.

참고 파이프라인 방식 HTTP 요청 패킷은 여러 URI를 포함합니다. **HTTP URL**을 선택하여 규칙 엔진이 파이프라인 방식 HTTP 요청 패킷을 탐지하면, 규칙 엔진은 콘텐츠 일치를 위해 패킷 내 모든 URI를 검색합니다.

HTTP 원시 URI

이 옵션을 선택하여 표준화된 요청 URI 필드에서 콘텐츠 일치를 검색합니다.

같은 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP URI (U) 옵션과 조합하여 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 Snort 특정 게시물 정규 표현식 수식자 표를 참고하십시오.

참고 파이프라인 방식 HTTP 요청 패킷은 여러 URI를 포함합니다. **HTTP URL**을 선택하여 규칙 엔진이 파이프라인 방식 HTTP 요청 패킷을 탐지하면, 규칙 엔진은 콘텐츠 일치를 위해 패킷 내 모든 URI를 검색합니다.

HTTP 메서드

이 옵션을 선택하여 요청 메서드 필드에서 콘텐츠 일치를 검색하는데, 이는 URI에서 식별된 리소스를 사용하는 GET 및 POST와 같은 작업을 확인합니다.

HTTP 헤더

이 옵션을 선택하여 표준화된 헤더 필드의 콘텐츠 일치를 검색하는데, HTTP 요청에서는 쿠키를 제외합니다. 또한 HTTP 검사 전처리기 **Inspect HTTP Responses(HTTP 응답 검사)** 옵션이 활성화된 응답에서도 쿠키를 제외합니다.

동일한 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP 헤더 (H) 옵션과 조합하여 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 Snort 특정 게시물 정규 표현식 수식자 표를 참고하십시오.

HTTP 원시 헤더

이 옵션을 선택하여 원시 헤더 필드의 콘텐츠 일치를 검색하는데, HTTP 요청에서는 쿠키를 제외합니다. 또한 HTTP 검사 전처리기 **Inspect HTTP Responses(HTTP 응답 검사)** 옵션이 활성화된 응답에서도 쿠키를 제외합니다.

동일한 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP 원시 헤더(D) 옵션과 조합하여 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 Snort 특정 게시물 정규 표현식 수식자 표를 참고하십시오.

HTTP 쿠키

이 옵션을 선택하여 표준화된 HTTP 클라이언트 요청 헤더에서 식별된 모든 쿠키에서와 HTTP 검사 전처리기 **Inspect HTTP Responses(HTTP 응답 검사)** 옵션이 활성화된 경우의 set-cookie 응답 데이터에서 콘텐츠 일치를 검색합니다. 시스템이 본문 내용으로서의 메시지 본문에 포함되는 쿠키를 처리한다는 점에 유의하십시오.

반드시 HTTP 검사 전처리기 **Inspect HTTP Cookies(HTTP 쿠키 검사)** 옵션을 활성화하여 일치하는 쿠키만 검색해야 합니다. 그렇지 않을 경우, 규칙 엔진은 쿠키를 포함하는 전체 헤더를 검색합니다. 자세한 내용은 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택을 참고하십시오.

다음 사항을 참고하십시오.

- 동일한 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP 쿠키 (C) 옵션과 조합하여 사용할 수 없습니다. 자세한 내용은 Snort 특정 게시물 정규 표현식 수식자 표를 참고하십시오.
- `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스 및 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않습니다.

HTTP 원시 쿠키

이 옵션을 선택하여 원시 HTTP 클라이언트 요청 헤더에서 식별된 모든 쿠키에서와 HTTP 검사 전처리기 **Inspect HTTP Responses(HTTP 응답 검사)** 옵션이 활성화된 경우의 set-cookie 응답 데이터에서 콘텐츠 일치를 검색합니다. 시스템이 메시지 본문에 포함되는 쿠키를 본문 내용으로 처리한다는 점에 유의하십시오.

반드시 HTTP 검사 전처리기 **Inspect HTTP Cookies(HTTP 쿠키 검사)** 옵션을 활성화하여 일치하는 쿠키만 검색해야 합니다. 그렇지 않을 경우, 규칙 엔진은 쿠키를 포함하는 전체 헤더를 검색합니다. 자세한 내용은 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택을 참고하십시오.

다음 사항을 참고하십시오.

- 동일한 콘텐츠를 검색하기 위해 이 옵션을 `pcre` 키워드 HTTP 원시 쿠키 (K) 옵션과 조합하여 사용할 수 없습니다. 자세한 내용은 Snort 특정 게시물 정규 표현식 수식자 표를 참고하십시오.
- `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스 및 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않습니다.

HTTP 클라이언트 본문

이 옵션을 선택하여 HTTP 클라이언트 요청에서 메시지 본문의 콘텐츠 일치를 검색합니다.

이 옵션이 작동하도록 하려면, HTTP 검사 전처리기 **HTTP Client Body Extraction Depth(HTTP 클라이언트 본문 추출 수준)** 옵션에 대해 0에서 65535까지의 값을 지정해야 합니다. 자세한 내용은 15-34 페이지의 서버 수준 HTTP 표준화 옵션 선택을 참고하십시오.

HTTP 상태 코드

이 옵션을 선택하여 HTTP 응답에 세 자리로 된 상태 코드의 콘텐츠 일치를 검색합니다.

이 옵션이 일치를 되돌릴 수 있도록 HTTP 검사 전처리기 **Inspect HTTP Responses(HTTP 응답 검사)** 옵션을 활성화해야 합니다. 자세한 내용은 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택을 참고하십시오.

HTTP 상태 메시지

이 옵션을 선택하여 HTTP 응답의 상태 코드에 동반되는 본문 설명에서 콘텐츠 일치를 검색합니다.

이 옵션이 일치를 되돌릴 수 있도록 HTTP 검사 전처리기 **Inspect HTTP Responses(HTTP 응답 검사)** 옵션을 활성화해야 합니다. 자세한 내용은 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택을 참고하십시오.

TCP 트래픽의 콘텐츠를 검색할 때 HTTP 콘텐츠 옵션을 지정하려면 다음을 수행합니다.

단계 1 또는, HTTP 검사 전처리기 표준화를 이용하고 성능을 개선하기 위해 다음을 선택합니다.

- 추가하는 `content` 또는 `protected_content` 키워드에 대해 **HTTP URI**, **HTTP Raw URI(HTTP 원시 URI)**, **HTTP Method(HTTP 메서드)**, **HTTP Header(HTTP 헤더)**, **HTTP Raw Header(HTTP 원시 헤더)** 또는 **HTTP Client Body(HTTP 클라이언트 본문)** 옵션 중 하나 이상
- **HTTP Cookie(HTTP 쿠키)** 또는 **HTTP Raw Cookie(HTTP 원시 쿠키)** 옵션

단계 2 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 23-17페이지의 콘텐츠 일치 제한, 23-15페이지의 콘텐츠 일치 검색, 23-101페이지의 새규칙 작성 또는 23-103페이지의 기존 규칙 변경을 참고하십시오.

빠른 패턴 매처 사용

라이센스: 보호

참고 `protected_content` 키워드를 구성할 때 이 옵션은 지원되지 **않습니다**. 자세한 내용은 23-15페이지의 protected_content 키워드 사용을 참고하십시오.

빠른 패턴 매처는 패킷을 규칙 엔진에 전달하기 전에 평가할 규칙을 신속하게 결정합니다. 이 초기 결정은 패킷 평가에 사용되는 규칙의 수를 크게 줄여 성능을 개선합니다.

기본적으로, 빠른 패턴 매처는 규칙에 지정된 가장 긴 콘텐츠를 위한 패킷을 검색합니다. 이는 규칙의 필요 없는 평가를 최대한 제거하기 위한 것입니다. 다음의 예제 규칙 조각을 고려하십시오.

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

거의 모든 HTTP 클라이언트 요청은 GET 콘텐츠를 포함하지만, /exploit.cgi 콘텐츠를 포함하는 요청은 거의 없습니다. 빠른 패턴 콘텐츠로 GET을 사용하는 것은 대부분의 경우 규칙 엔진이 이 규칙을 평가하도록 하며 일치로 귀결되는 경우가 거의 없도록 합니다. 그러나, 대부분의 클라이언트 GET 요청은 /exploit.cgi를 사용하여 평가되지 않으므로 성능을 높입니다.

빠른 패턴 매처가 지정된 콘텐츠를 탐지하는 경우에만 규칙 엔진이 규칙에 대해 패킷을 평가합니다. 예를 들어, 규칙 내 하나의 content 키워드가 콘텐츠를 short로 지정하는데, 다른 키워드는 longer로 지정하고, 세 번째 키워드는 longest로 지정하는 경우, 빠른 패턴 매처는 longest 콘텐츠를 사용하며, 규칙 엔진이 페이로드에서 longest로 평가된 경우에만 규칙이 평가됩니다.

Use Fast Pattern Matcher(빠른 패턴 매처 사용) 옵션을 사용하여 빠른 패턴 매처가 사용하는 짧은 검색 패턴을 지정할 수 있습니다. 원칙적으로, 지정한 패턴은 패킷 내에서 발견될 가능성이 가장 긴 패턴보다 낮으므로 표적 공격을 더욱 구체적으로 식별합니다.

동일한 content 키워드에서 **Use Fast Pattern Matcher(빠른 패턴 매처 사용)** 옵션 및 다른 옵션을 선택할 때 다음 제한을 참고하시기 바랍니다.

- 규칙 당 한 번만 **Use Fast Pattern Matcher(빠른 패턴 매처 사용)**를 지정할 수 있습니다.
- **Use Fast Pattern Matcher(빠른 패턴 매처 사용)**를 **Not(아님)**과 함께 선택하는 경우 **Distance(영역)**, **Within(내부)**, **Offset(오프셋)** 또는 **Depth(수준)**를 사용할 수 없습니다.
- Use Fast Pattern Matcher(빠른 패턴 매처 사용)은 다음 HTTP 필드 옵션 중 어느 것과도 조합하여 선택할 수 없습니다.

  HTTP Raw URI(HTTP 원시 URI), **HTTP Raw Header(HTTP 원시 헤더)**, **HTTP Raw Cookie(HTTP 원시 쿠키)**, **HTTP Cookie(HTTP 쿠키)**, **HTTP Method(HTTP 메서드)**, **HTTP Status Message(HTTP 상태 메시지)** 또는 **HTTP Status Code(HTTP 상태 코드)**

  그러나, 빠른 패턴 매처 또한 사용하는 content 키워드에 상기 옵션을 포함하여 다음 표준화된 필드 중 하나를 검색할 수 있습니다.

  HTTP URI, **HTTP Header(HTTP 헤더)** 또는 **HTTP Client Body(HTTP 클라이언트 본문)**

  예를 들어, **HTTP Cookie(HTTP 쿠키)**, **HTTP 헤더(HTTP Header)**, 및 **Use Fast Pattern Matcher(빠른 패턴 매처 사용)**를 선택한 경우, 규칙 엔진은 HTTP 쿠키 및 HTTP 헤더 모두에서 콘텐츠를 검색하지만 빠른 패턴 매처는 HTTP 헤더에만 적용되고 HTTP 쿠키에는 적용되지 않습니다.

  동일한 content 키워드 내의 원시 HTTP 필드 옵션(**HTTP Raw URI(HTTP 원시 URI)**, **HTTP Raw Header(HTTP 원시 헤더)** 또는 **HTTP Raw Cookie(HTTP 원시 쿠키)**)을 표준화된 대응물(**HTTP URI**, **HTTP Header(HTTP 헤더)** 또는 **HTTP Cookie(HTTP 쿠키)**, 순서대로)와 함께 사용할 수 없다는 데 유의하십시오. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오.

  제한 옵션과 무제한 옵션을 결합할 때, 빠른 패턴 매처는 사용자가 지정하는 무제한 필드만을 검색하여 제한된 필드의 평가를 포함하는 전체 평가를 위한 규칙 엔진으로 패킷을 전달할지 여부를 테스트합니다.
- 선택적으로, **Use Fast Pattern Matcher(빠른 패턴 매처 사용)**를 선택하면, **Fast Pattern Matcher Only(빠른 패턴 매처 한정)** 또는 **Fast Pattern Matcher Offset and Length(빠른 패턴 매처 오프셋 및 길이)** 중 하나를 선택할 수 있지만 둘 다 선택할 수는 없습니다.
- Base64 데이터를 검사할 때는 빠른 패턴 매처를 사용할 수 없습니다. 자세한 내용은 23-99페이지의 Base64 데이터 디코딩 및 검사를 참고하십시오.

빠른 패턴 매처만 사용

Fast Pattern Matcher Only(빠른 패턴 매처 한정) 옵션을 사용하면 규칙 옵션이 아닌 빠른 패턴 매처 옵션으로만 content 키워드를 사용할 수 있습니다. 지정된 콘텐츠의 규칙 엔진 평가가 필요하지 않은 경우 이 옵션을 사용하여 리소스를 유지할 수 있습니다. 예를 들어, 콘텐츠 12345가 페이로드 안에서 어디든 있어야 한다고만 요구하는 규칙의 경우를 생각해 보십시오. 빠른 패턴 매처가 패턴을 탐지하면, 패킷이 규칙의 추가 키워드에 대해 평가될 수 있습니다. 패턴 12345를 포함하는지 확인하기 위해 패킷을 재평가하는 규칙 엔진은 없어도 됩니다.

규칙이 지정된 콘텐츠에 연결된 다른 조건을 포함할 때는 이 옵션을 사용하지 않습니다. 예를 들어 `1234` 전에 `abcd`가 발생하는지 여부를 다른 규칙 조건이 결정하고자 하는 경우, 콘텐츠 `1234`를 찾기 위해 이 옵션을 사용하지는 않을 것입니다. 이 경우, **Fast Pattern Matcher Only(빠른 패턴 매처 한정)**를 지정하면 규칙 엔진이 지정된 콘텐츠를 검색하지 않도록 지시하기 때문에 규칙 엔진은 상대적 위치를 결정할 수 없습니다.

이 옵션을 사용할 때 다음 사항에 유의하십시오:

- 지정된 내용은 위치와 무관합니다. 즉 페이로드 어디에서나 발생할 수 있습니다. 따라서, 위치의 옵션(**Distance(영역)**, **Within(내부)**, **Offset(오프셋)**, **Depth(수준)**, 또는 **Fast Pattern Matcher Offset and Length(빠른 패턴 매처 오프셋 및 길이)**)을 사용할 수 없습니다.
- 이 옵션을 **Not(아님)**과 조합하여 사용할 수 없습니다.
- 이 옵션을 **Fast Pattern Matcher Offset and Length(빠른 패턴 매처 오프셋 및 길이)**와 조합하여 사용할 수 없습니다.
- 모든 패턴이 대소문자를 구분하지 않는 방식으로 빠른 패턴 매처에 삽입되므로, 지정된 콘텐츠는 대소문자를 구분하지 않는 방식으로 처리될 것입니다. 이는 자동적으로 처리되므로, 이 옵션을 선택하면 **Case Insensitive(대소문자 구분 안 함)**를 선택할 필요가 없습니다.
- 사용자는 즉시 다음 키워드와 **Fast Pattern Matcher Only(빠른 패턴 매처 한정)** 옵션을 함께 사용하는 `content` 키워드를 따르지 말아야 하며, 이는 현재 검색 위치에 관련된 검색 위치를 설정하는 것입니다.
- `isdataat`
- `pcre`
- **Distance(영역)** 또는 **Within(내부)**를 선택한 경우 `content`
- **HTTP URI**를 선택한 경우 `content`
- `asn1`
- `byte_jump`
- `byte_test`
- `byte_extract`
- `base64_decode`

빠른 패턴 매처 오프셋 및 길이 지정

Fast Pattern Matcher Offset and Length(빠른 패턴 매처 오프셋 및 길이) 옵션을 사용하면 검색할 콘텐츠의 일부를 지정할 수 있습니다. 이는 패턴이 너무 길어 패턴의 일부만으로도 규칙을 가능한 일치로 확인하기에 충분한 경우 메모리 사용량을 줄일 수 있습니다. 규칙이 빠른 패턴 매처에서 선택되면, 규칙에 대해 전체 패턴이 평가됩니다.

다음 구문을 사용하여 검색을 시작할 위치(오프셋) 및 검색 범위(길이)를 바이트 단위로 지정함으로써 빠른 패턴 매처의 일부를 사용하기로 결정합니다.

```
offset,length
```

예를 들어, 다음과 같은 콘텐츠의 경우:

```
1234567
```

오프셋과 길이 바이트 수를 다음과 같이 지정할 경우:

```
1,5
```

빠른 패턴 매처가 콘텐츠 `23456`만 검색합니다.

이 옵션을 **Fast Pattern Matcher Only(빠른 패턴 매처 한정)**와 함께 사용할 수 없습니다.

빠른 패턴 매처에서 검토할 내용을 지정하려면 다음을 수행합니다.

단계 1 추가하려는 `content` 키워드에 대해 **Use Fast Pattern Matcher(빠른 패턴 매처 사용)**를 선택합니다.

단계 2 또는, 패킷에 지정된 패턴이 존재하는 경우 규칙 엔진 평가 없이 결정하려면 **Fast Pattern Matcher Only(빠른 패턴 매처 한정)**를 선택합니다.

평가는 빠른 패턴 매처가 지정된 콘텐츠를 탐지하는 경우에만 진행됩니다.

단계 3 또는, **Fast Pattern Matcher Offset and Length(빠른 패턴 매처 오프셋 및 길이)**에서 구문을 사용하여 콘텐츠를 검색하는 패턴의 일부를 지정합니다.

```
offset,length
```

*offset*은 콘텐츠의 시작부터 얼마나 많은 바이트가 검색을 시작하는지를 지정하고, *length*는 계속되는 바이트 수를 지정합니다.

단계 4 규칙 만들기 또는 수정을 계속합니다. 자세한 내용은 23-17페이지의 콘텐츠 일치 제한, 23-35페이지의 PCRE를 사용한 콘텐츠 검색, 23-101페이지의 새 규칙 작성 또는 23-103페이지의 기존 규칙 변경을 참고하십시오.

인라인 배포에서 콘텐츠 대체

라이센스: 보호

인라인 배포에서 대체하는 지정된 내용을 바꾸려면 `replace` 키워드를 사용할 수 있습니다.

`replace` 키워드를 사용하려면, 특수 문자열 검색을 위해 `content` 키워드를 사용하는 사용자 지정 표준 텍스트 규칙을 구성합니다. `replace` 키워드를 사용하여 콘텐츠를 대체할 문자열을 지정합니다. 대체 값 및 콘텐츠 값은 동일한 길이여야 합니다.

참고 `protected_content` 키워드 내 해시된 콘텐츠를 대체하기 위해 `replace` 키워드를 사용할 수 **없습니다**. 자세한 내용은 23-15페이지의 protected_content 키워드 사용을 참고하십시오.

또는, 이전 ASA FirePOWER 모듈 소프트웨어 버전과의 이전 버전 호환성에 대해 따옴표로 교체 문자열을 묶을 수 있습니다. 따옴표를 포함하지 않은 경우, 따옴표는 규칙에 자동으로 추가되므로 규칙은 구문적으로 정확합니다. 교체 텍스트의 일부로 앞 뒤 따옴표를 포함하려면, 다음의 예시에서 볼 수 있듯이, 백슬래시를 사용하여 이스케이프해야 합니다.

```
"replacement text plus \"quotation\" marks""
```

규칙은 여러 `replace` 키워드를 포함할 수 있지만, `content` 키워드 하나 당 하나만 포함됩니다. 규칙에서 찾은 콘텐츠의 첫 번째 인스턴스만 대체됩니다.

다음은 `replace` 키워드의 예제 용도를 설명합니다.

- 시스템이 공격을 포함한 수신 패킷을 탐지하는 경우, 악성 문자열을 무해한 것으로 바꿀 수 있습니다. 때때로 이 기술은 단순히 문제를 일으키는 패킷을 중단하는 것보다 더욱 성공적입니다. 일부 공격 시나리오에서, 공격자는 삭제된 패킷이 네트워크 방어를 무시하거나 네트워크를 초과할 때까지 다시 보냅니다. 패킷을 삭제하는 대신 다른 문자열로 한 문자열을 대체하여, 취약하지 않았던 대상에 대해 공격이 개시되었다고 공격자가 믿도록 속일 수 있습니다.
- 예를 들어, 취약한 버전의 웹 서버를 실행하고 있는지 여부를 알기 위해 시도하는 정찰 공격이 우려되는 경우, 발신 패킷을 탐지하고 본인의 텍스트로 배너를 바꿀 수 있습니다.

참고 대체 규칙을 사용하려는 인라인 침입 정책에서 규칙 상태를 Generate Events(이벤트 생성)로 설정했는지 확인합니다. 규칙을 Drop and Generate events(이벤트 중단 및 생성)로 설정하면 패킷이 중단될 수 있고, 이는 콘텐츠를 대체하는 것을 방지합니다.

문자열 교체 프로세스의 일부로서, 대상 호스트가 패킷을 오류 없이 받을 수 있도록 시스템은 자동으로 패킷 체크섬을 업데이트합니다.

`replace` 키워드를 HTTP 요청 메시지 `content` 키워드 옵션과 함께 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 23-15페이지의 콘텐츠 일치 검색 및 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오.

인라인 배포에서 콘텐츠를 대체하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **content(콘텐츠)**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`content` 키워드가 나타납니다.

단계 2 **content(콘텐츠)** 필드에 검색할 콘텐츠를 지정하고, 선택적으로, 모든 해당 인수를 선택합니다. HTTP 요청 메시지 `content` 키워드 옵션을 `replace` 키워드와 함께 사용할 수 없다는 점에 유의하십시오.

단계 3 드롭다운 목록에서 **replace(대체)**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`content` 키워드 아래에 `replace` 키워드가 나타납니다.

단계 4 **replace:(대체:)** 필드에서 지정한 내용에 대한 교체 문자열을 지정합니다.

Byte_Jump 및 Byte_Test 사용

라이센스: 보호

`byte_jump` 및 `byte_test`를 사용하여 규칙 엔진이 데이터 일치에 대한 테스트를 시작할 패킷의 위치와 평가할 바이트를 계산할 수 있습니다.

또한 `byte_jump` 및 `byte_test` **DCE/RPC** 인수를 사용하여 DCE/RPC 전처리기가 처리한 트래픽을 위한 키워드에 맞출 수 있습니다. **DCE/RPC** 인수를 사용할 때, 또한 `byte_jump` 및 `byte_test`를 다른 특정 DCE/RPC 키워드와 함께 사용할 수 있습니다. 자세한 내용은 15-2페이지의 DCE/RPC 트래픽 디코딩 및 23-58페이지의 DCE/RPC 키워드를 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-30페이지의 byte_jump
- 23-33페이지의 byte_test

byte_jump

라이센스: 보호

`byte_jump` 키워드는 지정된 바이트 세그먼트에서 정의된 바이트 수를 계산한 후 패킷 내 바이트 수를 건너뜁니다. 지정된 바이트 세그먼트의 끝에서부터 또는 패킷 페이로드의 시작으로부터 앞으로 움직이며, 이는 사용자가 지정하는 옵션에 따라 달라집니다. 이는 특정 세그먼트 바이트가 패킷 내 변수 데이터에 포함된 바이트 수를 설명하는 패킷에 유용합니다.

다음 표에서는 `byte_jump` 키워드에 필요한 인수에 대해 설명합니다.

표 23-8 필수 byte_jump 인수

인수	설명
Bytes	패킷에서 계산할 바이트 수.
Offset	처리를 시작할 페이로드에 들어가는 바이트 수. `offset` 카운터는 0바이트에서 시작하므로, 패킷 페이로드의 시작 또는 마지막으로 성공한 콘텐츠 일치로부터 계산에 넣기를 원하는 바이트 수에서 1을 빼 `offset` 값을 계산합니다. 기존의 `byte_extract` 변수를 사용하여 이 인수에 대한 값을 지정할 수 있습니다. 자세한 내용은 23-81페이지의 패킷 데이터를 키워드 인수로 읽어들이기를 참고하십시오.

다음 표에서는 시스템이 필수 인수에 지정한 값을 해석하는 방식을 정의하는 데 사용할 수 있는 옵션을 설명합니다.

표 23-9 추가 선택 byte_jump 인수

인수	설명
Relative	오프셋이 마지막으로 성공한 콘텐츠 일치에 포함된 마지막 패턴에 연결되도록 합니다.
Align	최대 다음 32비트 경계까지 변환한 바이트 수를 묶습니다.
Multiplier	마지막 `byte_jump` 값을 얻기 위해 규칙 엔진이 곱해야 하는, 패킷에서 얻어지는 `byte_jump` 값을 표시합니다. 즉 규칙 엔진은 지정된 바이트 세그먼트에서 정의한 바이트 수를 건너뛰는 대신, Multiplier 인수로 지정한 정수로 곱해진 바이트 수를 건너뜁니다.
Post Jump Offset	다른 `byte_jump` 인수를 적용한 후 앞 뒤로 건너뛰는 -63535에서 63535까지의 바이트 수. 양수 값은 앞으로 건너뛰고 음수 값은 뒤로 건너뜁니다. 필드를 비워 두거나 `0`을 입력하여 비활성화합니다. **DCE/RPC** 인수를 선택할 때 적용하지 않는 `byte_jump` 인수를 보려면 엔디언 기능 표에서 **DCE/RPC** 인수를 참고하십시오.
From Beginning(처음부터)	규칙 엔진이 건너뛸 바이트 수를 지정하는 바이트 세그먼트 끝이 아닌, 패킷 페이로드의 처음부터 시작하는 페이로드 내 지정된 바이트 수를 건너뛰어야 한다는 것을 표시합니다.

DCE/RPC, **Endian** 또는 **Number Type** 중 하나만 지정할 수 있습니다.

`byte_jump` 키워드가 바이트를 계산하는 방법을 정의하려는 경우, 다음 표에 설명된 인수 중에서 선택할 수 있습니다(인수를 지정하지 않는 경우, 네트워크 바이트 순서가 사용됩니다).

표 23-10 엔디언 기능

인수	설명
Big Endian	빅 엔디언 바이트 순서의 프로세스 데이터. 기본 네트워크 바이트 순서입니다.

표 23-10 엔디언 기능 (계속)

인수	설명
Little Endian	리틀 엔디언 순서의 프로세스 데이터
DCE/RPC	DCE/RPC 전처리기에서 처리된 트래픽에 byte_jump 키워드를 지정합니다. 자세한 내용은 15-2페이지의 DCE/RPC 트래픽 디코딩을 참고하십시오. DCE/RPC 전처리기는 빅 엔디언 또는 리틀 엔디언 바이트 순서를 결정하고, **Number Type**, **Endian**, **From Beginning** 인수는 적용되지 않습니다. 이 인수를 활성화하면, byte_jump를 다른 DCE/RPC 특정 키워드와 함께 사용할 수 있습니다. 자세한 내용은 23-58페이지의 DCE/RPC 키워드를 참고하십시오.

시스템이 다음 표에 있는 인수 중 하나를 사용하여 패킷 내 문자열을 보는 방식을 정의합니다.

표 23-11 번호 유형 인수

인수	설명
Hexadecimal String	변환된 문자열 데이터를 16진수 형태로 나타냅니다.
Decimal String	변환된 문자열 데이터를 십진수 형태로 나타냅니다.
Octal String	변환된 문자열 데이터를 8진수 형태로 나타냅니다.

예를 들어, 사용자가 byte_jump로 설정한 값이 다음과 같은 경우:

- Bytes = 4
- Offset = 12
- Relative 활성화
- Align 활성화

규칙 엔진은 마지막으로 성공한 콘텐츠 일치 후 13바이트를 나타내는 4개의 바이트로 표시된 수를 계산하고, 패킷 내 해당 수의 바이트를 건너뜁니다. 예를 들어, 특정 패킷 내 4개의 계산된 바이트가 00 00 00 1F인 경우, 규칙 엔진은 이를 31로 환산합니다. align이 지정되었으므로(엔진이 다음 32비트 경계로 움직이도록 지시함), 규칙 엔진은 패킷 내 32바이트를 건너뜁니다.

또는, 사용자가 byte_jump로 설정한 값이 다음과 같은 경우:

- Bytes = 4
- Offset = 12
- From Beginning 활성화
- Multiplier = 2

규칙 엔진은 패킷의 시작 후 13바이트를 나타내는 4개의 바이트로 표시된 수를 계산합니다. 다음, 엔진은 이 수에 2를 곱하여 건너뛸 총 바이트 수를 얻습니다. 예를 들어, 특정 패킷 내 4개의 계산된 바이트가 00 00 00 1F인 경우, 규칙 엔진은 이를 31로 환산한 후 2를 곱하여 62를 얻습니다. From Beginning이 활성화되어 있으므로, 규칙 엔진은 패킷의 처음 63바이트를 건너뜁니다.

byte_jump를 사용하려면 다음을 수행합니다.

단계 1 드롭다운 목록에서byte_jump를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.
선택한 마지막 키워드 아래에 byte_jump 섹션이 나타납니다.

byte_test

라이센스: 보호

byte_test 키워드는 지정된 바이트 세그먼트에서 바이트 수를 계산하고 연산자와 지정한 값에 따라 이들을 비교합니다.

다음 표에서는 byte_test 키워드에 필요한 인수에 대해 설명합니다.

표 23-12 필수 byte_test 인수

인수	설명
Bytes	패킷에서 계산할 바이트 수. 1 - 10 바이트를 지정할 수 있습니다.
Operator 및 Value	지정된 값을 <, >, =, !, &, ^, !>, !<, !=, !&, or !^와 비교합니다. 예를 들어, ! 1024, 를 지정한 경우, byte_test는 지정된 번호를 변환하며, 변환한 값이 1024와 같지 않은 경우, 이벤트를 생성합니다(모든 다른 키워드 매개 변수가 일치하는 경우). !와 !=는 같다는 점에 유의하십시오. 기존의 byte_extract 변수를 사용하여 이 인수에 대한 값을 지정할 수 있습니다. 자세한 내용은 23-81페이지의 패킷 데이터를 키워드 인수로 읽어들이기를 참고하십시오.
Offset	처리를 시작할 페이로드에 들어가는 바이트 수. offset 카운터는 0바이트에서 시작하므로, 패킷 페이로드의 시작 또는 마지막으로 성공한 콘텐츠 일치로부터 계산에 넣기를 원하는 바이트 수에서 1을 뺀 offset 값을 계산합니다. 기존의 byte_extract 변수를 사용하여 이 인수에 대한 값을 지정할 수 있습니다. 자세한 내용은 23-81페이지의 패킷 데이터를 키워드 인수로 읽어들이기를 참고하십시오.

시스템이 다음 표에 설명된 인수와 함께 byte_test 인수를 사용하는 방법을 더욱 자세히 정의할 수 있습니다.

표 23-13 추가 선택 byte_test 인수

인수	설명
Relative	오프셋이 마지막으로 성공한 패턴 일치와 연결되도록 합니다.
Align	최대 다음 32비트 경계까지 변환한 바이트 수를 묶습니다.

DCE/RPC, **Endian** 또는 **Number Type** 중 하나만 지정할 수 있습니다.

byte_test 키워드가 테스트할 바이트를 계산하는 방법을 정의하려면, 다음 표의 인수 중에서 선택합니다. 인수가 지정되지 않으면, 네트워크 바이트 순서가 사용됩니다.

표 23-14 엔디언 byte_test 인수

인수	설명
Big Endian	빅 엔디언 바이트 순서의 프로세스 데이터. 기본 네트워크 바이트 순서입니다.
Little Endian	리틀 엔디언 순서의 프로세스 데이터
DCE/RPC	DCE/RPC 전처리기에서 처리된 트래픽에 byte_test 키워드를 지정합니다. 자세한 내용은 15-2페이지의 DCE/RPC 트래픽 디코딩을 참고하십시오. DCE/RPC 전처리기는 빅 엔디언 또는 리틀 엔디언 바이트 순서를 결정하고, **Number Type(번호 유형)** 및 **Endian(엔디언)** 인수는 적용되지 않습니다. 이 인수를 활성화하면, byte_test를 다른 DCE/RPC 특정 키워드와 함께 사용할 수 있습니다. 자세한 내용은 23-58페이지의 DCE/RPC 키워드를 참고하십시오.

시스템이 다음 표에 있는 인수 중 하나를 사용하여 패킷 내 문자열 데이터를 보는 방식을 정의할 수 있습니다.

표 23-15 번호 유형 byte-test 인수

인수	설명
Hexadecimal String	변환된 문자열 데이터를 16진수 형태로 나타냅니다.
Decimal String	변환된 문자열 데이터를 십진수 형태로 나타냅니다.
Octal String	변환된 문자열 데이터를 8진수 형태로 나타냅니다.

예를 들어, byte_test에 대한 값이 다음과 같이 지정된 경우:

- Bytes = 4
- Operator 및 Value > 128
- Offset = 8
- Relative 활성화

규칙 엔진은 마지막으로 성공한 콘텐츠 일치와 떨어진(연결된) 9바이트를 나타내는 4개 바이트로 표시된 수를 계산합니다. 이 계산된 수가 128바이트보다 클 경우, 규칙이 트리거됩니다.

byte_test를 사용하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 byte_test를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

선택한 마지막 키워드 아래에 byte_test 섹션이 나타납니다.

PCRE를 사용한 콘텐츠 검색

라이센스: 보호

pcre 키워드를 사용하면 펄 호환 정규 표현식(PCRE)을 통해 특정 콘텐츠를 위해 패킷 페이로드를 검사할 수 있습니다. PCRE를 사용하여 동일한 콘텐츠의 약간의 차이에 따라 일치하는 여러 규칙을 작성하는 것을 방지할 수 있습니다.

정규 표현식은 다양한 방법으로 표시할 수 있는 콘텐츠를 검색할 때 유용합니다. 콘텐츠는 패킷의 페이로드에서 메시지를 찾는 시도에서 고려할 다른 특성을 가질 수 있습니다.

침입 규칙에서 사용되는 정규 표현식 구문은 전체 정규 표현식의 하위 집합이며, 전체 라이브러리의 지침에 사용되는 구문에서 어느 정도 변경된다는 점에 유의하십시오. 규칙 편집기를 사용하여 pcre 키워드를 추가할 경우, 전체 값을 다음 형식으로 입력합니다.

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

여기에서 각 항목은 다음을 나타냅니다.

- !는 선택적 무효화입니다(정규 표현식에 일치**하지 않는** 패턴에 일치시키기를 원할 때 이를 사용합니다).
- /*pcre*/는 펄 호환 정규 표현식입니다.
- ismxAEGRBUIPHDMCKSY 수식자 옵션의 모든 조합입니다.

패킷 페이로드에서 특정 콘텐츠를 검색하기 위해 PCRE에서 이들을 사용할 때 규칙 엔진이 정확하게 해석할 수 있도록 하려면 다음 표에 나열된 문자를 이스케이프해야 한다는 점에 유의하십시오.

표 23-16 이스케이프된 PCRE 문자

이스케이프 대상	백슬래시	헥사 코드
#(해시 부호)	\#	\x23
;(세미콜론)	\;	\x3B
|(세로 선)	\\|	\x7C
:(콜론)	\:	\x3A

팁 선택적으로, 인용 부호로 펄 호환 정규 표현식을 묶을 수 있습니다. 예를 들어, *pcre_expression* 또는 *"pcre_expression"*입니다. 따옴표 사용 옵션은 따옴표가 선택 대신 필수인 경우 이전 버전에 익숙한 기존 사용자에게 제공됩니다. 규칙 편집기는 보고서를 저장한 후 규칙을 표시할 때 따옴표를 표시하지 않습니다.

또한 /가 아닌 ?가 구분 문자일 때 m?regex?를 사용할 수 있습니다. 정규 표현식에서 슬래시와 일치해야 하는 상황에서 이를 사용하고자 할 수도 있지만 백슬래시로 이스케이프하지 않습니다. 예를 들어, *regex*가 펄 호환 정규 표현식이고 ismxAEGRBUIPHDMCKSY가 수식자 옵션의 모든 조합인 경우 m?*regex*? ismxAEGRBUIPHDMCKSY를 사용할 수 있습니다. 정규 표현식 구문에 대한 자세한 내용은 23-36페이지의 펄 호환 정규 표현식의 기본 사항을 참고하십시오.

다음 섹션에서는 pcre 키워드에 대해 유효한 값을 설정하는 데 대한 추가 정보를 제공합니다.

- 23-36페이지의 펄 호환 정규 표현식의 기본 사항은 펄 호환 정규 표현식에 사용되는 일반 구문을 설명합니다.
- 23-37페이지의 PCRE 수식자 옵션은 정규 표현식을 수정하는 데 사용할 수 있는 옵션을 설명합니다.
- 23-40페이지의 PCRE 키워드 값 예시는 규칙에 pcre 키워드를 사용하는 예를 제공합니다.

펄 호환 정규 표현식의 기본 사항

라이센스: 보호

pcre 키워드는 표준 펄 호환 정규 표현식(PCRE) 구문을 허용합니다. 다음 섹션에서는 각 구문에 대해 설명합니다.

팁 이 섹션은 PCRE에 사용할 수 있는 기본 구문을 설명하지만, 더 많은 고급 정보를 Perl(펄) 및 PCRE에 할애하는 온라인 참조 또는 도서를 참고할 수 있습니다.

메타 문자

라이센스: 보호

메타 문자는 정규 표현식에서 특정 의미가 있는 리터럴 문자입니다. 정규 표현식에서 이를 사용할 때, 이들 앞에 백슬래시를 두어 "이스케이프"해야 합니다.

다음 표에서는 PCRE에 사용할 수 있는 메타 문자를 설명하고 각각의 예를 제공합니다.

표 23-17 PCRE 메타 문자

메타 문자	설명	예
.	줄 바꿈을 제외한 모든 문자와 일치합니다. s가 수정 옵션으로 사용되는 경우, 이는 또한 줄 바꿈 문자를 포함합니다.	abc.는 abcd, abc1, abc# 등에 일치시킵니다.
*	0 이상의 문자 또는 표현이 나타나는 것에 일치시킵니다.	abc*는 abc, abcc, abccc, abcccccc 등에 일치시킵니다.
?	0 또는 하나의 문자/표현이 나타나는 것에 일치시킵니다.	abc?는 abc에 일치시킵니다.
+	하나 이상의 문자 또는 표현이 나타나는 것에 일치시킵니다.	abc+는 abc, abcc, abccc, abcccccc 등에 일치시킵니다.
()	표현을 그룹화합니다.	(abc)+는 abc, abcabc, abcabcabc 등에 일치시킵니다.
{}	문자 또는 표현에 일치하는 수에 대한 한계를 지정합니다. 상한 및 하한을 설정하고자 하는 경우, 쉼표로 상한 및 하한을 구분합니다.	a{4,6}은 aaaa, aaaaa 또는 aaaaaa에 일치시킵니다. (ab){2}는 abab에 일치시킵니다.
[]	문자 클래스를 정의하도록 허용하며, 집합에 설명된 문자의 조합 또는 모든 문자에 일치시킵니다.	[abc123]은 a 또는 b 또는 c 등에 일치시킵니다.
^	문자열의 시작 지점에 있는 콘텐츠에 일치시킵니다. 문자 클래스 내에서 사용되는 경우에도 무효화에 사용됩니다.	^in은 info 내 "in"에 일치하지만, bin에서는 일치하지 않습니다. [^a]은 a를 포함하지 않는 모든 문자열에 일치합니다.
$	문자열이 끝나는 지점에 있는 콘텐츠에 일치시킵니다.	ce$는 announce 내 "ce"에 일치하지만, cent에서는 일치하지 않습니다.
|	또는(OR) 표현을 나타냅니다.	(MAILTO|HELP)은 MAILTO 또는 HELP에 일치시킵니다.
\	메타 문자를 실제 문자로 사용할 수 있으며, 미리 정의된 문자 클래스를 지정하는 데 사용할 수도 있습니다.	\.는 기간에 일치하고, *는 별표에 일치하며, \\는 백슬래시에 일치합니다. \d는 숫자에 일치하며, \w는 영숫자에 일치합니다. PCRE의 문자 클래스 사용에 대한 자세한 내용은 23-37페이지의 문자 클래스를 참고하십시오.

문자 클래스

라이센스: 보호

문자 클래스는 알파벳 문자, 영숫자, 숫자 및 공백 문자를 포함합니다. 괄호 안에서 본인의 문자 클래스를 만들 수 있지만(23-36페이지의 메타 문자 참고), 다른 유형의 문자 유형에 대한 바로 가기로 사전 정의된 클래스를 사용할 수 있습니다. 추가 수식자 없이 사용할 경우, 문자 클래스는 한 자릿수 또는 문자와 일치됩니다.

다음 표에서는 PCRE가 수용한 사전 정의된 문자 클래스의 예를 설명하고 제공합니다.

표 23-18 PCRE 문자 클래스

문자 클래스	설명	문자 클래스 정의
\d	숫자 문자("디지트")에 일치합니다.	[0-9]
\D	숫자 문자가 아닌 모든 문자에 일치합니다.	[^0-9]
\w	영숫자 문자("단어")에 일치합니다.	[a-zA-Z0-9_]
\W	영숫자 문자가 아닌 모든 문자에 일치합니다.	[^a-zA-Z0-9_]
\s	공백, 복귀, 탭, 줄 바꿈 및 서식 이송을 포함하여 공백 문자에 일치시킵니다.	[\r\t\n\f]
\S	공백 문자가 아닌 모든 문자에 일치시킵니다.	[^ \r\t\n\f]

PCRE 수식자 옵션

라이센스: 보호

`pcre` 키워드 값의 정규 표현식 구문을 지정한 후 변경 옵션을 사용할 수 있습니다. 이 수식자는 Perl, PCRE 및 Snort에 특정한 처리 기능을 수행합니다. 수식자는 언제나 PCRE 값의 끝에 표시되며, 다음과 같은 형식으로 표시됩니다.

`/pcre/ismxAEGRBUIPHDMCKSY`

이 경우 `ismxAEGRBUPHMC`가 다음 표에 나타나는 모든 수정 옵션을 포함할 수 있습니다.

팁 또는, 정규 표현식 및 모든 수정 옵션을 따옴표로 둘러쌀 수 있습니다(예: `"/pcre/ismxAEGRBUIPHDMCKSY"`). 따옴표 사용 옵션은 따옴표가 선택 사항이 아닌 필수인 경우 이전 버전에 익숙한 기존 사용자에게 제공됩니다. 규칙 편집기는 보고서를 저장한 후 규칙을 표시할 때 따옴표를 표시하지 않습니다.

다음 표에서는 사용자가 Perl 처리 기능을 수행하는 데 사용할 수 있는 옵션을 설명합니다.

표 23-19 Perl 관련 게시물 정규 표현식 옵션

옵션	설명
i	정규 표현식에서 대소문자 구별이 없도록 합니다.
s	점 문자(.)는 줄 바꿈 또는 `\n` 문자를 제외한 모든 문자를 설명합니다. `"s"` 를 옵션으로 사용하여 이를 무시할 수 있으며, 점 문자가 줄 바꿈 문자를 포함한 모든 문자에 일치하도록 할 수 있습니다.
m	기본적으로, 문자열은 문자의 단선으로 처리되며, `^` 및 `$`는 특정 문자열의 시작 및 끝 지점에 일치됩니다. `"m"`을 옵션으로 사용할 때, `^` 및 `$`는 버퍼의 시작 또는 끝 부분뿐만 아니라 버퍼에서 모든 줄 바꿈 문자 바로 앞 또는 바로 뒤 콘텐츠에 일치시킵니다.
x	패턴에 나타날 수 있는 공백 데이터 문자를 무시합니다. 이스케이프 되었을 때(앞에 백슬래시가 있을 때) 또는 문자 클래스 안에 포함되었을 때는 제외합니다.

다음 표에서는 정규 표현식 뒤에 사용할 수 있는 PCRE 수식자를 설명합니다.

표 23-20 PCRE 관련 게시물 정규 표현식 옵션

옵션	설명
A	패턴은 문자열의 시작 지점과 일치해야 합니다(정규 표현식의 ^를 사용하는 것과 동일).
E	$가 제목 문자열 끝에만 일치하도록 설정합니다. (마지막 문자가 줄바꿈인 경우 E가 없는 $는 또한 마지막 문자 바로 앞에 일치하지만 다른 모든 줄바꿈 문자 앞에서는 일치하지 않습니다).
G	기본적으로, * + 및 ?는 "최대값에 일치"시킵니다. 이는 두 개 이상의 일치가 발견되는 경우, 가장 긴 일치 항목을 선택한다는 것을 의미합니다. 이를 변경하려면 G 문자를 사용하며, 이는 그 뒤에 물음표 문자(?)가 나오지 않는 한 이 문자들이 항상 첫 번째 일치 항목을 선택하도록 하기 위한 것입니다. 예를 들면 *? +? 및 ??는 G 수식자를 사용하는 구조에서 최대값에 일치시킵니다. 그리고 추가적인 물음표가 없는 *, + 또는 ?의 모든 예는 최대값에 일치시키지 않습니다.

다음 표에서는 정규 표현식 뒤에 사용할 수 있는 Snort 특정 수식자를 설명합니다.

표 23-21 Snort 특정 게시물 정규 표현식 수식자

옵션	설명
R	규칙 엔진으로 발견된 마지막 일치 끝부분과 관련된 일치하는 콘텐츠를 검색합니다.
B	전처리기에서 해독하기 전에 데이터 내의 내용을 검색합니다(이 옵션은 Raw Data 인수와 content 또는 protected_content 키워드를 함께 사용하는 것과 유사합니다).
U	HTTP 검사 전처리기에서 해독된 표준화된 HTTP 요청 메시지에 대해 URI 내의 콘텐츠를 검색합니다. 같은 콘텐츠를 검색하기 위해 이 옵션을 content 또는 protected_content 키워드 **HTTP URI** 옵션과 함께 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오. **참고** 파이프라인 방식 HTTP 요청 패킷은 여러 URI를 포함합니다. U 옵션을 포함하는 PCRE 표현은 규칙 엔진이 파이프라인 방식 HTTP 요청 패킷의 첫 URI에서만 콘텐츠 일치를 검색하도록 합니다. 패킷의 모든 URI를 검색하려면, content 또는 protected_content 키워드에 **HTTP URI** 옵션을 선택하여 사용하는데, U 옵션을 사용하는 PCRE 표현을 동반하거나 동반하지 않습니다.
I	HTTP 검사 전처리기에서 해독된 원시 HTTP 요청 메시지에 대해 URI 내의 콘텐츠를 검색합니다. 같은 콘텐츠를 검색하기 위해 이 옵션을 content 또는 protected_content 키워드 **HTTP Raw URI(HTTP 원시 URI)** 옵션과 조합하여 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오.
P	HTTP 검사 전처리기에서 해독된 표준화된 HTTP 요청 메시지에 대해 본문 내의 콘텐츠를 검색합니다. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션의 content 또는 protected_content 키워드 **HTTP Client Body(HTTP 클라이언트 본문)** 옵션을 참고하십시오.
H	HTTP 검사 전처리기에서 해독된 HTTP 요청 또는 응답 메시지의 헤더 내 콘텐츠를 검색합니다. 쿠키는 제외합니다. 같은 콘텐츠를 검색하기 위해 이 옵션을 content 또는 protected_content 키워드 **HTTP Header(HTTP 헤더)** 옵션과 함께 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오.
D	HTTP 검사 전처리기에서 해독된 원시 HTTP 요청 또는 응답 메시지의 헤더 내 콘텐츠를 검색합니다. 쿠키는 제외합니다. 같은 콘텐츠를 검색하기 위해 이 옵션을 content 또는 protected_content 키워드 **HTTP Header(HTTP 헤더)** 옵션과 조합하여 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오.

표 23-21 Snort 특정 게시물 정규 표현식 수식자 (계속)

옵션	설명
M	HTTP 검사 전처리기에서 해독된 표준화된 HTTP 요청 메시지의 메서드 필드에서 콘텐츠를 검색합니다. 메서드 필드는 URI에서 식별된 리소스를 만들기 위해 GET, PUT, CONNECT 등의 작업을 식별합니다. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션의 `content` 또는 `protected_content` 키워드 **HTTP Method(HTTP 메서드)** 옵션을 참고하십시오.
C	HTTP 검사 전처리기 **Inspect HTTP Cookies(HTTP 쿠키 검사)** 옵션이 활성화되면 HTTP 요청 헤더의 모든 쿠키 내 표준화된 콘텐츠를 검색합니다. 전처리기 **Inspect HTTP Responses(HTTP 응답 검사)** 옵션이 활성화되면 HTTP 응답 헤더의 모든 set-cookie 내 표준화된 콘텐츠도 검색합니다. **Inspect HTTP Cookies(HTTP 쿠키 검사)**가 활성화되지 않은 경우, 쿠키 또는 set-cookie 데이터를 포함한 전체 헤더를 검색합니다. 다음 사항을 참고하십시오. • 메시지 본문에 포함된 쿠키는 본문 콘텐츠로 처리됩니다. • 같은 콘텐츠를 검색하기 위해 이 옵션을 `content` 또는 `protected_content` 키워드 **HTTP Cookie(HTTP 쿠키)** 옵션과 함께 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오. • `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스 및 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않습니다.
K	HTTP 검사 전처리기 **Inspect HTTP Cookies(HTTP 쿠키 검사)** 옵션이 활성화되면 HTTP 요청 헤더의 모든 쿠키 내의 원시 콘텐츠를 검색합니다. 전처리기 **Inspect HTTP Responses(HTTP 응답 검사)** 옵션이 활성화되면 HTTP 응답 헤더의 모든 set-cookie 내 표준화된 콘텐츠를 검색합니다. **Inspect HTTP Cookies(HTTP 쿠키 검사)**가 활성화되지 않은 경우, 쿠키 또는 set-cookie 데이터를 포함한 전체 헤더를 검색합니다. 다음 사항을 참고하십시오. • 메시지 본문에 포함된 쿠키는 본문 콘텐츠로 처리됩니다. • 같은 콘텐츠를 검색하기 위해 이 옵션을 `content` 또는 `protected_content` 키워드 **HTTP Raw Cookie(HTTP 원시 쿠키)** 옵션과 함께 사용할 수 없다는 점에 유의하십시오. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오. • `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 행의 주요 스페이스 및 헤더 행을 종료하는 `CRLF`는 헤더의 일부로 검사되지만 쿠키의 일부로는 검사되지 않습니다.
S	HTTP 응답에서 3자릿수 상태 코드를 검색합니다. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션의 `content` 또는 `protected_content` 키워드 **HTTP Status Code(HTTP 상태 코드)** 옵션을 참고하십시오.
Y	HTTP 응답의 상태 코드를 동반하는 텍스트 설명을 검색합니다. 자세한 내용은 23-23페이지의 HTTP 콘텐츠 옵션의 `content` 또는 `protected_content` 키워드 **HTTP Status Message(HTTP 상태 메시지)** 옵션을 참고하십시오.

참고 U 옵션을 R 옵션과 함께 사용하지 마십시오. 이는 성능 문제를 야기할 수 있습니다. 또한, U 옵션을 다른 HTTP 콘텐츠 옵션(I, P, H, D, M, C, K, S, 또는 Y)과 함께 사용하지 마십시오.

PCRE 키워드 값 예시

라이센스: 보호

다음의 예시는 일치하는 각 예의 설명과 함께 pcre에 입력할 수 있는 값을 보여줍니다.

- **/feedback[(\d{0,1})]?\.cgi/U**

  이 예는 feedback 뒤에 0 또는 1개의 숫자 문자와 .cgi가 차례로 나오며 URI 데이터에만 위치하는 feedback에 대한 패킷 페이로드를 검색합니다.

  이 예는 다음에 일치됩니다.

- feedback.cgi
- feedback1.cgi
- feedback2.cgi
- feedback3.cgi

  이 예는 다음과 일치되지 **않습니다**.

- feedbacka.cgi
- feedback11.cgi
- feedback21.cgi
- feedbackzb.cgi
- **/^ez(\w{3,5})\.cgi/iU**

  이 예는 문자열의 시작 지점에 위치하며, 그 뒤에 3-5개의 문자와 .cgi가 차례로 나오는 ez에 대한 패킷 페이로드를 검색합니다. 검색은 대소문자 구분을 하지 않으며 URI 데이터에만 위치합니다.

  이 예는 다음에 일치됩니다.

- EZBoard.cgi
- ezman.cgi
- ezadmin.cgi
- EZAdmin.cgi

  이 예는 다음과 일치되지 **않습니다**.

- ezez.cgi
- fez.cgi
- abcezboard.cgi
- ezboardman.cgi
- **/mail(file|seek)\.cgi/U**

  이 예는 mail 뒤에 file 또는 seek가 나오며 URI 데이터에 있는 mail에 대한 패킷 페이로드를 검색합니다.

  이 예는 다음에 일치됩니다.

- mailfile.cgi
- mailseek.cgi

  이 예는 다음과 일치되지 **않습니다**.

- MailFile.cgi
- mailfilefile.cgi
- **m?http\\x3a\x2f\x2f.*(\n|\t)+?U**

  이 예는 HTTP 요청의 탭 또는 줄 바꿈 문자에 대한 URI 콘텐츠의 패킷 페이로드를 검색하며, 어떤 수의 문자가 앞에 와도 됩니다. 이 예는 m?*regex*?를 사용하여 표현식에서 http\:\/\/를 사용하는 것을 방지합니다. 콜론은 백슬래시 앞에 위치한다는 점을 참고하십시오.

이 예는 다음에 일치됩니다.

- `http://www.example.com?scriptvar=x&othervar=\n\..\..`
- `http://www.example.com?scriptvar=\t`

이 예는 다음과 일치되지 **않습니다**.

- `ftp://ftp.example.com?scriptvar=&othervar=\n\..\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`
- **`m?http\\x3a\x2f\x2f.*=\|.*\|+?sU`**

이 예에서는 등호 및 모든 수의 문자를 포함하는 파이프 문자 또는 공백이 뒤따르는 줄 바꿈을 포함하는 모든 문자 수와 함께 URL에 대한 패킷 페이로드를 검색합니다. 이 예는 `m?`*`regex`*`?`를 사용하여 표현식에서 `http\:\/\/`를 사용하는 것을 방지합니다.

이 예는 다음에 일치됩니다.

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

이 예는 다음과 일치되지 **않습니다**.

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- **`/[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i`**

이 예는 MAC 주소에 대한 패킷 페이로드를 검색합니다. 백슬래시로 콜론 문자를 이스케이프한다는 점에 유의하십시오.

규칙에 메타데이터 추가

라이센스: 보호

`metadata` 키워드를 사용하여 규칙에 설명 정보를 추가할 수 있습니다. 추가한 정보를 사용하여 필요에 맞춘 방법으로 규칙을 구성하거나 확인하고, 검색할 수 있습니다.

시스템이 형식에 따라 메타데이터를 확인합니다.

```
key value
```

*key*와 *value*가 스페이스로 구분된 결합 설명을 제공합니다. 이는 Cisco가 제공한 규칙에 메타데이터를 추가하기 위해 CiscoVRT가 사용하는 형식입니다.

또는, 다음 형식을 사용할 수 있습니다.

```
key=value
```

예를 들어, *key value* 형식을 사용하여 다음과 같은 카테고리 및 하위 카테고리로 작성자 및 날짜별로 규칙을 확인할 수 있습니다.

```
author SnortGuru_20050406
```

규칙에서 여러 `metadata` 키워드를 사용할 수 있습니다. 다음의 예시에 표시된 대로 쉼표를 사용하여 단일 `metadata` 키워드에서 여러 *key value* 문을 구분할 수 있습니다.

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003, revised_by
SnortUser1_20070123
```

key value 또는 *key=value* 형식을 사용하는 데 대한 제한은 없습니다. 하지만, 이 형식에 기반한 확인의 결과로 파생되는 제한에 유의해야 합니다.

제한된 문자 방지

라이센스: 보호

다음과 같은 문자 제한 사항을 참고하십시오.

- `metadata` 키워드에 세미콜론(;) 또는 콜론(:)을 사용하지 마십시오.
- 쉼표를 사용할 때는 시스템이 쉼표를 여러 *key value* 또는 *key=value* 문장을 위한 구분자로 해석한다는 점에 유의하십시오. 예를 들면 다음과 같습니다.

```
key value, key value, key value
```

- 등호(=) 문자 또는 공백 문자를 사용할 때는 시스템이 이 문자를 *key*와 *value* 사이를 나누는 구분자로 해석한다는 점에 유의하십시오. 예를 들면 다음과 같습니다.

```
key value
key=value
```

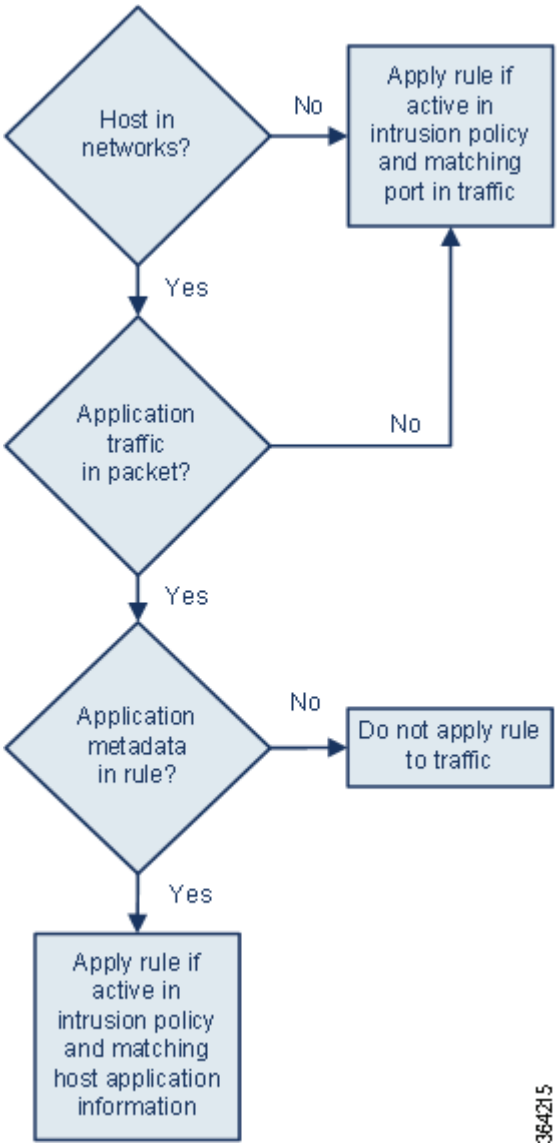
다른 모든 문자는 허용됩니다.

서비스 메타데이터 추가

라이센스: 보호

규칙 엔진은 트래픽을 분석하고 처리하기 위해 패킷 내 호스트의 애플리케이션 프로토콜 정보와 일치하는 `service(서비스)` 메타데이터와 함께 활성 규칙을 적용합니다. 일치하지 않을 경우, 시스템은 트래픽에 규칙을 적용하지 않습니다. 호스트에 애플리케이션 프로토콜 정보가 없거나, 규칙에 `service(서비스)` 메타데이터가 없는 경우, 시스템은 트래픽에 규칙을 적용할지 여부를 결정하기 위해 규칙 내 포트에 대해 트래픽 내 포트를 확인합니다.

다음 다이어그램은 애플리케이션 정보에 따라 트래픽에 규칙을 일치시키는 것을 설명합니다.



규칙을 식별된 애플리케이션 프로토콜에 일치시키려면, `metadata` 키워드 및 *`key value`* 문, `service`(*`key`*) 그리고 *`value`*를 위한 애플리케이션을 정의해야 합니다. 예를 들어, 다음 `metadata` 키워드 안의 *`key value`* 문장은 HTTP 트래픽과 규칙을 연결합니다.

```
service http
```

다음 표에서는 일반적인 애플리케이션 값을 나타냅니다.

참고 표에 없는 애플리케이션 정의에 도움을 받으려면 Support(지원부)에 연락하십시오.

표 23-22 서비스 값

값	설명
`dcerpc`	분산 컴퓨팅 환경/원격 절차 호출 시스템
`dns`	Domain Name System

표 23-22 서비스 값 (계속)

값	설명
finger	핑거 사용자 정보 프로토콜
ftp	파일 전송 프로토콜
ftp-data	파일 전송 프로토콜(데이터 채널)
HTTP	Hypertext Transfer Protocol
imap	Internet Message Access Protocol
isakmp	Internet Security Association and Key Management Protocol
netbios-dgm	NETBIOS 데이터그램 서비스
netbios-ns	NETBIOS 이름 서비스
netbios-ssn	NETBIOS 세션 서비스
nntp	Network News Transfer Protocol
oracle	Oracle Net Services
pop2	포스트 오피스 프로토콜, 버전 2
POP3	포스트 오피스 프로토콜, 버전 3
smtp	간단한 메일 전송 프로토콜
ssh	Secure Shell 네트워크 프로토콜
telnet	텔넷 네트워크 프로토콜
tftp	Trivial File Transfer Protocol
x11	X 윈도우 시스템

예약된 메타데이터 방지

라이센스: 보호

다음 단어를 `metadata` 키워드 안에 사용하지 마십시오. 단일 인수 또는 *`key value`* 문 내 키로도 사용하지 마십시오. 이들은 VRT 사용을 위해 남겨두어야 합니다.

```
application
engine
impact_flag
os
policy
rule-type
rule-flushing
soid
```

참고 예상과 다르게 기능했을 수도 있는 로컬 규칙에 제한된 메타데이터를 추가하는 것에 관한 도움을 받으려면 Support(지원부)에 연락하십시오. 자세한 내용은 35-15페이지의 로컬 규칙 파일 가져오기를 참고하십시오.

IP 헤더 값 검사

라이센스: 보호

키워드를 사용하여 패킷의 IP 헤더 내 가능한 공격 또는 보안 정책 위반을 식별할 수 있습니다. 자세한 내용은 다음 섹션을 참고하십시오.

조각 및 예약 비트 검사

라이센스: 보호

`fragbits` 키워드는 IP 헤더의 단편 및 예약 비트를 검사합니다. Reserved Bit(예약 비트), More Fragments bit(추가 단편 비트)에서 각 패킷을 확인할 수 있으며, 어떤 조합에서나 Don't Fragment bit(단편화 금지 비트)를 확인할 수 있습니다.

표 23-23 단편 비트 인수 값

인수	설명
R	예약 비트
M	추가 단편 비트
D	단편화 금지 비트

`fragbits` 키워드를 사용하여 규칙을 개선하기 위해 규칙에서 인수 값 다음에 다음 표에 설명된 모든 연산자를 지정할 수 있습니다.

표 23-24 단편 비트 연산자

연산자	설명
더하기 기호(`+`)	패킷은 모든 지정된 비트와 일치해야 합니다.
별표(`*`)	패킷은 모든 지정된 비트에 일치할 수 있습니다.
느낌표(`!`)	지정된 비트가 하나도 설정되지 않은 경우 패킷은 기준을 충족합니다.

예를 들어, 설정된 Reserved Bit(예약 비트) (및 가능한 다른 모든 비트)가 있는 패킷에 대한 이벤트를 생성하려면, `fragbits` 값으로 `R+`를 사용합니다.

IP 헤더 ID 값 검사

라이센스: 보호

ID 키워드는 키워드의 인수에 지정된 값에 대한 IP 헤더 단편 ID 필드를 테스트합니다. 일부 서비스 거부 공격(DoS) 도구 및 스캐너는 이 필드에 탐지하기 쉬운 특정 숫자를 설정합니다. 예를 들어, Synscan 포트 스캔을 탐지하는 SID 630에서는 ID 값이 스캐너에서 전송하는 패킷에 ID 번호로 사용된 정적 값 39426으로 설정됩니다.

참고 ID의 값은 숫자여야 합니다.

지정된 IP 옵션 식별

라이센스: 보호

IPopts 키워드를 사용하면 지정된 IP 헤더 옵션을 위한 패킷을 검색할 수 있습니다. 다음 표에는 사용 가능한 인수 값이 나열되어 있습니다.

표 23-25 IPoption 인수

인수	설명
rr	레코드 경로
eol	목록 끝
nop	무연산
ts	타임 스탬프
초	IP 보안 옵션
lsrr	느슨한 소스 라우팅
ssrr	엄격한 소스 라우팅
satid	스트림 식별자

분석가가 가장 자주 살펴보는 것은 엄격한 소스 라우팅과 느슨한 소스 라우팅입니다. 그 이유는 이 옵션이 도용된 소스 IP 주소를 나타낼 수 있기 때문입니다.

지정된 IP 프로토콜 번호 식별

라이센스: 보호

ip_proto 키워드를 사용하면 키워드 값으로 지정된 IP 프로토콜을 통해 패킷을 식별할 수 있습니다. 0에서 255까지의 번호로 IP 프로토콜을 지정할 수 있습니다.
http://www.iana.org/assignments/protocol-numbers에서 프로토콜 번호의 전체 목록을 찾을 수 있습니다. 이 번호를 <, >, 또는 ! .연산자와 결합할 수 있습니다. 예를 들어, ICMP가 아닌 모든 프로토콜을 통해 트래픽을 검사하려면, ip_proto 키워드에 대한 값으로 !1을 사용합니다. 또한 단일 규칙에서 ip_proto 키워드를 여러 번 사용할 수 있습니다. 하지만, 규칙 엔진은 키워드의 여러 인스턴스를 Boolean AND 관계를 갖는 것으로 해석한다는 점에 유의하십시오. 예를 들어, ip_proto:!3; ip_proto:!6을 포함하는 규칙을 생성하는 경우, 규칙은 GGP 프로토콜 및 TCP 프로토콜을 사용하는 트래픽을 무시합니다.

패킷의 서비스 유형 검사

라이센스: 보호

일부 네트워크는 서비스 유형(ToS) 값을 사용하여 네트워크로 이동하는 패킷의 우선 순위를 설정합니다. `tos` 키워드는 키워드의 인수로 지정한 값에 대한 패킷의 IP 헤더 ToS 값을 테스트합니다. `tos` 키워드를 사용하는 규칙은 해당 ToS가 특정 값으로 설정된 패킷과 규칙에서 제시된 기준의 나머지 부분을 충족하는 패킷에서 트리거됩니다.

참고 `tos`의 인수 값은 숫자여야 합니다.

ToS 필드는 IP 헤더 프로토콜에서 더 이상 사용되지 않으며 DSCP(Differentiated Services Code Point) 필드로 대체되었습니다.

패킷의 TTL(Time-To-Live) 값 검사

라이센스: 보호

패킷의 ttl(time-to-live) 값은 중단되기 전에 얼마나 많은 홉을 만들 수 있는지를 나타냅니다. `ttl` 키워드를 사용하여 키워드의 인수로 지정한 값 또는 값 범위에 대한 패킷의 IP 헤더 ttl 값을 테스트할 수 있습니다. 낮은 TTL 값은 때로 traceroute 또는 침입 회피 시도를 표시하므로 `ttl` 키워드 매개 변수를 0이나 1과 같은 낮은 값으로 설정하는 것이 도움이 될 수 있습니다. (하지만 이 키워드에 대한 적절한 값은 디바이스 배치 및 네트워크 토폴로지에 따라 다르다는 점을 참고하십시오.) 다음과 같이 구문을 사용합니다.

- 0에서 255 사이의 정수를 사용하여 TTL 값으로 특정 값을 설정합니다. 또한 등호(=)로 값을 입력할 수 있습니다(예를 들어 `5` 또는 `=5`를 지정할 수 있습니다).
- 하이픈(-)을 사용하여 TTL 값의 범위를 지정합니다(예를 들어, `0-2` 는 0에서 2까지의 모든 값을, `-5`는 0에서 5까지의 모든 값을, 그리고 `5-`는 5에서 255까지의 모든 값을 지정합니다).
- 부등호(>)를 사용하여 특정 값보다 큰 TTL 값을 지정합니다(예를 들어, `>3`은 3보다 큰 모든 값을 지정합니다).
- 크거나 같음 기호(>=)를 사용하여 특정 값보다 크거나 같은 TTL 값을 지정합니다(예를 들어, `>=3`은 3보다 크거나 같은 모든 값을 지정합니다).
- 부등호(<)를 사용하여 특정 값보다 작은 TTL 값을 지정합니다(예를 들어, `<3`은 3보다 작은 모든 값을 지정합니다).
- 작거나 같음 기호(<=)를 사용하여 특정 값보다 작거나 같은 TTL 값을 지정합니다(예를 들어, `<=3`은 3보다 작거나 같은 모든 값을 지정합니다).

ICMP 헤더 값 검사

라이센스: 보호

ASA FirePOWER 모듈은 ICMP 패킷의 헤더에 있는 공격 및 보안 정책 위반을 식별하는 데 사용할 수 있는 키워드를 지원합니다. 하지만 대부분의 ICMP 유형 및 코드를 탐지하는 사전 정의된 규칙이 존재한다는 점을 참고하십시오. 기존 규칙을 활성화하거나 기존 규칙에 기반한 로컬 규칙을 생성하는 것을 고려하십시오. ICMP 규칙을 처음부터 구축하면 요구를 충족시키는 규칙을 더욱 신속하게 찾을 수 있습니다.

ICMP 특정 키워드에 대한 자세한 내용은 다음 섹션을 참고하십시오.

- 23-48페이지의 정적 ICMP ID 및 시퀀스 값 식별
- 23-48페이지의 ICMP 메시지 유형 검사
- 23-48페이지의 ICMP 메시지 코드 검사

정적 ICMP ID 및 시퀀스 값 식별

라이센스: 보호

ICMP ID 및 시퀀스 번호는 ICMP 응답과 ICMP 요구를 연결하는 데 도움이 됩니다. 일반적인 트래픽에서 이 값은 패킷에 동적으로 할당됩니다. 일부 은닉 채널 및 분산서비스거부(DDoS) 프로그램은 정적 ICMP ID 및 시퀀스 값을 사용합니다. 다음 키워드를 사용하면 정적 값으로 ICMP 패킷을 확인할 수 있습니다.

icmp_id

`icmp_id` 키워드는 ICMP 에코 요청 또는 회신 패킷의 ICMP ID 번호를 검사합니다. `icmp_id` 키워드에 대한 인수로 ICMP ID 번호에 해당하는 숫자를 사용합니다.

icmp_seq

`icmp_seq` 키워드는 ICMP 에코 요청 또는 회신 패킷의 ICMP 시퀀스를 검사합니다. `icmp_seq` 키워드에 대한 인수로 ICMP 시퀀스 번호에 해당하는 숫자를 사용합니다.

ICMP 메시지 유형 검사

라이센스: 보호

특정 ICMP 메시지 유형 값으로 패킷을 검색하려면 `itype` 키워드를 사용합니다. 유효한 ICMP 유형 값을 지정하거나(ICMP 유형 번호의 전체 목록은 http://www.iana.org/assignments/icmp-parameters 또는 http://www.faqs.org/rfcs/rfc792.html 참고) 또는 유효하지 않은 ICMP 유형 값을 지정하여 다양한 유형의 트래픽을 테스트할 수 있습니다. 예를 들어, 공격자는 범위에서 서비스 거부 및 플러딩 공격을 야기할 사정 거리 밖의 ICMP 유형 값을 설정할 수 있습니다.

보다 작음(<) 및 보다 큼(>)을 사용하여 `itype` 인수 값의 범위를 지정할 수 있습니다.

예를 들면 다음과 같습니다.

- <35
- >36
- 3<>55

팁 ICMP 유형 번호의 전체 목록은 http://www.iana.org/assignments/icmp-parameters 또는 http://www.faqs.org/rfcs/rfc792.html을 참고하십시오.

ICMP 메시지 코드 검사

라이센스: 보호

ICMP 메시지는 때로 목적지에 도달할 수 없는 경우 정보를 제공하는 코드 값을 포함합니다. (사용될 수 있는 메시지 유형과 상관 관계가 있는 ICMP 메시지 코드의 전체 목록은 http://www.iana.org/assignments/icmp-parameters 의 두 번째 섹션을 참고하십시오.)

특정 ICMP 코드 값으로 패킷을 확인하려면 icode 키워드를 사용할 수 있습니다. 유효한 ICMP 코드 값 또는 유효하지 않은 ICMP 코드 값을 지정하여 다양한 트래픽 유형을 테스트할 수 있습니다.

보다 작음(<) 및 보다 큼(>)을 사용하여 icode 인수 값의 범위를 지정할 수 있습니다.

예를 들면 다음과 같습니다.

- 35보다 작은 값을 찾으려면, <35를 지정합니다.
- 36보다 큰 값을 찾으려면, >36을 지정합니다.
- 3에서 55 사이의 값을 찾으려면, 3<>55를 지정합니다.

팁 icode 및 itype 키워드를 사용하여 둘 다에 일치하는 트래픽을 식별할 수 있습니다. 예를 들어, ICMP Destination Unreachable(목적지 도달 불가) 코드 유형과 ICMP Port Unreachable(포트 연결 불가) 코드 유형을 포함하는 ICMP 트래픽을 식별하려면 Destination Unreachable(목적지 도달 불가)에 대한 3의 값과 함께 itype 키워드를, Port Unreachable(포트 연결 불가)에 대한 3의 값과 함께 icode 키워드를 사용합니다.

TCP 헤더 값과 스트림 크기 검사

라이센스: 보호

ASA FirePOWER 모듈은 패킷의 TCP 헤더와 TCP 스트림 크기를 사용하여 시도된 공격을 식별하도록 설계된 키워드를 지원합니다. TCP 특정 키워드에 대한 자세한 내용은 다음 섹션을 참고하십시오.

- 23-49페이지의 TCP 확인 응답 값 검사
- 23-49페이지의 TCP 플래그 조합 검사
- 23-51페이지의 TCP 또는 UDP 클라이언트 또는 서버 흐름에 규칙 적용
- 23-52페이지의 정적 TCP 시퀀스 번호 식별
- 23-52페이지의 지정된 크기의 TCP 창 확인
- 23-52페이지의 지정된 크기의 TCP 스트림 식별

TCP 확인 응답 값 검사

라이센스: 보호

패킷의 TCP 확인 응답 수에 대한 값을 비교하려면 ack 키워드를 사용할 수 있습니다. ack 키워드에 지정된 값이 패킷의 TCP 확인 응답 수에 일치하는 경우 규칙이 트리거됩니다.

ack의 인수 값은 숫자여야 합니다.

TCP 플래그 조합 검사

라이센스: 보호

flags 키워드를 사용하여 검사한 패킷에 지정되었을 때, 규칙이 트리거되도록 하는 TCP 플래그의 조합을 지정할 수 있습니다.

참고 관례상 `flags` 값으로 `A+`를 사용할 경우, `established` 값으로 `flow` 키워드를 사용해야 합니다. 일반적으로 모든 플래그 조합 탐지를 확인하기 위해 플래그를 사용하는 경우, `stateless` 값으로 `flow` 키워드를 사용해야 합니다. `flow` 키워드에 대한 자세한 내용은 23-51페이지의 TCP 또는 UDP 클라이언트 또는 서버 흐름에 규칙 적용을 참고하십시오.

`flags`키워드는 다음 표에 설명된 값을 확인하거나 무시할 수 있습니다.

표 23-26 플래그 인수

인수	TCP 플래그
Ack	데이터를 확인합니다.
Psh	데이터는 이 패킷에 보내야 합니다.
Syn	새로운 연결입니다.
Urg	패킷은 긴급한 데이터를 포함합니다.
Fin	닫힌 연결입니다.
Rst	중지된 연결입니다.
CWR	ECN 정체 창이 줄었습니다. 이는 이전에 R1 인수였으며 하위 호환성을 위해 계속 지원됩니다.
ECE	ECN 에코입니다. 이는 이전에 R2 인수였으며 하위 호환성을 위해 계속 지원됩니다.

팁 ECN(명시적 정체 알림)에 대한 자세한 내용은 http://www.faqs.org/rfcs/rfc3168.html의 정보를 참고하십시오.

`flags` 키워드를 사용하면, 연산자를 사용하여 시스템이 다중 플래그에 대한 일치를 수행하는 방법을 나타낼 수 있습니다. 다음 표에서 이 연산자를 설명합니다.

표 23-27 플래그와 함께 사용되는 연산자

연산자	설명	예
all	패킷은 모든 지정된 플래그를 포함해야 합니다.	`Urg` 및 `all`을 선택하여 패킷이 Urgent(긴급) 플래그를 포함해야 하며 다른 모든 플래그를 포함하도록 지정합니다.
any	패킷은 지정된 플래그를 모두 포함할 수 있습니다.	`Ack`, `Psh` 및 `any`를 선택하여 `Ack` 및 `Psh` 플래그 둘 중 하나 또는 둘 다 규칙을 트리거할 수 있도록 설정되어야 하며 모든 플래그가 하나의 패킷에도 설정될 수 있도록 지정합니다.
not	패킷은 지정된 플래그 집합을 포함할 수 **없습니다**.	`Urg`와 `not`을 선택하여 Urgent(긴급) 플래그가 이 규칙을 트리거하는 패킷에 설정되지 **않도록** 지정합니다.

TCP 또는 UDP 클라이언트 또는 서버 흐름에 규칙 적용

라이센스: 보호

flow 키워드를 사용하여 세션 특징에 기반한 규칙에 따라 검사를 위한 패킷을 선택할 수 있습니다. flow 키워드를 사용하면 클라이언트 흐름 또는 서버 흐름에 규칙을 적용하여 규칙이 적용된 트래픽 흐름의 방향을 지정할 수 있습니다. flow 키워드가 패킷을 검사하는 방법을 지정하려면, 분석을 원하는 트래픽의 방향과 검사된 패킷의 상태, 그리고 패킷이 재구축된 스트림의 일부인지 여부를 설정할 수 있습니다.

규칙을 처리할 때 패킷의 상태 저장 검사가 이루어집니다. TCP 규칙이 상태 비저장 트래픽(설정된 세션 컨텍스트가 없는 트래픽)을 무시하기를 원하는 경우, 규칙에 flow 키워드를 추가하고 키워드의 **Established** 인수를 선택해야 합니다. UDP 규칙이 상태 비저장 트래픽 무시하기를 원하는 경우, 규칙에 flow 키워드를 추가하고 **Established** 인수 또는 방향 인수 중 하나, 또는 둘 다를 선택해야 합니다. 이것은 TCP 또는 UDP 규칙이 패킷의 상태 저장 검사를 수행하도록 합니다.

방향 인수를 추가하면, 규칙 엔진은 지정된 방향과 일치하는 흐름과 함께 설정한 상태가 있는 해당 패킷만 검사합니다. TCP 또는 UDP 연결이 탐지되었을 때 트리거되는 규칙에 established 인수 및 From Client 인수와 함께 flow 키워드를 추가하는 경우, 규칙 엔진은 클라이언트에서 전송된 패킷만 검사합니다.

팁 최대 성능을 위해, TCP 규칙 또는 UDP 세션 규칙에서 항상 flow 키워드를 포함합니다.

흐름을 지정하려면, Create Rule(규칙 생성) 페이지의 **Detection Options(탐지 옵션)** 목록에서 flow 키워드를 선택하고 **Add Option(옵션 추가)**을 클릭합니다. 다음으로, 각 필드에 제공된 목록에서 함수를 선택합니다.

다음 표에서는 flow 키워드에 대해 지정할 수 있는 스트림 관련 인수를 설명합니다.

표 23-28 상태 관련 흐름 인수

인수	설명
Established	연결이 설정된 경우 트리거됩니다.
Stateless	스트림 프로세서의 상태에 상관없이 트리거됩니다.

다음 표에서는 flow 키워드에 대해 지정할 수 있는 방향 옵션을 설명합니다.

표 23-29 흐름 방향 인수

인수	설명
To Client	서버 응답 시 트리거됩니다.
To Server	클라이언트 응답 시 트리거됩니다.
From Client	클라이언트 응답 시 트리거됩니다.
From Server	서버 응답 시 트리거됩니다.

From Server 및 To Client는 같은 기능을 수행하며, To Server 및 From Client도 같은 기능을 수행한다는 점에 유의하십시오. 이 옵션은 규칙에 컨텍스트 및 가독성을 추가하기 위해 존재합니다. 예를 들어 서버에서 클라이언트에 취해지는 공격을 탐지하기 위해 설계된 규칙을 작성하는 경우, From Server를 사용하십시오. 하지만 클라이언트에서 서버에 취해지는 공격을 탐지하기 위해 설계된 규칙을 작성하는 경우, From Client를 사용합니다.

다음 표에서는 flow 키워드에 대해 지정할 수 있는 스트림 관련 인수를 설명합니다.

표 23-30 스트림 관련 흐름 인수

인수	설명
Ignore Stream Traffic	재작성한 스트림 패킷에서 트리거되지 않습니다.
Only Stream Traffic	재작성된 스트림 패킷에서만 트리거됩니다.

예를 들어, 설정된 세션에서 클라이언트로부터 서버로 이동하면서 스트림 전처리기가 리어셈블한 트래픽을 탐지하려면 `flow` 키워드의 값으로 `To Server, Established, Only Stream Traffic`을 사용할 수 있습니다.

정적 TCP 시퀀스 번호 식별

라이센스: 보호

`seq` 키워드로 정적 시퀀스 번호 값을 지정할 수 있습니다. 시퀀스 번호가 특정 인수에 일치하는 패킷은 키워드를 포함하는 규칙을 트리거합니다. 이 키워드는 거의 사용되지 않지만 정적 시퀀스 번호로 생성된 패킷을 사용한 스캔 네트워크와 공격 식별에 도움이 됩니다.

지정된 크기의 TCP 창 확인

라이센스: 보호

`window` 키워드를 사용하여 관심 있는 TCP 창 크기를 지정할 수 있습니다. 이 키워드를 포함하는 규칙은 지정된 TCP 창 크기의 패킷이 발생할 때마다 트리거됩니다. 이 키워드는 거의 사용되지 않지만 정적 TCP 창 크기로 생성된 패킷을 사용한 스캔 네트워크와 공격 식별에 도움이 됩니다.

지정된 크기의 TCP 스트림 식별

라이센스: 보호

다음 형식을 사용하여 `stream_size` 키워드를 TCP 스트림 바이트의 크기를 결정하는 스트림 전처리기와 함께 사용할 수 있습니다.

direction,*operator*,*bytes*

*bytes*가 바이트 수인 경우. 쉼표(,)로 인수의 각 옵션을 구분해야 합니다.

다음 표에서는 `stream_size` 키워드에 대해 지정할 수 있는 대소문자를 구분하는 방향 옵션을 설명합니다.

표 23-31 stream_size 키워드 방향 인수

인수	설명
client	지정된 스트림 크기와 일치하는 클라이언트의 스트림에서 트리거됩니다.
server	지정된 스트림 크기와 일치하는 서버의 스트림에서 트리거됩니다.
both	클라이언트 트래픽 및 지정된 스트림 크기와 일치하는 서버의 트래픽 모두에서 트리거됩니다. 예를 들어, `both, >, 200` 인수는 클라이언트 발신 트래픽이 200바이트보다 큰 경우 및 서버 발신 트래픽이 200바이트보다 큰 경우에 트리거됩니다.

표 23-31 stream_size 키워드 방향 인수 (계속)

인수	설명
either	무엇이 먼저 발생하든 지정된 스트림 크기와 일치하는 클라이언트 또는 서버의 트래픽에서 트리거됩니다. 예를 들어, `either, >, 200` 인수는 클라이언트 발신 트래픽이 200바이트보다 큰 경우 또는 서버 발신 트래픽이 200바이트보다 큰 경우에 트리거됩니다.

다음 표에서는 `stream_size` 키워드와 함께 사용할 수 있는 연산자를 설명합니다.

표 23-32 stream_size 키워드 인수 연산자

연산자	설명
=	같음
!=	같지 않음
>	보다 큼
<	보다 작음
>=	보다 크거나 같음
<=	보다 작거나 같음

예를 들어, `client, >=, 5001216`을 `stream_size` 키워드의 인수로 사용하여 클라이언트에서 5001216바이트와 같거나 큰 서버로 이동하는 TCP 스트림을 탐지할 수 있습니다.

TCP 스트림 리어셈블리 활성화 및 비활성화

라이센스: 보호

`stream_reassemble` 키워드를 사용하여 연결 시 검사된 트래픽이 규칙 조건에 일치할 때 단일 연결에 대한 TCP 스트림 리어셈블리를 활성화 및 비활성화할 수 있습니다. 또는, 규칙에서 이러한 키워드를 여러 번 사용할 수 있습니다.

스트림 리어셈블리를 활성화하거나 비활성화하려면 다음 구문을 사용합니다.

```
enable|disable, server|client|both, option, option
```

다음 표에서는 `stream_reassemble` 키워드와 함께 사용할 수 있는 선택적 인수를 설명합니다.

표 23-33 stream_reassemble 선택적 인수

인수	설명
noalert	규칙에 지정된 다른 모든 탐지 옵션에 관계없이 어떤 이벤트도 생성하지 않습니다.
fastpath	일치할 때 연결 트래픽의 나머지 부분을 무시합니다.

예를 들어, 다음 규칙은 200개의 OK(확인) 상태 코드가 HTTP 응답에서 탐지된 연결에 대해 이벤트를 생성하지 않고 TCP 클라이언트 측 스트림 리어셈블리를 비활성화합니다.

```
alert tcp any 80 -> any any (flow:to_client, established; content: "200 OK";
stream_reassemble:disable, client, noalert
```

stream_reassemble을 사용하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 `stream_reassemble`을 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`stream_reassemble` 섹션이 나타납니다.

세션에서 SSL 정보 추출

라이센스: 보호

SSL 규칙 키워드를 사용하여 SSL(Secure Sockets Layer) 전처리기를 호출할 수도 있고 암호화된 세션에서 패킷으로부터 SSL 버전 및 세션 상태에 관한 정보를 추출할 수 있습니다.

클라이언트와 서버가 SSL 또는 TLS(전송 레이어 보안)을 사용하여 암호화된 세션을 설정하기 위해 통신할 때 핸드쉐이크 메시지를 교환합니다. 세션에서 전송되는 데이터는 암호화되지만, 핸드쉐이크 메시지는 그렇지 않습니다.

SSL 전처리기는 특정 핸드쉐이크 필드의 상태 및 버전 정보를 추출합니다. 핸드쉐이크 내 두 필드는 핸드쉐이크의 세션 및 단계를 암호화하는 데 사용된 SSL 또는 TLS 버전을 나타냅니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-54페이지의 ssl_state
- 23-55페이지의 ssl_version

ssl_state

라이센스: 보호

`ssl_state` 키워드는 암호화된 세션에 대한 상태 정보를 비교하는 데 사용될 수 있습니다. 동시에 사용된 2개 이상의 SSL 버전을 확인하려면, 규칙에서 여러 `ssl_version` 키워드를 사용합니다.

규칙이 `ssl_state` 키워드를 사용하면, 규칙 엔진은 SSL 전처리기를 호출하여 SSL 상태 정보에 대한 트래픽을 확인하도록 합니다.

예를 들어, 너무 긴 챌린지 길이 및 너무 많은 데이터를 가진 `ClientHello` 메시지를 보내 서버에 버퍼 오버플로를 일으키는 공격자의 시도를 검색하려면, `client_hello`와 함께 `ssl_state` 키워드를 인수로 사용한 후 비정상적으로 규모가 큰 패킷을 확인할 수 있습니다.

쉼표로 구분된 목록을 사용하여 SSL 상태에 대한 여러 인수를 지정합니다. 여러 인수를 나열할 경우, 시스템은 OR 연산자를 사용하여 이를 평가합니다. 예를 들어, 인수로 `client_hello` 및 `server_hello`를 지정한 경우, 시스템은 `client_hello` 또는 `server_hello`가 있는 트래픽에 대한 규칙을 평가합니다.

또한 모든 인수를 무효화할 수 있습니다. 예를 들면 다음과 같습니다.

```
!client_hello, !unknown
```

연결이 각 상태 집합에 도달했음을 확인하려면 ssl_state 규칙 옵션을 사용하는 여러 규칙이 사용되어야 합니다. `ssl_state` 키워드는 다음 식별자를 인수로 취합니다.

표 23-34 `ssl_state` *인수*

인수	목적
`client_hello`	메시지 유형으로 `client_hello`를 가진 핸드쉐이크 메시지와 비교하며, 클라이언트가 암호화된 세션을 요청합니다.
`server_hello`	메시지 유형으로 `server_hello`를 가진 핸드쉐이크 메시지와 비교하며, 클라이언트의 암호화된 세션 요청에 서버가 응답합니다.
`client_keyx`	메시지 유형으로 `ClientKeyExchange`를 가진 핸드쉐이크 메시지와 비교하며, 서버로부터 키를 수신했음을 확인하기 위해 클라이언트가 서버에 키를 전송합니다.
`server_keyx`	메시지 유형으로 `serverKeyExchange`를 가진 핸드쉐이크 메시지와 비교하며, 서버로부터 키를 수신했음을 확인하기 위해 클라이언트가 서버에 키를 전송합니다.
`unknown`	모든 핸드쉐이크 메시지 유형과 비교합니다.

ssl_version

라이센스: 보호

`ssl_version` 키워드는 암호화된 세션의 버전 정보와 일치시키는 데 사용될 수 있습니다. 규칙이 `ssl_version` 키워드를 사용하면, 규칙 엔진은 SSL 전처리기를 호출하여 SSL 버전 정보에 대한 트래픽을 확인하도록 합니다.

예를 들어, SSL 버전 2에 버퍼 오버플로 취약성이 있다는 것을 알고 있는 경우, `ssl_version` 키워드를 `sslv2` 인수와 함께 사용하여 SSL의 해당 버전을 사용하는 트래픽을 식별할 수 있습니다.

쉼표로 구분된 목록을 사용하여 SSL 버전에 대한 여러 인수를 지정합니다. 여러 인수를 나열할 경우, 시스템은 OR 연산자를 사용하여 이를 평가합니다. 예를 들어, SSLv2를 사용하지 않는 모든 암호화된 트래픽을 식별하고자 한다면 규칙에 `ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2`를 추가할 수 있습니다. 규칙은 SSL 버전 3, TLS 버전 1.0, TLS 버전 1.1, 또는 TLS 버전 1.2를 사용하여 모든 트래픽을 평가합니다.

`ssl_version` 키워드는 다음 SSL/TLS 버전 식별자를 인수로 취합니다.

표 23-35 `ssl_version` *인수*

인수	목적
`sslv2`	SSL(Secure Sockets Layer) 버전 2를 사용하여 인코딩된 트래픽과 비교합니다.
`sslv3`	SSL(Secure Sockets Layer) 버전 3을 사용하여 인코딩된 트래픽과 비교합니다.
`tls1.0`	TLS(전송 레이어 보안) 버전 1.0을 사용하여 인코딩된 트래픽과 비교합니다.
`tls1.1`	TLS(전송 레이어 보안) 버전 1.1을 사용하여 인코딩된 트래픽과 비교합니다.
`tls1.2`	TLS(전송 레이어 보안) 버전 1.2를 사용하여 인코딩된 트래픽과 비교합니다.

애플리케이션 레이어 프로토콜 값 검사

라이센스: 보호

전처리기가 대부분의 애플리케이션 레이어 프로토콜 값의 정규화 및 검사 작업을 수행하지만, 다음 섹션에 설명된 키워드를 사용하여 계속해서 애플리케이션 레이어 값을 검사할 수 있습니다.

RPC

라이센스: 보호

rpc 키워드는 TCP 또는 UDP 패킷의 ONC RPC(Open Network Computing Remote Procedure Call) 서비스를 식별합니다. 이를 통해 호스트에서 RPC 프로그램을 확인하려는 시도를 탐지할 수 있습니다. 침입자는 RPC 포트매퍼를 사용하여 네트워크에서 실행되는 RPC 서비스가 공격받을 가능성이 있는지 결정할 수 있습니다. 이들은 포트매퍼를 사용하지 않고 RPC를 실행하는 다른 포트에 액세스를 시도할 수도 있습니다. 다음 표에서는 rpc 키워드가 수용하는 인수를 나열합니다.

표 23-36 rpc 키워드 인수

인수	설명
application	RPC 애플리케이션 번호
절차	호출된 RPC 절차
버전	RPC 버전

rpc 키워드에 대한 인수를 지정하려면, 다음 구문을 사용합니다.

application,*procedure*,*version*

*application*이 RPC 애플리케이션 번호인 경우, *procedure*는 RPC 절차 번호이며, *version*은 RPC 버전 번호입니다. rpc 키워드에 대한 모든 인수를 지정해야 합니다. 인수 중 하나를 지정할 수 없는 경우, 별표(*)로 교체합니다.

예를 들어, 모든 절차 또는 버전으로 RPC 포트매퍼를 검색하려면(번호 100000으로 표시된 RPC 애플리케이션), 100000,*,*를 인수로 사용합니다.

ASN.1

라이센스: 보호

asn1 키워드를 사용하면 패킷 또는 패킷의 일부를 해독하여 다양한 악성 인코딩을 찾을 수 있습니다.

다음 표에서는 asn1 키워드에 대한 인수를 설명합니다.

표 23-37 asn.1 키워드 인수

인수	설명
Bitstring Overflow	원격으로 공격 가능한 유효하지 않은 비트 스트링 인코딩을 탐지합니다.
Double Overflow	표준 버퍼보다 큰 이중 ASCII 인코딩을 탐지합니다. 이것은 Microsoft Windows에서 악용 가능한 기능이라고 알려져 있지만, 현재로서는 알 수 없습니다. 서비스는 개발 가능할 수 있습니다.
Oversize Length	제공된 인수보다 큰 ASN.1 유형 길이를 탐지합니다. 예를 들어, Oversize Length로 500을 설정한 경우, 500보다 큰 모든 ASN.1 유형이 규칙을 트리거합니다.
Absolute Offset	패킷 페이로드의 시작 지점으로부터 절대적 오프셋을 설정합니다. (오프셋 카운터가 0바이트부터 시작한다는 점에 유의하십시오.) 예를 들어, SNMP 패킷을 해독할 경우, Absolute Offset은 0으로 설정하고 Relative Offset은 설정하지 않습니다. Absolute Offset은 양수이거나 음수일 수 있습니다.
Relative Offset	이것은 마지막으로 성공한 콘텐츠 일치로부터의 상대적 오프셋이며, `pcre` 또는 `byte_jump`입니다. 콘텐츠 "foo" 바로 다음에 있는 ASN.1 시퀀스를 해독하려면, Relative Offset은 0으로 설정하고 Absolute Offset은 설정하지 않습니다. Relative Offset은 양수이거나 음수일 수 있습니다. (오프셋 카운터가 0바이트부터 시작한다는 점에 유의하십시오.)

예를 들어, 버퍼 오버플로를 만드는 Microsoft ASN.1 라이브러리에는 알려진 취약성이 있는데, 공격자가 특별히 만들어진 인증 패킷으로 조건을 공격하도록 허용합니다. 시스템이 asn.1 데이터를 해독할 때, 패킷의 악용 코드는 시스템 수준 권한이 있는 호스트에서 수행할 수 있거나 DoS 상태를 야기할수 있습니다. 다음 규칙은 `asn1` 키워드를 사용하여 이 취약점을 이용하려는 시도를 탐지합니다.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|"; nocase;
offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length
100,relative_offset 54;)
```

위 규칙은 포트 445를 사용하여 $EXTERNAL_NET 변수에 정의된 모든 IP 주소, 모든 포트로부터 $HOME_NET 변수에 정의된 모든 IP 주소로 이동하는 TCP 트래픽에 대한 이벤트를 생성합니다. 또한, 서버로 연결된 TCP 연결에만 규칙을 수행합니다. 규칙은 다음으로 특정 위치에서 특정 내용을 테스트합니다. 마지막으로, 규칙은 `asn1` 키워드를 사용하여 비트 스트링 인코딩 및 이중 ASCII 인코딩을 탐지하고, 마지막으로 성공한 콘텐츠 일치의 끝 지점에서 55바이트 길이부터 100바이트 이상의 길이를 가진 asn.1 유형을 식별합니다. (오프셋 카운터가 0바이트부터 시작한다는 점에 유의하십시오.)

urilen

라이센스: 보호

`urilen` 키워드를 HTTP 검사 전처리기와 함께 사용하여 최대 길이보다는 작고 최소 길이보다는 크며, 특정 범위 안에 있는 특정 길이 URI의 HTTP 트래픽을 검사할 수 있습니다.

HTTP 검사 전처리기가 패킷을 표준화하고 검사한 후, 규칙 엔진은 규칙에 대한 패킷을 평가하고, `urilen` 키워드가 지정한 길이 상태에 URI가 일치하는지 결정합니다. 이 키워드를 사용하여 URI 길이 취약성을 이용하려고 하는 공격을 탐지할 수 있습니다. 예를 들면, 공격자가 DoS 상태를 야기하거나 시스템 레벨 권한으로 호스트에서 코드를 실행할 수 있는 버퍼 오버플로를 생성하는 것입니다.

`urilen` 키워드를 규칙에서 사용할 때 다음 사항에 유의하십시오.

- 실전에서는 항상 `urilen` 키워드와 `flow:established` 키워드 및 하나 이상의 다른 키워드를 조합하여 사용합니다.
- 규칙 프로토콜은 항상 TCP입니다. 자세한 내용은 23-4페이지의 프로토콜 지정을 참고하십시오.
- 대상 포트는 항상 HTTP 포트입니다. 자세한 내용은 23-8페이지의 침입 규칙 내 포트 정의 및 2-15페이지의 미리 정의된 기본 변수 최적화를 참고하십시오.

십진수로 나타낸 바이트 수와 보다 작음(<) 또는 보다 큼(>)을 사용하여 URI 길이를 지정합니다.

예를 들면 다음과 같습니다.

- 5바이트 길이의 URI를 탐지하려면 `5`를 지정합니다.
- 5바이트 길이보다 짧은 URI를 탐지하려면 `< 5`(스페이스 문자 하나로 분리)를 지정합니다.
- 5바이트 길이보다 긴 URI를 탐지하려면 `> 5`(스페이스 문자 하나로 분리)를 지정합니다.
- 길이가 3에서 5바이트 사이에 들어가는 URI를 탐지하려면 `3 <> 5`(`<>` 전후에 스페이스 문자 하나씩 표시)를 지정합니다.

예를 들어, eDirectory 버전 8.8과 함께 제공된 Novell의 서버 모니터링 및 진단 유틸리티 iMonitor 버전 2.4에는 알려진 취약성이 있습니다. 과도하게 긴 URI을 포함하는 패킷은 버퍼 오버플로를 생성하며 이로 인해 공격자가 시스템 수준 권한으로 호스트에서 실행하거나 DoS 상태를 야기할 수 있는 특수하게 조작된 패킷이 포함된 조건을 악용할 수 있습니다. 다음 규칙은 `urilen` 키워드를 사용하여 이 취약성을 악용하려는 시도를 탐지합니다.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt";flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

위 규칙은 $HTTP_PORTS 변수에 정의된 포트를 사용하여 $EXTERNAL_NET 변수에 정의된 모든 IP 주소, 모든 포트로부터 $HOME_NET 변수에 정의된 모든 IP 주소로 이동하는 TCP 트래픽에 대한 이벤트를 생성합니다. 또한, 패킷은 서버로 설정된 TCP 연결에서만 규칙에 대해 평가됩니다. 규칙은 `urilen` 키워드를 사용하여 길이가 8192바이트 이상인 모든 URI를 탐지합니다. 마지막으로, 규칙은 대소문자를 구별하지 않는 특정 콘텐츠 `/nds/`에 대한 URI를 검색합니다.

DCE/RPC 키워드

라이센스: 보호

다음 표에 설명된 세 개의 DCE/RPC 키워드로 DCE/RPC 세션 트래픽의 공격 위험을 모니터링할 수 있습니다. 시스템이 이 키워드로 규칙을 처리할 때, DCE/RPC 전처리기를 호출합니다. 자세한 내용은 15-2페이지의 DCE/RPC 트래픽 디코딩을 참고하십시오.

표 23-38 DCE/RPC 키워드

사용 키워드	사용 방법	탐지 대상
`dce_iface`	단독으로	특정 DCE/RPC DP 서비스를 식별하는 패킷
`dce_opnum`	`dce_iface`가 앞에 오는 경우	특정 DCE/RPC DP 서비스 작업을 식별하는 패킷
`dce_stub_data`	`dce_iface` + `dce_opnum`이 앞에 오는 경우	특정 작업 요청 또는 응답을 정의하는 스텁 데이터

표에서 `dce_opnum` 및 `dce_iface`가 항상 앞에 와야 한다는 점과 `dce_stub_data` 및 `dce_iface` + `dce_opnum`이 항상 앞에 와야 한다는 점에 유의하시기 바랍니다.

DCE/RPC 키워드를 다른 규칙 키워드와 조합하여 사용할 수 있습니다. DCE/RPC 규칙의 경우, `byte_jump`, `byte_test`, and `byte_extract` 키워드를 선택한 **DCE/RPC** 인수와 함께 사용합니다. 자세한 내용은 23-30페이지의 Byte_Jump 및 Byte_Test 사용 및 23-81페이지의 패킷 데이터를 키워드 인수로 읽어들이기를 참고하십시오.

Cisco는 DCE/RPC 키워드를 포함하는 규칙에 최소 하나의 `content` 키워드를 포함할 것을 권장합니다. 이는 규칙 엔진이 빠른 패턴 매처를 사용하도록 하는 것인데, 이는 처리 속도를 높이고 성능을 향상시킵니다. 규칙에 최소 하나의 `content` 키워드가 포함될 때, `content` 키워드 **Use Fast Pattern Matcher(빠른 패턴 매처 사용)** 인수를 활성화했는지 여부에 상관 없이 규칙 엔진이 빠른 패턴 매처를 사용한다는 점에 유의하십시오. 자세한 내용은 23-15페이지의 콘텐츠 일치 검색 및 23-26페이지의 빠른 패턴 매처 사용을 참고하십시오.

다음의 경우 일치 내용으로 DCE/RPC 버전 및 연속되는 헤더 정보를 사용할 수 있습니다.

- 규칙은 다른 `content` 키워드를 포함하지 않습니다
- 규칙은 다른 `content` 키워드를 포함하지만, DCE/RPC 버전 및 연속된 정보는 다른 콘텐츠보다 고유한 패턴을 나타냅니다

  예를 들어, DCE/RPC 버전 및 연속되는 정보는 단일 바이트의 콘텐츠보다 고유할 가능성이 더 높습니다.

다음 버전 중 하나 및 연속되는 정보 콘텐츠 일치로 자격 심사 규칙을 종료해야 합니다.

- 연결 지향 DCE/RPC 규칙은 주요 버전 05, 비주요 버전 00, 요청 PDU(프로토콜 데이터 장치) 유형 00에 대해 콘텐츠 `|05 00 00|`을 사용합니다.
- 연결 없는 DCE/RPC 규칙은 버전 04, 요청 PDU 유형 00에 대해 콘텐츠 `|04 00|`을 사용합니다.

어느 경우에든, 이미 DCE/RPC 전처리기에서 완료된 처리를 반복하지 않고 빠른 패턴 매처를 호출하는 규칙에서 마지막 키워드로 버전 및 연속된 정보를 위한 `content` 키워드를 배치합니다. 규칙 끝에 `content` 키워드를 배치하는 것은 빠른 패턴 매처를 호출하는 디바이스로 사용되는 버전 콘텐츠에 적용되지만 규칙에 일치하는 다른 콘텐츠에는 반드시 해당되지는 않는다는 점에 유의하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-59페이지의 dce_iface
- 23-60페이지의 dce_opnum
- 23-61페이지의 dce_stub_data

dce_iface

라이센스: 보호

`dce_if ace` 키워드를 사용하여 특정 DCE/RPC 서비스를 확인할 수 있습니다.

선택적으로, `dce_opnum` 및 `dce_stub_data` 키워드와 조합하여 `dce_iface`를 사용해 검사해야 할 DCE/RPC 트래픽을 추가로 제한할 수 있습니다. 자세한 내용은 23-60페이지의 dce_opnum 및 23-61페이지의 dce_stub_data를 참고하십시오.

고정된 16바이트 UUID(보편적 고유 식별자)는 각 DCE/RPC 서비스에 할당된 애플리케이션 인터페이스를 식별합니다. 예를 들어, UUID 4b324fc8-670-01d3-1278-5a47bf6ee188은 DCE/RPC lanmanserver 서비스를 식별하는데, 이는 srvsvc 서비스로도 알려져 있으며, p2p 프린터, 파일 및 SMB 명명된 파이프 공유를 위한 다양한 관리 기능을 제공합니다. DCE/RPC 전처리기는 UUID 및 DCE/RPC 세션을 추적하기 위한 관련 헤더 값을 사용합니다.

인터페이스 UUID는 하이픈으로 구분된 5개의 16진수 문자열로 구성됩니다.

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

넷로그온 인터페이스에 대해 다음 UUID에 표시된 대로 하이픈을 포함하는 전체 UUID를 입력하여 인터페이스를 지정합니다.

```
12345678-1234-abcd-ef00-01234567cffb
```

빅 엔디언 바이트 순서로 UUID에 처음 3개 문자열을 지정해야 한다는 점에 유의하십시오. 게시된 인터페이스 목록 및 프로토콜 분석기는 일반적으로 UUID를 정확한 바이트 순서로 정렬하지만 이를 입력하기 전에 UUID 바이트 순서를 다시 정렬해야 할 수 있습니다. 경우에 따라 리틀 엔디언 바이트 순서로 처음 3개 문자열과 함께 원시 ASCII 텍스트로 표시될 수 있으므로 다음 메신저 서비스를 보여진 UUID로 생각하십시오.

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

다음과 같이 하이픈을 삽입하고 처음 3개 문자열을 빅 엔디언 바이트 순서로 나열함으로써 `dce_iface` 키워드에 동일한 UUID를 지정합니다.

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

DCE/RPC 세션이 여러 인터페이스에 요청을 포함할 수 있지만, 한 규칙에서 한 개의 `dce_iface` 키워드만 포함해야 합니다. 추가 인터페이스를 검색하려면 추가 규칙을 만듭니다.

DCE/RPC 애플리케이션 인터페이스에는 또한 인터페이스 버전 번호가 있습니다. 선택적으로 동일한 버전, 동일하지 않은 버전, 특정 값보다 적거나 큰 버전을 나타내는 연산자와 인터페이스 버전을 지정할 수 있습니다.

모든 TCP 세분화 또는 IP 단편화에 더해 연결 지향 DCE/RPC와 연결 없는 DCE/RPC 모두 단편화될 수 있습니다. 일반적으로, 첫 번째 이외의 다른 DCE/RPC 조각을 지정된 인터페이스와 연결하는 것은 유용하지 않고, 이렇게 하면 그 결과로 많은 양의 잘못된 긍정을 얻을 수 있습니다. 그러나, 유연성을 위해 지정된 인터페이스에 대한 모든 조각을 선택적으로 평가할 수 있습니다.

다음 표에는`dce_iface` 키워드 인수가 요약되어 있습니다.

표 23-39 `dce_iface` ***인수***

인수	설명
Interface UUID	하이픈을 포함하는 UUID는 사용자가 DCE/RPC 트래픽에서 탐지할 특정 서비스의 애플리케이션 인터페이스를 식별합니다. 특정 인터페이스에 연결된 모든 요청은 인터페이스 UUID에 일치됩니다.
Version	또는, 0에서 65535까지의 애플리케이션 인터페이스 버전 번호 및 특정 값보다 큰(>), 작은(<), ?은(=), 같지 않은(!) 버전을 탐지할지 여부를 나타내는 연산자.
All Fragments	또는, 모든 관련 DCE/RPC 조각의 인터페이스와 일치하는 것을 가능하게 합니다. 지정되어 있는 경우, 인터페이스 버전에서도 가능합니다. 이 인수는 기본적으로 비활성화되어 있는데, 첫 번째 조각 또는 조각화되지 않은 전체 패킷이 특정 인터페이스와 연결되어 있는 경우에만 키워드 일치를 나타냅니다. 이 인수를 활성화하면 잘못된 긍정을 얻을 수 있다는 점에 유의하십시오.

dce_opnum

라이센스: 보호

`dce_opnum` 키워드를 DCE/RPC 전처리기와 함께 사용하여 DCE/RPC 서비스가 제공하는 하나 이상의 특정 작업을 확인하는 패킷을 탐지할 수 있습니다.

클라이언트 함수 호출은 특정 서비스 함수를 요구하는데, 이는 DCE/RPC 사양에서 *작업*으로 참조됩니다. 작업 번호(opnum)는 DCE/RPC 헤더에서 특정 작업을 식별합니다. 공격이 특정 작업을 대상으로 할 가능성이 높습니다.

예를 들어, UUID 12345678-1234-abcd-ef00-01234567cffb는 여러 다양한 작업을 제공하는 넷로그온 서비스에 대한 인터페이스를 식별합니다. 그중 하나는 작업 6의 NetrServerPasswordSet 작업입니다.

작업을 위한 서비스를 식별하려면 `dce_iface` 키워드 다음에 `dce_opnum` 키워드를 입력해야 합니다. 자세한 내용은 23-59페이지의 dce_iface를 참고하십시오.

단일 십진수 0에서 65535를 지정하여 특정 작업, 하이픈으로 구분된 작업의 범위 또는 쉼표로 구분된 작업 및 범위의 목록을 어떤 순서로도 나타낼 수 있습니다.

다음의 예시 중 하나를 통해 유효한 넷로그온 작업 번호를 지정합니다.

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data

라이센스: 보호

dce_stub_data 키워드를 DCE/RPC 전처리기와 함께 사용하여 다른 규칙 옵션에 관계 없이 스텁 데이터 시작 시 규칙 엔진이 검사를 시작하도록 지정할 수 있습니다. dce_stub_data 키워드를 따르는 패킷 페이로드 규칙 옵션은 스텁 데이터 버퍼에 관련하여 적용됩니다.

DCE/RPC 스텁 데이터는 클라이언트 절차 호출과 DCE/RPC 실행 시간 시스템 사이의 인터페이스를 제공하며, DCE/RPC의 중심이 되는 과정 및 서비스를 제공하는 메커니즘을 제공합니다. DCE/RPC 공격은 DCE/RPC 패킷의 스텁 데이터 부분에 표시됩니다. 스텁 데이터는 특정 작업 또는 함수 호출에 연결되어 있으므로, 관련 서비스 및 작업을 식별하려면 dce_stub_data에 앞에 항상 dce_iface 및 dce_opnum을 입력해야 합니다.

dce_stub_data 키워드는 인수를 갖지 않습니다. 자세한 내용은 23-59페이지의 dce_iface 및 23-60페이지의 dce_opnum을 참고하십시오.

SIP 키워드

라이센스: 보호

4개의 SIP 키워드를 사용하면 SIP 세션 트래픽을 모니터링하여 공격을 탐지할 수 있습니다.

SIP 프로토콜은 서비스 거부(DoS) 공격에 취약하다는 점을 참고하십시오. 이러한 공격을 해결할 규칙은 속도 기반 공격 방지를 활용할 수 있습니다. 자세한 내용은 20-28페이지의 동적 규칙 상태 추가 및 21-10페이지의 속도 기반 공격 방지를 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-61페이지의 sip_header
- 23-62페이지의 sip_body
- 23-62페이지의 sip_method
- 23-62페이지의 sip_stat_code

sip_header

라이센스: 보호

sip_header 키워드를 사용하여 추출된 SIP 요청 또는 응답 헤더 시작 시 검사를 시작하고 헤더 필드에 검사를 제한할 수 있습니다.

sip_header 키워드는 인수를 갖지 않습니다. 자세한 내용은 23-62페이지의 sip_method 및 23-62페이지의 sip_stat_code를 참고하십시오.

다음의 예제 규칙 조각 SIP 헤더를 가리키고 CSeq 헤더 필드에 일치됩니다.

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

sip_body

라이센스: 보호

sip_body 키워드를 사용하여 추출된 SIP 요청 또는 응답 메시지 본문 시작 지점에서 검사를 시작하고 메시지 본문 검사를 제한할 수 있습니다.

sip_body 키워드는 인수를 갖지 않습니다.

다음의 예제 규칙 조각은 SIP 메시지 본문을 가리키고 추출된 SDP 데이터의 c(연결 정보) 필드에서 특정 IP 주소에 일치됩니다.

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

규칙은 SDP 내용을 검색하는 것에 제한되지 않습니다. SIP 전처리기는 전체 메시지 본문을 추출하고 이를 규칙 엔진이 사용할 수 있도록 합니다.

sip_method

라이센스: 보호

각 SIP 요청의 *method* 필드는 요청의 목적을 확인합니다. sip_method 키워드를 사용하여 특정 방법을 위한 SIP 요청을 테스트할 수 있습니다. 메서드가 여러 개인 경우 쉼표로 구분하십시오.

다음 중 하나로 현재 정의된 SIP 메서드를 지정할 수 있습니다.

```
ack, benotify, bye, cancel, do, info, invite, join, message, notify, options, prack,
publish, quath, refer, register, service, sprack, subscribe, unsubscribe, update
```

메서드는 대소문자를 구분하지 않습니다. 쉼표로 여러 방법을 분리할 수 있습니다.

새로운 SIP 방법은 향후에 정의될 수도 있기 때문에, 사용자는 또한 사용자 지정 방법, 즉, 현재 정의된 SIP 방법이 아닌 방법을 지정할 수 있습니다. 수락된 필드 값은 RFC 2616에서 정의되는데, =, (, 및)와 같은 제어 문자 및 구분 기호를 제외한 모든 문자를 허용합니다. 제외되는 구분 기호의 전체 목록을 보려면 RFC 2616을 참고하십시오. 시스템은 트래픽의 지정된 사용자 지정 메서드가 발생할 경우, 패킷 헤더를 검사하지만 메시지는 검사하지 않습니다.

시스템은 최대 32개의 메서드까지 지원하는데, 최근 정의된 메서드 21개에 메서드 11개를 추가한 것입니다. 시스템은 사용자가 구성할 수 있는 정의되지 않은 모든 메서드를 무시합니다. 총 32개의 메서드는 SIP 전처리기 옵션을 **Methods to Check(확인하는 메서드)**를 사용하여 지정된 방법을 포함한다는 점에 유의하십시오. 자세한 내용은 15-50페이지의 SIP 전처리기 옵션 선택을 참고하십시오.

무효화를 사용하면 단 한 개의 방법만 지정할 수 있습니다. 예를 들면 다음과 같습니다.

```
!invite
```

그러나 규칙 내 여러 sip_method 키워드는 **AND** 작업으로 연결되어 있다는 점을 참고하십시오. 예를 들어, invite와 cancel을 제외한 추출된 모든 메서드를 테스트하려면 무효화된 sip_method 키워드를 두 개 사용합니다.

```
sip_method: !invite
sip_method: !cancel
```

Cisco는 sip_method 키워드를 포함하는 규칙에 최소 하나의 content 키워드를 포함할 것을 권장합니다. 이는 규칙 엔진이 빠른 패턴 매처를 사용하도록 하여 처리 속도를 높이고 성능을 향상시키기 위함입니다. 규칙에 최소 하나의 content 키워드가 포함될 때, content 키워드 **Use Fast Pattern Matcher(빠른 패턴 매처 사용)** 인수를 활성화했는지 여부에 상관 없이 규칙 엔진이 빠른 패턴 매처를 사용한다는 점에 유의하십시오. 자세한 내용은 23-15페이지의 콘텐츠 일치 검색 및 23-26페이지의 빠른 패턴 매처 사용을 참고하십시오.

sip_stat_code

라이센스: 보호

각 SIP 응답에 있는 세 자리의 상태 코드는 요청된 작업의 결과를 나타냅니다. sip_stat_code 키워드를 사용하여 특정 상태 코드에 대한 SIP 응답을 테스트할 수 있습니다.

한 자리 응답 유형 번호 1-9, 특정 세 자리 번호 100-999 또는 둘 중 어느 조합으로도 쉼표로 구분된 목록을 지정할 수 있습니다. 목록은 목록의 단일 번호가 SIP 응답의 코드에 일치하는 경우 일치합니다.

다음 표에서는 지정할 수 있는 SIP 상태 코드 값을 나타냅니다.

표 23-40 sip_stat_code 값

탐지 대상	지정 대상	예시	탐지 대상
특정 상태 코드	세 자리 상태 코드	189	189
지정된 단일 디지트로 시작하는 모든 세 자리 코드	단일 디지트	1	1xx. 즉, 100, 101, 102 등
값 목록	쉼표로 구분된 특정 코드 및 단일 디지트의 모든 조합	222, 3	222 + 300, 301, 302 등

사용자의 규칙이 content 키워드를 포함하는지 여부에 상관 없이 규칙 엔진이 sip_stat_code 키워드를 사용하여 지정된 값을 검색하기 위해 빠른 패턴 매처를 사용하지 않는다는 점에 유의하십시오.

GTP 키워드

라이센스: 보호

세 개의 GTP(GSRP 터널링 프로토콜) 키워드를 통해 GTP 버전, 메시지 유형 및 정보 요소에 대한 GTP 명령 계통을 검사할 수 있습니다. content 또는 byte_jump와 같은 다른 침입 규칙 키워드와 조합된 GTP 키워드를 사용할 수 없습니다. gtp_info 또는 gtp_type 키워드를 사용하는 각 규칙에서 gtp_version 키워드를 사용해야 합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-63페이지의 gtp_version
- 23-64페이지의 gtp_type
- 23-68페이지의 gtp_info

gtp_version

GTP 버전 0, 1, 2를 위한 GTP 컨트롤 메시지를 검사하려면 gtp_version 키워드를 사용할 수 있습니다.

다양한 GTP 버전이 다양한 메시지 유형 및 정보 요소를 정의하기 때문에, gtp_type 또는 gtp_info 키워드를 사용할 때 반드시 이 키워드를 사용해야 합니다. 값 0, 1, 2를 지정할 수 있습니다.

GTP 버전을 지정하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **gtp_version**을 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

gtp_version 키워드가 나타납니다.

단계 2 GTP 버전을 확인하기 위해 0, 1 또는 2를 지정합니다.

gtp_type

각 GTP 메시지는 숫자 값 및 문자열 모두로 구성된 메시지 유형으로 식별됩니다. `gtp_version` 키워드를 `gtp_type` 키워드와 조합하여 사용하여 특정 GTP 메시지 유형의 트래픽을 검사할 수 있습니다.

메시지 유형, 정의된 문자열 또는 다음의 예시에 표시된 대로 모든 조합 중 하나 또는 모두의 쉼표로 구분된 목록에 대한 정의된 십진수 값을 지정할 수 있습니다.

```
10, 11, echo_request
```

시스템은 OR 연산자를 사용하여 사용자가 나열하는 각 값 또는 문자열에 일치시킵니다. 사용자가 값 및 문자열을 표시하는 순서는 상관 없습니다. 목록의 단일 값 또는 문자열과 키워드를 일치시킵니다. 인식되지 않은 문자열 또는 외부 범위 값을 포함하는 규칙을 저장하려고 하는 경우 오류 메시지가 표시됩니다.

동일한 메시지 유형을 위한 서로 다른 값을 사용하는 다양한 GTP 버전이 표에 있다는 점에 유의하십시오. 예를 들어, `sgsn_context_request` 메시지 유형은 GTPv0 및 GTPv1에서 50의 값을 갖지만, GTPv2에서는 130의 값을 갖습니다.

패킷의 버전 번호에 따라 `gtp_type` 키워드는 서로 다른 값에 일치합니다. 위의 예제에서, 키워드는 GTPv0 또는 GTPv1 패킷의 메시지 유형 값 50 및 GTPv2 패킷의 값 130에 일치합니다. 패킷의 메시지 유형 값이 패킷에 지정된 버전에 대해 알려진 값이 아닌 경우 패킷이 키워드에 일치하지 않습니다.

메시지 유형을 위해 정수를 지정한 경우, 키워드의 메시지 유형이 GTP 패킷의 값에 일치하는 경우, 패킷에 지정된 버전에 관계없이 키워드는 일치합니다.

다음 표에서는 각 GTP 메시지 유형에 대해 시스템에서 인식하는 정의된 값 및 문자열을 나열합니다.

표 23-41 GTP 메시지 유형

값	버전 0	버전 1	버전 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	해당 없음
5	node_alive_response	node_alive_response	해당 없음
6	redirection_request	redirection_request	해당 없음
7	redirection_response	redirection_response	해당 없음
16	create_pdp_context_request	create_pdp_context_request	해당 없음
17	create_pdp_context_response	create_pdp_context_response	해당 없음
18	update_pdp_context_request	update_pdp_context_request	해당 없음
19	update_pdp_context_response	update_pdp_context_response	해당 없음
20	delete_pdp_context_request	delete_pdp_context_request	해당 없음
21	delete_pdp_context_response	delete_pdp_context_response	해당 없음
22	create_aa_pdp_context_request	init_pdp_context_activation_request	해당 없음
23	create_aa_pdp_context_response	init_pdp_context_activation_response	해당 없음
24	delete_aa_pdp_context_request	해당 없음	해당 없음
25	delete_aa_pdp_context_response	해당 없음	해당 없음
26	error_indication	error_indication	해당 없음
27	pdu_notification_request	pdu_notification_request	해당 없음

표 23-41 GTP 메시지 유형 (계속)

값	버전 0	버전 1	버전 2
28	pdu_notification_response	pdu_notification_response	해당 없음
29	pdu_notification_reject_request	pdu_notification_reject_request	해당 없음
30	pdu_notification_reject_response	pdu_notification_reject_response	해당 없음
31	해당 없음	supported_ext_header_notification	해당 없음
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	해당 없음	해당 없음	change_notification_request
39	해당 없음	해당 없음	change_notification_response
48	identification_request	identification_request	해당 없음
49	identification_response	identification_response	해당 없음
50	sgsn_context_request	sgsn_context_request	해당 없음
51	sgsn_context_response	sgsn_context_response	해당 없음
52	sgsn_context_ack	sgsn_context_ack	해당 없음
53	해당 없음	forward_relocation_request	해당 없음
54	해당 없음	forward_relocation_response	해당 없음
55	해당 없음	forward_relocation_complete	해당 없음
56	해당 없음	relocation_cancel_request	해당 없음
57	해당 없음	relocation_cancel_response	해당 없음
58	해당 없음	forward_srns_contex	해당 없음
59	해당 없음	forward_relocation_complete_ack	해당 없음
60	해당 없음	forward_srns_contex_ack	해당 없음
64	해당 없음	해당 없음	modify_bearer_command
65	해당 없음	해당 없음	modify_bearer_failure_indication
66	해당 없음	해당 없음	delete_bearer_command
67	해당 없음	해당 없음	delete_bearer_failure_indication
68	해당 없음	해당 없음	bearer_resource_command
69	해당 없음	해당 없음	bearer_resource_failure_indication
70	해당 없음	ran_info_relay	downlink_failure_indication
71	해당 없음	해당 없음	trace_session_activation
72	해당 없음	해당 없음	trace_session_deactivation
73	해당 없음	해당 없음	stop_paging_indication
95	해당 없음	해당 없음	create_bearer_request

표 23-41 GTP 메시지 유형 (계속)

값	버전 0	버전 1	버전 2
96	해당 없음	mbms_notification_request	create_bearer_response
97	해당 없음	mbms_notification_response	update_bearer_request
98	해당 없음	mbms_notification_reject_request	update_bearer_response
99	해당 없음	mbms_notification_reject_response	delete_bearer_request
100	해당 없음	create_mbms_context_request	delete_bearer_response
101	해당 없음	create_mbms_context_response	delete_pdn_request
102	해당 없음	update_mbms_context_request	delete_pdn_response
103	해당 없음	update_mbms_context_response	해당 없음
104	해당 없음	delete_mbms_context_request	해당 없음
105	해당 없음	delete_mbms_context_response	해당 없음
112	해당 없음	mbms_register_request	해당 없음
113	해당 없음	mbms_register_response	해당 없음
114	해당 없음	mbms_deregister_request	해당 없음
115	해당 없음	mbms_deregister_response	해당 없음
116	해당 없음	mbms_session_start_request	해당 없음
117	해당 없음	mbms_session_start_response	해당 없음
118	해당 없음	mbms_session_stop_request	해당 없음
119	해당 없음	mbms_session_stop_response	해당 없음
120	해당 없음	mbms_session_update_request	해당 없음
121	해당 없음	mbms_session_update_response	해당 없음
128	해당 없음	ms_info_change_request	identification_request
129	해당 없음	ms_info_change_response	identification_response
130	해당 없음	해당 없음	sgsn_context_request
131	해당 없음	해당 없음	sgsn_context_response
132	해당 없음	해당 없음	sgsn_context_ack
133	해당 없음	해당 없음	forward_relocation_request
134	해당 없음	해당 없음	forward_relocation_response
135	해당 없음	해당 없음	forward_relocation_complete
136	해당 없음	해당 없음	forward_relocation_complete_ack
137	해당 없음	해당 없음	forward_access
138	해당 없음	해당 없음	forward_access_ack
139	해당 없음	해당 없음	relocation_cancel_request
140	해당 없음	해당 없음	relocation_cancel_response
141	해당 없음	해당 없음	configuration_transfer_tunnel
149	해당 없음	해당 없음	detach
150	해당 없음	해당 없음	detach_ack

표 23-41 GTP 메시지 유형 (계속)

값	버전 0	버전 1	버전 2
151	해당 없음	해당 없음	cs_paging
152	해당 없음	해당 없음	ran_info_relay
153	해당 없음	해당 없음	alert_mme
154	해당 없음	해당 없음	alert_mme_ack
155	해당 없음	해당 없음	ue_activity
156	해당 없음	해당 없음	ue_activity_ack
160	해당 없음	해당 없음	create_forward_tunnel_request
161	해당 없음	해당 없음	create_forward_tunnel_response
162	해당 없음	해당 없음	suspend
163	해당 없음	해당 없음	suspend_ack
164	해당 없음	해당 없음	resume
165	해당 없음	해당 없음	resume_ack
166	해당 없음	해당 없음	create_indirect_forward_tunnel_request
167	해당 없음	해당 없음	create_indirect_forward_tunnel_response
168	해당 없음	해당 없음	delete_indirect_forward_tunnel_request
169	해당 없음	해당 없음	delete_indirect_forward_tunnel_response
170	해당 없음	해당 없음	release_access_bearer_request
171	해당 없음	해당 없음	release_access_bearer_response
176	해당 없음	해당 없음	downlink_data
177	해당 없음	해당 없음	downlink_data_ack
179	해당 없음	해당 없음	pgw_restart
180	해당 없음	해당 없음	pgw_restart_ack
200	해당 없음	해당 없음	update_pdn_request
201	해당 없음	해당 없음	update_pdn_response
211	해당 없음	해당 없음	modify_access_bearer_request
212	해당 없음	해당 없음	modify_access_bearer_response
231	해당 없음	해당 없음	mbms_session_start_request
232	해당 없음	해당 없음	mbms_session_start_response
233	해당 없음	해당 없음	mbms_session_update_request
234	해당 없음	해당 없음	mbms_session_update_response
235	해당 없음	해당 없음	mbms_session_stop_request
236	해당 없음	해당 없음	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	해당 없음
241	data_record_transfer_response	data_record_transfer_response	해당 없음
254	해당 없음	end_marker	해당 없음
255	pdu	pdu	해당 없음

GTP 메시지 유형을 지정하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **gtp_type**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`gtp_type` 키워드가 나타납니다.

단계 2 메시지 유형, 정의된 문자열 또는 모든 조합 중 하나 또는 모두의 쉼표로 구분된 목록에 대한 정의된 십진수 값 0 - 255를 지정합니다. 시스템에서 인식되는 값 및 문자열은 GTP 메시지 유형 표를 참고하십시오.

gtp_info

GTP 메시지는 여러 요소 정보를 포함할 수 있는데, 이들 각각은 정의된 숫자 값 및 정의된 문자열 모두에서 확인됩니다. `gtp_info` 키워드를 `gtp_version` 키워드와 조합하여 사용하여 지정된 정보 요소 시작 시 검사를 시작하고 지정된 정보 요소에 검사를 제한할 수 있습니다.

정보 요소에 대해 정의된 십진수 또는 정의된 문자열을 지정할 수 있습니다. 단일 값 또는 문자열을 지정할 수 있고, 규칙 안에서 여러 `gtp_info` 키워드를 사용하여 여러 요소 정보를 검사할 수 있습니다.

메시지가 동일한 유형의 여러 요소 정보를 포함할 때, 모두가 일치 여부를 위해 검사됩니다. 정보 요소가 잘못된 순서대로 발생하는 경우, 마지막 인스턴스만 검사됩니다.

동일한 정보 요소에 대해 서로 다른 값을 사용하는 다양한 GTP 버전이 있다는 점에 유의하십시오. 예를 들어, `cause`정보 요소는 GTPv0 및 GTPv1에서 1의 값을 갖지만, GTPv2에서는 2의 값을 갖습니다.

패킷의 버전 번호에 따라 `gtp_info` 키워드는 서로 다른 값에 일치합니다. 위의 예제에서, 키워드는 GTPv0 또는 GTPv1 패킷의 정보 요소 값 1 및 GTPv2 패킷의 값 2에 일치합니다. 패킷의 정보 요소 값이 패킷에 지정된 버전에 대해 알려진 값이 아닌 경우 패킷이 키워드에 일치하지 않습니다.

정보 요소 값에 정수를 지정한 경우, 키워드의 메시지 유형이 GTP 패킷의 값에 일치하는 경우, 패킷에 지정된 버전에 관계없이 키워드에 일치합니다.

다음 표에서는 각 GTP 정보 요소에 대해 시스템에서 인식하는 값 및 문자열을 나열합니다.

표 23-42 GTP 정보 요소

값	버전 0	버전 1	버전 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	recovery
4	tlli	tlli	해당 없음
5	p_tmsi	p_tmsi	해당 없음
6	qos	해당 없음	해당 없음
8	recording_required	recording_required	해당 없음
9	authentication	authentication	해당 없음
11	map_cause	map_cause	해당 없음
12	p_tmsi_sig	p_tmsi_sig	해당 없음
13	ms_validated	ms_validated	해당 없음
14	recovery	recovery	해당 없음

표 23-42 GTP 정보 요소 (계속)

값	버전 0	버전 1	버전 2
15	selection_mode	selection_mode	해당 없음
16	flow_label_data_1	teid_1	해당 없음
17	flow_label_signalling	teid_control	해당 없음
18	flow_label_data_2	teid_2	해당 없음
19	ms_unreachable	teardown_ind	해당 없음
20	해당 없음	nsapi	해당 없음
21	해당 없음	ranap	해당 없음
22	해당 없음	rab_context	해당 없음
23	해당 없음	radio_priority_sms	해당 없음
24	해당 없음	radio_priority	해당 없음
25	해당 없음	packet_flow_id	해당 없음
26	해당 없음	charging_char	해당 없음
27	해당 없음	trace_ref	해당 없음
28	해당 없음	trace_type	해당 없음
29	해당 없음	ms_unreachable	해당 없음
71	해당 없음	해당 없음	apn
72	해당 없음	해당 없음	ambr
73	해당 없음	해당 없음	ebi
74	해당 없음	해당 없음	ip_addr
75	해당 없음	해당 없음	mei
76	해당 없음	해당 없음	msisdn
77	해당 없음	해당 없음	indication
78	해당 없음	해당 없음	pco
79	해당 없음	해당 없음	paa
80	해당 없음	해당 없음	bearer_qos
80	해당 없음	해당 없음	flow_qos
82	해당 없음	해당 없음	rat_type
83	해당 없음	해당 없음	serving_network
84	해당 없음	해당 없음	bearer_tft
85	해당 없음	해당 없음	tad
86	해당 없음	해당 없음	uli
87	해당 없음	해당 없음	f_teid
88	해당 없음	해당 없음	tmsi
89	해당 없음	해당 없음	cn_id
90	해당 없음	해당 없음	s103pdf
91	해당 없음	해당 없음	s1udf

표 23-42 GTP 정보 요소 (계속)

값	버전 0	버전 1	버전 2
92	해당 없음	해당 없음	delay_value
93	해당 없음	해당 없음	bearer_context
94	해당 없음	해당 없음	charging_id
95	해당 없음	해당 없음	charging_char
96	해당 없음	해당 없음	trace_info
97	해당 없음	해당 없음	bearer_flag
99	해당 없음	해당 없음	pdn_type
100	해당 없음	해당 없음	pti
101	해당 없음	해당 없음	drx_parameter
103	해당 없음	해당 없음	gsm_key_tri
104	해당 없음	해당 없음	umts_key_cipher_quin
105	해당 없음	해당 없음	gsm_key_cipher_quin
106	해당 없음	해당 없음	umts_key_quin
107	해당 없음	해당 없음	eps_quad
108	해당 없음	해당 없음	umts_key_quad_quin
109	해당 없음	해당 없음	pdn_connection
110	해당 없음	해당 없음	pdn_number
111	해당 없음	해당 없음	p_tmsi
112	해당 없음	해당 없음	p_tmsi_sig
113	해당 없음	해당 없음	hop_counter
114	해당 없음	해당 없음	ue_time_zone
115	해당 없음	해당 없음	trace_ref
116	해당 없음	해당 없음	complete_request_msg
117	해당 없음	해당 없음	guti
118	해당 없음	해당 없음	f_container
119	해당 없음	해당 없음	f_cause
120	해당 없음	해당 없음	plmn_id
121	해당 없음	해당 없음	target_id
123	해당 없음	해당 없음	packet_flow_id
124	해당 없음	해당 없음	rab_contex
125	해당 없음	해당 없음	src_rnc_pdcp
126	해당 없음	해당 없음	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	해당 없음

표 23-42 GTP 정보 요소 (계속)

값	버전 0	버전 1	버전 2
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	해당 없음	qos	node_type
136	해당 없음	authentication_qu	fqdn
137	해당 없음	tft	ti
138	해당 없음	target_id	mbms_session_duration
139	해당 없음	utran_trans	mbms_service_area
140	해당 없음	rab_setup	mbms_session_id
141	해당 없음	ext_header	mbms_flow_id
142	해당 없음	trigger_id	mbms_ip_multicast
143	해당 없음	omc_id	mbms_distribution_ack
144	해당 없음	ran_trans	rfsp_index
145	해당 없음	pdp_context_pri	uci
146	해당 없음	addi_rab_setup	csg_info
147	해당 없음	sgsn_number	csg_id
148	해당 없음	common_flag	cmi
149	해당 없음	apn_restriction	service_indicator
150	해당 없음	radio_priority_lcs	detach_type
151	해당 없음	rat_type	ldn
152	해당 없음	user_loc_info	node_feature
153	해당 없음	ms_time_zone	mbms_time_to_transfer
154	해당 없음	imei_sv	throttling
155	해당 없음	camel	arp
156	해당 없음	mbms_ue_context	epc_timer
157	해당 없음	tmp_mobile_group_id	signalling_priority_indication
158	해당 없음	rim_routing_addr	tmgi
159	해당 없음	mbms_config	mm_srvcc
160	해당 없음	mbms_service_area	flags_srvcc
161	해당 없음	src_rnc_pdcp	nmbr
162	해당 없음	addi_trace_info	해당 없음
163	해당 없음	hop_counter	해당 없음
164	해당 없음	plmn_id	해당 없음
165	해당 없음	mbms_session_id	해당 없음
166	해당 없음	mbms_2g3g_indicator	해당 없음

표 23-42 GTP 정보 요소 (계속)

값	버전 0	버전 1	버전 2
167	해당 없음	enhanced_nsapi	해당 없음
168	해당 없음	mbms_session_duration	해당 없음
169	해당 없음	addi_mbms_trace_info	해당 없음
170	해당 없음	mbms_session_repetition_num	해당 없음
171	해당 없음	mbms_time_to_data	해당 없음
173	해당 없음	bss	해당 없음
174	해당 없음	cell_id	해당 없음
175	해당 없음	pdu_num	해당 없음
177	해당 없음	mbms_bearer_capab	해당 없음
178	해당 없음	rim_routing_disc	해당 없음
179	해당 없음	list_pfc	해당 없음
180	해당 없음	ps_xid	해당 없음
181	해당 없음	ms_info_change_report	해당 없음
182	해당 없음	direct_tunnel_flags	해당 없음
183	해당 없음	correlation_id	해당 없음
184	해당 없음	bearer_control_mode	해당 없음
185	해당 없음	mbms_flow_id	해당 없음
186	해당 없음	mbms_ip_multicast	해당 없음
187	해당 없음	mbms_distribution_ack	해당 없음
188	해당 없음	reliable_inter_rat_handover	해당 없음
189	해당 없음	rfsp_index	해당 없음
190	해당 없음	fqdn	해당 없음
191	해당 없음	evolved_allocation1	해당 없음
192	해당 없음	evolved_allocation2	해당 없음
193	해당 없음	extended_flags	해당 없음
194	해당 없음	uci	해당 없음
195	해당 없음	csg_info	해당 없음
196	해당 없음	csg_id	해당 없음
197	해당 없음	cmi	해당 없음
198	해당 없음	apn_ambr	해당 없음
199	해당 없음	ue_network	해당 없음
200	해당 없음	ue_ambr	해당 없음
201	해당 없음	apn_ambr_nsapi	해당 없음
202	해당 없음	ggsn_backoff_timer	해당 없음
203	해당 없음	signalling_priority_indication	해당 없음
204	해당 없음	signalling_priority_indication_nsapi	해당 없음

표 23-42 GTP 정보 요소 (계속)

값	버전 0	버전 1	버전 2
205	해당 없음	high_bitrate	해당 없음
206	해당 없음	max_mbr	해당 없음
251	charging_gateway_addr	charging_gateway_addr	해당 없음
255	private_extension	private_extension	private_extension

다음 절차를 사용하여 GTP 정보 요소를 지정할 수 있습니다.

GTP 정보 요소를 지정하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **gtp_info**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`gtp_info` 키워드가 나타납니다.

단계 2 정보 요소에 대해 단일 정의된 십진수 0에서 255 또는 단일 정의된 문자열을 지정합니다. 시스템에서 인식되는 값 및 문자열은 GTP 정보 요소 표를 참고하십시오.

Modbus 키워드

라이센스: 보호

Modbus 키워드를 사용하여 Modbus 요청 또는 응답 내 Data(데이터) 필드의 시작 부분을 나타내고, Modbus 기능 코드 및 Modbus 장치 ID에 일치시킬 수 있습니다. Modbus 키워드는 단독으로 또는 `content` 및 `byte_jump`와 같은 다른 키워드와 조합하여 사용할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-73페이지의 modbus_data
- 23-74페이지의 modbus_func
- 23-75페이지의 modbus_unit

modbus_data

`modbus_data` 키워드를 사용하여 Modbus(모드버스) 요청 또는 응답 내 Data(데이터) 필드의 시작 부분을 나타낼 수 있습니다.

Modbus Data(모드버스 데이터) 필드의 시작 부분을 나타내려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **modbus_data**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`modbus_data` 키워드가 나타납니다.

`modbus_data` 키워드는 인수를 갖지 않습니다.

modbus_func

modbus_func 키워드를 사용하여 Modbus(모드버스) 애플리케이션 레이어 요청 또는 응답 헤더의 Function Code(기능 코드) 필드에 대해 일치하도록 할 수 있습니다. Modbus(모드버스) 기능 코드에 대해 단일 정의된 십진수 또는 단일 정의된 문자열을 지정할 수 있습니다.

다음 표에서는 Modbus(모드버스) 기능 코드를 위한 시스템에서 인식하는 정의된 값 및 문자열을 나열합니다.

표 23-43 모드버스 기능 코드

값	문자열
1	read_coils
2	read_discrete_inputs
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

Modbus(모드버스) 기능 코드를 지정하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **modbus_func**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

modbus_func 키워드가 나타납니다.

단계 2 기능 코드에 대해 단일 정의된 십진수 0에서 255 또는 단일 정의된 문자열을 지정합니다. 시스템에서 인식되는 값 및 문자열은 모드버스 기능 코드 표를 참고하십시오.

modbus_unit

modbus_unit 키워드를 사용하여 Modbus(모드버스) 요청 또는 응답 헤더에 Unit ID(장치 ID) 필드에 대한 단일 십진수와 일치시킬 수 있습니다.

Modbus(모드버스) 장치 ID를 지정하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **modbus_unit**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

modbus_unit 키워드가 나타납니다.

단계 2 십진수 0~255를 지정합니다.

DNP3 키워드

라이센스: 보호

DNP3 키워드를 사용하여 애플리케이션 레이어 조각의 시작 부분을 나타낼 수 있고, DNP3 기능 코드 및 DNP3 응답과 요청 내 개체에 일치시킬 수 있으며 DNP3 응답의 내부 디스플레이 플래그에 일치시킬 수도 있습니다. DNP3 키워드는 단독으로 또는 content 및 byte_jump와 같은 다른 키워드와 조합하여 사용할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-75페이지의 dnp3_data
- 23-76페이지의 dnp3_func
- 23-77페이지의 dnp3_ind
- 23-78페이지의 dnp3_obj

dnp3_data

리어셈블된 DNP3 애플리케이션 레이어 조각의 시작 부분을 나타낼 때 dnp3_data 키워드를 사용할 수 있습니다.

DNP3 전처리기는 연결 레이어 프레임을 애플리케이션 레이어 조각으로 리어셈블합니다. dnp3_data 키워드는 각 애플리케이션 레이어 조각의 시작 부분을 나타냅니다. 다른 규칙 옵션은 데이터를 구분하고 매 16 바이트마다 체크섬을 추가할 필요 없이 단편 내 리어셈블된 데이터를 일치시킬 수 있습니다.

리어셈블된 DNP3 조각의 시작 부분을 나타내려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **modbus_data**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

dnp3_data 키워드가 나타납니다.

dnp3_data 키워드는 인수를 갖지 않습니다.

dnp3_func

dnp3_func 키워드를 사용하여 DNP3 애플리케이션 레이어 요청 또는 응답 헤더의 Function Code(기능 코드) 필드에 일치시킬 수 있습니다. DNP3 기능 코드에 대해 단일 정의된 십진수 또는 단일 정의된 문자열을 지정할 수 있습니다.

다음 표에서는 DNP3 기능 코드의 시스템에서 인식하는 정의된 값 및 문자열을 나열합니다.

표 23-44 DNP3 기능 코드

값	문자열
0	confirm
1	read
2	write
3	select
4	operate
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file

표 23-44 DNP3 기능 코드 (계속)

값	문자열
31	activate_config
32	authenticate_req
33	authenticate_err
129	대응
130	unsolicited_response
131	authenticate_resp

DNP3 기능 코드를 지정하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **dnp3_func**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`dnp3_func` 키워드가 나타납니다.

단계 2 기능 코드에 대해 단일 정의된 십진수 0에서 255 또는 단일 정의된 문자열을 지정합니다. 시스템에서 인식되는 값 및 문자열은 DNP3 기능 코드 표를 참고하십시오.

dnp3_ind

`dnp3_ind` 키워드를 사용하여 DNP3 애플리케이션 레이어 응답 헤더의 Internal Indications(내부 표시) 필드의 플래그에 일치시킬 수 있습니다.

알려진 단일 플래그에 대한 문자열 또는 다음의 예시에 표시된 대로 쉼표로 구분된 플래그 목록을 지정할 수 있습니다.

```
class_1_events, class_2_events
```

여러 플래그를 지정할 때, 키워드는 목록의 모든 플래그에 일치시킵니다. 플래그 조합을 검색하려면, 규칙에서 `dnp3_ind` 키워드를 여러 번 사용합니다.

다음 목록은 정의된 DNP3 내부 표시 플래그를 시스템에서 인식하는 문자열 구문을 제공합니다.

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

DNP3 내부 표시 플래그를 지정하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **dnp3_ind**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`dnp3_ind` 키워드가 나타납니다.

단계 2 알려진 단일 플래그에 대한 문자열 또는 쉼표로 구분된 플래그 목록을 지정할 수 있습니다.

dnp3_obj

`dnp3_obj` 키워드를 사용하여 요청 또는 응답의 DNP3 개체 헤더에 일치시킬 수 있습니다.

DNP3 데이터는 아날로그 입력 및 이진 입력 등과 같은 다양한 유형의 일련의 DNP3 개체로 구성됩니다. 각 유형은 아날로그 입력 그룹, 이진 입력 그룹과 같이 *그룹*으로 식별되는데, 이들 각각은 십진수 값으로 식별됩니다. 각 그룹의 개체는 16비트 정수, 32비트 정수, 짧은 부동 소수점 등과 같은 *개체 변수*에 의해 추가 식별되며 이들 각각은 개체의 데이터 형식을 지정합니다. 각 유형의 개체 변수는 또한 십진수로 식별할 수 있습니다.

개체 헤더 그룹 유형에 대한 십진수 및 개체 변수 유형에 대한 십진수를 지정하여 개체 헤더를 식별합니다. 이 둘의 조합은 DNP3 개체의 특정 유형을 정의합니다.

DNP3 개체를 지정하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **dnp3_obj**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`dnp3_obj` 키워드가 나타납니다.

단계 2 십진수 0~255를 지정하여 알려진 객체 그룹을 식별하고, 다른 십진수 0~255를 지정하여 알려진 개체 변수 유형을 식별합니다.

패킷 특성 검사

라이센스: 보호

특정 패킷 특성을 가진 패킷에 대해서만 이벤트를 생성하는 규칙을 작성할 수 있습니다. ASA FirePOWER 모듈은 패킷 특성을 평가하는 데 다음 키워드를 제공합니다.

- 23-79페이지의 dsize
- 23-79페이지의 isdataat
- 23-80페이지의 sameip
- 23-80페이지의 fragoffset
- 23-80페이지의 cvs

dsize

라이센스: 보호

dsize 키워드는 패킷 페이로드 크기를 테스트합니다. 이 키워드와 보다 큼 연산자 및 보다 작음 연산자(<와 >)를 사용하여 값의 범위를 지정할 수 있습니다. 다음 구문을 사용하여 범위를 지정할 수 있습니다.

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

예를 들어, 400바이트보다 큰 패킷 크기를 나타내려면, dtype 값으로 >400을 사용합니다. 500바이트 미만의 패킷 크기를 나타내려면, <500을 사용합니다. 400바이트와 500바이트 사이의 모든 패킷에 대한 규칙 트리거를 포함하는 것으로 지정하려면, 400<>500를 사용합니다.

주의 dsize 키워드는 모든 전처리기가 해독하기 전에 패킷을 테스트합니다.

isdataat

라이센스: 보호

isdataat 키워드는 데이터가 페이로드의 특정 위치에 있다는 것을 규칙 엔진이 확인하도록 지시합니다.

다음 표에서는 isdataat 키워드와 함께 사용할 수 있는 인수를 나열합니다.

표 23-45 isdataat 인수

인수	유형	설명
Offset(오프셋)	필수	페이로드에서 특정 위치입니다. 예를 들어, 패킷 페이로드에서 데이터가 50바이트에 나타난다는 것을 테스트하려면, 오프셋 값으로 50을 지정합니다. ! 수식자는 isdataat 테스트의 결과를 무효화합니다. 페이로드에 일정량의 데이터가 나타나지 않으면 경고합니다. 기존의 byte_extract 변수를 사용하여 이 인수에 대한 값을 지정할 수 있습니다. 자세한 내용은 23-81페이지의 패킷 데이터를 키워드 인수로 읽어 들이기를 참고하십시오.
Relative	선택 사항	위치가 마지막으로 성공한 콘텐츠 일치와 연결되도록 합니다. 상대적 위치를 지정한 경우, 카운터가 0바이트에서 시작하므로, 계산하는 마지막으로 성공한 콘텐츠 일치에서 앞으로 이동할 바이트 수에서 1를 빼 위치를 계산한다는 점에 유의하십시오. 예를 들어, 데이터가 마지막으로 성공한 콘텐츠 일치 후 아홉 번째 바이트에 표시되도록 지정하려면, 8의 상대적 오프셋을 지정합니다.
Raw Data	선택 사항	데이터가ASA FirePOWER 모듈 전처리기에서 암호 해독 또는 애플리케이션 레이어 표준화가 이루어지기 전에 원래 패킷 페이로드에 위치하도록 지정합니다. 이전 콘텐츠 일치 항목이 원시 데이터 패킷에 있는 경우 이 인수를 **Relative(연결)**와 함께 사용할 수 있습니다.

예를 들어, 콘텐츠 foo를 검색하는 규칙에서 isdataat에 대한 값이 다음과 같이 지정될 경우

- Offset =!10
- Relative = 활성화

페이로드가 끝나기 전 foo 다음에 오는 10바이트를 규칙 엔진이 탐지하지 않는 경우 시스템에서 경고합니다.

isdataat를 사용하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 isdataat를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

isdataat 섹션이 나타납니다.

sameip

라이센스: 보호

sameip 키워드는 패킷의 소스와 대상 IP 주소가 동일한지 테스트합니다. 이 키워드는 인수를 취하지 않습니다.

fragoffset

라이센스: 보호

fragoffset 키워드는 단편화된 패킷의 오프셋을 테스트합니다. (WinNuke 서비스 거부 공격과 같은) 일부 공격이 특정 오프셋을 가진 수동 생성된 패킷 조각을 사용하기 때문에 이 기능은 유용합니다.

예를 들어, 단편화된 패킷의 오프셋이 31337바이트인지 여부를 테스트하려면, fragoffset 값으로 31337을 지정합니다.

fragoffset 키워드에 인수를 지정할 때 다음 연산자를 사용할 수 있습니다.

표 23-46 fragoffset 키워드 인수 연산자

연산자	설명
!	not
>	보다 큼
<	보다 작음

not 연산자(!)를 < 또는 >와 조합하여 사용할 수 없음에 유의하십시오.

cvs

라이센스: 보호

cvs 키워드는 잘못된 형식의 CVS 항목에 대해 Concurrent Versions System(공동 버전 시스템, CVS) 트래픽을 테스트합니다. 공격자는 잘못된 형식의 항목을 사용하여 힙 오버플로를 강제하고 CSV 서버에서 악성 코드를 실행할 수 있습니다. 이 키워드는 두 개의 알려진 CVS 취약성에 대한 공격을 식별하는 데 사용될 수 있습니다. CVE-2004-0396(CVS 1.11 x~1.11.15, 1.12 x~1.12.7) 및 CVS-2004-0414(CVS 1.12 x~1.12.8, 1.11 x~1.11.16). cvs 키워드는 잘 형성된 항목을 점검하며 잘못된 형식의 항목이 발견되면 경고를 생성합니다.

사용자 규칙은 CVS 실행 포트를 포함해야 합니다. 또한, 트래픽이 발생할 수 있는 모든 포트는 CVS 세션을 위해 상태가 유지될 수 있도록 TCP 정책 내 스트림 리어셈블리에 대한 포트 목록에 추가해야 합니다. TCP 포트 2401(pserver) 및 514(rsh)는 스트림 리어셈블리가 발생하는 클라이언트 포트 목록에 포함됩니다. 그러나 사용자 서버가 xinetd 서버(즉, pserver)로 실행되는 경우, 이는 모든 TCP 포트에서 실행될 수 있다는 점에 유의하십시오. 스트림 리어셈블리 **Client Ports(클라이언트 포트)** 목록에 모든 비표준 포트를 추가합니다. 자세한 내용은 17-27페이지의 스트림 리어셈블리 옵션 선택을 참고하십시오.

잘못된 형식의 CVS 항목을 검색하려면 다음을 수행합니다.

단계 1 규칙에 cvs 옵션을 추가하고 키워드 인수로 invalid-entry를 입력합니다.

패킷 데이터를 키워드 인수로 읽어들이기

라이센스: 보호

byte_extract 키워드를 사용하여 패킷에서 지정한 바이트 수를 변수로 읽어들일 수 있습니다. 해당 변수는 나중에 동일한 규칙에서 다른 특정 검색 키워드 내 특정 인수에 대한 값으로 사용할 수 있습니다.

예를 들면, 이는 특정 세그먼트 바이트가 패킷 내 데이터에 포함된 바이트 수를 나타내는 패킷에서 데이터 크기를 추출하는 데 유용합니다. 예를 들어, 특정 세그먼트 바이트는 후속 데이터가 4바이트로 구성되어 있다고 표시할 수 있습니다. 사용자는 사용자 변수 값으로 사용하기 위해 4바이트의 데이터 크기를 추출할 수 있습니다.

byte_extract를 사용하여 규칙에서 최대 두 개의 개별 변수를 동시에 만들 수 있습니다. 몇 번이든 byte_extract 변수를 재정의할 수 있습니다. 동일한 변수 이름 및 기타 변수 정의를 새로운 byte_extract 키워드와 함께 입력하면 해당 변수의 이전 정의를 덮어씁니다.

다음 표에서는 byte_extract 키워드가 요구하는 인수를 설명합니다.

표 23-47 필수 byte_extract 인수

인수	설명
Bytes to Extract	패킷에서 추출할 바이트 수. 1, 2, 3, 4 바이트를 지정할 수 있습니다.
Offset	데이터 추출을 시작할 페이로드 내 바이트 수. -65534에서 65535까지 바이트를 지정할 수 있습니다. 오프셋 카운터는 0바이트에서 시작하므로, 계산에 넣으려는 바이트 수에서 1을 뺀 오프셋 값을 계산합니다. 예를 들어, 8바이트를 계산에 넣으려면 7을 지정합니다. 규칙 엔진은 패킷의 페이로드의 처음부터 계산에 넣거나 사용자가 또한 **Relative(연결)**를 지정한 경우, 마지막으로 성공한 콘텐츠 일치 후에 계산에 넣습니다. 또한 **Relative(연결)**를 지정할 때만 음수를 지정할 수 있다는 점에 유의하십시오. 자세한 내용은 추가 옵션 byte_extract 인수 표를 참고하십시오.
Variable Name	다른 탐지 키워드에 대한 인수에 사용할 변수 이름입니다. 영숫자 문자열이 반드시 문자로 시작되도록 지정할 수 있습니다.

시스템이 추출할 데이터를 찾는 방식을 더욱 자세히 정의하려면 다음 표에 설명된 인수를 사용할 수 있습니다.

표 23-48 추가 옵션 byte_extract 인수

인수	설명
Multiplier	패킷에서 추출된 값에 대한 승수입니다. 0에서 65535를 지정할 수 있습니다. 승수를 지정하지 않은 경우, 기본값은 1입니다.
Align	가장 가까운 2바이트 또는 4바이트 경계까지 추출한 값을 둘러쌉니다. 또한 **Multiplier**를 선택하는 경우, 시스템은 정렬 전에 승수를 적용합니다.
Relative	**Offset**이 페이로드의 시작 대신 마지막으로 성공한 콘텐츠 일치의 끝에 연결되도록 합니다. 자세한 내용은 필수 byte_extract 인수 표를 참고하십시오.

DCE/RPC, **Endian** 또는 **Number Type** 중 하나만 지정할 수 있습니다.

`byte_extract` 키워드가 테스트할 바이트를 계산하는 방법을 정의하려면, 다음 표의 인수 중에서 선택합니다. 어느 인수도 선택하지 않는 경우 규칙 엔진은 빅 엔디언 바이트 순서를 사용합니다.

표 23-49 엔디언 byte_extract 인수

인수	설명
Big Endian	빅 엔디언 바이트 순서의 프로세스 데이터. 기본 네트워크 바이트 순서입니다.
Little Endian	리틀 엔디언 순서의 프로세스 데이터
DCE/RPC	DCE/RPC 전처리기에서 처리된 트래픽에 `byte_extract` 키워드를 지정합니다. 자세한 내용은 15-2페이지의 DCE/RPC 트래픽 디코딩을 참고하십시오. DCE/RPC 전처리기는 빅 엔디언 또는 리틀 엔디언 바이트 순서를 결정하고, **Number Type** 및 **Endian** 인수는 적용되지 않습니다. 이 인수를 활성화하면, `byte_extract`를 다른 DCE/RPC 특정 키워드와 함께 사용할 수도 있습니다. 자세한 내용은 23-58페이지의 DCE/RPC 키워드를 참고하십시오.

데이터를 ASCII 문자열로 읽으려면 숫자 유형을 지정할 수 있습니다. 다음 표에 있는 인수 중 하나를 선택하여 패킷 내 문자열 데이터를 보는 방식을 정의할 수 있습니다.

표 23-50 번호 유형 byte_extract 인수

인수	설명
Hexadecimal String	추출된 문자열 데이터를 16진수 형태로 읽어들입니다.
Decimal String	추출된 문자열 데이터를 십진수 형태로 읽어들입니다.
Octal String	추출된 문자열 데이터를 8진수 형태로 읽어들입니다.

예를 들어, byte_extract에 대한 값이 다음과 같이 지정된 경우

- Bytes to Extract = 4
- Variable Name = var
- Offset = 8
- Relative = 활성화

규칙 엔진은 마지막으로 성공한 콘텐츠 일치(에 연결)에서 9바이트 떨어져서 나타나는 네 개의 바이트에 설명된 번호를 var로 명명된 변수로 읽어들이는데, 이는 나중에 규칙에서 특정 키워드 인수에 대한 값으로 지정할 수 있습니다.

다음 표는 byte_extract 키워드에 정의된 변수를 지정할 수 있는 키워드 인수를 나열합니다.

표 23-51 byte_extract 변수를 받아들이는 인수

키워드	인수	자세한 내용은 다음을 참고하십시오.
content	Depth, Offset, Distance, Within	23-17페이지의 콘텐츠 일치 제한
byte_jump	Offset(오프셋)	23-30페이지의 byte_jump
byte_test	Offset, Value	23-33페이지의 byte_test
isdataat	Offset(오프셋)	23-79페이지의 isdataat

byte_extract를 사용하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 byte_extract를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

선택한 마지막 키워드 아래에 byte_extract 섹션이 나타납니다.

규칙 키워드로 활성 응답 시작

라이센스: 보호

시스템은 트리거된 TCP 규칙에 대한 응답으로 TCP 연결을 종료하거나 트리거된 UDP 규칙에 대한 응답으로 UDP 세션을 닫는 활성 응답을 시작할 수 있습니다. 두 개의 키워드는 활성 응답을 시작하는 데 구분된 액세스를 제공합니다. 패킷이 키워드 중 하나를 포함하는 규칙을 시작할 때, 시스템은 단일 활성 응답을 시작합니다. config response 명령을 사용하여 수동 배포에서 시도할 TCP 재설정 수 및 수동 배포에서 사용할 활성 응답 인터페이스를 구성할 수 있습니다.

재설정이 연결 또는 세션에 영향을 줄 수 있는 시간에 맞게 도착할 가능성이 크기 때문에 활성 응답은 인라인 배포에서 가장 효과적입니다. 예를 들어, 인라인 배포의 react 키워드에 대한 응답으로, 시스템은 연결의 각 첨단 트래픽에 TCP 재설정(RST) 패킷을 직접 삽입하는데, 이는 보통 연결을 종료하게 합니다.

활성 응답은 방화벽을 대신하는 것이 아닙니다. 여기에는 다양한 이유가 있는데, 시스템이 수동 배포에서 패킷을 삽입할 수 없다는 것과 공격자가 활성 응답을 무시하거나 우회하도록 선택할 수 있다는 점이 포함됩니다.

활성 응답이 다시 라우팅될 수 있기 때문에, 시스템은 TCP 재설정이 TCP 재설정을 시작하도록 허용하지 않습니다. 이는 활성 응답의 무한 시퀀스를 방지합니다. 시스템은 또한 표준 관행에 따라 ICMP에서 연결할 수 없는 패킷이 ICMP에서 연결할 수 없는 패킷을 시작하도록 허용하지 않습니다.

침입 규칙이 활성 응답을 시작한 후 TCP 스트림 전처리기를 구성하여 연결 또는 세션에서 추가 트래픽을 탐지할 수 있습니다. 전처리기가 추가 트래픽을 탐지하면, 연결 또는 세션의 양쪽 끝에 지정된 최대 값까지 추가 활성 응답을 보냅니다. 자세한 내용은 17-2페이지의 침입 드롭 규칙으로 활성 응답 시작을 참고하십시오.

사용자가 활성 응답을 시작하는 데 사용할 수 있는 키워드 관련 정보는 다음 섹션을 참고하십시오.

- 23-84페이지의 유형과 방향으로 활성 응답 시작
- 23-85페이지의 TCP를 재설정하기 전에 HTML 페이지 전송
- 23-86페이지의 활성 응답 재설정 시도 및 인터페이스 설정

유형과 방향으로 활성 응답 시작

라이센스: 보호

규칙 헤더에서 TCP 또는 UDP 프로토콜 지정 여부에 따라 `resp` 키워드를 사용하여 TCP 연결 또는 UDP 세션에 적극적으로 응답할 수 있습니다. 자세한 내용은 23-4페이지의 프로토콜 지정을 참고하십시오.

키워드 인수를 통해 패킷 방향을 지정하고 TCP 재설정(RST) 패킷 또는 ICMP에서 연결할 수 없는 패킷을 활성 응답으로 사용할지 여부를 지정할 수 있습니다.

TCP 재설정(RST) 패킷 또는 ICMP에서 연결할 수 없는 패킷 중 무엇이든 사용하여 TCP 연결을 종료할 수 있습니다. UDP 세션을 종료하려면 ICMP에서 연결할 수 없는 인수만 사용해야 합니다.

다양한 TCP 재설정 인수를 통해 패킷 소스, 대상 또는 둘 다에 대한 활성 응답을 대상으로 할 수도 있습니다. 모든 ICMP에서 연결할 수 없는 인수는 패킷 소스를 대상으로 하며, 이러한 인수를 사용하여 ICMP 네트워크, 호스트, 포트에서 연결할 수 없는 패킷 또는 셋 모두를 사용할지 여부를 지정할 수 있습니다.

다음 표는 규칙이 트리거할 때 ASA FirePOWER 모듈이 수행할 작업을 정확히 지정하기 위해 `resp` 키워드와 함께 사용할 수 있는 인수를 나열합니다.

표 23-52 resp 인수

인수	설명
reset_source	TCP 재설정 패킷을 규칙을 시작했던 패킷을 전송한 엔드 포인트에 보냅니다. 또는, 이전 버전과의 호환성을 위해 지원되는 `rst_snd`를 지정할 수 있습니다.
reset_dest	TCP 재설정 패킷을 규칙을 트리거한 패킷의 해당 대상 엔드 포인트에 보냅니다. 또는, 이전 버전과의 호환성을 위해 지원되는 `rst_rcv`를 지정할 수 있습니다.
reset_both	TCP 재설정 패킷을 전송 및 수신 엔드 포인트 모두에 보냅니다. 또는, 이전 버전과의 호환성을 위해 지원되는 `rst_all`을 지정할 수 있습니다.
icmp_net	ICMP 네트워크에서 연결할 수 없는 메시지를 발신자에게 보냅니다.
icmp_host	ICMP 호스트에서 연결할 수 없는 메시지를 발신자에게 보냅니다.
icmp_port	ICMP 포트에서 연결할 수 없는 메시지를 발신자에게 보냅니다. 이 인수는 UDP 트래픽을 종료하는 데 사용됩니다.
icmp_all	다음 ICMP 메시지를 발신자에게 보냅니다. • 네트워크에서 연결할 수 없음 • 호스트에서 연결할 수 없음 • 포트에서 연결할 수 없음

예를 들어 규칙을 시작할 때, 연결의 양 끝 모두를 재설정하는 규칙을 구성하려면 resp 키워드 값으로 reset_both를 사용합니다.

쉼표로 구분된 목록을 사용하여 다음과 같은 여러 인수를 지정할 수 있습니다.

argument,*argument*,*argument*

config response 명령을 사용하여 수동 배포에서 시도할 TCP 재설정 수 및 수동 배포에서 사용할 활성 응답 인터페이스를 구성하는 것에 대한 자세한 내용은 23-86페이지의 활성 응답 재설정 시도 및 인터페이스 설정을 참고하십시오.

활성 응답을 지정하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **resp**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

resp 키워드가 나타납니다.

단계 2 **resp** 필드의 resp 인수 표에 모든 인수를 지정합니다. 쉼표로 구분된 목록을 사용하여 다음과 같은 여러 인수를 지정할 수 있습니다.

TCP를 재설정하기 전에 HTML 페이지 전송

라이센스: 보호

react 키워드를 사용하여 패킷이 규칙을 트리거할 때 TCP 연결 클라이언트에 기본 HTML 페이지를 보낼 수 있습니다. HTML 페이지를 보낸 후, 시스템은 TCP 재설정 패킷을 사용하여 연결 양쪽 끝에 활성 응답을 시작합니다. react 키워드는 UDP 트래픽에 대한 활성 응답을 시작하지 않습니다.

선택적으로, 다음 인수를 지정할 수 있습니다.

msg

패킷이 msg 인수를 사용하는 react 규칙을 트리거할 때, HTML 페이지는 규칙 이벤트 메시지를 포함합니다. 이벤트 메시지 필드에 대한 설명은 23-2페이지의 규칙 구조의 이해를 참고하십시오.

msg 인수를 지정하지 않은 경우, HTML 페이지는 다음 메시지를 포함합니다.

금지된 사이트에 액세스하려고 합니다.
자세한 내용은 시스템 관리자에게 문의하십시오.

참고 활성 응답이 다시 라우팅될 수 있으므로, HTML 페이지가 react 규칙을 시작하지 않도록 확인합니다. 이는 활성 응답의 무한 시퀀스를 방지합니다. Cisco는 프로덕션 환경에서 이를 활성화하기 전에 react규칙을 광범위하게 테스트하는 것을 권장합니다.

config response 명령을 사용하여 수동 배포에서 시도할 TCP 재설정 수 및 수동 배포에서 사용할 활성 응답 인터페이스를 구성하는 것에 대한 자세한 내용은 23-86페이지의 활성 응답 재설정 시도 및 인터페이스 설정을 참고하십시오.

활성 응답을 시작하기 전에 HTML 페이지를 전송하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **react**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

react 키워드가 나타납니다.

단계 2 다음 2가지 옵션을 사용할 수 있습니다.

- 연결을 종료하기 전에 규칙에 대해 구성된 이벤트 메시지를 포함하는 HTML 페이지를 클라이언트에 전송하려면 **react** 필드에 `msg`를 입력합니다.
- 연결을 종료하기 전에 다음 기본 메시지를 포함하는 HTML 페이지를 클라이언트에 전송하려면, **react** 필드를 비워 둡니다.

```
금지된 사이트에 액세스하려고 합니다.
자세한 내용은 시스템 관리자에게 문의하십시오.
```

활성 응답 재설정 시도 및 인터페이스 설정

라이센스: 보호

config response 명령을 사용하여`resp` 및 `react` 규칙에 의해 시작된 TCP 재설정 작업을 더욱 자세히 구성할 수 있습니다. 이 명령은 또한 드롭 규칙이 시작한 활성 응답의 작업에 영향을 미칩니다. 자세한 내용은 17-2페이지의 침입 드롭 규칙으로 활성 응답 시작을 참고하십시오.

config response 명령을 USER_CONF 고급 변수의 개별 행에 삽입하여 사용할 수 있습니다. USER_CONF 변수 사용에 대한 내용은 2-28페이지의 고급 변수의 이해를 참고하십시오.

주의 기능 설명에서 또는 지원을 통해 침입 정책 기능을 구성하라는 지시를 받지 않은 한 침입 정책 기능을 구성하는 데 `USER_CONF` 고급 변수를 사용하지 **마십시오**. 충돌이나 이중 설정은 시스템을 중단시킵니다.

활성 응답 재설정 시도, 활성 응답 인터페이스 또는 둘 다 지정하려면 다음을 수행합니다.

단계 1 활성 응답의 수만 지정할 것인지, 활성 응답 인터페이스만 지정할 것인지, 또는 둘 다 지정할 것인지 여부에 따라 USER_CONF 고급 변수의 개별 행에 `config response` 명령의 형식을 삽입합니다. 다음 옵션을 이용할 수 있습니다.

- 활성 응답 시도의 수만 지정하려면, 명령을 삽입합니다.
  `config response: attempts att`

  예: `config response: attempts 10`
- 활성 응답 인터페이스만 지정하려면, 명령을 삽입합니다.
  `config response: device dev`

  예: `config response: device eth0`
- 활성 응답 시도 횟수와 활성 응답 인터페이스를 모두 지정하려면 다음 명령을 삽입합니다.
  `config response: attempts att, device dev`

  예: `config response: attempts 10, device eth0`

  여기에서 각 항목은 다음을 나타냅니다.

  *att*는 수신 호스트가 패킷을 수락할 수 있도록 현재 연결 창에서 각 TCP 재설정 패킷을 수신하는 1~20까지의 시도입니다. 이 *strafing* 시퀀스는 수동 배포에만 유용합니다. 인라인 배포에서, 시스템은 패킷 트리거 대신 재설정 패킷을 스트림으로 직접 삽입합니다. 시스템은 ICMP에서 연결할 수 있는 활성 응답을 단 하나만 보냅니다.

  *dev*는 시스템이 수동 배포에서 활성 응답을 전송하거나 인라인 배포에서 활성 응답을 삽입하려는 대체 인터페이스입니다.

필터링 이벤트

라이센스: 보호

지정된 패킷 수가 지정된 시간 안에 규칙을 트리거하지 않는 한 `detection_filter` 키워드를 사용하여 이벤트 생성에서 규칙을 방지할 수 있습니다. 이를 통해 규칙이 조기에 이벤트를 생성하는 것을 중지할 수 있습니다. 예를 들어, 몇 초 동안 둘 또는 세 번의 로그인 실패는 예상된 작업일 수 있지만, 동일한 시간 동안 많은 시도가 있었다면 무차별 암호 대입 공격(brute force attack)을 나타낼 수 있습니다.

`detection_filter` 키워드에는 시스템이 소스 또는 대상 IP 주소를 추적하는지 여부, 이벤트를 트리거하기 전에 탐지 기준이 충족해야 하는 횟수, 횟수를 세는 기간을 정의하는 인수가 필요합니다.

이벤트 트리거를 연기하려면 다음 구문을 사용합니다.

```
track by_src/by_dst, count count, seconds number_of_seconds
```

`track` 인수는 규칙의 탐지 기준에 맞는 패킷 수를 셀 때 패킷의 소스 또는 대상 IP 주소를 사용할지 여부를 지정합니다. 시스템이 이벤트 인스턴스를 추적하는 방식을 지정하려면 다음 표에 설명된 인수 값에서 선택합니다.

표 23-53 detection_filter 추적 인수

인수	설명
by_src	소스 IP 주소로 세는 탐지 기준입니다.
by_dst	대상 IP 주소로 세는 탐지 기준입니다.

`count` 인수는 규칙이 이벤트를 생성하기 전에 지정된 시간 내에 지정된 IP 주소에 대한 규칙을 트리거해야 하는 패킷 수를 지정합니다.

`seconds` 인수는 규칙이 이벤트를 생성하기 전에 패킷의 지정된 수가 규칙을 트리거해야 하는 초를 지정합니다.

콘텐츠 `foo`에 대한 패킷을 검색하고 다음 인수와 함께 `detection_filter` 키워드를 사용하는 규칙의 사례를 고려해 보십시오.

```
track by_src, count 10, seconds 20
```

예제에서, 규칙이 특정 소스 IP 주소에서 20초 내에 10개 패킷에서 `foo`를 탐지할 때까지 이벤트를 생성하지 않습니다. 시스템이 처음 20 초 내에 `foo`를 포함하는 패킷을 7개만 검색할 경우, 어떤 이벤트도 생성되지 않습니다. 그러나,처음 20초 안에 `foo`가 40번 발생하면 규칙은 30개의 이벤트를 생성하고, 20초가 경과할 때 카운트가 다시 시작됩니다.

임계값과 detection_filter 키워드 비교

`detection_filter` 키워드는 더 이상 사용되지 않는 `threshold` 키워드를 대체합니다. `threshold` 키워드는 하위 버전 호환성을 계속 지원하며 침입 정책 안에서 설정한 임계값과 동일하게 실행합니다.

`detection_filter` 키워드는 패킷이 규칙을 트리거하기 전에 적용되는 탐지 기능입니다. 규칙은 지정된 패킷을 카운트하기 전에 탐지된 패킷 트리거에 대한 이벤트를 생성하지 않으며, 인라인 배포에서 규칙이 패킷을 삭제하도록 설정된 경우라도 해당 패킷을 삭제하지 않습니다. 반대로, 규칙은 규칙을 트리거하고 지정된 패킷 수 후에 발생하는 이벤트를 생성하며, 인라인 배포에서 규칙이 패킷을 삭제하도록 설정된 경우라면 해당 패킷을 삭제합니다.

임계값 설정은 탐지 작업으로 귀결되지 않는 이벤트 알림 기능입니다. 이는 패킷이 이벤트를 트리거한 후 적용됩니다. 인라인 배포에서 패킷을 삭제하도록 설정된 규칙은 규칙 임계값과는 별개로 규칙을 트리거하는 모든 패킷을 삭제합니다.

detection_filter 키워드를 침입 이벤트 임계값 설정, 침입 이벤트 억제, 침입 정책의 속도 기반 공격 방지 기능 중 어느 것과도 조합하여 사용할 수 있다는 점을 참고하십시오. 또한 더 이상 사용되지 않는 threshold 키워드를 침입 정책의 침입 이벤트 임계값 설정 기능과 함께 사용하는, 가져온 로컬 규칙을 활성화한 경우 정책 인증이 실패할 수 있다는 점을 참고하십시오. 자세한 내용은 20-22페이지의 이벤트 임계값 설정 구성, 20-26페이지의 침입 정책에 따른 삭제 구성, 20-30페이지의 동적 규칙 상태 설정 및 35-15페이지의 로컬 규칙 파일 가져오기를 참고하십시오.

공격 후 트래픽 평가

라이센스: 보호

tag 키워드를 사용하여 시스템이 호스트 또는 세션에 대한 추가 트래픽을 로깅하도록 지시합니다. tag 키워드를 사용하여 캡처할 트래픽 유형 및 볼륨을 지정할 때 다음 구문을 사용합니다.

tagging_type, count, metric, optional_direction

다음 3개의 표에서는 사용 가능한 기타 인수를 설명합니다.

태그 지정의 2가지 유형을 선택할 수 있습니다. 다음 표에서는 태그 지정의 2가지 유형을 나타냅니다. 침입 규칙에 규칙 헤더 옵션만 구성한 경우 세션 태그 인수 유형은 다른 세션에서 가져온 것과 동일한 세션에서 가져온 패킷을 시스템이 로깅한다는 점에 유의하십시오. 동일한 세션에서 가져온 패킷을 그룹화하려면, 동일한 침입 규칙 내에서 하나 이상의 규칙 옵션(flag 키워드 또는 content 키워드)을 구성합니다.

표 23-54 태그 인수

인수	설명
session	규칙을 트리거한 세션의 패킷을 로깅합니다.
host	규칙을 트리거한 패킷을 전송한 호스트의 패킷을 로깅합니다. 방향 수식자를 추가하여 호스트에서 가져오는 트래픽만 로깅(src)하거나 호스트로 이동하는 트래픽만 로깅(dst)할 수 있습니다.

트래픽을 얼마나 로깅할지 나타내려면 다음 인수를 사용합니다.

표 23-55 count 인수

인수	설명
count	규칙이 트리거된 후 로깅하려는 패킷 또는 시간(초)입니다. 이 측정 단위는 count 인수 다음에 오는 메트릭 인수로 지정됩니다.

다음 표에 설명된 메트릭 중 시간 단위나 트래픽 볼륨으로 로깅하려는 메트릭을 선택하십시오.

주의 높은 대역폭 네트워크는 초당 수 천 개의 패킷을 볼 수 있고, 많은 수의 패킷을 태그하는 것은 성능에 심각한 영향을 미치게 될 수도 있으므로, 네트워크 환경에 맞춰 이 설정을 조정하십시오.

표 23-56 로깅 메트릭 인수

인수	설명
packets	규칙이 트리거된 후 메트릭에 의해 지정된 패킷 수를 로깅합니다.
seconds	규칙이 트리거된 후 메트릭에 의해 지정된 시간(초)를 로깅합니다.

예를 들어, 다음 tag 키워드 값을 가진 규칙이 트리거되면

```
host, 30, seconds, dst
```

다음 30초 동안 클라이언트에서 호스트로 전송된 모든 패킷이 로깅됩니다.

다중 패킷을 포함하는 공격 탐지

라이센스: 보호

flowbits 키워드를 사용하여 세션에 상태 이름을 지정합니다. 이전에 표시된 상태에 따라 세션의 후속 패킷을 분석함으로써, 시스템은 단일 세션에서 여러 패킷을 포함하는 공격을 탐지하고 경고할 수 있습니다.

flowbits 상태 이름은 세션의 특정 부분에서 패킷에 할당된 사용자가 정의한 레이블입니다. 경고하기를 원하지 않는 패킷과 악성 패킷을 구별할 수 있도록 패킷 내용에 따라 상태 이름으로 패킷을 표시할 수 있습니다. 최대 1024개의 상태 이름을 정의할 수 있습니다. 예를 들어, 성공적인 로그인 후에만 발생하는 악성 패킷을 경고하려는 경우, flowbits 키워드를 사용하여 초기 로그인 시도를 구성하는 패킷을 제거할 수 있으므로 악성 패킷에만 집중할 수 있습니다. 먼저 logged_in 상태로 설정된 로그인이 있는 세션의 모든 패킷에 표시하는 규칙을 생성한 다음 flowbits가 첫 번째 규칙에 설정한 상태를 가진 패킷을 확인하고 해당 패킷에만 작동하는 두 번째 규칙을 생성하여 이 작업을 수행할 수 있습니다. 사용자가 로그인되어 있는지 확인하기 위해 flowbits를 사용하는 예를 보려면 23-91페이지의 state_name를 사용하는 flowbits 예제를 참고하십시오.

선택적 *그룹 이름*을 사용하면 상태 그룹에 상태 이름을 포함할 수 있습니다. 상태 이름은 여러 그룹에 속할 수 있습니다. 그룹과 연관되지 않은 상태는 상호 배타적이지 않으며, 따라서 그룹과 연관되지 않은 상태를 트리거하고 설정하는 규칙은 다른 현재 설정 상태에 영향을 주지 않습니다. 그룹에 상태 이름을 포함하는 것이 동일 그룹 내 다른 상태의 설정을 해제함으로써 잘못된 긍정을 어떻게 차단할 수 있는지를 설명하는 예시에 대한 자세한 내용은 23-91페이지의 잘못된 긍정으로 귀결되는 flowbits 예제를 참고하십시오.

다음 표에서는 연산자, 상태 및 flowbits 키워드에 사용 가능한 그룹의 다양한 조합에 대해 설명합니다. 상태 이름은 영숫자 문자, 점(.), 밑줄(_), 대시(-)를 포함할 수 있습니다.

표 23-57 flowbits 옵션

연산자	상태 옵션	그룹	설명
set	state_name	선택 사항	패킷에 대해 지정된 상태를 설정합니다. 그룹이 정의된 경우 지정된 그룹의 상태를 설정합니다.
	state_name&state_name	선택 사항	패킷에 대해 지정된 상태를 설정합니다. 그룹이 정의된 경우 지정된 그룹의 상태를 설정합니다.
setx	state_name	필수	패킷에 대해 지정된 그룹에서 지정한 상태를 설정하고, 그룹의 다른 모든 상태를 해제합니다.
	state_name&state_name	필수	패킷에 대해 지정된 그룹에서 지정한 상태를 설정하고, 그룹의 다른 모든 상태를 해제합니다.
unset	state_name	그룹 없음	패킷에 대해 지정된 상태를 해제합니다.
	state_name&state_name	그룹 없음	패킷에 대해 지정된 상태를 해제합니다.
	all	필수	지정된 그룹의 모든 상태를 해제합니다.

표 23-57 flowbits 옵션 (계속)

연산자	상태 옵션	그룹	설명
toggle	state_name	그룹 없음	설정된 경우 지정된 상태를 해제하고, 해제된 경우 지정된 상태를 설정합니다.
	state_name&state_name	그룹 없음	설정된 경우 지정된 상태를 해제하고, 해제된 경우 지정된 상태를 설정합니다.
	all	필수	지정된 그룹에 설정된 모든 상태를 해제하고, 지정된 그룹에서 해제된 모든 상태를 설정합니다.
isset	state_name	그룹 없음	지정된 상태가 패킷에서 설정되었는지 확인합니다.
	state_name&state_name	그룹 없음	지정된 상태가 패킷에서 설정되었는지 확인합니다.
	state_name|state_name	그룹 없음	지정된 상태 중 무엇이든 패킷에서 설정되었는지 확인합니다.
	any	필수	어느 상태든 지정된 그룹에서 설정되었는지 확인합니다.
	all	필수	모든 상태가 지정된 그룹에서 설정되었는지 확인합니다.
isnotset	state_name	그룹 없음	지정된 상태가 패킷에 설정되지 않았는지 확인합니다.
	state_name&state_name	그룹 없음	지정된 상태가 패킷에 설정되지 않았는지 확인합니다.
	state_name|state_name	그룹 없음	지정된 상태 중 무엇이든 패킷에 설정되지 않았는지 확인합니다.
	any	필수	어느 상태든 패킷에 설정되지 않았는지 확인합니다.
	all	필수	모든 상태가 패킷에 설정되지 않았는지 확인합니다.
reset	(상태 없음)	선택 사항	모든 패킷에 대한 모든 상태를 해제합니다. 그룹이 지정된 경우 그룹의 모든 상태를 해제합니다.
noalert	(상태 없음)	그룹 없음	이를 이벤트 발생을 억제할 다른 모든 연산자와 함께 사용합니다.

flowbits 키워드를 사용할 때 다음 사항에 유의하십시오.

- setx 연산자를 사용할 때, 지정된 상태는 지정된 그룹에만 속하며, 다른 그룹에는 속할 수 없습니다.
- setx 연산자는 여러 번 정의할 수 있으며, 각 인스턴스로 다른 상태와 동일 그룹을 지정합니다.
- setx 연산자를 사용하여 그룹을 지정할 때, 지정된 해당 그룹에서 set, toggle 또는 unset 연산자를 사용할 수 없습니다.
- isset 및 isnotset 연산자는 상태가 그룹 내에 있는지 여부에 상관 없이 지정된 상태를 평가합니다.
- 침입 정책이 저장하는 동안 침입 정책은 재적용되며 액세스 제어 정책은 적용됩니다. (액세스 제어 정책이 하나의 침입 정책 또는 여러 침입 정책을 참조하는지 여부는 상관 없습니다.) 지정된 그룹 **없이** isset 또는 isnotset 연산자를 포함하는 규칙을 활성화하고, 해당하는 상태 이름 및 프로토콜에 대한 flowbits 할당(set, setx, unset, toggle)에 영향을 주는 최소 하나의 규칙을 활성화하지 않는 경우, 해당하는 상태 이름의 flowbits 할당에 영향을 미치는 모든 규칙이 활성화됩니다.
- 침입 정책이 저장하는 동안 침입 정책은 재적용되며 액세스 제어 정책은 적용됩니다. (액세스 제어 정책이 하나의 침입 정책 또는 여러 침입 정책을 참조하는지 여부는 상관 없습니다.) 지정된 그룹**으로** isset 또는 isnotset 연산자를 포함하는 규칙을 활성화하는 경우, flowbits 할당(set, setx, unset, toggle)에 영향을 미치고 해당하는 그룹 이름을 정의하는 모든 규칙이 활성화됩니다.

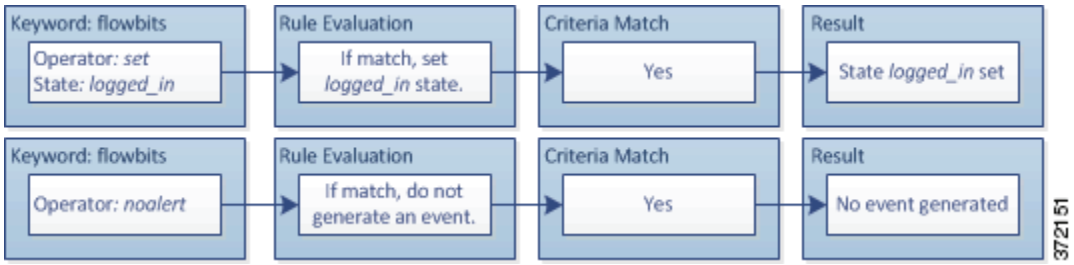
state_name를 사용하는 flowbits 예제

Bugtraq ID #1110에 설명된 IMAP 취약성을 고려하십시오. 이러한 취약성은 IMAP 구현에서 존재하는데, 특히 LIST, LSUB, RENAME, FIND 및 COPY 명령에 존재합니다. 그러나, 취약성을 사용하려면 공격자는 IMAP 서버에 로그인해야 합니다. IMAP 서버의 로그인 인증 및 이후 공격이 다른 패킷에서는 필수적이므로 이 공격을 잡아내는 흐름에 기반하지 않는 규칙을 구성하는 일은 어렵습니다. `flowbits` 키워드를 사용하여, 사용자가 IMAP 서버에 로그인되어 있는지 여부를 추적하는 일련의 규칙을 구성할 수 있으며, 로그인되어 있는 경우, 그리고 공격 중 하나가 탐지된 경우 이벤트를 생성할 수 있습니다. 사용자가 로그인되어 있지 않은 경우, 공격은 취약성을 사용할 수 없고 어떤 이벤트도 생성되지 않습니다.

다음 두 가지 규칙 조각이 이 예를 보여줍니다. 첫 번째 규칙 조각은 IMAP 서버에서 IMAP 로그인 인증을 검색합니다.

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK
LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.

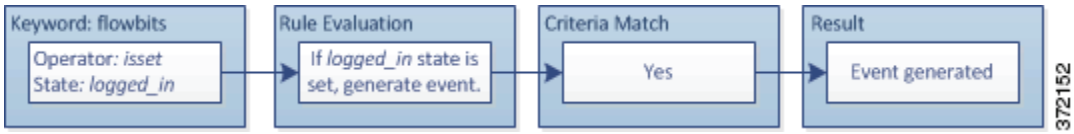


IMAP 서버에서 여러 무해한 로그인 세션을 볼 가능성이 크기 때문에 `flowbits:set`는 `logged_in`의 상태를 설정하는 반면, `flowbits:noalert`는 경고를 억제한다는 점에 유의하십시오.

logged_in 상태가 세션에서 일부의 이전 패킷의 결과로 설정되어 있지 않는 한 다음 규칙 조각은 LIST 문자열을 검색하지만 이벤트를 생성하지 않습니다:

```
alert tcp any any -> any 143 (msg:"IMAP LIST";
content:"LIST"; flowbits:isset,logged_in;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.



이 경우, 이전 패킷이 첫 번째 조각을 포함하는 규칙을 트리거하도록 야기하는 경우, 두 번째 조각을 포함하는 규칙이 트리거되고 이벤트를 생성합니다.

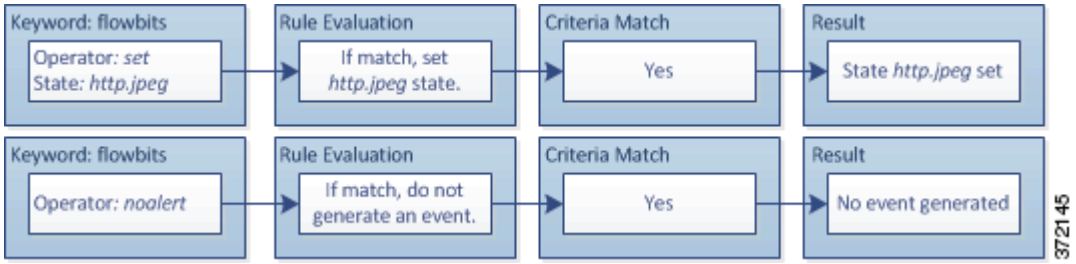
잘못된 긍정으로 귀결되는 flowbits 예제

그룹의 다양한 규칙에 설정된 여러 상태 이름을 포함하는 것은 뒤따르는 패킷의 콘텐츠가 더 이상 유효하지 않은 상태의 규칙에 일치할 때 발생할 가능성이 있는 잘못된 긍정 이벤트를 방지할 수 있습니다. 다음의 예제는 그룹의 여러 상태 이름을 포함하지 않을 때 잘못된 긍정을 얻을 수 있는 방법에 대해 설명합니다.

여기서 단일 세션 동안 표시된 다음 세 가지 규칙 조각이 순서대로 트리거하는 케이스를 고려해 보십시오.

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
flowbits:set,http.jpeg; flowbits:noalert;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.

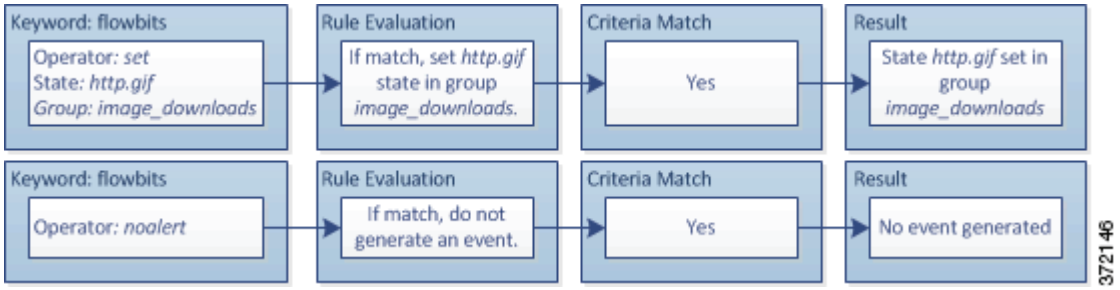


첫 번째 규칙 조각의 `content` 및 `pcre` 키워드는 JPEG 파일 다운로드에 일치하고, `flowbits:set,http.jpeg`는 `http.jpeg` `flowbits` 상태를 설정하며, `flowbits:noalert`는 규칙의 이벤트 생성을 중단합니다. 규칙의 목적은 파일 다운로드를 탐지하고 `flowbits` 상태를 설정하는 것이며 하나 이상의 동반 규칙이 악성 콘텐츠와 조합된 상태 이름을 테스트하여 악성 콘텐츠가 탐지되면 이벤트를 생성할 수 있도록 하는 것이므로 어떤 이벤트도 생성되지 않습니다.

다음 규칙 조각은 위의 JPEG 파일 다운로드 다음에 일어나는 GIF 파일 다운로드를 탐지합니다.

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
flowbits:set,http.tif,image_downloads; flowbits:noalert;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.

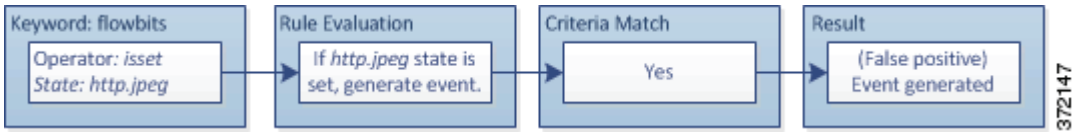


두 번째 규칙의 `content` 및 `pcre` 키워드는 GIF 파일 다운로드에 일치하고, `flowbits:set,http.tif`는 `http.tif` flowbit 상태를 설정하며, `flowbits:noalert`는 규칙의 이벤트 생성을 중단합니다. 첫 번째 규칙 조각에 의해 설정된 `http.jpeg` 상태는 더 이상 필요없더라도 여전히 설정되어 있다는 점에 유의하십시오. 이는 후속 GIF 다운로드가 발견되는 경우 JPEG 다운로드가 반드시 완료되어 있어야 하기 때문입니다.

세 번째 규칙 조각은 첫 번째 규칙 조각에 사용됩니다.

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"
/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.



세 번째 규칙 조각에서, `flowbits:isset,http.jpeg`는 이제는 관련 없는 `http.jpeg` 상태가 설정되고, `content` 및 `pcre`가 JPEG 파일에서는 악성일 수 있지만 GIF 파일에서는 그렇지 않은 콘텐츠에 일치한다는 것을 확인합니다. 세 번째 규칙 조각은 JPEG 파일에는 없는 공격을 위한 잘못된 긍정 이벤트로 귀결됩니다.

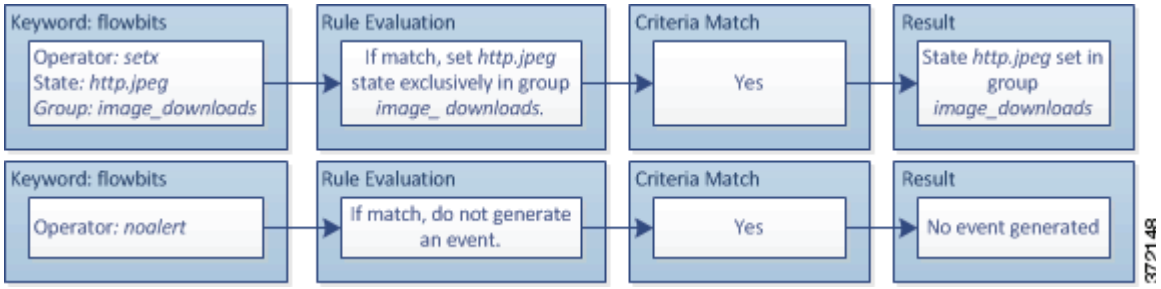
잘못된 긍정 방지를 위한 flowbits 예제

다음의 예시는 그룹에 상태 이름을 포함하고 `setx` 연산자를 사용하여 잘못된 긍정을 차단할 수 있는 방법에 대해 설명합니다.

이전 예와 동일한 경우를 고려하십시오. 이제는 동일한 상태 그룹에서 자신의 두 가지 상태 이름을 포함하는 처음 두 개의 규칙은 제외합니다.

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.

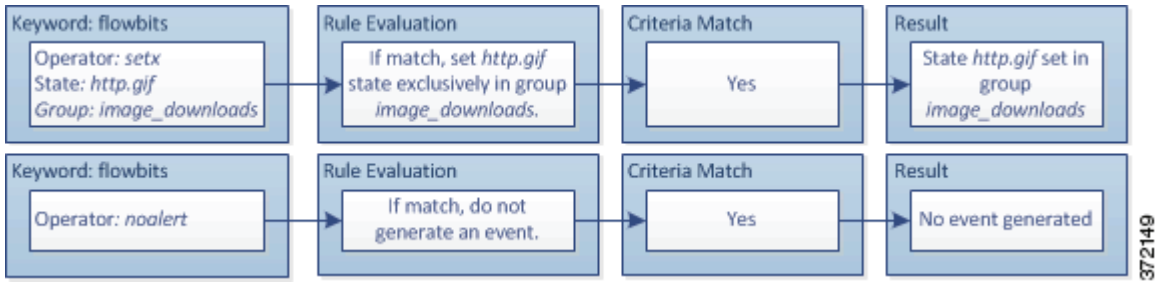


첫 번째 규칙 조각이 JPEG 파일 다운로드를 탐지하면, `flowbits:setx,http.jpeg,image_downloads` 키워드는 `flowbits` 상태를 `http.jpeg`로 설정하고 `image_downloads` 그룹의 상태를 포함합니다.

다음 규칙은 후속 GIF 파일 다운로드를 탐지합니다.

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
flowbits:setx,http.tif,image_downloads; flowbits:noalert;)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.

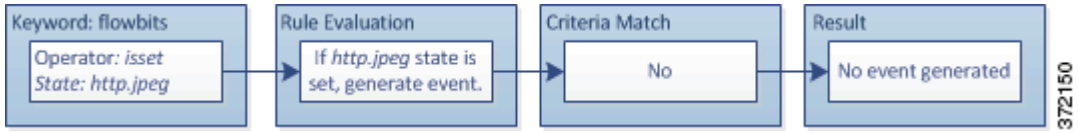


두 번째 규칙 조각이 GIF 파일 다운로드에 일치되면, `flowbits:setx,http.tif,image_downloads` 키워드는 `http.tif flowbits` 상태를 설정하고 그룹의 `http.jpeg` 및 다른 상태의 설정을 해제합니다.

세 번째 규칙 조각이 잘못된 긍정으로 귀결되지 않습니다.

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"/
\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

다음 다이어그램은 앞의 조각 규칙에서 `flowbits` 키워드의 영향에 대해 설명합니다.



`flowbits:isset,http.jpeg`가 거짓이므로, 규칙 엔진은 규칙 처리를 중지하고 어떤 이벤트도 생성되지 않으며, 따라서 GIF 파일 내 콘텐츠가 JPEG 파일에 대한 공격 콘텐츠에 일치하는 경우에도 잘못된 긍정이 차단됩니다.

HTTP 인코딩 유형 및 위치에서 이벤트 생성

라이센스: 보호

http_encode 키워드를 사용하여 표준화 전에 HTTP 요청 또는 응답의 인코딩 유형에서 이벤트를 생성할 수 있습니다. HTTP URI, HTTP 헤더의 비쿠키 데이터, HTTP 요청 헤더의 쿠키 또는 HTTP 응답의 set-cookie 데이터 중 하나에서 가능합니다.

http_encode 키워드를 사용하여 규칙에 대한 일치 항목을 반환하는 HTTP 응답 및 HTTP 쿠키를 검사하는 HTTP Inspect(HTTP 검사) 전처리기를 구성해야 합니다. 자세한 내용은 15-32페이지의 HTTP 트래픽 디코딩 및 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택을 참고하십시오.

또한, HTTP Inspect(HTTP 검사) 전처리기 구성에서 각 특정 인코딩 유형에 대한 디코딩 및 경고 옵션 모두를 활성화하여 침입 규칙의 http_encode 키워드가 해당 인코딩 유형에 이벤트를 트리거할 수 있도록 해야 합니다. 자세한 내용은 15-42페이지의 서버 수준 HTTP 표준화 인코딩 옵션 선택을 참고하십시오.

base36 인코딩 유형이 더 이상 사용되지 않는다는 점을 참고하십시오. 하위 버전 호환성을 위해, 기존 규칙에서는 base36 인수가 허용되지만, 규칙 엔진이 base36 트래픽을 검사하지는 않습니다.

다음 표에서는 이 옵션이 HTTP URI, 헤더, 쿠키 및 set-cookie에서 이벤트를 생성할 수 있는 인코딩 유형을 설명합니다.

표 23-58 http_encode 인코딩 유형

인코딩 유형	설명
utf8	이 인코딩 유형이 HTTP Inspect(HTTP 검사) 전처리기에 의한 디코딩에 대해 활성화되는 경우 지정된 위치에서 UTF - 8 인코딩을 탐지합니다.
double_encode	이 인코딩 유형이 HTTP Inspect(HTTP 검사) 전처리기에 의한 디코딩에 대해 활성화되는 경우 지정된 위치에서 이중 인코딩을 탐지합니다.
non_ascii	비ASCII 문자가 검색되었지만 탐지된 인코딩 유형이 활성화되지 않은 경우 지정된 위치에서 비ASCII 문자를 탐지합니다.
uencode	이 인코딩 유형이 HTTP Inspect(HTTP 검사) 전처리기에 의한 디코딩에 대해 활성화되는 경우 지정된 위치에서 Microsoft %u 인코딩을 탐지합니다.
bare_byte	이 인코딩 유형이 HTTP Inspect(HTTP 검사) 전처리기에 의한 디코딩에 대해 활성화되는 경우 지정된 위치에서 베어 바이트 인코딩을 탐지합니다.

HTTP 인코딩 유형 및 침입 규칙의 위치를 확인하려면 다음을 수행합니다.

단계 1 규칙에 http_encode 키워드를 추가합니다.

단계 2 **Encoding Location(인코딩 위치)** 드롭다운 목록에서 HTTP URI, 헤더, 또는 집합 쿠키를 포함하는 쿠키에서 지정된 인코딩을 검색할지 여부를 선택합니다.

단계 3 다음 중 한 형식을 사용하여 하나 이상의 인코딩 유형을 지정합니다.

```
encode_type
encode_type|encode_type|encode_type...
!encode_type
```

여기서 *encode_type*은 다음 중 하나입니다.

```
utf8, double_encode, non_ascii, uencode, bare_byte
```

부정 연산자(!)와 OR 연산자(|)를 함께 사용할 수 없음에 유의하십시오.

단계 4 또는, 각각에 대한 조건을 AND 연산하기 위해 동일한 규칙에 여러 `http_encode` 키워드를 추가합니다. 예를 들어, 다음 조건과 함께 두 개의 키워드를 입력합니다.

첫 번째 `http_encode` 키워드:

- **Encoding Location(인코딩 위치)**: `HTTP URI`
- **Encoding Type(인코딩 유형)**: `utf8`

추가적인 `http_encode` 키워드:

- **Encoding Location(인코딩 위치)**: `HTTP URI`
- **Encoding Type(인코딩 유형)**: `uencode`

예제 구성은 UTF-8 AND Microsoft IIS %u 인코딩에 대해 HTTP URI를 검색합니다.

파일 유형 및 버전 탐지

라이센스: 보호

`file_type` 및 `file_group` 키워드를 사용하면 FTP, HTTP, SMTP, IMAP, POP3, 그리고 해당 유형 및 버전에 따라 NetBIOS ssn(SMB)을 통해 전송되는 파일을 탐지할 수 있습니다. 단일 침입 규칙에서 하나 이상의 `file_type` 또는 `file_group` 키워드를 사용하지 **마십시오**.

팁 취약성 데이터베이스(VDB)를 업데이트하여 최신 파일 유형, 버전 및 그룹으로 규칙 편집기를 채웁니다. 자세한 내용은 35-8페이지의 취약성 데이터베이스 업데이트를 참고하십시오.

`file_type` 또는 `file_group` 키워드에 일치하는 트래픽에 대한 침입 이벤트를 생성하려면 **반드시** 특정 전처리기를 활성화해야 합니다.

표 23-59 file_type 및 file_group 침입 이벤트 생성

전송 프로토콜	필수 전처리기 또는 전처리기 옵션
FTP	FTP/Telnet 전처리기 및 **Normalize TCP Payload(TCP 페이로드 표준화)** 인라인 표준화 전처리기 옵션은 15-18페이지의 FTP 및 텔넷 트래픽 디코딩 및 17-6페이지의 인라인 트래픽 표준화를 참고하십시오.
HTTP	HTTP Inspect(HTTP 검사) 전처리기는 15-32페이지의 HTTP 트래픽 디코딩을 참고하십시오.
SMTP	SMTP 전처리기는 15-61페이지의 SMTP 트래픽 디코딩을 참고하십시오.
IMAP	IMAP 전처리기는 15-55페이지의 IMAP 트래픽 디코딩을 참고하십시오.
POP3	POP 전처리기는 15-58페이지의 POP 트래픽 디코딩을 참고하십시오.
NetBIOS-ssn(SMB)	**SMB File Inspection(SMB 파일 검사)** DCE/RPC 옵션은 15-2페이지의 DCE/RPC 트래픽 디코딩을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-96페이지의 file_type
- 23-96페이지의 file_group

file_type

file_type 키워드를 사용하면 트래픽에서 탐지된 파일의 파일 유형 및 버전을 지정할 수 있습니다. 파일 유형 인수(예를 들어, **JPEG** 및 **PDF**)는 트래픽에서 찾을 파일의 형식을 식별합니다.

참고 동일한 침입 규칙에서 file_type 키워드를 다른file_type 또는 file_group 키워드와 함께 사용하지 **마십시오**.

시스템은 기본적으로 **Any Version(모든 버전)**을 선택하지만, 일부 파일 유형을 사용하면 트래픽에서 찾을 특정 파일 유형 버전을 식별할 수 있도록 버전 옵션을 선택할 수 있습니다(예를 들어, PDF 버전 **1.7**).

최신 파일 유형 및 버전을 보고 구성하려면, VDB를 업데이트합니다. 자세한 내용은 35-8페이지의 취약성 데이터베이스 업데이트를 참고하십시오.

침입 규칙의 파일 유형 및 버전을 선택하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **file_type**을 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

file_type 키워드가 나타납니다.

단계 2 드롭다운 목록에서 하나 이상의 파일 유형을 선택합니다. 파일 유형을 선택하면 규칙에 인수를 자동으로 추가합니다.

규칙에서 파일 유형 인수를 제거하려면, 제거할 파일 유형 옆에 있는 삭제 아이콘( )을 클릭합니다.

단계 3 또는, 각 파일 유형에 대한 대상 버전을 사용자 정의할 수 있습니다. 시스템은 기본적으로 **Any Version(모든 버전)**을 선택하지만, 일부 파일 유형을 사용하면 개별 대상 버전을 선택할 수 있습니다.

참고 VDB를 업데이트하면 최신 파일 유형 및 버전으로 규칙 편집기가 채워집니다. **Any Version(모든 버전)**을 선택한 경우, 시스템은 나중에 VDB 업데이트에 새 버전을 추가할 때 이를 포함하는 규칙을 구성합니다.

file_group

file_group 키워드를 사용하면 트래픽에서 Cisco가 정의한 비슷한 파일 유형 그룹을 선택할 수 있습니다(예를 들어, **멀티미디어** 또는 **오디오**). 파일 그룹은 또한 그룹 내 각 파일 유형에 대해 Cisco가 정의한 버전을 포함합니다.

참고 동일한 침입 규칙에서는 **절대** file_type 키워드를 다른 file_type 또는 file_group 키워드와 함께 사용하지 마십시오.

최신 파일 그룹을 보고 구성하려면, VDB를 업데이트합니다. 자세한 내용은 35-8페이지의 취약성 데이터베이스 업데이트를 참고하십시오.

침입 규칙에서 파일 그룹을 선택하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **file_group**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`file_group` 키워드가 나타납니다.

단계 2 파일 그룹을 선택하여 규칙에 추가합니다.

특정 페이로드 유형 나타내기

라이센스: 보호

`file_data` 키워드는 `content`, `byte_jump`, `byte_test` 및 `pcre`와 같은 다른 키워드에 대해 사용 가능한 위치 인수를 위한 참고 사항으로 기능하는 포인터를 제공합니다. 탐지된 트래픽은 `file_data` 키워드가 나타내는 데이터 유형을 확인합니다. `file_data` 키워드를 사용하여 다음 페이로드 유형의 시작을 나타낼 수 있습니다.

- HTTP 응답 본문

  HTTP 응답 패킷을 검사하려면, HTTP Inspect(HTTP 검사) 전처리기를 활성화해야 하고 HTTP 응답을 검사하는 전처리기를 구성해야 합니다. 자세한 내용은 15-32페이지의 HTTP 트래픽 디코딩 및 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택의 **Inspect HTTP Responses(HTTP 응답 검사)**를 참고하십시오. HTTP Inspect(HTTP 검사) 전처리기가 HTTP 응답 본문 데이터를 탐지할 경우 `file_data` 키워드가 일치됩니다.

- 미압축 gzip 파일 데이터

  HTTP 응답 본문의 미압축 gzip 파일을 검사하려면, HTTP Inspect(HTTP 검사) 전처리기를 활성화해야 하고 HTTP 응답을 검사하고 HTTP 응답 본문의 gzip 기반 압축 파일을 압축 풀기하기 위해 전처리기를 구성해야 합니다. 자세한 내용은 15-32페이지의 HTTP 트래픽 디코딩 및 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택의 **Inspect HTTP Responses(HTTP 응답 검사)**와 **Inspect Compressed Data(압축 데이터 검사)** 옵션을 참고하십시오. HTTP Inspect(HTTP 검사) 전처리기가 HTTP 응답 본문 내 미압축 gzip 데이터를 탐지할 경우 `file_data` 키워드가 일치됩니다.

- 표준화된 Javascript

  표준화된 Javascript 데이터를 검사하려면, HTTP Inspect(HTTP 검사) 전처리기를 활성화해야 하고 HTTP 응답을 검사하는 전처리기를 구성해야 합니다. 자세한 내용은 15-32페이지의 HTTP 트래픽 디코딩 및 15-34페이지의 서버 수준 HTTP 표준화 옵션 선택의 **Inspect HTTP Responses(HTTP 응답 검사)**를 참고하십시오. HTTP Inspect(HTTP 검사) 전처리기가 HTTP 응답 본문 데이터 내 Javascript를 탐지할 경우 `file_data` 키워드가 일치됩니다.

- SMTP 페이로드

  SMTP 페이로드를 검사하려면, SMTP 전처리기를 활성화해야 합니다. 자세한 내용은 15-66페이지의 SMTP 디코딩 구성을 참고하십시오. SMTP 전처리기가 SMTP 데이터를 탐지할 경우 `file_data` 키워드가 일치됩니다.

- SMTP, POP 또는 IMAP 트래픽의 인코딩된 이메일 첨부 파일

  SMTP, POP 또는 IMAP 트래픽의 인코딩된 이메일 첨부 파일을 검사하려면 SMTP, POP 또는 IMAP 전처리기를 각각 활성화해야 하며 단독으로 또는 조합하여 활성화합니다. 다음, 각 활성화된 전처리기를 위해, 해독할 각 첨부 파일 인코딩 유형을 디코딩하기 위해 전처리기가 구성되어 있는지 확인해야 합니다. 사용자가 각 전처리기에 대해 구성할 수 있는 첨부 파일 디코딩 옵션은 다음과 같습니다: **Base64 Decoding Depth(베이스64 디코딩 수준)**, **7-Bit/8-Bit/Binary Decoding Depth(7비트/8비트/이진 디코딩 수준)**, **Quoted-Printable Decoding Depth(발췌되어 인쇄 가능한 디코딩 수준)** 그리

고 **Unix-to-Unix Decoding Depth(유닉스 투 유닉스 디코딩 수준)**. 자세한 내용은 15-55페이지의 IMAP 트래픽 디코딩, 15-58페이지의 POP 트래픽 디코딩 및 15-61페이지의 SMTP 트래픽 디코딩을 참고하십시오.

규칙에서 여러 `file_data` 키워드를 사용할 수 있습니다.

특정 페이로드 유형의 초기를 나타내려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **file_data**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`file_data` 키워드가 나타납니다.

`file_data` 키워드는 인수를 갖지 않습니다.

패킷 페이로드의 시작 나타내기

라이센스: 보호

`pkt_data` 키워드는 `content`, `byte_jump`, `byte_test` 및 `pcre`와 같은 다른 키워드에 대해 사용 가능한 위치 인수를 위한 참고 사항으로 기능하는 포인터를 제공합니다.

표준화된 FTP, 텔넷 또는 SMTP 트래픽이 발견되면, `pkt_data` 키워드는 표준화된 패킷 페이로드의 시작을 나타냅니다. 다른 트래픽이 발견되면 `pkt_data` 키워드는 원시 TCP 또는 UDP 페이로드의 시작을 나타냅니다.

다음 표준화 옵션은 시스템이 침입 규칙에 의한 검사를 위해 해당 트래픽을 표준화할 수 있도록 활성화되어야 합니다.

- 검사를 위해 FTP 트래픽을 정규화하려면, FTP 및 텔넷 전처리기 **Detect Telnet Escape codes within FTP commands(FTP 명령에서 텔넷 Escape(이스케이프) 코드 탐지)**를 활성화해야 합니다(15-26페이지의 서버 수준 FTP 옵션 구성 참고).
- 검사를 위해 텔넷 트래픽을 정규화하려면, FTP 및 텔넷 전처리기 **Normalize(정규화)** 텔넷 옵션을 활성화해야 합니다(15-20페이지의 텔넷 옵션의 이해 참고).
- 검사를 위해 SMTP 트래픽을 정규화하려면, SMTP 전처리기 **Normalize(정규화)** 옵션을 활성화해야 합니다(15-62페이지의 SMTP 디코딩 이해 참고).

규칙에서 여러 `pkt_data` 키워드를 사용할 수 있습니다.

패킷 페이로드의 시작을 나타내려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **pkt_data**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`pkt_data` 키워드가 나타납니다.

`pkt_data` 키워드는 인수를 갖지 않습니다.

Base64 데이터 디코딩 및 검사

라이센스: 보호

base64_decode 및 base64_data 키워드를 함께 사용하여 규칙 엔진이 Base64 데이터로 지정된 데이터를 해독하고 검사하도록 지시할 수 있습니다. 이는 예를 들어, Base64로 인코딩된 HTTP 인증 요청 헤더 및 HTTP PUT 및 POST 요청에서 Base64로 인코딩된 데이터 검사에 유용합니다.

이 키워드는 특히 HTTP 요청의 Base64 데이터를 해독하고 검사하는 데 유용합니다. 그러나, 또한 이 키워드를 여러 행 위의 길이가 긴 헤더 행을 확장하기 위해 HTTP가 스페이스 및 탭 문자를 사용하는 것과 같은 방식으로 이 문자를 사용하는 SMTP와 같은 모든 프로토콜과 함께 사용할 수 있습니다. 폴딩으로 알려진 이와 같은 행 확장이 이를 사용하는 프로토콜에 나타나지 않는 경우, 검사는 스페이스 또는 탭이 뒤따르지 않는 모든 복귀 또는 라인 피드에서 끝납니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-99페이지의 base64_decode
- 23-100페이지의 base64_data

base64_decode

라이센스: 보호

base64_decode 키워드는 규칙 엔진이 패킷 데이터를 Base64 데이터로 해독하도록 지시합니다. 선택적 인수는 디코딩할 바이트 수와 디코딩을 시작할 데이터 내 위치를 지정하도록 합니다.

규칙에서 base64_decode 키워드를 한 번 사용할 수 있습니다. 이는 최소한 base64_data 키워드의 인스턴스 하나를 선행해야 합니다. 자세한 내용은 23-100페이지의 base64_data를 참고하십시오.

Base64 데이터를 해독하기 전에, 규칙 엔진은 여러 행을 가로질러 접힌 긴 헤더를 펼칩니다. 규칙 엔진에 다음이 발생할 때 디코딩은 종료됩니다.

- 헤더 행 끝
- 디코딩할 지정된 바이트 수
- 패킷 종료

다음 표에서는 base64_decode 키워드와 함께 사용할 수 있는 인수를 설명합니다.

표 23-60 선택적 base64_디코딩 인수

인수	설명
Bytes	디코딩할 바이트 수를 지정합니다. 지정되지 않은 경우, 디코딩은 헤더 행 끝 또는 패킷 페이로드의 끝 중 먼저 오는 것까지 계속합니다. 0이 아닌 양수 값을 지정할 수 있습니다.
Offset(오프셋)	패킷 페이로드의 시작과 관련된 오프셋을 지정하거나, **Relative(연결)**를 지정한 경우, 현재 검사 위치에 관련된 오프셋을 지정합니다. 0이 아닌 양수 값을 지정할 수 있습니다.
Relative	현재 검사 위치에 관련된 검사를 지정합니다.

Base64 데이터를 해독하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **base64_decode**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`base64_decode` 키워드가 나타납니다.

단계 2 또는, 선택적 base64_디코딩 인수 표에 설명된 인수 중 하나를 선택합니다.

base64_data

라이센스: 보호

`base64_data` 키워드는 `base64_decode` 키워드를 사용하여 디코딩된 Base64 데이터 검사를 위한 참고 자료를 제공합니다. `base64_data` 키워드는 디코딩된 Base64 데이터 시작 시 검사가 시작되도록 설정합니다. 선택적으로, `content` 또는 `byte_test`와 같은 다른 키워드를 위한 사용 가능한 위치 인수를 사용하여 검사할 위치를 더욱 상세히 지정할 수 있습니다.

`base64_decode` 키워드를 사용한 후 반드시 `base64_data` 키워드를 최소한 한 번 사용해야 합니다. 선택적으로, `base64_data`를 여러 번 사용하여 디코딩된 Base64 데이터의 처음으로 돌아갈 수 있습니다.

Base64 데이터를 검사할 때 다음에 유의하십시오.

- 빠른 패턴 매처를 사용할 수 없습니다. 자세한 내용은 23-26페이지의 빠른 패턴 매처 사용을 참고하십시오.
- 개입하는 HTTP 콘텐츠 인수로 규칙에서 Base64 검사를 중지하는 경우, Base64 데이터의 상세 검사 전에 규칙에 다른 `base64_data` 키워드를 삽입해야 합니다. 자세한 내용은23-23페이지의 HTTP 콘텐츠 옵션을 참고하십시오.

디코딩된 Base64 데이터를 검사하려면 다음을 수행합니다.

단계 1 Create Rule(규칙 생성) 페이지의 드롭다운 목록에서 **base64_data**를 선택하고 **Add Option(옵션 추가)**을 클릭합니다.

`base64_data` 키워드가 나타납니다.

규칙 구성

라이센스: 보호

사용자가 고유의 사용자 지정 표준 텍스트 규칙을 생성할 수 있는 것처럼, 사용자는 또한 Cisco가 제공한 기존의 표준 텍스트 규칙 및 공유 객체 규칙을 수정하고 변경한 사항을 새로운 규칙으로 저장할 수 있습니다. Cisco가 제공한 공유 객체 규칙의 경우, 소스와 대상 포트 및 IP 주소와 같은 규칙 헤더 정보를 수정하는 데 제한된다는 점에 유의하십시오. 공유 객체 규칙의 규칙 키워드 및 인수를 수정할 수 없습니다.

자세한 내용은 다음 섹션을 참고하십시오.

새규칙 작성

라이센스: 보호

사용자 고유의 표준 텍스트 규칙을 생성할 수 있습니다.

사용자 지정 표준 텍스트 규칙에서, 규칙 헤더 구성과 규칙 키워드 및 인수를 설정할 수 있습니다. 또는, 규칙 헤더 설정을 사용하여 특정 프로토콜을 사용하고 특정 IP 주소 또는 포트를 오가는 트래픽에만 일치하는 규칙에 집중할 수 있습니다.

새 규칙을 생성한 후 `GID:SID:Rev` 형식으로 된 규칙 번호를 사용하여 빠르게 다시 찾을 수 있습니다. 모든 표준 텍스트 규칙에 대한 규칙 번호는 1로 시작됩니다. 규칙 번호의 두 번째 부분인 Snort ID(SID) 번호는 해당 규칙이 로컬 규칙인지 아니면 Cisco가 제공한 규칙인지를 나타냅니다. 새 규칙을 생성할 때, 시스템은 해당 규칙에 로컬 규칙을 위한 사용 가능한 다음 Snort ID 번호를 지정하고 해당 규칙을 로컬 규칙 카테고리에 저장합니다. 로컬 규칙에 대한 Snort ID 번호는 1,000,000에서 시작하고 각 새로운 로컬 규칙에 대한 SID는 하나씩 증가됩니다. 규칙 번호의 마지막 부분은 수정 번호입니다. 새 규칙의 경우, 수정 번호는 1입니다. 사용자 지정 규칙을 변경할 때마다 수정 번호가 하나씩 증가합니다.

참고 시스템은 사용자가 가져오는 침입 정책에서 모든 사용자 지정 규칙에 새 SID를 할당합니다. 자세한 내용은 B-1페이지의 구성 가져오기 및 내보내기를 참고하십시오.

규칙 편집기를 사용하여 사용자 지정 표준 텍스트 규칙을 작성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책) > Rule Editor(규칙 편집기)**.를 선택합니다.

Rule Editor(규칙 편집기) 페이지가 나타납니다.

단계 2 **Create Rule(규칙 생성)**을 클릭합니다.

Create Rule(규칙 생성) 페이지가 나타납니다.

단계 3 **Message(메시지)** 필드에, 사용자가 이벤트로 표시하려는 메시지를 입력합니다.

이벤트 메시지 상세 정보는 23-11페이지의 이벤트 메시지 정의를 참고하십시오.

팁 규칙 메시지를 지정해야 합니다. 또한, 공백, 하나 이상의 따옴표, 하나 이상의 아포스트로피 또는 공백, 따옴표, 아포스트로피로의 조합만으로는 메시지를 구성할 수 없습니다.

단계 4 **Classification(분류)** 목록에서 이벤트 유형을 설명하는 분류를 선택합니다.

사용 가능한 분류에 대한 자세한 내용은 23-12페이지의 침입 이벤트 분류 정의를 참고하십시오.

단계 5 **Action(작업)** 목록에서 작성할 규칙 유형을 선택합니다. 다음 중 하나를 사용할 수 있습니다.

- 트래픽이 규칙을 시작할 때 이벤트를 생성하는 규칙을 만들려면 **alert(경고)**를 선택합니다.
- 규칙을 시작하는 트래픽을 무시하는 규칙을 만들려면 **pass(통과)**를 선택합니다.

단계 6 **Protocol(프로토콜)** 목록에서 규칙이 검사하기를 원하는 패킷의 트래픽 프로토콜(**tcp**, **udp**, **icmp** 또는 **ip**)을 선택합니다.

프로토콜 유형 선택에 관한 자세한 내용은 23-4페이지의 프로토콜 지정을 참고하십시오.

단계 7 **Source IP(소스 IP)** 필드에 규칙을 시작해야 하는 트래픽의 시작 IP 주소 또는 주소 블록을 입력합니다. **Destination IPs(대상 IP)** 필드에 규칙을 시작해야 하는 트래픽의 목적지 IP 주소 또는 주소 블록을 입력합니다.

규칙 편집기가 수용하는 IP 주소 구문에 대한 자세한 내용은 23-5페이지의 침입 규칙 내 IP 주소 지정을 참고하십시오.

단계 8 **Source IP(소스 IP)** 필드에, 규칙을 시작해야 하는 트래픽의 시작 포트 번호를 입력합니다. **Destination IP(대상 IP)** 필드에 규칙을 시작해야 하는 트래픽에 대한 수신 포트 번호를 입력합니다.

참고 프로토콜이 `ip`로 설정되면 시스템은 침입 규칙 헤더의 포트 정의를 무시합니다.

규칙 편집기가 수락하는 포트 구문에 대한 자세한 내용은 23-8페이지의 침입 규칙 내 포트 정의를 참고하십시오.

단계 9 **Direction(방향)** 목록에서 규칙을 시작하고자 하는 트래픽의 방향을 나타내는 연산자를 선택합니다. 다음 중 하나를 사용할 수 있습니다.

- 소스 IP 주소에서 대상 IP 주소로 이동하는 트래픽에 일치시키기 위해 **Directional(방향성)**을 사용합니다.
- 어느 방향으로든 이동하는 트래픽에 일치시키기 위해 **Bidirectional(양방향성)**을 사용합니다.

단계 10 **Detection Options(탐지 옵션)** 목록에서 사용할 키워드를 선택합니다.

단계 11 **Add Option(옵션 추가)**를 클릭합니다.

단계 12 사용자가 추가한 키워드에 대해 지정할 모든 인수를 입력합니다. 규칙 키워드와 그 사용 방법에 관한 자세한 내용은 23-9페이지의 규칙 내 키워드 및 인수의 이해를 참고하십시오.

키워드 및 인수를 추가할 때, 다음을 수행할 수 있습니다.

- 이들을 추가한 후 키워드를 다시 정렬하려면, 사용자가 이동할 키워드 옆의 위쪽 또는 아래쪽 화살표를 클릭합니다.
- 키워드를 삭제하려면, 해당 키워드 옆에 있는 **X**를 클릭합니다.

추가할 각 키워드 옵션을 보려면 단계 10부터 12까지 반복합니다.

단계 13 새 규칙을 저장하려면 **Save As New(다른 이름으로 저장)**를 클릭합니다.

시스템은 로컬 규칙을 위한 규칙 번호 시퀀스에서 해당 규칙에 다음 사용 가능한 Snort ID(SID) 번호를 지정하고 이를 로컬 규칙 카테고리에 저장합니다.

시스템은 적절한 침입 정책에서 활성화할 때까지 새로운 규칙 또는 변경된 규칙에 대한 트래픽 평가를 시작하지 않으며, 이후 액세스 제어 정책의 일부로서 침입 정책을 적용합니다. 자세한 내용은 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

기존 규칙 변경

라이센스: 보호

사용자 지정 표준 텍스트 규칙을 수정할 수 있습니다. 또한 Cisco가 제공한 표준 텍스트 규칙 또는 공유 객체 규칙을 수정하고 저장하여 하나 이상의 새로운 규칙 인스턴스를 생성할 수 있습니다.

규칙을 만들거나 Cisco 규칙을 변경하면 로컬 규칙 카테고리에 새 규칙 또는 수정본을 복사하여 규칙에 100000보다 큰 수의 다음 사용 가능한 Snort ID(SID)를 할당합니다.

공유 객체 규칙의 헤더 정보만 수정할 수 있습니다. 공유 객체 규칙 또는 해당 인수에 사용되는 규칙 키워드를 수정할 수 없습니다. 공유 객체 규칙에 대한 헤더 정보를 수정하고 변경 사항을 저장하면 3의 생성자 ID(GID) 및 사용자 지정 규칙에 대한 다음 사용 가능한 SID로 규칙의 새 인스턴스를 만듭니다. Rule Editor(규칙 편집기)는 공유 객체 규칙의 새 인스턴스를 예약된 `soid` 키워드에 연결하는데, 이는 VRT에서 만든 규칙에 사용자가 만든 규칙을 매핑합니다. 사용자가 생성한 공유 객체 규칙 인스턴스는 삭제할 수 있지만, Cisco가 제공한 공유 객체 규칙은 삭제할 수 없습니다. 자세한 내용은 23-3페이지의 규칙 헤더의 이해 및 23-104페이지의 사용자 지정 규칙 삭제를 참고하십시오.

참고 공유 객체 규칙에 대한 프로토콜을 수정하지 마십시오. 이를 삭제하면 규칙이 무효화됩니다.

규칙을 변경하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책) > Rule Editor(규칙 편집기)**.를 선택합니다.

Rule Editor(규칙 편집기) 페이지가 나타납니다.

단계 2 수정할 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 규칙 카테고리를 검색하여 규칙을 찾으려면 폴더를 탐색하여 원하는 규칙을 찾고, 해당 규칙 옆에 있는 수정 아이콘()을 클릭합니다.
- 페이지에 표시된 규칙을 필터링하여 규칙을 찾으려면, 규칙 목록의 왼쪽 상단에 필터링 아이콘()이 표시된 텍스트 상자에 규칙 필터를 입력합니다. 해당 규칙 옆에 있는 수정 아이콘()을 클릭하여 원하는 규칙을 탐색합니다. 자세한 내용은 23-105페이지의 규칙 편집기 페이지의 규칙 필터링을 참고하십시오.

규칙 편집기가 열리고, 선택한 규칙이 표시됩니다.

공유 객체 규칙을 선택하는 경우, 규칙 편집기는 규칙 헤더 정보만 표시한다는 점에 유의하십시오. 공유 객체 규칙은 Rule Editor(규칙 편집기) 페이지에서 숫자 3(GID)으로 시작하는 목록, 예를 들어, 3:1000004로 확인할 수 있습니다.

단계 3 규칙을 수정(규칙 옵션에 대한 자세한 내용은 23-101페이지의 새규칙 작성 참고)하고 **Save As New(다른 이름으로 저장)**를 클릭합니다.

규칙은 로컬 규칙 카테고리에 저장됩니다.

팁 시스템 규칙 대신에 규칙의 로컬 변경을 사용하고자 할 경우, 20-19페이지의 규칙 상태 설정의 절차를 사용하여 시스템 규칙을 비활성화하고 로컬 규칙을 활성화합니다.

단계 4 변경 사항을 적용하려면 4-10페이지의 액세스 제어 정책 적용에 설명된 대로 침입 정책을 액세스 제어 정책의 일부로 적용하여 활성화합니다.

규칙에 코멘트 추가

라이센스: 보호

모든 침입 규칙에 코멘트를 추가할 수 있습니다. 그러면 식별된 정책 위반 또는 공격 및 규칙에 대한 자세한 컨텍스트 및 정보를 제공할 수 있습니다.

규칙에 코멘트를 추가하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책) > Rule Editor(규칙 편집기)**.를 선택합니다.

Rule Editor(규칙 편집기) 페이지가 나타납니다.

단계 2 코멘트를 달고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 규칙 카테고리를 검색하여 규칙을 찾으려면 폴더를 탐색하여 원하는 규칙을 찾고, 해당 규칙 옆에 있는 수정 아이콘( )을 클릭합니다.
- 페이지에 표시된 규칙을 필터링하여 규칙을 찾으려면, 규칙 목록의 왼쪽 상단에 필터 아이콘( )이 표시된 텍스트 상자에 규칙 필터를 입력합니다. 해당 규칙 옆에 있는 수정 아이콘( )을 클릭하여 원하는 규칙을 탐색합니다. 자세한 내용은 23-105페이지의 규칙 편집기 페이지의 규칙 필터링을 참고하십시오.

규칙 편집기가 나타납니다.

단계 3 **Rule Comment(규칙 코멘트)**를 클릭합니다.

Rule Comment(규칙 코멘트) 페이지가 나타납니다.

단계 4 입력란에 코멘트를 입력하고 **Add Comment(코멘트 추가)**를 클릭합니다.

코멘트가 코멘트 텍스트 상자에 저장됩니다.

사용자 지정 규칙 삭제

라이센스: 보호

침입 정책에서 현재 활성화되지 않은 사용자 지정 규칙을 삭제할 수 있습니다. Cisco가 제공한 표준 텍스트 규칙 또는 공유 객체 규칙의 규칙은 삭제할 수 없습니다.

시스템은 삭제된 카테고리에 삭제된 규칙을 저장하며, 사용자는 삭제한 규칙을 새로운 규칙의 기준으로 사용할 수 있습니다. 규칙 수정에 대한 내용은 23-103페이지의 기존 규칙 변경을 참고하십시오.

침입 정책의 Rules(규칙) 페이지가 삭제된 카테고리를 표시하지 않으므로, 삭제된 사용자 지정 규칙을 사용할 수 없습니다.

또한 Rule Updates(규칙 업데이트) 페이지의 모든 로컬 규칙을 삭제할 수 있다는 점에 유의하십시오. 예를 들어, 35-11페이지의 일회성 규칙 업데이트 사용을 참고하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 사용자 지정 규칙 생성에 대한 자세한 내용은 23-101페이지의 새규칙 작성을 참고하십시오.
- 로컬 규칙 가져오기에 대한 자세한 내용은 35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기를 참고하십시오.
- 규칙 상태 설정에 대한 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.

사용자 지정 규칙을 삭제하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책) > Rule Editor(규칙 편집기)**.를 선택합니다.

Rule Editor(규칙 편집기) 페이지가 나타납니다.

단계 2 다음 2가지 옵션을 사용할 수 있습니다.

- **Delete Local Rules(로컬 규칙 삭제)**를 클릭한 후 **OK(확인)**를 클릭합니다.

  사용자가 변경 사항을 저장한 침입 정책에서 현재 활성화되어 있지 않은 모든 규칙은 로컬 규칙 카테고리에서 삭제되고 삭제된 카테고리로 옮겨집니다.

- 로컬 규칙 카테고리의 폴더를 탐색합니다. 로컬 규칙 카테고리를 클릭하여 확장한 다음, 삭제할 규칙 옆에 있는 삭제 아이콘( )을 클릭합니다.

  규칙은 로컬 규칙 카테고리에서 삭제되고 삭제된 카테고리로 옮겨집니다.

  사용자 지정 표준 텍스트 규칙은 생성자 ID(GID) 1(예를 들어, 1:1000012)을 갖고, 사용자 지정 공유 객체 규칙은 GID 3(예를 들어, 3:1000005)을 갖는다는 점에 유의하십시오.

팁 시스템은 또한 수정된 헤더 정보로 저장할 수 있는 공유 객체 규칙을 로컬 규칙 카테고리에 저장하고 GID 3으로 나열합니다. 공유 객체 규칙의 사용자 수정본은 삭제할 수 있지만, 원본 공유 객체 규칙은 삭제할 수 없습니다.

규칙 편집기 페이지의 규칙 필터링

라이센스: 보호

규칙의 하위 집합을 표시하기 위해 Rule Editor(규칙 편집기) 페이지에서 규칙을 필터링할 수 있습니다. 예를 들어, 규칙을 수정하거나 상태를 변경하기를 원하지만 수 천 개의 규칙 중에서 이를 찾는 데 어려움이 있는 경우, 이는 유용할 수 있습니다.

필터를 입력하면, 페이지는 적어도 하나의 일치하는 규칙을 포함하는 모든 폴더를 표시하거나, 규칙이 하나도 일치하지 않을 때는 메시지를 표시합니다. 필터는 특수 키워드 및 해당 인수, 문자열 및 텍스트 문자열, 그리고 여러 필터 상태를 분리하는 스페이스를 포함할 수 있습니다. 필터에는 정규 표현식, 와일드카드 문자 또는 부정 문자(!), 보다 큼 기호(>), 보다 작음 기호(<)와 같은 특별 연산자를 포함할 수 없습니다.

모든 키워드, 키워드 인수 및 문자열은 대/소문자 구분이 없습니다. `gid` 및 `sid` 키워드를 제외한, 모든 인수 및 문자열은 부분 문자열로 처리됩니다. `gid` 및 `sid`의 인수는 정확히 일치하는 것만 반환합니다.

또는, 원래의 필터링되지 않은 페이지의 폴더 및 후속 필터가 해당 폴더의 일치 항목을 반환할 때 확장 상태를 유지하는 폴더를 확장할 수 있습니다. 이는 찾고자 하는 규칙이 많은 규칙을 포함하는 폴더에 있을 때 유용할 수 있습니다.

후속 필터로 필터를 제한할 수 없습니다. 입력한 모든 필터는 전체 규칙 데이터베이스를 검색하고 일치하는 규칙을 모두 반환합니다. 페이지가 계속 이전 검색 결과를 표시하고 있는데 필터를 입력하는 경우, 페이지는 이를 지우고 새 필터의 결과로 돌아갑니다.

필터링된 목록이나 필터링되지 않은 목록의 규칙과 같은 기능을 사용할 수 있습니다. 예를 들어, Rule Editor(규칙 편집기) 페이지에서 필터링된 목록이나 필터링되지 않은 목록의 규칙을 수정할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 23-106페이지의 규칙 필터에서 키워드 사용
- 23-107페이지의 규칙 필터의 문자열 사용
- 23-107페이지의 규칙 필터에서 키워드와 문자열 결합
- 23-107페이지의 규칙 필터링

규칙 필터에서 키워드 사용

라이센스: 보호

각 규칙 필터의 형식에는 하나 이상의 키워드를 포함할 수 있습니다.

keyword:*argument*

*keyword*가 규칙 필터링 키워드 표의 키워드 중 하나인 경우 및 *argument*가 특정 필드 또는 키워드 관련 필드에서 검색할 대소문자를 구분하는 단일 영숫자 문자열인 경우입니다.

`gid` 및 `sid`를 제외한 모든 키워드에 대한 인수는 부분 문자열로 처리됩니다. 예를 들어, 인수 `123`은 `"12345"`, `"41235"`, `"45123"` 등을 반환합니다. `gid` 및 `sid`의 인수는 정확하게 일치하는 경우에만 반환됩니다. 예를 들어, `sid:3080`은 SID 3080만 반환합니다.

팁 하나 이상의 문자열로 필터링하여 부분 SID를 검색할 수 있습니다. 자세한 내용은 23-107페이지의 규칙 필터의 문자열 사용을 참고하십시오.

다음 표는 규칙을 필터링하는 데 사용할 수 있는 인수 및 특정 필터링 키워드를 나타냅니다.

표 23-61 규칙 필터링 키워드

키워드	설명	예
`arachnids`	규칙 참조에서 Arachnids ID의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다. 자세한 내용은 23-14페이지의 이벤트 참조 정의를 참고하십시오.	`arachnids:181`
`bugtraq`	규칙 참조에서 Bugtraq ID의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다. 자세한 내용은 23-14페이지의 이벤트 참조 정의를 참고하십시오.	`bugtraq:2120`
`cve`	규칙 참조에서 CVE 번호의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다. 자세한 내용은 23-14페이지의 이벤트 참조 정의를 참고하십시오.	`cve:2003-0109`
`gid`	인수 `1`은 표준 텍스트 규칙을 반환합니다. 인수 `3`은 공유 객체 규칙을 반환합니다. 자세한 내용은 20-2페이지의 표 20-1을 참고하십시오.	`gid:3`
`mcafee`	규칙 참조에서 McAfee ID의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다. 자세한 내용은 23-14페이지의 이벤트 참조 정의를 참고하십시오.	`mcafee:10566`
`msg`	이벤트 메시지로도 알려진 규칙 Message(메시지) 필드의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다. 자세한 내용은 23-11페이지의 이벤트 메시지 정의를 참고하십시오.	`msg:chat`
`nessus`	규칙 참조에서 Nessus ID의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다. 자세한 내용은 23-14페이지의 이벤트 참조 정의를 참고하십시오.	`nessus:10737`

표 23-61 규칙 필터링 키워드 (계속)

키워드	설명	예
참조	규칙 참조 또는 규칙 Message(메시지) 필드에서 단일 영숫자 문자열의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다. 자세한 내용은 23-14페이지의 이벤트 참조 정의 및 23-11페이지의 이벤트 메시지 정의를 참고하십시오.	ref:MS03-039
sid	정확한 Signature ID(서명 ID)로 규칙을 반환합니다.	sid:235
url	규칙 참조에서 URL의 전체 또는 일부에 따라 하나 이상의 규칙을 반환합니다. 자세한 내용은 23-14페이지의 이벤트 참조 정의를 참고하십시오.	url:faqs.org

규칙 필터의 문자열 사용

라이센스: 보호

각 규칙 필터는 하나 이상의 영숫자 문자열을 포함할 수 있습니다. 문자열은 규칙 **Message(메시지)** 필드, 서명 ID 및 생성자 ID를 검색합니다. 예를 들어, 문자열 `123`은 규칙 메시지에서 문자열 `"Lotus123"`, `"123mania"` 등을 반환하며, 또한 SID 6123, SID 12375 등을 반환합니다. 규칙 **Message(메시지)** 필드에 대한 자세한 내용은 23-11페이지의 이벤트 메시지 정의를 참고하십시오.

모든 문자열은 대소문자를 구분하지 않으며 부분 문자열로 처리됩니다. 예를 들어, 문자열 `ADMIN`, `admin` 또는 `Admin`은 모두 `"admin"`, `"CFADMIN"`, `"Administrator"` 등을 반환합니다.

정확히 일치하는 항목을 반환하기 위해 인용구에서 문자열을 묶을 수 있습니다. 예를 들어, 인용구 내 문자열 `"overflow attempt"`는 정확한 문자열만 반환하지만, 인용구가 없는 두 개의 문자열 `overflow` 및 `attempt`로 구성된 필터는 `"overflow attempt"`, `"overflow multipacket attempt"`, `"overflow with evasion attempt"` 등을 반환합니다.

규칙 필터에서 키워드와 문자열 결합

라이센스: 보호

키워드, 문자열 또는 둘 다로 이루어진 스페이스로 구분된 문자열의 조합을 입력하여 필터링 결과를 좁힐 수 있습니다. 결과는 필터링 조건과 일치하는 모든 규칙을 포함합니다.

순서에 상관없이 여러 필터 상태를 입력할 수 있습니다. 예를 들어, 다음 필터 각각은 동일한 규칙을 반환합니다.

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

규칙 필터링

라이센스: 보호

규칙의 하위 집합을 표시하여 더욱 쉽게 특정 규칙을 찾을 수 있도록 하기 위해 Rule Editor(규칙 편집기) 페이지에서 규칙을 필터링할 수 있습니다. 그러면 모든 페이지 기능을 사용할 수 있습니다.

특정 규칙을 필터링하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책) > Rule Editor(규칙 편집기)**.를 선택합니다.

Rule Editor(규칙 편집기) 페이지가 나타납니다.

규칙 필터링은 수정하는 규칙을 찾을 때 Rule Editor(규칙 편집기) 페이지에서 특히 유용할 수 있습니다. 자세한 내용은 23-103페이지의 기존 규칙 변경을 참고하십시오.

단계 2 또는, Group Rules By(규칙 분류 기준) 목록에서 다양한 정렬 방법을 선택합니다.

팁 필터링은 규칙이 여러 카테고리에 표시되기 때문에 모든 하위 그룹 내 결합된 총 규칙 수가 큰 경우 특히 오래 걸릴 수 있으며 고유 규칙의 총 수가 훨씬 적을 때에도 그렇습니다.

단계 3 또는, 확장할 모든 그룹 옆에 있는 폴더를 클릭합니다.

폴더는 해당 그룹에서 규칙을 표시하도록 확장됩니다. 일부 규칙 그룹에도 또한 확장할 수 있는 하위 그룹이 있다는 점에 유의하십시오.

원래의 필터링되지 않은 페이지의 그룹을 확장하는 것은 규칙이 해당 그룹에 있을 것으로 예상하는 경우 유용할 수 있다는 점을 참고하십시오. 후속 필터가 해당 폴더와 일치할 때, 그리고 필터링 지우기 아이콘( )을 클릭하여 원래의 필터링되지 않은 페이지로 돌아온 경우 해당 그룹은 확장된 채로 유지됩니다.

단계 4 필터 텍스트 상자를 활성화하려면 규칙 목록의 왼쪽 상단에 있는 텍스트 상자 내에 있는 필터 아이콘( )의 오른쪽을 클릭합니다.

단계 5 필터 제약 조건을 입력하고 Enter(입력)를 누릅니다.

필터는 키워드 및 인수, 인용구가 있는 문자열 또는 인용구가 없는 문자열, 그리고 여러 필터 상태를 분리하는 스페이스를 포함할 수 있습니다. 자세한 내용은 23-105페이지의 규칙 편집기 페이지의 규칙 필터링을 참고하십시오.

페이지는 새로 고침되어 최소 한 개의 일치하는 규칙이 포함된 모든 그룹을 표시합니다.

단계 6 또는, 이미 열려 있지 않은 폴더가 있으면 모두 열어서 일치 규칙을 표시합니다. 다음 필터링 옵션을 이용할 수 있습니다.

- 새 필터를 입력하려면, 필터 텍스트 상자 내에 커서를 두고 클릭하여 활성화합니다. 필터를 입력하고 Enter(입력)를 누릅니다.
- 현재 필터링된 목록을 지우고 원래의 필터링되지 않은 페이지로 돌아가려면, 필터 지우기 아이콘( )을 클릭합니다.

단계 7 선택적으로, 페이지에서 일반적으로 수행하는 모든 변경 사항은 규칙에 적용할 수 있습니다. 23-103페이지의 기존 규칙 변경을 참고하십시오.

변경 사항이 무엇이든 효력을 가지도록 하려면, 액세스 제어 정책의 침입 정책 부분을 4-10페이지의 액세스 제어 정책 적용에 설명된 대로 적용합니다.

24장

악성코드 및 금지 파일 차단

악성 소프트웨어 또는 *악성코드*는 여러 경로를 통해 조직의 네트워크에 침입할 수 있습니다. 악성코드의 효과를 파악하고 경감하기 위해 ASA FirePOWER 모듈의 파일 제어 및 AMP 구성 요소는 악성코드 및 네트워크 트래픽 내 다른 유형의 파일을 전송하는 것을 탐지, 추적, 저장, 분석하고 선택적으로 차단할 수 있습니다.

전체 액세스 제어 구성에 악성코드 차단 및 파일 제어를 포함하여 이를 수행하도록 시스템을 구성합니다. 사용자가 생성하고 액세스 제어 규칙과 연결하는 *파일 정책*은 규칙과 일치하는 네트워크 트래픽을 처리합니다.

어느 라이센스로도 파일 정책을 생성할 수 있지만, 악성코드 차단 및 파일 제어의 특정 측면이 요구하는 바는 사용자가 다음 표에 설명된 대로 ASA FirePOWER 모듈의 사용이 허가된 특정 기능을 활성화하는 것입니다.

표 24-1 침입 및 파일 검사를 위한 라이센스 및 어플라이언스 요건

기능	설명	추가할 라이센스
침입 방지	침입과 공격을 탐지하고 선택적으로 차단	보호
파일 제어	파일 유형의 전송을 탐지하고 선택적으로 차단	보호
AMP(Advanced Malware Protection)	악성코드의 전송을 탐지,추적하고 선택적으로 차단	악성코드

자세한 내용은 다음을 참고하십시오.

- 24-1페이지의 악성코드 차단 및 파일 제어 이해
- 24-4페이지의 파일 정책 이해 및 생성

악성코드 차단 및 파일 제어 이해

라이센스: 보호, 악성코드 또는 모두

AMP(Advanced Malware Protection) 기능을 사용하여 ASA FirePOWER 모듈을 사용자 네트워크에 전송되고 있는 악성코드 파일을 탐지, 추적하고 선택적으로 차단하도록 구성할 수 있습니다.

시스템은 PDF, Microsoft Office 문서 및 기타 파일을 비롯한 다양한 유형의 파일에서 악성코드를 탐지하고 선택적으로 차단할 수 있습니다. ASA FirePOWER 모듈은 해당 파일 유형의 전송을 위해 특정 애플리케이션 프로토콜 기반의 네트워크 트래픽을 모니터링합니다. ASA FirePOWER 모듈이

적합한 파일을 탐지한 경우, ASA FirePOWER 모듈은 다음으로 파일의 SHA-256 해시 값을 사용하여 *악성코드 클라우드 조회*를 수행합니다. 이러한 결과를 바탕으로, Cisco 클라우드는 파일 속성을 ASA FirePOWER 모듈에 반환합니다.

클라우드의 파일에 잘못된 속성이 있는 경우, 파일의 SHA-256 값을 파일 목록에 추가할 수 있습니다.

- 클라우드가 정상 성향을 할당한 것처럼 파일을 취급하려면 *정상 목록*에 파일을 추가합니다.
- 클라우드가 악성코드 속성으로 할당한 것처럼 파일을 처리하려면 파일을 *사용자 지정 탐지 목록*에 추가합니다.

시스템이 파일 목록에서 파일의 SHA-256 값을 탐지한 경우, 시스템은 악성코드 조회 또는 파일 속성 확인을 수행하지 않고 적절한 조치를 취합니다. 반드시 **Malware Cloud Lookup(악성코드 클라우드 조회)** 또는 **Block Malware(악성코드 차단)** 작업 중 하나 및 파일의 SHA 값을 계산하는 일치 파일 유형과 함께 파일 정책 내 규칙을 구성해야 한다는 점에 유의하십시오. 파일별 정책 기반의 정상 목록 및 사용자 탐지 목록의 사용을 활성화할 수 있습니다.

파일을 조사하거나 차단하려면 보호 라이센스를 ASA FirePOWER 모듈에서 활성화해야 합니다. 파일 목록에 파일을 추가하려면 반드시 악성코드 라이센스를 활성화해야 합니다.

파일 속성의 이해

시스템은 Cisco 클라우드에 의해 반환된 속성을 기준으로 파일 속성을 확인합니다. 파일 목록에 파일을 추가하거나 위협 점수가 제공된 결과로 인해, 파일에는 Cisco 클라우드에 의해 반환된 다음과 같은 파일 속성 중 하나가 포함될 수 있습니다.

- `Malware(악성코드)`는 클라우드가 파일을 악성코드로 분류했음을 나타냅니다.
- `Clean(정상)`은 클라우드가 파일을 안전한 것으로 분류했음을 나타내거나 사용자가 파일을 정상 목록에 추가했음을 나타냅니다.
- `Unknown(알 수 없음)`은 클라우드가 속성을 할당하기 전에 악성코드 클라우드 조회가 발생했음을 나타냅니다. 클라우드에서 파일의 카테고리를 분류하지 않았습니다.
- `Custom Detection(사용자 지정 탐지)`은 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다.
- `Unavailable(사용 불가)`은 ASA FirePOWER 모듈이 악성코드 클라우드 조회를 수행하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.

팁 빠른 상속에서 여러 `Unavailable(사용 불가)` 악성코드 이벤트를 볼 경우 클라우드 연결 및 포트 구성을 확인하십시오. 자세한 내용은 D-1페이지의 보안, 인터넷 액세스 및 통신 포트를 참고하십시오.

파일 속성에 따라 ASA FirePOWER 모듈이 파일을 차단하거나 파일의 업로드 또는 다운로드를 차단합니다. 시스템이 SHA-256 값에 기반하여 파일의 속성을 이미 아는 경우, 성능 향상을 위해 어플라이언스는 Cisco클라우드에 쿼리하는 대신 캐시된 속성을 사용합니다.

파일 속성은 변경할 수 있습니다. 예를 들어, 클라우드는 이전에는 정상인 것으로 간주되었던 파일이 지금은 악성코드로 식별되는 경우 또는 그 반대의 경우(악성코드로 식별된 파일이 실제로 정상임)를 결정할 수 있습니다. 지난주에 악성코드를 조회한 파일의 속성이 변경된 경우, 클라우드에서 ASA FirePOWER 모듈에 이를 알려 시스템이 다음번에 해당 파일의 전송을 탐지할 경우 적절한 조치를 취할 수 있도록 합니다. 변경된 파일 속성은 *회귀적* 속성이라고 합니다.

악성코드 클라우드 조회에서 반환된 파일 속성에는 TTL(time-to-live) 값이 포함됩니다. TTL 값에 지정된 기간 동안 파일 속성이 업데이트되지 않고 유지될 경우, 시스템에서는 캐시된 정보를 삭제합니다. 속성에는 다음과 같은 TTL 값이 포함됩니다.

- 안전-4시간
- 알 수 없음-1시간
- 악성코드-1시간

캐시에 대한 악성코드 클라우드 조회를 통해 캐시된 속성이 시간을 초과한 것으로 식별된 경우, 시스템은 새로운 조회를 수행하여 파일 속성을 확인합니다.

파일 제어의 이해

조직에서 악성코드뿐만 아니라 특정 유형의 모든 파일(파일의 악성코드 여부 포함 여부에 상관없이)의 전송을 차단하려는 경우, *파일 제어* 기능을 사용하면 폭넓은 범위를 포괄할 수 있습니다. 악성코드 차단에서와 마찬가지로 ASA FirePOWER 모듈 특정 파일 유형의 전송을 위해 네트워크 트래픽을 모니터링한 후, 파일을 차단하거나 허용합니다.

파일 제어는 시스템이 악성코드와 더불어 다양한 추가 파일 유형을 탐지할 수 있는 경우 모든 파일 유형을 지원합니다. 이러한 파일 유형은 멀티미디어(swf, mp3), 실행 파일(exe, torrent), PDF를 비롯한 기본적인 카테고리로 그룹화됩니다. 파일 제어는 악성코드 차단과 달리 Cisco 클라우드의 쿼리가 필요하지 않습니다.

악성코드 차단 및 파일제어 구성

라이센스: 보호 또는 악성코드

파일 정책을 액세스 제어 규칙과 연결하여 악성코드 차단 및 파일 제어를 전반적 액세스 제어 구성의 일부로 구성합니다. 이 연결은 시스템이 액세스 제어 규칙의 조건에 일치하는 트래픽에 파일을 통과시키기 전에 먼저 파일을 검사하도록 합니다.

상위 액세스 제어 정책과 마찬가지로, 파일 정책에는 각 규칙의 조건과 일치하는 파일을 처리하는 방식을 결정하는 규칙이 포함됩니다. 별도의 파일 규칙을 구성하여 각기 다른 파일 유형, 애플리케이션 프로토콜 또는 전송 방향마다 다른 작업을 실행할 수 있습니다.

파일이 규칙과 일치할 경우 규칙에서는 다음을 수행할 수 있습니다.

- 간단한 파일 유형 일치를 기준으로 파일 허용 또는 차단
- 악성코드 파일 속성을 기준으로 파일 차단
- 또한 파일 정책으로 다음을 수행할 수 있습니다. 정상 목록 또는 맞춤형 탐지 목록의 항목을 기준으로 파일을 안전한 파일 또는 악성코드로 자동 처리

간단한 예로, 사용자가 실행 파일을 다운로드하는 것을 차단하는 파일 정책을 구현할 수 있습니다. 파일 정책 및 이를 액세스 제어 규칙과 연결하는 방법에 대한 자세한 내용은 24-4페이지의 파일 정책 이해 및 생성을 참고하십시오.

악성 코드 차단 및 파일 제어를 기반으로 이벤트 로깅

라이센스: 보호 또는 악성코드

ASA FirePOWER 모듈은 시스템의 파일 검사 로깅 및 캡처된 파일처럼, 파일 이벤트 및 악성코드 이벤트 처리 레코드를 로깅합니다.

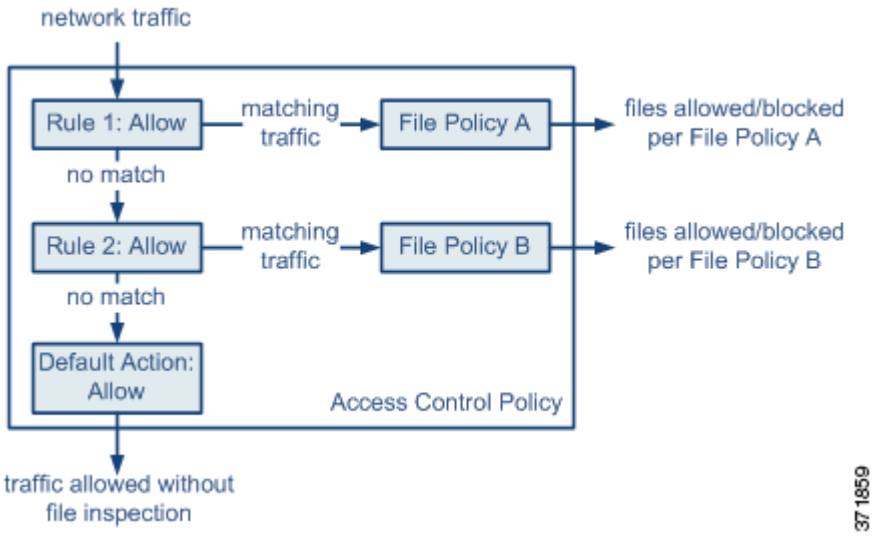
- *파일 이벤트*는 시스템이 네트워크 트래픽에서 탐지하고 선택적으로 차단한 파일을 나타냅니다.
- *악성코드 이벤트*는 시스템이 네트워크 트래픽에서 탐지하고 선택적으로 차단한 악성코드 파일을 나타냅니다.
- *소급 적용되는 악성코드 이벤트*는 악성코드 파일 속성이 변경된 파일을 나타냅니다.

시스템이 네트워크 트래픽에서 악성코드를 탐지하거나 차단하는 것에 기반하여 악성코드 이벤트를 생성하는 경우, 시스템은 또한 파일 이벤트도 생성합니다. 이는 파일에서 악성코드를 탐지하기 위해서는 시스템이 반드시 파일 자체를 먼저 탐지해야 하기 때문입니다.

파일 정책 이해 및 생성

라이센스: 보호 또는 악성코드

파일 정책은 지능형 악성코드 차단 및 파일 제어를 수행하기 위해 시스템에서 전체 액세스 제어 구성의 일부로 사용하는 구성 집합입니다.



정책에 두 개의 액세스 제어 규칙이 있으며, 두 규칙 모두 Allow(허용) 작업을 사용하고 파일 정책과 연결되어 있습니다. 정책의 기본 작업은 또한 파일 정책 검사 없이 트래픽을 허용하는 것입니다. 이 시나리오에서, 트래픽은 다음과 같이 처리됩니다.

- `Rule 1(규칙 1)`에 일치하는 트래픽은 `File Policy A(파일 정책 A)`로 검사합니다.
- `Rule 1(규칙 1)`에 일치하지 않는 트래픽은 `Rule 2(규칙 2)`에 대해 평가됩니다. `Rule 2(규칙 2)`에 일치하는 트래픽은`File Policy B(파일 정책 B)`로 검사합니다.
- 둘 중 어느 규칙과도 일치하지 않는 트래픽은 허용됩니다. 파일 정책을 기본 작업과 연결할 수 없습니다.

상위 액세스 제어 정책과 마찬가지로, 파일 정책에는 각 규칙의 조건과 일치하는 파일을 처리하는 방식을 결정하는 규칙이 포함됩니다. 별도의 파일 규칙을 구성하여 각기 다른 파일 유형, 애플리케이션 프로토콜 또는 전송 방향마다 다른 작업을 실행할 수 있습니다.

파일이 규칙과 일치할 경우, 규칙을 통해 다음을 수행할 수 있습니다.

- 간단한 파일 유형 일치를 기준으로 파일 허용 또는 차단
- 악성코드 파일 속성을 기준으로 파일 차단
- 또한 파일 정책으로 다음을 수행할 수 있습니다. 정상 목록 또는 맞춤형 탐지 목록의 항목을 기준으로 파일을 안전한 파일 또는 악성코드로 자동 처리

Allow(허용), **Interactive Block(인터랙티브 차단)** 또는 **Interactive Block with reset(인터랙티브 차단 후 재시작)**의 작업을 가진 액세스 제어 규칙과 단일 파일 정책을 연결할 수 있습니다. 그런 다음 시스템에서는 해당 파일 정책을 사용하여 액세스 제어 규칙의 조건을 충족하는 네트워크 트래픽을 검사합니다. 다양한 파일 정책을 서로 다른 액세스 제어 규칙과 연결할 경우, 네트워크에 전송된 파일을 식별하고 차단하는 방법을 세부적으로 제어할 수 있습니다. 그러나 파일 정책을 사용하여 액세스 제어 기본 작업에 의해 처리된 트래픽을 검사할 수는 **없습니다**. 자세한 내용은 10-2페이지의 침입 및 악성코드에 대해 허용된 트래픽 검사를 참고하십시오.

파일 규칙

파일 규칙으로 파일 정책을 채웁니다. 다음 표에는 파일 규칙의 구성 요소가 설명되어 있습니다.

표 24-2 파일 규칙 구성 요소

파일 규칙 구성 요소	설명
애플리케이션 프로토콜:	시스템에서는 FTP, HTTP, SMTP, IMAP, POP3, NetBIOS-ssn(SMB)을 통해 전송된 파일을 탐지하고 검사할 수 있습니다. 성능 향상을 위해 파일별 규칙을 기반으로 한 애플리케이션 프로토콜 중 하나만 대상으로 하여 파일 탐지를 제한할 수 있습니다.
전송 방향	다운로드한 파일에 대해 수신 FTP, HTTP, POP3, IMAP 및 NetBIOS-ssn(SMB) 트래픽을 검사할 수 있으며, 업로드한 파일에 대해서는 발신 FTP, HTTP, SMTP 및 NetBIOS-ssn(SMB) 트래픽을 검사할 수 있습니다.
파일 카테고리 및 유형	시스템에서는 다양한 유형의 파일을 탐지할 수 있습니다. 이 파일 유형은 멀티미디어(swf, mp3), 실행 파일(exe, torrent) 및 PDF를 포함하여 기본 카테고리로 분류됩니다. 개별 파일 유형을 탐지하거나, 파일 유형의 전체 카테고리를 탐지하는 파일 규칙을 구성할 수 있습니다. 예를 들어, 모든 멀티미디어 파일을 차단할 수도 있고, ShockWave Flash(swf) 파일만 차단할 수도 있습니다. 또는 사용자가 BitTorrent(torrent) 파일을 다운로드할 경우 알림을 제공하도록 시스템을 구성할 수 있습니다. ⚠ **주의** 빈번하게 트리거되는 파일 규칙은 시스템 성능에 영향을 줄 수 있습니다. 예를 들어, HTTP 트래픽(예: 상당량의 Flash 콘텐츠를 전송하는 YouTube)의 멀티미디어 파일을 탐지할 경우 지나치게 많은 이벤트가 생성될 수 있습니다.
파일 규칙 작업	파일 규칙 작업에서는 규칙의 조건과 일치하는 트래픽을 처리하는 방법을 결정합니다. **참고** 파일 규칙은 숫자나 순서가 아닌 규칙 작업으로 평가됩니다. 자세한 내용은 파일 규칙 작업 및 평가 순서 섹션을 참고하십시오.

파일 규칙 작업 및 평가 순서

각 파일 규칙에는 시스템이 규칙의 조건과 일치하는 트래픽을 처리하는 방법을 결정하는 관련 작업이 포함됩니다. 파일 정책 내에 별도의 규칙을 설정하여 서로 다른 파일 유형, 애플리케이션 프로토콜 또는 전송 방향에 맞는 다양한 작업을 실행할 수 있습니다. 규칙 작업은 다음과 같이 규칙-작업의 순서로 이루어집니다.

- *Block Files(파일 차단)* 규칙을 사용하면 특정 파일 유형을 차단할 수 있습니다.
- *Block Malware(악성코드 차단)* 규칙을 사용하면 특정 파일 유형의 SHA-256 해시 값을 계산할 수 있으며, 클라우드 조회 프로세스를 사용하여 네트워크를 통과하는 파일이 악성코드를 포함하는지 확인한 후 위협을 나타내는 파일을 차단할 수 있습니다.
- *Malware Cloud Lookup(악성코드 클라우드 조회)* 규칙을 사용하면 네트워크를 통과하는 파일의 악성코드 속성을 클라우드 조회에 기반하여 로깅할 수 있지만 여전히 해당 전송을 허용합니다.
- *Detect Files(파일 탐지)* 규칙을 사용하면 특정 파일 유형의 탐지를 로깅할 수 있지만, 여전히 해당 전송을 허용합니다.

각 파일 규칙 작업에 대해 파일 전송이 차단되었을 때 연결을 초기화하는 옵션 및 캡처된 파일을 ASA FirePOWER 모듈에 저장하는 옵션을 구성할 수 있습니다. 다음 표는 각 파일 작업에서 사용할 수 있는 옵션을 자세히 설명합니다.

표 24-3 파일 규칙 작업

작업	연결 초기화 여부
파일 차단	예(권장)
악성코드 차단	예(권장)
파일 탐지	아니요
악성코드 클라우드 조회	아니요

파일 및 악성코드 탐지, 캡처, 차단 참고 사항 및 제한 사항

파일 및 악성코드 탐지, 캡처, 그리고 차단 작업에 대한 다음 세부 사항 및 제한을 참고하십시오.

- 파일이 세션에서 탐지 및 차단될 때까지 세션의 패킷은 침입 확인의 대상이 될 수 있습니다.
- 파일 종료 마커가 파일을 위해 탐지되지 않는 경우, 전송 프로토콜에 관계 없이 해당 파일은 **Block Malware(악성코드 차단)** 규칙 또는 사용자 지정 탐지 목록에 의해 차단되지 않습니다. 시스템은 파일 종료 마커에 표시된 대로 전체 파일을 받을 때까지 파일을 차단하기 위해 대기하며, 마커가 탐지된 후 파일을 차단합니다.
- FTP 파일 전송을 위한 파일 종료 마커가 마지막 데이터 세그먼트와 별도로 전송되는 경우 마커는 차단되며 FTP 클라이언트는 파일 전송이 실패했다고 표시하지만 실제로 파일은 디스크에 완전히 전송됩니다.
- FTP는 다른 채널에 명령 및 데이터를 전송합니다. 수동 배포에서 FTP 데이터 세션 및 제어 세션 트래픽은 동일한 Snort로 부하 균형되어 있지 않습니다.
- 파일이 애플리케이션 프로토콜 조건을 갖춘 규칙에 일치하는 경우, 파일 이벤트 생성은 시스템이 파일의 애플리케이션 프로토콜을 확인한 후에 발생합니다. 확인되지 않은 파일은 파일 이벤트를 생성하지 않습니다.
- FTP를 위한 **Block Malware(악성코드 차단)** 규칙을 비롯한 파일 정책을 사용하는 액세스 제어 정책의 경우, 기본 작업을 **Drop when Inline(인라인 시 드롭)**을 비활성화한 침입 정책으로 설정한다면 시스템은 탐지된 파일 또는 규칙에 일치하는 악성코드를 위한 이벤트를 생성하지만 파일을 드롭하지 않습니다. 파일 정책을 선택하는 액세스 제어 정책에 대해 기본 작업으로 FTP 파일 전송을 차단하고 파일 정책을 사용하려면 반드시 침입 정책을 선택하고 **Drop when Inline(인라인 시 드롭)**을 활성화해야 합니다.
- **Block Files(파일 차단)** 및 **Block Malware(악성코드 차단)** 작업을 가진 파일 규칙은 초기 파일 전송 시도가 발생한 후 24시간 동안 탐지된 동일한 파일, URL, 서버 및 클라이언트 애플리케이션의 새로운 세션을 차단함으로써 HTTP를 통한 파일 다운로드가 자동으로 재개되는 것을 차단합니다.
- 드물게 HTTP 업로드 세션의 트래픽이 작동하지 않는 경우, 시스템은 트래픽을 제대로 다시 어셈블할 수 없으므로 트래픽을 차단하거나 파일 이벤트를 생성하지 않습니다.
- **Block Files(파일 차단)** 규칙으로 차단된 파일을 NetBIOS-ssn으로 전송하는 경우(SMB 파일 전송 등), 대상 호스트에서 파일을 확인할 수 있습니다. 그러나, 파일은 다운로드가 시작된 후 차단되기 때문에 사용할 수 없으며, 그 결과 파일 전송은 완료되지 않습니다.
- NetBIOS-ssn에 전송(SMB 파일 전송 등)된 파일을 검색하거나 차단하는 파일 규칙을 만드는 경우, 시스템은 파일 정책을 호출하는 액세스 제어 정책을 적용하기 전에 시작된, 설정된 TCP 또는 SMB 세션에서 전송된 파일을 검사하지 않으므로 해당 파일은 탐지 또는 차단되지 않습니다.

- 수동 배포에 파일을 차단하기 위해 구성된 규칙은 일치하는 파일을 차단하지 않습니다. 연결이 계속해서 파일을 전송하므로, 연결의 시작을 로깅하는 규칙을 구성하는 경우, 이 연결에 대해 로깅된 여러 이벤트를 볼 수 있습니다.
- POP3, POP, SMTP 또는 IMAP 세션에서 파일에 대한 모든 파일 이름의 총 바이트 수가 1024를 초과할 경우, 세션에서 파일 이벤트는 파일 이름 버퍼가 채워진 후 발견된 파일의 정확한 파일 이름을 반영하지 않을 수 있습니다.
- 텍스트 기반의 파일을 SMTP에 전송할 경우, 일부 메일 클라이언트는 줄 바꿈을 CRLF 줄 바꿈 문자 표준으로 변환합니다. Mac 기반의 호스트가 캐리지 리턴(CR) 문자를 사용하고 Unix/Linux 기반의 호스트가 라인 피드(LF) 문자를 사용하기 때문에, 메일 클라이언트에 의한 줄 바꿈 변환은 파일의 크기를 변경할 수 있습니다. 인식 불가능한 파일 유형을 처리할 때 일부 메일 클라이언트가 줄 바꿈 변환을 기본값으로 설정한다는 점에 유의하십시오.
- Cisco는 TCP 연결이 재설정될 때까지 차단된 애플리케이션 세션이 계속 열려있는 것을 방지하기 위해 **Block Files(파일 차단)** 및 **Block Malware(악성코드 차단)** 작업을 위한 **Reset Connection(연결 재설정)**을 활성화할 것을 권장합니다. 연결을 재설정하지 않은 경우, TCP 연결이 스스로 재설정될 때까지 클라이언트 세션은 열려 있습니다.
- 파일 규칙이 **Malware Cloud Lookup(악성코드 클라우드 조회)** 또는 **Block Malware(악성코드 차단)** 작업으로 구성되어 있고 ASA FirePOWER 모듈이 클라우드와의 연결을 설정할 수 없는 경우, 클라우드 연결이 복원될 때까지 시스템은 설정된 어떤 규칙도 수행할 수 없습니다.

파일 규칙 평가 예

규칙이 번호 순서대로 평가되는 액세스 제어 정책과 달리, 파일 정책은 24-5페이지의 파일 규칙 작업 및 평가 순서 내 파일을 처리합니다. 즉 단순 차단은 악성코드 탐지 및 차단보다 우선하는데, 이는 단순 탐지 및 로깅에 우선하는 것입니다. 예를 들어, 단일 파일 정책에서 PDF 파일을 처리하는 네 가지 규칙을 고려하십시오. 모듈 인터페이스에 나타나는 순서에 상관없이, 이 규칙은 다음 순서대로 평가됩니다.

표 24-4 파일 규칙 평가 순서 예

애플리케이션 프로토콜	방향	작업	작업 옵션	결과
SMTP	업로드	파일 차단	연결 재설정	사용자를 이메일링 PDF 파일로부터 차단하고 연결을 재설정합니다.
FTP	다운로드	악성코드 차단	연결 재설정	파일 전송을 통해 악성코드 PDF 파일 다운로드를 차단하고, 연결을 재설정합니다.
POP3 IMAP	다운로드	악성코드 클라우드 조회		악성코드 탐지를 위해 이메일을 통해 수신된 PDF 파일을 검사합니다.
모두	모두	파일 탐지	없음	사용자가 웹에서 PDF를 볼 때(즉 HTTP를 통해), 트래픽을 탐지하고 로깅하지만 허용합니다.

ASA FirePOWER 모듈은 경고 아이콘(⚠)을 사용하여 충돌하는 파일 규칙을 지정합니다.

시스템에서 탐지된 모든 파일 유형에서 악성코드 분석을 수행할 수 없다는 점에 유의하십시오. 사용자가 **Application Protocol(애플리케이션 프로토콜)**, **Direction of Transfer(전송 방향)**, 및 **Action(작업)** 드롭다운 목록에서 값을 선택한 후에는 시스템이 파일 유형 목록을 제한합니다.

로깅 파일 이벤트, 악성코드 이벤트 및 경고

액세스 제어 정책 규칙과 파일 정책을 연결할 때, 시스템은 일치하는 트래픽을 위한 파일 및 악성코드 이벤트 로깅을 자동으로 활성화합니다. 시스템이 파일을 검사할 때, 다음 유형의 이벤트를 생성할 수 있습니다.

- *파일 이벤트*, 탐지되거나 차단된 파일 및 탐지된 악성코드 파일을 나타냄
- *악성코드 이벤트*, 탐지된 악성코드 파일을 나타냄
- *소급 적용되는 악성코드 이벤트*, 이전에 탐지된 파일에 대한 악성코드 파일 속성이 변경되는 경우 생성됨

파일 정책이 파일 또는 악성코드 이벤트를 생성하거나 파일을 캡처하는 경우, 시스템은 액세스 제어 규칙 호출이라는 로깅 구성에 상관 없이 결합된 연결의 종료를 자동으로 로깅합니다.

참고 클라이언트와 서버에 지속적인 연결이 설정되어 있기 때문에 NetBIOS-ssn (SMB) 트래픽 검사에 의해 생성된 파일 이벤트가 즉시 연결 이벤트를 생성하지는 않습니다. 시스템은 클라이언트 또는 서버가 세션을 종료한 후 연결 이벤트를 생성합니다.

각 연결 이벤트의 경우

- **Files(파일)** 필드는 (악성코드 파일을 포함하여) 연결에서 탐지된 파일의 수를 나타내는 아이콘 ( )에 표시됩니다. 해당 파일의 목록을 보려면 해당 아이콘을 클릭하고, 악성코드 파일에 대해 보려면 파일 속성 목록을 클릭합니다.
- **Reason(원인)** 필드는 연결 이벤트가 로깅된 이유를 나타내는데, 파일 작업 규칙에 따라 다릅니다.
  - `File Monitor(파일 모니터링)`. Detect Files(파일 탐지) 및 Malware Cloud Lookup(악성코드 클라우드 조회) 파일 규칙, 그리고 정상 목록 상의 파일의 경우
  - `File Block(파일 차단)`. Block Files(파일 차단) 또는 Block Malware(악성코드 차단) 파일 규칙의 경우
  - 시스템이 사용자 지정 탐지 목록에서 파일을 발견한 경우 `File Custom Detection(파일 사용자 지정 탐지)`
  - 파일 전송이 Block Files(파일 차단) 또는 Block Malware(악성코드 차단) 파일 규칙에 의해 근원적으로 차단된 경우 `File Resume Allow(파일 재시작 허용)` 새로운 액세스 제어 정책이 적용되어 파일이 허용되면 HTTP 세션은 자동으로 다시 시작됩니다.
  - 파일 전송이 Detect Files(파일 탐지) 및 Malware Cloud Lookup(악성코드 클라우드 조회) 파일 규칙에 의해 근원적으로 차단된 경우 `File Resume Block(파일 재시작 차단)` 새로운 액세스 제어 정책이 적용되어 파일이 차단되면 HTTP 세션은 자동으로 중단됩니다.
- 파일 또는 악성코드가 차단된 연결의 경우 **Action(작업)**은 `Block(차단)`입니다.

ASA FirePOWER 모듈에 의해 생성된 모든 종류의 이벤트와 마찬가지로 사용자는 파일 및 악성코드 이벤트를 보고 분석할 수 있습니다. 사용자는 또한 악성코드 이벤트를 사용하여 , SNMP 또는 syslog를 통해 경고합니다.

인터넷 액세스

시스템은 포트 443을 사용하여 네트워크 기반 AMP를 위한 악성코드의 클라우드 검색을 수행합니다. 사용자는 반드시 ASA FirePOWER 모듈의 아웃바운드 포트를 열어야 합니다.

파일 정책 관리

사용자는 파일 정책 페이지(**Policies(정책) > Files(파일)**)에서 파일 정책을 작성, 수정, 삭제, 비교합니다. 이는 사용자의 최종 수정 날짜와 함께 기존 파일 정책 목록을 표시합니다.

파일 정책을 위해 적용 아이콘( )을 클릭하면 어떤 액세스 제어 정책이 파일 정책을 사용하는지 알려주는 대화 상자가 표시된 다음, Access Control Policy(액세스 제어 정책) 페이지로 리디렉션됩니다. 이는 파일 정책이 상위 액세스 제어 정책의 일부로 간주되어 독립적으로 적용할 수 없기 때문입니다. 새 파일 정책을 사용하거나, 기존 파일 정책에 수정을 가하기 위해서는 반드시 상위 액세스 제어 정책을 적용하거나 재적용해야 합니다.

사용자는 저장되거나 적용된 액세스 제어 정책에서 사용되는 파일 정책을 삭제할 수 없다는 점에 유의하십시오.

파일 정책 관리에 대한 자세한 내용은 다음 섹션을 참고하십시오.

- 24-9페이지의 파일 정책 생성
- 24-10페이지의 파일 규칙 작업
- 24-12페이지의 두 개의 파일 정책 비교

파일 정책 생성

라이센스: 보호 또는 악성코드

파일 정책을 만들고 규칙으로 채운 후에는 액세스 제어 정책에서 이를 사용할 수 있습니다.

팁 기존 파일 정책의 복사본을 만들려면, 복사 아이콘( )을 클릭한 다음, 표시되는 대화 상자에서 새로운 정책의 고유한 이름을 입력합니다. 그러면 복사본을 수정할 수 있습니다.

파일 정책을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Files(파일)**를 선택합니다.

File Policies(파일 정책) 페이지가 나타납니다.

단계 2 **New File Policy(새 파일 정책)**를 클릭합니다.

New File Policy(새 파일 정책) 대화 상자가 나타납니다.

새로운 정책의 경우, 모듈 인터페이스는 정책이 사용되고 있지 않음을 표시합니다. 사용 중인 파일 정책을 수정할 경우, 모듈 인터페이스는 얼마나 많은 액세스 제어 정책이 파일 정책을 사용하는지 보여줍니다. 둘 중 어느 경우에도 텍스트를 클릭하여 Access Control Policies(액세스 제어 정책) 페이지로 이동합니다(4-1페이지의 액세스 제어 정책 시작하기 참고).

단계 3 새로운 정책을 위한 **Name(이름)**과 선택적으로 **Description(설명)**을 입력한 후 **Save(저장)**를 클릭합니다.

File Policy Rules(파일 정책 규칙) 탭이 나타납니다.

단계 4 파일 정책에 하나 이상의 규칙을 추가합니다.

파일 규칙은 악성코드 탐지를 위해 어떤 파일 유형을 로깅하거나, 차단, 확인하기를 원하는지에 대해 세분화된 제어 기능을 제공합니다. 파일 추가 규칙에 대한 자세한 내용은 24-10페이지의 파일 규칙 작업을 참고하십시오.

단계 5 고급 옵션을 구성합니다. 자세한 내용은 24-11페이지의 고급 파일 정책 일반 옵션 구성을 참고하십시오.

단계 6 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항)**를 클릭합니다.

새로운 정책을 사용하려면 반드시 액세스 제어 정책 규칙에 파일을 추가한 후 다음 액세스 제어 정책을 적용해야 합니다. 기존 파일 정책을 수정할 경우, 반드시 파일 정책을 사용하는 액세스 제어 정책을 재적용해야 합니다.

파일 규칙 작업

라이센스: 보호 또는 악성코드

파일 정책은 하나 이상의 규칙을 포함해야 적용할 수 있습니다. 새로운 파일 정책을 만들거나 기존 정책을 수정할 때 표시되는 File Policy Rules(파일 정책 규칙 페이지)에서 규칙을 작성, 수정, 삭제합니다. 페이지는 각 규칙의 기본 특성과 함께 정책의 모든 규칙을 나열합니다.

해당 페이지는 또한 얼마나 많은 액세스 제어 정책이 이 파일 정책을 사용하는지 알려줍니다. 상위 정책 목록을 표시하고 선택적으로, Access Control Policies(액세스 제어 정책) 페이지로 이동하려면 알림을 클릭합니다.

파일 규칙을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Files(파일)**를 선택합니다.

File Policies(파일 정책) 페이지가 나타납니다.

단계 2 다음 옵션을 이용할 수 있습니다.

- 새로운 정책에 규칙을 추가하려면, **New File Policy(신규 파일 정책)**를 클릭하여 새로운 정책을 만듭니다(24-9페이지의 파일 정책 생성 참고).
- 기존 정책에 규칙을 추가하려면, 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

단계 3 이때 표시되는 File Policy Rules(파일 정책 규칙)에서 **Add File Rule(파일 규칙 추가)**을 클릭합니다.

Add File Rule(파일 규칙 추가) 대화 상자가 표시됩니다.

단계 4 드롭다운 목록에서 **Application Protocol(애플리케이션 프로토콜)**을 선택합니다.

기본값인 **Any(모두)**는 HTTP, SMTP, POP3, IMAP, FTP 및 NetBIOS-ssn (SMB) 트래픽에서 파일을 탐지합니다.

단계 5 드롭다운 목록에서 **Direction of Transfer(전송 방향)**를 선택하십시오.

다운로드한 파일에 대해 다음 유형의 수신 트래픽을 검사할 수 있습니다.

- HTTP
- IMAP
- POP3
- FTP
- NetBIOS-ssn(SMB)

업로드한 파일에 대해 다음 유형의 발신 트래픽을 검사할 수 있습니다.

- HTTP
- FTP
- SMTP
- NetBIOS-ssn(SMB)

사용자가 전송하는지 또는 수신하는지에 상관 없이, **Any(모두)**를 사용하여 여러 애플리케이션 프로토콜에서 파일을 탐색합니다.

단계 6 파일 규칙 **Action(작업)**을 선택합니다. 자세한 내용은 파일 규칙 작업 표를 참고하십시오.

Block Files(파일 차단) 또는 **Block Malware(악성코드 차단)**를 선택하면 **Reset Connection(연결 재설정)**이 기본값으로 활성화됩니다. 차단된 파일 전송이 발생한 연결을 재설정하지 **않으려면 Reset Connection(연결 재설정)** 확인 상자를 비워둡니다.

참고 Cisco는 TCP 연결이 재설정될 때까지 차단된 애플리케이션 세션이 계속 열려있는 것을 방지하기 위해 **Reset Connection(연결 재설정)**을 활성화 상태로 유지할 것을 권장합니다.

파일 규칙 작업에 대한 자세한 내용은 24-5페이지의 파일 규칙 작업 및 평가 순서를 참고하십시오.

단계 7 하나 이상의 **File Types(파일 유형)**를 선택합니다. Ctrl 키와 Shift 키를 사용하여 여러 파일의 유형을 선택합니다. 파일 유형 목록을 다음 방법으로 필터링할 수 있습니다.

- 하나 이상의 **File Type Categories(파일 유형 카테고리)**를 선택합니다.
- 해당 이름 또는 설명으로 파일 유형을 검색합니다. 예를 들어, Microsoft Windows 특유의 파일 목록을 표시하려면 `Windows`를 **Search name and description(이름 및 설명 검색)** 필드에 입력합니다.

파일 규칙에서 사용할 수 있는 파일 유형은 **Application Protocol(애플리케이션 프로토콜)**, **Direction of Transfer(전송 방향)** 및 **Action(작업)**에 대한 선택에 따라 달라집니다.

예를 들어, **Direction of Transfer(전송 방향)**로 **Download(다운로드)**를 선택하면 파일 이벤트의 초과를 방지하기 위해 `GIF`, `PNG`, `JPEG`, `TIFF` 및 `ICO`를 **Graphics(그래픽)** 카테고리에서 삭제합니다.

단계 8 **Selected Files Categories and Types(선택한 파일 카테고리 및 유형)** 목록에 선택한 파일 카테고리를 추가합니다.

- 규칙에 선택한 파일 유형을 추가하려면 **Add(추가)**를 클릭합니다.
- **Selected Files Categories and Types(선택한 파일 카테고리 및 유형)** 안에 하나 이상의 파일 유형을 끌어 놓습니다.
- 카테고리를 선택한 상태에서, **All types in selected Categories(선택한 카테고리의 모든 유형)**를 클릭한 후 **Add(추가)**를 클릭하거나 선택한 사항을 **Selected Files Categories and Types(선택한 파일 카테고리 및 유형)** 목록 안에 끌어 놓습니다.

단계 9 **Store ASA FirePOWERChanges(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

파일 규칙이 정책에 추가됩니다. 기존 파일 정책을 수정할 경우 반드시 변경 사항이 적용되도록 파일 정책을 사용하는 액세스 제어 정책을 재적용해야 합니다.

고급 파일 정책 일반 옵션 구성

라이센스: 악성코드

파일 정책 내 General(일반) 섹션에서 다음 고급 옵션을 설정할 수 있습니다.

표 24-5 고급 파일 정책 일반 옵션

필드	설명	기본값
사용자 지정 탐지 목록 활성화	사용자 지정 탐지 목록에서 탐지된 파일을 차단하려면 선택합니다.	활성화
정상 목록 활성화	정상 목록에서 탐지된 파일을 허용하려면 선택합니다.	활성화

고급 파일 정책 일반 옵션을 구성하려면

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Files(파일)**를 선택합니다.

File Policies(파일 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

File Policy Rule(파일 정책 규칙) 페이지가 나타납니다.

단계 3 **Advanced(고급)** 탭을 선택합니다.

Advanced(고급) 탭이 나타납니다.

단계 4 고급 파일 정책 일반 옵션 표에 설명된 대로 옵션을 수정합니다.

단계 5 **Store ASA FirePOWERChanges(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

수정한 파일 정책을 사용한 액세스 제어 정책을 다시 적용해야 합니다.

두 개의 파일 정책 비교

라이센스: 보호

사용자 조직의 표준 준수를 위한 정책 변경 사항을 검토하거나 시스템 성능을 최적화하기 위해 두 개의 파일 정책 간 차이, 또는 동일한 정책의 2가지 수정 버전 간 차이를 검토할 수 있습니다.

파일 정책 *비교 보기*는 두 개의 파일 정책 또는 수정 버전을 나란한 형식으로 표시하는데, 각 정책 이름 옆에 최종 수정 시간 및 최종 수정 사용자를 보여줍니다. 두 정책 간 차이점은 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책 사이에서 다름을 나타내고, 그러한 차이점은 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 한 정책에서는 나타하지만 다른 정책에서는 나타나지 않음을 표시합니다.

Previous(이전) 및 **Next(다음)**를 클릭하여 차이점을 살펴볼 수 있습니다. 좌우 측면 사이에 있는 이중 화살표 아이콘()을 움직여 **Difference(차이)** 수를 조정하여 표시되는 차이점이 무엇인지 확인합니다. 또는, 비교 보기의 PDF 버전인 파일 정책 *비교 보고서*를 생성할 수 있습니다.

두 개의 파일 정책을 비교하려면

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Files(파일)**를 선택합니다.

File Policies(파일 정책) 페이지가 나타납니다.

단계 2 **Compare Policies(정책 비교)**를 클릭합니다.

Select Comparison(항목 선택) 대화 상자가 표시됩니다.

단계 3 **Compare Against(비교 대상)** 드롭다운 목록에서 비교를 원하는 유형을 선택합니다.

- 두 가지 정책을 비교하려면, **Running Configuration(운영 구성)** 또는 **Other Policy(다른 정책)** 중 하나를 선택합니다. 두 가지 옵션 간 실제적인 차이점은 **Running Configuration(운영 구성)**을 선택한 경우 시스템이 비교 선택 중 하나를 최근 적용된 파일 정책의 집합으로 제한한다는 것입니다.
- 동일한 정책의 수정 버전을 비교하려면, **Other Revision(다른 수정 버전)**을 선택합니다.

대화 상자는 새로 복구되고, 비교 옵션을 표시합니다.

단계 4 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 가지 서로 다른 정책을 비교할 경우, 비교를 원하는 정책을 선택합니다. **Policy A(정책 A)** 또는 **Target/Running Configuration A(대상/운영 구성 A)** 및 **Policy B(정책 B)**.
- 동일한 정책의 수정 버전을 비교하는 경우, 사용을 원하는 **Policy(정책)**를 선택하고, 두 가지 버전 중에서 선택합니다. **Revision A(수정 버전 A)**와 **Revision B(수정 버전 B)**. 수정 버전은 날짜 및 사용자 이름으로 나열됩니다.

단계 5 **OK(확인)**를 클릭합니다.

비교 보기가 나타납니다.

또는, **Comparison Report(비교 보고서)**를 클릭하여 파일 정책 비교 보고서를 생성합니다.사용자에게 보고서를 컴퓨터에 저장하라는 메시지가 표시됩니다.

네트워크 트래픽의 연결 로깅

디바이스에서 네트워크의 호스트에 의해 생성되는 트래픽을 모니터링하면 디바이스는 탐지한 연결의 로그를 생성할 수 있습니다. 액세스 제어 정책의 다양한 설정을 통해 로깅할 연결, 로깅할 시점 및 데이터를 저장할 위치를 세부적으로 제어할 수 있습니다. 또한 액세스 제어 규칙의 특정 로깅 구성을 통해 연결과 관련된 파일 및 악성코드 이벤트의 로깅 여부가 결정됩니다.

대부분의 경우 연결이 시작될 때 및 연결이 끝날 때 연결을 로깅할 수 있습니다. 연결을 로깅하면 시스템에서 *연결 이벤트*가 생성됩니다. 또한 연결이 신뢰도에 기반을 둔 Security Intelligence(보안 인텔리전스) 기능을 통해 차단 목록에 추가(차단)되어 있는 경우 언제든지 *Security Intelligence(보안 인텔리전스) 이벤트*라는 특수한 유형의 연결 이벤트를 로깅할 수도 있습니다.

연결 이벤트에는 탐지된 세션에 관한 데이터가 포함되어 있습니다.

조직의 보안 및 규정 준수 필요에 따라 연결을 로깅해야 합니다.

연결 데이터 로깅에 대한 자세한 내용은 다음을 참고하십시오.

로깅할 연결 결정하기

라이센스: 모두

액세스 제어 정책의 다양한 설정을 사용하여 ASA FirePOWER 모듈에서 모니터링하는 모든 연결을 로깅할 수 있습니다. 대부분의 경우 연결이 시작될 때 및 연결이 끝날 때 연결을 로깅할 수 있습니다. 하지만 차단된 트래픽이 추가 검사 없이 즉시 거부되므로 시스템에서 차단되거나 차단 목록에 추가된 트래픽에 대한 연결 시작 이벤트만 로깅할 수 있으며, 고유한 연결의 종료는 로깅할 수 없습니다.

연결 이벤트를 로깅하면 이벤트 뷰어에서 로깅한 이벤트를 확인할 수 있습니다. 또한 외부 syslog 또는 SNMP 트랩 서버로 연결 데이터를 보낼 수 있습니다.

팁 ASA FirePOWER 모듈을 사용하여 연결 데이터에 대한 자세한 분석을 수행할 때 Cisco는 에 대한 중요한 연결의 종료를 로깅할 것을 권장합니다.

자세한 내용은 다음을 참고하십시오.

중요한 연결 로깅

라이센스: 모두

조직의 보안 및 규정 준수 필요에 따라 연결을 로깅해야 합니다. 사용자가 생성하고 기능을 향상시키는 이벤트의 수를 제한하는 것이 사용자의 목표라면 사용자의 분석에 중요한 연결에 대한 로깅만 활성화합니다. 그러나, 자료 수집을 목적으로 사용자의 네트워크 트래픽에 대한 광범위한 견해를 원할 경우, 추가 연결에 대한 로깅을 활성화할 수 있습니다. 액세스 제어 정책의 다양한 설정을 통해 로깅할 연결, 로깅할 시점 및 데이터를 저장할 위치를 세부적으로 제어할 수 있습니다.

주의 서비스 거부(DoS) 공격 중 차단된 TCP 연결을 로깅하는 것은 수 있고, 다수의 유사한 이벤트로 시스템을 마비시킬 수 있습니다. Block(차단) 규칙에 대한 로깅을 활성화하기 전에, 해당 규칙이 인터넷에 연결된 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스의 트래픽을 모니터링하고 있는지 여부를 고려하시기 바랍니다.

시스템은 사용자가 구성하는 로깅 외에도 시스템이 금지된 파일, 악성코드, 또는 침입 시도를 탐지한 곳에서 대부분의 연결을 자동으로 로깅합니다. 시스템은 추가 분석을 위해 연결 이벤트 종료 상황을 저장합니다. 모든 연결 이벤트는 Action and Reason(실행 및 원인) 필드를 사용하여 자동으로 로깅한 이유를 반영합니다.

보안 인텔리전스 차단 목록 추가 결정(선택 사항)

평판 기반 보안 인텔리전스 기능을 통해 차단 목록에 추가된(차단된) 경우에는 언제나 연결을 로깅할 수 있습니다. 또는, 수동 배포에서 권장되는 대로, 보안 인텔리전스 필터링을 위한 모니터링 전용 설정을 사용할 수 있습니다. 이를 통해 시스템은 차단 목록에 추가되었을 수도 있지만 여전히 차단 목록에 일치하여 로깅하는 연결을 추가로 분석할 수 있습니다.

보안 인텔리전스 로깅을 활성화하면 차단 목록 일치는 보안 인텔리전스 이벤트 및 연결 이벤트를 생성합니다. 보안 인텔리전스 이벤트는 연결 이벤트의 특수 카테고리로서, 사용자가 별도로 살펴보고 분석할 수 있으며, 또한 별도로 저장하거나 각각 잘라낼 수도 있습니다. 자세한 내용은 25-8페이지의 보안 인텔리전스(차단 목록 추가) 결정 로깅을 참고하십시오.

액세스 제어 처리(선택 사항)

액세스 제어 규칙 또는 액세스 제어 기본값 실행이 처리되면 연결을 로깅할 수 있습니다. 중요한 연결만 로깅하도록 하려면 각 액세스 제어 규칙 기반으로 이 로깅을 구성합니다. 자세한 내용은 25-9페이지의 액세스 제어 처리에 기반한 연결 로깅을 참고하십시오.

침입과 결합된 연결(자동)

액세스 제어 규칙에 의해 호출된 침입 정책(6-1페이지의 액세스 제어 규칙을 사용한 트래픽 흐름 조정 참고)이 침입을 탐지하고 침입 이벤트를 생성하면, 규칙의 로깅 구성에 상관 없이 시스템에서에 침입이 발생한 연결의 종료를 자동으로 로깅합니다.

그러나, 액세스 제어 기본 작업과 관련된 침입 정책(4-4페이지의 네트워크 트래픽에 대한 기본 처리와 검사 설정 참고)이 침입 이벤트를 생성할 때 시스템은 결합된 연결의 종료를 자동으로 로깅하지 **않습니다**. 대신, 사용자는 반드시 기본 작업 연결 로깅을 명시적으로 활성화해야 합니다. 이는 사용자가 연결 데이터를 로깅하는 것을 원하지 않을 때 침입 방지 전용 배포에 유용합니다.

침입이 차단된 연결을 위한 연결 로그 내 연결 작업은 `Block(차단)`입니다. 그 이유는 `Intrusion Block(침입 차단)`이며, 침입 탐지 수행을 위해서라면 반드시 Allow(허용) 규칙을 사용해야 합니다.

파일 및 악성 프로그램 이벤트와 결합된 연결(자동)

액세스 제어 규칙에 의해 호출된 파일 정책이 금지된 파일(악성코드 포함)을 탐지하고 파일 또는 악성코드 이벤트를 생성하면, 액세스 제어 규칙의 로깅 구성에 상관 없이에 대한 파일이 탐지된 연결의 종료를 시스템에서 자동으로 로깅합니다. 사용자는 이 로깅을 비활성화 할 수 **없습니다**.

참고 클라이언트와 서버에 지속적인 연결이 설정되어 있기 때문에 NetBIOS-ssn(SMB) 트래픽 검사에 의해 생성된 파일 이벤트가 즉시 연결 이벤트를 생성하지는 않습니다. 시스템은 클라이언트 또는 서버가 세션을 종료한 후 연결 이벤트를 생성합니다.

파일이 차단된 경우의 연결을 위한 연결 로그 내 연결 작업은 `Block(차단)`입니다. 파일 또는 악성코드 탐지를 수행하려는 경우에도 Allow(허용) 규칙을 사용해야 합니다. 연결하는 이유는 `File Monitor`(파일 모니터링, 파일 유형 또는 악성코드가 탐지된 경우), `Malware Block`(악성 프로그램 차단) 또는 `File Block`(파일 차단, 파일이 차단된 경우)입니다.

연결 시작 및 종료 로깅

라이센스: 모두

시스템이 연결을 탐지하면, 대부분의 경우 해당 시작 및 종료 시 로깅할 수 있습니다.

하지만 차단된 트래픽은 추가 검사 없이 즉시 거부당하기 때문에, 대부분의 경우 사용자는 차단 또는 차단 목록에 추가된 트래픽에 대한 연결 이벤트가 시작만을 로깅할 수 있으며, 연결을 로깅하는 데 고유한 마무리 단계는 없습니다.

참고 단일 비차단 연결의 경우, 연결 종료 이벤트에는 연결 시작 이벤트의 모든 정보가 포함되며, 세션 기간 동안 수집된 정보 또한 포함됩니다.

어떤 이유로든 연결 모니터링은 연결 종료 로깅을 강제한다는 것에 주의하십시오(25-5페이지의 모니터링된 연결 로깅에 대한 이해 참조).

다음 표는 연결 시작 이벤트와 연결 종료 이벤트 간의 차이를 자세히 설명하며, 각 로깅의 이점이 포함되어 있습니다.

표 25-1 연결 시작 이벤트와 연결 종료 이벤트 비교

	연결 시작 이벤트	연결 종료 이벤트
생성이 가능합니다...	시스템이 연결 시작을 탐지하는 경우 (또는 이벤트 발생이 애플리케이션 또는 URL ID에 의존하는 경우 처음 몇 패킷 후)	시스템에서 • 연결 차단을 탐지하는 경우 • 일정 시간이 지난 후 연결 종료를 탐지하지 않는 경우 • 메모리 제약 조건 때문에 더 이상 세션을 추적할 수 없는 경우
로깅할 수 있습니다...	보안 인텔리전스 또는 액세스 제어 규칙에서 평가한 모든 연결	모든 연결이 구성 가능합니다. 시스템이 차단된 또는 차단 목록에 추가된 연결 종료를 로깅할 수 없습니다
포함합니다...	첫 번째 패킷 (또는 이벤트 생성이 애플리케이션 또는 URL ID에 의존하는 경우 처음 몇 패킷)에서 확인될 수 있는 정보만	연결 시작 이벤트의 모든 정보와 더불어 세션 기간 동안의 트래픽을 검토하여 결정되는 정보. 예를 들어, 전송되는 데이터의 총량 또는 연결에서 마지막 패킷의 타임 스탬프
유용합니다...	다음을 로깅하려는 경우 • 보안 인텔리전스 차단 목록 추가 결정을 포함한 차단된 연결	다음을 원하는 경우 • 세션 기간 동안 수집된 정보에 관한 모든 종류의 상세 분석 작업을 수행 • 그래픽 형식으로 연결 데이터를 살펴보기

ASA FirePOWER 모듈 또는 외부 서버에 대한 연결 로깅

라이센스: 모두

사용자는ASA FirePOWER 모듈 및 외부 syslog 또는 SNMP 트랩 서버에 대한 연결 이벤트를 로깅할 수 있습니다. 사용자는 *alert response(경고 응답)*라는 외부 서버에 대한 연결을 구성해야 해당 서버에 대한 연결 데이터를 로깅할 수 있습니다(27-2페이지의 경고 응답 작업 참조).

액세스 제어 규칙 작업이 로깅에 영향을 미치는 방식에 대한 이해

라이센스: 기능에 따라 다름

각 액세스 제어 규칙에는 시스템이 규칙과 일치하는 트래픽을 탐지하고 처리하는 방식뿐 아니라 사용자가 해당 트래픽에 대한 세부 정보를 로깅하는 시기와 방식을 결정하는 *작업*이 있습니다.

자세한 내용은 다음을 참고하십시오.

- 6-6페이지의 규칙 작업을 사용하여 트래픽 관리 및 검사 결정
- 25-5페이지의 모니터링된 연결 로깅에 대한 이해
- 25-5페이지의 신뢰할 수 있는 연결에 대한 로깅 이해
- 25-5페이지의 차단된 연결 및 인터랙티브 차단된 연결 로깅에 대한 이해
- 25-6페이지의 허용된 연결에 대한 로깅 이해
- 25-7페이지의 허용된 연결에 대한 파일 및 악성코드 이벤트 로깅 비활성화

모니터링된 연결 로깅에 대한 이해

라이센스: 기능에 따라 다름

시스템은 나중에 연결을 처리하게 될 규칙 또는 기본 작업의 로깅 구성에 관계없이 항상ASA FirePOWER 모듈에 대한 다음 연결의 종료를 로깅합니다.

- 모니터에 설정된 보안 인텔리전스 차단 목록과 일치하는 연결
- 액세스 제어 모니터링 규칙과 일치하는 연결

즉 모니터링 규칙 또는 보안 인텔리전스에서 모니터링된 차단 목록에 패킷에 일치하는 경우, 패킷이 다른 규칙에 일치하지 않고 기본 작업 로깅을 활성화하지 않은 경우에도 연결은 항상 로깅됩니다. 보안 인텔리전스 필터링의 결과로 시스템에서 연결 이벤트를 로깅할 때마다 시스템은 또한 일치하는 보안 인텔리전스 이벤트도 로깅합니다. 이는 사용자가 별도로 살펴보고 분석할 수 있는 특수한 연결 이벤트입니다(25-8페이지의 보안 인텔리전스(차단 목록 추가) 결정 로깅 참조).

모니터링된 트래픽은 항상 추후 다른 규칙 또는 기본 작업에 의해 처리되므로, 모니터링 규칙으로 인해 로깅된 연결과 결합된 작업은 절대 모니터링할 수 없습니다. 대신, 이는 추후 연결을 처리할 규칙 또는 기본 작업의 실행을 반영합니다.

단일 연결이 SSL 또는 액세스 제어 모니터링 규칙에 일치할 때마다 시스템이 개별 이벤트를 생성하는 것은 **아닙니다**. 단일 연결이 다수의 모니터링 규칙과 일치할 수 있으므로,ASA FirePOWER 모듈에 로깅된 각 연결 이벤트는 연결과 일치하는 첫 8개의 모니터링 액세스 제어 규칙에 관한 정보를 포함하고 표시할 수 있습니다.

마찬가지로, 사용자가 외부 syslog 또는 SNMP 트랩 서버에 연결 이벤트를 보낼 경우, 시스템은 단일 연결이 모니터링 규칙에 일치할 때마다 별도의 경고를 보내지는 않습니다. 그보다, 연결 종료 시 시스템이 보내는 경고는 연결과 일치하는 모니터링 규칙에 관한 정보를 포함합니다.

신뢰할 수 있는 연결에 대한 로깅 이해

라이센스: 기능에 따라 다름

신뢰할 수 있는 연결이란 액세스 제어 정책에서 신뢰 액세스 제어 규칙 또는 기본 작업이 처리한 것입니다. 사용자는 연결의 시작 및 종료를 로깅할 수 있습니다. 하지만 신뢰할 수 있는 연결은, 침입, 또는 금지된 파일 및 악성코드 검사의 대상이 되지 않는다는 점에 유의하십시오. 따라서, 신뢰할 수 있는 연결에 대한 연결 이벤트는 제한된 정보를 포함합니다.

차단된 연결 및 인터랙티브 차단된 연결 로깅에 대한 이해

라이센스: 기능에 따라 다름

트래픽을 차단하는 액세스 제어 규칙 및 액세스 제어 정책 기본 작업(인터랙티브 차단 규칙 포함)의 경우, 시스템은 **연결의** 시작 이벤트를 로깅합니다. 일치하는 트래픽은 추가 검사 없이 거부됩니다.

액세스 제어 규칙에 따라 차단된 세션의 연결 이벤트에는 `Block(차단)` 또는 `Block with reset(차단 후 초기화)` 작업이 있습니다.

인터랙티브 차단 액세스 제어 규칙은 사용자가 차단된 웹 사이트를 탐색할 때 시스템이 경고 페이지를 표시하도록 하며,연결 종료를 로깅합니다. 이는 사용자가 경고 페이지를 통해 클릭할 경우, 이 연결은 시스템이 모니터링 및 로깅할 수 있는 새롭게 허용된 연결로 간주되기 때문입니다(25-6페이지의 허용된 연결에 대한 로깅 이해 참조).

따라서, 인터랙티브 차단 또는 인터랙티브 차단 후 초기화 규칙과 일치하는 패킷의 경우, 시스템은 다음 연결 이벤트를 생성할 수 있습니다.

- 사용자 요구가 초기에 차단되고 경고 페이지가 표시된 연결 시작 이벤트. 이 이벤트에는 Interactive Block(인터랙티브 차단) 또는 Interactive Block with reset(인터랙티브 차단 후 초기화)이라는 관련 작업이 있습니다.
- 사용자가 경고 페이지를 통해 클릭하고 원래 요청된 페이지를 로드하는 경우 다중의 연결 시작 또는 종료 이벤트. 이 이벤트에는 Allow(허용) 및 User Bypass(사용자 우회)의 이유와 관련된 작업이 있습니다.

인라인으로 구축된 디바이스만이 트래픽을 차단할 수 있음을 참고하기 바랍니다. 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에, 시스템은 각 차단된 연결에 대한 여러 연결 시작 이벤트를 보고할 수 있습니다.

주의 서비스 거부(DoS) 공격 중 차단된 TCP 연결을 로깅하는 것은 수 있고, 다수의 유사한 이벤트로 시스템을 마비시킬 수 있습니다. Block(차단) 규칙에 대한 로깅을 활성화하기 전에, 해당 규칙이 인터넷에 연결된 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스의 트래픽을 모니터링하고 있는지 여부를 고려하시기 바랍니다.

허용된 연결에 대한 로깅 이해

라이센스: 기능에 따라 다름

액세스 제어 규칙 허용 일치 트래픽을 통해 다음 단계 검사 및 트래픽 처리로 넘어갈 수 있습니다.

사용자가 액세스 제어 규칙을 통해 트래픽을 허용할 때, 연결된 침입 또는 파일 정책을 (또는 둘 다를) 사용하여 트래픽이 최종 목적지에 도달하기 전에 트래픽 및 침입 차단, 금지된 파일과 악성코드를 자세히 검사할 수 있습니다.

액세스 제어 규칙 허용과 일치하는 트래픽에 대한 연결은 다음과 같이 로깅됩니다.

- 액세스 제어 규칙이 호출한 침입 정책이 침입을 탐지하고 침입 이벤트를 생성하면, 시스템은 규칙의 로깅 구성에 상관 없이ASA FirePOWER 모듈에 침입이 발생한 연결의 종료를 자동으로 로깅합니다.
- 액세스 제어 규칙에 의해 호출된 파일 정책이 금지된 파일(악성코드 포함)을 탐지하고 파일 또는 악성코드 이벤트를 생성하면, 액세스 제어 규칙의 로깅 구성에 상관 없이ASA FirePOWER 모듈에 대한 파일이 탐지된 연결의 종료를 시스템에서 자동으로 로깅합니다.
- 선택적으로, 시스템이 안전하다고 파악한 트래픽 또는 사용자가 침입 또는 파일 정책을 탐지하지 않은 트래픽을 포함하여 허용된 모든 트래픽에 대한 연결의 시작 및 종료 로깅을 활성화할 수 있습니다.

이러한 결과로 초래된 연결 이벤트 모두에 대해 Action and Reason(실행 및 원인) 필드는 이벤트가 로깅된 이유를 반영합니다. 다음을 참고하십시오.

- Allow(허용) 작업은 배타적으로 허용되고 사용자에 의해 우회된, 그리고 최종 목적지에 도달한 인터랙티브 차단 연결을 나타냅니다.
- Block(차단) 작업은 처음에는 액세스 제어 규칙에서 허용되었지만 침입, 차단 파일 또는 악성코드가 탐지된 연결을 나타냅니다.

허용된 연결에 대한 파일 및 악성코드 이벤트 로깅 비활성화

라이센스: 보호 또는 악성코드

사용자가 액세스 제어 규칙으로 트래픽을 허용할 때, 관련 파일 정책을 사용하여 트래픽이 목적지에 도달하기 전에 전송된 파일을 검사하고 금지된 파일과 악성코드를 차단할 수 있습니다(10-6페이지의 침입 방지 성능 조정 참조).

시스템이 금지된 파일을 탐지하면,ASA FirePOWER 모듈에 대한 다음과 같은 유형의 이벤트 중 하나를 자동으로 로깅합니다.

- *파일 이벤트*, 악성코드 파일을 포함하여 탐지되거나 차단된 파일을 나타냄
- *악성코드 이벤트*, 탐지되거나 차단된 악성코드 파일만 한정적으로 냄
- *소급 적용되는 악성코드 이벤트*, 이전에 탐지된 파일에 대한 악성코드 처리가 변경되는 경우 생성됨

파일 또는 악성코드 이벤트를 로깅하지 않으려면, 액세스 제어 규칙 편집기의 로깅 탭에서 **로그 파일** 확인 상자의 선택을 취소하면 액세스 제어 규칙에 따라 이 로깅을 비활성화할 수 있습니다.

참고 Cisco는 파일과 악성코드 이벤트 로깅 활성화를 유지하는 것을 권장합니다.

사용자가 파일 및 악성코드 이벤트를 저장하는 것에 관계 없이 네트워크 트래픽이 파일 정책을 위반하는 경우, 시스템은 액세스 제어 규칙 호출의 로깅 구성에 상관 없이 ASA FirePOWER 모듈에 대한 결합된 연결의 종료를 자동으로 로깅합니다(25-3페이지의 파일 및 악성 프로그램 이벤트와 결합된 연결(자동) 참조).

연결 로깅을 위한 라이센스 및 요건

라이센스: 기능에 따라 다름

사용자가 액세스 제어 정책 내 연결 로깅을 구성하기 때문에, 해당 정책이 성공적으로 처리할 수 있는 모든 연결을 로깅할 수 있습니다.

사용자는 액세스 제어 정책을 ASA FirePOWER 모듈의 라이센스에 상관 없이 생성할 수 있지만, 액세스 제어의 특정 부분은 사용자가 정책을 적용하기 전 사용이 허가된 특정 기능을 활성화하도록 요청합니다.

다음 표는 액세스 제어를 성공적으로 구성하여 액세스 제어 정책에 의해 처리되는 연결을 로깅하기 위해 사용자가 반드시 보유해야 하는 라이센스에 대해 설명합니다.

표 25-2 액세스 제어 정책 내 연결 로깅을 위한 라이센스 요건

다음에 대한 연결을 로깅하려면...	라이센스
네트워크 포트 또는 문자 URL 기준을 사용하여 처리되는 트래픽	모두
위치 정보 데이터를 사용하여 처리되는 트래픽	모두
연결 대상: • 안전하지 못한 IP 주소(보안 인텔리전스 필터링) • 침입 또는 금지 파일	보호
악성코드와 결합된 연결	악성코드

표 25-2 액세스 제어 정책 내 연결 로깅을 위한 라이센스 요건 (계속)

다음에 대한 연결을 로깅하려면...	라이센스
사용자 정의 컨트롤 또는 애플리케이션 제어에 의해 처리된 트래픽에 대한 연결	제어
시스템이 URL 카테고리 및 평판 데이터를 사용하여 필터링하는 트래픽에 대해, 그리고 모니터링된 호스트가 요청한 URL을 위해 URL 카테고리 및 URL 평판 정보를 표시하기 위한 연결	URL 필터링

보안 인텔리전스(차단 목록 추가) 결정 로깅

라이센스: 보호

ASA FirePOWER 모듈은 악성 인터넷 콘텐츠에 대한 1차 방어선으로서, 사용자가 최신 평판 정보에 근거하여 연결을 즉시 차단 목록에 추가(차단)할 수 있도록 하는 보안 인텔리전스 기능을 포함하며, 동시에 더욱 리소스 집약적이고 심도 깊은 분석을 수행해야 한다는 부담을 덜어줍니다. 이 트래픽 필터링은 빠른 경로처럼 하드웨어 수준의 처리 후에 발생하지만 여타의 정책 기반 검사, 분석 또는 트래픽 처리 **전에** 이루어집니다.

또는, 수동 배포에서 권장되는 대로, 보안 인텔리전스 필터링을 위한 모니터링 전용 설정을 사용할 수 있습니다. 이를 통해 시스템은 차단 목록에 추가되었을 수도 있지만 여전히 차단 목록에 일치하여 로깅하는 연결을 추가로 분석할 수 있습니다.

보안 인텔리전스 로깅을 활성화하면 액세스 제어 정책에 의해 처리된 모든 차단된 연결 및 모니터링된 연결이됩니다. 그러나, 시스템은 허용 목록에 일치하는 연결은 로깅하지 않습니다. 허용 목록으로 분류된 연결의 로깅은 최종 처리에 따라 다릅니다.

보안 인텔리전스 필터링의 결과로 시스템이 연결 이벤트를 로깅할 때 시스템은 또한 일치하는 보안 인텔리전스 이벤트도 로깅합니다. 이는 사용자가 별도로 살펴보고 분석할 수 있는 특수한 연결 이벤트입니다. 두 가지 유형의 이벤트 모두 차단 목록과 일치하는 바를 반영하기 위해 **Action(실행)** 및 **Reason(원인)** 필드를 사용합니다. 또한 사용자가 연결 내 차단 목록에 추가된 IP 주소를 확인할 수 있도록 차단 목록에 추가되어 모니터링되는 IP 주소 옆의 호스트 아이콘은 이벤트 뷰어에서 약간 다르게 보입니다.

차단 목록에 추가되어 차단된 연결 로깅

시스템은 차단된 연결에 대해 연결 시작 보안 인텔리전스 및 연결 이벤트를 로깅합니다. 차단 목록에 추가된 트래픽은 추가 검사 없이 즉시 거부당하기 때문에, 연결을 로깅하는 데 고유한 마무리 단계는 없습니다. 이러한 이벤트에 대한 작업은 `Block(차단)`이며, 그 이유는 `IP Block(IP 차단)`입니다.

`IP Block(IP 차단)` 연결 이벤트는 고유 초기자-응답자 쌍 당 15초의 임계값이 있습니다. 즉 시스템이 연결을 차단하여 이벤트를 생성하는 즉시, 포트 또는 프로토콜에 관계없이 다음 15초 동안 추가 호스트 둘 사이의 연결이 추가로 차단되고, 이 추가 차단된 연결에 대한 다른 연결 이벤트는 생성되지 않습니다.

모니터링되어 차단 목록에 추가된 연결 로깅

보안 인텔리전스가 차단하지는 않고 모니터링하는 연결에 대해, 시스템은 보안 인텔리전스 연결 종료와ASA FirePOWER 모듈에 대한 연결 이벤트를 로깅합니다. 이러한 로깅은 나중에 연결이 과 액세스 제어 규칙 또는 액세스 제어 기본 작업에 의해 처리되는 방식에 상관 없이 발생합니다.

이러한 연결 이벤트에 대한 작업은 연결의 최종 처리에 따라 다릅니다. **Reason(원인)** 필드는 `IP Monitor(IP 모니터링)` 및 연결이 로깅되었을 수 있는 다른 이유를 포함합니다.

시스템은 또한 추후 연결을 처리할 액세스 제어 규칙 또는 기본 작업의 로깅 설정에 따라 모니터링된 연결을 위해 연결 시작 이벤트를 생성할 수 있습니다.

차단 목록에 추가된 연결을 로깅하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 구성하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 Security Intelligence(보안 인텔리전스) 탭을 선택합니다.

액세스 제어 정책에 대한 보안 인텔리전스 설정이 나타납니다.

단계 4 로깅 아이콘( )을 클릭합니다.

Blacklist Options(차단 목록 옵션) 팝업 창이 열립니다.

단계 5 **Log Connections(로그 연결)** 확인 상자를 선택합니다.

단계 6 연결 및 보안 인텔리전스 이벤트를 전송할 위치를 지정합니다. 다음 옵션을 이용할 수 있습니다.

- ASA FirePOWER 모듈로 이벤트를 전송하려면 **Event Viewer(이벤트 뷰어)**를 선택합니다.
- 외부 syslog 서버로 이벤트를 전송하려면, **Syslog**를 선택한 다음, 드롭다운 목록에서 syslog 경고 응답을 선택합니다. 또는 추가 아이콘( )을 클릭하여 syslog 경고 응답을 추가할 수 있습니다(27-3페이지의 Syslog 알림 응답 생성 참조).
- SNMP 트랩 서버로 연결 이벤트를 전송하려면 **SNMP Trap(SNMP 트랩)**을 선택한 다음, 드롭다운 목록에서 SNMP 경고 응답을 선택합니다. 또는 추가 아이콘( )을 클릭하여 SNMP 경고 응답을 추가할 수 있습니다(27-2페이지의 SNMP 경고 응답 생성 참조).

다음의 경우 **반드시 Event Viewer(이벤트 뷰어)**로 이벤트를 전송해야 합니다. 차단 목록에 추가한 개체를 모니터링 전용으로 설정하거나 보안 인텔리전스 필터링이 생성한 연결 이벤트에서 다른 모든 ASA FirePOWER 모듈 기반의 분석을 수행하려는 경우. 자세한 내용은 25-4페이지의 ASA FirePOWER 모듈 또는 외부 서버에 대한 연결 로깅을 참고하십시오.

단계 7 **OK(확인)**를 클릭하여 로깅 옵션을 설정합니다.

보안 인텔리전스 탭이 다시 표시됩니다.

단계 8 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 저장)**를 클릭합니다.

변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참조).

액세스 제어 처리에 기반한 연결 로깅

라이센스: 모두

액세스 제어 정책 내, 액세스 제어 규칙은 네트워크 트래픽을 처리하는 세분화된 방법을 제공합니다. 중요한 연결만 로깅할 수 있도록 하려면, 액세스 제어 규칙 기반의 연결 로깅을 활성화합니다. 사용자가 규칙에 대한 연결 로깅을 활성화하면 시스템은 해당 규칙이 처리하는 모든 연결을 로깅합니다.

사용자는 또한 액세스 제어 정책의 기본 작업에 의해 처리된 트래픽에 대한 연결도 로깅할 수 있습니다. 기본 작업은 시스템이 정책 내 액세스 제어 규칙 중 어느 것과도 일치하지 않는 트래픽을 어떻게 처리할 것인지 결정합니다(일치 및 로깅되지만 트래픽을 검사하거나 처리하지 않는 모니터링 규칙은 예외).

사용자가 모든 액세스 제어 규칙 및 기본 작업에 대한 로깅을 비활성화하는 경우에도 연결 종료 이벤트가 여전히 ASA FirePOWER 모듈에 로깅될 수 있음을 참고하십시오. 이는 연결이 액세스 제어 규칙에 일치하며 침입 시도, 금지 파일 또는 악성코드를 포함하거나

사용자가 구성하는 관련 탐지 옵션 및 기본값 정책 작업 또는 규칙에 따라 사용자의 로깅 옵션은 달라집니다. 자세한 내용은 다음을 참고하십시오.

- 25-10페이지의 액세스 제어 규칙과 일치하는 연결 로깅
- 25-11페이지의 액세스 제어 정책 기본 작업이 처리하는 연결 로깅

액세스 제어 규칙과 일치하는 연결 로깅

라이센스: 모두

중요한 연결만 로깅하려는 사용자는 액세스 제어 규칙 기반의 연결 로깅을 활성화합니다. 규칙에 대한 로깅을 활성화한 경우, 시스템은 해당 규칙에 따라 처리된 모든 연결을 로깅합니다.

규칙 작업 및 규칙에 대한 침입 및 파일 검사 구성에 따라, 사용자의 로깅 옵션이 달라집니다. 25-4페이지의 액세스 제어 규칙 작업이 로깅에 영향을 미치는 방식에 대한 이해를 참고하십시오. 또한 사용자가 액세스 제어 규칙에 대한 로깅을 비활성화하는 경우에도 연결이 다음과 같은 경우 해당 규칙과 일치하는 연결의 연결 종료 이벤트는 여전히 ASA FirePOWER 모듈에 로깅될 수 있음을 참고하십시오.

- 침입 시도, 금지 파일 또는 악성코드가 연결에 포함된 경우
- 이전에 하나 이상의 액세스 제어 모니터링 규칙에 연결이 일치한 경우

연결, 파일 및 악성코드 정보를 로깅할 액세스 제어 규칙을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘(✎)을 클릭합니다.

액세스 제어 정책 편집기가 규칙 탭에 집중되어 나타납니다.

단계 3 로깅 구성을 원하는 규칙 옆에 있는 수정 아이콘(✎)을 클릭합니다.

액세스 제어 규칙 편집기가 나타납니다.

단계 4 Logging(로깅) 탭을 선택합니다.

Logging(로깅) 탭이 나타납니다.

단계 5 **Log at Beginning and End of Connection(연결 시작 및 종료 시 로깅)**, **Log at End of Connection(연결 종료 시 로깅)**을 원하는지, 아니면 **No Logging at Connection(연결 시 로깅하지 않음)**을 원하는지 지정합니다.

단일 비차단 연결의 경우, 연결 종료 이벤트에는 연결 시작 이벤트의 모든 정보가 포함되며, 세션 기간 동안 수집된 정보 또한 포함됩니다. 차단된 트래픽은 추가 검사 없이 즉시 거부당하기 때문에, 시스템 로그 Block(차단) 규칙을 위한 연결 시작 이벤트만 로깅할 수 있습니다. 이러한 이유로, 사용자가 **Block(차단)** 또는 **Block with reset(차단 후 초기화)**하는 규칙 작업을 설정할 때 **Log at Beginning of Connection(연결 시작 시 로깅)**이라는 메시지가 표시됩니다.에 대한 연결 종료 로깅인, 일치하는 트래픽을 로깅하는 것이기 때문임을 참고하십시오.

단계 6 **Log Files(로그 파일)** 확인 상자를 사용하여 시스템이 연결과 결합된 모든 파일 및 악성코드 이벤트를 로깅해야 할지 여부를 지정하십시오.

시스템은 사용자가 파일 정책을 파일 제어 또는 AMP를 수행하는 규칙과 연결할 때 이 옵션을 자동으로 사용합니다. Cisco는 이 옵션을 활성화해 둘 것을 권장합니다. 25-7페이지의 허용된 연결에 대한 파일 및 악성코드 이벤트 로깅 비활성화를 참고하십시오.

단계 7 연결 이벤트를 전송할 위치를 지정합니다. 다음 옵션을 이용할 수 있습니다.

- ASA FirePOWER 모듈로 이벤트를 전송하려면, **Event Viewer(이벤트 뷰어)**를 선택합니다. 모니터링 규칙에 대해 이 옵션을 비활성화할 수 없습니다.
- 외부 syslog 서버로 이벤트를 전송하려면, **Syslog**를 선택한 다음, 드롭다운 목록에서 syslog 경고 응답을 선택합니다. 또는 추가 아이콘( )을 클릭하여 syslog 경고 응답을 추가할 수 있습니다. 27-3페이지의 Syslog 알림 응답 생성을 참고하십시오.
- SNMP 트랩 서버로 이벤트를 전송하려면, **SNMP Trap(SNMP 트랩)**을 선택한 다음, 드롭다운 목록에서 SNMP 경고 응답을 선택합니다. 또는 추가 아이콘( )을 클릭하여 SNMP 경고 응답을 추가할 수 있습니다. 27-2페이지의 SNMP 경고 응답 생성을 참고하십시오.

다음의 경우 **반드시** 이벤트 뷰어로 이벤트를 전송해야 합니다. 연결 이벤트에서 ASA FirePOWER 모듈 기반의 분석을 수행하려는 경우. 자세한 내용은 25-4페이지의 ASA FirePOWER 모듈 또는 외부 서버에 대한 연결 로깅을 참고하십시오.

단계 8 규칙을 저장하려면 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 저장)**를 클릭합니다.

사용자의 규칙이 저장됩니다. 변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다. 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

액세스 제어 정책 기본 작업이 처리하는 연결 로깅

라이센스: 모두

사용자는 액세스 제어 정책의 기본 작업에 의해 처리된 트래픽에 대한 연결을 로깅할 수 있습니다. 기본 작업은 시스템이 정책 내 액세스 제어 규칙 중 어느 것과도 일치하지 않는 트래픽을 어떻게 처리할 것인지 결정합니다(일치 및 로깅되지만 트래픽을 검사하거나 처리하지 않는 모니터링 규칙은 예외). 4-4페이지의 네트워크 트래픽에 대한 기본 처리와 검사 설정을 참고하십시오.

정책 기본 작업에 의해 처리된 로깅 연결을 위한 메커니즘 및 옵션은 다음 표에 설명된 대로 개별 액세스 제어 규칙에 따라 처리된 로깅 연결을 위한 옵션에 대체로 필적합니다. 즉 차단된 트래픽을 제외하고, 시스템 로그 연결의 시작과 끝을 로깅할 수 있으며,ASA FirePOWER 모듈 또는 외부 syslog나 SNMP 트랩 서버에 연결 이벤트를 전송할 수 있습니다.

표 25-3 액세스 제어 기본 작업 로깅 옵션

기본 작업	비교	참고 사항
액세스 제어: 모든 트래픽 차단	차단 규칙	25-5페이지의 차단된 연결 및 인터랙티브 차단된 연결 로깅에 대한 이해
액세스 제어: 모든 트래픽 신뢰	신뢰 규칙	25-5페이지의 신뢰할 수 있는 연결에 대한 로깅 이해
침입 방지	관련 침입 정책과 함께 규칙 허용	25-6페이지의 허용된 연결에 대한 로깅 이해

그러나, 액세스 제어 규칙으로 처리한 로깅 연결과 기본 작업으로 처리한 로깅 연결 간에는 몇 가지 차이점이 있습니다.

- 기본 작업은 파일 로깅 옵션이 없습니다. 사용자는 기본 작업을 사용하여 파일 제어 또는 AMP를 수행할 수 없습니다.
- 액세스 제어 기본 작업과 관련된 침입 정책이 침입 이벤트를 생성할 때 시스템은 결합된 연결의 종료를 자동으로 로깅하지 **않습니다**. 이는 사용자가 연결 데이터를 로깅하는 것을 원하지 않을 때 침입 탐지와 방지 전용 배포에 유용합니다.

  이 규칙의 예외는 사용자가 기본 작업에 대한 연결 시작 및 종료 로깅을 활성화한 경우에 발생합니다. 이 경우, 시스템은 연결의 시작을 로깅하는 것 이외에도 관련 침입 정책이 작동을 이끌어낼 때 연결 종료를 **분명히** 로깅합니다.

사용자가 기본 작업에 대한 로깅을 비활성화한 경우에도 해당 규칙과 일치하는 연결의 연결 종료 이벤트는 여전히 ASA FirePOWER 모듈에 로깅될 수 있음을 참고하십시오. 이는 연결이 이전에 하나 이상의 액세스 제어 모니터링 규칙에 일치한 적이 있거나.

액세스 제어 기본 작업이 처리한 트래픽 내에서 연결을 로깅하려면

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 수정하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 규칙 탭에 집중되어 나타납니다.

단계 3 Default Action(기본 작업) 드롭다운 목록 옆에 있는 로깅 아이콘( )을 클릭합니다.

로깅 팝업 창이 열립니다.

단계 4 **Log at Beginning and End of Connection(연결 시작 및 종료 시 로깅)**, **Log at End of Connection(연결 종료 시 로깅)**을 원하는지, 아니면 **No Logging at Connection(연결 시 로깅하지 않음)**을 원하는지 지정합니다.

단일 비차단 연결의 경우, 연결 종료 이벤트에는 연결 시작 이벤트의 모든 정보가 포함되며, 세션 기간 동안 수집된 정보 또한 포함됩니다. 차단된 트래픽은 추가 검사 없이 즉시 거부당하기 때문에, 시스템에서 모든 트래픽 차단 기본 작업에 대한 연결 시작 이벤트만 로깅합니다. 이러한 이유로, 사용자가 **Access Control: Block All Traffic(액세스 제어: 모든 트래픽 차단)**에 대한 기본 작업을 설정할 때 **Log at Beginning of Connection(연결 시작 시 로깅)**이라는 메시지가 표시됩니다.

단계 5 연결 이벤트를 전송할 위치를 지정합니다. 다음 옵션을 이용할 수 있습니다.

- ASA FirePOWER 모듈로 이벤트를 전송하려면, **Event Viewer(이벤트 뷰어)**를 선택합니다. 모니터링 규칙에 대해 이 옵션을 비활성화할 수 없습니다.
- 외부 syslog 서버로 이벤트를 전송하려면, **Syslog**를 선택한 다음, 드롭다운 목록에서 syslog 경고 응답을 선택합니다. 또는 추가 아이콘( )을 클릭하여 syslog 경고 응답을 추가할 수 있습니다. 27-3페이지의 Syslog 알림 응답 생성을 참고하십시오.
- SNMP 트랩 서버로 이벤트를 전송하려면, **SNMP Trap(SNMP 트랩)**을 선택한 다음, 드롭다운 목록에서 SNMP 경고 응답을 선택합니다. 또는 추가 아이콘( )을 클릭하여 SNMP 경고 응답을 추가할 수 있습니다. 27-2페이지의 SNMP 경고 응답 생성을 참고하십시오.

다음의 경우 **반드시** 이벤트 뷰어로 이벤트를 전송해야 합니다. 연결 이벤트에서 ASA FirePOWER 모듈 기반의 분석을 수행하려는 경우. 자세한 내용은 25-4페이지의 ASA FirePOWER 모듈 또는 외부 서버에 대한 연결 로깅을 참고하십시오.

단계 6 정책을 저장하려면 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 저장)**를 클릭합니다.

사용자의 정책이 저장됩니다. 변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다. 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

연결에서 탐지된 URL 로깅

라이센스: 모두

사용자가 HTTP 트래픽에 대한 ASA FirePOWER 모듈의 연결 종료 이벤트를 로깅할 때 시스템은 세션 중 모니터링된 호스트가 요청한 URL을 기록합니다.

기본적으로, 시스템은 연결 로그 안에서 URL의 처음 1024개 문자를 저장합니다. 그러나, 사용자는 모니터링된 호스트가 요청한 전체 URL을 확실히 캡처하기 위해 URL 당 최대 4096개의 문자를 저장하는 시스템을 구성할 수 있습니다. 또는, 사용자가 방문한 개별 URL에 관심이 없는 경우, 문자가 없는 것으로 저장하여 URL 스토리지를 완전히 비활성화할 수 있습니다. 사용자의 네트워크 트래픽에 따라, 저장된 URL 문자 수를 비활성화하거나 제한하면 시스템 성능을 높일 수 있습니다.

URL 로깅을 비활성화하는 것은 URL 필터링에 영향을 주지 않습니다. 해당 규칙에 의해 처리된 트래픽 내 요청된 개별 URL을 시스템이 로깅하지 않더라도 액세스 제어 규칙은 요청된 URL 및 해당 카테고리와 평판에 기반하여 트래픽을 적절히 필터링합니다. 자세한 내용은 8-7페이지의 URL 차단을 참고하십시오.

사용자가 저장한 URL 문자 수를 사용자 정의하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Access Control Policy(액세스 제어 정책)**를 선택합니다.

Access Control Policy(액세스 제어 정책) 페이지가 나타납니다.

단계 2 구성하려는 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

단계 3 Advanced(고급) 탭을 선택합니다.

액세스 제어 정책에 대한 고급 설정이 나타납니다.

단계 4 General Settings(일반 설정) 옆에 있는 수정 아이콘( )을 클릭합니다.

General Settings(일반 설정) 팝업 창이 열립니다.

단계 5 **연결 이벤트에 저장하고자 하는 최대 URL 문자**를 입력합니다.

0에서 4096까지의 수를 지정할 수 있습니다. 문자가 없는 것으로 저장하면 URL 필터링을 비활성화하지 않은 상태로 URL 스토리지가 비활성화됩니다.

단계 6 **OK(확인)**를 클릭합니다.

액세스 제어 정책에 대한 고급 설정이 나타납니다.

단계 7 정책을 저장하려면 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 저장)**를 클릭합니다.

사용자의 정책이 저장됩니다. 변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다. 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

이벤트 보기

ASA FirePOWER 모듈에 의해 검사된 트래픽에 대해 로깅된 실시간 이벤트를 볼 수 있습니다.

참고 모듈은 메모리에 가장 최근의 이벤트 100개만 캐시합니다.

자세한 내용은 다음 섹션을 참고하십시오.

ASA FirePOWER 실시간 이벤트 액세스

미리 정의된 여러 이벤트 보기에서 ASA FirePOWER 모듈이 탐지한 이벤트를 보거나 사용자 정의 이벤트 보기를 생성하여 선택한 이벤트 필드를 볼 수 있습니다.

참고 모듈은 메모리에 가장 최근의 이벤트 100개만 캐시합니다.

ASA FirePOWER 이벤트를 보려면 다음을 수행합니다.

단계 1 **Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Real-time Eventing(실시간 이벤트 처리)**을 선택합니다.

단계 2 다음 2가지 옵션을 사용할 수 있습니다.

- 연결 이벤트, 보안 인텔리전스 이벤트, 침입 이벤트, 파일, 이벤트 또는 악성코드 이벤트 중에서 확인하려는 이벤트 유형의 기존 탭을 클릭합니다.
- + 아이콘을 클릭하여 사용자 정의 이벤트 보기를 생성하고 보기에 포함하려는 이벤트 필드를 선택합니다.

자세한 내용은 26-2페이지의 ASA FirePOWER 이벤트 유형 이해 및 26-3페이지의 ASA FirePOWER 이벤트의 이벤트 필드를 참고하십시오.

ASA FirePOWER 이벤트 유형 이해

ASA FirePOWER 모듈은 연결 이벤트, 보안 인텔리전스 이벤트, 침입 이벤트, 파일 이벤트 및 악성 코드 이벤트의 5개 이벤트 유형에서 이벤트 필드의 실시간 이벤트 보기를 제공합니다. .

연결 이벤트

*연결 이벤트*라고 불리는 연결 로그에는 탐지된 세션에 대한 데이터가 포함됩니다. 모든 개별 연결 이벤트에 대한 정보는 몇 가지 요소에 따라 가용성이 결정되지만, 일반적으로는 다음과 같습니다.

- 기본 연결 속성: 타임 스탬프, 소스 및 대상 IP 주소, 인그레스 및 이그레스 영역, 연결을 처리한 디바이스 등
- 시스템에서 검색하거나 유추한 추가 연결 속성: 애플리케이션, 요청된 URL 또는 연결과 관련된 사용자 등
- 연결이 로깅된 이유에 대한 메타데이터: 어떤 정책의 어떤 액세스 제어 규칙(또는 다른 구성)이 트래픽을 처리했는지, 연결이 허용 또는 차단되었는지 여부 등

액세스 제어의 다양한 설정은 로깅할 연결의 종류, 로깅할 시기 및 데이터 저장 위치를 세부적으로 제어할 수 있도록 합니다. 액세스 제어 정책이 성공적으로 처리할 수 있는 모든 연결을 로깅할 수 있습니다. 다음 상황에서 연결 로깅을 활성화할 수 있습니다.

- 연결이 신뢰도 기반의 Security Intelligence(보안 인텔리전스) 기능에 의해 차단 목록에 추가(차단)되거나 모니터링되는 경우
- 액세스 제어 규칙 또는 액세스 제어 기본 작업에 의해 연결이 처리된 경우

시스템은 사용자가 구성하는 로깅 외에도 시스템이 금지된 파일, 악성코드, 또는 침입 시도를 탐지한 곳에서 대부분의 연결을 자동으로 로깅합니다.

보안 인텔리전스 이벤트

Security Intelligence(보안 인텔리전스) 로깅을 활성화하면 차단 목록 일치는 자동적으로 *Security Intelligence(보안 인텔리전스) 이벤트* 및 연결 이벤트를 생성합니다. Security Intelligence(보안 인텔리전스) 이벤트는 사용자가 별도로 확인하고 분석할 수 있는 연결 이벤트의 특수 유형입니다. Security Intelligence(보안 인텔리전스) 차단 목록 추가 결정을 포함하여 연결 로깅 구성에 대한 자세한 내용은 25-1페이지의 네트워크 트래픽의 연결 로깅을 참고하십시오.


팁

연결 이벤트에 대한 일반 정보는 별도로 지정하지 않는 한 Security Intelligence(보안 인텔리전스) 이벤트와도 관련이 있습니다. Security Intelligence(보안 인텔리전스)에 대한 자세한 내용은 5-1페이지의 보안 인텔리전스 IP 주소 평판을 사용한 차단 목록 추가를 참고하십시오.

침입 이벤트

시스템은 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성에 영향을 미칠 수 있는 악성 활동 탐지를 위해 네트워크를 통과하는 패킷을 검토합니다. 시스템이 침입 가능성을 식별하는 경우, 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 컨텍스트 정보의 레코드인 *침입 이벤트*를 생성합니다.

파일 이벤트

*파일 이벤트*는 시스템이 네트워크 트래픽에서 탐지하고 선택적으로 차단한 파일을 나타냅니다.

현재 적용된 파일 정책의 규칙에 따라, 시스템은 매니지드 디바이스가 네트워크 트래픽에서 파일을 탐지하거나 차단할 때 생성되는 파일 이벤트를 로깅합니다.

악성코드 이벤트

*악성코드 이벤트*는 시스템이 네트워크 트래픽에서 탐지하고 선택적으로 차단한 악성코드 파일을 나타냅니다.

악성코드 라이센스가 있으면 ASA FirePOWER 모듈은 악성코드를 네트워크 트래픽에서 전체 액세스 제어 구성의 일부로 탐지할 수 있습니다(24-4페이지의 파일 정책 이해 및 생성 참고).

다음 시나리오는 악성코드 이벤트 생성으로 이어질 수 있습니다.

- 매니지드 디바이스가 특정 파일 유형의 집합 중 하나를 탐지하는 경우, ASA FirePOWER 모듈은 악성코드 클라우드 조회를 수행하는데, 이는 ASA FirePOWER 모듈에 `Malware`, `Clean` 또는 `Unknown`이라는 파일 속성을 반환합니다.
- ASA FirePOWER 모듈이 클라우드와 연결할 수 없거나, 다른 방법으로는 클라우드를 사용할 수 없는 경우 파일 속성은 `Unavailable`이 됩니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.
- 매니지드 디바이스가 정상 목록에서 파일을 탐지하는 경우, ASA FirePOWER 모듈은 해당 파일에 `Clean`이라는 파일 속성을 할당합니다.

다른 컨텍스트 데이터와 함께, ASA FirePOWER 모듈은 파일 탐지 및 속성의 레코드를 악성코드 이벤트로 로깅합니다.

네트워크 트래픽에서 탐지되고 ASA FirePOWER 모듈에 의해 악성코드로 식별된 파일은 파일 이벤트 및 악성코드 이벤트를 모두 생성합니다. 이는 시스템이 파일에서 악성코드를 탐지하려면 파일 자체를 먼저 탐지해야 하기 때문입니다.

ASA FirePOWER 이벤트의 이벤트 필드

작업

연결 또는 보안 인텔리전스 이벤트에 대해 연결을 로깅한 액세스 제어 규칙 또는 기본 작업과 관련된 작업.

- `Allow(허용)`는 명시적으로 허용되고 사용자가 우회한 쌍방향으로 차단된 연결을 나타냅니다.
- `Trust(신뢰)`는 신뢰된 연결을 나타냅니다. 첫 번째 패킷의 신뢰 규칙에 의해 탐지된 TCP 연결은 연결 종료 이벤트만 생성합니다. 시스템에서는 최종 세션 패킷이 끝난 지 한 시간 후에 이벤트를 생성합니다.
- `Block(차단)` 및 `Block with reset(차단 후 초기화)`는 차단된 연결을 나타냅니다. 시스템은 또한 `Block(차단)` 작업을 Security Intelligence(보안 인텔리전스)가 차단한 연결과 침입 정책에서 익스플로잇이 탐지된 연결, 그리고 파일이 파일 정책에 따라 차단된 연결과 결합합니다.
- `Interactive Block(인터랙티브 차단)` 및 `Interactive Block with reset(인터랙티브 차단 후 초기화)`는 시스템이 Interactive Block rule(인터랙티브 차단) 규칙을 사용하여 사용자의 HTTP 요청을 처음에 차단할 때 로깅할 수 있는 연결 시작 이벤트를 표시합니다. 사용자가 시스템에 표시된 경고 페이지를 클릭할 경우, 세션에 대해 로깅하는 모든 추가 연결 이벤트에는 `Allow(허용)` 작업이 포함됩니다.
- `Default Action(기본 작업)`은 연결이 기본 작업에 의해 처리되었음을 나타냅니다.
- Security Intelligence(보안 인텔리전스)가 모니터링한 연결의 경우, 작업은 연결이 시작한 최초의 Monitor(모니터링)이 아닌 액세스 제어 규칙의 작업이거나 기본 작업입니다. 이와 마찬가지로, Monitor(모니터링) 규칙과 일치하는 트래픽은 항상 후속 규칙 또는 기본 규칙에 의해 처리되므로 모니터링 규칙에 의해 로깅된 연결과 관련된 작업은 `Monitor(모니터링)`가 될 수 없습니다.

파일 또는 악성코드 이벤트의 경우, 파일과 일치하는 규칙에 대한 규칙 작업과 관련된 파일 규칙 작업 및 관련된 모든 파일 규칙 작업 옵션.

허용된 연결

시스템이 이벤트에 대한 트래픽 흐름을 허용하는지 여부

애플리케이션

연결에서 탐지된 애플리케이션

애플리케이션 비즈니스 관련성

연결에서 탐지된 애플리케이션 트래픽과 연계된 사업 타당성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음), 또는 Very Low(매우 낮음). 연결에서 탐지된 각 애플리케이션 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

애플리케이션 카테고리

애플리케이션 기능을 이해하는 데 도움이 되는 애플리케이션의 특성을 나타내는 카테고리

애플리케이션 위험성

연결에서 탐지된 애플리케이션 트래픽과 관련된 위험성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음), 또는 Very Low(매우 낮음). 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

애플리케이션 태그

애플리케이션 기능을 이해하는 데 도움이 되는 애플리케이션의 특성을 나타내는 태그

차단 유형

이벤트의 트래픽 흐름과 일치하는 액세스 제어 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

클라이언트

연결에서 탐지된 클라이언트 애플리케이션.

시스템이 연결에 사용되는 특정 클라이언트를 식별할 수 없는 경우, 이 필드는 애플리케이션 프로토콜 이름에 첨부된 client(클라이언트)를 표시하여 일반 이름, 예를 들어, FTP client(FTP 클라이언트)를 제공합니다.

클라이언트 비즈니스 관련성

연결에서 탐지된 클라이언트 트래픽과 관련된 사업 타당성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음), 또는 Very Low(매우 낮음). 연결에서 탐지된 각 클라이언트 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

클라이언트 카테고리

클라이언트의 기능을 이해할 수 있도록 트래픽에서 탐지된 클라이언트의 특성을 나타내는 카테고리.

클라이언트 위험성

연결에서 탐지된 클라이언트 트래픽과 관련된 위험성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음), 또는 Very Low(매우 낮음). 연결에서 탐지된 클라이언트의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

클라이언트 태그
클라이언트의 기능을 이해하는 데 도움이 되는 트래픽에서 탐지된 클라이언트의 특성을 나타내는 태그

클라이언트 버전
연결에서 탐지된 클라이언트의 버전

연결
내부에서 생성되는 트래픽 흐름의 고유 ID

연결 차단 유형 표시기
이벤트의 트래픽 흐름과 일치하는 액세스 제어 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

연결 바이트
연결에 대한 총 바이트

연결 시간
연결 시작 시간

연결 타임 스탬프
연결이 탐지된 시간

컨텍스트
트래픽이 전달된 보안 컨텍스트를 식별하는 메타데이터. 시스템이 다중 컨텍스트 모드의 디바이스에 대해 이 필드만 입력한다는 점에 유의하십시오.

거부된 연결
시스템이 이벤트에 대한 트래픽 흐름을 거부하는지 여부

대상 국가 및 대륙
수신 호스트의 국가와 대륙

대상 IP
수신 호스트에서 사용하는 IP 주소

대상 포트, 대상 포트 Icode, 대상 Port/ICMP 코드
세션 응답기가 사용하는 대상 포트 또는 ICMP 코드

방향
파일의 전송 방향

속성
다음 파일 속성 중 하나가 표시됩니다.

- `Malware(악성코드)`는 클라우드가 파일을 악성코드로 분류했음을 나타냅니다.
- `Clean(정상)`은 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다

- Unknown(알 수 없음)은 클라우드가 속성을 할당하기 전에 악성코드 클라우드 조회가 발생했음을 나타냅니다. 파일이 분류되지 않은 상태입니다.
- Custom Detection(사용자 지정 탐지)은 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다.
- Unavailable(사용 불가)은 ASA FirePOWER 모듈이 악성코드 클라우드 조회를 수행하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.
- N/A는 Detect Files(파일 탐지) 또는 Block Files(파일 차단) 규칙이 파일을 처리하였으며 ASA FirePOWER 모듈이 악성코드 클라우드 검색을 수행하지 않았음을 나타냅니다.

이그레스 인터페이스

연결과 관련된 이그레스 인터페이스. 배포에 비동기 라우팅 구성이 포함되어 있는 경우, 인그레스 및 이그레스 인터페이스가 동일한 인터페이스 세트에 포함될 수 있다는 점에 유의하십시오.

이그레스 보안 영역

연결과 관련된 이그레스 보안 영역

이벤트

이벤트 유형

이벤트 마이크로초

이벤트가 탐지된 시간(단위: 마이크로초)

이벤트 사간(단위: 초)

이벤트가 탐지된 시간(단위: 초)

이벤트 유형

이벤트 유형.

파일 카테고리

파일 유형의 일반적인 카테고리. 예: Office 문서, 아카이브, 멀티미디어, 실행 파일, PDF 파일, 인코딩, 그래픽 또는 시스템 파일.

파일 이벤트 타임 스탬프

파일 또는 악성코드 파일이 생성된 시간 및 날짜

파일 이름

파일 또는 악성코드 파일의 이름

파일 SHA256

파일의 SHA-256 해시 값

파일 크기

파일 또는 악성코드 파일의 크기(단위: 킬로바이트)

파일 유형

파일 또는 악성코드 파일의 유형(예: HTML 또는 MSEXE).

파일/악성 프로그램 정책

이벤트 생성과 관련된 파일 정책.

파일 로그 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 파일 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

방화벽 정책 규칙/SI 카테고리

연결의 블랙리스트 IP 주소를 나타내거나 포함하는 블랙리스트 객체의 이름. Security Intelligence(보안 인텔리전스) 카테고리는 네트워크 개체 또는 그룹, 전역 차단 목록, 사용자 지정 Security Intelligence(보안 인텔리전스) 목록이나 피드 또는 Intelligence Feed(인텔리전스 피드) 내 카테고리 중 하나의 이름일 수 있습니다. 이 필드는 **Reason(이유)**가 `IP Block(IP 차단)`이거나 `IP Monitor(IP 모니터링)`인 경우에만 입력되며 Security Intelligence(보안 인텔리전스) 이벤트 보기의 항목에는 항상 이유가 표시된다는 점에 유의하십시오.

방화벽 규칙

연결을 처리한 액세스 제어 규칙 또는 기본 작업이자, 해당 연결과 일치한 최대 8개의 Monitor(모니터링) 규칙.

첫 번째 패킷

세션의 첫 번째 패킷이 표시된 날짜 및 시간

HTTP 참조 페이지

연결(다른 URL에 링크를 제공하는 웹 사이트 또는 다른 URL에서 링크를 가져온 웹 사이트 등)에서 탐지된 HTTP 트래픽에 대해 요청된 URL의 참조 페이지를 나타내는 HTTP 참조 페이지

IDS 분류

이벤트를 생성한 규칙이 속하는 분류. 규칙 분류 이름 및 번호의 목록은 규칙 분류 테이블을 참조하십시오.

영향

이 필드의 영향 수준은 침입 데이터, 네트워크 검색 데이터 및 취약성 정보 사이의 상관 관계를 나타냅니다.

영향 플래그

Impact(영향)을 참고하십시오.

인그레스 인터페이스

연결과 관련된 인그레스 인터페이스. 배포에 비동기 라우팅 구성이 포함되어 있는 경우, 인그레스 및 이그레스 인터페이스가 동일한 인터페이스 세트에 포함될 수 있다는 점에 유의하십시오.

인그레스 보안 영역

연결과 관련된 이그레스 보안 영역

초기자 바이트

세션 초기자에 의해 제공된 총 바이트 수

초기자 국가 및 대륙

라우팅 가능한 IP가 탐지될 때 세션을 시작한 호스트 IP 주소와 관련된 국가 및 대륙

초기자 IP

세션 응답기를 시작한 호스트 IP 주소(DNS 확인이 활성화된 경우, 호스트 이름)

초기자 패킷

세션 초기자에 의해 제공된 총 패킷 수

인라인 결과

다음 중 하나의 결과를 나타냅니다.

- 검은색 아래쪽 화살표. 시스템이 규칙을 트리거한 패킷을 삭제했음을 나타냅니다.
- 회색 아래쪽 화살표. (인라인 배포의) **Drop when Inline(인라인 시 삭제)** 침입 정책 옵션을 활성화하거나 시스템을 잘라내는 동안 Drop and Generate(삭제 및 생성) 규칙이 이벤트를 생성한 경우, IPS가 패킷을 삭제했음을 나타냅니다.
- 공백. 트리거된 규칙이 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되지 않았음을 나타냅니다.
- 인라인 인터페이스가 탭 모드에 있는 경우를 포함하여 침입 정책의 규칙 상태 또는 인라인 삭제 작업에 상관없이 수동 배포에서 시스템이 패킷을 삭제하지 않는다는 점에 유의하십시오.

IPS 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 침입 규칙의 작업

마지막 패킷

세션의 마지막 패킷이 표시된 날짜 및 시간

MPLS 레이블

이 침입 이벤트를 트리거한 패킷에 연결된 Multiprotocol Label Switching(다중 프로토콜 레이블 스위칭) 레이블

악성 프로그램 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 파일 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

메시지

이벤트에 대한 설명 텍스트

규칙 기반 침입 이벤트의 경우, 이벤트 메시지는 규칙에서 발생합니다. 디코더 및 전처리기 기반 이벤트의 경우, 이벤트 메시지는 하드 코드됩니다.

악성코드 이벤트의 경우, 악성코드 이벤트와 관련된 모든 추가 정보입니다. 네트워크 기반 악성코드 이벤트의 경우, 이 필드는 해당 속성이 변경된 파일에만 입력됩니다.

모니터링 규칙

해당 연결에 일치하는 최대 8개의 Monitor(모니터링) 규칙

NetBIOS 도메인

세션에서 사용되는 NetBIOS 도메인

정책

이벤트 생성과 관련된 액세스 제어, 침입 또는 NAP(네트워크 분석 정책)(있는 경우)

정책 수정

이벤트 생성과 관련된 액세스 제어, 파일, 침입 또는 NAP(네트워크 분석 정책)의 수정(있는 경우)

우선순위

Cisco VRT에 따라 결정된 이벤트 우선순위

프로토콜

연결에서 탐지된 프로토콜

이유

다음과 같은 상황에서 연결이 로깅된 이유

- `User Bypass(사용자 우회)`는 시스템이 사용자의 HTTP 요청을 처음에는 차단했지만 사용자가 경고 페이지를 통해 클릭하여 원래 요청한 사이트에 계속 남아 있도록 선택했음을 나타냅니다. `User Bypass(사용자 우회)`의 이유는 항상 `Allow(허용)` 작업과 페어링됩니다.
- `IP Block(IP 차단)`은 시스템이 Security Intelligence(보안 인텔리전스) 데이터를 기반으로 검사 없이 연결을 거부했음을 나타냅니다. `IP Block(IP 차단)`의 이유는 항상 `Block(차단)` 작업과 페어링됩니다.
- `IP Monitor(IP 모니터링)`는 시스템이 Security Intelligence(보안 인텔리전스) 데이터에 따라 연결을 거부할 수도 있었지만 사용자가 시스템을 구성하여 연결을 거부하지 않고 모니터링했음을 나타냅니다.
- `File Monitor(파일 모니터링)`는 시스템이 연결에서 파일의 특정 유형을 탐지했음을 나타냅니다.
- `File Block(파일 차단)`은 시스템이 전송을 차단한 파일 또는 악성코드 파일을 연결에 포함했음을 나타냅니다. `File Block(파일 차단)`의 이유는 항상 `Block(차단)` 작업과 페어링됩니다.
- `File Custom Detection(파일 사용자 지정 탐지)`은 시스템이 전송되지 않도록 한 사용자 정의 탐지 목록에서 파일을 연결에 포함했음을 나타냅니다.
- `File Resume Allow(파일 재시작 허용)`는 원래는 파일 전송이 Block Files(파일 차단) 또는 Block Malware(악성코드 차단) 파일 규칙에 의해 차단되었음을 나타냅니다. 새로운 액세스 제어 정책이 적용되어 파일이 허용되면 HTTP 세션은 자동으로 다시 시작됩니다. 이러한 이유는 인라인 배포에만 표시된다는 점에 유의하십시오.
- `File Resume Block(파일 재시작 차단)`은 원래는 파일 전송이 Detect Files(파일 탐지) 및 Malware Cloud Lookup(악성코드 클라우드 조회) 파일 규칙에 의해 허용되었음을 나타냅니다. 새로운 액세스 제어 정책이 적용되어 파일이 차단되면 HTTP 세션은 자동으로 중단됩니다. 이러한 이유는 인라인 배포에만 표시된다는 점에 유의하십시오.
- `Intrusion Block(침입 차단)`은 시스템이 연결에서 탐지된 익스플로잇(침입 정책 위반)을 차단했거나 차단할 수도 있었음을 나타냅니다. `Intrusion Block(침입 차단)`의 이유는 차단된 익스플로잇의 경우에는 `Block(차단)` 작업과, 차단될 수도 있었던 익스플로잇의 경우에는 `Allow(허용)` 작업과 페어링됩니다.
- `Intrusion Monitor(침입 모니터링)`는 시스템이 연결에서 탐지된 익스플로잇을 탐지했지만 차단하지 않았음을 나타냅니다. 이는 시작된 침입 규칙의 상태가 **Generate Events(이벤트 생성)**로 설정된 경우에 발생합니다.

수신된 시간

대상 호스트 또는 응답기가 이벤트에 응답한 시간

참조된 호스트
연결의 프로토콜이 DNS, HTTP, 또는 HTTPS인 경우, 이 필드는 각 프로토콜이 사용했던 호스트 이름을 나타냅니다.

응답기 바이트
세션 응답기가 제공한 총 바이트 수

응답기 국가 및 대륙
라우팅 가능한 IP가 탐지될 때 세션 응답기를 위한 호스트 IP 주소와 관련된 국가 및 대륙

응답기 패킷
세션 응답기가 제공한 총 패킷 수

응답기 IP
세션 초기자에 응답한 호스트 IP 주소(DNS 확인이 활성화된 경우, 호스트 이름)

서명
이벤트의 트래픽과 일치하는 침입 규칙의 서명 ID

소스 국가 및 대륙
전송 호스트의 국가와 대륙

소스 IP
침입 이벤트에서 전송 호스트가 사용하는 IP 주소

소스 또는 대상
이벤트의 연결을 시작하거나 수신하는 호스트

소스 포트, 소스 포트 유형, 소스 포트/ICMP 유형
세션 초기자가 사용하는 소스 포트 또는 ICMP 유형

TCP 플래그
연결에서 탐지된 TCP 플래그

URL
세션 도중 모니터링된 호스트가 요청한 URL

URL 카테고리
사용 가능한 경우 세션 도중 모니터링된 호스트가 요청한 URL과 관련된 카테고리

URL 신뢰도
사용 가능한 경우 세션 도중 모니터링된 호스트가 요청한 URL과 관련된 신뢰도

URL 신뢰도 점수
사용 가능한 경우 세션 도중 모니터링된 호스트가 요청한 URL과 관련된 신뢰도 점수

사용자
이벤트가 발생한 호스트(**수신 IP**)의 사용자

사용자 에이전트

연결에서 탐지된 HTTP 트래픽에서 추출된 사용자 에이전트 애플리케이션 정보

VLAN

이벤트를 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID

웹 애플리케이션 사업 타당성

연결에서 탐지된 웹 애플리케이션 트래픽과 연계된 비즈니스 관련성: `Very High`, `High`, `Medium`, `Low`, 또는 `Very Low`. 연결에서 탐지된 웹 애플리케이션의 각 유형은 관련된 비즈니스 관련성을 가지며, 이 필드는 가장 낮은(가장 타당성이 적은) 것을 표시합니다.

웹 애플리케이션 카테고리

웹 애플리케이션의 기능을 이해하는 데 도움이 되는 트래픽에서 탐지된 웹 애플리케이션의 특성을 나타내는 카테고리

웹 애플리케이션 위험성

연결에서 탐지된 웹 애플리케이션 트래픽과 관련된 위험성: `Very High(매우 높음)`, `High(높음)`, `Medium(중간)`, `Low(낮음)` 또는 `Very Low(매우 낮음)`. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

웹 애플리케이션 태그

웹 애플리케이션의 기능을 이해하는 데 도움이 되는 트래픽에서 탐지된 웹 애플리케이션의 특성을 나타내는 태그

웹 애플리케이션

트래픽에서 탐지된 웹 애플리케이션

침입 규칙 분류

침입 규칙에는 공격 그룹이 포함됩니다. 다음 표에는 각 분류의 이름과 번호가 나열되어 있습니다.

표 26-1 규칙 분류

번호	분류 이름	설명
1	not-suspicious	의심스럽지 않은 트래픽
2	unknown	알 수 없는 트래픽
3	bad-unknown	잠재적인 악성 트래픽
4	attempted-recon	정보 유출 시도
5	successful-recon-limited	정보 유출
6	successful-recon-largescale	대규모 정보 유출
7	attempted-dos	서비스 거부 시도
8	successful-dos	서비스 거부
9	attempted-user	사용자 권한 획득 시도
10	unsuccessful-user	사용자 권한 획득 실패
11	successful-user	사용자 권한 획득 성공

표 26-1 규칙 분류

번호	분류 이름	설명
12	attempted-admin	관리자 권한 획득 시도
13	successful-admin	관리자 권한 획득 성공
14	rpc-portmap-decode	RPC 쿼리 디코드
15	shellcode-detect	실행 가능한 코드가 탐지됨
16	string-detect	의심스러운 문자열이 탐지됨
17	suspicious-filename-detect	의심스러운 파일 이름이 탐지됨
18	suspicious-login	의심스러운 사용자 이름을 사용한 로그인 시도가 탐지됨
19	system-call-detect	시스템 호출이 탐지됨
20	tcp-connection	TCP 연결이 탐지됨
21	trojan-activity	네트워크 트로이 목마가 탐지됨
22	unusual-client-port-connection	클라이언트가 비정상적인 포트를 사용하고 있음
23	network-scan	네트워크 스캔이 탐지됨
24	denial-of-service	서비스 거부 공격(DoS)이 탐지됨
25	non-standard-protocol	비표준 프로토콜 또는 이벤트가 탐지됨
26	protocol-command-decode	일반적인 프로토콜 명령 디코드
27	web-application-activity	잠재적으로 취약한 웹 애플리케이션에 액세스
28	web-application-attack	웹 애플리케이션 공격
29	misc-activity	기타 활동
30	misc-attack	기타 공격
31	icmp-event	일반 ICMP 이벤트
32	inappropriate-content	부적절한 콘텐츠가 발견됨
33	policy-violation	잠재적인 기업 개인 정보 보호 위반
34	default-login-attempt	기본 사용자 이름 및 비밀번호로 로그인 시도
35	sdf	중요한 데이터
36	malware-cnc	알려진 악성코드 명령 및 제어 트래픽
37	client-side-exploit	알려진 클라이언트 측 익스플로잇 시도
38	file-format	알려진 악성 파일 또는 파일 기반 익스플로잇

27 장

외부 경고 구성

ASA FirePOWER 모듈이 모듈 인터페이스 안에서 다양한 관점의 이벤트를 제공하는 동안 중요한 시스템에 대한 지속적인 모니터링을 지원하기 위해 외부 이벤트 알림을 구성할 수 있습니다. 다음 중 한 가지 상황이 발생했을 때 모듈을 구성하여 이메일, SNMP 트랩 또는 syslog를 통해 사용자에게 알리는 경고를 생성할 수 있습니다.

- 네트워크 기반 악성코드 이벤트 또는 소급 적용되는 악성코드 이벤트
- 특정 액세스 제어 규칙에 의해 시작된 연결 이벤트

ASA FirePOWER 모듈 이 이 경고를 보내도록 하려면 *경고 응답*을 먼저 생성해야 합니다. 이 경고 응답은 사용자가 경고를 보내려고 계획하고 있는 외부 시스템과 모듈이 상호 작용할 수 있는 구성 집합입니다. 해당 구성이 지정할 수 있는 것은, 예를 들어, SNMP 경고 매개 변수, 또는 syslog 기능 및 우선 순위 등입니다.

경고 응답을 만든 다음, 경고를 시작하기 위해 사용하고자 하는 이벤트와 연결합니다. 경고 응답을 연결하는 프로세스는 이벤트의 유형에 따라 달라진다는 점에 유의하십시오.

- 고유의 구성 페이지를 사용하는 악성코드 이벤트와 경고 응답을 연결합니다.
- 액세스 제어 규칙과 정책을 사용하여 로깅된 연결에 SNMP 및 syslog 경고 응답을 연결합니다.

ASA FirePOWER 모듈 안에서 수행할 수 있는 다른 종류의 경고가 있는데, SNMP 및 개별 침입 이벤트를 위한 syslog 침입 이벤트 알림을 구성하는 것입니다. 침입 정책에서 이 알림을 구성합니다 (28-1페이지의 침입 규칙을 위한 외부 경고 구성 및 20-32페이지의 SNMP 알림 추가 참고). 다음 표에서는 경고 생성을 위해 반드시 보유해야 하는 라이센스를 설명합니다.

표 27-1 경고 생성을 위한 라이센스 요건

경고 생성의 근거	필요한 라이센스
침입 이벤트	보호
네트워크 기반 악성코드 이벤트	악성코드
연결 이벤트	연결을 로깅하는 데 필요한 라이센스

자세한 내용은 다음을 참고하십시오.

- 27-2페이지의 경고 응답 작업
- 25-1페이지의 네트워크 트래픽의 연결 로깅

경고 응답 작업

라이센스: 모두

외부 경고 구성의 첫 단계는 경고 응답을 생성하는 것인데, 이는 ASA FirePOWER 모듈 사용자가 경고를 보내려고 계획하고 있는 외부 시스템과 상호 작용할 수 있는 구성 집합입니다. 경고 응답을 만들어서 이메일 및 단순 네트워크 관리 프로토콜(SNMP) 트랩, 또는 시스템 로그(syslog)를 통해 전송 경고를 보낼 수 있습니다.

사용자가 경고에서 가져오는 정보는 경고를 시작한 이벤트 유형에 따라 다릅니다.

이는 사용자가 경고 응답을 만들면 자동으로 활성화됩니다. 활성화된 경고 응답만 알림을 생성할 수 있습니다. 구성을 삭제하는 대신 응답 경고를 한시적으로 비활성화하여 경고가 생성되는 것을 중지할 수 있습니다.

Alerts(경고) 페이지(**ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Actions Alerts(작업 경고)**)에서 경고 응답을 관리합니다. 각 경고 응답 옆에 있는 슬라이더는 경고 응답이 활성화되었는지 여부를 나타냅니다. 활성화된 경고 응답만 알림을 생성할 수 있습니다. 페이지는 또한 경고 응답이 구성에서 사용되고 있는지 여부를 나타냅니다. 예를 들면, 액세스 제어 규칙에서 연결을 로깅하는 것입니다. 적절한 열 머리글을 클릭하여 경고 응답을 이름, 유형, 사용 상태 및 활성화/비활성화 상태에 따라 정렬 할 수 있습니다. 정렬 순서를 바꾸려면 다시 열 머리글을 클릭합니다.

자세한 내용은 다음을 참고하십시오.

- 27-2페이지의 SNMP 경고 응답 생성
- 27-3페이지의 Syslog 알림 응답 생성
- 27-5페이지의 알림 응답 수정
- 27-6페이지의 알림 응답 삭제
- 27-6페이지의 알림 응답 활성화 및 비활성화

SNMP 경고 응답 생성

라이센스: 모두

SNMPv1, SNMPv2 또는 SNMPv3을 사용하여 SNMP 경고 응답을 만들 수 있습니다.

참고 SNMP로 64비트 값을 모니터링하려는 경우, SNMPv2 또는 SNMPv3을 사용해야 합니다. SNMPv1은 64비트 모니터링을 지원하지 않습니다.

SNMP 경고 응답을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Actions Alerts(작업 경고)**를 선택합니다.

Alerts(경고) 페이지가 표시됩니다.

단계 2 **Create Alert(경고 생성)** 드롭다운 메뉴에서 **Create SNMP Alert(SNMP 경고 생성)**를 선택합니다.

Create SNMP Alert Configuration(SNMP 경고 구성 생성) 팝업 창이 표시됩니다.

단계 3 **Name(이름)** 필드에 SNMP를 식별하는 데 사용하려는 이름을 입력합니다.

단계 4 **Trap Server(트랩 서버)** 필드에 영숫자를 사용하여 호스트 이름 또는 SNMP 트랩 서버의 IP 주소를 입력합니다.

이 필드에 유효하지 않은 IPv4 주소(예를 들어 192.169.1.456)를 입력한다고 해도 시스템에서 경고하지 **않는다**는 점에 유의하십시오. 잘못된 주소는 호스트 이름으로 처리됩니다.

단계 5 **Version(버전)** 드롭다운 목록에서 사용하려는 SNMP 버전을 선택합니다.

SNMP v3은 기본값입니다. SNMP v1 또는 SNMP v2를 선택한 경우, 다른 옵션이 나타납니다.

단계 6 어느 버전의 SNMP를 선택하셨습니까?

- SNMP v1 또는 SNMP v2의 경우,영숫자 또는 특수 문자 * 또는 $를 사용하여 **Community String(커뮤니티 문자열)** 필드에 SNMP 커뮤니티 이름을 입력하고 12단계로 건너뜁니다.
- SNMP v3의 경우, **User Name(사용자 이름)** 필드에 SNMP 서버로 인증하려는 사용자 이름을 입력하고 다음 단계로 넘어갑니다.

단계 7 **Authentication Protocol(인증 프로토콜)** 드롭다운 목록에서 인증을 위해 사용하려는 프로토콜을 선택합니다.

단계 8 **Authentication Password(인증 비밀번호)** 필드에 SNMP 서버 인증에 필요한 비밀번호를 입력합니다.

단계 9 **Privacy Protocol(프라이버시 프로토콜)** 목록에서 **None(없음)**을 선택하여 프라이버시 프로토콜을 사용하지 않거나 **DES**를 선택하여 데이터 암호화 표준을 프라이버시 프로토콜로 사용할 수 있습니다.

단계 10 **Privacy Password(프라이버시 비밀번호)** 필드에 SNMP 서버에 필요한 프라이버시 비밀번호를 입력합니다.

단계 11 **Engine ID(엔진 ID)** 필드에 짝수를 사용하여 16진법으로 SNMP 엔진을 위한 식별자를 입력합니다.

SNMPv3을 사용할 때, 시스템은 엔진 ID 값을 사용하여 메시지를 암호화합니다. SNMP 서버에서는 메시지를 해독하는 데 이 값이 필요합니다.

Cisco는 ASA FirePOWER 모듈의 IP 주소를 16진법 버전으로 사용할 것을 권장합니다. 예를 들어, ASA FirePOWER 모듈의 IP 주소가 `10.1.1.77`일 경우 `0a01014D0`을 사용하십시오.

단계 12 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

알림 응답이 저장되고 자동으로 활성화됩니다.

Syslog 알림 응답 생성

라이센스: 모두

syslog 경고 응답을 설정할 때, syslog 메시지와 연결된 심각도 및 기능을 지정하여 syslog 서버에 의해 제대로 처리되었음을 확인할 수 있습니다. 기능은 메시지를 생성하는 하위 시스템을 나타내며, 심각도는 메시지의 심각도를 정의합니다. 기능 및 심각도는 syslog에 나타나는 실제 메시지에 표시되지 않지만, syslog 메시지를 수신하는 시스템에 메시지 카테고리화 방법을 전달하는 데 사용됩니다.

팁 syslog의 작동 방식 및 구성 방법에 대한 자세한 내용은 시스템에 대한 설명서를 참고하십시오. UNIX 시스템에서는 `syslog` 및 `syslog.conf`의 `man` 페이지에서 개념 정보 및 구성 지침을 제공합니다.

syslog 경고 응답을 생성할 때 기능의 모든 유형을 선택할 수 있지만, 사용자의 syslog 서버에 따라 합리적인 한 유형을 선택해야 합니다. 모든 syslog 서버가 모든 기능을 지원하는 것은 아닙니다. UNIX syslog 서버의 경우, `syslog.conf` 파일은 어느 기능이 서버의 어느 로그 파일에 저장되는지 나타냅니다.

다음 표에는 사용자가 선택할 수 있는 syslog 기능이 나열되어 있습니다.

표 27-2 사용 가능한 Syslog 기능

기능	설명
ALERT	알림 메시지입니다.
AUDIT	감사 하위 시스템에 의해 생성된 메시지입니다.
AUTH	보안 및 인증과 관련된 메시지입니다.
AUTHPRIV	보안 및 인증과 관련된 제한적 액세스 메시지입니다. 많은 시스템에서 이러한 메시지는 보안 파일로 전달됩니다.
CLOCK	클록 데몬에 의해 생성된 메시지입니다. Windows 운영 체제를 실행하는 syslog 서버는 CLOCK기능을 사용합니다.
CRON	클록 데몬에 의해 생성된 메시지입니다. Linux 운영 체제를 실행하는 syslog 서버는 CRON 기능을 사용합니다.
DAEMON	시스템 데몬에서 생성된 메시지입니다.
FTP	FTP 데몬에 의해 생성된 메시지입니다.
KERN	커널에 의해 생성된 메시지입니다. 여러 시스템에서 이 메시지가 나타나면 콘솔에 인쇄됩니다.
LOCAL0-LOCAL7	내부 프로세스에 의해 생성된 메시지입니다.
LPR	인쇄 하위 시스템에 의해 생성된 메시지입니다.
MAIL	메일 시스템에 의해 생성된 메시지입니다.
NEWS	네트워크 뉴스 하위 시스템에 의해 생성된 메시지입니다.
NTP	NTP 데몬에 의해 생성된 메시지입니다.
SYSLOG	syslog 데몬에 의해 생성된 메시지입니다.
USER	사용자 레벨 프로세스에 의해 생성된 메시지입니다.
UUCP	UUCP 하위 시스템에 의해 생성된 메시지입니다.

다음 표는 사용자가 선택할 수 있는 표준 syslog 심각도 레벨을 나열합니다.

표 27-3 Syslog 심각도 레벨

수준	설명
ALERT	즉시 해결해야 하는 상태입니다.
CRIT	심각한 상태입니다.
DEBUG	디버깅 정보를 포함하는 메시지입니다.
EMERG	모든 사용자에게 알려진 위험 상태입니다.
ERR	오류 상태입니다.
INFO	정보를 제공하는 메시지입니다.
NOTICE	오류 상태는 아니지만 주의가 필요한 상태입니다.
WARNING	경고 메시지입니다.

Syslog 알림 전송을 시작하기 전에, syslog 서버가 원격 메시지를 허용할 수 있는지 확인해야 합니다.

syslog 알림을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Actions Alerts(작업 경고)**를 선택합니다.

Alerts(경고) 페이지가 열립니다. **Create Alert(경고 생성)** 드롭다운 메뉴에서 **Create Syslog Alert(Syslog 경고 생성)**를 선택합니다.

Create Syslog Alert Configuration(Syslog 경고 구성 생성) 팝업 창이 표시됩니다.

단계 2 저장된 응답을 식별하는 데 사용할 이름을 **Name(이름)** 필드에 입력합니다.

단계 3 **Host(호스트)** 필드에 호스트 이름 또는 syslog 서버의 IP 주소를 입력합니다.

이 필드에 유효하지 않은 IPv4 주소(예를 들어 192.168.1.456)를 입력한다고 해도 시스템에서 경고하지 **않는다**는 점에 유의하십시오. 잘못된 주소는 호스트 이름으로 처리됩니다.

단계 4 서버가 syslog 메시지에 사용할 포트를 **Port(포트)** 필드에 입력합니다.

기본적으로 이 값은 514로 설정됩니다.

단계 5 **Facility(기능)** 목록에서 기능을 선택합니다.

사용 가능한 기능 목록은 사용 가능한 Syslog 기능 표를 참고하십시오.

단계 6 **Severity(심각도)** 목록에서 심각도를 선택합니다.

사용 가능한 심각도 목록은 Syslog 심각도 레벨 표를 참고하십시오.

단계 7 **Tag(태그)** 필드에 syslog 메시지로 표시할 태그 이름을 입력합니다.

태그 이름에는 영숫자 문자만 사용해야 합니다. 공백이나 밑줄은 사용할 수 **없습니다**.

예를 들어, syslog로 전송되는 모든 메시지가 `FromDC`으로 시작되기를 원하는 경우, 필드에 `FromDC`을 입력합니다.

단계 8 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

경고 응답이 저장되고 자동으로 활성화됩니다.

알림 응답 수정

라이센스: 모두

대부분의 알림 유형에서, 알림 응답이 활성화되었고 사용 중인 경우 알림 응답에 대한 변경 사항은 즉시 반영됩니다. 그러나 연결 이벤트 기록을 위해 액세스 제어 규칙에서 사용되는 알림 응답의 경우, 액세스 제어 정책을 다시 적용하기까지 변경 사항이 반영되지 않습니다.

알림 응답을 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Actions Alerts(작업 경고)**를 선택합니다.

Alerts(경고) 페이지가 표시됩니다.

단계 2 수정하려는 알림 응답 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 알림 응답에 대한 구성 팝업 창이 나타납니다.

단계 3 필요에 따라 변경합니다.

단계 4 **Store ASA FirePOWER Changes(ASA FirePOWER 변경 사항 저장)**를 클릭합니다.

알림 응답이 저장됩니다.

알림 응답 삭제

라이센스: 모두

사용하지 않는 알림 응답을 삭제할 수 있습니다.

알림 응답을 삭제하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Actions Alerts(작업 경고)**를 선택합니다.

Alerts(경고) 페이지가 표시됩니다.

단계 2 삭제하려는 알림 응답 옆에 있는 수정 아이콘( )을 클릭합니다.

단계 3 알림 응답을 삭제할 것인지 확인합니다.

알림 응답이 삭제됩니다.

알림 응답 활성화 및 비활성화

라이센스: 모두

활성화된 경고 응답만 알림을 생성할 수 있습니다. 구성을 삭제하는 대신 응답 경고를 한시적으로 비활성화하여 경고가 생성되는 것을 중지할 수 있습니다. 알림이 사용 중일 때 비활성화하면, 비활성화된 후에도 여전히 사용 중인 것으로 간주됩니다.

알림 응답을 활성화 또는 비활성화하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Actions Alerts(작업 경고)**를 선택합니다.

Alerts(경고) 페이지가 표시됩니다.

단계 2 활성화 또는 비활성화할 알림 응답 옆에 있는 활성화/비활성화 슬라이더를 클릭합니다.

알림 응답이 활성화되었던 경우에는 비활성화되고, 비활성화되었던 경우에는 활성화됩니다.

28장 침입 규칙을 위한 외부 경고 구성

ASA FirePOWER 모듈이 사용자 인터페이스 안에서 다양한 관점의 침입 이벤트를 제공하는 동안, 일부 엔터프라이즈는 중요한 시스템에 대한 지속적인 모니터링을 지원하기 위해 외부 침입 이벤트 알림을 정의하는 것을 선호합니다. syslog 기능에 로깅을 활성화하거나 SNMP 트랩 서버에 이벤트 데이터를 보낼 수 있습니다.

각 침입 정책 내에서 침입 이벤트 알림 제한을 지정하고, 외부 로깅 기능에 침입 이벤트 알림을 설정하며, 침입 이벤트에 외부 응답을 구성할 수 있습니다.

팁

일부 분석가는 동일한 침입 이벤트의 여러 경고를 받지 않는 것을 선호하지만, 주어진 침입 이벤트 발생에 대해 얼마나 자주 알림을 받을지 제어하기를 원합니다. 자세한 내용은 20-21페이지의 정책에 따른 침입 이벤트 알림 필터링을 참고하십시오.

침입 정책 외부에는 ASA FirePOWER 모듈에 사용자가 실행할 수 있는 다른 유형의 경고가 있습니다. 다른 유형의 이벤트를 위해 SNMP 및 syslog 경고 응답을 구성할 수 있는데, 여기에는 특정 액세스 제어 규칙에 의해 로깅된 연결 이벤트가 포함됩니다. 자세한 내용은 27-1페이지의 외부 경고 구성을 참고하십시오.

외부 침입 이벤트 알림에 대한 자세한 내용은 다음 섹션을 참고하십시오.

- 28-1페이지의 SNMP 응답 사용은 지정된 SNMP 트랩 서버에 이벤트 데이터를 보내기 위해 사용자가 구성할 수 있는 옵션을 설명하고 SNMP 경고 옵션을 지정하는 절차를 제공합니다.
- 28-4페이지의 Syslog 응답 사용은 외부 syslog에 이벤트 데이터를 보내기 위해 사용자가 구성할 수 있는 옵션을 설명하고 syslog 경고 옵션을 지정하는 절차를 제공합니다.

SNMP 응답 사용

라이센스: 보호

*SNMP 트랩*은 네트워크 관리 알림입니다. *SNMP 경고*로도 알려진 SNMP 트랩으로 침입 이벤트 알림을 전송하기 위해 디바이스를 구성할 수 있습니다. 각 SNMP 경고는 다음을 포함합니다.

- 트랩을 생성하는 서버의 이름
- 이를 탐지한 디바이스의 IP 주소
- 이를 탐지한 디바이스의 이름
- 이벤트 데이터

다양한 SNMP 경고 매개 변수를 설정할 수 있습니다. 사용 가능한 매개 변수는 사용하는 SNMP 버전에 따라 달라집니다. SNMP 경고의 활성화 및 비활성화에 대한 자세한 내용은 19-7페이지의 침입 정책 내 고급 설정 구성을 참고하십시오.

팁 네트워크 관리 시스템에 관리 정보 베이스 파일(MIB)이 필요한 경우 ASA FirePOWER 모듈(`/etc/sf/DCEALERT.MIB`)에서 다운로드할 수 있습니다.

SNMP v2 옵션

SNMP v2의 경우, 다음 표에 설명된 옵션을 지정할 수 있습니다.

표 28-1 SNMP v2 옵션

옵션	설명
트랩 유형	경고에 나타나는 IP 주소를 사용할 트랩 유형입니다. 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 렌더링하는 경우, **as Binary(이진으로)**를 선택할 수 있습니다. 그렇지 않으면, **as String(스트링으로)**을 선택합니다. 예를 들어, HP Openview는 스트링 유형을 요청합니다.
트랩 서버	SNMP 트랩 알림을 받을 서버입니다. 단일 IP 주소 또는 호스트 이름을 지정할 수 있습니다.
커뮤니티 문자열	커뮤니티 이름입니다.

SNMP v3 옵션

SNMP v3의 경우, 다음 표에 설명된 옵션을 지정할 수 있습니다.

참고 SNMP v3을 사용할 때, 어플라이언스는 엔진 ID 값을 사용하여 메시지를 암호화합니다. SNMP 서버에서는 메시지를 해독하는 데 이 값이 필요합니다. 현재로서 이 엔진 ID 값은 항상 스트링 끝에 `01`을 포함하는 어플라이언스 IP 주소의 16진수 버전입니다. 예를 들어, SNMP 알림을 전송하는 어플라이언스가 `172.16.1.50`의 IP 주소를 가질 경우 엔진 ID가 `0xAC10013201`이거나, 어플라이언스의 IP 주소가 `10.1.1.77`일 경우, 엔진 ID로 `0x0a01014D01`이 사용됩니다.

표 28-2 SNMP v3 옵션

옵션	설명
트랩 유형	경고에 나타나는 IP 주소를 사용할 트랩 유형입니다. 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 렌더링하는 경우, **as Binary(이진으로)**를 선택할 수 있습니다. 그렇지 않으면, **as String(스트링으로)**을 선택합니다. 예를 들어, HP Openview는 스트링 유형을 요청합니다.
트랩 서버	SNMP 트랩 알림을 받을 서버입니다. 단일 IP 주소 또는 호스트 이름을 지정할 수 있습니다.
인증 비밀번호	인증을 위해 필요한 비밀번호입니다. SNMP v3은 이 비밀번호를 암호화하기 위해 메시지 다이제스트 5(MD5) 해시 함수 또는 보안 해시 알고리즘(SHA) 해시 함수를 사용하며, 이는 구성에 따른 것입니다. 인증 비밀번호를 지정한 경우, 인증이 활성화됩니다.

표 28-2 SNMP v3 옵션 (계속)

옵션	설명
개인 비밀번호	프라이버시를 위한 SNMP 키입니다. SNMP v3은 이 비밀번호를 암호화하기 위해 데이터 암호화 표준(DES) 블록 암호를 사용합니다. 개인 비밀번호를 지정한 경우, 프라이버시가 활성화됩니다. 개인 비밀번호를 지정한 경우, 인증 비밀번호 또한 반드시 지정해야 합니다.
사용자 이름	SNMP 사용자 이름입니다.

SNMP 경고 구성에 대한 내용은 28-3페이지의 SNMP 응답 구성을 참고하십시오.

SNMP 응답 구성

라이센스: 보호

침입 정책에서 SNMP 경고를 구성할 수 있습니다. 사용자가 액세스 제어 정책의 일부로서 정책을 적용하면, 시스템은 SNMP 트랩을 통해 탐지하는 모든 침입 이벤트에 대해 사용자에게 알립니다. SNMP 경고에 대한 자세한 내용은 28-1페이지의 SNMP 응답 사용을 참고하십시오.

SNMP 경고 옵션을 설정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**를 선택합니다.

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 왼쪽 탐색 패널에서 **Advanced Settings(고급 설정)**를 클릭합니다.

Advanced Settings(고급 설정) 페이지가 나타납니다.

단계 4 외부 응답 조건에서 **SNMP Alerting(SNMP 경고)**이 활성화되어 있는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

SNMP Alerting(SNMP 경고) 페이지가 나타납니다.

페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 5 **as Binary(이진으로)** 또는 **as String(스트링으로)**으로 경고에 나타나는 IP 주소로 사용하려는 트랩 유형 형식을 지정합니다.

참고 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 렌더링하는 경우, **as Binary(이진으로)** 옵션을 사용할 수 있습니다. 그렇지 않으면, **as String(스트링으로)** 옵션을 사용합니다. 예를 들어, HP OpenView에는 **as String(스트링으로)** 옵션이 필요합니다.

단계 6 SNMP v2 또는 SNMP v3 중 하나를 선택합니다:

- SNMP v2를 구성하려면, 해당 필드에서 사용하고자 하는 트랩 서버의 IP 주소 및 커뮤니티 이름을 입력합니다. 28-2페이지의 SNMP v2 옵션을 참고하십시오.
- SNMP v3을 구성하려면, 사용하려는 트랩 서버의 IP 주소, 인증 비밀번호, 개인 비밀번호 그리고 해당 필드의 사용자 이름을 입력합니다. 자세한 내용은 28-2페이지의 SNMP v3 옵션을 참고하십시오.

참고 반드시 SNMP v2 **또는** SNMP v3 중 하나를 선택해야 합니다.

참고 SNMP v3 비밀번호를 입력할 때, 해당 비밀번호는 초기 구성 중에 일반 텍스트로 표시되지만 암호화된 형식으로 저장됩니다.

단계 7 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Syslog 응답 사용

라이센스: 보호

시스템 로그 또는 *syslog*는 네트워크 이벤트 로깅의 표준 로깅 메커니즘입니다. 어플라이언스 syslog에 침입 이벤트 알림인 *syslog 경고*를 전송할 수 있습니다. syslog를 통해 우선 순위 및 기능별로 syslog 내 정보를 분류할 수 있습니다. *우선 순위*는 경고의 심각도를 반영하며 *기능*은 경고를 생성한 하위 시스템을 나타냅니다. 기능 및 우선 순위는 syslog에 나타나는 실제 메시지에 표시되지 않으며, syslog 메시지를 수신하는 시스템에 메시지 카테고리화 방법을 전달하는 데 사용됩니다.

syslog 경고는 다음 정보를 포함합니다.

- 경고 생성 날짜 및 시간
- 이벤트 메시지
- 이벤트 날짜
- 시작 이벤트의 생성자 ID
- 시작 이벤트의 Snort ID
- 개정

침입 정책에서, syslog 경고를 켜서 syslog 내 침입 이벤트 알림과 연결된 syslog 우선 순위 및 기능을 지정할 수 있습니다. 사용자가 액세스 제어 정책의 일부로서 침입 정책을 적용하면, 시스템은 다음 로컬 호스트 또는 정책에 지정된 로깅 호스트에서 syslog 기능에 탐지하는 침입 이벤트에 대한 syslog 경고를 보냅니다. 알림을 수신하는 호스트는 경고를 정렬하기 위해 syslog 경고를 구성할 때 사용자가 설정한 위치 및 우선 순위 정보를 사용합니다.

다음 표는 syslog 경고를 구성할 때 선택할 수 있는 기능을 나열합니다. 사용하는 원격 syslog 서버의 구성에 따라 기능을 구성해야 합니다. (UNIX 또는 Linux 기반 시스템에 syslog 메시지를 로깅하는 경우) 원격 시스템에 위치한 `syslog.conf` 파일은 어느 기능이 서버의 어느 로그 파일에 저장되었는지 나타냅니다.

표 28-3 사용 가능한 Syslog 기능

기능	설명
AUTH	보안 및 인증과 관련된 메시지입니다.
AUTHPRIV	보안 및 인증과 관련된 제한적 액세스 메시지입니다. 많은 시스템에서 이러한 메시지는 보안 파일로 전달됩니다.
CRON	클록 데몬에 의해 생성된 메시지입니다.
DAEMON	시스템 데몬에서 생성된 메시지입니다.
FTP	FTP 데몬에 의해 생성된 메시지입니다.
KERN	커널에 의해 생성된 메시지입니다. 여러 시스템에서 이 메시지가 나타나면 콘솔에 인쇄됩니다.
LOCAL0-LOCAL7	내부 프로세스에 의해 생성된 메시지입니다.
LPR	인쇄 하위 시스템에 의해 생성된 메시지입니다.
MAIL	메일 시스템에 의해 생성된 메시지입니다.
NEWS	네트워크 뉴스 하위 시스템에 의해 생성된 메시지입니다.
SYSLOG	syslog 데몬에 의해 생성된 메시지입니다.
USER	사용자 레벨 프로세스에 의해 생성된 메시지입니다.
UUCP	UUCP 하위 시스템에 의해 생성된 메시지입니다.

다음 표준 syslog 우선 순위 중 이 경고에 의해 생성된 모든 알림에 표시할 하나를 선택합니다.

표 28-4 Syslog 우선 순위

수준	설명
EMERG	모든 사용자에게 브로드캐스팅되는 공황 상태
ALERT	즉시 수정되어야 하는 상태
CRIT	심각한 상태
ERR	오류 상태
WARNING	경고 메시지
NOTICE	오류 상태는 아니지만 주의 필요
INFO	정보를 제공하는 메시지
DEBUG	디버그 정보를 포함하는 메시지

syslog의 작동 방식 및 구성 방법에 대한 자세한 내용은 시스템에 딸린 설명서를 참고하십시오. UNIX 또는 Linux 기반 시스템의 syslog에 로깅하는 경우 `syslog.conf` man 파일(명령줄에 `man syslog.conf` 입력) 및 syslog man 파일(명령줄에 `man syslog` 입력)은 syslog가 작동하는 방식과 이를 구성하는 방식에 관한 정보를 제공합니다.

Syslog 응답 구성

라이센스: 보호

침입 정책에서 syslog 경고를 구성할 수 있습니다. 사용자가 액세스 제어 정책의 일부로서 정책을 적용하면, 시스템은 syslog를 통해 탐지하는 모든 침입 이벤트에 대해 사용자에게 알립니다. syslog 경고에 대한 자세한 내용은 28-4페이지의 Syslog 응답 사용을 참고하십시오.

syslog 경고 옵션을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 정책)**를 선택합니다.

Intrusion Policy(침입 정책) 페이지가 나타납니다.

단계 2 수정하려는 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장되지 않은 변경 사항이 있는 경우, **OK(확인)**를 클릭하여 해당 변경 사항을 삭제하고 다음으로 넘어갑니다. 다른 정책에서 저장되지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

Policy Information(정책 정보) 페이지가 나타납니다.

단계 3 왼쪽 탐색 패널에서 **Advanced Settings(고급 설정)**를 클릭합니다.

Advanced Settings(고급 설정) 페이지가 나타납니다.

단계 4 외부 응답 조건에서 **Syslog Alerting(Syslog 경고)**이 활성화되었는지 여부에 따라 두 가지 옵션이 있습니다.

- 구성이 활성화된 경우, **Edit(수정)**를 클릭합니다.
- 구성이 비활성화된 경우, **Enabled(활성화)**를 클릭한 후 **Edit(수정)**를 클릭합니다.

Syslog Alerting(Syslog 경고) 페이지가 나타납니다.

페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. 자세한 내용은 12-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을 참고하십시오.

단계 5 또는 **Logging Hosts(로깅 호스트)** 필드에서 로그 호스트로 지정하려는 원격 액세스 IP 주소를 입력합니다. 호스트가 여러 개인 경우 쉼표로 구분하십시오.

단계 6 드롭다운 목록에서 기능 및 우선 순위를 선택합니다.

기능 및 우선 순위 옵션에 대한 자세한 내용은 28-4페이지의 Syslog 응답 사용을 참고하십시오.

단계 7 변경 사항을 시스템 캐시에 유지하면서 정책을 저장하고, 수정을 계속하고, 변경 사항을 삭제하고, 기본 정책 내 기본 구성 설정으로 돌아가거나 종료합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

ASA FirePOWER대시보드 사용

ASA FirePOWER 모듈 대시보드는 현재 시스템 상태에 대한 일견을 제공합니다. 대시보드는3열 레이아웃에서 위젯을 표시합니다. 위젯은 ASA FirePOWER 모듈의 다양한 측면에 대한 통찰력을 제공하는 크기가 작은 자체 구성 요소입니다. 미리 정의된 여러 가지 위젯이 사용자의 시스템에 제공됩니다. 예를 들어, Appliance Information(어플라이언스 정보) 위젯은 어플라이언스 이름, 모델, 및 ASA FirePOWER 모듈 소프트웨어의 현재 실행 중인 버전을 알려줍니다.

대시보드에는 해당 위젯을 제한하는 시간 범위가 있습니다. 시간 범위를 마지막 시간 단위로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수 있습니다.

각 어플라이언스는 Summary Dashboard(요약 대시보드)라는 기본 대시보드를 제공합니다. 이 대시보드는 임시 사용자에게 일반 사용자의 ASA FirePOWER 모듈 배포를 위한 시스템 상태 정보를 제공합니다.

대시보드 및 콘텐츠에 관한 자세한 내용은, 다음 섹션을 참고하십시오.

- 29-1페이지의 대시 보드 위젯의 이해
- 29-2페이지의 미리 정의된 위젯의 이해
- 29-6페이지의 대시보드작업

대시 보드 위젯의 이해

라이센스: 모두

대시보드는 3열 레이아웃에서 다수의 위젯을 표시합니다. ASA FirePOWER 모듈은 미리 정의된 여러 대시보드 위젯을 제공받는데, 각 위젯은 시스템의 여러 측면에 대한 통찰을 제공합니다. 위젯을 최소화 및 최대화하고 위젯을 다시 정렬할 수도 있습니다.

자세한 내용은 다음을 참고하십시오.

- 29-2페이지의 위젯 환경 설정의 이해
- 29-2페이지의 미리 정의된 위젯의 이해
- 29-6페이지의 대시보드작업

위젯 환경 설정의 이해

라이센스: 모두

각 위젯에는 해당 작업을 결정하는 환경 설정 집합이 있습니다.

위젯 환경 설정은 간소화할 수 있습니다. 예를 들어, 사용자가 설정할 수 있는 부분은 Current Interface Status(현재 인터페이스 상태) 위젯에 대한 환경 설정이며, 이는 내부 네트워크에서 활성화된 모든 인터페이스의 현재 상태를 표시합니다. 이 위젯에 대해서는 업데이트 빈도만 구성할 수 있습니다.

위젯의 환경 설정을 수정하려면 다음을 수행합니다.

단계 1 환경 설정을 변경하고자 하는 위젯의 제목 표시줄에서 환경 설정 표시 아이콘( )을 클릭합니다.

해당 위젯에 대한 환경 설정 섹션이 나타납니다.

단계 2 필요에 따라 적절히 변경합니다.

변경 사항은 즉시 적용됩니다. 개별 위젯에 대해 지정할 수 있는 환경 설정에 대한 자세한 내용은 29-2페이지의 미리 정의된 위젯의 이해를 참조하십시오.

단계 3 환경 설정 섹션을 숨기려면 위젯의 제목 표시줄에서 환경 설정 숨기기 아이콘( )을 클릭합니다.

미리 정의된 위젯의 이해

라이센스: 모두

ASA FirePOWER 모듈에는 현재 시스템 상태에 대한 일견을 제공하는 미리 정의된 여러 가지 위젯이 제공됩니다.

위젯에 대한 자세한 정보는 다음 섹션을 참고하십시오.

어플라이언스 정보 위젯의 이해

라이센스: 모두

Appliance Information(어플라이언스 정보) 위젯은 다음을 제공합니다.

- 어플라이언스 이름, IPv4 주소, IPv6 주소 및 모델
- ASA FirePOWER 모듈 소프트웨어의 버전, 규칙 업데이트 및 어플라이언스에 설치된 위치 정보 업데이트

단순 보기 또는 고급 보기를 표시하는 위젯 환경 설정을 수정하여 더 많은 정보 또는 더 적은 정보를 표시하도록 위젯을 구성할 수 있습니다. 환경 설정에서는 또한 위젯 업데이트의 빈도를 제어합니다. 자세한 내용은 29-2페이지의 위젯 환경 설정의 이해를 참고하십시오.

현재 인터페이스 상태 위젯의 이해

라이센스: 모두

Current Interface Status(현재 인터페이스 상태) 위젯은 활성화되어 있거나 사용하지 않는 어플라이언스의 모든 인터페이스의 상태를 보여줍니다. 각 인터페이스의 경우, 위젯은 다음을 제공합니다.

- 인터페이스의 이름
- 인터페이스의 연결 상태
- 인터페이스의 연결 모드(예: 전이중 100Mb 또는 반이중 10Mb)
- 인터페이스 유형(즉, 구리 또는 파이버)
- 인터페이스로 수신(Rx) 및 전송(Tx)된 데이터 양

링크 상태를 나타내는 공 색상은 다음과 같이 현재 상태를 표시합니다.

- 녹색: 링크가 최대 속도로 작동 중
- 노란색: 링크가 최대 속도로 작동 중
- 빨간색: 링크가 작동하지 않음
- 회색: 링크가 관리 목적으로 비활성화됨
- 파란색: 연결 상태 정보를 사용할 수 없음(예: ASA)

위젯 환경 설정은 위젯 업데이트의 빈도를 제어합니다. 자세한 내용은 29-2페이지의 위젯 환경 설정의 이해를 참고하십시오.

디스크 사용량 위젯의 이해

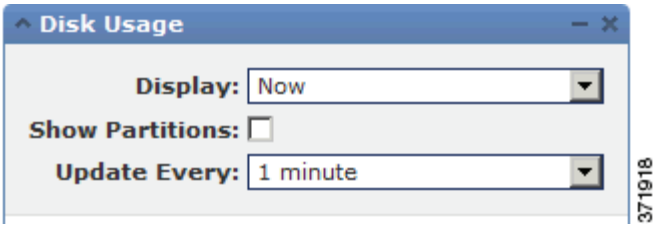
라이센스: 모두

Disk Usage(디스크 사용량) 위젯은 디스크 사용량 카테고리에 근거하여 하드 드라이브에 사용되는 공간을 표시합니다. 이는 또한 어플라이언스 하드 드라이브의 각 파티션에 대한 용량 및 사용되는 공간을 나타냅니다. By Category(By 카테고리) 누적 막대는 총 사용 가능한 디스크 공간 중 사용되고 있는 비율로 각 디스크 사용량 카테고리를 나타냅니다. 다음 표에서는 사용 가능한 카테고리를 설명합니다.

표 29-1 디스크 사용량 카테고리

디스크 사용량 카테고리	설명
이벤트	시스템에서 로깅된 모든 이벤트
파일	시스템에서 저장된 모든 파일
백업	모든 백업 파일
업데이트	규칙 업데이트 및 시스템 업데이트와 같은 업데이트와 관련된 모든 파일
기타	시스템 문제 해결 파일 및 기타 파일
여유 공간	어플라이언스에 남아 있는 여유 공간

악성코드 스토리지 팩이 설치된 경우, 위젯 설정을 수정하여 위젯이 By Category(By 카테고리) 누적 막대만 표시하도록 구성하거나 누적 막대와 관리(/), /Volume, 및 /boot 파티션 사용, 그리고 /var/storage 파티션을 함께 표시할 수 있습니다.



위젯 설정은 또한 위젯 업데이트의 빈도뿐 아니라 대시보드 시간 범위에 현재 디스크 사용량 또는 수집한 디스크 사용량 통계량을 표시 여부를 제어합니다. 자세한 내용은 29-2페이지의 위젯 환경 설정의 이해를 참고하십시오.

제품 라이센싱 위젯의 이해

라이센스: 모두

Product Licensing(제품 라이센싱) 위젯은 현재 설치된 기능 라이센스와 디바이스를 보여줍니다. 또한 (사용자 또는 호스트와 같은) 라이센싱된 항목 수 및 라이센싱된 항목 중 남아 있는 허용된 항목 수를 나타냅니다.

위젯의 상단 섹션은 에 설치된 모든 디바이스 및 기능을 표시합니다. 여기에는 임시 라이센스가 포함되지만 Expiring Licenses(만료 라이센스) 섹션은 임시 라이센스와 만료된 라이센스만 표시합니다.

위젯 백그라운드의 막대는 사용 중인 라이센스의 각 유형에 대한 백분율을 나타냅니다. 막대는 오른쪽에서 왼쪽으로 읽어야 합니다. 만료된 라이센스는 취소 회선으로 표시됩니다.

위젯 환경 설정을 수정하여 현재 라이센싱된 기능 또는 라이센싱할 수 있는 모든 기능 중 하나를 표시하는 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다. 자세한 내용은 29-2페이지의 위젯 환경 설정의 이해를 참고하십시오.

라이센스 유형을 클릭하여 로컬 구성의 License(라이센스) 페이지로 이동하거나 기능 라이센스를 추가 또는 삭제할 수 있습니다. 자세한 내용은 34-1페이지의 ASA FirePOWER 모듈 라이센싱을 참고하십시오.

제품 업데이트 위젯의 이해

라이센스: 모두

Product Updates(제품 업데이트) 위젯은 최근 어플라이언스에 설치된 소프트웨어(ASA FirePOWER 모듈 소프트웨어 및 규칙 업데이트)의 요약뿐 아니라 해당 소프트웨어에 다운로드했으나 아직 설치하지 않은 사용 가능한 업데이트에 관한 정보를 제공합니다.

소프트웨어 업데이트의 다운로드, 푸시 또는 설치에 대해 예약된 작업을 구성하지 않는 한 위젯이 소프트웨어의 최신 버전으로 Unknown(알 수 없음)을 표시한다는 점에 유의하십시오. 위젯은 예약된 작업을 사용하여 최신 버전을 결정합니다. 자세한 내용은 31-1페이지의 작업 일정 관리를 참고하십시오.

위젯은 또한 소프트웨어를 업데이트할 수 있는 페이지 링크를 제공합니다

위젯 설정을 수정하여 최신 버전을 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다. 자세한 내용은 29-2페이지의 위젯 환경 설정의 이해를 참고하십시오.

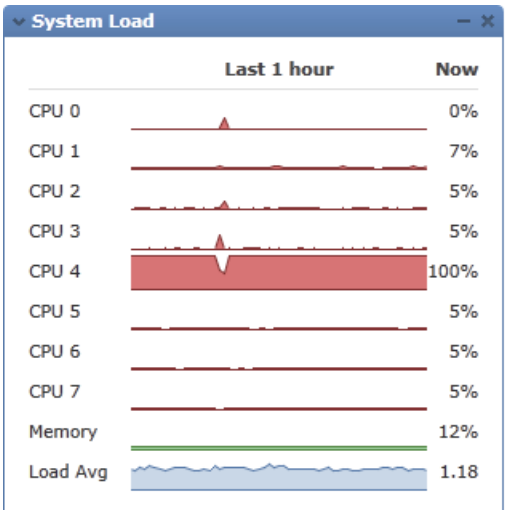
Product Updates(제품 업데이트) 위젯에서 다음을 수행할 수 있습니다.

- ASA FirePOWER 모듈 소프트웨어, 규칙 업데이트 또는 위치 정보 업데이트의 최신 버전을 클릭하여 어플라이언스를 수동으로 업데이트할 수 있습니다.
- 시스템 소프트웨어, 또는 위치 정보 데이터베이스를 업데이트하려면 35-1페이지의 ASA FirePOWER 모듈 소프트웨어 업데이트를 참고하십시오.
- 최신 규칙 업데이트를 가져오려면 35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기를 참고하십시오.
- ASA FirePOWER 모듈 소프트웨어 또는 규칙 업데이트의 최신 버전을 다운로드하는 예약 작업은 최신 버전)을 클릭하여 생성할 수 있습니다(31-1페이지의 작업 일정 관리 참고).

시스템 로드 위젯의 이해

라이센스: 모두

System Load(시스템 로드) 위젯은 CPU 사용량(각 CPU), 메모리(RAM) 사용량, 어플라이언스에서 시스템 로드(또한 실행을 기다리는 프로세스의 수로 측정된 로드 평균)를 보여줍니다. 이는 현재 및 대시보드 시간 범위 모두를 보여주는 것입니다.



위젯 환경 설정을 수정하여 로드 평균을 보여주거나 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다. 자세한 내용은 29-2페이지의 위젯 환경 설정의 이해를 참고하십시오.

시스템 시간 위젯의 이해

라이센스: 모두

System Time(시스템 시간) 위젯은 어플라이언스의 로컬 시스템 시간, 가동 시간 및 부팅 시간을 보여줍니다.

위젯 환경 설정을 수정하여 부팅 시간을 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 어플라이언스의 시계와 위젯 동기화의 빈도를 제어합니다. 자세한 내용은 29-2페이지의 위젯 환경 설정의 이해를 참고하십시오.

대시보드작업

라이센스: 모두

대시보드에 나타나는 위젯을 보고 수정할 수 있습니다.

대시보드 작업에 대한 자세한 정보는 다음을 참고하십시오.

- 29-6페이지의 대시보드보기
- 29-7페이지의 대시보드 수정
- B-1페이지의 구성 내보내기

대시보드보기

라이센스: 모두

언제든지 대시보드(ASA FirePOWER 모듈에 대함)를 보려면 **ASA FirePOWER Dashboard(ASA FirePOWER 대시보드)**를 선택합니다.

대시보드에는 해당 위젯을 제한하는 시간 범위가 있습니다. 시간 범위를 변경하여 지난 시간처럼 짧은 기간(기본값) 또는 지난 해처럼 긴 기간을 반영할 수 있습니다. 시간 범위를 변경할 때, 시간을 통해 자동 제한될 수 있는 위젯은 새로운 시간 범위를 반영하도록 업데이트합니다.

모든 위젯을 시간으로 제한할 수 있는 것은 아님에 유의하십시오. 예를 들어, 대시보드 시간 범위는 ASA FirePOWER 모듈 소프트웨어의 이름, 모델 및 최신 버전을 포함한 정보를 제공하는 Appliance Information(어플라이언스 정보) 위젯에 영향을 주지 않습니다.

대시보드를 보려면 다음을 수행합니다.

단계 1 **Home(홈) > ASA FirePOWER Dashboard(ASA FirePOWER 대시보드)**를 선택합니다.

선택한 ASA FirePOWER대시보드가 나타납니다.

대시보드 시간 범위를 변경하려면 다음을 수행합니다.

단계 1 **Show the Last(마지막 선택 표시)** 드롭다운 목록에서 시간 범위를 선택합니다.

페이지의 모든 해당 위젯은 새로운 시간 범위를 반영하도록 업데이트됩니다.

대시보드 수정

라이센스: 모두

대시보드는 3열 레이아웃에서 위젯을 표시합니다. 위젯을 최소화 및 최대화하고 위젯을 다시 정렬할 수도 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 29-7페이지의 위젯 재배치
- 29-7페이지의 위젯 최소화 및 최대화

위젯 재배치

라이센스: 모두

모든 위젯의 위치를 변경할 수 있습니다..

위젯을 이동하려면 다음을 수행합니다.

단계 1 이동을 원하는 위젯의 제목 표시줄을 클릭한 다음, 새 위치로 끌어 놓습니다.

위젯 최소화 및 최대화

라이센스: 모두

보기를 간소화하는 위젯을 최소화할 수 있으며, 이후 다시 보기를 원할 때 해당 항목을 최대화할 수 있습니다.

위젯을 최소화하려면 다음을 수행합니다.

단계 1 위젯의 제목 표시줄에서 최소화 아이콘(−)을 클릭합니다.

위젯을 확대하려면 다음을 수행합니다.

단계 1 최소화한 위젯의 제목 표시줄에서 최대화 아이콘(□)을 클릭합니다.

ASA FirePOWER 보고서 사용

사용자 네트워크의 트래픽을 분석하기 위해 다양한 기간에 대한 보고서를 볼 수 있습니다. 보고서는 사용자 네트워크 트래픽의 다양한 부분에 대한 정보를 통합합니다. 대부분의 경우, 일반 정보에서 특정 정보로 드릴 다운할 수 있습니다. 예를 들어, 모든 사용자에 관한 보고서를 본 후 특정 사용자에 대한 세부 정보를 볼 수 있습니다.

요약 및 세부 정보 보고서는 상위 정책 및 웹 카테고리와 같은 여러 보고서 구성 요소를 포함합니다. 이 보고서는 사용자가 보고 있는 보고서에 대해 해당 유형에서 가장 자주 발생하는 항목을 보여줍니다. 예를 들어, 특정 사용자에 대한 세부 정보 보고서를 확인하는 경우, 상위 정책은 해당 사용자와 가장 관련이 있는 정책 히트를 보여줍니다.

자세한 내용은 다음을 참고하십시오.

- 30-1페이지의 사용 가능한 보고서 이해
- 30-3페이지의 보고서 기본 사항

사용 가능한 보고서 이해

라이센스: 모두

사용 가능한 보고서에는 ASA FirePOWER 모듈에서 사용 가능한 주요 보고서가 포함됩니다. ASA FirePOWER Reporting(보고서) 메뉴에서 이 보고서를 볼 수 있습니다.

일반적으로, 이름 및 View More(더 보기) 링크를 포함한 여러 항목을 클릭하여 개별 항목 또는 모니터링된 카테고리에 대한 더욱 자세한 정보를 전체적으로 파악할 수 있습니다.

네트워크 개요

이 보고서는 네트워크의 트래픽에 대한 요약 정보를 보여줍니다. 심층 분석이 필요한 분야를 식별하거나 네트워크가 일반적으로 예상되는 범위 내에서 작동하고 있는지 확인하기 위해 이 정보를 사용합니다.

사용자

이 보고서는 네트워크의 상위 사용자를 보여줍니다. 이 정보를 사용하면 사용자의 비정상적 활동을 파악하는 데 도움이 됩니다.

팁 사용자 이름은 사용자 ID 정보가 트래픽 흐름에 관련된 경우에만 사용할 수 있습니다. 사용자 ID가 대다수의 트래픽에 대한 보고서에서 사용할 수 있도록 하려는 경우, 다수의 액세스 제어 정책은 활성 인증을 사용해야 합니다.

애플리케이션

이 보고서는 애플리케이션을 표시하는데, 이러한 애플리케이션은 침입 이벤트를 시작한 트래픽에서 탐지된 HTTP 트래픽에 대한 컨텐츠 또는 요청된 URL을 나타냅니다. 모듈이 HTTP의 애플리케이션 프로토콜을 탐지하지만 특정 웹 애플리케이션을 탐지할 수 없는 경우, 모듈은 여기에서 일반 웹 탐색 지정을 제공한다는 점에 유의하십시오.

웹 카테고리

이 보고서는 방문한 웹 사이트의 카테고리화에 기반하여 네트워크에서 사용되고 있는 도박, 광고 또는 검색 엔진 및 포털 등의 웹 사이트 카테고리를 보여줍니다. 이 정보를 사용하면 사용자가 방문한 주요 카테고리를 식별하는 데 도움이 되고 액세스 제어 정책이 원치 않는 카테고리를 충분히 차단하고 있는지 여부를 확인할 수 있습니다.

정책

이 보고서는 액세스 제어 정책이 네트워크 내 트래픽에 적용된 방식을 보여줍니다. 이 정보를 사용하면 정책 효율성을 평가하는 데 도움이 됩니다.

인그레스 영역

이 보고서는 이벤트를 트리거한 패킷의 인그레스 보안 영역을 표시합니다.

이그레스 영역

이 보고서는 이벤트를 트리거한 패킷의 이그레스 보안 영역을 표시합니다.

대상

이 보고서는 네트워크의 트래픽 분석에 따라 네트워크에서 사용되고 있는 Facebook 등의 애플리케이션을 보여줍니다. 이 정보를 사용하면 네트워크에서 사용되는 최상위 애플리케이션을 식별하는 데 도움이 되고 원치 않는 애플리케이션의 사용을 줄이기 위해 추가 액세스 제어 정책이 필요한지 여부를 결정할 수 있습니다.

공격자

이 보고서는 이벤트를 시작한 송신 호스트가 사용하는 소스 IP 주소를 표시합니다.,

대상

이 보고서는 이벤트를 시작한 수신 호스트가 사용하는 대상 IP 주소를 표시합니다.

위협

이 보고서는 사용자 네트워크에 대해 탐지된 각각의 위협에 할당된 고유한 식별 번호 및 설명 텍스트를 표시합니다.

파일 로그

이 보고서는 탐지된 파일의 유형, 예를 들어, HTML 또는 MSEXE를 표시합니다.

보고서 기본 사항

라이센스: 모두

다음 섹션에서는 보고서 사용의 기본 사항에 대해 설명합니다. 이 항목은 단일 특정 보고서가 아닌 일반적인 보고서 전반에 적용됩니다.

자세한 내용은 다음을 참고하십시오.

- 30-3페이지의 보고서 데이터 이해
- 30-3페이지의 보고서 드릴 다운
- 30-4페이지의 보고서 시간 범위 변경
- 30-4페이지의 보고서에 표시된 데이터 제어
- 30-5페이지의 보고서 열 이해

보고서 데이터 이해

라이센스: 모두

보고서 데이터는 디바이스에서 즉시 수집되므로 보고서에 반영된 데이터와 네트워크 활동 사이에는 지연 시간이 거의 없습니다. 하지만 데이터를 분석할 경우, 다음 사항에 주의하십시오.

- 데이터는 ASA FirePOWER 모듈에 적용된 액세스 제어 정책과 일치하는 트래픽에 대해 수집됩니다.
- 데이터는 5분 분량의 버킷으로 집계되며 30분 및 1시간 그래프는 5분 증분 시마다 데이터 포인트를 보여줍니다. 1시간이 경과하면, 5분 분량의 버킷은 1시간 분량의 버킷으로 집계되는데, 이는 이후에 하루 및 주 단위 버킷으로 집계됩니다. 5분 분량의 버킷은 7일간 보관되며, 1시간 분량의 버킷은 31일, 1일 분량의 버킷은 최대 365일간 보관됩니다. 더 이전으로 이동할수록 더 많은 데이터가 집계됩니다. 이전 데이터를 쿼리할 때, 이러한 데이터 버킷의 가용성에 쿼리를 맞춘 경우 최상의 결과를 얻을 수 있습니다.

참고 예를 들면, 데이터 포인트가 없는 경우, 디바이스가 5분 이상 연결할 수 없으므로, 선형 차트에 차이가 있습니다.

보고서 드릴 다운

라이센스: 모두

보고서에는 사용자가 필요한 정보로 드릴 다운하는 데 도움이 될 수 있도록 많은 링크가 포함됩니다. 어느 항목이 해당 항목에 대해 더 많은 정보를 제공하는지 보려면 항목 위에 마우스를 올려 놓습니다.

예를 들어, 일반적인 보고서 항목에서 View More(더 보기) 링크를 클릭하여 해당 항목에 대한 요약 보고서로 이동할 수 있습니다.

또한 요약 보고서의 항목을 클릭하여 특정 항목에 대한 세부 정보 보고서로 이동할 수 있습니다. 예를 들어, 애플리케이션 요약 보고서에서 HTTP(Hypertext Transfer Protocol)를 클릭하면 HTTP의 애플리케이션 세부 정보 보고서로 이동할 수 있습니다.

보고서 시간 범위 변경

라이센스: 모두

보고서를 볼 때, Time Range(시간 범위) 목록을 사용하는 보고서에 포함할 정보를 정의하는 시간 범위를 변경할 수 있습니다. 시간 범위 목록은 각 보고서 상단에 표시되며, 이를 사용하여 지난 시간 또는 지난 주와 같은 미리 정의된 시간 범위를 선택하거나 특정 시작 및 종료 시간을 지닌 사용자 지정 시간 범위를 정의할 수 있습니다. 선택한 시간 범위는 선택 항목을 변경할 때까지 사용자가 보는 다른 모든 보고서에 계속 적용됩니다.

보고서는 10분마다 자동으로 업데이트됩니다.

다음 표는 시간 범위 옵션에 대해 설명합니다.

표 30-1 보고서의 시간 범위

시간 범위	데이터가 반환되는 시간
지난 30분	5분 간격으로 총 30분, 추가 5분 포함
지난 1시간	5분 간격으로 총 60분, 추가 5분 포함
지난 24시간	지난 시간 범위에 포함된 지난 24시간에 대한 1시간 간격. 예를 들어, 현재 시간이 13시 45분인 경우, Last 24 Hour(지난 24 시간)이라는 기간은 어제 13시부터 오늘 13시까지입니다.
지난 7일	지난 시간 범위에 포함된 지난 7일에 대한 1시간 간격
지난 7일	지난 자정에 시작된 지난 30일에 대한 1일 간격
사용자 지정 범위	사용자가 정의하는 시간 범위 시작 날짜, 시작 시간, 종료 날짜 및 종료 시간을 위한 Edit(수정) 상자가 표시됩니다. 각 상자를 클릭하고 원하는 값을 선택합니다. 종료 시 **Apply(적용)**를 클릭하여 보고서를 업데이트합니다. 사용자 지정 시간 범위를 구성할 때, 지정하는 범위를 데이터 버킷의 가용성에 맞추어 조정해야 합니다. 과거 7~31일 범위의 경우 쿼리를 시간에 맞춥니다. 그보다 이전 범위의 경우, 일자별로 맞춥니다. 1년이 넘는 범위에 대해서는 주별로 맞춥니다.

보고서에 표시된 데이터 제어

라이센스: 모두

요약 및 세부 정보 보고서에는 Top Policies(상위 정책) 및 Web Categories(웹 카테고리)와 같은 여러 부수적인 보고서가 포함됩니다. 각 보고서 패널에는 데이터의 다양한 부분을 확인할 수 있는 제어 기능이 포함되어 있습니다. 다음 제어 기능을 사용할 수 있습니다.

트랜잭션 또는 데이터 사용

트랜잭션 수 또는 거래의 데이터 볼륨에 따라 차트를 보려면 이 링크를 클릭합니다.

모두, 거부됨, 허용됨

각 보고서의 오른쪽 상단에 있는 레이블이 없는 드롭다운 목록에는 이러한 옵션이 포함됩니다. 이를 사용하여 거부된 연결만 볼지, 허용된 연결만 볼지, 또는 거부 또는 허용 여부에 상관없이 모든 연결을 볼지 여부를 변경합니다.

더 보기

보고 있는 항목에 대한 보고서로 이동하려면 View More(더 보기) 링크를 클릭합니다. 예를 들어, Destinations(대상) 보고서의 Web Categories(웹 카테고리) 차트에서 **View More(더 보기)**을 클릭하면 Web Categories(웹 카테고리) 보고서로 이동합니다. 상세 보고서에서 보고서를 보고 있는 경우, 사용자가 세부 정보를 보고 있는 항목에 대한 상세 Web Categories(웹 카테고리) 보고서로 이동합니다.

보고서 열 이해

라이센스: 모두

보고서에는 일반적으로 그래픽 형식으로 표시된 정보 외에도 정보를 나타내는 하나 이상의 표가 포함됩니다.

- 여러 열의 의미는 열이 포함된 보고서에 의해 변경됩니다. 예를 들어, 트랜잭션 열은 보고된 항목의 유형에 대한 트랜잭션 수를 나타냅니다. 또한 **Values(값)** 또는 **Percentages(백분율)**를 클릭하여 원시 수 사이의 값 및 항목에 대해 보고된 전체 원시 값의 비율로 값을 토글할 수 있습니다.
- 열 제목을 클릭하여 열의 정렬 순서를 변경할 수 있습니다.

다음 표에서는 다양한 보고서에서 찾을 수 있는 표준 열에 대해 설명합니다.

표 30-2 보고서 열

열	설명
트랜잭션	보고된 항목에 대한 총 거래 수
허용된 트랜잭션	보고된 항목에 허용된 트랜잭션의 수
거부된 트랜잭션	정책에 기반하여 보고된 항목에 대해 차단된 트랜잭션의 수
전체 바이트	보고된 항목에 송수신된 바이트의 합계
수신된 바이트	보고된 항목에 수신된 바이트의 수.
전송된 총 바이트	보고된 항목에 전송된 바이트의 수.

31장 작업 일정 관리

여러 다양한 유형의 관리 작업이 한 번에 또는 주기적으로 지정된 시간에 실행되도록 일정을 관리할 수 있습니다.

참고 (자동화된 소프트웨어 업데이트를 포함하는 작업과 같은) 일부 작업은 낮은 대역폭을 가진 네트워크에 상당한 로드를 배치할 수 있습니다. 이와 같은 작업이 네트워크 사용 정도가 낮은 기간 동안 실행되도록 일정을 관리해야 합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 31-2페이지의 반복 작업 구성에서는 작업이 일정한 간격을 두고 실행되도록 예약된 작업을 설정하는 방법에 대해 설명합니다.
- 31-3페이지의 백업 작업 자동화에서는 백업 작업 일정 관리하는 절차를 제공합니다.
- 31-4페이지의 인증서 철회 목록 다운로드 자동화에서는 어플라이언스를 위한 CRL(인증서 철회 목록)을 자동으로 새로 고치는 절차를 제공합니다.
- 31-5페이지의 침입 정책 적용의 자동화에서는 침입 정책 적용을 대기시키는 절차를 제공합니다.
- 31-6페이지의 위치 정보 데이터베이스 업데이트 자동화에서는 위치 정보 데이터베이스(GeoDB)의 자동 업데이트 일정 관리를 위한 절차를 제공합니다.
- 31-6페이지의 소프트웨어 업데이트 자동화에서는 소프트웨어 업데이트 다운로드, 푸시 및 설치의 일정을 관리하는 절차를 제공합니다.
- 31-9페이지의 URL 필터링 업데이트 자동화에서는 URL 필터링 데이터의 업데이트를 자동화하는 절차를 제공합니다.
- 31-10페이지의 작업 보기에서는 작업이 예약된 후 보고 관리하는 방법에 대해 설명합니다.
- 31-11페이지의 예약된 작업 수정에서는 기존 작업을 수정하는 방법에 대해 설명합니다.
- 31-12페이지의 예약된 작업 삭제에서는 일회성 작업 및 반복 작업의 모든 인스턴스를 삭제하는 방법에 대해 설명합니다.

반복 작업 구성

라이센스: 모두

모든 유형의 작업에 동일한 프로세스를 사용하여 반복 작업의 빈도를 설정합니다.

사용자 인터페이스에서 대부분의 페이지에 표시되는 시간은 로컬 시간이며, 이는 로컬 구성에서 지정하는 시간대를 사용하여 결정된다는 점에 유의하십시오. 또한 ASA FirePOWER 모듈은 해당하는 경우 DST(일광 절약 시간)를 위해 해당 지역 시간 표시를 자동으로 조정합니다. 그러나, DST와 표준 시간을 오가는 전환 날짜를 포괄하는 반복 작업은 전환을 위해 조정되지 않습니다. 즉, 표준 시간 동안 오전 2시에 예약된 작업을 생성하는 경우, 이는 DST 동안 오전 3시에 실행됩니다. 유사하게, DST 동안 오전 2시에 예약된 작업을 생성하는 경우, 이는 표준 시간 동안 오전 1시에 실행됩니다.

반복 작업을 설정하려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

Scheduling(일정 관리) 페이지가 나타납니다.

단계 2 **Add Task(작업 추가)**를 클릭합니다.

새 작업(New Task) 페이지가 표시됩니다.

단계 3 **Job Type(작업 유형)** 목록에서 일정을 예약할 작업 유형을 선택합니다.

예약할 수 있는 각각의 작업 유형은 해당하는 섹션에 설명되어 있습니다.

단계 4 **Schedule task to run(실행할 작업 예약)** 옵션의 경우 **Recurring(반복)**을 선택합니다.

페이지가 다시 로드되어 반복 작업 옵션이 표시됩니다.

단계 5 **Start On(착수 일자)** 필드에서 반복 작업을 시작할 날짜를 지정합니다. 드롭다운 목록을 사용하여 월, 일, 연도를 선택할 수 있습니다.

단계 6 **Repeat Every(반복 빈도)** 필드에서 작업의 반복 빈도를 지정합니다. 시간, 일, 주, 달을 지정할 수 있습니다.

팁 숫자를 입력하거나 위 아이콘(▲) 및 아래 아이콘(▼)을 클릭하여 간격을 지정할 수 있습니다. 예를 들어, 이틀마다 작업을 실행하려면 2를 입력하고 Days(일)를 선택합니다.

단계 7 **Run At(착수 시간)** 필드에서 반복 작업을 시작할 시간을 지정합니다.

단계 8 `Weeks(주)`를 **Repeat Every(반복 빈도)**로 선택한 경우, **Repeat On(반복 일자)** 필드가 나타납니다. 작업을 실행할 주의 날짜 옆에 있는 확인 상자를 선택합니다.

단계 9 `Months(달)`를 **Repeat Every(반복 빈도)**로 선택한 경우, **Repeat On(반복 일자)** 필드가 나타납니다. 드롭다운 목록을 사용하여 작업을 실행할 달의 날짜를 선택합니다.

New Task(새 업무) 페이지의 나머지 옵션은 생성하는 작업에 따라 결정됩니다. 자세한 내용은 다음 섹션을 참고하십시오.

- 31-3페이지의 백업 작업 자동화
- 31-4페이지의 인증서 철회 목록 다운로드 자동화
- 31-5페이지의 침입 정책 적용의 자동화
- 31-6페이지의 소프트웨어 업데이트 자동화
- 31-9페이지의 URL 필터링 업데이트 자동화

백업 작업 자동화

스케줄러를 사용하여 ASA FirePOWER 모듈의 백업을 자동화할 수 있습니다. 백업을 예약된 작업으로 구성하기 전에 반드시 백업 프로파일을 설계해야 합니다. 자세한 내용은 37-3페이지의 백업 프로파일 생성을 참고하십시오.

백업 작업을 자동화하려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

Scheduling(일정 관리) 페이지가 나타납니다.

단계 2 **Add Task(작업 추가)**를 클릭합니다.

새 작업(New Task) 페이지가 표시됩니다.

단계 3 **Job Type(작업 유형)** 목록에서 **Backup(백업)**을 선택합니다.

페이지가 다시 로드되어 백업 옵션이 표시됩니다.

단계 4 **Once(한 번에)** 또는 **Recurring(반복)** 중에서 백업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time(현재 시간)** 필드는 어플라이언스의 현재 시간을 나타냅니다.
- 반복 작업의 경우, 작업의 인스턴스 간 간격을 설정하는 여러 옵션이 있습니다. 자세한 내용은 31-2페이지의 반복 작업 구성을 참고하십시오.

단계 5 **Job Name(작업 이름)** 필드에 최대 255자의 영숫자, 스페이스 또는 대시를 사용한 이름을 입력합니다.

단계 6 **Backup Profile (백업 프로파일)** 목록에서 해당 백업 프로파일을 선택합니다.

새로운 백업 프로파일 생성에 대한 자세한 내용은 37-3페이지의 백업 프로파일 생성을 참고하십시오.

단계 7 또는 **Comment(코멘트)** 필드에 최대 255자의 영숫자, 스페이스 또는 마침표를 사용한 코멘트를 입력합니다.

팁 코멘트 필드는 페이지의 View Tasks(작업 보기) 섹션에 표시되므로 이를 상대적으로 짧게 유지하십시오.

단계 8 또는, **Email Status To:(전자 메일 상태 전송지)** 필드에 작업 상태 메시지가 전송되기를 원하는 이메일 주소(또는 쉼표로 구분된 여러 전자 메일 주소)를 입력합니다.

상태 메시지를 보내려면 구성된 유효한 이메일 릴레이 서버가 있어야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 32-7페이지의 메일 릴레이 호스트 및 알림 주소 구성을 참고하십시오.

단계 9 **Save(저장)**를 클릭합니다.

작업이 추가됩니다. Task Status(작업 상태) 페이지에서 실행되는 작업 상태를 확인할 수 있습니다(C-1페이지의 장기 작업 상태 보기 참고).

인증서 철회 목록 다운로드 자동화

스케줄러를 사용하여 어플라이언스의 사용자 인증서를 활성화하는 어플라이언스에서 어플라이언스 웹 서버의 CRL(인증서 철회 목록)을 자동으로 새로 고칠 수 있습니다. 로컬 어플라이언스 구성에서 CRL 페칭을 활성화하는 경우 CRL 다운로드 작업이 자동으로 생성되므로 이 절차는 예약된 작업을 열어 빈도를 설정하는 방법에 대해 설명합니다.

팁 이러한 작업을 예약하기 전에 사용자 인증서를 활성화 및 구성하고 CRL 다운로드 URL을 설정해야 합니다. 사용자 인증서 구성에 대한 내용은 33-5페이지의 사용자 인증서 요청을 참고하십시오.

인증서 철회 목록의 다운로드를 자동화하려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

Scheduling(일정 관리) 페이지가 나타납니다.

단계 2 Task Details(작업 세부 정보)에서 **download CRL(CRL 다운로드)** 작업을 찾아 수정 아이콘( )을 클릭합니다.

Edit Task(작업 수정) 페이지가 나타나고, 다운로드 옵션이 표시됩니다.

단계 3 **Once(한 번에)** 또는 **Recurring(반복)** 중에서 CRL 다운로드를 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time(현재 시간)** 필드는 어플라이언스의 현재 시간을 나타냅니다.
- 반복 작업의 경우, 작업의 인스턴스 간 간격을 설정하는 여러 옵션이 있습니다. 자세한 내용은 31-2페이지의 반복 작업 구성을 참고하십시오.

단계 4 또는 **Comment(코멘트)** 필드에 최대 255자의 영숫자, 스페이스 또는 마침표를 사용한 코멘트를 입력합니다.

팁 코멘트 필드는 페이지의 View Tasks(작업 보기) 섹션에 표시되므로 이를 상대적으로 짧게 유지하십시오.

단계 5 또는, **Email Status To:(전자 메일 상태 전송지)** 필드에 작업 상태 메시지가 전송되기를 원하는 이메일 주소(또는 쉼표로 구분된 여러 전자 메일 주소)를 입력합니다.

상태 메시지를 보내려면 ASA FirePOWER 모듈에 구성된 유효한 이메일 릴레이 서버가 있어야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 32-7페이지의 메일 릴레이 호스트 및 알림 주소 구성을 참고하십시오.

단계 6 **Save(저장)**를 클릭합니다.

작업이 추가됩니다. Task Status(작업 상태) 페이지에서 실행되는 작업 상태를 확인할 수 있습니다 (C-1페이지의 장기 작업 상태 보기 참고).

침입 정책 적용의 자동화

라이센스: 보호

ASA FirePOWER 모듈에 침입 정책 적용을 대기시킬 수 있습니다. 이 작업은 작업 실행 시 침입 정책을 참조하는 액세스 제어 정책이 ASA FirePOWER 모듈에 적용된 경우에만 침입 정책을 적용합니다. 그렇지 않으면, 완료 전에 작업이 중단됩니다.

이 작업을 예약하기 전에 침입 정책을 액세스 제어 정책과 연결하고 디바이스에 액세스 제어 정책을 적용해야 합니다. 10-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어를 참고하십시오.

정책 적용을 대기시키려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

이번 달의 일정 달력 페이지가 나타납니다.

단계 2 **Add Task(작업 추가)**를 클릭합니다.

새 작업(New Task) 페이지가 표시됩니다.

단계 3 **Job Type(작업 유형)** 목록에서 **Queue Intrusion Policy Apply(침입 정책 적용 대기)**를 선택합니다.

페이지가 다시 로드되어 정책 적용 대기 옵션이 표시됩니다.

단계 4 **Once(한 번에)** 또는 **Recurring(반복)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time(현재 시간)** 필드는 ASA FirePOWER 모듈에서 현재 시간을 나타냅니다.
- 반복 작업의 경우, 작업의 인스턴스 간 간격을 설정하는 여러 옵션이 있습니다. 자세한 내용은 31-2페이지의 반복 작업 구성을 참고하십시오.

단계 5 **Job Name(작업 이름)** 필드에 최대 255자의 영숫자, 스페이스 또는 대시를 사용한 이름을 입력합니다.

단계 6 **Intrusion Policy(침입 정책)** 필드에는 다음과 같은 옵션이 있습니다.

- ASA FirePOWER 모듈에 적용할 침입 정책을 선택합니다.
- **All intrusion policies(모든 침입 정책)**를 선택하여 ASA FirePOWER 모듈에서 선택한 디바이스에 이미 적용된 모든 침입 정책을 적용합니다.

단계 7 또는 **Comment(코멘트)** 필드에 최대 255자의 영숫자, 스페이스 또는 마침표를 사용한 코멘트를 입력합니다.

팁 코멘트 필드는 일정 달력 페이지 하단의 Tasks Details(작업 세부 정보) 섹션에 표시되므로, 코멘트의 크기를 제한해야 합니다.

단계 8 또는, **Email Status To:(전자 메일 상태 전송지)** 필드에 작업 상태 메시지가 전송되기를 원하는 이메일 주소(또는 쉼표로 구분된 여러 전자 메일 주소)를 입력합니다.

상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 32-7페이지의 메일 릴레이 호스트 및 알림 주소 구성을 참고하십시오.

단계 9 **Save(저장)**를 클릭합니다.

작업이 추가됩니다. 달력 페이지의 Task Details(작업 세부 정보) 섹션에서 실행되는 작업의 상태를 확인할 수 있습니다(C-1페이지의 장기 작업 상태 보기 참고).

단계 10 저장된 작업을 수정하려면 일정 달력 페이지에 나타나는 어디에서나 작업을 클릭합니다.

Task Details(작업 세부 정보) 섹션이 페이지 하단에 나타납니다. 변경하려면, 수정 아이콘( )을 클릭합니다.

위치 정보 데이터베이스 업데이트 자동화

라이센스: 모두

스케줄러를 사용하여 반복되는 위치 정보 데이터베이스(GeoDB) 업데이트를 자동화할 수 있습니다. 반복되는 GeoDB 업데이트는 일주일마다(매주) 한 번씩 실행됩니다. 매주 업데이트가 발생하는 시간을 구성할 수 있습니다. GeoDB 업데이트에 대한 자세한 내용은 35-20페이지의 위치 정보 데이터베이스 업데이트를 참고하십시오.

위치 정보 데이터베이스 업데이트를 자동화하려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택합니다.

Product Updates(제품 업데이트) 페이지가 나타납니다.

단계 2 **Geolocation Updates(위치 정보 업데이트)** 탭을 클릭합니다.

Geolocation Updates(위치 정보 업데이트) 페이지가 나타납니다.

단계 3 **Recurring Geolocation Updates(반복되는 위치 정보 업데이트)**에서 **Enable Recurring Weekly Updates(반복되는 주간 업데이트 활성화)** 확인 상자를 선택합니다.

Update Start Time(업데이트 시작 시간) 필드가 나타납니다.

단계 4 **Update Start Time(업데이트 시작 시간)** 필드에서 매주 GeoDB 업데이트가 발생하기를 원하는 시간 및 요일을 지정합니다.

단계 5 **Save(저장)**를 클릭합니다.

작업이 추가됩니다. Task Status(작업 상태) 페이지에서 실행되는 작업 상태를 확인할 수 있습니다(C-1페이지의 장기 작업 상태 보기 참고).

소프트웨어 업데이트 자동화

대부분의 패치 및 기능 릴리스를 ASA FirePOWER 모듈에 자동으로 다운로드 및 적용할 수 있습니다.

참고 다음과 같은 두 상황에서는 업데이트를 수동으로 업로드하고 설치해야 합니다. 먼저, 중요한 업데이트를 ASA FirePOWER 모듈에 예약할 수 없는 상황입니다. 다음으로, Support(지원팀) 사이트에 액세스할 수 없는 어플라이언스의 업데이트 또는 해당 어플라이언스로부터의 푸시를 예약할 수 없는 경우입니다. ASA FirePOWER 모듈의 수동 업데이트에 대한 자세한 내용은 35-1페이지의 ASA FirePOWER 모듈 소프트웨어 업데이트를 참고하십시오.

이 프로세스를 세부적으로 제어하려면 업데이트가 해제되었음을 확인한 후 **Once(한 번에)** 옵션을 사용하여 오프 피크 시간 동안 업데이트를 다운로드하고 설치할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

소프트웨어 다운로드 자동화

Cisco에서 최신 소프트웨어 업데이트를 자동으로 다운로드하는 예약된 작업을 생성할 수 있습니다. 이 작업을 사용하여 수동 설치하려는 업데이트의 다운로드를 예약할 수 있습니다.

소프트웨어 업데이트 다운로드를 자동화하려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

Scheduling(일정 관리) 페이지가 나타납니다.

단계 2 **Add Task(작업 추가)**를 클릭합니다.

새 작업(New Task) 페이지가 표시됩니다.

단계 3 **Job Type(작업 유형)** 목록에서 **Download Latest Update(최신 업데이트 다운로드)**를 선택합니다.

새 업무(New Task) 페이지가 다시 로드되어 업데이트 옵션이 표시됩니다.

단계 4 **Once(한 번에)** 또는 **Recurring(반복)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time(현재 시간)** 필드는 어플라이언스의 현재 시간을 나타냅니다.
- 반복 작업의 경우, 작업의 인스턴스 간 간격을 설정하는 여러 옵션이 있습니다. 자세한 내용은 31-2페이지의 반복 작업 구성을 참고하십시오.

단계 5 **Job Name(작업 이름)** 필드에 최대 255자의 영숫자, 스페이스 또는 대시를 사용한 이름을 입력합니다.

단계 6 **Update Items(항목 업데이트)** 섹션에서 **Software(소프트웨어)**를 선택합니다.

단계 7 또는 **Comment(코멘트)** 필드에 최대 255자의 영숫자, 스페이스 또는 마침표를 사용한 코멘트를 입력합니다.

팁 코멘트 필드는 페이지의 View Tasks(작업 보기) 섹션에 표시되므로 이를 상대적으로 짧게 유지하십시오.

단계 8 또는, **Email Status To:(전자 메일 상태 전송지)** 필드에 작업 상태 메시지가 전송되기를 원하는 이메일 주소(또는 쉼표로 구분된 여러 전자 메일 주소)를 입력합니다.

상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 32-7페이지의 메일 릴레이 호스트 및 알림 주소 구성을 참고하십시오.

단계 9 **Save(저장)**를 클릭합니다.

작업이 추가됩니다. Task Status(작업 상태) 페이지에서 실행되는 작업 상태를 확인할 수 있습니다(C-1페이지의 장기 작업 상태 보기 참고).

소프트웨어 설치 자동화

주의 설치되고 있는 업데이트에 따라, 소프트웨어가 설치된 후 어플라이언스가 재부팅될 수 있습니다.

소프트웨어 설치 작업을 예약하려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

Scheduling(일정 관리) 페이지가 나타납니다.

단계 2 **Add Task(작업 추가)**를 클릭합니다.

새 작업(New Task) 페이지가 표시됩니다.

단계 3 **Job Type(작업 유형)** 목록에서 **Install Latest Update(최신 업데이트 설치)**를 선택합니다.

페이지가 다시 로드되어 업데이트 설치 옵션이 표시됩니다.

단계 4 **Once(한 번에)** 또는 **Recurring(반복)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time(현재 시간)** 필드는 어플라이언스의 현재 시간을 나타냅니다.
- 반복 작업의 경우, 작업의 인스턴스 간 간격을 설정하는 여러 옵션이 있습니다. 자세한 내용은 31-2페이지의 반복 작업 구성을 참고하십시오.

단계 5 **Job Name(작업 이름)** 필드에 최대 255자의 영숫자, 스페이스 또는 대시를 사용한 이름을 입력합니다.

단계 6 또는 **Comment(코멘트)** 필드에 최대 255자의 영숫자, 스페이스 또는 마침표를 사용한 코멘트를 입력합니다.

팁 코멘트 필드는 페이지의 View Tasks(작업 보기) 섹션에 표시되므로 이를 상대적으로 짧게 유지하십시오.

단계 7 또는, **Email Status To:(전자 메일 상태 전송지)** 필드에 작업 상태 메시지가 전송되기를 원하는 이메일 주소(또는 쉼표로 구분된 여러 전자 메일 주소)를 입력합니다.

상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 32-7페이지의 메일 릴레이 호스트 및 알림 주소 구성을 참고하십시오.

단계 8 **Save(저장)**를 클릭합니다.

작업이 추가됩니다. Task Status(작업 상태) 페이지에서 실행되는 작업 상태를 확인할 수 있습니다 (C-1페이지의 장기 작업 상태 보기 참고).

URL 필터링 업데이트 자동화

라이센스: URL 필터링

스케줄러를 사용하여 종합적 보안 인텔리전스 클라우드에서 URL 필터링 데이터의 업데이트를 자동화할 수 있습니다. URL 필터링 업데이트 작업이 성공하려면 다음 조건이 필요합니다.

- ASA FirePOWER 모듈이 인터넷에 접속할 수 있어야 합니다. 그렇지 않으면 클라우드에 연결할 수 없습니다.
- 33-6페이지의 클라우드 커뮤니케이션 활성화에 설명된 대로 URL 필터링을 활성화해야 합니다.

URL 필터링을 활성화하면 자동 업데이트 또한 활성화할 수 있다는 점에 유의하십시오. 이는 ASA FirePOWER 모듈이 URL 필터링 데이터 업데이트를 위해 30분마다 클라우드에 강제로 연결되도록 합니다. 자동 업데이트를 활성화한 경우, URL 필터링 데이터를 업데이트하는 예약된 작업을 생성하지 **마십시오**.

일일 업데이트 양이 적다고 생각될 수도 있으나, 마지막 업데이트 이후 5일 이상 경과하면 새로운 URL 필터링 데이터를 다운로드하는 데 대역폭에 따라 20분 이상이 소요될 수 있습니다. 그런 다음 업데이트 자체를 수행하는 데 30분이 걸릴 수 있습니다.

URL 필터링 데이터 작업을 자동화하려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

Scheduling(일정 관리) 페이지가 나타납니다.

단계 2 **Add Task(작업 추가)**를 클릭합니다.

새 작업(New Task) 페이지가 표시됩니다.

단계 3 **Job Type(작업 유형)** 목록에서 **Update URL Filtering Database(URL 필터링 데이터베이스 업데이트)**를 선택합니다.

페이지가 다시 로드되어 URL 필터링 업데이트 옵션이 표시됩니다.

단계 4 **Once(한 번에)** 또는 **Recurring(반복)** 중에서 업데이트를 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time(현재 시간)** 필드는 어플라이언스의 현재 시간을 나타냅니다.
- 반복 작업의 경우, 작업의 인스턴스 간 간격을 설정하는 여러 옵션이 있습니다. 자세한 내용은 31-2페이지의 반복 작업 구성을 참고하십시오.

단계 5 **Job Name(작업 이름)** 필드에 최대 255자의 영숫자, 스페이스 또는 대시를 사용한 이름을 입력합니다.

단계 6 또는 **Comment(코멘트)** 필드에 최대 255자의 영숫자, 스페이스 또는 마침표를 사용한 코멘트를 입력합니다.

팁 코멘트 필드는 페이지의 View Tasks(작업 보기) 섹션에 표시되므로 이를 상대적으로 짧게 유지하십시오.

단계 7 또는, **Email Status To(전자 메일 상태 전송지)** 필드에 작업 상태 메시지가 전송되기를 원하는 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다.

상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 32-7페이지의 메일 릴레이 호스트 및 알림 주소 구성을 참고하십시오.

단계 8 **Save(저장)**를 클릭합니다.

작업이 추가됩니다. Task Status(작업 상태) 페이지에서 실행되는 작업 상태를 확인할 수 있습니다 (C-1페이지의 장기 작업 상태 보기 참고).

작업 보기

예약된 작업을 추가한 후, 이들을 확인하고 상태를 평가할 수 있습니다. 페이지의 View Options(보기 옵션) 섹션에서는 예약된 작업의 달력 및 목록을 사용하여 예약된 작업을 확인할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 31-10페이지의 달력 사용
- 31-10페이지의 작업 목록 사용

달력 사용

Calendar(달력) 보기 옵션을 사용하면 날짜별로 발생하는 예약된 작업을 확인할 수 있습니다.

달력을 사용하여 예약된 작업을 보려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

Scheduling(일정 관리) 페이지가 나타납니다.

단계 2 캘린더 보기를 사용하여 다음 작업을 수행할 수 있습니다.

- 이전 연도로 이동하려면 이중 왼쪽 화살표 아이콘(≪)을 클릭합니다.
- 이전 달로 이동하려면 단일 왼쪽 화살표 아이콘(‹)을 클릭합니다.
- 다음 달로 이동하려면 단일 오른쪽 화살표 아이콘(›)을 클릭합니다.
- 다음 연도로 이동하려면 이중 오른쪽 화살표 아이콘(≫)을 클릭합니다.
- 이번 달과 연도로 돌아가려면 **Today(오늘)**를 클릭합니다.
- 새로운 작업을 예약하려면 **Add Task(작업 추가)**를 클릭합니다.
- 달력 아래의 작업 목록 표에서 특정 날짜에 예약된 모든 작업을 보려면 날짜를 클릭합니다.
- 달력 아래의 작업 목록 표에서 작업을 확인하려면 날짜에서 특정 작업을 클릭합니다.

참고 작업 목록 사용에 대한 자세한 내용은 작업 목록 사용을 참고하십시오.

작업 목록 사용

Task List(작업 목록)에는 상태와 함께 작업 목록이 표시됩니다. 달력을 열면 일정 아래에 작업 목록이 나타납니다. 또한, 달력에서 날짜 또는 작업을 선택하여 작업 목록에 액세스할 수 있습니다. 자세한 내용은 31-10페이지의 달력 사용을 참고하십시오.

표 31-1 작업 목록 열

열	설명
이름	예약된 작업의 이름 및 관련 코멘트를 표시합니다.
유형	예약된 작업의 유형을 표시합니다.
시작 시간	예약된 시작 날짜 및 시간을 표시합니다.
빈도	작업이 실행되는 빈도를 표시합니다.
상태	예약된 작업의 현재 상황을 설명합니다. • 체크 표시 아이콘( )은 작업이 성공적으로 실행되었음을 나타냅니다. • 물음표 아이콘( )은 작업이 알 수 없는 상태임을 나타냅니다. • 느낌표 아이콘( )은 작업이 실패했음을 나타냅니다.
생성자	예약된 작업을 생성한 사용자의 이름을 표시합니다.
수정	예약된 작업을 수정합니다.
삭제	예약된 작업을 삭제합니다.

예약된 작업 수정

이전에 생성한 예약된 작업을 수정할 수 있습니다. 이 기능은 매개 변수가 올바른지 확인하기 위해 예약된 작업을 한 번 테스트하려는 경우에 특히 유용합니다. 나중에, 작업이 성공적으로 완료된 후 이를 반복 작업으로 변경할 수 있습니다.

기존 예약된 작업을 수정하려면 다음을 수행합니다.

단계 1 **System(시스템) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

Scheduling(일정 관리) 페이지가 나타납니다.

단계 2 수정할 작업이나 작업이 나타나는 날짜를 클릭합니다.

선택된 작업을 포함하는 Task Details(작업 세부 정보) 표가 나타납니다.

단계 3 표에서 수정할 작업을 찾아 수정 아이콘( )을 클릭합니다.

Edit Task(작업 수정) 페이지가 나타나고, 선택한 작업의 세부 정보가 표시됩니다.

단계 4 시작 시간, 작업 이름, 코멘트, 그리고 작업 실행 빈도(한 번에 또는 반복)를 포함하여, 필요에 맞게 작업을 수정합니다. 작업 유형은 변경할 수 없습니다.

나머지 옵션은 수정 중인 작업에 따라 결정됩니다. 자세한 내용은 다음 섹션을 참고하십시오.

- 31-3페이지의 백업 작업 자동화
- 31-4페이지의 인증서 철회 목록 다운로드 자동화
- 31-6페이지의 소프트웨어 업데이트 자동화
- 31-9페이지의 URL 필터링 업데이트 자동화

단계 5 **Save(저장)**를 클릭하여 수정 사항을 저장합니다.

변경 사항이 저장되고 Scheduling(일정 관리) 페이지가 다시 나타납니다.

예약된 작업 삭제

Schedule View(일정 보기) 페이지에서 수행할 수 있는 2가지 유형의 삭제가 있습니다. 아직 실행되지 않은 특정 일회성 작업을 삭제하거나 반복 작업의 각 인스턴스를 삭제할 수 있습니다. 반복 작업의 인스턴스를 삭제할 경우, 작업의 모든 인스턴스가 삭제됩니다. 한 번 실행하도록 예약된 작업을 삭제할 경우, 해당 작업만 삭제됩니다.

다음 섹션에서는 작업을 삭제하는 방법에 대해 설명합니다.

- 작업의 모든 인스턴스를 삭제하려면 31-12페이지의 반복 작업 삭제를 참고하십시오.
- 작업의 단일 인스턴스를 삭제하려면 31-12페이지의 일회성 작업 삭제를 참고하십시오.

반복 작업 삭제

반복 작업의 인스턴스 1개를 삭제하면, 해당 작업의 모든 인스턴스가 자동으로 삭제됩니다.

반복 작업을 삭제하려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

Scheduling(일정 관리) 페이지가 나타납니다.

단계 2 달력에서 삭제하려는 반복 작업의 인스턴스를 선택합니다.

페이지가 다시 로드되어 달력 아래에 작업 표가 나타납니다.

단계 3 표에서 삭제하려는 반복 작업의 인스턴스를 찾아 수정 아이콘( )을 클릭합니다.

반복 작업의 모든 인스턴스가 삭제됩니다.

일회성 작업 삭제

일회성 예약 작업을 삭제하거나 작업 목록을 사용하는 이전에 실행된 예약 작업의 레코드를 삭제할 수 있습니다.

단일 작업을 삭제하려면, 또는 이미 실행한 경우 작업 레코드를 삭제하려면 다음을 수행합니다.

단계 1 ASDM에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Scheduling(일정 관리)**을 선택합니다.

Scheduling(일정 관리) 페이지가 나타납니다.

단계 2 삭제할 작업이나 작업이 나타나는 날짜를 클릭합니다.

선택된 작업이 포함된 표가 나타납니다.

단계 3 표에서 삭제할 작업을 찾아 수정 아이콘( )을 클릭합니다.

선택한 작업의 인스턴스가 삭제됩니다.

시스템 정책 관리

시스템 정책을 통해 ASA FirePOWER 모듈에서 다음을 관리할 수 있습니다.

- 감사 로그 설정
- 메일 릴레이 호스트 및 알림 주소
- SNMP 폴링 설정
- STIG 규정 준수

자세한 내용은 다음 섹션을 참고하십시오.

시스템 정책 생성

라이센스: 모두

시스템 정책을 생성하는 경우, 이름 및 설명을 할당합니다. 다음으로, 정책의 다양한 측면을 구성합니다. 이들 각각은 자체 섹션에서 설명됩니다.

새로운 정책을 생성하는 대신 다른 ASA FirePOWER 모듈에서 시스템 정책을 내보낸 다음 ASA FirePOWER 모듈로 가져올 수 있습니다. 그런 다음 가져온 정책을 적용하기 전에 필요에 맞게 수정할 수 있습니다. 자세한 내용은 B-1페이지의 구성 가져오기 및 내보내기를 참고하십시오.

시스템 정책을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > System Policy(시스템 정책)**를 선택합니다.

System Policy(시스템 정책) 페이지가 나타납니다.

단계 2 **Create Policy(정책 생성)**를 클릭합니다.

Create Policy(정책 생성) 페이지가 나타납니다.

단계 3 드롭다운 목록에서 새 시스템 정책의 템플릿으로 사용할 기존 정책을 선택합니다.

단계 4 **New Policy Name(새 정책 이름)** 필드에 새 정책의 이름을 입력합니다.

단계 5 **New Policy Description(새 정책 설명)** 필드에 새 정책에 대한 설명을 입력합니다.

단계 6 **Create(생성)**를 클릭합니다.

시스템 정책이 저장되고 Edit System Policy(시스템 정책 수정) 페이지가 나타납니다. 시스템 정책의 각 측면 구성에 대한 내용은 다음 섹션 중 하나를 참고하십시오.

- 32-5페이지의 감사 로그 설정 구성
- 32-7페이지의 메일 릴레이 호스트 및 알림 주소 구성
- 32-8페이지의 SNMP 폴링 구성
- 32-10페이지의 STIG 준수 활성화

시스템 정책 수정

라이센스: 모두

기존 시스템 정책을 수정할 수 있습니다. ASA FirePOWER 모듈에 현재 적용된 시스템 정책을 수정할 경우, 변경 내용을 저장한 후 정책을 재적용하십시오. 자세한 내용은 32-3페이지의 시스템 정책 적용을 참고하십시오.

기존 시스템 정책을 수정하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > System Policy(시스템 정책)**를 선택합니다.

System Policy(시스템 정책) 페이지가 나타나며, 여기에는 기존 시스템 정책의 목록이 포함되어 있습니다.

단계 2 수정하려는 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Policy(정책 수정) 페이지가 나타납니다. 정책 이름 및 정책 설명을 변경할 수 있습니다. 시스템 정책의 각 측면 구성에 대한 내용은 다음 섹션 중 하나를 참고하십시오.

- 32-5페이지의 감사 로그 설정 구성
- 32-7페이지의 메일 릴레이 호스트 및 알림 주소 구성
- 32-8페이지의 SNMP 폴링 구성
- 32-10페이지의 STIG 준수 활성화

참고 ASA FirePOWER 모듈에 적용된 시스템 정책을 수정할 경우, 완료 시 업데이트된 정책을 재적용하십시오. 32-3페이지의 시스템 정책 적용을 참고하십시오.

단계 3 변경 사항을 저장하려면 **Save Policy and Exit(정책 저장 및 종료)**를 클릭합니다. 변경 사항이 저장되며, System Policy(시스템 정책) 페이지가 나타납니다.

시스템 정책 적용

라이센스: 모두

시스템 정책을 ASA FirePOWER 모듈에 적용할 수 있습니다. 시스템 정책이 이미 적용된 경우, 변경 사항은 재적용할 때까지 적용되지 않습니다.

시스템 정책을 적용하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > System Policy(시스템 정책)**를 선택합니다.

System Policy(시스템 정책) 페이지가 나타납니다.

단계 2 적용하려는 시스템 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

단계 3 **Apply(적용)**를 클릭합니다.

System Policy(시스템 정책) 페이지가 나타납니다. 메시지가 시스템 정책이 적용된 상태를 나타냅니다.

시스템 정책 삭제

라이센스: 모두

시스템 정책이 사용 중인 경우에도 이를 삭제할 수 있습니다. 정책이 여전히 사용 중인 경우, 새로운 정책이 적용될 때까지 사용됩니다. 기본 시스템 정책은 삭제할 수 없습니다.

시스템 정책을 삭제하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > System Policy(시스템 정책)**를 선택합니다.

System Policy(시스템 정책) 페이지가 나타납니다.

단계 2 삭제하려는 시스템 정책 옆에 있는 삭제 아이콘( )을 클릭합니다. 정책을 삭제하려면 **OK(확인)**를 클릭합니다.

System Policy(시스템 정책) 페이지가 나타납니다. 정책 삭제를 확인하는 팝업 메시지가 표시됩니다.

시스템 정책 구성

라이센스: 모두

다양한 시스템 정책 설정을 구성할 수 있습니다. 시스템 정책의 각 측면 구성에 대한 내용은 다음 섹션 중 하나를 참고하십시오.

사용자 어플라이언스의 액세스 목록 구성

라이센스: 모두

Access List(액세스 목록) 페이지를 통해 특정 포트의 어플라이언스에 액세스할 컴퓨터를 제어할 수 있습니다. 기본적으로, 웹 인터페이스에 액세스하는 데 사용되는 포트 443(Hypertext Transfer Protocol Secure, 또는 HTTPS)과 명령줄에 액세스하는 데 사용되는 포트 22(Secure Shell, 또는 SSH)는 모든 IP 주소에서 활성화됩니다. 또한 포트 161을 통해 SNMP 액세스를 추가할 수 있습니다. SNMP 정보의 폴링에 사용할 모든 컴퓨터에 SNMP 액세스를 추가해야 한다는 점에 유의하십시오.

주의 기본적으로, 어플라이언스에 대한 액세스는 제한되지 **않습니다**. 어플라이언스를 더 안전한 환경에서 작동하려면 특정 IP 주소의 어플라이언스에 액세스를 추가한 후 기본 any 옵션을 삭제하는 것을 고려하십시오.

액세스 목록은 시스템 정책의 일부입니다. 새 시스템 정책을 생성하거나 기존 시스템 정책을 수정하여 액세스 목록을 지정할 수 있습니다. 어느 경우에나, 액세스 목록은 시스템 정책을 적용할 때까지 적용되지 않습니다.

이 액세스 목록은 외부 데이터베이스 액세스를 제어하지도 않는다는 점에 유의하십시오. 외부 데이터베이스 액세스 목록에 대한 자세한 내용은 33-6페이지의 클라우드 커뮤니케이션 활성화를 참고하십시오.

액세스 목록을 구성하려면 다음을 수행합니다.

액세스: Admin(관리)

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > System Policy(시스템 정책)**를 선택합니다.

System Policy(시스템 정책) 페이지가 나타납니다.

단계 2 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책의 액세스 목록을 수정하려면, 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 새 시스템 정책의 일부로 액세스 목록을 구성하려면, **Create Policy(정책 생성)**를 클릭합니다.

  32-1페이지의 시스템 정책 생성에 설명된 대로 시스템 정책의 이름 및 설명을 입력하고, **Save(저장)**를 클릭합니다.

어느 경우에나, Access List(액세스 목록) 페이지가 나타납니다.

단계 3 또는, 현재 설정 중 하나를 삭제하려면, 삭제 아이콘( )을 클릭합니다.

설정이 제거됩니다.

주의 어플라이언스 인터페이스에 연결하기 위해 현재 사용하고 있는 IP 주소에 대한 액세스를 삭제할 경우, `"IP=any port=443"`에 대한 항목이 없으며, 정책을 적용할 때 시스템에 대한 액세스 권한을 잃게 됩니다.

단계 4 또는, 하나 이상의 IP 주소에 대한 액세스를 추가하려면 **Add Rules(규칙 추가)**를 클릭합니다.

Add IP Address(IP 주소 추가) 페이지가 나타납니다.

단계 5 **IP Address(IP 주소)** 필드에서 추가하려는 IP 주소에 따라 다음 옵션이 있습니다.

- 정확한 IP 주소(예를 들어, 192.168.1.101)
- CIDR 코멘트(예: 192.168.1.1/24)을 사용하는 IP 주소 블록

  FireSIGHT 시스템에서 CIDR를 사용하는 방법에 대한 내용은 1-4페이지의 IP 주소 규칙을 참고하십시오.
- `any(모두)`(IP 주소 지정)

단계 6 **SSH**, **HTTPS**, **SNMP** 또는 이 옵션의 조합을 선택하여 이 IP 주소에 활성화할 포트를 지정합니다.

단계 7 **Add(추가)**를 클릭합니다.

Access List(액세스 목록) 페이지가 다시 나타나며, 사용자의 변경 내용이 반영됩니다.

단계 8 **Save Policy and Exit(정책 저장 및 종료)**를 클릭합니다.

시스템 정책이 업데이트됩니다. 변경 내용은 시스템 정책을 적용할 때까지 적용되지 않습니다. 자세한 내용은 32-3페이지의 시스템 정책 적용을 참고하십시오.

감사 로그 설정 구성

라이센스: 모두

ASA FirePOWER 모듈이 외부 호스트로 감사 로그를 스트리밍하도록 시스템 정책을 구성할 수 있습니다.

참고 외부 호스트가 작동하며 감사 로그를 보내는 ASA FirePOWER 모듈에서 액세스할 수 있어야 합니다.

발신 호스트 이름은 전송되는 정보의 일부입니다. 기능, 심각도 및 선택적 태그로 감사 로그 스트림을 더 자세히 확인할 수 있습니다. ASA FirePOWER 모듈은 시스템 정책을 적용할 때까지 감사 로그를 전송하지 않습니다.

활성화된 이 기능을 통해 정책을 적용하고 대상 호스트가 감사 로그를 수락하도록 구성되면 syslog 메시지가 전송됩니다. 다음은 출력 구조의 예입니다.

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

로컬 날짜, 시간 및 호스트 이름이 괄호로 묶인 선택적 태그 앞에 오는 경우, 그리고 발신 디바이스 이름이 감사 로그 메시지 앞에 오는 경우

예를 들면 다음과 같습니다.

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3000: admin@10.1.1.2, Operations > Monitoring, Page
View
```

감사 로그 설정을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > System Policy(시스템 정책)**를 선택합니다.

System Policy(시스템 정책) 페이지가 나타납니다.

단계 2 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책의 감사 로그 설정을 수정하려면, 시스템 정책 옆에 있는 수정아이콘()을 클릭합니다.
- 새 시스템 정책의 일부로 감사 로그 설정을 구성하려면 **Create Policy(정책 생성)**를 클릭합니다.

  32-1페이지의 시스템 정책 생성에 설명된 대로 시스템 정책의 이름 및 설명을 입력하고, **Save(저장)**를 클릭합니다.

단계 3 **Audit Log Settings(감사 로그 설정)**를 클릭합니다.

Audit Log Settings(감사 로그 설정) 페이지가 나타납니다.

단계 4 **Send Audit Log to Syslog(Syslog에 감사 로그 전송)** 드롭다운 메뉴에서 **Enabled(활성화)**를 선택합니다. (기본 설정은 **Disabled(비활성화)**입니다.)

단계 5 IP 주소를 사용하여 감사 정보에 대한 대상 호스트를 지정하거나 **Host(호스트)** 필드에 호스트의 FQDN(정규화된 도메인 이름)을 지정합니다. 기본 포트(514)가 사용됩니다.

주의 감사 로그를 수신하도록 구성한 컴퓨터가 원격 메시지를 수락하도록 설정되지 않은 경우, 호스트에서 감사 로그를 허용하지 않습니다.

단계 6 **Facility(기능)** 필드에서 syslog 기능을 선택합니다.

단계 7 **Severity(심각도)** 필드에서 심각도를 선택합니다.

단계 8 또는, **Tag(태그)**(선택 사항) 필드에 참조 태그를 삽입합니다.

단계 9 외부 HTTP 서버에 정기 감사 로그 업데이트를 전송하려면 **Enabled(활성화)**를 **Send Audit Log to HTTP Server(HTTP 서버에 감사 로그 전송)** 드롭다운 메뉴에서 선택합니다. 기본 설정은 **Disabled(비활성화)**입니다.

단계 10 **URL to Post Audit(사후 감사 URL)** 필드에서 감사 정보를 전송할 URL을 지정합니다. 다음과 같이 나열된 대로 HPPT POST 변수를 기대하는 listener 프로그램에 해당하는 URL을 입력해야 합니다.

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`
- `result`
- `time`
- `tag`(위와 같이 정의된 경우)

주의 암호화된 게시물을 허용하려면, HTTPS URL을 사용해야 합니다. 외부 URL에 감사 정보를 보내면 시스템 성능에 영향을 미칠 수 있음에 유의하십시오.

단계 11 **Save Policy and Exit(정책 저장 및 종료)**를 클릭합니다.

시스템 정책이 업데이트됩니다. 에 시스템 정책을 적용할 때까지 변경 사항은 적용되지 않습니다. 자세한 내용은 32-3페이지의 시스템 정책 적용을 참고하십시오.

메일 릴레이 호스트 및 알림 주소 구성

라이센스: 모두

다음을 수행하려는 경우 메일 호스트를 구성해야 합니다.

- 이벤트 기반의 보고서 이메일 보내기
- 예약된 작업의 상태 보고서 이메일 보내기
- 변경 조정 보고서 이메일 보내기
- 알림을 잘라내는 데이터 이메일 보내기
- 침입 이벤트 경고를 받도록 이메일 사용하기

어플라이언스와 메일 릴레이 호스트 간 통신을 위한 암호화 방법을 선택할 수 있고 필요한 경우 메일 서버의 인증 자격 증명을 제공할 수 있습니다. 설정을 구성한 후, 제공된 설정을 사용하여 어플라이언스와 메일 서버 간 연결을 테스트할 수 있습니다.

메일 릴레이 호스트를 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > System Policy(시스템 정책)**를 선택합니다.

System Policy(시스템 정책) 페이지가 나타납니다.

단계 2 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책의 이메일 설정을 수정하려면, 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 새 시스템 정책의 일부로 이메일 설정을 구성하려면, **Create Policy(정책 생성)**를 클릭합니다.

  32-1페이지의 시스템 정책 생성에 설명된 대로 시스템 정책의 이름 및 설명을 입력하고, **Save(저장)**를 클릭합니다.

단계 3 **Email Notification(이메일 알림)**을 클릭합니다.

Configure Email Notification(이메일 알림 구성) 페이지가 나타납니다.

단계 4 **Mail Relay Host(메일 릴레이 호스트)** 필드에서 사용할 메일 서버의 호스트 이름 또는 IP 주소를 입력합니다.

참고 입력한 메일 호스트는 어플라이언스에서 접속할 수 있어야 합니다.

단계 5 **Port Number(포트 번호)** 필드에 이메일 서버에서 사용할 포트 번호를 입력합니다. 암호화를 사용하지 않을 때 일반적인 포트는 25를 포함하고, SSLv3를 사용할 때 465를 포함하며, TLS를 사용하면 587을 포함합니다.

단계 6 암호화 방법을 선택하려면 다음 옵션을 사용할 수 있습니다.

- 전송 레이어 보안을 사용하여 어플라이언스와 메일 서버 간 통신을 암호화하려면, **Encryption Method(암호화 방법)** 드롭다운 목록에서 **TLS**를 선택합니다.
- Secure Socket Layer을 사용하여 어플라이언스와 메일 서버 간 통신을 암호화하려면, **Encryption Method(암호화 방법)** 드롭다운 목록에서 **SSLv3**를 선택합니다.
- 어플라이언스와 메일 서버 간 비암호화된 통신을 허용하려면, **Encryption Method(암호화 방법)** 드롭다운 목록에서 **None(없음)**을 선택합니다.

어플라이언스와 메일 서버 간 암호화된 통신에는 인증서 유효성 검사가 필요하지 않다는 점을 참고하십시오.

단계 7 어플라이언스에서 보낸 메시지에 대한 소스 이메일 주소로 사용할 유효한 전자 메일 주소를 **From Address(발신 주소)** 필드에 입력합니다.

단계 8 또는, 메일 서버에 연결 시 사용자 이름 및 비밀번호를 제공하려면 **Use Authentication(인증 사용)**을 선택합니다. **Username(사용자 이름)** 필드에 사용자 이름을 입력합니다. **Password(비밀번호)** 필드에 비밀번호를 입력합니다.

단계 9 구성된 메일 서버를 사용하는 테스트 이메일을 전송하려면 **Test Mail Server Settings(메일 서버 설정 테스트)**를 클릭합니다.

테스트의 성공 또는 실패를 나타내는 메시지가 단추 옆에 나타납니다.

단계 10 **Save Policy and Exit(정책 저장 및 종료)**를 클릭합니다.

시스템 정책이 업데이트됩니다. 변경 내용은 시스템 정책을 적용할 때까지 적용되지 않습니다. 자세한 내용은 32-3페이지의 시스템 정책 적용을 참고하십시오.

SNMP 폴링 구성

라이센스: 모두

시스템 정책을 사용하는 어플라이언스의 SNMP(Simple Network Management Protocol) 폴링을 활성화할 수 있습니다. SNMP 기능은 SNMP 프로토콜의 1, 2, 3 버전 사용을 지원합니다.

시스템 정책 SNMP 기능을 활성화한다고 해서 어플라이언스에서 SNMP 트랩을 전송하지 않으며, MIB의 정보를 네트워크 관리 시스템을 통한 폴링에 사용할 수 있도록 지원할 뿐임을 참고하십시오.

참고 어플라이언스 폴링에 사용할 모든 컴퓨터에 SNMP 액세스를 추가해야 합니다. 자세한 내용은 32-4페이지의 사용자 어플라이언스의 액세스 목록 구성을 참고하십시오. SNMP MIB에는 어플라이언스를 공격하는 데 사용할 수 있는 정보가 포함되어 있음을 참고하십시오. Cisco는 MIB를 폴링하는 데 사용되는 특정 호스트에 대한 SNMP 액세스용 액세스 목록을 제한할 것을 권장합니다. Cisco는 또한 SNMPv3를 사용할 것과 네트워크 관리 액세스에 강력한 비밀번호를 사용할 것을 권장합니다.

SNMP 폴링을 구성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > System Policy(시스템 정책)**를 선택합니다.

System Policy(시스템 정책) 페이지가 나타납니다.

단계 2 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책의 SNMP 폴링 설정을 수정하려면, 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 새 시스템 정책의 일부로 SNMP 폴링 설정을 구성하려면, **Create Policy(정책 생성)**를 클릭합니다.

  32-1페이지의 시스템 정책 생성에 설명된 대로 시스템 정책의 이름 및 설명을 입력하고, **Create(생성)**를 클릭합니다.

단계 3 어플라이언스 폴링에 사용할 각 컴퓨터에 SNMP 액세스를 아직 추가하지 않은 경우 지금 추가하십시오. 자세한 내용은 32-4페이지의 사용자 어플라이언스의 액세스 목록 구성을 참고하십시오.

단계 4 **SNMP**를 클릭합니다.

SNMP 페이지가 나타납니다.

단계 5 **SNMP Version(SNMP 버전)** 드롭다운 목록에서 사용하려는 SNMP 버전을 선택합니다.

드롭다운 목록이 사용자가 선택한 버전을 표시합니다.

단계 6 다음 옵션을 이용할 수 있습니다.

- **Version 1(버전 1)** 또는 **Version 2(버전 2)**를 선택한 경우, **Community String(커뮤니티 스트링)** 필드에 SNMP 커뮤니티 이름을 입력합니다. 15 단계로 이동합니다.
- **Version 3(버전 3)**을 선택한 경우, **Add User(사용자 추가)**를 클릭하여 사용자 정의 페이지를 표시합니다.

단계 7 **Username(사용자 이름)** 필드에 사용자 이름을 입력합니다.

단계 8 **Authentication Protocol(인증 프로토콜)**드롭다운 목록에서 인증에 사용할 프로토콜을 선택합니다.

단계 9 **Authentication Password(인증 비밀번호)** 필드에 SNMP 서버와 함께 인증에 필요한 비밀번호를 입력합니다.

단계 10 **Verify Password(비밀번호 확인)** 필드에 인증 비밀번호를 다시 입력합니다. 이는 **Authentication Password(인증 비밀번호)** 필드 바로 아래에 있습니다.

단계 11 **Privacy Protocol(프라이버시 프로토콜)** 목록에서 사용할 프라이버시 프로토콜을 선택하거나, 프라이버시 프로토콜을 사용하지 않으려면 **None(없음)**을 선택합니다.

단계 12 **Privacy Password(프라이버시 비밀번호)** 필드에 SNMP 서버에 필요한 SNMP 프라이버시 키를 입력합니다.

단계 13 **Verify Password(비밀번호 확인)** 필드에 프라이버시 비밀번호를 다시 입력합니다. 이는 **Privacy Password(프라이버시 비밀번호)** 필드 바로 아래에 있습니다.

단계 14 **Add(추가)**를 클릭합니다.

사용자가 추가됩니다. 6~13단계를 반복하여 사용자를 더 추가할 수 있습니다. 사용자를 삭제하려면 삭제 아이콘( )을 클릭합니다.

단계 15 **Save Policy and Exit(정책 저장 및 종료)**를 클릭합니다.

시스템 정책이 업데이트됩니다. 변경 내용은 시스템 정책을 적용할 때까지 적용되지 않습니다. 자세한 내용은 32-3페이지의 시스템 정책 적용을 참고하십시오.

STIG 준수 활성화

라이센스: 모두

미국 연방 정부 내 기구는 경우에 따라 Security Technical Implementation Guides(보안 기술 구현 가이드, STIG)에 정리된 일련의 보안 검사 목록을 준수해야 합니다. STIG Compliance(STIG 준수) 옵션은 미 국방부에서 정한 특정 요구 사항 준수를 지원하기 위한 설정을 활성화합니다.

배포의 모든 ASA FirePOWER 모듈에서 STIG 규정 준수를 활성화하는 경우, 모든 ASA FirePOWER 모듈에서 이를 활성화해야 합니다.

STIG 규정 준수를 활성화해도 적용 가능한 모든 STIG에 대한 엄격한 규정 준수가 보장되지는 않습니다. 이 제품 버전에 이 모드를 사용하는 경우 ASA FirePOWER 모듈 STIG 규정 준수에 대한 자세한 내용을 확인하려면 Support(지원팀)에 문의하여 ASA FirePOWER 모듈 STIG Release Notes(STIG 릴리스 참고 사항)의 사본을 얻을 수 있습니다. 이는 버전 5.4.1용입니다.

STIG 규정 준수를 활성화할 경우, 로컬 셸 액세스 계정의 비밀번호 복잡성 및 보관 규칙이 변경됩니다. 이 설정에 대한 자세한 내용은 STIG Release Notes(STIG 릴리스 참고 사항)를 참고하십시오. 이는 버전 5.4.1용입니다. 또한, STIG 준수 모드에서는 `ssh` 원격 스토리지를 사용할 수 없습니다.

STIG 규정 준수가 활성화된 시스템 정책을 적용하면 어플라이언스가 강제로 재부팅된다는 점에 유의하십시오. STIG가 활성화된 시스템 정책을 STIG가 이미 활성화된 어플라이언스에 적용하는 경우, 어플라이언스는 재부팅되지 않습니다. STIG가 비활성화된 시스템 정책을 STIG가 활성화된 어플라이언스에 적용하는 경우, STIG의 활성화 상태는 유지되고 어플라이언스는 재부팅되지 않습니다.

주의 Support(지원팀)의 도움 없이는 이 설정을 비활성화할 수 없습니다. 또한, 이 설정은 사용자 시스템의 성능에 상당한 영향을 줄 수 있습니다. Cisco는 국방부 보안 요구 사항 준수 이외에는 STIG 준수의 활성화를 권장하지 않습니다.

STIG 규정 준수를 활성화하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > System Policy(시스템 정책)**를 선택합니다.

System Policy(시스템 정책) 페이지가 나타납니다.

단계 2 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책의 시간 설정을 수정하려면, 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 새 시스템 정책의 일부로 시간 설정을 구성하려면, **Create Policy(정책 생성)**를 클릭합니다.

  32-1페이지의 시스템 정책 생성에 설명된 대로 시스템 정책의 이름 및 설명을 입력하고, **Save(저장)**를 클릭합니다.

단계 3 **STIG Compliance(STIG 준수)**를 클릭합니다.

STIG Compliance(STIG 준수) 페이지가 나타납니다.

단계 4 어플라이언스에서 STIG 준수를 *영구적으로* 활성화하려는 경우, **Enable STIG Compliance(STIG 규정 준수 활성화)**를 선택합니다.

주의 STIG 준수가 활성화된 정책을 적용한 후 어플라이언스에서 STIG 준수를 비활성화할 수 없습니다. 규정 준수를 비활성화해야 하는 경우, Support(지원팀)에 문의하십시오.

단계 5 **Save Policy and Exit(정책 저장 및 종료)**를 클릭합니다.

시스템 정책이 업데이트됩니다. 변경 내용은 시스템 정책을 적용할 때까지 적용되지 않습니다. 자세한 내용은 32-3페이지의 시스템 정책 적용을 참고하십시오.

어플라이언스에 STIG 규정 준수를 활성화하는 시스템 정책을 적용하면 어플라이언스가 재부팅된다는 점에 유의하십시오. STIG가 활성화된 시스템 정책을 STIG가 이미 활성화된 어플라이언스에 적용하는 경우, 어플라이언스는 재부팅되지 않는다는 점에 유의하십시오.

ASA FirePOWER 모듈 설정 구성

다음 표는 ASA FirePOWER 모듈의 로컬 구성을 요약합니다.

표 33-1 로컬 구성 옵션

옵션	설명	자세한 내용은 다음을 참고하십시오.
정보	어플라이언스에 대한 현재 정보를 볼 수 있습니다. 또한 어플라이언스 이름을 변경할 수 있습니다.	33-1페이지의 어플라이언스 정보 보기 및 수정하기
HTTPS 인증서	필요한 경우, 신뢰된 권한 및 업로드 인증서에서 어플라이언스에 HTTPS 서버 인증서를 요구할 수 있습니다.	33-2페이지의 사용자 지정 HTTPS 인증서 사용
클라우드 서비스	URL 필터링 데이터를 종합적 보안 인텔리전스 클라우드에서 다운로드하고, 분류되지 않은 URL에 대한 검색을 수행하고, 탐지한 파일의 진단 정보를 Cisco에 보낼 수 있습니다.	33-6페이지의 클라우드 커뮤니케이션 활성화

어플라이언스 정보 보기 및 수정하기

라이센스: 모두

Information(정보) 페이지는 ASA FirePOWER 모듈에 대한 정보를 제공합니다. 정보는 제품 이름 및 모델 번호, 운영 체제와 버전, 그리고 현재 시스템 정책 과 같은 읽기 전용 정보를 포함합니다. 페이지는 어플라이언스의 이름을 변경할 수 있는 옵션을 제공합니다.

다음 표는 각 필드를 설명합니다.

표 33-2 어플라이언스 정보

필드	설명
이름	이 어플라이언스에 할당한 이름입니다. 이 이름은 ASA FirePOWER 모듈의 컨텍스트에서만 사용된다는 점에 유의하십시오. 어플라이언스의 이름으로 호스트 이름을 사용할 수 있지만 이 필드에 다른 이름을 입력하면 호스트 이름을 변경하지 않습니다.
제품 모델	어플라이언스의 모델 이름입니다.
일련 번호	어플라이언스의 섀시 일련 번호입니다.
소프트웨어 버전	현재 설치된 소프트웨어 버전입니다.
운영 체제	현재 어플라이언스에서 실행되는 운영 체제입니다.

표 33-2 어플라이언스 정보 (계속)

필드	설명
운영 체제 버전	현재 어플라이언스에서 실행되는 운영 체제의 버전입니다.
IPv4 주소	어플라이언스의 기본(eth0) 관리 인터페이스의 IPv4 주소입니다. IPv4 관리가 어플라이언스에서 비활성화된 경우, 이 필드는 이를 나타냅니다.
IPv6 주소	어플라이언스의 기본(eth0) 관리 인터페이스의 IPv6 주소입니다. IPv6 관리가 어플라이언스에서 비활성화된 경우, 이 필드는 이를 나타냅니다.
현재 정책	현재 적용된 어플라이언스 수준 정책입니다. 마지막으로 적용된 후부터 정책이 업데이트된 경우, 정책 이름은 기울임 꼴로 표시됩니다.
모델 번호	어플라이언스의 모델 번호입니다. 이 번호는 문제 해결을 위해 중요할 수 있습니다.

어플라이언스 정보를 변경하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성)**을 선택합니다.

Information(정보) 페이지가 나타납니다.

단계 2 어플라이언스 이름을 변경하려면, **Name(이름)** 필드에 새 이름을 입력합니다.

이름은 **반드시** 영숫자여야 하며 숫자만으로 구성할 수 없습니다.

단계 3 변경 사항을 저장하려면 **Save(저장)**를 클릭하십시오.

페이지는 새로 고침되며 변경 사항이 저장됩니다.

사용자 지정 HTTPS 인증서 사용

라이센스: 모두

ASA FirePOWER 모듈은 기본 SSL(Secure Sockets Layer) 인증서를 포함하는데, 사용자는 이를 사용하여 ASDM 및ASA FirePOWER 모듈 간의 암호화된 커뮤니케이션 채널을 시작할 수 있습니다. 그러나, 기본 인증서가 전역으로 알려진 인증 기관(CA)의 신뢰를 받는 인증 기관에서 생성되지 않으므로 이를 전역으로 알려졌거나 내부적으로 신뢰할 수 있는 CA에서 서명된 사용자 지정 인증서로 바꿀 수 있습니다.

ASA FirePOWER 모듈의 로컬 구성을 통해 인증서를 관리할 수 있습니다. 자세한 내용은 다음을 참고하십시오.

- 33-3페이지의 현재 HTTPS 서버 인증서 보기
- 33-3페이지의 서버 인증서 요청 생성
- 33-4페이지의 서버 인증서 업로드
- 33-5페이지의 사용자 인증서 요청

현재 HTTPS 서버 인증서 보기

라이센스: 모두

어플라이언스를 위해 현재 사용되고 있는 서버 인증서의 세부 정보를 볼 수 있습니다. 이 인증서는 다음 정보를 제공합니다.

표 33-3 HTTPS 서버 인증서 정보

필드	설명
제목	인증서가 설치된 어플라이언스의 경우, commonName, countryName, organizationName 및 organizationalUnitName을 제공합니다.
발급자	인증서를 생성한 어플라이언스의 경우, commonName, countryName, organizationName 및 organizationalUnitName을 제공합니다.
유효성	인증서가 유효한 시간대를 나타냅니다.
버전	인증서 버전을 나타냅니다.
일련 번호	인증서 일련 번호를 나타냅니다.
서명 알고리즘	인증서 서명에 사용되는 알고리즘을 나타냅니다.

인증서 세부 정보를 보려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성)**을 선택합니다.

Information(정보) 페이지가 나타납니다.

단계 2 **HTTPS Certificate(HTTPS 인증서)**를 클릭합니다.

ASA FirePOWER 모듈에 대한 현재 인증서의 세부 사항과 함께 HTTPS Certificate(HTTPS 인증서) 페이지가 나타납니다.

서버 인증서 요청 생성

라이센스: 모두

사용자가 제공하는 어플라이언스 정보 및 ID 정보에 따라 인증서 요청을 생성할 수 있습니다. 인증 기관에 서버 인증서를 요청하는 결과 요청을 보낼 수 있습니다. 브라우저가 신뢰하는 설치된 내부 인증 기관(CA)이 있는 경우 이를 사용하여 인증서에 직접 서명할 수 있습니다. 생성된 키는 Base-64 인코딩된 PEM 형식입니다.

로컬 구성 HTTPS Certificate(HTTPS 인증서) 페이지를 통해 인증서 요청을 생성할 때, 단일 서버에 대해서만 인증서를 생성할 수 있다는 점에 유의하십시오. **Common Name(공용 이름)** 필드의 인증서에 나타나도록 서버의 정규화된 도메인 이름을 올바르게 입력해야 합니다. 공용 이름과 DNS 호스트 이름이 일치하지 않는 경우, 어플라이언스에 연결하면 경고를 받습니다. 유사하게, 어플라이언스에 연결할 때 전역으로 알려졌거나 내부적으로 신뢰할 수 있는 CA에서 서명되지 않은 인증서를 설정하는 경우 보안 경고가 표시됩니다.

인증서 요청을 생성하려면 다음을 수행합니다,

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성)**을 선택합니다.

Information(정보) 페이지가 나타납니다.

단계 2 **HTTPS Certificate(HTTPS 인증서)**를 클릭합니다.

HTTPS Certificate(HTTPS 인증서) 페이지가 나타납니다.

단계 3 **Generate New CSR(새로운 CSR 생성)**을 클릭합니다.

Generate Certificate Signing Request(인증서 서명 요청 생성) 팝업 창이 나타납니다.

단계 4 **Country Name(국가 이름, 2자 코드)** 필드에 국가에 대한 2자 국가 코드를 입력합니다.

단계 5 **State or Province(주 또는 도)** 필드에 주 또는 도에 대한 우편 약자를 입력합니다.

단계 6 **Locality or City(지역 또는 도시)** 이름을 입력합니다.

단계 7 **Organization(조직)** 이름을 입력합니다.

단계 8 **Organizational Unit(조직 단위)(Department(부서))** 이름을 입력합니다.

단계 9 **Common Name(공용 이름)** 필드에 인증서를 요청할 서버의 정규화된 도메인 이름을 사용자가 인증서에 나타나길 원하는 방식대로 올바르게 입력합니다.

단계 10 **Generate(생성)**를 클릭합니다.

Generate Signing Request(서명 요청 생성) 팝업 창이 나타납니다.

단계 11 텍스트 편집기를 엽니다.

단계 12 `BEGIN CERTIFICATE REQUEST(인증서 요청 시작)` 및 `END CERTIFICATE REQUEST(인증서 요청 끝)`를 포함하는 인증서 요청의 전체 텍스트 블록을 복사하여 비어있는 텍스트 파일에 붙여 넣습니다.

단계 13 파일을 *servername*`.csr`로 저장합니다. 여기서 *servername*은 인증서 사용을 계획하고 있는 서버의 이름입니다.

단계 14 인증서를 요청할 인증 기관에 CSR 파일을 업로드하거나 CSR를 사용하여 자체 서명된 인증서를 만드십시오.

서버 인증서 업로드

라이센스: 모두

인증 기관(CA)으로부터 서명된 인증서를 확보한 후, 이를 업로드할 수 있습니다. 인증서를 생성한 서명 기관이 중간 CA를 신뢰하기를 요청하는 경우, 또한 인증서 체인을 제공해야 하는데, 이는 때로 인증서 경로라고 합니다. 사용자 인증서를 요청하는 경우, 중간 권한이 인증서 체인에 포함된 인증 기관에서 생성된 것이어야 합니다.

인증서를 업로드하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성)**을 선택합니다.

Information(정보) 페이지가 나타납니다.

단계 2 **HTTPS Certificate(HTTPS 인증서)**를 클릭합니다.

HTTPS Certificate(HTTPS 인증서) 페이지가 나타납니다.

단계 3 **Import HTTPS Certificate(HTTPS 인증서 가져오기)**를 클릭합니다.

Import HTTPS Certificate(HTTPS 인증서 가져오기) 팝업 창이 나타납니다.

단계 4 텍스트 편집기의 서버 인증서를 열어 `BEGIN CERTIFICATE(인증서 시작)` 및 `END CERTIFICATE(인증서 끝)` 문구를 포함하는 전체 텍스트 블록을 복사하여 **Server Certificate(서버 인증서)** 필드에 붙여 넣습니다.

단계 5 또는, 개인 키 파일을 열어 `BEGIN RSA PRIVATE KEY(RSA 개인 키 시작)` 및 `END RSA PRIVATE KEY(RSA 개인 키 끝)` 문구를 포함하는 전체 텍스트 블록을 복사하여 **Private Key(개인 키)** 필드에 붙여 넣습니다.

단계 6 사용자가 제공해야 하는 중간 인증서를 열어서 전체 텍스트 블록을 복사하여 각각을 **Certificate Chain(인증서 체인)** 필드에 붙여 넣습니다.

단계 7 **Save(저장)**를 클릭하여 인증서를 업로드하십시오.

인증서는 업로드되며 HTTPS 인증서 페이지가 업데이트되어 새 인증서를 반영합니다.

사용자 인증서 요청

라이센스: 모두

클라이언트 브라우저 인증서 확인을 사용하여 ASA FirePOWER 모듈 인터페이스에 대한 액세스를 제한할 수 있습니다. 사용자 인증서를 활성화하면, 웹 서버는 사용자의 브라우저 클라이언트가 올바른 사용자 인증서가 선택되도록 했는지 확인합니다. 해당 사용자 인증서는 반드시 서버 인증서에 사용되는 인증 기관과 동일한 신뢰 기관에서 생성된 것이어야 합니다. 사용자가 디바이스 상의 인증서 체인 내 인증 기관에서 생성하지 않았거나 유효하지 않은 브라우저에서 인증서를 선택한 경우, 브라우저는 모듈 인터페이스를 로드할 수 없습니다.

또한 서버에 대한 CRL(인증서 해치 목록)을 로드할 수 있습니다. CRL은 인증 기관에서 해지한 모든 인증서를 나열하므로, 웹 서버는 클라이언트 브라우저 인증서가 해지되지 않았음을 확인할 수 있습니다. 사용자가 해지된 인증서로서 CRL에 나열된 인증서를 선택한 경우, 브라우저는 모듈 인터페이스를 로드할 수 없습니다. 어플라이언스는 식별 부호화 규칙(DER) 형식의 CRL 업로드를 지원합니다. 한 서버에 대해 단 하나의 CRL만 로드할 수 있습니다.

해지된 인증서 목록이 통용되고 있음을 확인하기 위해, CRL을 업데이트하는 예약된 작업을 생성할 수 있습니다. 가장 최근 재생된 CRL이 인터페이스에 나열됩니다.

서버 인증서에 사용된 것과 동일한 인증 기관을 사용했음을, 그리고 인증서를 위해 중간 인증서를 업로드했음을 확인합니다. 자세한 내용은 33-4페이지의 서버 인증서 업로드를 참고하십시오.

주의 **반드시** 사용자 브라우저(또는 판독기에 삽입된 CAC)에 유효한 사용자 인증서가 있어야 사용자 인증서를 활성화할 수 있고, 실행 후 모듈 인터페이스에 액세스할 수 있습니다.

유효한 사용자 인증서를 요청하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성)**을 선택합니다.

Information(정보) 페이지가 나타납니다.

단계 2 **HTTPS Certificate(HTTPS 인증서)**를 클릭합니다.

HTTPS Certificate(HTTPS 인증서) 페이지가 나타납니다.

단계 3 **Enable User Certificates(사용자 인증서 활성화)**를 선택합니다. 메시지가 표시되면, 드롭다운 목록에서 적절한 인증서를 선택합니다.

Enable Fetching of CRL(CRL 페칭 활성화) 옵션이 나타납니다.

단계 4 선택적으로, **Enable Fetching of CRL(CRL 페칭 활성화)**을 선택할 수 있습니다.

나머지 CRL 구성 옵션이 나타납니다.

단계 5 기존 CRL 파일에 유효한 URL을 입력하고 **Refresh CRL(CRL 새로 복구)**을 클릭합니다.

제공된 URL에서 현재 CRL을 로드합니다.

참고 CRL 페칭을 활성화하면 정기적으로 CRL을 업데이트하는 예약된 작업을 생성합니다. 작업을 수정하여 업데이트의 빈도를 설정합니다. 자세한 내용은 31-4페이지의 인증서 철회 목록 다운로드 자동화를 참고하십시오.

단계 6 가지고 있는 사용자 인증서가 서버 인증서를 만든 것과 동일한 인증 기관에서 생성한 것인지 확인합니다.

주의 활성화된 사용자 인증서로 구성을 저장하면, 브라우저 인증서 스토어에 유효한 사용자 인증서가 없는 경우, 어플라이언스에 모든 웹 서버 액세스를 비활성화합니다. 구성을 저장하기 전에 설치된 사용 가능한 인증서가 있는지 확인합니다.

단계 7 사용자 인증서 구성을 적용하려면, **Save(저장)**를 클릭합니다.

클라우드 커뮤니케이션 활성화

라이센스: URL 필터링 또는 악성코드

ASA FirePOWER 모듈은 Cisco의 종합적 보안 인텔리전스 클라우드에 접속하여 다양한 유형의 정보를 확보합니다.

- 액세스 제어 규칙과 관련된 파일 정책을 사용하면 네트워크 트래픽에서 전송된 파일을 디바이스로 탐지할 수 있습니다. ASA FirePOWER 모듈은 Cisco클라우드 데이터를 사용하여 파일이 악성코드를 나타내는지 결정합니다(24-4페이지의 파일 정책 이해 및 생성 참고).
- URL 필터링을 사용할 경우, ASA FirePOWER 모듈은 많은 일반적으로 방문하는 URL에 대한 카테고리 및 평판 데이터를 검색하고, 분류되지 않은 URL에 대한 조회를 수행할 수 있습니다. 그러면 신속하게 액세스 제어 규칙을 위한 URL 조건을 만들 수 있습니다(8-8페이지의 평판 기반 URL 차단 수행 참고).

다음 옵션을 지정하려면 ASA FirePOWER 모듈의 로컬 구성을 사용하십시오.

URL 필터링 활성화

카테고리 및 평판 기반 기반 URL 필터링을 수행하려면 이 옵션을 활성화해야 합니다.

알 수 없는 URL에 대한 클라우드 쿼리

모니터링할 네트워크에 사람이 로컬 데이터 세트에 없는 URL를 탐색하려고 시도할 때 시스템이 클라우드를 쿼리할 수 있습니다.

클라우드가 URL 카테고리 또는 평판을 모르거나,ASA FirePOWER 모듈이 클라우드에 접속할 수 없는 경우, 해당 URL은 카테고리 또는 평판 기반의 URL 조건을 가진 액세스 제어 규칙을 이끌어내지 **않습니다**. URL에 카테고리 또는 평판을 수동으로 할당할 수 없습니다.

분류되지 않은 URL이 Cisco클라우드에서 목록화되는 것을 원하지 않는 경우, 예를 들면, 사생활 보호를 위해, 이 옵션을 비활성화합니다.

자동 업데이트 활성화

시스템이 클라우드에 정기적으로 접속하여 사용자 어플라이언스 로컬 데이터 집합의 URL 데이터에 대한 업데이트를 얻을 수 있습니다. 일반적으로 클라우드에서는 하루에 한 번씩 데이터를 업데이트하지만, 자동 업데이트를 사용하면 ASA FirePOWER 모듈이 30분마다 업데이트를 확인하여 항상 시스템을 최신 정보로 업데이트합니다.

일일 업데이트 양이 적다고 생각될 수도 있으나, 마지막 업데이트 이후 5일 이상 경과하면 새로운 URL 필터링 데이터를 다운로드하는 데 대역폭에 따라 20분 이상이 소요될 수 있습니다. 그런 다음 업데이트 자체를 수행하는 데 30분이 걸릴 수 있습니다.

시스템이 클라우드에 접속할 때 엄격한 제어를 갖고 싶은 경우, 자동 업데이트를 비활성화하고 31-9페이지의 URL 필터링 업데이트 자동화에 설명된 대로 일정 관리기를 대신 사용할 수 있습니다.

참고 Cisco는 업데이트를 예약하기 위해 자동 업데이트를 활성화하거나 일정 관리기를 사용하는 것을 권장합니다. 온 디맨드 업데이트를 수동으로 수행할 수 있지만, 시스템이 자동으로 클라우드에 정기적으로 접속할 수 있도록 하면 가장 최신의 관련된 URL 데이터를 제공합니다.

라이센싱

카테고리 및 평판 기반의 URL 필터링 실행과 디바이스 기반 악성코드 탐지를 실행하면 ASA FirePOWER 모듈에 적절한 라이센스를 활성화하도록 요구합니다(34-1페이지의 ASA FirePOWER 모듈 라이센싱 참고).

클라우드 접속 옵션을 구성할 수 **없는** 경우는 URL 필터링라이센스가 ASA FirePOWER 모듈에 없는 경우입니다. Cloud Services(클라우드 서비스) 페이지는 라이센싱된 옵션만 표시합니다. 만료된 라이센스를 가진 ASA FirePOWER 모듈은 클라우드에 접속할 수 없습니다.

URL Filtering(URL 필터링) 구성 옵션이 나타나도록 야기하는 것 외에도, URL 필터링라이센스를 ASA FirePOWER 모듈에 추가하면 **Enable URL Filtering(URL 필터링 활성화)** 및 **Enable Automatic Updates(자동 업데이트 활성화)**를 자동으로 활성화할 수 있습니다. 필요한 경우 옵션을 수동으로 비활성화할 수 있습니다.

인터넷 액세스

시스템은 포트 80/HTTP 및 443/HTTPS를 사용하여 Cisco클라우드를 연결합니다.

다음 절차는 Cisco클라우드 커뮤니케이션을 활성화하는 방법과 URL 데이터의 온 디맨드 업데이트를 수행하는 방법을 설명합니다. 업데이트가 이미 진행중인 경우 온 디맨드 업데이트를 시작할 수 없다는 점에 유의하십시오.

클라우드와의 통신을 활성화하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성)**을 선택합니다.

Information(정보) 페이지가 나타납니다.

단계 2 **Cloud Services(클라우드 서비스)**를 클릭합니다.

Cloud Services(클라우드 서비스) 페이지가 나타납니다. URL 필터링라이센스가 있는 경우, 페이지는 URL 데이터가 마지막으로 업데이트된 시간을 표시합니다.

단계 3 위에서 설명한 대로 클라우드 연결 옵션을 구성합니다.

반드시 **Enable URL Filtering(URL 필터링 활성화)** 다음에 **Enable Automatic Updates(자동 업데이트 활성화)** 또는 **Query Cloud for Unknown URLs(알 수 없는 URL에 대한 클라우드 쿼리)**할 수 있습니다.

단계 4 **Save(저장)**를 클릭합니다.

설정이 저장됩니다. URL 필터링을 활성화한 경우, URL 필터링이 마지막으로 활성화된 이후 얼마나 되었는지에 따라, 또는 이번이 처음으로 URL 필터링을 활성화한 경우, ASA FirePOWER 모듈은 클라우드에서 URL 필터링 데이터를 검색합니다.

시스템의 URL 데이터의 온 디맨드 업데이트를 수행하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Local(로컬) > Configuration(구성)**을 선택합니다.

Information(정보) 페이지가 나타납니다.

단계 2 **URL Filtering(URL 필터링)**을 클릭합니다.

URL Filtering(URL 필터링) 페이지가 나타납니다.

단계 3 **Update Now(지금 업데이트)**를 클릭합니다.

업데이트를 사용할 수 있는 경우 ASA FirePOWER 모듈이 클라우드에 접속하여 해당 URL 필터링 데이터를 업데이트합니다.

ASA FirePOWER 모듈 라이센싱

다양한 기능의 라이센스를 취득하여 조직에 최적의 ASA FirePOWER 구축을 만들 수 있습니다. 자세한 내용은 다음을 참고하십시오.

라이센싱의 이해

라이센스: 모두

다양한 기능의 라이센스를 취득하여 조직에 최적의 ASA FirePOWER 구축을 만들 수 있습니다. 라이센스를 통해 디바이스에서 다음을 포함하는 다양한 기능을 수행할 수 있습니다.

- 침입 탐지 및 방지
- 보안 인텔리전스 필터링
- 파일 제어 및 지능형 악성코드 차단
- 애플리케이션, 사용자 및 URL 제어

ASA FirePOWER 모듈의 라이센싱된 기능에 대한 액세스 권한이 차단될 수 있는 방법이 몇 가지 있습니다. 라이센싱된 기능을 제거할 수 있습니다. 또한, 일부 라이센스가 만료될 수 있습니다. 일부 예외가 있지만, 만료 또는 삭제된 라이센스와 관련된 기능을 사용할 수 없습니다.

이 섹션에서는 ASA FirePOWER 모듈 배포에서 사용 가능한 라이센스 유형을 설명합니다. 어플라이언스에 활성화할 수 있는 라이센스는 활성화된 다른 라이센스에 따라 달라질 수 있습니다.

다음 표에서는 ASA FirePOWER 모듈 라이센스를 요약합니다.

표 34-1 ASA FirePOWER 모듈 라이센스

라이센스	부여된 기능	필수 요건
보호	침입 탐지 및 방지 파일 제어 보안 인텔리전스 필터링	없음
제어	사용자 및 애플리케이션 제어	보호

표 34-1 ASA FirePOWER 모듈 라이센스 (계속)

라이센스	부여된 기능	필수 요건
악성코드	지능형 악성코드 차단(네트워크 기반 악성 코드 탐지 및 차단)	보호
URL 필터링	카테고리 및 평판 기반 URL 필터링	보호

자세한 내용은 다음을 참고하십시오.

- 34-2페이지의 보호
- 34-2페이지의 제어
- 34-3페이지의 악성코드
- 34-3페이지의 URL 필터링

보호

라이센스: 보호

보호 라이센스는 침입 탐지 및 방지, 파일 제어 및 보안 인텔리전스 필터링을 수행할 수 있습니다.

- *침입 탐지 및 방지*를 사용하면 침입 및 공격의 트래픽을 분석하고, 선택적으로 문제가 되는 패킷을 삭제할 수 있습니다.
- *파일 제어*를 사용하면 사용자가 특정 애플리케이션 프로토콜에 특정 유형의 파일을 업로드(전송)하거나 다운로드(수신)하는 것을 탐지하고, 선택적으로 차단할 수 있습니다. 악성코드 라이센스(34-3페이지의 악성코드 참고)를 사용하여 악성코드 위치에 따라 해당 파일 유형의 제한된 집합을 검사하고 차단할 수도 있습니다.
- *보안 인텔리전스 필터링*은 트래픽이 액세스 제어 규칙에 따라 분석의 대상이 되기 전에 특정 IP 주소를 오가는 트래픽을 차단 목록에 추가하고 거부하도록 합니다. 동적 피드는 즉시 최신 인텔리전스에 따라 연결을 차단 목록에 추가하도록 합니다. 또는, 보안 인텔리전스 필터링을 위한 "모니터링 전용" 설정을 사용할 수 있습니다.

액세스 제어 정책을 구성하여 라이센스 없이 보호에 관련된 검사를 수행할 수 있지만, 먼저 보호 라이센스를 ASA FirePOWER 모듈에 추가해야 정책을 적용할 수 있습니다.

보호 라이센스를 ASA FirePOWER 모듈에서 삭제하면, ASA FirePOWER 모듈은 침입 및 파일 이벤트를 탐지하는 것을 중지합니다. 또한, ASA FirePOWER 모듈은 Cisco에서 제공한 보안 인텔리전스 또는 서드파티 보안 인텔리전스 정보를 위해 인터넷에 접속하지 않습니다. 보호을 다시 활성화할 때까지 현재 정책을 재적용할 수 없습니다.

보호 라이센스는 URL 필터링, 악성코드, 제어 라이센스를 필요로 하므로, 보호 라이센스를 삭제하거나 비활성화하는 것은 URL 필터링, 악성코드, 제어 라이센스를 삭제하거나 비활성화하는 것과 동일한 영향을 미칩니다.

제어

라이센스: 제어

제어 라이센스를 사용하면 액세스 제어 규칙에 사용자 및 애플리케이션 상태를 추가하여 사용자 및 애플리케이션 제어를 수행할 수 있습니다. 제어를 활성화하려면 보호도 활성화해야 합니다.

제어 라이센스 없이 액세스 제어 규칙에 사용자 및 애플리케이션 상태를 추가할 수 있지만, 제어 라이센스를 ASA FirePOWER 모듈할 때까지 정책을 적용할 수 없습니다.

제어 라이센스를 삭제할 경우, 기존 액세스 제어 정책에 사용자 또는 애플리케이션 상태를 가진 규칙이 포함된 경우 이를 재적용할 수 없습니다.

URL 필터링

라이센스: URL 필터링

URL 필터링을 사용하면 모니터링된 호스트에 의해 요청된 URL에 기반한 사용자 네트워크를 통과할 수 있는 트래픽을 결정하는 액세스 제어 규칙을 작성할 수 있는데, 이는 해당 URL에 관한 정보와 관련하여 Cisco 클라우드에서 ASA FirePOWER 모듈에 의해 확보된 것입니다. URL 필터링을 활성화하려면, 보호 라이센스도 활성화해야 합니다.

팁 URL 필터링 라이센스 없이, 허용하거나 차단할 개별 URL 또는 URL 그룹을 지정할 수 있습니다. 이를 통해 웹 트래픽에 대한 세분화된 사용자 지정 제어를 가질 수 있지만 URL 카테고리와 평판 데이터를 사용하여 네트워크 트래픽을 필터링할 수는 없습니다.

URL 필터링을 사용하려면 등록 기반 URL 필터링 라이센스가 필요합니다. URL 필터링 라이센스 없이 액세스 제어 규칙에 카테고리 및 평판 기반 URL 상태를 추가할 수 있지만, ASA FirePOWER 모듈은 URL 정보를 위한 클라우드에 접속하지 않습니다. 먼저 URL 필터링 라이센스를 ASA FirePOWER 모듈에 추가할 때까지 액세스 제어 정책을 적용할 수 없습니다.

ASA FirePOWER 모듈에서 라이센스를 삭제하는 경우 URL 필터링에 대한 액세스가 차단될 수 있습니다. 또한,URL 필터링 라이센스가 만료될 수 있습니다. 라이센스가 만료되었거나 삭제한 경우, URL 조건을 가진 액세스 제어 규칙은 즉시 URL 필터링을 중지하며, ASA FirePOWER 모듈은 더 이상 클라우드에 연결하지 않습니다. 기존 액세스 제어 정책에 카테고리 및 평판 기반 URL 조건을 가진 규칙이 포함된 경우 이를 재적용할 수 없습니다.

악성코드

라이센스: 악성코드

악성코드 라이센스를 사용하면 지능형 악성코드 차단을 수행할 수 있으며, 이는 디바이스를 사용하여 네트워크를 통해 전송된 파일에서 악성코드를 탐지 및 차단할 수 있음을 의미합니다. 악성코드를 디바이스에서 활성화하려면 보호도 활성화해야 합니다.

사용자는 파일 정책의 일부로서 악성코드 탐지를 구성하는데, 이후 하나 이상의 액세스 제어 규칙과 연결합니다. 파일 정책은 사용자가 특정 애플리케이션 프로토콜에 특정 유형의 파일을 업로드 또는 다운로드하는 것을 탐지할 수 있습니다. 악성코드 라이센스를 사용하면 악성코드 탐지를 위해 해당 파일 유형의 제한된 집합을 검사할 수 있습니다. 악성코드 라이센스는 또한 특정 파일을 파일 목록에 추가하고 파일 정책 내에서 파일 목록을 활성화하며, 해당 파일이 탐지되면 자동으로 허용하거나 차단하도록 허용합니다.

악성코드 라이센스 없이 액세스 제어 규칙에 악성코드 탐지 파일 정책을 추가할 수 있지만, 파일 정책은 액세스 제어 정책 규칙 편집기에서 경고 아이콘(⚠)으로 표시됩니다. 파일 정책 안에서, Malware Cloud Lookup(악성코드 클라우드 조회) 규칙 또한 경고 아이콘으로 표시됩니다. 악성코드 탐지 파일 정책을 포함하는 액세스 제어 정책을 적용하기 전에 **반드시** 악성코드 라이센스를 추가해야 합니다. 나중에 라이센스를 삭제할 경우, 기존 액세스 제어 정책이 악성코드 탐지를 수행하는 파일 정책을 포함할 경우 이를 해당 디바이스에 재적용할 수 없습니다.

사용자 악성코드 라이센스를 삭제하거나 라이센스가 만료되는 경우, ASA FirePOWER 모듈은 악성코드 클라우드 조회 수행을 중단하며, Cisco 클라우드에서 보낸 소급 적용되는 이벤트 인지 또한 중단합니다. 악성코드 탐지를 수행하는 파일 정책을 포함하는 경우 기존 액세스 제어 정책을 재적용할 수 없습니다. 악성코드 라이센스가 만료되거나 삭제된 후 매우 짧은 시간 동안 시스템은 Malware Cloud Lookup(악성코드 클라우드 조회) 파일 규칙에서 탐지된 파일에 대해 캐시된 속성을 사용할 수 있습니다. 시간 창이 만료된 후, 시스템은 조회를 수행하는 대신 해당 파일에 `Unavailable` 속성을 할당합니다.

라이센스보기

라이센스: 모두

Licenses(라이센스) 페이지를 사용하여 ASA FirePOWER 모듈 및 매니지드 디바이스에 대한 라이센스를 봅니다.

Licenses(라이센스) 페이지 외에도, 라이센스 및 라이센스 제한을 볼 수 있는 몇 가지 다른 방법이 있습니다.

- Product Licensing(제품 라이센싱) 대시보드 위젯은 사용자 라이센스를 한 눈에 볼 수 있는 개요를 제공합니다.
- Device(디바이스) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Device Management(디바이스 관리) > Device(디바이스)**)는 라이센스를 나열합니다.

라이센스를 보려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Licenses(라이센스)**를 선택합니다.

Licenses(라이센스) 페이지가 나타납니다.

ASA FirePOWER 모듈에 라이센스 추가

라이센스: 모두

ASA FirePOWER 모듈에 라이센스를 추가하기 전에, 라이센스를 구매할 때 Cisco가 제공한 활성화 키를 보유하고 있는지 확인합니다. 사용자가 **반드시** 추가해야 하는 것은 라이센스이며, 추가한 이후에 라이센싱된 기능을 사용할 수 있습니다.

참고 백업이 완료된 후 라이센스를 추가할 경우, 이 라이센스는 백업이 복구된다고 해도 제거되거나 덮어써지지 않습니다. 복원 시 충돌을 방지하려면 백업을 복원하기 전에 라이센스가 어디에 사용되었는지에 유의하여 해당 라이센스를 제거합니다. 그리고 백업을 복원한 후 라이센스를 추가하고 재구성합니다. 충돌이 발생하면 Support(지원부)에 문의하십시오.

라이센스를 추가하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Licenses(라이센스)**를 선택합니다.

Licenses(라이센스) 페이지가 나타납니다.

단계 2 **Add New License(새 라이센스 추가)**를 클릭합니다.

Add License(라이센스 추가) 페이지가 나타납니다.

단계 3 라이센스가 첨부된 이메일을 받았습니까?

- 받은 경우 이메일에서 라이센스를 복사하여 **Licenses(라이센스)** 필드에 붙여 넣고, **Submit License(라이센스 제출)**를 클릭합니다.

  올바른 라이센스일 경우, 라이센스가 추가됩니다. 나머지 절차를 건너뜁니다.

- 아니면 **Get License(라이센스 가져오기)**를 클릭합니다.

  Licensing Center(라이센싱 센터) 웹 사이트가 나타납니다. 인터넷에 액세스할 수 없는 경우, 액세스할 수 있는 컴퓨터로 전환합니다. 페이지 하단의 라이센스 키를 메모하고 https://keyserver.sourcefire.com/을 찾습니다.

단계 4 화면 지침에 따라 라이센스를 가져옵니다. 이는 전자 메일로 전송될 것입니다.

팁 또한 Support Site(지원 사이트)에 로그인한 후 **Licenses(라이센스)** 탭에서 라이센스를 요청할 수 있습니다.

단계 5 이메일에서 라이센스를 복사하여 **License(라이센스)** 필드에 붙여 넣습니다. 이는 ASA FirePOWER 모듈의 웹 사용자 인터페이스에 있습니다. 그리고 **Submit License(라이센스 제출)**를 클릭합니다.

올바른 라이센스일 경우, 라이센스가 추가됩니다.

라이센스 삭제

라이센스: 모두

어떤 이유로 라이센스를 삭제하려면 다음 절차를 수행합니다. Cisco는 각 ASA FirePOWER 모듈의 고유한 라이센스 키에 따라 라이센스를 생성하기 때문에, 한 ASA FirePOWER 모듈에서 라이센스를 삭제한 후 이를 다른 ASA FirePOWER 모듈에서 다시 사용할 수 없다는 점을 명심하십시오.

대부분의 경우, 라이센스를 삭제하면 해당 라이센스로 활성화된 기능을 사용하는 기능을 제거합니다. 자세한 내용은 34-1페이지의 라이센싱의 이해를 참고하십시오.

라이센스를 삭제하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Licenses(라이센스)**를 선택합니다.

Licenses(라이센스) 페이지가 나타납니다.

단계 2 삭제할 라이센스 옆에 있는 삭제 아이콘( )을 클릭합니다.

단계 3 라이센스를 삭제할 것인지 확인합니다.

라이센스가 삭제됩니다.

ASA FirePOWER 모듈 소프트웨어 업데이트

Cisco는 전자 방식으로 여러 다양한 유형의 업데이트를 배포하는데, 여기에는 ASA FirePOWER 모듈소프트웨어 자체에 대한 주요 및 사소한 업데이트뿐만 아니라 규칙 업데이트, 위치 정보 데이터베이스(GeoDB) 업데이트 및 VDB(취약성 데이터베이스) 업데이트가 포함됩니다.

주의 이 섹션에는ASA FirePOWER 모듈 업데이트에 관한 일반적인 정보가 포함되어 있습니다. VDB, GeoDB 또는 침입 규칙을 포함하여 을 업데이트하기 전에 업데이트에 포함된 릴리스 노트 또는 권고 문구를 **반드시** 읽어야 합니다. 릴리스 노트는 전제 조건, 경고, 특정 설치 및 제거 지침과 같은 중요한 정보를 제공합니다.

릴리스 노트 또는 권고 문구에서 다르게 문서화되지 않는 한, 업데이트는 구성을 변경하지 않으며, 설정이 그대로 유지됩니다.

자세한 내용은 다음 섹션을 참고하십시오.

업데이트 유형 이해

라이센스: 모두

Cisco는 컴퓨터로 여러 다양한 유형의 업데이트를 배포하는데, 여기에는 ASA FirePOWER 모듈 소프트웨어 자체에 대한 주요 및 사소한 업데이트뿐만 아니라 침입 규칙 업데이트 및 VDB 업데이트가 포함됩니다.

다음 표는 Cisco에서 제공된 업데이트 유형에 대해 설명합니다. 대부분의 업데이트 유형의 경우, 해당 다운로드 및 설치를 예약할 수 있습니다(31-1페이지의 작업 일정 관리 및 35-13페이지의 반복적 규칙 업데이트 사용 참고).

표 35-1 ASA FirePOWER 모듈 업데이트 유형

업데이트 유형	설명	예약 여부	제거 여부
패치	패치는 제한된 범위의 수정 프로그램을 포함(하며 일반적으로 버전 번호, 예를 들어, 5.4.0.1의 네 번째 수를 변경)합니다.	예	예
기능 업데이트	기능 업데이트는 패치보다 포괄적이며 일반적으로 새로운 기능을 포함(하고 일반적으로 버전 번호, 예를 들어, 5.4.1의 세 번째 수를 변경)합니다.	예	예
중요 업데이트(주요 및 사소한 버전 릴리스)	주요 업데이트는 업그레이드라고도 하는데, 새로운 특징 및 기능을 포함하며, 에 대규모 변경을 수반(하며 일반적으로 버전 번호, 예를 들어, 5.3 또는 5.4의 첫 번째 또는 두 번째 수를 변경)합니다.	아니요	아니요
VDB	VDB 업데이트는 호스트가 영향을 받기 쉬운 알려진 취약점의 데이터베이스에 영향을 줍니다.	예	아니요
침입 규칙	침입 규칙은 업데이트된 새로운 침입 규칙과 전처리기 규칙, 기존 규칙의 수정된 상태, 수정된 기본 침입 정책 설정을 제공합니다. 규칙 업데이트는 또한 규칙을 삭제하고, 새로운 규칙 카테고리와 기본 변수를 제공하며, 기본 변수 값을 변경할 수 있습니다.	예	아니요
위치 정보 데이터베이스(GeoDB)	GeoDB 업데이트는 물리적 위치, 연결 유형 등의 업데이트된 정보를 제공하여 시스템이 라우팅 가능한 탐지된 IP 주소에 연결할 수 있습니다. 위치 정보 데이터를 액세스 제어 규칙의 조건으로 사용할 수 있습니다. 자세한 위치 정보를 보려면 GeoDB를 설치해야 합니다.	예	아니요

패치 및 기타 사소한 업데이트를 제거할 수 있지만 주요 업데이트를 제거하거나 VDB, GeoDB 또는 침입 규칙의 이전 버전으로 돌아갈 수는 없다는 점에 유의하십시오. 새로운 주요 버전으로 업데이트했는데 이전 버전으로 되돌려야 하는 경우, Support(지원팀)에 문의하십시오.

소프트웨어 업데이트 수행

라이센스: 모두

업데이트에는 몇 가지 기본 단계가 있습니다. 먼저, 릴리스 노트를 읽고 필요한 모든 업데이트 사전 작업을 완료하여 업데이트를 준비**해야 합니다**. 그런 다음, 업데이트를 시작할 수 있습니다. 업데이트가 성공했는지 확인해야 합니다. 마지막으로, 필요한 업데이트 사후 단계를 모두 완료하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- 35-3페이지의 업데이트 계획
- 35-3페이지의 업데이트 프로세스 이해
- 35-5페이지의 ASA FirePOWER 모듈 소프트웨어 업데이트
- 35-6페이지의 주요 업데이트 상태 모니터링

업데이트 계획

라이센스: 모두

업데이트를 시작하기 전에, 릴리스 노트를 철저하게 읽고 이해해야 합니다. 릴리스 노트는 Support Sites(지원 사이트)에서 다운로드할 수 있습니다. 릴리스 노트는 새로운 특징 및 기능, 그리고 알려진 해결된 문제에 대해 설명합니다. 릴리스 노트에는 또한 전제 조건, 경고 및 특정 설치 및 삭제 지침에 관한 중요한 정보가 포함되어 있습니다.

다음 섹션에서는 업데이트를 계획할 때 고려해야 하는 몇 가지 요소에 대한 개요를 제공합니다.

소프트웨어 버전 요구 사항

가 올바른 소프트웨어 버전을 실행하는지 확인해야 합니다. 릴리스 노트에는 필수 버전이 나와 있습니다. 이전 버전을 실행하는 경우, Support Sites(지원 사이트)에서 업데이트를 다운로드할 수 있습니다.

시간 및 디스크 공간 요구 사항

충분한 여유 디스크 공간이 있는지 확인하고 업데이트에 충분한 시간을 할당하십시오. 릴리스 노트에는 공간 및 시간 요구 사항이 나와 있습니다.

구성 백업 지침

Cisco는 사용자가 주요 업데이트를 시작하기 전에 ASA FirePOWER 모듈에 있는 모든 백업을 외부 장소로 복사한 후 삭제할 것을 권장합니다. 업데이트 유형에 관계없이 현재 구성 데이터 또한 외부 장소에 백업해야 합니다. 37-1페이지의 백업 및 복원 사용을 참고하십시오.

업데이트 수행 시기

업데이트 프로세스는 트래픽 검사와 트래픽 흐름에 영향을 미칠 수 있고 데이터 상관기는 업데이트가 진행 중인 동안 비활성화되므로, Cisco는 사용자가 유지 보수 창에서 업데이트를 수행하거나 중단이 가장 영향을 덜 줄 때 수행할 것을 권장합니다.

업데이트 프로세스 이해

라이센스: 모두

ASA FirePOWER 모듈 인터페이스를 사용하여 ASA FirePOWER 모듈을 업데이트합니다.

Product Updates(제품 업데이트) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**)는 각 업데이트 버전뿐만 아니라, 생성된 날짜 및 시간도 표시합니다. 이는 또한 소프트웨어 재부팅이 업데이트 과정의 일부로 필요한지 여부를 나타냅니다. Support(지원) 사이트에서 다운로드한 업데이트를 업로드하는 경우 페이지에 표시됩니다. 패치 및 기능 업데이트에 대한 제거 프로그램도 표시됩니다(35-7페이지의 소프트웨어 업데이트 제거 참고). 페이지에는 또한 VDB 업데이트가 나열될 수 있습니다.

팁 패치 및 기능 업데이트의 경우 자동화된 업데이트 기능을 사용할 수 있습니다. 31-6페이지의 소프트웨어 업데이트 자동화를 참고하십시오.

트래픽 흐름 및 검사

업데이트를 설치하거나 제거하는 경우 다음과 같은 기능이 영향을 받을 수 있습니다.

- 애플리케이션과 사용자 인식 및 제어를 포함하는 트래픽 검사, URL 필터링, Security Intelligence(보안 인텔리전스) 필터링, 침입 탐지 및 방지 및 연결 로그
- 트래픽 흐름

데이터 상관기는 시스템이 업데이트되는 동안에는 실행되지 않습니다. 업데이트가 완료되면 재개됩니다.

네트워크 트래픽의 중단 방식 및 기간은 ASA FirePOWER 모듈이 구성되고 배치되는 방식 그리고 업데이트가 ASA FirePOWER 모듈을 재부팅하는지 여부에 따라 달라집니다. 네트워크 트래픽이 특정 업데이트의 영향을 받는 방식과 시기에 대한 자세한 내용은 릴리스 노트를 참고하십시오.

업데이트 중에 ASA FirePOWER 모듈 사용

업데이트 유형에 관계없이, **절대로** ASA FirePOWER 모듈을 사용하여 업데이트 모니터링이 아닌 작업을 수행하지 마십시오.

주요 업데이트 중에ASA FirePOWER 모듈의 사용을 차단하고 주요 업데이트의 진행 상황을 쉽게 모니터링하려면 시스템은 ASA FirePOWER 모듈 인터페이스를 간소화합니다. 작업 큐(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 소규모 업데이트의 진행 상황을 모니터링할 수 있습니다. 소규모 업데이트 중에 ASA FirePOWER 모듈을 사용해도 되지만, Cisco는 이를 사용하지 말 것을 권장합니다.

소규모 업데이트의 경우에도 ASA FirePOWER 모듈은 업데이트 프로세스 동안 사용하지 못할 수 있습니다. 이는 정상적인 작업입니다. 이러한 문제가 발생하는 경우, ASA FirePOWER 모듈에 다시 액세스할 수 있을 때까지 기다리십시오. 업데이트가 여전히 실행되고 있는 경우, **반드시** 업데이트가 완료될 때까지 계속해서ASA FirePOWER 모듈을 사용하지 말아야 합니다. 업데이트하는 동안 ASA FirePOWER 모듈이 한 번 더 재부팅될 수 있다는 점에 유의하십시오. 이는 정상적인 작업입니다.

주의 업데이트에 문제가 발생한 경우(예를 들어, 업데이트가 실패했거나 수동으로 새로 고침한 Update Status(업데이트 상태) 페이지에 어떤 진행 상태도 표시되지 않는 경우), 업데이트를 다시 시작하지 **마십시오**. 대신, Support(지원팀)에 문의하십시오.

업데이트 후

배포가 제대로 실행되고 있는지 확인하려면 **반드시** 릴리스 노트에 나열된 업데이트 사후 작업을 모두 완료해야 합니다.

가장 중요한 업데이트 사후 작업은 액세스 제어 정책을 재적용하는 것입니다. 액세스 제어 정책을 적용하면 트래픽 흐름 및 처리 내에서 짧은 휴지기를 야기할 수 있으며, 또한 일부 패킷을 검사하지 않고 통과시킬 수 있다는 점에 유의하십시오(4-10페이지의 액세스 제어 정책 적용 참고).

또한, 다음을 수행해야 합니다.

- 업데이트가 성공했음을 확인합니다.
- 필요한 경우, 침입 규칙, VDB, 및 GeoDB를 업데이트합니다.
- 릴리스 노트의 정보에 기반하여 필요한 구성 변경을 적용합니다.
- 릴리스 노트에 나열된 부가적인 업데이트 사후 작업을 수행합니다.

ASA FirePOWER 모듈 소프트웨어 업데이트

라이센스: 모두

ASA FirePOWER 모듈 소프트웨어를 두 가지 중 하나의 방식으로 업데이트합니다. 이는 업데이트의 유형 및 ASA FirePOWER 모듈에 인터넷 액세스가 있는지 여부에 따라 다릅니다.

- Support Site(지원 사이트)에서 업데이트를 직접 다운로드할 수 있습니다. 이는 ASA FirePOWER 모듈에 인터넷 액세스가 있는 경우에 해당합니다. 이 옵션은 주요 업데이트에 지원되지 **않습니다**.
- Support Site(지원 사이트)에서 업데이트를 수동으로 다운로드한 다음 ASA FirePOWER 모듈에 업로드할 수 있습니다. ASA FirePOWER 모듈에 인터넷 액세스가 없거나 주요 업데이트를 수행하는 경우 이 옵션을 선택합니다.

주요 업데이트의 경우 ASA FirePOWER 모듈 업데이트는 이전 업데이트에 대한 제거 프로그램을 삭제합니다.

ASA FirePOWER 모듈 소프트웨어를 업데이트하려면 다음을 수행합니다.

단계 1 릴리스 노트를 읽고 필요한 모든 업데이트 사전 작업을 완료합니다.

업데이트 사전 작업에는 다음 사항의 확인이 포함될 수 있습니다. ASA FirePOWER 모듈이 올바른 버전의 Cisco 소프트웨어를 실행하고 있으며, 업데이트를 실행할 수 있는 여유 디스크 공간이 충분하고, 업데이트를 실행할 수 있는 충분한 시간을 확보했으며, 구성 데이터를 백업했는지 등입니다.

단계 2 업데이트를 업로드합니다. 업데이트 유형 및 사용자 ASA FirePOWER 모듈에 인터넷 액세스가 있는지 여부에 따라 두 가지 옵션이 있습니다.

- 주요 업데이트를 제외한 모든 경우, 그리고 ASA FirePOWER 모듈에 인터넷 액세스가 있는 경우 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택한 다음 **Download Updates(업데이트 다운로드)**를 클릭하여 다음 Support Sites(지원 사이트) 중 하나에서 최신 업데이트를 확인합니다.
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)
- 주요 업데이트의 경우, 또는 사용자 ASA FirePOWER 모듈이 인터넷에 액세스할 수 없는 경우 먼저 다음 Support Sites(지원 사이트) 중 하나에서 수동으로 업데이트를 다운로드해야 합니다.
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)
- **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택한 다음 **Upload Update(업데이트 업로드)**를 클릭합니다. 탐색할 **Choose File(파일 선택)**을 클릭하고 업데이트를 선택한 후 **Upload(업로드)**를 클릭합니다.

참고 수동으로, 또는 Product Updates(제품 업데이트) 탭에서 **Download Updates(다운로드 업데이트)**를 클릭하여 Support Sites(지원 사이트)에서 업데이트를 직접 다운로드합니다. 업데이트 파일을 이메일로 전송하는 경우, 손상될 수 있습니다.

업데이트가 업로드됩니다.

단계 3 **Monitoring(모니터링) > ASA FirePOWER(ASA FirePOWER 모니터링) Monitoring(모니터링) > Task Status(작업 상태)**를 선택하여 작업 큐를 살펴보고 진행 중인 작업이 없는지 확인합니다.

업데이트를 시작할 때 실행되고 있는 작업은 중단되며 다시 시작할 수 없습니다. 업데이트가 완료된 후 작업 큐에서 수동으로 삭제해야 합니다. 작업 큐는 10초마다 자동으로 새로 고침됩니다. 업데이트를 시작하기 전에 오랫동안 실행되는 작업이 모두 완료될 때까지 기다려야 합니다.

단계 4 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택합니다.

Product Updates(제품 업데이트) 페이지가 나타납니다.

단계 5 사용자가 업로드한 업데이트 옆에 있는 설치 아이콘을 클릭합니다.

업데이트 프로세스가 시작됩니다. 업데이트를 모니터링하는 방법은 업데이트가 주요 업데이트인지 또는 사소한 업데이트인지 여부에 따라 다릅니다. ASA FirePOWER 모듈 업데이트 유형 표 및 릴리스 노트를 참고하여 업데이트 유형을 결정하십시오.

- 사소한 업데이트의 경우, 작업 큐(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 업데이트의 진행 상황을 모니터링할 수 있습니다.
- 주요 업데이트의 경우, 작업 큐에서 업데이트의 진행 상황에 대한 모니터링을 시작할 수 있습니다. 그러나, ASA FirePOWER 모듈이 필요한 업데이트 사전 확인을 마친 후에는 모듈 인터페이스에 진입할 수 없습니다. 액세스를 다시 확보하면 Upgrade Status(상태 업그레이드) 페이지가 나타납니다. 자세한 내용은 35-6페이지의 주요 업데이트 상태 모니터링을 참고하십시오.

주의 업데이트 유형에 관계없이, **절대로** 업데이트가 완료될 때까지 ASA FirePOWER 모듈을 사용하여 업데이트 모니터링 이외의 작업을 수행하지 마십시오. 필요한 경우, ASA FirePOWER 모듈이 재부팅됩니다. 자세한 내용은 35-4페이지의 업데이트 중에 ASA FirePOWER 모듈 사용을 참고하십시오.

단계 6 업데이트가 완료되면 ASA FirePOWER 모듈 인터페이스에 액세스하고 페이지를 새로 고칩니다. 그렇지 않으면, 인터페이스는 예상되지 않은 작업을 나타낼 수 있습니다. 주요 업데이트 후 인터페이스에 액세스하는 첫 번째 사용자인 경우 EULA(최종 사용자 라이센스 계약)가 표시될 수 있습니다. 계속하려면 EULA를 검토 및 승인해야 합니다.

단계 7 Support Sites(지원 사이트)에서 사용할 수 있는 규칙 업데이트가 ASA FirePOWER 모듈의 규칙보다 새로운 경우 더 새로운 규칙을 가져옵니다.

자세한 내용은 35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기를 참고하십시오.

단계 8 액세스 제어 정책을 재적용합니다.

액세스 제어 정책을 적용하면 트래픽 흐름 및 처리 내에서 짧은 휴지기를 야기할 수 있으며, 또한 일부 패킷을 검사하지 않고 통과시킬 수 있습니다. 자세한 내용은 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

단계 9 Support Sites(지원 사이트)에서 사용할 수 있는 VDB가 가장 최근에 설치된 VDB보다 새로운 버전인 경우, 최신 VDB를 설정합니다.

VDB 업데이트를 설치하면 트래픽 흐름 및 처리 내에서 짧은 휴지기가 야기될 수 있으며, 또한 일부 패킷이 검사되지 않은 상태로 통과될 수 있습니다. 자세한 내용은 35-8페이지의 취약성 데이터베이스 업데이트를 참고하십시오.

주요 업데이트 상태 모니터링

라이센스: 모두

주요 업데이트의 경우, ASA FirePOWER 모듈에서 간소화된 인터페이스가 제공되므로 업데이트 프로세스를 쉽게 모니터링할 수 있습니다. 간소화된 인터페이스는 또한 ASA FirePOWER 모듈을 사용하여 업데이트 모니터링 이외의 작업을 수행하지 못하도록 합니다. 사용자는 작업 큐(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 업데이트의 진행 상황에 대한 모니터링을 시작할 수 있습니다. 그러나, ASA FirePOWER 모듈에서 필수 업데이트 사전 확인을 완료한 후 사용자는 사용자 인터페이스에 진입할 수 없습니다 간편한 업데이트 페이지가 나타납니다.

간소화된 인터페이스는 업데이트를 시작하는 버전, 업데이트 중인 버전, 그리고 업데이트가 시작된 이후 경과한 시간을 표시합니다. 이는 또한 진행 막대를 표시하고 현재 실행되고 있는 스크립트에 대한 세부 정보를 제공합니다.

팁 업데이트 로그를 보려면 **show log for current script(현재 스크립트의 로그 보기)**를 클릭합니다. 로그를 다시 숨기려면 **hide log for current script(현재 스크립트의 로그 숨기기)**를 클릭합니다.

어떤 이유로든 업데이트가 실패하면, 실패 시간 및 날짜, 업데이트가 실패했을 때 실행 중이었던 스크립트, 그리고 Support(지원팀)에 문의하는 방법에 대한 지침을 나타내는 오류 메시지가 페이지에 표시됩니다. 업데이트를 다시 시작하지 **마십시오**.

주의 업데이트와 함께 기타 다른 문제가 발생하는 경우(예를 들어, 페이지를 수동으로 새로 고침하면 장기간 동안 진행되지 않은 경우), 업데이트를 다시 시작하지 **마십시오**. 대신, Support(지원팀)에 문의하십시오.

업데이트가 완료되면,ASA FirePOWER 모듈이 성공 메시지를 표시하고 재부팅됩니다. ASA FirePOWER 모듈이 재부팅을 완료한 후, 필요한 업데이트 사후 단계를 모두 완료합니다.

소프트웨어 업데이트 제거

라이센스: 모두

패치 또는 기능 업데이트를 적용하는 경우, 업데이트 프로세스는 업데이트를 제거할 수 있는 제거 프로그램을 생성합니다.

업데이트를 제거하는 경우 결과 Cisco 소프트웨어 버전은 업데이트 경로에 따라 다릅니다. 예를 들어, 버전 5.0에서 버전 5.0.0.2로 직접 업데이트한 시나리오를 고려하십시오. 버전 5.0.0.2 패치를 제거하면 버전 5.0.0.1의 결과를 얻을 수 있습니다. 버전 5.0.0.1 업데이트를 설치하지 않은 경우에도 마찬가지입니다. 업데이트를 제거하는 경우 결과 Cisco 소프트웨어 버전 정보에 대한 정보는 릴리스 노트를 참고하십시오.

참고 제거는 주요 업데이트에서 지원되지 않습니다. 새로운 주요 버전으로 업데이트했는데 이전 버전으로 되돌려야 하는 경우, Support(지원팀)에 문의하십시오.

트래픽 흐름 및 검사

업데이트를 제거하면 트래픽 검사 및 트래픽 흐름에 영향을 줄 수 있습니다. 네트워크 트래픽이 특정 업데이트의 영향을 받는 방식과 시기에 대한 자세한 내용은 릴리스 노트를 참고하십시오.

제거 후

업데이트를 제거한 후, 제거가 성공적으로 완료되었는지 확인하는 것입니다. 각 업데이트에 대한 특정 정보는 릴리스 노트를 참고하십시오.

패치 또는 기능 업데이트를 제거하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택합니다.

Product Updates(제품 업데이트) 페이지가 나타납니다.

단계 2 제거하려는 업데이트의 제거 프로그램 옆에 있는 설치 아이콘을 클릭합니다.

메시지가 표시되면 업데이트를 제거하고 ASA FirePOWER 모듈의 재부팅을 원하는지 확인합니다.

제거 프로세스가 시작됩니다. 작업 큐(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 진행 상황을 모니터링할 수 있습니다.

주의 **절대로** 제거가 완료될 때까지 ASA FirePOWER 모듈 인터페이스를 사용하여 작업을 수행하지 마십시오. 필요한 경우, ASA FirePOWER 모듈이 재부팅됩니다. 자세한 내용은 35-4페이지의 업데이트 중에 ASA FirePOWER 모듈 사용을 참고하십시오.

단계 3 페이지를 새로 고치십시오. 그렇지 않으면, 인터페이스는 예상되지 않은 작업을 나타낼 수 있습니다.

취약성 데이터베이스 업데이트

라이센스: 모두

Cisco 취약성 데이터베이스(VDB)는 호스트가 영향을 받기 쉬운 잘 알려진 취약성의 데이터베이스입니다. Cisco VRT(취약성 연구단)는 VDB에 대한 주기적인 업데이트를 생성합니다. VDB를 업데이트하려면, Product Updates(제품 업데이트) 페이지를 참고하십시오.

참고 검색 업데이트로 VDB 업데이트를 설치하면 트래픽 흐름 및 처리 내에서 짧은 휴지기가 야기될 수 있으며, 또한 일부 패킷이 검사되지 않은 상태로 통과될 수 있습니다. 모든 시스템 다운타임의 영향을 최소화하기 위해 시스템 사용량이 낮은 시간 동안 업데이트하도록 예약할 수 있습니다.

참고 VDB 업데이트를 완료한 후, 오래된 액세스 제어 정책을 재적용합니다. VDB 설치 또는 액세스 제어 정책을 재적용하면 트래픽 흐름 및 처리 내에서 짧은 휴지기가 야기될 수 있으며, 또한 일부 패킷이 검사되지 않은 상태로 통과될 수 있다는 점에 유의하십시오. 자세한 내용은 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

이 섹션에서는 수동 VDB 업데이트를 계획하고 수행하는 방법에 대해 설명합니다.

취약성 데이터베이스를 업데이트하려면 다음을 수행합니다.

단계 1 업데이트를 수행하려면 VDB Update Advisory Text(VDB 업데이트 권고 문구)를 읽어 보십시오.

권고 문구에는 업데이트에 나열된 VDB 변경에 대한 정보가 포함됩니다.

단계 2 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택합니다.

Product Updates(제품 업데이트) 페이지가 나타납니다.

단계 3 업데이트를 업로드합니다.

- ASA FirePOWER 모듈에서 인터넷에 액세스할 수 있는 경우 **Download Updates(다운로드 업데이트)**를 클릭하여 다음 Support Sites(지원 사이트) 중 하나에서 최신 업데이트를 확인합니다.
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

- ASA FirePOWER 모듈에서 인터넷에 액세스할 수 없는 경우, 다음 Support Sites(지원 사이트) 중 하나에서 수동으로 업데이트를 다운로드한 다음 **Upload Update(업데이트 업로드)**를 클릭합니다. 탐색할 **Choose File(파일 선택)**을 클릭하고 업데이트를 선택한 후 **Upload(업로드)**를 클릭합니다.
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

참고 수동으로, 또는 **Download Updates(업데이트 다운로드)**를 클릭하여 Support Sites(지원 사이트)에서 업데이트를 직접 다운로드합니다. 업데이트 파일을 이메일로 전송하는 경우, 손상될 수 있습니다.

업데이트가 업로드됩니다.

단계 4 VDB 업데이트 옆에 있는 설치 아이콘을 클릭합니다.

Install Update(업데이트 설치) 페이지가 나타납니다.

단계 5 **Install(설치)**을 클릭합니다.

주의 업데이트 프로세스가 시작됩니다. 작업 큐 (**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 업데이트의 진행 상황을 모니터링할 수 있습니다. 업데이트에 문제가 발생한 경우(예를 들어, 작업 큐에 업데이트가 실패했음이 표시된 경우), 업데이트를 다시 시작하지 **마십시오**. 대신, Support(지원팀)에 문의하십시오.

VDB 업데이트를 적용하려면 오래된 액세스 제어 정책을 모두 재적용해야 합니다(4-10페이지의 액세스 제어 정책 적용 참고).

규칙 업데이트 및 로컬 규칙 업데이트 가져오기

라이센스: 모두

새로운 취약성이 알려지면 CiscoVRT(취약성 연구단)는 ASA FirePOWER 모듈에 먼저 가져올 수 있는 규칙 업데이트를 릴리스한 후, 영향을 받는 액세스 제어, 네트워크 분석 및 침입 정책을 적용하여 구현합니다.

규칙 업데이트는 누적되며, Cisco에서는 항상 최신 업데이트를 가져올 것을 권장합니다. 현재 설치된 규칙의 버전과 일치하거나 이전의 규칙 업데이트는 가져올 수 없습니다.

참고 규칙 업데이트에는 새로운 바이너리가 포함될 수 있지만, 이들을 다운로드하고 설치하는 프로세스가 보안 정책을 준수해야 합니다. 또한 규칙 업데이트의 규모가 클 수 있으므로 네트워크 이용률이 낮은 시간 동안 규칙을 가져오십시오.

규칙 업데이트는 다음을 제공할 수 있습니다.

- **신규 및 수정된 규칙 및 규칙 상태** — 규칙 업데이트는 신규 및 업데이트된 침입 규칙과 전처리기 규칙을 제공합니다. 새 규칙의 경우, 규칙 상태는 각 시스템이 제공하는 침입 정책에서 다를 수 있습니다. 예를 들어, 새 규칙은 Security Over Connectivity(연결성에 우선하는 보안) 침입 정책에서 활성화되며 Connectivity Over Security(보안에 우선하는 연결성) 침입 정책에서는 비활성화됩니다. 규칙 업데이트는 기존 규칙의 기본 상태를 변경하거나, 기존 규칙을 완전히 삭제할 수 있습니다.

- **새 규칙 카테고리** — 규칙 업데이트에는 새 규칙 카테고리가 포함될 수 있는데, 이는 항상 추가됩니다.
- **수정된 전처리기 및 고급 설정** — 규칙 업데이트는 시스템이 제공한 침입 정책에 있는 고급 설정 및 시스템이 제공한 네트워크 분석 정책에 있는 전처리기 설정을 변경할 수 있습니다. 이들은 또한 액세스 제어 정책의 고급 전처리 및 성능 옵션에 대한 기본값을 업데이트할 수 있습니다.
- **신규 및 수정된 변수** — 규칙 업데이트는 기존의 기본 변수에 대한 기본값을 변경할 수 있지만, 변경 사항을 재정의하지 않습니다. 새로운 변수는 항상 추가됩니다.

규칙 업데이트가 정책을 수정하는 시점에 대한 이해

규칙 업데이트는 모든 액세스 제어 정책뿐만 아니라 시스템이 제공한 네트워크 분석 정책 및 사용자 지정 네트워크 분석 정책 모두에도 영향을 미칠 수 있습니다.

- **시스템 제공** — 시스템이 제공한 네트워크 분석 및 침입 정책에 대한 변경 사항뿐만 아니라 고급 액세스 제어 설정에 대한 모든 변경 사항은 업데이트한 후 정책을 재적용할 때 자동으로 적용됩니다.
- **사용자 지정** — 각 사용자 지정 네트워크 분석 및 침입 정책은 시스템이 제공한 정책을 자체 기반으로, 또는 정책 체인의 궁극적인 기반으로 사용하므로 규칙 업데이트는 사용자 지정 네트워크 분석 및 침입 정책에 영향을 미칠 수 있습니다. 하지만, 규칙 업데이트가 자동으로 해당 변경 사항을 적용하는 것을 방지할 수 있습니다. 이를 통해 규칙 업데이트를 가져오는 것과 별개로 시스템 제공 기본 정책을 수동으로 업데이트할 수 있습니다. (사용자 지정 정책별 기반으로 실행되는) 선택 사항과 관계없이, 시스템이 제공한 정책에 대한 업데이트는 사용자 지정한 어떤 설정도 재지정하지 **않습니다**. 자세한 내용은 12-4페이지의 규칙 업데이트를 통해 시스템이 제공하는 기본 정책 수정 허용을 참고하십시오.

규칙 업데이트를 가져오면 네트워크 분석 및 침입 정책에 캐시된 변경 사항이 모두 제거된다는 점에 유의하십시오. 사용자의 편의를 위해, Rule Updates(규칙 업데이트) 페이지는 캐시된 변경 사항이 있는 정책을 나열합니다. 자세한 내용은 11-14페이지의 문제 해결 및 정책 변경 사항 커밋을 참고하십시오.

정책 재적용

규칙 업데이트가 수행한 변경 사항이 적용되려면 수정된 정책을 모두 재적용해야 합니다. 규칙 업데이트를 가져올 때, 시스템이 침입 또는 액세스 제어 정책을 자동으로 재적용하도록 설정할 수 있습니다. 이는 규칙 업데이트가 시스템이 제공하는 기본 정책을 수정할 수 있는 경우에 특히 유용합니다.

- 액세스 제어 정책을 재적용하면 또한 관련된 네트워크 분석 및 파일 정책이 재적용되지만, 침입 정책은 재적용되지 **않습니다**. 이는 또한 모든 변경된 고급 설정에 대한 기본값을 업데이트합니다. 네트워크 분석 정책을 개별적으로 적용할 수 없으므로, 네트워크 분석 정책에서 전처리기 설정을 업데이트하려는 경우 **반드시** 액세스 제어 정책을 재적용해야 합니다.
- 침입 정책을 재적용하면 규칙 및 기타 변경된 침입 정책 설정을 업데이트할 수 있습니다. 액세스 제어 정책과 함께 침입 정책을 재적용할 수 있으며, 침입 정책만 적용하여 다른 액세스 제어 구성을 업데이트하지 않은 상태로 침입 규칙을 업데이트할 수도 있습니다.

규칙 업데이트에 공유 객체 규칙이 포함된 경우, 액세스 제어 또는 침입 정책을 가져온 후 처음 적용하면 트래픽 흐름 및 처리 내에서 짧은 휴지기가 야기될 수 있으며, 또한 일부 패킷이 검사되지 않은 상태로 통과될 수 있습니다. 요구 사항, 기타 영향 및 권장 사항을 포함하여, 액세스 제어 및 침입 정책 적용에 대한 자세한 내용은 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

규칙 업데이트를 가져오는 방법에 대한 자세한 내용은 다음을 참고하십시오.

- 35-11페이지의 일회성 규칙 업데이트 사용에서는 Support Sites(지원 사이트)에서 단일 규칙을 가져오는 방법에 대해 설명합니다.
- 35-13페이지의 반복적 규칙 업데이트 사용에서는 자동화된 기능을 사용하여 Support Sites(지원 사이트)에서 규칙 업데이트를 다운로드하고 설정하는 방법에 대해 설명합니다.

- 35-15페이지의 로컬 규칙 파일 가져오기에서는 사용자가 로컬 컴퓨터에서 생성한 표준 텍스트 규칙 파일의 복사본을 가져오는 방법에 대해 설명합니다.
- 35-16페이지의 규칙 업데이트 로그 보기에서는 규칙 업데이트 로그에 대해 설명합니다.

일회성 규칙 업데이트 사용

라이센스: 모두

일회성 규칙 업데이트에 사용할 수 있는 2가지 방법이 있습니다.

- 35-11페이지의 수동 일회성 규칙 업데이트 사용에서는 Support Sites(지원 사이트)에서 규칙 업데이트를 수동으로 다운로드한 후 설치하는 방법에 대해 설명합니다.
- 35-12페이지의 일회성 규칙 업데이트 자동으로 사용에서는 자동화된 기능을 사용하여 Support Sites(지원 사이트)에서 새 규칙 업데이트를 검색하고 업로드하는 방법에 대해 설명합니다.

수동 일회성 규칙 업데이트 사용

라이센스: 모두

다음 절차는 새 규칙 업데이트를 수동으로 가져오는 방법에 대해 설명합니다. 이 절차는 사용자 ASA FirePOWER 모듈에 인터넷 액세스가 없는 경우 특히 유용합니다.

수동으로 규칙 업데이트를 가져오려면 다음을 수행합니다.

단계 1 인터넷에 액세스할 수 있는 컴퓨터에서 다음 사이트 중 하나에 액세스합니다.

- **Sourcefire:** (https://support.sourcefire.com/)
- **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

단계 2 **Download(다운로드)**를 클릭한 후 **Rules(규칙)**를 클릭합니다.

단계 3 최신 규칙 업데이트를 탐색합니다.

규칙 업데이트는 누적되며, 현재 설치된 규칙의 버전과 일치하거나 이전의 규칙 업데이트는 가져올 수 없습니다.

단계 4 다운로드할 규칙 업데이트 파일을 클릭하여 컴퓨터에 저장합니다.

단계 5 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택한 후 **Rule Updates(규칙 업데이트)** 탭을 선택합니다.

Rule Updates(규칙 업데이트) 페이지가 나타납니다.

팁 또한 **Import Rules(규칙 가져오기)**를 클릭할 수 있는데, 이는 Rule Editor(규칙 편집기) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 규칙) > Rule Editor(규칙 편집기)**)에서 찾을 수 있습니다.

단계 6 또는, **Delete All Local Rules(모든 로컬 규칙 삭제)**를 클릭한 다음 **OK(확인)**를 클릭하여 사용자가 생성했거나 가져온 사용자 정의 규칙을 모두 삭제된 폴더에 옮깁니다. 자세한 내용은 23-104페이지의 사용자 지정 규칙 삭제를 참고하십시오.

단계 7 **Rule Update or text rule file to upload and install(규칙 업데이트 또는 업로드 및 설치할 텍스트 규칙 파일)**을 선택하고 **Choose File(파일 선택)**을 클릭하여 규칙 업데이트 파일을 탐색하고 선택합니다.

단계 8 또는, 업데이트가 완료되면 정책을 재적용합니다.

- **Reapply intrusion policies after the rule update import completes(규칙 업데이트 가져오기가 완료된 후 침입 정책 재적용)**를 선택하여 침입 정책을 자동으로 재적용합니다. 생성했을 수 있는 다른 액세스 제어 구성을 업데이트할 필요 없이 규칙 및 기타 변경된 침입 정책 설정을 업데이트하려면 이 옵션만 선택합니다. 액세스 제어 정책과 함께 침입 정책을 재적용하려면 **반드시** 이 옵션을 선택해야 합니다. 이 경우 액세스 제어 정책을 재적용하더라도 완전히 적용되지는 않습니다.
- **Reapply access control policies after the rule update import completes(규칙 업데이트 가져오기가 완료된 후 액세스 제어 정책 재적용)**를 선택하여 침입 정책이 아닌, 액세스 제어 정책과 관련 네트워크 분석 및 파일 정책을 자동으로 재적용합니다. 이 옵션을 선택하면 모든 변경된 액세스 제어 고급 설정에 대한 기본값이 업데이트됩니다. 네트워크 분석 정책을 상위 액세스 제어 정책과 개별적으로 적용할 수 없으므로, 네트워크 분석 정책에서 전처리기 설정을 업데이트하려는 경우 **반드시** 액세스 제어 정책을 재적용해야 합니다.

단계 9 **Import(가져오기)**를 클릭합니다.

시스템에 규칙 업데이트가 설치되고 Rule Update Log(규칙 업데이트 로그) 상세 보기가 표시됩니다(35-18페이지의 규칙 업데이트 가져오기 로그 상세 보기 이해 참고). 시스템은 또한 이전 단계에서 지정한 대로 정책을 적용합니다(4-10페이지의 액세스 제어 정책 적용 및 19-8페이지의 침입 정책 적용 참고).

참고 규칙 업데이트를 설치하는 동안 오류 메시지를 수신할 경우 Support(지원팀)에 문의하십시오.

일회성 규칙 업데이트 자동으로 사용

라이센스: 모두

다음 절차는 Support Site(지원 사이트)에 자동으로 연결하여 새 규칙을 가져오는 방법에 대해 설명합니다. ASA FirePOWER 모듈에 인터넷 액세스가 있는 경우에만 이 절차를 사용할 수 있습니다.

자동으로 규칙 업데이트를 가져오려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택한 후 **Rule Updates(규칙 업데이트)** 탭을 선택합니다.

Rule Updates(규칙 업데이트) 페이지가 나타납니다.

팁 또한 **Import Rules(규칙 가져오기)**를 클릭할 수 있는데, 이는 Rule Editor(규칙 편집기) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 규칙) > Rule Editor(규칙 편집기)**)에서 찾을 수 있습니다.

단계 2 또는, **Delete All Local Rules(모든 로컬 규칙 삭제)**를 클릭한 다음 **OK(확인)**를 클릭하여 사용자가 생성했거나 가져온 사용자 정의 규칙을 모두 삭제된 폴더에 옮깁니다. 자세한 내용은 23-104페이지의 사용자 지정 규칙 삭제를 참고하십시오.

단계 3 **Download new Rule Update from the Support Site(지원 사이트에서 새로운 규칙 업데이트 다운로드)**를 선택합니다.

단계 4 또는, 업데이트가 완료되면 정책을 재적용합니다.

- **Reapply intrusion policies after the rule update import completes(규칙 업데이트 가져오기가 완료된 후 침입 정책 재적용)**를 선택하여 침입 정책을 자동으로 재적용합니다. 생성했을 수 있는 다른 액세스 제어 구성을 업데이트할 필요 없이 규칙 및 기타 변경된 침입 정책 설정을 업데이트하려면 이 옵션만 선택합니다. 액세스 제어 정책과 함께 침입 정책을 재적용하려면 **반드시** 이 옵션을 선택해야 합니다. 이 경우 액세스 제어 정책을 재적용하더라도 완전히 적용되지는 않습니다.
- **Reapply access control policies after the rule update import completes(규칙 업데이트 가져오기가 완료된 후 액세스 제어 정책 재적용)**를 선택하여 침입 정책이 아닌, 액세스 제어 정책과 관련 네트워크 분석, 및 파일 정책을 자동으로 재적용합니다. 이 옵션을 선택하면 모든 변경된 액세스 제어 고급 설정에 대한 기본값이 업데이트됩니다. 네트워크 분석 정책을 상위 액세스 제어 정책과 개별적으로 적용할 수 없으므로, 네트워크 분석 정책에서 전처리기 설정을 업데이트하려는 경우 **반드시** 액세스 제어 정책을 재적용해야 합니다.

단계 5 **Import(가져오기)**를 클릭합니다.

시스템에 규칙 업데이트가 설치되고 Rule Update Log(규칙 업데이트 로그) 상세 보기가 표시됩니다(35-18페이지의 규칙 업데이트 가져오기 로그 상세 보기 이해 참고). 시스템은 또한 이전 단계에서 지정한 대로 정책을 적용합니다(4-10페이지의 액세스 제어 정책 적용 및 19-8페이지의 침입 정책 적용 참고).

참고 규칙 업데이트를 설치하는 동안 오류 메시지를 수신할 경우 Support(지원팀)에 문의하십시오.

반복적 규칙 업데이트 사용

라이센스: 모두

Rule Updates(규칙 업데이트) 페이지를 사용하여 일 단위, 주 단위 또는 월 단위로 규칙 업데이트를 가져올 수 있습니다.

규칙 업데이트 가져오기에서 적용 가능한 하위 태스크는 다운로드, 설치, 기본 정책 업데이트 및 정책 재적용 순서로 나타납니다. 1개의 하위 태스크가 완료되면, 다음 하위 태스크가 시작됩니다. 반복적 가져오기가 구성된 ASA FirePOWER 모듈이 이전에 적용한 정책만 적용할 수 있다는 점에 유의하십시오.

반복적 규칙 업데이트를 예약하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택한 후 **Rule Updates(규칙 업데이트)** 탭을 선택합니다.

Rule Updates(규칙 업데이트) 페이지가 나타납니다.

팁 또한 **Import Rules(규칙 가져오기)**를 클릭할 수 있는데, 이는 Rule Editor(규칙 편집기) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 규칙) > Rule Editor(규칙 편집기)**)에서 찾을 수 있습니다.

단계 2 또는, **Delete All Local Rules(모든 로컬 규칙 삭제)**를 클릭한 다음 **OK(확인)**를 클릭하여 사용자가 생성했거나 가져온 사용자 정의 규칙을 모두 삭제된 폴더에 옮깁니다. 자세한 내용은 23-104페이지의 사용자 지정 규칙 삭제를 참고하십시오.

단계 3 **Enable Recurring Rule Update Imports(반복적 규칙 업데이트 가져오기 활성화)**를 선택합니다.

페이지가 확장되어 반복적 가져오기에 대한 옵션이 표시됩니다. **Recurring Rule Update Imports(반복적 규칙 업데이트 가져오기)** 섹션 제목 아래에 가져오기 상태 메시지가 나타납니다. 설정을 저장하면 반복적 가져오기가 활성화됩니다.

팁 반복적 가져오기를 비활성화하려면, **Enable Recurring Rule Update Imports(반복적 규칙 업데이트 가져오기 활성화)** 확인 상자를 비워두고 **Save(저장)**를 클릭합니다.

단계 4 **Import Frequency(가져오기 빈도)** 필드의 드롭다운 목록에서 **Daily(매일)**, **Weekly(매주)** 또는 **Monthly(매달)** 중 하나를 선택합니다.

가져오기 빈도를 매주 또는 매달로 선택한 경우, 표시되는 드롭다운 목록을 사용하여 규칙 업데이트를 가져올 주 또는 달의 요일을 선택합니다. 선택한 첫 번째 문자 또는 첫 번째 숫자를 한 번 이상 클릭하거나 입력하고 Enter 키를 눌러 반복적 태스크 드롭다운 목록에서 선택합니다.

단계 5 **Import Frequency(가져오기 빈도)** 필드에서 반복적 규칙 업데이트 가져오기를 시작할 시간을 지정합니다.

단계 6 또는, 업데이트가 완료되면 정책을 재적용합니다.

- **Reapply intrusion policies after the rule update import completes(규칙 업데이트 가져오기가 완료된 후 침입 정책 재적용)**를 선택하여 침입 정책을 자동으로 재적용합니다. 생성했을 수 있는 다른 액세스 제어 구성을 업데이트할 필요 없이 규칙 및 기타 변경된 침입 정책 설정을 업데이트하려면 이 옵션만 선택합니다. 액세스 제어 정책과 함께 침입 정책을 재적용하려면 **반드시** 이 옵션을 선택해야 합니다. 이 경우 액세스 제어 정책을 재적용하더라도 완전히 적용되지는 않습니다.
- **Reapply access control policies after the rule update import completes(규칙 업데이트 가져오기가 완료된 후 액세스 제어 정책 재적용)**를 선택하여 침입 정책이 아닌, 액세스 제어 정책과 네트워크 분석 및 파일 정책을 자동으로 재적용합니다. 이 옵션을 선택하면 모든 변경된 액세스 제어 고급 설정에 대한 기본값이 업데이트됩니다. 네트워크 분석 정책을 상위 액세스 제어 정책과 개별적으로 적용할 수 없으므로, 네트워크 분석 정책에서 전처리기 설정을 업데이트하려는 경우 **반드시** 액세스 제어 정책을 재적용해야 합니다.

단계 7 **Save(저장)**을 클릭하여 설정을 사용하는 반복적 규칙 업데이트 가져오기를 활성화합니다.

Recurring Rule Update Imports(반복적 규칙 업데이트 가져오기) 섹션 제목 아래의 상태 메시지가 변경되어 규칙 업데이트가 아직 실행되지 않았음을 나타냅니다. 시스템은 이전 단계에서 지정한 대로 예약된 시간에 규칙 업데이트를 설치하고 정책을 적용합니다(4-10페이지의 액세스 제어 정책 적용 및 19-8페이지의 침입 정책 적용 참고).

가져오기 작업 중 또는 작업 이전에 로그 오프하거나 다른 작업을 수행할 수 있습니다. 가져오기 작업 중에 액세스된 경우, Rule Update Log(규칙 업데이트 로그)는 빨간색 상태 아이콘( )을 표시하며, Rule Update Log(규칙 업데이트 로그) 상세 보기에서 메시지가 나타나면 이를 볼 수 있습니다. 규칙 업데이트 크기 및 콘텐츠에 따라, 몇 분이 지난 후에 상태 메시지가 표시될 수 있습니다. 자세한 내용은 35-16페이지의 규칙 업데이트 로그 보기를 참고하십시오.

참고 규칙 업데이트를 설치하는 동안 오류 메시지를 수신할 경우 Support(지원팀)에 문의하십시오.

로컬 규칙 파일 가져오기

라이센스: 모두

로컬 규칙은 로컬 컴퓨터에 ASCII 또는 UTF - 8로 인코딩한 일반 텍스트 파일로 가져오는 사용자 지정 표준 텍스트 규칙입니다. Snort 사용자 설명서의 지침을 사용하여 로컬 규칙을 생성할 수 있습니다. 지침은 http://www.snort.org에서 다운로드할 수 있습니다.

로컬 규칙 가져오기에 대해 다음에 유의하십시오.

- 텍스트 파일 이름은 영숫자 및 공백을 포함할 수 있지만 밑줄(_), 마침표(.) 및 대시(-)를 제외한 특수 문자는 포함할 수 없습니다.
- 생성기 ID(GID)를 지정할 필요는 없습니다. 이를 지정할 경우, 표준 텍스트 규칙에 GID 1을, 또는 중요한 데이터 규칙에는 138만을 지정할 수 있습니다.
- 규칙을 처음 가져올 때 Snort ID(SID) 또는 수정 번호를 지정하지 **마십시오**. 그러면 삭제한 규칙을 비롯한 기타 규칙의 SID로 충돌을 방지할 수 있습니다.

  시스템은 해당 규칙에 다음으로 사용 가능한 1000000 이상의 사용자 지정 규칙 SID와 수정 번호 1을 자동으로 할당합니다.
- 이전에 가져온 로컬 규칙의 업데이트된 버전을 가져올 경우에는 **반드시** 현재 수정 번호보다 큰 수정 번호와 시스템이 할당한 SID를 포함해야 합니다.

  현재 로컬 규칙의 수정 번호를 확인하려면, Rule Editor(규칙 편집기) 페이지를 표시하고 로컬 규칙 카테고리를 클릭하여 폴더를 확장한 후 규칙 옆에 있는 **Edit(수정)**를 클릭합니다.
- 시스템이 할당한 SID를 사용하는 규칙 및 현재 수정 번호보다 큰 수정 번호를 가져와 삭제한 로컬 규칙을 복구할 수 있습니다. 로컬 규칙을 삭제하면 시스템에서 자동으로 수정 번호를 증대시킨다는 점에 유의하십시오. 디바이스를 통해 로컬 규칙을 복구할 수 있습니다.

  삭제된 로컬 규칙의 수정 번호를 확인하려면 Rule Editor(규칙 편집기) 페이지를 표시하고 삭제된 규칙 카테고리를 클릭하여 폴더를 확장한 후 규칙 옆에 있는 **Edit(수정)**를 클릭합니다.
- SID가 2147483647보다 큰 규칙이 포함된 규칙 파일은 가져올 수 없습니다. 가져오기가 실패합니다.
- 64자보다 긴 소스 또는 대상 포트 목록을 포함하는 규칙을 가져오는 경우, 가져오기가 실패합니다.
- 시스템은 비활성화된 규칙 상태에 가져오는 로컬 규칙을 항상 설정합니다. 침입 정책에서 이를 사용하려면 먼저 수동으로 로컬 규칙 상태를 설정해야 합니다. 자세한 내용은 20-19페이지의 규칙 상태 설정을 참고하십시오.
- 반드시 파일의 규칙에 Escape 문자가 포함되지 않아야 합니다.
- 규칙 가져오기 도구를 사용하려면 모든 사용자 지정 규칙을 ASCII 또는 UTF - 8 인코딩에서 가져와야 합니다.
- 가져온 모든 로컬 규칙은 로컬 규칙 카테고리에 자동으로 저장됩니다.
- 삭제된 모든 로컬 규칙은 로컬 규칙 카테고리에서 삭제된 규칙 카테고리로 이동합니다.
- 시스템이 단일 파운드 문자(#)로 시작되는 로컬 규칙을 제공합니다.
- 시스템은 2개의 파운드 문자(##)로 시작되는 로컬 규칙은 무시하며 가져오지 않습니다.
- 더 이상 사용되지 않는 `threshold` 키워드를 침입 정책의 침입 이벤트 임계값 설정 기능과 조합하여 사용하는, 가져온 로컬 규칙을 활성화하는 경우 정책 인증이 실패합니다. 자세한 내용은 20-22페이지의 이벤트 임계값 설정 구성을 참고하십시오.

로컬 규칙 파일을 가져오려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택한 후 **Rule Updates(규칙 업데이트)** 탭을 선택합니다.

Rule Updates(규칙 업데이트) 페이지가 나타납니다.

단계 2 **Rule Update or text rule file to upload and install(규칙 업데이트 또는 업로드 및 설치할 텍스트 규칙 파일)**을 선택하고 **Choose File(파일 선택)**을 클릭하여 규칙 파일을 탐색합니다. 이러한 방식으로 업로드된 모든 규칙은 로컬 규칙 카테고리에 저장된다는 점에 유의하십시오.

팁 ASCII 또는 UTF - 8로 인코딩한 일반 텍스트 파일**만** 가져올 수 있습니다.

단계 3 **Import(가져오기)**를 클릭합니다.

규칙 파일을 가져옵니다. 반드시 침입 정책에서 적절한 규칙을 활성화하십시오. 규칙이 적용된 정책을 다음에 적용할 때까지 규칙은 활성화되지 않습니다.

참고 시스템이 확인을 위해 설정된 새 규칙을 사용하지 **않는** 것은 사용자가 침입 정책을 적용할 때까지입니다. 절차는 4-10페이지의 액세스 제어 정책 적용을 참고하십시오.

규칙 업데이트 로그 보기

라이센스: 모두

ASA FirePOWER 모듈은 가져오는 로컬 파일 규칙 및 각 규칙 업데이트에 대한 레코드를 생성합니다.

각 레코드에는 파일을 가져온 사용자의 타임 스탬프, 이름 및 가져오기가 성공 또는 실패되었음을 나타내는 상태 아이콘이 포함됩니다. 가져온 모든 규칙 업데이트 및 로컬 파일 규칙의 목록을 유지할 수 있고, 목록에서 가져온 모든 레코드를 삭제할 수 있으며, 가져온 모든 규칙 및 규칙 업데이트 구성 요소에 대한 세부 레코드에 액세스할 수 있습니다. 다음 표는 Rule Update Log(규칙 업데이트 로그)에서 수행할 수 있는 작업에 대해 설명합니다.

표 35-2 규칙 업데이트 로그 작업

목적	방법
표 열의 내용에 대해 자세히 알아보기	35-17페이지의 규칙 업데이트 로그 표 이해에서 추가 정보를 찾습니다.
파일에 포함된 모든 개체에 대한 세부 레코드를 포함하여 가져오기 로그에서 가져오기 파일 레코드 삭제하기	가져오기 파일의 파일 이름 옆에 있는 삭제 아이콘( )을 클릭합니다. **참고** 로그에서 파일을 삭제해도 가져오기 파일에서 가져온 모든 개체를 삭제하는 것은 아니며, 가져오기 로그 레코드만 삭제합니다.
규칙 업데이트 또는 로컬 파일 규칙에서 가져온 각 개체에 대한 세부 정보 보기	가져오기 파일의 파일 이름 옆에 있는 보기 아이콘( )을 클릭합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 35-17페이지의 규칙 업데이트 로그 표 이해에서는 가져오는 로컬 규칙 파일 및 규칙 업데이트 목록의 필드에 대해 설명합니다.
- 35-18페이지의 규칙 업데이트 가져오기 로그 세부 정보 보기에서는 규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 개체에 대한 세부 레코드에 대해 설명합니다.
- 35-18페이지의 규칙 업데이트 가져오기 로그 상세 보기 이해에서는 Rule Update Log(규칙 업데이트 로그) 상세 보기의 각 필드에 대해 설명합니다.

규칙 업데이트 로그를 보려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택한 후 **Rule Updates(규칙 업데이트)** 탭을 선택합니다.

Rule Updates(규칙 업데이트) 페이지가 나타납니다.

팁 또한 **Import Rules(규칙 가져오기)**를 클릭할 수 있는데, 이는 Rule Editor(규칙 편집기) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 규칙) > Rule Editor(규칙 편집기)**)에서 찾을 수 있습니다.

단계 2 **Rule Update Log(규칙 업데이트 로그)**를 클릭합니다.

Rule Update Log(규칙 업데이트 로그) 페이지가 나타납니다. 이 페이지에서는 가져온 각각의 규칙 업데이트 및 로컬 규칙 파일을 나열합니다.

규칙 업데이트 로그 표 이해

라이센스: 모두

다음 표는 가져오는 로컬 규칙 파일 및 규칙 업데이트 목록의 필드에 대해 설명합니다.

표 35-3 규칙 업데이트 로그 필드

필드	설명
요약	가져오기 파일의 이름입니다. 가져오기가 실패한 경우, 실패 이유에 대한 간략한 설명이 파일 이름 아래에 나타납니다.
시간	가져오기가 시작된 날짜 및 시간입니다.
사용자 ID	가져오기를 시작한 사용자의 사용자 이름입니다.
상태	가져오기 여부: • 성공( ) • 실패 또는 현재 진행 중( ) **팁** 가져오기 작업 진행 중에는 실패했거나 완료되지 않은 가져오기를 나타내는 빨간색 상태 아이콘이 Rule Update Log(규칙 업데이트 로그) 페이지에 나타나고 가져오기가 성공적으로 완료된 경우에만 이 아이콘이 녹색으로 바뀝니다.

규칙 업데이트 또는 파일 이름 옆에 있는 보기 아이콘( )을 클릭하여 Rule Update Log(규칙 업데이트 로그) 상세 페이지에서 규칙 업데이트 또는 로컬 파일을 보거나, 삭제 아이콘( )을 클릭하여 파일에서 가져온 파일 레코드 및 모든 상세 개체 레코드를 삭제합니다.

팁 규칙 업데이트 진행 중에 나타나는 가져오기 세부 정보를 볼 수 있습니다.

규칙 업데이트 가져오기 로그 세부 정보 보기

라이센스: 모두

Rule Update Import Log(규칙 업데이트 가져오기 로그) 상세 보기에서는 규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 개체에 대한 세부 레코드가 나열됩니다. 특정 요건에 일치하는 정보만 포함하는 나열된 레코드로부터 사용자 지정 워크플로 또는 보고서를 생성할 수도 있습니다.

다음 표는 Rule Update Import Log(규칙 업데이트 가져오기 로그) 상세 보기에서 수행할 수 있는 특정 작업에 대해 설명합니다.

표 35-4 규칙 업데이트 가져오기 로그 상세 보기 작업

목적	방법
표 열의 내용에 대해 자세히 알아보기	35-18페이지의 규칙 업데이트 가져오기 로그 상세 보기 이해에서 추가 정보를 찾습니다.

규칙 업데이트 가져오기 로그를 보려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택한 후 **Rule Updates(규칙 업데이트)** 탭을 선택합니다.

Rule Updates(규칙 업데이트) 페이지가 나타납니다.

팁 또한 **Import Rules(규칙 가져오기)**를 클릭할 수 있는데, 이는 Rule Editor(규칙 편집기) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Policies(정책) > Intrusion Policy(침입 규칙) > Rule Editor(규칙 편집기)**)에서 찾을 수 있습니다.

단계 2 **Rule Update Log(규칙 업데이트 로그)**를 클릭합니다.

Rule Update Log(규칙 업데이트 로그) 페이지가 나타납니다.

단계 3 보려는 상세 레코드의 파일 옆에 있는 보기 아이콘( )을 클릭합니다.

세부 레코드의 표 보기가 나타납니다.

규칙 업데이트 가져오기 로그 상세 보기 이해

라이센스: 모두

규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 개체에 대한 세부 레코드를 볼 수 있습니다. 다음 표에는 Rule Update Log(규칙 업데이트 로그) 상세 보기 내 필드에 대해 설명되어 있습니다.

표 35-5 규칙 업데이트 가져오기 로그 상세 보기 필드

필드	설명
시간	가져오기가 시작된 날짜 및 시간입니다.
이름	규칙 Message(메시지) 필드에 해당하는 규칙 및 규칙 업데이트 구성 요소에 대해 가져온 개체의 이름이 구성 요소 이름입니다.
유형	가져온 개체 유형. 다음 중 하나일 수 있습니다. • rule update component(규칙 업데이트 구성 요소)(규칙 팩 또는 정책 팩과 같은 가져온 구성 요소) • rule(규칙)(규칙의 경우, 신규 또는 업데이트된 규칙입니다. 버전 5.0.1에서 이 값이 더 이상 사용되지 않는 update(업데이트) 값을 대체했다는 점에 유의하십시오.) • policy apply(정책 적용)(가져오기를 위해 **Reapply intrusion policies after the Rule Update import completes(규칙 업데이트 가져오기가 완료된 후 침입 정책 재적용)** 옵션이 활성화되었습니다.)
작업	다음 중 하나가 개체 유형에 발생했음을 나타냅니다. • new(신규)(규칙의 경우, 해당 규칙이 ASA FirePOWER 모듈에 처음 저장되었습니다.) • changed(변경됨)(규칙 업데이트 구성 요소 또는 규칙의 경우, 규칙 업데이트 구성 요소가 변경되었거나 규칙이 더 높은 수정 번호 및 동일한 GID 및 SID을 지닙니다.) • collision(충돌)(규칙 업데이트 구성 요소 또는 규칙의 경우, 가져오기의 수정이 기존 구성 요소 또는 규칙과 충돌하므로 가져오기를 건너뜁니다. • deleted(탐지됨)(규칙의 경우, 규칙이 규칙 업데이트에서 삭제되었습니다.) • enabled(활성화됨)(규칙 업데이트 편집의 경우 전처리기, 규칙 및 기타 기능이 시스템에서 제공된 정책에서 활성화되었습니다.) • disabled(비활성화됨)(규칙의 경우, 규칙이 시스템에서 제공된 정책에서 비활성화되었습니다.) • drop(삭제)(규칙의 경우, 규칙이 시스템에서 제공된 정책에서 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되었습니다) • error(오류)(규칙 업데이트 또는 로컬 규칙 파일의 경우, 가져오기가 실패했습니다.) • apply(적용)(가져오기를 위해 **Reapply intrusion policies after the Rule Update import completes(규칙 업데이트 가져오기가 완료된 후 침입 정책 재적용)** 옵션이 활성화되었습니다.)
기본 작업	규칙 업데이트에 의해 정의된 기본 작업. 가져온 개체 유형이 rule(규칙)인 경우, 기본 작업은 Pass(통과), Alert(경고) 또는 Drop(삭제)입니다. 다른 모든 가져온 개체 유형의 경우, 기본 작업이 없습니다.
GID	규칙에 대한 생성기 ID. 예를 들어, 1(표준 텍스트 규칙) 또는 3(공유 객체 규칙)
SID	규칙의 SID.
Rev	규칙의 수정 번호.
정책	가져온 규칙의 경우, 이 필드는 All을 표시하는데, 이는 가져온 규칙이 모든 시스템에서 제공하는 침입 정책에 포함되었음을 나타냅니다. 가져온 개체의 다른 유형의 경우, 이 필드는 비어 있습니다.
세부 사항	구성 요소 또는 규칙에 고유한 문자열. 규칙의 경우, 변경된 규칙의 GID, SID 및 이전 수정 번호이며, previously (GID:SID:Rev)(이전(GID:SID:Rev))로 표시됩니다. 변경되지 않은 규칙의 경우 이 필드는 비어 있습니다.
개수	각 레코드의 개수(1). 표를 제한할 때 표 보기에 Count(개수) 필드가 나타나며, Rule Update Log(규칙 업데이트 로그) 상세 보기는 기본적으로 규칙 업데이트 레코드에 제한됩니다.

위치 정보 데이터베이스 업데이트

라이센스: 모두

Cisco Geolocation Database(위치 정보 데이터베이스, GeoDB)는 라우팅 가능한 IP 주소와 관련된 지리 데이터의 데이터베이스입니다. ASA FirePOWER 모듈은 국가 및 대륙을 제공합니다. 시스템이 탐지된 IP 주소와 일치하는 GeoDB 정보를 탐지하면, 해당 IP 주소와 관련된 위치 정보 정보를 볼 수 있습니다. Cisco는 GeoDB에 주기적인 업데이트를 생성합니다.

GeoDB를 업데이트하려면, Geolocation Updates(위치 정보 업데이트) 페이지(**Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트) > Geolocation Updates(위치 정보 업데이트)**)를 사용합니다. , GeoDB 업데이트를 업로드하면 이 페이지에 나타납니다.

일반적으로 설치하는 데 30~40분이 수요됩니다. GeoDB 업데이트가 다른 시스템 기능(위치 정보의 지속적 수집을 포함하는)을 중단하지 않지만, 업데이트를 완료하는 동안 시스템 리소스를 소모합니다. 업데이트를 예약하는 경우 이를 고려하십시오.

이 섹션에서는 수동 GeoDB 업데이트를 계획하고 수행하는 방법에 대해 설명합니다. GeoDB 업데이트를 예약하기 위해 자동화된 업데이트 기능을 사용할 수 있습니다. 31-6페이지의 위치 정보 데이터베이스 업데이트 자동화를 참고하십시오.

위치 정보 데이터베이스를 업데이트하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Updates(업데이트)**를 선택합니다.

Product Updates(제품 업데이트) 페이지가 나타납니다.

단계 2 **Geolocation Updates(위치 정보 업데이트)** 탭을 클릭합니다.

Geolocation Updates(위치 정보 업데이트) 페이지가 나타납니다.

단계 3 업데이트를 업로드합니다.

- ASA FirePOWER 모듈이 인터넷에 액세스할 수 있는 경우, **Download and install geolocation update from the Support Site(지원 사이트)에서 위치 정보 업데이트 다운로드 및 설치**를 클릭하여 다음 Support Sites(지원 사이트) 중 하나에서 최신 업데이트를 확인합니다:
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)
- ASA FirePOWER 모듈이 인터넷에 액세스할 수 없는 경우, 다음 Support Sites(지원 사이트) 중 하나에서 수동으로 업데이트를 다운로드한 다음 **Upload and install geolocation update(위치 정보 업데이트 업로드 및 설치)**를 클릭합니다. **Choose File(파일 선택)**을 클릭하고 업데이트를 선택한 후 **Import(가져오기)**를 클릭합니다.
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

참고 수동으로, 또는 위치 정보 업데이트 페이지에서 **Download and install geolocation update from the Support Site(지원 사이트에서 위치 정보 업데이트 다운로드 및 설치)**를 클릭하여 Support Sites(지원 사이트)에서 업데이트를 직접 다운로드합니다. 업데이트 파일을 이메일로 전송하는 경우, 손상될 수 있습니다.

업데이트 프로세스가 시작됩니다. 업데이트 설치의 평균 시간은 30~40분입니다. 작업 큐(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 업데이트의 진행 상황을 모니터링할 수 있습니다.

단계 4 업데이트 완료 후, Geolocation Updates(위치 정보 업데이트) 페이지로 돌아가기**를 선택하여** 설치한 업데이트에 GeoDB 구축 번호가 일치하는지 확인합니다.

GeoDB 업데이트는 GeoDB의 이전 버전을 무시하고 즉시 적용됩니다. GeoDB 업데이트가 배포 전반에 적용되는 데는 몇 분 정도 걸릴 수 있지만, 업데이트 후 액세스 제어 정책을 재적용할 필요는 없습니다.

36장 시스템 모니터링

ASA FirePOWER 모듈ASA FirePOWER 모듈은 사용자의 일상적인 시스템 관리를 지원하기 위해 유용한 많은 모니터링 기능을 제공하는데, 한 페이지에서 모두 제공합니다. 예를 들어, Host Statistics(호스트 통계 자료) 페이지에서 기본 호스트 통계 자료를 모니터링할 수 있습니다. 다음 섹션에서는 시스템에서 제공하는 모니터링 기능에 대한 추가 정보를 제공합니다.

- 36-1페이지의 호스트 통계 자료 보기에서는 다음과 같은 호스트 정보를 확인하는 방법에 대해 설명합니다.
- 시스템 가동 시간
- 디스크 및 메모리 사용량
- 시스템 프로세스
- 침입 이벤트 정보
- 36-2페이지의 시스템 상태 및 디스크 공간 사용 모니터링에서는 기본 이벤트 및 디스크 분할 정보를 확인하는 방법에 대해 설명합니다.
- 36-3페이지의 시스템 프로세스 상태 보기에서는 기본 프로세스의 상태를 확인하는 방법에 대해 설명합니다.
- 36-4페이지의 실행 중인 프로세스의 이해에서는 어플라이언스에서 실행되는 기본 시스템 프로세스에 대해 설명합니다.

호스트 통계 자료 보기

라이센스: 모두

Statistics(통계 자료) 페이지는 다음의 현재 상태를 나열합니다.

- 일반적인 호스트 통계 자료. 자세한 내용은 호스트 통계 자료 표를 참고하십시오.
- 침입 이벤트 정보(보호 필요). 26-1페이지의 이벤트 보기 또는 세부 정보를 참고하십시오.

다음 표는 Statistics(통계 자료) 페이지에 나열된 호스트 통계 자료에 대해 설명합니다.

표 36-1 호스트 통계 자료

카테고리	설명
시간	시스템의 현재 시간
실행 시간	시스템이 마지막으로 시작된 후 경과한 날짜 수(해당되는 경우), 시간 및 분
메모리 사용	사용 중인 시스템 메모리의 백분율

표 36-1 호스트 통계 자료 (계속)

카테고리	설명
로드 평균	지난 1분, 5분 15분 동안 CPU 대기열 프로세스의 평균 수.
디스크 사용	사용 중인 디스크의 백분율 자세한 호스트 통계 자료를 보려면 화살표를 클릭합니다. 자세한 내용은 36-2페이지의 시스템 상태 및 디스크 공간 사용 모니터링을 참고하십시오.
프로세스	시스템에서 실행 중인 프로세스의 요약. 자세한 내용은 36-3페이지의 시스템 프로세스 상태 보기를 참고하십시오.

통계 자료 페이지를 보려면 다음을 수행합니다.

단계 1 **Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Statistics(통계 자료)**를 선택합니다.

Statistics(통계 자료) 페이지가 나타납니다.

시스템 상태 및 디스크 공간 사용 모니터링

라이센스: 모두

Statistics(통계 자료) 페이지의 Disk Usage(디스크 사용) 섹션에서는 디스크 사용에 대한 즉각적인 개요를 카테고리 및 파티션 상태별로 제공합니다. 디바이스에 악성코드 스토리지 팩이 설치되어 있는 경우, 스토리지 팩의 파티션 상태도 확인할 수 있습니다. 이 페이지를 자주 모니터링하여 시스템 프로세스와 데이터베이스에 충분한 디스크 공간을 사용할 수 있는지 확인할 수 있습니다.

디스크 사용 정보에 액세스하려면 다음을 수행합니다.

단계 1 **Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Statistics(통계 자료)**를 선택합니다.

Statistics(통계 자료) 페이지가 나타납니다.

디스크 사용량 카테고리에 대한 자세한 내용은 29-3페이지의 디스크 사용량 위젯의 이해를 참고하십시오.

단계 2 이를 확장하려면 **Total(합계)** 옆에 있는 아래쪽 화살표를 클릭합니다.

Disk Usage(디스크 사용) 섹션이 확장되어 파티션 사용이 표시됩니다. 악성코드 스토리지 팩이 설치되어 있는 경우, `/var/storage` 파티션 사용도 표시됩니다.

시스템 프로세스 상태 보기

라이센스: 모두

Host Statistics(호스트 통계 자료) 페이지의 Processes(프로세스) 섹션에서 현재 어플라이언스에서 실행 중인 프로세스를 볼 수 있습니다. 이 섹션에서는 실행되고 있는 각 프로세스에 대한 일반 처리 정보 및 특정 정보를 제공합니다.

다음 표는 프로세스 목록에 표시되는 각 열에 대해 설명합니다.

표 36-2 처리 상태

열	설명
Pid	프로세스 ID 번호
사용자 이름	프로세스를 실행하는 사용자 또는 그룹 이름
Pri	프로세스 우선 순위
Nice	*nice* 값. 프로세스의 예약 우선 순위를 나타내는 값입니다. 값의 범위는 -20(가장 높은 우선 순위)~19(가장 낮은 우선 순위)입니다.
크기	프로세스가 사용하는 메모리 크기(메가바이트를 나타내는 m표시가 없는 경우 킬로바이트 값)
Res	메모리 내 상주 페이징 파일의 볼륨(메가바이트를 나타내는 m표시가 없는 경우 킬로바이트 값)
상태	프로세스 상태: • D — 프로세스가 중단할 수 없는 잠자기 상태에 있습니다(일반적으로 입력/출력). • N — 프로세스가 양수인 nice 값을 지닙니다. • R — 프로세스가 실행 가능합니다(실행을 위해 대기열에서 대기). • S — 프로세스가 절전 모드에 있습니다. • T — 프로세스가 추적 또는 중지되고 있습니다. • W — 프로세스가 호출되고 있습니다. • X — 프로세스가 작동하지 않습니다. • Z — 프로세스가 작동하지 않습니다. • < — 프로세스가 음수인 nice 값을 지닙니다.
시간	프로세스가 실행되고 있는 시간(시간:분:초 단위)
Cpu	프로세스가 사용하고 있는 CPU의 백분율
명령	프로세스의 실행 가능한 이름

프로세스 목록을 확장하려면 다음을 수행합니다.

단계 1 **Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Statistics(통계 자료)**를 선택합니다.

Statistics(통계 자료) 페이지가 나타납니다.

단계 2 **Processes(프로세스)** 옆에 있는 아래쪽 화살표를 클릭합니다.

프로세스 목록이 확장되어 실행되는 작업의 수와 유형, 현재 시간, 현재 시스템 실행 시간, 시스템 로드 평균, CPU, 메모리 및 교체 정보, 각 실행 프로세스에 대한 특정 정보를 포함하는 일반 프로세스 상태 정보를 나열합니다.

Cpu는 다음 CPU 사용 정보를 나열합니다.

- 사용자 처리 사용 백분율
- 시스템 처리 사용 백분율
- nice 사용 백분율(더 높은 우선 순위를 나타내는 음수인 nice 값을 지닌 프로세스의 CPU 사용)

  nice 값은 시스템 프로세스에 대한 예약된 우선순위를 나타내며 -20(가장 높은 우선 순위)에서 19(가장 낮은 우선 순위)까지의 범위에 이를 수 있습니다.
- 유휴 사용 백분율

Mem은 다음 메모리 사용 정보를 나열합니다.

- 메모리 내 총 킬로바이트 수
- 메모리 내 사용된 킬로바이트의 총 수
- 메모리 내 무료 킬로바이트의 총 수
- 메모리 내 버퍼된 킬로바이트의 총 수

Swap(교체)는 다음 교체 사용 정보를 나열합니다.

- 스왑 내 총 킬로바이트 수
- 스왑 내 사용된 킬로바이트의 총 수
- 스왑 내 무료 킬로바이트의 총 수
- 스왑 내 캐시된 킬로바이트의 총 수

참고 어플라이언스에서 실행 중인 프로세스의 유형에 대한 자세한 내용은 36-4페이지의 실행 중인 프로세스의 이해를 참고하십시오.

프로세스 목록을 축소하려면 다음을 수행합니다.

단계 1 **Processes(프로세스)** 옆에 있는 위쪽 화살표를 클릭합니다.

프로세스 목록이 축소됩니다.

실행 중인 프로세스의 이해

라이센스: 모두

어플라이언스에서 실행 중인 프로세스에는 2가지 유형인 데몬 및 실행 파일이 있습니다. 데몬은 항상 실행되며, 실행 파일은 필요한 경우 실행됩니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 36-5페이지의 시스템 데몬 이해
- 36-6페이지의 실행 파일 및 시스템 유틸리티 이해

시스템 데몬 이해

라이센스: 모두

데몬은 어플라이언스에서 계속 실행됩니다. 데몬은 필요한 경우 서비스의 가용성을 확인하고 프로세스를 생성합니다. 다음 표에서는 Process Status(처리 상태) 페이지에서 볼 수 있는 데몬을 나열하고 해당 기능에 대한 간단한 설명을 제공합니다.

참고 아래 표는 어플라이언스에서 실행할 수 있는 모든 프로세스의 전체 목록이 아닙니다.

표 36-3 시스템 데몬

데몬	설명
crond	예약된 명령의 실행을 관리합니다(cron 작업).
dhclient	동적 호스트 IP 주소 부여를 관리합니다.
httpd	HTTP(Apache 웹 서버) 프로세스를 관리합니다.
httpsd	HTTPS(SSL를 사용하는 Apache 웹 서버) 서비스를 관리하고 작동하는 SSL 및 유효한 인증서 인증을 확인하며, 어플라이언스에 보안 웹 액세스를 제공하는 백그라운드에서 실행됩니다.
keventd	Linux 커널 이벤트 알림 메시지를 관리합니다.
klogd	Linux 커널 메시지의 차단 및 로깅을 관리합니다.
kswapd	Linux 커널 스왑 메모리를 관리합니다.
kupdated	디스크 동기화를 수행하는 Linux 커널 업데이트 프로세스를 관리합니다.
mysqld	ASA FirePOWER 모듈 데이터베이스 프로세스를 관리합니다.
ntpd	NTP(Network Time Protocol)프로세스를 관리합니다
pm	모든 Cisco 프로세스를 관리하고 필요한 프로세스를 시작하며, 예기치 않게 실패한 모든 프로세스를 다시 시작합니다.
reportd	보고서를 관리합니다.
safe_mysqld	데이터베이스의 안전 모드 운영을 관리하고 오류가 발생하고 파일에 런타임 정보를 로깅할 경우 데이터베이스 데몬을 다시 시작합니다.
sfmgr	어플라이언스로 향하는 sftunnel 연결을 사용하여 어플라이언스의 원격 관리 및 구성을 위한 RPC 서비스를 제공합니다.
sftroughd	수신 소켓에서 연결을 수신한 후 요청을 처리하기 위해 올바른 실행 파일(일반적으로 Cisco 메시지 브로커, sfmb)을 호출합니다.
sftunnel	원격 어플라이언스와의 통신이 필요한 모든 프로세스에 안전한 커뮤니케이션 채널을 제공합니다.
sshd	SSH(Secure Shell) 프로세스를 관리하고 어플라이언스에 SSH 액세스를 제공하는 백그라운드에서 실행됩니다.
syslogd	시스템 로깅(syslog) 프로세스를 관리합니다.

실행 파일 및 시스템 유틸리티 이해

라이센스: 모두

다른 프로세스에 의해 또는 사용자 작업을 통해 수행될 때 실행되는 시스템에는 많은 실행 파일이 있습니다. 다음 표는 Process Status(처리 상태) 페이지에서 볼 수 있는 실행 파일에 대해 설명합니다.

표 36-4 시스템 실행 파일 및 유틸리티

실행 파일	설명
awk	awk 프로그래밍 언어로 작성된 프로그램을 실행하는 유틸리티입니다.
bash	GNU Bourne-Again 셸
cat	파일을 읽고 표준 출력에 콘텐츠를 작성하는 유틸리티입니다.
chown	사용자 및 그룹 파일 권한을 변경하는 유틸리티입니다.
chsh	기본 로그인 셸을 변경하는 유틸리티입니다.
cp	파일을 복제하는 유틸리티입니다.
df	어플라이언스의 여유 공간에 대한 볼륨을 나열하는 유틸리티입니다.
echo	표준 출력에 콘텐츠를 작성하는 유틸리티입니다.
egrep	지정된 입력에 대한 파일 및 폴더를 검색하는 유틸리티이며, 표준 grep에서 지원되지 않는 확장된 정규식 집합을 지원합니다.
find	지정된 입력에 대한 디렉토리를 되풀이하여 검색하는 유틸리티입니다.
grep	지정된 입력에 대한 파일 및 디렉토리를 검색하는 유틸리티입니다.
halt	서버를 중지하는 유틸리티입니다.
httpsdctl	보안 Apache 웹 프로세스를 처리합니다.
hwclock	하드웨어 클럭에 대한 액세스를 허용하는 유틸리티입니다.
ifconfig	네트워크 구성 실행 파일을 나타냅니다. MAC 주소가 일정한 상태를 유지하는지 확인합니다.
iptables	Access Configuration(액세스 구성) 페이지에 적용된 변경 사항에 기반하여 액세스 제한을 처리합니다. 액세스 구성에 대한 자세한 내용은 32-4페이지의 사용자 어플라이언스의 액세스 목록 구성을 참고하십시오.
iptables-restore	iptables 파일 복원을 처리합니다
iptables-save	iptables에 저장된 변경 사항을 처리합니다.
kill	세션 및 프로세스를 종료하는 데 사용할 수 있는 유틸리티입니다.
killall	모든 세션 및 프로세스를 종료하는 데 사용할 수 있는 유틸리티입니다
ksh	Korn 셸의 공개 도메인 버전입니다.
logger	명령줄에서 syslog 데몬에 액세스하는 방법을 제공하는 유틸리티입니다.
md5sum	지정된 파일에 대한 체크섬 및 블록 횟수를 인쇄하는 유틸리티입니다.
mv	파일을 옮기는 (재명명하는) 유틸리티입니다
myisamchk	데이터베이스 표 확인 및 복구를 나타냅니다.
mysql	데이터베이스 프로세스를 나타내며 여러 인스턴스가 표시될 수 있습니다.
openssl	인증서 인증 생성을 나타냅니다.
perl	perl 프로세스를 나타냅니다.

표 36-4 시스템 실행 파일 및 유틸리티 (계속)

실행 파일	설명
ps	표준 출력에 처리 정보를 작성하는 유틸리티입니다.
sed	하나 이상의 텍스트 파일을 수정하는 데 사용하는 유틸리티입니다.
sh	Korn 셸의 공개 도메인 버전입니다.
shutdown	어플라이언스를 종료하는 유틸리티입니다.
sleep	지정된 시간(초)동안 프로세스를 중지하는 유틸리티입니다.
smtpclient	이메일 이벤트 알림 기능이 활성화된 경우 이메일 전송을 처리하는 메일 클라이언트입니다.
snmptrap	SNMP 알림 기능이 활성화된 경우 지정된 SNMP 트랩 서버에 SNMP 트랩 데이터를 전달합니다.
snort (보호가 필요함)	Snort가 실행되고 있음을 나타냅니다.
ssh	어플라이언스로 향하는 SSH(Secure Shell) 연결을 나타냅니다.
sudo	관리자가 아닌 사용자가 실행 파일을 실행할 수 있는 sudo 프로세스를 나타냅니다.
top	상위 CPU 프로세스에 대한 정보를 표시하는 유틸리티입니다.
touch	지정된 파일의 액세스 및 변경 횟수를 변경하는 데 사용할 수 있는 유틸리티입니다.
vim	텍스트 파일을 수정하는 데 사용하는 유틸리티입니다.
wc	지정된 파일에서 회선, 단어 및 바이트 계산을 수행하는 유틸리티입니다.

37 장

백업 및 복원 사용

백업 및 복원은 시스템 유지 계획의 핵심적인 부분입니다. 각 조직의 백업 계획은 매우 개별화되어 있지만, ASA FirePOWER 모듈은 에서 가져온 데이터가 재해 시 복원될 수 있도록 하기 위해서 데이터를 보관하는 메커니즘을 제공합니다.

백업 및 복원에 대한 다음 제한을 참고하십시오.

- 백업은 사용자가 만드는 제품 버전에만 유효합니다.
- 백업을 생성하기 위해 사용된 것과 동일한 버전의 ASA FirePOWER 모듈 소프트웨어를 실행하는 경우에만 백업을 복원할 수 있습니다.

주의 ASA FirePOWER 모듈 간 구성 파일을 복사하기 위해 백업 및 복원 프로세스를 사용하지 마십시오. 구성 파일은 ASA FirePOWER 모듈을 고유하게 식별하고 공유할 수 없는 정보를 포함합니다.

주의 모든 침입 규칙 업데이트를 적용한 경우, 해당 업데이트는 백업되지 않습니다. 복원 **후** 최신 규칙 업데이트를 적용해야 합니다.

어플라이언스 또는 로컬 컴퓨터에 백업 파일을 저장할 수 있습니다.

자세한 내용은 다음 섹션을 참고하십시오.

- 백업 파일 생성에 대한 자세한 내용은 37-2페이지의 백업 파일 생성을 참고하십시오.
- 나중에 백업 생성을 위해 템플릿으로 사용할 수 있는 백업 프로파일 생성에 대한 자세한 내용은 37-3페이지의 백업 프로파일 생성을 참고하십시오.
- 로컬 호스트에서 백업 파일 업로드에 대한 내용은 37-4페이지의 로컬 호스트에서 백업 업로드를 참고하십시오.
- 어플라이언스에 백업 파일을 복원하는 방법에 대한 내용은 37-4페이지의 백업 파일로부터 어플라이언스 복원을 참고하십시오.

백업 파일 생성

라이센스: 모두

모듈 인터페이스를 사용하여 ASA FirePOWER 모듈의 백업을 수행할 수 있습니다. 기존의 시스템 백업을 살펴보고 사용하려면 Backup Management(백업 관리) 페이지를 확인합니다. 이벤트 데이터 이외에 정기적으로 어플라이언스를 복원하는 데 필요한 구성 파일을 모두 포함하는 백업 파일을 저장해야 합니다. 구성 변경을 테스트할 때 필요하다면 저장된 구성으로 되돌릴 수 있도록 시스템 백업을 원할 수도 있습니다. 선택적으로 어플라이언스 또는 로컬 컴퓨터에 백업 파일을 저장할 수 있습니다.

어플라이언스에 충분한 디스크 공간이 없는 경우 백업 파일을 만들 수 없습니다. 백업 절차가 사용 가능한 디스크 공간의 90% 이상을 사용할 경우 백업이 실패할 수 있습니다. 필요한 경우, 이전 백업 파일을 삭제하거나, 어플라이언스에서 이전 백업 파일을 이동합니다.

대안적으로, 백업 파일이 4GB보다 큰 경우 SCP를 통해 원격 호스트에 이를 복사합니다. 로컬 컴퓨터의 백업을 업로드하면 4GB보다 큰 백업 파일에서는 작동하지 않습니다. 이는 .

주의 보안 영역으로 모든 인터페이스 연결을 구성한 경우, 이 연결은 백업되지 않습니다. 복원 후 이를 재설정해야 합니다. 자세한 내용은 2-33페이지의 보안 영역 작업을 참고하십시오.

ASA FirePOWER 모듈의 백업 파일을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Backup/Restore(백업/복원)**를 선택합니다.

Backup Management(백업 관리) 페이지가 나타납니다.

단계 2 **Device Backup(디바이스 백업)**을 클릭합니다.

Create Backup(백업 생성) 페이지가 나타납니다.

단계 3 **Name(이름)** 필드에 백업 파일 이름을 입력합니다. 영숫자, 기호 및 스페이스를 사용할 수 있습니다.

단계 4 선택적으로, 백업이 완료되면 알림을 받기 위해서는 **Email(이메일)** 확인 상자를 선택하고 관련 텍스트 상자에 이메일 주소를 입력합니다.

참고 이메일 알림을 수신하려면, 32-7페이지의 메일 릴레이 호스트 및 알림 주소 구성에 설명된 대로 릴레이 호스트를 구성해야 합니다.

단계 5 선택적으로, SCP(Secure Copy)를 사용하여 다른 시스템에 백업 아카이브를 복사하려면 **Copy when complete(완료 시 복사)** 확인 상자를 선택한 후 동반 텍스트 상자에 다음 정보를 입력합니다.

- **Host(호스트)** 필드. 호스트 이름 또는 백업을 복사하고자 하는 컴퓨터의 IP 주소
- **Path(경로)** 필드. 백업을 복사하고자 하는 디렉터리 경로
- **User(사용자)** 필드. 원격 시스템에 로그온하는 데 사용하려는 사용자 이름
- **Password(비밀번호)** 필드. 해당 사용자 이름에 대한 비밀번호
  비밀번호 대신 SSH 공유 키로 원격 시스템에 액세스하는 것을 선호하는 경우, **SSH Public Key(SSH 공유 키)** 필드의 내용을 해당 시스템에서 지정된 사용자의 `authorized_keys` 파일에 복사해야 합니다.

이 옵션이 선택되지 않은 상태에서 시스템은 원격 서버 백업 중에 사용되는 임시 파일을 저장합니다. 이 옵션을 선택하면 임시 파일은 원격 서버에 저장되지 **않습니다**.

팁 Cisco는 시스템 장애 시 어플라이언스가 복원될 수 있도록 원격 위치에 정기적으로 백업을 저장할 것을 권장합니다.

단계 6 다음 옵션을 이용할 수 있습니다.

- 어플라이언스에 백업 파일을 저장하려면, **Start Backup(백업 시작)**을 클릭합니다.

  백업 파일이 `/var/sf/backup` 디렉터리에 저장됩니다.

  백업 프로세스가 완료되면, Restoration Database(데이터베이스 복원) 페이지에서 파일을 볼 수 있습니다. 백업 파일 검색에 대한 자세한 내용은 37-4페이지의 백업 파일로부터 어플라이언스 복원을 참고하십시오.

- 이 구성을 나중에 사용할 수 있는 백업 프로파일로 저장하려면, **Save As New(새 이름으로 저장)**를 클릭합니다.

  Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Backup/Restore(백업/복원)를 선택한 후 **Backup Profiles(백업 파일)**를 클릭하여 백업 파일을 수정하거나 삭제할 수 있습니다. 자세한 내용은 37-3페이지의 백업 프로파일 생성을 참고하십시오.

백업 프로파일 생성

라이센스: 모두

백업 프로파일 페이지를 사용하여 사용자가 백업의 다른 유형에 대해 사용하고자 하는 설정을 포함하는 백업 프로필을 생성할 수 있습니다. 어플라이언스에 파일을 백업할 때 이러한 프로파일 중 하나를 선택할 수 있습니다.

팁 37-2페이지의 백업 파일 생성에 설명된 대로 백업 파일을 만들면, 백업 프로파일이 자동으로 생성됩니다.

백업 프로파일을 생성하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Backup/Restore(백업/복원)**를 선택합니다.

Backup Management(백업 관리) 페이지가 나타납니다.

단계 2 **Backup Profiles(백업 프로파일)** 탭을 클릭합니다.

기존 백업 프로파일 목록과 함께 Backup Profiles(백업 프로파일) 페이지가 나타납니다.

팁 수정아이콘( )을 클릭하여 기존 프로파일을 수정하거나 삭제 아이콘( )을 눌러 목록에서 프로파일을 삭제할 수 있습니다.

단계 3 **Create Profile(프로파일 생성)**을 클릭합니다.

Create Backup(백업 생성) 페이지가 나타납니다.

단계 4 백업 프로파일 이름을 입력합니다. 영숫자, 기호 및 스페이스를 사용할 수 있습니다.

단계 5 필요에 따라 백업 프로파일을 구성합니다.

이 페이지의 옵션에 대한 자세한 내용은 37-2페이지의 백업 파일 생성을 참고하십시오.

단계 6 백업 프로파일을 저장하려면 **Save As New(새 이름으로 저장)**를 클릭합니다.

Backup Profiles(백업 프로파일) 페이지가 표시되고 새 프로파일이 목록에 나타납니다.

로컬 호스트에서 백업 업로드

라이센스: 모두

백업 관리 표에 설명된 다운로드 기능을 사용하여 로컬 호스트에 백업 파일을 다운로드할 경우, ASA FirePOWER 모듈에 업로드할 수 있습니다.

백업 파일이 PKI 개체를 포함하는 경우, 내부 CA 인증서와 연결된 개인 키와 내부 인증 개체는 임의로 생성된 키로 업로드 시 다시 암호화됩니다.

팁 로컬 호스트에서 4GB보다 큰 백업을 업로드할 수 없습니다. 대안으로, SCP를 통해 백업을 원격 호스트에 복사하고 해당 호스트에서 이를 검색합니다.

로컬 호스트에서 백업을 업로드하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Backup/Restore(백업/복원)**를 선택합니다.

Backup Management(백업 관리) 페이지가 나타납니다.

단계 2 **Upload Backup(백업 업로드)**을 클릭합니다.

Upload Backup(백업 업로드) 페이지가 나타납니다.

단계 3 **Choose File(파일 선택)**을 클릭하고 업로드할 백업 파일을 탐색합니다.

업로드할 파일을 선택한 후, **Upload Backup(백업 업로드)**을 클릭합니다.

단계 4 Backup Management(백업 관리) 페이지로 돌아가려면 **Backup Management(백업 관리)**를 클릭합니다.

백업 파일이 업로드되어 백업 목록에 나타납니다. ASA FirePOWER 모듈이 파일 무결성을 확인한 후, Backup Management(백업 관리) 페이지를 새로 고침하여 파일 시스템 세부 정보를 나타냅니다.

백업 파일로부터 어플라이언스 복원

라이센스: 모두

Backup Management(백업 관리) 페이지를 사용하여 백업 파일의 어플라이언스를 복원할 수 있습니다. 백업을 복원하려면, 백업 파일의 VDB 버전은 반드시 어플라이언스의 현재 VDB 버전과 일치해야 합니다. 복원 프로세스를 완료한 후, **반드시** 최신 Cisco 규칙 업데이트를 적용해야 합니다.

로컬 스토리지를 사용할 경우, 백업 파일은 `/var/sf/backup`에 저장되는데, 이는 Backup Management(백업 관리) 페이지 하단에 위치한 `/var` 파티션에 사용된 디스크 공간의 양으로 나열됩니다.

참고 백업이 완료된 후 라이센스를 추가할 경우, 이 라이센스는 백업이 복구된다고 해도 제거되거나 덮어써지지 않습니다. 복원 시 충돌을 방지하려면 백업을 복원하기 전에 라이센스가 어디에 사용되었는지에 유의하여 해당 라이센스를 제거합니다. 그리고 백업을 복원한 후 라이센스를 추가하고 재구성합니다. 충돌이 발생하면 Support(지원부)에 문의하십시오.

다음 표는 Backup Management(백업 관리) 페이지에서 각 열 및 아이콘에 대해 설명합니다.

표 37-1 백업 관리

기능	설명
시스템 정보	시작 어플라이언스의 이름, 유형 및 버전. 동일한 어플라이언스 유형 및 버전에서만 백업을 복원할 수 있습니다.
생성 날짜	백업 파일을 생성한 날짜 및 시간
파일 이름	백업 파일의 전체 이름
VDB 버전	백업 시 어플라이언스에서 실행되는 취약성 데이터베이스(VDB)의 구조
위치	백업 파일의 위치
크기(MB)	백업 파일의 크기(메가바이트로 표시)
보기	압축 백업 파일에 포함된 파일 목록을 보려면 백업 파일의 이름을 클릭합니다.
복원	선택된 백업 파일을 클릭하여 어플라이언스에서 복원합니다. 사용자의 VDB 버전이 백업 파일의 VDB 버전에 일치하지 않는 경우, 이 옵션은 비활성화됩니다.
다운로드	선택한 백업 파일을 클릭하여 로컬 컴퓨터에 저장합니다.
삭제	선택한 백업 파일을 클릭하여 삭제합니다.
이동	이전에 생성한 로컬 백업을 선택한 경우, 클릭하여 지정된 원격 백업 위치에 백업을 보냅니다.

백업 파일의 어플라이언스를 복원하려면 다음을 수행합니다.

단계 1 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Backup/Restore(백업/복원)**를 선택합니다.

Backup Management(백업 관리) 페이지가 나타납니다.

단계 2 백업 파일의 내용을 보려면, 파일의 이름을 클릭합니다.

매니페스트가 나타나고 각 파일의 이름, 해당 소유자 및 권한과 파일 크기 및 날짜가 나열됩니다.

단계 3 Backup Management(백업 관리) 페이지로 돌아가려면 **Backup Management(백업 관리)**를 클릭합니다.

단계 4 복원하려는 백업 파일을 선택하고 **Restore(복원)**를 클릭합니다.

Restore Backup(백업 복원) 페이지가 나타납니다.

현재 어플라이언스에 설치된 VDB 버전이 백업의 VDB 버전과 일치하지 않는 경우, **Restore(복원)** 단추는 사용할 수 없습니다.

주의 이 절차는 모든 구성 파일 및 모든 이벤트 데이터를 덮어씁니다.

단계 5 파일을 복원하려면 하나 또는 모두를 선택합니다.

- **구성 데이터 대체**
- **이벤트 데이터 복원**

단계 6 **Restore(복원)**를 클릭하여 복원을 시작합니다.

어플라이언스는 사용자가 지정한 백업 파일을 사용하여 복원됩니다.

단계 7 어플라이언스를 재부팅합니다.

단계 8 규칙 업데이트를 다시 적용하려면 최신 Cisco 규칙 업데이트를 적용합니다.

단계 9 복구 시스템에 모든 액세스 제어, 침입 및 시스템 정책을 다시 적용합니다.

문제 해결 파일 생성

경우에 따라 어플라이언스에 문제가 발생하면 Support(지원팀)이 문제 진단에 도움이 될 수 있도록 문제 해결 파일을 생성하도록 요청할 수 있습니다. 다음 표에 나열된 옵션을 모두 선택하여 ASA FirePOWER 모듈이 보고하는 문제 해결 데이터를 사용자 정의할 수 있습니다.

표 A-1 선택 가능한 문제 해결 옵션

옵션	보고 내용
Snort 성능 및 구성	어플라이언스의 Snort에 관련된 데이터 및 구성 설정
하드웨어 성능 및 로그	어플라이언스 하드웨어의 성능에 관련된 데이터 및 로그
시스템 구성, 정책 및 로그	어플라이언스의 현재 시스템 구성에 관련된 구성 설정, 데이터 및 로그
탐지 구성, 정책 및 로그	어플라이언스의 탐지에 관련된 구성 설정, 데이터 및 로그
인터페이스 및 네트워크 관련 데이터	어플라이언스의 인라인 집합 및 네트워크 구성에 관련된 구성 설정, 데이터 및 로그
검색, 인식, VDB 데이터 및 로그	어플라이언스의 현재 검색 및 인식 구성에 관련된 구성 설정, 데이터 및 로그
데이터 및 로그 업그레이드	어플라이언스의 이전 업그레이드와 관련된 데이터 및 로그
모든 데이터베이스 데이터	문제 해결 보고서에 포함된 모든 데이터베이스 관련 데이터
모든 로그 데이터	어플라이언스 데이터베이스에 의해 수집된 모든 로그
네트워크 맵 정보	현재 네트워크 토폴로지 데이터

일부 옵션은 보고하는 데이터의 측면에서 겹치지만, 문제 해결 파일은 선택하는 옵션에 관계없이 중복된 사본을 포함하지 않는다는 점에 유의하십시오.

자세한 내용은 다음 섹션을 참고하십시오.

- A-2페이지의 어플라이언스 문제 해결 파일 생성
- A-2페이지의 문제 해결 파일 다운로드

어플라이언스 문제 해결 파일 생성

라이센스: 모두

다음 절차를 사용하여 사용자가 Support(지원팀)에 전송할 수 있는 사용자 지정 문제 해결 파일을 생성합니다.

문제 해결 파일을 생성하려면 다음을 수행합니다.

단계 1 ASDM에서 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Troubleshooting(문제 해결)**을 선택합니다.

단계 2 **Generate Troubleshooting Files(문제 해결 파일 생성)**를 클릭합니다.

Troubleshooting Options(문제 해결 옵션) 팝업 창이 표시됩니다.

단계 3 **All Data(모든 데이터)**를 선택하여 가능한 문제 해결 데이터를 모두 생성하거나, 개별 확인 상자를 선택하여 보고서를 사용자 정의합니다. 자세한 내용은 선택 가능한 문제 해결 옵션 표를 참고하십시오.

단계 4 **OK(확인)**를 클릭합니다.

ASA FirePOWER 모듈은 문제 해결 파일을 생성합니다. 작업 큐(**Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**)에서 파일 생성 프로세스를 모니터링할 수 있습니다.

단계 5 다음 섹션인, 문제 해결 파일 다운로드에서 절차를 계속 진행합니다.

문제 해결 파일 다운로드

라이센스: 모두

다음 절차를 사용하여 생성된 문제 해결 파일의 복사본을 다운로드합니다.

문제 해결 파일을 다운로드하려면 다음을 수행합니다.

단계 1 ASDM에서 **Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**를 선택합니다.

Task Status(작업 상태) 페이지가 나타납니다.

단계 2 사용자가 생성한 문제 해결 파일에 해당하는 작업을 찾습니다.

단계 3 어플라이언스가 문제 해결 파일을 생성하고 작업 상태가 `Completed`로 변경된 후 **Click to retrieve generated files(생성된 파일을 검색하려면 클릭)**를 클릭합니다.

단계 4 파일을 다운로드하려면 브라우저의 프롬프트를 따릅니다.

파일이 단일 `.tar.gz` 파일에 다운로드됩니다.

단계 5 Cisco에 문제 해결 파일을 보내려면 Support(지원팀)의 지시에 따르십시오.

구성 가져오기 및 내보내기

가져오기/내보내기 기능을 사용하면 정책을 비롯한 여러 유형의 구성을 한 어플라이언스에서 동일한 유형의 다른 어플라이언스로 복사할 수 있습니다. 구성 가져오기 및 내보내기는 백업 도구용이 아니지만 새로운 ASA FirePOWER 모듈에 사용될 수 있습니다.

다음 구성을 가져오고 내보낼 수 있습니다.

- 액세스 제어 정책 및 관련 네트워크 분석 및 파일 정책
- 침입 정책
- 시스템 정책
- 알림 응답

내보낸 구성을 가져오려면 ASA FirePOWER 모듈 모두 동일한 소프트웨어 버전을 실행해야 합니다. 내보낸 침입 또는 액세스 제어 정책을 가져오려면, 두 어플라이언스 모두에서 규칙 업데이트 버전 또한 일치해야 합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- B-1페이지의 구성 내보내기
- B-3페이지의 구성 가져오기

구성 내보내기

라이센스: 모두

단일 구성을 내보낼 수도 있고, 동일한 유형 또는 서로 다른 유형의 구성 집합을 동시에 내보낼 수도 있습니다. 나중에 패키지를 다른 어플라이언스로 가져올 때 패키지의 어떤 구성을 가져올지 선택할 수 있습니다.

구성을 내보낼 때 어플라이언스는 해당 구성의 개정 정보도 내보냅니다. ASA FirePOWER 모듈은 다른 어플라이언스에 구성을 가져올 수 있는지 여부를 확인하기 위해 해당 정보를 사용합니다. 어플라이언스에 이미 존재하는 구성 수정 사항을 가져올 수 없습니다.

또한, 구성을 내보낼 때 어플라이언스는 또한 구성이 종속된 시스템 구성을 내보냅니다..

팁 ASA FirePOWER 모듈의 많은 목록 페이지는 목록 항목 옆에 있는 내보내기 아이콘( )을 포함합니다. 이 아이콘이 있으면 내보내기 절차의 빠른 대안으로서 사용할 수 있습니다.

다음 구성을 내보낼 수 있습니다.

- *알림 응답* — 알림 응답은 알림을 전송할 외부 시스템과 ASA FirePOWER 모듈이 상호 작용할 수 있는 구성 집합입니다.
- *액세스 제어 정책* — 액세스 제어 정책에는 시스템이 네트워크 트래픽을 관리하는 방법을 결정하기 위해 구성할 수 있는 다양한 요소가 포함됩니다. 이 구성 요소에는 액세스 제어 규칙, 관련 침입, 파일 및 네트워크 분석 정책, 그리고 침입 변수 집합을 포함하여 규칙과 정책에서 사용하는 객체가 포함됩니다. 액세스 제어 정책을 내보낼 경우 (현재) URL 평판 및 카테고리를 제외한 정책의 모든 설정 및 구성 요소를 내보내는데, 이는 모든 플라이언스에 동등한 것이며 사용자가 변경할 수 없는 것입니다. 액세스 제어 정책을 가져오려면 ASA FirePOWER 모듈을 내보내고 가져오는 규칙 업데이트 버전이 반드시 일치해야 합니다.

  사용자가 내보내는 액세스 제어 정책이 위치 정보 데이터를 참조하는 규칙을 포함하는 경우, 모듈의 위치 정보 데이터베이스(GeoDB) 업데이트 버전 가져오기가 사용됩니다.
- *침입 정책* — 침입 정책에는 침입 및 정책 위반 탐지를 목적으로 네트워크 트래픽을 검사하기 위해 구성할 수 있는 다양한 요소가 포함됩니다. 이러한 구성 요소는 프로토콜 헤더 값, 페이로드 내용 및 특정 패킷 크기 특성을 검사하는 침입 규칙 및 기타 고급 설정으로 구성됩니다.

  침입 정책을 내보내면 정책에 대한 모든 설정도 내보내게 됩니다. 예를 들어, 이벤트를 생성하는 규칙 설정을 선택하거나, 규칙을 위해 SNMP 경고를 설정하거나 정책에서 중요한 데이터 전처리기를 켜두는 경우, 이 설정은 내보낸 정책에 계속 남아 있습니다. 사용자 지정 규칙, 사용자 지정 규칙 분류 및 사용자가 정의한 변수도 정책과 함께 내보내집니다.

  두 번째 침입 정책과 공유되는 레이어를 사용하는 침입 정책을 내보내는 경우, 해당 공유 레이어는 내보내는 정책에 복사되며 공유 관계는 해제됩니다. 다른 어플라이언스로 침입 정책을 가져오면, 레이어를 삭제, 추가 및 공유하는 등 가져온 정책을 필요에 맞게 수정할 수 있습니다.

  하나의ASA FirePOWER 모듈에서 다른 하나로 침입 정책을 내보내는 경우, 두 번째 ASA FirePOWER 모듈이 기본 변수를 다르게 구성했다면 가져온 정책이 다르게 작동할 수 있습니다.

  참고 가져오기/내보내기 기능은 VRT(Vulnerability Research Team)에서 생성한 규칙을 업데이트하는 데 사용할 수 없습니다. 대신, 최신 규칙 업데이트 버전을 다운로드하고 적용합니다(35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기 참고).

- *시스템 정책* — 시스템 정책은 ASA FirePOWER 모듈의 측면(사용자 배포의 다른 ASA FirePOWER 모듈과 유사할 가능성이 있음)을 제어합니다. 여기에는 시간 설정, SNMP 설정 등이 포함됩니다.

참고 내보내는 구성 수 및 그러한 구성이 참조하는 객체의 수에 따라 내보내기 프로세스가 몇 분 정도 걸릴 수 있습니다.

하나 이상의 구성을 내보내려면 다음을 수행합니다.

단계 1 사용자가 구성을 내보내는 ASA FirePOWER 모듈 사용자가 구성을 가져오려고 계획하는 ASA FirePOWER 모듈이 동일한 버전을 실행하는지 확인합니다. 침입 또는 액세스 제어 정책을 내보내는 경우, 규칙 업데이트 버전이 일치하는지 확인합니다.

ASA FirePOWER 모듈의 버전(및 해당하는 경우, 규칙 업데이트 버전)이 일치하지 않는 경우, 가져오기가 실패하게 됩니다.

단계 2 **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Import Export(가져오기 내보내기)**를 선택합니다.

Import/Export(가져오기/내보내기) 페이지가 나타나며, 여기에는 ASA FirePOWER 모듈의 구성 목록이 포함되어 있습니다. 내보낼 구성이 없는 구성 카테고리는 이 목록에 나타나지 않습니다.

팁 구성 목록을 축소하려면 구성 옆에 있는 축소 아이콘()을 클릭합니다. 구성을 표시하려면 구성 옆에 있는 폴더 확장 아이콘()을 클릭합니다.

단계 3 내보낼 구성 옆에 있는 확인란을 선택한 다음 **Export(내보내기)**를 클릭합니다.

단계 4 컴퓨터에 내보낸 패키지를 저장하려면 프롬프트를 따릅니다.

구성 가져오기

라이센스: 모두

어플라이언스에서 구성을 내보냈으면, 이를 지원하는 다른 어플라이언스로 가져올 수 있습니다.

가져오는 구성 유형에 따라 다음 사항에 유의해야 합니다.

- 구성을 가져오는 ASA FirePOWER 모듈이 구성을 내보내는 데 사용한 ASA FirePOWER 모듈과 동일한 버전을 실행하고 있는지 확인해야 합니다. 침입 또는 액세스 제어 정책을 가져오려면 두 어플라이언스의 규칙 업데이트 버전도 일치해야 합니다. 버전이 일치하지 않으면 가져오기가 실패합니다.
- 영역에 따라 트래픽을 평가하는 액세스 제어 정책을 가져오는 경우 가져온 정책 내 영역을 ASA FirePOWER 모듈을 가져오는 영역과 매핑해야 합니다. 영역을 매핑할 경우, 해당 유형이 일치해야 합니다. 따라서, 가져오기를 시작하기 전에 ASA FirePOWER 모듈을 가져오는 데 필요한 모든 영역 유형을 생성해야 합니다. 보안 영역에 대한 자세한 내용은 2-33페이지의 보안 영역 작업을 참조하십시오.
- 기존 객체 또는 그룹과 같은 이름을 가진 객체 또는 객체 그룹을 포함하는 액세스 제어 정책을 가져오는 경우, 객체 또는 그룹 이름을 변경해야 합니다.
- 액세스 제어 정책 또는 침입 정책을 가져오는 경우, 가져오기 프로세스는 기본 변수 값 집합의 기존 기본 변수 값을 가져온 기본 변수 값으로 대체합니다. 기존 기본 변수 값 집합이 가져온 기본 변수 값 집합에 없는 사용자 지정 변수를 포함하는 경우, 고유 변수는 유지됩니다.
- 두 번째 침입 정책에서 공유 레이어를 사용하는 침입 정책을 가져오는 경우, 내보내기 프로세스는 공유 관계를 중단하고 이전에 공유된 레이어는 패키지로 복사됩니다. 즉 가져온 침입 정책은 공유된 레이어를 포함하지 않습니다.

참고 가져오기/내보내기 기능을 사용하여 VRT(취약성 연구단)가 만든 규칙을 업데이트할 수 없습니다. 대신, 최신 규칙 업데이트 버전을 다운로드하고 적용합니다(35-9페이지의 규칙 업데이트 및 로컬 규칙 업데이트 가져오기 참고).

ASA FirePOWER 모듈단일 패키지에서 여러 구성을 내보낼 수 있으므로, 패키지를 가져오는 경우 패키지의 어떤 구성을 가져올지 선택해야 합니다.

구성 가져오기를 시도할 때, ASA FirePOWER 모듈은 어플라이언스에 이미 있는 구성인지 확인합니다. 충돌이 존재할 경우, 다음을 수행할 수 있습니다.

- 기존 구성 유지
- 새 구성으로 기존 구성을 교체
- 최신 구성 유지 또는
- 해당 구성을 새 구성으로 가져오기

구성을 가져온 다음 대상 시스템의 구성을 수정한 경우, 해당 구성을 다시 가져온 후 유지할 구성 버전을 선택해야 합니다.

가져오는 구성의 수 및 해당 구성이 참조하는 개체의 수에 따라 가져오기 절차에는 몇 분 정도 걸릴 수 있습니다.

하나 이상의 구성을 가져오려면 다음을 수행합니다.

단계 1 구성을 내보내는 ASA FirePOWER 모듈 및 구성을 가져오려고 계획하는 모듈이 동일한 버전의 을 실행하는지 확인합니다. 침입 또는 액세스 제어 정책을 가져오는 경우, 규칙 업데이트 버전이 일치하는지도 확인해야 합니다.

ASA FirePOWER 모듈의 버전(및 해당하는 경우, 규칙 업데이트 버전)이 일치하지 않는 경우, 가져오기가 실패하게 됩니다.

단계 2 가져오려는 구성을 내보내십시오(B-1페이지의 구성 내보내기 참고).

단계 3 구성을 가져오려는 어플라이언스에서, **Configuration(구성) > ASA FirePOWER Configuration(ASA FirePOWER 구성) > Tools(도구) > Import Export(가져오기 내보내기)**를 선택합니다.

Import Export(가져오기 내보내기) 페이지가 나타납니다.

팁 구성 목록을 축소하려면 구성 유형 옆에 있는 축소 아이콘()을 클릭합니다. 구성을 보려면 구성 유형 옆에 있는 확장 아이콘()을 클릭합니다.

단계 4 **Upload Package(패키지 업로드)**를 클릭합니다.

Upload Package(패키지 업로드) 페이지가 나타납니다.

단계 5 다음 2가지 옵션을 사용할 수 있습니다.

- 사용자가 업로드할 패키지의 경로를 입력합니다.
- 패키지 위치를 파악하려면 **Upload File(파일 업로드)**를 클릭합니다.

단계 6 **Upload(업로드)**를 클릭합니다.

업로드 결과는 패키지의 내용에 따라 달라집니다.

- 패키지의 구성 이 어플라이언스에 이미 있는 버전과 정확히 일치하는 경우, 버전이 이미 있음을 알리는 메시지가 나타납니다. 어플라이언스는 최근 구성을 가지므로 가져올 필요가 없습니다.
- 어플라이언스와 패키지를 내보낸 어플라이언스 간 ASA FirePOWER 모듈 는 (해당하는 경우) 사용자 업데이트 버전이 불일치하는 경우, 패키지를 가져올 수 없음을 알리는 메시지가 나타납니다. ASA FirePOWER 모듈 또는 규칙 업데이트 버전을 업데이트하고 프로세스를 다시 시도하십시오.
- 패키지가 어플라이언스에 존재하지 않는 규칙 버전 또는 구성을 포함하는 경우, Package Import(패키지 가져오기) 페이지가 나타납니다. 다음 단계를 계속합니다.

단계 7 가져오려는 구성을 선택하고 **Import(가져오기)**를 클릭합니다.

가져오기 프로세스는 다음 결과와 함께 해결됩니다.

- 사용자가 가져오는 구성에 ASA FirePOWER 모듈의 이전 수정 버전이 없는 경우, 가져오기는 자동으로 완료되고 성공 메시지가 나타납니다. 나머지 절차를 건너뜁니다.
- 보안 영역을 포함하는 액세스 제어 정책을 가져오는 경우, Access Control Import Resolution(액세스 제어 가져오기 해결) 페이지가 나타납니다. 8단계를 계속 진행합니다.
- 사용자가 가져올 구성에 어플라이언스의 이전 수정 버전이 없는 경우, Import Resolution(가져오기 해결) 페이지가 나타납니다. 9단계를 계속 진행합니다.

단계 8 가져오는 각 보안 영역 옆에, 매핑을 위해 일치하는 유형의 기존 로컬 보안 영역을 선택하고 **Import(가져오기)**를 클릭합니다.

7단계로 돌아갑니다.

단계 9 각 구성을 확장하고 적절한 옵션을 선택합니다.

- 어플라이언스에서 구성을 유지하려면 **Keep existing(기존 구성 유지)**을 선택합니다.
- 어플라이언스의 구성을 가져온 구성으로 대체하려면, **Replace existing(기존 구성 대체)**을 선택합니다.
- 최신 구성을 유지하려면 **Keep newest(최신 구성 유지)**를 선택합니다.
- 가져온 구성을 새 구성으로 저장하려면 **Import as new(새 구성으로 가져오기)**를 선택하고, 선택적으로 구성 이름을 수정합니다.

  활성화된 정상 목록 또는 사용자 지정 탐지 목록과 함께 파일 정책을 포함하는 액세스 제어 정책을 가져오는 경우, **Import as new(새 구성으로 가져오기)** 옵션을 사용할 수 없습니다.
- 종속된 개체를 포함하는 저장된 검색 또는 액세스 제어 정책을 가져오는 경우, 제안된 이름을 수락하거나 개체 이름을 변경합니다. 시스템은 항상 종속된 개체를 새 개체로 가져옵니다. 기존 개체를 유지하거나 대체하는 옵션을 가질 수 없습니다. 시스템이 개체 및 개체 그룹을 동일하게 처리한다는 점에 유의하십시오.

단계 10 **Import(가져오기)**를 클릭합니다.

구성을 가져옵니다.

장기 작업 상태 보기

정책 적용 또는 업데이트 설치와 같이 ASA FirePOWER 모듈에서 수행할 수 있는 일부 작업은 즉시 완료되지 않으며, 실행하는 데 일정 시간이 필요합니다. 작업 큐에서 이러한 장기 작업의 진행 상태를 확인할 수 있습니다. 작업 큐는 또한 이러한 작업이 성공적으로 해결되었는지 또는 실패했는지 여부에 대해 보고합니다.

자세한 내용은 다음 섹션을 참고하십시오.

- C-1페이지의 작업 큐 보기
- C-2페이지의 작업 큐 관리

작업 큐 보기

라이센스: 모두

정책 적용 또는 업데이트 설치와 같은 장기 작업을 수행할 때 이 작업의 상태가 작업 큐에서 보고됩니다. 작업이 완료되면 작업 큐는 복잡한 작업 및 보고서에 대한 정보를 제공합니다.

Task Status(작업 상태) 페이지에서 작업 큐를 볼 수 있는데, 10초마다 자동으로 새로 고침됩니다.

Job Summary(작업 요약) 섹션에서는 다음 표에서 설명된 대로 페이지에 나열된 작업 상태가 표시됩니다.

표 C-1 작업 큐 작업 유형

작업 유형	설명
실행 중	현재 진행 중인 작업 수입니다.
대기 중	실행되기 전에 진행 중인 작업이 완료되기를 기다리는 작업 수입니다.
완료됨	성공적으로 완료된 작업 수입니다.
재시도 중	자동으로 재시도하는 작업 수입니다. 모든 작업의 재시도가 허용되는 것은 아니라는 점에 유의하십시오.
중지됨	시스템 업데이트로 인해 중지된 작업 수입니다. 중지된 작업은 다시 시작할 수 없으며 작업 큐에서 수동으로 삭제해야 합니다.
실패함	성공적으로 완료되지 않은 작업 수입니다.

Jobs(작업) 섹션에서는 작업 시작 시기와 작업의 현재 상태, 그리고 상태가 마지막으로 변경된 시기 등 간단한 설명을 포함하여 각 작업에 대한 정보를 제공합니다. 동일한 유형의 작업은 작업 그룹에 함께 나타납니다.

Task Status(작업 상태) 페이지가 신속하게 로드되도록 하기 위해 ASA FirePOWER 모듈은 일주일에 한 번씩 대기열에서 완료된 작업과 실패한 작업 및 한 달 이상 전에 중지된 작업은 물론 1000개 이상의 작업을 포함하는 작업 그룹에서 가장 오래된 작업을 제거합니다. 대기열에서 수동으로 작업을 제거할 수도 있습니다. 지침은 작업 큐 관리를 참고하십시오.

작업 큐를 보려면 다음을 수행합니다.

단계 1 다음 2가지 옵션을 사용할 수 있습니다.

- 작업을 수동으로 시작한 경우, 작업을 시작할 때 나타난 알림 상자에서 **Task Status(작업 상태)** 링크를 클릭합니다.

  Task Status(작업 상태) 페이지가 팝업 창에 나타납니다.

- 작업을 예약한 경우 또는 작업이 표시되지 않는 페이지에서 시작된 경우 **Monitoring(모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) > Task Status(작업 상태)**를 선택합니다.

  Task Status(작업 상태) 페이지가 나타납니다.

Task Status(작업 상태) 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 작업 큐 관리를 참고하십시오.

작업 큐 관리

라이센스: 모두

다음 표에 설명된 대로 작업 큐(C-1페이지의 작업 큐 보기 참고)을 보면서 수행할 수 있는 여러 가지 작업이 있습니다.

표 C-2 작업 큐 작업

목적	방법
작업 큐에서 완료된 작업 모두 제거	**Remove Completed Jobs(완료된 작업 제거)**를 클릭합니다.
작업 큐에서 실패한 작업 모두 제거	**Remove Failed Jobs(실패한 작업 제거)**를 클릭합니다.
작업 큐에서 단일 작업 제거	삭제할 작업 옆에 있는 삭제 아이콘( )을 클릭합니다. 실행 중인 작업은 삭제할 수 없습니다. 실행 중인 작업을 삭제해야 하는 경우(예를 들어, 작업이 반복적으로 실패할 경우), Support(지원팀)에 문의하십시오.
작업 그룹 축소 및 작업 숨기기	확장된 작업 그룹 옆에 있는 열린 폴더 아이콘( )을 클릭합니다.
작업 그룹 확장 및 작업 보기	축소된 작업 그룹 옆에 있는 닫힌 폴더 아이콘( )을 클릭합니다.

보안, 인터넷 액세스 및 통신 포트

ASA FirePOWER 모듈을 보호하려면 보호된 내부 네트워크에 설치합니다. ASA FirePOWER 모듈에서 필수 서비스와 사용 가능한 포트만 사용하도록 구성한 경우에도 방화벽 밖의 공격이 방어 센터에 도달할 수 없도록 해야 합니다.

또한 ASA FirePOWER 모듈의 특정 기능에는 인터넷 연결이 필요합니다. 기본적으로, ASA FirePOWER 모듈은 인터넷에 직접 연결할 수 있도록 구성됩니다. 또한 특정 포트는 보안 어플라이언스 액세스를 제공하고 특정 시스템 기능

이 올바르게 작동하는 데 로컬 또는 인터넷 리소스에 액세스할 수 있도록 개방된 상태여야 합니다.

자세한 내용은 다음을 참고하십시오.

인터넷 액세스 요구 사항

기본적으로, ASA FirePOWER 모듈 ASA FirePOWER 모듈에서 기본적으로 개방되는 포트 443/tcp(HTTPS) 및 80/tcp(HTTP)에서 인터넷에 직접 연결하도록 구성되었습니다(D-2페이지의 통신 포트 요구 사항 참고).

다음 표는 ASA FirePOWER 모듈의 특정 기능에 대한 인터넷 액세스 요구 사항을 설명합니다.

표 D-1 ASA FirePOWER 모듈 기능의 인터넷 액세스 요구 사항

기능	인터넷 액세스가 필요한 이유
침입 규칙, VDB, GeoDB 업데이트	침입 규칙, GeoDB 또는 VDB 업데이트를 어플라이언스로 직접 다운로드하거나 다운로드 일정 예약
네트워크 기반 AMP	악성코드 클라우드 조회 수행
보안 인텔리전스 필터링	인텔리전트 피드를 포함한 외부 소스에서 보안 인텔리전스 피드 데이터 다운로드
시스템 소프트웨어 업데이트	시스템 업데이트를 어플라이언스로 직접 다운로드하거나 다운로드 일정 예약
URL 필터링	액세스 제어를 위해 클라우드 기반 URL 카테고리 및 평판 데이터 다운로드, 분류되지 않은 URL에 대한 조회 수행
whois	외부 호스트의 whois 정보 요청

통신 포트 요구 사항

개방된 포트는 다음을 허용합니다.

- 어플라이언스의 사용자 인터페이스에 액세스
- 어플라이언스로 안전하게 원격 연결
- 시스템의 특정 기능이 올바르게 작동하는 데 필요한 로컬 또는 인터넷 리소스에 액세스

일반적으로 기능과 관련된 포트는 관련 기능을 활성화 또는 구성할 때까지 닫은 상태를 유지해야 합니다.

주의 개방된 포트를 닫음으로써 구축에 어떤 영향을 미칠지 이해하기 전까지 개방된 포트를 **닫지 마십시오**.

예를 들어, 매니지드 디바이스 블록에서 아웃바운드 25/tcp(SMTP) 포트를 닫을 경우 기기가 개별 침입 이벤트에 대한 이메일 알림을 전송할 수 없습니다(28-1페이지의 침입 규칙을 위한 외부 경고 구성 참고).

다음 표는 필요한 개방 포트를 나열하며, 이를 통해 ASA FirePOWER 모듈 기능을 완전히 활용할 수 있습니다.

표 D-2 ASA FirePOWER 모듈기능 및 작동을 위한 기본 통신 포트

포트	설명	방향	개방 위치
22/tcp	SSH/SSL	양방향	어플라이언스에 대한 안전한 원격 연결 허용
25/tcp	SMTP	아웃바운드	어플라이언스의 이메일 알림 및 경고 전송
53/tcp	DNS	아웃바운드	DNS 사용
67/udp 68/udp	DHCP	아웃바운드	DHCP 사용 **참고** 이러한 포트는 기본적으로 **닫혀** 있습니다.
		양방향	HTTP를 통해 사용자 정의 및 서드파티 보안 인텔리전스 피드 업데이트 URL 카테고리 및 평판 데이터 다운로드(포트 443도 필요)
161/udp	SNMP	양방향	SNMP 폴링을 통해 어플라이언스의 MIB에 대한 액세스 허용
162/udp	SNMP	아웃바운드	SNMP 경고를 원격 트랩 서버로 전송
389/tcp 636/tcp	LDAP	아웃바운드	외부 인증을 위해 LDAP 서버와 통신
389/tcp 636/tcp	LDAP	아웃바운드	탐지된 LDAP 사용자의 메타데이터 가져오기
443/tcp	HTTPS	인바운드	어플라이언스의 사용자 인터페이스에 액세스

표 D-2 ASA FirePOWER 모듈기능 및 작동을 위한 기본 통신 포트 (계속)

포트	설명	방향	개방 위치
443/tcp	HTTPS 클라우드 통신	양방향	가져오기: • 소프트웨어, 침입 규칙, VDB, GeoDB 업데이트 • URL 카테고리 및 평판 데이터(포트 80도 필요) • 인텔리전트 피드 및 다른 보안 인텔리전스 피드 • 네트워크 트래픽에서 탐지된 파일의 악성코드 처리
			디바이스의 로컬 사용자 인터페이스를 사용하여 소프트웨어 업데이트 다운로드
514/udp	syslog	아웃바운드	원격 syslog 서버에 대한 경보 전송
8305/tcp	어플라이언스 통신	양방향	구축의 어플라이언스 간 안전하게 통신. **필수**
8307/tcp	호스트 입력 클라이언트	양방향	호스트 입력 클라이언트와 통신