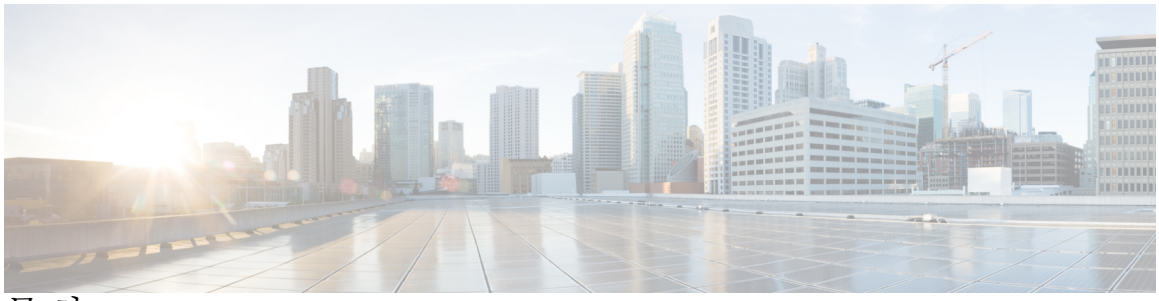
Cisco Secure Firewall Management Center 관리 가이드, 7.3

초판: 2022년 11월 29일

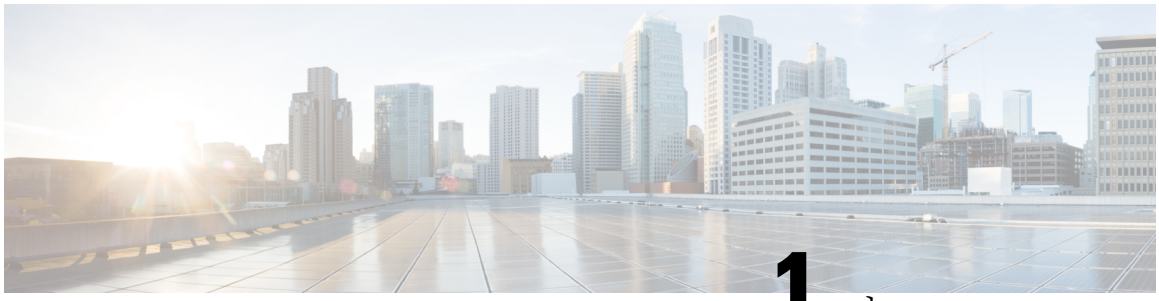
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차

부

시작하기



1 장

Management Center 개요

이 가이드는 온프레미스 Secure Firewall Management Center에 기본 관리자 또는 분석 전용 관리자로 적용됩니다. Cisco Defense Orchestrator(CDO)클라우드 제공 management center을 기본 관리자로 사용하는 경우, 분석을 위해 온프레미스 management center를 사용할 수 있습니다. 이 가이드를 CDO 관리에 사용하지 마십시오. Cisco Defense Orchestrator에서 클라우드 제공 방화벽 관리 센터를 사용하여 방화벽 위협 방어 관리의 내용을 참조하십시오.

Secure Firewall Management Center는 자체 서버 하드웨어에서 실행되거나 하이퍼바이저에서 가상 디바이스로 실행되는 강력한 웹 기반 다중 디바이스 관리자입니다. 다중 디바이스 관리자를 사용하려면 management center를 사용해야 하며, threat defense의 모든 기능이 필요합니다. management center에서는 또한 트래픽 및 이벤트에 대한 강력한 분석 및 모니터링을 제공합니다.

참고 CDO 매니지드 디바이스가 있고 분석용으로만 온프레미스 management center를 사용하는 경우 온프레미스 management center는 정책 구성 또는 업그레이드를 지원하지 않습니다. 이 가이드의 일부 장 및 절차는 기본 관리자가 CDO인 디바이스에는 적용되지 않을 수 있습니다.

기본 관리자로 사용되는 management center의 경우:management center는 management center가 threat defense 구성을 소유하고 있으므로 다른 관리자와 호환되지 않으며 사용자는 management center를 우회하여 threat defense를 직접 구성할 수 없습니다.

빠른 시작: 기본 설정

Firepower 기능 설정은 강력하고 유연하게 기본 및 고급 구성을 지원할 수 있습니다. 다음 섹션을 사용하여 신속하게 Secure Firewall Management Center 및 해당 매니지드 디바이스를 설정하고 제어 및 분석 트래픽을 시작합니다.

물리적 어플라이언스에서 초기 설정 설치 및 수행

프로시저

해당 어플라이언스에 대한 문서를 사용하여 모든 물리적 어플라이언스에서 초기 설정을 설치 및 수행합니다.

- **Management Center**
  - 해당 하드웨어 모델의 *Cisco Firepower Management Center* 시작 가이드

    http://www.cisco.com/go/firepower-mc-install
- **Threat Defense** 매니지드 디바이스
  - Cisco Firepower 1010 시작 가이드
  - Cisco Firepower 1100 시작 가이드
  - Cisco Firepower 2100 시작 가이드
  - Cisco Secure Firewall 3100 시작 가이드
  - Cisco Firepower 4100 시작 가이드
  - Cisco Firepower 9300 시작 가이드
  - Firepower Management Center를 사용하는 ISA 3000용 Cisco Firepower Threat Defense 빠른 시작 가이드

가상 어플라이언스 구축

구축에 가상 어플라이언스가 포함된 경우 이러한 단계를 수행합니다. 문서 로드맵을 사용하여 아래에 나열된 문서를 찾습니다. http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html

프로시저

단계 **1** Management Center 및 디바이스에 사용할 지원되는 가상 플랫폼을 결정합니다(모두 동일하지는 않음). *Cisco Firepower* 호환성 가이드를 참조하십시오.

단계 **2** 다음과 같은 사용자 환경에 대한 문서를 사용하여 가상 Firepower Management Center를 구축합니다.

- VMware에서 실행되는 Firepower Management Center Virtual: *VMware* 구축용 *Cisco Firepower Management Center* 빠른 시작 가이드
- AWS에서 실행되는 Firepower Management Center Virtual: *AWS* 구축용 *Cisco Firepower Management Center* 빠른 시작 가이드
- KVM에서 실행되는 Firepower Management Center Virtual: *KVM* 구축용 *Cisco Firepower Management Center* 빠른 시작 가이드

단계 **3** 다음과 같은 어플라이언스에 대한 문서를 사용하여 가상 디바이스를 구축합니다.

- VMware에서 실행되는 Firepower Threat Defense Virtual: *Cisco Firepower Threat Defense Virtual for VMware* 시작 가이드
- AWS에서 실행되는 Firepower Threat Defense Virtual: *AWS* 구축용 *Cisco Firepower Threat Defense Virtual* 빠른 시작 가이드
- KVM에서 실행되는 Firepower Threat Defense Virtual: *KVM* 구축용 *Cisco Firepower Threat Defense Virtual* 빠른 시작 가이드
- Azure에서 실행되는 Firepower Threat Defense Virtual: *Azure* 구축용 *Cisco Firepower Threat Defense Virtual* 빠른 시작 가이드

최초 로그인

새 management center에 처음 로그인하기 전에, 물리적 어플라이언스에서 초기 설정 설치 및 수행, 2 페이지 또는 가상 어플라이언스 구축, 2 페이지의 설명에 따라 어플라이언스를 준비합니다.

새 management center(또는 출고 시 설정으로 새로 복원된 management center)에 처음 로그인할 때는, CLI 또는 웹 인터페이스용 관리자 계정을 사용하고 사용자의 management center 모델에 맞는 *Cisco Firepower Management Center* 시작 가이드의 지침을 따르십시오. 초기 구성 프로세스가 끝나면 시스템의 다음 요소를 구성하게 됩니다.

- 두 관리자 계정(웹 인터페이스 액세스용 하나와 CLI 액세스용 하나)의 비밀번호는 Management Center용 사용자 계정 지침 및 제한 사항, 122 페이지에서 설명하는 강력한 비밀번호 요구 사항을 준수해, 같은 값으로 설정됩니다. 시스템은 초기 구성 프로세스에서만 두 관리자 계정의 비밀번호를 동기화합니다. 나중에 아무 관리자 계정의 비밀번호를 변경하면 두 계정의 비밀번호가 달라지며, 강력한 비밀번호 요건이 웹 인터페이스 관리자 계정에 적용되지 않게 됩니다. (내부 사용자 추가, 123 페이지 참조)

- management center이(가) 자체 관리 인터페이스(eth0)를 통한 네트워크 통신에 사용하는 다음 네트워크 설정은 기본값이나 사용자가 입력한 값으로 설정됩니다.
  - FQDN(Fully Qualified Domain Name)(`<hostname>.<domain>`)
  - IPv4 구성에 대한 부팅 프로토콜(DHCP 또는 고정/수동)
  - IPv4 주소
  - 네트워크 마스크
  - 게이트웨이
  - DNS 서버
  - NTP 서버

  이러한 설정의 값은 management center 웹 인터페이스에서 확인하고 변경할 수 있습니다. 자세한 내용은 Management Center 관리 인터페이스 수정, 82 페이지 및 시간 동기화, 102 페이지의 내용을 참조하십시오.
- 시스템은 초기 구성의 일부로 매주 GeoDB 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 GeoDB 업데이트 예약, 237 페이지.
- 시스템은 초기 구성의 일부로 새로 사용 가능한 업그레이드와 최신 VDB의 다운로드를 매주 예약합니다. 이 작업을 검토하고 필요한 경우 소프트웨어 다운로드 자동화, 512 페이지.

중요 이 작업은 업데이트만 다운로드합니다. 이 작업으로 다운로드하는 업데이트의 설치는 사용자의 책임입니다.

- 시스템은 초기 구성의 일부로 구성 전용 management center 백업(로컬로 저장)을 매주 예약합니다. 이 작업을 검토하고 필요한 경우 Management Center 백업 예약, 503 페이지.
- 시스템은 초기 구성의 일부로 최신 VDB를 다운로드하고 설치합니다. 시스템을 최신 상태로 유지하려면 취약성 데이터베이스 업데이트 자동화, 515 페이지.
- 시스템은 초기 구성의 일부로 매일 침입 규칙 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 침입 규칙 업데이트 예약, 240 페이지.

management center 초기 구성이 완료되면, Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 설명하는 디바이스 관리 페이지가 웹 인터페이스에 표시됩니다.

(이것은 첫 번째 관리자 사용자 로그인에서만 표시되는 기본 로그인 페이지입니다. 관리자나 다른 사용자가 하는 이후 로그인에서는 홈 페이지 지정, 209 페이지에서 설명하는 방법에 따라 기본 로그인 페이지가 결정됩니다.)

초기 구성이 끝나면, 기본 정책 및 구성 설정, 5 페이지에 설명된 대로 기본 정책을 구성하여 트래픽 제어 및 분석을 시작합니다.

기본 정책 및 구성 설정

대시보드, Context Explorer 및 이벤트 테이블에서 데이터를 확인하려면 기본 정책을 구축해야 합니다.

참고 이것이 정책 또는 특징 및 기능에 대한 전체 설명은 아닙니다. 다른 기능 및 고급 구성에 대한 지침은 이 가이드의 나머지 부분을 참조하십시오.

시작하기 전에

- 웹 인터페이스 또는 CLI용 관리자 계정으로 웹 인터페이스에 로그인하고, https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-guides-list.html에서 제공하는 하드웨어 모델별 *Cisco Firepower Management Center* 시작 가이드의 설명에 따라 초기 구성을 수행합니다.

프로시저

단계 **1** 기본 표준 시간대 설정, 214 페이지에 설명된 대로 이 어카운트의 시간대를 설정합니다.

단계 **2** 필요하다면 라이선스, 261 페이지의 설명에 따라 라이선스를 추가합니다.

단계 **3** 의 설명에 따라 매니지드 디바이스를 구축에 추가합니다Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Management Center*에 디바이스를 추가합니다.

단계 **4** 다음에 설명된 대로 매니지드 디바이스를 구성합니다.

- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 인터페이스 개요, Firepower Threat Defense 디바이스에 투명 또는 라우팅 모드 구성
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 인터페이스 개요, threat defense 디바이스에 인터페이스 구성

단계 **5** 에 설명된 대로 액세스 제어 정책 구성Cisco Secure Firewall Management Center 디바이스 구성 가이드에 기본 액세스 제어 정책 생성.

- 대부분의 경우 Cisco는 Balanced Security and Connectivity(보안과 연결의 균형 유지) 침입 정책을 기본 작업으로 설정할 것을 제안합니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 액세스 제어 정책 기본 작업 및 시스템 제공 네트워크 분석 및 침입 정책을 참고하십시오.
- 대부분의 경우 Cisco는 조직의 보안 규제 준수 요구사항을 충족시키기 위해 연결 로깅 활성화를 제안합니다. 디스플레이를 복잡하게 만들거나 시스템을 마비시키지 않도록 로깅할 연결을 결정하는 경우 네트워크에서의 트래픽을 고려합니다. 자세한 내용은 연결 로깅 정보, 753 페이지를 참고하십시오.

단계 **6** 상태 정책 적용, 384 페이지에 설명된 대로 시스템 제공 기본 상태 정책을 적용합니다.

단계 **7** 시스템 구성 설정 중 일부를 맞춤화합니다.

- 서비스에 대 한 인바운드 연결을 허용하려면(예: SNMP 또는 시스템 로그) 액세스 목록 구성, 45 페이지에 설명된 대로 액세스 목록에서 포트를 수정합니다.
- 데이터베이스 이벤트 제한 구성, 59 페이지에 설명된 대로 데이터베이스 이벤트 제한에 대해 알아보고 편집하는 것이 좋습니다.
- 디스플레이 언어를 변경하려는 경우, 웹 인터페이스의 언어 설정, 74 페이지에 설명된 대로 언어 설정을 편집합니다.
- 조직에서 프록시 서버를 사용하는 네트워크 액세스를 제한하는 경우 Management Center 관리 인터페이스 수정, 82 페이지의 설명에 따라 프록시 설정을 편집합니다.

단계 **8** 에 설명된 대로 네트워크 검색 정책 사용자 지정Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 검색 정책 구성. 기본적으로 네트워크 검색 정책은 네트워크의 모든 트래픽을 분석합니다. 대부분의 경우 Cisco는 RFC 1918에서 주소 검색을 제한합니다.

단계 **9** 다음과 같이 다른 일반 설정을 맞춤화하는 것이 좋습니다.

- 시스템 변수에 대한 기본값을 맞춤화하려는 경우, 에 설명된 대로 변수 사용에 대해 알아봅니다 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 변수 집합.
- 추가 로컬 인증 사용자 계정를 생성하고 management center에 액세스하려는 경우, 내부 사용자 추가, 123 페이지의 내용을 참조하십시오.
- LDAP 또는 RADIUS 외부 인증을 사용하여 management center에 대한 액세스를 허용하려는 경우, Management Center에 대한 외부 인증 구성, 126 페이지의 내용을 참조하십시오.

단계 **10** 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

다음에 수행할 작업

- 기능, 7 페이지 및 이 가이드의 나머지 부분에 설명된 다른 기능을 검토하고 구성하는 것이 좋습니다.

Threat Defense 디바이스

일반적인 구축에서는 여러 트래픽 처리 디바이스가 같은 Secure Firewall Management Center에 보고하는 데, 이곳에서는 운영, 관리, 분석, 보고 작업을 수행할 수 있습니다.

threat defense 디바이스는 NGIPS 기능을 제공하는 NGFW(차세대 방화벽)입니다. NGFW 및 플랫폼 기능에는 사이트 대 사이트 및 원격 액세스 VPN, 강력한 라우팅, NAT, 클러스터링 및 기타 애플리케이션 검사 및 액세스 제어 최적화가 있습니다.

Threat Defense는 다양한 물리적 및 가상 플랫폼에서 사용할 수 있습니다.

호환성

특정 디바이스 모델, 가상 호스팅 환경, 운영 체제 등과 호환되는 소프트웨어를 포함한 관리자-디바이스 호환성에 대한 자세한 내용은 Cisco Secure Firewall Threat Defense 릴리스 노트 및 Cisco FirePOWER 호환성 가이드를 참조하십시오.

기능

이러한 테이블에는 몇 가지 흔히 사용되는 기능 목록이 표시됩니다.

어플라이언스 및 시스템 관리 기능

생소한 문서를 찾으려면 http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html을 참조하십시오.

기능	구성...	설명...
Firepower 어플라이언스 로그인 사용자 어카운트 관리	Firepower 인증	Management Center의, 117 페이지 및 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스 사용자
시스템 하드웨어 및 소프트웨어의 상태 모니터링	상태 모니터링 정책	상태 모니터링 정보, 369 페이지
어플라이언스 데이터 백업	백업 및 복구	백업/복구, 465 페이지
새 Firepower 버전으로 업그레이드	시스템 업데이트	Cisco Firepower Management Center 업그레이드 설명서, 버전 6.0–7.0 Firepower 릴리스 노트
물리적 어플라이언스 기준	공장 기본값으로 복원(리이미징)	Cisco Firepower Management Center 업그레이드 설명서, 버전 6.0–7.0, 신규 설치 수행에 관한 지침 링크 목록.
어플라이언스에서 VDB, 침입 규칙 업데이트 또는 GeoDB 업데이트	VDB(취약성 데이터베이스) 업데이트, 침입 규칙 업데이트, GeoDB(지리위치 데이터베이스) 업데이트	업데이트, 231 페이지
라이선스 제어 기능을 활용하기 위해 라이선스를 적용합니다.	스마트 라이선싱	라이선스 정보, 261 페이지

기능	구성...	설명...
어플라이언스 운영의 연속성을 보장	매니지드 디바이스 고가용성 및/또는 Firepower Management Center 고가용성	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Firepower Threat Defense* 고가용성 정보 Management Center 고가용성 정보, 311 페이지
디바이스를 구성하고 두 개 이상의 인터페이스 사이에 트래픽을 라우팅합니다.	라우팅	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 라우팅을 위한 참조
두 개 이상의 네트워크 사이에 패킷 스위칭을 구성합니다.	디바이스 전환	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 브리지 그룹 인터페이스 구성
인터넷 연결을 위해 비공개 주소를 공용 주소로 변환합니다.	NAT(네트워크 주소 변환)	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 주소 변환
매니지드 Firepower Threat Defense 간에 보안 터널을 설정합니다.	Site-to-Site(사이트 대 사이트) 가상사설망(VPN)	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *VPN* 개요
원격 사용자와 매니지드 Firepower Threat Defense 디바이스 간에 보안 터널을 설정합니다.	원격 액세스 VPN	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *VPN* 개요
매니지드 디바이스, 구성 및 이벤트에 대한 사용자 액세스 구분	도메인을 사용하는 다중 테넌시	도메인을 사용하는 다중 테넌시 소개, 219 페이지
REST API 클라이언트를 사용하여 어플라이언스 구성 보기 및 관리	REST API 및 REST API Explorer	REST API 환경 설정, 88 페이지 *Firepower REST API* 빠른 시작 가이드
문제 해결	해당 없음	문제 해결, 437 페이지

잠재적 위협 탐지, 방지 및 처리 기능

생소한 문서를 찾으려면 http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html을 참조하십시오.

기능	구성...	설명...
네트워크 트래픽 검사, 로그 및 작업 수행	일부 다른 정책보다 상위에 있는 액세스 제어 정책	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 액세스 제어 소개
IP 주소, URL 및/또는 도메인 이름 연결 차단 또는 모니터링	액세스 제어 정책 내 보안 인텔리전스	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 인텔리전스 정보
네트워크의 사용자가 액세스할 수 있는 웹 사이트를 제어	정책 규칙 내 URL 필터링	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *URL* 필터링
네트워크의 악성 트래픽 및 침입을 모니터링	침입 정책	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 침입 정책 기본 사항
검사 없이 암호화된 트래픽 차단 암호화 또는 해독된 트래픽 검사	SSL 정책	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *SSL* 정책 개요
캡슐화된 트래픽 심층 검사 맞춤화 및 빠른 경로 지정으로 성능 향상	사전 필터 정책	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사전 필터링 정보
액세스 제어에서 허용되거나 신뢰하는 네트워크 트래픽 속도 제한	QoS(Quality of Service) 정책	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *QoS* 정책 정보
네트워크에서 파일(악성코드 포함) 허용 또는 차단	파일/악성코드 정책	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 악성코드 보호 및 파일 정책
위협 정보 소스 데이터 운용	Cisco Threat Intelligence Director(TID)	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Secure Firewall Threat Intelligence Director* 개요

기능	구성...	설명...
패시브 또는 액티브 사용자 인증을 구성하여 사용자 인식 및 사용자 제어 수행	사용자 인식, 사용자 ID, ID 정책	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사용자 *ID* 소스 정보 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *ID* 정책 정보
네트워크의 트래픽에서 호스트, 애플리케이션 및 사용자 데이터를 수집하고 사용자 제어 수행	네트워크 검색 정책	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 검색 정책
Firepower 시스템 외부의 툴을 사용하여 네트워크 트래픽 및 잠재적인 위협에 대한 데이터를 수집하고 분석합니다.	외부 툴과 통합	외부 툴을 사용하여 이벤트 분석, 641 페이지
애플리케이션 탐지 및 제어 수행	애플리케이션 탐지기	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 애플리케이션 탐지
문제 해결	해당 없음	문제 해결, 437 페이지

외부 툴과 통합

생소한 문서를 찾으려면 http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html을 참조하십시오.

기능	구성...	설명...
네트워크의 조건이 관련 정책을 위반할 때 자동으로 치료를 시작	교정	교정 소개, 1071 페이지 *Firepower System Remediation API* 설명서
맞춤 개발 된 클라이언트 애플리케이션으로 Firepower Management Center 스트림 이벤트 데이터	eStreamer 통합	eStreamer 서버 스트리밍, 669 페이지 *Firepower System eStreamer* 통합 가이드

기능	구성...	설명...
서드파티 클라이언트를 사용하여 Firepower Management Center에서 데이터베이스 테이블 쿼리	외부 데이터베이스 액세스	External Database Access(외부 데이터베이스 액세스), 63 페이지 *Firepower System* 데이터베이스 액세스 설명서
서드파티 소스에서 데이터를 가져오는 방법으로 검색 데이터를 보완	호스트 입력	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 호스트 입력 데이터 *Firepower System Host Input API* 설명서
외부 이벤트 데이터 스토리지 도구 및 기타 데이터 리소스를 사용하여 이벤트 조사	외부 이벤트 분석 툴과 통합	외부 툴을 사용하여 이벤트 분석, 641 페이지
문제 해결	해당 없음	문제 해결, 437 페이지

FMC 검색

전역 검색 기능을 사용하여 Secure Firewall Management Center 구성의 요소를 신속하게 찾고 탐색할 수 있습니다.

참고 이 기능은 Light 및 Dusk 테마에서만 지원됩니다. 테마를 변경하려면 웹 인터페이스 모양 변경, 209 페이지의 내용을 참조하십시오.

다음 엔터티에 대한 management center 구성을 검색할 수 있습니다.

- 최상위 메뉴의 웹 인터페이스 페이지 이름입니다. (웹 인터페이스 메뉴 옵션 검색, 14 페이지 참조)
- 특정 정책 유형의 경우:
  - 정책 이름
  - 정책 설명
  - 규칙 이름
  - 규칙 코멘트

  (정책 검색, 15 페이지 참조)
- 특정 개체 유형의 경우:

- 개체 이름
- 개체 설명
- 구성된 값

(개체 검색, 17 페이지 참조)

- 방법 워크스루

  검색에서는 검색어가 포함된 워크스루 목록과 각 링크를 반환합니다. (방법 워크스루 검색, 21 페이지 참조)

전역 검색을 사용할 때는 다음 사항에 유의하십시오.

- 전역 검색 툴을 열면 검색 텍스트 상자 아래의 기록 목록에 최근 10개의 검색이 나타납니다. 이 목록에서 항목을 선택하여 검색을 다시 실행할 수 있습니다.
- 검색 식을 입력하면 인터페이스는 검색 기록을 사용자가 입력할 때 업데이트되는 검색 결과로 대체합니다. 검색을 실행하기 위해 Enter 키를 누를 필요가 없습니다.
- 마우스 또는 키보드 화살표 키와 Enter 키를 사용하여 기록 목록 또는 검색 결과를 탐색할 수 있습니다. Enter 키를 누르면 검색 결과에서 현재 강조 표시된 항목이 선택됩니다. 웹 인터페이스 페이지에 대한 결과의 경우, 이렇게 하면 management center 인터페이스에 강조 표시된 페이지가 표시됩니다. 개체 및 정책의 경우 발견된 엔터티에 대한 세부 정보가 표시됩니다.
- 검색은 대/소문자를 구분하지 않습니다.
- 검색에는 다음 와일드카드 문자를 사용할 수 있습니다.
  - ?는 하나의 문자와 일치합니다.
  - *는 0개 이상의 문자와 일치합니다.
  - ^는 일치하는 엔터티의 앞에 오는 검색 용어를 고정합니다.
  - $는 일치하는 엔터티의 끝에 따라오는 검색어를 고정합니다.

  와일드카드는 이스케이프할 수 없습니다.
- 효율성을 높이기 위해 전역 검색은 간접 검색 결과를 반환하지 않습니다. 즉, 전역 검색은 검색어가 발견된 개체를 참조하는 정책 또는 개체를 반환하지 않습니다. 그러나 검색 상세정보 창에서 발견된 개체의 **Usages(**사용법**)** 탭을 확인하여 발견된 여러 개체를 참조하는 정책 또는 개체를 확인할 수 있습니다.
- 전역 검색은 management center에서 가장 일반적으로 사용되는 구성 엔터티와의 관련성에 따라 결정된 검색 식의 상위 결과를 반환합니다. 전역 검색에서 원하는 결과가 반환되지 않으면 검색을 구체화하거나 여러 GUI 페이지의 상단에 표시되는 검색 또는 필터 툴을 사용해 보거나 웹 인터페이스에서 제공하는 구성별 검색 기능을 사용해 보십시오.
  - Cisco Secure Firewall Management Center 디바이스 구성 가이드의 규칙 검색
  - Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *NAT* 규칙 테이블 검색 및 필터링

- 이벤트 검색
- 맞춤형 테이블 검색

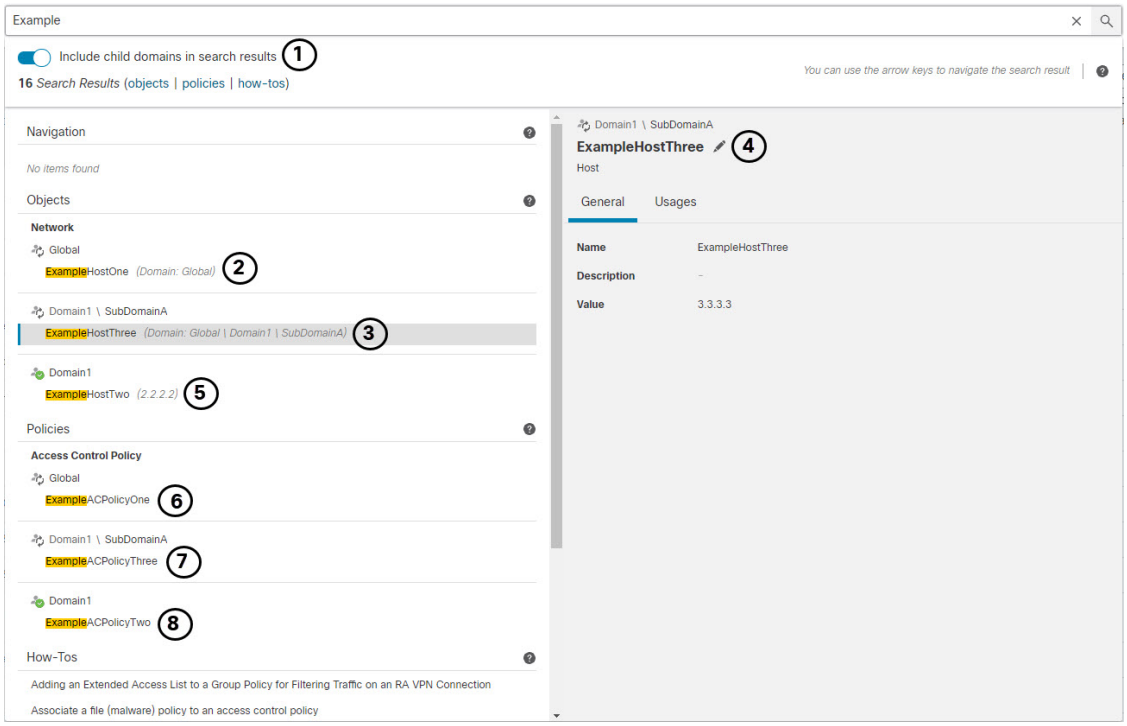
다중 도메인 구축의 전역 검색:

다중 도메인 구축에서 기본적으로 검색은 현재 도메인 및 상위 도메인 내에 정의된 개체 및 정책만 반환합니다. 검색 결과 대화 상자에서 옵션을 전환하여 하위 도메인의 개체 및 정책을 볼 수 있습니다.

개체 검색의 경우 검색 식이 현재 도메인 이외의 도메인에 정의된 개체에서 발견되면 검색 결과에는 해당 개체가 상주하는 도메인의 이름이 표시됩니다. 검색 식이 현재 도메인 내에 정의된 개체에서 발견되면 검색 결과에 개체 값이 표시됩니다.

아래의 예시 스크린샷에서 구축은 Global, Domain1 및 SubDomainA라는 3개 레벨의 3개 도메인으로 구성됩니다. 현재 도메인이 Domain1인 사용자가 상위 도메인과 하위 도메인 모두에서 문자열 "example"에 대한 검색을 입력했습니다.

그림 ***1:*** 다중 도메인 환경에서의 전역 검색 예



1	사용자가 하위 도메인(SubDomainA)과 현재 도메인(Domain1) 및 상위 도메인(Global)을 검색하도록 선택했습니다.	2	상위 도메인 Global에 정의된 일치하는 네트워크 개체 ExampleHostOne이 도메인 이름과 함께 표시되며, 사용자가 세부 정보를 편집하려면 도메인을 전환해야 함을 나타내는 외부 도메인( ) 아이콘이 표시됩니다.

3	하위 도메인 SubDomainA에 정의된 일치하는 네트워크 개체 ExampleHostThree가 도메인 이름 및 세부 정보를 편집하려면 사용자가 도메인을 전환해야 함을 나타내는 외부 도메인() 아이콘과 함께 표시됩니다. 이 개체가 현재 선택되어 있습니다.	4	일치하는 네트워크 개체 ExampleHostThree가 현재 선택되어 있으며 오른쪽 창에 정보가 제공됩니다. 외부 도메인() 아이콘은 사용자가 **Edit(**수정**)** ()을 클릭하면 개체에 대한 수정 액세스를 허용하기 전에 도메인 변경을 확인하라는 메시지가 사용자에게 표시됨을 나타냅니다.
5	현재 도메인에 정의된 일치하는 네트워크 개체 ExampleHostTwo가 개체 값과 함께 표시되며, 사용자가 도메인을 전환하지 않고도 이 개체를 편집할 수 있음을 나타내는 현재 도메인() 아이콘이 함께 표시됩니다.	6	상위 도메인 Global(글로벌)에 정의된 일치하는 액세스 제어 정책 ExampleACPolicyOne이 도메인 이름과 함께 표시되며, 세부 정보를 편집하려면 사용자가 도메인을 전환해야 함을 나타내는 외부 도메인() 아이콘이 표시됩니다.
7	하위 도메인 SubDomainA에 정의된 일치하는 액세스 제어 정책 ExampleACPolicyThree가 도메인 이름과 함께 표시되며, 사용자가 상세 정보를 수정하려면 도메인을 전환해야 함을 나타내는 외부 도메인() 아이콘이 표시됩니다.	8	현재 도메인에 정의된 일치하는 액세스 제어 정책 ExampleACPolicyTwo는 사용자가 도메인을 전환하지 않고도 세부 정보를 수정할 수 있음을 나타내는 현재 도메인() 아이콘과 함께 표시됩니다.

웹 인터페이스 메뉴 옵션 검색

웹 인터페이스의 최상위 메뉴에서 페이지의 위치를 찾으려면 검색할 수 있습니다. 예를 들어 서비스 품질 설정을 보거나 구성하려면 **QoS**를 검색합니다.

시작하기 전에

이 기능은 클래식 테마에서 사용할 수 없습니다. 테마를 변경하려면 웹 인터페이스 모양 변경, 209 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 다음 두 가지 방법 중 하나를 사용하여 검색을 시작합니다.

- Firepower Management Center 웹 인터페이스 상단의 메뉴 모음에서 **Search(**검색**)** ()을 클릭합니다.
- 텍스트 상자 외부에 포커스를 두고 /(슬래시)를 입력합니다.

단계 **2** 원하는 메뉴 옵션 이름의 문자를 하나 이상 입력합니다. 검색 결과는 텍스트 상자 아래에 나타나며 입력에 따라 업데이트됩니다. 검색을 실행하기 위해 Enter 키를 누를 필요가 없습니다.

단계 **3** 검색 결과는 범주별로 그룹화되어 나타납니다. **Navigation(**탐색**)** 아래에 나열된 페이지로 이동하려면 검색 결과 목록에서 메뉴 경로를 클릭합니다.

정책 검색

다음 표에는 이름을 검색할 수 있는 정책 유형이 나와 있습니다.

범위 내	범위 외
액세스 제어 정책	위협 방어 플랫폼 설정
사전 필터 정책	Firepower 설정 정책
위협 방어 NAT 정책	Firepower NAT 정책
침입 범주 • 침입 정책 • 네트워크 분석 정책	QoS 정책 FlexConfig 정책 DNS 정책 악성코드 및 파일 정책 SSL 정책 ID 정책 네트워크 검색 애플리케이션 탐지기 상관관계 정책 VPN 범주 • Dynamic Access Policy • 사이트 대 사이트 • 원격 액세스

전역 검색은 이름 또는 코멘트가 검색어와 일치하는 규칙을 사용하는 액세스 제어 정책뿐만 아니라 이름이 검색어와 일치하는 정책을 반환합니다. 이름이 검색과 일치하지 않는 액세스 제어 정책이 검색 결과 목록에 표시되는 경우, 정책 내에 구성된 규칙의 이름 또는 설명이 일치하는 것입니다.

중요 전역 검색은 management center에서 가장 일반적으로 사용되는 구성 엔터티와의 관련성에 따라 결정된 검색 식의 상위 결과를 반환합니다. 이 검색 기능의 범위에 속하지 않는 정책 유형에 검색어가 있을 수 있습니다. 전역 검색 기능 및 대체 검색 방법에 대한 전체 설명은 FMC 검색을 참조하십시오.

시작하기 전에

이 기능은 클래식 테마에서 사용할 수 없습니다. 테마를 변경하려면 웹 인터페이스 모양 변경, 209 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 다음 두 가지 방법 중 하나를 사용하여 검색을 시작합니다.

- Firepower Management Center 웹 인터페이스 상단의 메뉴 모음에서 **Search(**검색**)** ( )을 클릭합니다.
- 텍스트 상자 외부에 포커스를 두고 /(슬래시)를 입력합니다.

단계 **2** 검색 텍스트 상자에 검색 식을 입력합니다. 검색 결과는 텍스트 상자 아래에 나타나며 입력에 따라 업데이트됩니다. 검색을 실행하기 위해 Enter 키를 누를 필요가 없습니다.

단계 **3** (선택 사항) 다중 도메인 구축에서 현재 도메인에 하위 도메인이 있는 경우 검색 결과에 하위 도메인 포함을 전환하여 해당 하위 도메인의 정책을 확인할 수 있습니다.

단계 **4** 검색 결과는 범주별로 그룹화되어 나타납니다. 다중 도메인 구축에서 **Policies(**정책**)** 범주 내에서 검색 결과는 발견된 정책이 정의된 도메인을 기준으로 그룹화됩니다. **Policies(**정책**)** 범주에서 다음을 수행할 수 있습니다.

작업:	방법:
단일 정책 유형에 대한 검색 결과를 봅니다.	검색 결과에서 정책 유형(예: Access Control Policy)을 클릭합니다.
정책에 대한 세부 정보를 확인합니다.	검색 결과 목록에서 정책 이름을 클릭하여 세부 정보 창을 보고 **General(**일반**)** 탭을 표시합니다.
침입 및 네트워크 분석) 정책을 참조하는 액세스 제어 정책을 봅니다.	검색 결과에서 침입 또는 네트워크 분석 정책의 이름을 클릭하여 Details(세부 정보) 창을 보고 **Usages(**사용**)** 탭을 표시합니다.

작업:	방법:
별도의 브라우저 창에서 정책에 대한 정책 구성 페이지를 엽니다.	검색 결과에서 정책 이름을 클릭하고 세부 정보 창에서 **Edit(**편집**)**()를 클릭합니다. 다중 도메인 구축에서 현재 도메인 내에 정의되지 않은 정책을 편집하도록 선택하면 시스템은 현재 도메인을 변경하라는 메시지를 표시합니다.

개체 검색

다음 표에는 개체 관리 페이지(**Objects(**개체**)** > **Object Management(**개체 관리**)**)에 나열된 개체 유형이 전역 검색 기능의 범위에 속하는지 나와 있습니다.

범위 내	범위 외
AAA 서버 범주 • RADIUS 서버 그룹 • SSO(Single Sign-On) 서버 액세스 목록 범주 • 확장 액세스 목록 • 표준 액세스 목록 주소 풀 범주 • IPv4 풀 • IPv6 풀 AS 경로 커뮤니티 목록 범주 • 확장 커뮤니티 DNS 서버 그룹 외부 속성 범주 • 동적 개체 • Security Group Tag(보안 그룹 태그) 지리위치 인터페이스 범주 • 보안 영역 • 인터페이스 그룹 키 체인 네트워크(네트워크, 호스트, 범위, FQDN, 네트워크 그룹 포함) PKI 범주 인증서 등록	애플리케이션 필터 암호 그룹 목록 커뮤니티 목록 범주 • 커뮤니티 고유 이름 범주 • 개별 고유 이름 개체 • 고유 이름 개체 그룹 파일 목록 FlexConfig 범주 • FlexConfig 개체 • 텍스트 개체 PKI 범주 • 외부 인증서 그룹 • 외부 인증서 • 내부 CA 그룹 • 내부 CA • 내부 인증서 그룹 • 내부 인증서 • 신뢰하는 CA 그룹 • 신뢰할 수 있는 CA 보안 인텔리전스 범주 • DNS Lists and Feeds(DNS 목록 및 피드) • Network Lists and Feeds(네트워크 목록 및 피드) • URL Lists and Feeds(URL 목록 및 피드)

범위 내	범위 외
정책 목록 포트(개체 및 그룹, TCP, UDP, ICMP, ICMP6 등) 접두사 목록 범주 • IPV4 접두사 목록 • IPV6 접두사 목록 경로 맵 SLA 모니터링 시간 범위 표준 시간대 터널 영역 URL(개체, 그룹) VLAN 태그(개체, 그룹) VPN 범주 • 인증서 맵 • 그룹 정책 • IKEv1 IPsec 제안 • IKEv1 정책 • IKEv2 IPSec 제안 • IKEv2 정책	싱크홀 변수 세트 VPN 범주 • Secure Client 파일 • 맞춤형 속성

전역 검색은 이름 또는 설명이 검색어와 일치하는 개체 및 검색 용어와 일치하는 구성된 값을 가진 개체를 반환합니다. 이름이 검색과 일치하지 않는 개체가 검색 결과 목록에 표시되면 개체 내의 설명 또는 구성된 값에서 일치가 이루어진 것입니다.

중요 전역 검색은 management center에서 가장 일반적으로 사용되는 구성 엔터티와의 관련성에 따라 결정된 검색 식의 상위 결과를 반환합니다. 이 검색 기능의 범위에 속하지 않는 개체 유형에 검색어가 있을 수 있습니다. 전역 검색 기능 및 대체 검색 방법에 대한 전체 설명은 FMC 검색을 참조하십시오.

개체 검색은 구축 내에서 네트워크 정보를 찾아야 할 때 특히 유용할 수 있습니다. 개체 이름, 설명 또는 구성된 값에서 다음을 검색할 수 있습니다.

- IPv4 및 IPv6 주소 정보(다음 형식 포함):
  - 전체 주소(예: `194.164.0.23`, `2001:0db8:85a3:0000:0000:8a2e:0370:7334`.)
  - 부분 주소(예: `194.164`, `2001:db8`.)
  - 범위(예: `192.164.1.1-192.168.1.5` 또는 `2001:db8::0202-2001:db8::8329`. 하이픈 전후에 공백을 추가하지 마십시오.) 전역 검색은 지정된 범위 내에서 일치하는 네트워크 주소를 사용하여 개체를 반환합니다.
  - CIDR 표기법. (예: `192.168.1.0/24`, `2002::1234:abcd:ffff:101/64`.) 전역 검색은 지정된 CIDR 블록 내에서 일치하는 네트워크 주소를 사용하여 개체를 반환합니다.
- 포트 정보:
  - 포트 번호(예: `22` 또는 `80`.)
  - 프로토콜. (예: `https` 또는 `ssh`.)
- 정규화된 도메인 이름. (예: `www.cisco.com`.)
- 선택하십시오. (예: `http://www.cisco.com`.)
- 암호화 표준 또는 해시 유형 (예: `AES-128` 또는 `SHA`.)
- VLAN 태그 번호. (예: `568`.)

시작하기 전에

이 기능은 클래식 테마에서 사용할 수 없습니다. 테마를 변경하려면 웹 인터페이스 모양 변경, 209 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 다음 두 가지 방법 중 하나를 사용하여 검색을 시작합니다.

- management center 웹 인터페이스의 맨 위에 있는 메뉴 모음에서 **Search(**검색**)** ( )을 클릭합니다.
- 텍스트 상자 외부에 포커스를 두고 /(슬래시)를 입력합니다.

단계 **2** 검색 텍스트 상자에 검색 식을 입력합니다. 검색 결과는 텍스트 상자 아래에 나타나며 입력에 따라 업데이트됩니다. 검색을 실행하기 위해 Enter 키를 누를 필요가 없습니다.

검색 식이 현재 기본 도메인 이외의 도메인에 정의된 개체에서 발견되는 경우, 검색 결과에는 해당 개체가 상주하는 도메인의 이름이 표시됩니다. 검색 식이 현재 도메인 내에 정의된 개체에서 발견되면 검색 결과에 개체 값이 표시됩니다.

단계 **3** (선택 사항) 다중 도메인 구축에서 현재 도메인에 하위 도메인이 있는 경우 검색 결과에 하위 도메인 포함을 전환하여 해당 하위 도메인의 개체를 확인할 수 있습니다.

단계 **4** 검색 결과는 범주별로 나뉘어 나타납니다. 다중 도메인 구축에서 **Objects(**개체**)** 범주 내에서 검색 결과는 발견된 개체가 정의된 도메인을 기준으로 그룹화됩니다. **Objects(**개체**)** 범주에서 다음을 수행할 수 있습니다.

작업:	방법:
단일 개체 유형에 대한 검색 결과를 봅니다.	검색 결과에서 **Network(**네트워크**)**와 같은 개체 유형을 클릭합니다.
검색 결과에서 개체에 대한 세부 정보를 봅니다.	검색 결과에서 개체 이름을 클릭하여 세부 정보 창을 보고 **General(**일반**)** 탭을 표시합니다.
검색 결과에서 개체를 사용하는 정책 또는 개체의 목록을 봅니다.	검색 결과에서 개체 이름을 클릭하여 세부 정보 창을 보고 **Usages(**사용**)** 탭을 표시합니다. 참고 전역 검색은 모든 개체 유형에 대한 사용 정보를 제공하지 않습니다.
개체에 대한 개체 구성 페이지를 별도의 브라우저 창에서 엽니다.	검색 결과에서 개체 이름을 클릭하고 세부 정보 창에서 **Edit(**편집**)**( )를 클릭합니다. 다중 도메인 구축에서 현재 도메인 내에 정의되지 않은 개체를 편집하도록 선택하면 시스템은 현재 도메인을 변경하라는 메시지를 표시합니다.

방법 워크스루 검색

관심 있는 작업을 다루는 방법 워크스루를 검색할 수 있습니다. 예를 들어 디바이스 설정 절차를 설명하는 워크스루를 찾으려면 "디바이스"라는 용어를 검색하면 됩니다.

시작하기 전에

이 기능은 클래식 테마에서 사용할 수 없습니다. 테마를 변경하려면 웹 인터페이스 모양 변경, 209 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 다음 두 가지 방법 중 하나를 사용하여 검색을 시작합니다.

- Firepower Management Center 웹 인터페이스 상단의 메뉴 모음에서 **Search(**검색**)** ( )을 클릭합니다.
- 텍스트 상자 외부에 포커스를 두고 /(슬래시)를 입력합니다.

단계 **2** 워크스루를 보려는 작업과 관련된 검색어를 입력합니다. 검색 결과는 텍스트 상자 아래에 나타나며 입력에 따라 업데이트됩니다. 검색을 실행하기 위해 Enter 키를 누를 필요가 없습니다.

단계 **3** 검색 결과는 범주별로 그룹화되어 나타납니다. **How-Tos(**방법**)** 아래에 나열된 워크스루를 보려면 검색 결과 목록에서 워크스루 제목을 클릭합니다. 방법 워크스루에 대한 자세한 내용은 Firepower 온라인 도움말, 방법 및 문서, 24 페이지의 내용을 참조하십시오.

도메인 전환 Secure Firewall Management Center

다중 도메인 구축에서 사용자 역할 권한은 사용자가 액세스할 수 있는 도메인과 그러한 각 도메인 내에서 사용자가 갖는 권한을 결정합니다. 단일 사용자 어카운트를 여러 도메인에 연결하고 각 도메인에서 해당 사용자에 대해 서로 다른 권한을 할당할 수 있습니다. 예를 들어 전역 도메인에서 사용자에게 읽기 전용 권한을 할당할 수 있지만 하위 도메인에서는 관리자 권한을 할당할 수 있습니다.

여러 도메인과 연결된 사용자는 동일한 웹 인터페이스 세션 내에서 도메인 간에 전환할 수 있습니다.

툴바에서 사용자 이름 하단에 시스템이 사용 가능한 도메인 트리를 표시합니다. 트리:

- 상위 도메인이 표시되지만, 사용자 어카운트에 할당된 권한에 따라 이러한 도메인에 대한 액세스를 비활성화할 수 있습니다.
- 동위 및 하위 도메인을 포함하여 사용자 어카운트가 액세스할 수 없는 다른 모든 도메인을 숨깁니다.

특정 도메인으로 전환하는 경우, 시스템에 다음과 같이 표시됩니다.

- 해당 도메인에만 관련된 데이터.
- 해당 도메인에 대해 사용자에게 할당된 사용자 역할에 따라 결정되는 메뉴 옵션.

프로시저

사용자 이름 하단에 있는 드롭다운 목록에서 액세스하려는 도메인을 선택합니다.

상황 메뉴

Firepower System 웹 인터페이스의 특정 페이지는 Firepower System의 다른 기능에 액세스하기 위한 바로가기로 사용할 수 있는 오른쪽 클릭(가장 일반적) 또는 왼쪽 클릭 상황 메뉴를 지원합니다. 상황 메뉴의 내용은 액세스하는 위치(페이지 및 특정 데이터)에 따라 달라집니다.

예를 들면 다음과 같습니다.

- IP 주소 핫스팟은 사용 가능한 whois 및 호스트 프로파일 정보를 포함하여, 해당 주소와 관련된 호스트에 대한 정보를 제공합니다.
- SHA-256 해시 값 핫스팟을 사용하면 파일의 SHA-256 해시 값을 정상 목록 또는 맞춤형 탐지 목록에 추가하거나, 복사할 전체 해시 값을 볼 수 있습니다.

Firepower System 상황 메뉴를 지원하지 않는 페이지 또는 위치에는 브라우저의 일반적인 상황 메뉴가 표시됩니다.

정책 편집기

수많은 정책 편집기에는 각 규칙에 대한 핫스팟이 포함되어 있습니다. 규칙 잘라내기, 복사 및 붙여넣기, 규칙 상태 설정, 규칙 수정 등 새 규칙 및 카테고리를 삽입할 수 있습니다.

침입 규칙 편집기

침입 규칙 편집기에는 각 침입 규칙에 대한 핫스팟이 포함되어 있습니다. 규칙을 수정하고, 규칙 상태를 설정하고, 임계값 및 억제 옵션을 구성하고, 규칙 문서를 볼 수 있습니다. 경우에 따라 콘텍스트 메뉴의 **Rule documentation(**규칙 문서**)**을 클릭한 후 문서 팝업창에 있는 **Rule Documentation(**규칙 문서**)**을 클릭하고 더 구체적인 규칙 세부 정보를 확인할 수 있습니다.

이벤트 뷰어

Event(이벤트) 페이지(Analysis(분석) 메뉴 하단에서 사용 가능한 드릴다운 페이지 및 테이블 보기)에는 각 이벤트, IP 주소, URL, DNS 쿼리, 특정 파일의 SHA-256 해시 값에 대한 핫스팟이 포함되어 있습니다. 대부분의 이벤트 유형을 보는 동안 다음을 수행할 수 있습니다.

- Context Explorer에서 관련 정보 보기
- 새 창에서 이벤트 정보로 드릴다운
- 이벤트 필드에 포함된 텍스트가 너무 길어 이벤트 보기에 모두 표시할 수 없는 경우(예: 파일의 SHA-256 해시 값, 취약성 설명, URL) 전체 텍스트 보기
- 상황별 크로스 실행 기능을 사용하여, 외부 소스에서 Firepower로 제공되는 요소에 대한 세부 정보를 표시하는 웹 브라우저 창을 엽니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지를 참고하십시오.

연결 이벤트를 보는 동안 항목을 기본 보안 인텔리전스 차단 목록 및 차단 안 함 리스트에 추가할 수 있습니다.

- IP 주소 핫스팟의 IP 주소
- URL 핫스팟의 URL 또는 도메인 이름
- DNS 쿼리 핫스팟의 DNS 쿼리

캡처된 파일, 파일 이벤트, 악성코드 이벤트를 보는 동안 다음을 수행할 수 있습니다.

- 정상 목록 또는 맞춤형 탐지 목록에 파일을 추가하거나 이 목록에서 파일 제거
- 파일의 복사본 다운로드
- 아카이브 파일 내의 중첩된 파일 보기
- 중첩된 파일의 상위 아카이브 파일 다운로드
- 파일 구성 보기
- 로컬 악성코드 및 동적 분석을 위해 파일 제출

침입 이벤트를 보는 동안 침입 규칙 편집기 또는 침입 정책에서와 유사한 작업을 수행할 수 있습니다.

- 트리거 규칙 수정
- 규칙 상태 설정(규칙 비활성화 포함)
- 임계값 및 억제 옵션 구성
- 규칙 문서 보기 경우에 따라 콘텍스트 메뉴의 **Rule documentation(**규칙 문서**)**을 클릭한 후 문서 팝업창에 있는 **Rule Documentation(**규칙 문서**)**을 클릭하고 더 구체적인 규칙 세부 정보를 확인할 수 있습니다.

침입 이벤트 패킷 보기

침입 이벤트 패킷 보기에는 IP 주소 핫스팟이 포함되어 있습니다. 패킷 보기는 왼쪽 클릭 상황 메뉴를 사용합니다.

대시보드

많은 대시보드 위젯에 Context Explorer에서 관련 정보를 볼 수 있는 핫스팟이 포함되어 있습니다. 대시보드 위젯에는 또한 IP 주소 및 SHA-256 해시 값 핫스팟도 포함할 수 있습니다.

Context Explorer(상황 탐색기**)**

Context Explorer에는 차트, 테이블 및 그래프에 핫스팟이 포함되어 있습니다. Context Explorer에서 허용하는 것보다 더 자세히 그래프 또는 목록의 데이터를 검사하려면 관련 데이터의 테이블 보기로 드릴다운할 수 있습니다. 관련 호스트, 사용자, 애플리케이션, 파일 및 침입 규칙 정보도 볼 수 있습니다.

Context Explorer는 왼쪽 클릭 상황 메뉴를 사용하며, 여기에는 Context Explorer의 고유한 필터링 및 기타 옵션도 포함됩니다.

Cisco와 데이터 공유

다음 기능을 이용하면 Cisco와의 데이터 공유를 선택할 수 있습니다.

- Cisco Success Network

  Cisco Success Network 등록 구성, 647 페이지의 내용을 참조하십시오.

- 웹 분석

  웹 분석, 111 페이지의 내용을 참조하십시오.

Firepower 온라인 도움말, 방법 및 문서

웹 인터페이스 온라인 도움말 연결 방법:

- 각 페이지에서 상황별 도움말 링크 클릭

- 온라인 > 도움말 선택

How To는 Firepower Management Center에서의 작업을 통해 이동하는 워크스루를 제공하는 위젯입니다. 이 워크스루를 통해 사용자가 탐색해야 할 수도 있는 다양한 UI 화면과 상관없이 각 단계를 차례로 수행하여 작업을 완료하는 데 필요한 단계를 수행할 수 있습니다. How To 위젯은 기본적으로 활성화됩니다. 이 위젯을 비활성화하려면 **User Preferences(**사용자 환경 설정**)**를 사용자 이름 하단에 있는 드롭다운 목록에서 선택하고 **How-To Settings(How-To** 설정**)**에서 **Enable How-Tos(How-To** 활성화**)** 확인란의 선택을 취소합니다. 워크스루를 열려면 **Help(**도움말**)** > **How-Tos(**도움말 방법**)**를 선택합니다.

참고 이 워크스루는 일반적으로 모든 UI 페이지에 사용할 수 있으며 사용자 역할에 따라 제한되지 않습니다. 그러나 사용자의 권한에 따라 일부 메뉴 항목이 Firepower Management Center 인터페이스에 나타나지 않습니다. 따라서 워크스루는 그러한 페이지에서는 실행되지 않습니다.

다음 워크스루는 Firepower Management Center에서 사용할 수 있습니다.

- Register FMC with Cisco Smart Account(Cisco Smart Account으로 FMC 등록): 이 워크스루를 통해 Cisco Smart Account으로 Firepower Management Center를 등록할 수 있습니다.
- Set up a Device and add it to FMC(디바이스 설정 및 FMC에 추가): 이 워크스루를 통해 디바이스를 설정하고 Firepower Management Center에 디바이스를 추가할 수 있습니다.
- Configure Date and Time(날짜 및 시간 구성): 이 워크스루를 통해 플랫폼 설정 정책을 사용하여 Firepower Threat Defense 디바이스의 날짜 및 시간을 구성할 수 있습니다.
- Configure Interface Settings(인터페이스 설정 구성): 이 워크스루를 통해 Firepower Threat Defense 디바이스에서 인터페이스를 구성할 수 있습니다.
- Create an Access Control Policy(액세스 제어 정책 생성): 액세스 제어 정책은 하향식으로 평가되는 순서가 정해진 규칙 집합으로 구성됩니다. 이 워크스루를 통해 액세스 제어 정책을 생성할 수 있습니다.
- Add an Access Control Rule(액세스 제어 규칙 추가) - A Feature Walkthrough(기능 워크스루): 이 워크스루는 액세스 제어 규칙의 구성 요소와 Firepower Management Center에서 해당 규칙을 사용하는 방법을 설명합니다.
- Configure Routing Settings(라우팅 설정 구성): 다양한 라우팅 프로토콜이 Firepower Threat Defense에서 지원됩니다. 고정 경로는 특정 목적지 네트워크로 향하는 트래픽을 어디로 보낼지 정의합니다. 이 워크스루를 통해 디바이스에 대한 정적 라우팅을 구성할 수 있습니다.
- (Create a NAT Policy) - (A Feature Walkthrough): 이 워크스루를 통해 NAT 정책을 생성하고 NAT 규칙의 다양한 기능을 연습할 수 있습니다.

문서 로드맵을 사용하여 Firepower 시스템에서 관련 추가 문서를 찾을 수 있습니다: http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html

Cisco.com의 사용 설명서

Secure Firewall Management Center 구축, 버전 6.0 +을 구성하는 경우 다음 문서가 도움이 될 수 있습니다.

참고 일부 연결된 문서는 Secure Firewall Management Center 구축에 적용할 수 없습니다. 예를 들어, 일부 링크는 Secure Firewall Threat Defense 페이지에서 Secure Firewall device manager에 의해 관리되는 구축에 연결되며 하드웨어 페이지에 있는 일부 링크는 management center와 무관합니다. 혼동을 피하기 위해 문서 제목에 주의하십시오. 또한 일부 문서는 여러 제품을 다루며 여러 제품 페이지에 표시될 수 있습니다.

Secure Firewall Management Center

- Secure Firewall Management Center 하드웨어 어플라이언스:

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Secure Firewall Management Center 가상 어플라이언스:

  - http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html
  - http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

Secure Firewall Threat DefenseNGFW(Next Generation Firewall) 디바이스라고도 함.

- Secure Firewall Threat Defense 소프트웨어:

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html

- Secure Firewall Threat Defense 가상:

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html

- Firepower 1000 Series:

  https://www.cisco.com/c/en/us/support/security/firepower-1000-series/tsd-products-support-series-home.html

- Firepower 2100 Series:

  https://www.cisco.com/c/en/us/support/security/firepower-2100-series/tsd-products-support-series-home.html

- Secure Firewall 3100:

  https://www.cisco.com/c/en/us/support/security/secure-firewall-3100-series/series.html

- Firepower 4100 Series:

https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html

- Firepower 9300:

  https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html

- ISA 3000:

  https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html

문서 내 라이선스 설명

섹션 앞부분에 있는 License(라이선스) 설명문에는 섹션에 설명된 기능을 활성화하기 위해 매니지드 디바이스에 할당해야 하는 Classic(클래식) 또는 Smart(스마트) 라이선스에 대해 나와 있습니다.

라이선스 기능은 추가된 경우가 많기 때문에 라이선스 설명문에는 각 기능에 대해 가장 필요한 라이선스만 제시됩니다.

License(라이선스) 설명문에 있는 "or(또는)" 문장은 섹션에 설명된 기능을 활성화하기 위해 매니지드 디바이스에 특정 라이스를 할당해야 하지만 라이선스를 추가하면 기능을 추가할 수 있다는 의미를 나타냅니다. 예를 들어, 파일 정책 내에서 일부 파일 규칙 작업에는 디바이스에 Protection(보호) 라이선스가 필요하지만 다른 작업에는 악성코드 방어 라이선스가 필요합니다.

라이선스에 대한 자세한 내용은 라이선스 정보, 261 페이지를 참조하십시오.

관련 항목

라이선스 정보, 261 페이지

문서 내 지원 디바이스 설명

특정 장이나 주제 앞부분에 있는 Supported Devices(지원 디바이스) 설명문은 지정된 디바이스 시리즈, 제품군 또는 모델에서만 지원되는 기능을 설명합니다. 예를 들어 많은 기능은 Secure Firewall Threat Defense 디바이스에서만 지원됩니다.

이 릴리스에서 지원되는 플랫폼에 대한 자세한 내용은 릴리스 노트를 참조하십시오.

문서 내 액세스 설명

이 문서 각 절차의 앞부분에 있는 Access(액세스) 설명문은 절차 수행에 필요한 사전 정의된 사용자 역할을 설명합니다. 목록에 표시된 역할이 해당 절차를 수행할 수 있습니다.

맞춤형 역할이 있는 사용자는 사전 정의 역할이 있는 사용자와 다른 권한 집합을 가질 수 있습니다. 특정 절차에 대한 액세스 요구 사항을 나타내는 데 사전 정의 역할이 사용된 경우, 권한이 유사한 맞춤형 역할도 액세스 권한을 갖게 됩니다. 맞춤형 역할이 있는 일부 사용자는 약간 다른 메뉴 경로를 사용하여 구성 페이지에 도달할 수 있습니다. 예를 들어 침입 정책 권한만 있는 맞춤형 역할을 가진

사용자는 액세스 제어 정책을 통한 표준 경로가 아니라 침입 정책을 통해 네트워크 분석 정책에 액세스할 수 있습니다.

Firepower System IP 주소 규칙

IPv4 CIDR(Classless Inter-Domain Routing) 표기법 및 유사한 IPv6 접두사 길이 표기법을 사용하여 Firepower System의 여러 위치에서 주소 블록을 정의할 수 있습니다.

CIDR 또는 접두사 길이 표기법을 사용하여 IP 주소 블록을 지정하려는 경우, Firepower System은 마스크 또는 접두사 길이에 의해 지정된 네트워크 IP 주소의 일부만 사용합니다. 예를 들어, 10.1.2.3/8을 입력한 경우 Firepower System은 10.0.0.0/8을 사용합니다.

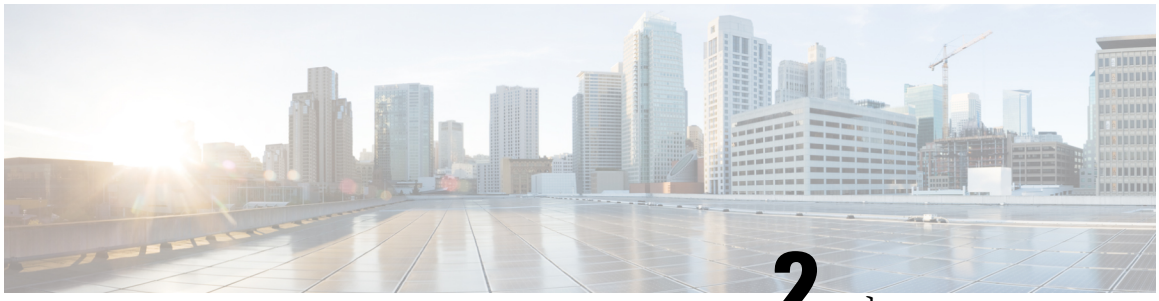
즉 Cisco에서는 CIDR 또는 접두사 길이 표기법을 사용하는 경우 비트 경계에 있는 네트워크 IP 주소를 사용하는 표준 방식을 권장하지만 Firepower System은 이를 요구하지 않습니다.

추가 리소스

Firewalls Community(방화벽 커뮤니티)는 Cisco의 광범위한 문서를 보완하는 참조 자료의 완전한 저장소입니다. 여기에는 하드웨어 3D 모델, 하드웨어 구성 선택기, 제품 참고자료, 구성 예시, 문제 해결 기술 노트, 교육용 동영상, 실습 및 Cisco Live 세션, 소셜 미디어 채널, Cisco Blogs 및 Technical Publications 팀에서 게시한 모든 문서에 대한 링크가 포함됩니다.

조정자를 비롯하여 커뮤니티 사이트 또는 동영상 공유 사이트에 게시하는 개인 중 일부는 Cisco Systems의 직원입니다. 그러한 사이트에 게시한 의견 및 해당 코멘트에 대한 의견은 원래 저자의 개인적 의견이며 Cisco의 의견이 아닙니다. 내용은 정보 제공 목적으로만 제공되며 Cisco 또는 타사의 추천 또는 의사표현으로 간주되어서는 안 됩니다.

참고 Firewalls Community(방화벽 커뮤니티)에 있는 동영상, 기술 노트 및 참조 자료는 management center의 이전 버전을 가리킵니다. 동영상이나 기술 노트에 참조된 management center 버전이 유저 인터페이스에서와 차이가 있어 절차가 동일하지 않을 수 있습니다.



2 장

Management Center에 로그인

다음 주제에서는 Firepower System에 로그인 하는 방법을 설명합니다.

Firepower System 사용자 어카운트

사용자 이름과 비밀번호를 제공해야 웹 인터페이스나 management center 또는 매니지드 디바이스의 CLI에 액세스할 수 있습니다. 매니지드 디바이스에서, 구성 레벨 액세스 권한이 있는 CLI 사용자는 `expert` 명령을 이용해 Linux 셸에 액세스할 수 있습니다. management center에서는 모든 CLI 사용자가 `expert` 명령을 사용할 수 있습니다. management center 및 FTD를 외부 인증을 사용하도록 구성하면 사용자 자격 증명을 외부 LDAP 또는 RADIUS 서버에 저장합니다. CLI 액세스 권한을 취소하거나 외부 사용자에게 제공할 수 있습니다.management center는 인증 및 권한 부여를 위해 SAML(Security Assertion Markup Language) 2.0 개방형 표준을 준수하는 SSO 제공자를 사용하여 SSO(Single Sign-On)를 지원하도록 구성할 수 있습니다.

management center CLI는 모든 명령에 액세스할 수 있는 단일 관리자 사용자를 제공합니다. management center 웹 인터페이스 사용자가 액세스할 수 있는 기능은 관리자가 사용자 계정에 부여하는 권한에 의해 제어됩니다. 매니지드 디바이스의 경우 사용자가 CLI 및 웹 인터페이스에서 액세스할 수 있는 기능은 사용자 계정에 부여된 권한과 관리자에 의해 제어됩니다.

참고 시스템은 사용자 어카운트를 기반으로 사용자 활동을 감사합니다. 따라서 사용자들이 올바른 어카운트로 시스템에 로그인하도록 해야 합니다.

주의 모든 management center CLI 사용자 및 (매니지드 디바이스의 경우) 구성 레벨 CLI 액세스 권한이 있는 사용자는 Linux 셸에서 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- 외부 인증을 설정하는 경우 CLI 액세스 권한이 있는 사용자 목록을 적절하게 제한해야 합니다.
- 매니지드 디바이스에 CLI 액세스 권한을 부여할 때는, 구성 레벨 CLI 액세스로 내부 사용자 목록을 제한합니다.
- Linux 셸 사용자는 설정해선 안 됩니다. 사전 정의된 관리자 사용자 및 CLI에서 관리자 사용자가 생성한 사용자만 사용해야 합니다.

주의 Cisco TAC가 지시하거나 Firepower 사용자 설명서에서 명시적으로 지시하지 않는 한, Linux 셸은 사용하지 않는 것이 좋습니다.

다양한 어플라이언스가 각기 다른 기능으로 서로 다른 유형의 사용자 어카운트를 지원합니다.

Secure Firewall Management Centers

Secure Firewall Management Center다음 같은 사용자 어카운트를 지원합니다.

- 웹 인터페이스 액세스를 위한 사전 정의된 관리자 어카운트. 관리자 역할이 주어지며 웹 인터페이스를 통해 관리할 수 있습니다.
- 맞춤형 사용자 계정으로, 웹 인터페이스 액세스를 제공하며 관리자 사용자와 관리자 권한이 있는 사용자가 생성하고 관리할 수 있습니다.
- CLI 액세스를 위한 사전 정의된 관리자 계정입니다. 이 계정으로 로그인하는 사용자는 `expert` 명령을 사용해 Linux 셸 액세스 권한을 얻을 수 있습니다.

  초기 구성에서 CLI 관리자 계정과 웹 인터페이스 관리자 계정의 비밀번호가 동기화되지만, 원한다면 이후 두 관리자 계정에 별도의 비밀번호를 설정할 수 있습니다.

주의 시스템 보안을 위해 Cisco에서는 Linux 셸 사용자를 어플라이언스에서 추가로 설정하지 않도록 권장합니다.

Secure Firewall Threat Defense및 Secure Firewall Threat Defense Virtual 디바이스

Secure Firewall Threat Defense및 Secure Firewall Threat Defense Virtual 디바이스는 다음 사용자 어카운트 유형을 지원합니다.

- 사전 정의된 관리자 어카운트. 모든 형태의 디바이스 액세스에 사용될 수 있습니다.
- 맞춤형 사용자 어카운트. 관리자 사용자 및 Config(구성) 액세스 권한이 있는 사용자가 생성하고 관리할 수 있습니다.

Secure Firewall Threat Defense는 SSH 사용자에 대한 외부 인증을 지원합니다.

Firepower System 유저 인터페이스

어플라이언스 유형에 따라 웹 기반 GUI, 보조 CLI 또는 Linux 셸을 사용하여 Firepower 어플라이언스와 상호작용할 수 있습니다. Secure Firewall Management Center 구축에서는 management center GUI로 대부분의 구성 작업을 수행합니다. 소수의 작업에서만 CLI나 Linux 셸을 이용해 어플라이언스에 바로 액세스해야 합니다. Cisco TAC가 지시하거나 Firepower 사용자 설명서에서 명시적으로 지시하지 않는 한, Linux 셸 사용은 권장하지 않습니다.

브라우저 요구 사항에 대한 내용은 Firepower 릴리스 노트를 참조하십시오.

참고 어플라이언스에 상관없이 사용자가 SSH를 통한 CLI 로그인에 3회 연속 실패하면, 시스템이 SSH 연결을 종료합니다.

어플라이언스	웹 기반 **GUI**	보조 **CLI**	**Linux** 셸
Secure Firewall Management Center	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • 운영, 관리 및 분석 작업에 사용할 수 있습니다.	• 사전 정의된 관리자 사용자 및 맞춤형 외부 사용자 계정에서 지원됩니다. • SSH, 직렬 또는 키보드 및 모니터 연결을 사용하여 액세스할 수 있습니다. • Cisco TAC가 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.	• 사전 정의된 관리자 사용자에 대해 지원됩니다. • Secure Firewall Management Center CLI에서 `expert` 명령을 통해 액세스해야 합니다. • SSH, 직렬 또는 키보드 및 모니터 연결을 사용하여 액세스할 수 있습니다. • Cisco TAC가 지시하거나 management center 설명서에서 명시적으로 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.

어플라이언스	웹 기반 **GUI**	보조 **CLI**	**Linux** 셸
Secure Firewall Threat Defense Secure Firewall Threat Defense Virtual	—	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • SSH, 직렬 또는 키보드 및 모니터 연결을 사용하여 물리적 디바이스에 액세스할 수 있습니다. SSH 또는 VM 콘솔을 통해 가상 디바이스에 액세스할 수 있습니다. • Cisco TAC가 지시한 설정 및 문제해결 목적으로만 사용해야 합니다.	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • 구성 액세스 권한이 있는 CLI 사용자가 `expert` 명령으로 액세스할 수 있습니다. • Cisco TAC가 지시하거나 management center 설명서에서 명시적으로 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.

관련 항목

내부 사용자 추가, 123 페이지

웹 인터페이스 고려 사항

- 조직에서 인증에 CAC(Common Access Cards)를 사용한다면, LDAP로 인증한 외부 사용자는 CAC 자격 증명을 사용하여 어플라이언스의 웹 인터페이스에 대한 액세스를 얻을 수 있습니다.
- 기본 홈페이지 상단에 나열되는 메뉴 및 메뉴 옵션은 사용자 어카운트에 대한 권한을 기반으로 합니다. 그러나 기본 홈 페이지에 대한 링크에는 사용자 어카운트 권한 전반을 포괄하는 옵션이 포함되어 있습니다. 사용자 어카운트에 부여된 권한과 다른 권한을 필요로 하는 링크를 클릭하는 경우, 시스템 경고 메시지가 나타나고 활동을 기록합니다.
- 상당한 시간이 걸리는 프로세스의 경우 웹 브라우저에 스크립트가 응답하지 않는다는 메시지가 표시될 수 있습니다. 이러한 경우 완료될 때까지 스크립트가 계속 진행되도록 해야 합니다.

관련 항목

홈 페이지 지정, 209 페이지

세션 시간 초과

세션 시간 초과에서 제외되도록 달리 구성하지 않는 한, 기본적으로 1시간 동안 활동이 없으면 시스템에서 자동으로 로그아웃됩니다.

참고 SSO 사용자의 경우 management center 세션이 시간 초과되면 디스플레이가 IdP 인터페이스로 잠시 리디렉션된 다음 management center로그인 페이지로 리디렉션됩니다. SSO 세션이 다른 곳에서 종료되지 않는 한 누구나 로그인 페이지에서 **Single Sign-On(**단일 로그인**)** 링크를 클릭하여 로그인 자격 증명을 제공하지 않고 management center에 액세스 할 수 있습니다. management center보안을 유지하고 다른 사용자가 SSO 계정을 사용하여 management center에 액세스하는 것을 방지하려면 management center 로그인 세션을 무인 상태로 두지 말고 management center에서 로그아웃할 때 IdP의 SSO 페더레이션에서 로그아웃하는 것이 좋습니다.

Administor(관리자) 역할이 부여된 사용자는 다음 설정을 통해 어플라이언스에 대한 세션 시간 초과 간격을 변경할 수 있습니다.

System(시스템**)** > **Configuration(**구성**)** > **Shell Timeout(**셸 시간 초과**)**

관련 항목

세션 시간 제한 구성, 100 페이지
SAML SSO(Single Sign-On) 구성, 145 페이지

Secure Firewall Management Center 웹 인터페이스 로그인

참고 이 작업은 LDAP 또는 RADIUS 서버로 인증된 내부 사용자 및 외부 사용자에게 적용됩니다. SSO 로그인에 대해서는 SSO를 사용한 FMC 웹 인터페이스 로그인, 34 페이지의 내용을 참조하십시오.

사용자는 단일 활성 세션으로 제한됩니다. 이미 활성 세션이 있는 사용자 어카운트로 로그인하려고 할 경우 다른 세션을 종료하거나 다른 사용자로 로그인하라는 프롬프트가 나타납니다.

여러 management center이(가) 동일한 IP 주소를 공유하는 NAT 환경의 경우:

- 각 management center은(는) 한 번에 하나의 로그인 세션만 지원합니다.
- 다른 management center에 액세스하려면 로그인할 때마다 (Firefox나 Chrome 같은) 다른 브라우저를 사용하거나, 브라우저를 시크릿 모드 또는 사생활 보호 모드로 설정해야 합니다.

시작하기 전에

- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 연락하여 어카운트 권한을 수정해 달라고 하거나, 관리자 액세스 권한이 있는 사용자로 로그인하여 어카운트에 대한 권한을 수정하십시오.
- 내부 사용자 추가, 123 페이지에 설명된 대로 사용자 어카운트를 생성합니다.

프로시저

단계 **1** 브라우저에서 **https://***ipaddress_or_hostname/*으로 이동합니다. 여기서 *ipaddress* 또는 *hostname*은 management center와(과) 일치합니다.

단계 **2** **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 사용자 이름과 비밀번호를 입력합니다. 다음 지침에 유의하십시오.

- 사용자 이름은 대/소문자를 구분하지 않습니다.
- 다중 도메인 구축에서 사용자 이름 앞에 사용자 어카운트가 생성된 도메인을 추가합니다. 모든 상위 도메인을 앞에 추가할 필요는 없습니다. 예를 들어 사용자 어카운트가 SubdomainB에서 생성되고 상위 도메인이 DomainA인 경우, 사용자 이름을 다음 형식에 입력합니다.

  ```
  SubdomainB\username
  ```

- 조직에서 로그인할 때 SecurID® 토큰을 사용하는 경우, 토큰을 사용자의 SecurID PIN에 추가하고 로그인 시 비밀번호로 사용하십시오. 예를 들어, PIN이 `1111`이고 SecurID 토큰이 `222222`인 경우 `1111222222`를 입력하십시오. SecurID PIN을 먼저 생성해야 시스템에 로그인할 수 있습니다.

단계 **3** **Login(**로그인**)**을 클릭합니다.

관련 항목

세션 시간 초과, 32 페이지

SSO를 사용한 FMC 웹 인터페이스 로그인

management center는 SAML(Security Assertion Markup Language) 2.0 개방형 표준을 준수하는 SSO 제공자로 구현된 SSO(Single-Sign On) 페더레이션에 참여하도록 구성할 수 있습니다. SSO 사용자 계정은 IdP(Identityy Provider)에서 설정해야 하며 계정 이름으로 이메일 주소를 사용해야 합니다. 사용자 이름이 이메일 주소가 아니거나 SSO 로그인이 실패하면 시스템 관리자에게 문의하십시오.

참고 management center는 SSO 계정에 대한 CAC 자격 증명을 사용한 로그인을 지원하지 않습니다.

사용자는 단일 활성 세션으로 제한됩니다. 이미 활성 세션이 있는 사용자 어카운트로 로그인하려고 할 경우 다른 세션을 종료하거나 다른 사용자로 로그인하라는 프롬프트가 나타납니다.

여러 management center이(가) 동일한 IP 주소를 공유하는 NAT 환경의 경우:

- 각 management center은(는) 한 번에 하나의 로그인 세션만 지원합니다.
- 다른 management center에 액세스하려면 로그인할 때마다 (Firefox나 Chrome 같은) 다른 브라우저를 사용하거나, 브라우저를 시크릿 모드 또는 사생활 보호 모드로 설정해야 합니다.

시작하기 전에

- SSO 액세스를 위해 management center를 구성합니다. SAML SSO(Single Sign-On) 구성, 145 페이지의 내용을 참조하십시오.
- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 문의하여 SSO IdP에서 계정을 구성하십시오.

프로시저

단계 **1** 브라우저에서 **https://***ipaddress_or_hostname*/으로 이동합니다. 여기서 *ipaddress* 또는 *hostname*은 management center와(과) 일치합니다.

참고 SSO 사용자는 SSO 액세스를 위해 특별히 구성된 로그인 URL을 사용하여 management center에 지속적으로 액세스해야 합니다. 관리자에게 문의하십시오.

단계 **2** **Single Sign-On(**단일 인증**)** 링크를 클릭합니다.

단계 **3** 시스템은 다음 두 가지 방법 중 하나로 응답합니다.

- SSO 페더레이션에 이미 로그인한 경우 management center 기본 홈 페이지가 나타납니다.
- SSO 페더레이션에 아직 로그인하지 않은 경우에는 management center가 브라우저를 IdP의 로그인 페이지로 리디렉션합니다. IdP에서 로그인 프로세스를 완료하면 management center 기본 홈 페이지가 나타납니다.

관련 항목

세션 시간 초과, 32 페이지
SAML SSO(Single Sign-On) 구성, 145 페이지

CAC 인증서로 Secure Firewall Management Center에 로그인

사용자는 단일 활성 세션으로 제한됩니다. 이미 활성 세션이 있는 사용자 어카운트로 로그인하려고 할 경우 다른 세션을 종료하거나 다른 사용자로 로그인하라는 프롬프트가 나타납니다.

여러 management center이(가) 동일한 IP 주소를 공유하는 NAT 환경의 경우:

- 각 management center은(는) 한 번에 하나의 로그인 세션만 지원합니다.
- 다른 management center에 액세스하려면 로그인할 때마다 (Firefox나 Chrome 같은) 다른 브라우저를 사용하거나, 브라우저를 시크릿 모드 또는 사생활 보호 모드로 설정해야 합니다.

주의 활성 브라우징 세션 중에는 CAC를 제거하지 마십시오. 세션 중에 CAC를 제거하거나 대체할 경우 웹 브라우저는 세션을 종료하며 웹 인터페이스에서 로그아웃됩니다.

시작하기 전에

- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 연락하여 어카운트 권한을 수정해 달라고 하거나, 관리자 액세스 권한이 있는 사용자로 로그인하여 어카운트에 대한 권한을 수정하십시오.
- 내부 사용자 추가, 123 페이지에 설명된 대로 사용자 어카운트를 생성합니다.
- LADP로 CAC(Common Access Card) 인증 구성, 143 페이지에 설명된 대로 CAC 인증 및 권한 부여를 구성합니다.

프로시저

단계 **1** 조직에서 안내하는 대로 CAC를 삽입합니다.

단계 **2** 브라우저에서 **https://***ipaddress_or_hostname*/으로 이동합니다. 여기서 *ipaddress* 또는 *hostname*은 management center와(과) 일치합니다.

단계 **3** 메시지가 표시되면 1단계에서 삽입한 CAC의 PIN을 입력합니다.

단계 **4** 메시지가 표시되면, 드롭다운 목록에서 적절한 인증서를 선택합니다.

단계 **5** **Continue(**계속**)**를 클릭합니다.

관련 항목

LADP로 CAC(Common Access Card) 인증 구성, 143 페이지
세션 시간 초과, 32 페이지
Management Center에 대한 SSO 지침, 145 페이지

Management Center Command Line Interface에 로그인

관리자 CLI 사용자와 특정 사용자 지정 외부 사용자는 management center CLI에 로그인할 수 있습니다.

주의 Cisco TAC가 지시하거나 management center 설명서에서 명시적으로 지시하지 않는 한, Linux 셸은 사용하지 않는 것이 좋습니다.

참고 어플라이언스에 상관없이 사용자가 SSH를 통한 CLI 로그인에 3회 연속 실패하면 시스템이 SSH 연결을 종료합니다.

시작하기 전에

관리자 사용자로 초기 구성 프로세스를 완료합니다. 최초 로그인, 3 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 관리자 사용자 이름과 비밀번호를 사용하여, SSH 또는 콘솔 포트를 통해 management center에 연결합니다.

조직에서 로그인할 때 SecurID® 토큰을 사용하는 경우, 토큰을 사용자의 SecurID PIN에 추가하고 로그인 시 비밀번호로 사용하십시오. 예를 들어, PIN이 `1111`이고 SecurID 토큰이 `222222`인 경우 `1111222222`를 입력하십시오. 로그인하기 전에 SecurID PIN을 생성해야 합니다.

단계 **2** 사용 가능한 CLI 명령을 사용합니다.

마지막 로그인 보기

권한이 없는 사용자가 여러분의 자격 증명을 이용해 Secure Firewall Management Center에 로그인할 것 같다면, 마지막으로 자격 증명을 이용해 로그인한 날짜, 시간, IP 주소를 확인하십시오.

시작하기 전에

이 기능은 클래식 테마를 사용할 때만 지원됩니다. 사용자 환경 설정에서 이 UI 테마를 선택할 수 있습니다.

프로시저

단계 **1** Secure Firewall Management Center에 로그인합니다.

단계 **2** 브라우저 창의 오른쪽 상단에서 로그인하는 데 사용한 사용자 ID를 찾습니다.

단계 **3** 자신의 사용자 이름을 클릭합니다.

단계 **4** 이전 로그인 관련 정보가 메뉴 하단에 표시됩니다.

Firepower System 웹 인터페이스에서 로그아웃

Firepower System 웹 인터페이스를 더 이상 활발하게 사용하지 않는 경우, Cisco에서는 로그아웃할 것을 권장합니다. 잠시 웹 브라우저에서 떨어져 있는 경우에도 마찬가지입니다. 로그아웃하면 웹 세션이 종료되며, 내 크리덴셜로 타인이 어플라이언스를 사용할 수 없도록 합니다.

참고 management center에서 SSO 세션에서 로그 아웃하는 경우 시스템에서 로그 아웃하면 브라우저가 조직의 SSO IdP로 리디렉션됩니다. management center 보안을 유지하고 다른 사용자가 SSO 계정을 사용하여 management center에 액세스하는 것을 방지하려면 IdP의 SSO 페더레이션에서 로그 아웃하는 것이 좋습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **Logout(**로그아웃**)**를 선택합니다.

단계 **2** management center의 SSO 세션에서 로그 아웃하는 경우 시스템이 조직의 SSO IdP로 리디렉션합니다. management center 보안을 위해 IdP에서 로그 아웃합니다.

관련 항목

세션 시간 초과, 32 페이지

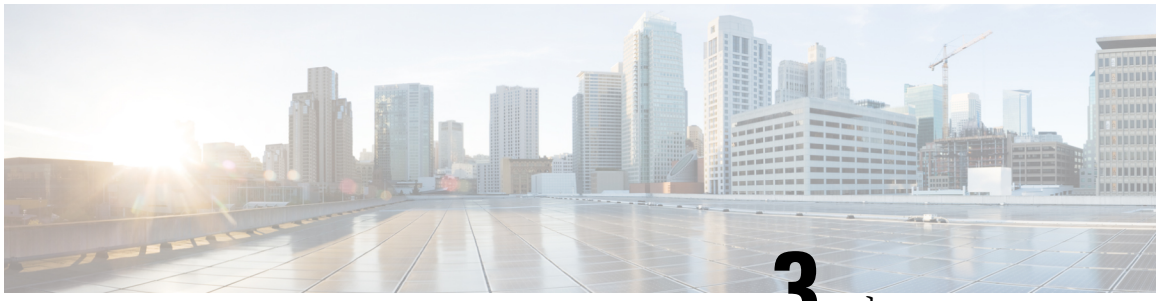
Firepower 시스템 로그인 기록

기능	버전	세부 사항
SAML 2.0 준수 SSO 제공자를 사용하는 SSO(Single Sign-On) 지원을 추가했습니다.	6.7	타사 SAML 2.0 준수 ID 제공자(IdP)에서 설정된 사용자가 로그인 페이지에서 새로운 **SSO(Single Sign-On)** 링크를 사용하여 management center에 로그인하는 기능을 추가했습니다. 신규/수정된 화면: 로그인 화면
다음에 대한 마지막 로그인 정보 확인 Secure Firewall Management Center	6.5	마지막으로 로그인한 날짜, 시간 및 IP 주소를 확인합니다. 신규/수정된 메뉴: 창의 오른쪽 상단에 있는 메뉴로, 로그인하는 데 사용한 사용자 이름을 표시합니다. 지원되는 플랫폼: management center
다음에 대한 자동 CLI 액세스 management center	6.5	SSH를 이용해 management center에 로그인하면, CLI에 자동으로 액세스하게 됩니다. 권장 사항은 아니지만, 이후 CLI `expert` 명령을 사용하면 Linux 셸에 액세스할 수 있습니다. 참고 이 기능을 이용하면 버전 6.3 기능인 management center에 대한 CLI 액세스 활성화/비활성화가 중단됩니다. 이 옵션이 중단되면 가상 management center에서는 **System(**시스템**)** > **Configuration(**구성**)** > **Console Configuration(**콘솔 구성**)** 페이지가 표시되지 않습니다. 물리적 management center에서는 계속 표시됩니다.
SSH 로그인 실패 횟수를 제한합니다.	6.3	사용자가 SSH를 통해 디바이스에 액세스하고 3회 연속 로그인 시도가 실패한 경우, 해당 디바이스가 SSH 세션을 종료합니다.

기능	버전	세부 사항
CLI 액세스를 활성화 및 비활성화 하는 기능 management center	6.3	신규/수정된 화면: management center 웹 인터페이스 관리자가 사용할 수 있는 새 체크박스: **Enable CLI Access(CLI** 액세스 활성화**)**(시스템 (⚙) > **Configuration(**구성**)**에 위치) > (**Console Configuration(**콘솔 구성**))** 페이지 • 선택: SSH를 사용하여 management center에 로그인하면 CLI에 액세스할 수 있습니다. • 선택 취소: SSH를 사용하여 management center에 로그인하면 Linux 셸에 액세스할 수 있습니다. 이는 새 버전 6.3 설치 뿐만 아니라 이전 릴리스에서 버전 6.3으로 업그레이드 할 때의 기본 상태입니다. 지원되는 플랫폼: management center

II 부

시스템 설정



3 장

시스템 구성

이 장에서는 Secure Firewall Management Center에서 시스템 구성 설정을 구성하는 방법을 설명합니다.

시스템 구성 요구 사항 및 전제 조건

모델 지원

Management Center

지원되는 도메인

글로벌

사용자 역할

관리자

Secure Firewall Management Center 시스템 구성 관리

시스템 구성은 management center를 위한 기본적인 설정을 나타냅니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.
단계 **2** 탐색 패널을 사용하여 변경할 구성을 선택합니다.

액세스 목록

IP 주소 및 포트를 기준으로 FMC에 대한 액세스를 제한할 수 있습니다. 기본적으로 모든 IP 주소에 대해 다음과 같은 포트가 활성화됩니다.

- 웹 인터페이스 액세스용 443(HTTPS)
- CLI 액세스용 22(SSH)

포트 161을 통해 SNMP 정보를 폴링할 수 있는 액세스 권한을 추가할 수도 있습니다. SNMP는 기본적으로 비활성화되며, 따라서 먼저 SNMP를 활성화해야 SNMP 액세스 규칙을 추가할 수 있습니다. 자세한 내용은 SNMP 폴링 구성, 99 페이지을 참조하십시오.

주의 기본적으로 액세스는 제한되지 않습니다. 더 안전한 환경에서 작동하려면 특정 IP 주소의 액세스를 추가한 후 기본 **any** 옵션을 삭제하는 것을 고려하십시오.

액세스 목록 구성

이 액세스 목록은 외부 데이터베이스 액세스를 제어하지 않습니다. 데이터베이스에 대한 외부 액세스 활성화, 64 페이지의 내용을 참조하십시오.

주의 FMC에 연결하기 위해 현재 사용 중인 IP 주소에 대한 액세스를 삭제하면, '`IP=any port=443`'에 대한 항목은 존재하지 않으며, 저장할 때 액세스 권한을 잃게 됩니다.

시작하기 전에

기본적으로 액세스 목록에는 HTTPS 및 SSH에 대한 규칙이 포함됩니다. SNMP 규칙을 액세스 목록에 추가하려면 먼저 SNMP를 활성화해야 합니다. 자세한 내용은 SNMP 폴링 구성, 99 페이지을 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** (선택 사항) SNMP 규칙을 액세스 목록에 추가하려면 **SNMP**를 클릭해 SNMP를 구성합니다. 기본적으로 SNMP는 비활성화되어 있습니다. 자세한 내용은 SNMP 폴링 구성, 99 페이지을 참조하십시오.

단계 **3** 액세스 목록을 클릭합니다.

단계 **4** 하나 이상의 IP 주소에 대한 액세스를 추가하려면 **Add Rules(**규칙 추가**)**를 클릭합니다.

단계 **5** **IP** 주소 필드에 IP 주소 또는 어드레스 레인지 또는 `모두`를 입력하십시오.

단계 **6** **SSH**, **HTTPS**, **SNMP** 또는 이 옵션의 조합을 선택하여 이 IP 주소에 활성화할 포트를 지정합니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

Firepower System IP 주소 규칙, 28 페이지

액세스 제어 환경 설정

사용자가 액세스 제어를 수정할 때 코멘트 기능을 사용하여 정책 관련 변경 사항을 추적하도록 시스템을 구성할 수 있습니다. 정책 변경 코멘트를 활성화하면 관리자는 배포의 중요한 정책이 수정된 이유를 신속하게 평가할 수 있습니다. 정책 변경에 대한 코멘트를 활성화하는 경우, 코멘트를 선택 사항 또는 의무 사항으로 설정할 수 있습니다. 정책에 대한 새로운 변경 사항이 저장될 때마다 시스템은 사용자에게 코멘트를 입력하라는 메시지를 표시합니다. 액세스 제어 정책의 규칙 변경 환경 설정에 대한 설명 구성, 46 페이지의 내용을 참조하십시오.

액세스 제어 정책의 규칙 변경 환경 설정에 대한 설명 구성

액세스 제어 정책에서 규칙을 추가하거나 수정할 때 규칙 코멘트를 입력하라는 메시지를 사용자에게 표시하도록 시스템을 구성할 수 있습니다. 이를 사용하여 사용자가 정책을 변경한 이유를 추적할 수 있습니다. 액세스 제어 규칙 변경에 대한 코멘트를 활성화하는 경우, 규칙 코멘트를 선택 사항 또는 필수 사항으로 설정할 수 있습니다. 규칙에 대한 새로운 변경 사항이 저장될 때마다 시스템은 사용자에게 코멘트를 입력하라는 메시지를 표시합니다.

사용자가 규칙을 저장하면 규칙의 코멘트 기록에 코멘트가 추가됩니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)** > **Access Control Preferences(**액세스 제어 환경 설정**)**을(를) 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- **Disabled(**비활성화**)** - 변경 코멘트를 비활성화합니다.
- **Optional(**선택 사항**)** - 코멘트에서 변경 사항을 설명할 수 있는 옵션을 사용자에게 제공합니다.
- **Required(**필수**)** - 사용자는 저장 전에 코멘트에서 변경 사항을 설명해야 합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

개체 그룹 최적화

방화벽 디바이스에 규칙 정책을 구축할 경우 디바이스에서 연결된 네트워크 개체 그룹을 생성할 때 규칙에서 사용하는 네트워크/호스트 정책 개체를 평가하고 최적화하도록 management center를 구성할 수 있습니다. 최적화 기능은 인접 네트워크를 병합하고 중복 네트워크 항목을 제거합니다. 이는 런타임 액세스 목록 데이터 구조 및 구성의 크기를 줄여서 메모리가 제한된 일부 방화벽 디바이스에 유용할 수 있습니다.

예를 들어, 다음 항목을 포함하고 액세스 규칙에서 사용되는 네트워크/호스트 개체를 가정해보겠습니다.

```
192.168.1.0/24
192.168.1.23
10.1.1.0
10.1.1.1
10.1.1.2/31
```

최적화가 활성화된 상태에서 정책을 구축할 때 그 결과로 개체 그룹 구성이 생성됩니다.

```
object-group network test
description (Optimized by management center)
network-object 10.1.1.0 255.255.255.252
network-object 192.168.1.0 255.255.255.0
```

최적화가 비활성화된 경우 그룹 구성은 다음과 같습니다.

```
object-group network test
network-object 192.168.1.0 255.255.255.0
network-object 192.168.1.23 255.255.255.255
network-object 10.1.1.0 255.255.255.255
network-object 10.1.1.1 255.255.255.255
network-object 10.1.1.2 255.255.255.254
```

이러한 최적화는 네트워크/호스트 개체의 정의를 변경하지 않으며, 새 네트워크/호스트 정책 개체를 생성하지도 않습니다.

참고 네트워크 개체 그룹에 다른 네트워크, 호스트 개체 또는 개체 그룹이 포함될 경우 개체가 결합되지 않습니다. 대신 각 네트워크 개체 그룹은 개별적으로 최적화됩니다. 또한 구축 중에는 최적화 프로세스의 일부로 네트워크 개체 그룹의 인라인 값만 수정됩니다.

이 기능은 다음과 같이 지원됩니다.

- 버전 7.2.0~7.2.3에서는 이 기능이 지원되지 않습니다. 이러한 릴리스 중 하나로 업그레이드하거나 이미지를 재설치하면 기능이 비활성화됩니다.
- 버전 7.2.4~7.2.5의 경우, 이 기능은 이미지를 재설치한 Management Center 및 업그레이드된 Management Center에 대해 기본적으로 활성화됩니다. 해당 기능을 비활성화하려면 Cisco TAC에 문의하십시오.

감사 로그

management center는 사용자 활동을 읽기 전용 감사 로그로 기록합니다. 여러 가지 방법으로 감사 로그 데이터를 검토할 수 있습니다.

- 웹 인터페이스인 감사 및 시스템 로그, 417 페이지를 사용합니다.

  감사 로그는 감사 보기의 항목을 기준으로 감사 로그 메시지를 보고, 정렬하고, 필터링할 수 있는 표준 이벤트 보기에서 제공됩니다. 감사 정보를 손쉽게 삭제하고 보고할 수 있으며, 사용자가 변경한 내용에 대한 자세한 보고서를 볼 수 있습니다.

- 시스템 로그인 시스템 로그로의 감사 로그 스트리밍, 48 페이지에 감사 로그 메시지를 스트리밍합니다..

- HTTP 서버인 HTTP 서버에 대한 감사 로그 스트리밍, 49 페이지에 감사 로그 메시지를 스트리밍합니다.

외부 서버로 감사 로그 메시지를 스트리밍하면 management center의 공간을 절약할 수 있습니다. 외부 URL에 감사 정보를 보내면 시스템 성능에 영향을 미칠 수 있음에 유의하십시오.

원한다면 감사 로그 스트리밍용 채널을 보호하고, TLS 인증서를 사용하여 TLS 및 상호 인증을 활성화할 수 있습니다. 감사 로그 인증서, 51 페이지 섹션을 참조하십시오.

여러 시스템 로그 서버로 스트리밍

감사 로그 데이터를 최대 5개의 시스템 로그 서버로 스트리밍할 수 있습니다. 그러나 보안 감사 로그 스트리밍에 대해 TLS를 활성화한 경우, 단일 시스템 로그 서버로만 스트리밍할 수 있습니다.

시스템 로그로의 감사 로그 스트리밍

이 기능이 활성화되는 경우, 감사 로그 기록이 다음 형식으로 시스템 로그에 나타납니다.

Date(날짜) *Time*(시간) *Host*(호스트) [*Tag*(태그)] *Sender*(발신자): *User_Name@User_IP*, *Subsystem*(하위 시스템), *Action*(작업)

로컬 날짜, 시간 및 원래 호스트 이름이 괄호로 묶인 선택적 태그 앞에 오는 경우, 그리고 발신 디바이스 이름이 감사 로그 메시지 앞에 오는 경우.

예를 들어 Management Center의 감사 로그 메시지에 대해 `FMC-AUDIT-LOG` 태그를 지정하면 management center의 샘플 감사 로그 메시지가 다음과 같이 표시될 수 있습니다.

```
Mar 01 14:45:24 localhost [FMC-AUDIT-LOG] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring, Page View
```

심각도 및 시설을 지정하면 이러한 값은 시스템 로그 메시지에 표시되지 않고 시스템 로그 메시지를 수신하는 시스템에 해당 분류 방법을 알려줍니다.

Threat Defense 기능 기록**:**

시작하기 전에

management center가 시스템 로그 서버와 통신할 수 있는지 확인합니다. 구성을 저장할 때 시스템은 ICMP/ARP 및 TCP SYN를 사용하여 시스템 로그 서버에 연결할 수 있는지 확인합니다. 그런 다음 시스템은 기본적으로 포트 514/UDP를 사용하여 감사 로그를 스트리밍합니다. 채널을 보호하는 경우(선택 사항, 감사 로그 인증서, 51 페이지 참조) TCP에 대해 포트 1470을 수동으로 구성해야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Audit Log(**로그 감사**)**를 클릭합니다.

단계 **3** **Enabled(**활성화**)**를 **Send Audit Log to Syslog(**감사 로그를 시스템 로그로 전송**)** 드롭다운 메뉴에서 선택합니다.

단계 **4** 다음 필드는 시스템 로그로 전송된 감사 로그에만 적용됩니다.

옵션	설명
호스트	감사 로그를 전송할 시스템 로그 서버의 IP 주소 또는 정규화된 이름입니다. 최대 5개의 시스템 로그 호스트를 쉼표로 구분하여 추가할 수 있습니다. 참고 감사 서버 인증서에 대해 TLS가 비활성화된 경우에만 여러 시스템 로그 호스트를 지정할 수 있습니다.
기능	메시지를 생성하는 하위 시스템 시스템 로그 알림 시설, 574 페이지에 설명된 시설을 선택합니다. 예를 들어 AUDIT를 선택합니다.
심각도	메시지의 심각도입니다. 시스템 로그 심각도 레벨, 575 페이지에 설명된 심각도를 선택합니다.
태그	감사 로그 시스템 로그 메시지에 포함할 선택적 태그입니다. Best practice(모범 사례): 이 필드에 값을 입력하여 상태 로그와 같은 다른 유사한 시스템 로그 메시지와 감사 로그 메시지를 쉽게 구분합니다. 예를 들어 시스템 로그로 전송된 모든 감사 로그 기록에 `FMC-AUDIT-LOG` 레이블이 붙도록 하려는 경우, `FMC-AUDIT-LOG`를 필드에 입력합니다.

단계 **5** (선택 사항) 시스템 로그 서버의 IP 주소가 유효한지 테스트하려면 **Test Syslog Server(**시스템 로그 서버 테스트**)**를 클릭합니다.

시스템은 시스템 로그 서버에 연결할 수 있는지 확인하기 위해 다음 패킷을 전송합니다.

1. ICMP echo request(ICMP 에코 요청)
2. 443 및 80 포트의 TCP SYN
3. ICMP 타임스탬프 쿼리
4. 임의 포트의 TCP SYN

참고 Management Center 및 시스템 로그 서버가 동일한 서브넷에 있는 경우 ICMP 대신 ARP가 사용됩니다.

시스템은 각 서버에 대한 결과를 표시합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

HTTP 서버에 대한 감사 로그 스트리밍

이 기능을 활성화하는 경우 어플라이언스는 감사 로그 기록을 다음 형식으로 HTTP 서버에 전송합니다.

Date(날짜) Time(시간) Host(호스트) [Tag(태그)] Sender(발신자): User_Name@User_IP, Subsystem(하위 시스템), Action(작업)

로컬 날짜, 시간 및 원래 호스트 이름이 괄호로 묶인 선택적 태그 앞에 오는 경우, 그리고 발신 어플라이언스 이름이 감사 로그 메시지 앞에 오는 경우.

예를 들어 FROMMC의 태그를 지정하는 경우, 샘플 감사 로그 메시지가 다음과 같이 표시될 수 있습니다.

```
Mar 01 14:45:24 localhost [FROMMC] Dev-MC7000: admin@10.1.1.2, Operations > Monitoring,
Page View
```

시작하기 전에

디바이스가 HTTP 서버와 통신할 수 있는지 확인합니다.선택 사항으로, 채널을 보호합니다. 감사 로그 인증서, 51 페이지섹션을 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Audit Log(**로그 감사**)**를 클릭합니다.

단계 **3** 경우에 따라 **Tag(**태그**)** 필드에 메시지에 표시하려는 태그 이름을 입력합니다. 예를 들어 모든 감사 로그 기록을 FROMMC앞에 오도록 하는 경우, 필드에 FROMMC를 입력합니다.

단계 **4** **Enabled(**활성화**)**를 **Send Audit Log to HTTP Server(**감사 로그를 **HTTP** 서버로 전송**)** 드롭다운 리스트에서 선택합니다.

단계 **5** **URL to Post Audit(**사후 감사 **URL)** 필드에서 감사 정보를 전송할 URL을 지정합니다. 다음과 같이 나열된 HPPT POST 변수를 예상하는 Listener 프로그램에 해당하는 URL을 입력합니다.

- subsystem
- actor
- event_type
- message
- action_source_ip
- action_destination_ip
- result
- 시간
- 태그 (정의된 경우. 3단계 참조)

주의 암호화된 게시물을 허용하려면 HTTPS URL을 사용하십시오. 외부 URL에 감사 정보를 보내면 시스템 성능에 영향을 미칠 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

감사 로그 인증서

TLS(Transport Layer Security) 인증서를 사용하여 FMC와 신뢰할 수 있는 감사 로그 서버 간의 통신을 보호할 수 있습니다.

클라이언트 인증서**(**필수**)**

CSR(인증서 서명 요청)을 생성하고 서명을 위해 CA(인증 기관)에 제출한 다음 서명한 인증서를 FMC로 가져옵니다. 로컬 시스템 구성인 다음에 대해 서명된 감사 로그 클라이언트 인증서를 가져옵니다. Management Center, 52 페이지 및 다음에 대한 감사 로그 클라이언트 인증서 가져오기 Management Center, 53 페이지을(를) 사용합니다.

서버 인증서**(**선택 사항**)**

추가 보안을 위해, FMC와 감사 로그 서버 간의 상호 인증을 요구하는 것이 좋습니다. 이렇게 하려면 하나 이상의 CRL(인증서 해지 목록)을 로드해야 합니다. 이러한 CRL에 나열된 해지된 인증서가 있는 서버에는 감사 로그를 스트리밍할 수 없습니다.

Firepower는 식별 부호화 규칙(DER) 형식으로 인코딩된 CRL을 지원합니다. FMC 웹 인터페이스에 대한 HTTPS 클라이언트 인증서를 검증하는 데 사용하는 CRL과 동일합니다.

로컬 시스템 구성인 유효한 감사 로그 서버 인증서 필요, 54 페이지을(를) 사용합니다.

안전한 감사 로그 스트리밍

감사 로그를 신뢰할 수 있는 HTTP 서버 또는 시스템 로그 서버로 스트리밍하는 경우, TLS(Transport Layer Security) 인증서를 사용하여 management center와 서버 사이의 채널을 보호할 수 있습니다. 감사하려는 각 어플라이언스에 대해 고유한 클라이언트 인증서를 생성해야 합니다.

시작하기 전에

감사 로그 인증서, 51 페이지에서 클라이언트 및 서버 인증서 요청에 대한 영향을 참조하십시오.

프로시저

단계 **1** 서명된 클라이언트 인증서를 획득하여 management center에 설치합니다.

a) 다음에 대해 서명된 감사 로그 클라이언트 인증서를 가져옵니다. Management Center, 52 페이지:

사용자가 제공하는 시스템 정보 및 ID 정보에 따라 management center에서 인증서 서명 요청(CSR)을 생성합니다.

CSR을 신뢰할 수 있고 잘 알려진 인증 기관(CA)에 제출하여 서명된 클라이언트 인증서를 요청합니다.

management center와 감사 로그 서버 간에 상호 인증이 필요하면, 클라이언트 인증서는 연결에 사용될 서버 인증서에 서명한 동일한 CA가 서명해야 합니다.

b) 인증 기관에서 서명된 인증서를 받으면 이를 management center로 가져옵니다. 다음에 대한 감사 로그 클라이언트 인증서 가져오기 Management Center, 53 페이지의 내용을 참조하십시오.

단계 **2** TLS(Transport Layer Security)를 사용하고 상호 인증을 사용하도록 서버와의 통신 채널을 구성합니다.

유효한 감사 로그 서버 인증서 필요, 54 페이지의 내용을 참조하십시오.

단계 **3** 아직 수행하지 않았다면 감사 로그 스트리밍을 구성합니다.

시스템 로그로의 감사 로그 스트리밍, 48 페이지 또는 HTTP 서버에 대한 감사 로그 스트리밍, 49 페이지를 참조하십시오.

다음에 대해 서명된 감사 로그 클라이언트 인증서를 가져옵니다. Management Center

중요 고가용성 설정의 대기 management center에서는 **Audit Log Certificate(**감사 로그 인증서**)** 감사 페이지를 사용할 수 없습니다. 대기 management center에서 이 작업을 수행할 수 없습니다.

시스템은 Base-64로 인코딩된 PEM 형식의 인증서 요청 키를 생성합니다.

시작하기 전에

다음에 유의해야 합니다.

- 보안을 위해 세계적으로 인정되고 신뢰할 수 있는 인증 기관(CA)을 사용하여 인증서에 서명합니다.
- 어플라이언스와 감사 로그 서버 간에 상호 인증이 필요하면 동일한 인증 기관이 클라이언트 인증서와 서버 인증서에 모두 서명해야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Audit Log Certificate(**감사 로그 인증서**)**를 클릭합니다.

단계 **3** **Generate New CSR(**새로운 **CSR** 생성**)**을 클릭합니다.

단계 **4** **Country Name (two-letter code)(**국가 이름**(2**글자 코드**))** 필드에 국가 번호를 입력합니다.

단계 **5** **State or Province(**주 또는 도**)** 필드에 주 또는 도에 대한 우편 약자를 입력합니다.

단계 **6** **Locality or City(**구/군/시**)**를 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 올바르게 입력합니다.

참고 공용 이름과 DNS 호스트네임이 일치하지 않으면 감사 로그 스트리밍이 실패합니다.

단계 10 **Generate(**생성**)**를 클릭합니다.

단계 11 텍스트 편집기로 비어 있는 새 파일을 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 *clientname*`.csr`로 저장합니다. 여기서 *clientname*은 인증서 사용을 계획하고 있는 어플라이언스의 이름입니다.

단계 14 **Close(**닫기**)**를 클릭합니다.

다음에 수행할 작업

- 이 절차의 "시작하기 전에" 섹션의 지침에 따라 선택한 인증 기관에 인증서 서명 요청을 제출합니다.
- 서명된 인증서를 수신하면 해당 인증서를 어플라이언스에 가져옵니다. 다음에 대한 감사 로그 클라이언트 인증서 가져오기 Management Center, 53 페이지 섹션을 참조하십시오.

다음에 대한 감사 로그 클라이언트 인증서 가져오기 Management Center

management center 고가용성 설정에서는 액티브 피어를 반드시 사용해야 합니다.

시작하기 전에

- 다음에 대해 서명된 감사 로그 클라이언트 인증서를 가져옵니다. Management Center, 52 페이지.
- 올바른 management center에 대해 서명된 인증서를 가져오는지 확인합니다.
- 인증서를 생성한 서명 기관이 중간 CA를 신뢰하기를 요청하는 경우, 필요한 인증서 체인(또는 인증서 경로)을 제공할 수 있도록 준비합니다. 클라이언트 인증서에 서명한 CA는 인증서 체인에 중간 인증서를 서명한 동일한 CA여야 합니다.

프로시저

단계 1 management center에서 시스템 (⚙) > **Configuration(**구성**)**를 선택합니다.

단계 2 **Audit Log Certificate(**감사 로그 인증서**)**를 클릭합니다.

단계 3 **Import Audit Client Certificate(**감사 클라이언트 인증서 가져오기**)**를 클릭합니다.

단계 4 텍스트 편집기에서 클라이언트 인증서를 열고 `BEGIN CERTIFICATE` 및 `END CERTIFICATE` 행이 포함된 전체 텍스트 블록을 복사합니다. **Client Certificate(**클라이언트 인증서**)** 필드에 이 텍스트를 붙여 넣습니다.

단계 **5** 개인 키 파일을 업로드하고 해당 개인 키 파일을 연 다음 `BEGIN RSA PRIVATE KEY` 및 `END RSA PRIVATE KEY` 행이 포함된 전체 텍스트 블록을 복사합니다. **Private Key(**개인 키**)** 필드에 이 텍스트를 붙여 넣습니다.

단계 **6** 필요한 중간 인증서를 열어서 전체 텍스트 블록을 복사하여 각각을 **Certificate Chain(**인증서 체인**)** 필드에 붙여 넣습니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

유효한 감사 로그 서버 인증서 필요

시스템은 DER(Distinguished Encoding Rules) 형식으로 가져온 CRL을 사용하여 감사 로그 서버 인증서의 유효성을 검증합니다.

참고 CRL을 사용하여 인증서를 확인하도록 선택한 경우 시스템은 동일한 CRL을 사용하여 감사 로그 서버 인증서와 어플라이언스와 웹 브라우저 간의 HTTP 연결을 보호하는 데 사용되는 인증서의 유효성을 검사합니다.

중요 고가용성 쌍의 대기 management center에서는 이 절차를 수행할 수 없습니다.

시작하기 전에

- 상호 인증을 요구하고 CRL(인증서 해지 목록)을 사용하여 인증서가 여전히 유효함을 보장하는 데 따른 영향을 이해합니다. 감사 로그 인증서, 51 페이지의 내용을 참조하십시오.
- 안전한 감사 로그 스트리밍, 51 페이지의 단계와 해당 절차에서 참조하는 항목에 따라 클라이언트 인증서를 획득하고 가져옵니다.

프로시저

단계 **1** management center에서 시스템 (⚙) > **Configuration(**구성**)**를 선택합니다.

단계 **2** **Audit Log Certificate(**감사 로그 인증서**)**를 클릭합니다.

단계 **3** Transport Layer Security를 사용하여 감사 로그를 외부 서버로 안전하게 스트리밍하려면 **Enable TLS(TLS** 활성화**)**를 선택합니다.

TLS가 활성화되면 syslog 클라이언트(management center)가 서버에서 수신한 인증서를 확인합니다. 클라이언트와 서버 간의 연결은 서버 인증서 확인이 성공한 경우에만 성공합니다. 이 확인 프로세스의 경우 다음 조건을 충족해야 합니다.

- 클라이언트에 인증서를 전송하도록 시스템 로그 서버를 구성합니다.
- CA 인증서를 클라이언트에 추가(가져오기)하여 서버 인증서를 확인합니다.

- 클라이언트 인증서를 가져오는 동안 CA 인증서를 가져와야 합니다.
- 발급 CA가 하위 CA인 경우 하위 CA(루트 CA)에서 서명 CA를 추가하기 전에 발급 CA를 추가해야 합니다.

단계 **4** 클라이언트가 서버에 대해 자신을 인증하지 않도록 하려면 인증서가 동일한 CA에서 발급된 경우 서버 인증서를 수락합니다(권장하지 않음).

a) **Enable Mutual Authentication(**상호 인증 활성화**)**을 선택 취소합니다.

중요 클라이언트 인증서를 확인하지 않고 클라이언트를 신뢰하도록 서버가 구성되었는지 확인합니다.

b) **Save(**저장**)**를 클릭하고 이 절차의 나머지 부분은 건너뛰어도 됩니다.

단계 **5** (선택 사항) 감사 로그 서버에 의한 클라이언트 인증서 확인을 활성화하려면 **Enable Mutual Authentication(**상호 인증 활성화**)**을 선택합니다.

중요 **Enable Mutual Authentication(**상호 인증 활성화**)** 옵션은 TLS가 활성화된 경우에만 적용 가능합니다.

상호 인증이 활성화되면 시스템 로그 클라이언트(management center)가 확인을 위해 클라이언트 인증서를 시스템 로그 서버로 전송합니다. 클라이언트는 시스템 로그 서버의 서버 인증서에 서명한 CA와 동일한 CA 인증서를 사용합니다. 클라이언트 인증서 확인이 성공한 경우에만 연결이 성공합니다. 이 확인 프로세스의 경우 다음 조건을 충족해야 합니다.

- 클라이언트에서 수신한 인증서를 확인하도록 시스템 로그 서버를 구성합니다.
- 시스템 로그 서버로 전송할 클라이언트 인증서를 추가합니다. 이 인증서는 시스템 로그 서버의 서버 인증서에 서명한 동일한 CA가 서명해야 합니다.

참고 감사 로그를 시스템 로그 서버로 스트리밍하는 데 상호 인증을 사용하려면 개인 키에 PKCS#1 형식 대신 PKCS#8 형식을 사용합니다. 다음 명령줄을 사용하여 PKCS#1 키를 PKCS#8 형식으로 변환합니다.

```
openssl pkcs8 -topk8 -inform PEM -outform PEM
-nocrypt -in PKCS1 key file name -out PKCS8 key filename
```

단계 **6** (선택 사항) 더 이상 유효하지 않은 서버 인증서를 자동으로 인식하려면 다음을 수행합니다.

a) **Enable Fetching of CRL(CRL** 페칭 활성화**)**을 선택합니다.

중요 이 옵션은 **Enable Mutual Authentication(**상호 인증 활성화**)** 확인란을 선택한 경우에만 표시됩니다. 그러나 **Enable Fetching of CRL(CRL** 가져오기 활성화**)** 옵션은 TLS 옵션이 활성화된 경우에만 적용 가능합니다. CRL은 서버 인증 확인에 사용되며, 클라이언트 인증서 확인을 활성화하기 위한 상호 인증 사용에 의존하지 않습니다.

CRL 가져오기를 활성화하면 클라이언트가 CRL 또는 CRL을 정기적으로 업데이트(다운로드)하도록 예약된 작업이 생성됩니다. CRL은 서버 인증서 확인에 사용됩니다. 여기서는 확인 중인 서버 인증서가 CA에 의해 폐기되었음을 지정하는 CRL이 있는 경우 확인에 실패합니다.

b) 기존 CRL 파일에 유효한 URL을 입력하고 **Add CRL(CRL** 추가**)**을 클릭합니다.

최대 25개의 CRL을 추가하려면 반복합니다.

c) **Refresh CRL(CRL** 새로 복구**)**을 클릭하여 지정된 URL에서 현재 CRL을 로드합니다.

단계 **7** 가지고 있는 유효한 서버 인증서가 클라이언트 인증서를 만든 것과 동일한 인증 기관에서 생성한 것인지 확인합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

(선택 사항) CRL 업데이트 빈도를 설정합니다. CRL(Certificate Revocation List) 다운로드 구성, 505 페이지의 내용을 참조하십시오.

감사 로그 클라이언트 인증서 보기: Management Center

로그인한 어플라이언스에 대해서만 감사 로그 클라이언트 인증서를 볼 수 있습니다. management center 고가용성 쌍에서는 활성 피어의 인증서만 볼 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Audit Log Certificate(**감사 로그 인증서**)**를 클릭합니다.

검증 변경

사용자가 변경하는 내용을 모니터링하고 그러한 변경이 회사의 기본 표준을 따르는지 확인하려면 지난 24시간 동안 변경 사항의 자세한 보고서를 이메일로 전송하도록 시스템을 구성할 수 있습니다. 사용자가 시스템 구성에 변경 사항을 저장할 때마다 변경에 대한 스냅샷이 생성됩니다. 변경 조정 보고서는 이러한 스냅샷의 정보를 결합하여 최신 시스템 변경 사항에 대한 명확한 요약을 제공합니다.

다음 샘플 그림에는 예제 변경 조정 보고서의 User 페이지가 표시되며, 각 구성의 이전 값과 변경 이후의 값이 모두 나열되어 있습니다. 여러 사용자가 동일한 구성을 여러 번 변경하면 보고서에는 최근 것부터 시간순으로 각 변경 사항의 요약이 나열됩니다.

지난 24시간 동안 변경된 내용을 볼 수 있습니다.

검증 변경 구성

시작하기 전에

- 이메일 서버가 24시간 동안 시스템 변경 사항에 대한 이메일 보고서를 수신하도록 구성합니다. 자세한 내용은 메일 릴레이 호스트 및 알림 주소 구성, 62 페이지 섹션을 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Change Reconciliation(**검증 변경**)**을 클릭합니다.

단계 **3** **Enable(**사용**)** 확인란을 선택합니다.

단계 **4** 시스템에서 변경 검증 보고서를 전송하도록 할 시간을 **Time to Run(**실행 시간**)** 드롭다운 목록에서 선택합니다.

단계 **5** **Email to(**수신자**)** 필드에 이메일 주소를 입력합니다.

팁 이메일 주소를 추가한 후 **Resend Last Report(**마지막 보고서 다시 보내기**)**를 클릭하여 받는 사람에게 최신 변경 검증 보고서 사본을 전송합니다.

단계 **6** 정책 변경 사항을 포함하려면 **Include Policy Configuration(**정책 구성 포함**)** 확인란을 선택합니다.

단계 **7** 지난 24시간 동안 모든 변경 사항을 포함하려는 경우 **Show Full Change History(**전체 변경 기록 표시**)** 확인란을 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

감사 로그를 사용하여 변경 검사, 422 페이지

검증 변경 옵션

Include Policy Configuration(정책 구성 포함**)** 옵션은 시스템에 정책 변경 기록이 변경 검증 보고서에 포함되는지 여부를 제어합니다. 여기에는 액세스 제어, 침입, 시스템, 상태 및 네트워크 검색 정책에 대한 변경 사항이 포함됩니다. 이 옵션을 선택하지 않으면 정책에 대한 변경 사항이 보고서에 표시되지 않습니다. 이 옵션은 management center에서만 사용할 수 있습니다.

Show Full Change History(전체 변경 기록 표시**)** 옵션은 시스템이 변경 검증 보고서에 지난 24시간 동안 발생한 모든 변경 사항의 기록을 포함할지 여부를 제어합니다. 이 옵션을 선택하지 않으면 보고서에는 각 카테고리에 대한 변경 사항의 통합된 보기만 포함됩니다.

참고 변경 조정 보고서에는 threat defense 인터페이스 및 라우팅 설정에 대한 변경 사항이 포함되지 않습니다.

DNS 캐시

이벤트 보기 페이지에서 자동으로 IP 주소를 확인하도록 시스템을 구성할 수 있습니다. 어플라이언스가 수행하는 DNS 캐싱의 기본 등록 정보를 구성할 수도 있습니다. DNS 캐싱을 구성하면 추가 조회를 수행하지 않고도 전에 확인한 IP 주소를 식별할 수 있습니다. 이렇게 하면 네트워크의 트래픽 양을 줄이고, IP 주소 확인이 활성화된 경우 이벤트 페이지의 표시 속도를 높일 수 있습니다.

DNS 캐시 속성 설정

DNS 확인 캐싱은 전에 확인된 DNS 조회의 캐싱을 허용하는 시스템 전체의 설정입니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **DNS Cache(DNS** 캐시**)**를 선택합니다.

단계 **3** **DNS Resolution Caching(DNS** 확인 캐싱**)** 드롭다운 목록에서 다음 중 하나를 선택합니다.

- **Enabled(**활성화**)** - 캐싱을 활성화합니다.
- **Disabled(**비활성화**)** - 캐싱을 비활성화합니다.

단계 **4** DNS 항목이 제거되어 비활성화되기 전 메모리에 캐시되어 머무는 시간(분)을 **DNS Cache Timeout (in minutes)** 필드에 입력합니다.

기본 설정은 300분(5시간)입니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

관련 항목

이벤트 보기 구성, 210 페이지

대시보드

대시보드는 시스템의 여러 부분에 대한 통찰력을 제공하는 소규모의 자족적 구성 요소인 위젯을 사용하여 현재 시스템 상태에 대한 간략한 보기를 제공합니다. 시스템은 여러 대시보드 위젯이 사전 정의된 상태로 제공됩니다.

맞춤형 분석 위젯이 대시보드에서 활성화되도록 management center를 구성할 수 있습니다.

관련 항목

대시보드 정보, 345 페이지

대시보드에 대한 맞춤형 분석 위젯 활성화

맞춤형 분석 대시보드 위젯을 사용하여 유연하고 사용자가 구성할 수 있는 쿼리를 기반으로 이벤트를 시각적으로 표현할 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Dashboard(**대시보드**)**를 클릭합니다.

단계 **3** 사용자가 Custom Analysis 위젯을 대시보드에 추가하도록 허용하려면 **Enable Custom Analysis Widgets(**맞춤형 분석 위젯 활성화**)** 확인란을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

관련 항목

대시보드 정보, 345 페이지

데이터베이스

디스크 공간을 관리하기 위해서 management center은 이벤트 데이터베이스에서 가장 오래된 침입 이벤트, 감사 기록, 보안 인텔리전스 데이터 또는 URL 필터링 데이터를 자동으로 제거합니다. 각 이벤트 유형에 대해 정리 후 management center가 보유할 레코드 수를 지정할 수 있습니다. 해당 유형에 대해 구성된 보유 제한보다 많은 유형의 레코드를 포함하는 이벤트 데이터베이스에도 의존하지 않습니다. 성능을 높이려면 정기적으로 작업하는 이벤트 수에 대한 이벤트 제한을 조정해야 합니다. 선택적으로 정리가 발생할 때 이메일 알림을 수신하도록 선택할 수 있습니다. 일부 이벤트 유형의 경우 스토리지를 비활성화할 수 있습니다.

개별 이벤트를 수동으로 삭제하려면 이벤트 뷰어를 사용합니다. (버전 6.6.0 이상에서는 이러한 방식으로 연결 또는 보안 인텔리전스 이벤트를 수동으로 삭제할 수 없습니다.) 데이터베이스를 수동으로 제거할 수도 있습니다. 데이터 비우기 및 저장, 531 페이지의 내용을 참조하십시오.

데이터베이스 이벤트 제한 구성

시작하기 전에

- 이벤트가 management center 데이터베이스에서 정리될 때 이메일 알림을 받으려면 이메일 서버를 구성해야 합니다. 메일 릴레이 호스트 및 알림 주소 구성, 62 페이지 섹션을 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Database(**데이터베이스**)**를 선택합니다.

단계 **3** 각 데이터베이스에 대해 저장할 레코드의 수를 입력합니다.

각 데이터베이스가 유지 관리할 레코드 수에 대한 정보는 데이터베이스 이벤트 제한 수, 60 페이지 섹션을 참조하십시오.

단계 **4** 선택적으로 **Data Pruning Notification Address(**데이터 제거 알림 주소**)** 필드에 제거 알림을 수신할 이메일 주소를 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

데이터베이스 이벤트 제한 수

다음 표에는 management center당 저장할 수 있는 각 이벤트 유형의 최소 및 최대 레코드 수가 나열되어 있습니다.

표 *1:* 데이터베이스 이벤트 제한 수

이벤트 유형	상한 제한	하한 제한
침입 이벤트	1,000만(management center Virtual) 3,000만(management center1000, management center1600) 6,000만(management center2500, management center2600, FMCv 300) 3억(management center4500, management center4600)	10,000
검색 이벤트	1,000만(management center Virtual) 2,000만(management center2500, management center2600, management center4500, management center4600, FMCv 300)	0(스토리지 비활성화)
연결 이벤트 보안 인텔리전스 이벤트	5,000만(management center Virtual) 1억(management center1000, management center1600) 3억(management center2500, management center2600, FMCv 300) 10억(management center4500, management center4600) 제한은 연결 이벤트와 보안 인텔리전스 이벤트 간에 공유됩니다. 구성된 최대 값의 합은 이 제한을 초과할 수 없습니다.	0(스토리지 비활성화) **Maximum Connection Events(**최대 연결 이벤트**)** 값을 0으로 설정하면 보안 인텔리전스, 침입, 파일 및 악성 코드 이벤트와 연결되지 않은 연결 이벤트가 management center에 저장되지 않습니다. 주의 **Maximum Connection Events(**최대 연결 이벤트**)**를 0으로 설정하면 보안 인텔리전스 이벤트 이외의 기존 연결 이벤트가 즉시 제거됩니다. 이 설정이 최대 플로우 속도에 미치는 영향은 아래를 참조하십시오. 이러한 설정은 연결 요약에 영향을 주지 않습니다.

이벤트 유형	상한 제한	하한 제한
연결 요약(취합된 연결 이벤트)	5,000만(management center Virtual) 1억(management center1000, management center1600) 3억(management center2500, management center2600, FMCv 300) 10억(management center4500, management center4600)	0(스토리지 비활성화)
상관관계 이벤트 및 컴플라이언스 허용 목록 이벤트	1만(management center Virtual) 200만(management center2500, management center2600, management center4500, management center4600, FMCv 300)	1개
악성코드 이벤트	1,000만(management center Virtual) 2,000만(management center2500, management center2600, management center4500, management center4600, FMCv 300)	10,000
파일 이벤트	1,000만(management center Virtual) 2,000만(management center2500, management center2600, management center4500, management center4600, FMCv 300)	0(스토리지 비활성화)
상태 이벤트	100만	0(스토리지 비활성화)
감사 기록	100,000	1개
교정 상태 이벤트	1,000만	1개
허용 리스트 위반 기록	30일 위반 기록	일일 이력
사용자 활동(사용자 이벤트)	1,000만	1개
사용자 로그인(사용자 이력)	1,000만	1개
침입 규칙 업데이트 가져오기 로그 기록	1백만	1개

이벤트 유형	상한 제한	하한 제한
VPN 문제 해결 데이터베이스	1,000만	0(스토리지 비활성화)

최대 플로우 속도

management center 하드웨어 모델의 **Maximum flow rate(**최대 플로우 속도**)**(초당 흐름) 값은 https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html?cachemode=refresh에 있는 management center데이터시트의 **Platform Specifications(**플랫폼 사양**)** 섹션에 나와 있습니다.

플랫폼 설정에서 **Maximum Connection Events(**최대 연결 이벤트**)**값을 0으로 설정하면 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트와 연결되지 않은 연결 이벤트는 management center 하드웨어의 최대 플로우 속도에 포함되지 않습니다.

이 필드의 값이 0이 아니면 모든 연결 이벤트가 최대 플로우 속도로 계산됩니다.

이 페이지의 다른 이벤트 유형은 최대 플로우 속도에 포함되지 않습니다.

이메일 알림

다음을 수행하려는 경우 메일 호스트를 구성합니다.

- 이벤트 기반 보고서 이메일 전송
- 예약 작업에 대한 상태 보고서 이메일 전송
- 변경 검증 보고서 이메일 전송
- 데이터 정리 알림 이메일 전송
- 검색 이벤트, 영향 플래그, 상관 이벤트 알림, 침입 이벤트 알림 및 상태 이벤트 알림에 이메일 사용

이메일 알림을 구성할 때 시스템과 메일 릴레이 호스트 간 통신을 위한 암호화 방법을 선택할 수 있고 필요한 경우 메일 서버의 인증 자격 증명을 제공할 수 있습니다. 구성한 후 연결을 테스트할 수 있습니다.

메일 릴레이 호스트 및 알림 주소 구성

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을 선택합니다.

단계 **2** **Email Notification(**이메일 알림**)**을 클릭합니다.

단계 **3** **Mail Relay Host(**메일 릴레이 호스트**)** 필드에서 사용할 메일 서버의 호스트 이름 또는 IP 주소를 입력합니다. 입력한 메일 호스트는 어플라이언스의 액세스를 허용해야 합니다.

단계 **4** **Port Number(**포트 번호**)** 필드에 이메일 서버에서 사용할 포트 번호를 입력합니다.

일반적인 포트는 다음과 같습니다.

- 25: 암호화를 사용하지 않는 경우
- 465: SSLv3를 사용하는 경우
- 587: TLS를 사용하는 경우

단계 **5** **Encryption(**암호화**)** 방법을 선택합니다.

- **TLS**-전송 계층 보안을 사용하여 통신을 암호화합니다
- **SSLv3**-Secure Socket Layer을 사용 하 여 통신을 암호화 합니다.
- **None (**없음**)**-암호화 되지 않은 통신을 허용 합니다.

참고 어플라이언스와 메일 서버 간의 암호화된 통신에는 인증서 유효성 검사가 필요하지 않습니다.

단계 **6** **From Address(**보낸 사람 주소**)** 필드에 어플라이언스에서 보낸 메시지의 원본 이메일 주소로 사용할 유효한 이메일 주소를 입력합니다.

단계 **7** 선택적으로 메일 서버에 연결할 때 사용자 이름과 비밀번호를 입력하려면 **Use Authentication(**인증 사용**)**을 선택합니다. **Username(**사용자 이름**)** 필드에 사용자 이름을 입력합니다. **Password(**비밀번호**)** 필드에 비밀번호를 입력합니다.

단계 **8** 구성된 메일 서버를 사용하는 테스트 이메일을 전송하려면 **Test Mail Server Settings(**메일 서버 설정 테스트**)**를 클릭합니다.

테스트의 성공 또는 실패를 나타내는 메시지가 버튼 옆에 나타납니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

External Database Access(외부 데이터베이스 액세스)

서드파티 클라이언트에 데이터베이스에 대한 읽기 전용 액세스를 허용하도록 management center를 구성할 수 있습니다. 그러면 다음 중 하나를 사용하여 SQL로 데이터베이스에 쿼리할 수 있습니다.

- Actuate BIRT, JasperSoft iReport 또는 Crystal Reports와 같은 산업 표준 보고 툴
- JDBC SSL 연결을 지원하는 기타 보고 애플리케이션(사용자 지정 애플리케이션 포함)
- 인터랙티브 방식으로 실행하거나 단일 쿼리에 대해 쉼표로 구분된 결과를 얻기 위해 사용할 수 있는 RunQuery라는 Cisco 제공 명령줄 Java 애플리케이션

management center의 시스템 구성을 사용하여 데이터베이스 액세스를 활성화하고 선택한 호스트가 데이터베이스를 쿼리할 수 있도록 액세스 목록을 만듭니다. 이 액세스 목록은 어플라이언스 액세스를 제어하지 않습니다.

다음이 포함된 패키지를 다운로드할 수도 있습니다.

- RunQuery - Cisco 제공 데이터베이스 쿼리 툴
- InstallCert - 액세스하려는 management center에서 SSL 인증서를 검색하고 승인하기 위해 사용할 수 있는 툴
- 데이터베이스에 연결하기 위해 사용해야 하는 JDBC 드라이버

데이터베이스 액세스를 구성하기 위해 다운로드한 패키지의 툴 사용에 대한 내용은 *Firepower System* 데이터베이스 액세스 설명서 섹션을 참조하십시오.

데이터베이스에 대한 외부 액세스 활성화

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **External Database Access(**외부 데이터베이스 액세스**)**를 클릭합니다.

단계 **3** **Allow External Database Access**(외부 데이터베이스 액세스 허용) 확인란을 선택합니다.

단계 **4** **Server Hostname(**서버 호스트네임**)** 필드에 적절한 값을 입력합니다. 서드파티 애플리케이션 요건에 따라 이 값은 management center의 QDN(정규화된 도메인 이름), IPv4 주소 또는 IPv6 주소일 수 있습니다.

참고 management center 고가용성 설정에서는 활성 피어 세부 정보만 입력합니다. 스탠바이 피어의 세부 정보는 입력하지 않는 것이 좋습니다.

단계 **5** **Client JDBC Driver**(클라이언트 JDBC 드라이버) 옆에 있는 **Download**(다운로드)를 클릭하고 브라우저의 지시에 따라 `client.zip` 패키지를 다운로드합니다.

단계 **6** 하나 이상의 IP 주소에 대한 데이터베이스 액세스를 추가하려면 **Add Hosts**(호스트 추가)를 클릭합니다. **Access List**(액세스 목록) 필드에 **IP Address**(IP 주소) 필드가 나타납니다.

단계 **7** **IP** 주소 필드에 IP 주소 또는 어드레스 레인지 또는 `모두`를 입력하십시오.

단계 **8** **Add(**추가**)**를 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

팁 마지막으로 저장된 데이터베이스 설정으로 되돌리려면 **Refresh(**새로 고침**)**를 클릭합니다.

관련 항목

Firepower System IP 주소 규칙, 28 페이지

HTTPS 인증서

SSL(Secure Sockets Layer)/TLS 인증서를 사용하면 management center 시스템과 웹 브라우저 간에 암호화된 채널을 활성화할 수 있습니다. 기본 인증서는 모든 Firepower 디바이스에 포함되어 있지만 전역적으로 알려진 CA가 신뢰할 수 있는 인증 기관(CA)에서 생성되지는 않습니다. 따라서 전역적으로 알려졌거나 내부에서 신뢰할 수 있는 CA가 서명한 사용자 정의 인증서로 교체하는 것이 좋습니다.

주의 management center는 4096 비트 HTTPS 인증서를 지원합니다. management center에서 사용 중인 인증서가 4096비트보다 큰 공개 서버 키로 생성되었다면 management center 웹 인터페이스에 로그인할 수 없습니다. 이러한 현상이 발생한다면 Cisco TAC에 문의하십시오.

참고 HTTPS 인증서는 Management Center REST API에서 지원되지 않습니다.

기본 HTTPS 서버 인증서

어플라이언스와 함께 제공된 기본 서버 인증서를 사용하는 경우 기본 서버 인증서가 클라이언트 인증서에 서명한 CA에 의해 서명되지 않았으므로 시스템에서 웹 인터페이스 액세스에 유효한 HTTPS 클라이언트 인증서를 요구하도록 구성하지 마십시오.

기본 서버 인증서의 수명은 인증서가 생성된 시점에 따라 달라집니다. 기본 서버 인증서 만료일을 보려면 시스템 (⚙) > **Configuration(구성)** > **HTTPS Certificate(HTTPS 인증서)**을 선택합니다.

일부 Firepower 소프트웨어 업그레이드는 인증서를 자동으로 갱신할 수 있습니다. 자세한 내용은 Cisco Firepower 릴리스 노트를 참조하십시오.

management center 시스템 (⚙) > **Configuration(구성)** > **HTTPS Certificate(HTTPS 인증서)** 페이지에서 기본 인증서를 갱신할 수 있습니다.

맞춤형 HTTPS 서버 인증서

사용자가 제공하는 시스템 정보 및 ID 정보에 따라 management center 웹 인터페이스를 사용하여 서버 인증서 요청을 생성할 수 있습니다. 브라우저가 신뢰하는 설치된 내부 인증 기관(CA)이 있는 경우 요청을 사용하여 인증서에 서명할 수 있습니다. 또한 인증 기관에 서버 인증서를 요청하는 결과 요청을 보낼 수 있습니다. 인증 기관(CA)으로부터 서명된 인증서를 확보한 후, 이를 가져올 수 있습니다.

HTTPS 서버 인증서 요구 사항

HTTPS 인증서를 이용하여 웹 브라우저와 Firepower 어플라이언스 웹 인터페이스 간의 연결을 보호한다면 Internet X.509 Public Key Infrastructure Certificate(인터넷 X.509 공개 키 인프라 인증서) 및 CRL(Certificate Revocation List) 프로파일(RFC 5280)을 준수하는 인증서를 사용해야 합니다. 서버 인

증서를 어플라이언스로 가져올 때, 해당 표준의 버전 3(x.509 v3)을 준수하지 않는다면 시스템은 인증서를 거부합니다.

HTTPS 서버 인증서를 가져오기 전에 다음 필드가 있는지 확인하십시오.

인증서 필드	설명
버전	인코딩된 인증서의 버전입니다. 버전 3을 사용합니다. RFC 5280, 섹션 4.1.2.1을 참조하십시오.
일련 번호	발급 CA에 의해 인증서에 할당된 양의 정수입니다. 발급자와 일련번호 조합으로 인증서를 고유하게 식별합니다. RFC 5280, 섹션 4.1.2.2를 참조하십시오.
서명	인증서 서명을 위해 CA에서 사용하는 알고리즘의 식별자입니다. signatureAlgorithm 필드와 일치해야 합니다. RFC 5280, 섹션 4.1.2.3을 참조하십시오.
발급자	인증서를 서명하고 발급한 개체를 식별합니다. RFC 5280, 섹션 4.1.2.4를 참조하십시오.
유효성	CA가 인증서 상태 관련 정보를 유지를 보장하는 간격입니다. RFC 5280, 섹션 4.1.2.5를 참조하십시오.
제목	주체 공개 키 필드에 저장된 공개 키와 연결된 엔터티를 식별합니다. X.500 DN(disinguished name)이어야 합니다. RFC 5280, 섹션 4.1.2.6을 참조하십시오.
주체 대체 이름	인증서로 보호되는 도메인 이름 및 IP 주소입니다. 주체 대체 이름은 RFC 5280, 섹션 4.2.1.6에 정의되어 있습니다. 인증서가 여러 도메인 또는 IP 주소에 사용되는 경우, 이 필드를 활용하는 것이 좋습니다.
주체 공개 키 정보	알고리즘에 대한 공개 키 및 식별자입니다. RFC 5280, 섹션 4.1.2.7을 참조하십시오.
기관 키 식별자	인증서 서명에 사용한 개인 키에 대응하는 공개 키를 식별하는 방법을 제공합니다. RFC 5280, 섹션 4.2.1.1을 참조하십시오.
주체 키 식별자	특정 공개 키를 포함하는 인증서를 식별하는 방법을 제공합니다. RFC 5280, 섹션 4.2.1.2를 참조하십시오.

인증서 필드	설명
키 사용	인증서에 포함된 키의 용도를 정의합니다. RFC 5280, 섹션 4.2.1.3을 참조하십시오.
기본 제한조건	인증서 주체가 CA인지 여부와, 이 인증서를 포함하는 유효한 인증 경로의 최대 수준을 식별합니다. RFC 5280, 섹션 4.2.1.9를 참조하십시오. Firepower 어플라이언스에서 사용하는 서버 인증서의 경우에는 `critical CA: FALSE`를 사용합니다.
확장된 키 사용 확장	키 사용 확장에 나온 기본 용도 외에, 인증된 공개 키를 사용하는 하나 이상의 용도를 나타냅니다. RFC 5280, 섹션 4.2.1.12를 참조하십시오. 서버 인증서로 사용할 수 있는 인증서를 가져와야 합니다.
signatureAlgorithm	인증서 서명을 위해 CA에서 사용하는 알고리즘의 식별자입니다. Signature(서명) 필드와 일치해야 합니다. RFC 5280, 섹션 4.1.1.2를 참조하십시오.
signatureValue	디지털 서명입니다. RFC 5280, 섹션 4.1.1.3을 참조하십시오.

HTTPS 클라이언트 인증서

클라이언트 브라우저 인증서 확인을 사용하여 Firepower System 웹 서버에 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. 브라우저는 다음과 같은 경우 웹 인터페이스를 로드할 수 없습니다.

- 사용자가 유효하지 않은 브라우저에서 인증서를 선택합니다.
- 사용자가 브라우저에서 서버 인증서에 서명한 인증 기관이 생성하지 않은 인증서를 선택합니다.
- 사용자가 브라우저에서 디바이스의 인증서 체인에 있는 인증 기관이 생성하지 않은 인증서를 선택합니다.

클라이언트 브라우저 인증서를 확인하려면 OCSP(Online Certificate Status Protocol)를 사용하거나 하나 이상의 인증서 해지 목록(CRL)을 로드하도록 시스템을 구성합니다. OCSP를 사용하여 웹 서버가 연결 요청을 받으면 연결을 설정하기 전에 인증 기관과 통신하여 클라이언트 인증서의 유효성을 확인합니다. 하나 이상의 CRL을 로드하도록 서버를 구성하면 웹 서버는 클라이언트 인증서를 CRL에 나열된 인증서와 비교합니다. 사용자가 해지된 인증서로서 CRL에 나열된 인증서를 선택한 경우, 브라우저는 웹 인터페이스를 로드할 수 없습니다.

참고 CRL을 사용하여 인증서를 확인하도록 선택하면 시스템은 동일한 CRL을 사용하여 클라이언트 브라우저 인증서와 감사 로그 서버 인증서의 유효성을 확인합니다.

현재 **HTTPS** 서버 인증서 보기

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

HTTPS 서버 인증서 서명 요청 생성

웹 인터페이스에 연결할 때 전역으로 알려졌거나 내부적으로 신뢰할 수 있는 CA에서 서명되지 않은 인증서를 설정하는 경우 사용자의 브라우저에 보안 경고가 표시됩니다.

CSR(인증서 서명 요청)은 생성한 어플라이언스 또는 디바이스별로 고유합니다. 단일 어플라이언스에서 여러 디바이스에 대한 CSR을 생성할 수는 없습니다. 모든 필드는 선택 사항이지만 CN, Organization(조직), Organization Unit(조직 단위), City/Locality (구/군/시), State/Province(주/도), Country/Region(국가/지역) 및 Subject Alternative Name(주체 대체 이름)의 값을 입력하는 것이 좋습니다.

인증서 요청에 대해 생성된 키는 Base-64로 인코딩된 PEM 형식입니다.

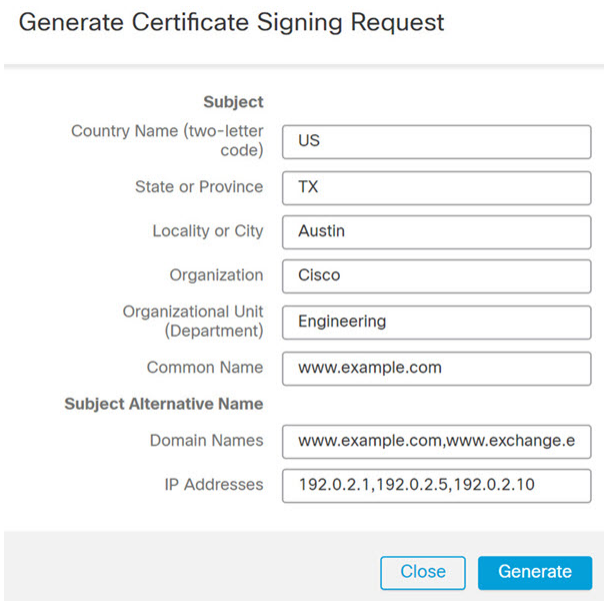
프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

단계 **3** **Generate New CSR(**새로운 **CSR** 생성**)**을 클릭합니다.

다음 그림은 예를 보여줍니다.



단계 **4** **Country Name (two-letter code)(**국가 이름**(2**글자 코드**))** 필드에 국가 번호를 입력합니다.

단계 **5** **State or Province(**주 또는 도**)** 필드에 주 또는 도에 대한 우편 약자를 입력합니다.

단계 **6** **Locality or City(**구/군/시**)**를 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 올바르게 입력합니다.

참고 **Common Name(**공용 이름**)** 필드의 인증서에 나타나도록 서버의 정규화된 도메인 이름을 올바르게 입력합니다. 공용 이름과 DNS 호스트 이름이 일치하지 않는 경우, 어플라이언스에 연결하면 경고를 받습니다.

단계 **10** 여러 도메인 이름 또는 IP 주소를 보호하는 인증서를 요청하려면 주체 대체 이름 섹션에 다음 정보를 입력합니다.

a) **Domain Names(**도메인 이름**)**: 주체 대체 이름으로 보호되는 정규화된 도메인 및 하위 도메인 (있는 경우)을 입력합니다.

b) **IP Addresses(IP** 주소**)**: 주체 대체 이름으로 보호되는 IP 주소를 입력합니다.

단계 **11** **Generate(**생성**)**를 클릭합니다.

단계 **12** 텍스트 편집기를 엽니다.

단계 **13** `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 **14** 파일을 `servername.csr`로 저장합니다. 여기서 *servername*은 인증서 사용을 계획하고 있는 서버의 이름입니다.

단계 **15** **Close(**닫기**)**를 클릭합니다.

다음에 수행할 작업

- 인증서 요청을 인증 기관에 제출합니다.
- 서명된 인증서를 수신하면 해당 인증서를 management center에 가져옵니다. HTTPS 서버 인증서 가져오기, 70 페이지 섹션을 참조하십시오.

HTTPS 서버 인증서 가져오기

인증서를 생성한 서명 기관이 중간 CA를 신뢰하기를 요청하는 경우, 또한 인증서 체인(또는 인증서 경로)을 제공해야 합니다.

클라이언트 인증서가 필요한 경우 서버 인증서가 다음 기준 중 하나를 충족하지 않으면 웹 인터페이스를 통해 어플라이언스에 액세스할 수 없습니다.

- 인증서는 클라이언트 인증서에 서명한 동일한 CA에 의해 서명됩니다.
- 인증서는 인증서 체인의 중간 인증서에 서명한 CA에 의해 서명됩니다.

주의 management center는 4096비트 HTTPS 인증서를 지원합니다. management center에서 사용 중인 인증서가 4096비트보다 큰 공개 서버 키로 생성되었다면 Secure Firewall Management Center 웹 인터페이스에 로그인할 수 없습니다. HTTPS 인증서를 버전 6.0.0으로 업데이트하는 방법에 대한 자세한 내용은 *Firepower System* 릴리스 노트 버전 *6.0*입니다.의 "Management Center HTTPS 인증서를 버전 6.0으로 업데이트"를 참조하십시오. HTTPS 인증서를 생성하거나 가져오고 management center 웹 인터페이스에 로그인할 수 없는 경우 지원 부서에 문의하십시오.

시작하기 전에

- 인증서 서명 요청을 생성합니다. HTTPS 서버 인증서 서명 요청 생성, 68 페이지 섹션을 참조하십시오.
- 인증서를 요청할 인증 기관에 CSR 파일을 업로드하거나 CSR를 사용하여 자체 서명된 인증서를 만드십시오.
- 인증서가 HTTPS 서버 인증서 요구 사항, 65 페이지에서 설명하는 요구 사항을 충족하는지 확인합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

단계 **3** **Import HTTPS Server Certificate(HTTPS** 서버 인증서 가져오기**)**를 클릭합니다.

참고 암호화된 HTTPS 인증서는 가져올 수 없습니다.

단계 4 텍스트 편집기에서 서버 인증서를 열고 `BEGIN CERTIFICATE` 및 `END CERTIFICATE` 행이 포함된 전체 텍스트 블록을 복사합니다. **Server Certificate(**서버 인증서**)** 필드에 이 텍스트를 붙여 넣습니다.

단계 5 **Private Key(**개인 키**)**를 제공해야 하는지 여부는 인증서 서명 요청을 생성한 방법에 따라 다릅니다.

- HTTPS 서버 인증서 서명 요청 생성, 68 페이지에 설명된 대로 Secure Firewall Management Center 웹 인터페이스를 사용하여 인증서 서명 요청을 생성한 경우 시스템에 이미 개인 키가 있으므로 여기에 비밀번호를 입력할 필요가 없습니다.
- 다른 방법을 사용하여 인증서 서명 요청을 생성한 경우 여기에 개인 키를 제공해야 합니다. 개인 키 파일을 열고 `BEGIN RSA PRIVATE KEY` 및 `END RSA PRIVATE KEY` 행이 포함된 전체 텍스트 블록을 복사합니다. **Private Key(**개인 키**)** 필드에 이 텍스트를 붙여 넣습니다.

단계 6 필요한 중간 인증서를 열어서 전체 텍스트 블록을 복사하여 각각을 **Certificate Chain(**인증서 체인**)** 필드에 붙여 넣습니다. 루트 인증서를 받은 경우 여기에 붙여넣습니다. 중간 인증서를 받은 경우 루트 인증서 아래에 붙여넣습니다. 두 경우 모두 `BEGIN CERTIFICATE`(인증서 시작) 및 `END CERTIFICATE`(인증서 끝)를 포함하는 전체 텍스트 블록을 복사합니다.

단계 7 **Save(**저장**)**를 클릭합니다.

유효한 HTTPS 클라이언트 인증서 필요

사용자가 management center 웹 인터페이스에 연결하여 사용자 인증서를 제공하도록 하려면 이 절차를 사용합니다. 시스템은 OCSP 또는 PEM(Privacy-Enhanced Mail) 형식으로 가져온 CRL을 사용하여 HTTPS 클라이언트 인증서 확인을 지원합니다.

CRL을 사용하기로 선택하는 경우 해지된 인증서 목록이 통용되고 있음을 확인하기 위해, CRL을 업데이트하는 예약된 작업을 생성할 수 있습니다. 시스템에 CRL의 최신 새로 고침이 표시됩니다.

참고 클라이언트 인증서를 활성화한 후 웹 인터페이스에 액세스하려면 반드시 사용자 브라우저(또는 판독기에 삽입된 CAC)에 유효한 사용자 인증서가 있어야 합니다.

시작하기 전에

- 연결에 사용할 클라이언트 인증서에 서명한 것과 동일한 인증 기관에서 서명한 서버 인증서를 가져옵니다. HTTPS 서버 인증서 가져오기, 70 페이지 섹션을 참조하십시오.
- 필요한 경우 서버 인증서 체인을 가져옵니다. HTTPS 서버 인증서 가져오기, 70 페이지 섹션을 참조하십시오.

프로시저

단계 1 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 2 **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

단계 **3** **Enable Client Certificates(**클라이언트 인증서 활성화**)**를 선택합니다. 메시지가 표시되면, 드롭다운 목록에서 적절한 인증서를 선택합니다.

단계 **4** 3가지 옵션이 제공됩니다.

- 하나 이상의 CRL을 사용하여 클라이언트 인증서를 확인하려면 **Enable Fetching of CRL(CRL** 가져오기 사용**)**을 선택하고 5단계로 계속 진행합니다.
- OCSP를 사용하여 클라이언트 인증서를 확인하려면 **Enable OCSP(OCSP** 활성화**)**를 선택하고 7단계로 건너뜁니다.
- 해지를 확인하지 않고 클라이언트 인증서를 허용하려면 8단계로 건너뜁니다.

단계 **5** 기존 CRL 파일에 유효한 URL을 입력하고 **Add CRL(CRL** 추가**)**을 클릭합니다. 최대 25개의 CRL을 추가하려면 반복합니다.

단계 **6** **Refresh CRL(CRL** 새로 복구**)**을 클릭하여 지정된 URL에서 현재 CRL을 로드합니다.

참고 CRL 가져오기를 활성화하면 정기적으로 CRL을 업데이트하는 예약된 작업을 생성합니다. 작업을 수정하여 업데이트의 빈도를 설정합니다.

단계 **7** 어플라이언스에 로드된 인증 기관에서 클라이언트 인증서를 서명했는지, 브라우저 인증서 저장소에 로드된 인증 기관이 서버 인증서를 서명했는지 확인합니다. (동일한 인증 기관이어야 함)

주의 브라우저 인증서 저장소에 유효한 클라이언트 인증서가 없는 클라이언트 인증서가 활성화된 구성을 저장하면 어플라이언스에 대한 모든 웹 서버 액세스가 비활성화됩니다. 구성을 저장하기 전에 설치된 유효한 클라이언트 인증서가 있는지 확인합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

CRL(Certificate Revocation List) 다운로드 구성, 505 페이지

기본 HTTPS 서버 인증서 갱신

로그인한 어플라이언스의 서버 인증서만 볼 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

이 버튼은 시스템이 기본 HTTPS 서버 인증서를 사용하도록 구성된 경우에만 나타납니다.

단계 **3** **Renew HTTPS Certificate(HTTPS** 인증서 갱신**)**을 클릭합니다. (이 옵션은 시스템이 기본 HTTPS 서버 인증서를 사용하도록 구성된 경우에만 인증서 정보 아래 화면에 나타납니다.)

단계 **4** (선택 사항) **Renew HTTPS Certificate(HTTPS** 인증서 갱신**)** 대화 상자에서 인증서에 대한 새 키를 생성하기 위한 **Generate New Key(**새 키 생성**)**를 선택합니다.

단계 **5** **Renew HTTPS Certificate(HTTPS** 인증서 갱신**)** 대화 상자에서 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

HTTPS Certificate(HTTPS 인증서**)** 페이지에 표시된 인증서 유효 기간이 업데이트되었는지 확인하여 인증서가 갱신되었는지 확인할 수 있습니다.

정보

웹 인터페이스의 **System(**시스템**) > Configuration(**구성**)** 페이지에는 아래 표에 나열된 정보가 포함됩니다. 달리 명시되지 않는 한 모든 필드는 읽기 전용입니다.

참고 **Help(**도움말**) > About(**정보**(** 페이지를 참조하십시오. 비슷하지만 약간 다른 정보를 제공합니다.

필드	설명
이름	management center어플라이언스에 할당한 설명 이름입니다. 어플라이언스 이름으로 호스트 이름을 사용할 수 있지만 이 필드에 다른 이름을 입력해도 호스트 이름은 변경되지 않습니다. 이 이름은 특정 통합에서 사용됩니다. 예를 들어 SecureX 및 SecureX threat response와의 통합을 위해 디바이스 목록에 표시됩니다. 이름을 변경하면 등록된 모든 디바이스가 오래된 것으로 표시되며 디바이스에 새 이름을 푸시하려면 구축이 필요합니다.
제품 모델	어플라이언스의 모델 이름입니다.
일련 번호	어플라이언스의 일련 번호입니다.
소프트웨어 버전	어플라이언스에 현재 설치된 소프트웨어 버전입니다.
운영 체제	현재 어플라이언스에서 실행되는 운영 체제입니다.
운영 체제 버전	현재 어플라이언스에서 실행되는 운영 체제의 버전입니다.
IPv4 주소	기본(`eth0`) 관리 인터페이스의 IPv4 주소입니다. IPv4 관리가 비활성화된 경우, 이 필드는 이를 나타냅니다.
IPv6 주소	기본(`eth0`) 관리 인터페이스의 IPv6 주소입니다. IPv6 관리가 비활성화된 경우, 이 필드는 이를 나타냅니다.
현재 정책	현재 구축된 시스템 레벨 정책입니다. 마지막으로 구축된 후부터 정책이 업데이트된 경우, 정책 이름은 기울임 꼴로 표시됩니다.

필드	설명
모델 번호	내부 플래시 드라이브에 저장된 어플라이언스별 모델 번호입니다. 이 번호는 문제 해결을 위해 중요할 수 있습니다.

침입 정책 환경 설정

사용자가 침입 정책을 수정할 때 코멘트 기능을 사용하여 정책 관련 변경 사항을 추적하도록 시스템을 구성할 수 있습니다. 정책 변경 코멘트를 활성화하면 관리자는 배포의 중요한 정책이 수정된 이유를 신속하게 평가할 수 있습니다.

정책 변경에 대한 코멘트를 활성화하는 경우, 코멘트를 선택 사항 또는 의무 사항으로 설정할 수 있습니다. 정책에 대한 새로운 변경 사항이 저장될 때마다 시스템은 사용자에게 코멘트를 입력하라는 메시지를 표시합니다.

필요에 따라 감사 로그에 작성된 침입 정책을 변경할 수 있습니다.

LSP 업데이트 중에 재정의된 시스템 정의 규칙의 변경 사항에 대한 알림을 받으려면 **Retain user overrides for deleted Snort 3 rules(**삭제된 **Snort 3** 규칙에 대한 사용자 재정의 유지**)** 체크 박스가 선택되어 있는지 확인합니다. 시스템 기본값으로 이 체크 박스는 선택되어 있습니다. 이 체크 박스를 선택하면 시스템은 LSP 업데이트의 일부로 추가된 새 교체 규칙에서 규칙 재정의를 유지합니다. 알림은 톱니바퀴 (⚙) 옆에 있는 **Tasks(**작업**)** 탭의 알림 아이콘 아래에 표시됩니다.

언어

웹 인터페이스에 대해 다른 언어를 지정하려면 Language 페이지를 사용할 수 있습니다.

웹 인터페이스의 언어 설정

여기서 지정하는 언어는 모든 사용자에 대한 웹 인터페이스에 사용됩니다. 다음 항목을 선택할 수 있습니다.

- 영어
- 프랑스어
- 중국어(간체)
- 중국어(번체)
- 일본어
- 한국어

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Language**를 클릭합니다.

단계 **3** 사용하려는 언어를 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

로그인 배너

Login Banner(로그인 배너) 페이지를 사용하여 보안 어플라이언스 또는 공유 정책에 대한 세션, 로그인 또는 사용자 정의 메시지 배너를 지정할 수 있습니다.

ASCII 문자와 캐리지 리턴을 사용하여 사용자 정의 로그인 배너를 만들 수 있습니다. 시스템은 탭 간격을 유지하지 않습니다. 로그인 배너가 너무 크거나 오류가 발생하면 시스템에서 배너를 표시하려고 시도할 때 텔넷 또는 SSH 세션이 실패할 수 있습니다.

로그인 배너 사용자 지정

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Login Banner(**로그인 배너**)**를 선택합니다.

단계 **3** **Custom Login Banner(**사용자 정의 로그인 배너_ 필드에서 사용하려는 로그인 배너 텍스트를 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

관리 인터페이스

설정 후 management center에 관리 인터페이스, 호스트 이름, 검색 도메인, DNS 서버 및 HTTP 프록시를 추가하는 것을 포함하여 관리 네트워크 설정을 변경할 수 있습니다.

Management Center 관리 인터페이스 정보

기본적으로 management center는 모든 디바이스를 단일 관리 인터페이스에서 관리합니다. 또한 관리 인터페이스에 대한 초기 설정을 수행하고 이 인터페이스에서 관리자로 management center에 로그인

할 수도 있습니다. 관리 인터페이스는 Smart Licensing 서버와 통신하고, 업데이트를 다운로드하고, 기타 관리 기능을 수행하는 작업에도 사용됩니다.

디바이스 관리 인터페이스에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스 관리 인터페이스 정보를 참조하십시오.

디바이스 관리 관련 정보

management center는 디바이스를 관리할 때 자체와 디바이스 간에 양방향 SSL 암호화 통신 채널을 설정합니다. management center는 이 채널을 사용하여 네트워크 트래픽을 분석하고 관리하고자 하는 방법에 대한 정보를 디바이스로 전송합니다. 디바이스는 트래픽을 평가할 때 이벤트를 생성하고 동일한 채널을 사용하여 management center로 전송합니다.

management center를 사용하여 디바이스를 관리하면 다음을 수행할 수 있습니다.

- 단일 위치에서 모든 디바이스에 대한 정책을 구성하므로 설정을 좀 더 쉽게 변경할 수 있습니다.
- 디바이스에 각종 소프트웨어 업데이트를 설치할 수 있습니다.
- 관리되는 디바이스에 상태 정책을 푸시하고 management center에서 상태를 모니터링할 수 있습니다.

참고 CDO 매니지드 디바이스가 있고 분석용으로만 온프레미스 management center를 사용하는 경우 온프레미스 management center는 정책 구성 또는 업그레이드를 지원하지 않습니다. 장치 구성 및 기타 지원되지 않는 기능과 관련된 이 안내서의 장 및 절차는 기본 관리자가 CDO인 디바이스에는 적용되지 않습니다.

management center는 침입 이벤트, 네트워크 검색 정보 및 디바이스 성능 데이터를 집계하고 상호 연결하므로 사용자는 디바이스가 상호 관계에 대해 보고하는 정보를 모니터링하고 네트워크에서 발생하는 전반적인 활동을 평가할 수 있습니다.

management center를 사용하면 디바이스 동작의 거의 모든 부분을 관리할 수 있습니다.

참고 하지만 management center은 http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html에서 사용 가능한 호환성 매트릭스에서 지정된 일부 이전 릴리스가 실행되는 디바이스를 관리할 수 있으며 이런 이전 릴리스를 사용하는 threat defense 소프트웨어의 최신 버전이 필요한 디바이스에서는 새로운 기능을 사용할 수 없습니다. 일부 management center 기능은 이전 버전에서 사용할 수 있습니다.

관리 연결

management center 정보를 사용하여 디바이스를 구성하고 management center에 디바이스를 추가한 후에는 디바이스 또는 management center에서 관리 연결을 설정할 수 있습니다. 초기 설정에 따라:

- 디바이스 또는 management center를 시작할 수 있습니다.

- 디바이스만 시작할 수 있습니다.
- management center만 시작할 수 있습니다.

시작은 항상 management center의 eth0 또는 디바이스에서 번호가 가장 낮은 관리 인터페이스에서 시작됩니다. 연결이 설정되지 않은 경우 추가 관리 인터페이스가 시도됩니다. management center의 여러 관리 인터페이스를 사용하면 개별 네트워크에 연결하거나 관리 및 이벤트 트래픽을 분리할 수 있습니다. 그러나 이니시에이터는 라우팅 테이블을 기반으로 최상의 인터페이스를 선택하지 않습니다.

참고 관리 연결은 디바이스와 디바이스 사이의 보안 SSL 암호화 통신 채널입니다. 보안을 위해 사이트 간 VPN과 같은 추가 암호화 터널을 통해 이 트래픽을 실행할 필요가 없습니다. 예를 들어 VPN이 다운되면 관리 연결이 끊어지므로 간단한 관리 경로를 사용하는 것이 좋습니다.

관리 인터페이스: **Management Center**

management center는 초기 설정, 관리자를 위한 HTTP 액세스, 디바이스 관리, 라이선스 및 업데이트와 같은 기타 관리 기능을 위해 eth0 인터페이스를 사용합니다.

추가 관리 인터페이스를 구성할 수도 있습니다. management center에서 다른 네트워크에 있는 많은 수의 디바이스를 관리할 때 관리 인터페이스를 추가하면 처리량과 성능이 향상될 수 있습니다. 다른 모든 관리 기능에 대해 이 인터페이스를 사용할 수도 있습니다. 특정 기능을 위해 각 관리 인터페이스를 사용할 수도 있습니다. 예를 들어 HTTP 관리자 액세스용으로 하나의 인터페이스를 사용하고 디바이스 관리용으로 하나의 인터페이스를 사용할 수 있습니다.

디바이스 관리의 경우 관리 인터페이스에는 두 개의 별도 트래픽 채널이 있습니다. 즉, 관리 트래픽 채널은 모든 내부 트래픽(예: 디바이스 관리와 관련된 디바이스 간 트래픽)을 전달하고, 이벤트 트래픽 채널은 모든 이벤트 트래픽(예: 웹 이벤트)을 전달합니다. 선택적으로 이벤트 트래픽을 처리하기 위해 management center에 별도의 이벤트 전용 인터페이스를 구성할 수 있습니다. 하나의 이벤트 인터페이스만 구성할 수 있습니다. 또한 항상 관리 트래픽 채널에 대한 관리 인터페이스가 있어야 합니다. 이벤트 트래픽은 많은 양의 대역폭을 사용할 수 있으므로 관리 트래픽에서 이벤트 트래픽을 분리하면 management center의 성능이 향상될 수 있습니다. 예를 들어 관리를 위해 1GigabitEthernet 인터페이스를 사용하는 경우 10GigabitEthernet 인터페이스를 이벤트 인터페이스로 할당할 수 있습니다. 예를 들어 인터넷 액세스가 포함된 네트워크의 일반 관리 인터페이스를 사용하는 동안 완전히 안전한 프라이빗 네트워크에 이벤트 전용 인터페이스를 구성할 수 있습니다. 또한 증가된 처리량만 활용하는 것이 목표인 경우 동일한 네트워크에서 관리 및 이벤트 인터페이스를 모두 사용할 수 있습니다. 매니지드 디바이스는 관리 트래픽을 management center 관리 인터페이스로 보내고 이벤트 트래픽을 management center 이벤트 전용 인터페이스로 보냅니다. 매니지드 디바이스가 이벤트 전용 인터페이스에 연결할 수 없는 경우 관리 인터페이스로 이벤트를 전송합니다.

management center에서 관리 연결 시작은 항상 eth0에서 먼저 시도된 다음 다른 인터페이스가 순서대로 시도됩니다. 라우팅 테이블은 최적의 인터페이스를 결정 하는 데 사용 되지 않습니다.

참고 모든 관리 인터페이스는 액세스 목록 구성 (액세스 목록 구성, 45 페이지)에 의해 제어되는 HTTP 관리자 액세스를 지원합니다. 반대로 인터페이스를 HTTP 액세스 전용으로 제한할 수는 없습니다. 관리 인터페이스는 항상 디바이스 관리(관리 트래픽, 이벤트 트래픽 또는 둘 다)를 지원합니다.

참고 eth0 인터페이스만 DHCP IP 주소를 지원합니다. 다른 관리 인터페이스는 고정 IP 주소만 지원합니다.

FMC 모델별 관리 인터페이스 지원

관리 인터페이스 위치에 대한 모델의 하드웨어 설치 가이드를 참조하십시오.

각 FMC 모델에서 지원되는 관리 인터페이스는 다음 표를 참조하십시오.

표 *2: FMC*의 관리 인터페이스 지원

모델	관리 인터페이스
MC1000	eth0(기본값) eth1
MC2500, MC4500	eth0(기본값) eth1 eth2 eth3
MC1600, MC2600, MC4600	eth0(기본값) eth1 eth2 eth3 CIMC(Lights-Out 관리에만 지원됨)
Firepower Management Center Virtual	eth0(기본값)

Management Center 관리 인터페이스의 네트워크 라우트

관리 인터페이스(이벤트 전용 인터페이스 포함)는 정적 경로만 지원하여 원격 네트워크에 연결할 수 있습니다. management center를 설정하면 설정 과정에서 지정한 게이트웨이 IP 주소에 대한 기본 경로가 생성됩니다. 이 경로는 삭제할 수 없으며 게이트웨이 주소만 수정할 수 있습니다.

일부 플랫폼에서는 여러 관리 인터페이스를 구성할 수 있습니다. 기본 경로는 인그레스 인터페이스를 포함하지 않으므로 선택한 인터페이스는 지정한 게이트웨이 주소와 게이트웨이가 속한 인터페이

스의 네트워크에 따라 다릅니다. 기본 네트워크의 여러 인터페이스의 경우 디바이스는 더 낮은 번호의 인터페이스를 인그레스 인터페이스로 사용합니다.

원격 네트워크에 액세스하기 위해서는 관리 인터페이스당 최소 1개의 정적 경로가 권장됩니다. 다른 디바이스에서 management center로의 라우팅 문제를 비롯하여 잠재적인 라우팅 문제를 방지하려면 각 인터페이스를 별도의 네트워크에 배치하는 것이 좋습니다.

참고 관리 연결에 사용되는 인터페이스는 라우팅 테이블에 의해 결정되지 않습니다. 연결은 항상 먼저 eth0을 사용하여 시도된 다음, 매니지드 디바이스에 도달할 때까지 후속 인터페이스가 순서대로 시도됩니다.

NAT 환경

NAT(Network Address Translation)는 소스 또는 대상 IP 주소를 재할당하는 작업에 관여하는 라우터를 통해 네트워크 트래픽을 보내고 받는 방법입니다. NAT는 일반적으로 프라이빗 네트워크와 인터넷이 통신하는 데 사용됩니다. 정적 NAT는 1:1 변환을 수행하여 디바이스와 management center의 통신에 문제를 일으키지 않지만 포트 주소 변환(PAT)이 더욱 일반적입니다. PAT를 사용하면 단일 공용 IP 주소에 고유한 포트를 사용해 공용 네트워크에 접속할 수 있습니다. 이러한 포트는 필요에 따라 동적으로 할당되므로 PAT 라우터 뒤에 있는 디바이스에 연결을 시작할 수 없습니다.

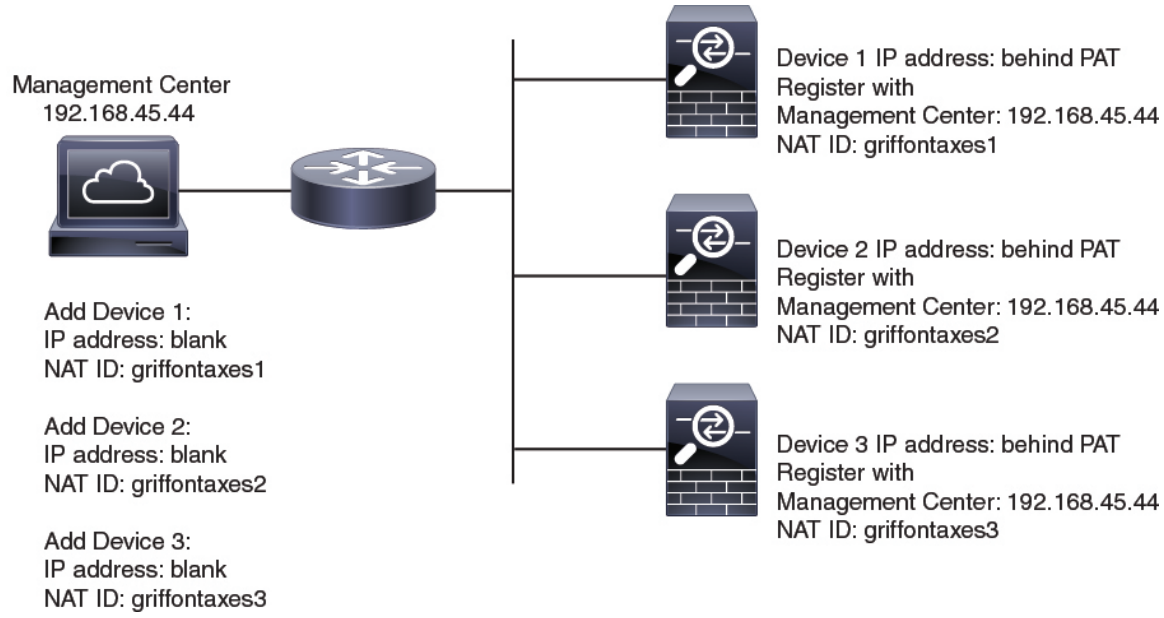
일반적으로 라우팅 목적과 인증 두 가지 목적에 IP 주소(등록 키와 함께)가 모두 필요합니다. management center는 디바이스 IP 주소를 지정하고 디바이스는 management center IP 주소를 지정합니다. 그러나 라우팅을 위한 최소 요구 사항인 IP 주소 중 하나만 알고 있는 경우, 초기 통신에 대한 신뢰를 설정하고 올바른 등록 키를 조회하려면 연결의 양쪽에서 고유 NAT ID도 지정해야 합니다. management center 및 디바이스는 등록 키 및 NAT ID(IP 주소 대신)를 사용하여 초기 등록을 인증하고 권한을 부여합니다.

예를 들어 management center에 디바이스를 추가하지만 디바이스 IP 주소를 모르는 경우(디바이스가 PAT 라우터 뒤에 있는 경우) management center에 NAT ID와 등록 키만 지정하고 IP 주소는 공백으로 둡니다. 디바이스에 management center IP 주소, 동일한 NAT ID와 동일한 등록 키를 지정합니다. management center의 IP 주소에 디바이스를 등록합니다. 이때 management center은 IP 주소 대신 NAT ID를 사용해 디바이스를 인증합니다.

NAT 환경에서 NAT ID 사용은 일반적이지만 management center에 많은 디바이스를 추가하려고 할 때에도 NAT ID를 선택할 수 있습니다. management center에는 추가하려는 각 디바이스에 고유한 NAT ID를 지정하고 IP 주소를 공백으로 두고, 각 디바이스에서 management center IP 주소 및 NAT ID를 지정하십시오. 주의: NAT ID는 디바이스별로 고유해야 합니다.

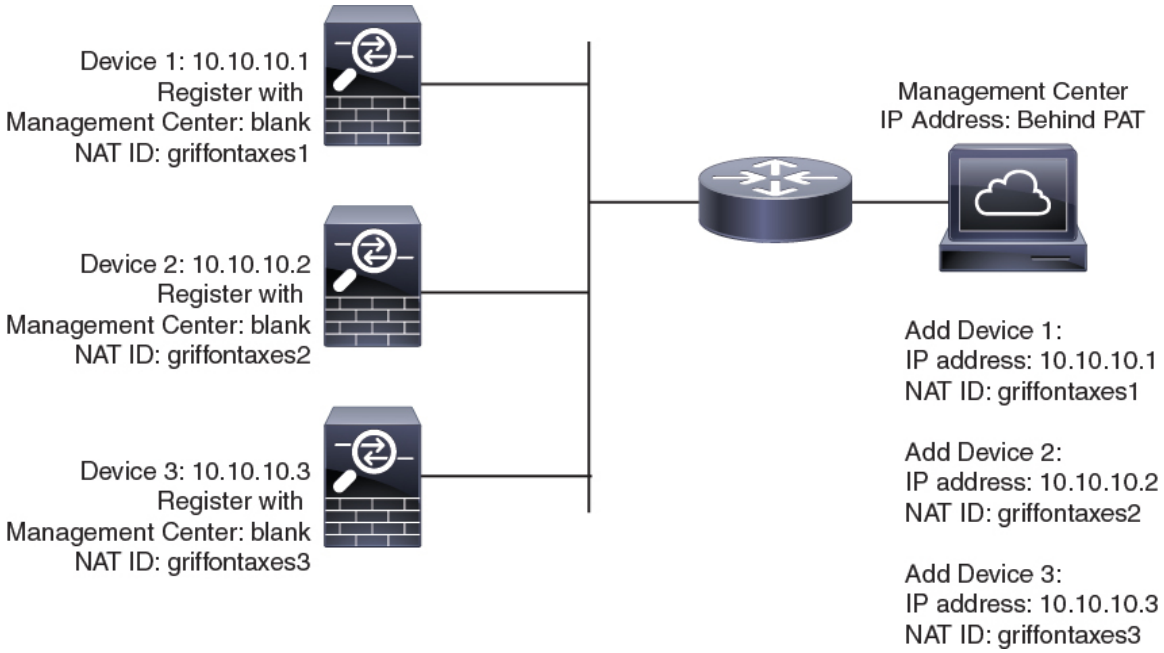
다음 예에서는 PAT IP 주소 뒤에 3개의 장치가 있음을 보여줍니다. 이 경우 management center 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 디바이스에 management center IP 주소를 지정하십시오.

그림 *2: PAT* 뒤의 관리되는 디바이스의 *NAT ID*



다음 예는 PAT ID 주소 뒤의 management center을 보여줍니다. 이 경우 management center 및 디바이스에 디바이스별로 고유 NAT ID를 지정하고 management center에 디바이스 IP 주소를 지정하십시오.

그림 *3: PAT* 뒤의 *FMC*에 대한 *NAT ID*

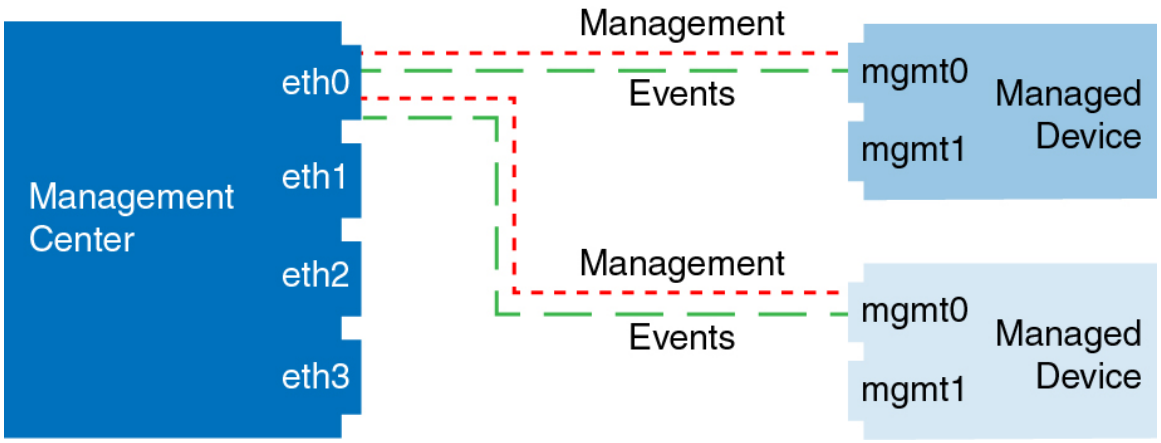


관리 및 이벤트 트래픽 채널 예시

참고 threat defense에서 관리를 위해 데이터 인터페이스를 사용하는 경우 해당 디바이스에 대해 별도의 관리 및 이벤트 인터페이스를 사용할 수 없습니다.

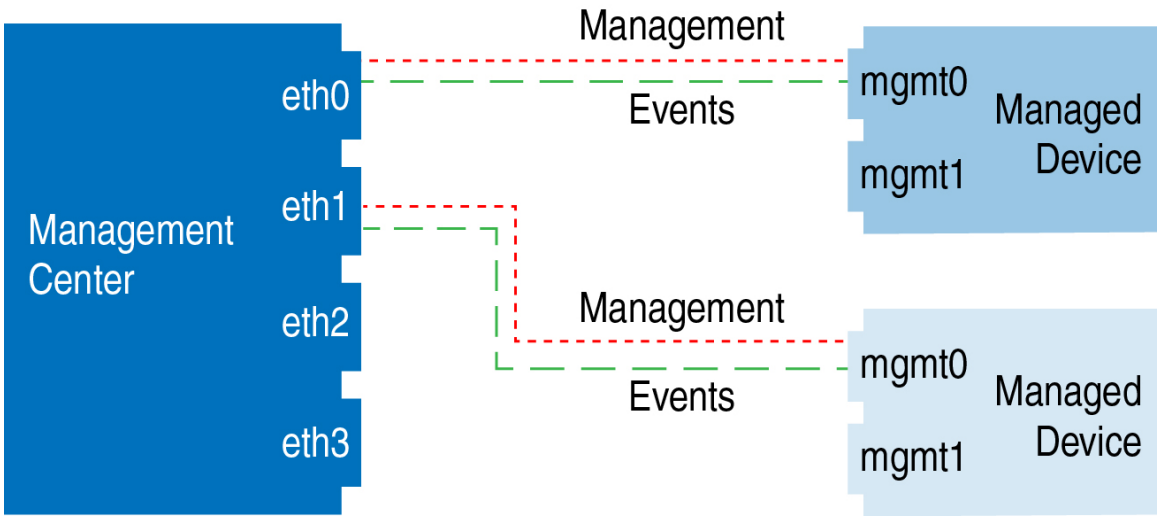
다음 예에서는 기본 관리 인터페이스만 사용하는 management center 및 매니지드 디바이스를 보여 줍니다.

그림 ***4:*** 단일 관리 인터페이스***: Secure Firewall Management Center***



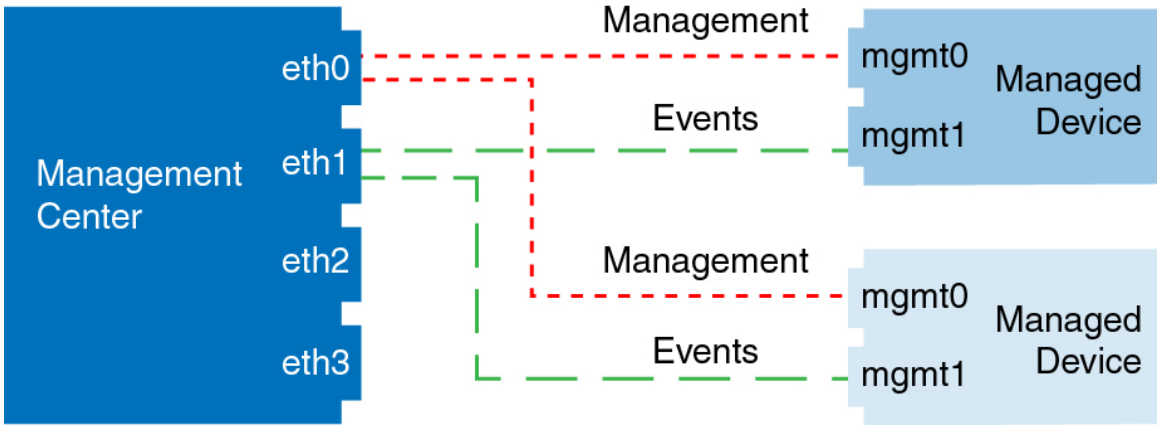
다음 예는 디바이스에 별도의 관리 인터페이스를 사용하는 management center를 보여 줍니다. 관리되는 각 디바이스는 1개의 관리 인터페이스를 사용합니다.

그림 ***5:*** 다중 관리 인터페이스***: Secure Firewall Management Center***



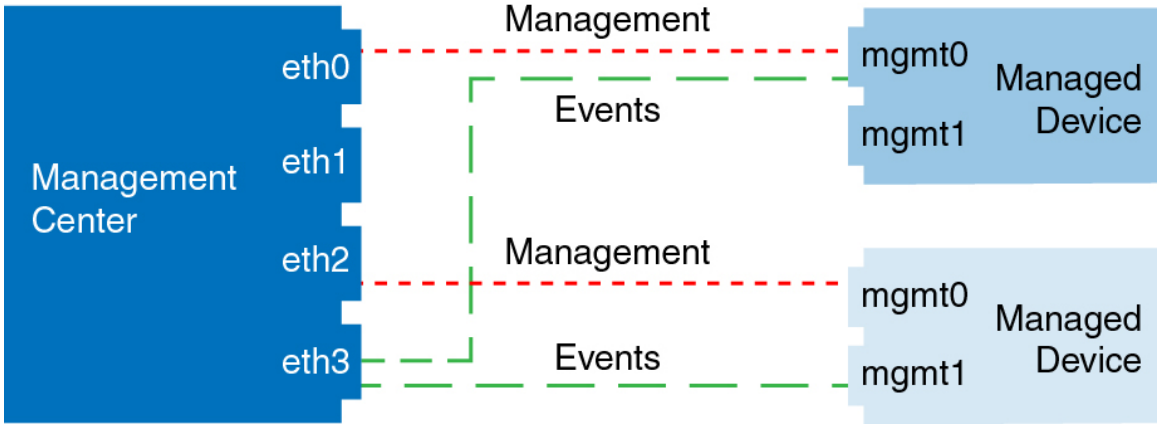
다음 예에서는 별도의 이벤트 인터페이스를 사용하는 management center 및 매니지드 디바이스를 보여 줍니다.

그림 *6: Secure Firewall Management Center* 및 매니지드 디바이스에 대한 별도의 이벤트 인터페이스



다음 예는 별도의 이벤트 인터페이스를 사용하거나 단일 관리 인터페이스를 사용하는 management center 및 여러 매니지드 디바이스에 대한 다중 관리 인터페이스 및 별도의 이벤트 인터페이스를 보여 줍니다.

그림 *7:* 혼합 관리 및 이벤트 인터페이스 사용



Management Center 관리 인터페이스 수정

management center에서 관리 인터페이스 설정을 수정합니다. 필요에 따라 추가 관리 인터페이스를 활성화하거나 이벤트 전용 인터페이스를 구성할 수 있습니다.

⚠

주의 연결된 관리 인터페이스를 변경할 때 주의하십시오. 구성 오류로 인해 다시 연결할 수 없는 경우 management center 콘솔 포트에 액세스하여 Linux 셸의 네트워크 설정을 다시 구성해야 합니다. 이 작업에 대한 안내를 받으려면 Cisco TAC에 문의해야 합니다.

management center IP 주소를 변경하는 경우 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스의 *management center IP* 주소 또는 호스트 이름을 참조하십시오. management center IP 주소 또는 호스트네임을 변경하는 경우, 설정이 일치하도록 디바이스 CLI의 값도 변경해야 합니

다. 대부분 디바이스에서 management center IP 주소 또는 호스트네임을 변경하지 않고 관리 연결이 다시 설정되지만, 적어도 management center에 디바이스를 추가하고 NAT ID만 지정한 경우 연결을 다시 설정하려면 이 작업을 수행해야 합니다. 다른 경우에도 네트워크의 복원력을 높이려면 management center IP 주소 또는 호스트네임을 최신 상태로 유지하는 것이 좋습니다

고가용성 구성에서 등록된 디바이스의 관리 IP 주소를 디바이스 CLI 또는 management center에서 수정하면 보조 management center는 HA 동기화가 끝나도 변경 사항을 반영하지 않습니다. 보조 management center도 업데이트되게 하려면 두 management center의 역할을 바꿔 보조 management center를 액티브 유닛으로 설정해야 합니다. 현재 액티브 management center의 Device Management(디바이스 관리) 페이지에 등록된 디바이스의 관리 IP 주소를 수정합니다.

시작하기 전에

- 디바이스 관리 작동 방식에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스 관리 인터페이스 정보를 참조하십시오.
- 프록시를 사용하는 경우:
  - NTLM(NT LAN Manager) 인증을 사용하는 프록시는 지원되지 않습니다.
  - 스마트 라이선스를 사용하거나 사용할 예정인 경우 프록시 FQDN은 64자를 초과할 수 없습니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을 선택한 다음 **Management Interface(**관리 인터페이스**)**를 선택합니다.

단계 **2** **Interfaces(**인터페이스**)** 영역에서 구성하려는 인터페이스 옆에 있는 **Edit(**편집**)**를 클릭합니다.

이 섹션에는 사용 가능한 모든 인터페이스가 나열되어 있습니다. 다른 인터페이스를 추가할 수 없습니다.

각 관리 인터페이스에서 다음 옵션을 구성할 수 있습니다.

- **Enabled(**활성화됨**)** - 관리 인터페이스를 활성화합니다. 기본 eth0 관리 인터페이스를 비활성화하지 마십시오. 일부 프로세스에는 eth0 인터페이스가 필요합니다.
- **Channels(**채널**)** — 관리 트래픽이 활성화된 인터페이스가 하나 이상 있어야 합니다. 선택적으로 이벤트 전용 인터페이스를 구성할 수 있습니다. management center에서는 하나의 이벤트 인터페이스만 구성할 수 있습니다. 이렇게 하려면 **Management Traffic(**관리 트래픽**)** 확인란을 선택 취소하고 **Event Traffic(**이벤트 트래픽**)** 확인란을 선택한 상태로 유지합니다. 나머지 관리 인터페이스에 대한 **Event Traffic(**이벤트 트래픽**)**을 비활성화할 수 있습니다. 두 경우 모두에서 디바이스는 이벤트 전용 인터페이스로 이벤트를 전송하려고 시도하며 해당 인터페이스가 다운되면 이벤트 채널을 비활성화하는 경우에도 관리 인터페이스에서 이벤트를 전송합니다. 인터페이스에서 이벤트 및 관리 채널을 비활성화할 수 없습니다.
- **Mode(**모드**)** - 연결 모드를 지정합니다. GigabitEthernet 인터페이스의 경우 자동 협상에 대한 변경 사항은 무시됩니다.

- **MDI/MDIX** - **Auto-MDIX**를 설정합니다.
- **MTU** - 1280 및 1500 간에 최대 전송 단위(MTU)를 설정합니다. 기본값은 1500입니다.
- **IPv4 Configuration(IPv4** 구성**)** - IPv4 IP 주소를 설정합니다. 선택:
  - **Static(**정적**)** - 수동으로 **IPv4 Management IP(IPv4** 관리 **IP)** 주소 및 **IPv4 Netmask(IPv4** 넷마스크**)**를 입력합니다.
  - **DHCP** - DHCP를 사용하도록 인터페이스를 설정합니다(eth0 전용).

    DHCP를 사용하는 경우 DHCP 예약을 사용해야 할당된 주소가 변경되지 않습니다. DHCP 주소가 변경되면 management center 네트워크 구성이 동기화되지 않아 디바이스 등록에 실패합니다. DHCP 주소 변경에서 복구하려면 management center에 연결하고(호스트 이름 또는 새 IP 주소 사용) 시스템 (⚙) > **Configuration(**구성**)** > **Management Interfaces(**관리 인터페이스**)**로 이동하여 네트워크를 재시작합니다.
  - **Disabled(**비활성화됨**)** - IPv4를 비활성화합니다. IPv4와 IPv6을 모두 비활성화해서는 안 됩니다.
- **IPv6 Configuration(IPv6** 구성**)** - IPv6 IP 주소를 설정합니다. 선택:
  - **Static(**정적**)** - 수동으로 **IPv6 Management IP(IPv6** 관리 **IP)** 주소 및 **IPv6 Prefix Length(IPv6** 프리픽스 길이**)**를 입력합니다.
  - **DHCP** - DHCPv6를 사용하도록 인터페이스를 설정합니다(eth0 전용).
  - **Router Assigned(**라우터 할당**)** - 상태 비저장 자동 구성을 활성화합니다.
  - **Disabled(**비활성화됨**)** - IPv6를 비활성화합니다. IPv4와 IPv6을 모두 비활성화해서는 안 됩니다.
  - **IPv6 DAD** - IPv6을 활성화할 때 DAD(Duplicate Address Detection)를 활성화 또는 비활성화합니다. DAD를 사용하면 서비스 거부(DoS) 공격 가능성이 발생하기 때문에 DAD를 비활성화하려고 할 수 있습니다. 이 설정을 비활성화하면 이 인터페이스가 이미 할당된 주소를 사용하고 있지 않은지 수동으로 확인해야 합니다.

단계 **3** **Routes(**경로**)** 영역에서 **Edit(**수정**)** ( )을 클릭하여 정적 경로를 편집하거나 **Add(**추가**)** ( )를 클릭하여 경로를 추가합니다.

을 클릭하여 경로 테이블을 확인합니다.

각 추가 인터페이스가 원격 네트워크에 도달할 수 있는 정적 경로가 필요합니다. 새 경로가 필요한 시점에 대한 자세한 내용은 Management Center 관리 인터페이스의 네트워크 라우트, 78 페이지 섹션을 참조하십시오.

참고 기본 경로의 경우 게이트웨이 IP 주소만 변경할 수 있습니다. 이그레스 인터페이스는 지정된 게이트웨이를 인터페이스의 네트워크와 연결하여 자동으로 선택됩니다.

정적 경로에 대해 다음 설정을 구성할 수 있습니다.

- **Destination(**대상**)** - 경로를 생성할 네트워크의 대상 주소를 설정합니다.

- **Netmask(**넷마스크**)** 또는 **Prefix Length(**프리픽스 길이**)** - 네트워크의 넷마스크(IPv4) 또는 프리픽스 길이(IPv6)를 설정합니다.
- **Interface(**인터페이스**)** - 이그레스 관리 인터페이스를 설정합니다.
- **Gateway(**게이트웨이**)** - 게이트웨이 IP 주소를 설정합니다.

단계 **4** **Shared Settings(**공유 설정**)** 영역의 모든 인터페이스에서 공유하는 네트워크 파라미터를 설정합니다.

참고 eth0 인터페이스에 **DHCP**를 선택한 경우 DHCP 서버에서 파생된 일부 공유 설정을 수동으로 지정할 수 없습니다.

다음 공유 설정을 구성할 수 있습니다.

- **Hostname(**호스트네임**)** - management center 호스트네임을 설정합니다. 호스트 이름은 최대 64자여야 하고, 문자 또는 숫자로 시작하고 끝나야 하며 문자, 숫자 또는 하이픈만 사용할 수 있습니다. 호스트네임을 변경하는 경우 새 호스트네임을 시스템 로그 메시지에 반영하려면 management center를 리부팅합니다. 시스템 로그 메시지는 리부팅될 때까지 새 호스트네임을 반영하지 않습니다.
- **Domains(**도메인**)** - management center에 대한 검색 도메인을 쉼표로 구분하여 설정합니다. 이 도메인은 명령(예: **ping system**)에서 FQDN(Fully Qualified Domain Name)을 지정하지 않은 경우 호스트 이름에 추가됩니다. 도메인은 관리 인터페이스에서 사용되거나 관리 인터페이스를 통과하는 명령에 대해서만 사용됩니다.
- **Primary DNS Server(**기본 **DNS** 서버**)**, **Secondary DNS Server(**보조 **DNS** 서버**)Tertiary DNS Server(3**차 **DNS** 서버**)** - 환경설정 순서대로 사용할 DNS 서버를 설정합니다.
- **Remote Management Port(**원격 관리 포트**)** - 매니지드 디바이스와의 통신을 위한 원격 관리 포트를 설정합니다. management center 및 매니지드 디바이스는 기본적으로 포트 8305에 있는 양방향 SSL-암호화 통신을 사용하여 통신합니다.

  참고 Cisco에서는 원격 관리 포트에 대해 기본 설정을 유지할 것을 적극 권장하지만, 관리 포트가 네트워크의 다른 통신과 충돌하면 다른 포트를 선택할 수 있습니다. 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 디바이스의 설정을 변경해야 합니다.

단계 **5** **ICMPv6** 영역에서 ICMPv6 설정을 구성합니다.

- **Allow Sending Echo Reply Packets(**에코 응답 패킷 전송 허용**)** - 에코 응답 패킷을 활성화 또는 비활성화합니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다. 에코 응답 패킷을 비활성화하면 테스트 목적으로 management center 관리 인터페이스에 IPv6 ping을 사용할 수 없습니다.
- **Allow Sending Destination Unreachable Packets(**대상에 연결할 수 없는 패킷 전송 허용**)** - 대상에 연결할 수 없는 패킷을 활성화 또는 비활성화합니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다.

단계 **6** **Proxy(**프록시**)** 영역에서 HTTP 프록시 설정을 구성합니다.

management center는 TCP/443(HTTPS) 및 TCP/80(HTTP) 포트에서 직접 인터넷에 연결되도록 구성됩니다. HTTP 다이제스트를 통해 인증할 수 있는 프록시 서버를 사용할 수 있습니다.

이 주제의 사전 요구 사항에서 프록시 요구 사항을 참조하십시오.

a) **Enable(**활성화**)** 확인란을 선택합니다.
b) 프록시 서버의 IP 주소 또는 정규화된 도메인 이름을 **HTTP Proxy(HTTP** 프록시**)** 필드에 입력합니다.

   이 주제의 사전 요구 사항에서 해당 요구 사항을 참조하십시오.

c) **Port(**포트**)** 필드에서 포트 번호를 입력합니다.
d) **Use Proxy Authentication(**프록시 인증 사용**)**을 선택하여 인증 자격 증명을 제공하고 **User Name(**사용자 이름**)** 및 **Password(**비밀번호**)**를 제공합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** management center IP 주소를 변경하는 경우 management center IP 주소를 변경하는 경우를 참조하고 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스의 *management center IP* 주소 또는 호스트 이름 편집을 참조하십시오.

management center IP 주소 또는 호스트네임을 변경하는 경우, 설정이 일치하도록 디바이스 CLI의 값도 변경해야 합니다. 대부분 디바이스에서 management center IP 주소 또는 호스트네임을 변경하지 않고 관리 연결이 다시 설정되지만, 적어도 management center에 디바이스를 추가하고 NAT ID만 지정한 경우 연결을 다시 설정하려면 이 작업을 수행해야 합니다. 다른 경우에도 네트워크의 복원력을 높이려면 management center IP 주소 또는 호스트네임을 최신 상태로 유지하는 것이 좋습니다

네트워크 분석 정책 환경 설정

사용자가 네트워크 분석 정책을 수정할 때 코멘트 기능을 사용하여 정책 관련 변경 사항을 추적하도록 시스템을 구성할 수 있습니다. 정책 변경 코멘트를 활성화하면 관리자는 배포의 중요한 정책이 수정된 이유를 신속하게 평가할 수 있습니다.

정책 변경에 대한 코멘트를 활성화하는 경우, 코멘트를 선택 사항 또는 의무 사항으로 설정할 수 있습니다. 정책에 대한 새로운 변경 사항이 저장될 때마다 시스템은 사용자에게 코멘트를 입력하라는 메시지를 표시합니다.

필요에 따라 감사 로그에 작성된 네트워크 분석 정책을 변경할 수 있습니다.

프로세스

웹 인터페이스를 사용하여 management center의 프로세스 종료 및 재시작을 제어합니다. 다음 작업을 수행할 수 있습니다.

- 종료: 어플라이언스의 정상 종료를 시작합니다.

주의 전원 버튼을 사용하여 Firepower 어플라이언스를 종료하지 마십시오. 데이터가 손실될 수 있습니다. 웹 인터페이스(또는 CLI)를 사용하여 구성 데이터 손실 없이 시스템의 전원을 안전하게 끄고 재시작할 수 있도록 준비합니다.

- 재부팅: 종료한 다음 정상적으로 재시작합니다.
- 콘솔 재시작: 통신, 데이터베이스 및 HTTP 서버 프로세스를 다시 시작합니다. 이는 일반적으로 문제 해결 중에 사용됩니다.

팁 가상 디바이스의 경우에는 가상 플랫폼 설명서를 참조하십시오. 특히 VMware의 경우 사용자 지정 전원 옵션을 VMware 도구로 제공합니다.

FMC를 종료하거나 재시작합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Process(**프로세스**)**를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

종료	**Shutdown Management Center(Management Center** 종료**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다.
재부팅	**Reboot Management Center(Management Center** 재부팅**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다. 참고 리부팅하면 로그아웃되며, 완료하는 데 최대 1시간이 소요될 수 있는 데이터베이스 검사가 실행됩니다.
콘솔 재시작	**Restart Management Center Console(Management Center** 콘솔 재시작**)** 옆에 있는 **Run Command(**명령 실행**)**를 클릭합니다. 참고 재시작하면 삭제된 호스트가 네트워크 맵에 다시 나타날 수 있습니다.

REST API 환경 설정

Management Center REST API는 타사 애플리케이션이 REST 클라이언트 및 표준 HTTP 메서드를 사용하여 디바이스 구성을 보고 관리할 수 있는 간단한 인터페이스를 제공합니다. Management Center REST API에 대한 자세한 내용은 Secure Firewall Management Center REST API 빠른 시작 가이드의 내용을 참고하십시오.

참고 HTTPS 인증서는 Management Center REST API에서 지원되지 않습니다.

기본적으로 management center는 REST API를 사용하는 애플리케이션의 요청을 허용합니다. 이 액세스를 차단하도록 management center를 구성할 수 있습니다.

REST API 액세스 활성화

참고 management center의 고가용성을 활용한 배포의 경우 이 기능은 활성화된 management center에서만 사용할 수 있습니다.

프로시저

단계 **1** 우측 상단의 톱니 바퀴( )를 선택하여 시스템 메뉴를 엽니다.

단계 **2** **REST API Preferences(REST API 환경설정)**를 클릭합니다.

단계 **3** management center에 대한 REST API 액세스를 활성화 또는 비활성화하려면 **Enable REST API(REST API 활성화)** 확인란을 선택하거나 선택 취소합니다.

단계 **4** **Save(저장)**를 클릭합니다.

단계 **5** 다음 주소에서 REST API Explorer에 액세스:

```
https://<management_center_IP_or_name>:<https_port>/api/api-explorer
```

원격 콘솔 액세스 관리

VGA 포트(기본값) 또는 물리적 어플라이언스의 시리얼 포트를 통해 지원되는 시스템에 원격으로 액세스하도록 하려면 Linux 시스템 콘솔을 사용할 수 있습니다. Console Configuration(콘솔 구성) 페이지를 사용하여 조직 내 Firepower 구축의 실제 레이아웃에 가장 적합한 옵션을 선택합니다.

지원되는 물리적 하드웨어 기반 시스템에서는 SOL(Serial Over LAN) 연결에서 LOM(Lights-Out Management)을 사용하여 시스템의 관리 인터페이스에 로그인하지 않고 시스템을 원격으로 모니터링하거나 관리할 수 있습니다. OOB(Out of Band) 관리 연결에서 명령줄 인터페이스를 사용하여 새시

일련 번호 보기, 팬 속도와 온도 등의 조건 모니터링 등 제한적인 작업을 수행할 수 있습니다. LOM을 지원하기 위한 케이블 연결은 management center 모델에 따라 다릅니다.

- management center 모델 MC1600, MC2600 및 MC4600의 경우, CIMC 포트와의 연결을 사용하여 LOM을 지원합니다. 자세한 내용은 *Cisco Firepower Managemenet Center 1600, 2600 및 4600 시작 가이드*를 참조하십시오.
- 다른 모든 management center 하드웨어 모델의 경우, 기본(eth0) 관리 포트가 있는 연결을 사용하여 LOM을 지원합니다. 해당 하드웨어 모델의 *Cisco Firepower Management Center 시작 가이드*를 참조하십시오.

시스템을 관리하려는 사용자와 시스템 모두에 대해 LOM을 활성화해야 합니다. 시스템 및 사용자를 활성화한 후 시스템에 대한 액세스 및 관리를 위해 서드파티 IPMI(Intelligent Platform Management Interface) 유틸리티를 사용합니다.

시스템에서 원격 콘솔 설정

이 절차를 수행하려면 관리자 사용자여야 합니다.

시작하기 전에

- 디바이스의 관리 인터페이스에 연결된 모든 서드파티 스위칭 장비에서 STP(Spanning Tree Protocol)를 비활성화해야 합니다.
- Lights-Out 관리를 활성화하려는 경우 IPMI(Intelligent Platform Management Interface) 유틸리티 설치 및 사용에 대한 정보는 어플라이언스의 시작하기 가이드를 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Console Configuration(**콘솔 구성**)**을 클릭합니다.

단계 **3** 원격 콘솔 액세스 옵션을 선택합니다.

- 어플라이언스의 VAG 포트를 사용하려면 **VGA**를 선택합니다.
- **Physical Serial Port(**물리적 시리얼 포트**)**를 선택해 어플라이언스의 시리얼 포트를 사용합니다.
- management center에서 SOL 연결을 사용하려면 **Lights-Out** 관리를 선택합니다. (management center 모델에 따라 기본 관리 포트 또는 CIMC 포트를 사용할 수 있습니다. 자세한 내용은 모델에 맞는 시작 가이드를 참조하십시오.

단계 **4** SOL을 통해 LOM을 구성하려면:

- 시스템(**DHCP** 또는 **Manual(**수동**)**)에 대한 주소 **Configuration(**구성**)**을 선택합니다.
- 수동 구성을 선택한 경우 필요한 IPv4 설정을 입력합니다.
  - LOM에 사용될 **IP Address(IP** 주소**)**를 입력합니다.

참고 LOM IP 주소는 management center 관리 인터페이스 IP 주소와 달라야 합니다.

- 시스템에 대한 **Netmask(**넷마스크**)**를 입력합니다.
- 시스템에 대한 **Default Gateway(**기본 게이트웨이**)**를 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** "다음 변경 사항을 적용하려면 시스템을 재부팅해야합니다."라는 경고가 표시됩니다. 지금 재부팅하려면 **OK(**확인**)**를 클릭하고 나중에 재부팅하려면 **Cancel(**취소**)**을 클릭합니다.

다음에 수행할 작업

- 직렬 액세스를 구성한 경우, management center 모델용 시작 가이드에 설명된 대로 이더넷을 통한 원격 직렬 액세스를 지원할 수있는 로컬 컴퓨터, 터미널 서버 또는 기타 디바이스에 후면 패널 직렬 포트가 연결되어 있는지 확인합니다.
- Lights-Out Management를 구성한 경우 Lights-Out Management 사용자를 활성화합니다. LOM(Lights-Out Management) 사용자 액세스 구성, 90 페이지 섹션을 참조하십시오.

LOM(Lights-Out Management) 사용자 액세스 구성

또한 기능을 사용할 사용자에게 Lights-Out Management 권한을 명시적으로 부여해야 합니다. 또한 LOM 사용자에는 다음과 같은 제한이 있습니다.

- 사용자에게 관리자 역할을 할당해야 합니다.
- 사용자 이름은 최대 16자의 영숫자로 지정할 수 있습니다. LOM 사용자는 16자보다 긴 사용자 이름과 하이픈을 사용할 수 없습니다.
- 사용자의 LOM 비밀번호는 해당 사용자의 시스템 비밀번호와 동일합니다. 비밀번호는 사용자 암호, 120 페이지에 설명된 요구 사항을 준수해야 합니다. 어플라이언스에서 지원되는 최대 길이로 사전에 없는 복잡한 암호를 사용하고 3개월마다 변경하는 것이 좋습니다.
- 물리적 management center 에는 최대 13명의 LOM 사용자가 있을 수 있습니다.

그러한 사용자가 로그인한 상태에서 LOM으로 해당 사용자를 비활성화했다가 다시 활성화할 경우 또는 사용자의 로그인 세션 중에 백업에서 사용자를 복원할 경우, 해당 사용자가 다시 웹 인터페이스에 로그인해야 `impitool` 명령에 다시 액세스할 수 있습니다.

LOM(Lights-Out Management) 사용자 액세스 활성화

이 절차를 수행하려면 관리자 사용자여야 합니다.

이 작업을 통해 기존 사용자에게 LOM 액세스 권한을 부여할 수 있습니다. 새 사용자에게 LOM 액세스 권한을 부여하려면 내부 사용자 추가, 123 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 시스템 ( ) > **Users(**사용자**)** > **Users(**사용자**)**을(를) 선택합니다.

단계 **2** 기존 사용자에 대해 LOM 사용자 액세스 권한을 부여하려면 목록의 사용자 이름 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **User Configuration(**사용자 구성**)** 아래에서 Administrator 역할을 활성화합니다.

단계 **4** **Allow Lights-Out Management Access(Lights-Out Management** 액세스 허용**)** 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

SoL(Serial over LAN) 연결 구성

컴퓨터에서 타사 IPMI 유틸리티를 사용하여 어플라이언스에 대한 Serial Over LAN 연결을 만듭니다. Linux와 유사한 컴퓨터 환경 또는 Mac 환경에서는 IPMItool을 사용하고, Windows 환경에서는 Windows 버전에 따라 IPMIutil 또는 IPMItool을 사용할 수 있습니다.

참고 IPMItool 버전 1.8.12 이상을 사용하는 것이 좋습니다.

Linux

IPMItool은 많은 배포의 표준이며 곧바로 사용 가능합니다.

Mac

Mac에는 IPMItool을 설치해야 합니다. 먼저 Mac에 Apple의 XCode Developer 툴이 설치되었는지 확인하고, 명령줄 개발을 위한 선택적인 구성 요소가 설치되었는지 확인합니다(새 버전에서는 UNIX Development 및 System Tools, 이전 버전에서는 Command Line Support). 그런 다음 macports 및 IPMItool을 설치할 수 있습니다. 자세히 알아보려면 자주 사용하는 검색 엔진을 사용하거나 다음 사이트를 이용하십시오.

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
http://github.com/ipmitool/ipmitool/
```

Windows

Linux용 Windows 하위 시스템(WSL)이 활성화된 Windows 버전 10 이상 및 일부 이전 버전의 Windows Server의 경우 IPMItool을 사용할 수 있습니다. 그렇지 않으면 Windows 시스템에서 IPMIutil을 컴파일해야 합니다. IPMIutil 자체를 사용하여 컴파일 할 수 있습니다. 자세히 알아보려면 자주 사용하는 검색 엔진을 사용하거나 다음 사이트를 이용하십시오.

```
http://ipmiutil.sourceforge.net/man.html#ipmiutil
```

IPMI 유틸리티 명령 이해

IPMI 유틸리티에 사용되는 명령은 Mac에서 다음 IPMItool 예와 같은 세그먼트로 구성됩니다.

```
ipmitool -I lanplus -H IP_address -U user_name command
```

여기서 각 항목은 다음을 나타냅니다.

- `ipmitool`은 유틸리티를 호출합니다.
- `-I lanplus`는 세션에 대해 암호화된 IPMI v2.0 RMCP + LAN 인터페이스를 사용하도록 지정합니다.
- `-H IP_address`는 액세스하려는 어플라이언스의 LOM(Lights-Out Management)을 위해 구성한 IP 주소를 나타냅니다.
- `-U user_name`는 권한 있는 원격 세션 사용자의 이름입니다.
- *command*는 사용할 명령의 이름입니다.

참고 IPMItool 버전 1.8.12 이상을 사용하는 것이 좋습니다.

Windows의 IMPIutil에서는 동일한 명령이 다음과 같이 표시됩니다.

```
ipmiutil command -V 4 -J 3 -N IP_address -Uuser_name
```

이 명령은 어플라이언스에서 실제로 존재 하는 것 처럼 로그인 할 수 있는 기기의 명령행에 연결 합니다. 비밀번호를 입력하라는 프롬프트가 표시될 수 있습니다.

IPMItool을 사용한 SoL(Serial over LAN) 설정

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMItool을 사용하여 다음 명령을 입력하고 메시지가 표시되면 암호를 입력합니다.

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

IPMIutil을 사용한 SoL(Serial over LAN) 설정

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMIutil을 사용하여 다음 명령을 입력하고 메시지가 표시되면 암호를 입력합니다.

```
ipmiutil -J 3 -N IP_address -U username sol -a
```

LOM(Lights-Out Management) 개요

Lights-Out Management(LOM)를 사용하면 시스템에 로그인하지 않고도 기본(`eth0`) 관리 인터페이스에서 SOL 연결을 통해 제한된 작업을 수행할 수 있습니다. 이 명령을 사용하여 SOL 연결을 생성한 후 LOM 명령 중 하나를 사용합니다. 명령이 완료되면 연결이 종료됩니다.

주의 드물긴 하지만, 시스템의 관리 인터페이스와 다른 서브넷에 있으며 시스템이 DHCP로 구성되어 있는 경우 LOM 기능에 액세스하려고 시도하면 실패할 수 있습니다. 이런 일이 발생하면 시스템에서 LOM을 비활성화한 후 다시 활성화하거나, 동일한 서브넷의 컴퓨터를 시스템으로 사용하여 관리 인터페이스를 ping할 수 있습니다. 이렇게 하면 LOM을 사용할 수 있게 됩니다.

주의 Cisco에서는 IPMI(Intelligent Platform Management Interface) 표준(CVE-2013-4786)에 내재된 취약성에 대해 잘 알고 있습니다. 시스템에서 LOM(Lights-Out Management)을 활성화하면 이 취약성이 노출됩니다. 이 취약성을 완화하려면 신뢰할 수 있는 사용자만 액세스할 수 있는 안전한 관리 네트워크에 시스템을 구축하고, 시스템에서 지원되는 최대 길이로 사전에 없는 복잡한 비밀번호를 사용하고 3개월에 한 번씩 변경하십시오. 이 취약성이 노출되지 않도록 하려면 LOM을 활성화하지 마십시오.

시스템에 대한 모든 액세스 시도가 실패한 경우 LOM을 사용하여 시스템을 원격으로 재시작할 수 있습니다. SOL 연결이 활성화된 상태에서 시스템을 다시 시작하면 LOM 세션이 끊어지거나 시간이 초과될 수 있습니다.

주의 다시 시작하려는 다른 시도에 응답하지 않는 상황이 아니면 시스템을 다시 시작하지 마십시오. 원격으로 다시 시작하는 경우 시스템이 정상적으로 재부팅되지 않으며, 데이터가 손실될 수 있습니다.

표 *3: Lights-Out Management* 명령

IPMItool	IPMIutil	설명
(해당 없음)	`-V 4`	IPMI 세션의 관리자 권한을 활성화합니다.
`-I lanplus`	`-J 3`	IPMI 세션의 암호화를 활성화합니다.

IPMItool	IPMIutil	설명
`-H 호스트 이름/IP 주소`	`-N 노드 이름/IP 주소`	다음에 대한 LOM IP 주소 또는 호스트 이름을 나타 management center
`-U`	`-U`	권한이 있는 LOM 계정의 사용자 이름을 나타냅니
`sol activate`	`sol -a`	SOL 세션을 시작합니다.
`sol deactivate`	`sol -d`	SOL 세션을 종료합니다.
`chassis power cycle`	`power -c`	어플라이언스를 다시 시작합니다.
`chassis power on`	`power -u`	어플라이언스 전원을 켭니다.
`chassis power off`	`power -d`	어플라이언스 전원을 끕니다
`sdr`	`sensor`	팬 속도와 온도 등 어플라이언스 정보를 표시합니

예를 들어 어플라이언스 정보 목록을 표시하려면 다음 IPMItool 명령을 사용합니다.

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

참고 IPMItool 버전 1.8.12 이상을 사용하는 것이 좋습니다.

IPMIutil 유틸리티에서는 동일한 명령이 다음과 같습니다.

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

IPMItool을 사용한 LOM(Lights-Out Management) 구성

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMItool에 대해 다음 명령을 입력하고 메시지가 표시되면 비밀번호를 입력합니다.

```
ipmitool -I lanplus -H IP_address -U user_name command
```

IPMIutil을 사용한 LOM(Lights-Out Management) 구성

이 절차를 수행하려면 LOM 액세스 권한이 있는 관리자 사용자여야 합니다.

프로시저

IPMIutil에 대해 다음 명령을 입력하고 메시지가 표시되면 비밀번호를 입력합니다.

```
ipmiutil -J 3 -N IP_address -U username command
```

원격 스토리지 디바이스

management center에서 백업 및 보고를 위해 로컬 또는 원격 스토리지 다음을 사용할 수 있습니다.

- NFS(Network File System)
- Server Message Block (SMB)/Common Internet File System (CIFS)
- SSH(Secure Shell)

백업은 한 원격 시스템으로 전송하고 보고서는 다른 원격 시스템으로 전송할 수는 없습니다. 그러나 둘 중 하나는 원격 시스템으로 전송하고 나머지는 management center에 저장할 수는 있습니다.

팁 원격 스토리지를 구성 및 선택한 경우, 오직 연결 데이터베이스 한도를 높이지 않은 경우에만 로컬 스토리지로 다시 전환할 수 있습니다.

관리 센터 원격 스토리지 - 지원되는 프로토콜 및 버전

Mangement Center 버전	**NFS** 버전	**SSH** 버전	**SMB** 버전
6.4	V3/V4	openssh 7.3p1	V2/V3
6.5	V3/V4	ciscossh 1.6.20	V2/V3
6.6	V3/V4	ciscossh 1.6.20	V2/V3
6.7	V3/V4	ciscossh 1.6.20	V2/V3

프로토콜 버전을 활성화하는 명령

프로토콜 버전을 활성화하려면 루트 사용자로 다음 명령을 실행합니다.

- **NFS**—`/bin/mount -t nfs '10.10.4.225':'/home/manual-check' '/mnt/remote-storage' -o 'rw,vers=4.0'`
- **SMB**—`/usr/bin/mount.cifs //10.10.0.100/pyallapp-share/testing-smb /mnt/remote-storage -o username=administrator,password=******,vers=3.0`

로컬 스토리지 설정

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Remote Storage Device(**원격 스토리지 디바이스**)**를 선택합니다.

단계 **3** **Storage Type(**스토리지 유형**)** 드롭다운 목록에서 **Local (No Remote Storage)(**로컬**(**원격 스토리지 아님**))**을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

원격 스토리지에 대한 **NFS** 설정

시작하기 전에

- 외부 원격 스토리지 시스템이 정상적으로 작동하는지와 management center에서 액세스할 수 있는지를 확인합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Remote Storage Device(**원격 스토리지 디바이스**)**를 클릭합니다.

단계 **3** **Storage Type(**스토리지 유형**)** 드롭다운 목록에서 **NFS**를 선택합니다.

단계 **4** 연결 정보를 추가합니다.

- 스토리지 시스템의 IPv4 주소 또는 호스트 이름을 **Host(**호스트**)** 필드에 입력합니다.
- 스토리지 영역에 대한 경로를 **Directory(**디렉터리**)** 필드에 입력합니다.

단계 **5** 선택적으로 **Use Advanced Options(**고급 옵션 사용**)** 확인란을 선택하고 필요한 명령줄 옵션을 입력합니다. 원격 스토리지 관리 고급 옵션, 98 페이지 섹션을 참조하십시오.

단계 **6** **System Usage(**시스템 사용**)**에서:

- 지정된 호스트에 백업을 저장하려면 **Use for Backups(**백업용으로 사용**)**를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports(**보고서용으로 사용**)**를 선택합니다.
- 원격 스토리지용 백업에 대해 **Disk Space Threshold**를 입력합니다. 기본값은 90%입니다.

단계 **7** 설정을 테스트하려면 **Test(**테스트**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

원격 스토리지에 대한 SMB 설정

시작하기 전에

외부 원격 스토리지 시스템이 정상적으로 작동하는지와 management center에서 액세스할 수 있는지를 확인합니다.

- 시스템에서는 전체 파일 경로가 아니라 상위 레벨의 공유만 인식합니다. 사용하려는 정확한 디렉토리를 공유하려면 Windows를 사용해야 합니다.
- FMC에서 SMB 공유에 액세스하는 데 사용할 Windows 사용자에게 공유 위치에 대한 소유권과 읽기/변경 액세스 권한이 있는지 확인합니다.
- 보안을 유지하려면 SMB 2.0 이상을 설치해야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration**(구성)을(를) 선택합니다.

단계 **2** **Remote Storage Device**(원격 스토리지 디바이스)를 클릭합니다.

단계 **3** **Storage Type**(스토리지 유형) 드롭다운 목록에서 **SMB**를 선택합니다.

단계 **4** 연결 정보를 추가합니다.

- 스토리지 시스템의 IPv4 주소 또는 호스트 이름을 **Host**(호스트) 필드에 입력합니다.
- 스토리지 영역의 공유를 **Share**(공유) 필드에 입력합니다.
- 선택적으로, 원격 스토리지 시스템의 도메인 이름을 **Domain**(도메인) 필드에 입력합니다.
- **Username**(사용자 이름) 필드에 스토리지 시스템의 사용자 이름을 입력하고 **Password**(비밀번호) 필드에 해당 사용자의 비밀번호를 입력합니다.

단계 **5** 선택적으로 **Use Advanced Options**(고급 옵션 사용) 확인란을 선택하고 필요한 명령줄 옵션을 입력합니다. 원격 스토리지 관리 고급 옵션, 98 페이지 섹션을 참조하십시오.

단계 **6** **System Usage**(시스템 사용)에서:

- 지정된 호스트에 백업을 저장하려면 **Use for Backups**(백업용으로 사용)를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports**(보고서용으로 사용)를 선택합니다.

단계 **7** 설정을 테스트하려면 **Test**(테스트)를 클릭합니다.

단계 **8** **Save**(저장)를 클릭합니다.

원격 스토리지에 대한 SSH 설정

시작하기 전에

- 외부 원격 스토리지 시스템이 정상적으로 작동하는지와 management center에서 액세스할 수 있는지를 확인합니다.

프로시저

단계 1 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 2 **Remote Storage Device(**원격 스토리지 디바이스**)**를 클릭합니다.

단계 3 **Storage Type(**스토리지 유형**)** 드롭다운 목록에서 **SSH**를 선택합니다.

단계 4 연결 정보를 추가합니다.

- 스토리지 시스템의 IP 주소 또는 호스트네임을 **Host(**호스트**)** 필드에 입력합니다.
- 스토리지 영역에 대한 경로를 **Directory(**디렉터리**)** 필드에 입력합니다.
- **Username(**사용자 이름**)** 필드에 스토리지 시스템의 사용자 이름을 입력하고 **Password(**비밀번호**)** 필드에 해당 사용자의 비밀번호를 입력합니다. 연결 사용자 이름의 일부로 네트워크 도메인을 지정하려면 사용자 이름 앞에 슬래시(/)가 오는 도메인을 지정합니다.
- SSH 키를 사용하려면 **SSH Public Key** 필드의 내용을 복사하여 authorized_keys 파일에 붙여넣습니다.

단계 5 선택적으로 **Use Advanced Options(**고급 옵션 사용**)** 확인란을 선택하고 필요한 명령줄 옵션을 입력합니다. 원격 스토리지 관리 고급 옵션, 98 페이지 섹션을 참조하십시오.

단계 6 System Usage(시스템 사용)에서:

- 지정된 호스트에 백업을 저장하려면 **Use for Backups(**백업용으로 사용**)**를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports(**보고서용으로 사용**)**를 선택합니다.

단계 7 설정을 테스트하려면 **Test(**테스트**)**를 클릭해야 합니다.

단계 8 **Save(**저장**)**를 클릭합니다.

원격 스토리지 관리 고급 옵션

SFMB(보안 파일 전송 프로토콜)를 사용하여 보고서 및 백업을 저장하기 위해 NFS(Network File System) 프로토콜, SMB(Server Message Block) 프로토콜 또는 SSH를 선택하는 경우 **Use Advanced Options(**고급 옵션 사용**)** 확인란을 선택하여 NFS, SMB 또는 SSH 마운트 메인 페이지에 설명된 마운트 바이너리 옵션 중 하나를 사용할 수 있습니다

SMB 또는 NFS 스토리지 유형을 선택하는 경우 다음 형식을 사용하여 **Command Line Option(**명령줄 옵션**)** 필드에서 원격 스토리지의 버전 번호를 지정할 수 있습니다.

`vers=version`

여기서 `version`은 사용할 SMB 또는 NFS 원격 스토리지의 버전 번호입니다. 예를 들어 NFSv4를 선택하려면 `vers=4.0`을 입력합니다.

파일 서버에 대해 SMB 암호화가 활성화된 경우 SMB 버전 3.0 클라이언트만 파일 서버에 액세스할 수 있습니다. management center에서 암호화된 SMB 파일 서버에 액세스하려면 **Command Line Option(**명령줄 옵션**)** 필드에 다음을 입력합니다.

`vers=3.0`

여기서 암호화된 SMBv3를 선택하여 management center에서 암호화된 SMB 파일 서버로 백업 파일을 복사하거나 저장합니다.

SNMP

SNMP(Simple Network Management Protocol) 폴링을 활성화할 수 있습니다. 이 기능은 SNMP 프로토콜의 1, 2, 3 버전 사용을 지원합니다. 이 기능을 이용하면 연락처, 관리, 위치, 서비스 정보, IP 주소 지정 및 라우팅 정보, 전송 프로토콜 사용 통계 등의 시스템 세부사항을 포함하는 표준 MIB(management information base)에 액세스할 수 있습니다.

참고 SNMP 프로토콜을 위한 SNMP 버전을 선택하는 경우, SNMPv2는 일기 전용 커뮤니티만 지원하며 SNMPv3는 읽기 전용 사용자만 지원한다는 사실을 유념하십시오. SNMPv3는 AES128을 이용한 암호화도 지원합니다.

SNMP 폴링을 활성화한다고 해서 시스템에서 SNMP 트랩을 전송하지는 않습니다. MIB의 정보를 네트워크 관리 시스템을 통한 폴링에 사용할 수 있도록 지원할 뿐입니다.

SNMP 폴링 구성

시작하기 전에

시스템 폴링에 사용할 각 컴퓨터에 대해 SNMP 액세스를 추가합니다. 액세스 목록 구성, 45 페이지의 내용을 참조하십시오.

참고 SNMP MIB에는 구축을 공격하는 데 사용할 수 있는 정보가 있습니다. Cisco에서는 MIB를 폴링하는 데 사용하는 특정 호스트에 대한 SNMP 액세스용 액세스 목록을 제한할 것을 권장합니다. 또한 SNMPv3을 사용하고 네트워크 관리 액세스에 강력한 비밀번호를 사용할 것도 권장합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **SNMP**를 클릭합니다.

단계 **3** **SNMP Version(SNMP** 버전**)** 드롭다운 목록에서, 사용할 SNMP 버전을 선택합니다.

- **Version(**버전**) 1** 또는 **Version(**버전**) 2**: 커뮤니티 문자열 필드에 읽기 전용 SNMP 커뮤니티 이름을 넣고 절차 종료로 건너뜁니다.

  참고 SNMP 커뮤니티 문자열 이름에는 특수문자(< > / % # & ? ', 등)를 포함하지 않습니다.

- **Version 3(**버전 **3)**: **Add User(**사용자 추가**)**를 클릭하여 사용자 정의 페이지를 표시합니다. SNMPv3는 읽기 전용 사용자 및 AES128 암호화만 지원합니다.

단계 **4** 사용자 이름을 입력합니다.

단계 **5** **Authentication Protocol(**인증 프로토콜**)** 드롭다운 목록에서 인증에 사용할 프로토콜을 선택합니다.

단계 **6** **Authentication Password(**인증 비밀번호**)** 필드에 SNMP 서버와 함께 인증에 필요한 비밀번호를 입력합니다.

단계 **7** **Verify Password(**비밀번호 확인**)** 필드에 인증 비밀번호를 다시 입력합니다.

단계 **8** 사용할 비공개 프로토콜을 **Privacy Protocol** 목록에서 선택하거나, 비공개 프로토콜을 사용하지 않으려면 **None**을 선택합니다.

단계 **9** **Privacy Password(**프라이버시 비밀번호**)** 필드에 SNMP 서버에 필요한 SNMP 프라이버시 키를 입력합니다.

단계 **10** **Verify Password(**비밀번호 확인**)** 필드에 프라이버시 비밀번호를 다시 입력합니다.

단계 **11** **Add(**추가**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

세션 시간 초과

무인 로그인 세션은 보안 위험이 될 수 있습니다. 비활성으로 인해 사용자 로그인 세션이 시간 초과되기까지의 유휴 시간을 구성할 수 있습니다.

시스템을 오랫동안 패시브 방식으로 안전하게 모니터링하려는 상황이라면, 특정 웹 인터페이스 사용자를 시간 제한에서 제외할 수 있습니다. 메뉴 옵션에 완전히 액세스할 수 있으므로 손상 시 더 큰 위험을 초래하는 Administrator 역할의 사용자는 세션 시간 초과에서 제외할 수 없습니다.

세션 시간 제한 구성

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **CLI Timeout(CLI** 시간 초과**)**를 클릭합니다.

단계 **3** 세션 시간 제한 구성

- 웹 인터페이스(management center에만 해당): 브라우저 세션 시간 제한(분)을 구성합니다. 기본값은 60이고 최대값은 1440(24시간)입니다.

  이 세션 시간 제한에서 사용자를 제외하는 방법은 내부 사용자 추가, 123 페이지의 내용을 참조하십시오.

- CLI: **CLI** 시간 제한(분) 필드를 구성합니다. 기본값은 0이고 최대값은 1440(24시간)입니다.

단계 **4** **Save**(저장)를 클릭합니다.

시간

시간 설정이 대부분의 페이지에서 로컬 시간으로 표시됩니다. 여기서 사용되는 시간대는 User Preferences(사용자 환경 설정)의 Time Zone(표준 시간대) 페이지에서 설정하며(기본값은 미국/뉴욕), UTC 시간을 사용해 어플라이언스에 저장합니다.

제한 Time Zone(표준 시간대) 기능(User Preferences(사용자 환경 설정))에서는 기본 시스템 시계가 UTC 시간으로 설정되었다고 가정합니다. 시스템 시간을 변경하지 마십시오. UTC 시스템 시간 변경은 지원되지 않으며, 그러할 경우 지원되지 않는 상태에서 복구하기 위해 디바이스 이미지를 다시 생성해야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration**(구성)을(를) 선택합니다.

단계 **2** **Time**(시간)을 클릭합니다.

현재 시간은 사용자 기본 설정에서 계정에 지정된 표준 시간대를 사용하여 표시됩니다.

어플라이언스에서 NTP 서버를 사용하는 경우: 테이블 항목에 대한 자세한 내용은 NTP 서버 상태, 101 페이지 섹션을 참조하십시오.

NTP 서버 상태

NTP 서버에서 시간을 동기화한다면, **Time**(시간) 페이지에서 연결 상태를 볼 수 있습니다(**System**(시스템) > **Configuration**(구성)선택).

표 *4: NTP* 상태

열	설명
NTP 서버	구성된 NTP 서버의 IP 주소 및 이름.
상태	NTP 서버 시간 동기화의 상태: • **Being Used(**사용 중**)** - 어플라이언스가 NTP 서버와 동기화됨을 나타냅니다. • **Available(**사용 가능**)** - NTP 서버를 사용할 수 있지만 시간이 아직 동기화되지 않았음을 나타냅니다. • **Not Available(**사용 불가**)** - NTP 서버가 설정에 있지만 NTP 디먼이 이를 사용할 수 없음을 나타냅니다. • **Pending(**보류 중**)** - NTP 서버가 새로운 것이거나 NTP 디먼이 최근에 다시 시작되었음을 나타냅니다. 시간 경과에 따라 값이 **Being Used(**사용 중**)**, **Available(**사용 가능**)** 또는 **Not Available(**사용 불가**)**로 변경됩니다. • **Unknown(**알 수 없음**)** - NTP 서버의 상태를 알 수 없음을 나타냅니다.
인증	management center 및 NTP 서버 간의 통신에 대한 인증 상태입니다. • **none(**없음**)**은 인증을 구성하지 않았다는 뜻입니다. • **bad(**불량**)**은 인증을 구성했지만 실패했다는 뜻입니다. • **ok(**양호**)**는 인증에 성공했다는 뜻입니다. 인증을 구성했다면, 시스템은 상태 값 다음에 키 번호와 키 유형(SHA-1, MD5 또는 AES-128 CMAC)을 표시합니다. 예: **bad, key 2, MD5**.
오프셋	어플라이언스 및 구성된 NTP 서버 간 밀리초 단위의 시간 차이. 음수 값은 어플라이언스가 NTP 서버 뒤에 있음을 나타내고, 양수 값은 그 반대를 나타냅니다.
마지막 업데이트	시간이 NTP 서버와 마지막으로 동기화된 후 경과한 기간(초). NTP 디먼은 몇 가지 조건을 기반으로 동기화 시간을 자동으로 조정합니다. 예를 들어 300초와 같이 업데이트 시간이 좀 더 긴 경우, 이는 시간이 비교적 안정적이며 NTP 디먼이 더 낮은 업데이트 증분을 사용할 필요가 없다고 결정했음을 나타냅니다.

시간 동기화

Secure Firewall Management Center(management center)와 매니지드 디바이스에서 시스템 시간을 동기하하는 작업은 시스템의 성공적인 작업을 위해 반드시 필요합니다. Cisco에서는 management center 초기 구성 중에 NTP 서버를 지정할 것을 권장하지만, 초기 구성이 끝난 후 이 섹션의 정보를 이용해 시간 동기화 설정을 구성하거나 변경할 수 있습니다.

management center 및 모든 디바이스에서 시스템 시간을 동기화하려면 NTP(Network Time Protocol) 서버를 사용합니다. management center는 MD5, SHA-1 또는 AES-128 CMAC 대칭 키 인증을 통해 NTP 서버와의 안전한 통신을 지원합니다. Cisco에서는 시스템 보안을 위해 이 기능을 사용하도록 권장합니다.

또한 인증된 NTP 서버에만 연결하도록 management center를 구성할 수도 있습니다. 혼합 인증 환경을 이용 중이거나 시스템을 다른 NTP 서버로 마이그레이션할 때 이 옵션을 이용하면 보안을 강화할 수 있습니다. 연결 가능한 모든 NTP 서버가 인증된 환경에서 이 설정을 사용하는 것은 중복 행위입니다.

참고 초기 구성 중에 management center에 NTP 서버를 지정하면, 해당 NTP 서버와의 연결은 보호되지 않습니다. 연결이 MD5, SHA-1 또는 AES-128 CMAC 키를 지정하도록 설정을 편집해야 합니다.

주의 시간이 management center 및 매니지드 디바이스 간에 동기화되지 않으면 의도하지 않은 결과가 발생할 수 있습니다.

management center 및 매니지드 디바이스의 시간을 동기화하는 방법은 다음을 참조하십시오.

- 권장: Management Center의 시간을 NTP 서버와 동기화, 103 페이지

  이 주제에서는 management center를 NTP 서버 또는 서버와 동기화하도록 설정하는 데 필요한 지침을 제공하며, 동일한 NTP 서버와 동기화하도록 매니지드 디바이스를 설정하는 방법을 안내하는 링크를 제공합니다.

- 그렇지 않을 경우, 네트워크 NTP 서버에 액세스하지 않고 시간 동기화, 105 페이지

  이 주제에서는 management center에서 시간을 설정하고 NTP 서버 역할을 하도록 management center를 설정하는 방법에 대한 지침과 management center NTP 서버와 동기화하도록 매니지드 디바이스를 설정하는 지침으로 연결되는 링크를 제공합니다.

Management Center의 시간을 NTP 서버와 동기화

시스템의 모든 구성 요소 간의 시간 동기화는 매우 중요합니다.

management center 및 모든 매니지드 디바이스 간의 적절한 시간 동기화를 보장하는 가장 좋은 방법은 네트워크에서 NTP 서버를 사용하는 것입니다.

management center은(는) NTPv4를 지원합니다.

이 절차를 수행하려면 관리자 또는 네트워크 관리자 권한이 있어야 합니다.

시작하기 전에

다음에 유의하십시오.

- management center 및 매니지드 디바이스가 네트워크 NTP 서버에 액세스할 수 없다면 이 절차를 사용하지 마십시오. 대신 네트워크 NTP 서버에 액세스하지 않고 시간 동기화, 105 페이지 섹션을 참조하십시오.

- 신뢰할 수 없는 NTP 서버를 지정하지 마십시오.
- (시스템 보안 상 권장되는) NTP 서버와의 보안 연결을 설정하려면, 해당 NTP 서버에 설정된 SHA-1, MD5 또는 AES-128 CMAC 키 번호 및 값을 얻어야 합니다.
- NTP 서버에 대한 연결에는 구성된 프록시 설정이 사용되지 않습니다.
- Firepower 4100 시리즈 디바이스 및 Firepower 9300 디바이스는 이 절차를 사용하여 시스템 시간을 설정할 수 없습니다. 대신 이 절차를 사용하여 설정한 것과 동일한 NTP 서버를 사용하도록 해당 디바이스를 설정합니다. 자세한 내용은 하드웨어 모델의 설명서를 참조하십시오.

⚠

주의 management center가 재부팅되고 DHCP 서버가 NTP 서버 레코드를 여기에 지정된 것과 다르게 설정하는 경우 DHCP 제공 NTP 서버가 대신 사용됩니다. 이 상황을 피하려면 DHCP 서버를 동일한 NTP 서버를 사용하게 설정하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Time Synchronization(**시간 동기화**)**을 클릭합니다.

단계 **3** **Serve Time via NTP(NTP**를 통해 시간 제공**)**가 **Enabled(**활성화됨**)**인 경우라면, **Disabled(**비활성화됨**)**를 선택해 management center을(를) NTP 서버로 비활성화합니다.

단계 **4** **Set My Clock(**내 시계 설정**)** 옵션에서 **Via NTP(NTP**를 통해**)**를 선택합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** **Add NTP Server(NTP** 서버 추가**)** 대화상자에 NTP 서버의 호스트 이름, IPv4 또는 IPv6 주소를 입력합니다.

단계 **7** (선택 사항) management center 및 NTP 서버 간의 통신을 보호하려면 다음을 수행합니다.

a) **Key Type(**키 유형**)** 드롭다운 목록에서 **MD5**, **SHA-1** 또는 **AES-128 CMAC**를 선택합니다.

b) 지정된 NTP 서버에서 해당 MD5, SHA-1 또는 AES-128 CMAC 키 번호와 키 값을 입력합니다.

단계 **8** **Add(**추가**)**를 클릭합니다.

단계 **9** 다른 NTP 서버를 추가하려면 5~8 단계를 반복합니다.

단계 **10** (선택 사항) management center에서 인증에 성공한 NTP 서버만 사용하게 하려면, **Use the authenticated NTP server only(**인증된 **NTP** 서버만 사용**)** 확인란을 선택합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

다음과 같이 매니지드 디바이스를 동일한 NTP 서버나 서버 모음과 동기화되도록 설정합니다.

- 디바이스 플랫폼 설정 구성: Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Threat Defense*를 위한 *NTP* 시간 동기화 구성.

management center가 NTP 서버와 보안 연결을 구성하도록 강제하더라도(인증된 **NTP** 서버만 사용), 해당 서버에 대한 디바이스 연결은 인증을 사용하지 않습니다.

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

네트워크 NTP 서버에 액세스하지 않고 시간 동기화

디바이스에서 네트워크 NTP 서버에 직접 연결할 수 없는 경우 또는 조직에 네트워크 NTP 서버가 없는 경우, 물리적 하드웨어 management center가 NTP 서버 역할을 수행할 수 있습니다.

중요

- 다른 NTP 서버가 없는 경우가 아니면 이 절차를 사용하지 마십시오. 대신 Management Center의 시간을 NTP 서버와 동기화, 103 페이지의 절차를 사용하십시오.
- 가상 management center를 NTP 서버로 사용하지 마십시오.

management center를 NTP 서버로 설정한 후 수동으로 시간을 변경하려면 NTP 옵션을 비활성화하고 수동으로 시간을 변경한 다음 NTP 옵션을 다시 활성화해야 합니다.

프로시저

단계 **1** 다음과 같이 management center에서 시스템 시간을 수동으로 설정합니다.

a) 시스템 (⚙) > **Configuration**(구성)을(를) 선택합니다.
b) **Time Synchronization**(시간 동기화)을 클릭합니다.
c) **Serve Time via NTP**(NTP를 통해 시간 제공)가 **Enabled**(활성화됨)인 경우 **Disabled**(비활성화됨)를 선택합니다.
d) **Save**(저장)를 클릭합니다.
e) **Set My Clock**(내 클럭 설정)에서 **Manually in Local Configuration**(로컬 구성에서 수동으로)을 선택합니다.
f) **Save**(저장)를 클릭합니다.
g) 화면 왼쪽 탐색 패널에서 **Time**(시간)을 클릭합니다.
h) **Set Time**(시간 설정) 드롭다운 목록을 사용하여 시간을 설정합니다.
i) 표시된 표준 시간대가 UTC가 아닌 경우, 이를 클릭하고 표준 시간대를 **UTC**로 설정합니다.
j) **Save**(저장)를 클릭합니다.
k) **Done**(완료)을 클릭합니다.
l) **Apply**(적용)를 클릭합니다.

단계 **2** 다음과 같이 management center가 NTP 서버 역할을 하도록 설정합니다.

a) 화면 왼쪽 탐색 패널에서 **Time Synchronization**(시간 동기화)을 클릭합니다.
b) **Serve Time via NTP**(NTP를 통해 시간 제공)에 대해 **Enabled**(활성화됨)를 선택합니다.
c) **Save**(저장)를 클릭합니다.

단계 **3** 다음과 같이 매니지드 디바이스를 management center NTP 서버와 동기화되도록 설정합니다.

a) 매니지드 디바이스에 할당된 플랫폼 설정 정책에 대한 Time Synchronization(시간 동기화) 설정에서 **Via NTP from Management Center(Management Center**에서 **NTP**를 통해**)**를 사용하여 동기화하도록 클럭을 설정합니다.

b) 매니지드 디바이스에 변경 사항을 구축합니다.

지침은 다음 내용을 참조하십시오.

threat defense 디바이스의 경우 Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *Threat Defense*를 위한 *NTP* 시간 동기화 구성을 참조하십시오.

시간 동기화 설정 변경 정보

- management center 및 매니지드 디바이스는 주로 정확한 시간에 의존합니다. 시스템 시계는 시스템의 시간을 유지하는 시스템 기능입니다. 시스템 시계는 전 세계가 시계와 시간을 규제하는 기본 시간 기준인 UTC(Universal Coordinated Time)로 설정됩니다.

  시스템 시간을 변경하지 마십시오. UTC 시스템 시간 변경은 지원되지 않으며, 변경할 경우 지원되지 않는 상태에서 복구하기 위해 디바이스 이미지를 다시 생성해야 합니다.

- NTP를 사용하여 시간을 서비스하도록 management center를 구성한 다음 나중에 이를 비활성화하면, 매니지드 디바이스의 NTP 서비스는 계속해서 management center와 시간을 동기화하려고 시도합니다. 새 시간 소스를 설정하려면 해당 플랫폼 설정 정책을 업데이트하고 다시 구축해야 합니다.

- management center를 NTP 서버로 설정한 후 수동으로 시간을 변경하려면 NTP 옵션을 비활성화하고 수동으로 시간을 변경한 다음 NTP 옵션을 다시 활성화해야 합니다.

UCAPL/CC 규정준수

조직에서는 미국국방부 및 글로벌 인증 기관이 마련한 보안 표준을 준수하는 장비 및 소프트웨어만 사용해야 할 수 있습니다. 이 설정에 대한 자세한 내용은 보안 인증서 컴플라이언스 모드, 335 페이지의 내용을 참고하십시오.

사용자 구성

전역 사용자 구성 설정은 management center에 있는 모든 사용자에게 영향을 줍니다. User Configuration(사용자 구성) 페이지(시스템 (⚙) > **Configuration(**구성**)** > **User Configuration(**사용자 구성**)**)에서 이러한 설정을 구성합니다.

- **Password Reuse Limit(**비밀번호 재사용 한도**)**: 재사용할 수 없는 사용자의 최근 기록에 있는 비밀번호 수입니다. 이 제한은 모든 사용자의 웹 인터페이스 액세스에 적용됩니다. 관리자 사용자의 경우 이는 CLI 액세스에도 적용됩니다. 시스템은 각 액세스 형식에 대해 별도의 비밀번호 목록

을 유지합니다. 한도를 0(기본값)으로 설정하면 비밀번호 재사용에 대한 제한이 없습니다. 암호 재사용 한도 설정, 108 페이지의 내용을 참조하십시오.

- **Track Successful Logins(**성공적인 로그인 추적**)**: 시스템이 사용자별, 액세스 방법별(웹 인터페이스 또는 CLI)로 management center에 대한 성공적인 로그인을 추적하는 일수입니다. 사용자가 로그인하면 사용 중인 인터페이스에 대한 로그인 성공 횟수가 표시됩니다. **Track Successful Logins(**성공적인 로그인 추적**)**가 가 0으로 설정되면(기본값) 시스템은 로그인 활동을 추적하거나 보고하지 않습니다. 성공적인 로그인 추적, 108 페이지의 내용을 참조하십시오.
- **Max Number of Login Failures(**최대 로그인 실패 횟수**)**: 시스템이 구성 가능한 시간 동안 계정 액세스를 일시적으로 차단하기 전에 사용자가 잘못된 웹 인터페이스 로그인 자격 증명을 연속적으로 입력할 수 있는 횟수입니다. 임시 잠금이 적용되는 동안 사용자가 로그인 시도를 계속하는 경우:
  - 시스템은 사용자에게 임시 잠금이 적용되었음을 알리지 않고 해당 계정에 대한 액세스(유효한 비밀번호 포함)를 거부합니다.
  - 시스템은 로그인 시도가 있을 때마다 해당 계정의 로그인 실패 횟수를 계속 누적합니다.
  - 사용자가 개별 User Configuration(사용자 구성) 페이지에서 해당 계정에 대해 구성된 **Maximum Number of Failed Logins(**최대 실패 로그인 횟수**)**를 초과하면 관리자 사용자가 다시 활성화할 때까지 계정이 잠깁니다.
- **Set Time in Minutes to Temporarily Lockout Users(**사용자에 대한 임시 잠금 시간**(**분**)** 설정**)**: **Maximum Number of Failed Logins(**최대 실패 로그인 횟수**)**가 0이 아닌 경우 임시 웹 인터페이스 사용자 잠금 기간(분)입니다.
- **Max Concurrent Sessions Allowed(**허용되는 최대 동시 세션 수**)**: 동시에 열 수 있는 특정 유형(읽기 전용 또는 읽기/쓰기)의 세션 수입니다. 세션 유형은 사용자에게 할당된 역할을 기준으로 결정됩니다. 사용자에게 읽기 전용 역할만 할당되었다면, 해당 사용자의 세션은 **(**읽기 전용**)** 세션 제한 수에 적용됩니다. 사용자에게 쓰기 권한을 제공하는 역할이 있다면, 세션은 읽기/쓰기 세션 제한 수에 적용됩니다. 예를 들어 사용자에게 관리자 역할이 할당되고 **Maximum sessions for users with Read/Write privileges/CLI users(**읽기/쓰기 권한이 있는 사용자**/CLI** 사용자의 최대 세션 수**)**를 5로 설정했다면, 사용자는 읽기/쓰기 권한이 있는 다른 사용자 5명이 로그인한 상태에서는 로그인할 수 없습니다.

참고 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 사전 정의된 사용자 역할과 맞춤형 사용자 역할은 시스템 (⚙) > **Users(**사용자**)** > **Users(**사용자**)** 및 시스템 (⚙) > **Users(**사용자**)** > **User Roles(**사용자 역할**)**의 역할 이름에 **(**읽기 전용**)**이라고 표시됩니다. 사용자 역할의 역할 이름에 **(**읽기 전용**)**이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다. 시스템은 **(**읽기 전용**)**을 필수 기준을 충족하는 역할에 자동으로 적용합니다. 텍스트 문자열을 역할 이름에 수동으로 추가하는 방법으로는 역할을 읽기 전용을 만들 수 없습니다.

각 세션 유형에 대해 1~1024 범위의 최대 제한을 설정할 수 있습니다. **Max Concurrent Sessions Allowed(**허용되는 최대 동시 세션**)**을 0(기본값)으로 설정하면, 동시 세션 수는 무제한이 됩니다.

동시 세션 제한을 더 제한적인 값으로 변경하면, 시스템은 현재 열린 세션을 닫지는 않습니다. 대신 지정된 숫자 이상의 신규 세션이 열리지 않게 합니다.

암호 재사용 한도 설정

Password Reuse Limit(비밀번호 재사용 한도**)**을 활성화하면 시스템은 management center 사용자에 대한 암호화된 비밀번호 기록을 유지합니다. 사용자는 기록에 있는 비밀번호는 다시 사용할 수 없습니다. 액세스 방법(웹 인터페이스 또는 CLI)별로 각 사용자에 대해 저장된 비밀번호 수를 지정할 수 있습니다. 사용자의 현재 비밀번호도 이 숫자에 적용됩니다. 한도를 낮추면 시스템은 기록에서 이전 비밀번호를 삭제합니다. 한도를 늘려도 삭제된 비밀번호는 복원되지 않습니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **User Configuration(**사용자 구성**)**을 클릭합니다.

단계 **3** **Password Reuse Limit(**비밀번호 재사용 한도**)**을 기록에서 유지할 비밀번호 수(최대 256)로 설정합니다.

비밀번호 재사용 검사를 비활성화하려면 0을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

성공적인 로그인 추적

이 절차를 사용하면 지정된 일수 동안 각 사용자에 대해 성공적인 로그인을 추적할 수 있습니다. 이 추적을 활성화하면 사용자가 웹 인터페이스 또는 CLI에 로그인할 때 로그인 성공 횟수가 표시됩니다.

참고 일수를 낮추면 시스템은 이전 로그인 기록을 삭제합니다. 그런 다음 한도를 늘리면 시스템은 해당 일수의 계산을 복원하지 않습니다. 이 경우 보고된 로그인 성공 횟수가 실제 수보다 일시적으로 낮을 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **User Configuration(**사용자 구성**)**을 클릭합니다.

단계 **3** **Track Successful Login Days(**성공적인 로그인 일수 추적**):**를 성공한 로그인을 추적하는 일수로 설정합니다(최대 365일).

로그인 추적을 비활성화하려면 0을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

임시 잠금 활성화

잠금이 적용되기 전에 시스템에서 허용하는 연속적인 로그인 시도 횟수를 지정하여 임시 시간 지정 잠금 기능을 활성화합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **User Configuration(**사용자 구성**)**을 클릭합니다.

단계 **3** 사용자가 일시적으로 잠금 처리되기 전에 **Max Number of Login Failures(**최대 로그인 실패 횟수**)**를 연속 로그인 실패 시도의 최대 횟수로 설정합니다.

임시 잠금을 비활성화하려면 0을 입력합니다.

단계 **4** **Time in Minutes to Temporarily Lockout Users(**사용자에 대한 임시 잠금 시간**(**분**))**를 임시 잠금을 트리거한 사용자를 잠금 처리하는 시간(분)으로 설정합니다.

이 값이 0이면 **Max Number of Login Failures(**최대 로그인 실패 횟수**)**가 0이 아니더라도 사용자가 로그인을 다시 시도할 때까지 기다릴 필요가 없습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

최대 동시 세션 수 설정

동시에 열 수 있는 특정 유형(읽기 전용 또는 읽기/쓰기)의 최대 세션 수를 지정할 수 있습니다. 세션 유형은 사용자에게 할당된 역할을 기준으로 결정됩니다. 사용자에게 읽기 전용 역할만 할당되었다면, 해당 사용자의 세션은 읽기 전용 세션 제한 수에 적용됩니다. 사용자에게 쓰기 권한을 제공하는 역할이 있다면, 세션은 읽기/쓰기 세션 제한 수에 적용됩니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **User Configuration(**사용자 구성**)**을 클릭합니다.

단계 **3** 각 세션 유형(읽기 전용 및 읽기/쓰기)에 대해, **Max Concurrent Sessions Allowed(**허용되는 최대 동시 세션**)**를 해당 유형에 대해 동시에 열 수 있는 최대 세션 수로 설정합니다.

세션 유형별 동시 사용자 수를 제한하지 않으려면 0을 입력합니다.

참고 동시 세션 제한을 더 제한적인 값으로 변경하면, 시스템은 현재 열린 세션을 닫지는 않습니다. 대신 지정된 숫자 이상의 신규 세션이 열리지 않게 합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

VMware Tools

VMware Tools는 가상 머신용 성능 향상 유틸리티 모음입니다. 이러한 유틸리티를 사용하면 VMware 제품의 편리한 기능을 최대한 활용할 수 있습니다. VMware에서 실행되는 Firepower 가상 어플라이언스는 다음 플러그인을 지원합니다.

- guestInfo
- powerOps
- timeSync
- vmbackup

또한 모든 지원되는 ESXi 버전에서 VMware Tools를 활성화할 수 있습니다. VMware Tools의 전체 기능에 대한 자세한 내용은 VMware 웹 사이트(http://www.vmware.com/)를 참조하십시오.

VMware용 Secure Firewall Management Center의 VMWare Tools 활성화

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **VMware Tools**를 클릭합니다.

단계 **3** **Enable VMware Tools(VMware Tools** 활성화**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

취약성 매핑

서버의 검색 이벤트 데이터베이스에 애플리케이션 ID가 있고 트래픽에 대한 패킷 헤더에 공급업체 및 버전이 포함된 경우, 호스트 IP 주소에서 주고받는 모든 애플리케이션 프로토콜 트래픽에 대해 시스템은 해당 주소에 취약성을 자동으로 매핑합니다.

패킷에 공급업체 또는 버전 정보가 포함되어 있지 않은 서버의 경우 시스템이 취약성을 해당 공급업체 및 버전 없는 서버의 서버 트래픽과 연결할지 여부를 구성할 수 있습니다.

예를 들어, 호스트가 헤더에 공급업체 또는 버전을 가지고 있지 않은 SMTP 트래픽을 서비스할 수 있습니다. 시스템 구성의 Vulnerability Mapping 페이지에서 SMTP 서버를 활성화한 다음 트래픽을 탐지하는 디바이스를 관리하는 management center에 해당 구성을 저장하면, SMTP 서버와 관련된 모든 취약성이 호스트의 호스트 프로파일에 추가됩니다.

탐지기는 서버 정보를 수집하여 호스트 프로파일에 추가하지만, 애플리케이션 프로토콜 탐지기는 취약성 매핑에 사용되지 않습니다. 사용자 지정 애플리케이션 프로토콜 탐지기에 대해 공급업체 및 버전을 지정할 수 없으며 취약성 매핑을 위해 서버를 선택할 수 없기 때문입니다.

서버의 취약성 매핑

이 절차를 수행하려면 스마트 라이선스 또는 보호 클래식 라이선스가 필요합니다.

프로시저

단계 **1** 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.

단계 **2** **Vulnerability Mapping(**취약성 매핑**)**을 선택합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 서버에 대한 취약성이 공급업체 또는 버전 정보 없는 애플리케이션 프로토콜 트래픽을 수신하는 호스트에 매핑되지 않도록 하려면 해당 서버의 확인란을 선택 취소합니다.
- 서버에 대한 취약성이 공급업체 또는 버전 정보 없는 애플리케이션 프로토콜 트래픽을 수신하는 호스트에 매핑되도록 하려면 해당 서버의 확인란을 선택합니다.

팁 **Enabled(**활성화됨**)** 옆에 있는 확인란을 사용하여 모든 확인란을 동시에 선택하거나 선택 취소할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

웹 분석

기본적으로 Firepower 제품의 개선을 위해 Cisco에서는 개인 식별 사용 데이터 외의 데이터를 수집합니다. 이러한 데이터에는 페이지 상호작용, 브라우저 버전, 제품 버전, 사용자 위치, management center 어플라이언스의 관리 IP 주소 또는 호스트네임 등이 포함되나 이에 국한되지 않습니다.

최종 사용자 라이선스 계약에 동의하면 데이터 수집이 시작됩니다. Cisco가 이 데이터 수집을 계속하는 것을 원하지 않는다면, 다음 절차를 이용해 거부할 수 있습니다.

프로시저

단계 **1** **System(**시스템**) > Configuration(**구성**)**을 선택합니다.

단계 **2** **Web Analytics(**웹 분석**)**를 클릭합니다.

단계 **3** 선택하고 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

(선택 사항) Cisco Success Network 등록 구성를 통해 데이터를 공유할지 여부를 결정합니다.

시스템 구성 기록

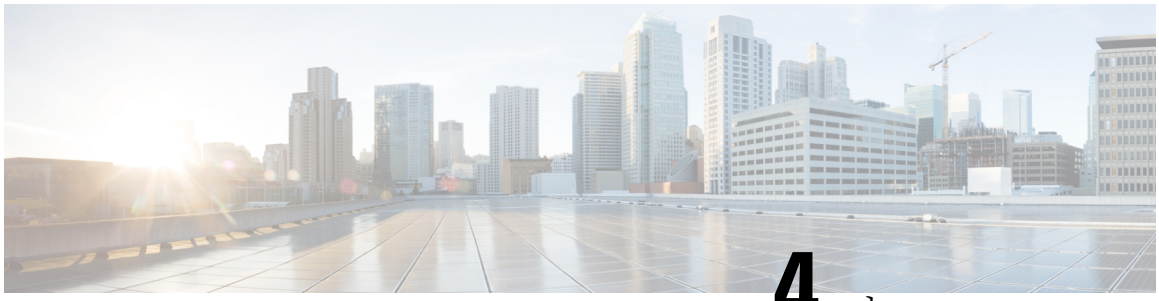
기능	버전	세부정보
액세스 제어 성능 개선(개체 최적화).	7.2.4	액세스 제어 개체 최적화는 중복 네트워크에 액세스 제어 규칙이 있는 경우 성능을 개선하고 더 적은 디바이스 리소스를 사용합니다. 최적화는 Management Center에서 기능이 활성화된 후 첫 번째 구축 시 매니지드 디바이스에서 이루어집니다(업그레이드를 통해 활성화된 경우 포함). 규칙 수가 많으면 시스템이 정책을 평가하고 개체 최적화를 수행하는 데 몇 분에서 1시간 정도 걸릴 수 있습니다. 이 시간 동안에는 디바이스의 CPU 사용률이 더 높을 수도 있습니다. 기능이 비활성화된 후 첫 번째 구축에서도 유사한 일이 발생합니다(업그레이드로 인해 비활성화된 경우 포함). 이 기능을 활성화하거나 비활성화한 후에는 유지 보수 기간이나 트래픽이 적은 시간과 같이 영향이 가장 적을 때 구축하기를 권장합니다. 다음을 계획할 수 있습니다. • 버전 7.2.0~7.2.3 및 7.3에서는 이 기능이 지원되지 않습니다. 이러한 릴리스 중 하나로 업그레이드하거나 이미지를 재설치하면 기능이 비활성화됩니다. • 버전 7.2.4~7.2.5의 경우, 이 기능은 이미지를 재설치한 Management Center 및 업그레이드된 Management Center에 대해 기본적으로 활성화됩니다. 해당 기능을 비활성화하려면 Cisco TAC에 문의하십시오. 최소 위협 방어: 모두
프랑스어 옵션.	7.2	이제 시스템 (⚙) > **Configuration(**구성**)** > **Lanaguage(**언어**)**에서 Management Center 웹 인터페이스를 프랑스어로 전환할 수 있습니다.
가장 높은 연결 이벤트를 이벤트 속도 제한에서 제외.	7.0	연결 데이터베이스의 최대 연결 이벤트 값을 0으로 설정하면 우선순위가 낮은 연결 이벤트가 FMC 하드웨어의 플로우 속도 제한에 포함되지 않습니다. 이전에는 이 값을 0으로 설정하면 이벤트 스토리지에만 적용되었으며, 플로우 속도 제한에는 영향을 주지 않았습니다. 신규/수정된 화면: 시스템 (⚙) > **Configuration(**구성**)** > **Database(**데이터베이스**)** 지원되는 플랫폼: 하드웨어 FMC.

기능	버전	세부정보
NTP 서버에 대한 AES-128 CMAC 인증을 지원합니다.	7.0	AES-128 CMAC 키와 이전에 지원된 MD5 및 SHA-1 키를 사용하여 FMC 및 NTP 서버 간의 연결을 보호할 수 있습니다. 신규/수정된 화면: 시스템 (⚙) > **Configuration(**구성**)** > **Time Synchronization(**시간 동기화**)**
SAN(Subject Alternative Name).	6.6	FMC의 HTTPS 인증서를 생성할 때 SAN 필드를 지정할 수 있습니다. 인증서가 여러 도메인 이름 또는 IP 주소를 보호하는 경우, SAN을 사용하는 것이 좋습니다. SAN에 대한 자세한 내용은 RFC 5280, 섹션 4.2.1.6을 참조하십시오. 신규/수정된 화면: 시스템 (⚙) > **Configuration(**구성**)** > **HTTPS Certificate(HTTPS** 인증서**)**
HTTPS 인증서.	6.6	시스템과 함께 제공되는 기본 HTTPS 서버 인증서는 이제 800일 후에 만료됩니다. 어플라이언스가 버전 6.6으로 업그레이드되기 전에 생성된 기본 인증서를 사용하는 경우, 인증서 수명은 인증서 생성 시 사용되던 Firepower 버전에 따라 달라집니다. 자세한 내용은 기본 HTTPS 서버 인증서, 65 페이지를 참조하십시오. 지원되는 플랫폼: 하드웨어 FMC.
보안 NTP.	6.5	FMC는 SHA1 또는 MD5 대칭 키 인증을 이용하여 NTP 서버와의 보안 연결을 지원합니다. 신규/수정된 화면: 시스템 (⚙) > **Configuration(**구성**)** > **Time Synchronization(**시간 동기화**)**
웹 분석.	6.5	EULA에 동의하면 웹 분석 데이터 수집이 시작됩니다. 예전처럼, 데이터 공유를 계속하지 않도록 선택할 수 있습니다. 웹 분석, 111 페이지의 내용을 참조하십시오.
FMC에 대한 자동 CLI 액세스.	6.5	SSH를 이용하여 FMC에 로그인하면 CLI에 자동으로 액세스하게 됩니다. 권장 사항은 아니지만, 이후 CLI `expert` 명령을 사용하면 Linux 셸에 액세스할 수 있습니다. 참고 이 기능을 이용하면 버전 6.3 기능인 FMC에 대한 CLI 액세스 활성화/비활성화가 중단됩니다. 이 옵션이 중단되면 가상 FMC는 더 이상 시스템 (⚙) > **Configuration(**구성**)** > **Console Configuration(**콘솔 구성**)** 페이지를 표시하지 않습니다. 이 페이지는 물리적 FMC에 계속 표시됩니다.

기능	버전	세부정보
읽기 전용 및 읽기/쓰기 액세스에 구성 가능한 세션 제한.	6.5	**Max Concurrent Sessions Allowed(**허용되는 최대 동시 세션**)** 설정을 추가했습니다. 이 설정을 이용하면 관리자는 동시에 열 수 있는 특정 유형(읽기 전용 또는 읽기/쓰기)의 최대 세션 수를 지정할 수 있습니다. 참고 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 사전 정의된 사용자 역할과 맞춤형 사용자 역할은 시스템 (⚙) > **Users(**사용자**)** > **Users(**사용자**)** 및 시스템 (⚙) > **Users(**사용자**)** > **User Roles(**사용자 역할**)**의 역할 이름에 **(Read Only)(**읽기 전용**)**이라고 표시됩니다. 사용자 역할의 역할 이름에 **(**읽기 전용**)**이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다. 신규/수정된 화면: • 시스템 (⚙) > **Configuration(**구성**)** > **User Configuration(**사용자 구성**)** • 시스템 (⚙) > **Users(**사용자**)** > **User Roles(**사용자 역할**)**
관리 인터페이스에서 DAD(Duplicate Address Detection)를 비활성화하는 기능.	6.4	IPv6를 활성화하면 DAD를 비활성화할 수 있습니다. DAD를 사용하면 서비스 거부(DoS) 공격 가능성이 발생하기 때문에 DAD를 비활성화하려고 할 수 있습니다. 이 설정을 비활성화하면 이 인터페이스가 이미 할당된 주소를 사용하고 있지 않은지 수동으로 확인해야 합니다. 신규/수정된 화면: 시스템 (⚙) > **Configuration(**구성**)(** > **Management Interfaces(**관리 인터페이스**)** > **Interfaces(**인터페이스**)** > **Edit Interface(**인터페이스 편집**)** > **IPv6 DAD** 지원되는 플랫폼: FMC
관리 인터페이스에서 ICMPv6 Echo Reply(ICMPv6 에코 응답) 및 Destination Unreachable(대상 연결 불가) 메시지를 비활성화하는 기능.	6.4	IPv6를 활성화할 때 이제 ICMPv6 Echo Reply 및 Destination Unreachable 메시지를 비활성화할 수 있습니다. 잠재적인 서비스 거부 공격으로부터 보호하기 위해 이러한 패킷을 비활성화할 수 있습니다. 에코 응답 패킷을 비활성화하면 테스트 목적으로 디바이스 관리 인터페이스에 IPv6 ping을 사용할 수 없습니다. 신규/수정된 화면: 시스템 (⚙) > **Management Interfaces(**관리 인터페이스**)** > **ICMPv6** 신규/수정된 명령: **configure network ipv6 destination-unreachable**, **configure network ipv6 echo-reply** 지원되는 플랫폼: FMC(웹 인터페이스에만 해당), FMC(CLI에만 해당)

기능	버전	세부정보
전역 사용자 구성 설정.	6.3	**Track Successful Logins(**성공적인 로그인 추적**)** 설정을 추가했습니다. 시스템은 선택한 일수 이내에 각 FMC 계정이 수행한 성공적인 로그인 수를 추적할 수 있습니다. 이 기능을 활성화하면 로그인 사용자는 구성된 일수 전에 시스템에 성공적으로 로그인한 횟수를 나타내는 메시지를 볼 수 있습니다. (셸/CLI 액세스뿐만 아니라 웹 인터페이스에도 적용됩니다.) **Password Reuse Limit(**비밀번호 재사용 한도**)** 설정을 추가했습니다. 시스템은 구성 가능한 수의 이전 비밀번호에 대해 각 계정의 비밀번호 기록을 추적할 수 있습니다. 시스템은 모든 사용자가 해당 기록에 나타나는 비밀번호를 다시 사용할 수 없게 방지합니다. (셸/CLI 액세스뿐만 아니라 웹 인터페이스에도 적용됩니다.) **Max Number of Login Failures(**최대 로그인 실패 횟수**)** 및 **Set Time in Minutes to Temporarily Lockout Users(**사용자에 대한 임시 잠금 시간**(**분**)** 설정**)** 설정을 추가했습니다. 이는 시스템이 구성 가능한 시간 동안 계정을 일시적으로 차단하기 전에 사용자가 잘못된 웹 인터페이스 로그인 자격 증명을 연속적으로 입력할 수 있는 횟수를 제한하는 기능을 관리자에게 제공합니다. 신규/수정된 화면: 시스템 (⚙) > **Configuration(**구성**)** > **User Configuration(**사용자 구성**)** 지원되는 플랫폼: FMC
HTTPS 인증서.	6.3	시스템과 함께 제공되는 기본 HTTPS 서버 인증서는 이제 3년 후에 자동으로 만료됩니다. 어플라이언스가 버전 6.3으로 업그레이드하기 전에 생성된 기본 서버 인증서를 사용하는 경우 해당 서버 인증서는 처음 생성된 시점에서 20년 후에 만료됩니다. 기본 HTTPS 서버 인증서를 사용하는 경우 시스템은 이제 이 인증서를 갱신할 수 있는 기능을 제공합니다. 신규/수정된 화면: 시스템 (⚙) > **Configuration(**구성**)** > **HTTPS Certificate(HTTPS** 인증서**)** > **Renew HTTPS Certificate(HTTPS** 인증서 갱신**)** 지원되는 플랫폼: FMC

기능	버전	세부정보
FMC에 대해 CLI 액세스를 활성화 및 비활성화 하는 기능.	6.3	시스템 (⚙) > **Configuration(**구성**)** > **Console Configuration(**콘솔 구성**)**의 **Enable CLI Access(CLI** 액세스 활성화**)**는 FMC 웹 인터페이스에서 관리자가 사용할 수 있는 새 체크 박스입니다. • 선택: SSH를 사용하여 FMC에 로그인하면 CLI에 액세스할 수 있습니다. • 선택 취소: SSH를 사용하여 FMC에 로그인하면 Linux 쉘(shell)에 액세스할 수 있습니다. 이는 새 버전 6.3 설치 뿐만 아니라 이전 릴리스에서 버전 6.3으로 업그레이드 할 때의 기본 상태입니다. 버전 6.3 이전에는 **Console Configuration(**콘솔 구성**)** 페이지에 하나의 설정만 있었으며 물리적 디바이스에만 적용되었습니다. 따라서 가상 FMC에서는 **Console Configuration(**콘솔 구성**)** 페이지를 사용할 수 없었습니다. 이제 이 새로운 옵션의 추가를 통해 **Console Configuration(**콘솔 구성**)** 페이지가 물리적 디바이스 및 가상 FMC 모두에 나타납니다. 하지만 가상 FMC의 경우 이 체크 박스만 페이지에 나타납니다. 지원되는 플랫폼: FMC



4 장

Management Center의

management center에는 웹 및 CLI 액세스에 필요한 기본 관리자 계정이 포함되어 있습니다. 이 장에서는 맞춤형 사용자 계정을 생성하는 방법을 설명합니다. Management Center에 로그인, 29 페이지의 내용을 참조하여 management center에 사용자 계정으로 로그인하는 방법을 자세히 알아보십시오.

사용자 정보

매니지드 디바이스에서 맞춤형 사용자 계정을 내부 사용자로 추가할 수 있으며, LDAP 또는 RADIUS 서버에 외부 사용자로 추가할 수 있습니다. 매니지드 디바이스 각각은 별도 사용자 계정을 유지 관리합니다. 예를 들어 사용자를 management center에 추가하는 경우, 해당 사용자만 management center에 액세스할 수 있습니다. 해당 사용자 이름을 사용해 매니지드 디바이스에 직접 로그인할 수 없습니다. 매니지드 디바이스에서 사용자를 별도로 추가해야 합니다.

내부 및 외부 사용자

매니지드 디바이스는 두 가지 유형의 사용자를 지원합니다.

- 내부 사용자—디바이스는 사용자 인증을 위해 로컬 데이터베이스를 검사합니다.
- 외부 사용자—사용자가 로컬 데이터베이스에 없는 경우, 시스템이 외부 LDAP 또는 RADIUS 인증 서버에 쿼리합니다.

웹 인터페이스 및 CLI 액세스

management center에는 웹 인터페이스, CLI(콘솔 (시리얼 포트 또는 키보드 및 모니터)에서 액세스하거나 SSH를 사용하여 관리 인터페이스에 액세스할 수 있음) 및 Linux 셸이 있습니다. 관리 UI에 대한 자세한 내용은 Firepower System 유저 인터페이스, 31 페이지을 참조하십시오.

FMC 사용자 유형 및 액세스 가능한 UI에 대한 다음 정보를 참조하십시오.

- 관리 사용자 - management center은 두 개의 서로 다른 내부 관리자 사용자를 지원합니다. 하나는 웹 인터페이스용이며 다른 하나는 CLI 액세스용입니다. 시스템 초기화 프로세스에서 두 관리자 계정의 비밀번호를 동기화하기 때문에 처음에는 두 계정이 동일하지만, 서로 다른 내부 메커니즘을 이용해 추적하며 초기 구성 후에 달라질 수 있습니다. 시스템 초기화에 관한 자세한 내용은 모델에 맞는 시작 가이드를 참조하십시오. (웹 인터페이스 관리자의 암호를 변경하려면 시스템 (⚙) > **Users(**사용자**)** > **Users(**사용자**)**를 사용합니다. CLI 관리자의 암호를 변경하려면, management center CLI 명령 **configure password**을 사용합니다.)
- 내부 사용자 - 웹 인터페이스에 추가된 내부 사용자는 웹 인터페이스 액세스만 할 수 있습니다.
- 외부 사용자 - 외부 사용자가 웹 인터페이스에 액세스할 수 있으며, 선택적으로 CLI 액세스를 구성할 수 있습니다.
- SSO 사용자 - SSO 사용자는 웹 인터페이스 액세스만 가능합니다.

⚠

주의 CLI 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스할 수 있습니다. Cisco TAC가 지시하거나 management center 설명서에서 명시적으로 지시하지 않는 한, Linux 셸은 사용하지 않는 것이 좋습니다. CLI 사용자는 Linux 셸에서 `sudoers` 권한을 얻을 수 있으며 이로 인해 보안 위험이 발생됩니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- CLI 액세스 권한이 있는 외부 사용자 목록을 적절하게 제한해야 합니다.
- Linux 셸에서 바로 사용자를 추가하지 마십시오. 이 장에서 설명하는 절차만 사용해야 합니다.

사용자 역할

CLI 사용자 역할

management center의 CLI 외부 사용자는 사용자 역할이 없습니다. CLI 사용자는 사용 가능한 명령을 모두 사용할 수 있습니다.

웹 인터페이스 사용자 역할

사용자 권한은 할당된 사용자 역할을 기반으로 합니다. 예를 들어, 분석가에게 Security Analyst(보안 분석가) 및 Discovery Admin(검색 관리자) 같은 사전 정의된 역할을 부여하고 디바이스를 관리하는 보안 관리자를 위해 Admin(관리자) 역할을 남겨둘 수 있습니다. 조직의 요구 사항에 부합하는 액세스 권한을 가진 맞춤형 사용자 역할을 생성할 수도 있습니다.

management center는 다음의 사전 정의된 사용자 역할을 포함합니다.

참고 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 사전 정의된 사용자 역할은 시스템 (⚙) > **Users(**사용자**)** > **Users(**사용자**)** 및 시스템 (⚙) > **Users(**사용자**)** > **User Roles(**사용자 역할**)**의 역할 이름에 **(**읽기 전용**)**이라고 표시됩니다. 사용자 역할의 역할 이름에 **(**읽기 전용**)**이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다. 동시 세션 제한에 대해 알아보려면 사용자 구성, 106 페이지의 내용을 참고하십시오.

액세스 관리자

Policies(정책**)** 메뉴에서 액세스 제어 정책 및 관련된 기능에 대한 액세스를 제공합니다. 액세스 관리자는 정책을 구축할 수 없습니다.

관리자

관리자는 제품의 모든 항목에 액세스할 수 있습니다. 해당 세션은 보안 침해 시 더 심각한 위험을 초래하므로 로그인 세션 시간 초과에서 면제할 수 없습니다.

관리자 역할의 사용은 보안을 위해 필요한 경우로 제한해야 합니다.

검색 관리자

Policies(정책**)** 메뉴에서 네트워크 검색, 애플리케이션 탐지 및 상관 관계 기능에 대한 액세스를 제공합니다. 검색 관리자는 정책을 구축할 수 없습니다.

외부 데이터베이스 사용자**(**읽기 전용**)**

JDBC SSL 연결을 지원하는 애플리케이션을 사용하여 데이터베이스에 읽기 전용 액세스를 제공합니다. 타사 애플리케이션으로 어플라이언스를 인증하려면 시스템 설정에서 데이터베이스 액세스를 활성화해야 합니다. 외부 데이터베이스 사용자는 웹 인터페이스에서 **Help(**도움말**)** 메뉴의 온라인 도움말 관련 옵션에만 액세스할 수 있습니다. 이 역할의 기능이 웹 인터페이스와 무관하므로 용이한 지원 및 비밀번호 변경에 대한 액세스만 제공됩니다.

침입 관리자

Policies(정책**)** 및 **Objects(**개체**)** 메뉴에서 모든 침입 정책, 침입 규칙 및 네트워크 분석 정책 기능에 대한 액세스를 제공합니다. 침입 관리자는 정책을 구축할 수 없습니다.

유지 보수 사용자

모니터링 및 유지 보수 기능에 대한 액세스를 제공합니다. 유지 보수 사용자는 **Health(**상태**)** 및 **System(**시스템**)** 메뉴에서 유지 보수 관련 옵션에 액세스할 수 있습니다.

네트워크 관리자

Policies(정책**)** 메뉴에서 액세스 제어, SSL 검사, DNS 정책 및 ID 정책 기능에 대한 액세스를 비롯해 **Devices(**디바이스**)** 메뉴에서 디바이스 구성 기능에 대한 액세스도 제공합니다. 네트워크 관리자는 디바이스에 구성 변경 사항을 구축할 수 있습니다.

보안 분석가

Overview(개요**)**, **Analysis(**분석**)**, **Health(**상태**)** 및 **System(**시스템**)** 메뉴에서 보안 이벤트 분석 기능에 대한 액세스와 상태 이벤트에 대한 읽기 전용 액세스를 제공합니다.

보안 분석가**(**읽기 전용**)**

Overview(개요**)**, **Analysis(**분석**)**, **Health(**상태**)** 및 **System(**시스템**)** 메뉴에서 보안 이벤트 분석 기능과 상태 이벤트 기능에 대한 읽기 전용 액세스를 제공합니다.

이 역할의 사용자는 다음 작업도 수행할 수 있습니다.

- 특정 디바이스에 대한 상태 모니터 페이지에서 문제 해결 파일을 생성하고 다운로드합니다.
- 사용자 기본 설정에서 파일 다운로드 기본 설정을 지정합니다.
- 사용자 기본 설정에서 이벤트 로그 보기의 기본 기간을 설정합니다**(Audit Log Time Window(**감사 로그 시간 기간**)** 제외).

보안 승인자

Policies(정책**)** 메뉴에서 액세스 제어 및 관련된 정책과 네트워크 검색 정책에 대한 제한된 액세스를 제공합니다. 보안 승인자는 이러한 정책을 확인하고 구축할 수 있지만 정책을 변경할 수는 없습니다.

TID(Threat Intelligence Director) 사용자

Intelligence(인텔리전스**)** 메뉴에서 Threat Intelligence Director 구성에 대한 액세스를 제공합니다. TID(Threat Intelligence Director) 사용자는 TID를 확인하고 구성할 수 있습니다.

사용자 암호

다음 규칙은 LOM(Lights-Out Management)을 사용하거나 사용하지 않도록 설정한 management center의 내부 사용자 계정에 대한 비밀번호에 적용됩니다. 외부에서 인증한 계정이나 보안 인증 규정 준수를 활성화한 시스템에서는 다른 비밀번호 요구 사항이 적용됩니다. 자세한 내용은 Management Center에 대한 외부 인증 구성, 126 페이지 및 보안 인증서 컴플라이언스, 335 페이지를 참고하십시오.

management center 초기 설정에서, 시스템은 관리자 사용자에게 아래 테이블에서 설명하는 강력한 비밀번호 요구 사항을 준수하는 계정 비밀번호를 설정하도록 요구합니다. 물리적 management center의 경우 LOM이 활성화된 강력한 비밀번호 요건이 사용되며, 가상 Management Center의 경우 LOM이 활성화되지 않은 강력한 비밀번호 요건이 사용됩니다. 이때 시스템은 웹 인터페이스 관리자와 CLI 액세스 관리자의 비밀번호를 동기화합니다. 초기 구성이 끝나면 웹 인터페이스 관리자는 강력한 비밀번호 요구 사항을 제거할 수 있지만, CLI 액세스 관리자는 LOM이 활성화되지 않은 강력한 비밀번호 요구사항을 준수해야 합니다.

	LOM 활성화되지 않음	**LOM** 활성화
비밀번호 강도 확인 설정	비밀번호는 다음을 포함해야 합니다. • 최소 8자 또는 관리자가 사용자에 대해 설정한 문자 수 중 더 긴 값 • 반복되는 문자 2개 미만 • 소문자 1개 이상 • 대문자 1개 이상 • 하나 이상의 숫자가 필요합니다. • 특수문자 1개 이상(! @ # * - _ + 등) 시스템은 영어사전에 실린 수많은 단어는 물론 일반적인 비밀번호 해킹 기법으로 쉽게 해독할 수 있는 문자열을 포함하는 특수한 사전을 이용해 비밀번호를 검사합니다.	비밀번호는 다음을 포함해야 합니다. • 8~20개 사이의 문자(MC 1000, MC 2500, MC 4500의 경우 상한은 20자가 아닌 14자입니다.) • 반복되는 문자 2개 미만 • 소문자 1개 이상 • 대문자 1개 이상 • 하나 이상의 숫자가 필요합니다. • 특수문자 1개 이상(! @ # * - _ + 등) 특수 문자 규칙은 물리적 management center 시리즈에 따라 다릅니다. 아래 마지막 글머리 기호에 나열된 특수 문자만 선택하는 방법을 권장합니다. 비밀번호에는 사용자 이름을 포함하지 마십시오. 시스템은 영어사전에 실린 수많은 단어는 물론 일반적인 비밀번호 해킹 기법으로 쉽게 해독할 수 있는 문자열을 포함하는 특수한 사전을 이용해 비밀번호를 검사합니다.

	LOM 활성화되지 않음	LOM 활성화

비밀번호 강도 확인 해제	비밀번호는 관리자가 사용자에 대해 설정한 최소 문자 수 이상을 포함해야 합니다. (자세한 내용은 내부 사용자 추가, 123 페이지의 내용을 참조하십시오.)	비밀번호는 다음을 포함해야 합니다.
		• 8~20개 사이의 문자(MC 1000, MC 2500, MC 4500의 경우 상한은 20자가 아닌 14자입니다.)
		• 다음 4개 범주 중 3개 이상의 문자:
		  • 대문자
		  • 소문자
		  • 숫자
		  • 특수 문자(! @ # * - _ + 등)
		특수 문자 규칙은 물리적 management center 시리즈에 따라 다릅니다. 아래 마지막 글머리 기호에 나열된 특수 문자만 선택하는 방법을 권장합니다.
		비밀번호에는 사용자 이름을 포함하지 마십시오.

Management Center용 사용자 계정 지침 및 제한 사항

- management center는 모든 형태의 액세스에 대해 로컬 사용자 계정으로 관리자 사용자를 포함합니다. 관리자 사용자를 삭제할 수 없습니다. 기본 초기 비밀번호는 **Admin123**입니다. 시스템은 초기화 프로세스 중에 비밀번호를 변경하게 합니다. 시스템 초기화에 관한 자세한 내용은 모델에 맞는 시작 가이드를 참조하십시오.
- 기본적으로 다음 설정이 management center의 모든 사용자 계정에 적용됩니다.
  - 비밀번호 재사용에는 제한이 없습니다.
  - 시스템은 성공한 로그인을 추적하지 않습니다.
  - 시스템에서 잘못된 로그인 크리덴셜을 입력한 사용자에 대해 시간이 정해진 임시 잠금을 강제 적용하지 않습니다.
  - 동시에 열 수 있는 읽기 전용 및 읽기/쓰기 세션 수에 대한 사용자 정의 제한은 없습니다.

  모든 사용자에 대한 이러한 설정을 시스템 구성으로 변경할 수 있습니다. (시스템 (⚙) > **Configuration**(구성) > **User Configuration**(사용자 구성)) 사용자 구성, 106 페이지 참조.
- 초기 설정에서 사용자에게 기본 액세스 역할을 할당할 때는 최소 권한 원칙을 따라야 합니다. 사용자가 크리덴셜로 처음 시스템에 로그인하면 해당 계정에 이 기본 액세스 역할이 할당됩니다. 기본 액세스 역할은 누구나 시스템에 로그인하는 데 필요한 가능한 가장 낮은 권한으로 설정하

는 것이 좋습니다. 예를 들어 일반 사용자에게 기본 액세스 역할로 보안 분석가(읽기 전용) 역할을 부여할 수 있으며, 관리자를 별도의 관리자 그룹에 추가하여 전체 관리자 권한을 부여할 수 있습니다. 기본 액세스 역할을 할당할 때 최소 권한 원칙을 따르지 않는 경우 후속 로그인 시 사용자에게 의도하지 않은 권한 수준이 할당될 수 있습니다. 그러면 사용자가 필요한 액세스 역할 이상의 권한을 갖게 될 수 있습니다. 이 지침은 모든 사용자(내부 사용자, 외부 사용자 또는 CAC 사용자)에게 적용됩니다.

기본 액세스 역할로 로그인한 사용자가 권한을 일시적으로 승격해야 하는 경우, 관리 권한이 있는 사용자는 더 높은 권한을 가진 역할을 할당하여 해당 사용자에게 필요한 더 높은 액세스 레벨을 일시적으로 제공할 수 있습니다. 이 권한은 24시간 동안 활동이 없으면 취소되며, 사용자는 기본 액세스 역할로 돌아갑니다.

사용자가 시스템 관리자와 같은 더 높은 권한 레벨에 영구적으로 액세스 역할을 재할당해야 하는 경우, 그룹 제어 액세스 역할 방법을 통해 사용자에게 관리자 액세스 권한을 제공합니다. 이 방법을 사용하면 제공된 액세스 역할이 24시간 이상 유지되며, 사용자는 그룹 할당에 따라 올바른 권한 레벨을 갖습니다. Group Controlled Access Roles(그룹 제어 액세스 역할) 구성에 대한 자세한 내용은 단계 13 섹션을 참고하십시오.

FMC 사용자 계정 요구 사항 및 사전 요건

모델 지원

Management Center

지원되는 도메인

- SSO 구성 - 전역 전용.
- 기타 모든 기능 - 모두.

사용자 역할

- SSO 구성 - 내부 또는 LDAP 또는 RADIUS에 의해 인증된 관리자 역할의 사용자만 SSO를 설정할 수 있습니다.
- 기타 모든 기능 - 관리자 역할의 모든 사용자
- LADP로 CAC(Common Access Card) 인증 구성, 143 페이지에서는 네트워크 관리자 역할도 지원합니다.

내부 사용자 추가

이 절차에서는 management center에 대한 사용자 지정 내부 사용자 계정을 추가하는 방법을 설명합니다.

System(시스템**)** > **Users(**사용자**)** > **Users(**사용자**)**에는 사용자가 LDAP 또는 RADIUS 인증을 통해 로그인할 때 수동으로 추가한 내부 사용자와 자동으로 추가된 외부 사용자가 모두 표시됩니다. 외부 사용자의 경우 더 높은 권한이 있는 역할을 할당하면 이 화면에서 사용자 역할을 수정할 수 있지만 비밀번호 설정은 수정할 수 없습니다.

management center의 다중 도메인 구축에서 사용자는 생성된 도메인에서만 표시될 수 있습니다. 글로벌 도메인에서 사용자를 추가한 다음, 리프 도메인에 사용자 역할을 할당하는 경우 사용자가 리프 도메인에 "속하는" 경우에도 해당 사용자는 추가된 전역 **Users(**사용자**)** 페이지에 계속해서 표시됩니다.

디바이스에서 보안 인증 컴플라이언스 또는 LOM(Lights-Out Management)을 활성화하면 다른 비밀번호 제한이 적용됩니다. 보안 인증 컴플라이언스에 대한 자세한 내용은 보안 인증서 컴플라이언스, 335 페이지의 내용을 참조하십시오.

리프 도메인에서 사용자를 추가하면 해당 사용자는 글로벌 도메인에서 표시되지 않습니다.

참고 여러 관리자 사용자가 동시에 management center에서 새 사용자를 생성하지 않도록 하십시오. 사용자 데이터베이스 액세스 충돌로 인해 오류가 발생할 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Users(**사용자**)**을 선택합니다.

단계 **2** **Create User**(사용자 생성)를 클릭합니다.

단계 **3** **User Name(**사용자 이름**)**을 입력합니다.

사용자 이름은 다음 제한 사항을 준수해야 합니다.

- 최대 32개의 영문숫자 문자와 하이픈(-) 및 밑줄 표시(_)로 구성해야 합니다.
- 문자는 대문자 또는 소문자일 수 있습니다.
- 마침표(.), 하이픈(-), 밑줄 표시(_) 이외의 특수 문자 또는 문장 부호를 포함할 수 없습니다.

단계 **4** **Real Name(**실명**)**: 계정이 속한 사용자 또는 부서를 식별하기 위한 설명 정보를 입력합니다.

단계 **5** **Use External Authentication Method(**외부 인증 방법 사용**)** 확인란은 LDAP 또는 RADIUS를 통해 로그인할 때 자동으로 추가된 사용자를 대상으로 확인됩니다. 외부 사용자를 사전 구성할 필요가 없으므로 이 필드를 무시할 수 있습니다. 외부 사용자의 경우 확인란을 선택 취소하여 이 사용자를 내부 사용자로 되돌릴 수 있습니다.

단계 **6** **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 값을 입력합니다.

값은 이 사용자에게 설정한 비밀번호 옵션을 준수해야 합니다.

단계 **7** **Maximum Number of Failed Logins(**최대 실패 로그인 시도 횟수**)**를 설정합니다.

공백 없이 정수를 입력하여 각 사용자가 로그인에 실패한 후 어카운트가 잠길 때까지 로그인을 시도할 수 있는 최대 횟수를 지정합니다. 기본 설정은 5회입니다. **0**을 사용하면 로그인 실패 횟수의 제한

이 사라집니다. 관리자 어카운트는 보안 인증 컴플라이언스를 활성화한 경우를 제외하고 실패한 로그인의 최대 수 이후에 잠금에서 제외됩니다.

단계 **8** **Minimum Password Length(**최소 비밀번호 길이**)**를 설정합니다.

공백 없이 정수를 입력하여 사용자 비밀번호의 최소 길이를 글자 수로 지정합니다. 기본 설정은 **8**입니다. 값이 **0**이면 최소 길이 제한이 없습니다.

단계 **9** **Days Until Password Expiration(**비밀번호 만료 시까지의 일수**)**을 설정합니다.

여기에 입력한 일수가 지나면 사용자의 비밀번호가 만료됩니다. 기본 설정은 **0**이며, 이렇게 하면 비밀번호가 만료되지 않습니다. 기본값에서 변경하는 경우, 사용자 목록의 **Password Lifetime(**비밀번호 수명**)** 열에는 각 사용자의 비밀번호에서 남아 있는 일수가 나타납니다.

단계 **10** **Days Before Password Expiration Warning(**비밀번호 만료 경고까지 남은 일수**)**을 설정합니다.

비밀번호가 만료되기 전에 사용자에게 비밀번호를 변경하게 하는 경고 일수를 입력합니다. 기본 설정은 **0**일입니다.

단계 **11** 사용자 **Options(**옵션**)**를 설정합니다.

- **Force Password Reset on Login(**로그인 시 비밀번호 재설정 강제 실행**)** - 사용자가 다음에 로그인할 때 비밀번호를 변경하도록 강제 실행합니다.
- **Check Password Strength(**비밀번호 보안 수준 확인**)** - 강력한 비밀번호가 필요합니다. 비밀번호 강도 확인을 활성화하면, 비밀번호는 사용자 암호, 120 페이지에서 설명하는 강력한 비밀번호 요구 사항을 준수해야 합니다.
- **Exempt from Browser Session Timeout(**브라우저 세션 시간 초과에서 제외**)** - 사용자의 로그인 세션이 비활성화로 인한 종료에서 제외됩니다. 관리자 역할의 사용자는 면제받을 수 없습니다.

단계 **12** **User Role Configuration(**사용자 역할 구성**)** 영역에서 사용자 역할을 할당합니다. 사용자 역할에 대한 자세한 내용은 웹 인터페이스의 사용자 역할 맞춤화, 201 페이지의 내용을 참조하십시오.

외부 사용자의 경우, 사용자 역할이 그룹 구성원 자격(LDAP)을 통해 할당되거나 사용자 속성(RADIUS)을 기반으로 할당되면 최소 액세스 권한을 제거할 수 없습니다. 단, 추가 권한은 할당할 수 있습니다. 사용자 역할이 디바이스에서 설정하는 기본 사용자 역할인 경우, 제한 없이 사용자 어카운트에서 역할을 수정할 수 있습니다. 사용자 역할을 수정하는 경우 **Users(**사용자**)** 탭의 **Authentication Method(**인증 방법**)** 열에 **External - Locally Modified(**외부 - 로컬로 수정됨**)** 상태가 나타납니다.

표시되는 옵션은 디바이스가 단일 도메인 또는 다중 도메인 구축에 있는지 여부에 따라 달라집니다.

- 단일 도메인 - 사용자를 할당할 사용자 역할을 선택합니다.
- 다중 도메인 — 다중 도메인 구축에서 관리자 액세스 권한이 할당된 모든 도메인에서 사용자 계정을 생성할 수 있습니다. 사용자는 각 도메인에서 다른 권한을 가질 수 있습니다. 상위 도메인 및 하위 도메인 모두에서 사용자 역할을 할당할 수 있습니다. 예를 들어 글로벌 도메인에서 사용자에게 읽기 전용 권한을 할당할 수 있지만 하위 도메인에서는 관리자 권한을 할당할 수 있습니다. 다음 단계를 참조하십시오.

  1. **Add Domain(**도메인 추가**)**을 클릭합니다.
  2. **Domain(**도메인**)** 드롭다운 목록에서 도메인을 선택합니다.

3. 사용자를 할당할 사용자 역할을 선택합니다.
4. **Save(**저장**)**를 클릭합니다.

단계 **13** (선택 사항, 물리적 management center의 경우에만 해당됨) 사용자에게 관리자 역할을 할당한 경우, 관리자 옵션이 나타납니다. **Allow Lights-Out Management Access(Lights-Out Management** 액세스 허용**)**를 선택하여 사용자에게 Lights-Out Management 액세스 권한을 부여할 수 있습니다. Lights-Out Management에 대한 자세한 내용은 LOM(Lights-Out Management) 개요, 93 페이지의 내용을 참조하십시오.

단계 **14** **Save(**저장**)**를 클릭합니다.

Management Center에 대한 외부 인증 구성

외부 인증을 활성화하려면 하나 이상의 외부 인증 개체를 추가해야 합니다.

Management Center에 대한 외부 인증 정보

외부 인증을 활성화하는 경우, 외부 인증 개체에 지정된 대로 management center에서 LDAP 또는 RADIUS 서버로 사용자 자격 증명을 확인합니다.

웹 인터페이스 액세스를 위한 여러 외부 인증 개체를 구성할 수 있습니다. 예를 들어 외부 인증 개체가 5개인 경우, 그러한 개체에서 사용자는 웹 인터페이스 액세스를 인증받을 수 있습니다. CLI 액세스는 외부 인증 개체를 하나만 사용할 수 있습니다. 외부 인증 개체를 하나 이상 활성화하는 경우, 사용자는 목록에서 첫 번째 개체로만 인증할 수 있습니다.

외부 인증 개체는 management center 및 threat defense 디바이스가 사용할 수 있습니다. 다양한 어플라이언스/디바이스 유형 간에 동일한 개체를 공유하거나 별도 개체를 생성할 수 있습니다.

참고 시간 제한 범위는 threat defense와 management center가 다르므로 개체를 공유할 때는 threat defense의 더 적은 시간 제한 범위(LDAP의 경우 1~30초, RADIUS의 경우 1~300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 threat defense 외부 인증 설정이 작동하지 않습니다.

management center의 경우, 외부 인증 객체를 **System(**시스템**)** > **User(**사용자**)** > **External Authentication(**외부 인증**)** 탭에서 직접 활성화합니다. 이 설정은 management center 사용에만 영향을 주며 매니지드 디바이스 사용에 대해 이 탭에서 활성화할 필요는 없습니다. threat defense 디바이스의 경우, 디바이스에 구축하는 플랫폼 설정에서 외부 인증 객체를 활성화해야 합니다.

웹 인터페이스 사용자는 내부 인증 개체에 있는 CLI 사용자와 별개로 정의됩니다. RADIUS의 CLI 사용자의 경우, 외부 인증 개체의 RADIUS 사용자 이름목록을 사전 구성해야 합니다. LDAP의 경우, 필터를 지정하여 LDAP 서버의 CLI 사용자와 매칭할 수 있습니다.

CAC 인증을 위해 구성된 CLI 액세스를 위한 LDAP 개체를 사용할 수 없습니다.

참고 CLI 액세스 권한이 있는 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스할 수 있습니다. Linux 셸 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 다음을 확인하십시오.

- CLI 또는 Linux 셸 액세스 권한이 있는 사용자 목록 제한
- Linux 셸 사용자를 생성하지 마십시오.

LDAP 정보

LDAP(Lightweight Directory Access Protocol)를 사용하면 중앙의 한 위치에 개체(예: 사용자 크리덴셜)를 조직하는 네트워크에서 디렉토리를 설정할 수 있습니다. 그러면 여러 애플리케이션에서 이 크리덴셜 및 크리덴셜 설명에 사용된 정보에 액세스할 수 있습니다. 사용자 크리덴셜을 변경해야 하는 경우, 한 곳에서 변경할 수 있습니다.

Microsoft는 Active Directory 서버가 2020년에 LDAP 바인딩 및 LDAP 서명을 시행할 것이라고 발표했습니다. Microsoft는 이러한 설정을 기본 설정으로 사용할 때 Microsoft Windows에 권한 상승 취약점이 존재하여 MITM(man-in-the-middle) 공격자가 Windows LDAP 서버에 인증 요청을 성공적으로 전달할 수 있기 때문에 이러한 요구 사항을 적용하고 있습니다. 자세한 내용은 Microsoft 지원 사이트에서 2020 LDAP 채널 바인딩 및 Windows용 LDAP 서명 요구 사항을 참조하십시오.

아직 수행하지 않은 경우 TLS/SSL 암호화를 사용하여 Active Directory 서버에서 인증을 시작하는 것이 좋습니다.

RADIUS 정보

RADIUS(Remote Authentication Dial In User Service)는 네트워크 리소스에 대한 사용자 액세스의 인증, 권한 부여, 어카운팅에 사용되는 인증 프로토콜입니다. RFC 2865를 준수하는 모든 RADIUS 서버에 대해 인증 개체를 생성할 수 있습니다.

Firepower 디바이스는 SecurID 토큰 사용을 지원합니다. SecurID를 사용하여 서버에서 인증을 구성하는 경우, 해당 서버에서 인증된 사용자는 SecurID PIN 끝에 SecurID 토큰을 추가하고 이를 로그인 비밀번호로 사용합니다. SecurID를 지원하기 위해 Firepower 디바이스에서 추가로 구성할 사항은 없습니다.

Management Center에 대한 LDAP 외부 인증 개체 추가

LDAP 서버를 추가하고 디바이스 관리를 위해 외부 사용자를 지원합니다.

다중 도메인 구축에서 외부 인증 개체는 생성된 도메인에서만 사용할 수 있습니다.

시작하기 전에

- 해당 장치에서 도메인 이름 조회를 위해 DNS 서버를 지정해야 합니다. 이 절차에서 IP 주소는 지정하고 LDAP 서버에 대한 호스트 이름은 지정하지 않더라도, LDAP 서버는 인증을 위한 URI를 반환할 수 있으며 여기에는 호스트 이름이 포함됩니다. 호스트 이름을 지정하려면 DNS 조회가

필요합니다. Management Center 관리 인터페이스 수정, 82 페이지를 참조하고 DNS 서버를 추가합니다.

- CAC 인증과 함께 사용할 LDAP 인증 개체를 구성하는 경우 컴퓨터에 삽입된 AC를 제거해서는 안 됩니다. 사용자 인증서를 활성화한 다음에는 항상 CAC가 삽입된 상태여야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Users(**사용자**)**을 선택합니다.

단계 **2** **External Authentication(**외부 인증**)** 탭을 클릭합니다.

단계 **3** 아이콘 추가(➕)**Add External Authentication Object(**외부 인증 개체 추가**)**를 클릭합니다.

단계 **4** **Authentication Method(**인증 방법**)**을 **LDAP**로 설정합니다.

단계 **5** (선택 사항) CAC 인증 및 권한 부여에 이 인증 개체를 사용하려는 경우 **CAC** 확인란을 선택할 수도 있습니다.

CAC 인증 및 권한 부여를 전부 구성하려면 LADP로 CAC(Common Access Card) 인증 구성, 143 페이지에 있는 절차를 따라야 합니다. 이 개체는 CLI 사용자에게는 사용할 수 없습니다.

단계 **6** **Name(**이름**)**과 **Description(**설명**)**(선택 사항)을 입력합니다.

단계 **7** 드롭다운 목록에서 **Server Type(**서버 유형**)**을 선택합니다.

팁 **Set Defaults(**기본 설정**)**을 클릭하면 디바이스가 **User Name Template(**사용자 이름 템플릿**)**, **UI Access Attribute(UI** 액세스 속성**)**, **CLI Access Attribute(CLI** 액세스 속성**)**, **Group Member Attribute(**그룹 구성원 속성**)** 및 **Group Member URL Attribute(**그룹 구성원 **URL** 속성**)** 필드를 서버 유형의 기본값으로 채웁니다.

단계 **8** **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 일치해야 합니다. 또한 IPv6 주소는 암호화된 연결이 지원되지 않습니다.

단계 **9** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 **10** (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

단계 **11** **LDAP-Specific Parameters(LDAP** 전용 파라미터**)**를 입력합니다.

a) 액세스를 원하는 LDAP 디렉터리에 대해 **Base DNs(**기본 **DN)**를 입력합니다. 예를 들어, 예시 회사의 보안 조직에서 이름을 인증하려면 `ou=security,dc=example,dc=com`을 입력합니다. 아니면 **Fetch DN(DN** 가져오기**)**을 클릭하고, 드롭다운 목록에서 적절한 기본 고유 이름을 선택합니다.

b) (선택 사항) **Base Filter(**기본 필터**)**를 입력합니다. 예를 들어 디렉토리 트리의 사용자 개체에 `physicalDeliveryOfficeName` 속성이 있고 뉴욕 사무실의 사용자는 그 속성 값이 `NewYork`인 경우 뉴욕 사무실의 사용자만 가져오려면 `(physicalDeliveryOfficeName=NewYork)`이라고 입력합니다.

CAC 인증을 사용하는 경우 활성 사용자 계정만 필터링하려면(비활성화된 사용자 계정 제외) `(!(userAccountControl:1.2.840.113556.1.4.803:=2))`를 입력합니다. 이 기준은 `ldpgrp` 그룹에 속하는 AD 내에서 사용자 계정을 검색하며 `userAccountControl` 속성 값이 `2`(비활성화됨)가 아닙니다.

c) LDAP 서버를 검색하기에 크리덴셜이 충분한 사용자의 경우, **User Name(**사용자 이름**)**을 입력합니다. 예를 들어 OpenLDAP 서버에 연결하려는 경우, 해당 사용자 개체에 `uid` 속성이 있으며 예시 회사 보안 부서 관리자 개체의 `uid`값이 `NetworkAdmin`이라면 `uid=NetworkAdmin,ou=security,dc=example,dc=com`과 같이 입력할 수 있습니다.

d) **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 사용자 비밀번호를 입력합니다.

e) (선택 사항) **Show Advanced Options(**고급 옵션 표시**)**를 클릭하고 다음 고급 옵션을 구성합니다.

- **Encryption(**암호화**)- None (**해당 없음**)**, **TLS**또는 **SSL**을 클릭 합니다.

  포트를 지정한 다음 암호화 방식을 변경할 경우, 그 방법에 대해서는 포트가 기본값으로 재설정됩니다. **None(**해당 없음**)** 또는 **TLS**인 경우, 포트는 기본값인 389로 재설정됩니다. SSL 암호화를 선택할 경우 포트는 636로 재설정됩니다.

- **SSL Certificate Upload Path(SSL** 인증서 업로드 경로**)**—SSL 또는 TLS 암호화인 경우, **Choose File(**파일 선택**)**을 클릭하여 인증서를 선택해야 합니다.

  이전에 업로드한 인증서를 대체하려는 경우, 새 인증서를 업로드하고 구성을 디바이스에 다시 적용하여 새 인증서로 복사합니다.

  참고 TLS 암호화는 모든 플랫폼에서 인증서가 필요합니다. 항상 끼어들기 공격을 방지하기 위해 SSL에 대한 인증서를 업로드하는 것이 좋습니다.

- **User Name Template(**사용자 이름 템플릿**)**— **UI Access Attribute(UI** 액세스 속성**)**에 해당하는 템플릿을 제공합니다. 예를 들어 예시 회사의 보안 조직에서 근무하는 모든 사용자를 인증하기 위해 UI 액세스 속성이 `uid`인 OpenLDP 서버에 연결하는 경우, `uid=%s,ou=security,dc=example,dc=com`를 **User Name Template(**사용자 이름 템플릿**)** 필드에 입력합니다. Microsoft Active Directory 서버에서는 `%s@security.example.com`이라고 입력할 수 있습니다.

  이 필드는 CAC 인증을 위해 필요합니다.

- **Shell User Name Template(**쉘 사용자 이름 템플릿**)**— CLI 사용자 인증을 위해 **CLI Access Attribute(CLI** 액세스 속성**)**에 해당하는 템플릿을 제공합니다. 예를 들어 보안 조직에서 근무하는 모든 사용자를 인증하기 위해 CLI 액세스 속성이 `sAMAccountName`인 OpenLDP 서버에 연결하는 경우, `%s`를 **Shell User Name Template(**쉘 사용자 이름 템플릿**)** 필드에 입력합니다.

- **Timeout(Seconds)(**시간 초과**(**초**))** - 백업 연결로 전환하기 전 시간(초)을 1과 1024 사이로 입력합니다. 기본값은 30입니다.

  참고 시간 초과 범위는 threat defense와 management center에 따라 다르므로 개체를 공유하는 경우 threat defense의 더 작은 시간 초과 범위 (1 ~ 30초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 threat defense LDAP 구성이 작동하지 않습니다.

단계 **12** (선택 사항) **Attribute Mapping(**속성 매핑**)**을 구성하고 속성에 따라 사용자를 검색합니다.

- **UI Access Attribute(UI** 액세스 속성**)**을 입력하거나 **Fetch Attrs(**속성 가져오기**)**를 클릭하여 사용 가능한 속성 목록을 검색합니다. 예를 들어 Microsoft Active Directory Server의 경우 Active Directory

Server 사용자 개체에 `uid` 속성이 없기 때문에 UI Access Attribute(UI 액세스 속성)를 사용하여 사용자를 검색할 수도 있습니다. 그 대신 `userPrincipalName` 속성을 검색할 수 있는데, `userPrincipalName`을 **UI Access Attribute(UI** 액세스 속성**)** 필드에 입력하면 됩니다.

이 필드는 CAC 인증을 위해 필요합니다.

- 사용자 고유 유형 이외의 쉘(shell) 액세스 속성을 사용하려는 경우 **CLI Access Attribute(CLI** 액세스 속성**)**를 입력합니다. 예를 들어 `sAMAccountName` CLI 액세스 속성을 사용하여 셸 액세스 사용자를 가져오려면 `sAMAccountName`을 입력합니다.

단계 **13** (선택 사항) **Group Controlled Access Roles(**그룹 제어 액세스 역할**)**를 구성합니다.

액세스 제어 그룹에 역할을 사용하여 사용자의 권한을 구성하지 않는 경우, 사용자는 외부 인증 정책에서 기본적으로 부여된 권한만 갖습니다.

a) (선택 사항) 사용자 역할에 해당하는 필드에 해당 역할이 부여되는 사용자를 포함하는 LDAP 그룹의 DN을 입력합니다.

참조하는 모든 그룹이 LDAP 서버에 있어야 합니다. 고정 LDAP 그룹 또는 동적 LDAP 그룹을 참조할 수 있습니다. 고정 LDAP 그룹은 특정 사용자를 가리키는 그룹 개체 특성에 의해 멤버십이 결정되며, 동적 LDAP 그룹에서는 사용자 개체 특성에 따라 그룹 사용자를 가져오는 LDAP 검색을 생성하여 멤버십을 결정합니다. 어떤 역할에 대한 그룹 액세스 권한은 그룹의 멤버인 사용자에게만 영향을 미칩니다.

동적 그룹을 사용하는 경우 LDAP 서버에 구성된 대로 LDAP 쿼리가 사용됩니다. 이런 이유로 Firepower 디바이스는 검색 반복 횟수를 4회로 제한하여 검색 구문 오류로 인한 무한 루프를 방지합니다.

예제**:**

Administrator(관리자**)** 필드에 다음과 같이 입력하여 예시 회사의 정보 기술 조직에서 이름을 인증할 수 있습니다.

```
cn=itgroup,ou=groups, dc=example,dc=com
```

b) 지정된 어떤 그룹에도 속하지 않는 사용자에 대해 **Default User Role(**기본 사용자 역할**)**을 선택합니다.

c) 정적 그룹을 사용하는 경우, **Group Member Attribute(**그룹 멤버 속성**)**을 입력합니다.

예제**:**

기본 Security Analyst 액세스에 대한 고정 그룹의 멤버십을 표시하기 위해 `member(멤버)` 속성을 사용하는 경우 `member(멤버)`라고 입력합니다.

d) 동적 그룹을 사용하는 경우, **Group Member URL Attribute(**그룹 멤버 **URL** 속성**)**을 입력합니다.

예제**:**

`memberURL` 속성이 기본 관리자 액세스에 대해 지정한 동적 그룹의 멤버를 가져오는 LDAP 검색을 포함할 경우 `memberURL`이라고 입력합니다.

사용자의 역할을 변경하는 경우, 변경된 외부 인증 개체는 저장/배포하고 **Users(**사용자**)** 화면에서 해당 사용자를 제거해야 합니다. 이 사용자는 다음 로그인 시 자동으로 재추가됩니다.

단계 **14** (선택 사항) CLI 사용자를 허용하도록 **CLI Access Filter(CLI** 액세스 필터**)**를 설정합니다.

CLI 액세스에 대해 LDAP 인증을 하지 않으려면 이 필드를 비워 둡니다. CLI 사용자를 지정하려면 다음 방법 중 하나를 선택합니다.

- 인증 설정을 구성할 때 지정한 것과 동일한 필터를 사용하려면 **Same as Base Filter(**기본 필터와 동일**)** 체크 박스를 선택합니다.
- 속성 값에 따라 관리자 사용자 엔트리를 검색하려면 속성 이름, 비교 연산자, 필터로 사용할 속성 값을 괄호로 묶어 입력합니다. 예를 들어 모든 네트워크 관리자에게 `manager` 속성이 있고 그 값이 `shell`이라면 `(manager=shell)`이라는 기본 필터를 설정할 수 있습니다.

사용자 이름은 다음과 같은 Linux 기준을 준수해야 합니다.

- 최대 32개의 영숫자 문자와 마침표(.), 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

참고 CLI 액세스 권한이 있는 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스할 수 있습니다. Linux 셸 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. CLI 또는 Linux 셸 액세스 권한을 갖는 사용자의 목록을 제한해야 합니다.

참고 **CLI Access Filter(CLI** 액세스 필터**)**에 포함된 사용자와 사용자 이름이 동일한 내부 사용자를 만들지 마십시오. 내부 management center 사용자만 관리자여야 합니다. **CLI Access Filter(CLI** 액세스 필터**)**에 관리자를 포함하지 마십시오.

단계 **15** (선택 사항) **Test(**테스트**)**를 클릭하고 LDAP 서버와의 연결을 테스트합니다.

테스트 출력에서는 유효한 사용자 이름과 유효하지 않은 사용자 이름을 나열합니다. 사용자 이름은 고유해야 하며 밑줄(_), 마침표(.), 하이픈(-), 영숫자를 포함할 수 있습니다. 1,000명이 넘는 사용자로 서버와의 연결을 테스트할 경우 UI 페이지 크기 제한 때문에 1,000명의 사용자만 반환됩니다. 테스트에 실패하는 경우 LDAP 인증 연결 문제 해결, 206 페이지을 참조하십시오.

단계 **16** (선택 사항) **Additional Test Parameters(**추가 테스트 파라미터**)**를 입력하고 인증 가능한 사용자의 크리덴셜을 테스트할 수도 있습니다. **User Name(**사용자 이름**)** `uid` 및 **Password(**비밀번호**)**를 입력한 다음 **Test(**테스트**)**를 클릭합니다.

Microsoft Active Directory Server에 연결하는 경우 `uid` 대신 UI 액세스 속성을 제공했다면 해당 속성의 값을 사용자 이름으로 사용합니다. 해당 사용자의 정규화된 DN을 지정할 수도 있습니다.

팁 테스트 사용자의 이름이나 비밀번호를 잘못 입력할 경우 서버 구성이 맞더라도 테스트는 실패합니다. 서버 구성이 올바른지 확인하려면 먼저 **Test(**테스트**)**를 클릭합니다. 여기서 **Additional Test Parameters(**추가 테스트 파라미터**)** 필드에는 사용자 정보를 입력할 필요가 없습니다. 테스트가 성공하면 사용자 이름과 비밀번호를 입력하고 특정 사용자로 테스트하십시오.

예제:

예를 들어 예시 회사의 `JSmith` 사용자 크리덴셜을 가져올 수 있는지 테스트하려면 `JSmith`를 입력하고 올바른 비밀번호를 입력합니다.

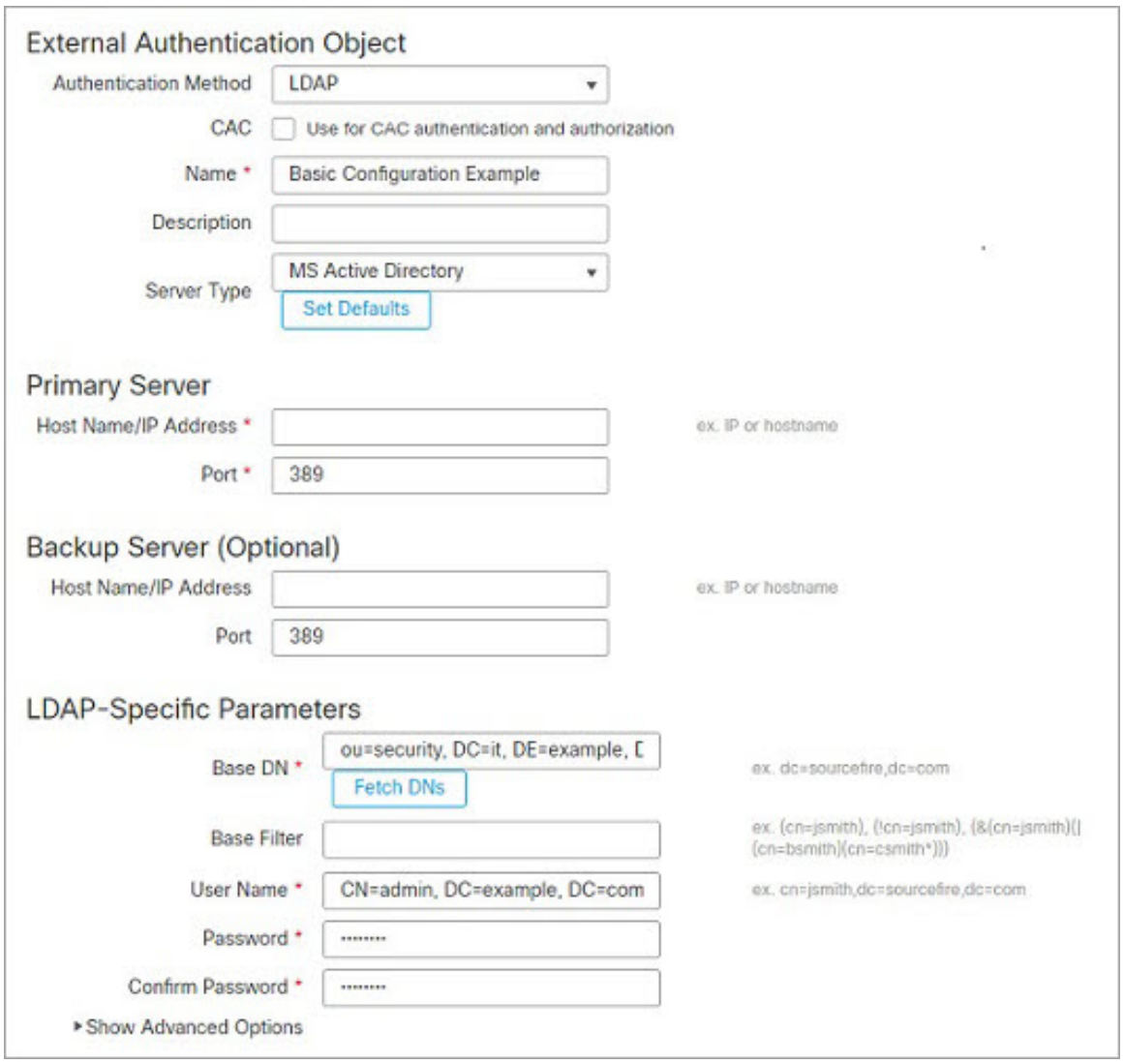
단계 **17** **Save(**저장**)**를 클릭합니다.

단계 **18** 이 서버의 사용을 활성화합니다. Management Center 사용자에 대한 외부 인증 활성화, 142 페이지를 참조하십시오.

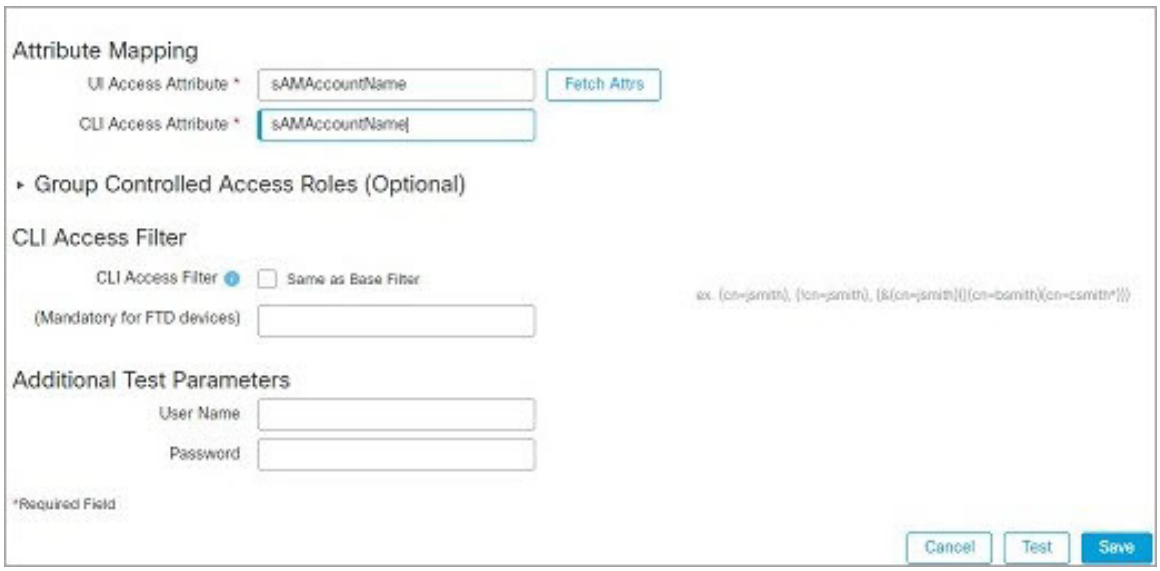
예

기본 예시

다음 그림은 Microsoft Active Directory Server를 위한 LDAP 로그인 인증 개체의 기본 구성입니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 389을 액세스에 사용합니다.



이 예는 예시 회사의 정보 기술 도메인에 있는 보안 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다.



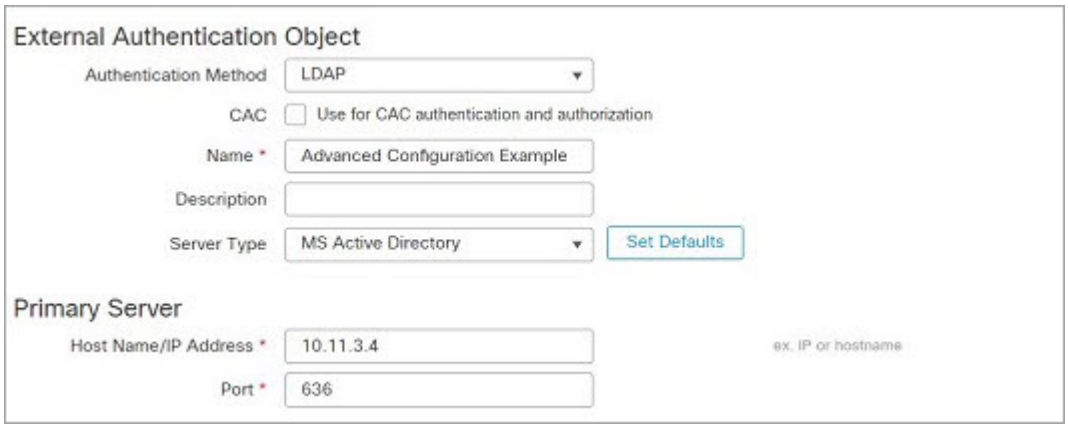
그러나 이 서버는 Microsoft Active Directory Server이므로 `sAMAccountName` 속성을 사용해 사용자 이름을 저장하며 `uid` 속성을 사용하지 않습니다. MS Active Directory Server 유형을 선택하고 **Set Defaults(**기본값 설정**)**을 클릭하면 UI Access Attribute(UI 액세스 속성)이 `sAMAccountName`으로 설정됩니다. 이에 따라 시스템에서는 사용자가 시스템에 대한 로그인을 시도하는 경우 각 개체에 대해 `sAMAccountName` 속성을 검사하면서 사용자 이름을 매칭합니다.

또한 CLI액세스 속성이 `sAMAccountName`이면 사용자가 어플라이언스의 CLI 계정에 로그인할 때 디렉터리의 모든 개체에 대해 각 `sAMAccountName`속성을 검사하여 매칭하는지 확인합니다.

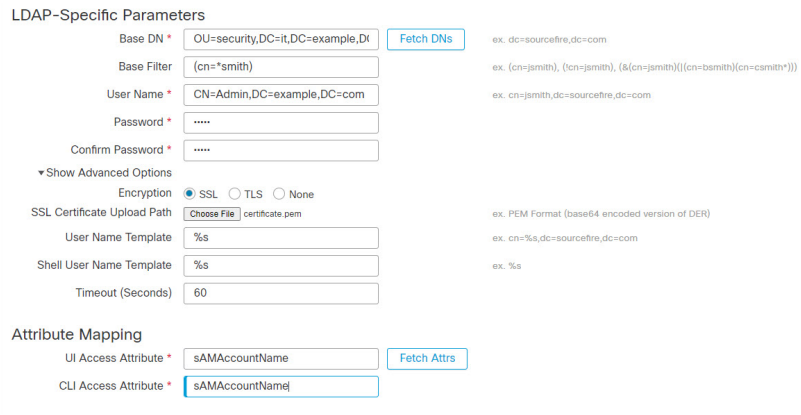
이 서버에는 기본 필터가 적용되지 않으므로 시스템은 기본 DN이 나타내는 디렉터리의 모든 개체에 대해 속성을 검사합니다. 기본 기간(또는 LDAP 서버에 설정된 시간 초과 기간)이 경과하면 서버와의 연결이 시간 초과됩니다.

고급 예시

이 예에서는 Microsoft Active Directory Server에 대한 LDAP 로그인 인증 개체의 고급 구성을 보여줍니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 636을 액세스에 사용합니다.



이 예는 예시 회사의 정보 기술 도메인에 있는 보안 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다. 그러나 이 서버는 기본 필터 `(cn=*smith)`가 있습니다. 이 필터는 CN이 `smith`로 끝나는 사용자만 서버에서 가져오도록 제한합니다.

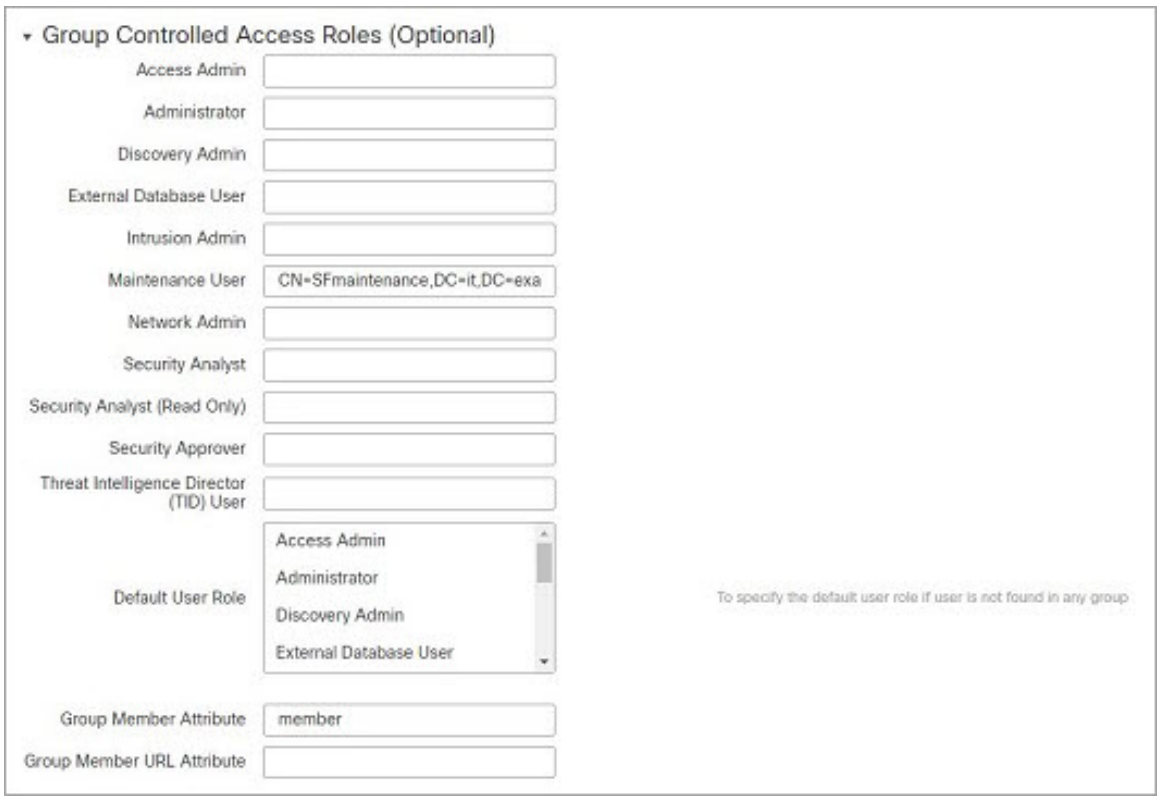


서버와의 연결은 SSL로 암호화되고 `certificate.pem`이라는 인증서가 연결에 사용됩니다. 또한 **Timeout(Seconds)(**시간 초과**(**초**))** 설정 때문에 60초가 지나면 서버와의 연결이 시간 초과됩니다.

이 서버는 Microsoft Active Directory Server이므로 `sAMAccountName` 속성을 사용해 사용자 이름을 저장하며 `uid` 속성을 사용하지 않습니다. 구성에 `sAMAccountName`이라는 **UI Access Attribute(UI** 액세스 속성**)**가 포함되어 있습니다. 이에 따라 시스템에서는 사용자가 시스템에 대한 로그인을 시도하는 경우 각 개체에 대해 `sAMAccountName` 속성을 검사하면서 사용자 이름을 매칭합니다.

또한 **CLI Access Attribute(CLI** 액세스 속성**)**가 `sAMAccountName`이면 사용자가 어플라이언스의 CLI 계정에 로그인할 때 디렉토리의 모든 개체에 대해 각 `sAMAccountName` 속성을 검사하여 매칭하는지 확인합니다.

여기에는 그룹 설정도 포함되어 있습니다. `member` 그룹 속성과 `CN=SFmaintenance,DC=it,DC=example,DC=com`이라는 기본 도메인 이름을 갖는 그룹의 모든 멤버에게 Maintenance User(유지 보수 사용자) 역할이 자동으로 지정됩니다.



CLI 액세스 필터는 기본 필터와 동일하게 설정되므로, 동일한 사용자가 웹 인터페이스뿐 아니라 CLI를 통해서도 어플라이언스에 액세스할 수 있습니다.

Management Center에 대한 RADIUS 외부 인증 개체 추가

RADIUS 서버를 추가하고 디바이스 관리를 위해 외부 사용자를 지원합니다.

다중 도메인 구축에서 외부 인증 개체는 생성된 도메인에서만 사용할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Users(**사용자**)**를 선택합니다.

단계 **2** **External Authentication(**외부 인증**)**을 클릭합니다.

단계 **3** 아이콘 추가( )**Add External Authentication Object(**외부 인증 개체 추가**)**를 클릭합니다.

단계 **4** **Authentication Method(**인증 방법**)**을 **RADIUS**로 설정합니다.

단계 **5** **Name(**이름**)**과 **Description(**설명**)**(선택 사항)을 입력합니다.

단계 **6** **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

단계 **7** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 **8** **RADIUS Secret Key(RADIUS** 비밀 키**)**를 입력합니다.

단계 **9** (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

단계 **10** (선택 사항) **RADIUS-Specific Parameters(RADUIS** 특정 파라미터**)**를 입력합니다.

a) **Timeout(**시간 초과**)**을 초 단위(1~1024)로 입력하고 기본 서버를 다시 시도합니다. 기본값은 30입니다.

참고 시간 초과 범위는 threat defense와 management center에 따라 다르므로 개체를 공유하는 경우 threat defense의 더 작은 시간 초과 범위 (1 ~ 300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 threat defense RADIUS 구성이 작동하지 않습니다.

b) **Retries(**재시도**)**를 입력하고 백업 서버로 이동합니다. 기본값은 3입니다.

c) 사용자 역할에 해당하는 필드에 각 사용자의 이름을 입력하거나 해당 역할에 지정될 식별 특성-값 쌍을 입력합니다.

사용자 이름과 속성-값 쌍은 쉼표로 구분합니다.

예제**:**

보안 분석가인 모든 사용자가 `Analyst(분석가)`를 `User-Category(사용자-카테고리)` 속성 값으로 갖는 경우, `User-Category=Analyst`를 **Security Analyst(**보안 분석가 목록**)** 필드에 입력하고 해당 사용자에게 해당 역할을 부여할 수 있습니다.

예제**:**

Administrator(관리자) 역할을 사용자인`jsmith`와 `jdoe`에게 부여하려면 `jsmith, jdoe`를 **Administrator(**관리자**)** 필드에 입력합니다.

예제**:**

Maintenance User(유지 보수 사용자) 역할을 `User-Category(사용자-카테고리)` 값이 `Maintenance(유지 보수)`인 모든 사용자에게 부여하려면 `User-Category=Maintenance`를 **Maintenance User(**유지 보수 사용자**)** 필드에 입력합니다.

d) 지정된 어떤 그룹에도 속하지 않는 사용자에 대해 **Default User Role(**기본 사용자 역할**)**을 선택합니다.

사용자의 역할을 변경하는 경우, 변경된 외부 인증 개체는 저장/배포하고 **Users(**사용자**)** 화면에서 해당 사용자를 제거해야 합니다. 이 사용자는 다음 로그인 시 자동으로 재추가됩니다.

단계 **11** (선택 사항) **Define Custom RADIUS Attributes(**맞춤형 **RADIUS** 속성 정의**)**.

RADIUS 서버가 `/etc/radiusclient`의 `dictionary` 파일에 없는 속성의 값을 반환할 경우, 이러한 속성을 사용하여 해당 속성을 갖는 사용자에 대한 역할을 설정하려면 그러한 속성을 정의해야 합니다. RADIUS 서버에서 사용자 프로파일을 확인하여 사용자에 대해 반환되는 속성을 찾을 수 있습니다.

a) **Attribute Name(**속성 이름**)**을 입력합니다.

속성을 정의할 때 영숫자로 구성된 속성의 이름을 제공합니다. 속성 이름의 단어는 공백이 아닌 대시로 구분해야 합니다.

b) 정수로 **Attribute ID(**속성 **ID)**를 입력합니다.

속성 ID는 정수이며 `etc/radiusclient/dictionary` 파일에 있는 기존 속성 ID와 충돌해서는 안 됩니다.

c) **Attribute Type(**속성 유형**)** 드롭다운 목록에서 선택합니다.

속성의 유형을 문자열, IP 주소, 정수 또는 날짜로 지정합니다.

d) **Add(**추가**)**를 클릭하고 맞춤형 속성을 추가합니다.

RADIUS 인증 개체를 생성하는 경우 해당 개체에 대한 새로운 사전 파일이 `/var/sf/userauth` 디렉토리에 있는 디바이스에 생성됩니다. 추가하는 모든 맞춤형 속성은 사전 파일에 추가됩니다.

예제**:**

RADIUS 서버가 Cisco 라우터가 있는 네트워크에서 사용되는 경우 `Ascend-Assign-IP-Pool` 속성을 사용하여 특정 IP 주소 풀에서 로그인한 모든 사용자에게 특정 역할을 부여할 수 있습니다.
`Ascend-Assign-IP-Pool`은 정수 속성으로서 사용자가 로그인할 수 있는 주소 풀을 정의합니다. 여기서 정수는 지정된 IP 주소 풀의 번호를 나타냅니다.

맞춤형 속성을 표시하려면 속성 이름 `Ascend-IP-Pool-Definition`, 속성 ID `218`, 속성 유형 `integer`로 맞춤형 속성을 생성합니다.

그런 다음 `Ascend-Assign-IP-Pool=2`를 **Security Analyst (Read Only)(**보안 분석가**(**읽기 전용**))** 필드에 입력하여 `Ascend-IP-Pool-Definition` 속성의 값이 `2`인 모든 사용자에게 읽기 전용 보안 분석가 권한을 부여할 수 있습니다.

단계 **12** (선택 사항) **CLI Access Filter(CLI** 액세스 필터**)** 영역 **Administrator CLI Access User List(**관리자 **CLI** 액세스 사용자 목록**)** 필드에 CLI 액세스 권한이 있어야 하는 사용자 이름을 쉼표로 구분하여 입력합니다.

이러한 사용자 이름은 RADIUS 서버의 사용자 이름과 일치해야 합니다. 이름은 다음과 같은 Linux 기준을 준수하는 사용자 이름이어야 합니다.

- 최대 32개의 영숫자 문자와 마침표(.), 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

CLI 액세스에 대해 RADIUS 인증을 하지 않으려면 이 필드를 비워 둡니다.

참고 CLI 액세스 권한이 있는 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스할 수 있습니다. Linux 셸 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. CLI 또는 Linux 셸 액세스 권한을 갖는 사용자의 목록을 제한해야 합니다.

참고 셸 액세스 필터에 포함된 사용자와 사용자 이름이 동일한 내부 사용자를 모두 제거합니다. management center에서는 내부 CLI 사용자만 관리자이니, 관리자 외부 사용자를 생성하지 마십시오.

단계 **13** (선택 사항) **Test(**테스트**)**를 클릭해 RADIUS 서버와 management center 연결을 테스트합니다.

단계 **14** (선택 사항) **Additional Test Parameters(**추가 테스트 파라미터**)**를 입력하고 인증 가능한 사용자의 크리덴셜을 테스트할 수 있습니다. **User Name(**사용자 이름**)** 및 **Passowrd(**비밀번호**)**를 입력한 다음 **Test(**테스트**)**를 클릭합니다.

팁 테스트 사용자의 이름이나 비밀번호를 잘못 입력할 경우 서버 구성이 맞더라도 테스트는 실패합니다. 서버 구성이 올바른지 확인하려면 먼저 **Test(**테스트**)**를 클릭합니다. 여기서 **Additional Test Parameters(**추가 테스트 파라미터**)** 필드에는 사용자 정보를 입력할 필요가 없습니다. 테스트가 성공하면 사용자 이름과 비밀번호를 입력하고 특정 사용자로 테스트하십시오.

예제**:**

예를 들어 예시 회사의 `JSmith` 사용자 크리덴셜을 가져올 수 있는지 테스트하려면 `JSmith`를 입력하고 올바른 비밀번호를 입력합니다.

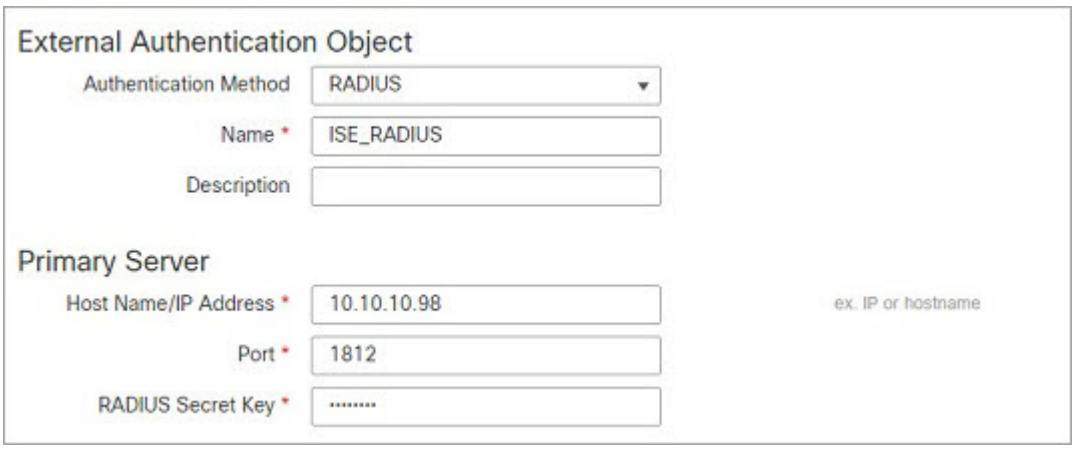
단계 **15** **Save(**저장**)**를 클릭합니다.

단계 **16** 이 서버의 사용을 활성화합니다. Management Center 사용자에 대한 외부 인증 활성화, 142 페이지를 참조하십시오.

예

단순한 사용자 역할 할당

다음 그림은 포트 1812에서 IP 주소 10.10.10.98을 사용하여 Cisco ISE(Identity Services Engine)를 실행하는 서버를 위한 RADIUS 로그인 인증 개체의 예를 보여줍니다. 정의된 백업 서버가 없습니다.



다음 예는 RADIUS 관련 매개변수를 보여줍니다. 여기에는 시간 초과(30초) 및 Firepower System이 백업 서버에 연결을 시도하기 전 실패한 재시도 횟수(있는 경우)가 포함됩니다.

이 예에서는 RADIUS 사용자 역할 구성의 주요 측면을 보여줍니다.

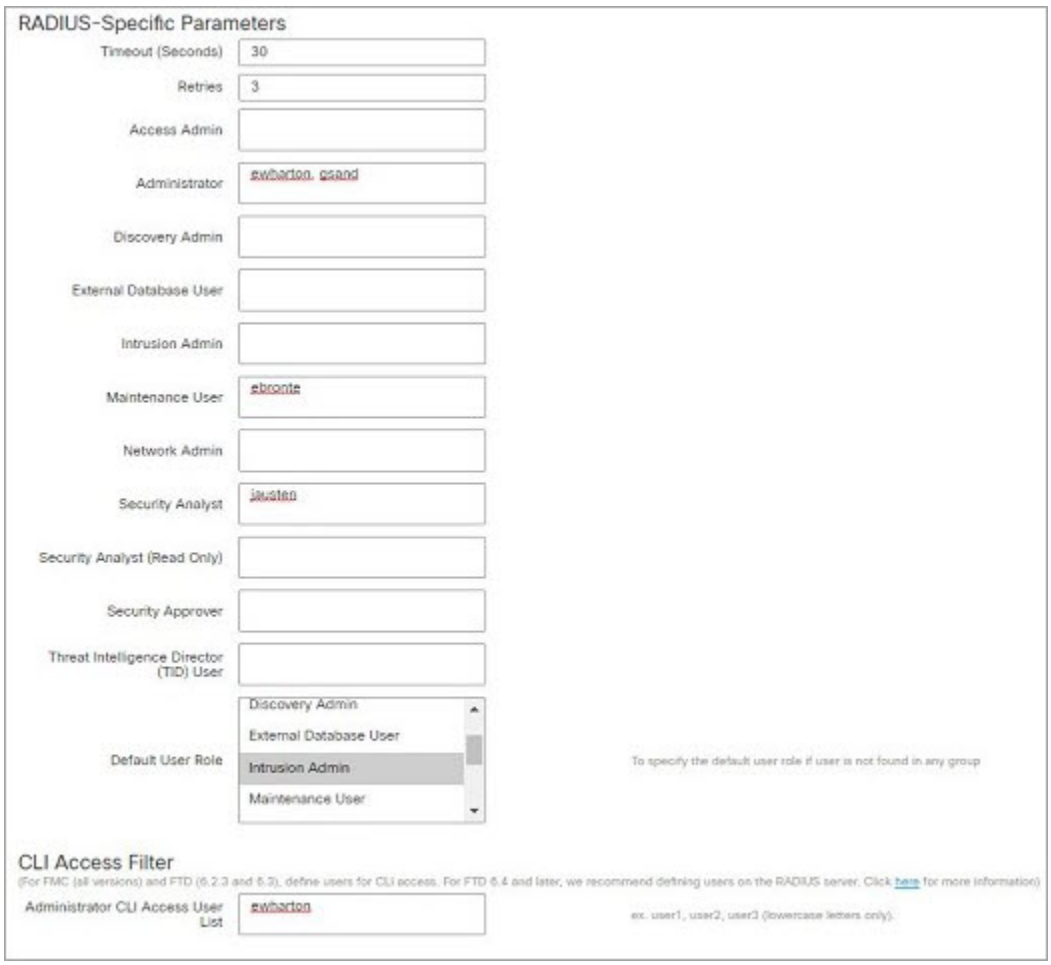
사용자 `ewharton` 및 `gsand`에게 웹 인터페이스 Administrator(관리자) 액세스 권한이 주어집니다.

사용자 `cbronte`에게 웹 인터페이스 Maintenance User(유지 보수 사용자) 액세스 권한이 주어집니다.

사용자 `jausten`에게 웹 인터페이스 Security Analyst(보안 분석가) 액세스 권한이 주어집니다.

사용자 `ewharton`은 CLI 계정을 사용하여 디바이스에 로그인할 수 있습니다.

다음 그림은 이 예시에서의 역할 구성을 나타냅니다.

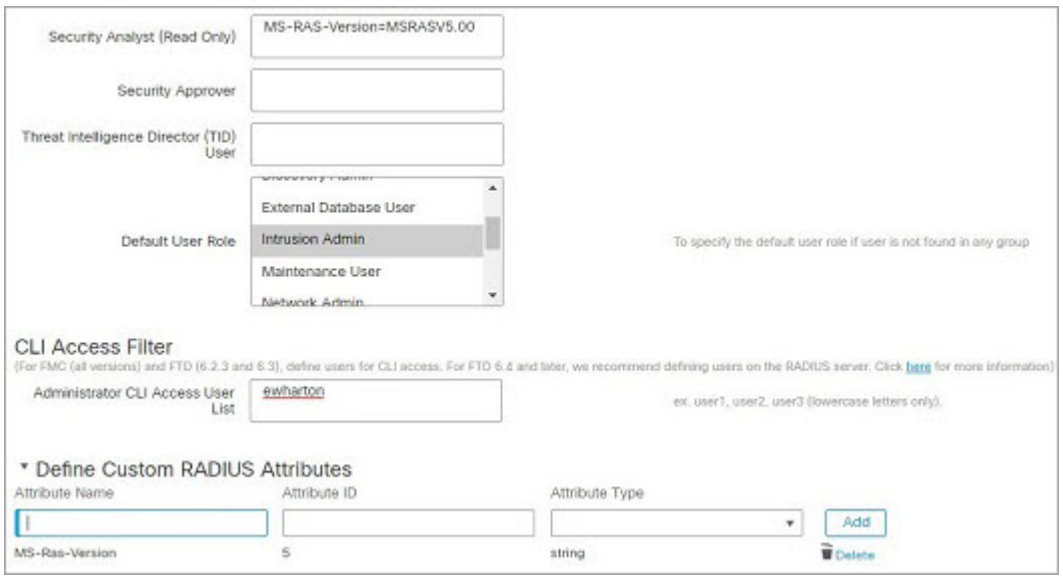


속성-값 쌍을 매칭하는 사용자의 역할

속성-값 쌍을 사용하여 특정 사용자 역할을 갖는 사용자를 식별할 수 있습니다. 사용하는 속성이 맞춤형 속성일 경우 해당 맞춤형 속성을 정의해야 합니다.

다음 그림은 이전의 예와 동일한 ISE 서버를 위한 샘플 RADIUS 로그인 인증 개체에 포함된 역할 설정 및 맞춤형 속성 정의를 보여줍니다.

그러나 여기서는 Microsoft 원격 액세스 서버가 사용 중이므로 `MS-RAS-Version` 맞춤형 속성 한 명 이상의 사용자에게 반환됩니다. 참고로 `MS-RAS-Version` 맞춤형 속성은 문자열입니다. 이 예에서는 Microsoft v. 5.00 원격 액세스 서버를 통해 RADIUS로 로그인하는 모든 사용자가 Security Analyst(Read Only)(보안 분석가(읽기 전용)) 역할을 받아야 하므로 속성-값 쌍 `MS-RAS-Version= MSRASV5.00`을 **Security Analyst(Read Only)(**보안 분석가**(**읽기 전용**))** 필드에 입력합니다.



Management Center 사용자에 대한 외부 인증 활성화

관리 사용자에 대한 외부 인증을 활성화하는 경우, 외부 인증 객체에 지정된 대로 management center에서 LDAP 또는 RADIUS 서버로 사용자 자격 증명을 확인합니다.

시작하기 전에

Management Center에 대한 LDAP 외부 인증 개체 추가, 127 페이지 및 Management Center에 대한 RADIUS 외부 인증 개체 추가, 136 페이지에 따라 외부 인증 개체를 1개 이상 추가합니다.

프로시저

단계 **1** 시스템 (⚙) > **Users(**사용자**)**를 선택합니다.

단계 **2** **External Authentication(**외부 인증**)**을 클릭합니다.

단계 **3** 외부 웹 인터페이스 사용자에 대한 기본 사용자 역할을 설정합니다.

역할이 없는 사용자가 어떤 작업도 수행할 수 없습니다. 외부 인증 개체에 정의된 사용자 역할이 이 기본 사용자 역할보다 우선합니다.

a) **Default User Role(**기본 사용자 역할**)** 값을 클릭합니다(기본적으로 none(해당 없음) 선택됨).

a) **Default User Role Configuration(**기본 사용자 역할 구성**)** 대화 상자에서 사용하려는 역할(복수 가능)을 선택합니다.

b) **Save(**저장**)**를 클릭합니다.

단계 **4** 사용하려는 각 외부 인증 개체 옆 **Slider enabled(**슬라이더 활성화됨**)** ( )를 클릭합니다. 개체를 1개 이상 활성화하는 경우, 사용자가 지정된 순서대로 서버와 비교됩니다. 다음 단계를 참조하고 서버를 재정렬합니다.

셸 인증을 활성화하는 경우에 **CLI** 액세스 필터를 포함하는 외부 인증 개체를 활성화해야 합니다. 또한 CLI 액세스 사용자는 인증 개체가 목록에서 순위가 가장 높은 서버에 대해서만 인증할 수 있습니다.

단계 **5** (선택 사항) 인증 요청이 발생한 경우 서버를 드래그 앤 드롭하고 인증 순서를 변경합니다.

단계 **6** 외부 사용자에 대해 CLI 액세스를 허용하려면, **Shell Authentication(**셸 인증**)** > **Enabled(**활성화**)**를 선택합니다.

첫 번째 외부 인증 개체 이름이 **Enabled(**활성화**)** 옵션 옆에 표시되고 첫 번째 개체만 CLI 액세스에 사용된다고 알립니다.

단계 **7** **Save and Apply(**저장 및 적용**)**를 클릭합니다.

LADP로 CAC(Common Access Card) 인증 구성

조직에서 CAC(Common Access Card)를 사용할 경우, LDAP 인증을 설정하여 웹 인터페이스에 로그인하는 management center 사용자를 인증할 수 있습니다. CAC 인증으로 사용자는 어플라이언스에 별도의 사용자 이름과 비밀번호를 제공하지 않고 곧바로 로그인할 수 있습니다.

CAC 인증 사용자는 EDIPI(electronic data interchange personal identifier) 번호로 식별됩니다.

24시간 동안 활동이 없는 경우, 디바이스가 CAC 인증 사용자를 **Users(**사용자**)** 탭에서 삭제합니다. 다음에 로그인할 때마다 사용자가 다시 추가되지만, 사용자 역할에 대한 수동 변경사항은 다시 구성해야 합니다.

⚠

주의 LDAP를 사용하여 CAC 인증을 구성하는 경우 사용자에게 기본 액세스 역할을 할당하는 동시에 최소 권한 원칙을 준수해야 합니다. 사용자가 CAC 자격 증명으로 시스템에 처음 로그인하면 해당 계정에 이 기본 액세스 역할이 할당됩니다.

기본 액세스 역할을 할당할 때 최소 권한 원칙을 따르지 않는 경우 후속 로그인 시 사용자에게 의도하지 않은 권한 수준이 할당될 수 있습니다. 그러면 사용자가 필요한 액세스 역할 이상의 권한을 갖게 될 수 있습니다.

기본 액세스 역할로 로그인한 사용자가 권한을 일시적으로 승격해야 하는 경우, 관리 권한이 있는 사용자는 더 높은 권한을 가진 역할을 할당하여 해당 사용자에게 필요한 더 높은 액세스 레벨을 일시적으로 제공할 수 있습니다. 이 권한은 24시간 동안 활동이 없으면 취소되며, 사용자는 기본 액세스 역할로 돌아갑니다.

사용자가 시스템 관리자와 같은 더 높은 권한 레벨에 영구적으로 액세스 역할을 재할당해야 하는 경우, 그룹 제어 액세스 역할 방법을 통해 사용자에게 관리자 액세스 권한을 제공합니다. 이 방법을 사용하면 제공된 액세스 역할이 24시간 이상 유지되며, 사용자는 그룹 할당에 따라 올바른 권한 레벨을 갖습니다. Group Controlled Access Roles(그룹 제어 액세스 역할) 구성에 대한 자세한 내용은 단계 13 섹션을 참고하십시오.

시작하기 전에

CAC 컨피그레이션 프로세스의 일환으로 사용자 인증서를 활성화하려면 브라우저에 유효한 사용자 인증서(여기서는 CAC를 통해 브라우저에 전달된 인증서)가 반드시 있어야 합니다. CAC 인증 및 권한 부여를 구성하면 네트워크의 사용자는 브라우징 세션 내내 CAC 연결을 유지해야 합니다. 세션 중에 CAC를 제거하거나 대체할 경우 웹 브라우저는 세션을 종료하며 웹 인터페이스에서 로그아웃됩니다.

프로시저

단계 **1** 조직의 지침대로 CAC를 삽입합니다.

단계 **2** 브라우저에서 **https://***ipaddress_or_hostname*/로 이동합니다. 여기서*ipaddress* 또는 *hostname*은 사용자 디바이스와 일치합니다.

단계 **3** 메시지가 표시되면 1단계에서 삽입한 CAC의 PIN을 입력합니다.

단계 **4** 메시지가 표시되면, 드롭다운 목록에서 적절한 인증서를 선택합니다.

단계 **5** Login(로그인) 페이지의 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에서 Administrator(관리자) 권한이 있는 사용자로 로그인합니다. 아직 CAC 크리덴셜을 사용하여 로그인 할 수 없습니다 .

단계 **6** **System** > **Users** > **External Authentication**(시스템 사용자 외부 인증)을 선택합니다.

단계 **7** Management Center에 대한 LDAP 외부 인증 개체 추가, 127 페이지의 절차에 따라 CAC 전용 LDAP 인증 개체를 생성합니다. 다음 항목을 구성해야 합니다.

- **CAC** 확인란
- **LDAP-Specific Parameters(LDAP** 관련 매개변수**)** > **Show Advanced Options(**고급 옵션 표시**)** > **User Name Template(**사용자 이름 템플릿**)**
- **Attribute Mapping(**속성 매핑**)** > **UI Access Attribute(UI** 액세스 속성**)**

단계 **8** **Save(**저장**)**를 클릭합니다.

단계 **9** Management Center 사용자에 대한 외부 인증 활성화, 142 페이지에 설명된 대로 외부 인증 및 CAC 인증을 활성화합니다.

단계 **10** 시스템 (⚙) > **Configuration(**구성**)**를 선택하고 **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

단계 **11** 필요하다면 HTTPS 서버 인증서 가져오기, 70 페이지에 설명된 절차에 따라 HTTPS 서버 인증서를 가져옵니다.

사용하려는 CAC에서 동일한 CA(인증 기관)이 HTTPS 서버 인증서와 사용자 인증서를 발급해야 합니다.

단계 **12** **HTTPS Client Certificate Settings(HTTPS** 클라이언트 인증서 설정**)**에서 **Enable Client Certificates(**클라이언트 인증서 활성화**)**를 선택합니다. 자세한 내용은 유효한 HTTPS 클라이언트 인증서 필요, 71 페이지를 참고하십시오.

단계 **13** CAC 인증서로 Secure Firewall Management Center에 로그인, 35 페이지에 따라 디바이스에 로그인합니다.

SAML SSO(Single Sign-On) 구성

조직의 다른 애플리케이션뿐만 아니라 management center에 로그인하는 사용자에게 인증 및 권한 부여를 제공하는 시스템 인 SSO(Single Sign-On)를 사용하도록 management center를 구성할 수 있습니다. 이러한 SSO 설정에 참여하도록 구성된 애플리케이션은 페더레이션 서비스 제공자 애플리케이션이라고 합니다. SSO 사용자는 한 번 로그인하면 동일한 페더레이션의 멤버인 모든 서비스 제공자 애플리케이션에 액세스할 수 있습니다.

SAML SSO(Single Sign-On)

SSO용으로 구성된 management center는 로그인 페이지에 단일 로그인 링크를 제공합니다. SSO 액세스를 위해 구성된 사용자가 이 링크를 클릭하면 management center 로그인 페이지에서 사용자 이름과 암호를 제공하지 않고 인증 및 권한 부여를 위해 IdP로 리디렉션됩니다. IdP에서 성공적으로 인증되면 SSO 사용자는 management center 웹 인터페이스로 다시 리디렉션되고 로그인됩니다.이를 수행하기 위해 management center와 IdP 간의 모든 통신은 브라우저를 중개자로 사용하여 수행됩니다. 따라서 management center에서는 ID 제공자에 직접 액세스하기 위해 네트워크 연결이 필요하지 않습니다.

management center에서는 인증 및 권한 부여를 위해 SAML(Security Assertion Markup Language) 2.0 공개 표준을 준수하는 SSO 제공자를 사용하는 SSO를 지원합니다.

Note 관리 센터는 SAML 인증 요청 메시지에 서명할 수 없습니다. 따라서 IdP가 인증 요청에 서비스 제공자의 서명을 요구하는 경우 관리 센터의 SSO가 실패합니다.

management center 웹 인터페이스는 다음 SSO 제공자에 대한 구성 옵션을 제공합니다.

- Okta
- OneLogin
- Azure
- PingID의 PingOne for Customers 클라우드 솔루션
- 기타

Note Cisco Secure Sign On SSO 제품은 management center를 사전 통합된 서비스 제공자로 인식하지 않습니다.

Management Center에 대한 SSO 지침

management center를 SSO 연합 멤버로 설정할 때는 다음 사항에 유의하십시오.

- management center는 한 번에 하나의 SSO 제공자만 있는 SSO를 지원할 수 있습니다. 예를 들어, SSO용 OneLogin 및 Okta를 모두 사용하도록 management center를 설정할 수 없습니다.

- management center고가용성 설정의 FMC는 SSO를 지원할 수 있지만, 다음 사항을 고려해야 합니다.
  - SSO 설정은 고가용성 쌍의 멤버 간에 동기화되지 않습니다. 쌍의 각 멤버에서 SSO를 별도로 설정해야 합니다.
  - 고가용성 쌍의 두 management center는 모두 SSO에 동일한 IdP를 사용해야 합니다. SSO에 대해 설정된 각 management center의 IdP에서 서비스 제공자 애플리케이션을 설정해야 합니다.
  - 둘 다 SSO를 지원하도록 설정된 management center 고가용성 쌍에서는 사용자가 SSO를 사용하여 보조 management center에 처음으로 액세스하기 전에 먼저 사용자가 SSO를 통해 기본 management center에 한 번 이상 로그인해야합니다.
  - 고가용성 쌍에서 management center에 대해 SSO를 설정하는 경우:
    - 기본 management center에서 SSO를 설정하는 경우, 보조 management center에서 SSO를 설정할 필요가 없습니다.
    - 보조 management center에서 SSO를 설정하는 경우, 기본 management center에서도 SSO를 설정해야 합니다. (SSO 사용자는 보조 management center에 로그인하기 전에 기본 management center에 한 번 이상 로그인해야 하기 때문입니다.)
- 멀티테넌시를 사용하는 management center에서 SSO 구성은 전역 도메인 레벨에서만 적용할 수 있으며, 전역 도메인 및 모든 하위 도메인에 적용됩니다.
- 내부 또는 LDAP 또는 RADIUS에 의해 인증된 관리자 역할의 사용자만 SSO를 설정할 수 있습니다.
- management center는 IdP에서 시작된 SSO를 지원하지 않습니다.
- management center는 SSO 계정에 대한 CAC 자격 증명을 사용한 로그인을 지원하지 않습니다.
- CC 모드를 사용하는 구축에서는 SSO를 설정하지 마십시오.
- SSO 활동은 Subsystem(하위 시스템) 필드에 Login(로그인) 또는 Logout(로그아웃)이 지정된 management center 감사 로그에 기록됩니다.

Related Topics

고가용성, 311 페이지
도메인, 219 페이지
CAC 인증서로 Secure Firewall Management Center에 로그인, 35 페이지
보안 인증서 컴플라이언스, 335 페이지
감사 기록, 419 페이지

SSO 사용자 계정

ID 공급자는 사용자 및 그룹 구성을 직접 지원할 수도 있고, Active Directory, RADIUS 또는 LDAP와 같은 다른 사용자 관리 애플리케이션에서 사용자 및 그룹을 가져올 수도 있습니다. 이 문서에서는 IdP 사용자 및 그룹이 이미 설정되어 있다고 가정하고 SSO를 지원하도록 IdP와 작동하도록 management

center를 구성하는 방법을 중점적으로 다룹니다. 다른 사용자 관리 애플리케이션의 사용자 및 그룹을 지원하도록 IdP를 구성하려면 IdP 벤더 설명서를 참조하십시오.

사용자 이름 및 암호를 포함하여 SSO 사용자에 대한 대부분의 계정 특성은 IdP에서 설정됩니다. SSO 계정은 처음 로그인할 때까지 management center 웹 인터페이스 사용자 페이지에 나타나지 않습니다.

Note 시스템에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 management center에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이것이 IdP에 해당하는지 확인해야 합니다. IdP에서 통신 사업자 애플리케이션을 구성하고 management center에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

SSO 사용자에 대한 다음 계정 특성은 시스템 (⚙) > **Users(**사용자**)** > **Edit User(**사용자 편집**)** 아래의 management center 웹 인터페이스에서 구성할 수 있습니다.

- 실제 이름
- 브라우저 세션 시간 초과에서 제외

SSO 사용자에 대한 사용자 역할 매핑

기본적으로 management center에 대한 SSO 액세스 권한이 부여된 모든 사용자에게는 보안 분석가(읽기 전용) 역할이 할당됩니다. 이 기본값을 변경하고 사용자 역할 매핑이 있는 특정 SSO 사용자 또는 그룹에 대해 이 기본값을 재정의할 수 있습니다. management center SSO 구성을 설정하고 성공적으로 테스트한 후 management center SSO 사용자가 로그인할 때 할당되는 사용자 역할을 설정하도록 사용자 역할 매핑을 구성할 수 있습니다.

사용자 역할을 매핑하려면 management center에서 구성 설정을 SSO IdP 애플리케이션의 설정과 조정해야 합니다. 사용자 역할은 사용자 또는 IdP 애플리케이션에 정의된 그룹에 할당할 수 있습니다. 사용자는 그룹의 구성원일 수도 있고 아닐 수도 있으며, 사용자 또는 그룹 정의는 조직 내의 다른 사용자 관리 시스템(예: Active Directory)에서 IdP로 가져오거나 가져올 수 없습니다. 따라서 management center SSO 사용자 역할 매핑을 효과적으로 구성하려면 SSO 페더레이션이 구성되는 방식과 SSO IdP 애플리케이션에서 사용자, 그룹 및 해당 역할이 할당되는 방식을 숙지해야 합니다. 이 문서에서는 사용자 역할 매핑을 지원하기 위해 IdP와 함께 작동하도록 management center를 구성하는 방법을 중점적으로 다룹니다. IdP 내에서 사용자 또는 그룹을 생성하거나 사용자 관리 애플리케이션에서 IdP로 사용자 또는 그룹을 가져오려면 IdP 벤더 설명서를 참조하십시오.

사용자 역할 매핑에서 IdP는 management center 서비스 공급자 애플리케이션에 대한 역할 특성을 유지하며, 해당 management center에 대한 액세스 권한이 있는 각 사용자 또는 그룹은 역할 특성에 대한 문자열 또는 식으로 구성됩니다(속성 값에 대한 요구 사항은 각 IdP마다 다름). management center에서 해당 역할 속성의 이름은 SSO 구성의 일부입니다. management center SSO 구성에는 management center 사용자 역할 목록에 할당된 식 목록도 포함됩니다. 사용자가 SSO를 사용하여 management center에 로그인하면 management center에서는 해당 사용자(또는 구성에 따라 해당 사용자 그룹)의 역할 속성 값을 각 management center 사용자 역할의 식과 비교합니다. management center에서는 식이 사용자가 제공한 속성 값과 일치하는 모든 역할을 사용자에게 할당합니다.

Note 개별 권한 또는 그룹 권한에 따라 management center 역할을 매핑하도록 설정할 수 있지만, 단일 management center 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다.

Management Center에서 SSO(Single Sign-On) 활성화

Before you begin

- SAML SSO 관리 애플리케이션에서 management center에 대한 서비스 제공자 애플리케이션을 구성하고 서비스 제공자 애플리케이션에 사용자 또는 그룹을 할당합니다.
  - Okta용 management center 서비스 제공자 애플리케이션을 구성하려면 Okta를 위한 Management Center 서비스 제공자 애플리케이션 구성, on page 150의 내용을 참조하십시오.
  - OneLogin용 management center 서비스 제공자 애플리케이션을 구성하려면 OneLogin에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 164의 내용을 참조하십시오.
  - Azure용 management center 서비스 제공자 애플리케이션을 구성하려면 Azure용 Management Center 서비스 제공자 애플리케이션 구성, on page 176의 내용을 참조하십시오.
  - PingID의 PingOne for Customers 클라우드 솔루션에 대해 management center 서비스 제공자 애플리케이션을 구성하려면 PingID PingOne for Customers에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 190의 내용을 참조하십시오.
  - SAML 2.0 호환 SSO 제공자에 대해 management center 서비스 제공자 애플리케이션을 구성하려면 SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 195의 내용을 참조하십시오.

Procedure

단계 **1** 시스템 (⚙) > **Users(**사용자**)** > **SSO(Single Sign-On,** 단일 인증**)**를 선택합니다.

단계 **2** **SSO(Single Sign-On)** 구성 슬라이더를 클릭하여 SSO를 활성화합니다.

단계 **3** **Configure SSO(SSO** 구성**)** 버튼을 클릭합니다.

단계 **4** **Select FMC SAML Provider(FMC SAML** 제공자 선택**)** 대화 상자에서 선택한 SSO IdP 라디오 버튼을 클릭하고 **Next(**다음**)**를 클릭합니다.

What to do next

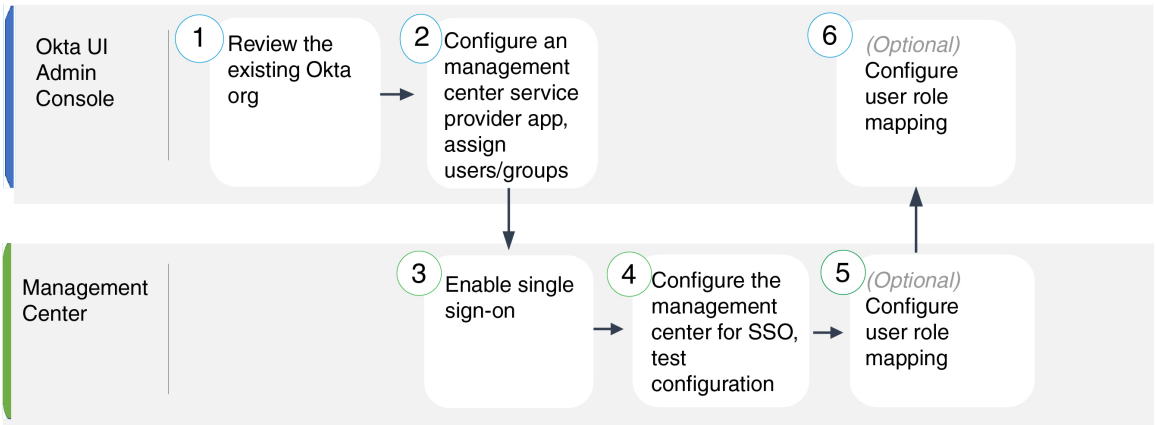
선택한 SSO 제공자에 적합한 지침을 진행합니다.

- Okta SSO용 management center를 구성합니다. Okta SSO용 Management Center 구성, on page 152의 내용을 참조하십시오.

- PingID의 PingOne for Customers 클라우드 솔루션을 사용하여 SSO용 management center를 구성합니다. PingID PingOne for Customers을 사용하여 SSO용 Management Center을 구성합니다., on page 192의 내용을 참조하십시오.
- Azure SSO용 management center를 구성합니다. Azure SSO용 Management Center 구성, on page 179의 내용을 참조하십시오.
- OneLogin SSO용 management center를 구성합니다. OneLogin SSO용 Management Center 구성, on page 165의 내용을 참조하십시오.
- SAML 2.0 호환 제공자를 사용하여 SSO용 management center를 구성합니다. SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 Management Center 구성, on page 197의 내용을 참조하십시오.

Okta로 SSO(Single Sign-On) 구성

Okta를 사용하여 SSO를 구성하려면 다음 작업을 참조하십시오.



1	Okta UI 관리 콘솔	Okta 조직 검토, on page 150
2	Okta UI 관리 콘솔	Okta를 위한 Management Center 서비스 제공자 애플리케이션 구성, on page 150
3	management center	Management Center에서 SSO(Single Sign-On) 활성화, on page 148
4	management center	Okta SSO용 Management Center 구성, on page 152
5	management center	Okta에 대한 사용자 역할 매핑 구성 Management Center, on page 153
6	Okta UI 관리 콘솔	Okta IdP에서 사용자 역할 매핑 구성, on page 154

Okta 조직 검토

Okta에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션 디바이스 및 애플리케이션을 포함하는 엔티티를 *org*라고 합니다. Okta 조직에 management center를 추가하기 전에 해당 구성을 숙지하십시오. 다음 질문을 검토하십시오.

- management center에 액세스할 수 있는 사용자는 몇 명입니까?
- 사용자가 Okta org 내 그룹 구성원입니까?
- 사용자 및 그룹 정의가 Okta의 기본 설정이거나 Active Directory, RADIUS 또는 LDAP와 같은 사용자 관리 애플리케이션에서 가져온 것입니까?
- management center에서 SSO를 지원하려면 Okta org에 더 많은 사용자 또는 그룹을 추가해야 합니까?
- 어떤 종류의 사용자 역할을 지정 하시겠습니까? (사용자 역할을 할당하지 않는 경우 management center가 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 필요한 사용자 역할 매핑을 지원하려면 Okta org 내의 사용자 및 그룹을 어떻게 구성해야 합니까?

개별 권한 또는 그룹 권한에 따라 management center 역할을 매핑하도록 구성할 수 있지만, 단일 management center 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다.

이 문서에서는 Okta Classic UI 관리 콘솔에 대해 잘 알고 있으며 슈퍼 관리자 권한이 필요한 구성 기능을 수행할 수 있는 계정이 있다고 가정합니다. 자세한 내용은 온라인에서 확인 가능한 Okta 문서를 참조하십시오.

Okta를 위한 Management Center 서비스 제공자 애플리케이션 구성

Okta Classic UI 관리 콘솔에서 이 지침을 사용하여 Okta 내에 management center 서비스 공급자 애플리케이션을 생성하고 해당 애플리케이션에 사용자 또는 그룹을 할당합니다. SAML SSO 개념 및 Okta 관리 콘솔에 대해 숙지해야 합니다. 이 문서에서는 모든 기능을 갖춘 SSO 조직을 설정하는 데 필요한 모든 Okta 기능에 대해 설명하지는 않습니다. 예를 들어 사용자 및 그룹을 생성하거나 다른 사용자 관리 애플리케이션에서 사용자 및 그룹 정의를 가져오려면 Okta 문서를 참조하십시오.

Note management center 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note management center는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 OneLogin에서 management center로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- SSO 페더레이션 그리고 해당 사용자 및 그룹을 숙지하십시오. Okta 조직 검토, on page 150을 참조하십시오.
- 필요한 경우 Okta 조직에서 사용자 계정 및/또는 그룹을 생성합니다.

Note 시스템에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 management center에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이것이 IdP에 해당하는지 확인해야 합니다. IdP에서 통신 사업자 애플리케이션을 구성하고 management center에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 management center(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

Note 여러 URL(예: 정규화된 도메인 이름 및 IP 주소)로 management center 웹 인터페이스에 연결할 수 있는 경우, SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 management center에 일관되게 액세스해야 합니다.

Procedure

단계 **1** Okta Classic UI 관리 콘솔에서 management center용 서비스 공급자 애플리케이션을 생성합니다. 다음 항목을 선택하여 management center 애플리케이션을 구성합니다.

- 플랫폼에 대해 **Web(**웹**)**을 선택합니다.
- **Sign on(**로그온**)** 방법으로 `SAML 2.0`을 선택합니다.
- **SSO(Single Sign On) URL**을 제공합니다.

  이는 브라우저가 IdP를 대신하여 정보를 전송하는 management center URL입니다.

  management center 로그인 URL에 `saml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **Use this for Recipient URL and Destination URL(**수신자 **URL** 및 대상 **URL**에 사용**)**를 활성화합니다.
- 대상 **URI(SP** 엔티티 **ID)**를 입력합니다.

  이 이름은 종종 URL로 형식이 지정되는 서비스 제공자(management center)의 전역 고유 이름입니다.

  management center 로그인 URL에 `/saml/metadata` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/metadata`

- **Name ID Format(**이름 **ID** 형식**)**에서 `Unspecified(지정되지 않음)`를 선택합니다.

단계 **2** (애플리케이션에 그룹을 할당하는 경우엔 선택 사항입니다.) 개별 Okta 사용자를 management center 애플리케이션에 할당합니다. (management center 애플리케이션에 그룹을 할당하려는 경우 해당 그룹의 멤버인 사용자를 개인으로 할당하지 마십시오.)

단계 **3** (애플리케이션에 개별 사용자를 할당하는 경우엔 선택 사항입니다.) Okta 그룹을 management center 애플리케이션에 할당합니다.

단계 **4** (선택 사항) management center에서 SSO를 보다 쉽게 설정할 수 있도록 management center 서비스 공급자 애플리케이션용 SAML XML 메타 데이터 파일을 Okta에서 로컬 컴퓨터로 다운로드할 수 있습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148의 내용을 참조하십시오.

Okta SSO용 Management Center 구성

management center 웹 인터페이스에서 다음 지침을 사용하십시오.

시작하기 전에

- Okta Classic UI 관리 콘솔에서 management center 서비스 제공자 애플리케이션을 생성합니다. Okta를 위한 Management Center 서비스 제공자 애플리케이션 구성, on page 150의 내용을 참조하십시오.
- SSO(Single Sign-On)을 활성화합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148의 내용을 참조하십시오.

Procedure

단계 **1** (이 단계는 Management Center에서 SSO(Single Sign-On) 활성화, on page 148에서 곧바로 이어집니다.) **Configure Okta Metadata(Okta** 메타데이터 구성**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 설정 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. Okta SSO 서비스 제공자 애플리케이션에서 다음 값을 입력합니다. (Okta Classic UI 관리 콘솔에서 이러한 값을 검색합니다.)
     - **ID** 제공자 **SSO(Single Sign-On) URL**
     - **ID** 제공자 발급자
     - **X.509** 인증서

- Okta에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우(Okta를 위한 Management Center 서비스 제공자 애플리케이션 구성, on page 150의 4단계) 파일을 management center에 업로드할 수 있습니다.

  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.

  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 management center의 SSO 구성과 Okta 서비스 제공자 애플리케이션 구성을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **5** 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 사용자 역할 매핑을 구성할 수 있습니다. Okta에 대한 사용자 역할 매핑 구성 Management Center, on page 153의 내용을 참조하십시오. 역할 매핑을 설정하지 않기로 선택하는 경우, 기본적으로 management center에 로그인하는 모든 SSO 사용자에게 Okta에 대한 사용자 역할 매핑 구성 Management Center, on page 153의 4단계에서 설정한 사용자 역할이 할당됩니다.

Okta에 대한 사용자 역할 매핑 구성 Management Center

management center 웹 인터페이스에서 사용자 역할 매핑을 구성할 수 있는 필드는 선택한 SSO 제공자와 상관없이 동일합니다. 그러나 구성하는 값의 경우, 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방식을 고려해야 합니다.

Before you begin

- Okta 사용자 그룹 매핑 정보를 검토합니다. Okta 조직 검토, on page 150의 내용을 참조하십시오.
- management center에 대한 SSO 서비스 제공자 애플리케이션을 구성합니다. Okta를 위한 Management Center 서비스 제공자 애플리케이션 구성, on page 150를 참조하십시오.
- management center에서 SSO(Single Sign-On)를 활성화하고 설정합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148 및 Okta SSO용 Management Center 구성, on page 152의 내용을 참조하십시오.

Procedure

단계 **1** 시스템 (⚙) > **Users(**사용자**)**를 선택합니다.

단계 **2** **SSO(Single Sign-On,** 단일 인증**)** 탭을 클릭합니다.

단계 **3** **Advanced Configuration (Role Mapping)**(고급 구성(역할 매핑))을 펼칩니다.

단계 **4** **Default User Role**(기본 사용자 역할) 드롭다운에서 management center 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **5** **Group Member Attribute**(그룹 멤버 속성)을 입력합니다. 이 문자열은 사용자 또는 그룹에 대한 사용자 역할을 매핑하는 데 Okta management center 제공자 애플리케이션에 설정된 속성 이름과 일치해야 합니다. (Okta IdP에서 역할 매핑을 위한 사용자 속성 구성, on page 155의 1단계 또는 Okta IdP에서 역할 매핑을 위한 그룹 속성 구성, on page 156의 1단계 참조)

단계 **6** SSO 사용자에게 할당할 각 management center 사용자 역할 옆에 정규식을 입력합니다. (management center는 Golang 및 Perl에서 지원하는 Google의 RE2 정규식 표준의 제한된 버전을 사용합니다.) management center에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 management center에 전송하는 사용자 역할 매핑 속성값과 비교합니다. management center는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

- 서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. Okta IdP에서 사용자 역할 매핑 구성, on page 154의 내용을 참조하십시오.

Okta IdP에서 사용자 역할 매핑 구성

개별 사용자 권한 또는 그룹 권한에 따라 Okta Classic UI 관리 콘솔에서 SSO 사용자 역할 매핑을 설정할 수 있습니다.

- 개별 사용자 권한에 따라 매핑하려면 Okta IdP에서 역할 매핑을 위한 사용자 속성 구성, on page 155의 내용을 참조하십시오.
- 그룹 권한에 따라 매핑하려면 Okta IdP에서 역할 매핑을 위한 그룹 속성 구성, on page 156의 내용을 참조하십시오.

SSO 사용자가 management center에 로그인하면 Okta는 Okta IdP에서 설정된 사용자 또는 그룹 역할 속성값을 management center에 제공합니다. management center에서는 해당 속성값을 SSO 설정의 각 management center 사용자 역할에 할당된 정규식과 비교하고, 일치하는 항목이 있는 모든 역할을 사용자에게 부여합니다. (일치 항목이 없으면 management center는 사용자에게 설정 가능한 기본 사용자 역할을 부여합니다.) 각 management center 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다. management center는 management center 사용자 역할 식과의 비교를 위해 동일한 표준을 사용하여 Okta에서 받은 속성값을 정규식으로 처리합니다.

Note 단일 management center는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. management center 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. 또한 FMC는 management center에 설정된 management center 서비스 제공자 애플리케이션당 하나의 그룹 속성 명령문만 사용하여 그룹 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 롤 매핑은 management center에 더 효율적입니다. Okta 조직 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

Okta IdP에서 역할 매핑을 위한 사용자 속성 구성

Okta 클래식 UI 관리 콘솔에서 다음 지침을 통해 Okta 기본 사용자 프로파일에 맞춤형 역할 매핑 속성을 추가합니다.

Okta 서비스 제공자 애플리케이션은 다음 두 가지 유형의 사용자 프로파일 중 하나를 사용할 수 있습니다.

- Okta 사용자 프로파일: 모든 맞춤형 속성으로 확장할 수 있습니다.
- 앱 사용자 프로파일: 지원되는 속성에 대해 타사 애플리케이션 또는 디렉토리(예: Active Directory, LDAP 또는 Radius)를 쿼리하여 Okta가 생성하는 사전 정의된 목록의 속성으로만 확장할 수 있습니다.

Okta 조직에서 사용자 프로파일 유형을 사용할 수 있습니다. 설정 방법에 대한 자세한 내용은 Okta 설명서를 참조하십시오. 어떤 사용자 프로파일 유형을 사용하든, management center와 함께 사용자 역할 매핑을 지원하려면 management center에 각 사용자의 역할 매핑 식을 전달하도록 프로파일에 맞춤형 속성을 구성해야 합니다.

이 문서에서는 Okta 사용자 프로파일을 통한 역할 매핑에 대해 설명합니다. 앱 프로파일을 사용하여 매핑하려면 맞춤형 속성을 설정하기 위해 조직에서 사용 중인 타사 사용자 관리 애플리케이션에 익숙해야 합니다. 자세한 내용은 Okta 설명서를 참조하십시오.

Before you begin

- Okta를 위한 Management Center 서비스 제공자 애플리케이션 구성, on page 150에 설명된 대로 Okta IdP에서 management center 서비스 제공자 애플리케이션을 설정합니다.
- Okta에 대한 사용자 역할 매핑 구성 Management Center, on page 153에 설명된 대로 management center에서 SSO 사용자 역할 매핑을 설정합니다.

Procedure

단계 **1** 기본 Okta 사용자 프로파일에 새 속성을 추가합니다.

- **Data type(**데이터 유형**)**은 `string`으로 선택합니다.
- Okta IdP가 management center로 보낼 변수 이름을 제공합니다. 여기에는 사용자 역할 매핑에 일치하는 식이 포함되어 있습니다. 이 변수 이름은 **Group Member Attribute(**그룹 멤버 속성**)**에 대

해 management center SSO 설정에서 입력한 문자열과 일치해야 합니다. (Okta에 대한 사용자 역할 매핑 구성 Management Center, on page 153의 5단계 참조)

단계 **2** 이 프로파일을 사용하여 management center 서비스 제공자 애플리케이션에 할당된 각 사용자에 대해 방금 생성한 사용자 역할 속성에 값을 할당합니다.

식을 사용하여 management center에서 사용자에게 할당할 역할을 나타냅니다. management center에서는 이 문자열을 Okta에 대한 사용자 역할 매핑 구성 Management Center, on page 153의 6단계에서 각 management center 사용자 역할에 할당한 식과 비교합니다. (management center 사용자 역할 식과 비교하기 위해 management center에서는 Okta에서 수신한 속성값을 Golang 및 Perl에서 지원하는 Google RE2 정규식 표준의 제한된 버전을 준수하는 식으로 처리합니다.)

Okta IdP에서 역할 매핑을 위한 그룹 속성 구성

Okta Classic UI 관리 콘솔에서 다음 지침을 통해 사용자 지정 역할 매핑 그룹 속성을 management center 서비스 공급자 애플리케이션에 추가하십시오. management center는 Okta management center 서비스 제공자 애플리케이션당 하나의 그룹 속성 명령문만 사용하여 그룹 역할 매핑을 지원할 수 있습니다.

Okta 서비스 제공자 애플리케이션은 다음 두 가지 유형의 그룹 중 하나를 사용할 수 있습니다.

- Okta 그룹: 모든 맞춤형 속성으로 확장할 수 있습니다.
- 애플리케이션 그룹: 지원되는 속성에 대해 타사 애플리케이션 또는 디렉토리(예: Active Directory, LDAP 또는 Radius)를 쿼리하여 Okta가 생성하는 사전 정의된 목록의 속성으로만 확장할 수 있습니다.

Okta 조직에서 두 가지 유형의 그룹을 사용할 수 있습니다. 설정 방법에 대한 자세한 내용은 Okta 설명서를 참조하십시오. 어떤 그룹 유형을 사용하든 간에 management center와 함께 사용자 역할 매핑을 지원하려면 management center에 그룹에 대한 역할 매핑 식을 전달하기 위한 맞춤형 속성을 설정해야 합니다.

이 문서에서는 Okta 그룹을 사용한 역할 매핑에 대해 설명합니다. 애플리케이션 그룹과 매핑하려면 맞춤형 속성을 설정하기 위해 조직에서 사용 중인 타사 사용자 관리 애플리케이션에 익숙해야 합니다. 자세한 내용은 Okta 설명서를 참조하십시오.

Before you begin

- Okta IdP에서 management center 서비스 제공자 애플리케이션을 설정합니다. Okta를 위한 Management Center 서비스 제공자 애플리케이션 구성, on page 150의 내용을 참조하십시오.
- management center에서 사용자 역할 매핑을 설정합니다. Okta에 대한 사용자 역할 매핑 구성 Management Center, on page 153의 내용을 참조하십시오.

Procedure

management center 서비스 제공자 애플리케이션에 대한 새 SAML 그룹 속성을 생성합니다.

- **Name(**이름**)**에는 management center SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 대해 입력한 것과 같은 문자열을 사용합니다. (Okta에 대한 사용자 역할 매핑 구성 Management Center, on page 153의 5단계 참조)
- **Filter(**필터**)**에서 management center가 그룹의 멤버에 할당할 역할을 나타내는 식을 지정합니다. Okta는 이 값을 사용자가 멤버인 그룹의 이름과 비교하여 management center에 일치하는 그룹 이름을 전송합니다. 그다음 management center는 Okta에 대한 사용자 역할 매핑 구성 Management Center, on page 153의 6단계에서 각 management center 사용자 역할에 할당한 정규식과 해당 그룹 이름을 비교합니다.

Okta 사용자 역할 매핑 예

다음 예에서와 같이 사용자 역할 매핑을 지원하기 위한 management center의 SSO 설정은 개별 사용자 및 그룹에 대해 동일합니다. 차이점은 Okta의 management center 서비스 제공자 애플리케이션 설정에 있습니다.

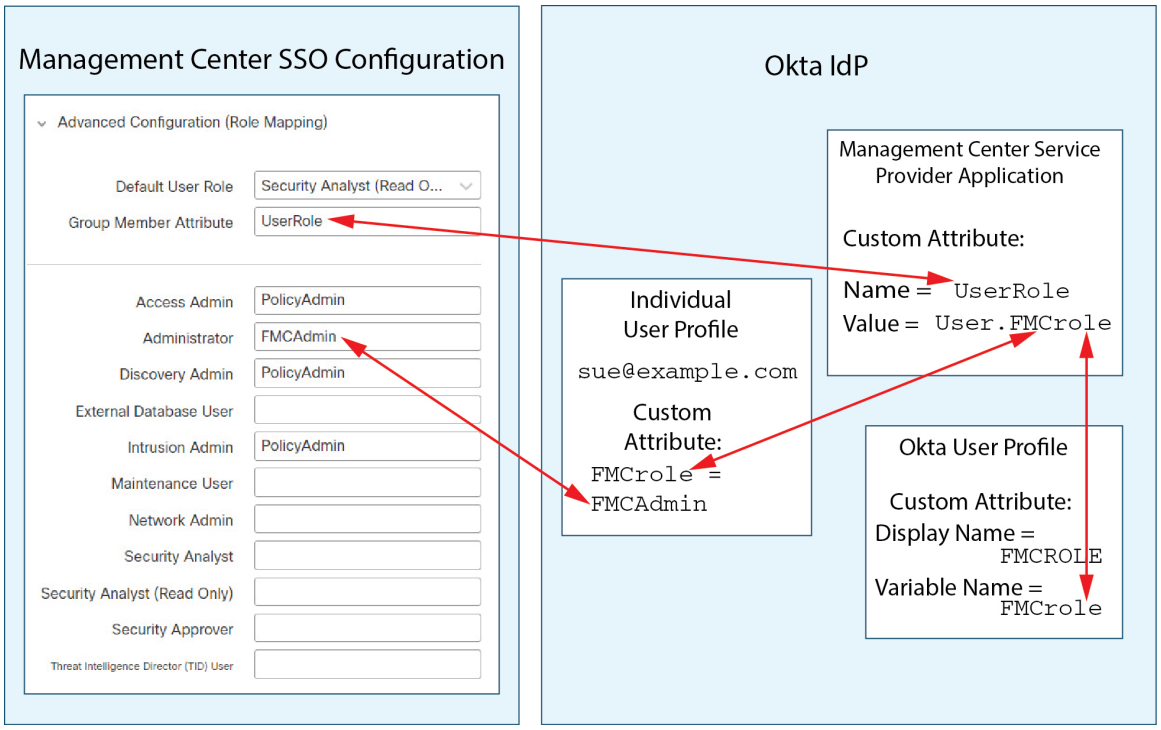
Note 개별 권한 또는 그룹 권한에 따라 management center 역할을 매핑하도록 설정할 수 있지만, 단일 management center 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. 또한 FMC는 management center에 설정된 management center 서비스 제공자 애플리케이션당 하나의 그룹 속성 명령문만 사용하여 그룹 역할 매핑을 지원할 수 있습니다.

개별 사용자 계정의 Okta 역할 매핑 예제

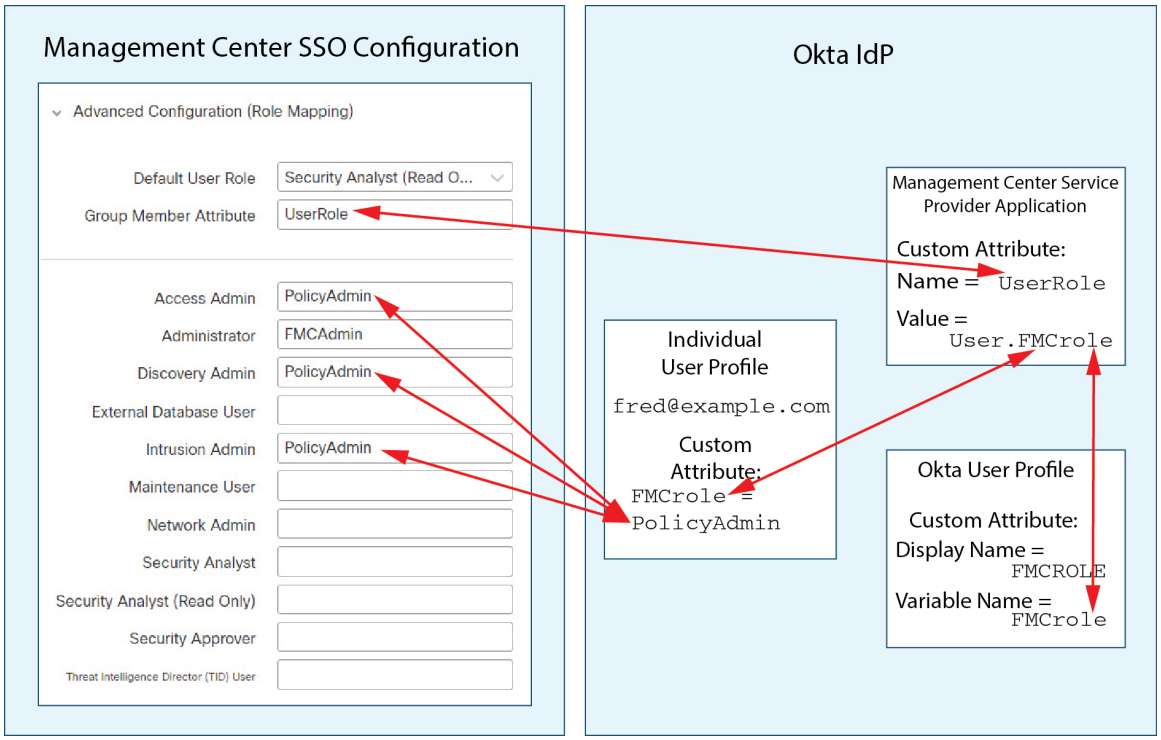
개별 사용자에 대한 역할 매핑에서 Okta management center 서비스 애플리케이션에는 management center의 그룹 멤버 속성 이름과 일치하는 이름을 갖는 사용자 지정 속성이 있습니다 (이 예에서는 `UserRole`). Okta의 사용자 프로파일에도 사용자 지정 속성이 있습니다(이 예에서는 `FMCrole`이라는 변수). 애플리케이션 사용자 지정 속성 `UserRole`에 대한 정의는 Okta가 사용자 역할 매핑 정보를 management center에 전달할 때 해당 사용자에게 할당된 사용자 지정 속성값을 사용하도록 설정합니다.

다음 다이어그램은 management center 및 Okta 설정의 관련 필드와 값이 개별 어카운트에 대한 사용자 역할 매핑에서 서로 어떻게 대응되는지를 보여줍니다. 각 다이어그램은 management center 및 Okta UI 관리 콘솔에서 동일한 SSO 설정을 사용하지만, Okta UI 관리 콘솔의 각 사용자에 대한 설정은 management center에서 서로 다른 방법으로 각 사용자에게 상이한 역할을 할당합니다.

- 이 다이어그램에서 sue@example.com은 `FMCrole` 값 `FMCAdmin`을 사용하며, management center는 관리자 역할을 할당합니다.



- 이 다이어그램에서 fred@example.com은 `FMCrole` 값 `PolicyAdmin`을 사용하며, management center는 액세스 관리자, 검색 관리자 및 침입 관리자 역할을 할당합니다.



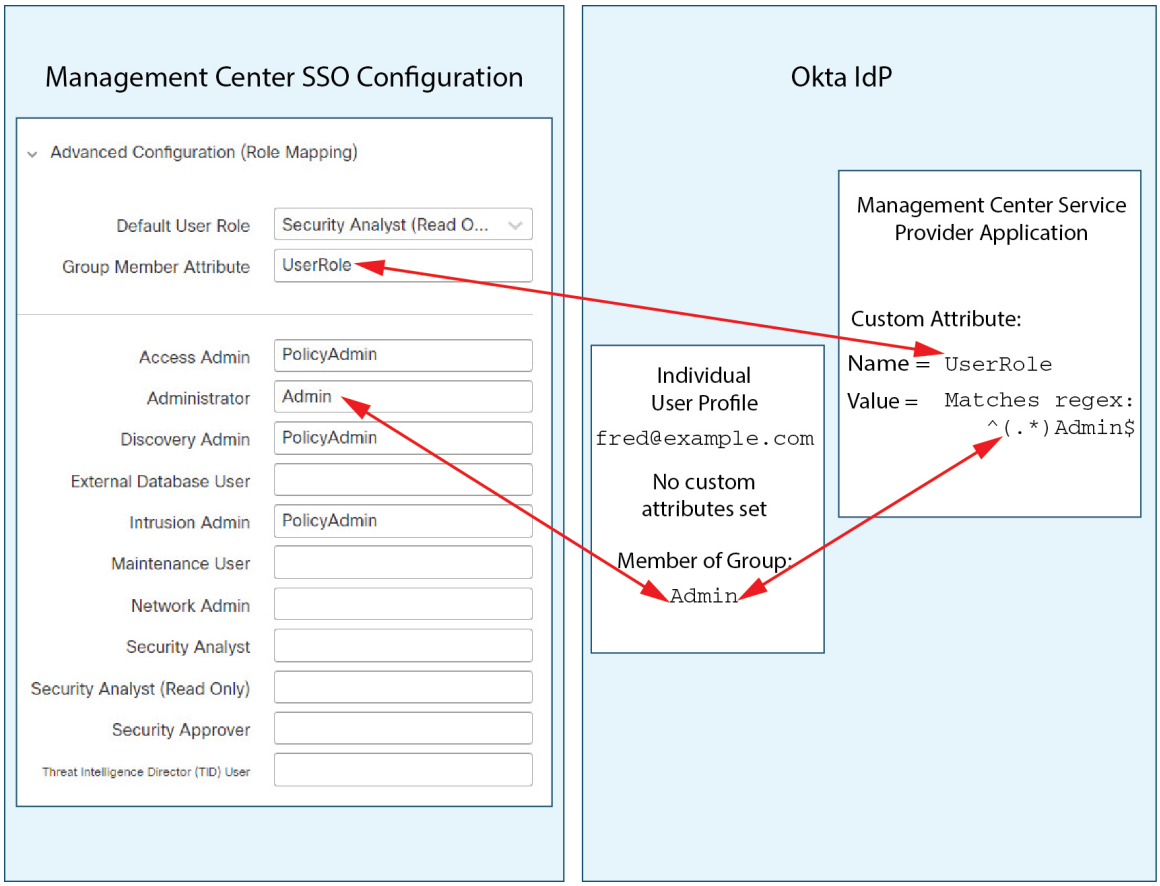
- management center를 위해 Okta 서비스 애플리케이션에 할당된 다른 사용자에게는 다음 중 하나의 이유로 기본 사용자 역할 보안 분석가(읽기 전용)가 할당됩니다.
  - Okta 사용자 프로파일에서 `FMCrole` 변수에 할당된 값이 없습니다.
  - Okta 사용자 프로필에서 `FMCrole` 변수에 할당된 값이 management center의 SSO 설정에서 사용자 역할에 대해 구성된 식과 일치하지 않습니다.

그룹에 대한 **Okta** 역할 매핑 예

그룹에 대한 역할 매핑에서 Okta management center 서비스 애플리케이션에는 management center의 그룹 멤버 속성의 이름(이 예에서는 `UserRole`)과 일치하는 이름을 갖는 사용자 지정 그룹 속성이 있습니다. Okta는 management center SSO 로그인 요청을 처리할 때 사용자의 그룹 멤버십을 서비스 management center 애플리케이션 그룹 속성(이 경우에는 `^(.*)Admin$`)에 할당된 식과 비교합니다. Okta는 그룹 속성과 일치하는 사용자의 그룹 멤버십을 management center에게 전송합니다. management center에서는 수신하는 그룹 이름을 각 사용자 역할에 대해 구성한 정규식과 비교하고 그에 따라 사용자 역할을 할당합니다.

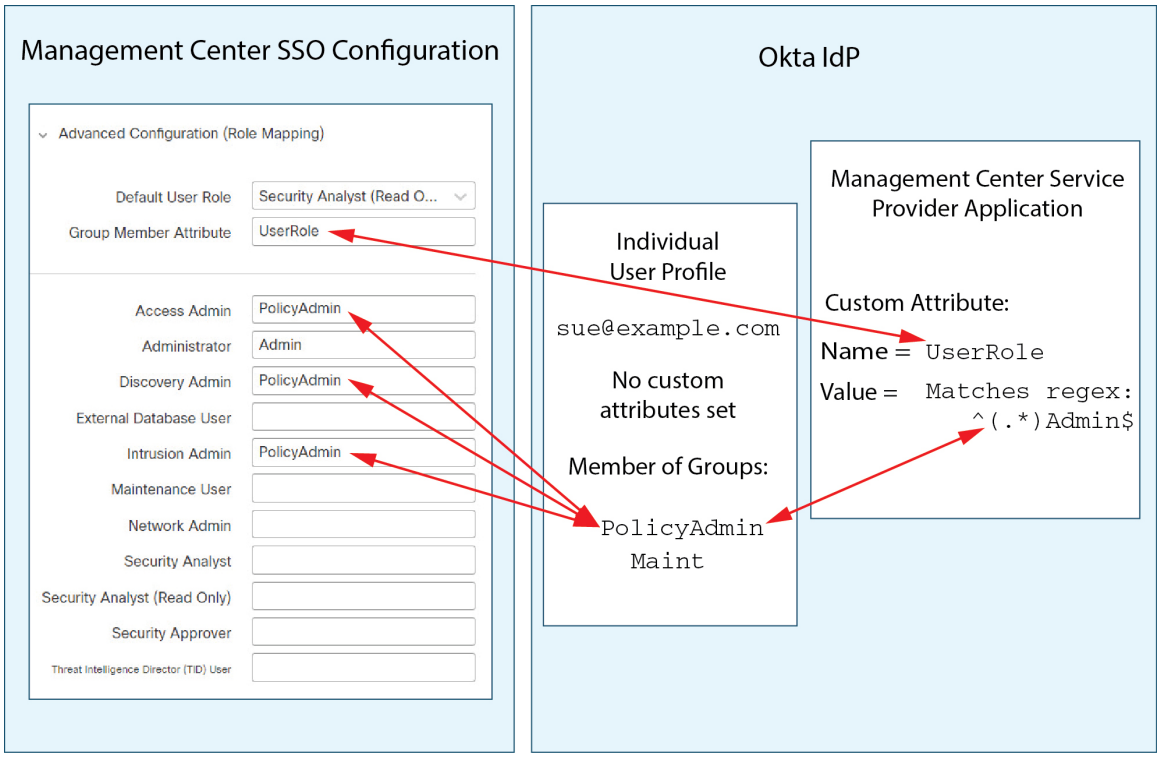
다음 다이어그램은 management center 및 Okta 구성의 관련 필드와 값이 그룹에 대한 사용자 역할 매핑에서 서로 어떻게 일치하는지를 보여줍니다. 각 다이어그램은 management center 및 Okta UI 관리 콘솔에서 동일한 SSO 설정을 사용하지만, Okta UI 관리 콘솔의 각 사용자에 대한 설정은 management center에서 서로 다른 방법으로 각 사용자에게 상이한 역할을 할당합니다.

- 이 다이어그램에서 fred@example.com은 Okta IdP 그룹 `Admin`의 멤버이며 `^ (.*)Admin$` 식과 일치합니다. Okta는 management center Fred의 `관리자` 그룹 멤버십을 전송하고 management center는 관리자에게 관리자 역할을 할당합니다.

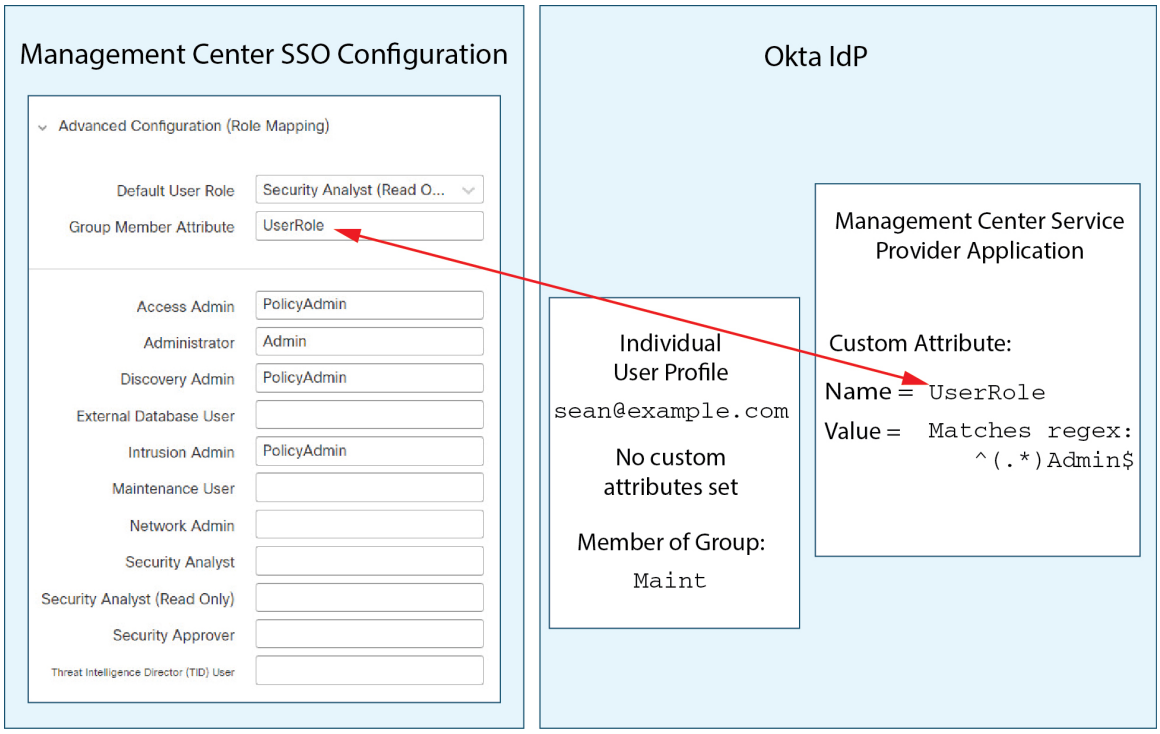


- 이 다이어그램에서 sue@example.com은 `^(.*)Admin$` 식과 일치하는 Okta IdP 그룹 `PolicyAdmin`의 멤버입니다. Okta는 management center Sue의 `PolicyAdmin` 그룹 멤버십을 전송하고 management center에서 Access Admin, Discovery Admin 및 Intrusion Admin 역할을 할당합니다.

  Sue는 Okta 그룹 `Maint`의 멤버이지만이 그룹 이름이 Okta management center 서비스 애플리케이션의 그룹 멤버십 속성에 할당된 식과 일치하지 않으므로 Okta는 Sue의 `Maint` 그룹 멤버십에 대한 정보를 management center에 전송하지 않습니다. `Maint` 그룹은 management center가 그녀에게 할당하는 역할에 참여하지 않습니다.



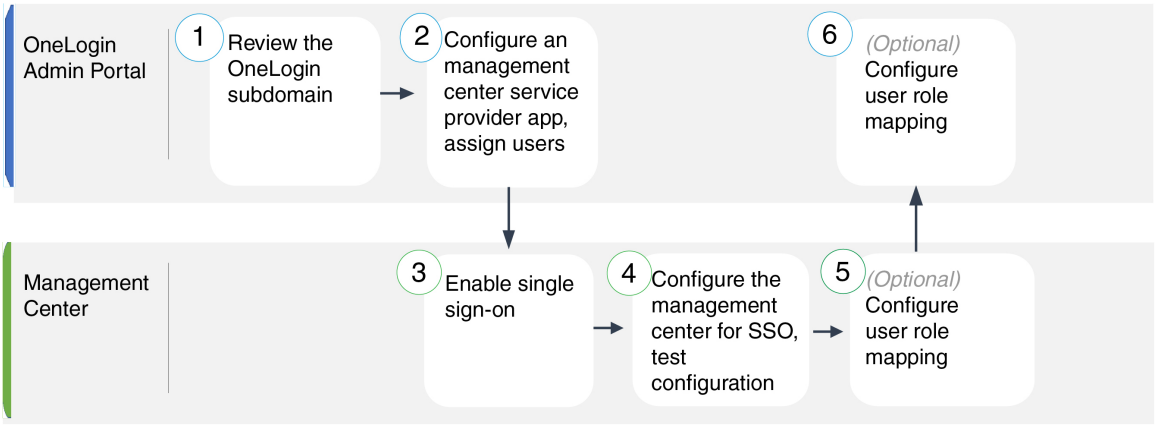
- 이 다이어그램에서 sean@example.com은 Okta IdP 그룹 `Maint`의 멤버입니다. 이 그룹 이름은 `^(.*)Admin$` 식과 일치하지 않습니다. 따라서 sean@example.com이 management center에 로그인하면 Okta는 `Maint` 그룹 멤버십에 대한 정보를 management center로 전송하지 않으며, Sean은 유지 보수 사용자 역할이 아닌(보안 분석가(읽기 전용)) 기본 사용자 역할(보안)을 할당 받습니다.



이 다이어그램은 역할 매핑 전략을 설정할 때 사전 계획의 중요성을 보여줍니다. 이 예에서는 `Maint` 그룹의 멤버인 이 management center에 대한 액세스 권한이 있는 모든 Okta 사용자에게 기본 사용자 역할만 할당할 수 있습니다. management center는 Okta 서비스 애플리케이션 구성에서 하나의 맞춤형 그룹 특성만 사용하도록 지원합니다. 해당 속성에 할당하는 식과 일치하도록 설정한 그룹 이름은 신중하게 작성해야 합니다. management center SSO 구성의 사용자 역할 할당 문자열에서 정규식을 사용하여 역할 매핑에 유연성을 추가할 수 있습니다. 각 management center 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다.

OneLogin으로 SSO(Single Sign-On) 구성

OneLogin을 사용하여 SSO를 구성하려면 다음 작업을 참조하십시오.



1	management center	OneLogin 하위 도메인 검토, on page 163
2	management center	OneLogin에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 164
3	OneLogin 관리 포털	Management Center에서 SSO(Single Sign-On) 활성화, on page 148
4	OneLogin 관리 포털	OneLogin SSO용 Management Center 구성, on page 165
5	OneLogin 관리 포털	Management Center에서 OneLogin 사용자 역할 매핑 구성, on page 167
6	management center	OneLogin IdP에서 사용자 역할 매핑 구성, on page 168

OneLogin 하위 도메인 검토

OneLogin에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션 디바이스 및 애플리케이션을 포함하는 엔티티를 하위 도메인이라고 합니다. OneLogin 하위 도메인에 management center를 추가하기 전에 해당 구성을 숙지하십시오. 다음 질문을 검토하십시오.

- management center에 액세스할 수 있는 사용자는 몇 명입니까?
- 사용자가 그룹의 OneLogin 하위 도메인 구성원 내에 있습니까?
- Active Directory, Google Apps 또는 LDAP와 같은 서드 파티 디렉터리의 사용자 및 그룹이 OneLogin 하위 도메인과 동기화됩니까?
- management center에서 SSO를 지원하려면 OneLogin 하위 도메인에 더 많은 사용자 또는 그룹을 추가해야 합니까?
- 어떤 종류의 management center 사용자 역할을 지정 하시겠습니까? (사용자 역할을 할당하지 않는 경우 management center가 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 필요한 사용자 역할 매핑을 지원하려면 OneLogin 하위 도메인 내의 사용자 및 그룹을 어떻게 구성해야 합니까?

개별 사용자 또는 그룹을 기준으로 매핑할 management center 역할을 구성할 수 있지만 단일 management center 애플리케이션이 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수는 없습니다.

이 문서에서는 사용자가 OneLogin 관리 포털에 대해 잘 알고 있으며 슈퍼 사용자 권한이 있는 계정을 가지고 있다고 가정합니다. 사용자 역할 매핑을 구성하려면 맞춤형 사용자 필드를 지원하는 OneLogin Unlimited 요금제를 구독해야 합니다. 자세한 내용은 온라인에서 사용 가능한 OneLogin 설명서를 참조하십시오.

OneLogin에 대한 Management Center 서비스 제공자 애플리케이션 구성

OneLogin 관리 포털에서 이 지침을 사용하여 OneLogin 내에 management center 서비스 공급자 애플리케이션을 생성하고 해당 애플리케이션에 사용자 또는 그룹을 할당합니다. SAML SSO 개념 및 OneLogin 관리 포털에 대해 숙지해야 합니다. 이 문서에서는 모든 기능을 갖춘 SSO 조직을 설정하는 데 필요한 모든 OneLogin 기능에 대해 설명하지는 않습니다. 예를 들어 사용자 및 그룹을 생성하거나 다른 사용자 관리 애플리케이션에서 사용자 및 그룹 정의를 가져오려면 OneLogin 문서를 참조하십시오.

Note management center 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note management center는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 OneLogin에서 management center로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- OneLogin 하위 도메인과 해당 사용자 및 그룹을 숙지하십시오. OneLogin 하위 도메인 검토, on page 163의 내용을 참조하십시오.
- 필요한 경우 OneLogin 하위 도메인에 사용자 계정을 생성합니다.

Note 시스템에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 management center에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이것이 IdP에 해당하는지 확인해야 합니다. IdP에서 통신 사업자 애플리케이션을 구성하고 management center에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 management center(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

Note 여러 URL로 management center 웹 인터페이스에 연결할 수 있는 경우 (예: 정규화된 도메인 이름 및 IP 주소) SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 management center에 일관되게 액세스해야 합니다.

Procedure

단계 **1** **SAML Test Connector (Advanced)**를 기본으로 사용하여 management center서비스 제공자 애플리케이션을 생성합니다.

단계 **2** 다음 설정으로 애플리케이션을 구성합니다.

- **Audience (Entity ID)(**대상**(**엔티티 **ID))**의 경우, `/saml/metadata` 문자열을 management center 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/metadata`
- **Recipient(**수신자**)**에 대해 management center 로그인 URL에 `/aml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **ACS(**소비자**) URL** 검사기의 경우 OneLogin에서 올바른 management center URL을 사용하고 있는지 확인하는 데 사용하는 식을 입력합니다. ACS URL을 사용하고 다음과 같이 변경하여 간단한 유효성 검사기를 만들 수 있습니다.
  - ACS URL의 시작 부분에 `^`를 추가합니다.
  - ACS URL의 끝에 `$`를 추가합니다.
  - ACS URL 내에서 모든 `/` 및 `?` 앞에 `\`를 삽입합니다.

  예를 들어, ACS URL `https://ExampleFMC/saml/acs`의 경우 적절한 URL 유효성 검사기는 `^https:\/\/ExampleFMC\/saml\/acs$`가 됩니다.
- **ACS(**소비자**) URL**의 경우 management center 로그인 URL에 `/saml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **Login URL(**로그인 **URL)**의 경우 management center 로그인 URL에 `/saml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **SAML Initiator(SAML** 개시자**)**에 대해 `Service Provider(통신 사업자)`를 선택합니다.

단계 **3** OneLogin 사용자를 management center 사업자 애플리케이션에 할당합니다.

단계 **4** (선택 사항) management center에서 SSO를 보다 쉽게 설정할 수 있도록 management center 서비스 공급자 애플리케이션용 SAML XML 메타 데이터를 OneLogin에서 로컬 컴퓨터로 다운로드할 수 있습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148의 내용을 참조하십시오.

OneLogin SSO용 Management Center 구성

management center 웹 인터페이스에서 다음 지침을 사용하십시오.

Before you begin

- OneLogin 관리 포털에서 management center 서비스 제공자 애플리케이션을 생성합니다. OneLogin에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 164의 내용을 참조하십시오.
- SSO(Single Sign-On)을 활성화합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148의 내용을 참조하십시오.

Procedure

단계 **1** 이 단계는 Management Center에서 SSO(Single Sign-On) 활성화, on page 148에서 곧바로 이어집니다. **Configure OneLogin Metadata(OneLogin** 메타데이터 설정**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 설정 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. OneLogin 서비스 제공 애플리케이션에서 다음 SSO 설정 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**: OneLogin에서 **SAML 2.0** 엔드포인트**(HTTP)**를 입력합니다.
     - **ID** 제공자 발급자: OneLogin의 발급자 **URL**을 입력합니다.
     - **X.509** 인증서: OneLogin에서 **X.509** 인증서를 입력합니다.
- OneLogin에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우(OneLogin에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 164의 4단계), 파일을 management center에 업로드할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 management center의 SSO 설정과 OneLogin 서비스 제공자 애플리케이션 설정을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **5** 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 사용자 역할 매핑을 구성할 수 있습니다. Management Center에서 OneLogin 사용자 역할 매핑 구성, on page 167의 내용을 참조하십시오. 역할 매핑을 설정하지 않기로 선택하는 경우, 기본적으로 management center에 로그인하는 모든 SSO 사용자에게 Management Center에서 OneLogin 사용자 역할 매핑 구성, on page 167의 4단계에서 설정한 사용자 역할이 할당됩니다.

Management Center에서 OneLogin 사용자 역할 매핑 구성

management center 웹 인터페이스에서 사용자 역할 매핑을 구성할 수 있는 필드는 선택한 SSO 제공자와 상관없이 동일합니다. 그러나 구성하는 값의 경우, 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방식을 고려해야 합니다.

Before you begin

- OneLogin 사용자 및 그룹을 검토합니다. OneLogin 하위 도메인 검토, on page 163의 내용을 참조하십시오.
- management center에 대한 SSO 서비스 제공자 애플리케이션을 구성합니다. OneLogin에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 164를 참조하십시오.
- management center에서 SSO(Single Sign-On)를 활성화하고 설정합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148 및 OneLogin에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 164의 내용을 참조하십시오.

Procedure

단계 **1** 시스템 (⚙) > **Users(**사용자**)** > **SSO(Single Sign-On,** 단일 인증**)System(**시스템**)** > **Users(**사용자**)**를 선택합니다.

단계 **2** **Advanced Configuration (Role Mapping)(**고급 설정**(**역할 매핑**))**을 펼칩니다.

단계 **3** **Default User Role(**기본 사용자 역할**)** 드롭다운에서 management center 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **4** **Group Member Attribute(**그룹 멤버 속성**)**을 입력합니다. 이 문자열은 OneLogin의 management center 서비스 공급자 애플리케이션에서 역할 매핑에 대해 정의하는 사용자 지정 매개 변수의 필드 이름과 일치해야 합니다. (OneLogin IdP에서 개별 사용자에 대한 사용자 역할 매핑 구성, on page 168의 1단계 또는 OneLogin IdP에서 그룹에 대한 사용자 역할 매핑 구성, on page 169의 1단계 참조)

단계 **5** SSO 사용자에게 할당할 각 management center 사용자 역할 옆에 정규식을 입력합니다. management center에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 management center에 전송하는 사용자 역할 매핑 속성과 비교합니다. management center는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. OneLogin IdP에서 사용자 역할 매핑 구성, on page 168의 내용을 참조하십시오.

OneLogin IdP에서 사용자 역할 매핑 구성

개별 권한 또는 그룹 권한을 기반으로 Onelogin 관리 포털에서 SSO 사용자 역할 매핑을 설정할 수 있습니다.

- 개별 사용자 권한에 따라 매핑하려면 OneLogin IdP에서 개별 사용자에 대한 사용자 역할 매핑 구성, on page 168의 내용을 참조하십시오.
- 그룹 권한에 따라 매핑하려면 OneLogin IdP에서 그룹에 대한 사용자 역할 매핑 구성, on page 169의 내용을 참조하십시오.

SSO 사용자가 management center에 로그인하면 OneLogin은 OneLogin IdP에서 설정된 사용자 정의 사용자 필드에서 사용자 또는 그룹 역할 속성값을 management center에 제공합니다. management center에서는 해당 속성값을 SSO 설정의 각 management center 사용자 역할에 할당된 정규식과 비교하고, 일치하는 항목이 있는 모든 역할을 사용자에게 부여합니다. (일치 항목이 없으면 management center는 사용자에게 설정 가능한 기본 사용자 역할을 부여합니다.) 각 management center 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다. management center는 management center 사용자 역할 식과의 비교를 위해 동일한 표준을 사용하여 OneLogin에서 받은 속성값을 정규식으로 처리합니다.

Note 단일 management center는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. management center 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. management center는 OneLogin에 설정된 하나의 맞춤형 사용자 필드만 이용한 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 롤 매핑은 management center에 더 효율적입니다. OneLogin 하위 도메인 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

OneLogin IdP에서 개별 사용자에 대한 사용자 역할 매핑 구성

OneLogin 관리 포털을 사용하여 management center 서비스 제공자 애플리케이션 및 맞춤형 사용자 필드에 대한 맞춤형 파라미터를 생성합니다. 이는 SSO 로그인 프로세스 중에 OneLogin이 사용자 역할 정보를 management center에 전달할 수 있는 수단을 제공합니다.

Before you begin

- OneLogin 하위 도메인과 해당 사용자 및 그룹을 검토합니다. OneLogin 하위 도메인 검토, on page 163을 참조하십시오.
- OneLogin에서 management center 서비스 제공자 애플리케이션을 생성하고 구성합니다. OneLogin에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 164의 내용을 참조하십시오.
- Management Center에서 OneLogin 사용자 역할 매핑 구성, on page 167에 설명된 대로 SSO 사용자 역할 매핑을 구성합니다.

Procedure

단계 **1** management center 서비스 제공자 애플리케이션에 대한 맞춤형 매개 변수를 생성합니다.

- **Field Name(**필드 이름**)**의 경우 management center SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 이름을 사용합니다. (Management Center에서 OneLogin 사용자 역할 매핑 구성, on page 167의 4단계 참조)
- **Value(**값**)**에 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는 이 절차의 2단계에서 구성할 고객 사용자 필드의 이름과 일치해야 합니다.

단계 **2** management center 액세스 권한이 있는 각 OneLogin 사용자에 대한 사용자 역할 정보를 포함할 맞춤형 사용자 필드를 만듭니다.

- **Name(**이름**)** 필드의 경우 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는 이 절차의 1단계에 설명된 애플리케이션 맞춤형 매개 변수에 대해 제공된 값과 일치해야 합니다.
- **Short name(**축약 이름**)**의 경우 필드의 축약된 대체 이름을 제공합니다. (이는 OneLogin 프로그래밍 인터페이스에 사용됩니다.)

단계 **3** management center 서비스 제공자 애플리케이션에 대한 액세스 권한이 있는 각 사용자에 대해 이 절차의 2단계에서 생성한 맞춤형 사용자 필드에 값을 할당합니다.

사용자가 SSO를 사용하여 management center에 로그인할 때 해당 사용자에 대해 이 필드에 할당하는 값은 management center이(가) SSO 구성에서 management center 사용자 역할에 할당한 식과 비교하는 값입니다. (Management Center에서 OneLogin 사용자 역할 매핑 구성, on page 167의 5단계 참조)

What to do next

- 다양한 계정에서 SSO를 사용하여 management center에 로그인하고 사용자에게 예상대로 management center 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

OneLogin IdP에서 그룹에 대한 사용자 역할 매핑 구성

OneLogin 관리 포털을 사용하여 management center 서비스 제공자 애플리케이션 및 맞춤형 사용자 필드에 대한 맞춤형 파라미터를 생성합니다. OneLogin 사용자를 그룹에 할당합니다. 그런 다음 맞춤형 사용자 필드와 사용자 그룹 간에 하나 이상의 매핑을 생성하여 OneLogin이 사용자의 그룹 멤버십을 기반으로 맞춤형 사용자 필드에 값을 할당하도록 합니다. 이는 SSO 로그인 프로세스 중에 OneLogin이 그룹 기반 사용자 역할 정보를 management center에 전달할 수 있는 수단을 제공합니다.

OneLogin 서비스 제공자 애플리케이션은 다음 두 가지 유형의 그룹 중 하나를 사용할 수 있습니다.

- OneLogin 기본 그룹.
- Active Directory, Google Apps 또는 LDAP와 같은 서드 파티 애플리케이션에 동기화된 그룹입니다.

management center 그룹 역할 매핑을 위해 그룹 유형 중 하나를 사용할 수 있습니다. 이 문서에서는 OneLogin 그룹을 사용한 역할 매핑에 대해 설명합니다. 서드파티 애플리케이션 그룹을 사용하려면 사용자의 조직에서 사용하고 있는 서드파티 사용자 관리 애플리케이션을 숙지해야 합니다. 자세한 내용은 OneLogin 문서를 참고하십시오.

Before you begin

- OneLogin 하위 도메인과 해당 사용자 및 그룹을 검토합니다. OneLogin 하위 도메인 검토, on page 163을 참조하십시오.
- OneLogin에서 management center 서비스 제공자 애플리케이션을 생성하고 구성합니다. OneLogin에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 164의 내용을 참조하십시오.
- Management Center에서 OneLogin 사용자 역할 매핑 구성, on page 167에 설명된 대로 SSO 사용자 역할 매핑을 구성합니다.

Procedure

단계 **1** management center 서비스 제공자 애플리케이션에 대한 맞춤형 매개 변수를 생성합니다.

- **Field Name(**필드 이름**)**의 경우 management center SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 이름을 사용합니다. (Management Center에서 OneLogin 사용자 역할 매핑 구성, on page 167의 4단계 참조)
- **Value(**값**)**에 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는 이 절차의 2단계에서 구성할 고객 사용자 필드의 이름과 일치해야 합니다.

단계 **2** management center 액세스 권한이 있는 각 OneLogin 사용자에 대한 사용자 역할 정보를 포함할 맞춤형 사용자 필드를 만듭니다.

- **Name(**이름**)** 필드의 경우 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는 이 절차의 1단계에 설명된 애플리케이션 맞춤형 매개 변수에 대해 제공된 값과 일치해야 합니다.
- **Short name(**축약 이름**)**의 경우 필드의 축약된 대체 이름을 제공합니다. (이는 OneLogin 프로그래밍 인터페이스에 사용됩니다.)

단계 **3** 이 절차의 2단계에서 생성한 맞춤형 사용자 필드에 그룹 기반 값을 할당하려면 하나 이상의 사용자 필드 매핑을 만듭니다. 각 OneLogin 사용자 그룹에 올바른 management center 사용자 역할을 할당하는 데 필요한 수의 매핑을 생성합니다.

- 사용자 그룹 필드와 그룹 이름을 비교하여 매핑에 대해 하나 이상의 조건을 생성합니다.
- 여러 조건을 생성하는 경우 사용자 그룹이 매핑을 수행할 조건 중 하나 또는 모두와 일치해야 하는지 여부를 선택합니다.
- 매핑에 대한 **Action(**동작**)**을 생성해서 이 절차의 2단계에서 생성한 맞춤형 사용자 필드에 값을 할당합니다. **Name(**이름**)** 필드 그리고 사용자가 지정한 조건을 충족하는 모든 사용자에 대해 OneLogin이 맞춤형 사용자 필드에 할당하는 문자열을 제공합니다.

management center에서는 이 문자열을 Management Center에서 OneLogin 사용자 역할 매핑 구성, on page 167의 5단계에서 각 management center 사용자 역할에 할당한 식과 비교합니다.

- 변경을 완료하면 모든 매핑을 다시 적용합니다.

What to do next

- 다양한 계정에서 SSO를 사용하여 management center에 로그인하고 사용자에게 예상대로 management center 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

OneLogin 사용자 역할 매핑 예

다음 예에서와 같이 사용자 역할 매핑을 지원하기 위한 management center의 SSO 설정은 개별 사용자 및 그룹에 대해 동일합니다. 차이점은 OneLogin의 management center 서비스 제공자 애플리케이션 설정에 있습니다.

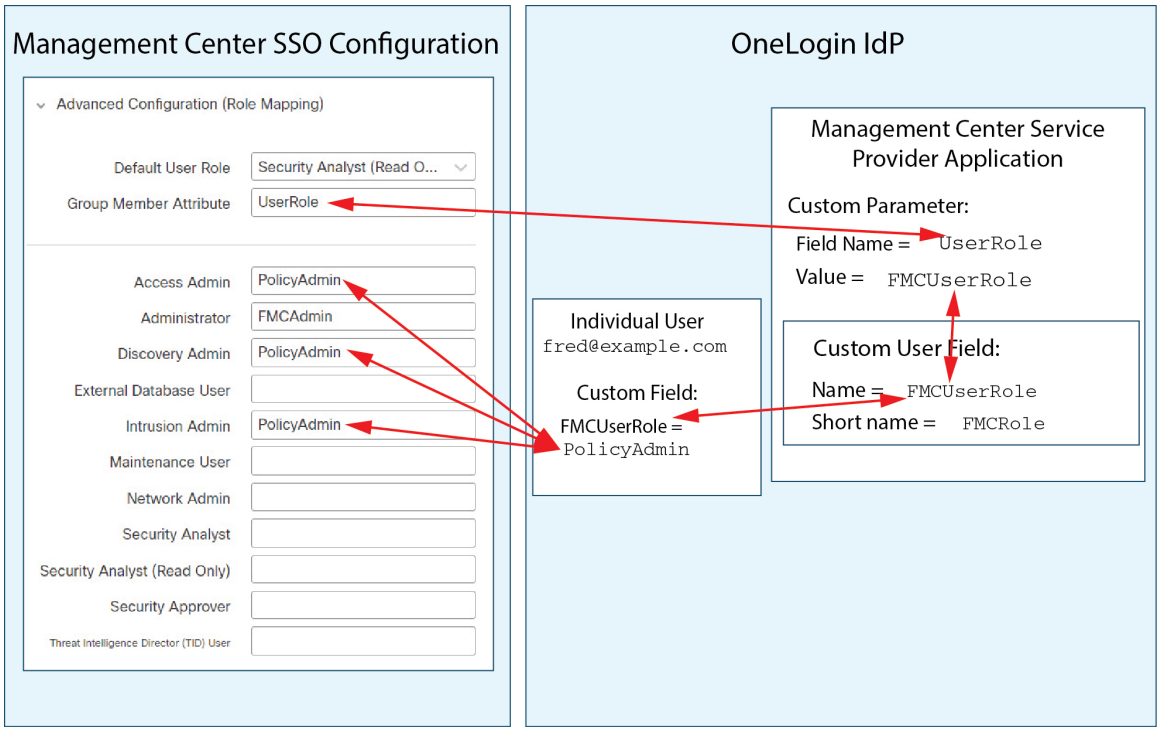
Note 단일 management center는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. management center 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. management center는 OneLogin에 설정된 하나의 맞춤형 사용자 필드만 이용한 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 롤 매핑은 management center에 더 효율적입니다. OneLogin 하위 도메인 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

개별 사용자 계정에 대한 OneLogin 역할 매핑 예

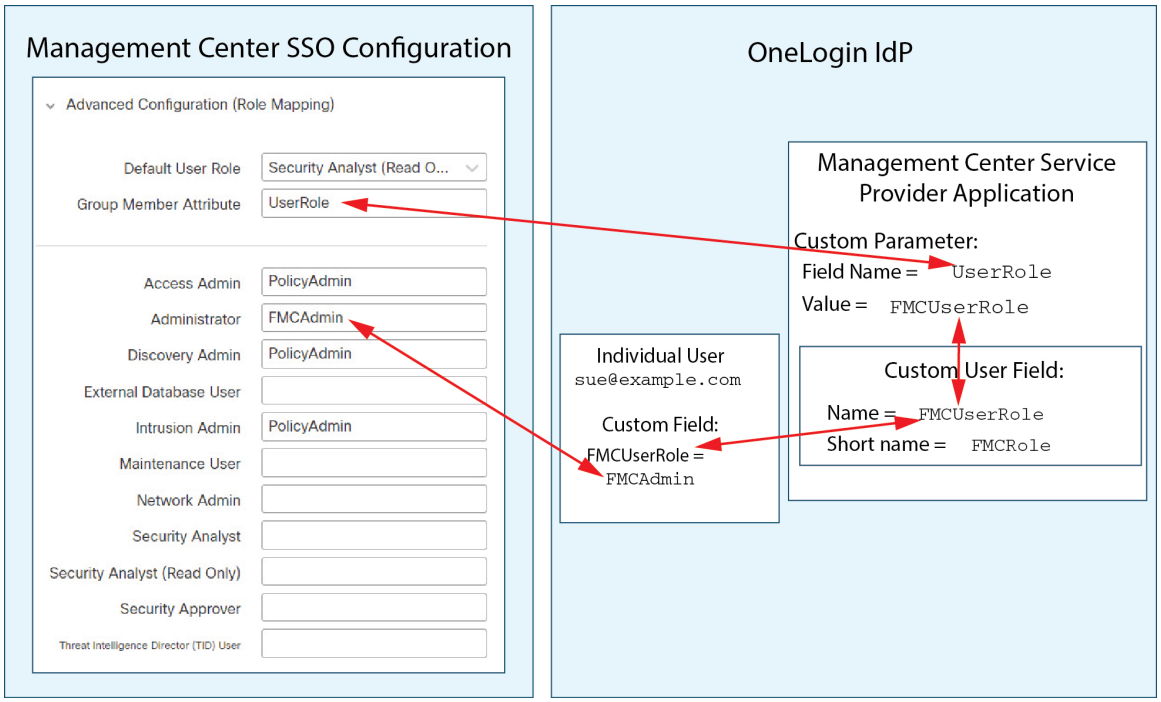
개별 사용자에 대한 역할 매핑에서 OneLogin management center 서비스 애플리케이션에는 management center의 그룹 멤버 속성 이름과 일치하는 이름을(이 예에서는 `UserRole`) 갖는 사용자 지정 속성이 있습니다. OneLogin에는 맞춤형 사용자 필드도 정의되어 있습니다(이 예에서는 `FMCUserRole`). 애플리케이션 사용자 지정 속성 `UserRole`에 대한 정의는 OneLogin이 사용자 역할 매핑 정보를 management center에 전달할 때 해당 사용자의 사용자 지정 필드 `FMCUserRole`의 값을 사용하도록 설정합니다.

다음 다이어그램은 management center 및 OneLogin 구성의 관련 필드와 값이 개별 계정에 대한 사용자 역할 매핑에서 서로 어떻게 대응하는지를 보여줍니다. 각 다이어그램은 management center 및 OneLogin 관리 포털에서 동일한 SSO 구성을 사용하지만, OneLogin 관리 포털의 각 사용자에 대한 구성은 각 사용자에게 management center에서 서로 다른 역할을 할당하기 위해서 달라집니다.

- 이 다이어그램에서 fred@example.com은 `FMCUserrole` 값 `PolicyAdmin`을 사용하며, management center는 액세스 관리자, 검색 관리 및 침입 관리자 역할을 할당합니다.



- 이 다이어그램에서 sue@example.com은 `FMCUserRole` 값 `FMCAdmin`을 사용하며, management center는 관리자 역할을 할당합니다.



- 이 management center를 위해 OneLogin 서비스 애플리케이션에 할당된 다른 사용자에게는 다음 중 하나의 이유로 기본 사용자 역할 보안 분석(읽기 전용)이 할당됩니다.

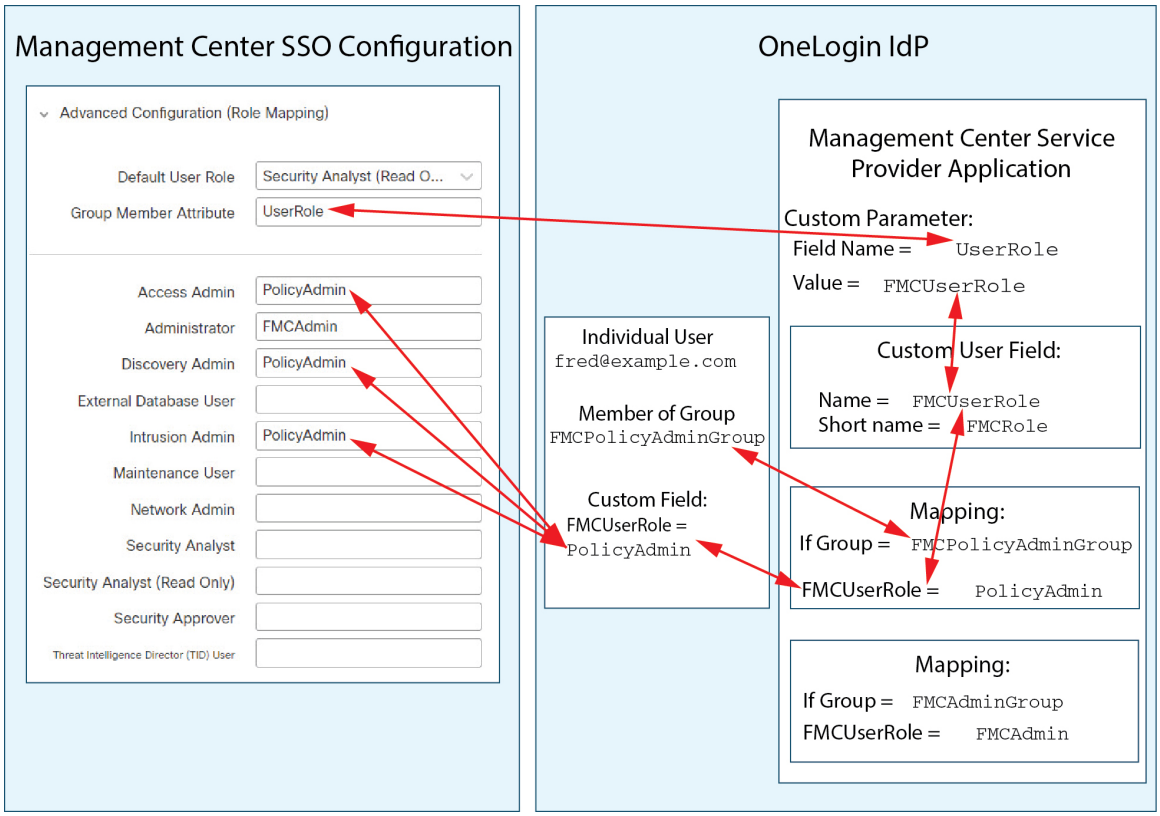
- `FMCUserRole` 맞춤형 사용자 필드에 할당된 값이 없습니다.
- `FMCUserRole` 맞춤형 사용자 필드에 할당된 값이 management center의 SSO 구성에서 사용자 역할에 대해 구성된 식과 일치하지 않습니다.

그룹에 대한 **OneLogin** 역할 매핑 예

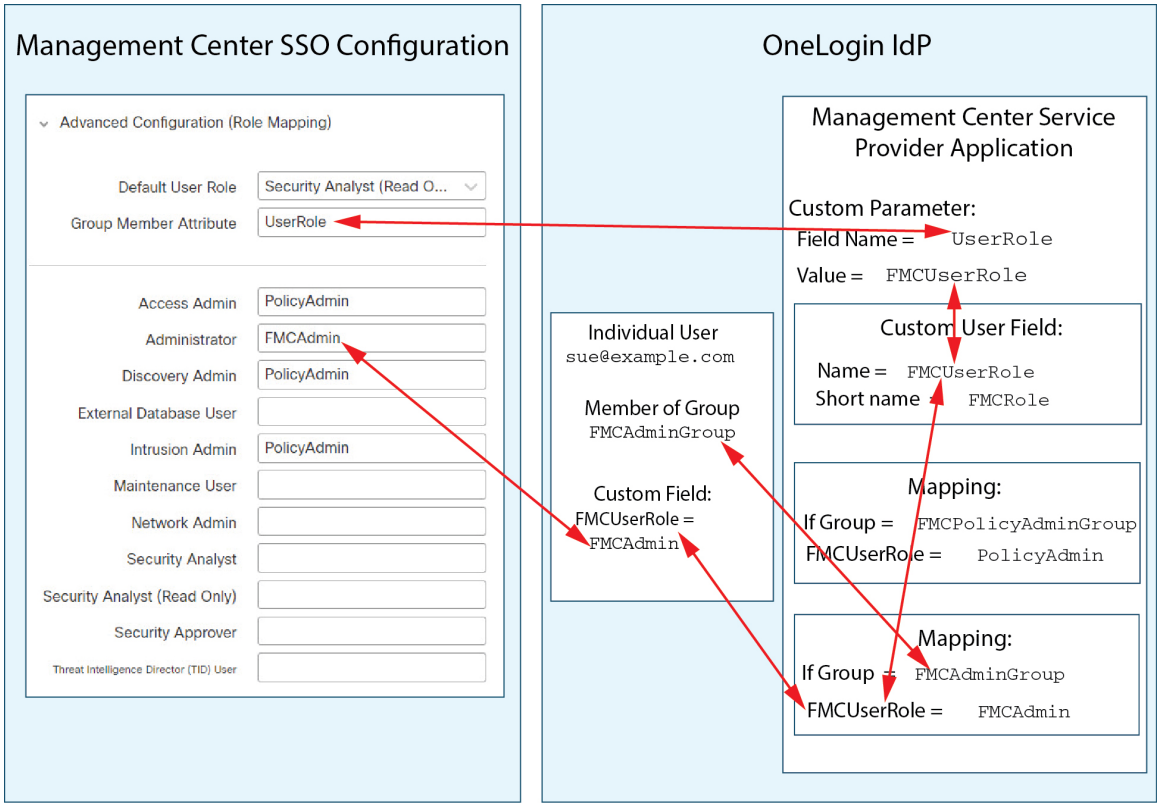
그룹에 대한 역할 매핑에서 OneLogin management center 서비스 애플리케이션에는 management center의 그룹 멤버 속성의 이름(이 예에서는 `UserRole`)과 일치하는 이름을 갖는 사용자 지정 매개 변수가 있습니다. OneLogin에는 맞춤형 사용자 필드도 정의되어 있습니다(이 예에서는 `FMCUserRole`). 애플리케이션 사용자 지정 속성 `UserRole`에 대한 정의는 OneLogin이 사용자 역할 매핑 정보를 management center에 전달할 때 해당 사용자의 사용자 지정 필드 `FMCUserRole`의 값을 사용하도록 설정합니다. 사용자 그룹 매핑을 지원하려면 OneLogin 내에서 매핑을 설정하여 해당 사용자의 OneLogin 그룹 멤버십을 기반으로 각 사용자의 `FMCUserRole` 필드에 값을 할당해야 합니다.

다음 다이어그램은 management center 및 OneLogin 구성의 관련 필드와 값이 그룹에 대한 사용자 역할 매핑에서 서로 어떻게 일치 하는지를 보여줍니다. 각 다이어그램은 management center 및 OneLogin 관리 포털에서 동일한 SSO 구성을 사용하지만, OneLogin 관리 포털의 각 사용자에 대한 구성은 각 사용자에게 management center에서 서로 다른 역할을 할당하기 위해서 달라집니다.

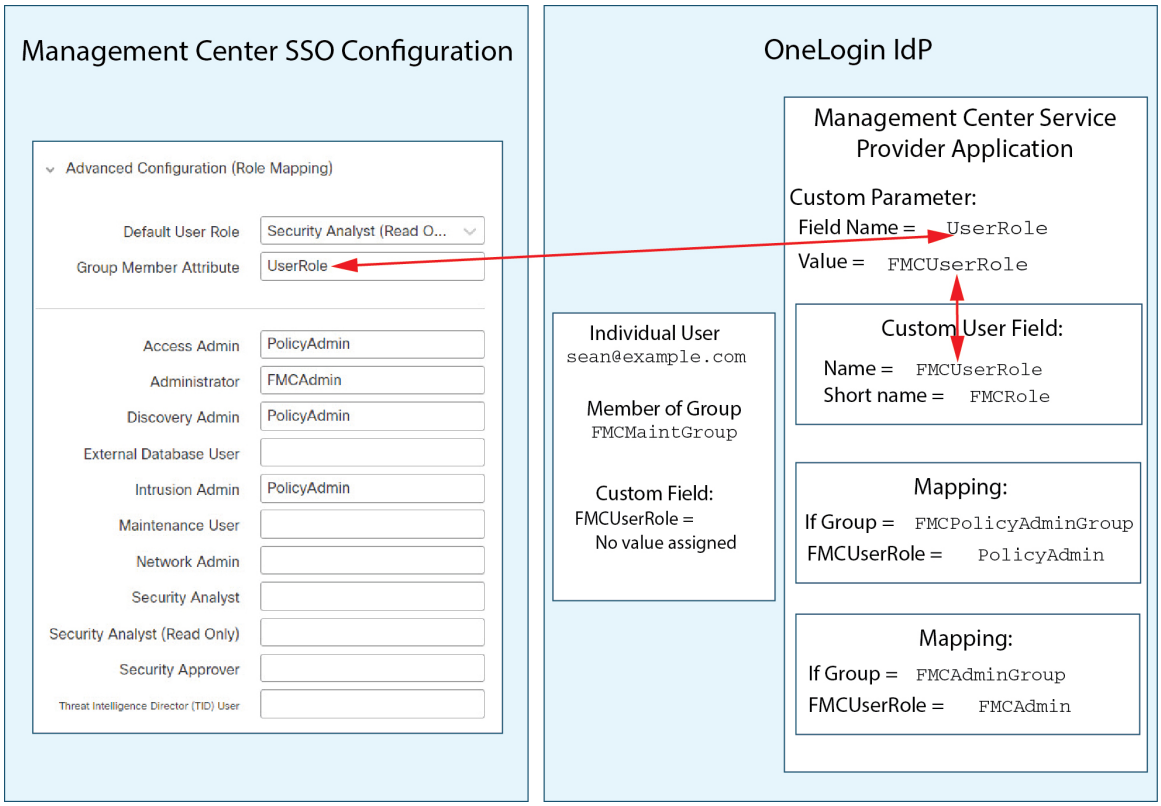
- 이 다이어그램에서 fred@example.com은 OneLogin IdP 그룹 `FMCPolicyAdminGroup`의 멤버입니다. OneLogin 매핑은 `PolicyAdmin` 값을 `FMCPolicyAdminGroup` 멤버에 대한 맞춤형 사용자 필드 `FMCUserRole`에 할당합니다. management center에서는 프레드 및 `FMCPolicyAdminGroup`의 다른 멤버에게 Access Admin, Discovery Admin 및 Intrusion Admin 역할을 할당합니다.



- 이 다이어그램에서 sue@example.com은 OneLogin IdP 그룹 `FMCAdminGroup`의 멤버입니다. OneLogin 매핑은 FMCAdmin 값을 `FMCPolicyAdminGroup` 멤버에 대한 맞춤형 사용자 필드 `FMCUserRole`에 할당합니다. management center는 Sue 및 `FMCAdminGroup`의 다른 멤버에게 관리자 역할을 할당합니다.

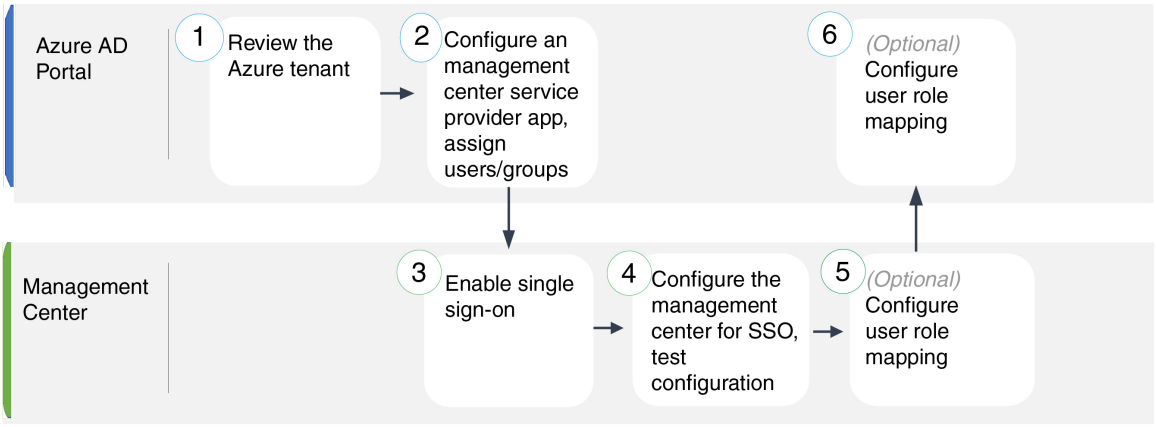


- 이 다이어그램에서 sean@example.com은 Idp 그룹 `FMCMaintGroup`의 멤버입니다. 이 그룹과 연결된 OneLogin 매핑이 없으므로 OneLogin은 사용자 지정 사용자 필드 `FMCUserRole`에 대해 값을 할당하지 않습니다. management center에서는 유지 보수 사용자 역할이 아닌 기본 사용자 역할(보안 분석가 (읽기 전용))을 할당합니다.



Azure AD로 SSO(Single Sign-On, 단일 인증) 구성

Azure를 사용하여 SSO를 설정하려면 다음 작업을 참조하십시오.



1	Azure AD 포털	Azure 테넌트 검토, on page 176
2	Azure AD 포털	Azure용 Management Center 서비스 제공자 애플리케이션 구성, on page 176

3	management center	Management Center에서 SSO(Single Sign-On) 활성화, on page 148
4	management center	Azure SSO용 Management Center 구성, on page 179
5	management center	Management Center에서 Azure에 대한 사용자 역할 매핑 구성, on page 180
6	Azure AD 포털	Azure IdP에서 사용자 역할 매핑 구성, on page 181

Azure 테넌트 검토

Azure AD는 Microsoft의 멀티 테넌트 클라우드 기반 ID 및 액세스 관리 서비스입니다. Azure에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션된 디바이스를 포함하는 엔터티를 테넌트라고 합니다. Azure 테넌트에 management center를 추가하기 전에 해당 조직에 대해 잘 알고 있어야 합니다. 다음 질문을 고려해보십시오.

- management center에 액세스할 수 있는 사용자는 몇 명입니까?
- 사용자가 그룹의 Azure 테넌트 구성원 내에 있습니까?
- 사용자 및 그룹이 다른 디렉토리 제품입니까?
- management center에서 SSO를 지원하려면 Azure 테넌트에 더 많은 사용자 또는 그룹을 추가해야 합니까?
- 어떤 종류의 management center 사용자 역할을 지정 하시겠습니까? (사용자 역할을 할당하지 않는 경우 management center가 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 필요한 사용자 역할 매핑을 지원하려면 Azure 테넌트 내의 사용자 및 그룹을 어떻게 구성해야합니까?
- 개별 사용자 또는 그룹을 기준으로 매핑할 management center 역할을 구성할 수 있지만 단일 management center 애플리케이션이 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수는 없습니다.

이 문서에서는 사용자가 이미 Azure Active Directory 포털에 익숙하며 Azure AD 테넌트에 대한 애플리케이션 관리자 권한이 있는 계정을 가지고 있다고 가정합니다. management center는 테넌트별 단일 로그인 및 단일 로그 아웃 엔드포인트에서만 Azure SSO를 지원합니다. Azure AD Premium P1 이상 라이선스 및 전역 관리자 권한이 있어야 합니다. 자세한 내용은 Azure 설명서를 참조하십시오.

Azure용 Management Center 서비스 제공자 애플리케이션 구성

Azure Active Directory 포털을 사용하여 Azure Active Directory 테넌트 내에 management center 서비스 제공자 애플리케이션을 만들고 기본 구성 설정을 구성합니다.

Note management center 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note management center는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 OneLogin에서 management center로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- Azure 테넌트와 해당 사용자 및 그룹을 숙지하십시오. Azure 테넌트 검토, on page 176 참조하십시오.
- 필요한 경우 Azure 테넌트에서 사용자 계정 및/또는 그룹을 생성합니다.

Note 시스템에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 management center에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이것이 IdP에 해당하는지 확인해야 합니다. IdP에서 통신 사업자 애플리케이션을 구성하고 management center에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 management center(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

Note 여러 URL(예: 정규화된 도메인 이름 및 IP 주소)로 management center 웹 인터페이스에 연결할 수 있는 경우, SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 management center에 일관되게 액세스해야 합니다.

Procedure

단계 **1** Azure AD SAML 툴킷을 기본으로 사용하여 management center 서비스 제공자 애플리케이션을 생성합니다.

단계 **2** 기본 **SAML** 구성에 대한 다음 설정을 사용하여 애플리케이션을 구성합니다.

- **Identifier(**엔티티 **ID)**의 경우, `/saml/metadata` 문자열을 management center 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/metadata`

- 회신 **URL(**어설션 소비자 서비스 **URL)**의 경우 `/saml/acs` 문자열을 management center 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **URL** 로그인의 경우 `/sam/acs` 문자열을 management center 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/acs`

단계 **3** management center에서 로그인을 위한 사용자 이름을 사용자 계정과 연결된 이메일 주소로 지정하도록 애플리케이션의 고유 사용자 식별자 이름**(**이름 **ID)** 클레임을 편집합니다.

- **Source(**소스**)**에 대해 `Attribute(속성)`를 선택합니다.
- 소스 속성의 경우: `user.mail`을 선택합니다.

단계 **4** management center에서 SSO를 보호하기 위한 인증서를 생성합니다. 인증서에 다음 옵션을 사용합니다.

- Signing option(서명 옵션)을 Sign SAML response and assertion(SAML 응답 및 어설션 서명)으로 변경합니다.
- Signing Algorithm(서명 알고리즘)으로 SHA-256을 선택합니다.

단계 **5** 인증서의 Base-64 버전을 로컬 컴퓨터에 다운로드합니다. management center 웹 인터페이스에서 Azure SSO를 구성할 때 필요합니다.

단계 **6** 애플리케이션의 SAML 기반 로그인 정보에서 다음 값을 확인합니다.

- 로그인 **URL**
- **Azure AD** 식별자

management center 웹 인터페이스에서 Azure SSO를 구성할 때 이러한 값이 필요합니다.

단계 **7** (선택 사항) management center에 SSO를 보다 쉽게 설정할 수 있도록 management center 서비스 제공자 애플리케이션(Azure 포털의 페더레이션 메타데이터 **XML**이라고 하는)의 SAML XML 메타데이터 파일을 로컬 컴퓨터에 다운로드할 수 있습니다.

단계 **8** 기존 Azure 사용자 및 그룹을 management center 서비스 애플리케이션에 할당합니다.

Note management center 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note 사용자 역할 매핑을 구성하려는 경우 개별 사용자 권한 또는 그룹 권한에 따라 역할을 매핑하도록 구성할 수 있지만 단일 management center 애플리케이션이 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수는 없습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148의 내용을 참조하십시오.

Azure SSO용 Management Center 구성

management center 웹 인터페이스에서 다음 지침을 사용하십시오.

Before you begin

- Azure AD 포털에서 management center 서비스 제공자 애플리케이션을 생성합니다. Azure용 Management Center 서비스 제공자 애플리케이션 구성, on page 176의 내용을 참조하십시오.
- SSO(Single Sign-On)을 활성화합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148의 내용을 참조하십시오.

Procedure

단계 **1** 이 단계는 Management Center에서 SSO(Single Sign-On) 활성화, on page 148에서 곧바로 이어집니다. **Configure Azure Metadata(Azure** 메타 데이터 구성**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 설정 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. Azure SSO 서비스 제공자 애플리케이션에서 검색한 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**의 경우 Azure용 Management Center 서비스 제공자 애플리케이션 구성, on page 176의 6단계에서 적어둔 로그인 **URL**을 입력합니다.
     - **Identity Provider Issuer(ID** 공급자 발급자**)**에 대해 Azure용 Management Center 서비스 제공자 애플리케이션 구성, on page 176의 6단계에서 적어둔 **Azure AD** 식별자를 입력합니다.
     - **X.509** 인증서의 경우 Azure용 Management Center 서비스 제공자 애플리케이션 구성, on page 176의 5단계에서 Azure에서 다운로드한 인증서를 사용합니다. (텍스트 편집기를 사용하여 인증서 파일을 열고 내용을 복사하여 **X.509 Certificate(X.509** 인증서**)** 필드에 붙여 넣습니다.)
- Azure에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우(Azure용 Management Center 서비스 제공자 애플리케이션 구성, on page 176의 7단계) 파일을 management center에 업로드할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 management center의 SSO 구성과 Azure 서비스 제공자 애플리케이션을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **5** 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 역할 매핑을 구성할 수 있습니다. Management Center에서 Azure에 대한 사용자 역할 매핑 구성, on page 180의 내용을 참조하십시오. 역할 매핑을 구성하지 않도록 선택하는 경우, 기본적으로 management center에 로그인하는 모든 SSO 사용자에게 Management Center에서 Azure에 대한 사용자 역할 매핑 구성, on page 180의 4단계에서 구성한 기본 사용자 역할이 할당됩니다.

Management Center에서 Azure에 대한 사용자 역할 매핑 구성

management center 웹 인터페이스에서 사용자 역할 매핑을 구성할 수 있는 필드는 선택한 SSO 제공자와 상관없이 동일합니다. 그러나 구성하는 값의 경우, 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방식을 고려해야 합니다.

Before you begin

- 기존 Azure 사용자 및 그룹을 검토합니다. Azure 테넌트 검토, on page 176을 참조하십시오.
- management center에 대한 SSO 서비스 제공자 애플리케이션을 구성합니다. Azure용 Management Center 서비스 제공자 애플리케이션 구성, on page 176를 참조하십시오.
- management center에서 SSO(Single Sign-On)를 활성화하고 설정합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148 및 Azure SSO용 Management Center 구성, on page 179의 내용을 참조하십시오.

Procedure

단계 **1** **System(**시스템**)** > **Users(**사용자**)**를 선택합니다.

단계 **2** **Single Sign-On(**단일 인증**)** 탭을 클릭합니다.

단계 **3** **Advanced Configuration (Role Mapping)(**고급 구성**(**역할 매핑**))**을 펼칩니다.

단계 **4** **Default User Role(**기본 사용자 역할**)** 드롭다운에서 management center 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **5** **Group Member Attribute(**그룹 멤버 속성**)**을 입력합니다. 이 문자열은 Azure의 management center 서비스 제공자 애플리케이션에 대해 생성하는 사용자 클레임의 이름과 일치해야 합니다. Azure IdP에서 개별 사용자의 사용자 역할 매핑 구성, on page 181의 1 단계 또는 Azure IdP에서 그룹용 사용자 역할 매핑 구성, on page 183의 1 단계를 참조하십시오.

단계 **6** SSO 사용자에게 할당할 각 management center 사용자 역할 옆에 정규식을 입력합니다. (management center는 Golang 및 Perl에서 지원하는 Google의 RE2 정규식 표준의 제한된 버전을 사용합니다.) management center에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 management center에 전송

하는 사용자 역할 매핑 속성값과 비교합니다. management center는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. Azure IdP에서 사용자 역할 매핑 구성, on page 181의 내용을 참조하십시오.

Azure IdP에서 사용자 역할 매핑 구성

개별 사용자 권한 또는 그룹 권한을 기반으로 Azure AD 포털에서 SSO 사용자 역할 매핑을 설정할 수 있습니다.

- 개별 사용자 권한을 기반으로 매핑하려면 Azure IdP에서 개별 사용자의 사용자 역할 매핑 구성을 참조하십시오.
- 그룹 권한을 기준으로 매핑하려면 Azure IdP에서 그룹용 사용자 역할 매핑 구성을 참조하십시오.

SSO 사용자가 management center에 로그인하면 Azure는 Azure AD 포털에 설정된 애플리케이션 역할에서 값을 얻는 사용자 또는 그룹 역할 속성값을 management center에 제공합니다. management center에서는 해당 속성값을 SSO 설정의 각 management center 사용자 역할에 할당된 정규식과 비교하고, 일치하는 항목이 있는 모든 역할을 사용자에게 부여합니다. (일치 항목이 없으면 management center는 사용자에게 설정 가능한 기본 사용자 역할을 부여합니다.) 각 management center 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다. management center는 management center 사용자 역할 식과의 비교를 위해 동일한 표준을 사용하여 Azure에서 받은 속성값을 정규식으로 처리합니다.

Note 단일 management center는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. management center 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. management center는 Azure에 설정된 하나의 클레임만 사용하여 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 롤 매핑은 management center에 더 효율적입니다. Azure 테넌트 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

Azure IdP에서 개별 사용자의 사용자 역할 매핑 구성

Azure에서 management center 서비스 애플리케이션의 개별 사용자에 대한 역할 매핑을 설정하려면 Azure AD Portal을 사용하여 애플리케이션에 클레임을 추가하고, 애플리케이션의 등록 매니페스트에 역할을 추가한 다음 사용자에게 역할을 할당합니다.

Before you begin

- Azure 테넌트를 검토합니다. Azure 테넌트 검토, on page 176의 내용을 참조하십시오.
- Azure에서 management center 서비스 제공자 애플리케이션 생성하고 구성합니다. Azure용 Management Center 서비스 제공자 애플리케이션 구성, on page 176의 내용을 참조하십시오.

- Management Center에서 Azure에 대한 사용자 역할 매핑 구성, on page 180에 설명된 대로 SSO 사용자 역할 매핑을 구성합니다.

Procedure

단계 **1** 다음 특성을 사용하여 management center 서비스 애플리케이션의 SSO 설정에 사용자 클레임을 추가합니다.

- **Name(**이름**)**: management center SSO 구성에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 문자열을 사용합니다. (Management Center에서 Azure에 대한 사용자 역할 매핑 구성, on page 180의 5단계 참조)
- 이름 식별자 형식: `Persistent(영구)`를 선택합니다.
- **Source(**소스**)**: `Attribute(속성)`를 선택합니다.
- **Source attribute(**소스 속성**)**: `user.assignedroles`를 선택합니다.

단계 **2** management center 서비스 애플리케이션의 매니페스트(JSON 형식)를 편집하고 애플리케이션 역할을 추가하여 SSO 사용자에게 할당할 management center 사용자 역할을 나타냅니다. 가장 간단한 방법은 기존 애플리케이션 역할 정의를 복사하고 다음 속성을 변경하는 것입니다.

- `displayName`: AD Azure Portal에 표시될 역할의 이름입니다.
- `description`: 역할에 대한 짧은 설명입니다.
- `Id`: 매니페스트 내의 ID 속성 중에서 고유해야 하는 영문숫자 문자열입니다.
- `value`: 하나 이상의 management center 사용자 역할을 나타내는 문자열입니다. (참고: Azure에서는 이 문자열에 공백을 허용하지 않습니다.)

단계 **3** management center 서비스 애플리케이션에 할당된 각 사용자에 대해 해당 애플리케이션의 매니페스트에 추가한 애플리케이션 역할 중 하나를 할당합니다. 사용자가 SSO를 사용하여 management center에 로그인할 때 해당 사용자에게 할당하는 애플리케이션 역할은 서비스 애플리케이션에 대한 클레임에서 Azure가 management center에 전송하는 값입니다. management center에서는 클레임을 SSO 설정에서 management center 사용자 역할에 할당한 식과 비교하고(Management Center에서 Azure에 대한 사용자 역할 매핑 구성, on page 180의 6단계 참조), 일치하는 모든 management center 사용자 역할을 사용자에게 할당합니다.

What to do next

- 다양한 계정에서 SSO를 사용하여 management center에 로그인하고 사용자에게 예상대로 management center 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

Azure IdP에서 그룹용 사용자 역할 매핑 구성

Azure에서 management center 서비스 애플리케이션의 사용자 그룹에 대한 역할 매핑을 설정하려면 Azure AD Portal을 사용하여 애플리케이션에 클레임을 추가하고, 애플리케이션의 등록 매니페스트에 역할을 추가한 다음 그룹에 역할을 할당합니다.

Before you begin

- Azure 테넌트를 검토합니다. Azure 테넌트 검토, on page 176의 내용을 참조하십시오.
- Azure에서 management center 서비스 제공자 애플리케이션 생성하고 구성합니다. Azure용 Management Center 서비스 제공자 애플리케이션 구성, on page 176의 내용을 참조하십시오.
- Management Center에서 Azure에 대한 사용자 역할 매핑 구성, on page 180에 설명된 대로 SSO 사용자 역할 매핑을 구성합니다.

Procedure

단계 **1** 다음 특성을 사용하여 management center 서비스 애플리케이션의 SSO 설정에 사용자 클레임을 추가합니다.

- **Name(**이름**)**: management center SSO 구성에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 문자열을 사용합니다. (Management Center에서 Azure에 대한 사용자 역할 매핑 구성, on page 180의 5단계 참조)
- 이름 식별자 형식: `Persistent(영구)`를 선택합니다.
- **Source(**소스**)**: `Attribute(속성)`를 선택합니다.
- **Source attribute(**소스 속성**)**: `user.assignedroles`를 선택합니다.

단계 **2** management center 서비스 애플리케이션의 매니페스트(JSON 형식)를 편집하고 애플리케이션 역할을 추가하여 SSO 사용자에게 할당할 management center 사용자 역할을 나타냅니다. 가장 간단한 방법은 기존 애플리케이션 역할 정의를 복사하고 다음 속성을 변경하는 것입니다.

- `displayName`: AD Azure Portal에 표시될 역할의 이름입니다.
- `description`: 역할에 대한 짧은 설명입니다.
- `Id`: 매니페스트 내의 ID 속성 중에서 고유해야 하는 영문숫자 문자열입니다.
- `value`: 하나 이상의 management center 사용자 역할을 나타내는 문자열입니다. (Azure에서는이 문자열에 공백을 허용하지 않습니다.)

단계 **3** management center 서비스 애플리케이션에 할당된 각 그룹에 대해 해당 애플리케이션의 매니페스트에 추가한 애플리케이션 역할 중 하나를 할당합니다. 사용자가 SSO를 사용하여 management center에 로그인할 때 해당 사용자 그룹에 할당하는 애플리케이션 역할은 서비스 애플리케이션에 대한 클레임에서 Azure가 management center에 전송하는 값입니다. management center에서는 클레임을 SSO 설정에서 management center 사용자 역할에 할당한 식과 비교하고 (Management Center에서 Azure에 대

한 사용자 역할 매핑 구성, on page 180의 6단계 참조), 일치하는 모든 management center 사용자 역할을 사용자에게 할당합니다.

What to do next

다양한 계정에서 SSO를 사용하여 management center에 로그인하고 사용자에게 예상대로 management center 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

Azure 사용자 역할 매핑 예

다음 예에서와 같이 사용자 역할 매핑을 지원하기 위한 management center의 SSO 설정은 개별 사용자 및 그룹에 대해 동일합니다. 차이점은 Azure의 FMC 서비스 제공자 애플리케이션 설정에 있습니다.

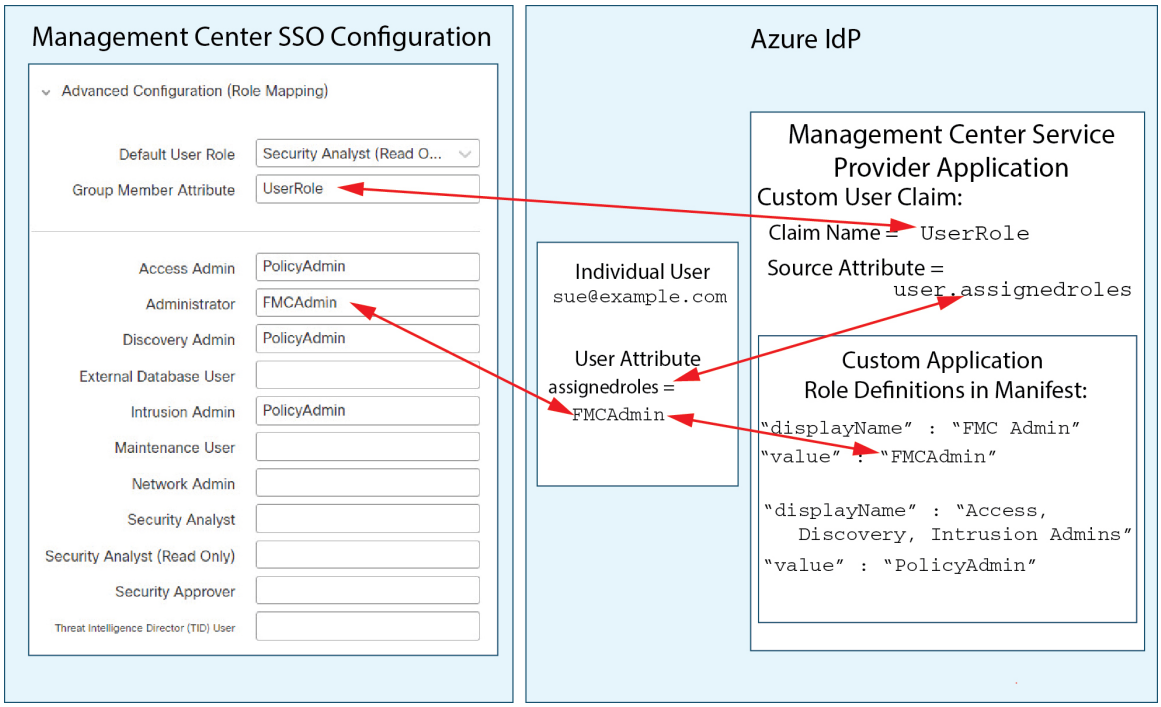
Note 개별 권한 또는 그룹 권한에 따라 management center 역할을 매핑하도록 설정할 수 있지만, 단일 FMC 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. management center는 Azure에 설정된 하나의 클레임만 사용하여 역할 매핑을 지원할 수 있습니다.

개별 사용자 계정에 대한 Azure 역할 매핑 예제

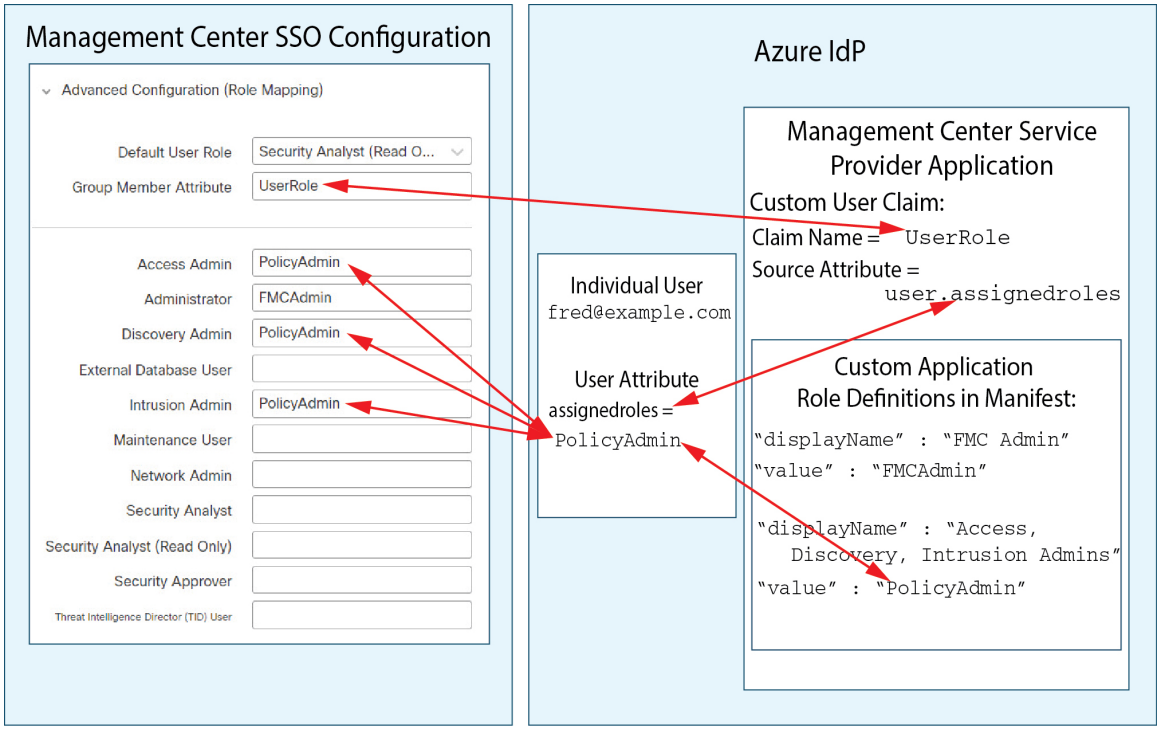
개별 사용자에 대한 역할 매핑에서 Azure management center 서비스 애플리케이션에는 매니페스트 내에 정의된 사용자 지정 역할이 있습니다. (이 경우에는 FMCAdmin 및 PolicyAdmin입니다.) 이러한 역할은 사용자에게 할당할 수 있습니다. Azure는 해당 사용자의 할당된 역할 속성에 각 사용자에 대한 역할 할당을 저장합니다. 애플리케이션에 맞춤형 사용자 클레임도 정의되어 있으며, 이 클레임은 SSO를 통해 FMC에 로그인하는 사용자에 대해 할당된 사용자 역할에서 해당 값을 가져오도록 설정됩니다. Azure는 SSO 로그인 프로세스 중에 management center에 클레임 값을 전달하고 management center에서는 클레임 값을 management centerSSO 설정의 각 management center 사용자 역할에 할당된 문자열과 비교합니다.

다음 다이어그램은 management center 및 Azure 설정의 관련 필드와 값이 개별 계정에 대한 사용자 역할 매핑에서 서로 어떻게 대응하는지를 보여줍니다. 각 다이어그램은 management center 및 Azure AD 포털에서 동일한 SSO 구성을 사용하지만, Azure AD 포털의 각 사용자에 대한 설정은 management center에서 각 사용자에게 서로 다른 역할을 할당하는 방식이 다릅니다.

- 이 다이어그램에서 sue@example.com은 assignedroles 속성값 `FMCAdmin`을 사용하며, management center는 management center 관리자 역할을 할당합니다.



- 이 다이어그램에서 fred@example.com은 assignedroles 속성값 `PolicyAdmin`을 사용하며 management center는 액세스 관리자, 검색 관리자 및 침입 관리자 역할을 할당합니다.



- management center를 위해 Azure 서비스 애플리케이션에 할당된 기타 사용자에게는 다음 중 하나의 이유로 기본 사용자 역할 보안 분석가(읽기 전용)가 할당됩니다.

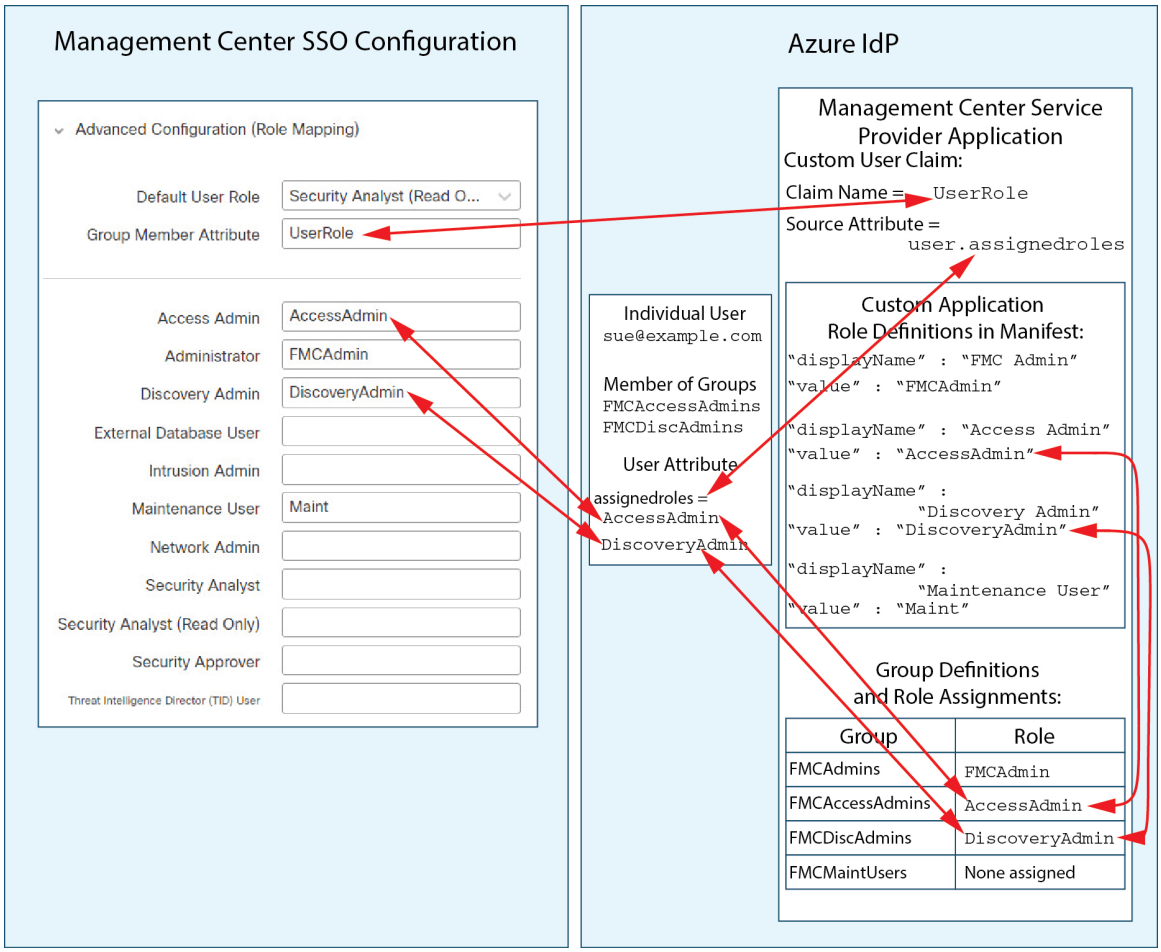
- assignedroles 속성에 할당된 값이 없습니다.
- assignedroles 속성에 할당된 값이 management center의 SSO 설정에서 사용자 역할에 대해 구성된 식과 일치하지 않습니다.

그룹에 대한 **Azure** 역할 매핑 예

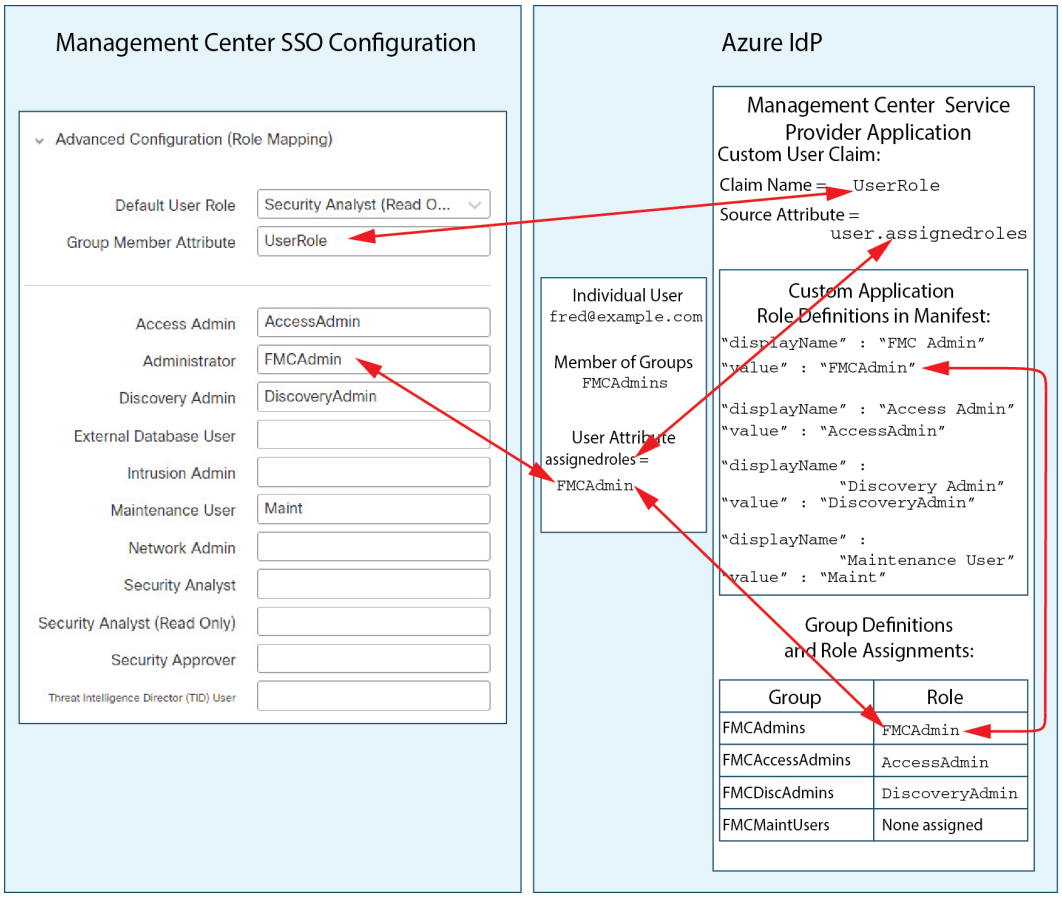
그룹에 대한 역할 매핑에서 Azure management center 서비스 애플리케이션에는 매니페스트 내에 정의된 사용자 지정 역할이 있습니다. (이 경우 FMCAdmin, AccessAdmin, Discovery Admin 및 Maint입니다.) 이러한 역할은 그룹에 할당할 수 있습니다. Azure는 해당 그룹의 할당된 역할 속성에 각 그룹 멤버에 대한 역할 할당을 전달합니다. 애플리케이션에 맞춤형 사용자 클레임도 정의되어 있으며, 이 클레임은 SSO를 통해 management center에 로그인하는 사용자에 대해 할당된 사용자 역할에서 해당 값을 가져오도록 설정됩니다. Azure는 SSO 로그인 프로세스 중에 management center에 클레임 값을 전달하고 management center에서는 클레임 값을 management centerSSO 설정의 각 management center 사용자 역할에 할당된 문자열과 비교합니다.

다음 다이어그램은 management center 및 Azure 구성의 관련 필드와 값이 그룹에 대한 사용자 역할 매핑에서 서로 어떻게 일치하는지를 보여줍니다. 각 다이어그램은 management center 및 Azure AD 포털에서 동일한 SSO 구성을 사용하지만, Azure AD 포털의 각 사용자에 대한 설정은 management center에서 각 사용자에게 서로 다른 역할을 할당하는 방식이 다릅니다.

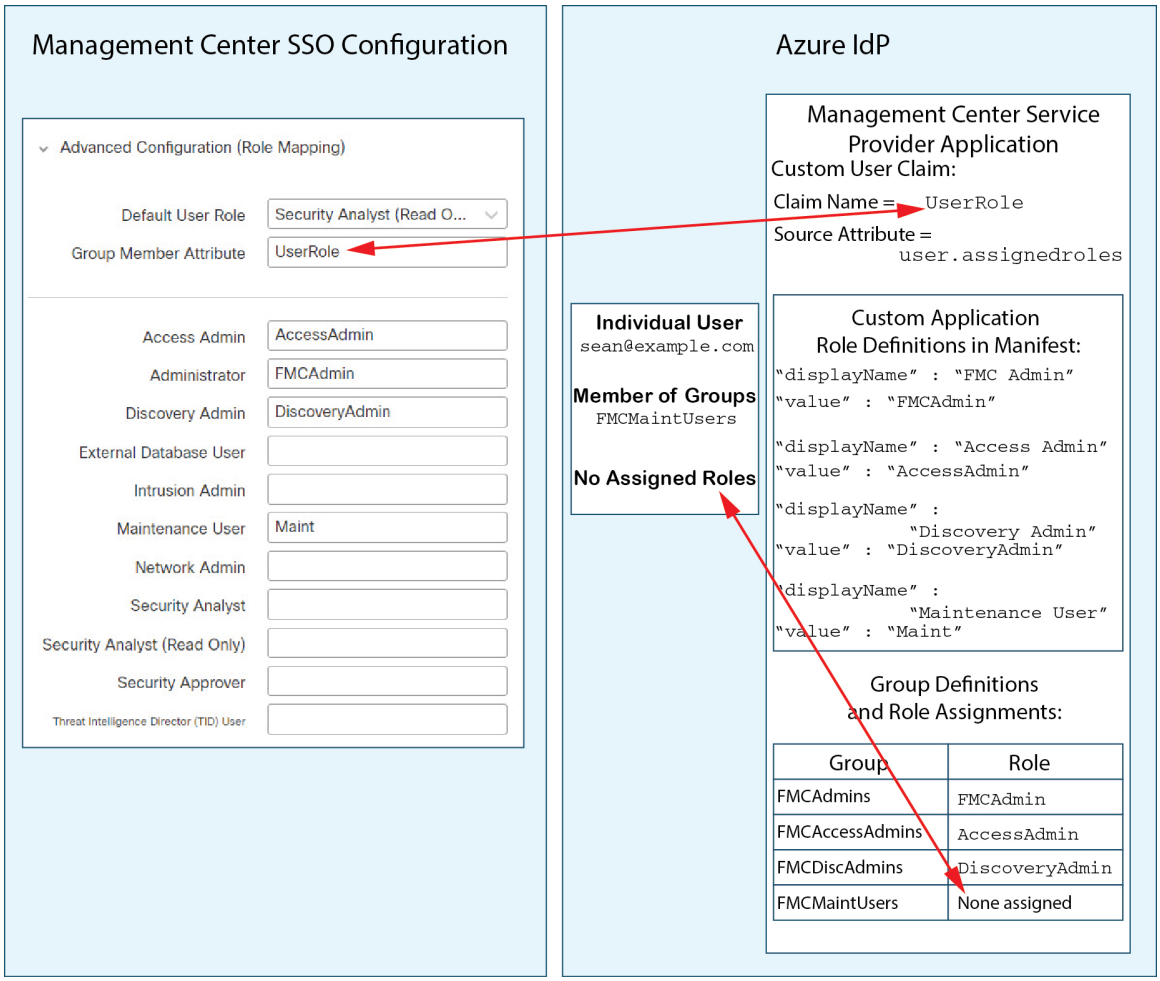
- 이 다이어그램에서 sue@example.com은 `FMCAccessAdmins` 및 `FMCDiscoveryAdmins` 그룹의 멤버입니다. 이러한 그룹에서 맞춤형 역할 `AccessAdmin` 및 `DiscoveryAdmin`을 상속합니다. Sue가 SSO를 사용하여 management center에 로그인하면 management center에서는 액세스 관리자 및 검색 관리자 역할을 할당합니다.



- 이 다이어그램에서 fred@example.com은 `FMCAdmins` 그룹의 멤버이며, 이 그룹에서 맞춤형 역할 `FMCAdmin`을 상속합니다. 프레드가 SSO를 사용하여 management center에 로그인하면 management center는 관리자 역할을 할당합니다.

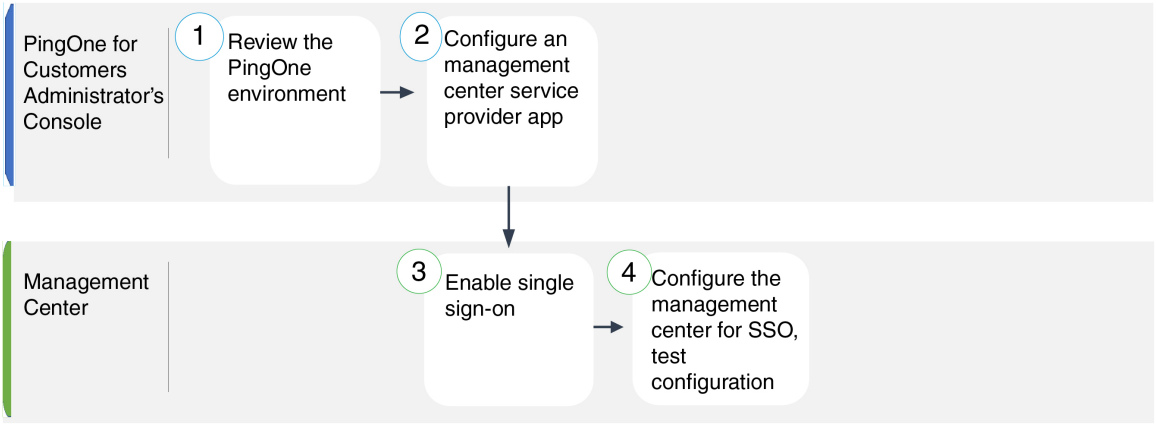


- 이 다이어그램에서 sean@example.com은 `FMCMaintUsers` 그룹의 멤버입니다. 그러나 Azure management center 서비스 제공자 애플리케이션 내에서 `FMCMaintUsers`에 맞춤형 역할이 할당되지 않았기 때문에, 해당 사용자에게 할당된 역할이 없으며, SSO를 사용하여 management center에 로그인할 때, management center는 기본 역할인 Security Analyst(읽기 전용)를 지정합니다.



PingID로 SSO(Single Sign-On) 구성

PingID의 PingOne for Customers 제품을 사용하여 SSO를 설정하려면 다음 작업을 참조하십시오.



1	PingOne for Customers 관리자 콘솔	PingID PingOne for Customers 환경 검토, on page 190.
2	PingOne for Customers 관리자 콘솔	PingID PingOne for Customers에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 190.
3	management center	Management Center에서 SSO(Single Sign-On) 활성화, on page 148.
4	management center	PingID PingOne for Customers을 사용하여 SSO용 Management Center을 구성합니다., on page 192.

PingID PingOne for Customers 환경 검토

PingOne for Customers는 PingID의 클라우드 호스팅 IDaaS(Identity-as-a-Service) 제품입니다. PingOne for Customers에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션된 디바이스를 포함하는 엔터티를 환경이라고 합니다. PingOne 환경에 management center를 추가하기 전에 해당 조직에 대해 잘 알고 있어야합니다. 다음 질문을 고려해 보십시오.

- management center에 액세스할 수 있는 사용자는 몇 명입니까?
- management center에 대한 SSO 액세스를 지원하려면 사용자를 더 추가해야 합니까?

이 문서에서는 사용자가 PingOne for Customers 관리자 콘솔에 대해 잘 알고 있으며 조직 관리자 역할의 계정을 가지고 있다고 가정합니다.

PingID PingOne for Customers에 대한 Management Center 서비스 제공자 애플리케이션 구성

PingOne for Customers 관리자 콘솔을 사용하여 PingOne for Customers 환경에서 management center 서비스 제공자 애플리케이션을 생성하고 기본 구성 설정을 구성합니다. 이 문서에서는 모든 기능을 갖춘 SSO 환경을 설정하는 데 필요한 PingOne for Customers 기능을 전부 설명하지 않습니다. 가령 사용자를 생성하려면 PingOne for Customers 문서를 참조하면 됩니다.

Before you begin

- PingOne for Customers 환경 및 해당 사용자를 숙지하십시오.
- 필요한 경우, 사용자를 추가로 생성합니다.

Note 시스템에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 management center에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이것이 IdP에 해당하는지 확인해야 합니다. IdP에서 통신 사업자 애플리케이션을 구성하고 management center에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 management center(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

Note 여러 URL(예: 정규화된 도메인 이름 및 IP 주소)로 management center 웹 인터페이스에 연결할 수 있는 경우, SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 management center에 일관되게 액세스해야 합니다.

Procedure

단계 **1** 다음 설정을 사용하여 사용자 환경에서 애플리케이션을 생성하려면 PingOne for Customers 관리자 콘솔을 확인하십시오.

- **Web App(**웹 앱**)** 애플리케이션 유형을 선택합니다.
- **SAML** 연결 유형을 선택합니다.

단계 **2** SAML 연결에 대해 다음 설정으로 애플리케이션을 구성합니다.

- **ACS URL**의 경우, `/sam/acs` 문자열을 management center 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **Signing Certificate(**서명 인증서**)**에 대해 Sign Assertion & Response(어설션 서명 및 응답)를 선택합니다.
- **Signing Algorithm(**서명 알고리즘**)**에 대해 RSA_SHA256을 선택합니다.
- **Entity ID(**엔티티 **ID)**의 경우, `/saml/metadata` 문자열을 management center 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/metadata`
- **SLO Binding(SLO** 바인딩**)**의 경우, HTTP POST를 선택합니다.
- **Assertion Validity Duration(**어설션 유효 기간**)**에 300을 입력합니다.

단계 **3** 애플리케이션의 SAMLConnection 정보에서 다음 값을 확인합니다.

- **SSO(Single Sign-On)** 서비스
- 발급자 **ID**

management center 웹 인터페이스에서 PingID의 PingOne for Customers 제품을 사용하여 SSO를 설정할 때 이러한 값이 필요합니다.

단계 **4** **SAML ATTRIBUTES(SAML** 속성**)**의 경우, 단일 필수 속성에 대해 다음을 선택합니다.

- **PINGONE USER ATTRIBUTE(PINGONE** 사용자 속성**):** `이메일 주소`
- **APPLICATION ATTRIBUTE(**애플리케이션 속성**):** `saml_subject`

단계 **5** X509 PEM(`.crt`) 형식으로 서명 인증서를 다운로드하여 로컬 컴퓨터에 저장합니다.

단계 **6** (선택 사항) management center에 SSO를 보다 쉽게 설정할 수 있도록 management center 서비스 제공자 애플리케이션의 SAML XML 메타데이터 파일을 로컬 컴퓨터에 다운로드할 수 있습니다.

단계 **7** 애플리케이션을 활성화합니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148의 내용을 참조하십시오.

PingID PingOne for Customers을 사용하여 SSO용 Management Center을 구성합니다.

management center 웹 인터페이스에서 다음 지침을 사용하십시오.

Before you begin

- PingOne for Customers Administrator Console에서 management center 서비스 제공자 애플리케이션을 생성합니다. PingID PingOne for Customers에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 190의 내용을 참조하십시오.
- SSO(Single Sign-On)을 활성화합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148의 내용을 참조하십시오.

Procedure

단계 **1** 이 단계는 Management Center에서 SSO(Single Sign-On) 활성화, on page 148에서 곧바로 이어집니다. **Configure PingID Metadata(PingID** 메타데이터 구성**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 설정 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. PingOne for Customers Administrator Console에서 검색한 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**의 경우 PingID PingOne for Customers에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 190 3단계에서 적어둔 **SSO(Single Sign-On)** 서비스를 입력합니다.

- **Identity Provider Issuer(ID** 제공자 발급자**)**의 경우 PingID PingOne for Customers에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 190 3단계에서 적어둔 발급자 **ID**를 입력합니다.
- **X.509** 인증서의 경우 PingID PingOne for Customers에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 190 5단계 중 PingOne for Customers에서 다운로드한 인증서를 사용합니다. (텍스트 편집기를 사용하여 인증서 파일을 열고 내용을 복사하여 **X.509 Certificate(X.509** 인증서**)** 필드에 붙여 넣습니다.)

- PingOne for Customers에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우, (PingID PingOne for Customers에 대한 Management Center 서비스 제공자 애플리케이션 구성, on page 190의 6단계) 파일을 management center에 업로드할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Advanced Configuration (Role Mapping)(**고급 구성**(**역할 매핑**))**을 펼칩니다.

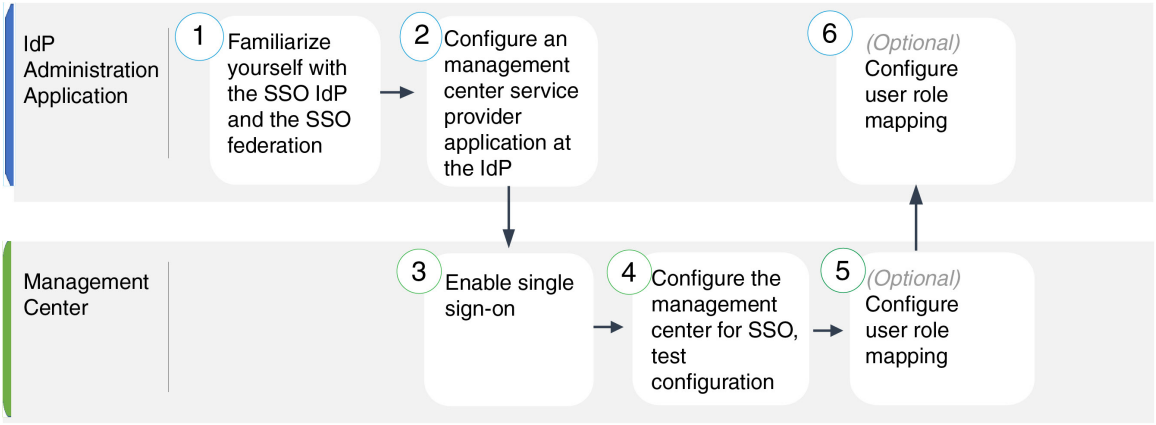
단계 **5** **Default User Role(**기본 사용자 역할**)** 드롭다운에서 management center 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **6** **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 management center의 SSO 구성과 PingOne for Customers 서비스 제공자 애플리케이션 구성을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **7** 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

SAML 2.0 규정준수 SSO 제공자로 SSO(Single Sign-On) 구성

management center에서는 SAML 2.0 SSO 프로토콜을 준수하는 모든 SSO ID 제공자(IdP)에서 SSO(Single Sign-On)를 지원합니다. 광범위한 SSO 제공자를 사용하기 위한 일반적인 지침은 높은 수준에서 수행할 작업을 처리해야 합니다. 이 문서에서 구체적으로 다루지 않은 제공자를 사용하여 SSO를 설정하려면 선택한 IdP를 능숙하게 다루어야 합니다. 이러한 작업을 통해 SAML 2.0을 준수하는 SSO 제공자를 사용하여 SSO(Single Sign-On)에 대해 management center를 설정하는 단계를 결정할 수 있습니다.



1	IdP 관리 애플리케이션	SSO ID 제공자 및 SSO 페더레이션을 숙지합니다., on page 194.
2	IdP 관리 애플리케이션	SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 195.
3	management center	Management Center에서 SSO(Single Sign-On) 활성화, on page 148.
4	management center	SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 Management Center 구성, on page 197.
5	management center	SAML 2.0 호환 SSO 제공자에 대해 Management Center에서 사용자 역할 매핑 설정, on page 199.
6	IdP 관리 애플리케이션	SAML 2.0 호환 SSO 제공자에 대해 IdP에서 Management Center 사용자 역할 매핑 설정, on page 200.

SSO ID 제공자 및 SSO 페더레이션을 숙지합니다.

다음 사항을 고려하여 IdP 벤더 설명서를 읽으십시오.

- SSO 제공자가 사용자에게 IdP를 사용하기 전에 서비스를 구독하거나 등록하도록 요구합니까?
- SSO 제공자가 일반적인 SSO 개념에 사용하는 용어는 무엇입니까? 예를 들어 페더레이션 서비스 공급자 애플리케이션 그룹을 참조하기 위해 Okta는 "org"를 사용하고 Azure는 "tenant"를 사용합니다.

- SSO 제공자가 SSO만 지원합니까 아니면 여러 요인(예: 다단계 인증 또는 도메인 관리)을 지원합니까? (이는 기능 간에 공유되는 일부 요소(특히 사용자 및 그룹)의 구성에 영향을 줄 수 있습니다.)
- IdP 사용자 계정에서 SSO를 구성하려면 어떤 권한이 필요합니까?
- SSO 제공자가 서비스 제공자 애플리케이션에 대해 설정해야 하는 구성은 무엇입니까? 예를 들어 Okta는 management center와의 통신을 보호하기 위해 X509 인증서를 자동으로 생성하지만, Azure에서는 Azure 포털 인터페이스를 사용하여 해당 인증서를 생성해야 합니다.
- 사용자 및 그룹은 어떻게 생성되고 구성됩니까? 사용자는 그룹에 어떻게 할당됩니까? 사용자 및 그룹은 어떻게 서비스 제공자 애플리케이션에 대한 액세스 권한을 부여 받습니까?
- SSO 연결을 테스트하기 전에 SSO 제공자가 하나 이상의 사용자를 서비스 제공자 애플리케이션에 할당해야 합니까?
- SSO 제공자가 사용자 그룹을 지원합니까? 사용자 및 그룹 속성은 어떻게 구성됩니까? SSO 구성에서 어떻게 management center 사용자 역할에 속성을 매핑할 수 있습니까
- management center에서 SSO를 지원하려면 페더레이션에 사용자 또는 그룹을 더 추가해야 합니까?
- 사용자가 그룹의 페더레이션 구성원 내에 있습니까?
- 사용자 및 그룹 정의가 IdP에 기본적이거나 Active Directory, RADIUS 또는 LDAP와 같은 사용자 관리 애플리케이션에서 가져온 것입니까?
- 어떤 종류의 사용자 역할을 지정하시겠습니까? (사용자 역할을 할당하지 않도록 선택하는 경우 management center는 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 사용자 역할 매핑을 위한 계획을 지원하려면 페더레이션 내의 사용자 및 그룹을 어떻게 구성해야 합니까?

SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성

일반적으로 SSO 제공자는 각 연동 애플리케이션에 대해 IdP에서 서비스 제공자 애플리케이션을 구성해야 합니다. SAML 2.0 SSO를 지원하는 모든 IdP는 서비스 제공자 애플리케이션에 대해 동일한 구성 정보가 필요하지만 일부 IdP는 자동으로 일부 구성 설정을 생성하는 반면, 일부는 모든 설정을 직접 구성해야 합니다.

Note management center 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note management center는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 IdP에서 management center로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- SSO 페더레이션 그리고 해당 사용자 및 그룹을 숙지하십시오. SSO ID 제공자 및 SSO 페더레이션을 숙지합니다., on page 194의 내용을 참조하십시오.
- IdP 계정에 이 작업을 수행하는 데 필요한 권한이 있는지 확인합니다.
- 필요한 경우 SSO 페더레이션에서 사용자 계정 및/또는 그룹을 생성합니다.

Note 시스템에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 management center에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이것이 IdP에 해당하는지 확인해야 합니다. IdP에서 통신 사업자 애플리케이션을 구성하고 management center에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 management center(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

Note 여러 URL로 management center 웹 인터페이스에 연결할 수 있는 경우 (예: 정규화된 도메인 이름 및 IP 주소) SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 management center에 일관되게 액세스해야 합니다.

Procedure

단계 **1** IdP에서 새 서비스 제공자 애플리케이션을 생성합니다.

단계 **2** IdP에 필요한 값을 구성합니다. management center에 SAML 2.0 SSO 기능을 지원하는 데 필요한 아래에 나열된 필드를 포함해야 합니다. 각기 다른 SSO 서비스 제공자가 SAML 개념에 대해 다른 용어를 사용하므로 이 목록은 IdP 애플리케이션에서 올바른 설정을 찾는 데 도움이 되도록 이러한 필드에 대한 대체 이름을 제공합니다.

- 서비스 제공자 엔티티 ID, 서비스 제공자 식별자, 대상 URI: URL 형식의 서비스 제공자(management center)에 대한 전역 고유 이름. 이를 생성하려면 `/saml/metadata` 문자열(예: `https://ExampleFMC/saml/metadata`)을 management center 로그인 URL에 추가합니다.

- SSO(Single Sign-On, 단일 인증) URL, 수신자 URL, 어설션 소비자 서비스 URL: 브라우저가 IdP를 대신하여 정보를 전송하는 서비스 제공자(management center) 주소입니다. 이를 생성하려면 management center 로그인 URL에 `saml/acs` 문자열(예: `https://ExampleFMC/saml/acs`)을 추가합니다.
- X.509 인증서: management center와 IdP 간의 통신을 보호하기 위한 인증서입니다. 일부 IdP는 인증서를 자동으로 생성할 수 있으며, 일부는 IdP 인터페이스를 사용하여 명시적으로 생성해야 할 수 있습니다.

단계 **3** (선택적으로 애플리케이션에 그룹을 할당하는 경우) 개별 사용자를 management center 애플리케이션에 할당합니다. (management center 애플리케이션에 그룹을 할당하려는 경우 해당 그룹의 멤버를 개인으로 할당하지 마십시오.)

단계 **4** (애플리케이션에 개별 사용자를 할당하는 경우엔 선택 사항입니다.) management center 애플리케이션에 사용자 그룹을 할당합니다.

단계 **5** (선택 사항) 일부 IdP는 이 작업에서 구성한 정보가 포함된 SAML XML 메타데이터 파일을 생성하는 기능을 제공합니다. IdP가 이 기능을 제공하는 경우, 파일을 로컬 컴퓨터에 다운로드하여 management center에서 SSO 구성 프로세스를 쉽게 수행할 수 있습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148의 내용을 참조하십시오.

SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 Management Center 구성

management center 웹 인터페이스에서 다음 지침을 사용하십시오. SAML 2.0 호환 SSO 제공자를 사용하여 SSO에 대해 management center를 구성하려면 IdP의 정보가 필요합니다.

Before you begin

- SSO 페더레이션의 조직과 해당 사용자 및 그룹을 검토합니다.
- IdP에서 management center 서비스 제공자 애플리케이션을 구성합니다. SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 Management Center 구성, on page 197의 내용을 참조하십시오.
- IdP에서 서비스 제공자 애플리케이션에 대한 다음 SSO 구성 정보를 수집합니다. 각기 다른 SSO 서비스 제공자가 SAML 개념에 대해 다른 용어를 사용하므로 이 목록은 IdP 애플리케이션에서 올바른 값을 찾는 데 도움이 되도록 이러한 필드에 대한 대체 이름을 제공합니다.
  - ID 공급자 SSO(Single Sign-On) URL, 로그인 URL: 브라우저가 management center 대신 정보를 전송하는 IdP URL입니다.
  - ID 제공자 발급자, ID 제공자 발급자 URL, 발급자 URL: IdP의 전역 고유 이름으로, 대개 URL 형식으로 지정됩니다.
  - management center와 IdP 간의 통신을 보호하기 위한 X.509 디지털 인증서.

- SSO(Single Sign-On)을 활성화합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148의 내용을 참조하십시오.

Procedure

단계 **1** (이 단계는 Management Center에서 SSO(Single Sign-On) 활성화, on page 148에서 곧바로 이어집니다.) **Configure SAML Metadata(SAML** 메타데이터 구성**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 설정 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. SSO 서비스 제공자 애플리케이션에서 이전에 얻은 다음 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**
     - **ID** 제공자 발급자
     - **X.509** 인증서

- IdP에서 생성된 XML 메타데이터 파일을 저장한 경우(SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 195의 5 단계) management center에 파일을 업로드 할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 management center의 SSO 구성과 IdP의 서비스 제공자 애플리케이션 구성을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **5** 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 사용자 역할 매핑을 구성할 수 있습니다. SAML 2.0 호환 SSO 제공자에 대해 Management Center에서 사용자 역할 매핑 설정, on page 199의 내용을 참조하십시오. 역할 매핑을 구성하지 않도록 선택하는 경우, 기본적으로 management center에 로그인하는 모든 SSO 사용자에게 SAML 2.0 호환 SSO 제공자에 대해 Management Center에서 사용자 역할 매핑 설정, on page 199의 4단계에서 구성한 기본 사용자 역할이 할당됩니다.

SAML 2.0 호환 SSO 제공자에 대해 Management Center에서 사용자 역할 매핑 설정

SAML SSO 사용자 역할 매핑을 구현하려면 IdP 및 management center에서 조정 구성을 설정해야 합니다.

- IdP에서 사용자 또는 그룹 속성을 설정하여 사용자 역할 정보를 전달하고 값을 할당합니다. IdP는 SSO 사용자를 인증하고 권한을 부여하고 나서 management center에 이를 전송합니다.
- management center에서 값을 사용자에게 할당할 각 management center 사용자 역할과 연결합니다.

IdP가 권한 있는 사용자와 연결된 사용자 또는 그룹 속성을 management center에 전송하는 경우, management center에서는 속성값을 각 management center 사용자 역할에 연결된 값과 비교하고 일치를 생성하는 모든 역할을 사용자에게 할당합니다. management center는 Golang 및 Perl에서 지원하는 Google RE2 정규식 표준의 제한된 버전을 준수하는 정규식으로 두 값을 모두 처리하며 비교를 수행합니다.

management center 웹 인터페이스에서 사용자 역할 매핑을 구성할 수 있는 필드는 선택한 SSO 제공자와 상관없이 동일합니다. 그러나 구성하는 값의 경우, 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방식을 고려해야 합니다. IdP가 사용자 또는 그룹 속성에 대해 구문 제한을 적용할 수 있습니다. 그러한 경우에는 역할 이름 및 해당 요건과 호환되는 정규식으로 사용자 역할 매핑 체계를 구성해야 합니다.

Before you begin

- management center에 대한 SSO 서비스 제공자 애플리케이션을 설정합니다. SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 195의 내용을 참조하십시오.
- management center에서 SSO(Single Sign-On)를 활성화하고 설정합니다. Management Center에서 SSO(Single Sign-On) 활성화, on page 148 및 SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 Management Center 구성, on page 197의 내용을 참조하십시오.

Procedure

단계 **1** **System**(시스템) > **Users**(사용자)를 선택합니다.

단계 **2** **Single Sign-On**(단일 인증) 탭을 클릭합니다.

단계 **3** **Advanced Configuration (Role Mapping)**(고급 구성(역할 매핑))을 펼칩니다.

단계 **4** **Default User Role**(기본 사용자 역할) 드롭다운에서 management center 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **5** **Group Member Attribute**(그룹 멤버 속성)을 입력합니다. 이 문자열은 사용자 또는 그룹에 대한 사용자 역할을 매핑하기 위해 IdP management center 서비스 제공자 애플리케이션에 설정된 속성 이름과 일치해야 합니다. (SAML 2.0 호환 SSO 제공자에 대해 IdP에서 Management Center 사용자 역할 매핑 설정, on page 200의 1단계 참조)

단계 **6** SSO 사용자에게 할당할 각 management center 사용자 역할 옆에 정규식을 입력합니다. (management center는 Golang 및 Perl에서 지원하는 Google의 RE2 정규식 표준의 제한된 버전을 사용합니다.) management center에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 management center에 전송

하는 사용자 역할 매핑 속성값과 비교합니다. management center는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. SAML 2.0 호환 SSO 제공자에 대해 IdP에서 Management Center 사용자 역할 매핑 설정, on page 200의 내용을 참조하십시오.

SAML 2.0 호환 SSO 제공자에 대해 IdP에서 Management Center 사용자 역할 매핑 설정

사용자 역할 매핑을 구성하는 자세한 단계는 IdP마다 다릅니다. 통신 사업자 애플리케이션에 대한 사용자 지정 사용자 또는 그룹 특성을 생성하는 방법을 결정하고 IdP에서 각 사용자 또는 그룹의 특성에 값을 할당하여 management center에 사용자 또는 그룹 권한을 전달해야 합니다. 다음 사항에 주의하십시오.

- IdP가 서드 파티 사용자 관리 애플리케이션(예: Active Directory, LDAP 또는 Radius)에서 사용자 또는 그룹 프로파일을 가져오는 경우, 이는 역할 매핑에 속성을 사용하는 방법에 영향을 줄 수 있습니다.
- SSO 페더레이션 전체에서 사용자 및 그룹 역할 정의를 고려합니다.
- management center는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 IdP에서 management center로 전달하도록 단일 속성을 구성해야 합니다.
- 여러 사용자가 있는 경우, 그룹 역할 매핑은 일반적으로 management center에 더 효율적입니다.
- management center 애플리케이션에 사용자 그룹을 할당하는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.
- management center 사용자 역할과의 일치를 확인하기 위해 management center에서는 IdP에서 수신한 사용자 및 그룹 역할 속성 값을 Golang 및 Perl에서 지원하는 Google RE2 정규식 표준의 제한된 버전을 준수하는 정규식으로 처리합니다. IdP가 사용자 또는 그룹 속성에 대해 특정 구문 제한을 적용할 수 있습니다. 그러한 경우에는 역할 이름 및 해당 요건과 호환되는 정규식으로 사용자 역할 매핑 체계를 구성해야 합니다.

Before you begin

- IdP 계정에 이 작업을 수행하는 데 필요한 권한이 있는지 확인합니다.
- IdP에서 management center 서비스 제공자 애플리케이션을 구성합니다. SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 195의 내용을 참조하십시오.

Procedure

단계 **1** IdP에서 management center로 전송될 속성을 생성하거나 지정하여 각 사용자 로그인에 대한 역할 매핑 정보를 포함합니다. 이는 사용자 속성, 그룹 속성 또는 IdP 또는 서드 파티 사용자 관리 애플리케이

션에서 유지 관리하는 사용자 또는 그룹 정의와 같은 소스에서 값을 가져오는 다른 속성일 수 있습니다.

단계 **2** 속성의 값을 가져오는 방법을 구성합니다. 가능한 값을 management center SSO 구성의 사용자 역할과 연결된 값으로 조정합니다.

웹 인터페이스의 사용자 역할 맞춤화

각 사용자 어카운트는 사용자 역할과 함께 정의해야 합니다. 이 섹션에서는 사용자 역할을 관리하는 방법 및 웹 인터페이스 액세스에 대한 맞춤형 사용자 역할을 구성하는 방법을 설명합니다. 기본 사용자 역할에 대해서는 사용자 역할, 118 페이지의 내용을 참조하십시오.

맞춤형 사용자 역할 생성

맞춤형 사용자 역할은 메뉴 기반 및 시스템 권한 집합을 보유할 수 있으며, 사전 정의된 사용자 역할 또는 또 다른 맞춤형 사용자 역할을 원래 그대로 유지하거나 복사하거나 또 다른 management center에서 가져올 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Users(**사용자**)**을(를) 선택합니다.

단계 **2** **User Roles(**사용자 역할**)**을 클릭합니다.

단계 **3** 다음 방법 중 하나로 새 사용자 역할을 추가합니다.

- **Create User Role(**사용자 역할 생성**)**을 클릭합니다.
- 복사하려는 사용자 역할 옆에 있는 **Copy(**복사**)** ( )을 클릭합니다.
- 또 다른 management center에서 맞춤형 사용자 역할을 가져옵니다.

  1. 기존 management center에서 **Export(**내보내기**)** ( )을 클릭하고 해당 역할을 컴퓨터에 저장합니다.
  2. 새 management center에서 시스템 ( ) > **Tools(**툴**)** > **Import/Export(**임포트/익스포트**)**을 선택합니다.
  3. **Upload Package(**패키지 업로드**)**를 클릭한 후 지침에 따라 새 management center에 저장된 사용자 역할을 가져옵니다.

단계 **4** 새 사용자 역할의 **Name(**이름**)**을 입력합니다. 사용자 역할 이름은 대/소문자를 구별합니다.

단계 **5** (선택 사항) **Description(**설명**)**을 추가합니다.

단계 **6** 새 역할에 대해 **Menu-Based Permissions(**메뉴 기반 권한**)**를 선택합니다.

권한을 선택하면 모든 하위 항목이 선택되고 다중 값 권한이 첫 번째 값을 사용합니다. 상위 수준 권한의 선택을 취소할 경우 모든 하위 권한의 선택도 취소됩니다. 권한을 선택하지만 권한의 하위 항목은 선택하지 않는 경우, 권한이 기울임꼴 텍스트로 나타납니다.

사전 정의된 사용자 역할을 맞춤형 역할의 기반으로 사용하기 위해 복사하면 사전 정의 역할과 관련된 권한이 미리 선택됩니다.

맞춤형 사용자 역할에 제한적 검색을 적용할 수 있습니다. 이러한 검색은 사용자가 Analysis(분석) 메뉴에서 사용 가능한 페이지의 테이블에서 볼 수 있는 데이터를 제한합니다. 먼저 비공개 저장 검색을 생성하고 해당 메뉴 기반 권한의 **Restrictive Search(**제한된 검색**)** 드롭다운 메뉴에서 이를 선택하는 방법으로 제한적 검색을 구성할 수 있습니다.

단계 **7** (선택 사항) **External Database Access(**외부 데이터 액세스**)(**읽기 전용**)** 체크 박스를 선택하고 새 역할에 대한 데이터베이스 액세스 권한을 설정합니다.

이 옵션은 JDBC SSL 연결을 지원하는 애플리케이션을 사용하여 데이터베이스에 읽기 전용 액세스를 제공합니다. 타사 애플리케이션으로 management center를 인증하려면 시스템 설정에서 데이터베이스 액세스를 활성화해야 합니다.

단계 **8** (선택 사항) 새 사용자 역할에 대한 확대 권한을 설정하려면 사용자 역할 에스컬레이션 활성화, 203 페이지을 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.
맞춤형 역할이 저장됩니다. 시스템에서 읽기 전용 역할이라고 판단하는 경우 시스템은 해당 역할에 '(Read Only)(읽기 전용)' 레이블을 지정합니다. 이는 읽기 전용 및 읽기-쓰기 사용자의 동시 세션 수를 구성할 때 관련이 있습니다. '(Read Only)(읽기 전용)'를 역할 이름에 추가하는 방법으로는 역할을 읽기 전용으로 만들 수 없습니다. 동시 세션 제한에 대해 알아보려면 사용자 구성, 106 페이지의 내용을 참고하십시오.

예

액세스 제어 관련 기능을 위한 맞춤형 사용자 역할을 생성해 사용자가 액세스 제어 및 연결된 정책을 보고 수정할 수 있는지 여부를 지정할 수 있습니다.

다음 테이블에는 생성할 수 있는 맞춤형 역할과 각 예에 대해 부여되는 사용자 권한이 나열되어 있습니다. 이 테이블에는 각 맞춤형 역할에 필요한 권한이 나열되어 있습니다. 이 예에서 정책 승인자는 액세스 제어 및 침입 정책을 볼 수 있지만 수정할 수는 없습니다. 정책 승인자는 디바이스에 구성 변경 사항을 구축할 수도 있습니다.

표 ***5:*** 샘플 액세스 제어 맞춤형 역할

메뉴 기반 권한	예시 역할		
	액세스 제어 편집기	침입 및 네트워크 분석 편집기	정책 승인자
액세스 제어	예	아니요	예
액세스 제어 정책	예	아니요	예

메뉴 기반 권한	예시 역할		
	액세스 제어 편집기	침입 및 네트워크 분석 편집기	정책 승인자
액세스 제어 정책 수정	아니요	아니요	아니요
침입 정책	아니요	예	예
침입 정책 수정	아니요	예	아니요
디바이스에 구성 구축	아니요	아니요	예

사용자 역할 비활성화

어떤 역할을 비활성화하면 해당 역할을 할당 받은 모든 사용자에게서 역할 및 관련 권한이 제거됩니다. 사전 정의 사용자 역할은 삭제할 수 없지만 이를 비활성화할 수는 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 사용자 역할을 표시하며 이러한 역할은 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 사용자 역할도 표시되지만, 이러한 역할은 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 사용자 역할을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Users(**사용자**)**을(를) 선택합니다.

단계 **2** **User Roles(**사용자 역할**)**을 클릭합니다.

단계 **3** 활성화하거나 비활성화할 사용자 역할의 옆에 있는 슬라이더를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

어떤 역할의 사용자가 로그인한 상태에서 Lights-Out Management로 해당 역할을 비활성화했다가 다시 활성화할 경우 또는 사용자의 로그인 세션 중에 백업에서 사용자 또는 사용자 역할을 복원할 경우, 사용자가 다시 웹 인터페이스에 로그인해야 IPMItool 명령에 다시 액세스할 수 있습니다.

사용자 역할 에스컬레이션 활성화

이러한 기본 역할 외에 대상 지정된 다른 사용자 역할의 권한을 임시로 얻을 수 있는 권한과 비밀번호를 맞춤형 사용자 역할에 제공할 수 있습니다. 그러면 부재 시 어떤 사용자를 손쉽게 다른 사용자로 대체하거나 고급 사용자 권한의 사용을 면밀하게 추적하는 것이 가능합니다. 기본 사용자 역할은 에스컬레이션을 지원하지 않습니다.

예를 들어 기반 역할의 권한이 매우 제한적인 사용자가 관리자 역할로 에스컬레이션하여 관리 작업을 수행할 수 있습니다. 사용자가 자신의 비밀번호를 사용하거나 지정된 다른 사용자의 비밀번호를

사용하도록 이 기능을 구성할 수 있습니다. 두 번째 옵션에서는 해당되는 모든 사용자를 대상으로 하나의 확대 비밀번호를 손쉽게 관리할 수 있습니다.

사용자 역할 확대를 구성하려면 다음 워크플로를 참조하십시오.

프로시저

단계 **1** 에스컬레이션 대상 역할 설정, 204 페이지. 한 번에 하나의 사용자 역할만 확대 대상 역할이 될 수 있습니다.

단계 **2** 에스컬레이션을 위한 맞춤형 사용자 역할 구성, 204 페이지.

단계 **3** (로그인된 사용자의 경우) 사용자 역할 에스컬레이트, 205 페이지.

에스컬레이션 대상 역할 설정

어떤 사전 정의 또는 맞춤형 사용자 역할도 시스템 차원 확대 대상 역할이 되도록 지정할 수 있습니다. 이는 맞춤형 역할이 능력이 된다면 에스컬레이션할 수 있는 역할입니다. 한 번에 하나의 사용자 역할만 확대 대상 역할이 될 수 있습니다. 각 확대는 로그인 세션 동안 지속되며 감사 로그에 기록됩니다.

프로시저

단계 **1** 시스템 (⚙) > **Users(**사용자**)**을(를) 선택합니다.

단계 **2** **User Roles(**사용자 역할**)**을 클릭합니다.

단계 **3** **Configure Permission Escalation(**권한 확대 구성**)**을 클릭합니다.

단계 **4** **Excalation Target(**확대 대상**)** 드롭다운 목록에서 사용자 역할을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

확대 대상 역할의 변경은 즉시 적용됩니다. 확대된 세션의 사용자는 이제 새 확대 대상의 권한을 갖습니다.

에스컬레이션을 위한 맞춤형 사용자 역할 구성

확대 활성화의 대상이 되는 사용자는 확대가 활성화된 맞춤형 사용자 역할에 속해야 합니다. 이 절차에서는 맞춤형 사용자 역할에 대한 에스컬레이션을 활성화하는 방법을 설명합니다.

맞춤형 역할에 대해 에스컬레이션 비밀번호를 구성할 때 조직의 요구 사항을 고려하십시오. 여러 에스컬레이션 사용자를 손쉽게 관리하길 원할 경우 또 다른 사용자를 선택하여 해당 비밀번호를 확대 비밀번호로 사용하는 방법이 있습니다. 해당 사용자의 비밀번호를 변경하거나 사용자를 비활성화할 경우 해당 비밀번호를 필요로 하는 모든 에스컬레이션 사용자가 영향을 받습니다. 이 작업은 더 효율적으로 사용자 역할 확대를 관리할 수 있습니다. 특히 중앙에서 관리할 수 있는 외부 인증 사용자를 선택할 경우 더욱 그렇습니다.

시작하기 전에

에스컬레이션 대상 역할 설정, 204 페이지에 따라 대상 사용자 역할을 설정합니다.

프로시저

단계 **1** 맞춤형 사용자 역할 생성, 201 페이지에 설명된 대로 맞춤형 사용자 역할의 구성을 시작합니다.

단계 **2** **System Permissions(**시스템 권한**)**에서 **Set this role to escalate to: Maintenance User(**이 역할을 다음으로 에스컬레이션하도록 설정**:** 유지 보수 사용자**)** 확인란을 선택합니다.

현재 에스컬레이션 대상 목표가 확인란 옆에 나열됩니다.

단계 **3** 이 역할에서 에스컬레이션에 사용할 비밀번호를 선택합니다. 다음 2가지 옵션을 사용할 수 있습니다.

- 이 역할을 갖는 사용자가 확대 시 각자의 비밀번호를 사용하게 하려면 **Authenticate with the assigned user's password(**할당된 사용자의 비밀번호로 인증**)**를 선택합니다.
- 이 역할의 사용자가 다른 사용자의 비밀번호를 사용하게 하려면 **Authenticate with the specified user's password(**지정한 사용자의 비밀번호로 인증**)**를 선택하고 해당 사용자 이름을 입력합니다.

  참고 다른 사용자의 비밀번호로 인증할 경우 어떠한 사용자 이름이라도, 심지어 비활성화되었거나 존재하지 않는 사용자의 이름도 입력할 수 있습니다. 비밀번호가 에스컬레이션에 사용되는 사용자를 비활성화할 경우 해당 비밀번호를 필요로 하는 역할의 사용자는 에스컬레이션이 불가능해집니다. 에스컬레이션을 신속하게 제거해야 하는 경우 이 기능을 사용할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

사용자 역할 에스컬레이트

사용자가 확대 권한이 있는 맞춤형 사용자 역할이 있는 경우, 해당 사용자는 언제라도 대상 역할의 권한으로 확대할 수 있습니다. 확대는 사용자 환경 설정에 영향을 주지 않습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **Escalate Permissions(**권한 확대**)**를 선택합니다.

이 옵션이 표시되지 않는다면 관리자가 사용자 역할에 대해 확대를 활성화 하지 않은 것입니다

단계 **2** 인증 비밀번호를 입력합니다.

단계 **3** **Escalate(**확대**)**를 클릭합니다. 이제 현재 역할 외에도 확대 대상 역할의 모든 권한을 갖게 되었습니다.

확대 로그인 세션의 남은 시간 동안 지속됩니다. 다시 기본 역할의 권한만 가지려면 로그아웃했다가 새 세션을 시작해야 합니다.

LDAP 인증 연결 문제 해결

LDAP 인증 개체를 생성하는 경우, 선택한 서버와의 연결에 실패하거나 원하는 사용자 목록을 가져오지 않는다면 개체의 설정을 조정할 수 있습니다.

연결 테스트 결과 연결에 실패할 경우, 다음 방법으로 구성 문제를 해결해보십시오.

- 웹 인터페이스 화면 상단 및 테스트 출력에 표시된 메시지를 참조하여 개체의 어느 영역에서 문제를 일으키는지 확인합니다.
- 개체에 사용한 사용자 이름과 비밀번호가 올바른지 확인합니다.
  - 사용자가 기본 DN에 나타난 디렉토리로 이동할 권한이 있는지 확인하기 위해 서드파티 LDAP 브라우저를 사용하여 LDAP 서버에 연결해봅니다.
  - 사용자 이름이 LDAP 서버의 디렉토리 정보 트리에서 고유한지 확인합니다.
  - 테스트 출력에 LDAP 바인드 오류 49가 있을 경우 해당 사용자에 대한 사용자 바인딩이 실패한 것입니다. 서드파티 애플리케이션을 통해 서버 인증을 시도하여 해당 연결에서도 바인딩이 실패하는지 확인합니다.
- 서버를 정확하게 식별했는지 확인합니다.
  - 서버 IP 주소 또는 호스트 이름이 정확한지 확인합니다.
  - 로컬 어플라이언스에서 연결할 인증 서버까지 TCP/IP 액세스 권한이 있는지 확인합니다.
  - 서버에 대한 액세스가 방화벽에 의해 차단되지 않고 개체에 구성한 포트가 열려 있는지 확인합니다.
  - TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 서버에 사용된 호스트 이름과 일치해야 합니다.
  - CLI 액세스를 인증하는 경우, 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
  - 서버 유형 기본값을 사용한 경우 정확한 서버 유형인지 확인하고 **Set Defaults(**기본값 설정**)**를 다시 클릭하여 기본값을 재설정합니다.
- 기본 DN을 입력한 경우 **Fetch DNs(DN** 가져오기**)**를 클릭하여 서버에서 사용 가능한 모든 기본 DN을 가져오고 그 목록에서 이름을 선택합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각각이 올바르고 제대로 입력되었는지 확인합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각 설정을 제거하고 그 설정 없이 개체를 테스트해봅니다.
- 기본 필터 또는 CLI 액세스 필터를 사용하는 경우, 필터가 괄호로 묶여 있고 올바른 비교 연산자를 사용하고 있는지 확인합니다. 묶인 괄호를 포함하여 최대 450자까지 입력할 수 있습니다.

- 더 제한적인 기본 필터를 테스트하려면 사용자의 기본 DN으로 설정하여 그 사용자만 검색해봅니다.
- 암호화 연결을 사용하는 경우:
  - 인증서에 있는 LDAP 서버의 이름이 연결에 사용하는 호스트 이름과 매칭되는지 확인합니다.
  - 암호화 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 이름과 비밀번호가 제대로 입력되었는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 크리덴셜을 제거하고 개체를 테스트합니다.
- LDAP 서버에 연결하고 다음 구문을 사용하여 사용 중인 쿼리를 테스트합니다.

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

에를 들어 `myrtle.example.com`의 보안 도메인에 연결하기 위해 `domainadmin@myrtle.example.com` 사용자와 (`cn=*`) 기본 필터를 사용하는 경우, 다음 구문으로 연결을 테스트할 수 있습니다.

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

연결 테스트에 성공했지만 플랫폼 설정 정책을 적용한 후 인증이 되지 않을 경우, 디바이스에 적용되는 플랫폼 설정 정책에서 인증 및 사용할 개체가 모두 활성화되었는지 확인합니다.

성공적으로 연결했지만 연결에서 검색되는 사용자 목록을 조정하려는 경우, 기본 필터 또는 CLI 액세스 필터를 추가하거나 변경할 수 있습니다. 또는 더 제한적이거나 덜 제한적인 기본 DN을 사용할 수 있습니다.

AD(Active Directory) 서버에 대한 연결을 인증하는 동안에는 AD 서버에 대한 연결에 성공하더라도 연결 이벤트 로그에 차단된 LDAP 트래픽이 표시되는 경우가 거의 없습니다. 이 잘못된 연결 로그는 AD 서버가 중복 재설정 패킷을 전송할 때 발생합니다. 위협 방어 디바이스는 두 번째 재설정 패킷을 새 연결 요청의 일부로 식별하고 Block(차단) 작업으로 연결을 로깅합니다.

사용자 기본 설정 구성

사용자 역할에 따라 사용자 계정에 대한 특정 기본 설정을 지정할 수 있습니다.

다중 도메인 구축에서 사용자 환경설정은 계정이 액세스하는 모든 도메인에 적용됩니다. 홈페이지 및 대시보드 환경설정을 지정하는 경우, 특정 페이지와 대시보드 위젯은 도메인에 의해 제한됩니다.

비밀번호 변경

모든 사용자 어카운트는 비밀번호로 보호됩니다. 언제라도 비밀번호를 변경할 수 있으며, 사용자 어카운트에 대한 설정에 따라 정기적으로 비밀번호를 변경해야 하는 경우도 있습니다.

비밀번호 강도 확인을 활성화하면, 비밀번호는 Management Center용 사용자 계정 지침 및 제한 사항, 122 페이지에서 설명하는 강력한 비밀번호 요구 사항을 준수해야 합니다.

LDAP 또는 RADIUS 사용자일 경우 웹 인터페이스를 통해 비밀번호를 변경할 수 없습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다.

단계 **2** **Change Password(**비밀번호 변경**)**를 클릭합니다.

단계 **3** 선택 사항으로, **Show password(**비밀번호 표시**)** 확인란을 선택하면 이 대화상자를 이용하는 동안 비밀번호를 확인할 수 있습니다.

단계 **4** **Current Password(**현재 비밀번호**)**를 입력합니다.

단계 **5** 다음 2가지 옵션을 사용할 수 있습니다.

- **New Password(**새 비밀번호**)**와 **Confirm Password(**비밀번호 확인**)**에 새 비밀번호를 입력합니다.
- **Generate Password(**비밀번호 생성**)**을 클릭하면 나열된 기준을 준수하는 비밀번호를 시스템이 대신 생성합니다. (이렇게 생성되는 비밀번호는 기억하기가 쉽지 않습니다. 이 옵션을 선택한다면 비밀번호를 기록해 두십시오.)

단계 **6** **Apply(**적용**)**를 클릭합니다.

만료된 비밀번호 변경

사용자 어카운트의 설정에 따라 비밀번호가 만료될 수 있습니다. 비밀번호 만료 기한은 계정 생성 시 설정됩니다. 비밀번호가 만료된 경우 Password Expiration Warning(비밀번호 만료 경고) 페이지가 나타납니다.

프로시저

Password Expiration Warning(비밀번호 만료 경고) 페이지에는 다음과 같이 두 가지 옵션이 있습니다.

- 지금 비밀번호를 변경하려면 **Change Password(**비밀번호 변경**)**를 클릭합니다. 남은 경고 일수가 0일 경우, 반드시 비밀번호를 변경해야 합니다.

  팁 비밀번호 강도 확인을 활성화하면, 비밀번호는 Management Center용 사용자 계정 지침 및 제한 사항, 122 페이지에서 설명하는 강력한 비밀번호 요구 사항을 준수해야 합니다.

- 비밀번호를 나중에 변경하려면 **Skip(**넘어가기**)**을 클릭합니다.

웹 인터페이스 모양 변경

웹 인터페이스가 표시되는 방식을 변경할 수 있습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다. **General(**일반**)** 탭은 기본적으로 표시됩니다.

단계 **2** 테마를 선택합니다.

- 밝게
- **Dusk(**일몰**)**
- 클래식(6.6 이전 릴리스의 모양과 느낌)

홈 페이지 지정

웹 인터페이스에서 어플라이언스의 홈페이지로 사용할 페이지를 지정할 수 있습니다. 기본 홈 페이지는 기본 대시보드(**Overview(**개요**)** > **Dashboards(**대시보드**)**)이며, 외부 데이터베이스 사용자처럼 대시보드 액세스 권한이 없는 사용자 계정은 제외됩니다. (기본 대시보드를 설정하는 방법은 기본 대시보드 지정, 215 페이지을 참조하십시오.)

다중 도메인 구축에서 선택한 홈페이지가 사용자 어카운트가 액세스하는 모든 도메인에 적용됩니다. 참고로 여러 도메인에 자주 액세스하는 계정에 대한 홈페이지를 선택하는 경우, 특정 페이지가 전역 도메인으로 제한됩니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다.

단계 **2** **Home Page(**홈페이지**)**를 클릭합니다.

단계 **3** 홈페이지로 사용할 페이지를 드롭다운 목록에서 선택합니다.

드롭다운 목록의 옵션은 사용자 어카운트의 액세스 권한에 따라 달라집니다. 자세한 내용은 사용자 역할, 118 페이지를 참고하십시오.

단계 **4** **Save(**저장**)**를 클릭합니다.

이벤트 보기 구성

management center의 이벤트 보기 특성을 구성하려면 Event View Settings(이벤트 보기 설정) 페이지를 사용합니다. 일부 이벤트 보기 구성은 특정 사용자 역할만 사용할 수 있습니다. External Database User(외부 데이터베이스 사용자) 역할이 주어진 사용자는 이벤트 보기 설정 유저 인터페이스의 일부를 볼 수 있으나, 그러한 설정을 변경하더라도 크게 달라지지 않습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다.

단계 **2** **Event View Settings(**이벤트 보기 설정**)**를 클릭합니다.

단계 **3** **Event Preferences(**이벤트 환경 설정**)** 섹션에서 이벤트 보기의 기본 특징을 구성합니다. 이벤트 보기 환경 설정, 210 페이지를 참조하십시오.

단계 **4** **File Preferences(**파일 환경설정**)** 섹션에서 구성 파일 다운로드 환경 설정을 구성합니다. 파일 다운로드 기본 설정, 211 페이지를 참조하십시오.

단계 **5** **Default Time Windows(**기본 시간대**)** 섹션에서 기본 시간 창(복수 가능)을 구성합니다. 기본 시간대, 212 페이지를 참조하십시오.

단계 **6** **Default Workflow(**기본 워크플로**)** 섹션에서 기본 워크플로를 구성합니다. 기본 워크플로, 214 페이지를 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭합니다.

이벤트 보기 환경 설정

Event View Settings(이벤트 보기 설정) 페이지의 Event Preferenes(이벤트 환경설정) 섹션을 사용하여 Firepower System의 이벤트 보기 기본 특징을 구성합니다. 이 섹션은 모든 사용자 역할에서 사용할 수 있으나 이벤트 보기 권한이 없는 사용자에게는 별 의미가 없습니다.

다음 필드가 Event Preferences(이벤트 환경설정) 섹션에 나타납니다.

- **Confirm "All" Actions("**모든**" 작업 확인)** 필드는 어플라이언스에서 이벤트 보기의 모든 이벤트에 적용될 작업에 대해 반드시 사용자에게 확인하는지 여부를 제어합니다.

  예를 들어 이 설정이 활성화된 상태에서 이벤트 보기의 **Delete All(**모두 삭제**)**을 클릭할 경우, 현재 제약 조건을 충족하는 모든 이벤트(현재 페이지에 표시되지 않은 이벤트 포함)를 삭제할 것임을 사용자가 확인해야 어플라이언스가 데이터베이스에서 이를 삭제합니다.

- **Resolve IP Addresses(IP** 주소 분해**)** 필드는 어플라이언스가 이벤트 보기에서 가급적 IP 주소 대신 호스트 이름을 표시하도록 합니다.

  많은 IP 주소를 포함하고 이 옵션을 활성화한 경우 이벤트 보기에 표시되는 속도가 느려질 수 있습니다. 참고로 이 설정을 적용하려면 관리 인터페이스 구성을 사용해 시스템 설정에서 DNS 서버를 설정해야 합니다.

- **Expand Packet View(**패킷 보기 확대**)** 필드에서는 침입 이벤트에 대한 패킷 보기가 나타나는 방식을 구성할 수 있습니다. 기본적으로 어플라이언스는 패킷 보기의 축소 버전을 표시합니다.

- **None(**해당 없음**)** - 패킷 보기 중 Packet Information(패킷 정보) 섹션의 모든 하위 섹션을 축소합니다.
- **Packet Text(**패킷 텍스트**)** - Packet Text(패킷 텍스트) 하위 섹션만 확장합니다.
- **Packet Bytes(**패킷 바이트**)** - Packet Bytes(패킷 바이트) 하위 섹션만 확장합니다.
- **All(**모두**)** - 모든 섹션을 확장합니다.

기본 설정과 무관하게 언제라도 패킷 보기에서 섹션을 수동 확장하여 캡처된 패킷에 대한 세부 정보를 볼 수 있습니다.

- **Rows Per Page(**페이지당 행 수**)** 필드에서는 페이지당 몇 개의 이벤트 행을 드릴다운 페이지 및 테이블 보기에 표시할 것인지를 제어합니다.
- **Refresh Interval(**새로 고침 간격**)** 필드에서는 이벤트 보기의 새로 고침 간격을 분 단위로 설정합니다. 0을 입력하면 새로 고침 옵션이 비활성화됩니다. 이 간격은 대시보드에 적용되지 않습니다.
- **Statistics Refresh Interval(**통계 새로 고침 간격**)**은 Intrusion Event Statistics(침입 이벤트 통계) 페이지, Discovery Statistics(탐색 통계) 페이지와 같은 이벤트 요약 페이지의 새로 고침 간격을 제어합니다. 0을 입력하면 새로 고침 옵션이 비활성화됩니다. 이 간격은 대시보드에 적용되지 않습니다.
- **Deactivate Rules(**규칙 비활성화**)** 필드는 다음과 같이 표준 텍스트 규칙에 의해 생성된 침입 이벤트의 패킷 보기에 표시되는 링크를 제어합니다.
  - **All Policies(**모든 정책**)** - 로컬에 정의된 모든 사용자 지정 침입 정책에서 표준 텍스트 규칙을 비활성화하는 단일 링크
  - **Current Policy(**현재 정책**)** - 현재 배포된 침입 정책에서만 표준 텍스트 규칙을 비활성화하는 단일 링크 기본 정책의 규칙은 비활성화할 수 없습니다.
  - **Ask(**질문**)** - 이 옵션 각각의 링크

패킷 보기에서 이 링크를 표시하려면 사용자 어카운트가 관리자 또는 침입 관리자 액세스 권한을 가져야 합니다.

파일 다운로드 기본 설정

로컬 파일 다운로드의 기본 특성을 구성하려면 Event View Settings(이벤트 보기 설정) 페이지의 File Preferences(파일 환경설정)섹션을 사용합니다. 이 섹션은 Administrator(관리자), Security Analyst(보안 분석가) 또는 Security Analyst(Read Only)(보안 분석가(읽기 전용)) 사용자 역할만 사용할 수 있습니다.

어플라이언스에서 캡처된 파일의 다운로드를 지원하지 않을 경우 이 옵션은 비활성화됩니다.

다음 필드가 File Preferences(파일 환경설정) 섹션에 나타납니다.

- **Confirm 'Download File' Actions('**다운로드 파일' 확인 작업**)** 확인란은 파일을 다운로드할 때마다 File Download(파일 다운로드) 팝업 창이 나타나 경고를 표시하고 계속 또는 취소를 선택하게 할지를 제어합니다.

주의 Cisco에서는 악성코드를 다운로드하지 않을 것을 적극 권장합니다. 유해한 결과를 초래할 수 있습니다. 파일을 다운로드할 때는 주의하십시오. 악성코드가 포함되었을 수 있습니다. 파일을 다운로드하기 전에 다운로드 대상을 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.

파일을 다운로드할 때마다이 옵션을 비활성화할 수 있습니다.

- 캡처된 파일을 다운로드할 때 비밀번호로 보호되는 .zip 아카이브가 생성되며 여기에 파일이 들어 있습니다. **Zip File Passward(Zip** 파일 비밀번호**)** 필드에서는 .zip 파일에 대한 액세스 권한을 제한하기 위해 사용할 비밀번호를 정의합니다. 이 필드를 비워 둘 경우 비밀번호 없이 아카이브 파일이 생성됩니다.
- The **Show Zip File Password(Zip** 파일 비밀번호 표시**)** 확인란에서는 **Zip File Password(Zip** 파일 비밀번호**)** 필드에 일반 텍스트 아니면 난독 문자를 표시할지 선택합니다. 이 필드의 값을 지우면 **Zip File Password(Zip** 파일 비밀번호**)**는 난독 문자를 표시합니다.

기본 시간대

시간 범위라고도 하는 시간대는 임의의 이벤트 보기에서 이벤트에 대한 시간 제약 조건을 부여합니다. 시간대의 기본 동작을 제어하려면 Event View Settings(이벤트 보기 설정) 페이지의 Default Time Windows(기본 시간대) 섹션을 사용합니다.

이 섹션에 대한 사용자 역할 액세스 권한은 다음과 같습니다.

- Administor(관리자) 및 Maintenance Users(유지 보수 사용자)는 전체 섹션에 액세스할 수 있습니다.
- Security Analysts(보안 분석가)와 Security Analysts(Read Only)(보안 분석가(읽기 전용))는 **Audit Log Time Window(**감사 로그 시간대**)**을 제외한 모든 옵션에 액세스할 수 있습니다.
- Access Admins(액세스 관리자), Discovery Admins(검색 관리자), External Database Users(외부 데이터베이스 사용자), Intrusion Admins(침입 관리자), Network Admins(네트워크 관리자), Security Approvers(보안 승인자)는 **Events Time Window(**이벤트 시간대**)** 옵션만 액세스할 수 있습니다.

기본 시간대 설정과 무관하게 이벤트 분석 중 언제라도 개별 이벤트 보기의 시간대를 수동 변경할 수 있습니다. 또한 시간대 설정은 현재 세션에 대해서만 유효합니다. 로그아웃했다가 다시 로그인하면 시간대는 이 페이지에서 구현한 기본값으로 재설정됩니다.

3가지 이벤트 유형에 대해 기본 시간대를 설정할 수 있습니다.

- **Events Time Window(**이벤트 시간대**)**에서는 시간에 의한 제약이 가능한 대부분의 이벤트에 대해 단일 기본 시간 창을 설정합니다.
- **Audit Log Time Window(**감사 로그 시간대**)**에서는 감사 로그에 대한 기본 시간 창을 설정합니다.
- **Health Monitoring Time Window(**상태 모니터링 시간대**)**에서는 상태 이벤트에 대한 기본 시간 창을 설정합니다.

사용자 어카운트에서 액세스 가능한 이벤트 유형에 대해서만 시간대를 설정할 수 있습니다. 모든 사용자 유형이 이벤트 시간대를 설정할 수 있습니다. Administrators(관리자), Maintenance Users(유지 보수 사용자), Security Analysts(보안 분석가)는 상태 모니터링 시간 창을 설정할 수 있습니다. Administrators(관리자)와 Maintenance Users(유지 보수 사용자)는 감사 로그 시간대를 설정할 수 있습니다.

모든 이벤트 보기를 시간으로 제약할 수 없으므로, 시간 창 설정은 호스트, 호스트 속성, 애플리케이션, 클라이언트, 취약점, 사용자 ID 또는 규정준수 허용리스트 위반을 표시하는 이벤트 보기에는 적용되지 않습니다.

이벤트 유형별로 하나씩 **Multiple(**다중**)** 시간대를 사용하거나 모든 이벤트에 적용되는 **Single(**단일**)** 시간대를 사용할 수 있습니다. 단일 시간 창을 사용할 경우 3가지 시간 창 유형에 대한 설정이 사라지고 새로운 **Global Time Window(**전역 시간대**)** 설정이 나타납니다.

시간대에는 3가지 유형이 있습니다.

- 고정*(static)* 유형은 특정 시작 시간부터 종료 시간까지 생성된 모든 이벤트를 표시합니다.
- 확장*(expanding)* 유형은 특정 시작 시간부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 시간대가 확장되고 새 이벤트가 이벤트 보기에 추가됩니다.
- 슬라이딩*(sliding)* 유형은 특정 시작 시간(예: 1일 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 시간 창이 "슬라이딩"하므로 구성된 범위(이 예에서는 지난 1일)의 이벤트만 볼 수 있습니다.

모든 시간대의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다.

다음 옵션이 **Time Window Settings(**시간대 설정**)** 드롭다운 목록에 나타납니다.

- **Show the Last - Sliding(**마지막 표시 - 슬라이딩**)** 옵션에서는 사용자가 지정한 길이의 슬라이딩 기본 시간대를 구성할 수 있습니다.

  어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하면 시간대가 "슬라이딩"하므로 항상 지난 1시간의 이벤트가 표시됩니다.

- **Show the Last - Static/Expanding(**마지막 표시 - 고정/확장**)** 옵션에서는 사용자가 지정한 길이의 고정 또는 확장 기본 시간대를 구성할 수 있습니다.

  static(고정**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 활성화합니다. 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 사용자가 처음으로 이벤트를 본 시점까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다.

  expanding(확장**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 비활성화합니다. 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대 현재 시간으로 확장됩니다.

- **Current Day - Static/Expanding(**현재 날짜 - 고정/확장**)** 옵션에서는 현재 날짜에 대해 고정 또는 확장 기본 시간대를 구성할 수 있습니다. 현재 날짜는 현재 세션의 표준 시간대 설정에 따라 자정에 시작합니다.

static(고정**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 활성화합니다. 어플라이언스는 자정부터 사용자가 처음으로 이벤트를 본 시점까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다.

expanding(확장**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 비활성화합니다. 어플라이언스는 자정부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대가 현재 시간으로 확장됩니다. 로그아웃하기 전 24시간 이상 분석이 계속될 경우 이 시간대가 24시간을 초과할 수 있습니다.

- **Current Week - Static/Expanding(**현재 주 - 고정/확장**)** 옵션에서는 현재 주에 대해 고정 또는 확장 기본 시간대를 구성할 수 있습니다. 현재 주는 현재 세션의 표준 시간대 설정에 따라 이전 일요일 자정에 시작합니다.

  static(고정**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 활성화합니다. 어플라이언스는 자정부터 사용자가 처음으로 이벤트를 본 시점까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다.

  expanding(확장**)** 시간대에서는 **Use End Time(**사용 종료 시간**)** 확인란을 비활성화합니다. 어플라이언스는 일요일 자정부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대는 현재 시간으로 확장됩니다. 로그아웃하기 전 1주일 이상 분석이 계속될 경우, 시간대는 1주를 초과할 수 있습니다.

기본 워크플로

워크플로는 분석가가 이벤트 평가에 사용하는 데이터를 표시하는 일련의 페이지입니다. 어플라이언스는 이벤트 유형별로 하나 이상의 사전 정의된 워크플로를 기본적으로 제공합니다. 예를 들어 Security Analyst(보안 분석가)라면 수행하는 분석 유형에 따라 10가지 침입 이벤트 워크플로 중에서 선택할 수 있으며, 각 워크플로는 각기 다른 방식으로 침입 이벤트 데이터를 전달합니다.

어플라이언스는 이벤트 유형별로 하나의 기본 워크플로가 구성되어 있습니다. 예를 들어 Events by Priority and Classification(우선순위 및 분류별 이벤트) 워크플로는 침입 이벤트의 기본 워크플로입니다. 즉 침입 이벤트(검토된 침입 이벤트 포함)를 볼 때마다 Events by Priority and Classification(우선순위 및 분류별 이벤트) 워크플로가 표시됩니다.

그러나 각 이벤트 유형에 대한 기본 워크플로를 변경할 수 있습니다. 구성 가능한 기본 워크플로는 사용자 역할에 따라 달라집니다. 예를 들어 침입 이벤트 분석가는 기본 검색 이벤트 워크플로를 설정할 수 없습니다.

기본 표준 시간대 설정

이 설정은 작업 예약 및 대시보드 보기와 같은 사용자 계정에 대해서만 웹 인터페이스에 표시되는 시간을 결정합니다. 이 설정은 시스템 시간을 변경하거나 다른 사용자에게 영향을 주지 않으며, 일반적으로 UTC를 사용하는 시스템에 저장된 데이터에는 영향을 미치지 않습니다.

경고! User Preferences(사용자 환경 설정)의 Time Zone(표준 시간대) 기능에서는 시스템 시계가 UTC 시간으로 설정되었다고 가정합니다. 시스템 시간을 변경하지 마십시오. UTC 시스템 시간 변경은 지원되지 않으며, 변경할 경우 지원되지 않는 상태에서 복구하기 위해 디바이스 이미지를 다시 생성해야 합니다.

참고 이 기능은 시간 기반 정책 적용에 사용되는 표준 시간대에 영향을 주지 않습니다. **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**)**에서 디바이스의 표준 시간대를 설정합니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다.

단계 **2** **Time Zone(**표준 시간대**)** 드롭다운을 클릭합니다.

단계 **3** 사용하려는 표준 시간대가 속한 대륙이나 지역을 선택합니다.

단계 **4** 사용하려는 표준 시간대에 해당하는 국가 및 주 이름을 선택합니다.

기본 대시보드 지정

Overview(개요**) > Dashboards(**대시보드**)**를 선택하는 경우 기본 대시보드가 나타납니다. 변경되지 않는 경우, 모든 사용자에 대한 기본 대시보드는 요약(Summary) 대시보드입니다. 사용자 역할이 Administrator(관리자), Maintenance(유지 관리) 또는 Security Analyst(보안 분석가)인 경우 기본 대시보드를 변경할 수 있습니다.

다중 도메인 구축에서 선택한 기본 대시보드가 사용자 어카운트가 액세스하는 모든 도메인에 적용됩니다. 여러 도메인에 자주 액세스하는 계정에 대한 대시보드를 선택하는 경우, 특정 대시보드 위젯이 도메인에 의해 제한됩니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **User Preferences(**사용자 환경설정**)**를 선택합니다.

단계 **2** **Dashboard Settings(**대시보드 설정**)**을 클릭합니다.

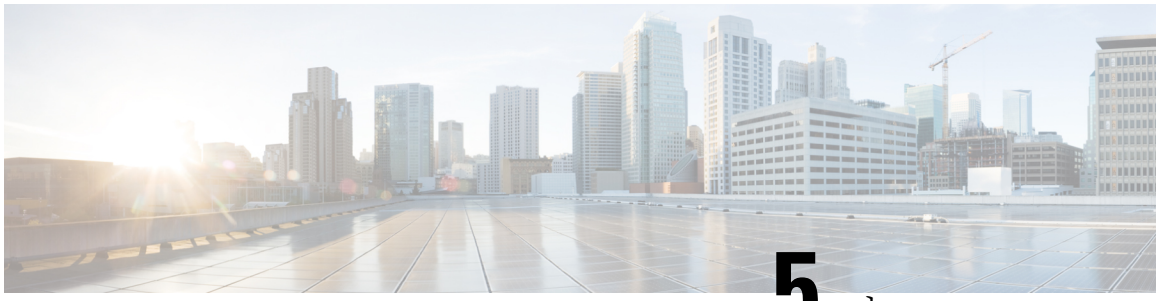
단계 **3** 기본으로 사용할 대시보드를 드롭다운 목록에서 선택합니다. **None(**해당 없음**)**을 선택하는 경우 **Overview(**개요**) > Dashboards(**대시보드**)**를 선택하면 확인할 대시보드를 선택할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

사용자 계정 히스토리

기능	버전	세부정보
셸 사용자 이름 템플릿 할당을 위한 새 필드를 추가했습니다.	7.0	LDAP 외부 인증을 위한 CLI 액세스 속성에 대한 템플릿을 지정하기 위한 프로비저닝-셸 사용자 이름 템플릿이 도입되었습니다. 따라서 CLI 속성에는 LDAP CLI 사용자를 식별하기 위한 고유한 템플릿이 있습니다. 신규/수정된 화면: 시스템 (⚙) > **Users(**사용자**)** > **External Authentication(**외부 인증**)**
SAML 2.0 호환 SSO 제공자를 사용하는 단일 로그인 지원을 추가했습니다.	6.7	타사 SAML 2.0 준수 ID 제공자 (IdP)에 구성된 외부 사용자에 대해 단일 로그인을 지원하는 기능을 추가했습니다. 여기에는 IdP에서 management center 사용자 역할로 사용자 또는 그룹 역할을 매핑하는 기능이 포함됩니다. 내부 또는 LDAP 또는 RADIUS에 의해 인증된 관리자 역할의 사용자만 SSO를 설정할 수 있습니다. 신규/수정된 화면: 시스템 (⚙) > **Users(**사용자**)** > **SSO(Single Sign-On,** 단일 인증**)**
웹 인터페이스의 테마.	6.6	웹 인터페이스의 모양과 느낌을 선택할 수 있습니다. Light 또는 Dusk 테마를 선택하거나 이전 릴리스에서 사용된 Classic 테마를 사용합니다. 신규/수정된 화면: User Name(사용자 이름) > **User Preferences(**사용자 환경 설정**)** > **General(**일반**)** > **UI Themes(UI** 테마**)** 지원되는 플랫폼: management center
사용자 계정의 이름에 대한 새 필드를 추가했습니다.	6.6	내부 사용자 계정을 담당하는 사용자 또는 부서를 식별할 수 있는 필드를 추가했습니다. 신규/수정된 화면: 시스템 (⚙) > **Users(**사용자**)** > **Users(**사용자**)> Real Name(**실제 이름**)** 필드
Cisco Security Manager SSO(Single Sign-On)가 더 이상 지원되지 않음	6.5	management center와 Cisco Security Manager 간의 SSO(Single Sign-On)는 Firepower 6.5부터 더 이상 지원되지 않습니다. 신규/수정된 화면: 시스템 (⚙) > **Users(**사용자**)CSM SSO(CSM Single Sign-on)**을 선택합니다.

기능	버전	세부정보
향상된 비밀번호 보안.	6.5	이제 새로운 강력한 비밀번호 요구 사항이 장의 단일 위치에 표시되며, 다른 장에서 상호참조됩니다. 비밀번호 변경 인터페이스에 새 필드인 **Show Password(**비밀번호 표시**)** 및 **Generate Password(**비밀번호 생성**)**가 추가되었습니다. 신규/수정된 화면: User Name(사용자 이름) > **User Preferences(**사용자 환경 설정**)** > **General(**일반**)** > **Change Password(**비밀번호 변경**)**



5 장

도메인

다음 주제는 도메인을 사용해 멀티 테넌시를 관리하는 방법을 설명합니다.

도메인을 사용하는 다중 테넌시 소개

management center을 사용하면 도메인을 사용하는 멀티 테넌시를 구현할 수 있습니다. 도메인에 따라 매니지드 디바이스, 구성 및 이벤트에 대한 사용자 액세스가 구분됩니다. 최고 수준 글로벌 도메인에 2~3개의 레벨로 최대 100개의 하위 도메인을 생성할 수 있습니다.

management center에 로그인하는 경우, *current domain(*현재 도메인*)*이라고 하는 단일 도메인에 로그인합니다. 사용자 어카운트에 따라 다른 도메인으로 전환할 수 있습니다.

사용자 역할에 의해 부과된 제한 외에도 현재 도메인 레벨이 다양한 구성을 수정할 수 있는 기능을 제한할 수 있습니다. management center은 시스템 소프트웨어 업데이트와 같은 대부분의 관리 작업을 전역 도메인으로 제한합니다.

management center은 다른 작업을 하위 도메인이 없는 리프 도메인으로 제한합니다. 예를 들어 각 매니지드 디비아스를 리프 도메인과 연결하고 해당 리프 도메인의 컨텍스트에서 디바이스 관리 작업을 수행해야합니다. 각 디바이스는 단일 도메인에만 속할 수 있습니다.

각 리프 도메인은 해당 리프 도메인의 디바이스에서 수집한 검색 데이터를 기반으로 자체 네트워크 맵을 작성합니다. 매니지드 디바이스에서 보고한 이벤트(연결, 침입, 악성코드 등)도 디바이스의 리프 도메인에 연결됩니다.

도메인 레벨 **1:** 전역

멀티 테넌시를 구성하지 않는 경우, 모든 디바이스, 설정 및 이벤트가 전역 도메인에 속하며 이 시나리오에서는 리프 도메인이기도 합니다. 도메인 관리를 제외하고 시스템은 하위 도메인이 추가될 때까지 도메인별 구성 및 분석 옵션을 숨깁니다.

두 개의 도메인 레벨**:** 전역 및 **2**차 레벨

2단계 다중 도메인 구축에서 전역 도메인에는 직계 하위 도메인만 있습니다. 예를 들어 MSSP(매니지드 보안 서비스 제공자)는 여러 고객에 대한 네트워크 보안을 관리하기 위해 단일 management center를 사용할 수 있습니다.

- 전역 도메인에 로그인하는 MSSP 관리자는 고객의 구축을 보거나 편집할 수 없습니다. 고객의 구축을 관리하려면 각각 두 번째 수준의 명명된 하위 도메인에 로그인해야 합니다.
- 각 고객의 관리자는 두 번째 수준의 이름이 지정된 하위 도메인에 로그인하여 조직에 적용 가능한 디바이스, 구성 및 이벤트만 관리할 수 있습니다. 이런 로컬 관리자는 MSSP 내 다른 고객의 구축을 보거나 영향을 줄 수 없습니다.

세 개의 도메인 레벨**:** 전역**, 2**차 레벨 및 **3**차 레벨

3단계 다중 도메인 구축에서 전역 도메인에는 하위 도메인이 있으며, 그 중 적어도 하나가 자체 하위 도메인입니다. 앞의 예를 확장해, 이미 하위 도메인으로 제한되어 있는 MSSP 고객이 구축을 더욱 세분화하려는 시나리오를 생각해 보겠습니다. 이 고객은 디바이스 두 부류를 따로 관리하고자 합니다(네트워크 에지에 배치된 디바이스 및 내부에 배치된 디바이스).

- 두 번째 수준 하위 도메인에 로그인하는 고객의 관리자는 고객의 엣지 네트워크 구축을 보거나 편집할 수 없습니다. 네트워크 엣지에 구축된 디바이스를 관리하려면 해당 리프 도메인에 로그인해야 합니다.
- 고객의 엣지 네트워크 관리자는 세 번째 수준(리프) 도메인에 로그인하여 네트워크 엣지에 구축된 디바이스에 적용 가능한 디바이스, 구성 및 이벤트만 관리할 수 있습니다. 마찬가지로 고객의 내부 네트워크 관리자는 내부 디바이스, 구성 및 이벤트를 관리하기 위해 다른 3차 도메인에 로그인할 수 있습니다. 엣지 및 내부 관리자는 서로의 구축을 볼 수 없습니다.

참고 멀티테넌시를 사용하는 management center에서 SSO 구성은 전역 도메인 레벨에서만 적용할 수 있으며, 전역 도메인 및 모든 하위 도메인에 적용됩니다.

관련 항목

SAML SSO(Single Sign-On) 구성, 145 페이지

도메인 용어

이 문서에서는 도메인 및 다중 도메인 배포에 대해 다음 용어를 사용합니다.

전역 도메인

다중 도메인 구축의 경우, 최상위 도메인을 표시 합니다. 멀티 테넌시를 구성하지 않는 경우 모든 디바이스, 설정 및 이벤트는 전역 도메인에 해당됩니다. 관리자가 전역 도메인의 전체 Firepower System 구축을 관리할 수 있습니다.

서브도메인

이차 또는 삼차 도메인입니다.

이차 도메인

전역 도메인의 하위 도메인입니다. 이차 도메인은 리프 도메인 또는 하위 도메인이 될 수 있습니다.

삼차 도메인

이차 도메인의 하위 도메인입니다. 삼차 도메인은 항상 리프 도메인입니다.

리프 도메인

하위 도메인이 없는 도메인입니다. 각 디바이스는 리프 도메인에 속해야 합니다.

하위 도메인

계층 구조에서 현재 도메인의 하위 단계에 있는 도메인입니다.

하위 도메인

도메인의 직접 하위 도메인입니다.

최상위 도메인

현재 도메인을 하위 도메인으로 갖는 도메인입니다.

상위 도메인

도메인의 직접 상위 도메인입니다.

동기 도메인

상위 도메인이 동일한 도메인입니다.

현재 도메인

현재 로그인한 도메인입니다. 시스템은 웹 인터페이스의 오른쪽 상단 사용자 이름 앞에 현재 도메인의 이름을 표시합니다. 사용자 역할이 제한된 경우가 아니라면 현재 도메인의 설정을 수정할 수 있습니다.

도메인 속성

도메인 속성을 수정하려면 해당 도메인의 상위 도메인에서 관리자 권한이 있어야 합니다.

이름 및 설명

각 도메인의 이름은 계층 내에서 고유해야 합니다. 설명은 선택 사항입니다.

상위 도메인

두 번째 및 세 번째 레벨 도메인에는 상위 도메인이 있습니다. 도메인을 생성한 후에는 도메인의 상위 항목을 변경할 수 없습니다.

디바이스

리프 도메인만 디바이스를 포함할 수 있습니다. 즉, 도메인은 하위 도메인이나 디바이스 중 하나만 포함할 수 있으며 둘 다 포함할 수는 없습니다. 리프가 아닌 도메인이 디바이스를 직접 제어하는 구축은 저장할 수 없습니다.

도메인 편집기에서 웹 인터페이스에는 도메인 계층 내의 현재 위치에 따라 사용 가능한 디바이스와 선택한 디바이스가 표시됩니다.

호스트 제한

management center에서 모니터링할 수 있는 호스트의 수, 즉 네트워크 맵에 저장할 수 있는 호스트 수는 해당 모델에 따라 다릅니다. 다중 도메인 구축에서 리프 도메인은 모니터링되는 호스트의 사용 가능 풀을 공유하지만, 네트워크 맵은 각기 다릅니다.

각 리프 도메인이 네트워크 맵을 채울 수 있도록 각 하위 도메인 레벨에서 호스트 제한을 설정할 수 있습니다. 도메인의 호스트 제한을 **0**으로 설정하면 도메인이 일반 풀을 공유합니다.

호스트 제한을 설정할 때 각 도메인 레벨에 미치는 영향은 서로 다릅니다.

- 리프 - 리프 도메인의 경우 호스트 제한은 리프 도메인이 모니터링할 수 있는 호스트 수에 대한 단순한 제한입니다.
- 두 번째 레벨 - 세 번째 레벨 리프 도메인을 관리하는 두 번째 레벨 도메인의 경우 호스트 제한은 리프 도메인이 모니터링할 수 있는 총 호스트 수를 나타냅니다. 리프 도메인은 사용 가능한 호스트 풀을 공유합니다.
- 글로벌 - 글로벌 도메인의 경우 호스트 제한은 management center에서 모니터링할 수 있는 총 호스트 수와 같습니다. 이 값은 변경할 수 없습니다.

하위 도메인의 호스트 제한을 합한 값이 상위 도메인의 호스트 제한보다 커질 수 있습니다. 예를 들어 글로벌 도메인 호스트 제한이 150,000이면 각기 호스트 제한이 100,000인 하위 도메인을 여러 개 구성할 수 있습니다. 이러한 각 도메인은 100,000개의 호스트를 모니터링할 수 있지만 모든 도메인이 100,000개의 호스트를 모니터링할 수 있는 것은 아닙니다.

네트워크 검색 정책은 호스트 제한에 도달한 후 새 호스트가 탐지될 때 수행되는 작업을 제어합니다. 새 호스트를 삭제하거나 가장 오랫동안 비활성 상태였던 호스트를 교체할 수 있습니다. 각 리프 도메인에 자체 네트워크 검색 정책이 있으므로, 각 리프 도메인은 시스템에서 새 호스트를 검색할 때 고유한 동작을 관리합니다.

도메인의 호스트 제한을 줄이는 경우 네트워크 맵에 새 제한보다 많은 호스트가 포함되어 있으면 가장 오랫동안 비활성 상태였던 호스트가 삭제됩니다.

관련 항목

Firepower System 호스트 제한
네트워크 검색 데이터 스토리지 설정

도메인 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

도메인 관리

도메인 속성을 수정하려면 해당 도메인의 상위 도메인에서 관리자 권한이 있어야 합니다.

프로시저

단계 **1** 시스템 ( ) > **Domains(**도메인**)**를 선택합니다.

단계 **2** 도메인을 관리합니다.

- Add(추가) - **Add Domain(**도메인 추가**)**을 클릭하거나 상위 도메인 옆에 있는 **Add Subdomain(**하위 도메인 추가**)**을 클릭합니다. 새 도메인 생성, 224 페이지를 참조하십시오.
- Edit(수정) - 수정할 도메인 옆에 있는 아이콘**(Edit(**수정**)** ( ))을 클릭합니다. 도메인 속성, 221 페이지를 참조하십시오.
- Delete(삭제) - 삭제할 빈 도메인 옆에 있는 아이콘**(Delete(**삭제**)** ( ))을 클릭한 다음 선택 내용을 확인합니다. 대상 도메인을 수정하여 삭제할 도메인에서 디바이스를 이동합니다.

단계 **3** 도메인 구조를 변경하고 모든 디바이스를 리프 도메인과 연결한 후에 **Save(**저장**)**를 클릭하여 변경사항을 구현합니다.

단계 **4** 메시지가 표시되면 추가로 다음과 같이 변경합니다.

- 리프 도메인을 상위 도메인으로 변경한 경우 이전 네트워크 맵을 이동하거나 삭제합니다. 도메인 간 데이터 이동, 225 페이지를 참조하십시오.
- 도메인 간에 디바이스를 이동했으며 새 정책과 보안 영역 또는 인터페이스 그룹을 할당해야 하는 경우 도메인 간 디바이스 이동, 225 페이지를 참조하십시오.

다음에 수행할 작업

- 모든 새 도메인에 대한 사용자 역할 및 정책(액세스 제어, 네트워크 검색 등)을 구성합니다. 필요한 경우 디바이스 속성을 업데이트합니다.
- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

새 도메인 생성

최고 수준 글로벌 도메인에 2~3개의 레벨로 최대 100개의 하위 도메인을 생성할 수 있습니다.

모든 디바이스를 리프 도메인에 할당해야 도메인 컨피그레이션을 구현할 수 있습니다. 리프 도메인에 하위 도메인을 추가하면 도메인은 더 이상 리프 도메인이 아니며, 해당 도메인의 디바이스를 재할당해야 합니다.

프로시저

단계 **1** 글로벌 또는 두 번째 수준 도메인에서 시스템 (⚙) > **Domains(**도메인**)**를 선택합니다.

단계 **2** **Add Domain(**도메인 추가**)**을 클릭하거나 상위 도메인 옆에 있는 **Add Subdomain(**하위 도메인 추가**)**을 클릭합니다.

단계 **3** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **4** **Parent Domain(**상위 도메인**)**을 선택합니다.

단계 **5** **Devices(**디바이스**)**에서 도메인에 추가할 **Available Devices(**사용 가능한 디바이스**)**를 선택한 다음 **Add to Domain(**도메인에 추가**)**을 클릭하거나 **Selected Devices(**선택한 디바이스**)** 목록으로 끌어다 놓습니다.

단계 **6** 필요한 경우 **Advanced(**고급**)**을 클릭하여 새 도메인이 모니터링할 수 있는 호스트 수를 제한합니다. 도메인 속성, 221 페이지를 참조하십시오.

단계 **7** **Save(**저장**)**를 클릭하여 도메인 관리 페이지로 돌아갑니다.

리프 도메인이 아닌 도메인에 할당된 디바이스가 있는지 확인하라는 경고가 표시됩니다. **Create New Domain(**새 도메인 생성**)**을 클릭하여 해당 디바이스용으로 새 도메인을 생성합니다. 디바이스를 기존 도메인으로 이동하려는 경우에는 **Keep Unassigned(**미할당 상태 유지**)**를 클릭합니다.

단계 **8** 도메인 구조를 변경하고 모든 디바이스를 리프 도메인과 연결한 후에 **Save(**저장**)**를 클릭하여 변경사항을 구현합니다.

단계 **9** 메시지가 표시되면 추가로 다음과 같이 변경합니다.

- 리프 도메인을 상위 도메인으로 변경한 경우 이전 네트워크 맵을 이동하거나 삭제합니다. 도메인 간 데이터 이동, 225 페이지를 참조하십시오.
- 도메인 간에 디바이스를 이동했으며 새 정책과 보안 영역 또는 인터페이스 그룹을 할당해야 하는 경우 도메인 간 디바이스 이동, 225 페이지를 참조하십시오.

다음에 수행할 작업

- 모든 새 도메인에 대한 사용자 역할 및 정책(액세스 제어, 네트워크 검색 등)을 구성합니다. 필요한 경우 디바이스 속성을 업데이트합니다.
- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

도메인 간 데이터 이동

이벤트 및 네트워크 맵은 리프 도메인과 연결되므로 리프 도메인을 상위 도메인으로 변경하는 경우 다음 두 가지 작업 중에서 선택할 수 있습니다.

- 네트워크 맵과 연결된 이벤트를 새 리프 도메인으로 이동합니다.
- 네트워크 맵을 삭제하되 이벤트는 유지합니다. 이 경우 시스템이 필요에 따라 또는 구성된 대로 이벤트를 정리할 때까지 이벤트는 상위 도메인과 연결된 상태로 유지됩니다. 또는 기존 이벤트를 수동으로 삭제할 수 있습니다.

시작하기 전에

이전의 리프 도메인이 이제 상위 도메인이 되는 도메인 컨피그레이션을 구현합니다. 도메인 관리, 223 페이지를 참조하십시오.

프로시저

단계 **1** 현재는 상위 도메인인 이전의 각 리프 도메인에 대해 다음 작업을 수행합니다.

- **Parent Domain(**상위 도메인**)**의 이벤트와 네트워크 맵을 상속할 새 **Leaf Domain(**리프 도메인**)**을 선택합니다.
- **None(**없음**)**을 선택하여 상위 도메인의 네트워크 맵을 삭제하되 기존 이벤트는 유지합니다.

단계 **2** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

도메인 간 디바이스 이동

디바이스를 이동하는 도메인에서 소스 및 대상 도메인을 볼 수 있는 한 도메인 간에 디바이스를 이동할 수 있습니다. 도메인 간에 디바이스를 이동하면 해당 디바이스에 적용된 컨피그레이션과 정책에

영향을 줄 수 있습니다. 시스템은 도메인 간에 디바이스를 이동하는 동안 다음 디바이스 구성을 유지합니다.

- 인터페이스
- 인라인 세트
- 라우팅
- DHCP
- 연결된 개체
- SNMP(사용 가능한 경우)

도메인 간에 이동할 때 디바이스 구성에 다음 변경 사항이 발생할 수 있습니다.

- 디바이스를 대상 도메인으로 이동한 후 시스템에서 디바이스 구성을 유지하려면 다음을 확인하십시오.
  - 공유 액세스 제어 정책은 전역 도메인에 있습니다. 또한 다른 공유 정책은 전역 도메인에 있는 것이 좋습니다.
- VPN 구성의 경우,
  - 사이트 간 VPN 구성은 대상 도메인에 있습니다.
  - 원격 액세스 VPN 구성 및 디바이스 인증서는 글로벌 또는 대상 도메인에 있습니다.
  - 디바이스에 원격 액세스 VPN 정책을 할당할 때는 대상 도메인이 원격 액세스 VPN이 구성되어 있는 도메인의 하위 도메인이어야 도메인 간에 디바이스를 이동할 수 있습니다.
- SNMP의 네트워크 개체는 전역 도메인에 있습니다.
- 디바이스에 등록된 인증서를 삭제하지 않고도 하위 도메인으로 디바이스를 이동할 수 있습니다. 구체적으로,
  - 이동한 디바이스에 적용된 상태 정책이 새 도메인에서 액세스할 수 없는 경우 새 상태 정책을 선택할 수 있습니다.
  - 이동한 디바이스에 할당된 액세스 제어 정책이 새 도메인에서 유효하지 않거나 액세스할 수 없는 경우 새 정책을 선택합니다. 각 디바이스에 액세스 제어 정책이 할당되어 있어야 합니다.
  - 이동한 디바이스의 인터페이스가 새 도메인에서 액세스할 수 없는 보안 영역에 속해 있는 경우 새 영역을 선택할 수 있습니다.
  - 다음 항목에서 인터페이스가 제거됩니다.
    - 새 도메인에서 액세스할 수 없으며 액세스 제어 정책에서 사용되지 않는 보안 영역
    - 모든 인터페이스 그룹

디바이스에서 정책을 업데이트해야 하는데 영역 간에 인터페이스를 이동할 필요가 없는 경우에는 영역 컨피그레이션이 최신 상태라는 메시지가 표시됩니다. 예를 들어 디바이스의 인터페이스가 공통 상위 도메인에 구성된 보안 영역에 속해 있는 경우에는 하위 도메인 간에 디바이스를 이동할 때 영역 컨피그레이션을 업데이트할 필요가 없습니다.

시작하기 전에

- 새 도메인 생성 자세한 내용은 새 도메인 생성, 224 페이지을 참고하십시오.
- 도메인 간에 디바이스를 이동했으며 이제 새 정책과 보안 영역을 할당해야 하는 도메인 컨피그레이션을 구현합니다. 도메인 관리, 223 페이지를 참조하십시오.

프로시저

단계 **1** 글로벌 도메인에서, **System(**시스템**)** (⚙) > **Domains(**도메인**)**을 선택합니다.

단계 **2** 디바이스를 이동하려는 대상 도메인을 편집합니다.

단계 **3** **Edit Domain(**도메인 편집**)** 대화 상자에서 다음을 수행합니다.

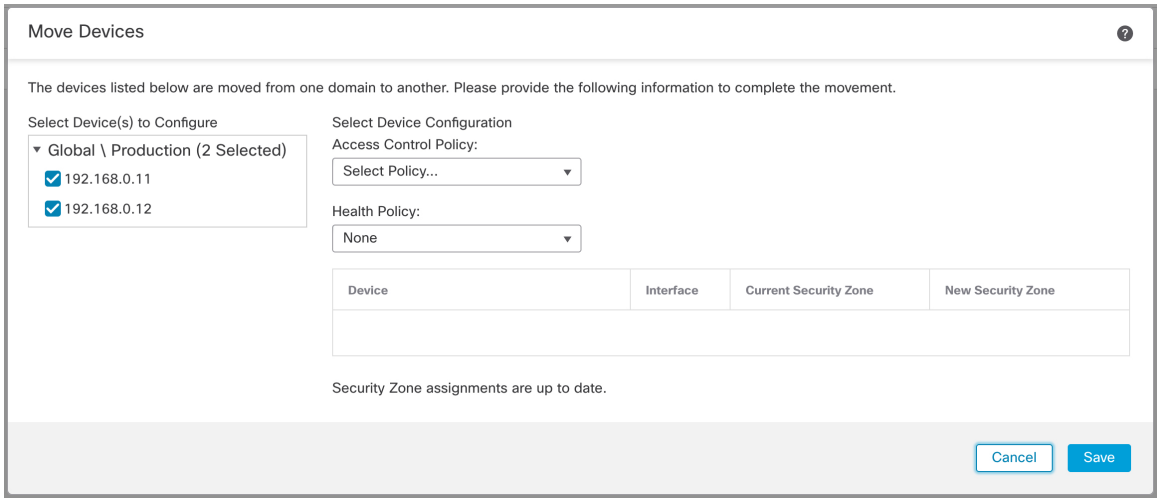
1. 이동할 디바이스를 선택하고 **Add to Domain(**도메인에 추가**)**를 클릭합니다.
2. **Save(**저장**)**를 클릭합니다.

단계 **4** 도메인 페이지에서 **Save(**저장**)**을 클릭합니다.

단계 **5** **(**액세스 제어 정책이 전역 도메인에 없는 경우**) Move Devices(**디바이스 이동**)** 대화 상자에서 다음을 수행합니다.

1. **Select Device(s) to Configure(**구성할 디바이스 선택**)**에서 구성하려는 디바이스를 선택하십시오.

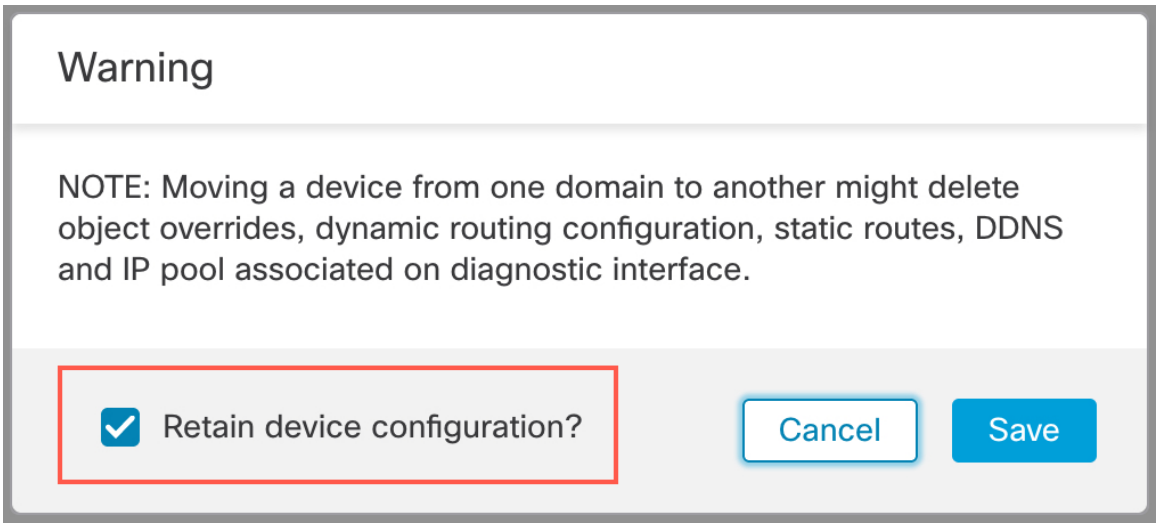
   동일한 상태 및 액세스 제어 정책을 할당할 디바이스를 여러 개 선택합니다.



2. 디바이스에 적용할 **Access Control Policy(**액세스 제어 정책**)**를 선택하거나 **New Policy(**새 정책**)**를 선택하여 새 정책을 생성합니다.

3. 디바이스에 적용할 **Health Policy(**상태 정책**)**를 선택하거나 **None(**없음**)**을 선택하여 상태 정책이 없는 상태로 디바이스를 유지합니다.
4. 새 영역에 인터페이스를 할당하라는 메시지가 표시되면 나열된 각 인터페이스에 대해 **New Security Zone(**새 보안 영역**)**을 선택하거나 **None(**없음**)**을 선택하여 나중에 인터페이스를 할당합니다.
5. 영향받는 모든 디바이스를 구성한 후 **Save(**저장**)**를 클릭하여 정책 및 영역 할당을 저장합니다.

단계 **6** 이동 후 디바이스 구성을 유지하려면, 디바이스 구성을 유지하시겠습니까**?** 확인란을 선택합니다.



이 옵션을 선택하면 디바이스가 대상 도메인으로 이동된 후 시스템이 디바이스 구성을 유지합니다. 이 옵션을 선택하지 않으면 이동의 영향을 받은 이동된 디바이스에서 디바이스 구성을 수동으로 업데이트해야 합니다.

다음 표에서는 다양한 시나리오에서 개체를 처리하는 방법을 보여줍니다.

시나리오	시스템 작업
개체가 대상 도메인에 있습니다.	개체를 재사용합니다.
동일한 이름 및 값을 가진 개체가 대상 도메인에 존재합니다.	개체를 재사용합니다.
이름은 같지만 값이 다른 개체가 대상 도메인에 존재합니다.	• 네트워크 및 포트 - 개체 오버라이드를 생성합니다. • 인터페이스 개체 - 유형이 다른 경우 새 개체를 생성합니다. • 이름 일치에 따라 다른 모든 개체 유형을 재사용합니다.
대상 도메인에 개체가 없습니다.	새 개체를 생성합니다.

단계 **7** **Save(**저장**)**를 클릭하여 도메인 컨피그레이션을 구현합니다.

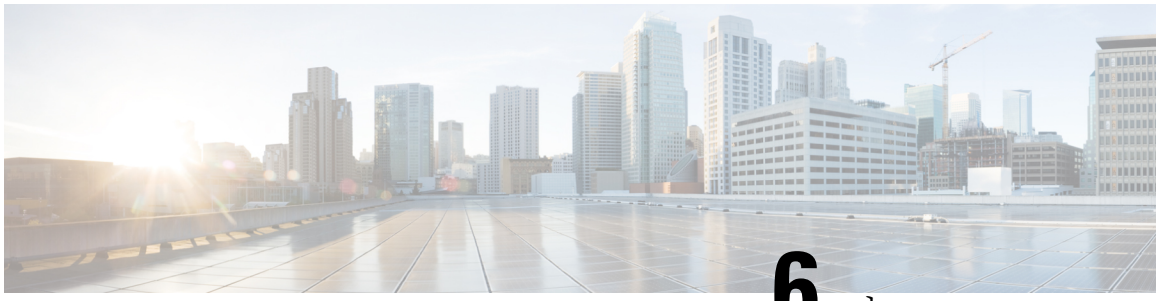
단계 **8** 도메인 구성이 완료되면 **OK(**확인**)**을 클릭합니다.

다음에 수행할 작업

- 이동의 영향을 받은 이동한 디바이스의 기타 컨피그레이션을 업데이트합니다.
- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.
- 도메인 간에 디바이스를 이동한 후 시스템이 디바이스 구성을 유지하지 못하는 경우 디바이스 구성을 수동으로 복원할 수 있습니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스 구성 내보내기 및 가져오기를 참고하십시오.

도메인 관리 기록

기능	버전	세부 사항
사이트 대 사이트 VPN과 관련된 디바이스 구성 유지	7.3	이제 한 도메인에서 다른 도메인으로 디바이스를 이동하는 동안, 대상 도메인에 사이트 대 사이트 VPN이 구성된 경우에만 사이트 대 사이트 VPN과 연결된 디바이스 구성을 유지할 수 있습니다.
디바이스 구성 유지	7.2	이제 도메인 간에 디바이스를 이동하는 동안 디바이스 구성을 유지할 수 있습니다.
지원되는 최대 도메인 수 증가	6.5	이제는 도메인을 100개까지 추가할 수 있습니다. 이전에는 최대 50개의 도메인만 구축할 수 있었습니다. 지원되는 플랫폼: Secure Firewall Management Center



6 장

업데이트

이 장에서는 시스템 소프트웨어 및 데이터베이스를 업데이트하는 방법을 설명합니다.

시스템 업데이트 정보

management center를 사용하여 자체 및 관리하는 디바이스의 시스템 소프트웨어를 업그레이드할 수 있습니다. 또한 고급 서비스를 제공하는 다양한 데이터베이스 및 피드를 업데이트할 수 있습니다.

인터넷에 액세스할 수 있는 management center의 경우, 시스템은 종종 Cisco에서 직접 업데이트를 가져올 수 있습니다. 가능한 경우 자동 콘텐츠 업데이트를 예약하거나 활성화하는 것이 좋습니다. 일부 업데이트는 초기 설정 프로세스에서 또는 관련 기능을 활성화할 때 자동으로 활성화됩니다. 기타 업데이트는 직접 예약해야 합니다. 초기 설정 후 모든 자동 업데이트를 검토하고 필요한 경우 조정하는 것이 좋습니다.

표 *6:* 업그레이드 및 업데이트

구성 요소	설명	세부정보
시스템 소프트웨어	주요 소프트웨어 릴리스에는 새로운 기능과 향상된 기능이 포함되어 있습니다. 여기에는 인프라 또는 아키텍처 변경 사항이 포함될 수 있습니다. 유지 보수 릴리스에는 일반적인 버그 및 보안 관련 수정 사항이 포함되어 있습니다. 동작 변경은 거의 포함되지 않으며, 동작 변경이 포함되는 경우 이러한 수정과 관련이 있습니다. 패치는 온디맨드 업데이트로, 시급한 중요 수정 사항만을 제공합니다. 핫픽스는 특정 고객 문제를 해결할 수 있습니다.	직접 다운로드: 패치 및 유지 보수 릴리스만 선택합니다. 보통 릴리스 이후에 얼마간 수동으로 다운로드할 수 있습니다. 지연되는 기간은 릴리스 유형, 릴리스 채택 및 기타 요인에 따라 달라집니다. 온디맨드 다운로드 및 예약 다운로드가 모두 지원됩니다. 설치 예약: 패치와 유지 보수 릴리스만 예약 작업으로 수행합니다. 제거: 패치만 해당됩니다. 되돌리기: threat defense를 위한 주요 릴리스 및 유지 보수 릴리스에만 해당됩니다. management center 또는 Classic 디바이스에서는 되돌리기가 지원되지 않습니다. 이미지 재설치: 주요 릴리스 및 유지 보수 릴리스에만 해당됩니다. 참조: management center가 현재 실행 중인 버전에 대한 Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드입니다.
VDB(Vulnerability Database)	Cisco VDB(취약성 데이터베이스)는 호스트가 영향을 받기 쉬운 알려진 취약성의 데이터베이스인 동시에 운영 체제, 클라이언트 및 애플리케이션의 지문이기도 합니다. 시스템이 VDB를 사용하여 특정 호스트가 침해 위험을 높이는지 여부를 결정합니다.	직접 다운로드: 예. 예약: 예. 예약된 작업으로 수행됩니다. 제거: VDB 357부터 management center에 대한 기준 VDB까지 모든 VDB를 설치할 수 있습니다. 참조: 취약성 데이터베이스(VDB) 업데이트, 234 페이지
GeoDB(지리위치 데이터베이스)	Cisco 지리위치 데이터베이스(GeoDB)는 라우팅 가능한 IP 주소와 관련된 지리적 및 연결 관련 데이터의 데이터베이스입니다.	직접 다운로드: 예. 예약: 예. 자체 업데이트 페이지에서 수행됩니다. 제거: 아니요. 참조: GeoDB(지리위치 데이터베이스) 업데이트, 236 페이지

구성 요소	설명	세부정보
침입 규칙(SRU/LSP)	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.	직접 다운로드: 예. 예약: 예. 자체 업데이트 페이지에서 수행됩니다. 제거: 아니요. 참조: 침입 규칙 업데이트, 238 페이지
보안 인텔리전스 피드	보안 인텔리전스 피드는 항목과 일치하는 트래픽을 빠르게 필터링하는 데 사용할 수 있는 IP 주소, 도메인 이름 및 URL의 모음입니다.	직접 다운로드: 예. 예약: 예. 개체 관리자에서 수행됩니다. 제거: 아니요. 참조: Cisco Secure Firewall Management Center 디바이스 구성 가이드
URL 범주 및 평판	URL 필터링을 사용하면 URL의 일반 분류(범주) 및 위험 수준(평판)을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다.	직접 다운로드: 예. 예약: 예. 통합/클라우드 서비스를 구성할 때 또는 예약된 작업으로 수행됩니다. 제거: 아니요. 참조: Cisco Secure Firewall Management Center 디바이스 구성 가이드

시스템 업데이트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

글로벌 달리 명시되지 않은 경우

사용자 역할

관리자

시스템 업데이트에 대한 가이드라인 및 제한 사항

업데이트 하기 전에

구축 구성 요소(침입 규칙, VDB 또는 GeoDB 포함)를 업데이트하기 전에 업데이트와 함께 제공되는 릴리스 정보 또는 권고 텍스트를 읽어 보십시오. 호환성, 사전 요구 사항, 새로운 기능, 동작 변경, 경고 등 중요 및 릴리스 별 정보를 제공합니다.

예약된 업데이트

시스템은 UTC 기준으로 작업을 예약합니다(업데이트 포함). 즉, 로컬에서 발생하는 시간은 날짜와 사용자의 특정 위치에 따라 달라집니다. 또한 업데이트는 UTC 기준으로 예약되기 때문에 일광 절약 시간, 서머 타임 또는 사용자 위치에서 발생할 수 있는 계절 조정의 영향을 받지 않습니다. 영향을 받는다면, 예약된 업데이트는 현지 시간에 따라 여름에는 겨울보다 1시간 '후'에 실행됩니다

중요 예약된 업데이트가 의도한 시점에 수행되는지 확인하기를 적극 권장합니다.

대역폭 지침

시스템 소프트웨어를 업그레이드하거나 준비도 확인을 실행하려면 업그레이드 패키지가 어플라이언스에 있어야 합니다. 업그레이드 패키지 크기는 다양합니다. 관리되는 디바이스로 대량 데이터 전송을 수행할 수 있는 대역폭을 사용하고 있는지 확인합니다. Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(문제 해결 TechNote)

시스템 소프트웨어 업그레이드

이 설명서에는 시스템 소프트웨어 또는 함께 제공되는 운영 체제에 대한 자세한 업그레이드 지침이 포함되어 있지 않습니다. Management Center를 업그레이드하든 Threat Defense를 업그레이드하든 관계없이 management center을 현재 실행 중인 버전에서는 Management Center용 Cisco Secure Firewall Threat Defense 업그레이드 가이드의 내용을 참고하십시오.

업그레이드 예약에 대한 자세한 내용은 소프트웨어 업그레이드 자동화, 512 페이지의 내용을 참고하십시오. 초기 설정 프로세스에서는 자동으로 매주 다운로드를 예약합니다. 설정 후 자동 예약 구성을 검토하고 필요한 경우 조정해야 합니다.

취약성 데이터베이스(VDB) 업데이트

Cisco VDB(취약성 데이터베이스)는 호스트가 영향을 받기 쉬운 알려진 취약성의 데이터베이스인 동시에 운영 체제, 클라이언트 및 애플리케이션의 지문이기도 합니다. 시스템이 VDB를 사용하여 특정 호스트가 침해 위험을 높이는지 여부를 결정합니다.

Cisco는 VDB에 주기적인 업데이트를 제공합니다. management center에서 VDB 및 관련 매핑 업데이트에 걸리는 시간은 네트워크 맵에 있는 호스트 수에 따라 달라집니다. 호스트 수를 1000으로 나누면 업데이트 수행에 걸리는 대략적인 시간(분)이 나옵니다.

VDB 343부터는 Cisco Secure Firewall 애플리케이션 탐지기를 통해 모든 애플리케이션 탐지기 정보를 사용할 수 있습니다. 이 사이트에는 검색 가능한 애플리케이션 탐지기 데이터베이스가 포함되어 있습니다. 릴리스 노트에서는 특정 VDB 릴리스의 변경 사항에 대한 정보를 제공합니다.

참고 management center의 초기 설정에서는 일회성 작업으로 Cisco에서 최신 VDB를 자동으로 다운로드하여 설치합니다. 또한 최신 VDB를 포함하여 사용 가능한 최신 소프트웨어 업데이트를 다운로드하는 매주 작업을 예약합니다. 이 주간 작업을 검토하고 필요한 경우 조정하는 것이 좋습니다. 선택적으로, 새로운 주간 작업을 예약하여 실제로 VDB를 업데이트하고 구성을 구축합니다. 자세한 내용은 취약성 데이터베이스 업데이트 자동화, 515 페이지를 참조하십시오.

VDB 업데이트 예약

management center이 인터넷 액세스 권한이 있는 경우 정기적인 VDB 업데이트를 예약하는 것이 좋습니다. 취약성 데이터베이스 업데이트 자동화, 515 페이지의 내용을 참조하십시오.

VDB 수동 업데이트

이 절차를 사용하여 VDB를 수동으로 업데이트합니다.VDB 357부터 management center에 대한 기준 VDB까지 모든 VDB를 설치할 수 있습니다.

주의 VDB가 업데이트되는 동안에는 매핑된 취약성과 관련된 작업을 수행하지 마십시오. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

대부분의 경우 VDB 업데이트 후 첫 번째 구축은 Snort 프로세스를 재시작하여 트래픽 검사를 중단합니다. 이러한 상황이 발생하면 시스템에서 사용자에게 경고합니다(업데이트된 애플리케이션 탐지기 및 운영 체제 핑거프린트는 재시작이 필요하지만 취약성 정보는 그렇지 않음). 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작를 참조하십시오.

시작하기 전에

management center가 인터넷에 액세스할 수 없는 경우 Cisco 지원 및 다운로드 사이트(https://www.cisco.com/go/firepower-software)에서 업데이트를 가져옵니다. 모델을 선택하거나 검색한 다음(또는 모든 management center에 대해 동일한 VDB를 사용하는 모델을 선택), *Coverage and Content Updates*(커버리지 및 콘텐츠 업데이트) 페이지로 이동합니다.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)** > **Product Updates(**제품 업데이트**)**을(를) 선택합니다.

단계 **2** VDB를 management center로 가져오는 방법을 선택합니다.

- 직접 다운로드: **Download Updates(**업데이트 다운로드**)** 버튼을 클릭하여 최신 VDB, 최신 유지보수 릴리스 및 구축을 위한 최신 중요 패치를 즉시 다운로드합니다.
- 수동 업로드: **Upload Update(**업데이트 업로드**)**를 클릭한 후, **Choose File(**파일 선택**)**을 클릭하고 VDB로 이동합니다.

단계 **3** VDB를 설치합니다.

a) 설치하려는 Vulnerability and Fingerprint Database(취약성 및 핑거프린트 데이터베이스) 업데이트 옆에 있는 **Install(**설치**)** 아이콘(새 VDB) 또는 **Rollback(**롤백**)** 아이콘(이전 VDB)을 클릭합니다.

b) management center을(를) 선택합니다.

c) **Install(**설치**)**을 클릭합니다.

메시지 센터에서 업데이트 진행 상황을 모니터링합니다. 업데이트가 완료된 후, 시스템이 새 취약성 정보를 사용합니다. 그러나 구성을 구축해야 업데이트된 애플리케이션 탐지기 및 운영 체제 지문을 적용할 수 있습니다.

단계 **4** 업데이트 성공을 확인합니다.

도움말(?) > 정보 를 선택하고 VDB 현재 버전을 확인합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.
- 더 이상 사용할 수 없는 취약성, 애플리케이션 탐지기 또는 핑거프린트를 기반으로 하는 구성인 경우 해당 구성을 검토하여 트래픽을 정상적으로 처리하고 있는지 확인합니다. 또한 VDB를 업데이트하기 위해 예약된 작업이 롤백을 취소할 수 있다는 점에 유의하십시오. 이를 방지하려면 예약된 작업을 변경하거나 최신 VDB 패키지를 삭제하십시오.

GeoDB(지리위치 데이터베이스) 업데이트

GeoDB(지리위치 데이터베이스)는 지리적 위치를 기준으로 트래픽을 보고 필터링하는 데 사용할 수 있는 데이터베이스입니다. GeoDB 업데이트는 주기적으로 제공되므로, 정확한 지리위치 정보를 얻으려면 GeoDB를 정기적으로 업데이트해야 합니다. 최신 버전은 도움말(?) > 정보 에서 확인할 수 있습니다.

시스템은 IP 주소를 국가/대륙에 매핑하는 초기 GeoDB 국가 코드 패키지와 함께 제공되므로 정보를 항상 사용할 수 있습니다. 시스템은 GeoDB 업데이트(온디맨드 또는 일정에 따름)를 다운로드할 때

상황별 데이터가 있는 IP 패키지를 포함하여 설치합니다. 여기에는 추가 위치 세부 정보는 물론 ISP, 연결 유형, 프록시 유형, 도메인 이름 등의 연결 정보가 포함됩니다. VDB를 수동으로 업데이트하는 경우두 패키지를 모두 업데이트합니다.두 패키지 모두 있어야 합니다.

참고 시스템은 초기 구성의 일부로 매주 GeoDB 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 GeoDB 업데이트 예약, 237 페이지.

GeoDB 업데이트는 GeoDB의 이전 버전을 무시하고 즉시 적용됩니다. management center는 자동으로 매니지드 디바이스를 업데이트합니다. 재구축할 필요가 없습니다.

GeoDB를 업데이트하는 데 필요한 시간은 어플라이언스에 따라 다르지만, 업데이트 크기에 따라 최대 45분이 걸릴 수 있습니다. 시스템에서 전체 IP 패키지 집합을 다운로드하여 처리하는 경우를 예로 들 수 있습니다. GeoDB 업데이트를 수행해도 지리위치 정보의 지속적인 수집을 비롯한 기타 시스템 기능이 중단되지는 않지만, 업데이트를 완료하는 동안 시스템 리소스가 사용됩니다. 업데이트를 예약하는 경우 이를 고려하십시오.

GeoDB 업데이트 예약

시스템은 초기 구성의 일부로 매주 GeoDB 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 이 절차.

시작하기 전에

management center이 인터넷에 액세스할 수 있는지 확인합니다.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**을(를) 선택합니다.

단계 **2** **Recurring Geolocation Updates(**반복되는 지리위치 업데이트**)**에서 **Enable Recurring Weekly Updates(**반복되는 주간 업데이트 활성화**)**를 체크합니다..

단계 **3** **Update Start Time(**업데이트 시작 시간**)**을 지정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

GeoDB 수동 업데이트

온디맨드 GeoDB 업데이트를 수행하려면 이 절차를 사용합니다.

시작하기 전에

management center가 인터넷에 액세스할 수 없는 경우 Cisco 지원 및 다운로드 사이트 (https://www.cisco.com/go/firepower-software)에서 업데이트를 가져옵니다. 모델을 선택하거나 검색한 다음(또는 모든 management center에 대해 동일한 GeoDB를 사용하는 모델을 선택) *Coverage and*

Content Updates(커버리지 및 콘텐츠 업데이트) 페이지로 이동합니다. 국가 코드 패키지와 IP 패키지를 다운로드합니다.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)** > **Geolocation Updates(**지리위치 업데이트**)**을(를) 선택합니다.

단계 **2** **One-Time Geolocation Update(**일회성 지리위치 업데이트**)** 아래에서 GeoDB를 업데이트할 방법을 선택합니다.

- 직접 다운로드: **Download and install...(**다운로드 및 설치**...)**를 선택합니다..
- 수동 업로드: **Upload and install...(**업로드 및 설치**...)**을 선택한 다음, **Choose File(**파일 선택**)**을 클릭하고 이전에 다운로드한 국가 코드 패키지를 찾습니다.

단계 **3** **Import(**가져오기**)**를 클릭합니다.

메시지 센터에서 업데이트 진행 상황을 모니터링합니다.

단계 **4** 업데이트 성공을 확인합니다.

Geolocation Updates(지리위치 업데이트) 페이지와 도움말(?) > 정보 페이지 모두 현재 버전을 나열합니다.

단계 **5** 수동으로 업데이트를 업로드하는 경우, IP 패키지에 대해 이 절차를 반복합니다.

침입 규칙 업데이트

새로운 취약성이 알려지면 Talos 인텔리전스 그룹은 가져올 수 있는 침입 규칙 업데이트를 management center로 릴리스하고, 그런 다음 변경된 구성을 매니지드 디바이스에 구축하여 구현합니다. 이러한 업데이트는 침입 규칙, 전처리기 규칙 및 규칙을 사용하는 정책에 영향을 줍니다.

규칙 업데이트는 누적되며, Cisco에서는 항상 최신 업데이트를 가져올 것을 권장합니다. 현재 설치된 규칙의 버전과 일치하거나 이전의 침입 규칙 업데이트는 가져올 수 없습니다.

management center의 고가용성 쌍이 배포에 포함된 경우, 기초 수준의 업데이트만 가져옵니다. 이차적 management center는 일반 동기화 프로세스의 일부로 규칙 업데이트를 수신합니다.

침입 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 프리프로세서 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.

다중 도메인 구축에서는 로컬 침입 규칙을 모든 도메인에 가져올 수 있지만 Talos의 침입 규칙 업데이트는 전역 도메인에만 가져올 수 있습니다.

침입 규칙 업데이트가 정책을 수정하는 시점에 대한 이해

침입 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 다시 구축할 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.

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 정책및 변경한 사용자을 나열합니다.

침입 규칙 업데이트 구축

침입 규칙 업데이트를 통해 수행된 변경 사항을 적용하려면 구성을 재구축해야 합니다. 규칙 업데이트를 가져올 때 영향을 받는 디바이스에 자동으로 재구축하도록 시스템을 구성할 수 있습니다. 이 접근법은 침입 규칙 업데이트가 시스템이 제공하는 기본 침입 정책을 수정할 수 있는 경우에 특히 유용합니다.

주의 규칙 업데이트 자체는 구축 시 Snort 프로세스를 재시작하지 않지만 다른 변경 사항으로 인해 재시작될 수도 있습니다. Snort를 다시 시작하면 고가용성/확장성을 위해 구성된 디바이스를 포함하여 모든 디바이스의 트래픽 흐름 및 검사가 잠시 중단됩니다. 인터페이스 구성에 따라 중단되는 동안 트래픽이 삭제되는지 아니면 검사 없이 통과되는지가 결정됩니다. Snort를 다시 시작하지 않고 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다.

반복 침입 규칙 업데이트

Rule Updates(규칙 업데이트) 페이지를 사용하여 일 단위, 주 단위 또는 월 단위로 규칙 업데이트를 가져올 수 있습니다.

management center의 고가용성 쌍이 배포에 포함된 경우, 기초 수준의 업데이트만 가져옵니다. 이차적 management center는 일반 동기화 프로세스의 일부로 규칙 업데이트를 수신합니다.

침입 규칙 업데이트 가져오기에서 적용 가능한 하위 태스크는 다운로드, 설치, 기본 정책 업데이트 및 구성 구축 순서로 수행됩니다. 1개의 하위 태스크가 완료되면, 다음 하위 태스크가 시작됩니다.

시스템은 이전 단계에서 지정한 대로 예약된 시간에 규칙 업데이트를 설치하고 변경된 구성을 구축합니다. 가져오기 작업 중 또는 작업 이전에 로그 오프하거나 웹 인터페이스를 사용하여 다른 작업을 수행할 수 있습니다. 가져오기 작업 중에 액세스된 경우, Rule Update Log(규칙 업데이트 로그)는 **Red Status(**빨간색 상태**)** ( )를 표시하며, Rule Update Log(규칙 업데이트 로그) 상세 보기에서 메시지가 나타나면 이를 확인할 수 있습니다. 규칙 업데이트 크기 및 콘텐츠에 따라, 몇 분이 지난 후에 상태 메시지가 표시될 수 있습니다.

시스템은 초기 구성의 일부로 매일 침입 규칙 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 침입 규칙 업데이트 예약, 240 페이지.

로컬 침입 규칙 가져오기

로컬 침입 규칙은 로컬 컴퓨터에 ASCII 또는 UTF-8로 인코딩한 일반 텍스트 파일로 가져오는 맞춤형 표준 텍스트 규칙입니다. Snort 사용자 설명서의 지침을 사용하여 로컬 규칙을 생성할 수 있습니다. 지침은 http://www.snort.org에서 다운로드할 수 있습니다.

다중 도메인 구축에서 로컬 침입 규칙을 모든 도메인으로 가져올 수 있습니다. 현재 도메인 및 상위 도메인에서 가져온 로컬 침입 규칙을 볼 수 있습니다.

침입 규칙 업데이트 예약

시스템은 초기 구성의 일부로 매일 침입 규칙 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 이 절차.

시작하기 전에

- 침입 규칙을 업데이트하는 프로세스가 보안 정책을 준수하는지 확인합니다.
- 대역폭 제한 및 Snort 재시작으로 인해 업데이트가 트래픽 플로우 및 검사에 미치는 영향을 고려합니다. 유지 보수 창에서 업데이트를 수행하는 것이 좋습니다.
- management center이 인터넷에 액세스할 수 있는지 확인합니다.

프로시저

단계 **1** 시스템 ( ) > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**을(를) 선택합니다.

단계 **2** **Recurring Rule Update Imports(**반복 규칙 업데이트 가져오기**)**에서 **Enable Recurring Rule Update Imports(**반복 규칙 업데이트 가져오기 활성화**)**를 선택합니다.

단계 **3** **Import Frequency(**가져오기 빈도**)** 및 시작 시간을 지정합니다.

단계 **4** (선택 사항) 각 업데이트 이후에 구축하려면 **Reapply all policies...(**모든 정책 재적용**...)**를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

침입 규칙 수동 업데이트

온디맨드 침입 규칙 업데이트를 수행하려면 이 절차를 사용합니다.

시작하기 전에

- 침입 규칙을 업데이트하는 프로세스가 보안 정책을 준수하는지 확인합니다.
- 대역폭 제한 및 Snort 재시작으로 인해 업데이트가 트래픽 플로우 및 검사에 미치는 영향을 고려합니다. 유지 보수 창에서 업데이트를 수행하는 것이 좋습니다.
- management center가 인터넷에 액세스할 수 없는 경우 Cisco 지원 및 다운로드 사이트(https://www.cisco.com/go/firepower-software)에서 업데이트를 가져옵니다. 모델을 선택하거나 검색한 다음(또는 모든 management center에 대해 동일한 SRU 또는 LSP를 사용하는 모델을 선택), *Coverage and Content Updates(*커버리지 및 콘텐츠 업데이트*)* 페이지로 이동합니다.

프로시저

단계 **1** 시스템 ( ) > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**을(를) 선택합니다.

단계 **2** **One-Time Rule Update/Rules Import(**일회성 규칙 업데이트/규칙 가져오기**)**에서 침입 규칙을 업데이트할 방법을 선택합니다.

- 직접 다운로드: **Download new rule update...(**새 규칙 업데이트 다운로드**...)**를 선택합니다..
- 수동 업로드: **Rule update or text rule file...(**규칙 업데이트 또는 텍스트 규칙 파일**...)**을 선택한 다음, **Choose File(**파일 선택**)**을 클릭하고 침입 규칙 업데이트를 찾습니다.

단계 **3** (선택 사항) 업데이트 이후에 구축하려면 **Reapply all policies...(**모든 정책 재적용**...)**를 선택합니다.

단계 **4** **Import(**가져오기**)**를 클릭합니다.

메시지 센터에서 업데이트 진행 상황을 모니터링합니다. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업그레이드에서 장애가 발생했다고 나타나더라도 업그레이드를 재시작하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

단계 **5** 업데이트 성공을 확인합니다.

도움말( ) > 정보 를 선택하고 현재 규칙 업데이트 버전을 확인합니다.

다음에 수행할 작업

업데이트의 일부로 구축하지 않은 경우에는 지금 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

로컬 침입 규칙 가져오기

이 절차를 사용하여 로컬 침입 규칙을 가져옵니다. 가져온 침입 규칙이 로컬 규칙 카테고리에 비활성화된 상태로 나타납니다. 모든 도메인에서 이 작업을 수행할 수 있습니다.

시작하기 전에

- 로컬 규칙 파일이 로컬 침입 규칙 가져오기 모범 사례, 243 페이지에 설명된 지침을 따르는지 확인합니다.
- 로컬 침입 규칙을 가져오는 프로세스가 보안 정책을 준수하는지 확인합니다.
- 대역폭 제한 및 Snort 재시작으로 인해 가져오기가 트래픽 흐름 및 검사에 미치는 영향을 고려합니다. 유지 보수 기간 중 규칙 업데이트를 예약하는 것이 좋습니다.

프로시저

단계 **1** 시스템 (⚙) > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**을(를) 선택합니다.

침입 규칙 편집기(**Objects(**개체**)** > **Intrusion Rules(**침입 규칙**)**)에서 **Import Rules(**규칙 가져오기**)**를 클릭할 수도 있습니다.

단계 **2** (선택 사항) 기존 로컬 규칙을 삭제합니다.

Delete All Local Rules(모든 로컬 규칙 삭제**)**를 클릭한 후, 생성했거나 가져온 모든 침입 규칙을 삭제된 폴더로 옮기는지 확인합니다.

단계 **3** **One-Time Rule Update/Rules Import(**일회성 규칙 업데이트/규칙 가져오기**)** 아래에서 **Rule update or text rule file to upload and install(**업로드 및 설치할 규칙 업데이트 또는 텍스트 규칙 파일**)**을 선택한 다음 **Choose File(**파일 선택**)**을 클릭하여 로컬 규칙 파일을 찾습니다.

단계 **4** **Import(**가져오기**)**를 클릭합니다.

Message Center의 가져오기 진행 상황을 모니터링할 수 있습니다. Message Center에서 몇 분간 진행 상황이 표시되지 않거나 업데이트에서 장애가 발생했다고 나타나더라도 가져오기를 재시작하지 마십시오. 그 대신 Cisco TAC에 문의하십시오.

다음에 수행할 작업

- 침입 정책을 수정하고 가져온 규칙을 활성화합니다.
- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

로컬 침입 규칙 가져오기 모범 사례

로컬 규칙 파일을 가져올 때 다음 지침을 따르십시오.

- 규칙 가져오기 도구를 사용하려면 모든 맞춤형 규칙을 ASCII 또는 UTF-8로 인코딩된 일반 텍스트로 가져와야 합니다.
- 텍스트 파일 이름은 영숫자 및 공백을 포함할 수 있지만 밑줄(_), 마침표(.) 및 대시(-)를 제외한 특수 문자는 포함할 수 없습니다.
- 시스템이 단일 파운드 문자(#)로 시작되는 로컬 규칙을 가져오지만, 삭제된 것으로 플래그 표시됩니다.
- 시스템이 단일 파운드 문자(#)로 시작하는 로컬 규칙을 가져오지만, 파운드 문자 2개(##)로 시작하는 로컬 규칙은 가져오지 않습니다.
- 규칙은 확장 문자를 사용할 수 없습니다.
- 다중 도메인 구축에서 시스템은 전역 도메인으로 가져오거나 생성된 규칙에 GID 1을 할당하고 다른 모든 도메인에서는 도메인 별 GID를 1000과 2000 사이로 할당합니다.
- 로컬 규칙을 가져올 때 GID(Generator ID)를 지정할 필요가 없습니다. 이렇게 하면 표준 텍스트 규칙에 GID 1만 지정됩니다.
- 처음으로 규칙을 가져오는 경우, Snort ID (SID) 또는 개정 번호를 지정하지 마십시오. 이렇게 하면 삭제된 규칙을 포함해 다른 규칙의 SID와 충돌을 피할 수 있습니다. 시스템은 해당 규칙에 다음으로 사용 가능한 1000000 이상의 사용자 지정 규칙 SID와 수정 번호 1을 자동으로 할당합니다.

  SID가 있는 규칙을 가져와야 하는 경우, SID는 1,000,000 이상의 고유 숫자가 될 수 있습니다.

  다중 도메인 구축에서 여러 관리자가 동시에 로컬 규칙을 가져오는 경우, 시스템이 시퀀스의 중간 숫자를 다른 도메인에 할당했기 때문에 개별 도메인 내의 SID가 비순차적으로 보일 수 있습니다.
- 이전에 가져온 로컬 규칙의 업데이트된 버전을 가져올 경우 또는 삭제한 로컬 규칙을 되돌리는 경우, 반드시 시스템이 할당한 SID와 현재 개정 번호보다 큰 개정 번호를 포함해야 합니다. 규칙을 편집하여 현재 또는 삭제된 규칙의 개정 번호를 결정할 수 있습니다.

참고 로컬 규칙을 삭제하면 자동으로 개정 번호가 증가합니다. 이 디바이스를 통해 로컬 규칙을 복원할 수 있습니다. 삭제된 모든 로컬 규칙은 로컬 규칙 카테고리에서 삭제된 규칙 카테고리로 이동합니다.

- 고가용성 쌍으로 된 기본 Firepower Management Center의 로컬 규칙을 가져오고 SID 번호 매기기 문제를 방지합니다.
- 규칙에 다음 중 하나가 포함되는 경우 가져오기가 실패합니다.
  - 2147483647 보다 큰 SID.
  - 64자를 초과하는 소스 또는 대상 포트의 목록.

- 다중 도메인 구축에서 전역 도메인으로 가져오는 경우, GID:SID 조합은 GID 1과 이미 다른 도메인에 있는 SID를 사용합니다. 이는 해당 조합이 버전 6.2.1 이전에 존재했음을 나타냅니다. GID 1과 고유한 SID를 사용하여 규칙을 다시 가져올 수 있습니다.

- 더 이상 사용되지 않는 `threshold` 키워드를 침입 정책의 침입 이벤트 임계값 설정 기능과 조합하여 사용하는, 가져온 로컬 규칙을 활성화하는 경우 정책 인증이 실패합니다.
- 가져온 모든 로컬 규칙은 로컬 규칙 카테고리에 자동으로 저장됩니다.
- 시스템은 사용자가 가져오는 로컬 규칙을 항상 비활성화된 규칙 상태로 설정합니다. 로컬 규칙을 침입 정책에서 사용하기 전에 상태를 수동으로 설정해야 합니다.

침입 규칙 업데이트 로그 보기

시스템에서 타임스탬프, 사용자, 각 업데이트의 성공 또는 실패 여부를 기준으로 나열되는 규칙 업데이트/가져오기 로그를 생성합니다. 이러한 로그에는 업데이트된 모든 규칙 및 구성 요소에 대한 자세한 가져오기 정보가 포함됩니다. 침입 규칙 업데이트 로그 세부 정보, 244 페이지의 내용을 참고하십시오.

규칙 가져오기 로그를 보려면 이 절차를 사용합니다. 가져오기 로그를 삭제해도 가져온 개체는 삭제되지 않습니다. 다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** 시스템 ( ) > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**을(를) 선택합니다.

단계 **2** **Rule Update Log(**규칙 업데이트 로그**)**를 클릭합니다.

단계 **3** (선택 사항) 로그 파일 옆에 있는 **View(**보기**)** ( )을 클릭하여 규칙 업데이트의 세부 정보를 봅니다.

침입 규칙 업데이트 로그 세부 정보

팁 단일 가져오기 파일에 대한 레코드만 표시된 Rule Update Import Log(규칙 업데이트 가져오기 로그) 상세 보기의 툴바에서 **Search(**검색**)**를 클릭하여 검색을 시작하는 경우에도 Rule Update Import Log(규칙 업데이트 가져오기 로그) 데이터베이스 전체를 검색합니다. 검색에 포함할 모든 개체를 포함하도록 시간 제약 조건을 설정해야 합니다.

표 *7:* 침입 규칙 업데이트 로그 세부 정보

필드	설명
조치	다음 중 하나가 개체 유형에 발생했음을 나타냅니다. • `new(신규)` (해당 규칙이 어플라이언스에 처음 저장된 경우) • `changed(변경됨)`(규칙 업데이트 구성 요소 또는 규칙의 경우, 규칙 업데이트 구성 요소가 변경되었거나 규칙이 더 높은 수정 번호 및 동일한 GID 및 SID를 지닙니다.) • `collision(충돌)` (규칙 업데이트 구성 요소 또는 규칙의 경우, 해당 수정 버전이 기존 구성 요소 또는 규칙과 충돌하여 가져오기를 건너뛰었습니다.) • `deleted(탐지됨)`(규칙의 경우, 규칙이 규칙 업데이트에서 삭제되었습니다.) • `enabled(활성화됨)`(규칙 업데이트 수정에서 전처리기, 규칙 또는 다른 기능이 시스템 제공 기본 정책에서 활성화되었습니다.) • `disabled(비활성화됨)` (규칙의 경우, 시스템 제공 기본 정책에서 규칙이 비활성화되었습니다.) • `drop(삭제)`(규칙의 경우, 시스템 제공 기본 정책에서 규칙이 Drop and Generate Events(삭제 후 이벤트 생성)로 설정되었습니다.) • `error(오류)`(규칙 업데이트 또는 로컬 규칙 파일의 경우, 가져오기가 실패했습니다.) • `apply(적용)`(해당 가져오기에 대해 **Reapply intrusion policies after the Rule Update import completes(**규칙 업데이트 가져오기가 완료된 후 침입 정책 다시 적용**)** 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.
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.
도메인	침입 정책이 업데이트된 규칙을 사용할 수 있는 도메인. 하위 도메인의 침입 정책도 규칙을 사용할 수 있습니다. 이 필드는 다중 도메인 구축에서만 나타납니다.
GID	규칙에 대한 생성기 ID. 예를 들어, `1` (표준 텍스트 규칙, 전역 도메인 또는 레거시 GID) 또는 `3` (공유 개체 규칙).
이름	규칙 Message(메시지) 필드에 해당하는 규칙 및 규칙 업데이트 구성 요소에 대해 가져온 개체의 이름이 구성 요소 이름입니다.
정책	가져온 규칙의 경우, 이 필드는 `All(모두)`로 표시됩니다. 이는 해당 규칙 가져오기가 성공하였고 모든 적절한 기본 침입 정책에서 활성화될 수 있다는 의미입니다. 가져온 개체의 다른 유형의 경우, 이 필드는 비어 있습니다.
Rev	규칙의 수정 번호.
규칙 업데이트	규칙 업데이트 파일 이름.

필드	설명
SID	규칙의 SID.
시간	가져오기가 시작된 날짜 및 시간입니다.
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.) • `policy apply(정책 적용)`(해당 가져오기에 대해 **Reapply intrusion policies after the Rule Update import completes(**규칙 업데이트 가져오기가 완료된 후 침입 정책 다시 적용**)** 옵션이 활성화되었습니다.)
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. 이 필드는 검색할 수 없습니다.

에어-갭(Air-Gapped) 구축 유지 관리

management center이 인터넷에 연결되어 있지 않으면, 필수 업데이트가 자동으로 발생하지 않습니다. 이러한 업데이트를 수동으로 가져오고 설치해야 합니다.

자세한 내용은 다음 링크를 참조하십시오.

- 소프트웨어 업그레이드 가이드: https://cisco.com/go/ftd-fmc-upgrade
- VDB 수동 업데이트, 235 페이지
- 침입 규칙 수동 업데이트, 241 페이지
- GeoDB 수동 업데이트, 237 페이지

시스템 업데이트 히스토리

표 ***8:***

기능	버전	세부정보
사용 편의성 개선.	7.3	위협 방어 업그레이드 마법사의 몇 가지 사용 편의성이 개선되었습니다. • 이제 마법사를 사용하여 업그레이드할 디바이스를 선택할 수 있습니다. 선택한 디바이스, 남은 업그레이드 후보, 부적격 디바이스(이유 포함), 업그레이드 패키지가 필요한 디바이스 간 보기를 전환할 수 있습니다. 이전에는 디바이스 관리 페이지만 사용할 수 있었으며 프로세스의 유연성이 훨씬 낮았습니다. • 이제 마법사를 사용하여 위협 방어 업그레이드 패키지를 업로드하거나 업그레이드 패키지 위치를 지정할 수 있습니다. 이전에는 System Updates(시스템 업데이트) 페이지만 사용할 수 있었습니다. • 이제 서로 다른 디바이스를 업그레이드하는 경우에 한해 서로 다른 사용자의 동시 업그레이드 워크플로우를 허용합니다. 시스템은 이미 다른 사람의 워크플로우에 있는 디바이스를 업그레이드하는 것을 방지합니다. 이전에는 모든 사용자에게 한 번에 하나의 업그레이드 워크플로우만 허용되었습니다. 모든 위협 방어 업그레이드에 대해 더 작은 업그레이드 패키지와 더 빠른 업그레이드 및 준비 상태 확인을 제공합니다.
무인 위협 방어 업그레이드.	7.3	위협 방어 업그레이드 마법사는 이제 새로운 무인 모드 메뉴를 사용하여 무인 업그레이드를 지원합니다. 업그레이드할 대상 버전 및 디바이스를 선택하고 몇 가지 업그레이드 옵션을 지정한 다음 단계를 수행하면 됩니다. 로그아웃하거나 브라우저를 닫을 수도 있습니다. 무인 업그레이드에서는 시스템에서 자동으로 필요한 업그레이드 패키지를 디바이스에 복사하고 호환성 및 준비도 확인을 수행한 다음 업그레이드를 시작합니다. 마법사를 수동으로 진행할 때와 마찬가지로 업그레이드 단계를 "통과"하지 않는 디바이스(예: 검사 실패)는 다음 단계에 포함되지 않습니다. 업그레이드가 완료되면 확인 및 업그레이드 후 작업을 시작합니다. 복사 및 확인 단계 중에 무인 모드를 일시 중지하고 다시 시작할 수 있습니다. 그러나 무인 모드를 일시 중지해도 진행 중인 작업은 중지되지 않습니다. 시작된 복사 및 확인은 완료될 때까지 실행됩니다. 마찬가지로, 무인 모드를 중지하여 진행 중인 업그레이드를 취소할 수 없습니다. 업그레이드를 취소하려면 Device Management(디바이스 관리) 페이지의 Upgrade(업그레이드) 탭 및 메시지 센터에서 액세스할 수 있는 Upgrade Status(업그레이드 상태) 팝업을 사용합니다.

기능	버전	세부정보
위협 방어 사전 업그레이드 문제 해결 생성을 건너뜁니다.	7.3	이제 위협 방어 업그레이드 마법사에서 새로운 **Generate Troubleshooting files before upgrade starts(**업그레이드 시작 전에 문제 해결 파일 생성**)** 옵션을 비활성화하여 주요 및 유지 보수 업그레이드 전에 문제 해결 파일을 자동으로 생성하는 작업을 건너뛸 수 있습니다. 이렇게 하면 시간과 디스크 공간이 절약됩니다. 위협 방어 디바이스에 대한 문제 해결 파일을 수동으로 생성하려면 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**을 선택하고 왼쪽 패널에서 디바이스를 클릭한 다음 **View System & Troubleshoot Details(**시스템 및 문제 해결 세부 정보 보기**), Generate Troubleshooting Files(**문제 해결 파일 생성**)**를 선택합니다.

기능	버전	세부정보
Secure Firewall 3100용 통합 업그레이드 및 설치 패키지	7.3	버전 7.3에서는 다음과 같이 Secure Firewall 3100에 대한 위협 방어 설치 및 업그레이드 패키지를 통합했습니다. • 버전 7.1–7.2 설치 패키지: cisco-ftd-fp3k.*version*.SPA • 버전 7.1–7.2 업그레이드 패키지: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • 버전 7.3 이상 통합 패키지: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar 문제 없이 위협 방어를 업그레이드할 수 있지만, 이전 위협 방어 및 ASA 버전에서 직접 위협 방어 버전 7.3 이상으로 이미지 재설치할 수는 없습니다. 이는 새 이미지 유형에 필요한 ROMMON 업데이트 때문입니다. 이러한 이전 버전에서 이미지를 재설치하려면 이전 ROMMON에서 지원되지만 새 ROMMON으로 업데이트되는 ASA 9.19 이상을 "처리"해야 합니다. 별도의 ROMMON 업데이터는 없습니다. 위협 방어 버전 7.3 이상을 사용하기 위한 옵션은 다음과 같습니다. • Threat Defense 버전 7.1 또는 7.2에서 업그레이드 - 일반 업그레이드 프로세스를 사용합니다. 해당 업그레이드 가이드를 참조하십시오. • Threat Defense 버전 7.1 또는 7.2에서 이미지 재설치 - 먼저 ASA 9.19 이상으로 이미지 재설치한 다음 Threat Defense 버전 7.3 이상으로 이미지 재설치. Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드에서 *Threat Defense(*위협 방어*)→ASA: Firepower 1000, 2100; Secure Firewall 3100* 및 *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode(Firepower 1000, 2100* 어플라이언스 모드*) Secure Firewall 3100*을 참조하십시오. • ASA 9.17 또는 9.18에서 이미지 재설치 - ASA 9.19 이상으로 먼저 업그레이드한 다음 Threat Defense 버전 7.3 이상으로 이미지 재설치. Cisco Secure Firewall ASA 업그레이드 가이드를 참조한 다음 Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드에서 *ASA→*위협 방어*: Firepower 1000, 2100* 어플라이언스 모드*, Secure Firewall 3100*을 참조하십시오. • 위협 방어 버전 7.3 이상에서 이미지 재설치 - 일반 이미지 재설치 프로세스를 사용합니다. Firepower Threat Defense를 사용하는 Firepower 1000/2100 및 Secure Firewall 3100용 Cisco FXOS 문제 해결 가이드에서 새 소프트웨어 버전으로 시스템 이미지 재설치를 참조하십시오.

기능	버전	세부정보
위협 방어 업그레이드에 성공한 후 Snort 3으로의 자동 업그레이드는 더 이상 선택 사항이 아닙니다.	7.3	위협 방어에서 버전 7.3 이상으로 업그레이드하는 경우 더 이상 **Snort 2**를 **Snort 3**으로 업그레이드 옵션을 비활성화할 수 없습니다. 소프트웨어 업그레이드 후에는 설정을 구축할 때 모든 적격 디바이스가 Snort 2에서 Snort 3으로 업그레이드됩니다. 개별 디바이스를 다시 전환할 수는 있지만 Snort 2는 향후 릴리스에서 더 이상 사용되지 않으므로 지금 사용을 중지하는 것이 좋습니다. 맞춤형 침입 또는 네트워크 분석 정책 사용으로 인한 자동 업그레이드 부적격 디바이스의 경우, 향상된 탐지 및 성능을 위해 Snort 3으로 수동 업그레이드하는 것이 좋습니다. 마이그레이션 지원은 버전에 맞는 Cisco Secure Firewall Management Center Snort 3 구성 가이드의 내용을 참조하십시오. 최소 위협 방어: 모두
Cisco에서 선택한 업그레이드 패키지를 선택하고 직접 다운로드합니다.	7.3	이제 관리 센터로 직접 다운로드할 위협 방어 업그레이드 패키지를 선택할 수 있습니다. > **Updates(**업데이트**)** > **Product Updates(**제품 업데이트**)**에서 새 **Download Updates(**업데이트 다운로드**)**를 사용합니다.
자동 VDB 다운로드.	7.3	관리 센터의 초기 설정에서는 사용 가능한 최신 소프트웨어 업데이트를 다운로드하는 주간 작업을 예약합니다. 여기에는 최신 VDB(취약성 데이터베이스)가 포함되어 있습니다. 이 주간 작업을 검토하고 필요한 경우 조정하는 것이 좋습니다. 선택적으로, 새로운 주간 작업을 예약하여 실제로 VDB를 업데이트하고 구성을 구축합니다. 신규/수정된 화면: 이제 시스템에서 생성한 **Weekly Software Download(**주간 소프트웨어 다운로드**)** 예약 작업에서 **Vulnerability Database(**취약성 데이터베이스**)** 확인란이 기본적으로 활성화됩니다.
VDB를 설치합니다.	7.3	이제 VDB 357부터 해당 관리 센터에 대한 베이스라인 VDB까지 모든 VDB를 설치할 수 있습니다. VDB를 업데이트한 후 구성 변경 사항을 구축합니다. 더 이상 사용할 수 없는 취약성, 애플리케이션 탐지기 또는 핑거프린트를 기반으로 하는 구성인 경우 해당 구성을 검토하여 트래픽을 정상적으로 처리하고 있는지 확인합니다. 또한 VDB를 업데이트하기 위해 예약된 작업이 롤백을 취소할 수 있다는 점에 유의하십시오. 이를 방지하려면 예약된 작업을 변경하거나 최신 VDB 패키지를 삭제하십시오. 신규/수정된 화면: 에서시스템 (⚙) > **Updates(**업데이트**)** > **Product Updates(**제품 업데이트**)** > **Available Updates(**사용 가능한 업데이트**)**에서 이전 VDB를 업로드하면 **Install(**설치**)** 아이콘 대신 새 **Rollback(**롤백**)** 아이콘이 나타납니다.

기능	버전	세부정보
디바이스 간에 업그레이드 패키지("peer-to-peer sync")를 복사합니다.	7.2	management center 또는 내부 웹 서버에서 각 디바이스로 업그레이드 패키지를 복사하는 대신 threat defense CLI를 사용하여 디바이스 간에 업그레이드 패키지를 복사할 수 있습니다("피어 간 동기화"). 이 안전하고 신뢰할 수 있는 리소스 공유는 관리 네트워크를 통해 이루어지지만 management center에 의존하지 않습니다. 각 디바이스는 5개의 패키지 동시 전송을 수용할 수 있습니다. 이 기능은 동일한 독립형에서 관리하는 버전 7.2 이상의 독립형 디바이스에서 지원됩니다management center. 다음에 대해서는 지원되지 않습니다. • 컨테이너 인스턴스. • 디바이스 고가용성 쌍 및 클러스터. 이러한 디바이스는 일반 동기화 프로세스의 일부로 서로 패키지를 가져옵니다. 업그레이드 패키지를 한 그룹 멤버에 복사하면 모든 그룹 멤버에 자동으로 동기화됩니다. • 고가용성 management center에서 관리하는 디바이스. • 클라우드 제공 관리 센터에서 관리하지만 분석 모드에서 고객이 구축한 management center에 추가된 디바이스입니다. • 서로 다른 도메인에 있는 디바이스 또는 NAT 게이트웨이로 분리된 디바이스 • management center 버전에 관계없이 버전 7.1 이하에서 업그레이드하는 디바이스 신규/수정된 CLI 명령: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status** 최소 위협 방어: 7.2
위협 방어 업그레이드가 완료되면 Snort 3으로 자동 업그레이드됩니다.	7.2	버전 7.2 이상 관리 센터를 사용하여 위협 방어를 업그레이드하는 경우 이제 **Snort 2**를 **Snort 3**으로 업그레이드할지 여부를 선택할 수 있습니다. 소프트웨어 업그레이드 후에는 설정을 구축할 때 적격 디바이스가 Snort 2에서 Snort 3으로 업그레이드됩니다. 맞춤형 침입 또는 네트워크 분석 정책 사용으로 인한 부적격 디바이스의 경우, 향상된 탐지 및 성능을 위해 Snort 3으로 수동 업그레이드하는 것이 좋습니다. 마이그레이션 지원은 버전에 맞는 Cisco Secure Firewall Management Center Snort 3 구성 가이드의 내용을 참조하십시오. 이 옵션은 버전 7.2 이상에 대한 주요 및 유지 관리 Threat Defense 업그레이드에 지원됩니다. 버전 7.0 또는 7.1로의 위협 방어 업그레이드 또는 모든 버전의 패치에는 지원되지 않습니다.

기능	버전	세부정보
단일 노드 클러스터를 업그레이드합니다.	7.2	이제 디바이스 업그레이드 페이지(디바이스 > 디바이스 업그레이드)를 사용하여 활성 노드가 하나뿐인 클러스터를 업그레이드할 수 있습니다. 비활성화된 노드도 업그레이드됩니다. 이전에는 이러한 유형의 업그레이드가 실패했습니다. 이 기능은 시스템 업데이트 페이지(시스템 (⚙)**Updates(**업데이트**)**)에서 지원되지 않습니다. 이 경우 무중단 업그레이드도 지원되지 않습니다. 트래픽 흐름 및 검사 중단은 독립형 디바이스와 마찬가지로 단독 액티브 유닛의 인터페이스 구성에 따라 달라집니다. 지원되는 플랫폼: Firepower 4100/9300, Secure Firewall 3100
CLI에서 위협 방어 업그레이드를 되돌립니다.	7.2	이제 관리 센터와 디바이스 간의 통신이 중단되는 경우 디바이스 CLI에서 위협 방어 업그레이드를 되돌릴 수 있습니다. 고가용성/확장성 구축에서는 모든 유닛이 동시에 복귀될 때 복귀가 더 성공적입니다. CLI를 사용하여 되돌릴 때는 모든 유닛에서 세션을 열고 각 유닛에서 되돌리기가 가능한지 확인한 다음 프로세스를 동시에 시작합니다. 주의 CLI에서 되돌리면 업그레이드 후 변경한 내용에 따라 디바이스와 관리 센터 간의 구성이 동기화되지 않을 수 있습니다. 이로 인해 추가 통신 및 구축 문제가 발생할 수 있습니다. 신규/수정된 CLI 명령: **upgrade revert**, **show upgrade revert-info**.
GeoDB는 두 개의 패키지로 나뉩니다.	7.2	버전 7.2 릴리스 직전인 2022년 5월에 GeoDB를 두 개의 패키지로 분할했습니다. IP 주소를 국가/대륙에 매핑하는 국가 코드 패키지와 라우팅 가능한 IP 주소와 관련된 추가 상황 데이터를 포함하는 IP 패키지입니다. IP 패키지의 상황 데이터에는 추가 위치 세부 정보는 물론 ISP, 연결 유형, 프록시 유형, 도메인 이름 등의 연결 정보가 포함될 수 있습니다. 버전 7.2 이상 관리 센터에서 인터넷에 액세스할 수 있고 반복 업데이트를 활성화하거나 Cisco 지원 및 다운로드 사이트에서 일회성 업데이트를 수동으로 시작하는 경우, 시스템은 자동으로 두 패키지를 모두 얻어 가져옵니다. 그러나 업데이트를 수동으로 다운로드하는 경우(예: 에어 갭(air-gapped) 구축의 경우) 두 GeoDB 패키지를 모두 가져와야 합니다. • 국가 코드 패키지: Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP 패키지: Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar Geolocation Updates(시스템 (⚙)**> Updates(**업데이트**) > Geolocation Updates(**지리위치 업데이트**)**) 페이지 및 About(정보) 페이지(**Help(**도움말**) > About(**정보**)**)에는 시스템에서 현재 사용 중인 패키지의 버전이 나열됩니다.

기능	버전	세부정보
Management Center 업그레이드가 더 이상 문제 해결 파일을 자동으로 생성하지 않습니다.	7.2	시간과 디스크 공간을 절약하기 위해 업그레이드가 시작되기 전에 관리 센터 업그레이드 프로세스에서 더 이상 문제 해결 파일을 자동으로 생성하지 않습니다. 디바이스 업그레이드는 영향을 받지 않으며 계속해서 문제 해결 파일을 생성합니다. 관리 센터에 대한 문제 해결 파일을 수동으로 생성하려면 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**를 선택하고 왼쪽 패널에서 **Firewall Management Center**를 클릭한 다음 **View System & Troubleshoot Details(**시스템 및 문제 해결 세부 정보 보기**)**, **Generate Troubleshooting Files(**문제 해결 파일 생성**)**를 클릭합니다.
성공한 디바이스 업그레이드 되돌리기	7.1	이제 FMC 웹 인터페이스에서 주요 및 유지 보수 업그레이드를 FTD로 되돌릴 수 있습니다. 되돌리면 소프트웨어가 마지막 업그레이드 직전의 상태로 돌아갑니다(스냅샷이라고도 함). 패치를 적용한 후 되돌리면 패치도 제거됩니다. 되돌릴 필요가 있다고 생각되면 .시스템 (⚙) > **Updates(**업데이트**)**를 사용하여 FTD를 업그레이드해야 합니다. System Updates(시스템 업데이트) 페이지에서는 업그레이드를 시작할 때 되돌리기 스냅샷을 저장하도록 시스템을 구성하는 **Enable revert after successful upgrade(**업그레이드 후 되돌리기 활성화**)** 옵션을 활성화할 수 있는 유일한 곳입니다. 이는 **Devices(**디바이스**)** > **Device Upgrade(**디바이스 업그레이드**)** 페이지에서 마법사를 사용하는 일반적인 권장 사항과 다릅니다. 이는 컨테이너 인스턴스에는 지원되지 않습니다.
클러스터링된 디바이스 및 고가용성 디바이스에 대한 업그레이드 워크플로우가 개선되었습니다.	7.1	이제 FTD 업그레이드 마법사에서 클러스터링된 고가용성 유닛을 개별 디바이스가 아닌 그룹으로 올바르게 표시합니다. 시스템은 사용자에게 발생할 수 있는 그룹 관련 문제를 식별하고, 보고하고, 사전에 수정을 요구할 수 있습니다. 예를 들어 섀시 관리자에서 동기화되지 않은 변경 사항을 적용한 경우 Firepower 4100/9300에서 클러스터를 업그레이드할 수 없습니다. 클러스터에서 데이터 유닛의 업그레이드 순서를 지정할 수도 있습니다.
FTD 업그레이드 성능 및 상태 보고 기능이 개선되었습니다.	7.0	이제 FTD 업그레이드가 더 쉽고 빠르고 안정적이며 디스크 공간을 덜 차지합니다. 메시지 센터의 새로운 **Upgrades(**업그레이드**)** 탭은 업그레이드 상태 및 오류 보고에 대한 추가 개선 사항을 제공합니다.

기능	버전	세부정보
따르기 쉬운 FTD 업그레이드 마법사.	7.0	새 디바이스 업그레이드 페이지(**Devices(**디바이스**)** > **Device Upgrade(**디바이스 업그레이드**)**)에서는 버전 6.4 이상 FTD를 업그레이드하기 위한 따라하기 쉬운 마법사를 제공합니다. 시스템은 다음과 같은 중요한 업그레이드 전 단계를 안내합니다. • 업그레이드할 디바이스 선택. • 업그레이드 패키지를 디바이스에 복사. • 호환성 및 준비도 확인. 시작하려면 Device Management(디바이스 관리) 페이지(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Select Action(**작업 선택**)**)에서 새로운 **Upgrade Firepower Software(Firepower** 소프트웨어 업그레이드**)** 작업을 사용합니다. 참고 FTD 업그레이드 패키지의 위치를 업로드하거나 지정하려면 여전히 시스템 (⚙) > **Updates(**업데이트**)**를 사용해야 합니다. FMC 자체는 물론 모든 비 FTD 매니지드 디바이스를 업그레이드하려면 System Updates(시스템 업데이트) 페이지를 사용해야 합니다. 계속 진행하면 선택한 디바이스에 대한 기본 정보와 현재 업그레이드 관련 상태가 표시됩니다. 여기에는 업그레이드할 수 없는 모든 이유가 포함됩니다. 디바이스가 단계를 "통과"하지 않으면 다음 단계에 표시되지 않습니다. 마법사에서 빠져나가도 진행 상황은 유지되지만 관리자 액세스 권한이 있는 다른 사용자는 워크플로우를 재설정, 수정 또는 계속할 수 있습니다. 참고 버전 7.0에서는 Device Upgrade(디바이스 업그레이드) 페이지가 클러스터 또는 고가용성 쌍의 디바이스를 올바르게 표시하지 않습니다. 이러한 디바이스를 하나의 유닛으로 선택하고 업그레이드해야 하지만 시스템에서는 이러한 디바이스를 독립형 디바이스로 표시합니다. 디바이스 상태 및 업그레이드 준비 상태는 개별적으로 평가 및 보고됩니다. 즉, 한 유닛은 다음 단계로 "전달"되는 것으로 표시되지만 다른 유닛은 그렇지 않을 수 있습니다. 그러나 이러한 디바이스는 여전히 그룹화됩니다. 하나에서 준비 확인을 실행하면 모두에서 실행됩니다. 하나에서 업그레이드를 시작하면 모두에서 시작됩니다. 시간이 오래 걸리는 업그레이드 실패를 방지하려면 **Next(**다음**)**를 클릭하기 전에 모든 그룹 멤버가 다음 단계로 이동할 준비가 되었는지 수동으로 확인합니다.

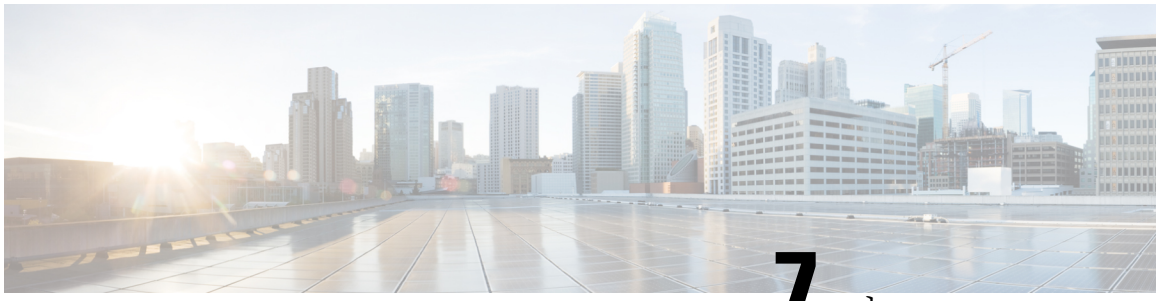
기능	버전	세부정보
한 번에 더 많은 FTD 디바이스를 업그레이드합니다.	7.0	FTD 업그레이드 마법사는 다음 제한을 해제합니다. • 동시 디바이스 업그레이드. 한 번에 업그레이드할 수 있는 디바이스의 수가 이제 동시 업그레이드를 관리하는 시스템의 기능이 아니라 관리 네트워크 대역폭에 의해 제한됩니다. 이전에는 한 번에 5개 이상의 디바이스를 업그레이드하지 않는 것을 권장했습니다. 중요 *FTD* 버전 *6.7* 이상으로 업그레이드하는 경우에만 이 개선 사항이 표시됩니다. 디바이스를 이전 FTD 릴리스로 업그레이드하는 경우(새 업그레이드 마법사를 사용하는 경우에도) 한 번에 5개의 디바이스로 제한하는 것이 좋습니다. • 디바이스 모델별 업그레이드 그룹화 이제 시스템이 적절한 업그레이드 패키지에 액세스할 수 있는 한 모든 FTD 모델을 동시에 대기열에 넣고 업그레이드를 호출할 수 있습니다. 이전에는 업그레이드 패키지를 선택한 다음 해당 패키지를 사용하여 업그레이드할 디바이스를 선택했습니다. 즉, 업그레이드 패키지를 공유하는 경우에만 여러 디바이스를 동시에 업그레이드할 수 있었습니다. 예를 들어 Firepower 2100 Series 디바이스 2개를 동시에 업그레이드할 수 있지만 Firepower 2100 Series와 Firepower 1000 Series는 업그레이드할 수 없었습니다.

기능	버전	세부정보
FTD 업그레이드 상태 보고 및 취소/재시도 옵션이 개선되었습니다.	6.7	이제 Device Management(디바이스 관리) 페이지에서 진행 중인 FTD 디바이스 업그레이드 및 준비도 확인 상태와 7일간의 업그레이드 성공/실패 기록을 볼 수 있습니다. 메시지 센터는 향상된 상태 및 오류 메시지도 제공합니다. 클릭 한 번으로 디바이스 관리 및 메시지 센터에서 액세스할 수 있는 새로운 Upgrade Status(업그레이드 상태) 팝업에 남은 비율/시간, 특정 업그레이드 단계, 성공/실패 데이터, 업그레이드 로그 등의 자세한 업그레이드 정보가 표시됩니다. 또한 이 팝업에서 실패 또는 진행 중인 업그레이드를 수동으로 취소하거나(**Cancel Upgrade(**업그레이드 취소**)**) 실패한 업그레이드를 재시도 할 수 있습니다(**Retry Upgrade(**업그레이드 재시도**)**). 업그레이드를 취소하면 디바이스가 업그레이드 전 상태로 돌아갑니다. 참고 수동으로 취소하거나 실패한 업그레이드를 재시도하려면 FMC를 사용하여 FTD 디바이스를 업그레이드할 때 나타나는 새로운 자동 취소 옵션을 비활성화해야 합니다. **Automatically cancel on upgrade failure and roll back to the previous version(**업그레이드 실패 시 자동으로 취소하고 이전 버전으로 롤백합니다**)**. 이 옵션을 활성화하면 업그레이드 실패시 디바이스가 자동으로 업그레이드 전 상태로 돌아갑니다. 패치에 대해서는 자동 취소가 지원되지 않습니다. HA 또는 클러스터형 구축에서는 자동 취소가 각 디바이스에 개별적으로 적용됩니다. 즉, 한 디바이스에서 업그레이드에 실패하면 해당 디바이스만 복귀됩니다. 신규/수정된 화면: • FTD 업그레이드 패키지의 시스템 (⚙) > **Updates(**업데이트**)** > **Product Updates(**제품 업데이트**)** > **Available Updates(**사용 가능한 업데이트**)** > **Install(**설치**)** 아이콘 • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Upgrade(**업그레이드**)** • **Message Center(**메시지 센터**) > Tasks(**작업**)** 신규/수정된 CLI 명령: **show upgrade status detail**, **show upgrade status continuous**, **show upgrade status**, **upgrade cancel**, **upgrade retry**
업그레이드는 디스크 공간을 절약하기 위해 PCAP 파일 제거.	6.7	업그레이드시 이제 로컬에 저장된 PCAP 파일이 제거됩니다. 사용 가능한 디스크 공간이 충분해야 합니다. 그렇지 않으면 업그레이드에 실패합니다.

기능	버전	세부정보
사용자 정의 침입 규칙 가져오기에서 규칙 충돌 경고	6.7	FMC에서는 이제 사용자 지정(로컬) 침입 규칙을 가져올 때 규칙 충돌을 경고합니다. 이전에는 충돌이 발생한 규칙 가져오기가 완전히 실패하는 버전 6.6.0.1을 제외하고 시스템은 충돌을 일으키는 규칙을 자동으로 건너 뛰었습니다. Rule Updates(규칙 업데이트) 페이지에서 규칙 가져오기에 충돌이 발생한 경우 Status(상태) 열에 경고 아이콘이 표시됩니다. 자세한 내용을 보려면 경고 아이콘 위에 포인터를 올려 놓고 툴팁을 확인하십시오. 기존 규칙과 동일한 SID/수정 번호를 가진 침입 규칙을 가져오려고 할 때 충돌이 발생합니다. 항상 업데이트된 버전의 사용자 정의 규칙에 새 수정 번호가 포함되어 있는지 확인해야 합니다. 자세한 모범 사례는 로컬 침입 규칙 가져오기 모범 사례, 243 페이지의 내용을 참조하십시오. 신규/수정된 화면: 시스템 (⚙) > **Updates(**업데이트**)** > **Rule Updates(**규칙 업데이트**)**에 경고 아이콘이 추가되었습니다
내부 웹 서버에서 FTD 업그레이드 패키지를 가져옵니다.	6.6	이제 FTD 디바이스가 FMC가 아닌 자체 내부 웹 서버에서 업그레이드 패키지를 가져올 수 있습니다. 이는 FMC와 해당 디바이스 간의 대역폭이 제한된 경우 특히 유용합니다. 또한 FMC의 공간을 절약합니다. 참고 이 기능은 버전 6.6 이상을 실행하는 FTD 디바이스에서만 지원됩니다. 버전 6.6으로의 업그레이드에는 지원되지 않으며, FMC 또는 클래식 디바이스에서는 지원되지 않습니다. 신규/수정된 화면: 업그레이드 패키지를 업로드하는 페이지에 **Specify software update source(**소프트웨어 업데이트 소스 지정**)** 옵션이 추가되었습니다.
초기 설정 중 자동 VDB 업데이트	6.6	새 이미지 또는 재이미징된 FMC를 설정하면 시스템이 자동으로 VDB(취약점 데이터베이스) 업데이트를 시도합니다. 이 작업은 한 번만 수행하면 됩니다. FMC에서 인터넷에 액세스할 수 있는 경우 자동 반복 VDB 업데이트 다운로드 및 설치를 수행하도록 작업을 예약하는 것이 좋습니다.
자동 소프트웨어 다운로드 및 GeoDB 업데이트.	6.5	새 이미지 또는 재이미징된 FMC를 설정하면 시스템에서 다음 일정을 자동으로 예약합니다. • FMC 및 매니지드 디바이스의 소프트웨어 업데이트를 다운로드하는 주간 작업. • GeoDB 주간 업데이트 이런 작업은 UTC 기준으로 예약되므로, 사용자가 있는 위치와 날짜에 따라 지역적으로 실행됩니다. 또한 작업은 UTC 기준으로 예약되기 때문에 일광 절약 시간, 서머 타임 또는 사용자 위치에서 발생할 수 있는 계절 조정의 영향을 받지 않습니다. 영향을 받을 경우 예약된 작업은 현지 시간에 따라 여름에는 겨울보다 1시간 '늦게' 실행됩니다. 자동 예약 구성을 검토하고 필요한 경우 조정할 것을 강력하게 권장합니다.

기능	버전	세부정보
FMC 업그레이드 중에 예약된 작업이 연기됩니다.	6.7 6.6.3 6.4.0.10	이제 FMC 업그레이드 중에 예약된 작업이 연기됩니다. 업그레이드 중에 시작하도록 예약된 모든 작업은 업그레이드 후 재부팅하고 5분 후에 시작됩니다. 참고 업그레이드를 시작하기 전에 실행 중인 작업이 완료되었는지 확인해야 합니다. 업그레이드를 시작할 때 실행 중인 작업은 중지되어 실패한 작업이 되며 다시 시작할 수 없습니다. 이 기능은 지원되는 버전에서 모든 업그레이드를 지원합니다. 여기에는 버전 6.4.0.10 이상 패치, 버전 6.6.3 이상 유지 보수 릴리스, 버전 6.7 이상이 포함됩니다. 이 기능은 지원되지 않는 버전에서 지원되는 버전으로 업그레이드 할 때는 지원되지 않습니다.
서명된 SRU, VDB 및 GeoDB 업데이트	6.4	따라서 시스템에서는 올바른 업데이트 파일을 사용하고 있는지 확인할 수 있습니다. 이제 시스템은 SRU(침입 규칙), VDB(취약점 데이터베이스) 및 GeoDB(지리위치 데이터베이스)에 서명된 업데이트를 사용합니다. 이전 버전은 서명되지 않은 패키지를 계속 사용합니다. Cisco 지원 및 다운로드 사이트에서 업데이트를 수동으로 다운로드하지 않는 한(예: 무선 연결 구축) 기능에 차이가 있어서는 안 됩니다. 그러나 SRU, VDB 및 GeoDB 업데이트를 수동으로 다운로드하여 설치하는 경우 현재 버전에 맞는 패키지를 다운로드해야 합니다. 서명된 업데이트 파일은 'Sourcefire'대신 'Cisco'로 시작하고 .sh 대신 .sh.REL.tar로 끝납니다. • SRU: Cisco_Firepower_SRU-날짜-빌드-vrt.sh.REL.tar • VDB: Cisco_VDB_Fingerprint_Database-4.5.0-버전.sh.REL.tar • GeoDB: Cisco_GEODB_Update-날짜-빌드.sh.REL.tar 서명된(.tar) 패키지의 압축을 풀지 마십시오.
더 빠른 업그레이드	6.4	이벤트 데이터베이스가 개선되어 더 빠른 업그레이드가 가능합니다.
업그레이드 전에 관리되는 디바이스에 업그레이드 패키지 복사	6.2.3	이제 실제 업그레이드를 실행하기 전에 FMC에서 업그레이드 패키지를 매니지드 디바이스로 복사 또는 푸시할 수 있습니다. 이는 업그레이드 유지 보수 기간이 아닌 낮은 대역폭 사용 시간 동안 푸시할 수 있으므로 유용합니다. 고가용성, 클러스터형 또는 스택형 디바이스로 푸시할 경우, 시스템은 먼저 업그레이드 패키지를 액티브/컨트롤/기본에 전송한 다음 스탠바이/데이터/보조에 전송합니다. 신규/수정된 화면: 시스템 (⚙) > **Updates(**업데이트**)**

기능	버전	세부정보
FMC에서 VDB 업데이트 전에 Snort 재시작을 경고합니다.	6.2.3	이제 FMC에서 VDB(Vulnerability Database) 업데이트 시 Snort 프로세스가 재시작된다는 경고가 표시됩니다. 이렇게 하면 트래픽 검사가 중단되며, 매니지드 디바이스가 트래픽을 처리하는 방식에 따라 트래픽 흐름이 중단될 수 있습니다. 유지 보수 기간과 같이 편리한 시간까지 설치를 취소할 수 있습니다. 다음과 같은 경고가 표시될 수 있습니다. • VDB를 다운로드하고 수동으로 설치한 후 • VDB를 설치하기 위해 예약된 작업을 생성할 때 • 이전에 예약 된 작업이나 소프트웨어 업그레이드의 일부로 VDB가 백그라운드에서 설치되는 경우



7 장

라이선스

이 장에서는 다양한 라이선스 유형, 서비스 구독, 라이선스 요구 사항 등에 대한 자세한 정보를 제공합니다.

참고 Management Center는 플랫폼 라이선스에 대해 스마트 라이선스 또는 레거시 PAK(제품 활성화 키) 라이선스를 지원합니다. PAK 라이센싱에 대한 자세한 내용은 레거시 Management Center PAK 기반 라이선스 구성, 308 페이지의 내용을 참조하십시오.

라이선스 정보

시스코 스마트 라이선싱은 시스코 포트폴리오 및 조직 전체에서 소프트웨어를 보다 쉽고 빠르고 일관적인 방식으로 구매하고 관리할 수 있는 유연한 라이선싱 모델입니다. 또한 사용자가 액세스할 수 있는 항목을 제어할 수 있어 안전합니다. 스마트 라이선싱을 사용하면 다음과 같은 이점을 누릴 수 있습니다.

- 손쉬운 활성화: 스마트 라이선싱은 전체 조직에서 사용할 수 있는 소프트웨어 라이선스 풀을 설정하므로 더 이상 PAK(제품 활성화 키)가 필요하지 않습니다.
- 통합 관리: MCE(My Cisco Entitlements)는 사용하기 쉬운 포털에서 모든 시스코 제품 및 서비스에 대한 완벽한 보기를 제공하므로 무엇을 보유하고 있으며 무엇을 사용 중인지 항상 파악할 수 있습니다.

- 라이선스 유연성: 소프트웨어가 하드웨어에 노드로 고정되어 있지 않으므로 필요에 따라 라이선스를 쉽게 사용하고 전송할 수 있습니다.

스마트 라이선싱을 사용하려면 먼저 Cisco Software Central(software.cisco.com)에서 스마트 어카운트를 설정해야 합니다.

시스코 라이선싱에 대한 자세한 내용은 cisco.com/go/licensingguide를 참조하세요.

Smart Software Manager 및 어카운트

라이선스를 1개 이상 구매한 경우, Smart Software Manager에서 라이선스를 관리할 수 있습니다.https://software.cisco.com/#module/SmartLicensing Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다. 아직 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

기본적으로는 마스터 어카운트의 기본 가상 어카운트에 라이선스가 할당됩니다. 어카운트 관리자는 지역, 부서, 자회사 등에 대해 가상 어카운트를 추가로 생성할 수 있습니다. 여러 가상 어카운트가 있으면 수많은 라이선스 및 디바이스를 관리할 수 있습니다.

가상 어카운트에서 라이선스를 관리합니다. 해당 가상 어카운트의 디바이스만 어카운트에 할당된 라이선스를 사용할 수 있습니다. 추가 라이선스가 필요할 경우 다른 가상 계정의 미사용 라이선스를 이전할 수 있습니다. 또한 가상 어카운트 간에 디바이스를 이전할 수도 있습니다.

에어 갭(Air-Gapped) 구축 라이선싱 옵션

다음 표에서는 인터넷 액세스가 없는 환경에서 사용 가능한 라이선싱 옵션을 비교합니다. 영업 담당자가 특정 상황에 대한 추가적인 조언을 할 수 있습니다.

표 *9:* 에어 갭*(Air-Gapped)* 네트워크에 대한 라이선싱 옵션 비교

Smart Software Manager 온프레미스	특정 라이선스 예약
다수의 제품에 대한 확장 가능성	소수의 디바이스에 대한 최적성
자동화된 라이선싱 관리, 사용 및 자산 관리 가시성	제한된 사용 및 자산 관리 가시성
디바이스 추가 시 운영비 증가 없음	디바이스 추가 시 시간 경과에 따라 선형 운영비
유연성, 사용 용이성, 오버헤드 감소	이동, 추가 및 변경에 대한 중요한 관리 및 수동 오버헤드
규정 위반(out-of-compliance) 상태는 초기 및 여러 만료 상태로 허용됩니다.	규정 위반 상태는 시스템 기능에 영향을 줍니다.
자세한 내용은 Management Center를 Smart Software Manager 온프레미스로 등록, 287 페이지을 참조해 주십시오.	자세한 내용은 SLR(Specific License Reservation) 구성, 297 페이지을 참조해 주십시오.

Management Center 및 디바이스에 대한 라이선싱 작동 방식

management center는 Smart Software Manager에 등록한 다음 각 매니지드 디바이스에 대해 라이선스를 할당합니다. 디바이스는 Smart Software Manager에 직접 등록되지 않습니다.

물리적 management center은 자체 사용을 위한 라이선스가 필요하지 않습니다. management center virtual에는 플랫폼 라이선스가 필요합니다.

Smart Software Manager와의 정기적인 통신

제품 라이선스 엔타이틀먼트를 유지하기 위해 제품은 Smart Software Manager와 주기적으로 통신해야 합니다.

제품 인스턴스 등록 토큰을 사용하여 management center을 Smart Software Manager에 등록합니다. Smart Software Manager는 management center와 Smart Software Manager 간의 통신을 위해 ID 인증서를 발급합니다. 이 인증서는 6개월마다 갱신되지만 1년간 유효합니다. ID 인증서가 만료되면(1년 후) management center은 계정에서 제거될 수 있습니다.

management center는 주기적으로 Smart Software Manager와 통신합니다. Cisco Smart Software Manager에 변경이 있는 경우, management center에서 권한을 새로 고침하고 변경 사항을 즉시 적용할 수 있습니다. 또는 management center에서 예정대로 통신할 때까지 기다릴 수 있습니다.

management center은 Smart Software Manager에 대한 직접 인터넷 액세스 권한이 있거나 에어 갭(Air-Gapped) 구축 라이선싱 옵션, 262 페이지에 설명된 옵션 중 하나를 사용해야 합니다. 비 에어 갭(Air-Gapped) 구축에서 일반 라이선스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 management center는 최대 90일간 Smart Software Manager에 접촉하지 않고 작동할 수 있습니다. 90일이 지나기 전에 management center가 Smart Software Manager에 접촉하는지 확인합니다. 그렇지 않으면 management center가 등록되지 않은 상태로 되돌아갑니다.

평가 모드

management center는 Smart Software Manager에 등록하기 전에 평가 모드에서 90일 동안 작동합니다. 매니지드 디바이스에 기능 라이선스를 할당할 수 있으며, 평가 모드 기간 동안 규정을 준수합니다. 이 기간이 끝나면 management center의 등록이 취소됩니다.

management center를 Smart Software Manager에 등록하면 평가 모드가 종료됩니다. 나중에 management center의 등록을 취소하면 처음에 90일을 모두 사용하지 않았더라도 평가 모드를 다시 시작할 수 없습니다.

등록되지 않은 상태에 대한 자세한 내용은 등록 취소 상태, 264 페이지의 내용을 참조하십시오.

참고 강력한 암호화(3DES/AES)를 위한 평가 라이선스를 받을 수 없습니다. 강력한 암호화(3DES/AES) 라이선스를 활성화하는 내보내기-컴플라이언스 토큰을 받으려면 Smart Software Manager에 등록해야 합니다.

규정 위반 상태

다음과 같은 상황에서 management center가 규정 위반이 될 수 있습니다.

- 과다 사용 — 매니지드 디바이스 또는 management center virtual에서 사용 불가한 라이선스를 사용할 경우.
- 라이선스 만료—매니지드 디바이스 기반 라이선스가 만료된 경우.

컴플라이언스 미준수 상태에서는 다음 효과를 확인할 수 있습니다.

- Management Center Virtual 플랫폼 라이선스 - 작업이 영향을 받지 않습니다.
- 모든 매니지드 디바이스 라이선스 - 작업은 영향을 받지 않습니다.

라이선싱 문제를 해결하면 management center에 Smart Software Manager를 통해 정기적으로 예약된 권한 부여 후 현재 컴플라이언스 상태임을 표시합니다. 권한 부여를 강제로 수행하려면 시스템 (⚙) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 페이지에서 **Re-Authorize(**재권한 부여**)**를 클릭합니다.

등록 취소 상태

다음과 같은 경우 management center가 등록 취소될 수 있습니다.

- 평가 모드 만료 - 평가 모드는 90일 후에 만료됩니다.
- management center의 수동 등록 해제
- Smart Software Manager와의 통신 부족 - management center는 1년 동안 Smart Software Manager와 통신하지 않습니다. 참고: 90일 후에 management center 권한 부여가 만료되지만 1년 이내에 통신을 성공적으로 재개하여 자동으로 다시 권한을 부여할 수 있습니다. 1년이 지나면 ID 인증서가 만료되고 management center가 어카운트에서 제거되므로 수동으로 management center를 다시 등록해야 합니다.

등록되지 않은 상태에서 management center는 라이선스가 필요한 기능에 대한 구성 변경 사항을 디바이스에 구축할 수 없습니다.

최종 사용자 라이선스 계약

이 제품의 사용에 대한 Cisco EULA(최종 사용자 라이선스 계약) 및 SEULA(적용 가능한 보완 계약은 http://www.cisco.com/go/softwareterms에서 제공됩니다.

라이선스 유형 및 제한 사항

이 섹션에서는 사용할 수 있는 라이선스 유형에 대해 설명합니다.

표 *10:* 스마트 라이선스

사용자가 할당한 라이선스	기간	부여된 기능
Essentials	영구 또는 구독 참고 Essentials 구독 라이선스는 Threat Defense Virtual에서만 지원됩니다.	특정 라이선스 예약과 Secure Firewall 3100을 제외하고 Essentials 영구 라이선스가 모든 threat defense에 자동으로 할당됩니다. 사용자 및 애플리케이션 제어 스위칭 및 라우팅 NAT 자세한 내용은 Essentials 라이선스, 267 페이지 섹션을 참조해 주십시오.
IPS	구독	침입 탐지 및 방지 파일 제어 보안 인텔리전스 필터링 자세한 내용은 다음을 참조하십시오. IPS 라이선스, 268 페이지
악성코드 방어	구독	악성코드 방어 Secure Malware Analytics 파일 스토리지 (IPS 라이선스는 악성코드 방어 라이선스의 사전 요건입니다.) 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 악성코드 방어 라이선스, 267 페이지 및 파일 및 악성코드 정책을 위한 라이선스 요구 사항을 참조하십시오.
캐리어	Firepower 4100/9300, Secure Firewall 3100 및 Threat Defense Virtual 구독	Diameter, GTP/GPRS, M3UA 및 SCTP 검사 자세한 내용은 통신 사업자 라이선스, 269 페이지 섹션을 참조해 주십시오.
URL	구독	카테고리 및 평판 기반 URL 필터링 자세한 내용은 URL 라이선스, 270 페이지 섹션을 참조해 주십시오. (IPS 라이선스는 URL 라이선스의 사전 요건입니다.)

사용자가 할당한 라이선스	기간	부여된 기능
Management Center Virtual	• 일반 Smart Licensing - 영구 • 특정 라이선스 예약—구독	플랫폼 라이선스는 management center virtual가 관리할 수 디바이스 수를 결정합니다. 자세한 내용은 Management Center Virtual 라이선스, 266 페이지 섹션을 참조해 주십시오.
내보내기 제어 기능	영구	국가 보안, 외교 정책, 테러 방지법 및 규제의 적용을 받는 기능. 내보내기 제어 기능 라이선싱, 271 페이지를 참조하십시오.
원격 액세스 VPN: • Secure Client Premier • Secure Client Advantage • Secure Client VPN Only	구독 또는 영구	원격 액세스 VPN 컨피그레이션 계정은 원격 액세스 VPN을 구성하기 위해 내보내기 제어 기능을 허용해야 합니다. 디바이스를 등록할 때 내보내기 요구사항을 충족하는지를 선택합니다. threat defense는 유효한 Secure Client 라이선스를 사용할 수 있습니다. 제공되는 기능은 라이선스 유형에 따라 달라지지 않습니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 Secure Client 라이선스, 270 페이지 및 *VPN* 라이선싱을 참조하십시오.

참고 구독 라이선스는 조건 기반 라이선스입니다.

Management Center Virtual 라이선스

management center virtual에는 관리할 수 있는 디바이스의 수와 상관관계가 있는 플랫폼 라이선스가 필요합니다.

management center virtual는 스마트 라이선싱을 지원합니다.

일반 스마트 라이선싱에서 이러한 라이선스는 영구적입니다.

SLR(특정 라이선스 예약)에서는 이러한 라이선스가 구독 기반입니다.

참고 FMCv에 있는 새 디바이스의 애드온 라이선스 요구 사항은 추가 디바이스를 지원하는 상위 management center virtual 모델로 마이그레이션하는 것이 좋습니다.

Essentials 라이선스

Essentials 라이선스를 통해 다음을 수행할 수 있습니다.

- 디바이스를 구성하고 스위칭 및 라우팅(DHCP 릴레이 및 NAT 포함)을 수행합니다.
- 디바이스를 고가용성 쌍으로 구성합니다.
- 클러스터링 구성
- 액세스 제어 규칙에 사용자 및 애플리케이션 상태를 추가하여 사용자 및 애플리케이션 제어를 수행할 수 있습니다.
- VDB(취약점 데이터베이스) 및 GeoDB(지리적 데이터베이스)를 업데이트합니다.
- SRU/LSP와 같은 침입 규칙을 다운로드합니다. 그러나 IPS 라이선스가 활성화되어 있지 않으면 액세스 제어 정책 또는 침입 정책이 있는 규칙을 디바이스에 구축할 수 없습니다.

Secure Firewall 3100

Secure Firewall 3100을 구매하면 Essentials 라이선스를 받게 됩니다.

다른 모든 모델

Specific License Reservation(특정 라이선스 예약)을 사용하는 구축을 제외하고 Essentials 라이선스는 디바이스를 management center에 등록하면 자동으로 사용자 어카운트에 추가됩니다. 특정 라이선스 예약의 경우 Essentials 라이선스를 어카운트에 추가해야 합니다.

악성코드 방어 라이선스

악성코드 방어 라이선스를 사용하면 악성코드 대응 및 Secure Malware Analytics을 수행할 수 있습니다. 이러한 기능으로 디바이스를 사용하여 네트워크를 통해 전송된 파일에서 악성코드를 탐지 및 차단할 수 있습니다. 이러한 기능 라이선스를 지원하려면 악성코드 방어(AMP) 서비스 구독을 독립 실행형 구독으로 구매하거나 IPS(TM) 또는 IPS 및 URL(TMC) 구독과 함께 구매할 수 있습니다. IPS 라이선스는 악성코드 방어 라이선스의 사전 요건입니다.

참고 악성코드 방어 라이선스가 정기적으로 활성화되는 매니지드 디바이스는 사용자가 동적 분석을 구성하지 않은 경우에도 Secure Malware Analytics 클라우드 연결을 시도합니다. 따라서, 디바이스의 Interface Traffic(인터페이스 트래픽) 대시보드 위젯은 전송된 트래픽을 보여주며, 이는 예상된 작업입니다.

사용자는 파일 정책의 일부로서 악성코드 대응 를 구성한 후 하나 이상의 액세스 제어 규칙과 연결합니다. 파일 정책은 사용자가 특정 애플리케이션 프로토콜을 통해 특정 유형의 파일을 업로드 또는 다운로드하는지를 탐지할 수 있습니다. 악성코드 대응 을 통해 로컬 악성 코드 분석 및 파일 사전 분류를 사용하여 그러한 제한된 파일 유형의 집합에 악성코드가 있는지 검사할 수 있습니다. 또한 Secure Malware Analytics 클라우드에서 특정 파일 유형을 다운로드 및 전송하여 동적 분석과 Spero 분석으로 해당 파일에 악성코드가 포함되었는지 여부를 결정합니다. 이러한 파일에서 네트워크 파일 경로를 상세히 볼 수 있습니다. 악성코드 방어 라이선스는 또한 특정 파일을 파일 목록에 추가하고 파일

정책 내에서 파일 목록을 활성화하며, 해당 파일이 탐지되면 자동으로 허용하거나 차단하도록 허용합니다.

참고로 악성코드 대응 및 Secure Malware Analytics를 구축하는 경우에만 악성코드 방어 라이선스가 필요합니다. 악성코드방어라이선스가 없는 경우, management center은 엔드포인트 Secure Endpoint 악성코드 이벤트 및 보안 침해 지표(IOC)를 Secure Malware Analytics 클라우드에서 받을 수 있습니다.

Cisco Secure Firewall Management Center 디바이스 구성 가이드의 파일 및 악성코드 정책에 대한 라이선스 요구 사항의 중요 정보도 참조하십시오.

이 라이선스를 비활성화하는 경우:

- 시스템에서 Secure Malware Analytics 클라우드에 대한 쿼리를 중단하며 Secure Malware Analytics 클라우드에서 전송한 회귀적 이벤트 확인도 중지합니다.
- 악성코드 대응 구성이 포함된 경우, 기존 액세스 제어 정책은 재적용할 수 없습니다.
- 악성코드 방어 라이선스가 비활성화된 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 시간대가 만료된 후 시스템은 해당 파일에 `Unavailable(사용 불가)` 속성을 할당합니다.

라이선스가 만료되면 위 기능에 대한 엔타이틀먼트가 중지되고 management center가 규정을 준수하지 않는 상태로 전환됩니다.

IPS 라이선스

IPS 라이선스는 침입 탐지 및 방지, 파일 제어 및 보안 인텔리전스 필터링을 수행할 수 있습니다.

- 침입 탐지 및 방지를 사용하면 침입 및 공격의 트래픽을 분석하고, 선택적으로 문제가 되는 패킷을 삭제할 수 있습니다.
- *File control(*파일 제어*)*를 사용하면 사용자가 특정 애플리케이션 프로토콜에 특정 유형의 파일을 업로드(전송)하거나 다운로드(수신)하는 것을 탐지하고, 선택적으로 차단할 수 있습니다. 악성코드 차단 라이선스가 필요한 악성코드 대응 는 제한적인 해당 파일 유형 집합을 속성에 따라 검사 및 차단할 수 있습니다.
- *Security Intelligence filtering(*보안 인텔리전스 필터링*)*을 사용하면 트래픽이 액세스 제어 규칙에 따라 분석의 대상이 되기 전에 특정 IP 주소, URL 및 DNS 도메인 이름을 차단 목록에 추가하고 이를 오고가는 트래픽을 거부할 수 있습니다. 동적 피드를 사용하면 최신 인텔리전스를 기반으로 연결을 즉시 차단할 수 있습니다. 경우에 따라 Seurity Intelligence 필터링에 "모니터링 전용" 설정을 사용할 수 있습니다.

IPS 라이선스를 독립형 서브스크립션(T) 또는 URL (TC), 악성코드 차단(TM)과 각각 결합하거나 동시에 결합(TMC)한 서브스크립션으로 구입할 수 있습니다.

이 라이선스를 비활성화하는 경우:

- management center이 영향을 받는 디바이스에서 침입 및 파일 이벤트 인지를 중단합니다. 결과적으로, 해당 이벤트를 트리거 기준으로 사용하는 상관성 규칙이 실행을 중지합니다.
- management center은 Cisco 제공 정보나 서드파티 Security Intelligence 정보를 검색하기 위해 인터넷에 접속하지 않습니다.

- IPS 라이선스를 다시 활성화할 때까지 현재 침입 정책을 다시 배포할 수 없습니다.

라이선스가 만료되면 위 기능에 대한 엔타이틀먼트가 중지되고 management center가 규정을 준수하지 않는 상태로 전환됩니다.

통신 사업자 라이선스

통신 사업자 라이선스를 사용하면 다음 프로토콜을 검사할 수 있습니다:

- Diameter - Diameter는 LTE(Long Term Evolution) 및 IMS(IP Multimedia Subsystem)용 EPS(Evolved Packet System)와 같은 차세대 모바일 및 고정 통신 네트워크에서 사용되는 AAA(Authentication, Authorization, and Accounting) 프로토콜입니다. 이는 이러한 네트워크에서 RADIUS 및 TACACS를 대체합니다.
- GTP/GPRS - GTP(GPRS Tunneling Protocol)는 GSM, UMTS 및 LTE 네트워크에서 GPRS(General Packet Radio Service) 트래픽에 사용됩니다. GTP는 SGSN에서 터널을 생성, 수정 및 삭제하여 이동 통신국용 GPRS 네트워크 액세스를 제공하는 터널 제어 및 관리 프로토콜을 제공합니다. GTP는 또한 사용자 데이터 패킷을 전송하기 위해 터널링 메커니즘을 사용합니다.
- M3UA - M3UA(MTP3 User Adaptation)는 SS7 MTP3(Message Transfer Part 3) 레이어와 인터페이스하는 IP 기반 애플리케이션에 대해 SS7(Signaling System 7) 네트워크에 대한 게이트웨이를 제공하는 클라이언트/서버 프로토콜입니다. M3UA를 사용하면 IP 네트워크를 통해 SS7 사용자 부분(예: ISUP)을 실행할 수 있습니다.
- SCTP - SCTP(Stream Control Transmission Protocol)는 IP 네트워크를 통해 SS7 프로토콜을 지원하는 전송 계층 프로토콜입니다. 4G LTE 모바일 네트워크 아키텍처를 지원합니다. SCTP는 여러 동시 스트림, 다중 스트림을 처리할 수 있으며 더 많은 보안 기능을 제공합니다.

참고 디바이스에서 이 라이선스를 활성화한 후 FlexConfig 정책을 사용하여 프로토콜 검사를 활성화합니다.

통신 사업자 라이선스 PID는 디바이스 모델이 아닌 제품군별로 사용할 수 있습니다. 평가 모드에서 또는 스마트 라이선스를 사용하여 각 디바이스에 대해 이 라이선스를 활성화할 수 있습니다.

Firepower4100/9300, Secure Firewall 3100 및 Threat Defense Virtual에 대한 통신 사업자 라이선스는 기간별입니다. 이 라이선스는 특정 라이선스 예약도 지원합니다.

지원되는 장치

통신 사업자 라이선스를 지원하는 디바이스는 다음과 같습니다.

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140

- Firepower 4112
- Firepower 4115
- Firepower 4125
- Firepower 4145
- Firepower 9300
- Threat Defense Virtual

URL 라이선스

URL 라이선스를 사용하면 액세스 제어 규칙을 작성할 수 있습니다. 이 규칙은 모니터링된 호스트에서 요청하고 URL 정보와 상호 연결된 해당 URL을 기준으로 네트워크를 이동할 수 있는 트래픽을 결정합니다. 이러한 기능 라이선스를 지원하려면 URL 서비스 구독을 독립 실행형 구독으로 구매하거나 IPS(TC) 또는 위협 및 악성코드 방어(TMC) 구독과 함께 구매할 수 있습니다. IPS 라이선스는 이 라이선스의 사전 요건입니다.

팁 URL 라이선스 없이, 허용하거나 차단할 개별 URL 또는 URL 그룹을 지정할 수 있습니다. 이 옵션을 통해 웹 트래픽에 대한 세분화된 사용자 지정 제어를 가질 수 있지만 URL 카테고리와 평판 데이터를 사용하여 네트워크 트래픽을 필터링할 수는 없습니다.

URL 라이선스 없이도 액세스 제어 규칙에 카테고리 및 평판 기반 URL 조건을 추가할 수 있지만, management center은 URL 정보를 다운로드하지 않습니다. 먼저 URL 라이센스를 management center에 추가한 후 정책의 대상이 되는 디바이스에서 활성화에 추가할 때까지 액세스 제어 정책을 구축할 수 없습니다.

이 라이선스를 비활성화하는 경우:

- URL 필터링에 액세스하지 못할 수 있습니다.
- URL 조건이 포함된 액세스 제어 규칙은 즉시 URL 필터링을 중지합니다.
- management center는 더 이상 URL 데이터에 대한 업데이트를 다운로드할 수 없습니다.
- 카테고리 및 평판 기반 URL 조건이 들어 있는 규칙을 포함하는 기존 액세스 제어 정책은 재적용할 수 없습니다.

라이선스가 만료되면 위 기능에 대한 엔타이틀먼트가 중지되고 management center가 규정을 준수하지 않는 상태로 전환됩니다.

Secure Client 라이선스

Secure Client 및 표준 기반 IPSec/IKEv2를 사용하여 원격 액세스 VPN을 구성할 수 있습니다.

원격 액세스 VPN을 사용하려면 Secure Client Advantage, Secure Client Premier 또는 Secure Client VPN Only 라이선스 중 하나를 구입하여 활성화해야 합니다. 두 라이선스가 둘 다 있으며 모두 사용하려는 경우 Secure Client Advantage 및 Secure Client Premier를 선택할 수 있습니다. Secure Client VPN Only

라이선스는 **Apex** 또는 **Plus**와 사용할 수 없습니다. Secure Client 라이선스는 스마트 어카운트와 공유해야 합니다. 자세한 설명은 http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf을 참조하십시오.

지정된 디바이스에 지정된 Secure Client 라이선스 유형 중 하나에 대한 최소한의 엔타이틀먼트가 없는 경우, 원격 액세스 VPN 구성을 디바이스에 배포할 수 없습니다. 등록된 라이선스를 준수하지 않거나 엔타이틀먼트가 만료된 경우, 시스템에 라이선스 경고 및 상태 이벤트가 나타납니다.

원격 액세스 VPN을 사용하는 동안 스마트 어카운트는 내보내기 제어 기능(강력한 암호화)가 활성화되어 있어야 합니다. threat defense는 원격 액세스 VPN과 Secure Client의 성공적인 연결을 위해 강력한 암호화(DES 보다 더 높은 수준)를 필요로 합니다.

다음의 경우에 원격 액세스 VPN을 구축할 수 없습니다.

- management center에서 스마트 라이선싱이 평가판 모드로 실행됩니다.
- 스마트 어카운트가 내보내기 제어 기능(강력한 암호화)를 사용하도록 구성되지 않습니다.

내보내기 제어 기능 라이선싱

내보내기 제어 기능이 필요한 기능

특정 소프트웨어 기능은 국가 보안, 외교 정책, 테러 방지법 및 규제의 적용을 받습니다. 이러한 내보내기 제어 기능은 다음을 포함합니다.

- 보안 인증서 컴플라이언스
- 원격 액세스 VPN
- 사이트 간 VPN 및 강력한 암호화
- SSH 플랫폼 정책 및 강력한 암호화
- SSL 정책 및 강력한 암호화
- SNMPv3 같은 기능 및 강력한 암호화

시스템에서 현재 내보내기 제어 기능이 활성화되어 있는지를 결정하는 방법

시스템에서 현재 내보내기 제어 기능이 활성화되어 있는지를 결정하는 방법: **System(**시스템**) > Licenses(**라이선스**) > Smart Licenses(**스마트 라이선스**)**로 이동하고 **Export-Controlled Features(**내보내기 제어 기능**)**에 **Enabled(**활성화 완료**)**로 나타나는지 확인합니다.

내보내기 제어 기능 활성화 정보

Export-Controlled Features(내보내기 제어 기능**)**이 **Disabled(**비활성화**)**로 표시되고 강력한 암호화를 필요로 하는 기능을 사용하려는 경우, 강력한 암호화 기능을 활성화하는 방법에는 두 가지가 있습니다. 해당 기관에서는 둘 중 하나를 사용할 수 있겠지만(또는 둘 다 아님) 둘 모두를 사용할 수는 없습니다.

- Smart Software Manager에서 새 Product Instance Registration(제품 인스턴스 등록)을 생성할 때 내보내기 제어 기능을 활성화하는 옵션이 없는 경우 계정 담당자에게 문의하십시오.

  Cisco에서 승인하면 내보내기 제어 기능을 사용할 수 있도록 강력한 암호화 라이선스를 계정에 수동으로 추가할 수 있습니다. 자세한 내용은 (전역 권한이 없는 어카운트의) 내보내기 제어 기능 활성화, 288 페이지을 참조해 주십시오.

- Smart Software Manager에서 새 제품 인스턴스 등록 토큰을 생성할 때 "Allow export-controlled features on the products registered with this token(이 토큰으로 등록된 제품에서 내보내기 제어 기능 허용)" 옵션이 표시되는 경우, 토큰을 생성하기 전에 해당 토큰을 선택해야 합니다.

  management center 등록에 사용한 제품 인스턴스 등록 토큰에 대해 내보내기 제어 기능을 활성화하지 않은 경우, 내보내기 제어 기능이 활성화된 상태에서 새 제품 인스턴스 등록 토큰을 사용하여 management center를 등록 취소한 다음 다시 등록해야 합니다.

평가 모드에서 또는 management center에서 강력한 암호화를 활성화하기 전에 management center에 디바이스를 등록한 경우, 각 매니지드 디바이스를 재부팅하여 강력한 암호화를 사용할 수 있게 합니다. 고가용성 구축에서, 액티브-액티브 상태를 방지하기 위해 액티브 디바이스 및 스탠바이 디바이스를 함께 재부팅해야 합니다.

엔타이틀먼트는 영구적이며 서브스크립션이 필요하지 않습니다.

추가 정보

내보내기 제어에 대한 일반 정보는 https://www.cisco.com/c/en/us/about/legal/global-export-trade.html를 참조하십시오.

Threat Defense Virtual 라이선스

이 섹션에서는 threat defense virtual에서 사용 가능한 성능 계층 라이선스 자격을 설명합니다.

모든 threat defense virtual 라이선스는 지원되는 threat defense virtual vCPU/메모리 설정에서 사용할 수 있습니다. 따라서 threat defense virtual 고객은 다양한 VM 리소스 사용 공간에서 실행할 수 있습니다. 또한 지원되는 AWS 및 Azure 인스턴스 유형의 수가 증가합니다. threat defense virtual VM을 설정할 때 지원되는 최대 코어 수(vCPU)는 16개이고 지원되는 최대 메모리는 32GB RAM입니다.

Threat Defense Virtual 스마트 라이선싱의 성능 계층

RA VPN의 세션 제한은 설치된 threat defense virtual 플랫폼 엔타이틀먼트 계층에 따라 결정되고, 속도 제한기를 통해 적용됩니다. 다음 테이블에는 엔타이틀먼트 계층 및 속도 제한기에 따른 세션 제한이 요약되어 있습니다.

표 ***11:*** 자격 기준 ***Threat Defense Virtual*** 라이선스 기능 제한

성능 계층	디바이스 사양 **(Core/RAM)**	속도 제한	**RA VPN** 세션 제한
FTDv5, 100Mbps	4 코어/8GB	100Mbps	50
FTDv10, 1Gbps	4 코어/8GB	1Gbps	250

성능 계층	디바이스 사양 (Core/RAM)	속도 제한	RA VPN 세션 제한
FTDv20, 3Gbps	4 코어/8GB	3Gbps	250
FTDv30, 5Gbps	8 코어/16GB	5Gbps	250
FTDv50, 10Gbps	12 코어/24GB	10Gbps	750
FTDv100, 16Gbps	16 코어/32GB	16Gbps	10,000

FTDv 성능 계층 라이선싱 지침 및 제한

threat defense virtual 디바이스 라이선싱 시 다음 지침과 제한 사항에 유의하십시오.

- threat defense virtual에서는 구축 요건에 따라 다양한 처리량 레벨 및 VPN 연결 제한을 제공하는 성능 계층 라이선싱을 지원합니다.
- 모든 threat defense virtual 라이선스는 지원되는 threat defense virtual 코어/메모리 설정에서 사용할 수 있습니다. 따라서 threat defense virtual 고객은 다양한 VM 리소스 사용 공간에서 실행할 수 있습니다.
- 디바이스가 평가 모드인지 또는 이미 Cisco Smart Software Manager에 등록되어 있는지 여부와 무관하게 threat defense virtual 구축 시 성능 계층을 선택할 수 있습니다.

참고 Smart Licensing 계정에서 필요한 라이선스가 사용 가능한지 확인합니다. 어카운트에 있는 라이선스와 일치하는 계층을 선택하는 것이 중요합니다. threat defense virtual를 버전 7.0으로 업그레이드하는 경우 **FTDv - Variable(FTDv - 변수)**를 선택하여 현재 라이선스 컴플라이언스를 유지할 수 있습니다. threat defense virtual는 디바이스 기능(코어/RAM 수)에 따라 계속 세션 제한을 수행합니다.

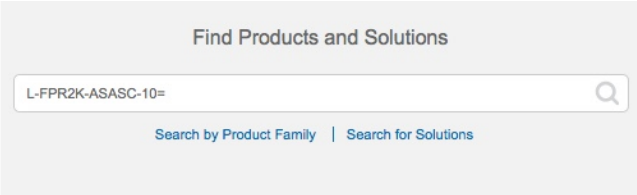
- 새 threat defense virtual 디바이스를 구축하거나 REST API를 사용한 threat defense virtual 프로비저닝 시 기본 성능 계층은 FTDv50입니다.
- Essentials 라이선스는 구독 기반이며 성능 계층에 매핑됩니다. 가상 어카운트에는 IPS, 악성코드 방어 및 URL 라이선스는 물론, threat defense virtual 디바이스에 대한 Essentials 라이센스 자격이 있어야 합니다.
- 각 HA 피어는 하나의 자격을 사용하고, Essentials 라이선스를 포함하여 각 HA 피어의 자격이 일치해야 합니다.
- HA 쌍의 성능 계층 변경 사항을 기본 피어에 적용해야 합니다.
- 개별 노드가 아니라 전체 피처 클러스터에 라이선스를 할당합니다. 그러나 클러스터의 각 노드는 각 기능에 대한 별도 라이선스를 사용합니다. 클러스터링 기능 자체에는 라이선스가 필요하지 않습니다.

- 범용 PLR 라이선싱은 HA 쌍의 각 디바이스에 개별적으로 적용됩니다. 보조 디바이스는 기본 디바이스의 성능 계층을 자동으로 미러링하지 않습니다. 수동으로 업데이트해야 합니다.

라이선스 PID

Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 Smart Software License 계정에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace에서 **Find Products and Solutions(**제품 및 솔루션 찾기**)** 검색 필드를 사용합니다. 다음 라이선스 제품 ID(PID)를 검색합니다.

그림 *8:* 라이선스 검색



Management Center Virtual PID

- VMware:
  - SF-FMC-VMW-2-K9 - 디바이스 2개
  - SF-FMC-VMW-10-K9 - 디바이스 10개
  - SF-FMC-VMW-K9 - 디바이스 25개
  - SF-FMC-VMW-300-K9 — 디바이스 300개
- KVM
  - SF-FMC-KVM-2-K9 - 디바이스 2개
  - SF-FMC-KVM-10-K9 — 디바이스 10개
  - SF-FMC-KVM-K9 - 디바이스 25개
- PAK 기반 VMware:
  - FS-VMW-2-SW-K9 - 디바이스 2개
  - FS-VMW-10-SW-K9 - 디바이스 10개
  - FS-VMW-SW-K9 - 디바이스 25개

Threat Defense Virtual PID

FTDV-SEC-SUB를 주문할 때 Essentials 라이선스 및 선택적 기능 라이선스(12개월 기간)를 선택해야 합니다.

- Essentials 라이선스:
  - FTD-V-5S-BSE-K9
  - FTD-V-10S-BSE-K9
  - FTD-V-20S-BSE-K9
  - FTD-V-30S-BSE-K9
  - FTD-V-50S-BSE-K9
  - FTD-V-100S-BSE-K9
- IPS, Malware 방어 및 URL 라이선스 조합:
  - FTD-V-5S-TMC
  - FTD-V-10S-TMC
  - FTD-V-20S-TMC
  - FTD-V-30S-TMC
  - FTD-V-50S-TMC
  - FTD-V-100S-TMC
- Carrier—FTDV_CARRIER
- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Firepower 1010 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR1010T-TMC =

  위의 PID를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Firepower 1100 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR1120T-TMC =

- L-FPR1140T-TMC =
- L-FPR1150T-TMC =

위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.

- L-FPR1120T-TMC-1Y
- L-FPR1120T-TMC-3Y
- L-FPR1120T-TMC-5Y
- L-FPR1140T-TMC-1Y
- L-FPR1140T-TMC-3Y
- L-FPR1140T-TMC-5Y
- L-FPR1150T-TMC-1Y
- L-FPR1150T-TMC-3Y
- L-FPR1150T-TMC-5Y

- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Firepower 2100 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-TMC=

위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.

- FPR2110T-TMC-1Y
- L-FPR2110T-TMC-3Y
- L-FPR2110T-TMC-5Y
- L-FPR2120T-TMC-1Y
- L-FPR2120T-TMC-3Y
- L-FPR2120T-TMC-5Y
- L-FPR2130T-TMC-1Y

- L-FPR2130T-TMC-3Y
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Secure Firewall 3100 PID

- Essentials 라이선스:
  - L-FPR3110-BSE=
  - L-FPR3120-BSE=
  - L-FPR3130-BSE=
  - L-FPR3140-BSE=
- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR3110T-TMC=
  - L-FPR3120T-TMC=
  - L-FPR3130T-TMC=
  - L-FPR3140T-TMC=

  위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - L-FPR3105T-TMC-1Y
  - L-FPR3105T-TMC-3Y
  - L-FPR3105T-TMC-5Y
  - L-FPR3110T-TMC-1Y
  - L-FPR3110T-TMC-3Y
  - L-FPR3110T-TMC-5Y
  - L-FPR3120T-TMC-1Y
  - L-FPR3120T-TMC-3Y
  - L-FPR3120T-TMC-5Y
  - L-FPR3130T-TMC-1Y

- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-TMC-5Y

- 캐리어:
  - L-FPR3K-FTD-CAR=

- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Firepower 4100 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR4112T-TMC=
  - L-FPR4115T-TMC =
  - L-FPR4125T-TMC =
  - L-FPR4145T-TMC =

  위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - L-FPR4112T-TMC-1Y
  - L-FPR4112T-TMC-3Y
  - L-FPR4112T-TMC-5Y
  - FPR4115T-TMC-1Y
  - L-FPR4115T-TMC-3Y
  - L-FPR4115T-TMC-5Y
  - L-FPR4125T-TMC-1Y
  - L-FPR4125T-TMC-3Y
  - L-FPR4125T-TMC-5Y
  - L-FPR4145T-TMC-1Y
  - L-FPR4145T-TMC-3Y
  - L-FPR4145T-TMC-5Y

- 캐리어:
  - L-FPR4K-FTD-CAR=
- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

Firepower 9300 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-FPR9K-40T-TMC =
  - L-FPR9K-48T-TMC =
  - L-FPR9K-56T-TMC =

  위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - L-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y
  - L-FPR9K-48T-TMC-1Y
  - L-FPR9K-48T-TMC-3Y
  - L-FPR9K-48T-TMC-5Y
  - L-FPR9K-56T-TMC-1Y
  - L-FPR9K-56T-TMC-3Y
  - L-FPR9K-56T-TMC-5Y
- 캐리어:
  - L-FPR9K-FTD-CAR=
- Cisco Secure Client - Cisco AnyConnect 주문 가이드를 참고하십시오.

ISA 3000 PID

- IPS, Malware 방어 및 URL 라이선스 조합:
  - L-ISA3000T-TMC=

  위의 PID를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - L-ISA3000T-TMC-1Y

- L-ISA3000T-TMC-3Y
- L-ISA3000T-TMC-5Y

- Cisco Secure Client - Cisco AnyConnect 주문 가이드를 참고하십시오.

라이선싱 요구 사항 및 사전 요건

특정 라이선스 예약 요구 사항의 경우 특정 라이센스 예약에 대한 요구 사항 및 사전 요건, 297 페이지의 내용을 참조하십시오.

일반적인 사전 요건

- management center 및 매니지드 디바이스에 NTP가 설정되어 있는지 확인합니다. 등록에 성공하려면 시간을 동기화해야 합니다.

  Firepower 4100/9300의 경우 management center와 동일한 NTP 서버를 사용하여 섀시에 NTP를 구성해야 합니다.

지원되는 도메인

글로벌, 표시된 경우를 제외하고.

사용자 역할

- 관리자

고가용성, 클러스터링 및 다중 인스턴스 라이선싱 요구 사항 및 사전 요건

이 섹션에서는 고가용성(디바이스 고가용성 및 management center virtual 고가용성), 클러스터링 및 다중 인스턴스 구축을 위한 라이선싱 요구 사항에 대해 설명합니다.

Management Center 고가용성을 위한 라이선싱

각 디바이스에는 단일 management center 또는 고가용성 쌍(하드웨어 또는 가상)의 management center로 관리되는 동일한 라이선스가 필요합니다.

예: management center 쌍으로 관리되는 두 디바이스에 대해 고급 악성코드 보호를 활성화하고 싶은 경우, 2개의 악성코드 방어 라이선스와 TM 서브스크립션을 구매하고 액티브 management center을 Smart Software Manager에 등록한 뒤 두 기기의 라이선스를 액티브 management center에 할당합니다.

액티브 management center만 Smart Software Manager에 등록됩니다. 페일오버가 발생하면 시스템은 Smart Software Manager와 통신하여 원래 활성 management center에서 라이선스 등록을 해제하고 새로운 액티브 management center에 할당합니다.

특정 라이선스 예약 구축에서는 기본 management center에서만 특정 라이선스 예약이 요구됩니다.

하드웨어 **Management Center**

고가용성 쌍의 하드웨어 management center에 필요한 특별한 라이선스는 없습니다.

Management Center Virtual

라이선스가 동일한 두 개의 management center virtual가 필요합니다.

예**:** 10개의 디바이스를 관리하는 management center virtual 고가용성 쌍의 경우 다음을 사용할 수 있습니다.

- management center virtual 10 엔타이틀먼트 2개
- 디바이스 라이선스 10개

고가용성 쌍을 분리하면 보조 management center virtual와 연결된 management center virtual 엔타이틀먼트가 해제됩니다. (이 예에서는 독립형 management center virtual 10이 2개 있습니다.)

디바이스 고가용성을 위한 라이선싱

고가용성 구성의 두 threat defense 유닛은 모두 동일한 라이선스를 가지고 있어야 합니다.

고가용성 구성에서는 디바이스 쌍의 각 디바이스에 대해 하나씩, 두 개의 라이선스 자격이 필요합니다.

고가용성을 설정하기 전에는 보조/스탠바이 디바이스에 어떤 라이선스가 할당되든 상관이 없습니다. 고가용성 설정 중에 management center은 스탠바이 유닛에 할당된 불필요한 라이선스를 해제하고 기본/액티브 유닛에 할당된 것과 동일한 라이선스로 교체합니다. 예를 들어 액티브 유닛에는 Essentials 라이선스와 IPS 라이선스가 있는데 스탠바이 유닛에 Essentials 라이선스만 있는 경우, management center은 Smart Software Manager와 통신하여 스탠바이 유닛의 어카운트에서 사용 가능한 IPS 라이선스를 가져옵니다. 라이선스에 포함되어 있는 구매한 엔타이틀먼트가 충분하지 않으면 정확한 수의 라이선스를 구매할 때까지 어카운트는 컴플라이언스 위반 상태가 됩니다.

디바이스 클러스터에 대한 라이선싱

각 threat defense virtual 클러스터 노드에는 동일한 성능 계층 라이선스가 필요합니다. 모든 멤버에 대해 동일한 수의 CPU 및 메모리를 사용하는 것이 좋습니다. 그렇지 않으면 성능이 가장 낮은 멤버와 일치하도록 모든 노드에서 제한됩니다. 처리량 레벨은 제어 노드에서 각 데이터 노드로 복제되어 일치합니다.

개별 노드가 아니라 전체 피처 클러스터에 라이선스를 할당합니다. 그러나 클러스터의 각 노드는 각 기능에 대한 별도 라이선스를 사용합니다. 클러스터링 기능 자체에는 라이선스가 필요하지 않습니다.

management center에 제어 노드를 추가하는 경우 클러스터에 사용하려는 기능 라이선스를 지정할 수 있습니다. 클러스터를 생성하기 전에는 데이터 노드에 할당된 라이선스가 중요하지 않습니다. 제어 노드의 라이선스 설정은 각 데이터 노드에 복제됩니다. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Cluster(**클러스터**)** > **License(**라이선스**)** 영역에서 클러스터 라이선스를 수정할 수 있습니다.

참고 management center이 라이선스 되기 전에 (평가 모드에서 실행 되기 전에) 클러스터를 추가하는 경우, management center를 라이선스하면 클러스터에 정책 변경을 구축할 때 트래픽 중단이 발생할 수 있습니다. 라이선스 모드를 변경하면 모든 데이터 유닛이 클러스터를 벗어났다가 다시 참가합니다.

다중 인스턴스 구축용 라이선싱

모든 라이선스는 (Firepower 4100의) 보안 엔진/섀시 또는 (Firepower 9300의) 보안 모듈에 대해 소비되지만 컨테이너 라이선스에 대해서는 소비되지 않습니다. 자세한 내용은 다음을 참조하십시오.

- Essentials 라이선스는 보안 모듈/엔진당 하나씩 자동으로 할당됩니다.
- 기능 라이선스는 각 인스턴스에 대해 수동으로 할당되지만 사용자는 보안 모듈/엔진의 기능당 하나의 라이선스를 소비합니다. 예를 들어 3개의 보안 모듈이 있는 Firepower 9300에 대해서는 모듈당 하나의 URL 라이선스가 필요하므로 사용 중인 인스턴스 수와 관계없이 총 3개의 라이선스가 필요합니다.

대표적인 예는 다음과 같습니다.

표 ***12: Firepower 9300***의 컨테이너 인스턴스에 대한 샘플 라이선스 사용

Firepower 9300	인스턴스	라이선스
보안 모듈 1	인스턴스 1	Essentials, URL, 악성코드 방어
	인스턴스 2	Essentials, URL
	인스턴스 3	Essentials, URL
보안 모듈 2	인스턴스 4	Essentials, IPS
	인스턴스 5	Essentials, URL, 악성코드 방어, IPS
보안 모듈 3	인스턴스 6	Essentials, 악성코드 방어, IPS
	인스턴스 7	Essentials, IPS

표 ***13:*** 수총 라이선스 수

Essentials	**URL**	악성코드 방어	**IPS**
3	2	3	2

스마트 어카운트 생성 및 라이선스 추가

이 어카운트를 설정하고 라이선스를 구입해야 합니다.

시작하기 전에

어카운트 담당자 또는 리셀러가 사용자 대신 스마트 어카운트를 설정했을 수도 있습니다. 그렇다면 이 절차를 사용하는 대신 해당 사용자의 어카운트에 액세스하는 데 필요한 정보를 얻은 후 해당 어카운트에 액세스할 수 있는지 확인합니다.

스마트 어카운트에 대한 일반 정보는 http://www.cisco.com/go/smartaccounts를 참조하십시오.

프로시저

단계 **1** 스마트 어카운트 요청:

자세한 내용은 https://community.cisco.com/t5/licensing-enterprise-agreements/request-a-smart-account-for-customers/ta-p/3636515?attachment-id=150577 섹션을 참조해 주십시오.

추가 정보는 https://communities.cisco.com/docs/DOC-57261 내용을 참조하십시오.

단계 **2** 스마트 어카운트 설정 준비가 완료되었다는 이메일이 올 때까지 기다립니다. 이메일이 도착하면, 지시된 대로 거기에 포함된 링크를 클릭합니다.

단계 **3** 스마트 어카운트를 설정하빈다.

https://software.cisco.com/software/company/smartaccounts/home?route=module/accountcreation로 이동합니다.

자세한 내용은 https://community.cisco.com/t5/licensing-enterprise-agreements/complete-smart-account-setup-for-customers/ta-p/3636631?attachment-id=132604 섹션을 참조해 주십시오.

단계 **4** Smart Software Manager에서 어카운트에 액세스할 수 있는지 확인합니다.

https://software.cisco.com/#module/SmartLicensing로 이동하여 로그인합니다.

단계 **5** Smart Licensing 계정에서 필요한 라이선스가 사용 가능한지 확인합니다.

Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 스마트 어카운트에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace를 참조하십시오. 라이선스 PID는 라이선스 PID, 274 페이지 섹션을 참조하십시오.

Smart Licensing 구성

이 섹션에서는 Smart Software Manager 또는 Smart Software Manager On-Prem을 사용하여 스마트 라이선싱을 사용하는 방법을 설명합니다. 특정 라이선스 예약을 사용하려면 SLR(Specific License Reservation) 구성, 297 페이지의 내용을 참조하십시오.

스마트 라이선싱을 위한 Management Center 등록

인터넷을 통해 또는 Air-Gapped 네트워크를 사용하는 경우 Smart Software Manager On-Prem을 사용하여 Smart Software Manager에 직접 management center를 등록할 수 있습니다.

Management Center를 Smart Software Manager로 등록

management center를 Smart Software Manager로 등록

시작하기 전에

- Smart Licensing 계정에서 필요한 라이선스가 사용 가능한지 확인합니다.

  Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 스마트 어카운트에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace를 참조하십시오. 라이선스 PID는 라이선스 PID, 274 페이지 섹션을 참조하십시오.

- management center가 Smart Software Manager(tools.cisco.com:443)에 연결할 수 있는지 확인합니다.

- NTP를 구성해야 합니다. 등록 중 스마트 에이전트 및 Smart Software Manager 간에 키 교환이 발생합니다. 따라서 시간을 해당 등록에 동기화해야 합니다.

  Firepower 4100/9300의 경우 management center와 동일한 NTP 서버를 사용하여 섀시에 NTP를 구성해야 합니다.

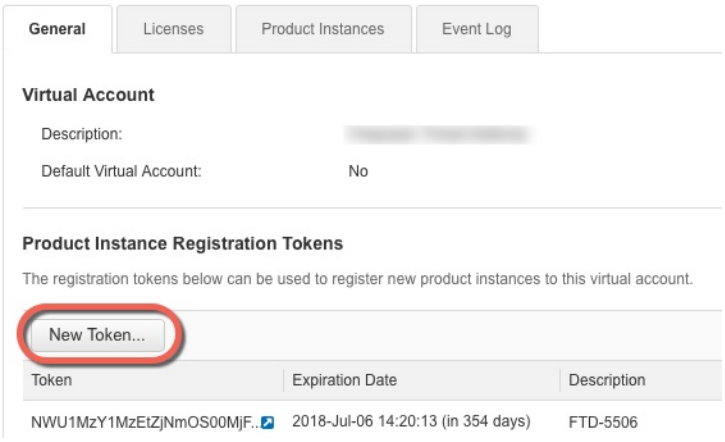
- 조직에 management center이(가) 여러 개 있다면, 각 management center의 이름이 동일한 가상 계정에 등록될 수 있는 다른 management center와(과) 명확하게 식별되는 고유한 이름인지 확인합니다. 이 이름은 스마트 라이선스 엔타이틀먼트 관리에 매우 중요하며 애매한 이름은 나중에 문제가 될 수 있습니다.

프로시저

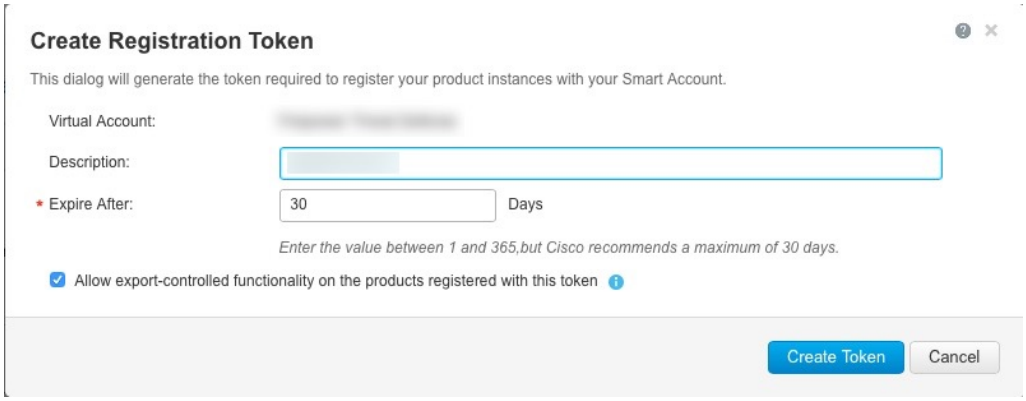
단계 **1** Smart Software Manager에서 이 디바이스를 추가할 가상 어카운트에 대한 등록 토큰을 요청 및 복사합니다.

a) **Inventory(**인벤토리**)**를 클릭합니다.

b) **General(**일반**)** 탭에서 **New Token(**새 토큰**)**을 클릭합니다.



c) **Create Registration Token(**등록 토큰 생성**)** 대화 상자에서 다음 설정을 입력한 다음 **Create Token(**토큰 생성**)**을 클릭합니다.



- 설명
- **Expire After(**다음 이후에 만료**)** — 30일로 설정하는 것이 좋습니다.
- **Allow export-controlled functionaility on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)**—강력한 암호화를 허용하는 국가에 있는 경우 내보내기-규정 준수 플래그를 활성화합니다. 해당 기능을 사용하려는 경우 이 옵션을 지금 선택해야 합니다. 나중에 이 기능을 활성화하는 경우 새 제품 키로 디바이스를 다시 등록하고 디바이스를 다시 로드해야 합니다. 이 옵션이 표시되지 않으면 계정이 내보내기 제어 기능을 지원하지 않는 것입니다.

토큰이 인벤토리에 추가됩니다.

d) 토큰의 오른쪽에 있는 화살표 아이콘을 클릭하여 **Token(**토큰**)** 대화 상자를 열면 토큰 ID를 클립보드에 복사할 수 있습니다. 나중에 절차에서 threat defense를 등록해야 하는 경우 사용하기 위해 이 토큰을 준비해 두십시오.

그림 *9:* 토큰 보기

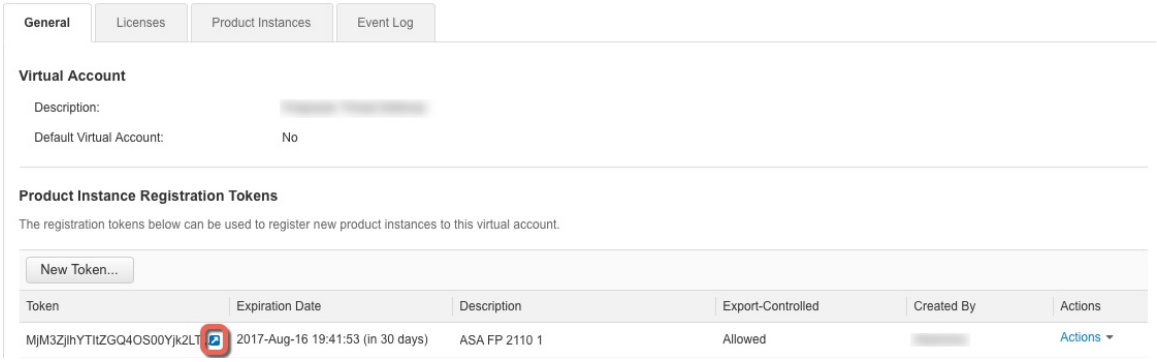
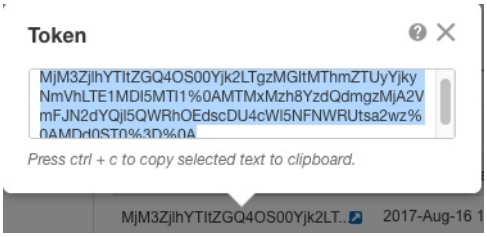


그림 *10:* 토큰 복사



단계 **2** management center에서 시스템 (⚙) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 선택합니다.

단계 **3** **Register(**등록**)**를 클릭합니다.

단계 **4** Smart Software Manager에서 생성한 토큰을 **Product Instance Registration Token(**제품 인스턴스 등록 토큰**)** 필드에 붙여넣기 합니다.

텍스트 시작이나 끝에 공백이나 빈 행이 없는지 확인합니다.

단계 **5** 사용량 데이터를 Cisco에 보낼지를 결정합니다.

- **Enable Cisco Success Network(Cisco Success Network** 활성화**)**는 기본적으로 활성화됩니다. 샘플 데이터를 클릭하고 Cisco에서 수집하는 데이터의 종류를 참조하십시오. 자세한 내용은 Cisco Success Network 등록 구성, 647 페이지를 참고하십시오.
- **Cisco Support Diagnostics** 활성화는 기본적으로 비활성화됩니다. 확인란 위에 있는 링크에서 Cisco가 수집하는 데이터 종류를 확인할 수 있습니다. 자세한 내용은 Cisco 지원 진단 등록 구성, 648 페이지를 참고하십시오.

  참고
  - 활성화하면, Cisco Support Diagnostics은 다음 동기화 주기에 디바이스에서 활성화됩니다. 디바이스와 management center 동기화는 30분마다 한 번씩 실행됩니다.
  - 활성화되면 Cisco Support Diagnostics가 이 management center에 등록된 모든 새 디바이스에서 자동으로 활성화됩니다.

단계 **6** **Apply Changes(**변경 사항 적용**)**를 클릭합니다.

다음에 수행할 작업

- 디바이스를 management center에 추가합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Management Center*에 디바이스 추가를 참조하십시오.
- 라이선스를 디바이스에 할당합니다. 여러 매니지드 디바이스에 라이선스 할당, 291 페이지의 내용을 참조하십시오.

Management Center를 Smart Software Manager 온프레미스로 등록

Smart Software Manager와의 정기적인 통신, 263 페이지에 설명된 대로, management center에서는 Cisco와 정기적으로 통신하여 라이선스 자격을 유지해야 합니다. 다음 상황 중 하나에 해당하는 경우 Smart Software Manager 온프레미스(이전 명칭: "Smart Software Satellite Server")을 Smart Software Manager에 연결하는 프록시로 사용할 수 있습니다.

- management center가 오프라인 상태이거나 연결이 제한적이거나 연결되지 않은 경우(즉, 에어 갭 네트워크에 구축).

  (공개 네트워크에 대한 대체 솔루션은 에어 갭(Air-Gapped) 구축 라이선싱 옵션, 262 페이지의 내용을 참조하십시오.)

- management center가 영구적으로 연결되어 있지만 네트워크에서 단일 연결을 통해 스마트 라이선스를 관리하려는 경우.

Smart Software Manager 온프레미스을(를) 사용하면 Smart Software Manager와의 동기화를 예약하거나 스마트 라이선스 인증을 수동으로 동기화할 수 있습니다.

Smart Software Manager 온프레미스에 대한 자세한 내용은 https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem 의 내용을 참조하십시오.

프로시저

단계 **1** Smart Software Manager 온프레미스을 구축하고 설정합니다.

- https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem에서 확인 가능한 Smart Software Manager 온프레미스에 대한 설명서를 참조하십시오.
- Smart Software Manager 온프레미스에서 TLS/SSL 인증서 CN을 메모합니다.
- http://www.cisco.com/security/pki/certs/clrca.cer로 이동한 다음, TLS/SSL 인증서 전체 본문("-----BEGIN CERTIFICATE-----" 부터 "-----END CERTIFICATE-----"까지)을 구성하는 동안 액세스할 수 있는 위치에 복사합니다.

단계 **2** management center을 Smart Software Manager 온프레미스에 등록합니다.

a) **Integration(**통합**)** > **Other Integrations(**기타 통합**)**를 선택합니다.

b) **Smart Software Satellite**를 클릭합니다.
c) **Connect to Cisco Smart Software Satellite Server(Cisco Smart Software Satellite Server**에 연결**)**을 선택합니다.
d) 이 절차의 사전 요구 사항에서 수집된 CN 값을 사용하여 Smart Software Manager 온프레미스의 **URL**을 다음 형식으로 입력합니다.

`https://FQDN_or_hostname_of_your_SSM_On-Prem/SmartTransport`

FQDN 또는 호스트 이름은 Smart Software Manager 온프레미스에서 제시하는 인증서의 CN 값과 일치해야 합니다.

e) 새 **SSL Certificate(SSL** 인증서**)**를 추가하고 이전에 복사한 인증서 텍스트를 붙여넣습니다.
f) **Apply(**적용**)**를 클릭합니다.
g) **System(**시스템**) > Licenses(**라이선스**) > Smart Licenses(**스마트 라이선스**)**를 선택하고 **Register(**등록**)**를 클릭합니다.
h) Smart Software Manager 온프레미스에서 신규 토큰을 생성합니다.
i) 토큰을 복사합니다.
j) 토큰을 관리 센터 페이지에 있는 양식에 붙여 넣습니다.
k) **Apply Changes(**변경 사항 적용**)**를 클릭합니다.

이제 관리 센터가 Smart Software Manager 온프레미스에 등록되었습니다.

단계 **3** 디바이스에 라이선스를 할당한 후 Smart Software Manager 온프레미스을 Smart Software Manager와 동기화합니다.

위의 Smart Software Manager 온프레미스 설명서를 참조하십시오.

단계 **4** 진행 중인 동기화 일정을 선택합니다.

(전역 권한이 없는 어카운트의) 내보내기 제어 기능 활성화

스마트 어카운트가 강력한 암호화에 대해 인증되지 않았지만 Cisco에서 강력한 암호화를 사용할 수 있다고 결정한 경우, 수동으로 어카운트에 강력한 암호화 라이선스를 추가할 수 있습니다.

시작하기 전에

- 구축에 이미 내보내기 제어 기능이 지원되지 않는지 확인합니다.

  구축에서 내보내기 제어 기능을 지원할 경우 등록 토큰 생성 페이지에는 Smart Software Manager 내보내기 제어 기능을 사용할 수 있는 옵션이 표시됩니다. 자세한 내용은 https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html를 참고하십시오.

- 구축에 평가판 라이선스가 사용되고 있지 않은지 확인합니다.
- Smart Software Manager의 **Inventory(**재고 목록**) > Licenses(**라이선스**)** 페이지에 다음과 같이 management center에 해당하는 라이선스가 있는지 확인합니다.

내보내기 제어 라이선스	**Management Center** 모델
Cisco Virtual FMC 시리즈 강력한 암호화 (3DES/AES)	모든 management center virtual
Cisco FMC 1K시리즈 강력한 암호화 (3DES/AES)	1000, 1600
Cisco FMC 2K 시리즈 강력한 암호화 (3DES/AES)	2500, 2600
Cisco FMC 4K 시리즈 강력한 암호화 (3DES/AES)	4500, 4600

프로시저

단계 **1** **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 선택합니다.

참고 **Request Export Key(**내보내기 키 요청**)**가 표시되는 경우, 해당 어카운트는 내보내기 제어 기능이 승인된 것이며 이 필요 기능 사용을 진행할 수 있습니다.

단계 **2** **Request Export Key(**내보내기 키 요청**)**를 클릭하고 내보내기 키를 생성합니다.

팁 내보내기 제어 키 요청이 실패하는 경우, 가상 어카운트에 유효한 내보내기 제어 라이선스가 있는지 확인합니다.

Return Export Key(내보내기 키 반환**)**를 클릭하여 내보내기 제어 라이선스를 비활성화합니다.

다음에 수행할 작업

이제 내보내기 제어 기능을 사용하는 구성이나 정책을 배포할 수 있습니다.

기억 새로운 내보내기 제어 라이선스 및 이 라이선스에 의해 활성화된 모든 기능은 디바이스가 재부팅될 때까지 threat defense 디바이스에 적용되지 않습니다. 그 때까지 이전 라이선스에서 지원하는 기능만 활성화됩니다.

고가용성 구축에서 threat defense 디바이스를 모두 동시에 재부팅해야 액티브-액티브 상태를 방지할 수 있습니다.

매니지드 디바이스에 라이선스 할당

디바이스를 management center에 등록할 때 대부분의 라이선스를 할당할 수 있습니다. 디바이스당 또는 여러 디바이스에 대해 라이선스를 할당할 수도 있습니다.

단일 디바이스에 라이선스 할당

몇 가지 예외는 있지만 매니지드 디바이스에서 비활성화한 라이선스와 관련된 기능은 사용할 수 없습니다.

참고 동일한 보안 모듈/엔진에 있는 컨테이너 인스턴스의 경우, 각 인스턴스에 라이선스를 적용합니다. 참고로 보안 모듈/엔진는 보안 모듈/엔진의 모든 인스턴스에 대해 기능당 하나의 라이선스만 사용합니다.

참고 threat defense 클러스터의 경우, 라이선스를 클러스터 전체에 적용합니다. 참고로 클러스터의 각 유닛은 기능당 별도의 라이선스를 필요로 합니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 네트워크 관리자 권한으로 로그인해야 합니다. 여러 도메인을 사용하여 작업하는 경우 리프 도메인에서 이 작업을 수행해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 라이선스를 활성화 또는 비활성화하려는 디바이스 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **Device(**디바이스**)**를 클릭합니다.

단계 **4** **License(**라이선스**)** 섹션 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **5** 해당 확인란을 선택하거나 지우고 디바이스에 대한 라이선스를 할당하거나 비활성화합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

다음에 수행할 작업

라이선스 상태 확인: 시스템 ( ) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**로 이동하여 Smart License(스마트 라이선스) 테이블 상단에 있는 필터에 디바이스의 호스트 이름 또는 IP 주소를 입력한 후, 라이선스 유형별 각 디바이스에 녹색 원(**Check Mark(**확인 표시**)** ( ))만 표시되는지 확인합니다. 다른 아이콘이 표시되는 경우, 아이콘 위에 마우스를 놓으면 자세한 정보가 표시됩니다.

여러 매니지드 디바이스에 라이선스 할당

management center로 관리하는 디바이스는 라이선스를 management center를 통해 얻습니다. Smart Software Manager에서 직접 하지 않습니다.

이 절차를 사용하여 여러 디바이스에서 한 번에 라이선스를 활성화합니다.

참고 동일한 보안 모듈/엔진에 있는 컨테이너 인스턴스의 경우, 각 인스턴스에 라이선스를 적용합니다. 참고로 보안 모듈/엔진는 보안 모듈/엔진의 모든 인스턴스에 대해 기능당 하나의 라이선스만 사용합니다.

참고 threat defense 클러스터의 경우, 라이선스를 클러스터 전체에 적용합니다. 참고로 클러스터의 각 유닛은 기능당 별도의 라이선스를 필요로 합니다.

프로시저

단계 **1** 시스템 ( ) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 또는 **Specific Licenses(**특정 라이선스**)**를 선택합니다.

단계 **2** **Edit Licenses(**라이선스 편집**)**을 클릭합니다.

단계 **3** 디바이스에 추가하려는 각 라이선스 유형:

a) 라이선스 유형에 대한 탭을 클릭합니다.

b) 왼쪽 목록에서 디바이스를 클릭합니다.

c) **Add(**추가**)**를 클릭하고 오른쪽 목록으로 해당 디바이스를 이동합니다.

d) 각 디바이스에 대해 이를 반복하고 라이선스 유형을 받습니다.

이제 추가하려는 모든 디바이스에 라이선스가 있는지에 대해서는 걱정하지 마십시오.

e) 추가하려는 라이선스 각 유형에 대해 라이선스의 각 유형에 대해 이 하위 절차를 반복합니다.

f) 라이선스를 제거하려면 디바이스 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

g) **Apply(**적용**)**를 클릭합니다.

다음에 수행할 작업

라이선스가 올바르게 설치되어 있는지 확인합니다. 스마트 라이선스 모니터링, 293 페이지에서 절차를 따릅니다.

스마트 라이선싱 관리

이 섹션에서는 스마트 라이선싱을 관리하는 방법을 설명합니다.

등록 취소Management Center

Smart Software Manager에서 management center의 등록을 취소하여 다른 디바이스에서 사용할 수 있도록 모든 라이선스 자격을 스마트 어카운트에 다시 릴리스합니다. 예를 들어 management center를 해제하거나 이미지를 재설치해야 하는 경우 등록을 취소합니다.

등록되지 않은 상태에서 라이선스를 시행하는 방법에 대한 자세한 내용은 등록 취소 상태, 264 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 시스템 ( ) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 선택합니다.

단계 **2** **Deregister(**등록 해제**)**( ) 버튼을 클릭합니다.

Management Center 동기화 또는 재인증

기본적으로 ID 인증서는 6개월마다 자동으로 갱신되며, 라이선스 엔타이틀먼트는 30일마다 갱신됩니다. 예를 들어 인터넷 액세스 기간이 제한된 경우 또는 Smart Software Manager에서 라이선싱을 변경한 경우, 이러한 항목 중 하나에 대한 등록을 수동으로 갱신할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**을(를) 선택합니다.

단계 **2** ID 인증서를 갱신하려면, 동기화( )를 클릭합니다.

단계 **3** 라이센스 엔타이틀먼트를 갱신하려면 **Re-Authorize(**재승인**)**를 클릭합니다.

스마트 라이선스 상태 모니터링

System(시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 페이지의 스마트 라이선스 상태**(Smart License Status)** 섹션은 아래 설명된 대로 management center의 라이선스 사용에 대한 개요를 보여줍니다.

사용 권한 부여

가능한 상태 값:

- **In-compliance(**인 컴플라이언스**)**( ) — 매니지드 디바이스에 할당된 모든 라이선스가 준수 상태이고 management center가 Smart Software Manager와 성공적으로 통신합니다.
- **License is in compliance but communication with licensing authority has failed(**라이선스는 준수 상태이지만 **licensing authority**와의 통신은 실패하였습니다**)**— 디바이스 라이선스는 준수 상태이지만 management center가 Cisco licensing authority와 통신할 수 없습니다.

- **Out-of-compliance icon or unable to communicate with License Authority(**미준수 아이콘 또는 **License Authority**와 통신 불가**)**—하나 이상의 매니지드 디바이스는 미준수 상태의 라이선스를 사용 중이거나 management center가 Smart Software Manager와 90일 이상 통신하지 못했습니다.

제품 등록

management center이 Smart Software Manager에 연결하고 등록한 마지막 날짜를 나타냅니다.

할당된 가상 어카운트

제품 인스턴스 등록 토큰을 생성하고 management center 등록을 등록하는 데 사용한 스마트 어카운트에 속한 가상 어카운트를 나타냅니다. 이 구축이 스마트 어카운트 내의 특정 가상 어카운트와 연결되지 않는 경우, 이 정보는 표시되지 않습니다.

내보내기 제어 기능

이 옵션을 활성화하는 경우, 제한된 기능을 배포할 수 있습니다. 자세한 내용은 내보내기 제어 기능 라이선싱, 271 페이지 섹션을 참조해 주십시오.

Cisco Success Network

management center에 대해 Cisco Success Network를 활성화했는지 여부를 나타냅니다. 이 옵션을 활성화하는 경우, 기술 지원에 필요한 사용 정보 및 통계가 Cisco에 제공됩니다. 또한, 이 정보를 통해 Cisco는 제품을 개선할 수 있으며 사용 가능하지만 사용되지 않은 기능을 알려 네트워크의 제품 가치를 최대화하도록 할 수 있습니다. 자세한 내용은 Cisco Success Network 등록 구성, 647 페이지를 참조하십시오.

스마트 라이선스 모니터링

management center 및 해당 매니지드 디바이스의 라이선스 상태를 확인하려면 Smart License(스마트 라이선스) 페이지를 사용합니다.

구축에서 라이선스의 각 유형에 대해 이 페이지는 사용된 라이선스 총 수, 라이선스 컴플라이언스 상태, 디바이스 유형, 디바이스가 구축된 도메인 및 그룹에 대한 목록을 보여줍니다. management center의 스마트 라이선스 상태도 볼 수 있습니다. 컨테이너 인스턴스는 동일한 보안 모듈/엔진에서 보안 모듈/엔진당 하나의 라이선스만 사용합니다. 따라서 management center에 각 라이선스 유형별 각 컨테이너 인스턴스 목록이 별도로 표시되지만, 기능 라이선스 유형에 대해 사용된 라이선스 수는 오직 1이 됩니다.

Smart Licenses(스마트 라이선스**)** 페이지 외에도, 라이선스를 볼 수 있는 몇 가지 다른 방법이 있습니다.

- **Product Licensing(**제품 라이선싱**)** 대시보드 위젯은 사용자 라이선스를 한눈에 볼 수 있는 개요를 제공합니다.

  대시보드에 위젯 추가, 362 페이지, 사용자 역할별 대시보드 위젯 가용성, 348 페이지 및 제품 라이선싱 위젯, 358 페이지를 참조하십시오.

- **Device Management(**디바이스 관리**)** 페이지(**Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**)에 각 매니지드 디바이스에 적용된 라이선스 목록이 표시됩니다.

- **Smart License Monitor(**스마트 라이선스 모니터**)** 상태 모듈이 상태 정책에서 사용되는 경우 라이선스 상태를 알려줍니다.

프로시저

단계 **1** 시스템 ( ) > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**를 선택합니다.

단계 **2** **Smart Licenses(**스마트 라이선스**)** 테이블에서 각 **License Type(**라이선스 유형**)** 폴더의 왼쪽에 있는 화살표를 클릭하고 해당 폴더를 확장합니다.

단계 **3** 각 폴더에서 각 디바이스의 **License Status(**라이선스 상태**)** 열에 **Check Mark(**확인 표시**)** ( )와 함께 녹색 원이 있는지 확인합니다.

참고 중복 management center virtual 라이선스가 표시되는 경우, 각각은 하나의 매니지드 디바이스를 나타냅니다.

모든 디바이스에 **Check Mark(**확인 표시**)** ( )와 함께 녹색 원이 있는 경우, 디바이스에 정상적으로 라이선스가 부여되고 사용할 준비가 된 것입니다.

녹색 원(**Check Mark(**확인 표시**)** ( )) 이외의 License Status(라이선스 상태)가 표시되는 경우, 해당 상태 아이콘 위에 마우스를 놓고 메시지를 확인합니다.

다음에 수행할 작업

- 녹색 원(**Check Mark(**확인 표시**)** ( ))이 없는 디바이스가 있는 경우, 라이선스를 추가로 구입해야 할 수도 있습니다.

스마트 라이선싱 트러블슈팅

예상했던 라이선스가 내 스마트 어카운트에 표시되지 않습니다

예상했던 라이선스가 스마트 어카운트에 없는 경우 다음을 시도하십시오.

- 해당 라이선스가 다른 가상 어카운트에 없는지 확인합니다. 조직의 라이선스 관리자가 이 문제 해결을 도와야 할 수도 있습니다.
- 라이선스 판매자에게 해당 어카운트로의 전송이 완료되었는지 확인합니다.

스마트 라이선스 서버에 연결할 수 없음

먼저 확실한 원인을 확인하십시오. 예를 들어, management center에 외부 연결이 있는지 확인합니다. 인터넷 액세스 요구 사항, 1096 페이지의 내용을 참조하십시오.

예상하지 않은 미준수 알림 또는 기타 오류

- 디바이스가 이미 다른 management center에 등록된 경우, 새 management center에서 디바이스에 라이선스를 부여하기 전에 원래 management center를 등록 취소해야 합니다. 등록 취소Management Center, 292 페이지을 참조하십시오.
- 구독 라이선스의 기간이 만료되었는지 확인합니다.

다른 문제 해결

다른 일반적인 문제에 대한 솔루션은 다음을 참조하십시오. https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215838-fmc-and-ftd-smart-license-registration-a.html

Threat Defense에서 사용할 클래식 라이선스 변환

라이선스 등록 포털 또는 Smart Software Manager를 사용하여 라이선스를 전환할 수 있으며, 디바이스에 이미 할당된 미사용 PAK(제품 인증 키) 또는 기본 라이선스를 전환할 수 있습니다.

참고 이 프로세스를 취소할 수 없습니다. 라이선스가 원래 기본 라이선스였더라도 스마트 라이선스를 기본 라이선스로 전환할 수 없습니다.

Cisco.com에 있는 문서에서 기본 라이선스는 "traditional(전통적)" 라이선스라도고 합니다.

시작하기 전에

- 기본 라이선스가 아직 제품 인스턴스에 할당되지 않은 미사용 PAK인 경우, 기본 라이선스를 스마트 라이선스로 전환하는 것은 어렵지 않습니다.
- 하드웨어가 threat defense를 실행할 수 있어야 합니다. *Cisco Firepower* 호환성 가이드 (https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html)를 참조하십시오.
- 스마트 어카운트가 있어야 합니다. 어카운트가 없는 경우 하나를 생성합니다. 스마트 어카운트 생성 및 라이선스 추가, 282 페이지의 내용을 참조하십시오.
- 변환하려는 PAK 또는 라이선스가 스마트 어카운트에 나타나야 합니다.
- Smart Software Manager 대신 라이선스 등록 포털을 사용하여 전환하는 경우, 스마트 어카운트 크리덴셜이 있어야 전환 프로세스를 개시할 수 있습니다.

프로시저

단계 **1** 수행할 전환 프로세스는 라이선스 사용 여부에 따라 달라집니다.

- 전환하려는 PAK가 미사용인 경우, PAK 전환에 대한 지침을 따르십시오.

- 전환하려는 PAK가 이미 디바이스에 할당된 경우, 기본 라이선스 전환에 대한 지침을 따르십시오.

  기존 기본 라이선스가 아직 디바이스에 등록되어 있는지 확인합니다.

단계 **2** 다음 문서에서 전환 유형(PAK 또는 설치된 기본 라이선스)에 대한 지침을 참조하십시오.

- 라이선스 등록 포털을 사용하여 PAK 또는 라이선스를 변환하는 경우:
  - 라이선스 등록 포털을 통한 전환 프로세스 단계에 대한 비디오를 보시려면 https://salesconnect.cisco.com/#/content-detail/7da52358-0fc1-4d85-8920-14a1b7721780를 클릭합니다.
  - 다음 https://cisco.app.box.com/s/mds3ab3fctk6pzonq5meukvcpjizt7wu 문서에서 "Convert(전환)"을 검색합니다.

    전환 절차는 세 가지가 있습니다. 상황에 맞는 전환 절차를 선택합니다.
  - 라이선스 등록 포털(https://tools.cisco.com/SWIFT/LicensingUI/Home)에 로그인하고 위 문서의 지침을 따르십시오.

- Smart Software Manager를 사용하여 PAK 또는 라이선스를 변환하려면 다음을 수행합니다.
  - 하이브리드 라이선스를 스마트 소프트웨어 라이선스 *QRG*로 전환:

    https://community.cisco.com/t5/licensing-enterprise-agreements/converting-hybrid-licenses-to-smart-software-licenses-qrg/ta-p/3628609?attachment-id=134907
  - Smart Software Manager(https://software.cisco.com/#SmartLicensing-LicenseConversion)에 로그인하고 위 다음 문서에 있는 전환 유형(PAK 또는 설치된 기본 라이선스)에 대한 지침을 따르십시오.

단계 **3** 하드웨어에 threat defense를 새로 설치합니다.

하드웨어에 대한 지침을 참조하십시오(https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html).

단계 **4** device manager을 사용하여 이 디바이스를 독립형 디바이스로 관리하려는 경우:

https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html의 device manager 구성 가이드에서 디바이스 라이선싱에 대한 정보를 참조하십시오.

이 절차의 나머지 부분을 건너뜁니다.

단계 **5** 이미 management center에 스마트 라이선싱을 구축한 경우:

a) 새 threat defense에서 스마트 라이선싱을 설정합니다.

여러 매니지드 디바이스에 라이선스 할당, 291 페이지의 내용을 참조하십시오.

b) 새 스마트 라이선스가 디바이스에 성공적으로 적용되었는지 확인합니다.

스마트 라이선스 모니터링, 293 페이지의 내용을 참조하십시오.

단계 **6** 아직 management center에 스마트 라이선싱을 구축하지 않은 경우:

Smart Licensing 구성, 283 페이지의 내용을 참조하십시오. (적용되지 않거나 이미 완료한 단계를 모두 건너뜁니다.)

SLR(Specific License Reservation) 구성

에어 갭 네트워크에서 스마트 라이선싱을 배포하는 특정 라이선스 예약 기능을 사용할 수 있습니다.

참고 Cisco에서는 SLR, SPLR, PLR, 영구 라이선스 예약을 비롯한 다양한 이름이 특정 라이선스 예약에 사용됩니다. 이러한 용어는 Cisco에서 유사한 라이선싱 모델을 지칭하는 데 사용할 수 있지만, 반드시 동일한 라이선싱 모델을 나타내지는 않습니다.

특정 라이선스 예약을 활성화하는 경우, management center는 Smart Software Manager 또는 Smart Software Satellite Server에 액세스하거나 Smart Software Manager 온프레미스을 사용하지 않고 가상 어카운트에서 라이선스를 지정된 기간 동안 예약합니다.

인터넷에 액세스해야 하는 기능(예: URL 조회 또는 공용 웹 사이트 상황별 크로스 실행)이 작동하지 않습니다.

Cisco는 특정 라이선스 예약을 사용하는 배포에 대한 웹 분석 또는 텔레메트리 분석 데이터를 수집하지 않습니다.

특정 라이센스 예약에 대한 요구 사항 및 사전 요건

- 현재 일반 스마트 라이선싱을 사용하는 경우, management center를 등록 취소하고 특정 라이선스 예약을 구현합니다. 자세한 내용은 등록 취소Management Center, 292 페이지 섹션을 참조해 주십시오.

  management center에 현재 배포된 모든 스마트 라이선스는 사용자 어카운트에서 사용 가능한 라이선스 풀로 반환되며, 특정 라이선스 예약을 구현하는 경우 다시 이를 사용할 수 있습니다.

- 특정 라이선스 예약은 일반 스마트 라이선싱과 동일한 라이선스 유형을 사용합니다.
- (권장 사항) 고가용성 구성으로 management center 쌍을 구축하는 경우 라이선스를 할당하기 전에 고가용성을 구성해야 합니다. 보조 management center의 디바이스에 이미 라이선스를 할당한 경우 할당을 취소해야 합니다.

스마트 어카운트가 특정 라이선스 예약을 구축할 준비가 되었는지 확인

특정 라이선스 예약을 배포할 때 문제를 방지하기 위해 management center를 변경하기 전에 이 절차를 완료합니다.

시작하기 전에

- 특정 라이센스 예약에 대한 요구 사항 및 사전 요건, 297 페이지에서 요건을 충족했는지 확인합니다.
- Smart Software Manager 크리덴셜을 갖추도록 합니다.

프로시저

단계 **1** Smart Software Manager에 로그인합니다.

https://software.cisco.com/#SmartLicensing-Inventory

단계 **2** 해당하는 경우 페이지 오른쪽 상단에서 올바른 계정을 선택합니다.

단계 **3** 필요한 경우 **Inventory(**재고**)**를 클릭합니다.

단계 **4** **Licenses(**라이선스**)**를 클릭합니다.

단계 **5** 다음을 확인합니다.

- **License Reservation(**라이선스 예약**)** 단추가 있습니다.
- 구축하려는 디바이스와 기능을 위한 플랫폼과 기능 라이선스가 충분합니다(예: 해당되는 경우 디바이스에 대한 management center virtual 엔타이틀먼트).

단계 **6** 이러한 항목 중 하나라도 누락되었거나 잘못된 경우, 어카운트 담당자에게 문의하고 문제를 해결합니다.

참고 문제를 해결할 때까지 이 과정을 계속 진행하지 마십시오.

특정 라이선싱 메뉴 옵션 활성화

이 절차는 management center의 "Smart Licenses(스마트 라이선스)" 메뉴 옵션을 "Specific Licenses(특정 라이선스)"로 변경합니다.

프로시저

단계 **1** USB 키보드와 VGA 모니터를 사용하여 management center 콘솔에 액세스하거나 SSH를 사용하여 관리 인터페이스에 액세스합니다.

단계 **2** management center CLI 관리자 계정에 로그인합니다.

단계 **3** **expert** 명령을 입력하여 Linux 셸에 액세스합니다.

단계 **4** 다음 명령을 실행하고 특정 라이선스 예약 옵션에 액세스합니다.

sudo manage_slr.pl

예제**:**

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

단계 **5** 옵션 **2**를 선택하고 Specific License Reservation(특정 라이선스 예약)을 활성화합니다.

단계 **6** 옵션 **0**을 선택하고 manage_slr 유틸리티를 종료합니다.

단계 **7** **exit**를 입력하고 Linux 셸을 종료합니다.

단계 **8** **exit**를 입력하여 명령줄 인터페이스를 종료합니다.

단계 **9** management center 웹 인터페이스의 **Specific License Reservation(**특정 라이선스 예약**)** 페이지에 액세스할 수 있는지 확인합니다.

- **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)**페이지가 현재 표시된 경우, 페이지를 새로 고칩니다.
- 아니면 **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.

특정 라이선스 예약 인증 코드를 **Management Center**에 입력

프로시저

단계 **1** 예약 요청 코드를 생성합니다.

a) management center에서 **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.

b) **Generate(**생성**)**를 클릭합니다.

c) **Reservation Request Code(**예약 요청 코드**)**를 메모합니다.

단계 **2** 예약 인증 코드를 생성합니다.

a) Cisco Smart Software Manager로 이동합니다.https://software.cisco.com/#SmartLicensing-Inventory

b) 필요한 경우 페이지 오른쪽 상단에서 올바른 계정을 선택합니다.

c) 필요한 경우 **Inventory(**재고**)**를 클릭합니다.

d) **Licenses(**라이선스**)**를 클릭합니다.

e) **License Reservation(**라이선스 예약**)**을 클릭합니다.

f) management center에서 생성한 코드를 **Reservation Request Code(**예약 요청 코드**)** 상자에 입력합니다.

g) **Next(**다음**)**를 클릭합니다.

h) **Reserve a specific license(**특정 라이선스 예약**)**를 선택합니다.

i) 아래로 스크롤하여 전체 라이선스 그리드를 표시합니다.

j) **Quantity To Reserve(**예약 수량**)**에 구축에 필요한 각 플랫폼 및 기능 라이선스의 수를 입력합니다.

참고

- 각 매니지드 디바이스 또는 다중 인스턴스 구축의 경우 각 컨테이너에 대한 Essentials 라이선스를 명시적으로 포함해야 합니다.
- management center virtual를 사용하는 경우, 각 컨테이너(다중 인스턴스 구축의 경우)이나 각 매니지드 디바이스(그 외 모든 구축의 경우)에 대한 자격을 포함해야 합니다.
- 강력한 암호화 기능을 사용하는 경우:
  - 내보내기 제어 기능에서 Smart Account(스마트 어카운트) 전체를 활성화하는 경우, 여기서 어떠한 작업도 수행할 필요가 없습니다.
  - 해당 조직의 자격이 management center에 따르는 경우, 적절한 라이선스를 선택해야 합니다.

  management center에 대한 정확한 라이선스 이름은 (전역 권한이 없는 어카운트의) 내보내기 제어 기능 활성화, 288 페이지에서 해당 사전 요구 사항을 참조하십시오.

k) **Next(**다음**)**를 클릭합니다.

l) **Generate Authorization Code(**인증 코드 생성를 클릭합니다.

이 시점에서는 Smart Software Manager에 따라 라이선스가 사용됩니다.

m) 인증 코드를 다운로드하고 management center에 입력할 준비를 합니다.

단계 **3** management center에 인증 코드를 입력합니다.

a) management center에서 **Browse(**찾아보기**)** 를 클릭하여 Smart Software Manager에서 생성한 인증 코드로 텍스트 파일을 업로드합니다.

b) **Install(**설치**)**을 클릭합니다.

c) **Specific License Reservation(**특정 라이선스 예약**)** 페이지에 **Usage Authorization(**사용 권한 부여**)** 상태가 authorized(권한 있음)로 표시되는지 확인합니다.

d)

단계 **4** **Reserved License(**예약된 라이선스**)** 탭을 클릭하고 선택된 라이선스를 확인하는 한편 **Authorization Code(**인증 코드**)**를 생성합니다.

필요한 라이선스가 표시되지 않는 경우, 필요한 라이선스를 추가합니다. 자세한 정보는 특정 라이선스 예약 업데이트를 참조하십시오.

매니지드 디바이스에 특정 라이선스 할당

이 절차를 사용하여 한 번에 여러 매니지드 디바이스에 라이선스를 신속하게 할당합니다.

또한 이 절차를 사용하여 라이선스를 비활성화하거나 디바이스 간에 라이선스를 이동시킬 수 있습니다. 디바이스에 대한 라이선스를 비활성화하는 경우, 해당 디바이스에서 그 라이선스와 관련된 기능을 사용할 수 없습니다.

프로시저

단계 **1** **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.

단계 **2** **Edit Licenses(**라이선스 편집**)**을 클릭합니다.

단계 **3** 각 탭을 클릭하고 필요에 따라 디바이스에 라이선스를 할당합니다.

단계 **4** **Apply(**적용**)**를 클릭합니다.

단계 **5** **Assigned Licenses(**할당된 라이선스**)** 탭을 클릭하고 각 디바이스에 라이선스가 올바르게 설치되어 있는지 확인합니다.

단계 **6** 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

특정 라이선스 예약 관리

이 섹션에서는 특정 라이선스 예약을 관리하는 방법을 설명합니다.

중요! 특정 라이선스 예약 구축 유지 관리

위협 데이터 및 소프트웨어를 업데이트하고 구축을 효과적으로 유지하려면 에어-갭(Air-Gapped) 구축 유지 관리, 246 페이지을 참조하십시오.

모든 기능이 중단 없이 계속 작동되도록 하려면 라이선스 만료 날짜를 모니터링합니다(**Reserved Licenses(**예약된 라이선스**)** 탭).

특정 라이선스 예약 업데이트

management center에 특정 라이선스를 성공적으로 구축한 경우, 이 절차를 사용하여 엔타이틀먼트를 언제든 추가 또는 제거할 수 있습니다.

라이선스가 만료된 후 라이선스를 갱신해야 하는 경우 이 절차를 사용합니다. 필요한 라이선스가 없는 경우 다음 작업이 제한됩니다.

- 디바이스 등록
- 정책 구축

프로시저

단계 **1** management center에서 management center의 고유한 제품 인스턴스 식별자를 가져옵니다.

a) **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.

b) **Product Instance(**제품 인스턴스**)** 값을 메모합니다.

이 프로세스가 진행되는 동안 이 값이 여러 번 필요합니다.

단계 **2** Smart Software Manager에서 업데이트할 management center를 식별합니다.

a) Smart Software Manager로 이동합니다.

https://software.cisco.com/#SmartLicensing-Inventory

b) 필요한 경우 **Inventory(**재고**)**를 클릭합니다.

c) **Product Instances(**제품 인스턴스**)**를 클릭합니다.

d) **Type(**유형**)** 열에 **FT**, **Name(**이름**)** 열에 일반 SKU(호스트네임 아님)로 되어 있는 제품 인스턴스를 찾습니다. 다른 테이블 열에 있는 값을 사용하여 어떤 management center가 올바른 management center인지 결정할 수 있습니다. 이름을 클릭합니다.

e) **UUID**를 보고 수정하려는 management center의 UUID인지 확인합니다.

그렇지 않으면 올바른 management center를 찾을 때까지 이러한 단계를 반복해야 합니다.

단계 **3** 올바른 management center를 Smart Software Manager에서 찾은 경우, 예약된 라이선스를 업데이트하고 새 인증 코드를 생성합니다.

a) 올바른 UUID를 나타내는 페이지에서 **Actions(**작업**)** > **Update Reserved Licenses(**예약된 라이선스 업데이트**)**를 선택합니다.

b) 필요에 따라 예약된 라이선스를 업데이트합니다.

참고

- 각 매니지드 디바이스 또는 다중 인스턴스 구축의 경우 각 컨테이너에 대한 Essentials 라이선스를 명시적으로 포함해야 합니다.
- management center virtual를 사용하는 경우, 각 컨테이너(다중 인스턴스 구축의 경우)이나 각 매니지드 디바이스(그 외 모든 구축의 경우)에 대한 자격을 포함해야 합니다.
- 강력한 암호화 기능을 사용하는 경우:
  - 내보내기 제어 기능에서 Smart Account(스마트 어카운트) 전체를 활성화하는 경우, 여기서 어떠한 작업도 수행할 필요가 없습니다.
  - 해당 조직의 자격이 management center에 따르는 경우, 적절한 라이선스를 선택해야 합니다.

  management center에 대한 정확한 라이선스 이름은 (전역 권한이 없는 어카운트의) 내보내기 제어 기능 활성화, 288 페이지에서 해당 사전 요구 사항을 참조하십시오.

c) **Next(**다음**)**를 클릭하고 상세정보를 확인합니다.

d) **Generate Authorization Code(**인증 코드 생성를 클릭합니다.
e) 인증 코드를 다운로드하고 management center에 입력할 준비를 합니다.
f) **Update Reservation(**예약 업데이트**)** 페이지를 열어 둡니다. 이 절차의 뒷부분에서 해당 페이지로 돌아갑니다.

단계 **4** management center에서 특정 라이선스를 업데이트합니다.

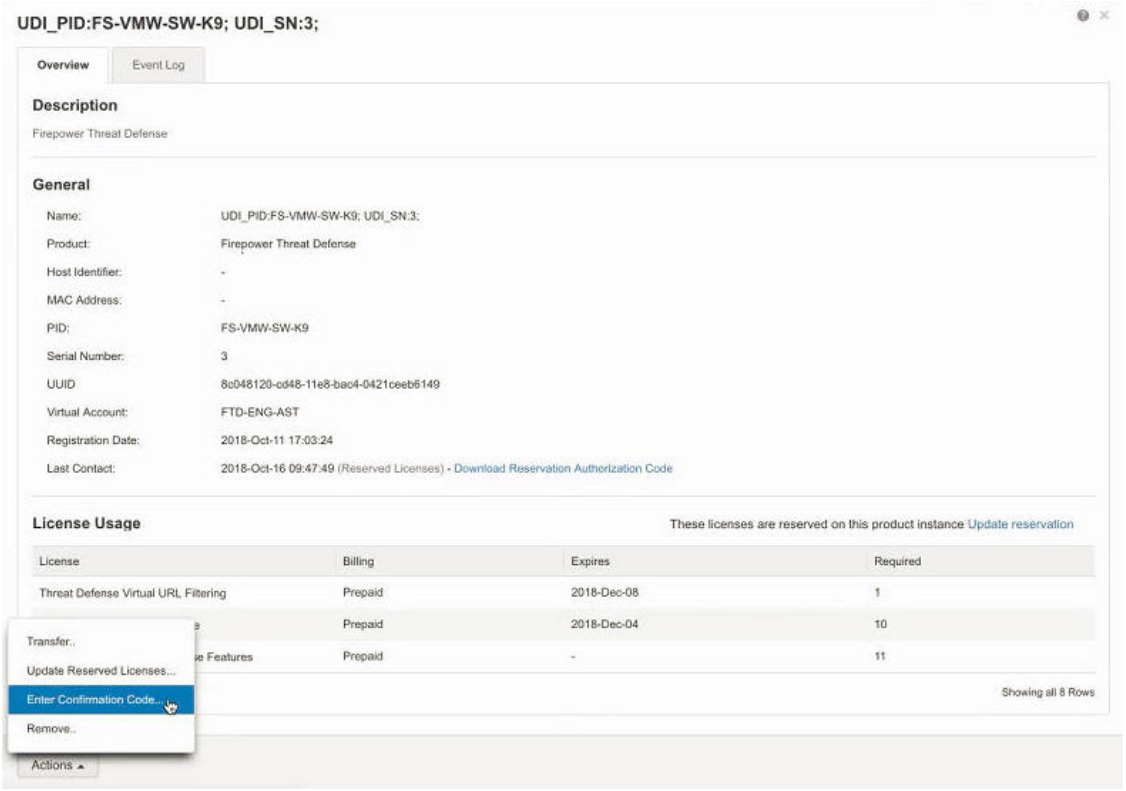
a) **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.
b) **Edit SLR(SLR** 편집**)**을 클릭합니다.
c) **Browse(**브라우저**)**를 클릭하고 새로 생성된 인증 코드를 업로드합니다.
d) **Install(**설치**)**을 클릭하고 라이선스를 업데이트합니다.

인증 코드가 성공적으로 설치된 경우, management center의 **Reserved**(예약된 라이선스) 열에 표시된 라이선스가 Smart Software Manager에 예약한 라이선스와 일치하는지 확인합니다.

e) **Confirmation Code(**인증 코드**)**를 메모합니다.

단계 **5** Smart Software Manager에서 인증 코드를 입력합니다.

a) 이 절차의 앞부분에서 열어 둔 Smart Software Manager 페이지를 돌아갑니다.
b) **Actions(**작업**)** >**Enter Confirmation Code(**인증 코드 입력**)**을 선택합니다.



c) management center에서 생성된 인증 코드를 입력합니다.

단계 **6** management center에서 라이선스가 예상대로 예약이 되었는지 그리고 각 매니지드 디바이스의 각 기능에 **Check Mark(**확인 표시**)** (✓)가 있는 녹색 원이 있는지 확인합니다.

필요한 경우, 자세한 내용은 특정 라이선스 예약 상태 모니터링, 306 페이지를 참조하십시오.

단계 **7** 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

특정 라이선스 예약 비활성화 및 반환

특정 라이선스가 더 이상 필요하지 않은 경우, 반드시 스마트 어카운트로 반환해야 합니다. 스마트 라이선싱 계정을 등록하려면 특정 라이선스 예약을 비활성화해야 합니다(아래 절차의 6단계).

중요 이 절차의 모든 단계를 수행하지 않는 경우, 라이선스는 사용 중 상태로 남게 되고 다시 사용할 수 없습니다.

이 절차는 management center와 연결되는 모든 라이선스 엔타이틀먼트를 가상 계정에 다시 릴리스합니다. 등록 취소 후에는 라이선스된 기능에 대한 업데이트나 변경은 허용되지 않습니다.

프로시저

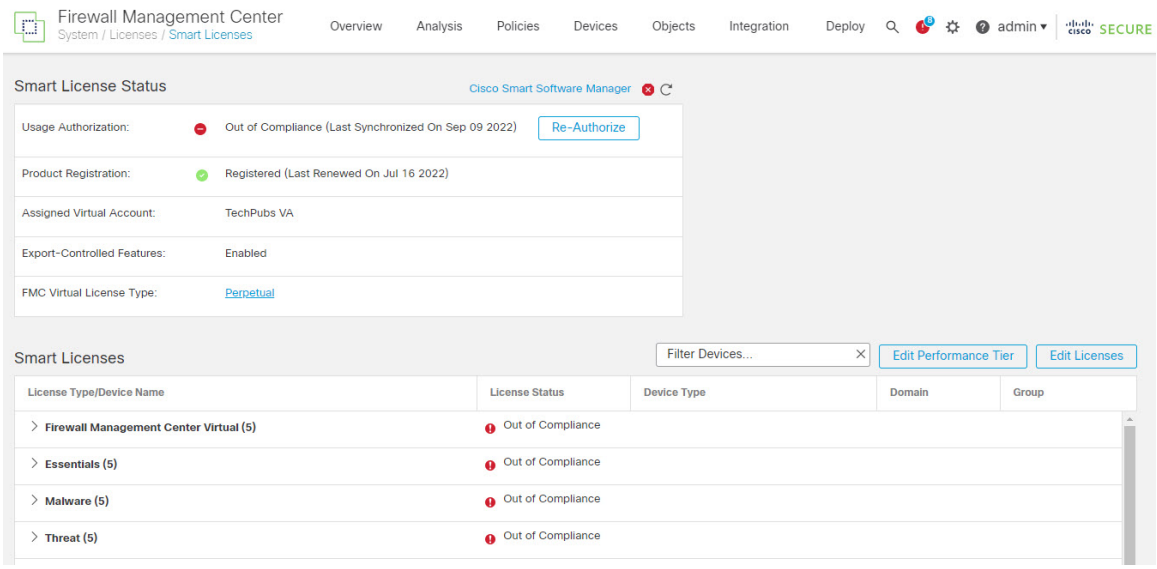
단계 **1** management center 웹 인터페이스에서 **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)**를 선택합니다.

단계 **2** management center에 대한 **Product Instance(**제품 인스턴스**)** 식별자를 메모합니다.

단계 **3** management center에서 반환 코드를 생성합니다.

a) **SLR(SLR**로 돌아가기**)**를 클릭합니다.

다음 그림에는 Return SLR(SLR 반환)이 나와 있습니다.



디바이스의 라이선스가 해제되고 management center은 등록 취소 상태로 전환됩니다.

b) **Return Code(**코드 반환**)**을 메모합니다.

단계 **4** Smart Software Manager에서 등록을 취소할 management center을 식별합니다.

a) Smart Software Manager로 이동합니다.

https://software.cisco.com/#SmartLicensing-Inventory

b) 필요한 경우 **Inventory(**재고**)**를 클릭합니다.

c) **Product Instances(**제품 인스턴스**)**를 클릭합니다.

d) **Type(**유형**)** 열에 **FT**, **Name(**이름**)** 열에 일반 SKU(호스트네임 아님)로 되어 있는 제품 인스턴스를 찾습니다. 다른 테이블 열에 있는 값을 사용하여 어떤 management center가 올바른 management center인지 결정할 수 있습니다. 이름을 클릭합니다.

e) **UUID**를 보고 수정하려는 management center의 UUID인지 확인합니다.

그렇지 않으면 올바른 management center를 찾을 때까지 이러한 단계를 반복해야 합니다.

단계 **5** 올바른 management center를 찾은 경우, 다음과 같이 스마트 어카운트에 라이선스를 반환합니다.

a) 올바른 UUID를 나타내는 페이지에서 **Actions(**작업**)** > **Remove(**제거**)**를 선택합니다.

b) management center에서 생성한 예약 반환 코드를 **Remove Product Instance(**제품 인스턴스 제거**)** 대화 상자에 입력합니다.

c) **Remove Product Instance(**제품 인스턴스 제거**)**를 클릭합니다.

특정 예약된 라이선스는 스마트 어카운트에서 사용 가능한 풀로 반환되고, 이 management center는 Smart Software Manager 제품 인스턴스 목록에서 제거됩니다.

단계 **6** management center Linux 셸에서 특정 라이선스 비활성화:

a) USB 키보드와 VGA 모니터를 사용하여 management center 콘솔에 액세스하거나 SSH를 사용하여 관리 인터페이스에 액세스합니다.

b) management center CLI 관리자 계정에 로그인합니다. 이렇게 하면 명령줄 인터페이스에 액세스할 수 있습니다.

c) **expert** 명령을 입력하여 Linux 셸에 액세스합니다.

d) 다음 명령을 실행합니다.

sudo manage_slr.pl

예제**:**

```
admin@fmc63betaslr: ~$ sudo manage_slr.pl
Password:


*************** Configuration Utility **************

1   Show SLR Status
2   Enable SLR
3   Disable SLR
0   Exit

************************************************************
Enter choice:
```

e) 특정 라이선스 예약을 비활성화 하려면 메뉴 옵션 **3**을 선택합니다.
f) 옵션 **0**을 선택하고 manage_slr 유틸리티를 종료합니다.
g) **exit**을(를) 입력하여 Linux 셸을 종료합니다.
h) **exit**를 입력하여 명령줄 인터페이스를 종료합니다.

특정 라이선스 예약 상태 모니터링

System(시스템) > **Licenses**(라이선스) > **Specific Licenses**(특정 라이선스) 페이지는 아래 설명된 대로 management center의 라이선스 사용에 대한 개요를 보여줍니다.

사용 권한 부여

가능한 상태 값:

- **Authorized**(권한 있음) — management center가 준수 상태이고, 어플라이언스에 대한 라이선스 엔타이틀먼트를 부여하는 License Authority에 정상적으로 등록됩니다.
- **Out-of-compliance**(미준수) — 라이선스가 만료되거나 management center가 예약되지 않은 라이선스를 과다하게 사용한 경우, 상태가 Out-of-Compliance(미준수)로 표시됩니다. 라이선스 엔타이틀먼트는 특정 라이선스 예약에 적용되므로 반드시 작업을 수행해야 합니다.

제품 등록

등록 상태 및 인증 코드가 management center에 마지막으로 설치되거나 갱신된 날짜를 나타냅니다.

내보내기 제어 기능

management center에 대해 내보내기 제어 기능을 활성화했는지 여부를 나타냅니다.

내보내기 제어 기능에 대한 자세한 내용은 내보내기 제어 기능 라이선싱, 271 페이지을 참조하십시오.

제품 인스턴스

management center의 UUID(Universally Unique Identifier). 이 값은 Smart Software Manager에서 디바이스를 식별합니다.

확인 코드

Confirmation Code(확인 코드)는 특정 라이선스를 업데이트 또는 비활성화하고 반환하는 경우 필요합니다.

Assigned Licenses(할당된 라이선스) 탭

각 디바이스에 할당된 라이선스와 각각의 상태를 표시합니다.

Reserved Licenses(예약된 라이선스) 탭

사용된 라이선스 및 할당이 가능한 라이선스의 수와 라이선스 만료 날짜를 표시합니다.

특정 라이선스 예약 문제 해결

Smart Software Manager의 제품 인스턴스 목록에서 특정 **management center** 항목을 식별하려면 어떻게 해야 합니까**?**

Smart Software Manager의 Product Instances(제품 인스턴스) 페이지에서 한 테이블 열의 값을 기반으로 제품 인스턴스를 식별할 수 없는 경우, **FP** 유형의 각 일반 제품 인스턴스의 이름을 클릭하고 제품 인스턴스 상세정보 페이지를 확인해야 합니다. 이 페이지의 **UUID** 값은 하나의 관리 센터를 고유하게 식별합니다.

management center 웹 인터페이스에서 Management Center의 UUID는 **System(**시스템**) > Licenses(**라이선스**) > Specific Licenses(**특정 라이선스**)** 페이지에 표시된 **Product Instance(**제품 인스턴스**)** 값입니다.

Smart Software Manager에서 **License Reservation(**라이선스 예약**)** 버튼이 보이지 않는 경우

License Reservation(라이선스 예약**)** 버튼이 표시되지 않으면 어카운트가 특정 라이선스 예약에 대해 인증되지 않은 것입니다. Linux 셸에서 이미 Specific License Reservation(특정 라이선스 예약)을 활성화하고 요청 코드를 생성했다면, 다음을 수행합니다.

1. 관리 센터 웹 인터페이스에서 이미 **Request Code(**요청 코드**)**를 생성한 요청 코드를 취소합니다.
2. 섹션 특정 라이선스 예약 비활성화 및 반환, 304 페이지의 설명에 따라 관리 센터 Linux 셸에서 Specific License Reservation(특정 라이선스 예약)을 비활성화합니다.
3. 스마트 토큰을 사용하여 일반 모드에서 Smart Software Manager에 관리 센터를 등록합니다.
4. Cisco TAC에 문의하고 스마트 어카운트에 대한 Specific License(특정 라이선스)를 활성화합니다.

라이선스 프로세스 중간에 중단된 경우 남은 부분을 어떻게 계속 진행할 수 있을까요**?**

Smart Software Manager에서 인증 코드를 생성은 했지만 아직 다운로드하지 않은 경우, Smart Software Manager에 있는 **Product Instance(**제품 인스턴스**)** 페이지로 이동하고 제품 인스턴스를 클릭한 후 **Download Reservation Authorization Code(**예약 인증 코드**)** 다운로드를 클릭합니다.

management center virtual에 디바이스를 등록할 수 없습니다**.**

스마트 어카운트에 등록하려는 디바이스에 대한 충분한 management center virtual 엔타이틀먼트가 있는지 확인한 후, 구축을 업데이트하여 필요한 엔타이틀먼트를 추가합니다.

특정 라이선스 예약 업데이트, 301 페이지의 내용을 참조하십시오.

Specific Licensing(특정 라이선싱**)**을 활성화했지만 **Smart License(**스마트 라이선스**)** 페이지가 보이지 않는 경우

이는 정상적인 동작입니다. Specific Licensing(특정 라이선싱)을 활성화하는 경우, Smart Licensing(스마트 라이선싱)이 비활성화됩니다. Specific License(특정 라이선스) 페이지를 사용하여 라이선싱 작업을 수행할 수 있습니다.

스마트 라이선싱을 사용하려는 경우, 특정 라이선스를 반환해야 합니다. 자세한 내용은 특정 라이선스 예약 비활성화 및 반환, 304 페이지를 참조하십시오.

management center virtual에서 **Specific License(**특정 라이선스**)** 페이지가 보이지 않는 경우

Specific License(특정 라이선스)를 활성화해야 Specific License(특정 라이선스) 페이지를 볼 수 있습니다. 자세한 내용은 특정 라이선싱 메뉴 옵션 활성화, 298 페이지를 참조하십시오.

Specific Licensing(특정 라이선싱**)**을 비활성화했지만 **Return Code(**반환 코드**)** 복사를 잊어버린 경우 어떻게 해야 합니까**?**

반환 코드는 management center virtual에 저장됩니다. Linux 셸에서 Specific License(특정 라이선스)를 다시 활성화하고(특정 라이선싱 메뉴 옵션 활성화, 298 페이지 참조), management center virtual 웹 인터페이스를 새로 고침해야 합니다. **Return Code(**반환 코드**)**가 표시됩니다.

레거시 Management Center PAK 기반 라이선스 구성

management center는 플랫폼 라이선스에 대해 스마트 라이선스 또는 레거시 PAK(제품 활성화 키) 라이선스를 지원합니다. 이 절차에서는 PAK 기반 라이선스를 적용하는 방법을 설명합니다.

시작하기 전에

- 라이선스를 구매할 때 Cisco가 제공한 소프트웨어 클레임 인증서에 PAK(제품 활성화 키)가 있는지 확인합니다. 레거시, Cisco 이전 라이선스가 있는 경우 지원팀에 문의합니다.

프로시저

단계 **1** 라이선스 키는 Smart Software Manager에서 management center를 고유하게 식별합니다. 관리 포트(eth0)의 MAC 주소와 제품 코드 (예를 들어, 66)의 구성 된는 management center; 예를 들어, 66:00:00:77:FF:CC:88 합니다.

a) 시스템 (⚙) > **Licenses(**라이선스**)** > **Classic Licenses(**기본 라이선스**)**를 선택합니다.
b) **Add New License(**새 라이선스 추가**)**를 클릭합니다.
c) **Add Feature License(**기능 라이선스 추가**)** 대화상자 상단에 있는 **License Key(**라이선스 키**)** 필드 값을 참조하십시오.

단계 **2** 시스템 (⚙) > **Licenses(**라이선스**)** > **Classic Licenses(**기본 라이선스**)**를 선택합니다.

단계 **3** **Add New License(**새 라이선스 추가**)**를 클릭합니다.

단계 **4** 해당하는 작업을 계속 진행합니다.

- 이미 라이선스 텍스트를 가져온 경우 8단계로 건너뜁니다.
- 여전히 라이선스 텍스트를 가져와야 한다면 다음 단계로 이동합니다

단계 **5** **Get License(**라이선스 가져오기**)**를 클릭하여 라이선스 등록 포털을 엽니다.

참고 현재 컴퓨터를 사용하여 인터넷에 액세스할 수 없는 경우, 액세스가 가능한 컴퓨터로 전환하고 http://cisco.com/go/license로 이동합니다.

단계 **6** 라이선스 등록 포털: https://cisco.com/go/license에서 PAK로 라이선스를 생성합니다.

이 단계에는 구매 과정에서 받은 PAK 뿐만 아니라 management center에 대한 라이선스 키도 필요합니다.

이 포털을 사용에 관한 자세한 내용은 다음을 참조하십시오.

https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart

이러한 링크에 액세스하려면 계정 자격 증명이 필요합니다.

단계 **7** 라이선스 등록 포털이나 라이선스 등록 포털에서 발송한 이메일에서 라이선스 텍스트를 복사합니다.

중요 포털 또는 이메일 메시지에 있는 라이선스 텍스트 블록에는 하나 이상의 라이선스가 포함될 수 있습니다. 각 라이선스는 BEGIN LICENSE 행과 END LICENSE 행으로 구분됩니다. 한 번에 라이선스 하나만 복사하고 붙이도록 합니다.

단계 **8** management center virtual 웹 인터페이스에서 **Add Feature License(**기능 라이선스 추가**)** 페이지로 돌아갑니다.

단계 **9** 라이선스 텍스트를 **License(**라이선스**)** 필드에 붙입니다.

단계 **10** **Verify License(**라이선스 확인**)**을 클릭합니다.

라이선스가 유효하지 않은 경우, 라이선스 텍스트를 제대로 복사했는지 확인합니다.

단계 **11** **Submit License(**라이선스 제출**)**을 클릭합니다.

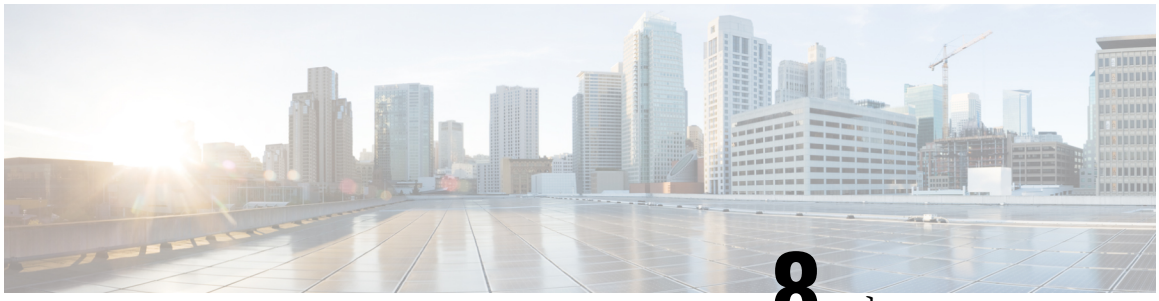
라이선싱 관련 추가 정보

일반 라이선싱 관련 질문 해결을 위한 자세한 내용은 다음 문서를 참조하시기 바랍니다.

- FAQ—https://www.cisco.com/c/en/us/td/docs/security/firepower/licensing/faq/firepower-license-FAQ.html
- 라이선스 로드맵 -https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html

라이센스 내역

기능	버전	세부정보
스마트 라이선싱 표준화	7.3	management center GUI에서 다음 라이선스 이름을 변경했습니다. • 기본은 이제 필수입니다 • 위협은 이제 IPS입니다. • 악성코드는 이제 악성코드 방어입니다 • RA VPN/AnyConnect 라이선스가 이제 Cisco Secure Client임 • AnyConnect Plus는 이제 Secure Client Advantage입니다 • AnyConnect Apex는 이제 Secure Client Premier입니다 • AnyConnect Apex 및 Plus는 이제 Secure Client Premier 및 Advantage입니다 • AnyConnect VPN Only는 이제 Secure Client VPN Only입니다
통신 사업자 라이선스 지원	7.3	통신 사업자 라이선스는 Diameter, GTP/GPRS, SCTP 및 M3UA 프로토콜의 검사를 활성화합니다. 신규/수정된 화면: **System(**시스템**)** > **Smart Licenses(**스마트 라이선스**)**
threat defense virtual의 성능 계층 라이선싱	7.0	성능 계층 라이센싱은 배포 요구 사항에 따라 다양한 처리량 레벨 및 VPN 연결 제한을 제공합니다. 라이선스 계층은 새 threat defense virtual 모델에 매핑됩니다.
Firepower 4100/9300의 threat defense에 대한 다중 인스턴스 기능 라이선스	6.3	이제 Firepower 4100/9300에서 다중 threat defense 컨테이너 인스턴스를 구축할 수 있습니다. 보안 모듈/엔진별 기능당 하나의 라이선스만 필요합니다. 기본 라이선스가 각 인스턴스에 자동으로 할당됩니다. 신규/수정된 화면: **System(**시스템**)** > **Licenses(**라이선스**)** > **Smart Licenses(**스마트 라이선스**)** 지원되는 플랫폼: Firepower 4100/9300에서의 threat defense
에어 갭(Air-Gapped) 구축을 위한 특정 라이선스 예약	6.3	Cisco License Authority와 통신하기 위해 인터넷에 연결할 수 없는 고객은 특정 라이선스 예약을 사용할 수 있습니다. 신규/수정된 화면: **System(**시스템**)** > **Licenses(**라이선스**)** > **Specific Licenses(**특정 라이선스**)** (이 옵션은 기본적으로 사용할 수 없습니다.) 지원되는 플랫폼: management center, threat defense
제한된 고객에 대한 내보내기 제어 기능	6.3	제한된 기능을 사용할 수 없는 스마트 어카운트를 보유한 특정 고객은 승인을 얻고 기간이 정해진 라이선스를 구매할 수 있습니다. 지원되는 플랫폼: management center, threat defense



8 장

고가용성

다음 주제에서는 Cisco Secure Firewall Management Center의 액티브/스탠바이 고가용성 구성 방법을 설명합니다.

Management Center 고가용성 정보

운영의 연속성을 보장하려면 고가용성 기능을 사용하여 디바이스 관리를 위한 이중 management center를 지정할 수 있습니다. management center는 하나의 어플라이언스가 액티브 유닛이며 디바이스를 관리하는 액티브/스탠바이 고가용성을 지원합니다. 스탠바이 유닛은 디바이스를 활동적으로 관리하지 않습니다. 액티브 유닛은 구성 데이터를 데이터 저장소로 기록하고 두 유닛 모두에 대해 데이터를 복제하며 필요한 경우 동기화를 사용하여 스탠바이 유닛과 정보를 공유합니다.

Active/Standby(액티브/스탠바이) 고가용성을 사용하면 보조 management center을 구성하고 장애가 발생한 경우 기본 management center의 기능을 대체합니다. 기본 management center에 장애가 발생하는 경우 보조 management center을 승격하여 액티브 유닛으로 만들 수 있습니다.

이벤트 데이터는 매니지드 디바이스에서 고가용성 쌍에 있는 management center 모두로 흐릅니다. 한 management center가 실패하면 다른 management center를 사용하여 중단 없이 네트워크를 모니터링할 수 있습니다.

참고로 고가용성 쌍으로 구성된 management center는 신뢰할 수 있는 동일한 관리 네트워크에 있어야 할 필요가 없으며 동일한 지리적 위치에 있어야 할 필요도 없습니다.

주의 시스템이 일부 기능을 액티브 management center로 제한하므로 해당 어플라이언스가 실패하면 스탠바이 management center를 액티브로 승격해야 합니다.

참고 변경 구축에 성공한 직후 management center에서 전환을 트리거하면 새 액티브 management center에서 미리보기 구성이 작동하지 않을 수 있습니다. 이는 정책 구축 기능에 영향을 주지 않습니다. 필요한 동기화가 완료된 후 management center에서 전환을 트리거하는 것이 좋습니다.

마찬가지로,management center HA 동기화 상태가 저하된 상태에서 전환을 트리거하거나 역할을 변경하면 management centerHA가 데이터베이스를 손상시키고 심각한 상황을 초래할 수 있습니다. 이 문제를 해결하기 위해 추가 지원이 필요하면 Cisco TAC(Technical Assistance Center)에 즉시 문의하는 것이 좋습니다.

이 HA 동기화는 여러 가지 이유로 성능이 저하된 상태로 끝날 수 있습니다. 이 장의 고가용성 쌍의 Management Center 교체, 328 페이지 섹션에서는 일부 실패 시나리오와 문제를 해결하는 후속 절차를 다룹니다. 성능 저하의 이유 또는 시나리오가 설명된 시나리오와 일치하는 경우 다음 단계에 따라 문제를 해결합니다. 다른 작업은 TAC에 문의하는 것이 좋습니다.

원격 액세스 VPN 고가용성에 대한 정보

기본 디바이스에 Remote Access(원격 액세스) VPN 구성과 CertEnrollment 개체로 등록한 ID 인증서가 있는 경우, 보조 디바이스에 동일한 CertEnrollment 개체로 등록한 ID 인증서가 있어야 합니다. CertEnrollment 개체는 디바이스별 재정의로 인해 기본 및 보조 디바이스에 대해 서로 다른 값을 가질 수 있습니다. 고가용성 형성 하기 전에 두 개의 디바이스를 등록 하는 동일한 CertEnrollment 개체에만 개로 제한이 됩니다.

Management Center 고가용성에서의 SNMP 동작

SNMP 구성 HA 쌍에서 알림 정책을 구축하면 기본 management center가 SNMP 트랩을 전송합니다. 기본 management center에 오류가 발생하면 액티브 유닛이 되는 보조 management center는 추가 구성 없이 SNMP 트랩을 전송합니다.

Firepower Management Center 고가용성의 역할 및 상태 비교

기본/보조 역할

Secure Firewall Management Center의 고가용성 쌍을 설정할 때 한 Secure Firewall Management Center를 기본, 다른 하나를 보조로 구성합니다. 컨피그레이션 중에는 기본 유닛의 정책이 보조 유닛에 동기화됩니다. 동기화가 끝나면 기본 Secure Firewall Management Center은 액티브 피어가 되고 보조 Secure Firewall Management Center는 보조 피어로 두 유닛이 매니지드 디바이스 및 정책 설정에 단일 어플라이언스로 작동합니다.

액티브/스탠바이 상태

고가용성 쌍에서 두 Secure Firewall Management Center의 가장 큰 차이는 액티브 및 스탠바이 피어와 관련이 있습니다. 액티브 Secure Firewall Management Center는 모든 기능을 사용할 수 있으며 디바이스와 정책을 관리할 수 있습니다. 스탠바이 Secure Firewall Management Center는 기능이 숨겨져 있으며 설정 변경을 할 수 없습니다.

Management Center 고가용성 쌍의 이벤트 처리

고가용성 쌍의 두 management center가 관리된 디바이스에서 이벤트를 수신하므로 어플라이언스용 관리 IP 주소를 공유하지 않습니다. 즉 management center 중 하나에 오류가 발생하는 경우 이벤트를 지속적으로 처리하기 위해 개입할 필요가 없습니다.

AMP 클라우드 연결 및 악성코드 정보

이들은 파일 정책 및 관련 컨피그레이션을 공유하지만 고가용성 쌍의 management center과 Cisco AMP Cloud 연결과 악성코드 성향을 공유하지 않습니다. 운영 연속성을 보장하고 탐지된 파일의 악성코드 속성이 두 management center및 기본과 보조 management center에 동일하려면 AMP 클라우드에 대한 액세스 권한이 있어야 합니다.

URL 필터링 및 보안 인텔리전스

URL 필터링과 보안 인텔리전스의 설정 및 정보는 고가용성 구축에서 Secure Firewall Management Center 간에 동기화됩니다. 그러나 기본 Secure Firewall Management Center만 URL 카테고리 및 평판 데이터 그리고 보안 인텔리전스 피드에 대한 업데이트를 다운로드합니다.

기본 Secure Firewall Management Center에 장애가 발생하면 위협 인텔리전스 데이터 업데이트를 위해 보조 Secure Firewall Management Center가 인터넷에 액세스할 수 있는지 확인하고 보조 Secure Firewall Management Center의 웹 인터페이스를 사용해 액티브로 전환합니다.

Management Center 페일오버 중에 사용자 데이터 처리

기본 management center 에 장애가 발생하면 보조 management center 가 TS Agent ID 소스 소스 에서 관리되는 디바이스 사용자 - IP 매핑을 전파하고, ISE / ISE-PIC ID 소스에서 SGT 매핑을 전파합니다. ID 소스로 아직 확인되지 않은 사용자는 알 수 없음으로 식별됩니다.

다운타임이 끝나면 ID 정책의 규칙에 따라 알 수 없는 사용자가 다시 식별되고 처리됩니다.

Management Center 고가용성 쌍에서 구성 관리

고가용성 구축에서 액티브 management center만 디바이스를 관리하고 정책을 적용할 수 있습니다. 두 management center 모두 지속적인 동기화 상태를 유지합니다.

액티브 management center에 오류가 발생하는 경우 고가용성 쌍은 사용자가 수동으로 스탠바이 어플라이언스를 액티브 상태로 승격할 때까지 저하 상태에 돌입합니다. 승격이 완료되면 어플라이언스는 유지 관리 모드 상태가 됩니다.

Management Center 고가용성 재해 복구

재해 복구 상황에서는 수동 전환을 수행해야 합니다. 기본 management center - FMC1에 오류가 발생하면 보조 management center인 FMC2의 웹 인터페이스에서 액세스하여 피어를 교체합니다. 이는 보조(FMC2)에 장애가 발생하는 경우에도 반대로 적용됩니다. 자세한 내용은 Management Center 고가용성 쌍에서 피어 전환, 325 페이지를 참고하십시오.

실패한 management center 복원에 대해서는 고가용성 쌍의 Management Center 교체, 328 페이지의 내용을 참조하십시오.

SSO 및 고가용성 쌍

Management Center고가용성 설정의 FMC는 SSO(Single Sign-On, 단일 인증)를 지원할 수 있지만, 다음 사항을 고려해야 합니다.

- SSO 설정은 고가용성 쌍의 멤버 간에 동기화되지 않습니다. 쌍의 각 멤버에서 SSO를 별도로 설정해야 합니다.
- 고가용성 쌍의 두 management center는 모두 SSO에 동일한 ID 공급자(IdP)를 사용해야 합니다. SSO에 대해 설정된 각 management center의 IdP에서 서비스 제공자 애플리케이션을 설정해야 합니다.
- 둘 다 SSO를 지원하도록 설정된 management center 고가용성 쌍에서는 사용자가 SSO를 사용하여 보조 management center에 처음으로 액세스하기 전에 먼저 사용자가 SSO를 통해 기본 management center에 한 번 이상 로그인해야합니다.
- 고가용성 쌍에서 management center에 대해 SSO를 설정하는 경우:
  - 기본 management center에서 SSO를 설정하는 경우, 보조 management center에서 SSO를 설정할 필요가 없습니다.
  - 보조 management center에서 SSO를 설정하는 경우, 기본 management center에서도 SSO를 설정해야 합니다. (SSO 사용자는 보조 management center에 로그인하기 전에 기본 management center에 한 번 이상 로그인해야 하기 때문입니다.)

관련 항목

SAML SSO(Single Sign-On) 구성, 145 페이지

Management Center 백업 중에 고가용성 동작

management center 고가용성 쌍에서 백업을 수행할 경우 백업 작업은 피어 간 동기화를 일시 중지합니다. 이 작업을 수행하는 동안 액티브 management center을 계속 사용할 수 있지만 스탠바이 피어는 사용할 수 없습니다.

백업이 완료되면 동기화가 재시작되어 액티브 피어의 프로세스를 일시적으로 비활성화합니다. 이 일시 중지 상태에 고가용성 페이지는 모든 프로세스가 다시 시작될 때까지 일시적으로 보류 페이지를 표시합니다.

Management Center 고가용성 스플릿 브레인

고가용성 쌍에서 액티브 management center이 중단(전원 문제, 네트워크/연결 문제)되는 경우 스탠바이 management center를 액티브 상태로 승격시킵니다. 원래 액티브 피어가 복구되면 두 피어 모두 액티브 상태로 간주할 수 있습니다. 이 상태를 '스플릿 브레인' 상태라고 합니다. 이러한 상황이 발생하면 시스템은 액티브 어플라이언스를 선택하고 다른 어플라이언스를 스탠바이로 전환하도록 합니다.

액티브 management center이 중단(또는 네트워크 오류로 연결 끊기)되는 경우 고가용성 또는 스위치 역할을 중단할 수 있습니다. 스탠바이 management center는 성능 저하 상태에 진입합니다.

참고 스플릿 브레인을 해결하면 보조로 사용하는 어플라이언스의 모든 디바이스 등록 및 정책 설정이 손실됩니다. 예를 들어 보조에 존재하던 정책 수정 내용을 전부 잃지만 기본에 있던 것은 보존됩니다. management center이 두 어플라이언스가 액티브 상태인 고가용성 스플릿 브레인 시나리오에 돌입하고 스플릿 브레인을 해소하기 전에 관리되는 디바이스를 등록하고 정책을 구축하는 경우 모든 정책을 내보내고 관리되는 디바이스를 새 고가용성이 재구성되기 전에 해당 스탠바이 management center에서 등록 해제해야 합니다. 그런 다음 액티브 management center에서 관리되는 디바이스를 등록하고 정책을 가져올 수 있습니다.

고가용성 쌍에서 Management Center 업그레이드

Cisco는 온라인으로 다양한 유형의 업데이트를 주기적으로 배포합니다. 시스템 소프트웨어의 주요 및 사소한 업그레이트를 포함합니다. 고가용성 설정에서 management center에 이런 업데이트를 설치해야 할 수 있습니다.

경고! 업그레이드 중 하나 이상의 운영 management center이 있는지 확인하십시오.

시작하기 전에

업그레이드와 함께 배포된 릴리스 노트 또는 권고 사항을 읽습니다. 릴리스 정보에는 지원되는 플랫폼, 호환성, 전제 조건, 경고, 특정 설치 및 제거 지침과 같은 중요 정보가 제공됩니다.

프로시저

단계 **1** 액티브 management center의 웹 인터페이스에 액세스하고 데이터 동기화를 중단시키려면 쌍을 이룬 Management Center 간에 통신 일시 중지, 326 페이지를 참조하십시오.

단계 **2** 스탠바이 management center을 업그레이드합니다.
업그레이드가 완료되면 스탠바이 유닛이 액티브상태가 됩니다. 두 피어가 액티브인 경우 고가용성 쌍은 저하(스플릿 브레인) 상태가 됩니다.

단계 **3** 다른 management center을 업그레이드합니다.

단계 **4** 어떤 management center을 스탠바이로 사용할지 결정합니다. 동기화가 중지된 뒤 스탠바이에 추가된 모든 추가 장치 또는 정책은 액티브 management center에 동기화되지 않습니다. 이러한 추가 디바이스만 등록을 취소하고 유지하려는 설정을 내보냅니다.

새 액티브 management center을 선택한 경우 보조로 지정한 management center는 디바이스 등록 및 동기화되지 않은 정책 설정 구축을 잃게 됩니다.

단계 **5** 정책 및 디바이스의 최신 요구 설정이 있는 새 액티브 management center을 선택하여 스플릿 브레인을 해결합니다.

Management Center 고가용성 문제 해결

이 섹션에서는 management center 고가용성 운영 오류에 대한 일반적인 정보를 설명합니다.

오류	설명	해결책
스탠바이에 로그인하려면 먼저 활성 management center에서 비밀번호를 재설정해야 합니다.	계정에 강제 비밀번호 재설정이 활성화된 상태에서 대기 management center에 로그인하려 했습니다.	데이터베이스가 대기 management center에 대해 읽기 전용이므로, 액티브 management center의 로그인 페이지에서 비밀번호를 재설정해야 합니다.
500 내부	피어 역할 전환이나 동기화 중지 또는 재개 등 중요한 management center 고가용성 작업을 수행하는 동안 웹 인터페이스 접속을 시도할 때 표시될 수 있습니다.	작업이 완료되기를 기다린 뒤 웹 인터페이스를 사용합니다.

오류	설명	해결책
시스템 프로세스가 시작 중이니 기다려 주시기 바랍니다. 웹 인터페이스가 응답하지 않을 수 있습니다.	이는 고가용성 또는 데이터 동기화 중 management center이 재부팅될 때(수동 또는 전원 복구 중) 표시될 수 있습니다.	1. management center 셸에 액세스하여 `manage_hadc.pl` 명령을 사용해 management center 고가용성 구성 유틸리티에 액세스합니다. 참고 `sudo`를 사용하여 루트 사용자로 우틸리트를 실행합니다. 2. 옵션 5를 사용하여 미러링 작업을 일시 중지합니다. management center 웹 인터페이스를 재로딩합니다. 3. 웹 인터페이스를 사용하여 동기화를 다시 시작합니다. **Integration(**통합**)** > **Other Integrations(**기타 통합**)**를 선택한 다음, **High Availability(**고가용성**)** 탭을 클릭하고 **Resume Synchronization(**재시작 동기화**)**을 선택합니다.
디바이스 등록 상태:호스트 <*string*> 연결할 수 없음	threat defense의 초기 구성 중에 management center IP 주소 및 NAT ID가 지정된 경우 **Host(**호스트**)** 필드를 비워 둘 수 있습니다. 그러나 NAT 뒤에 management center가 모두 있는 HA 환경에서는 보조 management center에 threat defense를 추가하면 이 오류가 발생합니다.	1. 기본 management center에서 threat defense을 삭제합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 Management Center에서 디바이스 삭제를 참조하십시오. 2. **configure manager delete** 명령을 사용하여 threat defense에서 관리자를 제거합니다. Cisco Secure Firewall Threat Defense 명령 참조을 참조하십시오. 3. **Host(**호스트**)** 필드에 threat defense 디바이스의 IP 주소와 함께 management center에 threat defense를 추가합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 Management Center에 디바이스 추가를 참조하십시오.

Firepower Management Center 고가용성을 위한 요구 사항

모델 지원

하드웨어 요구 사항, 318 페이지의 내용을 참조하십시오.

가상 모델 지원

가상 플랫폼 요건, 318 페이지의 내용을 참조하십시오.

지원되는 도메인

글로벌

사용자 역할

관리자

하드웨어 요구 사항

- 모든 management center 하드웨어는 고가용성을 지원합니다. 피어는 동일한 모델이어야 합니다.
- 피어는 서로 다른 데이터 센터에서 물리적 및 지리적으로 분리되어 있을 수 있습니다.
- 고가용성 구성에 대한 대역폭 요구 사항은 네트워크 크기, 매니지드 디바이스 수, 이벤트와 로그 양, 구성 업데이트 크기 및 빈도 등의 다양한 요인에 따라 달라집니다. 일반적인 management center 고가용성 구축의 경우에는 피어 간 최소 5Mbps 네트워크 대역폭이 권장됩니다.
- 기본 피어의 백업을 보조 피어로 복원하지 마십시오.
- Management Center 고가용성 설정에 대한 라이선스 요구 사항, 319 페이지도 참조하십시오.

가상 플랫폼 요건

두 개의 management center virtual 어플라이언스를 사용하여 고가용성(HA)을 설정하기 위한 요구 사항:

- VMware, AWS, OCI, Azure, KVM, HyperFlex에 대해서만 management center virtual에서 지원됩니다.
- management center virtual 10, 25 및 300에서 지원됩니다. management center virtual 2에서는 지원되지 않습니다.
- 고가용성 쌍의 디바이스 관리 용량은 동일해야 합니다. 예를 들어, management center virtual 25를 management center virtual 300과 페어링할 수 없습니다.
- threat defense 디바이스를 관리하려면 management center virtual 라이선스가 동일한 인스턴스 2개와 각 매니지드 디바이스에 대한 threat defense 엔타이틀먼트가 필요합니다. 버전 7.0 이하 클래

식 디바이스만 관리하는 경우에는 management center virtual 엔타이틀먼트가 필요하지 않습니다. 자세한 내용은 Management Center 고가용성 설정에 대한 라이선스 요구 사항, 319 페이지를 참고하십시오.

소프트웨어 요구 사항

소프트웨어 버전, 침입 규칙 업데이트 버전, 취약성 데이터베이스 업데이트를 확인하려면 어플라이언스 정보 위젯에 액세스합니다. 이 위젯은 기본적으로 **Detailed Dashboard(**상세 대시보드**)** 및 **Summary Dashboard(**요약 대시보드**)**의 **Status(**상태**)** 탭에 나타납니다. 자세한 내용은 어플라이언스 정보 위젯, 349 페이지을 참조해 주십시오.

- 고가용성 구성의 두 management center는 주(첫 번째 번호), 부(두 번째 번호), 유지 보수(세 번째 번호) 소프트웨어 버전이 동일해야 합니다.
- 고가용성 구성의 두 management center에는 동일한 침입 규칙 업데이트가 설치되어 있어야 합니다.
- 고가용성 구성의 두 management center에는 동일한 취약성 데이터베이스 업데이트가 설치되어 있어야 합니다.
- 고가용성 구성의 두 management center에는 동일한 버전의 LSP(Lightweight Security Package)가 설치되어 있어야 합니다.

경고! 두 management center의 소프트웨어 버전, 침입 규칙 업데이트 버전, 취약성 데이터베이스 업데이트 버전이 동일하지 않은 경우 고가용성을 설정할 수 없습니다.

Management Center 고가용성 설정에 대한 라이선스 요구 사항

각 디바이스에는 단일 management center 또는 고가용성 쌍(하드웨어 또는 가상)의 management center로 관리되는 동일한 라이선스가 필요합니다.

예: management center 쌍으로 관리되는 두 디바이스에 대해 고급 악성코드 보호를 활성화하고 싶은 경우, 2개의 악성코드 방어 라이선스와 TM 서브스크립션을 구매하고 액티브 management center을 Smart Software Manager에 등록한 뒤 두 기기의 라이선스를 액티브 management center에 할당합니다.

액티브 management center만 Smart Software Manager에 등록됩니다. 페일오버가 발생하면 시스템은 Smart Software Manager와 통신하여 원래 활성 management center에서 라이선스 등록을 해제하고 새로운 액티브 management center에 할당합니다.

특정 라이선스 예약 구축에서는 기본 management center에서만 특정 라이선스 예약이 요구됩니다.

하드웨어 **Management Center**

고가용성 쌍의 하드웨어 management center에 필요한 특별한 라이선스는 없습니다.

Management Center Virtual

라이선스가 동일한 두 개의 management center virtual가 필요합니다.

예: 10개의 디바이스를 관리하는 management center virtual 고가용성 쌍의 경우 다음을 사용할 수 있습니다.

- management center virtual 10 엔타이틀먼트 2개
- 디바이스 라이선스 10개

고가용성 쌍을 분리하면 보조 management center virtual와 연결된 management center virtual 엔타이틀먼트가 해제됩니다. (이 예에서는 독립형 management center virtual 10이 2개 있습니다.)

Management Center 고가용성의 전제조건

management center 고가용성 쌍을 설정하기 전에:

- 해당 보조 management center에서 해당 기본 management center에서 필요한 정책 내보내기 자세한 내용은 구성 내보내기, 526 페이지를 참고하십시오.
- 해당 보조 management center에 추가 장치가 부착되어 있지 않은지 확인하십시오. 해당 보조 management center에서 디바이스를 삭제하고 해당 기본 management center에 디바이스를 등록합니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Management Center*에서 디바이스 삭제 및 *Management Center*에 디바이스 추가를 참조하십시오.
- 해당 기본 management center에 정책을 가져옵니다. 자세한 내용은 구성 가져오기, 526 페이지를 참고하십시오.
- 해당 기본 management center에서 가져온 정책을 확인하고, 필요한 경우 편집하고, 적절한 장치에 구축합니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 구성 변경 사항 구축을 참조하십시오.
- 해당 기본 management center에 새로 추가된 디바이스에 적절한 라이선스를 연결합니다. 자세한 내용은 단일 디바이스에 라이선스 할당, 290 페이지를 참조하십시오.

이제 고가용성 설정을 위한 진행이 가능합니다. 자세한 내용은 Management Center 고가용성 설정, 320 페이지를 참고하십시오.

Management Center 고가용성 설정

고가용성 설정에는 피어 간 대역폭 및 정책 수에 따라 최대 몇 시간까지 상당한 시간이 걸릴 수 있습니다. 또한 스탠바이 management center에 동기화되어야 하는 액티브 management center에 등록된 디바이스 수에 따라 다릅니다. 고가용성 피어의 상태를 확인하기 위해 고가용성 페이지를 볼 수 있습니다.

시작하기 전에

- 모든 management center이 고가용성 시스템 요구 사항을 준수하는지 확인하십시오. 자세한 내용은 Firepower Management Center 고가용성을 위한 요구 사항, 318 페이지를 참조하십시오.
- 고가용성을 설정하기 위한 사전 요건을 완료하였는지 확인합니다. 자세한 내용은 Management Center 고가용성의 전제조건, 320 페이지를 참고하십시오.

프로시저

단계 **1** 보조로 지정하려는 management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 이 management center의 역할에서 보조를 선택합니다.

단계 **5** 기본 **Firepower Managememt Center** 호스트 텍스트 상자에서 기본 management center의 호스트 이름 또는 IP 주소를 입력합니다.

기본 management center에 피어 management center(공용 또는 프라이빗 IP 주소일 수 있음)에서 연결할 수 있는 IP 주소가 없는 경우에는 비워 둘 수 있습니다. 이 경우 등록 키와 고유 **NAT ID** 필드를 모두 사용하십시오. HA 연결을 활성화하려면 하나 이상의 management center에 대한 IP 주소를 지정해야 합니다.

단계 **6** 등록 키 텍스트 상자에서 일회용 등록 키를 입력합니다.

등록 키는 최대 37자의 사용자가 정의한 영숫자 값입니다. 이 등록 키는 보조 및 기본 management center을 등록할 때 사용합니다.

단계 **7** 기본 IP 주소를 지정하지 않거나 기본 management center에서 보조 IP 주소를 지정하지 않을 경우 고유 **NAT ID** 필드에서 고유의 영숫자 ID를 입력합니다. 자세한 내용은 NAT 환경, 79 페이지를 참조하십시오.

단계 **8** **Register(**등록**)**를 클릭합니다.

단계 **9** Admin 액세스 권한이 있는 계정을 사용하여 기본으로 지정할 management center에 로그인합니다.

단계 **10** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**을 선택합니다.

단계 **11** 고가용성을 선택합니다.

단계 **12** 이 management center의 역할에서 기본을 선택합니다.

단계 **13** 보조 **Firepower Managememt Center** 호스트 텍스트 상자에서 보조 management center의 호스트 이름 또는 IP 주소를 입력합니다.

보조 management center에 피어 management center(공용 또는 프라이빗 IP 주소일 수 있음)에서 연결 가능한 IP 주소가 없는 경우에는 비워 둘 수 있습니다. 이 경우 등록 키와 고유 **NAT ID** 필드를 모두 사용하십시오. HA 연결을 활성화하려면 하나 이상의 management center에 대한 IP 주소를 지정해야 합니다.

단계 **14** 6단계에서 사용한 것과 동일한 1회용 등록 키를 등록 키 텍스트 상자에 입력합니다.

단계 **15** 필요한 경우 고유 **NAT ID** 텍스트 상자에 7단계에서 사용한 것과 동일한 NAT ID를 입력합니다.

단계 **16** **Register(**등록**)**를 클릭합니다.

다음에 수행할 작업

management center 고가용성 쌍을 설정한 후 액티브 management center에 등록된 디바이스는 자동으로 스탠바이 management center에 등록됩니다.

참고 등록된 디바이스에 NAT IP 주소가 있는 경우 자동 디바이스 등록이 실패하고 보조 management center의 고가용성 페이지가 디바이스를 로컬, 보류중으로 표시합니다. 스탠바이 management center 고가용성 페이즈에 표시된 디바이스에 다른 NAT IP 주소를 할당할 수 있습니다. 자동 등록이 스탠바이 management center에 실패하지만 디바이스가 액티브 Firepower Management Center에 등록된 것으로 표시되는 경우 Management Center 고가용성에서 CLI를 사용하여 디바이스 등록 확인, 325 페이지를 참조합니다.

Management Center 고가용성 상태 보기

액티브 및 스탠바이 management center을 확인한 후 로컬 management center와 해당 피어에 대한 정보를 볼 수 있습니다.

참고 이때 로컬 피어는 시스템 상태를 확인하는 어플라이언스를 가리킵니다. 원격 피어는 액티브 또는 스탠바이 상태에 관계없이 다른 어플라이언스를 가리킵니다.

프로시저

단계 **1** 고가용성을 사용해 페어링된 management center 중 하나에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

다음을 볼 수 있습니다.

요약 정보

- 고가용성 쌍의 상태 스탠바이 유닛이 액티브 유닛에서 구성 변경 사항을 수신하면 올바르게 작동하는 시스템의 상태가 "정상"과 "동기화 작업이 진행 중입니다."로 표시됩니다.
- 고가용성 쌍의 현재 동기화 상태
- 액티브 피어의 IP 주소와 최근 동기화 시간
- 스탠바이 피어의 IP 주소와 최근 동기화 시간

시스템 상태

- 두 피어의 IP 주소
- 두 피어의 운영 체제
- 두 피어의 소프트웨어 버전
- 두 피어의 어플라이언스 모델

참고 활성 management center에서만 내보내기 제어 및 컴플라이언스 상태를 볼 수 있습니다.

Management Center 고가용성 쌍에서 동기화된 구성

두 management center 사이에 고가용성을 설정하면 다음 설정 데이터가 동기화됩니다.

- 라이선스 등록
- 액세스 제어 정책
- 침입 규칙
- 악성코드 및 파일 정책
- DNS 정책
- ID 정책
- SSL 정책
- 사전 필터 정책
- 네트워크 검색 규칙
- 애플리케이션 탐지기
- 상관 관계 정책 규칙
- 알림
- 스캐너
- 응답 그룹
- 조사 이벤트에 대한 외부 리소스의 상황별 교차 실행
- 보안정책 교정 설정을 위해 두 management center에 사용자 정의 모듈을 설치해야 합니다. 보안 정책 교정 설정에 대한 자세한 내용은 교정 모듈 관리, 1082 페이지를 참조하십시오.

동기화 최적화 구성

페일오버 일시 중단 또는 재개 후 노드가 리부팅되거나 노드가 다시 참가하는 경우 참가하는 유닛은 실행 중인 구성을 지웁니다. 액티브 유닛은 전체 구성 동기화를 위해 전체 구성을 참가하는 유닛으로 전송합니다. 액티브 유닛에 대규모 구성이 있는 경우, 참가하는 유닛에서 구성을 동기화하는 데 몇 분 정도 걸립니다.

구성 동기화 최적화 기능을 사용하면 구성 해시 값을 교환하여 참가 유닛과 액티브 유닛의 구성을 비교할 수 있습니다. 액티브 유닛과 조인 유닛 모두에서 계산된 해시가 일치하는 경우, 조인 유닛은 전체 config-sync를 건너뛰고 HA에 다시 조인합니다. 이 기능을 사용하면 HA 피어링 속도가 빨라지고 유지 관리 기간과 업그레이드 시간이 단축됩니다.

구성 동기화 최적화의 지침 및 제한 사항

- 구성 동기화 최적화 기능은 threat defense 버전 7.2 이상에서 기본적으로 활성화됩니다.
- Threat Defense 다중 상황 모드는 전체 구성 동기화 중에 상황 순서를 공유하여 후속 노드 다시 조인 중에 상황 순서를 비교할 수 있도록 구성 동기화 최적화 기능을 지원합니다.
- 암호 및 페일오버 IPsec 키를 구성하는 경우 액티브 유닛과 스탠바이 유닛에서 계산되는 해시 값이 다르기 때문에 Config Sync Optimization(동기화 최적화 구성)이 적용되지 않습니다.
- 동적 ACL 또는 SNMPv3를 사용하여 디바이스를 구성하는 경우 Config Sync Optimization(구성 동기화 최적화) 기능이 적용되지 않습니다.
- 액티브 유닛은 기본 동작으로 플래핑 LAN 링크를 사용하여 전체 구성을 동기화합니다. 액티브 유닛과 스탠바이 유닛 간의 페일오버 플랩 중에는 구성 동기화 최적화 기능이 트리거되지 않고 전체 구성 동기화를 수행합니다.

구성 동기화 최적화 모니터링

Config Sync Optimization(구성 동기화 최적화) 기능이 활성화된 경우 시스템 로그 메시지가 생성되어 액티브 유닛과 조인 유닛에서 계산된 해시 값이 일치하는지 여부 또는 작업 시간 초과가 만료되는지 여부를 표시합니다. 시스템 로그는 또한 해시 요청을 전송한 시간부터 해시 응답을 가져오고 비교하는 시간까지 경과된 시간을 표시합니다.

고가용성 쌍의 **Management Center** 데이터베이스에 대한 외부 액세스 구성

고가용성 설정에서는 활성 피어만 사용하여 데이터베이스에 대한 외부 액세스를 구성하는 것이 좋습니다. 외부 데이터베이스 액세스를 위해 대기 피어를 구성하는 경우 연결이 자주 끊어집니다. 연결을 복원하려면 스탠바이 피어의 동기화를 쌍을 이룬 Management Center 간에 통신 일시 중지하고 쌍을 이룬 Management Center 간에 통신 다시 시작해야 합니다. management center에 대한 외부 데이터

베이스 액세스를 활성화하는 방법에 대한 내용은 데이터베이스에 대한 외부 액세스 활성화, 64 페이지을 참조하십시오.

Management Center 고가용성에서 CLI를 사용하여 디바이스 등록 확인

스탠바이 management center에 자동 디바이스 등록이 실패하지만 액티브 management center로 등록된 경우 다음 단계를 완료합니다.

경고! 보조 management center RMA를 수행하거나 보조 management center를 추가하는 경우 매니지드 디바이스가 등록 취소되며, 결과적으로 구성이 삭제될 수 있습니다.

프로시저

단계 **1** 액티브 management center에서 디바이스를 삭제합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *management center*의 디바이스 삭제*(*등록 취소*)*를 참고하십시오.

단계 **2** 영향을 받는 디바이스의 CLI에 로그인합니다.

단계 **3** CLI 명령을 실행합니다. **configure manager delete**.

이 명령은 현재 management center을 비활성화하고 제거합니다.

단계 **4** CLI 명령을 실행합니다. **configure manager add**.

이 멸영은 management center에 연결하기 위한 디바이스를 구성합니다.

팁 액티브 management center에 한해 디바이스의 원격 관리를 구성합니다. 고가용성을 설정하면 디바이스가 자동으로 스탠바이 management center에 등록됩니다.

단계 **5** 액티브 management center에 로그인하고 디바이스를 등록합니다.

Management Center 고가용성 쌍에서 피어 전환

시스템이 일부 기능을 액티브 management center로 제한하므로 해당 어플라이언스가 실패하면 스탠바이 management center를 액티브로 승격해야 합니다.

프로시저

단계 **1** 고가용성을 사용해 페어링된 management center 중 하나에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 액티브를 스탠바이로, 스탠바이를 액티브로 로컬 역할을 변경하려면 피어 역할 전환을 선택합니다. 그러면 기본 또는 보조 지정은 변경되지 않은 채 두 피어 간 역할이 전환됩니다.

쌍을 이룬 **Management Center** 간에 통신 일시 중지

일시적으로 고가용성을 비활성화하려는 경우 management center 간의 통신 채널을 비활성화할 수 있습니다. 액티브 피어에서 동기화를 중단하면 액티브 또는 스탠바이 피어 중 하나에서 동기화를 재개할 수 있습니다. 그러나 스탠바이 피어의 동기화를 중단하면 스탠바이 피어에서만 동기화를 재개할 수 있습니다.

프로시저

단계 **1** 고가용성을 사용해 페어링된 management center 중 하나에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 동기화 일시 정지를 선택합니다.

쌍을 이룬 **Management Center** 간에 통신 다시 시작

일시적으로 고가용성을 비활성화하려는 경우 management center 간 통신 채널을 활성화하여 고가용성을 재시작할 수 있습니다. 액티브 유닛에서 동기화를 중단한 경우 스탠바이 또는 액티브 유닛 모두에서 동기화를 재개할 수 있습니다. 그러나 스탠바이 유닛의 동기화를 중단하면 스탠바이 유닛에서만 동기화를 재개할 수 있습니다.

프로시저

단계 **1** 고가용성을 사용해 페어링된 management center 중 하나에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 동기화 재개를 선택합니다.

고가용성 쌍의 **Management Center IP** 주소 변경

고가용성 피어 중 하나에 대한 IP 주소가 변경되면 고가용성이 저하 상태에 진입합니다. 고가용성을 복구하려면 수동으로 IP 주소를 변경해야 합니다.

프로시저

단계 **1** 고가용성을 사용해 페어링된 management center 중 하나에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 피어 관리자를 선택합니다.

단계 **5** **Edit(**수정**)** ( )를 선택합니다.

단계 **6** 시스템의 컨텍스트 내에서만 사용되는 어플라이언스의 표시 이름을 입력합니다.

다른 표시 이름을 입력해도 어플라이언스에 대한 호스트 이름은 변경되지 않습니다.

단계 **7** FQDN(Fully Qualified Domain Name) 또는 로컬 DNS를 통해 확인한 유효한 IP 주소(호스트 이름) 또는 호스트 IP 주소를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

Management Center 고가용성 비활성화

프로시저

단계 **1** 고가용성 쌍의 management center 중 하나에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**을 선택합니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 고가용성 분리를 선택합니다.

단계 **5** 관리되는 디바이스를 처리하기 위해 다음 옵션 중 하나를 선택합니다.

- 이 management center의 모든 관리되는 디바이스를 제어하기 위해 이 콘솔에서 등록된 디바이스 관리를 선택합니다. 피어에서 모든 디바이스가 등록 해제됩니다.
- 다른 management center의 모든 관리되는 디바이스를 제어하기 위해 피어 콘솔에서 등록된 디바이스 관리를 선택합니다. 이 management center에서 모든 디바이스가 등록 해제됩니다.
- 모든 디바이스 관리를 중지하려면 두 콘솔에서 등록된 디바이스 관리 중지를 선택합니다. 두 management center에서 모든 디바이스가 등록 해제됩니다.

참고 보조 management center에서 등록된 디바이스를 관리하도록 선택할 경우 디바이스는 기본 management center에서 등록 해제됩니다. 디바이스가 이제 보조 management center에서 관리되도록 등록됩니다. 그러나 이런 디바이스에 적용된 라이선스는 고가용성 해제 작업에 의해 등록 해제됩니다. 이제 보조 management center에서 디바이스 라이선스 재등록(활성화)를 진행해야 합니다. 자세한 내용은 매니지드 디바이스에 라이선스 할당, 289 페이지를 참조하십시오.

단계 **6** **OK(**확인**)**를 클릭합니다.

고가용성 쌍의 **Management Center** 교체

management center 고가용성 쌍에서 장애가 발생한 장치를 교체하는 경우 다음 절차 중 하나를 따라야 합니다. 다음 표는 4개의 오류 상황과 해당 교체 절차를 설명합니다.

오류 상태	데이터 백업 상태	교체 절차
기본 management center 오류	데이터 백업 성공	오류가 발생한 기본 Management Center 교체(백업 성공), 328 페이지
	데이터 백업 실패	오류가 발생한 기본 Management Center 교체(백업 실패), 329 페이지
보조 management center 오류	데이터 백업 성공	오류가 발생한 보조 Management Center 교체(백업 성공), 330 페이지
	데이터 백업 실패	오류가 발생한 보조 Management Center 교체(백업 실패), 331 페이지

오류가 발생한 기본 **Management Center** 교체(백업 성공)

두 management center, *FMC1* 및 *FMC2*는 고가용성 쌍의 일부입니다. *FMC1*은 기본이며 *FMC2*는 보조입니다. 이 작업은 데이터 백업이 성공한 경우 오류가 발생한 기본 management center인 *FMC1*을 교체하는 단계를 설명합니다.

시작하기 전에

오류가 발생한 기본 management center의 데이터 백업이 성공했는지 확인합니다.

프로시저

단계 **1** 오류가 발생한 management center - *FMC1*에 대한 교체를 요청하려면 지원팀에 문의합니다.

단계 **2** 기본 management center - *FMC1*에 오류가 발생하면 보조 management center인 *FMC2*의 웹 인터페이스에서 액세스하여 피어를 교체합니다. 자세한 내용은 Management Center 고가용성 쌍에서 피어 전환, 325 페이지를 참고하십시오.

이때 보조 management center - *FMC2*를 액티브로 전환합니다.

기본 management center - *FMC1*이 교체될 때까지 *FMC2*를 액티브 management center로 사용할 수 있습니다.

주의 management center 고가용성을 *FMC2*에서 분리하지 마십시오. (오류 발생 전에) *FMC1*에서 *FMC2*에 동기화된 라이선스가 *FMC2*에서 제거되어 *FMC2*에서 구축 작업을 수행할 수 없게 됩니다.

단계 **3** *FMC1*과 동일한 소프트웨어 버전으로 management center을 리이미징하고 교체합니다.

단계 **4** *FMC1*에서 생성한 데이터 백업을 새 management center에 복원합니다.

단계 **5** *FMC2*와 일치시키기 위해 필수 management center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.

새 management center 및 *FMC2* 모두 액티브 피어이므로 고가용성에 스플릿 브레인이 발생합니다.

단계 **6** management center 웹 인터페이스가 액티브 어플라이언스를 선택하도록 할 경우 *FMC2*를 액티브로 선택합니다.

이때 *FMC2*의 최신 설정이 새 management center - *FMC1*에 동기화됩니다.

단계 **7** 설정 동기화가 성공하면 보조 management center - *FMC2*의 웹 인터페이스에 액세스하여 기본 management center - *FMC1*의 역할을 액티브로 전환합니다. 자세한 내용은 Management Center 고가용성 쌍에서 피어 전환, 325 페이지를 참고하십시오.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 management center이 정상적으로 작동합니다.

오류가 발생한 기본 **Management Center** 교체(백업 실패)

두 management center, *FMC1* 및 *FMC2*는 고가용성 쌍의 일부입니다. *FMC1*은 기본이며 *FMC2*는 보조입니다. 이 작업은 데이터 백업이 실패한 경우 오류가 발생한 기본 management center인 *FMC1*을 교체하는 단계를 설명합니다.

프로시저

단계 **1** 오류가 발생한 management center - *FMC1*에 대한 교체를 요청하려면 지원팀에 문의합니다.

단계 **2** 기본 management center - *FMC1*에 오류가 발생하면 보조 management center인 *FMC2*의 웹 인터페이스에서 액세스하여 피어를 교체합니다. 자세한 내용은 Management Center 고가용성 쌍에서 피어 전환, 325 페이지를 참고하십시오.

이때 보조 management center - *FMC2*를 액티브로 전환합니다.

기본 management center - *FMC1*이 교체될 때까지 *FMC2*를 액티브 management center로 사용할 수 있습니다.

주의 management center 고가용성을 *FMC2*에서 분리하지 마십시오. (오류 발생 전에) *FMC1*에서 *FMC2*에 동기화된 라이선스가 *FMC2*에서 제거되어 *FMC2*에서 구축 작업을 수행할 수 없게 됩니다.

단계 **3** *FMC1*과 동일한 소프트웨어 버전으로 management center을 리이미징하고 교체합니다.

단계 **4** *FMC2*와 일치시키기 위해 필수 management center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.

단계 **5** management center - *FMC2* 중 하나를 Cisco Smart Software Manager에서 등록 취소합니다. 자세한 내용은 등록 취소Management Center, 292 페이지을 참고하십시오.

management center을 Cisco Smart Software Manager에서 등록 취소하면 가상 어카운트에서 Managememt Center가 제거됩니다. management center와 연결되는 모든 라이선스 엔타이틀먼트를 가상 어카운트에 다시 릴리스합니다. 등록 취소 후 라이선스 기능에 대한 어떤 업데이트 또는 변경도 허용되지 않는 부분에서 management center가 Enforcement(시행) 모드를 입력합니다.

단계 **6** 보조 management center - *FMC2*의 웹 인터페이스에 액세스하여 management center 고가용성을 해제합니다. 자세한 내용은 Management Center 고가용성 비활성화, 327 페이지를 참고하십시오. 관리되는 디바이스를 처리하기 위한 옵션 선택 메시지가 표시되면 이 콘솔에서 등록된 디바이스 관리를 선택합니다.

따라서 보조 management center - *FMC2*에서 동기화된 라이선스가 제거되고 *FMC2*에서 구축 작업을 수행할 수 없습니다.

단계 **7** management center - *FMC2*를 기본으로 설정하고 management center - *FMC1*을 보조로 설정하여 management center 고가용성을 다시 설정합니다. 자세한 내용은 Management Center 고가용성 설정, 320 페이지를 참조하십시오.

단계 **8** 기본 management center - *FMC2*에 스마트 라이선스를 등록합니다. 자세한 내용은 Management Center를 Smart Software Manager로 등록, 284 페이지를 참조하십시오.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 management center이 정상적으로 작동합니다.

오류가 발생한 보조 **Management Center** 교체(백업 성공)

두 management center, *FMC1* 및 *FMC2*는 고가용성 쌍의 일부입니다. *FMC1*은 기본이며 *FMC2*는 보조입니다. 이 작업은 데이터 백업이 성공한 경우 오류가 발생한 보조 management center인 *FMC2*를 교체하는 단계를 설명합니다.

시작하기 전에

오류가 발생한 보조 management center의 데이터 백업이 성공했는지 확인합니다.

프로시저

단계 **1** 오류가 발생한 management center - *FMC2*에 대한 교체를 요청하려면 지원팀에 문의합니다.

단계 **2** 기본 management center - *FMC1*을 액티브 management center로 계속 사용합니다.

단계 **3** *FMC2*과 동일한 소프트웨어 버전으로 management center을 리이미징하고 교체합니다.

단계 **4** *FMC2*에서 생성한 데이터 백업을 새 management center에 복원합니다.

단계 **5** *FMC1*와 일치시키기 위해 필수 management center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.

단계 **6** (중단된 경우) 기본 management center - *FMC1*의 최신 설정을 동기화하기 위해 새 management center의 웹 인터페이스 *FMC2*에서 데이터 동기화를 재개합니다. 자세한 내용은 쌍을 이룬 Management Center 간에 통신 다시 시작, 326 페이지를 참고하십시오.

클래식 및 스마트 라이선스가 원활하게 작동합니다.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 management center이 정상적으로 작동합니다.

오류가 발생한 보조 **Management Center** 교체(백업 실패)

두 management center, *FMC1* 및 *FMC2*는 고가용성 쌍의 일부입니다. *FMC1*은 기본이며 *FMC2*는 보조입니다. 이 작업은 데이터 백업이 성공한 경우 오류가 발생한 보조 management center인 *FMC2*를 교체하는 단계를 설명합니다.

프로시저

단계 **1** 오류가 발생한 management center - *FMC2*에 대한 교체를 요청하려면 지원팀에 문의합니다.

단계 **2** 기본 management center - *FMC1*을 액티브 management center로 계속 사용합니다.

단계 **3** *FMC2*과 동일한 소프트웨어 버전으로 management center을 리이미징하고 교체합니다.

단계 **4** *FMC1*와 일치시키기 위해 필수 management center 패치, 지리위치 데이터베이스(GeoDB) 업데이트, 취약성 데이터베이스(VDB) 업데이트, 시스템 소프트웨어 업데이트를 설치합니다.

단계 **5** 기본 management center - *FMC1*의 웹 인터페이스에 액세스하여 management center 고가용성을 해제합니다. 자세한 내용은 Management Center 고가용성 비활성화, 327 페이지를 참고하십시오. 관리되는 디바이스를 처리하기 위한 옵션 선택 메시지가 표시되면 이 콘솔에서 등록된 디바이스 관리를 선택합니다.

단계 **6** management center - *FMC2*를 기본으로 설정하고 management center - *FMC1*을 보조로 설정하여 management center 고가용성을 다시 설정합니다. 자세한 내용은 Management Center 고가용성 설정, 320 페이지를 참조하십시오.

- 고가용성이 성공적으로 설정된 경우 기본 management center - *FMC1*의 최신 설정이 보조 management center - *FMC2*에 동기화됩니다.
- 클래식 및 스마트 라이선스가 원활하게 작동합니다.

다음에 수행할 작업

고가용성이 재설정되고 기본 및 보조 management center이 정상적으로 작동합니다.

Management Center 고가용성 재해 복구

재해 복구 상황에서는 수동 전환을 수행해야 합니다. 기본 management center - FMC1에 오류가 발생하면 보조 management center인 FMC2의 웹 인터페이스에서 액세스하여 피어를 교체합니다. 이는 보조(FMC2)에 장애가 발생하는 경우에도 반대로 적용됩니다. 자세한 내용은 Management Center 고가용성 쌍에서 피어 전환, 325 페이지를 참고하십시오.

실패한 management center 복원에 대해서는 고가용성 쌍의 Management Center 교체, 328 페이지의 내용을 참조하십시오.

고가용성 쌍의 Management Center 복원(하드웨어 장애 없음)

하드웨어 장애가 없는 경우 고가용성 쌍을 복원하려면 다음 절차를 수행합니다.management center

- 기본 Management Center에서 백업 복원 , 332 페이지
- 보조 Management Center에서 백업 복원, 333 페이지

기본 Management Center에서 백업 복원

시작하기 전에

- 관리 센터의 하드웨어 오류 및 교체가 없습니다.
- 백업 및 복원 프로세스를 잘 알고 있어야 합니다. 백업/복구, 465 페이지를 참조하십시오.

프로시저

단계 1 기본 management center의 백업을 사용할 수 있는지 확인합니다(/var/sf/backup/의 로컬 스토리지 또는 원격 네트워크 볼륨).

단계 2 기본 management center에서 동기화를 일시 정지합니다. **Integration(통합)** > **Other Integrations(기타 통합)**를 선택한 다음 **High Availability(고가용성)** 탭으로 이동하여 동기화를 일시 정지합니다.

단계 3 기본 management center에서 백업을 복원합니다. 복원이 완료되면 management center가 재부팅됩니다.

단계 4 기본 management center가 활성 상태이고 해당 사용자 인터페이스에 연결할 수 있으면 보조 management center에서 동기화를 다시 시작합니다. **Integration(통합)** > **Other Integrations(기타 통합)**를 선택한 다음 **High Availability(고가용성)** 탭으로 이동하여 동기화를 다시 시작합니다.

보조 Management Center에서 백업 복원

시작하기 전에

- 관리 센터의 하드웨어 오류 및 교체가 없습니다.
- 백업 및 복원 프로세스를 잘 알고 있어야 합니다. 백업/복구, 465 페이지를 참조하십시오.

프로시저

단계 1 보조 management center의 백업을 사용할 수 있는지 확인합니다(/var/sf/backup/의 로컬 스토리지 또는 원격 네트워크 볼륨).

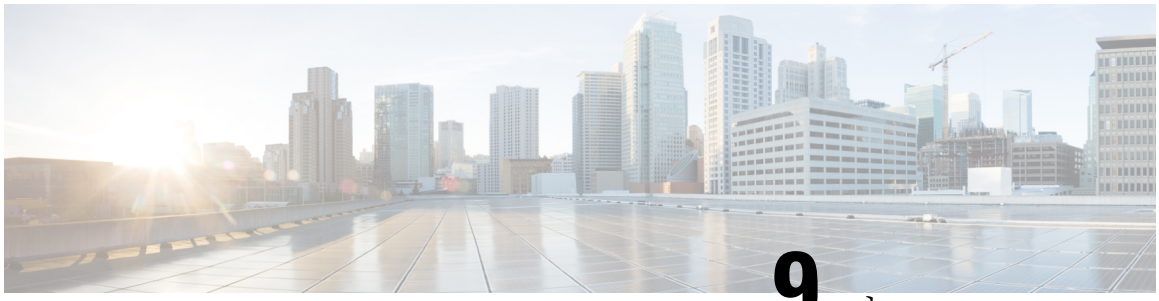
단계 2 기본 management center에서 동기화를 일시 정지합니다. **Integration(통합)** > **Other Integrations(기타 통합)**를 선택한 다음 **High Availability(고가용성)** 탭으로 이동하여 동기화를 일시 정지합니다.

단계 3 보조 management center에서 백업을 복원합니다. 복원이 완료되면 management center가 재부팅됩니다.

단계 4 보조 management center가 활성 상태이고 해당 사용자 인터페이스에 연결할 수 있으면 기본 management center에서 동기화를 다시 시작합니다. **Integration(통합)** > **Other Integrations(기타 통합)**를 선택한 다음 **High Availability(고가용성)** 탭으로 이동하여 동기화를 다시 시작합니다.

Management Center 고가용성 히스토리

기능	버전	세부정보
Azure 및 KVM에서 고가용성을 지원합니다.	7.3	이제 Azure 및 KVM에 대해 management center virtual에서 고가용성을 지원합니다. 자세한 내용은 가상 플랫폼 요건, 318 페이지 및 Management Center 고가용성 설정에 대한 라이선스 요구 사항, 319 페이지를 참조하십시오.
AWS 및 OCI에서 고가용성을 지원합니다.	7.1	이제 AWS 및 OCI에 대한 management center virtual의 고가용성을 지원합니다. 자세한 내용은 가상 플랫폼 요건, 318 페이지 및 Management Center 고가용성 설정에 대한 라이선스 요구 사항, 319 페이지를 참조하십시오.
HyperFlex의 고가용성을 지원합니다.	7.0	이제 HyperFlex에 대한 management center virtual의 고가용성을 지원합니다. 자세한 내용은 가상 플랫폼 요건, 318 페이지 및 Management Center 고가용성 설정에 대한 라이선스 요구 사항, 319 페이지를 참조하십시오.
VMware의 고가용성을 지원합니다.	6.7	이제 VMware에 대한 management center virtual의 고가용성을 지원합니다. 자세한 내용은 가상 플랫폼 요건, 318 페이지 및 Management Center 고가용성 설정에 대한 라이선스 요구 사항, 319 페이지를 참조하십시오.
SSO(Single Sign-On)	6.7	SSO(Single Sign-On)를 위해 고가용성 쌍의 멤버 하나 또는 둘 다를 구성할 때는 특별한 고려 사항이 있습니다.



9 장

보안 인증서 컴플라이언스

다음 주제에서는 보안 인증 표준을 준수하도록 시스템을 구성하는 방법에 대해 설명합니다.

보안 인증서 컴플라이언스 모드

조직에서는 미국국방부 및 글로벌 인증 기관이 마련한 보안 표준을 준수하는 장비 및 소프트웨어만 사용해야 할 수 있습니다. Firepower에서는 다음 보안 인증 표준에 대한 컴플라이언스를 지원합니다.

- CC(Common Criteria): 국제상호인정협정(Common Criteria Recognition Arrangement)에서 마련한 글로벌 표준으로, 보안 제품의 속성이 정의되어 있음
- UCAPL(Unified Capabilities Approved Products List): 미국국방부 정보시스템 계획국(U.S. Defense Information Systems Agency, DISA)이 마련한 보안 요구 사항을 충족하는 제품의 목록

참고 미국 정부에서 UCAPL(Unified Capabilities Approved Products List)의 이름을 DODIN APL(국방부 정보 네트워크 승인 제품 목록)로 변경했습니다. Secure Firewall Management Center 웹 인터페이스 및 이 문서의 UCAPL에 대한 참조를 DODIN APL에 대한 참조로 해석할 수 있습니다.

- FIPS(Federal Information Processing Standard) 140: 암호화 모듈에 대한 요구 사항 사양

CC 모드 또는 UCAPL 모드에서 보안 인증서 컴플라이언스를 활성화할 수 있습니다. 보안 인증 컴플라이언스를 활성화한다고 해서 선택한 보안 모드의 모든 요구 사항이 반드시 엄격하게 준수되는 것은 아닙니다. 강화 절차에 대한 자세한 내용은 엔티티 인증을 통해 제공된 이 제품에 대한 지침을 참조하십시오.

⚠

주의 이 설정을 활성화한 후에는 비활성화할 수 없습니다. 어플라이언스를 CC 또는 UCAPL 모드에서 해제해야 한다면, 이미지로 다시 설치해야 합니다.

보안 인증서 컴플라이언스 특성

다음 표에서는 CC 또는 UCAPL 모드를 활성화하는 경우 동작 변경에 대해 설명합니다. (로그인 계정에 대한 제한은 웹 인터페이스 액세스가 아닌 명령줄 액세스를 의미합니다.)

시스템 변경	**Secure Firewall Management Center**		클래식 관리 디바이스		**Secure Firewall Threat Defense**	
	CC 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드
FIPS 컴플라이언스 활성화됨	예	예	예	예	예	예
시스템에서 백업 또는 보고서를 위한 원격 스토리지를 허용하지 않습니다.	예	예	—	—	—	—
시스템이 추가 시스템 감사 데몬을 시작합니다.	아니요	예	아니요	예	아니요	아니요
시스템 부트 로더가 보호됩니다.	아니요	예	아니요	예	아니요	아니요
시스템은 로그인 계정에 추가 보안을 적용합니다.	아니요	예	아니요	예	아니요	아니요
시스템은 재부팅 키 시퀀스 Ctrl+Alt+Del을 비활성화합니다.	아니요	예	아니요	예	아니요	아니요
시스템은 최대 10개의 동시 로그인 세션을 시행합니다.	아니요	예	아니요	예	아니요	아니요
비밀번호는 대/소문자가 혼합된 영숫자 15자 이상이고 숫자를 하나 이상 포함해야 합니다.	아니요	예	아니요	예	아니요	아니요
로컬 관리자 CLI의 최소 필수 암호 길이는 로컬 장치 CLI를 사용하여 구성할 수 있습니다.	아니요	아니요	아니요	아니요	예	예
비밀번호는 사전에 나와 있는 단어를 사용할 수 없고 연속적으로 반복되는 문자를 포함할 수 없습니다.	아니요	예	아니요	예	아니요	아니요
세 번 연속으로 로그인 시도에 실패한 후 시스템이 관리자가 아닌 사용자를 잠금 처리합니다. 이 경우 관리자가 비밀번호를 재설정해야 합니다.	아니요	예	아니요	예	아니요	아니요

시스템 변경	**Secure Firewall Management Center**		클래식 관리 디바이스		**Secure Firewall Threat Defense**	
	CC 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드	**CC** 모드	**UCAPL** 모드
시스템은 기본적으로 비밀번호 기록을 저장합니다.	아니요	예	아니요	예	아니요	아니요
관리자는 웹 인터페이스를 통해 구성할 수 있는 최대 로그인 시도 실패 횟수가 초과된 후에 잠금 처리될 수 있습니다.	예	예	예	예	—	—
관리자는 로컬 어플라이언스 CLI를 통해 구성할 수 있는 최대 로그인 시도 실패 횟수가 초과된 후에 잠금 처리될 수 있습니다.	아니요	아니요	예, 보안 인증서 컴플라이언스 활성화 여부와 관계없습니다.	예, 보안 인증서 컴플라이언스 활성화 여부와 관계없습니다.	예	예
다음의 경우 시스템이 어플라이언스와 함께 SSH 세션을 자동으로 재설정합니다. • 세션 활동 1시간 동안 키가 사용된 후 • 연결을 통해 1GB의 데이터를 전송하는 데 키가 사용된 후	예	예	예	예	예	예
시스템은 부팅 시 FSIC(파일 시스템 무결성 검사)를 수행합니다. FSIC가 실패하면 Firepower 소프트웨어가 시작되지 않고 원격 SSH 액세스가 비활성화되며 로컬 콘솔을 통해서만 어플라이언스에 액세스할 수 있습니다. 이러한 현상이 발생하는 경우 Cisco TAC에 문의하십시오.	예	예	예	예	예	예

보안 인증서 컴플라이언스 추천

보안 인증서 컴플라이언스가 설정된 시스템을 사용하는 경우 다음 모범 사례를 준수하는 것이 좋습니다.

- 구축에서 보안 인증서 컴플라이언스를 활성화하려면 먼저 Secure Firewall Management Center에서 보안 인증을 활성화한 다음 모든 매니지드 디바이스에서 동일한 모드로 활성화합니다.

주의 Secure Firewall Management Center는 둘 다 동일한 보안 인증서 컴플라이언스 모드에서 작동하지 않는 한 매니지드 디바이스에서 이벤트 데이터를 수신하지 않습니다.

- 모든 사용자에 대해 비밀번호 강도 검사를 활성화하고 인증 기관에 요구하는 값으로 최소 비밀번호 길이를 설정합니다.
- 고가용성 구성에서 Secure Firewall Management Center를 사용하는 경우 동일한 보안 인증서 컴플라이언스 모드를 사용하도록 구성합니다.
- Firepower 4100/9300에서 Secure Firewall Threat Defense가 CC 또는 UCAPL 모드에서 작동하도록 구성하는 경우 CC 모드에서 작동하도록 Firepower 4100/9300도 구성해야 합니다. 자세한 내용은 *Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager* 구성 가이드를 참고하십시오.
- 다음 기능 중 하나를 사용하도록 시스템을 구성하지 마십시오.
  - 이메일 보고서, 알림 또는 데이터 정리 알림.
  - Nmap 스캔, Cisco IOS Null Route, 속성 값 설정 또는 ISE EPS 재조정
  - 백업 또는 보고서를 위한 원격 스토리지
  - 시스템 데이터베이스에 대한 타사 클라이언트 액세스
  - 이메일(SMTP), SNMP 트랩 또는 시스템 로그를 통해 전송되는 외부 알림 또는 경고
  - 어플라이언스와 서버 사이의 채널을 보호하기 위해 SSL 인증서를 사용하지 않고 HTTP 서버 또는 시스템 로그 서버로 전송된 감사 로그 메시지
- CC 모드를 이용하는 구축에서는 LDAP 또는 RADIUS를 사용하여 외부 인증을 활성화하지 마십시오.
- CC 모드를 사용하는 구축에서는 CAC를 활성화하지 마십시오.
- CC 또는 UCAPL 모드를 사용하는 구축에서는 Firepower REST API를 통해 Secure Firewall Management Center 및 매니지드 디바이스에 대한 액세스를 비활성화합니다.
- UCAPL 모드를 사용하는 구축에서 CAC를 활성화합니다.
- CC 모드를 사용하는 구축에서는 SSO를 설정하지 마십시오.
- 디바이스가 모두 동일한 보안 인증서 컴플라이언스 모드를 사용하지 않는 한 고가용성 쌍으로 Secure Firewall Threat Defense 디바이스를 구성하지 마십시오.

참고 시스템은 다음에 대해 CC 또는 UCAPL 모드를 지원하지 않습니다.

- Secure Firewall Threat Defense 클러스터의 디바이스
- Secure Firewall Threat Defense 컨테이너 인스턴스: Firepower 4100/9300
- eStreamer를 사용하여 이벤트 데이터를 외부 클라이언트로 내보내기

어플라이언스 강화

시스템을 더욱 강화할 수 있는 기능 관련 정보는 최신 버전 *Cisco Firepower Mangement Center* 강화 가이드와 *Cisco Secure Firewall Threat Defense* 강화 가이드 및 이 문서의 다음 주제에서 확인할 수 있습니다.

- 라이선스, 261 페이지
- Management Center의, 117 페이지
- Management Center에 로그인, 29 페이지
- 감사 로그, 47 페이지
- 감사 로그 인증서, 51 페이지
- 시간 동기화, 102 페이지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Threat Defense*를 위한 *NTP* 시간 동기화 구성
- 이메일 알림 응답 생성, 575 페이지
- 침입 이벤트에 대한 이메일 알림 설정, 584 페이지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *SMTP* 구성
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Firepower 1000/2100* 시리즈용 *SNMP* 정보
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *SNMP* 구성
- SNMP 알림 응답 생성, 571 페이지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 동적 *DNS* 구성
- DNS 캐시, 57 페이지
- 감사 및 시스템 로그, 417 페이지
- 액세스 목록, 44 페이지
- 보안 인증서 컴플라이언스, 335 페이지

- 원격 스토리지에 대한 SSH 설정, 98 페이지
- 감사 로그 인증서, 51 페이지
- HTTPS 인증서, 65 페이지
- 웹 인터페이스의 사용자 역할 맞춤화, 201 페이지
- 내부 사용자 추가, 123 페이지
- 세션 시간 초과, 100 페이지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 시스템 로그 구성 관련 정보
- Management Center 백업 예약, 503 페이지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사이트 간 *VPNThreat Defense*
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 원격 액세스 *VPN*
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *FlexConfig* 정책

네트워크 보호

네트워크 보호를 위해 구성 할 수 있는 기능에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 액세스 제어 정책
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 인텔리전스
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 침입 정책 시작하기
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 규칙을 사용하여 침입 정책 조정
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 맞춤형 침입 규칙
- 침입 규칙 업데이트, 238 페이지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 침입 이벤트 로깅에 대한 글로벌 제한
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 전송 및 네트워크 레이어 전처리기
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 특정 위협 탐지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 애플리케이션 레이어 프리프로세서
- 감사 및 시스템 로그, 417 페이지
- 침입 이벤트, 807 페이지
- 이벤트 검색, 721 페이지

- 워크플로우, 679 페이지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스 관리
- 로그인 배너, 75 페이지
- 업데이트, 231 페이지

보안 인증서 컴플라이언스 활성화

이 구성은 Secure Firewall Management Center 또는 매니지드 디바이스에 적용됩니다.

- Secure Firewall Management Center의 경우 이 구성은 시스템 구성에 포함되어 있습니다.
- 매니지드 디바이스의 경우, management center의 이 구성을 플랫폼 설정 정책의 일부로 적용합니다.

두 경우 모두, 시스템 구성 변경 사항을 저장하거나 공유 플랫폼 설정 정책을 구축할 때까지 구성이 적용되지 않습니다.

주의 이 설정을 활성화한 후에는 비활성화할 수 없습니다. 어플라이언스를 CC 또는 UCAPL 모드에서 해제해야 한다면, 이미지로 다시 설치해야 합니다.

시작하기 전에

- Cisco에서는 모든 어플라이언스에서 보안 인증서 컴플라이언스를 활성화하기 전에 구축에 포함할 모든 디바이스를 management center에 등록하는 방법을 권장합니다.
- Secure Firewall Threat Defense 디바이스는 평가 라이선스를 사용할 수 없습니다. Smart Software Manager 계정에서 내보내기 제어 기능을 활성화해야 합니다.
- Secure Firewall Threat Defense 디바이스는 라우팅 모드에서 구축해야 합니다.
- 이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** management center 또는 매니지드 디바이스 중 무엇을 구성하는지에 따라 다음 작업을 수행합니다.

- management center: 시스템 (⚙) > **Configuration(**구성**)**을(를) 선택합니다.
- threat defense 디바이스: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**을(를) 선택하고 Secure Firewall Threat Defense 정책을 생성하거나 편집합니다.

단계 **2** **UCAPL/CC Compliance(UCAPL/CC** 규정준수**)**를 클릭합니다.

참고 UCAPL 또는 CC 컴플라이언스를 활성화하면 어플라이언스가 재부팅됩니다. 시스템 구성을 저장할 때 management center가 재부팅됩니다. 매니지드 디바이스는 구성 변경 사항을 구축할 때 재부팅됩니다.

단계 **3** 어플라이언스에서 보안 인증서 컴플라이언스를 영구적으로 활성화하려면 다음 두 가지 중에서 선택할 수 있습니다.

- Common Criteria 모드에서 보안 인증서 컴플라이언스를 활성화하려면 드롭다운 목록에서 **CC**를 선택합니다.
- Unified Capabilities Approved Products List 모드에서 보안 인증서 컴플라이언스를 활성화하려면 드롭다운 목록에서 **UCAPL**을 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 인증 엔티티가 제공한 이 제품의 지침에 설명된 대로 추가 구성 변경을 설정합니다.
- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

III 부

상태 및 모니터링

10 장

대시보드

다음 항목에서는 Firepower System에서 대시보드를 사용하는 방법을 설명합니다.

대시보드 정보

Firepower System 대시보드는 시스템에 의해 수집 및 생성된 이벤트에 대한 데이터를 비롯하여 현재 시스템 상태를 한눈에 볼 수 있는 보기를 제공합니다. 또한 구축에서 어플라이언스의 전체적인 상태에 대한 정보를 확인하는 데에도 대시보드를 사용할 수 있습니다. 참고로 대시보드가 제공하는 정보는 시스템 라이선싱, 구성 및 구축 방법에 따라 달라집니다.

참고 대시보드에서 상관관계가 있는 디바이스 메트릭을 보려면 REST API(**Settings(**설정**)** > **Configuration(**구성**)** > **REST API Preferences(REST API** 기본 설정**)**)를 활성화했는지 확인합니다.

팁 대시보드는 철저한 데이터를 제공하는 복잡한 맞춤형 가능 모니터링 기능입니다. 모니터링되는 네트워크의 광범위하고 간결하고 다채로운 그림을 보려면 컨텍스트 탐색기를 사용하십시오.

대시보드는 탭을 사용하여 위젯을 표시합니다. 위젯은 시스템의 여러 측면을 파악할 수 있는 자체 포함형 소형 구성 요소입니다. 예를 들어, 사전 정의된 Appliance Information(어플라이언스 정보) 위젯에서는 어플라이언스 이름, 모델 및 현재 실행 중인 Firepower System 소프트웨어의 버전을 확인할 수 있습니다. 시스템은 위젯을 대시보드 시간 범위로 제한합니다. 이 범위를 변경해 전 시간만큼 짧거나 지난해처럼 긴 기간을 반영할 수 있습니다.

이 시스템에는 사전 정의된 여러 대시보드가 함께 제공됩니다. 이 대시보드는 사용 및 수정할 수 있습니다. 사용자 역할이 대시보드(관리자, 유지 보수 사용자, 보안 분석가, 보안 분석가[읽기 전용] 및 대시보드 권한이 있는 맞춤형 역할)에 액세스 할 수 있는 경우, 기본적으로 홈페이지는 사전 정의된 요약 대시보드입니다. 그러나 비 대시보드를 포함하여 다른 기본 홈페이지를 구성할 수 있습니다. 기본 대시보드를 변경할 수도 있습니다. 사용자 역할이 대시보드에 액세스 할 수 없는 경우, 기본 홈페

이지는 역할과 관련이 있습니다. 예를 들어, 검색 관리자는 Network Discovery(네트워크 검색) 페이지를 봅니다.

사전 정의된 대시보드를 맞춤형 대시보드의 기본으로 사용할 수도 있습니다. 이 대시보드는 공유하거나 비공개로 제한할 수 있습니다. 관리자 액세스 권한이 없으면 다른 사용자가 생성한 개인 대시보드를 보거나 수정할 수 없습니다.

참고 일부 드릴다운 페이지 및 이벤트의 테이블 보기에는 사전 정의된 관련 대시보드를 보기 위해 클릭할 수 있는 **Dashboard(**대시보드**)** 툴바 링크가 포함되어 있습니다. 사전 정의 대시보드 또는 탭을 삭제하면 연결된 툴바 링크가 작동하지 않습니다.

다중 도메인 구축에서는 상위 도메인의 대시보드를 볼 수 없습니다. 그러나 상위 대시보드의 복사본인 새 대시보드를 생성할 수 있습니다.

Firepower System 대시보드 위젯

대시보드는 하나 이상의 탭을 가지며, 각 탭은 3열 레이아웃에서 하나 이상의 위젯을 표시합니다. Firepower System에는 많은 사전 정의된 대시보드 위젯이 제공되며, 각 위젯은 Firepower System의 다른 측면에 대한 통찰력을 제공합니다. 위젯은 세 카테고리로 그룹화됩니다.

- *Analysis & Reporting widgets(*분석&보고 위젯*)*은 Firepower System에 의해 수집 및 생성된 이벤트를 표시합니다.
- *Miscellaneous widgets(*기타 위젯*)* 이벤트 데이터와 작업 데이터를 모두 표시하지 않습니다. 현재 이 카테고리의 유일한 위젯은 RSS 피드를 표시합니다.
- *Operations widgets(*운영 위젯*)*은 Firepower System의 상태 및 전체 상태에 대한 정보를 표시합니다.

표시되는 대시보드 위젯은 다음에 따라 달라집니다.

- 사용 중인 어플라이언스 유형
- 사용자 역할
- 현재 도메인(다중 도메인 구축의 경우)

또한, 각 대시보드에는 해당 작업을 결정하는 환경 설정 집합이 있습니다.

위젯을 최소화 및 최대화하고 탭에서 위젯을 추가하거나 제거하며, 탭에서위젯을 다시 정렬할 수도 있습니다.

참고 일정 기간 동안 이벤트 수를 표시하는 위젯의 경우, 전체 이벤트 수는 Analysis(분석) 메뉴 하단 페이지에 있는 테이블에서 상세 데이터를 사용할 수 있는 이벤트 수를 반영하지 않을 수 있습니다. 이는 디스크 공간 사용량을 관리하기 위해 때때로 오래된 이벤트의 세부사항을 삭제하기 때문입니다. 이벤트 세부사항이 삭제되는 경우를 최소화하기 위해 이벤트 로깅을 세밀하게 조정하여 구축에 가장 중요한 이벤트만 로깅하게 할 수 있습니다.

위젯 가용성

표시되는 대시보드 위젯은 사용 중인 어플라이언스 유형, 사용자 역할 및 현재 도메인(다중 도메인 구축의 경우)에 따라 달라집니다.

다중 도메인 구축에서, 예상했던 위젯이 보이지 않으면 전역 도메인으로 전환하십시오. 도메인 전환 Secure Firewall Management Center, 22 페이지의 내용을 참조하십시오.

다음을 참고하십시오.

- *invalid(*유효하지 않은*)* 위젯이란 잘못된 어플라이언스 유형을 사용하고 있기 때문에 볼 수 없는 위젯을 말합니다.
- *unauthorized(*무단*)* 뒤젯은 사용자 어카운트에 필요한 권한이 없기 때문에 볼 수 없는 위젯입니다.

예를 들어 어플라이언스 상태 위젯은 관리자, 유지 보수 사용자, 보안 분석가 또는 보안 분석가 (읽기 전용) 계정 권한이 있는 사용자만 management center에서 사용할 수 있습니다.

무단 또는 유효하지 않은 위젯을 대시보드에 추가할 수는 없지만, 가져온 대시보드에는 무단 또는 유효하지 않은 위젯이 포함될 수 있습니다. 예를 들어, 가져온 대시보드가 다음에 해당되는 경우 그러한 위젯이 나타날 수 있습니다.

- 상이한 액세스 권한이 있는 사용자가 생성하였습니다.
- 상위 도메인에 속합니다.

사용할 수없는 위젯은 비활성화되며, 표시되지 않는 이유를 나타내는 오류 메시지가 표시됩니다.

위젯이 시간 초과되거나 다른 문제가 발생하는 경우에도 개별 위젯에 오류 메시지가 표시됩니다.

참고 무단 위젯이나 잘못된 위젯 또는 데이터가 표시되지 않는 위젯은 삭제하거나 최소화할 수 있습니다. 공유 대시보드에서 위젯을 수정하면 어플라이언스의 모든 사용자에 대해 수정됩니다.

사용자 역할별 대시보드 위젯 가용성

다음 표에는 각 위젯을 보기 위해 필요한 사용자 어카운트 권한이 나열되어 있습니다. 관리자, 유지 보수 관리자, 보안 분석가 또는 보안 분석가(읽기 전용) 액세스 권한이 있는 사용자 어카운트만 대시보드를 사용할 수 있습니다.

맞춤형 역할이 부여된 사용자는 사용자 역할이 허용하는 만큼 위젯 조합에 액세스할 수 있습니다. 전부일 수도 전혀 없을 수도 있습니다.

표 ***14:*** 사용자 역할 및 대시보드 위젯 가용성

위젯	관리자	유지 보수 사용자	보안 분석가	보안 분석가**(RO)**
어플라이언스 정보	예	예	예	예
어플라이언스 상태	예	예	예	아니요
상관관계 이벤트	예	아니요	예	예
현재 인터페이스 상태	예	예	예	예
현재 세션	예	아니요	아니요	아니요
맞춤형 분석	예	아니요	예	예
디스크 사용	예	예	예	예
인터페이스 트래픽	예	예	예	예
침입 이벤트	예	아니요	예	예
네트워크 컴플라이언스	예	아니요	예	예
제품 라이선싱	예	예	아니요	아니요
제품 업데이트	예	예	아니요	아니요
RSS 피드	예	예	예	예
시스템 로드	예	예	예	예
시스템 시간	예	예	예	예
허용 이벤트 나열	예	아니요	예	예

사전 정의된 대시보드 위젯

Firepower System에는 대시보드에서 사용할 때 현재 시스템 상태를 한 눈에 볼 수 있는 몇 가지 사전 정의된 위젯이 제공됩니다. 볼 수 있는 항목은 다음과 같습니다.

- 시스템에서 수집하고 생성 한 이벤트에 대한 데이터

- 배포의 어플라이언스 상태 및 전반적인 상태에 대한 정보

참고 표시되는 대시보드 위젯은 사용 중인 어플라이언스 유형, 사용자 역할 및 현재 도메인(다중 도메인 구축의 경우)에 따라 달라집니다.

어플라이언스 정보 위젯

Appliance Information(애플리케이션 정보) 위젯은 어플라이언스의 스냅샷을 제공합니다. 이는 **Detailed Dashboard(**상세 대시보드**)** 및 **Summary Dashboard(**요약 대시보드**)**의 Status(상태) 탭에 기본적으로 나타납니다.

management center가 고가용성으로 구성된 경우 management center의 어플라이언스 정보 위젯에 management center 고가용성에 대한 정보가 표시됩니다. 예를 들어 management center Role(역할), Status(상태), Detail Status(상세 정보 상태) 및 Last Contact(마지막 연락처)에 대한 정보가 표시됩니다. 위젯에서는 다음을 제공합니다.

- 어플라이언스 이름, IPv4 주소, IPv6 주소 및 모델
- 시스템 소프트웨어 버전, 운영 체제, Snort, 규칙 업데이트, 규칙 팩, 모듈 팩, VDB(취약성 데이터베이스) 및 가상 management center virtual을 제외한 대시보드를 포함한 어플라이언스에 설치된 지리위치 업데이트
- 관리되는 어플라이언스의 경우, 관리되는 어플라이언스와의 통신 링크 상태 및 이름

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.

어플라이언스 상태 위젯

Appliance Status(어플라이언스 상태) 위젯은 어플라이언스 및 관리 중인 어플라이언스의 상태를 나타냅니다. management center는 매니지드 디바이스에 상태 정책을 자동으로 적용하지 않으므로 상태 정책을 디바이스에 수동으로 적용해야 합니다. 그렇지 않으면 상태가 `Disabled(비활성화)`로 표시됩니다. 이 위젯은 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

위젯 환경 설정을 수정하여 어플라이언스 상태를 원그래프 또는 테이블로 표시하도록 위젯을 구성할 수 있습니다.

환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

원 그래프의 섹션을 클릭하거나 어플라이언스 상태 테이블의 숫자 중 하나를 클릭하여 Health Monitor(상태 모니터) 페이지로 이동한 다음 어플라이언스 및 관리 중인 어플라이언스의 컴파일된 상태를 볼 수 있습니다.

상관관계 이벤트 위젯

Correlation Events(상관관계 이벤트) 위젯은 대시보드 시간 범위 중 초당 상관관계 이벤트의 평균 개수를 우선순위 기준으로 보여줍니다. 이 위젯은 Detailed Dashboard(상세 대시보드)의 Correlation(상관관계) 탭에 기본적으로 나타납니다.

위젯 환경 설정을 수정하여 서로 다른 우선순위의 상관관계 이벤트를 표시하고, 선형(증분) 또는 로그(10배) 비율을 선택하도록 위젯을 구성할 수 있습니다.

하나 이상의 **Priorities(**우선순위**)** 확인란을 선택하고 특정 우선순위의 이벤트(우선순위가 없는 이벤트 포함)에 대해 별도의 그래프를 표시합니다. **Show All(**모두 표시**)**를 선택하고 우선순위와 상관없이 모든 상관관계 이벤트에 대해 추가 그래프를 표시합니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

특정 우선순위의 상관관계 이벤트를 보려면 그래프 하나를 클릭하고, 모든 상관관계 이벤트를 보려면 **All(**모두**)** 그래프를 클릭합니다. 어떤 경우든 이벤트는 대시보드 시간 범위에 의해 제한됩니다. 대시보드를 통해 상관관계 이벤트에 액세스하면 어플라이언스에 대한 이벤트(또는 전역) 시간 창이 변경됩니다.

현재 인터페이스 상태 위젯

Current Interface Status(현재 인터페이스 상태) 위젯은 활성화되어 있거나 사용하지 않는 어플라이언스의 모든 인터페이스의 상태를 보여줍니다. management center에서 관리(`eth0`, `eth1` 등) 인터페이스를 표시할 수 잇습니다. 매니지드 디바이스에서 센싱(`s1p1` 등) 인터페이스만 표시하거나 관리 및 센싱 인터페이스를 모두 표시하도록 선택할 수 있습니다. 인터페이스는 관리, 인라인, 수동, 스위치드, 라우티드, 사용되지 않음 등의 유형별로 그룹화됩니다.

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.

현재 세션 위젯

Current Sessions(현재 세션) 위젯은 어플라이언스에 현재 로그인한 사용자, 세션이 시작된 시스템과 관련된 IP 주소, 각 사용자가 어플라이언스에서 페이지에 액세스한 마지막 시간(어플라이언스의 현지 시간 기준)을 보여줍니다. 자신을 나타내는 사용자, 즉 현재 위젯을 보고 있는 사용자는 사용자 아이콘과 함께 굵은 글꼴로 표시됩니다. 세션은 로그 오프 1 시간 이내에이 위젯의 데이터에서 정리 됩니다. 이 위젯은 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

Current Sessions(현재 세션) 위젯에서 다음을 수행할 수 있습니다.

- 사용자 관리 페이지에서 사용자 어카운트를 관리하려면 사용자 이름을 클릭합니다.
- IP 주소 옆에 있는 호스트 아이콘 또는 손상된 호스트 아이콘을 클릭하여 연결된 컴퓨터의 호스트 프로필을 확인합니다.
- IP 주소나 액세스 시간을 클릭하여 해당 IP 주소에 의해, 그리고 웹 IP 주소와 연결된 사용자가 웹 인터페이스에 로그온한 시간에 의해 제한되는 감사 로그를 볼 수 있습니다

위젯 환경 설정은 위젯 업데이트의 빈도를 제어합니다.

맞춤형 분석 위젯

사용자 지정 기능이 뛰어난 위젯인 Custom Analysis(맞춤형 분석) 위젯을 사용하면 시스템에 의해 수집 및 생성된 이벤트에 대한 자세한 정보를 표시할 수 있습니다.

위젯에는 구축에 대한 정보에 빠르게 액세스 할 수 있는 여러 사전 설정이 제공됩니다. 사전 정의된 대시보드가 이러한 사전 설정을 광범위하게 사용합니다. 이러한 사전 설정을 사용할 수도 있고 맞춤형 구성을 생성할 수도 있습니다. 맞춤형 구성에서는 최소한 사용자가 관심있는 데이터(테이블 및 필드)와 해당 데이터의 집계 방법을 지정합니다. 다른 디스플레이 관련 환경 설정도 지정할 수도 있습니다. 예를 들어, 이벤트를 상대적 발생(막대 그래프) 또는 시간 경과에 따라(선 그래프) 표시할 수 있습니다.

위젯은 로컬 시간을 기준으로 업데이트한 마지막 시간을 표시합니다. 위젯은 대시보드 시간 범위에 따른 빈도로 업데이트됩니다. 예를 들어 대시보드 시간 범위를 시로 설정하면 위젯은 5분마다 업데이트됩니다. 반면, 대시보드 시간 범위를 연도로 설정하면 위젯은 일주일에 한 번 업데이트됩니다. 대시보드의 다음번 업데이트 시기를 확인하려면 위젯의 왼쪽 아래에 있는 **Last updated(**마지막 업데이트**)** 알림으로 포인터를 이동합니다.

참고 빨간색으로 표시된 Custom Analysis(맞춤 분석) 위젯은 위젯 사용으로 시스템 성능이 저하되고 있음을 나타냅니다. 위젯이 계속해서 빨간색으로 표시되면 해당 위젯을 제거해야 합니다. 시스템 구성(**System(**시스템**)** > **Configuration(**구성**)** > **Dashboard(**대시보드**)**)의 Dashboard(대시보드) 설정에서 모든 Custom Analysis(맞춤 분석) 위젯을 비활성화할 수도 있습니다.

이벤트 상대적 발생**(**막대 그래프**)** 표시

Custom Analysis(맞춤 분석) 위젯의 막대 그래프의 경우, 위젯 배경에 있는 색상이 지정된 막대는 각 이벤트의 상대적 횟수를 표시합니다. 막대를 오른쪽에서 왼쪽으로 읽습니다.

방향 아이콘 은 표시의 정렬 순서를 나타내고 제어합니다. 아래로 향하는 아이콘은 내림차순, 위로 향하는 아이콘은 오름차순을 나타냅니다. 정렬 순서를 바꾸려면 아이콘을 클릭합니다.

각 이벤트 옆에는 최신 결과에서 변경된 내용을 나타내는 세 가지 아이콘 중 하나가 표시됩니다.

- 새 이벤트 아이콘 **Add(**추가**)** (+)은 이벤트가 결과에 새로 추가되었음을 나타냅니다.
- 위쪽 화살표 아이콘은 위젯이 마지막으로 업데이트된 이후 이벤트 순위가 위로 이동했음을 나타냅니다. 이벤트가 몇 단계 올라갔는지 알려주는 숫자가 아이콘 옆에 나타납니다.
- 아래쪽 화살표 아이콘은 위젯이 마지막으로 업데이트된 이후 이벤트 순위가 아래로 이동했음을 나타냅니다. 이벤트가 몇 단계 내려갔는지 알려주는 숫자가 아이콘 옆에 나타납니다.

시간 경과에 따른 이벤트 표시**(**선형 그래프**)**

시간에 따라 발생한 이벤트 또는 기타 수집된 데이터에 대한 정보(예: 구축에서 시간에 따라 생성된 침입 이벤트의 총수)를 보려면 선 그래프를 표시하도록 Custom Analysis(맞춤 분석) 위젯을 구성할 수 있습니다.

맞춤 분석 위젯 제한 사항

Custom Analysis(맞춤 분석) 위젯에는 표시되도록 구성된 데이터를 사용자가 볼 권한이 없다고 나타날 수도 있습니다. 예를 들어, 유지 보수 사용자는 검색 이벤트를 볼 권한이 없습니다. 또 다른 예로, 이 위젯은 라이선스가 없는 기능과 관련된 정보를 표시하지 않습니다. 그러나 사용자(대시보드를 공유하는 모든 사용자)는 자신이 볼 수 있는 데이터를 표시하도록 위젯 환경 설정을 수정할 수 있으며 위젯을 삭제할 수도 있습니다. 이런 일이 발생하지 않도록 하려면 대시보드를 비공개로 저장하십시오.

사용자 데이터를 보는 경우, 시스템에는 권한 있는 사용자만 표시됩니다.

URL 카테고리 정보를 보는 경우, 시스템에는 분류되지 않은 URL이 표시되지 않습니다.

Count(개수**)**로 집계된 침입 이벤트를 보는 경우, 개수에는 침입 이벤트에 대한 검토된 이벤트가 포함됩니다. Analysis(분석) 메뉴 하단 페이지에 있는 테이블 개수를 보는 경우, 개수에는 검토된 이벤트가 포함되지 않습니다.

참고 다중 도메인 구축에서 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 따라서 리프 도메인은 네트워크 내에서는 고유하지만 다른 리프 도메인과 동일한 IP 주소를 포함할 수 있습니다. 상위 도메인에서 맞춤 분석(Custom Analysis) 위젯을 보는 경우, 반복되는 IP 주소의 여러 인스턴스가 표시될 수 있습니다. 처음에는 이것이 중복된 항목으로 보일 수 있습니다. 하지만 각 IP 주소의 호스트 프로파일 정보로 드릴다운하는 경우, 시스템은 이들이 서로 다른 리프 도메인에 속한다고 표시합니다.

디바이스에 대한 대시보드 위젯을 생성하는 방법

디바이스의 이벤트를 표시하는 모든 위젯은 지정된 디바이스 또는 디바이스 집합에 대한 이벤트 표시를 제한하는 필터를 사용하도록 구성할 수 있습니다.

1. 검색 생성 및 저장: **Analysis(**분석**)** > **Search(**검색**)**로 이동하고 특정 디바이스 이름과 일치하는 검색 매개변수를 입력합니다.

참고 구축된 디바이스 이름을 나열하는 드롭다운이 없으므로, 정확히 일치하는 텍스트를 입력해야 합니다.

2. **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Add Widgets(**위젯 추가**)**로 이동하여 **Custom Analysis(**맞춤형 분석**)** 위젯을 생성합니다.
3. **Overview(**개요**)** > 대시보드로 돌아가 새 위젯을 수정하여 검색 범위를 사용자 지정할 수 있습니다.

예: **Custom Analysis(**맞춤형 분석**)** 위젯 구성

Intrusion Events(침입 이벤트**)** 테이블의 데이터를 표시하도록 위젯을 구성하여 최신 침입 이벤트 목록을 표시하도록 Custom Analysis(맞춤형 분석) 위젯을 구성할 수 있습니다. **Classification(**분류**)** 필드를 선택하고 **Count(**개수**)**로 이 데이터를 집계하면 각 유형에 대해 생성된 이벤트 수를 표시합니다.

반면, **Unique Events(**고유한 이벤트**)**로 집계하면 각 유형의 고유 침입 이벤트 수(예: 네트워크 트로이 목마의 탐지 수, 잠재적인 회사 정책 위반, 서비스 거부 공격 시도 등)가 표시됩니다

저장된 검색(어플라이언스와 함께 제공된 사전 정의된 검색 중 하나 또는 자신이 생성한 사용자 지정 검색)을 사용하여 위젯을 추가로 사용자 지정할 수 있습니다. 예를 들어, **Dropped Events(**삭제된 이벤트**)** 검색으로 첫 번째 예제(**Classification(**분류**)** 필드를 사용하고 **Count(**개수**)**로 집계한 침입 이벤트)를 제한하면 각 유형에 대해 삭제된 침입 이벤트 수를 표시합니다.

관련 항목

대시보드 시간 설정 수정, 365 페이지

맞춤형 분석 위젯 환경설정

다음 표에서는 Custom Analysis(맞춤 분석) 위젯에서 설정할 수 있는 환경 설정에 대해 설명합니다.

위젯을 구성하는 방법에 따라 다양한 환경 설정이 표시됩니다. 예를 들어, 이벤트의 상대적 발생(막대 그래프)과 시간 경과그래프(선형 그래프)를 표시하도록 위젯을 구성하면 여러 환경 설정 집합이 나타납니다. 필터와 같은 일부 환경 설정은 데이터를 표시하는 특정 테이블을 선택하는 경우에만 표시됩니다.

표 *15:* 맞춤형 분석 위젯 환경설정

기본 설정	세부 사항
직함	위젯의 제목을 지정하지 않으면 시스템은 구성된 이벤트 유형을 제목으로 사용합니다.
프리셋	맞춤 분석(Custom Analysis) 사전 설정을 통해 구축에 대한 정보에 빠르게 액세스할 수 있습니다. 사전 정의된 대시보드가 이러한 사전 설정을 광범위하게 사용합니다. 이러한 사전 설정을 사용할 수도 있고 맞춤형 구성을 생성할 수도 있습니다.
테이블(필수)	위젯이 표시하는 데이터가 포함된 이벤트 또는 자산 테이블
필드(필수)	표시하려는 이벤트 유형의 특정 필드입니다. 시간에 따른 데이터를 표시하려면(선형 그래프) **Time(**시간**)**을 선택합니다. 이벤트의 상대적 발생(막대 그래프)을 표시하려면 다른 옵션을 선택하십시오.
집계(필수)	집계 방식은 위젯이 표시하는 데이터를 그룹화하는 방법을 구성합니다. 대부분의 이벤트 유형에 대해 기본 옵션은 **Count(**개수**)**입니다.
필터	애플리케이션 필터를 사용하여 Application Statistics(애플리케이션 통계) 및 Intrusion Event Statistics(침입 이벤트 통계) 데이터를 Application(애플리케이션) 테이블별로 제한할 수 있습니다.
검색	저장된 검색을 사용하여 위젯이 표시하는 데이터를 제한할 수 있습니다. 일부 프리셋에서는 사전 정의된 검색을 사용하지만, 검색을 지정해야 할 필요는 없습니다. 비공개로 저장한 검색에는 저장한 당사자만 액세스할 수 있습니다. 공유 대시보드에서 위젯을 구성하고 비공개 검색을 사용하도록 해당 이벤트를 제한하면, 다른 사용자가 로그인할 때 검색을 사용할 수 없도록 위젯이 재설정됩니다. 이것이 위젯 보기에도 영향을 줍니다. 이런 일이 발생하지 않도록 하려면 대시보드를 비공개로 저장하십시오. 연결 요약을 표시하는 필드만이 연결 이벤트를 기반으로 Custom Analysis(맞춤 분석) 대시보드 위젯을 제한할 수 있습니다. 유효하지 않은 저장된 검색은 흐리게 표시됩니다. 저장된 검색을 사용하여 Custom Analysis(맞춤 분석) 위젯을 제한한 다음 검색을 수정하면, 다음 업데이트 시간까지 위젯에 변경 사항이 반영되지 않습니다.
표시	가장 많이(**Top(**상단**)**) 또는 가장 적게(**Bottom(**하단**)**) 발생하는 이벤트를 표시할지 여부를 선택합니다.
결과	표시할 결과 행 수를 선택합니다.
변경 이벤트 표시	가장 최근 결과의 변경 사항을 나타내는 아이콘을 표시할지 여부를 선택합니다.
표준 시간대	결과 표시에 사용할 시간대를 선택합니다.
색상	위젯의 막대 그래프에서 막대의 색상을 변경할 수 있습니다.

관련 항목

위젯 환경설정 구성, 362 페이지

맞춤형 분석 위젯에서 관련 이벤트 보기

Custom Analysis(맞춤 분석) 위젯에서 위젯에 표시된 이벤트에 대한 자세한 정보를 제공하는 이벤트 보기(워크플로)를 호출할 수 있습니다. 이벤트는 해당 이벤트 유형에 대한 기본 워크플로에 표시되며 대시보드 시간 범위로 제한됩니다. 또한 구성한 시간대 개수와 이벤트 유형에 따라 management center에서 해당 기간을 변경합니다.

예를 들면 다음과 같습니다.

- 여러 시간대를 구성한 다음 Custom Analysis(맞춤 분석) 위젯에서 상태 이벤트에 액세스하면, 이벤트는 기본 상태 이벤트 워크플로에 나타나고 상태 모니터링 시간대는 대시보드 시간 범위로 변경됩니다.
- 단일 시간대를 구성한 다음 Custom Analysis(맞춤 분석) 위젯에서 임의의 이벤트 유형에 액세스하면 그 이벤트는 해당 이벤트 유형의 기본 워크플로에 나타나고 전역 시간대는 대시보드 시간 범위로 변경됩니다.

프로시저

다음 옵션을 이용할 수 있습니다.

- Custom Analysis(맞춤 분석) 위젯에서 위젯 오른쪽 아래에 있는 **View(**보기**)** ( )을 클릭하면 위젯 환경설정에 의해 제한되는 모든 관련 이벤트를 볼 수 있습니다.
- 이벤트의 상대적 발생을 보여주는 Custom Analysis(맞춤 분석) 위젯(막대 그래프)에서, 이벤트를 클릭하면 위젯 환경 설정 및 해당 이벤트로 제한된 관련 이벤트를 볼 수 있습니다.

디스크 사용량 위젯

Disk Usage(디스크 사용량) 위젯은 디스크 사용량 카테고리에 따라 하드 드라이브에서 사용된 공간의 백분율을 표시합니다. 이는 또한 어플라이언스 하드 드라이브의 각 파티션에 대한 용량 및 사용되는 공간의 백분율을 나타냅니다. 디바이스에 악성코드 스토리지 팩이 설치되어 있거나 management center가 악성코드 스토리지 팩이 포함된 디바이스를 관리하는 경우, Disk Usage(디스크 사용량) 위젯은 악성코드 스토리지 팩에 대해서도 동일한 정보를 표시합니다. 이 위젯은 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

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 ***16:*** 디스크 사용량 카테고리

디스크사용량카테고리	설명
이벤트	시스템에서 로깅된 모든 이벤트
파일	시스템에서 저장된 모든 파일
백업	모든 백업 파일

디스크사용량카테고리	설명
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

By Category(카테고리별) 누적 막대에서 디스크 사용량 카테고리 위로 포인터를 이동하면 해당 카테고리에 사용된 가용 디스크 공간의 비율, 디스크의 실제 저장 공간 및 해당 카테고리의 총 가용 디스크 공간을 볼 수 있습니다. 악성코드 스토리지 팩이 설치되어 있으면, Files(파일) 카테고리에 대한 총 가용 디스크 공간은 악성코드 스토리지 팩의 가용 디스크 공간입니다.

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.

인터페이스 트래픽 위젯

Interface Traffic(인터페이스 트래픽) 위젯은 수신된 트래픽(Rx) 및 어플라이언스의 관리 인터페이스에 전송된(Tx) 트래픽 비율을 표시합니다. 이 위젯은 사전 정의된 모든 대시보드에 기본적으로 표시되지는 않습니다.

악성코드 방어 라이선스가 정기적으로 활성화되는 디바이스는 사용자가 동적 분석을 구성하지 않은 경우에도 AMP 클라우드 연결을 시도합니다. 따라서 이러한 디바이스는 전송된 트래픽을 표시하는데, 이는 자연스러운 동작입니다.

위젯 환경 설정은 위젯 업데이트의 빈도를 제어합니다.

침입 이벤트 위젯

Intrusion Events(침입 이벤트) 위젯은 대시보드 시간 범위 중에 발생한 침입 이벤트를 우선순위별로 구성하여 보여줍니다. 여기에는 삭제된 패킷 및 서로 다른 영향과 함께 침입 이벤트에 대한 통계도 포함됩니다. 이 위젯은 Summary Dashboard(요약 대시보드)의 Intrusion Events(침입 이벤트) 탭에 기본적으로 나타납니다.

위젯 환경 설정에서 다음을 선택할 수 있습니다.

- **Event Flags(**이벤트 플래그**)**는 삭제된 패킷, 삭제 가능성이 있는 패킷 또는 특정 영향이 있는 이벤트를 별도 그래프로 표시합니다. **All(**모두**)**를 선택하고 영향 또는 규칙 상태와 상관없이 모든 침입 이벤트에 대한 추가 그래프를 표시합니다.

  아이콘에 대한 설명은 침입 이벤트, 807 페이지를 참조하십시오. 영향 레벨 번호 위에 나타나는 화살표(해당되는 경우)는 인라인 결과를 설명하며 다음과 같이 정의됩니다.

표 *17:* 워크플로 및 테이블 보기에서 인라인 결과 필드 내용

아이콘	표시 내용
	시스템이 규칙을 트리거한 패킷을 삭제했음을 나타냅니다.
	(인라인 구축에서) **Drop when Inline(**인라인 시 삭제**)** 침입 정책 옵션을 활성화하는 경우 또는 시스템 정리 중 Drop and Generate(삭제 및 생성) 규칙이 이벤트를 생성한 경우 IPS가 패킷을 삭제했음을 나타냅니다.
	IPS가 패킷을 대상에 전송했거나 전달했을 수 있지만 이 패킷을 포함했던 연결은 이제 차단됩니다.
아이콘 없음(공란)	트리거된 규칙이 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되지 않았음을 나타냅니다.

수동 구축에서 인라인 인터페이스가 탭 모드에 있는 경우를 포함하여 침입 정책의 규칙 상태 또는 인라인 삭제 작업에 상관없이 시스템은 패킷을 삭제하지 않습니다.

- **Show(**표시**)**는 **Average Events Per Second(**초당 평균 이벤트**)**(EPS) 또는 **Total Events(**총 이벤트**)**를 지정합니다.
- **Vervical Scale(**세로 비율**)**은 **Linear(**선형**)**(증분) 또는 **Logarithmic(**로그**)**(10배) 비율을 지정합니다.
- 위젯 업데이트 빈도입니다.

이 위젯에서 다음을 수행할 수 있습니다.

- 삭제된 패킷, 삭제 가능성이 있는 패킷 또는 특정 영향에 해당하는 그래프를 클릭하여 해당 유형의 침입 이벤트를 볼 수 있습니다.
- 삭제된 이벤트에 해당하는 그래프를 클릭하여 해당 이벤트를 볼 수 있습니다.
- 삭제 가능성이 있는 이벤트에 해당하는 그래프를 클릭하여 해당 이벤트를 볼 수 있습니다.
- **All(**모두**)** 그래프를 클릭하여 모든 침입 이벤트를 볼 수 있습니다.

결과 이벤트 보기는 대시보드 시간 범위에 의해 제한됩니다. 대시보드를 통해 침입 이벤트에 액세스하면 어플라이언스에 대한 이벤트(또는 전역) 시간대가 변경됩니다. 참고로 침입 규칙 상태 또는 침입 정책의 인라인 삭제 동작과 상관없이, 패시브 구축의 패킷은 삭제되지 않습니다.

네트워크 컴플라이언스 위젯

Network Compliance(네트워크 컴플라이언스) 위젯은 사용자가 설정한 허용리스트에 대한 호스트의 규정준수를 요약하여 보여줍니다. 기본적으로 이 위젯은 활성 상관관계 정책에 있는 모든 규정준수 허용리스트에 대해 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 수를 보여주는 원도표를 표시합니다. 이 위젯은 Detailed Dashboard(상세 대시보드)의 Correlation(상관관계) 탭에 기본적으로 나타납니다.

위젯 환경설정을 수정하여 모든 허용리스트 또는 특정 허용리스트에 대한 네트워크 규정준수를 표시하도록 위젯을 설정할 수 있습니다.

모든 허용리스트에 대한 네트워크 규정준수를 표시하도록 선택하는 경우, 호스트가 활성 상관관계 정책에서 임의의 허용리스트를 따르지 않으면 위젯은 해당 호스트를 규정을 준수하지 않는 호스트로 간주합니다.

또한 위젯 환경 설정을 사용하여 네트워크 규정준수를 표시하기 위해 사용할 세 가지 서로 다른 스타일 중 하나를 지정할 수 있습니다.

Network Compliance(네트워크 컴플라이언스**)** 스타일(기본값)은 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 수를 보여주는 원 그래프를 표시합니다. 원도표를 클릭하면 호스트 위반 횟수를 볼 수 있습니다. 그러면 하나 이상의 허용리스트를 위반하는 호스트가 나열됩니다.

Network Compliance over Time(시간에 따른 네트워크 컴플라이언스**)(%)** 스타일은 대시보드 시간 범위 중에 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 상대 비율을 보여주는 누적 영역 그래프를 표시합니다.

Network Compliance over Time(시간에 따른 네트워크 컴플라이언스**)**스타일은 대시보드 시간 범위 중에 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 수를 보여주는 선 그래프를 표시합니다.

환경 설정은 위젯 업데이트의 빈도를 제어합니다. **Show Not Evaluated(**평가되지 않은 이벤트 표시**)** 확인란을 선택하고 평가되지 않은 이벤트를 숨깁니다.

제품 라이선싱 위젯

Product Licensing(제품 라이선싱) 위젯은 현재 management center에 설치된 디바이스와 기능 라이선스를 보여줍니다. 또한 라이선싱된 항목 수 및 허용된 나머지 라이선싱된 항목 수를 나타냅니다. 미리 정의된 모든 대시보드에 기본적으로 표시되지는 않습니다.

위젯의 상단 섹션은 management center에 설치된 모든 디바이스 및 기능을 표시합니다. 여기에는 임시 라이선스가 포함되지만 Expiring Licenses(만료 라이선스) 섹션은 임시 라이선스와 만료된 라이선스만 표시합니다.

위젯 백그라운드의 막대는 사용 중인 라이선스의 각 유형에 대한 백분율을 나타냅니다. 막대는 오른쪽에서 왼쪽으로 읽어야 합니다. 만료된 라이선스는 취소 회선으로 표시됩니다.

위젯 환경 설정을 수정하여 현재 라이선싱된 기능 또는 라이선싱할 수 있는 모든 기능 중 하나를 표시하는 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

라이선스 유형을 클릭하여 로컬 구성의 License(라이선스) 페이지로 이동하거나 기능 라이선스를 추가 또는 삭제할 수 있습니다.

제품 업데이트 위젯

Product Updates(제품 업데이트) 위젯은 어플라이언스에 현재 설치된 소프트웨어의 요약과 함께 다운로드했지만 아직 설치하지 않은 업데이트에 대한 정보도 표시합니다. 이 위젯은 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

위젯은 예약된 작업을 사용하여 최신 버전을 확인하기 때문에 업데이트를 다운로드, 푸시 또는 설치하는 예약된 작업을 구성할 때까지 Unknwon(알 수 없음)을 표시합니다.

위젯 설정을 수정하여 최신 버전을 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

이 위젯에서는 소프트웨어를 업데이트할 수 있는 페이지의 링크도 제공합니다. 다음 작업을 수행할 수 있습니다.

- 현재 버전을 클릭하여 어플라이언스를 수동으로 업데이트합니다.
- 최신 버전을 클릭하여 업데이트를 다운로드하는 예약된 작업을 생성합니다.

RSS 피드 위젯

RSS Feed 위젯은 RSS 피드를 대시보드에 추가합니다. 기본적으로 이 위젯은 Cisco 보안 뉴스의 피드를 보여줍니다. 이는 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

회사 뉴스, Snort.org 블로그 또는 Cisco Threat Research 블로그의 사전 구성된 피드를 표시하도록 위젯을 구성할 수도 있고, 위젯 환경 설정에서 URL을 지정하여 다른 RSS 피드에 대한 사용자 지정 연결을 생성할 수도 있습니다. management center는 management center에서 인식하는 CA(Certificate Authority)에서 서명한 신뢰할 수 있는 서버 인증서를 사용하는 경우에만 암호화된 RSS 피드를 표시할 수 있습니다. CA를 사용하는 암호화된 RSS 피드를 management center에서 인식하지 못하거나 자체 서명 인증서를 사용하는 RSS 피드 위젯을 표시하도록 구성하면 검증이 실패하고 위젯이 피드를 표시하지 않습니다.

피드는 24시간마다 업데이트되며(수동으로 업데이트 가능), 위젯은 어플라이언스의 현지 시간을 기반으로 피드가 업데이트된 마지막 시간을 표시합니다. 어플라이언스는 웹사이트(사전 구성된 두 피드의 경우) 또는 구성한 사용자 지정 피드에 액세스할 수 있어야 합니다.

위젯을 구성할 때에는 또한 위젯에 표시할 피드의 스토리 수는 물론 헤드라인과 함께 스토리의 설명을 표시할지 여부도 선택할 수 있습니다. 모든 RSS 피드가 설명을 사용하는 것은 아닙니다.

RSS Feed 위젯에서 다음을 수행할 수 있습니다.

- 스토리를 보려는 피드에서 스토리 중 하나를 클릭할 수 있습니다.
- **more** 링크를 클릭하여 피드의 웹사이트로 이동할 수 있습니다.
- 업데이트( ) 을 클릭하여 피드를 수동으로 업데이트할 수 있습니다.

시스템 로드 위젯

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. 이는 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

위젯 환경 설정을 수정하여 로드 평균을 보여주거나 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

시스템 시간 위젯

System Time(시스템 시간) 위젯은 어플라이언스의 로컬 시스템 시간, 가동 시간 및 부팅 시간을 보여줍니다. 이는 Detailed Dashboard(상세 대시보드) 및 Summary Dashboard(요약 대시보드)의 Status(상태) 탭에 기본적으로 나타납니다.

위젯 환경 설정을 수정하여 부팅 시간을 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 어플라이언스의 시계와 위젯 동기화의 빈도를 제어합니다.

허용 목록 이벤트 위젯

허용 목록 이벤트 위젯은 대시보드 시간 범위 중에 우선순위별 초당 평균 이벤트 수를 보여줍니다. 이 위젯은 Default Dashboard(상세 대시보드)의 Correlation(상관관계) 탭에 기본적으로 나타납니다.

위젯 환경 설정을 수정하여 서로 다른 우선순위의 허용 목록 이벤트를 표시하도록 위젯을 구성할 수 있습니다.

위젯 환경 설정에서 다음을 수행할 수 있습니다.

- 하나 이상의 **Priorities(**우선순위**)** 확인란을 선택하고 특정 우선순위의 이벤트(우선순위가 없는 이벤트 포함)에 대해 별도의 그래프를 표시합니다.
- **Show All(**모두 표시**)**를 선택하고 우선순위와 상관없이 모든 허용 목록 이벤트에 대해 추가 그래프를 표시합니다.
- **Vervical Scale(**세로 비율**)**을 선택하고 **Linear(**선형**)**(증분) 또는 **Logarithmic(**로그**)**(10배) 비율을 선택합니다.

환경 설정은 또한 위젯 업데이트의 빈도를 제어합니다.

특정 우선순위의 허용 목록 이벤트를 보려면 그래프 하나를 클릭하고, 모든 허용 목록 이벤트를 보려면 **All(**모두**)** 그래프를 클릭합니다. 어떤 경우든 이벤트는 대시보드 시간 범위에 의해 제한됩니다. 대시보드를 통해 허용 목록 이벤트에 액세스하면 management center에 대한 이벤트(또는 전역) 시간대가 변경됩니다.

대시보드 관리

프로시저

단계 **1** **Overview(**개요**)** > **Dashboards(**대시보드**)**를 선택한 후, 메뉴에서 수정하려는 대시보드를 선택합니다.

단계 **2** 대시보드 관리:

- Create Dashboards(대시보드 생성) — 맞춤형 대시보드를 생성합니다. 맞춤형 대시보드 생성, 363 페이지을 참조하십시오.
- Delete Dashboards(대시보드 삭제) - 대시보드를 삭제하려면 삭제하려는 대시보드 옆에 있는 **Delete(**삭제**)** ( )를 클릭합니다. 기본 대시보드를 삭제하는 경우 새 기본 대시보드를 정의해야

합니다. 그렇지 않으면 대시보드 보기를 시도할 때마다 대시보드를 선택하라는 메시지가 어플라이언스에 표시됩니다.

- Edit Options(편집 옵션) — 맞춤형 대시보드 옵션을 편집합니다. 대시보드 옵션 수정, 365 페이지을 참조하십시오.
- Modify Time Constraints(시간 제한 수정) — 대시보드 시간 설정 수정, 365 페이지에 설명된 대로 시간 표시를 수정하거나 대시보드를 일시중지/일시중지 취소합니다.

단계 **3** 대시 보드를 추가(대시보드 추가, 361 페이지 참조), 삭제(**Close(**닫기**)** (×) 클릭) 및 이름 변경(대시보드 이름 변경, 367 페이지 참조)합니다.

참고 대시보드 순서는 변경할 수 없습니다.

단계 **4** 대시보드 위젯 관리:

- Add Widgets(위젯 추가) — 대시보드에 위젯을 추가합니다. 대시보드에 위젯 추가, 362 페이지을 참조하십시오.
- Configure Preferences(환경설정 구성) — 위젯 환경설정을 구성합니다. 위젯 환경설정 구성, 362 페이지을 참조하십시오.
- Customize Display(디스플레이 맞춤화) — 위젯 디스플레이를 맞춤화합니다. 위젯 디스플레이 맞춤 설정, 364 페이지을 참조하십시오.
- View Events(이벤트 보기) — Custom Analysis(맞춤 분석) 위젯에서 관련 이벤트를 확인합니다. 맞춤형 분석 위젯에서 관련 이벤트 보기, 355 페이지을 참조하십시오.

팁 Cisco 사전 정의 대시보드에 있는 Custom Analysis(맞춤 분석) 위젯의 모든 구성은 해당 위젯에 대한 시스템 사전 설정과 일치합니다. 이러한 위젯 중 하나를 변경 또는 삭제하는 경우, 적절한 사전 설정을 기반으로 새 Custom Analysis(맞춤 분석) 위젯을 생성하여 복원할 수 있습니다.

대시보드 추가

프로시저

단계 **1** 수정하려는 대시보드를 확인니다. 대시보드 보기, 367 페이지을 참조하십시오.

단계 **2** **Add(**추가**)** (+) 버튼을 클릭합니다.

단계 **3** 이름을 입력합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

대시보드에 위젯 추가

각 탭은 3단 레이아웃에 하나 이상의 위젯을 표시할 수 있습니다. 대시보드에 위젯을 추가하는 경우, 위젯을 추가하려는 탭을 선택합니다. 시스템에서 위젯이 가장 적은 열에 자동으로 위젯을 추가합니다. 모든 열의 위젯 수가 동일하면 새 위젯은 맨 왼쪽 열에 추가됩니다. 대시보드 탭 하나에 최대 15개의 위젯을 추가할 수 있습니다.

팁 위젯을 추가한 후에는 탭에서 원하는 위치로 이동할 수 있습니다. 그러나 탭 간에는 위젯을 이동할 수 없습니다.

표시되는 대시보드 위젯은 사용 중인 어플라이언스 유형, 사용자 역할 및 현재 도메인(다중 도메인 구축의 경우)에 따라 달라집니다. 모든 사용자 역할이 모든 대시보드 위젯에 액세스할 수 있는 것은 아니므로, 권한이 더 적은 사용자가 권한이 더 많은 사용자가 생성한 대시보드를 볼 때 대시보드의 위젯 중 일부가 표시되지 않을 수 있습니다. 무단 위젯이 대시보드에 나타날 수 있지만 비활성화된 상태로 나타납니다.

프로시저

단계 **1** 위젯을 추가하려는 대시보드를 확인합니다. 대시보드 보기, 367 페이지을 참조하십시오.

단계 **2** 위젯을 추가하려는 탭을 클릭합니다.

단계 **3** **Add Widgets(**위젯 추가**)**를 클릭합니다. 카테고리 이름을 클릭하여 각 카테고리의 위젯을 볼 수 있습니다. 모든 위젯을 보려면 **All Categories(**모든 카테고리**)**를 클릭합니다.

단계 **4** 추가하려는 위젯 옆에 있는 **Add(**추가**)**를 클릭합니다. Add Widgets(위젯 추가) 페이지는 추가하려는 위젯을 포함하여 탭에 있는 각 유형의 위젯 수를 나타냅니다

팁 동일한 유형의 여러 위젯을 추가하려면(예: 여러 RSS Feed 위젯 또는 여러 Custom Analysis 위젯 추가) **Add(**추가**)**를 다시 클릭합니다.

단계 **5** 위젯 추가가 끝나면 **Done(**완료**)**를 클릭하고 대시보드로 돌아갑니다.

다음에 수행할 작업

- Custom Analysis(맞춤 분석) 위젯을 추가한 경우, 위젯 환경 설정을 구성합니다. 위젯 환경설정 구성, 362 페이지을 참조하십시오.

관련 항목

위젯 가용성, 347 페이지

위젯 환경설정 구성

각 위젯에는 해당 작업을 결정하는 환경 설정 집합이 있습니다.

프로시저

단계 **1** 환경 설정을 변경하고자 하는 위젯의 제목 표시줄에서 **Show Preferences(**기본 설정 표시**)** ( )을 클릭합니다.

단계 **2** 필요에 따라 변경합니다.

단계 **3** 환경 설정 섹션을 숨기려면 위젯의 제목 표시줄에서 **Hide Preferences(**기본 설정 숨기기**)** ( )을 클릭합니다.

맞춤형 대시보드 생성

팁 새 대시보드를 생성하지 않고 다른 어플라이언스에서 대시보드를 내보낸 다음 현재 어플라이언스로 가져올 수 있습니다. 그런 다음 가져온 대시보드를 필요에 맞게 수정할 수 있습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Management(**관리**)**를 선택합니다.

단계 **2** **Create Dashboard(**대시보드 생성**)**를 클릭합니다.

단계 **3** 맞춤형 대시보드 옵션, 363 페이지에 설명된 대로 맞춤형 대시보드 옵션을 수정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

맞춤형 대시보드 옵션

아래 표에서는 맞춤형 대시 보드를 만들거나 편집할 때 사용할 수 있는 옵션을 설명합니다.

표 ***18:*** 맞춤형 대시보드 옵션

옵션	설명
대시보드 복사	맞춤형 대시보드를 생성 할 때 사용자 생성 또는 시스템 정의 여부와 상관없이 기존 대시보드를 기반으로 선택할 수 있습니다. 이 옵션을 사용하면 기존 대시보드를 복사하여 필요에 맞게 수정할 수 있습니다. 경우에 따라 **none (**없음**)**을 선택하여 비어 있는 새 대시보드를 생성할 수 있습니다. 이 옵션은 새 대시보드를 생성하는 경우에만 사용할 수 있습니다. 다중 도메인 구축에서는 상위 도메인의 모든 공개 대시보드를 복사할 수 있습니다.
이름	맞춤형 대시보드의 고유한 이름.
설명	맞춤형 대시보드에 대한 간략한 설명.

옵션	설명
탭 변경 간격	대시보드가 탭을 순환하는 빈도를 지정합니다(분 단위). 대시보드를 일시 중지하거나 대시보드에 탭이 하나뿐인 경우가 아니면, 여기서 지정한 간격으로 보기가 다음 탭으로 이동합니다. 탭 순환을 비활성화하려면, **Change Tabs Every(**탭 변경 간격**)** 필드에 0을 입력합니다.
페이지 새로 고침 간격:	전체 대시보드 페이지가 자동으로 새로 고쳐지는 빈도를 결정합니다. 전체 대시보드를 새로 고치면, 마지막 대시보드 새로 고침 이후 다른 사용자가 공유 대시보드에 대해 수행한 환경 설정 또는 레이아웃 변경 사항이나, 자신이 다른 컴퓨터에서 비공개 대시보드에 대해 수행한 변경 사항을 볼 수 있습니다. 빈번한 새로 고침은 예를 들어 대시보드가 항상 표시되는 NOC(네트워크 운영 센터)에서 유용 할 수 있습니다. 로컬 컴퓨터에서 대시보드를 변경하는 경우, NOC의 대시보드가 지정된 간격으로 자동으로 새로 고쳐져 수동 새로 고침이 필요하지 않습니다. 새로 고침은 데이터를 업데이트하지 않으며 데이터 업데이트를 보기 위해 전체 대시보드를 새로 고칠 필요는 없습니다. 개별 위젯은 환경 설정에 따라 업데이트됩니다. 이 값은 **Change Tabs Every(**탭 변경 간격**)** 설정보다 큰 수여야 합니다. 대시보드를 일시 중지하지 않는 한, 여기서 지정한 간격으로 전체 대시보드 새로 고침이 수행됩니다. 주기적인 페이지 새로 고침을 비활성화하려면, **Refresh Page Every(**페이지 새로 고침 간격**)** 필드에 0을 입력합니다. 참고 이 설정은 많은 개별 위젯에서 사용할 수 있는 업데이트 간격과는 별개입니다. 대시보드 페이지를 새로 고치면 개별 위젯의 업데이트 간격이 재설정되지만 **Refresh Page Every(**페이지 새로 고침 간격**)** 설정을 비활성화하더라도 위젯은 개별 환경 설정에 따라 업데이트됩니다.
비공개로 저장	어플라이언스의 모든 사용자가 맞춤형 대시보드를 보고 수정할 수 있는지 여부를 결정하거나 사용자 전용으로 사용자 어카운트에 연결됩니다. 참고로 역할과 상관없이 대시보드 액세스 권한이 있는 사용자는 공유 대시보드를 수정할 수 있습니다. 자신만이 특정 대시보드를 수정할 수 있도록 하려면 비공개로 저장해야 합니다.

위젯 디스플레이 맞춤 설정

위젯은 최대화/최소화할 수 있으며 탭에서 다시 정렬할 수도 있습니다.

프로시저

단계 **1** 대시보드를 확인합니다. 대시보드 보기, 367 페이지을 참조하십시오.

단계 **2** 위젯 디스플레이 맞춤 설정:

- 탭에서 위젯을 다시 정렬하려면 이동시키려는 위젯의 제목 표시줄을 클릭한 다음, 새 위치로 끌어 놓습니다.

참고 탭 간에는 위젯을 이동할 수 없습니다. 위젯이 다른 탭에 표시되기를 원하는 경우, 기존 탭에서 삭제하고 새 탭에 추가해야 합니다.

- 대시보드에서 위젯을 최소화하거나 최대화하려면 위젯의 제목 표시줄에서 **Minimize(**최소화**)**( ) 또는 **Maximize(**최대화**)**( )를 클릭합니다.
- 위젯을 삭제해서 더 이상 탭에서 보지 않으려면 위젯의 제목 표시줄에서 **Close(**닫기**)** ( )를 클릭합니다.

대시보드 옵션 수정

프로시저

단계 **1** 편집하려는 대시보드를 확인합니다. 대시보드 보기, 367 페이지을 참조하십시오.

단계 **2** **Edit(**수정**)** ( ) 버튼을 클릭합니다.

단계 **3** 맞춤형 대시보드 옵션, 363 페이지에 설명된 대로 옵션을 변경합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

대시보드 시간 설정 수정

시간 범위를 변경하여 지난 시간처럼 짧은 기간(기본값) 또는 지난해처럼 긴 기간을 반영할 수 있습니다. 시간 범위를 변경할 때, 시간을 통해 자동 제한될 수 있는 위젯은 새로운 시간 범위를 반영하도록 업데이트합니다.

그래프의 최대 데이터 포인트 수는 300이며, 시간 설정은 각 데이터 포인트 내에 요약되는 시간을 결정합니다. 다음은 각 시간 범위에 대한 대시보드에서 다루는 데이터 포인트 수 및 시간 범위입니다.

- 1시간 = 12개의 데이터 포인트, 각 5분
- 6시간 = 72개 데이터 포인트, 각 5분
- 1일 = 288개의 데이터 포인트, 각 5분
- 1주 = 300개의 데이터 포인트, 각 33.6분
- 2주 = 300개의 데이터 포인트, 각 67.2분
- 30일 = 300개 데이터 포인트, 각 144분
- 90일 = 300개의 데이터 포인트, 각 432분
- 180일 = 300개 데이터 포인트, 각 864분
- 1년 = 300개의 데이터 포인트, 각 1752분

모든 위젯을 시간으로 제한할 수 있는 것은 아님에 유의하십시오. 예를 들어, 대시보드 시간 범위는 Firepower System 소프트웨어의 이름, 모델 및 최신 버전을 포함한 정보를 제공하는 Appliance Information(어플라이언스 정보) 위젯에 영향을 주지 않습니다.

Firepower System의 엔터프라이즈 구축에서 시간 범위를 긴 기간으로 변경하는 것은, 새 이벤트가 이전 이벤트를 교체하는 빈도에 따라 Custom Analysis(맞춤 분석) 등의 위젯에는 유용하지 않을 수 있습니다.

대시보드를 일시 중지할 수도 있는데, 그렇게 하면 표시를 변경하고 분석을 중단하지 않아도 위젯에서 제공하는 데이터를 검토할 수 있습니다. 대시보드 일시 중지는 다음과 같은 효과가 있습니다.

- **Update Every(**업데이트 간격**)** 위젯 환경 설정과 상관없이 개별 위젯의 업데이트가 중지됩니다.
- 대시보드 탭은 대시보드 속성의 **Cycle Tabs Every(**탭 순환 간격**)** 설정과 상관없이 순환을 중지합니다.
- 대시보드 속성의 **Refresh Page Every(**페이지 새로 고침 간격**)** 설정과 상관없이 대시보드 페이지 새로 고침이 중지됩니다.
- 시간 범위 변경이 영향을 미치지 않습니다.

분석을 마치면 대시보드의 일시 중지를 취소할 수 있습니다. 대시보드의 일시 중지를 취소하면 현재 시간 범위를 반영하여 페이지의 모든 해당 위젯이 업데이트됩니다. 또한 대시보드 속성에서 지정한 설정에 따라 대시보드 탭의 순환이 다시 시작되고, 대시보드 페이지의 새로 고침도 다시 시작됩니다.

시스템 정보를 대시보드로 보내는 플로우가 중단되는 연결 문제나 기타 문제가 발생하면, 대시보드가 자동으로 일시 중지되고 문제가 해결될 때까지 오류 알림이 나타납니다.

참고 대시보드의 일시 중지 여부와 상관없이, 비활성 상태가 1시간(또는 구성된 다른 간격 동안) 지속되면 일반적으로 세션에서 로그아웃됩니다. 대시보드를 오랫동안 수동으로 모니터링할 계획이면 세션 시간 초과에서 일부 사용자를 제외하거나 시스템 시간 초과 설정을 변경하는 방법을 고려해 보십시오.

프로시저

단계 **1** 위젯을 추가하려는 대시보드를 확인합니다. 대시보드 보기, 367 페이지을 참조하십시오.

단계 **2** 경우에 따라 대시보드 시간 범위를 변경하려면 시간 범위를 **Show the Last(**마지막으로 표시**)** 드롭다운 목록에서 선택합니다.

단계 **3** 경우에 따라 **Pause(**일시 중지**)** ( ) 또는 **Play(**재생**)** ( )를 사용하여 시간 범위 제어에서 대시보드를 일시 중지 또는 일시 중지 취소합니다.

대시보드 이름 변경

프로시저

단계 **1** 수정하려는 대시보드를 확인니다. 대시보드 보기, 367 페이지을 참조하십시오.

단계 **2** 이름을 변경할 대시보드를 클릭합니다.

단계 **3** 이름을 입력합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

대시보드 보기

기본적으로 어플라이언스의 홈페이지에는 기본 대시보드가 표시됩니다. 기본 대시보드가 정의되어 있지 않은 경우, 홈페이지는 Dashboard Management(대시보드 관리) 페이지를 표시하는데, 여기에서 표시할 대시보드를 선택할 수 있습니다.

프로시저

언제든지 다음 중 하나를 수행할 수 있습니다.

- 어플라이언스에 대한 기본 대시보드를 보려면 **Overview(**개요**)** > **Dashboards(**대시보드**)**을 선택합니다.
- 특정 대시보드를 보려면 **Overview(**개요**)** > **Dashboards(**대시보드**)**을 선택하고 메뉴에서 해당 대시보드를 선택합니다.
- 모든 사용 가능한 대시보드를 보려면 **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Management(**관리**)**을 선택합니다. 그러면 개별 대시보드 옆에 있는 **View(**보기**)** ( )를 선택하여 대시보드를 볼 수 있습니다.

11 장

상태

다음 항목에서는 Firepower System에서 상태 모니터링을 사용하는 방법에 대해 설명합니다.

상태 모니터링 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

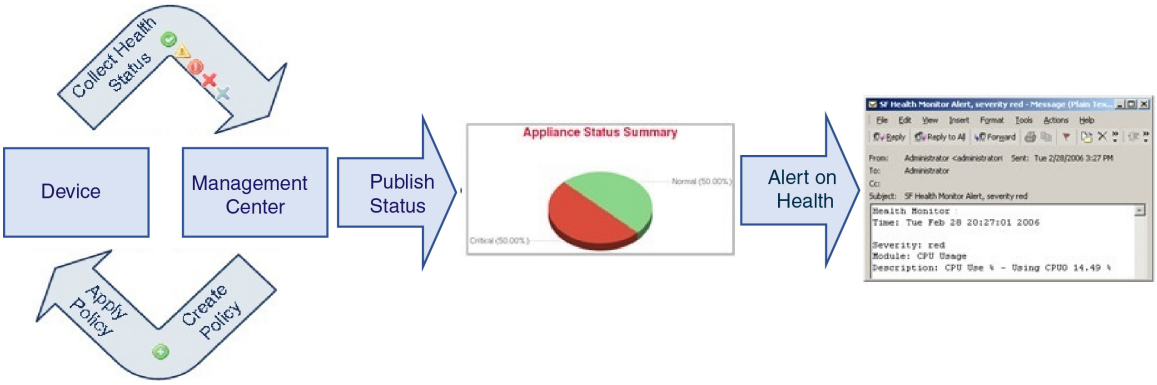
관리자

유지 보수 사용자

상태 모니터링 정보

management center에서 상태 모니터는 다양한 상태 표시기를 추적하고 시스템의 하드웨어 및 소프트웨어가 올바르게 작동하는지 확인합니다. 상태 모니터를 사용하여 구축에서 중요한 기능의 상태를 확인할 수 있습니다.

알림을 위해 상태 모듈을 실행하는 빈도를 구성할 수 있습니다. Management Center는 시계열 데이터 수집도 지원합니다. 디바이스와 디바이스 상태 모듈에서 시계열 데이터를 수집하는 빈도를 구성할 수 있습니다. 디바이스 모니터는 기본적으로 여러 미리 정의된 상태 모니터 대시보드에서 이러한 메트릭을 보고합니다. 메트릭 데이터는 분석을 위해 수집되므로 경고가 연결되지 않습니다.



상태 모니터를 사용하여 *health policy(*상태 정책*)*라고 하는 테스트 집합을 생성하고 하나 이상의 어플라이언스에 상태 정책을 적용할 수 있습니다. *health modules(*상태 모듈*)*라고도 하는 테스트는 지정한 기준을 테스트하는 스크립트입니다. 테스트를 활성화 또는 비활성화하거나 테스트 설정을 변경하여 상태 정책을 수정할 수 있으며, 더 이상 필요하지 않은 상태 정책을 삭제할 수 있습니다. 선택한 어플라이언스를 제외하여 해당 메시지를 억제할 수도 있습니다.

상태 정책의 테스트는 구성한 간격으로 자동 실행됩니다. 필요에 따라 모든 테스트 또는 특정 테스트를 실행할 수 있습니다. 상태 모니터는 구성한 테스트 조건을 기반으로 상태 이벤트를 수집합니다.

참고 모든 어플라이언스는 하드웨어 알람 상태 모듈을 통해 하드웨어 상태를 자동으로 보고합니다. management center도 기본 상태 정책에 구성된 모듈을 사용하여 상태를 자동으로 보고합니다. Appliance Heartbeat 모듈과 같은 일부 상태 모듈은 management center에서 실행되어 management center의 매니지드 디바이스의 상태를 보고합니다. 상태 모듈에서 매니지드 디바이스 상태를 제공하려면 모든 상태 정책을 디바이스에 구축해야 합니다.

상태 모니터를 사용하여 전체 시스템, 특정 어플라이언스 또는 다중 도메인 구축에서 특정 도메인의 상태 정보에 액세스할 수 있습니다. Health Monitor(상태 모니터) 페이지의 육각 차트 및 상태 테이블은 management center를 포함해 네트워크의 모든 어플라이언스 상태를 시각적으로 요약하여 보여줍니다. 개별 어플라이언스 상태 모니터에서는 특정 어플라이언스의 상태로 드릴다운할 수 있습니다.

완전히 사용자 지정 가능한 이벤트 보기에서는 상태 모니터에서 수집한 상태 이벤트를 빠르고 쉽게 분석할 수 있습니다. 이러한 이벤트 보기에서는 이벤트 데이터를 검색하고 볼 수 있으며, 조사 중인 이벤트와 관련이 있을 수 있는 다른 정보에 액세스할 수 있습니다. 예를 들어 CPU 사용량이 특정 비율에 도달한 모든 경우를 보려면 CPU 사용량 모듈을 검색하고 비율 값을 입력합니다.

상태 이벤트에 대한 응답으로 이메일, SNMP 또는 syslog 알림을 구성할 수도 있습니다. *health alert(*상태 알림*)*는 표준 알림과 상태 레벨을 연결한 것입니다. 예를 들어, 하드웨어 과부하 때문에 어플라이언스가 실패하지 않도록 하려면 이메일 알림을 설정할 수 있습니다. 그런 다음 CPU, 디스크 또는 메모리 사용량이 어플라이언스에 적용된 상태 정책에서 구성한 경고(Warning) 레벨에 도달할 때마다

이메일 알림을 트리거하는 상태 알림을 생성할 수 있습니다. 반복해서 알림을 수신하는 횟수를 최소화하려면 알림 임계값을 설정할 수 있습니다.

참고 상태 모니터링은 상태 이벤트 발생 후 상태 알림을 생성하는 데 5~6분 정도 걸릴 수 있습니다.

또한 고객 지원에서 요청할 경우 어플라이언스에 대한 문제 해결 파일을 생성할 수도 있습니다.

상태 모니터링은 관리 활동이므로 관리자 사용자 역할 권한이 있는 사용자만 시스템 상태 데이터에 액세스할 수 있습니다.

상태 모듈

*Health modules(*상태 모듈*)* 또는 *health tests(*상태 테스트*)*는 상태 정책에서 지정한 기준을 테스트합니다.

표 ***19:*** 상태 모듈*(*모든 어플라이언스*)*

모듈	설명
CPU 사용량(코어당)	이 모듈은 모든 코어의 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
디스크 상태	이 모듈은 하드 디스크의 성능과 어플라이언스의 악성코드 스토리지 팩(설치된 경우)을 점검합니다. 이 모듈에서는 하드 디스크와 RAID 컨트롤러(설치된 경우)가 실패할 위험이 있을 때 또는 악성코드 스토리지 팩이 아닌 추가 하드 드라이브가 설치된 경우 Warning(노란색) 상태 알림을 생성합니다. 설치된 악성코드 스토리지 팩을 탐지할 수 없는 경우에는 Alert(빨간색) 상태 알림이 생성됩니다.

모듈	설명
디스크 사용	이 모듈은 어플라이언스 하드 드라이브 및 악성코드 스토리지 팩의 디스크 사용량을 모듈에 대해 구성된 제한과 비교하고, 사용량이 모듈에 대해 구성된 비율을 초과하면 알림을 전송합니다. 또한 시스템이 모니터링되는 디스크 사용량 카테고리에서 과도하게 파일을 삭제하는 경우 또는 모듈 임계값을 기반으로 그러한 카테고리 외의 디스크 사용량이 과도한 수준에 도달하는 경우에도 알림을 전송합니다. 디스크 사용량 알림의 문제 해결 시나리오에 대한 내용은 이벤트 상태 모니터 알림의 디스크 사용량 및 소모, 446 페이지의 내용을 참조하십시오. 디스크 사용량 상태 모듈을 사용 하 여 기기에서 `/및/` 또는 `볼륨` 파티션의 디스크 사용량을 모니터링 하 고 배수 빈도를 추적 합니다. 디스크 사용 모듈은 `/boot` 파티션을 모니터링되는 파티션으로 나열하지만 파티션의 크기는 정적이므로 모듈은 부팅 파티션에서 경고를 보내지 않습니다. 주의 파티션/볼륨에 대한 관리되지 않는 디스크 사용량이 높음에 대한 알림이 상태 정책에 지정된 위험 또는 경고 임계값보다 낮더라도 시스템에서 수동으로 삭제해야 하는 파일이 있음을 나타낼 수 있습니다. 이러한 알림을 받으면 TAC에 문의하십시오.
파일 시스템 무결성 확인	이 모듈은 시스템에서 CC 모드 또는 UCAPL 모드가 활성화되어 있거나 시스템이 DEV 키로 서명된 이미지를 실행하는 경우 파일 시스템 무결성 검사를 수행하고 실행합니다. 이 모듈은 기본적으로 활성화되어 있습니다.
상태 모니터 프로세스	이 모듈은 상태 모니터 자체의 상태를 모니터링하고, management center에서 마지막으로 상태 이벤트를 수신한 후 시간(분 단위)이 Warning(경고) 또는 Critical(심각) 한도를 초과하면 알림을 전송합니다.
상태 모니터 프로세스	이 모듈은 상태 모니터 자체의 상태를 모니터링하고, management center에서 마지막으로 상태 이벤트를 수신한 후 시간(분 단위)이 Warning(경고) 또는 Critical(심각) 한도를 초과하면 알림을 전송합니다.

모듈	설명
인터페이스 상태	이 모듈은 디바이스가 현재 트래픽을 수집하는지 확인하고, 물리적 인터페이스와 집계 인터페이스의 트래픽 상태를 기준으로 알림을 제공합니다. 물리적 인터페이스의 경우 정보에 인터페이스 이름, 링크 상태 및 대역폭이 포함됩니다. 집계 인터페이스의 경우 정보에 인터페이스 이름, 활성 링크의 수, 총 집계 대역폭이 포함됩니다. 참고 이 모듈은 HA 스탠바이 디바이스 트래픽 흐름도 모니터링합니다. 스탠바이 디바이스는 트래픽을 수신하지 않는 것으로 알려져 있지만, management center는 인터페이스에서 트래픽을 수신하고 있지 않음을 알립니다. 포트 채널의 일부 하위 인터페이스에서 트래픽을 수신하지 않는 경우에도 동일한 알림 원칙이 적용됩니다. **show interface** CLI 명령을 사용하여 디바이스의 인터페이스 통계를 확인하는 경우 CLI 명령 결과의 입력 및 출력 속도는 인터페이스 모듈에 표시되는 트래픽 속도와 다를 수 있습니다. 이 모듈은 Snort 성능 모니터링의 값에 따라 트래픽 속도를 표시합니다. Snort 성능 모니터링 및 management center 인터페이스 통계의 샘플링 간격은 서로 다릅니다. 샘플링 간격의 차이로 인해 management center GUI의 처리량 값은 threat defense CLI 결과에 표시되는 처리량 값과 다를 수 있습니다.
로컬 악성코드 분석	이 모듈은 로컬 악성코드 분석에 대한 ClamAV 업데이트를 모니터링합니다.
메모리 사용	이 모듈은 어플라이언스의 메모리 사용량을 모듈에 대해 구성된 제한과 비교하고, 사용량이 모듈에 대해 구성된 레벨을 초과하면 알림을 전송합니다. 메모리가 4GB를 넘는 어플라이언스의 경우 프리셋 알림 임계값은 시스템 문제를 일으킬 수 있는 사용 가능한 메모리의 비율을 고려하는 공식을 기반으로 합니다. 4GB를 넘는 어플라이언스에서는 Warning 임계값과 Critical 임계값 사이의 간격이 매우 좁기 때문에 Cisco에서는 **Warning Threshold %(**경고 임계값 **%)** 값을 50으로 수동으로 설정할 것을 권장합니다. 이렇게 하면 문제를 해결할 수 있도록 적시에 어플라이언스에 대한 메모리 알림을 받을 수 있습니다. 임계값 계산 방법에 대한 추가 정보는 상태 모니터 알림의 메모리 사용량 임계값, 445 페이지의 내용을 참조하십시오. 버전 6.6.0부터 management center virtual를 버전 6.6.0 이상으로 업그레이드하는 데 필요한 최소 RAM은 28GB이며, management center virtual 구축에 권장되는 RAM은 32GB입니다. 기본 설정을 줄이지 않는 것이 좋습니다. 대부분의 management center virtual 인스턴스의 경우 32GB RAM, management center virtual 300의 경우 64GB가 필요합니다(VMware만 해당). 주의 RAM이 부족하여 management center virtual 구축에 할당되면 상태 모니터에서 중요 알림이 생성됩니다. 복잡한 액세스 제어 정책 및 규칙을 적용할 경우 상당한 리소스가 소모되어 성능이 저하될 수 있습니다.

모듈	설명
프로세스 상태	이 모듈은 어플라이언스의 프로세스가 프로세스 관리자 외부에서 종료되는지를 확인합니다. 프로세스가 프로세스 관리자 외부에서 고의로 종료되면 모듈 상태가 Warning으로 변경되며, 모듈이 다시 실행되고 프로세스가 다시 시작될 때까지 상태 이벤트 메시지에 프로세스가 종료되었음이 표시됩니다. 프로세스가 프로세스 관리자 외부에서 비정상적으로 종료되거나 충돌되면 모듈 상태가 Critical로 변경되며, 모듈이 다시 실행되고 프로세스가 다시 시작될 때까지 상태 이벤트 메시지에 프로세스가 종료되었음이 표시됩니다.

모듈	설명
디바이스에서 위협 데이터 업데이트	디바이스가 위협을 탐지하는 데 사용하는 특정 인텔리전스 데이터 및 구성은 30분마다 클라우드의 management center에서 업데이트됩니다. 이 모듈은 사용자가 지정한 기간 내에 해당 정보가 디바이스에 업데이트 되지 않은 경우 경고를 보냅니다. 모니터링되는 업데이트는 다음을 포함합니다. • 로컬 URL 카테고리 및 평판 데이터 • 보안 인텔리전스 URL 목록 및 피드. Threat Intelligence Director의 전역 차단 및 차단 안 함 목록 및 URL이 포함됩니다. • 보안 인텔리전스 네트워크 목록 및 피드(IP 주소). Threat Intelligence Director의 전역 차단 및 차단 안 함 목록 및 IP 주소가 포함됩니다. • 보안 인텔리전스 DNS 목록 및 피드. Threat Intelligence Director의 전역 차단 및 차단 안 함 목록 및 도메인이 포함됩니다. • 에서 로컬 악성코드 분석 서명(ClamAV) • Threat Intelligence Director의 SHA 목록. **Objects(**개체**) > Object Management(**개체 관리**) > Security Intelligence(**보안 인텔리전스**) > Network Lists and Feeds(**네트워크 목록 및 피드**)** 페이지에 나와 있습니다. • 동적 분석 설정. **Integration(**통합**) > AMP > Dynamic Analysis Connections(**동적 분석 연결**)** 페이지에 구성되어 있습니다. • 캐시된 URL 만료와 관련한 Threat Configuration(위협 구성) 설정. **Integration(**통합**) > Other Integrations(**기타 통합**) > Cloud Services(**클라우드 서비스**)** 페이지의 Cached URLs Expire(캐시된 URL 만료) 설정을 포함합니다. (URL 캐시에 대한 업데이트는 이 모듈에서 모니터링하지 않습니다.) • 이벤트 전송에서의 Cisco Cloud와의 통신 이슈 **Integration(**통합**) > Other Integrations(**기타 통합**) > Cloud Services(**클라우드 서비스**)** 페이지의 **Cisco Cloud** 상자를 참고하십시오. 참고 Threat Intelligence Director 업데이트는 TID가 시스템에 구성되어 있고 피드가 있는 경우에만 포함됩니다. 기본적으로 이 모듈은 1시간 후에 warning(경고) 알림을 보내고 24시간 후에 critical(심각) 알림을 보냅니다. 이 모듈에서 management center 또는 어떠한 디바이스에 실패가 표시되는 경우, management center가 디바이스에 연결되는지 확인합니다.

표 ***20: Management Center*** 상태 모듈

모듈	설명
AMP for Endpoints 상태	이 모듈은 management center가 초기 연결에 성공한 후 AMP 클라우드 또는 Cisco AMP 프라이빗 클라우드에 연결할 수 없거나 프라이빗 클라우드가 공용 AMP 클라우드에 연결할 수 없는 경우에 경고를 보냅니다. 또한 Secure Endpoint 관리 콘솔을 사용하여 AMP 클라우드 연결을 등록 취소하면 경고를 보냅니다.
AMP for Firepower 상태	이 모듈은 다음의 경우에 경고를 보냅니다. • management center은 AMP 클라우드(퍼블릭 또는 프라이빗) 또는 Secure Malware Analytics 클라우드 또는 어플라이언스에 연결할 수 없으며 또는 AMP 프라이빗 클라우드는 퍼블릭 AMP 클라우드에 연결할 수 없습니다. • 연결에 사용되는 암호화 키가 유효하지 않습니다. • 디바이스는 Secure Malware Analytics 클라우드 또는 Secure Malware Analytics 어플라이언스에 연결하여 동적 분석을 위한 파일을 제출할 수 없습니다. • 파일 정책 구성을 기반으로 네트워크 트래픽에서 과도한 수의 파일이 검색됩니다. management center에서 인터넷 연결이 끊어지는 경우, 시스템이 상태 알림을 생성하는 데 최대 30분이 걸릴 수 있습니다.
어플라이언스 하트비트	이 모듈은 어플라이언스에서 어플라이언스 하트비트가 전송되는지 확인하고, 어플라이언스 하트비트 상태를 기반으로 알림을 전송합니다.
데이터베이스 크기	이 모듈은 구성 데이터베이스 크기를 확인하고, 크기가 모듈에 대해 구성된 값(기가바이트)을 초과하면 알림을 보냅니다.
검색 호스트 한도	이 모듈은 management center가 모니터할 수있는 호스트의 수가 한계에 가까워지고 모듈에 구성된 경고 수준에 따라 경고를 할지 결정합니다. 자세한 내용은 Firepower System 호스트 제한의 내용을 참고하십시오.
이벤트 백로그 상태	이 모듈은 디바이스에서 management center로의 전송을 기다리는 이벤트 데이터의 백로그가 30분 이상 지속적으로 증가한 경우 알림을 표시합니다. 백로그를 줄이려면 대역폭을 평가하고 이벤트 기록을 줄이는 것이 좋습니다.
이벤트 모니터	이 모듈은 management center에 대한 전체 수신 이벤트 비율을 모니터링합니다.
이벤트 스트림 상태	이 모듈은 management center에서 Event Streamer를 사용하는 서드파티 클라이언트 애플리케이션에 대한 연결을 모니터링합니다.
하드웨어 통계	이 모듈은 management center 하드웨어 엔티티의 상태, 즉 팬 속도, 온도 및 전원 공급 장치를 모니터링합니다. 이 모듈은 임계값이 구성된 Warning(경고) 또는 Critical(심각) 제한을 초과할 경우 알림을 전송합니다.

모듈	설명
ISE 연결 모니터	이 모듈은 Cisco ISE(Identity Services Engine)와 management center간의 서버 연결 상태를 모니터링 합니다. ISE는 추가 사용자 데이터, 디바이스 유형 데이터, 디바이스 위치 데이터, SGT(Security Group Tags) 및 SXP(Security Exchange Protocol) 서비스를 제공합니다.
라이선스 모니터	이 모듈은 라이선스 만료를 모니터링합니다.
Management Center 액세스 구성 변경	이 모듈은 **configure network management-data-interface** 명령을 사용하여 management center에서 직접 수행한 액세스 구성 변경을 모니터링합니다.
Management Center HA 상태	이 모듈은 management center의 고가용성 상태를 모니터링하고 경고합니다. management center 고가용성이 설정되지 않은 경우, HA 상태는 `Not in HA(HA가 아님)` 입니다. 참고 이 모듈은 이전에 management center의 HA 상태를 제공했던 HA 상태 모듈을 대체합니다. 버전 7.0에서는 매니지드 디바이스에 대한 HA 상태를 추가했습니다.
MySQL 통계	이 모듈은 데이터베이스 크기, 활성 연결 수 및 메모리 사용을 포함하여 MySQL 데이터베이스의 상태를 모니터링합니다. 기본적으로 비활성화되어 있습니다.
전력 공급 장치	이 모듈은 어플라이언스의 전력 공급 장치를 교체해야 하는지 여부를 확인하고, 전력 공급 장치 상태를 기반으로 알림을 전송합니다.
RabbitMQ 상태	이 모듈은 RabbitMQ에 대한 다양한 통계를 수집합니다.
RRD 서버 프로세스	이 모듈은 시계열 데이터를 저장하는 라운드 로빈 데이터 서버가 제대로 실행되고 있는지 확인합니다. 마지막으로 업데이트된 이후 RRD 서버가 다시 시작되면 알림이 전송됩니다. RRD 서버 다시 시작의 연속 업데이트 수가 모듈 컨피그레이션에 지정된 수에 도달하면 Critical 또는 Warning 상태로 들어가게 됩니다.
보안 인텔리전스	이 모듈은 보안 인텔리전스를 사용 중이고 management center가 피드를 업데이트할 수 없거나 피드 데이터가 손상되었거나 인식할 수 없는 IP 주소를 포함하는 경우 알림을 표시합니다. 디바이스의 위협 데이터 업데이트 모듈도 참조하십시오.
스마트 라이선스 모니터	이 모듈은 스마트 라이선싱 상태를 모니터링합니다.
스마트 라이선스 모니터	이 모듈은 다음의 경우에 경고를 보냅니다. • 스마트 라이선싱 에이전트(Smart Agent)와 스마트 소프트웨어 매니저 간에 통신 오류가 있습니다. • 제품 인스턴스 등록 토큰이 만료되었습니다. • 스마트 라이선스 사용량이 미준수 상태입니다. • 스마트 라이선스 권한 부여 또는 평가 모드 만료 되었습니다.
Sybase 통계	이 모듈은 데이터베이스 크기, 활성 연결 수 및 메모리 사용을 포함하여 management center에서 Sybase 데이터베이스의 상태를 모니터링합니다.

모듈	설명
시계열 데이터(RRD) 모니터링	이 모듈은 시계열 데이터(예: 상관관계 이벤트 카운트)가 저장된 디렉토리에 손상된 파일이 있는지를 추적하고, 손상되어 제거된 것으로 파일에 플래그가 표시되는 경우 알림을 전송합니다.
동기화 상태	이 모듈은 NTP를 사용하여 시간을 가져오는 디바이스 시계와 NTP 서버에 있는 시계의 동기화를 추적하고, 두 시계 간 차이가 10초를 넘으면 알림을 전송합니다.
확인할 수 없는 그룹 모니터	정책에 사용된 확인되지 않은 그룹을 모니터링합니다.
URL 필터링 모니터	management center가 다음에 실패하는 경우 이 모듈이 경고를 보냅니다. • Cisco Cloud에 등록 • Cisco Cloud에서 URL 위협 데이터 업데이트 다운로드 • 완전한 URL 조회 이러한 경고에 대해 시간 임계값을 구성할 수 있습니다. 디바이스의 위협 데이터 업데이트 모듈도 참조하십시오.
VPN 통계	이 모듈은 Firepower 디바이스 간의 사이트 대 사이트 및 RA VPN 터널을 모니터링합니다.
VPN 상태	이 모듈은 Firepower 디바이스 간에 하나 이상의 VPN 터널이 다운되면 알림을 보냅니다. 이 모듈을 다음을 추적합니다. • Site-to-Site VPN Secure Firewall Threat Defense • 원격 액세스 VPN Secure Firewall Threat Defense

표 ***21:*** 디바이스 상태 모듈

모듈	설명
AMP 연결 상태	이 모듈은 threat defense가 초기 연결에 성공한 후 AMP 클라우드 또는 Cisco AMP 프라이빗 클라우드에 연결할 수 없거나 프라이빗 클라우드가 공용 AMP 클라우드에 연결할 수 없는 경우에 경고를 보냅니다. 기본적으로 비활성화되어 있습니다.
AMP Threat Grid 연결성	모듈은 초기 연결에 성공한 후 threat defense이 AMP Threat Grid 클라우드에 연결할 수 없는 경우 경고를 표시합니다.
ASP 삭제	이 모듈은 데이터 플레인 가속화된 보안 경로에 의해 삭제된 연결을 모니터링합니다.
AAB(Automatic Application Bypass)	이 모듈은 우회된 탐지 애플리케이션을 모니터링합니다.

모듈	설명
클러스터/HA 페일오버 상태	이 모듈은 디바이스 클러스터의 상태를 모니터링합니다. 이 모듈은 다음의 경우 경고를 보냅니다. • 새 기본 유닛이 클러스터에 선택됩니다. • 새 보조 유닛에서 클러스터에 가입합니다. • 기본 또는 보조 유닛이 클러스터를 떠납니다.
설정 리소스 사용률	이 모듈은 구축된 구성의 크기로 인해 디바이스에서 메모리가 부족해질 위험이 있는지를 알려줍니다. 알림에는 구성에 필요한 메모리의 양과 사용 가능한 메모리를 초과하는 양이 표시됩니다. 이 경우 구성을 재평가하십시오. 종종 액세스 제어 규칙 또는 침입 정책의 수 또는 복잡성을 줄일 수 있습니다. **Snort** 메모리 할당 • *Total Snort Memory(*총 *Snort* 메모리*)*는 threat defense 디바이스에서 실행 중인 Snort 2 인스턴스에 할당된 메모리를 나타냅니다. • *Available Memory(*사용 가능한 메모리*)*는 시스템에서 Snort 2 인스턴스에 할당한 메모리를 나타냅니다. 이 값은 총 *Snort* 메모리와 다른 모듈용으로 예약된 통합 메모리 간의 차이가 아닙니다. 이 값은 몇 가지 다른 계산 후에 파생된 다음 Snort 2 프로세스의 수로 나뉩니다. *Available Memory(*사용 가능한 메모리*)* 값이 음수이면 Snort 2 인스턴스에 구축된 구성에 대한 메모리가 충분하지 않음을 나타냅니다. 지원은 Cisco Technical Assistance Center (TAC)에 문의하십시오.
연결 통계	이 모듈은 연결 통계 및 NAT 변환 수를 모니터링합니다.
CPU 사용 데이터 플레인	이 모듈은 디바이스에 있는 모든 데이터 플레인의 평균 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
CPU 사용량 Snort	이 모듈은 디바이스에 있는 Snort 프로세스의 평균 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
CPU 사용량 시스템	이 모듈은 디바이스에 있는 모든 시스템의 평균 CPU 사용량이 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 설정된 비율을 초과하면 알림을 전송합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
중요한 프로세스 통계	이 모듈은 중요한 프로세스의 상태, 리소스 소비 및 재시작 횟수를 모니터링합니다.

모듈	설명
구축된 컨피그레이션 통계	이 모듈은 구축된 설정에 대한 통계(예: ACE 수 및 IPS 규칙)를 모니터링합니다.
Firepower Platform 결함	이 모듈은 Firepower 1000, 2100 및 3000 Series 디바이스의 플랫폼 결함에 대한 알림을 생성합니다. 결함은 management center에서 관리하는 변경 가능한 개체입니다. 각 결함은 Firepower 1000, 2100 및 3000 인스턴스의 장애 또는 경고 임계값 증가를 나타냅니다. 결함의 라이프사이클 중에 상태 또는 심각도가 서로 변경될 수 있습니다. 각 결함에는 결함이 제기된 시점에 영향을 받은 개체의 운영 상태에 대한 정보가 포함됩니다. 결함이 과도적이고 실패가 해결될 경우, 개체가 기능적 상태로 전환됩니다. 자세한 내용은*Cisco Firepower 1000 /2100 FXOS* 결함 및 오류 메시지 가이드를 참조하십시오.
플로우 오프로드 통계	이 모듈은 관리되는 디바이스에 대한 하드웨어 플로우 오프로드 통계를 모니터링합니다.
하드웨어 경보	이 모듈은 하드웨어의 교체가 필요한지 여부를 판단하고, 하드웨어 상태를 기반으로 알림을 전송합니다. 이 모듈은 하드웨어 관련 데몬의 상태도 보고합니다.
인라인 링크 불일치 경보	이 모듈은 인라인 집합과 관련된 포트를 모니터링하고, 인라인 쌍의 두 인터페이스가 서로 다른 속도를 협상하는 경우 알림을 전송합니다.
침입 및 파일 이벤트 비율	이 모듈은 초당 침입 이벤트 수를 모듈에 대해 구성된 제한과 비교하고, 제한을 초과하는 경우 알림을 전송합니다. 침입 및 파일 이벤트 비율이 0이면 침입 프로세스가 다운되거나 매니지드 디바이스가 이벤트를 전송하지 못할 수 있습니다. **Analysis(**분석**)** > **Intrusions(**침입**)** > **Events(**이벤트**)**을 선택하고 이벤트가 디바이스에서 수신되는지 확인합니다. 일반적으로 네트워크 세그먼트의 이벤트 속도는 초당 이벤트 20개입니다. 이 평균 속도의 네트워크 세그먼트에서 Events per second(Critical)는 `50`, Events per second (Warning)는 `30`으로 설정해야 합니다. 시스템에 대한 제한을 확인하려면 디바이스의 Statistics(통계) 페이지에서 Events/Sec 값을 찾고(시스템 (⚙) > **Monitoring(**모니터링**)** > **Statistics(**통계**)**), 다음 공식을 사용하여 제한을 계산합니다. • Events per second (Critical) = Events/Sec * 2.5 • Events per second (Warning) = Events/Sec * 1.5 두 가지 제한 중 하나에 대해 설정할 수 있는 최대 이벤트 수는 999이며, Critical 제한이 Warning 제한보다 높아야 합니다.
링크 상태 전파	ISA 3000에만 해당. 페어링된 인라인 집합의 링크가 실패하는 경우를 확인하고 링크 상태 전파 모드를 트리거합니다. 링크 상태가 쌍으로 전파되면 해당 모듈에 대한 상태 분류가 Critical로 변경되고 다음과 같은 메시지가 나타납니다. `Module Link State Propagation: ethx_ethy is Triggered` 여기서 `x`및 `y`는 쌍을 이룬 인터페이스 번호입니다.

모듈	설명
메모리 사용량 데이터 플레인	이 모듈은 데이터 플레인 프로세스에서 사용하는 할당된 메모리의 백분율을 확인하고 메모리 사용량이 모듈에 대해 설정된 백분율을 초과할 때 경고를 표시합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
메모리 사용량 Snort	이 모듈은 Snort 프로세스에서 사용하는 할당된 메모리의 백분율을 확인하고 메모리 사용량이 모듈에 대해 설정된 백분율을 초과할 때 경고를 표시합니다. **Warning Threshold %(**경고 임계값 **%)** 기본값은 80입니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 90입니다.
네트워크 카드 재설정	이 모듈은 하드웨어 장애 때문에 다시 시작된 네트워크 카드를 확인하고, 재설정이 발생하면 알림을 전송합니다.
NTP 통계	이 모듈은 매니지드 디바이스의 NTP 클럭 동기화 상태를 모니터링합니다. 기본적으로 비활성화되어 있습니다.
영역	영역 또는 사용자 불일치에 대한 경고 임계값을 설정할 수 있습니다. • 사용자 불일치: 사용자가 다운로드되지 않고 management center에 보고됩니다. 사용자 불일치가 발생하는 일반적인 이유는 사용자가 management center 다운로드에서 제외된 그룹에 속하기 때문입니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 논의된 정보를 검토합니다. • 영역 불일치: 사용자가 management center의 알 수 없는 영역에 해당하는 도메인에 로그인합니다. 자세한 내용은Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오. 이 모듈은 또한 영역당 지원되는 다운로드된 사용자의 최대 수보다 많은 사용자를 다운로드하려고 할 때 상태 알림을 표시합니다. 단일 영역에 대해 다운로드되는 최대 사용자 수는 관리 센터 모델에 따라 다릅니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사용자 제한을 참조하십시오.
라우팅 통계	이 모듈은 라우팅 테이블의 현재 상태를 모니터링합니다.
Snort3 통계	이 모듈은 이벤트, 플로우 및 패킷에 대한 Snort3 통계를 수집하고 모니터링합니다.

모듈	설명
Snort ID 메모리 사용량	메모리 사용량이 모듈에 대해 설정된 레벨을 초과할 때 Snort ID 처리 및 알림에 대한 경고 임계값을 설정할 수 있습니다. **Critical Threshold %(**위험 임계값 **%)** 기본값은 `80`입니다. 이 상태 모듈은 Snort에서 사용자 ID 정보에 사용된 총 공간을 추적합니다. 여기에는 현재 메모리 사용량 세부 정보, 총 사용자-IP 바인딩 수 및 사용자-그룹 매핑 세부 정보가 표시됩니다. Snort는 이러한 세부 정보를 파일에 기록합니다. 메모리 사용량 파일을 사용할 수 없는 경우 이 모듈에 대한 Health Alert(상태 알림)에 *Waiting for data(*데이터 대기 중*)*가 표시됩니다. 이는 신규 설치 또는 주요 업데이트, Snort2에서 Snort3 또는 그 반대로의 전환 또는 주요 정책 구축으로 인해 Snort 재시작 중에 발생할 수 있습니다. 상태 모니터링 주기에 따라 그리고 파일을 사용할 수 있는 경우 경고가 사라지고 상태 모니터에 이 모듈의 상세정보가 녹색으로 표시됩니다.
Snort 재구성 탐지	이 모듈은 디바이스 재구성이 실패한 경우 경고를 보냅니다.
Snort 통계	이 모듈은 이벤트, 플로우 및 패킷에 대한 Snort 통계를 모니터링합니다.
SSE 연결 상태	모듈은 초기 연결에 성공한 후 threat defense이 SSE 클라우드에 연결할 수 없는 경우 경고를 표시합니다. 기본적으로 비활성화되어 있습니다.
Threat Defense HA(스플릿 브레인 검사)	이 모듈은 threat defense의 고가용성 상태를 모니터링하고 경고하며 분할 브레인 시나리오에 대한 상태 경고를 제공합니다. threat defense 고가용성이 설정되지 않은 경우, HA 상태는 `Not in HA(HA가 아님)` 입니다.
XTLS 카운터	이 모듈은 XTLS/SSL 플로우, 메모리 및 캐시 효율성을 모니터링합니다. 기본적으로 비활성화되어 있습니다.

상태 모니터링 구성

프로시저

단계 **1** 상태 모듈, 371 페이지에 설명된 대로 모니터링 하려는 상태 모듈을 결정합니다.

Firepower System에 있는 각 어플라이언스 종류에 대해 특정 정책을 설정하고 해당 어플라이언스에 맞는 테스트만 활성화할 수 있습니다.

팁 모니터링 동작을 사용자 지정하지 않고 빠르게 상태 모니터링을 활성화하려면 이 용도로 제공되는 기본 정책을 적용할 수 있습니다.

단계 **2** 상태 정책 생성, 383 페이지에 설명된 대로 상태를 추적하려는 각 어플라이언스에 상태 정책을 적용합니다.

단계 **3** (선택 사항). 상태 모니터 알림 생성, 390 페이지에 설명된 대로 상태 모니터 알림을 구성합니다.

상태 레벨이 특정 상태 모듈에 대해 특정 심각도에 도달할 때 트리거되는 이메일, syslog 또는 SNMP 알림을 설정할 수 있습니다.

상태 정책

상태 정책에는 여러 모듈용으로 구성된 상태 테스트 기준이 포함되어 있습니다. 각 어플라이언스에 대해 어떤 상태 모듈을 실행할지 제어할 수 있으며, 각 모듈에 의해 실행되는 테스트에서 사용할 특정 제한을 구성할 수 있습니다.

상태 정책을 구성할 때에는 해당 정책에 대해 각 상태 모듈을 활성화할지 여부를 결정합니다. 또한 각 사용 가능 모듈에서 프로세스의 상태를 평가 하는 때마다 보고할 상태를 제어 하는 조건을 선택합니다.

시스템의 모든 어플라이언스에 적용할 수 있는 하나의 상태 정책을 생성하거나, 특정 어플라이언스에 적용하고자 하는 각 상태 정책을 사용자 지정하거나, 제공되는 기본 상태 정책을 사용할 수 있습니다. 다중 도메인 구축에서, 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

기본 상태 정책

management center설정 프로세스에서는 초기 상태 정책을 생성하고 적용하며, 모든 상태 모듈이 아닌 대부분의 사용 가능한 상태 모듈이 활성화됩니다. 시스템은 management center에 추가된 디바이스에도 이 초기 정책을 적용합니다.

이 초기 상태 정책은 기본 상태 정책을 기반으로 합니다. 이 정책은 보거나 편집할 수 없지만 맞춤형 상태 정책을 생성할 때 복사할 수 있습니다.

업그레이드 및 기본 상태 정책

management center을 업그레이드할 때 모든 새 상태 모듈이 초기 상태 정책, 기본 상태 정책 및 기타 사용자 지정 상태 정책을 포함하여 모든 상태 정책에 추가됩니다. 일반적으로 새 상태 모듈은 활성화된 상태로 추가됩니다.

참고 새 상태 모듈에서 모니터링 및 알림을 시작하려면 업그레이드 후 상태 정책을 다시 적용합니다.

상태 정책 생성

어플라이언스와 함께 사용할 상태 정책을 사용자 지정하려면 새 정책을 생성할 수 있습니다. 초기에는 정책의 설정이 새 정책의 기반으로 선택한 상태 정책에서 오는 설정으로 채워집니다. 정책을 수정하여 정책 내에서 모듈 활성화 또는 비활성화와 같은 환경 설정을 지정하고, 필요에 따라 각 모듈에 대한 알림 기준을 변경하고, 실행 시간 간격을 지정할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오. 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Policy(**정책**)**을(를) 선택합니다.

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다.

단계 **3** 정책의 이름을 입력합니다.

단계 **4** 새 정책의 기본으로 사용할 기존 정책을 **Base Policy(**기본 정책**)** 드롭다운 목록에서 선택합니다.

단계 **5** 이 정책에 대한 설명을 입력합니다.

단계 **6** **Save(**저장**)**를 선택합니다.

다음에 수행할 작업

- 상태 정책 적용, 384 페이지에 설명된 대로 디바이스에 상태 정책을 적용합니다.
- 상태 정책 수정, 385 페이지에 설명된 대로 정책을 편집하여 모듈 레벨 정책 설정을 지정합니다.

상태 정책 적용

어플라이언스에 상태 정책을 적용하면, 정책에서 활성화한 모든 모듈에 대한 상태 테스트가 어플라이언스의 프로세스 및 하드웨어의 상태를 모니터링합니다. 상태 테스트는 정책에 구성된 간격으로 계속 실행되면서 어플라이언스에 대한 상태 데이터를 수집한 다음 management center로 전달합니다.

상태 정책에서 모듈을 활성화한 다음 상태 테스트가 필요하지 않은 어플라이언스에 정책을 적용하면, 상태 모니터는 해당 상태 모듈의 상태를 비활성으로 보고합니다.

모든 모듈이 비활성화된 정책을 어플라이언스에 적용하면, 적용된 모든 상태 정책이 어플라이언스에서 제거됩니다.

정책이 이미 적용된 어플라이언스에 다른 정책을 적용하면, 새로 적용된 테스트를 기반으로 새 데이터의 표시에 약간의 레이턴시가 발생합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오. 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Policy(**정책**)**을(를) 선택합니다.

단계 **2** 적용하려는 정책 옆에 있는 상태 정책 구축( )를 클릭합니다.

단계 **3** 상태 정책을 적용할 어플라이언스를 선택합니다.

참고 구축한 후에는 어플라이언스에서 정책을 제거할 수 없습니다. 어플라이언스에 대한 상태 모니터링을 중지하려면 모든 모듈이 비활성화된 상태 정책을 생성하여 어플라이언스에 적용합니다.

단계 **4** **Apply(**적용**)**를 클릭하고 선택한 어플라이언스에 정책을 적용합니다.

다음에 수행할 작업

- 필요한 경우 작업 상태를 모니터링합니다. 작업 메시지 보기, 444 페이지를 참조하십시오.

정책이 성공적으로 적용됨과 동시에 어플라이언스의 모니터링이 시작됩니다.

상태 정책 수정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오. 상위 도메인의 관리자는 하위 도메인에 있는 디바이스에 상태 정책을 적용할 수 있습니다. 하위 도메인은 이를 사용하거나 맞춤형 로컬 정책으로 대체합니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Policy(**정책**)**을(를) 선택합니다.

단계 **2** 수정하려는 NAT 정책 옆의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** 정책 이름 및 설명을 편집하려면 정책 이름 옆에 있는 **Edit(**수정**)** ( ) 아이콘을 클릭합니다.

단계 **4** **Health Modules(**상태 모듈**)** 탭에는 모든 디바이스 모듈 및 해당 속성이 표시됩니다. 모듈 및 해당 속성에 대해 제공되는 토글 버튼을 클릭합니다. 켜거나 ( ) 끄면 ( ) 각각 상태 테스트를 활성화하거나 비활성화합니다. 상태 모듈에서 대량 활성화 또는 비활성화 테스트를 실행하려면 **Select All(**모두 선택**)** 토글 버튼을 클릭합니다. 모듈에 대한 자세한 내용은 상태 모듈, 371 페이지을(를) 참조하십시오.

참고
- 모듈 및 속성은 지원 어플라이언스(threat defense, management center 또는 둘 다)로 플래그가 지정됩니다.
- CPU 및 메모리 모듈의 개별 속성을 포함하거나 제외하도록 선택할 수 없습니다.

단계 **5** 해당되는 경우, **Critical(**심각**)**및 **Warning(**경고**)** 임계값 백분율을 설정합니다.

단계 **6** **Run Time Intervals(**실행 시간 간격**)** 탭에서 필드에 관련 값을 입력합니다.

- **Health Module Run Interval(**상태 모듈 실행 간격**)** - 상태 모듈을 실행할 빈도입니다. 최소 간격은 5분입니다.
- **Metric Collection Interval(**메트릭 수집 간격**)** - 디바이스 및 해당 상태 모듈에서 시계열 데이터를 수집하는 빈도입니다. 디바이스 모니터는 기본적으로 여러 미리 정의된 상태 모니터 대시보드에서 이러한 메트릭을 보고합니다. 대시보드에 대한 자세한 내용은 대시보드 정보, 345 페이지의 내용을 참조하십시오. 메트릭 데이터는 분석을 위해 수집되므로 경고가 연결되지 않습니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** 상태 정책 적용, 384 페이지에 설명된 대로 해당 어플라이언스에 상태 정책을 적용합니다.

상태를 추적하려는 각 어플라이언스에 상태 정책을 적용합니다. 어플라이언스에 상태 정책을 적용하면, 정책에서 활성화한 모든 모듈에서 어플라이언스의 프로세스 및 하드웨어의 상태가 모니터링되고 관련 데이터가 management center에 전달되니다.

상태 정책 삭제

더 이상 필요 없는 상태 정책을 삭제할 수 있습니다. 어플라이언스에 여전히 적용된 정책을 삭제하면, 다른 정책을 적용할 때까지 정책 설정이 그대로 유지됩니다. 또한 장치에 적용 되는 상태 정책을 삭제 하면 기본 연결 된 알림 응답을 비활성화할 때까지 장치에 적용 되는 모든 상태 모니터링 경고가 활성 상태로 유지 됩니다.

다중 도메인 구축에서는 현재 도메인에서 만든 상태 정책만 삭제할 수 있습니다.

팁 어플라이언스에 대한 상태 모니터링을 중지하려면 모든 모듈이 비활성화된 상태 정책을 생성하여 어플라이언스에 적용합니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Policy(**정책**)**을(를) 선택합니다.

단계 **2** 삭제할 정책 옆의 **Delete(**삭제**)** (🗑)을 클릭한 다음 **Delete health policy (**상태 정책 삭제**)**를 클릭하여 삭제합니다.
성공적으로 삭제했음을 알리는 메시지가 나타납니다.

상태 모니터링에서 디바이스 제외

일반적인 네트워크 유지 보수 과정에서 어플라이언스를 비활성화하거나 일시적으로 사용할 수 없도록 만들 수 있습니다. 이러한 중단은 고의적인 것이므로 해당 어플라이언스의 상태가 management center의 요약 상태에 영향을 미치지 않도록 할 수 있습니다.

어플라이언스나 모듈에 대한 상태 모니터링 상태 보고를 비활성화하려면 상태 모니터 제외 기능을 사용할 수 있습니다. 예를 들어, 네트워크의 한 세그먼트를 사용할 수 없게 될 것임을 알고 있는 경우 해당 세그먼트의 매니지드 디바이스에 대한 상태 모니터링을 일시적으로 비활성화할 수 있습니다. 그러면 디바이스에 대한 연결이 무효화되므로 management center의 상태가 Warning 또는 Critical 상태로 표시되지 않습니다.

상태 모니터링 상태를 비활성화하면 상태 이벤트는 여전히 생성되지만 비활성화된 상태를 갖게 되어 상태 모니터의 상태에 영향을 미치지 않습니다. 어플라이언스나 모듈을 제외 목록에서 제거하면 제외에 있는 동안 생성된 이벤트는 계속해서 비활성 상태를 표시합니다.

어플라이언스에서 일시적으로 상태 이벤트를 비활성화하려면 제외 구성 페이지로 이동하고 디바이스 제외 목록에 어플라이언스를 추가합니다. 설정이 적용되면 시스템은 전체적인 상태를 계산할 때 제외된 어플라이언스를 더 이상 고려하지 않습니다. Health Monitor Appliance Status Summary(상태 모니터 어플라이언스 상태 요약)에는 어플라이언스가 비활성 상태로 나열됩니다.

개별 상태 모듈을 비활성화할 수도 있습니다. 예를 들어 management center에서 호스트 제한에 도달하는 경우, 호스트 제한 상태 메시지를 비활성화할 수 있습니다.

기본 Health Monitor 페이지에서, 특정 상태 행의 화살표를 클릭하여 해당 상태의 어플라이언스 목록을 볼 수 있도록 확장하면 제외된 여러 어플라이언스를 구분할 수 있습니다.

참고 management center에서 Health Monitor 제외 설정은 로컬 구성 설정입니다. 따라서 디바이스를 제외한 다음, 삭제 후 management center에서 다시 등록하는 경우 제외 설정이 계속 유지됩니다. 새롭게 다시 등록한 디바이스는 계속 제외 상태를 유지합니다.

다중 도메인 구축에서 상위 도메인의 관리자는 하위 도메인의 어플라이언스 또는 상태 모듈을 제외할 수 있습니다. 그러나 하위 도메인의 관리자는 상위 구성을 무시하고 해당 도메인의 디바이스에 대한 제외를 지울 수 있습니다.

상태 모니터링에서 어플라이언스 제외

어플라이언스를 개별적으로 또는 그룹, 모델 또는 관련 상태 정책별로 제외할 수 있습니다.

개별 어플라이언스의 이벤트 및 상태를 비활성으로 설정하려면 어플라이언스를 제외할 수 있습니다. 제외 설정이 적용되면 어플라이언스가 Health Monitor Appliance Module Summary(상태 모니터 어플라이언스 모듈 요약)에서 Disabled(비활성)로 표시되고, 어플라이언스에 대한 상태 이벤트에 상태가 Disabled(비활성)로 표시됩니다.

다중 도메인 구축에서 상위 도메인의 어플라이언스를 제외하면 모든 하위 도메인에 대해 어플라이언스가 제외됩니다. 하위 도메인은 이 상속된 구성을 무시하고 제외를 지울 수 있습니다. 전역 수준에서 management center만 제외할 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Exclude(**제외**)**을(를) 선택합니다.

단계 **2** **Add Device(**디바이스 추가**)**를 클릭합니다.

단계 **3** **Device Exclusion(**디바이스 제외**)**대화 상자의 **Available Devices(**사용 가능한 디바이스**)** 아래에서 상태 모니터링에서 제외할 디바이스의 **Add(**추가**)** (⊕)를 클릭합니다.

단계 **4** **Exclude(**제외**)**를 클릭합니다. 선택한 디바이스가 제외 기본 페이지에 표시됩니다.

단계 **5** 제외 목록에서 디바이스를 제거하려면 **Delete(**삭제**)** (🗑)를 클릭합니다.

단계 **6** **Apply(**적용**)**를 클릭합니다.

다음에 수행할 작업

어플라이언스에서 개별 상태 정책 모듈을 제외하려면 상태 정책 모듈 제외, 388 페이지의 내용을 참조하십시오.

상태 정책 모듈 제외

어플라이언스에서 개별 상태 정책 모듈을 제외할 수 있습니다. 모듈의 이벤트가 어플라이언스의 상태를 Warning(경고) 또는 Critical(심각)로 변경하지 못하게 하려면 이 기능을 사용할 수 있습니다.

제외 설정이 적용되면 어플라이언스는 상태 모니터링에서 디바이스에서 제외되는 모듈의 수를 표시합니다.

팁 개별적으로 제외한 모듈은 필요 시 다시 활성화할 수 있도록 계속 추적해야 합니다. 실수로 모듈을 비활성 상태로 남겨 두면 필요한 Warning(경고) 또는 Critical(심각) 메시지를 놓칠 수 있습니다.

다중 도메인 구축에서 상위 도메인의 관리자는 하위 도메인의 상태 모듈을 제외할 수 있습니다. 그러나 하위 도메인의 관리자는 이러한 상위 구성을 무시하고 해당 도메인의 디바이스에 대한 제외를 지울 수 있습니다. 전역 수준에서 management center 상태 모듈만 제외할 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Exclude(**제외**)**를 선택합니다.

단계 **2** 수정하려는 어플라이언스 옆에 있는 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **3** **Exclude Health Modules(**상태 모듈 제외**)** 대화 상자에서는 기본적으로 디바이스의 모든 모듈이 상태 모니터링에서 제외됩니다. 특정 모듈은 특정 디바이스만 적용됩니다. 자세한 내용은 상태 모듈, 371 페이지을 참조 하십시오.

단계 **4** 디바이스의 제외 기간을 지정하려면 **Exclude Period(**제외 기간**)** 드롭다운 목록에서 기간을 선택합니다.

단계 **5** 상태 모니터링에서 제외할 모듈을 선택하려면 **Enable Module Level Exclusion(**모듈 레벨 제외 활성화**)** 링크를 클릭합니다. **Exclude Health Modules(**상태 모듈 제외**)** 대화 상자에 디바이스의 모든 모듈이 표시됩니다. 연결된 상태 정책에 적용할 수 없는 모듈은 기본적으로 비활성화되어 있습니다. 모듈을 제외하려면 다음을 수행합니다.

1. 원하는 모듈 옆에 있는 **Slider(**슬라이더**)(**) 버튼을 클릭합니다.
2. 선택한 모듈의 제외 기간을 지정하려면 **Exclude Period(**제외 기간**)** 드롭다운 목록에서 기간을 선택합니다.

단계 **6** 제외 구성에 대해 **Permanent(**영구**)** 이외의 **Exclude Period(**제외 기간**)**를 선택하는 경우 구성이 만료될 때 자동으로 삭제하도록 선택할 수 있습니다. 이 설정을 활성화하려면 **Auto-delete expire Configurings(**만료된 구성 자동 삭제**)** 확인란을 선택합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** 디바이스 제외 기본 페이지에서 **Apply(**적용**)**를 클릭합니다.

만료된 상태 모니터 제외

디바이스 또는 모듈에 대한 제외 기간이 경과하면 제외를 지우거나 갱신할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Exclude(**제외**)**을(를) 선택합니다.

디바이스 또는 모듈이 알림에서 제외되는 기간의 만료를 나타내는 **Warning(**경고**)** ( ) 아이콘이 디바이스에 표시됩니다.

단계 **2** 디바이스의 제외를 갱신하려면 어플라이언스 옆에 있는 **Edit(**수정**)**( )을 클릭합니다. **Exclude Health Modules(**상태 모듈 제외**)** 대화 상자에서 **Renew(**갱신**)** 링크를 클릭합니다. 디바이스의 제외 기간이 현재 값으로 연장됩니다.

단계 **3** 디바이스를 제외에서 지우려면 어플라이언스 옆에 있는 **Delete(**삭제**)** ( )를 클릭하고 **Remove the device from exclusion(**제외에서 디바이스 제거**)**을 클릭한 다음 **Apply(**적용**)**를 클릭합니다.

단계 **4** 모듈을 갱신하거나 제외에서 지우려면 어플라이언스 옆에 있는 **Edit(**수정**)**( )을 클릭합니다. **Exclude Health Modules(**상태 모듈 제외**)** 대화 상자에서 **Enable Module Level Exclusion(**모듈 레벨 제외 활성화**)** 링크를 클릭한 다음 모듈에 대해 **Renew(**갱신**)** 또는 **Clear(**지우기**)** 링크를 클릭합니다. **Renew(**갱신**)**를 클릭하면 현재 값으로 모듈에서 제외 기간이 연장됩니다.

상태 모니터 알림

상태 정책에서 모듈에 대한 상태가 변경될 때 이메일, SNMP 또는 시스템 로그를 통해 알리도록 알림을 설정할 수 있습니다. 기존 알림 응답을 트리거할 상태 이벤트 레벨과 연결하고, 특별한 레벨의 상태 이벤트가 발생할 때 알릴 수 있습니다.

예를 들어 어플라이언스의 하드 디스크 공간이 부족해질 것이 우려되면, 남은 디스크 공간이 Warning(경고) 수준에 도달할 때 시스템 관리자에게 이메일을 자동으로 전송할 수 있습니다. 하드 디스크가 계속 채워지면 하드 드라이브가 Critical(심각) 수준에 도달할 때 두 번째 이메일을 전송할 수 있습니다.

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

상태 모니터 알림 정보

상태 모니터에 의해 생성되는 알림에는 다음 정보가 포함됩니다.

- Severity(심각도) - 알림의 심각도를 나타냅니다.
- Module(모듈) - 테스트 결과가 알림을 트리거한 상태 모듈을 지정합니다.
- Description(설명) - 테스트 결과가 알림을 트리거한 상태 테스트를 포함합니다.

아래 표는 이러한 심각도 수준을 설명합니다.

표 ***22:*** 알림 심각도

심각도	설명
중대	상태 테스트 결과가 Critical(심각) 알림 상태를 트리거하는 기준을 충족함.
경고	상태 테스트 결과가 Warning(경고) 알림 상태를 트리거하는 기준을 충족함.
정상	상태 테스트 결과가 Normal(정상) 알림 상태를 트리거하는 기준을 충족함.
오류	상태 테스트가 실행되지 않음.
복원됨	상태 테스트 결과가 Critical(심각) 또는 Warning(경고) 알림 상태에 이어 Normal(정상) 알림 상태로 전환되는 기준을 충족함.

상태 모니터 알림 생성

이 절차를 수행하려면 관리자 사용자여야 합니다.

상태 모니터 알림을 생성할 때 심각도, 상태 모듈 및 알림 응답 간에 연결을 생성합니다. 기존 알림을 사용할 수도 있고 특별히 시스템 상태에 대해 보고하도록 새 알림을 구성할 수도 있습니다. 선택한 모듈에 대해 심각도가 발생하면 알림이 트리거됩니다.

기존 임계값을 복제하는 방식으로 임계값을 생성하거나 업데이트하는 경우 충돌이 발생합니다. 중복된 임계값이 존재하면 상태 모니터는 가장 적은 알림을 생성하는 임계값을 사용하고 나머지는 무시합니다. 임계값의 시간 제한 값은 범위가 5~4,294,967,295분이어야 합니다.

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

시작하기 전에

- 상태 경고를 보내는 SNMP, syslog 또는 이메일 서버와 management center의 통신을 제어하는 알림 응답을 구성합니다. Secure Firewall Management Center 알림 응답, 569 페이지를 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Health(상태)** > **Monitor Alerts(모니터 알림)**를 선택합니다.

단계 **2** **Add(추가)**를 클릭합니다.

단계 **3** **Add Health Alert(상태 알림 추가)** 대화 상자의 **Health Alert Name(상태 알림 이름)** 필드에 상태 알림 이름을 입력합니다.

단계 **4** **Severity(심각도)** 드롭다운 목록에서 알림을 트리거하기 위해 사용하려는 심각도 수준을 선택합니다.

단계 **5** **Alert(알림)** 드롭다운 목록에서 지정된 심각도 수준에 도달할 때 트리거하려는 알림 응답을 선택합니다. 알림 응답을 Secure Firewall Management Center 알림 응답 **Alerts(알림)**를 클릭하여 **Alerts(알림)** 페이지로 이동하여 설정합니다.

단계 **6** **Health Modules(상태 모듈)** 목록에서 경고를 적용하려는 상태 정책 모듈을 선택합니다.

단계 **7** 경우에 따라 각 임계값 기간이 끝나고 임계값 카운트가 재설정되기까지의 시간(분 단위)을 **Threshold Timeout(임계값 시간 초과)** 필드에 입력합니다.

정책 실행 시간 간격 값이 임계값 시간 초과 값보다 작은 경우에도 지정된 모듈에서 보고된 두 가지 상태 이벤트 사이의 간격은 항상 더 큽니다. 예를 들어 임계값 시간 초과를 8 분으로 변경하고 정책 실행 시간 간격을 5분으로 설정하는 경우, 보고된 이벤트 사이의 간격은 10분(5 x 2)입니다.

단계 **8** **Save(저장)**를 클릭하고 상태 알림을 저장합니다.

상태 모니터 알림 수정

이 절차를 수행하려면 관리자 사용자여야 합니다.

상태 모니터 알림과 관련된 심각도, 상태 모듈 또는 알림 응답을 변경하려면 기존의 상태 모니터 알림을 수정할 수 있습니다.

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(상태)** > **Monitor Alerts(모니터 알림)**를 선택합니다.

단계 **2** 수정하려는 필수 상태 알림에 대해 제공된 **Edit(**수정**)** ( ) 아이콘을 클릭합니다.

단계 **3** **Edit Health Alert(**상태 알림 편집**)** 대화 상자의 **Alert(**알림**)** 드롭다운 목록에서 필요한 알림 항목을 선택하거나 **Alerts(**알림**)** 링크를 클릭하여 새 알림 항목을 구성합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

상태 모니터 알림 삭제

다중 도메인 구축에서는 현재 도메인에서 생성된 상태 모니터 알림을 보고 수정할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Monitor Alerts(**모니터 알림**)**를 선택합니다.

단계 **2** 삭제할 상태 알림 옆의 **Delete(**삭제**)** ( )을 클릭한 다음 **Delete health alert(**상태 알림 삭제**)**를 클릭하여 삭제합니다.

다음에 수행할 작업

- 알림이 계속 전송되지 않도록 하려면 기본 알림 응답을 비활성화하거나 삭제해야 합니다. Secure Firewall Management Center 알림 응답, 569 페이지을 참조하십시오.

상태 모니터 정보

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

상태 모니터는 management center뿐만 아니라 management center에서 관리하는 모든 디바이스에 대한 편집된 상태를 제공합니다. 상태 모니터는 다음으로 구성됩니다.

- Health Status(상태) 요약 페이지 - management center에서 관리하는 모든 디바이스 및 management center의 상태를 한눈에 볼 수 있습니다. 디바이스는 해당하는 경우 지리위치, 고가용성 또는 클러스터 상태에 따라 개별적으로 나열되거나 그룹화됩니다.
  - 디바이스 상태를 나타내는 육각형 위에 마우스를 올려놓으면 management center 및 디바이스의 상태 요약을 확인할 수 있습니다.
  - 디바이스의 왼쪽에 있는 점은 해당 상태를 나타냅니다.
    - 녹색 - 알람 없음
    - 주황색 - 하나 이상의 상태 경고가 표시됨
    - 빨간색 - 하나 이상의 중대 상태 알람

- Monitoring(모니터링) 탐색창 - 디바이스 계층 구조를 탐색할 수 있습니다. 탐색창에서 개별 디바이스에 대한 상태 모니터를 볼 수 있습니다.

다중 도메인 구축에서 상위 도메인의 상태 모니터는 모든 하위 도메인의 데이터를 표시합니다. 하위 도메인에서 상태 모니터는 현재 도메인의 데이터만 표시합니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

단계 **2** **Health Status(**상태**)** 랜딩 페이지에서 management center 및 매니지드 디바이스의 상태를 확인합니다.

a) 디바이스의 상태 요약을 보려면 육각형 위로 마우스 포인터를 올려놓습니다. 팝업 윈도우에는 상위 5개 상태 알림의 요약이 잘려서 표시됩니다. 팝업을 클릭하여 상태 알림 요약의 세부사항 보기를 엽니다.

b) 디바이스 목록에서 **Expand(**확장**)** ( ) 및 **Collapse(**축소**)** ( )를 클릭하여 디바이스의 상태 알림 목록을 확장하고 축소합니다.

행을 확장하면 상태, 제목 및 상세 정보를 포함한 모든 상태 알림이 나열됩니다.

참고 상태 알림은 심각도 레벨을 기준으로 정렬됩니다.

단계 **3** Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다. Monitoring(모니터링) 탐색창을 사용하는 경우, 다음을 수행합니다.

a) **Home(**홈**)**을 클릭하여 Health Status(상태) 요약 페이지로 돌아갑니다.

b) **Firewall Management Center**를 클릭하여 Secure Firewall Management Center 자체에 대한 상태 모니터를 봅니다.

c) 디바이스 목록에서 **Expand(**확장**)** ( ) 및 **Collapse(**축소**)** ( )를 클릭하여 관리되는 디바이스 목록을 확장하고 축소합니다.

행을 확장하면 모든 디바이스가 나열됩니다.

d) 디바이스별 상태 모니터를 보려면 디바이스를 클릭합니다.

다음에 수행할 작업

- management center에서 관리하는 모든 디바이스의 편집된 상태 및 메트릭에 대한 자세한 내용은 디바이스 상태 모니터, 397 페이지의 내용을 참조하십시오.
- management center의 상태에 대한 자세한 내용은 Management Center 상태 모니터 사용, 394 페이지의 내용을 참조하십시오.

언제든지 **Home(**홈**)**을 클릭하여 Health Status(상태) 랜딩 페이지로 돌아갈 수 있습니다.

Management Center 상태 모니터 사용

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

management center 모니터는 management center의 상태에 대한 자세한 보기를 제공합니다. 상태 모니터는 다음으로 구성됩니다.

- 고가용성(구성된 경우) - HA(고가용성) 패널에는 액티브 및 스탠바이 유닛의 상태, 마지막 동기화 시간, 전체 디바이스 상태를 비롯한 현재 HA 상태가 표시됩니다.
- Event Rate(이벤트 속도) - Event Rate(이벤트 속도) 패널에는 management center에서 수신한 전체 이벤트 속도 및 최대 이벤트 속도가 기준선으로 표시됩니다.
- Event Capacity(이벤트 용량) - Event Capacity(이벤트 용량) 패널은 이벤트 보유 시간, 현재 및 최대 이벤트 용량, 이벤트가 management center의 구성된 최대 용량을 초과하여 저장될 때 알림을 받는 용량 오버플로 메커니즘 등을 포함하여 이벤트 범주별 현재 사용량을 보여줍니다. .
- Process Health(프로세스 상태) - Process Health(프로세스 상태) 패널에는 중요 프로세스를 한눈에 볼 수 있는 보기와 각 프로세스의 CPU 및 메모리 사용량을 포함하여 처리된 모든 프로세스의 상태를 볼 수 있는 탭이 있습니다.
- CPU - CPU 패널에서는 평균 CPU 사용량(기본값)과 모든 코어의 CPU 사용량 간에 전환할 수 있습니다.
- Memory(메모리) - Memory(메모리) 패널에는 management center의 전체 메모리 사용량이 표시됩니다.
- Interface(인터페이스) - Interface(인터페이스) 패널에는 모든 인터페이스의 평균 입력 및 출력 속도가 표시됩니다.
- Disk Usage(디스크 사용량) - Disk Usage(디스크 사용량) 패널에는 전체 디스크의 사용량과 management center 데이터가 저장된 중요 파티션의 사용량이 표시됩니다.
- 하드웨어 통계 - 하드웨어 통계는 Management Center 섀시의 팬 속도, 전원 공급 장치 및 온도를 보여줍니다. 자세한 내용은 Management Center의 하드웨어 통계, 396 페이지을 참고하십시오.

팁 비활성 상태가 1시간(또는 구성된 다른 간격 동안) 지속되면 일반적으로 세션에서 로그아웃됩니다. 상태를 오랫동안 수동으로 모니터링할 계획이면 세션 시간 초과에서 일부 사용자를 제외하거나 시스템 시간 초과 설정을 변경하는 방법을 고려해 보십시오. 자세한 내용은 내부 사용자 추가, 123 페이지 및 세션 시간 제한 구성, 100 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

단계 **2** **Monitoring(**모니터링**)** 탐색 창을 사용하여 management center 및 디바이스별 상태 모니터에 액세스합니다.

- 독립형 management center은 단일 노드로 표시됩니다. 고가용성 management center은 노드 쌍으로 표시됩니다.
- 상태 모니터는 HA 쌍의 액티브 및 스탠바이 management center 모두에서 사용할 수 있습니다.

단계 **3** management center 대시보드를 탐색합니다.

management center 대시보드에는 management center의 HA 상태에 대한 요약 보기(구성된 경우)뿐만 아니라 management center 프로세스 및 디바이스 메트릭(예: CPU, 메모리, 디스크 사용량)을 한눈에 볼 수 있는 보기가 포함되어 있습니다.

어플라이언스에 대해 모든 모듈 실행

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

상태 모듈 테스트는 상태 정책을 생성할 때 구성하는 정책 실행 시간 간격으로 자동 실행됩니다. 그러나 어플라이언스에 대한 최신 상태 정보를 수집하기 위해 온디맨드 방식으로 모든 상태 모듈 테스트를 실행할 수도 있습니다.

다중 도메인 구축에서 현재 도메인 및 모든 하위 도메인의 어플라이언스에 대한 상태 모듈 테스트를 실행할 수 있습니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다.의 내용을 참조하십시오.

단계 **2** **Run All Modules(**모든 모듈 실행**)**를 클릭합니다. 상태 표시줄에 테스트의 진행 상황이 표시되고, Health Monitor Appliance(상태 모니터 어플라이언스) 페이지가 새로 고쳐집니다.

참고 상태 모듈을 수동으로 실행할 때, 자동으로 수행되는 첫 번째 새로 고침에서는 수동으로 실행한 테스트의 데이터가 반영되지 않을 수 있습니다. 방금 수동으로 실행한 모듈에 대한 값이 변경되지 않은 경우 잠시 기다렸다가 디바이스 이름을 클릭하여 페이지를 새로 고치십시오. 페이지의 자동 새로 고침이 다시 수행될 때까지 기다릴 수도 있습니다.

특정 상태 모듈 실행

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

상태 모듈 테스트는 상태 정책을 생성할 때 구성하는 정책 실행 시간 간격으로 자동 실행됩니다. 그러나 모듈에 대한 최신 상태 정보를 수집하기 위해 온디맨드 방식으로 해당 상태 모듈 테스트를 실행할 수도 있습니다.

다중 도메인 구축에서 현재 도메인 및 모든 하위 도메인의 어플라이언스에 대한 상태 모듈 테스트를 실행할 수 있습니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다.의 내용을 참조하십시오.

단계 **2** **Module Status Summary(**모듈 상태 요약**)** 그래프에서 확인하려는 상태 알림 카테고리의 색상을 클릭합니다.

단계 **3** 이벤트 목록을 보려는 알림에 대한 **Alert Detail(**알림 세부정보**)**열에서 **Run(**실행**)**을 클릭합니다.

상태 표시줄에 테스트의 진행 상황이 표시되고, Health Monitor Appliance(상태 모니터 어플라이언스) 페이지가 새로 고쳐집니다.

참고 상태 모듈을 수동으로 실행할 때, 자동으로 수행되는 첫 번째 새로 고침에서는 수동으로 실행한 테스트의 데이터가 반영되지 않을 수 있습니다. 방금 수동으로 실행한 모듈에 대한 값이 변경되지 않은 경우 잠시 기다렸다가 디바이스 이름을 클릭하여 페이지를 새로 고치십시오. 페이지의 자동 새로 고침이 다시 수행될 때까지 기다릴 수도 있습니다.

상태 모듈 알림 그래프 생성

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

특정 어플라이언스에 대한 특별한 상태 테스트 기간 중에 발생한 결과를 그래프로 표시할 수 있습니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다의 내용을 참조하십시오.

단계 **2** Health Monitor Appliance(상태 모니터 어플라이언스) 페이지의 **Module Status Summary** 그래프에서 확인하려는 상태 알림 상태 카테고리의 색상을 클릭합니다.

단계 **3** 이벤트 목록을 보려는 알림에 대한 **Alert Detail(**알림 세부정보**)**열에서 **Graph(**그래프**)**를 클릭합니다.

팁 이벤트가 나타나지 않으면 시간 범위를 조정해야 할 수 있습니다.

Management Center의 하드웨어 통계

Management Center 어플라이언스(물리적 어플라이언스만 해당)의 하드웨어 통계에는 팬 속도, 전원 공급 장치 및 온도와 같은 하드웨어 엔터티에 대한 정보가 포함됩니다. SNMP가 관리 센터의 상태를 모니터링하기 위해 트랩을 폴링하고 전송하는 경우:

1. MIB 폴링을 위해 관리 센터에서 SNMP를 활성화합니다. 기본적으로 관리 센터의 SNMP는 비활성화되어 있습니다. SNMP 폴링 구성, 99 페이지를 참조하십시오.
2. 트랩을 활성화하려면 필요한 각 SNMP 호스트에 대한 ACL 항목을 추가합니다. 호스트의 IP 주소를 지정하고 포트를 SNMP로 선택해야 합니다. 액세스 목록 구성, 45 페이지을 참조하십시오.

Health(상태**)** > **Monitor(**모니터**)** 페이지에서 하드웨어 통계를 보려면 다음을 수행합니다.

1. **Health(**상태**)** > **Policy(**정책**)** 페이지에서 Hardware Statistics(하드웨어 통계) 모듈이 활성화되어 있는지 확인합니다. 기본 임계값은 변경할 수 있습니다.
2. 관리 센터 상태 모니터링 대시보드에 포틀릿을 추가합니다. Hardware Statistics(하드웨어 통계) 메트릭 그룹을 선택한 다음 Fan Speed(팬 속도) 및 Temperature(온도) 메트릭을 선택합니다.

Health Monitoring(상태 모니터링**)** > **Home(**홈**)** 페이지의 방화벽 관리 센터에서 전원 공급 장치 상태를 볼 수 있습니다.

참고

- 팬 속도는 RPM으로 표시됩니다.
- 온도는 °C(섭씨 단위)로 표시됩니다.
- 전원 공급 장치의 슬롯 중 하나가 활성화되면 대시보드에 해당 슬롯이 *Online(*온라인*)*으로 표시되고 다른 슬롯은 *No Power(*전력 공급 없음*)*로 표시됩니다.
- 그래프의 각 가로선은 각 PSU 및 팬의 상태를 보여줍니다.
- 그래프 위에 마우스를 올려놓으면 해당 개별 통계의 데이터를 볼 수 있습니다.

디바이스 상태 모니터

디바이스 상태 모니터는 management center에서 관리하는 모든 디바이스에 대한 편집된 상태를 제공합니다. 디바이스 상태 모니터는 Firepower 디바이스에 대한 상태 메트릭을 수집하여 시스템 이벤트를 예측하고 이에 응답합니다. 디바이스 상태 모니터는 다음 구성 요소로 이루어집니다.

- System Details(시스템 세부 사항) - 설치된 Firepower 버전 및 기타 구축 세부 사항을 포함하여 매니지드 디바이스에 대한 정보를 표시합니다.
- Troubleshooting & Links(문제 해결 및 링크) - 자주 사용하는 문제 해결 주제 및 절차에 대한 편리한 링크를 제공합니다.
- Health Alerts(상태 알림) - 상태 알림 모니터에서 디바이스의 상태를 한눈에 볼 수 있습니다.
- Time Range(시간 범위) - 다양한 디바이스 메트릭 창에 표시되는 정보를 제한하도록 조정할 수 있는 시간 창입니다.
- Device Metrics(디바이스 메트릭) - 다음을 포함하여 사전 정의된 대시보드에서 범주화된 주요 Firepower 디바이스 상태 메트릭의 어레이입니다.
  - CPU - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
  - 메모리-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
  - Interfaces(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
  - Connections(연결) - 연결 통계(예: 엘리펀트 플로우, 활성 연결, 최대 연결 등) 및 NAT 변환 수.

- Snort - Snort 프로세스와 관련된 통계
- Disk Usage(디스크 사용량) - 파티션별 디스크 크기 및 디스크 사용률을 포함한 디바이스 디스크 사용량
- Critical Processes(중요 프로세스) - 프로세스 재시작과 CPU 및 메모리 사용률과 같이 기타 선택된 상태 모니터를 포함하여 관리 프로세스와 관련된 통계

지원되는 디바이스 메트릭의 전체 목록은 Cisco Secure Firewall Threat Defense 상태 메트릭을 참고하십시오.

시스템 세부 사항 및 문제 해결 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

System Details(시스템 세부 사항) 섹션에서는 선택한 디바이스에 대한 일반 시스템 정보를 제공합니다. 해당 디바이스에 대한 문제 해결 작업을 시작할 수도 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(상태)** > **Monitor(모니터)**를 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다.

단계 **2** 디바이스 목록에서 **Expand(확장)** (>) 및 **Collapse(축소)** (⌄)를 클릭하여 관리되는 디바이스 목록을 확장하고 축소합니다.

단계 **3** 디바이스별 상태 모니터를 보려면 디바이스를 클릭합니다.

단계 **4** **View System & Troubleshoot Details** ⋯**(시스템 및 문제 해결 세부 사항 보기...)** 링크를 클릭합니다.

이 패널은 기본적으로 축소되어 있습니다. 링크를 클릭하면 축소된 섹션이 확장되어 디바이스의 **System Details(시스템 세부 사항)** 및 **Troubleshooting & Links(문제 해결 및 링크)**가 표시됩니다. 시스템 세부 사항은 다음으로 구성됩니다.

- **Version(버전):** Firepower 소프트웨어 버전
- **Model(모델):** 디바이스 모델
- **Mode(모드):** 방화벽 모드 Firepower Threat Defense 디바이스는 일반 방화벽 인터페이스에 대해 라우팅 방화벽 모드 및 투명 방화벽 모드의 두 가지 방화벽 모드를 지원합니다.
- **VDB:** Cisco VDB(취약성 데이터베이스) 버전
- **SRU:** 침입 규칙 집합 버전
- **Snort:** Snort 버전

단계 **5** 다음 문제 해결 옵션을 이용할 수 있습니다.

- 문제 해결 파일 생성(다음 참조) 특정 시스템 기능에 대한 문제 해결 파일 생성, 450 페이지

- 고급 문제 해결 파일을 생성하고 다운로드합니다. 고급 문제 해결 파일 다운로드, 451 페이지의 내용을 참조하십시오.
- 상태 정책을 생성하고 수정합니다. 상태 정책 생성, 383 페이지의 내용을 참조하십시오.
- 상태 모니터 알림을 생성하고 수정합니다. 상태 모니터 알림 생성, 390 페이지의 내용을 참조하십시오.

디바이스 상태 모니터 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

디바이스 상태 모니터는 방화벽 디바이스의 상태에 대한 자세한 보기를 제공합니다. 디바이스 상태 모니터는 디바이스 메트릭을 컴파일하고 대시보드 어레이에 있는 디바이스의 상태 및 추세를 제공합니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다.

단계 **2** 디바이스 목록에서 **Expand(**확장**)** ( ) 및 **Collapse(**축소**)** ( )를 클릭하여 관리되는 디바이스 목록을 확장하고 축소합니다.

단계 **3** 페이지 상단에서 디바이스 이름의 바로 오른쪽에 있는 알림에서 디바이스의 **Health Alerts(**상태 알림**)**를 확인합니다.

Health Alerts(상태 알림**)** 위에 포인터를 올려놓으면 디바이스의 상태 요약이 표시됩니다. 팝업 윈도우에는 상위 5개 상태 알림의 요약이 잘려서 표시됩니다. 팝업을 클릭하여 상태 알림 요약의 세부사항 보기를 엽니다.

단계 **4** 오른쪽 상단의 드롭다운에서 시간 범위를 설정할 수 있습니다. 시간 범위는 지난 시간처럼 짧은 기간(기본값) 또는 지난 주처럼 긴 기간을 반영할 수 있습니다. 드롭다운에서 **Custom(**사용자 지정**)**을 선택하여 사용자 지정 시작 및 종료 날짜를 설정합니다.

새로 고침 아이콘을 클릭하여 자동 새로 고침을 5분으로 설정하거나 자동 새로 고침을 해제합니다.

단계 **5** 선택한 시간 범위와 관련하여 추세 그래프의 구축 오버레이를 보려면 **Show Deployment Info(**구축 정보 표시**)** ( ) 아이콘을 클릭합니다.

Show Deployment Info(구축 정보 표시**)** ( ) 아이콘은 선택한 기간 동안의 구축 수를 나타냅니다. 세로 줄은 구축 시작 및 종료 시간을 나타냅니다. 다수의 구축이 있는 경우 여러 대역/라인이 나타납니다. 점선 위에 있는 아이콘을 클릭하여 구축 세부 정보를 확인합니다.

단계 **6** 디바이스 모니터는 기본적으로 사전 정의된 여러 대시보드에서 상태 및 성능 메트릭을 보고합니다. 메트릭 대시보드에는 다음이 포함됩니다.

- Overview(개요) - CPU, 메모리, 인터페이스, 연결 통계 등 사전 정의된 다른 대시보드의 주요 메트릭을 강조 표시합니다. 디스크 사용량 및 중요 프로세스 정보도 포함됩니다.

- CPU - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
- 메모리-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
- Interfaces(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
- Connections(연결) - 연결 통계(예: 엘리펀트 플로우, 활성 연결, 최대 연결 등) 및 NAT 변환 수.
- Snort - Snort 프로세스와 관련된 통계
- ASP 삭제 - ASP(Accelerated Security Path) 성능 및 동작과 관련된 통계입니다.

레이블을 클릭하여 다양한 메트릭 대시보드를 탐색할 수 있습니다. 지원되는 디바이스 메트릭의 전체 목록은 Cisco Secure Firewall Threat Defense 상태 메트릭을 참고하십시오.

단계 **7** **Add Dashboard(**대시보드 추가**)(+)**를 클릭한 후 사용 가능한 메트릭 그룹에서 사용자 고유의 변수 집합을 구성하여 사용자 지정 상관관계 대시보드를 생성할 수 있습니다. 디바이스 메트릭 연계, 400 페이지의 내용을 참고하십시오.

디바이스 메트릭 연계

디바이스 상태 모니터에는 시스템 이벤트를 예측하고 응답하는 데 사용되는 주요 threat defense 디바이스 메트릭 어레이가 포함되어 있습니다. 보고된 메트릭을 통해 모든 threat defense 디바이스의 상태를 확인할 수 있습니다.

디바이스 모니터는 기본적으로 여러 미리 정의된 대시보드에서 이러한 메트릭을 보고합니다. 이러한 대시보드에는 다음이 포함됩니다.

- Overview(개요) - CPU, 메모리, 인터페이스, 연결 통계 등 사전 정의된 다른 대시보드의 주요 메트릭을 강조 표시합니다. 디스크 사용량 및 중요 프로세스 정보도 포함됩니다.
- CPU - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
- 메모리-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
- Interfaces(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
- Connections(연결) - 연결 통계(예: 엘리펀트 플로우, 활성 연결, 최대 연결 등) 및 NAT 변환 수.
- Snort - Snort 프로세스와 관련된 통계
- ASP 삭제 - ASP(Accelerated Security Path) 성능 및 동작과 관련된 통계입니다.

사용자 정의 대시보드를 추가하여 상호 연결된 메트릭을 상호 연결할 수 있습니다. 사전 정의된 상관관계 그룹(예: CPU 및 Snort) 중에서 선택합니다. 또는 사용 가능한 메트릭 그룹에서 고유한 변수 집합을 작성하여 사용자 정의 상관 관계 대시보드를 생성할 수도 있습니다. 지원되는 디바이스 메트릭의 전체 목록은 Cisco Secure Firewall Threat Defense 상태 메트릭을 참고하십시오.

시작하기 전에

- 상태 모니터 대시보드에서 시계열 데이터(디바이스 메트릭)를 보고 상관 관계를 지정하려면 REST API(**Settings(**설정**)** > **Configuration(**구성**)** > **REST API Preferences(REST API** 기본 설정**)**)를 활성화합니다.
- 이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

참고 디바이스 메트릭 상관은 threat defense 6.7 이상 버전에서만 사용할 수 있습니다. 따라서 threat defense 6.7 이전 버전의 경우 REST API를 활성화하더라도 상태 모니터 대시보드에 이러한 메트릭이 표시되지 않습니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Monitor(**모니터**)**를 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 디바이스별 상태 모니터에 액세스합니다.

단계 **2** **Devices(**디바이스**)** 목록에서 **Expand(**확장**)** ( ) 및 **Collapse(**축소**)** ( )를 클릭하여 매니지드 디바이스 목록을 확장하고 축소합니다.

단계 **3** 대시보드를 수정할 디바이스를 선택합니다.

단계 **4** 디바이스 모니터의 오른쪽 상단 모서리에 있는 **Add Dashboard(**대시보드 추가**)**(+) 아이콘을 클릭하여 새 대시보드를 추가합니다.

단계 **5** **Select Correlation Group(**상관관계 그룹 선택**)** 드롭다운에서 미리 정의된 상관관계 그룹을 선택하거나 사용자 지정 그룹을 생성합니다.

단계 **6** 미리 정의된 상관관계 그룹에서 대시보드를 생성하려면 그룹을 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **7** 사용자 정의 상관 관계 대시보드를 생성하려면:

a) **Custom(**사용자 정의**)**을 선택합니다.

b) **Dashboard Name(**대시보드 이름**)** 필드에 고유한 이름을 입력하거나 기본값을 수락합니다.

c) **Select Metric Group(**메트릭 그룹 선택**)** 드롭다운에서 그룹을 선택한 다음 **Select Metrics(**메트릭 선택**)** 드롭다운에서 해당 메트릭을 선택합니다.

지원되는 디바이스 메트릭의 전체 목록은 Cisco Secure Firewall Threat Defense 상태 메트릭을 참고하십시오.

단계 **8** **Add Metrics(**메트릭 추가**)**를 클릭하여 다른 그룹에서 메트릭을 추가하고 선택합니다.

단계 **9** 개별 메트릭을 제거하려면 항목의 오른쪽에 있는 **x** 아이콘을 클릭합니다. 전체 그룹을 제거하려면 삭제 아이콘을 클릭합니다.

단계 **10** **Add(**추가**)**를 클릭하여 상태 모니터에 대시보드를 추가합니다.

단계 **11** 사용자 정의 상관 관계 대시보드를 편집하거나 삭제할 수 있습니다.

클러스터 상태 모니터

threat defense가 클러스터의 제어 노드인 경우 management center는 디바이스 메트릭 데이터 컬렉터에서 다양한 메트릭을 주기적으로 수집합니다. 클러스터 상태 모니터는 다음 구성 요소로 이루어집니다.

- 대시보드 개요 - 클러스터 토폴로지, 클러스터 통계 및 메트릭 차트에 대한 정보를 표시합니다.
  - 토폴로지 섹션에는 클러스터의 라이브 상태, 개별 위협 방어의 상태, 위협 방어 노드 유형(제어 노드 또는 데이터 노드) 및 디바이스의 상태가 표시됩니다. 디바이스의 상태는 *Disabled(*비활성화됨*)*(디바이스가 클러스터에서 나갈 때), *Added out of box*(퍼블릭 클라우드 클러스터에서 management center에 속하지 않는 추가 노드) 또는 *Normal*(노드의 이상적인 상태)일 수 있습니다.
  - 클러스터 통계 섹션에는 CPU 사용량, 메모리 사용량, 입력 속도, 출력 속도, 활성 연결 및 NAT 변환과 관련된 클러스터의 현재 메트릭이 표시됩니다.

참고 CPU 및 메모리 메트릭은 데이터 플레인 및 Snort 사용량의 개별 평균을 표시합니다.

  - CPU Usage(CPU 사용량), Memory Usage(메모리 사용량), Throughput(처리량) 및 Connections(연결)와 같은 메트릭 차트는 지정된 기간 동안의 클러스터 통계를 도식적으로 표시합니다.
- 부하 분포 대시보드 - 클러스터 노드 전체의 부하 분포를 다음 두 가지 위젯으로 표시합니다:
  - Distribution(배포) 위젯은 클러스터 노드 전체에서 시간 범위의 평균 패킷 및 연결 분포를 표시합니다. 이 데이터는 노드에서 부하가 분산되는 방식을 나타냅니다. 이 위젯을 사용하면 부하 분포의 이상을 쉽게 식별하고 수정할 수 있습니다.
  - Node Statistics(노드 통계) 위젯은 노드 레벨 메트릭을 테이블 형식으로 표시합니다. 클러스터 노드 전체에서 CPU 사용량, 메모리 사용량, 입력 속도, 출력 속도, 활성 연결 및 NAT 변환에 대한 메트릭 데이터를 표시합니다. 이 테이블 보기를 사용하면 데이터의 상관관계를 파악하고 불일치를 쉽게 식별할 수 있습니다.
- Member Performance(멤버 성능) 대시보드 - 클러스터 노드의 현재 메트릭을 표시합니다. 선택기를 사용하여 노드를 필터링하고 특정 노드의 세부 정보를 볼 수 있습니다. 메트릭 데이터에는 CPU 사용량, 메모리 사용량, 입력 속도, 출력 속도, 활성 연결 및 NAT 변환이 포함됩니다.
- CCL 대시보드 - 클러스터 제어 링크 데이터, 즉 입력 및 출력 속도를 그래픽으로 표시합니다.
- 문제 해결 및 링크 - 자주 사용하는 문제 해결 주제 및 절차에 대한 편리한 링크를 제공합니다.
- 시간 범위 - 다양한 클러스터 메트릭 대시보드 및 위젯에 표시되는 정보를 제한하기 위한 조정 가능한 시간 창입니다.
- 사용자 지정 대시보드 - 클러스터 전체 메트릭 및 노드 레벨 메트릭 모두에 대한 데이터를 표시합니다. 그러나 노드 선택은 위협 방어 메트릭에만 적용되며 노드가 속한 전체 클러스터에는 적용되지 않습니다.

클러스터 상태 모니터 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

클러스터 상태 모니터는 클러스터와 해당 노드의 상태에 대한 자세한 보기를 제공합니다. 이 클러스터 상태 모니터는 대시보드 어레이에서 클러스터의 상태 및 추세를 제공합니다.

시작하기 전에

- management center에서 하나 이상의 디바이스에서 클러스터를 생성했는지 확인합니다.

프로시저

단계 **1** 시스템 ( ) > **Health(**상태**)** > **Monitor(**모니터**)**을(를) 선택합니다.

Monitoring(모니터링) 탐색 창을 사용하여 노드별 상태 모니터에 액세스합니다.

단계 **2** 디바이스 목록에서 **Expand(**확장**)** ( ) 및 **Collapse(**축소**)** ( )를 클릭하여 관리되는 클러스터 디바이스 목록을 확장하고 축소합니다.

단계 **3** 클러스터 상태 통계를 보려면 클러스터 이름을 클릭합니다. 클러스터 모니터는 기본적으로 사전 정의된 여러 대시보드에서 상태 및 성능 메트릭을 보고합니다. 메트릭 대시보드에는 다음이 포함됩니다.

- 개요 - 노드, CPU, 메모리, 입출력 속도, 연결 통계, NAT 변환 정보 등 미리 정의된 다른 대시보드의 주요 메트릭을 강조 표시합니다.
- Load Distribution(로드 분포) - 클러스터 노드 전체의 트래픽 및 패킷 분포입니다.
- Member Performance(멤버 성능) - CPU 사용량, 메모리 사용량, 입력 처리량, 출력 처리량, 활성 연결 및 NAT 변환에 대한 노드 레벨 통계.
- CCL - 인터페이스 상태 및 집계 트래픽 통계

레이블을 클릭하여 다양한 메트릭 대시보드를 탐색할 수 있습니다. 지원되는 클러스터 메트릭의 전체 목록은 Cisco Secure Firewall Threat Defense 상태 메트릭을 참고하십시오.

단계 **4** 오른쪽 상단의 드롭다운에서 시간 범위를 설정할 수 있습니다. 시간 범위는 지난 시간처럼 짧은 기간(기본값) 또는 지난 주처럼 긴 기간을 반영할 수 있습니다. 드롭다운에서 **Custom(**사용자 지정**)**을 선택하여 사용자 지정 시작 및 종료 날짜를 설정합니다.

새로 고침 아이콘을 클릭하여 자동 새로 고침을 5분으로 설정하거나 자동 새로 고침을 해제합니다.

단계 **5** 선택한 시간 범위와 관련하여 추세 그래프에서 구축 오버레이를 보려면 구축 아이콘을 클릭합니다.

구축 아이콘은 선택한 시간 범위 동안의 구축 수를 나타냅니다. 세로 줄은 구축 시작 및 종료 시간을 나타냅니다. 다수의 구축이 있는 경우 여러 대역/라인이 나타납니다. 점선 위에 있는 아이콘을 클릭하여 구축 세부 사항을 확인합니다.

단계 **6** (노드별 상태 모니터의 경우) 페이지 상단에서 디바이스 이름의 바로 오른쪽에 있는 알림에서 노드의 **Health Alerts(**상태 알림**)**를 확인합니다.

Health Alerts(상태 알림**)** 위에 포인터를 올려놓으면 노드의 상태 요약이 표시됩니다. 팝업 윈도우에는 상위 5개 상태 알림의 요약이 잘려서 표시됩니다. 팝업을 클릭하여 상태 알림 요약의 세부사항 보기를 엽니다.

단계 **7** (노드별 상태 모니터의 경우) 디바이스 모니터는 기본적으로 사전 정의된 여러 대시보드에서 상태 및 성능 메트릭을 보고합니다. 메트릭 대시보드에는 다음이 포함됩니다.

- Overview(개요) - CPU, 메모리, 인터페이스, 연결 통계 등 사전 정의된 다른 대시보드의 주요 메트릭을 강조 표시합니다. 디스크 사용량 및 중요 프로세스 정보도 포함됩니다.
- CPU - CPU 사용률(프로세스 및 물리적 코어별 CPU 사용률 포함)
- 메모리-데이터 플레인 및 Snort 메모리 사용량을 포함한 디바이스 메모리 사용량입니다.
- Interfaces(인터페이스) - 인터페이스 상태 및 집계 트래픽 통계
- Connections(연결) - 연결 통계(예: 엘리펀트 플로우, 활성 연결, 최대 연결 등) 및 NAT 변환 수.
- Snort - Snort 프로세스와 관련된 통계
- ASP 삭제 - 여러 이유로 인해 삭제된 패킷과 관련된 통계입니다.

레이블을 클릭하여 다양한 메트릭 대시보드를 탐색할 수 있습니다. 지원되는 디바이스 메트릭의 전체 목록은 Cisco Secure Firewall Threat Defense 상태 메트릭을 참고하십시오.

단계 **8** 사용 가능한 메트릭 그룹에서 고유한 변수 집합을 작성하여 사용자 지정 대시보드를 생성하려면 상태 모니터의 오른쪽 상단 모서리에 있는 더하기 기호(+)를 클릭합니다.

클러스터 전체 대시보드의 경우 Cluster metric group(클러스터 메트릭 그룹)을 선택한 다음 메트릭을 선택합니다.

상태 모니터 상태 카테고리

사용 가능한 상태 카테고리가 아래 표에 심각도별로 나열됩니다.

표 ***23:*** 상태 표시기

상태 레벨	상태 아이콘	원 그래프의 상태 색상	설명
오류	**Error(**오류**)** (✖)	검은색	어플라이언스에서 하나 이상의 상태 모니터링 모듈이 실패했으며, 실패 이후 성공적으로 다시 실행되지 않았습니다. 상태 모니터링 모듈의 업데이트를 얻으려면 기술 지원 담당자에게 문의하십시오.
중대	**Critical(**중요**)** (❗)	빨간색	어플라이언스에서 하나 이상의 상태 모듈에 대해 Critical(심각) 한도가 초과되었으며 문제가 해결되지 않았음을 나타냅니다.

상태 레벨	상태 아이콘	원 그래프의 상태 색상	설명
경고	**Warning(**경고**)** ()	노란색	어플라이언스에서 하나 이상의 상태 모듈에 대해 Warning(경고) 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다. 이 상태는 또한 과도기 상태를 나타냅니다. 즉, 디바이스 구성의 변경으로 인해 필요한 데이터를 일시적으로 사용할 수 없거나 처리할 수 없습니다. 모니터링 주기에 따라 이 과도 상태는 자동으로 수정됩니다.
정상	**Normal(**정상**)** ()	녹색	어플라이언스의 모든 상태 모듈이 어플라이언스에 적용된 상태 정책에 구성된 제한 내에서 실행되고 있습니다.
복원됨	**Recovered(**복구됨**)** ()	녹색	어플라이언스의 모든 상태 모듈(Critical(심각) 또는 Warning(경고) 상태에 있던 모듈 포함)이 어플라이언스에 적용된 상태 정책에 구성된 제한 내에서 실행되고 있음을 나타냅니다.
Disabled(비활성화)	**Disabled(**비활성화됨**)** ()	파란색	어플라이언스가 비활성화되었거나 제외되었거나, 어플라이언스에 상태 정책이 적용되지 않았거나, 어플라이언스에 현재 도달할 수 없음을 나타냅니다.

상태 이벤트 보기

상태 이벤트 보기(Health Event View) 페이지에서는 management center로그 상태 이벤트의 상태 모니터가 기록한 상태 이벤트를 볼 수 있습니다. 완전하게 맞춤화가 가능한 이벤트 보기에서는 상태 모니터에서 수집한 상태 이벤트를 빠르고 쉽게 분석할 수 있습니다. 조사하는 이벤트와 관련된 기타 정보에 쉽게 액세스 할 수 있도록 이벤트 데이터를 검색 할 수 있습니다. 각 상태 모듈이 테스트하는 조건을 이해하면 상태 이벤트에 대한 알림을 좀 더 효과적으로 구성할 수 있습니다.

상태 이벤트 보기 페이지에서 많은 표준 이벤트 보기 기능을 수행할 수 있습니다.

상태 이벤트 보기

이 절차를 수행하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.

Health Events(상태 이벤트) 페이지의 Table View(테이블 보기)에는 지정된 어플라이언스의 모든 상태 이벤트가 나열됩니다.

management center의 Health Monitor(상태 모니터) 페이지에서 상태 이벤트에 액세스하면 모든 관리되는 어플라이언스에 대한 모든 상태 이벤트가 검색됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

팁 Health Events(상태 이벤트) 테이블이 포함된 상태 이벤트 워크플로의 페이지로 돌아가려면 이 보기에 북마크를 지정할 수 있습니다. 북마크 지정된 보기는 현재 보고 있는 시간 범위 내에서 이벤트를 검색하지만, 필요한 경우 시간 범위를 수정하여 좀 더 최신 정보로 테이블을 업데이트할 수 있습니다.

프로시저

시스템 (⚙) > **Health(**상태**)** > **Events(**이벤트**)**를 선택합니다.

팁 상태 이벤트의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭하십시오. Select Workflow(워크플로 선택) 페이지에서 **Health Events(**상태 이벤트**)**를 클릭합니다.

참고 이벤트가 나타나지 않으면 시간 범위를 조정해야 할 수 있습니다.

모듈 및 어플라이언스별로 상태 이벤트 보기

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다. 디바이스 상태 모니터 보기, 399 페이지을 참조하십시오.

단계 **2** **Module Status Summary(**모듈 상태 요약**)** 그래프에서 확인하려는 이벤트 상태 카테고리의 색상을 클릭합니다.

Alert Detail(알림 세부정보) 목록은 디스플레이를 토글하여 이벤트를 표시하거나 숨깁니다.

단계 **3** 이벤트 목록을 보려는 알림에 대한 **Alert Detail(**알림 세부정보**)** 열에서 **Events(**이벤트**)**를 클릭합니다.

어플라이언스의 이름 및 제약 조건으로써 지정된 상태 알림 모듈의 이름과 함께 쿼리에 대한 결과가 포함된 Health Events(상태 이벤트) 페이지가 나타납니다. 이벤트가 나타나지 않으면 시간 범위를 조정해야 할 수 있습니다.

단계 **4** 지정한 어플라이언스에 대한 모든 상태 이벤트를 보려면 **Search Constraints(**검색 제약 조건**)**를 확장하고 **Module Name(**모듈 이름**)** 제약 조건을 클릭하여 제거합니다.

상태 이벤트 테이블 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** 시스템 (⚙) > **Health(**상태**)** > **Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Bookmark(즐겨찾기) — 현재 페이지에 즐겨찾기에 등록해 빠르게 돌아오려면, **Bookmark This Page(**이 페이지를 즐겨찾기에 등록**)**를 클릭하고 즐겨찾기 이름을 지정한 후 **Save(**저장**)**를 클릭합니다.
- Change Workflow(워크플로 변경) — 다른 상태 이벤트 워크플로 선택하려면, **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- Delete Events(이벤트 삭제) — 상태 이벤트를 삭제하려, 삭제하려는 이벤트 옆에 있는 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다. 현재 제한된 보기에서 모든 이벤트를 삭제하려면 **Delete All(**모두 삭제**)**을 클릭하고 모든 이벤트를 삭제할 것인지를 확인합니다.
- Generate Reports(보고서 생성) — 테이블 보기에서 데이터를 기반으로 보고서를 생성하고 **Report Designer(**리포트 디자이너**)**를 클릭합니다.
- Modify(수정) — 상태 테이블 보기에 나열된 이벤트의 시간 및 날짜 범위를 수정합니다. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
- Navigate(탐색) — 이벤트 보기 페이지를 탐색합니다.
- Navigate Bookmark(즐겨찾기 탐색) — 즐겨찾기 관리 페이지로 이동하려면 이벤트 보기에서 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다.
- Navigate Other(기타 탐색) — 관련 이벤트를 보기 위해 다른 이벤트 테이블로 이동합니다.
- Sort(정렬) — 표시되는 이벤트를 정렬하고, 이벤트 테이블에 표시되는 열을 변경하며, 표시되는 이벤트를 제한합니다.
- View All(모두 보기) — 보기에서 모든 이벤트에 대한 이벤트 세부 정보를 보려면, **View All(**모두 보기**)**를 클릭합니다.
- View Details(세부 정보 보기) — 단일 상태 이벤트와 관련된 세부 사항을 보려면, 이벤트의 왼쪽에 있는 아래쪽 화살표 링크를 클릭합니다.
- View Multiple(다중 보기) — 여러 상태 이벤트의 이벤트 세부 정보를 보려면, 세부 정보를 보려는 이벤트에 해당하는 행 옆의 확인란을 선택한 후 **View(**보기**)**를 클릭합니다.
- View Status(상태 보기) - 특정 상태의 모든 이벤트를 보려면 Status(상태) 열의 상태를 클릭하여 해당 상태의 이벤트를 찾습니다.

상태 이벤트 테이블

상태 정책에서 활성화하기 위해 선택하는 Health Monitor(상태 모니터) 모듈은 다양한 테스트를 실행하여 어플라이언스 상태를 결정합니다. 상태가 지정된 기준을 충족하면 상태 이벤트가 생성됩니다.

아래 표에서는 상태 이벤트 테이블에서 보고 검색 할 수 있는 필드를 설명합니다.

표 ***24:*** 상태 이벤트 필드

필드	설명
모듈 이름	보려는 상태 이벤트를 생성한 모듈의 이름을 지정합니다. 예를 들어 CPU 성능을 측정하는 이벤트를 보려면, `CPU`를 입력합니다. 그러면 해당 CPU Usage 및 CPU 온도 이벤트가 검색됩니다.
테스트 이름 (검색만 해당)	이벤트를 생성한 상태 모듈의 이름입니다.
시간 (검색만 해당)	상태 이벤트의 타임스탬프.
설명	이벤트를 생성한 상태 모듈의 설명. 예를 들어, 프로세스를 실행할 수 없을 때 생성되는 상태 이벤트에는 `Unable to Execute`라는 레이블이 지정됩니다.
값	이벤트를 생성한 상태 테스트에서 얻은 결과의 값(단위의 수). 예를 들어 management center에서 모니터링 중인 디바이스가 CPU 리소스의 80% 이상을 사용할 때마다 상태 이벤트가 생성된다면 값은 80~100의 숫자가 될 수 있습니다.
단위	결과의 단위 설명자. 와일드카드 검색을 생성하려면 별표(*)를 사용할 수 있습니다. 예를 들어 management center에서 모니터링 중인 디바이스가 CPU 리소스의 80% 이상을 사용할 때 상태 이벤트가 생성된다면 단위 설명자는 퍼센트 기호(%)입니다.
상태	어플라이언스에 대해 보고된 상태(Critical(심각), Yellow(노란색), Green(녹색) 또는 Disabled(비활성화)).
도메인	매니지드 디바이스에서 보고한 상태 이벤트의 경우, 상태 이벤트를 보고한 디바이스의 도메인. management center에서 보고한 상태 이벤트의 경우, `Global(전역)`. 이 필드는 다중 도메인 구축에서만 나타납니다.
디바이스	상태 이벤트가 보고된 어플라이언스.

상태 모니터링 기록

표 ***25:***

기능	버전	세부정보
새 클러스터 상태 모니터 대시보드.	7.3	클러스터 상태 모니터 메트릭을 볼 수 있는 새 대시보드가 다음 구성 요소와 함께 도입되었습니다. • Overview(개요) - 클러스터 토폴로지, 클러스터 통계 및 메트릭 차트에 대한 정보를 표시합니다. • Load Distribution(로드 분포) - 클러스터 노드 전체의 로드 분포를 표시합니다. • Member Performance(멤버 성능) - 클러스터의 모든 멤버 노드의 현재 메트릭을 표시합니다. • CCL—클러스터 제어 링크 데이터, 즉 입력 및 출력 속도를 그래픽으로 표시합니다. 참고 이러한 기능은 클러스터에만 적용됩니다. 따라서 클러스터 대시보드를 보고 사용하려면 **Monitoring(**모니터링**)** 창의 **Devices(**디바이스**)** 목록에서 클러스터를 선택해야 합니다. 신규/수정된 화면: 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**.
새 하드웨어 통계 모듈.	7.3	management center 하드웨어 및 환경 상태 통계가 상태 모니터 대시보드에 추가되었습니다. • 관리 센터 하드웨어에서 하드웨어 데몬의 모니터링을 활성화하기 위해 새로운 정책 모듈인 **Hardware Statistics(**하드웨어 통계**)**가 도입되었습니다. 메트릭에는 팬 속도, 온도 및 전원 공급 장치가 포함되었습니다. • 모니터링 대시보드에서 하드웨어 상태 메트릭의 그래픽 표현을 볼 수 있도록 맞춤형 메트릭 그룹인 **Hardware Statistics(**하드웨어 통계**)**도 추가되었습니다. • 전원 공급 장치 상태는 관리 센터의 상태 알림에서 캡처됩니다. 참고 이러한 기능은 Management Center에만 적용됩니다. 따라서 관리 센터 대시보드에서만 사용할 수 있습니다. 신규/수정된 화면: • 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)** • 시스템 (⚙) > **Health(**상태**)** > **Policy(**정책**)**

기능	버전	세부정보
새 하드웨어 및 환경 상태 메트릭 그룹.	7.3	위협 방어 하드웨어 및 환경 상태 통계가 상태 모니터 대시보드에 추가되었습니다. • 위협 방어에 대한 하드웨어 관련 통계를 보기 위해 맞춤형 메트릭 그룹인 **Hardware / Environment Status(**하드웨어/환경 상태**)**가 도입되었습니다. 메트릭에는 팬 속도, 섀시 온도, SSD 상태 및 전원 공급 장치가 포함되었습니다. • 디바이스 상태 알림이 위협 방어 하드웨어의 전원 공급 장치 상태를 포함하도록 개선되었습니다. *Critical(*심각*)* 알림은 비정상적인 열 상태에 대해 표시되고 *Normal(*정상*)* 알림은 정상적인 열 상태에 대해 표시됩니다. 참고 이러한 기능은 Threat Defense에만 적용됩니다. 따라서 **Monitoring(**모니터링**)** 창의 **Devices(**디바이스**)** 목록에서 적절한 디바이스를 선택해야 합니다. 신규/수정된 화면: 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**.
상태 모니터 사용 편의성 개선 사항.	7.1	다음 UI 페이지는 더 나은 사용성과 데이터 표시를 위해 개선되었습니다. • 정책 • 제외 • 모니터 알림 신규/수정된 화면: • 시스템 (⚙) > **Health(**상태**)** > **Policy(**정책**)** • 시스템 (⚙) > **Health(**상태**)** > **Exclude(**제외**)** • 시스템 (⚙) > **Health(**상태**)** > **Monitor Alerts(**모니터 알림**)**
엘리펀트 플로우 탐지.	7.1	상태 모니터에는 다음과 같은 향상된 기능이 포함됩니다. • 연결 통계에는 활성 엘리펀트 플로우가 포함됩니다. • Connection Group Metrics(연결 그룹 메트릭)에는 활성 엘리펀트 플로우의 수가 포함됩니다. 엘리펀트 플로우 탐지 기능은 Cisco Firewall 2100 시리즈에서 지원되지 않습니다.
중단된 높은 비관리 디스크 사용량 알림.	7.0.6	디스크 사용량 상태 모듈은 더 이상 높은 비관리 디스크 사용량에 대해 알림을 전송하지 않습니다. 업그레이드 후에는 매니지드 디바이스에 상태 정책을 구축하거나(알림 표시 중지) 디바이스를 업그레이드(알림 전송 중지)할 때까지 이러한 알림이 계속 표시될 수 있습니다. 참고 버전 7.0–7.0.5, 7.1.x, 7.2.0–7.2.3 및 7.3.x는 이러한 알림을 계속 지원합니다. management center에서 이러한 버전을 실행하는 경우에도 알림이 계속 표시될 수 있습니다.

기능	버전	세부정보
새 상태 모듈.	7.0	

기능	버전	세부정보
		다음 상태 모듈을 추가했습니다. • AMP Connection Status(AMP 연결 상태): threat defense에서 AMP 클라우드 연결을 모니터링합니다. • AMP Threat Grid Status(AMP Threat Grid 상태): threat defense에서 AMP Threat Grid 클라우드 연결을 모니터링합니다. • ASP Drop(ASP 삭제): 데이터 플레인 가속 보안 경로에 의해 삭제된 연결을 모니터링합니다. • Advanced Snort Statistics(고급 Snort 통계): 패킷 성능, 흐름 카운터 및 흐름 이벤트와 관련된 Snort 통계를 모니터링합니다. • Event Stream Status(이벤트 스트림 상태): Event Streamer를 사용하는 서드파티 클라이언트 애플리케이션에 대한 연결을 모니터링합니다. • FMC Access Configuration Changes(FMC 액세스 구성 변경): management center에서 직접 수행한 액세스 구성 변경 사항을 모니터링합니다. • FMC HA Status(FMC HA 상태): 액티브 및 스탠바이 management center와 디바이스 간의 동기화 상태를 모니터링합니다. HA 상태 모듈을 교체합니다. • FTD HA Status(FTD HA 상태): 액티브 및 스탠바이 threat defense HA 쌍과 디바이스 간의 동기화 상태를 모니터링합니다. • File System Integrity Check(파일 시스템 무결성 검사): 시스템에 CC 모드 또는 UCAPL 모드가 활성화되어 있는 경우 파일 시스템 무결성 검사를 수행합니다. • Flow Offload(플로우 오프로드): Firepower 9300 및 4100 플랫폼에서 하드웨어 플로우 오프로드 통계를 모니터링합니다. • Hit Count(적중 횟수): 액세스 제어 정책에서 특정 규칙이 적중된 횟수를 모니터링합니다. • MySQL Status(MySQL 상태): MySQL 데이터베이스의 상태를 모니터링합니다. • NTP Status FTD(NTP 상태 FTD): 매니지드 디바이스의 NTP 클럭 동기화 상태를 모니터링합니다. • RabbitMQ Status(RabbitMQ 상태): RabbitMQ 메시징 브로커의 상태를 모니터링합니다. • Routing Statistics(라우팅 통계): 에서 IPv4 및 IPv6 경로 정보를 모두 모니터링합니다.threat defense • SSE Connection Status(SSE 연결 상태): threat defense에서 SSE 클라우드 연결을 모니터링합니다. • Sybase Status(Sybase 상태): Sybase 데이터베이스의 상태를 모니터링합니다. • Unresolved Groups Monitor(확인되지 않은 그룹 모니터): 액세스 제어 정책에 사용

기능	버전	세부정보
		되는 확인되지 않은 그룹을 모니터링합니다. • VPN Statistics(VPN 통계): 사이트 간 및 원격 액세스 VPN 터널 통계를 모니터링합니다. • xTLS Counters(xTLS 카운터): xTLS/SSL 플로우, 메모리 및 캐시 효율성을 모니터링합니다.
상태 모니터 개선 사항.	7.0	상태 모니터에는 다음과 같은 향상된 기능이 추가되었습니다. • 다음의 요약 보기가 있는 향상된 management center 대시보드: • 고가용성 • 이벤트 비율 및 용량 • 프로세스 상태 • CPU 임계값 • 메모리 • 인터페이스 속도 • 디스크 사용 • 향상된 threat defense 대시보드: • 스플릿 브레인 시나리오에 대한 상태 알림 • 새 상태 모듈에서 사용 가능한 추가 상태 메트릭

기능	버전	세부정보
새 상태 모듈.	6.7	CPU 사용 모듈은 더 이상 사용되지 않습니다. 대신 다음 CPU 사용 모듈을 참조하십시오. • CPU 사용(코어 당): 모든 코어의 CPU 사용을 모니터링합니다. • CPU 사용 데이터 플레인: 디바이스에서 모든 데이터 플레인 프로세스의 평균 CPU 사용을 모니터링합니다. • CPU 사용 데이터 Snort: 디바이스에서 Snort 프로세스의 평균 CPU 사용을 모니터링합니다. • CPU 사용량 시스템: 디바이스에 있는 모든 시스템 프로세스의 평균 CPU 사용량을 모니터링합니다. 통계를 추적하기 위해 다음 모듈이 추가되었습니다. • 연결 통계: 연결 통계 및 NAT 변환 수를 모니터링합니다. • 중요 프로세스 통계: 이 모듈은 중요한 프로세스의 상태, 리소스 소비 및 재시작 횟수를 모니터링합니다. • 구축된 구성 통계: 구축 된 구성에 대한 통계(예: ACE 및 IPS 규칙 수)를 모니터링합니다. • Snort 통계: 이 모듈은 이벤트, 플로우 및 패킷에 대한 Snort 통계를 모니터링합니다. 메모리 사용을 추적하기 위해 다음 모듈이 추가되었습니다. • 메모리 사용 데이터 플레인: 데이터 플레인 프로세스에서 사용하는 할당된 메모리의 백분율을 모니터링합니다. • 메모리 사용량 Snort: Snort 프로세스에서 사용하는 할당된 메모리의 백분율을 모니터링합니다.

기능	버전	세부정보
상태 모니터 개선 사항.	6.7	상태 모니터에는 다음과 같은 향상된 기능이 추가되었습니다. • 상태 요약 페이지는 Firepower Management Center 및 management center가 관리하는 모든 디바이스의 상태를 한눈에 볼 수 있도록 합니다. • Monitoring(모니터링) 탐색창에서는 디바이스 계층 구조를 탐색할 수 있습니다. • 매니지드 디바이스는 개별적으로 나열되거나 해당하는 경우 지리적 위치, 고 가용성 또는 클러스터 상태에 따라 그룹화됩니다. • 탐색창에서 개별 디바이스에 대한 상태 모니터를 볼 수 있습니다. • 상호 관련된 메트릭을 상호 연결하는 맞춤형 대시 보드입니다. 사전 정의된 상관 관계 그룹(예: CPU 및 Snort) 중에서 선택합니다. 또는 사용 가능한 메트릭 그룹에서 고유한 변수 집합을 작성하여 사용자 정의 상관 관계 대시보드를 생성할 수도 있습니다.
기능이 디바이스에서 위협 데이터 업데이트 모듈로 이동되었습니다.	6.7	로컬 악성 코드 분석 모듈은 더 이상 사용되지 않습니다. 대신 이 정보는 디바이스의 위협 데이터 업데이트 모듈을 참조하십시오. 이전에는 보안 인텔리전스 모듈 및 URL 필터링 모듈에서 제공한 일부 정보가 디바이스의 위협 데이터 업데이트 모듈에서 제공되었습니다.
새 상태 모듈: 구성 메모리 할당.	7.0 6.6.3	버전 6.6.3에서는 디바이스 메모리 관리를 개선하고 새로운 상태 모듈인 구성 메모리 할당을 도입했습니다. 이 모듈은 구축된 구성의 크기로 인해 디바이스에서 메모리가 부족해질 위험이 있을 때 알려줍니다. 알림에는 구성에 필요한 메모리의 양과 사용 가능한 메모리를 초과하는 양이 표시됩니다. 이 경우 구성을 재평가하십시오. 종종 액세스 제어 규칙 또는 침입 정책의 수 또는 복잡성을 줄일 수 있습니다.
URL 필터링 모니터링 개선 사항.	6.5	이제 URL 필터링 모니터 모듈은 management center가 Cisco Cloud에 등록하지 못하면 알림을 보냅니다.
URL 필터링 모니터링 개선 사항.	6.4	이제 URL 필터링 모니터 경고에 대한 시간 임계값을 구성할 수 있습니다.
새 상태 모듈: 디바이스에서 위협 데이터 업데이트.	6.3	새 모듈 **Threat Data Updates on Devices(**디바이스에서 위협 데이터 업데이트**)**이 삭제되었습니다. 이 모듈은 디바이스가 위협 탐지에 사용하는 특정 인텔리전스 데이터 및 구성이 사용자가 지정한 기간 내에 디바이스에서 업데이트되지 않은 경우 알림을 보냅니다.

12 장

감사 및 시스템 로그

다음 주제에서는 시스템에서의 활동을 감사하는 방법을 설명합니다.

시스템 로그

시스템 로그(syslog) 페이지에서는 어플라이언스에 대한 시스템 로그 정보를 제공합니다.

시스템에서의 활동은 다음 두 가지 방법으로 감사할 수 있습니다. Firepower System에 속하는 어플라이언스는 사용자와 웹 인터페이스의 각 상호 작용에 대한 감사 기록을 생성하고 시스템 로그에 시스템 상태 메시지도 로깅합니다.

시스템 로그는 시스템에서 생성된 각 메시지를 표시합니다. 다음 항목이 순서대로 나열됩니다.

- 메시지가 생성된 날짜
- 메시지가 생성된 시간
- 메시지를 생성한 호스트
- 메시지 자체

시스템 로그 보기

시스템 로그 정보는 로컬입니다. 예를 들어 management center를 사용하여 매니지드 디바이스에서 시스템 로그의 시스템 상태 메시지를 볼 수 없습니다.

UNIX 파일 검색 유틸리티 Grep에서 허용되는 대부분의 구문을 사용하여 메시지를 필터링할 수 있습니다. 이에 따라 패턴 매칭에 Grep 호환 정규식을 사용할 수 있습니다.

시작하기 전에

시스템 통계를 보려면 관리자 또는 유지 보수 사용자여야 하며 전역 도메인에 있어야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Monitoring(**모니터링**)** > **Syslog(**시스템 로그**)**을(를) 선택합니다.

단계 **2** 시스템 로그에서 특정 메시지 내용을 검색하려면

a) 시스템 로그 필터 구문, 418 페이지에 설명된 대로 필터 필드에 단어 또는 쿼리를 입력합니다.

Grep 호환 검색 구문만 지원됩니다.

예:

사용자 이름 "Admin"이 포함된 모든 로그 항목을 검색하려면 `Admin`을 사용합니다.

11월 27일에 생성된 모든 로그 항목을 검색하려면 `Nov[[:space:]]*27` 또는 `Nov.*27`을 사용합니다(하지만 `Nov 27` 또는 `Nov*27` 은 사용하지 마십시오).

11월 5일의 권한 부여 디버깅 정보를 포함하는 모든 로그 항목을 검색하려면 `Nov[[:space:]]*5.*AUTH.*DEBUG`를 사용합니다.

b) 검색에서 대소문자를 구분하려면 **Case-sensitive**를 선택합니다. (기본적으로 필터는 대소문자를 구분하지 않습니다.)

c) 입력한 기준을 충족하지 않는 모든 시스템 로그 메시지를 검색하려면 **Exclusion**을 선택합니다.

d) **Go(**이동**)**를 클릭합니다.

시스템 로그 필터 구문

다음 표에서는 System Log 필터에서 사용할 수 있는 정규식 구문을 보여줍니다.

표 ***26:*** 시스템 로그 필터 구문

구문 구성 요소	설명	예
.	문자나 공백과 일치	`Admi.`는 `Admin`, `AdmiN`, `Admi1`, `Admi&`와 일치
`[[:alpha:]]`	알파벳 문자와 일치	`[[:alpha:]]dmin`은 `Admin`, `bdmin`, `Cdmin`과 일
`[[:upper:]]`	알파벳 대문자와 일치	`[[:upper:]]dmin`은 `Admin`, `Bdmin`, `Cdmin`과 일
`[[:lower:]]`	알파벳 소문자와 일치	`[[:lower:]]dmin`은 `admin`, `bdmin`, `cdmin`과 일
`[[:digit:]]`	숫자와 일치	`[[:digit:]]dmin`은 `0dmin`, `1dmin`, `2dmin`과 일
`[[:alnum:]]`	영숫자 문자와 일치	`[[:alnum:]]dmin`은 `1dmin`, `admin`, `2dmin`, `bdmi`
`[[:space:]]`	탭을 포함한 공백과 일치	`Feb[[:space:]]29`는 2월 29일의 로그와 일치
*	앞에 오는 0개 이상의 문자 또는 식 인스턴스와 일치	`ab*`는 `a`, `ab`, `abb`, `ca`, `cab`, `cabb`과 일치 `[ab] *`는 모두 일치

구문 구성 요소	설명	예
?	0개 또는 1개 인스턴스와 일치	ab?는 a 또는 ab와 일치
\	일반적으로 정규식 구문으로 해석되는 문자에 대한 검색 허용	alert\?는 alert?와 일치

시스템 감사 정보

Firepower System에 속하는 어플라이언스는 사용자와 웹 인터페이스의 각 상호 작용에 대한 감사 레코드를 생성합니다.

관련 항목

Standard Reports(표준 보고서), 541 페이지

감사 기록

Secure Firewall Management Center 사용자 활동에 대한 읽기 전용 감사 정보를 로깅합니다. 감사 로그는 감사 보기의 항목을 기준으로 감사 로그 메시지를 보고, 정렬하고, 필터링할 수 있는 표준 이벤트 보기에서 제공됩니다. 감사 정보를 손쉽게 삭제하고 보고할 수 있으며, 사용자가 변경한 내용에 대한 자세한 보고서를 볼 수 있습니다.

감사 로그에는 최대 100,000개의 항목이 저장됩니다. 감사 로그 항목 수가 100,000개를 초과하면 어플라이언스는 데이터베이스에서 가장 오래된 기록을 삭제하여 항목 수를 100,000개로 줄입니다.

감사 로그는 로그인 오류에 대한 사용자 또는 소스 IP를 표시하지 않습니다.

- 잘못된 비밀번호를 사용하면 소스 IP가 표시되지 않습니다.
- 사용자 계정이 없으면 소스 IP와 사용자가 모두 표시되지 않습니다.
- LDAP 사용자에 대한 시도가 실패하면 감사 로그가 트리거되지 않습니다.

관련 항목

Management Center에 대한 SSO 지침, 145 페이지

감사 레코드 보기

management center 감사 레코드의 테이블을 볼 수 있습니다. 사전 정의된 감사 워크플로에는 이벤트의 단일 테이블 보기가 포함되어 있습니다. 찾고 있는 정보에 따라 테이블 보기를 조작할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 절차를 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Monitoring(**모니터링**)** > **Audit(**감사**)**를 사용하여 감사 로그 워크플로에 액세스합니다.

단계 **2** 이벤트가 나타나지 않으면 시간 범위를 조정해야 할 수 있습니다. 자세한 내용은 이벤트 시간 제약 조건, 707 페이지를 참고하십시오.

참고 어플라이언스의 구성된 타임 윈도우(전역 또는 이벤트 전용 모두 해당)를 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 테이블의 열 내용을 자세히 알아보려면 시스템 로그, 417 페이지를 참조하십시오.
- 현재 워크플로 페이지에서 이벤트를 정렬하고 제한하려면 테이블 보기 페이지 사용, 698 페이지를 참조하십시오.
- 현재 제약 조건을 유지하면서 현재 워크플로의 페이지 사이를 이동하려면 워크플로 페이지의 왼쪽 위에서 해당 페이지 링크를 클릭합니다. 자세한 내용은 워크플로 사용, 689 페이지를 참고하십시오.
- 워크플로에서 다음 페이지로 드릴다운하려면 드릴다운 페이지 사용, 697 페이지 섹션을 참조하십시오.
- 특정 값으로 제한하려면 행 내의 값을 클릭합니다. 드릴다운 페이지에서 값을 클릭하면 다음 페이지로 이동하며 해당 값으로 제한됩니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 않습니다. 자세한 내용은 이벤트 보기 제약 조건, 713 페이지를 참조하십시오.

  팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

- 감사 레코드를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭하여 현재 제한된 보기의 모든 이벤트를 삭제합니다.
- 빠르게 돌아올 수 있도록 현재 페이지를 즐겨찾기하려면 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다. 자세한 내용은 북마크, 717 페이지를 참고하십시오.
- 즐겨찾기 관리 페이지로 이동하려면 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다. 자세한 내용은 북마크, 717 페이지를 참고하십시오.
- 현재 보기의 데이터를 기반으로 보고서를 생성하려면 **Report Designer(**리포트 디자이너**)**를 클릭합니다. 자세한 내용은 이벤트 보기에서 보고서 템플릿 생성, 546 페이지를 참고하십시오.
- 감사 로그에 기록된 변경의 요약을 보려면 **Message(**메시지**)** 열의 해당 이벤트 옆에 있는 **Compare(**비교**)**를 클릭합니다. 자세한 내용은 감사 로그를 사용하여 변경 검사, 422 페이지를 참고하십시오.

관련 항목

이벤트 보기 제약 조건, 713 페이지

감사 로그 워크플로 필드

다음 표는 보고 검색할 수 있는 감사 로그 필드를 설명합니다.

표 *27:* 감사 로그 필드

필드	설명
시간	어플라이언스가 감사 레코드를 생성한 시간과 날짜.
사용자	감사 이벤트를 트리거한 사용자의 사용자 이름.
하위 시스템	감사 레코드를 생성하기 위해 사용자가 따른 전체 메뉴 경로. 예를 들어 시스템 (⚙) > **Monitoring(**모니터링**)** > **Audit(**감사**)**는 감사 로그를 보기 위한 메뉴 경로입니다. 메뉴 경로와 관련이 없는 몇몇 경우에는 Subsystem(하위 시스템) 필드에 이벤트 유형만 표시됩니다. 예를 들어 **Login(**로그인**)**은 사용자 로그인 시도를 분류합니다.
메시지	사용자가 수행한 작업 또는 사용자가 페이지에서 클릭한 버튼. 예를 들어 `Page View(페이지 보기)`는 단순히 사용자가 Subsystem(하위 시스템)에 표시된 페이지를 봤음을 의미하는 반면, `Save(저장)`는 사용자가 페이지에서 **Save(**저장**)** 버튼을 클릭했음을 의미합니다. 시스템에 대한 변경 사항은 클릭하면 변경 사항 요약을 볼 수 있는 비교 아이콘과 함께 나타납니다.
소스 IP	사용자가 사용한 호스트와 연결된 IP 주소. 참고: 이 필드를 검색할 때는 특정 IP 주소를 입력해야 합니다. 로그 감사를 검색할 때는 IP 범위를 사용할 수 없습니다.
도메인	감사 이벤트가 트리거되었을 때 사용자의 현재 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
구성 변경 (검색만 해당)	검색 결과에서 구성 변경의 감사 레코드를 볼지 여부를 지정합니다. (예 또는 아니오)
개수	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

관련 항목

이벤트 검색, 721 페이지

감사 이벤트 테이블 보기

이벤트 보기의 레이아웃을 변경하거나 보기의 이벤트를 필드 값으로 제한할 수 있습니다. 열을 비활성화할 때 나타나는 팝업 윈도우에서 숨기려는 컬럼 헤드의 **Close(**닫기**)** (✕)를 클릭한 다음 **Apply(**적용**)**를 클릭합니다. 비활성화한 열은 나중에 다시 추가하지 않는 한 세션 기간 동안 비활성화됩니다. 첫 번째 열을 비활성화하면 Count(카운트) 열이 추가됩니다.

다른 열을 숨기거나 표시하려면, 또는 비활성화된 열을 다시 보기에 추가하려면, 해당 확인란을 선택하거나 선택 취소한 후 **Apply(**적용**)**를 클릭하십시오.

테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되고 워크플로의 다음 페이지로 드릴다운되지 않습니다.

팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

관련 항목

워크플로 사용, 689 페이지

감사 로그를 사용하여 변경 검사

일부 시스템 변경 사항에 대한 자세한 보고서를 보려면 감사 로그를 사용할 수 있습니다. 이러한 보고서는 시스템의 현재 구성을 지원되는 변경 이전의 최신 구성과 비교합니다.

Compare Configurations 페이지에는 차이점을 쉽게 파악할 수 있도록 변경 이전의 시스템 구성과 실행 중인 구성이 나란히 배치됩니다. 감사 이벤트 유형, 마지막 수정 시간 및 변경을 수행한 사용자의 이름이 각 구성 위의 제목 표시줄에 표시 됩니다.

두 구성의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 구성 사이에서 다름을 나타내고, 그러한 차이점은 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 구성에만 나타남을 의미합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 절차를 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Monitoring(**모니터링**)** > **Audit(**감사**)**을(를) 선택합니다.

단계 **2** **Message(**메시지**)** 열의 해당 감사 로그 이벤트 옆에 있는 **Compare(**비교**)**를 클릭합니다.

팁 제목 표시줄 위에 있는 **Previous(**이전**)** 또는 **Next(**다음**)**를 클릭하여 변경 사항을 개별적으로 탐색할 수 있습니다. 변경 요약의 길이가 한 페이지를 넘으면 오른쪽에 있는 스크롤바를 이용해 추가 변경 내용을 볼 수 있습니다.

감사 레코드 억제

감사 정책에서 Firepower System과의 특정 사용자 상호 작용 유형을 감사하도록 요구하지 않는 경우, 그러한 상호 작용이. 예를 들어 기본적으로 사용자가 온라인 도움말을 볼 때마다 Firepower System은 감사 레코드를 생성합니다. 이러한 상호 작용 레코드를 유지할 필요가 없으면 자동으로 억제할 수 있습니다.

감사 이벤트 억제를 구성하려면 어플라이언스의 `admin` 사용자 계정에 대한 액세스 권한이 있어야 하며, 어플라이언스의 콘솔에 액세스하거나 SSH(Secure Shell)를 열 수 있어야 합니다.

주의 권한이 있는 사용자만 어플라이언스 및 `admin` 계정에 액세스할 수 있습니다.

시작하기 전에

이 절차를 수행하려면 관리자 사용자여야 합니다.

프로시저

`/etc/sf` 디렉터리에서 다음 형식으로 `AuditBlock` 파일을 생성합니다. 여기서 type은 감사 블록 유형, 423 페이지에 설명된 유형 중 하나입니다.

`AuditBlock.type`

참고 특정 유형의 감사 메시지에 대해 `AuditBlock.type` 파일을 생성한 후 억제를 해제하려는 경우 `AuditBlock.type` 파일의 내용을 삭제하되 파일 자체는 Firepower System에 남겨두어야 합니다.

감사 블록 유형

각 감사 블록 유형의 내용은 다음 표에 설명한 것처럼 특정 형식으로 지정해야 합니다. 파일 이름에 대/소문자를 정확하게 사용해야 합니다. 파일의 내용 역시 대/소문자를 구분합니다.

`AuditBlock` 파일을 추가하면 `Audit` 하위 시스템과 `Audit Filter type Changed` 메시지가 있는 감사 레코드가 감사 이벤트에 추가됩니다. 보안상의 이유로 이 감사 레코드는 억제할 수 없습니다.

표 ***28:*** 감사 블록 유형

유형	설명
주소	`AuditBlock.address` 파일을 생성하고, 감사 로그에서 억제하려는 각 IP 주소를 한 줄에 하나씩 포함합니다. 주소의 시작 부분부터 매핑되는 경우, 부분적인 IP 주소를 사용할 수 있습니다. 예를 들어 부분 주소 `10.1.1`은 `10.1.1.0~10.1.1.255` 범위의 주소와 일치합니다.

유형	설명
메시지	이름이 `AuditBlock.message`인 파일을 생성하고, 억제하려는 메시지 하위 문자열을 한 줄에 하나씩 포함합니다. 파일에 `backup`을 포함하면 `backup`이라는 단어가 포함된 모든 메시지가 억제되도록 하위 문자열이 매칭됩니다.
하위 시스템	이름이 `AuditBlock.subsystem`인 파일을 생성하고, 억제하려는 각 하위 시스템을 한 줄에 하나씩 포함합니다. 하위 문자열은 매칭되지 않습니다. 정확한 문자열을 사용해야 합니다. 감사 대상 하위 시스템 목록은 감사 하위 시스템, 424 페이지를 참조하십시오.
사용자	이름이 `AuditBlock.user`인 파일을 생성하고, 억제하려는 각 사용자 계정을 한 줄에 하나씩 포함합니다. 사용자 이름의 시작 부분부터 매핑되는 것이라면 부분적인 문자열 매칭을 사용할 수 있습니다. 예를 들어 부분적 사용자 이름 `IPSAnalyst`는 사용자 이름 `IPSAnalyst1` 및 `IPSAnalyst2`과 일치합니다.

감사 하위 시스템

다음 표에는 감사 대상 하위 시스템이 나열되어 있습니다.

표 ***29:*** 하위 시스템 이름

이름	포함되는 사용자 상호 작용
Admin(관리자)	시스템 및 액세스 구성, 시간 동기화, 백업 및 복원, 디바이스 관리, 사용자 계정 예약 등의 관리 기능
알림	이메일, SNMP, syslog 알림 등의 알림 기능
감사 로그	감사 이벤트 보기
감사 로그 검색	감사 이벤트 검색
명령행	명령줄 인터페이스
구성	이메일 알림
상황별로 크로스 실행	시스템에 추가되거나 대시보드 및 이벤트 보기에서 액세스한 외부 리소스
COOP	운영 연속성 기능
날짜	이벤트 보기의 날짜 및 시간 범위
기본 하위 시스템	할당된 하위 시스템이 없는 옵션
탐지 및 예방 정책	침입 정책에 대한 메뉴 옵션
오류	시스템 레벨 오류

이름	포함되는 사용자 상호 작용
eStreamer	eStreamer 구성
최종 사용자 라이선스 계약	최종 사용자 라이선스 계약 검토
이벤트	침입 및 검색 이벤트 보기
검토된 이벤트	검토된 침입 이벤트
이벤트 검색	모든 이벤트 검색
규칙 업데이트 `rule_update_id` 설치 실패	규칙 업데이트 설치 중
헤더	사용자 로그인 후 유저 인터페이스의 초기 표시
상태	상태 모니터링
상태 이벤트	상태 모니터링 이벤트 보기
도움말	온라인 도움말
고가용성	고가용성 쌍에서 management center 설정 및 처리
IDS 영향 플래그	침입 이벤트에 대한 영향 플래그 구성
IDS 정책	침입 정책
IDSRule sid:`sig_id` rev:`rev_num`	SID 기준 침입 규칙
설치	업데이트 설치
침입 이벤트	침입 이벤트
로그인	웹 인터페이스 로그인 및 로그 아웃 기능
Logout	웹 인터페이스 로그아웃 기능
메뉴	모든 메뉴 옵션
Configuration export > `config_type` > `config_name`	특정 유형 및 이름의 구성가져오기
권한 에스컬레이션	사용자 역할 에스컬레이션
선호	사용자 계정의 표준 시간대와 개별 이벤트 환경 설정 등의 사용자 환경
정책	침입 정책을 비롯한 모든 정책
등록	다음에서 디바이스 등록: management center
RemoteStorageDevice	원격 스토리지 디바이스 구성

이름	포함되는 사용자 상호 작용
보고서	보고서 나열 및 리포트 디자이너 기능
규칙	침입 규칙 편집기 및 규칙 가져오기 프로세스를 비롯한 침입 규칙
규칙 업데이트 가져오기 로그	규칙 업데이트 가져오기 로그 보기
규칙 업데이트 설치	규칙 업데이트 설치 중
세션 만료	웹 인터페이스 세션 시간 초과
상태	Syslog, 호스트 및 성능 통계
시스템	다양한 시스템 전체 설정
작업 대기열	백그라운드 프로세스 상태 보기
사용자	사용자 계정과 역할 생성 및 수정

외부 위치로 감사 로그 전송 정보

감사 로그를 FMC에서 외부 위치로 전송하는 방법은 다음을 참조하십시오.

- 감사 로그, 47 페이지
- 감사 로그 인증서, 51 페이지

13 장

통계

다음 항목에서는 Firepower 시스템을 모니터링 하는 방법을 설명합니다.

시스템 통계 관련 정보

Statistics(통계) 페이지에는 디스크 사용 및 시스템 프로세스, Data Correlator(데이터 상관 처리) 통계 및 침입 이벤트 정보를 포함한 일반 어플라이언스 통계의 현재 상태가 나와 있습니다.

호스트 통계 섹션

다음 표는 Statistics(통계 자료) 페이지에 나열된 호스트 통계 자료에 대해 설명합니다.

표 ***30:*** 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
로드 평균	지난 1분, 5분 15분 동안 CPU 큐 프로세스의 평균 수.

카테고리	설명
디스크 사용	사용 중인 디스크의 백분율 자세한 호스트 통계 자료를 보려면 화살표를 클릭합니다.
프로세스	시스템에서 실행 중인 프로세스의 요약.

Disk Usage(디스크 사용량) 섹션

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.

팁 또한 디스크 사용량 상태 모니터를 통해 디스크 사용량을 모니터링하고 디스크 공간 부족에 대해 알림을 보낼 수도 있습니다.

Processes(프로세스) 섹션

통계 페이지의 Processes(프로세스) 섹션에서는 현재 어플라이언스에서 실행 중인 프로세스를 볼 수 있습니다. 이 섹션에서는 실행되고 있는 각 프로세스에 대한 일반 처리 정보 및 특정 정보를 제공합니다. management center의 웹 인터페이스를 사용해 관리되는 모든 디바이스의 프로세스 상태를 볼 수 있습니다.

어플라이언스에서는 데몬 및 실행 파일이라는 두 가지 유형의 프로세스가 실행됩니다. 데몬은 항상 실행되며, 실행 파일은 필요한 경우 실행됩니다.

프로세스 상태 필드

통계 페이지의 프로세스 섹션을 확장하는 경우 다음을 확인할 수 있습니다.

CPU

다음 CPU 사용 정보를 확인할 수 있습니다.

- 사용자 처리 사용 백분율
- 시스템 처리 사용 백분율
- nice 사용 백분율(더 높은 우선 순위를 나타내는 음수인 nice 값을 지닌 프로세스의 CPU 사용량) nice 값은 시스템 프로세스에 대해 예약된 우선 순위를 나타내며 그 범위는 -20(가장 높은 우선 순위)에서 19(가장 낮은 우선 순위)까지입니다.
- 유휴 사용 백분율

MEM

다음 메모리 사용 정보를 확인할 수 있습니다.

- 메모리 내 총 킬로바이트 수
- 메모리 내 사용된 킬로바이트의 총 수
- 메모리 내 무료 킬로바이트의 총 수
- 메모리 내 버퍼된 킬로바이트의 총 수

Swap(스왑)

다음 스왑 사용 정보를 확인할 수 있습니다.

- 스왑 내 총 킬로바이트 수
- 스왑 내 사용된 킬로바이트의 총 수
- 스왑 내 무료 킬로바이트의 총 수
- 스왑 내 캐시된 킬로바이트의 총 수

다음 테이블은 프로세스 섹션의 각 열에 대해 설명합니다.

표 ***31:*** 프로세스 목록 열

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. 그 범위는 -20(가장 높은 우선 순위)에서 19(가장 낮은 우선 순위)까지입니다.
크기	프로세스가 사용하는 메모리 크기(메가바이트를 나타내는 m표시가 없는 경우 킬로바이트 값)
Res	메모리에 상주하는 페이징 파일의 양(메가바이트를 나타내는 m이 값 뒤에 오지 않는 한 킬로바이트 단위)

열	설명
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 큐에서 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

관련 항목

시스템 데몬, 430 페이지
실행 파일및 시스템 유틸리티, 432 페이지

시스템 데몬

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 ***32:*** 시스템 데몬

데몬	설명
crond	예약된 명령의 실행을 관리합니다(cron 작업).
dhclient	동적 호스트 IP 주소 부여를 관리합니다.
fpcollect	클라이언트 및 서버 지문의 컬렉션을 관리합니다.

데몬	설명
httpd	HTTP(Apache 웹 서버) 프로세스를 관리합니다.
httpsd	HTTPS(SSL을 사용하는 Apache 웹 서버) 서비스를 관리하고 작동하는 SSL 및 유 인증을 확인하며, 어플라이언스에 보안 웹 액세스를 제공하는 백그라운드에서
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	데이터베이스 프로세스를 관리합니다.
ntpd	NTP(Network Time Protocol)프로세스를 관리합니다
pm	모든 시스템 프로세스를 관리하고 필요한 프로세스를 시작하며, 예기치 않게 실 로세스를 다시 시작합니다.
reportd	보고서를 관리합니다.
safe_mysqld	데이터베이스의 안전 모드 운영을 관리하고 오류가 발생하고 파일에 런타임 정 경우 데이터베이스 데몬을 다시 시작합니다.
SFDataCorrelator	데이터 전송을 관리합니다.
sfestreamer(management center만)	Event Streamer를 사용하는 서드파티 클라이언트 애플리케이션에 대한 연결을
sfmgr	어플라이언스로 향하는 sftunnel 연결을 사용하여 어플라이언스의 원격 관리 및 RPC 서비스를 제공합니다.
SFRemediateD(management center만)	교정 응답을 관리합니다.
sftimeserviced(management center만)	시간 동기화 메시지를 관리되는 디바이스에 전달합니다.
sfmbservice	어플라이언스에 대한 sftunnel 연결을 사용하여 원격 어플라이언스에서 실행되는 지 브로커 프로세스에 대한 액세스를 제공합니다. 현재는 상태 모니터가 매니지 에서 management center로 상태 이벤트 및 알림을 전송하는 데 사용됩니다.
sftroughd	수신 소켓에서 연결을 수신한 후 요청을 처리하기 위해 올바른 실행 파일(일반적 메시지 브로커, sfmb)을 호출합니다.
sftunnel	원격 어플라이언스와의 통신이 필요한 모든 프로세스에 안전한 커뮤니케이션 채 니다.

데몬	설명
sshd	SSH(Secure Shell) 프로세스를 관리하고 어플라이언스에 SSH 액세스를 제공하는 백에서 실행됩니다.
syslogd	시스템 로깅(syslog) 프로세스를 관리합니다.

실행 파일및 시스템 유틸리티

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 ***33:*** 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.
SFDataCorrelator(management center만)	이벤트, 연결 데이터, 네트워크 맵을 생성하기 위해 시스템이 생성한 이진 파일을 분석합니다.
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.

실행 파일	설명
iptables	Access Configuration(액세스 구성) 페이지에 적용된 변경 사항에 기반하여 액세스 제한을 처리합니다.
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 (이름을 바꾸는) 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.
ps	표준 출력에 처리 정보를 작성하는 유틸리티입니다.
sed	하나 이상의 텍스트 파일을 수정하는 데 사용하는 유틸리티입니다.
sfheartbeat	어플라이언스가 활성 상태임을 나타내는 하트비트 브로드캐스트를 식별합니다. 하트비트는 디바이스와 management center 사이의 연결을 유지하는 데 사용됩니다.
sfmb	메시지 브로커 프로세스를 나타내며 management center과 디바이스 간 통신을 처리합니다.
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.

실행 파일	설명
snmptrap	SNMP 알림 기능이 활성화된 경우 지정된 SNMP 트랩 서버에 SNMP 트랩 데이터를 전달합니다.
snort	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. 참고 이 유틸리티의 CPU 사용량 출력은 CPU 코어의 여러 사용량 유형이 분할된 것입니다. 실제 총 CPU 사용량을 확인하려면 사용자 프로세스와 시스템 프로세스 사용량을 모두 추가해야 합니다. top 명령의 출력 예: `%Cpu(s): 76.6 us, 22.1 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 1.3 si, 0.0 st` 여기서 CPU 시간의 76.6%는 사용자 프로세스에 의해, CPU 시간의 22.1%는 시스템(커널) 프로세스에 의해 사용됩니다. 총 CPU 사용량은 98.7%입니다. 따라서 이 유틸리티에서 보고되는 CPU 사용량은 상태 모니터 대시보드와 다르게 나타납니다. 또한, 이 유틸리티는 3초 간격을 사용하여 CPU 사용량을 계산합니다. 반면 Management Center 상태 모니터는 1초 간격을 사용합니다.
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.

관련 항목

액세스 목록 구성, 45 페이지

SFDataCorrelator 프로세스 통계 섹션

management center에서 현재 날짜까지의 Data Correlator 및 네트워크 검색 프로세스에 대한 통계를 볼 수 있습니다. 관리되는 디바이스가 데이터 수집, 디코딩 및 분석을 수행하는 동안 네트워크 검색 프로세스는 데이터를 지문 및 취약성 데이터베이스와 상호 연결한 다음, management center에서 실행되는 Data Correlator에 의해 처리되는 이진 파일을 생성합니다. The Data Correlator는 이진 파일의 정보를 분석하고 이벤트를 생성하고 네트워크 맵을 만듭니다.

네트워크 검색 및 Data Correlator에 표시되는 통계는 현재 날짜의 평균으로 오전 12:00부터 오후 11:59 사이에 각 기기에서 수집된 통계가 사용됩니다.

다음 테이블은 Data Correlator 프로세스에 표시되는 통계에 대해 설명합니다.

표 ***34: Data Correlator*** 프로세스 통계

카테고리	설명
이벤트/초	Data Correlator에서 초당 수신하여 처리하는 검색 이벤트의 수
연결/초	Data Correlator에서 초당 수신하여 처리하는 연결의 수
CPU 사용량 — 사용자(%)	현재 날짜에 대해 사용자 프로세스에 소비되는 평균 CPU 시간의 비율
CPU 사용량 — 시스템(%)	현재 날짜에 대해 시스템 프로세스에 소비되는 평균 CPU 시간의 비율
VmSize(KB)	현재 날짜에 대해 Data Correlator에 할당된 평균 메모리의 크기(킬로바이트 단위)
VmRSS	현재 날짜에 대해 Data Correlator에서 사용하는 평균 메모리의 양(킬로바이트 단위)

침입 이벤트 정보 섹션

management center 및 관리되는 디바이스의 통계 페이지에서 침입 이벤트에 대한 요약 정보를 볼 수 있습니다. 이 정보에는 마지막 침입 이벤트 날짜 및 시간, 이전 시간 및 날짜에 발생한 총 이벤트 수, 데이터베이스의 총 이벤트 수가 포함됩니다.

참고 통계 페이지 내 침입 이벤트 정보 섹션의 정보는 management center에 전송된 침입 이벤트가 아니라 관리되는 디바이스에 저장된 침입 이벤트를 기반으로 합니다. 만약 관리되는 디바이스가 로컬에서 침입 이벤트를 저장할 수 없는 (또는 저장하지 않도록 설정된) 경우 이 페이지에 침입 이벤트가 표시되지 않습니다.

다음 테이블은 통계 페이지의 침입 이벤트 정보 섹션에 표시되는 통계에 대해 설명합니다.

표 ***35:*** 침입 이벤트 정보

통계	설명
최근 경보	마지막 이벤트가 발생한 날짜 및 시간을 나타냅니다.
최근 1시간의 전체 이벤트	최근 1시간 동안 발생한 전체 이벤트 수를 나타냅니다.
최근 1일의 전체 이벤트	지난 24시간 동안 발생한 전체 이벤트 수를 나타냅니다.

통계	설명
데이터베이스의 전체 이벤트	이벤트 데이터베이스에 있는 전체 이벤트 수를 나타냅니다.

시스템 통계 보기

management center 및 관련 매니지드 디바이스에 대한 통계도 표시됩니다.

시작하기 전에

시스템 통계를 보려면 관리자 또는 유지 보수 사용자여야 하며 전역 도메인에 있어야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Monitoring(**모니터링**)** > **Statistics(**통계**)**을(를) 선택합니다.

단계 **2** **Select Device(s)(**디바이스 선택**)** 목록에서 디바이스를 선택하고 **Select Devices(**디바이스 선택**)**를 클릭합니다.

단계 **3** 사용 가능한 통계를 봅니다.

단계 **4** 디스크 사용량 섹션에서 다음을 수행할 수 있습니다.

- 다음을 보려면 **By Category(**카테고리별로**)** 누적 막대의 디스크 사용량 카테고리 위에 포인터를 올려 놓습니다. (순서대로)
  - 해당 카테고리에 사용된 사용 가능한 디스크 공간의 백분율
  - 디스크의 실제 저장 공간
  - 해당 카테고리에 사용 가능한 모든 디스크 공간
- **By Partition(**파티션별**)** 옆의 화살표를 클릭하여 확대합니다. 악성코드 스토리지 팩이 설치되어 있는 경우, `/var/storage` 파티션 사용량이 표시됩니다.

단계 **5** (선택 사항) 시스템 통계 보기, 436 페이지에 설명된 정보를 보려면 **Processes(**프로세스**)** 옆의 화살표를 클릭합니다.

14 장

문제 해결

다음 주제에서는 Firepower System에서 발생할 수 있는 문제를 진단하는 방법을 설명합니다.

문제 해결의 첫 번째 단계

- 문제 해결을 위해 변경을 수행하기 전에 원래 문제를 캡처하기 위한 문제 해결 파일을 생성합니다. 문제 해결을 위한 상태 모니터 보고서, 450 페이지 및 그 하위 섹션을 참조하십시오.

  Cisco TAC에 지원 문의를 하는 경우 이 문제 해결 파일이 필요한 경우가 있습니다.

- 메시지 센터에서 오류 및 경고 메시지를 확인하여 검사를 시작합니다. 시스템 메시지, 438 페이지의 내용을 참조하십시오.

- 제품의 제품 문서 중 "문제 해결 및 알림"에 수록된 관련 기술 노트 및 다른 문제 해결 자료를 참고하십시오. 문제 해결의 첫 번째 단계, 437 페이지의 내용을 참조하십시오.

시스템 메시지

Firepower System에서 발생한 문제를 추적하려면 메시지 센터에서 조사를 시작하십시오. 이 기능을 사용하면 Firepower System에서 지속적으로 생성하는 시스템 활동 및 상태에 대한 메시지를 볼 수 있습니다.

메시지 센터를 열려면 메인 메뉴의 Deploy(구축) 메뉴 옆에 있는 시스템 상태 아이콘을 클릭합니다. 이 아이콘은 시스템 상태에 따라 다음 중 하나의 형태를 취합니다.

- - 시스템에 하나 이상의 오류 및 경고가 발생했음을 나타냅니다.
- - 시스템에 오류 없이 하나 이상의 경고가 발생했음을 나타냅니다.
- - 시스템에 발생한 오류 및 경고가 없음을 나타냅니다.

아이콘에 표시된 숫자는 전체 오류 및 경고 메시지의 수를 나타냅니다.

메시지 센터를 닫으려면 Firepower System 웹 인터페이스에서 메시지 센터의 범위를 벗어난 아무 곳이나 클릭합니다.

메시지 센터 외에도 웹 인터페이스는 사용자 활동 및 현재 진행 중인 시스템 활동에 대해 즉시 팝업 알림을 표시합니다. 일부 팝업 알림은 5초 후 자동으로 사라지지만 "스티커" 알림은 **Dismiss(해제)** ()을 클릭해 취소하기 전까지 표시됩니다. 모든 알림을 취소하려면 알림 목록 상단의 취소 링크를 클릭합니다.

팁 비 스티커 팝업 알림 위에 커서를 올려 놓으면 알림이 고정됩니다.

시스템은 라이선스, 도메인, 액세스 역할에 따라 사용자에게 팝업 알림과 메시지 센터 중 하나를 선택하여 메시지를 표시합니다.

메시지 유형

메시지 센터의 시스템 활동 및 상태를 보고하는 메시지는 세 가지 탭으로 구성됩니다.

구축

이 탭에는 도메인별로 그룹화된 시스템의 각 어플라이언스에 대한 설정 구축과 관련된 현재 상태가 표시됩니다. 이 탭에서 시스템은 다음 구축 상태 값을 보고합니다. 기록 표시를 클릭하여 구축에 대한 추가 상세정보를 얻을 수 있습니다.

- 실행 중(회전 중인) - 설정이 구축 중입니다.
- 성공 - 설정이 성공적으로 구축되었습니다.
- **Warning(경고)** () - 경고 구축 상태는 경고 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

- 실패 - 설정 구축에 실패했습니다. 만료된 정책의 내용을 참조하시기 바랍니다. 구축 실패는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

업그레이드

이 탭에는 매니지드 디바이스의 소프트웨어 업그레이드 작업과 관련된 현재 상태가 표시됩니다. 이 탭에서 시스템은 다음 업그레이드 상태 값을 보고합니다.

- **In progress(**진행 중**)** — 업그레이드 작업이 진행 중임을 나타냅니다.
- **Completed(**완료됨**)** - 소프트웨어 업그레이드 작업이 성공적으로 완료되었음을 나타냅니다.
- **Failed(**실패**)** - 소프트웨어 업그레이드 작업을 완료하지 못했음을 나타냅니다.

상태

이 탭은 도메인별로 그룹화된 시스템의 각 어플라이언스에 대한 현재 상태 정보가 표시됩니다. 상태는 상태 모니터링 정보, 369 페이지에서 설명한 상태 모듈에 의해 생성됩니다. 이 탭에서 시스템은 다음 상태 값을 보고합니다.

- **Warning(**경고**)** () - 어플라이언스의 상태 모듈에 대한 경고 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다. 상태 모니터링 페이지는 **Yellow Triangle(**노란색 삼각형**)** ()을 사용하여 이 상태를 표시합니다. 경고 상태는 경고 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- **Critical(**중요**)** () - 어플라이언스의 상태 모듈에 대한 위험 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다. 상태 모니터링 페이지는 **Critical(**중요**)** () 아이콘을 사용하여 이 상태를 표시합니다. 위험 상태는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- **Error(**오류**)** () - 어플라이언스에서 상태 모니터링 모듈의 오류가 발생했으며 오류 발생 이후 성공적으로 다시 실행되지 않았음을 나타냅니다. 상태 모니터링 페이지는 오류 아이콘을 사용하여 이 상태를 표시합니다. 오류 상태는 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.

상태 모니터링 페이지에서 관련 상세정보를 보려면 상태 탭의 링크를 클릭하십시오. 현재 상태 조건이 없는 경우 상태 탭은 메시지를 표시하지 않습니다.

작업

일부 작업(구성 백업 또는 업데이트 설치)을 완료하는 데 시간이 걸릴 수 있습니다. 이 탭은 이러한 장기 작업 및 사용자 또는 적절한 액세스가 가능한 시스템의 다른 사용자가 시작한 작업 상태를 표시합니다. 이 탭은 각 메시지의 최신 업데이트를 기준으로 시간 반대순으로 메시지를 표시합니다. 일부 작업 상태 메시지는 문제의 작업에 대한 자세한 정보를 안내하는 링크를 포함합니다. 이 탭에서 시스템은 다음 작업 상태 값을 보고합니다.

- 대기() - 실행 중인 다른 작업이 완료될 때까지 작업이 실행 대기 중임을 나타냅니다. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.

- 실행 중 - 작업이 실행 중임을 나타냅니다. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 재시도() - 작업이 자동으로 재시도함을 나타냅니다. 모든 작업의 재시도가 허용되는 것은 아니라는 점에 유의하십시오. 이 메시지 유형은 업데이트 진행 표시줄을 표시합니다.
- 성공() - 작업이 성공적으로 완료됨을 나타냅니다.
- 실패() - 작업이 성공적으로 완료되지 않음을 나타냅니다. 오류 작업은 오류 시스템 상태 아이콘과 함께 표시되는 메시지 수와 관련이 있습니다.
- 중단 또는 정지() - 작업이 시스템 업데이트 때문에 중단됨을 나타냅니다. 중단된 작업은 다시 시작할 수 없습니다. 정상 작업이 복구되면 작업을 다시 시작합니다.
- 건너뜀 - 진행 중인 프로세스 때문에 작업을 시작할 수 없었습니다. 다시 시도해 작업을 시작하십시오.

새 작업이 시작되면 이 탭에 새 메시지가 표시됩니다. 작업이 완료(상태 성공, 실패, 중단)되면 이 탭은 사용자가 제거할 때까지 최종 상태 메시지를 표시합니다. 작업 탭 및 메시지 데이터베이스가 불필요하게 복잡해지지 않도록 메시지를 제거하는 것이 좋습니다.

메시지 관리

메시지 센터에서 다음을 수행할 수 있습니다.

- 팝업 알림을 표시하려면 선택합니다.
- 시스템 데이터베이스에서 추가 작업 상태 메시지를 표시합니다(제거되지 않아 사용 가능한 경우).
- 작업 상태 메시지를 하나씩 제거합니다. (제거된 메시지를 볼 수 있는 모든 사용자에게 적용됩니다.)
- 작업 상태 메시지를 한꺼번에 제거합니다. (제거된 메시지를 볼 수 있는 모든 사용자에게 적용됩니다.)

팁 데이터베이스 및 표시가 불필요하게 복잡해지지 않도록 작업 탭에서 누적된 작업 상태 메시지를 정기적으로 제거하는 것이 좋습니다. 데이터베이스의 메시지 수가 100,000개에 근접하면 시스템이 자동으로 제거한 작업 상태 메시지를 삭제합니다.

기본 시스템 정보 보기

About(정보) 페이지에는 시스템의 모델, 일련 번호, 다양한 구성 요소에 대한 버전 정보 등 어플라이언스에 대한 정보가 표시됩니다. 또한 Cisco 저작권 정보도 포함되어 있습니다.

프로시저

단계 **1** 페이지 상단에 있는 툴바에서 도움말( )를 클릭합니다.

단계 **2** **About(**정보**)**를 선택합니다.

어플라이언스 정보 보기

프로시저

시스템 ( ) > **Configuration(**구성**)**을(를) 선택합니다.

시스템 메시지 관리

프로시저

단계 **1** **Notifications(**알림**)**를 클릭하여 메시지 센터를 표시합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 구성 구축과 관련된 메시지를 보려면 배포를 클릭합니다. 구축 메시지 보기, 442 페이지의 내용을 참조하십시오. 이러한 메시지를 보려면 관리자 사용자이거나 디바이스에 구성 구축 권한이 있어야합니다.
- 디바이스 업그레이드 작업과 관련된 메시지를 보려면 **Upgrades(**업그레이드**)**를 클릭합니다. 업그레이드 메시지 보기를 참조하십시오. 업그레이드 메시지 보기를 참조하십시오. 이러한 메시지를 보려면 관리자 사용자이거나 **Updates(**업데이트**)** 권한이 있어야 합니다.
- management center 및 등록된 디바이스의 상태와 관련된 메시지를 보려면 상태를 클릭합니다. 상태 메시지 보기, 443 페이지의 내용을 참조하십시오. 이러한 메시지를 보려면 관리자 사용자이거나 상태 권한이 있어야 합니다.
- 장기 작업과 관련된 메시지를 보려면 작업를 클릭합니다. 작업 메시지 보기, 444 페이지 또는 작업 메시지 관리, 444 페이지를 참조하십시오. 누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks(**다른 사용자의 작업 보기**)** 권한이 있어야 합니다.
- 알림 표시 슬라이더를 클릭하여 팝업 알림 표시를 활성화하거나 비활성화합니다.

구축 메시지 보기

이러한 메시지를 보려면 관리자 사용자이거나 디바이스에 구성 구축 권한이 있어야합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** **Deployments(**구축**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- **total(**전체**)**을 클릭하여 모든 현재 구축 상태를 확인합니다.
- 특정 상태 값을 클릭하여 해당 구축 상태의 메시지만 확인합니다.
- 경과된 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **1m 5s(1**분 **5**초**)**)에서 구축의 경과된 시간과 시작 및 중지 시간을 확인합니다.

단계 **4** **show deployment history(**구축 내역 표시**)**를 클릭하여 구축 작업에 대한 자세한 정보를 확인합니다.

Deployment History(구축 내역) 테이블의 왼쪽 열에는 구축 작업이 시간의 역순으로 나열됩니다.

a) 구축 작업을 선택합니다.

테이블의 오른쪽 열에는 작업에 포함된 각 디바이스와 디바이스별 구축 상태가 표시됩니다.

b) 디바이스의 응답과 구축 중에 디바이스로 전송된 명령을 확인하려면 디바이스의 **Transcript(**기록**)** 열에 있는 다운로드를 클릭합니다.

기록은 다음 섹션으로 구성되어 있습니다.

- **Snort Apply(Snort** 적용**)** - Snort 관련 정책에서 장애 또는 응답이 발생하는 경우 이 섹션에 메시지가 표시됩니다. 일반적으로 이 섹션은 비어 있습니다.
- **CLI Apply(CLI** 적용**)** - 이 섹션에는 Lina 프로세스로 전송된 명령을 사용하여 구성된 기능이 포함되어 있습니다.
- **Infrastructure Messages(**인프라 메시지**)** - 이 섹션에는 여러 구축 모듈의 상태가 표시됩니다.

CLI Apply(CLI 적용**)** 섹션의 구축 기록에는 디바이스로 전송된 명령과 디바이스에서 반환된 응답이 포함되어 있습니다. 이러한 응답은 정보 메시지 또는 오류 메시지일 수 있습니다. 장애가 발생한 구축의 경우 명령 오류를 나타내는 메시지를 확인합니다. FlexConfig 정책을 사용하여 맞춤화된 기능을 구성하는 경우 이러한 오류를 검사하면 특히 유용할 수 있습니다. 이 오류를 확인하여 명령을 구성하려는 FlexConfig 개체의 스크립트를 수정할 수 있습니다.

참고 관리 기능에 대해 전송된 명령과 FlexConfig 정책에서 생성된 명령이 기록에서 구분되지는 않습니다.

예를 들어 다음 시퀀스에서는 management center가 외부에서 논리적 이름으로 GigabitEthernet0/0을 구성하기 위해 명령을 전송했음을 확인할 수 있습니다. 디바이스가 보안 레벨을 0으로 자동 설정했다고 응답했습니다. threat defense는 보안 레벨을 사용하지 않습니다.

```
========== CLI APPLY ==========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

업그레이드 메시지 보기

이러한 메시지를 보려면 관리자 사용자이거나 **Updates(**업데이트**)** 권한이 있어야 합니다.

프로시저

단계 **1** **Notifications(**알림**)**를 클릭하여 메시지 센터를 표시합니다.

단계 **2** **Upgrades(**업그레이드**)**를 클릭합니다.

단계 **3** 다음을 수행할 수 있습니다.

- **total(**전체**)**을 클릭하여 모든 현재 업그레이드 작업을 확인합니다.
- 특정 상태 메시지만을 보려면 상태 값을 클릭합니다.
- 업그레이드 작업에 대한 자세한 내용을 보려면 **Device Management(**디바이스 관리**)**를 클릭합니다.

상태 메시지 보기

이러한 메시지를 보려면 관리자 사용자이거나 상태 권한이 있어야 합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** **Health(**상태**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 모든 현재 상태를 확인하려면 **total(**전체**)**을 클릭합니다.
- 특정 상태 메시지만을 확인하려면 상태 메시지를 클릭합니다.
- 상대 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **3 day(s) ago(3**일 전**)**)에서 해당 메시지에 대한 가장 최근 업데이트 시간을 확인합니다.
- 특정 메시지에 대한 자세한 상태 정보를 보려면 메시지를 클릭합니다.

- 상태 모니터링 페이지에서 전체 상태를 보려면 상태 모니터를 클릭합니다.

관련 항목

상태 모니터링 정보, 369 페이지

작업 메시지 보기

누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks(**다른 사용자의 작업 보기**)** 권한이 있어야 합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** **Tasks(**작업**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- **total(**전체**)**을 클릭하여 모든 현재 작업 상태를 확인합니다.
- 특정 상태 값을 클릭하여 해당 상태의 작업에 대한 메시지만 확인합니다.

  참고 중지된 작업에 대한 메시지는 작업 상태 메시지의 전체 목록에만 표시됩니다. 중지된 작업을 필터링할 수는 없습니다.

- 상대 시간 표시기 위에 커서를 놓으면 표시되는 메시지(예: **3 day(s) ago(3**일 전**)**)에서 해당 메시지에 대한 가장 최근 업데이트 시간을 확인합니다.
- 메시지 내의 링크를 클릭하여 작업에 대한 자세한 정보를 확인합니다.
- 추가 작업 상태 메시지를 표시할 수 있는 경우 메시지 목록의 맨 아래에 있는 **Fetch more messages(**메시지 더 가져오기**)**를 클릭하여 해당 메시지를 검색합니다.

작업 메시지 관리

누구나 자신의 작업을 볼 수 있습니다. 다른 사용자의 작업을 보려면 관리자 사용자이거나 **View Other Users' Tasks(**다른 사용자의 작업 보기**)** 권한이 있어야 합니다.

프로시저

단계 **1** 시스템 상태를 클릭하여 메시지 센터를 표시합니다.

단계 **2** Tasks(작업)를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 추가 작업 상태 메시지를 표시할 수 있는 경우 메시지 목록의 맨 아래에 있는 **Fetch more messages(**메시지 더 가져오기**)**를 클릭하여 해당 메시지를 검색합니다.

- 완료된 작업(상태 중단, 성공, 실패)에 대한 단일 메시지를 제거하려면 메시지 옆의 **Remove(**제거**)** ( )를 클릭합니다.
- 모든 완료된 작업(상태 중간, 성공, 실패)에 대한 전체 메시지를 제거하려면 **Total(**전체**)**에서 메시지를 필터링하 고 **Remove all completed tasks(**모든 완료된 작업 제거**)**를 클릭합니다.
- 성공적으로 완료된 모든 작업에 대한 전체 메시지를 제거하려면 **Success(**성공**)** 메시지를 필터링하고 **Remove all completed tasks(**모든 성공적인 작업 제거**)**를 클릭합니다.
- 실패한 모든 작업에 대한 전체 메시지를 제거하려면 **Failure(**실패**)** 메시지를 필터링하고 **Remove all failed tasks(**모든 실패한 작업 제거**)**를 클릭합니다.

상태 모니터 알림의 메모리 사용량 임계값

Memory Usage 상태 모듈은 어플라이언스의 메모리 사용량을 모듈에 대해 설정된 제한과 비교하고, 사용량이 레벨을 초과하면 알림을 전송합니다. 모듈은 매니지드 디바이스 및 FMC 자체의 데이터를 모니터링합니다.

메모리 사용에 대해 설정 가능한 두 가지 임계값인 Critical(심각) 및 Warning(경고)을 사용된 메모리의 백분율로 설정할 수 있습니다. 이러한 임계값을 초과하면 심각도 레벨이 지정된 상태 알람이 생성됩니다. 그러나 상태 경보 시스템은 이러한 임계 값을 정확한 방식으로 계산하지 않습니다.

높은 메모리 디바이스를 사용하는 경우 특정 프로세스에서는 낮은 메모리 공간 디바이스에서보다 전체 시스템 메모리의 비율이 더 많이 사용됩니다. 이 설계에서는 보조 프로세스에 사용할 수있는 작은 메모리 값을 남겨 두면서 최대한 많은 물리적 메모리를 사용합니다.

두 개의 디바이스(하나는 32GB 메모리, 다른 하나는 4GB 메모리)를 비교합니다. 32GB의 메모리가 있는 디바이스에서 메모리의 5%(1.6GB)는 4GB의 메모리가 있는 디바이스(4GB의 5% = 200MB)보다 보조 프로세스에서 남겨야 할 메모리 값이 훨씬 더 큽니다.

특정 프로세스에서 시스템 메모리를 더 많이 사용하는 비율을 고려하기 위해 FMC는 총 물리적 메모리와 총 스왑 메모리를 모두 포함하도록 총 메모리를 계산합니다. 따라서 사용자가 설정한 임계값 입력에 대해 시행된 메모리 임계값은 이벤트의 "Value(값)" 열이 초과된 임계값을 결정하기 위해 입력한 값과 일치하지 않는 상태 이벤트를 초래할 수 있습니다.

다음 표에는 설치된 시스템 메모리에 따라 사용자 입력 임계값 및 시행 된 임계값의 예가 나와 있습니다.

참고 이 표의 값은 예시입니다. 이 정보를 사용하여 여기에 표시된 설치된 RAM과 일치하지 않는 디바이스에 대한 임계값을 추정할 수 있습니다. 또는 더 정확한 임계값 계산을 위해 Cisco TAC에 문의할 수 있습니다.

표 ***36:*** 설치된 ***RAM*** 기반 메모리 사용량 임계값

사용자 입력 임계값	설치된 메모리당 시행된 임계값**(RAM)**			
	4GB	**6 GB**	**32GB**	**48GB**
10%	10%	34%	72%	81%
20%	20%	41%	75%	83%
30%	30%	48%	78%	85%
40%	40%	56%	81%	88%
50%	50%	63%	84%	90%
60%	60%	70%	88%	92%
70%	70%	78%	91%	94%
80%	80%	85%	94%	96%
90%	90%	93%	97%	98%
100%	100%	100%	100%	100%

이벤트 상태 모니터 알림의 디스크 사용량 및 소모

디스크 사용량 상태 모듈은 매니지드 디바이스의 하드 드라이브 및 악성코드 스토리지 팩의 디스크 사용량을 모듈에 대해 구성된 제한과 비교하고, 사용량이 모듈에 대해 구성된 비율을 초과하면 알림을 전송합니다. 또한 시스템이 모니터링되는 디스크 사용량 카테고리에서 과도하게 파일을 삭제하는 경우 또는 모듈 임계값을 기반으로 그러한 카테고리 외의 디스크 사용량이 과도한 수준에 도달하는 경우에도 알림을 전송합니다.

이 주제에서는 디스크 사용량 상태 모듈에서 생성되는 두 가지 상태 경고에 대한 증상 및 문제 해결 지침에 대해 설명합니다.

- 이벤트의 빈번한 드레인
- 처리되지 않은 이벤트의 드레인

디스크 관리자 프로세스는 디바이스의 디스크 사용량을 관리합니다. 디스크 관리자가 모니터링하는 각 파일 유형에는 사일로가 할당됩니다. 시스템에서 사용 가능한 디스크 공간의 양에 따라 디스크 관리자는 각 사일로에 대해 HWM(상위 워터마크) 및 LWM(하위 워터마크)을 계산합니다.

시스템의 각 부분(silo, LWM 및 HWM 등)에 대한 자세한 디스크 사용량 정보를 표시하려면 **show disk-manager** 명령을 사용합니다.

예

다음은 디스크 관리자 정보의 예입니다.

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
Updates                             0 KB        5.850 GB    14.625 GB
Other Detection Engine              0 KB        2.925 GB    5.850 GB
Performance Statistics              33 KB       998.395 MB  11.700 GB
Other Events                        0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering       0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs        0 KB        3.900 GB    19.500 GB
Unified Low Priority Events         1.329 MB    4.875 GB    24.375 GB
RNA Events                          0 KB        3.900 GB    15.600 GB
File Capture                        0 KB        9.750 GB    19.500 GB
Unified High Priority Events        0 KB        14.625 GB   34.125 GB
IPS Events                          0 KB        11.700 GB   29.250 GB
```

상태 알림 형식

management center의 상태 모니터 프로세스가 실행되면(5분마다 또는 수동 실행이 트리거될 때) 디스크 사용량 모듈이 diskmanager.log 파일을 살펴보고 올바른 조건이 충족되면 해당 상태 알림이 트리거됩니다.

이러한 상태 알림의 구조는 다음과 같습니다.

- <사일로 이름>의 빈번한 드레인
- <사일로 이름>에서 처리되지 않은 이벤트의 드레인

예를 들면 다음과 같습니다.

- 낮은 우선순위 이벤트의 빈번한 드레인
- 낮은 우선순위 이벤트에서 처리되지 않은 이벤트의 드레인

사일로에서 <사일로 이름>의 빈번한 드레인 상태 알림을 생성할 수 있습니다. 그러나 이벤트와 관련된 알림이 가장 일반적으로 표시됩니다. 이벤트 사일로 중에는 이러한 유형의 이벤트가 디바이스에서 더욱 빈번하게 생성되므로 낮은 우선순위 이벤트가 자주 표시됩니다.

<사일로 이름>의 빈번한 드레인 이벤트는 이벤트가 management center로 전송되도록 대기하기 때문에 이벤트 관련 사일로에 대해서 표시할 때 **Warning(**경고**)** 심각도 레벨을 갖습니다. 백업 사일로와 같이 이벤트와 관련이 없는 사일로의 경우, 이 정보가 손실되므로 경고의 심각도는 **Critical(**중대**)**입니다.

중요 이벤트 사일로만이 <사일로 이름> 에서 처리되지 않은 이벤트의 드레인 상태 알림을 생성합니다. 이 알림의 심각도 레벨은 항상 **Critical(**중대**)**입니다.

알림 외에 추가 증상은 다음과 같습니다.

- management center 사용자 인터페이스의 속도 저하

- 이벤트 손실

일반적인 문제 해결 시나리오

<사일로 이름>의 빈번한 드레인 이벤트가 그 크기로 인해 사일로에 너무 많이 입력되어 발생합니다. 이 경우, 디스크 관리자는 마지막 5분 간격으로 해당 파일을 두 번 이상 비우거나 제거합니다. 이벤트 유형 사일로에서 이는 일반적으로 해당 이벤트 유형의 과도한 로깅으로 인해 발생합니다.

<사일로 이름>의 처리되지 않은 이벤트의 드레인 상태 알림의 경우, 이벤트 처리 경로의 병목 현상으로 인해 발생할 수도 있습니다.

이러한 디스크 사용량 알림과 관련하여 발생 가능한 세 가지 병목 현상이 있습니다.

- 과도한 로깅 - threat defense의 EventHandler 프로세스가 초과 서브스크립션됩니다(Snort가 쓰는 것보다 느리게 읽음).
- Sftunnel 병목 현상 - Eventing 인터페이스가 불안정하거나 초과 서브스크립션됩니다.
- SFDataCorrelator 병목 현상 - management center와 매니지드 디바이스 간의 데이터 전송 채널이 초과 서브스크립션됩니다.

과도한 로깅

이 유형의 상태 알림의 가장 일반적인 원인 중 하나는 과도한 입력입니다. **show disk-manager** 명령에서 수집한 LWM(하위 워터마크)과 HWM(상위 워터마크)의 차이점은 LWM(새로 드레인됨)에서 HWM 값으로 이동하기 위해 해당 사일로에서 사용할 수 있는 공간의 양을 나타냅니다. 처리되지 않은 이벤트의 유무에 관계없이 이벤트가 자주 비워지는 경우, 로깅 설정을 가장 먼저 검토해야 합니다.

- 이중 로깅 확인 - management center에서 상관기 *perfstats*를 보면 이중 로깅 시나리오를 확인할 수 있습니다.

  ```
  admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
  ```

- ACP에 대한 로깅 설정 확인 - ACP(Access Control Policy, 액세스 제어 정책)의 로깅 설정을 검토합니다. 연결의 "시작" 및 "종료"를 모두 로깅하는 경우, 시작을 기록할 때 포함된 모든 항목을 포함하고 이벤트의 양을 줄이므로 종료만 기록합니다.

  연결 로깅 모범 사례, 762 페이지에 설명된 모범 사례를 따라야 합니다.

통신 병목 현상 - **Sftunnel**

sftunnel은 management center와 매니지드 디바이스 간의 암호화된 통신을 담당합니다. 이벤트는 터널을 통해 management center로 전송됩니다. 매니지드 디바이스와 management center 간의 통신 채널(sftunnel)에서 연결 문제 및/또는 불안정은 다음과 같은 원인으로 발생할 수 있습니다.

- sftunnel이 다운되었거나 불안정합니다(플랩).

  management center와 매니지드 디바이스가 TCP 포트 8305의 관리 인터페이스 간에 연결 가능한지 확인합니다.

  sftunnel 프로세스는 안정적이어야 하며 예기치 않게 재시작되지 않아야 합니다. **/var/log/message** 파일을 점검하여 이를 확인하고 ***sftunneld*** 문자열이 포함된 메시지를 검색합니다.

- sftunnel이 초과 서브스크립션되었습니다.

  상태 모니터에서 추세 데이터를 검토하고 관리 트래픽이 급증하거나 지속적인 초과 서브스크립션이 될 수 있는 management center 관리 인터페이스의 초과 서브스크립션 징후를 확인합니다.

  Firepower 이벤트를 위한 보조 관리 인터페이스로 사용합니다. 이 인터페이스를 사용하려면 **configure network management-interface** 명령을 사용하여 threat defense CLI에서 해당 IP 주소 및 기타 매개변수를 구성해야 합니다.

통신 병목 현상 - SFDataCorrelator

SFDataCorrelator는 management center와 매니지드 디바이스 간의 데이터 전송을 관리합니다. management center는 시스템에서 생성된 이진 파일을 분석하여 이벤트, 연결 데이터 및 네트워크 맵을 생성합니다. 첫 번째 단계는 **diskmanager.log** 파일에서 다음과 같이 수집할 중요한 정보를 검토하는 것입니다.

- 드레인의 빈도
- 처리되지 않은 이벤트가 드레인된 파일의 수
- 처리되지 않은 이벤트가 있는 드레인의 발생

디스크 관리자 프로세스가 실행될 때마다 **[/ngfw]/var/log/diskmanager.log**에 있는 자체 로그 파일에서 각기 다른 사일로에 대한 항목을 생성합니다. diskmanager.log에서 수집한 정보(CSV 형식)를 사용하면 원인을 찾는 범위를 좁힐 수 있습니다.

추가 문제 해결 단계:

- **stats_unified.pl** 명령을 사용하면 매니지드 디바이스에 management center로 전송해야 하는 데이터가 있는지 확인할 수 있습니다. 이 상태는 매니지드 디바이스와 management center에 연결 문제가 있을 때 발생할 수 있습니다. 매니지드 디바이스는 로그 데이터를 하드 드라이브에 저장합니다.

  ```
  admin@FMC:~$ sudo stats_unified.pl
  ```

- **manage_proc.pl** 명령은 management center 측의 상관기를 재설정할 수 있습니다.

  ```
  root@FMC:~# manage_procs.pl
  ```

Cisco TAC(Technical Assistance Center)에 연락하기 전에

Cisco TAC에 연락하기 전에 다음 항목을 수집하는 것이 좋습니다.

- 표시되는 상태 알림의 스크린샷
- management center에서 생성된 문제 해결 파일
- 영향을 받는 매니지드 디바이스에서 생성된 문제 해결 파일

  문제가 처음 확인된 날짜 및 시간

- 정책에 적용된 최근 변경 사항에 대한 정보(해당되는 경우)

  통신 병목 현상 - SFDataCorrelator, 449 페이지에 설명된 stats_unified.pl 명령의 출력

문제 해결을 위한 상태 모니터 보고서

경우에 따라 어플라이언스에 문제가 발생하면 support(지원팀)가 문제 진단에 도움이 될 수 있도록 문제 해결 파일을 제공하도록 요청할 수 있습니다. 시스템은 특정 기능 영역을 대상으로 하는 정보 뿐만 아니라 사용자가 지원팀과 협력하여 검색하는 고급 문제 해결 파일을 사용하여 문제 해결 파일을 생성할 수 있습니다. 아래 표에 나열된 옵션 중 하나를 선택하여 특정 기능에 대한 문제 해결 파일의 내용을 맞춤화할 수 있습니다.

일부 옵션은 보고하는 데이터의 측면에서 겹치지만, 문제 해결 파일은 선택하는 옵션에 관계없이 중복된 사본을 포함하지 않는다는 점에 유의하십시오.

표 ***37:*** 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

특정 시스템 기능에 대한 문제 해결 파일 생성

지원 시 전송할 수 있는 맞춤 문제 해결 파일을 생성 및 다운로드할 수 있습니다.

다중 도메인을 구축한 경우, 하위 도메인의 디바이스에서 문제 해결 파일을 생성하고 다운로드할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 유지 보수, 보안 분석가 또는 보안 분석가(읽기 전용) 사용자여야 합니다.

프로시저

단계 **1** 디바이스 상태 모니터 보기, 399 페이지의 단계를 수행합니다.

단계 **2** 시스템 (⚙) > **Health(상태)** > **Monitor(모니터링)**를 선택하고 왼쪽 패널에서 디바이스를 클릭한 다음 **View System & Troubleshoot Details(**시스템 및 문제 해결 세부 정보 보기**)**를 클릭하고 **Generate Troubleshooting Files(**문제 해결 파일 생성**)**를 클릭합니다.

참고

- Management Center 웹 인터페이스에서 management center 문제 해결 파일을 생성하면 파일은 management center에 저장됩니다. 최신 문제 해결 파일만 management center에 저장됩니다.
- Management Center 웹 인터페이스에서 threat defense 문제 해결 파일을 생성하면 파일은 threat defense에 생성되고 management center에 복사됩니다. 최신 threat defense 문제 해결 파일만 management center에 저장됩니다.
- management center 및 threat defense에 대한 문제 해결 파일이 CLI에서 생성된 경우, 문제 해결 파일의 모든 버전은 각각 management center 및 threat defense에서 유지됩니다.

단계 **3** 모든 생성 가능한 문제 해결 날짜의 파일을 생성하려면 모든 데이터를 선택하거나 작업 메시지 보기, 444 페이지의 설명에 따라 개별 상자를 체크합니다.

단계 **4** **Generate(**생성**)**를 클릭합니다.

단계 **5** Message Center에서 작업 메시지를 확인하려면 작업 메시지 보기, 444 페이지를 참고하십시오.

단계 **6** 사용자가 생성한 문제 해결 파일에 해당하는 작업을 찾습니다.

단계 **7** 어플라이언스가 문제 해결 파일을 생성하고 작업 상태가 `Completed(완료)`로 변경된 후 **Click to retrieve generated files(**생성된 파일을 검색하려면 클릭**)**를 클릭합니다.

단계 **8** 파일을 다운로드하려면 브라우저의 프롬프트를 따릅니다. (문제 해결 파일은 단일 `.tar.gz` 파일에 다운로드 됩니다.)

단계 **9** Cisco에 문제 해결 파일을 보내려면 Support(지원팀)의 지시에 따르십시오.

고급 문제 해결 파일 다운로드

다중 도메인을 구축한 경우, 하위 도메인의 디바이스에서 문제 해결 파일을 생성하고 다운로드할 수 있습니다. 파일의 다운로드는 글로벌 도메인의 management center에서만 할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 유지 보수, 보안 분석가 또는 보안 분석가(읽기 전용) 사용자여야 합니다.

프로시저

단계 **1** 어플라이언스의 상태 모니터를 확인합니다. 디바이스 상태 모니터 보기, 399 페이지의 내용을 참조하십시오.

단계 **2** 시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터링**)**를 선택하고 왼쪽 패널에서 디바이스를 클릭한 다음, **View System & Troubleshoot Details(**시스템 및 문제 해결 세부 정보 보기**)**를 클릭하고 **Advanced Troubleshooting(**고급 문제 해결**)**을 클릭합니다.

단계 **3** **File Download(**파일 다운로드**)**에서 지원팀이 제공한 파일 이름을 입력합니다.

단계 **4** **Download(**다운로드**)**를 클릭합니다.

단계 **5** 파일을 다운로드하려면 브라우저의 프롬프트를 따릅니다.

참고 매니지드 디바이스의 경우, 시스템 이름 앞에 장치 이름을 추가하여 파일의 이름을 바꿉니다.

단계 **6** Cisco에 문제 해결 파일을 보내려면 Support(지원팀)의 지시에 따르십시오.

일반 문제 해결

내부 전원 장애(하드웨어 장애, 전원 서지) 또는 외부 전원 장애(플러그 뽑힘)로 인해 예기치 않은 시스템 셧다운 또는 재부팅이 발생할 수 있습니다. 이러한 경우 결국 데이터 손상이 발생할 수 있습니다.

연결 기반 문제 해결

연결 기반 문제 해결 또는 디버깅은 특정 연결에 대한 적절한 로그를 수집하기 위해 모듈에 균일한 디버깅을 제공합니다. 또한 최대 레벨 7까지 레벨 기반 디버깅을 지원하고 액세스 모듈에 대한 균일한 로그 수집 메커니즘을 활성화합니다. 연결 기반 디버깅은 다음을 지원합니다.

- Firepower Threat Defense에서 문제를 해결하는 공통 연결 기반 디버깅 하위 시스템
- 모듈에서 일관된 디버그 메시지 형식
- 재부팅에서 지속적인 디버그 메시지
- 모듈에서 기존 연결 기반 엔드 투 엔드 디버깅
- 진행 중인 연결 디버깅

참고 연결 기반 디버깅은 Firepower 2100 시리즈 디바이스에서는 지원되지 않습니다.

문제 해결 연결에 대한 자세한 내용은 연결 문제 해결 , 453 페이지를 참조하십시오.

연결 문제 해결

프로시저

단계 **1** **debug packet-condition** 명령을 사용하여 연결을 식별하는 필터를 구성합니다.

예:

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

단계 **2** 관심 있는 모듈 및 해당 레벨에 대한 디버그를 활성화합니다. **debug packet** 명령을 사용합니다.

예:

```
Debug packet acl 5
```

단계 **3** 다음 명령을 사용하여 패킷 디버깅을 시작합니다.

```
debug packet-start
```

단계 **4** 다음 명령을 사용하여 데이터베이스에서 디버그 메시지를 가져오고 디버그 메시지를 분석합니다.

```
show packet-debugs
```

단계 **5** 다음 명령을 사용하여 패킷 디버깅을 중지합니다.

```
debug packet-stop
```

Secure Firewall Threat Defense 디바이스의 고급 문제 해결

Secure Firewall Threat Defense 디바이스의 자세한 문제 해결 분석을 수행하기 위해 패킷 트레이서 및 패킷 캡처 기능을 사용할 수 있습니다. 패킷 트레이서는 방화벽 관리자가 가상 패킷을 보안 어플라이언스에 삽입하고 인그레스에서 이그레스로의 흐름을 추적하도록 합니다. 그 과정에서 패킷은 흐름 및 경로 조회, ACL, 프로토콜 검사, NAT, 침입 탐지에 대해 평가됩니다. 유틸리티 전원은 프로토콜 및 포트 정보로 소스 및 대상 주소를 지정하여 실제 트래픽을 시뮬레이션하는 기능에서 가져옵니다. 패킷 캡처는 패킷의 성공 실패 판정을 제공하는 추적 옵션을 통해 사용 가능합니다.

문제 해결 파일에 대한 자세한 내용은 고급 문제 해결 파일 다운로드, 451 페이지의 내용을 참조하십시오.

웹 인터페이스에서 Threat Defense 진단 CLI 사용

management center에서 선택한 threat defense 진단 명령줄 인터페이스(진단 CLI) 명령을 실행할 수 있습니다. 이러한 명령은 일반 CLI가 아닌 진단 CLI에서 실행됩니다. 이러한 명령은 **ping**(**ping system** 제외), **traceroute**이며, **show** 명령을 선택합니다.

show 명령의 경우 “Unable to execute the command properly. Please See logs for more details.(명령을 제대로 실행할 수 없습니다. 자세한 내용은 로그를 참고하십시오.)" 메시지가 나타나며 명령이 진단 CLI에서 유효하지 않음을 의미합니다. 예를 들어, **show access-list**은 작동하지만 **show access-control-policy**을 입력하면 이 메시지가 표시됩니다. 비진단 CLI 명령을 사용해야 하는 경우 Management Center 외부의 디바이스에 SSH로 연결해야 합니다.

threat defense CLI에 대한 자세한 내용은 Cisco Secure Firewall Threat Defense 명령 참조의 내용을 참조하십시오.

시작하기 전에

- 진단 CLI를 사용하려면 관리자, 유지 보수 또는 보안 분석가 사용자여야 합니다.
- 이 기능의 목적은 디바이스의 문제를 해결할 때 유용할 수 있는 몇 가지 명령을 빠르게 사용할 수 있도록 하는 것입니다. 전체 명령 범위에 대한 액세스를 포함하여 중요한 CLI 작업을 수행하려면 디바이스에서 직접 SSH 세션을 여십시오.
- 다중 도메인 구축 시 하위 도메인에서 관리되는 디바이스를 위한 threat defense CLI 명령을 입력할 수 있습니다.
- management center의 고가용성을 활용한 배포의 경우 이 기능은 활성화된 management center에서만 사용할 수 있습니다.

프로시저

단계 **1** 디바이스 > **Threat Defense CLI**을(를) 선택합니다.

디바이스(시스템 (⚙) > **Health(**상태**)** > **Monitor(**모니터**)**)의 상태 모니터를 통해 CLI 도구에 액세스할 수도 있습니다. 여기에서 디바이스를 선택하고 **View System and Troubleshoot Details(**시스템 및 문제 해결 세부 사항 보기**)** 링크를 클릭한 다음 **Advanced Troubleshooting(**고급 문제 해결**)**을 클릭한 후 해당 페이지에서 **Threat Defense CLI**를 클릭할 수 있습니다.

단계 **2** **Device(**디바이스**)** 목록에서 진단 명령을 실행할 디바이스를 선택합니다.

단계 **3** **Command(**명령**)** 목록에서 실행할 명령을 선택합니다.

단계 **4** **Parameters(**매개변수**)** 텍스트 상자에 명령 매개변수를 입력합니다.

유효한 매개변수는 명령 참조를 참고하십시오.

예를 들어, **show access-list**을 실행하려면 **Command(**명령**)** 목록에서 **show**를 선택한 다음, **Parameters(**매개변수**)** 상자에 **access-list**를 입력해야 합니다.

Parameters(매개변수**)** 상자에 전체 명령을 입력하지 마십시오.

단계 **5** 명령 출력을 보려면 **Execute(**실행**)**를 클릭합니다.

“Unable to execute the command properly. Please see logs for more details.(명령을 올바르게 실행할 수 없습니다. 자세한 내용은 로그를 참고하십시오.)” 메시지가 표시되면 매개변수를 면밀하게 검사합니다. syntax(명령문) 오류가 있을 수 있습니다.

이 메시지는 실행하려는 명령이 진단 CLI 컨텍스트 내에서 유효한 명령(**system support diagnostic-cli** 명령을 사용하여 디바이스에서 입력)이 아님을 의미할 수도 있습니다. SSH를 사용하여 디바이스에 로그인하여 이러한 명령을 사용합니다.

패킷 트레이서 개요

패킷 트레이서를 사용하면 소스 및 대상 주소, 프로토콜 특성에 따라 패킷을 모델링하여 정책 구성을 테스트할 수 있습니다. 추적 시 액세스 규칙, NAT, 라우팅, 속도 제한 정책을 테스트하고 패킷이 허용 또는 거부되는지 여부를 확인하기 위해 정책 조회를 수행합니다. 인터페이스, 소스 주소, 대상 주소, 포트 및 프로토콜에 따라 패킷 흐름을 시뮬레이션합니다. 이 방식으로 패킷을 테스트하면 정책의 결과를 확인하고 허용 또는 거부할 트래픽 유형이 사용자가 원하는 대로 처리되는지 여부를 테스트할 수 있습니다. 구성 확인 이외에도 추적기를 사용하여 패킷이 허용되어야 할 때 거부되고 있는지와 같이 예상하지 못한 동작을 디버깅할 수 있습니다. 패킷을 완전히 시뮬레이션하기 위해 패킷 트레이서는 느린 경로 및 빠른 경로 모듈의 데이터 패스를 추적합니다. 프로세스는 세션별 및 패킷별로 처리됩니다. 추적이 있는 추적 패킷 및 캡처는 차세대 방화벽(NGFW)이 패킷으로 세션당 패킷을 처리하는 경우 패킷별로 추적 데이터를 기록합니다.

이제 완전한 플로우가 있는 PCAP 파일을 사용하여 패킷 트레이서를 시작할 수 있습니다. 현재는 최대 100개의 패킷만 포함하는 단일 TCP/UDP 기반 플로우를 사용하는 PCAP가 지원됩니다. IPsec, VPN, SSL 또는 HTTP 암호 해독, NAT 등 재생 중에 패킷을 동적으로 수정하는 기능에 대해서는 PCAP 재생이 지원되지 않습니다.

패킷 트레이서 툴은 PCAP 파일을 읽고 클라이언트 및 서버 재생 엔터티의 상태를 초기화합니다. 이 툴은 후속 처리 및 표시를 위해 PCAP 내에서 각 패킷의 추적 출력을 수집하고 저장하여 동기화된 방식으로 패킷 재생을 시작합니다.

패킷 재생은 PCAP 파일에 있는 패킷의 시퀀스에 의해 실행되며 재생 활동에 대한 간섭으로 인해 패킷이 종료되고 재생이 종료됩니다.

지정된 인그레스 인터페이스 및 이그레스 인터페이스에서 PCAP의 모든 패킷에 대해 추적 출력이 생성되므로 플로우 평가의 전체 컨텍스트가 제공됩니다.

패킷 트레이서 사용

Secure Firewall Threat Defense 디바이스에서 패킷 트레이서를 사용할 수 있습니다. 이 도구를 사용하려면 관리자 또는 유지 보수 사용자여야 합니다.

프로시저

단계 **1** management center에서 **Devices(**디바이스**)** > **Packet Tracer(**패킷 트레이서**)**를 선택합니다.

단계 **2** **Select Device(**디바이스 선택**)** 드롭다운에서 추적을 실행할 디바이스를 선택합니다.

단계 **3** **Ingress Interface(**인그레스 인터페이스**)** 드롭다운에서 패킷 추적을 위한 인그레스 인터페이스를 선택합니다.

참고 VTI를 선택하지 마십시오. 인그레스 인터페이스로서의 VTI는 패킷 트레이서에 대해 지원되지 않습니다.

단계 **4** 패킷 트레이서에서 PCAP 재생을 사용하려면 다음을 수행합니다.

a) **Select a PCAP File(PCAP** 파일 선택**)**을 클릭합니다.

b) 새 PCAP 파일을 업로드하려면 **Upload a PCAP(PCAP** 파일 업로드**)**를 클릭합니다. 최근에 업로드한 파일을 재사용하려면 목록에서 파일을 클릭합니다.

참고 .pcap 및 .pcapng 파일 형식만 지원됩니다. PCAP 파일은 최대 100개의 패킷을 가진 단일 TCP/UDP 기반 플로우만 포함할 수 있습니다. PCAP 파일 이름(파일 형식 포함)의 최대 문자 수는 64자입니다.

c) **Upload PCAP(PCAP** 업로드**)** 상자에서 PCAP 파일을 끌어오거나 상자를 클릭하여 파일을 찾아 업로드할 수 있습니다. 파일을 선택하면 업로드 프로세스가 자동으로 시작됩니다.

d) 이 단계 13로 이동합니다.

단계 **5** 추적 매개변수를 정의하려면 **Protocol(**프로토콜**)** 드롭다운 메뉴에서 추적에 대한 패킷 유형을 선택하고 프로토콜 특성을 지정합니다.

- **ICMP** — ICMP 유형, ICMP 코드(0-255) 및 선택 사항인 ICMP ID를 입력합니다.
- **TCP/UDP/SCTP**— 소스 및 대상 포트 번호를 입력합니다.
- **GRE/IPIP**—0-255 사이의 프로토콜 번호를 입력합니다.
- **ESP** — Source(소스)에 SPI 값을 입력합니다(0~4294967295).
- **RAWIP**—0-255 사이의 포트 번호를 입력합니다.

단계 **6** 패킷 추적에 대한 **Source Type(**소스 유형**)**을 선택하고 소스 IP 주소를 입력합니다.

소스 및 대상 유형은 IPv4, IPv6 및 정규화된 도메인 이름(FQDN)을 포함합니다. Cisco TrustSec을 사용하는 경우 IPv4 또는 IPv6 주소와 FQDN을 지정할 수 있습니다.

단계 **7** 패킷 추적의 소스 포트를 선택합니다.

단계 **8** 패킷 추적에 대한 대상 유형을 선택하고 대상 IP 주소를 입력합니다.

대상 유형 옵션은 선택하는 소스 유형에 따라 달라집니다.

단계 **9** 패킷 추적의 대상 포트를 선택합니다.

단계 **10** 선택 사항으로 레이어 2 CMD 헤더(TrustSec)에 보안 그룹 태그(SGT) 값이 내장되어 있는 패킷을 추적하려는 경우, 유효한 **SGT** 번호를 입력합니다.

단계 **11** 이후 하위 인터페이스로 리디렉션되는 상위 인터페이스에 패킷 트레이서를 입력하려면 **VLAN ID**를 입력합니다.

모든 인터페이스 유형은 하위 인터페이스에 구성할 수 있으므로 이 값은 비 하위 인터페이스에만 선택적으로 사용됩니다.

단계 **12** 패킷 추적용 대상 **MAC** 주소를 지정합니다.

Secure Firewall Threat Defense 디바이스가 투명 방화벽 모드에서 실행되고 인그레스 인터페이스가 VTEP인 경우, **VLAN ID**에 값을 입력하려는 경우 대상 **MAC** 주소가 필요합니다. 반면 인터페이스가 브리지 그룹 구성원인 경우 **VLAN ID** 값을 입력하는 경우 대상 **MAC** 주소는 선택 사항이지만 **VLAN ID** 값을 입력하지 않는 경우에는 필수입니다.

Secure Firewall Threat Defense가 라우팅된 방화벽 모드에서 실행 중인 경우, 입력 인터페이스가 브리지 그룹 구성원인 경우 **VLAN ID** 및 대상 **MAC** 주소는 선택 사항입니다.

단계 **13** (선택 사항) 패킷 트레이서가 시뮬레이션된 패킷에 대한 보안 검사를 무시하도록 하려면 **Bypass all security checks for satellited packet(**시뮬레이션된 패킷에 대한 모든 보안 검사 우회**)**을 클릭합니다. 이렇게 하면 패킷 트레이서가 시스템 전체에서 패킷 추적을 계속할 수 있습니다. 그렇지 않으면 삭제될 수 있습니다.

단계 **14** (선택사항) 패킷이 디바이스에서 이그레스 인터페이스를 통해 전송되도록 허용하려면 **Allow Simulated packet to transmission from device(**디바이스에서 시뮬레이션된 패킷 전송 허용**)**를 클릭합니다.

단계 **15** (선택 사항) 패킷 트레이서가 주입된 패킷을 IPsec/SSL VPN 암호 해독된 패킷으로 간주하게 하려면 **Treat Simulated packet as IPsec/SSL VPN decrypt(IPsec/SSL VPN** 암호 해독으로 처리**)**를 클릭합니다.

단계 **16** **Trace(**추적**)**를 클릭합니다.

Trace Result(추적 결과**)**에는 PCAP 패킷이 시스템을 통해 이동한 각 단계에 대한 결과가 표시됩니다. 패킷에 대한 추적 결과를 보려면 개별 패킷을 클릭합니다. 다음을 수행할 수 있습니다.

- 추적 결과를 클립보드에 복사( )합니다.
- 표시된 결과를 확장하거나 축소( )합니다.
- 추적 결과 화면을 최대화( )합니다.

처리 노력을 측정하는 데 유용한 경과 시간 정보가 각 단계에 대해 표시됩니다. 인그레스에서 이그레스 인터페이스로 흐르는 전체 패킷 플로우에 소요된 총 시간도 결과 섹션에 표시됩니다.

Trace History(추적 기록**)** 창에는 각 PCAP 추적에 대해 저장된 추적 세부 정보가 표시됩니다. 최대 100개의 패킷 추적을 저장할 수 있습니다. 저장된 추적을 선택하고 패킷 추적 활동을 다시 실행할 수 있습니다. 다음을 수행할 수 있습니다.

- 추적 매개변수 중 하나를 사용하여 추적을 검색합니다.
- 버튼을 사용하여 기록에 대한 추적 저장을 비활성화합니다.
- 특정 추적 결과를 삭제합니다.
- 모든 추적을 지웁니다.

패킷 캡처 개요

추적 옵션이 있는 패킷 캡처 기능은 인그레스 인터페이스에 캡처된 실제 패킷을 시스템에서 추적할 수 있도록 허용합니다. 추적 정보는 다음 단계에 표시됩니다. 이러한 패킷은 실제 데이터 경로 트래

픽이기 때문에 이그레스 인터페이스에서 삭제되지 않습니다. Firepower Threat Defense 디바이스를 위한 패킷 캡처는 데이터 패킷 문제 해결 및 분석을 지원합니다.

패킷을 취득하면 Snort가 패킷에서 활성화된 추적 플래그를 탐지합니다. Snort는 패킷이 통과하는 추적 요소를 기록합니다. 패킷 캡처의 결과인 Snort 판정은 다음 중 하나가 될 수 있습니다.

표 ***38: Snort*** 판정

판정	설명
통과	분석된 패킷을 허용합니다.
차단	패킷이 전달되지 않음
교체	패킷이 수정됨
AllowFlow	플로우가 검사 없이 통과됨
BlockFlow	플로우가 차단됨
무시	플로우가 차단되었습니다. 이는 패시브 인터페이스에서 플로우가 차단된 세션에 대해서만 발생합니다.
재시도	에나멜웨어 또는 URL 카테고리 / 평판 쿼리를 기다리는 중 플로우가 중단되었습니다. 시간 초과 시 알 수 없는 결과로 처리가 계속됩니다. 에나멜웨어의 경우 파일이 허용됩니다. URL 범주 / 평판의 경우 AC 규칙 조회는 분류되지 않은 알 수 없는 평판으로 계속 진행됩니다.

Snort 판정에 따라 패킷이 삭제되거나 허용됩니다. 예를 들어 Snort 판정이 **BlockFlow(**차단플로우**)**인 경우 패킷이 삭제되고 세션의 후속 패킷은 Snort에 도달하기 전에 삭제됩니다. Snort 판정이 **Block(**차단**)** 또는 **BlockFlow(**차단플로우**)**인 경우 삭제 이유는 다음 중 하나일 수 있습니다.

표 ***39:*** 삭제 이유

차단 또는 플로우 차단 원인	원인
Snort	Snort가 패킷을 처리할 수 없습니다. snort가 손상되었거나 형식이 잘못되었으므로 패킷을 디코딩할 수 없습니다.
전처리된 앱 ID	앱 ID 모듈/전처리는 패킷 자체를 차단하지 않습니다. 그러나 이는 앱 ID 탐지로 인해 다른 모듈(에르그, 방화벽)이 차단 규칙과 일치함을 나타낼 수 있습니다.
전처리된 SSL	SSL 정책에는 트래픽과 일치하는 차단/재설정 규칙이 있습니다.

차단 또는 플로우 차단 원인	원인
방화벽	방화벽 정책에 트래픽과 일치하는 차단/재설정 규칙이 있습니다.
전처리된 종속 포털	트래픽을 일치시키기 위해 ID 정책을 사용하는 차단/재설정 규칙이 있습니다.
전처리된 안전 검색	방화벽 정책의 안전 검색 기능을 사용하여 트래픽과 일치하는 차단/재설정 규칙이 있습니다.
전처리된 SI	AC 정책의 Security Intelligence(보안 인텔리전스) 탭에 차단/재설정 규칙이 있어 트래픽, 에르그, DNS 또는 URL SI 규칙을 차단합니다.
전처리된 필터	트래픽과 일치시키기 위한 AC 정책의 필터 탭에 차단/재설정 규칙이 있습니다.
전처리된 스트림	TCP 정규화 오류가 발생하면 침입 규칙 차단/재설정 스트림 연결, 에르그, 차단이 있습니다.
전처리된 세션	이 세션은 다른 모듈에 의해 이미 차단되었으므로 전처리된 세션이 동일한 세션의 추가 패킷을 차단하고 있습니다.
전처리된 단편화	이전 데이터 조각이 차단되었으므로 차단 중입니다.
전처리된 Snort 응답	특정 HTTP 트래픽에 대한 응답 페이지를 전송하는 snort 반응 규칙이 있습니다.
전처리된 Snort 응답	패킷 일치 조건에 대한 맞춤형 응답을 전송하는 Snort 규칙이 있습니다.
전처리된 평판	패킷이 평균 규칙, 예를 들면 주어진 IP 주소를 차단하는 규칙과 일치합니다.
전처리된 x-Link2State	SMTP에서 버퍼 오버플로우 취약점이 탐지되어 차단되었습니다.
back orifice 전처리됨	Back orifice 데이터 탐지로 인한 차단
전처리된 SMB	SMB 트래픽을 차단하는 Snort 규칙이 있습니다.
전처리된 파일 프로세스	파일을 차단하는 파일 정책, 예를 들면 악성 코드 차단 정책이 있습니다.
전처리된 IPS	IPS를 사용하는 snort 규칙, 예를 들면 속도 필터링 규칙이 있습니다.

패킷 캡처 기능을 사용하면 시스템 메모리에 저장되어 있는 패킷을 캡처하고 다운로드할 수 있습니다. 그러나 메모리 제약 때문에 버퍼 크기는 32MB로 제한됩니다. 많은 양의 패킷 캡처를 처리할 수 있는 시스템은 최대 버퍼 크기를 빠르게 초과하기 때문에 패킷 캡처 제한이 필요합니다. 이때 보조 메모리에서 (캡처 데이터를 쓰기 위해 파일을 생성하여) 수행합니다. 지원되는 최대 파일 크기는 10GB입니다.

파일 크기를 구성하는 경우 캡처된 데이터가 파일에 저장되고 파일 이름은 캡처명 **recapture**를 기준으로 할당됩니다.

파일 크기 옵션은 캡처하는 패킷 크기가 32MB를 초과하는 경우에 필요합니다.

자세한 내용은 *Command Reference for Firepower Threat Defense*를 참조하십시오.

캡처 추적 사용

패킷 캡처는 정의된 기준에 따라 디바이스의 지정된 인터페이스를 전달하는 네트워크 트래픽의 라이브 스냅샷을 제공하는 유틸리티입니다. 이 프로세스는 일시 중지되지 않았거나 할당된 메모리가 소진되지 않은 한 계속해서 패킷을 캡처합니다.

패킷 캡처 데이터에는 패킷을 처리하는 동안 시스템의 판정과 작업에 대한 Snort와 프리프로세서의 정보가 포함됩니다. 한 번에 여러 패킷의 캡처도 가능합니다. 캡처를 수정, 삭제, 제거, 저장하도록 시스템을 구성할 수 있습니다.

참고 패킷 데이터 캡처에는 패킷 복사가 필요합니다. 이 작업을 위해 패킷을 처리하는 동안 지연이 발생할 수 있으며 패킷 처리량을 저하시킬 수 있습니다. 특정 트래픽 데이터를 캡처할 때는 패킷 필터를 사용하는 것이 좋습니다.

시작하기 전에

Secure Firewall Threat Defense 디바이스에서 패킷 캡처 툴을 사용하려면 관리자 또는 유지 보수 사용자여야 합니다.

프로시저

단계 **1** management center에서 **Devices(**디바이스**)** > **Packet Capture(**패킷 캡처**)**를 선택합니다.

단계 **2** 디바이스 선택

단계 **3** **Add Capture(**캡처 추가**)**를 클릭합니다.

단계 **4** 추적 캡처의 이름을 입력합니다.

단계 **5** 추적 캡처의 인터페이스를 선택합니다.

단계 **6** 일치 기준에 대한 세부 정보를 지정합니다.

a) **Protocol(**프로토콜**)**을 선택합니다.
b) 소스 호스트에 대한 IP 주소를 입력합니다.
c) 대상 호스트에 대한 IP 주소를 입력합니다.
d) (선택 사항) **SGT** 번호 체크 박스를 선택하고 보안 그룹 태그(SGT)를 입력합니다.

단계 **7** 버퍼 세부 정보를 지정합니다.

a) (선택 사항) 최대 패킷 크기를 입력합니다.
b) (선택 사항) 최소 버퍼 크기를 입력합니다.
c) 중단 없이 트래픽을 캡처하기 위해 지속 캡처를 선택하거나 최대 버퍼 크기에 도달했을 때 캡처를 중지하기 위해 가득 차면 중지를 선택하십시오.

참고 **Continues Capture(**캡처 계속**)**가 활성화되어 있고 할당된 메모리가 꽉 차면 새 캡처된 패킷이 메모리에서 가장 오래된 캡처된 패킷을 덮어씁니다.

d) 각 패킷에 대한 세부 정보를 캡처하려면 **Trace(**추적**)** 체크 박스를 선택합니다.
e) **Trace Count(**추적 카운트**)** 필드에 값을 입력합니다. 기본값은 128입니다. 1-1000 범위의 값을 입력할 수 있습니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

패킷 캡처 화면에는 패킷 캡처 세부 정보 및 해당 상태가 표시됩니다. 패킷 캡처 페이지를 자동으로 새로 고치려면 **Enable Auto Refresh(**자동 새로 고침 활성화**)** 확인란을 선택하고 자동 새로 고침 간격을 초 단위로 입력합니다.

패킷 캡처에서 다음을 수행할 수 있습니다.

- **Edit(**수정**)** ( )를 사용하여 캡처 기준을 수정합니다.
- **Delete(**삭제**)** ( )를 사용하여 패킷 캡처 및 캡처된 패킷을 삭제합니다.
- **Clear(**지우기**)** ( )를 사용하여 패킷 캡처에서 모든 캡처된 패킷을 지웁니다. 모든 기존 패킷 캡처에서 캡처된 패킷을 지우려면 **Clear All Packets(**모든 패킷 지우기**)**를 클릭합니다.
- **Pause(**일시 중지**)** ( )를 사용하여 패킷 캡처를 일시적으로 중지합니다.
- **Save(**저장**)** ( )를 사용하여 캡처된 패킷의 복사본을 로컬 시스템에 ASCII 또는 PCAP 형식으로 저장합니다. 필수 형식 옵션을 선택하고 **Save(**저장**)**를 클릭합니다. 저장된 패킷 캡처가 로컬 시스템에 다운로드됩니다.
- 캡처 중인 패킷의 세부 정보를 보려면 필요한 캡처 행을 클릭합니다.

기능별 문제 해결

기능 관련 문제 해결 팁과 기술은 다음 표를 참조하십시오.

표 ***40:*** 기능 관련 문제 해결 주제

기능	관련 문제 해결 정보
애플리케이션 제어	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 애플리케이션 제어 모범 사례

기능	관련 문제 해결 정보
LDAP 외부 인증	LDAP 인증 연결 문제 해결, 206 페이지
라이선싱	스마트 라이선싱 트러블슈팅, 294 페이지 특정 라이선스 예약 문제 해결, 307 페이지
Management Center 고가용성	Management Center 고가용성 문제 해결, 316 페이지
사용자 규칙 조건	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사용자 제어 문제 해결
사용자 ID 소스	ISE/ISE-PIC, TS 에이전트 ID 소스, 캡티브 포털 ID 소스 및 원격 액세스 VPN ID 소스에 대한 문제 해결 정보는 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 해당 섹션을 참조하십시오. LDAP 인증 연결 문제 해결, 206 페이지
URL 필터링	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *URL* 필터링 문제 해결
영역 및 사용자 데이터 다운로드	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 영역 및 사용자 다운로드 문제 해결
네트워크 검색	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 검색 전략 문제 해결
맞춤 설정 보안 그룹 태그(SGT) 규칙 조건	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 맞춤형 *SGT* 규칙 조건
SSL 규칙	Cisco Secure Firewall Device Manager 구성 가이드의 SSL 규칙에 대한 장
Cisco Threat Intelligence Director(TID)	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Secure Firewall Threat Intelligence Director* 문제 해결
Secure Firewall Threat Defense syslog	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 시스템 로그 구성 관련 정보
침입 성능 통계	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 침입 성능 통계 로깅 구성
연결 기반 문제 해결	연결 기반 문제 해결, 452 페이지

IV 부

툴

15 장

백업/복구

백업 및 복원 정보

재해부터 복구할 수 있는 능력은 모든 시스템 유지 보수 계획에서 필수적인 부분입니다. 재해 복구 계획의 일환으로, 정기적인 백업을 수행하여 원격 위치를 보호하는 것이 좋습니다.

온디맨드 백업

management center 및 여러 threat defense 디바이스에 대해 management center에서 온 디맨드 백업을 수행할 수 있습니다.

자세한 내용은 Management Center 또는 매니지드 디바이스 백업, 474 페이지를 참고하십시오.

예약 백업

management center에서 스케줄러를 사용하여 백업을 자동화할 수 있습니다. management center에서의 원격 디바이스 백업은 예약할 수 없습니다.

management center 설정 프로세스는 매주 설정 전용 백업을 예약하여 로컬에 저장합니다. 이는 전체 오프 사이트 백업을 대체하지 않습니다. 초기 설정이 완료되면 예약된 작업을 검토하고 조직의 요구에 맞게 조정해야 합니다.

자세한 내용은 예약 백업, 503 페이지를 참고하십시오.

백업 파일 저장

로컬로 백업을 저장할 수 있습니다. 그러나 NFS, SMB 또는 SSHFS 네트워크 볼륨을 원격 스토리지로 마운트하여 management center 및 매니지드 디바이스를 안전한 원격 위치에 백업하는 것이 좋습니다. 이렇게 하면 모든 후속 백업이 해당 볼륨에 복사되지만, 계속해서 management center를 사용하여 백업을 관리할 수 있습니다.

자세한 내용은 원격 스토리지 디바이스, 95 페이지 및 백업 및 원격 스토리지 관리, 495 페이지를 참조하십시오.

Management Center 및 매니지드 디바이스 복원

Backup Management(백업 관리) 페이지에서 management center를 복구합니다. SD 카드와 재설정 버튼을 사용하는 ISA 3000 제로 터치 복원을 제외하고 threat defense CLI를 사용하여 threat defense 디바이스를 복원해야 합니다..

자세한 내용은 Management Center 및 매니지드 디바이스 복원, 479 페이지를 참고하십시오.

백업이란**?**

Management Center 백업에는 다음이 포함될 수 있습니다.

- 설정

  management center 웹 인터페이스에서 설정할 수 있는 모든 설정은 원격 스토리지 및 감사 로그 서버 인증서 설정을 제외하고 설정 백업에 포함됩니다. 다중 도메인 구축에서는 설정을 백업해야 합니다. 이벤트 또는 TID 데이터만 백업할 수는 없습니다.

- 이벤트.

  이벤트 백업에는 management center 데이터베이스의 모든 이벤트가 포함됩니다. 그러나 management center 이벤트 백업에는 침입 이벤트 검토 상태가 포함되지 않습니다. 복구된 침입 이벤트는 Reviewed Events(검토된 이벤트) 페이지에 나타나지 않습니다.

- TID(Threat Intelligence Director) 데이터.

  자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *threat intelligence director* 데이터 백업 및 복원 정보를 참조하십시오.

디바이스 백업은 항상 설정 전용입니다.

복구되는 항목

설정을 복구하면 극히 드문 예외를 제외하고 모든 백업된 설정을 덮어씁니다. management center에서 이벤트 및 TID 데이터를 복구하면 침입 이벤트를 제외한 모든 기존 이벤트 및 TID 데이터를 덮어씁니다.

다음 사항을 이해하고 계획해야 합니다.

- 백업되지 않은 항목은 복구할 수 없습니다.

  Management Center 설정 백업에는 원격 스토리지 및 감사 로그 서버 인증서 설정이 포함되지 않으므로 복구 후에 이러한 설정을 다시 구성해야 합니다. 또한 management center 이벤트 백업에

는 침입 이벤트 검토 상태가 포함되지 않으므로 복구된 침입 이벤트는 Reviewed Events(검토된 이벤트) 페이지에 나타나지 않습니다.

- VPN 인증서 복구에 실패했습니다.

  threat defense 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense 디바이스에서 VPN 인증서 및 모든 VPN 구성을 제거합니다. threat defense 디바이스를 복구한 후에는 모든 VPN 인증서를 다시 추가/다시 등록하고 디바이스를 다시 구축해야 합니다.

- 구성된 management center 복구 - 공장 설정으로 새로 고침 또는 이미지 재설치 대신 침입 이벤트와 파일 목록이 병합됩니다.

  management center 이벤트 복구 프로세스는 침입 이벤트를 덮어쓰지 않습니다. 대신 백업의 침입 이벤트가 데이터베이스에 추가됩니다. 중복을 방지하려면 복구 전에 기존 침입 이벤트를 삭제하십시오.

  management center 설정 복구 프로세스는 악성코드 대응 에서 사용되는 정상 및 사용자 지정 탐지 파일 목록을 덮어쓰지 않습니다. 대신 기존 파일 목록을 백업의 파일 목록과 병합합니다. 파일 목록을 교체하려면 복구하기 전에 기존 파일 목록을 삭제하십시오.

백업 및 복구 요구 사항

백업 및 복구에는 다음 요구 사항이 있습니다.

모델 요구 사항**:** 백업

다음을 백업할 수 있습니다.

- 이 management center
- threat defense 독립형 디바이스, 네이티브 인스턴스, 컨테이너 인스턴스, 고가용성 쌍 및 클러스터
- 프라이빗 클라우드 독립형 디바이스, 고가용성 쌍 및 클러스터용 threat defense virtual

백업은 다음에 대해 지원되지 않습니다.

- 퍼블릭 클라우드용 threat defense virtual

백업 및 복구가 지원되지 않는 디바이스를 교체해야 한다면 디바이스별 설정을 수동으로 다시 생성해야 합니다. 하지만 management center 백업은 매지니드 디바이스에 구축하는 정책과 다른 구성은 백업하지 않으며, 디바이스에서 이미 management center로 전송된 이벤트도 백업하지 않습니다.

모델 요구 사항**:** 복구

교체 매니지드 디바이스는 교체하려는 디바이스와 동일한 모델이어야 하며 동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스를 사용해야 합니다.

management center의 경우 RMA 시나리오에서 백업 및 복구를 사용할 수 있을 뿐 아니라 management center 간에 설정 및 이벤트를 마이그레이션할 수도 있습니다. 지원되는 대상 및 대상 모델을 포함한 자세한 내용은 Firepower Management Center 모델 마이그레이션 가이드의 내용을 참조하십시오.

버전 요구 사항

모든 백업의 첫 번째 단계로 패치 레벨을 참고합니다. 백업을 복구하려면 이전 어플라이언스와 새 어플라이언스에서 패치를 포함하여 동일한 소프트웨어 버전을 실행해야 합니다.

또한 Firepower 4100/9300 섀시에서 소프트웨어를 복구하려면 섀시에서 호환되는 FXOS 버전을 실행해야 합니다.

management center 백업의 경우 동일한 VDB 또는 SRU가 없어도됩니다. 그러나 백업을 복구하면 기존 VDB가 백업 파일의 VDB로 대체됩니다.

라이선스 요건

모범 사례 및 절차에 설명된 대로 라이선싱 또는 고아 엔타이틀먼트 문제를 해결합니다. 라이선싱 충돌이 발견되면 Cisco TAC에 문의하십시오.

도메인 요구 사항

작업:

- management center 백업 또는 복구: 전역 전용.
- management center에서 디바이스 백업: 전역 전용.
- 디바이스 복구 : 없음. CLI에서 로컬로 디바이스를 복구합니다.

다중 도메인 구축에서는 이벤트/TID 데이터만백업할 수는 없습니다. 구성도 함께 백업해야 합니다.

백업 및 복원 지침 및 제한 사항

백업 및 복원에는 다음과 같은 지침 및 제한 사항이 있습니다.

백업 및 복원은 재해 복구**/RMA**에 사용됩니다**.**

백업 및 복원은 주로 RMA 시나리오를 위한 것입니다. 결함이 있거나 고장난 물리적 어플라이언스의 복원 프로세스를 시작하기 전에, Cisco TAC에 연락해 교체 하드웨어를 요청하십시오.

백업 및 복원을 사용하여 management center 간에 구성 및 이벤트를 마이그레이션할 수도 있습니다. 따라서 조직의 성장, 물리적 구현에서 가상 구현으로의 마이그레이션, 하드웨어 새로 고침 등의 기술적 또는 비즈니스적 이유로 인해 management center를 쉽게 교체할 수 있습니다.

백업 및 복원은 구성 가져오기**/**내보내기가 아닙니다**.**

백업 파일에는 어플라이언스를 고유하게 식별하며 공유할 수 없는 정보가 들어 있습니다. 백업 및 복원 프로세스를 사용하여 어플라이언스 또는 디바이스 간에 구성을 복사하거나, 새 구성을 테스트하는 동안 다른 구성을 저장하지는 마십시오. 대신 가져오기/내보내기 기능을 사용해야 합니다.

예를 들어 threat defense 디바이스 백업에는 디바이스의 관리 IP 주소 및 디바이스가 관리 management center에 연결하는 데 필요한 모든 정보가 포함됩니다. 다른 management center에서 매니지드 디바이스에 threat defense 백업을 복구하지 마십시오. 복구된 디바이스는 백업에 지정된 management center에 연결을 시도합니다.

복구는 개별적으로 그리고 로컬에서 진행됩니다.

management center 및 매니지드 디바이스에 개별적으로 및 로컬로 복원합니다. 이것은 다음을 의미합니다:

- 고가용성 또는 클러스터링 management center 또는 디바이스는 일괄 복구할 수 없습니다.
- management center를 사용하여 디바이스를 복구할 수는 없습니다. management center의 경우 웹 인터페이스를 사용하여 복구할 수 있습니다. threat defense 디바이스의 경우 SD 카드 및 재설정 버튼을 사용하는 ISA 3000 제로 터치 복원을 제외하고 threat defense CLI를 사용해야 합니다.
- management center 사용자 계정을 사용하여 매니지드 디바이스 중 하나에 로그인하고 복구할 수 없습니다. Management Center 및 디바이스는 자체 사용자 계정을 유지합니다.

Firepower 4100/9300용 구성 가져오기/내보내기 지침

구성 내보내기 기능을 사용하여 Firepower 4100/9300 섀시의 논리적 디바이스 및 플랫폼 구성 설정을 포함하는 XML 파일을 원격 서버 또는 로컬 컴퓨터로 내보낼 수 있습니다. 나중에 해당 구성 파일을 가져와서 구성 설정을 Firepower 4100/9300 섀시에 빠르게 적용하여, 알려진 정상적인 구성으로 돌아가거나 시스템 장애로부터 복구할 수 있습니다.

지침 및 제한 사항

- 구성 파일의 내용을 수정하지 마십시오. 구성 파일을 수정하면 해당 파일을 사용한 구성 가져오기가 실패할 수 있습니다.
- 애플리케이션 관련 구성 설정은 구성 파일에 포함되지 않습니다. 애플리케이션 관련 설정 및 구성을 관리하려면 애플리케이션에서 제공하는 구성 백업 도구를 사용해야 합니다.
- Firepower 4100/9300 섀시에서 설정을 가져오면 Firepower 4100/9300 섀시에 있는 모든 기존의 설정(논리적 디바이스 포함)이 삭제되고 가져오기 파일에 포함된 설정으로 완전히 교체됩니다.
- RMA 시나리오를 제외하고 설정을 내보낸 곳과 동일한 Firepower 4100/9300 섀시로 설정 파일만 가져오는 것이 좋습니다.
- 구성을 가져오는 Firepower 4100/9300 섀시의 플랫폼 소프트웨어 버전은 내보낼 때와 동일한 버전이어야 합니다. 버전이 다르면 가져오기 작업의 성공이 보장되지 않습니다. Firepower 4100/9300 섀시를 업그레이드 또는 다운그레이드할 때마다 백업 설정을 내보내는 것이 좋습니다.
- 구성을 가져오는 Firepower 4100/9300 섀시에는 내보냈을 때와 동일한 슬롯에 동일한 네트워크 모듈이 설치되어 있어야 합니다.
- 구성을 가져오는 Firepower 4100/9300 섀시에는, 가져오는 내보내기 파일에 정의된 논리적 디바이스에 대해 올바른 소프트웨어 애플리케이션 이미지가 설치되어 있어야 합니다.

- 기존 백업 파일을 덮어쓰지 않으려면, 백업 작업 시 파일 이름을 변경하거나 기존 파일을 다른 위치에 복사합니다.

참고 FXOS 가져오기/내보내기는 FXOS 구성만 백업하므로 논리적 앱을 별도로 백업해야 합니다. FXOS 구성 가져오기로 인해 논리적 디바이스가 재부팅되고 디바이스가 공장 기본 구성으로 재구축됩니다.

백업 및 복구 모범 사례

백업 및 복구에는 다음과 같은 모범 사례가 있습니다.

백업 시기

유지 보수 기간 또는 사용률이 낮은 다른 시간에 백업하는 것이 좋습니다.

시스템이 백업 데이터를 수집하는 동안 데이터 상관관계(management center만 해당) 도출이 일시적으로 일시 중지될 수 있으며, 백업 관련된 구성은 할 수 없게 됩니다. 이벤트 데이터를 포함하는 경우 eStreamer와 같은 이벤트 관련 기능을 사용할 수 없습니다.

다음 상황에서 백업해야 합니다.

- 정기 예약 백업.

  재해 복구 계획의 일환으로, 정기적인 백업 수행을 권장합니다.

  management center 설정 프로세스는 매주 설정 전용 백업을 예약하여 로컬에 저장합니다. 이는 전체 오프 사이트 백업을 대체하지 않습니다. 초기 설정이 완료되면 예약된 작업을 검토하고 조직의 요구에 맞게 조정해야 합니다. 자세한 내용은 예약 백업, 503 페이지를 참고하십시오.

- SLR 변경 후.

  SLR(Specific Licensing Reservations)을 변경한 후 management center를 백업합니다. 변경을 수행한 다음 이전 백업을 복원할 경우, 특정 라이선싱 반환 코드에 문제가 발생하여 고아 엔타이틀먼트가 발생할 수 있습니다.

- 업그레이드 또는 이미지 재설치 전.

  업그레이드가 심각하게 실패할 경우, 이미지를 재설치하고 복구해야 할 수 있습니다. 이미지를 재설치하면 시스템 암호를 포함하여 대부분의 설정이 공장 기본값으로 돌아갑니다. 최근 백업이 있는 경우, 보다 신속하게 정상 작업으로 돌아갈 수 있습니다.

- 업그레이드 후.

  새로 업그레이드한 구축의 스냅샷을 생성할 수 있도록 업그레이드 후 백업합니다. 매니지드 디바이스를 업그레이드한 후 management center를 백업하는 것이 좋습니다. 그러면 새 management center 백업 파일이 해당 디바이스가 업그레이드되었음을 '인식'합니다.

백업 파일 보안 유지

백업은 암호화되지 않은 아카이브(.tar) 파일로 저장됩니다.

PKI 개체의 개인 키 - 구축 지원에 필요한 공개 키 인증서 및 페어링된 개인 키가 백업되기 전에 암호 해독됨을 나타냅니다. 키는 백업을 복원할 때 임의로 생성된 키로 다시 암호화됩니다.

참고 management center와 디바이스를 안전한 원격 위치에 백업하고 전송 성공을 확인하는 것이 좋습니다. 로컬에 남아 있는 백업은 수동으로 또는 업그레이드 프로세스에 의해 삭제되어 로컬에 저장된 백업을 제거할 수 있습니다.

특히 백업 파일은 암호화되지 않으므로 무단 액세스를 허용하지 않습니다. 백업 파일이 수정되면 복원 프로세스가 실패하게 됩니다. Admin/Maint(관리/유지 관리) 역할의 사용자는 원격 스토리지에서 파일을 이동하고 삭제할 수 있는 백업 관리 페이지에 액세스할 수 있습니다.

management center의 시스템 설정에서 NFS, SMB 또는 SSHFS 네트워크 볼륨을 원격 스토리지로 마운트할 수 있습니다. 이렇게 하면 모든 후속 백업이 해당 볼륨에 복사되지만, 계속해서 management center를 사용하여 백업을 관리할 수 있습니다. 자세한 내용은 원격 스토리지 디바이스, 95 페이지 및 백업 및 원격 스토리지 관리, 495 페이지를 참조하십시오.

management center만 네트워크 볼륨을 마운트합니다. 매니지드 디바이스 백업 파일은 management center를 통해 라우팅됩니다. management center와 해당 디바이스 간에 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다. 자세한 내용은 Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(문제 해결 TechNote)을 참조하십시오.

Management Center 고가용성 구축의 백업 및 복구

management center 고가용성 구축에서는 한 management center를 백업해도 다른 FMC는 백업되지 않습니다. 두 피어를 정기적으로 백업해야 합니다. 특정 HA 피어를 다른 HA 피어의 백업 파일을 사용하여 복구하지 마십시오. 백업 파일에는 어플라이언스를 고유하게 식별하며 공유할 수 없는 정보가 들어 있습니다.

백업에 성공하지 않고도 HA management center를 교체할 수 있습니다. 백업 성공 여부에 관계없이 HA management center를 교체하는 방법에 대한 자세한 내용은 고가용성 쌍의 Management Center 교체, 328 페이지의 내용을 참조하십시오.

Threat Defense 고가용성 구축의 백업 및 복구

threat defense 고가용성 구축에서는 다음을 수행해야 합니다.

- management center에서 디바이스 쌍을 백업하되, threat defense CLI에서 개별적으로 로컬에서 복구합니다.

  백업 프로세스에서는 threat defense 고가용성 디바이스용으로 고유한 백업 파일을 생성합니다. 특정 고가용성 피어를 다른 HA 피어의 백업 파일을 사용하여 복구하지 마십시오. 백업 파일에는 어플라이언스를 고유하게 식별하며 공유할 수 없는 정보가 들어 있습니다.

  threat defense 고가용성 디바이스의 역할은 백업 파일 이름에 표시됩니다. 복구할 때는 적절한 백업 파일(기본 및 보조)을 선택해야 합니다.

- 복구하기 전에 고가용성을 일시 중단하거나 해제하지 마십시오.

  고가용성 설정을 유지 관리하면 복구 후 교체 디바이스를 쉽게 다시 연결할 수 있습니다. 이 작업을 수행하려면 고가용성 동기화를 다시 시작해야 합니다.

- 두 피어에서 동시에 **restore** CLI 명령을 실행하지 마십시오.

  백업이 성공했다고 가정하면 고가용성 쌍의 피어 중 하나 또는 둘 다를 교체할 수 있습니다. 동시에 수행할 수 있는 모든 물리적 교체 작업에는 랙킹 해제, 재랙킹 등이 있습니다. 그러나 재부팅을 포함하여 첫 번째 디바이스에 대한 복구 프로세스가 완료될 때까지 두 번째 디바이스에서 **restore** 명령을 실행하지 마십시오.

백업에 성공하지 않고도 threat defense 고가용성 디바이스를 교체할 수 있습니다..

Threat Defense 클러스터링 구축의 백업 및 복원

threat defense 클러스터링 구축에서는 다음을 수행해야 합니다.

- management center에서 전체 클러스터를 백업하지만 threat defense CLI에서 노드를 개별적으로 로컬로 복원합니다.

  백업 프로세스는 각 클러스터 노드에 대한 고유한 백업 파일을 포함하는 번들 tar 파일을 생성합니다. 한 노드를 다른 노드의 백업 파일로 복원하지 마십시오. 백업 파일에는 디바이스를 고유하게 식별하며 공유할 수 없는 정보가 들어 있습니다.

  노드의 역할은 백업 파일 이름에 표시됩니다. 복구할 때는 적절한 백업 파일(제어 또는 데이터)을 선택해야 합니다.

  개별 노드는 백업할 수 없습니다. 데이터 노드가 백업에 실패하는 경우에도 management center는 다른 모든 노드를 백업합니다. 제어 노드가 백업에 실패하면 백업이 취소됩니다.

- 복구하기 전에 클러스터링을 일시 중단하거나 해제하지 마십시오.

  클러스터 구성을 유지 관리하면 복구 후 교체 디바이스를 쉽게 다시 연결할 수 있습니다.

- 여러 노드에서 동시에 **restore** CLI 명령을 실행하지 마십시오. 데이터 노드를 복원하기 전에 먼저 제어 노드를 복원하고 클러스터에 다시 조인할 때까지 기다리는 것이 좋습니다.

  백업에 성공한 경우 클러스터의 여러 노드를 교체할 수 있습니다. 동시에 수행할 수 있는 모든 물리적 교체 작업에는 랙킹 해제, 재랙킹 등이 있습니다. 그러나 재부팅을 포함하여 이전 노드에 대한 복구 프로세스가 완료될 때까지 추가 노드에서 **restore** 명령을 실행하지 마십시오.

Firepower 4100/9300 섀시 백업 및 복구

Firepower 4100/9300 섀시에서 threat defense 소프트웨어를 복구하려면 섀시에서 호환되는 FXOS 버전을 실행해야 합니다.

Firepower 4100/9300 섀시를 백업할 때는 FXOS 설정도 백업하는 것이 좋습니다. 추가 모범 사례는 Firepower 4100/9300용 구성 가져오기/내보내기 지침 , 469 페이지의 내용을 참조하십시오.

백업 전

백업하기 전에 다음을 수행해야 합니다.

- management center에서 VDB 및 SRU를 업데이트합니다.

  항상 최신 취약성 데이터베이스(VDB) 및 침입 규칙(SRU)을 사용하는 것이 좋습니다. management center를 백업하기 전에 Cisco 지원 및 다운로드 사이트에서 최신 버전을 확인하십시오.

- 디스크 공간을 확인합니다.

  백업을 시작하기 전에 어플라이언스 또는 원격 스토리지 서버에 충분한 디스크 공간이 있는지 확인하십시오. 사용 가능한 공간이 Backup Management(백업 관리) 페이지에 표시됩니다.

  공간이 충분하지 않으면 백업이 실패할 수 있습니다. 특히 백업을 예약하는 경우, 정기적으로 백업 파일을 정리하거나 원격 스토리지 위치에 추가 디스크 공간을 할당해야 합니다.

복구 전

복구하기 전에 다음을 수행해야 합니다.

- 라이선스 변경 사항을 되돌립니다.

  백업 이후에 수행한 라이선싱 변경 사항을 되돌립니다.

  그렇지 않으면 복구 후 라이선스 충돌 또는 고아 엔타이틀먼트가 발생할 수 있습니다. 그러나 CSSM(Cisco Smart Software Manager)에서 등록을 취소하지 마십시오. CSSM에서 등록을 취소하는 경우, 복구 후 다시 등록을 취소한 다음 재등록해야 합니다.

  복구가 완료되면 라이선싱을 다시 설정합니다. 라이선싱 충돌 또는 분리 자격이 확인되면 Cisco TAC에 문의하십시오.

- 결함이 있는 어플라이언스의 연결을 끊습니다.

  관리 인터페이스와 데이터 인터페이스(디바이스의 경우)의 연결을 끊습니다.

  threat defense 디바이스를 복구하면 교체 디바이스의 관리 IP 주소가 이전 디바이스의 관리 IP 주소로 설정됩니다. IP 충돌 방지를 위해, 교체 디바이스에 백업을 복구하기 전에 관리 네트워크와 이전 디바이스의 연결을 끊으십시오.

  management center를 복구해도 관리 IP 주소는 변경되지 않습니다. 교체 시 수동으로 설정해야 하는데, 작업 전에 네트워크에서 이전 어플라이언스의 연결을 해제해야 합니다.

- 매니지드 디바이스를 등록 취소하지 마십시오.

  management center 또는 매니지드 디바이스를 복구하든 관계없이 네트워크에서 어플라이언스의 물리적 연결을 끊더라도 management center에서 디바이스를 등록 취소하지 마십시오.

  등록을 취소한다면 보안 구역에서 인터페이스 매핑 같은 일부 디바이스 구성을 다시 설정해야 합니다. 복구 후에는 management center와 디바이스가 정상적으로 통신을 시작해야 합니다.

- 이미지 재설치.

  RMA 시나리오에서는 교체 어플라이언스가 공장 기본값으로 설정된 상태로 제공됩니다. 그러나 교체 어플라이언스가 이미 설정된 경우, 이미지를 재설치하는 것이 좋습니다. 이미지를 재설치하면 시스템 암호를 포함하여 대부분의 설정이 공장 기본값으로 돌아갑니다. 주 버전으로만 이미지를 재설치할 수 있으므로 이미지를 재설치한 후에 패치를 적용해야 할 수 있습니다.

이미지를 재설치하지 않을 경우, management center 침입 이벤트 및 파일 목록이 덮어쓰이지 않고 병합됩니다.

복원 후

복구 후 다음을 수행해야 합니다.

- 복구되지 않은 항목을 재구성합니다.

  여기에는 라이선싱, 원격 스토리지 및 감사 로그 서버 인증서 설정 재구성이 포함될 수 있습니다. 또한 실패한 threat defense VPN 인증서를 다시 추가/다시 등록해야 합니다.

- management center에서 VDB 및 SRU를 업데이트합니다.

  항상 최신 취약성 데이터베이스(VDB) 및 침입 규칙(SRU)을 사용하는 것이 좋습니다. 이는 백업의 VDB가 교체 management center의 VDB를 덮어쓰기 때문에 VDB에 특히 중요합니다.

- 구축.

  management center를 복구한 후 모든 매니지드 디바이스에 구축합니다. 디바이스를 복원한 후에는 Device Management(디바이스 관리) 페이지에서 강제 구축해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스에 기존 구성 재구축을 참조하십시오. 또는 구축해야 하는 management center 또는 디바이스를 복원하는지 여부.

Management Center 또는 매니지드 디바이스 백업

지원되는 어플라이언스에 대해 온 디맨드 또는 예약 백업을 수행할 수 있습니다.

management center에서 디바이스를 백업하는 데 백업 프로필이 필요하지 않습니다. 그러나 7000/8000 시리즈 디바이스의 로컬 백업과 마찬가지로 management center 백업에는 백업 프로파일이. 온 디맨드 백업 프로세스를 통해 새 백업 프로파일을 생성할 수 있습니다.

FMC 백업

온 디맨드 FMC 백업을 수행하려면 이 절차를 사용합니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 467 페이지
- 백업 및 복원 지침 및 제한 사항, 468 페이지
- 백업 및 복구 모범 사례, 470 페이지

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에는 로컬 및 원격으로 저장된 모든 백업이 나열됩니다. 또한 백업을 저장하는 데 사용할 수 있는 디스크 공간의 양도 나열합니다. 공간이 충분하지 않으면 백업이 실패할 수 있습니다.

단계 **2** 기존 백업 프로파일을 사용할지 아니면 새로 시작할지를 선택합니다.

FMC 백업을 사용하려면 백업 프로파일을 사용하거나 생성해야 합니다.

- 기존 백업 프로파일을 사용하려면 **Backup Profiles(**백업 프로파일**)**를 클릭합니다.

  사용하려는 프로파일 옆에 있는 편집 아이콘을 클릭합니다. 그런 다음 **Start Backup(**백업 시작**)**을 클릭하여 지금 백업을 시작할 수 있습니다. 또는 프로파일을 편집하려면 다음 단계로 이동합니다.

- **Firepower Management Backup(Firepower** 관리 백업**)**을 클릭하여 새로 시작하고 새 백업 프로파일을 생성합니다.

  백업 프로파일의 이름을 입력합니다.

단계 **3** 백업할 항목을 선택합니다.

- 구성 백업
- 이벤트 백업
- **Threat Intelligence Director** 백업

다중 도메인 구축에서는 설정을 백업해야 합니다. 이벤트 또는 TID 데이터만 백업할 수는 없습니다. 이러한 각 선택 항목에 대해 백업 및 백업되지 않는 항목에 대한 자세한 내용은 백업 및 복원 정보, 465 페이지의 내용을 참조하십시오.

단계 **4** FMC 백업 파일의 스토리지 위치를 적어둡니다.

이는 `/var/sf/backup/`의 로컬 스토리지이거나 원격 네트워크 볼륨입니다. 자세한 내용은 백업 및 원격 스토리지 관리, 495 페이지를 참고하십시오.

단계 **5** (선택 사항) **Copy when complete(**완료 시 복사**)**를 활성화하여 완료된 FMC 백업을 원격 서버에 복사합니다.

호스트 이름 또는 IP 주소, 원격 디렉토리의 경로, 사용자 이름 및 암호를 제공합니다. 암호 대신 SSH 공유 키를 사용하려면 **SSH Public Key(SSH** 공유 키**)** 필드의 내용을 원격 서버에 있는 지정된 사용자의 `authorized_keys` 파일에 복사합니다.

참고 이 옵션은 백업을 로컬에 저장하거나 SCP를 원격 위치에 저장하려는 경우 유용합니다. SSH 원격 스토리지를 설정한 경우, **Copy when complete(**완료 시 복사**)**를 사용하여 동일한 디렉터리에 백업 파일을 복사하지 마십시오.

단계 **6** (선택 사항) **Email(**이메일**)**을 활성화하고 백업이 완료되면 알림을 받을 이메일 주소를 입력합니다.

이메일 알림을 받으려면 메일 서버에 연결하도록 FMC를 설정해야 합니다.메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

단계 **7** 온 디맨드 백업을 시작하려면 **Start Backup(**백업 시작**)**을 클릭합니다.

기존 백업 프로파일을 사용하지 않는 경우 시스템에서 자동으로 생성하여 사용합니다. 지금 백업을 실행하지 않으려는 경우 **Save(**저장**)** 또는 **Save As New(**새로 저장**)**를 클릭하여 프로파일을 저장할 수 있습니다. 두 경우 모두 새로 생성된 프로파일을 사용하여 예약된 백업을 설정할 수 있습니다.

단계 **8** 메시지 센터에서 진행 상황을 모니터링합니다.

시스템이 백업 데이터를 수집하는 동안 데이터 상관관계 도출이 일시적으로 일시 중지될 수 있으며, 백업 관련된 구성은 할 수 없게 됩니다. 원격 스토리지를 설정했거나 **Copy when complete(**완료시 복사**)**를 활성화한 경우 FMC가 원격 서버에 임시 파일을 쓸 수 있습니다. 이러한 파일은 백업 프로세스가 끝나면 정리됩니다.

다음에 수행할 작업

원격 스토리지를 설정했거나 **Copy when complete(**완료시 복사**)**를 활성화한 경우 백업 파일의 전송 성공을 확인합니다.

Management Center에서 디바이스 백업

이 절차를 사용하여 다음 디바이스에 대한 온 디맨드 백업을 수행합니다.

- threat defense: 물리적 디바이스, 독립형, 고가용성, 클러스터
- threat defense virtual: 프라이빗 클라우드, 독립형, 고가용성, 클러스터

백업 및 복구는 클러스터된 디바이스.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 467 페이지
- 백업 및 복원 지침 및 제한 사항, 468 페이지
- 백업 및 복구 모범 사례, 470 페이지

Firepower 4100/9300 섀시를 백업하는 경우에는 FXOS구성FXOS 구성 파일 내보내기, 477 페이지도 백업하는 것이 특히 중요합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(툴)** > **Backup/Restore(백업/복구)**을 선택한 다음 **Managed Device Backup(매니지드 디바이스 백업)**을 클릭합니다.

단계 **2** 하나 이상의 **Managed Devices(매니지드 디바이스)**를 선택합니다.

클러스터링의 경우 클러스터를 선택합니다. 개별 노드에서는 백업을 수행할 수 없습니다.

단계 **3** 디바이스 백업 파일의 스토리지 위치를 적어 둡니다.

이는 `/var/sf/remote-backup/`의 로컬 스토리지이거나 원격 네트워크 볼륨입니다. ISA 3000의 경우 SD 카드가 설치되어있는 경우 백업 사본이 SD 카드의 `/mnt/disk3/backup`에도 생성됩니다. 자세한 내용은 백업 및 원격 스토리지 관리, 495 페이지를 참고하십시오.

단계 **4** 원격 스토리지를 설정하지 않은 경우, **Management Center**로 검색할지 여부를 선택합니다.

- 활성화됨(기본값): `/var/sf/remote-backup/`에 있는 management center에 백업을 저장합니다.

  클러스터의 경우 이 옵션은 항상 선택되어 있습니다. 개별 노드 백업 파일은 management center에 복사된 다음 단일 압축 tar 파일로 번들된 다음 원격 스토리지에 복사됩니다.

- Disabled: `/var/sf/backup`의 디바이스에 백업을 저장합니다.

단계 **5** 온 디맨드 백업을 시작하려면 **Start Backup(백업 시작)**을 클릭합니다.

단계 **6** 메시지 센터에서 진행 상황을 모니터링합니다.

다음에 수행할 작업

원격 저장소를 구성한 경우 백업 파일이 성공적으로 전송되었는지 확인합니다.

FXOS 구성 파일 내보내기

Firepower 4100/9300 섀시의 논리적 디바이스 및 플랫폼 구성 설정을 포함하는 XML 파일을 원격 서버 또는 로컬 컴퓨터로 내보내려면 구성 내보내기 기능을 사용합니다.

참고 이 절차에서는 위협 방어를 백업할 때 Secure Firewall 섀시 관리자을(를) 사용하여 FXOS 설정을 내보내는 방법을 설명합니다. CLI 절차는 Cisco Firepower 4100/9300 FXOS CLI 설정 가이드의 해당 버전을 참조하십시오.

시작하기 전에

Firepower 4100/9300용 구성 가져오기/내보내기 지침 을 검토합니다.

프로시저

단계 **1** Secure Firewall 섀시 관리자에서 **System(**시스템**)** > **Configuration(**설정**)** > **Export(**내보내기**)**를 선택합니다.

단계 **2** 구성 파일을 로컬 컴퓨터로 내보내려면:

a) **Local(**로컬**)**을 클릭합니다.

b) **Export(**내보내기**)**를 클릭합니다.
구성 파일이 생성되고, 브라우저에 따라 기본 다운로드 위치로 파일이 자동으로 다운로드되거나 파일을 저장하라는 프롬프트가 표시될 수 있습니다.

단계 **3** 구성 파일을 원격 서버로 내보내려면:

a) **Remote(**원격**)**를 클릭합니다.

b) 원격 서버와의 통신에서 사용할 프로토콜을 선택합니다. FTP, TFTP, SCP, SFTP 중 하나일 수 있습니다.

c) 백업 파일을 저장할 위치의 IP 주소 또는 호스트 이름을 입력합니다. 이는 Firepower 4100/9300 섀시가 네트워크를 통해 액세스할 수 있는 서버, 스토리지 어레이, 로컬 드라이브, 기타 읽기/쓰기 미디어일 수 있습니다.

IP 주소가 아니라 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.

d) 기본값 이외의 포트를 사용하려는 경우 **Port(**포트**)** 필드에 포트 번호를 입력합니다.

e) 시스템이 원격 서버에 로그인할 때 사용할 사용자 이름을 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.

f) 원격 서버 사용자 이름의 비밀번호를 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.

g) **Location(**위치**)** 필드에 구성 파일을 내보낼 전체 경로(파일 이름 포함)를 입력합니다.

h) 사용할 원격 구성에 대해 **Export(**내보내기**)**.
구성 파일이 생성되고 지정된 위치로 내보내기가 수행됩니다.

백업 프로파일 생성

백업 프로파일은 백업된 환경 설정 집합, 즉 백업 대상, 백업 파일을 저장할 위치 등입니다.

FMC 백업 및 7000/8000 Series 로컬 백업에는 백업 프로파일이 필요합니다. 백업 프로파일은 FMC에서 디바이스를 백업하는 데 필요하지 않습니다.

온 디맨드 FMC을 수행할 때 기존 백업 프로파일을 선택하지 않으면 시스템에서 자동으로 생성하여 사용합니다. 그런 다음 새로 생성된 프로파일을 사용하여 예약된 백업을 설정할 수 있습니다.

다음 절차에서는 온 디맨드 백업을 수행하지 않고 백업 프로필을 생성하는 방법을 설명합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**를 선택하고 **Backup Profiles(**백업 프로파일**)**를 클릭합니다.

단계 **2** **Create Profile(**프로필 생성**)**을 클릭하고 **Name(**이름**)**을 입력합니다.

단계 **3** 백업할 항목을 선택합니다.

- 구성 백업
- 이벤트 백업
- **Threat Intelligence Director** 백업

다중 도메인 구축에서는 설정을 백업해야 합니다. 이벤트 또는 TID 데이터만 백업할 수는 없습니다. 이러한 각 선택 항목에 대해 백업 및 백업되지 않는 항목에 대한 자세한 내용은 백업 및 복원 정보, 465 페이지의 내용을 참조하십시오.

단계 **4** 백업 파일의 스토리지 위치를 적어둡니다.

이는 `/var/sf/backup/`의 로컬 스토리지이거나 원격 네트워크 볼륨입니다. ISA 3000의 경우 SD 카드가 설치되어있는 경우 백업 사본이 SD 카드의 `/mnt/disk3/backup`에도 생성됩니다. 자세한 내용은 백업 및 원격 스토리지 관리, 495 페이지를 참고하십시오.

단계 **5** (선택 사항) **Copy when complete(**완료 시 복사**)**를 활성화하여 완료된 FMC 백업을 원격 서버에 복사합니다.

호스트 이름 또는 IP 주소, 원격 디렉토리의 경로, 사용자 이름 및 암호를 제공합니다. 암호 대신 SSH 공유 키를 사용하려면 **SSH Public Key(SSH** 공유 키**)** 필드의 내용을 원격 서버에 있는 지정된 사용자의 `authorized_keys` 파일에 복사합니다.

참고 이 옵션은 백업을 로컬에 저장하거나 SCP를 원격 위치에 저장하려는 경우 유용합니다. SSHFS 원격 스토리지를 설정한 경우, **Copy when complete(**완료 시 복사**)**를 사용하여 동일한 디렉터리에 백업 파일을 복사하지 마십시오.

단계 **6** (선택 사항) **Email(**이메일**)**을 활성화하고 백업이 완료되면 알림을 받을 이메일 주소를 입력합니다.

이메일 알림을 받으려면 메일 서버에 연결하도록 FMC를 설정해야 합니다.메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

단계 **7** **Save(**저장**)**를 클릭합니다.

Management Center 및 매니지드 디바이스 복원

management center 웹 인터페이스를 사용하여 백업에서 복구합니다. threat defense 디바이스의 경우 threat defense CLI를 사용해야 합니다. management center를 사용하여 디바이스를 복구할 수는 없습니다.

다음 섹션에서는 management center 및 매니지드 디바이스를 복구하는 방법을 설명합니다.

백업에서 Management Center 복원

management center 백업을 복구할 때 백업 파일에 포함된 구성 요소(이벤트, 설정, TID 데이터) 중 일부 또는 전체를 복구하도록 선택할 수 있습니다.

참고 설정을 복구하면 극히 드문 예외를 제외하고 모든 설정을 덮어씁니다. 또한 management center가 재부팅됩니다. 이벤트 및 TID 데이터를 복구하면 침입 이벤트를 제외한 모든 기존 이벤트 및 TID 데이터를 덮어씁니다. 준비가 되었는지 확인하십시오.

백업에서 management center를 복구하려면 이 절차를 사용합니다.management center HA 구축에서의 백업 및 복구에 대한 자세한 내용은 고가용성 쌍의 Management Center 교체, 328 페이지의 내용을 참고하십시오.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 467 페이지
- 백업 및 복원 지침 및 제한 사항, 468 페이지
- 백업 및 복구 모범 사례, 470 페이지

프로시저

단계 **1** 복구하려는 management center에 로그인합니다.

단계 **2** 시스템 (⚙) > **Tools(툴)** > **Backup/Restore(백업/복구)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에는 로컬 및 원격으로 저장된 모든 백업 파일이 나열됩니다. 백업 파일을 클릭하고 내용을 확인할 수 있습니다.

백업 파일이 목록에 없고 로컬 컴퓨터에 저장한 경우 **Upload Backup(백업 업로드)**을 클릭합니다. 백업 및 원격 스토리지 관리, 495 페이지의 내용을 참조하십시오.

단계 **3** 복구하려는 백업 파일을 선택하고 **Restore(복구)**를 클릭합니다.

단계 **4** 복구할 수 있는 구성 요소 중에서 선택한 다음 **Restore(복구)**를 다시 클릭하여 시작합니다.

단계 **5** 메시지 센터에서 진행 상황을 모니터링합니다.

구성을 복구하는 경우, management center를 재부팅한 후 다시 로그인하면 됩니다.

다음에 수행할 작업

- 필요에 따라 복구 전에 되돌린 라이선싱 설정을 다시 구성합니다. 라이선싱 충돌 또는 분리 자격이 확인되면 Cisco TAC에 문의하십시오.
- 필요에 따라 원격 스토리지 및 감사 로그 서버 인증서 설정을 다시 구성합니다. 이러한 설정은 백업에 포함되지 않습니다.
- (선택 사항) SRU 및 VDB를 업데이트합니다. Cisco 지원 및 다운로드 사이트에서 제공되는 SRU 또는 VDB가 현재 실행 중인 버전보다 최신 상태이면 최신 버전을 설치하는 것이 좋습니다.
- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

백업에서 Threat Defense 복원: Firepower 1000/2100, Secure Firewall 3100, ISA 3000(비제로 터치)

Threat Defense 백업 및 복구는 RMA용입니다. 설정을 복구하면 관리 IP 주소를 포함하여 디바이스의 모든 설정을 덮어씁니다. 또한 디바이스를 재부팅합니다.

하드웨어 장애 시 이 절차에서는 Firepower 1000/2100, Secure Firewall 3100 또는 ISA 3000 threat defense 디바이스를 독립형이나 고가용성 쌍 또는 클러스터로 교체하는 방법을 설명합니다. 여기서는 교체하려는 디바이스 또는 디바이스의 백업에 액세스할 수 있다고 가정합니다. Management Center에서 디바이스 백업, 476 페이지의 내용을 참조하십시오.SD 카드를 사용하는 ISA 3000에서의 제로 터치 복원에 대해서는 백업에서 제로 터치 복원 Threat Defense: ISA 3000, 485 페이지의 내용을 참조하십시오.

threat defense 고가용성 및 클러스터링 구축에서는 이 절차를 사용하여 모든 피어를 교체할 수 있습니다. 모두 교체하려면 **restore** CLI 명령을 제외한 모든 디바이스에서 모든 단계를 동시에 수행합니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 467 페이지
- 백업 및 복원 지침 및 제한 사항, 468 페이지
- 백업 및 복구 모범 사례, 470 페이지

프로시저

단계 1 교체 하드웨어에 대해서는 Cisco TAC에 문의하십시오.

동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스의 동일한 모델을 가져옵니다. Cisco는 Portal을 반환합니다.에서 RMA 프로세스를 시작할 수 있습니다.

단계 2 결함이 있는 디바이스의 성공적인 백업을 찾습니다.

클러스터링의 경우 노드 백업 파일은 클러스터의 단일 압축 파일(*cluster_name*.*timestamp*.**tar.gz**)에 번들로 제공됩니다. 노드를 복원하려면 먼저 개별 노드 백업 파일 (*node_name*_**control**_*timestamp*.**tar** 또는 *node_name*_**data**_*timestamp*.**tar**)을 추출해야 합니다.

백업 설정에 따라 다음 위치에 디바이스 백업이 저장될 수 있습니다.

- `/var/sf/backup`의 결함 있는 디바이스 자체
- `/var/sf/remote-backup`의 management center
- 원격 스토리지 위치

threat defense 고가용성 구축에서는 쌍을 유닛으로 백업하지만 백업 프로세스에서 고유한 백업 파일을 생성합니다. 디바이스의 역할은 백업 파일 이름에 표시됩니다.

백업의 유일한 복사본이 결함이 있는 디바이스에 있는 경우 지금 다른 위치에 복사합니다. 디바이스 이미지를 재설치하면 백업이 지워집니다. 다른 문제가 발생하면 백업을 복구하지 못할 수 있습니다. 자세한 내용은 백업 및 원격 스토리지 관리, 495 페이지를 참고하십시오.

교체 디바이스에는 백업이 필요하지만 복구 프로세스 중에 SCP를 사용하여 검색할 수 있습니다. 교체 디바이스에서 SCP가 액세스할 수 있는 위치에 백업을 배치하는 것이 좋습니다. 또는 교체 디바이스 자체에 백업을 복사할 수 있습니다.

단계 3 결함이 있는 디바이스를 제거(분리)합니다.

모든 인터페이스의 연결을 끊습니다. threat defense 고가용성 구축에서는 페일오버 링크가 포함됩니다. 클러스터링의 경우 클러스터 제어 링크가 포함됩니다.

사용 중인 모델의 하드웨어 설치 및 시작 가이드를 참조하십시오.Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

단계 4 교체 디바이스를 설치하고 관리 네트워크에 연결합니다.

디바이스를 전원에 연결하고 관리 인터페이스를 관리 네트워크에 연결합니다. threat defense 고가용성 구축에서 페일오버 링크를 연결합니다. 클러스터링의 경우 클러스터 제어 링크를 연결합니다. 그러나 데이터 인터페이스를 연결하지 마십시오.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

단계 **5** (선택 사항) 교체 디바이스 이미지를 재설치합니다.

RMA 시나리오에서는 교체 장치가 공장 기본값으로 설정된 상태로 제공됩니다. 교체 디바이스가 결함이 있는 디바이스와 동일한 주 버전을 실행하지 않는 경우 이미지를 재설치하는 것이 좋습니다.

Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드를 참조하십시오.

단계 **6** 교체 디바이스에서 초기 설정을 수행합니다.

관리자로 threat defense CLI에 액세스합니다. 설정 마법사에서 관리 IP 주소, 게이트웨이 및 기타 기본 네트워크 설정을 설정하라는 메시지를 표시합니다.

결함이 있는 디바이스와 동일한 관리 IP 주소를 설정하지 마십시오. 따라서 패치를 적용하기 위해 디바이스를 등록해야 하는 경우 문제가 발생할 수 있습니다. 복구 프로세스에서 관리 IP 주소가 올바르게 재설정됩니다.

사용 중인 모델에 대한 시작 가이드의 초기 설정 항목을 참조하십시오.Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

참고 교체 디바이스를 패치해야 하는 경우 시작 가이드의 설명에 따라 management center 등록 프로세스를 시작합니다. 패치를 적용할 필요가 없으면 등록하지 마십시오.

단계 **7** 교체 디바이스가 결함이 있는 디바이스와 동일한 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

기존 디바이스를 management center에서 삭제해서는 안됩니다. 교체 디바이스는 물리적 네트워크에서 관리되지 않아야 하며 새 하드웨어와 교체 threat defense 패치의 버전이 동일해야 합니다. threat defense CLI에는 업그레이드 명령이 없습니다. 패치하려면 다음을 수행합니다.

a) management center 웹 인터페이스에서 디바이스 등록 프로세스를 완료합니다.

새 AC 정책을 생성하고 기본 작업인 "Network Discovery(네트워크 검색)"를 사용합니다. 이 정책은 그대로 유지합니다. 기능 또는 수정 사항을 추가하지 마십시오. 이는 디바이스를 등록하고 기능이 없는 정책을 구축하는 데 사용되므로 라이센스가 필요하지 않으며 디바이스를 패치할 수 있습니다. 백업이 복구되면 라이선싱 및 정책이 예상 상태로 복구됩니다.

b) 디바이스를 패치합니다: Cisco Firepower Management Center 업그레이드 설명서.

c) management center에서 새로 패치한 디바이스 등록을 취소합니다.

등록을 취소하지 않으면 복구 프로세스에서 "오래된" 디바이스가 다시 가동된 후 management center에 고스트 디바이스가 등록됩니다.

단계 **8** 교체 디바이스가 백업 파일에 액세스할 수 있는지 확인합니다.

복구 프로세스에서 SCP를 사용하여 백업을 검색할 수 있으므로 백업을 액세스 가능한 위치에 두는 것이 좋습니다. 또는 백업을 교체 디바이스 자체에 수동으로 `/var/sf/backup`에 복사할 수 있습니다. 클러스터링의 경우 기본 클러스터 번들에서 개별 노드 백업 파일을 추출했는지 확인합니다.

단계 **9** threat defense CLI에서 백업을 복구합니다.

관리자로 threat defense CLI에 액세스합니다. 콘솔을 사용하거나 새로 설정된 관리 인터페이스(IP 주소 또는 호스트 이름)에 SSH를 통해 연결할 수 있습니다. 복구 프로세스에서 이 IP 주소가 변경됩니다.

복구하려면 다음을 수행합니다.

- SCP 사용: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- 로컬 디바이스에서: **restore remote-manager-backup** *backup tar-file*

threat defense 고가용성 및 클러스터링 구축에서는 적절한 백업 파일(기본 대 보조 또는 제어 대 데이터)을 선택해야 합니다. 역할은 백업 파일 이름에 표시됩니다. 모든 디바이스를 복원하는 경우 순차적으로 수행합니다. 재부팅을 포함하여 첫 번째 디바이스에 대한 복구 프로세스가 완료될 때까지 다음 디바이스에서 **restore** 명령을 실행하지 마십시오.

단계 **10** management center에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

복구가 완료되면 디바이스는 사용자를 CLI에서 로그아웃하고 재부팅하며 management center에 자동으로 연결합니다. 현재 디바이스가 오래된 것으로 표시됩니다.

단계 **11** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.
- 고가용성 동기화를 다시 시작합니다. threat defense CLI에서 `configure high-availability resume`을 입력합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 고가용성 일시 중단 또는 재개를 참조하십시오.
- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense디바이스에서 VPN 인증서를 제거합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *VPN* 인증서 관리를 참조하십시오.

단계 **12** 설정을 구축합니다.

반드시 구축해야 합니다. 디바이스를 복원한 후에는 Device Management(디바이스 관리) 페이지에서 강제 구축해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 디바이스에 기존 구성을 재구축을 참조하십시오.

단계 **13** 디바이스의 데이터 인터페이스를 연결합니다.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

백업에서 제로 터치 복원 Threat Defense: ISA 3000

Threat Defense 백업 및 복구는 RMA용입니다. 설정을 복구하면 관리 IP 주소를 포함하여 디바이스의 모든 설정을 덮어씁니다. 또한 디바이스를 재부팅합니다.

하드웨어 장애 시 이 절차에서는 ISA 3000 threat defense 디바이스를 독립형 또는 HA 쌍으로 교체하는 방법을 간략하게 설명합니다. 장애가 발생한 유닛의 백업이 SD 카드에 있다고 가정합니다. Management Center에서 디바이스 백업, 476 페이지의 내용을 참조하십시오.

threat defense 고가용성 및 클러스터링 구축에서는 이 절차를 사용하여 모든 피어를 교체할 수 있습니다. 모두 교체하려면 **restore** CLI 명령을 제외한 모든 디바이스에서 모든 단계를 동시에 수행합니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 467 페이지
- 백업 및 복원 지침 및 제한 사항, 468 페이지
- 백업 및 복구 모범 사례, 470 페이지

프로시저

단계 **1** 교체 하드웨어에 대해서는 Cisco TAC에 문의하십시오.

동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스의 동일한 모델을 가져옵니다. Cisco는 Portal을 반환합니다.에서 RMA 프로세스를 시작할 수 있습니다.

단계 **2** 결함이 있는 디바이스에서 SD 카드를 제거하고 디바이스를 랙에서 분리합니다.

모든 인터페이스의 연결을 끊습니다. threat defense HA 구축에서는 페일오버 링크가 포함됩니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

단계 **3** 교체 디바이스를 다시 랙킹하고 관리 네트워크에 연결합니다. threat defense HA 구축에서는 페일오버 링크를 연결합니다. 그러나 데이터 인터페이스를 연결하지 마십시오.

디바이스 이미지를 재설치하거나 소프트웨어 패치를 적용해야 하는 경우, 전원 커넥터를 연결합니다.

단계 **4** (필요할 수 있음) 교체 디바이스 이미지를 재설치합니다.

RMA 시나리오에서는 교체 장치가 공장 기본값으로 설정된 상태로 제공됩니다. 교체 디바이스가 결함이 있는 디바이스와 동일한 주 버전을 실행하지 않는 경우 이미지를 재설치해야 합니다. https://www.cisco.com/go/isa3000-software에서 설치 프로그램을 가져옵니다.

이미지를 재설치하려면 Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드의 내용을 참조하십시오.

단계 **5** (필요할 수 있음) 교체 디바이스가 결함이 있는 디바이스와 동일한 Firepower 소프트웨어 버전(동일한 패치 버전 포함)을 실행 중인지 확인합니다. 디바이스를 패치해야하는 경우 Secure Firewall device manager(device manager)에 연결하여 패치를 설치할 수 있습니다.

다음 절차에서는 공장 기본 구성이 있다고 가정합니다. 디바이스를 이미 구성한 경우 device manager에 로그인하여 **Device(**디바이스**)** > **Upgrades(**업그레이드**)** 페이지로 직접 이동한 후 패치를 설치할 수 있습니다.

어느 경우든 패치 패키지를 https://www.cisco.com/go/isa3000-software에서 구합니다.

a) 컴퓨터를 내부(이더넷 1/2) 인터페이스에 직접 연결하고 기본 IP 주소(**https://192.168.95.1**)에서 device manager에 액세스합니다.
b) **admin** 사용자 이름과 비밀번호 **Admin123**을 입력하고 **Login(**로그인**)**을 클릭합니다.
c) 설정 마법사를 완료합니다. device manager에서 구성한 내용은 유지하지 않습니다. 패치를 적용할 수 있도록 초기 구성을 통과하기만 하면 되므로 설정 마법사에서 입력하는 내용은 중요하지 않습니다.
d) **Device(**디바이스**)** > **Upgrades(**업그레이드**)** 페이지로 이동합니다.

   System Upgrade(시스템 업그레이드**)** 섹션에는 현재 실행 중인 소프트웨어 버전이 표시됩니다.

e) **Browse(**찾아보기**)**를 클릭하여 패치 파일을 업로드합니다.
f) **Install(**설치**)**을 클릭하여 설치 프로세스를 시작합니다.

   아이콘 옆의 정보는 디바이스가 설치 중에 재부팅되는지 여부를 나타냅니다. 디바이스가 재부팅되면 시스템에서 자동으로 로그아웃됩니다. 설치에는 30분 이상 소요될 수 있습니다.

   이 시간 동안 기다렸다가 시스템에 다시 로그인하십시오. 디바이스 요약 또는 시스템 모니터링 대시보드에 새 버전이 표시됩니다.

   참고 브라우저 창을 그냥 새로 고치지 말고, URL의 경로를 삭제한 다음 홈페이지에 다시 연결하십시오. 이렇게 하면 캐시된 정보가 최신 코드로 새로고침됩니다.

단계 **6** 교체 디바이스에 SD 카드를 삽입합니다.

단계 **7** 디바이스의 전원을 켜거나 재부팅하고 부팅을 시작한 직후 Reset(재설정) 버튼을 3초 이상 15초 이하로 길게 누릅니다.

패치를 설치하는 데 device manager를 사용한 경우 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Reboot/Shutdown(**재부팅/종료**)** 페이지에서 재부팅할 수 있습니다. threat defense CLI에서는 **reboot** 명령을 사용하십시오. 아직 전원을 연결하지 않은 경우 지금 연결합니다.

와이어 게이지 0.033인치 이하의 표준 사이즈 #1 용지 클립을 사용하여 Reset(재설정) 버튼을 누릅니다. 복원 프로세스는 부팅 중에 트리거됩니다. 디바이스가 구성을 복원한 다음 재부팅합니다. 그러면 디바이스가 management center에 자동으로 등록됩니다.

HA 쌍의 두 디바이스를 모두 복원하는 경우 순차적으로 수행합니다. 재부팅을 포함하여 첫 번째 디바이스에 대한 복원 프로세스가 완료될 때까지 두 번째 디바이스를 복원하지 마십시오.

단계 **8** management center에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

현재 디바이스가 오래된 것으로 표시됩니다.

단계 **9** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.
- 고가용성 동기화를 다시 시작합니다. threat defense CLI에서 `configure high-availability resume`을 입력합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 고가용성 일시 중단 또는 재개를 참조하십시오.
- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense디바이스에서 VPN 인증서를 제거합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *VPN* 인증서 관리를 참조하십시오.

단계 **10** 설정을 구축합니다.

반드시 구축해야 합니다. 디바이스를 복원한 후에는 Device Management(디바이스 관리) 페이지에서 강제 구축해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 디바이스에 기존 구성을 재구축을 참조하십시오.

단계 **11** 디바이스의 데이터 인터페이스를 연결합니다.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

백업에서 Threat Defense 복원: Firepower 4100/9300 섀시

Threat Defense 백업 및 복구는 RMA용입니다. 설정을 복구하면 관리 IP 주소를 포함하여 디바이스의 모든 설정을 덮어씁니다. 또한 디바이스를 재부팅합니다.

이 절차에서는 하드웨어 장애가 발생한 경우 Firepower 4100/9300, 독립형, 고가용성 쌍 또는 클러스터로 교체하는 방법을 간략하게 설명합니다. 다음의 백업에 액세스할 수 있다고 가정합니다.

- 논리적 디바이스 또는 하나 이상의 디바이스를 교체합니다. Management Center에서 디바이스 백업, 476 페이지의 내용을 참조하십시오.
- FXOS 설정. FXOS 구성 파일 내보내기, 477 페이지의 내용을 참조하십시오.

threat defense 고가용성 및 클러스터링 구축에서는 이 절차를 사용하여 모든 피어를 교체할 수 있습니다. 모두 교체하려면 **restore** CLI 명령을 제외한 모든 디바이스에서 모든 단계를 동시에 수행합니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 467 페이지
- 백업 및 복원 지침 및 제한 사항, 468 페이지
- 백업 및 복구 모범 사례, 470 페이지

프로시저

단계 **1** 교체 하드웨어에 대해서는 Cisco TAC에 문의하십시오.

동일한 수의 네트워크 모듈과 동일한 유형 및 물리적 인터페이스의 동일한 모델을 가져옵니다. Cisco는 Portal을 반환합니다.에서 RMA 프로세스를 시작할 수 있습니다.

단계 **2** 결함이 있는 디바이스의 성공적인 백업을 찾습니다.

클러스터링의 경우 노드 백업 파일은 클러스터의 단일 압축 파일(*cluster_name*.*timestamp*.**tar.gz**)에 번들로 제공됩니다. 노드를 복원하려면 먼저 개별 노드 백업 파일 (*node_name*_**control**_*timestamp*.**tar** 또는 *node_name*_**data**_*timestamp*.**tar**)을 추출해야 합니다.

백업 설정에 따라 다음 위치에 디바이스 백업이 저장될 수 있습니다.

- `/var/sf/backup`의 결함 있는 디바이스 자체
- `/var/sf/remote-backup`의 management center
- 원격 스토리지 위치

threat defense 고가용성 구축에서는 쌍을 유닛으로 백업하지만 백업 프로세스에서 고유한 백업 파일을 생성합니다. 디바이스의 역할은 백업 파일 이름에 표시됩니다.

백업의 유일한 복사본이 결함이 있는 디바이스에 있는 경우 지금 다른 위치에 복사합니다. 디바이스 이미지를 재설치하면 백업이 지워집니다. 다른 문제가 발생하면 백업을 복구하지 못할 수 있습니다. 자세한 내용은 백업 및 원격 스토리지 관리, 495 페이지를 참고하십시오.

교체 디바이스에는 백업이 필요하지만 복구 프로세스 중에 SCP를 사용하여 검색할 수 있습니다. 교체 디바이스에서 SCP가 액세스할 수 있는 위치에 백업을 배치하는 것이 좋습니다. 또는 교체 디바이스 자체에 백업을 복사할 수 있습니다.

단계 **3** FXOS 설정의 성공적인 백업을 찾습니다.

단계 **4** 결함이 있는 디바이스를 제거(분리)합니다.

모든 인터페이스의 연결을 끊습니다. threat defense 고가용성 구축에서는 페일오버 링크가 포함됩니다. 클러스터링의 경우 클러스터 제어 링크가 포함됩니다.

사용 중인 모델의 하드웨어 설치 및 시작 가이드를 참조하십시오.Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

단계 **5** 교체 디바이스를 설치하고 관리 네트워크에 연결합니다.

디바이스를 전원에 연결하고 관리 인터페이스를 관리 네트워크에 연결합니다. threat defense 고가용성 구축에서 페일오버 링크를 연결합니다. 클러스터링의 경우 클러스터 제어 링크를 연결합니다. 그러나 데이터 인터페이스를 연결하지 마십시오.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

단계 **6** (선택 사항) 교체 디바이스 이미지를 재설치합니다.

RMA 시나리오에서는 교체 장치가 공장 기본값으로 설정된 상태로 제공됩니다. 교체 디바이스가 결함이 있는 디바이스와 동일한 주 버전을 실행하지 않는 경우 이미지를 재설치하는 것이 좋습니다.

해당 Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager 설정 가이드에서 공장 기본 설정 복구에 대한 지침을 참조하십시오.

단계 **7** FXOS가 호환되는 버전을 실행 중인지 확인합니다.

논리적 디바이스를 다시 추가하기 전에 호환되는 FXOS 버전을 실행 중이어야 합니다. 섀시 관리자를 사용하여 백업된 FXOS 설정을 가져올 수 있습니다.구성 파일 가져오기, 491 페이지

단계 **8** 섀시 관리자를 사용하여 논리적 디바이스를 추가하고 초기 설정을 수행합니다.

결함이 있는 섀시의 논리적 디바이스와 동일한 관리 IP 주소를 설정하지 마십시오. 따라서 패치를 적용하기 위해 논리적 디바이스를 등록해야 하는 경우 문제가 발생할 수 있습니다. 복구 프로세스에서 관리 IP 주소가 올바르게 재설정됩니다.

사용 중인 모델의 시작 설명서에서 management center 구축 장을 참조하십시오.Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

참고 논리적 디바이스를 패치해야 하는 경우 시작 가이드의 설명에 따라 management center에 등록합니다. 패치를 적용할 필요가 없으면 등록하지 마십시오.

단계 **9** 교체 디바이스가 결함이 있는 디바이스와 동일한 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

기존 디바이스를 management center에서 삭제해서는 안됩니다. 교체 디바이스는 물리적 네트워크에서 관리되지 않아야 하며 새 하드웨어와 교체 threat defense 패치의 버전이 동일해야 합니다. threat defense CLI에는 업그레이드 명령이 없습니다. 패치하려면 다음을 수행합니다.

a) management center 웹 인터페이스에서 디바이스 등록 프로세스를 완료합니다.

새 AC 정책을 생성하고 기본 작업인 "Network Discovery(네트워크 검색)"를 사용합니다. 이 정책은 그대로 유지합니다. 기능 또는 수정 사항을 추가하지 마십시오. 이는 디바이스를 등록하고 기능이 없는 정책을 구축하는 데 사용되므로 라이센스가 필요하지 않으며 디바이스를 패치할 수 있습니다. 백업이 복구되면 라이선싱 및 정책이 예상 상태로 복구됩니다.

b) 디바이스를 패치합니다: Cisco Firepower Management Center 업그레이드 설명서.

c) management center에서 새로 패치한 디바이스 등록을 취소합니다.

등록을 취소하지 않으면 복구 프로세스에서 "오래된" 디바이스가 다시 가동된 후 management center에 고스트 디바이스가 등록됩니다.

단계 **10** 교체 디바이스가 백업 파일에 액세스할 수 있는지 확인합니다.

복구 프로세스에서 SCP를 사용하여 백업을 검색할 수 있으므로 백업을 액세스 가능한 위치에 두는 것이 좋습니다. 또는 백업을 교체 디바이스 자체에 수동으로 `/var/sf/backup`에 복사할 수 있습니다. 클러스터링의 경우 기본 클러스터 번들에서 개별 노드 백업 파일을 추출했는지 확인합니다.

단계 **11** threat defense CLI에서 백업을 복구합니다.

관리자로 threat defense CLI에 액세스합니다. 콘솔을 사용하거나 새로 설정된 관리 인터페이스(IP 주소 또는 호스트 이름)에 SSH를 통해 연결할 수 있습니다. 복구 프로세스에서 이 IP 주소가 변경됩니다.

복구하려면 다음을 수행합니다.

- SCP 사용: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- 로컬 디바이스에서: **restore remote-manager-backup** *backup tar-file*

threat defense 고가용성 및 클러스터링 구축에서는 적절한 백업 파일(기본 대 보조 또는 제어 대 데이터)을 선택해야 합니다. 역할은 백업 파일 이름에 표시됩니다. 모든 디바이스를 복원하는 경우 순차적으로 수행합니다. 재부팅을 포함하여 첫 번째 디바이스에 대한 복구 프로세스가 완료될 때까지 다음 디바이스에서 **restore** 명령을 실행하지 마십시오.

단계 **12** management center에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

복구가 완료되면 디바이스는 사용자를 CLI에서 로그아웃하고 재부팅하며 management center에 자동으로 연결합니다. 현재 디바이스가 오래된 것으로 표시됩니다.

단계 **13** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.

- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense디바이스에서 VPN 인증서를 제거합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *VPN* 인증서 관리를 참조하십시오.

단계 **14** 설정을 구축합니다.

반드시 구축해야 합니다. 디바이스를 복원한 후에는 Device Management(디바이스 관리) 페이지에서 강제 구축해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 디바이스에 기존 구성을 재구축을 참조하십시오.

단계 **15** 디바이스의 데이터 인터페이스를 연결합니다.

사용 중인 모델의 하드웨어 설치 가이드를 참조하십시오. Cisco Secure Firewall Threat Defense: 설치 및 업그레이드 가이드

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

구성 파일 가져오기

Firepower 4100/9300 섀시에서 전에 내보낸 구성 설정을 적용하려면 구성 가져오기 기능을 사용할 수 있습니다. 이 기능을 사용하면 알려진 양호한 구성으로 돌아가거나 시스템 장애로부터 복구할 수 있습니다.

참고 이 절차에서는 소프트웨어를 복구하기 전에 섀시 관리자을(를) 사용하여 FXOS 설정을 가져오는 방법을 설명합니다. CLI 절차는 Cisco Firepower 4100/9300 FXOS CLI 설정 가이드의 해당 버전을 참조하십시오.

시작하기 전에

Firepower 4100/9300용 구성 가져오기/내보내기 지침 을 검토합니다.

프로시저

단계 **1** 섀시 관리자에서 **System(**시스템**)** > **Tools(**도구**)** > **Import(**가져오기/내보내기**)**를 선택합니다.

단계 **2** 로컬 구성 파일로부터 가져오려면:

a) **Local(**로컬**)**을 클릭합니다.

b) **Choose File(**파일 선택**)**을 클릭하고 가져올 구성 파일을 찾아 선택합니다.

c) **Import(**가져오기**)**를 클릭합니다.
확인 대화 상자가 열리면서 계속 진행할 것인지를 물어보고 섀시를 재시작해야 한다고 경고합니다.

d) **Yes(**예**)**를 클릭하여 지정된 구성 파일을 가져올 것임을 확인합니다.
기존의 구성이 삭제되고, 가져오기 파일에 지정된 구성이 Firepower 4100/9300 섀시에 적용됩니다. 가져오는 동안 Breakout 포트 구성이 변경되는 경우 Firepower 4100/9300 섀시를 다시 시작해야 합니다.

단계 **3** 원격 서버에 있는 구성 파일로부터 가져오려면:

a) **Remote(**원격**)**를 클릭합니다.
b) 원격 서버와의 통신에서 사용할 프로토콜을 선택합니다. FTP, TFTP, SCP, SFTP 중 하나일 수 있습니다.
c) 기본값 이외의 포트를 사용하려는 경우 **Port(**포트**)** 필드에 포트 번호를 입력합니다.
d) 백업 파일을 저장할 위치의 IP 주소 또는 호스트 이름을 입력합니다. 이는 Firepower 4100/9300 섀시가 네트워크를 통해 액세스할 수 있는 서버, 스토리지 어레이, 로컬 드라이브, 기타 읽기/쓰기 미디어일 수 있습니다.

   IP 주소가 아니라 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.

e) 시스템이 원격 서버에 로그인할 때 사용할 사용자 이름을 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.
f) 원격 서버 사용자 이름의 비밀번호를 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.
g) **File Path(**파일 경로**)** 필드에 설정 파일의 전체 경로(파일 이름 포함)를 입력합니다.
h) 사용할 원격 구성에 대해 **Import(**가져오기**)**.
확인 대화 상자가 열리면서 계속 진행할 것인지를 물어보고 섀시를 재시작해야 한다고 경고합니다.
i) **Yes(**예**)**를 클릭하여 지정된 구성 파일을 가져올 것임을 확인합니다.
기존의 구성이 삭제되고, 가져오기 파일에 지정된 구성이 Firepower 4100/9300 섀시에 적용됩니다. 가져오는 동안 Breakout 포트 구성이 변경되는 경우 Firepower 4100/9300 섀시를 다시 시작해야 합니다.

백업에서 **Threat Defense** 복원**: Threat Defense Virtual**

프라이빗 클라우드, 독립형, 고가용성 쌍 또는 클러스터에서 결함이 있거나 장애가 발생한 threat defense virtual 디바이스를 교체하려면 이 절차를 사용합니다.

threat defense 고가용성 및 클러스터링 구축에서는 이 절차를 사용하여 모든 피어를 교체할 수 있습니다. 모두 교체하려면 **restore** CLI 명령을 제외한 모든 디바이스에서 모든 단계를 동시에 수행합니다.

참고 네트워크에서 디바이스의 연결을 끊을 때도 management center에서 등록을 취소하지 마십시오. threat defense 고가용성 또는 클러스터링 구축에서는 고가용성 또는 클러스터링을 일시 중단하거나 중단하지 마십시오. 이러한 링크를 유지 관리하면 복구 후 교체 디바이스가 자동으로 다시 연결될 수 있습니다.

시작하기 전에

요구 사항, 지침, 제한 및 모범 사례를 읽고 이해해야 합니다. 어떤 단계도 건너 뛰거나 보안 문제를 무시하지 않습니다. 면밀하게 계획 및 준비를 하면 잘못된 단계 수행을 방지할 수 있습니다.

- 백업 및 복구 요구 사항, 467 페이지
- 백업 및 복원 지침 및 제한 사항, 468 페이지
- 백업 및 복구 모범 사례, 470 페이지

프로시저

단계 **1** 결함이 있는 디바이스의 성공적인 백업을 찾습니다.

클러스터링의 경우 노드 백업 파일은 클러스터의 단일 압축 파일(*cluster_name*.*timestamp*.**tar.gz**)에 번들로 제공됩니다. 노드를 복원하려면 먼저 개별 노드 백업 파일 (*node_name*_**control**_*timestamp*.**tar** 또는 *node_name*_**data**_*timestamp*.**tar**)을 추출해야 합니다.

백업 설정에 따라 다음 위치에 디바이스 백업이 저장될 수 있습니다.

- `/var/sf/backup`의 결함 있는 디바이스 자체
- `/var/sf/remote-backup`의 management center
- 원격 스토리지 위치

threat defense 고가용성 구축에서는 쌍을 유닛으로 백업하지만 백업 프로세스에서 고유한 백업 파일을 생성합니다. 디바이스의 역할은 백업 파일 이름에 표시됩니다.

백업의 유일한 복사본이 결함이 있는 디바이스에 있는 경우 지금 다른 위치에 복사합니다. 디바이스 이미지를 재설치하면 백업이 지워집니다. 다른 문제가 발생하면 백업을 복구하지 못할 수 있습니다. 자세한 내용은 백업 및 원격 스토리지 관리, 495 페이지를 참고하십시오.

교체 디바이스에는 백업이 필요하지만 복구 프로세스 중에 SCP를 사용하여 검색할 수 있습니다. 교체 디바이스에서 SCP가 액세스할 수 있는 위치에 백업을 배치하는 것이 좋습니다. 또는 교체 디바이스 자체에 백업을 복사할 수 있습니다.

단계 **2** 결함이 있는 디바이스를 제거합니다.

가상 시스템을 종료, 전원 끄기 및 삭제합니다. 절차는 가상 환경을 위한 설명서를 참조하십시오.

단계 **3** 교체 디바이스를 구축합니다.

단계 **4** 교체 디바이스에서 초기 설정을 수행합니다.

콘솔을 사용하여 관리자로 threat defense CLI에 액세스합니다. 설정 마법사에서 관리 IP 주소, 게이트웨이 및 기타 기본 네트워크 설정을 설정하라는 메시지를 표시합니다.

결함이 있는 디바이스와 동일한 관리 IP 주소를 설정하지 마십시오. 따라서 패치를 적용하기 위해 디바이스를 등록해야 하는 경우 문제가 발생할 수 있습니다. 복구 프로세스에서 관리 IP 주소가 올바르게 재설정됩니다.

참고 교체 디바이스를 패치해야 하는 경우 시작 가이드의 설명에 따라 management center 등록 프로세스를 시작합니다. 패치를 적용할 필요가 없으면 등록하지 마십시오.

단계 **5** 교체 디바이스가 결함이 있는 디바이스와 동일한 소프트웨어 버전(패치 포함)을 실행 중인지 확인합니다.

기존 디바이스를 management center에서 삭제해서는 안됩니다. 교체 디바이스는 물리적 네트워크에서 관리되지 않아야 하며 새 하드웨어와 교체 threat defense 패치의 버전이 동일해야 합니다. threat defense CLI에는 업그레이드 명령이 없습니다. 패치하려면 다음을 수행합니다.

a) management center 웹 인터페이스에서 디바이스 등록 프로세스를 완료합니다.

새 AC 정책을 생성하고 기본 작업인 "Network Discovery(네트워크 검색)"를 사용합니다. 이 정책은 그대로 유지합니다. 기능 또는 수정 사항을 추가하지 마십시오. 이는 디바이스를 등록하고 기능이 없는 정책을 구축하는 데 사용되므로 라이센스가 필요하지 않으며 디바이스를 패치할 수 있습니다. 백업이 복구되면 라이선싱 및 정책이 예상 상태로 복구됩니다.

b) 디바이스를 패치합니다: Cisco Firepower Management Center 업그레이드 설명서.

c) management center에서 새로 패치한 디바이스 등록을 취소합니다.

등록을 취소하지 않으면 복구 프로세스에서 "오래된" 디바이스가 다시 가동된 후 management center에 고스트 디바이스가 등록됩니다.

단계 **6** 교체 디바이스가 백업 파일에 액세스할 수 있는지 확인합니다.

복구 프로세스에서 SCP를 사용하여 백업을 검색할 수 있으므로 백업을 액세스 가능한 위치에 두는 것이 좋습니다. 또는 백업을 교체 디바이스 자체에 수동으로 `/var/sf/backup`에 복사할 수 있습니다. 클러스터링의 경우 기본 클러스터 번들에서 개별 노드 백업 파일을 추출했는지 확인합니다.

단계 **7** threat defense CLI에서 백업을 복구합니다.

관리자로 threat defense CLI에 액세스합니다. 콘솔을 사용하거나 새로 설정된 관리 인터페이스(IP 주소 또는 호스트 이름)에 SSH를 통해 연결할 수 있습니다. 복구 프로세스에서 이 IP 주소가 변경됩니다.

복구하려면 다음을 수행합니다.

- SCP 사용: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- 로컬 디바이스에서: **restore remote-manager-backup** *backup tar-file*

threat defense 고가용성 및 클러스터링 구축에서는 적절한 백업 파일(기본 대 보조 또는 제어 대 데이터)을 선택해야 합니다. 역할은 백업 파일 이름에 표시됩니다. 모든 디바이스를 복원하는 경우 순차적으로 수행합니다. 재부팅을 포함하여 첫 번째 디바이스에 대한 복구 프로세스가 완료될 때까지 다음 디바이스에서 **restore** 명령을 실행하지 마십시오.

단계 **8** management center에 로그인하고 교체 디바이스가 연결될 때까지 기다립니다.

복구가 완료되면 디바이스는 사용자를 CLI에서 로그아웃하고 재부팅하며 management center에 자동으로 연결합니다. 현재 디바이스가 오래된 것으로 표시됩니다.

단계 **9** 구축하기 전에 복구 후 작업을 수행하고 복구 후 문제를 해결합니다.

- 라이선싱 충돌 또는 고아 엔타이틀먼트를 해결합니다. Cisco TAC에 문의합니다.

- 모든 VPN 인증서를 다시 추가/다시 등록합니다. 복구 프로세스는 백업이 수행된 후 추가된 인증서를 포함하여 threat defense디바이스에서 VPN 인증서를 제거합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *VPN* 인증서 관리를 참조하십시오.

단계 **10** 설정을 구축합니다.

반드시 구축해야 합니다. 디바이스를 복원한 후에는 Device Management(디바이스 관리) 페이지에서 강제 구축해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 디바이스에 기존 구성을 재구축을 참조하십시오.

단계 **11** 데이터 인터페이스를 추가 및 설정합니다.

다음에 수행할 작업

복구가 성공했으며 교체 디바이스가 예상대로 트래픽을 전달하는지 확인합니다.

백업 및 원격 스토리지 관리

백업은 암호화되지 않은 아카이브(.tar) 파일로 저장됩니다. 파일 이름에는 다음을 포함할 수 있는 식별 정보가 포함됩니다.

- 백업 프로파일 또는 백업과 연결된 예약된 작업의 이름입니다.
- 백업된 어플라이언스의 표시 이름 또는 IP 주소입니다.
- 어플라이언스의 역할(예: HA 쌍의 멤버).

어플라이언스를 안전한 원격 위치에 백업하고 전송 성공을 확인하는 것이 좋습니다. 어플라이언스에 남아 있는 백업은 수동으로 또는 업그레이드 프로세스에 의해 삭제될 수 있습니다. 업그레이드는 로컬에 저장된 백업을 제거합니다. 옵션에 대한 자세한 내용은 백업 스토리지 위치, 497 페이지의 내용을 참조하십시오.

주의 특히 백업 파일은 암호화되지 않으므로 무단 액세스를 허용하지 않습니다. 백업 파일이 수정되면 복원 프로세스가 실패하게 됩니다. Admin/Maint(관리/유지 관리) 역할의 사용자는 원격 스토리지에서 파일을 이동하고 삭제할 수 있는 백업 관리 페이지에 액세스할 수 있습니다.

다음 절차에서는 백업 파일을 관리하는 방법을 설명합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Backup/Restore(**백업/복구**)**을(를) 선택합니다.

Backup Management(백업 관리) 페이지에 사용 가능한 백업이 나열됩니다. 또한 백업을 저장하는 데 사용할 수 있는 디스크 공간의 양도 나열합니다. 공간이 충분하지 않으면 백업이 실패할 수 있습니다.

단계 **2** 다음 중 하나를 수행합니다.

표 ***41:*** 원격 스토리지 및 백업 파일 관리

변경 후	수행해야 할 작업
FMC 시스템 설정을 편집할 필요 없이 백업을 위한 원격 스토리지를 활성화하거나 비활성화합니다.	**Enable Remote Storage for Backups(**백업에 원격 스토리지 활성화**)**를 클릭합니다. 이 옵션은 원격 스토리지를 설정한 후에만 나타납니다. 여기에서 토글하면 시스템 설정 (**System(**시스템**) > Configuration(**설정**) > Remote Storage Device(**원격 스토리지 디바이스**))**에서도 토글됩니다. 팁 원격 스토리지 설정에 빠르게 액세스하려면 Backup Management(백업 관리) 페이지의 오른쪽 위에 있는 **Remote Storage(**원격 스토리지**)**를 클릭합니다. 참고 원격 스토리지 위치에 백업을 저장하려면 Retrieve to Management Center(Management Center로 검색) 옵션도 활성화해야 합니다(참조).Management Center에서 디바이스 백업, 476 페이지
FMC와 원격 스토리지 위치 간에 파일을 이동합니다.	**Move(**이동**)**를 클릭합니다. 원하는 만큼 파일을 앞뒤로 이동할 수 있습니다. 이렇게 하면 현재 위치에서 파일이 복사되지 않고 삭제됩니다. 백업 파일을 원격 스토리지에서 FMC로 이동할 때 FMC에 저장되는 위치는 백업의 종류에 따라 달라집니다. • FMC 백업: `/var/sf/backup` • 디바이스 백업: `/var/sf/remote-backup`
백업의 내용을 봅니다.	백업 파일을 클릭합니다.
백업 파일을 삭제합니다.	백업 파일을 선택하고 **Delete(**삭제**)**를 클릭합니다. 로컬 및 원격에 저장된 백업 파일을 모두 삭제할 수 있습니다.
컴퓨터에서 연락처 파일을 업로드합니다.	**Upload Backup(**백업 업로드**)**을 클릭하고 백업 파일을 선택한 다음 **Upload Backup(**백업 업로드**)**을 다시 클릭합니다.
백업을 컴퓨터에 다운로드합니다.	백업 파일을 선택하고 **Download(**다운로드**)**를 클릭합니다. 백업 파일을 이동하는 것과 달리 FMC에서 백업을 삭제하지 않습니다.

백업 스토리지 위치

다음 표에서는 management center 및 매니지드 디바이스의 백업 스토리지 옵션에 대해 설명합니다.

표 *42:* 백업 스토리지 위치

위치	세부 정보
원격(네트워크 볼륨(NFS, SMB, SSHFS) 마운트를 통해)	참고 원격 스토리지를 구성하고 **Retrieve to Management Center(**관리 센터로 검색**)** 옵션을 활성화한 경우에만 원격 스토리지 위치에 백업이 저장됩니다(Management Center에서 디바이스 백업, 476 페이지 참조). management center의 시스템 설정에서 NFS, SMB 또는 SSHFS 네트워크 볼륨을 management center 및 디바이스 백업용 원격 스토리지로 마운트할 수 있습니다. 원격 스토리지 디바이스, 95 페이지의 내용을 참조하십시오.) 이렇게 하면 모든 후속 management center 백업 및 *management center*시작 디바이스 백업이 해당 볼륨에 복사되지만, 계속해서 management center를 사용하여 관리할 수 있습니다(복구, 다운로드, 업로드, 삭제, 이동). management center만 네트워크 볼륨을 마운트합니다. 매니지드 디바이스 백업 파일은 management center를 통해 라우팅됩니다. management center와 해당 디바이스 간에 대량 데이터 전송을 수행할 수 있는 대역폭이 있는지 확인합니다. 자세한 내용은 Firepower Management Center에서 매니지드 디바이스로 데이터를 다운로드하기 위한 지침(문제 해결 TechNote)을 참조하십시오.

위치	세부 정보
원격(복사를 통해)(SCP)	참고 원격 스토리지를 구성하고 **Retrieve to Management Center(**관리 센터로 검색**)** 옵션을 활성화한 경우에만 원격 스토리지 위치에 백업이 저장됩니다(Management Center에서 디바이스 백업, 476 페이지 참조). management center의 경우, **Copy when complete(**완료 시 복사**)** 옵션을 사용하여 완료된 백업을 원격 서버에 안전하게 복사(SCP)할 수 있습니다. 네트워크 볼륨을 마운트하여 원격 스토리지와 비교할 때 **Copy when complete(**완료 시 복사**)**는 NFS 또는 SMB 볼륨에 복사할 수 없습니다. CLI 옵션을 제공하거나 디스크 공간 임계값을 설정할 수 없으며, 보고서의 원격 스토리지에는 영향을 주지 않습니다. 또한 백업 파일을 복사한 후에는 관리할 수 없습니다. 이 옵션은 백업을 로컬에 저장하고 SCP를 원격 위치에 저장하려는 경우 유용합니다. 참고 management center 시스템 설정에서 SSHFS 원격 스토리지를 설정하는 경우, **Copy when complete(**완료 시 복사**)**를 사용하여 동일한 디렉토리에 백업 파일을 복사하지 마십시오.
로컬, management center에 있음.	네트워크 볼륨을 마운트하여 원격 스토리지를 설정하지 않은 경우, management center에 백업 파일을 저장할 수 있습니다. • management center 백업은 `/var/sf/backup`에 저장됩니다. • 백업을 수행할 때 **Retrieve to Management Center(**관리 센터로 가져오기**)** 옵션을 활성화하면 디바이스 백업이 management center의 `/var/sf/remote-backup`에 저장됩니다.
로컬, 디바이스 내부 플래시 메모리.	디바이스 백업 파일은 다음의 경우 디바이스의 `/var/sf/backup`에 저장됩니다. • 네트워크 볼륨을 마운트하여 원격 스토리지를 설정하지 마십시오. • **Retrieve to Management Center(Management Center**로 검색**)**를 활성화하지 마십시오.
로컬, 디바이스 SD 카드.	ISA 3000의 경우, 디바이스를 로컬 `/var/sf/backup` 내부 플래시 메모리 위치에 백업할 때 SD 카드가 설치되어 있으면 제로 터치 복원에 사용할 수 있도록 백업이 `/mnt/disk3/backup/`에 있는 SD 카드에 자동으로 복사됩니다.

백업 및 복원 기록

기능	버전	세부정보
클러스터의 백업 및 복원 지원	7.3	이제 management center를 사용하여 클러스터의 백업을 수행할 수 있습니다. 클러스터 노드를 복원하려면 디바이스 CLI를 사용해야 합니다. 신규/수정된 화면: **System(**시스템**)** > **Tools(**도구**)** > **Backup/Restore(**백업/복원**)** > **Managed Device Backup(**매니지드 디바이스 백업**)** 신규/수정된 명령: **restore remote-manager-backup** 참고 가상 방화벽의 경우 클러스터의 백업 및 복원은 VMware에서만 지원됩니다.
SD 카드를 사용한 ISA 3000의 제로 터치 복구	7.0	로컬 백업을 수행하면 백업 파일이 SD 카드에 복사됩니다(있는 경우). 교체 디바이스에서 구성을 복원하려면 새 디바이스에 SD 카드를 설치하고 디바이스가 부팅되는 동안 Reset(재설정) 버튼을 3~15초 동안 누릅니다.
threat defense 컨테이너 인스턴스의 백업 및 복원 지원	6.7	이제 management center를 사용하여 Firepower 4100/9300에서 threat defense 컨테이너 인스턴스의 온디맨드 원격 백업을 수행할 수 있습니다.
복원을 위한 VDB 요구 사항	6.6	백업에서 management center를 복원하면 기존 VDB가 백업 파일의 VDB로 대체됩니다. 복원하기 전에 VDB 버전을 더 이상 일치시킬 필요가 없습니다.
자동으로 예약된 백업	6.5	신규 또는 이미지가 재설치된 management center의 경우, 설정 프로세스는 management center 구성을 백업하고 로컬에 저장하기 위해 매주 예약된 작업을 생성합니다.
매니지드 디바이스의 온디맨드 원격 백업	6.3	이제 management center를 사용하여 특정 매니지드 디바이스의 온디맨드 원격 백업을 수행할 수 있습니다. 지원되는 플랫폼은 백업 및 복구 요구 사항, 467 페이지의 내용을 참고하십시오. 신규/수정된 화면: **System(**시스템**) > Tools(**도구**) > Backup/Restore(**백업/복원**) > Managed Device Backup(**매니지드 디바이스 백업**)** 신규/수정된 threat defense CLI 명령: **restore**

16 장

일정

다음 항목에서는 작업을 예약하는 방법에 대해 설명합니다.

작업 예약 관련 정보

다양한 작업이 한 번에 또는 주기적으로 지정된 시간에 실행되도록 일정을 관리할 수 있습니다.

이런 작업은 백엔드에서 UTC 기준으로 예약되므로, 사용자가 있는 위치와 날짜에 따라 지역적으로 실행됩니다. 또한 작업은 UTC 기준으로 예약되기 때문에 일광 절약 시간, 서머 타임 또는 사용자 위치에서 발생할 수 있는 계절 조정의 영향을 받지 않습니다. 영향을 받을 경우 예약된 작업은 현지 시간에 따라 여름에는 겨울보다 1시간 '늦게' 실행됩니다.

일부 작업은 초기 설정 프로세스에서 자동으로 예약되거나 수행됩니다.

- 최신 VDB를 다운로드하고 설치하는 일회성 작업입니다.
- 사용 가능한 최신 소프트웨어 업데이트 및 VDB를 다운로드하기 위해 매주 예약된 작업입니다.
- 로컬에 저장된 management center의 구성 전용 백업을 수행하는 매주 예약된 작업입니다.

주간 작업을 검토하고 필요한 경우 조정해야 합니다. 선택적으로, 실제로 VDB 및/또는 소프트웨어를 업데이트하고 구성을 구축하기 위해 새로운 반복 작업을 예약합니다.

중요 예약된 작업이 의도한 시점에 수행되는지 확인하기를 적극 권장합니다. (자동화된 소프트웨어 업데이트를 포함하는 작업 또는 매니지드 디바이스에 업데이트를 푸시해야 하는 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. 구성 구축과 같은 다른 작업으로 인해 트래픽이 중단될 수 있습니다. 유지 보수 기간에 이와 같은 작업을 예약해야 합니다.

작업 스케줄링 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 유지 보수 사용자

반복 작업 구성

모든 유형의 작업에 동일한 프로세스를 사용하여 반복 작업의 빈도를 설정합니다.

웹 인터페이스에서 대부분의 페이지에 표시되는 시간은 로컬 시간입니다. 이 시간은 로컬 구성에서 지정하는 표준 시간대를 사용하여 결정됩니다. 또한 management center은 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.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)** 드롭다운 목록에서 일정을 예약할 작업 유형을 선택합니다.

단계 **4** **Schedule tast to run(**실행 작업 예약**)** 옵션 옆에 있는 **Recurring(**반복**)**을 클릭합니다.

단계 **5** **Start On(**착수 일자**)** 필드에서 반복 작업을 시작할 날짜를 지정합니다.

단계 **6** **Repeat Every(**반복 빈도**)** 필드에서 작업의 반복 빈도를 지정합니다.

숫자를 입력하거나 **Up(**가동**)** (▲) 및 **Down(**중단**)** (▼)을 클릭하여 간격을 지정할 수 있습니다. 예를 들어 이틀마다 작업을 실행하려면 2를 입력하고 **Days(**일**)**를 클릭합니다.

단계 **7** **Run At(**착수 시간**)** 필드에서 반복 작업을 시작할 시간을 지정합니다.

단계 **8** 작업을 매주 또는 매월 실행하려면 **Repeat On(**반복 실행일**)** 필드에서 작업을 실행하려는 요일을 선택합니다.

단계 **9** 생성하려는 작업 유형에 대한 나머지 옵션을 선택합니다.

- 백업 - Management Center 백업 예약, 503 페이지에 설명된 대로 백업 작업을 예약합니다.
- CRL 다운로드 - CRL(Certificate Revocation List) 다운로드 구성, 505 페이지에 설명된 대로 인증서 해지 목록 다운로드를 예약합니다.
- 정책 구축 - 정책 구축 자동화, 506 페이지에 설명된 대로 정책 구축을 예약합니다.
- Nmap 스캔 - Nmap 스캔 예약, 508 페이지에 설명된 대로 Nmap 스캔을 예약합니다.
- 보고 - 설명된 대로 보고서 생성을 예약합니다. 보고서 생성 자동화, 509 페이지
- Cisco 권장 규칙 - Cisco 추천 자동화, 511 페이지에 설명된 대로 Cisco 권장 규칙 자동 업데이트를 예약합니다.
- 최신 업데이트 다운로드 - 소프트웨어 다운로드 자동화, 512 페이지 또는 VDB 업데이트 다운로드 자동화, 515 페이지에 설명된 대로 소프트웨어 또는 VDB 업데이트 다운로드를 예약합니다.
- 최신 업데이트 설치 - 소프트웨어 설치 자동화, 514 페이지 또는VDB 업데이트 설치 자동화, 516 페이지에 설명된 대로 Secure Firewall Management Center 또는 매니지드 디바이스에 소프트웨어 또는 VDB 업데이트 설치를 예약합니다.
- 최신 업데이트 푸시 - 소프트웨어 푸시 자동화, 513 페이지에 설명된 매니지드 디바이스에 대한 소프트웨어 업데이트 푸시를 예약합니다.
- URL 필터링 데이터베이스 업데이트 - 설명된 대로 URL 필터링 데이터 자동 업데이트를 예약합니다. 예약된 작업을 통해 URL 필터링 업데이트 자동화, 517 페이지

단계 **10** **Save(**저장**)**를 클릭합니다.

예약 백업

Secure Firewall Management Center의 스케줄러를 사용하면 자체 백업을 자동화할 수 있습니다. management center에서의 원격 디바이스 백업은 예약할 수 없습니다. 백업에 대한 자세한 내용은 백업/복구, 465 페이지의 내용을 참조하십시오.

원격 백업을 지원하지 않는 디바이스도 있습니다.

Management Center 백업 예약

management center의 스케줄러를 사용하면 management center와 디바이스 백업 모두를 자동화할 수 있습니다. 원격 백업을 지원하지 않는 디바이스도 있습니다. 자세한 내용은 백업/복구, 465 페이지를 참고하십시오.

참고 시스템은 초기 구성의 일부로 구성 전용 management center 백업(로컬로 저장)을 매주 예약합니다. 이 작업을 검토하고 필요한 경우 이 주제.

시작하기 전에

백업 기본 설정을 지정하는 백업 프로 파일을 생성합니다. 백업 프로파일 생성, 478 페이지의 내용을 참조하십시오.

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을(를) 선택합니다.

단계 **2** **Job Type** 목록에서 **Backup**을 선택합니다.

단계 **3** 백업을 한 번할지 반복 실행할지를 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업 관련 정보는 반복 작업 구성, 502 페이지의 내용을 참조하십시오.

단계 **4** 작업 이름을 입력합니다.

단계 **5** **Backup Type(**백업 유형**)**으로 **Management Center(**관리 센터**)**를 클릭합니다.

단계 **6** **Backup Profile(**백업 프로파일**)**을 선택합니다.

단계 **7** (선택 사항) **Comment(**코멘트**)**를 입력합니다.

코멘트를 간략하게 합니다. 코멘트는 schedule calendar(일정 달력) 페이지의 Task Details(작업 정보) 섹션에 나타납니다.

단계 **8** (선택 사항) **Email Status To:(**다음에 대한 이메일 상태**)** 필드에 이메일 주소 또는 쉼표로 구분된 이메일 주소 목록을 입력합니다.

작업 상태 메시지를 전송하도록 이메일 릴레이 서버를 설정하는 방법은 메일 릴레이 호스트 및 알림 주소 구성, 62 페이지의 내용을 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.

원격 디바이스 백업 예약

management center의 스케줄러를 사용하면 management center와 디바이스 백업 모두를 자동화할 수 있습니다. 원격 백업을 지원하지 않는 디바이스도 있습니다. 자세한 내용은 백업/복구, 465 페이지을 참조하십시오.

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을(를) 선택합니다.

단계 **2** **Job Type** 목록에서 **Backup**을 선택합니다.

단계 **3** 백업을 한 번할지 반복 실행할지를 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업 관련 정보는 반복 작업 구성, 502 페이지의 내용을 참조하십시오.

단계 **4** 작업 이름을 입력합니다.

단계 **5** **Backup Type(**백업 유형**)**으로 **Device(**디바이스**)**를 클릭합니다.

단계 **6** 하나 이상의 디바이스를 선택합니다.

목록에 없는 디바이스는 원격 백업을 지원하지 않습니다.

단계 **7** 백업용 원격 스토리지를 설정하지 않은 경우, **Management Center**로 검색할지 여부를 선택합니다.

- 활성화됨(기본값): `/var/sf/remote-backup/`에 있는 management center에 백업을 저장합니다.
- Disabled(비활성화됨)(기본값): `/var/sf/backup`의 디바이스에 백업을 저장합니다.

원격 백업 스토리지를 구성하면 백업 파일은 원격으로 저장되며 이 옵션은 적용되지 않습니다.자세한 내용은 백업 및 원격 스토리지 관리, 495 페이지를 참조하십시오.

단계 **8** (선택 사항) **Comment(**코멘트**)**를 입력합니다.

코멘트를 간략하게 합니다. 코멘트는 schedule calendar(일정 달력) 페이지의 Task Details(작업 정보) 섹션에 나타납니다.

단계 **9** (선택 사항) **Email Status To:(**다음에 대한 이메일 상태**)** 필드에 이메일 주소 또는 쉼표로 구분된 이메일 주소 목록을 입력합니다.

작업 상태 메시지를 전송하도록 이메일 릴레이 서버를 설정하는 방법은 메일 릴레이 호스트 및 알림 주소 구성, 62 페이지의 내용을 참조하십시오.

단계 **10** **Save(**저장**)**를 클릭합니다.

CRL(Certificate Revocation List) 다운로드 구성

management center에 대한 로컬 웹 인터페이스를 사용하여 이 절차를 수행해야 합니다. 다중 도메인 구축에서 이 작업은 management center에 대해 전역 도메인에서만 지원됩니다.

사용자가 어플라이언스에 대한 사용자 인증서 또는 감사 로그 인증서를 사용하는 어플라이언스의 로컬 구성에서 CRL(인증서 해지 목록) 다운로드를 활성화하는 경우, 시스템에서 자동으로 CRL 다운로드 작업을 생성합니다. 스케줄러를 사용하여 작업을 편집하고 업데이트 빈도를 설정할 수 있습니다.

시작하기 전에

- 사용자 인증서 또는 감사 로그 인증서를 활성화 및 구성하고, 하나 이상의 CRL 다운로드 URL을 설정합니다. 자세한 내용은 유효한 HTTPS 클라이언트 인증서 필요, 71 페이지 및 유효한 감사 로그 서버 인증서 필요, 54 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)**에서 **Download CRL(CRL** 다운로드**)**을 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 CRL 다운로드를 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **7** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 management center에 구성된 유효한 이메일 릴레이 서버가 있어야 합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

정책 구축 자동화

management center에서 구성 설정을 수정한 후, 영향을 받는 디바이스에 해당 변경 사항을 구축해야 합니다.

다중 도메인 구축에서, 현재 도메인에 대해서만 정책 구축을 예약할 수 있습니다.

⚠

주의 구축 시 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. Snort 재시작 트래픽 동작 및 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션을 참조하십시오.

프로시저

단계 1 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 2 **Add Task(**작업 추가**)**를 클릭합니다.

단계 3 **Job Type(**작업 유형**)**에서 **Deploy Policies(**정책 구축**)**를 선택합니다.

단계 4 **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 5 **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 6 **Device(**디바이스**)** 필드에서 정책을 구축하려는 디바이스를 선택합니다.

단계 7 필요에 따라 **Skip deployment for up-to-date devices(**최신 디바이스에 대한 구축 건너뛰기**)** 확인란을 선택하거나 선택 취소합니다.

기본적으로 **Skip deployment for up-to-date devices(**최신 디바이스에 대한 구축 건너뛰기**)** 옵션이 활성화되어 정책 구축 프로세스에서 성능을 향상시킵니다.

참고 시스템은 Firepower Management Center 웹 인터페이스에서 시작된 정책 배포가 진행 중인 경우 예약된 정책 구축 작업을 수행하지 않습니다. 따라서 예약된 정책 배포 작업이 진행 중인 경우, 시스템은 웹 인터페이스에서 정책 구축을 시작할 수 없습니다.

단계 8 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 9 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 10 **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 62 페이지
만료된 정책

Nmap 스캔 자동화

네트워크에 있는 대상에 대해 정기적인 Nmap 스캔을 예약할 수 있습니다. 스캔을 자동화하면 Nmap 스캔에서 전에 제공한 정보를 새로 고칠 수 있습니다. Firepower System이 Nmap 제공 데이터를 업데이트할 수 없으므로 데이터를 최신 상태로 유지하려면 정기적으로 다시 스캔해야 합니다. 네트워크의 호스트에서 식별되지 않은 애플리케이션이나 서버를 자동으로 테스트하도록 스캔을 예약할 수도 있습니다.

Discovery Administrator(검색 관리자)는 Nmap 스캔을 교정으로서 사용할 수도 있습니다. 예를 들어, 호스트에서 운영 체제 충돌이 발생하면 해당 충돌이 Nmap 스캔을 트리거할 수 있습니다. 스캔을 실행하면 호스트에 대한 업데이트된 운영 체제 정보를 얻게 되며, 이를 통해 충돌이 해결됩니다.

이전에 Nmap 검색 기능을 사용하지 않은 경우, 예약 검색을 정의하기 전에 Nmap 검색을 구성합니다.

관련 항목

Nmap 스캐닝

Nmap 스캔 예약

시스템에서 탐지된 호스트의 운영 체제, 애플리케이션 또는 서버가 Nmap 스캔 결과와 교체되면, 시스템은 호스트에 대해 Nmap에 의해 교체된 정보를 더 이상 업데이트하지 않습니다. Nmap 제공 서비스 및 운영 체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트를 스캔하려는 경우 Nmap 제공 운영 체제, 애플리케이션 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다. 호스트가 네트워크 맵에서 삭제된 후 다시 추가된 경우, Nmap 스캔 결과가 삭제되며 시스템은 호스트에 대한 모든 운영 체제 및 서비스 데이터의 모니터링을 다시 시작합니다.

다중 도메인 구축의 경우:

- 현재 도메인에 대해서만 스캔을 예약할 수 있습니다.
- 선택된 교정 및 Nmap 대상은 현재 도메인 또는 상위 도메인에 존재해야 합니다.
- 리프 도메인이 아닌 도메인에서 Nmap 스캔을 수행하도록 선택하면 해당 도메인의 각 하위 노드에서 동일한 대상을 검색합니다

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)**에서 **Nmap Scan(Nmap** 스캔**)**을 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **map Remediation(Nmap** 교정**)**필드에서 Nmap 교정을 선택합니다.

단계 **7** **Nmap Target(Nmap** 대상**)** 필드에서 스캔 대상을 선택합니다.

단계 **8** **Domain(**도메인**)** 필드에서 네트워크 맵을 보강하려는 도메인을 선택합니다.

단계 **9** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

팁 코멘트 필드는 calendar schedule(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **10** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

보고서 생성 자동화

일정한 간격으로 실행되도록 보고를 자동화할 수 있습니다.

다중 도메인 구축에서, 현재 도메인에 대해서만 보고를 예약할 수 있습니다.

시작하기 전에

- 위험 보고 이외의 보고: 보고서 템플릿을 생성합니다. 자세한 내용은 보고서 템플릿, 542 페이지를 참조하십시오.
- 스케줄러를 사용하여 이메일 보고를 배포하려는 경우, 메일 릴레이 호스트를 구성하고 보고 수신자와 메시지 정보를 지정하십시오. 메일 릴레이 호스트 및 알림 주소 구성, 62 페이지 및 (위험 보고 이외의 보고) 생성 시 이메일로 보고서 배포, 564 페이지또는 (위험 보고) 위험 보고서 생성, 보기 및 인쇄, 540 페이지를 참조하십시오.
- (선택 사항) 예약된 보고의 파일 이름, 출력 형식, 기간 또는 이메일 배포 설정을 설정하거나 변경합니다. 예약된 보고서에 대한 보고서 생성 설정 지정, 510 페이지의 내용을 참조하십시오.
- 보고서 출력 형식으로 PDF를 선택하는 경우, 보고서 템플릿을 확인하고 템플릿 각 섹션에 있는 결과 수가 PDF 제한을 초과하지 않는지 확인하십시오. 자세한 내용은 보고서 템플릿 필드, 542 페이지 섹션을 참조해 주십시오.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)** 목록에서 **Report(**보고**)**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Report Template(**보고서 템플릿**)** 필드에서 risk report(위험 보고) 또는 report template(보고서 템플릿)을 선택합니다.

단계 **7** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **8** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

참고 이 옵션을 구성해도 보고가 배포되지는 않습니다.

단계 **9** 보고서에 데이터가 없는 경우(예: 보고서 기간에 특정 유형의 이벤트가 발생하지 않은 경우) 보고서 이메일 첨부 파일을 수신하지 않으려면 **If report is empty, still attach to email(**보고서가 비어 있는 경우에도 이메일에 첨부**)** 확인란을 선택합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

예약된 보고서에 대한 보고서 생성 설정 지정

이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

지정하거나 파일 이름, 출력 형식, 타임 윈도우를 변경하거나 예약된 보고서의 메일 설정을 이메일:

프로시저

단계 **1** 선택 **Overview(**개요**) > Reporting(**보고**) > Report Templates(**보고서 템플릿**)**을 선택합니다.

단계 **2** 변경하려는 보고서 템플릿에 대한 **Edit(**편집**)**을 클릭합니다.

단계 **3** PDF 출력을 선택합니다.

a) 결과 수가 옆의 노란색 삼각형 표시 보고서에서 섹션의 여부를 확인합니다.
b) PDF 출력에 대한 해당 섹션에 대한 허용된 결과의 최대 수를 보려면 삼각형 위에 마우스로 모든 노란색 삼각형을 표시합니다.
c) 노란색 삼각형이 있는 각 섹션에 대한 제한된 수의 결과 수를 줄입니다.
d) 더 이상 노란색 삼각형이 없는 경우 저장을 클릭 합니다.

단계 **4** **Generate(**생성**)**를 클릭합니다.

참고 이제 보고서를 생성하지 않고 보고서 생성 설정을 변경하려는 경우에 템플릿 구성 페이지에서 생성을 클릭해야 합니다. 보고서를 생성하지 않는 한 템플릿 목록 보기에서 생성을 클릭하는 경우 변경 사항은 저장되지 않습니다.

단계 **5** 설정을 수정합니다.

단계 **6** 보고서를 생성하지 않고 새 설정을 저장하려면 **Cancel (**취소**)**을 클릭합니다.

새 설정을 저장하고 보고서를 생성하려면 **Generate(**생성**)**를 클릭하고 이 절차의 나머지를 건너뛰고 합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** 변경 하지 않은 경우에 저장 하 라는 프롬프트가 표시 되 면 **OK(**확인**)**를클릭 합니다.

Cisco 추천 자동화

사용자 지정 침입 정책에서 가장 최근에 저장된 구성 설정을 사용하여 네트워크에 대한 네트워크 검색 데이터를 기반으로 규칙 상태 권장 사항을 자동으로 생성할 수 있습니다.

참고 저장되지 않은 변경 사항이 있는 침입 정책에 대해 시스템이 예약 권장 사항을 자동으로 생성하는 경우, 자동으로 생성된 권장 사항을 규칙에 반영하려면 해당 정책에서 변경 사항을 취소하고 정책을 커밋해야 합니다.

작업이 실행되면 시스템에서 권장되는 규칙 상태를 자동으로 생성하고 정책 구성에 따라 침입 규칙의 상태를 수정합니다. 다음에 침입 정책을 구축할 때 수정된 규칙 상태가 반영됩니다.

다중 도메인 구축에서 현재 도메인 수준의 침입 정책 권장 사항을 자동화 할 수 있습니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우 상위 도메인의 침입 정책에서 이 기능을 활성화하면 모든 하위 리프 도메인의 데이터를 사용하여 권장 사항이 생성됩니다. 이로 인해 일부 리프 도메인에는 없는 자산에 맞게 조정된 침입 규칙이 활성화되어 성능에 영향을 줄 수 있습니다.

시작하기 전에

- Cisco Secure Firewall Management Center 디바이스 구성 가이드에 설명된 대로 침입 정책에서 Cisco 권장 규칙을 구성합니다.
- 작업 상태 메시지가 이메일 하려는 경우 유효한 이메일 릴레이 서버를 구성 합니다.
- 권장 사항을 생성하려면 IPS 스마트 라이선스 또는 보호 클래식 라이선스가 있어야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)**에서 **Cisco Recommended Rules(Cisco** 권장 규칙**)**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Policies(**정책**)** 옆에서 권장 사항을 생성하려는 침입 정책을 하나 이상 선택합니다. 모든 침입 정책을 선택하려면 **All Policies(**모든 정책**)** 확인란을 선택합니다.

단계 **7** (선택 사항) **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트를 간략하게 합니다. 코멘트는 schedule calendar(일정 달력) 페이지의 Task Details(작업 정보) 섹션에 나타납니다.

단계 **8** (선택 사항) 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

관련 항목

충돌 및 변경: 네트워크 분석 및 침입 정책
Cisco 권장 규칙 정보
메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

소프트웨어 업그레이드 자동화

자동으로 유지 보수 릴리스와 패치를 적용할 수 있습니다.

management center를 업그레이드하려면 다운로드 및 설치 작업을 예약합니다. 매니지드 디바이스를 업그레이드하려면 다운로드, 푸시 및 설치 작업을 예약합니다. 작업 사이에 적절한 시간을 두어야 합니다. 예를 들어, 푸시가 아직 실행 중인 동안 수행하도록 예약된 설치는 실패합니다.

이 기능은 주요 릴리스에서는 지원되지 않습니다. 업그레이드 패키지를 다운로드하려면 인터넷 액세스가 필요합니다. 디바이스 그룹에 대한 업그레이드를 예약하는 경우 그룹화된 모든 디바이스에서 업그레이드가 동시에 실행됩니다.

참고 시스템은 초기 구성의 일부로 새로 사용 가능한 업그레이드와 최신 VDB의 다운로드를 매주 예약합니다. 이 작업을 검토하고 필요한 경우 소프트웨어 다운로드 자동화, 512 페이지. 이 작업은 업데이트만 다운로드합니다. 이 작업으로 다운로드하는 업데이트의 설치는 사용자의 책임입니다.

관련 항목

관리 인터페이스, 75 페이지
업데이트, 231 페이지

소프트웨어 다운로드 자동화

이 절차를 사용하여 일부 패치 및 유지 보수 릴리스의 패치 다운로드를 예약합니다. 전역 도메인에 있어야 합니다.

시작하기 전에

management center이 인터넷에 액세스할 수 있는지 확인합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type** 목록에서 **Download Latest Update**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Update Items(**업데이트 항목**)**옆에 있는 **Software(**소프트웨어**)** 체크 박스를 선택합니다.

단계 **7** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **8** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

소프트웨어 푸시 자동화

매니지드 디바이스에서 소프트웨어 업데이트의 설치를 자동화하려면 설치 전에 디바이스에 업데이트를 푸시해야 합니다.

매니지드 디바이스에 소프트웨어 업데이트를 푸시하기 위한 작업을 생성하는 경우, 디바이스에 업데이트를 복사할 수 있도록 푸시 작업과 예약 설치 작업 사이에 충분한 시간을 두어야 합니다.

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)** 목록에서 **Push Latest Update(**최신 업데이트 푸시**)**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.

- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Device(**디바이스**)** 드롭다운 목록에서 업데이트할 디바이스를 선택합니다.

단계 **7** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **8** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

소프트웨어 설치 자동화

업데이트를 매니지드 디바이스에 푸시하는 작업과 업데이트를 설치하는 작업 사이에 충분한 시간을 두어야 합니다.

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

주의 설치되고 있는 업데이트에 따라, 소프트웨어가 설치된 후 어플라이언스가 재부팅될 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type** 목록에서 **Install Latest Update**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Device(**디바이스**)** 드롭다운 목록에서 업데이트를 설치하려는 어플라이언스(management center 포함)를 선택합니다.

단계 **7** **Update Items(**업데이트 항목**)**옆에 있는 **Software(**소프트웨어**)** 확인란을 선택합니다.

단계 **8** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **9** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

취약성 데이터베이스 업데이트 자동화

예약 기능을 사용하여 VDB(Cisco 취약성 데이터베이스)를 업데이트할 수 있으며 이를 통해 최신 정보를 사용하여 네트워크의 호스트를 평가할 수 있습니다. 다운로드, 설치 및 후속 구축을 별도의 작업으로 예약하여 작업 간에 충분한 시간을 확보해야 합니다.

참고 management center의 초기 설정에서는 일회성 작업으로 Cisco에서 최신 VDB를 자동으로 다운로드하여 설치합니다. 또한 최신 VDB를 포함하여 사용 가능한 최신 소프트웨어 업데이트를 다운로드하는 매주 작업을 예약합니다. 이 주간 작업을 검토하고 필요한 경우 조정하는 것이 좋습니다. 선택적으로, 새로운 주간 작업을 예약하여 실제로 VDB를 업데이트하고 구성을 구축합니다.

관련 항목

관리 인터페이스, 75 페이지

VDB 업데이트 다운로드 자동화

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

시작하기 전에

management center에서 인터넷에 액세스할 수 있는지 확인합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type** 목록에서 **Download Latest Update**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Update Items(**업데이트 항목**)**옆에 있는 **Vulnerability Database(**취약성 데이터베이스**)** 확인란을 선택합니다.

단계 **7** (선택 사항) **Comment(**코멘트**)** 필드에 간단한 코멘트를 입력합니다.

단계 **8** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

VDB 업데이트 설치 자동화

VDB 업데이트를 다운로드하는 작업과 업데이트를 설치하는 작업 사이에 충분한 시간을 두십시오.

이 작업을 수행하려면 전역 도메인에 있어야 합니다.

주의 대부분의 경우 VDB 업데이트 후 첫 번째 구축은 Snort 프로세스를 재시작하여 트래픽 검사를 중단합니다. 이러한 상황이 발생하면 시스템에서 사용자에게 경고합니다(업데이트된 애플리케이션 탐지기 및 운영 체제 핑거프린트는 재시작이 필요하지만 취약성 정보는 그렇지 않음). 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작를 참조하십시오.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type** 목록에서 **Install Latest Update**를 선택합니다.

단계 **4** **Once(**한 번에**)** 또는 **Recurring(**반복**)** 중에서 작업을 예약할 방식을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** **Device(**디바이스**)** 드롭다운 목록에서 management center를 선택합니다.

단계 **7** **Update Items(**업데이트 항목**)**옆에 있는 **Vulnerability Database(**취약성 데이터베이스**)** 확인란을 선택합니다.

단계 **8** (선택 사항) **Comment(**코멘트**)** 필드에 간단한 코멘트를 입력합니다.

단계 **9** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

예약된 작업을 통해 URL 필터링 업데이트 자동화

URL 필터링을 위한 위협 데이터를 최신 상태로 유지하려면 시스템이 Cisco 종합적 보안 인텔리전스(CSI) 클라우드에서 데이터 업데이트를 얻어야 합니다.

기본적으로 URL 필터링을 사용하는 경우 자동 업데이트가 활성화됩니다. 그러나 이러한 업데이트가 발생할 시기를 제어해야 하는 경우, 기본 업데이트 메커니즘 대신 이 항목에서 설명하는 절차를 사용합니다.

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.

시작하기 전에

- management center에서 인터넷에 액세스할 수 있는지 확인합니다. 보안, 인터넷 액세스 및 통신 포트, 1095 페이지의 내용을 참조하십시오.
- URL 필터링이 활성화되었는지 확인합니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 범주 및 평판을 사용하여 *URL* 필터링 활성화를 참조하십시오.
- **Integration(**통합**)** > **Other Integrations(**기타 통합**)** 메뉴 아래의 클라우드 서비스에서 **Enable Automatic Updates(**자동 업데이트 활성화**)**가 선택되어 있지 않은지 확인합니다.
- 이 작업을 수행하려면 전역 도메인에 있어야 합니다. URL 필터링 라이선스도 있어야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** **Add Task(**작업 추가**)**를 클릭합니다.

단계 **3** **Job Type(**작업 유형**)** 목록에서 **Update URL Filtering Database(URL** 필터링 데이터베이스 업데이트**)**를 선택합니다.

단계 **4** 업데이트 예약 방법으로 **Once(**한 번**)** 또는 **Recurring(**반복**)**을 지정합니다.

- 일회성 작업의 경우, 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다.
- 반복 작업의 경우, 세부 정보는 반복 작업 구성, 502 페이지를 참조하십시오.

단계 **5** **Job Name(**작업 이름**)** 필드에 이름을 입력합니다.

단계 **6** 작업에 대해 코멘트하려는 경우, **Comment(**코멘트**)** 필드에 코멘트를 입력합니다.

코멘트 필드는 schedule calendar(일정 달력) 페이지의 Task Details(작업 세부 정보) 섹션에 표시 됩니다. 코멘트를 간략하게 합니다.

단계 **7** 작업 상태 메시지를 이메일로 보내려는 경우, **Email Status To:** 필드에 이메일 주소(또는 쉼표로 구분된 여러 이메일 주소)를 입력합니다. 상태 메시지를 보내려면 유효한 이메일 릴레이 서버가 구성되어 있어야 합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

예약된 작업 검토

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.

Calendar(달력) 보기 옵션을 사용하면 날짜별로 발생하는 예약된 작업을 확인할 수 있습니다.

Task List(작업 목록)에는 상태와 함께 작업 목록이 표시됩니다. 달력을 열면 일정 아래에 작업 목록이 나타납니다. 또한, 달력에서 날짜 또는 작업을 선택하여 작업 목록을 볼 수 있습니다.

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.

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.

작업 목록 세부 정보

표 ***43:*** 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.

열	설명
마지막 실행 시간	실제 시작 날짜 및 시간을 표시합니다. 반복 작업의 경우, 가장 최근의 실행에 적용됩니다.
마지막 실행 상태	예약된 작업의 현재 상황을 설명합니다. • **Check Mark(**확인 표시**)(****)**는 작업이 성공적으로 실행되었음을 나타냅니다. • 물음표 아이콘(**Question Mark(**물음표**)(****)**)은 작업이 알 수 없는 상태임을 나타냅니다. • 느낌표 아이콘()은 작업이 실패했음을 나타냅니다. 반복 작업의 경우, 가장 최근의 실행에 적용됩니다.
다음 런타임	반복 작업의 경우, 다음 실행 시간이 표시됩니다. 일회성 작업에 N/A가 표시됩니다.
생성자	예약된 작업을 생성한 사용자의 이름을 표시합니다.
수정	예약된 작업을 수정합니다.
삭제	예약된 작업을 삭제합니다.

일정표에서 예약된 작업 보기

다중 도메인 구축에서, 현재 도메인에 대해서만 예약된 작업을 볼 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.

단계 **2** 캘린더 보기를 사용하여 다음 작업을 수행할 수 있습니다.

- 이전 연도로 이동하려면 **Double Left Arrow(**이중 왼쪽 화살표**)** ( )를 클릭합니다.
- 이전 달로 이동하려면 **Single Left Arrow(**단일 왼쪽 화살표**)** ( )를 클릭합니다.
- 다음 달로 이동하려면 **Single Right Arrow(**단일 오른쪽 화살표**)** ( )를 클릭합니다.
- 다음 연도로 이동하려면 **Double Right Arrow(**이중 오른쪽 화살표**)** ( )를 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.

예약된 작업 수정

다중 도메인 구축에서, 현재 도메인에 대해서만 예약된 작업을 편집할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.
단계 **2** 달력에서 편집하려는 작업 또는 작업이 표시되는 날짜를 클릭하십시오.
단계 **3** **Task Details(**작업 세부 정부**)** 테이블에서, 편집할 작업 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.
단계 **4** 작업을 편집합니다.
단계 **5** **Save(**저장**)**를 클릭합니다.

예약된 작업 삭제

다중 도메인 구축에서, 현재 도메인에 대해서만 예약된 작업을 삭제할 수 있습니다.

프로시저

단계 **1** 시스템 ( ) > **Tools(**툴**)** > **Scheduling(**예약**)**을 선택합니다.
단계 **2** 달력에서 삭제하려는 작업을 클릭합니다. 반복 작업의 경우, 작업의 인스턴스를 클릭합니다.
단계 **3** **Task Details(**작업 세부 사항**)** 테이블에서 **Delete(**삭제**)** ( )를 클릭한 후 선택 내용을 확인합니다.

예약된 작업 기록

기능	버전	세부정보
자동 VDB 다운로드.	7.3	management center 예약의 초기 설정은 이제 최신 VDB를 포함하여 사용 가능한 최신 소프트웨어 업데이트를 다운로드하는 매주 작업을 예약합니다. 이 주간 작업을 검토하고 필요한 경우 조정하고, 실제로 VDB를 업데이트할 새 주간 작업을 예약하는 것이 좋습니다. 새 애플리케이션 탐지기 및 운영 체제 지문을 적용하려면 구성을 구축해야 합니다. 신규/수정된 화면: 이제 시스템에서 생성한 **Weekly Software Download(**주간 소프트웨어 다운로드**)** 예약 작업에서 **Vulnerability Database(**취약성 데이터베이스**)** 확인란이 기본적으로 활성화됩니다.
디바이스에 대한 자동 침입 규칙 업데이트.	6.6	이제 management center의 초기 설정에서 매일 침입 규칙 업데이트를 활성화합니다. 이 작업을 검토하고 필요한 경우 조정하는 것이 좋습니다. 업데이트된 규칙을 적용하려면 구성을 구축해야 합니다.
자동 소프트웨어 다운로드 및 구성 백업.	6.5	management center의 초기 설정은 이제 다음을 수행하도록 주간 작업을 예약합니다. • management center 및 매니지드 디바이스에 대해 사용 가능한 최신 소프트웨어 업데이트를 다운로드합니다. • 로컬로 저장된 구성 전용 백업을 수행합니다. 이러한 작업을 검토하고 필요에 따라 조정하는 것이 좋습니다.
여러 매니지드 디바이스의 원격 백업을 예약할 수 있는 기능.	6.4	이제 management center를 사용하여 온디맨드 백업을 지원하는 모든 매니지드 디바이스의 원격 백업을 예약할 수 있습니다. 백업 및 복구 요구 사항, 467 페이지의 내용을 참조하십시오. 신규/수정된 화면: 반복 백업을 구성할 때 이제 **Backup Type(**백업 유형**)**: 관리 센터 또는 디바이스를 선택할 수 있습니다.

17 장

가져오기/내보내기

다음 항목에서는 가져오기/내보내기 기능 사용 방법을 설명합니다.

컨피그레이션 가져오기/내보내기 정보

가져오기/내보내기 기능을 사용하여 어플라이언스 간에 구성을 복사할 수 있습니다. 구성 가져오기 및 내보내기는 백업 도구용이 아니지만 새로운 어플라이언스를 추가하는 프로세스를 간소화하는 데 사용될 수 있습니다.

단일 구성을 내보내거나 단일 동작으로 같은 유형 또는 다른 유형의 구성 집합을 내보낼 수 있습니다. 나중에 패키지를 다른 어플라이언스로 가져올 때 패키지의 어떤 구성을 가져올지 선택할 수 있습니다.

내보낸 패키지에는 해당 구성에 대한 개정 정보가 들어 있으며, 해당 구성을 다른 어플라이언스로 가져올 수 있는지 여부를 결정합니다. 어플라이언스 호환 되는 경우 패키지에 중복 구성, 시스템은 해결 옵션을 제공 합니다.

참고 가져오기 및 내보내기 어플라이언스는 동일한 버전의 Firepower System을 실행해야 합니다. 액세스 제어 및 해당 하위 정책(침입 정책 포함)의 경우 침입 규칙 업데이트 버전도 일치해야 합니다. 버전이 일치하지 않으면 가져오기가 실패합니다. 침입 규칙 업데이트 가져오기/내보내기 기능을 사용할 수 없습니다. 대신 최신 규칙 업데이트 버전을 다운로드하고 적용합니다.

가져오기/내보내기를 지원하는 구성

가져오기/내보내기는 다음 구성을 지원합니다.

- 액세스 제어 정책 및 이 정책에서 호출하는 정책: 사전 필터, 네트워크 분석, 침입, SSL, 파일, Threat Defense Service Policy
- 액세스 제어와 무관한 침입 정책
- NAT 정책(Secure Firewall Threat Defense만 해당)
- FlexConfig 정책. 그러나 정책을 내보내는 경우 모든 비밀 키 변수의 내용이 지워집니다. 비밀 키를 사용하는 FlexConfig 정책을 가져온 후 모든 비밀 키의 값을 수동으로 편집해야 합니다.
- 플랫폼 설정
- 상태 정책
- 알림 응답
- 애플리케이션 탐지기(사용자 정의 및 Cisco Professional Services 제공 모두)
- 대시보드
- 사용자 지정 표
- 사용자 지정 워크플로
- 저장된 검색
- 맞춤형 사용자 역할
- 보고서 템플릿
- 서드파티 제품 및 취약성 매핑
- 사용자 제어에 대한 사용자 및 그룹

구성 가져오기/내보내기에 대한 특별 고려 사항

구성을 내보내는 경우 시스템도 다른 필수 구성을 내보냅니다. 예를 들어, 액세스 제어 정책 내보내기는 해당 정책이 호출하는 하위 정책, 해당 정책이 사용하는 개체 및 개체 그룹, 상위 정책 (다중 도메인 구축의 경우) 등을 내보냅니다. 또 다른 예로, 외부 인증이 활성화된 플랫폼 설정 정책을 내보내는 경우 인증 개체도 내보내게 됩니다. 그러나 몇 가지 예외가 있습니다.

- 시스템 제공 데이터베이스 및 피드— 시스템은 URL 필터링 카테고리 및 평판 데이터, Cisco Intelligence Feed 데이터 또는 GeoDB(지리위치 데이터베이스)를 내보내지 않습니다. 구축에 있는 모든 어플라이언스가 Cisco의 최신 정보를 받는지 확인하십시오.
- 전역 보안 인텔리전스 목록—시스템은 내보낸 구성과 관련된 전역 보안 인텔리전스 차단 리스트 및 차단 안 함 목록을 내보냅니다. (다중 도메인 구축에서 이는 현재 도메인과 상관없이 발생합니다.) 시스템은 하위 도메인 목록을 내보내지 않습니다.) 가져오기 프로세스는 이들 목록을 사용자가 생성한 목록으로 전환한 다음 가져온 구성으로 새 목록을 사용합니다. 이렇게 하면 가져온 목록이 기존의 전역 차단 목록 및 차단 안 함 목록과 충돌하지 않습니다. management center 가져오기에서 글로벌 목록을 사용하려면 가져온 구성에 목록을 수동으로 추가합니다.

- 침입 정책 공유 계층 - 내보내기 프로세스가 침입 정책 공유 계층을 끊습니다. 이전에 공유된 계층은 패키지에 포함되며, 가져온 침입 정책에는 공유 계층이 포함되지 않습니다.
- 침입 정책 기본 변수 집합 - 내보내기 패키지에는 맞춤형 변수 및 시스템 제공 변수가 포함된 기본 변수 집합과 사용자 정의 값이 포함됩니다. 가져오기 프로세스는 기본 변수 집합을 가져오는 management center에서 가져온 값으로 업데이트합니다. 그러나 가져오기 프로세스는 내보내기 패키지에 없는 사용자 지정 변수를 삭제하지 않습니다. 가져오기 프로세스는 또한 내보내기 패키지에서 설정되지 않은 값에 대해 가져오는 management center에서 사용자 정의 값을 되돌리지 않습니다. 따라서 가져오는 management center이 기본 변수를 다르게 구성한 경우, 가져온 침입 정책이 예상과 다르게 작동할 수 있습니다.
- 맞춤형 사용자 개체—맞춤형 사용자 그룹 또는 개체를 management center에 생성한 경우 그리고 그러한 맞춤형 사용자 개체가 액세스 정책에 있는 어느 규칙의 일부인 경우, 내보내기 파일(.sfo)은 사용자 개체 정보를 전달하지 않습니다. 따라서 그러한 정책을 가져오는 경우, 그러한 맞춤형 사용자 개체에 대한 참조는 제거되며 대상 management center로 가져올 수 없습니다. 누락된 사용자 그룹으로 인한 탐지 문제를 방지하려면, 맞춤형 사용자 개체를 새 management center에 수동으로 추가하고 가져오기 후 액세스 제어 정책을 다시 구성합니다.

가져올 때 개체 및 개체 그룹:

- 일반적으로 가져오기 프로세스는 개체 및 그룹을 새 항목으로 가져 오며 기존 개체 및 그룹을 대체할 수 없습니다. 그러나 가져온 구성의 네트워크 및 포트 개체 또는 그룹이 기존 개체 또는 그룹과 일치하는 경우, 가져온 구성은 새 개체/그룹을 생성하는 대신 기존 개체/그룹을 다시 사용합니다. 시스템은 이름(자동 생성된 숫자 제외)과 각 네트워크 및 포트 개체/그룹의 내용을 비교하여 일치하는 항목을 결정합니다.
- 가져온 개체의 이름이 가져오는 management center에서 기존 개체와 일치하는 경우, 시스템이 가져온 개체 및 그룹 이름에 자동 생성된 번호를 추가하여 고유하게 만듭니다.
- 가져온 구성에서 사용되는 보안 영역 및 인터페이스 그룹을 가져오는 management center에 의해 관리되는 매칭 유형 영역 및 그룹에 매핑해야 합니다.
- 개인 키를 포함하는 PKI 개체를 사용하는 구성을 내보내는 경우, 시스템은 내보내기 전에 개인 키를 암호 해독합니다. 가져올 때 시스템은 무작위로 생성된 키로 해당 키를 암호화합니다.

구성 가져오기/내보내기 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

구성 내보내기

내보내는 구성 수 및 그러한 구성이 참조하는 개체의 수에 따라 내보내기 프로세스가 몇 분 정도 걸릴 수 있습니다.

팁 Firepower System의 많은 목록 페이지에는 목록 항목 옆에 **YouTube EDU** ( )이 있습니다. 이 아이콘이 있으면 내보내기 절차의 빠른 대안으로서 사용할 수 있습니다.

시작하기 전에

- 가져오기 및 내보내기 어플라이언스에서 동일한 버전의 Firepower System 실행 중인지 확인합니다. 액세스 제어 및 해당 하위 정책(침입 정책 포함)의 경우 침입 규칙 업데이트 버전도 일치해야 합니다.

프로시저

단계 **1** 시스템 ( ) > **Tools(**툴**)** > **Import/Export(**임포트/익스포트**)**을(를) 선택합니다.

단계 **2** **Collapse(**축소**)** ( ) 및 **Expand(**확장**)** ( ) 아이콘을 클릭하여 사용 가능한 설정 목록을 축소하고 확대합니다.

단계 **3** 내보내려는 구성을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **4** 웹 브라우저의 프롬프트에 따라 내보낸 패키지를 컴퓨터에 저장합니다.

구성 가져오기

가져오는 구성의 수 및 해당 구성이 참조하는 개체의 수에 따라 가져오기 절차에는 몇 분 정도 걸릴 수 있습니다.

참고 시스템에서 로그아웃하거나 다른 도메인으로 변경한 경우 또는 **Import(**가져오기**)**를 클릭한 후 사용자 세션이 만료된 경우, 가져오기 프로세스가 완료될 때까지 백그라운드에서 계속 진행됩니다. 새 개체 또는 정책을 생성하기 전에 가져오기 프로세스가 완료될 때까지 기다리는 것이 좋습니다. 가져오기 프로세스가 아직 실행 중인 상태에서 생성을 시도하면 오류가 발생할 수 있습니다.

시작하기 전에

- 가져오기 및 내보내기 어플라이언스에서 동일한 소프트웨어 버전을 실행 중인지 확인합니다. 액세스 제어 및 해당 하위 정책(침입 정책 포함)의 경우 침입 규칙 업데이트 버전도 일치해야 합니다.

프로시저

단계 **1** 가져오는 어플라이언스에서 시스템 (⚙) > **Tools(**툴**)** > **Import/Export(**임포트/익스포트**)**을 선택합니다.

단계 **2** **Upload Package(**패키지 업로드**)**를 클릭합니다.

단계 **3** 내보내기한 패키지의 경로를 입력하거나 해당 위치를 찾은 다음 **Upload(**업로드**)**를 클릭합니다.

단계 **4** 버전 불일치 또는 기타 문제가 없는 경우 가져오려는 구성을 선택한 다음 **Import(**가져오기**)**를 클릭합니다.
충돌 해결 또는 인터페이스 개체 매핑을 수행할 필요가 없는 경우, 가가져오기가 완료되고 성공 메시지가 나타납니다. 이 절차의 나머지 부분을 건너뜁니다.

단계 **5** 메시지가 나타나면, Import Conflict Resolution(가져오기 충돌 해결) 페이지에서 영역 및 그룹으로 가져온 구성에서 사용된 인터페이스 개체를 가져오는 management center이 관리하는 매칭된 인터페이스 유형과 매핑합니다.

소스 및 대상 개체의 인터페이스 개체 유형(보안 영역 또는 인터페이스 그룹) 및 인터페이스 유형(수동, 인라인, 라우팅 등)이 일치해야 합니다. 자세한 내용은 Interface(인터페이스) 섹션을 참조해 주십시오.

가져오는 구성이 이미 존재하지 않는 보안 영역이나 인터페이스 그룹을 참조하는 경우, 기존 인터페이스 개체에 매핑하거나 새 인터페이스 개체를 생성할 수 있습니다.

참고 개별 액세스 제어 정책의 경우, 기존 정책을 가져온 정책으로 대체할 수 있습니다. 그러나 중첩된 액세스 제어 정책의 경우, 새 정책으로만 가져올 수 있습니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.

단계 **7** 메시지가 나타나면, Import Resolution(가져오기 해결) 페이지에서 가져오기 충돌 해결, 528 페이지에 설명된 대로 각 구성을 확장하고 적절한 옵션을 선택합니다.

단계 **8** **Import(**가져오기**)**를 클릭합니다.

단계 **9** 모든 피드를 업데이트합니다.

예를 들어, **Objects(**개체**) > Object Management(**개체 관리**) > Security Intelligence(**보안 인텔리전스**)**로 이동하여 URL, Network(네트워크), DNS Lists(DNS 목록) 및 Feeds(피드) 페이지에서 **Update Feed(**피드 업데이트**)** 버튼을 클릭합니다.

가져온 정책은 피드 내용을 포함하지 않습니다.

단계 **10** 디바이스에 정책을 구축하기 전에 모든 피드 업데이트가 완료될 때까지 기다리십시오.

다음에 수행할 작업

참고 Microsoft Active Directory 사용자 및 그룹으로 **Keep Newest(**최신 구성 유지**)**를 선택한 경우 해독 정책, 액세스 제어 정책 및 기타 정책의 문제를 방지하기 위해 가져온 후 모든 사용자 및 그룹을 다운로드하는 것이 좋습니다. (**Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)**, 그런 다음 **(Download Now(**지금 다운로드**))**를 클릭합니다.

- 경우에 따라, 가져온 구성을 요약한 보고서를 확인합니다. 작업 메시지 보기, 444 페이지을 참조하십시오.

가져오기 충돌 해결

구성 가져오기를 시도하는 경우, 시스템에서 동일한 이름 및 유형의 구성이 이미 어플라이언스에 존재하는지 여부를 확인합니다. 다중 도메인 구축에서 시스템은 구성이 현재 도메인이나 상위 도메인 또는 하위 도메인에 정의 된 구성의 복제인지 여부도 결정합니다. (하위 도메인의 구성은 볼 수 없지만, 하위 도메인에 중복된 이름이 있는 구성이 존재하는 경우 시스템이 충돌을 알립니다.) 가져오기에 중복 구성이 포함된 경우, 시스템은 다음 중 구축에 적합한 해결 옵션을 제공합니다.

- 기존 항목 유지

  시스템이 해당 구성을 가져오지 않습니다.

- 기존 항목 교체

  시스템이 가져오기에서 선택된 구성으로 현재 구성을 덮어씁니다.

- 최신 항목 유지

  타임 스탬프가 어플라이언스의 현재 구성에 대한 타임 스탬프보다 최근인 경우에만 시스템이 선택된 구성을 가져옵니다.

참고 Microsoft Active Directory 사용자 및 그룹으로 **Keep Newest(**최신 구성 유지**)**를 선택한 경우 해독 정책, 액세스 제어 정책 및 기타 정책의 문제를 방지하기 위해 가져온 후 모든 사용자 및 그룹을 다운로드하는 것이 좋습니다. (**Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)**, 그런 다음 **(Download Now(**지금 다운로드**))**를 클릭합니다.

- 새 항목으로 가져오기

  시스템이 선택된 중복 구성을 가져오고 시스템 생성 번호를 이름에 추가하여 고유하게 만듭니다. (가져오기 프로세스를 완료하기 전에 이 이름을 변경할 수 있습니다.) 어플라이언스의 원래 구성이 변경되지 않습니다.

시스템에서 제공하는 해결 옵션은 구축에서 도메인을 사용하는지 여부, 가져온 구성이 현재 도메인에 정의된 구성과 중복되는지 여부 또는 현재 도메인의 상위 또는 하위 도메인에 정의된 구성인지 여

부에 따라 달라집니다. 다음 표는 시스템에서 해결 옵션을 제공하거나 제공하지 않는 경우를 나열합니다.

해결 옵션	**Secure Firewall Management Center**		매니지드 디바이스
	현재 도메인에서 중복	상위 또는 하위 도메인의 중복	
기존 항목 유지	예	예	예
기존 항목 교체	예	아니요	예
최신 항목 유지	예	아니요	예
새 항목으로 가져오기	예	예	예

사용자가 정상 또는 맞춤형 검색 파일 목록을 사용하는 파일 정책으로 액세스 제어 정책을 가져오고 파일 목록에는 중복 이름 충돌이 나타나는 경우, 시스템에서 위의 표에 설명된 대로 충돌 해결 옵션을 제공합니다. 그러나 시스템이 정책 및 파일 목록에 대해 수행하는 작업은 아래 표에 설명된 대로 다양합니다.

해결 옵션	시스템 작업	
	액세스 제어 정책 및 관련 파일 정책을 새 항목으로 가져오고 파일 목록을 병합합니다.	기존 액세스 제어 정책, 관련 파일 정책 및 파일 목록이 그대로 유지됩니다.
기존 항목 유지	아니요	예
기존 항목 교체	예	아니요
새 항목으로 가져오기	예	아니요
Keep newest(최신 상태로 유지**)**하고 가져오는 액세스 제어 정책이 최신 항목이 됩니다.	예	아니요
Keep newest(최신 상태로 유지**)**하고 기존 액세스 제어 정책이 최신 항목이 됩니다.	아니요	예

어플라이언스에서 가져온 구성을 수정하고 나중에 해당 어플라이언스로 해당 구성을 다시 가져 오는 경우, 유지할 구성 버전을 선택해야 합니다.

18 장

데이터 비우기 및 저장

FMC에 저장된 데이터

대상	확인
FMC의 데이터 스토리지에 대한 일반 정보	디스크 사용량 위젯, 355 페이지
오래된 데이터 제거	Management Center 데이터베이스에서 데이터 제거, 532 페이지
FMC의 데이터에 대한 외부 액세스 허용(고급 기능)	External Database Access(외부 데이터베이스 액세스), 63 페이지
백업	백업 및 원격 스토리지 관리, 495 페이지 및 하위 항목
보고서	로컬 스토리지 설정, 96 페이지
이벤트	연결 로깅, 753 페이지 데이터베이스, 59 페이지 및 하위 항목
네트워크 검색 데이터	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 검색 데이터 스토리지 설정 및 후속 항목

대상	확인
파일	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 악성코드 보호 및 파일 정책 장에서 모범 사례를 포함한 파일 저장에 관한 정보를 참고하십시오. 파일 및 악성코드 검사 성능 및 스토리지 조정 Cisco Secure Firewall Management Center 디바이스 구성 가이드
패킷 데이터	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 일반 설정 편집
사용자 및 사용자 활동	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사용자 데이터베이스 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 사용자 활동 데이터베이스

Management Center 데이터베이스에서 데이터 제거

데이터베이스 제거 페이지를 사용하여 검색, ID, 연결 및 보안 인텔리전스 데이터 파일을 management center 데이터베이스에서 제거할 수 있습니다. 데이터베이스를 삭제하면 해당 프로세스가 다시 시작됩니다.

⚠

주의 데이터베이스를 삭제하면 management center에서 지정한 데이터가 제거됩니다. 데이터를 삭제한 후에는 복구할 수 없습니다 .

시작하기 전에

데이터를 제거하려면 관리자 또는 보안 분석가 권한이 있어야 합니다. 글로벌 도메인에만 속할 수 있습니다.

프로시저

단계 **1** 시스템 (⚙) > **Tools(**툴**)** > **Data Purge(**데이터 제거**)**을(를) 선택합니다.

단계 **2** **Discovery and Identity(**검색 및 **ID)**에서 다음 중 하나 또는 모두를 실행합니다.

- 데이터베이스에서 모든 네트워크 검색 이벤트를 제거하려면 **Network Discovery Events(**네트워크 검색 이벤트**)** 확인란을 선택합니다.
- **Hosts(**호스트**)** 확인란을 선택하여 모든 호스트 및 Host(호스트)Indications of Compromise flags(보안 침해 플래그 표시)를 데이터베이스에서 제거합니다.

- **User Activity(**사용자 활동**)** 확인란을 선택하고 모든 사용자 활동 이벤트를 데이터베이스에서 제거합니다.
- **User Identities(**사용자 **ID)** 확인란을 선택하고 모든 사용자 로그인 및 사용자 기록 데이터 뿐만 아니라 User Indications of Compromise flags(보안 침해 플래그 사용자 표시)를 데이터베이스에서 제거합니다.

단계 **3** **Connections(**연결**)** 아래에서 다음 중 하나 또는 모두를 실행합니다.

- **Connection Events(**연결 이벤트**)** 확인란을 선택하고 모든 연결 데이터를 데이터베이스에서 제거합니다.
- **Connection Summary Events(**연결 요약 이벤트**)** 확인란을 선택하고 모든 연결 요약 데이터를 데이터베이스에서 제거합니다.
- **Security Intelligence Events(**보안 인텔리전스 이벤트**)** 확인란을 선택하고 모든 보안 인텔리전스 데이터를 데이터베이스에서 제거합니다.

참고 **Connection Events(**연결 이벤트**)** 확인란을 선택해도 보안 인텔리전스 이벤트는 제거되지 않습니다. 보안 인텔리전스 데이터와의 연결은 계속 보안 인텔리전스(Security Intelligence) 이벤트 페이지에 나타납니다(Analysis(분석)> Connections(연결) 메뉴 하단) 따라서 **Security Intelligence Events(**보안 인텔리전스 이벤트**)** 확인란을 선택해도 보안 인텔리전스 데이터 관련 연결 이벤트는 제거되지 않습니다.

단계 **4** **Purge Selected Events(**선택된 이벤트 제거**)**를 클릭합니다.
항목이 삭제되고 해당 프로세스가 다시 시작됩니다.

외부 데이터 스토리지

선택적으로 원격 데이터 스토리지를 사용하여 특정 유형의 데이터를 저장할 수 있습니다.

대상	확인
백업	백업 및 원격 스토리지 관리, 495 페이지 및 하위 항목 원격 스토리지 디바이스, 95 페이지 및 하위 항목
보고서	원격 스토리지 디바이스, 95 페이지 및 하위 항목 원격 스토리지로 보고서 이동, 567 페이지

대상	확인
Events(이벤트)	시스템 로그 및 기타 리소스에 대한 정보 외부 툴을 사용하여 이벤트 분석, 641 페이지 Cisco Secure Cloud Analytics의 원격 데이터 스토리지, 535 페이지 Secure Network Analytics 어플라이언스의 원격 데이터 스토리지, 535 페이지 연결 이벤트를 원격으로 저장하는 경우, FMC에서 연결 이벤트 스토리지를 비활성화하는 것이 좋습니다. 자세한 정보는 데이터베이스, 59 페이지 및 하위 주제를 참조하십시오.

중요 Syslog를 사용하거나 이벤트를 외부에 저장하려는 경우 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

Security Analytics and Logging 원격 이벤트 스토리지 옵션 비교

다음은 이벤트 데이터를 외부적으로 management center에 저장하는 비슷하지만, 다른 옵션입니다.

온프레미스	**SaaS**
방화벽 뒤에서 스토리지 시스템을 구매, 라이선싱, 설정합니다.	라이선스 및 데이터 스토리지 요금제를 구매하고 Cisco 클라우드로 데이터를 전송합니다.
지원되는 이벤트 유형: • 연결 • 보안 인텔리전스 • 침입 • 파일 및 악성코드 • LINA	지원되는 이벤트 유형: • 연결 • 보안 인텔리전스 • 침입 • 파일 및 악성코드
시스템 로그 및 직접 통합을 모두 지원합니다.	시스템 로그 및 직접 통합을 모두 지원합니다.
• Secure Network Analytics Manager에서 모든 이벤트 확인합니다. • FMC 이벤트 뷰어에서 교차 실행하여 Secure Network Analytics Manager의 이벤트를 확인합니다. • FMC에서 원격으로 저장된 연결 및 보안 인텔리전스 이벤트 보기	라이선스에 따라 CDO 또는 Secure Network Analytics의 이벤트를 확인합니다. FMC 이벤트 뷰어에서 교차 실행합니다.

온프레미스	SaaS
자세한 내용은 Secure Network Analytics 어플라이언스의 원격 데이터 스토리지, 535 페이지의 링크를 참조하십시오.	자세한 내용은 Cisco Secure Cloud Analytics의 원격 데이터 스토리지, 535 페이지의 링크를 참조하십시오.

Cisco Secure Cloud Analytics의 원격 데이터 스토리지

Security Analytics and Logging(SaaS)를 사용하여 선택한 Firepower 이벤트 데이터를 Secure Cloud Analytics로 전송합니다. 지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다.

자세한 내용은 https://cisco.com/go/firepower-sal-saas-integration-docs에 있는 *Firepower Management Center* 및 *Cisco SaaS(Security Analytics and Logging)* 통합 가이드를 참조하십시오

직접 또는 시스템 로그를 통해 이벤트를 전송할 수 있습니다.

중요 Syslog를 사용하거나 이벤트를 외부에 저장하려는 경우 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

Secure Network Analytics 어플라이언스의 원격 데이터 스토리지

Firepower 어플라이언스가 제공할 수 있는 것보다 더 많은 데이터 스토리지가 필요한 경우, Security Analytics and Logging(보안 애널리틱스)을 사용하여 Firepower 데이터를 Secure Network Analytics 어플라이언스에 저장할 수 있습니다. 자세한 내용은 https://cisco.com/go/sal-on-prem-docs에서 확인 가능한 설명서를 참조하십시오.

Secure Network Analytics 어플라이언스에 저장된 경우에도 management center에서 연결 이벤트를 볼 수 있습니다. Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Secure Firewall Management Center에서 작업, 699 페이지의 내용을 참조하십시오.

중요 Syslog를 사용하거나 이벤트를 외부에 저장하려는 경우 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

데이터 스토리지 기록

기능	버전	세부 사항
낮은 우선순위 연결 이벤트를 이벤트 속도 제한에서 제외	7.0	원격 볼륨에 저장하므로 FMC에 연결 이벤트를 저장하지 않기로 선택하는 경우, 해당 이벤트는 FMC 하드웨어 디바이스의 플로우 속도 제한에 포함되지 않습니다. 새 7.0 설정을 사용하여 Security Analytics and Logging(보안 애널리틱스)에 이벤트를 전송하는 경우, 이 설정을 해당 통합의 일부로 구성합니다. 그렇지 않으면 데이터베이스 이벤트 제한 수, 60 페이지의 연결 데이터베이스에 대한 정보를 참조하십시오. 신규/수정된 페이지: 없음 동작 변경만 해당됩니다.
Secure Network Analytics 어플라이언스로 이벤트를 전송하기 위한 향상된 프로세스	7.0	새로운 마법사를 사용하면 Security Analytics and Logging(보안 애널리틱스)을(를) 통해 Secure Network Analytics 어플라이언스로 직접 이벤트를 전송할 수 있습니다. 또한 이 마법사로 FMC에서 이벤트 페이지를 보는 동안 원격으로 저장된 연결 이벤트를 볼 수 있으며, Secure Network Analytics 어플라이언스에서 이벤트를 확인할 수 있도록 FMC에서 교차 실행할 수 있습니다. 시스템 로그를 사용하여 이벤트를 전송하도록 시스템을 이미 설정한 경우, 해당 설정을 비활성화하지 않는 한 이벤트는 시스템 로그를 통해 계속 전송됩니다. 자세한 내용은 Secure Network Analytics 어플라이언스의 원격 데이터 스토리지, 535 페이지의 참조 설명서를 확인하십시오. 신규/수정된 페이지: 이제 **System(**시스템**) > Logging(**로깅**) > Security Analytics & Logging(**보안 분석 및 로깅**)** 페이지에 교차 실행 옵션을 생성하는 데 설정 대신 마법사가 표시됩니다.
Secure Network Analytics 어플라이언스의 원격 데이터 스토리지	6.7	이제 Security Analytics and Logging(보안 애널리틱스)을 사용하여 대량의 Firepower 이벤트 데이터를 원격으로 저장할 수 있습니다. FMC에서 이벤트를 볼 때 신속하게 교차 실행을 수행하여 원격 데이터 스토리지 위치에서 이벤트를 확인할 수 있습니다. 지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다. 이벤트는 시스템 로그를 사용하여 전송됩니다. 이 솔루션은 SWE(Stealthwatch Enterprise) 버전 7.3을 실행하는 SMC(Stealthwatch Management Console) 가상 버전의 사용 가용성에 따라 달라집니다. Secure Network Analytics 어플라이언스의 원격 데이터 스토리지, 535 페이지의 내용을 참조하십시오.
Cisco Secure Cloud Analytics의 원격 데이터 스토리지	6.4	시스템 로그를 사용하여 Security Analytics and Logging(SaaS)을 통해 선택한 Firepower 데이터를 전송합니다. 지원되는 이벤트는 연결, 보안 인텔리전스, 침입, 파일, 악성코드입니다. 자세한 내용은 https://cisco.com/go/firepower-sal-saas-integration-docs에 있는 *Firepower Management Center* 및 *Cisco SaaS(Security Analytics and Logging)* 통합 가이드를 참조하십시오

V 부

보고 및 알림

19 장

리포트

다음 주제에서는 Firepower System의 보고서를 이용하는 방법을 설명합니다.

보고서 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 유지 보수 사용자 (위험 보고서만 해당)
- 보안 분석가

보고서 소개

Firepower System은 두 가지 유형의 보고서를 제공합니다.

- 위험 보고서, 540 페이지 - 네트워크에서 발견한 위험에 대한 개괄적인 요약

- Standard Reports(표준 보고서), 541 페이지 - Firepower 의 모든 요소에 대한 상세하고 맞춤형 가능한 보고서

위험 보고서

위험 보고서는 조직에서 발견한 리스트에 대한 휴대 가능하며, 개괄적이고, 쉽게 해석할 수 있는 요약입니다. 이러한 보고서를 이용하면 위험 영역 관련 정보와 이러한 위험 해결을 위한 권장사항을 사용자 시스템에 대한 액세스 권한이 없으며, 네트워크 보안 전문 지식이 없을 수도 있는 사람과 공유할 수 있습니다. 보고서는 네트워크 보안에 대한 투자 영역 관련 논의를 촉진할 용도로 제작됩니다.

위험 보고서 템플릿

- 지능형 악성코드 위험 보고서
- 공격 위험 보고서. 다음은 이 보고서의 필드입니다.
  - **Total Attacks(**전체 공격**)** - 총 IPS 이벤트 수입니다.
  - **Relevant Attacks(**관련 공격**)** - 영향 플래그가 1인 IPS 이벤트의 수입니다.
  - **Hosts Targeted(**대상 호스트**)** - 영향 플래그가 1인 IPS 이벤트에서 고유한 대상 IP 주소의 수입니다.
  - **Irrelevant Attacks(**무관한 공격**)** - 영향 플래그가 1이 아닌 IPS 이벤트의 백분율입니다.
  - **Events Requiring Attention(**주의가 필요한 이벤트**)** - 영향 플래그가 1인 IPS 이벤트의 백분율입니다.
  - **Hosts Connected to CnC Servers(C&C** 서버에 연결된 호스트**)** -IOC 범주가 "CnC Connected(C&C 에 연결됨)"인 고유한 호스트의 총 수입니다.
- 네트워크 위험 보고서

위험 보고서 생성, 보기 및 인쇄

표준 보고서용 템플릿은 위험 보고서에는 적용되지 않습니다.

보고서는 현재 도메인에만 적용됩니다.

각각의 위험 보고서는 HTML 파일을 생성합니다.

위험 보고서 생성을 예약하는 방법은 보고서 생성 자동화, 509 페이지 섹션을 참조하십시오.

시작하기 전에

- 요약할 위험을 탐지하도록 시스템이 설정돼 있는지 확인하십시오.

- 보고서를 이메일로 전송하고 싶지만 아직 Relay Host(릴레이 호스트)를 설정하지 않았다면 , 지금 설정하십시오. 자세한 내용은 메일 릴레이 호스트 및 알림 주소 구성, 62 페이지 섹션을 참조해 주십시오.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 원하는 보고서의 **Generate Report(**보고서 생성**)**를 클릭합니다.

단계 **4** 정보를 입력합니다.

- Input Parameters(입력 파라미터) 섹션에 입력하는 정보는 보고서의 제목 페이지에 표시됩니다. 이러한 필드는 입력하지 않아도 됩니다.

단계 **5** **Generate(**생성**)**를 클릭합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 위험 보고서를 보고, 다운로드하고, 옮기고 삭제하는 방법은 생성된 보고서 작업 정보, 565 페이지 섹션을 참조하십시오.
- 지원되는 대부분의 브라우저에서 위험 보고서를 PDF 형식으로 인쇄할 수 있습니다. 최상의 결과를 얻으려면 브라운저의 인쇄 또는 인쇄 미리보기 설정에서 배경색과 이미지를 활성화하고, 원한다면 머리글과 바닥글도 활성화하십시오. 지원되는 페이지 크기는 A4 및 US 레터입니다.

Standard Reports(표준 보고서)

시스템은 management center에 나타나는 대시보드 또는 이벤트 보기와 함께 다중 섹션의 보고서를 빠르고 쉽게 생성할 수 있는 유연한 보고 시스템을 제공합니다. 맞춤형 보고서를 처음부터 디자인할 수도 있습니다.

보고서는 전달할 내용이 포함된 PDF, HTML 또는 CSV 형식의 문서 파일입니다. 보고서 템플릿은 보고서 및 보고서 섹션에 대한 데이터 검색과 형식을 지정합니다. 시스템에는 보고서 템플릿의 디자인을 자동화하는 강력한 보고서 디자이너가 포함되어 있습니다. 웹 인터페이스에 표시되는 이벤트 보기 테이블 또는 대시보드 그래픽의 내용을 복제할 수 있습니다.

보고서 템플릿을 필요한 만큼 작성할 수 있습니다. 각 보고서 템플릿은 보고서의 개별 섹션을 정의하며, 보고서의 내용을 생성하는 데이터베이스 검색은 물론 표시 형식(테이블, 차트, 상세 보기 등)과 시간 프레임도 지정합니다. 템플릿은 또한 커버 페이지와 목차, 문서 페이지에 머리글과 바닥글 포함(PDF 형식의 보고서에서만 사용 가능) 여부 등의 문서 속성도 지정합니다. 단일 설정 패키지 파일로 보고서 템플릿을 내보내고, 다른 management center에서 재사용하기 위해 가져올 수 있습니다.

유용성 확장을 위해 템플릿에 입력 파라미터를 포함할 수 있습니다. 입력 파라미터를 사용하면 동일한 보고서를 원하는 형태로 변형할 수 있습니다. 입력 파라미터로 보고서를 생성할 경우 생성 과정 중에 각 입력 파라미터의 값을 입력하라는 프롬프트가 표시됩니다. 입력하는 값은 1회 기반으로 보고서 내용을 제한합니다. 예를 들어 침입 이벤트 보고서를 생성하는 검색의 목적지 IP 필드에 입력 파라미터를 둘 수 있습니다. 보고서 생성 시 목적지 IP 주소를 입력하라는 프롬프트가 표시될 때 부서의 네트워크 세그먼트를 지정할 수 있습니다. 그러면 생성된 보고서에는 해당 특정 부서와 관련된 정보만 포함됩니다.

설계 보고서 정보

보고서 템플릿

보고서 템플릿을 사용하면 각 보고서 섹션에서 데이터의 내용과 형식을 정의하는 것은 물론, 보고서 파일의 문서 특성(커버 페이지, 목차, 페이지 머리글과 바닥글)도 정의할 수 있습니다. 보고서를 생성한 후 템플릿은 삭제될 때까지 계속 재사용 가능합니다.

보고서에는 하나 이상의 정보 섹션이 포함되어 있습니다. 각 섹션의 형식(텍스트, 테이블 또는 차트)을 개별적으로 선택합니다. 한 섹션에 대해 선택한 형식은 포함 가능한 데이터를 제한할 수 있습니다. 예를 들어 원 그래프 형식을 사용하는 특정 테이블에는 시간 기반 정보를 표시할 수 없습니다. 최적의 상태로 표시하기 위해 언제든지 섹션의 형식 또는 데이터 기준을 변경할 수 있습니다.

사전 정의된 이벤트 보기를 기반으로 보고서의 초기 디자인을 작성할 수도 있고, 정의된 대시보드, 워크플로 또는 요약에서 내용을 가져와 디자인을 시작할 수도 있습니다. 빈 템플릿에서 시작하여 하나씩 섹션을 추가하고 특성을 정의할 수도 있습니다.

참고 다중 도메인 구축에서는 상위 도메인에 속한 보고서 템플릿을 볼 수는 있지만 편집할 수는 없습니다. 이러한 템플릿에서 보고서를 생성하려면 현재 도메인에 템플릿을 복사해야 합니다.

보고서 템플릿 필드

다음 표에서는 보고서 템플릿의 섹션을 작성하는 데 사용할 수 있는 필드를 설명합니다. 섹션 유형에 따라 사용할 수 없는 필드도 있습니다. 섹션 형식을 선택하면 시스템은 적절한 필드를 표시합니다.

필드 이름	섹션 유형	정의
형식	해당 없음	섹션 데이터의 형식을 선택합니다. **Bar chart(**막대그래프**)** (): 선택한 변수의 수량을 비교합니다. **Line chart(**선형 차트**)** (): 선택한 변수의 시간에 따른 추세/변경 사항을 표시합니다. 시간 기반 테이블에만 사용할 수 있습니다. **Pie chart(**원도표**)** (): 선택한 각 변수를 전체의 비율로 표시합니다. 수량이 0인 변수는 차트에서 삭제됩니다. 매우 소량의 항목들은 **Other(**기타**)**라는 카테고리로 묶입니다. **Table view(**테이블 보기**)** (): 각 레코드의 속성값을 표시합니다. 요약 또는 통계 데이터에는 사용할 수 없습니다. **Detail view(**상세정보 보기**)** (): 패킷(침입 이벤트의 경우) 및 호스트 프로파일(호스트 이벤트의 경우) 등 특정 이벤트와 관련된 복잡한 개체 데이터를 표시합니다. 이 형식은 해당 개체와 관련된 특정 이벤트 유형에 대해서만 사용할 수 있습니다. 요청 수가 많을 경우 출력 성능이 저하될 수 있습니다.
표	모두	섹션 데이터를 추출하는 테이블을 선택합니다.
프리셋	모두	사전 정의된 검색입니다. 새 검색을 정의할 때 검색 기준을 시작할 적절한 프리셋을 선택합니다.
검색 또는 필터	모두	대부분의 테이블에서 사전 정의 또는 저장된 **Search(**검색**)**를 사용하여 보고서를 제한할 수 있습니다. 또한 **Edit(**수정**)** ()을 클릭하여 새 검색을 생성할 수 있습니다. Application Statistics(애플리케이션 통계) 테이블에서는 사용자 정의 애플리케이션 필터를 이용해 보고서를 제한할 수 있습니다.
X축	막대 그래프 라인 차트 원형 차트	선택한 차트의 X축에 대해 사용할 수 있는 데이터입니다. 선 그래프의 경우 X축 값은 항상 **Time(**시간**)**입니다. 막대 및 원도표의 경우 X축 값으로 **Time(**시간**)**을 선택할 수 없습니다.
Y축	막대 그래프 라인 차트 원형 차트	선택한 차트의 Y축에 대해 사용할 수 있는 데이터입니다.
섹션 설명	모두	섹션의 검색 데이터 앞에 오는 설명 텍스트입니다. 텍스트 및 입력 파라미터의 조합을 입력합니다. 새로운 색션의 기본값은 `$<Time Window>` 및 `$<Constraints>`입니다.
기간	모두	섹션에 나타나는 데이터의 시간 창입니다. 섹션에서 시간 기반 테이블을 검색하는 경우, 보고서의 전역 시간 창을 상속하는 확인란을 선택할 수 있습니다. 또는 섹션에 대한 특정 시간 창을 설정할 수 있습니다.

필드 이름	섹션 유형	정의
데이터 소스	모두	Security Analytics and Logging(보안 애널리틱스)을(를) 통해 원격(외부) 데이터 스토리지를 설정하기 위해 마법사를 사용한 경우, 연결 및 보안 인텔리전스 이벤트에 사용할 데이터 소스를 선택할 수 있습니다. 다음 중에서 선택할 수 있습니다. • **Auto(**자동**)**: 사용 가능한 경우, FMC에 저장된 데이터를 표시합니다. 선택한 전체 기간 동안 FMC의 데이터를 사용할 수 없는 경우, 원격으로 저장된 데이터만 표시합니다. • **Local(**로컬**)**: 선택한 기간에 관계없이 FMC에 저장된 데이터만 표시합니다. 원격 볼륨에 이벤트를 전송하도록 설정되지 않은 디바이스에서 생성된 이벤트와 같이 원격 볼륨에서 사용할 수 없는 데이터를 포함하려면 이 옵션을 선택합니다. • **Extended(**확장**)**: 원격 볼륨에 저장된 데이터만 표시합니다.
최대 결과 수	테이블 보기 세부 정보 보기	포함할 일치하는 레코드의 최대 수입니다. CSV 또는 HTML 보고서에 비해 PDF 보고서에는 포함할 수 있는 레코드 수가 더 적습니다. 웹 인터페이스는 숫자가 너무 크면 경고 및 오류 아이콘을 사용하여 이를 표시합니다. 아이콘 위에 마우스 포인터를 올리면 한도를 확인할 수 있습니다.
결과	막대 그래프 원형 차트	**Top(**위쪽**)** 또는 **Bottom(**아래쪽**)**을 선택하고 차트 작성에 사용할 일치하는 레코드의 수를 입력합니다.
색상	막대 그래프 라인 차트	섹션에서 그래프로 표시하는 데이터의 색상입니다.

보고서 템플릿 생성

보고서 템플릿은 섹션의 프레임워크이며, 각각은 자체 데이터베이스 쿼리에서 독립적으로 작성됩니다.

새 보고서 템플릿은 새 템플릿을 만들거나, 기존 템플릿을 이용하거나, 이벤트 보기의 템플릿을 기반으로 하거나, 대시보드 또는 워크플로를 가져와 작성합니다.

기존 보고서 템플릿을 복사하지 않으려는 경우 완전히 새로운 템플릿을 생성할 수 있습니다. 템플릿 생성의 첫 단계는 섹션을 추가하고 형식을 지정할 수 있는 프레임워크를 생성하는 것입니다. 그런 다음 원하는 순서대로 개별 템플릿 섹션을 디자인하고 보고서 문서의 속성을 설정합니다.

각 템플릿 섹션은 검색 또는 필터에 의해 생성된 데이터 집합으로 구성되며, 표시 모드를 결정하는 형식 사양(테이블, 원도표 등)을 가지고 있습니다. 출력에 포함하려는 데이터 레코드의 필드 및 표시할 레코드의 시간 프레임과 수를 선택하여 섹션 내용을 더 자세히 지정할 수 있습니다.

참고 윈도표 색상 등 출력 특성과 열 선택을 확인하려면 섹션 미리 보기 유틸리티를 사용할 수 있지만, 구성한 검색의 정확성이 신뢰할 수 있는 수준으로 표시되지는 않습니다.

템플릿에서 생성하는 보고서에는 커버 페이지, 머리글과 바닥글, 페이지 번호 지정 등 모든 섹션 및 제어 기능에 해당하는 몇 가지 문서 속성이 있습니다.

문서 형식으로 CSV를 선택한 경우에는 문서 속성을 설정하지 않아도 됩니다.

기존 템플릿 중에서 좋은 모델을 찾은 경우 해당 템플릿을 복사하고 특성을 수정하여 새 보고서 템플릿을 생성할 수 있습니다. Cisco에서는 사전 정의 보고서 템플릿 집합도 제공하며, 템플릿 목록의 **Reports Tab(**보고서 탭**)**에서 확인할 수 있습니다.

이벤트 보기에서는 보고서 템플릿을 만들고 필요에 맞게 수정할 수 있습니다. 섹션을 더 추가하고, 포함된 섹션을 자동으로 수정하고, 섹션을 삭제할 수 있습니다.

대시보드, 워크플로 및 통계 요약을 가져와서 새 보고서를 빠르게 생성할 수 있습니다. 가져오기를 수행하면 대시보드 및 워크플로의 각 이벤트 보기에 각 위젯 그래픽에 대한 섹션이 생성됩니다. 가장 중요한 정보에 집중할 수 있도록 불필요한 섹션을 모두 삭제할 수 있습니다.

맞춤형 보고서 템플릿 생성

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** **Create Report Template(**보고서 템플릿 생성**)**을 클릭합니다.

단계 **4** **Report Title(**보고서 제목**)** 필드에 새 템플릿의 이름을 입력합니다.

단계 **5** 보고서 제목에 입력 매개변수를 추가하려면 매개변수의 값이 나타나야 할 제목에 커서를 두고 입력 **Input Parameter(**입력 매개변수**)** (+)를 클릭합니다.

단계 **6** Report Sections(보고서 섹션) 제목 표시줄 아래에 있는 추가 집합을 사용하여 필요한 만큼 섹션을 삽입합니다.

단계 **7** 보고서 템플릿 구성, 548 페이지에 설명된 대로 섹션 콘텐츠를 설정합니다.

팁 섹션 창 아래에 있는 **Preview(**미리보기**)**를 클릭하면 선택한 열 배치나 그래픽 형식을 볼 수 있습니다.

단계 **8** **Advanced(**고급**)**를 클릭하고 보고서 템플릿의 문서 속성, 557 페이지에 설명된 대로 PDF와 HTML 보고서의 속성을 설정합니다 .

단계 **9** **Save(**저장**)**를 클릭합니다.

오류가 표시되는 경우에는 각 섹션의 결과 값 옆에 노란색 삼각표가 있는지 확인하십시오. 삼각형이 보인다면 다음 중 하나를 수행합니다.

- 노란색 화살표가 있는 각 필드에서 삼각형 위에 마우스 포인터를 올리고 결과 값을 표시되는 값으로 줄입니다.
- **Generate(**생성**)**를 클릭하고 PDF 이외의 출력 형식을 포함합니다.

기존 템플릿에서 보고서 템플릿 생성

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 복사할 보고서 템플릿 옆에 있는 아이콘**(Copy(**복사**)** ( ))을 클릭합니다.

단계 **4** **Report Title(**보고서 제목**)** 필드에 이름을 입력합니다.

단계 **5** 필요한 대로 템플릿을 변경합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이벤트 보기에서 보고서 템플릿 생성

프로시저

단계 **1** 보고서에 표시할 이벤트를 이용해 이벤트 보기를 채웁니다.

- 확인할 이벤트를 이벤트 검색을 사용하여 정의합니다.
- 이벤트 보기에 적절한 이벤트가 표시될 때까지 워크플로에서 드릴다운합니다.

단계 **2** 이벤트 보기 페이지에서 **Report Designer(**보고서 디자이너**)**를 클릭합니다.

캡처한 워크플로의 각 보기에 대한 섹션과 함께 Report Sections(보고서 섹션) 페이지가 표시됩니다.

단계 **3** 선택적으로, **Report Title(**보고서 제목**)** 필드에 새 이름을 입력하고 **Save(**저장**)**를 클릭합니다.

단계 **4** 다음 작업을 수행할 수 있습니다.

- 커버 페이지, 목차, 시작 페이지 번호 또는 머리글과 바닥글 텍스트 추가 - **Advanced(**고급**)** 설정을 클릭합니다.
- 페이지 나누기 추가 - **Add Page Break(**페이지 구분 추가**)** ( )을 클릭하고, 새 페이지 나누기 개체를 템플릿 아래쪽에서 새 페이지를 시작할 섹션 앞으로 드래그합니다.
- 텍스트 섹션 추가 - **Add Text Section(**텍스트 섹션 추가**)** ( )을 클릭하고, 새 텍스트 섹션을 템플릿 아래쪽에서 보고서 템플릿에 표시할 위치까지 드래그합니다.
- 섹션 제목 변경 - 제목 표시줄에 있는 섹션 제목을 클릭하고, 섹션 제목을 입력하고, **OK(**확인**)**를 클릭합니다.

- 보고서 섹션 설정 - 각 섹션의 필드 설정을 조정합니다.

  팁 섹션의 현재 열 레이아웃 또는 차트 형식을 보려면 해당 섹션의 **Preview(**미리보기**)** 링크를 클릭하십시오.

- 보고서에서 템플릿 섹션 제외 - 섹션의 제목 표시줄에서 **Delete(**삭제**)** ( )을 클릭하고 삭제 여부를 확인합니다.

  참고 일부 워크플로의 마지막 보고서 섹션에는 워크플로에 따라 패킷, 호스트 프로파일 또는 취약성을 보여주는 상세정보 보기가 포함됩니다. 보고서를 생성할 때 이러한 상세정보 보기가 있는 다수의 이벤트를 검색하면 management center의 성능이 저하될 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

대시보드 또는 워크플로를 가져와 보고서 템플릿 생성

프로시저

단계 **1** 보고서에서 복제할 대시보드, 워크플로 또는 요약을 식별합니다.

단계 **2** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **3** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **4** **Create Report Template(**보고서 템플릿 생성**)**을 클릭합니다.

단계 **5** **Report Title(**보고서 제목**)** 필드에 새 보고서 템플릿의 이름을 입력합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

단계 **7** 가져오기 섹션 ( ) 버튼을 클릭합니다. 보고서 가져오기 섹션의 데이터 소스 옵션, 548 페이지에서 설명하는 데이터 소스 중 하나를 선택할 수 있습니다.

단계 **8** 드롭다운 메뉴에서 대시보드, 워크플로 또는 요약을 선택합니다.

단계 **9** 추가할 데이터 소스에 대해 **Import(**가져오기**)**를 클릭합니다.

대시보드의 경우 각 위젯 그래픽이 자체 섹션을 가지며, 워크플로의 경우 각 이벤트 보기가 자체 섹션을 가집니다.

단계 **10** 필요한 대로 섹션의 내용을 변경합니다.

참고 일부 워크플로의 마지막 보고서 섹션에는 워크플로에 따라 패킷, 호스트 프로파일 또는 취약성을 보여주는 상세정보 보기가 포함됩니다. 보고서를 생성할 때 이러한 상세정보 보기가 있는 다수의 이벤트를 검색하면 management center의 성능이 저하될 수 있습니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

보고서 가져오기 섹션의 데이터 소스 옵션

표 ***44:*** 보고서 가져오기 섹션 창의 데이터 소스 옵션

이 옵션 선택	가져오기
대시보드 가져오기	선택한 대시보드의 맞춤형 분석 위젯
워크플로 가져오기	사전 정의 또는 맞춤형 워크플로 선택 형식은 다음과 같습니다. `Table - Workflow name` 예를 들어 `Connection Events - Traffic by Port`는 Connection Events(연결 이벤트) 테이블에서 생성된 Traffic by Port(포트별 트래픽) 워크플로의 보기를 가져옵니다.
Import Summary Sections(요약 섹션 가져오기)	다음 일반 요약 중 하나: • Intrusion Detailed Summary(침입 상세 요약) • Intrusion Short Summary(침입 짧은 요약) • Discovery Detailed Summary(검색 짧은 요약) • Discovery Short Summary(검색 짧은 요약)

보고서 템플릿 구성

생성한 보고서 템플릿은 수정하거나 맞춤형할 수 있습니다. 다양한 보고서 섹션 속성을 수정하여, 섹션의 내용과 해당 데이터 표시 방식을 조정할 수 있습니다.

보고서 템플릿의 각 섹션은 데이터베이스 테이블을 쿼리하여 해당 섹션의 내용을 생성합니다. 섹션의 데이터 형식을 변경할 경우 동일한 데이터 쿼리가 사용되지만, 형식 유형의 분석 목적에 따라 섹션에 나타나는 필드가 수정됩니다. 예를 들어 침입 이벤트의 테이블 보기는 이벤트 레코드당 다수의 데이터 필드로 섹션을 채우는 반면, 원도표 섹션에는 개별 이벤트에 대한 상세정보 없이 선택한 각 특성이 나타내는 모든 일치하는 레코드의 일부가 표시됩니다. 막대 그래프는 특정 속성이 있는 일치하는 레코드의 총 수를 비교합니다. 선 그래프는 단일 특성을 기준으로 일치하는 레코드의 시간에 따른 변경 사항을 요약합니다. 선 그래프는 시간 기반의 데이터에만 사용할 수 있으며 호스트, 사용자, 서드파티 취약성 등에 대한 정보에는 사용할 수 없습니다.

보고서 섹션의 검색 또는 필터는 섹션 내용의 기반이 되는 데이터베이스 쿼리를 지정합니다. 대부분의 테이블에서 사전 정의 검색 또는 저장된 검색을 사용하여 보고서를 제한하거나, 즉석에서 새 검색을 생성할 수 있습니다.

- 사전 정의된 검색은 특정 이벤트 테이블을 검색하는 예제로 제공되며, 보고서에 포함할 네트워크 관련 중요 정보에 빠르게 액세스할 수 있습니다.
- 저장된 이벤트에는 자신이나 타인이 생성한 모든 공개 이벤트 검색은 물론, 자신이 저장한 모든 비공개 이벤트 검색도 포함됩니다.

- 현재 보고서 템플릿에 대해 저장된 검색은 보고서 템플릿 자체에서만 액세스 가능합니다. 저장한 보고서 템플릿 검색의 검색 이름은 “Custom Search” 문자열로 끝납니다. 사용자는 보고서를 디자인하는 도중 이러한 검색을 생성합니다.

Application Statistics(애플리케이션 통계) 테이블에서는 사용자 정의 애플리케이션 필터를 이용해 보고서를 제한할 수 있습니다.

섹션에 테이블 데이터를 포함하는 경우 데이터 레코드에 어떤 필드를 표시할지를 선택할 수 있습니다. 테이블의 모든 필드를 포함하거나 제외할 수 있습니다. 보고서 목적을 달성하는 필드를 선택한 다음 적절히 순서를 지정하고 정렬합니다.

전체 보고서 또는 개별 섹션에 대해 맞춤형 텍스트(예: 소개)를 제공하려면 템플릿에 텍스트 섹션을 추가할 수 있습니다.

템플릿의 섹션 전후에 페이지 나누기를 추가할 수 있습니다. 이 기능은 다양한 섹션을 소개하는 텍스트 페이지가 있는 다중 섹션 보고서에서 특히 유용합니다.

보고서 템플릿의 시간 창은 템플릿의 보고 기간을 정의합니다.

참고 보안 분석가는 자신이 생성한 보고서 템플릿만 수정할 수 있습니다. 다중 도메인 구축의 경우에는 상위 도메인의 보고서 템플릿은 편집할 수 없지만, 복사해서 하위 버전을 만들 수 있습니다.

보고서 템플릿 섹션에 대한 테이블 및 데이터 형식 설정

프로시저

단계 **1** 보고서 템플릿 섹션에서 **Table(**테이블**)** 드롭다운 메뉴를 사용하여, 쿼리할 테이블을 선택합니다.

Format(형식**)** 필드는 선택한 테이블에 사용할 수 있는 각 출력 형식을 나타냅니다.

단계 **2** 섹션에 해당하는 출력 형식을 선택합니다.

단계 **3** 검색 제약 조건을 변경하려면 **Section description(**섹션 설명**)** 필드 또는 **Filter(**필터**)** 필드 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** 그래픽 출력 형식(원도표, 막대 그래프 등)에 대해 드롭다운 메뉴를 사용하여 **X-Axis(X**축**)** 및 **Y-Axis(Y**축**)** 파라미터를 조정합니다.

X축에 대한 값을 선택하면 호환되는 값만 Y축 드롭다운 메뉴에 나타나고, 그 반대의 경우도 마찬가지입니다.

단계 **5** 테이블 출력에서는 열, 나타나는 순서 및 출력의 정렬 순서를 선택합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

관련 항목

보고서 템플릿 필드, 542 페이지

보고서 템플릿 섹션에 대한 검색 또는 필터 지정

프로시저

단계 **1** 보고서 템플릿 섹션에서 **Table(**테이블**)** 드롭다운 메뉴를 사용하여, 쿼리할 데이터베이스 테이블을 선택합니다.

- 대부분의 테이블에 대해 **Search(**검색**)** 드롭다운 목록이 나타납니다.
- Application Statistics(애플리케이션 통계) 테이블의 경우 **Filter(**필터**)** 드롭다운 목록이 나타납니다.

단계 **2** 보고서를 제한하기 위해 사용할 검색 또는 필터를 선택합니다.

검색 기준을 볼 수도 있고 **Edit(**수정**)** ( )을 클릭하여 새 검색을 생성할 수도 있습니다.

테이블 형식 섹션에 표시되는 검색 필드 설정

프로시저

단계 **1** 테이블 형식 보고서 섹션에서 **Fields(**필드**)** 매개변수 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **2** 섹션을 수정하려는 경우, 필드를 추가 및 삭제하고 필드를 원하는 열 순서대로 끌어와야 합니다.

단계 **3** 특정 열의 정렬 순서를 변경하려는 경우에는 각 필드의 드롭다운 목록을 사용하여 정렬 순서와 우선순위를 설정해야 합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

보고서 템플릿에 텍스트 섹션 추가

텍스트 섹션에서는 여러 글꼴 크기와 스타일(굵게, 기울임 등)의 풍부한 텍스트는 물론 입력 파라미터와 가져온 이미지도 사용할 수 있습니다.

팁 텍스트 섹션은 보고서 또는 보고서 섹션을 소개할 때 유용합니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Add Text Section(**텍스트 섹션 추가**)** ( )을 클릭합니다.

단계 **2** 보고서 템플릿의 원하는 위치로 새 텍스트 섹션을 끌어옵니다.

단계 **3** 텍스트 섹션을 페이지 처음이나 끝 부분에 배치하는 경우에는, 텍스트 섹션 앞이나 뒤에 페이지 나누기를 추가합니다.

단계 **4** 텍스트 섹션의 일반 이름을 변경하려는 경우에는 제목 표시줄에서 섹션의 이름을 클릭하고 새 이름을 입력합니다.

단계 **5** 텍스트 섹션의 본문에 서식이 지정된 텍스트와 이미지를 추가합니다.

보고서를 생성할 때 동적으로 업데이트되는 입력 파라미터를 포함할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

관련 항목

입력 매개변수, 553 페이지

보고서 템플릿에 페이지 나누기 추가

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Add Page Break(**페이지 구분 추가**)** ( )을 클릭합니다.

템플릿의 아래쪽에 페이지 나누기가 나타납니다.

단계 **2** 페이지 나누기를 섹션 전후의 원하는 위치로 끌어옵니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

글로벌 시간 창 및 보고서 템플릿 섹션

시간 기반 데이터(예: 침입 또는 검색 이벤트)가 포함된 보고서 템플릿에는 전역 시간 창이 있으며, 템플릿의 시간 기반 섹션은 생성될 때 기본적으로 이를 상속합니다. 전역 시간 창을 변경하면 전역 시간 창을 상속하도록 구성된 섹션에 대한 로컬 시간 창이 변경됩니다. **Inherit Time Window(**시간 창 상속**)** 확인란의 선택을 취소하여 개별 섹션에 대해 시간 창 상속을 비활성화할 수 있습니다. 그러면 로컬 시간 창을 편집할 수 있습니다.

참고 전역 시간 창 상속은 시간 기반 테이블의 데이터(예: 침입 이벤트 및 검색 이벤트)와 함께 보고서 섹션에만 적용됩니다. 네트워크 자산(호스트와 디바이스) 및 관련 정보(예: 취약성)에 대해 보고하는 섹션의 경우 각 시간 창을 개별적으로 설정해야 합니다.

보고서 템플릿 및 관련 섹션에 대한 글로벌 시간 창 설정

팁 보고서에서 섹션마다 다른 시간 범위를 사용할 수 있습니다. 예를 들어 첫 번째 섹션에는 월 요약을 포함하고, 나머지 섹션에는 각 주의 상세정보을 포함할 수 있습니다. 이 경우 섹션 레벨 시간 창을 개별적으로 설정합니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Generate(**생성**)**를 클릭합니다.

단계 **2** 전역 시간 창을 수정하려면 **Time Window(**시간 창**)(**)을 클릭합니다.

단계 **3** **Events Time Window(**이벤트 시간 창**)**에서 시간 설정을 수정합니다.

단계 **4** **Apply(**적용**)**를 클릭합니다.

단계 **5** **Generate(**생성**)**을 클릭해 보고서를 생성하고 **Yes(**예**)**를 클릭해 확인합니다.

보고서 템플릿 섹션에 대한 보고서 템플릿 섹션에 로컬 시간 창 설정

프로시저

단계 **1** 템플릿의 Report Sections 페이지에서 섹션에 대한 **Inherit Time Window(**시간 창 상속**)** 확인란(있는 경우)의 선택을 취소합니다.

단계 **2** 섹션의 로컬 시간 창을 변경하려면 **Time Window(**시간 창**)(**)를 클릭합니다.

참고 통계 테이블의 데이터가 있는 섹션에는 슬라이딩 시간 창만 포함할 수 있습니다.

단계 **3** Events Time Window(이벤트 시간 창)에서 **Apply(**적용**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

보고서 템플릿 섹션 이름 변경

프로시저

단계 **1** 보고서 템플릿 편집기에서 섹션 헤더에 있는 현재 섹션 이름을 클릭합니다.

단계 **2** 섹션의 새 이름을 입력합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

보고서 템플릿 섹션 미리 보기

미리 보기 기능은 테이블 보기의 필드 레이아웃과 정렬 순서, 그리고 원도표 색상과 같은 그래픽의 중요한 가독성 특성을 보여줍니다.

프로시저

단계 **1** 보고서 템플릿 섹션을 편집하는 동안 섹션에 대한 **Preview(**미리보기**)**를 클릭합니다.

단계 **2** **OK(**확인**)**를 클릭하여 미리보기를 닫습니다.

보고서 템플릿 섹션에서 검색

성공적인 보고서 생성의 핵심은 보고서 섹션을 채우는 검색을 정의하는 것입니다. Firepower System에서는 보고서 템플릿에서 사용할 수 있는 검색을 보고 새 맞춤형 검색을 정의할 수 있는 검색 편집기를 제공합니다.

보고서 템플릿 섹션에서 검색

프로시저

단계 **1** 보고서 템플릿의 관련 섹션에서 **Search(**검색**)** 필드 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **2** 사전 정의한 검색에서 맞춤형 검색을 기반으로 하려면, **Saved Searches(**저장된 검색**)** 드롭다운 목록에서 사정 정의한 검색을 선택해야 합니다.

이 목록에는 해당 테이블에 대해 사용할 수 있는 모든 사전 정의 검색(시스템 전체에 또는 특정 보고서에만 적용되는 검색 포함)이 포함됩니다.

단계 **3** 해당 필드에서 검색 기준을 수정합니다.

특정 필드에서는 제약 조건으로 이벤트 검색과 동일한 연산자(<, <> 등)를 포함할 수 있습니다. 여러 기준을 입력하면 모든 기준과 일치하는 레코드만 반환됩니다.

단계 **4** 제한 값을 입력하는 대신 드롭다운 메뉴에서 입력 매개변수를 삽입하려는 경우에는 **Input Parameter(**입력 매개변수**)** ( )를 클릭해야 합니다.

참고 보고 검색의 제약 조건을 수정하면 시스템은 수정된 검색을 *section* `custom search` 이름으로 저장합니다. 여기서 *section*은 섹션 제목 표시줄의 이름이며, 그 뒤에 `custom search` 문자열이 옵니다. 저장된 맞춤형 검색에 대해 의미 있는 이름을 지정하려면 수정된 검색을 저장하기 전에 섹션 이름을 변경해야 합니다. 저장된 보고 검색의 이름은 변경할 수 없습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

입력 매개변수

생성 시 보고서가 동적으로 업데이트할 수 있는 입력 파라미터를 보고서 템플릿에서 사용할 수 있습니다. **Input Parameter(**입력 매개변수**)** ( )는 처리 가능한 필드를 나타냅니다. 두 가지 종류의 입력 파라미터가 있습니다.

- 사전 정의 입력 파라미터는 내부 시스템 함수 또는 설정 정보에 의해 확인됩니다. 예를 들어 보고서 생성 시 시스템은 `$<Time>` 파라미터를 현재 날짜 및 시간과 교체합니다.
- 사용자 정의 입력 파라미터는 섹션 검색에서 제약을 제공합니다. 입력 파라미터로 검색을 제약하면 시스템은 보고서를 요청하는 사용자의 생성 시간에 값을 수집합니다. 이렇게 하면 템플릿

을 변경하지 않고도 데이터의 특별한 일부를 표시하도록 생성 시 보고서를 동적으로 맞춤화할 수 있습니다. 예를 들어 보고서 섹션 검색의 **Destination IP(**목적지 **IP)** 필드에 입력 파라미터를 제공할 수 있습니다. 그런 다음 보고서를 생성할 때 특정 부서의 데이터만 가져오려면 해당 부서의 IP 네트워크 세그먼트를 입력할 수 있습니다.

이메일(제목이나 본문), 보고서 파일 이름, 텍스트 섹션 등 보고서의 특정 필드에 동적 텍스트를 추가하려면 문자열 유형의 입력 파라미터를 정의할 수 있습니다. 동일한 템플릿을 사용하되 맞춤형된 보고서 파일 이름, 이메일 주소, 이메일 메시지 등을 사용하여 부서별로 보고서를 개별 설정할 수 있습니다.

사전 정의 입력 파라미터

표 ***45:*** 사전 정의 입력 파라미터

삽입할 파라미터	템플릿에 포함할 정보**:**
`$<Logo>`	선택한 업로드된 로고
`$<Report Title>`	보고서 제목
`$<Time>`	보고서가 실행된 날짜와 시간(1초 단위)
`$<Month>`	현재 월
`$<Year>`	현재 연도
`$<System Name>`	이름 management center
`$<Model Number>`	모델 번호 management center
`$<Time Window>`	현재 보고서 섹션에 적용된 시간 창
`$<Constraints>`	현재 보고서 섹션에 적용 된 검색 제약 조건

표 ***46:*** 사전 정의 입력 파라미터 사용법

매개변수	보고서 템플릿 커버 페이지	보고서 템플릿 보고서 제목	보고서 템플릿 섹션 설명	보고서 템플릿 텍스트 섹션	보고서 파일 이름 생성	보고서 이메일 제목**,** 본문 생성
`$<Logo>`	예	아니요	아니요	아니요	아니요	아니요
`$<Report Title>`	예	아니요	예	예	예	예
`$<Time>`	예	예	예	예	예	예
`$<Month>`	예	예	예	예	예	예
`$<Year>`	예	예	예	예	예	예
`$<System Name>`	예	예	예	예	예	예

매개변수	보고서 템플릿 커버 페이지	보고서 템플릿 보고서 제목	보고서 템플릿 섹션 설명	보고서 템플릿 텍스트 섹션	보고서 파일 이름 생성	보고서 이메일 제목, 본문 생성
`$<Model Number>`	예	예	예	예	예	예
`$<Time Window>`	아니요	아니요	예	아니요	아니요	아니요
`$<Constraints>`	아니요	아니요	예	아니요	아니요	아니요

사용자 정의 입력 파라미터

입력 파라미터를 사용하면 검색의 활용 범위를 확장할 수 있습니다. 입력 파라미터는 보고서를 요청하는 사용자의 생성 시간에 시스템에 값을 수집하도록 지시합니다. 이렇게 하면 검색을 변경하지 않고도 데이터의 특별한 일부를 표시하도록 생성 시 보고서를 동적으로 제한할 수 있습니다. 예를 들어 부서 수준에서 보안 이벤트를 드릴다운하는 보고서 섹션의 **Destination IP(**목적지 **IP)** 필드에 입력 파라미터를 제공할 수 있습니다. 보고서를 생성할 때 특정 부서의 데이터만 가져오려면 해당 부서의 IP 네트워크 세그먼트를 입력합니다.

입력 파라미터의 유형은 사용 가능한 검색 필드를 결정합니다. 유형은 적절한 필드에서만 사용할 수 있습니다. 예를 들어 문자열 유형으로 정의하는 사용자 파라미터는 텍스트 필드에 삽입할 수 있지만, IP 주소가 필요한 필드에는 사용할 수 없습니다.

정의하는 각 입력 파라미터에는 이름과 유형이 존재합니다.

표 ***47:*** 사용자 정의 입력 파라미터 유형

사용할 파라미터 유형	다음 데이터가 포함된 필드
네트워크/IP	CIDR 형식의 IP 주소 또는 네트워크 세그먼트
애플리케이션	애플리케이션 프로토콜, 클라이언트 애플리케이션 또는 웹 애플리케이션의 이름
이벤트 메시지	이벤트 보기 메시지
디바이스	management center 또는 매니지드 디바이스
사용자 이름	사용자 식별(예: 이니시에이터 사용자 및 응답자 사용자)
번호(VLAN ID, Snort ID, Vuln ID)	VLAN ID, Snort ID 또는 취약성 ID
문자열	애플리케이션이나 OS 버전, 메모, 설명 등의 텍스트 필드

사용자 정의 입력 파라미터 생성

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Add Input Parameter(**입력 매개변수 추가**)**( ) 버튼을 클릭합니다.

단계 **3** 파라미터 **Name(**이름**)**을 입력합니다.

단계 **4** **Type(**유형**)** 드롭다운 목록에서 값을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭하여 파라미터를 추가합니다.

단계 **6** **OK(**확인**)**를 클릭하여 편집기로 돌아갑니다.

사용자 정의 입력 파라미터 수정

보고서 템플릿의 **Input Parameters(**입력 파라미터**)** 섹션은 템플릿에 대해 사용할 수 있는 모든 사용자 정의 파라미터를 열거합니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** 수정할 매개변수 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** 새 **Name(**이름**)**을 입력합니다.

단계 **4** **Type(**유형**)** 드롭다운 목록을 사용하여 파라미터 유형을 변경합니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **6** 입력 매개 변수를 삭제하려는 경우에는 입력 매개변수 옆에 있는 **Delete(**삭제**)** ( )을 클릭하고 확인합니다.

단계 **7** **OK(**확인**)**를 클릭하여 보고서 템플릿 편집기로 돌아갑니다.

사용자 정의 입력 파라미터로 검색 제한

정의하는 입력 파라미터는 해당 파라미터 유형과 일치하는 검색 필드에서만 사용할 수 있습니다. 예를 들어 **Network/IP** 유형의 파라미터는 IP 주소 또는 CIDR 형식의 네트워크 세그먼트가 허용되는 필드에만 사용할 수 있습니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 섹션의 **Search(**검색**)** 필드 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

입력 매개변수를 사용할 수 있는 필드는 **Input Parameter(**입력 매개변수**)** ( )로 표시됩니다.

단계 **2** 필드 옆에 있는 **Input Parameter(**입력 매개변수**)** (+)를 클릭한 다음 드롭다운 메뉴에서 입력 매개변수를 선택합니다.

사용자 정의 입력 매개변수는 아이콘()으로 표시됩니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

보고서 템플릿의 문서 속성

보고서를 생성하기 전에 보고서 모양에 영향을 주는 문서 속성을 설정할 수 있습니다. 이러한 특성에는 선택적인 커버 페이지 및 목차가 포함됩니다. 일부 특성에 대한 지원은 선택한 보고서 형식(PDF, HTML 또는 CSV)에 따라 달라집니다.

표 ***48:*** 문서 속성 지원

특성	**PDF** 지원 여부	**HTML** 지원 여부	**CSV** 지원 여부
커버 페이지	예(로고 및 맞춤형 모양은 선택 사항)	예(로고 및 맞춤형 모양은 선택 사항)	아니요
목차	예	예	아니요
페이지 머리글 및 바닥글	예(필드의 텍스트 또는 로고는 선택 사항)	아니요	아니요
맞춤형 시작 페이지 번호	예	아니요	아니요
첫 페이지의 번호 억제 옵션	예	아니요	아니요

보고서 템플릿의 문서 속성 수정

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Add cover page(커버 페이지 추가) - 커버 페이지를 추가하려면 **Include Cover Page(**커버 페이지 추가**)** 확인란을 선택합니다.
- Customize cover page(커버 페이지 맞춤형) - 커버 페이지 디자인을 편집하는 방법은 커버 페이지 맞춤 설정, 558 페이지 섹션을 참조하십시오.
- Add table of contents(목차 추가) - 목차를 추가하라면 **Include Table of Contents(**목차 넣기**)** 확인란을 선택합니다.

- Manage logos(로고 관리) - 템플릿과 관련된 로고 이미지를 관리하는 방법은 보고서 템플릿 로고 관리, 558 페이지 섹션을 참조하십시오.
- Configure header and footer(머리글 및 바닥글 설정) - 템플릿의 머리글과 바닥글에 대한 요소를 지정하려면, **Header(**머리글**)** 및 **Footer(**바닥글**)** 필드의 드롭다운 목록을 사용하십시오.
- Set first page number(첫 번째 페이지 번호 설정) - 보고서 첫 번째 페이지의 페이지 번호를 지정하려면 **Page Number Start(**페이지 번호 시작**)** 값을 입력합니다.
- Show first page number(첫 번째 페이지 번호 표시) - 보고서 첫 번째 페이지에서 페이지 번호를 표시하려면 **Number First Page?(**첫 번째 페이지 번호 표시**)** 확인란을 선택합니다. 이 옵션을 선택하면 커버 페이지에는 번호가 지정되지 않습니다.

단계 **3** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

커버 페이지 맞춤 설정

보고서 템플릿의 커버 페이지를 맞춤형할 수 있습니다. 커버 페이지에서는 여러 글꼴 크기와 스타일(굵게, 기울임 등)의 풍부한 텍스트는 물론 입력 파라미터와 가져온 이미지도 사용할 수 있습니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Cover Page Design(**커버 페이지 디자인**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** 풍부한 텍스트 편집기 내에서 커버 페이지 디자인을 편집합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

보고서 템플릿 로고 관리

management center에 여러 로고를 저장하고 서로 다른 보고서 템플릿과 연결할 수 있습니다. 템플릿을 디자인할 때 로고 연결을 설정합니다. 템플릿을 내보내면 내보내기 패키지에 로고가 포함됩니다.

로고를 management center에 업로드하면 다음 대상에서 로고를 사용할 수 있습니다.

- management center의 모든 보고서 템플릿 또는
- 다중 도메인 구축의 경우에는 현재 도메인에 있는 모든 보고서 템플릿

로고 이미지는 GIF, JPG 또는 PNG 형식입니다.

보고서의 로고를 management center에 업로드된 JPG 이미지로 변경할 수 있습니다. 예를 들어 템플릿을 재사용하려면 다른 조직의 로고를 보고서와 연결할 수 있습니다.

업데이트된 로그는 삭제할 수 이습니다. 로고를 삭제하면 로고를 사용하는 모든 템플릿에서 해당 로고가 제거됩니다. 삭제는 취소할 수 없습니다. 사전 정의된 Cisco 로고는 삭제할 수 없습니다.

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

현재 템플릿과 연결된 로고는 **General Settings(**일반 설정**)**의 **Logo(**로고**)** 아래에 나타납니다.

단계 **2** 로고 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- Add(추가) - 새 로고 추가, 559 페이지에 설명된 대로 새 로고를 추가합니다.
- Change(변경) - 보고서 템플릿에 대한 로고 변경, 559 페이지에 설명된 대로 보고서 템플릿의 로고를 변경합니다.
- Delete(삭제) - 로고 삭제, 560 페이지에 설명된 대로 로고를 삭제합니다.

새 로고 추가

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Logo(**로고**)** 필드 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다.

단계 **3** **Upload Logo(**로고 업로드**)**를 클릭합니다.

단계 **4** **Browse(**찾기**)**를 클릭하고 파일의 위치로 이동한 다음 **Open(**열기**)**을 클릭합니다.

단계 **5** **Upload(**업로드**)**를 클릭합니다.

단계 **6** 새 로고를 현재 템플릿에 연결하려면 항목을 선택하고 **OK(**확인**)**를 클릭합니다.

보고서 템플릿에 대한 로고 변경

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Logo(**로고**)** 필드 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다.

단계 **3** Select Logo(로고 선택) 대화 상자에서 보고서 템플릿에 연결할 로고를 선택합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

로고 삭제

프로시저

단계 **1** 보고서 템플릿 편집기에서 **Advanced(**고급**)**를 클릭합니다.

단계 **2** **Logo(**로고**)** 필드 옆에 있는 **Edit(**수정**)** ( )를 클릭합니다.

단계 **3** Select Logo(로고 선택) 대화상자에서 삭제할 로고를 선택합니다.

단계 **4** **Delete Logo(**로고 삭제**)**를 클릭합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

보고서 템플릿 관리

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 보고서 템플릿을 표시하며, 이러한 템플릿은 편집할 수 있습니다. 상위 도메인에서 생성된 보고서 템플릿도 표시되지만, 이러한 템플릿은 편집할 수 없습니다. 하위 도메인에서 생성된 보고서 템플릿을 보고 편집하려면 해당 도메인으로 전환하십시오. 시스템은 현재 도메인에 생성된 보고서만 표시합니다.

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- Delete(삭제) - 삭제할 템플릿 옆에 있는 **Delete(**삭제**)** ( )을 클릭하고 확인합니다.

  시스템 제공 보고서 템플릿은 삭제할 수 없습니다. 보안 분석가는 자신이 생성한 보고서 템플릿만 삭제할 수 있습니다. 다중 도메인 구축의 경우에는 현재 도메인에 속한 보고서 템플릿만 삭제할 수 있습니다.

- Edit(편집) - 보고서 템플릿을 편집하는 방법은 보고서 템플릿 수정, 561 페이지 섹션을 참조하십시오.
- Export(내보내기) - 보고서 템플릿을 내보내는 방법은 보고서 템플릿 내보내기, 561 페이지 섹션을 참조하십시오.

  팁 표준 설정 내보내기 프로세스를 사용하여 보고서 템플릿을 내보낼 수도 있습니다(구성 내보내기, 526 페이지 참조).

- Import(가져오기) - 보고서 템플릿을 가져오는 방법은 구성 가져오기, 526 페이지 섹션을 참조하십시오.

보고서 템플릿 수정

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 보고서 템플릿을 표시하며, 이러한 템플릿은 편집할 수 있습니다. 상위 도메인에서 생성된 보고서 템플릿도 표시되지만, 이러한 템플릿은 편집할 수 없습니다. 하위 도메인에서 생성된 보고서 템플릿을 보고 편집하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 편집할 템플릿의 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 다음 옵션을 이용할 수 있습니다.

- 페이지 나누기를 추가합니다(보고서 템플릿에 페이지 나누기 추가, 551 페이지 참조).
- 텍스트 섹션을 추가합니다(보고서 템플릿에 텍스트 섹션 추가, 550 페이지 참조).
- 보고서 템플릿 구성, 548 페이지에 설명된 대로 섹션 콘텐츠를 구성합니다.
- 입력 파라미터를 생성합니다(사용자 정의 입력 파라미터 생성, 556 페이지 참조).
- 입력 파라미터를 편집합니다(사용자 정의 입력 파라미터 수정, 556 페이지 참조).
- 문서 속성을 편집합니다(보고서 템플릿의 문서 속성 수정, 557 페이지 참조).
- 템플릿 섹션을 검색합니다(보고서 템플릿 섹션에서 검색, 553 페이지 참조).
- **Advanced(**고급**)**를 클릭하여 보고서 템플릿의 문서 속성, 557 페이지에 설명된 대로 문서 속성을 설정합니다.
- 글로벌 타임 창을 설정합니다(보고서 템플릿 및 관련 섹션에 대한 글로벌 시간 창 설정, 551 페이지 참조).
- 로컬 타임 창을 설정합니다(보고서 템플릿 섹션에 대한 보고서 템플릿 섹션에 로컬 시간 창 설정, 552 페이지 참조).
- 검색 필드를 설정합니다(테이블 형식 섹션에 표시되는 검색 필드 설정, 550 페이지 참조).
- 테이블 및 데이터 형식을 설정합니다(보고서 템플릿 섹션에 대한 테이블 및 데이터 형식 설정, 549 페이지 참조).
- 검색 및 필터를 지정합니다(보고서 템플릿 섹션에 대한 검색 또는 필터 지정, 550 페이지 참조).

보고서 템플릿 내보내기

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**를 선택합니다.

단계 **2** **Report Templates(**보고서 템플릿**)**을 선택합니다.

단계 **3** 내보내려는 템플릿에 대해 **YouTube EDU** ( )을 클릭합니다.

단계 **4** **Save file(**파일 저장**)** 및 **OK(**확인**)**를 선택하여 파일을 로컬 컴퓨터에 저장합니다.

보고서 생성 정보

보고서 생성

보고서 템플릿을 생성 및 맞춤형했으면 이제 보고서를 생성할 준비가 된 것입니다. 생성 프로세스에서는 보고서의 형식(HTML, PDF 또는 CSV)을 선택할 수 있습니다. 제외한 섹션 이외의 모든 섹션에 일관된 기간을 적용하는 보고서의 전역 시간 창을 조정할 수도 있습니다.

PDF 보고서의 경우:

- 유니코드(UTF-8) 문자를 사용한 파일 이름은 지원되지 않습니다.
- 특정 유니코드 파일 이름(예: 파일 또는 악성코드 이벤트에 나타나는 이름)이 포함된 보고서 섹션에는 이러한 파일 이름이 음역 형식으로 표시됩니다.
- 각 보고서 섹션에 설정된 결과의 설정 숫자는 특정 한도 이내여야 합니다. 해당 한도를 확인하려면 보고서 템플릿에 표시되는 노란색 삼각형 위에 마우스 포인터를 올리십시오.

보고서 템플릿의 검색 사양에 사용자 입력 파라미터가 포함된 경우 일반 프로세스에서는 값을 입력하라는 프롬프트가 표시됩니다. 이러한 값은 데이터 일부에 대한 보고서 실행을 맞춤화합니다.

DNS 서버가 구성되어 있고 IP 주소 확인이 활성화된 경우 확인에 성공하면 보고서에 호스트 이름이 포함됩니다.

다중 도메인 구축의 경우 상위 도메인에서 보고서를 생성할 때, 모든 하위 도메인의 결과가 포함될 수 있습니다. 특정 리프 도메인에 대한 보고서를 생성하려면 해당 도메인으로 전환합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 보고서를 생성하는 데 사용할 템플릿 옆에 있는 **Report(**보고서**)** ( )를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

팁 상위 템플릿의 보고서를 생성하려면 템플릿을 현재 도메인으로 복사합니다.

단계 **4** 선택적으로, 보고서 이름을 설정합니다.

- 새 **File Name(**파일 이름**)**을 입력합니다. 새 이름을 입력하지 않는 경우 시스템은 보고서 템플릿에 지정된 이름을 사용합니다.

- 파일 이름에 하나 이상의 입력 매개변수를 추가하려면 **Input Parameter(**입력 매개변수**)** ( )를 사용하십시오.

단계 **5** HTML, PDF 또는 CSV를 클릭하여 보고서의 출력 형식을 선택합니다.

PDF 옵션이 흐리게 표시되는 경우에는, 하나 이상의 보고서 섹션에서 결과 설정 수가 너무 높을 수 있습니다. 구체적인 한도를 확인하려면 보고서 템플릿에서 노란색 삼각형을 찾은 다음 마우스 포인터를 옮기십시오.

단계 **6** 전역 시간 창을 변경하려면 **Time Window(**시간 창**)**( )를 클릭합니다.

참고 개별 보고서 섹션이 전역 설정을 상속하도록 구성된 경우에만 전역 시간 창 설정이 개별 보고서 섹션의 내용에 영향을 미칩니다.

단계 **7** **Input Parameters(**입력 파라미터**)** 섹션에 나타나는 필드의 값을 입력합니다.

팁 필드에 * 와일드카드 문자를 입력하여 사용자 파라미터를 무시할 수 있습니다. 이 경우 검색에 대한 사용자 파라미터의 제약 조건이 제거됩니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우 리터럴 IP 주소 또는 VLAN 태그를 사용하여 보고서 결과를 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **8** management center 설정에서 이메일 릴레이 호스트를 활성화한 경우, **Email(**이메일**)**을 클릭해 생성되는 보고서의 이메일 전송을 자동으로 처리하십시오.

단계 **9** 프롬프트가 표시되면 **Generate(**생성**)**를 클릭하고 확인합니다.

Generate(생성**)**를 클릭하면 일반 설정을 보고서 템플릿과 함께 저장합니다.

Close(닫기**)**을 클릭하면 선택한 내용은 세션 기간 동안에만 저장됩니다.

단계 **10** 다음 옵션을 이용할 수 있습니다.

- 보고서 링크를 클릭해 보고서를 새 창에서 표시합니다.
- **OK(**확인**)**를 클릭하여 보고서 템플릿 편집기로 돌아갑니다.

보고서 생성 옵션

보고서 생성 옵션을 설정해 다음 작업을 할 수 있습니다.

- 향후 보고서 생성을 일회 또는 반복 예약합니다. 보고서 생성 자동화, 509 페이지의 내용을 참조하십시오. 일별, 주별, 월별 등 전체 기간에 대한 일정을 맞춤형할 수 있습니다.
- 일정 관리기를 사용하여 이메일 보고서를 배포합니다. 작업을 예약하기 전에 먼저 보고서 템플릿과 메일 릴레이 호스트를 설정해야 합니다.
- 보고서를 생성할 때 보고서를 이메일 첨부파일로 수신자 목록에 자동으로 전송합니다. 보고서를 이메일로 전달하려면 메일 릴레이 호스트를 적절히 구성해야 합니다.

- 새로 생성한 보고서 파일을 설정된 원격 스토리지 위치에 저장합니다. 원격 스토리지를 사용하려면 먼저 원격 스토리지 위치를 설정해야 합니다.

참고 원격으로 저장한 후 로컬 스토리지로 전환하는 경우 원격 스토리지의 보고서가 Reports 탭 목록에 나타나지 않습니다. 마찬가지로, 원격 스토리지 위치 간에 전환하면 이전 위치의 보고서가 목록에 나타나지 않습니다.

생성 시 이메일로 보고서 배포

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports Templates(**보고서 템플릿**)**를 클릭합니다.

단계 **3** 보고서를 생성하는 데 사용할 템플릿 옆에 있는 **Report(**보고서**)** ( )를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

팁 상위 템플릿의 보고서를 생성하려면 템플릿을 현재 도메인으로 복사합니다.

단계 **4** 창의 **Email(**이메일**)** 섹션을 확장합니다.

단계 **5** **Email Options(**이메일 옵션**)** 필드에서 **Send Email(**이메일 전송**)**을 선택합니다.

단계 **6** **Recipient List**, **CC** 및 **BCC** 필드에서 쉼표로 구분된 목록에 수신자의 이메일 주소를 입력합니다.

단계 **7** **Subject(**제목**)** 필드에 이메일 제목을 입력합니다.

팁 타임스탬프나 management center의 이름과 같은 정보를 이메일에서 동적으로 생성하려면 **Subject(**제목**)** 필드 및 메시지 본문에 입력 파라미터를 제공할 수 있습니다.

단계 **8** 필요에 따라 이메일 본문에 설명 내용을 입력합니다.

단계 **9** **OK(**확인**)**를 클릭하고 확인합니다.

관련 항목

메일 릴레이 호스트 및 알림 주소 구성, 62 페이지

향후 보고서 예약

보고서 생성 자동화, 509 페이지의 내용을 참조하십시오.

생성된 보고서 작업 정보

Reports(보고서) 탭 페이지에 있는 이전에 생성한 보고서에 액세스하고 관련 작업을 합니다.

보고서 보기

Reports(보고서)에는 보고서 이름, 생성 날짜와 시간, 생성 사용자, 보고서가 로컬에 저장되었는지 원격에 저장되었는지 등의 정보와 함께 전에 생성된 모든 보고서가 나열됩니다. 상태 열에는 보고서가 이미 생성되었는지, 생성 대기열에 있는지(예: 예약된 작업) 또는 (디스크 공간 부족 등의 이유로) 생성에 실패했는지 등이 나타납니다.

Administrator(관리자) 액세스 권한이 있는 사용자는 모든 보고서를 볼 수 있습니다. 다른 사용자는 자신이 생성한 보고서만 볼 수 있습니다.

다중 도메인 구축의 경우에는 현재 도메인에서 생성한 보고서만 볼 수 있습니다.

Reports(보고서) 페이지에는 로컬에 저장된 모든 보고서가 표시됩니다. 현재 원격 스토리지가 구성된 경우 원격으로 저장된 보고서도 표시됩니다. 원격으로 저장한 보고서의 **Location(**위치**)** 열 데이터는 `Remote(원격)` 입니다.

참고 원격으로 저장한 후 로컬 스토리지로 전환하는 경우 원격 스토리지의 보고서가 Reports 탭 목록에 나타나지 않습니다. 마찬가지로, 원격 스토리지 위치 간에 전환하면 이전 위치의 보고서가 목록에 나타나지 않습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports(**보고서**)**를 클릭합니다.

단계 **3** 확인할 보고서를 클릭합니다.

보고서 다운로드

원하는 보고서 파일을 로컬 컴퓨터로 다운로드할 수 있습니다. 이곳에서는 보고서 파일을 이메일로 전송하거나 다른 사용 가능한 수단을 통해 전자 방식으로 배포할 수 있습니다.

다중 도메인 구축의 경우에는 현재 도메인에서 생성한 보고서만 다운로드할 수 있습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports(**보고서**)**를 클릭합니다.

단계 **3** 다운로드할 보고서 옆에 있는 확인란을 선택하고 **Download(**다운로드**)**를 선택합니다.

팁 페이지의 모든 보고서를 다운로드하려면 페이지 상단 왼쪽에 있는 확인란을 클릭합니다. 보고서에 여러 페이지가 있는 경우 클릭하면 모든 페이지의 모든 보고서를 다운로드하는 두 번째 확인란이 나타납니다.

단계 **4** 브라우저의 프롬프트에 따라 보고서를 다운로드합니다. 여러 보고서를 선택하면 단일 `.zip` 파일로 다운로드됩니다.

보고서 원격 저장

현재 구성된 보고서 스토리지의 위치는 Overview(개요)> Reporting(보고) > Reports(보고서) 아래쪽에 로컬, NFS 및 SMB 스토리지에 대한 디스크 사용량과 함께 나타납니다. SSH를 사용하여 원격 스토리지에 액세스하는 경우 디스크 사용량 데이터를 사용할 수 없습니다.

참고 원격으로 저장한 후 로컬 스토리지로 전환하는 경우 원격 스토리지의 보고서가 Reports 탭 목록에 나타나지 않습니다. 마찬가지로, 원격 스토리지 위치 간에 전환하면 이전 위치의 보고서가 목록에 나타나지 않습니다.

시작하기 전에

- 원격 스토리지 디바이스, 95 페이지에 설명된 대로 원격 스토리지 위치를 구성합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports(**보고서**)**를 선택합니다.

단계 **3** 페이지 아래쪽에서 **Enable Remote Storage of Reports(**보고서의 원격 스토리지 활성화**)** 확인란을 선택합니다.

다음에 수행할 작업

- 보고서를 원격 스토리지에서 원격 스토리지로 옮깁니다(원격 스토리지로 보고서 이동, 567 페이지 참조).

관련 항목

원격 스토리지 디바이스, 95 페이지
원격 스토리지로 보고서 이동, 567 페이지

원격 스토리지로 보고서 이동

배치 모드에서 또는 단독으로 로컬 스토리지의 보고서를 원격 스토리지 위치로 옮길 수 있습니다.

참고 원격으로 저장한 후 로컬 스토리지로 전환하는 경우 원격 스토리지의 보고서가 Reports 탭 목록에 나타나지 않습니다. 마찬가지로, 원격 스토리지 위치 간에 전환하면 이전 위치의 보고서가 목록에 나타나지 않습니다.

시작하기 전에

- 원격 스토리지 디바이스, 95 페이지에 설명된 대로 원격 스토리지 위치를 구성합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports(**보고서**)**를 선택합니다.

단계 **3** 이동할 보고서 옆에 있는 확인란을 선택하고 **Move(**이동**)**를 클릭합니다.

팁 페이지의 모든 보고서를 옮기려면 페이지 상단 왼쪽에 있는 확인란을 선택합니다. 보고서에 여러 페이지가 있는 경우 선택하면 모든 페이지의 모든 보고서를 옮길 수 있는 두 번째 확인란이 나타납니다.

단계 **4** 보고서 이동 여부를 확인합니다.

보고서 삭제

언제든지 보고서 파일을 삭제할 수 있습니다. 이 절차를 수행하면 파일이 완전히 제거되며 복구할 수 없습니다. 보고서를 생성 한 보고서 템플릿이 여전히 있지만 시간 창이 확장 또는 슬라이딩 되는 경우 특정 보고서 파일을 다시 생성 하기 어려울 수 있습니다. 템플릿에서 입력 파라미터를 사용하는 경우에도 재생성이 어려울 수 있습니다.

다중 도메인 구축의 경우에는 현재 도메인에서 생성한 보고서만 삭제할 수 있습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Reporting(**보고**)**을(를) 선택합니다.

단계 **2** **Reports(**보고서**)**를 클릭합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- Delete selected(선택사항 삭제) - 삭제할 보고서 옆에 있는 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.
- Delete all(모두 삭제) - 페이지의 모든 보고서를 삭제하려면 페이지 상단 왼쪽에 있는 확인란을 선택합니다. 보고서에 여러 페이지가 있는 경우 선택하면 모든 페이지의 모든 보고서를 삭제할 수 있는 두 번째 확인란이 나타납니다.

단계 **4** 삭제를 확인합니다.

보고 기록

기능	버전	세부 사항
보고서 템플릿에서 연결 이벤트에 대한 데이터 소스 선택	7.0	Security Analytics and Logging(보안 애널리틱스)를 사용하여 원격 데이터 스토리지를 구성하기 위해 마법사를 사용하는 경우 해당 볼륨에 저장된 데이터를 보고서에 포함하도록 선택할 수 있습니다. 수정된 페이지: 보고서 템플릿
취약점 보고서의 변경 사항	6.7	보고서 출력이 Bugtraq 데이터의 가용성이 부족하도록 조정되었습니다.

20 장

알림 응답을 사용한 외부 알림

다음 주제에서는 알림 응답을 사용하여 외부 이벤트 알림을 Secure Firewall Management Center에서 전송하는 방법을 설명합니다.

Secure Firewall Management Center 알림 응답

SNMP, 시스템 로그 또는 이메일을 통한 외부 이벤트 알림으로 중요 시스템 모니터링을 지원할 수 있습니다. Secure Firewall Management Center은(는) 설정 가능한 알림 응답을 이용해 외부 서버와 상호 작용합니다. 알림 응답은 이메일, SNMP 또는 시스템 로그 서버와의 연결을 나타나는 설정입니다. 응답이라고 부르는데, 이들을 이용해 Firepower가 탐지한 이벤트에 대한 응답으로 알림을 보낼 수 있기 때문입니다. 여러 알림 응답을 설정해 다양한 유형의 알림을 다양한 모니터링 서버 또는 사람에게 전송할 수 있습니다.

참고 디바이스와 Firepower 버전에 따라, 알림 응답이 시스템 로그 메시지를 전송하는 최상의 방법이 아닐 수도 있습니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드 및 보안 이벤트 시스템 로그 메시지 구성 모범 사례, 655 페이지의 시스템 로그 정보 장을 참조하십시오. .

참고 알림 응답을 사용하는 알림은 Secure Firewall Management Center(으)로 전송합니다. 알림 응답을 사용하지 않는 침입 이메일 알림도 Secure Firewall Management Center(으)로 전송합니다. 반면 개별 침입 규칙 트리거링에 기반을 두는 SNMP와 시스템 로그 알림은 매니지드 디바이스가 직접 전송합니다. 자세한 내용은 침입 이벤트에 대한 외부 알림, 579 페이지을 참조하십시오.

대부분의 경우 외부 알림에 있는 정보는 데이터베이스에 기록한 연결된 이벤트에 있는 정보와 동일합니다. 하지만 상관관계 규칙이 연결 추적기를 포함하는 상관관계 이벤트 알림의 경우, 수신하는 정보는 기본 이벤트 유형에 상관없이 트래픽 프로파일 변경에 대한 알림에 대한 정보와 동일합니다.

Alerts(알림) 페이지(**Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**)에서 알림 응답을 생성하고 관리합니다. 새 알림 응답은 자동으로 활성화됩니다. 알림 생성을 일시적으로 중단하려면, 알림 응답을 삭제하지 말고 비활성화하면 됩니다.

알림 응답 변경 사항은 즉시 적용되지만, 연결 로그를 SNMP 트랩 또는 시스템 로그 서버로 전송할 때는 예외입니다.

다중 도메인 구축의 경우에는, 알림 응답을 생성하면 해당 응답은 현재 도메인에 속하게 됩니다. 이 알림 응답은 하위 도메인이 사용할 수도 있습니다.

알림 응답 지원 구성

알림 응답 생성이 끝나면 이를 이용해 다음과 같은 외부 알림을 Secure Firewall Management Center에서 전송할 수 있습니다.

알림/이벤트 유형	추가 정보
영향 플래그별 침입 이벤트	영향 플래그 알림 설정, 576 페이지
유형별 검색 이벤트	검색 이벤트 알림 설정, 577 페이지
악성코드 대응 ("네트워크 기반")로 탐지한 악성코드 및 회귀 악성코드 이벤트	악성코드 대응 알림 설정, 577 페이지
상관관계 정책 위반별 상관관계 이벤트	규칙 및 허용 리스트에 응답 추가, 1020 페이지
로깅 규칙 또는 기본 작업별 연결 이벤트(이메일 알림은 지원되지 않음)	로깅할 수 있는 기타 연결, 755 페이지
상태 모듈 및 심각도 수준별 상태 이벤트	상태 모니터 알림 생성, 390 페이지

알림 응답 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

SNMP 알림 응답 생성

를 제외하고 디바이스 유형에 대해 SNMPv1, SNMPv2 또는 SNMPv3threat defense를 사용하여 SNMP 알림 응답을 만들 수 있습니다.

참고 SNMP 프로토콜을 위한 SNMP 버전을 선택하는 경우, SNMPv2는 일기 전용 커뮤니티만 지원하며 SNMPv3는 읽기 전용 사용자만 지원한다는 사실을 유념하십시오. SNMPv3는 AES128을 이용한 암호화도 지원합니다.

SNMP로 64비트 값을 모니터링하려는 경우, SNMPv2 또는 SNMPv3을 사용해야 합니다. SNMPv1은 64비트 모니터링을 지원하지 않습니다.

시작하기 전에

- 네트워크 관리 시스템에 Secure Firewall Management Center의 관리 정보 베이스(MIB) 파일이 필요한 경우 `/etc/sf/DCEALERT.MIB`에서 가져올 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Create Alert(**알림 생성**)** 드롭다운 메뉴에서 **Create SNMP Alert(SNMP** 알림 생성**)**을 선택합니다.

단계 **3** SNMP Alert Configuration(SNMP 알림 구성) 필드를 편집합니다.

a) **Name(**이름**)** - SNMP 응답 식별을 위한 이름을 입력합니다.

b) **Trap Server(**트랩 서버**)** - SNMP 트랩 서버의 호스트 이름 또는 IP 주소를 입력합니다.

참고 이 필드에 유효하지 않은 IPv4 주소(예를 들어 192.169.1.456)를 입력한다고 해도 시스템에서 경고하지 않는다는 점에 유의하십시오. 잘못된 주소는 호스트 이름으로 처리됩니다.

c) **Version(**버전**)** - 드롭다운 목록에서 사용하려는 SNMP 버전을 선택합니다. SNMPv3이 기본값입니다.

다음 중에서 선택합니다**.**

- **SNMPv1**or **SNMPv2**: **Community String(**커뮤니티 문자열**)** 필드에 읽기 전용 SNMP 커뮤니티 이름을 넣고 절차 종료로 건너뜁니다.

  참고 SNMP 커뮤니티 문자열 이름에는 특수문자(< > / % # & ? ', 등)를 포함하지 않습니다.

- **SNMP v3**의 경우: **User Name(**사용자 이름**)** 필드에 SNMP 서버로 인증하려는 사용자 이름을 입력하고 다음 단계로 넘어갑니다.

d) **Authentication Protocol(**인증 프로토콜**)** - 드롭다운 목록에서 인증을 암호화하는 데 사용할 프로토콜을 선택합니다.

다음 중에서 선택합니다**.**

- **MD5** — MD5(Message Digest 5) 해시 함수입니다.
- **SHA** — SHA(Secure Hash Algorithm) 해시 함수입니다.

e) **Authentication Password(**인증 비밀번호**)** - 인증을 활성화할 비밀번호를 입력합니다.

f) **Privacy Protocol(**프라이버시 프로토콜**)** —드롭다운 목록에서 개인 비밀번호를 암호화하는 데 사용할 프로토콜을 선택합니다.

다음 중에서 선택합니다**.**

- **DES** - 대칭 비밀 키 블록 알고리즘에서 56비트 키를 사용하는 데이터 암호화 표준(DES)입니다.
- **AES** — 대칭 암호 알고리즘에서 56비트 키를 사용하는 AES(Advanced Encryption Standard)입니다.
- **AES128** — 대칭 암호 알고리즘에서 128비트 키를 사용하는 AES입니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다.

g) **Privacy Password(**프라이버시 비밀번호**)** - SNMP 서버에 필요한 프라이버시 비밀번호를 입력합니다. 개인 비밀번호를 지정한 경우 프라이버시가 활성화되며, 인증 비밀번호도 반드시 지정해야 합니다.

h) **Engine ID(**엔진 **ID)** - 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.

Cisco에서는 Secure Firewall Management Center IP 주소의 16진수 버전을 사용할 것을 권장합니다. 예를 들어, Secure Firewall Management Center의 IP 주소가 10.1.1.77이면 0a01014D0을 사용합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

변경 사항은 즉시 적용됩니다. 단,

알림 응답을 사용해 연결 로그를 보내는 경우 해당 알림 응답을 편집한 후 설정 변경 사항을 구축해야 합니다.

시스템 로그 알림 응답 생성

syslog 알림 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.

시스템 로그 알림 응답을 생성할 때에는 어떤 유형의 기능이든 선택할 수 있지만, 모든 기능을 지원하는 모든 시스템 로그 서버가 아니라 현재의 시스템 로그 서버를 기반으로 합리적인 하나의 기능을 선택해야 합니다. UNIX syslog 서버의 경우, `syslog.conf` 파일은 어느 기능이 서버의 어느 로그 파일에 저장되는지 나타냅니다.

시작하기 전에

- 이 절차는 다양한 상황의 시스템 로그 메시지를 전송하기 위한 방법으로는 권장하지 않습니다.
- 시스템 로그 서버가 원격 메시지를 수락할 수 있는지 확인합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Create Alert(**알림 생성**)** 드롭다운 메뉴에서 **Create Syslog Alert(**시스템 로그 알림 생성**)**을 선택합니다.

단계 **3** 알림의 **Name(**이름**)**을 입력합니다.

단계 **4** **Host(**호스트**)** 필드에 시스템 로그 서버의 IP 주소나 호스트 이름을 입력합니다.

참고 이 필드에 유효하지 않은 IPv4 주소(예를 들어 192.168.1.456)를 입력한다고 해도 시스템에서 경고하지 않는다는 점에 유의하십시오. 잘못된 주소는 호스트 이름으로 처리됩니다.

단계 **5** 서버가 시스템 로그 메시지에 사용할 포트를 **Port(**포트**)** 필드에 입력합니다. 기본적으로 이 값은 514로 설정됩니다.

단계 **6** **Facility(**시설**)** 목록에서 시스템 로그 알림 시설, 574 페이지에 설명된 시설을 선택합니다.

단계 **7** **Severity(**심각도**)** 목록에서에 시스템 로그 심각도 레벨, 575 페이지에 설명된 심각도를 선택합니다.

단계 **8** **Tag(**태그**)** 필드에 시스템 로그 메시지와 함께 표시할 태그 이름을 입력합니다.

예를 들어 시스템 로그로 전송된 모든 메시지를 `FromMC` 앞에 오도록 하는 경우, 필드에 `FromMC`를 입력합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

변경 사항은 즉시 적용됩니다. 단,

알림 응답을 사용해 시스템 로그 서버로 연결 로그를 보내는 경우 해당 알림 응답을 편집한 후 설정 변경 사항을 구축해야 합니다.

이 알림 응답을 보안 이벤트를 위해 사용하려는 경우에는, 정책에서 알림 응답을 지정해야 합니다. 보안 이벤트 시스템 로그에 대한 구성 위치, 660 페이지의 내용을 참조하십시오.

시스템 로그 알림 시설

다음 표에는 선택 가능한 syslog 기능이 나와 있습니다.

표 ***49:*** 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 `CLOCK` 기능을 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.

기능	설명
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.

시스템 로그 심각도 레벨

다음 표에는 선택 가능한 표준 syslog 심각도 레벨이 나와 있습니다.

표 ***50:*** 시스템 로그 심각도 레벨

레벨	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.

이메일 알림 응답 생성

시작하기 전에

- Secure Firewall Management Center이(가) 자체 IP 주소를 역확인할 수 있는지 확인합니다.

- 메일 릴레이 호스트를 메일 릴레이 호스트 및 알림 주소 구성, 62 페이지에 설명된 대로 설정합니다.

참고 이메일 알림을 이용해 연결을 기록할 수는 없습니다.

프로시저

단계 1 **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 2 **Create Alert(**알림 생성**)** 드롭다운 메뉴에서 **Create Email Alert(**이메일 알림 생성**)**을 선택합니다.

단계 3 알림 응답의 **Name(**이름**)**을 입력합니다.

단계 4 **To(**수신인**)** 필드에 알림을 전송할 이메일 주소를 쉼표로 구분하여 입력합니다.

단계 5 **From(**발신인**)** 필드에 알림 전송자로 표시할 이메일 주소를 입력합니다.

단계 6 **Relay Host(**릴레이 호스트**)** 옆에 나열된 메일 서버가 알림을 전송하는 데 사용하려는 서버인지 확인합니다.

팁 이메일 서버를 변경하려면 **Edit(**수정**)** ( )을 클릭합니다.

단계 7 **Save(**저장**)**를 클릭합니다.

영향 플래그 알림 설정

특정 영향 플래그의 침입 이벤트가 발생할 때마다 알림을 전송하도록 시스템을 설정할 수 있습니다. 영향 플래그는 침입 데이터, 네트워크 검색 데이터 및 취약성 정보를 상호 연결하여, 침입이 네트워크에 미치는 영향을 평가하는 데 도움이 됩니다.

이러한 알림을 설정하려면 IPS 스마트 라이센스 또는 보호 클래식 라이센스가 있어야 합니다.

프로시저

단계 1 **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**를 선택합니다.

단계 2 **Impact Flag Alerts(**영향 플래그 알림**)**를 클릭합니다.

단계 3 **Alerts(**알림**)** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

팁 새 알림 응답을 생성하려면 드롭다운 목록에서 **New(**신규**)**을(를) 선택합니다.

단계 4 **Impact Configuration(**영향 설정**)** 섹션에서 적절한 확인란을 선택하여 각 영향 플래그에 대해 수신할 알림을 지정합니다.

영향 플래그 정의는 침입 이벤트 영향 레벨, 823 페이지 섹션을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭합니다.

검색 이벤트 알림 설정

특정 유형의 검색 이벤트가 발생할 때마다 알리도록 시스템을 설정할 수 있습니다.

시작하기 전에

- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 검색 정책 장에 설명된 대로 알림을 설정할 검색 이벤트 유형을 기록하도록 네트워크 검색 정책을 설정합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Discovery Event Alerts(**검색 이벤트 알림**)**를 클릭합니다.

단계 **3** **Alerts(**알림**)** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

팁 새 알림 응답을 생성하려면 드롭다운 목록에서 **New(**신규**)**을(를) 선택합니다.

단계 **4** **Events Configuration(**이벤트 설정**)** 섹션에서 각 검색 이벤트 유형에 대해 수신하고자 하는 알림에 해당하는 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

악성코드 대응 알림 설정

악성코드 대응 (네트워크용 AMP)가 회귀 이벤트를 포함한 악성코드 이벤트를 생성할 때마다(즉 "네트워크 기반 악성코드 이벤트"가 생성될 때마다) 알림을 전송하도록 시스템을 설정할 수 있습니다. AMP for Endpoints(엔드포인트용 AMP)("엔드포인트 기반 악성코드 이벤트")가 생성한 악성코드 이벤트에 대한 알림은 만들 수 없습니다.

시작하기 전에

- 악성코드 클라우드 조회를 수행하고 정책을 액세스 컨트롤 규칙과 연결하도록 파일 정책을 설정합니다.자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 액세스 제어 개요를 참조하십시오.
- 이러한 알림을 설정하려면 악성코드 방어 라이선스가 있어야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Advanced Malware Protections Alerts(**고급 악성코드 보호 알림**)**를 클릭합니다.

단계 **3** **Alerts(**알림**)** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

팁 새 알림 응답을 생성하려면 드롭다운 목록에서 **New(**신규**)**을(를) 선택합니다.

단계 **4** **Event Configuration(**이벤트 설정**)** 섹션에서 각 악성코드 이벤트 유형에 대해 수신하고자 하는 알림에 해당하는 확인란을 선택합니다.

All network-based malware events(모든 네트워크 기반 악성코드 이벤트**)**에는 **Retrospective Events(**회귀 이벤트**)**가 포함된다는 점에 유의하십시오.

(정의상, 네트워크 기반 악성코드 이벤트는 AMP for Endpoints(엔드포인트용 AMP)가 생성한 이벤트는 포함하지 않습니다.)

단계 **5** **Save(**저장**)**를 클릭합니다.

21 장

침입 이벤트에 대한 외부 알림

다음 주제에서는 침입 이벤트에 대한 외부 경고 설정 방법을 설명합니다.

침입 이벤트에 대한 외부 알림 정보

외부 침입 이벤트 알림으로 중요 시스템 모니터링을 지원할 수 있습니다.

- SNMP - 침입 정책별로 설정되며 매니지드 디바이스에서 전송됩니다. 침입 규칙별로 SNMP 알림을 활성화할 수 있습니다.
- Syslog(시스템 로그) - 침입 정책별로 설정되며 매니지드 디바이스에서 전송됩니다. 침입 규칙에서 시스템 로그 알림을 설정하는 경우, 정책의 모든 규칙에 대해 알림을 설정하게 됩니다.
- Email(이메일) - 모든 침입 정책에서 설정되며 Secure Firewall Management Center에서 전송합니다. 침입 규칙별로 이메일 알림을 활성화하고, 알림의 길이와 빈도를 제한할 수 있습니다.

침입 이벤트 억제 또는 임계값 설정을 설정하는 경우, 시스템은 규칙이 트리거될 때마다 침입 규칙을 생성하지는 않는다는 점을(그리고 그에 따라 알림을 전송하지 않을 수도 있음을) 유의하십시오.

다중 도메인 구축의 경우, 모든 도메인에서 외부 알림을 설정할 수 있습니다. 상위 도메인의 경우, 시스템은 하위 도메인의 침입 이벤트에 대한 알림을 생성합니다.

참고 또한 Secure Firewall Management Center은(는) SNMP, 시스템 로그, 이메일 알림 응답을 사용하여 다양한 유형의 외부 알림을 전송합니다(Secure Firewall Management Center 알림 응답, 569 페이지 참조). 시스템은 알림 응답을 이용해 개별 침입 이벤트를 바탕으로 알림을 보내지는 않습니다.

관련 항목

침입 정책의 침입 이벤트 알림 필터

침입 이벤트 외부 알림 라이선스 요구 사항

Threat Defense 라이선스

IPS

기본 라이선스

보호

침입 이벤트 외부 알림 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

침입 이벤트에 대한 SNMP 알림 설정

침입 정책에서 외부 SNMP 알림을 활성화하면, 개별 규칙을 설정해 트리거 시 SNMP 알림을 보낼 수 있습니다. 이러한 알림은 매니지드 디바이스에서 전송됩니다.

프로시저

단계 **1** 침입 정책 편집기의 탐색창에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **2** **SNMP Alerting(SNMP** 알림**)**이 **Enabled(**활성화**)**인지 확인하고 **Edit(**편집**)**를 클릭합니다.
페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다.

단계 **3** **SNMP** 버전을 클릭하고 침입 SNMP 알림 옵션, 581 페이지에 설명된 대로 설정 옵션을 지정합니다.

단계 **4** 탐색 창에서 **Rules(**규칙**)**를 클릭합니다.

단계 5 규칙 창에서 SNMP 알림을 설정할 규칙을 선택하고 **Alerting(**알림**)** > **Add SNMP Alert(SNMP** 알림 추가**)**을(를) 선택합니다.

단계 6 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 선택한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

침입 SNMP 알림 옵션

네트워크 관리 시스템에 Secure Firewall Management Center의 MIB(Management Information Base) 파일이 필요한 경우 `/etc/sf/DCEALERT.MIB`에서 가져올 수 있습니다.

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**)**을(를) 선택합니다. 그렇지 않은 경우에는 **as String(**문자열로**)**을 선택합니다. 예를 들어 HP OpenView는 **as String(**문자열로**)** 옵션이 필요합니다.
트랩 서버	SNMP 트랩 알림을 받을 서버입니다. 단일 IP 주소 또는 호스트 이름을 지정할 수 있습니다.
커뮤니티 문자열	커뮤니티 이름입니다.

SNMP v3 옵션

매니지드 디바이스는 SNMPv3 알림을 Engine ID 값으로 인코딩합니다. 알림을 디코딩할 때 SNMP 서버는 이 값을 요구합니다. 이 값은 전송하는 디바이스의 인터페이스 IP 주소의 16진수 버전으로, "01"이 붙습니다.

예를 들어 SNMP 알림을 전송하는 디바이스의 관리 인터페이스 IP 주소가 172.16.1.50인 경우, Engine ID 값은 0xAC10013201입니다.

옵션	설명
트랩 유형	경고에 나타나는 IP 주소를 사용할 트랩 유형입니다. 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 렌더링하는 경우, **as Binary(**이진으로**)**을(를) 선택합니다. 그렇지 않은 경우에는 **as String(**문자열로**)**을 선택합니다. 예를 들어 HP OpenView는 **as String(**문자열로**)** 옵션이 필요합니다.
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.
개인 비밀번호	프라이버시를 위한 SNMP 키입니다. SNMP v3은 이 비밀번호를 암호화하기 위해 데이터 암호화 표준(DES) 블록 암호를 사용합니다. SNMP v3 비밀번호를 입력할 때, 해당 비밀번호는 초기 구성 중에 일반 텍스트로 표시되지만 암호화된 형식으로 저장됩니다. 개인 비밀번호를 지정한 경우 프라이버시가 활성화되며, 인증 비밀번호도 반드시 지정해야 합니다.
User Name(사용자 이름)	SNMP 사용자 이름입니다.

침입 이벤트를 위한 시스템 로그 알림 설정

침입 정책에서 시스템 로그 알림을 활성화하면, 시스템은 모든 침입 이벤트를 매니지드 디바이스 자체 또는 외부 호스트의 시스템 로그로 전송합니다. 외부 호스트를 지정하는 경우, 시스템 로그 알림은 매니지드 디바이스에서 전송됩니다.

프로시저

단계 **1** 침입 정책 편집기의 탐색창에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

단계 **2** **Syslog Alerting(**시스템 로그 알림**)**이 **Enabled(**활성화**)**인지 확인하고 **Edit(**편집**)**를 클릭합니다.
페이지 하단의 메시지는 구성을 포함하는 침입 정책 레이어를 식별합니다. **Syslog Alerting(**시스템 로그**)** 알림 페이지가 **Advanced Settings(**고급 설정**)**에 추가됩니다.

단계 **3** 시스템 로그 알림을 전송할 **Logging Hosts(**기록 호스트**)**의 IP 주소를 입력합니다.

Logging Hosts(기록 호스트**)** 필드를 입력하지 않는 경우 기록 호스트 상세정보는 연결된 Access Control Policy(액세스 컨트롤 정책)의 Logging(기록)에서 가져옵니다.

시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

단계 **4** 침입 시스템 로그 알림에 대한 기능 및 심각도, 583 페이지에 설명된 대로 **Facility(**시설**)** 및 **Severity(**심각도**)**을(를) 선택합니다.

단계 **5** 마지막 정책 커밋 이후 이 정책에서 변경한 사항을 저장하려면 **Policy Information(**정책 정보**)**을 선택한 다음 **Commit Changes(**변경사항 커밋**)**를 클릭합니다.

변경 사항을 커밋하지 않고 정책을 나갈 경우, 다른 정책을 수정하면 마지막 커밋 이후의 변경 사항이 취소됩니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

침입 시스템 로그 알림에 대한 기능 및 심각도

매니지드 디바이스는 기록 호스트가 알림을 분류할 수 있도록, 특정 시설 및 **Severity(**심각도**)**를 사용하여 침입 이벤트를 시스템 로그 알림으로 전송할 수 있습니다. 시설은 이를 생성한 하위 시스템을 지정합니다. 이러한 시설 및 **Severity(**심각도**)** 값은 실제 시스템 로그 메시지에는 표시되지 않습니다.

환경에 맞는 합리적인 값을 선택합니다. 로컬 설정 파일(UNIX 기반 기록 호스트에서의 syslog.conf 등)은 어떤 시설이 어떤 로그 파일에 저장되는지를 나타내기도 합니다.

시스템 로그 알림 시설

기능	설명
ALERT	알림 메시지입니다.
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.

기능	설명
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.

시스템 로그 알림 심각도

레벨	설명
EMERG	모든 사용자에게 알려진 위험 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

침입 이벤트에 대한 이메일 알림 설정

침입 이메일 알림을 활성화한 경우, 시스템은 침입을 매니지드 디바이스가 탐지했는지 침입 정책이 탐지했지와는 상관없이, 침입 이벤트 생성 시 이메일을 전송할 수 있습니다. 이러한 알림은 Secure Firewall Management Center에서 전송됩니다.

시작하기 전에

- 이메일 알림을 받을 메일 호스트 설정합니다(메일 릴레이 호스트 및 알림 주소 구성, 62 페이지 참조).
- Secure Firewall Management Center이(가) 자체 IP 주소를 역확인할 수 있는지 확인합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Alerts(**알림**)**을(를) 선택합니다.

단계 **2** **Intrusion Email(**침입 이메일**)**을 클릭합니다.

단계 **3** 알림을 생성할 침입 규칙 또는 규칙 그룹을 포함한, 알림 옵션을 침입 이메일 알림 옵션, 585 페이지에 설명된 대로 선택합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

침입 이메일 알림 옵션

On/Off(켜기/끄기**)**

침입 이메일 알림을 활성화 또는 비활성화합니다.

참고 활성화하면 개별 규칙을 선택하기 전에는 모든 규칙에 대한 알림이 활성화됩니다.

From/To Addresses(발신자/수신자 주소**)**

이메일 발신자 및 수신자입니다. 쉼표로 구분된 수신자 목록을 지정할 수 있습니다s.

최대 알림 및 빈도

Secure Firewall Management Center이(가) 시간 간격(**Frequency(**빈도**)**)마다 전송할 이메일 알림의 최대 수(**Max Alerts(**최대 알림**)**)입니다.

알림 병합

같은 소스 IP와 규칙 ID를 이용하는 알림을 그룹화하여 전송하는 알림 수를 줄입니다.

요약 출력

텍스트 제한 디바이스에 적합한 짧은 알림을 활성화합니다. 짧은 알림은 다음 정보를 포함합니다.

- 타임스탬프
- 프로토콜
- 소스 및 목적지 IP와 포트
- 메시지
- 동일한 소스 IP에 대해 생성되는 침입 이벤트의 수

예: `2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: 알 수 없는 Datagram 디코딩 문제! (116:108)`

Summary Output(요약 출력**)**을 활성화하는 경우에는 **Coalesce Alerts(**알림 병합**)** 활성화도 고려해보십시오. 텍스트 메시지 제한 초과 예방을 위해 **Max Alerts(**최대 알림**)**를 낮춰야 할 수도 있습니다.

표준 시간대

알림 타임스탬프의 시간대입니다.

특정 규칙 설정에 관한 이메일 알림

이메일 알림을 설정할 규칙을 선택할 수 있습니다.

VI 부

이벤트 및 자산 분석 툴

22 장

Context Explorer(상황 탐색기)

다음 주제에서는 Firepower System에서 Context Explorer(상황 탐색기)를 사용하는 방법을 설명합니다.

Context Explorer(상황 탐색기) 정보

Firepower System Context Explorer(상황 탐색기)는 애플리케이션에 대한 데이터, 애플리케이션 통계, 연결, 지리위치, IOC, 침입 이벤트, 호스트, 서버, 보안 인텔리전스, 사용자, 파일(악성코드 파일 포함), 관련 URL 등 모니터링 중인 네트워크의 상태에 대한 자세한 인터랙티브 그래픽 정보를 콘텍스트에 맞게 표시합니다. 개별 섹션은 이 데이터를 선명한 선, 막대, 파이, 도넛 그래프 형식과 자세한 목록으로 표시합니다. 첫 번째 섹션인 시간 경과에 따른 트래픽 및 이벤트 카운트의 선 그래프는 네트워크 활동의 최신 추세를 한눈에 볼 수 있는 그림을 제공합니다.

간편하게 맞춤형 필터를 만들고 적용하여 정밀 분석을 수행할 수 있으며, 그래프 영역을 클릭하거나 커서를 올려놓기만 하면 데이터 섹션을 자세히 확인할 수 있습니다. 또한 탐색기의 시간 범위를 마지막 시간 단위로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수도 있습니다. Administrator(관리자), Security Analyst(보안 분석가) 또는 Security Analyst(Read Only)(보안 분석가(읽기 전용)) 사용자 역할이 있는 사용자만 Context Explorer(상황 탐색기)에 액세스할 수 있습니다.

Firepower System 대시보드는 세부적으로 맞춤화 및 구획화할 수 있으며 실시간으로 업데이트됩니다. 반면 Context Explorer(상황 탐색기)는 수동으로 업데이트되고, 데이터에 대한 더 넓은 범위의 콘텍스트를 제공하도록 설계되었으며, 활성 사용자 탐색에 편리하도록 일관된 단일 레이아웃을 제공합니다.

특정 요구에 맞게 네트워크 및 어플라이언스에서 실시간 활동을 모니터링하려면 대시보드를 사용합니다. 반대로, 매우 세분화되고 분명한 상황에서 사전 정의된 최신 데이터 세트를 조사하려면 Context

Explorer(상황 탐색기)를 사용합니다. 예를 들어 네트워크의 호스트 중 15%만 Linux를 사용하지만 여기에서 거의 모든 YouTube 트래픽이 생성되는 경우 필터를 신속하게 적용하여 Linux 호스트 또는 YouTube 관련 애플리케이션 데이터만 보거나 두 가지 데이터를 모두 볼 수 있습니다. 간결하고 매우 집중적인 대시보드 위젯과는 달리 Context Explorer(상황 탐색기) 섹션은 시스템 활동을 Firepower System의 전문가는 물론 일반 사용자도 알기 쉬운 유용한 형식으로 시각적으로 표시하도록 설계되었습니다.

표시되는 데이터는 매니지드 디바이스 허가 및 구축 방법, 데이터를 제공하는 기능 설정 여부 등의 요소에 따라 달라집니다. 필터를 적용해 모든 Context Explorer(상황 탐색기) 섹션에 표시되는 데이터를 제한할 수도 있습니다.

다중 도메인 구축의 경우, Context Explorer(상황 탐색기)는 사용자가 상위 도메인에서 데이터를 확인할 때 모든 하위 도메인에서 집계된 데이터를 표시합니다. 리프 도메인의 경우에는 해당 도메인과 관련된 데이터만 확인할 수 있습니다.

대시보드 및 **Context Explorer** 간 차이

다음 표에는 대시보드와 Context Explorer(상황 탐색기)의 주요 차이점이 요약되어 있습니다.

표 ***51:*** 비교*:* 대시보드 및 ***Context Explorer(***상황 탐색기***)***

기능	대시보드	**Context Explorer(**상황 탐색기**)**
표시 가능한 데이터	Firepower System이 모니터링하는 모든 데이터	애플리케이션, 애플리케이션 통계, 지리위치, 호스트 침해 지표, 침입 이벤트, 파일(악성코드 파일 포함), 호스트, Security Intelligence(보안 인텔리전스) 이벤트, 서버, 사용자, URL
맞춤형 가능	• 대시보드를 맞춤형할 수 있는 위젯 선택 • 개별 위젯은 다양한 수준으로 맞춤형할 수 있음	• 기본 레이아웃은 변경 불가 • 적용된 필터는 탐색기 URL에 나타나며 나중에 사용하도록 북마크 처리 가능
데이터 업데이트 빈도	자동(기본값): 사용자가 구성함	수동
데이터 필터링	일부 위젯에 대해 가능(위젯 환경설정을 수정해야 함)	(탐색기의 모든 부분에 대해 가능하며 다중 필터 지원
그래픽 콘텍스트	일부 위젯(특히 Custom Analysis)은 데이터를 그래픽 형식으로 표시 가능	매우 자세한 도넛 그래프를 포함하여 폭넓은 그래픽 콘텍스트로 모든 데이터 표시 가능
관련 웹 인터페이스 페이지에 대한 링크	일부 위젯에서	모든 섹션에서
표시된 데이터의 시간 범위	사용자가 구성함	사용자가 구성함

관련 항목

대시보드 정보, 345 페이지

트래픽 및 침입 이벤트 횟수 시간 그래프

Context Explorer(상황 탐색기) 상단에는 시간 경과에 따른 트래픽 및 침입 이벤트의 선 그래프가 있습니다. X축은 시간 간격을 나타냅니다(선택한 시간 창에 따라 5분에서 1개월까지). Y축은 킬로바이트 단위의 트래픽(파란색 선) 및 침입 이벤트 카운트(빨간색 선)를 나타냅니다.

X축의 최소 간격은 5분입니다. 이를 위해 시스템에서는 선택한 기간의 시작 지점과 종료 지점을 가장 가까운 5분 간격으로 반올림합니다.

기본적으로 이 섹션에는 선택한 기간의 모든 네트워크 트래픽 및 생성된 모든 침입 이벤트가 표시됩니다. 필터를 적용하면 필터에 지정된 기준과 관련이 있는 트래픽 및 침입 이벤트만 표시하도록 차트가 변경됩니다. 예를 들어 `Windows`의 **OS Name**으로 필터링하면 시간 그래프에는 Windows 운영체제를 사용하는 호스트와 관련된 트래픽 및 이벤트만 표시됩니다.

침입 이벤트 데이터로 Context Explorer(상황 탐색기)를 필터링하면(예: **Priority**가 `High`) 침입 이벤트에 더 집중할 수 있도록 파란색 트래픽 선이 숨겨집니다.

트래픽 및 이벤트 카운트에 대한 정확한 정보를 보려면 포인터를 그래프 선의 특정 지점에 올려놓을 수 있습니다. 색이 있는 선 중 하나로 포인터를 가져가면 해당 선이 그래프 앞으로 이동하므로 콘텍스트를 더 자세히 볼 수 있습니다.

이 섹션에서는 주로 Intrusion Events(침입 이벤트) 및 Connection Events(연결 이벤트) 테이블의 데이터를 보여줍니다.

보안 침해 지표 섹션

Context Explorer의 IOC(Indications of Compromise, 보안 침해 지표) 섹션에는 모니터링되는 네트워크에서 감염 가능성이 있는 호스트를 전체적으로 보여주는 두 개의 인터랙티브 섹션이 있습니다. 이 둘은 각각 트리거된 가장 일반적인 IOC 유형의 비례 보기 및 트리거된 지표 수 기준의 호스트 보기입니다.

IOC에 관한 자세한 내용은 보안 침해 지표 데이터, 946 페이지 섹션을 참조하십시오.

지표별 호스트 그래프

도넛 형식의 Hosts by Indication 그래프는 모니터링되는 네트워크에서 호스트별로 트리거된 IOC의 비례 보기를 제공합니다. 내부 원에는 카테고리(예: `CnC Connected` 또는 `Malware Detected`)로 구분된 내용이 표시되며, 외부 원에는 특정 이벤트 유형(예: `Impact 2 Intrusion Event - attempted-admin` 또는 `Threat Detected in File Transfer`)별로 그러한 데이터가 더 자세히 구분되어 표시됩니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 및 Host IOC 테이블의 데이터를 주로 보여줍니다.

호스트별 지표 그래프

막대 형식의 Indications by Host 그래프에는 모니터링되는 네트워크에서 IOC가 가장 높은 호스트 15개에 의해 트리거된 고유한 보안 침해 지표(IOC)의 개수가 표시됩니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 및 Host IOC 테이블의 데이터를 주로 보여줍니다.

네트워크 정보 섹션

Context Explorer(상황 탐색기)의 Network Information(네트워크 정보) 섹션에는 소스, 목적지, 사용자, 트래픽과 관련된 보안 영역, 네트워크의 호스트에서 사용하는 운영체제 구분, Firepower System이 네트워크에서 수행한 액세스 컨트롤 작업의 비례 보기 등 모니터링되는 네트워크의 연결 트래픽을 전체적으로 표시하는 6개의 인터랙티브 그래프가 포함되어 있습니다.

운영 체제 그래프

도넛 형식의 Operating Systems 그래프는 모니터링하는 네트워크의 호스트에서 탐지한 운영체제의 비율을 표시합니다. 내부 원에는 OS 이름(예: `Windows` 또는 `Linux`)으로 구분된 내용이 표시되며, 외부 원에는 특정 운영체제 버전(예: `Windows Server 2008` 또는 `Linux 11.x`)별 데이터가 더 자세히 구분되어 표시됩니다. 일부 긴밀하게 연결된 운영체제(예: Windows 2000, Windows XP 및 Windows Server 2003)는 그룹화됩니다. 매우 드물거나 인식되지 않는 운영체제는 **Other(**기타**)**로 그룹화됩니다.

이 그래프는 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. 탐색기 시간 범위가 변경되어도 그래프는 변경되지 않습니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 테이블의 데이터를 주로 보여줍니다.

소스 **IP**별 트래픽 그래프

막대 형식의 Traffic by Source IP 그래프는 모니터링되는 네트워크에서 가장 활발한 소스 IP 주소 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 소스 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Source IP 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

소스 사용자별 트래픽 그래프

막대 형식의 Traffic by Source User 그래프는 모니터링되는 네트워크에서 가장 활발한 소스 사용자 15명에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 소스 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Source User 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다. 신뢰할 수 있는 사용자 데이터를 표시합니다.

액세스 제어 작업별 연결 그래프

원 형식의 Connections by Access Control Action 그래프는 Firepower System이 모니터링되는 트래픽에서 수행한 액세스 컨트롤 작업(예: `Block(차단)` 또는 `Allow(허용)`)의 비례 보기를 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Source User 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

대상 **IP**별 트래픽 그래프

막대 형식의 Traffic by Destination IP 그래프는 모니터링되는 네트워크에서 가장 활발한 목적지 IP 주소 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 목적지 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Destination IP 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

인그레스/이그레스 보안 영역별 트래픽 그래프

막대 형식의 Traffic by Ingress/Egress Security Zone 그래프는 모니터링되는 네트워크에 구성된 각 보안 영역에 대한 들어오는 또는 나가는 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 필요에 따라 Ingress(기본값) 또는 Egress 보안 영역 정보를 표시하도록 이 그래프를 구성할 수 있습니다.

나열된 각 보안 영역에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 이그레스 보안 영역 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Egress**를 클릭합니다. 기본 보기로 돌아가려면 **Ingress**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Ingress 보기로 돌아갑니다.

참고 침입 이벤트 정보에 대해 필터링하면 Traffic by Ingress/Egress Security Zone 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

애플리케이션 정보 섹션

Context Explorer(상황 탐색기)의 Application Information(애플리케이션 정보) 섹션에는 모니터링되는 네트워크에서 전반적인 애플리케이션 활동 내용을 보여주는 인터랙티브 그래프 3개 및 테이블 형식의 목록 1개가 있습니다. 트래픽, 침입 이벤트, 애플리케이션과 관련된 호스트 등은 각 애플리케이션에 할당된 비즈니스 연관성 또는 추정 위험 단위로 더 세부적으로 구성됩니다. Application Details List(애플리케이션 상세정보 목록)는 위험, 비즈니스 연관성, 카테고리 및 호스트 카운트의 인터랙티브 목록을 제공합니다.

이 섹션의 모든 "애플리케이션" 인스턴스에서 기본적으로 애플리케이션 정보 그래프 집합은 특별히 애플리케이션 프로토콜(예: DNS 또는 SSH)을 검사합니다. 특별히 클라이언트 애플리케이션(예: PuTTY 또는 Firefox) 또는 웹 애플리케이션(예: Facebook 또는 Pandora)을 검사하도록 Application Information(애플리케이션 정보) 섹션을 설정할 수도 있습니다.

애플리케이션 정보 섹션 초점

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** **Application Protocol Information(**애플리케이션 프로토콜 정보**)** 섹션으로 포인터를 이동합니다.

참고 동일한 Context Explorer(상황 탐색기) 세션에서 전에 이 설정을 변경한 경우에는 섹션 제목이 **Client Application Information(**클라이언트 애플리케이션 정보**)** 또는 **Web Application Information(**웹 애플리케이션 정보**)**으로 표시될 수 있습니다.

단계 **3** **Application Protocol(**애플리케이션 프로토콜**)**, **Client Application(**클라이언트 애플리케이션**)** 또는 **Web Application(**웹 애플리케이션**)**을 클릭합니다.

위험/비즈니스 관련성 및 애플리케이션별 트래픽 그래프

도넛 형식의 Traffic by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크에서 탐지되는 애플리케이션 트래픽의 비례 표시를 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`)별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other(**기타**)**로 그룹화됩니다.

이 그래프는 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. 탐색기 시간 범위가 변경되어도 그래프는 변경되지 않습니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance(**비즈니스 연관성**)**를 클릭합니다. 기본 보기로 돌아가려면 **Risk(**위험**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Risk/Business Relevance and Application 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 및 Application Statistics(애플리케이션 통계) 테이블의 데이터를 주로 보여줍니다.

위험/비즈니스 관련성 및 애플리케이션별 침입 이벤트 그래프

도넛 형식의 Intrusion Events by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크 및 애플리케이션에서 탐지되는 침입 이벤트의 비례 표시를 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`)별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other(**기타**)**로 그룹화됩니다.

자세한 정보를 보려면 도넛 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다. 또는 해당되는 경우 애플리케이션 정보를 볼 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 침입 이벤트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance(**비즈니스 연관성**)**를 클릭합니다. 기본 보기로 돌아가려면 **Risk(**위험**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 및 Application Statistics(애플리케이션 통계) 테이블의 데이터를 주로 보여줍니다.

위험/비즈니스 관련성 및 애플리케이션별 호스트 그래프

도넛 형식의 Hosts by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크 및 애플리케이션에서 탐지되는 호스트의 비례 표시를 관련 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`) 별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other(**기타**)**로 그룹화됩니다.

자세한 정보를 보려면 도넛 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance(**비즈니스 연관성**)**를 클릭합니다. 기본 보기로 돌아가려면 **Risk(**위험**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

이 그래프에서는 Applications(애플리케이션) 테이블의 데이터를 주로 보여줍니다.

애플리케이션 상세정보 목록

Application Information(애플리케이션 정보) 섹션 아래쪽에는 Application Details List(애플리케이션 상세정보 목록)가 있습니다. 이 목록은 모니터링되는 네트워크에서 탐지되는 각 애플리케이션에 대한 예상 위험, 예상 비즈니스 연관성, 카테고리 및 호스트 카운트 정보를 제공하는 테이블입니다. 애플리케이션은 관련 호스트 카운트의 내림차순으로 나열됩니다.

Application Details List(애플리케이션 상세정보 목록) 테이블은 정렬할 수 없지만, 원하는 테이블 항목을 클릭하면 해당 정보로 필터링 또는 드릴다운할 수 있습니다. 또는 해당되는 경우 애플리케이션 정보를 볼 수 있습니다. 이 테이블에서는 Applications(애플리케이션) 테이블의 데이터를 주로 보여줍니다.

이 목록은 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. 탐색기 시간 범위가 변경되어도 목록은 변경되지 않습니다.

보안 인텔리전스 섹션

상황 탐색기의 Security Intelligence(보안 인텔리전스) 섹션에는 보안 인텔리전스에서 모니터링하거나 차단한 모니터링되는 네트워크의 트래픽을 전체적으로 보여주는 세 개의 인터랙티브 막대 그래프가 있습니다. 그래프에서 그러한 트래픽은 카테고리, 소스 IP 주소, 대상 IP 주소로 각각 정렬됩니다. 트래픽의 양(초당 킬로바이트 단위) 및 해당 연결 수가 모두 나타납니다.

카테고리별 보안 인텔리전스 트래픽 그래프

막대 형식의 Security Intelligence Traffic by Category 그래프는 모니터링되는 네트워크에서 상위 보안 인텔리전스 카테고리에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Security Intelligence Traffic by Category 그래프는 표시되지 않습니다.

이 그래프에서는 Security Intelligence Events(보안 인텔리전스 이벤트) 테이블의 데이터를 주로 보여줍니다.

소스 IP별 보안 인텔리전스 트래픽 그래프

막대 형식의 Security Intelligence Traffic by Source IP 그래프는 모니터링되는 네트워크에서 보안 인텔리전스로 모니터링하는 트래픽의 상위 소스 IP 주소에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Security Intelligence Traffic by Source IP 그래프는 표시되지 않습니다.

이 그래프에서는 Security Intelligence Events(보안 인텔리전스 이벤트) 테이블의 데이터를 주로 보여줍니다.

대상 IP별 보안 인텔리전스 트래픽 그래프

막대 형식의 Security Intelligence Traffic by Destination IP 그래프는 모니터링되는 네트워크에서 보안 인텔리전스로 모니터링하는 트래픽의 상위 목적지 IP 주소에 대한 네트워크 트래픽(초당 킬로바이

트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Security Intelligence Traffic by Destination IP 그래프는 표시되지 않습니다.

이 그래프에서는 Security Intelligence Events(보안 인텔리전스 이벤트) 테이블의 데이터를 주로 보여줍니다.

침입 정보 섹션

Context Explorer(상황 탐색기)의 Intrusion Information(침입 정보) 섹션에는 모니터링되는 네트워크의 침입 이벤트를 전체적으로 보여주는 인터랙티브 그래프 6개와 테이블 형식의 목록 1개가 있습니다. 여기에는 영향 레벨, 공격 소스, 대상 목적지, 사용자, 우선순위 레벨, 침입 이벤트와 관련된 보안 영역과 더불어 침입 이벤트 분류, 우선순위 및 카운트의 자세한 목록이 포함됩니다.

영향별 침입 이벤트 그래프

원 형식의 Intrusion Events by Impact 그래프는 모니터링되는 네트워크에서 침입 이벤트의 비례 보기를 예상 영향 레벨(0~4)로 그룹화하여 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프는 침입 탐지(IDS 통계) 및 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 공격자 그래프

막대 형식의 Top Attackers 그래프는 모니터링되는 네트워크에서 상위 공격 호스트 IP 주소(이벤트를 일으키는)에 대한 침입 이벤트의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 사용자 그래프

막대 형식의 Top Users 그래프는 최고 침입 이벤트 카운트와 관련된 모니터링되는 네트워크의 사용자를 이벤트 카운트 단위로 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프는 침입 탐지(IDS) 사용자 통계 및 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다. 신뢰할 수 있는 사용자 데이터를 표시합니다.

우선 순위별 침입 이벤트 그래프

원 형식의 Intrusion Events by Priority 그래프는 모니터링되는 네트워크에서 침입 이벤트의 비례 보기를 예상 우선순위 레벨(예: `High`, `Medium` 또는 `Low`)로 그룹화하여 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 대상 그래프

막대 형식의 Top Targets 그래프는 모니터링되는 네트워크에서 상위 대상 호스트 IP 주소(이벤트를 일으키는 연결의 대상)에 대한 침입 이벤트의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 인그레스/이그레스 보안 영역 그래프

막대 형식의 Top Ingress/Egress Security Zones 그래프는 모니터링되는 네트워크에 설정된 각 보안 영역(그래프 설정에 따라 Ingress 또는 Egress)과 관련된 침입 이벤트의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 이그레스 보안 영역 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Egress**를 클릭합니다. 기본 보기로 돌아가려면 **Ingress**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Ingress 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

필요에 따라 Ingress(기본값) 또는 Egress 보안 영역 정보를 표시하도록 이 그래프를 구성할 수 있습니다.

침입 이벤트 상세정보 목록

Intrusion Information(침입 섹션 아래쪽에는 Intrusion Event Details List(침입 이벤트 상세정보 목록)이 있습니다. 이 목록은 모니터링되는 네트워크에서 탐지되는 각 침입 이벤트에 대한 분류, 예상 우선순위 및 이벤트 카운트 정보를 제공하는 테이블입니다. 이벤트는 이벤트 카운트의 내림차순으로 나열됩니다.

Intrusion Event Details List(침입 이벤트 상세정보 목록) 테이블은 정렬할 수 없지만, 원하는 테이블 항목을 클릭하면 해당 정보로 필터링 또는 드릴다운할 수 있습니다. 이 테이블에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

파일 정보 섹션

Context Explorer의 Files Information(파일 정보) 섹션에는 모니터링되는 네트워크의 파일 및 악성코드 이벤트를 전체적으로 표시하는 6개의 인터랙티브 그래프가 포함되어 있습니다.

6개 중 5개 그래프에는 악성코드 대응 (구 AMP for Firepower) 관련 데이터, 즉 네트워크 트래픽에서 탐지되는 파일의 악성코드 속성, 파일 형식, 파일 이름과 이러한 파일을 보내는(업로드) 호스트 및 받는(다운로드) 호스트가 표시됩니다. 마지막 그래프에는 악성코드 대응 또는 AMP for Endpoints가 조직에서 탐지한 모든 악성코드 위협이 표시됩니다.

참고 침입 정보에 대해 필터링하는 경우 전체 Files Information(파일 정보) 섹션은 표시되지 않습니다.

상위 파일 유형 그래프

도넛 형식의 Top File Types 그래프는 네트워크 트래픽에서 탐지되는 파일 형식(외부 원)의 비례 보기를 파일 카테고리(내부 원)로 그룹화하여 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 악성코드 대응 데이터를 표시하려면 악성코드 방어 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 파일 이름 그래프

막대 형식의 Top File Names 그래프는 네트워크 트래픽에서 탐지되는 고유한 상위 파일 이름의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 악성코드 대응 데이터를 표시하려면 악성코드 방어 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

성향별 파일 그래프

원 형식의 Top File Types 그래프는 악성코드 대응 기능(구 AMP for Firepower)으로 탐지한 악성코드 성향의 비율을 표시합니다. 성향은 Secure Firewall Management Center이(가) 악성코드 클라우드 조회를 수행한 파일에만 있습니다. 클라우드 조회를 트리거하지 않은 파일은 `N/A` 성향을 갖습니다. `Unavailable` 성향은 Secure Firewall Management Center에서 악성코드 클라우드 조회를 수행할 수 없음을 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 악성코드 대응 데이터를 표시하려면 악성코드 방어 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 호스트 전송 파일 그래프

막대 형식의 Top Hosts Sending Files 그래프는 상위 파일 전송 호스트 IP 주소에 대한 네트워크 트래픽에서 탐지되는 파일 수의 카운트를 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 악성코드 전송 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Malware(**악성코드**)**를 클릭합니다. 기본 파일 보기로 돌아가려면 **Files(**파일**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 파일 보기로 돌아갑니다.

이 그래프가 악성코드 대응 데이터를 표시하려면 악성코드 방어 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 호스트 수신 파일 그래프

막대 형식의 Top Hosts Receiving Files 그래프는 상위 파일 수신 호스트 IP 주소에 대한 네트워크 트래픽에서 탐지되는 파일 수의 카운트를 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 악성코드 수신 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Malware(**악성코드**)**를 클릭합니다. 기본 파일 보기로 돌아가려면 **Files(**파일**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 파일 보기로 돌아갑니다.

이 그래프가 악성코드 대응 데이터를 표시하려면 악성코드 방어 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 악성코드 탐지 그래프

막대 형식의 Top Malware Detections 그래프에는 악성코드 대응 또는 Secure Endpoint가 조직에서 탐지한 상위 악성코드 위협 숫자가 표시됩니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 악성코드 대응 데이터를 표시하려면 악성코드 방어 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 및 Malware Events(악성코드 이벤트) 테이블의 데이터를 주로 보여줍니다.

지리위치 정보 섹션

Context Explorer(상황 탐색기)의 Geolocation Information(지리위치 정보) 섹션에는 모니터링되는 네트워크의 호스트가 데이터를 교환하는 국가를 전체적으로 보여주는 3개의 인터랙티브 도넛 그래프가 있습니다. 이러한 그래프는 각각 이니시에이터 또는 응답자 국가 단위의 고유한 연결, 소스 또는 대상 국가 단위의 침입 이벤트, 수신 또는 송신 국가 단위의 파일 이벤트에 대한 것입니다.

이니시에이터/응답자 국가별 연결 그래프

도넛 형식의 Connections by Initiator/Responder Country 그래프는 이니시에이터(기본값) 또는 응답자로서 네트워크의 연결과 관련된 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 연결에서 응답자 역할을 하는 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Responder(**응답자**)**를 클릭합니다. 기본 보기로 돌아가려면 **Initiator(**이니시에이터**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Initiator 보기로 돌아갑니다.

이 그래프에서는 Connection Summary Data(연결 요약 데이터) 테이블의 데이터를 주로 보여줍니다.

소스/목적지 국가별 침입 이벤트 그래프

도넛 형식의 Intrusion Events by Source/Destination Country 그래프는 이벤트의 소스(기본값) 또는 목적지로서 네트워크의 침입 이벤트와 관련된 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 연결에서 침입 이벤트의 목적지 역할을 하는 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Destination(**목적지**)**을 클릭합니다. 기본 보기로 돌아가려면 **Source(**소스**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Source 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

전송/수신 국가별 파일 이벤트 그래프

도넛 형식의 File Events by Sending/Receiving Country 그래프는 네트워크의 파일 이벤트에서 파일을 전송하거나(기본값) 수신하는 것으로 탐지되는 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 파일 수신 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Receiver(**수신자**)**를 클릭합니다. 기본 보기로 돌아가려면 **Sender(**발신자**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Sender 보기로 돌아갑니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

URL 정보 섹션

Context Explorer의 URL Information 섹션에는 모니터링되는 사용자 네트워크의 호스트가 데이터를 교환하는 URL을 전체적으로 보여주는 3개의 인터랙티브 막대 그래프가 있습니다. 여기에는 URL과 연결된 트래픽 및 고유한 연결이 포함되며 개별 URL, URL 카테고리 및 URL 평판 단위로 정렬됩니다. URL 정보에 대해서는 필터링할 수 없습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 전체 URL Information(URL 정보) 섹션은 표시되지 않습니다.

이 그래프가 URL 범주 및 평판 데이터를 포함하려면 URL 라이선스가 있어야 합니다.

URL별 트래픽 그래프

막대 형식의 Traffic by URL 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by URL 그래프는 표시되지 않습니다.

이 그래프가 URL 범주 및 평판 데이터를 포함하려면 URL 라이선스가 있어야 합니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

URL 카테고리별 트래픽 그래프

막대 형식의 Traffic by URL Category 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 카테고리(예: `Search Engines(검색 엔진)` 또는 `Streaming Media(스트리밍 미디어)`)에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by URL Category 그래프는 표시되지 않습니다.

이 그래프가 URL 범주 및 평판 데이터를 포함하려면 URL 라이선스가 있어야 합니다.

이 그래프에서는 URL Statistics(URL 통계) 및 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

URL 평판별 트래픽 그래프

막대 형식의 Traffic by URL Reputation(URL 평판별 트래픽) 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 평판 그룹(예: , Trusted(신뢰할 수 있는), 또는 , Neutral(보통))에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL 평판에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by URL Reputation 그래프는 표시되지 않습니다.

이 그래프가 URL 범주 및 평판 데이터를 포함하려면 URL 라이선스가 있어야 합니다.

이 그래프에서는 URL Statistics(URL 통계) 및 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

Context Explorer 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 보안 분석가

Context Explorer(상황 탐색기) 새로 고침

Context Explorer(상황 탐색기)는 표시되는 정보를 자동으로 업데이트하지 않습니다. 새로운 데이터를 표시하려면 탐색기를 수동으로 새로 고쳐야 합니다.

Context Explorer(상황 탐색기) 자체를 다시 고치면(브라우저 프로그램을 새로 고치거나 Context Explorer(상황 탐색기)에서 나간 후 다시 돌아오는 방법 사용) 표시되는 모든 정보를 새로 고칠 수 있지만, 섹션 설정에 대해 변경한 내용(예: Ingress/Egress 그래프 및 애플리케이션 정보 섹션)이 유지되지 않으며 로딩에 지연이 발생할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** 오른쪽 위에 있는 **Reload(**다시 로드**)**를 클릭합니다.

새로 고침이 완료되기 전까지 **Reload(**다시 로드**)**는 흐리게 표시됩니다.

Context Explorer(상황 탐색기) 시간 범위 설정

Context Explorer(상황 탐색기)의 시간 범위를 마지막 시간 단위(기본값)로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수 있습니다. 시간 범위를 변경해도 변경 사항을 반영하여 Context Explorer(상황 탐색기)가 자동으로 업데이트되지는 않습니다. 새로운 시간 범위를 적용하려면 탐색기를 수동으로 새로 고쳐야 합니다.

Context Explorer(상황 탐색기)에서 빠져나가거나 로그인 세션을 종료해도 시간 범위에 대한 변경 사항은 유지됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** **Show the last(**마지막 선택 표시**)** 드롭다운 목록에서 시간 범위를 선택합니다.

단계 **3** 선택적으로, 새 시간 범위의 데이터를 보려면 **Reload(**다시 로드**)**를 클릭합니다.

팁 **Apply Filters(**필터 적용**)**를 클릭해도 시간 범위 업데이트가 적용됩니다.

Context Explorer(상황 탐색기) 섹션 최소화 및 최대화

하나 이상의 Context Explorer(상황 탐색기) 섹션을 최소화할 수 있습니다. 이는 특정 섹션에만 집중하거나 더 간단한 보기를 원하는 경우 유용합니다. Traffic and Intrusion Event Counts Time 그래프는 최소화할 수 없습니다.

페이지를 새로 고치거나 어플라이언스에서 로그아웃해도 최소화 또는 최대화 구성 상태는 Context Explorer(상황 탐색기) 섹션에서 그대로 유지됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** 섹션을 최소화하려는 경우에는 섹션 제목 표시줄의 **Collapse Arrow(**축소 화살표**)**( )를 클릭합니다.

단계 **3** 섹션을 최대화하려면 최소화된 섹션에서 제목 표시줄의 최대화(**Expand Arrow(**확장 화살표**)**( ))를 클릭합니다.

Context Explorer(상황 탐색기) 데이터에 대해 드릴다운

Context Explorer(상황 탐색기)에서 허용하는 것보다 더 자세히 그래프 또는 목록의 데이터를 검사하려면 관련 데이터의 테이블 보기로 드릴다운할 수 있습니다. (Traffic and Intrusion Events over Time 그래프에서는 드릴다운할 수 없습니다.) 예를 들어 Traffic by Source IP 그래프에서 IP 주소를 드릴다운하면 Connection Events(연결 이벤트) 테이블의 Connections with Application Details(애플리케이션 상세정보 연결) 보기가 표시되며, 선택한 소스 IP 주소와 연결된 데이터만 포함됩니다.

검사하는 데이터 유형에 따라 콘텍스트 메뉴에 추가 옵션이 표시될 수 있습니다. 특정 IP 주소와 관련된 데이터 포인트는 선택하는 IP 주소에서 호스트 또는 whois 정보를 볼 수 있는 옵션을 제공합니다. 특정 애플리케이션과 관련된 데이터 포인트는 선택하는 애플리케이션에 대한 애플리케이션 정보를 볼 수 있는 옵션을 제공합니다. 특정 사용자와 관련된 데이터 포인트는 해당 사용자의 사용자 프로파일 페이지를 볼 수 있는 옵션을 제공합니다. 침입 이벤트 메시지와 관련된 데이터 포인트는 해당 이벤트와 관련된 침입 규칙에 대한 규칙 문서를 볼 수 있는 옵션을 제공하며, 특정 IP 주소와 관련된 데이터 포인트는 해당 주소를 차단 또는 차단 금지 목록에 추가할 수 있는 옵션을 제공합니다. 이러한

목록에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 전역 및 도메인 보안 인텔리전스 목록을 참고하십시오.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(분석)** > **Context Explorer(상황 탐색기)**을(를) 선택합니다.

단계 **2** **Traffic and Intrusion Events over Time(시간 경과에 따른 트래픽 및 침입 이벤트)**을 제외한 임의의 섹션에서 조사하려는 데이터 포인트를 클릭합니다.

단계 **3** 선택한 데이터 포인트에 따라 여러 가지 옵션이 표시됩니다.

- 테이블 보기에서 이 데이터를 더 자세히 살펴보려면 **Drill into Analysis(분석을 위해 드릴다운)**를 선택합니다.
- 특정 IP 주소와 관련된 데이터 포인트를 선택했으며 관련 호스트에 대해 자세히 알아보려면 **View Host Information(호스트 정보 보기)**을 선택합니다.
- 특정 IP 주소의 데이터 포인트를 선택했으며 해당 주소에서 whois 검색을 수행하려면 **Whois**를 선택합니다.
- 특정 애플리케이션과 관련된 데이터 포인트를 선택했으며 해당 애플리케이션에 대해 자세히 알아보려면 **View Application Information(애플리케이션 정보 보기)**을 선택합니다.
- 특정 사용자와 관련된 데이터 포인트를 선택했으며 해당 사용자에 대해 자세히 알아보려면 **View User Information(사용자 정보 보기)**을 선택합니다.
- 특징 침입 이벤트 사용자와 관련된 데이터 포인트를 선택했으며 관련된 침입 규칙에 대해 자세히 알아보려면 **View Rule Documentation(규칙 문서 보기)**을 선택합니다. 원한다면 **Rule Documentation(규칙 문서)**을 클릭해 더 구체적인 규칙 상세정보를 확인합니다.
- 특정 IP 주소와 관련된 데이터 포인트를 선택했으며 해당 IP 주소를 보안 인텔리전스 전역 차단 및 차단 금지 목록에 추가하려면 적절한 옵션을 선택합니다.

Context Explorer의 필터

Context Explorer(상황 탐색기)에 처음 표시되는 기본적인 광범위한 데이터를 이용해 네트워크의 활동에 대해 좀 더 세부적인 콘텍스트를 얻기 위해 이러한 데이터를 필터링할 수 있는 옵션이 제공됩니다. 필터는 모든 유형의 Firepower System 데이터(URL 정보 제외)를 포괄하며, 포함과 제외를 지원하고, Context Explorer(상황 탐색기) 그래프 데이터 포인트에서 클릭하여 빠르게 적용될 수 있으며, 전체 Explorer에 영향을 미칩니다. 한 번에 최대 20개의 필터를 적용할 수 있습니다.

Context Explorer(상황 탐색기) 데이터에 여러 방법으로 필터를 추가할 수 있습니다.

- Add Filter(필터 추가) 대화 상자에서
- 탐색기에서 데이터 포인트를 선택한 경우 콘텍스트 메뉴에서

- 특정 상세정보 보기 페이지(Application Detail, Host Profile, Rule Detail 및 User Profile)에 나타나는 텍스트 링크에서 이러한 링크를 클릭하면 상세정보 보기 페이지의 관련 데이터에 따라 Context Explorer(상황 탐색기)가 자동으로 열리고 필터링이 수행됩니다. 예를 들어 사용자 `jenkins`에 대한 사용자 상세정보 페이지에서 Context Explorer(상황 탐색기) 링크를 클릭하면 해당 사용자와 관련된 데이터만 표시하도록 탐색기가 제한됩니다.

일부 필터 유형은 다른 유형과 호환되지 않습니다. 예를 들어 침입 이벤트(예: **Device** 및 **Inline Result**)와 관련된 필터는 연결 이벤트와 관련된 필터(예: **Access Control Action**)와 동시에 적용할 수 없습니다. 시스템에서 연결 이벤트 데이터와 침입 이벤트 데이터를 정렬할 수 없기 때문입니다. 시스템에서는 호환되지 않는 필터가 동시에 적용되는 것을 방지합니다. 한 필터 유형이 좀 더 최근에 활성화되었으면, 비호환성이 존재하는 한 호환되지 않는 유형의 필터는 표시되지 않습니다.

여러 필터가 활성화된 경우 동일한 데이터 유형에 대한 값은 OR 검색 기준으로 취급되므로, 적어도 하나의 값과 일치하는 모든 데이터가 표시됩니다. 서로 다른 데이터 유형에 대한 값은 AND 검색 기준으로 취급되므로, 데이터는 필터링하는 각 데이터 유형에 대해 적어도 하나의 값과 일치해야 합니다. 예를 들어 `Application: 2channel`, `Application: Reddit` 및 `User: edickinson` 필터 집합에 대해 나타나는 데이터는 사용자 `edickinson` 및**(AND)** 애플리케이션 `2channel` 또는**(OR)** 애플리케이션 `Reddit`과 관련이 있어야 합니다.

다중 도메인 구축의 경우 상위 도메인에서 Context Explorer(상황 탐색기)를 볼 때 여러 하위 도메인을 필터링할 수 있습니다. 이 경우 **IP Address(IP 주소)** 필터를 추가할 때 주의해야 합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 리터럴 IP 주소를 사용하여 이 설정을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

표시되는 데이터는 매니지드 디바이스 허가 및 구축 방법, 데이터를 제공하는 기능 설정 여부 등의 요소에 따라 달라집니다.

참고 필터는 필요한 정확한 Firepower 데이터 콘텍스트를 특정 시간에 얻기 위한 간단하고 민첩한 툴 역할을 합니다. 필터의 목적은 영구적인 설정 설정이 아니며, Context Explorer(상황 탐색기)에서 빠져나가거나 세션을 종료하면 필터도 사라집니다. 나중에 사용하기 위해 필터 설정을 보존하려면 필터링된 Context Explorer(상황 탐색기) 보기 저장, 612 페이지 섹션을 참조하십시오.

데이터 유형 필드 옵션

다음 표에는 필터로 이용할 수 있는 데이터 유형과 각 유형에 대한 예제 및 간단한 정의가 나열되어 있습니다.

표 ***52:*** 필터 데이터 유형

유형	값 예	정의
액세스 컨트롤 작업	`Allow(허용)`, `Block(차단)`	트래픽을 허용 또는 차단하기 위해 액세스 컨트롤 정책에서 수행하는 작업입니다.
애플리케이션 범주	`web browser(웹 브라우저)`, `email(이메일)`	애플리케이션의 가장 핵심적인 기능에 대한 일반 분류입니다.

유형	값 예	정의
애플리케이션 이름	Facebook, HTTP	애플리케이션의 이름입니다.
애플리케이션 위험성	Very High(매우 높음), Medium(중간)	애플리케이션의 예상 보안 위험입니다.
애플리케이션 태그	encrypts communications(통신 암호화), sends mail(메일 전송)	애플리케이션에 대한 추가 정보(애플리케이션에는 0부터 원하는 수만큼의 태그 포함 가능)입니다.
애플리케이션 유형	Client(클라이언트), Web Application(웹 애플리케이션)	애플리케이션 유형(application protocol, client 또는 web application)입니다.
사업 타당성	Very Low(매우 낮음), High(높음)	비즈니스 활동에 대한 애플리케이션의 예상 연관성(레크리에이션과 반대)입니다.
대륙	North America(북미), Asia(아시아)	모니터링되는 네트워크에서 탐지되는 라우팅 가능한 IP 주소와 관련된 대륙입니다.
국가	Canada(캐나다), Japan(일본)	모니터링되는 네트워크에서 탐지되는 라우팅 가능한 IP 주소와 관련된 국가입니다.
디바이스	device1.example.com, 192.168.1.3	모니터링되는 네트워크에 있는 디바이스의 이름 또는 IP 주소입니다.
도메인	Asia Division(아시아 부서), Europe Division(유럽 부서)	네트워크 활동을 그래프로 작성할 디바이스의 도메인입니다. 이 데이터 유형은 다중 도메인 구축에서만 표시됩니다.
이벤트 분류	Potential Corporate Policy Violation(잠재적 기업 정책 위반), Attempted Denial of Service(시도된 서비스 거부)	침입 이벤트에 대한 설명으로, 침입 이벤트를 트리거한 규칙, 디코더 또는 전처리기의 분류에 의해 결정됩니다.
이벤트 메시지	dns response(dns 응답), P2P	이벤트에 의해 생성되는 메시지로, 이벤트를 트리거한 규칙, 디코더 또는 전처리기에 의해 결정됩니다.
파일 속성	Malware(악성코드), Clean(클린)	Secure Firewall Management Center가 악성코드 클라우드 조회를 수행한 파일의 성향입니다.
파일 이름	Packages.bz2	네트워크 트래픽에서 탐지되는 파일의 이름입니다.
파일 SHA256	임의의 32비트 문자열	Secure Firewall Management Center에서 악성코드 클라우드 조회를 수행한 파일의 SHA-256 해시 값입니다.
파일 유형	GZ, SWF, MOV	네트워크 트래픽에서 탐지되는 파일 형식입니다.
파일 유형 카테고리	Archive(아카이브), Multimedia(멀티미디어), Executables(실행파일)	네트워크 트래픽에서 탐지되는 파일 형식의 일반 카테고리입니다.

유형	값 예	정의
IP 주소	`192.168.1.3`, `2001:0db8:85a3::0000/24`	IPv4 또는 IPv6 주소, 주소 범위 또는 주소 블록입니다. IP 주소를 검색하면 이벤트가 반환되는데, 여기서 해당 주소는 이벤트의 소스 또는 대상입니다.
영향 레벨	`Impact Level 1(영향 레벨 1)`, `Impact Level 2(영향 레벨 2)`	모니터링되는 네트워크에서 이벤트의 예상 영향입니다.
인라인 결과	`dropped(삭제됨)`, `would have dropped(삭제된 것으로 추정됨)`	트래픽이 삭제되었는지, 삭제된 것으로 추정되는지 또는 시스템에 의해 작동되지 않았는지의 여부입니다.
IOC 카테고리	`High Impact Attack(강력한 공격)`, `Malware Detected(악성코드 탐지)`	트리거된 IOC(Indications of Compromise) 이벤트에 대한 카테고리입니다.
IOC 이벤트 유형	`exploit-kit`, `malware-backdoor`	특정 IOC(Indications of Compromise)와 관련된 식별자로, 이를 트리거한 이벤트를 가리킵니다.
악성코드 위협 이름	`W32.Trojan.a6b1`	악성코드 위협의 이름입니다.
OS 이름	`Windows`, `Linux`	운영체제의 이름입니다.
OS 버전	`XP`, `2.6`	운영체제의 특정 버전입니다.
우선순위	`high(높음)`, `low(낮음)`	이벤트의 예상 긴급도입니다.
보안 인텔리전스 범주	`Malware(악성코드)`, `Spam(스팸)`	보안 인텔리전스로 확인된 위험 트래픽의 카테고리입니다.
보안 영역	`My Security Zone(내 보안 영역)`, `Security Zone X(보안 영역 X)`	트래픽이 분석되고 통과되는(인라인 구축의 경우) 인터페이스 집합입니다.
SSL	`yes`, `no`	SSL 또는 TLS 암호화 트래픽입니다.
사용자	`wsmith`, `mtwain`	모니터링되는 네트워크의 호스트에 로그인하는 사용자의 ID입니다.

추가 필터 창에서 필터 생성

이 절차를 사용하면 Add Filter(필터 추가) 창에서 필터를 처음부터 만들 수 있습니다. (콘텍스트 메뉴를 사용하여 빠른 필터를 만들 수도 있습니다.)

Context Explorer(상황 탐색기) 왼쪽 위의 **Filters(**필터**)** 아래에 있는 **Plus(**더하기**)** (+)를 클릭하여 액세스할 수 있는 Add Filter(필터 추가) 창에는 필터가 2개만 있습니다.

- **Data Type(**데이터 유형**)** 드롭다운 목록에는 Context Explorer(상황 탐색기)를 제한하는 데 사용할 수 있는 많은 유형의 Firepower System 데이터가 포함되어 있습니다. 데이터 유형을 선택한 다음 **Filter(**필터**)** 필드에서 해당 유형에 대한 특정 값(예: **Continent** 유형에 대해 `Asia` 값)을 입력합니

다. 사용자에게 도움이 되도록 선택 가능한 데이터 유형에 대한 몇 가지 예제 값이 Filter(필터) 필드에 회색으로 표시됩니다. (필드에 데이터를 입력하면 이러한 값이 지워집니다.)

- 필터 필드 * 같은 특수 한 검색 파라미터 입력과 ! 이벤트의 수를 기본적으로 검색 합니다. 필터 파라미터 앞에 ! 기호를 추가하면 제외하는 필터를 만들 수 있습니다.

참고 추가하는 필터는 자동으로 적용되지 않습니다. Context Explorer(상황 탐색기)에서 필터를 보려면 **Apply Filters(**필터 적용**)**를 클릭해야 합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** 왼쪽 위의 **Filters(**필터**)** 아래에서 **Plus(**더하기**)** (+)를 클릭합니다.

단계 **3** **Data Type(**데이터 유형**)** 드롭다운 목록에서 필터링할 데이터 유형을 선택합니다.

단계 **4** **Filter(**필터**)** 필드에 필터링할 데이터 유형 값을 입력합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** 선택적으로, 원하는 필터 집합이 구성될 때까지 이전 단계를 반복하여 필터를 더 추가합니다.

단계 **7** **Apply Filters(**필터 적용**)**을 클릭합니다.

관련 항목

데이터 유형 필드 옵션, 608 페이지
검색 제약 조건, 722 페이지

콘텍스트 메뉴에서 빠른 필터 생성

Context Explorer(상황 탐색기) 그래프 및 목록 데이터를 탐색할 때 데이터 포인트를 클릭한 다음 콘텍스트 메뉴를 사용하여 해당 데이터를 기반으로 빠르게 필터를 만들 수 있습니다(포함 또는 제외). 콘텍스트 메뉴를 사용하여 데이터 유형(애플리케이션, 사용자, 침입 이벤트 메시지, 개별 호스트 등)의 정보에 대해 필터링하면 필터 위젯에는 해당 데이터 유형에 대한 관련 세부 사항 페이지(예: 애플리케이션 데이터의 경우 Application Detail(애플리케이션 세부 사항))로 연결되는 위젯 정보가 포함됩니다. URL 데이터에 대해서는 필터링할 수 없습니다.

특정 그래프나 목록 데이터를 좀 더 자세히 조사하려는 경우에도 콘텍스트 메뉴를 사용할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** Traffic and Intrusion Events over Time을 제외한 탐색기 섹션 또는 URL 데이터가 포함된 섹션에서 필터링할 데이터 포인트를 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 이 데이터에 대한 필터를 추가하려면 **Add Filter(**필터 추가**)**를 클릭합니다.
- 이 데이터에 대한 제외 필터를 추가하려면 **Add Exclude Filter(**제외 필터 추가**)**를 클릭합니다. 필터를 적용하면 제외된 값과 관련된 데이터 외의 모든 데이터가 표시됩니다. 제외 필터는 필터 값 앞에 느낌표(!)를 표시합니다.

필터링된 **Context Explorer(**상황 탐색기**)** 보기 저장

Context Explorer(상황 탐색기)에서 나오거나 세션 종료 후 필터 설정을 Context Explorer(상황 탐색기)에 저장하려면, 원하는 필터가 적용된 Context Explorer(상황 탐색기)의 브라우저 즐겨찾기를 생성합니다. 적용된 필터는 Context Explorer(상황 탐색기) 페이지 URL에 통합되므로 해당 페이지의 즐겨찾기를 로드하면 해당 필터도 로드됩니다.

프로시저

원하는 필터가 적용된 Context Explorer(상황 탐색기)의 브라우저 즐겨찾기를 생성합니다.

필터 데이터 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**를 선택합니다.

단계 **2** 해당 필터 위젯에서 **Information(**정보**)**을 클릭합니다.

필터 삭제

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**를 선택합니다.

단계 **2** 왼쪽 위의 **Filters(**필터**)** 아래에서 **Close(**닫기**)** (✕)을 클릭하여 필터 위젯을 개별적으로 삭제합니다.

팁 모든 필터를 동시에 삭제하려면 **Clear(**지우기**)** 버튼을 클릭합니다.

23 장

통합 이벤트

다음 항목에서는 통합 이벤트를 사용하는 방법을 설명합니다.

통합 이벤트 정보

통합 이벤트는 여러 유형의 방화벽 이벤트(연결, 침입, 파일, 악성코드 및 일부 보안 관련 연결 이벤트)를 단일 화면 보기로 제공합니다. 서로 연결된 이벤트는 테이블에 함께 누적되어 보안 이벤트에 대한 통합 보기와 추가 컨텍스트를 제공합니다. 통합 이벤트 테이블에 침입 이벤트가 있을 경우 침입 이벤트를 클릭하여 연결된 연결 이벤트를 강조 표시합니다. 이제 연결 이벤트를 침입 이벤트와 상호 전환하면 여러 이벤트 보기 간에 전환하지 않고도 네트워크 문제를 더 잘 해결할 수 있습니다.

통합 이벤트 테이블은 수준 높은 사용자 맞춤화가 가능합니다. 이벤트 보기에 표시되는 정보를 세부적으로 조정할 수 있도록 사용자 지정 필터를 생성하고 적용할 수 있습니다. 통합 이벤트 보기에는 특정 요구에 맞게 자주 사용하는 사용자 지정 필터를 저장한 다음, 저장된 필터를 빠르게 로드할 수 있는 옵션도 있습니다. 또한 열을 추가 또는 제거하여 사용자 지정 이벤트 보기 테이블을 만들거나, 열을 고정하거나, 열을 끌어서 순서를 변경할 수 있습니다.

통합 이벤트 테이블의 **Live View(**라이브 보기**)** 옵션을 사용하면 방화벽 이벤트를 실시간으로 확인하고 네트워크 활동을 모니터링할 수 있습니다. 예를 들어, 방화벽 관리자는 정책을 변경한 후 이벤트

업데이트를 실시간으로 확인하면 정책 변경 사항이 네트워크에 올바르게 적용되었는지 확인할 수 있습니다.

통합 이벤트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자
- 보안 분석가

통합 이벤트 보기로 작업

여러 이벤트 보기 간에 전환할 필요 없이 단일 테이블에서 다양한 방화벽 이벤트 유형을 보고 작업할 수 있습니다.

이 보기를 사용하여 다음을 수행합니다.

- 통합 보기에서 서로 다른 이벤트 유형 간의 관계를 찾습니다.
- 실시간으로 정책 변경의 영향을 확인하십시오.

시작하기 전에

다음 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 시간 범위(고정 또는 슬라이딩)를 선택합니다. 자세한 내용은 통합 이벤트 보기에서 시간 범위 설정 항목을 참고하십시오.

단계 **3** Secure Network Analytics 어플라이언스에 원격으로 이벤트를 저장하고 데이터 소스를 변경해야 하는 충분한 이유가 있는 경우 데이터 소스를 선택합니다. Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Secure Firewall Management Center에서 작업에서 자세한 정보를 참고하십시오.

단계 **4** 통합 이벤트 보기에 처음 표시되는 방대한 방화벽 이벤트 목록을 필터링할 수 있어 네트워크의 이벤트를 상황별로 더욱 상세히 파악할 수 있습니다. 자세한 내용은 통합 이벤트 보기의 필터를 참고하십시오.

단계 **5** 추가 옵션을 선택합니다.

변경 후	수행해야 할 작업
열 맞춤화	• 열을 추가하거나 제거합니다. 열 선택기(▥)를 클릭하고 열을 선택합니다. 참고 많은 열을 포함하면 성능이 저하될 수 있습니다. 이벤트 행을 확장하여 이벤트 세부 사항을 확인하여 숨겨진 열에 대한 데이터를 볼 수 있습니다. • 열 순서를 재지정합니다. 열 제목을 끌어다 놓습니다. • 스크롤하지 않도록 열을 테이블의 왼쪽 또는 오른쪽에 고정합니다. 열을 테이블의 왼쪽이나 오른쪽으로 끌어옵니다. 또는 열 제목을 고정된 영역으로 끌어서 놓습니다. 열 고정을 해제하려면 고정된 영역 밖으로 열을 드래그합니다. • 열 크기를 조정합니다. • 열을 기본 설정으로 되돌립니다. • 열 집합을 저장합니다. 자세한 내용은 통합 이벤트 보기에서 열 집합 저장 항목을 참고하십시오. 데이터는 항상 시간을 기준으로 정렬되며 가장 최근 이벤트가 맨 위에 옵니다.
관련 이벤트 식별	이 이벤트와 관련된 다른 이벤트를 강조 표시하려면 행을 클릭합니다. 필요한 경우 이벤트를 필터링하여 작은 이벤트 집합을 표시합니다. 참고 연결의 이니시에이터가 악성코드 파일의 발신자와 반드시 같을 필요는 없습니다. 소스 또는 대상 **IP** 필터를 통해 통합 이벤트 보기를 필터링하여 연결 이벤트에 연결된 파일 또는 악성코드 이벤트를 검색합니다.
이벤트 세부 정보 보기	행의 왼쪽 끝에서 >(확장) 아이콘을 클릭합니다. 표시할 데이터가 없는 필드는 이벤트 세부 사항에 포함되지 않습니다. 팁 **Event Details(**이벤트 세부 정보**)** 창을 보려면 이벤트를 더블 클릭합니다. **Event Details(**이벤트 세부 정보**)** 창이 열려 있으면 테이블에서 이벤트를 클릭하여 해당 이벤트의 세부 정보를 로드합니다.

변경 후	수행해야 할 작업
실시간으로 이벤트 보기	**Go Live(**라이브 상태로 전환**)**를 클릭합니다. 자세한 내용은 통합 이벤트 보기에서 이벤트의 라이브 보기를 참고하십시오. 이벤트가 너무 빨리 스트리밍되면 필터 기준을 입력합니다.
셀 값에 사용 가능한 옵션 보기	셀의 오른쪽 끝에 있는 **Options(**옵션**)** 아이콘을 클릭합니다.
외부 리소스에 대한 교차 실행	테이블 셀의 점을 클릭하면 해당 데이터와 관련된 기타 옵션이 표시됩니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지를 참고하십시오.
여러 통합 이벤트 뷰어 탭/창 열기	여러 브라우저 탭 또는 창을 사용하여 통합 이벤트 뷰어의 여러 보기를 표시할 수 있습니다. 각 새 탭 또는 창에는 가장 최근에 수정된 탭/창의 특성이 있습니다. 열려 있는 탭/창을 템플릿으로 만들려면 템플릿을 약간 변경합니다. 여러 탭의 쿼리는 순차적으로 처리됩니다. 보기(예: 수신 이벤트 비율이 높을 때의 복잡한 쿼리 또는 라이브 보기 모드에서 보기)에 따라 약 4개 이상의 탭을 동시에 열면 성능이 저하될 수 있습니다.
검색 저장	사용자 지정 검색을 즐겨찾기로 저장하고 나중에 빠르게 로드할 수 있습니다. 자세한 내용은 통합 이벤트 보기에서 검색 저장 항목을 참고하십시오.
쿼리 결과 즐겨찾기 추가 또는 공유	브라우저 창에서 URL을 즐겨찾기에 추가하거나 복사하여 붙여 넣습니다. URL은 슬라이딩 시간 범위를 사용하는 경우 나중에 다른 이벤트를 검색합니다. URL은 열 가시성, 크기 및 순서, 실시간 스트리밍 설정을 캡처하지 않습니다.

통합 이벤트 보기에서 시간 범위 설정

특정 기간의 방화벽 이벤트를 보려면 통합 이벤트 보기에서 시간 범위를 구성합니다. 시간 범위를 변경하면 통합 이벤트 보기가 자동으로 새로 고침되어 변경 사항을 반영합니다.

선택하는 시간 범위는 이벤트 보기의 다른 테이블에 적용되지 않습니다. 예를 들어, 연결 이벤트를 볼 때 선택하는 시간 범위는 통합 이벤트 보기에 적용되지 않으며 그 반대의 경우도 마찬가지입니다.

중요 기간이 연결 이벤트의 보존 기간을 초과하여 다시 연장되는 경우 **Analysis(분석)** > **Connections(연결)** > **Security-Related Connection Events(보안 관련 연결 이벤트)** 아래의 테이블에서 Security-Related Connection(보안 관련 연결) 이벤트를 찾습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(분석)** > **Unified Events(통합 이벤트)**를 선택합니다.

기본적으로, 통합 이벤트 보기에서는 지난 1시간의 이벤트가 표시됩니다.

단계 **2** 현재 시간 범위를 클릭합니다.

단계 **3** 다음 중 하나를 선택합니다.

- 고정 시간 범위에 대한 이벤트를 확인하려면 **Fixed Time Range(고정 시간 범위)**를 클릭하고 **Start time(시작 시간)** 및 **End time(종료 시간)**을 선택합니다.

  팁 **Now(지금)**를 클릭하여 현재 시간을 **End time(종료 시간)**으로 빠르게 설정합니다.

- 지정한 길이의 슬라이딩 기본 시간대를 구성하려면 **Sliding Time Range(슬라이딩 시간 범위)**를 클릭합니다.

  어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 새로고침하면 시간대가 슬라이딩하므로 항상 지난 1시간의 이벤트가 표시됩니다.

단계 **4** **Apply(적용)**를 클릭합니다.

통합 이벤트 보기에서 이벤트의 라이브 보기

수동으로 이벤트 보기를 새로 고치지 않고 방화벽 이벤트를 실시간으로 표시하도록 통합 이벤트 보기를 구성합니다. 라이브 보기 모드에서는 네트워크에서 보안 이벤트가 발생할 때 이벤트 로그가 실시간으로 표시되므로, 문제를 보다 쉽게 해결할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

기본적으로, 통합 이벤트 보기에서는 지난 1시간의 이벤트가 표시됩니다.

단계 **2** 라이브 이벤트 업데이트를 보려면 **Go Live(**라이브 상태로 전환**)**를 클릭합니다.

새 이벤트가 이벤트 테이블 상단에 채워집니다. 시간 범위 섹션에는 통합 이벤트 보기가 라이브 상태로 유지되는 기간을 알리는 타이머가 표시됩니다.

다음에 수행할 작업

라이브 보기 모드를 종료하려면 **Live(**라이브**)**를 클릭합니다.

통합 이벤트 보기의 필터

통합 이벤트 보기에는 지난 1시간 동안의 여러 방화벽 이벤트 유형이 표시됩니다. 통합 이벤트의 기본 보기를 필터링하여 네트워크의 활동에 대한 보다 세분화된 상황별 정보를 확인할 수 있습니다. 필터는 포함 필터 기준뿐 아니라 예외도 지원합니다.

필터를 사용하면 중요한 정보에 빠르게 액세스할 수 있습니다. 예를 들어, 방화벽 관리자가 일부 사용자에게 특정 애플리케이션 액세스를 허용하거나 거부하려면 방화벽 로그를 스캔하도록 사용자 검색 기준을 설정할 수 있습니다. 이벤트 보기에는 검색 기준과 일치하는 이벤트 로그가 표시됩니다.

시작하기 전에

다음 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 필터 기준 입력:

- 필터 기준을 수동으로 입력하려면 검색 텍스트 필드에 정확한 기준을 입력하거나 드롭다운 목록에서 기준을 선택합니다. 그런 다음 필터 기준 값을 제공합니다. 값을 입력하는 동안 가능할 때마다 드롭다운 목록에 제안 메시지가 나타납니다.
- 테이블의 이벤트에 대한 셀의 점을 클릭하고 필터 기준에서 해당 값을 포함하거나 제외할 옵션을 선택합니다.

팁
- 포함 필터 기준을 빠르게 추가하려면 **Ctrl+click**(Windows) 또는 **Command-click**(Mac) 키를 사용합니다.
- 예외 필터 기준을 빠르게 추가하려면 **Ctrl+click**(Windows) 또는 **Command-click**(Mac) 키를 사용합니다.

- 필터 조건을 구체화하십시오. 와일드 카드 및 검색 동작에 대한 중요한 정보는 이벤트 검색을 참고하십시오.
- 값 앞의 값 필드에 연산자(예: <, >, ! 등)를 포함합니다. 예를 들어, **Action(**작업**)** 필드에 `!Allow(허용)`를 입력하여 Allow(허용) 이외의 작업이 있는 모든 이벤트를 찾습니다.

단계 **3** 검색을 수행합니다.

팁 **Ctrl+Enter**(Windows) 또는 **Command-Enter**(Mac) 키 명령을 사용하여 검색을 시작할 수 있습니다.

다른 이벤트 보기 테이블과 달리, 통합된 이벤트 보기의 이벤트는 표시된 열이 모두 동일한 값을 가질 때 집계되지 않습니다. 필터 기준과 일치하는 모든 이벤트가 개별적으로 나열됩니다.

다음에 수행할 작업

사용자 지정 필터를 저장하려면 통합 이벤트 보기에서 검색 저장 항목을 참고하십시오.

통합 이벤트 보기에서 검색 저장

시작하기 전에

검색을 저장하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 통합 이벤트 보기의 필터 항목에 설명된 대로 검색 기준을 설정합니다.

단계 **3** 검색(Q) 아이콘을 클릭합니다.

단계 **4** **+ Save search(**검색 저장**)**를 클릭합니다.

단계 **5** 검색 이름을 지정하고 확인(✓) 아이콘을 클릭합니다.

다음에 수행할 작업

저장된 검색을 로드하려면 통합 이벤트 보기에 저장된 검색 로드 항목을 참고하십시오.

통합 이벤트 보기에 저장된 검색 로드

시작하기 전에

- 이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.
- 통합 이벤트 보기에서 검색 저장 항목에 설명된 대로 저장된 검색을 설정합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 검색 텍스트 상자에서 **Search(**검색**)**( ) 아이콘을 클릭하고 로드할 저장된 검색을 선택합니다.

단계 **3** 또는 **Open Saved search details(**저장된 검색 세부 정보 열기**)** 패널 아이콘을 클릭하고 저장된 검색을 선택하여 선택한 검색에 대한 필터 조건을 표시합니다. 검색을 로드하려면 **Apply search(**검색 적용**)**를 클릭합니다.

통합 이벤트 보기에서 열 집합 저장

시작하기 전에

열 집합을 저장하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** 열 선택기 아이콘( )을 클릭하고 저장할 열 집합을 선택합니다.

단계 **3** **Saved Column Sets(**저장된 열 집합**)** 드롭다운에서 **+ Create column set from current selection(+** 현재 선택 항목에서 열 집합 생성**)**을 클릭합니다.

단계 **4** 열 집합의 이름을 지정하고 **OK(**확인**)**( ) 아이콘을 클릭합니다.

다음에 수행할 작업

저장된 열 집합을 로드하려면 통합 이벤트 보기에서 저장된 열 집합 로드 항목을 참고하십시오.

통합 이벤트 보기에서 저장된 열 집합 로드

시작하기 전에

- 이 작업을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.
- 통합 이벤트 보기에서 열 집합 저장 항목에 설명된 대로 즐겨찾기 열 집합을 저장합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Unified Events(**통합 이벤트**)**를 선택합니다.
단계 **2** 열 선택기 아이콘(▥)을 클릭합니다.
단계 **3** **Saved Column Sets(**저장된 열 집합**)** 드롭다운에서 로드하려는 열 집합을 선택합니다.

통합 이벤트 보기 열 설명

일부 필드의 값은 이벤트 유형에 따라 달라집니다. 필드 통신은 다음과 같습니다.

통합 이벤트 뷰어 필드 이름	연결 또는 보안 인텔리전스 이벤트 필드 이름	침입 이벤트 필드 이름	파일 이벤트 필드 이름	악성코드 이벤트 필드 이름
시간	첫 번째 패킷 아래 참고를 참조하십시오.	시간	시간	시간
이벤트 유형	--	--	--	--
조치	작업	인라인 결과	작업	작업
이유	이유	이유	(해당 없음)	(해당 없음)
소스 **IP**	초기자 IP	소스 IP	송신 IP	송신 IP
목적지 **IP**	응답기 IP	목적지 IP	수신 IP	수신 IP
소스 포트/**ICMP** 유형	소스 포트	소스 포트	송신 포트	송신 포트
대상 포트/**ICMP** 유형	목적지 포트	목적지 포트	수신 포트	수신 포트
웹 애플리케이션	웹 애플리케이션	웹 애플리케이션	웹 애플리케이션	웹 애플리케이션

통합 이벤트 뷰어 필드 이름	연결 또는 보안 인텔리전스 이벤트 필드 이름	침입 이벤트 필드 이름	파일 이벤트 필드 이름	악성코드 이벤트 필드 이름
규칙	액세스 제어 규칙	액세스 제어 규칙	(해당 없음)	(해당 없음)
정책	액세스 제어 정책	침입 정책	파일 정책	파일 정책
디바이스	디바이스	디바이스	디바이스	디바이스
NAT 소스 **IP**	NAT 소스 IP	(해당 없음)	(해당 없음)	(해당 없음)
NAT 대상 **IP**	NAT 대상 IP	(해당 없음)	(해당 없음)	(해당 없음)
NAT 소스 포트	NAT 소스 포트	(해당 없음)	(해당 없음)	(해당 없음)
NAT 대상 포트	NAT 대상 포트	(해당 없음)	(해당 없음)	(해당 없음)
MITRE	(해당 없음)	MITRE	MITRE	MITRE
규칙 그룹	(해당 없음)	규칙 그룹	(해당 없음)	(해당 없음)

필드 설명은 다음 항목을 참조하십시오.

- 연결 및 보안 관련 연결 이벤트 필드, 773 페이지
- 침입 이벤트 필드, 810 페이지
- 파일 및 악성코드 이벤트 필드, 863 페이지

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 790 페이지도 참조하십시오.

참고 연결 시작시 로깅을 활성화하지 않은 경우에도 시스템은 이 값을 통합 이벤트 뷰어의 시간 필드로 사용합니다. 연결 시작 및 종료시 연결 이벤트가 기록되었는지 확인하려면 이벤트의 행을 확장하여 세부 정보를 확인합니다. 연결의 양쪽 끝에 기록된 경우 **Last Packet**(마지막 패킷) 필드가 표시됩니다.

통합 이벤트 기록

기능	버전	세부 사항
즐겨찾기 검색 저장	7.3	열 집합 및 검색을 즐겨찾기로 저장하고 나중에 빠르게 실행할 수 있습니다.
통합 이벤트 뷰어	7.0	연결(보안 인텔리전스 포함), 침입, 파일 및 악성 코드 등 여러 이벤트 유형이 포함된 단일 테이블을 보고 작업합니다. 새 페이지/수정 페이지: 분석 > 통합 이벤트 아래 새 페이지 지원되는 플랫폼: management center

24 장

네트워크 맵

다음 주제에서는 네트워크 맵을 사용하는 방법을 설명합니다.

네트워크 맵 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

Leaf

사용자 역할

- 관리자
- 검색 관리자

네트워크 맵

Firepower System은 네트워크를 통해 이동하는 트래픽을 모니터링하고, 트래픽 데이터를 디코딩한 다음 데이터를 설정된 운영체제 및 핑거프린트와 비교합니다. 그런 다음 시스템은 이 데이터를 사용하여 네트워크 맵이라고 하는, 네트워크의 자세한 표현을 작성합니다. 다중 도메인 구축의 경우, 시스템은 각 리프 도메인에 대한 개별 네트워크 맵을 생성합니다.

시스템은 네트워크 검색 정책에서 모니터링용으로 식별된 매니지드 디바이스에서 데이터를 수집합니다. 매지니드 디바이스는 네트워크 자산을 모니터링하는 트래픽에서는 직접적으로, 처리된 NetFlow

기록에서는 간접적으로 탐지합니다. 여러 디바이스가 동일한 네트워크 자산을 탐지하면 시스템은 하나의 복합 자산 표현으로 정보를 결합합니다.

수동 탐지에서 데이터를 보강하는 방법은 다음과 같습니다.

- 오픈 소스 스캐너인 Nmap™을 이용해 호스트를 적극적으로 스캔하고, 스캔 결과를 네트워크 맵에 추가합니다.
- 호스트 입력 기능을 이용해 타사 애플리케이션의 호스트 데이터를 수동으로 추가합니다.

네트워크 맵은 탐지한 호스트 및 네트워크 디바이스를 중심으로 네트워크 토폴로지를 표시합니다.

네트워크 맵을 사용하면 다음 작업을 수행할 수 있습니다.

- 전체 네트워크를 빠르게 확인.
- 수행할 분석에 맞게 각기 다른 보기 선택. 네트워크 맵의 각 보기는 확장 가능한 카테고리 및 하위 카테고리가 있는 계층적 트리의 동일한 형식을 가지고 있습니다. 카테고리를 클릭하면 그 아래의 하위 카테고리가 표시되도록 카테고리가 확장됩니다.
- 맞춤형 토폴로지 기능을 통해 서브넷 구성 및 식별. 예를 들어 조직의 각 부서에서 서로 다른 서브넷을 사용하는 경우 맞춤형 토폴로지 기능을 사용하여 친숙한 레이블을 서브넷에 할당할 수 있습니다.
- 임의의 모니터링 호스트의 호스트 프로파일로 드릴다운하여 상세 정보 확인
- 더 이상 조사하지 않으려는 자산 삭제

참고 네트워크 맵에서 삭제된 호스트와 관련된 활동이 탐지되면, 해당 호스트는 네트워크 맵에 다시 추가됩니다. 마찬가지로, 시스템에서 애플리케이션의 변경 사항(예: Apache 웹 서버가 새 버전으로 업그레이드됨)을 탐지하면 삭제된 애플리케이션이 네트워크 맵에 다시 추가됩니다. 호스트를 취약하게 만드는 변경 사항이 탐지되면 특정 호스트에서 취약성이 다시 활성화됩니다.

팁 네트워크 맵에서 호스트 또는 서브넷을 영구적으로 제외하려면 네트워크 검색 정책을 수정하십시오. 과도하거나 관련 없는 이벤트를 생성하는 것으로 확인된 로드 밸런서와 NAT 디바이스는 모니터링에서 제외할 수 있습니다.

호스트 네트워크 맵

Hosts(호스트) 탭의 네트워크 맵은 호스트 카운트와 호스트 IP 주소 및 기본 MAC 주소 목록을 표시합니다. 각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다. 이 네트워크 맵 보기는 시스템에서 탐지한 모든 고유한 (IP가 하나 또는 여러 개인) 호스트의 카운트를 제공합니다.

호스트 네트워크 맵을 사용하면 계층적 트리에 서브넷으로 구성된 네트워크의 호스트를 볼 수 있으며, 특정 호스트에 대한 호스트 프로파일로 드릴다운할 수도 있습니다.

시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

네트워크에 대한 맞춤형 토폴로지를 생성하면, 부서 이름과 같은 의미 있는 레이블(예: 부서 이름)을 서브넷에 할당할 수 있으며, 이는 호스트 네트워크 맵에 나타납니다. 또한 맞춤형 토폴로지에서 지정한 조직에 따라 호스트 네트워크 맵을 볼 수 있습니다.

호스트 네트워크 맵에서 전체 네트워크, 서브넷 또는 개별 호스트를 삭제할 수 있습니다. 특정 호스트가 네트워크에 더 이상 연결되어 있지 않음을 알고 있다면 분석을 간소화하기 위해 해당 호스트를 삭제할 수 있습니다. 삭제된 호스트와 관련된 활동이 이후에 탐지되면 해당 호스트는 네트워크 맵에 다시 추가됩니다. 네트워크 맵에서 호스트 또는 서브넷을 영구적으로 제외하려면 네트워크 검색 정책을 수정하십시오.

주의 네트워크 맵에서 네트워크 디바이스를 삭제하지 마십시오. 시스템은 이러한 디바이스를 이용해 네트워크 토폴로지를 확인합니다.

호스트 네트워크 맵 페이지에서는 기본 MAC 주소만 검색할 수 있으며, Hosts [MAC] 카운트에는 기본 MAC 주소만 포함됩니다. 기본 및 보조 MAC 주소에 대한 설명은 호스트 프로파일의 기본 호스트 정보, 896 페이지 섹션을 참조하십시오.

네트워크 디바이스 네트워크 맵

Network Devices(네트워크 디바이스) 탭의 네트워크 맵은 네트워크의 세그먼트를 다른 세그먼트와 연결하는 네트워크 디바이스(브리지, 라우터, NAT 디바이스, 로드 밸런서)를 표시합니다. 맵에는 IP 주소로 식별한 디바이스를 나열하는 섹션과 MAC 주소로 식별한 디바이스를 나열하는 섹션이 있습니다.

또한 맵은 시스템에서 탐지한 모든 고유한 (IP가 하나 또는 여러 개인) 네트워크 디바이스의 카운트도 제공합니다.

네트워크에 대해 맞춤형 토폴로지를 생성하면, 서브넷에 할당하는 레이블이 네트워크 디바이스 네트워크 맵에 나타납니다.

시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.
- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.

네트워크 디바이스가 CDP를 사용하여 통신하는 경우 IP 주소가 하나 이상일 수 있습니다. STP를 사용하여 통신하는 경우 MAC 주소가 하나뿐일 수 있습니다.

네트워크 맵에서는 네트워크 디바이스를 삭제할 수 없습니다. 시스템은 이러한 디바이스의 위치를 이용해 네트워크 토폴로지를 결정하기 때문입니다.

네트워크 디바이스의 호스트 프로파일에는 Operating Systems 섹션이 아닌 Systems 섹션이 있습니다. 여기에는 네트워크 디바이스 뒤에서 탐지되는 모바일 디바이스에 대한 하드웨어 플랫폼을 반영하는 Hardware 열이 포함됩니다. Systems 아래에 하드웨어 플랫폼에 대한 값이 나열되면 해당 시스템은 네트워크 디바이스 뒤에서 탐지된 하나 이상의 모바일 디바이스를 나타냅니다. 모바일 디바이스에는 하드웨어 플랫폼 정보가 있을 수도 있고 없을 수도 있지만, 모바일 디바이스가 아닌 시스템에 대해서는 하드웨어 플랫폼 정보가 탐지되지 않습니다.

모바일 디바이스 네트워크 맵

Mobile Devices(모바일 디바이스) 탭의 네트워크 맵은 네트워크에 연결된 모바일 디바이스를 표시합니다. 이 네트워크 맵은 시스템에서 탐지한 모든 고유한 (IP가 하나 또는 여러 개인) 모바일 디바이스의 카운트도 제공합니다.

각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다. 서브넷이나 IP 주소를 삭제할 수도 있습니다. 시스템이 디바이스를 다시 검색하면, 디바이스는 네트워크 맵에 다시 추가됩니다.

드릴다운을 통해 모바일 디바이스에 대한 호스트 프로파일을 확인할 수도 있습니다.

모바일 디바이스 식별을 위해 시스템은 다음을 수행합니다.

- 모바일 디바이스의 모바일 브라우저에서 HTTP 트래픽의 User-Agent(사용자 에이전트) 문자열 분석
- 특정 모바일 애플리케이션의 HTTP 트래픽 모니터링

네트워크에 대해 맞춤형 토폴로지를 생성하면, 서브넷에 할당하는 레이블이 모바일 디바이스 네트워크 맵에 나타납니다.

보안 침해 지표 네트워크 맵

Indications of Compromise(보안 침해 지표) 탭의 네트워크 맵은 IOC 카테고리별로 조직화된, 네트워크 상의 침해된 호스트를 표시합니다. 영향받는 호스트는 각 카테고리 아래에 나열됩니다. 각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다.

IOC 네트워크 맵에서는 특정 방법으로 침해된 것으로 판단된 각 호스트의 호스트 프로파일을 볼 수 있습니다. 특정 IOC 카테고리 또는 특정 호스트를 삭제(또는 해결된 것으로 표시)할 수 있는데, 그렇게 하면 관련 호스트에서 IOC 태그가 제거됩니다. 예를 들어 문제가 해결되어 재발하지 않을 것으로 판단한 경우 네트워크 맵에서 IOC 카테고리를 삭제할 수 있습니다.

네트워크 맵에서 호스트 또는 IOC 카테고리를 해결된 것으로 표시하더라도 해당 항목이 네트워크에서 제거되지는 않습니다. 해당 IOC를 트리거하는 정보가 새로 탐지되면 네트워크 맵에 해결된 호스트 또는 IOC 카테고리가 다시 나타납니다.

시스템이 보안 침해 지표를 결정하는 방법에 대한 자세한 내용은 보안 침해 지표 데이터, 946 페이지 및 하위 항목을 참조하십시오.

애플리케이션 프로토콜 네트워크 맵

Application Protocols(애플리케이션 프로토콜) 탭의 네트워크 맵은 애플리케이션 이름, 벤더, 버전별로, 그리고 마지막에는 각 애플리케이션을 실행하는 호스트별로 계층형 트리에 구성되어 있는, 네트워크 상의 애플리케이션을 표시합니다.

시스템 소프트웨어와 VDB가 업데이트되는 경우, 그리고 애드온 탐지기를 가져오는 경우 시스템에서 탐지하는 애플리케이션이 변경될 수 있습니다. 각 시스템 또는 VDB 업데이트에 대한 릴리스 정보나 자문 텍스트에는 새 탐지기 및 업데이트된 탐지기에 대한 정보가 포함되어 있습니다. 포괄적인 최신 탐지기 목록은 Cisco 지원 사이트(http://www.cisco.com/cisco/web/support/index.html)를 참조하십시오.

이 네트워크 맵에서는 특정 애플리케이션을 실행하는 각 호스트의 호스트 프로파일을 확인할 수 있습니다.

또한 모든 애플리케이션 카테고리, 모든 호스트에서 실행 중인 모든 애플리케이션, 특정 호스트에서 실행 중인 모든 애플리케이션을 삭제할 수 있습니다. 예를 들어 애플리케이션이 호스트에서 비활성화된 것을 알고 있으며 시스템이 영향 레벨 자격에 애플리케이션을 사용하지 않도록 하려면 네트워크 맵에서 해당 애플리케이션을 삭제할 수 있습니다.

네트워크 맵에서 애플리케이션을 삭제해도 네트워크에서 제거되지는 않습니다. 시스템에서 애플리케이션의 변경 사항(예: Apache 웹 서버가 새 버전으로 업그레이드됨)을 탐지하거나 시스템의 검색 기능을 다시 시작하는 경우 삭제된 애플리케이션이 네트워크 맵에 다시 나타납니다.

삭제한 내용에 따라 동작이 달라집니다.

- 애플리케이션 카테고리 - 삭제하면 네트워크 맵에서 애플리케이션 카테고리가 제거됩니다. 카테고리에 속하는 모든 애플리케이션이 해당 호스트 프로파일에서 제거됩니다.

  예를 들어 **http**를 삭제하면 **http**로 식별되는 모든 애플리케이션이 모든 호스트 프로파일에서 제거되며, 네트워크 맵의 애플리케이션 보기에 **http**가 더 이상 나타나지 않습니다.

- 특정 애플리케이션, 벤더 또는 버전 - 삭제하면 영향받는 애플리케이션이 네트워크 맵 및 해당 호스트 프로파일에서 제거됩니다.

  예를 들어 **http** 카테고리를 확장하고 **Apache**를 삭제하면, Apache 아래에 나열된 버전과 상관없이 Apache로서 나열된 모든 애플리케이션이 해당 호스트 프로파일에서 제거됩니다. 마찬가지로, **Apache**를 삭제하는 대신 특정 버전(예: **1.3.17**)을 삭제하면 선택한 버전만이 영향받는 호스트 프로파일에서 삭제됩니다.

- 특정 IP 주소 - 삭제하면 애플리케이션 목록에서 해당 IP 주소가 제거되며, 선택한 IP 주소의 호스트 프로파일에서 애플리케이션 자체도 제거됩니다.

  예를 들어 **http**, **Apache**, **1.3.17(Win32)**을 확장한 다음 **172.16.1.50:80/tcp**를 삭제하면 Apache 1.3.17(Win32) 애플리케이션이 IP 주소 172.16.1.50의 호스트 프로파일에서 삭제됩니다.

취약성 네트워크 맵

Vulnerabilities(취약성) 탭의 네트워크 맵은 시스템이 네트워크에서 탐지한 취약성을 레거시 취약성 ID(SVID), CVE ID 또는 Snort ID별로 조직화해 표시합니다.

이 네트워크 맵에서는 특정 취약성의 상세정보와, 특정 취약성에 대한 호스트의 호스트 프로파일을 확인할 수 있습니다. 이 정보는 해당 취약성이 영향받는 특정 호스트에 미치는 위협을 평가하는 데 도움이 됩니다.

특정 취약성이 (패치 적용 등의 이유로) 네트워크의 호스트에 영향을 미치지 않는 것 같다면 해당 취약성을 비활성화할 수 있습니다. 비활성화된 취약성은 여전히 네트워크 맵에 나타나지만 영향받는 이전 호스트의 IP 주소는 회색의 기울임꼴로 나타납니다. 그러한 호스트의 호스트 프로파일은 비활성화된 취약성을 무효 상태로 표시합니다(개별 호스트에 대해 수동으로 취약성을 유효 상태로 표시할 수는 있음).

호스트에서 애플리케이션이나 운영체제의 ID 충돌이 있는 경우 시스템은 잠재적인 두 ID에 대한 취약성을 나열합니다. ID 충돌이 해결되면 취약성과 현재 ID의 연결 상태가 유지됩니다.

기본적으로, 패킷에 애플리케이션의 벤더 및 버전이 포함된 경우에만 네트워크 맵에 탐지된 애플리케이션의 취약성이 표시됩니다. 그러나 management center 설정에서 애플리케이션에 대한 취약성 매핑 설정을 활성화함으로써, 벤더 및 버전 데이터가 없는 애플리케이션에 대한 취약성을 나열하도록 시스템을 구성할 수 있습니다.

취약성 ID(또는 취약성 ID의 범위) 옆에 있는 숫자는 두 개의 카운트를 나타냅니다.

영향받은 호스트

첫 번째 숫자는 취약성의 영향을 받는 고유하지 않은 호스트의 카운트입니다. 하나의 호스트가 둘 이상의 취약성에 의해 영향을 받으면 여러 번으로 계산됩니다. 따라서 카운트가 네트워크에 있는 호스트의 수보다 클 수 있습니다. 취약성을 비활성화하면 해당 취약성의 영향을 받을 가능성이 있는 호스트의 수만큼 이 카운트가 줄어듭니다. 취약성 또는 취약성 범위의 영향을 받을 가능성이 있는 호스트에 대해 취약성을 비활성화하지 않은 경우 이 카운트가 표시되지 않습니다.

영향받았을 가능성이 있는 호스트

두 번째 숫자는 시스템이 취약성의 영향을 받을 가능성이 있는 것으로 판단한, 고유하지 않은 총 호스트의 카운트입니다.

취약성을 비활성화하면 지정한 호스트에 대해서만 비활성이 적용됩니다. 취약한 것으로 판단한 모든 호스트에 대해 또는 취약한 개별 지정 호스트에 대해 취약성을 비활성화할 수 있습니다. 취약성이 비활성화되면, 해당하는 호스트의 IP 주소가 네트워크 맵에서 회색 기울임꼴로 표시됩니다. 또한 그러한 호스트의 호스트 프로파일에는 비활성화된 취약성이 무효 상태로 표시됩니다.

그 후 비활성화되지 않은 호스트(예: 네트워크 맵의 새 호스트)에서 취약성이 탐지되면, 시스템은 해당 호스트에 대해 취약성을 활성화합니다. 새로 검색된 취약성은 명시적으로 비활성화해야 합니다. 또한 호스트에 대해 운영체제 또는 애플리케이션 변경이 탐지되면 시스템은 비활성화된 관련 취약성을 다시 활성화할 수 있습니다.

호스트 속성 네트워크 맵

Host Attributes(호스트 속성) 탭의 네트워크 맵은 네트워크 상의 호스트를 사용자 정의 또는 규정준수 허용 목록 호스트 속성 중 하나를 기준으로 조직화해 표시합니다. 이 화면에서는 사전 정의된 호스트 속성을 이용해 호스트를 조직화할 수는 없습니다.

호스트를 구성하는 데 사용할 호스트 속성을 선택하면, management center은(는) 네트워크 맵에서 해당 특성에 대해 사용할 수 있는 값을 나열하고 할당된 값을 기반으로 호스트를 그룹화합니다. 예를 들어 허용 목록 호스트 속성을 기준으로 호스트를 조직화하는 경우, 시스템은 호스트를 Compliant(규정준수), Non-Compliant(규정 미준수), Not Evaluated(미평가) 카테고리로 구분해 표시합니다.

또한 특정 호스트 속성 값이 할당된 호스트의 호스트 프로파일을 볼 수도 있습니다.

관련 항목

호스트 프로파일의 호스트 속성, 910 페이지

네트워크 맵 보기

네트워크 맵을 보려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(분석)** > **Hosts(호스트)** > **Network Map(네트워크 맵)**를 선택합니다.

단계 **2** 보려는 네트워크 맵을 클릭합니다.

단계 **3** 해당하는 작업을 계속 진행합니다.

- 도메인 선택 — 다중 도메인 환경의 경우, **Domain(도메인)** 드롭다운 목록에서 리프 도메인을 선택합니다.
- 호스트 필터링 — IP 주소 또는 MAC 주소로 필터링하려는 경우, 검색 필드에 주소를 입력합니다. 검색을 지우려면 **Clear(지우기)** ( )을 클릭합니다.
- 드릴다운 — 카테고리 또는 호스트 프로파일을 조사하려는 경우, 맵의 카테고리 또는 서브넷을 드릴다운합니다. 맞춤형 토폴로지가 정의된 경우 보려는 **Hosts(호스트)**에서 **(topology)(토폴로지)**를 클릭한 다음, 기본 보기로 다시 토글하려면 **(hosts)(호스트)**를 클릭합니다.
- 삭제 — 해당 요소 옆에 있는 **Delete(삭제)** ( )을 클릭합니다.
  - **Hosts(호스트)**, **Network Devices(네트워크 디바이스)**, **Mobile Devices(모바일 디바이스)** 또는 **Application Protocols(애플리케이션 프로토콜)** 의 맵에서 요소를 제거합니다.
  - **Indications of Compromise(보안 침해 지표)**에서 확인된 IOC 카테고리, 보안 침해된 호스트 또는 보안 침해된 호스트 그룹을 표시합니다.
  - **Vulnerabilities(취약점)**에서 모든 호스트 또는 단일 호스트의 취약점을 비활성화합니다.
- 취약점 등급 지정 — **Vulnerabilities(취약점)**의 **Vulnerabilities(취약점)** 드롭다운 목록에서 보려는 취약점 등급을 선택합니다.

- 구성 속성 지정 — **Host Attributes(**호스트 속성**)**의 **Attribute(**속성**)** 드롭다운 목록에서 속성을 선택합니다.

관련 항목

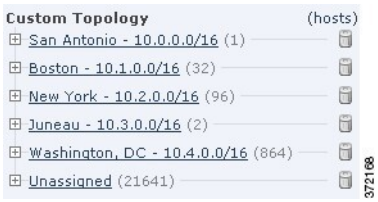
맞춤형 네트워크 토폴로지, 632 페이지
호스트 프로파일, 894 페이지

맞춤형 네트워크 토폴로지

맞춤형 토폴로지 기능을 사용하면 호스트 및 네트워크 디바이스 네트워크 맵에서 서브넷을 구성 및 식별하는 데 도움이 될 수 있습니다.

예를 들어 조직의 각 부서에서 서로 다른 서브넷을 사용하는 경우 맞춤형 토폴로지 기능을 사용하여 서브넷에 레이블을 지정할 수 있습니다.

또한 맞춤형 토폴로지에서 지정한 조직에 따라 호스트 네트워크 맵을 볼 수 있습니다.



다음 방법 중 하나 또는 모두를 사용하여 맞춤형 토폴로지의 네트워크를 지정할 수 있습니다.

- 네트워크 검색 정책에서 네트워크를 가져와 시스템이 모니터링하도록 설정한 네트워크에 추가할 수 있습니다.
- 네트워크를 수동으로 네트워크 토폴로지에 추가할 수 있습니다.

Custom Topology(맞춤형 토폴로지) 페이지는 맞춤형 토폴로지와 토폴로지의 상태를 열거합니다. 정책 이름 옆에 있는 전구 아이콘이 밝게 표시되면 토폴로지가 활성 상태이며 네트워크 맵에 영향을 미치게 됩니다. 아이콘 흐리게 표시된다면, 토폴로지는 비활성 상태입니다.

관련 항목

호스트 네트워크 맵, 626 페이지
네트워크 디바이스 네트워크 맵, 627 페이지

맞춤형 토폴로지 생성

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** 툴바에서 **Custom Topology(**맞춤형 토폴로지**)**를 클릭합니다.

단계 **3** **Create Topology(**토폴로지 생성**)**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **6** 네트워크를 토폴로지에 추가합니다. 다음의 전략 중 하나 또는 모두를 사용할 수 있습니다.

- 네트워크 검색 정책에서 네트워크 가져오기, 633 페이지에 설명된 대로 네트워크 검색 정책에서 네트워크를 가져옵니다.
- 맞춤형 토폴로지에 수동으로 네트워크 추가, 634 페이지에 설명된 대로 네트워크를 수동으로 추가합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 토폴로지 활성화 및 비활성화, 634 페이지에 설명된 대로 토폴로지를 활성화합니다.

네트워크 검색 정책에서 네트워크 가져오기

프로시저

단계 **1** 네트워크를 가져올 맞춤형 토폴로지에 액세스합니다.

- 맞춤형 토폴로지를 생성합니다(맞춤형 토폴로지 생성, 632 페이지 참조).
- 기존 맞춤형 토폴로지를 편집합니다(맞춤형 토폴로지 편집, 635 페이지 참조).

단계 **2** **Import Policy Networks(**정책 네트워크 가져오기**)**를 클릭합니다.

단계 **3** **Load(**로드**)**를 클릭합니다. 시스템은 네트워크 검색 정책에 대한 토폴로지 정보를 표시합니다.

단계 **4** 토폴로지를 정리하려면

- 네트워크 옆에 있는 **Edit(**수정**)** ( )을 클릭하고, 이름을 입력하고, **Rename(**이름 변경**)**을 클릭해 토폴로지의 네트워크 이름을 변경합니다.
- **Delete(**삭제**)** ( )을 클릭하고 **OK(**확인**)**를 클릭해 토폴로지에서 네트워크를 제거합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 토폴로지 활성화 및 비활성화, 634 페이지에 설명된 대로 토폴로지를 활성화합니다.

맞춤형 토폴로지에 수동으로 네트워크 추가

프로시저

단계 **1** 네트워크를 추가할 맞춤형 토폴로지에 액세스합니다.

- 맞춤형 토폴로지를 생성합니다(맞춤형 토폴로지 생성, 632 페이지 참조).
- 기존 맞춤형 토폴로지를 편집합니다(맞춤형 토폴로지 편집, 635 페이지 참조).

단계 **2** **Add Network(**네트워크 추가**)**를 클릭합니다.

단계 **3** 호스트 및 네트워크 디바이스 네트워크 맵에 네트워크에 대한 맞춤형 라벨을 추가하려면, **Name(**이름**)**을 입력합니다.

단계 **4** 추가할 네트워크를 나타내는 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**(IPv4)를 입력합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 맞춤형 토폴로지 활성화 및 비활성화, 634 페이지에 설명된 대로 토폴로지를 활성화합니다.

관련 항목

Firepower System IP 주소 규칙, 28 페이지

맞춤형 토폴로지 활성화 및 비활성화

참고 언제든 하나의 맞춤형 토폴로지만 활성 상태를 유지할 수 있습니다. 여러 토폴로지를 생성한 경우 하나를 활성화하면 현재 활성 상태인 토폴로지는 자동으로 비활성화됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Topology(**맞춤형 토폴로지**)**를 선택합니다.

단계 **3** 토폴로지 옆에 있는 슬라이더를 클릭하여 토폴로지를 활성화 또는 비활성화합니다.

맞춤형 토폴로지 편집

활성 토폴로지에 적용한 변경사항은 즉시 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**을(를) 선택합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **2** **Custom Topology(**맞춤형 토폴로지**)**를 클릭합니다.

단계 **3** 편집할 토폴로지 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** 맞춤형 토폴로지 생성, 632 페이지에 설명된 대로 토폴로지를 편집합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

25 장

조회

다음 주제에서는 Firepower System이 알거나 알지 못하는 개체 관련 정보를 조회하는 방법을 설명합니다.

조회 소개

management center이(가) 인터넷에 연결된 경우, 수동 조회 기능으로 다음 정보를 찾을 수 있습니다.

- 모든 IP 주소에 대한 RIR(Regional Information Registries) 정보(whois)
- URL 필터링 기능으로 분류한 URL 카테고리 및 평판
- 모든 IP 주소에 대한 지리위치 정보: 국가 이름, 국가 코드, 대륙 이름 (최신 지리위치 정보 사용을 위해, Cisco는 management center의 GeoDB(Geolocation Database)를 정기적으로 업데이트할 것을 강력하게 권장합니다.)

관련 항목

GeoDB(지리위치 데이터베이스) 업데이트, 236 페이지

Whois 조회 수행

시작하기 전에

- management center이(가) 인터넷에 액세스할 수 있는지 확인합니다(보안, 인터넷 액세스 및 통신 포트, 1095 페이지 참조).

프로시저

단계 1 **Analysis(분석)** > **Advanced(고급)** > **Whois**을(를) 선택합니다.

단계 2 IP 주소를 입력하고 **Search(검색)**를 클릭합니다.

관련 항목

상황 메뉴, 22 페이지

URL 카테고리 및 평판 찾기

URL의 카테고리와 평판을 수동으로 조회할 수 있습니다. 이 기능을 사용하면 특정 URL을 평가해 정책 처리를 계획, 조정, 문제 해결하거나, Cisco 솔루션 이외의 소스를 통해 사용자의 주의를 끌게 된 문제적 URL을 조사하는 방법을 설명합니다. 이러한 결과에 있는 카테고리와 평판은 URL Filtering(URL 필터링) 기능이 사용하는 것과 동일합니다.

시작하기 전에

- management center이(가) 인터넷에 액세스할 수 있어야 합니다(보안, 인터넷 액세스 및 통신 포트, 1095 페이지 참조).
- URL Filtering(URL 필터링) 및 **Query Cisco cloud for unknown URLs(**알 수 없는 **URL**에 대한 **Cisco Cloud** 쿼리**)** 옵션을 활성화해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *URL* 필터링 장을 참조하십시오.
- 적어도 한 대의 디바이스는 management center에 등록되고 유효한 URL 라이선스가 할당되어 있어야 합니다.
- 이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 1 **Analysis(분석)** > **Advanced(고급)** > **URL**을(를) 선택합니다.

단계 2 최대 250개의 일반적인 형식 퍼블릭, 라우팅 가능 IP 주소를 일반적인 형식으로 입력합니다(예를 들어 URL에는 "http", "www", 하위 도메인이 포함 또는 제외될 수 있으며, URL을 단축할 수도 있습니다). 공백 또는 리턴으로 각 엔터티를 구분합니다.

별표(*) 같은 와일드카드는 지원되지 않습니다.

단계 3 **Search(검색)**를 클릭합니다.

다수의 URL을 입력하면 네트워크가 느려져, 처리에 몇 분 정도 걸릴 수 있습니다.

URL이 유효하지 않다는 오류 메시지가 표시되는 경우에는 철자를 확인하거나 다른 형식의 URL을 입력하십시오. 예를 들자면, "www", "http" 또는 "https" 접두사를 추가하거나 생략하는 식입니다.

URL은 최대 6개의 카테고리에 속할 수 있지만 평판에은 하나만 존재합니다.

단계 **4** (선택 사항) 컬럼 헤드를 클릭하여 결과를 정렬합니다.

단계 **5** (선택 사항) 결과를 CSV 파일로 저장하려는 경우 **Export CSV(CSV** 내보내기**)**를 클릭합니다.

평판 레벨 추가 열은 CSV 파일에 포함되기 때문에 위험별로 정렬할 수 있습니다. 0은 알 수 없는 위험을 나타내며 시스템에 URL에 대한 위험 데이터가 부족한 경우입니다.

다음에 수행할 작업

사용 가능한 범주와 평판 목록을 확인하려는 경우에는 **Policies(**정책**) > Access Control(**액세스 제어**) > Access Control(**액세스 제어**)**로 이동한 다음 정책을 클릭하거나 새 정책을 추가하고, **Add Rule(**규칙 추가**)**을 클릭한 다음 **URLs(URL)**를 클릭합니다.

IP 주소에 대한 지리위치 정보 찾기

지리위치 조회 기능을 이용해 국가 이름, ISO 3166-1 3자리 국가 코드 및 특정 IP 주소와 관련된 대륙 이름을 찾을 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**) > Advanced(**고급**) > Geolocation(**지리위치**)**을(를) 선택합니다.

단계 **2** 하나 이사의 IP 주소에 대한 지리위치 정보를 보려면 주소 또는 주소 모음을 입력하고 **Search(**검색**)**를 클릭합니다. IPv4 주소나 IPv6 주소, 또는 둘 다를 지정할 수 있습니다. 쉼표, 세미콜론, 리턴, 또는 모든 공백 문자를 사용하여 여러 주소를 구분하십시오.

팁 텍스트 상자를 비우려면 **Clear(**지우기**)**를 클릭합니다.

단계 **3** 선택적으로, 열 제목을 클릭하여 데이터를 정렬합니다. IP 주소를 제외한 모든 필드별로 정렬할 수 있습니다.

단계 **4** (선택 사항) 결과를 CSV 파일로 저장하려는 경우 **Export CSV(CSV** 내보내기**)**를 클릭합니다.

관련 항목

GeoDB(지리위치 데이터베이스) 업데이트, 236 페이지

26 장

외부 툴을 사용하여 이벤트 분석

Cisco SecureX와의 통합

단일한 보안 창인 SecureX 클라우드 포털을 통해 모든 Cisco 보안 제품의 데이터를 보고 작업할 수 있습니다. SecureX를 통해 제공되는 툴을 사용하여 위협 추적 및 조사를 보강합니다. SecureX는 각 어플라이언스에서 최적의 소프트웨어 버전을 실행 중인지 여부와 같은 유용한 어플라이언스 및 디바이스 정보도 제공할 수 있습니다.

SecureX에 대한 자세한 내용은 Cisco SecureX 페이지를 참조하십시오.

SecureX 통합 활성화

Cisco SecureX 플랫폼은 가시성을 통합하고 자동화를 가능하게 하며 네트워크, 엔드포인트, 클라우드 및 애플리케이션 전반에서 보안을 강화하는 일관된 경험을 위해 Cisco의 광범위한 통합 보안 포트폴리오와 고객의 인프라를 연결합니다. SecureX에 대한 자세한 내용은 Cisco SecureX 제품 페이지를 참고하십시오.

SecureX를 management center와 통합하면 management center의 모든 데이터에 대한 완전한 개요를 볼 수 있습니다. management center를 SecureX와 통합하는 방법에 대한 자세한 내용은 Cisco Secure Firewall Management Center(7.2 이상 버전) 및 SecureX 통합 가이드를 참고하십시오.

시작하기 전에

조직에 속한 SecureX 계정이 필요합니다.

프로시저

단계 **1** management center에서 **Integration(통합)** > **SecureX**를 선택합니다.

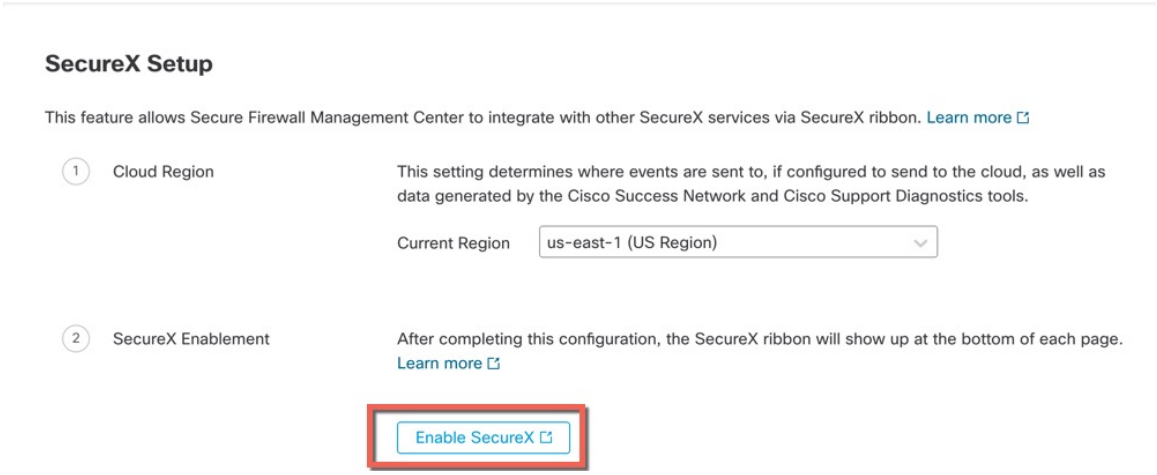
단계 **2** (선택 사항) **Cloud Region(클라우드 지역)**에서 **Current Region(현재 지역)**을 선택합니다.

기본적으로 선택되는 지역은 스마트 라이선싱 지역과 일치하므로 대개 지역을 변경하지 않아도 됩니다.

단계 **3** **SecureX Enablement(SecureX 활성화)**에서 다음 단계를 수행합니다.

a) **Enable SecureX(SecureX 활성화)**를 클릭합니다.

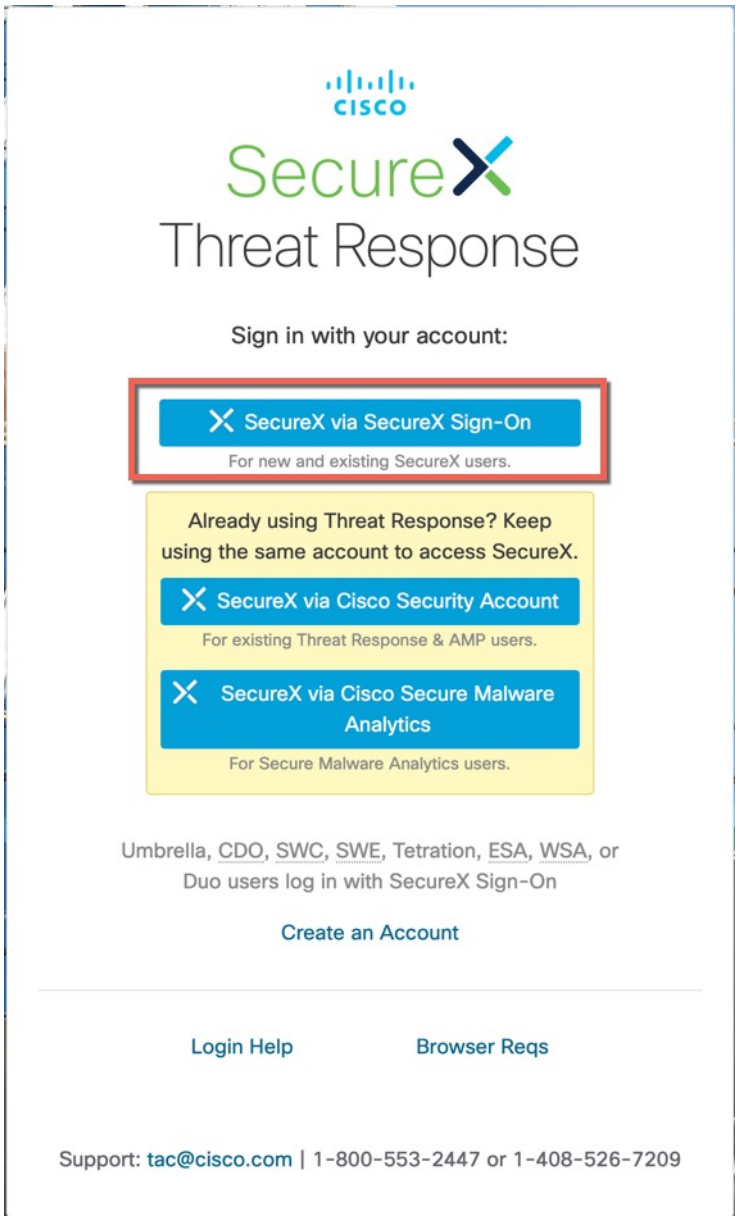
그림 ***11: SecureX*** 활성화



b) SecureX에 로그인합니다.

SecureX 계정에 로그인할 수 있는 별도의 브라우저 탭 또는 창이 열립니다. 이 페이지가 팝업 차단기로 차단되지 않았는지 확인하십시오.

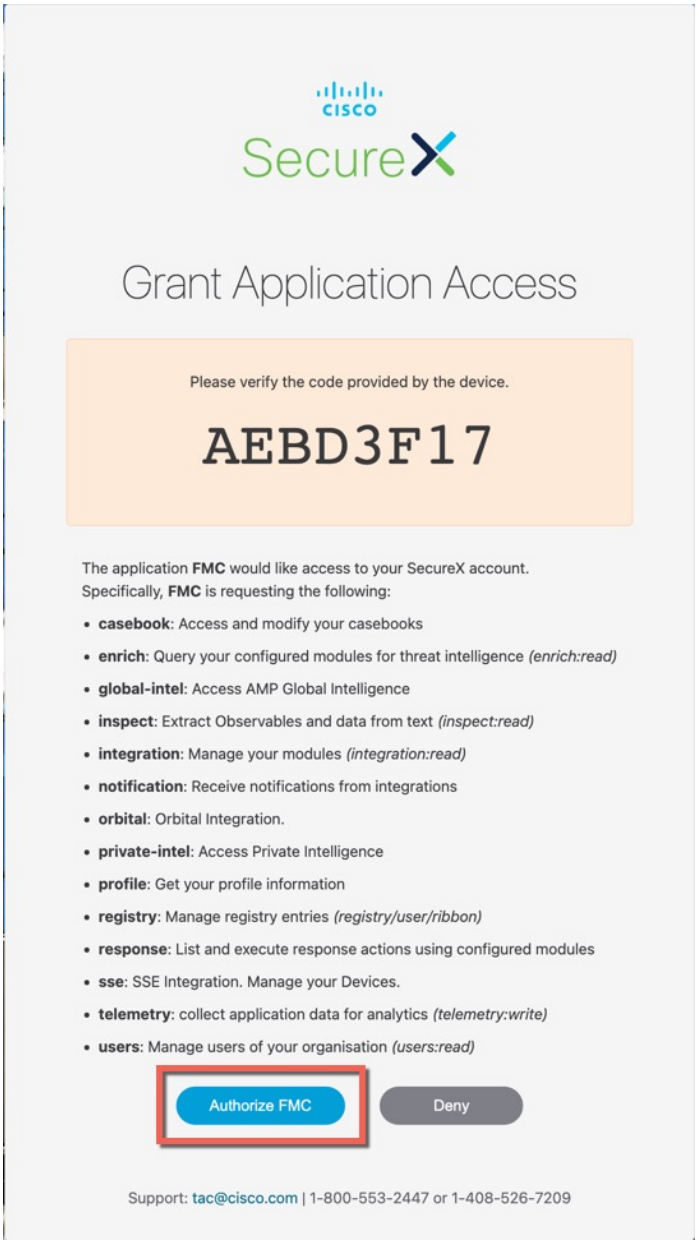
그림 *12: SecureX* 로그인



c) **Authorize FMC(FMC** 권한 부여**)**를 클릭합니다.

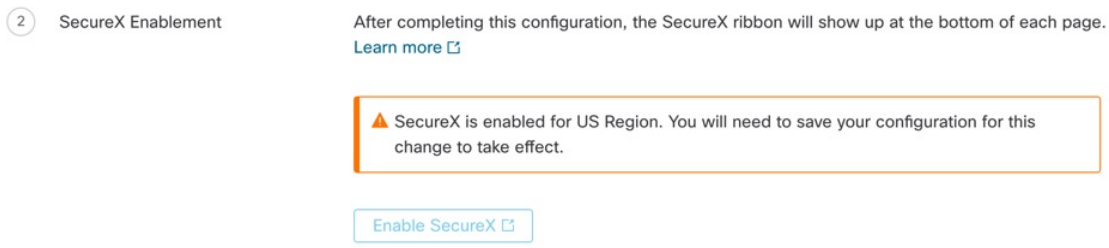
management center에 표시된 코드와 일치하는 코드가 표시됩니다.

그림 *13:* 애플리케이션 액세스 권한 부여



d) management center이 SecureX와 통합되면 성공 메시지가 표시됩니다. **Save(**저장**)**를 클릭합니다.

그림 *14:* 성공 메시지



Cisco Cloud에 이벤트를 전송하도록 Management Center 디바이스 구성

매니지드 위협 방어 디바이스가 이벤트를 클라우드로 직접 전송하도록 management center을 구성합니다. 이 페이지에서 구성하는 클라우드 지역 및 이벤트 유형은 적용 가능하고 활성화된 경우 여러 통합에 사용할 수 있습니다.

시작하기 전에

- management center에서 다음을 수행합니다.
  - **System(**시스템**) > Configuration(**구성**)** 페이지로 이동한 다음, 클라우드의 디바이스 목록에서 명확하게 확인할 수 있도록 management center에 고유한 이름을 지정합니다.
  - management center에 위협 방어 디바이스를 추가하고, 디바이스에 라이선스를 할당하고, 시스템이 올바르게 작동하는지 확인합니다. 필요한 정책을 만들었고 생성된 이벤트가 **Analysis(**분석**)** 탭 아래의 management center 웹 인터페이스에 예상대로 표시되는지 확인합니다.
- 클라우드 인증서가 있는지 확인하고 계정이 생성된 SecureX 지역 클라우드에 로그인할 수 있는지 확인합니다.

  SecureX 지역 클라우드 URL 및 지원되는 디바이스 버전에 대한 자세한 내용은 Cisco Secure Firewall Management Center 및 SecureX 통합 가이드를 참고하십시오.
- 현재 시스템 로그를 사용하여 클라우드로 이벤트를 전송하는 경우 중복을 방지하기 위해 이러한 전송을 비활성화합니다.

프로시저

단계 **1** 방화벽 이벤트 전송에 사용할 Cisco 지역 클라우드를 결정합니다. 지역 클라우드 선택에 대한 자세한 내용은 Cisco Secure Firewall Management Center 및 SecureX 통합 가이드를 참고하십시오.

참고 SecureX가 활성화되고 management center가 선택한 지역 클라우드에 등록된 경우, 지역 클라우드를 변경하면 SecureX가 비활성화됩니다. 지역 클라우드를 변경한 후 다시 SecureX를 활성화할 수 있습니다.

단계 **2** management center에서 **Integration(**통합**)** > **SecureX**로 이동합니다.

단계 **3** **Current Region(**현재 지역**)** 드롭다운에서 지역 클라우드를 선택합니다.

단계 **4** Cisco 클라우드 이벤트 구성을 활성화하고 클라우드에 전송할 이벤트 유형을 선택합니다.

1. 구성을 활성화하려면 **Send events to the cloud(**이벤트를 클라우드로 전송**)** 체크 박스를 선택합니다.
2. 클라우드로 보낼 이벤트 유형을 선택합니다.

참고 클라우드에 전송하는 이벤트를 여러 통합에 사용할 수 있습니다. 다음 테이블을 참고하십시오.

통합	지원되는 이벤트 옵션	**Notes(**참고**)**
Cisco Security Analytics and Logging(SaaS)	모두	높은 우선순위 연결 이벤트는 다음과 같습니다. • Security-related connection events(보안 관련 연결 이벤트) • 파일 및 악성코드 이벤트와 관련된 연결 이벤트 • 침입 이벤트와 관련된 연결 이벤트
Cisco SecureX 및 Cisco SecureX Threat Response	버전에 따라 다름: • 일부 연결 이벤트 • 침입 • 파일 및 악성코드 이벤트	연결 이벤트를 모두 전송하는 경우 Cisco SecureX 및 Cisco SecureX Threat Response에서는 Security Events(보안 이벤트)만 지원합니다.

참고
- **Intrusion Events(**침입 이벤트**)**를 활성화하면 management center 디바이스는 영향 플래그와 함께 이벤트를 전송합니다.
- **File and Malware Events(**파일 및 악성코드 이벤트**)**를 활성화하면 위협 방어 디바이스에서 전송된 이벤트 외에도 management center 디바이스에서 소급 이벤트를 전송합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Cisco Success Network 등록 구성

Cisco Success Network는 사용자가 활성화하는 클라우드 서비스입니다. Cisco Success Network를 활성화하는 경우, management center과 Cisco Cloud 사이에 보안 연결이 설정되어 사용 정보와 통계가 스트리밍됩니다. 이 스트리밍 텔레메트리는 위협 방어에서 관심 있는 데이터를 선택하고 구조화된 형식으로 원격 관리 스테이션에 전송하여 다음과 같은 이점을 얻을 수 있는 메커니즘을 제공합니다.

- 네트워크에서 제품의 효율성을 향상시킬 수있는 활용 가능한 미사용 기능을 알려줍니다.
- 제품에 사용할 수 있는 추가 기술 지원 서비스 및 모니터링에 대해 알려줍니다.
- (SecureX와 통합하는 경우) 어플라이언스 및 디바이스 상태를 SecureX 타일로 요약하고 모든 디바이스에서 최적의 소프트웨어 버전을 실행 중인지 확인합니다.
- Cisco가 제품을 개선할 수 있습니다.

Cisco에서 수집하는 텔레메트리 데이터에 대해 자세히 알아보려면 Cisco Secure Firewall Management Center 디바이스에서 수집한 Cisco Success Network 텔레메트리 데이터를 참고하십시오.

Cisco Support Diagnostics 또는 Cisco Success Network를 활성화하면 management center은 항상 Cisco Cloud와의 보안 연결을 설정하고 유지합니다. 언제든 Cisco Success Network와 Cisco Support Diagnostics를 모두 비활성화하면 이 연결을 끌 수 있으며, 이 경우 management center와(과) Cisco Cloud의 연결이 끊어집니다. 그러나 Cisco Support Diagnostics를 활성화하면 management center 및 위협 방어 둘 다 Cisco Cloud와의 보안 연결을 설정하고 유지합니다.

management center을 Smart Software Manager에 등록할 때 Cisco Success Network를 활성화하십시오. 다음 절차를 사용하여 등록 상태를 확인 또는 변경합니다.

참고 Cisco Success Network는 평가판 모드에서 작동하지 않습니다.

참고 management center에 유효한 Smart Software Manager 온프레미스(이전 명칭: Smart Software Satellite Server) 설정이 있거나 특정 라이선스 예약을 사용하는 경우, Cisco Success Network 기능이 비활성화됩니다.

프로시저

단계 **1** **Integration(통합)** > **SecureX**를 클릭합니다.

단계 **2** **Cisco Cloud Support(Cisco** 클라우드 지원**)** 아래에서 **Enable Cisco Success Network(Cisco Success Network** 활성화**)** 확인란을 선택하여 이 서비스를 활성화합니다.

참고 계속 진행하기 전에 **Enable Cisco Success Network(Cisco Success Network** 활성화**)** 확인란 옆에 있는 정보를 읽어보십시오.

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

Cisco Support Diagnostics를 활성화한 경우 **Integration(**통합**)** > **SecureX**를 클릭하고 **Cloud Region(**클라우드 지역**)** 아래에서 지역별 클라우드 설정을 확인합니다.

Cisco 지원 진단 등록 구성

Cisco Support Diagnostics는 사용자가 활성화하는 클라우드 기반 TAC 지원 서비스입니다. 활성화된 경우 management center 및 매니지드 디바이스는 Cisco 클라우드와의 보안 연결을 설정하여 시스템 상태 관련 정보를 스트리밍합니다.

Cisco Support Diagnostics는 TAC 사례 중에 Cisco TAC가 디바이스에서 필수 데이터를 안전하게 수집하게 하여, 문제 해결 중에 향상된 사용자 경험을 제공합니다. 또한 Cisco는 정기적으로 상태 데이터를 수집하고 자동화된 문제 감지 시스템을 사용하여 데이터를 처리하여 문제를 알려줍니다. TAC 사례 중의 데이터 수집 서비스는 지원 계약을 한 모든 사용자가 이용할 수 있지만, 알림 서비스는 특정 서비스 계약이 있는 사용자만 사용할 수 있습니다.

Cisco Support Diagnostics 또는 Cisco Success Network를 활성화하면 management center는 Cisco Cloud와의 보안 연결을 설정하고 유지합니다. 언제든 Cisco Success Network와 Cisco Support Diagnostics를 모두 비활성화하면 이 연결을 끌 수 있으며, 이 경우 이상의 기능과 Cisco Cloud의 연결이 끊어집니다. 그러나 Cisco Support Diagnostics를 활성화하면 위협 방어 및 management center 둘 다 Cisco Cloud와의 보안 연결을 설정하고 유지합니다.

management center에서 수집된 데이터의 샘플 파일을 보려면 특정 시스템 기능에 대한 문제 해결 파일 생성 단계를 수행합니다.

management center는 수집된 데이터를 **Integration(**통합**)** > **SecureX** 페이지의 **Current Region(**현재 지역**)** 드롭다운에서 선택한 지역 클라우드로 전송합니다.

Cisco Support Diagnostics는 Cisco Smart Software Manager를 이용해 management center를 등록할 때 활성화합니다. 다음 절차를 사용하여 Cisco Support Diagnostics 등록 상태를 확인 또는 변경합니다.

프로시저

단계 **1** **Integration(**통합**)** > **SecureX**를 클릭합니다.

단계 **2** **Cisco Cloud Support(Cisco** 클라우드 지원**)** 아래에서 **Enable Cisco Support Diagnostics(Cisco** 지원 진단 활성화**)** 확인란을 선택하여 이 서비스를 활성화합니다.

참고 계속 진행하기 전에 **Enable Cisco Support Diagnostics(Cisco** 지원 진단 활성화**)** 확인란 옆에 있는 정보를 읽어보십시오.

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

Cisco Support Diagnostics를 활성화한 경우 **Integration(통합)** > **SecureX**를 클릭하고 **Cloud Region(클라우드 지역)** 아래에서 지역별 클라우드 설정을 확인합니다.

Ribbon을 사용한 SecureX 액세스

리본은 management center 웹 인터페이스에서 모든 페이지의 하단에 표시됩니다. 이 리본을 사용하여 다른 Cisco 보안 제품으로 빠르게 피봇하고 여러 소스의 위협 데이터로 작업할 수 있습니다.

시작하기 전에

- management center 웹 인터페이스 페이지 하단에 SecureX 리본이 표시되지 않으면 이 절차를 사용하지 마십시오.

  대신 Cisco Secure Firewall Threat Defense 및 SecureX 통합 설명서를 참고하십시오.

- SecureX 계정이 아직없는 경우 IT 부서에서 구하십시오.

프로시저

단계 **1** management center에서 management center 페이지의 하단에 있는 리본을 클릭합니다.

단계 **2** **Get SecureX(SecureX 가져오기)**를 클릭합니다.

단계 **3** SecureX에 로그인합니다.

단계 **4** 액세스 권한을 부여하려면 링크를 클릭합니다.

단계 **5** 확장하여 사용하려면 해당 리본을 클릭합니다.

다음에 수행할 작업

리본 기능 및 사용 방법에 대한 자세한 내용은 SecureX의 온라인 도움말을 참조하십시오.

다음을 이용한 이벤트 분석 SecureX Threat Response

SecureX threat response는 이전에는 CTR (Cisco Threat Response)로 알려졌습니다.

Secure Firewall을 포함해 여러 제품에서 집계한 데이터를 사용하여 인시던트를 분석할 수 있는, Cisco Cloud의 통합 플랫폼인 SecureX threat response을(를) 사용하여 위협을 빠르게 탐지하고, 조사하고 응답할 수 있습니다.

- SecureX threat response에 대한 일반 정보는 다음을 참조하십시오

  Cisco SecureX Threat Response 제품 페이지.

- SecureX threat response과 Firepower 통합에 대한 자세한 지침은 다음을 참조하십시오.

- Cisco Secure Firewall Threat Defense 및 Cisco SecureX Threat Response 통합 가이드를 참조하십시오.

SecureX Threat Response에서 이벤트 데이터 보기

시작하기 전에

- Cisco Secure Firewall Threat Defense 및 Cisco SecureX Threat Response 통합 가이드에서 설명한 대로 통합을 설정합니다.
- SecureX threat response의 온라인 도움말을 검토해 위협을 찾고, 조사하고, 조치하는 방법을 확인하십시오.
- SecureX threat response에 액세스하려면 자격 증명이 필요합니다.

프로시저

단계 **1** Secure Firewall Management Center에서 다음과 같이 합니다.

- 특정 이벤트에서 SecureX threat response(으)로 피벗하는 방법:

  a. **Analysis(분석) > Intrusions(침입)** 메뉴에서 지원되는 이벤트를 나열하는 페이지로 이동합니다.

  b. 소스 또는 대상 IP 주소를 마우스 오른쪽 버튼으로 클릭하고 **View in SecureX(SecureX에서 보기)**를 선택합니다.

단계 **2** 메시지가 표시되면 SecureX threat response에 로그인합니다.

웹 기반 리소스를 사용한 이벤트 조사

상황별로 크로스 실행 기능을 사용하면 Secure Firewall Management Center 외부에 있는 웹 기반 리소스의 잠재 위협에 관한 자세한 정보를 빠르게 확인할 수 있습니다. 예를 들어 다음 작업을 할 수 있습니다.

- 알려졌거나 의심스러운 위협에 관한 정보를 게시하는, Cisco 또는 서드파티 클라우드가 호스트한 서비스에서 의심스러운 소스 IP 주소를 조회합니다.
- 조직의 기록 로그에서 특정 위협의 과거 인스턴스를 찾습니다(조직이 해당 데이터를 SIEM(Security Information and Event Management) 애플리케이션에 저장하는 경우).
- 파일 경로 정보를 포함한 특정 파일 관련 정보를 찾습니다(조직이 Cisco AMP for Endpoints를 구축한 경우).

이벤트를 조사할 때, Secure Firewall Management Center의 이벤트 뷰어나 대시보드에서 이벤트를 클릭하면 외부 리소스의 관련 정보로 바로 이동할 수 있습니다. 이렇게 하면 특정 이벤트 관련 정보를 해당 이벤트의 IP 주소, 포트, 프로토콜, 도메인 및 SHA 256 해시를 기반으로 빠르게 수집할 수 있습니다.

예를 들어 Top Attackers(상위 공격자) 대시보드 위젯을 찾는 중이며, 나열된 소스 IP 주소 중 하나에 관한 자세한 정보를 찾고 싶다고 가정하겠습니다. Talos가 이 IP 주소에 대해 게시하는 정보를 봐야 하니, "Talos IP" 리소스를 선택합니다. Talos 웹 사이트가 이 특정 IP 주소 관련 정보가 있는 페이지를 엽니다.

Cisco와 서드파티 위협 정보 서비스에 대한 사정 정의된 링크 모음에서 하나를 선택하고, 맞춤형 링크를 다른 웹 기반 서비스에 추가하고, SIEM 또는 웹 인터페이스가 있는 다른 제품에 추가합니다. 일부 리소스는 계정 또는 제품 구매를 요구할 수도 있습니다.

상황별 크로스 실행 리소스 관리 정보

Analysis(분석**) > Advanced(**고급**) > Contextual Cross-Launch(**상황별 크로스 실행**)** 페이지를 이용해 외부 웹 기반 리소스를 관리합니다.

예외: 다음에 대한 교차 실행 링크 설정 Secure Network Analytics, 654 페이지의 절차에 따라 Secure Network Analytics 어플라이언스에 대한 교차 실행 링크를 관리합니다.

Cisco가 제공하는 사정 정의된 리소스에는 Cisco 로고가 표시됩니다. 나머지 링크는 서드파티 리소스입니다.

필요 없는 리소스는 비활성화하거나 삭제할 수 있으며, 이름을 변경할 수도 있습니다. 리소스가 목록 맨 아래에 정렬되도록 소문자 "z"로 시작하는 이름을 지정하는 식입니다. 교차 실행 리소스를 비활성화하면 모든 사용자에 대해 비활성화됩니다. 삭제한 리소스는 다시 설치할 수 없지만 다시 만들 수는 있습니다.

리소스를 추가하려면 상황별 크로스 실행 리소스 추가, 652 페이지 섹션을 참조하십시오.

맞춤형 상황별 크로스 실행 리소스 요구 사항

맞춤형 상황별로 크로스 실행 리소스를 추가하는 경우:

- 웹 브라우저를 통해 리소스를 액세스할 수 있어야 합니다.
- Http 및 https 프로토콜만 지원됩니다.
- GET 요청만 지원됩니다. POST 요청은 지원되지 않습니다.
- URL의 변수 인코딩은 지원되지 않습니다. IPv6 주소는 콜론 구분자 인코딩을 요구할 수 있지만, 대부분의 서비스는 이러한 인코딩을 요구하지 않습니다.
- 사전 정의된 리소스를 포함한 리소스를 100개까지 설정할 수 있습니다.
- 교차 실행을 생성하려면 관리자 또는 보안 분석가 사용자여야 하지만 읽기 전용 보안 분석가로 사용할 수도 있습니다.

상황별 크로스 실행 리소스 추가

보안 인텔리전스 서비스나 SIEM(Security Information and Event Management) 툴 같은 상황별로 크로스 실행 리소스를 추가할 수 있습니다.

다중 도메인 구축의 경우, 상위 도메인의 리소스는 보고 사용할 수 있지만 현재 도메인의 리소스는 생성 및 편집만 할 수 있습니다. 전체 도메인의 총 리소스 수는 100개로 제한됩니다.

시작하기 전에

- Secure Network Analytics 어플라이언스에 링크를 추가하는 경우 원하는 링크가 이미 있는지 확인하십시오. 대부분의 링크는 설정 시 자동으로 생성됩니다.Security Analytics and Logging(보안 애널리틱스)의 내용을 참조하십시오..
- 맞춤형 상황별 크로스 실행 리소스 요구 사항, 651 페이지의 내용을 참조하십시오.
- 링크할 리소스에 필요하다면, 계정과 액세스에 필요한 자격 증명을 생성 또는 획득합니다. 선택적으로, 액세스가 필요한 각 사용자에게 자격 증명을 할당하고 배포합니다.
- 링크할 리소스에 대한 쿼리 링크의 구문을 확인합니다.

  브라우저를 통해 리소스에 액세스하고, 필요에 따라 해당 리소스에 대한 문서를 사용하여 쿼리 링크가 찾아야 할 정보 유형(예 IP 주소)의 샘플을 검색하는 데 필요한 쿼리 링크를 작성합니다

  쿼리를 실행하고 브라우저의 위치 표시줄에서 결과 URL을 복사합니다.

  예를 들어 쿼리 URL이 **`https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10`** 일 수 있습니다.

프로시저

단계 **1** **Analysis(분석) > Advanced(고급) > Contextual Cross-Launch(상황별 크로스 실행)**를 선택합니다.

단계 **2** **New Cross-Launch(새 크로스 실행)**를 클릭합니다.

표시되는 양식에서, 별표가 있는 필드는 값을 입력해야 합니다.

단계 **3** 고유한 리소스 이름을 입력합니다.

단계 **4** 리소스의 작업 URL 문자열을 복사해 **URL Template(URL 템플릿)** 필드에 붙여넣습니다.

단계 **5** 쿼리 문자열의 특정 데이터(IP 주소 등)를 적절한 변수로 교체합니다. 커서를 놓은 다음 변수(예: **ip**)를 한 번 클릭하여 변수를 삽입합니다.

위의 "Before You Begin(시작하기 전에)" 색션에서, 결과 URL은 **`https://www.talosintelligence.com/reputation_center/lookup?search={ip}`**일 것입니다. 상황별로 크로스 실행 링크를 사용하는 경우, URL의 {ip} 변수는 이벤트 뷰어 또는 대시보드에서 사용자가 오른쪽 클릭한 IP 주소로 교체됩니다.

각 변수에 대한 설명을 보려면 커서를 변수 위에 올리십시오.

하나의 툴이나 서비스로 여러 상황별로 크로스 실행 링크를 만들 수 있으며, 이 경우 각 항목에 다른 변수를 사용해야 합니다.

단계 **6** 예시 데이터로 링크를 테스트하려면 **Test with example data(**예제 데이터를 사용한 테스트**)** ( )을 클릭합니다.

단계 **7** 문제를 해결합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

상황별 크로스 실행을 이용한 이벤트 조사

시작하기 전에

액세스하는 리소스가 자격 증명을 요구하는 경우, 해당 자격 증명이 있는지 확인하십시오.

프로시저

단계 **1** 이벤트를 표시하는 Secure Firewall Management Center의 다음 페이지 중 하나로 이동합니다.

- 대시보드(**Overview(**개요**)** > **Dashboards(**대시보드**)**) 또는
- 이벤트 뷰어 페이지(이벤트의 테이블을 포함하는 **Analysis(**분석**)** 메뉴의 아무 메뉴 옵션)

단계 **2** 관심 있는 이벤트를 오른쪽 클릭하고 사용할 상황별로 크로스 실행 리소스를 선택합니다.

필요한 경우 콘텍스트 메뉴를 내려 사용할 수 있는 옵션을 모두 확인합니다

오른쪽 클릭한 데이터 유형에 따라 표시되는 옵션이 달라집니다. 예를 들어 IP 주소를 오른쪽 클릭하면 IP 주소 관련 상황별로 크로스 실행 옵션만 표시됩니다.

따라서 예를 들어 Cisco Talos에서 Top Attackers(상위 공격자) 대시보드 위젯의 소스 IP 주소 관련 위협 정보를 얻으려면, **Talos SrcIP** 또는 **Talos IP**를 선택합니다.

리소스에 여러 변수가 있는 경우, 해당 리소스를 선택하는 옵션은 포함된 각 변수에 대한 단일 유효 값이 있는 이벤트에서만 사용할 수 있습니다.

별도의 브라우저 창에 상황별로 크로스 실행 리소스가 열립니다.

쿼리하는 데이터 양, 리소스의 속도 및 요구 등의 요소에 따라 쿼리 처리에 시간이 오래 걸릴 수도 있습니다.

단계 **3** 필요한 경우 리소스에 로그인합니다.

다음에 대한 교차 실행 링크 설정 Secure Network Analytics

Firepower의 이벤트 데이터에서 Secure Network Analytics 어플라이언스의 관련 데이터로 교차 실행할 수 있습니다. Secure Network Analytics 제품에 대한 자세한 내용은 https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html의 내용을 참조하십시오.

상황별 교차 실행에 대한 일반적인 정보는 상황별 크로스 실행을 이용한 이벤트 조사, 653 페이지의 내용을 참조하십시오.

Secure Network Analytics 어플라이언스에 대한 일련의 교차 실행 링크를 빠르게 설정하려면 이 절차를 사용합니다.

참고

- 나중에 해당 링크를 변경해야 하는 경우 이 절차로 돌아갑니다. 상황별 교차 실행 목록 페이지에서는 직접 변경할 수 없습니다.
- 상황별 크로스 실행 리소스 추가, 652 페이지의 절차를 사용하여 Secure Network Analytics 어플라이언스에 교차 실행하는 추가 링크를 수동으로 생성할 수 있지만 해당 링크는 자동으로 생성된 리소스와 무관하므로 수동으로 관리(삭제, 업데이트 등)해야 합니다.

시작하기 전에

Secure Network Analytics 어플라이언스가 구축되어 실행되고 있어야 합니다.

Security Analytics and Logging(보안 애널리틱스)을 사용하여 Secure Network Analytics 어플라이언스에 Firepower 데이터를 전송하려면 Secure Network Analytics 어플라이언스의 원격 데이터 스토리지, 535 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **System(**시스템**) > Logging(**로깅**) > Security Analytics & Logging(**보안 분석 및 로깅**)**을 선택합니다.

단계 **2** 기능을 활성화합니다.

단계 **3** Secure Network Analytics 어플라이언스의 호스트 이름이나 IP 주소, 포트를 입력합니다.

기본 포트는 443입니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 새 교차 실행 링크를 확인합니다. **Analysis(**분석**) > Advanced(**고급**) > Contextual Cross-Launch(**상황별 교차 실행**)**를 선택합니다.

변경이 필요한 경우 이 절차로 돌아갑니다. 상황별 교차 실행 목록 페이지에서는 직접 변경할 수 없습니다.

다음에 수행할 작업

이벤트에서 Secure Network Analytics 이벤트 뷰어로 교차 실행하려면 Secure Network Analytics 자격 증명이 필요합니다.

management center 이벤트 보기 또는 대시보드의 이벤트에서 교차 실행하려면 관련 이벤트의 테이블 셀을 마우스 오른쪽 버튼으로 클릭하고 적절한 옵션을 선택합니다.

쿼리하는 데이터 양, Secure Network Analytics Manager의 속도 및 요구 등의 요소에 따라 쿼리 처리에 시간이 오래 걸릴 수도 있습니다.

보안 이벤트에 대한 시스템 로그 메시지 전송 정보

시스템 로그를 통해 연결, 보안 인텔리전스, 침입, 파일 및 악성 프로그램 이벤트 관련 데이터를 SIEM(Security Information and Event Management) 툴 또는 다른 외부 이벤트 스토리지 및 관리 솔루션에 전송할 수 있습니다.

때로는 이러한 이벤트를 Snort® 이벤트라고 지칭하기도 합니다.

보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 구성 정보

보안 이벤트 시스템 로그를 전송하도록 시스템을 설정하려면, 다음 항목을 알고 있어야 합니다.

- 보안 이벤트 시스템 로그 메시지 구성 모범 사례, 655 페이지
- 보안 이벤트 시스템 로그에 대한 구성 위치, 660 페이지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 이벤트 시스템 로그 메시지에 적용되는 *FTD* 플랫폼 설정을 참고하십시오.
- 정책에서 시스템 로그 설정을 변경하는 경우, 변경사항은 재구축해야 효력을 발휘합니다.

보안 이벤트 시스템 로그 메시지 구성 모범 사례

디바이스 및 버전	설정 위치
모두	Syslog를 사용하거나 이벤트를 외부에 저장하려는 경우 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.

디바이스 및 버전	설정 위치
Secure Firewall Threat Defense	1. **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**) > Threat Defense Settings(**위협 방어 설정**) > Syslog(**시스템 로그**)**에서 FTD 플랫폼 설정을 구성합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 이벤트 *Syslog* 메시지에 적용되는 *FTD* 플랫폼 설정을 참조하십시오. 2. 액세스 컨트롤 정책 Logging(로깅) 탭에서, FTD 플랫폼 설정 사용을 선택합니다. 3. (침입 이벤트의 경우) 액세스 제어 정책 Logging(로깅) 탭의 설정을 사용하도록 침입 정책을 구성합니다. (기본값입니다.) 이런 설정을 재정의하는 것은 권장하지 않습니다. 자세한 내용은 Threat Defense 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 656 페이지의 내용을 참조하십시오.
기타 모든 디바이스	1. 알림 응답을 생성합니다. 2. 알림 응답을 사용하도록 액세스 제어 정책 Logging(로깅)을 설정합니다. 3. (침입 이벤트) 침입 정책에서 시스템 로그 설정을 구성합니다. 자세한 내용은 클래식 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 659 페이지의 내용을 참조하십시오.

Threat Defense 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기

이 절차에서는 Secure Firewall Management Center 디바이스에서 보안 이벤트(연결, 보안 인텔리전스, 침입, 파일 및 악성코드 이벤트)에 대한 시스템 로그 메시지를 전송하기 위한 모범 사례 설정을 설명합니다.

참고 대부분의 threat defense 시스템 로그 설정은 보안 이벤트에 적용되지 않습니다. 이 절차에 설명된 옵션만 설정하십시오.

시작하기 전에

- Secure Firewall Management Center에서 보안 이벤트를 생성하도록 정책을 설정하고 표시될 것으로 예상되는 이벤트가 Analysis(분석) 메뉴의 해당 테이블에 나타나는지 확인합니다.
- 시스템 로그 서버 IP 주소, 포트 및 프로토콜(UDP 또는 TCP)을 수집합니다.
- 디바이스가 시스템 로그 서버에 연결할 수 있는지 확인합니다.

- 시스템 로그 서버가 원격 메시지를 수락할 수 있는지 확인합니다.
- 연결 로깅에 대한 중요 정보는 연결 로깅, 753 페이지의 관련 챕터를 참조하십시오.

프로시저

단계 **1** threat defense 디바이스에 대한 시스템 로그 설정을 구성합니다.

a) **Devices(**디바이스**) > Platform Settings(**플랫폼 설정**)**를 클릭합니다.
b) threat defense 디바이스와 연결된 플랫폼 설정 정책을 편집합니다.
c) 왼쪽 탐색 창에서 시스템 로그를 클릭합니다.
d) **Syslog Servers(**시스템 로그 서버**)**를 클릭하고 **Add(**추가**)** ( )를 클릭하여 서버, 프로토콜, 인터페이스 및 관련 정보를 입력합니다.

   이 페이지의 옵션에 대한 질문이 있는 경우 의 "시스템 로그 서버 설정" 항목Cisco Secure Firewall Management Center 디바이스 구성 가이드을 참조하십시오.

e) **Syslog Settings(**시스템 로그 설정**)**를 클릭하고 다음 설정을 구성합니다.
   - 시스템 로그 메시지에서 타임스탬프 활성화
   - 타임스탬프 형식
   - 시스템 로그 디바이스 **ID** 활성화

f) **Logging Setup(**로깅 설정**)**을 클릭합니다.
g) **Basic Logging Settings(**기본 로깅 설정**)**에서 **Send syslogs in EMBLEM format(EMBLEM** 형식으로 시스템 로그 전송**)** 여부를 선택합니다.
h) 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

단계 **2** 액세스 제어 정책(파일 및 악성코드 로깅 포함)에 대한 일반 로깅 설정을 구성합니다.

a) **Policies(**정책**) > Access Control(**액세스 제어**)**을 클릭합니다.
b) 해당 액세스 제어 정책을 편집합니다.
c) **More(**더 보기**) > Logging(**로깅**)**을 클릭합니다.
d) Threat Defense 6.3 이상: **Use the syslog settings configured in the Threat Defense Platform Settings policy deployed on the device(**디바이스에 구축된 **Threat Defense** 플랫폼 설정 정책에 구성된 시스템 로그 설정을 사용합니다**.)** 를 선택합니다.
e) (선택 사항) **Syslog Severity(**시스템 로그 심각도**)**를 선택합니다.
f) 파일 및 악성코드 이벤트를 전송하려면 **Send Syslog messages for File and Malware events(**파일 및 악성코드 이벤트에 대해 시스템 로그 메시지 전송**)**를 선택합니다.
g) **Save(**저장**)**를 클릭합니다.

단계 **3** 액세스 제어 정책에 대한 보안 인텔리전스 이벤트에 대한 로깅을 활성화합니다.

a) 동일한 액세스 제어 정책에서 **Security Intelligence(**보안 인텔리전스**)** 탭을 클릭합니다.
b) 다음 각 위치에서 **Logging(**로깅**)** ( )를 클릭하여 연결의 시작과 끝 및 시스템 로그 서버를 활성화합니다.

- **DNS Policy(DNS** 정책**)** 옆.
- **Block List(**차단 목록**)** 상자에서 **Networks(**네트워크**)** 및 **URL**에 대해.

c) **Save(**저장**)**를 클릭합니다.

단계 **4** 액세스 제어 정책에서 각 규칙에 대해 syslog 로깅을 활성화합니다.

a) 동일한 액세스 제어 정책에서 **Access Control(**액세스 제어**)** > **Add Rule(**규칙 추가**)**을 클릭합니다.
b) 편집할 규칙을 선택합니다.
c) 규칙에서 **Logging(**로깅**)** 탭을 클릭합니다.
d) 연결의 시작 또는 종료를 기록할지 아니면 둘 다 기록 할지를 선택합니다.

(연결 로깅은 많은 양의 데이터를 생성합니다. 시작과 끝을 모두 로깅하면 데이터 양이 약 2배 증가합니다. 모든 연결을 처음과 끝에서 모두 로깅할 수있는 것은 아닙니다.)

e) 파일 이벤트를 로깅할 경우 **Log Files(**로그 파일**)**를 선택합니다.
f) **Syslog Server(**시스템 로그 서버**)**를 활성화합니다.
g) 규칙이 "**Using default syslog configuration in Access Control Logging(**세스 제어 기록에서 기본 시스템 로그 컨피그레이션 사용**)**"인지 확인합니다.
h) **OK(**확인**)**를 클릭합니다.
i) 정책의 각 규칙에 대해 반복합니다.

단계 **5** 침입 이벤트를 전송할 경우 다음을 수행합니다.

a) 액세스 제어 정책과 연결된 침입 정책으로 이동합니다.
b) 침입 정책에서 **Advanced Settings(**고급 설정**)** > **Syslog Alerting(**시스템 로그 알림**)** > **Enabled(**활성화**)**를 선택합니다.
c) 필요한 경우 **Edit(**편집**)**을 클릭합니다.
d) 옵션을 입력합니다.

옵션	값
로깅 호스트	다른 시스템 로그 메시지를 전송하는 것 이외의 다른 시스템 로그 서버로 침입 이벤트 시스템 로그 메시지를 보내지 않는 한 위에서 구성한 설정을 사용하려면 이 필드를 비워 두십시오.
기능	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. 자세한 내용은 시스템 로그 알림 시설, 574 페이지를 참조하십시오.
심각도	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. 자세한 내용은 시스템 로그 심각도 레벨, 575 페이지를 참조하십시오.

e) **Back(**뒤로**)**을 클릭합니다.
f) 탐색창에서 **Policy Information(**정책 정보**)**을 클릭합니다.

g) **Commit Changes(**변경 커밋**)**를 클릭합니다.

다음에 수행할 작업

- (선택 사항) 개별 정책 및 규칙에 대해 서로 다른 로깅 설정을 구성합니다.

  연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치(모든 디바이스), 661 페이지의 해당 테이블 행을 참조하십시오.

  이러한 설정에는 시스템 로그 알림 응답 생성, 573 페이지에 설명된 대로 구성된 시스템 로그 알림 응답이 필요합니다. 이 절차에서 설정한 플랫폼 설정은 사용하지 않습니다.

- 클래식 디바이스에 대한 보안 이벤트 시스템 로그 로깅을 설정하려면 클래식 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 659 페이지의 내용을 참조하십시오.
- 변경을 완료한 경우, 매니지드 디바이스에 변경 사항을 구축합니다.

클래식 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기

시작하기 전에

- 보안 이벤트를 생성하도록 정책을 설정합니다.
- 디바이스가 시스템 로그 서버에 연결할 수 있는지 확인합니다.
- 시스템 로그 서버가 원격 메시지를 수락할 수 있는지 확인합니다.
- 연결 로깅에 대한 중요 정보는 연결 로깅, 753 페이지의 관련 챕터를 참조하십시오.

프로시저

단계 **1** 클래식 디바이스에 대한 알림 응답을 설정합니다.

시스템 로그 알림 응답 생성, 573 페이지의 내용을 참조하십시오.

단계 **2** 액세스 제어 정책에서 시스템 로그 설정을 구성합니다.

a) **Policies(**정책**) > Access Control(**액세스 제어**)**을 클릭합니다.
b) 해당 액세스 제어 정책을 편집합니다.
c) **Logging(**로깅**)**을 클릭합니다.
d) **Send using specific syslog alert(**특정 시스템 로그 알림을 사용하여 전송**)**을 선택합니다.
e) 위에서 생성한 시스템 로그 알림을 선택합니다.
f) **Save(**저장**)**를 클릭합니다.

단계 **3** 파일 및 악성코드 이벤트를 전송할 경우, 다음을 수행합니다.

a) **Send Syslog messages for File and Malware events(**파일 및 악성코드 이벤트에 대한 시스템 로그 메시지 전송**)**를 선택합니다.

b) **Save(**저장**)**를 클릭합니다.

단계 **4** 침입 이벤트를 전송할 경우, 다음을 수행합니다.

a) 액세스 제어 정책과 연결된 침입 정책으로 이동합니다.

b) 침입 정책에서 **Advanced Settings(**고급 설정**) > Syslog Alerting(**시스템 로그 알림**) > Enabled(**활성화**)**를 선택합니다.

c) 필요한 경우 **Edit(**편집**)**을 클릭합니다.

d) 옵션을 입력합니다.

옵션	값
로깅 호스트	다른 시스템 로그 메시지를 전송하는 것 이외의 다른 시스템 로그 서버로 침입 이벤트 시스템 로그 메시지를 보내지 않는 한 위에서 구성한 설정을 사용하려면 이 필드를 비워 두십시오.
기능	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. 시스템 로그 알림 시설, 574 페이지의 내용을 참조하십시오.
심각도	이 설정은 이 페이지에서 Logging Host(로깅 호스트)를 지정한 경우에만 적용할 수 있습니다. 시스템 로그 심각도 레벨, 575 페이지의 내용을 참조하십시오.

e) **Back(**뒤로**)**을 클릭합니다.

f) 탐색창에서 **Policy Information(**정책 정보**)**을 클릭합니다.

g) **Commit Changes(**변경 커밋**)**를 클릭합니다.

다음에 수행할 작업

- (선택 사항) 개별 액세스 제어 규칙에 대해 서로 다른 로깅 설정을 구성합니다. 연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치(모든 디바이스), 661 페이지의 해당 테이블 행을 참조하십시오. 이러한 설정에는 시스템 로그 알림 응답 생성, 573 페이지에 설명된 대로 구성된 시스템 로그 알림 응답이 필요합니다. 위에서 구성한 설정은 사용하지 않습니다.
- FTD 디바이스에 대한 보안 이벤트 시스템 로그 로깅을 설정하려면 Threat Defense 디바이스에서 보안 이벤트 시스템 로그 메시지 보내기, 656 페이지의 내용을 참조하십시오.

보안 이벤트 시스템 로그에 대한 구성 위치

- 연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치(모든 디바이스), 661 페이지
- 침입 이벤트에 대한 시스템 로그의 설정 위치(FTD 디바이스), 662 페이지
- 침입 이벤트에 대한 시스템 로그의 설정 위치(FTD 이전 버전의 디바이스), 663 페이지
- 파일 및 악성코드 이벤트에 대한 시스템 로그 구성 위치, 664 페이지

연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그 설정 위치(모든 디바이스)

로깅 설정은 여러 곳에서 설정할 수 있습니다. 아래 표를 사용하여 필요한 옵션을 설정했는지 확인합니다.

중요

- 시스템 로그 설정은 신중하게 수행해야 하며, 다른 설정에서 상속받은 기본값을 사용할 때는 특히 주의해야 합니다. 아래 표에서 설명하듯이, 매니지드 디바이스 모델과 소프트웨어 버전에 따라 사용할 수 없는 옵션도 있습니다.
- 연결 로깅 설정 관련 중요 정보는 연결 로깅, 753 페이지의 관련 챕터를 참조하십시오.

설정 위치	설명 및 상세정보
Devices(장치) > Platform Settings(플랫폼 설정), Threat Defense Settings(위협 방어 설정) 정책, **Syslog(시스템 로그)**	이 옵션은 threat defense 디바이스에만 적용됩니다. 여기서 구성하는 설정은 Access Control(액세스 컨트롤) 정책에 대한 Logging(기록) 설정에서 지정할 수 있으며, 이 표에 있는 나머지 정책과 규칙에서 사용하거나 재정의할 수 있습니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드을 참조하십시오.
Policies(정책) > Access Control(액세스 컨트롤), <각 정책>, **Logging(기록)**	여기서 구성하는 설정은 모든 연결 및 보안 인텔리전스 이벤트에 대한 시스템 로그의 기본 설정입니다. 단 이 표의 나머지 행에서 지정하는 위치에 있는 하위 정책 및 규칙에서 기본값을 재정의하는 경우는 예외입니다. threat defense 디바이스에 대한 권장 설정: Threat Defense Platform Settings(Threat Defense 플랫폼 설정 사용). 자세한 정보는 Cisco Secure Firewall Management Center 디바이스 구성 가이드. 다른 모든 디바이스의 필수 설정입니다. 시스템 로그 알림을 사용합니다. 시스템 로그 알림을 지정하는 경우에는 시스템 로그 알림 응답 생성, 573 페이지 섹션을 참조하십시오. Logging(기록) 탭의 설정에 관한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드섹션을 참조하십시오.
Policies(정책) > Access Control(액세스 컨트롤), <각 정책>, **Rules(규칙)**, **Default Action(기본 작업)** 행, **Logging(로깅)** ( )	액세스 컨트롤 정책과 관련된 기본 작업의 기록 설정입니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드 및 정책 기본 작업으로 연결 로깅, 768 페이지의 기록 관련 정보를 참조하십시오.

설정 위치	설명 및 상세정보
Policies(정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Rules(**규칙**)**, <각 규칙>, **Logging(**기록**)**	액세스 컨트롤 정책의 특정 규칙에 대한 기록 설정입니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 기록 관련 정보를 참조하십시오.
Policies(정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Security Intelligence(**보안 인텔리전스**)**, **Logging(**로깅**)** ( )	보안 인텔리전스 차단 목록의 기록 설정입니다. 버튼을 클릭해 다음을 설정합니다. • DNS 차단 목록 로깅 옵션 • URL 차단 목록 로깅 옵션 • 네트워크 차단 목록 기록 옵션(차단 목록의 IP 주소용) 사전 요건 섹션, 하위 항목 및 링크를 포함한 Cisco Secure Firewall Management Center 디바이스 구성 가이드
Policies(정책**) > SSL**, <각 정책>, **Default Action(**기본 작업**)** 행, **Logging(**로깅**)** ( )	SSL 정책과 관련된 기본 작업의 기록 설정입니다. 정책 기본 작업으로 연결 로깅, 768 페이지의 내용을 참조하십시오.
Policies(정책**) > SSL**, <각 정책>, <각 규칙>, **Logging(**로깅**)**	SSL 규칙에 대한 기록 설정입니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오.
Policies(정책**) > Prefilter(**사전 필터**)**, <각 정책>, **Default Action(**기본 작업**)** 행, **Logging(**로깅**)** ( )	사전 필터 정책과 관련된 기본 작업의 기록 설정입니다. 정책 기본 작업으로 연결 로깅, 768 페이지의 내용을 참조하십시오.
Policies(정책**) > Prefilter(**사전 필터**)**, <각 정책>, <각 사전 필터 규칙>, **Logging(**기록**)**	사전 필터 정책의 각 사전 필터 규칙에 대한 기록 설정입니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오.
Policies(정책**) > Prefilter(**사전 필터**)**, <각 정책>, <각 터널 규칙>, **Logging(**기록**)**	사전 필터 정책의 각 터널 규칙에 대한 기록 설정입니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오.
threat defense 클러스터 설정에 대한 추가 시스템 로그 설정:	Cisco Secure Firewall Management Center 디바이스 구성 가이드에는 시스템 로그에 대한 여러 참조자료가 있습니다. 챕터에서 "syslog"를 검색해 보십시오.

침입 이벤트에 대한 시스템 로그의 설정 위치(FTD 디바이스)

다양한 위치에서 침입 정책의 시스템 로그 설정을 지정할 수 있으며, 선택적으로 액세스 컨트롤 정책 또는 FTD Platform Settings(FTD 플랫폼 설정)이나 양쪽 모두의 설정을 상속할 수도 있습니다.

설정 위치	설명 및 상세정보
Devices(장치**) > Platform Settings(**플랫폼 설정**)**, Threat Defense Settings(위협 방어 설정) 정책, **Syslog(**시스템 로그**)**	여기서 구성하는 시스템 로그 대상은 침입 정책의 기본값이 될 수 있는, 액세스 컨트롤 정책의 Logging(기록) 탭에서 지정할 수 있습니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드을 참조하십시오.
Policies(정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Logging(**기록**)**	침입 정책이 다른 기록 호스트를 지정하지 않는 경우, 침입 이벤트에 대한 시스템 로그 대상의 기본 설정입니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오.
Policies(정책**) > Intrusion(**침입**)**, <각 정책>, **Advanced Settings(**고급 설정**)**에서 **Syslog Alerting(**시스템 로그 알림**)**을 활성화하고 **Edit(**편집**)** 클릭	Logging(기록) 탭의 액세스 컨트롤 정책에 지정된 대상이 아닌 다른 시스템 로그 수집기를 지정하고 시설과 심각도를 지정하려면, 침입 이벤트를 위한 시스템 로그 알림 설정, 582 페이지 섹션을 참조하십시오. 침입 정책에 설정된 **Severity(**심각도**)**나 **Facility(**시설**)** 또는 둘 다를 사용하고 싶다면, 정책에서 기록 호스트를 설정해야 합니다. 액세스 컨트롤 정책에서 지정하는 기록 호스트를 사용하는 경우, 침입 규칙에 지정된 심각도와 시설은 사용하지 않습니다.
Policies(정책**) > Access Control(**액세스 제어**) > Logging(**로깅**) > IPS settings(IPS** 설정**)**	IPS 이벤트에 대한 시스템 메시지를 보내려는 경우. 구성한 기본 시스템 로그 설정은 IPS 이벤트의 시스템 로그 대상에 사용됩니다.

침입 이벤트에 대한 시스템 로그의 설정 위치(FTD 이전 버전의 디바이스)

- (기본값) 액세스 컨트롤 정책Cisco Secure Firewall Management Center 디바이스 구성 가이드, 시스템 로그 알림을 지정하는 경우(시스템 로그 알림 응답 생성, 573 페이지 참조)
- 또는 침입 이벤트를 위한 시스템 로그 알림 설정, 582 페이지 섹션을 참조하십시오.

기본적으로, 침입 정책은 액세스 컨트롤 정책의 Logging(로깅) 탭에 있는 설정을 사용합니다. FTD 이아닌 디바이스에 적용 가능한 설정이 구성되어 있지 않다면, 시스템 로그는 FTD 이외의 디바이스에는 전송되지 않으며 경고도 표시되지 않습니다.

파일 및 악성코드 이벤트에 대한 시스템 로그 구성 위치

설정 위치	설명 및 상세정보
액세스 컨트롤 정책에서 **Policies(**정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, **Logging(**기록**)**	파일 및 악성코드 이벤트에 대한 시스템 로그를 전송하도록 시스템을 설정하는 기본 위치입니다. FTD Platform Settings(FTD 플랫폼 설정)에서 시스템 로그 설정을 사용하지 않는다면, 알림 응답도 생성해야 합니다. 시스템 로그 알림 응답 생성, 573 페이지의 내용을 참조하십시오.
Firepower Threat Defense 플랫폼 설정에서 **Devices(**장치**) > Platform Settings(**플랫폼 설정**)**, Threat Defense Settings(위협 방어 설정) 정책, **Syslog(**시스템 로그**)**	이러한 설정은 지원되는 버전을 실행하는 Firepower Threat Defense(Firepower 위협 방어) 디바이스에만 적용되며, FTD 플랫폼 설정을 사용할 액세스 컨트롤 정책에서 Logging(기록) 탭을 설정한 경우에만 적용됩니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드을 참조하십시오.
액세스 컨트롤 규칙에서 **Policies(**정책**) > Access Control(**액세스 컨트롤**)**, <각 정책>, <각 규칙>, **Logging(**기록**)**	FTD Platform Settings(FTD 플랫폼 설정)에서 시스템 로그 설정을 사용하지 않는다면, 알림 응답도 생성해야 합니다. 시스템 로그 알림 응답 생성, 573 페이지의 내용을 참조하십시오.

보안 이벤트 **Syslog** 메시지 구조

FTD에서 전송하는 보안 이벤트 메시지 예시**(**침입 이벤트**)**

```
  0        1                2              3        4  5     6

 ——  ————————  ———————————  ———————  ———  —  ———————

<37>2018-06-27 192.168.0.81 SFIMS : %FTD-5-430001:
192.168.1.10, DstIP: 192.168.1.102, SrcPort: 33994
Protocol: tcp, Priority: 2, GID: 133, SID: 17, Rev
Message: "DCE2_EVENT  SMB_INVALID_DSIZE", Classifi
Potentially Bad Traffic, User: No Authentication R
Client: NetBIOS-ssn (SMB) client, ApplicationProto
(SMB), ACPolicy: test, NAPPolicy: Balanced Securit
Connectivity, InlineResult: Blocked
```

표 ***53:*** 보안 이벤트 시스템 로그 메시지의 구성 요소

샘플 메시지의 항목 수	헤더 요소	설명
0	PRI	알림의 기능 및 심각도를 모두 나타내는 우선 순위 값입니다. 이 값은 FMC 플랫폼 설정을 사용하여 EMBLEM 형식으로 로깅을 활성화한 경우에만 시스템 로그 메시지에 나타납니다. 액세스 제어 정책 Logging(로깅) 탭을 통해 침입 이벤트 로깅을 활성화하면 PRI 값이 시스템 로그 메시지에 자동으로 표시됩니다. EMBLEM 형식을 활성화하는 방법에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오. PRI에 대한 자세한 내용은 RFC5424를 참조하십시오.
1	타임스탬프	디바이스에서 시스템 로그 메시지가 전송된 날짜와 시간입니다. • (FTD 디바이스에서 전송된 시스템 로그) 액세스 제어 정책 및 그 하위 항목의 설정을 사용해서 전송된 시스템 로그의 경우, 또는 이 형식을 FTD Platform Settings(FTD 플랫폼 설정)에서 사용하도록 지정한 경우 날짜 형식은 RFC 5424에 지정하는 ISO 8601 타임스탬프 형식에서 정의하는 형식(yyyy-MM-ddTHH:mm:ssZ)입니다. 여기서 Z는 UTC 시간대를 의미합니다. • (다른 모든 디바이스에서 전송된 시스템 로그) 액세스 제어 정책 및 그 하위 항목의 설정을 사용해서 전송된 시스템 로그의 경우, 날짜 형식은 RFC 5424에 지정하는 ISO 8601 타임스탬프 형식에서 정의하는 형식(yyyy-MM-ddTHH:mm:ssZ)입니다. 여기서 Z는 UTC 시간대를 의미합니다. • 그렇지 않은 경우에는 UTC 시간대의 월, 일, 시간이 되지만, 시간대는 표시되지 않습니다. FTD Platform Settings(FTD 플랫폼 설정)에서 타임스탬프 설정을 구성하는 방법은 Cisco Secure Firewall Management Center 디바이스 구성 가이드 섹션을 참조하십시오.

샘플 메시지의 항목 수	헤더 요소	설명
2	메시지를 보낸 디바이스 또는 인터페이스입니다. 다음을 선택할 수 있습니다. • 인터페이스의 IP 주소 • 디바이스 호스트 이름 • 맞춤형 디바이스 식별자	(FTD 디바이스에서 전송된 시스템 로그의 경우) 시스템 로그 메시지가 FTD Platform Settings(FTD 플랫폼 설정)을 사용하여 전송된 경우, 이것은 **Enable Syslog Device ID(**시스템 로그 디바이스 **ID)** 옵션(지정한 경우)의 **Syslog Settings(**시스템 로그 설정**)**에서 설정한 값입니다. 그렇지 않은 경우, 이 요소는 헤더에 존재하지 않습니다. FTD Platform Settings(FTD 플랫폼 설정)에서 이 설정을 구성하는 방법은 Cisco Secure Firewall Management Center 디바이스 구성 가이드 섹션을 참조하십시오.
3	맞춤형 값	알림 응답을 사용하여 메시지를 전송한 경우, 이것은 메시지를 전송한 알림 응답에서 설정한 **Tag(**태그**)** 값입니다(설정한 경우). (시스템 로그 알림 응답 생성, 573 페이지 참조) 그렇지 않은 경우, 이 요소는 헤더에 존재하지 않습니다.
4	%FTD	메시지를 전송한 디바이스의 유형입니다. %FTD는 Firepower Threat Defense입니다.
5	심각도	메시지를 트리거한 정책의 시스템 로그 설정에서 지정한 심각도입니다. 심각도 설명은 Cisco Secure Firewall Management Center 디바이스 구성 가이드 또는 시스템 로그 심각도 레벨, 575 페이지의 심각도 레벨을 참고하십시오.
6	이벤트 유형 식별자	• 430001: 침입 이벤트 • 430002: 연결 시작 시 기록된 연결 이벤트 • 430003: 연결 종료 시 기록된 연결 이벤트 • 430004: 파일 이벤트 • 430005: 파일 악성코드 이벤트
--	기능	보안 이벤트 시스템 로그 메시지의 시설, 667 페이지의 내용을 참조하십시오.

샘플 메시지의 항목 수	헤더 요소	설명
--	메시지의 나머지 부분	필드와 값은 콜론으로 구분합니다. 비어 있거나 알 수 없는 값이 있는 필드는 메시지에서 생략됩니다. 필드 설명은 다음을 참조하십시오. • 연결 및 보안 관련 연결 이벤트 필드, 773 페이지. • 침입 이벤트 필드, 810 페이지 • 파일 및 악성코드 이벤트 필드, 863 페이지 참고 필드 설명 목록은 시스템 필드와 이벤트 뷰어(Firepower Management Center 웹 인터페이스의 Analysis(분석) 메뉴에 있는 메뉴 옵션)에 표시되는 필드를 모두 포함합니다. 시스템 로그를 통해 사용할 수 있는 필드에는 다음과 같은 레이블이 지정됩니다. 이벤트 뷰어에 표시되는 필드 중 일부는 시스템 로그를 통해 사용할 수 없습니다. 또한 이벤트 뷰어에 포함되지 않는(하지만 검색을 통해 사용할 수 있는) 시스템 로그 필드도 있으며, 결합되거나 분리된 필드도 존재합니다.

보안 이벤트 시스템 로그 메시지의 시설

일반적으로 시설 값은 보안 이벤트의 시스템 로그 메시지와는 무관합니다. 그러나 Facility(시설)이 필요하다면, 다음 표를 사용하십시오.

디바이스	시설을 연결 이벤트에 포함하는 방법	시설을 침입 이벤트에 포함하는 방법	시스템 로그 메시지에서의 위치
FTD	FTD Platform Settings(FTD 플랫폼 설정)에서 EMBLEM 옵션을 사용합니다. FTD Platform Settings(FTD 플랫폼 설정)를 사용하여 시스템 로그 메시지를 전송하는 경우, 연결 이벤트에 대한 시설은 언제나 **ALERT**입니다.	FTD Platform Settings(FTD 플랫폼 설정)에서 EMBLEM 옵션을 사용하거나 침입 규칙의 시스템 로그 설정을 사용하여 기록을 구성합니다. 침입 정책을 사용하는 경우에는 침입 정책 설정에서 기록 호스트를 지정해야 합니다. 시스템 로그 알림을 활성화하고 침입 정책에서 시설 및 심각도를 구성합니다. 침입 이벤트를 위한 시스템 로그 알림 설정, 582 페이지의 내용을 참조하십시오.	시설은 메시지 헤더에는 표시되지 않지만, 시스템 수집기는 RFC 5424, 섹션 6.2.1을 바탕으로 값을 끌어낼 수 있습니다.
FTD 이외의 디바이스	알림 응답을 사용합니다.	침입 정책 고급 설정의 시스템 로그 설정을 사용하거나 액세스 컨트롤 정책 Logging(기록) 탭에서 식별한 응답 알림을 사용합니다.	

자세한 내용은 침입 시스템 로그 알림에 대한 기능 및 심각도, 583 페이지 및 시스템 로그 알림 응답 생성, 573 페이지의 내용을 참조하십시오.

Firepower System 로그 메시지 유형

Firepower는 다음 테이블에서 설명하는 것처럼 여러 시스템 로그 데이터 유형을 전송할 수 있습니다.

시스템 로그 데이터 유형	확인
FMC의 감사 로그	시스템 로그로의 감사 로그 스트리밍, 48 페이지 및 감사 및 시스템 로그, 417 페이지 챕터
디바이스 상태 및 FTD의 네트워크 관련 로그	Cisco Secure Firewall Management Center 디바이스 구성 가이드
연결, 보안 인텔리전스 및 FTD 디바이스의 침입 이벤트 로그	보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 구성 정보, 655 페이지.
연결, 보안 인텔리전스 및 기본 디바이스의 침입 이벤트 로그	보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 구성 정보, 655 페이지

시스템 로그 데이터 유형	확인
파일 및 악성코드 이벤트 로그	보안 이벤트 데이터를 시스템 로그로 전송하는 시스템 구성 정보, 655 페이지
IPS 설정	IPS 이벤트에 대한 시스템 로그 메시지를 전송합니다. 침입 이벤트에 대한 시스템 로그의 설정 위치(FTD 디바이스), 662 페이지

보안 이벤트에 대한 시스템 로그 제한 사항

- Syslog를 사용하거나 이벤트를 외부에 저장하려는 경우 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.
- 이벤트가 시스템 로그 수집기에 표시될 때까지 최대 15분이 걸릴 수 있습니다.
- 다음 파일 및 악성코드 이벤트의 데이터는 시스템 로그를 통해 사용할 수 없습니다.
  - 회귀 이벤트
  - AMP for Endpoints(엔드포인트용 AMP)가 생성한 이벤트

eStreamer 서버 스트리밍

Event Streamer(eStreamer)를 사용하면 여러 종류의 이벤트 데이터를 Secure Firewall Management Center에서 맞춤 개발된 클라이언트 애플리케이션으로 스트리밍할 수 있습니다. 자세한 내용은 *Firepower System Event Streamer* 통합 가이드를 참조하십시오.

eStreamer 서버로 사용할 어플라이언스가 외부 클라이언트로 eStreamer 이벤트의 스트리밍을 시작하기 전에 이벤트를 클라이언트로 전송하고, 클라이언트에 대한 정보를 제공하고, 통신 설정 시 사용할 인증 자격 증명 집합을 생성하도록 eStreamer 서버를 구성해야 합니다. 어플라이언스의 사용자 인터페이스에서 이 모든 작업을 수행할 수 있습니다. 설정이 저장되면, 선택한 이벤트는 요청 시 eStreamer 클라이언트에 전달됩니다.

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

표 ***54: eStreamer*** 서버가 전송할 수 있는 이벤트 유형

이벤트 유형	설명
침입 이벤트	매니지드 디바이스에서 생성된 침입 이벤트
침입 이벤트 패킷 데이터	침입 이벤트와 관련된 패킷

이벤트 유형	설명
침입 이벤트 추가 데이터	HTTP 프록시 또는 로드 밸런서를 통해 웹 서버에 연결하는 클라이언트의 원래 IP 주소와 같은 침입 이벤트와 관련된 추가 데이터
검색 이벤트	네트워크 검색 이벤트
상관관계 및 허용 목록 이벤트	상관관계 및 컴플라이언스 허용 목록 이벤트
영향 플래그 알림	다음이 생성한 영향 알림 management center
사용자 이벤트	사용자 이벤트
악성코드 이벤트	악성코드 이벤트
파일 이벤트	파일 이벤트
연결 이벤트	모니터링되는 호스트와 기타 모든 호스트 간의 세션 트래픽에 대한 정보입니다.

시스템 로그 및 eStreamer의 보안 이벤트 비교

일반적으로, eStreamer에 큰 투자를 하지 않은 조직은 시스템 로그 대신 eStreamer를 사용하여 보안 이벤트 데이터를 외부적으로 관리해야 합니다.

시스템 로그	**eStreamer**
맞춤형 필요 없음	각 릴리스의 변경사항을 수용하려면 상당한 수준의 맞춤형 및 유지관리가 필요함
표준	Proprietary
시스템 로그 표준은 데이터 손실을 방지하지 않으며, UDP를 사용할 때는 더욱 그렇습니다.	데이터 손실 방지
디바이스에서 직접 전송	FMC에서 전송하며, 처리 오버헤드 추가
파일 및 악성코드 이벤트, 연결 이벤트(보안 인텔리전스 이벤트 포함) 및 침입 이벤트를 지원합니다.	eStreamer 서버 스트리밍, 669 페이지에 나열된 모든 이벤트 유형을 지원합니다.
일부 이벤트 데이터는 FMC에서만 전송할 수 있습니다. (시스템 로그가 아닌) eStreamer로만 전송된 데이터, 671 페이지의 내용을 참조하십시오.	디바이스에서 시스템 로그를 통해 직접 전송될 수 없는 데이터를 포함합니다. (시스템 로그가 아닌) eStreamer로만 전송된 데이터, 671 페이지의 내용을 참조하십시오.

(시스템 로그가 아닌) eStreamer로만 전송된 데이터

다음 데이터는 에서만 사용할 수 있으며, 따라서 디바이스에서 시스템 로그를 통해 전송할 수 없습니다.Secure Firewall Management Center

- 패킷 로그
- 침입 이벤트 추가 데이터 이벤트

  자세한 내용은 eStreamer 서버 스트리밍, 669 페이지의 내용을 참조하십시오.
- 통계 및 통합 이벤트
- 네트워크 검색 이벤트
- 사용자 활동 및 로그인 이벤트
- 상관관계 이벤트
- 악성코드 이벤트:
  - 회귀 판정
  - 관련 SHA 정보가 디바이스에 이미 동기화되어 있지 않은 경우 ThreatName 및 분류
- 다음 필드:
  - Impact 및 ImpactFlag 필드

    자세한 내용은 eStreamer 서버 스트리밍, 669 페이지의 내용을 참조하십시오.
  - IOC_Count 필드
- 대부분의 원시 ID 및 UUID입니다.

  예외
  - 연결 이벤트에 대한 시스템 로그는 FirewallPolicyUUID, FirewallRuleID, TunnelRuleID, MonitorRuleID, SI_CategoryID, SSL_PolicyUUID, SSL_RuleID가 포함됩니다.
  - 침입 이벤트의 시스템 로그는 IntrusionPolicyUUID, GeneratorID, SignatureID를 포함합니다.
- 확장 메타데이터(다음을 포함하되 이에 제한되지 않음):
  - LDAP에서 제공한 사용자 상세정보(전체 이름, 부서, 전화 번호 등)

    시스템 로그는 이벤트의 사용자 이름만 제공합니다.
  - SSL 인증 상세정보 같은 상태 기반 정보

    시스템 로그는 인증서 지문과 같은 기본 정보를 제공하지만, cert CN 같은 다른 인증서 세부 정보는 제공하지 않습니다.
  - 앱 태그 및 범주 같은 자세한 애플리케이션 정보

    시스템 로그는 애플리케이션 이름만 제공합니다.

일부 메타데이터 메시지에는 개체에 대한 추가 정보도 포함됩니다.

- 지오로케이션 정보

eStreamer 이벤트 유형 선택

eStreamer Event Configuration(eStreamer 이벤트 설정**)** 확인란는 eStreamer 서버가 전송할 수 있는 이벤트를 제어합니다. 클라이언트에서는 여전히 eStreamer 서버로 전송하는 요청 메시지에서 수신하고자 하는 이벤트 유형을 구체적으로 요청해야 합니다. 자세한 내용은 *Firepower System Event Streamer* 통합 가이드를 참고하십시오.

다중 도메인 구축에서는 어떤 도메인 수준에서도 eStreamer 이벤트 설정을 구성할 수 있습니다. 그러나 상위 도메인이 특정 이벤트 유형을 활성화했다면, 하위 도메인에서는 이벤트 유형을 비활성화할 수 없습니다.

management center를 위해 이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**를 선택합니다.

단계 **2** **eStreamer**를 클릭합니다.

단계 **3** eStreamer 서버 스트리밍, 669 페이지에 설명된 대로, **eStreamer Event Configuration(eStreamer** 이벤트 설정**)**에서 eStreamer가 요청 클라이언트로 전달하도록 할 이벤트 유형 옆에 있는 확인란을 선택하거나 선택 해제합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

eStreamer 클라이언트 커뮤니케이션 설정

eStreamer가 eStreamer 이벤트를 클라이언트에 전송하려면, 먼저 eStreamer 페이지에서 클라이언트를 eStreamer 서버의 피어 데이터베이스에 추가해야 합니다. 또한 eStreamer 서버에서 생성된 인증 인증서를 클라이언트에 복사해야 합니다. 이상의 단계를 완료하면 eStreamer 서비스를 다시 시작하지 않고도 클라이언트를 eStreamer 서버에 연결할 수 있습니다.

다중 도메인 구축에서는 모든 도메인에서 eStreamer 클라이언트를 만들 수 있습니다. 인증 인증서를 이용하면 클라이언트가 클라이언트 인증서의 도메인 및 하위 도메인의 이벤트만 요청하게 할 수 있습니다. eStreamer 설정 페이지는 현재 도메인과 연결된 클라이언트만 표시하므로, 인증서를 다운로드하거나 취소하려면 클라이언트가 생성된 도메인으로 전환해야 합니다.

management center에 대해 이 작업을 수행하려면 관리자 또는 검색 관리자 사용자여야 합니다.

프로시저

단계 **1** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**를 선택합니다.

단계 **2** **eStreamer**를 클릭합니다.

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

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

참고 DNS 확인을 설정하지 않은 경우, IP 주소를 사용해야 합니다.

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

단계 **6** **Save(**저장**)**를 클릭합니다.
이제 eStreamer 서버는 호스트가 eStreamer 서버의 포트 8302에 액세스하는 것을 허용하고 클라이언트-서버 인증 중에 사용할 인증 인증서를 만듭니다.

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

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

단계 **9** 클라이언트에 대한 액세스를 취소하려면, 제거할 호스트 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

eStreamer 서비스를 다시 시작할 필요가 없으며, 액세스는 즉시 취소됩니다.

Splunk의 이벤트 분석

Splunk용 Cisco Secure Firewall(f.k.a. Firepower)(이전 명칭: Splunk용 Cisco Firepower App)를 외부 툴로 사용하여 Firepower 이벤트 데이터를 표시하고 사용하여 네트워크에서 위협을 추적하고 조사할 수 있습니다.

eStreamer가 필요합니다. 이는 고급 기능입니다. eStreamer 서버 스트리밍, 669 페이지를 참조하십시오.

자세한 내용은 https://cisco.com/go/firepower-for-splunk를 참고하십시오.

IBM QRadar의 이벤트 분석

IBM QRadar용 Cisco Firepower 앱을 대체 방법으로 사용하여 이벤트 데이터를 표시하고 네트워크에 대한 위협을 분석, 추적 및 조사할 수 있습니다.

eStreamer가 필요합니다. 이는 고급 기능입니다. eStreamer 서버 스트리밍, 669 페이지를 참조하십시오.

자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/QRadar/integration-guide-for-the-cisco-firepower-app-for-ibm-qradar.html를 참고하십시오.

외부 툴을 사용한 이벤트 데이터 분석 기록

기능	버전	세부 사항
SecureX 리본	7.0	SecureX 리본은 SecureX로 피벗되어 Cisco 보안 제품 전반에 걸쳐 위협 환경을 즉시 확인할 수 있습니다. FMC에서 SecureX 리본을 표시하려면 https://cisco.com/go/firepower-securex-documentation에서 *Firepower* 및 *SecureX* 통합 가이드를 참조하십시오. 신규/수정된 화면: 새 페이지: System(시스템) > SecureX
모든 연결 이벤트를 클라우드로 전송	7.0	이제 우선순위가 높은 연결 이벤트만 전송하지 않고 모든 연결 이벤트를 Cisco 클라우드로 전송할 수 있습니다. 신규/수정된 화면: System(시스템) > Integration(통합) > Cloud Services(클라우드 서비스) 페이지의 새로운 옵션
데이터를 보기 위한 교차 실행 Secure Network Analytics	6.7	이 기능을 사용하면 Analysis(분석) > Contextual Cross-Launch(상황별 교차 실행) 페이지에서 Secure Network Analytics 어플라이언스에 대한 여러 항목을 빠르게 생성할 수 있습니다. 이러한 항목을 사용하면 관련 이벤트를 마우스 오른쪽 버튼으로 클릭하여 Secure Network Analytics를 교차 실행하고 교차 시작한 데이터 지점과 관련된 정보를 표시할 수 있습니다. 새 메뉴 항목: System(시스템) > Logging(로깅) > Security Analytics and Logging(보안 분석 및 로깅) Secure Network Analytics로 이벤트 전송을 설정할 새 페이지입니다.
추가 필드 유형에서 상황별 교차 실행	6.7	이제 다음과 같은 추가 이벤트 데이터 유형을 사용하여 외부 애플리케이션으로 교차 실행할 수 있습니다. • 액세스 제어 정책 • 침입 정책 • 애플리케이션 프로토콜 • 클라이언트 애플리케이션 • 웹 애플리케이션 • 사용자 이름(영역 포함) 새로운 메뉴 옵션: 이제 Analysis(분석) 메뉴 아래의 페이지에서 대시보드 위젯 및 이벤트 테이블의 이벤트에 대한 위의 데이터 유형을 마우스 오른쪽 버튼으로 클릭하면 상황별 교차 실행 옵션을 사용할 수 있습니다. 지원되는 플랫폼: Secure Firewall Management Center

기능	버전	세부 사항
IBM QRadar와의 통합	6.0 이상	IBM QRadar 사용자는 새로운 Firepower 전용 앱을 통해 이벤트 데이터를 분석할 수 있습니다 사용 가능한 기능은 Firepower 버전에 따라 달라집니다. IBM QRadar의 이벤트 분석, 673 페이지의 내용을 참조하십시오.
개선 사항은 다음에 통합됩니다. SecureX threat response	6.5	• 지역 클라우드 지원: • 미합중국(북미) • 유럽 • 추가 이벤트 유형 지원: • 파일 및 악성코드 이벤트 • 높은 우선순위 연결 이벤트 다음과 관련된 연결 이벤트입니다. • 침입 이벤트 • 보안 인텔리전스 이벤트 • 파일 및 악성코드 이벤트 수정된 화면: **System(**시스템**) > Integration(**통합**) > Cloud Service(**클라우드 서비스**)**의 새 옵 지원 플랫폼: 이 버전에서는 직접 통합 또는 시스템 로그의 형태로 모든 디바이스를 지원합니다.
시스템 로그	6.5	이제 AccessControlRuleName 필드를 침입 이벤트 시스템 로그 메시지에서 사용할 수 있습니다
통합 Cisco Security Packet Analyzer	6.5	이 기능의 지원은 삭제되었습니다.
통합 SecureX threat response	6.3(시스템 로그를 통해, 프록시 수집기 사용) 6.4(직접)	Firepower 침입 이벤트 데이터를 다른 소스의 데이터와 통합해 SecureX threat response의 강력한 분석 도구를 사용하여 네트워크상의 위협을 통합적으로 확인합니다. 수정된 화면(버전 6.4): **System(**시스템**) > Integration(**통합**) > Cloud Services(**클라우드 서비스의 새 옵션 지원되는 플랫폼: 버전 6.3(시스템 로그를 통해) 또는 6.4를 실행하는 Secure Firewall Threat Defense 디바이스
파일 및 악성코드 이벤트에 대한 시스템 로그 지원	6.4	이제 완전히 인증된 파일 및 악성코드 이벤트 데이터를 시스템 로그를 통해 매니지드 디바이스에서 전송할 수 있습니다. 수정된 화면: **Policies(**정책**) > Access Control(**액세스 제어**) > Access Control(**액세스 제어**) > Logging(**로깅**)** 지원 되는 플랫폼: 버전 6.4를 실행하는 모든 매니지드 디바이스

기능	버전	세부 사항
Splunk와의 통합	모든 6.x 버전 지원.	Splunk 사용자는 새로운 별도의 Splunk 앱인 Splunk용 Cisco Secure Firewall(f.k.a. Firepower)을(를) 사용하여 이벤트를 분석할 수 있습니다. 사용 가능한 기능은 Firepower 버전에 따라 달라집니다. Splunk의 이벤트 분석, 673 페이지의 내용을 참조하십시오.
통합 Cisco Security Packet Analyzer	6.3	도입된 기능: 이벤트와 관련된 패킷의 Cisco Security Packet Analyzer을(를) 즉시 쿼리하고, 클릭하여 Cisco Security Packet Analyzer의 결과를 검사하거나 다운로드해 다른 외부 도구에서 분석합니다. 새 화면: **System(**시스템**)** > **Integration(**통합**)** > **Packet Analyzer(**패킷 분석기**)** **Analysis(**분석**)** > **Advanced(**고급**)** > **Packet Analyzer Queries(**패킷 분석기 쿼리**)** 새 메뉴 옵션: Dashboard(대시보드) 페이지와 Analysis(분석) 메뉴의 페이지에 있는 이벤트를 오른쪽 클릭할 때 나타나는 **Query Packet Analyzer(**쿼리 패킷 분석기**)** 지원되는 플랫폼: Secure Firewall Management Center
상황별로 크로스 실행	6.3	도입된 기능: 이벤트를 오른쪽 클릭해 사전 정의 또는 맞춤형 URL 기반 외부 리소스에서 관련 정보를 찾습니다. 새 화면: **Analysis(**분석**)** > **Advanced(**고급**)** > **Contextual Cross-Launch(**상황별 크로스 실행**)** 새 메뉴 옵션: Dashboard(대시보드) 페이지와 Analysis(분석) 메뉴의 페이지에 있는 이벤트를 오른쪽 클릭할 때 나타나는 여러 옵션 지원되는 플랫폼: Secure Firewall Management Center
연결 및 침입 이벤트용 시스템 로그 메시지	6.3	통합되고 단순화된 새로운 설정을 사용하여, 시스템 로그를 통해 완전히 인증된 연결 및 침입 이벤트를 외부 스토리지로 전송하는 기능 이제 메시지 헤더가 표준화되었고 이벤트 유형 식별자를 포함하며, 알 수 없거나 값이 없는 필드는 생략되기 때문에 미시지가 서로 비슷해집니다. 지원되는 플랫폼: • 모든 새 기능: 버전 6.3을 실행하는 FTD 디바이스 • 일부 새 기능: 버전 6.3을 실행하는 FTD 이외의 디바이스 • 소수의 새 기능: 버전 6.3 미만을 실행하는 모든 디바이스. 자세한 내용은 보안 이벤트에 대한 시스템 로그 메시지 전송 정보, 655 페이지 및 하위 항목의 주제를 참조하십시오.
eStreamer	6.3	eStreamer 콘텐츠를 Host Identity Sources(호스트 ID 소스) 챕터에서 이 챕터로 옮기고, eStreamer와 시스템 로그를 비교한 요약을 추가했습니다.

VII 부

워크플로우 및 테이블

27 장

워크플로우

다음 주제에서는 워크플로를 사용하는 방법을 설명합니다.

개요: 워크플로

워크플로는 management center 웹 인터페이스에 있는 일련의 맞춤 데이터 페이지이며, 분석가는 시스템에서 생성된 이벤트를 평가하는 데 이를 사용할 수 있습니다.

다음 워크플로 유형은 management center에서 사용할 수 있습니다.

사전 정의 워크플로

시스템으로 전달한 미리 설정된 워크플로입니다. 사전 정의한 워크플로는 편집하거나 삭제할 수 없습니다. 하지만 사전 정의한 워크플로를 복사하고 맞춤형 워크플로의 기반으로 사용하는 것은 가능합니다.

저장된 맞춤형 워크플로

management center(으)로 전달한 저장된 맞춤형 테이블을 기반으로 하는 맞춤형 워크플로입니다. 이러한 워크플로는 편집, 삭제, 복사할 수 있습니다.

사용자 지정 워크플로

생성하고 필요에 맞게 맞춤형한 워크플로 또는 맞춤형 테이블을 생성할 때 시스템이 자동으로 생성한 워크플로입니다. 이러한 워크플로는 편집, 삭제, 복사할 수 있습니다.

많은 경우 워크플로에 표시되는 데이터는 매니지드 디바이스 허가 및 구축 방법, 데이터를 제공하는 기능 설정 여부 등의 요소에 따라 달라집니다.

사전 정의 워크플로

다음 섹션에서 설명하는 사전 정의된 워크플로는 시스템을 통해 전달됩니다. 사전 정의된 워크플로는 편집하거나 삭제할 수 없지만, 사전 정의한 워크플로를 복사하고 맞춤형 워크플로의 기반으로 사용하는 것은 가능합니다.

사전 정의 침입 이벤트 워크플로

다음 표에서는 Firepower System에 포함된 사전 정의 침입 이벤트 워크플로에 대해 설명합니다.

표 ***55:*** 사전 정의 침입 이벤트 워크플로

워크플로 이름	설명
목적지 포트	대상 포트가 대개 애플리케이션과 연결되므로, 이 워크플로는 알림의 양이 비정상적으로 많은 애플리케이션을 탐지하는 데 사용할 수 있습니다. Destination Port(대상 포트) 열은 네트워크에 있어서는 안 될 애플리케이션을 식별하는 데에도 도움이 됩니다.
이벤트 관련	이 워크플로는 두 가지의 유용한 기능을 제공합니다. 자주 발생하는 이벤트는 다음을 의미할 수 있습니다. • 오탐 • 웜 • 잘못 구성된 네트워크 드물게 발생하는 이벤트는 표적 공격의 증거일 가능성이 높으므로 각별한 주의가 필요합니다.
우선순위 및 분류별 이벤트	이 워크플로는 이벤트와 그 유형을 이벤트 우선순위에 따라 나열하며 각 이벤트의 발생 횟수 카운트도 표시합니다.
대상에 대한 이벤트	이 워크플로는 어떤 호스트 IP 주소가 공격받고 있으며 공격의 특성이 어떠한지 총괄적으로 보여줍니다. 가능한 경우 공격 관련 국가에 대한 정보도 볼 수 있습니다.
IP 관련	이 워크플로에서는 어떤 호스트 IP 주소가 가장 많은 알림을 생성하는지를 보여줍니다. 이벤트 수가 가장 많은 호스트는 일반에게 공개되는 수신 웜 유형 트래픽이거나(튜닝을 위한 조사 대상으로 적합), 알림의 원인을 확인하기 위해 추가 조사가 필요한 곳입니다. 카운트가 가장 낮은 호스트 역시 조사가 필요한데, 표적 공격의 주체일 가능성이 있습니다. 카운트가 낮으면 네트워크에 속하지 않는 호스트일 수도 있습니다.
영향 및 우선순위	이 워크플로에서는 영향이 큰 반복적 이벤트를 신속하게 찾을 수 있습니다. 보고된 영향 레벨은 이벤트가 발생한 횟수와 함께 표시됩니다. 이 정보를 사용 하면 가장 자주 재발 하는 영향력이 큰 이벤트를 식별 하 여 네트워크에 대 한 광범위 한 공격의 지표가 될 수 있습니다.

워크플로 이름	설명
영향 및 소스	이 워크플로는 진행 중인 공격의 출처를 파악하는 데 도움이 될 수 있습니다. 보고된 영향 레벨은 이벤트의 소스 IP 주소와 함께 표시됩니다. 예를 들어 영향 레벨이 1인 이벤트가 동일한 IP 주소에서 반복적으로 발생하는 경우, 공격자가 취약한 시스템을 찾아내 표적으로 삼고 있음을 의미할 수 있습니다.
대상에 대한 영향	이 워크플로를 통해 취약한 컴퓨터에서 반복적으로 발생하는 이벤트를 식별할 수 있어 시스템의 취약성을 해결하고 진행 중인 공격이 있을 경우 공격을 중지시킬 수 있습니다.
소스 포트	이 워크플로는 어떤 서버에서 가장 많은 알림을 생성하는지 나타냅니다. 튜닝이 필요한 영역을 식별하고 주의가 필요한 서버를 확인하는 데 이 정보를 사용할 수 있습니다.
소스 및 대상	이 워크플로는 높은 수준의 알림을 공유하는 호스트 IP 주소를 식별합니다. 목록 맨 위의 쌍은 오탐일 가능성이 있으며, 따라서 튜닝이 필요한 영역을 나타내는 것일 수도 있습니다. 목록 맨 아래의 쌍은 표적 공격, 권한이 없는 리소스에 액세스하는 사용자, 네트워크에 속하지 않는 호스트인지의 여부에 대해 조사할 수 있습니다.

사전 정의 악성코드 워크플로

다음 표에서는 management center에 포함된 사전 정의 악성코드 워크플로에 대해 설명합니다. 모든 사전 정의 악성코드 워크플로에서는 악성코드 이벤트의 테이블 보기를 사용합니다.

표 ***56:*** 사전 정의 악성코드 워크플로

워크플로 이름	설명
악성코드 요약	이 워크플로는 네트워크 트래픽에서 또는 엔드포인트 기반 AMP for Endpoints Connector에 의해 탐지된 악성코드를 개별 위협을 기준으로 그룹화한 목록을 제공합니다.
악성코드 이벤트 요약	이 워크플로에서는 다양한 악성 코드 이벤트 유형 및 하위 유형을 신속하게 분석할 수 있습니다.
악성코드를 수신하는 호스트 수	이 워크플로는 악성코드를 수신한 호스트 IP 주소를 악성코드 파일의 관련 성향을 기준으로 그룹화한 목록을 제공합니다.
악성코드를 송신하는 호스트 수	이 워크플로는 악성코드를 전송한 호스트 IP 주소를 악성코드 파일의 관련 성향을 기준으로 그룹화한 목록을 제공합니다.
Applications Introducing Malware	이 워크플로는 파일을 수신한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.

사전 정의 파일 워크플로

다음 표에서는 management center에 포함된 사전 정의 파일 이벤트 워크플로에 대해 설명합니다. 모든 사전 정의 파일 이벤트 워크플로에서는 파일 이벤트의 테이블 보기를 사용합니다.

표 ***57:*** 사전 정의 파일 워크플로

워크플로 이름	설명
파일 요약	이 워크플로에서는 다양한 파일 이벤트 카테고리와 유형을 신속하게 분석할 수 있으며, 관련 악성코드 성향도 표시합니다.
파일을 수신하는 호스트 수	이 워크플로는 파일을 수신한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.
파일을 송신하는 호스트 수	이 워크플로는 파일을 전송한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.

사전 정의 캡처 파일 워크플로

다음 표에서는 management center에 포함된 사전 정의 캡처 파일 워크플로에 대해 설명합니다. 모든 사전 정의 캡처 파일 워크플로에서는 캡처 파일의 테이블 보기를 사용합니다.

표 ***58:*** 사전 정의 캡처 파일 워크플로

워크플로 이름	설명
캡처된 파일 요약	이 워크플로에서는 유형, 카테고리, 위협 점수를 기준으로 캡처 파일을 분석할 수 있습니다.
동적 분석 상태	이 워크플로에서는 캡처 파일이 동적 분석을 위해 제출되었는지 여부에 따라 그 카운트를 제공합니다.

사전 정의 연결 데이터 워크플로

다음 표에서는 management center에 포함된 사전 정의 연결 데이터 워크플로에 대해 설명합니다. 모든 사전 정의 연결 데이터 워크플로에서 연결 데이터의 테이블 보기를 사용합니다.

표 ***59:*** 사전 정의 연결 데이터 워크플로

워크플로 이름	설명
연결 이벤트	이 워크플로에서는 기본 연결 및 탐지된 애플리케이션 정보에 대한 요약 보기를 제공하며, 이를 사용하여 이벤트 테이블 보기로 드릴다운할 수 있습니다.
애플리케이션별 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 탐지된 연결 수를 기준으로 가장 활동적인 10개의 애플리케이션을 그래프로 나타냅니다.
이니시에이터를 이용한 연결	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 호스트가 연결 트랜잭션을 시작한 연결의 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
포트별 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 탐지된 연결 수를 기준으로 가장 활동적인 10개의 포트를 그래프로 나타냅니다.

워크플로 이름	설명
응답자별 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 호스트 IP 주소가 연결 트랜잭션의 응답자인 연결의 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
시간에 따른 연결 수	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 시간의 경과에 따른 총 연결 수를 그래프로 나타냅니다.
애플리케이션별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 전송된 킬로바이트 수를 기준으로 가장 활동적인 10개의 애플리케이션을 그래프로 나타냅니다. 애플리케이션 카운트는 애플리케이션 연결과 일치하는 각 탐지기를 반영합니다. 트래픽과 일치하는 것이 애플리케이션 프로토콜, 웹 애플리케이션, 클라이언트 탐지기, 내부 탐지기 중 무엇인지에 따라, 그리고 트래픽이 모바일 디바이스에서 발생했는지 암호화된 세션의 일부인지에 따라 같은 애플리케이션 세션이 목록에서 여러번 나타날 수도 있습니다. 클라이언트 플로우에 애플리케이션이 표시되며 특별한 클라이언트 탐지기가 존재하지 않는다면, 일반 클라이언트가 보고될 수 있습니다. 예를 들어 (YouTube 웹 애플리케이션 탐지기와 일치하기 때문에) **YouTube**로 보고되거나, (내부 YouTube 탐지기가 클라이언트 세션에서 일반적으로 표시되는 특성과 일치하기 때문에) **YouTube** 클라이언트로 보고된 YouTube 트래픽과 같은 세션이 표시될 수 있습니다. 네트워크의 연결 이벤트와 네트워크 맵에 있는 정보를 사용하여 특정 애플리케이션 연결에 대한 추가 정보를 확인합니다.
이니시에이터별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소로부터 전송된 총 킬로바이트 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
포트별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 전송된 킬로바이트 수를 기준으로 가장 활동적인 10개의 포트를 그래프로 나타냅니다.
응답자별 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소가 수신한 총 킬로바이트 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
시간에 따른 트래픽	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 시간의 경과에 따른 총 전송 킬로바이트 수를 그래프로 나타냅니다.
응답자별 고유 이니시에이터	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소에 연결한 고유 initiator 수를 기준으로 가장 활동적인 10개의 응답 호스트 IP 주소를 그래프로 나타냅니다.
이니시에이터별 고유 응답자	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소가 연결한 고유 responder 수를 기준으로 가장 활동적인 10개의 발신 호스트 IP 주소를 그래프로 나타냅니다.

사전 정의 보안 인텔리전스 워크플로

다음 표에서는 management center에 포함된 사전 정의 보안 인텔리전스 워크플로에 대해 설명합니다. 모든 사전 정의 보안 인텔리전스 워크플로에서는 보안 인텔리전스 이벤트의 테이블 보기를 사용합니다.

표 ***60:*** 사전 정의 보안 인텔리전스 워크플로

워크플로 이름	설명
보안 인텔리전스 이벤트	이 워크플로에서는 기본 보안 인텔리전스 및 탐지된 애플리케이션 정보에 대한 요약 보기를 제공하며, 이를 사용하여 이벤트 테이블 보기로 드릴다운할 수 있습니다.
보안 인텔리전스 요약	이 워크플로는 Security Intelligence Events(보안 인텔리전스 이벤트) 워크플로와 동일하지만 보안 인텔리전스 이벤트를 카테고리 및 카운트별로만 나열하는 Security Intelligence Summary(보안 인텔리전스 요약) 페이지로 시작합니다.
DNS 상세정보가 있는 보안 인텔리전스	이 워크플로는 Security Intelligence Events(보안 인텔리전스 이벤트) 워크플로와 동일하지만 Security Intelligence(보안 인텔리전스) 이벤트를 카테고리 및 DNS 관련 특성별로만 나열하는 Security Intelligence with DNS Details(DNS 상세정보가 있는 보안 인텔리전스) 페이지로 시작합니다.

사전 정의 호스트 워크플로

다음 표에서는 호스트 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***61:*** 사전 정의 호스트 워크플로

워크플로 이름	설명
호스트	이 워크플로에서는 호스트의 테이블 보기에 이어 호스트 보기가 표시됩니다. 호스트 테이블 기반의 워크플로 보기에서는 어떤 호스트와 관련된 모든 IP 주소의 데이터를 편리하게 볼 수 있습니다.
운영 체제 요약	이 워크플로를 사용하여 네트워크에서 사용 중인 운영체제를 분석할 수 있습니다.

사전 정의 보안 침해 지표 워크플로

다음 표에서는 IOC 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 **62:** 사전 정의 보안 침해 지표 워크플로

워크플로 이름	설명
Host(호스트) 보안 침해 지표	이 워크플로는 IOC 데이터를 카운트 및 범주별로 그룹화한 요약 보기로 시작하며, 요약 데이터를 이벤트 유형별로 세분화하는 세부사항 보기를 제공합니다. **Analysis(**분석**) > Hosts(**호스트**)** 메뉴를 통해 이 워크플로에 액세스합니다.
호스트별 보안 침해 지표	이 워크플로를 사용하여 네트워크의 어떤 호스트가 공격받을 가능성이 가장 높은지 (IOC 데이터를 기반으로) 평가할 수 있습니다. **Analysis(**분석**) > Hosts(**호스트**)** 메뉴를 통해 이 워크플로에 액세스합니다.
사용자 보안 침해 지표	이 워크플로는 IOC 데이터를 카운트 및 범주별로 그룹화한 요약 보기로 시작하며, 요약 데이터를 이벤트 유형별로 세분화하는 세부사항 보기를 제공합니다. **Analysis(**분석**) > Users(**사용자**)** 메뉴를 통해 이 워크플로에 액세스합니다.
사용자별 보안 침해 지표	이 워크플로를 사용하여 네트워크의 어떤 사용자가 잠재적 침해에 연관될 가능성이 가장 높은지 (IOC 데이터를 기반으로) 평가합니다. **Analysis(**분석**) > Users(**사용자**)** 메뉴를 통해 이 워크플로에 액세스합니다.

사전 정의 애플리케이션 워크플로

다음 표에서는 애플리케이션 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 **63:** 사전 정의 애플리케이션 워크플로

워크플로 이름	설명
애플리케이션 비즈니스 관련성	이 워크플로를 사용하여 네트워크의 예상 비즈니스 타당성 레벨별로 실행 중인 애플리케이션을 분석함으로써 네트워크 리소스가 적절하게 사용되는지 모니터링할 수 있습니다.
애플리케이션 범주	이 워크플로를 사용하여 네트워크에서 카테고리(예: 이메일, 검색 엔진, 소셜 네트워킹)별로 실행 중인 애플리케이션을 분석함으로써 네트워크 리소스가 적절하게 사용되는지 모니터링할 수 있습니다.
애플리케이션 위험성	이 워크플로를 사용하여 네트워크에서 각 예상 보안 위험 레벨의 실행 중인 애플리케이션을 분석함으로써 사용자 활동의 잠재적 리스크를 추정하고 적절한 조치를 취할 수 있습니다.
애플리케이션 요약	이 워크플로를 사용하여 네트워크의 애플리케이션 및 해당 호스트에 대한 세부 정보를 얻어 호스트 애플리케이션 활동을 면밀하게 조사할 수 있습니다.
애플리케이션	이 워크플로를 사용하여 네트워크에서 실행 중인 애플리케이션을 분석함으로써 네트워크가 어떻게 사용되고 있는가를 개괄적으로 파악할 수 있습니다.

사전 정의 애플리케이션 상세정보 워크플로

다음 표에서는 애플리케이션 상세정보 및 클라이언트 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***64:*** 사전 정의 애플리케이션 상세정보 워크플로

워크플로 이름	설명
애플리케이션 세부사항	이 워크플로를 사용하여 네트워크의 클라이언트 애플리케이션을 더 자세히 분석할 수 있습니다. 그런 다음 클라이언트 애플리케이션의 테이블 보기와 호스트 보기로 이어집니다.
클라이언트	이 워크플로에서는 클라이언트 애플리케이션의 테이블 보기에 이어 호스트 보기가 표시됩니다.

사전 정의 서버 워크플로

다음 표에서는 서버 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***65:*** 사전 정의 서버 워크플로

워크플로 이름	설명
카운트별 네트워크 애플리케이션	이 워크플로를 사용하여 네트워크에서 가장 자주 사용되는 애플리케이션을 분석할 수 있습니다.
히트별 네트워크 애플리케이션	이 워크플로를 사용하여 네트워크에서 가장 활동적인 애플리케이션을 분석할 수 있습니다.
서버 세부 정보	이 워크플로를 사용하여 탐지된 서버 애플리케이션 프로토콜의 벤더 및 버전을 더 자세히 분석할 수 있습니다.
서버	이 워크플로에서는 애플리케이션의 테이블 보기에 이어 호스트 보기가 표시됩니다.

사전 정의 호스트 속성 워크플로

다음 표에서는 호스트 속성 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***66:*** 사전 정의 호스트 속성 워크플로

워크플로 이름	설명
특성	이 워크플로를 사용하여 네트워크에 있는 호스트의 IP 주소 및 호스트의 상태를 모니터링할 수 있습니다.

사전 정의 검색 이벤트 워크플로

다음 표에서는 검색 및 ID 데이터를 확인하는 데 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***67:*** 사전 정의 검색 이벤트 워크플로

워크플로 이름	설명
검색 이벤트	이 워크플로에서는 검색 이벤트의 세부 목록을 테이블 보기 형태로 제공하고 이어서 호스트 보기를 표시합니다.

사전 정의 사용자 워크플로

다음 표에서는 사용자 검색 및 사용자 ID 데이터를 확인하는 데 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 ***68:*** 사전 정의 사용자 워크플로

워크플로 이름	설명
활성 세션	이 워크플로는 사용자 ID 소스가 수집한 활성 세션 목록을 제공합니다.
사용자	이 워크플로는 사용자 ID 소스가 수집한 사용자 정보 목록을 제공합니다.

사전 정의 취약성 워크플로

다음 표에서는 management center에 포함된 사전 정의 취약성 워크플로에 대해 설명합니다.

표 ***69:*** 사전 정의 취약성 워크플로

워크플로 이름	설명
취약성	이 워크플로를 이용하면 네트워크에서 탐지된 호스트에 적용되는 활성 취약성만 표시하는 테이블 보기 등을 이용해, 데이터베이스에 있는 취약성을 검토할 수 있습니다. 또한 제약 조건에 부합하는 모든 취약성에 대해 자세히 설명하는 취약성 세부사항 보기도 제공합니다.

사전 정의 서드파티 취약성 워크플로

다음 표에서는 management center에 포함된 사전 정의 서드파티 취약성 워크플로에 대해 설명합니다.

표 ***70:*** 사전 정의 서드파티 취약성 워크플로

워크플로 이름	설명
IP 주소별 취약성	이 워크플로를 사용하여 모니터링되는 네트워크의 호스트 IP 주소별로 탐지된 서드파티 취약성의 수를 신속하게 확인할 수 있습니다.
소스별 취약성	이 워크플로를 사용하여 서드파티 취약성 소스(예: QualysGuard Scanner)별로 탐지된 서드파티 취약성의 수를 신속하게 확인할 수 있습니다.

사전 정의 상관관계 및 허용 목록 워크플로

상관관계 데이터, 허용 목록 이벤트, 허용 목록 위반, 교정 상태 이벤트의 유형별로 사전 정의 워크플로가 있습니다.

표 ***71:*** 사전 정의 상관관계 워크플로

워크플로 이름	설명
상관관계 이벤트	이 워크플로는 상관관계 이벤트의 테이블 보기로 구성됩니다.
허용 이벤트 나열	이 워크플로는 허용 목록 이벤트의 테이블 보기로 구성됩니다.
호스트 위반 카운트	이 워크플로는 하나 이상의 허용 목록을 위반하는 모든 호스트 IP 주소를 나열하는 일련의 페이지로 구성됩니다.
허용 위반 목록	이 워크플로에는 모든 위반을 나열하는 허용 목록 위반의 테이블 보기가 포함되는데, 가장 최근에 탐지된 위반이 맨 위에 옵니다. 테이블의 각 행에는 탐지된 위반 사항이 하나씩 포함되어 있습니다.
상태	이 워크플로는 교정 상태의 테이블 보기로 구성됩니다. 여기에는 위반한 정책의 이름, 적용된 교정의 이름과 상태가 포함됩니다.

사전 정의 시스템 워크플로

Firepower System에서는 몇 가지 추가 워크플로를 제공하는데, 여기에는 감사 이벤트 및 상태 이벤트와 같은 시스템 이벤트 뿐만 아니라 규칙 업데이트 가져오기 및 활성 검사의 결과를 나열하는 워크플로도 포함됩니다.

표 ***72:*** 추가 사전 정의 워크플로

워크플로 이름	설명
감사 로그	이 워크플로는 감사 이벤트를 나열하는 감사 로그의 테이블 보기로 구성됩니다.

워크플로 이름	설명
상태 이벤트	이 워크플로에서는 상태 모니터링 정책에 의해 트리거되는 이벤트를 표시합니다.
규칙 업데이트 가져오기 로그	이 워크플로는 성공한 규칙 업데이트 가져오기 및 실패한 규칙 업데이트 가져오기에 대한 정보를 나열하는 테이블 보기로 구성됩니다.
스캔 결과	이 워크플로는 완료된 각 스캔을 나열하는 테이블 보기로 구성됩니다.

맞춤형 테이블 워크플로

맞춤형 테이블 기능을 사용하여 이벤트 유형 2가지 이상의 데이터를 사용하는 테이블을 생성할 수 있습니다. 이를테면 침입 이벤트 데이터를 검색 데이터와 연계하여 중요 시스템에 영향을 주는 이벤트의 단순 검색을 지원하는 테이블과 워크플로를 만들 때 유용한 기능입니다.

맞춤형 테이블을 생성하는 경우, 시스템은 테이블과 관련된 이벤트를 볼 수 있는 워크플로를 자동으로 생성합니다. 워크플로의 기능은 사용하는 테이블 유형에 따라 달라집니다. 예를 들어 침입 이벤트 테이블을 기반으로 하는 맞춤형 테이블 워크플로는 항상 패킷 보기로 끝납니다. 그러나 검색 이벤트를 기반으로 하는 맞춤형 테이블 워크플로는 호스트 보기로 끝납니다.

사전 정의 이벤트 테이블 기반의 워크플로와 달리 맞춤형 테이블 기반의 워크플로는 다른 워크플로 유형에 대한 링크가 없습니다.

워크플로 사용

프로시저

단계 **1** 워크플로 선택, 691 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택합니다.

단계 **2** 현재 워크플로 내에서 이동:

- 선택한 이벤트 데이터 유형에서 사용 가능한 행을 모두 보려면 테이블 보기 페이지를 사용하십시오(테이블 보기 페이지 사용, 698 페이지 참조).
- 선택한 이벤트 데이터 유형에서 사용 가능한 행의 하위 집합을 보려면 드릴다운 페이지를 사용하십시오(드릴다운 페이지 사용, 697 페이지 참조).
- 워크플로우의 다음 페이지에 해당 행을 표시하려면 **Down-Arrow(**아래쪽 화살표**)** (▼)을 클릭합니다.
- 여러 페이지가 있는 워크플로의 페이지 사이를 이동하려면 각 페이지 하단에 있는 툴을 사용하십시오(워크플로 페이지 이동 툴, 695 페이지 참조).
- 다른 유형의 워크플로에 적용된 같은 제약을 보려는 경우, **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.

단계 **3** 현재 워크플로의 표시 화면을 수정합니다.

- 페이지에서 하나 이상의 열 옆에 있는 체크 박스를 선택해 영향받는 열을 표시하고, 페이지 하단의 버튼 중 하나(예: **View(**보기**)**)를 클릭해 선택한 열 전체에 작업을 수행합니다.
- 열 상단에 있는 체크 박스를 선택해 페이지의 모든 열을 선택하고, 페이지 하단의 버튼 중 하나(예: **View(**보기**)**)를 클릭해 페이지의 열 전체에 작업을 수행합니다.
- 표시하지 않을 컬럼 헤드의 **Close(**닫기**)** (✕)을 클릭하여 화면에 표시되는 열을 제한합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 확인 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 확장 화살표를 클릭하여 검색 제약 조건을 확장한 다음, Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 선택한 필드의 선택된 값을 이용해 데이터 보기를 제한합니다. 자세한 내용은 이벤트 보기 제약 조건, 713 페이지 및 복합 이벤트 보기 제약, 715 페이지 섹션을 참고하십시오.
- 이벤트 보기의 시간 제약을 변경합니다. 페이지의 오른쪽 위에 있는 날짜 범위는 워크플로에 포함할 이벤트의 시간 범위를 설정합니다. 자세한 내용은 이벤트 시간 제약 조건, 707 페이지 섹션을 참조하십시오.

  참고 어플라이언스의 구성된 타임 윈도우(전역 또는 이벤트 전용 모두 해당)를 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

- 열을 기준으로 데이터를 정렬하려면 열의 이름을 클릭합니다. 정렬 순서를 반대로 하려면 열 이름을 다시 클릭합니다. 방향 아이콘은 데이터가 정렬되는 열과 정렬이 오름차순인지 내림차순인지를 표시합니다.
- 워크플로 페이지 링크를 클릭하여 활성 제약 조건을 사용해 해당 페이지를 표시합니다. 사전 정의된 워크플로 테이블 보기 및 드릴다운 페이지의 왼쪽 위에서 이벤트 위, 워크플로 이름 아래에 워크플로 페이지 링크가 나타납니다.

단계 **4** 현재 워크플로 내의 추가 데이터를 확인합니다.

- 파일의 경로 맵을 새 창에서 보려면, 파일 이름과 SHA-256 해시 값 열에서 네트워크 파일 경로를 클릭합니다. 아이콘은 파일 상태에 따라 달라집니다(파일 경로 아이콘, 695 페이지 참조).
- IP 주소와 관련된 호스트 프로파일의 팝업 윈도우를 표시하려는 경우, 아무 IP 주소 열의 호스트 프로파일을 클릭합니다. 아이콘은 파일 상태에 따라 달라집니다(호스트 프로파일 아이콘, 695 페이지 참조).
- 파일의 최고 위협 점수에 대한 Dynamic Analysis Summary(동적 분석 요약) 보고서를 보려는 경우, 위협 점수 열에 나타나는 위협 점수를 클릭합니다. 아이콘은 파일의 최고 위협 점수에 따라 달라집니다(위협 점수 아이콘, 696 페이지 참조).

- 사용자 프로파일 정보를 보려는 경우에는 아무 사용자 ID 열의 사용자 또는 보안 침해 지표와 관련된 사용자의 경우에는 빨간색 사용자를 클릭합니다. 해당 사용자가 데이터베이스에 존재할 수 없다면(즉 AMP for Endpoints Connector 사용자려면) 사용자 아이콘은 흐리게 표시됩니다.
- 서드파티 취약성의 취약성 상세정보를 보려는 경우네는 아무 서드파티 취약성 ID 열의 취약성을 클릭합니다.
- 집계된 데이터 포인트를 볼 때 마우스 포인터를 플래그 위에 올리면 국가 이름을 볼 수 있습니다.
- 개별 데이터 포인트를 볼 때 플래그를 클릭하면 지리위치, 700 페이지에서 설명하는 추가 지리위치 상세정보를 볼 수 있습니다.

단계 **5** 다른 워크플로로 이동합니다.

다른 워크플로를 이용하는 같은 이벤트 유형을 보려는 경우, 워크플로 제목 옆에 있는 **(switch workflow)**을 클릭하고 사용할 워크플로를 선택합니다. 스캔 결과에 대해 다른 워크플로를 사용할 수는 없습니다.

사용자 역할별 워크플로 액세스

워크플로에 대한 액세스는 사용자의 역할에 따라 결정됩니다. 자세한 내용은 아래 표를 참고하십시오.

사용자 역할	액세스 가능한 워크플로
관리자	어떤 워크플로에도 액세스할 수 있으며, 감사 로그, 검사 결과, 규칙 업데이트 가져오기 로그에 액세스할 수 있는 유일한 사용자입니다.
유지 보수 사용자	상태 이벤트에 액세스할 수 있습니다.
Security Analyst 및 Security Analyst(읽기 전용)	침입, 악성코드, 파일, 연결, 검색, 취약성, 상관관계, 상태 워크플로에 액세스할 수 있습니다.

워크플로 선택

시스템에서는 다음 테이블에 나열된 데이터 유형에 대해 사전 정의된 워크플로우를 제공합니다.

표 ***73:*** 워크플로를 사용하는 기능

기능	메뉴 경로	옵션
연결 이벤트	분석 > 연결	이벤트
보안 인텔리전스 이벤트	분석 > 연결	보안 인텔리전스 이벤트

기능	메뉴 경로	옵션
상관관계 이벤트	분석 > 상관관계	상관관계 이벤트 허용 이벤트 나열 허용 위반 목록 상태
악성코드 이벤트	분석 > 파일	악성코드 이벤트
파일 이벤트	분석 > 파일	파일 이벤트
캡처된 파일	분석 > 파일	캡처된 파일
호스트 이벤트	분석 > 호스트	네트워크 맵 호스트 보안 침해 지표 애플리케이션 애플리케이션 세부사항 서버 호스트 속성 검색 이벤트
침입 이벤트	분석 > 침입	이벤트 검사된 이벤트
사용자 이벤트	분석 > 사용자	활성 세션 사용자의 활동 사용자 보안 침해 지표
취약성 이벤트	분석 > 호스트	취약성 서드파티 취약성
스캔 결과	Policies(정책) > Actions(작업) > Scanners(스캐너)	—
상태 이벤트	System(시스템) > Health(상태) > Events(이벤트)	—
감사 이벤트	시스템 > 모니터링	감사
규칙 업데이트 가져오기 로그	시스템 > 업데이트 시스템 > 업데이트	규칙 업데이트

위 표에 있는 데이터 유형을 표시할 경우 그 데이터의 기본 워크플로 중 첫 페이지에 이벤트가 나타납니다. 이벤트 보기 설정을 구성하여 다른 기본 워크플로를 지정할 수 있습니다. 워크플로 액세스는 사용자 역할에 따라 달라집니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

관련 항목

이벤트 보기 구성, 210 페이지

워크플로 페이지

각 워크플로 유형의 데이터는 저마다 다르지만, 모든 워크플로가 공유하는 공통 기능이 있습니다. 워크플로는 페이지의 여러 유형을 포함할 수 있습니다. 워크플로 페이지에서 수행할 수 있는 작업은 페이지 유형에 따라 달라집니다.

워크플로의 드릴다운 및 테이블 보기 페이지를 통해 신속하게 데이터 보기의 범위를 한정하여 분석에 중요한 이벤트에 초점을 맞출 수 있습니다. 테이블 보기 페이지 및 드릴다운 페이지는 표시할 이벤트 집합을 제한하거나 워크플로를 이동하는 데 사용할 수 있는 여러 기능을 지원합니다. 워크플로의 드릴다운 페이지나 테이블 보기에서 데이터를 볼 때, 사용 가능한 아무 열을 기준으로 데이터를 오름차순이나 내림차순으로 정렬할 수 있습니다. 데이터베이스가 단일 워크플로 페이지에 표시할 수 있는 것보다 많은 이벤트를 포함할 경우, 페이지 맨 아래의 링크를 클릭하여 추가 이벤트를 표시할 수 있습니다. 이 링크 중 하나를 클릭할 때 동일한 이벤트가 두 번 표시되지 않도록 시장 창이 자동으로 일시 중지합니다. 언제라도 타임 윈도우의 일시 중지를 취소할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

테이블 보기

페이지가 기본적으로 활성화되는 경우, 테이블 보기에는 워크플로가 기반으로 하는 데이터베이스의 각 필드에 대한 열이 포함됩니다.

최상의 성능을 위해 필요한 열만 표시합니다. 열이 많이 표시될수록 데이터를 표시하는 데 더 많은 리소스가 필요합니다.

테이블 보기에서 어떤 열을 비활성화할 경우 그 열을 비활성화함으로써 둘 이상의 동일한 행이 생성되고 6개 미만의 열이 표시된다면(Count 열 제외) Firepower System에서는 이벤트 보기에 Count 열을 추가합니다.

테이블 보기 페이지에서 어떤 값을 클릭하면 그 값으로 제한할 수 있습니다.

맞춤형 워크플로를 생성할 때 **Add Table View(**테이블 보기 추가**)**를 클릭하여 여기에 테이블 보기를 추가합니다.

드릴다운 페이지

일반적으로 드릴다운 페이지는 보기 페이지로 이동하기 전에 조사 범위를 몇몇 이벤트로 한정하는 데 사용하는 중간 단계의 페이지입니다. 드릴다운 페이지는 데이터베이스에서 제공하는 열의 일부를 포함합니다.

예를 들어 검색 이벤트의 드릴다운 페이지에 IP Address, MAC Address, Time 열만 포함될 수 있습니다. 한편 침입 이벤트의 드릴다운 페이지는 Priority, Impact Flag, Inline Result, Message 열이 포함될 수 있습니다.

드릴다운 페이지에서는 표시하는 이벤트의 범위를 좁히고 워크플로에서 다음으로 진행할 수 있습니다. 이를테면 드릴다운 페이지에서 어떤 값을 클릭할 경우 그 값을 기준으로 제한하고 워크플로의 다음 페이지로 이동함으로써, 선택한 값과 매칭하는 이벤트에 더 초점을 맞출 수 있습니다. 드릴다운 페이지에서 어떤 값을 클릭하더라도 그 값이 있는 열이 비활성화되지 않습니다. 진행할 페이지가 테이블 보기인 경우도 마찬가지입니다. 사전 정의 워크플로의 드릴다운 페이지에는 항상 Count 열이 있습니다. 맞춤형 워크플로를 생성할 때 **Add Page(**페이지 추가**)**를 클릭하여 드릴다운 페이지를 추가합니다.

Graphs(그래프**)**

연결 데이터 기반의 워크플로는 연결 그래프라고도 하는 그래프 페이지를 포함할 수 있습니다.

예를 들어 연결 그래프에서 시간의 경과에 따른 탐지된 연결 수를 나타내는 선 그래프가 표시될 수 있습니다. 일반적으로 연결 그래프는 드릴다운 페이지처럼 조사 범위를 한정하는 데 사용하는 중간 단계의 페이지입니다.

최종 페이지

워크플로의 최종 페이지는 워크플로의 기반이 되는 이벤트의 유형에 따라 달라집니다.

- 호스트 보기는 애플리케이션, 애플리케이션 상세정보, 검색 이벤트, 호스트, 보안 침해 지표(IOC), 서버, 허용 목록 위반, 호스트 속성 또는 서드파티 취약성을 기반으로 하는 워크플로의 최종 페이지입니다. 이 페이지에서 호스트 프로파일을 보면서 다중 주소를 갖는 호스트의 모든 IP 주소에 대한 데이터를 편리하게 볼 수 있습니다.
- 사용자 상세정보 보기는 사용자, 사용자 활동, 사용자 보안 침해 지표를 기반으로 하는 워크플로의 최종 페이지입니다.
- 취약성 상세정보 보기는 Cisco 취약성을 기반으로 하는 워크플로의 최종 페이지입니다.
- 패킷 보기는 침입 이벤트를 기반으로 하는 워크플로의 최종 페이지입니다.

다른 종류의 이벤트(예: 감사 로그 이벤트, 악성코드 이벤트)를 기반으로 하는 워크플로는 최종 페이지가 없습니다.

워크플로의 마지막 페이지에서 세부사항 섹션을 확장하여 초점 대상인 집합의 각 개체에 대해 워크플로의 진행에 따른 구체적인 정보를 볼 수 있습니다. 웹 인터페이스에서는 워크플로의 최종 페이지에 제약 조건을 나열하지 않지만, 이미 설정된 제약 조건이 유지되어 데이터 집합에 적용됩니다.

워크플로 페이지 탐색 툴

워크플로 페이지는 각 페이지를 손쉽게 탐색하고 이벤트 분석 동안 표시할 정보를 선택하는 데 도움이 되는 시각적 단서를 제공합니다.

워크플로 페이지 이동 툴

워크플로에 여러 페이지의 데이터가 있는 경우, 각 페이지 하단에 워크플로의 페이지 숫자가 표시되며, 아래 표에 나열된 툴을 이용해 페이지를 이동할 수 있습니다.

표 ***74:*** 워크플로 페이지 이동 툴

페이지 이동 툴	조치
페이지 번호 (다른 페이지를 보려는 경우 확인할 페이지 번호를 입력하고 Enter를 누릅니다.)	다른 페이지 보기
>	다음 페이지 보기
<	이전 페이지 보기
>|	마지막 페이지로 바로 이동
|<	첫 페이지로 바로 이동

파일 경로 아이콘

워크플로 페이지에서 파일의 경로 맵을 새 창에서 볼 수 있다면, 네트워크 경로 아이콘이 표시됩니다. 이 아이콘은 파일 상태에 따라 달라집니다.

표 ***75:*** 파일 경로 아이콘

파일 경로 아이콘	파일 상태
정상	정상
악성코드	악성코드
맞춤형 탐지	맞춤형 탐지
알 수 없음	알 수 없음
사용 불가능	사용 불가능

호스트 프로파일 아이콘

워크플로 페이지에서 IP 주소와 연결된 호스트 프로파일을 팝업 윈도우에서 볼 수 있다면, 호스트 프로파일 아이콘이 표시됩니다. 호스트 프로파일 아이콘이 흐리게 표시될 경우 호스트가 네트워크 맵에 포함될 수 없으므로(예: `0.0.0.0`) 호스트 프로파일을 볼 수 없습니다. 이 아이콘은 호스트의 상태에 따라 다르게 표시됩니다.

표 **76:** 호스트 프로파일 아이콘

호스트 프로파일 아이콘	호스트 상태
	호스트가 침해 가능성 있음으로 태그되지 않았습니다.
	호스트가 트리거된 보안 침해 지표(IOC) 규칙에 의해 침해 가능성 있음으로 태그되었습니다.
	차단 목록에 추가됨(보안 인텔리전스 데이터를 바탕으로 트래픽 필터링을 수행하는 경우에만 표시됩니다.)
	차단 목록에 추가됨, 모니터링하도록 설정(보안 인텔리전스 데이터를 바탕으로 트래픽 필터링을 수행하는 경우에만 표시됩니다.)

위협 점수 아이콘

워크플로 페이지를 제공 하는 경우 가장 높은 위협 점수에 대 한 동적 분석 요약 보고서를 볼 수 있는 기회와 연결 파일을 위협 점수 아이콘 위에 표시 됩니다. 아이콘은 파일의 최고 위협 점수에 따라 다릅니다.

표 **77:** 위협 점수 아이콘

위협 점수 아이콘	위협 점수 레벨
낮음	낮음
중간	보통
높음	높음
매우 높음	매우 높음

사용자 아이콘

워크플로 페이지에서 사용자 이름과 연결된 사용자 ID를 팝업 윈도우에서 볼 수 있다면, 사용자 아이콘이 표시됩니다.

표 **78:** 사용자 아이콘

사용자 아이콘	사용자 상태
사용자	사용자가 어떠한 보안 침해 지표와도 연결되어 있지 않습니다.
빨간색 사용자	사용자가 하나 이상의 보안 침해 지표와 연결되어 있습니다.

워크플로 툴바

워크플로의 각 페이지에는 관련 기능에 빠르게 액세스할 수 있는 툴바가 있습니다. 다음 표에서는 툴바의 각 링크에 대해 설명합니다.

표 ***79:*** 워크플로 툴바 링크

기능	설명
이 페이지를 즐겨찾기에 추가	현재 페이지에 북마크를 지정하여 나중에 다시 돌아올 수 있게 합니다. 북마크는 현재 보고 있는 페이지에 적용된 제약 조건을 캡처하므로 나중에 (데이터가 그대로 있을 경우) 동일한 데이터로 돌아올 수 있습니다.
보고서 디자이너	현재 제약 조건이 적용된 워크플로를 선택 기준으로 하는 보고서 디자인 도구를 엽니다.
대시보드	현재 워크플로와 관련된 대시보드를 엽니다. 예를 들어 Connection Events(연결 이벤트) 워크플로는 Connection Summary(연결 요약) 대시보드와 연결됩니다.
즐겨찾기 보기	선택 가능한 저장된 즐겨찾기의 목록을 표시합니다.
검색	워크플로의 데이터에 대한 고급 검색을 수행할 수 있는 Search(검색) 페이지를 표시합니다. 아래쪽 화살표 아이콘을 클릭하여 저장된 검색을 선택하고 사용할 수도 있습니다.

관련 항목

이벤트 보기에서 보고서 템플릿 생성, 546 페이지
대시보드 정보, 345 페이지
이벤트 검색, 721 페이지
북마크, 717 페이지
즐겨찾기 생성, 718 페이지
즐겨찾기 보기, 718 페이지

드릴다운 페이지 사용

프로시저

단계 **1** 워크플로를 사용하는 기능에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 모든 워크플로에는 다음 옵션이 있습니다.

- 특정 값으로 제한하여 다음 워크플로 페이지로 드릴다운하려면 행 내의 값을 클릭합니다. 이 방법은 드릴다운 페이지에만 적용됩니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한될 뿐이고 다음 페이지로 드릴다운되지 않습니다.
- 일부 이벤트로 제한하여 다음 워크플로 페이지로 드릴다운하려면, 다음 워크플로 페이지에서 볼 이벤트의 옆에 있는 확인란을 선택하고 **View(보기)**를 클릭합니다.

- 현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운하려면 **View All(**모두 보기**)**을 클릭합니다.

팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

테이블 보기 페이지 사용

테이블 보기 페이지는 드릴다운, 호스트 보기, 패킷 보기 또는 취약성 세부사항 페이지에 없는 기능을 제공합니다. 이러한 기능은 아래 설명대로 사용하십시오.

프로시저

단계 **1** 워크플로 선택, 691 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 워크플로 이름 아래에 표시된 워크플로 경로에서 테이블 보기를 선택합니다.

단계 **3** 이벤트 데이터가 원격으로 저장된 경우, 로컬 데이터를 표시할지 아니면 원격 데이터를 표시할지를 선택하는 옵션이 나타날 수 있습니다.

Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Secure Firewall Management Center에서 작업, 699 페이지의 내용을 참조하십시오.

단계 **4** 필요에 따라 아래 나열된 기능을 사용하여 테이블 보기를 정렬하고 내부를 이동합니다.

- 비활성화된 열의 목록을 표시하려면 Search Constraints(검색 제약 조건) **Expand Arrow(**확장 화살표**)**( )를 클릭합니다.
- 비활성화된 열의 목록을 숨기려면 Search Constraints(검색 제약 조건) **Collapse Arrow(**축소 화살표**)**( )를 클릭합니다.
- 비활성화된 열을 이벤트 보기에 다시 추가하려면 Search Constraints(검색 제약 조건) **Expand Arrow(**확장 화살표**)**( )를 클릭하여 검색 제약 조건을 확장한 다음, Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.
- 열을 표시하거나 숨기려면(비활성화하려면) 아무 열 이름 옆에 있는 **Clear(**지우기**)** ( )를 클릭합니다. 표시되는 팝업 윈도우에서 적절한 체크 박스를 선택하거나 선택 취소해 표시할 열을 나타낸 다음, **Apply(**적용**)**를 클릭합니다.

Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Secure Firewall Management Center에서 작업

디바이스가 Security Analytics and Logging(보안 애널리틱스)을(를) 사용하여 Secure Network Analytics 어플라이언스에 연결 이벤트를 전송하는 경우, management center의 이벤트 뷰어 및 상황 탐색기에서 원격으로 저장된 이벤트를 확인하고 작업을 수행하고 보고서를 생성할 때 해당 이벤트를 포함할 수 있습니다. management center의 이벤트에서 교차 실행하여 Secure Network Analytics 어플라이언스의 관련 데이터를 볼 수도 있습니다.

기본적으로 시스템은 사용자가 지정한 시간 범위에 따라 적절한 데이터 소스를 자동으로 선택합니다. 데이터 소스를 재정의하려는 경우 이 절차를 사용합니다.

중요 데이터 소스를 변경하는 경우 로그아웃한 후에도 변경 사항이 있을 때까지 보고서를 포함하여 이벤트 데이터 소스를 사용하는 모든 관련 분석 기능에서 선택 사항이 유지됩니다. 다른 management center 사용자에게는 선택 항목이 적용되지 않습니다.

선택한 데이터 소스는 우선순위가 낮은 연결 이벤트에만 사용됩니다. 기타 모든 이벤트 유형(침입, 파일 및 악성 코드 이벤트, 해당 이벤트와 연결된 연결 이벤트, 보안 인텔리전스 이벤트)은 데이터 소스에 관계 없이 표시됩니다.

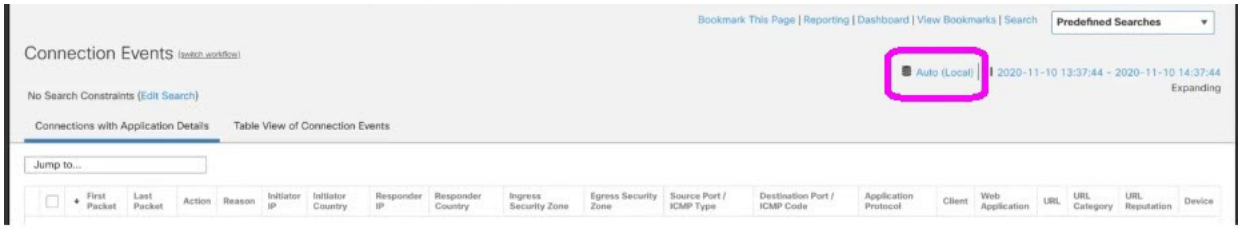
시작하기 전에

마법사를 사용하여 연결 이벤트를 Security Analytics and Logging(보안 애널리틱스)에 보냈습니다.

프로시저

단계 **1** management center 웹 인터페이스에서 **Analysis(분석) > Connections(연결) > Events(이벤트)**와 같은 연결 이벤트 데이터를 표시하는 페이지로 이동합니다.

단계 **2** 여기에 표시된 데이터 소스를 클릭하고 옵션을 선택합니다.



주의 **Local(로컬)**을 선택하면 선택한 전체 시간 범위에 대해 로컬 데이터를 사용할 수 없는 경우에도 management center에서 사용 가능한 데이터만 표시됩니다. 이러한 상황이 발생했다는 알림이 표시되지 않습니다.

단계 **3** (선택 사항) Secure Network Analytics 어플라이언스에서 관련 데이터를 직접 보려면 IP 주소 또는 도메인과 같은 값을 마우스 오른쪽 버튼으로 클릭(통합 이벤트 뷰어에서 클릭)하고 교차 실행 옵션을 선택합니다.

지리위치

지리위치 데이터베이스(GeoDB)를 활용하여 국가 및 대륙을 기준으로 트래픽을 보고 필터링할 수 있습니다. 한 국가에서 다른 국가로 이동하는 모바일 디바이스 및 다른 탐지된 호스트의 경우, 시스템은 특정 국가 대신 대륙을 보고하기도 합니다.

시스템은 IP 주소를 국가/대륙에 매핑하는 초기 GeoDB 국가 코드 패키지와 함께 제공되므로 정보를 항상 사용할 수 있습니다. GeoDB를 업데이트하면 시스템은 상황 데이터가 포함된 IP 패키지도 다운로드합니다. 여기에는 다음이 포함될 수 있습니다.

- 지역(주/도 또는 기타 국가 하위 지역), 도시 및 우편번호
- 위도/경도, 표준 시간대 및 클릭 가능한 맵
- ASN(Autonomous System Number) 및 ASN에 대한 추가 정보
- ISP(Internet Service Provider), 연결 유형 및 프록시 유형
- 홈/비즈니스, 조직 및 도메인 이름 정보

이 정보를 보려면 이벤트, 자산 프로파일, Context Explorer, 대시보드 및 기타 분석 툴에 표시되는 작은 국가 플래그 아이콘 및 ISO 국가 코드를 클릭합니다. Connection Summary(연결 요약) 대시보드 등에서는 종합 지리위치 정보에 대한 상세정보를 볼 수 없습니다.

참고 GeoDB에 주기적인 업데이트를 생성합니다. 정확한 지리적 위치 정보를 얻으려면 GeoDB를 정기적으로 업데이트해야 합니다. GeoDB(지리위치 데이터베이스) 업데이트, 236 페이지의 내용을 참조하십시오.

관련 항목

네트워크 조건
지리위치
상관관계 정책 및 규칙 소개, 1017 페이지
트래픽 프로파일 조건, 1059 페이지
GeoDB(지리위치 데이터베이스) 업데이트, 236 페이지

연결 이벤트 그래프

표 드릴다운 페이지와 이벤트의 최종 테이블 보기를 사용하는 워크플로 외에도, 시스템은 5분 간격으로 집계한 데이터를 이용해 특정 연결 데이터를 그래픽으로 표시할 수 있습니다. 데이터를 집계하

는 데 사용한 정보, 즉 소스 및 목적지 IP 주소(및 해당 호스트와 연결된 사용자), 대상 포트, 전송 프로토콜, 애플리케이션 프로토콜만 그래프로 표시할 수 있습니다.

팁 Security Intelligence(보안 인텔리전스) 이벤트를 관련된 연결 이벤트와 별도로 그래프로 표시할 수는 없습니다. Security Intelligence(보안 인텔리전스) 필터링 활동에 대한 그래픽 개요를 보려면 대시보드와 Context Explorer(맥락 탐색기)를 사용하십시오.

연결 그래프는 세 가지 유형이 있습니다.

- 원도표는 불연속 카테고리로 그룹화한 단일 데이터 집합의 데이터를 표시합니다.
- 막대 그래프는 불연속 카테고리로 그룹화한 하나 이상의 데이터 집합의 데이터를 표시합니다.
- 선 그래프는 표준 또는 속도(변경 속도) 보기 중 하나를 사용하여, 하나 이상의 데이터 집합에서 얻은 데이터의 시간에 따른 변화를 표시합니다.

참고 시스템은 트래픽 프로파일을 선 그래프로 표시하며, 이 그래프는 몇 가지 제한 사항은 있지만 다른 연결 그래프와 같은 방식으로 조작할 수 있습니다. 트래픽 프로파일을 보려면 관리자 액세스 권한이 있어야 합니다.

워크플로 테이블처럼, 워크플로 그래프도 분석에 집중할 수 있도록 드릴다운하고 제한할 수 있습니다.

막대 그래프와 선 그래프는 모두 여러 데이터 집합을 표시할 수 있습니다. 즉, 각 x축 데이터 포인트의 y축에 여러 값을 표시할 수 있습니다. 예를 들어 고유한 이니시에이터 및 응답자의 총 수를 표시할 수 있습니다. 원도표는 데이터 집합을 하나만 표시할 수 있습니다.

x축, y축 또는 두 축을 모두 변경하여 연결 그래프에 다른 데이터와 데이터 집합을 표시할 수 있습니다. 원도표의 경우, x축을 변경하면 독립 변수가 변경되고 y축을 변경하면 종속 변수가 변경됩니다.

관련 항목

연결 요약(그래프에 대한 집계된 데이터), 772 페이지

연결 이벤트 그래프 사용

management center에서는 연결 이벤트 그래프를 보고, 찾는 정보에 맞게 그래프를 조작할 수 있습니다.

연결 그래프에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 연결 이벤트의 테이블 보기에서 종료되는 사전 정의된 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**을(를) 선택합니다.

참고 그래프 대신 연결 이벤트 테이블이 표시되거나 다른 그래프를 보려는 경우, 워크플로 제목별로 **(switch workflow)**을 클릭하고 그래프를 포함하는 사전 정의된 워크플로 또는 맞춤형 워크플로를 선택합니다. 미리 정의된 연결 이벤트 워크플로(연결 그래프 포함)는 연결의 테이블 보기에서 종료됩니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- Time Range(시간 범위) - 시간 범위를 조정합니다. 그래프에 아무것도 표시되지 않는 경우에 유용합니다(타임 윈도우 변경, 710 페이지 참조).
- Field Names(필드 이름) - 그래프로 표시할 수 있는 데이터에 관한 자세한 정보는 연결 및 보안 관련 연결 이벤트 필드, 773 페이지 섹션을 참조하십시오.
- Host Profile(호스트 프로파일) - IP 주소에 대한 호스트 프로파일을 보려면, 연결 데이터를 이니시에이터 또는 응답자별로 표시하는 그래프에서 막대 그래프의 막대나 원도표의 쐐기를 클릭하고 **View Host Profile(**호스트 프로파일 보기**)**을 선택합니다.
- User Profile(사용자 프로파일) - 사용자 프로파일 정보를 보려면, 연결 데이터를 이니시에이터 사용자별로 표시하는 그래프에서 막대 그래프의 막대나 원도표의 쐐기를 클릭하고 **View User Profile(**사용자 프로파일 보기**)**을 선택합니다.
- Other Information(기타 정보) - 그래프로 표시한 데이터에 관해 자세히 알고 싶다면, 선 그래프의 특정 지점이나 막대 그래프의 막대 또는 원도표의 쐐기에 마우스 포인터를 올립니다.
- Constrain(제한) - 워크플로우를 다음 페이지로 진행하지 않고 아무 X축(독립 변수) 기준을 이용하여 연결 그래프를 제한하려는 경우, 선 그래프의 특정 지점이나 막대 그래프의 막대 또는 원도표의 쐐기를 클릭하고 **View by...(**보기 기준**)** 옵션을 선택합니다.
- Data Selection(데이터 선택) - 그래프에 표시되는 데이터를 변경하려면 **X-Axis(X**축**)** 또는 **Y-Axis(Y**축**)**를 클릭하고 그래프로 표시한 새 데이터를 선택합니다. X축을 **Time(**시간**)**으로 변경하거나 시간에서 다른 항목으로 변경하면 그래프 유형도 변경됩니다. Y축을 변경하면 표시되는 데이터 집합도 영향을 받습니다.
- Datasets(데이터 집합) - 그래프의 데이터 집합을 변경하는 경우, **Datasets(**데이터 집합**)**를 클릭하고 새 데이터 집합을 선택합니다.
- Detach(분리) - 기본 시간 범위에 영향을 주지 않고 추가 분석을 수행할 수 있도록 연결 그래프를 분리하려면 **Detach(**분리**)**를 클릭합니다.

  팁 분리된 그래프에서 **New Window(**새 창**)**를 클릭하여 복사본을 만듭니다. 그러면 각각의 분리된 그래프에 서로 다른 분석을 수행할 수 있습니다. 트래픽 프로파일은 분리된 그래프라는 점을 유의하십시오.

- Drill Down(드릴다운) - 워크플로의 다음 페이지로 드릴다운하려면, 선 그래프의 특정 지점이나 막대 그래프의 막대 또는 원도표의 쐐기를 클릭하고 **Drill-down(**드릴다운**)**을 선택합니다. 선 그래프의 특정 지점을 클릭하면 이 클릭한 지점을 중심으로 다음 페이지의 시간 범위가 10분 간격

으로 제한됩니다. 막대 그래프의 막대를 클릭하거나 원도표의 쐐기 모양을 클릭하면 막대 또는 쐐기 모양에 따라 표시된 기준에 의해 다음 페이지가 제한됩니다.

- Export(내보내기) - 그래프에 대한 연결 데이터를 CSV(쉼표로 구분된 값) 파일로 내보내려면 **Export Data(**데이터 내보내기**)**를 클릭합니다. 그런 다음 **Download CSV File(CSV** 파일 다운로드**)**을 클릭하고 파일을 저장합니다.
- Graph Type(그래프 유형): 선 - 표준 또는 속도(변경 속도) 그래프로 전환하려면 **Velocity(**속도**)**를 클릭하고 **Standard(**표준**)** 또는 **Velocity(**속도**)**를 선택합니다.
- Graph Type(그래프 유형): 막대 및 원 - 막대 그래프 또는 원도표로 전환하려면 **Switch to Bar(**막대 그래프로 전환**)** 또는 **Switch to Pie(**원도표로 전환**)**를 클릭합니다. 원도표에는 여러 데이터 집합을 표시할 수 없으며, 따라서 여러 데이터 집합이 있는 막대 그래프에서 원도표로 전환하면 원도표에는 자동으로 선택되는 데이터 집합 하나만 표시됩니다. 표시할 데이터세트를 선택할 경우, management center은(는) 이니시에이터 및 응답자 통계보다 전체 통계를 우선시하고, 응답자 통계보다는 이니시에이터 통계를 우선시합니다.
- 페이지 간 이동 - 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 이벤트 보기 간 이동 - 다른 이벤트 보기로 이동하여 연결된 이벤트를 보려면 **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.
- Recenter(중앙으로 지정) - 시간 범위를 변경하지 않고 특정 시간 지점을 선 그래프의 중앙으로 지정하려면, 해당 지점을 클릭하고 **Recenter(**중앙으로 지정**)**를 선택합니다.
- Zoom(확대/축소) - 확대 또는 축소하지 않고 특정 시간 지점을 선 그래프의 중앙으로 지정하려면, 해당 지점을 클릭하고 **Zoom(**확대/축소**)**을 선택한 다음 새 기간을 선택합니다.

참고 제한, 중앙으로 지정, 확대/축소 작업은 management center의 기본 시간 범위를 변경합니다. 단 분리된 그래프를 이용해 작업하는 경우는 예외입니다.

예**:** 연결 그래프 제한

예**:** 원도표의 **X**축과 **Y**축 변경

시간 추이에 따른 연결 그래프를 고려해 보십시오. 포트에 따라 그래프의 포인트를 제한할 경우, 탐지된 연결 이벤트 수를 기준으로 가장 활성화된 포트 10개가 제시되지만, 사용자가 클릭한 포인트를 중심으로 한 10분 간격으로 제한된 막대 그래프가 표시됩니다.

막대 중 하나를 클릭하고 **View by Initiator IP(**이니시에이터 **IP**별로 보기**)**를 선택하여 그래프를 추가로 제한할 경우, 이전과 동일한 10분 간격뿐만 아니라 클릭한 막대에 따라 표시되는 포트를 기준으로 제한된 새로운 막대 그래프가 표시됩니다.

포트당 킬로바이트 단위로 그래프를 작성하는 원도표를 고려해보십시오. 이 경우 x축은 **Responder Port**이고 y축은 **KBytes**입니다. 이러한 원도표는 특정 간격 동안 모니터링되는 네

트워크를 통해 전송된 데이터의 총 킬로바이트를 나타냅니다. 원의 쐐기 모양은 각 포트에서 탐지된 데이터의 비율을 나타냅니다.

- **Application Protocol(**애플리케이션 프로토콜**)**에 대한 차트의 x축을 변경할 경우 원도표에는 전송된 총 킬로바이트가 계속 표시되지만, 원형의 쐐기 모양은 각 탐지된 애플리케이션 프로토콜에 전송된 데이터의 비율을 나타냅니다.
- 도표의 y축을 **Packets**로 변경할 경우 원도표는 특정 간격 동안 모니터링되는 네트워크를 통해 전송된 총 패킷 수를 나타내며, 원의 쐐기 모양은 각 포트에서 탐지된 총 패킷 수의 비율을 나타냅니다.

관련 항목

워크플로 사용, 689 페이지
이벤트 보기 구성, 210 페이지

연결 그래프 데이터 옵션

x축, y축 또는 두 축을 모두 변경하여 연결 그래프에 다른 데이터를 표시할 수 있습니다. 원도표의 경우, x축을 변경하면 독립 변수가 변경되고 y축을 변경하면 종속 변수가 변경됩니다.

표 ***80: X***축 옵션

X축 옵션	그래프 유형	이 데이터를 그래프로 표시
애플리케이션 프로토콜	막대 또는 원	가장 활성화된 10가지 애플리케이션 프로토콜별
디바이스	막대 또는 원	가장 활성화된 10가지 매니지드 디바이스별
초기자 IP	막대 또는 원	가장 활성화된 10가지 이니시에이터 호스트 IP 주소별
이니시에이터 사용자	막대 또는 원	가장 활성화된 10가지 이니시에이터 사용자별
응답기 IP	막대 또는 원	가장 활성화된 10가지 응답자 호스트 IP 주소별
응답자 포트	막대 또는 원	가장 활성화된 10가지 응답자 포트별
소스 디바이스	막대 또는 원	가장 활성화된 10가지 NetFlow 데이터 엑스포터, 그리고 Firepower System 매니지드 디바이스가 탐지한 모든 연결에 대한 `Firepower` 라는 이름의 소스 디바이스별

X축 옵션	그래프 유형	이 데이터를 그래프로 표시
시간	라인	시간 추이 y축을 **Time(**시간**)**으로 변경하거나 시간에서 다른 항목으로 변경하면 그래프 유형도 변경되며, 데이터 집합이 변경될 수도 있습니다.

표 ***81: Y***축 옵션

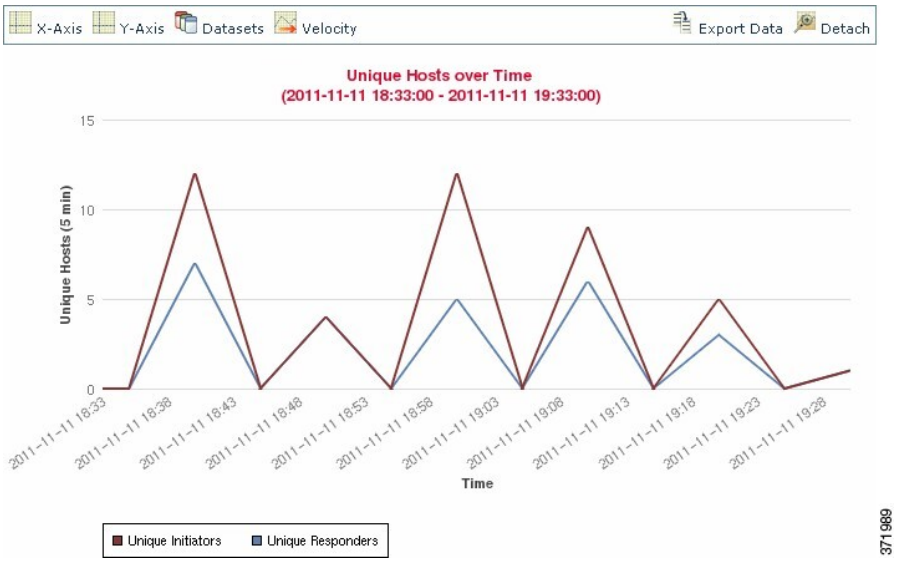
Y축 옵션	**X**축 기준을 사용하여 이 데이터를 그래프로 표시
바이트	전송된 바이트
연결	연결 수
KB	전송된 킬로바이트
초당 KB	초당 킬로바이트
패킷	전송된 패킷 수
고유 호스트	탐지한 고유 호스트 수
고유한 애플리케이션 프로토콜	고유 애플리케이션 프로토콜 수
고유한 사용자	고유한 사용자 수

여러 데이터 집합이 포함된 연결 그래프

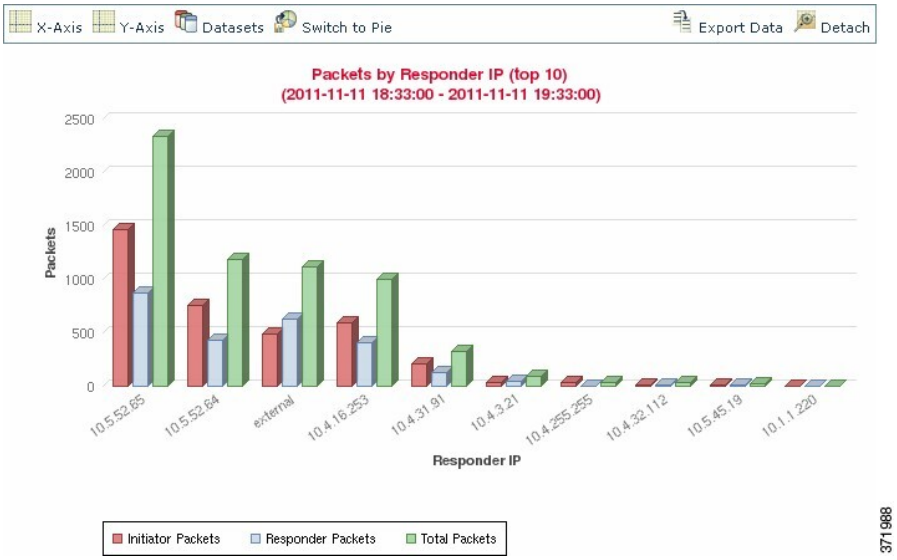
막대 그래프와 선 그래프는 모두 여러 데이터 집합을 표시할 수 있습니다. 즉, 각 x축 데이터 포인트의 y축에 여러 값을 표시할 수 있습니다. 예를 들어 고유한 이니시에이터 및 응답자의 총 수를 표시할 수 있습니다.

참고 원도표에서는 여러 데이터세트를 표시할 수 없습니다. 여러 데이터세트가 있는 막대 그래프에서 원도표로 전환할 경우, 원도표에는 자동으로 선택된 하나의 데이터세트만 표시됩니다. 표시할 데이터세트를 선택할 경우, management center은(는) 이니시에이터 및 응답자 통계보다 전체 통계를 우선시하고, 응답자 통계보다는 이니시에이터 통계를 우선시합니다.

선 그래프에서 여러 데이터세트는 각기 다른 색상의 여러 선으로 표시됩니다. 예를 들어 다음 그래픽에는 1시간 간격 동안 모니터링된 네트워크에서 탐지된 고유한 개시자의 총수 및 고유한 응답자의 총수가 표시됩니다.



막대 그래프에서 여러 데이터세트는 각 x축 데이터 포인트의 색상 막대로 표시됩니다. 예를 들어 다음 막대 그래프에는 모니터링된 네트워크에서 전송된 총 패킷, 이니시에이터가 전송한 패킷, 응답자가 전송한 패킷이 표시됩니다.



연결 그래프 데이터 집합 옵션

다음 표에서는 연결 그래프의 x축에 표시할 수 있는 데이터세트를 설명합니다.

표 ***82:*** 데이터 집합 옵션

y축에 표시되는 내용	선택 가능한 데이터 집합
연결	기본값 전용 - 모니터링되는 네트워크에서 탐지된 연결의 수(**Connections**) 이는 트래픽 프로파일 그래프의 유일한 옵션입니다.

y축에 표시되는 내용	선택 가능한 데이터 집합
KB	다음을 조합하여 선택 • 모니터링되는 네트워크에서 전송된 총 킬로바이트(**Total KBytes**) • 모니터링되는 네트워크의 호스트 IP 주소에서 전송한 킬로바이트 수(**Initiator KBytes**) • 모니터링되는 네트워크의 호스트 IP 주소가 수신한 킬로바이트 수(**Responder KBytes**)
초당 KB	기본값 전용 - 모니터링되는 네트워크에서 전송된 초당 총 킬로바이트(**Total KBytes Per Second**)
패킷	다음을 조합하여 선택 • 모니터링되는 네트워크에서 전송된 총 패킷(**Total Packets**) • 모니터링되는 네트워크의 호스트 IP 주소에서 전송한 패킷 수(**Initiator Packets**) • 모니터링되는 네트워크의 호스트 IP 주소가 수신한 패킷 수(**Responder Packets**)
고유 호스트	다음을 조합하여 선택 • 모니터링되는 네트워크의 고유한 세션 개시자 수(**Unique Initiators**) • 모니터링되는 네트워크의 고유한 세션 응답자 수(**Unique Responders**)
고유한 애플리케이션 프로토콜	기본값 전용 - 모니터링되는 네트워크의 고유한 애플리케이션 프로토콜 수(**Unique Application Protocols**)
고유한 사용자	기본값 전용 - 모니터링되는 네트워크의 세션 개시자에 로깅된 고유한 사용자 수(**Unique Initiator Users**)

이벤트 시간 제약 조건

각 이벤트에는 이벤트가 발생한 시점을 나타내는 타임스탬프가 있습니다. 시간 범위라고도 하는 타임 윈도우를 설정하여 일부 워크플로에 나타나는 정보를 제한할 수 있습니다.

시간을 기준으로 제한할 수 있는 이벤트를 기반으로 하는 워크플로는 페이지 상단에 시간 범위 줄이 나타납니다.

기본적으로 워크플로는 지난 시간으로 설정된 확장 타임 윈도우를 사용합니다. 예를 들어 오전 11:30분에 로그인할 경우 오전 10:30분부터 오전 11:30분까지의 이벤트를 볼 수 있습니다. 시간이 경과하면서 타임 윈도우가 확장됩니다. 오후 12:30분에는 오전 10:30분부터 오후 12:30분까지의 이벤트를 볼 수 있습니다.

이 동작은 이벤트 보기 설정에서 자체 기본 타임 윈도우를 설정해 변경할 수 있습니다. 이것은 세 가지 속성을 제어합니다.

- 타임 윈도우 유형(고정, 확장, 슬라이딩)
- 타임 윈도우 길이
- 타임 윈도우 개수(다중 타임 윈도우 또는 단일 글로벌 타임 윈도우)

기본 타임 윈도우 설정과 무관하게 이벤트 분석 과정에서 페이지 맨 위의 시간 범위를 클릭하면 표시되는 Date/Time(시간/날짜) 팝업 창에서 수동으로 타임 윈도우를 변경할 수 있습니다. 구성한 타임 윈도우의 개수 및 사용 중인 어플라이언스의 유형에 따라 Date/Time(시간/날짜) 창을 사용하여 현재 보고 있는 이벤트 유형의 기본 타임 윈도우를 변경할 수도 있습니다.

마지막으로, 슬라이딩 또는 확장 워크플로를 보는 도중 타임 윈도우를 일시 중지할 수 있습니다. 타임 윈도우 일시 중지로 데이터 집합 임시 중지, 711 페이지의 내용을 참조하십시오.

관련 항목

이벤트 보기 구성, 210 페이지
연결 및 보안 관련 연결 이벤트 테이블 사용, 799 페이지

이벤트에 대한 세션별 타임 윈도우 맞춤 설정

기본 타임 윈도우과 무관하게 이벤트 분석 과정에서 타임 윈도우를 수동으로 변경할 수 있습니다.

참고 수동 타임 윈도우 설정은 현재 세션에만 유효합니다. 로그아웃하고 다시 로그인하면 타임 윈도우는 기본값으로 돌아갑니다.

구성된 타임 윈도우의 수에 따라 어떤 워크플로의 타임 윈도우를 변경하면 어플라이언스의 다른 워크플로에 영향을 줄 수 있습니다. 예를 들어 단일 글로벌 타임 윈도우가 있을 경우 한 워크플로의 타임 윈도우를 변경하면 어플라이언스의 다른 워크플로에서도 변경됩니다. 이와 달리 다중 타임 윈도우를 사용하는 경우 감사 로그 또는 상태 이벤트 워크플로의 타임 윈도우를 변경하더라도 다른 타임 윈도우에 영향을 주지 않습니다. 반면에 다른 이벤트 종류의 타임 윈도우를 변경하면 (감사 이벤트 및 상태 이벤트를 제외하고) 시간의 제한을 받을 수 있는 모든 이벤트에 적용됩니다.

일부 워크플로는 시간의 제한을 받지 않을 수 있으므로 타임 윈도우 설정은 호스트, 호스트 속성, 애플리케이션, 애플리케이션 세부사항, 취약성, 사용자 또는 허용 목록 위반을 기반으로 한 워크플로에는 적용되지 않습니다.

Date/Time(시간/날짜) 창의 Time Window(타임 윈도우) 탭을 사용하여 수동으로 타임 윈도우를 구성합니다. 기본 타임 윈도우 설정에서 구성한 타임 윈도우의 수에 따라 탭의 제목은 다음 중 하나가 됩니다.

- **Events Time Window(**이벤트 타임 윈도우**)** - 다중 타임 윈도우를 구성했고 감사 로그 또는 상태 이벤트 워크플로가 아닌 워크플로의 타임 윈도우를 설정하는 경우
- **Health Monitoring Time Window(**상태 모니터링 타임 윈도우**)** - 다중 타임 윈도우를 구성했고 상태 이벤트 워크플로의 타임 윈도우를 설정하는 경우

- **Audit Log Time Window(**감사 로그 타임 윈도우**)** - 다중 타임 윈도우를 구성했고 감사 로그에 대한 타임 윈도우를 설정하는 경우
- **Global Time Window(**전역 타임 윈도우**)** - 단일 타임 윈도우를 구성한 경우

타임 윈도우를 구성할 때는 사용할 타임 윈도우 유형을 가장 먼저 결정해야 합니다.

- 고정(*static*) 타임 윈도우는 특정 시작 시간부터 종료 시간까지의 모든 이벤트를 표시합니다.
- 확장(*expanding*) 타임 윈도우는 특정 시작 시간부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 타임 윈도우가 확장되고 새 이벤트가 이벤트 보기에 추가됩니다.
- 슬라이딩(*sliding*) 타임 윈도우는 특정 시작 시간(예: 1주일 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 페이지를 새로고침하면 타임 윈도우가 "슬라이딩"하므로 구성된 범위(이 예에서는 지난주)의 이벤트만 볼 수 있습니다. 검사하는 동안 데이터 집합의 업데이트를 일시 중단하는 방법은 타임 윈도우 일시 중지로 데이터 집합 임시 중지, 711 페이지 섹션을 참조하십시오.

선택하는 유형에 따라 Date/Time(시간/날짜) 창이 바뀌어 각기 다른 설정 옵션을 제공합니다.

참고 Firepower System에서는 시간대 환경설정에서 지정한 시간에 따라 24시간 시계를 사용합니다.

타임 윈도우 설정

다음 표에서는 Time Window 탭에서 구성할 수 있는 다양한 설정에 대해 설명합니다.

표 ***83:*** 타임 윈도우 설정

설정	타임 윈도우 유형	설명
타임 윈도우 유형 드롭다운 목록	해당 없음	사용할 타임 윈도우의 유형을 고정, 확장, 슬라이딩 중에서 선택합니다. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
타임 캘린더 시작	고정, 확장	타임 윈도우의 시작 날짜와 시간을 지정합니다. 모든 시간대의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다. 달력 대신 아래에서 설명하는 미리 설정 옵션을 사용할 수 있습니다.

설정	타임 윈도우 유형	설명
타임 캘린더 종료	고정	타임 윈도우의 종료 날짜와 시간을 지정합니다. 모든 시간대의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다. 확장 타임 윈도우를 사용하는 경우 End Time 달력이 회색으로 표시되어 종료 시간이 "현재"임을 나타냅니다. 달력 대신 아래에서 설명하는 미리 설정 옵션을 사용할 수 있습니다.
최종 필드 및 드롭다운 목록 보기	슬라이딩	슬라이딩 타임 윈도우의 길이를 구성합니다.
미리 설정: 모두	모두	목록에 있는 시간 범위 중 하나를 클릭하여 어플라이언스의 로컬 시간에 따라 타임 윈도우를 변경합니다. 예를 들어 **1 week(1** 주**)**클릭하면 지난주를 나타내도록 타임 윈도우가 변경됩니다. 미리 설정된 값을 클릭하면 선택한 설정을 반영하여 달력이 변경됩니다.
미리 설정: 현재	고정, 확장	목록에 있는 시간 범위 중 하나를 클릭하여 어플라이언스의 로컬 시간 및 날짜에 따라 타임 윈도우를 변경합니다. 미리 설정된 값을 클릭하면 선택한 설정을 반영하여 달력이 변경됩니다. 다음을 참고하십시오. • 현재 요일은 자정에 시작합니다. • 현재 주는 일요일 자정에 시작합니다. • 현재 월은 월의 첫날 자정에 시작합니다.
미리 설정: 동기화	모두(글로벌 타임 윈도우를 사용하는 경우에는 사용 불가)	다음 중 하나를 클릭합니다. • **Events Time Window(**이벤트 타임 윈도우**)** - 현재 타임 윈도우를 이벤트 타임 윈도우dhk 동기화합니다. • **Health Monitoring Time Window(**상태 모니터링 타임 윈도우**)** - 현재 타임 윈도우를 상태 모니터링 타임 윈도우와 동기화합니다. • **Audit Log Time Window(**감사 로그 타임 윈도우**)** - 현재 타임 윈도우를 감사 로그 타임 윈도우와 동기화합니다.

타임 윈도우 변경

프로시저

단계 **1** 시간으로 제한된 워크플로우에서 **Time Range(**시간 범위**)** ( )를 클릭하여 Date/Time(날짜/시간) 창으로 이동합니다.

단계 **2** **Events Time Window(**이벤트 타임 윈도우**)**에서 타임 윈도우 설정, 709 페이지에 설명된 대로 타임 윈도우를 설정합니다.

팁 **Reset**을 클릭하여 타임 윈도우를 기본 설정으로 변경합니다.

단계 **3** **Apply(**적용**)**를 클릭합니다.

타임 윈도우 일시 중지로 데이터 집합 임시 중지

슬라이딩 또는 확장 타임 윈도우를 사용하는 경우, 타임 윈도우를 일시 중지해 워크플로가 제공하는 데이터의 스냅샷을 조사할 수 있습니다. 중지하지 않은 워크플로가 업데이트되면 조사할 이벤트가 제거되거나 조사 대상이 아닌 이벤트가 추가될 수 있습니다. 이 기능은 이런 경우에 유용합니다.

페이지 하단의 링크를 클릭해 다른 이벤트 페이지를 표시하면 타임 윈도우는 자동으로 일시 중지됩니다. 준비가 끝나면 타임 윈도우의 일시 중지를 취소하면 됩니다.

분석을 마치면 타임 윈도우의 일시 중지를 취소할 수 있습니다. 타임 윈도우 일시 중지를 취소하면 환경설정에 따라 업데이트되며, 이벤트 보기도 업데이트되어 일시 중지 취소된 타임 윈도우가 반영됩니다.

이벤트 타임 윈도우를 일시 중지하더라도 대시보드에 아무런 영향이 없으며, 또한 대시보드를 일시 중지하더라도 이벤트 타임 윈도우 일시 중지는 영향받지 않습니다.

프로시저

시간 기준으로 제한되는 워크플로에서, 원하는 시간 범위 제어를 선택합니다.

- 시간 창을 일시 중지하려면 시간 범위 제어 아이콘**(Pause(**일시 중지**)** ())을 클릭합니다.
- 시간 창 일시 중지를 취소하려면 시간 범위 제어 아이콘**(Play(**재생**)** ())을 클릭합니다.

이벤트에 대한 기본 타임 윈도우

이벤트 분석 과정에서 Date/Time(날짜/시간) 창의 Preferences(환경설정) 탭을 사용하면 이벤트 보기 설정을 사용하지 않고도 현재 표시하는 이벤트 유형의 기본 타임 윈도우를 변경할 수 있습니다.

이렇게 기본 타임 윈도우를 변경하면 현재 보고 있는 이벤트 유형의 기본 타임 윈도우만 바뀝니다. 예를 들어 다중 타임 윈도우를 구성한 경우 Preferences(환경설정) 탭에서 기본 타임 윈도우를 변경하면 이벤트, 상태 모니터링 또는 감사 로그 창, 즉 첫 번째 탭에 표시된 타임 윈도우의 설정이 바뀝니다. 단일 타임 윈도우를 구성한 경우 Preferences(환경설정) 탭에서 기본 타임 윈도우를 변경하면 모든 이벤트 유형의 기본 타임 윈도우가 바뀝니다.

관련 항목

기본 시간대, 212 페이지

이벤트 유형에 대한 기본 타임 윈도우 옵션

다음 표에서는 Preferences(환경설정) 탭에서 구성할 수 있는 다양한 설정에 대해 설명합니다.

표 ***84:*** 타임 윈도우 환경설정

기본 설정	설명
간격 새로고침	이벤트 보기의 새로 고침 간격을 분 단위로 설정합니다. 0을 입력하면 새로 고침 옵션이 비활성화됩니다.
타임 윈도우 수	사용할 타임 윈도우의 개수를 지정합니다. • 감사 로그, 상태 이벤트, 시간의 제한이 가능한 이벤트 기반 워크플로에 각각 기본 타임 윈도우를 구성하려면 **Multiple**을 선택합니다. • 모든 이벤트에 적용되는 글로벌 타임 윈도우를 사용하려면 **Single**을 선택합니다.
Default Time Window: Show the Last - Sliding	이 설정에서는 지정하는 길이의 슬라이딩 기본 타임 윈도우를 구성할 수 있습니다. 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하면 시간대가 "슬라이딩"하므로 항상 지난 1시간의 이벤트가 표시됩니다.
Default Time Window: Show the Last - Static/Expanding	이 설정에서는 지정하는 길이의 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 고정 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 활성화) 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다. 확장 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 비활성화) 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대 현재 시간으로 확장됩니다.
Default Time Window: Current Day - Static/Expanding	이 설정에서는 현재 일에 대해 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 현재 날짜는 현재 세션의 표준 시간대 설정에 따라 자정에 시작합니다. 고정 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 활성화) 어플라이언스는 자정부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다. 확장 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 비활성화) 어플라이언스는 자정부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대가 현재 시간으로 확장됩니다. 로그아웃하기 전 24시간 이상 분석이 계속될 경우 이 시간대가 24시간을 초과할 수 있습니다.

기본 설정	설명
Default Time Window: Current Week - Static/Expanding	이 설정에서는 현재 주에 대해 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 현재 주는 현재 세션의 표준 시간대 설정에 따라 이전 일요일 자정에 시작합니다. 고정 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 활성화) 어플라이언스는 자정부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경하는 경우, 시간대가 고정되어 있으므로 고정 시간대에 발생한 이벤트만 표시됩니다. 확장 타임 윈도우의 경우(**Use End Time(**종료 시간 사용**)** 확인란 비활성화) 어플라이언스는 일요일 자정부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간대는 현재 시간으로 확장됩니다. 로그아웃하기 전 1주일 이상 분석이 계속될 경우, 시간대는 1주를 초과할 수 있습니다.

이벤트 유형에 대한 기본 타임 윈도우 변경

프로시저

단계 **1** 시간으로 제한된 워크플로우에서 **Time Range(**시간 범위**)** ( )를 클릭하여 Date/Time(날짜/시간) 창으로 이동합니다.

단계 **2** **Preferences(**환경설정**)**를 클릭하고 이벤트 유형에 대한 기본 타임 윈도우 옵션, 712 페이지에 설명된 대로 환경설정을 변경합니다.

단계 **3** **Save Preferences(**환경설정 저장**)**를 클릭합니다.

단계 **4** 다음 2가지 옵션을 사용할 수 있습니다.

- 보고 있는 이벤트 보기에 새 기본 타임 윈도우 설정을 적용하려면 **Apply(**적용**)**를 클릭하여 Date/Time(날짜/시간) 창을 닫고 이벤트 보기를 새로 고칩니다.
- 기본 타임 윈도우 설정을 적용하지 않고 분석을 계속하려면 **Apply(**적용**)**를 클릭하지 않고 Date/Time(날짜/시간) 창을 닫습니다.

이벤트 보기 제약 조건

워크플로 페이지에 표시되는 정보는 지정된 제약 조건에 따라 결정됩니다. 예를 들어 초기에 이벤트 워크플로를 열 때 그 정보는 이전 시간 동안 생성된 이벤트로 제한됩니다.

워크플로의 다음 페이지로 이동하고 표시되는 데이터를 특정 값으로 제한하려면 페이지에서 해당 값의 행을 선택하고 **View(**보기**)**를 클릭합니다. 워크플로에서 다음 페이지로 이동하되 현재 제약 조건을 유지하고 모든 이벤트를 이월하려면 **View All(**모두 보기**)**을 선택합니다.

참고 카운트가 아닌 다중 값을 포함한 행을 선택하고 **View(**보기**)**를 클릭하면 복합 제약 조건이 생성됩니다.

워크플로에서 데이터를 제한하는 3번째 방법이 있습니다. 선택한 값의 행으로 페이지를 제한하고 선택한 값을 페이지 맨 위의 제약 조건 목록에 추가하려면 페이지에서 특정 행의 값을 클릭합니다. 예를 들어 로깅된 연결의 목록을 보는 중에 액세스 컨트롤을 통해 허용된 연결로 목록을 제한하려면 **Action(**작업**)** 열에서 **Allow(**허용**)**를 클릭합니다. 또 다른 예로 침입 이벤트를 보는 중에 목적지 포트가 80인 이벤트로 제한하려는 목록을 제한하려는 경우 **Destination Port/ICMP Code(**대상 포트**/ICMP** 코드**)** 열에서 **80 (http)/tcp**를 클릭합니다.

팁 모니터 규칙 기준에 따라 연결 이벤트를 제한하는 절차는 약간 다르며 추가 단계가 필요할 수 있습니다. 또한 관련된 파일 또는 침입 정보를 기준으로 연결 이벤트를 제한할 수는 없습니다.

검색을 사용하여 워크플로의 정보를 제한할 수도 있습니다. 단일 열에서 다중 값을 대상으로 제한하려면 이 기능을 사용합니다. 예를 들어 두 IP 주소와 관련된 이벤트를 보려는 경우 **Edit Search(**검색 편집**)**를 클릭하고 Search(검색) 페이지에서 해당 IP 주소 필드를 수정하여 두 주소를 모두 포함하게 한 다음 **Search(**검색**)**를 클릭합니다.

검색 페이지에 입력하는 검색 기준은 페이지 맨 위에 제약 조건으로 나열되며, 그에 따라 결과 이벤트가 제한됩니다. management center에서는 현재 제약 조건이 다른 워크플로로 이동할 때에도 적용됩니다. 단, 복합 제약 조건인 경우는 제외합니다.

검색할 때 검색 제약 조건이 검색 중인 테이블에 적용될 것인지를 각별히 주의해야 합니다. 예를 들어 클라이언트 데이터는 연결 요약에서 사용할 수 없습니다. 연결에서 탐지된 클라이언트를 기반으로 연결 이벤트를 검색한 다음 그 결과를 연결 요약 이벤트 보기에 표시할 경우 management center에서는 아무런 제한을 받지 않은 것처럼 연결 데이터를 표시합니다. 잘못된 제약 조건은 N/A(not applicable) 레이블이 지정되고 취소선으로 표시됩니다.

이벤트 제약

프로시저

단계 **1** 워크플로 선택, 691 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 모든 워크플로에는 다음 옵션이 있습니다.

- 단일 값과 일치하는 이벤트만 보도록 제한하려면, 페이지의 행에서 원하는 값을 클릭합니다.
- 여러 값과 일치하는 이벤트만 보도록 제한하려면, 해당 값이 있는 이벤트의 확인란을 선택하고 **View(**보기**)**를 클릭합니다.

  참고 행에 카운트가 아닌 다중 값이 있을 경우 복합 제약 조건이 추가됩니다.

- 제약 조건을 제거하려면 Search Constraints(검색 제약 조건) **Expand Arrow(**확장 화살표**)(**)를 클릭하고 확장된 Search Constraints(검색 제약 조건) 목록에서 제약 조건 이름을 클릭합니다.
- Search(검색) 페이지를 사용하여 제약 조건을 편집하려면 **Edit Search(**검색 편집**)**를 클릭합니다.
- 제약 조건을 저장된 검색으로 저장하려면 **Save Search(**저장 검색**)**를 클릭하고 쿼리에 이름을 지정합니다.

  참고 복합 제약 조건을 포함한 쿼리는 저장할 수 없습니다.

- 동일한 제약 조건을 다른 이벤트 보기와 함께 사용하려면 **Jump to(**이동**)**를 클릭하고 이벤트 보기를 선택합니다.

  참고 다른 워크플로로 전환하는 경우 복합 제약 조건은 유지되지 않습니다.

- 제약 조건 표시를 전환하려면 Search Constraints(검색 제한 조건) **Expand Arrow(**확장 화살표**)(**) 또는 Search Constraints(검색 제약 조건) **Collapse Arrow(**축소 화살표**)(**)를 클릭합니다. 제약 조건의 목록이 커서 화면의 대부분을 차지할 때 유용한 기능입니다.

복합 이벤트 보기 제약

복합 제약 조건은 특정 이벤트에 대해 카운트가 아닌 모든 값을 기반으로 합니다. 카운트가 아닌 다중 값이 있는 행을 선택할 때 해당 페이지에서 그 행의 카운트가 아닌 모든 값과 매칭하는 이벤트만 가져오는 복합 제약 조건이 설정됩니다. 예를 들어 소스 IP 주소 `10.10.31.17`, 목적지 IP 주소 `10.10.31.15`를 포함하는 행 및 소스 IP 주소가 `172.10.10.17`, 목적지 IP 주소가 `172.10.10.15`인 행을 선택할 경우 다음 사항이 모두 검색됩니다.

- 소스 IP 주소가 10.10.31.17이고 목적지 IP 주소가 10.10.31.15인 이벤트

  또는

- 소스 IP 주소가 172.10.31.17이고 목적지 IP 주소가 172.10.31.15인 이벤트

복합 제약 조건을 단순 제약 조건과 결합할 경우 단순 제약 조건은 복합 제약 조건의 전 범위에 배포됩니다. 예를 들어 프로토콜 값이 `tcp`인 단순 제약 조건을 위에 소개된 복합 제약 조건에 추가한 경우 다음 사항이 모두 검색됩니다.

- 소스 IP 주소가 10.10.31.17이고 목적지 IP 주소가 10.10.31.15이며 프로토콜이 tcp인 이벤트

  또는

- 소스 IP 주소가 172.10.31.17이고 목적지 IP 주소가 172.10.31.15이며 프로토콜이 tcp인 이벤트

복합 제약 조건에 대해서는 검색을 수행하거나 검색을 저장할 수 없습니다. 또한 이벤트 보기 링크를 사용하거나 **(switch workflow)**을 클릭하여 다른 워크플로로 전환할 때 복합 제약 조건을 유지할 수 없습니다. 복합 제약 조건이 적용된 이벤트 보기에 즐겨찾기를 지정할 경우 제약 조건은 즐겨찾기와 함께 저장되지 않습니다.

복합 이벤트 보기 제약 사용

프로시저

단계 **1** 워크플로 선택, 691 페이지에 설명된 대로 적절한 메뉴 경로 및 옵션을 선택하여 워크플로에 액세스합니다.

단계 **2** 복합 제약 조건은 다음 방법으로 관리할 수 있습니다.

- 복합 제약 조건을 생성하려면 카운트가 아닌 다중 값을 포함한 행을 하나 이상 선택하고 **View(**보기**)**를 클릭합니다.
- 복합 제약 조건을 지우려면 Search Constraints(검색 제약 조건) **Expand Arrow(**확장 화살표**)**( )를 클릭하고 **Compound Constraints(**복합 제약 조건**)**를 클릭합니다.

워크플로 간 탐색

워크플로 페이지에서 **Jump to...(**이동**...)** 드롭다운 목록의 링크를 사용하여 다른 워크플로로 이동할 수 있습니다. 드롭다운 목록을 선택하여 추가 워크플로를 표시하고 선택합니다.

새 워크플로를 선택하면 선택한 행에서 공유하는 속성 및 설정된 제약 조건이 새 워크플로에서 사용됩니다(적용 가능한 경우). 구성된 제약 조건 또는 이벤트 속성이 새 워크플로의 필드에 매핑되지 않을 경우 삭제됩니다. 또한 복합 제약 조건은 다른 워크플로로 전환할 때 유지되지 않습니다. 캡처 파일 워크플로의 제약 조건은 파일 및 악성코드 이벤트 워크플로로만 전송됩니다.

참고 어떤 시간 범위의 이벤트 수를 볼 때 총 이벤트 수가 세부사항 데이터가 있는 이벤트의 수를 반영하지 않을 수 있습니다. 이는 디스크 공간 사용량을 관리하기 위해 때때로 오래된 이벤트의 세부사항을 삭제하기 때문입니다. 이벤트 세부사항이 삭제되는 경우를 최소화하기 위해 이벤트 로깅을 세밀하게 조정하여 구축에 가장 중요한 이벤트만 로깅하게 할 수 있습니다.

타임 윈도우를 일시 중지하거나 고정 타임 윈도우를 구성한 경우를 제외하고 타임 윈도우는 워크플로를 변경할 때 바뀝니다.

이 기능으로 의심스러운 활동을 더 효과적으로 조사할 수 있습니다. 예를 들어 연결 데이터를 보는 중에 내부 호스트가 비정상적으로 많은 양의 데이터를 외부 사이트에 보내는 것이 확인될 경우 responder IP 주소와 포트를 제약 조건으로 선택한 다음 **Applications(**애플리케이션**)** 워크플로로 바로 이동할 수 있습니다. 애플리케이션 워크플로는 responder IP 주소와 포트를 IP Address 및 Port 제약 조건으로 사용하면서 애플리케이션에 대한 추가 정보, 이를테면 어떤 종류의 애플리케이션인가를 표시합니다. 페이지 맨 위의 **Hosts(**호스트**)**를 클릭하여 원격 호스트의 호스트 프로파일을 볼 수도 있습니다.

애플리케이션에 대한 추가 정보를 얻은 다음 **Correlation Events(**상관관계 이벤트**)**를 클릭하여 연결 데이터 워크플로로 돌아가거나 제약 조건에서 Responder IP를 제거하거나 제약 조건에 Initiator IP를

추가하거나 **Application Details(**애플리케이션 세부사항**)**를 선택하여 시작 호스트의 사용자가 원격 호스트에 데이터를 전송할 때 사용한 클라이언트를 확인할 수 있습니다. Port 제약 조건은 Application Details 페이지에 전송되지 않습니다. 로컬 호스트를 제약 조건으로 유지하지만 다른 탐색 버튼을 사용하여 추가 정보를 찾을 수도 있습니다.

- 로컬 호스트가 어떤 정책을 위반했는지 알아보려면 IP 주소를 제약 조건으로 유지하고 **Jump to(**이동**)** 드롭다운 목록에서 **Correlation Events(**상관관계 이벤트**)**를 선택합니다.
- 호스트에 대해 침입 규칙이 트리거되었는지(공격 지표) 확인하려면 **Jump to(**이동**)** 드롭다운 목록에서 **Intrusion Events(**침입 이벤트**)**를 선택합니다.
- 로컬 호스트에 대한 호스트 프로파일을 보고 호스트가 만일의 익스플로잇 취약성을 갖고 있는지 확인하려면 **Jump to(**이동**)** 드롭다운 목록에서 **Hosts(**호스트**)**를 선택합니다.

통합 이벤트 보기로 작업

통합 이벤트는 여러 유형의 방화벽 이벤트(연결, 침입, 파일, 악성코드 및 일부 보안 관련 연결 이벤트)를 단일 화면 보기로 제공합니다. 통합 이벤트 테이블은 수준 높은 사용자 맞춤화가 가능합니다. 이벤트 보기에 표시되는 정보를 세부적으로 조정할 수 있도록 사용자 지정 필터를 생성하고 적용할 수 있습니다. 통합 이벤트 테이블의 **Live View(**라이브 보기**)** 옵션을 사용하면 방화벽 이벤트를 실시간으로 확인하고 네트워크 활동을 모니터링할 수 있습니다.

통합 이벤트 보기를 사용하는 경우에는 다음을 수행할 수 있습니다.

- 다양한 유형의 이벤트 간 관계 찾기
- 실시간으로 정책 변경의 영향 확인

프로시저

단계 **1** 분석 > 통합 이벤트을 선택합니다.

단계 **2** 특정 기간의 방화벽 이벤트를 보려면 시간 범위(고정 또는 슬라이딩)를 선택합니다. 기본적으로 통합 이벤트 보기 테이블에는 이전 시간의 이벤트가 표시됩니다. 보안 이벤트의 더욱 세부적인 컨텍스트를 가져오거나, 테이블 열을 사용자 지정하거나, 라이브 보기를 활성화하고 이벤트의 업데이트를 실시간으로 확인하기 위해 테이블을 필터링할 수 있습니다.

북마크

이벤트 분석의 특정 위치 및 시점으로 신속하게 돌아갈 수 있게 하려면 즐겨찾기를 생성합니다. 즐겨찾기는 다음 사항에 대한 정보를 유지합니다.

- 사용 중인 워크플로
- 워크플로에서 표시 중인 부분

- 워크플로 내의 페이지 번호
- 모든 검색 제약 조건
- 모든 비활성 열
- 사용 중인 시간 범위

생성하는 즐겨찾기는 즐겨찾기 액세스 권한이 있는 모든 사용자 계정에서 사용할 수 있습니다. 즉 심층 분석이 필요한 이벤트 모음을 발견할 경우 편리하게 즐겨찾기를 생성한 다음 알맞은 권한을 가진 다른 사용자에게 조사를 맡길 수 있습니다.

참고 즐겨찾기에 나타난 이벤트가 삭제될 경우(사용자 직접 삭제 또는 자동 데이터베이스 정리에 의해 삭제) 즐겨찾기는 더 이상 원래의 이벤트 집합을 표시하지 않습니다.

즐겨찾기 생성

다중 도메인 구축의 경우에는 현재 도메인에서 생성된 즐겨찾기만 볼 수 있습니다.

프로시저

단계 **1** 이벤트를 분석할 때 관심 이벤트가 표시된 상태에서 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다.

단계 **2** **Bookmark Name(**즐겨찾기 이름**)** 필드에 이름을 입력합니다.

단계 **3** **Save Bookmark(**즐겨찾기 저장**)**를 클릭합니다.

즐겨찾기 보기

다중 도메인 구축의 경우에는 현재 도메인에서 생성된 즐겨찾기만 볼 수 있습니다.

프로시저

모든 이벤트 보기는 두 가지 옵션을 제공합니다.

- **View Bookmarks(**즐겨찾기 보기**)**에 마우스 포인터를 올리고, 드롭다운 메뉴에서 원하는 즐겨찾기를 클릭합니다.
- View Bookmarks(즐겨찾기 보기) 페이지에서 **View Bookmarks(**즐겨찾기 보기**)**를 클릭하고, 원하는 즐겨찾기 이름이나 옆에 있는 **View(**보기**)** ()을 클릭합니다.

참고 원래 즐겨찾기에 나타난 이벤트가 삭제될 경우(사용자 직접 삭제 또는 자동 데이터베이스 정리에 의해 삭제) 즐겨찾기는 더 이상 원래의 이벤트 집합을 표시하지 않습니다.

워크플로우 히스토리

기능	버전	세부 사항
IPS 이벤트 데이터스토어 교체	7.1	침입 인시던트 및 이벤트 클립보드 페이지는 더 이상 사용되지 않습니다. 사용되지 않는 페이지: • **Analysis(**분석**) > Intrusions(**침입**) > Clipboard(**클립보드**)** • **Analysis(**분석**) > Intrusions(**침입**) > Incidents(**인시던트**)** 지원되는 플랫폼: management center
통합 이벤트 뷰어	7.0	연결(보안 인텔리전스 포함), 침입, 파일 및 악성 코드 등 여러 이벤트 유형이 포함된 단일 테이블을 보고 작업합니다. 새 페이지/수정 페이지: 분석 > 통합 이벤트 아래 새 페이지 지원되는 플랫폼: management center
원격으로 저장된 이벤트 작업	7.0	Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 management center에서 작업할 수 있습니다. 시스템은 가장 적합한 데이터 소스를 자동으로 사용합니다. 또는 소스를 명시적으로 선택할 수 있습니다. 이 옵션은 Security Analytics and Logging(보안 애널리틱스) 마법사를 완료한 경우에만 나타납니다. 신규/수정 페이지: 연결 이벤트를 표시하는 경우, 즉 Analysis(분석) 메뉴 아래의 Workflow table(워크플로우 테이블), 대시 보드, 상황 탐색기 및 보고서. 지원되는 플랫폼: management center
특정 경우에 워크플로우 테이블의 개선된 로딩 속도	6.6	이제 워크플로우 페이지의 테이블에는 열이 6개 이하로 표시되는 경우에만 동일한 행에 대한 개수 열이 표시됩니다. 이렇게 하면 필요한 계산량이 최소화되므로 테이블 로드 속도가 향상됩니다. 신규/수정 페이지: Analysis(분석) 메뉴 아래의 모든 페이지에서 워크플로우 테이블을 표시합니다. 지원되는 플랫폼: management center

28 장

이벤트 검색

다음 주제에서는 워크플로내의 이벤트를 검색하는 방법을 설명합니다.

이벤트 검색

Firepower System은 데이터베이스 테이블에 이벤트로 저장되는 정보를 생성합니다. 이벤트에는 어플라이언스가 이벤트를 생성하도록 만든 활동을 설명하는 여러 필드가 포함되어 있습니다. 다양한 이벤트 유형에 대해 환경에 맞춤 설정된 검색을 생성하고 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

검색을 저장할 때 이름을 지정하고 검색을 사용자만 사용할 수 있는지 어플라이언스의 모든 사용자가 사용할 수 있는지 지정합니다. 맞춤형 사용자 역할을 위한 데이터 제한으로 검색을 사용하려면 반드시 비공개 검색으로 저장해야 합니다. 전에 검색을 저장한 경우, 이를 로드하여 필요한 수정을 한 다음 검색을 시작할 수 있습니다. 맞춤형 분석 대시보드 위젯, 보고서 템플릿, 사용자 지정 사용자 역할도 저장된 검색을 사용할 수 있습니다. 저장한 검색은 Search(검색) 페이지에서 삭제할 수 있습니다.

일부 이벤트 유형의 경우, Firepower System은 예제 역할을 하고 네트워크에 대한 중요한 정보에 빠르게 액세스하도록 도와주는 사전 정의된 검색을 제공합니다. 네트워크 환경에 대해 사전 정의된 검색 내에서 필드를 수정한 다음 나중에 다시 사용하기 위해 저장할 수 있습니다.

사용할 수 있는 검색 기준은 검색 유형에 따라 다를 수 있지만 원리는 동일합니다. 검색은 모든 필드에 지정된 검색 기준에 일치하는 레코드만 반환합니다.

참고 맞춤형 테이블을 검색하려면 약간 다른 절차가 필요합니다.

관련 항목

맞춤형 테이블 검색, 748 페이지

검색 제약 조건

각 데이터베이스 테이블에는 테이블에 대해 정의된 필드에 적용할 검색 제약 조건 값을 입력할 수 있는, 자체 검색 페이지가 있습니다. 필드 유형에 따라 와일드필드 문자 또는 숫자 값 범위 같은 특수 구문을 사용해 기준을 지정할 수 있습니다.

검색 결과는 열 레이아웃의 각 테이블 필드를 표시하는 워크플로 페이지에 표시됩니다. 워크플로 페이지에 열로 표시되지 않는 필드를 이용해 일부 데이터베이스 테이블을 추가로 검색할 수도 있습니다. 워크플로 페이지 상의 결과를 볼 때 검색 결과에 적용되는 제약을 확인하려면, **Expand Arrow(**확장 화살표**)**( )을 클릭하여 활성 검색 제약을 확인합니다.

일반 검색 제약 조건

이벤트를 검색하는 경우 다음 일반 지침을 따르십시오.

- 대부분의 필드에는 부분 일치 검색에 와일드 카드가 필요합니다. 모든 필드에서 이러한 검색에 와일드 카드를 사용할 수 있습니다.

  검색 내 와일드카드 및 특수문자, 723 페이지의 내용을 참조하십시오.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a`를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a`를 사용합니다.
- 많은 숫자 필드 앞에 초과(>), 이상(>=), 미만(**<**), 이하(<=), 같음(=) 또는 같지 않음(<>) 연산자를 붙일 수 있습니다.

팁 길고 복잡한 값(SHA-256 해시 값 등)을 이용해 필드를 검색하는 경우, 소스 자료에서 검색 기준을 복사해 검색 페이지의 적절한 필드에 붙여넣을 수 있습니다.

검색 내 와일드카드 및 특수문자

연결 및 보안 인텔리전스 이벤트의 모든 텍스트 필드 및 기타 이벤트 유형의 대부분의 텍스트 필드에서 검색할 때 텍스트 필드에서 부분 일치를 검색하려면 문자열에서 지정되지 않은 문자를 나타내는 별표(*)가 필요합니다. 별표가 없는 검색은 이러한 필드의 정확한 일치 검색입니다. 와일드 카드가 필요하지 않은 필드에서도 부분 일치 검색에는 항상 와일드 카드를 사용하는 것이 좋습니다.

예를 들어 `example.com`, `www.example.com` 또는 `department.example.com`을 찾으려면 `*.example.com`으로 검색합니다. 대부분의 경우 `example.com`을 검색하면 `example.com`만 반환됩니다.

영숫자 외의 문자를 검색하려면(별표 문자 포함) 검색 문자열을 따옴표로 감싸십시오. 예를 들어 다음 문자열을 검색하려면

```
Find an asterisk (*)
```

다음을 입력합니다.

```
"Find an asterisk (*)"
```

검색 내 개체 및 애플리케이션 필터

Firepower System에서는 네트워크 설정의 일부로 사용할 수 있는 명명된 개체, 개체 그룹 및 애플리케이션 필터를 생성할 수 있습니다. 검색을 수행하거나 저장할 때 이러한 개체, 그룹 및 필터를 검색 기준으로 사용할 수 있습니다.

검색을 수행하면 개체, 개체 그룹 및 애플리케이션 필터가 `${object_name}`의 형식으로 나타납니다. 예를 들어 개체 이름이 `ten_ten_network`인 네트워크 개체는 검색에 `${ten_ten_network}`로 나타납니다.

검색 기준으로 개체를 사용할 수 있는 검색 필드 옆에 나타나는 **Object(**개체**)**(+)를 클릭할 수 있습니다.

관련 항목

개체 관리자

검색 내 시간 제약 조건

시간 값을 입력하는 검색 기준 필드에서 허용되는 형식은 다음 표에 나와 있습니다.

표 ***85:*** 검색 필드의 시간 사양

시간 형식	예
`today [at HH:MMam|pm]`	현재 `today at 12:45pm`
*YYYY-DD*MM- *HH:MM:SS*	2006-03-22 14:22:59

다음 연산자 중 하나를 시간 값 앞에 사용할 수 있습니다.

표 86: 시간 사양 연산자

운영자	예	설명
<	`< 2006-03-22 14:22:59`	2006년 3월 22일 오후 2:23 이전 타임스탬프의 이벤트를 반환합니다.
>	`> today at 2:45pm`	오늘 오후 2:45 이후 타임스탬프의 이벤트를 반환합니다.

검색 내 IP 주소

검색에서 IP 주소를 지정할 때에는 개별 IP 주소, 쉼표로 구분된 주소 목록, 주소 블록, 또는 하이픈(-)으로 구분된 IP 주소 범위를 입력할 수 있습니다. 또한 부정을 사용할 수 있습니다.

침입 이벤트, 연결 데이터 및 상관 관계 이벤트 검색과 같은 IPv6을 지 원하는 검색의 경우 IPv4 및 IPv6 주소와 CIDR/접두사 길이 주소 블록을 임의의 조합으로 입력할 수 있습니다. IP 주소별로 호스트를 검색하면 하나 이상의 IP 주소가 검색 기준과 일치하는 모든 호스트가 결과에 포함됩니다. 즉, IPv6 주소를 검색하면 기본 주소가 IPv4인 호스트가 반환될 수 있습니다.

CIDR 또는 접두사 길이 표기법을 사용하여 IP 주소 블록을 지정하려는 경우, Firepower System은 마스크 또는 접두사 길이에 의해 지정된 네트워크 IP 주소의 일부만 사용합니다. 예를 들어 `10.1.2.3/8`을 입력한 경우 Firepower System은 `10.0.0.0/8`을 사용합니다.

IP 주소는 네트워크 개체로도 표현할 수 있으므로, IP 주소 검색 기준으로 네트워크 개체를 사용하려면 IP 주소 검색 필드 옆에 나타나는 네트워크 추가 **Object(**개체**)**(+)을 클릭할 수 있습니다.

표 87: 허용되는 IP 주소 구문

지정할 주소	입력할 내용	예시
단일 IP 주소	IP 주소	`192.168.1.1` `2001:db8::abcd`
목록을 사용하여 여러 IP 주소	쉼표로 구분된 IP 주소의 목록 쉼표 전후에 공백을 추가하지 마십시오.	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
CIDR 블록 또는 접두사 길이로 지정할 수 있는 IP 주소의 범위	IPv4 CIDR 또는 IPv6 접두사 길이 표기법으로 IP 주소 블록	`192.168.1.0/24` 192.168.1.0 네트워크에서 255.255.255.0(즉, 192.168.1.0~192.168.1.255)의 IP를 지정합니다.
CIDR 블록 또는 접두사로 지정할 수 없는 IP 주소의 범위	하이픈을 사용하여 IP 주소 범위 하이픈 전후에 공백을 추가하지 마십시오.	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

IP 주소 또는 IP 주소 범위를 지정하기 위한 기타 방법의 표기법	IP 주소, 블록 또는 범위 앞에 느낌표	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

지정할 주소	입력할 내용	예시
차단되었거나 모니터링되는(하지만 차단되었을 수 있는) 호스트 호스트 프로파일 아이콘, 695 페이지의 내용을 참조하십시오.	연결 및 보안 인텔리전스 이벤트의 이니시에이터 IP 및 응답자 IP 필드: • • 차단 • 모니터	--

관련 항목

Firepower System IP 주소 규칙, 28 페이지

검색의 URL

URL을 검색할 때 와일드 카드를 포함합니다. 예를 들어 ***example.com***을 사용하여 도메인의 모든 변형(예: **https://example.com**, **division.example.com** 및 **example.com/division/**)을 찾습니다.

검색 내 매니지드 디바이스

FMC에서만, 또는 실제 고가용성 또는 확장성 구성을 통해 디바이스를 그룹화하면 그룹의 이름을 검색했을 때 그룹 내의 모든 디바이스를 결과로 올바르게 반환합니다.

그룹, 시스템은 검색 수행을 위해 그룹 이름을 적절한 회원 디바이스 이름으로 교체합니다. 장치 필드에 디바이스 그룹, 시스템은 장치 필드에 지정된 이름을 저장하고 검색이 실행될 때마다 디바이스 이름 교체를 수행합니다.

검색 내 포트

Firepower System은 검색에서 포트 번호에 대한 특정 구문을 허용합니다. 다음을 입력할 수 있습니다.

- 단일 포트 번호
- 쉼표로 구분된 포트 번호 목록
- 대시로 구분된 두 개의 포트 번호(포트 번호의 범위를 나타냄)
- 포트 번호 뒤에는 (침입 이벤트를 검색할 때만) 슬래시 (/)로 구분 된 프로토콜 약어
- 앞에 느낌표가 있는 포트 번호 또는 포트 번호의 범위(지정된 포트의 부정을 나타냄)

참고 포트 번호 또는 범위를 지정할 때는 공백을 사용하지 마십시오.

표 *88:* 포트 구문 예

예	설명
`21`	TCP와 UDP 이벤트를 비롯한 포트 21의 모든 이벤트를 반환합니다.
`!23`	포트 23의 이벤트를 제외한 모든 이벤트를 반환합니다.
`25/tcp`	포트 25의 모든 TCP 관련 침입 이벤트를 반환합니다.
`21/tcp,25/tcp`	포트 21과 25의 모든 TCP 관련 침입 이벤트를 반환합니다.
`21-25`	포트 21~25의 모든 이벤트를 반환합니다.

검색 내 이벤트 필드

이벤트를 검색하는 경우 검색 기준으로 다음 필드를 사용할 수 있습니다.

- 감사 로그 워크플로 필드, 420 페이지
- 애플리케이션 데이터 필드, 955 페이지
- 애플리케이션 세부사항 데이터 필드, 958 페이지
- 캡처된 파일 필드, 881 페이지
- 허용 목록 이벤트 필드, 989 페이지
- 연결 및 보안 관련 연결 이벤트 필드, 773 페이지
- 상관관계 이벤트 필드, 985 페이지
- 검색 이벤트 필드, 936 페이지
- 상태 이벤트 테이블, 408 페이지
- 호스트 속성 데이터 필드, 944 페이지
- 호스트 데이터 필드, 938 페이지
- 파일 및 악성코드 이벤트 필드, 863 페이지
- 침입 이벤트 필드, 810 페이지
- 침입 규칙 업데이트 로그 세부 정보, 244 페이지
- 교정 상태 테이블 필드, 993 페이지
- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Nmap* 스캔 결과 필드를 참고하십시오.
- 서버 데이터 필드, 952 페이지
- 서드파티 취약성 데이터 필드, 965 페이지

- 사용자 관련 필드, 967 페이지
- 취약성 데이터 필드, 960 페이지
- 허용 목록 위반 필드, 991 페이지

검색 수행

검색을 수행하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Search(**검색**)**를 선택합니다.

팁 워크플로의 아무 페이지에서 **Search(**검색**)**를 클릭해도 됩니다.

단계 **2** 테이블 드롭다운 목록에서 검색할 이벤트 또는 데이터 유형을 선택합니다.

단계 **3** 해당 필드에 검색 기준을 입력합니다. 사용 가능한 검색 기준에 대해 자세히 알아보려면 다음 섹션을 참조하십시오.

- 검색 제약 조건, 722 페이지
- 감사 로그 워크플로 필드, 420 페이지
- 애플리케이션 데이터 필드, 955 페이지
- 애플리케이션 세부사항 데이터 필드, 958 페이지
- 캡처된 파일 필드, 881 페이지
- 허용 목록 이벤트 필드, 989 페이지
- 연결 및 보안 관련 연결 이벤트 필드, 773 페이지
- 상관관계 이벤트 필드, 985 페이지
- 검색 이벤트 필드, 936 페이지
- 상태 이벤트 테이블, 408 페이지
- 호스트 속성 데이터 필드, 944 페이지
- 호스트 데이터 필드, 938 페이지
- 파일 및 악성코드 이벤트 필드, 863 페이지
- 침입 이벤트 필드, 810 페이지
- 침입 규칙 업데이트 로그 세부 정보, 244 페이지
- 교정 상태 테이블 필드, 993 페이지

- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Nmap* 스캔 결과 필드를 참고하십시오.
- 서버 데이터 필드, 952 페이지
- 서드파티 취약성 데이터 필드, 965 페이지
- 사용자 데이터 필드
- 사용자 활동 데이터 필드
- 취약성 데이터 필드, 960 페이지
- 허용 목록 위반 필드, 991 페이지

단계 **4** 검색을 나중에 다시 사용하려면 검색 저장, 728 페이지에 설명된 대로 검색을 저장합니다.

단계 **5** 검색을 시작하려면 **Search(검색)**를 클릭합니다. 검색 결과가 시간으로 제한되어(적용 가능한 경우) 검색 중인 테이블에 대한 기본 워크플로우에 나타납니다.

다음에 수행할 작업

- 워크플로를 사용하여 검색 결과를 분석하는 방법은 워크플로 사용, 689 페이지 섹션을 참조하십시오.

관련 항목

이벤트 보기 구성, 210 페이지

검색 저장

검색을 저장하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 저장된 검색을 표시하며 이러한 검색은 수정할 수 있습니다. 상위 도메인에서 저장된 검색도 표시되지만, 이러한 검색은 수정할 수 없습니다. 하위 도메인에서 생성된 검색을 보고 수정하려면 해당 도메인으로 전환하십시오.

시작하기 전에

- 검색 수행, 727 페이지에 설명된 대로 검색 기준을 설정하거나, 저장된 검색 로드, 729 페이지에 설명된 대로 저장된 검색을 로드합니다.

프로시저

단계 **1** 자신만 액세스할 수 있도록 검색을 비공개로 저장하려면, Search(검색) 페이지에서 **Private(비공개)** 확인란을 선택합니다.

팁 맞춤형 사용자 역할을 위한 데이터 제한으로 검색을 사용하려면 반드시 비공개 검색으로 저장해야 합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 로드한 검색의 새 버전을 저장하려는 경우에는 **Save As New(**신규로 저장**)**를 클릭합니다.
- 새 검색을 저장하거나 같은 이름을 이용해 맞춤형 검색을 덮어쓰려는 경우에는 **Save(**저장**)**를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

저장된 검색 로드

저장된 검색을 로드하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 저장된 검색을 표시하며 이러한 검색은 수정할 수 있습니다. 상위 도메인에서 저장된 검색도 표시되지만, 이러한 검색은 수정할 수 없습니다. 하위 도메인에서 생성된 검색을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Search(**검색**)**을(를) 선택합니다.

팁 워크플로의 아무 페이지에서 **Search(**검색**)**를 클릭해도 됩니다.

단계 **2** 테이블 드롭다운 목록에서 검색할 이벤트 또는 데이터 유형을 선택합니다.

단계 **3** **Custom Searches(**맞춤형 검색**)** 목록 또는 **Predefined Searches(**사전 정의된 검색**)** 목록에서 로드하려는 검색을 선택합니다.

단계 **4** 다른 검색 기준을 사용하려는 경우에는 검색 제약 조건을 변경합니다.

단계 **5** 변경된 검색을 나중에 다시 사용하려면, 검색 저장, 728 페이지에 설명된 대로 검색을 저장합니다.

단계 **6** **Search(**검색**)**를 클릭합니다.

셸을 통해 쿼리 재정의

시스템 관리자는 Linux 셸 기반 쿼리 관리 도구를 사용해 오래 실행되는 쿼리를 찾아서 중지할 수 있습니다.

쿼리 관리 툴을 사용하면 지정된 기간(분)보다 오래 실행되는 쿼리를 찾아 중지할 수 있습니다. 쿼리를 중지하면 이벤트가 감사 로그 및 시스템 로그에 기록됩니다.

관리자 내부 사용자는 FMC CLI에 액세스할 수 있습니다. CLI 액세스를 허용하는 외부 인증 개체를 사용하는 경우 셸 액세스 필터와 일치하는 사용자는 CLI에도 로그인할 수 있습니다.

참고 웹 인터페이스에 검색 페이지를 열어 두면 쿼리가 중지되지 않습니다. 반환에 오랜 시간이 걸리는 쿼리는 쿼리 실행 중에 전체 시스템 성능에 영향을 미칩니다.

셸 기반 쿼리 관리 구문

장기 쿼리는 다음 구문을 사용하여 관리합니다.

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

표 89: `query_manager` Options(옵션)

옵션	설명
`-h, --help`	간략한 도움말 메시지를 인쇄합니다.
`-l, --list [minutes]`	지정된 기간(분)보다 오래 걸린 모든 쿼리를 나열합니다. 기본적으로, 1분 이상 걸리는 모든 쿼리가 표시됩니다.
`-k, --kill query_id [...]`	전달된 ID가 있는 쿼리를 중단합니다. 이 옵션은 여러 ID를 이용할 수 있습니다.
`--kill-all minutes`	지정된 기간(분)보다 오래 걸린 모든 쿼리를 중단합니다.
`-v, --verbose`	전체 SQL 쿼리를 포함하여 출력을 자세히 표시합니다.

주의 시스템 보안을 위해 Cisco에서는 Linux 셸 사용자를 어플라이언스에서 추가로 설정하지 않도록 권장합니다.

오래 실행되는 쿼리 중지

CLI 액세스 권한이 있는 관리자 사용자 또는 외부 인증된 사용자여야 합니다.

프로시저

단계 **1** `ssh`를 통해 Secure Firewall Management Center에 연결합니다.

단계 **2** CLI `expert` 명령을 사용하여 Linux 셸에 액세스합니다.

단계 **3** 셸 기반 쿼리 관리 구문, 730 페이지에 설명한 구문을 사용하여 `sudo` 아래에서 `query_manager`를 실행합니다.

이벤트 검색 히스토리

기능	버전	세부 사항
많은 필드에서 부분 일치 검색시 이제 와일드 카드가 필요합니다.	6.6	예를 들어 URL을 검색할 때 **example.com**의 모든 변형을 찾으려면 *** example.com***을 사용합니다. 이 동작 변경 사항은 **Analysis(**분석**) > Search(**검색**)** 페이지에서 연결 또는 보안 인텔리전스 이벤트를 검색할 때 적용됩니다. 이 검색 페이지는 다른 페이지의 링크를 통해 액세스할 수도 있습니다. 부분 일치 검색에 와일드 카드가 필요하지 않은 필드에서는 선택적으로 사용할 수 있습니다. 영향을 받는 플랫폼: FMC

29 장

사용자 지정 워크플로

다음 주제에서는 맞춤형 워크플로를 사용하는 방법을 설명합니다.

맞춤형 워크플로 소개

사전 정의된 워크플로와 Cisco에서 제공하는 맞춤형 워크플로가 필요에 부합하지 않을 경우, 맞춤형 워크플로를 생성하고 관리해야 합니다.

맞춤형 워크플로는 조직의 고유한 필요에 맞게 생성하는 워크플로입니다. 맞춤형 워크플로를 생성할 때 워크플로의 기반이 되는 이벤트(또는 데이터베이스 테이블)의 종류를 선택합니다. management center에서 맞춤형 테이블을 맞춤형 워크플로의 기반으로 선택할 수 있습니다. 또한 맞춤형 워크플로에 포함되는 페이지를 선택할 수 있습니다. 맞춤형 워크플로는 드릴다운, 테이블 보기, 호스트 또는 패킷 보기 페이지로 구성될 수 있습니다.

이벤트 평가 프로세스가 변경될 경우 새 필요에 맞게 맞춤형 워크플로를 수정할 수 있습니다. 사전 정의 워크플로는 수정할 수 없습니다.

팁 어떤 이벤트 유형에서도 맞춤형 워크플로를 기본 워크플로로 설정할 수 없습니다.

저장된 맞춤형 워크플로

수정 불가한 사전 정의 워크플로 외에도 management center에는 여러 저장된 맞춤형 워크플로가 있습니다. 이 워크플로 각각은 맞춤형 테이블을 기반으로 하며 수정 가능합니다.

다중 도메인 구축의 경우, 이러한 저장된 워크플로는 Global(전역) 도메인에 속하며 하위 도메인에서는 수정할 수 없습니다.

표 **90:** 저장된 맞춤형 워크플로

워크플로 이름	설명
우선순위 및 분류별 이벤트	이 워크플로는 이벤트와 그 유형을 이벤트 우선순위에 따라 나열하며 각 이벤트의 발생 횟수 카운트도 표시합니다. 이 워크플로는 Intrusion Events(침입 이벤트) 맞춤형 테이블을 기반으로 합니다.
Hosts with Servers Default Workflow(서버 기본 워크플로가 있는 호스트)	이 워크플로를 사용하여 Hosts with Servers(서버가 있는 호스트) 맞춤형 테이블의 기본 정보를 신속하게 볼 수 있습니다. 이 워크플로는 Hosts with Servers(서버가 있는 호스트) 사용자 지정 테이블을 기반으로 합니다.
Server and Host Details(서버 및 호스트 상세정보)	이 워크플로를 사용하여 네트워크에서 어떤 서버가 가장 많이 사용되었는지 그리고 어떤 호스트에서 이 서버를 실행하고 있는지를 확인할 수 있습니다. 이 워크플로는 Hosts with Servers(서버가 있는 호스트) 사용자 지정 테이블을 기반으로 합니다.

맞춤형 워크플로 생성

사전 정의된 워크플로와 Cisco에서 제공하는 맞춤형 워크플로가 필요에 부합하지 않을 경우, 맞춤형 워크플로를 생성해야 합니다.

팁 새 맞춤형 워크플로를 생성하지 않고 다른 어플라이언스에서 맞춤형 워크플로를 내보낸 다음 현재 어플라이언스로 가져올 수 있습니다. 그런 다음 가져온 워크플로를 필요에 맞게 수정할 수 있습니다.

맞춤형 워크플로를 생성할 때는 다음을 수행합니다.

- 워크플로의 소스가 될 테이블 선택
- 워크플로 이름 지정
- 워크플로에 드릴다운 페이지 및 테이블 보기 페이지 추가

워크플로의 각 드릴다운 페이지에 대해 다음을 수행할 수 있습니다.

- 웹 인터페이스에서 페이지의 맨 위에 나타날 이름 지정
- 페이지당 최대 5개의 열 포함
- 기본 정렬 순서 지정, 오름차순 또는 내림차순

일련의 워크플로 페이지에서 임의의 위치에 테이블 보기 페이지를 추가할 수 있습니다. 여기에는 페이지 이름, 정렬 순서, 맞춤형 열 위치와 같은 수정 가능한 속성이 없습니다.

참고 하나 이상의 드릴다운 페이지 또는 이벤트 테이블 보기를 맞춤형 워크플로에 추가해야 합니다.

참고 테이블 유형으로 **Vulnerabilities(**취약성**)**를 선택한 경우, **IP Address(IP** 주소**)**를 테이블 열로 추가하면 맞춤형 워크플로에서 취약성을 볼 때 IP Address 열이 나타나지 않습니다. 단, 검색 기능을 사용하여 특정 IP 주소 또는 주소 영역을 표시하도록 워크플로를 제한하는 경우는 제외합니다.

맞춤형 워크플로의 최종 페이지는 다음 표에서 설명하는 것처럼 워크플로의 기반이 되는 테이블에 따라 달라집니다. 이 최종 페이지는 워크플로 생성 시 기본적으로 추가됩니다.

표 ***91:*** 맞춤형 워크플로의 최종 페이지

이벤트**/**자산 유형	최종 페이지
검색 이벤트	호스트
취약성	취약성 상세정보
서드파티 취약성	호스트
사용자	사용자
보안 침해 지표	호스트 또는 사용자
침입 이벤트	패킷

시스템은 다른 종류의 이벤트(예: 감사 로그, 악성 코드 이벤트)를 기반으로 한 맞춤형 워크플로에는 최종 페이지를 추가하지 않습니다.

연결 데이터를 기반으로 하는 맞춤형 워크플로는 다른 맞춤형 워크플로와 동일하지만, 연결 요약 데이터가 있는 드릴다운 페이지와 연결 데이터 그래프 페이지, 개별 연결 및 테이블 보기 페이지가 있는 드릴다운 페이지를 포함할 수 있습니다.

비 연결 데이터 기반 맞춤형 워크플로 생성

비 연결 데이터를 기반으로 맞춤형 워크플로우를 생성하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**사용자 지정 워크플로**)**을(를) 선택합니다.

단계 **2** **Create Custom Workflow(**맞춤형 워크플로 생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 워크플로의 이름을 입력합니다.

단계 **4** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **5** **Table(**테이블**)** 드롭다운 목록에서 추가할 표를 선택합니다.

단계 **6** 워크플로에 드릴다운 페이지를 하나 이상 추가하려는 경우에는 **Add Page(**페이지 추가**)**를 클릭합니다.

단계 **7** **Page Name(**페이지 이름**)** 필드에 페이지의 이름을 입력합니다.

단계 **8** Column 1에서 정렬 우선순위와 테이블 열을 선택합니다. 이 열은 페이지의 맨 왼쪽 열로 나타납니다.

예제**:**

예를 들어 대상이 된 대상 포트를 표시하는 페이지를 생성하고 그 페이지를 카운트 순으로 정렬하려면, **Sort Priority(**정렬 우선순위**)** 드롭다운 목록에서 **2**를 선택하고 **Field(**필드**)**드롭다운 목록에서 **Destination Port/ICMP Code(**대상 포트**/ICMP** 코드**)**를 선택합니다.

단계 **9** 페이지에 표시할 필드가 모두 지정될 때까지, 포함할 필드를 선택하고 정렬 우선순위를 설정합니다.

단계 **10** 테이블 보기 페이지 워크플로를 추가 하려는 경우 추가 테이블 보기를 클릭 합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

맞춤형 연결 데이터 워크플로 생성

연결 데이터 기반의 맞춤형 워크플로는 다른 맞춤형 워크플로와 비슷하지만, 드릴다운 페이지 및 테이블 보기 페이지뿐 아니라 연결 데이터 그래프 페이지까지 포함할 수 있습니다. 각 페이지 유형을 원하는 개수와 순서로 워크플로에 포함할 수 있습니다. 각 연결 데이터 그래프 페이지는 단일 그래프를 포함하는데, 이는 선 그래프, 막대 그래프 또는 원도표가 될 수 있습니다. 선 그래프와 막대 그래프는 둘 이상의 데이터 집합을 포함할 수 있습니다.

연결 데이터를 기반으로 맞춤형 워크플로우를 생성하려면 관리자 권한이 있어야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**사용자 지정 워크플로**)**을(를) 선택합니다.

단계 **2** **Create Custom Workflow(**맞춤형 워크플로 생성**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 워크플로의 이름을 입력합니다.

단계 **4** 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **5** **Table(**표**)** 드롭다운 목록에서 **Connection Events(**연결 이벤트**)**를 선택합니다.

단계 **6** 워크플로에 드릴다운 페이지를 하나 이상 추가하려는 경우에는 두 가지 방법을 사용할 수 있습니다.

- **Add Page(**페이지 추가**)**를 클릭하여 개별 연결의 데이터를 포함하는 드릴다운 페이지를 추가합니다.
- **Add Summary Page(**요약 페이지 추가**)**를 클릭하여 연결 요약 데이터를 포함하는 드릴다운 페이지를 추가합니다.

단계 **7** **Page Name(**페이지 이름**)** 필드에 페이지의 이름을 입력합니다.

단계 **8** **Column 1**에서 정렬 우선순위와 테이블 열을 선택합니다. 이 열은 페이지의 맨 왼쪽 열로 나타납니다.

단계 **9** 페이지에 표시할 필드가 모두 지정될 때까지, 포함할 필드를 선택하고 정렬 우선순위를 설정합니다.

예제**:**

예를 들어 모니터링되는 네트워크를 통해 전송된 트래픽의 양을 표시하는 페이지를 생성하고 가장 많은 트래픽을 전송한 응답자의 순으로 페이지를 정렬하려면 **Sort Priority(**정렬 우선순위**)** 드롭다운 목록에서 **1**을 선택하고 **Field(**필드**)** 드롭다운 목록에서 **Responder Bytes(**응답자 바이트**)**를 선택합니다.

단계 **10** 워크플로에 그래프 페이지를 하나 이상 추가하려는 경우에는 **Add Graph(**그래프 추가**)**를 클릭합니다.

단계 **11** **Graph Name(**그래프 이름**)** 필드에 페이지의 이름을 입력합니다.

단계 **12** 페이지에 포함하려는 그래프의 유형을 선택합니다.

- 선 그래프(**Line chart(**선형 차트**)** ())
- 막대 그래프(**Bar chart(**막대그래프**)** ())
- 원형 차트(**Pie chart(**원도표**)** ())

단계 **13** 그래프의 X축과 Y축을 선택하여 그래프에 표시할 데이터 종류를 지정합니다.

원도표에서 X축은 독립 변수를, Y축은 종속 변수를 나타냅니다.

단계 **14** 그래프에 포함할 데이터 집합을 선택합니다.

원도표는 하나의 데이터 집합만 포함할 수 있습니다.

단계 **15** 연결 데이터의 테이블 보기를 추가하려는 경우에는 **Add Table View(**테이블 보기 추가**)**를 클릭합니다.

테이블 보기를 구성할 수 없습니다.

단계 **16** **Save(**저장**)**를 클릭합니다.

맞춤형 워크플로 사용 및 관리

워크플로를 표시하는 데 사용하는 방법은 워크플로가 사전 정의 이벤트 테이블 중 하나 또는 맞춤형 테이블을 기반으로 하느냐에 따라 달라집니다.

맞춤형 워크플로가 사전 정의 이벤트 테이블을 기반으로 할 경우 어플라이언스와 함께 제공되는 워크플로에 액세스하는 것과 동일한 방법으로 액세스합니다. 예를 들어 Hosts(호스트) 테이블을 기반으로 하는 맞춤형 워크플로에 액세스하려면 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Hosts(**호스트**)**을(를) 선택합니다. 반대로 맞춤형 워크플로가 맞춤형 테이블을 기반으로 한다면, Custom Tables(맞춤형 테이블) 페이지에서 액세스해야 합니다.

이벤트 평가 프로세스가 변경될 경우 새 필요에 맞게 맞춤형 워크플로를 수정할 수 있습니다. 사전 정의 워크플로는 수정할 수 없습니다.

팁 어떤 이벤트 유형에서도 맞춤형 워크플로를 기본 워크플로로 설정할 수 없습니다.

사전 정의 테이블 기반 맞춤형 워크플로 보기

맞춤형 워크플로우를 보려면 관리자, 유지 보수 또는 보안 분석가 권한이 있어야 합니다.

프로시저

단계 **1** 워크플로 선택, 691 페이지에서 설명한 대로 맞춤형 워크플로의 기반이 되는 테이블에 적합한 메뉴 경로와 옵션을 선택합니다.

단계 **2** 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 현재 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다.

단계 **3** 어떤 이벤트도 발생하지 않으며 워크플로를 시간으로 제한할 수 있다면, 시간 범위 조정이 필요할 수 있습니다. 이벤트 시간 제약 조건, 707 페이지 섹션을 참조하십시오.

맞춤형 테이블 기반 맞춤형 워크플로 보기

맞춤형 테이블을 기반으로 하는 맞춤형 워크플로우를 보려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 워크플로를 표시하며 이러한 워크플로는 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 워크플로도 표시되지만, 이러한 워크플로는 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 워크플로를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**사용자 지정 표**)**를 선택합니다.

단계 **2** 확인할 맞춤형 테이블 옆의 **View(**보기**)** ( )를 클릭하거나 맞춤형 테이블의 이름을 클릭합니다.

단계 **3** 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다.

단계 **4** 어떤 이벤트도 발생하지 않으며 워크플로를 시간으로 제한할 수 있다면, 시간 범위 조정이 필요할 수 있습니다. 이벤트 시간 제약 조건, 707 페이지 섹션을 참조하십시오.

맞춤형 워크플로

맞춤형 워크 플로우를 편집하려면 관리자 또는 보안 분석가 권한이 있어야 합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 워크플로를 표시하며 이러한 워크플로는 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 워크플로도 표시되지만, 이러한 워크플로는 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 워크플로를 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**사용자 지정 워크플로**)**를 선택합니다.

단계 **2** 편집하려는 워크플로 이름 옆의 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 원하는 변경사항을 워크플로에 적용합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

30 장

사용자 지정 표

다음 주제에서는 맞춤형 테이블을 사용하는 방법을 설명합니다.

맞춤형 테이블 소개

시스템이 네트워크에 대한 정보를 수집하면 management center에서 이를 일련의 데이터베이스 테이블에 저장합니다. 워크플로를 사용하여 결과 정보를 볼 경우 management center은(는) 이러한 테이블 중 하나에서 데이터를 가져옵니다. 예를 들어 Count 워크플로의 각 Network Applications(네트워크 애플리케이션) 페이지에 있는 열은 Applications(애플리케이션) 테이블의 필드에서 옵니다.

서로 다른 테이블의 필드를 조합하여 네트워크에서의 활동 분석을 개선할 수 있다고 생각되는 경우 맞춤형 테이블을 생성할 수 있습니다.

사전 정의 테이블 또는 맞춤형 테이블에 대한 맞춤형 워크플로를 생성할 수 있습니다.

사전 정의 맞춤형 테이블

맞춤형 테이블에는 둘 이상의 사전 정의 테이블에서 오는 필드가 포함됩니다. Firepower System에서는 다수의 시스템 정의 맞춤형 테이블을 제공하지만, 사용자는 특정 요구에 맞는 정보만 포함하는 맞춤형 테이블을 추가로 생성할 수 있습니다.

예를 들어 Firepower System에서는 침입 이벤트 데이터를 호스트 데이터와 상호 연결하는 시스템 정의 맞춤형 테이블을 제공하므로, 중요 시스템에 영향을 미치는 이벤트를 검색하고 하나의 워크플로에서 검색 결과를 볼 수 있습니다.

다중 도메인 구축의 경우, 사전 정의된 맞춤형 테이블은 Global(전역) 도메인에 속하며 하위 도메인에서는 수정할 수 없습니다.

다음 표에서는 시스템에서 제공하는 맞춤형 테이블에 대해 설명합니다.

표 **92:** 시스템 정의 맞춤형 테이블

표	설명
서버가 있는 호스트	Hosts(호스트) 및 Servers(서버) 테이블의 필드를 포함하며, 네트워크에서 실행 중인 탐지된 애플리케이션에 대한 정보는 물론 그러한 애플리케이션을 실행하는 호스트에 대한 기본 운영체제 정보도 제공합니다.

가능한 테이블 조합

맞춤형 테이블을 만들 때에는 관련 데이터가 포함된 사전 정의 테이블의 필드를 조합할 수 있습니다. 다음 표에는 새 맞춤형 테이블 생성을 위해 조합할 수 있는 사전 정의 테이블이 나열되어 있습니다. 둘 이상의 사전 정의된 맞춤형 테이블에서 오는 필드를 조합하는 맞춤형 테이블을 생성할 수 있습니다.

표 **93:** 맞춤형 테이블 조합

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
애플리케이션	• 상관관계 이벤트 • 침입 이벤트 • 연결 요약 데이터 • 호스트 속성 • 애플리케이션 세부사항 • 검색 이벤트 • 호스트 • 서버 • 허용 이벤트 나열
상관관계 이벤트	• 애플리케이션 • 호스트 속성 • 호스트
침입 이벤트	• 애플리케이션 • 호스트 속성 • 호스트 • 서버

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
연결 요약 데이터	• 애플리케이션 • 호스트 속성 • 호스트 • 서버
Host(호스트) 보안 침해 지표	• 애플리케이션 • 애플리케이션 세부사항 • 캡처된 파일 • 연결 요약 데이터 • 상관관계 이벤트 • 검색 이벤트 • 호스트 속성 • 호스트 • 침입 이벤트 • 보안 인텔리전스 이벤트 • 서버 • 허용 이벤트 나열
호스트 속성	• 애플리케이션 • 상관관계 이벤트 • 침입 이벤트 • 연결 요약 데이터 • 애플리케이션 세부사항 • 검색 이벤트 • 호스트 • 서버 • 허용 이벤트 나열

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
애플리케이션 세부사항	• 애플리케이션 • 호스트 속성 • 호스트
검색 이벤트	• 애플리케이션 • 호스트 속성 • 호스트
보안 인텔리전스 이벤트	• 애플리케이션 • 호스트 속성 • 호스트 • 서버
호스트	• 애플리케이션 • 상관관계 이벤트 • 침입 이벤트 • 연결 요약 데이터 • 호스트 속성 • 애플리케이션 세부사항 • 검색 이벤트 • 서버 • 허용 이벤트 나열
서버	• 애플리케이션 • 침입 이벤트 • 연결 요약 데이터 • 호스트 속성 • 호스트

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
허용 이벤트 나열	• 애플리케이션 • 호스트 속성 • 호스트

때때로 한 테이블의 한 필드가 또 다른 테이블의 둘 이상의 필드에 매핑됩니다.

새 맞춤형 테이블을 생성하면 테이블의 모든 열을 표시하는 기본 워크플로가 자동으로 생성됩니다. 또한 사전 정의 테이블과 마찬가지로, 네트워크 분석에서 사용할 데이터에 대한 맞춤형 테이블을 검색할 수 있습니다. 사전 정의 테이블과 마찬가지로, 맞춤형 테이블을 기반으로 보고서를 생성할 수 있습니다.

사용자 정의 맞춤형 테이블

팁 새 맞춤형 테이블을 생성하는 대신, 다른 management center에서 맞춤형 테이블을 내보낸 다음 현재 management center로 가져올 수 있습니다.

사용자 지정 테이블을 생성하려면 사전 정의 테이블 중 어디에 사용자 지정 테이블에 포함할 필드가 포함되어 있는지를 확인해야 합니다. 그런 다음, 포함하고자 하는 필드를 선택하고 필요한 경우 공통 필드에 대한 필드 매핑을 구성할 수 있습니다.

팁 Hosts(호스트) 테이블과 관련된 데이터에서는 하나의 특정 IP 주소보다는 한 호스트의 모든 IP 주소와 연결된 데이터를 볼 수 있습니다.

예를 들어 Correlation Events(상관관계 이벤트) 테이블과 Hosts(호스트) 테이블의 필드를 조합하는 맞춤형 테이블이 있다고 가정해보겠습니다. 이 맞춤형 테이블을 사용하면 상관관계 정책의 위반과 관련된 호스트에 대한 자세한 정보를 얻을 수 있습니다. Correlation Events(상관관계 이벤트) 테이블의 소스 IP 주소 또는 목적지 IP 주소와 일치하는 Hosts(호스트) 테이블의 데이터를 표시할지 여부를 결정해야 합니다.

이 맞춤형 테이블에 대한 이벤트를 테이블 보기로 보면 한 행에 하나씩 상관관계 이벤트가 표시됩니다. 다음 정보를 포함하도록 맞춤형 테이블을 설정할 수 있습니다.

- 이벤트가 생성된 날짜 및 시간
- 위반된 상관관계 정책의 이름
- 위반을 트리거한 규칙의 이름
- 상관관계 이벤트와 관련된 소스 또는 시작 호스트와 연결된 IP 주소
- 소스 호스트의 NetBIOS 이름

- 소스 호스트가 실행 중인 운영체제 및 버전
- 소스 호스트 중요도

팁 대상 또는 응답 호스트에 대한 동일한 정보를 표시하는 유사한 맞춤형 테이블을 생성할 수 있습니다.

맞춤형 테이블 생성

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**사용자 지정 표**)**을(를) 선택합니다.

단계 **2** **Create Custom Table(**맞춤형 테이블 생성**)**을 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 맞춤형 테이블의 이름을 입력합니다.

예제**:**

예를 들어 `Correlation Events with Host Information (Src IP)`을 입력할 수 있습니다.

단계 **4** **Tables(**테이블**)** 드롭다운 목록에서 **Correlation Events(**상관관계 이벤트**)**를 선택합니다.

단계 **5** **Fields(**필드**)**에서 **Time(**시간**)**을 선택하고 **Add(**추가**)**를 클릭하여 상관관계 이벤트가 생성된 날짜와 시간을 추가합니다.

단계 **6** 5단계를 반복하여 **Policy(**정책**)** 및 **Rule(**규칙**)** 필드를 추가합니다.

팁 여러 필드를 선택하려면 Ctrl 또는 Shift 키를 누른 상태에서 클릭합니다. 클릭하고 드래그하여 인접한 여러 값을 선택할 수도 있습니다. 그러나 테이블과 연결된 이벤트의 테이블 보기에 필드가 나타나는 순서를 지정하려면, 필드를 한 번에 하나씩 추가해야 합니다.

단계 **7** **Tables(**테이블**)** 드롭다운 목록에서 **Hosts(**호스트**)**를 선택합니다.

단계 **8** 맞춤형 테이블에 **IP Address(IP** 주소**)**, **NetBIOS Name(NetBIOS** 이름**)**, **OS Name(**운영체제 이름**)**, **OS Version(**운영체제 버전**)** 및 **Host Criticality(**호스트 중요도**)** 필드를 추가합니다.

단계 **9** **Common Fields(**공통 필드**)** 아래의 **Correlation Events(**상관관계 이벤트**)** 옆에 있는 **Source IP(**소스 **IP)**를 선택합니다.

상관관계 이벤트와 관련된 소스 또는 시작 호스트에 대해 8단계에서 선택한 호스트 정보를 표시하도록 맞춤형 테이블이 구성됩니다.

팁 이 절차를 수행하되 **Source IP(**소스 **IP)** 대신 **Destination IP(**목적지 **IP)**를 선택하여, 상관관계 이벤트와 관련된 대상 또는 응답 호스트에 대한 자세한 호스트 정보를 표시하는 맞춤형 테이블을 생성할 수 있습니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

맞춤형 테이블 수정

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 테이블을 표시하며 이러한 테이블은 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 테이블도 표시되지만, 이러한 테이블은 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 테이블을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**사용자 지정 표**)**를 선택합니다.

단계 **2** 편집하려는 테이블 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 선택적으로, 제거하려는 필드 옆에 있는 **Delete(**삭제**)** ( )을 클릭하여 테이블에서 필드를 제거합니다.

참고 보고서에 현재 사용되고 있는 필드를 삭제하는 경우, 해당 보고서에서 해당 필드를 사용하는 섹션을 제거할 것인지 묻는 메시지가 표시됩니다.

단계 **4** 필요에 따라 다른 변경사항을 적용합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

맞춤형 테이블 삭제

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 맞춤형 테이블을 표시하며, 이러한 테이블은 삭제할 수 있습니다. 상위 도메인에서 생성된 맞춤형 테이블도 표시되지만, 이러한 테이블은 삭제할 수 없습니다. 하위 도메인에서 생성된 맞춤형 테이블을 삭제하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**사용자 지정 표**)**을(를) 선택합니다.

단계 **2** 삭제하고자 하는 맞춤형 테이블 옆에 있는 아이콘(**Delete(**삭제**)** ( ))을 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

맞춤형 테이블 기반 워크플로 보기

맞춤형 테이블을 생성하면 시스템은 자동으로 이에 대한 기본 워크플로를 생성합니다. 이 워크플로의 첫 번째 페이지에는 이벤트의 테이블 보기가 표시됩니다. 맞춤형 테이블에 침입 이벤트를 포함하면 워크플로의 두 번째 페이지는 패킷 보기 페이지가 됩니다. 그렇지 않으면 워크플로의 두 번째 페이지는 호스트 페이지가 됩니다. 맞춤형 테이블을 기반으로 고유한 맞춤형 워크플로를 생성할 수도 있습니다.

팁 맞춤형 테이블을 기반으로 맞춤형 워크플로를 만드는 경우이를 해당 테이블의 기본 워크플로로 지정할 수 있습니다.

사전 정의 테이블을 기반으로 이벤트 보기에 대해 사용하는 맞춤형 테이블에서 이벤트를 보려면 이 방법을 사용할 수 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 테이블을 표시하며 이러한 테이블은 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 테이블도 표시되지만, 이러한 테이블은 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 테이블을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**사용자 지정 표**)**을(를) 선택합니다.

단계 **2** 확인할 워크플로와 관련된 맞춤형 테이블 옆에 있는 **View(**보기**)** ( )을 클릭합니다.

맞춤형 테이블 검색

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 테이블을 표시하며 이러한 테이블은 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 테이블도 표시되지만, 이러한 테이블은 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 테이블을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**사용자 지정 표**)**를 선택합니다.

단계 **2** 검색할 맞춤형 테이블 옆에 있는 **View(**보기**)** ( )을 클릭합니다.

팁 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다.

단계 **3** **Search(**검색**)**를 클릭합니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트 또는 데이터를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

단계 **4** 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다.

팁 검색 기준으로 개체를 사용하려면 검색 필드 옆에 있는 **Object(**개체**)**(+)을 클릭합니다.

단계 **5** 선택적으로, 검색을 저장하려면 **Private(**비공개**)** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 마십시오.

팁 맞춤형 사용자 역할을 위한 데이터 제한으로 검색을 사용하려면 반드시 비공개 검색으로 저장해야 합니다.

단계 **6** 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음과 같은 옵션이 있습니다.

- 검색 기준을 저장하려면 **Save(**저장**)**를 클릭합니다. **Private(**비공개**)** 확인란을 선택해야 검색이 계정에 표시됩니다.
- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New(**신규로 저장**)**를 클릭합니다. **Private(**비공개**)** 확인란을 선택해야 검색이 저장되고 계정에 표시됩니다.

단계 **7** 검색을 시작하려면 **Search(**검색**)**를 클릭합니다.

검색 결과가 현재 시간과 범위로 제한되어(적용 가능한 경우) 맞춤형 테이블에 대한 기본 워크플로에 나타납니다.

맞춤형 테이블 기록

기능	버전	세부 사항
맞춤형 테이블의 연결 이벤트 지원은 삭제되었습니다.	6.6	이제 연결 이벤트가 포함된 맞춤형 테이블을 생성할 수 없습니다. 6.6 버전으로 업그레이드한 경우: 연결 이벤트가 있는 기존 테이블은 사용되지 않음으로 표시되며 데이터가 표시되지 않고 테이블을 내보내거나 편집할 수 없습니다. 기존 보고서, 맞춤형 워크플로, 대시보드가 사용되지 않는 테이블을 포함할 수 있으며 사용자는 이를 검토할 수 있습니다. 수정된 화면: **Analysis(**분석**) > Advanced(**고급**) > Custom Tables(**맞춤형 테이블**)**과 맞춤형 테이블 추가 및 편집 페이지 영향을 받는 플랫폼: FMC

VIII 부

이벤트 및 자산

31 장

연결 로깅

다음 주제에서는 모니터링하는 네트워크 상의 호스트가 실행한 연결을 기록하도록 Firepower System을 설정하는 방법을 설명합니다.

연결 로깅 정보

시스템은 자신의 매니지드 디바이스가 탐지한 연결의 로그를 생성할 수 있습니다. 이러한 로그를 연결 이벤트라고 합니다. 규칙 및 정책의 설정은 로깅할 연결의 종류, 로깅을 실행할 시기, 데이터를 저장할 위치를 세부적으로 제어할 수 있도록 합니다. *security-related connection events(*보안 관련 연결 이벤트*)*라는 특수한 연결 이벤트는 평판 기반 Security Intelligence(보안 인텔리전스) 기능이 차단한 연결을 나타냅니다.

연결 이벤트에는 탐지된 세션에 관한 데이터가 포함되어 있습니다. 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 사유에 대한 메타데이터: 어떤 설정이 트래픽을 처리했는지, 연결이 허용 또는 차단되었는지, 암호화 및 해독된 연결에 대한 상세정보 등

조직의 보안 및 컴플라이언스 요구 사항에 따라 연결을 로깅해야 합니다. 연결 로깅을 설정할 때는 시스템이 여러 가지 이유로 연결을 로깅할 수 있으며, 따라서 한 곳의 로깅을 비활성화해도 일치하는 연결이 로깅되지 않는 것은 아님을 유의하십시오.

연결 이벤트에 있는 정보는 트래픽 특성, 연결을 마지막으로 처리한 설정 등의 다양한 요소에 따라 달라집니다.

참고 내보낸 NetFlow 기록에서 생성한 연결 데이터를 이용해, 매니지드 디바이스가 수집한 연결 로그를 보완할 수 있습니다. 이는 매니지드 디바이스가 모니터링할 수 없는 네트워크에서 NetFlow 지원 라우터 또는 기타 디바이스를 구축한 경우에 특히 유용합니다.

항상 로깅되는 연결

연결 이벤트 스토리지를 비활성화하지 않는 한, 시스템은 다른 로깅 설정과 관계없이 다음의 연결 종료 이벤트를 management center 데이터베이스에 자동으로 저장합니다.

침입과 연관된 연결

시스템은 연결이 액세스 제어 정책의 기본 작업에 의해 처리되지 않는 한, 침입 이벤트와 연관된 연결을 자동으로 로깅합니다.

액세스 제어 기본 작업과 관련된 침입 정책이 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.

그러나 기본 작업에 대한 연결 시작 로깅을 활성화하면, 시스템은 연결의 시작을 로깅하는 것 이외에도 관련 침입 정책이 작동을 이끌어낼 때 연결 종료를 분명히 로깅합니다.

파일 및 악성코드 이벤트와 연관된 연결

시스템은 파일 및 악성코드 이벤트와 연관된 연결을 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.

지능형 애플리케이션 우회와 연관된 연결

시스템은 우회했거나 우회했을 가능성이 있는 IAB 관련 연결을 자동으로 로깅합니다.

모니터링되는 연결

트래픽이 다른 어느 규칙과도 일치하지 않고 기본 작업 로깅을 사용자가 활성화하지 않은 경우에도, 시스템은 모니터링되는 트래픽의 연결 종료를 로깅합니다. 자세한 내용은 모니터링된 연결에 대한 로깅, 756 페이지를 참고하십시오.

로깅할 수 있는 기타 연결

중요한 연결만 로깅하려면 규칙별로 연결 로깅을 활성화합니다. 규칙에 대한 연결 로깅을 활성화할 경우, 시스템은 해당 규칙에서 처리하는 모든 연결을 로깅합니다.

정책 기본 작업이 처리하는 연결을 로깅할 수도 있습니다. 규칙 또는 기본 작업(액세스 제어의 경우, 규칙의 검사 설정)에 따라 로깅 옵션이 달라집니다.

사전 필터 정책**:** 규칙 및 기본 작업

사전 필터 정책으로 fastpath 또는 차단하는 연결(전체 일반 텍스트, 통과 터널 포함)을 로깅할 수 있습니다.

사전 필터링은 외부 헤더 기준을 사용하여 트래픽을 처리합니다. 사용자가 로깅하는 터널의 경우, 연결 이벤트에는 외부의 캡슐화 헤더의 정보가 포함됩니다.

추가 분석 대상 트래픽의 경우, 사전 필터 정책에서 로깅이 비활성화되지만 일치하는 연결은 다른 설정에 의해 계속 로깅될 수 있습니다. 시스템은 내부 헤더를 사용하여 모든 추가 분석을 수행합니다. 즉, 시스템은 허용되는 터널 내의 각 연결을 독립적으로 처리하고 로깅합니다.

암호 해독 정책**:** 규칙 및 기본 작업

암호 해독 규칙 또는 암호 해독 정책 기본 작업과 일치하는 연결을 로깅할 수 있습니다.

차단된 연결의 경우 시스템에서 즉시 세션을 종료하고 이벤트를 생성합니다. 모니터링된 연결 및 액세스 제어 규칙으로 전달하는 연결의 경우 시스템에서 세션 종료 시 이벤트를 생성합니다.

액세스 제어 정책**:** 보안 인텔리전스 결정

평판 기능 보안 인텔리전스 기능에 의해 연결이 차단될 때마다 해당 연결을 로깅할 수 있습니다.

원한다면 보안 인텔리전스 필터링에 모니터 한정 설정을 사용할 수 있으며, 이는 수동 구축에서 권장됩니다. 이를 통해 시스템은 차단되었을 수도 있지만 여전히 일치를 로깅하는 연결을 추가로 분석할 수 있습니다. 보안 인텔리전스 모니터링을 사용하면 또한 사용자가 보안 인텔리전스 정보를 사용하여 트래픽 프로파일을 작성할 수 있습니다.

보안 인텔리전스 필터링의 결과로 연결 이벤트를 로깅할 때 시스템은 일치하는 보안 인텔리전스 이벤트도 로깅합니다. 이 이벤트는 사용자가 별도로 보고 분석할 수 있는 특수한 연결 이벤트이며 별도로 저장되고 잘립니다. 연결에서 일치하는 IP 주소를 식별할 수 있도록 **Analysis(**분석**)** > **Connections(**연결**)** 메뉴 아래 페이지의 테이블에서 차단된 IP 주소 옆의 호스트 아이콘과 모니터링되는 IP 주소 옆의 호스트 아이콘은 약간 다르게 보입니다.

액세스 제어 정책**:** 규칙 및 기본 작업

액세스 제어 규칙 또는 액세스 제어 정책 기본 작업과 일치하는 연결을 로깅할 수 있습니다.

관련 항목

규칙 및 정책 작업이 로깅에 미치는 영향, 756 페이지

규칙 및 정책 작업이 로깅에 미치는 영향

연결 이벤트에는 어느 구성이 트래픽을 처리했는지를 포함하여 연결이 로깅된 이유에 관한 메타데이터가 포함됩니다. 연결 로깅, 규칙 작업, 정책 기본 작업을 구성할 수 있는 경우, 시스템이 일치하는 트래픽을 검사하고 처리하는 방법뿐 아니라 일치하는 트래픽에 대한 상세정보를 로깅할 수 있는 시기와 방법도 결정하십시오.

관련 항목

연결 및 보안 관련 연결 이벤트 필드, 773 페이지

빠른 경로 연결에 대한 로깅

사전 필터 정책의 다음 규칙 및 작업과 일치하는 트래픽을 포함하는, 단축 경로 지정 및 암호화되지 않은 터널을 로깅할 수 있습니다:

- 터널 규칙-**Fastpath(**단축 경로**)** 작업(외부 세션 로깅)
- 사전 필터 규칙-**Fastpath(**단축 경로**)** 작업

단축 경로 지정한 트래픽은 남은 액세스 컨트롤 및 QoS를 우회하며, 따라서 단축 경로 지정한 연결의 연결 이벤트는 제한된 정보를 포함합니다.

모니터링된 연결에 대한 로깅

트래픽이 다른 어느 규칙과도 일치하지 않고 기본 작업 로깅을 사용자가 활성화하지 않은 경우에도 시스템은 항상 다음 구성과 일치하는 트래픽의 연결 종료를 로깅합니다.

- 보안 인텔리전스 — 모니터링(또한 보안 인텔리전스도 생성)하도록 설정된 차단 목록
- SSL 규칙 — 모니터링 작업
- 액세스 제어 규칙 — 모니터링 작업

시스템은 단일 연결이 모니터 규칙과 일치할 때마다 별도의 이벤트를 생성하지 않습니다. 단일 연결이 여러 모니터 규칙과 일치할 수 있으므로 각 연결 이벤트는 일치하는 첫 번째 SSL 모니터 규칙뿐 아니라 연결과 일치하는 처음 8개의 모니터 액세스 제어 규칙에 대한 정보를 포함하고 표시합니다.

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

다음 규칙 및 작업과 일치하는 트래픽을 포함하는 신뢰할 수 있는 연결의 시작과 종료를 로깅할 수 있습니다.

- 액세스 제어 규칙 — 신뢰 작업
- 액세스 제어 기본 작업 — 모든 트래픽 신뢰

참고 신뢰할 수 있는 연결을 로깅할 수 있더라도 로깅하지 않는 것이 좋습니다. 신뢰할 수 있는 연결은 심층 검사 또는 검색 대상이 아니므로 신뢰할 수 있는 연결 이벤트에는 제한된 정보가 포함되어 있기 때문입니다.

첫 번째 패킷의 신뢰 규칙에 의해 탐지된 TCP 연결은 연결 종료 이벤트만 생성합니다. 시스템에서는 최종 세션 패킷이 끝난 지 한 시간 후에 이벤트를 생성합니다.

차단된 연결에 대한 로깅

다음 규칙 및 작업과 일치하는 트래픽을 포함하는 차단된 연결을 로깅할 수 있습니다.

- 터널 규칙 — 차단
- 사전 필터 규칙 — 차단
- 사전 필터 기본 작업 — 모든 터널 트래픽 차단
- 보안 인텔리전스 - 모니터링(보안 인텔리전스 이벤트도 생성)하도록 설정되지 않은 차단 목록
- 암호 해독 규칙—차단 및 차단 후 재설정
- SSL 기본 작업 — 차단 및 차단 후 재설정
- 액세스 제어 규칙 — 차단, 차단 후 재설정, 인터랙티브 차단
- 액세스 제어 기본 작업 — 모든 트래픽 차단

인라인이 구축된(즉, 라우팅, 스위칭 또는 투명 인터페이스 혹은 인라인 인터페이스 페어링을 사용하는) 디바이스만 트래픽을 차단할 수 있습니다. 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에, 시스템은 각 차단된 연결에 대한 여러 연결 시작 이벤트를 보고할 수 있습니다.

주의 DoS(서비스 거부) 공격 중에 차단된 TCP 연결을 로깅하는 경우 시스템 성능에 영향을 미칠 수 있으며, 데이터베이스가 유사한 다수의 이벤트로 가득 찰 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.

차단된 연결의 연결 시작 또는 종료 로깅

차단된 연결을 로깅할 때 그 로깅 방식은 연결이 차단된 이유에 따라 달라집니다. 연결 로그를 기반으로 상관관계 규칙을 구성할 때 이 점을 기억해야 합니다.

- 암호화된 트래픽을 차단하는 암호 해독 규칙 및 암호 해독 정책 기본 작업의 경우 연결 종료 이벤트가 로깅됩니다. 이는 세션의 첫 번째 패킷을 사용하여 연결의 암호화 여부를 확인할 수 없기 때문입니다.
- 다른 차단 작업은 연결 시작 이벤트가 로깅됩니다. 일치하는 트래픽은 추가 검사 없이 거부됩니다.

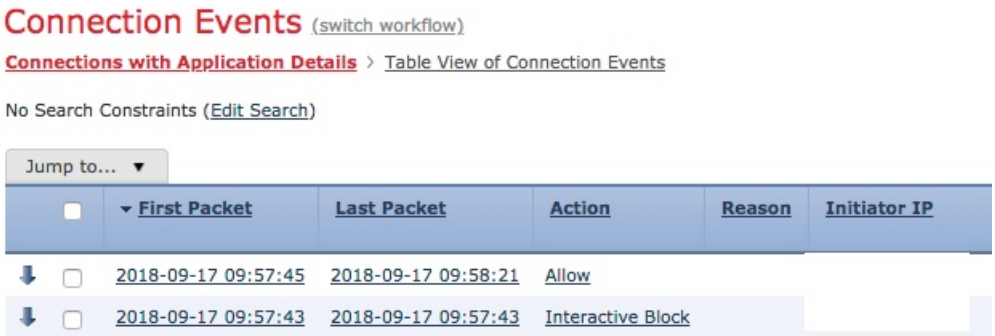
우회된 인터랙티브 차단 로깅

사용자가 금지된 웹사이트로 이동할 때 경고 페이지가 표시되도록 하는 인터랙티브 차단 액세스 제어 규칙을 사용하여 연결 종료 로깅을 구성할 수 있습니다. 이는 사용자가 경고 페이지를 클릭할 경우, 이 연결은 시스템이 모니터링 및 로깅할 수 있는 새롭게 허용된 연결로 간주되기 때문입니다.

따라서 인터랙티브 차단 또는 인터랙티브 차단 후 재설정 규칙과 일치하는 패킷의 경우, 시스템은 다음 연결 이벤트를 생성할 수 있습니다.

- 사용자 요구가 초기에 차단되고 경고 페이지가 표시되는 연결 시작 이벤트. 이 이벤트에는 인터랙티브 차단 또는 인터랙티브 차단 후 재설정이라는 연결된 작업이 있습니다.
- 사용자가 경고 페이지를 통해 클릭하고 원래 요청된 페이지를 로드하는 경우, 다중 연결 시작 또는 종료 이벤트. 이 이벤트에는 허용 및 사용자 우회의 이유라는 연결된 작업이 있습니다.

  다음 그림은 허용 다음의 인터랙티브 차단의 예를 보여줍니다.



허용된 연결에 대한 로깅

다음 규칙 및 작업과 일치하는 트래픽을 포함하 허용된 연결을 로깅할 수 있습니다.

- SSL 규칙 —**Decrypt(**암호 해독**)** 작업
- SSL 규칙 —**Do not decrypt(**암호 해독 안 함**)** 작업
- SSL 기본 작업—**Do not decrypt(**암호 해독 안 함**)**
- 액세스 제어 규칙—**Allow(**허용**)** 작업
- 액세스 제어 기본 작업 —**Network Discovery Only(**네트워크 검색 전용**)** 및 침입 방지 옵션

이러한 구성에 대한 로깅을 활성화하면 연결이 기록되며 다음 단계인 검사 및 트래픽 처리를 허가(또는 지정)합니다. SSL 로깅 시 항상 연결이 종료되며, 액세스 제어 구성에서 연결 시작 로깅을 다시 할 수 있습니다.

터널 및 사전 필터 규칙의 분석 작업도 액세스 제어를 통해 연결이 계속되도록 허용하지만 이 작업이 있는 규칙의 경우, 로깅이 비활성화됩니다. 일치하는 연결은 다른 구성에 의해 계속 로깅될 수 있습니다. 허용되는 터널에는 개별적으로 평가 및 로깅되는 캡슐화된 세션이 있을 수 있습니다.

액세스 제어 규칙 또는 기본 작업을 사용하여 트래픽을 허용하는 경우, 연결된 침입 정책을 사용하여 트래픽을 추가 검사하고 침입을 차단할 수 있습니다. 액세스 제어 규칙의 경우, 파일 정책을 사용하

여 악성코드를 비롯한 금지된 파일을 탐지하고 차단할 수도 있습니다. 연결 이벤트 스토리지를 비활성화하지 않으면 시스템은 침입, 파일, 악성코드 이벤트에 연결된 허용되는 연결 대부분을 자동으로 로깅합니다. 자세한 내용은 항상 로깅되는 연결, 754 페이지를 참조하십시오.

암호화된 페이로드와의 연결은 심층 검사 대상이 아니므로 암호화된 연결의 연결 이벤트에는 제한된 정보가 포함되어 있습니다.

허용된 연결에 대한 파일 및 악성코드 이벤트 로깅

파일 정책이 파일을 탐지하거나 차단하면 다음 이벤트 중 하나를 management center 데이터베이스에 로깅합니다.

- 파일 이벤트 - 악성코드 파일을 포함하여 탐지되거나 차단된 파일을 나타냅니다.
- 악성코드 이벤트 - 탐지되거나 차단된 악성코드 파일만 나타냅니다.
- 회귀적 악성코드 이벤트 - 이전에 탐지된 파일에 대한 악성코드 속성이 변경되는 경우 생성됩니다.

액세스 제어 규칙마다 이 로깅을 비활성화할 수 있습니다. 파일 및 악성코드 이벤트 스토리지를 완전히 비활성화할 수도 있습니다.

참고 파일 및 악성코드 이벤트 로깅 활성화를 유지하는 것이 좋습니다.

연결 시작 또는 종료 로깅

연결은 시작 또는 종료 시에 로깅할 수 있으며, 차단된 트래픽의 경우에는 다음 예외가 적용됩니다.

- 차단된 트래픽 - 차단된 트래픽은 추가 검사 없이 즉시 거부되기 때문에, 일반적으로는 차단된 트래픽의 연결 시작 이벤트만 로깅할 수 있습니다. 로깅할 고유 연결 종료는 존재하지 않습니다.
- 차단된 암호화된 트래픽 - 암호 해독 정책에서 연결 로깅을 활성화하면 연결 시작이 아닌 연결 종료가 로깅됩니다. 이는 시스템에서 세션의 첫 번째 패킷을 사용하여 연결의 암호화 여부를 확인할 수 없고 따라서 즉시 암호화 세션을 차단할 수 없기 때문입니다.

성능을 최적화하려면, 연결의 시작 또는 종료를 로깅하시기 바랍니다. 동시에 하는 것은 안됩니다. 어떤 이유로든 연결을 모니터링하면 반드시 연결 종료가 로깅됩니다. 차단되지 않은 단일 연결의 경우 연결 종료 이벤트는 연결 시작 이벤트의 모든 정보 및 세션 과정에서 수집된 정보를 포함합니다.

다음 표에서는 연결 시작 및 연결 종료 이벤트의 차이점과 각 로깅의 장점을 설명합니다.

표 *94:* 연결 시작 이벤트와 연결 종료 이벤트 비교

	연결 시작 이벤트	연결 종료 이벤트
생성 가능 대상	연결 시작이 탐지될 때(또는 애플리케이션이나 URL 식별에 따라 이벤트가 생성되는 경우 처음 몇 개의 패킷 이후에).	시스템이 다음을 수행하는 경우 • 연결 차단을 탐지하는 경우 • 일정 시간이 지난 후 연결 종료를 탐지하 우 • 메모리 제약 조건 때문에 더 이상 세션을 없는 경우
로깅 가능 대상	암호 해독 정책에 의해 차단된 연결을 제외한 모든 연결	대부분의 연결.
포함 대상	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 세션 기간에 검사하여 확인한 정보(예: 총 데이터 전송량, 지막 패킷의 타임스탬프).
유용한 경우	다음을 로깅하려는 경우 • 차단된 연결. • 연결 종료 정보가 사용자에게 상관 없기 때문에 연결의 시작 한정.	다음을 원하는 경우 • 암호 해독 정책에 의해 처리된 암호화된 록합니다. • 세션 기간 동안 수집된 정보에 관한 모든 세 분석 작업을 수행하거나, 해당 정보를 상호 규칙을 이끌어내려는 경우. • 연결 개요(집계된 연결 데이터)를 살펴보 형식으로 연결 데이터를 살펴보기 트래 일을 만들고 사용하려는 경우.

Secure Firewall Management Center 대 외부 로깅

연결 및 Security Intelligence(보안 인텔리전스) 이벤트 로그를 management center에 저장하는 경우 시스템의 보고, 분석, 데이터 상관관계 기능을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- 대시보드 및 컨텍스트 탐색기에서는 시스템에서 로깅한 연결을 그래픽 화면에서 한눈에 볼 수 있습니다.
- 이벤트 보기(Analysis(분석) 메뉴에서 사용할 수 있는 대부분의 옵션)는 시스템이 로깅한 연결에 대한 상세정보를 제공하며, 이러한 정보는 그래프 또는 표 형식 포맷으로 표시하거나 보고서로 요약할 수 있습니다.
- 트래픽 프로파일에서는 정상적인 네트워크 트래픽에 대한 프로파일을 생성하는 데 연결 데이터를 사용합니다. 그런 다음 이 프로파일을 비정상적인 동작을 탐지하고 추적하는 데 기준으로 사용할 수 있습니다.

- 상관관계 정책에서는 특정 유형의 연결 또는 트래픽 프로파일 변경에 대한 이벤트를 생성하고 응답(예: 알림, 외부 교정)을 트리거할 수 있습니다.

management center에서 저장할 수 있는 이벤트 숫자는 모델에 따라 달라집니다.

참고 이 기능을 사용하려면 반드시 연결을 (대부분의 경우에는 연결 시작이 아닌 연결 종료를) 로깅해야 합니다. 따라서 중요한 연결, 즉 로깅된 침입, 금지된 파일, 악성코드와 관련된 연결은 자동으로 로깅됩니다.

다음을 사용하여 외부 시스템 로그나 SNMP 트랩 서버 또는 다른 외부 툴에 이벤트를 로깅할 수도 있습니다.

- 모든 디바이스에서 외부 로깅:

  설정한 연결은 경고 응답이라고 합니다.

- threat defense 디바이스에서 외부 로깅:

  Cisco Secure Firewall Management Center 디바이스 구성 가이드의 시스템 로그 구성 정보 및 *SNMP* 트랩 구성을 참고하십시오.

- 외부 로깅과 관련된 추가 옵션:

  외부 툴을 사용하여 이벤트 분석, 641 페이지의 내용을 참조하십시오.

관련 항목

Secure Firewall Management Center 알림 응답, 569 페이지

연결 로깅 제한사항

다음 항목은 로깅할 수 없음:

- 일반 텍스트의 외부 세션, 캡슐화된 연결이 액세스 제어로 검사되는 통과 터널
- 3방향 핸드셰이크가 완료되지 않은 경우의 TCP 연결입니다.

  이러한 연결은 실행 시 Firepower 구축에 대한 서비스 거부 공격의 기회를 제공할 것으로 로깅되지는 않습니다.

  그러나 다음 해결 방법을 사용하여 실패한 연결을 모니터링하거나 디버깅할 수는 있습니다.

  - 명령줄 인터페이스에서 **show asp drops** 사용 명령을 사용합니다.
  - 패킷 캡처 기능을 사용하면 이러한 연결에 대한 상세정보를 얻을 수 있습니다. 패킷 캡처 개요, 457 페이지 및 하위 항목을 참조하십시오.

연결 이벤트에 있어야 할 정보가 존재하지 않는다면, 연결 이벤트 필드 채우기 요구 사항, 793 페이지 및 연결 이벤트 필드에서 제공되는 정보, 795 페이지 섹션을 참조하십시오.

이벤트가 이벤트 뷰어에 표시되는 경우

다음 내용은 모든 유형의 이벤트에 적용됩니다.

- Analysis(분석) 메뉴의 페이지를 찾는 경우에는 페이지를 새로고침해야 새 이벤트가 표시됩니다.
- 일반적으로 이벤트는 트래픽이 탐지된 시점에서 몇 초 이내에 확인할 수 있습니다. 그러나 외부의 과도한 트래픽 조건, 낮은 대역폭 네트워크에서 많은 디바이스를 관리하는 FMC, 이벤트 백업 등의 작업 중에 이벤트 처리가 일시 중지되는 등의 상황에서는 임의 지연이 발생할 수 있습니다.
- 정의된 규칙에 따라 로깅된 모든 연결 이벤트가 이벤트 보기에 나타납니다. 연결 이벤트의 통합 로깅에는 이벤트를 필터링하는 옵션을 사용할 수 없습니다.

연결 로깅 모범 사례

로깅하려는 연결만 로깅하려면 다음 모범 사례를 사용하십시오.

중요한 연결만 로깅하려면 액세스 제어 규칙별로 연결 로깅을 활성화합니다.

항상 로깅되는 연결

시스템이 자동으로 다음을 로깅합니다.

- 탐지된 파일, 악성코드, 침입, Intelligent Application Bypass(IAB)와 관련된 일부 연결.

  자세한 내용은 항상 로깅되는 연결, 754 페이지를 참고하십시오.

- 모니터링되는 연결.

  자세한 내용은 모니터링된 연결에 대한 로깅, 756 페이지를 참고하십시오.

로깅하지 않을 연결

다음에 대한 로깅을 활성화하지 마십시오.

- 신뢰 작업이 포함된 액세스 제어 규칙.

  신뢰할 수 있는 연결은 심층 검사 또는 검색 대상이 아니므로 신뢰할 수 있는 연결 이벤트에는 제한된 정보가 포함되어 있습니다.

- 수동 구축에서 차단 규칙에 대한 로깅을 활성화하지 마십시오. 디바이스가 인라인으로 구축되었다면 시스템이 차단했을 연결을 로깅하려면 차단 규칙 대신 모니터링 규칙을 사용합니다.

  인라인이 구축된(즉, 라우팅, 스위칭 또는 투명 인터페이스 혹은 인라인 인터페이스 페어링을 사용하는) 디바이스만 트래픽을 차단할 수 있습니다. 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에, 시스템은 각 차단된 연결에 대한 여러 연결 시작 이벤트를 보고할 수 있습니다.

- 관심이 없는 트래픽. 예는 다음과 같습니다.
  - 신뢰할 수 있는 DNS 호스트에 대한 DNS 요청과 같은 허용되는 특정 트래픽.

- 서비스 솔루션과 관련이 없는 인프라 트래픽.

(앞서 언급했듯이 이 트래픽에서 위협을 계속 모니터링할 수 있습니다.)

항상 로깅되는 연결, 754 페이지에서 설명한 것처럼 위 항목에 대한 로깅을 비활성화하더라도 침입 이벤트, 악성코드, IAB는 여전히 로깅됩니다.

다른 곳에서 로깅되는 것은 로깅하지 마십시오**.**

다른 디바이스 또는 서비스가 네트워크 세그먼트의 연결 데이터를 로깅하고 있는 경우, management center에서 해당 세그먼트의 데이터에 대한 로깅을 비활성화합니다. 예는 다음과 같습니다.

- 라우터가 management center와 동일한 네트워크 세그먼트에서 연결 이벤트를 로깅하는 경우, 상관관계 정책 또는 트래픽 프로파일 같은 다른 목적으로 이러한 연결 이벤트를 로깅해야 하는 경우가 아니라면 management center에서 동일한 연결을 로깅하지 마십시오.

  상관관계 정책에 대한 자세한 내용은 상관관계 정책 및 규칙 소개, 1017 페이지를 참조하십시오. 트래픽 프로파일에 대한 자세한 내용은 트래픽 프로파일 소개, 1057 페이지의 내용을 참조하십시오.

- Secure Network Analytics를 사용하여 스위치와 라우터에서 보고되는 NetFlow 레코드를 활용해 잠재적인 동작 이상 징후와 의심스러운 트래픽 패턴을 식별하는 경우, 이러한 세그먼트를 모니터링하는 규칙에 대한 연결 로깅을 비활성화하고 대신 네트워크의 해당 부분에 대한 동작 분석을 Secure Network Analytics에 의존할 수 있습니다.

  자세한 내용은 Secure Network Analytics 설명서를 참조하십시오.

연결의 시작 또는 종료를 로깅합니다**(**둘 다가 아니라**).**

연결 시작 또는 종료 로깅 중에서 선택할 수 있는 경우, 연결 종료 로깅을 활성화합니다. 이것은 연결 종료가 세션 기간 동안 수집된 정보뿐 아니라 연결 시작 이벤트의 정보도 로깅하기 때문입니다.

차단된 연결을 로깅하려고 하거나 연결 종료 정보가 중요하지 않은 경우에만 연결 시작을 로깅하십시오.

자세한 내용은 연결 시작 또는 종료 로깅, 759 페이지를 참고하십시오.

차단된 트래픽에 대한 로깅

차단된 트래픽은 추가 검사 없이 즉시 거부되기 때문에 일반적으로는 연결 시작 이벤트만 로깅할 수 있습니다.

자세한 내용은 차단된 연결에 대한 로깅, 757 페이지를 참고하십시오.

외부 위치에 이벤트 로깅

회사 보안 정책에서 허용하는 경우, 다음 중 하나를 사용하여 로그를 외부 소스에 스트리밍하면 management center에서 디스크 공간을 절약할 수 있습니다.

- management center 에서 맞춤 개발된 클라이언트 애플리케이션으로 로그를 스트리밍할 수 있는 eStreamer입니다. 자세한 내용은 *Firepower eStreamer* 통합 가이드를 참조하십시오.

- 알림 응답이라고 하는 Syslog 또는 SNMP 트랩. 자세한 내용은 Secure Firewall Management Center 알림 응답, 569 페이지를 참고하십시오.

이벤트 레코드의 최대 수를 지정합니다.

데이터베이스에 저장될 수 있는 레코드의 최소 및 최대 수를 고려하십시오. 예를 들어 가상 management center는 기본적으로 천만 개의 이벤트를 저장하지만 이벤트 최대 수는 5천만 개입니다. **System(**시스템**)** > **Configuration(**구성**)** > **Database(**데이터베이스**)**로 이동하여 필요에 맞게 크기를 조정하십시오.

모든 management center 모델 목록과 이벤트 데이터베이스 크기는 데이터베이스 이벤트 제한 수, 60 페이지의 내용을 참조하십시오.

연결 이벤트에 표시되는 항목 제어

연결 이벤트에 표시되는 행 수를 지정하려면 management center 오른쪽 상단에서 사용자 이름을 클릭하고 **User Preferences(**사용자 환경 설정**)** > **Event View Settings(**이벤트 보기 설정**)**를 클릭합니다. 페이지당 최대 1,000개의 이벤트를 설정할 수 있습니다.

연결 이벤트 보고서 설정

연결 이벤트가 누락되지 않도록 .csv 형식의 자동화된 보고서를 설정하여 필요에 따라 일정한 간격으로 생성되도록 예약할 수 있습니다. 자세한 내용은 다음을 참고하십시오.

- 리포트 디자이너(**Analysis(**분석**)** > **Connection(**연결**)** > **Events(**이벤트**)** > **Report Designer(**리포트 디자이너**)**): 설계 보고서 정보, 542 페이지 사용.
- 작업 예약(**System(**시스템**)** > **Tools(**도구**)** > **Scheduling(**예약**)**): 작업 예약 관련 정보, 501 페이지.

연결 로깅 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

연결 로깅 설정

다음 섹션에서는 다양한 규칙 및 조건에 맞게 연결 로깅을 설정하는 방법을 설명합니다.

터널 및 사전 필터 규칙으로 연결 로깅

사전 필터 정책은 Secure Firewall Threat Defense 디바이스에만 적용됩니다.

시작하기 전에

- 규칙 작업을 **Block(**차단**)** 또는 **Fastpath(**단축 경로**)**로 설정합니다. 액세스 제어로 연결을 계속 수행하도록 허용하는 **Analyze(**분석**)** 작업의 로깅이 비활성화되며, 다른 컨피그레이션이 처리 및 로깅을 결정합니다.
- 기록은 캡슐화 플로우가 아닌 내부 플로우에서 수행됩니다.

프로시저

단계 **1** 사전 필터 정책 편집기에서, 로깅을 설정하려는 규칙 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **2** **Logging(**로깅**)**을 클릭합니다.

단계 **3** **Log at Beginning of Connection(**연결 시작 시 로그**)** 또는 **Log at End of Connection(**연결 종료 시 로그**)** 중 원하는 로그 방식을 선택합니다.

성능을 최적화하려면, 연결의 시작 또는 종료를 로깅하시기 바랍니다. 동시에 하는 것은 안됩니다. 차단된 트래픽은 추가 검사 없이 즉시 거부되므로 차단 규칙에 대해서는 연결 종료 이벤트를 로깅할 수 없습니다.

단계 **4** 연결 이벤트를 전송할 위치를 지정합니다.

단계 **5** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

TLS/SSL 규칙으로 암호 해독 가능 연결 로깅

프로시저

단계 1 암호 해독 정책 편집기에서 로깅을 구성하려는 규칙 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 2 **Logging(**로깅**)**을 클릭합니다.

단계 3 **Log at End of Connection(**연결 종료 시 로깅**)** 확인란을 선택합니다.

모니터링되는 트래픽의 경우, 연결 종료 로깅이 필요합니다.

단계 4 연결 이벤트를 전송할 위치를 지정합니다.

이러한 연결 이벤트에서 management center 기반의 분석을 수행하려는 경우 이벤트 뷰어로 이벤트를 전송합니다. 이것은 모니터링되는 트래픽의 경우에 필요합니다.

단계 5 **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

단계 6 **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

보안 인텔리전스로 연결 로깅

보안 인텔리전스 정책에는 Threat Smart 라이선스 또는 Protection Classic 라이센스가 필요합니다.

프로시저

단계 1 액세스 제어 정책 편집기에서 **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다.

단계 2 **Logging(**로깅**)** ( )을 클릭하여 다음 기준을 바탕으로 Security Intelligenge(보안 인텔리전스) 로깅을 활성화합니다.

- IP 주소 기준 - **Networks(**네트워크**)** 옆에 있는 로깅을 클릭합니다.
- URL 기준 - **URLs** 옆에 있는 로깅을 클릭합니다.
- 도메인 이름 기준 - **DNS Policy(DNS** 정책**)** 드롭다운 목록 옆에 있는 로깅을 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** **Log Connections(**로그 연결**)** 확인란을 선택합니다.

단계 **4** 연결 및 보안 관련 연결 이벤트를 전송할 위치를 지정합니다.

management center 기반 분석을 수행하거나 차단 목록에 있는 개체를 모니터링 전용으로 설정하려면, 이벤트를 이벤트 뷰어로 전송합니다.

단계 **5** **OK(**확인**)**를 클릭하여 로깅 옵션을 설정합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

액세스 제어 규칙으로 연결 로깅

어떤 규칙 작업 및 심층 검사 옵션을 선택했는가에 따라 로깅 옵션이 달라집니다(규칙 및 정책 작업이 로깅에 미치는 영향, 756 페이지 참조).

프로시저

단계 **1** 액세스 컨트롤 정책 편집기에서 로깅을 구성하려는 규칙 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )가 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **2** **Logging(**로깅**)** 탭을 클릭합니다.

단계 **3** **Log at Beginning of Connection(**연결 시작 시 로그**)** 또는 **Log at End of Connection(**연결 종료 시 로그**)** 중 원하는 로그 방식을 선택합니다.

성능을 최적화하려면, 연결의 시작 또는 종료를 로깅하시기 바랍니다. 동시에 하는 것은 안됩니다.

단계 **4** (선택 사항) **Log Files(**로그 파일**)** 확인란을 선택하여 연결과 결합된 파일 및 악성코드 이벤트를 로깅합니다.

이 옵션은 활성화된 상태로 유지하는 것이 좋습니다.

단계 **5** 연결 이벤트를 전송할 위치를 지정합니다.

- **Event Viewer(**이벤트 뷰어**)**(또는 제품 이름): 이러한 연결 이벤트를 대상으로 management center 기반 분석을 수행하고 싶거나 규칙 작업이 **Monitor(**모니터링**)**일 경우, 연결 이벤트를 management center로 전송합니다.
- **Syslog Server(**시스템 로그 서버**)**: 연결 이벤트를 Access Control Policy(액세스 컨트롤 정책)의 Logging(로깅) 탭에 설정된 시스템 로그 서버로 전송합니다(재정의한 경우는 예외).

Show Overrides(재정의 표시**)**: 액세스 컨트롤 정책에 구성한 설정을 오버라이드하는 옵션을 표시합니다.

- **Override Severity(**심각도 재정의**)**: 이 옵션을 선택하고 규칙의 심각도를 선택하면, 해당 규칙에 대한 연결 이벤트는 Access Control Policy(액세스 컨트롤 정책)의 Logging(로깅) 탭에 설정된 심각도와는 상관없이 선택된 심각도를 갖게 됩니다.
- **Override Default Syslog Destination(**기본 시스템 로그 대상 재정의**)**: 이 규칙의 연결 이벤트에 대해 생성된 시스템 로그를 이 알림에서 지정하는 대상으로 전송합니다.

- **SNMP Trap(SNMP** 트랩**)**: 연결 이벤트는 선택된 SNMP 트랩으로 전송됩니다.

단계 **6** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

정책 기본 작업으로 연결 로깅

정책의 기본 작업은 시스템이 정책 내 규칙 중 어느 것과도 일치하지 않는 트래픽을 어떻게 처리할 것인지 결정합니다(일치 및 로깅되지만 트래픽을 검사하거나 처리하지 않는 액세스 제어 및 암호 해독 정책의 모니터링 규칙은 예외).

암호 해독 정책 기본 작업의 로깅 설정은 해독 불가능한 세션을 로깅하는 방법도 제어합니다.

시작하기 전에

- 사전 필터 기본 작업 로깅의 경우, 기본 작업을 **Block all tunnel traffic(**모든 터널 트래픽 차단**)**으로 설정합니다. 액세스 제어로 연결을 계속 수행하도록 허용하는 **Allow all tunnel traffic(**모든 터널 트래픽 허용**)** 작업의 로깅이 비활성화되며, 다른 구성이 처리 및 로깅을 결정합니다.

프로시저

단계 **1** 정책 편집기에서 **Default Action(**기본 작업**)** 드롭다운 목록 옆에 있는 **Logging(**로깅**)** ( )을 클릭합니다.

단계 **2** 일치하는 연결을 언제 로깅할지 지정합니다.

- Log at Beginning of Connection(연결 시작 시 로깅) — SSL 기본 작업에는 지원되지 않습니다.
- Log at End of Connection(연결 종료 시 로깅) — 액세스 제어 **Block All Traffic(**모든 트래픽 차단**)** 기본 작업 또는 사전 필터 **Block all tunnel traffic(**모든 터널 트래픽 차단**)** 기본 작업을 선택한 경우 지원되지 않습니다.

성능을 최적화하려면, 연결의 시작 또는 종료를 로깅하시기 바랍니다. 동시에 하는 것은 안됩니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다. 액세스 제어 정책의 경우, 상위 정책에서 컨피그레이션을 상속할 수도 있습니다.

단계 **3** 연결 이벤트를 전송할 위치를 지정합니다.

이러한 연결 이벤트에서 management center 기반의 분석을 수행하려는 경우 이벤트 뷰어로 이벤트를 전송합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

긴 URL의 로깅 제한

HTTP 트래픽에 대한 연결 종료 이벤트는 모니터링되는 호스트가 요청한 URL을 기록합니다. 저장된 URL 문자 수를 비활성화하거나 제한하면 시스템 성능을 높일 수 있습니다. URL 로깅을 비활성화해도(어떤 문자도 보관하지 않아도) URL 필터링은 영향받지 않습니다. 시스템은 요청된 URL을 기반으로 트래픽을 필터링하며, 시스템이 해당 URL을 기록하지 않는 경우도 마찬가지입니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)**를 클릭한 다음 **General Settings(**일반 설정**)** 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )가 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** 연결 이벤트에 저장하고자 하는 최대 **URL** 문자를 입력합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 구성 변경 사항을 구축합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참고하십시오.

32 장

연결 및 보안 관련 연결 이벤트

다음 주제에서는 연결 및 보안 이벤트 테이블을 사용하는 방법을 설명합니다.

연결 이벤트 정보

시스템은 자신의 매니지드 디바이스가 탐지한 연결의 로그를 생성할 수 있습니다. 이러한 로그를 연결 이벤트라고 합니다. 연결 이벤트는 *Security-Related(*보안 관련*)* 연결 이벤트(평판 기반 Security Intelligence(보안 인텔리전스) 기능이 차단한 연결)를 포함합니다.

연결 이벤트는 일반적으로 다음이 탐지한 트랜잭션을 포함합니다.

- 액세스 제어 정책
- 암호 해독 정책
- 사전 필터 정책(사전 필터나 터널 규칙이 캡처함)
- DNS 차단 목록
- URL 차단 목록
- 네트워크(IP 주소) 차단 목록

규칙 및 정책의 설정은 로깅할 연결의 종류, 로깅을 실행할 시기, 데이터를 저장할 위치를 세부적으로 제어할 수 있도록 합니다.

자세한 내용은 연결 로깅, 753 페이지를 참조하십시오.

관련 항목

보안 인텔리전스 정보

연결과 **Security-Related Connection Events**(보안 관련 연결 이벤트) 비교

Security-Related connection events(보안 관련 연결 이벤트)는 평판 기반 Security Intelligence(보안 인텔리전스) 기능으로 세션을 차단하거나 모니터링할 때마다 생성되는 연결 이벤트입니다.

그러나 모든 Security-Related Connection Events(보안 관련 연결 이벤트)에는 동일한 연결 이벤트가 존재합니다. Security-Related Connection Events(보안 관련 연결 이벤트)는 독립적으로 보고 분석할 수 있습니다. 또한 시스템은 Security-Related Connection Events(보안 관련 연결 이벤트) 이벤트를 개별적으로 저장하고 정리합니다.

시스템은 리소스 집약적인 평가를 실행하기 전에 먼저 Security Intelligence(보안 인텔리전스)를 실행합니다. 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.

참고 이 가이드에서 연결 이벤트에 대한 정보는 별도로 지정하지 않는 한 Security-Related Connection Events(보안 관련 연결 이벤트)와도 관련이 있습니다.

NetFlow 연결

매니지드 디바이스에 의해 수집된 연결 데이터를 보완하기 위해 NetFlow 엑스포터가 브로드캐스트하는 레코드를 사용하여 연결 이벤트를 생성할 수 있습니다. 이는 매니지드 디바이스에 의해 모니터링되는 것과 다른 네트워크를 NetFlow 엑스포터가가 모니터링하고 있는 경우 특히 유용합니다.

시스템은 NetFlow 레코드를 단방향 연결 종료 이벤트로 Secure Firewall Management Center 데이터베이스에 로깅합니다. 이 연결에 사용 가능한 정보는 액세스 제어 정책이 탐지하는 연결의 정보와 약간 다릅니다(NetFlow와 매니지드 디바이스 데이터의 차이점 참조).

관련 항목

NetFlow 데이터

연결 요약(그래프에 대한 집계된 데이터)

시스템에서는 5분 간격으로 수집된 연결 데이터를 연결 요약으로 취합하며, 시스템에서는 이를 사용하여 연결 그래프 및 트래픽 프로필을 생성합니다. 선택적으로, 연결 요약 데이터를 기준으로 맞춤형 워크플로를 생성할 수 있으며 이는 개별 연결 이벤트에 기반한 워크플로를 사용할 때와 같은 방식으로 사용합니다.

해당하는 연결 종료 이벤트를 연결 요약 데이터로 취합할 수는 있지만, 보안 관련 연결 이벤트에 대한 연결 요약 정보가 따로 제공되지는 않습니다.

여러 연결을 취합하려면 연결의 조건은 다음을 충족해야 합니다.

- 연결의 종료를 나타냄
- 소스 및 대상 IP 주소가 동일하며, 응답자(대상) 호스트에서 동일한 포트를 사용함
- 동일한 프로토콜을 사용함(TCP 또는 UDP)

- 동일한 애플리케이션 프로토콜을 사용함
- 동일한 매니지드 디바이스나 동일한 NetFlow 엑스포터를 사용하여 탐지함

각 연결 요약에는 총 트래픽 통계 및 요약에 나와 있는 연결 수가 포함됩니다. NetFlow 엑스포터는 단방향 연결을 생성하므로, 요약의 연결 수는 NetFlow 데이터를 기준으로 모든 연결마다 2배로 증가합니다.

연결 요약에는 요약의 취합된 연결과 관련된 모든 정보가 포함되지는 않습니다. 예를 들어, 클라이언트 정보는 연결 데이터를 연결 요약으로 취합하는 데 사용되지 않으므로 요약에는 클라이언트 정보가 포함되지 않습니다.

오래 실행되는 연결

모니터링되는 세션이 연결 데이터가 집계되는 5분 간격 2회 이상에 걸쳐 있는 경우, 해당 연결은 *long-running* 연결로 간주됩니다. 연결 요약의 연결 수를 계산할 때 long-running 연결이 시작된 5분 간격에 대해서만 수가 증가합니다.

또한 long-running 연결에서 이니시에이터 및 응답자가 전송한 패킷과 바이트 수를 계산할 때 각 5분 간격 동안 실제로 전송된 패킷과 바이트 수는 보고되지 않습니다. 그 대신, 시스템에서는 일정한 전송 속도를 추정하며 전송된 패킷과 바이트의 총 개수, 연결의 길이, 각 5분 간격 동안 발생한 연결의 부분을 기준으로 예측 수치를 계산합니다.

외부 응답자의 연결 요약 통합

연결 데이터를 저장하는 데 필요한 공간을 줄이고 연결 그래프의 렌더링 속도를 높이기 위해, 시스템에서는 다음과 같은 경우 연결 요약을 통합합니다.

- 모니터링되는 네트워크에 연결과 관련된 호스트 중 하나가 없는 경우
- 외부 호스트의 IP 주소를 제외하고 요약의 연결이 요약 어그리게이션 기준을 충족하는 경우

Analysis(분석) > Connections(연결) 하위 메뉴 페이지에서 연결 요약을 보고 연결 그래프 작업을 할 때 시스템은 모니터링되지 않는 호스트의 IP 주소 대신 외부 를 표시합니다.

이 어그리게이션으로 인해 외부 응답자와 관련된 연결 요약 또는 그래프에서 연결 데이터(즉, 개별 연결에 대한 액세스 데이터)의 테이블 보기로 드릴다운하려고 할 경우, 테이블 보기에 아무런 정보가 포함되지 않습니다.

연결 및 보안 관련 연결 이벤트 필드

참고 연결/Security-Related connection(보안 관련 연결) 이벤트 검색 페이지를 사용하여 연결과 관련된 이벤트를 검색할 수 없습니다.

액세스 제어 정책**(**시스템 로그**: ACPolicy)**

연결을 모니터링하는 액세스 제어 정책.

액세스 제어 규칙**(**시스템 로그**: AccessControlRuleName)**

연결을 처리한 액세스 제어 규칙 또는 기본 작업이자, 해당 연결과 일치한 최대 8개의 Monitor(모니터링) 규칙.

연결이 하나의 Monitor(모니터링) 규칙과 매칭될 경우, Secure Firewall Management Center에는 연결을 처리한 규칙의 이름이 표시되며 그 뒤에 Monitor(모니터링) 규칙 이름이 표시됩니다. 연결에 하나 이상의 Monitor(모니터링) 규칙과 매칭될 경우, 매칭되는 Monitor(모니터링) 규칙 수가 표시되며 `Default Action + 2 Monitor Rules(기본 작업 + 2개 모니터링 규칙)`가 그러한 예입니다.

팝업 창에 연결과 매칭되는 처음 8개 Monitor(모니터링) 규칙 목록을 표시하려면 ***N(***개수***)* Monitor Rules(**모니터링 규칙**)**를 클릭합니다.

작업**(**시스템 로그**: AccessControlRuleAction)**

연결을 로깅한 구성과 관련된 작업.

보안 인텔리전스로 모니터링된 연결의 경우, 작업은 연결에 의해 트리거되는 첫 번째 비 Monitor 액세스 제어 규칙 또는 기본 작업입니다. 이와 마찬가지로, Monitor(모니터링) 규칙과 매칭되는 트래픽은 항상 후속 규칙 또는 기본 규칙에 의해 처리되므로 Monitor(모니터링) 규칙에 의해 로깅된 연결과 관련된 작업은 Monitor(모니터링)가 될 수 없습니다. 그러나 Monitor(모니터링) 규칙과 매칭되는 연결에서 상관관계 정책 위반을 트리거할 수 있습니다.

작업	설명
허용	액세스 제어에 의해 명시적으로 허용되거나 사용자가 인터랙티브 차단을 우회했기 때문에 허용된 연결.
차단, 차단 및 재설정	차단된 연결. 예: • 사전 필터 정책에 의해 차단된 터널 및 기타 연결 • 보안 인텔리전스에 의해 차단된 연결. • SSL 정책에 의해 차단된 암호화된 연결. • 침입 정책에 따라 익스플로잇이 차단된 연결. • 파일 정책에 따라 파일(악성코드 포함)이 차단된 연결. 시스템이 침입 또는 파일을 차단하는 연결의 경우, 액세스 제어 Allow(허용) 규칙을 사용하여 심층 검사를 호출하더라도 시스템에 `Block(차단)`이 표시됩니다.
단축 경로	사전 필터 정책에 의해 경로가 단축된 비암호화 터널 및 기타 연결.
인터랙티브 차단, 인터랙티브 차단 후 재설정	시스템이 Interactive Block(인터랙티브 차단) 규칙을 사용해 사용자의 HTTP 요청을 초기에 차단하는 경우 로깅된 연결. 사용자가 시스템에 표시된 경고 페이지를 클릭할 경우, 해당 세션에 로깅된 추가 연결에는 Allow(허용) 작업이 포함됩니다.

작업	설명
신뢰	액세스 제어에서 신뢰하는 연결. 시스템은 기기 모델에 따라 신뢰하는 TCP 연결을 다르게 기록합니다.
기본 작업	액세스 제어 정책 기본 작업에서 처리한 연결
(비어 있음)	규칙과 일치하기에 충분한 패킷이 전달되기 전에 연결이 종료되었습니다. 이는 침입 방지 등의 액세스 제어 이외의 기능으로 인해 연결이 로깅되는 경우에만 발생할 수 있습니다.

애플리케이션 프로토콜**(**시스템 로그**: ApplicationProtocol)**

Secure Firewall Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

호스트 간 통신을 나타내며 연결에서 탐지되는 애플리케이션 프로토콜

애플리케이션 프로토콜 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

애플리케이션 위험성

연결에서 탐지된 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

사업 타당성

연결에서 탐지된 애플리케이션 트래픽과 연계된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

클라이언트 및 클라이언트 버전**(**시스템 로그**:** 클라이언트**, ClientVersion)**

연결에서 탐지된 클라이언트 애플리케이션 및 클라이언트 버전

시스템이 연결에 사용된 특정 클라이언트를 식별하지 못할 경우, 이 필드에는 애플리케이션 프로토콜 이름에 추가된 단어 "클라이언트"가 표시되어 일반 이름을 제공합니다(예:FTP 클라이언트).

클라이언트 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

Connection Counter(시스템 로그 전용**)**

다른 동시 연결에서 하나의 연결을 구분하는 카운터입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

Connection Instance ID(시스템 로그 전용**)**

연결 이벤트를 처리한 Snort 인스턴스입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

ConnectionDuration(시스템 로그만 있음**)**

이 필드는 시스템 로그 필드로만 존재합니다. Secure Firewall Management Center 웹 인터페이스에서는 존재하지 않습니다. (웹 인터페이스는 First Packet and Last PAcket(첫 번째 패킷 및 마지막 패킷) 열을 사용하여이 정보를 전달합니다.)

이 필드는 연결 종료 시 로깅이 발생하는 경우에만 값을 갖습니다. 연결 시작 시스템 로그 메시지의 경우, 이 필드는 해당 시점에 값을 알 수 없으므로 출력하지 않습니다.

연결 종료 시스템 로그 메시지의 경우, 이 필드는 첫 번째 패킷과 마지막 패킷 사이의 초 수를 나타내며 짧은 연결인 경우 0이 될 수 있습니다. 예를 들어, 시스템 로그의 타임스탬프가 12:34:56이며 ConnectionDuration이 5인 경우 첫 번째 패킷은 12:34:51입니다.

연결

연결 요약의 연결 개수. 여러 연결 요약 간격에 걸쳐 있는 long-running 연결의 경우, 첫 번째 연결 요약 간격만 증가합니다. **Connections(**연결**)** 기준을 사용하여 유의미한 검색 결과를 보려면 연결 요약 페이지가 있는 맞춤형 워크플로를 사용해야 합니다.

개수

각 행에 표시되는 정보와 매칭되는 연결의 개수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 **Count(**개수**)** 필드가 나타납니다. 사용자 지정 워크플로를 생성하고 **Count(**카운트**)** 열을 드릴다운 페이지에 추가하지 않은 경우, 각 연결은 개별적으로 낭려되고 패킷과 바이트는 합산되지 않습니다.

탐지 유형**(**시스템 로그**: DetectionType)**

이 필드에는 클라이언트 애플리케이션의 탐지 소스가 표시됩니다. **AppID** 또는 **Encrypted Visibility(**암호화된 가시성**)**일 수 있습니다.

대상 포트**/ICMP** 코드**(**시스템 로그**:** 별도 필드**- DstPort, ICMPCode)**

Secure Firewall Management Center 웹 인터페이스에서 이러한 값은 요약과 그래프를 제한합니다.

세션 responder가 사용하는 포트 또는 ICMP 코드

DestinationSecurityGroup(시스템 로그 전용**)**

이 필드는 사용 가능한 경우 **DestinationSecurityGroupTag**의 숫자 값과 연결된 텍스트 값을 보유합니다. 그룹 이름을 텍스트 값으로 사용할 수 없는 경우 이 필드에는 DestinationSecurityGroupTag 필드와 동일한 정수 값이 포함됩니다.

DestinationSecurityGroupType(시스템 로그만 해당**)**

이 필드는 보안 그룹 태그를 가져온 소스를 표시합니다.

값	설명
인라인	대상 SGT 값이 패킷에서 나옴
세션 디렉토리	대상 SGT 값이 세션 디렉토리 주제를 통해 ISE에서 제공됨
SXP	대상 SGT 값이 SXP 주제를 통해 ISE에서 제공됨

대상 **SGT(**시스템 로그**: DestinationSecurityGroupTag)**

연결에 사용되는 대상의 숫자 보안 그룹 태그(SGT) 속성입니다.

대상 SGT 값은 **DestinationSecurityGroupType** 필드에 지정된 소스에서 가져옵니다.

탐지 유형

이 필드에는 클라이언트의 탐지 소스가 표시됩니다.

디바이스

Secure Firewall Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

연결을 탐지한 매니지드 디바이스, 또는 NetFlow 데이터에서 생성된 연결의 경우 해당 데이터를 처리하는 매니지드 디바이스.

DeviceUUID(시스템 로그만 해당**)**

이벤트를 생성한 Firepower 디바이스의 고유 식별자입니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

DNS 쿼리**(**시스템 로그**: DNSQuery)**

연결에서 도메인 이름을 조회하기 위해 해당 이름 서버로 제출된 DNS 쿼리.

이 필드는 DNS 필터링이 활성화된 경우 URL 필터링 일치에 대한 도메인 이름을 포함할 수도 있습니다. 이 경우 URL 필드는 비어 있으며 URL 범주 및 URL 평판 필드에는 도메인과 연결된 값이 포함됩니다.

DNS 필터링에 대한 자세한 내용은 DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별의 내용을 참조하십시오.

DNS 레코드 종류**(**시스템 로그**: DNSRecordType)**

연결에서 제출된 DNS 쿼리 해결에 사용된 DNS 리소스 레코드의 유형.

DNS 응답**(**시스템 로그**: DNSResponseType)**

연결에서 쿼리를 받은 경우 이름 서버로 반환되는 DNS 응답.

DNS 싱크홀 이름**(**시스템 로그**: DNS_Sinkhole)**

시스템이 연결을 재전송한 싱크홀 서버의 이름.

DNS TTL(시스템 로그**: DNS_TTL)**

DNS 서버가 DNS 리소스 레코드를 캐시하는 초 수.

도메인

연결을 탐지한 매니지드 디바이스의 도메인, 또는 NetFlow 데이터에서 생성된 연결의 경우 해당 데이터를 처리하는 매니지드 디바이스의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

암호화된 가시성 프로세스 이름**(**시스템 로그**: EncryptedVisibilityProcessName)**

EVE(Encrypted Visibility Engine)에서 분석한 TLS 클라이언트 Hello 패킷의 프로세스 또는 클라이언트입니다.

암호화된 가시성 신뢰도 점수**(**시스템 로그**: EncryptedVisibilityConfidenceScore)**

암호화된 가시성 엔진이 올바른 프로세스를 탐지한 0~100% 범위의 신뢰도 값입니다. 예를 들어, 프로세스 이름이 Firefox이고 신뢰도 점수가 80%이면 엔진이 탐지한 프로세스가 Firefox임을 80% 신뢰하는 것입니다.

암호화된 가시성 위협 신뢰도**(**시스템 로그**: EncryptedVisibilityThreatConfidence)**

암호화된 가시성 엔진에서 탐지한 프로세스에 위협이 포함된 확률 레벨입니다. 이 필드는 위협 신뢰도 점수의 값을 기준으로 대역(Very High(매우 높음), High(높음), Medium(중간), Low(낮음) 또는 Very Low(매우 낮음))을 나타냅니다.

암호화된 가시성 위협 신뢰도 점수**(**시스템 로그**: EncryptedVisibilityThreatConfidenceScore)**

암호화된 가시성 엔진에서 탐지한 프로세스에 위협이 포함된 신뢰도 값(0~100%)입니다. 위협 신뢰도 점수가 매우 높은 경우(예: 90%) Encrypted Visibility Process Name(암호화된 가시성 프로세스 이름) 필드에 "Malware(악성코드)"가 표시됩니다.

Endpoint Location(엔드포인트 위치**)**

ISE에서 식별된 사용자를 인증하기 위해 ISE가 사용되는 네트워크 디바이스의 IP 주소.

엔드포인트 프로파일**(**시스템 로그**: Endpoint Profile)**

ISE에서 식별된 사용자의 엔드포인트 디바이스 유형.

이벤트 우선 순위**(**시스템 로그만 해당**)**

연결 이벤트가 우선 순위가 높은 이벤트인지 여부입니다. 우선 순위가 높은 이벤트는 침입, 보안 인텔리전스, 파일, 악성코드 이벤트와 관련된 연결 이벤트입니다. 이 외의 이벤트는 우선 순위가 낮은 이벤트입니다.

파일**(**시스템 로그**: FileCount)**

하나 이상의 파일 이벤트와 관련된 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수.

Secure Firewall Management Center 웹 인터페이스에서 파일 보기 아이콘이 파일 목록에 링크됩니다. 아이콘의 숫자는 해당 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수를 나타냅니다.

첫 번째 패킷 또는 마지막 패킷**(**시스템 로그**: ConnectionDuration** 필드를 참조하십시오**.)**

세션의 첫 번째 또는 마지막 패킷이 표시된 날짜 및 시간.

첫 번째 패킷 시간**(**시스템 로그만 해당**)**

시스템이 첫 번째 패킷을 수신한 시간입니다.

다음 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

HTTP 참조자**(**시스템 로그**: HTTPReferer)**

연결(다른 URL에 링크를 제공하는 웹사이트 또는 다른 URL에서 링크를 가져온 웹사이트 등)에서 탐지된 HTTP 트래픽에 대해 요청된 URL의 참조 페이지를 나타내는 HTTP 참조 페이지

HTTP 응답 코드**(**시스템 로그**: HTTPResponse)**

연결을 통해 클라이언트의 HTTP 요청에 대한 응답으로 전송된 HTTP 상태 코드

인그레스/이그레스 인터페이스**(**시스템 로그**: IngressInterface, EgressInterface)**

연결과 관련된 인그레스 또는 이그레스 인터페이스. 배포에 비대칭 라우팅 구성이 포함되어 있는 경우, 인그레스 및 이그레스 인터페이스가 동일한 인라인 쌍에 속하지 않을 수 있습니다.

인그레스/이그레스 보안 영역**(**시스템 로그**: IngressZone, EgressZone)**

연결과 관련된 인그레스 또는 이그레스 보안 영역

영역이 재지정된 캡슐화된 연결의 경우, 인그레스 필드는 원래 인그레스 보안 영역 대신 할당된 터널 영역을 표시합니다. 이그레스 필드는 공란입니다.

인그레스 가상 라우터/이그레스 가상 라우터**(**시스템 로그**: IngressVRF, EgressVRF**

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크를 진입하거나 벗어날 때 통과하는 가상 라우터의 이름입니다.

개시자/응답자 바이트**(**시스템 로그**: InitiatorBytes, ResponderBytes)**

세션 개시자가 전송했거나 세션 응답자가 수신한 총 바이트 수.

개시자/응답자 대륙

라우팅 가능한 IP가 탐지되는 경우 세션 개시자 또는 응답자의 IP 주소와 관련된 대륙.

개시자/응답자 국가

라우팅 가능한 IP가 탐지되는 경우 세션 개시자 또는 응답자의 IP 주소와 관련된 국가. 시스템에 해당 국가의 플래그 및 ISO 3166-1 alpha-3 국가 코드 아이콘이 표시됩니다. 국가의 전체 이름을 보려면 플래그 아이콘 위에 포인터를 올려놓습니다.

개시자/응답자 **IP(**시스템 로그**: SrcIP, DstIP)**

Secure Firewall Management Center 웹 인터페이스에서 이러한 값은 요약과 그래프를 제한합니다.

세션 이니시에어터 또는 응답기의 호스트 IP 주소(DNS 확인을 활성화한 경우 호스트 이름)

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 790 페이지도 참조하십시오.

Secure Firewall Management Center 웹 인터페이스에서 호스트 아이콘은 연결을 차단한 IP 주소를 식별합니다.

일반 텍스트의 경우 사전 필터 정책, 이니시에이터 및 응답자 IP 주소에 의해 차단되거나 경로가 단축된 통과 터널은 터널 엔드포인트를 나타냅니다. 이것은 터널 어느 한쪽에 있는 네트워크 디바이스의 라우팅된 인터페이스를 말합니다.

개시자/응답자 패킷**(**시스템 로그**: InitiatorPackets, ResponderPackets)**

세션 개시자가 전송했거나 세션 응답자가 수신한 총 패킷 수.

개시자 사용자**(**시스템 로그**: User)**

Secure Firewall Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

세션 개시자에 로그인한 사용자. 이 필드에 **No Authentication(**인증 없음**)**이 입력된 경우, 사용자 트래픽은 다음과 같습니다.

- 관련 ID 정책 없이 액세스 제어 정책과 매칭
- ID 정책에서 모든 규칙과 매칭되지 않음

해당하는 경우 사용자 이름 앞에 `<realm>\`을 입력합니다.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 790 페이지도 참조하십시오.

침입 이벤트**(**시스템 로그**: IPSCount)**

연결과 관련된 침입 이벤트의 수(해당되는 경우).

Secure Firewall Management Center 웹 인터페이스에서 침입 이벤트 보기 아이콘이 이벤트 목록에 링크됩니다.

IOC

이벤트가 연결과 관련된 호스트에 대해 IOC(indication of compromise)를 트리거했는지 여부.

NAT 소스/대상 **IP(**시스템 로그**: NAT_InitiatorIP, NAT_ResponderIP)**

세션 개시자 또는 응답자의 NAT 변환 IP 주소입니다.

NAT 소스/대상 포트**(**시스템 로그**: NAT_InitiatorPort, NAT_ResponderPort)**

세션 개시자 또는 응답자의 NAT 변환 포트입니다.

NetBIOS 도메인**(**시스템 로그**: NetBIOSDomain)**

세션에서 사용되는 NetBIOS 도메인

NetFlow SNMP 인풋/아웃풋

NetFlow 데이터에서 생성된 연결에서 연결 트래픽이 입력되거나 NetFlow 엑스포터를 종료하는 경우 인터페이스에 대한 인터페이스 인덱스.

NetFlow 소스/대상 자동 시스템

NetFlow 데이터에서 생성된 연결에서 트래픽 소스 또는 대상에 대한 경계 게이트웨이 프로토콜 자동 시스템 번호.

NetFlow 소스/대상 접두사

NetFlow 데이터에서 생성된 연결에서 소스 또는 대상 접두사 마스크로 AND 처리된 소스 또는 대상 IP 주소.

NetFlow 소스/대상 **TOS**

NetFlow 데이터에서 생성된 연결에서 연결 트래픽이 입력되거나 NetFlow 엑스포터를 종료하는 경우 서비스 유형(TOS) 바이트에 대한 설정.

네트워크 분석 정책**(**시스템 로그**: NAPPolicy)**

이벤드 생성과 관련된 NAP(네트워크 분석 정책) (해당되는 경우).

원본 클라이언트 국가

원래 클라이언트 IP 주소가 속하는 국가. 시스템은 이 값을 얻기 위해 XFF(X-Forwarded-For), True-Client-IP 또는 맞춤 정의된 HTTP 헤더에서 원래 클라이언트 IP 주소를 추출한 다음 GeoDB(지정학적 위치 데이터베이스)를 사용하여 국가에 매핑합니다. 이 필드에 값을 입력하려면 원래 클라이언트를 기준으로 프록시 설정된 트래픽을 처리하는 액세스 제어 규칙을 활성화해야 합니다.

원래 클라이언트 **IP(**시스템 로그**: originalClientSrcIP)**

XFF(X-Forwarded-For), True-Client-IP 또는 맞춤 정의된 HTTP 헤더의 원래 클라이언트 IP 주소. 이 필드에 값을 입력하려면 원래 클라이언트를 기준으로 프록시 설정된 트래픽을 처리하는 액세스 제어 규칙을 활성화해야 합니다.

사전 필터 정책**(**시스템 로그**: Profilter Policy)**

연결을 처리하는 사전 필터 정책.

프로토콜**(**시스템 로그**: Protocol)**

Secure Firewall Management Center 웹 인터페이스:

- 이 값은 요약과 그래프를 제한합니다.
- 이 필드는 검색 필드로만 사용할 수 있습니다.

연결에 사용된 전송 프로토콜 특정 프로토콜을 검색하려면 http://www.iana.org/assignments/protocol-numbers에 열거된 이름 또는 번호 프로토콜을 사용합니다.

QoS-적용 인터페이스

속도가 제한되는 연결에서 속도 제한이 적용되는 인터페이스 이름.

QoS-손실 개시자/응답자 바이트

속도 제한으로 인해 세션 개시자 또는 세션 응답자에서 삭제된 바이트 수.

QoS-손실 개시자/응답자 패킷

속도 제한으로 인해 세션 개시자 또는 세션 응답자에서 삭제된 패킷의 수.

QoS 정책

연결 속도를 제한하는 QoS 정책.

QoS 규칙

연결 속도를 제한하는 QoS 규칙.

이유**(**시스템 로그**: AccessControlRuleReason)**

다양한 상황에서 연결이 로깅된 이유. 전체 목록은 연결 이벤트 이유, 791 페이지를 참조하십시오.

IP Block(IP 차단), DNS Block(DNS 차단), URL Block(URL 차단) 이유와의 연결은 고유 개시자-응답자 쌍당 임계값이 15초입니다. 시스템이 이러한 연결 중 하나를 차단하는 경우, 포트 또는 프로토콜에 관계없이 다음 15초 동안 이러한 두 호스트 간에 추가로 차단된 연결에 대한 연결 이벤트는 생성되지 않습니다.

참조된 호스트**(**시스템 로그**: ReferencedHost)**

연결의 프로토콜이 HTTP, 또는 HTTPS인 경우 이 필드에는 각 프로토콜이 사용했던 호스트 이름이 표시됩니다.

SecIntMatchingIP(시스템 로그만 있음**)**

매칭되는 IP 주소.

가능한 값: **`None`** (없음), **`Destination`**(대상) 또는 **`Source`**(소스).

보안 상황**(**시스템 로그**: Context)**

여러 상황 모드에서 ASA FirePOWER가 처리한 연결의 경우 트래픽이 통과한 가상 방화벽 그룹을 식별하는 메타데이터.

보안 인텔리전스 카테고리**(**시스템 로그**: URLSICategory, DNSSICategory, IPReputationSICategory)**

연결에서 차단된 URL, 도메인 또는 IP 주소를 나타내거나 포함하는 개체의 이름. 보안 인텔리전스 카테고리는 네트워크 개체 또는 그룹, 차단 목록, 맞춤형 보안 인텔리전스 목록이나 피드, 관찰 관련 TID 카테고리, 인텔리전스 피드 내 카테고리 중 하나의 이름일 수 있습니다.

Secure Firewall Management Center 웹 인터페이스에서 DNS, 네트워크(IP 주소) 및 URL 보안 인텔리전스 연결 이벤트는 단일 카테고리 필드에 통합됩니다. 시스템 로그 메시지에서 해당 이벤트는 유형별로 지정됩니다.

Intelligence Feed 카테고리에 대한 자세한 내용은 보안 인텔리전스 카테고리를 참조하십시오.

소스 디바이스

Secure Firewall Management Center 웹 인터페이스에서 이 값은 요약과 그래프를 제한합니다.

연결 생성에 사용된 데이터를 브로드캐스트하는 NetFlow 엑스포터의 IP 주소. 매니지드 디바이스에서 연결이 탐지된 경우 이 필드에 `Firepower`가 표시됩니다.

소스 포트**/ICMP** 유형**(**시스템 로그**: SrcPort, ICMPType)**

Secure Firewall Management Center 웹 인터페이스에서 이러한 값은 요약과 그래프를 제한합니다.

세션 이니시에이터가 사용하는 포트 또는 ICMP 유형

SourceSecurityGroup(시스템 로그만 해당**)**

이 필드는 사용 가능한 경우 **SourceSecurityGroupTag**의 숫자 값과 연결된 텍스트 값을 보유합니다. 그룹 이름을 텍스트 값으로 사용할 수 없는 경우이 필드에는 SourceSecurityGroupTag 필드와 동일한 정수 값이 포함됩니다. 태그는 인라인 디바이스(소스 SGT 이름이 지정되지 않음) 또는 ISE(소스를 지정 함)에서 가져올 수 있습니다.

SourceSecurityGroupType (시스템 로그만 해당**)**

이 필드는 보안 그룹 태그를 가져온 소스를 표시합니다.

값	설명
인라인	소스 SGT 값이 패킷에서 나옴
세션 디렉토리	소스 SGT 값이 세션 디렉토리 주제를 통해 ISE에서 제공됨
SXP	소스 SGT 값은 SXP 주제를 통해 ISE에서 제공됨

소스 **SGT(**시스템 로그**: SourceSecurityGroupTag)**

연결에 사용되는 패킷의 보안 그룹 태그(SGT) 속성에 대한 숫자값 SGT는 신뢰할 수 있는 네트워크 내의 트래픽 소스 권한을 지정합니다. Cisco TrustSec 및 Cisco ISE 둘 다에서 제공되는 기능인 SGA(Security Group Access)는 패킷이 네트워크로 들어오면 속성을 적용합니다.

SSL 실제 작업**(**시스템 로그**: SSLActualAction)**

Secure Firewall Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

시스템에서 검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

시스템이 SSL 정책에서 암호화된 트래픽에 적용하는 작업.

작업	설명
차단/차단 및 재설정	차단된 암호화된 연결을 나타냅니다.
암호 해독(재서명)	다시 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.
암호 해독(대체 키)	대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.
암호 해독(알려진 키)	알려진 개인 키를 사용하여 암호 해독된 수신 연결을 나타냅니다.
기본 작업	연결이 기본 작업에 의해 처리되었음을 나타냅니다.
암호해독안함	시스템이 암호 해독하지 않은 연결을 나타냅니다.

SSL 인증서 정보**(**시스템 로그**: SSLCertificate)**

Secure Firewall Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

트래픽 암호화에 사용하는 공개 키 인증서에 저장된 정보로 다음을 포함합니다.

- Subject/Issuer Common Name(대상자/발급자 공용 이름)
- Subject/Issuer Organization(대상자/발급자 기관)
- Subject/Issuer Organization Unit(대상자/발급자 기관 부서)
- Not Valid Before/After(유효기간)
- Serial Number(일련 번호)
- Certificate Fingerprint(인증서 지문)
- Public Key Fingerprint(공개 키 지문)

SSL 인증서 상태**(**시스템 로그**: SSLServerCertStatus)**

이는 인증서 상태 SSL 규칙 조건을 구성한 경우에만 적용됩니다. 암호화된 트래픽이 SSL 규칙과 일치할 경우, 이 필드에는 다음 서버 인증서 상태 값 중 하나 이상이 표시됩니다.

- Self Signed(셀프 서명)
- Valid(유효)
- Invalid Signature(잘못된 서명)
- Invalid Issuer(잘못된 발급자)
- Expired(만료됨)
- Unknown(알 수 없음)
- Not Valid Yet(아직 유효하지 않음)
- Revoked(취소됨)

해독 불가능한 트래픽이 SSL 규칙과 매칭될 경우, 이 필드는 `Not Checked`(확인되지 않음)로 표시됩니다.

SSL 암호화 그룹**(**시스템 로그**: SSSLCipherSuite)**

연결을 암호화하는 데 사용되는 암호화 그룹을 나타내는 매크로 값. 암호 그룹 값 지정은 https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml의 내용을 참조하십시오.

연결에 적용된 **SSL** 암호화

이 필드는 Firepower Management Center 웹 인터페이스에서 검색 필드로만 사용할 수 있습니다.

Yes(예) 또는 **no**(아니오)를 **SSL** 검색 필드에 입력하고 TLS/SSL-암호화 또는 비암호화 연결을 확인합니다.

SSL 예상 작업**(**시스템 로그**: SSLExpectedAction)**

Secure Firewall Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

유효한 SSL 규칙을 감안하여 시스템에서 트래픽 암호화에 적용할 것으로 예상되는 작업.

SSL Actual Action(SSL 실제 작업**)**에 나열된 값 중 하나를 입력합니다.

SSL 실패 이유**(**시스템 로그**: SSLFlowStatus)**

시스템이 암호화된 트래픽의 암호 해독에 실패한 이유:

- Unknown(알 수 없음)
- No Match(일치하지 않음)
- Success(TLS 필수 성공)
- Uncached Session(캐시되지 않은 세션)
- Unknown Cipher Suite(알 수 없는 암호 그룹)
- Unsupported Cipher Suite(지원되지 않는 암호 그룹)
- Unsupported SSL Version(지원되지 않는 SSL 버전)
- SSL Compression Used(SSL 압축 사용됨)
- Session Undecryptable in Passive Mode(패시브 모드에서 세션 암호 해독 불가)
- Handshake Error(핸드셰이크 오류)
- Decryption Error(암호 해독 오류)
- Pending Server Name Category Lookup(서버 이름 카테고리 조회 보류 중)
- Pending Common Name Category Lookup(공용 이름 카테고리 조회 보류 중)
- Internal Error
- Network Parameters Unavailable(네트워크 파라미터 사용 불가)
- Invalid Server Certificate Handle(유효하지 않은 서버 인증서 처리)
- Server Certificate Fingerprint Unavailable(서버 인증서 지문 사용 불가)
- Cannot Cache Subject DN(대상자 DN 캐시 불가)
- Cannot Cache Issuer DN(발급자 DN 캐시 발가)
- Unknown SSL Version(알 수 없는 SSL 버전)
- External Certificate List Unavailable(외부 인증서 목록 사용 불가)
- External Certificate Fingerprint Unavailable(외부 인증서 지문 사용 불가)
- Internal Certificate List Invalid(내부 인증서 목록이 유효하지 않음)
- Internal Certificate List Unavailable(내부 인증서 목록 사용 불가)

- Internal Certificate Unavailable(내부 인증서 사용 불가)
- Internal Certificate Fingerprint Unavailable(내부 인증서 지문 사용 불가)
- Server Certificate Validation Unavailable(서버 인증서 검증 사용 불가)
- Server Certificate Validation Failure(서버 인증서 검증 장애)
- Invalid Action(유효하지 않은 작업)

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL 플로우 오류

TLS/SSL 세션 도중 오류가 발생하는 경우 오류 이름 및 16진수 코드, 오류가 발생하지 않는 경우 `Success(성공)`.

SSL 플로우 플래그

암호화된 연결에 대한 처음 10개의 디버깅 수준 플래그입니다. 워크플로 페이지에서 모든 플래그를 보려면 줄임표(**...**)를 클릭합니다.).

매니지드 디바이스가 오버로드되는 경우 OVER_SUBSCRIBED라는 메시지가 표시됩니다. 자세한 내용은 TLS/SSL 초과 서브스크립션 문제 해결를 참고하십시오.

SSL 플로우 메시지

아래 키워드는 암호화된 트래픽이 TLS/SSL 핸드셰이크 중 클라이언트와 서버 간에 교환된 지정 메시지 유형과 관련되어 있음을 나타냅니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246를 참조하십시오.

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC

- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER
- SERVER_NAME_MISMATCH

  세션에 표시되는 서버 인증서는 대상 도메인 이름과 일치하지 않는 공통 이름 또는 SAN 값을 갖습니다.

- CERTIFICATE_CACHE_HIT

  대상 도메인 이름과 일치하는 인증서가 캐시에 있습니다.

- CERTIFICATE_CACHE_MISS

  대상 도메인 이름과 일치하는 인증서가 캐시에 없습니다.

애플리케이션이 TLS/SSL 하트비트 확장을 사용하는 경우 메시지 HEARTBEAT가 표시됩니다. 자세한 내용은 TLS 하트비트 정보를 참고하십시오.

SSL 정책**(**시스템 로그**: SSLPolicy)**

연결을 처리한 SSL 정책.

TLS 서버 ID 검색이 액세스 제어 정책 고급 설정에서 활성화되어 있고 액세스 제어 정책과 연결된 SSL 정책이 없는 경우 이 필드는 모든 SSL 이벤트에 대해 아무것도 유지하지 않습니다.

SSL 규칙**(**시스템 로그**: SSLRuleName)**

연결을 처리한 SSL 규칙 또는 기본 작업이자 해당 연결과 매칭된 첫 번째 Monitor(모니터링) 규칙입니다. 연결이 하나의 Monitor(모니터링) 규칙과 매칭된 경우, 연결을 처리한 규칙의 이름이 필드에 표시되며 그 뒤에 Monitor(모니터링) 규칙 이름이 표시됩니다.

SSLServerName(시스템 로그만 있음**)**

이 필드는 시스템 로그 필드로만 존재합니다. Secure Firewall Management Center 웹 인터페이스에서는 존재하지 않습니다.

클라이언트가 암호화된 연결을 설정한 서버의 호스트 이름.

SSL 세션 **ID(**시스템 로그**: SSLSessionID)**

TLS/SSL 핸드셰이크 도중 클라이언트와 서버 간에 협상된 16진수 Session ID.

SSL 상태

암호화된 연결을 로깅한 **SSL Actual Action(SSL** 실제 작업**)** (SSL 규칙, 기본 작업 또는 암호 해독이 불가능한 트래픽 작업)과 관련된 작업. 잠금 아이콘은 SSL 인증서 세부 정보에 링크됩니다.

인증서를 사용할 수 없는 경우(예: TLS/SSL 핸드셰이크 오류로 연결 차단), 잠금 아이콘이 흐리게 표시됩니다.

시스템이 암호화된 연결을 해독하지 못할 경우, 실행된 **SSL Actual Action(SSL** 실제 작업**)** (해독 불가능한 트래픽 작업)과 **SSL Failure Reason(SSL** 실패 이유**)**가 표시됩니다. 예를 들어, 시스템이 알 수 없는 암호 그룹으로 암호화된 트래픽을 탐지하고 추가 검사 없이 이를 허용할 경우 이 필드는 `Do Not Decrypt (Unknown Cipher Suite)`(암호 해독 하지 않음(알려지지 않은 암호화 그룹))로 표시됩니다.

이 필드를 검색할 때 **SSL Actual Action(SSL** 실제 작업**)** 중 하나 이상과 **SSL Failure Reason(SSL** 실패 이유**)**를 입력하고 시스템이 처리했거나 암호 해독에 실패한 암호화된 트래픽을 확인합니다.

SSL 대상자/발급자 국가

이 필드는 Secure Firewall Management Center 웹 인터페이스에서만 검색 필드로만 사용 가능합니다.

암호화 인증서와 관련된 대상자 또는 발급자 국가의 2자 ISO 3166-1 alpha-2 국가 코드.

SSL 티켓 **ID(**시스템 로그**: SSLTicketID)**

TLS/SSL 핸드셰이크 도중 전송된 세션 티켓 정보의 16진수 해시 값

SSLURLCategory(시스템 로그만 있음**)**

암호화된 연결에서 방문한 URL의 URL 카테고리.

이 필드는 시스템 로그 필드로만 존재합니다. Secure Firewall Management Center 웹 인터페이스에서 이 필드의 값은 URL 카테고리 열에 포함됩니다.

URL도 참조하십시오.

SSL 버전**(**시스템 로그**: SSLVersion)**

연결 암호화에 사용되는 TLS/SSL 프로토콜 버전:

- 알 수 없음
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TLSV1.2
- TLSv1.3

TCP 플래그**(**시스템 로그**: TCPFlags)**

NetFlow 데이터에서 생성된 연결에서 탐지된 TCP 플래그.

이 필드를 검색할 때 쉼표로 구분된 TCP 플래그 목록을 입력하면 이러한 플래그 중 최소한 하나를 보유한 모든 연결을 볼 수 있습니다.

시간

연결 요약에서 연결을 취합하기 위해 시스템이 사용한 5분 간격의 종료 시간. 이 필드는 검색할 수 없습니다.

총 패킷

이 필드는 검색 필드로만 사용할 수 있습니다.

연결에서 전송된 패킷의 총 수.

트래픽**(KB)**

이 필드는 검색 필드로만 사용할 수 있습니다.

연결에서 전송된 데이터의 총량(단위: 킬로바이트)

터널/사전 필터 규칙**(**시스템 로그**: Tunnel** 또는 **Profiler Rule)**

연결을 처리하는 터널 규칙, 사전 필터 규칙 또는 사전 필터 정책 기본 작업.

URL, URL 카테고리 및 **URL** 평판**(**시스템 로그**: URL, URLCategory** 및 **SSLURLCategory, URLReputation)**

세션 중에 모니터링된 호스트에서 요청한 URL, 관련 카테고리 및 평판(해당되는 경우)

이벤트에서 URL 범주 및 평판을 표시하려면 액세스 제어 정책에 해당 URL 규칙을 포함하고 **URL** 탭 아래에서 URL 범주 및 URL 평판을 사용하여 규칙을 구성해야 합니다.

URL 범주 및 평판은 URL 규칙과 매칭되기 전에 연결이 처리되면 이벤트에 표시되지 않습니다.

URL 열이 비어 있고 DNS 필터링이 활성화된 경우 DNS Query(DNS 쿼리) 필드에 도메인이 표시되고 URL 범주 및 URL 평판 값이 도메인에 적용됩니다.

시스템에서 TLS/SSL 애플리케이션을 식별하거나 차단한 경우, 요청한 URL은 암호화된 트래픽에 있으므로 시스템은 SSL 인증서를 기준으로 해당 트래픽을 식별합니다. 따라서 TLS/SSL 애플리케이션의 경우, 이 필드는 인증서에 포함된 공용 이름을 나타냅니다.

위 **SSLURLCategory**도 참조하십시오.

사용자 에이전트**(**시스템 로그**: UserAgent)**

연결에서 탐지된 HTTP 트래픽에서 추출된 사용자 에이전트 문자열 애플리케이션 정보.

VLAN ID (시스템 로그**: VLAN_ID)**

연결을 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID.

웹 애플리케이션**(**시스템 로그**: WebApplication)**

연결에서 탐지된 HTTP 트래픽의 콘텐츠 또는 요청한 URL을 나타내는 웹 애플리케이션

웹 애플리케이션이 이벤트의 URL과 매칭되지 않을 경우, 해당 트래픽은 참조 트래픽(예: 광고 트래픽)일 가능성이 높습니다. 시스템이 참조 트래픽을 탐지할 경우, 시스템은 제공되는 참조 애플리케이션을 저장하고 해당 애플리케이션을 웹 애플리케이션으로 나열합니다.

시스템이 HTTP 트래픽에서 특정 웹 애플리케이션을 식별하지 못할 경우, 이 필드는 `Web Browsing(웹 브라우징)`으로 표시됩니다.

웹 애플리케이션 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

연결 및 **Security-Related Connection Event(**보안 관련 연결 이벤트**)** 필드 정보

Secure Firewall Management Center 웹 인터페이스에서 **Analysis(**분석**) > Connections(**연결**)** 하위 메뉴의 테이블 형식 및 그래픽 워크플로우를 사용하여 연결 및 Security-Related connection(보안 관련 연결) 이벤트를 보고 검색할 수 있습니다.

참고 Security-Related connection event(보안 관련 연결 이벤트)마다 별도로 저장되는 동일한 연결 이벤트가 있습니다. 모든 Security-Related connection event(보안 관련 연결 이벤트)에는 내용이 채워진 **Security Intelligence Category(**보안 인텔리전스 범주**)** 필드가 있습니다.

개별 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다.

검색 제약 조건

검색 페이지에서 별표(*****)로 표시된 필드는 연결 그래프 및 연결 요약을 제한 합니다. 연결 그래프는 연결 요약에 기반하므로, 연결 요약을 제한하는 동일한 기준은 연결 그래프도 제한합니다. 잘못된 검색 제한을 사용하여 연결 요약을 검색하고 맞춤형 워크플로의 연결 요약 페이지를 사용하여 결과를 볼 경우, 잘못된 제한은 해당 사항 없음(N/A)이라는 레이블로 표시되고 취소선이 그어집니다.

Syslog 필드

대부분의 필드는 Secure Firewall Management Center 웹 인터페이스와 syslog 메시지에 모두 표시됩니다. 나열된 동등한 syslog가 없는 필드는 syslog 메시지에서 사용할 수 없습니다. 언급한 것처럼 일부 필드는 syslog 전용이며, 그 밖의 소수의 필드는 syslog 메시지에서는 별도의 필드이지만 웹 인터페이스에서는 통합된 필드이며, 그 반대의 경우도 있습니다.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침

표 ***95:*** 용어 비교

필드	이벤트 유형	설명
이니시에이터/응답자	연결	연결의 이니시에이터/응답자. 연결의 이니시에이터가 침입 소스 또는 악성 코드 파일의 발신자와 반드시 같을 필요는 없습니다.

필드	이벤트 유형	설명
소스/대상	침입	공격의 소스/대상입니다. 침입 이벤트의 소스는 연결의 이니시에이터 또는 응답자일 수 있습니다.
발신자/수신자 (전송 중..., 수신 중...)	파일, 악성 코드	파일 또는 악성 코드의 발신자/수신자. 파일을 업로드하거나 다운로드할 수 있으므로 파일의 발신자가 반드시 연결의 이니시에이터일 필요는 없습니다.

연결 이벤트 이유

연결 이벤트의 Reason(이유) 필드는 다음과 같은 상황에서 연결이 로깅된 이유를 표시합니다.

이유	설명
콘텐츠 제한	시스템이 Safe Search 기능과 관련된 콘텐츠 제한을 적용하기 위해 패킷을 수정했습니다.
DNS 차단	시스템에서 도메인 이름 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. DNS 차단 이유는 DNS 규칙 작업에 따라 차단, 도메인을 찾을 수 없음 또는 싱크홀과 페어링됩니다.
DNS 모니터링	시스템에서 도메인 이름 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.
엘리펀트 플로우	연결은 전체 시스템 성능에 영향을 미칠 만큼 충분히 큰 플로우인 엘리펀트 플로우으로 간주되기에 충분합니다. 기본적으로 엘리펀트 플로우는 1GB/10초보다 큽니다. **system support elephant-flow-detection** 명령을 사용하여 threat defense CLI에서 엘리펀트 플로우 식별을 위한 바이트 및 시간 임계값을 조정할 수 있습니다. 자세한 내용은 Cisco Secure Firewall Threat Defense 명령 참조를 참고하십시오. 참고 바이트 및 시간 임계값을 모두 초과하는 경우에만 플로우가 엘리펀트 플로우로 간주됩니다. Snort, 시스템, 물리적 코어와 같은 CPU 메트릭 등의 플로우와 기타 상호 관련된 메트릭을 상호 연결하는 맞춤형 대시보드를 생성할 수 있습니다. 자세한 내용은 시스템 모니터링 및 문제 해결 장을 참조하십시오.
파일 차단	시스템이 전송을 차단한 파일 또는 악성코드 파일이 연결에 포함되었습니다. 파일 차단 이유는 항상 차단 작업과 페어링됩니다.
파일 맞춤형 탐지	시스템이 전송을 차단한 맞춤형 탐지 목록의 파일이 연결에 포함되었습니다.

이유	설명
파일 모니터링	시스템이 연결에서 특정 파일 유형을 탐지했습니다.
파일 재시작 허용	파일 전송이 파일 차단 또는 악성코드 차단 파일 규칙에 의해 원래 차단되었다가, 해당 파일을 허용하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 재시작되었습니다. 이 이유는 인라인 구축에서만 표시됩니다.
파일 재시작 차단	파일 전송이 파일 탐지 또는 악성코드 클라우드 조회 파일 규칙에 의해 원래 허용되었다가, 해당 파일을 차단하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 중지되었습니다. 이 이유는 인라인 구축에서만 표시됩니다.
인텔리전트 애플리케이션 바이패스	인텔리전트 애플리케이션 우회(IAB) 모드: • 작업이 Trust(신뢰)인 경우, IAB는 우회 모드였습니다. 일치하는 트래픽은 추가 검사 없이 통과합니다. • 작업이 Allow(허용)인 경우, IAB는 테스트 모드였습니다. 일치하는 트래픽은 추가 검사가 가능했습니다.
침입 차단	Snort2 엔진 - 시스템이 연결에서 탐지된 익스플로잇(침입 정책 위반)을 차단했거나 차단할 수도 있었음을 나타냅니다. 침입 차단 이유는 차단된 익스플로잇의 경우 차단 작업과, 차단될 수도 있었던 익스플로잇의 경우 허용과 페어링됩니다. Snort3 엔진 - "would have dropped(삭제되었을 수 있음)" 결과가 있는 경우 "Intrusion block(침입 차단)" 대신 연결 이벤트 이유가 비어 있습니다. "would have dropped(삭제되었을 수 있음)" 이벤트는 채워지는 연결 이벤트 사유와 관련하여 "Allow(허용)"과 동일하게 처리됩니다.
침입 모니터링	시스템이 연결에서 탐지된 익스플로잇을 탐지했지만 차단하지는 않았습니다. 트리거된 침입 규칙의 상태가 이벤트 생성으로 설정되어 있으면 이러한 현상이 나타납니다.
IP 차단	시스템에서 IP 주소 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. IP 차단 이유는 항상 차단 작업과 페어링됩니다.
IP 모니터	시스템에서 IP 주소 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.
SSL 차단	시스템에서 TLS/SSL 검사 구성에 기반하여 암호화된 연결을 차단했습니다. SSL 차단 이유는 항상 차단 작업과 페어링됩니다.
URL 차단	시스템에서 URL 및 보안 인텔리전스 데이터를 기준으로 하여 검사 없이 연결을 거부했습니다. URL 차단 이유는 항상 차단 작업과 페어링됩니다.
URL 모니터링	시스템에서 URL 및 보안 인텔리전스 데이터를 기준으로 하여 연결을 거부해야 했지만 사용자가 시스템에서 연결을 거부하는 대신 모니터링하도록 구성했습니다.

이유	설명
사용자 바이패스	시스템에서 사용자의 HTTP 요청을 처음에 차단했지만 사용자가 경고 페이지를 클릭하여 사이트를 봤습니다. 사용자 바이패스 이유는 항상 허용 작업과 페어링됩니다.

연결 이벤트 필드 채우기 요구 사항

연결 이벤트, , 보안 관련 연결 이벤트 또는 연결 요약에 사용할 수 있는 정보는 여러 요인에 따라 달라집니다.

어플라이언스 모델 및 라이선스

대다수의 기능은 대상 디바이스에서 특정 라이선스 기능을 활성화해야 하며, 특정 모델에서만 사용 가능한 기능도 많습니다.

트래픽 특성

시스템은 네트워크 트래픽에 존재하고 탐지 가능한 정보만 보고합니다. 예를 들어 이니시에이터 호스트와 연결된 사용자가 없거나, 프로토콜이 DNS, HTTP 또는 HTTPS가 아닌 연결에서 참조 호스트가 탐지되지 않을 수 있습니다.

기원/탐지 방법: 트래픽 기반 탐지 대 **NetFlow**

NetFlow 전용 필드를 제외하고, NetFlow 기록에서 사용 가능한 정보는 트래픽 기반 탐지가 생성한 정보에 비해 더욱 제한됩니다(NetFlow와 매니지드 디바이스 데이터의 차이점 참조).

평가 단계

각 유형의 트래픽 검사와 제어는 유연성과 성능을 최대화할 수 있는 방식으로 발생합니다.

예를 들어 시스템은 리소스 집약적인 평가를 실행하기 전에 먼저 보안 인텔리전스를 실행합니다. 보안 인텔리전스에 의해 연결이 차단된 경우, 그 결과로 생성된 이벤트에는 시스템이 후속 평가를 통해 수집했을 수 있는 정보(예: 사용자 ID)가 포함되지 않습니다.

로깅 방법: 연결의 시작 또는 종료

시스템이 연결을 탐지한 경우, 연결의 시작/종료(또는 두 시점 모두) 시점 중 연결을 언제 로깅할 수 있는지는 사용자가 시스템의 연결 탐지 및 처리 방식을 어떻게 구성하느냐에 따라 달라집니다.

Beginning-of-connection 이벤트에는 세션 기간 중에 트래픽을 검사하여 확인해야 하는 정보(예: 전송된 총 데이터의 양, 연결의 마지막 패킷의 타임스탬프)가 포함되지 않습니다. Beginning-of-connection 이벤트에는 세션의 애플리케이션 또는 URL 트래픽에 대한 정보가 없을 수 있으며, 세션의 암호화에 대한 세부 정보도 포함되지 않습니다. 일반적으로 Beginning-of-connection 로깅은 차단된 연결에 대한 유일한 옵션입니다.

연결 이벤트 유형: 개별 대 요약

연결 요약에는 취합된 연결과 관련된 모든 정보가 포함되지 않습니다. 예를 들어, 클라이언트 정보는 연결 데이터를 연결 요약으로 취합하는 데 사용되지 않으므로 요약에는 클라이언트 정보가 포함되지 않습니다.

연결 그래프는 연결 종료 로그만 사용하는 연결 요약 데이터를 기준으로 합니다. 연결 시작 데이터만 기록하도록 시스템을 설정하는 경우, 연결 그래프 및 연결 요약 이벤트 보기에 데이터가 포함되지 않습니다.

기타 설정

연결에 영향을 주는 기타 설정으로는 다음과 같은 항목이 있습니다.

- ISE 관련 필드는 Active Directory 도메인 컨트롤러를 통해 인증한 사용자와 관련된 연결에서 ISE를 설정하는 경우에만 채워집니다. 연결 이벤트는 LDAP, RADIUS, 또는 RSA 도메인 컨트롤러를 통해 인증한 사용자의 ISE 데이터는 포함하지 않습니다.
- 보안 그룹 태그 (SGT) 필드는 ISE를 ID 소스로 설정하거나 맞춤형 SGT 규칙 조건을 추가하는 경우에만 채워집니다.
- 사전 필터 관련 필드(보안 영역 필드의 터널 영역 정보 포함)는 사전 필터 정책이 처리한 연결에서만 채워집니다.
- TLS/SSL 관련 필드는 암호 해독 정책을 통해 처리되는 암호화된 연결에서만 채워집니다. 트래픽을 암호화하지 않아도 된다면 Do Not Decrypt 규칙 작업을 사용하여 필드의 값을 확인할 수 있습니다.
- 파일 정보 필드는 파일 정책과 관련된 액세스 컨트롤 규칙이 기록한 연결에서만 채워집니다.
- 침입 정보 필드는 침입 정책과 관련되거나 기본 작업을 사용하는 액세스 컨트롤 규칙이 기록한 연결에서만 채워집니다.
- QoS 관련 필드는 속도 제한의 영향을 받는 연결에서만 채워집니다.
- Reason(원인) 필드는 사용자가 Interactive Block(인터랙티브 차단) 설정을 우회하는 경우 같은 특정 상황에서만 채워집니다.
- Domain(도메인) 필드는 Secure Firewall Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
- 액세스 컨트롤 정책의 고급 설정에서는 HTTP 세션에서 모니터링된 호스트에서 요청한 각 URL의 연결 로그에 저장되는 특성의 수를 제어합니다. 이 설정을 사용하여 URL 로깅을 비활성화할 경우, 카테고리 및 평판 데이터가 존재하고 이를 계속 볼 수 있는 경우에도 시스템에서는 연결 로그에 개별 URL을 표시하지 않습니다.
- 연결 이벤트에서 URL 범주 및 평판을 표시하려면 액세스 제어 정책에 해당 URL 규칙을 포함하고 **URL** 탭 아래에서 URL 범주 및 URL 평판을 사용하여 규칙을 구성해야 합니다. URL 범주 및 평판은 URL 규칙과 매칭되기 전에 연결이 처리되면 이벤트에 표시되지 않습니다.

관련 항목

NetFlow와 매니지드 디바이스 데이터의 차이점

연결 이벤트 필드에서 제공되는 정보

이 항목의 표에는 시스템이 연결 및 보안 인텔리전스 필드를 채울 수 있는 경우가 나와 있습니다. 표의 열은 다음 이벤트 유형을 나타냅니다.

- 출처: 직접 - System 매니지드 디바이스에서 탐지 및 처리된 연결을 나타내는 이벤트.
- 출처: NetFlow - NetFlow 엑스포터에서 내보낸 연결을 나타내는 이벤트
- 로깅: 시작 - 시작 시에 로깅되는 연결을 나타내는 이벤트
- 로깅: 종료 - 종료 시에 로깅되는 연결을 나타내는 이벤트

표에서 "예"는 시스템이 연결 이벤트 필드를 채워야 한다는 의미가 아니라 채울 수 있다는 의미입니다. 시스템은 네트워크 트래픽에 존재하고 탐지 가능한 정보만 보고합니다. 예를 들어 TLS/SSL 관련 필드는 암호화 정책을 통해 처리되는 암호화된 연결의 기록에 대해서만 채워집니다.

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
액세스 제어 정책	예	아니요	예	예
액세스 제어 규칙	예	아니요	예	예
작업	예	아니요	예	예
애플리케이션 프로토콜	예	예	사용 가능한 경우	예
애플리케이션 프로토콜 카테고리 및 태그	예	아니요	사용 가능한 경우	예
애플리케이션 위험성	예	아니요	사용 가능한 경우	예
사업 타당성	예	아니요	사용 가능한 경우	예
클라이언트	예	아니요	사용 가능한 경우	예
클라이언트 카테고리 및 태그	예	아니요	사용 가능한 경우	예
클라이언트 버전	예	아니요	사용 가능한 경우	예
연결	예	예	아니요	예
개수	예	예	예	예
대상 포트/ICMP 유형	예	예	예	예

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
대상 SGT	예	아니요	예	예
디바이스	예	예	예	예
도메인	예	예	예	예
DNS 쿼리	예	아니요	예	예
DNS 레코드 유형	예	아니요	예	예
DNS 응답	예	아니요	예	예
DNS 싱크홀 이름	예	아니요	예	예
DNS TTL	예	아니요	예	예
이그레스 인터페이스	예	아니요	예	예
이그레스 보안 영역	예	아니요	예	예
엔드포인트 위치	예	아니요	예	예
엔드포인트 프로파일	예	아니요	예	예
파일	예	아니요	아니요	예
첫 번째 패킷	예	예	예	예
HTTP 참조 페이지	예	아니요	아니요	예
HTTP 응답 코드	예	아니요	예	예
인그레스 인터페이스	예	아니요	예	예
인그레스 보안 영역	예	아니요	예	예
초기자 바이트	예	예	유용하지 않음	예
초기자 국가	예	아니요	예	예
초기자 IP	예	예	예	예
초기자 패킷	예	예	유용하지 않음	예
이니시에이터 사용자	예	예	예	예
침입 이벤트	예	아니요	아니요	예
침입 정책	예	아니요	예	예
IOC(보안 침해 지표)	예	아니요	예	예

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
마지막 패킷	예	예	아니요	예
NetBIOS 도메인	예	아니요	예	예
NetFlow 소스/대상 자동 시스템	아니요	예	아니요	예
NetFlow 소스/대상 접두사	아니요	예	아니요	예
NetFlow 소스/대상 TOS	아니요	예	아니요	예
NetFlow SNMP 인풋/아웃풋	아니요	예	아니요	예
네트워크 분석 정책	예	아니요	예	예
원본 클라이언트 국가	예	아니요	예	예
원본 클라이언트 IP	예	아니요	예	예
사전 필터 정책	예	아니요	예	예
QoS-적용 인터페이스	예	아니요	아니요	예
QoS-손실 이니시에이터 바이트	예	아니요	아니요	예
QoS-손실 이니시에이터 패킷	예	아니요	아니요	예
QoS-손실 Responder 바이트	예	아니요	아니요	예
QoS-손실 Responder 패킷	예	아니요	아니요	예
QoS 정책	예	아니요	아니요	예
QoS 규칙	예	아니요	아니요	예
이유	예	아니요	예	예
참조된 호스트	예	아니요	아니요	예
응답기 바이트	예	예	유용하지 않음	예
응답기 국가	예	아니요	예	예
응답기 IP	예	예	예	예
응답기 패킷	예	예	유용하지 않음	예
보안 상황 (ASA 전용)	예	아니요	예	예
보안 인텔리전스 범주	예	아니요	예	예
소스 디바이스	예	예	예	예

연결 이벤트 필드	출처: 직접	출처: **NetFlow**	로깅: 시작	로깅: 종료
소스 포트/ICMP 유형	예	예	예	예
소스 SGT	예	아니요	예	예
SSL 인증서 상태	예	아니요	아니요	예
SSL 암호 그룹	예	아니요	아니요	예
SSL 플로우 오류	예	아니요	아니요	예
SSL 플로우 플래그	예	아니요	아니요	예
SSL 플로우 메시지	예	아니요	아니요	예
해독 정책	예	아니요	아니요	예
해독 규칙	예	아니요	아니요	예
SSL 세션 ID	예	아니요	아니요	예
SSL 상태	예	아니요	아니요	예
SSL 버전	예	아니요	아니요	예
TCP 플래그	아니요	예	아니요	예
시간	예	예	아니요	예
터널/사전 필터 규칙	예	아니요	예	예
URL	예	아니요	사용 가능한 경우	예
URL 범주	예	아니요	사용 가능한 경우	예
URL 평판	예	아니요	사용 가능한 경우	예
사용자 에이전트	예	아니요	아니요	예
VLAN ID	예	아니요	예	예
웹 애플리케이션	예	아니요	사용 가능한 경우	예
웹 애플리케이션 카테고리 및 태그	예	아니요	사용 가능한 경우	예

연결 및 보안 관련 연결 이벤트 테이블 사용

Secure Firewall Management Center을(를) 사용하여 연결 또는 보안 관련 연결의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

연결 그래프에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 이벤트의 테이블 보기에서 종료되는 미리 정의된 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

연결 또는 보안 인텔리전스 워크플로 테이블을 사용하는 경우, 여러 일반적인 작업을 수행할 수 있습니다.

드릴다운 페이지에서 연결 이벤트를 제한할 경우, 동일한 이벤트의 패킷 및 바이트가 합산됩니다. 하지만 맞춤형 워크플로를 사용 중이고 드릴다운 페이지에 **Count(**카운트**)** 열을 추가하지 않은 경우, 이벤트가 개별적으로 나열되고 패킷과 바이트는 합산되지 않습니다.

시스템에서 생성되는 연결 이벤트가 25개를 넘는 경우, **Connection Events(**연결 이벤트**)** 테이블 보기는 얼마나 많은 이벤트 페이지를 사용할 수 있는지 표시하는 대신 여러 개 중 하나를 표시합니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** 다음 중 하나를 선택합니다.

- **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)** (연결 이벤트의 경우)
- **Analysis(**분석**)** > **Connections(**연결**)** > **Security-Related Events(**보안 관련 이벤트**)**

참고 테이블 대신 연결 그래프가 표시되는 경우, 워크플로 제목별로 **(**워크플로 전환**)**을 클릭하고 미리 정의된 **Connection Events(**연결 이벤트**)** 워크플로 또는 맞춤형 워크플로를 선택합니다. 미리 정의된 연결 이벤트 워크플로(연결 그래프 포함)는 연결의 테이블 보기에서 종료됩니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- Time Range(시간 범위) - 시간 범위를 조정합니다. 이벤트가 표시되지 않는 경우에 유용합니다. 타임 윈도우 변경, 710 페이지 참조.
- Data Source(데이터 소스)-Security Analytics and Logging(보안 애널리틱스)를 사용하여 데이터가 원격으로 저장되어 있고 데이터 소스를 변경해야 하는 충분한 이유가 있는 경우 데이터 소스를 선택합니다. 이 옵션에 대한 중요한 정보는 Secure Network Analytics 어플라이언스에 저장된 연결 이벤트로 Secure Firewall Management Center에서 작업, 699 페이지의 내용을 참조하십시오.

- Field Names(필드 이름) - 테이블 열의 콘텐츠에 대해 자세히 알아봅니다. 연결 및 보안 관련 연결 이벤트 필드, 773 페이지 참조.

  팁 이벤트의 테이블 보기에는 여러 필드가 기본적으로 숨겨져 있습니다. 표시되는 필드를 변경하려면 임의의 열 이름에서 **x**를 클릭하여 필드 선택기를 표시합니다.

- 추가 정보 - 시스템 외부의 사용 가능한 소스에 있는 데이터를 보려면 이벤트 값을 마우스 오른쪽 버튼으로 클릭합니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지 섹션을 참조해 주십시오.

- 외부 인텔리전스 - 이벤트에 대한 정보를 수집하려면 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지를 참고하십시오.

- 호스트 프로필 - IP 주소의 호스트 프로필을 보려면 **Host Profile(**호스트 프로필**)**을 클릭하거나 활성 IOC(Indication of Compromise) 태그가 있는 호스트의 경우에는 IP 주소 옆에 표시되는 **Compromised Host(**보안 침해된 호스트**)**를 클릭합니다.

- 사용자 프로파일 - 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘 또는 IOC와 연결된 사용자라면 **Red User(**빨간색 사용자**)**를 클릭합니다.

- 파일 및 악성코드 - 연결에서 탐지되거나 차단된 악성코드를 포함한 파일을 보려면 **View Files(**파일 보기**)**을 클릭하고 연결 내에서 탐지된 파일 및 악성코드 보기, 801 페이지에 설명된 대로 계속합니다.

- 침입 이벤트 - 연결에 연결된 침입과 우선 순위 및 영향을 보려면 **Intrusion Events(**침입 이벤트**)** 열에서 **Intrusion Events(**침입 이벤트**)**을 클릭하고 연결과 관련된 침입 이벤트 보기, 802 페이지에 설명된 대로 계속합니다.

  팁 하나 이상의 연결에 연결된 침입, 파일 또는 악성코드 이벤트를 빠르게 보려면 테이블의 확인란을 사용하여 연결을 선택한 다음 **Jump to(**이동**)** 드롭다운 목록에서 적절한 옵션을 선택합니다. 액세스 제어 규칙 평가 전에 차단되기 때문에 보안 인텔리전스에 의해 차단된 연결에 연결된 파일 또는 침입이 없을 수도 있습니다. 연결을 차단하기보다는 모니터링하도록 보안 인텔리전스를 구성했다면 보안 인텔리전스 이벤트의 경우에만 이 정보를 볼 수 있습니다.

- 인증서 - 연결을 암호화하는 데 사용할 수 있는 인증서에 대한 상세정보를 보려면 **SSL Status(SSL** 상태**)** 열에서 **Enabled Lock(**활성화된 잠금**)**을 클릭합니다.

- 제한 - 표시되는 열을 제한하려면 숨기려는 열 머리글의 **Close(**닫기**)** (✕)을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 확인 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 검색 제약 조건을 확장한 다음 Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 이벤트 삭제 - (보안 관련 연결 이벤트 테이블만 해당) 현재 제한된 보기에서 일부 또는 모든 항목을 삭제하려면 삭제할 항목 옆의 확인란을 선택한 다음 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다.
- 드릴다운 - 드릴다운 페이지 사용, 697 페이지 참조.

  팁 로깅된 연결과 일치한 여러 모니터 규칙 중 하나를 사용하여 드릴다운하려면 *N* **Monitor Rules** 값을 클릭합니다. 표시되는 팝업 창에서 연결 이벤트를 제한하는 데 사용할 모니터 규칙을 클릭합니다.

- 이 페이지 탐색 - 워크플로 페이지 이동 툴, 695 페이지 참조.
- 페이지 간 이동 - 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 이벤트 보기 간 이동 - 다른 이벤트 보기로 이동하여 연결된 이벤트를 보려면 **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.
- 정렬 - 워크플로의 데이터를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.

관련 항목

개요: 워크플로, 679 페이지
이벤트 보기 구성, 210 페이지

연결 내에서 탐지된 파일 및 악성코드 보기

파일 정책과 하나 이상의 액세스 제어 규칙을 연결할 경우, 시스템은 일치하는 트래픽에서 파일(악성코드 포함)을 탐지할 수 있습니다. 이러한 규칙에 의해 로깅된 연결과 연결된 파일 이벤트(있는 경우)를 보려면 Analysis(분석) > Connections(연결) 메뉴 옵션을 사용하십시오. Secure Firewall Management Center에서는 파일 목록 대신 **Files(**파일**)** 열에 파일 보기()를 표시합니다. 파일 보기의 숫자는 해당 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수를 나타냅니다.

모든 파일 및 악성코드 이벤트가 연결에 연결되는 것은 아닙니다. 구체적으로 말씀드리면,

- AMP for Endpoints가 탐지하는 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")는 연결에 연결되지 않습니다. 이러한 이벤트는 AMP for Endpoints 구축에서 가져옵니다.
- 많은 IMAP 지원 이메일 클라이언트는 사용자가 애플리케이션을 종료해야 종료되는 단일 IMAP 세션을 사용합니다. long-running 연결은 시스템에 의해 로깅되지만 세션에서 다운로드된 파일은 세션이 종료될 때까지 연결에 연결되지 않습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**) > Connections(**연결**)**로 이동하여 관련 옵션을 선택합니다.

단계 **2** 연결 이벤트 테이블을 사용할 때 **View Files(**파일 보기**)**를 클릭합니다.
연결에서 탐지된 파일 목록과 그 유형 및 (해당되는 경우) 악성코드 속성이 포함된 팝업 창이 표시됩니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 보기 - 파일 이벤트의 테이블 보기를 보려면 파일의 **View(**보기**)**를 클릭합니다.
- 보기 - 악성코드 이벤트의 테이블 보기에서 세부 사항을 보려면 악성코드 악성코드 파일의 **View(**보기**)**를 클릭합니다.
- 추적 - 네트워크를 통한 파일의 전송을 추적하려면 파일의 **Trajectory(**경로 전송**)**를 클릭합니다.
- 보기 - AMP for Networks에 의해 탐지된 모든 연결의 탐지된 파일 또는 악성코드 이벤트("네트워크 기반 악성코드 이벤트")의 세부 정보를 보려면 **View File Events(**파일 이벤트 보기**)** 또는 **View Malware Events(**악성코드 이벤트 보기**)**를 클릭합니다.

관련 항목

개요: 워크플로, 679 페이지
이벤트 보기 구성, 210 페이지

연결과 관련된 침입 이벤트 보기

침입 정책을 액세스 제어 규칙 또는 기본 작업과 연결할 경우, 시스템은 일치하는 트래픽에서 익스플로잇을 탐지할 수 있습니다. 로깅된 연결에 연결된 침입 이벤트(있는 경우)와 우선 순위 및 영향을 보려면 Analysis(분석) > Connections(연결) 메뉴 옵션을 사용하십시오.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**) > Connections(**연결**)**로 이동하여 관련 옵션을 선택합니다.

단계 **2** 연결 이벤트 테이블을 사용할 때 **Intrusion Events(**침입 이벤트**)** 열에서 **Intrusion Events(**침입 이벤트**)**를 클릭합니다.

단계 **3** 나타나는 팝업 창에서 다음 옵션을 이용할 수 있습니다.

- **Listed Event's View(**나열된 이벤트의 보기**)**를 클릭하여 패킷 보기에서 세부 정보를 확인합니다.
- **View Intrusion Events(**침입 이벤트 보기**)**를 클릭하여 연결에 연결된 모든 침입 이벤트에 대한 세부 정보를 봅니다.

관련 항목

개요: 워크플로, 679 페이지
이벤트 보기 구성, 210 페이지

암호화된 연결 인증서 상세정보

Analysis(분석) > Connections(연결) 메뉴 아래의 옵션을 사용하여 시스템이 처리하는 연결을 암호화하는 데 사용되는 공개 키 인증서(사용할 수 있는 경우)를 표시할 수 있습니다. 인증서에는 다음 정보가 포함됩니다.

표 ***96:*** 암호화된 연결 인증서 상세정보

속성	설명
Subject/Issuer Common Name(주체/발급자 공용 이름)	인증서 주체 또는 인증서 발급자의 호스트 및 도메인 이름입니다.
Subject/Issuer Organization(주체/발급자 조직)	인증서 주체 또는 인증서 발급자가 속한 조직입니다.
Subject/Issuer Organization Unit(주체/발급자 조직 단위)	인증서 주체 또는 인증서 발급자가 속한 조직 단위입니다.
Not Valid Before/After(유효기간)	인증서가 유효한 날짜입니다.
일련 번호	발급 CA가 할당한 일련번호입니다.
Certificate Fingerprint(인증서 지문)	인증서를 인증하는 데 사용되는 SHA 해시 값입니다.
Public Key Fingerprint(공개 키 지문)	인증서 내에 있는 공개 키를 인증하는 데 사용되는 SHA 해시 값입니다.

관련 항목

개요: 워크플로, 679 페이지
이벤트 보기 구성, 210 페이지

연결 요약 페이지 보기

Connection Summary(연결 요약) 페이지는 연결 이벤트에 대한 검색에 의해 제한되는 맞춤형 역할이 있고 Connection Summary(연결 요약) 페이지에 대한 명시적인 메뉴 기반 액세스 권한이 부여된 사용자에게만 표시됩니다. 이 페이지는 다양한 기준으로 구성된 모니터링되는 네트워크에서의 활동 그래프를 제공합니다. 예를 들어 Connections over Time 그래프에는 사용자가 선택한 간격 동안 모니터링되는 네트워크에서의 총 연결 수가 표시됩니다.

연결 요약 그래프에서는 연결 그래프에서 수행할 수 있는 작업을 거의 모두 동일하게 수행할 수 있습니다. 하지만 Connection Summary(연결 요약) 페이지의 그래프는 집계된 데이터를 기반으로 하기 때문에 그래프가 기반하는 개별 연결 이벤트를 검사할 수는 없습니다. 즉, 연결 요약 그래프에서는 연결 데이터 테이블 보기로 드릴다운할 수 없습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Connection Summary(**연결 요약**)**을(를) 선택합니다.

단계 **2** **Select Device(**디바이스 선택**)** 목록에서 요약을 보려는 디바이스를 선택하거나 **All(**모두**)**을 선택하여 모든 디바이스의 요약을 봅니다.

단계 **3** 연결 그래프를 조작하고 분석하려면 연결 이벤트 그래프 사용, 701 페이지에 설명된 대로 진행합니다.

팁 기본 시간 범위에 영향을 주지 않고 추가 분석을 수행할 수 있도록 연결 그래프를 분리하려면 **View(**보기**)**를 클릭합니다.

관련 항목

사용자 역할 에스컬레이션 활성화, 203 페이지

연결 및 보안 인텔리전스 이벤트 기록

기능	버전	세부 사항
새 연결 이벤트 이유 - 엘리펀트 플로우.	7.1	연결 이벤트 이유, 791 페이지의 내용을 참조하십시오.

기능	버전	세부 사항
NAT 변환 IP 주소 및 포트	7.1	연결 및 보안 인텔리전스 이벤트 테이블에 4개의 새로운 필드가 추가되었습니다. • NAT 소스 IP • NAT 대상 IP • NAT 소스 포트 • NAT 대상 포트
원격으로 저장된 특정 이벤트로 작업할 때 데이터 소스를 선택하는 기능	7.0	워크플로우 히스토리, 719 페이지의 내용을 참조하십시오.
DNS 필터링	7.0 6.7(베타 기능)	DNS 필터링이 활성화된 경우: • DNS Query(DNS 쿼리) 필드에는 DNS 필터링 일치와 관련된 도메인이 포함될 수 있습니다. • URL 필드가 비어 있더라도 DNS 쿼리, URL 범주 및 URL 평판에 값이 있는 경우, DNS 필터링 기능으로 인해 이벤트가 생성되고 범주 및 평판이 DNS 쿼리에 지정된 도메인에 적용됩니다. • Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *DNS* 필터링 및 이벤트 참고하십시오.
사용자 지정 테이블의 연결 이벤트 지원 제거	6.6	이제 연결 이벤트에 대한 사용자 지정 테이블을 생성할 수 없습니다. 업그레이드하는 경우, 연결 이벤트에 대한 기존 사용자 지정 테이블을 계속 사용할 수 있으나 결과가 항상 반환되지 않습니다. 다른 유형의 사용자 지정 테이블에는 변화가 없습니다. 신규/수정된 화면: **Analysis(분석) > Advanced(고급) > Custom Tables(사용자 지정 테이블)**의 Tables(테이블) 옵션 플랫폼: FMC
삭제 및 모든 연결 이벤트 삭제 기능 제거	6.6	삭제 및 모두 삭제 버튼이 연결 이벤트 테이블 페이지에서 제거되었습니다. 모든 연결 이벤트를 제거하려면 데이터 비우기 및 저장, 531 페이지의 내용을 참조하십시오. 신규/수정된 화면: **Analysis(분석) > Connections(연결) > Events(이벤트)** 플랫폼: FMC
VRF 및 SGT의 새 필드	6.6	• 인그레스 가상 라우터(시스템 로그: IngressVRF) • 이그레스 가상 라우터(시스템 로그: EgressVRF) • DestinationSecurityGroupType(시스템 로그만 해당) • SourceSecurityGroupType(시스템 로그만 해당)

기능	버전	세부 사항
신규 및 변경된 보안 그룹 태그 필드	6.5	FMC 웹 인터페이스의 필드 변경 사항: • 변경된 필드: 보안 그룹 태그가 소스 SGT로 변경 • 새 필드: 대상 SGT 시스템 로그 필드 변경 사항: • 변경된 필드: SecurityGroup이 SourceSecurityGroupTag로 변경 • 새 필드: • SourceSecurityGroup • DestinationSecurityGroup • DestinationSecurityGroupTag 지원되는 플랫폼: FMC 및 매니지드 디바이스
새 시스템 로그 필드: 이벤트 우선순위	6.5	이 필드는 침입, 파일, 악성코드 또는 보안 인텔리전스 이벤트와 연관된 연결 이벤트를 높은 우선순위로 식별합니다.
시스템 로그의 연결 이벤트 통합 식별자	6.4.0.4	다음 시스템 로그 필드는 연결 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 전체적으로 개별 식별합니다.

33 장

침입 이벤트

다음 주제에서는 침입 이벤트 작업 방법을 설명합니다.

침입 이벤트 정보

Firepower System을 사용하면 네트워크에서 호스트와 호스트 데이터의 가용성, 무결성 및 신뢰성에 영향을 줄 수 있는 트래픽을 모니터링할 수 있습니다. 주요 네트워크 세그먼트에 매니지드 디바이스를 배치하면 악의적인 활동을 위해 네트워크에서 이동하는 패킷을 검토할 수 있습니다. 시스템에는 공격자들이 개발한 광범위한 익스플로잇을 찾는 데 사용하는 몇 가지 메커니즘에 있습니다.

시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트(이전 용어인 'IPS 이벤트'라고 부르기도 함)를 생성합니다. 패킷 기반 이벤트의 경우 이벤트를 트리거한 패킷의 사본도 기록됩니다. 매니지드 디바이스는 Secure Firewall Management Center에 자체 이벤트를 전송합니다. 여기서는 집계된 데이터를 보고 네트워크 자산에 대한 공격을 더 잘 이해할 수 있습니다.

또한 매니지드 디바이스를 인라인, 스위치드 또는 라우티드 침입 시스템으로 구축할 수 있으며, 이를 통해 해로운 것으로 알려진 패킷을 삭제 또는 교체하도록 디바이스를 구성할 수도 있습니다.

침입 이벤트 검토 및 평가용 도구

다음 도구를 사용하여 침입 이벤트를 검토하고 네트워크 환경 및 보안 정책의 컨텍스트에서 중요성을 평가하는 데 필요한 도구를 제공합니다.

- 매니지드 디바이스에서 현재 활동을 검토할 수 있는 이벤트 요약 페이지
- 선택한 기간에 대해 생성할 수 있는 텍스트 기반 보고서와 그래프 보고서. 사용자는 자신만의 보고서를 계획하고 정해진 간격으로 실행되도록 구성할 수 있습니다.
- 공격과 관련된 이벤트 데이터를 수집하기 위해 사용할 수 있는 인시던트 처리 툴. 조사와 응답을 추적하는 데 도움이 되도록 메모를 추가할 수도 있습니다.
- SNMP, 이메일 및 시스템 로그를 위해 구성할 수 있는 자동화된 알림
- 특정 침입 이벤트에 대한 응답과 교정에 사용할 수 있는 자동화된 상관관계 정책
- 더 자세히 조사할 이벤트를 식별하기 위해 데이터에서 드릴다운할 수 있는 사전 정의 및 사용자 지정 워크플로
- 데이터 관리 및 분석을 위한 외부 툴. 시스템 로그 또는 eStreamer를 사용할 수 있습니다. 자세한 내용은 다음을 참조하십시오. 외부 툴을 사용하여 이벤트 분석, 641 페이지

또한 **Analysis(분석) > Advanced(고급) > Contextual Cross-Launch(상황별 크로스 실행)** 페이지에서 사전 정의된 리소스 등 공개적으로 이용 가능한 정보를 사용하여 악의적인 엔터티에 대해 자세히 알아볼 수 있습니다.

특정 메시지 문자열을 검색하고 이벤트를 생성한 규칙에 대한 설명서를 검색하려면 https://www.snort.org/rule_docs/을 참조하십시오.

침입 이벤트 라이선스 요구 사항

Threat Defense 라이선스

IPS

기본 라이선스

보호

침입 이벤트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

침입 이벤트 보기

침입 이벤트를 보고 네트워크 보안에 위협이 있는지 판단할 수 있습니다.

초기 침입 이벤트 보기는 페이지에 액세스하는 데 사용하는 워크플로에 따라 다릅니다. 하나 이상의 드릴다운 페이지, 침입 이벤트의 테이블 보기, 종료 패킷 보기 등 사전 정의 워크플로 중 하나를 사용할 수도 있고 자체 워크플로를 생성할 수도 있습니다. 침입 이벤트가 포함되어 있을 수 있는 맞춤형 테이블을 기반으로 하는 워크플로를 볼 수도 있습니다.

포함된 IP 주소가 많고 **Resolve IP Addresses(IP** 주소 확인**)** 이벤트 보기 설정을 활성화한 경우, 이벤트 보기가 표시되는 속도가 느려질 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 시간 범위 조정 - 타임 윈도우 변경, 710 페이지의 설명에 따라 이벤트 보기의 시간 범위를 조정합니다.
- 워크플로 변경 - 침입 이벤트 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용하는 경우, 워크플로 제목 옆에 있는 **(**워크플로 전환**)**를 클릭하여 시스템 제공 워크플로 중에서 선택합니다.
- 제한 - 분석에 중요한 침입 이벤트로 보기 범위를 좁히려면 침입 이벤트 워크플로 사용, 829 페이지를 참조하십시오.
- 이벤트 삭제 - 데이터베이스에서 이벤트를 삭제하려면 **Delete(**삭제**)**를 클릭하여 패킷을 보고 있는 이벤트를 삭제하거나 **Delete All(**모두 삭제**)**을 클릭하여 이전에 패킷을 선택한 모든 이벤트를 삭제합니다.
- 검토 표시 - 검토한 침입 이벤트에 표시하려면 검토된 침입 이벤트 표시, 824 페이지를 참조하십시오.
- 연결 데이터 보기 - 침입 이벤트에 연결된 연결 데이터를 보려면 침입 이벤트 관련 연결 데이터 보기, 824 페이지를 참조하십시오.

- 콘텐츠 보기 - 테이블에서 열의 콘텐츠를 보려면 침입 이벤트 필드, 810 페이지의 설명에 따릅니다.

관련 항목

침입 이벤트 패킷 보기 사용, 833 페이지

침입 이벤트 필드 정보

시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트를 생성합니다. 패킷 기반 이벤트의 경우 이벤트를 트리거한 패킷의 사본도 기록됩니다.

Secure Firewall Management Center 웹 인터페이스 **Analysis(**분석**) > Intrusions(**침입**) > Events(**이벤트**)**에서 침입 이벤트 데이터를 보거나 외부 도구에서 사용할 수 있도록 일부 필드에서 데이터를 syslog 메시지로 내보낼 수 있습니다. Syslog 필드는 아래 목록에 표시됩니다. 나열된 동등한 syslog가 없는 필드는 syslog 메시지에서 사용할 수 없습니다.

침입 이벤트를 검색할 때 개별 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다. 예를 들면 해독된 트래픽에 대해 트리거된 침입 이벤트에만 TLS/SSL 정보가 포함됩니다.

참고 Secure Firewall Management Center 웹 인터페이스에서 침입 이벤트 테이블 보기의 일부 필드는 기본적으로 비활성화되어 있습니다. 세션 기간 동안 필드를 활성화하려면 검색 제약 조건을 확장한 다음 **Disabled Columns(**비활성화된 열**)** 아래에서 열 이름을 클릭합니다.

침입 이벤트 필드

액세스 제어 정책**(**시스템 로그**: ACPolicy)**

이벤트를 생성한 침입, 프리프로세서 또는 디코더 규칙이 활성화된 침입 정책과 관련된 액세스 제어 정책.

액세스 제어 규칙**(**시스템 로그**: AccessControlRuleName)**

이벤트를 생성한 침입 정책을 호출한 액세스 제어 규칙. `Default Action(기본 작업)`은 규칙이 활성화된 침입 정책이 특정 액세스 제어 규칙과 연결되지 않았지만, 대신 액세스 제어 정책의 기본 작업으로 구성되었음을 나타냅니다.

다음의 경우 (또는 시스템 로그 메시지의 경우 생략됨) 이 필드는 비어 있습니다.

- 관련 규칙/기본 작업 없음: 침입 검사가 액세스 제어 규칙 및 기본 작업과 모두 연결되지 않은 경우(예: 시스템이 어떤 규칙을 적용할지를 결정하기 전에 반드시 통과해야 하는 것으로서 패킷 처리를 위해 지정된 침입 정책에 의해 검토된 경우) (이 정책은 액세스 제어 정책의 Advanced (고급) 탭에서 지정됩니다.)

- 관련 연결 이벤트 없음: 세션에 로깅된 연결 이벤트가 데이터베이스에서 삭제된 경우(예: 연결 이벤트가 침입 이벤트보다 턴오버가 높은 경우)

애플리케이션 프로토콜(시스템 로그: **ApplicationProtocol**)

침입 이벤트를 트리거한 트래픽에서 탐지된 호스트 간 통신을 나타내는 애플리케이션 프로토콜(사용 가능한 경우).

애플리케이션 프로토콜 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

애플리케이션 위험성

침입 이벤트를 트리거한 트래픽에서 탐지된 애플리케이션과 관련된 위험성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음) 또는 Very Low(매우 낮음). 연결에서 탐지된 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그 중 가장 높은 위험이 표시됩니다.

사업 타당성

침입 이벤트를 트리거한 트래픽에서 탐지된 애플리케이션과 관련된 비즈니스 연관성: Very High(매우 높음), High(높음), Medium(중간), Low(낮음) 또는 Very Low(매우 낮음). 연결에서 탐지된 각 애플리케이션 유형에는 관련된 비즈니스 연관성이 있습니다. 이 필드에는 그 중 가장 낮은(가장 연관성이 적은) 값이 표시됩니다.

분류(시스템 로그: **Classification**)

이벤트를 생성한 규칙이 속하는 분류

침입 이벤트 세부 정보에서 가능한 분류 값 목록을 참조하십시오.

이 필드를 검색하는 경우, 확인하려는 이벤트를 생성한 규칙의 분류 번호 또는 분류 이름이나 설명의 전체 또는 일부를 입력합니다. 쉼표로 구분된 숫자, 이름 또는 설명의 목록을 입력할 수도 있습니다. 마지막으로, 사용자 지정 분류를 추가하는 경우 이름이나 설명의 전체 또는 일부를 사용하여 검색할 수도 있습니다.

클라이언트(시스템 로그: **Client**)

침입 이벤트를 트리거한 트래픽에서 탐지된 모니터링되는 호스트에서 실행 중인 소프트웨어를 나타내는 클라이언트 애플리케이션(사용 가능한 경우).

클라이언트 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

Connection Counter (시스템 로그만 해당)

다른 동시 연결에서 하나의 연결을 구분하는 카운터입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

Connection Instance ID (시스템 로그만 해당)

연결 이벤트를 처리한 Snort 인스턴스입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

CVE ID

이 필드는 검색 전용입니다.

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(https://cve.mitre.org/)에서 취약성과 관련된 식별 번호에 의한 검색.

Destination Continent(대상 대륙)

침입 이벤트와 관련된 수신 호스트의 대륙.

Destination Country(대상 국가)

침입 이벤트와 관련된 수신 호스트의 국가.

Destination Host Criticality(대상 호스트 심각도)

이벤트가 생성될 때의 대상 호스트 심각도(해당 호스트에 대한 호스트 심각도 속성 값).

호스트의 심각도가 변경되어도 이 필드는 업데이트되지 않습니다. 그러나 새 이벤트에는 새로운 심각도 값이 적용됩니다.

대상 **IP**(시스템 로그: **DstIP**)

침입 이벤트와 관련된 수신 호스트가 사용하는 IP 주소.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 790 페이지도 참조하십시오.

대상 포트/**ICMP** 코드(시스템 로그: **DstPort, ICMPCode**)

트래픽을 수신하는 호스트의 포트 번호입니다. ICMP 트래픽에서 포트 번호가 없는 경우 이 필드에 ICMP 코드가 표시됩니다.

대상 사용자

연결 이벤트의 응답자 IP와 연결된 사용자 이름입니다. 이 호스트는 익스플로잇을 수신하는 호스트일 수도 있고 아닐 수도 있습니다. 이 값은 일반적으로 네트워크의 사용자에게만 알려져 있습니다.

선택합니다.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 790 페이지도 참조하십시오.

디바이스

액세스 제어 정책이 구축된 매니지드 디바이스입니다.

DeviceUUID (시스템 로그만 해당**)**

이벤트를 생성한 Firepower 디바이스의 고유 식별자입니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

도메인

침입을 탐지한 디바이스의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

이그레스 인터페이스**(**시스템 로그**: EgressInterface)**

이벤트를 트리거한 패킷의 이그레스 인터페이스. 패시브 인터페이스에 대해서는 이 인터페이스 열이 채워지지 않습니다.

이그레스 보안 영역**(**시스템 로그**: EgressZone)**

이벤트를 트리거한 패킷의 이그레스 보안 영역입니다. 패시브 구축에서는 이 보안 영역 필드가 채워지지 않습니다.

이그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에서 벗어날 때 사용하는 가상 라우터의 이름입니다.

이메일 첨부 파일

MIME Content-Disposition 헤더에서 추출된 MIME 첨부 파일 이름. 첨부 파일 이름을 표시하려면 SMTP 프리프로세서 **Log MIME Attachment Names** 옵션을 활성화해야 합니다. 여러 첨부 파일 이름이 지원됩니다.

Email Headers(이메일 헤더**)**

이 필드는 검색 전용입니다.

이메일 헤더에서 추출된 데이터입니다.

이메일 헤더를 SMTP 트래픽의 침입 이벤트와 연결하려면 SMTP 프리프로세서 **Log Headers(**헤더 로깅**)** 옵션을 활성화해야 합니다.

Email Recipient(이메일 수신자**)**

SMTP RCPT TO 명령에서 추출된 이메일 수신자의 주소. 이 필드의 값을 표시하려면 SMTP 프리프로세서 **Log To Addresses(**주소로 로깅**)** 옵션을 활성화해야 합니다. 여러 수신자 주소가 지원됩니다.

Email Sender(이메일 발신자**)**

SMTP MAIL FROM 명령에서 추출된 이메일 발신자의 주소. 이 필드의 값을 표시하려면 SMTP 프리프로세서 **Log From Addresses(**주소에서 로깅**)** 옵션을 활성화해야 합니다. 여러 발신자 주소가 지원됩니다.

첫 번째 패킷 시간 **(**시스템 로그만 해당**)**

시스템이 첫 번째 패킷을 수신한 시간입니다.

다음 필드 전부는 특정 침입 이벤트와 관련된 연결 이벤트(디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)를 개별적으로 식별합니다.

Generator(생성기**)**

이벤트를 생성한 구성 요소.

다음에 나오는 침입 이벤트 필드인 GID, Message(메시지) 및 Snort ID에 대한 정보도 참조하십시오.

GID(시스템 로그만 있음**)**

Generator ID(생성기 ID)로, 이벤트를 생성한 구성 요소의 ID.

다음에 나오는 침입 이벤트 필드인 Generator(생성기), Message(메시지) 및 Snort ID에 대한 정보도 참조하십시오.

HTTP Hostname(HTTP 호스트네임**)**

HTTP 요청 Host 헤더에서 추출된 호스트 이름(해당되는 경우). 요청 패킷에 항상 호스트 이름이 포함되는 것은 아닙니다.

호스트 이름을 HTTP 클라이언트 트래픽에 대한 침입 이벤트와 연결하려면 HTTP Inspect 프리프로세서 **Log Hostname(**호스트네임 로깅**)** 옵션을 활성화해야 합니다.

테이블 보기에서 이 열에는 추출된 호스트 이름의 첫 50자가 표시됩니다. 약식 호스트 이름의 표시된 부분 위로 마우스 포인터를 이동하여 최대 256바이트까지 전체 이름을 표시할 수 있습니다. 패킷 보기에서 전체 호스트 이름을 최대 256바이트까지 표시할 수 있습니다.

HTTP 응답 코드**(**시스템 로그**: HTTPResponse)**

이벤트를 트리거한 연결을 통해 클라이언트의 HTTP 요청에 대한 응답으로 전송된 HTTP 상태 코드.

HTTP URI

침입 이벤트를 트리거한 HTTP 요청 패킷과 연결된 원시 URI(있는 경우). 요청 패킷에 항상 URI가 포함되는 것은 아닙니다.

URI를 HTTP 트래픽에 대한 침입 이벤트와 연결하려면 HTTP Inspect 프리프로세서 **Log URI(URI** 로깅**)** 옵션을 활성화해야 합니다.

HTTP 응답에 의해 트리거된 침입 이벤트에서 연결된 HTTP URI를 보려면 **Perform Stream Reassembly on Both Ports(**양쪽 포트에서 스트림 리어셈블리 수행**)** 옵션에서 HTTP 서버를 구성해야 합니다. 그러나 이렇게 하면 트래픽 리어셈블리를 위한 리소스 수요가 증가합니다.

이 열에는 추출된 URI의 첫 50자가 표시됩니다. 약식 URI의 표시된 부분 위로 마우스 포인터를 이동하여 최대 2048바이트까지 전체 URI를 표시할 수 있습니다. 패킷 보기에서 전체 URI를 최대 2048바이트까지 표시할 수 있습니다.

영향

이 필드의 영향 레벨은 침입 데이터, 네트워크 검색 데이터 및 취약성 정보 사이의 상관 관계를 나타냅니다.

이 필드를 검색하는 경우 영향 아이콘이 색상 또는 부분 문자열을 지정하지 않습니다. 예를 들어, 파란색, 레벨 **1**또는 **0**을 사용하지 마십시오. 대/소문자 유효한 값은 다음과 같습니다.

- 영향 0, 영향 레벨 0
- 영향 1, 영향 레벨 1
- 영향 2, 영향 레벨 2
- 영향 3, 영향 레벨 3
- 영향 4, 영향 레벨 4

NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에 대해서는 운영 체제 정보가 제공되지 않으므로 시스템은 이러한 호스트와 관련된 침입 이벤트에 대해 취약함(영향 레벨 1: 빨강) 영향 레벨을 할당할 수 없습니다. 이러한 경우에는 호스트 입력 기능을 사용하여 호스트에 대한 운영 체제 ID를 수동으로 설정합니다.

인그레스 인터페이스**(**시스템 로그**: IngressInterface)**

이벤트를 트리거한 패킷의 인그레스 인터페이스입니다. 패시브 인터페이스에 대해서는 이 인터페이스 열만 채워집니다.

인그레스 보안 영역**(**시스템 로그**: IngressZone)**

이벤트를 트리거한 패킷의 인그레스 보안 영역 또는 터널 영역. 수동 배포에서는 이 보안 영역 필드만 입력됩니다.

인그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에 진입할 때 사용하는 가상 라우터의 이름입니다.

인라인 결과**(**시스템 로그**: InlineResult)**

워크플로 및 테이블 보기에서 이 필드는 다음 중 하나를 표시합니다.

표 ***97:*** 워크플로 및 테이블 보기에서 인라인 결과 필드 내용

아이콘	표시 내용
	시스템이 규칙을 트리거한 패킷을 삭제했음을 나타냅니다.
	(인라인 구축에서) **Drop when Inline(**인라인 시 삭제**)** 침입 정책 옵션을 활성화하는 경우 또는 시스템 정리 중 Drop and Generate(삭제 및 생성) 규칙이 이벤트를 생성한 경우 IPS가 패킷을 삭제했음을 나타냅니다.
	IPS가 패킷을 대상에 전송했거나 전달했을 수 있지만 이 패킷을 포함했던 연결은 이제 차단됩니다.
아이콘 없음(공란)	트리거된 규칙이 Drop and Generate Events(이벤트 삭제 및 생성)로 설정되지 않았음을 나타냅니다.

다음 테이블에는 인라인 결과의 가능한 이유(Would have dropped(삭제됨) 및 Partially dropped(부분적으로 삭제됨))가 나열되어 있습니다.

인라인 결과	원인	상세 이유
Would Have Dropped(삭제됨)	패시브 또는 탭 모드의 인터페이스	인터페이스를 인라인 탭 또는 패시브 모드로 구성했습니다.
	"Detection(탐지)" 검사 모드의 침입 정책	침입 정책에서 검사 모드를 Detection(탐지)로 설정했습니다.
	Connection Timed Out(연결 시간 초과)	TCP/IP 연결이 시간 초과되어 Snort 검사 엔진이 검사를 일시 중단했습니다.
Partially Dropped(부분적으로 삭제됨)	연결 닫힘(0x01)	새 플로우를 생성하는 동안 할당된 플로우가 허용되는 플로우 수보다 많은 경우 Snort 검사 엔진이 가장 최근에 사용된 플로우를 정리합니다.
	연결 닫힘(0x02)	Snort 검사 엔진을 다시 로드하면 메모리 조정이 발생하며 가장 최근에 사용된 플로우가 제거됩니다.
	연결 닫힘(0x04)	Snort 검사 엔진이 정상적으로 종료되면 엔진은 모든 활성 플로우를 제거합니다.

수동 구축에서 인라인 인터페이스가 탭 모드에 있는 경우를 포함하여 침입 정책의 규칙 상태 또는 인라인 삭제 작업에 상관없이 시스템은 패킷을 삭제하지 않습니다.

이 필드를 검색하는 경우 다음 중 하나를 입력합니다.

- **dropped** - 패킷이 인라인 구축에서 삭제되는지 여부를 지정합니다.
- **would have dropped** - 인라인 구축에서 패킷을 삭제하도록 침입 정책을 설정했다면 패킷이 삭제되었을 것인지를 지정합니다.
- **partially dropped** - 패킷을 대상으로 전송하거나 전달할지 지정하지만, 이 패킷이 들어 있는 연결은 이제 차단됩니다.

침입 정책 (시스템 로그: IntrusionPolicy)

이벤트를 생성한 침입, 프리프로세서 또는 디코더 규칙이 활성화된 침입 정책. 액세스 제어 정책에 대한 기본 작업으로 침입 정책을 선택할 수 있습니다. 또는 침입 정책을 액세스 제어 규칙과 연결할 수 있습니다.

IOC(시스템 로그: NumIOC)

침입 이벤트를 트리거한 트래픽이 연결과 관련된 호스트에 대해 IOC(indication of compromise)도 트리거했는지 여부.

이 필드를 검색하는 경우 **triggered**(트리거됨) 또는 **n/a**(해당 없음)를 지정합니다.

메시지(시스템 로그: Message)

이벤트에 대한 설명 텍스트 규칙 기반 침입 이벤트의 경우, 이벤트 메시지는 규칙에서 가져옵니다. 디코더 및 프리프로세서 기반 이벤트의 경우, 이벤트 메시지는 하드 코드됩니다.

Generator ID(GID), Snort ID(SID) 및 SID 버전(Revision)이 각 메시지 끝에 콜론으로 구분되는 숫자 형식으로 괄호안에 추가됩니다(GID:SID:version). 예: **(1:36330:2)**.

MITRE

클릭하여 해당 계층 내에서 MITRE 전략 및 기술의 전체 목록을 나타내는 모달을 표시할 수 있는 기술의 수입니다.

MPLS 레이블(시스템 로그: MPLS_Label)

이 침입 이벤트를 트리거한 패킷에 연결된 Multiprotocol Label Switching(다중 프로토콜 레이블 스위칭) 레이블.

네트워크 분석 정책(시스템 로그: NAPPolicy)

이벤드 생성과 관련된 네트워크 분석(해당되는 경우).

이 필드에는 추출된 URI의 첫 50자가 표시됩니다. 약식 URI의 표시된 부분 위로 마우스 포인터를 이동하여 최대 2048바이트까지 전체 URI를 표시할 수 있습니다. 패킷 보기에서 전체 URI를 최대 2048바이트까지 표시할 수 있습니다.

원본 클라이언트 **IP**

XFF(X-Forwarded-For), True-Client-IP 또는 맞춤 정의된 HTTP 헤더에서 추출된 원래 클라이언트 IP 주소.

이 필드의 값을 표시하려면 네트워크 분석 정책에서 HTTP 프리프로세서 **Extract Original Client IP Address(**원래 클라이언트 **IP** 주소 추출**)** 옵션을 활성화해야 합니다. 또한 네트워크 분석 정책에서 최대 6개의 맞춤형 클라이언트 IP 헤더를 지정할 수 있으며 시스템이 Original Client IP 이벤트 필드에 대한 값을 선택하는 우선순위 순서를 설정할 수 있습니다.

우선순위**(**시스템 로그**: Priority)**

Talos 인텔리전스 그룹에 따라 결정된 이벤트 우선순위. 우선순위는 `priority` 키워드의 값 또는 `classtype`키워드의 값에 해당합니다. 기타 침입 이벤트의 경우, 우선순위는 디코더 또는 프리프로세서에 의해 결정됩니다. 유효한 값은 high(높음), medium(중간) 및 low(낮음)입니다.

프로토콜**(**시스템 로그**: Protocol)**

Secure Firewall Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

http://www.iana.org/assignments/protocol-numbers에 열거된 대로 연결에 사용된 전송 프로토콜의 이름 또는 번호. 이것은 소스 및 대상 포트/ICMP 열과 관련된 프로토콜입니다.

검토자

이벤트를 검토한 사용자의 이름. 이 필드를 검색하는 경우, **`unreviewed`(**검토 안 함**)**를 입력하고 검토되지 않은 이벤트를 검색할 수 있습니다.

Revision(시스템 로그만 있음**)**

이벤트 생성에 사용된 서명의 버전.

다음에 나오는 침입 이벤트 필드인 Generator(생성기), GID, Message(메시지), SID 및 Snort ID에 대한 정보도 참조하십시오.

규칙 그룹

규칙 그룹의 전체 목록을 나타내는 모달을 표시하기 위해 클릭할 수 있는 비 MITRE 규칙 그룹의 수입니다.

보안 상황**(**시스템 로그**: Context)**

트래픽이 통과한 가상 방화벽 그룹을 식별하는 메타데이터입니다. 시스템은 다중 상황 모드의 ASA FirePOWER에 대해서만 이 필드에 내용을 입력합니다.

SID(시스템 로그만 있음**)**

이벤트를 생성하는 규칙의 서명 ID(Snort ID로도 알려짐).

다음에 나오는 침입 이벤트 필드인 Generator(생성기), GID, Message(메시지), Revision(개정) 및 Snort ID에 대한 정보도 참조하십시오.

Snort ID

이 필드는 검색 전용입니다.

(시스템 로그 필드에서 SID 참조).

검색을 수행하는 경우 이벤트를 생성한 규칙의 Snort ID(SID)를 지정합니다. 또는 선택적으로 규칙의 GID(Generator ID)와 SID 조합을 지정합니다. 여기서 GID와 SID는 GID:SID 형식으로 콜론(:)으로 구분됩니다. 다음 표에서 어떠한 값도 지정할 수 있습니다.

표 ***98: Snort ID*** 검색 값

값	예
단일 SID	10000
SID 범위	10000-11000
SID보다 큼	>10000
SID보다 크거나 같음	>=10000
SID보다 작음	<10000
SID보다 작거나 같음	<=10000
쉼표로 구분된 SID 목록	10000,11000,12000
단일 GID:SID 조합	1:10000
쉼표로 구분된 GID:SID 조합의 목록	1:10000,1:11000,1:12000
쉼표로 구분된 SID 및 GID:SID 조합의 목록	10000,1:11000,12000

보고 있는 이벤트의 SID가 Message(메시지) 열에 나열됩니다. 자세한 내용은 Message(메시지) 필드에 대한 이 섹션의 설명을 참조하십시오.

소스 대륙

침입 이벤트와 관련된 전송 호스트의 대륙.

소스 국가

침입 이벤트와 관련된 전송 호스트의 국가.

Source Criticality(소스 심각도**)**

이벤트가 생성될 때의 소스 호스트 심각도(해당 호스트에 대한 호스트 심각도 속성 값).

호스트의 심각도가 변경되어도 이 필드는 업데이트되지 않습니다. 그러나 새 이벤트에는 새로운 심각도 값이 적용됩니다.

소스 **IP**(시스템 로그**: SrcIP**)

침입 이벤트와 관련된 전송 호스트가 사용하는 IP 주소.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 790 페이지도 참조하십시오.

소스 포트**/ICMP** 유형(시스템 로그**: SrcPort, ICMPType**)

전송 호스트의 포트 번호. ICMP 트래픽에서 포트 번호가 없는 경우 이 필드에 ICMP 유형이 표시됩니다.

소스 사용자(시스템 로그**: User**)

연결을 시작한 호스트의 IP 주소와 연결된 사용자 이름으로, 익스플로잇의 소스 호스트일 수도 있고 아닐 수도 있습니다. 이 사용자 값은 일반적으로 네트워크의 사용자에게만 알려져 있습니다.

해당하는 경우 사용자 이름 앞에 `<realm>\`을 입력합니다.

SSL 실제 작업(시스템 로그**: SSLActualAction**)

Secure Firewall Management Center 웹 인터페이스에서 이 필드는 검색 필드로만 사용됩니다.

시스템이 암호화된 트래픽에 적용하는 작업.

차단/차단 및 재설정

차단된 암호화된 연결을 나타냅니다.

암호 해독(재서명)

다시 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

암호 해독(대체 키)

대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

암호 해독(알려진 키)

알려진 개인 키를 사용하여 암호 해독된 수신 연결을 나타냅니다.

기본 작업

연결이 기본 작업에 의해 처리되었음을 나타냅니다.

암호 해독 안 함

시스템이 암호 해독하지 않은 연결을 나타냅니다.

검색 워크플로 페이지의 **SSL Status**(**SSL** 상태) 필드에 필드값이 표시됩니다.

SSL 인증서 정보

이 필드는 검색 전용입니다.

트래픽 암호화에 사용하는 공개 키 인증서에 저장된 정보로 다음을 포함합니다.

- Subject/Issuer Common Name(대상자/발급자 공용 이름)

- Subject/Issuer Organization(대상자/발급자 기관)
- Subject/Issuer Organization Unit(대상자/발급자 기관 부서)
- Not Valid Before/After(유효기간)
- Serial Number(일련 번호)
- Certificate Fingerprint(인증서 지문)
- Public Key Fingerprint(공개 키 지문)

SSL Failure Reason(SSL 실패 이유)

이 필드는 검색 전용입니다.

시스템이 암호화된 트래픽의 암호 해독에 실패한 이유:

- Unknown(알 수 없음)
- No Match(일치하지 않음)
- Success(TLS 필수 성공)
- Uncached Session(캐시되지 않은 세션)
- Unknown Cipher Suite(알 수 없는 암호 그룹)
- Unsupported Cipher Suite(지원되지 않는 암호 그룹)
- Unsupported SSL Version(지원되지 않는 SSL 버전)
- SSL Compression Used(SSL 압축 사용됨)
- Session Undecryptable in Passive Mode(패시브 모드에서 세션 암호 해독 불가)
- Handshake Error(핸드셰이크 오류)
- Decryption Error(암호 해독 오류)
- Pending Server Name Category Lookup(서버 이름 카테고리 조회 보류 중)
- Pending Common Name Category Lookup(공용 이름 카테고리 조회 보류 중)
- Internal Error
- Network Parameters Unavailable(네트워크 파라미터 사용 불가)
- Invalid Server Certificate Handle(유효하지 않은 서버 인증서 처리)
- Server Certificate Fingerprint Unavailable(서버 인증서 지문 사용 불가)
- Cannot Cache Subject DN(대상자 DN 캐시 불가)
- Cannot Cache Issuer DN(발급자 DN 캐시 발가)
- Unknown SSL Version(알 수 없는 SSL 버전)

- External Certificate List Unavailable(외부 인증서 목록 사용 불가)
- External Certificate Fingerprint Unavailable(외부 인증서 지문 사용 불가)
- Internal Certificate List Invalid(내부 인증서 목록이 유효하지 않음)
- Internal Certificate List Unavailable(내부 인증서 목록 사용 불가)
- Internal Certificate Unavailable(내부 인증서 사용 불가)
- Internal Certificate Fingerprint Unavailable(내부 인증서 지문 사용 불가)
- Server Certificate Validation Unavailable(서버 인증서 검증 사용 불가)
- Server Certificate Validation Failure(서버 인증서 검증 장애)
- Invalid Action(유효하지 않은 작업)

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL 상태

암호화된 연결을 로깅한 **SSL Actual Action(SSL** 실제 작업**)**(해독 규칙, 기본 작업 또는 암호 해독이 불가능한 트래픽 작업)과 관련된 작업.

시스템이 암호화된 연결을 해독하지 못할 경우, 실행된 **SSL Actual Action(SSL** 실제 작업**)** (해독 불가능한 트래픽 작업)과 **SSL Failure Reason(SSL** 실패 이유**)**가 표시됩니다. 예를 들어, 시스템이 알 수 없는 암호 그룹으로 암호화된 트래픽을 탐지하고 추가 검사 없이 이를 허용할 경우 이 필드는 `Do Not Decrypt (Unknown Cipher Suite)(암호 해독 하지 않음(알려지지 않은 암호화 그룹))`로 표시됩니다.

인증서 세부사항을 보려면 잠금 아이콘을 클릭합니다.

이 필드를 검색할 때 **SSL Actual Action(SSL** 실제 작업**)** 중 하나 이상과 **SSL Failure Reason(SSL** 실패 이유**)**를 입력하고 시스템이 처리했거나 암호 해독에 실패한 암호화된 트래픽을 확인합니다.

SSL Subject/Issuer Country(SSL 대상자**/**발급자 국가**)**

이 필드는 검색 전용입니다.

암호화 인증서와 관련된 대상자 또는 발급자 국가의 2자 ISO 3166-1 alpha-2 국가 코드.

시간

이벤트의 날짜 및 시간. 이 필드는 검색할 수 없습니다.

VLAN ID (시스템 로그**: VLAN_ID)**

침입 이벤트를 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID

웹 애플리케이션**(**시스템 로그**: WebApplication)**

침입 이벤트를 트리거한 트래픽에서 탐지된 HTTP 트래픽의 내용 또는 요청된 URL을 나타내는 웹 애플리케이션.

HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 그 대신 일반 웹 브라우징 지정을 제공합니다.

웹 애플리케이션 카테고리 및 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

관련 항목

이벤트 검색, 721 페이지

침입 이벤트 영향 레벨

이벤트가 네트워크에 미치는 영향을 평가할 수 있도록 Secure Firewall Management Center는 침입 이벤트의 테이블 보기에 영향 레벨을 표시합니다. 각 이벤트에 대해 시스템은 침입 데이터, 네트워크 검색 데이터 및 취약성 정보 사이의 상관관계를 색으로 나타내는 영향 레벨 아이콘을 추가합니다.

참고 NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에 대해서는 운영 체제 정보가 제공되지 않으므로 시스템은 이러한 호스트와 관련된 침입 이벤트에 대해 취약함(영향 레벨 1: 빨강) 영향 레벨을 할당할 수 없습니다. 이러한 경우에는 호스트 입력 기능을 사용하여 호스트에 대한 운영 체제 ID를 수동으로 설정합니다.

다음 표에서는 영향 레벨의 가능한 값에 대해 설명합니다.

표 ***99:*** 영향 레벨

영향 레벨	취약성	색상	설명
Unknown(알 수 없음)(0)	알 수 없음	그레이	소스 호스트나 대상 호스트 모두 네트워크 검색에 의해 모니터링되는 네트워크에 없습니다.
Vulnerable(취약)(1)	취약함	빨간색	다음 중 하나에 해당합니다. • 소스 또는 대상 호스트가 네트워크 맵에 있으며, 취약성이 호스트에 매핑됨 • 소스 또는 대상 호스트가 바이러스, 트로이 목마 또는 기타 악성 소프트웨어에 감염되었을 가능성이 있음
Potentially Vulnerable(잠재적으로 취약)(2)	잠재적으로 취약함	오렌지	소스 또는 대상 호스트가 네트워크 맵에 있으며, 다음 중 하나가 참임: • 포트로 향하는 트래픽의 경우 포트가 서버 애플리케이션 프로토콜을 실행함 • 포트로 향하는 트래픽이 아닌 경우 호스트가 프로토콜을 사용함

영향 레벨	취약성	색상	설명
Currently Not Vulnerable(현재 취약하지 않음**)**(3)	현재 취약하지 않음	노란색	소스 또는 대상 호스트가 네트워크 맵에 있으며, 다음 중 하나가 참임: • 포트로 향하는 트래픽의 경우(예: TCP 또는 UDP), 포트가 열려 있지 않음 • 포트로 향하는 트래픽이 아닌 경우(예: ICMP), 호스트가 프로토콜을 사용하지 않음
Unknown Target(알 수 없는 대상**)**(4)	알 수 없는 대상	블루	소스 호스트 또는 대상 호스트가 모니터링되는 호스트에 있지만 네트워크 맵에는 호스트에 대한 항목이 없음.

침입 이벤트 관련 연결 데이터 보기

시스템은 침입 이벤트가 탐지된 연결을 로깅할 수 있습니다. 이 로깅은 액세스 제어 규칙과 연결된 침입 정책에 대해 자동으로 수행되지만, 기본 작업에 대한 관련 연결 데이터를 보려면 연결 로깅을 수동으로 활성화해야 합니다.

이벤트의 테이블 보기 간에 탐색할 때에는 관련된 데이터를 보는 것이 가장 유용합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 테이블의 확인란을 사용하여 침입 이벤트를 선택한 다음 **Jump to(**이동**)** 드롭다운 목록에서 **Connections(**연결**)**를 선택합니다.

팁 특정 연결에 연결된 침입 이벤트도 비슷한 방법으로 볼 수 있습니다. 자세한 내용은 워크플로 간 탐색, 716 페이지를 참고하십시오.

관련 항목

허용된 연결에 대한 로깅, 758 페이지
침입 이벤트 워크플로 사용, 829 페이지
연결 및 보안 관련 연결 이벤트 테이블 사용, 799 페이지

검토된 침입 이벤트 표시

침입 이벤트가 악의적이지 않다고 확신하면 이벤트를 검토한 것으로 표시할 수 있습니다.

침입 이벤트를 검토한 결과 네트워크 보안에 위협이 되지 않을 것으로 확신하는 경우(예: 네트워크의 호스트 중 어떤 것도 탐지된 익스플로잇에 취약하지 않음을 알고 있음) 해당 이벤트를 검토한 것으로 표시할 수 있습니다. 검토된 이벤트는 이벤트 데이터베이스에 저장되며 이벤트 요약 통계에 포함되지만, 기본 침입 이벤트 페이지에는 더 이상 나타나지 않습니다. 사용자 이름이 검토자로 표시됩니다.

다중 도메인 구축에서 이벤트를 검토된 것으로 표시하는 경우, 시스템은 해당 이벤트를 볼 수 있는 모든 도메인에서 이를 검토된 것으로 표시합니다.

백업을 수행한 후 검토한 침입 이벤트를 삭제하면, 백업의 복원은 삭제된 침입 이벤트를 복원하지만 검토된 상태는 복원하지 않습니다. 복원된 침입 이벤트는 **Reviewed Events(**검토된 이벤트**)**가 아니라 **Intrusion Events(**침입 이벤트**)**에서 볼 수 있습니다.

프로시저

침입 이벤트를 보여주는 페이지에는 두 가지 옵션이 있습니다.

- 이벤트 목록에서 하나 이상의 침입 이벤트를 표시하려면, 이벤트 옆의 확인란을 선택하고 **Review(**검토**)**를 클릭합니다.
- 이벤트 목록에서 모든 침입 이벤트를 표시하려 **Review All(**모두 검토**)**을 클릭합니다.

관련 항목

침입 이벤트 워크플로 사용, 829 페이지

이전에 검토된 침입 이벤트 보기

다중 도메인 구축에서 이벤트를 검토된 것으로 표시하는 경우, 시스템은 해당 이벤트를 볼 수 있는 모든 도메인에서 이를 검토된 것으로 표시합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Reviewed Events(**검토한 이벤트**)**을(를) 선택합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 타임 윈도우 변경, 710 페이지에 설명된 대로 시간 범위를 조정합니다.
- 침입 이벤트 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용하는 경우, 워크플로 제목 옆에 있는 **(**워크플로 전환**)**를 클릭하여 시스템 제공 워크플로 중에서 선택합니다.
- 표시되는 이벤트에 대한 자세한 내용은 침입 이벤트 필드, 810 페이지를 참조하십시오.

관련 항목

침입 이벤트 워크플로 사용, 829 페이지

검토된 침입 이벤트를 검토되지 않은 것으로 표시

이벤트를 검토하지 않은 것으로 표시함으로써 검토된 이벤트를 기본 침입 이벤트 보기로 되돌릴 수 있습니다.

다중 도메인 구축에서 이벤트를 검토된 것으로 표시하는 경우, 시스템은 해당 이벤트를 볼 수 있는 모든 도메인에서 이를 검토된 것으로 표시합니다.

프로시저

검토된 이벤트를 표시하는 페이지에는 두 가지 옵션이 있습니다.

- 검토된 이벤트 목록에서 개별 침입 이벤트를 제거하려면 특정 이벤트 옆의 확인란을 선택하고 **Unreview(**검토 취소**)**를 클릭합니다.
- 검토된 이벤트의 목록에서 모든 침입 이벤트를 제거하려면 **Unreview All(**모두 검토 취소**)**을 클릭합니다.

전처리기 이벤트

전처리기는 다음 두 가지 기능을 제공합니다. 패킷에서 지정된 작업을 수행하고(예를 들어 HTTP 트래픽 디코딩 및 표준화) 패킷이 전처리기 옵션을 트리거하고 연결된 전처리기 규칙이 활성화될 때마다 이벤트를 생성하여 지정된 전처리기 옵션의 실행을 보고하는 것입니다. 예를 들어 `Double Encoding(이중 인코딩)` HTTP 검사 옵션과 HTTP 검사 생성기(GID)가 119이고 Snort ID(SID)가 2인 연결된 전처리기 규칙을 활성화하여 전처리기에 IIS 이중 인코딩된 트래픽이 발생할 때 이벤트를 생성할 수 있습니다.

전처리기의 실행을 보고하는 이벤트를 생성하면 비정상적인 프로토콜 익스플로잇을 탐지하는 데 도움이 됩니다. 예를 들어 공격자는 중복 IP 프래그먼트를 조작하여 호스트에서 DoS 공격을 일으킬 수 있습니다. IP 조각 모음 전처리기는 이 유형의 공격을 탐지하고 이에 대한 침입 이벤트를 생성할 수 있습니다.

패킷 표시에 이벤트에 대한 자세한 규칙 설명이 포함되지 않는다는 점에서 전처리기 이벤트는 규칙 이벤트와 다릅니다. 대신 패킷 표시에는 이벤트 메시지, GID, SID, 패킷 헤더 데이터 및 패킷 페이로드가 나타납니다. 이를 통해 패킷의 헤더 정보를 분석하고, 헤더 옵션이 사용 중인지와 시스템을 악용할 수 있는지를 파악하고, 패킷 페이로드를 검사할 수 있습니다. 전처리기가 각 패킷을 분석한 후 규칙 엔진은 잠재적인 콘텐츠 수준 위협을 추가 분석하고 보고할 수 있도록 이에 대해 적절한 규칙을 실행합니다(전처리기가 이를 조각 모음하고 유효한 세션의 일부로 설정할 수 있는 경우).

전처리기 생성기 **ID**

각 전처리기에는 어떤 전처리기가 패킷에 의해 트리거되었는지를 나타내는 자체 GID(Generator ID)가 있습니다. 일부 전처리기에는 잠재적 공격을 분류하는 ID 번호인 관련 SID도 있습니다. 이를 통해 규칙의 Snort ID(SID)가 규칙을 트리거하는 패킷의 컨텍스트를 제공하는 것과 유사한 방식으로 이벤트의 유형을 카테고리화하여 이벤트를 더 효과적으로 분석할 수 있습니다. 침입 정책 Rules(규칙) 페이지의 Preprocessors(전처리기) 필터 그룹에서 전처리기별로 전처리기 규칙을 나열할 수 있습니다.

또한 Category(카테고리) 필터 그룹의 전처리기 및 패킷 디코더 하위 그룹에 전처리기 규칙을 나열할 수도 있습니다.

참고 표준 텍스트 규칙에 의해 생성된 이벤트는 생성기 ID 1(전역 도메인 또는 레거시 GID) 또는 1000 - 2000(하위 도메인)을 갖습니다. 공유 개체 규칙의 경우, 이벤트의 생성기 ID는 3입니다. 두 규칙 모두 이벤트의 SID는 트리거된 특정 규칙을 나타냅니다.

다음 표에서는 각 GID를 생성하는 이벤트 유형에 대해 설명합니다.

표 ***100:*** 생성기 ***ID***

ID	구성 요소	설명
1	표준 텍스트 규칙	패킷이 표준 텍스트 규칙(전역 도메인 또는 레거시 GID)을 트리거할 때 이벤트가 생성되었습니다.
2	태그가 지정된 패킷	태그 지정된 세션에서 패킷을 생성하는 Tag 생성기에 의해 이벤트가 생성되었습니다. 이는 `tag` 규칙 옵션이 사용될 때 발생합니다.
3	공유 개체 규칙	패킷이 공유 개체 규칙을 트리거할 때 이벤트가 생성되었습니다.
102	HTTP 디코더	디코더 엔진이 패킷 내에서 HTTP 데이터를 디코딩했습니다.
105	Back Orifice 탐지기	Back Orifice 탐지기가 패킷에 연결된 Back Orifice 공격을 식별했습니다.
106	RPC 디코더	RPC 디코더가 패킷을 디코딩했습니다.
116	패킷 디코더	패킷 디코더에 의해 이벤트가 생성되었습니다.
119, 120	HTTP 검사 전처리기	HTTP 검사 전처리기에 의해 이벤트가 생성되었습니다. GID 120 규칙은 서버별 HTTP 트래픽과 관련이 있습니다.
122	포트스캔 탐지기	포트스캔 플로우 디코더에 의해 이벤트가 생성되었습니다.
123	IP 조각 모음기	조각난 IP 데이터그램을 제대로 리어셈블할 수 없을 때 이벤트가 생성되었습니다.
124	SMTP 디코더	SMTP 전처리기가 SMTP 동사에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.
125	FTP 디코더	FTP/텔넷 디코더가 FTP 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.
126	텔넷 디코더	FTP/텔넷 디코더가 텔넷 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.
128	SSH 전처리기	SSH 전처리기가 SSH 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.

ID	구성 요소	설명
129	스트림 전처리기	스트림 전처리기에 의한 스트림 전처리 중에 이벤트가 생성되었습니다.
131	DNS 전처리기	DNS 전처리기에 의해 이벤트가 생성되었습니다.
133	DCE/RPC 전처리기	DCE/RPC 전처리기에 의해 이벤트가 생성되었습니다.
134	규칙 레이턴시 패킷 레이턴시	규칙 레이턴시가 침입 규칙의 그룹을 일시 중지(134:1) 또는 다시 활성화(134:2)하거나 패킷 레이턴시 임계값이 초과되었기 때문에 시스템이 패킷 검사를 중지하여(134:3) 이벤트가 생성되었습니다.
135	속도 기반 공격 탐지기	속도 기반 공격 탐지기가 네트워크의 호스트에 대한 과도한 연결을 식별하여 이벤트가 생성되었습니다.
137	SSL 전처리기	TLS/SSL 전처리기에 의해 이벤트가 생성되었습니다.
138, 139	민감한 데이터 전처리기	민감한 데이터 전처리기에 의해 이벤트가 생성되었습니다.
140	SIP 전처리기	SIP 전처리기에 의해 이벤트가 생성되었습니다.
141	IMAP 전처리기	IMAP 전처리기에 의해 이벤트가 생성되었습니다.
142	POP 전처리기	POP 전처리기에 의해 이벤트가 생성되었습니다.
143	GTP 전처리기	GTP 전처리기에 의해 이벤트가 생성되었습니다.
144	Modbus 전처리기	Modbus SCADA 전처리기에 의해 이벤트가 생성되었습니다.
145	DNP3 전처리기	DNP3 SCADA 전처리기에 의해 이벤트가 생성되었습니다.
148	CIP 전처리기	CIP SCADA 전처리기에 의해 이벤트가 생성되었습니다.
149	S7Commplus 전처리기	Modbus SCADA 전처리기에 의해 이벤트가 생성되었습니다.
1000 - 2000	표준 텍스트 규칙	패킷이 표준 텍스트 규칙(하위 도메인)을 트리거할 때 이벤트가 생성되었습니다.

침입 이벤트 워크플로 페이지

현재 침입 정책에서 활성화된 전처리기, 디코더 및 침입 규칙은 모니터링하는 트래픽이 정책을 위반할 때마다 침입 이벤트를 생성합니다.

Firepower System은 이벤트 데이터로 채워치고 침입 이벤트를 보고 분석할 수 있는 사전 정의된 워크플로 집합을 제공합니다. 이러한 각 워크플로는 평가할 침입 이벤트를 정확히 찾아낼 수 있도록 일련의 페이지를 통해 사용자를 안내합니다.

사전 정의된 침입 이벤트 워크플로에는 세 가지 페이지 유형 또는 이벤트 보기가 포함되어 있습니다.

- 하나 이상의 드릴다운 페이지

- 침입 이벤트의 테이블 보기
- 패킷 보기

*Drill-down(*드릴다운*)* 페이지에는 일반적으로 한 테이블(일부 드릴다운 보기의 경우 둘 이상의 테이블)에 하나의 특정 정보 유형을 볼 수 있는 둘 이상의 열이 포함되어 있습니다.

하나 이상의 대상 포트에 대한 추가 정보를 찾기 위해 "드릴다운"할 때 자동으로 이러한 이벤트를 선택하게 되며, 워크플로의 다음 페이지가 나타납니다. 이런 식으로 드릴다운 테이블은 한 번에 분석하는 이벤트 수를 줄입니다.

침입 이벤트의 초기 테이블 보기에서는 각 침입 이벤트가 고유한 행에 나열됩니다. 테이블의 열에는 시간, 소스 IP 주소와 포트, 대상 IP 주소와 포트, 이벤트 우선순위, 이벤트 메시지 등의 정보가 나열됩니다.

워크플로에서 이벤트를 선택하고 다음 페이지를 표시하는 대신, 테이블 보기에서 이벤트를 선택하면 제약 조건이라는 것이 추가됩니다. 제약 조건이란 분석할 이벤트 유형에 적용하는 제한입니다.

예를 들어 임의의 열에서 **Close(**닫기**)** (✕)을 클릭하고 드롭다운 목록에서 **Time(**시간**)**을 지우면 열 중 하나로 Time(시간)을 제거할 수 있습니다. 분석에서 이벤트 목록을 좁히려면 테이블 보기의 행 중 하나에서 값의 링크를 클릭할 수 있습니다. 예를 들어 소스 IP 주소 중 하나(잠재적인 공격자)에서 생성되는 이벤트로 분석을 제한하려면 **Source IP Address(**소스 **IP** 주소**)** 열에서 해당 IP 주소를 클릭합니다.

테이블 보기에서 하나 이상의 행을 선택한 다음 **View(**보기**)**를 클릭하면 패킷 보기가 나타납니다. 패킷 보기는 규칙을 트리거한 패킷 또는 이벤트를 생성한 전처리기에 대한 정보를 제공합니다. 패킷 보기의 각 섹션에는 패킷의 특정 레이어에 대한 정보가 포함되어 있습니다. 더 많은 정보를 보려면 축소된 섹션을 확장할 수 있습니다.

참고 각 포트스캔 이벤트는 여러 패킷에 의해 트리거되므로, 포트스캔 이벤트는 패킷 보기의 특수 버전을 사용합니다.

미리 정의된 워크플로가 특정 요구 사항을 충족하지 않는 경우, 관심 있는 정보만 표시되는 맞춤형 워크플로를 만들 수 있습니다. 맞춤형 침입 이벤트 워크플로에는 드릴 다운 페이지나 이벤트의 테이블 보기 또는 둘 다가 포함될 수 있습니다. 시스템은 자동으로 패킷 페이지를 마지막 페이지로 포함합니다. 이벤트를 조사하려는 방법에 따라 사전 정의 워크플로와 맞춤형 워크플로 간에 손쉽게 전환할 수 있습니다.

침입 이벤트 워크플로 사용

이벤트의 드릴다운 보기 및 테이블 보기에는 몇 가지 공통된 기능이 있습니다. 이러한 기능을 사용하면 이벤트 목록의 범위를 좁히고 관련 이벤트의 그룹으로 분석을 집중할 수 있습니다.

서로 다른 워크플로 페이지에 동일한 침입 이벤트가 표시되지 않도록, 시간 범위는 다른 이벤트 페이지를 표시하기 위해 페이지 아래쪽에서 링크를 클릭할 때 일시 중지되고, 후속 페이지에서 다른 작업을 수행하기 위해 클릭할 때 다시 시작됩니다.

팁 프로세스의 어떤 지점에서든 제약 조건을 검색 기준 집합으로 저장할 수 있습니다. 예를 들어 지난 며칠 동안 네트워크가 단일 IP 주소의 공격자에 의해 프로브된 것을 발견한 경우, 조사 중에 제약 조건을 저장한 다음 나중에 다시 사용할 수 있습니다. 그러나 복합 제약 조건을 검색 기준 집합으로 저장할 수는 없습니다.

프로시저

단계 **1** **Analysis**(분석) > **Intrusions**(침입) > **Events**(이벤트)를 사용하여 침입 이벤트 워크플로에 액세스합니다.

단계 **2** 원하는 경우, 침입 이벤트 드릴다운 페이지 제약 조건, 831 페이지 또는 침입 이벤트 테이블 보기 제약 조건, 832 페이지에 설명된 대로 이벤트 보기에 나타나는 침입 이벤트 수를 제한합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 표시되는 열에 대한 자세한 내용은 침입 이벤트 필드, 810 페이지를 참조하십시오.
- 호스트의 프로파일을 보려면 호스트 IP 주소 옆에 표시되는 **Host Profile**(호스트 프로파일)을 클릭합니다.
- 지리위치 세부 사항을 보려면 Source Country(소스 국가) 또는 Destination Country(대상 국가) 열에 표시되는 플래그를 클릭합니다.
- Firepower 시스템 외부에서 이용할 수 있는 소스의 데이터를 보려면 이벤트 값에서 마우스 오른쪽 버튼으로 클릭합니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지 섹션을 참조해 주십시오.
- 이벤트에 대한 일반 정보를 수집하려면 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지를 참고하십시오.
- 표시된 이벤트의 시간 및 날짜 범위를 수정하려면 타임 윈도우 변경, 710 페이지를 참조하십시오.

  팁 이벤트 보기에 침입 이벤트가 나타나지 않는 경우 지정된 기간을 조정하면 결과가 반환될 수 있습니다. 더 오래된 시간 범위를 지정한 경우, 해당 시간 범위의 이벤트가 삭제되었을 수 있습니다. 규칙 임계값 지정 구성을 조정하면 이벤트가 생성될 수 있습니다.

  참고 어플라이언스의 구성된 기간(전역 또는 이벤트 전용 모두 해당)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

- 현재 워크플로 페이지에서 이벤트를 정렬하거나 현재 워크플로 페이지 내에서 이동하려면 워크플로 사용, 689 페이지을 참조하십시오.
- 현재 제약 조건을 유지하면서 현재 워크플로의 페이지 사이를 이동하려면 워크플로 페이지의 왼쪽 위에서 해당 페이지 링크를 클릭합니다.
- 이벤트 데이터베이스에서 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택한 다음 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다.
- 이벤트를 검토된 것으로 표시하여 침입 이벤트 페이지에서는 제거하되 이벤트 데이터베이스에서는 제거하지 않으려면 검토된 침입 이벤트 표시, 824 페이지을 참조하십시오.
- 선택된 각 이벤트를 트리거한 패킷의 로컬 사본(libpcap 형식의 패킷 캡처 파일)을 다운로드하려면 다운로드하려는 패킷이 트리거한 이벤트 옆의 확인란을 선택한 다음 **Download Packets(**패킷 다운로드**)**를 클릭하거나 **Download All Packets(**모든 패킷 다운로드**)**를 클릭합니다. 캡처된 패킷은 libpcap 형식으로 저장됩니다. 이 형식은 여러 인기 있는 프로토콜 분석기에서 사용됩니다.
- 다른 이벤트 보기로 이동해 연결된 이벤트를 보려면 워크플로 간 탐색, 716 페이지을 참조하십시오.
- 다른 워크플로우를 임시로 사용하려면 **(**워크플로우 전환**)**를 클릭합니다.
- 빠르게 돌아올 수 있도록 현재 페이지를 즐겨찾기하려면 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다.
- Summary Dashboard(요약 대시보드)의 Intrusion Events(침입 이벤트) 섹션을 보려면 **Dashboards(**대시보드**)**를 클릭합니다.
- 즐겨찾기 관리 페이지로 이동하려면 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다.
- 현재 보기의 데이터를 기반으로 보고서를 생성하려면 이벤트 보기에서 보고서 템플릿 생성, 546 페이지을 참조하십시오.

관련 항목

이벤트 검색, 721 페이지
북마크, 717 페이지

침입 이벤트 드릴다운 페이지 제약 조건

다음 표에서는 드릴다운 페이지를 사용하는 방법에 대해 설명합니다.

표 ***101:*** 드릴다운 페이지에서 이벤트 제한

목적	방법
다음 워크플로 페이지로 드릴다운하여 특정 값으로 제한	값을 클릭 합니다. 예를 들어 Destination Port(대상 포트) 워크플로에서 대상 포트 80으로 이벤트를 제한하려면 **DST Port/ICMP Code(DST** 포트**/ICMP** 코드**)** 열에서 **80/tcp**를 클릭합니다. 워크플로의 다음 페이지인 Events(이벤트)가 나타나고, 포트 80/tcp 이벤트만 포함됩니다.
다음 워크플로 페이지로 드릴다운하여 선택한 이벤트로 제한	다음 워크플로 페이지에서 보려는 이벤트 옆에 있는 확인란을 선택하고 **View(**보기**)**를 클릭합니다. 예를 들어 Destination Port(목적지 포트) 워크플로에서 목적지 포트 20/tcp 및 21/tcp로 이벤트를 제한하려면 해당 포트의 행 옆에 있는 확인란을 선택하고 **View(**보기**)**를 클릭합니다. 워크플로의 다음 페이지인 Events(이벤트)가 나타나고, 포트 20/tcp 및 21/tcp 이벤트만 포함됩니다. 여러 행으로 제한하려는 경우 테이블에 열이 두 개 이상이면(Count 열은 포함하지 않음) 복합 제약 조건을 구축해야 합니다. 복합 제약 조건은 의도한 것보다 더 많은 이벤트가 제약 조건에 포함되지 않도록 보장합니다. 예를 들어 Event and Destination(이벤트 및 목적지) 워크플로를 사용하는 경우 첫 번째 드릴다운 페이지에서 선택하는 각 행은 복합 제약 조건을 생성합니다. 목적지 IP 주소가 10.10.10.100인 이벤트 1:100을 선택하고 목적지 IP 주소가 192.168.10.100인 이벤트 1:200도 선택하는 경우, 복합 제약 조건은 1:100을 이벤트 유형으로, 192.168.10.100을 목적지 IP 주소로 포함하는 이벤트 또는 1:200을 이벤트 유형으로, 10.10.10.100을 목적지 IP 주소로 포함하는 이벤트도 선택되지 않도록 합니다.
현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운	**View All(**모두 보기**)**를 클릭합니다.

침입 이벤트 테이블 보기 제약 조건

다음 표에서는 테이블 보기를 사용하는 방법에 대해 설명합니다.

표 ***102:*** 이벤트의 테이블 보기에서 이벤트 제한

목적	방법
단일 속성이 있는 이벤트로 보기를 제한	속성을 클릭합니다. 예를 들어 목적지 포트가 80인 이벤트로 보기를 제한하려면 **DST Port/ICMP Code(DST** 포트**/ICMP** 코드**)** 열에서 **80/tcp**를 클릭합니다.
테이블에서 열 제거	숨기려는 열 머리글에서 **Close(**닫기**)** (✕)을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다. 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 확장 화살표를 클릭하여 검색 제약 조건을 확장한 다음, **Disabled Columns(**비활성화된 열**)** 아래에서 열 이름을 클릭합니다.

목적	방법
하나 이상의 이벤트에 연결된 패킷 보기	다음 중 하나: • 패킷을 보려는 이벤트 옆에 있는 아래쪽 화살표를 클릭합니다. • 패킷을 보려는 하나 이상의 이벤트를 선택하고 페이지 아래쪽에서 **View(**보기**)**를 클릭합니다. • 페이지 아래쪽에서, 현재 제약 조건과 일치하는 모든 이벤트에 대한 패킷을 보려면 **View All(**모두 보기**)**을 클릭합니다.

침입 이벤트 패킷 보기 사용

패킷 보기는 침입 이벤트를 생성한 규칙을 트리거한 패킷에 대한 정보를 제공합니다.

팁 이벤트를 탐지한 디바이스에 대해 **Transfer Packet(**패킷 전송**)** 옵션이 비활성화된 경우 Secure Firewall Management Center의 패킷 보기에는 패킷 정보가 포함되지 않습니다.

패킷 보기는 패킷이 트리거한 침입 이벤트에 대한 정보를 제공함으로써 특정 패킷이 캡처된 이유를 나타냅니다. 그러한 정보에는 이벤트의 타임스탬프, 메시지, 분류, 우선순위가 포함되며, 이벤트가 표준 텍스트 규칙에 의해 생성된 경우 이벤트를 생성한 규칙도 포함됩니다. 패킷 보기는 또한 크기를 비롯한 패킷에 대한 일반 정보도 제공합니다.

패킷 보기에는 데이터 링크, 네트워크, 전송 등 패킷의 각 레이어에 대해 설명하는 섹션은 물론, 패킷을 구성하는 바이트에 대해 설명하는 섹션도 있습니다. 시스템이 패킷을 해독하면 해독된 바이트를 볼 수 있습니다. 자세한 정보를 보려면 축소된 섹션을 확장할 수 있습니다.

참고 각 포트스캔 이벤트는 여러 패킷에 의해 트리거되므로, 포트스캔 이벤트는 패킷 보기의 특수 버전을 사용합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** 침입 이벤트의 테이블 보기에서 침입 이벤트 테이블 보기 제약 조건, 832 페이지에 설명된 대로 볼 패킷을 선택합니다.

단계 **2** 필요에 따라 하나 이상의 이벤트를 선택한 경우, 페이지 하단의 페이지 번호를 사용하여 패킷 보기에서 페이지를 전환할 수 있습니다.

단계 **3** 다음과 같은 옵션이 있습니다.

- 조정 - 패킷 보기에서 날짜 및 시간 범위를 수정하려면 타임 윈도우 변경, 710 페이지를 참조하십시오.
- 구성 - 이벤트를 트리거한 침입 규칙을 구성하려면 Actions(작업) 옆의 화살표를 클릭하고 패킷 보기 내 침입 규칙 설정, 837 페이지에 설명된 대로 계속합니다.
- 삭제 - 데이터베이스에서 이벤트를 삭제하려면 **Delete(**삭제**)**를 클릭하여 패킷을 보고 있는 이벤트를 삭제하거나 **Delete All(**모두 삭제**)**을 클릭하여 이전에 패킷을 선택한 모든 이벤트를 삭제합니다.
- 다운로드 - 이벤트를 트리거한 패킷의 로컬 사본(libpcap 형식의 패킷 캡처 파일)을 다운로드하려면 **Download Packet(**패킷 다운로드**)**을 클릭하여 보고 있는 이벤트의 캡처된 패킷 사본을 저장하거나 **Download All Packets(**모든 패킷 다운로드**)**를 클릭하여 패킷을 이전에 선택한 모든 이벤트의 캡처된 패킷 사본을 저장합니다. 캡처된 패킷은 libpcap 형식으로 저장됩니다. 이 형식은 여러 인기 있는 프로토콜 분석기에서 사용됩니다.

  참고 단일 포트스캔 이벤트는 여러 패킷을 기반으로 하기 때문에 포트스캔 패킷을 다운로드할 수 없습니다. 그러나 포트스캔 보기는 사용할 만한 모든 패킷 정보를 제공합니다. 다운로드하려면 사용 가능한 디스크 공간이 15% 이상 남아 있어야 합니다.

- 검토 표시 - 이벤트를 검토된 것으로 표시하여 이벤트 보기에서는 제외하되 이벤트 데이터베이스에서는 제외하지 않으려면 **Review(**검토**)**를 클릭하여 패킷을 보고 있는 이벤트를 표시하거나 **Review All(**모두 검토**)**을 클릭하여 이전에 패킷을 선택한 모든 이벤트를 표시합니다. 자세한 내용은 검토된 침입 이벤트 표시, 824 페이지를 참고하십시오.
- 추가 정보 보기 - 페이지 섹션을 확장하거나 축소하려면 섹션 옆에 있는 화살표를 클릭합니다. 자세한 내용은 이벤트 정보 필드, 834 페이지, 프레임 정보 필드, 841 페이지, 데이터 링크 레이어 정보 필드, 842 페이지을 참조하십시오.
- 네트워크 레이어 정보 보기 - 네트워크 레이어 정보 보기, 843 페이지를 참조하십시오.
- 패킷 바이트 정보 보기 - 패킷 바이트 정보 보기, 848 페이지를 참조하십시오.
- 전송 레이어 정보 보기 - 다음 참조 전송 레이어 정보 보기, 845 페이지

관련 항목

포트스캔 탐지

이벤트 정보 필드

패킷 보기에서는 Event Information(이벤트 정보) 섹션에서 패킷에 대한 정보를 볼 수 있습니다.

Event(이벤트**)**

이벤트 메시지입니다. 규칙 기반 이벤트의 경우에는 규칙 메시지에 해당합니다. 다른 이벤트의 경우에는 디코더 또는 전처리기에 의해 결정됩니다.

이벤트의 ID는 (GID:SID:Rev) 형식으로 메시지에 추가됩니다. GID는 이벤트를 생성한 규칙 엔진, 디코더 또는 전처리기의 생성자 ID입니다. SID는 규칙, 디코더 메시지 또는 전처리기 메시지의 식별자입니다. Rev는 규칙의 개정 번호입니다.

타임스탬프

패킷이 캡처된 시간(UTC 시간대)입니다.

분류

이벤트 분류입니다. 규칙 기반 이벤트의 경우 규칙 분류에 해당합니다. 다른 이벤트의 경우에는 디코더 또는 전처리기에 의해 결정됩니다.

우선순위

이벤트 우선순위입니다. 규칙 기반 이벤트의 경우 `priority` 키워드의 값 또는 `classtype` 키워드의 값에 해당합니다. 다른 이벤트의 경우에는 디코더 또는 전처리기에 의해 결정됩니다.

인그레스 보안 영역

이벤트를 트리거한 패킷의 인그레스 보안 영역입니다. 수동 배포에서는 이 보안 영역 필드만 입력됩니다.

이그레스 보안 영역

이벤트를 트리거한 패킷의 이그레스 보안 영역입니다. 패시브 구축에서는 이 필드가 채워지지 않습니다.

도메인

매니지드 디바이스가 속한 도메인입니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

디바이스

액세스 제어 정책이 구축된 매니지드 디바이스입니다.

보안 상황

트래픽이 통과한 가상 방화벽 그룹을 식별하는 메타데이터입니다. 시스템은 다중 상황 모드의 ASA FirePOWER에 대해서만 이 필드를 채웁니다.

인그레스 인터페이스

이벤트를 트리거한 패킷의 인그레스 인터페이스입니다. 패시브 인터페이스에 대해서는 이 인터페이스 열만 채워집니다.

이그레스 인터페이스

인라인 집합의 경우 이벤트를 트리거한 패킷의 이그레스 인터페이스입니다.

Source/Destination IP

이벤트(소스)를 트리거한 패킷이 시작된 호스트 IP 주소 또는 도메인 이름 또는 이벤트를 트리거한 트래픽의 대상(목적지) 호스트입니다.

소스 포트/**ICMP** 유형

이벤트를 트리거한 패킷의 소스 포트입니다. ICMP 트래픽의 경우 포트 번호가 없으면 시스템은 ICMP 유형을 표시합니다.

대상 포트/**ICMP** 코드

트래픽을 수신하는 호스트의 포트 번호입니다. ICMP 트래픽의 경우 포트 번호가 없으면 시스템은 ICMP 코드를 표시합니다.

Email Headers(이메일 헤더**)**

이메일 헤더에서 추출된 데이터입니다. 이메일 헤더는 침입 이벤트의 테이블 보기에 나타나지 않지만 이메일 헤더를 검색 기준으로 사용할 수 있습니다.

이메일 헤더를 SMTP 트래픽의 침입 이벤트와 연결하려면 SMTP 프리프로세서 **Log Headers(**헤더 로깅**)** 옵션을 활성화해야 합니다. 규칙 기반 이벤트의 경우 이메일 데이터가 추출될 때 이 행이 나타납니다.

HTTP Hostname(HTTP 호스트네임**)**

HTTP 요청 Host 헤더에서 추출된 호스트 이름(있는 경우). 이 행은 최대 256바이트까지 전체 호스트 이름을 표시합니다. 단일 행보다 길 경우 전체 호스트 이름을 확장할 수 있습니다.

호스트 이름을 표시하려면 HTTP Inspect 전처리기 **Log Hostname(**호스트 이름 로깅**)** 옵션을 활성화해야 합니다.

HTTP 요청 패킷에 항상 호스트 이름이 포함되는 것은 아닙니다. 규칙 기반 이벤트의 경우 이 행은 패킷에 HTTP 호스트 이름 또는 HTTP URI가 포함된 경우 나타납니다.

HTTP URI

침입 이벤트를 트리거한 HTTP 요청 패킷과 연결된 원시 URI(있는 경우). 이 행은 최대 2048바이트까지 전체 URI를 표시합니다. 단일 행보다 길 경우 전체 URI를 확장할 수 있습니다.

URI를 표시하려면 HTTP Inspect 전처리기 **Log URI(URI** 로깅**)** 옵션을 활성화해야 합니다.

HTTP 요청 패킷에 항상 URI가 포함되는 것은 아닙니다. 규칙 기반 이벤트의 경우 이 행은 패킷에 HTTP 호스트 이름 또는 HTTP URI가 포함된 경우 나타납니다.

HTTP 응답에 의해 트리거된 침입 이벤트에서 연결된 HTTP URI를 보려면 **Perform Stream Reassembly on Both Ports(**양쪽 포트에서 스트림 리어셈블리 수행**)** 옵션에서 HTTP 서버를 구성해야 합니다. 그러나 이렇게 하면 트래픽 리어셈블리를 위한 리소스 수요가 증가합니다.

침입 정책

침입 이벤트를 생성한 침입, 전처리기 또는 디코더 규칙이 활성화된 침입 정책(있는 경우). 액세스 제어 정책의 기본 작업으로 침입 정책을 선택하거나 침입 정책을 액세스 제어 규칙과 연결할 수 있습니다.

액세스 제어 정책

이벤트를 생성한 침입, 전처리기 또는 디코더 규칙이 활성화된 침입 정책을 포함하는 액세스 제어 정책.

액세스 제어 규칙

이벤트를 생성한 침입 규칙에 연결된 액세스 제어 규칙입니다. Default Action(기본 작업)은 규칙이 활성화된 침입 정책이 액세스 제어 규칙과 연결되지 않은 대신 액세스 제어 정책의 기본 작업으로 구성되었음을 나타냅니다.

규칙

표준 텍스트 규칙 이벤트의 경우, 이벤트를 생성한 규칙입니다.

이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

규칙 데이터에는 네트워크에 대한 민감한 정보가 포함될 수 있으므로 관리자는 사용자 역할 편집기의 View Local Rules(로컬 규칙 보기) 권한을 사용하여 패킷 보기에서 규칙 정보를 보는 사용자의 기능을 전환할 수 있습니다.

작업

표준 텍스트 및 맞춤형 규칙 이벤트의 경우, 이벤트를 트리거한 규칙에 대해 다음 작업을 수행하려면 **Actions(**작업**)**를 확장합니다.

- 규칙 수정
- 규칙의 개정 설명서를 봅니다. 표준 텍스트 규칙에 한해 Actions(작업)에서 **View Documentation(**설명서 보기**)**을 클릭한 후 설명서 팝업창에 있는 **Rule Documentation(**규칙 설명서**)**을 클릭하면 더 구체적인 규칙 세부 정보를 볼 수 있습니다.
- 규칙에 코멘트 추가
- 규칙의 상태 변경
- 규칙에 대한 임계값 설정
- 규칙 억제

이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

패킷 보기 내 침입 규칙 설정

침입 이벤트 패킷 보기 내에서 이벤트를 트리거한 규칙에 여러 작업을 수행할 수 있습니다. 이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

프로시저

단계 **1** 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information(이벤트 정보) 섹션의 **Actions(**작업**)**를 확장합니다.

단계 **2** 다음 옵션을 이용할 수 있습니다.

- 코멘트 - 표준 텍스트 규칙 이벤트의 경우, **Rule Comment(**규칙 코멘트**)**를 클릭하여 이벤트를 생성한 규칙에 텍스트 코멘트를 추가합니다. 그러면 식별된 정책 위반 또는 공격 및 규칙에 대한 자세한 컨텍스트 및 정보를 제공할 수 있습니다. 침입 규칙 편집기에서도 규칙 코멘트를 추가하고 볼 수 있습니다.
- Disable(비활성화) - 이 규칙을 비활성화하려면 다음 옵션 중 하나를 클릭합니다.
  - 현재 **Snort 2** 정책**(<policy_name>)**에서 이 규칙 비활성화
  - 로컬로 작성된 모든 **Snort 2** 정책에서 이 규칙 비활성화

  이 이벤트가 표준 텍스트 규칙에 의해 생성된 경우, 필요 시 규칙을 비활성화할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 규칙을 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 설정할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 정책은 수정할 수 없습니다.

  참고 패킷 보기에서 공유 개체 규칙을 비활성화할 수 없으며, 기본 정책에서도 규칙을 비활성화할 수 없습니다.

- 패킷 삭제 및 이벤트 생성 - 패킷을 트리거하고 이벤트를 생성하는 패킷을 삭제하도록 규칙을 설정하려면 다음 옵션 중 하나를 클릭합니다.
  - 현재 **Snort 2** 정책**(<policy_name>)**에서 트리거 패킷을 삭제하고 이벤트를 생성하도록 이 규칙 설정
  - 로컬로 작성된 모든 **Snort 2** 인라인 정책에서 트리거 패킷을 삭제하고 이벤트를 생성하도록 이 규칙 설정

  매니지드 디바이스가 네트워크에서 인라인으로 구축된 경우, 이벤트를 트리거한 규칙이 로컬로 수정할 수 있는 모든 정책에서 규칙을 트리거하는 패킷을 삭제하도록 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 설정할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 정책은 수정할 수 없습니다. 또한 이 옵션은 **Drop when Inline(**인라인 시 삭제**)**이 현재 정책에서 활성화된 경우에만 나타납니다.

- 편집 - 표준 텍스트 규칙 이벤트의 경우 **Edit(**편집**)**를 클릭하여 Snort 2 규칙을 편집하거나 **Edit Snort 3 Rule(Snort 3** 규칙 편집**)**을 클릭하여 이벤트를 생성한 규칙을 수정합니다. 이벤트가 공유 개체 규칙, 디코더 또는 전처리기를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

참고 (맞춤형 표준 텍스트 규칙과 달리) 시스템 제공 규칙을 수정하는 경우, 실제로는 새 로컬 규칙을 생성하는 것입니다. 이벤트를 생성하도록 로컬 규칙을 설정하고, 현재 침입 정책에서 원래 규칙을 비활성화해야 합니다. 그러나 기본 정책의 로컬 규칙은 활성화할 수 없습니다.

- 이벤트 생성 - 이벤트를 생성하도록 규칙을 설정하려면 **Set this rule to generate events in all locally created Snort 2 policies(**로컬로 작성된 모든 **Snort 2** 정책에서 이벤트를 생성하도록 이 규칙 설정**)**를 클릭합니다.

  이 이벤트가 표준 텍스트 규칙에 의해 생성된 경우, 로컬에서 수정할 수 있는 모든 정책에서 이벤트를 생성하도록 규칙을 설정할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 정책은 수정할 수 없습니다.

  참고 패킷 보기에서 공유 개체 규칙을 비활성화할 수 없으며, 기본 정책에서도 규칙을 비활성화할 수 없습니다.

- 억제 옵션 설정 - **Set Suppression Options(**억제 옵션 설정**)**를 확장하고 패킷 보기 내 삭제 옵션 설정, 840 페이지에 설명된 대로 계속합니다.

  이 옵션을 사용하면 로컬로 수정할 수 있는 모든 정책에서 이 이벤트를 트리거한 규칙을 억제할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 억제할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

- 임계값 옵션 설정 - **Set Thresholding Options(**임계값 옵션 설정**)**를 확장하고 패킷 보기 내 임계값 옵션 설정, 839 페이지의 설명에 따라 계속합니다.

  이 옵션을 사용하면 로컬로 수정할 수 있는 모든 정책에서 이 이벤트를 트리거한 규칙에 대해 임계값을 생성할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에 대해서만 임계값을 생성할 수 있습니다.

  현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 시스템에서 제공한 기본 침입 정책은 수정할 수 없습니다.

- 설명서 보기 - 이벤트를 생성한 규칙에 대해 자세히 알아보려면 **View Documentation(**설명서 보기**)**을 클릭합니다.원하는 경우, 더 구체적인 규칙 세부 사항을 보려면 **Rule Documentation(**규칙 설명서**)**을 클릭합니다.

패킷 보기 내 임계값 옵션 설정

침입 이벤트의 패킷 보기에서 임계값 옵션을 설정하여 시간이 지남에 따라 규칙당 생성되는 이벤트의 수를 제어할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 임계값 옵션을 설정하거나 로컬로 수정할 수 있는 경우, 현재 정책(즉, 이벤트 생성을 트리거한 정책)에서만 임계값 옵션을 설정할 수 있습니다.

프로시저

단계 **1** 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information(이벤트 정보) 섹션의 **Actions(**작업**)**를 확장합니다.

단계 **2** **Set Thresholding Options(**임계값 설정 옵션 설정**)**를 확장하고 가능한 다음 두 가지 옵션 중 하나를 선택합니다.

- 현재 **Snort 2** 정책**(<policy_name>)**에서
- 로컬로 작성된 모든 **Snort 2** 정책에서

단계 **3** 설정하려는 임계값 유형을 선택합니다.

- **Limit(**제한**)**를 클릭하여 기간당 지정된 이벤트 인스턴스 수로 알림을 제한합니다.
- 기간당 지정된 각 이벤트 인스턴스의 수에 대해 알림을 제공하려면 **Threshold(**임계값**)**를 클릭합니다.
- 지정된 이벤트 인스턴스의 수 이후 기간당 한 번 알림을 제공하려면 **Both(**모두**)**를 클릭합니다.

단계 **4** 이벤트 인스턴스를 소스 IP 주소로 추적할지 대상 IP 주소로 추적할지 나타내려면 해당 임계값을 클릭합니다.

단계 **5** 임계값으로 사용할 이벤트 인스턴스의 수를 **Count(**카운트**)** 필드에 입력합니다.

단계 **6** 이벤트 인스턴스를 추적할 기간을 지정하는 1~86400의 숫자를 **Seconds(**초**)** 필드에 입력합니다.

단계 **7** 기존 침입 정책에서 이 규칙에 대한 현재 임계값을 재정의하려면 **Override any existing settings for this rule(**이 규칙의 모든 기본 설정 재정의**)** 확인란을 선택합니다.

단계 **8** **Save Thresholding(**임계값 설정 저장**)**을 클릭합니다.

패킷 보기 내 삭제 옵션 설정

억제 옵션을 사용하여 침입 이벤트를 완전히 억제하거나 소스 또는 목적지 IP 주소를 기반으로 억제할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 억제 옵션을 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 억제 옵션을 설정할 수 있습니다.

프로시저

단계 **1** 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information(이벤트 정보) 섹션의 **Actions(**작업**)**를 확장합니다.

단계 **2** **Set Suppression Options(**억제 옵션 설정**)**를 확장하고 가능한 다음 두 가지 옵션 중 하나를 선택합니다.

- 현재 **Snort 2** 정책**(<policy_name>)**에서
- 로컬로 작성된 모든 **Snort 2** 정책에서

참고 현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어 맞춤형 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

단계 **3** 다음 **Track By(**추적 기준**)** 옵션 중 하나를 선택합니다.

- 지정된 소스 IP 주소에서 시작되는 패킷에 의해 생성된 이벤트를 억제하려면 **Source(**소스**)**를 클릭합니다.
- 지정된 대상 IP 주소로 가는 패킷에 의해 생성된 이벤트를 억제하려면 **Destination(**대상**)**을 클릭합니다.
- 이 이벤트를 트리거한 규칙의 이벤트를 완전히 억제하려면 **Rule(**규칙**)**을 클릭합니다.

단계 **4** 소스 또는 대상 IP 주소로 지정하려는 IP 주소 또는 CIDR 블록/접두사 길이를 **IP address or CIDR block(IP** 주소 또는 **CIDR** 블록**)** 필드에 입력합니다.

단계 **5** **Save Suppression(**억제 저장**)**을 클릭합니다.

관련 항목

Firepower System IP 주소 규칙, 28 페이지

프레임 정보 필드

패킷 보기에서 캡처된 프레임에 대한 정보를 볼 **Frame(**프레임**)** 옆에 있는 화살표를 클릭합니다. 패킷 보기에 단일 프레임 또는 다중 프레임이 표시될 수 있습니다. 각 프레임은 개별 네트워크 패킷에 대한 정보를 제공합니다. 예를 들면 태그가 지정된 패킷에서 또는 리어셈블된 TCP 스트림의 패킷에서 여러 프레임을 보게 될 수 있습니다.

Frame n

캡처된 프레임. 여기서 *n*은 단일 프레임 패킷의 경우 1이고 다중 프레임 패킷의 경우 증분 프레임 수입니다. 프레임에서 캡처된 바이트의 수가 프레임 수에 추가됩니다.

Arrival Time

프레임이 캡처된 날짜와 시간.

Time delta from previous captured frame

다중 프레임 패킷의 경우 이전 프레임이 캡처된 이후 경과한 시간.

Time delta from previous displayed frame

다중 프레임 패킷의 경우 이전 프레임이 표시된 이후 경과한 시간.

Time since reference or first frame

다중 프레임 패킷의 경우 첫 번째 프레임이 캡처된 이후 경과한 시간.

Frame Number

증분 프레임 수.

Frame Length

바이트 단위의 프레임 길이.

Capture Length

바이트 단위의 캡처된 프레임 길이.

Frame is marked

프레임이 표시되었는지 여부(true 또는 false).

Protocols in frame

프레임에 포함된 프로토콜.

관련 항목

tag 키워드
TCP 스트림 리어셈블리

데이터 링크 레이어 정보 필드

패킷 보기에서 데이터 링크 레이어 프로토콜(예: **Ethernet II**) 옆에 있는 화살표를 클릭하여 소스 및 대상 호스트의 48비트 MAC(media access control) 주소가 포함된 패킷에 대한 데이터 링크 레이어 정보를 봅니다. 하드웨어 프로토콜에 따라 패킷에 대한 기타 정보도 표시될 수 있습니다.

참고 이 예에서는 이더넷 링크 레이어 정보에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

패킷 보기는 데이터 링크 레이어에 사용된 프로토콜을 반영합니다. 다음 목록에서는 패킷 보기에 표시될 수 있는 Ethernet II 또는 IEEE 802.3 Ethernet 패킷 정보에 대해 설명합니다.

대상

대상 호스트의 MAC 주소.

참고 이더넷은 멀티캐스트 및 브로드캐스트 주소를 대상 주소로 사용할 수도 있습니다.

소스

소스 호스트의 MAC 주소.

유형

Ethernet II 패킷의 경우 이더넷 프레임으로 캡슐화된 패킷의 유형(예: IPv6 또는 ARP 데이터그램). 이 항목은 Ethernet II 패킷에 대해서만 나타납니다.

길이

IEEE 802.3 Ethernet 패킷의 경우 체크섬을 제외한 패킷의 전체 길이(바이트 단위). 이 항목은 IEEE 802.3 Ethernet 패킷에 대해서만 나타납니다.

네트워크 레이어 정보 보기

프로시저

패킷과 관련된 네트워크 레이어 정보에 대해 자세히 알아보려면 패킷 보기에서 네트워크 레이어 프로토콜(예: **Internet Protocol**) 옆에 있는 화살표를 클릭합니다.

참고 이 예에서는 IP 패킷에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

IPv4 Network Layer Information(IPv4 네트워크 레이어 정보) 필드

다음 목록에서는 IPv4 패킷에 나타날 수 있는 프로토콜 관련 정보에 대해 설명합니다.

버전

Internet Protocol version number(Internet Protocol 버전 번호).

Header Length(헤더 길이)

헤더의 바이트 수(IP 옵션 포함). 옵션이 없는 IP 헤더의 길이는 20바이트입니다.

Differentiated Services(차별화된 서비스) 필드

전송 호스트가 ECN(Explicit Congestion Notification)을 지원하는 방법을 나타내는 차별화된 서비스에 대한 값.

- `0x0` - ECT(ECN-Capable Transport)를 지원하지 않음
- `0x1` 및 `0x2` - ECT를 지원함
- `0x3` - CE(Congestion Experienced)

Total Length(총 길이)

IP 패킷에서 IP 헤더를 뺀 길이(바이트 단위).

식별

소스 호스트가 전송한 IP 데이터그램을 고유하게 식별하는 값. 이 값은 동일한 데이터그램의 프래그먼트를 추적하는 데 사용됩니다.

플래그

IP 프래그먼트화를 제어하는 값.

Last Fragment 플래그의 값은 데이터그램과 관련된 프래그먼트가 더 있는지 여부를 나타냅니다.

- 0 - 데이터그램에 연결된 프래그먼트가 더 이상 없음
- 1 - 데이터그램에 연결된 프래그먼트가 더 있음

Don't Fragment 플래그의 값은 데이터그램을 프래그먼트화할 수 있는지 여부를 나타냅니다.

- 0 - 데이터그램이 프래그먼트화될 수 있음
- 1 - 데이터그램이 프래그먼트화되어서는 안 됨

Fragment Offset(프래그먼트 오프셋**)**

데이터그램 시작에서부터 프래그먼트 오프셋의 값.

Time to Live(ttl)

데이터그램이 만료되기 전 데이터그램이 라우터 간에 만들 수 있는 나머지 홉(hop)의 수.

프로토콜

IP 데이터그램에서 캡슐화되는 전송 프로토콜(예: ICMP, IGMP, TCP 또는 UDP).

Header Checksum(헤더 체크섬**)**

IP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면, 데이터그램이 전송 중에 손상되었거나 침입 회피 시도에 사용 중일 수 있습니다.

소스**/**대상

소스(또는 대상) 호스트의 IP 주소나 도메인 이름.

도메인 이름을 표시하려면 IP 주소 확인을 활성화해야 합니다.

주소 또는 도메인 이름을 클릭하여 상황에 맞는 메뉴를 표시한 다음 호스트에서 whois 검색을 수행하려면 **Whois**를, 호스트 정보를 보려면 **View Host Profile(**호스트 프로파일 보기**)**을, 전역 차단 목록 또는 차단 안 함 목록에 주소를 추가하려면 옵션을 선택합니다.

IPv6 네트워크 레이어 정보 필드

다음 목록에서는 IPv6 패킷에 나타날 수 있는 프로토콜 관련 정보에 대해 설명합니다.

Traffic Class(트래픽 클래스**)**

IPv4에 대해 제공되는 차별화된 서비스 기능과 유사한 IPv6 패킷 클래스 또는 우선순위를 식별하기 위한 IPv6 헤더의 실험적인 8비트 필드. 사용되지 않는 경우 이 필드는 0으로 설정됩니다.

Flow Label

기본이 아닌 서비스 품질 또는 실시간 서비스 등의 특수 플로우를 식별하는 선택적인 20비트 IPv6 16진수 값 1~FFFFF. 사용되지 않는 경우 이 필드는 0으로 설정됩니다.

Payload Length(페이로드 길이**)**

IPv6 페이로드에서 옥텟 수를 식별하는 16비트 필드로, IPv6 헤더 뒤에 나오는 모든 패킷(확장 헤더 포함)으로 구성됨.

Next Header(다음 헤더**)**

IPv6 헤더 바로 뒤에 나오는 헤더 유형을 식별하는 8비트 필드로, IPv4 Protocol 필드와 같은 값 사용.

Hop Limit(홉 제한**)**

패킷을 전달하는 각 노드가 1씩 감소하는 8비트 10진수 정수. 감소한 값이 0에 도달하면 패킷이 취소됩니다.

소스

소스 호스트의 128비트 IPv6 주소.

대상

대상 호스트의 128비트 IPv6 주소.

전송 레이어 정보 보기

프로시저

단계 **1** 패킷 보기에서 전송 레이어 프로토콜(예: **TCP**, **UDP** 또는 **ICMP**) 옆의 화살표를 클릭합니다.

단계 **2** 원하는 경우, 패킷 보기의 Packet Information(패킷 정보) 섹션에서 바로 위에 있는 프로토콜에 대한 페이로드의 처음 24바이트를 보려면 **Data**(있는 경우)를 클릭하십시오.

단계 **3** TCP Packet View(TCP 패킷 보기) 필드, 845 페이지, UDP 패킷 보기 필드, 847 페이지 또는 ICMP 패킷 보기 필드, 847 페이지에 설명된 대로 TCP, UDP, ICMP 프로토콜 전송 계층의 콘텐츠를 확인합니다.

참고 이 예에서는 TCP, UDP 및 ICMP 패킷에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

TCP Packet View(TCP 패킷 보기**)** 필드

이 절에서는 TCP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

소스 포트

시작 애플리케이션 프로토콜을 식별하는 번호.

Destination Port(목적지 포트**)**

수신 애플리케이션 프로토콜을 식별하는 번호.

sequence number(시퀀스 번호**)**

현재 TCP 세그먼트의 첫 번째 바이트에 대한 값으로, TCP 스트림에서 초기 시퀀스 번호로 키가 지정됨.

Next sequence number(다음 시퀀스 번호**)**

응답 패킷에서, 전송할 다음 패킷의 시퀀스 번호.

Acknowledgement number(승인 번호**)**

전에 허용된 데이터의 시퀀스 번호로 키가 지정되는 TCP 승인.

Header Length(헤더 길이**)**

헤더의 바이트 수.

플래그

TCP 세그먼트의 전송 상태를 나타내는 6개 비트.

- `U` - Urgent Pointer가 유효함
- `A` - 승인 번호가 유효함
- `P` - 수신자가 데이터를 푸시해야 함
- `R` - 연결 재설정
- `S` - 새 연결을 시작하도록 시퀀스 번호 동기화
- `F` — 보낸 사람이 데이터 전송을 완료 했습니다.

Window size(창 크기**)**

수신 호스트가 허용하는, 승인되지 않은 데이터의 양(바이트 단위)

체크섬

TCP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면, 데이터그램이 전송 중에 손상되었거나 회피 시도에 사용 중일 수 있습니다.

Urgent Pointer(긴급 포인터**)**

긴급 데이터가 종료되는 TCP 세그먼트의 위치(있는 경우). U 플래그와 함께 사용됨.

옵션

TCP 옵션의 값(있는 경우)

UDP 패킷 보기 필드

이 절에서는 UDP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

소스 포트

시작 애플리케이션 프로토콜을 식별하는 번호.

목적지 포트

수신 애플리케이션 프로토콜을 식별하는 번호.

길이

UDP 헤더 및 데이터를 결합한 길이.

체크섬

UDP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면 전송 중 데이터그램이 손상되었을 수 있습니다.

ICMP 패킷 보기 필드

이 절에서는 ICMP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

유형

ICMP 메시지의 유형:

- 0 - 에코 응답
- 3 - 목적지 도달 불가
- 4 - 소스 억제
- 5 - 리디렉션
- 8 - 에코 요청
- 9 - 라우터 알림
- 10 - 라우터 요청
- 11 - 시간 초과
- 12 - 파라미터 문제

- 13 - 타임스탬프 요청
- 14 - 타임스탬프 응답
- 15 - 정보 요청(사용되지 않음)
- 16 - 정보 응답(사용되지 않음)
- 17 - 주소 마스크 요청
- 18 - 주소 마스크 응답

코드

ICMP 메시지 유형에 대해 함께 제공 되는 코드입니다. ICMP 메시지 유형 3, 5, 11, 12에는 RFC 792에 설명된 대로 해당 코드가 있습니다.

체크섬

ICMP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면 전송 중 데이터그램이 손상되었을 수 있습니다.

패킷 바이트 정보 보기

프로시저

패킷을 구성하는 바이트의 16진수 및 ASCII 버전을 보려면 패킷 보기에서 **Packet Bytes(**패킷 바이트**)** 옆에 있는 화살표를 클릭합니다. 시스템이 트래픽을 해독하면 해독된 패킷 바이트를 볼 수 있습니다.

내부 소스 침입 이벤트

내부 소스에서 들어오는 침입 이벤트는 네트워크의 호스트가 손상되었음을 나타냅니다. 소스 IP 주소가 네트워크에 있는 경우 이 호스트를 조사해야 한다는 신호입니다.

침입 이벤트 통계 보기

Intrusion Event Statistics(침입 이벤트 통계) 페이지에서는 어플라이언스의 현재 상태 및 네트워크에 대해 생성된 침입 이벤트에 대한 빠른 요약을 제공합니다.

페이지에 표시되는 각 IP 주소, 포트, 프로토콜, 이벤트 메시지 등은 링크입니다. 연결된 이벤트 정보를 보려면 링크를 클릭하십시오. 예를 들어 상위 10개 대상 포트 중 하나가 `80 (http)/tcp`인 경우 해당 링크를 클릭하면 기본 침입 이벤트 워크플로의 첫 번째 페이지가 표시되고, 해당 포트를 대상으로 하는 이벤트가 나열됩니다. 현재 시간 범위의 이벤트(및 이벤트를 생성하는 매니지드 디바이스)만 나타납니다. 또한 검토한 것으로 표시한 침입 이벤트는 통계에 계속 나타납니다. 예를 들어 현재의 시

간 범위가 과거 시간이지만 첫 번째 이벤트가 5시간 전에 생성된 경우, **First Event(**첫 번째 이벤트**)** 링크를 클릭하면 시간 범위를 변경하기 전에는 결과 이벤트 페이지에 이벤트가 표시되지 않습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Intrusion Event Statistics(**침입 이벤트 통계**)**을(를) 선택합니다.

단계 **2** 페이지 상단에 있는 두 개의 선택 상자에서 통계를 보려는 영역 및 디바이스를 선택합니다. 침입 이벤트를 수집하는 모든 디바이스에 대한 통계를 보려면 **All Security Zones(**모든 보안 영역**)** 및 **All Devices(**모든 디바이스**)**를 선택합니다.

단계 **3** **Get Statistics(**통계 가져오기**)**를 클릭합니다.

팁 맞춤형 시간 범위의 데이터를 보려면 페이지 오른쪽 위 영역의 링크를 클릭하고 타임 윈도우 변경, 710 페이지의 지침을 따르십시오.

호스트 통계 자료

Intrusion Event Statistics(침입 이벤트 통계) 페이지의 Host Statistics(호스트 통계) 절에서는 어플라이언스 자체에 대한 정보를 제공합니다. Secure Firewall Management Center에서 이 섹션은 매니지드 디바이스에 대한 정보도 제공합니다.

이 정보에는 다음 항목이 포함됩니다.

시간

어플라이언스의 현재 시간.

Uptime(실행 시간**)**

어플라이언스 자체를 다시 시작한 이후의 일 수, 시간, 분. Secure Firewall Management Center에서 업타임은 각 매니지드 디바이스가 마지막으로 재부팅된 시간, 로그인한 사용자 수 및 로드 평균도 보여줍니다.

디스크 사용

사용 중인 디스크의 백분율

메모리 사용

사용 중인 시스템 메모리의 백분율

로드 평균

지난 1분, 5분 15분 동안 CPU 큐 프로세스의 평균 수.

이벤트 개요

Intrusion Event Statistics(침입 이벤트 통계) 페이지의 Event Overview(이벤트 개요) 섹션에서는 침입 이벤트 데이터베이스의 정보 개요를 제공합니다.

이러한 통계에는 다음이 포함됩니다.

이벤트

침입 이벤트 데이터베이스의 이벤트 수.

시간 범위 내 이벤트

현재 선택된 시간 범위는 물론 시간 범위에 속하는 데이터베이스의 이벤트 수와 비율도 표시합니다.

첫 번째 이벤트

이벤트 데이터베이스에 있는 첫 번째 이벤트의 이벤트 메시지.

마지막 이벤트

이벤트 데이터베이스에 있는 마지막 이벤트의 이벤트 메시지.

참고 Secure Firewall Management Center에서 침입 이벤트 데이터를 보는 동안 매니지드 디바이스를 선택하면 해당 디바이스에 대 한 Event Overview(이벤트 개요) 섹션이 대신 표시됩니다.

이벤트 통계

Intrusion Event Statistics(침입 이벤트 통계) 페이지의 Event Statistics(이벤트 통계) 섹션에서는 침입 이벤트 데이터베이스의 정보에 대한 좀 더 구체적인 정보를 제공합니다.

이 정보에는 다음에 대한 세부사항이 포함됩니다.

- 상위 10개 이벤트 유형
- 상위 10개 소스 IP 주소
- 상위 10개 대상 IP 주소
- 상위 10개 대상 포트
- 이벤트 수가 가장 많은 프로토콜, 수신 및 송신 보안 영역, 디바이스

참고 다중 도메인 구축에서 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 따라서 리프 도메인은 네트워크 내에서는 고유하지만 다른 리프 도메인과 동일한 IP 주소를 포함할 수 있습니다. 상위 도메인에서 이벤트 통계를 볼 때 반복되는 IP 주소의 여러 인스턴스가 표시될 수 있습니다. 처음에는 이것이 중복된 항목으로 보일 수 있습니다. 하지만 각 IP 주소의 호스트 프로파일 정보로 드릴다운하는 경우, 시스템은 이들이 서로 다른 리프 도메인에 속한다고 표시합니다.

침입 이벤트 성능 그래프 보기

침입 이벤트 성능 페이지에서 특정 기간 동안 Secure Firewall Management Center 또는 매니지드 디바이스에 대한 침입 이벤트의 성능 통계를 보여주는 그래프를 생성할 수 있습니다. 초당 침입 이벤트의 수, 초당 메가비트의 수, 패킷당 평균 바이트 수, Snort에서 검사하지 않은 패킷의 비율, TCP 표준화로 인해 차단된 패킷의 수를 보여주는 그래프를 생성할 수 있습니다. 이러한 그래프는 운영의 마지막 시간, 마지막 날, 마지막 주 또는 마지막 달에 대한 통계를 보여줄 수 있습니다.

참고 새 데이터는 통계 그래프를 위해 5분마다 누적됩니다. 따라서 그래프를 빠르게 다시 로드하는 경우 다음 5분 증가분이 발생할 때까지 데이터가 변경되지 않을 수 있습니다. 각 그래프는 선택한 기간(마지막 달, 주, 날 또는 시간) 동안 표시된 간격(일, 시간 또는 5분) 내 평균 값을 표시합니다. 평균이 1보다 작으면 소수 값이 표시됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Intrusion Event Performance(**침입 이벤트 성능**)**을(를) 선택합니다.

단계 **2** 데이터를 보려는 디바이스를 **Select Device(**디바이스 선택**)** 목록에서 선택합니다.

단계 **3** 침입 이벤트 성능 통계 그래프 유형, 851 페이지에 설명된 대로 **Select Graph(s)(**그래프 선택**)** 목록에서 생성할 그래프 유형을 선택합니다.

단계 **4** **Select Time Range(**시간 범위 선택**)** 목록에서 그래프에 사용할 시간 범위를 선택합니다.

단계 **5** **Graph(**그래프**)**를 클릭합니다.

단계 **6** 그래프를 저장하려면 마우스 오른쪽 버튼으로 그래프를 클릭하고 브라우저의 지시에 따라 이미지를 저장합니다.

침입 이벤트 성능 통계 그래프 유형

다음 표에는 사용 가능한 그래프 유형이 나열되어 있습니다. 네트워크 분석 정책 **Inline Mode(**인라인 모드**)** 설정의 영향을 받는 데이터로 채워지는 경우 그래프 유형이 다르게 표시됩니다. **Inline Mode(**인라인 모드**)**가 비활성화되어 있으면 웹 인터페이스에서 별표(*)로 표시된 그래프 유형(아래 열에서 (yes로 표시된 행)은 **Inline Mode(**인라인 모드**)**가 활성화되었다면 시스템에서 수정 또는 삭제했을 트래픽에 대한 데이터로 채워집니다.

표 ***103:*** 침입 이벤트 성능 그래프 유형

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
평균 바이트/패킷	해당 없음	각 패킷에 포함된 평균 바이트 수입니다.	아니요
TCP 트래픽/패킷에서 표준화된 ECN 플래그	**Explicit Congestion Notification(**명시적 폭주 통지**)**을 활성화하고 **Packet(**패킷**)** 선택	협상 여부와 상관없이 패킷당 기준으로 ECN 플래그가 지워진 패킷의 수입니다.	예
TCP 트래픽/세션에서 표준화된 ECN 플래그	**Explicit Congestion Notification(**명시적 폭주 통지**)**을 활성화하고 **Stream(**스트림**)** 선택	ECN 사용이 협상되지 않은 경우 스트림 단위로 ECN 플래그가 지워진 횟수입니다.	예
이벤트/초	해당 없음	디바이스에서 생성되는 초당 이벤트 수입니다.	아니요
ICMPv4 에코 정규화	**Normalize ICMPv4** 활성화	Echo(Request) 또는 Echo Reply 메시지의 8비트 Code 필드가 지워진 ICMPv4 패킷의 수	예
ICMPv6 에코 정규화	**Normalize ICMPv6** 활성화	Echo(Request) 또는 Echo Reply 메시지의 8비트 Code 필드가 지워진 ICMPv4 패킷의 수입니다.	예
IPv4 DF 플래그 표준화	**Normalize IPv4** 및 **Normalize Don't Fragment Bit** 활성화	IPv4 Flags 헤더 필드의 단일 비트 Don't Fragment 하위 필드가 지워진 IPv4 패킷의 수입니다.	예
IPv4 옵션 정규화	**Normalize IPv4** 활성화	옵션 옥텟이 1(No Operation)로 설정된 IPv4 패킷의 수입니다.	예
IPv4 예약 플래그 표준화	**Normalize IPv4** 및 **Normalize Reserved Bit** 활성화	IPv4 Flags 헤더의 단일 비트 Reserved 하위 필드가 지워진 IPv4 패킷의 수입니다.	예
IPv4 크기 조정 표준화	**Normalize IPv4** 활성화	IP 헤더에 지정된 데이터그램 길이로 잘린, 과도한 길이의 페이로드가 있는 IPv4 패킷의 수입니다.	예
IPv4 TOS 표준화	**Normalize IPv4** 및 **Normalize TOS Bit** 활성화	1바이트 Differentiated Services(DS) 필드(이전의 Type of Service(TOS) 필드)가 지워진 IPv4 패킷의 수입니다.	예
IPv4 TTL 정규화	**Normalize IPv4**, **Maximum TTL** 및 **Reset TTL** 활성화	IPv4 Time to Live 표준화의 수입니다.	예

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
IPv6 옵션 정규화	**Normalize IPv6** 활성화	Hop-by-Hop Options(홉 바이 홉 옵션) 또는 Destination Options(대상 옵션) 확장 헤더의 Option Type(옵션 유형) 필드가 `00`(건너뛰고 계속 처리)으로 설정된 IPv6 패킷의 수입니다.	예
IPv6 TTL 정규화	**Normalize IPv6**, **Minimum TTL** 및 **Reset TTL** 활성화	IPv6 Hop Limit(TTL) 표준화의 수입니다.	예
메가비트/초	해당 없음	디바이스를 통해 전달되는 트래픽의 초당 메가비트 수입니다.	아니요
MSS 표준화에 맞게 크기 조정된 패킷	**Trim Data to MSS(MSS**로 데이터 절감**)** 활성화	페이로드가 TCP Data 필드보다 길어서 Maximum Segment Size로 잘리는 패킷의 수입니다.	예
TCP 창 표준화에 맞게 크기 조정된 패킷	**Trim Data to Window** 활성화	TCP Data 필드가 수신 호스트의 TCP 창에 맞게 잘리는 패킷의 수입니다.	예
삭제된 패킷 비율	해당 없음	선택한 모든 디바이스에서 검사하지 않은 패킷의 평균 비율입니다. 예를 들어 디바이스를 2개 선택하고 평균이 50%이면, 한 디바이스는 삭제율이 90%이고 나머지는 삭제율이 10%라는 뜻일 수 있습니다. 또는 두 디바이스 모두 삭제율이 50%임을 나타낼 수도 있습니다. 그래프는 단일 디바이스를 선택할 경우의 총 삭제 %만 나타냅니다.	아니요
데이터 스트립된 RST 패킷 표준화	**Remove Data on RST(RST** 데이터 제거**)** 활성화	TCP 재설정(RST) 패킷에서 데이터가 삭제된 패킷의 수입니다.	예
데이터 스트립된 SYN 패킷 표준화	**Remove Data on SYN(SYN** 데이터 제거**)** 활성화	TCP 운영체제가 Mac OS가 아닐 때 SYN 패킷에서 데이터가 제거된 패킷의 수입니다.	예
TCP 헤더 패딩 표준화	**Normalize/Clear Option Padding Bytes(**옵션 패딩 바이트 표준화/지우기**)** 활성화	옵션 패딩 바이트가 0으로 설정되었을 때 TCP 패킷의 수입니다.	예
TCP 옵션 없음 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	Time Stamp 옵션이 제거된 패킷의 수입니다.	예
TCP NS 플래그 표준화	**Explicit Congestion Notification(**명시적 폭주 통지**)**을 활성화하고 **Packet(**패킷**)** 선택	ECN Nonce Sum(NS) 옵션 표준화의 수입니다.	예

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
TCP 옵션 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	옵션 필드가 No Operation(TCP Option 1)으로 설정된 옵션(MSS, Window Scale, Time Stamp 및 명시적으로 허용된 옵션 제외)의 수입니다.	예
표준화에 의해 차단된 TCP 패킷	**Normalize TCP Payload** 활성화(세그먼트 리어셈블리가 실패함)	TCP 세그먼트를 제대로 리어셈블할 수 없기 때문에 삭제된 패킷의 수입니다.	예
TCP 예약 플래그 표준화	**Normalize/Clear Reserved Bits(**예약 비트 표준화/지우기**)** 활성화	Reserved 비트가 지워진 TCP 패킷의 수입니다.	예
TCP 세그먼트 리어셈블리 표준화	**Normalize TCP Payload** 활성화(세그먼트 리어셈블리가 성공함)	재전송된 데이터의 일관성을 보장하기 위해 TCP Data 필드가 표준화된 패킷의 수(제대로 리어셈블할 수 없는 세그먼트는 삭제됨)입니다.	예
TCP SYN 옵션 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	SYN 제어 비트가 설정되지 않아 Maximum Segment Size or Window Scale 옵션이 No Operation(TCP Option 1)으로 설정된 옵션의 수입니다.	예
TCP 타임스탬프 ECR 표준화	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	Acknowledgment(수신 확인, ACK) 제어 비트가 설정되지 않아 Time Stamp Echo Reply(타임 스탬프 에코 응답, TSecr) 옵션 필드가 지워진 패킷의 수입니다.	예
TCP 긴급 포인터 표준화	**Normalize Urgent Pointer(**긴급 포인터 표준화**)** 활성화	2바이트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드가 페이로드 길이보다 긴 패킷 및 페이로드 길이로 설정된 패킷의 수입니다.	예
총 차단된 패킷	**Inline Mode** 또는 **Drop when Inline** 설정	규칙, 디코더 및 전처리기 삭제를 비롯한 삭제된 패킷의 총 수입니다.	아니요
총 삽입된 패킷	**Inline Mode** 설정	재전송되기 전에 크기가 조정된 패킷의 수입니다.	아니요
총 TCP 필터링된 패킷	TCP 스트림 전처리 설정	TCP 포트 필터링 때문에 스트림에서 건너뛴 패킷의 수입니다.	아니요
총 UDP 필터링된 패킷	UDP 스트림 전처리 설정	UDP 포트 필터링 때문에 스트림에서 건너뛴 패킷의 수입니다.	아니요

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	**Inline Mode(**인라인 모드**)**의 영향 적용 여부
긴급 플래그 지워진 표준화	**Clear URG if Urgent Pointer is Not Set(**긴급 포인터가 설정되지 않은 경우 **URG** 지우기**)** 활성화	긴급 포인터가 설정되지 않아서 TCP 헤더 URG 제어 비트가 지워진 패킷의 수입니다.	예
긴급 포인터 및 긴급 플래그 지워진 표준화	**Clear Urgent Pointer/URG on Empty Payload(**빈 페이로드의 긴급 포인터**/URG** 지우기**)** 활성화	페이로드가 없어 TCP 헤더 Urgent Pointer(긴급 포인터) 필드 및 URG 제어 비트가 지워진 패킷의 수입니다.	예
긴급 포인터 지워진 표준화	**Clear Urgent Pointer if URG=0(URG=0**인 경우 긴급 포인터 지우기**)** 활성화	Urgent(URG) 제어 비트가 설정되지 않아 16비트 TCP 헤더 Urgent Pointer(긴급 포인터) 필드가 지워진 패킷의 수입니다.	예

관련 항목

- 인라인 정상화 전처리기
- 인라인 구축의 전처리기 트래픽 수정
- 인라인 구축의 삭제 작업

침입 이벤트 그래프 보기

Firepower System은 시간에 따른 침입 이벤트 추세를 보여주는 그래프를 제공합니다. 하나 또는 모든 매니지드 디바이스에 대해 지난 1시간부터 지난 달까지의 시간 동안의 침입 이벤트 그래프를 생성할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Intrusion Event Graphs(**침입 이벤트 그래프**)**을(를) 선택합니다.

단계 **2** **Select Device(**디바이스 선택**)** 아래에서 **all**을 선택하여 모든 디바이스를 포함하거나 그래프에 포함할 특정 디바이스를 선택합니다.

단계 **3** **Select Graph(s)(**그래프 선택**)**에서 생성할 그래프 유형을 선택합니다.

- 상위 10개 대상 포트
- 상위 10개 소스 IP 주소
- 상위 10개 이벤트 메시지

단계 **4** **Select Time Range(**시간 범위 선택**)**에서 그래프의 시간 범위를 선택합니다.

- 마지막 시간
- 지난 1일
- 지난주
- 지난달

단계 **5** **Graph(**그래프**)**를 클릭합니다.

침입 이벤트 기록

기능	버전	세부 사항
IPS 이벤트 데이터스토어 교체	7.1	• 침입 인시던트, 침입 이벤트 클립보드 및 기본 사용자 지정 테이블(침입 이벤트 열 - **Intrusion Events with Source Criticality(**소스 중요도가 있는 침입 이벤트**)** 및 **Intrusion Events with Destination Criticality(**대상 중요도가 있는 침입 이벤트**)** 사용)은 더 이상 사용되지 않습니다. 더 이상 **Copy(**복사**)** 및 **Copy All(**모두 복사**)** 버튼을 사용하여 클립보드에 이벤트를 추가할 수 없습니다. 사용되지 않는 페이지: • **Analysis(**분석**) > Intrusions(**침입**) > Clipboard(**클립보드**)** • **Analysis(**분석**) > Intrusions(**침입**) > Incidents(**인시던트**)** • 기본 침입 이벤트 테이블에 **Source Host Criticality(**소스 호스트 중요도**)**와 **Destination Host Criticality(**대상 호스트 중요도**)**의 두 필드가 새로 추가되었습니다. 지원되는 플랫폼: Secure Firewall Management Center
시스템 로그의 연결 이벤트 통합 식별자	6.4.0.4	다음 시스템 로그 필드는 함께 연결 이벤트를 개별적으로 식별하며, 침입 이벤트의 경우에는 시스템 로그에 디바이스 UUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터로 표시됩니다.
이제 IntrusionPolicy 필드가 시스템 로그에 포함됩니다.	6.4	침입 이벤트 시스템 로그는 이제 이벤트를 트리거한 침입 정책을 표시합니다.
새 침입 이벤트 검색 필드: CVE ID	6.4	이제 MITRE의 일반 취약성 및 노출 식별 번호로 검색할 수 있습니다. 수정된 화면: **Analysis(**분석**) > Intrusions(**침입**) > Events(**이벤트**) > Edit Search(**검색 편집**)** 지원되는 플랫폼: 전체.

34 장

파일/악성코드 이벤트 및 네트워크 파일 경로 분석

다음 주제에서는 파일 및 악성코드 이벤트, 로컬 악성코드 분석, 동적 분석, 캡처된 파일, 네트워크 파일 경로 분석의 개요를 제공합니다.

파일/악성코드 이벤트 및 네트워크 파일 경로 분석 정보

파일 정책은 일치된 트래픽에 대한 파일 및 악성코드 이벤트를 자동으로 생성하고 캡처된 파일 정보를 로깅합니다. 파일 정책이 파일 또는 악성코드 이벤트를 생성하거나 파일을 캡처하면 시스템도 연결된 연결 종료를 Secure Firewall Management Center 데이터베이스에 자동으로 로깅합니다. 이 데이터를 분석하여 모든 부정적 영향을 해결하고 향후 공격을 차단할 수 있습니다.

파일 분석 결과를 바탕으로 Analysis(분석) > Files(파일) 메뉴에서 사용할 수 있는 페이지의 테이블을 사용하여 캡처된 파일과 생성된 악성코드 및 파일 이벤트를 검토할 수 있습니다. 사용 가능한 경우, 파일의 구성, 속성, 위협 점수, 동적 분석 요약 보고서를 검사하여 악성코드 분석에 대한 추가 통찰을 얻을 수 있습니다.

보다 집중적인 분석을 위해 악성코드 파일의 네트워크 파일 경로 분석(파일이 호스트를 통과하여 네트워크에서 이동한 방법과 다양한 파일 속성을 보여주는 맵)을 사용하여 시간이 지남에 따른 호스트에서의 개별 위협의 확산을 추적할 수 있으며, 이를 통해 가장 유용한 보안 침해 통제 및 방지에 집중할 수 있습니다.

파일 규칙에서 로컬 악성코드 분석 또는 동적 분석을 구성하는 경우, 시스템은 규칙과 일치 하는 파일을 사전 분류하고 파일 구성 보고서를 생성합니다.

조직에서 *AMP for Endpoints*를 구축하여 해당 구축을 Secure Firewall Management Center에 통합한 경우, 해당 제품이 식별한 보안 침해 지표(IOC)뿐 아니라 스캔, 악성코드 탐지, 격리 레코드를 가져올 수 있습니다. 이 데이터는 네트워크에서 악성코드를 더 완벽하게 파악할 수 있도록 Firepower가 수집한 이벤트 데이터와 함께 표시됩니다.

Context Explorer, 대시보드, 보고 기능도 탐지, 캡처, 차단된 파일과 악성코드를 더욱 깊이 이해하는 데 도움이 됩니다. 이벤트를 사용하여 상관관계 정책 위반을 트리거하거나 이메일, SNMP 또는 syslog를 통해 알림을 받을 수도 있습니다.

참고 악성코드를 탐지하고 파일 및 악성코드 이벤트를 생성하도록 시스템을 구성하려면 Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 네트워크 악성코드 보호 및 파일 정책을 참고하십시오.

파일 및 악성코드 이벤트

Secure Firewall Management Center는 다양한 유형의 파일 및 악성코드 이벤트를 로깅할 수 있습니다. 개별 이벤트에 사용 가능한 정보는 정보 생성 방법과 이유에 따라 달라질 수 있습니다.

- 파일 이벤트는 Firepower system이 탐지한 악성코드를 포함한 파일을 나타냅니다(악성코드 대응 .) 파일 이벤트는 AMP for Endpoints 관련 필드를 포함하지 않습니다.
- 악성코드 이벤트는 악성코드 대응 또는 AMP for Endpoints에 의해 탐지된 악성코드를 나타냅니다. 악성코드 이벤트에는 스캔과 격리 등 AMP for Endpoints 구축이 제공하는 위협 외의 레코드 데이터도 포함될 수 있습니다.
- 회귀적 악성코드 이벤트는 악성코드 대응 에 의해 탐지된, 속성(파일이 악성코드인지 여부)이 변경된 파일을 나타냅니다.

참고

- 악성코드 대응 에 의해 악성코드로 식별된 파일은 파일 이벤트와 악성코드 이벤트를 모두 생성합니다. AMP for Endpoints에 의해 생성된 악성코드 이벤트에는 상응하는 파일 이벤트가 없습니다.
- 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.
- Firepower System은 유니코드(UTF-8) 문자를 사용하는 파일 이름의 표시와 입력을 지원합니다. 다만 유니코드 파일 이름은 문자 번역된 형식으로 PDF 보고서에 표시됩니다. 또한 SMB 프로토콜은 파일 이름에 있는 인쇄할 수 없는 문자를 마침표로 대체합니다.

파일 및 악성코드 이벤트 유형

파일 이벤트

시스템은 매니지드 디바이스가 네트워크 트래픽에서 파일을 탐지하거나 차단할 때 생성되는 파일 이벤트를 현재 구축된 파일 정책의 규칙에 따라 로깅합니다.

시스템은 파일 이벤트를 생성할 때 호출하는 액세스 제어 규칙의 로깅 구성과 관계없이 연결된 연결의 종료도 Secure Firewall Management Center 데이터베이스에 로깅합니다.

악성코드 이벤트

Firepower System(특히 악성코드 대응 기능)은 전체 액세스 제어 구성의 일부로 네트워크 트래픽에서 악성코드를 탐지할 때 악성코드 이벤트를 생성합니다. 악성코드 이벤트에는 결과 이벤트의 속성과 악성코드가 탐지된 방법, 위치, 시간에 대한 상황 데이터가 포함됩니다.

표 ***104:*** 악성코드 이벤트 생성 시나리오

시스템이 파일을 탐지하고 다음을 수행하는 경우	속성
AMP 클라우드(악성코드 클라우드 조회 수행)에서 파일의 속성을 성공적으로 쿼리	Malware(악성코드), Clean(정상) 또는 Unknown(알 수 없음)
AMP 클라우드를 쿼리하지만 연결을 설정할 수 없거나 연결을 사용할 수 없음	사용 불가능 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.
파일에 연결된 위협 점수가 파일을 탐지한 파일 정책에서 정의한 악성코드 임계값 위협 점수를 초과하거나 로컬 악성코드 분석이 악성코드를 식별	악성코드
맞춤형 탐지 목록에 있음(수동으로 악성코드로 표시됨)	맞춤형 탐지
정상 목록에 있음(수동으로 정상으로 표시됨)	정상

악성코드 이벤트의 파일 속성 및 파일 작업

각 파일 규칙에는 시스템이 규칙의 조건과 일치하는 트래픽을 처리하는 방법을 결정하는 관련 작업이 포함됩니다. 파일 규칙 작업으로 *Block Malware(*악성코드 차단*)* 또는 *Malware Cloud Lookup(*악성코드 클라우드 조회*)*을 선택하면 시스템이 AMP 클라우드를 쿼리하여 네트워크를 통과하는 파일에 악성코드가 포함되어 있는지 확인한 다음, 위협이 되는 파일을 차단합니다. 클라우드 조회를 사용하면 SHA-256 해시 값을 기반으로 한 파일의 속성을 가져오고 로깅할 수 있습니다.

다음 테이블에서는 AMP 클라우드에서 반환한 파일 속성과 연결되는 파일 작업을 설명합니다.

표 ***105:*** 악성코드 이벤트의 파일 속성 및 파일 작업

파일 규칙 작업 선택됨	파일 속성	악성코드 이벤트의 파일 작업
• 악성코드 차단 • 악성코드 클라우드 조회	악성코드	차단
	• 정상 • 알 수 없음 • 사용 불가능 • 해당 없음	클라우드 조회 참고 파일 정책 편집기 Advanced Settings(고급 설정)에서 **If AMP Cloud disposition is Unknown, override disposition based upon threat score(AMP Cloud** 속성이 **Unknown(**알 수 없음**)**인 경우 위협 점수를 기반으로 속성 재정의**)** 옵션의 임계값 위협 점수를 설정할 수 있습니다. 임계값 위협 점수를 설정한 경우 동적 분석 점수가 임계값과 같거나 이보다 나쁘면 AMP 클라우드가 알 수 없음으로 판정된 파일은 악성코드로 간주됩니다.

회귀적 악성코드 이벤트

네트워크 트래픽에서 탐지된 악성코드의 경우, 속성이 변경될 수 있습니다. 예를 들어 AMP 클라우드는 이전에는 정상으로 간주되었던 파일이 지금은 악성코드로 식별되는 경우 또는 그 반대의 경우(악성코드로 식별된 파일이 실제로 정상임)를 결정할 수 있습니다. 지난주에 쿼리한 파일의 속성이 변경되면 AMP 클라우드가 시스템에 알립니다. 그러면 두 가지가 발생합니다.

- Secure Firewall Management Center는 새로운 회귀적 악성코드 이벤트를 생성합니다.

  이 새로운 회귀적 악성코드 이벤트는 지난주에 탐지된 SHA-256 해시 값이 동일한 모든 파일의 속성 변경을 나타냅니다. 따라서 이러한 이벤트에는 Secure Firewall Management Center에 속성 변경을 알린 날짜와 시간, 새로운 속성, 파일의 SHA-256 해시 값 및 위협 이름 등 제한된 정보가 포함됩니다. IP 주소나 기타 컨텍스트 정보는 포함되지 않습니다.

- Secure Firewall Management Center은 이전에 탐지된 파일의 파일 속성을 회귀적 이벤트에 연결된 SHA-256 해시 값으로 변경합니다.

  파일의 속성이 Malware(악성코드)로 변경되면 Secure Firewall Management Center은 새 악성코드 이벤트를 데이터베이스에 기록합니다. 새 속성 외에도 이 새 악성코드 이벤트의 정보는 파일이 처음 탐지됐을 때 생성된 파일 이벤트의 정보와 동일합니다.

  파일의 속성이 Clean(정상)으로 변경되는 경우, Secure Firewall Management Center은 악성코드 이벤트를 삭제하지 않습니다. 대신 해당 이벤트는 속성의 변경을 반영합니다. 즉, 정상 속성의 파일이 악성코드 테이블에 나타날 수 있지만 원래 악성코드로 파악된 경우에 한합니다. 악성코드로 식별된 적이 없는 파일은 파일 테이블에만 나타납니다.

AMP for Endpoints에 의해 생성된 악성코드 이벤트

조직에서 AMP for Endpoints를 사용하는 경우, 개별 사용자가 엔드포인트(컴퓨터 및 모바일 디바이스)에 경량 커넥터를 설치합니다. 커넥터는 파일 업로드, 다운로드, 실행, 열기, 복사, 이동 등을 수행할 때 파일을 검사할 수 있습니다. 이러한 커넥터는 AMP 클라우드와 통신하여 검사된 파일에 악성코드가 포함되었는지 확인합니다.

파일이 악성코드로 식별되면 AMP 클라우드는 위협 식별 정보를 Secure Firewall Management Center에 전송합니다. 또한 AMP 클라우드는 검사, 격리, 차단된 실행, 클라우드 회수에 대한 데이터를 비롯한 다른 종류의 정보도 Secure Firewall Management Center에 전송할 수 있습니다. Secure Firewall Management Center는 이러한 정보를 악성코드 이벤트로 로깅합니다.

참고 AMP for Endpoints에 의해 생성된 악성코드 이벤트에서 보고된 IP 주소는 네트워크 맵에 없을 수 있으며, 모니터링되는 네트워크에도 없을 수 있습니다. 구축, 규정 준수 수준, 기타 요인에 따라 AMP for Endpoints가 모니터링하는 조직 내 엔드포인트가 악성코드 대응 에서 모니터링하는 것과 같은 호스트가 아닐 수 있습니다.

Secure Endpoint를 사용한 악성코드 이벤트 분석

조직에서 Cisco Secure Endpoint를 구축한 경우:

- management center 이벤트 페이지에 Secure Endpoint가 탐지한 이벤트와 함께 악성코드 대응 가 탐지한 악성코드 이벤트를 표시하도록 시스템을 구성할 수 있습니다.
- AMP 퍼블릭 클라우드를 사용 중인 경우, 파일 경로 분석과 Secure Endpoint의 특정 SHA에 대한 기타 정보를 볼 수 있습니다.

위의 기능을 구성하려면 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Firepower* 및 *Secure Endpoint* 통합을 참조하십시오.

Secure Endpoint의 이벤트 데이터

조직에서 악성코드 방지를 위해 Secure Endpoint를 구축한 경우, Secure Endpoint의 파일 및 악성코드 데이터를 사용하여 management center에서 작업을 수행할 수 있도록 시스템을 구성할 수 있습니다.

다만 Secure Endpoint의 파일 및 악성코드 데이터와 시스템 악성코드 대응 기능의 파일 및 악성코드 데이터 간의 차이를 알아야 합니다.

Secure Endpoint 악성코드 탐지는 다운로드 또는 실행 시 엔드포인트에서 수행되지만, 매니지드 디바이스는 네트워크 트래픽에서 악성코드를 탐지하기 때문에 두 가지 유형의 악성코드 이벤트에 있는 정보는 서로 다릅니다. 예를 들어 Secure Endpoint가 탐지하는 악성코드 이벤트("엔드포인트 기반 악성코드")에는 파일 경로, 클라이언트 애플리케이션 호출 등에 대한 정보가 포함됩니다. 반면 네트워크 트래픽에서의 악성코드 탐지에는 포트, 애플리케이션 프로토콜, 파일 전송에 사용되는 연결에 대한 원래 IP 주소 정보가 포함됩니다.

또 다른 예로 악성코드 대응 가 탐지하는 악성코드 이벤트("네트워크 기반 악성코드 이벤트")의 경우, 사용자 정보에는 네트워크 검색에서 확인된 내용에 따라, 악성코드가 목표로 한 호스트에 가장 최근

에 로그인한 사용자가 표시됩니다. 하지만 Secure Endpoint에서 보고하는 사용자는 악성코드가 탐지된 엔드포인트에 현재 로그인한 사용자를 나타냅니다.

참고 배포에 따라 Secure Endpoint에서 모니터링하는 엔드포인트는 악성코드 대응 에서 모니터링하는 엔드포인트와 동일한 호스트가 아닐 수 있 습니다. 따라서 Secure Endpoint에서 생성한 악성코드 이벤트는 네트워크 맵에 호스트를 추가하지 않습니다. 그러나 시스템은 IP 및 MAC 주소 데이터를 사용하여 Secure Endpoint 배포에서 가져온 보안 침해 지표로 모니터링되는 호스트에 태그를 지정합니다. 서로 다른 악성코드 솔루션을 통해 모니터링되는 두 호스트의 IP 및 MAC 주소가 같은 경우에는 시스템이 Secure Endpoint IOC로 모니터링되는 호스트에 태그를 잘못 지정할 수 있습니다.

다음 테이블에는 악성코드 방어 라이선스 사용 시 Firepower에서 생성되는 이벤트 데이터와 Secure Endpoint에서 생성되는 이벤트 데이터의 차이점이 요약되어 있습니다.

표 ***106: AMP*** 제품 간 데이터 차이점 요약

기능	악성코드 대응	**Secure Endpoint**
생성되는 이벤트	파일 이벤트, 캡처된 파일, 악성코드 이벤트, 회귀적 악성코드 이벤트	악성코드 이벤트
악성코드 이벤트의 정보	기본적인 악성코드 이벤트 정보 및 연결 데이터(IP 주소, 포트, 애플리케이션 프로토콜)	심층적인 악성코드 이벤트 정보, 연결 데이터 없음
네트워크 파일 전파 흔적 분석	management center기반	management center 및 Secure Endpoint 관리 콘솔에는 각각 네트워크 파일 경로 분석이 있습니다. 두 가지 모두 유용합니다.

관련 주제

Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 *Integrate Firepower* 및 *Secure Endpoint* 통합

파일 및 악성코드 이벤트 워크플로 사용

테이블에서 파일 및 악성코드 이벤트를 보고 분석에 관련된 정보에 따라 이벤트 보기를 조작하려면 이 절차를 사용하십시오. 이벤트에 액세스할 때 볼 수 있는 페이지는, 넓은 보기에서 좀 더 집중된 보기로 이동하여 이벤트를 평가하는 데 사용할 수 있는 일련의 페이지인 워크플로에 따라 달라집니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

다음 중 하나를 선택합니다.

- **Analysis(**분석**)** > **Files(**파일**)** > **File Events(**파일 이벤트**)**
- **Analysis(**분석**)** > **Files(**파일**)** > **Malware Events(**악성코드 이벤트**)**

팁 이벤트의 테이블 보기에는 여러 필드가 기본적으로 숨겨져 있습니다. 이벤트 보기에서 숨겨진 필드를 표시하려면 검색 제한 사항을 확장한 다음 **Disabled Columns(**비활성화된 열**)** 아래에서 필드 이름을 클릭합니다.

팁 특정 파일이 탐지된 연결을 신속하게 보려면 테이블의 확인란을 사용하여 파일을 선택한 다음 **Jump to(**이동**)** 드롭다운 목록에서 **Connections Events(**연결 이벤트**)**를 선택합니다.

팁 옵션을 보려면 테이블에서 항목을 마우스 오른쪽 버튼으로 클릭합니다. (옵션을 제공하지 않는 열도 있습니다.)

관련 항목

파일 및 악성코드 이벤트 필드, 863 페이지
사전 정의 파일 워크플로, 681 페이지
사전 정의 악성코드 워크플로, 681 페이지
이벤트 보기 구성, 210 페이지

파일 및 악성코드 이벤트 필드

워크플로를 사용하여 확인 및 검색할 수 있는 파일 및 악성코드 이벤트는 이 섹션에서 열거하는 필드를 포함합니다. 개별 이벤트에 사용 가능한 정보는 정보 생성 방법과 이유에 따라 달라질 수 있습니다.

참고 악성코드 대응 에 의해 악성코드로 식별된 파일은 파일 이벤트와 악성코드 이벤트를 모두 생성합니다. Secure Endpoint가 생성한 악성코드 이벤트에는 대응하는 파일 이벤트가 없으며, 파일 이벤트는 Secure Endpoint 관련 필드를 포함하지 않습니다.

시스템 로그 메시지는 초기 값으로 채워지며, management center 웹 인터페이스의 해당 필드가 회고 판정 등으로 업데이트되더라도 시스템 로그 메시지는 업데이트되지 않습니다.

작업**(**시스템 로그**: FileAction)**

파일을 탐지한 파일 정책 규칙과 연결된 작업 및 관련된 모든 파일 규칙 작업 옵션

AMP 클라우드

AMP for Endpoints 이벤트 출처인 AMP 클라우드의 이름.

애플리케이션 파일 이름

AMP for Endpoints 탐지가 발생했을 때 악성코드 파일에 액세스하는 클라이언트 애플리케이션. 이러한 애플리케이션은 네트워크 검색 또는 애플리케이션 제어에 연결되지 않습니다.

애플리케이션 파일 **SHA256**

탐지가 발생했을 때 AMP for Endpoints를 탐지 또는 격리하는 파일에 액세스한 상위 파일의 SHA-256 해시 값.

통합 이벤트 뷰어에서 이 필드는 **Application File SHA-256(**애플리케이션 파일 **SHA-256)**으로 표시됩니다.

애플리케이션 프로토콜**(**시스템 로그**: ApplicationProtocol)**

매니지드 디바이스가 파일을 탐지한 트래픽에 의해 사용되는 애플리케이션 프로토콜.

애플리케이션 프로토콜 카테고리 또는 태그

애플리케이션의 기능을 파악하도록 애플리케이션의 특성을 분류하는 기준.

애플리케이션 위험성

연결에서 탐지된 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

아카이브 깊이**(**시스템 로그**: ArchiveDepth)**

아카이브 파일에 중첩되는 파일의 레벨(해당되는 경우).

아카이브 이름**(**시스템 로그**: ArchiveFileName)**

악성코드 파일을 포함하는 아카이브 파일의 이름(해당되는 경우).

아카이브 파일의 내용을 보려면 **Analysis(**분석**) > Files(**파일**)**에 있는 아카이브 파일 목록 표로 이동하고 아카이브 파일의 테이블 행을 마우스 오른쪽 단추로 클릭한 다음 **View Archive Contents(**아카이브 내용 보기**)**를 클릭합니다.

아카이브 **SHA256(**시스템 로그**: ArchiveSHA256)**

악성코드 파일을 포함하는 아카이브 파일(해당되는 경우)의 SHA-256 해시 값.

아카이브 파일의 내용을 보려면 Analysis(분석) > Files(파일)에 있는 아카이브 파일 목록 표로 이동하고 아카이브 파일의 테이블 행을 마우스 오른쪽 단추로 클릭한 다음 **View Archive Contents(**아카이브 내용 보기**)**를 클릭합니다.

ArchiveFileStatus(시스템 로그만 있음**)**

검사 중인 아카이브의 상태. 다음과 같은 값을 사용할 수 있습니다.

- Pending(보류 중) - 아카이브를 검사하는 중

- Extracted(추출됨) - 문제없이 검사함
- Failed(장애 발생함) - 시스템 자원이 부족하여 검사하지 못함
- Depth Exceeded(수준 초과됨) - 검사는 성공했으나 아카이브에서 중첩 검사 수준이 초과됨
- Encrypted(암호화됨) - 검사가 일부분 성공함(아카이브가 암호화된 아카이브이거나 암호화된 아카이브를 포함함)
- Not Inspectable(검사 불가) - 검사가 일부분 성공함(파일이 손상되었거나 형식이 잘못되었을 수 있음)

사업 타당성

연결에서 탐지된 애플리케이션 트래픽과 연계된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

카테고리/파일 유형 카테고리

파일 유형의 일반적인 범주(예: Office 문서, 아카이브, 멀티미디어, 실행 파일, PDF 파일, 인코딩, 그래픽 또는 시스템 파일 등)

클라이언트(시스템 로그: **Client**)

한 호스트에서 실행되며 서버에 의존하여 파일을 전송하는 클라이언트 애플리케이션.

클라이언트 카테고리 또는 태그

애플리케이션의 기능을 파악하도록 애플리케이션의 특성을 분류하는 기준.

Connection Counter (시스템 로그만 해당)

다른 동시 연결에서 하나의 연결을 구분하는 카운터입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

Connection Instance ID (시스템 로그만 해당)

연결 이벤트를 처리한 Snort 인스턴스입니다. 이 필드 자체에는 중요한 의미가 없습니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

개수

동일한 행을 둘 이상 생성하는 제약 조건을 적용하는 경우, 각 행의 정보와 일치하는 이벤트의 수.

탐지 이름

탐지된 악성코드의 이름.

탐지기

악성코드를 식별하는 AMP for Endpoints 탐지기(예: ClamAV, Spero 또는 SHA).

디바이스

파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트에서 파일을 탐지한 디바이스의 이름.

AMP for Endpoints에 의해 생성된 악성코드 이벤트 및 AMP 클라우드에 의해 생성된 회귀적 악성코드 이벤트에서 management center의 이름.

DeviceUUID (시스템 로그만 해당**)**

이벤트를 생성한 Firepower 디바이스의 고유 식별자입니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

속성**/**파일 속성**(**시스템 로그**: SHA_Disposition)**

파일의 속성:

Malware(악성코드**)**

AMP 클라우드가 파일을 악성코드로 분류했거나, 로컬 악성코드 분석에서 악성코드가 식별되었거나, 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다.

정상

AMP 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. 정상 파일은 정상으로 변경된 경우에만 악성코드 테이블에 나타납니다.

알 수 없음

시스템이 AMP 클라우드를 쿼리했으나 파일에 상태가 할당되지 않았음을 나타냅니다. 즉, AMP 클라우드에서 파일을 분류하지 않았습니다.

맞춤형 탐지

사용자가 파일을 커스텀 탐지 목록에 추가했음을 나타냅니다.

사용 불가능

시스템이 AMP 클라우드를 쿼리하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.

해당 없음

파일 탐지 또는 파일 차단 규칙이 파일을 처리했으며 Secure Firewall Management Center이 AMP 클라우드를 쿼리하지 않았음을 나타냅니다.

파일 속성은 시스템이 AMP 클라우드를 쿼리하지 않은 파일에 대해서만 표시됩니다.

시스템 로그는 초기 속성만 반영합니다. 회귀적 판정을 반영하도록 업데이트 되지 않습니다.

도메인

파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트에서 파일을 탐지한 디바이스의 도메인. AMP for Endpoints에 의해 생성된 악성코드 이벤트 및 AMP 클라우드에 의해 생성된 회귀적 악성코드 이벤트에서 해당 이벤트를 보고한 AMP 클라우드 연결과 관련된 도메인.

이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

DstIP(시스템 로그만 있음**)**

연결에 응답한 호스트의 IP 주소. FileDirection 필드 값에 따라 파일 발신자나 수신자의 IP 주소일 수 있습니다.

FileDirection이 **`Upload`(**업로드**)** 인 경우 파일 수신자의 IP 주소입니다.

FileDirection이 **`Download`(**다운로드**)** 인 경우 파일 발신자의 IP 주소입니다.

SrcIP도 참조하십시오.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 790 페이지도 참조하십시오.

DstPort(시스템 로그만 있음**)**

DstIP아래 설명된 연결에 사용되는 포트.

이그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에서 벗어날 때 사용하는 가상 라우터의 이름입니다.

이벤트 하위 유형

악성코드 탐지로 이어진 AMP for Endpoints 작업(예: Create(생성), Execute(실행), Move(이동) 또는 Scan(스캔)).

이벤트 유형

악성코드 이벤트 하위 유형.

파일 이름(시스템 로그: **FileName)**

파일의 이름

파일 경로

AMP for Endpoints에 의해 탐지된 악성코드 파일의 파일 경로(파일 이름 제외).

파일 정책**(**시스템 로그**: FilePolicy)**

파일을 탐지한 파일 정책.

파일 스토리지**/**저장됨**(**시스템 로그**: FileStorageStatus)**

이벤트와 관련 된 파일의 저장 상태:

Stored(저장됨**)**

관련된 파일이 현재 저장되어 있는 모든 이벤트를 반환합니다.

Stored in connection(연결에 저장됨**)**

관련된 파일이 현재 저장되어 있는지와 상관없이, 시스템이 관련된 파일을 캡처 및 저장한 모든 이벤트를 반환합니다.

Failed(TLS 필수 실패**)**

시스템이 관련된 파일을 저장하지 못한 모든 이벤트를 반환합니다.

시스템 로그 필드는 초기 상태만 포함합니다. 변경된 상태를 반영하도록 업데이트되지 않습니다.

File Timestamp(파일 타임스탬프**)**

AMP for Endpoints가 악성코드 파일이 생성된 것으로 탐지한 시간 및 날짜.

FileDirection(시스템 로그만 있음**)**

연결 중 파일이 업로드되거나 다운로드되었는지 여부. 가능한 값은 다음과 같습니다.

- Download(다운로드) — DstIP에서 SrcIP로 파일이 전송되었습니다.
- Upload(업로드) — SrcIP에서 DstIP로 파일이 전송되었습니다.

FileSandboxStatus(시스템 로그만 있음**)**

동적 분석을 위해 파일이 전송되었는지 여부와 그러한 경우 해당 상태를 나타냅니다.

첫 번째 패킷 시간 **(**시스템 로그만 해당**)**

시스템이 첫 번째 패킷을 수신한 시간입니다.

다음 필드는 특정 파일 또는 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)와 관련된 연결 이벤트를 종합적으로 개별 식별합니다.

FirstPacketSecond(시스템 로그만 있음**)**

파일 다운로드 또는 업로드 플로우가 시작된 시간으로, .

이벤트가 발생한 시간이 메시지 헤더 타임스탬프에 캡처됩니다.

HTTP 응답 코드

파일이 전송된 경우 클라이언트의 HTTP 요청에 대한 응답으로 제출된 HTTP 상태 코드.

인그레스 가상 라우터

가상 라우팅을 사용하는 네트워크에서 트래픽이 네트워크에 진입할 때 사용하는 가상 라우터의 이름입니다.

IOC

악성코드 이벤트가 연결과 관련된 호스트에 대해 IOC(indication of compromise)를 트리거했는지 여부. AMP for Endpoints 데이터 IOC 규칙을 트리거하는 경우, 전체 악성코드 이벤트가 AMP IOC 유형으로 생성됩니다.

메시지

악성코드 이벤트와 연결된 추가 정보. 파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트의 경우, 이 필드는 속성이 변경되어 관련 회귀적 이벤트가 있는 파일에 대해서만 입력됩니다.

Protocol(시스템 로그만 있음)

연결에 사용된 프로토콜(예: TCP 또는 UDP).

Receiving Continent(수신 대륙)

파일을 수신하는 호스트의 대륙.

Receiving Country(수신 국가)

파일을 수신하는 호스트의 국가.

수신 **IP**

management center 웹 인터페이스에서 파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트에 대해 파일을 수신하는 호스트의 IP 주소. 이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 790 페이지도 참조하십시오.

AMP for Endpoints에 의해 생성된 악성코드 이벤트에서 커넥터가 이벤트를 보고한 엔드포인트의 IP 주소.

시스템 로그에 해당하는 항목(Firepower 디바이스에서 생성된 이벤트만 해당)은 **DstIP** 및 **SrcIP**를 참조하십시오.

수신 포트

management center 웹 인터페이스에서 파일이 탐지된 트래픽에 의해 사용된 대상 포트.

시스템 로그 해당 정보는 **DstIP**, **SrcIP**, **DstPort**, **SrcPort**를 참조하십시오.

보안 상황(시스템 로그: **Context**)

트래픽이 통과한 가상 방화벽 그룹을 식별하는 메타데이터입니다. 다중 상황 모드에서 실행되는 ASA FirePOWER 디바이스를 최소한 한 개 관리하는 경우 시스템에 이 필드만 표시됩니다.

Sending Continent(송신 대륙**)**

파일을 전송하는 호스트의 대륙.

Sending Country(송신 국가**)**

파일을 전송하는 호스트의 국가.

송신 **IP**

management center 웹 인터페이스에서 파일을 보내는 호스트의 IP 주소. 이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 790 페이지도 참조하십시오.

시스템 로그 해당 정보는 **DstIP** 및 **SrcIP**를 참조하십시오.

송신 포트

management center 웹 인터페이스에서 파일이 탐지된 트래픽에 의해 사용된 소스 포트.

시스템 로그 해당 정보는 **DstIP**, **SrcIP**, **DstPort**, **SrcPort**를 참조하십시오.

SHA256/파일 **SHA256(**시스템 로그**: FileSHA256)**

파일의 SHA-256 해시 값

SHA256 값을 생성하려면 다음 중 하나를 통해 파일을 처리해야 합니다.

- **Store files(**파일 저장**)**가 활성화된 Detect Files(파일 탐지) 파일 규칙
- **Store files(**파일 저장**)**가 활성화된 Block Files(파일 차단) 파일 규칙
- Malware Cloud Lookup file(악성코드 클라우드 검색) 파일 규칙
- Block Malware file(악성코드 차단) 파일 규칙
- AMP for Endpoints

이 열에는 가장 최근에 탐지된 파일 이벤트 및 파일 속성을 나타내고 네트워크 파일 경로로 링크되는 네트워크 파일 경로 아이콘도 표시됩니다.

크기**(KB)/**파일 크기**(KB)(**시스템 로그**: FileSize)**

management center 웹 인터페이스에서 킬로바이트 단위의 파일 크기.

시스템 로그 메시지에서 바이트 단위의 파일 크기.

파일을 완전히 수신하기 전에 시스템에서 파일 유형을 결정하는 경우, 파일 크기가 계산되지 않을 수 있습니다. 그러한 경우 이 필드는 공란입니다.

SperoDisposition(시스템 로그만 있음**)**

파일 분석에 SPERO 서명이 사용되었는지를 나타냅니다. 가능한 값은 다음과 같습니다.

- 파일에서 수행되는 Spero 탐지

- 파일에서 수행되지 않는 Spero 탐지.

SrcIP(시스템 로그만 있음)

연결을 시작한 호스트의 IP 주소. FileDirection 필드 값에 따라 파일 발신자나 수신자의 IP 주소일 수 있습니다.

FileDirection이 **`Upload`**(업로드) 인 경우 파일 발신자의 IP 주소입니다.

FileDirection이 **`Download`**(다운로드) 인 경우 파일 수신자의 IP 주소입니다.

DstIP도 참조하십시오.

이니시에이터/응답자, 소스/대상, 그리고 발신자/수신자 필드 지침, 790 페이지도 참조하십시오.

SrcPort(시스템 로그만 있음)

SrcIP아래 설명된 연결에 사용되는 포트.

SSL 실제 작업(시스템 로그: **SSLActualAction**)

시스템이 암호화된 트래픽에 적용하는 작업.

Block or Block with reset(차단 또는 차단 후 재설정)

차단된 암호화된 연결을 나타냅니다.

암호 해독(재서명)

다시 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

암호 해독(대체 키)

대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 암호 해독된 발신 연결을 나타냅니다.

암호 해독(알려진 키)

알려진 개인 키를 사용하여 암호 해독된 수신 연결을 나타냅니다.

기본 작업

연결이 기본 작업에 의해 처리되었음을 나타냅니다.

암호 해독 안 함

시스템이 암호 해독하지 않은 연결을 나타냅니다.

검색 워크플로 페이지의 **SSL Status**(SSL 상태) 필드에 필드값이 표시됩니다.

SSL 인증서 정보

트래픽 암호화에 사용하는 공개 키 인증서에 저장된 정보로 다음을 포함합니다.

- Subject/Issuer Common Name(대상자/발급자 공용 이름)
- Subject/Issuer Organization(대상자/발급자 기관)

- Subject/Issuer Organization Unit(대상자/발급자 기관 부서)
- Not Valid Before/After(유효기간)
- Serial Number, Certificate Fingerprint(일련 번호, 인증서 지문)
- Public Key Fingerprint(공개 키 지문)

시스템 로그는 **SSLCertificate**를 참조하십시오.

SSL 실패 이유**(**시스템 로그**: SSLFlowStatus)**

시스템이 암호화된 트래픽의 암호 해독에 실패한 이유:

- Unknown(알 수 없음)
- No Match(일치하지 않음)
- Success(TLS 필수 성공)
- Uncached Session(캐시되지 않은 세션)
- Unknown Cipher Suite(알 수 없는 암호 그룹)
- Unsupported Cipher Suite(지원되지 않는 암호 그룹)
- Unsupported SSL Version(지원되지 않는 SSL 버전)
- SSL Compression Used(SSL 압축 사용됨)
- Session Undecryptable in Passive Mode(패시브 모드에서 세션 암호 해독 불가)
- Handshake Error(핸드셰이크 오류)
- Decryption Error(암호 해독 오류)
- Pending Server Name Category Lookup(서버 이름 카테고리 조회 보류 중)
- Pending Common Name Category Lookup(공용 이름 카테고리 조회 보류 중)
- Internal Error
- Network Parameters Unavailable(네트워크 파라미터 사용 불가)
- Invalid Server Certificate Handle(유효하지 않은 서버 인증서 처리)
- Server Certificate Fingerprint Unavailable(서버 인증서 지문 사용 불가)
- Cannot Cache Subject DN(대상자 DN 캐시 불가)
- Cannot Cache Issuer DN(발급자 DN 캐시 발가)
- Unknown SSL Version(알 수 없는 SSL 버전)
- External Certificate List Unavailable(외부 인증서 목록 사용 불가)
- External Certificate Fingerprint Unavailable(외부 인증서 지문 사용 불가)

- Internal Certificate List Invalid(내부 인증서 목록이 유효하지 않음)
- Internal Certificate List Unavailable(내부 인증서 목록 사용 불가)
- Internal Certificate Unavailable(내부 인증서 사용 불가)
- Internal Certificate Fingerprint Unavailable(내부 인증서 지문 사용 불가)
- Server Certificate Validation Unavailable(서버 인증서 검증 사용 불가)
- Server Certificate Validation Failure(서버 인증서 검증 장애)
- Invalid Action(유효하지 않은 작업)

검색 워크플로 페이지의 **SSL Status(SSL** 상태**)** 필드에 필드값이 표시됩니다.

SSL 상태

암호화된 연결을 로깅한 **SSL Actual Action(SSL** 실제 작업**)**(해독 규칙, 기본 작업 또는 암호 해독이 불가능한 트래픽 작업)과 관련된 작업. 잠금 아이콘이 TLS/SSL 인증서 세부 사항으로 연결됩니다. 인증서를 사용할 수 없는 경우(예: TLS/SSL 핸드셰이크 오류로 연결 차단), 잠금 아이콘이 흐리게 표시됩니다.

시스템이 암호화된 연결을 해독하지 못할 경우, 실행된 **SSL Actual Action(SSL** 실제 작업**)** (해독 불가능한 트래픽 작업)과 **SSL Failure Reason(SSL** 실패 이유**)**가 표시됩니다. 예를 들어, 시스템이 알 수 없는 암호 그룹으로 암호화된 트래픽을 탐지하고 추가 검사 없이 이를 허용할 경우 이 필드는 `Do Not Decrypt (Unknown Cipher Suite)`(암호 해독 하지 않음(알려지지 않은 암호화 그룹))로 표시됩니다.

이 필드를 검색할 때 **SSL Actual Action(SSL** 실제 작업**)** 중 하나 이상과 **SSL Failure Reason(SSL** 실패 이유**)**를 입력하고 시스템이 처리했거나 암호 해독에 실패한 암호화된 트래픽을 확인합니다.

SSL 대상자**/**발급자 국가

암호화 인증서와 관련된 대상자 또는 발급자 국가의 2자 ISO 3166-1 alpha-2 국가 코드.

SSLCertificate(시스템 로그만 있음**)**

TLS/SSL 서버의 인증서 지문.

위협 이름**(**시스템 로그**: ThreatName)**

탐지된 악성코드의 이름.

위협 점수**(**시스템 로그**: ThreatScore)**

이 파일과 가장 최근에 연결된 위협 점수. 동적 분석 과정에서 관찰된 잠재적으로 악의적인 동작을 기준으로 한 0부터 100까지의 값입니다.

위협 점수 아이콘이 Dynamic Analysis Summary(동적 분석 요약) 보고서로 링크됩니다.

시간

이벤트가 생성된 날짜 및 시간 이 필드는 검색할 수 없습니다.

시스템 로그 메시지에서 **FirstPacketSecond**를 참조하십시오.

유형/파일 유형(시스템 로그: **FileType)**

HTML 또는 MSEXE 등의 파일 형식

URI/파일 **URI**(시스템 로그: **URI)**

파일 트랜잭션과 관련된 연결의 URI(예: 사용자가 파일을 다운로드하는 URL).

사용자(시스템 로그: **User)**

연결을 시작한 IP 주소에 연결된 사용자 이름입니다. 이 IP 주소가 네트워크 외부에 있는 경우, 일반적으로 연결된 사용자 이름을 알 수 없습니다.

해당하는 경우 사용자 이름 앞에 `<realm>\`을 입력합니다.

파일 이벤트 및 Firepower 디바이스에 의해 생성된 악성코드 이벤트의 경우, 이 필드에는 ID 정책 또는 권한 있는 로그인에 의해 결정된 사용자 이름이 표시됩니다. ID 정책이 없는 경우, No Authentication Required(인증 필요 없음)가 표시됩니다.

AMP for Endpoints에 의해 생성된 악성코드 이벤트에서 AMP for Endpoints가 사용자 이름을 결정합니다. 이러한 사용자는 사용자 검색 또는 제어에 연결할 수 없습니다. 이러한 사용자는 Users(사용자) 테이블에 나타나지 않으며 세부 사항도 확인할 수 없습니다.

웹 애플리케이션(시스템 로그: **WebApplication)**

연결에서 탐지된 HTTP 트래픽의 콘텐츠 또는 요청된 URL을 나타내는 웹 애플리케이.

웹 애플리케이션 카테고리 또는 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준

악성코드 이벤트 하위 유형

다음 표에는 악성코드 이벤트 하위 유형, AMP for Networks가 생성하는 악성코드 이벤트("네트워크 기반 악성코드 이벤트") 또는 AMP for Endpoints가 생성하는 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")에 해당 하위 유형이 있을 수 있는지 여부, 시스템이 해당 하위 유형을 사용하여 네트워크 파일 경로 분석을 작성하는지 여부가 나열되어 있습니다.

표 ***107:*** 악성코드 이벤트 유형

악성코드 이벤트 하위 유형/검색 값	악성코드 대응	**AMP for Endpoints**	파일 경로 분석
네트워크 파일 전송에서 탐지된 위협	예	아니요	예
네트워크 파일 전송에서 탐지된 위협(회귀적)	예	아니요	예

악성코드 이벤트 하위 유형/검색 값	악성코드 대응	**AMP for Endpoints**	파일 경로 분석
위협 탐지됨	아니요	예	예
제외에서 위협 탐지	아니요	예	예
위협 격리됨	아니요	예	예
AMP IOC(보안 침해 지표)	아니요	예	아니요
차단된 실행	아니요	예	아니요
Cloud Recall 격리	아니요	예	아니요
Cloud Recall 격리 시도 실패	아니요	예	아니요
클라우드 리콜 격리 시작	아니요	예	아니요
격리에서 Cloud Recall 복원	아니요	예	아니요
격리에서 Cloud Recall 복원 실패	아니요	예	아니요
격리에서 클라우드 리콜 복원 시작	아니요	예	아니요
격리 실패	아니요	예	아니요
격리 항목 복원	아니요	예	아니요
격리 복원 실패	아니요	예	아니요
격리 복원 시작	아니요	예	아니요
스캔 완료, 탐지 항목 없음	아니요	예	아니요
스캔 완료, 탐지 항목 있음	아니요	예	아니요
스캔 실패	아니요	예	아니요
스캔 시작	아니요	예	아니요

파일 및 악성코드 이벤트 필드에서 사용할 수 있는 정보

다음 표에는 시스템이 각 파일 및 악성코드 이벤트 필드에 정보를 표시하는지 여부가 나열되어 있습니다.

조직이 AMP for Endpoints를 구축하고 해당 제품을 Firepower 구축에 통합한 경우:

- AMP for Endpoints 구축에서 가져온 악성코드 이벤트 및 보안 침해 지표 (IOC)에는 컨텍스트 연결 정보가 포함되지 않지만 파일 경로와 호출 클라이언트 애플리케이션 등 다운로드 또는 실행 시 얻는 정보는 포함됩니다.
- 파일 이벤트 테이블 보기에는 AMP for Endpoints 관련 필드가 표시되지 않습니다.

표 ***108:*** 파일 및 악성코드 이벤트 필드에서 사용할 수 있는 정보

필드	파일 이벤트	**Firepower System**에서 탐지되는 악성코드 이벤트	**Firepower System**에서 탐지되는 회귀적 이벤트	**AMP for Endpoints**에서 탐지되는 악성코드 이벤트
작업	예	예	예	아니요
AMP 클라우드	아니요	아니요	아니요	예
애플리케이션 파일 이름	아니요	아니요	아니요	예
애플리케이션 파일 SHA256	아니요	아니요	아니요	예
애플리케이션 프로토콜	예	예	아니요	아니요
애플리케이션 프로토콜 카테고리 또는 태그	예	예	예	아니요
애플리케이션 위험성	예	예	예	아니요
아카이브 수준	예	예	아니요	예
아카이브 이름	예	예	아니요	예
아카이브 SHA256	예	예	아니요	예
사업 타당성	예	예	예	아니요
카테고리/파일 유형 카테고리	예	예	아니요	예
클라이언트	예	예	예	아니요
클라이언트 카테고리 또는 태그	예	예	예	아니요
개수	예	예	예	예
탐지 이름	아니요	예	아니요	아니요
탐지기	아니요	아니요	아니요	예
디바이스	예	예	예	예
속성/파일 속성	예	예	예	아니요
도메인	예	예	예	예
이벤트 하위 유형	아니요	아니요	아니요	예
이벤트 유형	아니요	예	예	예
파일 이름	예	예	아니요	예

필드	파일 이벤트	**Firepower System**에서 탐지되는 악성코드 이벤트	**Firepower System**에서 탐지되는 회귀적 이벤트	**AMP for Endpoints**에서 탐지되는 악성코드 이벤트
파일 경로	아니요	아니요	아니요	예
파일 정책	예	아니요	아니요	아니요
파일 타임스탬프	아니요	아니요	아니요	예
HTTP 응답 코드	예	예	아니요	아니요
IOC(보안 침해 지표)	아니요	예	예	예
메시지	예	예	아니요	예
수신 대륙	예	예	예	아니요
수신 국가	예	예	아니요	아니요
수신 IP	예	예	아니요	예
수신 포트	예	예	아니요	아니요
보안 상황	예	예	예	예
송신 대륙	예	예	예	아니요
송신 국가	예	예	아니요	아니요
송신 IP	예	예	아니요	아니요
송신 포트	예	예	아니요	아니요
SHA256/파일 SHA256	예	예	예	예
크기(KB)/파일 크기(KB)	예	예	아니요	예
SSL 실제 작업(검색만 해당)	예	예	아니요	아니요
SSL 인증서 정보(검색만 해당)	예	예	아니요	아니요
SSL 실패 이유(검색만 해당)	예	예	아니요	아니요
SSL 상태	예	예	아니요	아니요
SSL 주체/발급자 국가(검색만 해당)	예	예	아니요	아니요
파일 스토리지/저장됨(검색만 해당)	예	예	아니요	아니요
위협 이름	아니요	예	예	예

필드	파일 이벤트	**Firepower System**에서 탐지되는 악성 코드 이벤트	**Firepower System**에서 탐지되는 회귀적 이벤트	**AMP for Endpoints**에서 탐지되는 악성코드 이벤트
위협 점수	예	예	아니요	아니요
시간	예	예	예	예
파일/파일 형식	예	예	아니요	예
URI/파일 URI	예	예	아니요	아니요
사용자	예	예	아니요	예
웹 애플리케이션	예	예	예	아니요
웹 애플리케이션 카테고리 또는 태그	예	예	예	아니요

분석된 파일에 대한 세부 정보 보기

팁 추가 옵션을 보려면 이벤트 페이지의 테이블에서 파일 SHA를 마우스 오른쪽 버튼으로 클릭합니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지 섹션을 참조해 주십시오.

파일 구성 보고서

로컬 악성코드 분석 또는 동적 분석을 구성하는 경우, 시스템은 파일을 분석한 후 파일 구성 보고서를 생성합니다. 이 보고서를 사용하면 추가로 파일을 분석하여 포함된 악성 코드를 파일이 전달할 수 있는지 여부를 확인할 수 있습니다.

파일 구성 보고서에는 파일 속성, 파일에 포함된 개체, 탐지된 바이러스가 나열됩니다. 파일 구성 보고서에는 해당 파일 유형과 관련된 추가 정보도 나열될 수 있습니다. 시스템은 저장된 파일을 정리할 때 연결된 파일 구성 보고서도 정리합니다.

파일 구성 정보를 보려면 네트워크 파일 경로 분석 사용, 889 페이지를 참조하십시오.

AMP 프라이빗 클라우드에서 파일 세부 정보 보기

AMP 프라이빗 클라우드를 구축한 경우, 프라이빗 클라우드에서 분석된 파일에 대한 추가 세부 정보를 볼 수 있습니다.

자세한 내용은 프라이빗 클라우드 설명서를 참조하십시오.

프로시저

AMP 프라이빗 클라우드 콘솔에 직접 로그인합니다.

위협 점수 및 동적 분석 요약 보고서

위협 점수

표 ***109:*** 위협 점수 평가

위협 점수	숫자 점수	아이콘
Low	0-24	낮음
Medium	25-69	중간
High	70-94	높음
Very High	95-100	매우 높음

Secure Firewall Management Center은 파일의 속성과 동일한 시간 동안 파일의 위협 점수를 캐시합니다. 이러한 파일이 나중에 탐지되는 경우, 시스템은 Secure Malware Analytics 클라우드 또는 Secure Malware Analytics 어플라이언스를 다시 쿼리하는 대신 캐시된 위협 점수를 표시합니다. 위협 점수가 정의된 악성코드 임계값 점수를 초과하는 파일에 자동으로 악성코드 파일 속성을 할당할 수 있습니다.

동적 분석 요약

동적 분석 요약을 사용할 수 있는 경우 위협 점수 아이콘을 클릭하여 위협 점수를 볼 수 있습니다. 여러 보고서가 존재하는 경우, 이 요약은 정확한 위협 점수와 일치하는 최근 보고서를 기반으로 합니다. 정확한 위협 점수와 일치하는 보고서가 없으면 위협 점수가 가장 높은 보고서가 표시됩니다. 보고서가 둘 이상이면 위협 점수를 선택하여 각각의 보고서를 볼 수 있습니다.

요약에는 위협 점수를 구성하는 각 구성 요소 위협이 나열되어 있습니다. 각 위협 요소를 확장하여 AMP 클라우드에서 발견한 내용 및 이 구성 요소 위협과 관련된 프로세스를 나열할 수 있습니다.

프로세스 트리에는 Secure Malware Analytics 클라우드가 파일 실행을 시도했을 때 시작된 프로세스가 표시됩니다. 이는 악성코드가 포함된 파일이 예상을 뛰어넘어 프로세스 및 시스템 리소스에 대한 액세스를 시도했는지(예: Word 문서를 실행하여 Microsoft Word를 열고, Explorer를 시작한 다음 Java Runtime Environment 시작) 여부를 파악하는 데 도움이 될 수 있습니다.

나열된 각 프로세스에는 실제 프로세스 확인에 사용할 수 있는 프로세스 식별자가 포함되어 있습니다. 프로세스 트리의 하위 노드는 상위 프로세스의 결과로 시작된 프로세스를 나타냅니다.

동적 분석 요약에서 **View Full Report(**전체 보고서 보기**)**를 클릭하여 AMP 클라우드의 전체 분석이 자세히 설명된 전체 분석 보고서를 볼 수 있습니다. 여기에는 일반 파일 정보, 탐지된 모든 프로세스에 대한 보다 심층적인 검토, 파일 분석의 분류 및 기타 관련 정보가 포함되어 있습니다.

Cisco Secure Malware Analytics 클라우드에서 동적 분석 결과 보기

Secure Malware Analytics는 분석된 파일에 대해 management center에서 제공하는 것보다 자세한 보고를 제공합니다. 조직이 Secure Malware Analytics 클라우드 계정을 가지고 있다면 Secure Malware Analytics 포털에 직접 액세스하여 매니지드 디바이스에서 분석을 위해 전송한 파일에 대한 추가 세부 정보를 볼 수 있습니다.

시작하기 전에

- management center를 Secure Malware Analytics 클라우드 계정과 연결합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 퍼블릭 클라우드의 동적 분석 결과에 대한 액세스 활성화를 참조하십시오.
- 라이선스 요구 사항: 악성코드
- 이 작업을 수행하려면 전역 도메인에 있어야 합니다.
- 관리, 액세스 관리, 네트워크 관리 사용자 역할 중 하나가 있어야 합니다.

프로시저

단계 **1** Secure Malware Analytics 설명서에서 제공하는 주소에서 Secure Malware Analytics 클라우드 포털에 액세스합니다.

단계 **2** 이 작업의 사전 요구 사항에서 연결을 생성하는 데 사용한 계정 자격 증명을 사용하여 로그인합니다.

단계 **3** 조직이 전송한 파일을 보거나 SHA를 사용하여 특정 파일을 검색합니다.

질문이 있는 경우 Secure Malware Analytics 설명서를 참조하십시오.

캡처된 파일 워크플로 사용

매니지드 디바이스는 네트워크 트래픽에서 탐지된 파일을 캡처할 때 이벤트를 로깅합니다.

참고 악성코드가 포함된 파일을 디바이스가 캡처하는 경우, 디바이스는 2개의 이벤트를 생성합니다. 즉, 파일을 탐지하면 파일 이벤트를 생성하고 악성코드를 탐지하면 악성코드 이벤트를 생성합니다.

테이블에서 캡처된 파일 목록을 보고 분석과 관련된 정보에 따라 이벤트 보기를 조작하려면 이 절차를 사용하십시오. 캡처된 파일에 액세스할 때 볼 수 있는 페이지는, 넓은 보기에서 좀 더 집중된 보기로 이동하여 이벤트를 평가하는 데 사용할 수 있는 일련의 페이지인 워크플로에 따라 달라집니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

파일 정책 업데이트 등 구성 변경 후 시스템이 파일을 다시 캡처하는 경우, 시스템은 해당 파일의 기존 정보를 업데이트합니다.

예를 들어 악성 코드 클라우드 조회 작업을 사용하여 파일을 캡처하도록 파일 정책을 구성하는 경우, 시스템은 파일과 함께 파일 속성 및 위협 점수를 저장합니다. 그런 다음 파일 정책을 업데이트하고 시스템이 새로운 **Detect Files(**파일 탐지**)** 작업으로 인해 동일한 파일을 다시 캡처하는 경우, 시스템은 파일의 **Last Changed(**마지막으로 변경된**)** 값을 업데이트합니다. 하지만 사용자가 다른 악성코드 클라우드 조회를 수행하지 않았더라도 시스템은 기존 속성과 위협 점수를 제거하지 않습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

Analysis(분석**)** > **Files(**파일**)** > **Captured Files(**캡처된 파일**)**을(를) 선택합니다.

팁 이벤트의 테이블 보기에는 여러 필드가 기본적으로 숨겨져 있습니다. 이벤트 보기에서 숨겨진 필드를 표시하려면 검색 제한 사항을 확장한 다음 **Disabled Columns(**비활성화된 열**)** 아래에서 필드 이름을 클릭합니다.

관련 항목

캡처된 파일 필드, 881 페이지
사전 정의 캡처 파일 워크플로, 682 페이지
이벤트 보기 구성, 210 페이지

캡처된 파일 필드

사전 정의된 캡처된 파일 워크플로의 마지막 페이지이며 맞춤형 워크플로에 추가할 수 있는 캡처된 파일의 테이블 보기에는 캡처된 파일 테이블의 각 필드에 대한 열이 포함됩니다.

이 테이블을 검색할 때는 검색하는 이벤트에서 사용할 수 있는 데이터에 따라 검색 결과가 달라짐에 유의하십시오. 사용 가능한 데이터에 따라 검색 제약 조건이 적용되지 않을 수도 있습니다. 예를 들어 동적 분석을 위해 제출된 적이 없는 파일에는 연결된 위협 점수가 없을 수 있습니다.

표 ***110:*** 캡처된 파일 필드

필드	설명
아카이브 검사 상태	아카이브 파일의 경우 아카이브 검사의 상태: • Pending(보류 중)은 시스템이 아카이브 파일 및 내용을 여전히 검사 중임을 나타냅니다. 파일이 시스템을 다시 통과하면 완전한 정보를 이용할 수 있게 됩니다. • Extracted(추출됨)는 시스템이 아카이브의 내용을 추출 및 검사할 수 있게 되었음을 나타냅니다. • 매우 드물지만 시스템이 추출을 처리할 수 없는 경우 Failed(실패함)가 발생할 수 있습니다. • Depth Exceeded(수준 초과)는 아카이브에 허용되는 최대 깊이를 초과하여 중첩된 아카이브 파일이 포함되어 있음을 나타냅니다. • Encrypted(암호화됨)는 아카이브 파일의 내용이 암호화되어 검사할 수 없음을 나타냅니다. • Not Inspectable(검사 불가능)은 시스템이 아카이브의 내용을 추출 및 검사할 수 없음을 나타냅니다. 이 상태의 세 가지 주요 원인은 정책 규칙 작업, 정책 구성 및 손상된 파일입니다. 아카이브 파일의 내용을 보려면 테이블에서 해당 행을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 표시한 다음 **View Archive Contents(**아카이브 내용 보기**)**를 선택합니다.
카테고리	파일 유형의 일반적인 범주(예: Office 문서, 아카이브, 멀티미디어, 실행 파일, PDF 파일, 인코딩, 그래픽 또는 시스템 파일 등)
탐지 이름	탐지된 악성코드의 이름.
속성	파일의 악성코드 대응 속성: • Malware(악성코드)는 AMP 클라우드가 파일을 악성코드로 분류했거나 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다. • Clean(정상)은 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. • Unknown(알 수 없음)은 시스템이 AMP 클라우드를 쿼리했지만 파일에 속성이 할당되지 않았음을 나타냅니다. 즉, AMP 클라우드에서 파일을 분류하지 않았습니다. • Custom Detection(사용자 지정 탐지)은 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다. • Unavailable(사용할 수 없음)은 시스템이 AMP 클라우드를 쿼리할 수 없음을 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 처리했고 Secure Firewall Management Center이 AMP 클라우드를 쿼리하지 않았음을 나타냅니다.
도메인	캡처된 파일이 탐지된 도메인입니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

필드	설명
동적 분석 상태	파일이 동적 분석을 위해 제출되었는지 여부를 나타내는 다음 값 중 하나 이상: • Analysis Complete(분석 완료) - 위협 점수 및 동적 분석 요약 보고서를 받은, 동적 분석을 위해 제출된 파일 • Capacity Handled(처리된 용량) - 현재 제출할 수 없어서 저장된 파일 • Capacity Handled (Network Issue)(처리된 용량(네트워크 문제)) - 네트워크 연결 문제로 인해 제출할 수 없어서 저장된 파일 • Capacity Handled (Rate Limit)(처리된 용량(속도 제한)) - 최대 제출 수에 도달했기 때문에 제출할 수 없어 저장된 파일 • Device Not Activated(디바이스가 활성화되지 않음) - 디바이스가 온프레미스 Secure Malware Analytics 어플라이언스에서 활성화되지 않아 제출되지 않은 파일 이 상태가 표시되면 지원팀에 문의하십시오. • Failure (Analysis Timeout)(실패(분석 시간 초과)) - AMP 클라우드가 아직 결과를 반환하지 않은 제출된 파일 • Failure (Cannot Run File)(실패(파일 실행 불가)) - AMP 클라우드가 테스트 환경에서 실행할 수 없는 제출된 파일 • Failure (Network Issue)(실패(네트워크 문제)) - 네트워크 연결 오류로 인해 제출되지 않은 파일 • Not Sent for Analysis(분석을 위해 제출되지 않음) - 제출되지 않은 파일 • Not Suspicious (Not Sent For Analysis)(의심스럽지 않음(분석을 위해 제출되지 않음)) - 악성코드가 아닌 것으로 사전 분류된 파일 • 이전에 분석됨 - 캐시된 위협 점수가 있는 파일로, 이전에 전송되었음을 나타냅니다. • 분석이 거부됨 - 정적 분석을 기반으로 하는 파일은 예를 들어 동적 요소가 포함되어 있지 않으므로 위험할 가능성이 낮습니다. • Sent for Analysis(분석을 위해 전송) - 악성코드로 사전 분류되고 동적 분석을 위해 대기열에 넣은 파일
동적분석상태변경됨	파일의 동적 분석 상태가 마지막으로 변경된 시간.
파일 이름	파일의 SHA-256 해시 값에 연결된, 가장 최근에 탐지된 파일 이름.
마지막 변경 날짜	이 파일에 연결된 정보가 마지막으로 업데이트된 시간.
마지막 전송	동적 분석을 위해 파일이 가장 최근에 클라우드에 제출된 시간.

필드	설명
로컬 악성코드 분석 상태	시스템이 파일에서 로컬 악성코드 분석을 수행했는지 여부를 나타내는 다음 값 중 하나: • Analysis Complete(분석 완료) - 시스템이 로컬 악성코드 분석을 사용하여 파일을 검사하고 사전 분류했습니다 • Analysis Failed(분석 실패) - 시스템이 로컬 악성코드 분석을 사용하여 파일 검사를 시도하고 실패했습니다 • Manual Request Submitted(수동 요청 제출됨) - 사용자가 로컬 악성코드 분석을 위해 파일을 제출했습니다 • Not Analyzed(분석되지 않음) - 시스템이 로컬 악성코드 분석을 사용하여 파일을 검사하지 않았습니다
SHA256	파일의 SHA-256 해시 값 및 가장 최근에 탐지된 파일 이벤트 및 파일 속성을 나타내는 네트워크 파일 경로 분석 아이콘. 네트워크 파일 경로 분석을 보려면 경로 분석 아이콘을 클릭합니다.
스토리지 상태	파일이 매니지드 디바이스에 저장되는지 여부를 나타냅니다. • 파일 저장됨 • 저장되지 않음(속성 보류 중)
위협 점수	이 파일과 가장 최근에 연결된 위협 점수. 동적 분석 요약 보고서를 보려면 위협 점수 아이콘을 클릭합니다.
유형	파일 형식(예: HTML 또는 MSEXE).

저장된 파일 다운로드

디바이스가 파일을 저장하면 Secure Firewall Management Center가 해당 디바이스와 통신할 수 있고 파일을 삭제하지 않은 한 사용자는 장기 스토리지 및 분석을 위해 파일을 로컬 호스트에 다운로드하고 수동으로 파일을 분석할 수 있습니다. 연결된 파일 이벤트, 악성코드 이벤트, 캡처된 파일 보기 또는 파일의 경로 분석에서 파일을 다운로드할 수 있습니다.

악성코드는 유해하므로 기본적으로 모든 파일 다운로드를 확인해야 합니다. 하지만 사용자 환경설정에서 확인을 비활성화할 수 있습니다.

Unknown(알 수 없음) 속성의 파일에는 악성코드가 포함되어 있을 수 있으므로 파일을 다운로드할 때 시스템은 먼저 해당 파일을 `.zip` 패키지에 아카이브합니다. `.zip` 파일 이름에는 파일 속성과 파일 형식 및 SHA-256 값(사용 가능한 경우)이 포함됩니다. 실수로 압축을 해제하지 못하도록 `.zip` 파일을 비밀번호로 보호할 수 있습니다. 사용자 환경설정에서 기본 `.zip` 파일 비밀번호를 수정하거나 제거할 수 있습니다.

주의 Cisco에서는 악성코드를 다운로드하지 않을 것을 적극 권장합니다. 유해한 결과를 초래할 수 있습니다. 파일을 다운로드할 때는 주의하십시오. 악성코드가 포함되었을 수 있습니다. 파일을 다운로드하기 전에 다운로드 대상을 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.

분석을 위해 수동으로 파일 제출

분석을 위해 파일을 수동으로 제출하면 시스템은 로컬 분석을 실행한 다음 동적 분석을 위해 클라우드에 이 파일을 제출합니다. 하지만 파일 정책에서 로컬 분석이 활성화되어 있지 않고 분석을 위해 수동으로 파일을 제출하는 경우, 파일은 동적 분석을 위해서만 전송됩니다.

실행 파일 외에 .swf, .jar 등과 같이 자동 제출에 적합하지 않은 파일 형식도 제출할 수 있습니다. 이렇게 하면 속성에 상관없이 광범위한 파일을 더욱 신속히 분석하고 인시던트의 정확한 원인을 파악할 수 있습니다.

참고 시스템은 AMP 클라우드에서 동적 분석 대상 파일 형식 목록(하루에 한 번)과 제출 가능한 최소 및 최대 파일 크기 업데이트를 확인합니다.

상황에 따라 분석을 위해 두 가지 방법으로 파일을 제출할 수 있습니다.

시작하기 전에

분석을 위해 캡처된 파일을 수동으로 제출하려면, 하나 이상의 파일 규칙을 파일을 저장하도록 구성해야 합니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 네트워크 악성코드 보호 및 파일 정책 장을 참고하십시오.

프로시저

단계 **1** 분석을 위해 단일 파일을 제출하려면:

a) 다음 중 하나를 선택합니다.

- **Analysis(**분석**) > Files(**파일**) > File Events(**파일 이벤트**)**
- **Analysis(**분석**) > Files(**파일**) > Malware Events(**악성코드 이벤트**)**
- **Analysis(**분석**) > Files(**파일**) > Captured Files(**캡처된 파일**)**

b) <이벤트 유형 또는 파일>의 테이블 보기를 클릭합니다.

c) 테이블에서 파일을 마우스 오른쪽 버튼으로 클릭하고 **Analyze File(**파일 분석**)**을 선택합니다.

단계 **2** 캡처된 여러 파일을 제출하려면(한 번에 최대 25개):

a) **Analysis(**분석**) > Files(**파일**) > Captured Files(**캡처된 파일**)**를 선택합니다.

b) 분석할 각 파일 옆의 확인란을 선택합니다.

c) **Analyze(**분석**)**를 클릭합니다.

네트워크 파일 전파 흔적 분석

네트워크 파일 경로 분석 기능은 호스트가 네트워크에서 악성코드 파일을 포함한 파일을 전송한 방법을 매핑합니다. 경로 분석은 파일 전송 데이터, 파일의 속성, 파일 전송의 차단 여부 또는 파일의 격리 여부를 차트로 표시합니다. 어떤 호스트와 사용자가 악성코드를 전송했는지, 어떤 호스트가 위험한지를 확인하고 파일 전송 추세를 관찰할 수 있습니다.

AMP 클라우드가 속성을 할당한 모든 파일의 전송을 추적할 수 있습니다. 시스템은 악성코드 대응 및 AMP for Endpoints의 악성코드 탐지 및 차단 관련 정보를 사용하여 경로 분석을 작성할 수 있습니다.

최근 탐지된 악성코드 및 분석된 경로 분석

Network File Trajectory List(네트워크 파일 경로 분석 목록) 페이지에는 네트워크에서 가장 최근에 탐지된 악성코드는 물론 가장 최근에 경로 분석 맵을 살펴본 파일도 표시됩니다. 네트워크에서 각 파일을 가장 최근에 본 시간, 파일의 SHA-256 해시 값, 이름, 형식, 현재 파일 속성, 내용(아카이브 파일의 경우), 파일에 연결된 이벤트 수를 이러한 목록에서 확인할 수 있습니다.

이 페이지에는 SHA-256 해시 값이나 파일 이름을 기반으로, 또는 파일을 전송하거나 수신한 호스트의 IP 주소별로 파일을 찾을 수 있는 검색 상자도 포함되어 있습니다. 파일을 찾은 후 **File SHA256** 값을 클릭하여 자세한 경로 분석 맵을 볼 수 있습니다.

네트워크 파일 경로 분석 상세정보 보기

자세한 네트워크 파일 경로 분석을 살펴봄으로써 네트워크를 통해 파일을 추적할 수 있습니다. 파일의 세부 정보를 보려면 파일의 SHA 256 값을 검색하거나 Network File Trajectory(네트워크 파일 경로 분석) 목록에서 **File SHA 256** 링크를 클릭합니다.

네트워크 파일 경로 분석 세부 정보 페이지는 세 부분으로 구성됩니다.

- Summary Information(요약 정보) - 파일의 경로 분석 페이지에는 파일 식별 정보, 파일을 처음 본 시간과 네트워크에서 가장 최근에 본 시간, 파일을 본 사용자, 파일에 연결된 관련 이벤트 및 호스트 수, 파일의 현재 속성을 비롯하여 파일에 대한 요약 정보가 표시됩니다. 매니지드 디바이스가 파일을 저장한 경우, 이 섹션에서 로컬로 파일을 다운로드하거나 동적 분석을 위해 파일을 제출하거나 파일 목록에 파일을 추가할 수 있습니다.
- Trajectory Map(경로 분석 맵) - 파일의 경로 분석 맵은 네트워크에서 처음 탐지될 때부터 가장 최근까지 파일을 시각적으로 추적합니다. 맵에는 호스트가 파일을 전송하거나 수신한 시간, 파일 전송 빈도, 파일이 차단되거나 격리된 시간이 표시됩니다. 데이터 포인트 사이의 세로 줄은 호스트 간 파일 전송을 나타냅니다. 데이터 포인트를 연결하는 가로 줄은 시간에 따른 호스트의 파일 활동을 보여줍니다.

또한 파일의 파일 이벤트가 발생한 빈도와 시스템이 속성 또는 회귀적 속성을 할당한 시간도 표시됩니다. 맵에서 데이터 포인트를 선택하고 호스트가 해당 파일을 처음 전송한 인스턴스로 역추적하는 경로를 강조 표시할 수 있습니다. 이 경로는 또한 파일의 전송자 또는 수신자로서 호스트와 관련된 모든 시점과 교차하며, 관련된 사용자를 식별합니다.

- Related Events(관련 이벤트) - Events(이벤트) 테이블에는 맵의 각 데이터 포인트에 대한 이벤트 정보가 나열됩니다. 테이블과 맵을 사용하면 특정 파일 이벤트, 이 파일을 전송하거나 수신한 네트워크의 호스트와 사용자, 맵의 관련 이벤트, 선택한 값으로 제한된 테이블의 기타 관련 이벤트를 정확히 파악할 수 있습니다.

네트워크 파일 경로 분석 요약 정보

Network File Trajectory(네트워크 파일 경로 분석) 목록에 표시되는 파일의 세부 정보 페이지 상단에는 다음 요약 정보가 표시됩니다.

팁 관련 파일 이벤트를 보려면 필드 값 링크를 클릭하십시오. File Events(파일 이벤트) 기본 워크플로의 첫 번째 페이지가 새 창에서 열리고, 선택한 값도 포함된 모든 파일 이벤트가 표시됩니다.

표 ***111: Network File Trajectory Summary Information(***네트워크 파일 경로 분석 요약 정보***)*** 필드

이름	설명
아카이브 콘텐츠	검사된 아카이브 파일의 경우, 아카이브에 포함된 파일 수입니다.
현재 폐기	다음 악성코드 대응 파일 속성 중 하나: • `Malware(악성코드)`는 AMP 클라우드가 파일을 악성코드로 분류했거나 로컬 악성코드 분석에서 악성코드로 식별했거나 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다. • `Clean(정상)`은 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. • `Unknown(알 수 없음)`은 시스템이 AMP 클라우드를 쿼리했지만 파일에 속성이 할당되지 않았음을 나타냅니다. 즉, AMP 클라우드에서 파일을 분류하지 않았습니다. • `Custom Detection(사용자 지정 탐지)`은 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다. • `Unavailable(사용할 수 없음)`은 시스템이 AMP 클라우드를 쿼리할 수 없음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다. • `N/A`는 Detect Files(파일 탐지) 또는 Block Files(파일 차단) 규칙이 파일을 처리했고 Secure Firewall Management Center이 AMP 클라우드를 쿼리하지 않았음을 나타냅니다.
탐지 이름	로컬 악성코드 분석에서 탐지된 악성코드의 이름입니다.

이름	설명
이벤트 수	네트워크에 표시되는, 파일에 연결된 이벤트의 수, 그리고 탐지된 이벤트가 250개가 넘는 경우 맵에 표시되는 이벤트의 수.
파일 카테고리	파일 형식의 일반 카테고리(예: `Office 문서` 또는 `시스템 파일`).
파일 이름	네트워크에 표시되는, 이벤트와 연결된 파일의 이름. 여러 파일 이름이 하나의 SHA-256 해시 값에 연결되어 있으면 가장 최근에 탐지된 파일 이름이 나열됩니다. `more(더 보기)`를 클릭하여 이 항목을 확장하면 나머지 파일 이름을 볼 수 있습니다.
파일 SHA256	파일의 SHA-256 해시 값 해시는 기본적으로 압축된 형식으로 표시됩니다. 전체 해시 값을 보려면 포인터를 값 위로 이동합니다. 파일 이름 하나에 여러 SHA-256 해시 값이 연결되어 있는 경우 모든 해시 값을 보려면 포인터를 링크 위로 이동합니다.
파일 크기(KB)	킬로바이트 단위의 파일 크기.
파일 유형	파일의 파일 형식(예: `HTML` 또는 `MSEXE`).
처음 표시	악성코드 대응 또는 AMP for Endpoints가 처음으로 파일을 탐지한 시간, 파일을 처음 업로드한 호스트의 IP 주소 및 관련 사용자의 식별 정보.
최종 확인	악성코드 대응 또는 AMP for Endpoints가 가장 최근에 파일을 탐지한 시간, 파일을 마지막으로 다운로드한 호스트의 IP 주소 및 관련 사용자의 식별 정보.
상위 애플리케이션	AMP for Endpoints의 탐지가 발생했을 때 악성코드 파일에 액세스한 클라이언트 애플리케이션. 이러한 애플리케이션은 네트워크 검색 또는 애플리케이션 제어에 연결되지 않습니다.
표시	파일을 전송했거나 수신한 호스트의 수. 한 호스트가 서로 다른 시간에 파일을 업로드 및 다운로드할 수 있으므로 총 호스트 수는 `Seen On Breakdown` 필드에 지정된 총 전송자 수와 총 수신자 수의 합과 일치하지 않을 수 있습니다.
상세 분석에 표시	파일을 보낸 호스트의 수와 파일을 받은 호스트의 수.
위협 이름	AMP for Endpoints가 탐지한 악성코드에 연결된 위협의 이름.
위협 점수	파일의 위협 점수.

네트워크 파일 경로 분석 맵 및 관련 이벤트 목록

파일 궤적 맵의 y 축은 파일과 상호 작용 한 모든 호스트 IP 주소의 목록을 포함 합니다. IP 주소는 시스템이 해당 호스트에서 파일을 처음 탐지한 시점을 기준으로 내림차순으로 나열됩니다. 각 행에는 단일 파일 이벤트, 파일 전송 또는 회귀적 이벤트 등 해당 IP 주소에 연결된 모든 이벤트가 포함됩니다. x축에는 시스템이 각 이벤트를 탐지한 날짜와 시간이 포함됩니다. 타임스탬프는 시간순으로 나열됩니다. 1분 내에 여러 이벤트가 발생한 경우 모두가 동일한 열에 나열됩니다. 맵을 가로와 세로로 스크롤하면 추가 이벤트 및 IP 주소를 볼 수 있습니다.

맵에는 파일 SHA-256 해시에 연결된 최대 250개의 이벤트가 표시됩니다. 이벤트가 250개가 넘으면 처음 10개가 표시되고 추가 이벤트는 **Arrow(**화살표**)**와 함께 생략됩니다. 그런 다음 나머지 이벤트 240개가 표시됩니다.

File Events(파일 이벤트) 기본 워크플로의 첫 번째 페이지는 파일 형식을 기반으로 제한된 모든 추가 이벤트와 함께 새 창에 나타납니다. AMP for Endpoints에 의해 생성된 악성코드 이벤트가 표시되지 않으면 Malware Events(악성코드 이벤트) 테이블로 전환하여 이러한 이벤트를 표시해야 합니다.

각 데이터 포인트는 맵 아래의 범례에 설명된 대로 이벤트 및 파일 속성을 나타냅니다. 예를 들어 Malware Block 이벤트 아이콘은 Malicious Disposition 아이콘과 Block Event 아이콘을 결합합니다.

AMP for Endpoints에 의해 생성된 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")에는 하나의 아이콘이 포함됩니다. 회귀적이벤트는 파일이 탐지되는 각 호스트에 대한 열에 아이콘을 표시합니다. 파일 전송 이벤트에는 항상 두 개의 아이콘, 즉 파일 보내기 아이콘과 파일 받기 아이콘이 포함되며, 이 둘은 세로 선으로 연결됩니다. 화살표는 전송자에서 수신자로의 파일 전송 방향을 나타냅니다.

네트워크에서 파일의 진행 상황을 추적하려면 원하는 데이터 포인트를 클릭하여 선택한 데이터 포인트와 관련된 모든 데이터 포인트를 포함하는 경로를 강조 표시할 수 있습니다. 여기에는 다음 이벤트 유형에 연결된 데이터 포인트가 포함됩니다.

- 연결된 IP 주소 가 전송자 또는 수신자인 파일 전송
- 연결된 IP 주소와 관련하여 AMP for Endpoints가 생성한 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")
- 또 다른 IP 주소가 관련된 경우, 연결된 해당 IP 주소가 전송자 또는 수신자인 모든 파일 전송
- 다른 IP 주소가 관련된 경우, 다른 IP 주소와 관련하여 AMP for Endpoints가 생성한 안성코드 이벤트("엔드포인트 기반 악성코드 이벤트")

강조 표시된 데이터 포인트와 연결된 모든 IP 주소 및 타임스탬프도 강조 표시됩니다. Events(이벤트) 테이블의 해당 이벤트도 강조 표시됩니다. 경로에 생략된 이벤트가 포함된 경우 경로 자체는 점선으로 강조 표시됩니다. 생략된 이벤트는 경로와 교차할 수도 있지만 맵에는 표시되지 않습니다.

네트워크 파일 경로 분석 사용

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

팁 조직이 Secure Endpoint를 구축한 경우, 해당 제품에도 네트워크 파일 경로 분석 기능이 있습니다. management center에서 Secure Endpoint으로 피벗하려면 Secure Endpoint 콘솔의 이벤트 데이터 작업, 891 페이지의 내용을 참고하십시오. Secure Endpoint의 파일 경로 분석 기능에 대한 자세한 내용은 Secure Endpoint 설명서를 참고하십시오.

시작하기 전에

악성코드 대응 를 사용하는 경우 악성코드 방어 라이선스가 필요합니다.

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Files(**파일**)** > **Network File Trajectory(**네트워크 파일 경로**)**을(를) 선택합니다.

팁 Context Explorer, 대시보드 또는 파일 정보가 포함된 이벤트 보기에서도 파일의 분석 경로에 액세스할 수 있습니다.

단계 **2** 목록에서 **File SHA 256** 링크를 클릭합니다.

단계 **3** 원하는 경우, 전체 SHA-256 해시 값, 호스트 IP 주소 또는 추적할 파일의 파일 이름을 검색 필드에 입력하고 Enter 키를 누릅니다.

팁 일치하는 결과가 하나뿐이면 해당 파일의 Network File Trajectory(네트워크 파일 분석 경로) 페이지가 나타납니다.

단계 **4** Summary Information(요약 정보) 섹션에서 다음을 수행할 수 있습니다.

- 파일을 파일 목록에 추가 - 정상 목록 또는 맞춤형 탐지 목록에 파일을 추가 또는 제거하려면 **Edit(**수정**)** ( )을 클릭합니다.
- 파일 다운로드 - 파일을 다운로드하려면 **Download(**다운로드**)** ( )을 클릭하고 메시지가 표시되면 파일을 다운로드하려 한다고 확인합니다. 파일을 다운로드할 수 없는 경우에는 이 다운로드 파일이 흐리게 표시됩니다.
- 보고 - 동적 분석 요약 보고서를 보려면 위협 점수를 클릭합니다.
- 동적 분석을 위해 제출 - 동적 분석을 위해 파일을 제출하려면 **AMP** 클라우드를 클릭합니다. 파일을 제출할 수 없거나 AMP 클라우드에 연결할 수 없는 경우 이 AMP 클라우드가 흐리게 표시됩니다.
- 아카이브 내용 보기 - 아카이브 파일의 내용에 대한 정보를 보려면 **View(**보기**)** ( )을 클릭합니다.
- 파일 구성 보기 - 파일의 구성을 보려면 파일 목록을 클릭합니다. 시스템이 파일 구성 보고서를 생성하지 않은 경우, 이 파일 목록이 흐리게 표시됩니다.
- 위협 점수가 동일한 캡처된 파일 보기 - 해당 위협 점수의 모든 캡처 파일을 보려면 위협 점수 링크를 클릭합니다.

참고 Cisco에서는 악성코드를 다운로드하지 않을 것을 적극 권장합니다. 유해한 결과를 초래할 수 있습니다. 파일을 다운로드할 때는 주의하십시오. 악성코드가 포함되었을 수 있습니다. 파일을 다운로드하기 전에 다운로드 대상을 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.

단계 **5** 경로 분석 맵에서 다음을 수행할 수 있습니다.

- 첫 번째 인스턴스 찾기 - IP 주소와 관련하여 파일 이벤트가 처음 발생한 때를 찾으려면 IP 주소를 클릭합니다. 그러면 해당 데이터 포인트 경로는 물론 첫 번째 파일 이벤트와 관련된 중간 파

일 이벤트 및 IP 주소도 강조 표시됩니다. Events(이벤트) 테이블의 해당 이벤트도 강조 표시됩니다. 해당 데이터 포인트가 현재 보이지 않는 경우, 맵이 해당 데이터 포인트로 스크롤됩니다.

- 추적 - 데이터 포인트를 클릭하여 선택한 데이터 포인트와 관련된 모든 데이터 포인트를 포함하는 경로를 강조 표시하여 네트워크에서 파일의 진행 상황을 추적할 수 있습니다.
- 숨겨진 이벤트 보기 - File Summary(파일 요약) 이벤트 보기에 표시되지 않은 모든 이벤트를 보려면 화살표를 클릭합니다.
- 일치하는 파일 이벤트 보기 - 일치하는 파일 이벤트 위에 마우스 포인터를 올려놓으면 해당 이벤트의 요약 정보를 볼 수 있습니다. 이벤트 요약 정보 링크를 클릭할 경우, File Events(파일 이벤트) 기본 워크플로의 첫 번째 페이지가 파일 형식을 기반으로 제한된 모든 추가 이벤트와 함께 새 창에 나타납니다. File Summary(파일 요약) 이벤트 보기가 새 창에서 열리며, 클릭한 기준에 일치하는 모든 파일 이벤트가 표시됩니다.

단계 **6** Events(이벤트) 테이블에서 다음을 수행할 수 있습니다.

- 강조 표시 - 맵에서 데이터 포인트를 강조 표시하려면 테이블 행을 선택합니다. 선택한 파일 이벤트가 현재 보이지 않는 경우 해당 이벤트를 표시하도록 맵이 스크롤됩니다.
- 정렬 - 오름차순 또는 내림차순으로 이벤트를 정렬하려면 열 머리글을 클릭합니다.

Secure Endpoint 콘솔의 이벤트 데이터 작업

조직이 Secure Endpoint를 구축한 경우, Secure Endpoint 콘솔에서 악성코드 이벤트 데이터를 볼 수 있으며, 해당 애플리케이션의 전역 네트워크 파일 분석 경로 도구를 사용하거나.

팁 Secure Endpoint 및 콘솔 사용 방법은 콘솔의 온라인 도움말 또는 https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html에서 사용 가능한 기타 설명서를 참조하십시오.

Secure Firewall Management Center에서 Secure Endpoint 콘솔에 액세스하려면 다음 중 하나를 수행하십시오.

시작하기 전에

- Secure Endpoint에 대한 연결이 구성되어야 하며(Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *Firepower* 및 *Secure Endpoint* 통합 참조) Secure Firewall Management Center가 AMP 클라우드에 연결할 수 있어야 합니다.
- Secure Endpoint 자격 증명이 필요합니다.
- 이 작업을 수행하려면 관리자 사용자여야 합니다.

- management center의 악성코드 이벤트에서 피벗하려는 경우, Secure Endpoint 상황별 크로스 실행 옵션이 적절히 활성화되어 있어야 합니다. 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지의 항목을 참조하십시오.

프로시저

단계 **1** 방법 1:

a) **Integration(통합)** > **AMP** > **AMP Management(AMP 관리)**을(를) 선택합니다.
b) 테이블에서 클라우드 이름을 클릭합니다.

단계 **2** 방법 2:

a) **Analysis(분석)** > **Files(파일)**아래 테이블에서 악성코드 이벤트로 이동합니다.
b) 파일 SHA를 마우스 오른쪽 버튼으로 클릭하고 Secure Endpoint 옵션을 선택합니다.

파일, 악성코드 이벤트 및 네트워크 파일 경로 분석 기록

기능	버전	세부정보
동적 분석을 위해 파일 사전 분류가 개선되었습니다.	6.7	추가 평가를 통해 동적 분석을 위해 불필요한 파일 전송이 방지됩니다. 이 평가를 기반으로 클라우드로 전송되지 않은 파일에 대한 새로운 동적 분석이 **Rejected for Analysis(분석을 위해 거부)** 상태가 됩니다. 신규/수정된 화면: **Analysis(분석)** > **Captured Files(캡처된 파일)** > **Table View of Captured Files(캡처된 파일 테이블 보기)**
시스템 로그의 연결 이벤트 통합 식별자.	6.4.0.4	다음 시스템 로그 필드는 연결 이벤트를 전체적으로 고유하게 식별하며, 파일 및 악성코드 이벤트(DeviceUUID, 첫 번째 패킷 시간, 연결 인스턴스 ID, 연결 카운터)의 경우에는 시스템 로그에 표시됩니다.
시스템 로그를 통해 파일 및 악성코드 이벤트를 전송합니다.	6.4	이 장의 필드 설명은 시스템 로그 메시지에 포함된 필드를 지정합니다. 구성 정보는 파일 및 악성코드 이벤트에 대한 시스템 로그 구성 위치, 664 페이지의 내용을 참조하십시오.

35 장

호스트 프로파일

다음 주제에서는 호스트 프로파일을 사용하는 방법에 설명합니다.

호스트 프로파일에 대한 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

- 보안 분석가

호스트 프로파일

호스트 프로파일은 시스템이 단일 호스트에 대해 수집한 모든 정보를 완벽하게 보여줍니다. 호스트 프로파일을 액세스하려면

- 아무 네트워크 맵 보기에서 해당 프로파일로 이동합니다.
- 모니터링되는 네트워크 상의 호스트 IP 주소를 포함하는 아무 이벤트 보기에서 해당 프로파일로 이동합니다.

호스트 프로파일은 탐지한 호스트 또는 디바이스에 대한 (호스트 이름 또는 MAC 주소 같은) 기본 정보를 제공합니다. 라이선스 및 시스템 설정에 따라, 호스트 프로파일은 다음 정보를 제공하기도 합니다.

- 호스트에서 실행 중인 운영체제
- 호스트에서 실행 중인 서버
- 호스트에서 실행 중인 클라이언트 및 웹 애플리케이션
- 호스트에서 실행 중인 프로토콜
- 호스트의 보안 침해 지표(IOC) 태그
- 호스트의 VLAN 태그
- 네트워크에서의 최근 24시간 동안의 사용자 활동
- 호스트와 관련된 규정준수 허용리스트 위반
- 호스트에 대한 가장 최근의 악성코드 이벤트
- 호스트와 관련된 취약성
- 호스트에 대한 Nmap 스캔 결과

호스트 속성은 프로파일에도 나열됩니다. 호스트 속성을 사용하면 네트워크 환경에서 중요한 방법으로 호스트를 분류할 수 있습니다. 예를 들어, 다음이 가능합니다.

- 호스트가 위치한 건물을 나타내는 호스트 속성을 할당합니다.
- 호스트 중요도 특성을 사용하여 특정 호스트의 비즈니스 중요도를 할당하고 호스트 중요도를 기반으로 상관관계 정책 및 알림을 맞춤화합니다.

호스트 프로파일에서 해당 호스트에 적용된 기존 호스트 속성을 보고 호스트 속성 값을 수정합니다.

적응형 프로파일 업데이트을(를) 수동 침입 방지 배포의 일부로 사용하는 경우, 시스템이 트래픽을 수정하는 방식을 호스트와 서버 및 호스트를 실행하는 클라이언트의 운영체제에 가장 적합하게 조정할 수 있습니다.

선택적으로, 호스트 프로파일에서 Nmap 스캔을 수행하여 호스트 프로파일의 서버 및 운영체제 정보를 보강할 수도 있습니다. Nmap 스캐너는 호스트를 적극적으로 조사하여 호스트에서 실행 중인 운영체제와 서버에 대한 정보를 가져옵니다. 스캔 결과는 호스트에 대한 운영체제 및 서버 ID의 목록에 추가됩니다.

관련 항목

호스트 프로파일 보기, 895 페이지

호스트 프로파일 제한

사용할 수 없는 호스트

네트워크의 모든 호스트에 대해 호스트 프로파일을 이용할 수 있는 것은 아닙니다. 대표적인 가능한 원인:

- 시간 초과되어 호스트가 네트워크 맵에서 삭제됨
- 호스트 제한에 도달함
- 호스트가 네트워크 검색 정책에서 모니터링하지 않는 네트워크 세그먼트에 상주함

사용할 수 없는 정보

호스트 프로파일에 표시되는 정보는 호스트 유형 및 호스트에 대해 사용 가능한 정보에 따라 달라질 수 있습니다.

예를 들면 다음과 같습니다.

- 시스템에서 비 IP 기반 프로토콜(예: STP, SNAP, IPX)을 탐지한 경우, 호스트는 네트워크 맵에 MAC 호스트로 추가되는데 이 경우 IP 호스트에 비해 사용 가능한 정보가 훨씬 적습니다.
- 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

(VRF를 실행하는 구축**)** 단일 **IP** 주소가 여러 호스트를 나타낼 수 있습니다**.**

VRF를 실행하는 디바이스에서 호스트를 보고했다면, 단일 IP 주소가 실제로는 여러 호스트를 나타낼 수 있습니다. VRF는 중복 IP 주소가 있는 여러 네트워크를 모니터링할 수 있으므로, 동일한 IP 주소가 서로 다른 네트워크에 존재할 수 있습니다.

호스트 프로파일 보기

프로시저

다음 2가지 옵션을 사용할 수 있습니다.

- 네트워크 맵에서 프로파일을 보려는 호스트의 IP 주소로 드릴다운합니다.

- 이벤트 보기에서 프로필을 보려는 호스트의 IP 주소 옆에 있는 **Host Profile(**호스트 프로파일**)** 또는 **Compromised Host(**손상된 호스트**)**를 클릭합니다.

호스트 프로파일의 기본 호스트 정보

각 호스트 프로파일은 탐지된 호스트 또는 기타 디바이스에 대한 기본 정보를 제공합니다.

다음은 각각의 기본 호스트 프로파일 필드에 대한 설명입니다.

도메인

호스트와 연결된 도메인.

IP 주소

호스트와 연결된 모든 IP 주소(IPv4 및 IPv6). 시스템은 호스트와 연결된 IP 주소를 탐지하며, 지원되는 경우 동일한 호스트에 의해 사용되는 여러 IP 주소를 그룹화합니다. IPv6 호스트에는 흔히 2개 이상의 IPv6 주소(로컬 전용 및 전역 라우팅 가능)가 있으며 IPv4 주소도 있을 수 있습니다. IPv4 전용 호스트에는 여러 개의 IPv4 주소가 있을 수 있습니다.

호스트 프로파일에는 해당 호스트와 연결된 모든 탐지된 IP 주소가 나열됩니다. 사용 가능한 경우, 라우팅 가능한 호스트 IP 주소에는 해당 주소에 연결된 지오로케이션 데이터를 나타내는 국가 코드 및 플래그 아이콘도 포함될 수 있습니다.

기본적으로 처음 3개 주소만 표시됩니다. 호스트의 모든 주소를 표시하려면 **show all(**모두 표시**)**을 클릭하십시오.

호스트 이름

알려진 경우 호스트의 정규화된 도메인 이름.

NetBIOS 이름

사용 가능한 경우 호스트의 NetBIOS 이름. Microsoft Windows 호스트는 물론 Macintosh, Linux 또는 NetBIOS를 사용하도록 구성된 기타 플랫폼은 NetBIOS 이름을 가질 수 있습니다. 예를 들어 Samba 서버로 구성된 Linux 호스트는 NetBIOS 이름을 가질 수 있습니다.

디바이스**(**홉**)**

다음 중 하나에 해당합니다.

- 네트워크 검색 정책에 정의된 대로 호스트가 상주하는 네트워크에 대한 보고 디바이스 또는
- 호스트를 네트워크 맵에 추가한 NetFlow 데이터를 처리한 디바이스

디바이스 이름 뒤에 호스트를 탐지한 디바이스와 호스트 자체 간 네트워크 홉의 수가 괄호로 표시됩니다. 여러 디바이스가 호스트를 볼 수 있는 경우 보고 디바이스는 굵은 글꼴로 표시됩니다.

이 필드가 비어 있는 경우는 다음 중 하나입니다.

- 네트워크 검색 정책에 정의된 대로, 호스트 상주 네트워크를 명시적으로 모니터링하지 않는 디바이스에 의해 호스트가 네트워크 맵에 추가되었습니다.
- 호스트가 호스트 입력 기능으로 추가되었으며 시스템에 의해 탐지되지 않았습니다.

MAC 주소(TTL)

호스트의 탐지된 MAC 주소 및 관련 NIC 공급업체, NIC의 하드웨어 공급업체와 현재 TTL(time-to-live) 값은 괄호로 표시됩니다.

여러 디바이스가 호스트를 탐지한 경우, 이를 보고한 디바이스와 상관없이 management center에서는 호스트에 연결된 모든 MAC 주소 및 TTL 값을 표시합니다.

MAC 주소가 굵은 글꼴로 표시된 경우, MAC 주소는 호스트의 실제/참/기본 MAC 주소이며, ARP 및 DHCP 트래픽을 통한 탐지에 의해 IP 주소에 확실히 연결됩니다.

굵은 글꼴로 표시되지 않은 MAC 주소는 호스트의 IP 주소에 확실히 연결될 수 없는 보조 주소입니다. 예를 들어 Firepower 디바이스는 자신의 네트워크 세그먼트에 있는 호스트의 MAC 주소만 획득할 수 있으므로 Firepower 디바이스가 직접 연결되지 않은 네트워크 세그먼트에서 트래픽이 시작되는 경우, 관찰된 MAC 주소(즉, 라우터 MAC 주소)는 호스트의 보조 MAC 주소로 표시됩니다.

호스트 유형

호스트, 모바일 디바이스, 탈옥 모바일 디바이스, 라우터, 브리지, NAT 디바이스 또는 로드 밸런서 등 시스템이 탐지한 디바이스의 유형.

시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.
- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.
- 시스템이 모바일 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.
- 모바일 디바이스의 모바일 브라우저에서 HTTP 트래픽의 User-Agent(사용자 에이전트) 문자열 분석
- 특정 모바일 애플리케이션의 HTTP 트래픽 모니터링

네트워크 디바이스 또는 모바일 디바이스로 식별되지 않는 디바이스는 호스트로 분류됩니다.

최종 확인

호스트의 IP 주소가 마지막으로 탐지된 날짜 및 시간.

Current User(현재 사용자**)**

가장 최근에 이 호스트에 로그인한 사용자.

기존의 현재 사용자가 권한 있는 사용자가 아닌 경우, 호스트에 로그인한 권한 없는 사용자는 호스트에서 현재 사용자로만 등록됩니다.

보기

연결, 검색, 악성코드 및 침입 이벤트 데이터의 보기에 대한 링크. 해당 이벤트 유형에 대해 기본 워크플로를 사용하며 호스트와 관련된 이벤트를 표시하도록 제한됩니다. 가능한 경우 이러한 이벤트에는 호스트와 연결된 모든 IP 주소가 포함됩니다.

호스트 프로파일의 운영 체제

시스템은 호스트에 의해 생성되는 트래픽에서 네트워크 및 애플리케이션 스택을 분석하거나 사용자 에이전트에 의해 보고된 호스트 데이터를 분석하여 호스트에서 실행되는 운영 체제의 ID를 수동적으로 탐지합니다. 시스템은 또한 Nmap 스캐너 또는 호스트 입력 기능을 통해 가져온 애플리케이션 데이터 등의 다른 소스에서 운영 체제 정보를 취합합니다. 사용할 ID를 결정할 때 시스템은 각 ID 소스에 할당된 우선순위를 고려합니다. 기본적으로 사용자 입력의 우선순위가 가장 높고, 그다음은 애플리케이션 또는 스캐너 소스, 그다음은 검색된 ID입니다.

트래픽 및 기타 ID 소스는 더 구체적인 ID에 대해 충분한 정보를 제공하지 않으므로 때때로 시스템은 특정한 운영 체제보다는 일반적인 운영 체제 정의를 제공합니다. 시스템은 가능한 한 가장 자세한 정의를 사용하기 위해 여러 소스의 정보를 취합합니다.

운영 체제는 호스트의 취약성 목록과 호스트를 대상으로 하는 이벤트에 대한 이벤트 영향 상관 관계에 영향을 미치기 때문에 더 구체적인 운영 체제 정보를 수동으로 제공하는 것이 좋습니다. 또한 운영 체제에 수정(예: 서비스 팩 및 업데이트)이 적용되었음을 나타낼 수 있고, 수정에 의해 해결된 취약성을 무효화할 수 있습니다.

예를 들어 시스템에서 호스트의 운영 체제를 Microsoft Windows 2003으로 식별했지만 실제로 호스트에서는 Microsoft Windows XP Professional 서비스 팩 2가 실행되고 있음을 알고 있는 경우, 운영 체제 ID를 올바르게 설정할 수 있습니다. 운영 체제 ID를 더 구체적으로 설정하면 호스트의 취약성 목록이 세부적으로 조정되므로, 해당 호스트에 대한 영향 상관 관계가 더 구체적이고 정확해집니다.

시스템이 호스트의 운영 체제 정보를 탐지하고 그 정보가 활성 소스에 의해 제공된 현재 운영 체제 ID와 충돌하는 경우, ID 충돌이 발생합니다. ID 충돌이 발생하면 시스템에서는 취약성과 영향 상관 관계에 두 ID를 모두 사용합니다.

NetFlow 엑스포터가 모니터링하는 호스트의 네트워크 맵에 검색 데이터를 추가하도록 네트워크 검색 정책을 구성할 수 있습니다. 하지만 호스트 입력 기능을 사용하여 운영 체제 ID를 설정하지 않는 한 사용할 수 있는 이러한 호스트의 운영 체제 데이터는 없습니다.

활성화된 네트워크 검색 정책의 규정준수 허용리스트를 위반하는 운영체제가 호스트에서 실행되고 있는 경우, management center에서는 해당 운영체제 정보를 허용리스트 **Violation(**위반**)**으로 표시합니다. 또한 탈옥 모바일 디바이스가 활성 허용리스트를 위반하면 디바이스의 운영체제 옆에 아이콘이 나타납니다.

호스트의 운영 체제 ID에 대해 맞춤형 표시 문자열을 설정할 수 있습니다. 그러면 해당 표시 문자열이 호스트 프로파일에 사용됩니다.

참고 호스트의 운영체제 정보를 변경하면 규정준수 허용리스트 준수도 변경될 수 있습니다.

네트워크 디바이스의 호스트 프로파일에서 Operating Systems 섹션의 레이블이 Systems로 변경되며 추가 Hardware 열이 나타납니다. Systems 아래에 하드웨어 플랫폼에 대한 값이 나열되면 해당 시스템은 네트워크 디바이스 뒤에서 탐지된 하나 이상의 모바일 디바이스를 나타냅니다. 모바일 디바이스에는 하드웨어 플랫폼 정보가 있을 수도 있고 없을 수도 있지만, 모바일 디바이스가 아닌 시스템에 대해서는 하드웨어 플랫폼 정보가 탐지되지 않습니다.

다음은 호스트 프로파일에 표시되는 운영 체제 정보 필드에 대한 설명입니다.

Hardware(하드웨어)

모바일 디바이스용 하드웨어 플랫폼.

OS Vendor/Vendor

운영 체제의 공급업체입니다.

OS Product/Product

다음 값 중 하나:

- 모든 소스에서 수집한 ID 데이터에 기반할 때 호스트에서 실행되고 있을 가능성이 가장 높다고 판단되는 운영 체제
- 시스템이 아직 운영 체제를 식별하지 못했고 사용 가능한 다른 ID 데이터가 없는 경우 `Pending`
- 시스템이 운영 체제를 식별할 수 없고 운영 체제에 대해 사용 가능한 다른 ID 데이터가 없는 경우 `unknown`

참고 호스트의 운영 체제를 시스템이 탐지할 수 없는 경우 Cisco Secure Firewall Management Center 디바이스 구성 가이드호스트 *ID* 소스 장을 참고하십시오.

OS Version/Version

운영 체제 버전. 호스트가 탈옥 모바일 디바이스인 경우, 버전 뒤에 괄호로 `Jailbroken`이 표시됩니다.

소스

다음 값 중 하나:

- 사용자: user_name
- 애플리케이션: app_name

- 스캐너: scanner_type (Nmap 또는 기타 스캐너)
- Firepower

시스템에서는 운영 체제의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

운영 체제 ID 보기

호스트에 대해 추가되거나 검색된 특정 운영 체제 ID를 볼 수 있습니다. 시스템은 호스트에 대한 현재 ID를 확인하기 위해 소스 우선순위를 사용합니다. ID 목록에서 현재 ID는 굵은 글꼴로 강조 표시됩니다.

View(보기**)**는 호스트에 여러 운영체제 ID가 존재하는 경우에만 사용할 수 있습니다.

프로시저

단계 **1** 호스트 프로파일의 **Operating System(**운영 체제**)** 또는 **Operating System Conflicts(**운영 체제 충돌**)** 섹션에서 **View(**보기**)**를 클릭합니다.

단계 **2** 호스트 프로파일의 운영 체제, 898 페이지에 설명된 정보를 봅니다.

단계 **3** 원하는 경우, 운영체제 ID 옆에 있는 **Delete(**삭제**)** ( )를 클릭합니다.

참고 Cisco가 탐지한 운영 체제 ID는 삭제할 수 없습니다.

시스템은 Operating System Identity Information(운영 체제 ID 정보) 팝업 창에서 ID를 삭제하고, 해당되는 경우, 호스트 프로파일에서 운영 체제의 현재 ID를 업데이트합니다.

현재 운영 체제 ID 설정

Firepower System 웹 인터페이스를 사용하여 호스트의 현재 운영 체제 ID를 설정할 수 있습니다. 웹 인터페이스를 통해 ID를 설정하면 취약성 평가 및 영향 상관 관계에 ID가 사용될 수 있도록 다른 모든 ID 소스가 재정의됩니다. 그러나 사용자가 운영 체제를 수정한 후 시스템에서 호스트에 대해 충돌하는 운영 체제 ID를 탐지하면 운영 체제 충돌이 발생합니다. 이 경우 사용자가 충돌을 해결할 때까지 두 운영 체제 모두 현재 운영 체제로 간주됩니다.

프로시저

단계 **1** 호스트 프로파일의 **Operating System(**운영 체제**)** 섹션에서 **Edit(**수정**)**를 클릭합니다.

단계 **2** 다음과 같은 몇 가지 옵션이 있습니다.

- 호스트 입력을 통해 현재 운영 체제 ID를 확인하려면 **OS Definition(OS** 정의**)** 드롭다운 목록에서 **Current Definition(**현재 정의**)**을 선택하고 6단계로 건너뜁니다.
- **OS Definition(OS** 정의**)** 드롭다운 목록에서 현재 운영 체제 ID에 대한 변형을 선택하고 6단계로 건너뜁니다.

- **OS Definition(OS** 정의**)** 드롭다운 목록에서 **User-Defined(**사용자 정의**)**를 선택하고 3단계를 계속 진행합니다.

단계 **3** 원하는 경우, **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**, **Product String(**제품 문자열**)** 및 **Version String(**버전 문자열**)** 필드에 표시할 맞춤형 문자열을 수정합니다.

단계 **4** 원하는 경우, 다른 공급업체의 운영 체제로 변경하려면 **Product(**제품**)** 드롭다운 목록에서 **Vendor(**공급업체**)**를 선택합니다.

단계 **5** 원하는 경우, 운영 체제 제품 릴리스 수준을 구성하려면 **Major(**메이저**)**, **Minor(**마이너**)**, **Revision(**수정**)**, **Build(**빌드**)**, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록에서 선택합니다.

단계 **6** 원하는 경우, 운영 체제의 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭합니다.

단계 **7** 드롭다운 목록에서 해당 수정을 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **8** 원하는 경우, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록을 사용하여 관련 패치와 확장을 추가합니다.

단계 **9** **Finish(**종료**)**를 클릭합니다.

관련 항목

운영 체제 ID 충돌, 901 페이지

운영 체제 ID 충돌

현재 ID가 스캐너, 애플리케이션, 사용자 등의 활성 소스에 의해 제공된 경우, 시스템이 탐지한 새 ID가 현재 ID와 충돌하면 운영 체제 ID 충돌이 발생합니다.

충돌하는 운영 체제 ID 목록은 호스트 프로파일에서 굵은 글꼴로 표시됩니다.

시스템 웹 인터페이스를 통해 ID 충돌을 해결하고 호스트의 현재 운영 체제 ID를 설정할 수 있습니다. 웹 인터페이스를 통해 ID를 설정하면 취약성 평가 및 영향 상관 관계에 ID가 사용될 수 있도록 다른 모든 ID 소스가 재정의됩니다.

충돌하는 운영 체제 ID를 현재 ID로 만들기

프로시저

단계 **1** 호스트 프로파일의 **Operating System(**운영 체제**)** 섹션으로 이동합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 호스트의 운영 체제로 설정하려는 운영 체제 ID 옆에 있는 **Make Current(**현재 **ID**로 만들기**)**를 클릭합니다.
- 현재 ID로 지정하지 않으려는 ID가 활성 소스에서 온 것이면 원하지 않는 ID를 삭제합니다.

운영 체제 ID 충돌 해결

프로시저

단계 1 호스트 프로파일의 **Operating System(**운영 체제**)** 섹션에서 **Resolve(**해결**)**를 클릭합니다.

단계 2 다음 옵션을 이용할 수 있습니다.

- 호스트 입력을 통해 현재 운영 체제 ID를 확인하려면 **OS Definition(OS** 정의**)** 드롭다운 목록에서 **Current Definition(**현재 정의**)**을 선택하고 6단계로 건너뜁니다.
- **OS Definition(OS** 정의**)** 드롭다운 목록에서 충돌하는 운영 체제 ID 중 하나의 변형을 선택하고 6단계로 건너뜁니다.
- **OS Definition(OS** 정의**)** 드롭다운 목록에서 **User-Defined(**사용자 정의**)**를 선택하고 3단계를 계속 진행합니다.

단계 3 원하는 경우, **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**, **Product String(**제품 문자열**)** 및 **Version String(**버전 문자열**)** 필드에 표시할 맞춤형 문자열을 입력합니다.

단계 4 원하는 경우, 다른 공급업체의 운영 체제로 변경하려면 **Product(**제품**)** 드롭다운 목록에서 **Vendor(**공급업체**)**를 선택합니다.

단계 5 원하는 경우, 운영 체제 제품 릴리스 수준을 구성하려면 **Major(**메이저**)**, **Minor(**마이너**)**, **Revision(**수정**)**, **Build(**빌드**)**, **Patch(**패치**)** 및 **Extension(**확장**)** 드롭다운 목록에서 선택합니다.

단계 6 원하는 경우, 운영 체제의 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭합니다.

단계 7 적용한 수정을 수정 목록에 추가합니다.

단계 8 **Finish(**종료**)**를 클릭합니다.

호스트 프로파일의 서버

호스트 프로파일의 서버 섹션에는 모니터링되는 네트워크의 호스트에서 탐지되거나 내보낸 NetFlow 레코드에서 추가되거나 스캐너 또는 호스트 입력 기능 같은 활성 소스를 통해 추가된 서버가 나열됩니다.

목록은 호스트당 최대 100개의 서버를 포함할 수 있습니다. 이 제한에 도달하면 호스트에서 서버를 삭제하거나 서버가 시간 초과될 때까지 소스의 새 서버 정보(능동이든 수동이든)가 폐기됩니다.

Nmap을 사용하여 호스트를 스캔하면 Nmap은 열린 TCP 포트에서 실행되는, 전에 탐지되지 않은 서버의 결과를 Servers(서버) 목록에 추가합니다. Nmap 스캔을 수행하거나 Nmap 결과를 가져오는 경우, 호스트 프로파일에 Scan Results(스캔 결과) 섹션도 나타나며, 여기에 Nmap 스캔에 의해 호스트에서 탐지된 서버 정보가 나열됩니다. 또한 네트워크 맵에서 호스트가 삭제되면 호스트에 대한 해당 서버의 Nmap 스캔 결과가 삭제됩니다.

참고 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

호스트 프로파일의 서버 작업 프로세스는 프로파일에 액세스하는 방법에 따라 달라집니다.

- 네트워크 맵을 통해 드릴다운하여 호스트 프로파일에 액세스하는 경우, 굵은 글꼴로 강조 표시된 서버 이름과 함께 해당 서버에 대한 세부사항이 나타납니다. 호스트의 다른 서버에 대한 세부사항을 보려면 해당 서버 이름 옆에 있는 **View(**보기**)** ( )를 클릭합니다.
- 다른 방법으로 호스트 프로필에 액세스하는 경우, Servers(서버) 섹션을 확장하고 세부 사항을 보려는 서버 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

참고 활성화된 상관관계 정책의 규정준수 허용리스트를 위반하는 서버가 호스트에서 실행되고 있는 경우, management center에서는 규정을 준수하지 않는 서버를 허용리스트 **Violation(**위반**)**으로 표시합니다.

다음은 Servers(서버) 목록의 열에 대한 설명입니다.

프로토콜

서버가 사용하는 프로토콜의 이름.

Port(포트**)**

서버가 실행하는 포트.

애플리케이션 프로토콜

다음 중 하나에 해당합니다.

- 애플리케이션 프로토콜의 이름
- 여러 이유 중 하나 때문에 시스템이 애플리케이션 프로토콜을 긍정적으로 또는 부정적으로 식별할 수 없는 경우 `pending`
- 알려진 애플리케이션 프로토콜 지문을 기반으로 시스템이 애플리케이션 프로토콜을 식별할 수 없거나 서버 추가 없이 포트 정보와 함께 취약성을 추가하여 호스트 입력을 통해 해당 서버가 추가된 경우 `unknown`

마우스를 애플리케이션 프로토콜 이름 위로 이동하면 태그가 표시됩니다.

Vendor and Version

시스템, Nmap 또는 다른 활성 소스에 의해 식별되었거나 호스트 입력 기능을 통해 수집된 벤더 및 버전. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

호스트 프로파일의 서버 상세정보

management center는 서버당 최대 16개의 수동 탐지 ID를 나열합니다. 수동 탐지 소스에는 네트워크 검색 데이터 및 NetFlow 레코드가 포함됩니다. 시스템이 서버에 대해 여러 공급업체 또는 버전을 탐지하는 경우 해당 서버는 여러 수동 ID를 가질 수 있습니다. 예를 들어 웹 서버가 서버 소프트웨어와 동일한 버전을 실행하지 않는 경우, 매니지드 디바이스와 웹 서버 팜 간 로드 밸런서를 사용하면 시스템은 HTTP에 대해 여러 수동 ID를 식별하게 될 수 있습니다. management center는 사용자 입력, 스캐너 또는 기타 애플리케이션 등 활성 소스에서 오는 서버 ID의 수를 제한하지 않습니다.

현재 ID는 management center에서 굵은 글꼴로 표시됩니다. 시스템은 호스트에 취약성을 할당하고, 영향 평가를 수행하고, 호스트 프로파일 자격 및 규정준수 허용리스트에 대해 작성된 상관관계 규칙을 평가하는 등 여러 용도로 서버의 현재 ID를 사용합니다.

서버 세부사항에는 선택한 서버에 대해 알려진 업데이트된 하위 서버 정보도 표시될 수 있습니다.

서버 세부사항에는 서버 배너도 표시될 수 있습니다. 이 배너는 호스트 프로파일에서 서버를 볼 때 서버 세부사항 아래에 표시됩니다. 서버 배너는 서버 식별에 도움이 될 수 있는, 서버에 대한 추가 정보를 제공합니다. 공격자가 고의로 서버 배너 문자열을 변경하면 시스템이 서버를 식별하지 못하거나 잘못된 서버를 탐지할 수 있습니다. 서버 배너에는 서버에 대해 탐지된 첫 번째 패킷의 처음 256바이트가 표시됩니다. 이러한 정보는 시스템에서 서버를 처음 탐지할 때 한 번만 수집됩니다. 배너 내용은 왼쪽에는 16진수로, 오른쪽에는 ASCII로 표시되어 두 열에 나타납니다.

참고 서버 배너를 보려면 네트워크 검색 정책에서 **Capture Banners(**배너 캡처**)** 확인란을 활성화해야 합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

호스트 프로파일의 서버 세부정보 섹션에는 다음 정보가 포함됩니다.

프로토콜

서버가 사용하는 프로토콜의 이름.

Port(포트**)**

서버가 실행하는 포트.

Hits(히트**)**

매니지드 디바이스 또는 Nmap 스캐너에 의해 서버가 탐지된 횟수. 호스트 입력을 통해 가져온 서버에 대한 트래픽을 시스템에서 탐지하지 못하면 해당 서버의 히트 수는 0입니다.

Last Used(최종 사용**)**

서버가 마지막으로 탐지된 시간 및 날짜. 시스템이 서버에 대해 새 트래픽을 탐지하지 못하면 호스트 입력 데이터의 마지막 사용 시간은 초기 데이터 가져오기 시간을 반영합니다. 호스트 입력 기능을 통해 가져온 스캐너 및 애플리케이션 데이터는 management center 구성에 따라 시간 초과되지만 management center 웹 인터페이스를 통한 사용자 입력은 시간 초과되지 않습니다.

애플리케이션 프로토콜

알려진 경우, 서버에서 사용하는 애플리케이션 프로토콜의 이름.

Vendor(벤더**)**

서버 공급업체. 공급업체가 알려지지 않은 경우 이 필드는 나타나지 않습니다.

버전

서버 버전. 버전이 알려지지 않은 경우 이 필드는 나타나지 않습니다.

소스

다음 값 중 하나:

- 사용자: user_name
- 애플리케이션: app_name
- 스캐너: scanner_type (Nmap 또는 기타 스캐너)
- 시스템에서 탐지된 어플라이언스의 `Firepower`, `Firepower Port Match` 또는 `Firepower Pattern Match`
- NetFlow 레코드에서 네트워크 맵에 추가된 서버의 `NetFlow`

시스템에서는 서버의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

서버 상세정보 보기

프로시저

호스트 프로파일의 **Servers(**서버**)** 섹션 옆에 있는 **View(**보기**)** ( )을 클릭합니다.

서버 **ID** 수정

호스트의 서버에 대한 ID 설정을 수동으로 업데이트하고, 수정으로 해결된 취약성을 제거하도록 호스트에 적용한 수정을 구성할 수 있습니다. 서버 ID를 삭제할 수도 있습니다.

ID를 삭제해도 서버는 삭제되지 않습니다(유일한 ID를 삭제하는 경우에도). ID를 삭제하면 Server Detail(서버 세부정보) 팝업 창에서 ID가 제거되며, 해당되는 경우 호스트 프로파일에서 서버의 현재 ID가 업데이트됩니다.

Cisco가 관리하는 디바이스에 의해 추가된 서버 ID는 수정 또는 삭제할 수 없습니다.

프로시저

단계 **1** 호스트 프로파일의 **Servers(**서버**)** 섹션으로 이동합니다.

단계 **2** Server Details(서버 세부정보) 팝업 창을 열려면 **View(**보기**)**를 클릭합니다.

단계 **3** 서버 ID를 삭제하려면 제거할 서버 ID 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **4** 서버 ID를 수정하려면 서버 목록에서 서버 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **5** 다음 2가지 옵션을 사용할 수 있습니다.

- **Select Server Type(**서버 유형 선택**)** 드롭다운 목록에서 현재 정의를 선택합니다.
- **Select Server Type(**서버 유형 선택**)** 드롭다운 목록에서 서버 유형을 선택합니다.

단계 **6** 원하는 경우, 해당 서버 유형에 대한 공급업체와 제품만 나열하려면 **Restrict by Server Type(**서버 유형으로 제한**)** 확인란을 선택합니다.

단계 **7** 원하는 경우, 서버 이름과 버전을 맞춤 설정하려면 **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**과 **Version String(**버전 문자열**)**을 입력합니다.

단계 **8** **Product Mappings(**제품 매핑**)** 섹션에서 사용할 운영 체제, 제품 및 버전을 선택합니다.

예제**:**

예를 들어 서버를 Red Hat Linux 9에 매핑하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

단계 **9** 서버 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭하고 해당 서버에 적용하려는 패치를 수정 목록에 추가합니다.

단계 **10** **Finish(**종료**)**를 클릭합니다.

서버 **ID** 충돌 해결

애플리케이션이나 스캐너 같은 활성 소스가 서버의 ID 데이터를 호스트에 추가한 후 시스템이 해당 포트에서 서버 ID가 충돌함을 나타내는 트래픽을 탐지하면 서버 ID 충돌이 발생합니다.

프로시저

단계 **1** 호스트 프로파일에서 **Servers(**서버**)** 섹션으로 이동합니다.

단계 **2** 서버 옆에 있는 해결 아이콘을 클릭합니다.

단계 **3** **Select Server Type(**서버 유형 선택**)** 드롭다운 목록에서 서버 유형을 선택합니다.

단계 **4** 원하는 경우, 해당 서버 유형에 대한 공급업체와 제품만 나열하려면 **Restrict by Server Type(**서버 유형으로 제한**)** 확인란을 선택합니다.

단계 **5** 원하는 경우, 서버 이름과 버전을 맞춤 설정하려면 **Use Custom Display String(**맞춤형 표시 문자열 사용**)**을 선택하고 **Vendor String(**공급업체 문자열**)**과 **Version String(**버전 문자열**)**을 입력합니다.

단계 **6** **Product Mappings(**제품 매핑**)** 섹션에서 사용할 운영 체제, 제품 및 버전을 선택합니다.

예제**:**

예를 들어 서버를 Red Hat Linux 9에 매핑하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

단계 **7** 서버 수정이 적용되었음을 표시하려면 **Configure Fixes(**수정 구성**)**를 클릭하고 해당 서버에 적용하려는 패치를 수정 목록에 추가합니다.

단계 **8** **Finish(**종료**)**를 클릭합니다.

호스트 프로파일의 웹 애플리케이션

호스트 프로파일의 Web Application(웹 애플리케이션) 섹션에는 네트워크의 호스트에서 실행 중이라고 시스템이 식별하는 클라이언트 및 웹 애플리케이션이 표시됩니다. 시스템은 수동 탐지 소스와 능동 탐지 소스의 클라이언트 및 웹 애플리케이션 정보를 식별할 수 있지만 NetFlow 레코드에서 추가된 호스트에 대한 정보는 제한됩니다.

이 섹션의 세부 정보는 호스트에서 탐지되는 애플리케이션의 제품 및 버전, 사용 가능한 클라이언트 또는 웹 애플리케이션 정보, 그리고 애플리케이션 사용이 마지막으로 탐지된 시간을 표시합니다.

이 섹션은 호스트에서 실행 중인 클라이언트를 최대 16개 나열합니다. 이 한계에 도달하면 사용자가 호스트에서 클라이언트 애플리케이션을 삭제하거나 비활성(클라이언트 시간 초과)으로 인해 시스템이 호스트 프로파일에서 클라이언트를 삭제할 때까지 능동 및 수동 소스의 새 클라이언트 정보가 삭제됩니다.

또한 탐지된 각 웹 브라우저에 대해 시스템은 액세스된 처음 100개의 웹 애플리케이션을 표시합니다. 이 한계에 도달하면 다음과 같이 될 때까지 능동 및 수동 소스의 해당 브라우저에 연결된 새 웹 애플리케이션이 삭제됩니다.

- 웹 브라우저 클라이언트 애플리케이션이 시간 초과됨, 또는
- 호스트 프로파일에서 웹 애플리케이션과 관련된 애플리케이션 정보 삭제

활성화된 상관관계 정책의 규정 준수 허용 목록을 위반하는 애플리케이션이 호스트에서 실행되고 있는 경우, Firepower Management Center에서는 규정을 준수하지 않는 애플리케이션을 허용 목록 위반으로 표시합니다.

팁 호스트의 특정 애플리케이션에 연결된 연결 이벤트를 분석하려면 애플리케이션 옆에 있는 **Logging(**로깅**)** ( )을 클릭합니다. 연결 이벤트에 대한 기본 설정 워크플로의 첫 번째 페이지가 나타나고 애플리케이션의 유형, 제품 및 버전에 의해 제한되는 연결 이벤트 및 호스트의 IP 주소를 보여줍니다. 연결 이벤트에 대한 기본 설정 워크플로가 없다면 선택해야 합니다.

다음은 호스트 프로파일에 나타나는 애플리케이션 정보에 대한 설명입니다.

애플리케이션 프로토콜

애플리케이션(HTTP 브라우저, DNS 클라이언트 등)이 사용하는 애플리케이션 프로토콜을 표시합니다.

클라이언트

Firepower System에 의해 식별되거나 Nmap에 의해 캡처되거나 호스트 입력 기능을 통해 획득된 경우, 페이로드에서 추출되는 클라이언트 정보. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

버전

클라이언트의 버전을 표시합니다.

웹 애플리케이션

웹 브라우저의 경우 시스템이 http 트래픽에서 탐지한 콘텐츠. 웹 애플리케이션 정보는 Firepower System에 의해 식별되거나 Nmap에 의해 캡처되거나 호스트 입력 기능을 통해 수집된 특정 콘텐츠 유형(예: WMV 또는 QuickTime)을 나타냅니다. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

호스트 프로파일에서 웹 애플리케이션 삭제

호스트 프로파일에서 애플리케이션을 삭제하여 호스트에서 실행되고 있지 않은 애플리케이션을 제거할 수 있습니다. 호스트에서 애플리케이션을 삭제하면 해당 호스트는 허용 목록 규정 준수 상태로 전환될 수 있습니다.

참고 해당 애플리케이션이 다시 탐지되면 네트워크 맵 및 호스트 프로파일에 다시 추가됩니다.

프로시저

단계 **1** 호스트 프로파일에서 **Applications(**애플리케이션**)** 섹션으로 이동합니다.

단계 **2** 삭제할 애플리케이션 옆에 있는 **Delete(**삭제**)** ( )을 클릭합니다.

호스트 프로파일의 호스트 프로토콜

각 호스트 프로파일에는 호스트와 연결된 네트워크 트래픽에서 탐지된 프로토콜에 대한 정보가 포함되어 있습니다. 이 정보에는 다음이 포함됩니다.

프로토콜

호스트가 사용하는 프로토콜의 이름.

레이어

프로토콜이 실행되는 네트워크 레이어(`Network` 또는 `Transport`).

호스트 프로파일에 표시되는 프로토콜이 활성화된 상관관계 정책의 규정준수 허용리스트를 위반하는 경우, management center에서는 규정을 준수하지 않는 프로토콜을 허용리스트 위반으로 표시합니다.

호스트에서 실행되고 있지 않음을 알고 있는 프로토콜이 호스트 프로파일에 나열되는 경우, 해당 프로토콜을 삭제할 수 있습니다. 호스트에서 프로토콜을 삭제하면 해당 호스트가 규정준수 허용리스트를 준수하게 될 수 있습니다.

참고 시스템은 해당 프로토콜을 다시 탐지하면 네트워크 맵 및 호스트 프로파일에 다시 추가합니다.

호스트 프로파일에서 프로토콜 삭제

프로시저

단계 **1** 호스트 프로파일의 **Protocols(**프로토콜**)** 섹션으로 이동합니다.

단계 **2** 삭제할 프로토콜 옆에 있는 **Delete(**삭제**)** ( )를 클릭합니다.

호스트 프로파일의 보안 침해 지표

시스템은 다양한 유형의 데이터(침입 이벤트, 보안 인텔리전스, 연결 이벤트, 파일 또는 악성코드 이벤트)를 상호 연결하여 모니터링되는 네트워크의 호스트가 악의적인 수단에 의해 보안이 침해될 가능성이 있는지를 확인합니다. 이벤트 데이터의 특정 조합 및 빈도는 영향받는 호스트에서 IOC(보안 침해 지표) 태그를 트리거합니다.

호스트 프로파일의 Indications of Compromise(보안 침해 지표) 섹션에는 호스트에 대한 모든 보안 침해 지표 태그가 표시됩니다.

보안 침해 지표 태그를 지정하도록 시스템을 구성하려면 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 침해 지표 규칙 활성화를 참고하십시오.

보안 침해 지표를 사용하는 방법에 대한 자세한 내용은 보안 침해 지표 데이터, 946 페이지 및 해당 항목의 하위 항목을 참조하십시오.

호스트 프로파일의 VLAN 태그

호스트가 VLAN(Virtual LAN)의 멤버인 경우 호스트 프로파일의 VLAN Tag(VLAN 태그) 섹션이 나타납니다.

물리적 네트워크 장비는 종종 VLAN을 사용하여 서로 다른 네트워크 블록에서 논리적 네트워크 세그먼트를 생성합니다. 시스템은 802.1q VLAN 태그를 탐지하고 각각에 대해 다음과 같은 정보를 표시합니다.

- **VLAN ID**는 호스트가 멤버인 VLAN을 식별합니다. 802.1q VLAN의 경우 0~4095 사이의 정수일 수 있습니다.
- **Type**은 VLAN 태그를 포함하는 캡슐화된 패킷을 식별하며, 이더넷 또는 토큰 링일 수 있습니다.
- **Priority**는 VLAN 태그의 우선순위를 식별하며, 범위는 0~7의 정수이고 7이 가장 높은 우선순위입니다.

VLAN 태그가 패킷 내에 중첩된 경우 시스템은 가장 안쪽의 VLAN 태그를 처리하고 management center는 이를 표시합니다. 시스템은 ARP 및 DHCP 트래픽을 통해 식별하는 MAC 주소에 대해서만 VLAN 태그 정보를 수집하고 표시합니다.

예를 들면 VLAN이 프린터로만 구성되어 있고 시스템이 해당 VLAN에서 Microsoft Windows 2000 운영 체제를 탐지하는 경우에는 VLAN 태그 정보가 유용할 수 있습니다. VLAN 정보는 또한 시스템이 좀 더 정확한 네트워크 맵을 생성하는 데에도 도움이 됩니다.

호스트 프로파일의 사용자 기록

호스트 프로파일의 사용자 기록 부분은 사용자 활동의 마지막 24시간을 그래프로 보여줍니다. 일반적인 사용자는 저녁에 로그오프하고 호스트 리소스를 다른 사용자와 공유할 것입니다. 이메일 확인을 위한 요청 등 정기적인 로그인 요청은 짧은 일반 막대로 표시됩니다. 사용자 ID의 목록에는 사용자 로그인이 탐지된 시점을 나타내는 막대 그래프가 제공됩니다. 권한 없는 로그인의 경우에는 막대 그래프가 회색입니다.

시스템은 권한 없는 사용자의 호스트 로그인을 해당 호스트의 IP 주소와 연결하여, 사용자가 호스트의 사용자 기록에 나타나도록 합니다. 그러나 동일한 호스트에서 권한 있는 사용자 로그인이 탐지되면 권한 있는 사용자 로그인과 연결된 사용자가 호스트 IP 주소의 연결 관계를 인수하며, 권한 없는 새 사용자 로그인은 호스트 IP 주소와 사용자의 연결 관계를 중단하지 않습니다. 네트워크 검색 정책에서 실패한 로그인의 캡처를 구성하는 경우 목록에는 호스트 로그인에 실패한 사용자가 포함됩니다.

호스트 프로파일의 호스트 속성

호스트 속성을 사용하면 네트워크 환경에서 중요한 방법으로 호스트를 분류할 수 있습니다. Firepower System에는 3가지 속성이 존재합니다.

- 사전 정의된 호스트 속성
- 컴플라이언스 허용 리스트 호스트 속성
- 사용자 정의 호스트 속성

사전 정의된 속성을 설정하거나 사용자 정의 호스트 속성을 생성한 후에는, 호스트 속성 값을 할당해야 합니다.

참고 호스트 속성은 어떤 도메인 레벨에서도 정의할 수 있습니다. 현재 및 상위 도메인에서 생성된 호스트 속성을 할당할 수 있습니다.

사전 정의된 호스트 속성

management center은(는) 사전 정의된 호스트 속성 2개를 제공합니다.

호스트 중요도

이 속성을 사용하여 특정 호스트의 비즈니스 중요도를 지정하고 상관관계 응답을 호스트 중요도에 맞게 조정하십시오. 예를 들어 조직의 메일 서버가 일반적인 사용자 워크스테이션보다 비즈니스에 더 중요하다고 생각한다면 메일 서버에는 High, 다른 주요 비즈니스 디바이스에는 Medium, 기타 호스트에는 Low 값을 할당할 수 있습니다. 그런 다음 영향받는 호스트의 중요도를 기반으로 서로 다른 알림을 생성하는 상관관계 정책을 생성할 수 있습니다.

Notes(참고**)**

이 호스트 한정 속성을 사용하여 다른 분석가에게 보여줄 호스트에 대한 정보를 기록하십시오. 예를 들어 운영체제의 패치되지 않은 이전 버전이 있는 테스트용 컴퓨터가 네트워크에 있는 경우, Notes 기능을 사용하여 시스템을 의도적으로 패치하지 않았음을 표시할 수 있습니다.

허용 목록 호스트 속성

자동으로 생성되는 각 규정 준수 허용 목록은 허용 목록과 동일한 이름으로 호스트 속성을 생성합니다. 가능한 허용 목록 호스트 속성은 다음과 같습니다.

- Compliant - 허용 목록을 준수하는 호스트를 식별합니다.
- Non-Compliant - 허용 목록을 위반하는 호스트를 식별합니다.
- Not Evaluated - 허용 목록의 유효한 대상이 아니거나 어떤 이유로든 평가되지 않은 호스트를 식별합니다.

허용 목록 호스트 속성 값을 수정하거나 허용 목록 호스트 속성을 삭제할 수 없습니다.

사용자 정의 호스트 속성

사전 정의된 호스트 속성 또는 컴플라이언스 허용 목록 호스트 속성에서 사용하는 것과는 다른 기준을 이용해 호스트를 식별하고 싶다면, 사용자 정의 호스트 속성을 사용하면 됩니다. 예를 들어, 다음이 가능합니다.

- 호스트에 물리적 위치 식별자(예: 시설 코드, 도시 또는 방 번호)를 할당합니다.

- 특정 호스트의 담당 시스템 관리자가 누구인지를 나타내는 Responsible Party Identifier(담당자 식별자)를 할당합니다. 호스트와 관련된 문제가 탐지될 때 올바른 시스템 관리자에게 알림을 전송하도록 상관관계 규칙 및 정책을 구성할 수 있습니다.
- 호스트의 IP 주소를 기반으로 사전 정의된 목록에서 호스트로 값을 자동으로 할당합니다. 이 기능은 네트워크에 처음으로 표시되는 새 호스트에 값을 할당할 때 유용하게 활용할 수 있습니다.

사용자 정의 호스트 속성은 호스트 프로파일 페이지에 나타나며, 여기서 호스트 단위로 값을 할당할 수 있습니다. 다음 작업도 가능합니다.

- 상관관계 정책 및 검색에서 속성을 사용합니다.
- 호스트 속성 테이블 보기에서 속성을 보고 이를 기반으로 보고서를 생성합니다.

사용자 정의 호스트 속성의 유형은 다음과 같습니다.

텍스트

텍스트 문자열을 호스트에 수동으로 할당할 수 있습니다.

정수

양의 정수 범위의 첫 번째와 마지막 숫자를 지정한 다음 이러한 숫자 중 하나를 호스트에 수동으로 할당할 수 있습니다.

목록

문자열 값의 목록을 생성한 다음 이러한 값 중 하나를 호스트에 수동으로 할당할 수 있습니다. 호스트의 IP 주소를 기반으로 호스트에 값을 자동으로 할당할 수도 있습니다.

여러 IP 주소가 있는 호스트에서 한 IP 주소를 기반으로 값을 자동 할당하면, 그 호스트와 연결된 모든 주소에 해당 값이 적용됩니다. Host Attributes(호스트 속성) 테이블을 볼 때는 이러한 점에 유의해야 합니다.

목록 값을 자동으로 할당하는 경우에는 일반적인 IP 주소가 아닌 네트워크 개체 사용을 고려해 보십시오. 이 방법을 이용하면 관리 용이성을 개선할 수 있으며, 특히 재정의를 활성화한 개체가 하위 도메인 관리자가 자신의 로컬 환경에 맞게 상위 설정을 조정하도록 허용하는 다중 도메인 구축에서 더욱 효과적입니다. 다중 도메인 구축의 경우에는, 자동 할당된 목록을 상위 도메인 수준에서 정의하며 하위 도메인이 중복되는 IP 주소를 사용할 때 의도하지 않은 호스트가 매칭되지 않도록 주의하십시오.

URL

URL 값을 호스트에 수동으로 할당할 수 있습니다.

사용자 정의 호스트 속성을 삭제하면 이를 사용하는 모든 호스트 프로파일에서 해당 속성이 제거됩니다.

텍스트 또는 URL 기반 호스트 속성 생성

프로시저

단계 1 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Host Attributes(**호스트 속성**)**을(를) 선택합니다.
단계 2 **Host Attribute Management(**호스트 속성 관리**)**를 클릭합니다.
단계 3 **Create Attribute(**속성 생성**)**를 클릭합니다.
단계 4 **Name(**이름**)**을 입력합니다.
단계 5 사용자 정의 호스트 속성, 911 페이지에 설명된 대로 생성하려는 속성의 **Type(**유형**)**을 선택합니다.
단계 6 **Save(**저장**)**를 클릭합니다.

정수 기반 호스트 속성 생성

정수 기반 호스트 속성을 정의할 때는 호스트가 허용하는 숫자 범위를 지정해야 합니다.

프로시저

단계 1 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Host Attributes(**호스트 속성**)**을(를) 선택합니다.
단계 2 **Host Attribute Management(**호스트 속성 관리**)**를 클릭합니다.
단계 3 **Create Attribute(**속성 생성**)**를 클릭합니다.
단계 4 **Name(**이름**)**을 입력합니다.
단계 5 사용자 정의 호스트 속성, 911 페이지에 설명된 대로 생성하려는 속성의 **Type(**유형**)**을 선택합니다.
단계 6 호스트에 할당할 수 있는 최소 정수 값을 **Min(**최소**)** 필드에 입력합니다.
단계 7 호스트에 할당할 수 있는 최대 정수 값을 **Max(**최대**)** 필드에 입력합니다.
단계 8 **Save(**저장**)**를 클릭합니다.

목록 기반 호스트 속성 생성

목록 기반 호스트 속성을 정의할 때에는 목록의 각 값을 제공해야 합니다. 이러한 값에는 영숫자 문자, 공백 및 기호가 포함될 수 있습니다.

프로시저

단계 1 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Host Attributes(**호스트 속성**)**을(를) 선택합니다.
단계 2 **Host Attribute Management(**호스트 속성 관리**)**를 클릭합니다.

단계 **3** **Create Attribute(**속성 생성**)**를 클릭합니다.

단계 **4** **Name(**이름**)**을 입력합니다.

단계 **5** 사용자 정의 호스트 속성, 911 페이지에 설명된 대로 생성하려는 속성의 **Type(**유형**)**을 선택합니다.

단계 **6** 목록에 값을 추가하려면 **Add Value(**값 추가**)**를 클릭합니다.

단계 **7** 추가하려는 첫 번째 값을 **Name(**이름**)** 필드에 입력합니다.

단계 **8** 원하는 경우, 방금 추가한 속성 값을 호스트에 자동 할당하려면 **Add Networks(**네트워크 추가**)**를 클릭합니다.

단계 **9** 추가한 값을 **Value(**값**)** 드롭다운 목록에서 선택합니다.

단계 **10** 이 값을 자동 할당할 IP 주소 블록을 나타내는 IP 주소와 네트워크 마스크(IPv4)를 **IP Address(IP** 주소**)** 및 **Netmask(**넷마스크**)** 필드에 입력합니다.

단계 **11** 목록에 값을 더 추가하여 IP 주소 블록에 속하는 새 호스트에 자동으로 할당하려면 6~10단계를 반복합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

호스트 속성값 설정

미리 정의된 호스트 속성 및 사용자 정의 호스트 속성의 값을 설정할 수 있습니다. 시스템에서 생성된 컴플라이언스 허용 호스트 속성의 값은 설정할 수 없습니다.

프로시저

단계 **1** 수정하려는 호스트 프로파일을 엽니다.

단계 **2** **Attributes(**속성**)** 섹션에서 **Edit Attributes(**속성 수정**)**를 클릭합니다.

단계 **3** 원하는 대로 속성을 업데이트합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

호스트 프로파일의 허용 목록 위반

규정 준수 허용 목록(또는 허용 목록)는 특정 서브넷에서 실행 가능한 운영 체제, 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 및 프로토콜을 지정할 수 있는 기준 집합입니다.

활성 상관관계 정책에 허용 목록을 추가한 경우 시스템이 호스트에서 허용 목록 위반을 탐지하면, management center는 허용 목록 이벤트(특정 상관관계 이벤트 유형)를 데이터베이스에 로깅합니다. 이러한 각 허용 목록 이벤트는 특정 호스트가 어떻게, 왜 허용 목록을 위반했는지를 나타내는 허용목록 위반과 연결됩니다. 호스트가 하나 이상의 허용 목록을 위반하면 호스트 프로필에서 두 가지 방법으로 이러한 위반을 볼 수 있습니다.

첫째, 호스트 프로필은 호스트에 연결된 모든 개별 허용 목록 위반을 나열합니다.

다음은 호스트 프로필에 표시되는 허용 목록 위반 정보에 대한 설명입니다.

유형

위반의 유형, 즉 위반이 발생한 원인(규정을 준수하지 않는 운영 체제, 애플리케이션, 서버 또는 프로토콜).

이유

위반의 특정 이유. 예를 들어 Microsoft Windows 호스트만 허용하는 허용 목록이 있는 경우, 호스트 프로파일에는 호스트에서 실행 중인 현재 운영 체제(예: `Linux 2.4, 2.6`)가 표시됩니다.

허용 목록

위반과 연결된 허용 목록의 이름.

둘째, 운영 체제, 애플리케이션, 프로토콜 및 서버와 관련된 섹션에서 management center는 규정을 준수하지 않는 요소를 허용 목록 위반 아이콘으로 표시합니다. 예를 들어 Microsoft Windows 호스트만 허용하는 허용 목록의 경우, 호스트 프로필은 해당 호스트의 운영 체제 정보 옆에 허용 목록 위반 아이콘을 표시합니다.

참고 호스트의 프로필을 사용하여 규정 준수 허용 목록에 대한 공유 호스트 프로필을 생성할 수 있습니다.

공유 허용 목록 호스트 프로파일 생성

규정 준수 허용 목록 공유 호스트 프로필은 여러 허용 목록에 걸쳐 대상 호스트에서 실행 가능한 운영 체제, 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 및 프로토콜을 지정합니다. 여러 개의 허용 목록을 생성하지만 동일한 호스트 프로파일을 사용하여 허용 목록 전반에 걸쳐 특정 운영체제를 실행하는 호스트를 평가하려는 경우, 공유 호스트 프로파일을 사용합니다.

알려진 IP 주소가 있는 호스트의 호스트 프로필을 사용하여 규정 준수 허용 목록이 사용할 수 있는 공유 호스트 프로필을 생성할 수 있습니다. 그러나 시스템이 호스트의 운영 체제를 아직 식별하지 못한 경우에는 개별 호스트의 호스트 프로파일을 기반으로 공유 호스트 프로파일을 생성할 수 없습니다.

프로시저

단계 **1** 호스트 프로파일에서 **Generate(**생성**)**허용 목록 **Profile(**프로파일**)**을 클릭합니다.

단계 **2** 특정 요구에 맞게 공유 호스트 프로파일을 수정 및 저장합니다.

관련 항목

허용 리스트 호스트 프로필 빌드, 1008 페이지

호스트 프로파일의 악성코드 탐지

Most Recent Malware Detections(가장 최근의 악성코드 탐지) 섹션에는 호스트가 악성코드 파일을 주고받은 가장 최근의 악성코드 이벤트가 최대 100개까지 나열됩니다. 호스트 프로파일에는 네트워크 기반 악성코드 이벤트(악성코드 대응 에 의해 생성)와 엔드포인트 기반 악성코드 이벤트(AMP for Endpoints에 의해 생성)가 모두 나열됩니다.

파일이 악성코드로 소급 식별된 파일 이벤트에 호스트가 관련된 경우, 악성코드 식별이 발생한 후 파일이 전송된 원래 이벤트가 악성코드 탐지 목록에 나타납니다. 악성코드로 식별된 파일이 악성코드가 아닌 것으로 소급 결정되면 해당 파일과 연결된 악성코드 이벤트가 더 이상 목록에 나타나지 않습니다. 예를 들어 파일에 `Malware(악성코드)` 속성이 있고 해당 속성이 `Clean(정상)`으로 변경되면 해당 파일의 이벤트는 호스트 프로파일의 악성코드 탐지 목록에서 제거됩니다.

호스트 프로필에서 악성코드 탐지를 볼 때 **Malware(**악성코드**)**를 클릭하여 해당 호스트의 악성코드 이벤트를 볼 수 있습니다.

다음은 호스트 프로파일의 Most Recent Malware Detections(가장 최근의 악성코드 탐지) 섹션에 있는 열에 대한 설명입니다.

시간

이벤트가 생성된 날짜 및 시간

파일이 악성코드로 소급 식별된 이벤트의 경우, 악성코드가 식별된 시간이 아니라 원래 이벤트의 시간을 나타냅니다.

호스트 역할

탐지된 악성코드 전송에서 호스트의 역할(발신자 또는 수신자). AMP for Endpoints에 의해 생성된 악성코드 이벤트("엔드포인트 기반 악성코드 이벤트")의 경우, 호스트는 항상 수신자입니다.

위협 이름

탐지된 악성코드의 이름.

파일 이름

악성코드 파일의 이름.

파일 유형

`PDF` 또는 `MSEXE` 등의 파일 형식.

호스트 프로파일의 취약성

호스트 프로파일의 Vulnerabilities(취약성) 섹션에는 해당 호스트에 영향을 미치는 취약성이 나열됩니다. 이러한 취약성은 시스템이 호스트에서 탐지한 운영 체제, 서버, 애플리케이션에 기반합니다.

호스트의 운영 체제 ID 또는 호스트의 애플리케이션 프로토콜 중 하나에 ID 충돌이 있는 경우, 시스템은 충돌이 해결될 때까지 두 ID에 대한 취약성을 나열합니다.

NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에 대해서는 운영 체제 정보가 제공되지 않으므로 시스템은 이러한 호스트와 관련된 침입 이벤트에 대해 취약함(영향 레벨 1: 빨강) 영향 레벨을 할당할 수 없습니다. 이러한 경우에는 호스트 입력 기능을 사용하여 호스트에 대한 운영 체제 ID를 수동으로 설정합니다.

서버 공급업체 및 버전 정보는 대체로 트래픽에 포함되지 않습니다. 기본적으로 시스템은 트래픽을 보내고 받는 호스트에 대해 관련 취약성을 매핑하지 않습니다. 그러나 공급업체 또는 버전 정보가 없는 특정 애플리케이션 프로토콜에 대한 취약성을 매핑하도록 시스템을 구성할 수 있습니다.

호스트 입력 기능을 사용하여 네트워크의 호스트에 대한 서드파티 취약성 정보를 추가하는 경우 추가적인 Vulnerabilities(취약성) 섹션이 나타납니다. 예를 들어 QualysGuard Scanner에서 취약성을 가져오면 호스트 프로파일에 QualysGuard Vulnerabilities 섹션이 포함됩니다. 서드파티 취약성의 경우 호스트 프로파일의 해당 Vulnerabilities(취약성) 섹션에 표시되는 정보는 호스트 입력 기능을 사용하여 취약성 데이터를 가져올 때 제공한 정보로 제한됩니다.

서드파티 취약성을 운영 체제 및 애플리케이션 프로토콜과 연결할 수 있지만 클라이언트와는 연결할 수 없습니다. 서드파티 취약성 가져오기에 대한 자세한 내용은 *Firepower System Host Input API* 설명서를 참조하십시오.

다음은 호스트 프로파일의 Vulnerabilities(취약성) 섹션에 있는 열에 대한 설명입니다.

이름

취약성의 이름.

원격

취약성이 원격으로 악용될 수 있는지를 나타냅니다. 이 열이 비어 있으면 취약성 정의에 이 정보가 포함되지 않은 것입니다.

구성 요소

취약성과 관련된 운영 체제, 애플리케이션 프로토콜 또는 클라이언트의 이름.

Port(포트)

취약성이 지정된 포트에서 실행 중인 애플리케이션 프로토콜과 연결된 경우 포트 번호.

관련 항목

취약성 데이터 필드, 960 페이지
취약성 비활성화, 961 페이지

취약성 패치 다운로드

네트워크의 호스트에서 검색된 취약성을 완화하기 위한 패치를 다운로드할 수 있습니다.

프로시저

단계 **1** 패치를 다운로드할 호스트의 호스트 프로파일에 액세스합니다.

단계 **2** **Vulnerabilities(**취약성**)** 섹션을 확장합니다.

단계 **3** 패치를 적용할 취약성의 이름을 클릭합니다.

단계 **4** 취약성에 대한 패치의 목록을 표시하려면 **Fixes(**수정**)** 섹션을 확장합니다.

단계 **5** 다운로드할 패치 옆에 있는 **Download(**다운로드**)**를 클릭합니다.

단계 **6** 패치를 다운로드하고 영향받는 시스템에 적용합니다.

개별 호스트용 취약성 비활성화

호스트 취약성 편집기를 사용하여 호스트별로 취약성을 비활성화할 수 있습니다. 호스트에 대한 취약성을 비활성화할 경우 해당 호스트에 대한 영향 상관관계에는 여전히 사용되지만 영향 레벨은 자동으로 한 단계 줄어듭니다.

프로시저

단계 **1** 호스트 프로파일의 **Vulnerabilities(**취약성**)** 섹션으로 이동합니다.

단계 **2** **Edit Vulnerabilities(**취약성 수정**)**를 클릭합니다.

단계 **3** **Valid Vulnerabilities(**유효한 취약성**)** 목록에서 취약성을 선택하고 아래쪽 화살표를 클릭하여 **Invalid Vulnerabilities(**유효하지 않은 취약성**)** 목록으로 이동시킵니다.

팁 클릭하고 끌어 여러 인접 취약성을 선택할 수 있습니다. 또한 취약성을 두 번 클릭하여 다른 목록으로 이동시킬 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 원하는 경우, **Invalid Vulnerabilities(**유효하지 않은 취약성**)** 목록에서 **Valid Vulnerabilities(**유효한 취약성**)** 목록으로 취약성을 이동시켜 호스트의 취약성을 활성화합니다.

관련 항목

개별 취약성 비활성화, 919 페이지
다중 취약성 비활성화, 963 페이지

개별 취약성 비활성화

호스트 프로파일에서 취약성을 비활성화하면 해당 취약성은 네트워크 맵의 모든 호스트에서 비활성화됩니다. 하지만 언제든 다시 활성화할 수 있습니다.

다중 도메인 구축에서 상위 도메인의 취약성을 비활성화하면 모든 하위 도메인에서 해당 취약성이 비활성화됩니다. 취약성이 상위 도메인에서 활성화된 경우, 리프 도메인은 디바이스에서 해당 취약성을 활성화하거나 비활성화할 수 있습니다.

프로시저

단계 **1** 취약성 세부 정보에 액세스:

- 영향을 받는 호스트 프로파일에서 **Vulnerabilities(**취약성**)** 섹션을 확장하고 활성화 또는 비활성화하려는 취약성의 이름을 클릭합니다.
- 미리 정의된 워크플로우에서 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Vulnerabilities(**취약성**)**을 선택하고 클릭하고 활성화하거나 비활성화하려는 취약성 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **2** **Impact Qualification** 드롭다운 목록에서 **Disabled(**비활성화**)**를 선택합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **3** 네트워크 맵의 모든 호스트에 대해 **Impact Qualification** 값을 변경할 것인지 확인합니다.

단계 **4** **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 원하는 경우, 위의 단계를 수행하면서 **Impact Qualification** 드롭다운 목록에서 **Enabled(**활성화**)**를 선택하여 취약성을 활성화합니다.

관련 항목

개별 호스트용 취약성 비활성화, 918 페이지
다중 취약성 비활성화, 963 페이지
운영 체제 ID 충돌, 901 페이지

호스트 프로파일의 스캔 결과

Nmap을 사용하여 호스트를 스캔하거나 Nmap 스캔에서 결과를 가져오면 그러한 결과는 스캔에 포함된 호스트의 호스트 프로파일에 나타납니다.

필터링되지 않은 열린 포트에서 실행되는 호스트 운영 체제 및 서버에 대해 Nmap이 수집하는 정보는 각각 호스트 프로파일의 Operating System(운영 체제) 및 Servers(서버) 섹션에 직접 추가됩니다. 또한

Nmap은 해당 호스트에 대한 스캔 결과의 목록을 Scan Results(스캔 결과) 섹션에 추가합니다. Scan Results(스캔 결과) 섹션이 프로파일에 나타나려면 스캔은 호스트에서 열린 포트를 찾아야 합니다.

각 결과는 정보의 소스, 스캔된 포트의 번호와 유형, 포트에서 실행되는 서버의 이름, Nmap에서 탐지한 추가 정보(예: 포트의 상태 또는 서버의 공급업체 이름) 등을 나타냅니다. UDP 포트를 스캔하는 경우, 해당 포트에서 탐지된 서버는 Scan Results(스캔 결과) 섹션에만 나타납니다.

호스트 프로파일에서 Nmap 스캔을 수행할 수 있습니다.

호스트 프로파일에서 호스트 스캔

호스트 프로파일에서 호스트에 대해 Nmap 스캔을 수행할 수 있습니다. 스캔이 완료되면 해당 호스트의 서버 및 운영 체제 정보가 호스트 프로파일에서 업데이트됩니다. 호스트 프로파일의 Scan Results(스캔 결과) 섹션에 스캔 결과가 추가됩니다.

⚠

주의 또 다른 Nmap 스캔을 실행하거나 우선순위가 더 높은 호스트 입력으로 재정의할 때까지 Nmap 제공 서버 및 운영 체제 데이터는 고정 상태로 유지됩니다. Nmap을 이용해 호스트를 스캔하기로 했다면, 스캔을 정기적으로 예약하십시오.

시작하기 전에

- Nmap 스캔 인스턴스를 추가합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 호스트 *ID* 소스 장의 내용을 참고하십시오.

프로시저

단계 **1** 호스트 프로파일에서 **Scan Host(**호스트 스캔**)**를 클릭합니다.

단계 **2** 호스트 스캔에 사용할 스캔 교정 옆에 있는 **Scan(**스캔**)**을 클릭합니다.

시스템이 호스트를 스캔하고 결과를 호스트 프로파일에 추가합니다.

관련 항목

Nmap 스캔 자동화, 507 페이지

호스트 프로파일 기록

기능	버전	세부 사항
VRF 사용 시 제한 사항	6.6	사용자 환경에서 가상 라우팅 및 포워딩을 사용하는 경우 VRF가 중복 네트워크 공간을 포함할 수 있으므로 단일 IP 주소가 여러 호스트를 나타낼 수 있습니다. 지원되는 플랫폼: FMC

36 장

검색 이벤트

다음 주제에서는 검색 이벤트를 사용하는 방법을 설명합니다.

검색 이벤트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 보안 분석가

검색 이벤트의 검색 및 ID 데이터

시스템은 모니터링되는 네트워크에서 탐지된 변경을 나타내는 이벤트의 테이블을 생성합니다. 이러한 테이블을 사용하여 네트워크에서의 사용자 활동을 검토하고 대응 방법을 결정할 수 있습니다. 네트워크 검색 및 *ID* 정책은 수집할 데이터 종류, 모니터링할 네트워크 세그먼트, 이를 위해 사용할 특정 하드웨어 인터페이스를 지정합니다.

검색 및 ID 이벤트 테이블을 사용하여 네트워크의 호스트, 애플리케이션, 사용자에 연결된 위협을 식별할 수 있습니다. 시스템은 시스템에서 생성되는 이벤트 분석에 사용할 수 있는 사전 정의 워크플로 집합을 제공합니다. 특정 요구와 일치하는 정보만 표시하는 맞춤형 워크플로를 생성할 수도 있습니다.

분석을 위해 네트워크 검색 및 ID 데이터를 수집하고 저장하려면 네트워크 검색 및 ID 정책을 구성해야 합니다. ID 정책을 구성한 후에는 액세스 제어 정책에서 ID 정책을 호출하여 트래픽 모니터링에 사용할 디바이스에 구축해야 합니다.

네트워크 검색 정책은 호스트, 애플리케이션, 권한 없는 사용자 데이터를 제공합니다. ID 정책은 권한 있는 사용자 데이터를 제공합니다.

다음 검색 이벤트 테이블은 Analysis(분석) > Hosts(호스트) 및 Analysis(분석) > Users(사용자) 메뉴 아래 위치합니다.

검색 이벤트 테이블	검색 데이터로 채워지는지 여부	**ID** 데이터로 채워지는지 여부
호스트	예	아니요
호스트 보안 침해 지표	예	아니요
애플리케이션	예	아니요
애플리케이션 세부사항	예	아니요
서버	예	아니요
호스트 속성	예	아니요
검색 이벤트	예	예
사용자 보안 침해 지표	예	예
활성 세션	예	예
사용자의 활동	예	예
사용자	예	예
취약성	예	아니요
서드파티 취약성	예	아니요

검색 이벤트 통계 보기

Discovery Statistics(검색 통계) 페이지에는 시스템에서 탐지한 호스트, 이벤트, 프로토콜, 애플리케이션 프로토콜 및 운영 체제의 요약이 표시됩니다.

이 페이지에는 마지막 시간에 대한 통계 및 총 누적 통계가 나열됩니다. 특정 디바이스 또는 모든 디바이스에 대한 통계를 볼 수 있습니다. 요약 내에 나열된 이벤트, 서버, 운영 체제 또는 운영 체제 공급업체를 클릭하여 페이지의 항목과 일치하는 이벤트를 볼 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Discovery Statistics(**검색 통계**)**을(를) 선택합니다.

단계 **2** 통계를 보려는 디바이스를 **Select Device(**디바이스 선택**)** 목록에서 선택합니다. 선택적으로, 모든 관리하는 모든 디바이스에 대한 통계를 보려면 management center를 선택합니다.

단계 **3** 다음과 같은 옵션이 있습니다.

- Statistics Summary(통계 요약)에서 통계 요약 섹션, 923 페이지의 설명에 따라 일반 통계를 볼 수 있습니다.
- Event Breakdown(이벤트 분류)에서 보려고 하는 이벤트 유형을 클릭합니다. 이벤트가 표시되지 않는 경우, 타임 윈도우 변경, 710 페이지에 설명된 대로 시간 범위를 조정해야 할 수 있습니다.
- Protocol Breakdown(프로토콜 분류)에서 탐지된 이벤트가 현재 사용 중인 프로토콜을 볼 수 있습니다.
- Application Protocol Breakdown(애플리케이션 프로토콜 분류)에서 보려는 애플리케이션 프로토콜의 이름을 클릭합니다.
- OS Breakdown(OS 분류)에서 **OS Name(OS** 이름**)** 또는 **OS Vendor(OS** 공급업체**)**를 클릭합니다.

관련 항목

이벤트 분류 섹션, 924 페이지
프로토콜 분류 섹션, 925 페이지
애플리케이션 프로토콜 분류 섹션, 925 페이지
OS 분류 섹션, 925 페이지

통계 요약 섹션

다음은 Statistics Summary(통계 요약) 섹션의 행에 대한 설명입니다.

Total events

management center에 저장된 총 검색 이벤트 수.

최근 **1**시간의 전체 이벤트

마지막 시간에 생성된 총 검색 이벤트 수.

최근 **1**일의 전체 이벤트

마지막 날에 생성된 총 검색 이벤트 수

Total Application Protocols

탐지된 호스트에서 실행 중인 서버의 총 애플리케이션 프로토콜 수.

Total IP Hosts

고유한 IP 주소로 식별된 총 탐지된 호스트 수.

Total MAC Hosts

IP 주소로 식별되지 않은 총 탐지된 호스트 수.

모든 디바이스에 대한 검색 통계를 보든 특정 디바이스에 대한 검색 통계를 보든, Total MAC Hosts 통계는 동일합니다. 매니지드 디바이스는 IP 주소를 기반으로 호스트를 검색하기 때문입니다. 이 통계는 다른 수단에 의해 식별되는 총 호스트 수를 제공하며 특정 매니지드 디바이스와는 독립적입니다.

Total Routers

라우터로서 식별된 총 탐지된 노드 수.

Total Bridges

브리지로서 식별된 총 탐지된 노드 수.

Host Limit Usage

현재 사용 중인 호스트 제한의 총 비율. 호스트 제한은 management center의 모델로 정의됩니다. 모든 매니지드 디바이스에 대한 통계를 보는 경우에만 Host Limit Usage가 나타납니다.

참고 호스트 제한에 도달하고 호스트가 삭제되는 경우, 검색 데이터를 비운 네트워크 맵에 호스트가 다시 나타나지 않습니다.

Last Event Received

가장 최근 검색 이벤트가 발생한 날짜 및 시간.

Last Connection Received

가장 최근 연결이 완료된 날짜 및 시간.

이벤트 분류 섹션

Event Breakdown(이벤트 분류) 섹션에는 마지막 시간 내에 발생한 검색 및 호스트 입력 이벤트의 각 유형별 카운트는 물론 데이터베이스에 저장된 각 이벤트 유형의 총 카운트도 나열됩니다.

검색 및 호스트 입력 이벤트에 대한 세부사항을 보는 데에도 Event Breakdown(이벤트 분류) 섹션을 사용할 수 있습니다.

관련 항목

검색 및 호스트 입력 이벤트, 929 페이지

프로토콜 분류 섹션

Protocol Breakdown(프로토콜 분류) 섹션에는 탐지된 호스트에서 현재 사용 중인 프로토콜이 나열됩니다. 탐지된 각 프로토콜 이름, 프로토콜 스택에서의 "레이어", 프로토콜을 사용하여 통신하는 총 호스트 수가 표시됩니다.

애플리케이션 프로토콜 분류 섹션

Application Protocol Breakdown(애플리케이션 프로토콜 분류) 섹션에는 탐지된 호스트에서 현재 사용 중인 애플리케이션 프로토콜이 나열됩니다. 프로토콜 이름, 지난 시간 동안 애플리케이션 프로토콜을 실행하던 총 호스트 수, 특정 시점에 프로토콜을 실행하던 것으로 탐지된 총 호스트 수가 나열됩니다.

탐지된 프로토콜을 사용하는 서버에 대한 세부사항을 보는 데에도 Application Protocol Breakdown(애플리케이션 프로토콜 분류) 섹션을 사용할 수 있습니다.

관련 항목

서버 데이터, 950 페이지

OS 분류 섹션

OS Breakdown(OS 분류) 섹션에는 모니터링되는 네트워크에서 현재 실행 중인 운영 체제와 더불어 해당 공급업체 및 각 운영 체제를 실행 중인 총 호스트 수가 나열됩니다.

운영 체제 이름 및 버전에 사용되는 `unknown` 값은 해당 운영 체제 및 버전이 시스템의 핑거프린트와 일치하지 않음을 의미합니다. `pending` 값은 시스템이 운영 체제 및 버전을 식별하는 데 필요한 정보를 아직 충분히 수집하지 못했음을 의미합니다.

탐지된 운영 체제에 대한 세부사항을 보는 데에도 OS Breakdown(OS 분류) 섹션을 사용할 수 있습니다.

관련 항목

호스트 데이터, 937 페이지

검색 성능 그래프 보기

검색 이벤트와 함께 매니지드 디바이스에 대한 성능 통계를 표시하는 그래프를 생성할 수 있습니다.

새 데이터는 통계 그래프를 위해 5분마다 누적됩니다. 따라서 그래프를 빠르게 다시 로드하는 경우 다음 5분 증가분이 발생할 때까지 데이터가 변경되지 않을 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

애플리케이션 네트워크 검색 정책이 애플리케이션, 호스트, 사용자를 포함하도록 편집합니다. (이는 시스템 성능에 영향을 줄 수 있습니다.) 네트워크 검색 규칙 구성 및 작업 및 검색된 자산를 참조하십시오.

이 작업을 수행하려면 관리자 또는 유지보수 사용자여야 합니다.

프로시저

단계 **1** **Overview(**개요**)** > **Summary(**요약**)** > **Discovery Performance(**검색 성능**)**을(를) 선택합니다.

단계 **2** 포함할 management center 또는 매니지드 디바이스를 **Select Device(**디바이스 선택**)** 목록에서 선택합니다.

단계 **3** 검색 성능 그래프 유형, 926 페이지에 설명된 대로 **Select Graph(s)(**그래프 선택**)** 목록에서 생성할 그래프 유형을 선택합니다.

단계 **4** **Select Time Range(**시간 범위 선택**)** 목록에서 그래프에 사용할 시간 범위를 선택합니다.

단계 **5** 선택한 통계를 그래프로 표시하려면 **Graph(**그래프**)**를 클릭합니다.

검색 성능 그래프 유형

다음은 사용 가능한 그래프 유형에 대한 설명입니다.

Processed Events/Sec

Data Correlator가 초당 처리하는 이벤트 수를 나타내는 그래프를 표시합니다.

Processed Connections/Sec

Data Correlator가 초당 처리하는 연결 수를 나타내는 그래프를 표시합니다.

Generated Events/Sec

시스템이 초당 생성하는 이벤트 수를 나타내는 그래프를 표시합니다.

Mbits/Sec

초당 검색 프로세스에 의해 분석되는 트래픽의 메가비트 수를 나타내는 그래프를 표시합니다.

평균 바이트/패킷

검색 프로세스에 의해 분석되는 각 패킷에 포함된 평균 바이트 수를 나타내는 그래프를 표시합니다.

K Packets/Sec

초당 검색 프로세스에 의해 분석되는 패킷 수를 나타내는 그래프를 표시합니다(1,000 단위).

검색 및 ID 워크플로 사용

management center에서는 네트워크에 대해 생성되는 검색 및 ID 데이터 분석에 사용할 수 있는 이벤트 워크플로 집합을 제공합니다. 워크플로는 네트워크 맵과 더불어 네트워크 자산에 대한 핵심 정보 소스입니다.

management center에서는 검색 및 ID 데이터에 대한 사전 정의된 워크플로는 물론 탐지된 호스트와 호스트 속성, 서버, 애플리케이션, 애플리케이션 세부사항, 취약성, 사용자 활동, 사용자 등에 대한 사전 정의된 워크플로도 제공합니다. 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 사전 정의된 워크플로에 액세스하려면 다음을 수행합니다.

- 검색 및 호스트 입력 데이터 — 검색 및 호스트 입력 이벤트 보기, 935 페이지를 참조하십시오.
- 호스트 데이터 — 호스트 데이터 보기, 937 페이지를 참조하십시오.
- 호스트 속성 데이터 — 호스트 속성 보기, 944 페이지를 참조하십시오.
- 호스트 또는 사용자 보안 침해 지표 데이터 — 보안 침해 지표 데이터 보기 및 작업, 946 페이지를 참조하십시오.
- 서버 데이터 — 서버 데이터 보기, 951 페이지를 참조하십시오.
- 애플리케이션 데이터 — 애플리케이션 데이터 보기, 954 페이지를 참조하십시오.
- 애플리케이션 세부사항 데이터 — 애플리케이션 세부사항 데이터 보기, 957 페이지를 참조하십시오.
- 활성 세션 데이터 — 활성 세션 데이터 보기, 974 페이지를 참조하십시오.
- 사용자 데이터 — 사용자 데이터 보기, 977 페이지를 참조하십시오.
- 사용자 활동 데이터 — 사용자 활동 데이터 보기, 980 페이지를 참조하십시오.
- 네트워크 맵 — 네트워크 맵 보기, 631 페이지를 참조하십시오.

단계 **2** 맞춤형 워크플로에 액세스하려면 **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Workflows(**사용자 지정 워크플로**)**를 선택합니다.

단계 **3** 맞춤형 테이블에 기반한 워크플로에 액세스하려면 **Analysis(**분석**)** > **Advanced(**고급**)** > **Custom Tables(**사용자 지정 표**)**를 선택합니다.

단계 **4** 네트워크 검색 워크플로에서 액세스하는 모든 페이지에서 일반적으로 이루어지는 다음 작업을 수행합니다.

- 열 제한 — 표시되는 열을 제한하려면 숨기려는 열 머리글의 **Close(**닫기**)** (✕)을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 확인 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 확장 화살표를 클릭하여 검색 제약 조건을 확장한 다음, Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 삭제 — 현재 제한된 보기에서 일부 또는 모든 항목을 삭제하려면 삭제할 항목 옆의 확인란을 선택한 후 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다. 이러한 항목은 시스템의 검색 기능이 다시 시작될 때까지(이 경우 다시 탐지될 수도 있음) 삭제된 상태로 유지됩니다.

  주의 **Analysis(**분석**)** > **Users(**사용자**)** > **Active Sessions(**활동 세션**)** 페이지에서 non-VPN(비 VPN) 세션을 삭제하기 전에 해당 세션을 닫았는지 확인하십시오. 활성 세션을 삭제하면 해당 정책이 디바이스의 세션을 탐지할 수 없으므로, 이러한 작업을 수행하도록 정책을 구성한 경우에도 세션을 모니터링하거나 차단할 수 없습니다.

  참고 Analysis > Users > Active Sessions(분석 > 사용자 > 활성 세션) 페이지의 VPN 세션에 대한 자세한 내용은 원격 액세스 VPN 현재 사용자 보기를 참조하십시오.

  참고 Cisco(서드파티와 반대) 취약성은 삭제할 수 없습니다. 그러나 검토한 것으로 표시할 수는 있습니다.

- 드릴다운 — 워크플로에서 다음 페이지로 드릴다운하려면 드릴다운 페이지 사용, 697 페이지을 참조하십시오.
- 현재 페이지 이동 — 현재 워크플로 페이지 내에서 이동하려면 워크플로 페이지 탐색 툴, 694 페이지을 참조하십시오.
- 워크플로 내에서 이동 — 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 다른 워크플로로 이동 — 다른 이벤트 보기로 이동하여 관련 이벤트를 검토하려면 워크플로 간 탐색, 716 페이지을 참조하십시오.
- 데이터 정렬 — 워크플로의 데이터를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.
- 호스트 프로파일 보기 - IP 주소의 호스트 프로파일을 보려면 **Host Profile(**호스트 프로파일**)**을 클릭하거나 활성 IOC(Indication of Compromise) 태그가 있는 호스트의 경우에는 IP 주소 옆에 표시되는 **Compromised Host(**보안 침해된 호스트**)**를 클릭합니다.
- 사용자 프로파일 - 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘 또는 IOC와 연결된 사용자라면 **Red User(**빨간색 사용자**)**를 클릭합니다. 보기

관련 항목

워크플로 사용, 689 페이지

Management Center 데이터베이스에서 데이터 제거, 532 페이지

검색 및 호스트 입력 이벤트

시스템에서는 모니터링되는 네트워크 세그먼트의 변경 세부사항을 전달하는 검색 이벤트를 생성합니다. 새로 검색된 네트워크 기능에 대해서는 새 이벤트가 생성되고, 이전에 식별된 네트워크 자산의 변경 사항에 대해서는 변경 이벤트가 생성됩니다.

초기 네트워크 검색 단계에서 시스템은 각 호스트에 대해, 그리고 각 호스트에서 실행 중인 것으로 검색된 TCP 또는 UDP 서버에 대해 새 이벤트를 생성합니다. 원하는 경우, 내보낸 NetFlow 레코드를 사용하여 이러한 새 호스트 및 서버 이벤트를 생성하도록 시스템을 구성할 수 있습니다.

또한 시스템은 검색된 각 호스트에서 실행 중인 각 애플리케이션 프로토콜, 네트워크 및 전송에 대해 새 이벤트를 생성합니다. NetFlow 엑스포터를 모니터링하도록 구성된 검색 규칙에서는 애플리케이션 프로토콜 탐지를 비활성화할 수 있지만, 매니지드 디바이스를 모니터링하도록 구성된 검색 규칙에서는 비활성화할 수 없습니다. 비 NetFlow 검색 규칙에서 호스트 또는 사용자 검색을 비활성화하면 애플리케이션이 자동으로 검색됩니다.

초기 네트워크 매핑이 완료되면 시스템은 변경 이벤트를 생성하여 네트워크 변경 사항을 계속해서 기록합니다. 전에 검색된 자산의 구성이 변경될 때마다 변경 이벤트가 생성됩니다.

생성된 검색 이벤트는 데이터베이스에 로깅됩니다. management center 웹 인터페이스를 사용하여 검색 이벤트를 보고, 검색하고, 삭제할 수 있습니다. 상관관계 규칙에서도 검색 이벤트를 사용할 수 있습니다. 생성된 검색 이벤트 유형 및 지정한 다른 기준을 기반으로 상관관계 규칙을 작성할 수 있습니다. 상관관계 정책에서 사용할 경우 이러한 규칙은 네트워크 트래픽이 기준을 충족하면 교정과 syslog, SNMP, 이메일 알림 응답을 실행합니다.

호스트 입력 기능을 사용하여 네트워크 맵에 데이터를 추가할 수 있습니다. 운영 체제 정보를 추가, 수정 또는 삭제할 수 있으며, 이 경우 시스템은 해당 호스트에 대한 해당 정보의 업데이트를 중지합니다. 또한 애플리케이션 프로토콜, 클라이언트, 서버 및 호스트 속성을 수동으로 추가, 수정 또는 삭제하거나 취약성 정보를 수정할 수도 있습니다. 이렇게 하면 시스템은 호스트 입력 이벤트를 생성합니다.

검색 이벤트 유형

네트워크 검색 정책에서 시스템이 기록하는 검색 이벤트의 유형을 설정할 수 있습니다. 검색 이벤트 테이블을 볼 경우 **Event** 열에 이벤트 유형이 나열됩니다. 다음은 검색 이벤트 유형에 대한 설명입니다.

호스트에 대해 추가 **MAC** 탐지됨

시스템이 전에 검색된 호스트에 대해 새 MAC 주소를 탐지할 경우 이 이벤트가 생성됩니다.

시스템이 라우터를 통해 트래픽을 전달하는 호스트를 탐지할 경우 이 이벤트가 종종 생성됩니다. 각 호스트에는 서로 다른 IP 주소가 있지만, 모든 호스트는 라우터와 연결된 MAC 주소가 있는 것으로 표시됩니다. IP 주소와 연결된 실제 MAC 주소를 탐지할 경우 시스템은 호스트 프로파일 내에 MAC 주소를 굵은 텍스트로 표시하며, 이벤트 보기의 이벤트 설명 내에 "ARP/DHCP detected" 메시지를 표시합니다.

클라이언트 시간 초과

시스템이 비활성 상태를 이유로 클라이언트를 데이터베이스에서 삭제하면 이 이벤트가 생성됩니다.

클라이언트 업데이트

시스템이 HTTP 트래픽에서 페이로드(즉, 오디오, 비디오, 웹메일 등 특정 유형의 콘텐츠)를 탐지할 경우 이 이벤트가 생성됩니다.

DHCP: IP 주소 변경됨

DHCP 주소 할당 때문에 호스트 IP 주소가 변경된 것을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

DHCP: IP 주소 재할당

호스트가 IP 주소를 재사용할 경우, 즉 DHCP IP 주소 할당 때문에 호스트가 전에 다른 물리적 호스트에 사용되던 IP 주소를 얻는 경우 이 이벤트가 생성됩니다.

홉 변경

호스트 및 해당 호스트를 탐지하는 디바이스 간 다수의 네트워크 홉에서 시스템이 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다. 발생 조건은 다음과 같습니다.

- 디바이스가 여러 라우터를 통과하는 호스트 트래픽을 확인하고 호스트 위치에 대한 더 나은 결정을 내릴 수 있는 경우
- 디바이스가 호스트로부터 ARP 전송을 탐지하고 로컬 세그먼트에 호스트가 있음을 나타내는 경우

호스트 삭제됨**:** 호스트 한도 도달함

management center에서 호스트 제한이 초과되어 네트워크 맵에서 모니터링되는 호스트가 삭제될 경우 이 이벤트가 생성됩니다.

호스트 삭제됨**:** 호스트 한도 도달함

management center에서 호스트 제한에 도달하여 새 호스트가 삭제될 경우 이 이벤트가 생성됩니다. 이 이벤트를 호스트 제한에 도달할 경우 오래된 호스트가 네트워크 맵에서 삭제되는 이전 이벤트와 비교해보십시오.

호스트 제한에 도달할 경우 새 호스트를 삭제하려면 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)** > **Advanced(**고급**)**로 이동하여 **When Host Limit Reached(**호스트 제한 도달 시**)**를 **Drop hosts(**호스트 삭제**)**로 설정합니다.

호스트 **IOC** 설정

호스트에 대해 IOC(indication of compromise)가 설정되고 알림이 생성될 경우 이 이벤트가 발생합니다.

호스트 시간 초과

호스트가 네트워크 검색 정책에 정의된 간격 내에 트래픽을 생성하지 못했기 때문에 네트워크 맵에서 삭제될 경우 이 이벤트가 생성됩니다. 개별 호스트 IP 주소 및 MAC 주소는 개별적으로 시간 초과됩니다. 관련된 모든 주소가 시간 초과되기 전에는 호스트가 네트워크 맵에서 사라지지 않습니다.

네트워크 검색 정책에서 모니터링할 네트워크를 변경하는 경우, 호스트 제한에서 계산되지 않도록 네트워크 맵에서 오래된 호스트를 수동으로 삭제하고자 할 수 있습니다.

네트워크 디바이스로 호스트 유형 변경됨

탐지된 호스트가 실제로 네트워크 디바이스임을 시스템에서 확인할 경우 이 이벤트가 생성됩니다.

ID 충돌

서버 또는 운영체제에 대한 현재의 능동 ID와 충돌하는 새 서버 또는 운영체제 ID를 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

새로운 능동 ID 데이터를 얻기 위해 호스트를 다시 스캔하여 ID 충돌을 해결하려면 Nmap 교정을 트리거하는 Identity Conflict(ID 충돌) 이벤트를 사용할 수 있습니다.

ID 시간 초과

활성 소스의 서버 또는 운영체제 ID 데이터가 시간을 초과하면 이 이벤트가 생성됩니다.

새로운 능동 ID 데이터를 얻기 위해 호스트를 다시 스캔하여 ID 데이터를 새로 고치려면 Nmap 교정을 트리거하는 Identity Conflict(ID 충돌) 이벤트를 사용할 수 있습니다.

MAC 정보 변경

특정 MAC 주소 또는 TTL 값과 연결된 정보에서 시스템이 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

시스템이 라우터를 통해 트래픽을 전달하는 호스트를 탐지할 경우 이 이벤트가 종종 발생합니다. 각 호스트에는 서로 다른 IP 주소가 있지만, 모든 호스트는 라우터와 연결된 MAC 주소가 있는 것으로 표시됩니다. IP 주소와 연결된 실제 MAC 주소를 탐지할 경우 시스템은 호스트 프로파일 내에 MAC 주소를 굵은 텍스트로 표시하며, 이벤트 보기의 이벤트 설명 내에 "ARP/DHCP detected" 메시지를 표시합니다. 트래픽이 여러 라우터를 통과할 수 있으므로 TTL이 변경될 수 있습니다. 또는 시스템이 호스트의 실제 MAC 주소를 탐지하는 경우에도 TTL이 변경될 수 있습니다.

NETBIOS 이름 변경

시스템이 호스트 NetBIOS 이름의 변경을 탐지할 경우 이 이벤트가 생성됩니다. 이 이벤트는 NetBIOS 프로토콜을 사용하는 호스트에 대해서만 생성됩니다.

새 클라이언트

시스템이 새 클라이언트를 탐지할 경우 이 이벤트가 생성됩니다.

참고 분석용 클라이언트 데이터를 수집 및 저장하려면 네트워크 검색 정책의 검색 규칙에서 애플리케이션 탐지를 활성화하십시오.

새 호스트

시스템이 네트워크에서 실행 중인 새 호스트를 탐지할 경우 이 이벤트가 생성됩니다.

이 이벤트는 디바이스가 새 호스트와 관련된 NetFlow 데이터를 처리하는 경우에도 생성될 수 있습니다. 이 경우 이벤트를 생성하려면, NetFlow 데이터를 관리해 호스트를 검색하는 네트워크 검색 규칙을 설정해야 합니다.

새 네트워크 프로토콜

호스트가 새 네트워크 프로토콜(IP, ARP 등)과 통신 중임을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

새 **OS**

시스템이 호스트에 대한 새 운영체제를 탐지하거나 호스트 운영체제에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

새 **TCP** 포트

호스트에서 활성화된 새 TCP 서버 포트(예: SMTP 또는 웹 서비스에서 사용하는 포트)를 시스템이 탐지할 경우 이 이벤트가 생성됩니다. 이 이벤트는 애플리케이션 프로토콜 또는 이와 연결된 서버를 식별하는 데 사용되지 않습니다. 그러한 정보는 TCP Server Information Update(TCP 서버 정보 업데이트) 이벤트에서 전송됩니다.

또한 이 이벤트는 네트워크 맵에 존재하지 않는 모니터링되는 네트워크 상의 서버와 관련된 NetFlow 데이터를 디바이스가 처리할 때도 생성됩니다. 이 경우 이벤트를 생성하려면, NetFlow 데이터를 관리해 애플리케이션을 검색하는 네트워크 검색 규칙을 설정해야 합니다.

새 전송 프로토콜

호스트가 TCP, UDP 등의 새 네트워크 프로토콜과 통신 중임을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

새 **UDP** 포트

시스템이 호스트에서 실행 중인 새 UDP 서버 포트를 탐지할 경우 이 이벤트가 생성됩니다.

또한 이 이벤트는 네트워크 맵에 존재하지 않는 모니터링되는 네트워크 상의 서버와 관련된 NetFlow 데이터를 디바이스가 처리할 때도 생성됩니다. 이 경우 이벤트를 생성하려면, NetFlow 데이터를 관리해 애플리케이션을 검색하는 네트워크 검색 규칙을 설정해야 합니다.

TCP 포트 닫힘

시스템이 호스트에서 닫힌 TCP 포트를 탐지할 경우 이 이벤트가 생성됩니다.

TCP 포트 시간 초과

시스템이 네트워크 검색 정책에 정의된 간격 내에 TCP 포트로부터의 활동을 탐지하지 못한 경우 이 이벤트가 생성됩니다.

TCP 서버 정보 업데이트

시스템이 호스트에서 실행 중인 검색된 TCP 서버에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

TCP 서버가 업그레이드되는 경우에도 이 이벤트가 생성될 수 있습니다.

UDP 포트 닫힘

시스템이 호스트에서 닫힌 UDP 포트를 탐지할 경우 이 이벤트가 생성됩니다.

UDP 포트 시간 초과

시스템이 네트워크 검색 정책에 정의된 간격 내에 UDP 포트로부터의 활동을 탐지하지 못한 경우 이 이벤트가 생성됩니다.

UDP 서버 정보 업데이트

시스템이 호스트에서 실행 중인 검색된 UDP 서버에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

UDP 서버가 업그레이드되는 경우에도 이 이벤트가 생성될 수 있습니다.

VLAN 태그 정보 업데이트

시스템이 호스트에 속하는 VLAN 태그에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

관련 항목

호스트 입력 이벤트 유형, 933 페이지

호스트 입력 이벤트 유형

검색 이벤트의 테이블을 볼 경우 **Event** 열에 이벤트 유형이 나열됩니다.

사용자가 특정 작업(예: 수동으로 호스트 추가)을 수행할 때 생성되는 호스트 입력 이벤트를 시스템이 모니터링되는 네트워크에서 직접 변경 사항을 탐지(예: 전에 탐지되지 않던 호스트에서 트래픽 탐지)할 때 생성되는 검색 이벤트와 비교해보십시오.

네트워크 검색 정책을 수정하여, 시스템이 기록하는 호스트 입력 이벤트의 유형을 설정할 수 있습니다.

서로 다른 유형의 호스트 입력 이벤트가 제공하는 정보를 이해하면 어떤 이벤트를 기록하고 알림을 전송할지, 상관관계 정책에서 이러한 알림을 어떻게 사용할지를 좀 더 효과적으로 결정할 수 있습니다. 또한 이벤트 유형의 이름을 알면 좀 더 효과적으로 이벤트를 검색할 수 있습니다. 다음은 서로 다른 유형의 호스트 입력 이벤트에 대한 설명입니다.

클라이언트 추가

사용자가 클라이언트를 추가할 경우 이 이벤트가 생성됩니다.

호스트 추가

사용자가 호스트를 추가할 경우 이 이벤트가 생성됩니다.

프로토콜 추가

사용자가 프로토콜을 추가할 경우 이 이벤트가 생성됩니다.

스캔 결과 추가

시스템이 Nmap 스캔의 결과를 호스트에 추가할 경우 이 이벤트가 생성됩니다.

포트 추가

사용자가 서버 포트를 추가할 경우 이 이벤트가 생성됩니다.

클라이언트 삭제

사용자가 시스템에서 클라이언트를 삭제할 경우 이 이벤트가 생성됩니다.

호스트/네트워크 삭제

사용자가 시스템에서 IP 주소 또는 서브넷을 삭제할 경우 이 이벤트가 생성됩니다.

프로토콜 삭제

사용자가 시스템에서 프로토콜을 삭제할 경우 이 이벤트가 생성됩니다.

포트 삭제

사용자가 시스템에서 서버 포트 또는 서버 포트 그룹을 삭제할 경우 이 이벤트가 생성됩니다.

호스트 특성 추가

사용자가 새 호스트 속성을 생성할 경우 이 이벤트가 생성됩니다.

호스트 특성 삭제

사용자가 사용자 정의 호스트 속성을 삭제할 경우 이 이벤트가 생성됩니다.

호스트 특성 삭제 값

사용자가 호스트 속성에 할당된 값을 삭제할 경우 이 이벤트가 생성됩니다.

호스트 특성 설정 값

사용자가 호스트에 대한 호스트 속성 값을 설정할 경우 이 이벤트가 생성됩니다.

호스트 특성 업데이트

사용자가 사용자 정의 호스트 속성의 정의를 변경할 경우 이 이벤트가 생성됩니다.

호스트 중요도 설정

사용자가 호스트에 대한 호스트 중요도 값을 설정 또는 수정할 경우 이 이벤트가 생성됩니다.

운영 시스템 정의 설정

사용자가 호스트에 대한 운영체제를 설정할 경우 이 이벤트가 생성됩니다.

서버 정의 설정

사용자가 서버에 대한 벤더 및 버전 정의를 설정할 경우 이 이벤트가 생성됩니다.

취약성 영향 자격 설정

취약성 영향 자격이 설정될 경우 이 이벤트가 생성됩니다.

영향 자격에 대해 사용 중인 취약성이 전역 레벨에서 비활성화되거나 전역 레벨에서 취약성이 활성화될 경우 이 이벤트가 생성됩니다.

취약성 설정 유효하지 않음

사용자가 취약성을 무효화 또는 검토할 경우 이 이벤트가 생성됩니다.

취약성 설정 유효함

전에 잘못된 것으로 표시되었던 취약성을 사용자가 검증할 경우 이 이벤트가 생성됩니다.

관련 항목

검색 이벤트 유형, 929 페이지

검색 및 호스트 입력 이벤트 보기

검색 이벤트 워크플로를 사용하면 검색 이벤트와 호스트 입력 이벤트에서 데이터를 볼 수 있습니다. 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 검색 이벤트의 테이블 보기 및 호스트 보기 종료 페이지를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Hosts(**호스트**)** > **Discovery Events(**검색 이벤트**)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 타임 윈도우 변경, 710 페이지에 설명된 대로 시간 범위를 조정합니다.

  참고 어플라이언스의 구성된 타임 윈도우(전역 또는 이벤트 전용 모두 해당)를 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**(워크플로 전환)를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(검색 이벤트 필드, 936 페이지 참조).

관련 항목

검색 및 ID 워크플로 사용, 927 페이지

검색 이벤트 필드

다음은 검색 이벤트 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

시간

시스템이 이벤트를 생성한 시간

이벤트

검색 이벤트 유형 또는 호스트 입력 이벤트 유형.

IP 주소

이벤트와 관련된 호스트와 연결된 IP 주소

사용자

이벤트가 생성되기 전 이벤트와 관련된 호스트에 로그인한 마지막 사용자. 권한 있는 사용자 이후 권한 없는 사용자만 로그인한 경우, 권한 있는 사용자가 호스트에 대한 현재 사용자로 유지됩니다(또 다른 권한 있는 사용자가 로그인하지 않는 한).

MAC 주소

검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 주소. 이 MAC 주소는 이벤트와 관련된 호스트의 실제 MAC 주소일 수도 있고, 트래픽이 통과한 네트워크 디바이스의 MAC 주소일 수도 있습니다.

MAC Vendor(MAC 벤더**)**

검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 하드웨어 공급업체

이 필드를 검색할 경우 **virtual_mac_vendor**를 입력하여 가상 호스트와 관련된 이벤트와 일치시킵니다.

포트

이벤트를 트리거한 트래픽에서 사용하는 포트(해당되는 경우)

설명

이벤트의 텍스트 설명

도메인

호스트를 검색한 디바이스의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Device(디바이스)

이벤트를 생성한 매니지드 디바이스의 이름입니다. NetFlow 데이터를 기반으로 하는 새 호스트 및 새 서버 이벤트의 경우 이것이 해당 데이터를 처리한 매니지드 디바이스입니다.

관련 항목

이벤트 검색, 721 페이지

호스트 데이터

시스템은 호스트를 탐지하고 관련 정보를 수집하여 호스트 프로파일을 작성할 때 이벤트를 생성합니다. management center 웹 인터페이스를 사용하여 호스트를 보고, 검색하고, 삭제할 수 있습니다.

호스트를 보는 동안 선택한 호스트를 기반으로 트래픽 프로필 및 규정 준수 허용 목록을 생성할 수 있습니다. 또한 호스트 중요도 값(비즈니스 중요도를 지정)을 비롯한 호스트 속성을 호스트 그룹에 할당할 수 있습니다. 그런 다음 상관관계 규칙 및 정책 내에서 이러한 중요도 값, 허용 목록 및 트래픽 프로필을 사용할 수 있습니다.

시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

호스트 데이터 보기

management center를 사용하면 시스템에서 탐지한 호스트의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

호스트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 미리 정의된 두 워크플로는 사용자의 제한 사항을 충족하는 모든 호스트에 대한 호스트 프로파일이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 호스트 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Hosts(호스트)**를 선택합니다.
- 호스트의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Hosts(호스트)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(호스트 데이터 필드, 938 페이지 참조).
- 옵션을 보려면 테이블에서 항목을 마우스 오른쪽 버튼으로 클릭합니다. (옵션을 제공하지 않는 열도 있습니다.)
- 특정 호스트에 호스트 속성을 할당합니다(선택한 호스트에 대해 호스트 속성 설정, 945 페이지 참조).
- 특정 호스트에 대한 트래픽 프로파일을 생성합니다(선택한 호스트에 대한 트래픽 프로파일 생성, 942 페이지 참조).
- 특정 호스트를 기반으로 컴플라이언스 허용 목록을 생성합니다(선택한 호스트를 기반으로 컴플라이언스 허용 목록 생성, 943 페이지 참조).

호스트 데이터 필드

시스템은 호스트를 검색하면 해당 호스트에 대한 데이터를 수집합니다. 여기에는 호스트의 IP 주소, 실행 중인 운영 체제 등이 포함될 수 있습니다. 그러한 정보 중 일부는 호스트의 테이블 보기에서 볼 수 있습니다.

다음은 호스트 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Last Seen(최종 확인**)**

시스템에서 마지막으로 탐지한 호스트 IP 주소 중 하나의 날짜 및 시간. Last Seen(최종 확인) 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 호스트 IP 주소 중 하나에 대해 새 호스트 이벤트를 생성할 때 업데이트됩니다.

호스트 입력 기능을 사용하여 업데이트된 운영 체제 데이터가 있는 호스트의 경우 Last Seen(최종 확인) 값은 데이터가 원래 추가된 날짜 및 시간을 나타냅니다.

IP Address(IP 주소**)**

호스트와 연결된 IP 주소

MAC 주소

호스트에서 탐지한 NIC의 MAC 주소.

MAC Address 필드는 호스트 워크플로에서 찾을 수 있는 호스트의 테이블 보기에 나타납니다. MAC Address 필드를 다음에도 추가할 수 있습니다.

- 호스트 테이블의 필드를 포함하는 사용자 지정 테이블
- 호스트 테이블 기반의 사용자 지정 워크플로에 있는 드릴다운 페이지

MAC Vendor(MAC 벤더)

호스트에서 탐지한 NIC의 MAC 하드웨어 공급업체.

MAC Vendor 필드는 호스트 워크플로에서 찾을 수 있는 호스트의 테이블 보기에 나타납니다. MAC Vendor 필드를 다음에도 추가할 수 있습니다.

- 호스트 테이블의 필드를 포함하는 사용자 지정 테이블
- 호스트 테이블 기반의 사용자 지정 워크플로에 있는 드릴다운 페이지

이 필드를 검색할 경우 `virtual_mac_vendor`를 입력하여 가상 호스트와 관련된 이벤트와 일치시킵니다.

Current User(현재 사용자)

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

호스트 중요도

호스트에 할당된 사용자 지정 중요도 값.

NetBIOS 이름

호스트의 NetBIOS 이름. NetBIOS 프로토콜을 실행하는 호스트만이 NetBIOS 이름을 가질 수 있습니다.

VLAN ID

호스트에서 사용하는 VLAN ID.

Hops(홉)

호스트를 탐지한 디바이스에서 호스트로의 네트워크 홉 수

호스트 유형

호스트의 유형. 호스트, 모바일 디바이스, 탈옥 모바일 디바이스, 라우터, 브리지, NAT 디바이스 및 로드 밸런서 중 어떤 것이든 가능합니다.

시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.
- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.

네트워크 디바이스로 식별되지 않는 디바이스는 호스트로 분류됩니다.

이 필드를 검색할 경우 `!host`를 입력하여 모든 네트워크 디바이스를 검색합니다.

Hardware(하드웨어**)**

모바일 디바이스용 하드웨어 플랫폼.

OS

다음 중 하나에 해당합니다.

- 호스트에서 탐지되거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제(이름, 벤더 및 버전)
- `unknown` - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- `pending` - 시스템이 운영체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 ID를 탐지하면 쉼표로 구분된 목록으로 표시합니다.

대시보드의 Custom Analysis 위젯에서 호스트 이벤트 보기를 호출할 경우 이 필드가 나타납니다. 이것은 또한 호스트 테이블 기반의 사용자 지정 테이블에 있는 필드 옵션이기도 합니다.

이 필드를 검색할 경우 `n/a`를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

OS Conflict(OS 컨플릭트**)**

이 필드는 검색 전용입니다.

OS 벤더

다음 중 하나에 해당합니다.

- 호스트에서 탐지되었거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제의 벤더

- unknown - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- pending - 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 벤더를 탐지하면 쉼표로 구분된 목록으로 표시합니다.

이 필드를 검색할 경우 n/a를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

OS 이름

다음 중 하나에 해당합니다.

- 호스트에서 탐지되거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제
- unknown - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- pending - 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 이름을 탐지하면 쉼표로 구분된 목록으로 표시합니다.

이 필드를 검색할 경우 n/a를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

OS 버전

다음 중 하나에 해당합니다.

- 호스트에서 탐지되었거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제
- unknown - 운영 체제가 알려진 핑거프린트와 일치하지 않는 경우
- pending - 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못한 경우

시스템에서는 여러 버전을 탐지하면 쉼표로 구분된 목록으로 표시합니다.

이 필드를 검색할 경우 n/a를 입력하여 운영 체제가 아직 식별되지 않은 호스트를 포함합니다.

Source Type(소스 유형**)**

호스트의 운영 체제 ID를 설정하는 데 사용되는 소스의 유형입니다.

- 사용자: user_name
- 애플리케이션: app_name
- 스캐너: scanner_type(네트워크 검색 구성을 통해 추가된 Nmap 또는 스캐너)
- 시스템에서 탐지한 운영 체제용 Firepower

시스템에서는 운영 체제의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다.

신뢰

다음 중 하나에 해당합니다.

- 호스트에서 실행 중인 운영 체제의 ID에 대한 시스템의 신뢰도 비율 - 시스템에서 탐지한 호스트

- 100% - 호스트 입력 기능 또는 Nmap 스캐너 등 활성 소스에 의해 식별된 운영 체제
- `unknown` - 시스템이 운영 체제 ID를 확인할 수 없는 호스트 및 NetFlow 데이터를 기반으로 네트워크 맵에 추가된 호스트

이 필드를 검색할 경우 `n/a`를 입력하여 NetFlow 데이터에 기반한 네트워크 맵에 추가된 호스트를 포함합니다.

Notes(참고)

Notes 호스트 속성의 사용자 정의 내용.

도메인

호스트와 연결된 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Device(디바이스)

트래픽을 탐지한 매니지드 디바이스를 입력하거나, NetFlow 또는 호스트 입력 데이터를 처리한 디바이스를 입력합니다.

이 필드가 비어 있는 경우, 다음 조건 중 하나가 사실에 해당합니다.

- 네트워크 검색 정책에 정의된 대로, 호스트 상주 네트워크를 명시적으로 모니터링하지 않는 디바이스에 의해 호스트가 네트워크 맵에 추가되었습니다.
- 호스트가 호스트 입력 기능으로 추가되었으며 시스템에 의해 탐지되지 않았습니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 이 필드가 나타납니다.

관련 항목

이벤트 검색, 721 페이지
운영 체제 ID 충돌, 901 페이지

선택한 호스트에 대한 트래픽 프로파일 생성

트래픽 프로파일은 네트워크의 트래픽 프로파일로, 지정한 기간에 수집된 연결 데이터를 기반으로 합니다. 트래픽 프로파일을 생성한 후에는 프로파일을 기준으로 새 트래픽을 평가하여, 정상적인 것처럼 보일 수 있는 비정상적인 네트워크 트래픽을 탐지할 수 있습니다.

지정한 호스트 그룹에 대한 트래픽 프로파일을 생성하려면 Hosts 페이지를 사용할 수 있습니다. 트래픽 프로파일은 지정한 호스트 중 하나가 호스트를 시작하는 것으로 탐지된 연결을 기반으로 합니다. 프로파일을 생성하고자 하는 호스트를 격리하려면 정렬 또는 검색 기능을 사용할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** 호스트 워크플로의 테이블 보기에서 트래픽 프로파일을 생성하려는 호스트 옆에 있는 확인란을 선택합니다.

단계 **2** 페이지의 하단에서 **Create Traffic Profile(**트래픽 프로파일 생성**)**을 클릭합니다.

단계 **3** 특정 요구에 맞게 트래픽 프로파일을 수정 및 저장합니다.

관련 항목

트래픽 프로파일 소개, 1057 페이지

선택한 호스트를 기반으로 컴플라이언스 허용 목록 생성

규정준수 허용리스트를 사용하면 네트워크에서 허용한 운영체제와 클라이언트, 네트워크, 전송 또는 애플리케이션 프로토콜을 지정할 수 있습니다.

지정한 호스트 그룹의 호스트 프로파일을 기반으로 규정준수 허용리스트를 생성하려면 Hosts(호스트) 페이지를 사용하면 됩니다. 허용리스트를 생성하고자 사용하려는 호스트를 격리하려면 정렬 또는 검색 기능을 사용할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** 호스트 워크플로우의 테이블 보기에서 허용리스트를 생성하려는 호스트 옆에 있는 확인란을 선택합니다.

단계 **2** 페이지의 하단에서 **Create(**생성**)**허용 목록를 클릭합니다.

단계 **3** 특정 요구에 맞게 허용리스트를 수정 및 저장합니다.

관련 항목

컴플라이언스 허용 목록 소개, 999 페이지

호스트 속성 데이터

Firepower System은 탐지한 호스트에 대한 정보를 수집하고 이 정보를 사용하여 호스트 프로파일을 작성합니다. 그러나 분석가에게 제공하고자 하는, 네트워크의 호스트에 대한 추가 정보가 있을 수 있습니다. 호스트 프로파일에 메모를 추가하거나, 호스트의 비즈니스 중요도를 설정하거나, 선택한 다른 정보를 제공할 수 있습니다. 이러한 각각의 정보를 호스트 속성이라고 합니다.

호스트 프로파일 자격에 호스트 속성을 사용할 수 있습니다. 이러한 속성은 트래픽 프로파일 작성 중에 수집하는 데이터를 제한하며, 상관관계 규칙을 트리거할 조건을 제한할 수도 있습니다. 상관관계 규칙에 대한 응답에 속성 값을 설정할 수도 있습니다.

관련 항목

호스트 속성 보기, 944 페이지
세트 속성값 교정 구성, 1081 페이지

호스트 속성 보기

management center를 사용하면 시스템에서 탐지한 호스트의 테이블을 호스트 속성과 함께 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

호스트 속성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 호스트 및 해당 속성을 나열하는 호스트 속성의 테이블 보기를 포함하며, 제약 조건에 맞는 모든 호스트에 대한 호스트 프로파일이 포함된 호스트 보기 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 호스트 속성 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Host Attributes(호스트 속성)**를 선택합니다.
- 호스트 속성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(워크플로 전환)**를 클릭한 다음 **Attributes(속성)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(워크플로 전환)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(호스트 속성 데이터 필드, 944 페이지 참조).
- 특정 호스트에 호스트 속성을 할당합니다(선택한 호스트에 대해 호스트 속성 설정, 945 페이지 참조).

호스트 속성 데이터 필드

MAC 주소에 의해서만 식별되는 호스트는 속성 테이블에 표시되지 않습니다.

다음은 호스트 속성 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

IP Address(IP 주소)

호스트와 연결된 IP 주소

Current User(현재 사용자**)**

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

호스트 중요도

엔터프라이즈에 사용자가 할당하는 호스트의 중요도. 정책 위반 및 응답을 이벤트와 관련된 호스트의 중요도에 맞추려면 상관관계 규칙 및 정책에 호스트 중요도를 사용할 수 있습니다. Low, Medium, High 또는 None의 호스트 중요도를 할당할 수 있습니다.

Notes(참고**)**

다른 분석가에게 보여줄 호스트에 대한 정보.

임의의 사용자 정의 호스트 속성, 컴플라이언스 허용 목록 대상 포함

사용자 정의 호스트 속성의 값. 호스트 속성 테이블에는 각 사용자 정의 호스트 속성에 대한 필드가 포함되어 있습니다.

도메인

호스트와 연결된 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

관련 항목

이벤트 검색, 721 페이지

선택한 호스트에 대해 호스트 속성 설정

호스트 워크플로에서 사전 정의된 호스트 속성 및 사용자 정의 호스트 속성을 구성할 수 있습니다.

프로시저

단계 **1** 호스트 워크플로에서 호스트 속성을 추가하려는 호스트의 옆에 있는 확인란을 선택합니다.

팁 정렬 및 검색 기능을 사용하여, 특정 속성을 할당할 호스트를 격리합니다.

단계 **2** 페이지의 하단에서 **Set Attributes(**속성 설정**)**를 클릭합니다.

단계 **3** 선택적으로, 선택한 호스트의 호스트 중요도를 설정합니다. **None(**없음**)**, **Low(**낮음**)**, **Medium(**중간**)** 또는 **High(**높음**)**를 선택할 수 있습니다.

단계 **4** 필요한 경우, 텍스트 상자에서 선택한 호스트의 호스트 프로파일에 메모를 추가합니다.

단계 **5** 선택적으로, 이미 구성한 사용자 정의 호스트 속성을 설정합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

보안 침해 지표 데이터

시스템은 다양한 유형의 데이터(침입 이벤트, 보안 인텔리전스, 연결 이벤트, 파일 또는 악성코드 이벤트)를 상호 연결하여 모니터링되는 네트워크의 호스트가 악의적인 수단에 의해 보안이 침해될 가능성이 있는지를 확인합니다. 이벤트 데이터의 특정 조합 및 빈도는 영향받는 호스트에서 IOC(보안 침해 지표) 태그를 트리거합니다.이러한 호스트의 IP 주소는 이벤트 보기에서 빨간색의 보안 침해된 호스트 아이콘으로 표시됩니다.

보안 침해 가능성이 있는 호스트가 식별되면 해당 보안 침해에 연결된 사용자에게도 태그가 지정됩니다. 이러한 사용자는 이벤트 보기에서 빨간색 사용자 아이콘으로 표시됩니다.

악성코드가 포함된 파일이 IOC로 태그가 지정된 지 300초 내에 다시 발견되는 경우, 또 다른 IOC가 생성되지 않습니다. 동일한 파일이 300초 이상 지나 발견되는 경우에는 새 IOC가 생성됩니다.

보안 침해 지표로 이벤트에 태그를 지정하도록 시스템을 구성하려면 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 침해 지표 규칙 활성화를 참조하십시오.

관련 항목

서버 ID 수정, 905 페이지

보안 침해 지표 데이터 보기 및 작업

management center을 사용하여 IOC가 표시된 테이블을 볼 수 있습니다. 찾고 있는 정보에 따라 이벤트 보기를 조작합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

사용하는 워크플로에 따라 표시되는 페이지가 달라집니다. 제약 조건을 충족하는 모든 호스트 또는 사용자의 호스트 또는 사용자 프로파일이 포함된 프로파일 보기에서 사전 정의된 IOC 워크플로가 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

시작하기 전에

- 시스템에서 보안 침해 지표(Indications of compromise, IOC)를 탐지하고 태깅하려면 네트워크 검색 정책에서 IOC 기능을 활성화하고 하나 이상의 IOC 규칙을 활성화해야 합니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 침해 지표 규칙 활성화를 참조하십시오.
- 활성 ID 정책에서 사용자를 식별해야 합니다.

프로시저

단계 **1** 웹 인터페이스의 어느 위치가 요구 사항을 충족하는 정보를 제공하는지 확인합니다.

다음 위치를 사용하여 보안 침해 지표 데이터를 보거나 보안 침해 데이터 작업을 할 수 있습니다.

- 이벤트 뷰어(분석 메뉴 아래) - 연결, 보안 인텔리전스, 침입, 악성코드, IOC 검색 이벤트 보기는 이벤트가 IOC를 트리거했는지 여부를 나타냅니다. IOC 규칙을 트리거한 Secure Endpoint에 의해 생성된 악성코드 이벤트는 이벤트 유형 `AMP IOC`를 가지며, 보안 침해를 지정하는 이벤트 하위 유형과 함께 표시됩니다.
- 대시보드 - 대시보드에서는 Summary Dashboard(요약 대시보드)의 Threats(위협)에 호스트 및 사용자별 IOC 태그가 기본적으로 표시됩니다. Custom Analysis 위젯은 IOC 데이터를 기반으로 하는 사전 설정을 제공합니다.
- Context Explorer - Context Explorer의 Indications of Compromise(보안 침해 지표) 섹션에는 IOC 카테고리별 호스트의 그래프 및 호스트별 IOC 카테고리의 그래프가 표시됩니다.
- 네트워크 맵 페이지 - Analysis(분석) > Hosts(호스트) > Network Map(네트워크 맵) 아래의 Indications of Compromise(보안 침해 지표)는 보안 침해 유형과 IP 주소에 따라 보안 침해 가능성이 있는 네트워크의 호스트를 그룹화합니다.
- 네트워크 파일 분석 경로 세부 정보 페이지 - Analysis(분석) > Files(파일) > Network File Trajectory(네트워크 파일 분석 경로) 아래 나열된 파일 세부 정보 페이지를 사용하여 네트워크에서 보안 침해 지표를 추적할 수 있습니다.
- 호스트 보안 침해 지표 페이지 - Analysis(분석) > Hosts(호스트) 메뉴 아래의 Host Indications of Compromise(호스트 보안 침해 지표) 페이지에는 IOC 태그에 따라 그룹화된 모니터링되는 호스트가 나열됩니다. 이 페이지의 워크플로를 사용하여 데이터로 드릴다운합니다.
- 사용자 보안 침해 지표 페이지 - Analysis(분석) > Users(사용자) 메뉴 아래의 User Indications of Compromise(사용자 보안 침해 지표) 페이지에는 IOC 태그에 따라 그룹화된 잠재적 IOC 이벤트에 연결된 사용자가 나열됩니다. 이 페이지의 워크플로를 사용하여 데이터로 드릴다운합니다.
- 호스트 프로파일 페이지 - 보안 침해 가능성이 있는 호스트의 호스트 프로파일에는 해당 호스트에 연결된 모든 IOC 태그가 표시되며, 이를 사용하여 IOC 태그를 확인하고 IOC 규칙 상태를 구성할 수 있습니다.
- 사용자 프로파일 페이지 - 잠재적 IOC 이벤트에 연결된 사용자의 사용자 프로파일에는 해당 사용자에 연결된 모든 IOC 태그가 표시되며, 이를 사용하여 IOC 태그를 확인하고 IOC 규칙 상태를 구성할 수 있습니다. (management center 웹 인터페이스에서는 사용자 프로파일에 "User Identity" 레이블이 지정됩니다.)

단계 **2** 해당하는 경우 다음 중 하나를 수행하고 이 절차의 나머지 단계를 사용합니다.

옵션	설명
호스트에서 IOC를 조사하려면 다음을 수행합니다.	• 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Indications of Compromise(**보안 침해 지표**)**를 선택합니다.

옵션	설명
	• 호스트 IOC 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Host Indications of Compromise(**호스트 보안 침해 지표**)**를 선택합니다.
사용자와 관련된 IOC를 조사하려면 다음을 수행합니다.	• 사전 정의된 워크플로를 사용 중인 경우 **Analysis > Users > Indications of Compromise(**분석 > 사용자 > 보안 침해 지표**)**를 선택합니다. • 사용자 IOC 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **User Indications of Compromise(**사용자 보안 침해 지표**)**를 선택합니다.

단계 **3** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(보안 침해 지표 데이터 필드, 948 페이지 참조).
- Host Indications of Compromise(호스트 보안 침해 지표) 페이지에서: **IP Address(IP** 주소**)** 열의 **Compromised Host(**보안 침해된 호스트**)**를 클릭하여 보안 침해된 호스트의 호스트 프로파일을 봅니다.
- User Indications of Compromise(사용자 보안 침해 지표) 페이지에서: **User(**사용자**)** 열의 빨간색 사용자를 클릭하여 보안 침해와 관련된 사용자 프로파일을 봅니다.
- 목록에 더 이상 나타나지 않도록 IOC 이벤트를 확인된 것으로 표시합니다. 이렇게 하려면 수정할 IOC 이벤트 옆에 있는 확인란을 선택한 다음 **Mark Resolved(**확인된 것으로 표시**)**를 클릭합니다.
- **First Seen(**처음 확인 날짜**)** 또는 **Last Seen(**마지막 확인 날짜**)** 열에서 **View(**보기**)** ( )을 클릭하여 IOC를 트리거한 이벤트의 세부사항을 봅니다.
- 더 많은 옵션 보기: 테이블의 값을 마우스 오른쪽 단추로 클릭합니다.

보안 침해 지표 데이터 필드

다음은 호스트 또는 사용자 보안 침해 지표(Indications of compromise, IOC) 테이블의 필드입니다. 모든 IOC 관련 테이블에 전체 필드가 포함되어 있지는 않습니다.

IP Address(IP 주소**)(**호스트 **IOC** 데이터를 볼 경우**)**

IOC를 트리거한 호스트와 연결된 IP 주소.

User(사용자**)(**사용자 **IOC** 데이터를 볼 경우**)**

IOC를 트리거한 이벤트와 연결된 사용자의 사용자 이름, 영역, 인증 소스.

카테고리

표시된 감염 유형에 대한 짧은 설명(예: `Malware Executed` 또는 `Impact 1 Attack`).

이벤트 유형

특정 IOC와 연결된 식별자로, 이를 트리거한 이벤트를 가리킴.

설명

침해 가능성이 있는 호스트에 미치는 영향에 대한 설명(예: `This host may be under remote control`(이 호스트가 원격 제어 상태일 수 있습니다) 또는 `Malware has been executed on this host`(이 호스트에서 악성코드가 실행되었습니다)).

First Seen/Last Seen(최초 확인**/**최종 확인**)**

IOC를 트리거하는 이벤트가 발생한 최초의/가장 최근의 날짜 및 시간.

도메인

IOC를 트리거한 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

관련 항목

이벤트 검색, 721 페이지

단일 호스트 또는 사용자에 대한 보안 침해 지표 규칙 상태 수정

네트워크 검색 정책에서 활성화된 경우 보안 침해 지표 규칙은 모니터링되는 네트워크의 모든 호스트 및 해당 네트워크의 IOC 이벤트와 연결된 권한 있는 사용자에게 적용됩니다. 개별 호스트 또는 사용자에 대한 규칙을 비활성화하여 유용하지 않은 IOC 태그를 방지할 수 있습니다(예: DNS 서버에 IOC 태그를 표시하지 않으려는 경우). 적용 가능한 네트워크 검색 정책에서 규칙이 비활성화된 경우, 특정 호스트 또는 사용자에 대해 해당 규칙을 활성화할 수 없습니다. 특정 호스트에 대한 규칙을 비활성화할 경우 동일한 이벤트에 관련된 사용자에 대한 태깅에는 영향을 미치지 않으며, 그 반대의 경우에도 마찬가지입니다.

프로시저

단계 **1** 호스트 또는 사용자 프로파일의 **Indications of Compromise(**보안 침해 지표**)** 섹션으로 이동합니다.

단계 **2** **Edit Rule States(**규칙 상태 수정**)**를 클릭합니다.

단계 **3** 규칙의 **Enabled** 열에서 슬라이더를 클릭하여 규칙을 활성화 또는 비활성화합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

보안 침해 지표 태그의 소스 이벤트 보기

호스트 프로 파일 및 사용자 프로 파일의 보안 침해 지표 섹션을 사용 하 여 IOC 태그를 트리거한 이벤트를 빠르게 이동할 수 있습니다. 이러한 이벤트를 분석하면 보안 침해 위협을 해결하기 위해 조치가 필요한지 및 필요한 조치를 결정하는 데 필요한 정보를 얻을 수 있습니다.

IOC 태그의 타임스탬프 옆에 있는 **View(**보기**)** ( )을 클릭하면 IOC 태그를 트리거한 이벤트만 표시하도록 제한된, 관련 이벤트 유형에 대한 이벤트의 테이블 보기로 이동합니다.

사용자 IOC의 첫 번째 인스턴스만 management center에 표시됩니다. 후속 인스턴스는 DNS 서버에 의해 포착됩니다."

프로시저

단계 **1** 호스트 또는 사용자 프로파일에서 **Indications of Compromise(**보안 침해 지표**)** 섹션으로 이동합니다.

단계 **2** 조사하려는 IOC 태그의 **First Seen** 또는 **Last Seen** 열에서 **View(**보기**)** ( )을 클릭합니다.

보안 침해 지표 태그 해결

보안 침해 지표(IOC) 태그에 의해 표시된 위협을 분석 및 해결했거나 IOC 태그가 오탐인 것으로 확인되는 경우, 이벤트를 해결된 것으로 표시할 수 있습니다. 해결된 것으로 표시된 이벤트는 호스트 프로파일 및 사용자 프로파일에서 제거됩니다. 프로파일의 활성 IOC 태그가 모두 해결되면 보안 침해된 호스트 또는 사용자가 보안 침해와 관련되었다는 빨간색 사용자 아이콘이 더 이상 나타나지 않습니다. 해결된 IOC에 대해 여전히 IOC 트리거링 이벤트가 표시될 수 있습니다.

IOC 태그를 트리거한 이벤트가 반복되는 경우, 호스트 또는 사용자에 대해 IOC 규칙을 비활성화하지 않았다면 태그가 다시 설정됩니다.

프로시저

단계 **1** 호스트 또는 사용자 프로파일에서 **Indications of Compromise(**보안 침해 지표**)** 섹션으로 이동합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 개별 IOC 태그를 해결된 것으로 표시하려면 해결하려는 태그의 오른쪽에 있는 **Delete(**삭제**)** ( ) 을 클릭합니다.
- 프로파일의 모든 IOC 태그를 해결된 것으로 표시하려면 **Mark All Resolved(**모두 해결된 것으로 표시**)**를 클릭합니다.

서버 데이터

시스템은 모니터링되는 네트워크 세그먼트의 호스트에서 실행 중인 모든 서버에 대한 정보를 수집합니다. 이 정보에는 다음이 포함됩니다.

- 서버 이름
- 서버가 사용하는 애플리케이션 및 네트워크 프로토콜
- 서버 공급업체 및 버전
- 서버를 실행하는 호스트와 연결된 IP 주소.
- 서버 통신 포트

시스템은 서버를 탐지하면 연결된 호스트가 이미 최대 서버 수에 도달하지 않은 경우 검색 이벤트를 생성합니다. management center 웹 인터페이스를 사용하여 서버 이벤트를 보고, 검색하고, 삭제할 수 있습니다.

상관관계 규칙의 기반을 서버 이벤트에 둘 수도 있습니다. 예를 들어, 시스템이 호스트 중 하나에서 실행 중인 채팅 서버(예: ircd)를 검색할 경우 상관관계 규칙을 트리거할 수 있습니다.

시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

서버 데이터 보기

management center를 사용하면 탐지한 서버의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

서버에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 모든 사전 정의 워크플로는 제약 조건을 충족하는 모든 호스트에 대한 호스트 프로파일이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 서버 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Servers(서버)**를 선택합니다.
- 서버의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Servers(서버)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(서버 데이터 필드, 952 페이지 참조).
- 수정할 서버에 대한 이벤트 옆에 있는 확인란을 선택한 다음 **Set Server Identity(서버 ID 설정)**를 클릭합니다.

- 옵션을 보려면 테이블에서 항목을 마우스 오른쪽 버튼으로 클릭합니다. (옵션을 제공하지 않는 열도 있습니다.)

서버 데이터 필드

다음은 서버에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Last Used(최종 사용**)**

네트워크에서 서버가 마지막으로 사용된 날짜 및 시간, 또는 호스트 입력 기능을 사용하여 서버가 원래 업데이트된 날짜 및 시간. Last Used 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 시스템이 서버 정보 업데이트를 탐지할 때 업데이트됩니다.

IP Address(IP 주소**)**

서버를 실행하는 호스트와 연결된 IP 주소.

Port(포트**)**

서버가 실행 중인 포트.

Protocol(프로토콜**)**

서버에서 사용하는 네트워크 또는 전송 프로토콜.

애플리케이션 프로토콜

다음 중 하나에 해당합니다.

- 서버에 대한 애플리케이션 프로토콜의 이름
- `pending` - 여러 이유 중 하나 때문에 시스템이 서버를 긍정적으로 또는 부정적으로 식별할 수 없는 경우
- `unknown` - 시스템이 알려진 서버 핑거프린트를 기반으로 서버를 식별할 수 없는 경우 또는 서버가 호스트 입력을 통해 추가되었고 애플리케이션 프로토콜을 포함하지 않은 경우

Category, Tags, Risk, or Business Relevance for Application Protocols(애플리케이션 프로토콜의 카테고리**,** 태그**,** 위험 또는 사업 타당성**)**

애플리케이션 프로토콜에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다.

Vendor(벤더**)**

다음 중 하나에 해당합니다.

- 시스템, Nmap, 다른 활성 소스 등에 의해 식별된 서버 공급업체 또는 호스트 입력 기능을 사용하여 지정한 서버 공급업체

- blank - 시스템이 알려진 서버 핑거프린트를 기반으로 공급업체를 식별할 수 없는 경우 또는 NetFlow 데이터를 사용하여 서버가 네트워크 맵에 추가된 경우

Version(버전**)**

다음 중 하나에 해당합니다.

- 시스템, Nmap, 다른 활성 소스 등에 의해 식별된 서버 공급업체 또는 호스트 입력 기능을 사용하여 지정한 서버 버전
- blank - 시스템이 알려진 서버 핑거프린트를 기반으로 버전을 식별할 수 없는 경우 또는 NetFlow 데이터를 사용하여 서버가 네트워크 맵에 추가된 경우

Web Application(웹 애플리케이션**)**

HTTP 트래픽에서 시스템에 의해 탐지된 페이로드 내용을 기반으로 하는 웹 애플리케이션. `HTTP`의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 일반 웹 브라우징 지정을 제공합니다.

Category, Tags, Risk, or Business Relevance for Web Applications(웹 애플리케이션의 카테고리**,** 태그**,** 위험 또는 사업 타당성**)**

웹 애플리케이션에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다.

Hits(히트**)**

서버에 액세스한 횟수. 호스트 입력 기능을 사용하여 추가된 서버의 경우 이 값은 항상 0입니다.

Source Type(소스 유형**)**

다음 값 중 하나:

- 사용자: user_name
- 애플리케이션: app_name
- 스캐너: scanner_type(네트워크 검색 구성을 통해 추가된 Nmap 또는 스캐너)
- Firepower System에서 탐지된 서버의 `Firepower`, `Firepower Port Match` 또는 `Firepower Pattern Match`
- NetFlow 데이터를 사용하여 추가된 서버의 `NetFlow`

도메인

서버를 실행하는 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Device(디바이스)

트래픽을 탐지한 매니지드 디바이스를 입력하거나, NetFlow 또는 호스트 입력 데이터를 처리한 디바이스를 입력합니다.

Current User(현재 사용자)

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 이 필드가 나타납니다.

관련 항목

이벤트 검색, 721 페이지

애플리케이션 및 애플리케이션 상세정보 데이터

모니터링되는 호스트가 다른 호스트에 연결되면, 시스템은 많은 경우 어떤 애플리케이션이 사용되었는지를 확인할 수 있습니다. Firepower System에서는 이메일, 인스턴트 메시징, 피어 투 피어, 웹 애플리케이션 및 기타 유형의 애플리케이션 사용을 탐지합니다.

탐지된 각 애플리케이션에 대해 시스템은 애플리케이션을 사용한 IP 주소, 제품, 버전, 탐지된 사용 횟수 등을 로깅합니다. 웹 인터페이스를 사용하여 애플리케이션 이벤트를 보고, 검색하고, 삭제할 수 있습니다. 또한 호스트 입력 기능을 사용하여 호스트의 애플리케이션 데이터를 업데이트할 수 있습니다.

어떤 애플리케이션이 어떤 호스트에서 실행 중인지 안다면, 이를 통해 호스트 프로파일 자격을 생성할 수 있습니다. 이 자격은 트래픽 프로파일 작성 중에 수집하는 데이터를 제한하며, 상관관계 규칙을 트리거할 조건을 제한할 수도 있습니다. 상관관계 규칙의 기반을 애플리케이션 탐지에 둘 수도 있습니다. 예를 들어 직원이 특정 메일 클라이언트를 사용하도록 하려면, 호스트 중 하나에서 다른 메일 클라이언트가 실행 중임을 시스템에서 탐지할 때 상관관계 규칙을 트리거할 수 있습니다.

각 Firepower System 업데이트의 릴리스 노트와 각 VDB 업데이트의 권고를 꼼꼼히 읽으면 Firepower의 애플리케이션 탐지기에 대한 최신 정보를 얻을 수 있습니다.

분석을 위해 애플리케이션 데이터를 수집 및 저장하려면 네트워크 검색 정책에서 애플리케이션 탐지를 활성화하십시오.

애플리케이션 데이터 보기

management center를 사용하면 탐지한 애플리케이션의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

애플리케이션에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 애플리케이션 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Application Details(**애플리케이션 세부 정보**)**를 선택합니다.
- 애플리케이션 세부사항의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Clients(**클라이언트**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(애플리케이션 데이터 필드, 955 페이지 참조).
- 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션 옆에 있는 **Application Detail View(**애플리케이션 세부 사항 보기**)**를 클릭하여 특정 애플리케이션의 Application Detail View(애플리케이션 세부 사항 보기)를 엽니다.
- 이벤트 값에서 마우스 오른쪽 버튼으로 클릭하여 시스템 외부에서 소스의 데이터를 봅니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지 섹션을 참조해 주십시오.
- 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택하여 이벤트에 대한 인텔리전스를 수집합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지를 참고하십시오.

애플리케이션 데이터 필드

알려진 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션에 대한 트래픽을 탐지하면 시스템은 애플리케이션 및 이를 실행하는 호스트에 대한 정보를 기록합니다.

다음은 애플리케이션 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Application(애플리케이션**)**

탐지된 애플리케이션의 이름

IP Address(IP 주소)

애플리케이션을 사용하는 호스트와 연결된 IP 주소

Type(유형)

애플리케이션 유형:

애플리케이션 프로토콜

호스트 간의 통신을 나타냅니다.

클라이언트 애플리케이션

호스트에서 실행 중인 소프트웨어를 나타냅니다.

Web Applications

HTTP 트래픽에 대한 콘텐츠 또는 요청 URL을 나타냅니다.

카테고리

가장 중요한 기능을 설명하는 일반 애플리케이션 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.

태그

애플리케이션에 대한 추가 정보. 애플리케이션에는 0부터 원하는 수만큼의 태그를 포함할 수 있습니다.

위험

조직의 보안 정책을 거스를 수 있는 용도로 애플리케이션이 사용될 가능성. 애플리케이션 위험의 범위는 Very Low(매우 낮음)에서 Very High(매우 높음)까지입니다.

침입 이벤트를 트리거한 트래픽에서 탐지된 Application Protocol Risk, Client Risk, Web Application Risk의 세 가지 중 최고(사용 가능한 경우).

Business Relevance(사업 타당성)

조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 애플리케이션이 사용될 가능성. 애플리케이션 비즈니스 연관성의 범위는 Very Low(매우 낮음)에서 Very High(매우 높음)까지입니다.

침입 이벤트를 트리거한 트래픽에서 탐지된 Application Protocol Business Relevance, Client Business Relevance, Web Application Business Relevance의 세 가지 중 최저(사용 가능한 경우).

Current User(현재 사용자)

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에

의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

도메인

애플리케이션을 사용하는 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

관련 항목

이벤트 검색, 721 페이지

애플리케이션 세부사항 데이터 보기

management center를 사용하면 탐지한 애플리케이션 세부사항의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

애플리케이션 세부사항에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 두 가지 사전 정의 워크플로가 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 애플리케이션 세부사항 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Application Details(애플리케이션 세부 정보)**를 선택합니다.
- 애플리케이션 세부사항의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)(워크플로 전환)**를 클릭한 다음 **Clients(클라이언트)**를 선택하십시오.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(워크플로 전환)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(애플리케이션 세부사항 데이터 필드, 958 페이지 참조).
- 클라이언트 옆에 있는 **Application Detail View(애플리케이션 세부사항 보기)** 를 클릭하여 특정 애플리케이션의 애플리케이션 세부사항 보기를 엽니다.
- 이벤트 값에서 마우스 오른쪽 버튼으로 클릭하여 시스템 외부에서 이용할 수 있는 소스의 데이터를 봅니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는

구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지 섹션을 참조해 주십시오.

- 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택하여 이벤트에 대한 인텔리전스를 수집합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지를 참고하십시오.

애플리케이션 세부사항 데이터 필드

알려진 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션에 대한 트래픽을 탐지하면 시스템은 애플리케이션 및 이를 실행하는 호스트에 대한 정보를 기록합니다.

다음은 애플리케이션 세부사항 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Last Used(최종 사용)

애플리케이션이 마지막으로 사용된 시간 또는 호스트 입력 기능을 사용하여 애플리케이션 데이터가 업데이트된 시간. Last Used 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 시스템이 애플리케이션 정보 업데이트를 탐지할 때 업데이트됩니다.

IP Address(IP 주소)

애플리케이션을 사용하는 호스트와 연결된 IP 주소

클라이언트

애플리케이션의 이름. 시스템이 애플리케이션 프로토콜을 탐지했지만 특정 클라이언트를 탐지하지 못한 경우, 일반 이름을 제공하기 위해 애플리케이션 프로토콜 이름에 `client`가 첨부됩니다.

Version(버전)

애플리케이션의 버전

Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications(클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션의 카테고리, 태그, 위험 또는 사업 타당성)

애플리케이션에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다.

애플리케이션 프로토콜

애플리케이션에서 사용하는 애플리케이션 프로토콜. 시스템이 애플리케이션 프로토콜을 탐지했지만 특정 클라이언트를 탐지하지 못한 경우, 일반 이름을 제공하기 위해 애플리케이션 프로토콜 이름에 `client`가 첨부됩니다.

Web Application(웹 애플리케이션**)**

HTTP 트래픽에서 시스템에 의해 탐지된 페이로드 내용 또는 URL을 기반으로 하는 웹 애플리케이션. HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 여기에서 일반 웹 브라우징 지정을 제공합니다.

Hits(히트**)**

시스템이 사용 중인 애플리케이션을 탐지한 횟수. 호스트 입력 기능을 사용하여 추가된 애플리케이션의 경우 이 값은 항상 0입니다.

도메인

애플리케이션을 사용하는 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

Domain(디바이스**)**

애플리케이션 세부사항을 포함하는 검색 이벤트를 생성한 디바이스.

Current User(현재 사용자**)**

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

관련 항목

이벤트 검색, 721 페이지

취약성 데이터

시스템에는 자체 취약성 추적 데이터베이스가 포함되어 있습니다. 이 데이터베이스를 시스템의 핑거프린트 인식 기능과 함께 사용하면 네트워크의 호스트에 연결된 취약성을 식별할 수 있습니다. 호스트에서 실행 중인 운영 체제, 서버 및 클라이언트는 연결된 취약성 집합이 서로 다릅니다.

management center를 사용하여 다음을 수행할 수 있습니다.

- 각 호스트의 취약성을 추적하고 검토합니다.
- 호스트를 패치하거나 그 밖의 방법으로 호스트가 취약성에 대해 면역력이 있다고 판단한 후 취약성을 비활성화합니다.

서버가 사용하는 애플리케이션 프로토콜이 management center 구성에서 매핑되어 있지 않으면 공급업체가 없는 서버 및 버전이 없는 서버의 취약성은 매핑되지 않습니다. 공급업체가 없는 클라이언트 및 버전이 없는 클라이언트의 취약성은 매핑할 수 없습니다.

관련 항목

서버의 취약성 매핑, 111 페이지

취약성 데이터 필드

언급된 경우를 제외하고 이러한 필드는 **Analysis(분석) > Hosts(호스트) > Vulnerabilities(취약점)** 아래의 모든 페이지에 표시됩니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

CVE ID

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(https://cve.mitre.org/)의 취약성에 연결된 식별 번호.

NVD(National Vulnerability Database)에서 이 취약점에 대한 세부 정보를 보려면 CVE ID를 마우스 오른쪽 버튼으로 클릭하고 **View description in NVD(NVD**에서 설명 보기**)**를 선택합니다.

게시 날짜

취약성이 게시된 날짜입니다.

설명

NVD(National Vulnerability Database)의 취약점에 대한 간략한 설명입니다.

전체 설명을 보려면 CVE ID를 마우스 오른쪽 버튼으로 클릭하고 **View description in NVD(NVD**에서 설명 보기**)**를 선택하여 NVD(National Vulnerability Database)에서 세부 정보를 봅니다.

영향

"취약점 영향"(아래)을 참조하십시오.

영향 자격

이 필드는 Vulnerability Details(취약점 세부 사항) 페이지에서만 사용할 수 있습니다.

드롭다운 목록을 사용하여 취약성을 활성화 또는 비활성화합니다. management center는 영향 상관관계에서 비활성화된 취약성을 무시합니다.

여기서 지정하는 설정은 시스템 전체에서 취약성의 취급 방법을 결정하며, 값을 선택한 호스트 프로파일로 제한되지 않습니다.

원격

취약성이 원격으로 악용될 수 있는지 여부(TRUE/FALSE)를 나타냅니다.

심각도

NVD(National Vulnerability Database)의 기본 점수 및 CVSS(Common Vulnerability Scoring System) 점수입니다.

Snort ID

Snort ID(SID) 데이터베이스의 취약성에 연결된 ID 번호입니다. 즉, 침입 규칙이 특정 취약성을 악용하는 네트워크 트래픽을 탐지할 수 있으면 해당 취약성은 침입 규칙의 SID와 연결됩니다.

취약성은 둘 이상의 SID와 연결될 수 있습니다(SID와 연결되지 않을 수도 있음). 취약성이 둘 이상의 SID에 연결된 경우, 취약성 테이블에는 각 SID에 대한 행이 포함됩니다.

SVID

시스템에서 취약성 추적에 사용하는 취약성 ID 번호.

이 취약점에 대한 세부 정보를 보려면 **View(**보기**)** ( )을(를) 클릭합니다.

취약점 영향**/**영향

0에서 10까지의 범위에서 취약성의 심각도를 나타내며, 10이 가장 심각합니다.

관련 항목

이벤트 검색, 721 페이지

취약성 비활성화

취약성을 비활성화하면 시스템은 해당 취약성을 사용하여 침입 영향 상관관계를 평가할 수 없습니다. 네트워크의 호스트에 패치를 적용하거나 그 밖의 방법으로 호스트가 취약성의 영향을 받지 않는다고 판단한 후 취약성을 비활성화할 수 있습니다. 시스템이 해당 취약성의 영향을 받는 새 호스트를 검색하면, 이 취약성은 해당 호스트에 대해 유효한 것으로 간주됩니다(따라서 자동으로 비활성화되지 않음).

IP 주소로 제한되지 않은 취약성 워크플로 내에서 취약성을 비활성화하면 네트워크에서 탐지된 모든 호스트에 대해 취약성이 비활성화됩니다. 취약성 워크플로 내의 취약성은 다음에서만 비활성화할 수 있습니다.

- 기본 취약성 워크플로의 두 번째 페이지인 **Vulnerabilities on the Network(**네트워크의 취약성**)**. 여기에는 네트워크의 호스트에 해당되는 취약성만 표시됩니다.
- 검색을 사용하여 IP 주소를 기반으로 제한한 맞춤형 또는 사전 정의된 취약성 워크플로의 페이지.

네트워크 맵을 사용하거나 호스트의 호스트 프로파일을 사용하거나 취약성을 비활성화하려는 호스트의 IP 주소를 기반으로 취약성 워크플로를 제한하여 단일 호스트의 취약성을 비활성화할 수 있습

니다. 연결된 IP 주소가 여러 개인 호스트의 경우, 이 기능은 해당 호스트의 선택된 단일 IP에만 적용됩니다.

다중 도메인 구축에서 상위 도메인의 취약성을 비활성화하면 모든 하위 도메인에서 해당 취약성이 비활성화됩니다. 취약성이 상위 도메인에서 활성화된 경우, 리프 도메인은 디바이스에서 해당 취약성을 활성화하거나 비활성화할 수 있습니다.

관련 항목

개별 호스트용 취약성 비활성화, 918 페이지
개별 취약성 비활성화, 919 페이지
다중 취약성 비활성화, 963 페이지

취약성 데이터 보기

management center를 사용하여 취약성의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

취약성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 취약성의 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 탐지된 호스트가 취약성을 보이는지 여부와 상관없이 테이블 보기에는 데이터베이스의 각 취약성에 대한 행이 포함되어 있습니다. 사전 정의 워크플로의 두 번째 페이지에는 네트워크에서 탐지된 호스트에 적용되는 각 취약성의 행(비활성화하지 않은)이 포함되어 있습니다. 사전 정의 워크플로는 제약 조건을 충족하는 모든 취약성에 대한 자세한 설명이 포함된 취약성 세부사항 보기에서 종료됩니다.

팁 단일 호스트 또는 호스트 집합에 적용되는 취약성을 보려면 호스트의 IP 주소 또는 IP 주소 범위를 지정하여 취약성 검색을 수행하십시오.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

취약성 테이블은 다중 도메인 구축에서 도메인에 의해 제한되지 않습니다.

프로시저

단계 **1** 취약성 테이블에 액세스합니다.

- 사전 정의된 취약성 워크플로를 사용 중인 경우 **Analysis(분석)** > **Hosts(호스트)** > **Vulnerabilities(취약성)**를 선택합니다.
- 취약성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Vulnerabilities(취약성)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 현재 취약한 호스트의 침입 영향 상관관계에 더 이상 사용되지 않도록 취약성을 비활성화합니다(다중 취약성 비활성화, 963 페이지 참조).

- SVID 열에서 **View(**보기**)** ( )을 클릭하여 취약성의 세부사항을 봅니다. 또는 취약성 ID를 제한하고 취약성 세부사항 페이지로 드릴다운합니다. 취약성 세부사항 보기, 963 페이지에서 추가 세부 정보를 보는 옵션을 참조하십시오.
- 제목을 마우스 오른쪽 버튼으로 클릭하고 **Show Full Text(**전체 텍스트 표시**)**를 선택하여 취약성 제목의 전체 텍스트를 확인합니다.

취약성 세부사항 보기

프로시저

다음 방법 중 하나로 취약성 세부사항을 볼 수 있습니다.

- **Analysis(**분석**)** > **Hosts(**호스트**)** > **Vulnerabilities(**취약성**)**를 선택하고 SVID 옆에 있는 **View(**보기**)** ( )를 클릭합니다.
- **Analysis(**분석**)** > **Hosts(**호스트**)** > **Third-Party Vulnerabilities(**서드파티 취약성**)**를 선택하고 SVID 옆에 있는 **View(**보기**)** ( )를 클릭합니다.
- **Analysis(**분석**)** > **Hosts(**호스트**)** > **Network Map(**네트워크 맵**)**를 선택하고 **Vulnerabilities(**취약성**)**을 클릭합니다.
- 취약성의 영향을 받는 호스트의 프로필을 보고(**Analysis(**분석**)** > **Hosts(**호스트**)** > **Network Map(**네트워크 맵**)**, **Hosts(**호스트**)**를 클릭하고, 드릴다운해서 조사하는 호스트를 클릭합니다), 프로필의 **Vulnerabilities(**취약성**)** 섹션을 확장합니다.
- **Analysis(**분석**)> Hosts(**호스트**)> Vulnerabilities(**취약성**)** 아래의 테이블에서 **CVE ID** 열의 값을 마우스 오른쪽 버튼으로 클릭하고 **View description in NVD(NVD**에서 설명보기**)**를 선택하여 NVD(National Vulnerabilities Database) 웹 사이트에서 해당 CVE를 봅니다.

다중 취약성 비활성화

IP 주소로 제한되지 않은 취약성 워크플로 내에서 취약성을 비활성화하면 네트워크에서 탐지된 모든 호스트에 대해 취약성이 비활성화됩니다.

다중 도메인 구축에서 상위 도메인의 취약성을 비활성화하면 모든 하위 도메인에서 해당 취약성이 비활성화됩니다. 취약성이 상위 도메인에서 활성화된 경우, 리프 도메인은 디바이스에서 해당 취약성을 활성화하거나 비활성화할 수 있습니다.

프로시저

단계 **1** 취약성 테이블에 액세스합니다.

- 사전 정의된 취약성 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Vulnerabilities(**취약성**)**를 선택합니다.

- 취약성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Vulnerabilities(**취약성**)**를 선택합니다.

단계 **2** **Vulnerabilities on the Network(**네트워크의 취약성**)**를 클릭합니다.

단계 **3** 비활성화하려는 취약성 옆의 확인란을 선택합니다.

단계 **4** 페이지 하단의 **Review(**검토**)**를 클릭합니다.

관련 항목

개별 호스트용 취약성 비활성화, 918 페이지
개별 취약성 비활성화, 919 페이지

서드파티 취약성 데이터

Firepower System에는 자체 취약성 추적 데이터베이스가 포함되어 있습니다. 이 데이터베이스를 시스템의 핑거프린트 인식 기능과 함께 사용하면 네트워크의 호스트에 연결된 취약성을 식별할 수 있습니다.

서드파티 애플리케이션에서 가져온 네트워크 맵 데이터로 시스템의 취약성 데이터를 보강할 수 있습니다. 그러려면 조직이 스크립트를 작성하거나 명령줄 파일 가져오기를 만들어 데이터를 가져올 수 있어야 합니다. 자세한 내용은 *Firepower System Host Input API* 설명서을 참조하십시오.

가져온 데이터를 영향 상관관계에 포함하려면 서드파티 취약성 정보를 데이터베이스의 운영 체제 및 애플리케이션 정의에 매핑해야 합니다. 서드파티 취약성 정보를 클라이언트 정의에 매핑할 수는 없습니다.

서드파티 취약성 데이터 보기

호스트 입력 기능을 사용하여 서드파티 취약성 데이터를 가져왔으면 management center를 사용하여 서드파티 취약성의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

서드파티 취약성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 두 가지 사전 정의 워크플로가 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 서드파티 취약성 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Third-Party Vulnerabilities(**서드파티 취약성**)**를 선택합니다.

- 서드파티 취약성의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용하는 경우, **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Vulnerabilities by Source(**소스별 취약성**)** 또는 **Vulnerabilities by IP Address(IP** 주소별 취약성**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(서드파티 취약성 데이터 필드, 965 페이지 참조).
- SVID 열에서 **View(**보기**)** ( )를 클릭하여 서드파티 취약성의 취약성 세부 사항을 봅니다. 또는 취약성 ID를 제한하고 취약성 세부사항 페이지로 드릴다운합니다.

서드파티 취약성 데이터 필드

다음은 서드파티 취약성 테이블에서 보고 검색할 수 있는 필드에 대한 설명입니다.

Vulnerability Source

서드파티 취약성의 소스(예: QualysGuard 또는 NeXpose).

취약성 **ID**

소스의 취약성과 연결된 ID 번호.

IP 주소

취약성의 영향을 받는 호스트와 연결된 IP 주소.

Port(포트**)**

취약성이 특정 포트에서 실행 중인 서버와 연결된 경우 포트 번호.

Bugtraq ID

Bugtraq 데이터베이스의 취약성과 관련된 ID 번호입니다. (http://www.securityfocus.com/bid/)

CVE ID

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(https://cve.mitre.org/)의 취약성에 연결된 식별 번호.

SVID

시스템이 취약성 추적에 사용하는 레거시 취약성 식별 번호.

SVID에 대한 취약성 세부사항에 액세스하려면 **View(**보기**)** ( )을 클릭합니다.

Snort ID

Snort ID(SID) 데이터베이스의 취약성에 연결된 ID 번호입니다. 즉, 침입 규칙이 특정 취약성을 악용하는 네트워크 트래픽을 탐지할 수 있으면 해당 취약성은 침입 규칙의 SID와 연결됩니다.

취약성은 둘 이상의 SID와 연결될 수 있습니다(SID와 연결되지 않을 수도 있음). 취약성이 둘 이상의 SID에 연결된 경우, 취약성 테이블에는 각 SID에 대한 행이 포함됩니다.

직함

취약성의 제목입니다.

설명

취약성에 대한 간단한 설명.

도메인

취약성이 있는 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

관련 항목

이벤트 검색, 721 페이지

활성 세션, 사용자 및 사용자 활동 데이터

ID 소스는 활성 세션 데이터, 사용자 데이터, 사용자 활동 데이터를 수집합니다. 데이터는 개별 사용자 관련 워크플로에 표시됩니다.

- 활성 세션 - 이 워크플로는 네트워크의 모든 현재 사용자 세션을 표시합니다. 여러 활성 세션을 동시에 실행하는 단일 사용자는이 테이블에서 여러 행을 차지합니다. 이 워크플로에 표시되는 사용자 데이터 유형에 대한 자세한 내용은 활성 세션 데이터, 974 페이지를 참조하십시오.
- 사용자 - 이 워크플로는 네트워크에서 보이는 모든 사용자를 표시합니다. 단일 사용자는 이 테이블에서 단일 행을 차지합니다. 이 워크플로에 표시되는 사용자 데이터 유형에 대한 자세한 내용은 사용자 데이터, 975 페이지를 참조하십시오.
- 사용자 활동 - 이 워크플로는 네트워크에서 보이는 모든 사용자 활동을 표시합니다. 사용자 활동의 인스턴스가 여러 개 있는 단일 사용자는 이 테이블에서 여러 행을 차지합니다. 이 워크플로에 표시되는 사용자 활동 유형에 대한 자세한 내용은 사용자 활동 데이터, 978 페이지를 참조하십시오.

이러한 워크플로를 채우는 사용자 ID 소스에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오.

사용자 관련 필드

사용자 관련 데이터는 활성 세션, 사용자, 사용자 활동 테이블에 표시됩니다.

표 ***112:*** 활성 세션, 사용자, 사용자 활동 필드 설명

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
활성 세션 수	사용자와 연결된 활성 세션의 수.	아니요	예	아니요
인증 유형	인증 유형: `No Authentication(인증 없음)`, `Passive Authentication(패시브 인증)`, `Active Authentication(액티브 인증)`, `Guest Authentication(게스트 인증)`, `Failed Authentication(실패한 인증)` 또는 `VPN Authentication(VPN 인증)` 각 인증 유형에 지원되는 ID 소스에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드를 참조하십시오.	예	아니요	예
정책에 사용 가능	**Yes** 값은 사용자 저장소(예: Active Directory)에서 사용자가 검색되었음을 의미합니다. **No** 값은 management center가 해당 사용자의 로그인 보고를 수신했지만 해당 사용자가 사용자 저장소에 없음을 의미합니다. 이것이 일어날 수 있는 한 가지 방법은 제외된 그룹의 사용자가 사용자 저장소에 로그인하는 경우입니다. 영역을 구성할 때 그룹이 다운로드되는 것을 차단할 수 있습니다. 정책에 사용할 수 없는 사용자는 management center에 기록되지만 매니지드 디바이스에 전송되지 않습니다.	아니요	예	아니요
개수	참고 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 **Count(개수)** 필드가 표시됩니다. 테이블에 따라 특정 행에 표시되는 정보와 일치하는 세션, 사용자 또는 활동 이벤트의 수입니다.	예	예	예
현재 **IP**	사용자가 로그인하는 호스트와 연결된 IP 주소. 사용자의 활성 세션이 없는 경우 사용자 테이블에서 이 필드는 비어 있습니다.	예	예	아니요

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
부서	영역에서 가져온 사용자의 부서. 서버의 사용자와 명시적으로 연결된 부서가 없는 경우, 부서는 서버가 할당하는 기본 그룹으로 나열됩니다. 예를 들면 Active Directory에서는 `Users (ad)` 입니다. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • management center에서는 management center 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우).	예	예	아니요
설명	세션, 사용자 또는 사용자 활동에 대한 추가 정보(제공되는 경우).	아니요	아니요	예
디바이스	트래픽 기반 탐지 또는 액티브 인증 ID 소스에서 탐지된 사용자 활동의 경우, 사용자를 식별한 디바이스의 이름입니다. 다른 사용자 활동 유형의 경우, 관리하는 management center. 참고 고가용성 구축에서 VPN을 구성한 경우 활성 VPN 세션에 대해 표시되는 디바이스 이름은 사용자 세션을 식별한 기본 또는 보조 디바이스일 수 있습니다.	예	아니요	예
검색 애플리케이션	사용자를 탐지하는 데 사용된 애플리케이션 또는 프로토콜. • 트래픽 기반 탐지에서 탐지된 사용자 활동의 경우 다음 중 하나에 해당: ldap, pop3, imap, oracle, sip, ftp, http, mdns, aim. 참고 사용자는 SMTP 로그인에 기반한 데이터베이스에 추가되지 않습니다. • 모든 기타 사용자 활동의 경우: ldap	예	예	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
현재 **IP** 도메인/도메인	활성 세션 테이블에서 사용자 활동이 탐지된 멀티테넌시 도메인. 사용자 테이블에서 사용자의 영역과 연결된 멀티테넌시 도메인. 사용자 활동 테이블에서 사용자 활동이 탐지된 멀티테넌시 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.	예	예	예
이메일	사용자의 이메일 주소. 다음과 같은 경우 이 필드는 비어 있습니다. • AIM 로그인을 통해 사용자가 데이터베이스에 추가된 경우. • LDAP 로그인을 통해 사용자가 데이터베이스에 추가되었으며 LDAP 서버의 사용자와 연결된 이메일 주소가 없는 경우.	예	예	아니요
종료 포트	TS 에이전트에서 사용자를 보고하고 세션이 현재 활성화된 경우, 이 필드는 사용자에게 할당된 포트 범위의 종료 값을 식별합니다. 사용자의 TS 에이전트 세션이 비활성화되어 있거나 다른 ID 소스에서 사용자를 보고한 경우 이 필드는 비어 있습니다.	예	아니요	예
엔드포인트 위치	ISE에서 식별된 사용자를 인증하기 위해 ISE가 사용되는 네트워크 디바이스의 IP 주소. ISE를 구성하지 않은 경우 이 필드는 비어 있습니다.	아니요	아니요	예
엔드포인트 프로파일	Cisco ISE에서 식별된 사용자의 엔드포인트 디바이스 유형. ISE를 구성하지 않은 경우 이 필드는 비어 있습니다.	아니요	아니요	예
이벤트	사용자 활동 이벤트 유형.	아니요	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
이름	영역에서 가져온 사용자의 이름. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • management center에서는 management center 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우). • 서버의 사용자와 연결된 이름이 없는 경우.	예	예	아니요
IP 주소	**User Login(**사용자 로그인**)** 사용자 활동의 경우, 로그인과 관련된 IP 주소 또는 내부 IP 주소: • LDAP, POP3, IMAP, FTP, HTTP, MDNS, AIM 로그인 — 사용자 호스트의 주소 • SMTP 및 Oracle 로그인 — 서버의 주소 • SIP 로그인 — 세션 시작 주체의 주소 IP 주소가 연결되어 있다고 해서 사용자가 해당 IP 주소의 현재 사용자라는 의미는 아닙니다. 권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
성	영역에서 가져온 사용자의 성. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • management center에서는 management center 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우). • 서버의 사용자와 연결된 성이 없는 경우.	예	예	아니요

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
최종 확인	사용자의 세션이 마지막으로 시작된(또는 사용자 데이터가 업데이트된) 날짜 및 시간.	예	예	아니요
로그인 시간	사용자의 세션이 시작된 날짜 및 시간.	예	아니요	아니요
전화	영역에서 가져온 사용자의 전화 번호. 다음과 같은 경우 이 필드는 비어 있습니다. • 영역을 구성하지 않은 경우. • management center에서는 management center 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우). • 서버의 사용자와 연결된 전화 번호가 없는 경우.	예	예	아니요
영역	사용자와 연결된 ID 영역.	예	예	예
보안 그룹 태그	패킷이 신뢰할 수 있는 TrustSec 네트워크에 들어갔을 때 Cisco TrustSec에서 적용한 SGT(Security Group Tag) 속성. ISE를 구성하지 않은 경우 이 필드는 비어 있습니다.	아니요	아니요	예
세션 기간	**Login Time(**로그인 시간**)**과 현재 시간에서 계산된 사용자 세션의 기간.	예	아니요	아니요
시작 포트	TS 에이전트에서 사용자를 보고하고 세션이 현재 활성화된 경우, 이 필드는 사용자에게 할당된 포트 범위의 시작 값을 식별합니다. 사용자의 TS 에이전트 세션이 비활성화되어 있거나 다른 ID 소스에서 사용자를 보고한 경우 이 필드는 비어 있습니다.	예	아니요	예
시간	시스템이 사용자 활동을 탐지한 시간.	아니요	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
사용자	이 필드에는 최소한 사용자의 영역 및 사용자 이름이 표시됩니다. 예를 들어 `Lobby\jsmith`의 경우 Lobby는 영역이고 jsmith는 사용자 이름입니다. 영역이 LDAP 서버에서 사용자 추가 데이터를 다운로드하고 시스템이 이를 사용자와 연결할 경우, 이 필드에는 또한 사용자의 이름, 성, 유형이 표시됩니다. 예를 들어 `John Smith (Lobby\jsmith, LDAP)`의 경우 John Smith는 사용자의 이름이고 LDAP는 유형입니다. 참고 트래픽 기반 탐지는 실패한 AIM 로그인을 기록할 수 있으므로, management center에서는 잘못된 AIM 사용자(예: 사용자가 사용자 이름의 철자를 잘못 쓴 경우)를 저장할 수 있습니다.	예	예	아니요
Username	사용자와 연결된 사용자 이름.	예	예	예
VPN 바이트 인	원격 액세스 VPN에서 보고된 사용자 활동의 경우, threat defense에서 원격 피어 또는 클라이언트로부터 수신된 총 바이트 수입니다. 참고 사용자의 VPN 세션이 종료되면 수신된 총 바이트 수를 볼 수 있습니다. 진행 중인 VPN 세션의 경우, 이는 동적 카운터가 아닙니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN 바이트 아웃	원격 액세스 VPN에서 보고된 사용자 활동의 경우, threat defense에서 원격 피어 또는 클라이언트로 전송한 총 바이트 수입니다. 참고 사용자의 VPN 세션이 종료되면 전송한 총 바이트 수를 볼 수 있습니다. 진행 중인 VPN 세션의 경우, 이는 동적 카운터가 아닙니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN 클라이언트 애플리케이션	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 원격 사용자의 Cisco Secure Client의 AnyConnect VPN 애플리케이션입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예

필드	설명	활성 세션 테이블	사용자 테이블	사용자 활동 테이블
VPN 클라이언트 국가	원격 액세스 VPN에서 보고한 사용자 활동의 경우, Secure Client VPN에서 보고된 국가 이름입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN 클라이언트 **OS**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, Secure Client VPN에서 보고된 원격 사용자의 엔드포인트 운영 체제입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN 클라이언트 공개 **IP**	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 공개적으로 라우팅 가능한 Secure Client VPN 디바이스의 IP 주소입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN 연결 지속 시간	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 세션이 활성화된 총 시간(HH:MM:SS)입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	아니요	아니요	예
VPN 연결 프로파일	원격 액세스 VPN에서 보고한 사용자 활동의 경우, VPN 세션에서 사용된 연결 프로파일(터널 그룹)의 이름입니다. 연결 프로파일은 원격 액세스 VPN 정책의 일부입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN 그룹 정책	원격 액세스 VPN에서 보고한 사용자 활동의 경우, VPN 세션을 설정했을 때 클라이언트에 할당된 그룹 정책의 이름입니다. 이러한 정책은 VPN 연결 프로파일과 연결된 정적으로 할당된 그룹 정책이거나, RADIUS가 인증에 사용된 경우 동적으로 할당된 그룹 정책입니다. RADIUS 서버에서 할당한 경우, 이 그룹 정책은 VPN 연결 프로파일에 구성된 고정 정책을 재정의합니다. 그룹 정책은 원격 액세스 VPN 정책의 사용자 그룹에 대한 일반 속성을 구성합니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예
VPN 세션 유형	원격 액세스 VPN에서 보고한 사용자 활동의 경우, 세션의 유형(LAN 대 LAN 또는 원격)입니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.	예	아니요	예

활성 세션 데이터

Analysis(분석**)** > **Users(**사용자**)** > **Active Sessions(**활성 세션**)** 워크플로에는 현재 사용자 세션에 대한 선택 정보가 표시됩니다. 네트워크의 한 사용자가 여러 세션을 동시에 실행 중인 경우, Firepower System은 세션이 다음과 같은 상태인지 여부를 고유하게 식별할 수 있습니다.

- 세션에 고유한 **IP Address(IP** 주소**)** 값이 있는지 식별합니다.
- 세션에 Cisco TS(Terminal Services) 에이전트에서 제공한 고유한 **Start Port(**시작 포트**)** 및 **End Port(**종료 포트**)** 값이 있는지 식별합니다.
- 세션에 고유한 **Current IP Domain(**현재 **IP** 도메인**)** 값이 있는지 식별합니다.
- 다른 ID 소스에서 인증되었는지 식별합니다.
- 다른 ID 영역과 연결되었는지 식별합니다.

시스템에 저장된 사용자 및 사용자 활동 데이터에 대한 자세한 내용은 사용자 데이터, 975 페이지 및 사용자 활동 데이터, 978 페이지를 참조하십시오.

일반적인 사용자 관련 이벤트 문제 해결 및 원격 액세스 VPN 문제 해결에 대한 자세한 내용은 영역 및 사용자 다운로드 트러블슈팅및 *VPN* 트러블슈팅을 참조하십시오.

활성 세션 데이터 보기

활성 세션의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

사용자에게 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 사용자를 나열하는 사용자의 테이블 보기를 포함하며 사용자 세부사항 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 사용자 세부사항 페이지는 제약 조건을 충족하는 모든 사용자에 대한 정보를 제공합니다.

프로시저

단계 **1** 사용자 데이터에 액세스합니다.

- 사전 정의 워크플로우를 사용하는 경우 **Analysis(**분석**)** > **Users(**사용자**)** > **Active Sessions(**활동 세션**)**를 클릭합니다.
- 활성 세션의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음, **Active Sessions(**활성 세션**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).

- 테이블의 열에 대한 내용을 자세히 알아보십시오(활성 세션 데이터, 974 페이지 및 사용자 관련 필드, 967 페이지 참조).

사용자 데이터

ID 소스가 아직 데이터베이스에 없는 사용자의 사용자 로그인을 보고하면, 이러한 로그인 유형을 특별히 제한하지 않은 경우 해당 사용자는 데이터베이스에 추가됩니다.

시스템은 다음 중 한 가지 상황이 발생할 경우 사용자 데이터베이스를 업데이트합니다.

- management center의 사용자가 사용자 테이블에서 권한 없는 사용자를 수동으로 삭제합니다.
- ID 소스가 해당 사용자의 로그오프를 보고합니다.
- 영역은 영역의 **User Session Timeout: Authenticated Users(**사용자 세션 시간 초과**:** 인증된 사용자**)**, **User Session Timeout: Failed Authentication Users(**사용자 세션 시간 초과**:** 실패한 인증 사용자**)** 또는 **User Session Timeout: Guest Users(**사용자 세션 시간 초과**:** 게스트 사용자**)** 설정에서 지정된 대로 사용자 세션을 종료합니다.

참고 ISE/ISE-PIC를 구성한 경우, 사용자 테이블에 호스트 데이터가 표시될 수 있습니다. ISE/ISE-PIC에서는 호스트 탐지를 일부만 지원하므로, ISE에서 보고한 호스트 데이터를 사용하여 사용자 제어를 수행할 수 없습니다.

시스템에서 탐지한 사용자 로그인의 유형은 새로운 사용자에 대해 어떤 정보를 저장할지 결정합니다.

ID 소스	로그인 유형	저장되는 사용자 데이터
ISE/ISE-PIC	Active Directory LDAP RADIUS RSA	• 사용자 이름 • 현재 IP 주소 • SGT(Security Group Tag) — ISE-PIC에서 지원되지 않음 • 엔드포인트 프로파일/디바이스 유형 — ISE-PIC에서 지원되지 않음 • 엔드포인트 위치/위치 IP — ISE-PIC에서 지원되지 않음 • 유형(LDAP)

ID 소스	로그인 유형	저장되는 사용자 데이터
TS 에이전트	Active Directory	• 사용자 이름 • 현재 IP 주소 • 시작 포트 • 종료 포트 • 유형(LDAP)
캡티브 포털	Active Directory LDAP	• 사용자 이름 • 현재 IP 주소 • 유형(LDAP)
트래픽 기반 탐지	LDAP AIM Oracle SIP HTTP FTP MDNS	• 사용자 이름 • 현재 IP 주소 • 유형(AD)
	POP3 IMAP	• 사용자 이름 • 현재 IP 주소 • 이메일 주소 • 유형(`pop3` 또는 `imap`)

사용자를 자동으로 다운로드하도록 영역을 구성할 경우, management center에서는 지정된 간격을 기준으로 서버를 쿼리합니다. 시스템에서 새 사용자 로그인을 탐지한 후 management center 데이터베이스에서 사용자 메타데이터를 업데이트하는 데 5~10분 정도 걸릴 수 있습니다. management center에서는 각 사용자에 대한 다음과 같은 정보 및 메타데이터를 얻습니다.

- 사용자 이름
- 이름 및 성
- 이메일 주소
- department
- 전화번호

- 현재 IP 주소
- SGT(Security Group Tag) - 제공되는 경우
- 엔드포인트 프로파일 - 제공되는 경우
- 엔드포인트 위치 - 제공되는 경우
- 시작 포트 - 제공되는 경우
- 종료 포트 - 제공되는 경우

management center에서 데이터베이스에 저장할 수 있는 사용자 수는 management center 모델에 따라 다릅니다. 권한 없는 사용자가 호스트에 로그인한 것이 탐지되면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 해당 호스트에서 권한 있는 사용자 로그인이 탐지되면, 또 다른 권한 있는 사용자 로그인만이 현재 사용자를 변경합니다.

AIM, Oracle, SIP 로그인의 트래픽 기반 탐지는 시스템이 LDAP 서버에서 가져오는 사용자 메타데이터와 연결되지 않으므로 중복 사용자 레코드를 생성합니다. 이러한 프로토콜의 중복 사용자 레코드로 인한 사용자 수 남용을 방지하려면, 해당 프로토콜을 무시하도록 트래픽 기반 탐지를 구성합니다.

데이터베이스에서 사용자를 검색하고 보고 삭제할 수 있습니다. 또한 데이터베이스에서 모든 사용자를 삭제할 수도 있습니다.

일반적인 사용자 관련 이벤트 문제 해결에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드을 참조하십시오.

사용자 데이터 보기

사용자의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

사용자에게 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 사용자를 나열하는 사용자의 테이블 보기를 포함하며 사용자 세부사항 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 사용자 세부사항 페이지는 제약 조건을 충족하는 모든 사용자에 대한 정보를 제공합니다.

프로시저

단계 **1** 사용자 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(**분석**)** > **Users(**사용자**)** > **Users(**사용자**)**를 선택합니다.
- 사용자의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Users(**사용자**)**를 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(사용자 관련 필드, 967 페이지 참조).

사용자 활동 데이터

시스템은 네트워크에서 사용자 활동의 세부사항을 전달하는 이벤트를 생성합니다. 시스템이 사용자 활동을 탐지하면 사용자 활동 데이터가 데이터베이스에 로깅됩니다. 사용자 활동을 보고 검색하고 삭제할 수 있습니다. 또한 데이터베이스에서 모든 사용자 활동을 삭제할 수도 있습니다.

사용자가 네트워크에 최초로 나타나면 시스템은 사용자 활동 이벤트를 로깅합니다. 해당 사용자가 다음번에 나타날 경우에는 새로운 사용자 활동 이벤트를 로깅하지 않습니다. 그러나 사용자의 IP 주소가 변경되면 시스템은 새로운 사용자 활동 이벤트를 로깅합니다.

또한, 시스템은 사용자 활동을 다른 이벤트 유형과 서로 연관시킵니다. 예를 들어, 침입 이벤트는 이벤트 발생 시점에 소스 및 대상 호스트에 로그인한 사용자를 알려줄 수 있습니다. 이러한 상관관계를 통해 공격 대상인 호스트에 로그인한 사용자, 또는 내부 공격이나 포트스캔을 시작한 사용자를 알 수 있습니다.

상관관계 규칙에서 사용자 활동을 사용할 수도 있습니다. 사용자 활동 및 지정한 다른 기준을 기반으로 상관관계 규칙을 작성할 수 있습니다. 상관관계 정책에서 사용할 경우 이러한 규칙은 네트워크 트래픽이 조건을 충족하면 교정과 알림 응답을 실행합니다.

참고 ISE/ISE-PIC를 구성한 경우, 사용자 테이블에 호스트 데이터가 표시될 수 있습니다. ISE/ISE-PIC에서는 호스트 탐지를 일부만 지원하므로, ISE에서 보고한 호스트 데이터를 사용하여 사용자 제어를 수행할 수 없습니다.

다음은 네 가지 유형의 사용자 활동 데이터에 대한 설명입니다.

새로운 사용자 **ID**

시스템이 데이터베이스에 없는 알 수 없는 사용자의 로그인을 탐지할 경우 이 유형의 이벤트가 생성됩니다.

사용자가 네트워크에 최초로 나타나면 시스템은 사용자 활동 이벤트를 로깅합니다. 해당 사용자가 다음번에 나타날 경우에는 새로운 사용자 활동 이벤트를 로깅하지 않습니다. 그러나 사용자의 IP 주소가 변경되면 시스템은 새로운 사용자 활동 이벤트를 로깅합니다.

사용자 로그인

다음 중 하나가 발생할 경우 이 유형의 이벤트가 생성됩니다.

- 캡티브 포털(captive portal)은 성공 또는 실패한 사용자 인증을 수행합니다.
- 트래픽 기반 탐지는 성공 또는 실패한 사용자 로그인을 탐지합니다.

참고 트래픽 기반 탐지에서 탐지된 SMTP 로그인은 데이터베이스에 이미 일치하는 이메일 주소의 사용자가 있지 않은 한 기록되지 않습니다.

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다.

캡티브 포털(captive portal) 또는 트래픽 기반 탐지를 사용할 경우, 실패한 사용자 로그인 및 실패한 사용자 인증 데이터에 대한 다음 사항에 유의하십시오.

- 트래픽 기반 탐지(LDAP, IMAP, FTP 및 POP3 트래픽)에서 보고한 실패한 로그인은 사용자의 테이블 보기가 아닌 사용자 활동의 테이블 보기에 표시됩니다. 알려진 사용자가 로그인에 실패한 경우, 시스템은 사용자 이름으로 해당 사용자를 식별합니다. 알 수 없는 사용자가 로그인에 실패한 경우, 시스템은 **Failed Authentication(**실패한 인증**)**을 사용자 이름으로 사용합니다.
- 캡티브 포털(captive portal)에서 보고한 실패한 인증은 사용자 활동의 테이블 보기 및 사용자의 테이블 보기에 모두 표시됩니다. 알려진 사용자가 인증에 실패한 경우, 시스템은 사용자 이름으로 해당 사용자를 식별합니다. 알 수 없는 사용자가 인증에 실패한 경우, 시스템은 사용자가 입력한 사용자 이름으로 해당 사용자를 식별합니다.

사용자 **ID** 삭제

데이터베이스에서 사용자를 수동으로 삭제할 경우 이 유형의 이벤트가 생성됩니다.

User Identity Dropped: User Limit Reached(사용자 **ID** 차단**:** 사용자 한계 도달**)**

시스템이 데이터베이스에 없는 사용자를 탐지했지만, management center 모델에서 확인된 데이터베이스의 사용자 최대 수에 도달했기 때문에 해당 사용자를 추가할 수 없는 경우 이 유형의 이벤트가 생성됩니다.

사용자 제한에 도달하면 대부분의 경우 시스템에서는 데이터베이스에 새 사용자를 추가하지 않습니다. 새 사용자를 추가하려면 데이터베이스에서 오래된 사용자 또는 비활성 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다.

그러나 시스템은 권한 있는 사용자를 선호합니다. 제한에 도달한 상태에서 시스템이 전에 탐지하지 못한 권한 있는 사용자의 로그인을 탐지하면, 오랫동안 비활성 상태를 유지한 권한 없는 사용자를 삭제하고 새로운 권한 있는 사용자를 대신 추가합니다.

사용자 보안 침해 지표 이벤트

다음과 같은 사용자 IOC 변경 사항은 사용자 활동 데이터베이스에 로깅됩니다.

- 보안 침해 지표가 해결된 경우
- 사용자에 대해 보안 침해 지표 규칙이 활성화 또는 비활성화된 경우

일반적인 사용자 관련 이벤트 문제 해결에 대한 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 내용을 참조하십시오.

사용자 활동 데이터 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

사용자 활동의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다. 사용자 활동에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 사용자 활동의 테이블 보기를 포함하며 사용자 세부사항 페이지(제약 조건을 충족하는 모든 사용자에 대한 사용자 세부사항 포함)에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

프로시저

단계 **1** 사용자 활동 데이터에 액세스합니다.

- 사전 정의된 워크플로를 사용 중인 경우 **Analysis(분석)** > **Users(사용자)** > **User Activity(사용자의 활동)**를 선택합니다.
- 사용자 활동의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)(워크플로 전환)**를 클릭한 다음 **User Activity(사용자 활동)**를 선택합니다.

팁 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 타임 윈도우 변경, 710 페이지을 참조하십시오.

단계 **2** 다음과 같은 옵션이 있습니다.

- 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(워크플로 전환)**를 클릭합니다.
- 기본 워크플로 작업을 수행합니다(검색 및 ID 워크플로 사용, 927 페이지 참조).
- 테이블의 열에 대한 내용을 자세히 알아보십시오(사용자 관련 필드, 967 페이지 참조).

사용자 프로파일 및 호스트 기록

User(사용자) 팝업 창을 통해 특정 사용자에 대해 자세히 알아볼 수 있습니다. 이 문서에서 "User Profile"이라고 하는 표시되는 페이지의 웹 인터페이스에서의 제목은 "User Identity"입니다.

다음에서 창을 표시할 수 있습니다.

- 사용자 데이터를 다른 종류의 이벤트와 연결하는 이벤트 보기
- 활성 세션의 테이블 보기
- 사용자의 테이블 보기

사용자 정보는 사용자 워크플로의 종료 페이지에도 나타납니다.

표시되는 사용자 데이터는 사용자의 테이블 보기에 표시되는 것과 동일합니다.

보안 침해 지표 섹션

이 섹션에 대한 정보는 다음을 참조하십시오.

- Cisco Secure Firewall Management Center 디바이스 구성 가이드의 보안 침해 지표
- 보안 침해 지표 데이터 필드, 948 페이지
- 단일 호스트 또는 사용자에 대한 보안 침해 지표 규칙 상태 수정, 949 페이지
- 보안 침해 지표 태그 해결, 950 페이지
- 보안 침해 지표 태그의 소스 이벤트 보기, 950 페이지

호스트 기록 섹션

호스트 기록은 사용자 활동의 마지막 24시간을 그래프로 보여줍니다. 사용자가 로그인하고 로그오프한 호스트의 IP 주소 목록은 막대 그래프로 로그인 시간과 로그아웃 시간의 근사치를 계산합니다. 일반 사용자는 하루에 수차례 호스트에 로그인 및 로그오프할 수 있습니다. 예를 들어, 메일 서버에 대한 정기적인 자동 로그인은 여러 개의 짧은 세션으로 표시되고, 좀 더 긴 로그인(예: 근무 시간 중)은 더 긴 세션으로 표시될 수 있습니다.

트래픽 기반 탐지 또는 캡티브 포털을 사용하여 실패한 로그인을 캡처하는 경우, 호스트 기록에는 사용자가 로그인에 실패한 호스트도 포함됩니다.

호스트 기록을 생성하는 데 사용된 데이터는 사용자 기록 데이터베이스에 저장됩니다. 이 데이터베이스에는 기본적으로 1,000만 개의 사용자 로그인 이벤트가 저장됩니다. 특정 사용자에 대한 호스트 기록에 데이터가 없는 경우, 사용자가 비활성 상태이거나 데이터베이스 한도를 늘려야 할 수 있습니다.

관련 항목

사용자 데이터 필드

사용자 상세정보 및 호스트 기록 보기

프로시저

다음 2가지 옵션을 사용할 수 있습니다.

- 사용자를 나열하는 이벤트 보기에서 사용자 ID 옆에 표시되는 사용자 아이콘 또는 보안 침해 지표에 연결된 사용자의 경우, 빨간색 사용자 아이콘을 클릭합니다.
- 사용자 워크플로에서 Users 종료 페이지를 클릭합니다.

검색 이벤트 작업 히스토리

표 ***113:***

기능	버전	세부 사항
취약점 페이지 변경	6.7	Bugtraq 및 취약점 데이터는 더 이상 사용할 수 없습니다. 다음과 같이 변경되었습니다. • 현재 대부분의 취약점 데이터는 NVD(National Vulnerability Database)에서 제공됩니다. • 사용되지 않는 필드와 중복된 필드가 제거되었습니다. • 새 CVE ID 열이 테이블 보기에 추가되었으며 새 심각도 필드가 테이블 및 세부 사항 페이지에 추가되었습니다. • 이제 테이블에서 CVE ID를 마우스 오른쪽 버튼으로 클릭하여 NVD의 취약점에 대한 세부 정보를 볼 수 있습니다. • 테이블의 취약점 영향 열의 이름이 Impact로 변경되었습니다. (세부 사항 보기의 필드 이름은 변경되지 않습니다.) • Analysis(분석) > Hosts(호스트) > Network Map(네트워크 맵) > Hosts(호스트)에서 호스트 프로파일의 취약점을 볼 때 취약점에 대한 세부 정보(타사 취약점 제외)는 새로운 필드 집합을 사용합니다. • Bugtraq 옵션이 Analysis(분석) > Hosts(호스트) > Network Map(네트워크 맵) > Vulnerabilities(취약점) 페이지의 취약점 옵션에서 제거되었습니다. 수정된 화면: • Analysis(분석)> Hosts(호스트)> Vulnerabilities(취약점) 아래의 모든 페이지 • Hosts and Vulnerabilities(호스트 및 취약점) 탭의 Analysis(분석)> Hosts(호스트)> Network Map(네트워크 맵) 페이지 지원되는 플랫폼: FMC

37 장

상관관계 및 컴플라이언스 이벤트

다음 주제에서는 상관관계 및 규정 준수 이벤트를 보는 방법을 설명합니다.

상관관계 이벤트 보기

활성 상관관계 정책 내 상관관계 규칙이 트리거되면 시스템은 상관관계 이벤트를 생성하고 이를 데이터베이스에 로깅합니다.

참고 활성 상관관계 정책 내 규정준수 허용 목록이 트리거되면 시스템은 허용 목록 이벤트를 생성합니다.

상관관계 이벤트의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

상관관계 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 상관관계 이벤트의 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자 또는 보안 분석가 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**) > Correlation(**상관관계**) > Correlation Events(**상관관계 이벤트**)** 을(를) 선택합니다.

원하는 경우, 맞춤형 워크플로 등 다른 워크플로를 사용하려면 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.

팁 상관관계 이벤트의 테이블 보기가 포함되지 않은 맞춤형 워크플로를 사용 중인 경우 **(switch workflow)(**워크플로 전환**)**를 클릭한 다음 **Correlation Events(**상관관계 이벤트**)**를 선택합니다.

단계 **2** 원하는 경우, 타임 윈도우 변경, 710 페이지에 설명된 대로 시간 범위를 조정합니다.

단계 **3** 다음 작업 중 하나를 수행합니다.

- 표시되는 열에 대한 자세한 내용은 상관관계 이벤트 필드, 985 페이지를 참조하십시오.
- IP 주소의 호스트 프로파일을 보려면 IP 주소 옆에 표시되는 호스트 프로파일을 클릭합니다.
- 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘 또는 IOC와 연결된 사용자라면 **Red User(**빨간색 사용자**)**를 클릭합니다.
- 이벤트를 정렬 및 제한하거나 현재 워크플로 페이지 내에서 이동하려면 워크플로 사용, 689 페이지를 참조하십시오.
- 현재 제약 조건을 유지하면서 현재 워크플로의 페이지 사이를 이동하려면 워크플로 페이지의 왼쪽 위에서 해당 페이지 링크를 클릭합니다.
- 워크플로의 다음 페이지로 드릴다운하여 특정 값으로 제한하려면 드릴다운 페이지 사용, 697 페이지를 참조하십시오.
- 일부 또는 모든 상관관계 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭하여 현재 제한된 보기의 모든 이벤트를 삭제하려 한다고 확인합니다.
- 다른 이벤트 보기로 이동해 연결된 이벤트를 보려면 워크플로 간 탐색, 716 페이지을 참조하십시오.
- Firepower 시스템 외부에서 이용할 수 있는 소스의 데이터를 보려면 이벤트 값에서 마우스 오른쪽 버튼으로 클릭합니다. 표시되는 옵션은 데이터 유형에 따라 다르며 공개 소스를 포함합니다. 다른 소스는 구성한 리소스에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지 섹션을 참조해 주십시오.
- 이벤트에 대한 인텔리전스를 수집하려면 테이블에서 이벤트 값을 마우스 오른쪽 버튼으로 클릭하고 Cisco 또는 서드파티 인텔리전스 소스에서 선택합니다. 예를 들어 Cisco Talos에서 의심스러운 IP 주소에 대한 상세정보를 얻을 수 있습니다. 표시되는 옵션은 데이터 유형 및 시스템에서 구성된 통합에 따라 달라집니다. 자세한 내용은 웹 기반 리소스를 사용한 이벤트 조사, 650 페이지를 참고하십시오.

관련 항목

데이터베이스 이벤트 제한 수, 60 페이지
워크플로 페이지, 693 페이지

상관관계 이벤트 필드

상관관계 규칙이 트리거되면 시스템은 상관관계 이벤트를 생성합니다. 다음 표는 상관관계 테이블에서 보고 검색할 수 있는 필드를 설명합니다.

표 ***114:*** 상관관계 이벤트 필드

필드	설명
설명	상관관계 이벤트의 설명. 설명의 정보는 규칙이 트리거된 방식에 따라 달라집니다. 예를 들어 규칙이 운영 체제 정보 업데이트 이벤트에 의해 트리거된 경우 새 운영 체제 이름 및 신뢰도 레벨이 나타납니다.
디바이스	정책 위반을 트리거한 이벤트를 생성한 디바이스의 이름.
도메인	모니터링되는 트래픽이 정책 위반을 트리거한 디바이스의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
영향	침입 데이터, 검색 데이터, 취약성 정보 간 상관관계를 기반으로 상관관계 이벤트에 할당되는 영향 레벨. 이 필드를 검색할 때 대소문자를 구분하지 않는 유효한 값은 `Impact 0`, `Impact Level 0`, `Impact 1`, `Impact Level 1`, `Impact 2`, `Impact Level 2`, `Impact 3`, `Impact Level 3`, `Impact 4`, `Impact Level 4`입니다. 영향 아이콘 색 이나 부분 문자열을 사용하지 마십시오(예를 들어 `blue`, `level 1` 또는`0`을 사용하지 마십시오).
Ingress Interface(인그레스 인터페이스) 또는 Egress Interface(이그레스 인터페이스)	정책 위반을 트리거한 침입 또는 연결 이벤트의 인그레스 또는 이그레스 인터페이스.
Ingress Security Zone(인그레스 보안 영역) 또는 Egress Security Zone(이그레스 보안 영역)	정책 위반을 트리거한 침입 또는 연결 이벤트의 인그레스 또는 이그레스 보안 영역.

필드	설명
인라인 결과	다음 중 하나에 해당합니다. • 검은색 아래쪽 화살표 - 시스템이 침입 규칙을 트리거한 패킷을 삭제했음을 나타냄 • 회색 아래쪽 화살표 - **Drop when Inline(**인라인 시 삭제**)** 침입 정책 옵션을 활성화했다면 시스템이 인라인, 스위치드 또는 라우티드 구축에서 패킷을 삭제했을 것임을 나타냄 • 공백 - 트리거된 침입 규칙이 Drop and Generate Events(이벤트 삭제 및 생성)으로 설정되지 않았음을 나타냄 이 필드를 사용하여 침입 이벤트에 의해 트리거되는 정책 위반을 검색할 때는 다음 중 하나를 입력합니다. • `dropped` - 패킷이 인라인, 스위치드 또는 라우티드 구축에서 삭제되었는지 여부를 지정 • `would have dropped` - 인라인, 스위치드 또는 라우티드 구축에서 패킷을 삭제하도록 침입 정책을 구성했다면 패킷이 삭제되었을 것인지를 지정 침입 정책의 규칙 상태 또는 삭제 동작과 상관없이, 인라인 집합이 탭 모드인 경우를 포함하여 패시브 구축에서는 시스템이 패킷을 삭제하지 않습니다.
정책	위반된 정책의 이름.
우선순위	트리거된 규칙 또는 위반된 상관관계 정책의 우선순위에 의해 결정되는 상관관계 이벤트의 우선순위. 이 필드를 검색할 때 우선순위가 없는 경우, `none`을 입력합니다.
규칙	정책 위반을 트리거한 규칙의 이름.
보안 인텔리전스 범주	정책 위반을 트리거한 이벤트에서 차단된 IP 주소를 나타내거나 포함하는 개체의 이름. 이 필드를 검색할 때 정책 위반을 트리거한 상관 관계 이벤트에 연결된 보안 인텔리전스 카테고리를 지정합니다. 보안 인텔리전스 카테고리는 보안 인텔리전스 개체의 이름, 전역 차단 목록, 맞춤형 보안 인텔리전스 목록이나 피드 또는 인텔리전스 피드의 카테고리 중 하나일 수 있습니다.
Source Continent 또는 Destination Continent	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트 IP 주소에 연결된 대륙.
Source Country 또는 Destination Country	정책 위반을 트리거한 이벤트에서 소스 또는 대상 IP 주소에 연결된 국가.
Source Host Criticality 또는 Destination Host Criticality	상관관계 이벤트와 관련된 소스 또는 대상 호스트에 사용자가 할당하는 호스트 중요도: `None`, `Low`, `Medium`, `High`. 검색 이벤트, 호스트 입력 이벤트 또는 연결 이벤트 기반의 규칙에 의해 생성된 상관관계 이벤트에만 소스 호스트 중요도가 포함됩니다.
Source IP 또는Destination IP	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트의 IP 주소.

필드	설명
Source Port/ICMP Type 또는 Destination Port/ICMP Code	정책 위반을 트리거한 이벤트에 연결된 소스 트래픽의 소스 포트 또는 ICMP 유형 또는 대상 트래픽의 대상 포트 또는 ICMP 코드.
Source User 또는 Destination User	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트에 로그인한 사용자의 이름.
시간	상관관계 이벤트가 생성된 날짜 및 시간. 이 필드는 검색할 수 없습니다.
개수	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 **Count(**개수**)** 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

관련 항목

이벤트 검색, 721 페이지

컴플라이언스 허용 목록 워크플로우 사용

management center에서는 네트워크에 대해 생성되는 허용 목록 이벤트 및 위반의 분석에 사용할 수 있는 워크플로우 집합을 제공합니다. 워크플로는 네트워크 맵 및 대시보드와 더불어 네트워크 자산의 규정 준수에 대한 핵심 정보 소스입니다.

시스템은 허용 목록 이벤트 및 위반에 대한 사전 정의된 워크플로우를 제공합니다. 사용자 지정 워크플로를 생성할 수도 있습니다. 규정 준수 허용 목록 워크플로우를 사용하면 여러 일반적인 작업을 수행할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 보안 분석가 또는 검색 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관 관계**)** 메뉴를 사용하여 허용 목록 워크플로우에 액세스합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 워크플로 전환 - 맞춤형 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.
- 시간 범위 - 시간 범위를 조정합니다. 이벤트가 표시되지 않는 경우에 유용합니다(타임 윈도우 변경, 710 페이지 참조).
- 호스트 프로파일 - IP 주소의 호스트 프로파일을 보려면 호스트 프로파일()을 클릭하거나 활성 IOC(Indication of Compromise) 태그가 있는 호스트의 경우에는 IP 주소 옆에 표시되는 보안 침해된 호스트를 클릭합니다.
- 사용자 프로파일(이벤트만 해당) - 사용자 ID 정보를 보려면 **User Identity(**사용자 **ID)** 옆에 표시되는 사용자 아이콘 또는 IOC와 연결된 사용자라면 **Red User(**빨간색 사용자**)**를 클릭합니다.

- 제한 - 표시되는 열을 제한하려면 숨기려는 열 머리글의 **Close(**닫기**)** (✕)을 클릭합니다. 표시되는 팝업 창에서 **Apply(**적용**)**를 클릭합니다.

  팁 다른 열을 숨기거나 표시하려면 **Apply(**적용**)**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 검색 제약 조건을 확장한 다음 Disabled Columns(비활성화된 열) 아래에서 열 이름을 클릭합니다.

- 드릴다운 - 드릴다운 페이지 사용, 697 페이지 참조.
- 정렬 - 워크플로의 데이터를 정렬하려면 열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.
- 이 페이지 탐색 - 워크플로 페이지 이동 툴, 695 페이지 참조.
- 페이지 간 이동 - 현재 제약 조건을 유지한 상태로 현재 워크플로의 페이지 간에 이동하려면, 워크플로 페이지의 왼쪽 상단에서 해당하는 페이지 링크를 클릭합니다.
- 이벤트 보기 간 이동 - 다른 이벤트 보기로 이동하여 연결된 이벤트를 보려면 **Jump to(**이동**)**를 클릭하고 드롭다운 목록에서 이벤트 보기를 선택합니다.
- 이벤트 삭제(이벤트만 해당) - 현재 제한된 보기에서 일부 또는 모든 항목을 삭제하려면 삭제할 항목 옆의 확인란을 선택한 다음 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭합니다.

관련 항목

워크플로 페이지, 693 페이지
이벤트 보기 구성, 210 페이지

허용리스트 이벤트 보기

최초 평가 후 시스템은 모니터링되는 호스트가 활성 허용리스트 규정준수에서 벗어날 때마다 허용리스트 이벤트를 생성합니다. 리스트는 특수한 종류의 상관관계 이벤트이며, management center 상관관계 이벤트 데이터베이스에 로깅됩니다.

management center를 사용하여 규정준수 허용리스트 이벤트의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

허용리스트 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로우에 따라 달라집니다. 이벤트의 테이블 보기에서 종료되는 미리 정의된 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

시작하기 전에

이 작업을 수행하려면 관리자, 보안 분석가 또는 검색 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > 허용 목록**Events(**이벤트**)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 기본 워크플로 작업을 수행하려면 컴플라이언스 허용 목록 워크플로우 사용, 987 페이지를 참조하십시오.
- 테이블의 열 내용을 자세히 알아보려면 허용 목록 이벤트 필드, 989 페이지를 참조하십시오.
- 더 많은 옵션을 보려면 테이블의 값을 마우스 오른쪽 버튼으로 클릭합니다.

허용 목록 이벤트 필드

워크플로를 사용하여 보고 검색할 수 있는 허용 목록 이벤트에는 다음 필드가 포함됩니다.

디바이스

허용 목록 위반을 탐지한 매니지드 디바이스의 이름입니다.

설명

허용 목록을 어떤 식으로 위반했는지 설명합니다. 예를 들면 다음과 같습니다.

클라이언트 “AOL Instant Messenger”는 허용되지 않습니다.

애플리케이션 프로토콜과 관련된 위반은 애플리케이션 프로토콜 이름과 버전은 물론 애플리케이션 프로토콜이 사용 중인 포트와 프로토콜(TCP 또는 UDP)을 나타냅니다. 금지를 특정 운영 체제로 제한할 경우, 설명에는 해당 운영 체제 이름이 포함됩니다. 예를 들면 다음과 같습니다.

서버 "ssh / 22 TCP (OpenSSH 3.6.1p2)"는 운영 체제 “Linux Linux 2.4 또는 2.6”에서 허용되지 않습니다.

도메인

허용 목록을 준수하지 않게 된 호스트의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

호스트 중요도

허용 목록을 준수하지 않는 소스 호스트에 대해 사용자가 할당하는 호스트 중요도(None, Low, Medium, High)입니다.

IP 주소

허용 목록을 준수하지 않게 된 호스트의 IP 주소.

정책

위반된 상관관계 정책의 이름입니다. 즉, 허용 목록이 포함된 상관관계 정책입니다.

포트

애플리케이션 프로토콜 허용 목록 위반(규정을 준수하지 않는 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 검색 이벤트에 연결된 포트. 다른 유형의 허용 목록 위반의 경우, 이 필드는 비어 있습니다.

우선순위

정책 또는 정책 위반을 트리거한 허용 목록에 의해 지정된 우선순위. 상관관계 정책의 허용 목록 우선 순위 또는 상관관계 정책 자체의 우선 순위에 의해 결정됩니다. 허용 목록 우선 순위는 해당 정책의 우선 순위를 재정의합니다. 이 필드를 검색할 때 우선 순위가 없는 경우, `none`을 입력합니다.

시간

허용 목록 이벤트가 생성된 시간 및 날짜입니다. 이 필드는 검색할 수 없습니다.

사용자

허용 목록을 준수하지 않게 된 호스트에 로그인한 알려진 사용자의 ID.

허용 목록

허용 목록의 이름입니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

허용리스트 위반 보기

시스템은 네트워크에서 현재 허용리스트 위반의 레코드를 유지합니다. 각 위반은 호스트 중 하나에서 허용되지 않는 것이 실행 중임을 나타냅니다. 호스트가 규정을 준수하게 되면 시스템은 이제 수정된 위반을 데이터베이스에서 제거합니다.

management center를 사용하여 모든 활성 허용리스트에 대한 허용리스트 위반 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

허용리스트 위반에 액세스할 때 표시되는 페이지는 사용하는 워크플로우에 따라 달라집니다. 사전 정의 워크플로는 제약 조건을 충족하는 모든 호스트의 호스트 프로파일이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > 허용 목록**Violations(**위반**)**을(를) 선택합니다.

단계 **2** 다음과 같은 옵션이 있습니다.

- 기본 워크플로 작업을 수행하려면 컴플라이언스 허용 목록 워크플로우 사용, 987 페이지를 참조하십시오.
- 테이블의 열 내용을 자세히 알아보려면 허용 목록 위반 필드, 991 페이지를 참조하십시오.
- 더 많은 옵션을 보려면 테이블의 값을 마우스 오른쪽 버튼으로 클릭합니다.

허용 목록 위반 필드

워크플로를 사용하여 보고 검색할 수 있는 허용 목록 위반에는 다음 필드가 포함됩니다.

도메인

규정을 준수하지 않는 호스트가 있는 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

정보

허용 목록 위반과 관련하여 제공되는 모든 공급업체, 제품 또는 버전 정보입니다. 허용 목록을 위반하는 프로토콜의 경우, 이 필드에는 위반이 네트워크 프로토콜로 인한 것인지 전송 프로토콜로 인한 것이지도 표시됩니다.

IP 주소

규정 준수 위반 호스트의 IP 주소입니다.

Port(포트**)**

애플리케이션 프로토콜 허용 목록 위반(규정을 준수하지 않는 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 이벤트에 연결된 포트입니다. 다른 유형의 허용 목록 위반의 경우, 이 필드는 비어 있습니다.

프로토콜

애플리케이션 프로토콜 허용 목록 위반(규정을 준수하지 않는 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 이벤트에 연결된 프로토콜. 다른 유형의 허용 목록 위반의 경우, 이 필드는 비어 있습니다.

시간

허용 목록 위반이 탐지된 시간 및 날짜입니다.

유형

허용 목록 위반의 유형입니다. 즉, 규정을 준수하지 않아 발생한 위반인지 나타냅니다.

- 운영제체(os) (이 필드를 검색할 때는 **os** 또는 **operating system**을 입력합니다.)
- 애플리케이션 프로토콜(서버)
- 클라이언트
- protocol
- 웹 애플리케이션(웹) (이 필드를 검색할 때는 **web application**을 입력합니다.)

허용 목록

위반된 허용 목록의 이름입니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

교정 상태 이벤트

교정이 트리거되면 시스템은 교정 상태 이벤트를 데이터베이스에 로깅합니다. 이러한 이벤트는 Remediation Status(교정 상태) 페이지에서 볼 수 있습니다. 교정 상태 이벤트를 검색하고 보고 삭제할 수 있습니다.

관련 항목

교정 상태 테이블 필드, 993 페이지

교정 상태 이벤트 보기

교정 상태 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 교정 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 테이블 보기에는 각 교정 상태 이벤트의 행이 포함됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > **Status(**상태**)**을(를) 선택합니다.

단계 **2** 원하는 경우, 타임 윈도우 변경, 710 페이지에 설명된 대로 시간 범위를 조정합니다.

단계 **3** 원하는 경우, 맞춤형 워크플로 등 다른 워크플로를 사용하려면 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)**를 클릭합니다.

팁 교정의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)** 메뉴를 클릭한 다음 **Remediation Status(**교정 상태**)**를 선택하십시오.

단계 **4** 다음과 같은 옵션이 있습니다.

- 표시되는 열에 대한 자세한 내용은 교정 상태 테이블 필드, 993 페이지를 참조하십시오.
- 이벤트를 정렬하고 제한하려면 워크플로 사용, 689 페이지를 참조하십시오.
- 상관관계 이벤트 보기로 이동해 연결된 이벤트를 보려면 **Correlation Events(**상관관계 이벤트**)**를 클릭합니다.
- 빠르게 돌아올 수 있도록 현재 페이지를 즐겨찾기하려면 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다. 즐겨찾기 관리 페이지로 이동하려면 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다.
- 테이블 보기의 데이터를 기반으로 보고서를 생성하려면 이벤트 보기에서 보고서 템플릿 생성, 546 페이지의 설명에 따라 **Report Designer(**리포트 디자이너**)**를 클릭합니다.
- 워크플로에서 다음 페이지로 드릴다운하려면 드릴다운 페이지 사용, 697 페이지 섹션을 참조하십시오.
- 시스템에서 교정 상태 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭하여 현재 제한된 보기의 모든 이벤트를 삭제하려 한다고 확인합니다.
- 교정 상태 이벤트를 검색하려면 **Search(**검색**)**를 클릭합니다.

관련 항목

워크플로 사용, 689 페이지

교정 상태 테이블 필드

다음 표는 교정 상태 테이블에서 보고 검색할 수 있는 필드를 설명합니다.

표 *115:* 교정 상태 필드

필드	설명
도메인	모니터링되는 트래픽이 정책 위반을 트리거한 다음 교정을 트리거한 디바이스의 도메인. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
정책	위반되어 교정을 트리거한 상관관계 정책의 이름.
리미디에이션 이름	실행된 교정의 이름.
결과 메시지	교정이 실행되었을 때 발생한 상황을 설명하는 메시지. 상태 메시지는 다음을 포함합니다. • 성공적으로 교정 완료 • 교정 모듈에 제공된 입력에 오류가 있음 • 교정 모듈 구성에 오류가 있음 • 원격 디바이스 또는 서버에 로그인할 때 오류 발생 • 원격 디바이스 또는 서버에 대한 필요한 권한을 얻을 수 없음 • 원격 디바이스 또는 서버에 로그인할 때 시간 초과 • 원격 명령 또는 서버를 실행할 때 시간 초과 • 원격 디바이스 또는 서버에 연결하지 못했음 • 교정을 시도했으나 실패했음 • 리미디에이션 프로그램을 실행하지 못함 • 알 수 없는/예기치 않은 오류 맞춤형 교정 모듈이 설치된 경우 맞춤형 모듈에 의해 구현되는 추가 상태 메시지를 볼 수 있습니다.
규칙	교정을 트리거한 상관관계 규칙의 이름입니다.
시간	management center가 교정을 트리거한 날짜 및 시간
개수	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

관련 항목

이벤트 검색, 721 페이지

교정 상태 이벤트 테이블 사용

이벤트 보기의 레이아웃을 변경하거나 보기의 이벤트를 필드 값으로 제한할 수 있습니다.

비활성화한 열은 나중에 다시 추가하지 않는 한 세션 기간 동안 비활성화됩니다. 첫 번째 열을 비활성화하면 Count(카운트) 열이 추가됩니다.

테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 않습니다.

팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 작업을 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Correlation(**상관관계**)** > **Status(**상태**)**을(를) 선택합니다.

팁 교정의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 워크플로 제목 옆에 있는 **(switch workflow)(**워크플로 전환**)** 메뉴를 클릭한 다음 **Remediation Status(**교정 상태**)**를 선택하십시오.

단계 **2** 다음과 같은 옵션이 있습니다.

- 표시되는 열에 대한 자세한 내용은 교정 상태 테이블 필드, 993 페이지를 참조하십시오.
- 이벤트를 정렬하고 제한하려면 워크플로 사용, 689 페이지를 참조하십시오.

IX 부

상관관계 및 컴플라이언스

38 장

컴플라이언스 목록

다음 주제에서는 상관관계 정책에 추가하기 전에 규정준수 허용리스트를 설정하는 방법을 설명합니다.

컴플라이언스 허용 목록 소개

줄여서 허용 목록이라고도 하는 컴플라이언스 허용 목록은 네트워크의 호스트에서 허용할 운영체제, 애플리케이션(웹 및 클라이언트)을 지정하는 기준 모음입니다. 호스트가 이 목록에 없으면 시스템은 이벤트(위반)를 생성합니다.

컴플라이언스 허용 목록은 다음과 같은 두 가지 주요 구성 요소로 이루어집니다.

- 대상은 컴플라이언스 평가를 위해 선택한 호스트입니다. 모니터링되는 전체 또는 일부 호스트를 서브넷, VLAN 및 호스트 속성으로 제한해 평가할 수 있습니다. 다중 도메인 구축의 경우에는 도메인과 도메인 내부 또는 사이에 있는 서브켓을 지정할 수 있습니다.
- 호스트 프로파일은 대상의 규정준수 기준을 지정합니다. 전역 호스트 프로파일은 운영체제의 구속을 받지 않습니다. 하나의 허용 목록에 국한되거나 여러 허용 목록이 공유하는 운영체제별 호스트 프로파일을 설정할 수도 있습니다.

Talos 인텔리전스 그룹은(는) 권장 설정을 적용한 기본 허용 목록을 제공합니다. 맞춤형 허용 목록을 만들 수도 있습니다. 단순 맞춤형 목록은 특정 운영체제를 실행하는 호스트만 허용할 수 있습니다. 더 복잡한 목록은 모든 운영체제를 허용할 수 있지만, 특정 포트에서 특정 애플리케이션 프로토콜을 실행하기 위해 호스트가 사용해야 하는 운영체제를 지정합니다.

참고 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.이러한 제한은 컴플라이언스 허용 목록을 작성하는 방법에 영향을 미칠 수 있습니다.

컴플라이언스 허용 목록 구현

허용 목록을 구현하려면 해당 목록을 활성 상관관계 정책에 추가해야 합니다. 시스템은 대상을 평가하고 모든 호스트를 대응하는 속성에 할당합니다.

- 규정준수 - 호스트가 해당 목록을 위반하지 않습니다.
- 규정 미준수 - 호스트가 해당 목록을 위반합니다.
- 미평가 - 호스트가 해당 목록의 대상이 아니거나, 호스트가 현재 평가 중이거나, 정보가 부족해 시스템이 호스트의 규정준수 여부를 판단할 수 없습니다.

참고 호스트 속성을 삭제하려면 해당 허용 목록을 삭제해야 합니다. 상관관계 정책에서 허용 목록을 비활성화, 삭제 또는 제거하더라도 호스트 속성은 삭제되지 않으며, 각 호스트에 대한 속성의 값도 변경되지 않습니다.

최초 평가가 끝나면 시스템은 모니터링되는 호스트가 활성 허용 목록에 대한 규정준수에서 벗어날 때마다 허용 목록 이벤트를 생성하며, 허용 목록 위반을 기록합니다.

워크플로우, 대시보드, 네트워크 맵을 이용해 시스템 전반의 규정준수 활동을 모니터링하여 개별 호스트가 허용 목록을 언제 어떻게 위반하는지 확인할 수 있습니다. 그러한 위반에 대해 교정과 알림으로 자동 응답할 수도 있습니다.

예: HTTP를 웹 서버에 제한

보안 정책이 웹 서버만 HTTP를 실행하도록 규정합니다. 웹 팜을 제외한 전체 네트워크를 평가하는 허용 목록을 생성하여 어떤 호스트가 HTTP를 실행 중인지 확인합니다.

네트워크 맵과 대시보그를 사용하여, 네트워크 규정준수 상태를 한 눈에 확인할 수 있습니다. 조직 내의 어떤 호스트가 정책을 위반한 상태로 HTTP를 실행 중인지 단 몇 초 만에 정확히 확인하고, 적절한 조치를 취할 수 있습니다.

그런 다음 상관관계 기능을 사용하면 웹 팜에 없는 호스트가 HTTP 실행을 시작할 때마다 사용자에게 알림이 전송되도록 시스템을 구성할 수 있습니다.

관련 항목

상관관계 정책 설정, 1019 페이지

컴플라이언스 허용 목록 대상 네트워크

대상 네트워크는 규정준수에 대해 평가할 호스트를 지정합니다. 허용리스트는 하나 이상의 대상 네트워크를 가질 수 있으며, 대상 기준을 충족하는 호스트를 평가합니다.

처음에는 대상 네트워크를 IP 주소 또는 범위로 제한합니다. 다중 도메인 구축의 경우, 최초 제한에는 도메인도 포함됩니다.

시스템이 제공하는 기본 허용리스트는 모니터링되는 모든 호스트, 즉 0.0.0.0/0과 ::/0을 지정합니다. 다중 도메인 구축의 경우, 기본 허용리스트는 전역 도메인으로 제한됩니다. 그리고 전역 도메인에서만 사용할 수 있습니다.

대상 네트워크나 호스트를 수정하여 호스트가 허용리스트의 유효한 대상이 되지 않게 하면 호스트는 해당 리스트로 평가되지 않으며 규정준수 또는 미준수로 간주되지 않습니다.

대상 네트워크 조사 및 개선

대상 네트워크를 허용리스트를 추가하는 경우, 시스템은 규정준수 호스트를 특성화할 수 있도록 네트워크 맵을 조사하라는 프롬프트를 표시합니다. 조사를 통해 조사 대상인 호스트를 나타내는 대상이 허용리스트에 추가됩니다.

서브넷 또는 개별 호스트를 조사할 수 있습니다. 다중 도메인 구축의 경우에는 전체 도메인을 조사하거나 여러 도메인에 걸쳐 조사를 진행할 수 있습니다. 상위 도메인을 조사하면 시스템은 해당 도메인의 하위 요소를 조사합니다.

추가한 대상 외에, 조사에서 탐지된 각 운영체제에 대해 하나의 호스트 프로파일과 허용리스트도 채웁니다. 이러한 호스트 프로파일은 해당 운영체제에서 탐지된 모든 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 허용합니다.

대상 네트워크 조사가 끝나면(또는 조사를 건너뛰면), 대상을 개선합니다. 호스트를 IP 주소를 기준으로 제외하거나, 대상 네트워크를 호스트 속성이나 VLAN을 기준으로 제한할 수 있습니다.

규정준수 허용리스트를 이용한 도메인 지정

다중 도메인 구축의 경우, 도메인과 대상 네트워크는 밀접하게 연결됩니다.

- 리프 도메인 관리자는 자신의 리프 도메인 내에서 호스트를 평가하는 허용리스트를 만들 수 있습니다.
- 상위 도메인 관리자가 도메인에 걸쳐 호스트를 평가하는 허용리스트를 생성할 수 있습니다. 동일한 허용 목록에서 다른 도메인에 있는 다른 서브넷을 대상으로 지정할 수 있습니다.

자신이 Global(전역) 도메인 관리자이며, 전체 구축의 웹 서버에 같은 규정준수 기준을 적용하는 상황을 고려해보십시오. 규정준수 기준을 정의하는 허용리스트를 전역 도메인에서 생성합니다. 그런 다음 각 리프 도메인에 있는 웹 서버의 IP 공간(또는 개별 IP 주소)을 지정하는 대상 네트워크를 이용하여 허용리스트를 제한합니다.

참고 리프 도메인의 IP 주소와 범위를 대상으로 지정할 수도 있지만, 상위 도메인을 이용해 대상 네트워크를 제한할 수도 있습니다. 상위 도메인에 있는 서브넷을 대상으로 지정하면 각 하위 리프 도메인의 같은 서브넷이 대상으로 지정됩니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

컴플라이언스 허용 목록 호스트 프로필

컴플라이언스 허용 목록에서 호스트 프로파일은 대상 호스트에서 실행할 수 있는 운영체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정합니다. 컴플라이언스 허용 목록에서는 3가지 유형의 호스트 프로파일을 사용할 수 있습니다. 각 유형은 규정준수 편집기에서 다르게 표시됩니다.

표 ***116:*** 컴플라이언스 허용 목록 호스트 프로파일 유형

호스트 프로파일 유형	모양	설명
전역글로벌	모든 운영체제	운영체제에 상관없이 대상 호스트에서 실행할 수 있는 요소를 지정
운영체제 한정	일반 텍스트로 나열됨	특정 운영체제의 대상 호스트에서 실행할 수 있는 요소를 지정
공유됨	기울임꼴로 나열	여러 허용 리스트에서 사용할 수 있는 운영체제 기준을 지정

운영 체제별 호스트 프로파일

규정준수 허용 목록에서 운영체제 한정 호스트 프로파일은 네트워크에서 실행할 수 있는 운영체제뿐만 아니라, 해당 운영체제에서 실행할 수 있는 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜을 나타냅니다.

예를 들어 규정준수 호스트가 특정 버전의 Microsoft Windows를 실행하도록 요구할 수 있습니다. 다른 예로, SSH가 포트 22의 Linux 호스트에서 실행되도록 허용하고 SSH 클라이언트의 벤더와 버전을 추가로 제한할 수 있습니다.

네트워크에서 허용하려는 각 운영체제에 대한 하나의 호스트 프로파일을 생성합니다. 네트워크에서 특정 운영체제를 허용하지 않으려면, 해당 운영체제에 대한 호스트 프로파일을 생성하지 마십시오. 예를 들어 네트워크의 모든 호스트가 Windows를 실행하게 하려면, 허용 목록에 해당 운영체제에 대한 호스트 프로파일만 포함되도록 구성하십시오.

참고 확인되지 않은 호스트는 확인될 때까지 모든 허용 목록을 준수하는 상태로 유지됩니다. 그러나 알 수 없는 호스트에 대한 허용 목록 호스트 프로파일을 생성할 수 있습니다. *Unidentified(*미확인*)* 호스트는 시스템이 해당 호스트의 운영체제를 식별하기 위한 충분한 정보를 아직 수집하지 못한 호스트입니다. *Unknown(*알 수 없는*)* 호스트는 운영체제가 알려진 핑거프린트와 일치하지 않는 호스트입니다.

공유 호스트 프로파일

규정준수 허용리스트에서 공유 호스트 프로파일은 특정 운영체제에 연결되지만, 각 공유 호스트 프로파일을 두 개 이상의 허용리스트에서 사용할 수 있습니다.

예를 들어, 전 세계에 지사가 있고 각 위치에 별도의 허용리스트를 적용하지만, Apple Mac OS X를 실행하는 모든 호스트에 동일한 프로파일을 사용하려면 해당 운영체제에 대한 공유 프로파일을 생성하고 이를 모든 허용리스트에 사용할 수 있습니다.

기본 허용리스트는 내장형 호스트 프로파일이라고 하는 특수 카테고리의 공유 호스트 프로파일을 사용합니다. 이러한 프로파일은 내장된 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜 및 클라이언트를 사용합니다. 규정준수 허용리스트 편집기에서 시스템은 이러한 프로파일에 내장 호스트 프로파일 아이콘을 표시합니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 공유 호스트 프로파일을 표시하며, 이러한 규칙은 편집할 수 있습니다. 상위 도메인의 공유 호스트 프로파일도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 공유 호스트 프로파일을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 공유 호스트 프로파일(내장된 프로파일 포함)을 수정하거나 내장된 애플리케이션 프로토콜, 프로토콜 또는 클라이언트를 수정하는 경우, 변경사항은 이를 사용하는 모든 허용리스트에 영향을 미칩니다. 의도하지 않은 변경사항을 적용하거나 내장된 요소를 삭제했다면, 공장 기본값으로 재설정할 수 있습니다.

허용 위반 트리거

호스트의 허용리스트 규정준수는 시스템이 다음 작업을 할 때 변경할 수 있습니다.

- 호스트 운영체제의 변경 사항을 탐지한 경우
- 호스트의 운영체제 또는 호스트에 있는 애플리케이션 프로토콜의 ID 충돌을 탐지한 경우
- 호스트에서 새 TCP 서버 포트(예: SMTP 또는 웹 서버에서 사용된 포트)가 활성화되었거나, 호스트에서 새 UDP 서버가 실행 중인 것을 탐지한 경우
- 호스트에서 실행 중인 것으로 검색된 TCP 또는 UDP 서버의 변경 사항을 탐지한 경우(예: 업그레이드로 인한 버전 변경)
- 호스트를 실행하는 새 클라이언트나 웹 애플리케이션을 탐지한 경우

- 비활성 상태인 클라이언트나 웹 애플리케이션을 데이터베이스에서 삭제하는 경우
- 새 네트워크 또는 전송 프로토콜과 통신하는 호스트를 탐지한 경우
- 새 탈옥 모바일 디바이스를 탐지한 경우
- 시스템에서 종료되거나 시간 초과된 TCP 또는 UDP 포트를 탐지한 경우

이와 더불어, 호스트 입력 기능 또는 호스트 프로파일을 사용하여 호스트의 규정준수 변경을 트리거할 수 있습니다.

- 호스트에 클라이언트, 프로토콜 또는 서버 추가
- 호스트에서 클라이언트, 프로토콜 또는 서버 삭제
- 호스트의 운영체제 정의 설정
- 해당 호스트가 더 이상 유효 대상이 되지 않도록 호스트의 호스트 속성 변경

참고 이벤트 과잉을 방지하기 위해, 시스템은 최초 평가 시에는 규정 미준수 호스트에 대한 허용리스트 이벤트를 생성하지 않으며, 활성 허용리스트 또는 공유 호스트 프로파일을 수정해도 호스트는 규정 미준수가 되지 않습니다. 그러나 위반 사항은 계속 기록됩니다. 모든 규정 미준수 대상에 대한 허용리스트 이벤트를 생성하려면 검색 데이터를 비웁니다. 네트워크 자산을 재검색하면 허용리스트 이벤트가 트리거될 수도 있습니다.

운영체제 규정준수

네트워크에서 Microsoft Windows 호스트만 허용하도록 허용리스트를 지정할 경우, 시스템에서는 Mac OS X를 실행하는 호스트를 탐지하며 허용리스트 이벤트를 생성합니다. 또한 허용리스트와 연결된 호스트 속성은 해당 호스트에 대해 Compliant(규정준수)에서 Non-Compliant(규정 미준수)로 변경됩니다.

이 예시에 나온 호스트의 상태가 규정준수로 돌아가려면 다음 중 하나를 수행해야 합니다.

- Mac OS X 운영체제를 허용하도록 허용리스트 편집
- 호스트의 운영체제 정의를 Microsoft Windows로 수동으로 변경
- 운영체제가 Microsoft Windows로 다시 변경된 사실을 시스템에서 탐지함

네트워크 맵에서 규정 미준수 자산 삭제

허용리스트에서 FTP 사용이 허용되지 않고 사용자가 애플리케이션 프로토콜 네트워크 맵 또는 이벤트 보기에서 FTP를 삭제할 경우, FTP를 실행하는 호스트는 규정준수를 상태가 됩니다. 그러나 애플리케이션 프로토콜이 다시 탐지될 경우, 시스템에서는 허용리스트 이벤트를 생성하며 호스트는 규정준수 위반 상태가 됩니다.

완전한 정보에서만 트리거

허용리스트가 포트 21의 TCP FTP 트래픽만 허용하며 시스템이 포트 21/TCP에서의 불확정 활동을 탐지하면 허용리스트는 트리거하지 않습니다. 허용리스트는 시스템이 트래픽을 FTP가 아닌 다른 무언가로 식별하거나, 사용자가 호스트 입력 기능을 이용하여 트래픽을 비 FTP 트래픽으로 지정하는 경우에만 트리거합니다. 시스템은 부분적인 정보만 있는 위반은 기록하지 않습니다.

컴플라이언스 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

컴플라이언스 허용 목록 생성

규정준수 허용 목록을 생성하는 경우, 시스템은 최초 대상을 생성하고 규정준수 호스트 속성을 설명할 수 있도록 네트워크를 조사하라는 프롬프트를 표시합니다.

프로시저

단계 **1** 허용 목록을 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** 새로 만들기허용 목록를 클릭합니다.

단계 **3** 선택적으로, 최초 대상 네트워크의 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**를 입력합니다. 다중 도메인 구축인 경우에는 대상 네트워크가 상주하는 **Domain(**도메인**)**을 선택합니다.

팁 전체 모니터링된 네트워크를 조사하려면, 기본값 0.0.0.0/0 및 ::/0을 사용합니다.

참고 대상 네트워크의 도메인은 선택이 끝나면 변경할 수 없습니다. 상위 도메인에 있는 서브넷을 대상으로 지정하면 각 하위 리프 도메인의 같은 서브넷이 대상으로 지정됩니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **4** 대상 네트워크 추가:

- Add(추가) - 조사하지 않고 대상 네트워크를 추가하려면 **Add(**추가**)**를 클릭합니다.
- Add and Survey Network(추가 및 네트워크 조사) - 대상 네트워크를 추가하고 조사하려면 **Add and Survey Network(**네트워크 추가 및 조사**)**를 클릭합니다.
- Skip(건너뛰기) - 네트워크를 조사하지 않고 허용 목록을 생성하려면 **Skip(**건너뛰기**)**을 클릭합니다.

단계 **5** 선택적으로, 허용 목록의 새 **Name(**이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **6** 선택적으로, 네트워크에서 탈옥 모바일 디바이스를 허용합니다. 이 옵션을 비활성화하면 탈옥한 디바이스가 허용 목록 위반을 생성할 수 있습니다.

단계 **7** 규정준수 허용 목록에 대한 대상 네트워크 설정, 1007 페이지에 설명된 대로 하나 이상의 **Target Network(**대상 네트워크**)**를 허용 목록에 추가합니다.

단계 **8** **Allowed Host Profiles(**허용되는 호스트 프로파일**)**을 이용해 규정준수 호스트의 특성 설명:

- Global Host Profile(전역 호스트 프로파일) - 허용 목록의 전역 호스트 프로파일을 편집하려면 **Any Operating System(**모든 운영체제**)**을 클릭하고 허용 리스트 호스트 프로필 빌드, 1008 페이지에 설명된 대로 진행합니다.
- Edit Surveyed Profiles(조사한 프로파일 편집) - 네트워크 조사로 생성한 기존 운영체제 한정 호스트 프로파일을 편집하려면, 해당 프로파일의 이름을 클릭하고 허용 리스트 호스트 프로필 빌드, 1008 페이지에 설명된 대로 진행합니다.
- Create New Profiles(새 프로파일 생성) - 이 허용 목록에 대한 새로운 운영체제 한정 호스트 프로파일을 생성하려면, **Allowed Host Profiles(**허용되는 호스트 프로파일**)** 옆에 있는 **Add(**추가**)** (+)을 클릭하고 허용 리스트 호스트 프로필 빌드, 1008 페이지에 설명된 대로 진행합니다.
- Add Shared Host Profile(공유 호스트 프로파일 추가) - 기존 공유 호스트 프로파일을 허용 목록에 추가하려면, **Add Shared Host Profile(**공유 호스트 프로파일 추가**)**을 클릭하고 추가할 공유 호스트 프로파일을 선택한 다음 **OK(**확인**)**를 클릭합니다. 공유 호스트 프로파일은 기울임꼴로 표시됩니다.

단계 **9** **Save(**저장**)**허용 목록를 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 설정, 1019 페이지에 설명된 대로 활성 상관관계 정책에 허용 목록을 추가합니다. 시스템은 허용 목록 평가와 위반 생성을 즉시 시작합니다.

관련 항목

컴플라이언스 허용 목록 대상 네트워크, 1001 페이지
선택한 호스트를 기반으로 컴플라이언스 허용 목록 생성, 943 페이지
Firepower System IP 주소 규칙, 28 페이지

규정준수 허용 목록에 대한 대상 네트워크 설정

대상 네트워크를 추가할 때 해당 네트워크를 조사해 규정준수 호스트의 특성을 설명할 수 있습니다. 조사에서 탐지된 각 운영체제에 대해 하나의 호스트 프로파일과 허용 목록을 채웁니다. 이러한 호스트 프로파일은 해당 운영 체제에서 탐지된 모든 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 허용합니다.

프로시저

단계 **1** 규정준수 허용 목록 편집기에서 **Add Target Network(**대상 네트워크 추가**)**를 클릭합니다.

단계 **2** 대상 네트워크의 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**를 입력합니다.

단계 **3** 다중 도메인 구축인 경우에는 대상 네트워크가 상주하는 **Domain(**도메인**)**을 선택합니다.

참고 대상 네트워크의 도메인은 선택이 끝나면 변경할 수 없습니다. 상위 도메인에 있는 서브넷을 대상으로 지정하면 각 하위 리프 도메인의 같은 서브넷이 대상으로 지정됩니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **4** 대상 네트워크 추가:

- Add(추가) - 조사하지 않고 대상 네트워크를 추가하려면 **Add(**추가**)**를 클릭합니다.
- Add and Survey Network(추가 및 네트워크 조사) - 대상 네트워크를 추가하고 조사하려면 **Add and Survey Network(**네트워크 추가 및 조사**)**를 클릭합니다.

단계 **5** 선택적으로, 추가 설정할 새 대상을 클릭합니다.

- Name(이름) - 새 **Name(**이름**)**을 입력합니다.
- Add Networks(네트워크 추가) - 추가 호스트를 대상으로 지정하려면, **Add(**추가**)** (+)을 클릭하고 **IP Address(IP** 주소**)**와 **Netmask(**넷마스크**)**를 입력합니다. 네트워크를 허용 목록 규정준수에서 제외하려면, **Exclude(**제외**)**를 선택합니다.
- Add Host Attributes(호스트 속성 추가) - 호스트를 특정 호스트 속성과 함께 대상으로 지정하려면, **Add(**추가**)** (+)을 클릭하고 **Attribute(**속성**)**와 그 **Value(**값**)**를 지정합니다.
- Add VLANs(VLAN 추가) - VLAN을 대상으로 지정하려면 **Add(**추가**)** (+)을 클릭하고 (802.1q VLAN에 대한) VLAN 번호를 입력합니다.
- Delete(삭제) — 대상 제한을 제거하려면 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **6** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

관련 항목

컴플라이언스 허용 목록 대상 네트워크, 1001 페이지

Firepower System IP 주소 규칙, 28 페이지

허용 리스트 호스트 프로필 빌드

호스트 프로파일은 허용 리스트의 규정준수 기준, 즉 대상 호스트에서 실행할 수 있는 운영체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정합니다.

모든 허용 리스트에는 운영체제에 구속되지 않는 전역 호스트 프로파일이 있습니다. 예를 들어 여러 개의 Microsoft Windows 및 Linux 호스트 프로파일을 수정하는 대신 Mozilla Firefox를 허용하려면, Firefox가 탐지되는 운영체제에 상관없이 Firefox를 허용하도록 전역 호스트 프로파일을 구성할 수 있습니다.

개별 허용 리스트에 국한되거나 여러 허용 리스트가 공유하는 운영체제 한정 호스트 프로파일을 설정할 수도 있습니다.

참고 공유 호스트 프로파일(내장된 프로파일 포함)을 수정하거나 내장된 애플리케이션 프로토콜, 프로토콜 또는 클라이언트를 수정하는 경우, 변경사항은 이를 사용하는 모든 허용리스트에 영향을 미칩니다. 의도하지 않은 변경사항을 적용하거나 내장된 요소를 삭제했다면, 공장 기본값으로 재설정할 수 있습니다.

시작하기 전에

- 컴플라이언스 허용 목록 편집, 1012 페이지에 설명된 대로 허용내에서 호스트 프로파일을 생성 또는 편집하거나, 공유 호스트 프로파일 관리, 1014 페이지에 설명된 대로 공유 호스트 프로파일을 생성 또는 편집합니다.

프로시저

단계 **1** 규정준수 허용 리스트 호스트 프로파일 편집기에서 호스트 프로파일을 설정합니다.

- Name(이름) - **Name(**이름**)**을 입력합니다.
- Operating System(운영체제) - 호스트 프로파일을 특정 운영체제에 제한하려면, **OS Vendor(**운영체제 벤더**)**, **OS Name(**운영체제 이름**)**, **Version(**버전**)** 드롭다운 목록을 이용합니다. 운영체제 종류에 상관없이 운영체제를 실행하는 모든 호스트에 적용하는 것이 목표이므로, 전역 호스트 프로파일을 제한할 수는 없습니다.
- Application Protocol(애플리케이션 프로토콜) - 애플리케이션 프로토콜을 허용하려면 **Add(**추가**)** (+) 을 클릭하고 컴플라이언스 허용 목록에 애플리케이션 프로토콜 추가, 1009 페이지에 설명된 대로 진행합니다.
- Client(클라이언트) - 클라이언트를 허용하려면 **Add(**추가**)** (+) 을 클릭하고 컴플라이언스 허용 목록에 클라이언트 추가, 1010 페이지에 설명된 대로 진행합니다.

- Web Application(웹 애플리케이션) - 웹 애플리케이션을 허용하려면 **Add(추가)** (+) 을 클릭하고 컴플라이언스 허용 목록에 웹 애플리케이션 추가, 1010 페이지에 설명된 대로 진행합니다.
- Protocol(프로토콜) - 프로토콜을 허용하려면 **Add(추가)** (+) 을 클릭하고 컴플라이언스 허용 목록에 프로토콜 추가, 1011 페이지에 설명된 대로 진행합니다.
- Delete(삭제) - 이전에 허용한 항목을 허용하지 않으려면 아이콘(**Delete(삭제)** ( ))을 클릭합니다.
- Edit Properties(속성 편집) - 허용되는 애플리케이션 프로토콜, 클라이언트 또는 프로토콜의 속성을 편집하려면 해당 요소의 이름을 클릭합니다. 변경사항은 해당 요소를 사용하는 모든 호스트 프로파일에 반영됩니다.

팁 적절한 **Allow all...(모두 허용...)** 확인란을 선택해 이 프로파일과 일치하는 호스트에 대한 모든 애플리케이션 프로토콜, 클라이언트 또는 웹 애플리케이션을 허용합니다.

단계 **2** 마지막으로 저장한 이후 적용된 모든 변경사항을 즉시 구현하려면 **Save(저장)**허용 목록(공유 호스트 프로파일을 편집하는 경우에는 **Save All Profiles(모든 프로파일 저장)**)를 클릭합니다.

컴플라이언스 허용 목록에 애플리케이션 프로토콜 추가

허용 리스트 호스트 프로파일을 사용하면 애플리케이션 프로토콜을 전역적으로, 또는 특정 운영체제에서만 허용할 수 있습니다. 선택적으로, 애플리케이션 프로토콜을 포트, 벤더 또는 버전으로 제한할 수도 있습니다. 예를 들어 OpenSSH 특정 버전이 포트 22/TCP의 Linux 호스트에서 실행되도록 허용할 수 있습니다.

프로시저

단계 **1** 컴플라이언스 허용 리스트 호스트 프로파일을 생성하거나 수정할 경우, **Allowed Application Protocols(허용되는 애플리케이션 프로토콜)**(전역 호스트 프로파일을 수정할 경우에는 **Globally Allowed Application Protocols(전역적으로 허용되는 애플리케이션 프로토콜)**) 옆에 있는 **Add(추가)** (+)를 클릭합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 허용할 애플리케이션 프로토콜이 목록에 있다면 해당 프로토콜을 선택합니다. 웹 인터페이스는 허용 목록이 허용해 왔거나 현재 허용하는 애플리케이션 프로토콜을 나열합니다.
- 목록에 없는 애플리케이션 프로토콜을 허용하려면, **<New Application Protocol>**을 선택하고 **OK(확인)**를 클릭하여 애플리케이션 프로토콜 편집기를 표시합니다. 허용할 애플리케이션 프로토콜 **Type(유형)**과 **Protocol(프로토콜)**을 선택합니다. 선택적으로, 애플리케이션 프로토콜을 포트, **Vendor(벤더)**, **Version(버전)**으로 제한합니다.

  참고 애플리케이션의 테이블 보기에 표시되는 벤더와 버전을 정확하게 입력해야 합니다. 벤더 또는 버전을 지정하지 않을 경우, 허용 목록에서는 유형 및 프로토콜이 매칭될 때까지 모든 벤더와 버전을 허용합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

컴플라이언스 허용 목록에 클라이언트 추가

허용 목록 호스트 프로파일을 사용하면 클라이언트를 전역적으로 또는 특정 운영체제에서만 허용할 수 있습니다. 선택적으로, 클라이어트가 특정 버전이길 요청할 수 있습니다. 예를 들어 Microsoft Internet Explorer 10에서만 Microsoft Windows 호스트를 실행하도록 허용할 수 있습니다.

프로시저

단계 **1** 컴플라이언스 허용 리스트 호스트 프로파일을 생성하거나 수정할 경우 **Allowed Clients(**허용되는 클라이언트**)**(전역 호스트 프로파일을 수정할 경우에는 **Globally Allowed Clients(**전역적으로 허용되는 클라이언트**)**) 옆에 있는 **Add(**추가**)** (+)를 클릭합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 허용할 클라이언트가 목록에 있다면 해당 클라이언트를 선택합니다. 웹 인터페이스는 허용이 허용해 왔거나 현재 허용하는 클라이언트를 나열합니다.
- 목록에 없는 클라이언트를 허용하려면 **<New Client>**를 선택하고 **OK(**확인**)**를 클릭해 클라이언트 편집기를 표시합니다. 드롭다운 목록에서 허용할 **Client(**클라이언트**)**를 선택하고, 원한다면 클라이언트를 허용되는 **Version(**버전**)**에 제한합니다.

  참고 클라이언트의 테이블 보기에 표시되는 버전을 정확하게 입력해야 합니다. 버전을 지정하지 않으면 모든 버전이 허용됩니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

컴플라이언스 허용 목록에 웹 애플리케이션 추가

허용리스트 호스트 프로파일을 사용하면 웹 애플리케이션을 전역적으로, 또는 특정 운영체제만 허용할 수 있습니다.

프로시저

단계 **1** 규정준수 허용리스트 호스트 프로파일을 생성하거나 수정할 경우, **Allowed Web Applications(**허용되는 웹 애플리케이션**)**(전역 호스트 프로파일을수정할 경우에는 **Globally Allowed Web Applications(**전역적으로 허용되는 웹 애플리케이션**)**) 옆에 있는 **Add(**추가**)** (+)를 클릭합니다.

단계 **2** 허용할 웹 애플리케이션을 선택합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

컴플라이언스 허용 목록에 프로토콜 추가

허용리스트 호스트 프로파일을 사용하면 프로토콜을 전역적으로, 또는 특정 운영체제에서만 허용할 수 있습니다. ARP, IP, TCP, UDP는 항상 모든 호스트에서 허용되며 해당 프로토콜은 허용하지 않을 수 없습니다.

프로시저

단계 **1** 허용리스트 호스트 프로파일을 생성하거나 수정할 경우, **Allowed Protocols(**허용되는 프로토콜**)**(전역 호스트 프로파일을 수정할 경우에는 **Globally Allowed Protocols(**전역적으로 허용되는 프로토콜**))** 옆에 있는 **Add(**추가**)** (+)를 클릭합니다.

단계 **2** 다음 2가지 옵션을 사용할 수 있습니다.

- 허용할 프로토콜이 목록에 있다면 해당 프로토콜을 선택합니다. 웹 인터페이스는 허용되어 왔거나 허용리스트가 현재 허용하는 프로토콜을 나열합니다.
- 목록에 없는 프로토콜을 허용하려면, **<New Protocol>**을 선택하고 **OK(**확인**)**를 클릭하여 프로토콜 편집기를 표시합니다. **Type(**유형**)** 드롭다운 목록에서 프로토콜 유형**(Network(**네트워크**)** 또는 **Transport(**전송**))**을 선택하고, 드롭다운 목록에서 **Protocol(**프로토콜**)**을 선택합니다.

  팁 **Other (manual entry)(**기타**(**수동 입력**)**를 선택하여 목록에 없는 프로토콜을 지정합니다. 네트워크 프로토콜의 경우, http://www.iana.org/assignments/ethernet-numbers/에 나열된 적합한 번호를 입력합니다. 전송 프로토콜의 경우, http://www.iana.org/assignments/protocol-numbers/에 나열된 적합한 번호를 입력합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

컴플라이언스 허용 목록 관리

허용List(화이트리스트) 페이지를 이용하여 규정준수 허용리스트와 공유 호스트 프로파일을 관리할 수 있습니다. 기본 허용리스트는 권장 설정을 표시하며 내장형 호스트 프로파일이라고 하는 특수 범주의 공유 호스트 프로파일을 사용합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 규정준수 허용리스트를 표시하며, 이러한 리스트는 수정할 수 있습니다. 상위 도메인의 선택된 허용리스트도 표시되지만, 이는 편집할 수 없습니다. 하위 도메인에서 생성된 허용리스트를 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 상위 도메인의 컨피그레이션이 이름, 매니지드 디바이스 등 관련이 없는 도메인에 대한 정보를 표시하는 경우 상위 도메인의 컨피그레이션은 표시되지 않습니다. 기본 허용리스트는 전역 도메인에서만 사용할 수 있습니다.

프로시저

단계 **1** 허용 목록을 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** 다음과 같이 규정준수 허용리스트를 관리합니다.

- Create(생성) - 새 허용리스트를 생성하려면 **New(**신규**)**허용 목록를 클릭하고 컴플라이언스 허용 목록 생성, 1005 페이지에 설명된 대로 진행합니다.
- Delete(삭제) - 사용하지 않는 허용리스트를 삭제하려면 **Delete(**삭제**)** ( )를 클릭하고 허용리스트 삭제 여부를 확인합니다. 허용리스트를 삭제하면 관련된 호스트 속성이 네트워크의 모든 호스트에서 제거됩니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- Edit(편집) - 기존 허용리스트를 수정하려면 **Edit(**수정**)** ( )을 클릭하고 컴플라이언스 허용 목록 편집, 1012 페이지에 설명된 대로 진행합니다. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- Shared Host Profiles(공유 호스트 프로파일) - 허용리스트의 공유 호스트 프로파일을 관리하려면 **Edit Shared Profiles(**공유 프로파일 편집**)**를 클릭하고 공유 호스트 프로파일 관리, 1014 페이지에 설명된 대로 진행합니다.

컴플라이언스 허용 목록 편집

활성 상관관계 정책에 포함된 규정준수 허용 목록을 수정하고 저장하는 경우, 시스템은 허용 목록의 대상 네트워크에 있는 호스트의 규정준수 여부를 즉시 다시 평가합니다. 이러한 재평가로 인해 일부 호스트의 상태가 규정준수 또는 규정 미준수로 바뀔 수 있으나, 시스템은 어떤 허용 목록 이벤트도 생성하지 않습니다.

프로시저

단계 **1** 허용 목록을 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** 수정할 허용 목록 옆의 **Edit(**수정**)** ( )를 클릭합니다.

View(보기**)** ()이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 규정준수 허용 목록 편집:

- Name and Description(이름 및 설명) - 이름이나 설명을 변경하려면 왼쪽 패널에서 허용 목록 이름을 클릭해 기본 허용 목록 정보를 표시한 다음 새 정보를 입력합니다.
- Allow Jailbroken Devices(탈옥 디바이스 허용) - 네트워크에서 탈옥 모바일 디바이스를 허용하려면, 왼쪽 패널에서 허용 목록 이름을 클릭해 기본 허용 목록 정보를 표시하고 **Allow Jailbroken Mobile Devices(**탈옥 모바일 디바이스 허용**)**를 활성화합니다. 이 옵션을 비활성화하면 탈옥한 디바이스가 허용 목록 위반을 생성할 수 있습니다.
- Add Allowed Host Profile(허용되는 호스트 프로파일 추가) - 허용 목록에 대한 운영체제 한정 호스트 프로파일을 생성하려면, Allowed Host Profiles(허용되는 호스트 프로파일) 옆에 있는 **Add(**추가**)** ()을 클릭하고 허용 리스트 호스트 프로필 빌드, 1008 페이지에 설명된 대로 진행합니다.
- Add Shared Host Profile(공유 호스트 프로파일 추가) - 기존 공유 호스트 프로파일을 허용 목록에 추가하려면, **Add Shared Host Profile(**공유 호스트 프로파일 추가**)**을 클릭하고 추가할 공유 호스트 프로파일을 선택한 다음 **OK(**확인**)**를 클릭합니다. 공유 호스트 프로파일은 기울임꼴로 표시됩니다.
- Add Target Network(대상 네트워크 추가) - 호스트 조사 없이 새 대상 네트워크를 추가하려면, Target Networks(대상 네트워크) 옆에 있는 **Add(**추가**)** ()을 클릭하고 규정준수 허용 목록에 대한 대상 네트워크 설정, 1007 페이지에 설명된 대로 진행합니다.
- Delete Host Profile(호스트 프로파일 삭제) - 공유 또는 운영체제 한정 호스트 프로파일을 허용 목록에서 삭제하려면, 호스트 프로파일 옆에 있는 **Delete(**삭제**)** ()을 클릭하고 선택을 확인합니다. 공유 호스트 프로파일을 삭제하면 허용 목록에서 해당 프로파일이 제거되지만, 이를 사용하는 다른 허용 목록의 해당 프로파일은 삭제 또는 제거되지 않습니다. 허용 목록의 전역 호스트 프로파일은 삭제할 수 없습니다.
- Delete Target Network(대상 네트워크 삭제) - 대상 네트워크를 허용 목록에서 제거하려면, 네트워크 옆에 있는 **Delete(**삭제**)** ()을 클릭하고 선택을 확인합니다.
- Edit Global Host Profile(전역 호스트 프로파일 편집) - 허용 목록의 전역 호스트 프로파일을 편집하려면 **Any Operating System(**모든 운영체제**)**을 클릭하고 허용 리스트 호스트 프로필 빌드, 1008 페이지에 설명된 대로 진행합니다.
- Edit Other Host Profile(기타 호스트 프로파일 편집) - 공유 또는 운영체제 한정 호스트 프로파일을 편집하려면, 호스트 프로파일의 이름을 클릭하고 허용 리스트 호스트 프로필 빌드, 1008 페이지에 설명된 대로 진행합니다.
- Edit Target Network(대상 네트워크 편집) - 대상 네트워크를 편집하려면, 네트워크의 이름을 클릭하고 규정준수 허용 목록에 대한 대상 네트워크 설정, 1007 페이지에 설명된 대로 진행합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경 사항을 즉시 구현하려면 **Save(**저장**)**허용 목록를 클릭합니다.

공유 호스트 프로파일 관리

규정준수 허용리스트에서 공유 호스트 프로파일은 특정 운영체제에 연결되지만, 각 공유 호스트 프로파일을 두 개 이상의 허용리스트에서 사용할 수 있습니다. 여러 개의 허용리스트를 생성하지만 동일한 호스트 프로파일을 사용하여 허용리스트 전반에 걸쳐 특정 운영체제를 실행하는 호스트를 평가하려는 경우, 공유 호스트 프로파일을 사용합니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 공유 호스트 프로파일을 표시하며, 이러한 규칙은 편집할 수 있습니다. 상위 도메인의 공유 호스트 프로파일도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 공유 호스트 프로파일을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 공유 호스트 프로파일(내장된 프로파일 포함)을 수정하거나 내장된 애플리케이션 프로토콜, 프로토콜 또는 클라이언트를 수정하는 경우, 변경사항은 이를 사용하는 모든 허용리스트에 영향을 미칩니다. 의도하지 않은 변경사항을 적용하거나 내장된 요소를 삭제했다면, 공장 기본값으로 재설정할 수 있습니다.

프로시저

단계 **1** 허용 목록을 선택하고 **Policies(**정책**)** > **Correlation(**상관관계**)**를 클릭합니다.

단계 **2** **Edit Shared Profiles(**공유 프로파일 편집**)**를 클릭합니다.

단계 **3** 공유 호스트 프로파일 관리:

- Create Shared Host Profile(공유 호스트 프로파일 생성) - 호스트를 점검하지 않고 새 공유 호스트 프로파일을 생성하려면 Shared Host Profiles(공유 호스트 프로파일) 옆에 있는 **Add(**추가**)** ( )를 클릭하고 허용 리스트 호스트 프로필 빌드, 1008 페이지에 설명된 대로 진행합니다.
- Create Shared Host Profile by Survey(조사를 통해 공유 호스트 프로파일 생성) - 네트워크를 조사해 여러 새 공유 호스트 프로파일을 생성하려면, **Add Target Network(**대상 네트워크 추가**)**를 클릭하고 규정준수 허용 목록에 대한 대상 네트워크 설정, 1007 페이지에 설명된 대로 진행합니다.
- Delete(삭제) - 공유 호스트 프로파일을 삭제하려면 **Delete(**삭제**)** ( )를 클릭하고 선택을 확인합니다.
- Edit(편집) - 기존 공유 호스트 프로파일(내장된 공유 호스트 프로파일 포함)을 수정하려면, 이름을 클릭하고 허용 리스트 호스트 프로필 빌드, 1008 페이지에 설명된 대로 진행합니다.
- Reset Built-In Host Profiles(내장 호스트 프로파일 재설정) - 모든 내장 호스트 프로파일을 공장 기본값으로 재설정하려면, **Built-in Host Profiles(**내장 호스트 프로파일**)**를 클릭하고 **Reset to Factory Defaults(**공장 기본값으로 재설정**)** 를 클릭한 다음 선택을 확인합니다.

단계 **4** 마지막으로 저장한 이후 적용된 모든 변경사항을 즉시 구현하려면, **Save All Profiles(**모든 프로파일 저장**)**를 클릭합니다.

39 장

상관관계 정책

다음 주제에서는 상관관계 정책과 규칙을 설정하는 방법을 설명합니다.

상관관계 정책 및 규칙 소개

상관관계 기능을 이용하면 상관관계 정책을 바탕으로 네트워크에 대한 위협에 실시간으로 반응할 수 있습니다.

상관관계 정책 위반은 네트워크 상의 활동이 활성 상관관계 정책 내의 상관관계 규칙이나 규정준수 허용 목록을 트리거할 때 발생합니다.

상관관계 규칙

활성 상관관계 정책에서 상관관계 규칙이 트리거되면, 시스템은 상관관계 이벤트를 생성합니다. 상관관계 규칙은 다음 조건이 충족될 때 트리거됩니다.

- 시스템이 특정 유형의 이벤트(연결, 침입, 악성코드, 검색, 사용자 활동 등)를 생성합니다.
- 네트워크 트래픽이 자체 일반 프로파일에서 벗어납니다.

다음 방법으로 상관관계 규칙을 제한할 수 있습니다.

- 트리거링 이벤트와 관련된 호스트의 호스트 프로파일에서 정보를 사용하여 규칙을 제한하려면 호스트 프로파일 자격을 추가합니다.
- 규칙의 초기 기준이 충족된 후 시스템이 특정 연결 추적을 시작할 수 있도록 하려면 상관관계 규칙에 연결 추적기를 추가합니다. 그러면 추적된 연결이 추가 조건을 충족하는 경우에만 상관관계 이벤트가 생성됩니다.

- 특정 사용자 또는 사용자 그룹을 추적하려면 상관관계 규칙에 사용자 자격을 추가합니다. 예를 들어 특정 사용자의 트래픽 또는 특정 부서의 트래픽에 대해서만 트리거하도록 상관관계 규칙을 제한할 수 있습니다.
- 스누즈 기간을 추가합니다. 상관관계 규칙이 트리거될 때, 스누즈 기간 때문에 규칙이 지정된 간격 동안 다시 트리거되지 않을 수도 있습니다. 유휴 기간이 경과하면 규칙을 다시 트리거하고 새 스누즈 기간을 시작할 수 있습니다.
- 비활성 기간을 추가합니다. 비활성 기간 중에는 상관관계 규칙이 트리거되지 않습니다.

구축을 허가받지 않고도 상관과계 규칙을 구성할 수 있지만, 허가받지 않은 구성 요소를 사용하는 규칙은 트리거되지 않습니다.

컴플라이언스 허용 목록

규정준수 허용 목록은 네트워크에서 허용할 운영체제, 애플리케이션(웹 및 클라이언트), 프로토콜을 지정합니다. 호스트가 활성 상관관계 정책에서 사용하는 허용 목록을 위반하는 경우, 시스템은 허용 목록 이벤트를 생성합니다.

상관관계 응답

상관관계 정책 위반에 대한 응답은 단순 알림 및 다양한 교정(호스트 스캔 등)을 포함합니다. 각 상관관계 규칙 또는 허용 리스트를 단일 응답 또는 응답 그룹에 연결할 수 있습니다.

네트워크 트래픽이 여러 규칙 또는 허용 리스트를 트리거하는 경우 각 규칙 및 허용 리스트와 연결된 모든 응답이 시작됩니다.

상관관계 및 멀티 테넌시

다중 도메인 구축의 경우, 각 도메인 레벨에서 사용 가능한 규칙, 허용 목록과 응답을 이용해 어떤 도메인 수준에서도 상관관계 정책을 생성할 수 있습니다. 상위 도메인 관리자는 도메인 내부 또는 도메인 간에서 상관관계를 수행할 수 있습니다.

- 도메인을 이용한 상관관계 규칙 제한은 해당 도메인의 하위 항목에서 보고하는 이벤트와 일치합니다.
- 상위 도메인 관리자는 도메인 간의 호스트를 평가하는 규정준수 허용 목록을 생성할 수 있습니다. 동일한 허용 목록에서 다른 도메인에 있는 다른 서브넷을 대상으로 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 일반적인 설정(IP 주소, VLAN 태그, 사용자 이름 등)으로 도메인 간 상관관계 규칙을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

관련 항목

컴플라이언스 허용 목록 소개, 999 페이지
Secure Firewall Management Center 알림 응답, 569 페이지
교정 소개, 1071 페이지

컴플라이언스 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자

상관관계 정책 설정

상관관계 규칙, 규정준수 허용리스트, 알림 응답 및 교정을 사용하여 상관관계 정책을 만듭니다.

다중 도메인 구축의 경우에는, 각 도메인 레벨에서 사용 가능한 구성 요소 설정을 이용해 어떤 도메인 수준에서도 상관관계 정책을 생성할 수 있습니다.

각 상관관계 정책에, 그리고 해당 정책에서 사용하는 각 규칙과 허용리스트에 우선순위를 할당할 수 있습니다. 규칙 및 허용리스트 우선순위는 상관관계 정책 우선순위를 재정의합니다. 네트워크 트래픽이 상관관계 정책을 위반하는 경우, 그에 따른 상관관계 이벤트는 위반한 규칙이나 허용리스트에 자체 우선순위가 없다면 정책 우선순위 값을 표시합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택합니다.

단계 **2** **Create Policy(**정책 생성**)**를 클릭합니다.

단계 **3** **Policy Name(**정책 이름**)** 및 **Policy Desription(**정책 설명**)**을 입력합니다.

단계 **4** **Default Priority(**기본 우선순위**)** 드롭다운 목록에서 정책의 우선순위를 선택합니다. 규칙 우선순위만 사용하려면 **None(**없음**)**을 선택합니다.

단계 **5** **Add Rules(**규칙 추가**)**를 클릭하고, 정책에서 사용할 규칙 및 허용리스트를 확인한 다음 **Add(**추가**)**를 클릭합니다.

단계 **6** 각 규칙 또는 허용리스트의 **Priority(**우선순위**)** 목록에서 우선순위를 선택합니다.

- 1~5의 운선순위 값
- **None**
- **Default(**기본**)** - 정책의 기본 우선순위 사용

단계 **7** 규칙 및 허용 리스트에 응답 추가, 1020 페이지에 설명된 대로 규칙 및 허용리스트에 응답을 추가합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 슬라이더를 클릭하여 정책을 활성화합니다.

규칙 및 허용 리스트에 응답 추가

각 상관관계 규칙 또는 허용 리스트를 단일 응답 또는 응답 그룹에 연결할 수 있습니다. 네트워크 트래픽이 여러 규칙 또는 허용 리스트를 트리거하는 경우 각 규칙 및 허용 리스트와 연결된 모든 응답이 시작됩니다. 트래픽 프로파일 변경에 대한 응답으로 사용되는 경우에는 Nmap 치료가 시작되지 않습니다.

다중 도메인 구축에서는 현재 도메인 또는 상위 도메인에서 생성된 응답을 사용할 수 있습니다.

프로시저

단계 **1** 상관관계 정책 편집기에서 응답을 추가하려는 규칙 또는 허용 목록 옆에 있는 응답()를 클릭합니다.

단계 **2** Unassigned Responses(미할당 응답) 아래에서 규칙 또는 허용 리스트가 트리거될 때 시작할 응답을 선택하고 위로 화살표(^)를 클릭합니다.

단계 **3** **Update(**업데이트**)**를 클릭합니다.

관련 항목

Secure Firewall Management Center 알림 응답, 569 페이지
교정 소개, 1071 페이지

상관관계 정책 관리

활성 상관관계 정책에 적용된 변경사항은 즉시 적용됩니다.

상관관계 정책을 활성화하면, 시스템은 즉시 이벤트를 처리하고 응답을 트리거합니다. 시스템은 최초, 활성화 이후 평가에서는 규정 미준수 호스트에 대한 허용리스트 이벤트를 생성하지 않습니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 상관관계 정책을 표시하며, 이러한 정책은 편집할 수 있습니다. 상위 도메인의 선택된 상관관계 정책도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 상관관계 정책을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 상위 도메인의 컨피그레이션이 이름, 매니지드 디바이스 등 관련이 없는 도메인에 대한 정보를 표시하는 경우 상위 도메인의 컨피그레이션은 표시되지 않습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택합니다.

단계 **2** 상관관계 정책 관리:

- Activate(활성화) 또는 Deactivate(비활성화) - 슬라이더를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 생성 - **Create Policy(**정책 생성**)**를 클릭합니다(상관관계 정책 설정, 1019 페이지 참조).
- 편집 - **Edit(**수정**)** ( )을 클릭합니다. 상관관계 정책 설정, 1019 페이지의 내용을 참조하십시오. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 삭제 - **Delete(**삭제**)** ( )을(를) 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

상관관계 규칙 설정

단순한 상관관계 규칙은 특정 유형의 이벤트 발생만 요구합니다. 그 이상의 상세 조건은 입력하지 않아도 됩니다. 예를 들어 트래픽 프로파일 변경 기반의 상관관계 규칙에는 조건이 전혀 필요하지 않습니다. 여러 조건이 적용되며 제한이 추가된 복잡한 상관관계 규칙을 만들 수도 있습니다.

상관관계 규칙 트리거 기준, 호스트 프로파일 자격, 사용자 자격 또는 연결 추적기를 생성할 때 구문은 각기 다르지만 원리는 동일합니다.

참고 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 이벤트와 일치하는 상위 도메인을 기준으로 상관관계 규칙을 제한합니다.

시작하기 전에

- 구축이 상관관계 이벤트를 트리거하는 데 사용할 정보 유형을 수집하고 있는지 확인합니다. 예를 들어 개별 연결 또는 연결 요약 이벤트에 사용 가능한 정보는 탐지 방법, 로깅 방법, 이벤트 유형 등 여러 요인에 따라 달라집니다. 시스템에서는 내보낸 NetFlow 기록에서 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. NetFlow와 매니지드 디바이스 데이터의 차이점의 내용을 참조하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Rule Management(**규칙 관리**)**을 클릭합니다.

단계 **2** **Create Rule(**규칙 생성**)**을 클릭합니다.

단계 **3** **Rule Name(**규칙 이름**)** 및 **Rule Description(**규칙 설명**)**을 입력합니다.

단계 **4** 원한다면 규칙에 대한 **Rule Group(**규칙 그룹**)**을 선택합니다.

단계 **5** 기본 이벤트 유형을 선택하고, 원한다면 상관관계 규칙에 대한 추가 트리거 기준을 지정합니다. 다음 기본 이벤트 유형을 선택할 수 있습니다.

- 침입 이벤트 발생 - 침입 이벤트 트리거 기준 구문, 1023 페이지 섹션을 참조하십시오.
- 악성 코드 이벤트 발생 - 악성코드 이벤트 트리거 기준 구문, 1026 페이지 섹션을 참조하십시오.
- 검색 이벤트 발생 - 검색 이벤트 트리거 기준 구문, 1027 페이지 섹션을 참조하십시오.
- 사용자 활동 탐지됨 - 사용자 활동 이벤트 트리거 기준 구문, 1030 페이지 섹션을 참조하십시오.
- 호스트 입력 이벤트 발생 - 호스트 입력 이벤트 트리거 기준 구문, 1031 페이지 섹션을 참조하십시오.
- 연결 이벤트 발생 - 연결 이벤트 트리거 기준 구문, 1032 페이지 섹션을 참조하십시오.
- 트래픽 프로파일 변경사항 - 트래픽 프로파일 변경 구문, 1036 페이지 섹션을 참조하십시오.

단계 **6** 선택적으로, 다음 중 하나 또는 전부를 추가해 상관관계 규칙을 추가로 제한합니다.

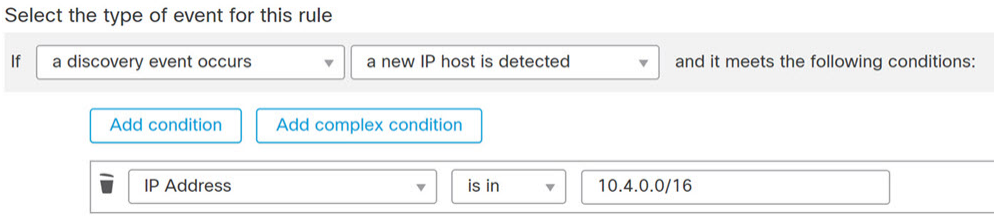
- 호스트 프로파일 자격 - **Add Host Profile Qualification(**호스트 프로파일 자격 추가**)**을 클릭합니다(상관관계 호스트 프로파일 자격 구문, 1038 페이지 참조).
- 연결 추적기 - **Add Connection Tracker(**연결 추적기 추가**)**를 클릭합니다(연결 추적기, 1042 페이지 참조).
- 사용자 자격 - **Add User Qualification(**사용자 자격 추가**)**을 클릭합니다(사용자 자격 구문, 1041 페이지 참조).
- 스누즈 기간 - Rule Options(규칙 옵션)에서 **Snooze(**스누즈**)** 텍스트 필드와 드롭다운 목록을 이용해 시스템에 규칙 트리거 후 상관관계 규칙을 다시 트리거할 때까지 기다려야 하는 기간을 정의합니다.
- 비활성 기간 - Rule Options(규칙 옵션)에서 **Add Inactive Period(**비활성 기간 추가**)**를 클릭합니다. 텍스트 필드와 드롭다운 목록을 사용하여, 시스템이 상관관계 규칙에 대한 네트워크 트래픽 평가를 억제하도록 할 시기와 빈도를 지정합니다.

팁 유휴 기간을 제거하려면 간격을 **0**으로 지정합니다(초, 분 또는 시간).

단계 **7** **Save Rule(**규칙 저장**)**을 클릭합니다.

단순 상관관계 규칙 예시

다음의 단순 상관관계 규칙은 특정 서브넷에서 새 호스트가 탐지되면 트리거됩니다. 카테고리가 IP 주소를 나타낼 때 **is in** 또는 **is not in**을 연산자로 선택하면, IP 주소가 CIDR 등의 특수 표기법으로 표현된 IP 주소 블록에서 *is in* 상태인지 *is not in* 상태인지를 지정할 수 있습니다.



다음에 수행할 작업

- 상관관계 정책 설정, 1019 페이지에 설명된 대로 상관관계 정책의 규칙을 사용합니다.

관련 항목

상관관계 규칙 관리, 1053 페이지
상관관계 규칙 빌드 메커니즘, 1050 페이지
스누즈 및 비활성 기간, 1050 페이지
NetFlow와 매니지드 디바이스 데이터의 차이점

침입 이벤트 트리거 기준 구문

다음 표에서는 기본 이벤트로 침입 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***117:*** 침입 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
액세스 제어 정책	침입 이벤트를 생성한 침입 정책을 사용하는 액세스 컨트롤 정책을 하나 이상 선택합니다.
액세스 제어 규칙 이름	침입 이벤트를 생성한 침입 정책을 사용하는 액세스 컨트롤 규칙의 이름 전체 또는 일부를 입력합니다.
애플리케이션 프로토콜	침입 이벤트와 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
분류	하나 이상의 분류를 선택합니다.
클라이언트	침입 이벤트와 관련된 클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	침입 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
목적지 IP, 소스 IP, 소스 IP 및 목적지 IP 모두, 또는 소스 IP 나 목적지 IP	단일 IP 주소 또는 주소 블록을 입력합니다.
대상 포트/ICMP 코드 또는 소스 포트/ICMP 유형	소스 트래픽의 포트 번호나 ICMP 코드 또는 대상 트래픽의 포트 번호나 ICMP 유형을 입력합니다.
디바이스	이벤트를 생성했을 가능성이 있는 디바이스를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
Egress Interface(이그레스 인터페이스) 또는 Ingress Interface(인그레스 인터페이스)	하나 이상의 인터페이스를 선택합니다.
Egress Security Zone(이그레스 보안 영역) 또는 Ingress Security Zone(인그레스 보안 영역)	보안 영역 또는 터널 영역을 하나 이상 선택합니다.
생성자 ID	전처리기를 하나 이상 선택합니다.
영향 플래그	침입 이벤트에 할당된 영향 레벨을 선택합니다. NetFlow 데이터에서 네트워크 맵에 추가되는 호스트에 대해서는 운영 체제 정보가 제공되지 않으므로 시스템은 이러한 호스트와 관련된 침입 이벤트에 대해 취약함(영향 레벨 1: 빨강) 영향 레벨을 할당할 수 없습니다. 이러한 경우에는 호스트 입력 기능을 사용하여 호스트에 대한 운영 체제 ID를 수동으로 설정합니다.
인라인 결과	침입 정책 위반에 따라 시스템이 패킷을 삭제했는지 또는 삭제할 가능성이 있는지를 선택합니다. 시스템은 인라인, 스위치드 또는 라우티드 구축의 패킷을 삭제할 수 있습니다. 침입 규칙 상태나 침입 정책의 삭제 작업에 상관없이, 수동 구축(인라인 설정이 탭 모드에 있는 경우 포함)에서는 패킷을 삭제하지 않습니다.
침입 정책	침입 이벤트를 생성한 침입 정책을 하나 이상 선택합니다.
IOC 태그	침입 이벤트의 결과로 침해 지표 태그가 설정되었는지를 선택합니다.
우선순위	규칙 우선순위를 선택합니다. 규칙 기반 침입 이벤트의 경우 우선순위는 `priority` 키워드의 값 또는 `classtype` 키워드의 값에 해당합니다. 기타 침입 이벤트의 경우, 우선순위는 디코더 또는 프리프로세서에 의해 결정됩니다.

다음을 지정할 경우...	연산자를 선택하고...
프로토콜	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.
규칙 메시지	규칙 메시지의 전체 또는 일부를 입력합니다.
규칙 SID	단일 Snort ID(SID) 또는 쉼표로 구분된 여러 SID를 입력합니다. 연산자로 **is in** 또는 **is not in**을 선택하는 경우 다중 선택 팝업 윈도우를 사용할 수 없습니다. 쉼표로 구분된 SID 목록을 입력해야 합니다.
규칙 유형	규칙이 로컬인지를 지정합니다. 로컬 규칙에는 맞춤형 표준 텍스트 침입 규칙, 수정된 표준 텍스트 규칙, 수정된 헤더 정보와 함께 규칙을 저장했을 때 생성된 공유 개체 규칙의 새 인스턴스가 포함됩니다.
SSL 실제 작업	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 선택합니다.
SSL 인증서 핑거프린트	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL 인증서 주체 일반 이름(CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL 인증서 주체 국가(C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL 인증서 주체 조직(O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL 인증서 주체 조직 단위(OU)	세션 암호화에 사용된 인증서의 주체 조직 단위 이름 전체 또는 일부를 입력합니다.
SSL 흐름 상태	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
사용자 이름	침입 이벤트의 소스 호스트에 로그인한 사용자의 사용자 이름을 입력합니다.
VLAN ID	침입 이벤트를 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID를 입력합니다.
웹 애플리케이션	침입 이벤트와 관련된 웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

침입 이벤트 필드, 810 페이지
Firepower System IP 주소 규칙, 28 페이지

악성코드 이벤트 트리거 기준 구문

악성코드 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 악성코드 이벤트의 유형을 지정해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 중에서 선택할 수 있습니다.

- **by endpoint-based malware detection(**엔드포인트 기반 악성코드 탐지 이용**)**(엔드포인트용 AMP를 이용한 탐지)
- **by network-based malware detection(**네트워크 기반 악성코드 탐지 이용**)**(네트워크용 AMP를 이용한 탐지)
- **by retrospective network-based malware detection(**회귀적 네트워크 기반 악성코드 탐지 이용**)**(네트워크용 AMP를 이용한 회귀적 탐지)

다음 표에서는 기본 이벤트로 악성코드 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***118:*** 악성코드 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
애플리케이션 프로토콜	악성코드 이벤트와 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트	악성코드 이벤트와 관련된 클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	악성코드 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.
목적지 IP, 호스트 IP 또는 소스 IP	단일 IP 주소 또는 주소 블록을 입력합니다.
대상 포트/ICMP 코드	대상 트래픽의 포트 번호 또는 ICMP 코드를 입력합니다.
속성	**Malware(**악성코드**)**나 **Custom Detection(**맞춤형 탐지**)** 중 하나 또는 둘 다를 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
이벤트 유형	엔드포인트용 AMP가 탐지한 악성코드 이벤트와 관련된 이벤트 유형을 하나 이상 선택합니다.
파일 이름	파일의 이름을 입력합니다.

다음을 지정할 경우...	연산자를 선택하고...
파일 유형	파일 형식을 선택합니다.
파일 유형 카테고리	파일 유형 카테고리를 하나 이상 선택합니다.
IOC 태그	악성코드 이벤트의 결과로 침해 지표 태그가 **is** 또는 **is not**으로 설정되었는지를 선택합니다.
SHA-256	파일의 SHA-256 해시 값을 입력하거나 붙여넣습니다.
SSL 실제 작업	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 선택합니다.
SSL 인증서 핑거프린트	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL 인증서 주체 일반 이름(CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL 인증서 주체 국가(C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL 인증서 주체 조직(O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL 인증서 주체 조직 단위(OU)	세션 암호화에 사용된 인증서의 주체 조직 단위 이름 전체 또는 일부를 입력합니다.
SSL 흐름 상태	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
소스 포트/ICMP 유형	소스 트래픽의 포트 번호 또는 ICMP 유형을 입력합니다.
웹 애플리케이션	악성코드 이벤트와 관련된 웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

파일 및 악성코드 이벤트 필드, 863 페이지
Firepower System IP 주소 규칙, 28 페이지

검색 이벤트 트리거 기준 구문

검색 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 검색 이벤트의 유형을 지정해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 표는 선택할 수 있는 검색 이벤트 유형을 나열합니다.

홉이 변경되는 경우 또는 호스트 제한에 도달하여 시스템이 새 호스트를 삭제하는 경우에는 상관관계 규칙을 트리거할 수 없습니다. 그러나 유형과 상관없이 검색 이벤트가 발생할 때 규칙을 트리거하려면 **there is any type of event(**아무 유형의 이벤트가 존재함**)**를 선택합니다.

표 ***119:*** 상관관계 규칙 트리거 기준 대 검색 이벤트 유형

옵션 선택	이 검색 이벤트 유형 사용
클라이언트가 변경됨	클라이언트 업데이트
클라이언트의 시간이 초과됨	클라이언트 시간 초과
호스트 IP 주소 재사용됨	DHCP: IP 주소 재할당
호스트 한도에 도달하여 호스트가 삭제됨	호스트 삭제됨: 호스트 한도 도달함
호스트가 네트워크 장치로 식별됨	네트워크 디바이스로 호스트 유형 변경됨
호스트의 시간이 초과됨	호스트 시간 초과
호스트 IP 주소가 변경됨	DHCP: IP 주소 변경됨
NETBIOS 이름 변경이 탐지됨	NETBIOS 이름 변경
새 클라이언트가 탐지됨	새 클라이언트
새 IP 호스트가 탐지됨	새 호스트
새 MAC 주소가 탐지됨	호스트에 대해 추가 MAC 탐지됨
새 MAC 호스트가 탐지됨	새 호스트
새 네트워크 프로토콜이 탐지됨	새 네트워크 프로토콜
새 전송 프로토콜이 탐지됨	새 전송 프로토콜
aTCP 포트가 닫힘	TCP 포트 닫힘
TCP 포트의 시간이 초과됨	TCP 포트 시간 초과
UDP 포트가 닫힘	UDP 포트 닫힘
UDP 포트의 시간이 초과됨	UDP 포트 시간 초과
VLAN 태그가 업데이트됨	VLAN 태그 정보 업데이트
IOC가 설정됨	보안 침해 지표
열린 TCP 포트가 탐지됨	새 TCP 포트
열린 UDP 포트가 탐지됨	새 UDP 포트
호스트에 대한 OS 정보가 변경됨	새 OS
호스트에 대한 OS 또는 서버 ID에 충돌이 발생함	ID 충돌
호스트에 대한 OS 또는 서버 ID의 시간이 초과됨	ID 시간 초과

옵션 선택	이 검색 이벤트 유형 사용
아무 유형의 이벤트가 존재함	아무 이벤트 유형
MAC 주소에 대한 새 정보가 있음	MAC 정보 변경
TCP 서버에 대한 새 정보가 있음	TCP 서버 정보 업데이트
UDP 서버에 대한 새 정보가 있음	UDP 서버 정보 업데이트

다음 표에서는 기본 이벤트로 검색 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***120:*** 검색 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
애플리케이션 프로토콜	애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
애플리케이션 포트	애플리케이션 프로토콜 포트 번호를 입력합니다.
클라이언트	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
클라이언트 버전	클라이언트의 버전 번호를 입력합니다.
디바이스	검색 이벤트를 생성했을 가능성이 있는 장치를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
하드웨어	모바일 디바이스의 하드웨어 모델을 입력합니다. 예를 들어 일치하는 모든 Apple iPhone을 찾으려면 **`iPhone`**을 입력합니다.
호스트 유형	호스트 유형을 하나 이상 선택합니다. 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.
IP 주소 또는 새 IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다.
탈옥됨	이벤트의 호스트가 탈옥 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
MAC 주소	호스트의 MAC 주소 전체 또는 일부를 입력합니다. 예를 들어 특정 하드웨어 제조업체 디바이스의 MAC 주소가 0A:12:34로 시작하는 것을 알고 있다면 연산자로 **begins with**를 선택하고 값으로 **`0A:12:34`**를 입력할 수 있습니다.

다음을 지정할 경우...	연산자를 선택하고...
MAC 유형	MAC 주소가 **ARP/DHCP Detected**인지 여부를 선택합니다. 즉 시스템에서 MAC 주소를 호스트에 속한 것(**ARP/DHCP Detected**)으로 확실하게 식별했는지, 또는 매니지드 디바이스와 호스트 간에 라우터가 있다는 등의 이유로 여러 호스트가 해당 MAC 주소를 갖는지(**is not ARP/DHCP Detected**) 여부를 선택합니다.
MAC 벤더	검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 하드웨어 벤더 이름 전체 또는 일부를 입력합니다.
모바일	이벤트의 호스트가 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
NETBIOS 이름	호스트의 NetBIOS 이름을 입력합니다.
네트워크 프로토콜	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
OS 이름	운영체제 이름을 하나 이상 선택합니다.
OS 벤더	운영체제 벤더를 하나 이상 선택합니다.
OS 버전	운영체제 버전을 하나 이상 선택합니다.
프로토콜 또는전송 프로토콜	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.
소스	(운영체제와 서버 ID의 변경 및 시간 초과에 대한) 호스트 입력 데이터의 소스를 선택합니다.
소스 유형	(운영체제와 서버 ID의 변경 및 시간 초과에 대한) 호스트 입력 데이터의 소스 유형을 선택합니다.
VLAN ID	이벤트와 관련된 호스트 VLAN ID를 입력합니다.
웹 애플리케이션	웹 애플리케이션을 선택합니다.

관련 항목

검색 이벤트 유형, 929 페이지
검색 이벤트 필드, 936 페이지
Firepower System IP 주소 규칙, 28 페이지

사용자 활동 이벤트 트리거 기준 구문

사용자 활동의 상관관계 규칙에 기반을 두려면, 먼저 사용할 사용자 활동의 유형을 선택해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 중에서 선택할 수 있습니다.

- 새 사용자 **ID**가 탐지됨
- 사용자가 호스트에 로그인함

다음 표에서는 기본 이벤트로 사용자 활동 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***121:*** 사용자 활동 구문

다음을 지정할 경우...	연산자를 선택하고...
디바이스	사용자 활동을 탐색했을 가능성이 있는 디바이스를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다.
사용자 이름	사용자 이름을 입력합니다.

관련 항목

사용자 활동 데이터 필드

Firepower System IP 주소 규칙, 28 페이지

호스트 입력 이벤트 트리거 기준 구문

호스트 입력 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 호스트 입력 이벤트의 유형을 지정해야 합니다. 사용자의 선택에 따라 사용할 수 있는 트리거 기준 집합이 결정됩니다. 다음 표는 선택할 수 있는 호스트 입력 이벤트 유형을 나열합니다.

사용자 정의 호스트 속성의 정의를 추가, 삭제 또는 변경할 때나 취약성 영향 자격을 설정할 때는 상관관계 규칙을 트리거할 수 없습니다.

표 ***122:*** 상관관계 규칙 트리거 기준 호스트 입력 이벤트 유형

옵션 선택	이 이벤트 유형에서 규칙을 트리거
클라이언트가 추가됨	클라이언트 추가
클라이언트가 삭제됨	클라이언트 삭제
호스트가 추가됨	호스트 추가
프로토콜이 추가됨	프로토콜 추가
프로토콜이 삭제됨	프로토콜 삭제
스캔 결과가 추가됨	스캔 결과 추가
서버 정의가 설정됨	서버 정의 설정
서버가 추가됨	포트 추가

옵션 선택	이 이벤트 유형에서 규칙을 트리거
서버가 삭제됨	포트 삭제
취약성이 유효하지 않음으로 표시됨	취약성 설정 유효하지 않음
취약성이 유효함으로 표시됨	취약성 설정 유효함
주소가 삭제됨	호스트/네트워크 삭제
속성 값이 삭제됨	호스트 특성 삭제 값
속성 값이 설정됨	호스트 특성 설정 값
운영체제 정의가 설정됨	운영 시스템 정의 설정
호스트 중요도가 설정됨	호스트 중요도 설정

다음 표에서는 기본 이벤트로 호스트 입력 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***123:*** 호스트 입력 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다.
소스	호스트 입력 데이터의 소스를 선택합니다.
소스 유형	호스트 입력 데이터의 소스 유형을 선택합니다.

관련 항목

호스트 입력 이벤트 유형, 933 페이지
검색 이벤트 필드, 936 페이지
Firepower System IP 주소 규칙, 28 페이지

연결 이벤트 트리거 기준 구문

연결 이벤트의 상관관계 규칙에 기반을 두려면, 먼저 사용할 연결 이벤트의 유형을 지정해야 합니다. 연결 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다. 다음 중에서 선택할 수 있습니다.

- 연결 시작 또는 종료 시
- 연결 시작 시

- 연결 종료 시

다음 표에서는 기본 이벤트로 연결 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 ***124:*** 연결 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고...
액세스 제어 정책	연결을 로깅한 액세스 컨트롤 정책을 하나 이상 선택합니다.
액세스 제어 규칙 작업	연결을 로깅한 액세스 컨트롤 규칙과 관련된 작업을 하나 이상 선택합니다. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, 네트워크 트래픽이 Monitor 규칙의 조건과 일치할 때 상관관계 이벤트를 트리거하려면 **Monitor**를 선택합니다.
액세스 제어 규칙	연결을 로깅한 액세스 컨트롤 규칙의 이름 전체 또는 일부를 입력합니다. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, 연결 기준으로 조건이 일치한 Monitor 규칙의 이름을 입력할 수 있습니다.
애플리케이션 프로토콜	연결과 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트의 카테고리를 하나 이상 선택합니다.
클라이언트 버전	클라이언트의 버전 번호를 입력합니다.
연결 지속시간	연결 이벤트의 기간을 초 단위로 입력합니다.
연결 유형	연결 이벤트를 획득한 방법에 따라 상관관계 규칙을 트리거할지 여부를 지정합니다. • 내보낸 NetFlow 데이터에서 생성한 연결 이벤트에 대해 **is**와 **Netflow**를 선택합니다. • Firepower System 매니지드 디바이스가 탐지한 연결 이벤트에 대하 **is not**과 **Netflow**를 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	연결 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.
디바이스	연결을 탐지했거나 (내보낸 NetFlow 기록에서 얻은 연결 데이터의 경우) 연결을 처리한 디바이스를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.

다음을 지정할 경우...	연산자를 선택하고...
Egress Interface(이그레스 인터페이스) 또는 Ingress Interface(인그레스 인터페이스)	하나 이상의 인터페이스를 선택합니다.
Egress Security Zone(이그레스 보안 영역) 또는 Ingress Security Zone(인그레스 보안 영역)	보안 영역 또는 터널 영역을 하나 이상 선택합니다.
이니시에이터 바이트, 응답자 바이트 또는 전체 바이트	다음 중 하나를 입력합니다. • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트) • 주고받은 바이트 수(전체 바이트)
이니시에이터 IP, 응답자 IP, 이니시에이터와 응답자 IP 모두, 또는 이니시에이터 IP나 응답자 IP	단일 IP 주소 또는 주소 블록을 지정합니다.
이니시에이터 패킷, 응답자 패킷 또는 총 패킷	다음 중 하나를 입력합니다. • 전송한 패킷 수(이니시에이터 패킷). • 수신한 패킷 수(응답자 패킷). • 주고받은 패킷 수(총 패킷)
이니시에이터 포트/ICMP 유형 또는 응답자 포트/ICMP 코드	이니시에이터 트래픽의 포트 번호나 ICMP 유형 또는 응답자 트래픽의 포트 번호나 ICMP 코드를 입력합니다.
IOC 태그	연결 이벤트 때문에 침해 지표 태그가 **is** 또는 **is not**으로 설정되었느지를 지정합니다.
NetBIOS 이름	연결에서 모니터링된 호스트의 NetBIOS 이름을 입력합니다.
NetFlow 디바이스	상관관계 규칙을 트리거하는 데 사용할 NetFlow 엑스포터의 IP 주소를 선택합니다. 네트워크 검색 정책에 어떤 NetFlow 엑스포터도 추가하지 않았다면, **NetFlow Device(NetFlow** 디바이스**)** 드롭다운 목록에는 아무것도 표시되지 않습니다.
사전 필터 정책	연결을 처리한 사전 필터 정책을 하나 이상 선택합니다.
이유	연결 이벤트와 관련된 이유를 하나 이상 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
보안 인텔리전스 범주	연결 이벤트와 관련된 보안 인텔리전스 카테고리를 하나 이상 선택합니다. 보안 인텔리전스 카테고리를 연결 종료 이벤트의 조건으로 사용하려면, 액세스 컨트롤 정책에서 해당 카테고리를 **Block**이 아닌 **Monitor**로 설정합니다.
SSL 실제 작업	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 지정합니다.
SSL 인증서 핑거프린트	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL 인증서 상태	세션 암호화에 사용된 인증서와 관련된 상태를 하나 이상 선택합니다.
SSL 인증서 주체 일반 이름(CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL 인증서 주체 국가(C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL 인증서 주체 조직(O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL 인증서 주체 조직 단위(OU)	세션 암호화에 사용된 인증서의 주체 조직 단위 이름 전체 또는 일부를 입력합니다.
SSL 암호 그룹	세션 암호화에 사용된 암호 그룹을 하나 이상 선택합니다.
SSL 암호화된 세션	**Successfully Decrypted(**성공적으로 해독**)**를 선택합니다.
SSL 흐름 상태	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
SSL 정책	암호화된 연결을 로깅한 SSL 정책을 하나 이상 선택합니다.
SSL 규칙 이름	암호화된 연결을 로깅한 SSL 규칙의 이름 전체 또는 일부를 입력합니다.
SSL 서버 이름	클라이언트가 암호화된 연결을 설정한 서버의 이름 전체 또는 일부를 입력합니다.
SSL URL 카테고리	암호화된 연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
SSL 버전	세션 암호화에 사용된 SSL 또는 TLS 버전을 하나 이상 선택합니다.
TCP 플래그	상관관계 규칙을 트리거하기 위해 연결 이벤트에 포함해야 할 TCP 플래그를 선택합니다. NetFlow에서 생성한 연결 데이터만 TCP 플래그를 가지고 있습니다.
전송 프로토콜	연결에 사용된 전송 프로토콜(**`TCP`** 또는 **`UDP`**)을 입력합니다.
터널/사전 필터 규칙	연결을 처리한 터널 또는 사전 필터 규칙 이름의 전체 또는 일부를 입력합니다.
URL	연결에서 방문한 URL 전체 또는 일부를 입력합니다.
URL 범주	연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
URL 평판	연결에서 방문한 URL의 URL 평판 값을 하나 이상 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
사용자 이름	연결의 두 호스트 중 하나에 로그인한 사용자의 사용자 이름을 입력합니다.
웹 애플리케이션	연결과 관련된 웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

연결 및 보안 관련 연결 이벤트 필드, 773 페이지
Firepower System IP 주소 규칙, 28 페이지

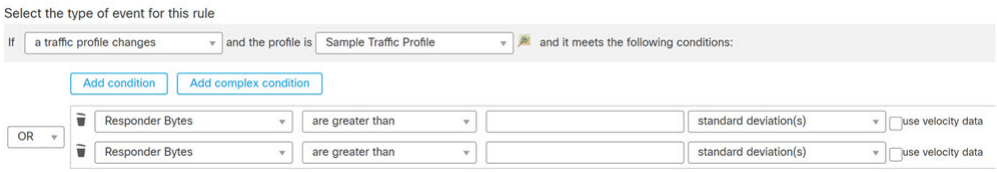
트래픽 프로파일 변경 구문

트래픽 프로파일 변경사항에 대한 상관관계 규칙을 기반으로 하려면, 먼저 사용할 트래픽 프로파일을 선택해야 합니다. 규칙은 네트워크 트래픽이 선택한 프로파일로 특성화되는 패턴에서 벗어날 때 트리거됩니다.

원시 데이터 또는 데이터에서 계산된 통계를 기반으로 규칙을 트리거할 수 있습니다. 예를 들어 네트워크를 통과하는 데이터의 양(바이트 단위로 측정됨)이 급증할 때(공격이나 기타 보안 정책 위반의 징후일 수 있음) 트리거되는 규칙을 작성할 수 있습니다. 다음의 경우 규칙이 트리거되도록 지정할 수 있습니다.

- 네트워크를 통과하는 바이트 수가 특정 바이트 수 위로 급증하는 경우
- 네트워크를 통과하는 바이트 수가 평균 트래픽 양의 위 또는 아래에서 표준 편차의 특정 수치 위로 급증하는 경우

  네트워크를 통과하는 바이트의 수가 표준 편차의 특정 수치(위 또는 아래)를 벗어날 때 트리거되는 규칙을 생성하려면 다음 그림에 보이는 것처럼 상한 또는 하한을 지정해야 합니다.



  통과하는 바이트 수가 평균 위에서 표준 편차의 특정 수보다 클 때 트리거되는 규칙을 생성하려면 그림에 보이는 첫 번째 조건만 사용하십시오.

  통과하는 바이트 수가 평균 아래에서 표준 편차의 특정 수보다 클 때 트리거되는 규칙을 생성하려면 두 번째 조건만 사용하십시오.

데이터 포인트 간 변경 속도를 기반으로 상관관계 규칙을 트리거하려면 **use velocity data(**속도 데이터 사용**)** 확인란을 선택합니다. 위의 예에서 속도 데이터를 사용한다면 다음과 같은 경우 규칙이 트리거되도록 지정할 수 있습니다.

- 네트워크를 통과하는 바이트의 양이 변경되어 평균 변경 속도 위에서 표준 편차의 특정 수치 위 또는 아래로 급증하는 경우

• 네트워크를 통과하는 바이트 수가 변경되어 특정 바이트 수 위로 급증하는 경우

다음 표에서는 기본 이벤트로 트래픽 프로파일 변경을 선택할 경우 상관관계 규칙에서 조건을 작성하는 방법에 대해 설명합니다.

표 ***125:*** 트래픽 프로파일 변경 구문

다음을 지정할 경우...	연산자를 선택하고 다음을 입력합니다.	그런 후에 다음 중 하나를 선택합니다.
연결 수	탐지된 총 연결 수 또는 규칙을 트리거하기 위해 탐지된 연결 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	연결 표준 편차
총 바이트, 이니시에이터 바이트 또는 응답자 바이트	다음 중 하나에 해당합니다. • 전송한 총 바이트(총 바이트) • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트) 또는 규칙을 트리거하기 위해 위 기준 중 하나가 속해야 하는 평균 위 또는 아래 표준 편차의 수	바이트 표준 편차
총 패킷, 이니시에이터 패킷 또는 응답자 패킷	다음 중 하나에 해당합니다. • 전송한 총 패킷(총 패킷) • 전송한 패킷 수(이니시에이터 패킷) • 수신한 패킷 수(응답자 패킷) 또는 규칙을 트리거하기 위해 위 기준 중 하나가 속해야 하는 평균 위 또는 아래 표준 편차의 수	packets 표준 편차
고유한 이니시에이터	세션을 시작한 고유한 호스트의 수 또는 규칙을 트리거하기 위해 탐지된 고유한 이니시에이터 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	개시자 표준 편차

다음을 지정할 경우...	연산자를 선택하고 다음을 입력합니다.	그런 후에 다음 중 하나를 선택합니다.
고유한 응답자	세션에 응답한 고유한 호스트의 수 또는 규칙을 트리거하기 위해 탐지된 고유한 응답자 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	응답자 표준 편차

상관관계 호스트 프로파일 자격 구문

이벤트와 관련된 호스트의 호스트 프로파일을 기준으로 상관관계 규칙을 제한하려면 *host profile qualification(*호스트 프로파일 자격*)*을 추가합니다. 악성코드 이벤트, 트래픽 프로파일 변경 또는 새 IP 호스트 탐색에 대해 트리거되는 상관관계 규칙에 호스트 프로파일 자격을 추가할 수 없습니다.

호스트 프로파일 자격을 작성할 때 먼저 상관관계 규칙을 제한하는 데 사용할 호스트를 지정해야 합니다. 선택할 수 있는 호스트는 규칙의 기본 이벤트 유형에 따라 달라집니다 .

- 연결 이벤트 - **Responder Host(**응답자 호스트**)** 또는 **Initiator Host(**이니시에이터 호스트**)**를 선택합니다.
- 침입 이벤트 - **Destination Host(**목적지 호스트**)** 또는 **Source Host(**소스 호스트**)**를 선택합니다.
- 검색 이벤트, 호스트 입력 이벤트 또는 사용자 활동 - **Host(**호스트**)**를 선택합니다.

다음 표에서는 상관관계 규칙에 대한 호스트 프로파일 자격을 만드는 방법을 설명합니다.

표 ***126:*** 호스트 프로파일 자격 구문

다음을 지정할 경우...	연산자를 선택하고...
애플리케이션 프로토콜 > 애플리케이션 프로토콜	애플리케이션 프로토콜을 선택합니다.
애플리케이션 프로토콜 > 애플리케이션 포트	애플리케이션 프로토콜 포트 번호를 입력합니다.
애플리케이션 프로토콜 > 프로토콜	프로토콜을 선택합니다.
애플리케이션프로토콜카테고리	카테고리를 선택합니다.
클라이언트 > 클라이언트	클라이언트를 선택합니다.
클라이언트 > 클라이언트 버전	클라이언트 버전을 입력합니다.
클라이언트 카테고리	카테고리를 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다.이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
하드웨어	모바일 디바이스의 하드웨어 모델을 입력합니다. 예를 들어 일치하는 모든 Apple iPhone을 찾으려면 **`iPhone`**을 입력합니다.
호스트 중요도	호스트 중요도를 선택합니다.
호스트 유형	호스트 유형을 하나 이상 선택합니다. 일반 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.
IOC 태그	침해 지표 태그를 하나 이상 선택합니다.
탈옥됨	이벤트의 호스트가 탈옥 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
MAC 주소 > MAC 주소	호스트의 MAC 주소 전체 또는 일부를 입력합니다.
MAC 주소 > MAC 유형	MAC 유형이 ARP/DHCP Detected인지 여부를 선택합니다. • 시스템이 MAC 주소가 호스트에 속한 것으로 명확하게 확인함(**is ARP/DHCP Detected**) • 디바이스와 호스트 간에 라우터가 있다는 등의 이유로, 시스템이 MAC 주소가 있는 다양한 호스트를 확인함(**is not ARP/DHCP Detected**) • MAC 유형이 올바르지 않음(**is any**)
MAC 벤더	호스트에서 사용하는 하드웨어의 MAC 벤더 전체 또는 일부를 입력합니다.
모바일	이벤트의 호스트가 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
NetBIOS 이름	호스트의 NetBIOS 이름을 입력합니다.
네트워크 프로토콜	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
운영체제 > OS 벤더	운영체제 벤더 이름을 하나 이상 선택합니다.
운영체제 > OS 이름	운영체제 이름을 하나 이상 선택합니다.
운영체제 > OS 버전	운영체제 버전을 하나 이상 선택합니다.
전송 프로토콜	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.
VLAN ID	호스트의 VLAN ID 번호를 입력합니다.
웹 애플리케이션	웹 애플리케이션을 선택합니다.
웹 애플리케이션 카테고리	카테고리를 선택합니다.

다음을 지정할 경우...	연산자를 선택하고...
사용 가능한 모든 호스트 속성(기본 규정준수 허용리스트 호스트 속성 포함)	호스트 속성 유형에 맞는 적절한 값을 입력하거나 선택합니다.

암시적 또는 일반 클라이언트를 사용하여 호스트 프로파일 자격 구축

시스템이 뒤에 클라이언트가 붙는 애플리케이션 프로토콜 이름(HTTPS 클라이언트 등)을 이용해 탐지 클라이언트를 보고하는 경우, 해당 클라이언트는 암시적 또는 일반 클라이언트가 됩니다. 이 경우 시스템은 특정 클라이언트를 탐지하지 않지만, 서버 응답 트래픽을 기준으로 클라이언트 존재를 추론합니다.

암시적 또는 일반 클라이언트를 사용하여 호스트 프로파일 자격을 생성하려면, 클라이언트가 아닌 응답자 호스트에서 실행하는 애플리케이션 프로토콜을 이용해 제한해야 합니다.

이벤트 데이터를 사용하여 호스트 프로파일 자격 작성

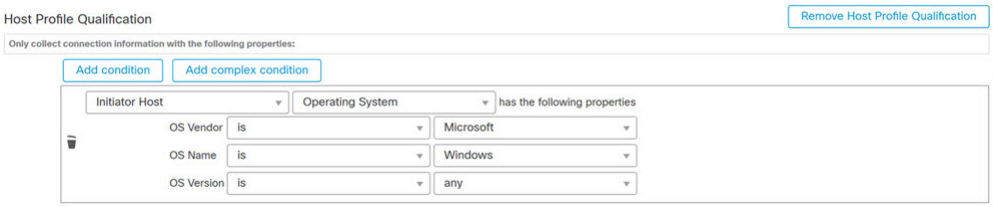
호스트 프로파일 자격을 구성할 때는 상관관계 규칙의 기본 이벤트에서 제공하는 데이터를 자주 사용하게 됩니다.

예를 들어 모니터링되는 호스트 중 하나에서 특정 브라우저를 사용하는 것을 시스템이 탐지할 때 상관관계 규칙이 트리거된다고 가정해보겠습니다. 그리고 이러한 사용을 탐지할 때, 브라우저 버전이 최신 버전이 아니라면 이벤트를 생성하려 합니다.

Client(클라이언트**)**가 **Event Client(**이벤트 클라이언트**)**지만 **Client Version(**클라이언트 버전**)**이 최신 버전이 아닐 경우에만 규칙이 트리거되도록 호스트 프로파일 자격을 이 상관관계 규칙에 추가할 수 있습니다.

호스트 프로파일 자격 예

다음 호스트 프로파일 자격은 규칙의 기반이 되는 검색 이벤트와 관련된 호스트가 Microsoft Windows 버전을 실행하는 경우에만 규칙이 트리거되는 방식으로 상관관계 규칙을 제한합니다.



관련 항목

호스트 데이터 필드, 938 페이지

사용자 자격 구문

연결, 침입, 검색 또는 호스트 입력 이벤트를 사용하여 상관관계 규칙을 트리거하는 경우, 이벤트와 관련된 사용자의 ID를 기반으로 규칙을 제한할 수 있습니다. 이러한 제약을 *user qualification(*사용자 자격*)*이라고 합니다. 예를 들어 소스 또는 대상 사용자의 ID가 영업 부서 사용자인 경우에만 트리거되도록 상관관계 규칙을 제한할 수 있습니다.

트래픽 프로파일 변경 또는 사용자 활동 탐색에 대해 트리거되는 상관관계 규칙에 사용자 자격을 추가할 수 없습니다. 또한 시스템은 management center-ID 영역에서 형성된 서버 연결을 통해 사용자 상세정보를 획득합니다. 데이터베이스의 일부 사용자에 대해서는 이 정보를 이용하지 못할 수 있습니다.

사용자 자격을 작성할 때 먼저 상관관계 규칙을 제한하는 데 사용할 ID를 지정해야 합니다. 선택할 수 있는 ID는 규칙의 기본 이벤트 유형에 따라 달라집니다 .

- 연결 이벤트 - 이니시에이터에서의 **ID** 또는 응답자에서의 **ID**를 선택합니다.
- 침입 이벤트 - 목적지에서의 **ID** 또는 소스에서의 **ID**를 선택합니다.
- 검색 이벤트 - 호스트에서의 **ID**를 선택합니다.
- 호스트 입력 이벤트 - 호스트에서의 **ID**를 선택합니다.

다음 표에서는 상관관계 규칙에 대한 사용자 자격을 만드는 방법을 설명합니다.

표 ***127:*** 사용자 자격 구문

다음을 지정할 경우...	연산자를 선택하고...
인증 프로토콜	사용자 탐지에 사용한 인증 프로토콜(또는 사용자 유형) 프로토콜을 선택합니다.
부서	부서를 입력합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다. 이 필드는 management center에 멀티테넌시를 구성한 경우에만 표시됩니다.
이메일	이메일 주소를 입력합니다.
이름	이름을 입력합니다.
성	성을 입력합니다.
전화 번호	전화번호를 입력합니다.
사용자 이름	사용자 이름을 입력합니다.

관련 항목

사용자 데이터 필드

연결 추적기

규칙의 초기 기준이 충족되면(호스트 프로파일 및 사용자 자격 포함) 시스템이 특정 연결 추적을 시작할 수 있도록, 연결 추적기는 상관관계 규칙을 제한합니다. 추적된 연결이 지정 기간 동안 수집된 추가 기준을 충족할 경우 시스템은 규칙에 대해 상관관계 이벤트를 생성합니다.

팁 연결 추적기는 일반적으로 매우 구체적인 트래픽을 모니터링하며, 트리거될 경우 지정된 기간에만 실행됩니다. 일반적으로 폭넓은 네트워크 트래픽을 모니터링하고 영구적으로 실행되는 트래픽 프로파일을 연결 추적기와 비교해보십시오.

연결 추적기는 두 가지 방법으로 이벤트를 생성할 수 있습니다.

조건이 충족될 때 즉시 실행되는 연결 추적기

네트워크 트래픽이 추적기의 조건을 충족하자마자 상관관계 규칙이 실행되도록 연결 추적기를 구성할 수 있습니다. 이러한 상황이 발생하면 시스템은 시간 초과 기간이 만료되지 않았더라도 이 연결 추적기 인스턴스에 대한 연결 추적을 중지합니다. 상관관계 규칙을 트리거한 동일한 정책 위반 유형이 다시 발생하면 시스템은 새 연결 추적기를 생성합니다.

하지만 네트워크 트래픽이 연결 추적기의 조건을 충족하기 전에 시간이 만료되면 시스템은 상관관계 이벤트를 생성하지 않으며, 동시에 해당 규칙 인스턴스에 대한 연결 추적을 중지합니다.

예를 들어 연결 추적기는 특정 유형의 연결이 지정된 기간 내에 지정된 횟수보다 더 많이 발생하는 경우에만 상관관계 이벤트를 생성함으로써 일종의 이벤트 임계값 역할을 할 수 있습니다. 또는 초기 연결 이후 시스템에서 과도한 데이터 전송을 탐지하는 경우에만 상관관계 이벤트를 생성할 수 있습니다.

시간 초과 기간 끝에 실행되는 연결 추적기

전체 시간 초과 기간에 수집된 데이터에 의존하도록, 따라서 시간 초과 기간이 끝날 때까지 실행될 수 없도록 연결 추적기를 구성할 수 있습니다.

예를 들어 일정 기간 동안 특정 바이트 수 미만이 탐지될 때 실행되도록 연결 추적기를 구성하는 경우, 시스템은 기간이 지날 때까지 기다렸다가 네트워크 트래픽이 해당 조건을 충족하면 이벤트를 생성합니다.

연결 추적기 추가

시작하기 전에

- 연결, 침입, 검색, 사용자 ID 또는 호스트 입력 이벤트를 기반으로 상관관계 규칙을 생성합니다. 악성코드 이벤트 또는 트래픽 프로파일 변경을 기반으로 하는 규칙에는 연결 추적기를 추가할 수 없습니다.

프로시저

단계 **1** 상관관계 규칙 편집기에서 **Add Connection Tracker(**연결 추적기 추가**)**를 클릭합니다.

단계 **2** 추적할 연결을 지정합니다(연결 추적기 구문, 1043 페이지 참조).

단계 **3** 추적한 연결을 바탕으로, 상관관계 이벤트를 생성할 시점을 지정합니다(연결 추적기 이벤트 구문, 1046 페이지 참조).

단계 **4** 추적기의 조건을 달성해야 하는 간격(단위: 초, 분 또는 시간)을 지정합니다.

연결 추적기 구문

다음 표에서는 추적하고자 하는 연결의 종류를 지정하는 연결 추적기 조건을 작성하는 방법에 대해 설명합니다.

표 ***128:*** 연결 추적기 구문

다음을 지정할 경우...	연산자를 선택하고...
액세스 제어 정책	추적할 연결을 처리한 액세스 컨트롤 정책을 하나 이상 선택합니다.
액세스 제어 규칙 작업	추적할 연결을 로깅한 액세스 컨트롤 규칙과 관련된 액세스 컨트롤 규칙 작업을 하나 이상 선택합니다. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, Monitor 규칙의 조건과 일치하는 연결을 추적하려면 **Monitor**를 선택합니다.
액세스 제어 규칙 이름	추적할 연결을 로깅한 액세스 컨트롤 규칙의 이름 전체 또는 일부를 입력합니다. Monitor 규칙과 일치하는 연결을 추적하려면 Monitor 규칙의 이름을 입력하십시오. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이 시스템은 연결을 추적합니다.
애플리케이션 프로토콜	애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트 카테고리를 하나 이상 선택합니다.
클라이언트 버전	클라이언트 버전을 입력합니다.
연결 지속시간	연결 이벤트 지속시간을 초 단위로 입력합니다.

다음을 지정할 경우...	연산자를 선택하고...
연결 유형	연결 이벤트를 획득한 방법에 따라 상관관계 규칙을 트리거할지 여부를 지정합니다. • 내보낸 NetFlow 기록에서 생성한 연결 이벤트에 대해 **is**와 **Netflow**를 선택합니다. • Firepower System 매니지드 디바이스가 탐지한 연결 이벤트에 대하 **is not**과 **Netflow**를 선택합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	국가를 하나 이상 선택합니다.
디바이스	탐지된 연결을 추적하려는 디바이스를 하나 이상 선택합니다. NetFlow 연결을 추적하려면 내보낸 NetFlow 기록의 연결 데이터를 처리하는 디바이스를 선택합니다.
Ingress Interface(인그레스 인터페이스) 또는 Egress Interface(이그레스 인터페이스)	하나 이상의 인터페이스를 선택합니다.
Ingress Security Zone(인그레스 보안 영역) 또는 Egress Security Zone(이그레스 보안 영역)	보안 영역 또는 터널 영역을 하나 이상 선택합니다.
이니시에이터 IP, 응답자 IP 또는 이니시에이터/응답자 IP	단일 IP 주소 또는 주소 블록을 입력합니다.
이니시에이터 바이트, 응답자 바이트 또는 전체 바이트	다음 중 하나를 입력합니다. • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트) • 전송 및 수신된 바이트 수(총 바이트)
이니시에이터 패킷, 응답자 패킷 또는 총 패킷	다음 중 하나를 입력합니다. • 전송한 패킷 수(이니시에이터 패킷) • 수신한 패킷 수(응답자 패킷) • 전송 및 수신된 패킷 수(총 패킷)
이니시에이터 포트/ICMP 유형 또는 응답자 포트/ICMP 코드	이니시에이터 트래픽의 포트 번호나 ICMP 유형 또는 응답자 트래픽의 포트 번호나 ICMP 코드를 입력합니다.
IOC 태그	침해 지표 태그가 **is** 또는 **is not**으로 설정되었는지를 선택합니다.
NETBIOS 이름	연결에서 모니터링된 호스트의 NetBIOS 이름을 입력합니다.

다음을 지정할 경우...	연산자를 선택하고...
NetFlow 디바이스	추적할 NetFlow 엑스포터의 IP 주소를 선택합니다. 네트워크 검색 정책에 어떤 NetFlow 엑스포터도 추가하지 않았다면, NetFlow Device(NetFlow 디바이스) 드롭다운 목록에는 아무것도 표시되지 않습니다.
사전 필터 정책	추적할 연결을 처리한 사전 필터 정책을 하나 이상 선택합니다.
이유	추적할 연결과 관련된 이유를 하나 이상 선택합니다.
보안 인텔리전스 범주	추적할 연결과 관련된 보안 인텔리전스 카테고리를 하나 이상 선택합니다.
TCP 플래그	추적을 위해 연결에 반드시 포함해야 하는 TCP 플래그를 선택합니다. 내보낸 NetFlow 기록에서 생성한 연결만 TCP 플래그 데이터를 가지고 있습니다.
전송 프로토콜	연결에 사용된 전송 프로토콜을 선택합니다.
URL	추적할 연결에서 방문한 URL 전체 또는 일부를 입력합니다.
URL 범주	추적할 연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
URL 평판	추적할 연결에서 방문한 URL의 URL 평판 값을 하나 이상 선택합니다.
사용자 이름	추적할 연결의 두 호스트 중 하나에 로그인한 사용자의 사용자 이름을 입력합니다.
웹 애플리케이션	웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

이벤트 데이터를 사용하여 연결 추적기 구축

연결 추적기를 구성할 때는 상관관계 규칙의 기본 이벤트에서 제공하는 데이터를 자주 사용하게 됩니다.

예를 들어 시스템이 새 클라이언트를 탐지할 때 상관관계 규칙이 트리거된다고 가정해 봅시다. 이러한 유형의 상관관계 규칙에 연결 추적기를 추가하면, 시스템은 기본 이벤트를 참조하는 제약 조건으로 추적기를 자동으로 채웁니다.

- **Initiator/Responder IP(**이니시에이터/응답자 **IP)**는 **Event IP Address(**이벤트 **IP** 주소**)**로 설정됩니다.
- **Client(**클라이언트**)**는 **Event Client(**이벤트 클라이언트**)**로 설정됩니다.

팁 특정 IP 주소 또는 IP 주소 블록의 연결을 추적하려면 **switch to manual entry(**수동 입력으로 전환**)**를 클릭하여 IP를 수동으로 지정하십시오. 이벤트의 IP 주소를 사용하는 방식으로 돌아가려면 **switch to event fields(**이벤트 필드로 전환**)**를 클릭합니다.

관련 항목

연결 및 보안 관련 연결 이벤트 필드, 773 페이지
Firepower System IP 주소 규칙, 28 페이지

연결 추적기 이벤트 구문

다음 표에서는 추적 중인 연결을 기반으로 상관관계 이벤트를 생성하고자 하는 시기를 지정하는 연결 추적기 조건의 작성 방법에 대해 설명합니다.

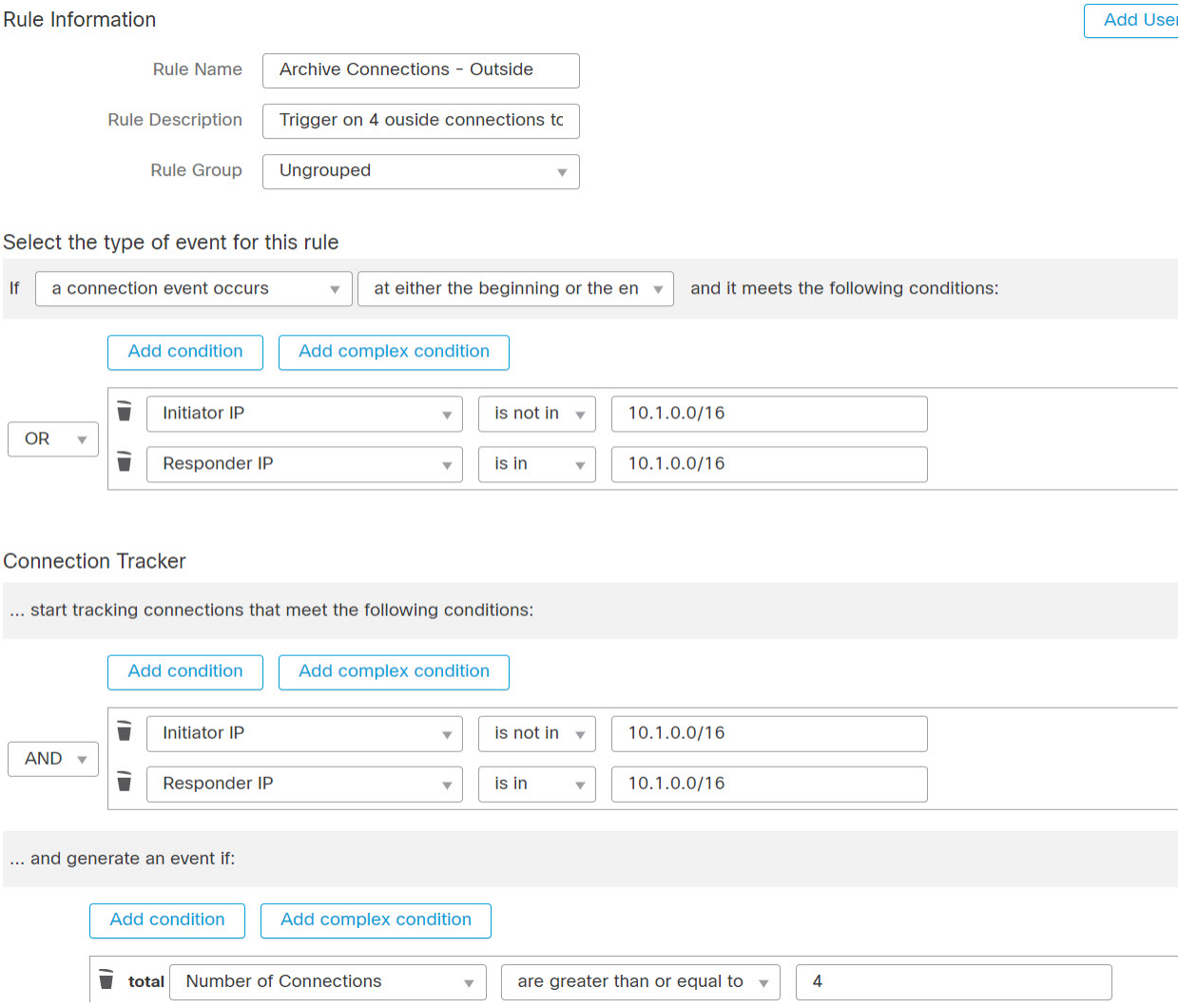
표 ***129:*** 연결 추적기 이벤트 구문

다음을 지정할 경우...	연산자를 선택하고 다음을 입력합니다.
연결 수	탐지된 총 연결 수
SSL 암호화된 세션 수	탐지된 총 SSL 또는 TLS 암호화 세션의 수를 입력합니다.
총 바이트, 이니시에이터 바이트 또는 응답자 바이트	다음 중 하나에 해당합니다. • 전송한 총 바이트(총 바이트) • 전송한 바이트 수(이니시에이터 바이트) • 수신한 바이트 수(응답자 바이트)
총 패킷, 이니시에이터 패킷 또는 응답자 패킷	다음 중 하나에 해당합니다. • 전송한 총 패킷(총 패킷) • 전송한 패킷 수(이니시에이터 패킷) • 수신한 패킷 수(응답자 패킷)
고유 이니시에이터 또는 고유 응답자	다음 중 하나에 해당합니다. • 탐지된 세션을 시작한 고유한 호스트의 수(고유 이니시에이터) • 탐지된 연결에 응답한 고유한 호스트의 수(고유 응답자)

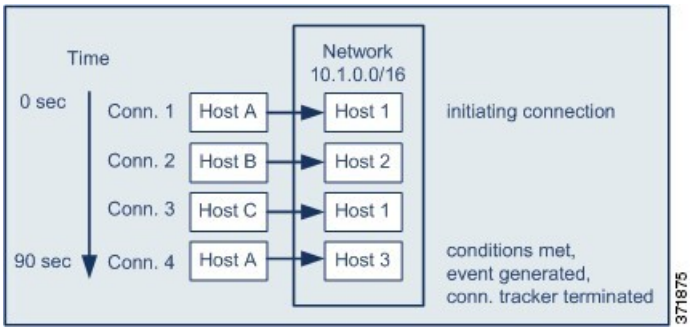
외부 호스트의 과도한 연결에 대한 샘플 구성

네트워크 10.1.0.0/16에 중요한 파일을 보관하며, 이 네트워크 외부의 호스트는 일반적으로 네트워크 내부의 호스트에 대해 연결을 시작하지 않는 시나리오를 고려해 보십시오. 네트워크 외부에서 더러 연결이 시작되었지만, 2분 내에 4개 이상의 연결이 시작되면 문제가 있는 것으로 판단했습니다.

다음 그림의 규칙에서는, 10.1.0.0/16 네트워크 외부에서 네트워크 내부로 연결이 시작될 때 시스템이 해당 조건을 충족하는 연결의 추적을 시작하는 것을 알 수 있습니다. 이제 시스템이 해당 서명과 일치하는 4개의 연결(원래 연결 포함)을 2분 내에 탐지할 경우 시스템은 상관관계 이벤트를 생성합니다.



다음 다이어그램은 네트워크 트래픽이 위의 상관관계 규칙을 트리거하는 방법을 보여줍니다.



이 예에서 시스템은 상관관계 규칙의 기본 조건을 충족한 연결, 즉 10.1.0.0/16 네트워크 외부 호스트에서 네트워크 내부 호스트로의 연결을 탐지했습니다. 여기에서 연결 추적기가 생성됩니다.

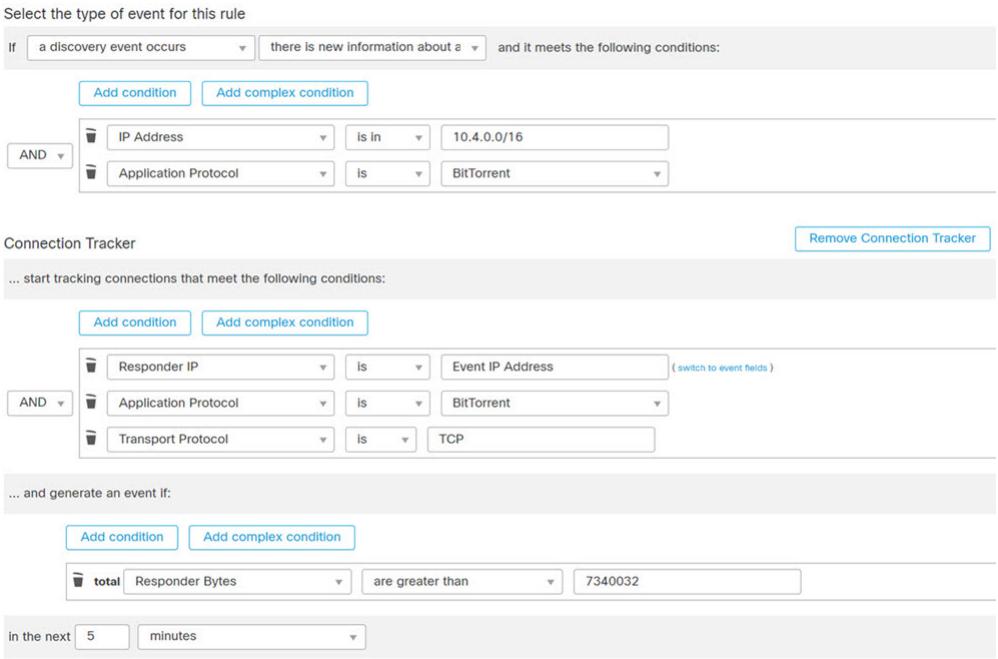
연결 추적기는 다음과 같이 처리됩니다.

- 먼저, 시스템은 네트워크 외부 Host A에서 네트워크 내부 Host 1로의 연결을 탐지하면 연결 추적을 시작합니다.
- 시스템은 연결 추적기 서명과 일치하는 연결을 2개 더 탐지합니다(Host B에서 Host 2, Host C에서 Host 1).
- 2분 시간 제한 내에 Host A가 Host 3에 연결되면 시스템은 4번째 해당 연결을 탐지하게 됩니다. 규칙 조건이 충족됩니다.
- 마지막으로, 시스템은 상관관계 이벤트를 생성하고 연결 추적을 중지합니다.

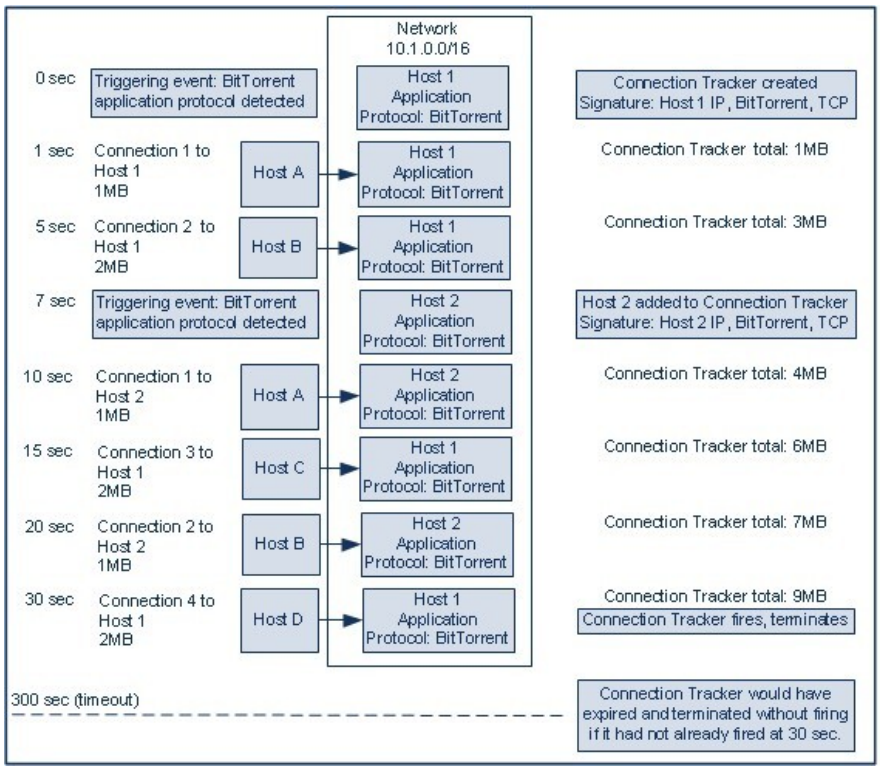
과도한 **BitTorrent** 데이터 전송에 대한 샘플 구성

모니터링되는 네트워크의 호스트에 대한 초기 연결 이후 시스템이 과도한 BitTorrent 데이터 전송을 탐지하는 경우 상관관계 이벤트를 생성하고자 하는 시나리오를 고려해보십시오.

다음 그림에서는 시스템이 모니터링되는 네트워크에서 BitTorrent 애플리케이션 프로토콜을 탐지할 때 트리거되는 상관관계 규칙을 보여줍니다. 이 규칙에는 모니터링되는 네트워크의 호스트(이 경우 10.1.0.0/16)가 초기 정책 위반 이후 5분 동안 BitTorrent를 통해 총 7MB(7340032바이트)가 넘는 데이터를 전송하는 경우 규칙이 트리거되도록 규칙을 제한하는 연결 추적기가 있습니다.



다음 다이어그램은 네트워크 트래픽이 위의 상관관계 규칙을 트리거하는 방법을 보여줍니다.



이 예에서 시스템은 두 호스트, 즉 Host 1과 Host 2에서 BitTorrent TCP 애플리케이션 프로토콜을 탐지했습니다. 이러한 두 호스트는 BitTorrent를 통해 4개의 다른 호스트(Host A, Host B, Host C, Host D)로 데이터를 전송합니다.

이 연결 추적기는 다음과 같이 처리됩니다.

- 먼저, 시스템은 Host 1에서 BitTorrent 애플리케이션 프로토콜을 탐지하면 0초 마커에서 연결 추적을 시작합니다. 시스템이 5분 내에(300초 마커까지) 7MB의 BitTorrent TCP 데이터가 전송되는 것을 탐지하지 못하면 연결 추적기가 만료됩니다.
- 5초에 Host 1이 서명과 일치하는 3MB의 데이터를 전송했습니다.
  - 1초 마커에 Host 1에서 Host A로 1MB(연결 추적기를 충족하기 위해 계산된 총 BitTorrent 트래픽 1MB)
  - 5초 마커에 Host 1에서 Host B로 2MB(총 3MB)
- 7초에 시스템은 Host 2에서 BitTorrent 애플리케이션 프로토콜을 탐지하고 해당 호스트에 대해서도 BitTorrent 연결 추적을 시작합니다.
- 20초에 시스템은 서명과 일치하는 추가 데이터가 Host 1과 Host2 모두에서 전송되는 것을 탐지했습니다.
  - 10초 마커에 Host 2에서 Host A로 1MB(총 4MB)
  - 15초 마커에 Host 1에서 Host C로 2MB(총 6MB)
  - 20초 마커에 Host 2에서 Host B로 1MB(총 7MB)

- Host 1과 Host 2에서 이제 총 7MB의 BitTorrent 데이터를 전송했지만, 전송된 총 바이트 수가 7MB(응답자 바이트가 **7340032** 초과**)**)보다 커야 하므로 규칙이 트리거되지 않습니다. 이 시점에 시스템이 추적기의 시간 초과 기간에 나머지 280초 동안 추가 BitTorrent 전송을 탐지하지 못하면, 추적기가 만료되고 시스템은 상관관계 이벤트를 생성하지 않습니다.
- 하지만 30초가 되면 시스템은 다른 BitTorrent 전송을 탐지하고, 규칙 조건이 충족됩니다.
  - 30초 마커에 Host 1에서 Host D로 2MB(총 9MB)
- 마지막으로, 시스템은 상관관계 이벤트를 생성합니다. 5분 기간이 만료되지 않았어도 시스템은 이 연결 추적기 인스턴스에 대한 연결 추적도 중지합니다. 이 시점에 BitTorrent TCP 애플리케이션 프로토콜을 사용하는 새 연결을 탐지하면 시스템은 새 연결 추적기를 생성합니다. 시스템은 세션이 끝날 때까지 연결 데이터를 집계하지 않으므로, Host 1이 총 2MB를 Host D로 전송한 후 상관관계 이벤트를 생성합니다.

스누즈 및 비활성 기간

상관관계 규칙에서 스누즈 기간을 구성할 수 있습니다. 상관관계 규칙이 트리거되면, 유휴 기간은 지정된 기간 동안(규칙 위반이 다시 발생해도) 규칙의 실행을 중지하도록 시스템에 지시합니다. 스누즈 기간이 경과하면 규칙을 다시 트리거할 수 있습니다(그리고 새 스누즈 기간을 시작할 수 있습니다).

예를 들면 트래픽을 생성해서는 안 되는 호스트가 네트워크에 있을지도 모릅니다. 시스템이 해당 호스트와 관련된 연결을 탐지할 때마다 트리거되는 간단한 상관관계 규칙은 호스트를 통과하는 네트워크 트래픽에 따라 짧은 기간에 여러 상관관계 이벤트를 생성할 수 있습니다. 정책 위반을 알리는 상관관계 이벤트의 수를 제한하려면 시스템이 해당 호스트와 관련하여 시스템이 탐지하는 첫 번째 연결(지정한 기간 내에)에 대해서만 상관관계 이벤트를 생성하도록 유휴 기간을 추가할 수 있습니다.

상관관계 규칙에서 비활성 시간도 설정할 수 있습니다. 비활성 기간 중에는 상관관계 규칙이 트리거되지 않습니다. 비활성 기간이 매일, 매주 또는 매월 반복되도록 설정할 수 있습니다. 예를 들어 호스트 운영체제 변경 사항을 찾기 위해 내부 네트워크에서 야간 Nmap 스캔을 수행할 수 있습니다. 이 경우 규칙이 잘못 트리거되지 않도록 스캔 시간 및 기간에 영향받는 상관관계 규칙에 대해 일일 비활성 기간을 설정할 수 있습니다.

상관관계 규칙 빌드 메커니즘

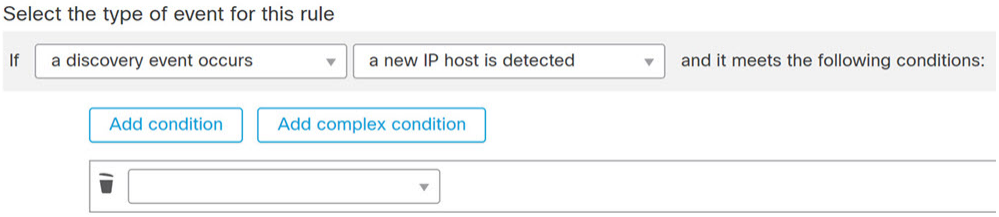
트리거 조건을 지정하여 상관관계 규칙을 작성합니다. 조건 내에서 사용할 수 있는 구문은 생성하는 요소에 따라 달라지지만, 그 원리는 동일합니다.

대부분의 조건은 카테고리, 연산자, 값이라는 3개 부분으로 구성됩니다.

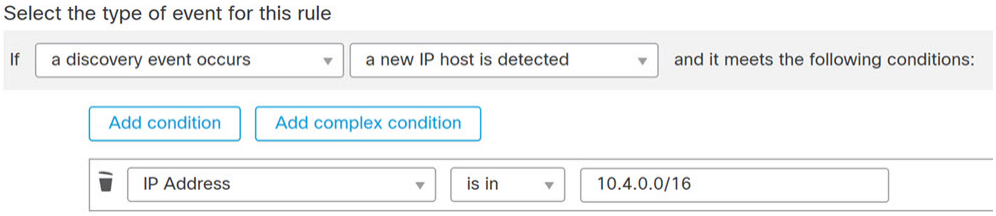
- 선택 가능한 카테고리는 상관관계 규칙 트리거, 호스트 프로파일 자격, 연결 추적기 또는 사용자 자격 중 어떤 것을 작성 중인지에 따라 달라집니다. 상관관계 규칙 트리거에서, 카테고리는 규칙에 대한 기본 이벤트 유형에 따라 달라집니다. 일부 조건은 여러 카테고리를 포함하는데, 각 카테고리마다 고유의 연산자와 값을 가질 수도 있습니다.
- 조건의 사용 가능한 연산자는 카테고리에 따라 달라집니다.

- 조건의 값을 지정하는 데 사용 가능한 구문은 카테고리와 연산자에 따라 달라집니다. 텍스트 필드에 직접 값을 입력해야 하는 경우도 있습니다. 그 외의 경우에는 드롭다운 목록에서 값(복수의 값 가능)을 선택할 수 있습니다.

예를 들어 새 호스트가 탐지될 때마다 상관관계 이벤트를 생성하려면, 어떤 조건도 없는 매우 단순한 규칙을 생성할 수 있습니다.



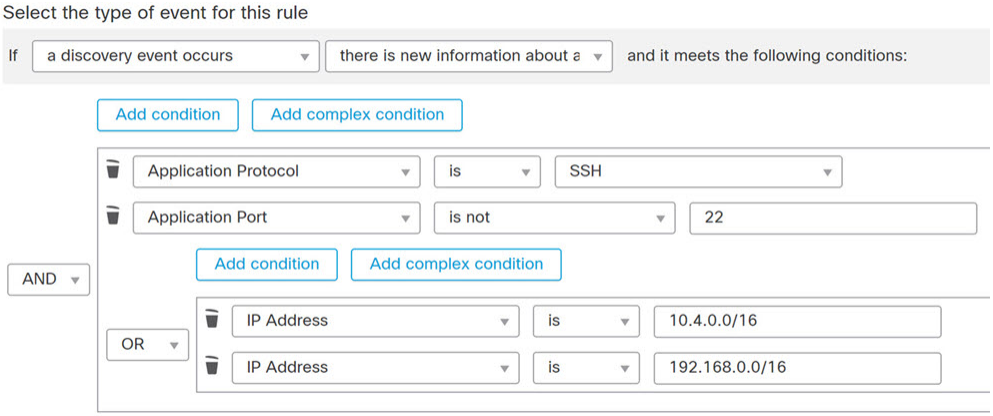
규칙을 더 제한하여 10.4.x.x 네트워크에서 새 호스트가 탐지되는 경우에만 이벤트를 생성하려는 경우 단일 조건을 추가할 수 있습니다.



여러 개의 조건을 포함할 경우 **AND** 또는 **OR** 연산자로 연결해야 합니다. 동일한 레벨의 조건은 함께 평가됩니다.

- **AND** 연산자를 사용하면 이 연산자가 제어하는 레벨의 모든 조건을 충족해야 합니다.
- **OR** 연산자를 사용하면 이 연산자가 제어하는 레벨의 조건 중 하나 이상을 충족해야 합니다.

10.4.x.x 네트워크 및 192.168.x.x 네트워크의 비표준 포트에서 SSH 활동을 탐지하는 다음 규칙에는 4개의 조건이 있으며, 그중 마지막 2개는 복합 조건입니다.



논리적으로, 이 규칙은 다음과 같이 평가됩니다.

```
(A and B and (C or D))
```

표 *130:* 규칙 평가

항목	조건의 내용
A	애플리케이션 프로토콜이 SSH임
B	애플리케이션 포트가 22가 아님
C	IP 주소는 10.0.0.0/8에 있음
D	IP 주소가 196.168.0.0/16에 있음

주의 자주 발생하는 이벤트에 대해 트리거되는 복잡한 상관관계 규칙을 평가하면 시스템 성능이 저하될 수 있습니다. 예를 들어 로깅된 모든 연결에 대해 시스템에서 반드시 평가해야 하는 다중 조건 규칙은 리소스 과부하를 일으킬 수 있습니다.

상관관계 규칙에 조건 추가 및 연결

프로시저

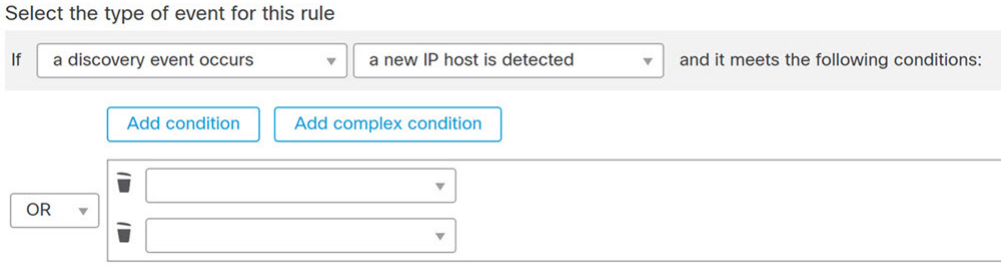
단계 **1** 상관관계 규칙 편집기에서 단순 또는 복합 조건을 추가합니다.

- 단순 - **Add condition(**조건 추가**)**을 클릭합니다.
- 복합 - **Add complex condition(**복합 조건 추가**)**을 클릭합니다.

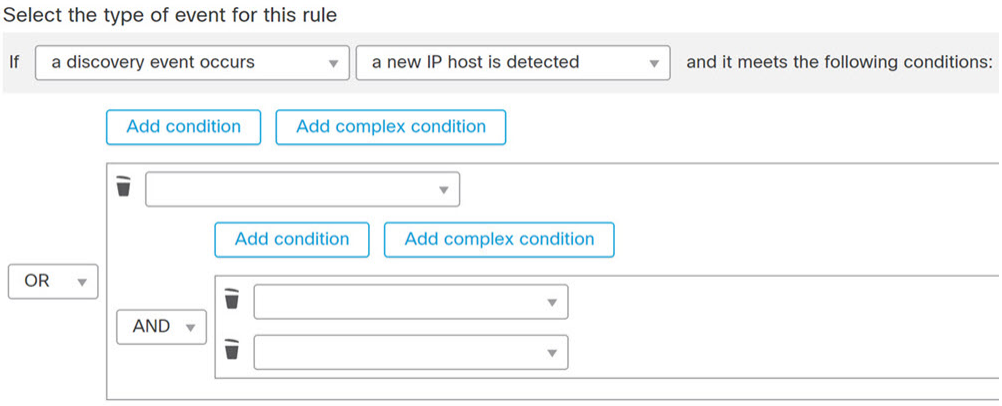
단계 **2** 조건 왼쪽에 있는 드롭다운 목록에서 **AND** 또는 **OR** 연산자를 선택해 조건을 연결합니다.

예**:** 단순 대 복합 조건

다음 그림은 두 가지 단순 조건이 **OR** 연산자로 결합된 상관관계 규칙을 보여줍니다.



다음 그림은 단순 조건 하나와 복합 조건 하나가 **OR** 연산자로 결합된 상관관계 규칙을 보여줍니다. 복합 조건은 **AND** 연산자로 결합된 단순 조건 2개로 구성됩니다.



상관관계 규칙 조건에 여러 값 사용

상관관계 조건을 작성할 때 조건 구문상 드롭다운 목록의 값 선택이 가능할 경우 대개는 목록에서 여러 값을 사용할 수 있습니다.

프로시저

단계 **1** 상관관계 규칙 편집기에서 조건을 작성하고, **is in** 또는 **is not in**을 연산자로 선택합니다.

단계 **2** 텍스트 필드의 아무 곳이나 클릭하거나 **Edit(편집)** 링크를 클릭합니다.

단계 **3** **Available(사용 가능)**에서 여러 값을 선택합니다. 클릭하고 드래그하여 인접한 여러 값을 선택할 수도 있습니다.

단계 **4** 오른쪽 화살표(>)를 클릭하여 선택한 항목을 **Selected**로 이동합니다.

단계 **5** **OK(확인)**를 클릭합니다.

상관관계 규칙 관리

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 상관관계 규칙 및 그룹을 표시하며, 이러한 정책은 편집할 수 있습니다. 상위 도메인의 선택된 상관관계 규칙 및 그룹도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 상관관계 규칙 및 그룹을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 상위 도메인의 컨피그레이션이 이름, 매니지드 디바이스 등 관련이 없는 도메인에 대한 정보를 표시하는 경우 상위 도메인의 컨피그레이션은 표시되지 않습니다.

활성 상관관계 정책의 규칙에 적용된 변경사항은 즉시 적용됩니다.

시작하기 전에

- 규칙을 삭제하려면 상관관계 정책 관리, 1020 페이지에 설명된 대로 해당 규칙을 모든 상관관계 정책에서 삭제합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Rule Management(**규칙 관리**)**을 클릭합니다.

단계 **2** 규칙 관리:

- Create(생성) - **Create Rule(**규칙 생성**)**를 클릭합니다(상관관계 규칙 설정, 1021 페이지 참조).
- Create Group(그룹 생성) - **Create Group(**그룹 생성**)**을 클릭하고, 그룹의 이름을 입력하고, **Save(**저장**)**를 클릭합니다. 그룹에 규칙을 추가하려면 규칙을 편집합니다.
- 편집 - **Edit(**수정**)** ( )을 클릭합니다. 상관관계 규칙 설정, 1021 페이지의 내용을 참조하십시오. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- Delete Rule or Rule Group(규칙 또는 규칙 그룹 삭제) - **Delete(**삭제**)** ( )을 클릭합니다. 규칙 그룹을 삭제하면 규칙의 그룹이 해제됩니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

상관관계 응답 그룹 설정

알림 및 교정의 상관관계 응답 그룹을 만든 다음, 해당 그룹을 활성화해 활성 상관관계 정책 내의 상관관계 규칙에 할당할 수 있습니다. 시스템은 네트워크 트래픽이 상관관계 규칙과 일치할 때 모든 그룹화된 응답을 실행합니다.

활성 상관관계 정책에서 사용하는 경우, 활성 그룹 또는 그룹화된 응답에 대한 변경사항은 즉시 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Groups(**그룹**)**를 클릭합니다.

단계 **2** **Create Group(**그룹 생성**)**을 클릭합니다.

단계 **3** **Name(**이름**)**을 입력합니다.

단계 **4** 생성 즉시 그룹을 활성화하려면 **Active(**활성**)** 확인란을 선택합니다.

비활성화된 그룹은 응답을 실행하지 않습니다.

단계 **5** 그룹에 대한 **Available Responses(**사용 가능한 응답**)**를 선택하고, 오른쪽 화살표(>)를 클릭해 응답을 **Responses in Group(**그룹 내 응답**)**으로 옮깁니다. 응답을 다른 방식으로 옮기려면 왼쪽 화살표(<)를 사용합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 생성과 동시에 활성화하지 않은 그룹을 지금 활성화하고 싶다면, 슬라이더를 클릭합니다.

관련 항목

Secure Firewall Management Center 알림 응답, 569 페이지
교정 소개, 1071 페이지

상관관계 응답 그룹 관리

상관관계 정책에서 사용하지 않는 응답 그룹을 삭제할 수 있습니다. 응답 그룹을 삭제하면 관련 응답의 그룹이 해제됩니다. 응답 그룹을 삭제하지 않고 일시적으로 비활성화할 수도 있습니다. 이렇게 하면 그룹은 시스템에서 삭제되지 않지만 정책 위반 시 실행되지도 않습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 그룹을 표시하며 이러한 그룹은 수정할 수 있습니다. 상위 도메인에서 생성된 그룹도 표시되지만, 이러한 그룹은 수정할 수 없습니다. 하위 도메인에서 생성된 그룹을 보고 수정하려면 해당 도메인으로 전환하십시오.

사용 중인 활성 응답 그룹에 대한 변경사항은 즉시 적용됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Groups(**그룹**)**를 클릭합니다.

단계 **2** 응답 그룹 관리:

- Activate(활성화) 또는 Deactivate(비활성화) - 슬라이더를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- Create(생성) - **Create Group(**그룹 생성**)**을 클릭합니다(상관관계 응답 그룹 설정, 1054 페이지 참조).
- 편집 - **Edit(**수정**)** ( )을 클릭합니다. 상관관계 응답 그룹 설정, 1054 페이지의 내용을 참조하십시오. **View(**보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 삭제 - **Delete(**삭제**)** ( )을(를) 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

40 장

트래픽 프로파일

다음 주제에서는 트래픽 프로파일을 설정하는 방법을 설명합니다.

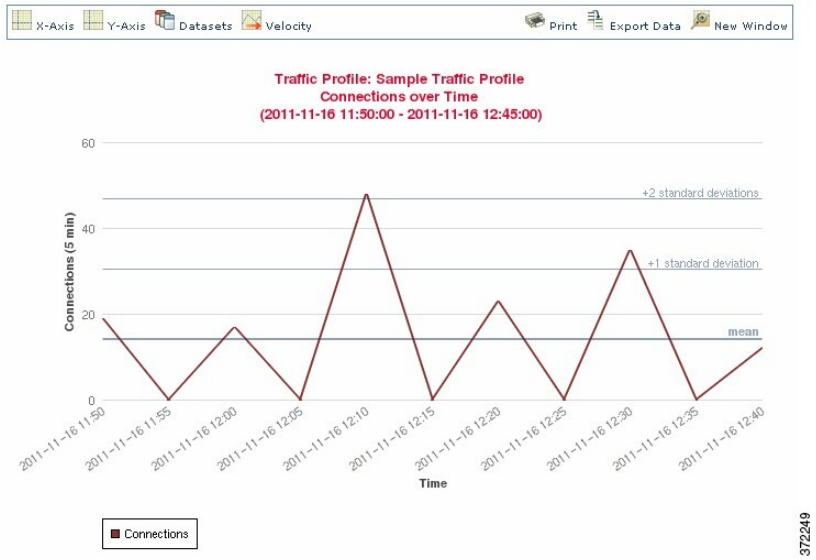
트래픽 프로파일 소개

트래픽 프로파일은 PTW(profiling time window) 동안 수집한 연결 데이터를 기반으로 하는 네트워크 트래픽 그래프입니다. 이 수치는 정상적인 네트워크 트래픽을 나타냅니다. 학습 기간이 지나면, 프로파일을 기준으로 새로운 트래픽을 평가해 비정상적인 네트워크 트래픽을 탐지할 수 있습니다.

기본 PTW는 1주이지만 짧게는 1시간, 길게는 몇 주까지 변경할 수 있습니다. 기본적으로 트래픽 프로파일은 시스템에서 발생한 연결 이벤트에 대한 통계를 5분 간격으로 생성합니다. 그러나 이 샘플링 속도는 최대 1시간까지 늘릴 수 있습니다.

팁 Cisco는 PTW에 100개 이상의 데이터 포인트가 포함되는 것을 권장합니다. 트래픽 프로파일에 통계적으로 유의미한 양의 데이터가 포함되도록 PTW와 샘플링 속도를 설정합니다.

다음 그림은 PTW가 1일, 샘플링 속도가 5분인 트래픽 프로파일을 보여줍니다.



트래픽 프로파일에서 비활성 시간도 설정할 수 있습니다. 트래픽 프로파일은 비활성 기간 동안 데이터를 수집하지만, 프로파일 통계를 계산할 때는 해당 데이터를 사용하지 않습니다. 시간 추이 트래픽 프로파일 그래프에서는 비활성 기간이 음영으로 나타납니다.

예를 들어 모든 워크스테이션이 매일 밤 자정에 백업되는 네트워크 인프라가 있습니다. 백업에는 약 30분이 소요되고 네트워크 트래픽이 급증합니다. 예약된 백업과 일치하도록 트래픽 프로파일에 대한 반복 비활성 기간을 설정할 수 있습니다.

참고 시스템은 연결 종료 시의 데이터를 사용하여 연결 그래프와 트래픽 프로파일을 생성합니다. 트래픽 프로파일을 사용하려면, management center 데이터베이스에 대한 연결 종료 시 이벤트를 기록하는지 확인하십시오.

트래픽 프로파일 구현

트래픽 프로파일을 활성화하면, 시스템은 사용자가 설정한 학습 기간(PTW) 동안 연결 데이터를 수집하고 평가합니다. 학습 기간이 지나면, 시스템은 트래픽 프로파일에 대해 작성된 상관관계 규칙을 평가합니다.

예를 들어 네트워크를 지나는 데이터의 양(패킷, KByte 또는 연결 수 단위로 측정됨)이 급증하여 트래픽 평균량보다 표준 편차의 3배만큼 많아질 때(공격이나 기타 보안 정책 위반의 징후일 수 있음) 트리거되는 규칙을 작성할 수 있습니다. 그런 다음 상관관계 정책에 그 규칙을 포함시켜 트래픽 급증을 알리거나 그에 대한 대응으로 개선 조치를 수행할 수 있습니다.

트래픽 프로파일을 대상으로 지정

프로파일 조건과 호스트 프로파일 자격은 트래픽 프로파일을 제한합니다.

프로파일 조건을 사용하면 모든 네트워크 트래픽의 프로파일을 생성하거나, 트래픽 프로파일을 제한해 도메인, 도메인 내부 또는 여러 도메인 사이에 있는 서브넷, 또는 개별 호스트를 모니터링하도록 제한할 수 있습니다. 다중 도메인 구축의 경우:

- 리프 도메인 관리자는 자신의 리프 도메인 내의 네트워크 트래픽에 대한 프로파일을 생성할 수 있습니다.
- 상위 도메인 관리자는 도메인 내부 또는 도메인 사이에 있는 트래픽에 대한 프로파일을 생성할 수 있습니다.

또한 프로파일 조건을 이용하면 연결 데이터를 기반으로 하는 기준을 사용하여 트래픽 프로파일을 제한할 수도 있습니다. 예를 들어 트래픽 프로파일이 반드시 특정 포트, 프로토콜 또는 애플리케이션을 사용하여 세션의 프로파일을 생성하도록 프로파일 조건을 설정할 수도 있습니다.

마지막으로, 추적한 호스트에 대한 정보를 이용해 트래픽 프로파일을 제한할 수 있습니다. 이러한 제약을 *host profile qualification(*호스트 프로파일 자격*)*이라고 합니다. 예를 들어 중요도가 높은 호스트의 연결 데이터만 수집할 수 있습니다.

참고 트래픽 프로파일을 상위 도메인에 제한하면 각각의 하위 리프 도메인에 있는 같은 유형의 트래픽을 집계하고 프로파일을 생성합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우, 도메인 사이의 트래픽에 대한 프로파일을 생성하면 예기치 않은 결과가 발생할 수 있습니다.

관련 항목

상관관계 정책 및 규칙 소개, 1017 페이지

트래픽 프로파일 조건

단순한 트래픽 프로파일 조건과 호스트 프로파일 자격을 생성하거나 조건을 연결하고 중첩시키는 방법으로 더 정교하게 구성할 수 있습니다.

대부분의 조건은 카테고리, 연산자, 값이라는 3개 부분으로 구성됩니다.

- 사용할 수 있는 카테고리는 트래픽 작성의 대상이 프로파일 조건인지 호스트 프로파일 자격인지에 따라 달라집니다.
- 사용할 수 있는 연산자는 선택한 카테고리에 따라 달라집니다.
- 조건의 값을 지정하는 데 사용 가능한 구문은 카테고리와 연산자에 따라 달라집니다. 텍스트 필드에 직접 값을 입력해야 하는 경우도 있습니다. 그 외의 경우에는 드롭다운 목록에서 하나 이상의 값을 선택할 수 있습니다.

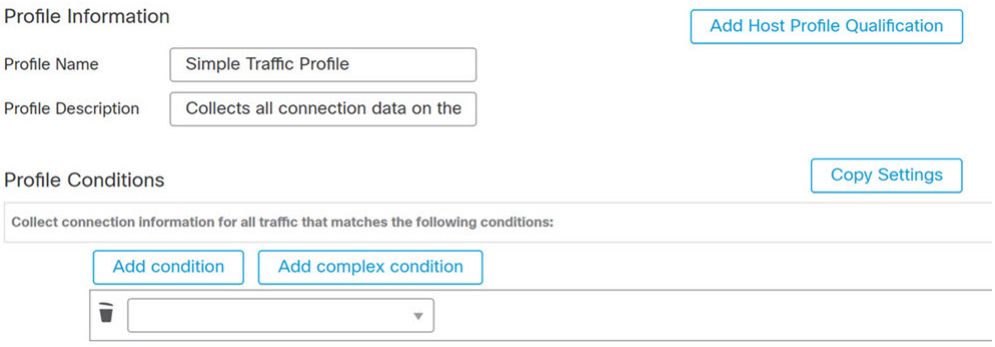
호스트 프로파일 자격의 경우에는, 이니시에이팅 또는 응답 호스트에 관한 정보 데이터를 사용하여 트래픽 프로파일을 제한하는지의 여부도 지정해야 합니다.

여러 개의 조건을 포함할 경우 **AND** 또는 **OR** 연산자로 연결해야 합니다. 동일한 레벨의 조건은 함께 평가됩니다.

- **AND** 연산자를 사용하면 이 연산자가 제어하는 레벨의 모든 조건을 충족해야 합니다.
- **OR** 연산자를 사용하면 이 연산자가 제어하는 레벨의 조건 중 하나 이상을 충족해야 합니다.

제한되지 않은 트래픽 프로파일

모니터링되는 전체 네트워크 세그먼트에 대해 데이터를 수집하는 트래픽 프로파일을 생성하려는 경우 다음 그림과 같이 조건 없는 매우 단순한 프로파일을 생성할 수 있습니다.



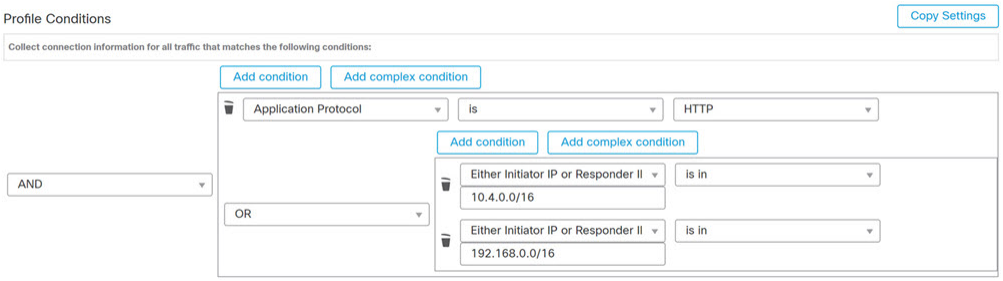
단순 트래픽 프로파일

프로파일을 제한하여 서브넷에 대해서만 데이터를 수집하게 하려는 경우 다음 그림과 같이 하나의 조건을 추가할 수 있습니다.

복합 트래픽 프로파일

다음 트래픽 프로파일에서는 2개의 조건이 **AND**로 연결되어 있습니다. 즉 이 트래픽 프로파일은 두 조건이 모두 참인 경우에만 연결 데이터를 수집합니다. 이 예에서는 IP 주소가 특정 서브넷에 있는 모든 호스트에 대해 HTTP 연결을 수집합니다.

반면 두 서브넷 중 하나의 HTTP 활동에 대한 연결 데이터를 수집하는 다음 트래픽 프로파일은 3개의 조건을 가지며, 그중 마지막은 복합 조건입니다.



논리적으로, 위 트래픽 프로파일은 다음과 같이 평가됩니다.

```
(A and (B or C))
```

항목	조건의 내용
A	Application Protocol Name(애플리케이션 프로토콜 이름)이 HTTP임
B	IP Address가 10.4.0.0/16에 있음
C	IP Address가 192.168.0.0/16에 있음

트래픽 프로필 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 검색 관리자

트래픽 프로파일 관리

활성 상태이며 온전한 트래픽 프로파일에 대해 작성한 규칙만 상관관계 정책 위반을 트리거할 수 있습니다. 각 트래픽 프로파일 옆에 있는 슬라이더는 프로파일이 활성 상태이며 데이터를 수집하고 있음을 나타냅니다. 진행 표시줄은 트래픽 프로파일의 학습 기간 상태를 보여줍니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 트래픽 프로파일을 표시하며, 이러한 규칙은 편집할 수 있습니다. 상위 도메인의 선택된 트래픽 프로파일도 표시되지만, 이러한 대상은 편집할 수는 없습니다. 하위 도메인에서 생성된 트래픽 프로파일을 보고 편집하려면 해당 도메인으로 전환하십시오.

참고 프로파일 조건이 관련이 없는 도메인에 대한 이름이나 매니지드 디바이스 등의 정보를 표시하는 경우, 시스템은 상위 도메인의 프로파일은 표시하지 않습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Traffic Profiles(**트래픽 프로파일**)**을 클릭합니다.

단계 **2** 트래픽 프로파일 관리:

- Activate/Deactivate(활성화/비활성화) - 트래픽 프로파일을 활성화 또는 비활성화하려면 슬라이더를 클릭합니다. 트래픽 프로파일을 비활성화하면 관련 데이터가 삭제됩니다. 프로파일을 재활성화하면, 해당하는 PTW가 지나야 프로파일에 대해 작성한 규칙이 트리거됩니다.
- Create(생성) - 새 트래픽 프로파일을 생성하려면 **New Profile(**새 프로파일**)**을 클릭하고 트래픽 프로파일 설정, 1062 페이지에 설명된 대로 진행합니다. **Copy(**복사**)** ( )를 클릭하여 기존 트래픽 프로파일의 복사본을 편집할 수도 있습니다.
- Delete(삭제) - 트래픽 프로파일을 삭제하려면 **Delete(**삭제**)** ( )를 클릭하고 선택을 확인합니다.
- Edit(편집) - 기존 트래픽 프로파일을 수정하려면 **Edit(**수정**)** ( )을 클릭하고 트래픽 프로파일 설정, 1062 페이지에 설명된 대로 진행합니다. 트래픽 프로파일이 활성 상태인 경우에는 이름과 설명만 바꿀 수 있습니다.
- Graph(그래프) - 트래픽 프로파일을 그래프로 보려면 **Graph(**그래프**)** ( )를 클릭합니다. 다중 도메인 구축의 경우, 그래프가 상관 없는 도메인 관련 정보를 표시한다면 상위 도메인에 속한 트래픽 프로파일의 그래프는 볼 수 없습니다.

트래픽 프로파일 설정

트래픽 프로파일을 상위 도메인에 제한하면 각각의 하위 리프 도메인에 있는 같은 유형의 트래픽을 집계하고 프로파일을 생성합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축의 경우, 도메인 사이의 트래픽에 대한 프로파일을 생성하면 예기치 않은 결과가 발생할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Correlation(**상관관계**)**을(를) 선택하고 **Traffic Profiles(**트래픽 프로파일**)**을 클릭합니다.

단계 **2** **New Profile(**새 프로파일**)**을 클릭합니다.

단계 **3** **Profile Name(**프로파일 이름**)**을 입력하고, 필요한 경우 **Profile Description(**프로파일 설명**)**을 입력합니다.

단계 **4** 선택적으로, 트래픽 프로파일을 제한합니다.

- Copy Settings(설정 복사) - 기본 트래픽 프로파일의 설정을 복사하려면 **Copy Settings(**설정 복사**)**를 클릭하고 사용할 트래픽 프로파일을 선택한 다음 **Load(**불러오기**)**를 클릭합니다.
- Profile Conditions(프로파일 조건) - 추적한 연결이 제공하는 정보를 사용하여 트래픽 프로파일을 제한하려면, 트래픽 프로파일 조건 추가, 1063 페이지에 설명된 대로 진행합니다.
- Host Profile Qualification(호스트 프로파일 자격) - 추적한 호스트가 제공하는 정보를 사용하여 트래픽 프로파일을 제한하려면, 트래픽 프로파일에 호스트 프로파일 자격 추가, 1064 페이지에 설명된 대로 진행합니다.
- PTW(Profiling Time Window) - **Profiling Time Window**를 변경하려면 시간 단위를 입력하고 **hour(s)(**시간**)**, **day(s)(**일**)** 또는 **week(s)(**주**)**를 선택합니다.
- Sampling Rate(샘플링 속도) - **Sampling Rate(**샘플링 속도**)**를 분 단위로 선택합니다.
- Inactive Period(비활성 기간) - **Add Inactive Period(**비활성 기간 추가**)**를 클릭하고 드롭다운 목록을 사용하여 트래픽 프로파일이 비활성 상태를 유지할 시점과 방법을 지정합니다. 비활성 트래픽 프로파일은 상관관계 규칙을 트리거하지 않습니다. 트래픽 프로파일은 비활성 기간에 속하는 데이터는 프로파일 통계에 포함하지 않습니다.

단계 **5** 트래픽 프로파일 저장:

- 프로파일을 저장하고 즉시 데이터 수집을 시작하려면 **Save & Activate(**저장 및 활성화**)**를 클릭합니다.
- 프로파일을 활성화하지 않고 저장하려면 **Save(**저장**)**를 클릭합니다.

트래픽 프로파일 조건 추가

프로시저

단계 **1** Profile Conditions(프로파일 조건)의 트래픽 프로파일 편집기에서 추가할 각 조건에 대해 **Add condition(**조건 추가**)** 또는 **Add complex condition(**복합 조건 추가**)**을 클릭합니다. 수준이 같은 조건은 함께 평가됩니다.

- 연산자가 제어하는 레벨의 모든 조건을 충족해야 하는 경우에는 **AND**를 선택합니다.
- 연산자가 제어하는 레벨의 조건 중 하나만 충족하면 되는 경우에는 **OR**를 선택합니다.

단계 **2** 트래픽 프로파일 조건 구문, 1065 페이지 및 트래픽 프로파일 조건, 1059 페이지에 설명된 대로 각 조건에 대한 카테고리, 연산자, 값을 지정합니다.

is in 또는 **is not in**을 연산자로 선택하면, 트래픽 프로파일 조건에서 여러 값 사용, 1069 페이지에 설명된 대로 단일 조건에서 여러 값을 선택할 수 있습니다.

카테고리가 IP 주소를 나타낼 때 **is in** 또는 **is not in**을 연산자로 선택하면, IP 주소가 IP 주소 범위에서 *is in* 상태인지 *is not in* 상태인지를 지정할 수 있습니다.

예

다음 트래픽 프로파일은 특정 서브넷에 대한 정보를 수집합니다. 이 조건의 카테고리는 **Initiator/Responder IP**, 연산자는 **is in**, 값은 `10.4.0.0/16`입니다.

관련 항목

Firepower System IP 주소 규칙, 28 페이지

트래픽 프로파일에 호스트 프로파일 자격 추가

프로시저

단계 **1** 트래픽 프로파일 편집기에서 **Add Host Profile Qualification(**호스트 프로파일 조건 추가**)**을 클릭합니다.

단계 **2** Host Profile Qualification(호스트 프로파일 자격)에서 추가할 각 조건에 대해 **Add condition(**조건 추가**)** 또는 **Add complex condition(**복합 조건 추가**)**을 클릭합니다. 수준이 같은 조건은 함께 평가됩니다.

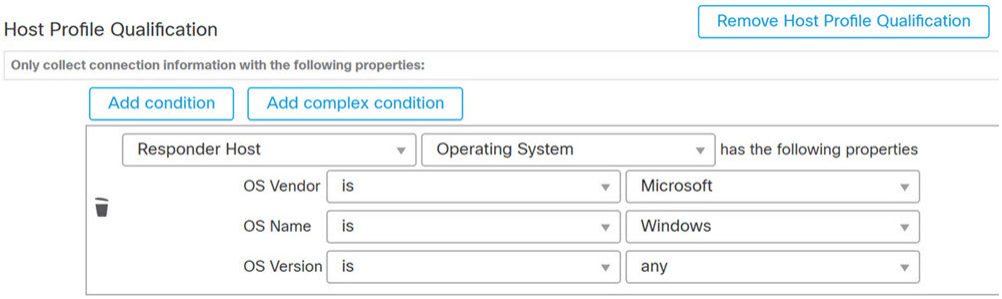
- 연산자가 제어하는 레벨의 모든 조건을 충족해야 하는 경우에는 **AND**를 선택합니다.
- 연산자가 제어하는 레벨의 조건 중 하나만 충족하면 되는 경우에는 **OR**를 선택합니다.

단계 **3** 트래픽 프로파일의 호스트 프로파일 자격 구문, 1066 페이지 및 트래픽 프로파일 조건, 1059 페이지에 설명된 대로 각 조건에 대한 호스트 유형, 카테고리, 연산자, 값을 지정합니다.

is in 또는 **is not in**을 연산자로 선택하면, 트래픽 프로파일 조건에서 여러 값 사용, 1069 페이지에 설명된 대로 단일 조건에서 여러 값을 선택할 수 있습니다.

예

다음 호스트 프로파일 자격은 탐지된 연결의 응답 호스트가 어떤 버전의 Microsoft Windows를 실행하는 경우에만 연결 데이터를 수집하도록 트래픽 프로파일을 제한합니다.



트래픽 프로파일 조건 구문

다음 표에서는 트래픽 프로파일 조건을 작성하는 방법을 설명합니다. 트래픽 프로파일 작성에 사용할 수 있는 연결 데이터는 트래픽 특성과 탐지 방법을 포함한 다양한 요소에 따라 달라집니다.

표 ***131:*** 트래픽 프로파일 조건 구문

다음을 선택하면...	연산자를 선택하고...
애플리케이션 프로토콜	애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트	클라이언트를 하나 이상 선택합니다.
클라이언트 카테고리	클라이언트 카테고리를 하나 이상 선택합니다.
연결 유형	프로파일이 Firepower System 매니지드 디바이스로 모니터링하는 트래픽의 연결 데이터를 사용하는지, 내보낸 NetFlow 기록의 연결 데이터를 사용하는지를 선택합니다. 연결 유형을 지정하지 않는 경우 트래픽 프로파일은 둘 항목을 모두 포함합니다.
Destination Country(목적지 국가) 또는 Source Country(소스 국가)	국가를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다.

다음을 선택하면...	연산자를 선택하고...
이니시에이터 IP, 응답자 IP 또는 이니시에이터/응답자 IP	IP 주소 또는 IP 주소 범위를 입력합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.
NetFlow 디바이스	데이터를 사용해 트래픽 프로파일을 생성할 NetFlow 엑스포터를 선택합니다.
응답자 포트/ICMP 코드	포트 번호 또는 ICMP 코드를 입력합니다.
보안 인텔리전스 범주	보안 인텔리전스 범주를 하나 이상 선택합니다. 트래픽 프로파일 조건에 대한 보안 인텔리전스 카테고리를 사용하려면, 액세스 컨트롤 정책에서 카테고리를 **Block**이 아닌 **Monitor**로 설정해야 합니다.
SSL 암호화된 세션	**Successfully Decrypted(**성공적으로 해독**)**를 선택합니다.
전송 프로토콜	전송 프로토콜로 **TCP** 또는 **UDP**를 입력합니다.
웹 애플리케이션	웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

관련 항목

연결 이벤트 필드 채우기 요구 사항, 793 페이지
Firepower System IP 주소 규칙, 28 페이지

트래픽 프로파일의 호스트 프로파일 자격 구문

호스트 프로파일 자격 조건을 작성할 때 먼저 트래픽 프로파일을 제한하는 데 사용할 호스트를 선택해야 합니다. **Responder Host(**응답자 호스트**)** 또는 **Initiator Host(**이니시에이터 호스트**)** 중 하나를 선택할 수 있습니다. 호스트 역할 선택이 끝나면, 호스트 프로파일 자격 조건 작성을 계속 진행합니다.

NetFlow 기록을 사용하여 네트워크 맵에 호스트를 추가할 수 있지만, 이러한 호스트에 사용할 수 있는 정보는 제한됩니다. 예를 들어 호스트 입력 기능을 사용하여 제공하지 않는 한, 이러한 호스트에 대해서는 어떤 운영체제 데이터도 사용할 수 없습니다. 또한 트래픽 프로파일이 내보낸 NetFlow 기록에의 연결 데이터를 사용할 경우, NetFlow 기록은 연결의 어떤 호스트가 이니시에이터이고 어떤 호스트가 응답자인지에 대한 정보를 포함하지 않습니다. 시스템은 NetFlow 기록을 처리할 때 특정 알고리즘을 사용하여 각 호스트에서 사용 중인 포트 및 해당 포트가 잘 알려진 포트인지 여부를 기반으로 이 정보를 확인합니다.

암시된 클라이언트 또는 일반 클라이언트에 매칭하려면, 클라이언트에 응답하는 서버에서 사용하는 애플리케이션 프로토콜에 따라 호스트 프로파일 자격을 생성합니다. 연결의 initiator 또는 소스가 되는 호스트의 클라이언트 목록에서 어떤 애플리케이션 프로토콜 이름 다음에 클라이언트가 올 경우 그 클라이언트는 암시된 클라이언트일 수 있습니다. 즉 시스템은 탐지된 클라이언트 트래픽이 아니라 해당 클라이언트에 대해 애플리케이션 프로토콜을 사용하는 서버 응답 트래픽을 기반으로 클라이언트를 보고합니다.

예를 들어 시스템에서 호스트의 클라이언트로 **HTTPS client(HTTPS** 클라이언트**)**를 보고할 경우 **Responder Host(**응답자 호스트**)**에 대한 호스트 프로파일 자격을 생성하며, 여기서 **Application Protocol(**애플리케이션 프로토콜**)**은 **HTTPS**로 설정됩니다. 응답자 또는 목적지 호스트에서 보낸 HTTPS 서버 응답 트래픽에 따라 HTTPS 클라이언트가 일반 클라이언트로 보고되기 때문입니다.

표 ***132:*** 호스트 프로파일 자격 구문

다음을 선택하면...	연산자를 선택하고...
애플리케이션 프로토콜 > 애플리케이션 프로토콜	애플리케이션 프로토콜을 하나 이상 선택합니다.
애플리케이션 프로토콜 > 애플리케이션 포트	애플리케이션 프로토콜 포트 번호를 입력합니다.
애플리케이션 프로토콜 > 프로토콜	프로토콜을 선택합니다.
애플리케이션 프로토콜 카테고리	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트 > 클라이언트	클라이언트를 하나 이상 선택합니다.
클라이언트 > 클라이언트 버전	클라이언트 버전을 입력합니다.
클라이언트 카테고리	클라이언트 카테고리를 하나 이상 선택합니다.
도메인	하나 이상의 도메인을 선택합니다. 다중 도메인 구축 시 상위 도메인의 하위 항목에서 보고한 데이터와 일치하는 상위 도메인을 기준으로 제한합니다.
하드웨어	모바일 디바이스 하드웨어 모델을 입력합니다. 예를 들어 일치하는 모든 Apple iPhone을 찾으려면 `iPhone`을 입력합니다.
호스트 중요도	호스트 중요도를 선택합니다.
호스트 유형	호스트 유형을 하나 이상 선택합니다. 일반 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.
IOC 태그	IOC 태그를 하나 이상 선택합니다.
탈옥됨	이벤트의 호스트가 탈옥 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
MAC 주소 > MAC 주소	호스트의 MAC 주소 전체 또는 일부를 입력합니다.

다음을 선택하면...	연산자를 선택하고...
MAC 주소 > MAC 유형	MAC 유형이**ARP/DHCP Detected**인지, 즉 다음인지를 선택합니다. • 시스템이 MAC 주소가 호스트에 속한 것으로 명확하게 확인함(**is ARP/DHCP Detected**) • 디바이스와 호스트 간에 라우터가 있다는 등의 이유로, 시스템이 MAC 주소가 있는 다양한 호스트를 확인함(**is not ARP/DHCP Detected**) • MAC 유형이 올바르지 않음(**is any**)
MAC 벤더	호스트에서 사용하는 하드웨어의 MAC 벤더 전체 또는 일부를 입력합니다.
모바일	이벤트의 호스트가 모바일 디바이스이면 **Yes(**예**)**, 아니면 **No(**아니오**)**를 선택합니다.
NETBIOS 이름	호스트의 NetBIOS 이름을 입력합니다.
네트워크 프로토콜	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
운영체제 > OS 벤더	운영체제 벤더 이름을 하나 이상 선택합니다.
운영체제 > OS 이름	운영체제 이름을 하나 이상 선택합니다.
운영체제 > OS 버전	운영체제 버전을 하나 이상 선택합니다.
전송 프로토콜	http://www.iana.org/assignments/protocol-numbers에 열거된 전송 프로토콜의 이름 또는 번호를 입력합니다.
VLAN ID	호스트의 VLAN ID 번호를 입력합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 VLAN 태그를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.
웹 애플리케이션	웹 애플리케이션을 하나 이상 선택합니다.
웹 애플리케이션 카테고리	웹 애플리케이션 카테고리를 하나 이상 선택합니다.
사용 가능한 모든 호스트 속성(기본 규정준수 허용리스트 호스트 속성 포함)	선택하는 호스트 속성의 유형에 따라 알맞은 값을 지정합니다. • 호스트 속성 유형이 Integer(정수)일 경우 그 특성에 대해 정의된 범위의 정수 값을 입력합니다. • 호스트 속성 유형이 Text(텍스트)일 경우 텍스트 값을 입력합니다. • 호스트 속성 유형이 List(목록)일 경우 유효한 목록 문자열을 선택합니다. • 호스트 속성 유형이 URL일 경우 URL 값을 입력합니다.

트래픽 프로파일 조건에서 여러 값 사용

조건을 작성할 때 조건 구문상 드롭다운 목록의 값 선택이 가능할 경우, 대개는 목록에서 여러 값을 사용할 수 있습니다.

예를 들어 호스트가 UNIX의 특정 버전을 실행해야한다는 조건을 호스트 프로파일 자격으로 트래픽 프로파일에 추가하려는 경우, 여러 조건을 OR 연산자로 연결하는 대신 다음 절차를 사용합니다.

프로시저

단계 **1** 트래픽 프로파일 또는 호스트 프로파일 자격 조건을 작성할 때, **is in** 또는 **is not in**을 연산자로 선택합니다.
드롭다운 목록이 텍스트 필드로 바뀝니다.

단계 **2** 텍스트 필드의 아무 곳이나 클릭하거나 **Edit(**편집**)** 링크를 클릭합니다.

단계 **3** **Available(**사용 가능**)**에서 여러 값을 선택합니다.

단계 **4** 오른쪽 화살표를 클릭하여 선택한 항목을 **Selected**로 옮깁니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

41 장

교정

다음 주제는 교정 설정 관련 정보를 제공합니다.

교정 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 검색 관리자

교정 소개

교정은 Firepower System이 상관관계 위반에 대한 응답으로 실행하는 프로그램입니다.

교정을 실행하면, 시스템은 교정 상태 이벤트를 생성합니다. 교정 상태 이벤트는 교정 이름, 상관관계 정책 및 이를 트리거한 규칙, 종료 상태 메시지 등의 상세정보를 포함합니다.

시스템은 여러 교정 모듈을 지원합니다.

- Cisco ISE ANC(Adaptive Network Control) - 상관관계 정책 위반과 관련된 ISE 설정 ANC 정책을 적용하거나 지웁니다.
- Cisco IOS Null Route - 상관관계 정책 위반과 관련된 호스트 또는 네트워크로 전송된 트래픽을 차단(Cisco IOS 버전 12.0 이상 필수)
- Nmap Scanning(Nmap 스캐닝) - 호스트를 스캔해 실행 중인 운영체제와 서버 확인
- Set Attribute Value(속성 값 설정) - 상관관계 정책 위반과 관련된 호스트에서 호스트 속성 설정

팁 다른 작업을 수행하는 맞춤형 모듈을 설치할 수 있습니다(*Firepower System Remediation API* 설명서 참조).

교정 구현

교정을 구현하려면, 먼저 선택한 모듈에 대한 인스턴스를 하나 이상 만들어야 합니다. 모듈당 여러 인스턴스를 만들 수 있으며, 이때 각 인스턴스는 저마다 다르게 설정됩니다. 예를 들어 Cisco IOS Null Route 교정 모듈을 사용하여 여러 라우터와 통신하려면, 해당 모듈이 인스턴스 다수를 설정해야 합니다.

그런 다음 정책 위반 시 수행할 작업을 설명하는 여러 교정을 각 인스턴스에 추가합니다.

마지막으로, 교정을 상관관계 정책에 있는 규칙과 연결해 시스템이 상관관계 정책 위반에 대한 응답으로 교정을 실행하게 합니다.

교정 및 멀티 테넌시

다중 도메인 구축의 경우에는, 어떤 도메인 레벨에서도 맞춤형 교정 모듈을 설치할 수 있습니다. 시스템 제공 모듈은 Global(전역) 도메인에 속합니다.

상위 도메인에서 생성한 인스턴스에는 교정을 추가할 수 없지만, 비슷하게 설정한 인스턴스를 현재 도메인에 생성하고 해당 인스턴스에 교정을 추가할 수는 있습니다. 상위 도메인에서 생성한 교정을 상관관계 응답으로 사용할 수도 있습니다.

관련 항목

Secure Firewall Management Center 알림 응답, 569 페이지
Nmap 스캐닝
규칙 및 허용 리스트에 응답 추가, 1020 페이지

Cisco ISE EPS 교정

ISE 구축에서 EPS(Endpoint Protection Service)를 활성화하고 설정하면, ISE를 사용하여 교정을 실행하도록 management center을(를) 설정할 수 있습니다. 완벽하게 구성되면, ISE EPS 교정은 상관관계 정책 위반과 관련된 소스 또는 목적지 호스트에서 다음 **Mitigation Actions(**완화 작업**)**을 실행합니다.

- **`quarantine`(**격리**)** - 엔드포인트의 네트워크 액세스를 제한 또는 거부

- **unquarantine(**격리 해제**)** - 엔드포인트의 격리 상태를 역전하고 네트워크에 대한 모든 액세스를 허가
- **shutdown(**종료**)** - 엔드포인트의 NAS(network attached system) 포트를 비활성화해 네트워크에서 분리

또한 특정 IP 주소를 ISE EPS 교정에서 제외할 수 있습니다.

참고 ISE 버전 및 구성은 ISE를 사용할 수 있는 방법에 영향을 미칩니다. 예를 들어 ISE-PIC를 사용하여 ISE EPS 교정을 수행할 수는 없습니다. 자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *ISE/ISE-PIC*를 이용한 사용자 제어 장을 참고하십시오.

ISE EPS 작업에 대한 자세한 내용은 *Cisco Identity Services Engine* 사용자 설명서를 참조하십시오.

ISE EPS 교정 설정

소스 또는 목적지 호스트에서 ISE EPS 교정을 실행하여 상관관계 정책 위반에 응답할 수 있습니다.

참고 ISE-PIC는 ISE EPS 치료를 수행할 수 없습니다.

시작하기 전에

- ISE 서버에서 EPS 작업을 설정합니다.
- 사용자 제어를 위한 ISE/ISE-PIC 설정에 설명된 대로 ISE에 대한 연결을 설정합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.
단계 **2** ISE EPS 인스턴스 추가, 1073 페이지에 설명된 대로 pxGrid 완화 인스턴스를 추가합니다.
단계 **3** ISE EPS 교정 추가, 1074 페이지에 설명된 대로 ISE EPS 교정을 하나 이상 추가합니다.

다음에 수행할 작업

- 규칙 및 허용 리스트에 응답 추가, 1020 페이지에 설명된 대로 상관관계 정책 위반에 대한 응답으로 교정을 할당합니다.

ISE EPS 인스턴스 추가

ISE EPS 인스턴스를 생성해 개별 교정을 유형별로 그룹화합니다.

프로시저

단계 1 **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 2 **Add a New Instance(**새 인스턴스 추가**)** 목록에서 **pxGrid Mitigation(v1.0)**을 모듈 유형으로 선택하고 **Add(**추가**)**를 클릭합니다.

단계 3 **Instance Name(**인스턴스 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 4 **Enable Logging(**기록 활성화**)** 옵션을 설정해 시스템 기록을 활성화 또는 비활성화합니다.

단계 5 **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- 속성값 설정 교정 추가, 1081 페이지에 설명된 대로 ISE EPS 교정을 생성합니다.

관련 항목

Firepower System IP 주소 규칙, 28 페이지

ISE EPS 교정 추가

인스턴스에서 ISE EPS 교정을 하나 이상 생성해 상관관계 정책 위반과 관련된 소스 또는 목적지 호스트에서 다음 **Mitigation Actions(**완화 작업**)**을 실행합니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- ISE EPS 인스턴스 추가, 1073 페이지에 설명된 대로 ISE EPS 인스턴스를 생성합니다.

프로시저

단계 1 **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 2 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 3 **Configured Remediations(**설정한 교정**)** 섹션에서 **Mitigate Destination(**목적지 완화**)** 또는 **Mitigate Source(**소스 완화**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 4 **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 5 **Mitigation Action(**완화 작업**)**: **quarantine(**격리**)**, **unquarantine(**격리 해제**)** 또는 **shutdown(**종료**)** 을 선택합니다.

단계 6 (선택 사항) 교정에서 IP 주소 또는 범위를 제외하려면 **Allow List(**허용 목록**)** 상자에 입력합니다.

단계 **7** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가, 1020 페이지를 참조하십시오.

Cisco IOS Null Route 교정

Cisco IOS Null Route 교정 모듈을 이용하면 Cisco의 "null route" 명령을 사용하여 IP 주소 또는 주소 범위를 차단할 수 있습니다. 이렇게 하면 라우터의 NULL 인터페이스로 라우팅하여 호스트나 네트워크에 전송한 모든 트래픽이 삭제됩니다. 위반 호스트 또는 네트워크에서 전송된 트래픽은 차단되지 않습니다.

참고 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

주의 Cisco IOS 교정이 활성화되는 경우에는 시간 초과 기간이 없습니다. IP 주소 또는 네트워크를 차단 해제하려면, 라우팅 변경사항을 라우터에서 수동으로 삭제해야 합니다.

Cisco IOS 라우터에 대한 교정 설정

참고 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

주의 Cisco IOS 교정이 활성화되는 경우에는 시간 초과 기간이 없습니다. IP 주소 또는 네트워크를 차단 해제하려면, 라우팅 변경사항을 라우터에서 수동으로 삭제해야 합니다.

시작하기 전에

- Cisco 라우터가 Cisco IOS 12.0 이상을 실행 중인지 확인합니다.
- 라우터에 대한 레벨 15 관리 액세스가 있는지 확인합니다.

프로시저

단계 **1** Cisco 라우터 또는 IOS 소프트웨어와 함께 제공된 문서에 설명된 대로 Cisco 라우터에서 텔넷을 활성화합니다.

단계 **2** management center에서, 사용할 각 Cisco IOS 라우터에 대해 Cisco IOS Null Route 인스턴스를 추가합니다(Cisco IOS 인스턴스 추가, 1076 페이지 참조).

단계 **3** 상관관계 정책이 위반될 때 라우터에서 이끌어낼 응답의 유형을 기반으로 각 인스턴스에 대한 교정을 생성합니다.

- Cisco IOS Block Destination 교정 추가, 1077 페이지
- Cisco IOS Block Destination Network 교정 추가, 1078 페이지
- Cisco IOS Block Source 교정 추가, 1079 페이지
- Cisco IOS Block Source Network 교정 추가, 1079 페이지

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가, 1020 페이지를 참조하십시오.

Cisco IOS 인스턴스 추가

여러 라우터로 교정을 전송하려는 경우 각 라우터에 대해 개별 인스턴스를 생성합니다.

시작하기 전에

- Cisco 라우터 또는 IOS 소프트웨어와 함께 제공된 문서에 설명된 대로 Cisco 라우터에서 텔넷 액세스를 설정합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** **Add a New Instance(**새 인스턴스 추가**)** 목록에서 **Cisco IOS Null Route**를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **3** **Instance Name(**인스턴스 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **4** 교정에 대해 사용하려는 Cisco IOS 라우터의 IP 주소를 **Router IP** 필드에 입력합니다.

단계 **5** 라우터에 대한 텔넷 사용자 이름을 **Username(**사용자 이름**)** 필드에 입력합니다. 이 사용자는 라우터에 대한 레벨 15 관리 액세스 권한이 있어야 합니다.

단계 **6** 텔넷 사용자의 사용자 비밀번호를 **Connection Password(**연결 비밀번호**)** 필드에 입력합니다.

단계 **7** 텔넷 사용자의 활성 비밀번호를 **Enable Password(**비밀번호 활성화**)** 필드에 입력합니다. 이 비밀번호는 라우터의 특권 모드로 들어가기 위해 사용되는 비밀번호입니다.

단계 **8** 교정에서 제외할 IP 주소 또는 범위를 한 줄에 하나씩 **Allow List(**허용 목록**)** 필드에 입력합니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

단계 **9** **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- Cisco IOS Block Destination 교정 추가, 1077 페이지, Cisco IOS Block Destination Network 교정 추가, 1078 페이지, Cisco IOS Block Source 교정 추가, 1079 페이지, Cisco IOS Block Source Network 교정 추가, 1079 페이지에 설명된 대로 상관관계 정책이 사용할 특정 교정을 추가합니다.

관련 항목

Firepower System IP 주소 규칙, 28 페이지

Cisco IOS Block Destination 교정 추가

Cisco IOS Block Destination 교정은 라우터에서 상관관계 정책 위반과 관련된 목적지 호스트로 전송된 트래픽을 차단합니다. 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 1076 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** (👁)를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Destination(**목적지 차단**)**을 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **5** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가, 1020 페이지를 참조하십시오.

Cisco IOS Block Destination Network 교정 추가

Cisco IOS Block Destination Network 교정은 라우터에서 상관관계 정책 위반과 관련된 목적지 호스트의 네트워크로 전송된 트래픽을 차단합니다. 검색 또는 호스트 입력 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 목적지 기반 교정을 사용하지는 마십시오. 이러한 이벤트는 소스 호스트와 연결됩니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 1076 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Destination Network(**목적지 네트워크 차단**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **5** **Netmask(**넷마스크**)** 필드에 서브넷 마스크를 입력하거나 CIDR 표기법을 사용하여 트래픽을 차단할 네트워크를 설명합니다.

예를 들어 단일 호스트가 규칙을 트리거했을 때 전체 Class C 네트워크에 대한 트래픽을 차단하려면 (권장 사항이 아님) 넷마스크로 `255.255.255.0` 또는 `24`를 사용합니다.

또 다른 예로, 트리거하는 IP 주소를 포함하는 30개 주소에 대한 트래픽을 차단하려면 넷마스크로 `255.255.255.224` 또는 `27`을 지정합니다. 이 경우 IP 주소 `10.1.1.15`가 교정을 트리거하면 `10.1.1.1`과 `10.1.1.30` 사이의 모든 IP 주소가 차단됩니다. 트리거하는 IP 주소만 차단하려면 필드를 비워두거나, `32`를 입력하거나, `255.255.255.255`를 입력합니다.

단계 **6** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가, 1020 페이지를 참조하십시오.

관련 항목

Firepower System IP 주소 규칙, 28 페이지

Cisco IOS Block Source 교정 추가

Cisco IOS Block Source 교정은 라우터에서 상관관계 정책 위반과 관련된 소스 호스트로 전송된 트래픽을 차단합니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 1076 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Source(**소스 차단**)**을 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **5** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가, 1020 페이지를 참조하십시오.

Cisco IOS Block Source Network 교정 추가

Cisco IOS Block Source Network 교정은 라우터에서 상관관계 정책 위반과 관련된 소스 호스트의 네트워크로 전송된 트래픽을 차단합니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- Cisco IOS 인스턴스 추가, 1076 페이지의 설명대로 Cisco IOS 인터페이스를 추가합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Block Source Network(**소스 네트워크 차단**)**을 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **5** **Netmask(**넷마스크**)** 필드에 서브넷 마스크를 입력하거나 트래픽을 차단할 네트워크를 설명하는 CIDR 표기법을 입력합니다.

예를 들어 단일 호스트가 규칙을 트리거했을 때 전체 Class C 네트워크에 대한 트래픽을 차단하려면 (권장 사항이 아님) 넷마스크로 `255.255.255.0` 또는 `24`를 사용합니다.

또 다른 예로, 트리거하는 IP 주소를 포함하는 30개 주소에 대한 트래픽을 차단하려면 넷마스크로 `255.255.255.224` 또는 `27`을 지정합니다. 이 경우 IP 주소 `10.1.1.15`가 교정을 트리거하면 `10.1.1.1`과 `10.1.1.30` 사이의 모든 IP 주소가 차단됩니다. 트리거하는 IP 주소만 차단하려면 필드를 비워두거나, `32`를 입력하거나, `255.255.255.255`를 입력합니다.

단계 **6** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가, 1020 페이지를 참조하십시오.

관련 항목

Firepower System IP 주소 규칙, 28 페이지

Nmap 스캔 교정

Firepower System은 네트워크 탐색 및 보안 감사를 위한 오픈 소스 활성 스캐너인 Nmap™과 통합됩니다. Nmap 교정을 사용하여 상관관계 정책 위반에 응답할 수 있으며, 이 경우 Nmap 스캔 교정이 트리거됩니다.

Nmap 스캔에 대한 자세한 정보는 Nmap 스캐닝 섹션을 참조하십시오.

속성 값 교정 설정

트리거링 이벤트가 발생한 호스트에서 호스트 속성 값을 설정하여 상관관계 정책 위반에 응답할 수 있습니다. 텍스트 호스트 속성의 경우에는 이벤트의 설명을 속성 값으로 사용할 수 있습니다.

세트 속성값 교정 구성

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 속성값 설정 인스턴스 추가, 1081 페이지에 설명된 대로 세트 속성 인스턴스를 생성합니다.

단계 **3** 속성값 설정 교정 추가, 1081 페이지에 설명된 대로 세트 속성 교정을 추가합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가, 1020 페이지를 참조하십시오.

관련 항목

사전 정의된 호스트 속성, 911 페이지
사용자 정의 호스트 속성, 911 페이지

속성값 설정 인스턴스 추가

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** **Add a New Instance(**새 인스턴스 추가**)** 목록에서 **Set Attribute Value(**속성 값 설정**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **3** **Instance Name(**인스턴스 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **4** **Create(**생성**)**를 클릭합니다.

다음에 수행할 작업

- 속성값 설정 교정 추가, 1081 페이지에 설명된 대로 속성 설정 교정을 생성합니다.

속성값 설정 교정 추가

Set Attribute Value(속성 값 설정) 교정은 상관관계 정책 위반과 관련된 호스트에서 호스트 속성을 설정합니다. 설정할 각 속성값에 대한 교정을 생성합니다. 텍스트 속성의 경우에는 트리거링 이벤트의 설명을 속성 값으로 사용할 수 있습니다.

다중 도메인 구축에서는 상위 도메인에서 생성된 인스턴스에 치료를 추가할 수 없습니다.

시작하기 전에

- 속성값 설정 인스턴스 추가, 1081 페이지에 설명된 대로 세트 속성 인스턴스를 생성합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정을 추가하려는 인스턴스 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** **Configured Remediations(**설정한 교정**)** 섹션에서 **Set Attribute Value(**속성값 설정**)**를 선택하고 **Add(**추가**)**를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **4** **Remediation Name(**교정 이름**)**과 **Description(**설명**)**을 입력합니다.

단계 **5** 소스 및 목적지 데이터가 있는 이벤트에 대한 응답으로 이 교정을 사용하려면, **Update Which Host(s) From Event(**이벤트의 호스트 업데이트**)** 옵션을 선택합니다.

단계 **6** 텍스트 속성의 경우에는 **Use Description From Event For Attribute Value(**속성값으로 이벤트의 설명 사용**)** 여부를 지정합니다.

- 이벤트의 설명을 속성값으로 사용하려면 **On(**설정**)**을 클릭하고 설정할 **Attribute Value(**속성값**)**를 입력합니다.
- 교정에 대한 **Attribute Value(**속성값**)** 설정을 속성값으로 사용하려면 **Off(**해제**)**를 선택합니다.

단계 **7** **Create(**생성**)**를 클릭하고 **Done(**완료**)**을 클릭합니다.

다음에 수행할 작업

- 상관관계 정책 위반에 대한 응답으로 치료를 할당합니다. 규칙 및 허용 리스트에 응답 추가, 1020 페이지를 참조하십시오.

교정 모듈 관리

다중 도메인 구축의 경우 시스템은 현재 도메인에 설치된 Nmap 교정 모듈을 표시하며, 이러한 모듈은 삭제할 수 있습니다. 상위 도메인에 설치된 모듈도 표시되지만, 이러한 모듈은 수정할 수 없습니다. 하위 도메인의 교정 모듈을 관리하려면 해당 도메인으로 전환하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Modules(**모듈**)**을(를) 선택합니다.

단계 **2** 교정 모듈 관리:

- Configure(설정) - 모듈에 대한 Module Detail(모듈 상세정보) 페이지를 확인하고 모듈의 인스턴스와 교정을 설정하려면, **View(**보기**)** ( )을 클릭합니다. 다중 도메인 구축의 경우에는 Module Detail(모듈 상세정보) 페이지를 사용하여 상위 도메인에 설치된 모듈의 현재 도메인에 있는 인

스턴스를 추가, 삭제 또는 편집할 수 없습니다. 대신 Instances(인스턴스) 페이지(**Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**)를 사용하십시오(교정 인스턴스 관리, 1083 페이지 참조).

- Delete(삭제) - 사용하지 않은 맞춤형 모듈을 삭제하려면 **Delete(**삭제**)** ( )을 클릭합니다. 시스템 제공 모듈은 삭제할 수 없습니다.
- Install(설치) - 맞춤형 모듈을 설치하려면 **Choose File(**파일 선택**)**을 클릭하고, 모듈을 찾은 다음 **Install(**설치**)**을 클릭합니다. 자세한 내용은 *Firepower System Remediation API* 설명서를 참조하십시오.

교정 인스턴스 관리

Instances(인스턴스) 페이지는 모든 교정 모듈을 대상으로, 설정된 인스턴스를 모두 열거합니다.

다중 도메인 구축의 경우 시스템은 현재 도메인에서 생성된 교정 인스턴스를 표시하며 이러한 인스턴스는 편집할 수 있습니다. 상위 도메인에서 생성된 인스턴스도 표시되지만, 이러한 인스턴스는 편집할 수 없습니다. 하위 도메인의 교정 인스턴스를 관리하려면 해당 도메인으로 전환하십시오.

상위 도메인에서 생성한 인스턴스에는 교정을 추가할 수 없지만, 비슷하게 설정한 인스턴스를 현재 도메인에 생성하고 해당 인스턴스에 교정을 추가할 수는 있습니다. 상위 도메인에서 생성한 교정을 상관관계 응답으로 사용할 수도 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**을(를) 선택합니다.

단계 **2** 교정 인스턴스 관리:

- Add(추가) - 인스턴스를 추가하려면 인스턴스를 추가할 교정 모듈을 선택하고 **Add(**추가**)**를 클릭합니다. 시스템 제공 모듈의 경우에는 다음을 참조하십시오.
  - ISE EPS 인스턴스 추가, 1073 페이지
  - Cisco IOS 인스턴스 추가, 1076 페이지
  - Cisco Secure Firewall Management Center 디바이스 구성 가이드
  - 속성값 설정 인스턴스 추가, 1081 페이지

  맞춤형 모듈 추가 관련 도움이 필요하다면 해당 모듈의 설명서(존재하는 경우)를 참조하십시오.
- Configure(구성) - 인스턴스 상세정보를 구성하고 교정을 인스턴스에 추가하려면 **View(**보기**)** ( )를 클릭합니다.
- Delete(삭제) - 사용하지 않는 인스턴스를 삭제하려면 **Delete(**삭제**)** ( )를 클릭합니다.

단일 교정 모듈 인스턴스 관리

Module Detail(모듈 상세정보) 페이지는 특정 교정 모듈에 대해 설정된 인스턴스와 교정을 모두 표시합니다.

다중 도메인 구축의 경우에는, 현재 도메인과 상위 도메인에 설치된 교정 모듈에 대한 Module Detail(모듈 상세정보) 페이지에 액세스할 수 있습니다. 그러나 Module Detail(모듈 상세정보) 페이지를 사용하여 상위 도메인에 설치된 모듈의 현재 도메인에 있는 인스턴스를 추가, 삭제 또는 편집할 수는 없습니다. 대신 Instances(인스턴스) 페이지(**Policies(**정책**)** > **Actions(**작업**)** > **Instances(**인스턴스**)**)를 사용하십시오(교정 인스턴스 관리, 1083 페이지 참조).

프로시저

단계 **1** **Policies(**정책**)** > **Actions(**작업**)** > **Modules(**모듈**)**을(를) 선택합니다.

단계 **2** 관리할 인스턴스가 있는 교정 모듈 옆에 있는 **View(**보기**)** ( )를 클릭합니다.

단계 **3** 교정 인스턴스 관리:

- Add(추가) - 인스턴스를 추가하려면 **Add(**추가**)**를 클릭합니다. 시스템 제공 모듈의 경우에는 다음을 참조하십시오.
  - ISE EPS 인스턴스 추가, 1073 페이지
  - Cisco IOS 인스턴스 추가, 1076 페이지
  - Cisco Secure Firewall Management Center 디바이스 구성 가이드
  - 속성값 설정 인스턴스 추가, 1081 페이지

  맞춤형 모듈을 위한 인스턴스 추가 관련 도움이 필요하다면 해당 모듈의 설명서(존재하는 경우)를 참조하십시오.
- Configure(구성) - 인스턴스 상세정보를 구성하고 교정을 인스턴스에 추가하려면 **View(**보기**)** ( )를 클릭합니다.
- Delete(삭제) - 사용하지 않는 인스턴스를 삭제하려면 **Delete(**삭제**)** ( )를 클릭합니다.

X 부

참조

42 장

Secure Firewall Management Center 명령줄 참조

이 참조에서는 Secure Firewall Management Center의 명령줄 인터페이스(CLI)에 대해 설명합니다.

참고 Secure Firewall Threat Defense의 경우에는 Cisco Secure Firewall Threat Defense 명령 참조의 내용을 참조하십시오.

Secure Firewall Management Center CLI 정보

SSH를 이용해 management center에 로그인하면, CLI에 액세스하게 됩니다. 권장하지는 않지만, `expert` 명령을 사용하여 Linux 셸에 액세스할 수도 있습니다.

주의 Cisco TAC가 지시하거나 Firepower 사용자 설명서에서 명시적으로 지시하지 않는 한, Linux 셸에 액세스하지 않는 것이 좋습니다.

주의 Linux 셸 액세스 권한이 있는 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- 외부 인증을 설정하는 경우 Linux 셸 액세스 권한이 있는 사용자 목록을 적절하게 제한해야 합니다.
- 사전 정의된 관리자 사용자 외에 Linux 셸 사용자를 설정하지 마십시오.

이 부록에 설명된 명령을 사용하여 Secure Firewall Management Center을(를) 보고 문제를 해결할 수 있을 뿐 아니라 제한된 구성 작업도 수행할 수 있습니다.

Secure Firewall Management Center CLI 모드

CLI는 4가지 모드를 포함합니다. 기본 모드인 CLI Management에는 CLI 자체 내에서 탐색하기 위한 명령이 포함됩니다. 나머지 모드에는 Secure Firewall Management Center 기능의 세 가지 영역을 처리하는 명령이 포함됩니다. 이러한 모드 내의 명령은 모드 이름(`system`, `show` 또는 `configure`)으로 시작합니다.

모드에 진입하면 CLI 프롬프트는 현재 모드를 반영하도록 변경됩니다. 예를 들어 시스템 구성 요소에 대한 버전 정보를 표시하려면 표준 CLI 프롬프트에서 전체 명령을 입력할 수 있습니다.

```
> show version
```

`show` 모드에 진입한 경우, show 모드 CLI 프롬프트에서 `show` 키워드 없이 명령을 입력할 수 있습니다.

```
show> version
```

Secure Firewall Management Center CLI 관리 명령

CLI 관리 명령은 CLI와 상호 작용하는 기능을 제공하며, 디바이스의 작동에는 영향을 미치지 않습니다.

exit

CLI 컨텍스트를 다음으로 가장 높은 CLI 컨텍스트 레벨로 이동합니다. 기본 모드에서 이 명령을 실행하면 현재 CLI 세션에서 사용자가 로그아웃됩니다.

Syntax

```
exit
```

예

```
system> exit
>
```

expert

Linux 셸을 호출합니다.

Syntax

```
expert
```

예

```
> expert
```

? (물음표)

CLI 명령 및 매개 변수에 대한 상황별 도움말을 표시합니다. 물음표(?) 명령은 다음과 같이 사용하십시오.

- 현재 CLI 컨텍스트 내에서 사용 가능한 명령의 도움말을 표시하려면 명령 프롬프트에서 물음표(?)를 입력합니다.
- 특별한 문자 집합으로 시작되는 사용 가능한 명령 목록을 표시하려면 약식 명령 바로 뒤에 물음표(?)를 입력합니다.
- 명령의 공식적인 인수에 대한 도움말을 표시하려면 명령 프롬프트에서 인수 자리에 물음표(?)를 입력합니다.

물음표(?)는 콘솔로 다시 에코되지 않습니다.

Syntax

```
?
abbreviated_command ?
command [arguments] ?
```

예

```
> ?
```

Secure Firewall Management Center CLI show 명령

show 명령은 어플라이언스의 상태에 대한 정보를 제공합니다. 이러한 명령은 어플라이언스의 작동 모드를 변경하지 않으며, 명령 실행 시 시스템 작동에 미치는 영향이 최소 수준입니다.

version

제품 버전 및 빌드를 표시합니다.

Syntax

```
show version
```

예

```
> show version
```

Secure Firewall Management Center CLI 구성 명령

configuration 명령을 통해 사용자는 시스템을 구성 및 관리할 수 있습니다. 이러한 명령은 시스템 작동에 영향을 줍니다.

password

현재 CLI 사용자가 자신의 비밀번호를 변경하도록 허용합니다.

주의 시스템 보안상의 이유로 모든 어플라이언스에서 사전 정의된 관리자 외에 셸 사용자를 설정하지 않는 것이 좋습니다.

참고 `password` 명령은 내보내기 모드에서 지원되지 않습니다. 보안 방화벽 시스템에서 관리자의 비밀번호를 재설정하려면 자세한 정보를 참조하십시오. 전문가 모드에서 `password` 명령을 사용하여 관리자 비밀번호를 재설정하는 경우 `configure user admin password` 명령을 사용하여 비밀번호를 재구성하는 것이 좋습니다. 비밀번호를 재구성한 후 전문가 모드로 전환하고 관리자 사용자의 비밀번호 해시가 /opt/cisco/config/db/sam.config 및 /etc/shadow 파일에서 동일한지 확인합니다.

이 명령을 실행하면 현재(또는 이전) 비밀번호를 입력하라는 CLI 프롬프트가 표시된 다음 새 비밀번호를 두 번 입력하라는 프롬프트가 표시됩니다.

Syntax

```
configure password
```

예

```
> configure password
```

```
Changing password for admin.
(current) UNIX password:
New UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Secure Firewall Management Center CLI 시스템 명령

system 명령을 사용하면 시스템 전반의 파일 및 액세스 제어 설정을 관리할 수 있습니다.

generate-troubleshoot

Cisco에서 분석할 문제 해결 데이터를 생성합니다.

Syntax

```
system generate-troubleshoot option1 optionN
```

여기서 옵션은 다음 중 하나 이상이며 공백으로 구분됩니다.

- `All`: 다음 옵션을 모두 실행.
- `SNT`: Snort 성능 및 구성
- `PER`: 하드웨어 성능 및 로그
- `SYS`: 시스템 구성, 정책, 로그
- `DES`: 탐지 구성, 정책, 로그
- `NET`: 인터페이스 및 네트워크 관련 데이터
- `VDB`: 검색, 인식, VDB 데이터, 로그
- `UPG`: 업그레이드 데이터 및 로그
- `DBO`: 모든 데이터베이스 데이터
- `LOG`: 모든 로그 데이터
- `NMP`: 네트워크 맵 정보

예

```
> system generate-troubleshoot VDB NMP
starting /usr/local/sf/bin/sf_troubleshoot.pl…
Please, be patient. This may take several minutes.
The troubleshoot options codes specified are VDB,NMP.
Getting filenames from [usr/local/sf/etc/db_updates/index]
Getting filenames from [usr/local/sf/etc/db_updates/base-6.2.3]
```

```
Troubleshooting information successfully created at
/var/common/results-06-14-2018—222027.tar.gz
```

lockdown

`expert` 명령과 디바이스의 Linux 셸에 대한 액세스를 제거합니다.

⚠

주의 이 명령은 고객 지원의 핫픽스 없이는 취소할 수 없습니다. 주의해서 사용해야 합니다.

Syntax

```
system lockdown
```

예

```
> system lockdown
```

reboot

어플라이언스를 재부팅합니다.

Syntax

```
system reboot
```

예

```
> system reboot
```

restart

어플라이언스 애플리케이션을 다시 시작합니다.

Syntax

```
system restart
```

예

```
> system restart
```

shutdown

어플라이언스를 종료합니다.

Syntax

```
system shutdown
```

예

```
> system shutdown
```

Secure Firewall Management Center CLI의 기록

기능	버전	세부 사항
다음에 대한 자동 CLI 액세스 management center	6.5	SSH를 이용해 management center에 로그인하면, CLI에 자동으로 액세스하게 됩니다. 권장 사항은 아니지만, 이후 CLI `expert` 명령을 사용하면 Linux 셸에 액세스할 수 있습니다. 참고 이 기능을 이용하면 버전 6.3 기능인 management center에 대한 CLI 액세스 활성화/비활성화가 중단됩니다. 이 옵션이 중단되면 가상 management center에서는 **System(**시스템**)** > **Configuration(**구성**)** > **Console Configuration(**콘솔 구성**)** 페이지가 표시되지 않습니다. 물리적 management center에서는 계속 표시됩니다.
CLI 액세스를 활성화 및 비활성화 하는 기능 management center	6.3	신규/수정된 화면: management center 웹 인터페이스 관리자가 사용할 수 있는 새 체크박스: **Enable CLI Access(CLI** 액세스 활성화**)**(시스템 (⚙) > **Configuration(**구성**)**에 위치) > (**Console Configuration(**콘솔 구성**)**) 페이지 • 선택: SSH를 사용하여 management center에 로그인하면 CLI에 액세스할 수 있습니다. • 선택 취소: SSH를 사용하여 management center에 로그인하면 Linux 셸에 액세스할 수 있습니다. 이는 새 버전 6.3 설치 뿐만 아니라 이전 릴리스에서 버전 6.3으로 업그레이드 할 때의 기본 상태입니다. 지원되는 플랫폼: management center

기능	버전	세부 사항
management center CLI	6.3	도입된 기능. 처음에는 다음 명령을 지원합니다. • `exit` • `expert` • `?` • `show version` • `configure password` • `system generate-troubleshoot` • `system lockdown` • `system reboot` • `system restart` • `system shutdown` 지원되는 플랫폼: management center

43 장

보안, 인터넷 액세스 및 통신 포트

다음 항목에서는 시스템 보안, 인터넷 액세스 및 통신 포트에 대한 정보를 제공합니다.

보안 요건

Secure Firewall Management Center를 보호하려면 보호된 내부 네트워크에 설치해야 합니다. 필요한 서비스와 사용 가능한 포트만 사용하도록 management center를 구성한 경우에도 방화벽 외부의 공격이 방어 센터(또는 매니지드 디바이스)에 도달할 수 없는지 확인해야 합니다.

management center 및 관리되는 디바이스가 동일한 네트워크에 상주하는 경우 디바이스의 관리 인터페이스를 management center와 동일한 보호된 내부 네트워크에 연결할 수 있습니다. 이렇게 하면 management center에서 디바이스를 안전하게 제어할 수 있습니다. 또한 management center에서 다른 네트워크에 있는 디바이스의 트래픽을 관리 및 격리할 수도 있도록 복수 관리 인터페이스를 구성할 수도 있습니다.

어플라이언스를 구축하는 방식과 상관없이 어플라이언스 간 통신은 암호화됩니다. 하지만 DDoS(Distributed Denial of Service) 또는 중간자 공격(man-in-the-middle attack)등으로 어플라이언스 간 통신이 중단, 차단 또는 변조될 수 없도록 방지하는 단계를 수행해야 합니다.

Cisco Cloud

management center는 다음 기능을 위해 Cisco Cloud의 리소스와 통신합니다.

- **AMP(Advanced Malware Protection)**

  퍼블릭 클라우드는 기본적으로 구성되어 있습니다. 변경하는 방법은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *AMP* 옵션 변경을 참조하십시오.

- **URL** 필터링

자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *URL* 필터링 장을 참조하십시오.

- 통합 **Security Analytics and Logging(SaaS)**

  Cisco Secure Cloud Analytics의 원격 데이터 스토리지, 535 페이지의 내용을 참조하십시오.

- **SecureX** 및 **SecureX threat response**의 통합

  자세한 내용은 다음에서 연결된 통합 문서를 참조하십시오.

  - Cisco SecureX와의 통합, 641 페이지
  - 다음을 이용한 이벤트 분석 SecureX Threat Response, 649 페이지

- 사전 지원 기능

  자세한 내용은 Cisco 지원 진단 등록 구성을 참조하십시오.

- **Cisco Success Network**

  자세한 내용은 Cisco Success Network 등록 구성, 647 페이지 섹션을 참조해 주십시오.

- **Cisco Umbrella** 연결

  자세한 내용은 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 *DNS* 정책을 참조하십시오.

인터넷 액세스 요구 사항

기본적으로 시스템은 포트 443/tcp(HTTPS) 및 80/tcp(HTTP)에서 인터넷에 연결하도록 구성됩니다. 어플라이언스가 인터넷에 직접 액세스하지 않도록 하려면 프록시 서버를 구성할 수 있습니다. 대부분의 기능에서 사용자의 위치에 따라 시스템이 액세스하는 리소스가 결정될 수 있습니다.

대부분의 경우, 인터넷에 액세스하는 것은 management center입니다. 고가용성 쌍의 두 management center 모두 인터넷에 액세스할 수 있어야 합니다. 기능에 따라 두 피어가 모두 인터넷에 액세스하는 경우도 있고 활성 피어만 인터넷에 액세스하는 경우도 있습니다.

경우에 따라 매니지드 디바이스도 인터넷에 액세스합니다. 예를 들어 악성코드 방지 구성이 동적 분석을 사용하는 경우, 매니지드 디바이스는 파일을 직접 Secure Malware Analytics 클라우드에 전송합니다. 또는 디바이스를 외부 NTP 서버와 동기화할 수 있습니다.

또한 웹 분석 추적을 비활성화하지 않았다면 브라우저가 Google(google.com) 또는 Amplitude(amplitude.com) 웹 분석 서버에 연결하여 개인 식별이 불가능한 사용 데이터를 Cisco에 제공할 수 있습니다.

표 ***133:*** 인터넷 액세스 요구 사항

기능	이유	**Management Center** 고가용성	리소스
악성코드 대응	악성코드 클라우드 조회.	두 피어 모두 조회를 수행합니다.	적절한 Cisco Secure Endpoint 및 악성코드 분석 작업에 필요한 서버 주소를 참조하십시오.
	파일 사전 분류 및 로컬 악성코드 분석을 위한 서명 업데이트를 다운로드합니다.	활성 피어가 다운로드하고, 대기에 동기화합니다.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	동적 분석을 위해 파일을 제출합니다(매니지드 디바이스). 동적 분석 결과를 쿼리합니다(management center).	두 피어 모두 동적 분석 보고서를 쿼리합니다.	fmc.api.threatgrid.com fmc.api.threatgrid.eu
AMP for Endpoints	AMP for Endpoints가 탐지한 악성코드 이벤트를 AMP 클라우드에서 수신합니다. 시스템이 탐지한 악성코드 이벤트를 AMP for Endpoints에 표시합니다. AMP for Endpoints에서 생성된 중앙 집중식 파일 차단 및 허용 목록을 사용하여 AMP 클라우드의 속성을 재정의합니다.	두 피어 모두 이벤트를 수신합니다. 또한 두 피어 모두에서 클라우드 연결을 구성해야 합니다(구성이 동기화되지 않음).	적절한 Cisco Secure Endpoint 및 악성코드 분석 작업에 필요한 서버 주소를 참조하십시오.
보안 인텔리전스	보안 인텔리전스 피드를 다운로드합니다.	활성 피어가 다운로드하고, 대기에 동기화합니다.	intelligence.sourcefire.com

기능	이유	**Management Center** 고가용성	리소스
URL 필터링	URL 카테고리 및 평판 데이터를 다운로드합니다. 수동으로 URL 카테고리 및 평판 데이터를 쿼리(조회)합니다. 미분류 URL을 쿼리합니다.	활성 피어가 다운로드하고, 대기에 동기화합니다.	URL: • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates.ironport.com IPV4 차단: • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 차단: • 2a04: e4c7: ffff::/48 • 2a04: e4c7: fffe::/48
Cisco Smart Licensing	Cisco Smart Software Manager와 통신합니다.	활성 피어가 통신합니다.	tools.cisco.com:443 www.cisco.com
Cisco Success Network	사용 정보 및 통계를 전송합니다.	활성 피어가 통신합니다.	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
Cisco Support Diagnostics	인증된 요청을 수락하고 사용량 정보 및 통계를 전송합니다.	활성 피어가 통신합니다.	api-sse.cisco.com:8989
시스템 업데이트	Cisco에서 management center로 직접 업데이트를 다운로드합니다. • 시스템 소프트웨어 • 침입 규칙 • VDB(Vulnerability Database) • GeoDB(지리위치 데이터베이스)	활성 피어에서 침입 규칙, VDB, GeoDB를 업데이트한 다음 대기에 동기화합니다. 각 피어에서 독립적으로 시스템 소프트웨어를 업그레이드합니다.	cisco.com sourcefire.com

기능	이유	**Management Center** 고가용성	리소스
SecureX threat response 통합	해당 통합 가이드를 참조하십시오.		
시간 동기화	구축에서 시간을 동기화합니다. 프록시 서버에서는 지원되지 않습니다.	외부 NTP 서버를 사용하는 모든 어플라이언스는 인터넷에 액세스할 수 있어야 합니다.	0.sourcefire.pool.ntp.org 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 3.sourcefire.pool.ntp.org
RSS 피드	대시보드에 Cisco Threat Research 블로그를 표시합니다.	RSS 피드를 표시하는 모든 어플라이언스는 인터넷에 액세스할 수 있어야 합니다.	blog.talosintelligence.com
Whois	외부 호스트의 whois 정보 요청 프록시 서버에서는 지원되지 않습니다.	whois 정보를 요청하는 어플라이언스는 인터넷에 액세스할 수 있어야 합니다.	whois 클라이언트는 쿼리할 적절한 서버를 추측하려 시도합니다. 추측할 수 없는 경우, 다음을 사용합니다. • NIC 핸들: whois.networksolutions.com • IPv4 주소 및 네트워크 이름: whois.arin.net

통신 포트 요구 사항

management center는 포트 8305/tcp의 양방향 SSL 암호화 통신 채널을 사용하여 매니지드 디바이스와 통신합니다. 이 포트는 기본 통신을 위해 반드시 열려 있어야 합니다.

다른 포트는 특정 기능에 필요한 외부 리소스에 대한 액세스뿐만 아니라 보안 관리도 허용합니다. 일반적으로 기능과 관련된 포트는 관련 기능을 활성화 또는 구성할 때까지 닫은 상태를 유지해야 합니다. 개방된 포트를 닫음으로써 구축에 어떤 영향을 미칠지 이해하기 전까지 개방된 포트를 변경하거나 닫지 마십시오.

표 ***134:*** 통신 포트 요구 사항

포트	프로토콜/기능	플랫폼	방향	세부 사항
22/tcp	SSH	Management Center Threat Defense	인바운드	어플라이언스에 대한 보안 원격 연결
53/tcp 53/udp	DNS		아웃바운드	DNS

포트	프로토콜/기능	플랫폼	방향	세부 사항
67/udp 68/udp	DHCP		아웃바운드	DHCP
123/udp	NTP		아웃바운드	시간 동기화
161/udp	SNMP	Management Center Threat Defense	인바운드	SNMP 폴링을 통해 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 감지된 LDAP 사용자의 메타데이터 가져오기(Management Center 전용) 구성 가능합니다.
443/tcp	HTTPS	Management Center	인바운드	웹 인터페이스 액세스
443/tcp	Remote Access VPN(SSL/IPSec)	Threat Defense	인바운드	원격 사용자로부터 네트워크에 보안 VPN 연결 허용
500/udp 4500/udp	Remote Access VPN(IKEv2)	Threat Defense	인바운드	원격 사용자로부터 네트워크에 보안 VPN 연결 허용
443/tcp	HTTPS	Management Center Threat Defense	인바운드	Cisco Terminal Services(TS) Agent를 포함하여 Firepower REST API를 사용하는 통합 및 타사 제품과 통신
443/tcp	HTTPS		아웃바운드	인터넷에서 데이터 송수신 자세한 내용은 인터넷 액세스 요구 사항, 1096 페이지 항목을 참조하십시오.
443	HTTPS	Management Center	both	AMP for Networks와의 통합
514/udp	시스템 로그(알림)		아웃바운드	원격 syslog 서버에 대한 경고 전송
623/udp	SOL/LOM	Management Center	인바운드	SOL(Serial Over LAN) 연결을 사용하여 Lights-Out Management(LOM) 수행
885/tcp	캡티브 포털	Threat Defense	인바운드	캡티브 포털 ID 소스와 통신
1500/tcp 2000/tcp	데이터베이스 액세스	Management Center	인바운드	서드파티 클라이언트의 이벤트 데이터베이스에 대한 읽기 전용 액세스 허용
1812/udp 1813/udp	RADIUS		아웃바운드	외부 인증 및 어카운트 관리를 위해 RADIUS 서버와 통신 구성 가능합니다.

포트	프로토콜/기능	플랫폼	방향	세부 사항
8302/tcp	eStreamer	Management Center	인바운드	eStreamer 클라이언트와 통신
8305/tcp	어플라이언스 통신		Both(모두)	구축 어플라이언스 간 보안 통신. 구성 가능합니다. 이 포트를 변경하는 경우 구축의 모든 어플라이언스에 대해 이 포트를 변경해야 합니다. 기본값을 유지하는 것이 좋습니다.
8307/tcp	호스트 입력 클라이언트	Management Center	인바운드	호스트 입력 클라이언트와 통신
8989/tcp	Cisco Support Diagnostics		Both(모두)	인증된 요청을 수락하고 사용량 정보 및 통계를 전송합니다.

관련 항목

Management Center에 대한 LDAP 외부 인증 개체 추가, 127 페이지
Management Center에 대한 RADIUS 외부 인증 개체 추가, 136 페이지