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 Secure Firewall 4200 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 사항에서 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 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 및 시간 동기화의 내용을 참조하십시오.
- 시스템은 초기 구성의 일부로 매주 GeoDB 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 GeoDB 업데이트 예약.
- 시스템은 초기 구성의 일부로 매주 GeoDB 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 소프트웨어 다운로드 자동화.

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.
- 시스템은 초기 구성의 일부로 최신 VDB를 다운로드하고 설치합니다. 시스템을 최신 상태로 유지하려면 취약성 데이터베이스 업데이트 자동화.
- 시스템은 초기 구성의 일부로 매일 침입 규칙 업데이트를 예약합니다. 이 작업을 검토하고 필요한 경우 침입 규칙 업데이트 예약.

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 지정에서 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 설정에 설명된 대로 이 어카운트의 시간대를 설정합니다.

단계 **2** 필요하다면 라이선스의 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 정보를 참고하십시오.

단계 **6** 상태 정책 적용에 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 구성에 설명된 대로 액세스 목록에서 포트를 수정합니다.
- 데이터베이스 이벤트 제한 구성에 설명된 대로 데이터베이스 이벤트 제한에 대해 알아보고 편집하는 것이 좋습니다.
- 디스플레이 언어를 변경하려는 경우, 웹 인터페이스의 언어 설정에 설명된 대로 언어 설정을 편집합니다.
- 조직에서 프록시 서버를 사용하는 네트워크 액세스를 제한하는 경우 Management Center 관리 인터페이스 수정의 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 추가의 내용을 참조하십시오.
- LDAP 또는 RADIUS 외부 인증을 사용하여 management center에 대한 액세스를 허용하려는 경우, Management Center에 대한 외부 인증 구성의 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 및 Cisco Secure Firewall Management Center 디바이스 구성 가이드의 디바이스 사용자
시스템 하드웨어 및 소프트웨어의 상태 모니터링	상태 모니터링 정책	상태 모니터링 정보
어플라이언스 데이터 백업	백업 및 복구	백업/복구
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
라이선스 제어 기능을 활용하기 위해 라이선스를 적용합니다.	스마트 라이선싱	라이선스 정보

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
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
REST API 클라이언트를 사용하여 어플라이언스 구성 보기 및 관리	REST API 및 REST API Explorer	REST API 환경 설정 *Firepower REST API* 빠른 시작 가이드
문제 해결	해당 없음	문제 해결

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* 위협 정보 디렉터 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
애플리케이션 탐지 및 제어 수행	애플리케이션 탐지기	Cisco Secure Firewall Management Center 디바이스 구성 가이드의 애플리케이션 탐지
문제 해결	해당 없음	문제 해결

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 *Firepower System Remediation API* 설명서
맞춤 개발 된 클라이언트 애플리케이션으로 Firepower Management Center 스트림 이벤트 데이터	eStreamer 통합	eStreamer 서버 스트리밍 *Firepower System eStreamer* 통합 가이드
서드파티 클라이언트를 사용하여 Firepower Management Center에서 데이터베이스 테이블 쿼리	외부 데이터베이스 액세스	외부 데이터베이스 액세스 *Firepower System* 데이터베이스 액세스 설명서

기능	구성...	설명...
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
문제 해결	해당 없음	문제 해결

Management Center 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 변경의 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

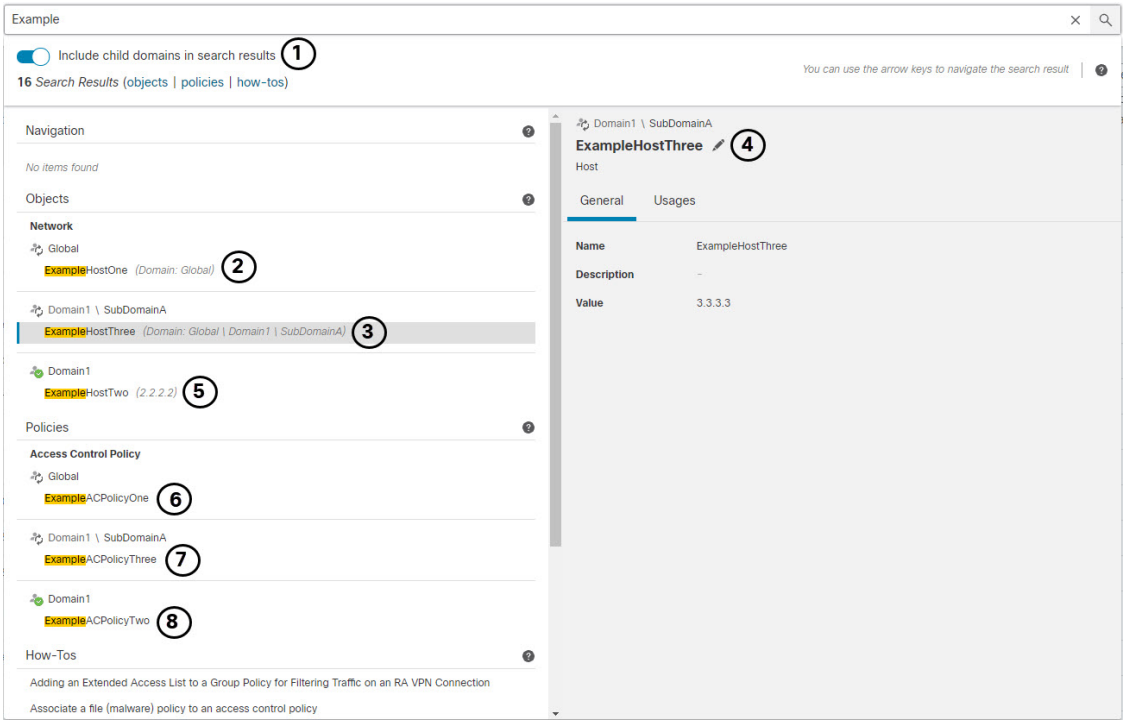
다중 도메인 구축의 전역 검색:

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 변경의 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 Management Center 검색을 참조하십시오.

시작하기 전에

이 기능은 클래식 테마에서 사용할 수 없습니다. 테마를 변경하려면 웹 인터페이스 모양 변경의 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 Management Center 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 변경의 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 변경의 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 온라인 도움말, How To, 설명서, 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 조사를 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 구성의 내용을 참조하십시오.

- 웹 분석

  웹 분석의 내용을 참조하십시오.

온라인 도움말, How To, 설명서

웹 인터페이스 온라인 도움말 연결 방법:

- 각 페이지에서 상황별 도움말 링크 클릭
- **Help(**도움말**)** > **Page-level Help(**페이지 수준 도움말**)** 선택

How To는 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. How To 위젯을 열려면 **Help(**도움말**)** > **How-Tos**를 선택합니다.

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

다음 워크스루는 management center에서 사용할 수 있습니다.

management center에서 지원되는 기능 워크스루 목록은 Secure Firewall Management Center에서 지원되는 기능 워크스루를 참조하십시오.

설명서 로드맵을 사용하여 추가 설명서를 찾아볼 수 있습니다.

Cisco Secure Firewall Threat Defense 문서로 이동.

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

- Secure Firewall 4200:

  https://www.cisco.com/c/en/us/support/security/secure-firewall-4200-series/series.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 정보를 참조하십시오.

관련 항목

라이선스 정보

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.