Firepower 시작하기

Cisco Firepower는 네트워크 보안 및 트래픽 관리 제품들로 구성된 통합 제품군으로, 특별히 구축된 플랫폼에 또는 소프트웨어 솔루션으로서 구축됩니다. 이 시스템에서는 조직의 보안 정책(네트워크 보호 지침)을 준수하는 방식으로 네트워크 트래픽을 처리할 수 있습니다.

일반적인 구축에서는 네트워크 세그먼트에 설치된 여러 트래픽 센싱 매니지드 디바이스가 분석을 위해 트래픽을 모니터링하고 관리자에게 보고합니다.

- Firepower Management Center
- Firepower Device Manager
- ASDM(Adaptive Security Device Manager)

관리자는 관리, 분석 및 보고 작업을 수행하는 데 사용할 수 있는 그래픽 유저 인터페이스가 포함된 중앙 집중식 관리 콘솔을 제공합니다.

이 가이드는 *Firepower Management Center* 관리 어플라이언스를 중점적으로 다룹니다. Firepower Device Manager 또는 ASDM을 통해 관리되는 ASA with FirePOWER Services에 관한 내용은 이러한 관리방법에 대한 가이드를 참조하십시오.

- *Firepower Device Manager*용 *Cisco Firepower Threat Defense* 구성 가이드
- *ASA with FirePOWER Services* 로컬 관리 구성 가이드

빠른 시작: 기본 설정

Firepower 기능 설정은 강력하고 유연하게 기본 및 고급 구성을 지원할 수 있습니다. 다음 섹션을 사용하여 신속하게 Firepower 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.

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

    http://www.cisco.com/go/firepower-mc-install

- **Firepower Threat Defense** 매니지드 디바이스

  중요 이 페이지에서 Firepower Device Manager 문서를 무시합니다.

  - Cisco Firepower 1010 시작 가이드
  - Cisco Firepower 1100 Series 시작 가이드
  - Cisco Firepower 2100 Series 시작 가이드
  - Cisco Firepower 4100 시작 가이드
  - Cisco Firepower 9300 시작 가이드
  - Firepower Management Center를 사용하는 ASA 5508-X 및 ASA 5516-X용 Cisco Firepower Threat Defense 빠른 시작 가이드
- 클래식 매니지드 디바이스
  - Cisco ASA FirePOWER 모듈 빠른 시작 가이드
  - Cisco Firepower 8000 Series 시작 가이드
  - Cisco Firepower 7000 Series 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 NGIPSv : *VMware*용 *Cisco Firepower NGIPSv* 빠른 시작 가이드
- VMware에서 실행되는 Firepower Threat Defense Virtual: *Firepower Management Center* 빠른 시작 가이드를 사용하는 *Firepower ASA 5508-X* 및 *ASA 5516-X*용 *Cisco Firepower Threat Defense*
- 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 FMC에 처음 로그인하기 전에, 물리적 어플라이언스에서 초기 설정 설치 및 수행, 2 페이지 또는 가상 어플라이언스 구축, 3 페이지의 설명에 따라 어플라이언스를 준비합니다.

새 FMC(또는 출고 시 설정으로 새로 복원된 FMC)에 처음 로그인할 때는, CLI 또는 웹 인터페이스용 관리자 계정을 사용하고 사용자의 FMC 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 사용자 어카운트 가이드라인 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. (웹 인터페이스에서 내부 사용자 추가 참조)
- FMC이(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 FMC 웹 인터페이스에서 확인하고 변경할 수 있습니다. 자세한 내용은 FMC 관리 인터페이스 수정 및 시간 및 시간 동기화의 내용을 참조하십시오.
- 초기 구성 중에 FMC는 주 단위로 자동 GeoDB 업데이트를 구성합니다. 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 업데이트 구성에 실패하고 FMC이 인터넷에 액세스할 수 있는 경우, GeoDB 업데이트 예약.
- 초기 구성 중 FMC는 주간 작업을 예약하여 FMC 및 매지니드 디바이스의 최신 소프트웨어를 다운로드합니다. 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 작업 예약이 실패하고 FMC가 인터넷에 액세스할 수 있다면 소프트웨어 다운로드 자동화.

  

  중요 이 작업은 FMC에 소프트웨어 업데이트만 다운로드합니다. 이 작업으로 다운로드하는 업데이트의 설치는 사용자의 책임입니다. 자세한 내용은 *Cisco Firepower Management Center* 업그레이드 설명서를 참조하십시오.
- 초기 구성 중에 FMC는 주간 작업을 예약하여 로컬에 저장된 구성 전용 백업을 수행합니다. 웹 인터페이스 메시지 센터를 사용하면 이 작업의 상태를 확인할 수 있습니다. 작업 예약에 실패하면 설명에 따라 백업을 수행하는 반복 작업을 예약하는 것이 좋습니다. FMC 백업 예약.
- 초기 구성 중 FMC는 Cisco 지원 사이트에서 최신 취약점 데이터베이스(VDB)를 다운로드하고 설치합니다. 이 작업은 한 번만 수행하면 됩니다. 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 시스템을 최신 상태로 유지하고자 하고 FMC가 인터넷에 액세스할 수 있다면 취약성 데이터베이스 업데이트 자동화.

- 초기 구성 중에 버전 FMC는 Cisco 지원 사이트에서 매일 자동 침입 규칙 업데이트를 구성합니다. (FMC는 다음에 영향을 받는 정책을 구축하는 경우 영향을 받는 관리되는 디바이스에 자동으로 침입 규칙 업데이트를 구축합니다.) 웹 인터페이스 메시지 센터를 사용하면 이 업데이트의 상태를 확인할 수 있습니다. 업데이트 구성에 실패하고 FMC이 인터넷에 액세스할 수 있는 경우, 반복 되는 침입 규칙 업데이트 구성.

FMC 초기 구성이 완료되면, 디바이스 관리 기본 사항에서 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 Firepower System 라이선싱의 설명에 따라 라이선스를 추가합니다.

단계 **3** FMC에 디바이스 추가의 설명에 따라 매니지드 디바이스를 구축에 추가합니다.

단계 **4** 다음에 설명된 대로 매니지드 디바이스를 구성합니다.

- IPS 디바이스 구축 및 구성 소개기본 디바이스에서 수동 또는 인라인 인터페이스 구성
- Firepower Threat Defense 인터페이스 개요Firepower Threat Defense 디바이스에 투명 또는 라우팅 모드 구성
- Firepower Threat Defense 인터페이스 개요Firepower Threat Defense 디바이스에 인터페이스 구성

단계 **5** 기본 액세스 제어 정책 만들기에 설명된 대로 액세스 제어 정책을 구성합니다.

- 대부분의 경우 Cisco는 Balanced Security and Connectivity(보안과 연결의 균형 유지) 침입 정책을 기본 작업으로 설정할 것을 제안합니다. 자세한 내용은 Access Control Policy Default Action(액세스 제어 정책 기본 작업) 및 시스템 제공 네트워크 분석 및 침입 정책를 참조하십시오.
- 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.
- 해당 조직에서 프록시 서버를 사용하여 네트워크 액세스를 제한하고, FMC 관리 인터페이스 수정에 설명된 대로 프록시 설정을 편집합니다.

단계 **8** 네트워크 검색 정책 설정에 설명된 대로 네트워크 검색 정책을 맞춤화합니다. 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.

- 메시지 센터 팝업 표시를 원하지 않는 경우, 알림 동작 설정에 설명된 대로 알림을 비활성화합니다.
- 시스템 변수에 대한 기본값을 맞춤화하려는 경우, 변수 집합에 설명된 대로 변수 사용에 대해 알아봅니다.
- 추가 로컬 인증 사용자 계정를 생성하고 FMC에 액세스하려는 경우, 사용자 어카운트 만들기내부 사용자 추가의 내용을 참조하십시오.
- LDAP 또는 RADIUS 외부 인증을 사용하여 FMC에 대한 액세스를 허용하려는 경우, 외부 인증외부 인증 구성의 내용을 참조하십시오.

단계 **10** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

다음에 수행할 작업

- Firepower 기능, 8 페이지 및 이 가이드의 나머지 부분에 설명된 다른 기능을 검토하고 구성하는 것이 좋습니다.

Firepower 디바이스

일반적인 구축에서는 여러 트래픽 처리 디바이스가 같은 Firepower Management Center에 보고하는데, 이곳에서는 운영, 관리, 분석, 보고 작업을 수행할 수 있습니다.

클래식 디바이스

클래식 디바이스는 차세대 IPS (NGIPS) 소프트웨어를 실행 합니다. 그 기능은 다음과 같습니다.

- Firepower 7000 시리즈와 Firepower 8000 시리즈는 물리적 디바이스입니다.
- VMware에서 호스팅되는 NGIPSv입니다.
- FirePOWER 서비스를 이용하는 ASA로, 일부 ASA 5500-X 시리즈 디바이스에서 사용할 수 있습니다(ISA 3000 포함). ASA는 우선 시스템 정책을 제공하고, 그런 다음 검색 및 액세스 제어를 위해 트래픽을 ASA FirePOWER 모듈로 전달합니다.

  ASA CLI나 ASDM을 사용하여 ASA FirePOWER 디바이스에서 ASA 기반 기능을 구성해야 합니다. 디바이스 고가용성, 스위칭, 라우팅, VPN, NAT 등이 이러한 기능에 속합니다. FMC를 사용하여 ASA FirePOWER 인터페이스를 구성할 수는 없으며, ASA FirePOWER를 SPAN 포트 모드로 구축한다면 FMC GUI에 ASA 인터페이스가 표시되지 않습니다. 또한 FMC를 사용하여 ASA FirePOWER 프로세스를 종료하거나, 다시 시작하거나, 관리할 수도 없습니다.

Firepower Threat Defense 디바이스

FTD(Firepower 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.

FTD는 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 Firepower 릴리스 노트 및 Cisco FirePOWER 호환성 가이드를 참조하십시오.

Firepower 7000/8000 시리즈 디바이스 판매 종료

7000/8000 시리즈 디바이스에서는 Firepower 버전 6.5 이상으로 업그레이드하거나 버전 6.5 이상을 새로 설치할 수 없습니다. 본 가이드 및 관련 온라인 도움말은 이러한 디바이스를 구성하거나 관리하는 방법은 설명하지 않습니다.

지원되는 이전 Firepower 버전을 실행하는 7000/8000 시리즈 디바이스를 관리한다면, 다음 리소스를 사용하십시오.

- FMC-디바이스 호환성에 관한 자세한 내용은 Cisco Firepower 호환성 가이드의 *Firepower Management Centers* 관련 정보 섹션을 참조하십시오.

- 디바이스 구성 및 관리에 대해서는 디바이스 버전에 맞는 Firepower Management Center 구성 가이드를 참조하십시오.

Firepower 기능

이러한 테이블에는 몇 가지 흔히 사용되는 Firepower 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.html의 내용을 참조하십시오.

기능	구성...	설명...
Firepower 어플라이언스 로그인 사용자 어카운트 관리	Firepower 인증	Firepower System 사용자 인증 FMC의 사용자 계정 및 디바이스 사용자 계정
시스템 하드웨어 및 소프트웨어의 상태 모니터링	상태 모니터링 정책	상태 모니터링 정보
어플라이언스 데이터 백업	백업 및 복원	백업 및 복원
새 Firepower 버전으로 업그레이드	시스템 업데이트	Cisco Firepower Management Center 업그레이드 설명서 Firepower 릴리스 노트
물리적 어플라이언스 기준	공장 기본값으로 복원(리이미징)	Cisco Firepower Management Center 업그레이드 설명서, 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	시스템 업데이트
라이선스 제어 기능을 활용하기 위해 라이선스를 적용합니다.	기본 또는 스마트 라이선싱	Firepower 라이선스 정보

기능	구성...	설명...
어플라이언스 운영의 연속성을 보장	매니지드 디바이스 고가용성 및/또는 Firepower Management Center 고가용성	7000 및 8000 Series 디바이스 고가용성 정보 Firepower Threat Defense 고가용성 정보 Firepower Management Center 고가용성 정보
여러 8000 Series디바이스의 처리 리소스를 결합	디바이스 스태킹	디바이스 스택 관련 정보
디바이스를 구성하고 두 개 이상의 인터페이스 사이에 트래픽을 라우팅합니다.	라우팅	가상 라우터 Firepower Threat Defense 라우팅 개요
두 개 이상의 네트워크 사이에 패킷 스위칭을 구성합니다.	디바이스 전환	가상 스위치 브리지 그룹 인터페이스 구성
인터넷 연결을 위해 비공개 주소를 공용 주소로 변환합니다.	NAT(네트워크 주소 변환)	NAT 정책 구성 Firepower Threat Defense용 NAT(네트워크 주소 변환)
매니지드 Firepower Threat Defense 또는 7000/8000 시리즈 디바이스 간에 보안 터널을 설정합니다.	Site-to-Site(사이트 대 사이트) 가상사설망(VPN)	Firepower Threat Defense VPN 개요
원격 사용자와 매니지드 Firepower Threat Defense 디바이스 간에 보안 터널을 설정합니다.	원격 액세스 VPN	Firepower Threat Defense 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	시스템 문제 해결

플랫폼별 고가용성 및 확장성 기능

고가용성 구성(페일오버라고도 함)은 운영 연속성을 보장합니다. 클러스터링 구성은 단일 논리 디바이스로 여러 디바이스를 함께 그룹화하여, 처리량 증가 및 이중화를 달성합니다.

플랫폼	고가용성	클러스터링
Firepower Management Center	예	—
Firepower Management Center Virtual	예(자세한 내용은 가상 플랫폼 요건을 참조하십시오.)	—
Firepower Threat Defense: • Firepower 1000 Series • Firepower 2100 Series • ASA 5500-X Series • ISA 3000	예	—
Firepower Threat Defense: • Firepower 4100/9300 섀시	예	예
Firepower Threat Defense Virtual: • VMWare • KVM	예	—
Firepower Threat Defense Virtual(퍼블릭 클라우드): • AWS • Azure	—	—
NGIPSv	—	—
ASA FirePOWER	이러한 구축에서 ASA 디바이스는 우선 시스템 정책을 제공하고 그런 다음 검색 및 액세스 제어를 위해 트래픽을 ASA FirePOWER 모듈로 전달합니다. 고가용성 및 확장성 구성에 대한 자세한 내용은 ASA 설명서를 참조하십시오.	

고가용성 구성은 운영 연속성을 보장합니다. 스태킹 구성은 단일 논리 디바이스로 여러 디바이스를 함께 그룹화하고, 처리량 증가 및 이중화를 달성합니다.

플랫폼	고가용성	스태킹
Firepower Management Center	예 MC750 제외	—
Firepower Management Center Virtual	—	—

플랫폼	고가용성	스태킹
Firepower NGIPS: • Firepower 7010, 7020, 7030, 7050 • Firepower 7110, 7115, 7120, 7125 • Firepower 8120, 8130 • AMP 7150, 8050, 8150	예	—
Firepower NGIPS: • Firepower 8140 • Firepower 8250, 8260, 8270, 8290 • Firepower 8350, 8360, 8370, 8390 • AMP 8350	예	—
Firepower NGIPS: • ASA FirePOWER • NGIPSv	—	—

관련 항목

7000 및 8000 Series 디바이스 고가용성 정보
Firepower Threat Defense 고가용성 정보
Firepower Management Center 고가용성 정보

잠재적 위협 탐지, 방지 및 처리 기능

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

기능	구성...	설명...
네트워크 트래픽 검사, 로그 및 작업 수행	일부 다른 정책보다 상위에 있는 액세스 제어 정책	액세스 제어 소개
IP 주소, URL 및/또는 도메인 이름 연결 차단 또는 모니터링	액세스 제어 정책 내 보안 인텔리전스	보안 인텔리전스 정보
네트워크의 사용자가 액세스할 수 있는 웹 사이트를 제어	정책 규칙 내 URL 필터링	URL 필터링
네트워크의 악성 트래픽 및 침입을 모니터링	침입 정책	침입 정책 기본 사항

기능	구성...	설명...
검사 없이 암호화된 트래픽 차단 암호화 또는 해독된 트래픽 검사	SSL 정책	SSL 정책 개요
캡슐화된 트래픽 심층 검사 맞춤화 및 빠른 경로 지정으로 성능 향상	사전 필터 정책	사전 필터링 정보
액세스 제어에서 허용되거나 신뢰하는 네트워크 트래픽 속도 제한	QoS(Quality of Service) 정책	QoS 정책 정보
네트워크에서 파일(악성코드 포함) 허용 또는 차단	파일/악성코드 정책	파일 정책 및 악성코드 보호
패시브 또는 액티브 사용자 인증을 구성하여 사용자 인식 및 사용자 제어 수행	사용자 인식, 사용자 ID, ID 정책	영역 및 ID 정책 정보 ID 정책 정보
네트워크의 트래픽에서 호스트, 애플리케이션 및 사용자 데이터를 수집하고 사용자 제어 수행	네트워크 검색 정책	개요: 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	개요: 애플리케이션 탐지
문제 해결	해당 없음	시스템 문제 해결

외부 툴과 통합

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

기능	구성...	설명...
네트워크의 조건이 관련 정책을 위반할 때 자동으로 치료를 시작	치료	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

기능	구성...	설명...
서드파티 클라이언트를 사용하여 Firepower Management Center에서 데이터베이스 테이블 쿼리	외부 데이터베이스 액세스	외부 데이터베이스 액세스 설정 *Firepower System* 데이터베이스 액세스 설명서
서드파티 소스에서 데이터를 가져오는 방법으로 검색 데이터를 보완	호스트 입력	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	시스템 문제 해결

FMC 검색

웹 인터페이스 메뉴 옵션 검색

웹 인터페이스의 최상위 메뉴에서 페이지의 위치를 찾으려면 검색합니다. 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** Firepower Management Center 웹 인터페이스 상단의 메뉴 모음에서 검색( )을 클릭합니다.

단계 **2** 원하는 메뉴 옵션 이름의 문자를 하나 이상 입력합니다.

단계 **3** 페이지로 이동하려면 제안 목록에서 항목을 클릭합니다.

도메인 전환 Firepower 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 도메인

에서 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 콘

텍스트 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

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.

관련 항목

보안 인텔리전스 목록 및 피드

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.

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

FMC 구축에 대한 최상위 문서 목록 페이지

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

참고 일부 연결된 문서는 Firepower Management Center 구축에 적용할 수 없습니다. 예를 들어, 일부 링크는 Firepower와 무관합니다. 혼동을 피하기 위해 문서 제목에 주의하십시오. 또한 일부 문서는 여러 제품을 다루며 여러 제품 페이지에 표시될 수 있습니다.

Firepower Management Center

- Firepower Management Center 하드웨어 어플라이언스:

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

- Firepower 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

NGIPS(Next Generation Intrusion Prevention System) 디바이스라고도 함.

- ASA with FirePOWER Services:
  - ASA 5500-X with FirePOWER Services:
    - https://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html
    - https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html
  - ISA 3000 with FirePOWER Services:

    https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html
- Firepower 8000 시리즈:

  https://www.cisco.com/c/en/us/support/security/firepower-8000-series-appliances/tsd-products-support-series-home.html
- Firepower 7000 시리즈:

  https://www.cisco.com/c/en/us/support/security/firepower-7000-series-appliances/tsd-products-support-series-home.html
- AMP for Networks:

  https://www.cisco.com/c/en/us/support/security/amp-appliances/tsd-products-support-series-home.html
- NGIPSv(가상 디바이스):

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

문서 내 라이선스 설명

섹션 앞부분에 있는 License(라이선스) 설명문에는 섹션에 설명된 기능을 활성화하기 위해 Firepower System에서 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 Malware(악성코드) 라이선스가 필요합니다.

라이선스에 대한 자세한 내용은 Firepower 라이선스 정보를 참조하십시오.

관련 항목

Firepower 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 Firepower 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.

사용자 역할에 대한 자세한 내용은 사전 정의된 사용자 역할사용자 역할과 맞춤형 사용자 역할웹 인터페이스의 사용자 역할 맞춤화를 참조하십시오.

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 Firepower Management Center의 이전 버전을 가리킵니다. 동영상이나 기술 노트에 참조된 Firepower Management Center 버전이 유저 인터페이스에서와 차이가 있어 절차가 동일하지 않을 수 있습니다.

Firepower 시작 기록

기능	버전	세부 사항
웹 인터페이스 페이지 검색	6.7	보거나 변경할 페이지를 검색할 수 있습니다. 예를 들어 **QoS**를 검색하여 QoS(Quality of Service) 설정을 구성할 페이지를 찾을 수 있습니다. 신규/수정된 화면: FMC 웹 인터페이스 창 상단에 새 돋보기 버튼이 있습니다. 플랫폼: FMC(클래식 테마를 사용할 때는 사용할 수 없음)
초기 구성 마법사	6.5	신규 또는 출고 시 설정으로 복원된 FMC에 처음으로 로그인하면, 이제 버전 6.5를 지원하는 FMC 모델에 대한 *Cisco Firepower Management Center* 시작 가이드에 문서화된 초기 구성 마법사가 관리자 사용자에게 표시됩니다. 마법사는 다음 항목을 구성합니다. • 두 관리자 계정(웹 인터페이스 액세스용 하나와 CLI 액세스용 하나)의 비밀번호는 강력한 비밀번호 요구 사항을 준수하는 같은 값으로 설정됩니다. • FMC이(가) 자체 관리 인터페이스(eth0)를 통한 네트워크 통신에 사용하는 네트워크 설정을 구성합니다. • GeoDB와 FMC 및 관련 매지니드 디바이스용 시스템 소프트웨어 주간 자동 업데이트를 예약합니다. • FMC에 대한 주간 로컬 저장 구성 전용 자동 백업을 예약합니다. 신규/수정된 화면: 관리자 사용자의 최초 로그인 지원되는 플랫폼: FMC