

Cisco FirePOWER Threat Defense for ISR

- Q.** Cisco FirePOWER™ Threat Defense for ISR 은 무엇입니까?
- A.** Cisco FirePOWER Threat Defense for ISR 은 업계 최고 Cisco® 위협 차단 기능의 적용 범위를 네트워크 에지와 데이터 센터에서 지사의 추가 플랫폼인 Cisco ISR(Integrated Services Router)까지 확장합니다.
- Q.** 왜 이 기능이 필요합니까?
- A.** 이제 지사에서 DIA(Direct Internet Access)의 비용 절감 및 향상된 사용자 환경을 활용하는 동시에, 상주하는 위치와 관계없이 디바이스와 호스트를 지능형 위협으로부터 보호할 수 있습니다.
- Q.** Cisco FirePOWER Threat Defense for ISR 의 요소는 무엇입니까?
- A.** 다음과 같이 다섯 가지의 구성 요소가 있습니다.
- **FirePOWER NGIPS(Next-Generation Intrusion Prevention System)**는 실시간 상황 인식 기능, 지능형 보안 자동화 기능 및 업계 최고의 위협 차단 효율성을 통합하여 지능형 위협 차단의 표준을 정립합니다.
 - **애플리케이션 가시성 및 제어(AVC)**는 수천 개의 애플리케이션에 대한 정밀한 제어를 사용하고 모바일 앱 정책, 소셜 미디어 앱 정책 및 제한적인 사용 정책을 적용하여 잠재적인 공격 표면을 줄입니다.
 - **AMP(Advanced Malware Protection) for Networks** 는 고도로 지능화되고 특정 표적을 노리는 제로 데이 공격과 지속적인 지능형 악성코드 위협을 차단합니다. 1 차 방어선을 우회하는 위협에 대해 파일 및 네트워크 트래픽을 지속적으로 분석하고, 위협의 활동과 행동을 세밀하게 가시화하여, 단 몇 번의 클릭만으로도 진행 중인 공격의 영향을 신속하게 관찰하고 억제합니다.
 - **평판 기반 URL 필터링**은 80 개 이상의 카테고리에서 2 억 8 천만 개가 넘는 URL 에 대한 액세스 제어를 통해 의심스럽고 허용되지 않는 도메인과 관련된 위험을 감소시켜 정교한 클라이언트 쪽 공격을 완화하고 직원의 생산성을 향상합니다.
 - **Cisco FireSIGHT® Management Center** 는 모든 FirePOWER Threat Defense for ISR 구성 요소의 이벤트와 정책 관리를 수행하는 중앙 지점입니다. 물리적 호스트와 가상 호스트, 운영 체제, 애플리케이션, 서비스, 프로토콜, 사용자, 지리적 위치 정보, 콘텐츠, 네트워크 행동, 네트워크 공격 및 악성코드 등 고객 네트워크 전체에 대한 가시성을 제공합니다. 또한, 운영을 효율화하고 반복되는 여러 보안 분석 및 관리 작업을 자동화하여 고객의 비용을 절감합니다.
- Q.** 어떤 ISR 모델에서 FirePOWER Threat Defense 를 실행할 수 있습니까?
- A.** 이 기능은 ISR G2 및 ISR 4000 Series 플랫폼 모두에서 사용할 수 있습니다. 구체적으로 말씀드리면,
- Cisco ISR G2 Series
 - 2911 ISR
 - 2921 ISR
 - 2951 ISR
 - 3925 ISR
 - 3945 ISR

- 3925E ISR
- 3945E ISR
- Cisco ISR 4000 Series
 - 4331 ISR
 - 4351 ISR
 - 4451 ISR
 - 4321 및 4431 ISR(2015 년에 릴리스 예정)

Q. Cisco FirePOWER Threat Defense for ISR 은 어떻게 관리합니까?

A. FireSIGHT Management Center 를 통해 중앙 집중식으로 관리합니다. 관리 센터는 어플라이언스와 가상 폼 팩터 모두에서 사용할 수 있습니다.

Q. 관리 센터에서 FirePOWER NGIPS 어플라이언스, Cisco ASA with FirePOWER Services(Cisco 의 차세대 방화벽)의 위협 방어 기능 및 Cisco FirePOWER Threat Defense for ISR 을 동시에 관리할 수 있습니까?

A. 예. 단일 관리 센터 인스턴스를 통해 최대 300 개의 FirePOWER 센서(가상 및 물리적)를 관리할 수 있습니다.

Q. FireSIGHT Management Center 에 인터넷 액세스가 없으면 플래시 드라이브와 CD-ROM 등의 리무버블 미디어로 서명 업데이트를 오프라인으로 업로드할 수 있습니까?

A. 예. 제품 업데이트는 Cisco 의 [소프트웨어 다운로드](#) 페이지에서 사용할 수 있습니다.

Q. Cisco FirePOWER Threat Defense for ISR 이 적합한 상황은 무엇입니까?

A. 여러 지역에 분포해 있는 지사나 소매 상점의 클라우드 애플리케이션, 비디오 및 BYOD(bring-your-own-device) 정책으로 인해 대역폭 요건과 비용이 점점 증가하고 있는 조직에게 특히 유용합니다. 이러한 증가로 인해, 여러 지역에 분포되어 있는 엔터프라이즈에서는 DIA(Direct Internet Access), 즉 데이터 센터를 통한 백홀링 트래픽을 요청하는 지사의 엄청난 요구를 처리해야 합니다. DIA 를 사용하면 비용은 절감할 수 있지만, 데이터 센터에서 제공하는 고유의 엔터프라이즈급 위협 차단은 상실할 수 있습니다. Cisco FirePOWER Threat Defense for ISR 을 사용하면 이 문제가 해결됩니다.

Q. 방화벽과 대조적으로 라우터에서 통합 위협 방어 기능을 구축해야 하는 경우는 언제입니까? 둘 다에서 해당 기능을 구축해야 하는 경우는 언제입니까?

A. 검사 및 콘텐츠 필터링을 위해 보안 터널을 사용하여 지사에서 들어오는 모든 트래픽을 데이터 센터에 백홀링하는 경우, 상태 보존 방화벽이 보안 요건을 만족합니다. 지사의 트래픽이 인터넷으로 직접 이동하면 상태 보존 방화벽과 FirePOWER Threat Defense for ISR 기능이 모두 필요합니다.

Q. 무선 디바이스에서 수신되는 트래픽을 검사하기 위해 FirePOWER Threat Defense for ISR 을 구축하는 방법은 무엇입니까?

A. FirePOWER Threat Defense for ISR 은 무선 네트워크 종단점 바로 다음에 구축해야 합니다. 강화된 위협 차단을 제공하는 모바일 디바이스용 Cisco AMP for Endpoints 버전이 있습니다. AMP for Endpoints 의 경고는 FireSIGHT Management Center 에도 전송됩니다.

Q. Cisco FirePOWER Threat Defense for ISR 에 대한 기술 구성 정보는 어디에 있습니까?

A. 다음 링크에는 아직 “Cisco FirePOWER Threat Defense for ISR” 브랜드가 없으며, 추가 기술 정보는 [여기](#)에 있습니다.

-
- Q.** Cisco FirePOWER Threat Defense for ISR 은 어떻게 주문합니까?
- A.** 도움이 필요하면 Cisco 어카운트 담당자 또는 Cisco 파트너 담당자에게 문의해 주십시오.
- Q.** FirePOWER Threat Defense for ISR 에 대한 자세한 정보는 어디에 있습니까?
- A.** 이 특정 제품에 대한 자세한 정보는 [여기](#)에 있으며, FirePOWER Threat Defense 솔루션에 대한 자세한 정보는 [여기](#)에 있습니다.



미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 www.cisco.com/go/offices에서 확인하십시오.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 언급된 타사 상표는 해당 소유주의 재산입니다. "파트너"라는 용어는 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)
Printed in USA

C67-734837-00 06/16