



귀하에게 적합한 애플리케이션 및 관리자는 무엇입니까?

하드웨어 플랫폼은 두 애플리케이션 Secure Firewall Threat Defense 또는 ASA 중 하나를 실행할 수 있습니다. 각 애플리케이션에 대해 관리자를 선택할 수 있습니다. 이 장에서는 애플리케이션 및 관리자 선택 사항에 대해 설명합니다.

- [애플리케이션, 1 페이지](#)
- [매니저, 1 페이지](#)

애플리케이션

하드웨어 플랫폼에서 다음 애플리케이션 중 하나를 사용할 수 있습니다.

- Threat Defense— threat defense (이전 명칭 Firepower Threat Defense)는 고급 스테이트풀 방화벽, VPN 집선 장치 및 차세대 IPS를 결합한 차세대 방화벽입니다.
- ASA — ASA는 기존의 고급 스테이트풀 방화벽 및 VPN 집선 장치입니다.

Cisco는 ASA로 시작한 다음 나중에 threat defense 이미지로 다시 설치하는 경우 ASA를 threat defense 로 변환하는 데 도움이 되는 ASA-threat defense 마이그레이션 툴을 제공합니다.

ASA와 threat defense간에 이미지를 재설치하려면 [Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드](#)를 참조하십시오.

매니저

threat defense 및 ASA는 여러 관리자를 지원합니다.

Threat Defense 관리자



참고 Secure Firewall Device Manager (이전 Firepower Device Manager)는 Secure Firewall 4200에서 지원되지 않습니다.

표 1: Threat Defense 관리자

매니저	설명
Secure Firewall Management Center (구 Firepower Management Center)	<p>management center는 자체 서버 하드웨어에서 실행되거나 하이퍼바이저에서 가상 디바이스로 실행되는 다중 디바이스 관리자입니다.</p> <p>로컬 management center의 경우, Management Center로 Threat Defense 구축의 내용을 참조하십시오.</p> <p>원격 management center의 경우 Threat Defense 원격으로 구축 Management Center의 내용을 참조하십시오.</p>
Cisco Defense Orchestrator(CDO) 클라우드 제공 Firewall Management Center	<p>CDO의 클라우드 제공 Firewall Management Center에는 온프레미스 Management Center의 모든 구성 기능이 있습니다. 분석 기능을 위해 클라우드 솔루션 또는 온프레미스 Management Center를 사용할 수 있습니다. CDO은(는) ASA와 같은 다른 보안 디바이스도 관리합니다.</p> <p>Threat Defense CDO을(를) 사용한 구축의 내용을 참조하십시오.</p>
Secure Firewall Threat Defense REST API	<p>Threat Defense REST API를 사용하면 threat defense의 직접 구성을 자동화할 수 있습니다. management center 또는 CDO를 사용하여 threat defense을 관리하는 경우에는 이 API를 사용할 수 없습니다.</p> <p>Threat Defense REST 는 이 가이드에서 다루지 않습니다. 자세한 내용은 Cisco Secure Firewall Threat Defense REST API 가이드를 참조하십시오.</p>
Secure Firewall Management Center REST API	<p>Management Center REST API를 사용하면 관리되는 threat defense에 적용할 수 있는 management center 정책 구성을 자동화할 수 있습니다. 이 API는 threat defense를 직접 관리하지 않습니다.</p> <p>Management Center REST API는 이 가이드에서 다루지 않습니다. 자세한 내용은 Secure Firewall Management Center REST API 빠른 시작 가이드를 참조하십시오.</p>

ASA 관리자

표 2: ASA 관리자

매니저	설명
CLI	<p>CLI를 사용하여 모든 ASA 기능을 구성할 수 있습니다.</p> <p>CLI는 이 가이드에서 다루지 않습니다. 자세한 내용은 ASA 컨피그레이션 가이드를 참조하십시오.</p>
ASDM(Adaptive Security Device Manager)	<p>ASDM은 전체 ASA 기능을 제공하는 Java 기반 온디바이스 관리자입니다.</p> <p>ASDM을 통한 ASA 구축의 내용을 참조하십시오.</p>
CDO	<p>CDO(는) 클라우드 기반 멀티 디바이스 관리자입니다. CDO(는) threat defense 와(과) 같은 다른 보안 디바이스도 관리합니다.</p> <p>ASA용 CDO(는) 이 가이드에서 다루지 않습니다. To get started with CDO, see the CDO home page.</p>
CSM(Cisco Security Manager)	<p>CSM은 자체 서버 하드웨어에서 실행되는 다중 디바이스 관리자입니다. CSM은 threat defense 관리를 지원하지 않습니다.</p> <p>CSM은 이 가이드에서 다루지 않습니다. 자세한 내용은 CSM 사용 설명서를 참조하십시오.</p>
ASA HTTP 인터페이스	<p>HTTP를 사용하면 자동화 도구가 특수하게 형식이 지정된 URL에 액세스하여 ASA에서 명령을 실행할 수 있습니다.</p> <p>ASA HTTP 인터페이스는 이 가이드에서 다루지 않습니다. 자세한 내용은 자동화를 위한 Cisco Secure Firewall ASA HTTP 인터페이스를 참조하십시오.</p>

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.