어떤 운영 체제 및 관리자가 적합합니까?

하드웨어 플랫폼은 두 운영 체제 중 하나를 실행할 수 있습니다. 각 운영 체제에 대해 관리자를 선택할 수 있습니다. 이 장에서는 운영 체제 및 관리자 선택 사항에 대해 설명합니다.

운영 체제

하드웨어 플랫폼에서 보안 방화벽 ASA 또는 (FTD)(이전 Firepower Threat Defense) 애플리케이션 운영 체제를 사용할 수 있습니다.Secure Firewall Threat Defense

- ASA — ASA는 기존의 고급 스테이트풀 방화벽 및 VPN 집선 장치입니다.

  threat defense의 고급 기능이 필요하지 않거나 threat defense에서 아직 사용할 수 없는 ASA 전용 기능이 필요한 경우 ASA를 사용할 수 있습니다. Cisco는 ASA로 시작한 다음 나중에 threat defense 이미지로 다시 설치하는 경우 ASA를 threat defense로 변환하는 데 도움이 되는 ASA-threat defense 마이그레이션 툴을 제공합니다.

- Threat Defense — 하는 위협 방어 FTD는 고급 스테이트풀 방화벽, VPN 집선 장치 및 차세대 IPS를 결합한 차세대 방화벽입니다. 즉, threat defense는 ASA 기능을 최대한 활용하여 최상의 NGFW 및 IPS 기능과 결합합니다.

  ASA에는 ASA의 주요 기능이 대부분 포함되어 있으며 NGFW 및 IPS 기능이 추가로 포함되어 있으므로 ASA보다 threat defense를 사용하는 것이 좋습니다.

ASA와 threat defense간에 이미지를 재설치하려면 Cisco Secure Firewall ASA 및 Threat Defense 이미지 재설치 가이드를 참조하십시오.

매니저

threat defense 및 ASA는 여러 관리자를 지원합니다.

Threat Defense 관리자

표 *1: Threat Defense* 관리자

매니저	설명
Secure Firewall Management Center (구 Firepower Management Center)	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. management center는 표준 관리 인터페이스 대신 외부(또는 기타 데이터) 인터페이스에서 threat defense를 관리할 수 있습니다. 이 기능은 원격 브랜치 구축에 유용합니다. 참고 management center이 threat defense구성을 소유하므로 management center는 다른 관리자와 호환되지 않으며, management center을(를) 우회하여 직접 threat defense를 구성할 수 없습니다. 관리 네트워크에서management center을(를) 시작하려면 Management Center로 Threat Defense 구축의 내용을 참조하십시오. 원격 네트워크에서 management center를 시작하려면 Threat Defense 원격으로 구축 Management Center를 참조하십시오.
Secure Firewall Device Manager(구 Firepower 디바이스 관리자)	device manager는 웹 기반의 간소화된 온디바이스 관리자입니다. 간소화되었기 때문에 일부 threat defense 기능은 device manager를 사용하여 지원되지 않습니다. 소수의 디바이스만 관리하고 다중 디바이스 관리자가 필요하지 않은 경우 device manager를 사용해야 합니다. 참고 device manager 및 CDO는 모두 방화벽에서 구성을 검색할 수 있으므로, device manager 및 CDO를 사용하여 동일한 방화벽을 관리할 수 있습니다. management center는 다른 관리자와 호환되지 않습니다. device manager를 시작하려면 Device Manager로 Threat Defense 구축를 참조하십시오.

매니저	설명
Cisco Defense Orchestrator(CDO)	CDO는 간소화된 클라우드 기반 다중 디바이스 관리자입니다. 이는 간소화 되었기 때문에 일부 threat defense 기능은 CDO를 사용 하 여 지원 되지 않습니다. 간소화된 관리 경험(device manager와 유사)을 제공하는 다중 디바이스 관리자를 원하는 경우 CDO를 사용해야 합니다. CDO는 클라우드 기반이므로 자체 서버에서 CDO를 실행하는 데 따른 오버헤드가 없습니다. CDO는 ASA와 같은 다른 보안 디바이스도 관리하므로 모든 보안 디바이스에 대해 단일 관리자를 사용할 수 있습니다. CDO는 브랜치 오피스에서 하드웨어를 연결하고 그대로 둘 수 있는 로우 터치(low-touch) 프로비저닝을 제공합니다. 방화벽이 CDO에 자동으로 등록됩니다. 참고 device manager 및 CDO는 모두 방화벽에서 구성을 검색할 수 있으므로, device manager 및 CDO를 사용하여 동일한 방화벽을 관리할 수 있습니다. management center는 다른 관리자와 호환되지 않습니다. CDO 프로비저닝을 시작하려면 Threat Defense CDO를 이용한 구축 섹션을 참조하십시오.
Secure Firewall Threat Defense REST API	Threat Defense REST API를 사용하면 threat defense의 직접 구성을 자동화할 수 있습니다. 이 API는 방화벽에서 컨피그레이션을 검색할 수 있으므로 device manager 및 CDO와 호환됩니다. management center를 사용하여 threat defense을 관리하는 경우에는 이 API를 사용할 수 없습니다. 위협 방어 REST 는 이 가이드에서 다루지 않습니다. 자세한 내용은 Cisco Secure Firewall Threat Defense REST API 가이드를 참조하십시오.
Secure Firewall Management Center REST API	관리 센터 REST API를 사용하면 관리되는 threat defense에 적용할 수 있는 management center 정책 구성을 자동화할 수 있습니다. 이 API는 threat defense를 직접 관리하지 않습니다. 관리 센터 REST API는 이 가이드에서 다루지 않습니다. 자세한 내용은 Secure Firewall Management Center REST API 빠른 시작 가이드를 참조하십시오.

ASA 관리자

표 *2: ASA* 관리자

매니저	설명
ASDM(Adaptive Security Device Manager)	ASDM은 전체 ASA 기능을 제공하는 Java 기반 온디바이스 관리자입니다. CLI 대신 GUI를 사용하고 소수의 ASA만 관리해야 하는 경우 ASDM을 사용해야 합니다. ASDM은 방화벽에서 구성을 검색할 수 있으므로 ASDM과 함께 CLI, CDO 또는 CSM을 사용할 수도 있습니다. ASDM을 시작하려면 ASDM을 통한 ASA 구축 섹션을 참조하십시오.

매니저	설명
CLI	GUI보다 CLI를 선호하는 경우 ASA CLI를 사용해야 합니다. CLI는 이 가이드에서 다루지 않습니다. 자세한 내용은 ASA 컨피그레이션 가이드를 참조하십시오.
CDO	CDO는 간소화된 클라우드 기반 다중 디바이스 관리자입니다. 간소화되었기 때문에 일부 ASA 기능은 CDO를 사용하여 지원되지 않습니다. 간소화된 관리 환경을 제공하는 다중 디바이스 관리자를 원하는 경우 CDO를 사용해야 합니다. CDO는 클라우드 기반이므로 자체 서버에서 CDO를 실행하는 데 따른 오버헤드가 없습니다. CDO는 threat defense와 같은 다른 보안 디바이스도 관리하므로 모든 보안 디바이스에 대해 단일 관리자를 사용할 수 있습니다. CDO는 방화벽에서 구성을 검색할 수 있으므로 CLI 또는 ASDM을 사용할 수도 있습니다. CDO는 이 가이드에서 다루지 않습니다. CDO를 시작하려면 CDO 홈 페이지를 참조하십시오.
CSM(Cisco Security Manager)	CSM은 자체 서버 하드웨어에서 실행되는 강력한 다중 디바이스 관리자입니다. 많은 수의 ASA를 관리해야 하는 경우 CSM을 사용해야 합니다. CSM은 방화벽에서 구성을 검색할 수 있으므로 CLI 또는 ASDM을 사용할 수도 있습니다. CSM은 threat defense 관리를 지원하지 않습니다. CSM은 이 가이드에서 다루지 않습니다. 자세한 내용은 CSM 사용 설명서를 참조하십시오.
ASA REST API	ASA REST API를 사용하면 ASA 구성을 자동화할 수 있습니다. 그러나 API는 모든 ASA 기능을 포함하지 않으며 더 이상 개선되지 않습니다. ASA REST API는 이 가이드에서 다루지 않습니다. 자세한 내용은 Cisco ASA Secure Firewall REST API 빠른 시작 설명서를 참조하십시오.