Cisco Secure Firewall 마이그레이션 툴 호환성 가이드

초판: 2020년 10월 29일

최종 변경: 2021년 7월 30일

Cisco Secure Firewall 마이그레이션 툴 호환성 가이드

이 가이드는 운영 체제 및 호스팅 환경 요구 사항을 포함해서 Cisco Secure Firewall 소프트웨어 및 하드웨어 호환성에 대한 내용을 제공합니다.

마이그레이션에 지원되는 플랫폼

Cisco Secure Firewall 마이그레이션 툴을 사용한 마이그레이션이 지원되는 ASA, FPS 포함 ASA , Check Point, PAN, Fortinet, 및 Firewall Threat Defense 플랫폼 지원되는 threat defense 플랫폼에 대한 자세한 내용은 Cisco Secure Firewall 호환성 가이드에서 참고하십시오.

참고 Firewall 마이그레이션 툴은 독립형 ASA 디바이스를 독립형 threat defense 디바이스로 마이그레이션하는 것만 지원합니다.

참고 Firewall 마이그레이션 툴은 독립형 모드 또는 분산형 Check Point 컨피그레이션을 독립형 threat defense 디바이스로 마이그레이션하는 것만 지원합니다.

지원되는 소스 **ASA** 플랫폼

Firewall 마이그레이션 툴을 사용하여 다음과 같은 단일 또는 멀티 컨텍스트 ASA 플랫폼에서 컨피그레이션을 마이그레이션할 수 있습니다.

- ASA5510
- ASA 5520
- ASA 5540
- ASA 5550
- ASA 5580
- ASA 5506

- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- ASA가 포함된 ASA 5585-X 전용(Firewall 마이그레이션 툴은 ASA FirePOWER 모듈에서 컨피그레이션을 마이그레이션하지 않음)
- Firepower 1000 Series
- Firepower 2100 시리즈
- Firepower 4100 Series
- Firepower 9300 시리즈
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- VMware ESXi, VMware vSphere Web Client 또는 vSphere 독립형 클라이언트를 사용하여 구축된 VMware 기반 ASA 가상

FPS 포함 **ASA** 마이그레이션에 지원되는 소스 **ASA** 모델**:**

Cisco ASA FirePOWER 모듈은 다음 디바이스에 구축됩니다.

- ASA5506-X
- ASA 5506H-X
- ASA5506W-X
- ASA5508-X

- ASA5512-X
- ASA5515-X
- ASA5516-X
- ASA5525-X
- ASA5545-X
- ASA5555-X
- ASA5585-X-SSP-10
- ASA5585-X-SSP-20
- ASA5585-X-SSP-40
- ASA5585-X-SSP-60

지원되는 대상 **Secure Firewall Threat Defense** 플랫폼

Firewall 마이그레이션 툴을 사용하여 ASA, FPS 포함 ASA, Check Point, PAN, 및 Fortinet 소스 컨피그레이션을 threat defense 플랫폼의 다음과 같은 독립형 또는 컨테이너 인스턴스로 마이그레이션할 수 있습니다.

- ASA 5506
- ASA 5506W-X
- ASA 5506H-X
- ASA 5508-X
- ASA 5512-X
- ASA 5515-X
- ASA 5516-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- Firepower 1000 Series
- Firepower 2100 시리즈
- Firepower 4100 Series
- 다음을 포함하는 Firepower 9300 시리즈:
    - SM-24

- SM-36
- SM-40
- SM-44
- SM-48
- SM-56

- VMware ESXi, VMware vSphere Web Client 또는 vSphere 독립형 클라이언트를 사용하여 구축된 VMware 기반 threat defense virtual

마이그레이션에 지원되는 소프트웨어 버전

다음은 마이그레이션에 대해 지원되는 ASA, FPS 포함 ASA, Check Point, PAN, Fortinet 및 threat defense 버전입니다.

지원되는 **ASA** 방화벽 버전

Firewall 마이그레이션 툴은 ASA 소프트웨어 버전 8.4 이상을 실행하는 디바이스에서 마이그레이션을 지원합니다.

지원되는 **FPS** 포함 **ASA** 방화벽 버전

Firewall 마이그레이션 툴은 FPS 포함 ASA 소프트웨어 버전 9.2.2 이상을 실행하는 디바이스에서 마이그레이션을 지원합니다.

자세한 내용은 Cisco ASA 호환성 가이드의 ASA FirePOWER 모듈 호환성 섹션에서 참조하십시오.

지원되는 **Check Point** 방화벽 버전

Firewall 마이그레이션 툴은 Check Point OS r75–r77.30 및 r80–r80.40 버전을 실행하는 threat defense로의 마이그레이션을 지원합니다. **Select Source(**소스 선택**)** 페이지에서 적절한 Check Point 버전을 선택합니다.

참고 VSX는 지원되지 않습니다.

Firewall 마이그레이션 툴은 Check Point 플랫폼 Gaia에서의 마이그레이션을 지원합니다.

지원되는 **Palo Alto Networks** 방화벽 버전

Firewall 마이그레이션 툴은 PAN 방화벽 OS 6.1.x 이상 버전을 실행하는 threat defense로의 마이그레이션을 지원합니다.

지원되는 Fortinet 방화벽 버전

Firewall 마이그레이션 툴은 FortiNet 방화벽 OS 5.0.x 이상 버전을 실행하는 threat defense로의 마이그레이션을 지원합니다.

소스 ASA 컨피그레이션에 지원되는 Secure Firewall Management Center 버전

ASA의 경우 Firewall 마이그레이션 툴은 6.2.3 또는 6.2.3 이상 버전을 실행하는 management center에서 관리되는 threat defense 디바이스로의 마이그레이션을 지원합니다.

참고 일부 기능은 management center 및 threat defense의 최신 버전에서만 지원됩니다.

참고 마이그레이션 시간을 최적화하기 위해 management center를 software.cisco.com/downloads에서 다운로드받을 수 있는 권장 릴리스 버전으로 업그레이드하는 것이 좋습니다.

FPS 포함 ASA 소스 컨피그레이션에 지원되는 Management Center 버전

FPS 포함 ASA의 경우 Firewall 마이그레이션 툴은 6.5 이상 버전을 실행하는 management center에서 관리되는 threat defense 디바이스로의 마이그레이션을 지원합니다.

Check Point, PAN, 및 Fortinet Firewall 소스 컨피그레이션에 지원되는 Management Center 버전

Check Point, PAN 및 Fortinet 방화벽의 경우 Firewall 마이그레이션 툴은 6.2.3.3 이상 버전을 실행하는 management center에서 관리되는 threat defense 디바이스로의 마이그레이션을 지원합니다.

참고 일부 기능은 management center 및 threat defense의 최신 버전에서만 지원됩니다. 예를 들어 Fortinet의 시간 기반 ACL은 management center 6.6 이상 버전에서 지원됩니다.

참고 6.7 threat defense 디바이스로의 마이그레이션은 현재 지원되지 않습니다. 따라서 디바이스가 management center 액세스용 데이터 인터페이스로 구성된 경우 마이그레이션이 실패할 수 있습니다.

지원되는 Threat Defense 버전

Firewall 마이그레이션 툴에서는 threat defense 6.2.3 이상 버전을 실행하는 디바이스로의 마이그레이션을 권장합니다.

threat defense의 운영체제 및 호스팅 환경 요구 사항을 포함한 Cisco Secure Firewall 소프트웨어 및 하드웨어 호환성 정보에 대한 자세한 내용은 Cisco Secure Firewall 호환성 가이드에서 참고하십시오.

Firewall 마이그레이션 툴의 플랫폼 요구 사항

Firewall 마이그레이션 툴에는 다음과 같은 인프라 및 플랫폼 요구 사항이 있습니다.

- Windows 10 64비트 운영체제 또는 macOS 10.13 이상 버전에서 실행
- Google Chrome을 시스템 기본 브라우저로 사용
- (Windows) 대규모 마이그레이션 푸시 중에 시스템이 절전 모드로 전환되지 않도록 Power & Sleep(전원 및 절전)에서 Sleep(절전) 설정을 Never put the PC to Sleep(절전 모드로 전환 안 함)으로 구성
- (macOS) 대규모 마이그레이션 푸시 중에 컴퓨터와 하드 디스크가 절전 모드로 전환되지 않도록 Energy Saver(에너지 절약) 설정 구성

관련 문서

이 섹션에는 Firewall 마이그레이션 툴 관련 문서가 요약되어 있습니다.

- Cisco Secure Firewall Threat Defense 호환성 가이드 - 운영 체제 및 호스팅 환경 요구 사항을 포함해서 Cisco Secure Firewall 소프트웨어 및 하드웨어 호환성에 대한 내용을 제공합니다.
- Cisco ASA Compatibility(Cisco ASA 호환성) - Cisco ASA 소프트웨어 및 하드웨어 호환성 및 요구 사항을 나열합니다.
- Cisco Firepower 4100/9300 FXOS 호환성 - FXOS, Cisco Firepower 9300 및 Cisco Firepower 4100 Series 보안 어플라이언스, 지원되는 논리적 디바이스에 대한 소프트웨어 및 하드웨어 호환성 정보를 나열합니다.