Palo Alto Networks를 Cisco Secure Firewall Threat Defense로 마이그레이션 사전 요건 가이드

최종 변경: 2026년 5월 20일

Palo Alto Networks를 Cisco Secure Firewall Threat Defense로 마이그레이션 사전 요건 가이드

이 문서는 Cisco Secure Firewall 마이그레이션 툴을 사용하여 방화벽 설정을 PAN(Palo Alto Networks)에서 Firewall Threat Defense(으)로 마이그레이션하려는 사용자에게 필수 정보를 제공합니다.

마이그레이션 전 요구 사항

PAN(Palo Alto Networks)에서 Firewall Threat Defense(으)로 마이그레이션하기 전에 다음 조건을 충족해야 합니다.

1. 안정적인 **IP** 연결: Secure Firewall 마이그레이션 툴과 사이를 안정적으로 연결해 줍니다.
2. 버전: Management Center은(는) 버전 6.2.3 이상을 실행하고 있어야 합니다. 최적의 마이그레이션 성능과 향상된 소프트웨어 품질을 얻으려면 사용자 Threat Defense 및 Management Center에서 권장되는 릴리스를 사용하십시오.

참고 권장 릴리스는 Cisco Software Central의 금색 별표를 참조하십시오.

3. 사용자 어카운트: 방화벽 마이그레이션 툴에 대한 관리자 권한이 있는 Management Center에서 전용 사용자 어카운트를 생성하고, 마이그레이션 중에 이 자격증명을 사용합니다.
4. **Firewall Threat Defense** 디바이스: 디바이스 구성(예: 인터페이스, 경로 등)을 마이그레이션하려면 마이그레이션 전에 대상 Firewall Threat Defense 디바이스를 에 추가합니다.

참고 공유 구성(예: 개체, NAT 및 ACL)만 마이그레이션하는 경우 이 단계를 건너뛸 수 있습니다.

5. **Palo Alto Networks** 구성 요구 사항: Palo Alto 방화벽에서 명명된 구성 스냅샷을 .xml 형식으로 내보냅니다.

중요 NAT 정책에서 동일한 소스 및 대상 영역을 사용하는 경우 라우팅 테이블을 .txt 형식으로 업로드합니다.

기능별 요구 사항

- 원격 구축: 원격 구축은 및 Firewall Threat Defense, 버전 6.7 이상에서 사용할 수 있습니다. 원격 구축을 활성화한 경우 방화벽 마이그레이션 툴은 ACL, 네트워크 개체, 포트 개체 및 NAT만 마이그레이션합니다. 따라서 에서는 반드시 수동으로 인터페이스와 경로를 마이그레이션해야 합니다.
- **ID** 기반 액세스 제어 규칙: (와)과의 AD/LDAP 통합은 반드시 수행해야 합니다. 또한 에서 ID 정책을 생성해야 합니다. 마이그레이션 후에는 구성을 구축하기 전에 ID 정책을 액세스 정책에 연결해야 합니다.
- 사이트 간 **VPN** 터널:
  - 마이그레이션하기 전에 에 Firewall Threat Defense을(를) 추가합니다.
  - Firewall Threat Defense 및 버전이 6.7 이상인지 확인합니다(VTI에 대한 지원은 버전 6.7부터 사용 가능).
  - 소스 방화벽이 버전 8.0 이상을 실행 중인지 확인합니다.
  - IP 주소가 없는 모든 VTI(Virtual Tunnel Interface) 터널은 지원되지 않습니다. 마이그레이션 프로세스 후에 수동으로 마이그레이션해야 합니다.

참고 경로 기반 VPN의 경우 VTI 터널 IP 주소가 있어야 합니다.

  - 방화벽 마이그레이션 툴은 VPN 터널을 포인트 투 포인트 네트워크 토폴로지로 마이그레이션합니다.
  - 인증서 기반 VPN 마이그레이션을 시작하기 전에 Palo Alto 트러스트 포인트를 수동으로 PKI 개체로 에 마이그레이션합니다.
- 원격 액세스 **VPN(RA VPN):**
  - 대상 버전은 7.2 이상이어야 합니다.
  - Firewall Threat Defense 버전은 7.0 이상이어야 합니다.
  - 소스 방화벽 구성(PAN)은 8.0 이상이어야 합니다.
  - 현재 RADIUS, LOCAL, SAML 및 LDAP 인증 대한 마이그레이션만 지원됩니다.
  - Firewall Threat Defense을(를) 반드시 에 추가해야 합니다.

- 사전 마이그레이션 활동의 일부로 필요한 AnyConnect 클라이언트 이미지를 업로드합니다.
- Palo Alto 트러스트 포인트(인증서)는 마이그레이션 전 단계에서 PKI 개체로 에 수동으로 마이그레이션해야 합니다.

인터페이스 요구 사항

- 소스 방화벽에 포트 채널 인터페이스가 포함된 경우, 에서 유사한 포트 채널을 생성합니다. 이 툴은 하위 인터페이스를 자동으로 생성합니다.
- 클러스터 인터페이스 컨피그레이션을 사용하여 Firewall Threat Defense(으)로 마이그레이션하는 경우 디바이스를 대상 Firewall Threat Defense(으)로 사용하기 전에 기존 클러스터 인터페이스 컨피그레이션을 제거합니다. 또는 "FTD 플로우 없음"으로 진행하여 "인터페이스 및 경로" 마이그레이션을 건너뜁니다.

시스템 요구 사항

- 전원 옵션**:** 대규모 마이그레이션 푸시 중에 시스템이 절전 모드로 들어가지 않도록 합니다.
- 지원되는 브라우저**:** Google Chrome 또는 Microsoft Edge.

필수조건

- 온프레미스 관리 센터**:**
  - 소프트웨어 버전 6.2.3 이상.
  - 마이그레이션해야 하는 모든 기능이 포함되도록 Firewall Threat Defense용 스마트 라이선스를 설치합니다.
  - 시스템 > 구성 > **REST API** 기본 설정에서 에 REST API를 활성화합니다.
  - REST API를 활성화하려면 관리자 사용자 역할이 있어야 합니다.
- 클라우드 제공 방화벽 관리 센터**:** 방화벽 마이그레이션 툴은 Security Cloud Control(이전 Cisco Defense Orchestrator)을 통해 클라우드 제공 Firewall Management Center을(를) 지원합니다. 이 툴을 사용하면 클라우드 제공 Firewall Management Center을(를) 대상 관리 센터로 사용할 수 있습니다.

지원되는 **PAN** 구성

방화벽 마이그레이션 툴에서 PAN-Firewall Threat Defense 마이그레이션을 위해 아래 기능이 지원됩니다.

- 액세스 제어 정책 규칙
- NAT 정책(특정 제한 사항 있음)
- 네트워크 개체 및 그룹
- 서비스 개체 및 그룹
- 주소 개체 및 그룹
- 보안 영역
- 정적 라우팅
- 레이어 3 인터페이스
- 하위 인터페이스
- VLAN 인터페이스
- 액세스 규칙 최적화(섀도우 및 중복 규칙 식별)

  이 옵션을 사용하는 것이 좋습니다.

참고 가상 유선 인터페이스는 마이그레이션되지 않는 반면 가상 유선 영역은 마이그레이션됩니다. 마이그레이션 후 Firewall Threat Defense에서 BVI 인터페이스를 수동으로 생성해야 합니다.

Palo Alto Networks 방화벽을 Cisco Secure Firewall Threat Defense로 마이그레이션에 대한 제한 사항

이 섹션에서는 방화벽 마이그레이션 툴에서 제한 사항이 있거나 지원되지 않는 구성 및 시나리오에 대해 설명합니다.

지원되지 않는 **PAN** 구성

방화벽 마이그레이션 툴은 PAN 에서 Firewall Threat Defense(으)로의 마이그레이션을 위해 다음 기능을 지원하지 않습니다.

- 시간 기반 액세스 제어 정책 규칙
- 특수 문자로 시작하거나 특수 문자를 포함하는 FQDN 개체
- 와일드카드 FQDN
- 변환된 소스에 FQDN 개체 및 FQDN 개체 그룹이 있는 NAT 규칙
- 원본 소스와 대상 모두에 FQDN 개체 및 FQDN 개체 그룹이 있는 NAT 규칙
- 변환된 대상에 FQDN 개체 그룹이 있는 NAT 규칙

- IPv6 NAT
- 동적 라우팅 프로토콜(OSPF 및 BGP)
- VRF
- 프로파일 소스 또는 대상 부정이 있는 정책

참고 모든 정책(지원됨 또는 지원되지 않음)은 (으)로 마이그레이션됩니다. 지원되지 않는 정책은 비활성화된 것으로 마이그레이션됩니다. 정책을 활성화하기 전에 요구 사항에 따라 시스템을 구성해야 합니다.

부분적으로 지원되는 **ASA** 구성

다음 구성은 부분적으로 지원됩니다. 일부 고급 옵션은 나열된 구성에 대해 마이그레이션되지 않을 수 있습니다.

- 프로파일을 사용하는 액세스 제어 정책 규칙.
- TCP, UDP 및 SCTP 프로토콜이 있는 서비스 개체를 포함하는 서비스 그룹입니다(SCTP 유형은 제거될 예정임).
- 지원되는 개체와 지원되지 않는 개체를 모두 포함하는 개체 그룹입니다(지원되지 않는 개체는 제거될 예정임).

VPN 기능

- 사용되지 않는 **1**단계/**2**단계**(IKE/IPsec)** 매개변수**:** IKEv1 DH 그룹 2, 5; IKEv2 DH 그룹 2, 5, 24; 해시 MD5; 암호화 des, 3des, null.
- **RAVPN(**원격 액세스 **VPN)** 인증**:** TACACS+ 및 Kerberos 인증은 현재 지원되지 않습니다.

인터페이스 요구 사항

- 클러스터 인터페이스 구성을 사용한 Firewall Threat Defense(으)로의 마이그레이션은 지원되지 않습니다.
- 가상 유선 인터페이스는 마이그레이션되지 않습니다(반면 가상 유선 영역은 마이그레이션됨). 마이그레이션 후 Firewall Threat Defense에서 BVI 인터페이스를 수동으로 생성해야 합니다.

버전

디바이스가 액세스를 위해 데이터 인터페이스를 사용하는 경우, Palo Alto Networks를 Firewall Threat Defense 버전 6.7로 마이그레이션하는 기능은 현재 지원되지 않습니다.

마이그레이션에 지원되는 플랫폼

지원되는 **PAN** 버전

방화벽 마이그레이션 툴은 PAN 방화벽 OS 버전 8.0 이상에서 마이그레이션을 지원합니다.

지원되는 대상 **Firewall Threat Defense** 플랫폼

- Firepower 1000 Series
- Firepower 2100 Series
- Secure Firewall 3100 Series
- Firepower 4100 Series
- Secure Firewall 4200 Series
- Firepower 9300 시리즈(SM-24, SM-36, SM-40, SM-44, SM-48, SM-56)
- VMware 기반 Threat Defense(ESXi, vSphere)
- Microsoft Azure Cloud 기반 Threat Defense Virtual
- AWS 클라우드 기반 Threat Defense Virtual

지원되는 버전

방화벽 마이그레이션 툴은 버전 6.2.3.3 이상으로 PAN 방화벽 마이그레이션을 지원합니다.

지원되는 **Firewall Threat Defense** 버전

PAN에서 Firewall Threat Defense 마이그레이션의 경우 Firewall Threat Defense 버전 6.5 이상으로 마이그레이션하는 것이 좋습니다.

보안 클라우드 제어 지역

보안 클라우드 제어는 아래 지역에서 사용할 수 있으며, 지역은 URL 확장명으로 식별할 수 있습니다.

표 ***1:*** 보안 클라우드 제어 지역 및 ***URL***

지역	보안 클라우드 제어 **URL**
유럽	https://eu.manage.security.cisco.com/
미국	https://us.manage.security.cisco.com/
APJC	https://apj.manage.security.cisco.com/

지역	보안 클라우드 제어 **URL**
호주	https://au.manage.security.cisco.com/
인도	https://in.manage.security.cisco.com/

참조

자세한 내용 및 전체 마이그레이션 가이드는 마이그레이션 툴을 사용하여 *Palo Alto Networks* 방화벽을 *Cisco Secure Firewall Threat Defense*로 마이그레이션을 참조하십시오.

추가 자료:

- Cisco Secure Firewall 호환성 가이드
- Threat Defense 컨피그레이션 가이드
- Cisco Smart Software Manager
- Security Cloud Control 문서

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.

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.