

FMT를 사용하여 Paloalto를 Firepower 위협 방어 로 마이그레이션

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[배경 정보](#)

[Paloalto 방화벽 컨피그레이션 zip 파일 가져오기](#)

[마이그레이션 전 체크리스트](#)

[구성](#)

[마이그레이션 단계](#)

[문제 해결](#)

[Secure Firewall 마이그레이션 툴 트러블슈팅](#)

[일반적인 마이그레이션 실패:](#)

[문제 해결을 위해 지원 번들 사용:](#)

소개

이 문서에서는 Paloalto Firewall을 Cisco Firepower 위협 디바이스로 마이그레이션하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 마이그레이션 도구
- Paloalto 방화벽
- FTD(보안 방화벽 위협 방어)
- Cisco FMC(Secure Firewall Management Center)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FMT(Firepower 마이그레이션 도구) v7.7이 포함된 Mac OS
- PAN NGFW 버전 8.0 이상
- FMCv(Secure Firewall Management Center) v7.6
- Secure Firewall Threat Defense 버전 7.4.2

경고문: 이 문서에서 참조하는 네트워크 및 IP 주소는 개별 사용자, 그룹 또는 조직과 연결되어 있지 않습니다. 이 컨피그레이션은 랩 환경에서만 사용하도록 만들어졌습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

이 문서의 구체적인 요구 사항은 다음과 같습니다.

- PAN NGFW 버전 8.4 이상
- FMCv(Secure Firewall Management Center) 버전 6.2.3 이상

Firewall Migration Tool은 다음 디바이스 목록을 지원합니다.

- Cisco ASA(8.4+)
- Cisco ASA(9.2.2+) with FPS
- Cisco Secure Firewall Device Manager(7.2+)
- 검사점(r75-r77)
- Check Point(r80-r81)
- Fortinet(5.0+)
- Palo Alto Networks(8.0+)

배경 정보

Paloalto 방화벽 컨피그레이션을 마이그레이션하기 전에 다음 작업을 실행합니다.

Paloalto 방화벽 컨피그레이션 zip 파일 가져오기

- Paloalto Firewall은 버전 8.4 이상이어야 합니다.
- Palo Alto 방화벽에서 현재 실행 중인 컨피그레이션을 내보냅니다(*.xml은 xml 형식이어야 합니다).
- Paloalto 방화벽 Cli에 로그인하여 show routing route를 실행하고 출력을 txt 형식(*.txt)으로 저장합니다.
- 실행 중인 구성 파일(*.xml) 및 라우팅 파일(*.txt)을 *.zip 확장자로 압축합니다.

마이그레이션 전 체크리스트

- 마이그레이션 프로세스를 시작하기 전에 FTD가 FMC에 등록되었는지 확인합니다.
- 관리 권한이 있는 새 사용자 계정이 FMC에 생성되었습니다. 또는 기존 관리자 자격 증명을 사용할 수 있습니다.
- configuration file.xml을 실행하는 내보낸 Palo Alto는 .zip 확장자로 압축되어야 합니다(이전 섹션에서 설명한 절차를 따르십시오).
- Firepower 디바이스의 물리적 또는 하위 인터페이스 또는 포트 채널 수가 Paloalto 방화벽 인

터페이스와 같거나 더 많아야 합니다.

구성

마이그레이션 단계

1. 컴퓨터와 호환되는 Cisco Software Central에서 최신 Firepower 마이그레이션 도구를 다운로드 합니다.

Software Download

Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.7.0

Expand All Collapse All

Latest Release

7.7.0

All Release

7

Secure Firewall Migration Tool

Release 7.7.0

▲ My Notifications

Related Links and Documentation

[Open Source](#)

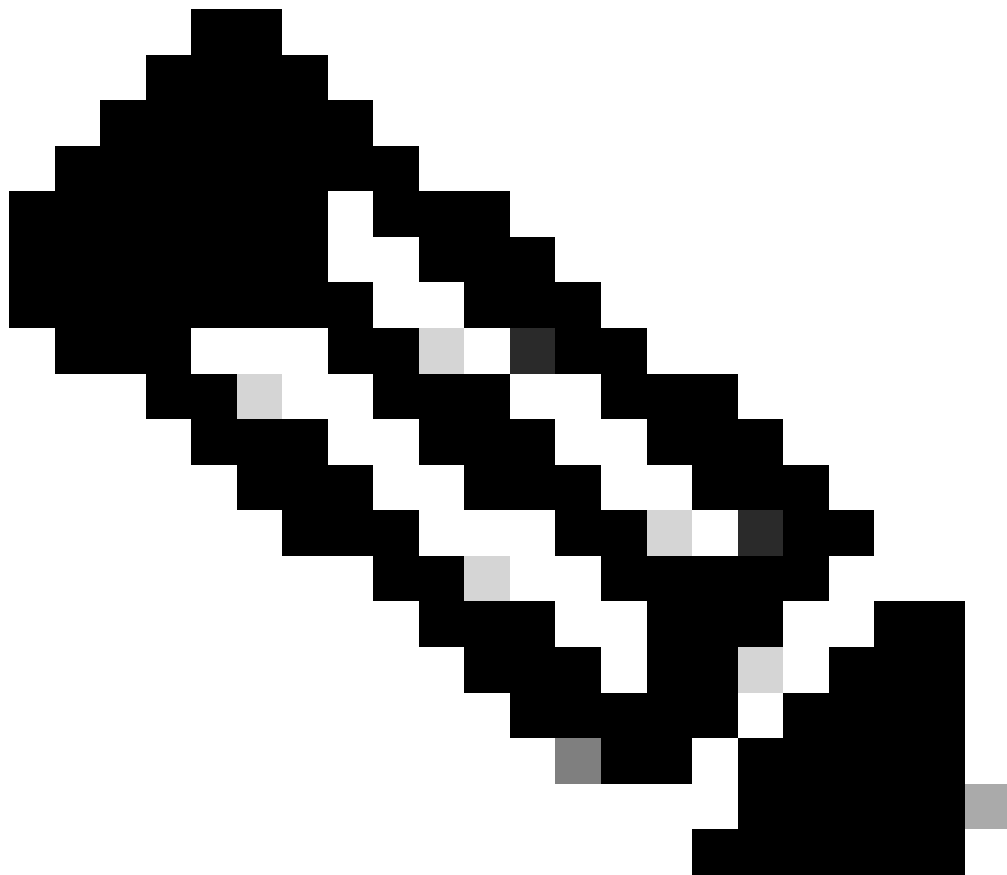
[Release Notes for 7.7.0](#)

[Install and Upgrade Guides](#)

File Information	Release Date	Size	
Firewall Migration Tool 7.7 for Mac Firewall_Migration_Tool_v7.7~12208.command Advisories	03-Feb-2025	78.72 MB	↓ 🛒
Firewall Migration Tool 7.7 for Windows Firewall_Migration_Tool_v7.7~12208.exe Advisories	03-Feb-2025	69.54 MB	↓ 🛒

FMT 다운로드

3. 이전에 컴퓨터에 다운로드한 파일을 엽니다.



참고: 프로그램이 자동으로 열리고 콘솔이 파일을 실행한 디렉토리에 내용을 자동으로 생성합니다.

-
4. 프로그램을 실행하면 최종 사용자 사용권 계약을 표시하는 웹 브라우저가 열립니다.
 1. 약관에 동의하려면 확인란을 선택합니다.
 2. Proceed(진행)를 클릭합니다.
 5. FMT GUI에 액세스하려면 유효한 CCO 자격 증명을 사용하여 로그인합니다.

Security Cloud Sign On

Email

s

Continue

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

[System status](#) [Policy statement](#)

FMT 로그인 프론트

6. 마이그레이션할 소스 방화벽을 선택하고 마이그레이션 시작을 클릭합니다.

Firewall Migration Tool (Version 7.7)

Select Source Configuration

Source Firewall Vendor

Palo Alto Networks (8.0+)

Start Migration Demo Mode

Palo Alto Networks (8.0+) Pre-Migration Instructions

This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) when migration is in progress.

Session Telemetry:
Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:
FMT: Firewall Migration Tool FMC: Firewall Management Center
FTD: Firewall Threat Defense

Before you begin your Palo Alto Networks (PAN) to Firewall Threat Defense migration, you must have the following items:

- Stable IP Connection:**
Ensure that the connection is stable between FMT and FMC.
- FMC Version:**
Ensure that the FMC version is 6.2.3 or later. For optimal migration time, improved software quality and stability, use the suggested release for your FTD and FMC. Refer to the gold star on CCO for the suggested release.
- FMC Account:**
Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration.
- FTD (Optional):**
To migrate the device configurations like interfaces, routes, and so on, add the target device to FMC. Skip this step if you want to migrate only the shared configurations like objects, NAT, ACL, and so on.
- Palo Alto Networks Configuration Requirements:**
Export named configuration snapshot file from palo alto firewall to .xml format. If your NAT has policies with the same source and destination zone, then

FMT GUI

7. 이제 Extraction Methods 섹션이 표시됩니다. 여기서 Paloalto Firewall의 Zip 컨피그레이션 파일을 FMT로 업로드해야 합니다.

Firewall Migration Tool (Version 7.7)

Extract Config Information

Extraction Methods

Manual Configuration Upload

The configuration file must be a zip file consisting of the following:

- Zip Config file derived from the PAN Tool.

Upload

Context Selection

Parsed Summary

Extract Config Information

Extraction Methods

Manual Configuration Upload

The configuration file must be a zip file consisting of the following:

- Zip Config file derived from the PAN Tool.

Upload

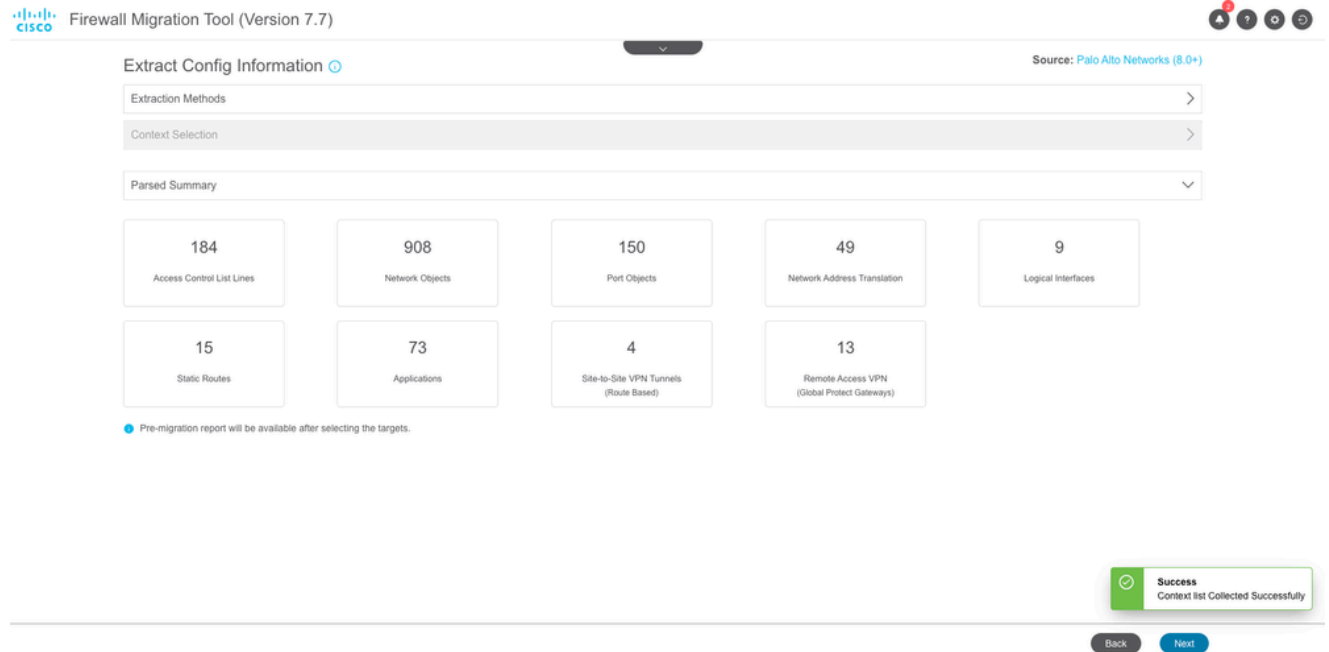
Context Selection

Parsed Summary

컨피그레이션 업로드 마법사

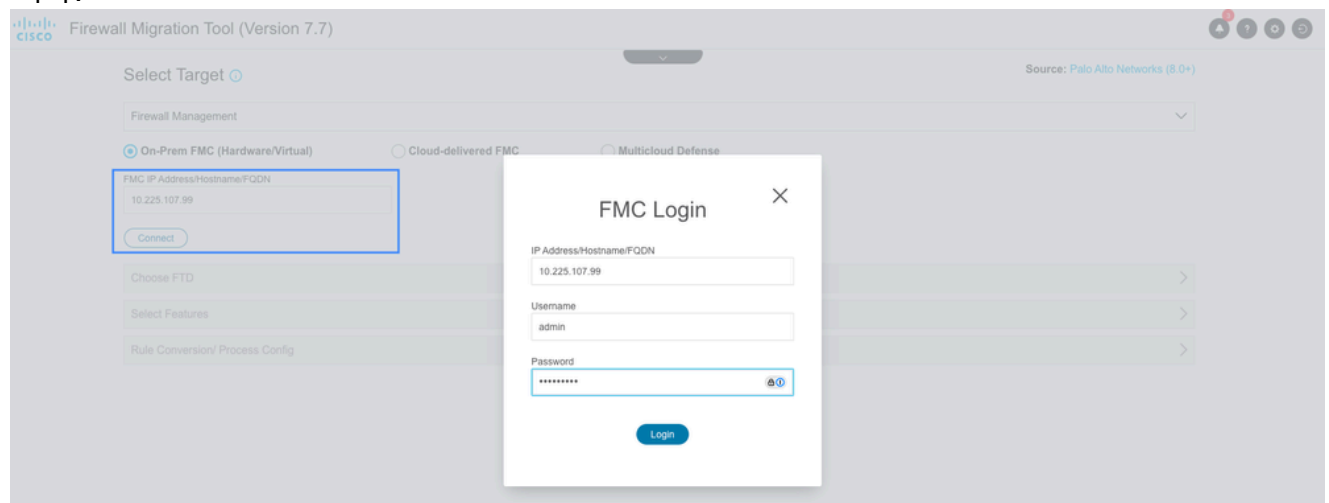
8. 구성 파일을 업로드한 후 구문 분석된 구성 요약이 표시됩니다. VSYS의 경우 별도의 VSYS 선택 항목을 사용할 수 있습니다. 각 항목을 구문 분석하고 차례로 마이그레이션해야 합니다.

구문 분석된 요약을 확인하고 Next(다음) 아이콘을 클릭합니다.



구성 유효성 검사 요약

9. 이 섹션에서 FMC 유형을 선택할 수 있습니다. 관리 IP 주소를 입력하고 Connect(연결)를 클릭합니다.
FMC 자격 증명을 제공할지 묻는 팝업이 표시됩니다. 자격 증명을 입력하고 로그인을 클릭합니다.



FMC 로그인

10. FMC에 성공적으로 연결하면 이제 도메인(있는 경우)을 선택하고 Proceed(계속)를 클릭할 수 있습니다.

Firewall Migration Tool (Version 7.7)

Source: Palo Alto Networks (8.0+)

Select Target

Firewall Management

On-Prem FMC (Hardware/Virtual) Cloud-delivered FMC Multicloud Defense

FMC IP Address/Hostname/FQDN: 10.225.107.99

Choose Domain: Global/Cisco

Connect

Proceed

Successfully connected to FMC

도메인 선택

11. 마이그레이션할 FTD를 선택하고 Proceed(진행)를 클릭합니다.

Firewall Migration Tool (Version 7.7)

Source: Palo Alto Networks (8.0+)

Select Target

Firewall Management

FMC IP Address/Hostname/FQDN: 10.225.107.99

Selected Domain: Global/Cisco

Choose FTD

Select FTD Device: FW1 (10.105.209.80) - NA (R)

Proceed without FTD

Proceed

Select Features

Rule Conversion/ Process Config

대상 FTD 선택

12. 이제 이 도구는 마이그레이션할 기능을 나열합니다. Proceed(진행)를 클릭합니다.

Firewall Migration Tool (Version 7.7)

Source: Palo Alto Networks (8.0+)

Select Target

Firewall Management

FMC IP Address/Hostname/FQDN: 10.225.107.99

Selected Domain: Global/Cisco

Choose FTD

Selected FTD: FW1

Select Features

Device Configuration

- ☒ Interfaces
- ☒ Routes
- ☒ Site-to-Site VPN Tunnels
- ☐ Policy Based (Unsupported)
- ☒ Route Based (VTI)

Shared Configuration

- ☒ Access Control
- ☐ Migrate policies with Application-default as Enabled
- ☒ Network Objects
- ☒ Port Objects
- ☒ Remote Access VPN

Advanced Configuration

Optimization

- ☒ Migrate Only Referenced Objects

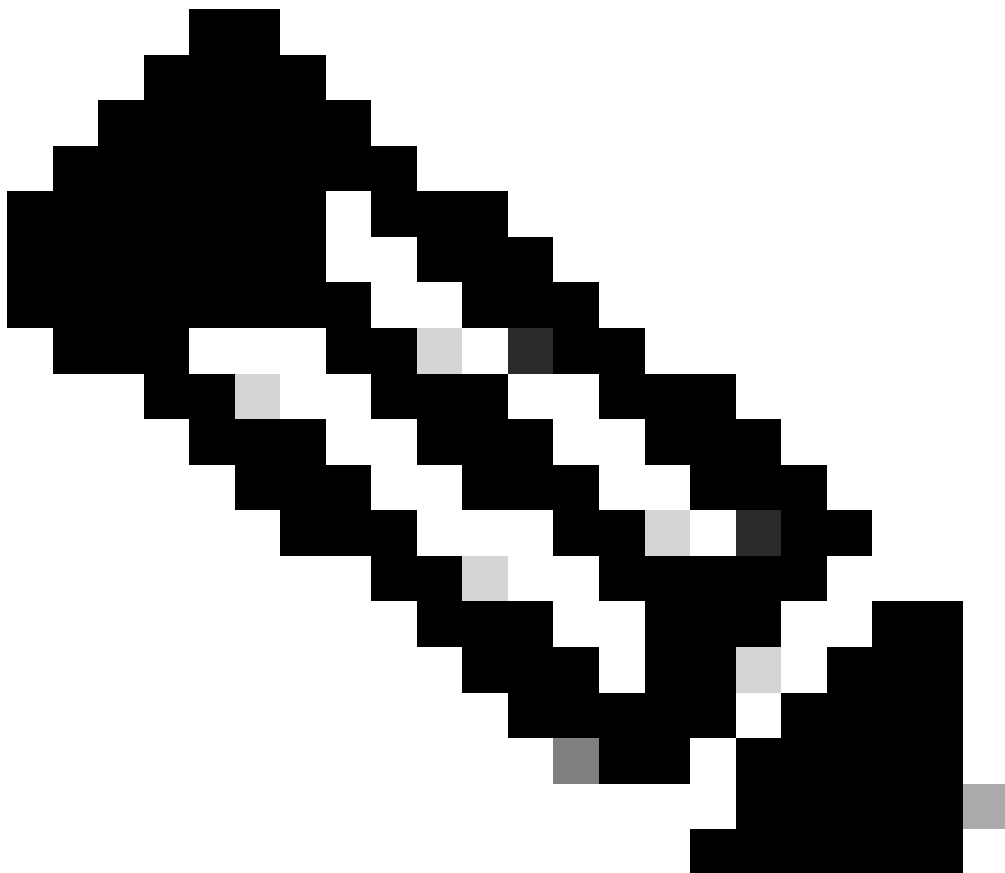
Access Control Options

- ☒ Discovered Identities

Proceed

Rule Conversion/ Process Config

기능 선택



참고: 기본적으로 모든 피처가 선택됩니다. 마이그레이션하지 않을 컨피그레이션은 선택 취소할 수 있습니다.

13. 컨피그레이션을 변환하려면 Start Conversion(변환 시작)을 클릭합니다.



구성 구문 분석

이 도구는 컨피그레이션을 구문 분석하고 이미지에 표시된 것처럼 변환 요약을 표시합니다. 마이그레이션된 컨피그레이션에 오류 또는 경고가 있는 경우 이를 검증하기 위한 마이그레이션 전 보고서를 다운로드할 수도 있습니다. 다음을 눌러 다음 페이지로 이동합니다.

Select Target Source: Palo Alto Networks (8.0+)

Firewall Management >

FMC IP Address/Hostname/FQDN: 10.225.107.99 Selected Domain: Global/Cisco

Choose FTD >

Selected FTD: FW1

Select Features >

Rule Conversion/ Process Config >

[Start Conversion](#)

No parsing error found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration. [Download Report](#)

For pre-migration report

Parsed configuration summary

195 Access Control List Lines	752 Network Objects	98 Port Objects	52 Network Address Translation	8 Logical Interfaces
2 Static Routes	0 Site-to-Site VPN Tunnels (Route Based)	70 Applications	9 Remote Access VPN (Global Protect Gateways)	

[Back](#) [Next](#)

구문 분석된 구성 요약

14. Interface Mapping(인터페이스 매핑) 섹션에서 각 인터페이스에 대한 인터페이스 이름을 편집할 수 있을 뿐 아니라 Paloalto-FTD 인터페이스 매핑을 정의할 수 있습니다. 인터페이스 매핑이 완료된 후 Next(다음)를 클릭합니다.

Map FTD Interface Source: Palo Alto Networks (8.0+)
Target FTD: FW1

PAN Interface Name	FTD Interface Name	Mapped Name
ethernet1/2	Select interface	ethernet1_2
ethernet1/3	✓ Ethernet1/1	ethernet1_3
ethernet1/4	Ethernet1/10	ethernet1_4
ethernet1/5	Ethernet1/11	ethernet1_5
ethernet1/6	Ethernet1/12	ethernet1_6
ethernet1/7	Ethernet1/13	ethernet1_7
	Ethernet1/14	
	Ethernet1/15	
	Ethernet1/16	
	Ethernet1/17	
	Ethernet1/18	
	Ethernet1/19	

FTD Interface name can be edited

Mapping of FTD interfaces

10 per page 1 to 6 of 6 Page 1 of 1

[Back](#) [Next](#)

인터페이스 매핑

15. 각 인터페이스에 대해 보안 영역을 수동으로 추가하거나 Map the Security Zone(보안 영역 매핑) 섹션에서 보안 영역을 자동으로 생성할 수 있습니다. 보안 영역을 생성하고 매핑한 후 Next(다음)를 클릭합니다.

Map Security Zones

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Add SZ

Auto-Create

Save

PAN Zone Name	FMC Security Zones
G...-Inside	Select Security Zone
Outside	Select Security Zone
GPVFN-	Select Security Zone
I...-Ine	Select Security Zone
DMZ	Select Security Zone
...C	Select Security Zone
Mel	Select Security Zone
OT-	Select Security Zone
Wireless-	Select Security Zone
I...-Inside	Select Security Zone

First option is to add Security Zone manually and second option is to auto create Security Zone

Note: Interfaces that are used in multiple configurations are allowed to have their unique security zones. The security zone mapping section for these interfaces will be grayed out.

10 per page 1 to 10 of 12 |< Page 1 of 2 >|

Back

Next

보안 영역 생성

보안 영역 수동 생성:

on Tool (Version 7.7)

Security Zones

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Add SZ

Security Zones (SZ)

Add

Max 48 characters for zone name. Allowed special characters are _-+*

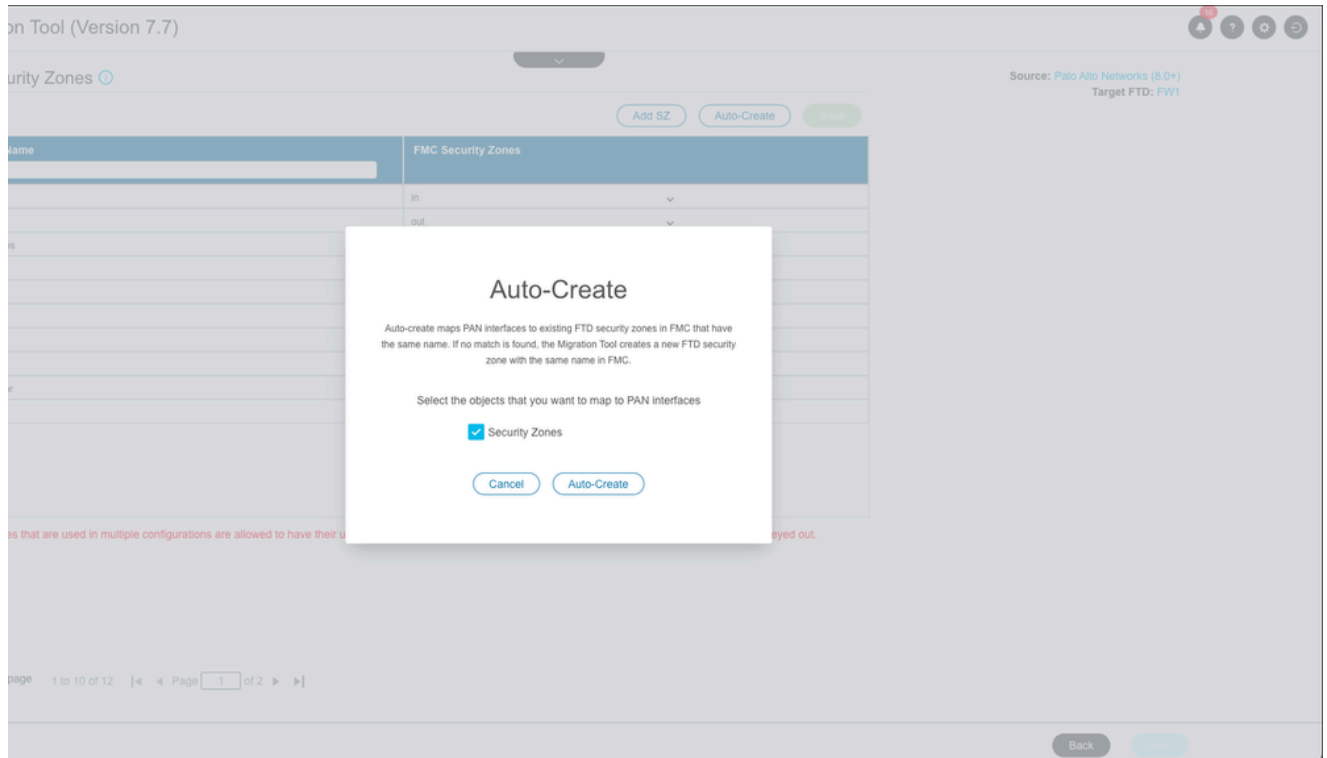
Security Zones	Type	Actions
DMZ	Select	X ✓
	SWITCHED	
	ROUTED	✓

0 - 0 of 0 |< 1 >|

Close

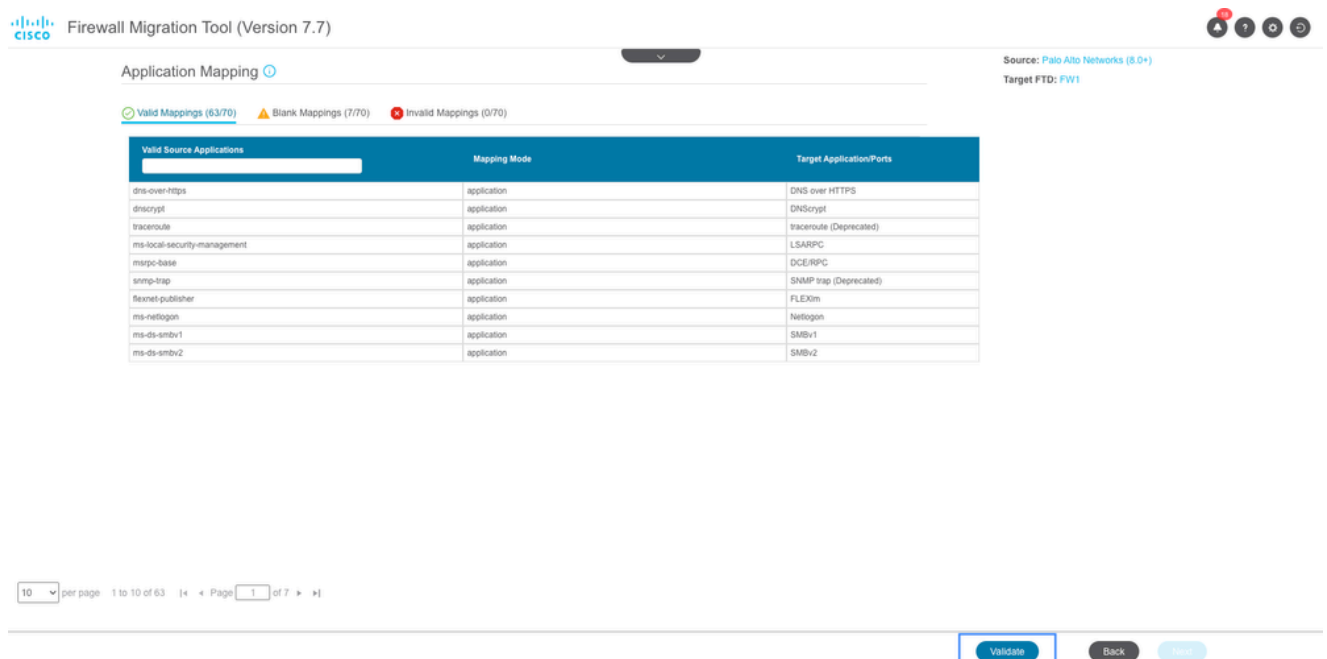
수동 보안 영역 생성

보안 영역 자동 생성:



자동 보안 영역 생성

16. 이제 Application Mapping(애플리케이션 매핑) 섹션으로 이동할 수 있습니다. Validate(검증) 버튼을 클릭하여 애플리케이션 매핑을 검증합니다.



애플리케이션 매핑

Application Mapping

Validation of application mapping is in progress. Please wait

Source: Palo Alto Networks (8.0+)

Target FTD: FW1

Valid Mappings (63/70) Blank Mappings (7/70) Invalid Mappings (0/70)

Valid Source Applications	Mapping Mode	Target Application/Ports
dns-over-https	application	DNS over HTTPS
dnscrypt	application	DNScrypt
traceroute	application	traceroute (Deprecated)
ms-local-security-management	application	LSARPC
snmp-base	application	DCE/RPC
snmp-trap	application	SNMP trap (Deprecated)
flexnet-publisher	application	FLEXlm
ms-netlogon	application	Netlogon
ms-ds-smbv1	application	SMBv1
ms-ds-smbv2	application	SMBv2

10 per page 1 to 10 of 63 Page 1 of 7

[Validate](#)
[Back](#)
[Next](#)

애플리케이션 매핑 검증

검증 시 FMT는 빈 매핑과 유효하지 않은 매핑을 나열합니다. 잘못된 매핑은 계속 진행하기 전에 수정해야 하며 빈 매핑은 선택 사항입니다.

수정된 매핑을 검증하려면 Validate(검증)를 다시 한 번 클릭합니다. 검증이 성공하면 다음을 클릭합니다.

Application Mapping

Clear Mapped Data

Source: Palo Alto Networks (8.0+)

Target FTD: FW1

Valid Mappings (61/70) Blank Mappings (7/70) Invalid Mappings (2/70)

Invalid Source Applications	Mapping Mode	Target Application/Ports
traceroute	Application	netmg-traceroute
snmp-trap	Port(s)	udp/162

10 per page 1 to 2 of 2 Page 1 of 1

[Validate](#)
[Back](#)
[Next](#)

공백 및 잘못된 응용 프로그램 매핑

- 필요한 경우 다음 섹션에서 ACL을 최적화할 수 있습니다. 액세스 제어, 객체, NAT, 인터페이스, 경로 및 원격 액세스 VPN과 같은 각 섹션의 컨피그레이션을 검토합니다. 컨피그레이션을 검토한 후 Validate(검증)를 클릭합니다.

Optimize, Review and Validate Configuration

Source: Palo Alto Networks (8.0+)
Target FTD: FW1

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Remote Access VPN

Verify configuration in each section

Select all 195 entries Selected: 0 / 195

Actions Save

Search

#	Name	Zone	SOURCE			Zone	DESTINATION		Port	Application	URLs	State	Action	TIME BASED
			Network	Port	User		Network	Port						
☐	1	Allow Tm...	Dt...	GRP_ADDR...	ANY	ANY			ANY	NTP	NA	✓	Allow	None
☐	2	Allow Tm...	Dt...	ANY	ANY	ANY			ANY	NTP	NA	✓	Allow	None
☐	3	Allow Tm...	Dt...	GRP_ADDR...	ANY	ANY			ANY	NTP	NA	✓	Allow	None
☐	4	Allow DNS	Dt...	ANY	ANY	ANY			ANY	DNS, DNSCrypt, DN...	NA	✓	Allow	None
☐	5	Allow DNS	Ot...	ANY	ANY	ANY			ANY	DNS	NA	✓	Allow	None
☐	6	Allow API	Dt...	ANY	ANY	ANY			ANY	TCP-80, TCP...	NA	✓	Allow	None
☐	7	Allow traffi	G...	ADDR_10.11...	ANY	ANY			2.16...	TCP-443	ANY	✓	Allow	None
☐	8	Allow Acco	G...	ADDR_192.16...	ANY	ANY			ANY	ANY	NA	✓	Allow	None
☐	9	Allow ICM	Ot...	ANY	ANY	ANY			ANY	netmg-traceroute	NA	✓	Allow	None
☐	10	Allow ICM	Ot...	ANY	ANY	ANY			ANY	ICMPv4	ANY	✓	Allow	None
☐	11	Allow DHCP	Ot...	ANY	ANY	ANY			ANY	DHCP	NA	✓	Allow	None
☐	12	Allow NetB	Ot...	ANY	ANY	ANY			ANY	NetBIOS-ns, NetBIO...	NA	✓	Allow	None
☐	13	Allow DNS	Ot...	ANY	ANY	ANY			ANY	DNS	NA	✓	Allow	None

50 per page 1 to 50 of 195 Page 1 of 4

Optimise access control list and validate

Optimize ACL Validate

구성 검증

18. 검증이 성공적으로 완료되면 검증 요약이 표시됩니다. Push Configuration(컨피그레이션 푸시)을 클릭하여 대상 FMC에 컨피그레이션을 푸시합니다.

Optimize, Review and

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Remote Access VPN

Select all 195 entries Selected: 0 / 195

#	Name
☐	1
☐	2
☐	3
☐	4
☐	5
☐	6
☐	7
☐	8
☐	9
☐	10
☐	11
☐	12
☐	13

Validation Status



Successfully Validated

Validation Summary (Pre-push)

195

Access Control List Lines

752

Network Objects

100

Port Objects

52

Network Address Translation

8

Logical Interfaces

2

Static Routes

0

Site-to-Site VPN Tunnels
(Route Based)

62

Applications

9

Remote Access VPN
(Global Protect Gateways)

Note: The configuration on the target FTD device FW1 (10.105.209.80) will be overwritten as part of this migration.

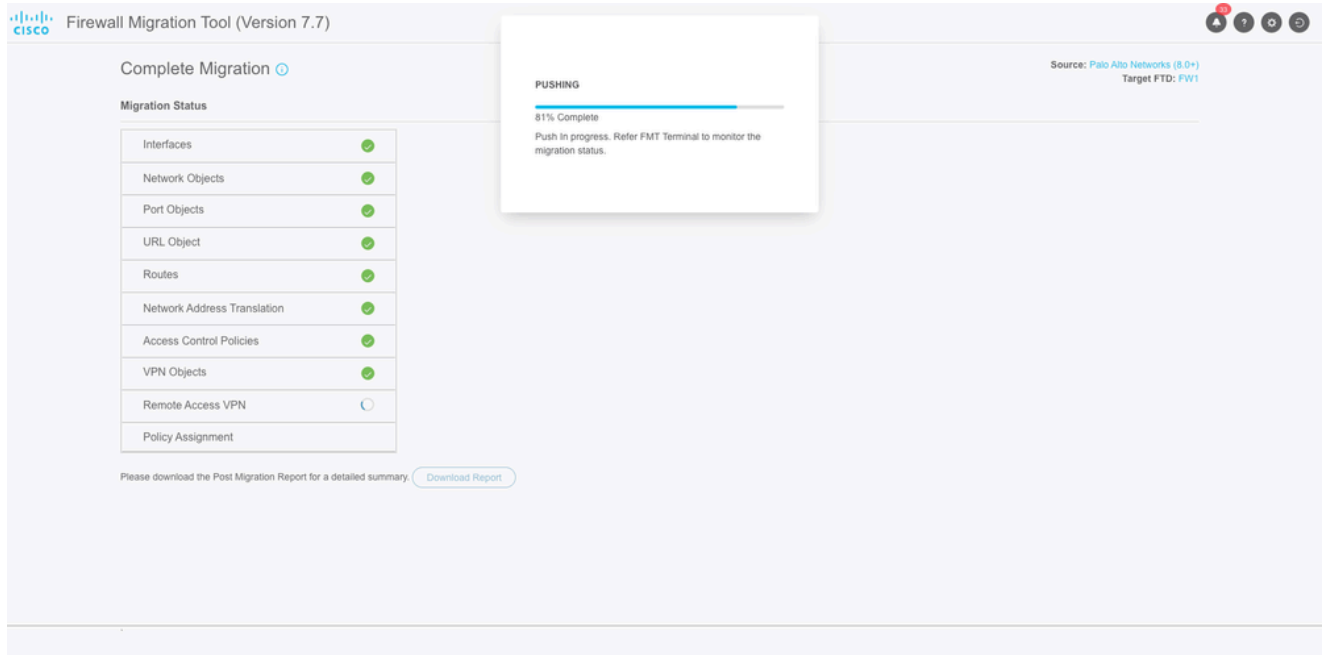
Push Configuration

50 per page 1 to 50 of 195 Page 1 of 4

Optimize ACL Validate

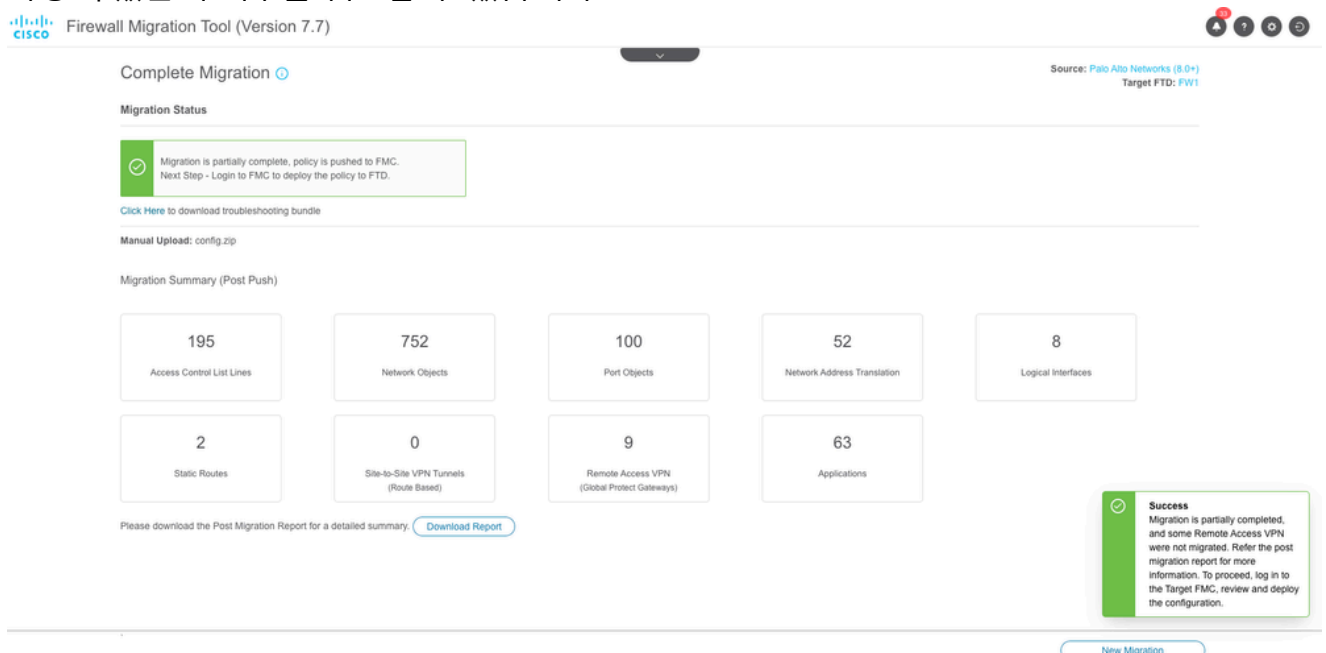
구성 유효성 검사 요약

19. 이제 FMC로의 컨피그레이션 밀어넣기 진행률이 Migration Status(마이그레이션 상태) 섹션에 표시됩니다. 마이그레이션 상태를 모니터링하기 위해 FMT 터미널 창도 사용할 수 있습니다.



마이그레이션 상태

20. 마이그레이션 요약은 성공적인 마이그레이션 시 툴에 의해 표시됩니다. 또한 부분적으로 마이그레이션된 컨피그레이션이 있는 경우 이를 나열합니다. 예를 들어, Secure Client Package가 없기 때문에 이 시나리오에서 원격 액세스 VPN 컨피그레이션을 수행할 수 있습니다. 또한 마이그레이션 후 보고서를 다운로드하여 마이그레이션된 구성을 검토하고 오류나 수정 사항이 있는지 여부를 검토할 수 있습니다.



마이그레이션 성공 요약

21. 마지막 단계는 FMC에서 마이그레이션된 컨피그레이션을 검토하고 FTD에 컨피그레이션을 구축하는 것입니다.

컨피그레이션을 구축하려면

1. FMC GUI에 로그인합니다.
2. Deploy(구축) 탭으로 이동합니다.
3. 방화벽에 컨피그레이션을 푸시하려면 구축을 선택합니다.

4. Deploy를 클릭합니다.

문제 해결

Secure Firewall 마이그레이션 툴 트러블슈팅

일반적인 마이그레이션 실패:

- PaloAlto 구성 파일에 알 수 없거나 잘못된 문자가 있습니다.
- 구성 요소가 없거나 불완전합니다.
- 네트워크 연결 문제 또는 레이턴시.
- PaloAlto 컨피그레이션 파일 업로드 중 또는 컨피그레이션을 FMC로 푸시하는 동안 문제가 발생했습니다.

문제 해결을 위해 지원 번들 사용:

- "마이그레이션 완료" 화면에서 지원 버튼을 클릭합니다.
- Support Bundle(지원 번들)을 선택하고 다운로드할 컨피그레이션 파일을 선택합니다.
- 로그 및 DB 파일은 기본적으로 선택됩니다.
- Download(다운로드)를 클릭하여 .zip 파일을 가져옵니다.
- 로그, DB 및 컨피그레이션 파일을 보려면 .zip의 압축을 풉니다.
- Email us(이메일)를 클릭하여 기술 팀에 실패 세부 정보를 보냅니다.
- 이메일에 지원 번들을 첨부합니다.
- TAC 방문 페이지를 클릭하여 지원을 위한 Cisco TAC 케이스를 생성합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.