

Migreer Paloalto naar Firepower Threat Defence met FMT

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht](#)

[Achtergrondinformatie](#)

[Aanvragen PaloAlto Firewall Configuration zip-bestand](#)

[Checklist vóór migratie](#)

[Configureren](#)

[Migratiestappen](#)

[Problemen oplossen](#)

[Problemen oplossen met Secure Firewall-migratietool](#)

[Veelvoorkomende migratieproblemen:](#)

[De ondersteuningsbundel gebruiken voor probleemoplossing:](#)

Inleiding

In dit document wordt de procedure beschreven om Paloalto Firewall te migreren naar Cisco Firepower Threat Device.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower-migratietool
- Paloalto-firewall
- Secure Firewall Threat Defence (FTD)
- Cisco Secure Firewall Management Center (FMC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Mac OS met Firepower Migration Tool (FMT) v7.7
- PAN NGFW versie 8.0+
- Secure Firewall Management Center (FMCv) v7.6
- Secure Firewall Threat Defense versie 7.4.2

Vrijwaring: De netwerken en IP-adressen waarnaar in dit document wordt verwezen, zijn niet gekoppeld aan individuele gebruikers, groepen of organisaties. Deze configuratie is exclusief gemaakt voor gebruik in een laboratoriumomgeving.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Specifieke eisen voor dit document zijn onder meer:

- PAN NGFW versie 8.4+ of hoger
- Secure Firewall Management Center (FMCv) versie 6.2.3 of hoger

De Firewall Migration Tool ondersteunt deze lijst met apparaten:

- Cisco ASA (8,4+)
- Cisco ASA (9.2.2+) met FPS
- Cisco Secure Firewall-apparaatbeheer (7.2+)
- Controlepunt (r75-r77)
- Controlepunt (r80-r81)
- Fortinet (5,0+)
- Palo Alto Networks (8.0+)

Achtergrondinformatie

Voordat u uw Paloalto Firewall configuratie migreert, voer deze activiteiten uit:

Aanvragen PaloAlto Firewall Configuration zip-bestand

- Paloalto Firewall moet versie 8.4+ zijn.
- Exporteer de huidige actieve configuratie vanuit de Palo Alto firewall (*.xml moet in xml Format zijn).
- Log in op de Paloalto Firewall-client om de routebeschrijving te tonen en de output in de txt-indeling op te slaan (*.txt).
- Comprimeer het actieve configuratiebestand (*.xml) en het Routing-bestand (*.txt) met de extensie *.zip.

Checklist vóór migratie

- Ervoor zorgen dat het FTD bij het VCC is geregistreerd voordat het migratieproces begint.
- Er is een nieuwe gebruikersaccount met administratieve rechten aangemaakt op het VCC. Of er kunnen bestaande Admin-referenties worden gebruikt.

- Uitgevoerde Palo Alto lopende configuratie file.xml moet worden gezippt met een extensie van .zip (volg de procedure vermeld in vorige sectie).
- Het FirePOWER-apparaat moet hetzelfde of meer fysieke of subinterface- of poortkanalen hebben in vergelijking met de Paloalto Firewall-interfaces.

Configureren

Migratiestappen

1. Download de meest recente Firepower Migration Tool van Cisco Software Central die compatibel is met uw computer:

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

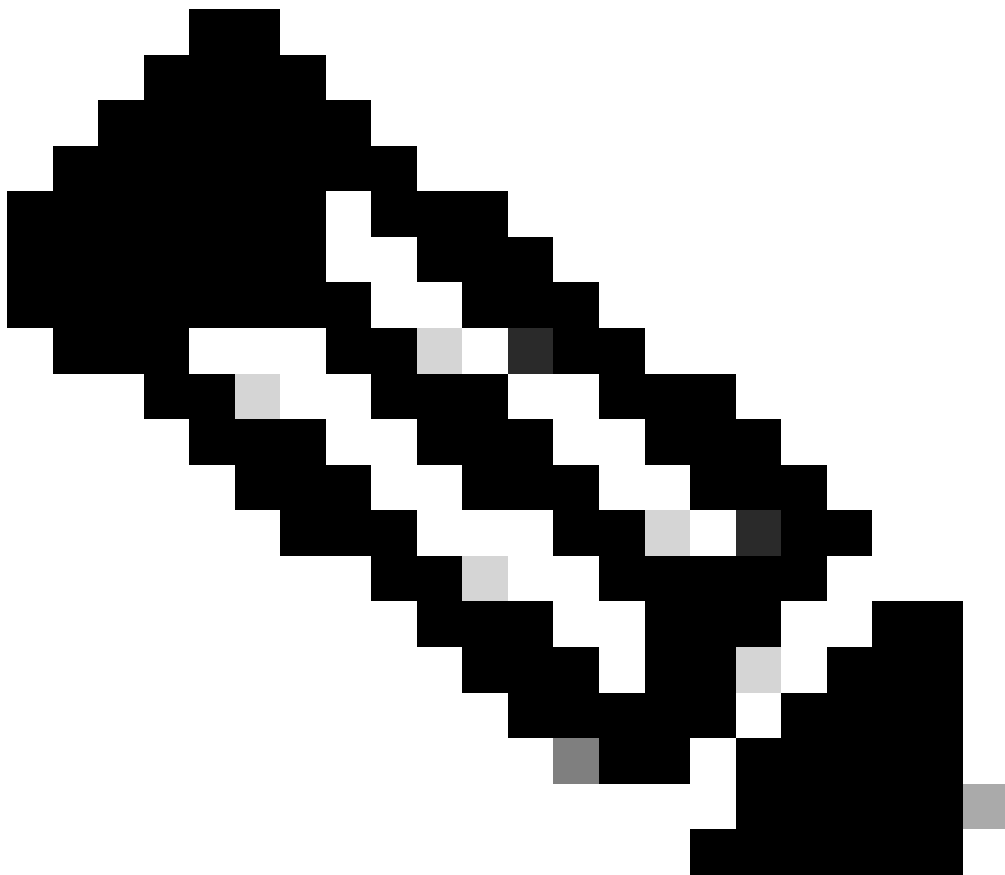
▲ My Notifications

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	Download Add to Cart
Firewall Migration Tool 7.7 for Windows Firewall_Migration_Tool_v7.7-12208.exe Advisories	03-Feb-2025	69.54 MB	Download Add to Cart

FMT-download

3. Open het bestand dat u eerder naar uw computer hebt gedownload.



Opmerking: Het programma wordt automatisch geopend en een console-auto genereert inhoud in de map waarin u het bestand hebt uitgevoerd.

-
4. Nadat u het programma hebt uitgevoerd, opent het een webbrowser die de Gebruiksrechtovereenkomst weergeeft.
 1. Selecteer het aankruisvakje om de voorwaarden te aanvaarden.
 2. Klik op Doorgaan.
 5. Log in met een geldige CCO-referenties om toegang te krijgen tot FMT GUI.

Security Cloud Sign On

Email

Continue

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

Or

[Other login options](#)

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

Aanvraag voor FMT-aanmelding

6. Selecteer de te migreren bronfirewall en klik op Start Migration.

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. De sectie van de Methodes van de extractie wordt nu getoond, waar u het dossier van de Zip configuratie van de Firewall van Paloalto aan FMT moet uploaden.

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

Manual Configuration Upload

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

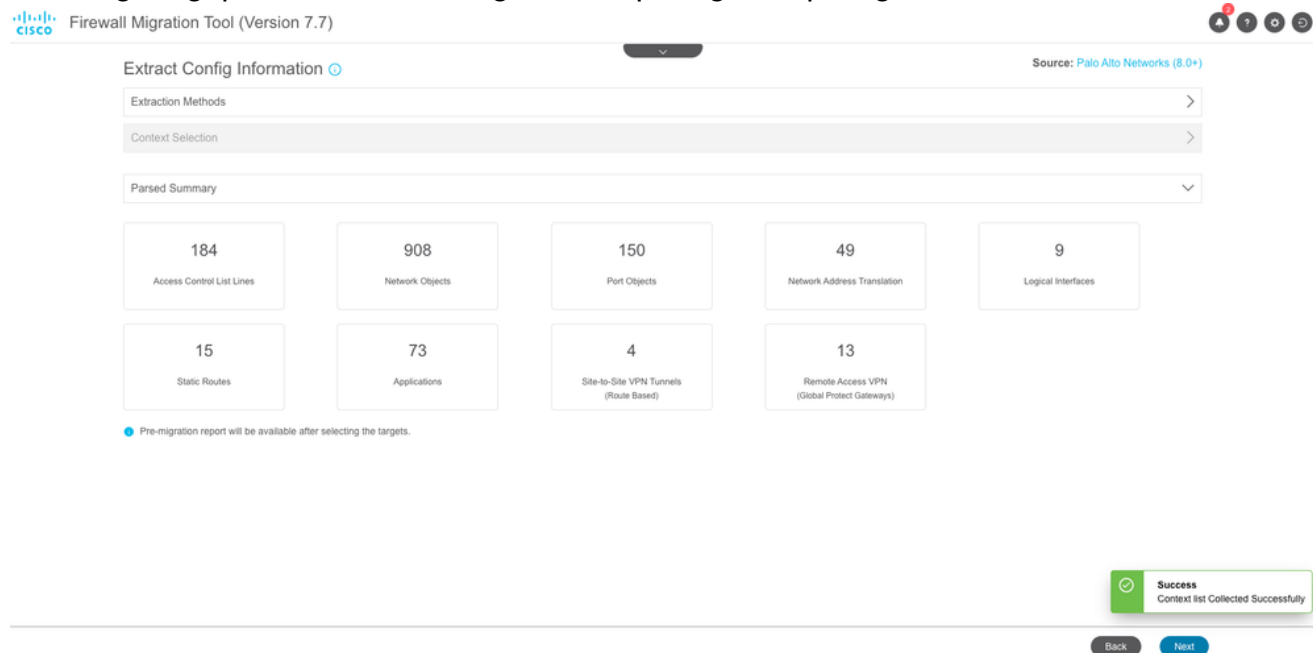
- Zip Config

config.zip

Wizard Configuratie uploaden

8. De geparseerde samenvatting van de Configuratie wordt nu weergegeven nadat het configuratiebestand is geüpload. In het geval van VSYS zijn afzonderlijke VSYS-selecties

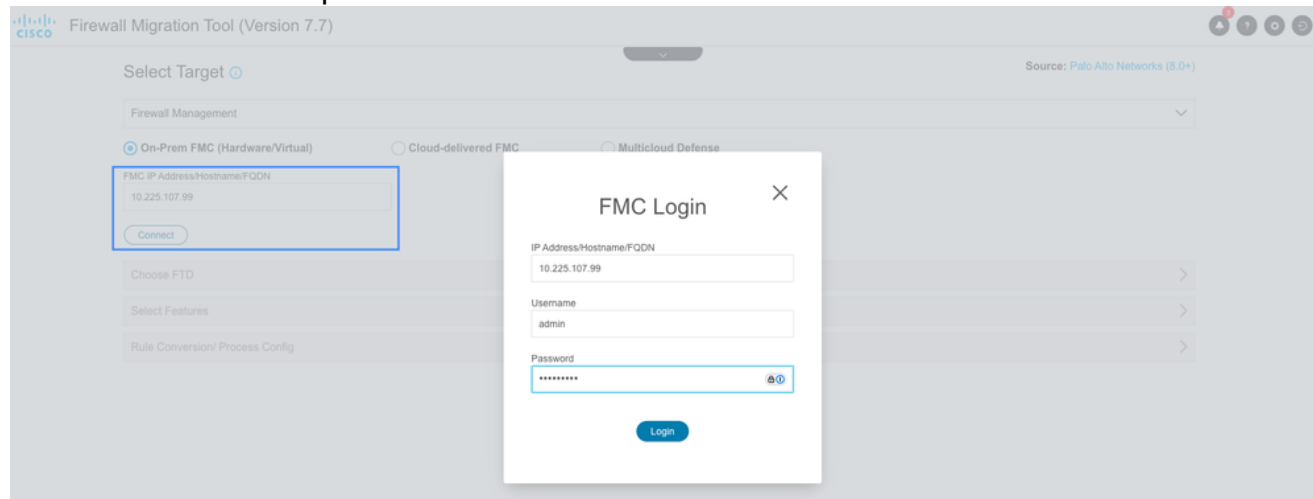
beschikbaar. Elk van hen moet worden geparseerd en de een na de ander migreren. Bevestig de geparseerde samenvatting en klik op Volgende pictogram.



Samenvatting van configuratievalidatie

9. U kunt het type VCC in deze sectie kiezen. Geef het IP-adres voor beheer op en klik op Connect.

Er wordt een pop-up weergegeven waarin wordt gevraagd om FMC-referenties. Voer de referenties in en klik op Aanmelden.



Aanmelden bij FMC

10. Nadat u met succes verbinding hebt gemaakt met FMC, kunt u nu het domein kiezen (indien aanwezig) en op Doorgaan klikken.

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

Domeinselectie

11. Kies het FTD waarnaar u gaat migreren en klik op Doorgaan.

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

Selecteer Doel FTD

12. De tool maakt nu een lijst van de functies die zullen worden gemigreerd. Klik op Doorgaan.

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

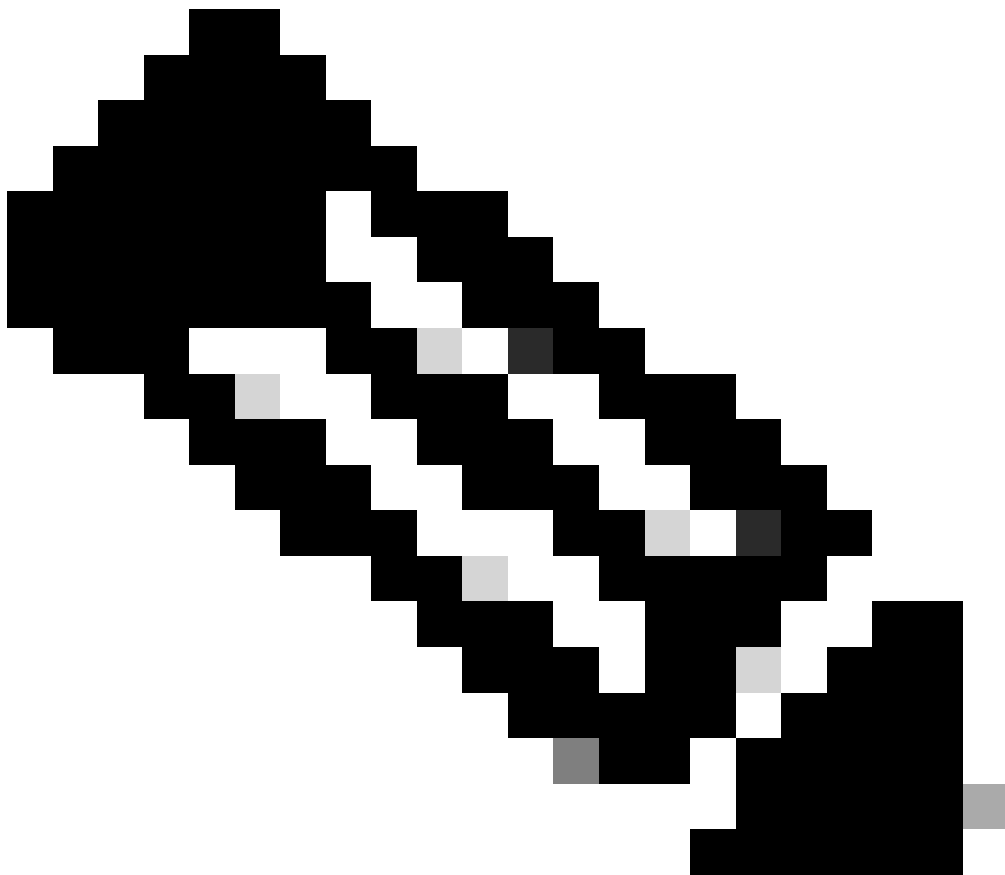
Access Control Options

☒ Discovered Identities

Proceed

Rule Conversion/ Process Config

Functieselectie



Opmerking: Alle functies zijn standaard geselecteerd. U kunt elke configuratie die niet gemigreerd hoeft te worden, deselecteren.

13. Klik op Start Conversion om de configuratie te converteren.



Configuratie parsen

Het gereedschap parseert de configuratie en geeft de conversiesamenvatting weer zoals in de afbeelding. U kunt ook het Pre-Migration Report downloaden voor het valideren van de gemigreerde configuratie voor eventuele fouten of waarschuwingen. Navigeer naar de

volgende pagina door op Volgende te klikken.

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

Back Next

Samenvatting van geparseerde configuratie

14. U kunt Paloalto-FTD-interfacekaarten definiëren en de interfacenaam voor elke interface bewerken in de sectie Interfacekaarten. Klik op Volgende nadat de interfacekaart is voltooid.

Map FTD Interface

Source: Palo Alto Networks (8.0+)

Target FTD: FW1

PAN Interface Name	FTD Interface Name	Mapped Name
ethern12	Select interface	ethern1_2
ethern13	Ethernet1/1	ethern1_3
ethern14	Ethernet1/2	ethern1_4
ethern15	Ethernet1/3	ethern1_5
ethern16	Ethernet1/4	ethern1_6
ethern17	Ethernet1/5	ethern1_7

FTD Interface name can be edited

Mapping of FTD interfaces

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

Back Next

Toewijzing van interfaces

15. U kunt de Security Zone voor elke interface handmatig toevoegen of automatisch maken in Map de Security Zone sectie. Klik op Volgende na het maken en toewijzen van Security Zones.

Map Security Zones

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

PAN Zone Name	FMC Security Zones
G-Inside	Select Security Zone
Outside	Select Security Zone
GPVFN-	Select Security Zone
l-Ins	Select Security Zone
DMZ	Select Security Zone
SC	Select Security Zone
Mel	Select Security Zone
OT-	Select Security Zone
Wireless-	Select Security Zone
l-Inside	Select 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

Security zone maken

Handmatige instelling van beveiligingszones:

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	
	SWITCHED	
	ROUTED	

0 - 0 of 0 |< 1 >|

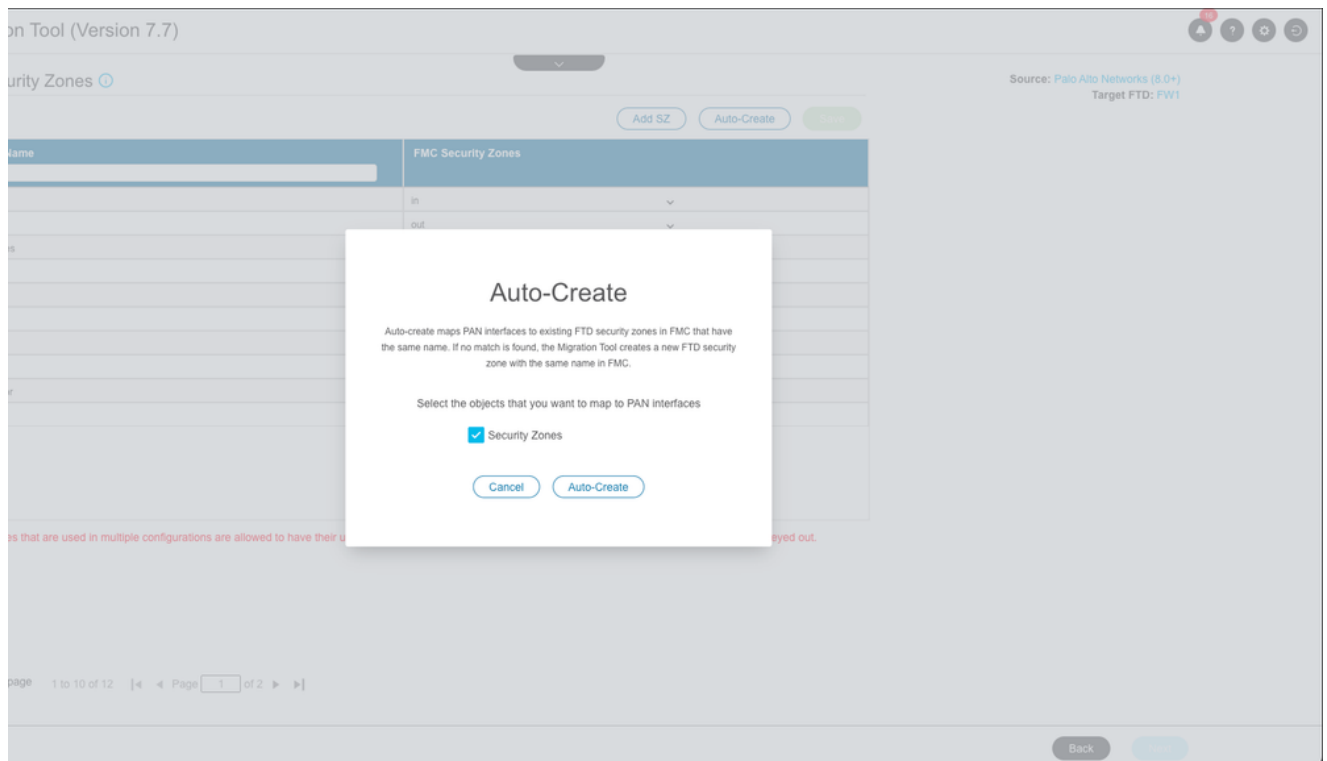
Close

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

Back

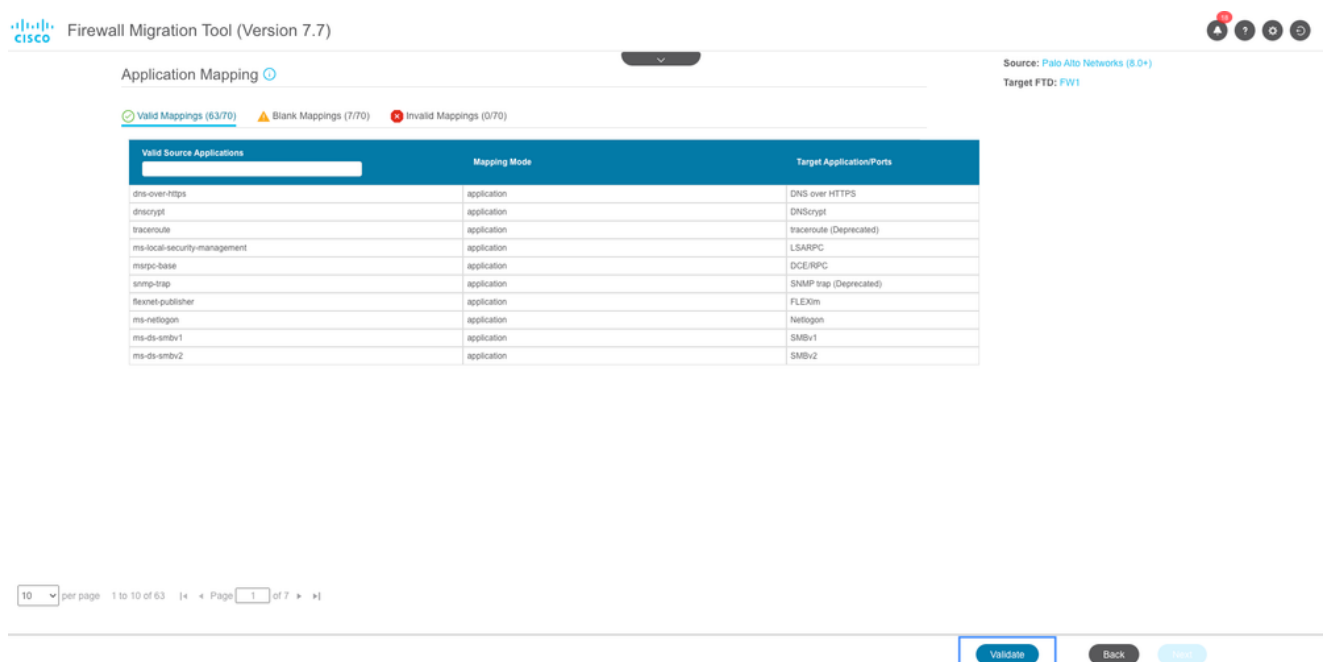
Handmatige security zone maken

Beveiligingszones automatisch maken:



Auto Security Zone maken

- U kunt nu overgaan naar het gedeelte Toewijzing van toepassingen. Klik op de knop Validate om de applicatie-mapping te valideren.



Toewijzing van toepassingen

Firewall Migration Tool (Version 7.7)

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

Validatie van Toewijzing van toepassingen

Na validatie vermeldt FMT de lege en ongeldige toewijzingen. Ongeldige toewijzingen moeten worden gecorrigeerd voordat u verder gaat en blanco toewijzingen zijn optioneel.

Klik nogmaals op Valideren om de gecorrigeerde toewijzingen te valideren. Klik op Volgende nadat de validatie is geslaagd.

Firewall Migration Tool (Version 7.7)

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

Blind en ongeldig Toewijzing van toepassingen

- ACL kan indien nodig in de volgende sectie worden geoptimaliseerd. Herzie de configuratie in elke sectie zoals Toegangsbeheer, Voorwerpen, NAT, Interfaces, Routes, en Verre Toegang VPN. Klik op Validate na het bekijken van de configuraties.

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

SOURCE						DESTINATION						TIME BASED	
#	Name	Zone	Network	Port	User	Zone	Network	Port	Application	URLs	State	Action	Objects
1	Allow Time	Dt	GRP_ADDR...	ANY	ANY			ANY	NTP	NA	✓	Allow	None
2	Allow Time	Dt	ANY	ANY	ANY			ANY	NTP	NA	✓	Allow	None
3	Allow Time	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 traffic	G...	ADDR_10.11...	ANY	ANY			ANY	TCP-443	NA	✓	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	NA	✓	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

Configuratievalidatie

18. Een valideringssamenvatting wordt weergegeven nadat de validering met succes is voltooid. Klik op Push Configuration om de configuratie naar het beoogde VCC te duwen.

Validation Status

Successfully Validated

Validation Summary (Pre-push)

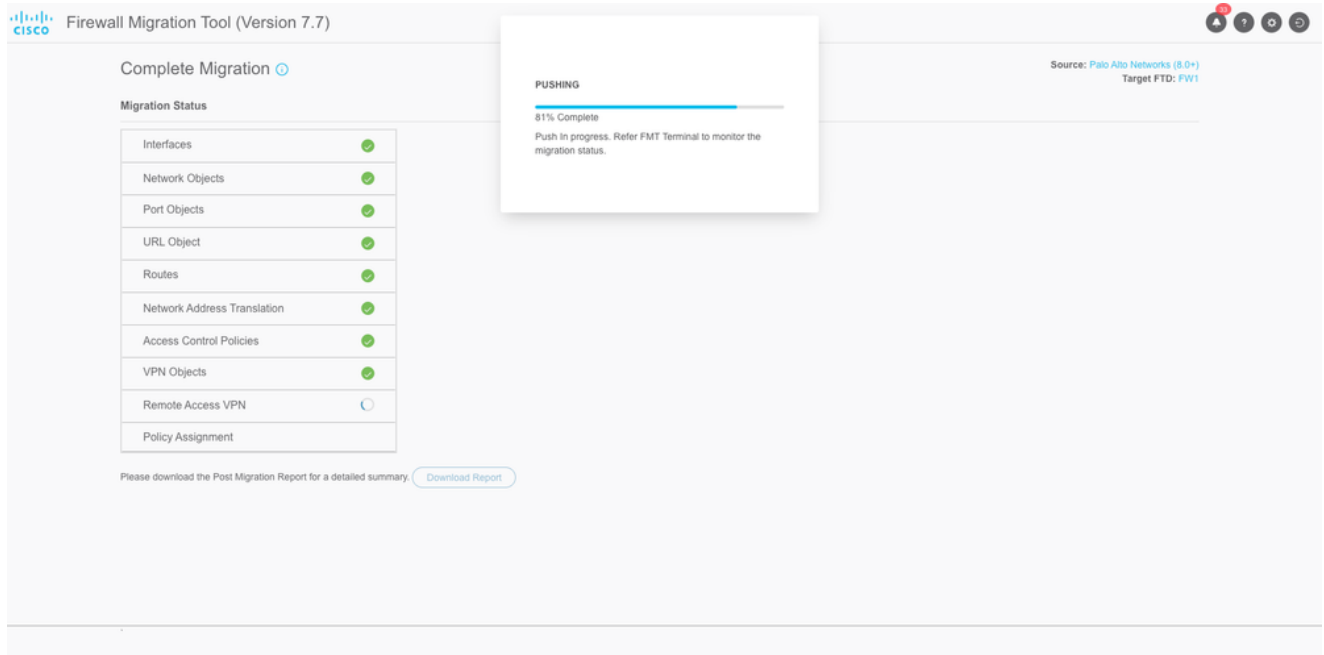
195	752	100	52	8
Access Control List Lines	Network Objects	Port Objects	Network Address Translation	Logical Interfaces
2	0	62	9	
Static Routes	Site-to-Site VPN Tunnels (Route Based)	Applications	Remote Access VPN (Global Protect Gateways)	

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

Push Configuration

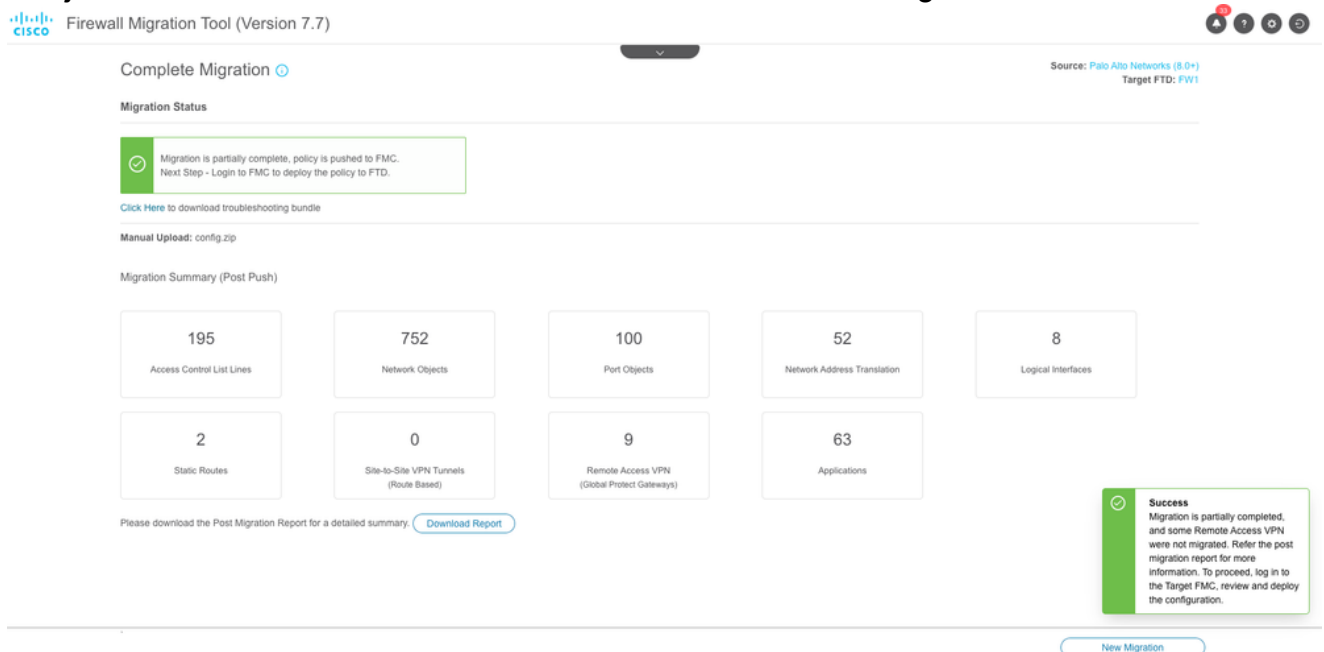
Samenvatting van configuratievalidatie

19. De voortgang van de configuratie van het VCC is nu zichtbaar in de sectie Migratiestatus. U kunt het FMT terminal venster ook gebruiken voor de controle van de migratiestatus.



Migratiestatus

20. Een migratieoverzicht wordt weergegeven door de tool omhoog op succesvolle migratie. Tevens worden eventuele gedeeltelijk gemigreerde configuraties vermeld. Bijvoorbeeld, de configuratie van de Verre toegang VPN in dit scenario toe te schrijven aan het missen Veilig Pakket van de Cliënt.
- U kunt ook het Post Migration Report downloaden om de gemigreerde configuraties te bekijken en om te zien of er fouten of correcties moeten worden gemaakt.



Samenvatting van succesvolle migratie

21. De laatste stap is het bekijken van de gemigreerde configuratie van het VCC en implementeren van de configuratie naar FTD.
- Zo implementeert u de configuratie:
1. Log in op de GUI van het VCC.
 2. Navigeer naar het tabblad Implementatie.

3. Selecteer de implementatie om de configuratie naar de firewall te duwen.
4. Klik op Implementeren.

Problemen oplossen

Problemen oplossen met Secure Firewall-migratietool

Veelvoorkomende migratieproblemen:

- Onbekende of ongeldige tekens in het configuratiebestand van PaloAlto.
- Ontbrekende of onvolledige configuratie-elementen.
- Problemen met netwerkconnectiviteit of latentie.
- Problemen tijdens het uploaden van het configuratiebestand van PaloAlto of tijdens het indrukken van de configuratie in het VCC.

De ondersteuningsbundel gebruiken voor probleemoplossing:

- Klik in het scherm "Complete Migration" op de knop Support.
- Selecteer Ondersteuningsbundel en kies de configuratiebestanden die u wilt downloaden.
- Log- en DB-bestanden worden standaard geselecteerd.
- Klik op Downloaden om een .zip-bestand te krijgen.
- Haal de .zip om logbestanden, DB en configuratiebestanden te bekijken.
- Klik op E-mail ons om storingsgegevens naar het technische team te sturen.
- Bevestig het ondersteuningsbundel in uw e-mail.
- Klik op Bezoek TAC-pagina om een Cisco TAC-case voor ondersteuning te maken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.