

# Migration von Paloalto zu Firepower Threat Defense mit FMT

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Überblick](#)

[Hintergrundinformationen](#)

[Laden Sie die ZIP-Datei für die Paloalto Firewall-Konfiguration herunter.](#)

[Checkliste vor der Migration](#)

[Konfigurieren](#)

[Migrationsschritte](#)

[Fehlerbehebung](#)

[Fehlerbehebung Secure Firewall Migration-Tool](#)

[Häufige Migrationsfehler:](#)

[Verwenden des Support-Pakets zur Fehlerbehebung:](#)

---

## Einleitung

In diesem Dokument wird das Verfahren zur Migration der Paloalto Firewall auf Cisco Firepower Threat Device beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER Migrationstool
- Paloalto Firewall
- Sichere Firewall-Bedrohungsabwehr (FTD)
- Cisco Secure Firewall Management Center (FMC)

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Mac OS mit Firepower Migration Tool (FMT) v7.7
- PAN NGFW Version 8.0+
- Secure Firewall Management Center (FMCv) v7.6

- Secure Firewall Threat Defense Version 7.4.2

Haftungsausschluss: Die in diesem Dokument erwähnten Netzwerke und IP-Adressen sind keinen einzelnen Benutzern, Gruppen oder Organisationen zugeordnet. Diese Konfiguration wurde exklusiv für den Einsatz in einer Laborumgebung erstellt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Überblick

Spezifische Anforderungen für dieses Dokument:

- PAN NGFW ab Version 8.4
- Secure Firewall Management Center (FMCv) Version 6.2.3 oder höher

Das Firewall Migration-Tool unterstützt diese Liste von Geräten:

- Cisco ASA (8,4+)
- Cisco ASA (9.2.2+) mit FPS
- Cisco Secure Firewall Device Manager (7.2+)
- Prüfpunkt (r75-r77)
- Prüfpunkt (r80-r81)
- Fortinet (5,0+)
- Palo Alto Networks (8.0+)

## Hintergrundinformationen

Führen Sie vor der Migration Ihrer Paloalto Firewall-Konfiguration folgende Schritte aus:

Laden Sie die ZIP-Datei für die Palalto Firewall-Konfiguration herunter.

- Paloalto Firewall muss Version 8.4+ sein.
- Exportieren Sie die aktuelle Konfiguration von der Palo Alto Firewall (\*.xml muss im XML-Format vorliegen).
- Melden Sie sich bei der Paloalto Firewall-CLI an, um die Show-Routing-Route auszuführen und die Ausgabe im TXT-Format (\*.txt) zu speichern.
- Komprimieren Sie die aktuelle Konfigurationsdatei (\*.xml) und die Routing-Datei (\*.txt) mit der Erweiterung \*.zip.

Checkliste vor der Migration

- Stellen Sie sicher, dass die FTD beim FMC registriert wurde, bevor Sie mit der Migration

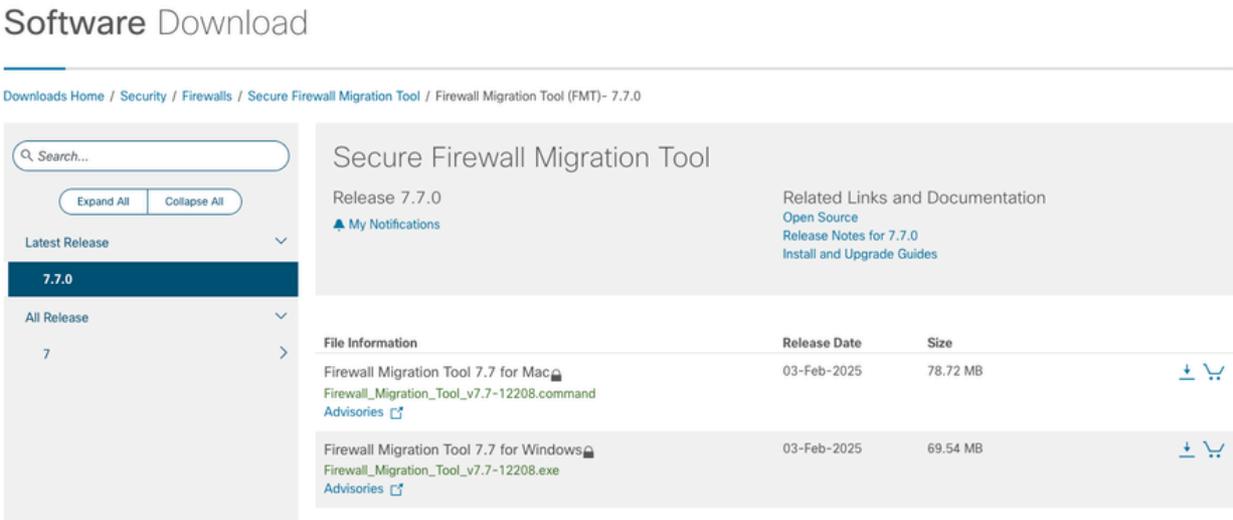
beginnen.

- Auf dem FMC wurde ein neues Benutzerkonto mit Administratorberechtigungen erstellt. Sie können auch vorhandene Admin-Anmeldedaten verwenden.
- Exportierte Palo Alto-Konfigurationsdatei.xml muss mit der Erweiterung .zip gezippt werden (befolgen Sie die Prozedur, die im vorherigen Abschnitt erwähnt wurde).
- Das FirePOWER-Gerät muss im Vergleich zu den Paloalto Firewall-Schnittstellen die gleiche oder eine größere Anzahl von physischen Schnittstellen oder Subschnittstellen bzw. Port-Kanälen aufweisen.

## Konfigurieren

### Migrationsschritte

1. Laden Sie das neueste Firepower Migration Tool von Cisco Software Central herunter, das mit Ihrem Computer kompatibel ist:



The screenshot shows the Cisco Software Central download page for the Secure Firewall Migration Tool (FMT) 7.7.0. The page includes a search bar, navigation links, and a table of available files for Mac and Windows.

Software Download

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

Search...  
Expand All Collapse All

Latest Release  
7.7.0  
All Release  
7

### Secure Firewall Migration Tool

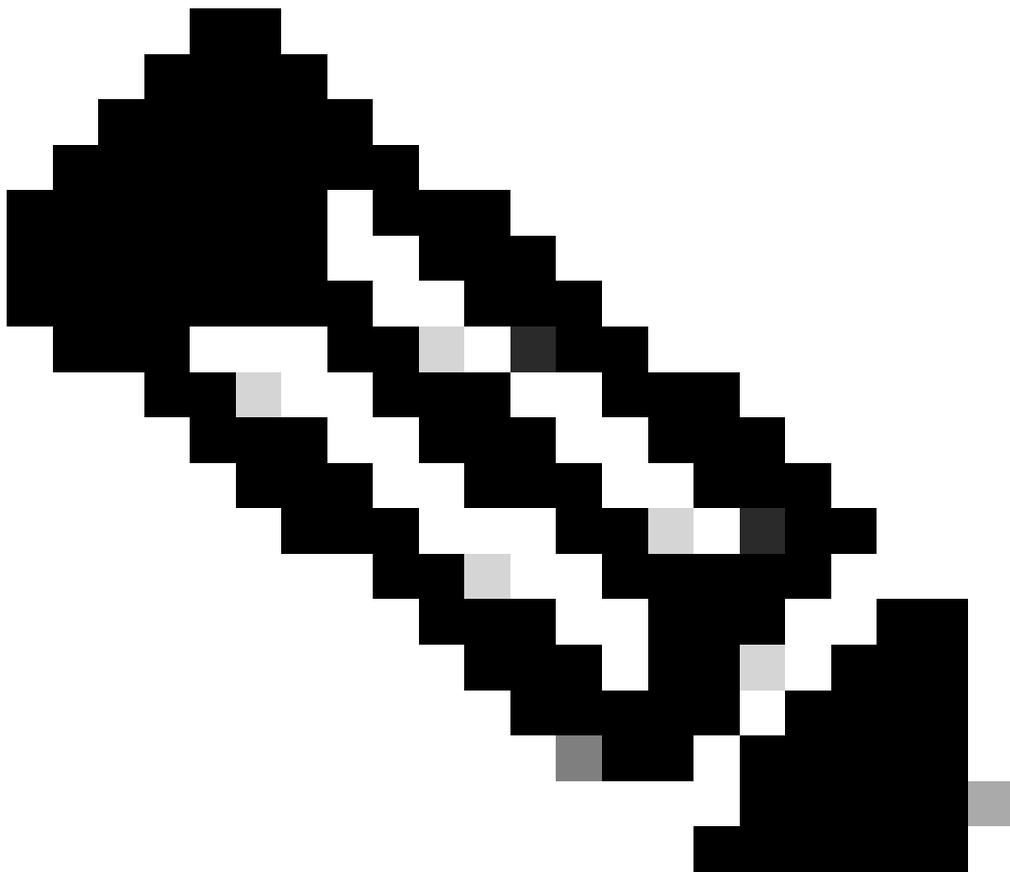
Release 7.7.0  
My Notifications

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

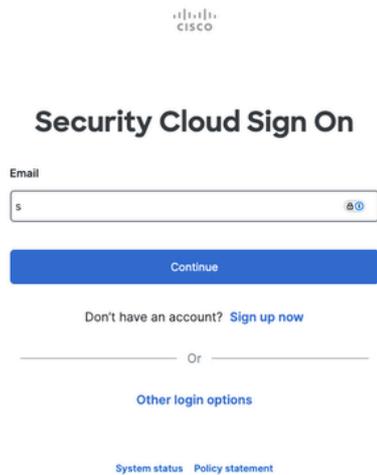
FMT-Download

3. Öffnen Sie die zuvor auf Ihren Computer heruntergeladene Datei.



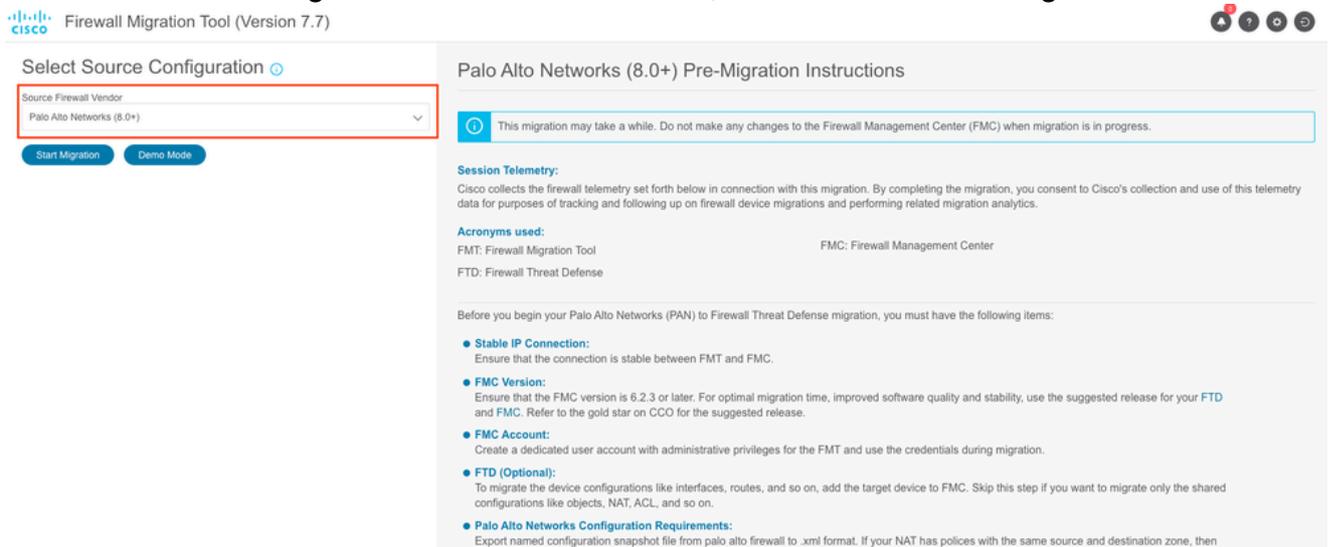
Anmerkung: Das Programm wird automatisch geöffnet, und eine Konsole generiert automatisch Inhalte für das Verzeichnis, in dem Sie die Datei ausgeführt haben.

- 
4. Nach dem Ausführen des Programms wird ein Webbrowser geöffnet, in dem die Endbenutzer-Lizenzvereinbarung angezeigt wird.
    1. Aktivieren Sie das Kontrollkästchen, um die Geschäftsbedingungen zu akzeptieren.
    2. Klicken Sie auf Fortfahren.
  5. Melden Sie sich mit gültigen CCO-Anmeldeinformationen an, um auf die FMT-GUI zuzugreifen.



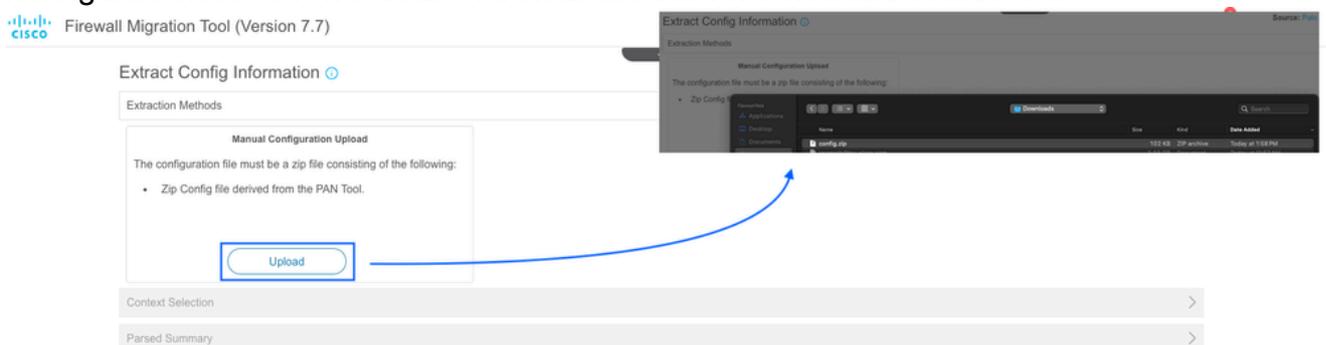
FMT-Anmeldeaufforderung

6. Wählen Sie die zu migrierende Quell-Firewall aus, und klicken Sie auf Migration starten.



FMT-GUI

7. Der Abschnitt "Extraction Methods" wird nun angezeigt, in dem Sie die Zip-Konfigurationsdatei von Paloalto Firewall auf das FMT hochladen müssen.



Assistent zum Hochladen von Konfigurationen

8. Die Zusammenfassung der analysierten Konfiguration wird jetzt angezeigt, nachdem die Konfigurationsdatei hochgeladen wurde. Im Fall von VSYS stehen separate VSYS-Optionen

zur Verfügung. Jeder von ihnen muss analysiert und nacheinander migriert werden. Validieren Sie die analysierte Zusammenfassung, und klicken Sie auf das Symbol Weiter.

Firewall Migration Tool (Version 7.7) Source: Palo Alto Networks (8.0+)

Extract Config Information

Extraction Methods

Context Selection

Parsed Summary

184 Access Control List Lines	908 Network Objects	150 Port Objects	49 Network Address Translation	9 Logical Interfaces
15 Static Routes	73 Applications	4 Site-to-Site VPN Tunnels (Route Based)	13 Remote Access VPN (Global Protect Gateways)	

Pre-migration report will be available after selecting the targets.

Success  
Context list Collected Successfully

Back Next

Zusammenfassung der Konfigurationsvalidierung

9. In diesem Abschnitt können Sie den Typ des FMC auswählen. Geben Sie die Management-IP-Adresse an, und klicken Sie auf Verbinden.

Es wird ein Popup mit der Aufforderung zur Eingabe der FMC-Anmeldeinformationen angezeigt. Geben Sie die Anmeldeinformationen ein, und klicken Sie auf Anmelden.

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  
Connect

Choose FTD

Select Features

Rule Conversion/ Process Config

FMC Login

IP Address/Hostname/FQDN  
10.225.107.99

Username  
admin

Password  
\*\*\*\*\*

Login

FMC-Anmeldung

10. Nach erfolgreicher Verbindung mit FMC können Sie jetzt die Domäne auswählen (falls vorhanden) und auf Proceed (Weiter) klicken.

Select Target ⊙ Source: Palo Alto Networks (8.0+)

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

Domänenauswahl

11. Wählen Sie das FTD aus, zu dem Sie migrieren möchten, und klicken Sie auf Proceed (Fortfahren).

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 ⌵

Select FTD Device
  Proceed without FTD

FW1 (10.105.209.80) - NA (R) ⌵

Proceed

Select Features ⌵

Rule Conversion/ Process Config ⌵

Ziel-FTD auswählen

12. Das Tool listet nun die Funktionen auf, die migriert werden sollen. Klicken Sie auf Fortfahren.

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

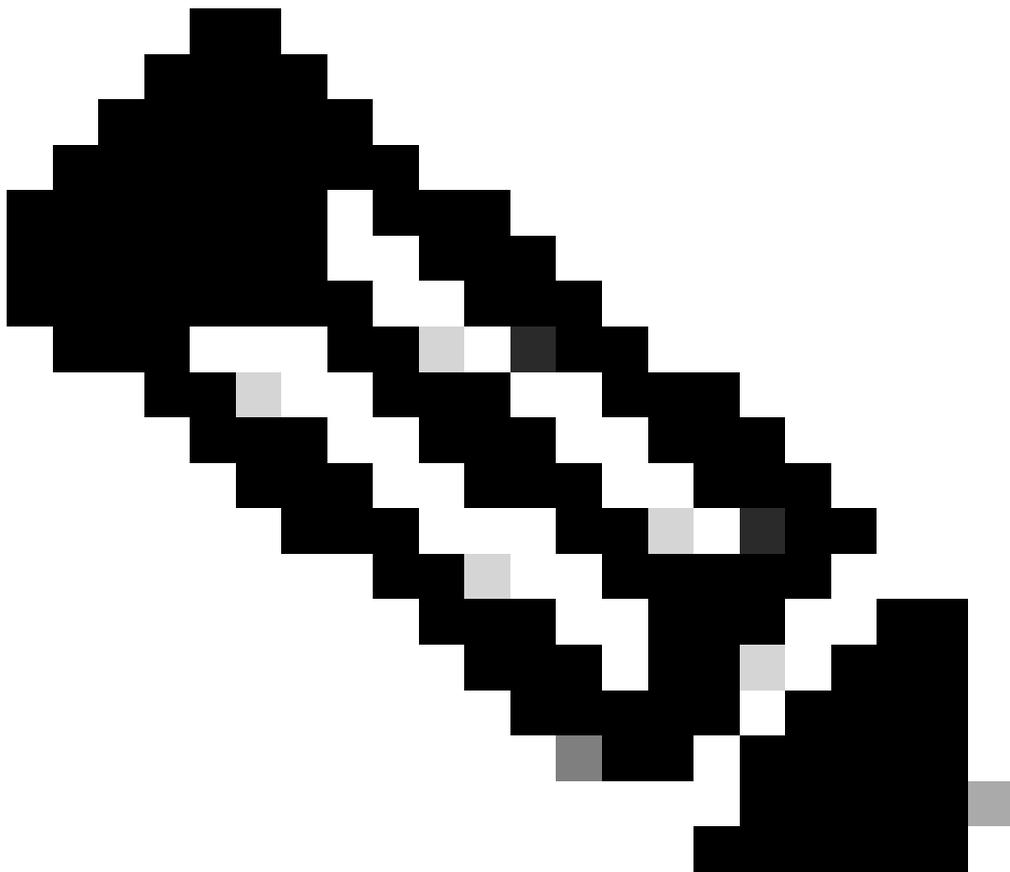
Select Features ⌵

<b>Device Configuration</b> <input checked="" type="checkbox"/> Interfaces <input checked="" type="checkbox"/> Routes <input checked="" type="checkbox"/> Site-to-Site VPN Tunnels <input type="checkbox"/> Policy Based (Unsupported) <span>⊙</span> <input checked="" type="checkbox"/> Route Based (VTI)	<b>Shared Configuration</b> <input checked="" type="checkbox"/> Access Control <input type="checkbox"/> Migrate policies with Application-default as Enabled <span>⊙</span> <input checked="" type="checkbox"/> Network Objects <input checked="" type="checkbox"/> Port Objects <input checked="" type="checkbox"/> Remote Access VPN	<b>Advanced Configuration</b> <b>Optimization</b> <input checked="" type="checkbox"/> Migrate Only Referenced Objects <b>Access Control Options</b> <input checked="" type="checkbox"/> Discovered Identities <span>⌵</span> <span>⊙</span>
--	---	---

Proceed

Rule Conversion/ Process Config ⌵

Funktionsauswahl



Anmerkung: Alle Funktionen sind standardmäßig ausgewählt. Sie können jede Konfiguration deaktivieren, die nicht migriert werden soll.

13. Klicken Sie auf Konvertierung starten, um die Konfiguration zu konvertieren.



Parsing-Konfiguration

Das Tool analysiert die Konfiguration und zeigt die Konvertierungsübersicht an, wie im Bild dargestellt. Sie können auch den Bericht zur Vormigration herunterladen, um die migrierte Konfiguration auf Fehler oder Warnungen zu überprüfen. Navigieren Sie zur nächsten Seite,

indem Sie auf Weiter klicken.

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

Zusammenfassung der analysierten Konfiguration

14. Im Schnittstellenzuordnungsabschnitt können Sie die Schnittstellenzuordnung von Paloalto zu FTD sowie den Schnittstellennamen für jede Schnittstelle bearbeiten. Klicken Sie nach Abschluss der Schnittstellenzuordnung auf Weiter.

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

Target FTD: FW1

PAN Interface Name	FTD Interface Name	Mapped Name
ethemet12	Select Interface	ethemet1_2
ethemet13	✓ Ethernet11	ethemet1_3
ethemet14	Ethernet110	ethemet1_4
ethemet15	Ethernet111	ethemet1_5
ethemet16	Ethernet112	ethemet1_6
ethemet17	Ethernet113	ethemet1_7
	Ethernet114	
	Ethernet115	
	Ethernet116	
	Ethernet117	
	Ethernet118	
	Ethernet119	

FTD Interface name can be edited

Mapping of FTD interfaces

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

Back Next

Schnittstellenzuordnung

15. Sie können die Sicherheitszone entweder manuell für jede Schnittstelle hinzufügen oder sie im Abschnitt Sicherheitszone zuordnen automatisch erstellen. Klicken Sie nach dem Erstellen und Zuordnen von Sicherheitszonen auf Weiter.

Map Security Zones

PAN Zone Name	FMC Security Zones
G...-inside	Select Security Zone
Outside	Select Security Zone
GP/PA-	Select Security Zone
Line	Select Security Zone
DMZ	Select Security Zone
C	Select Security Zone
Mel	Select Security Zone
OT-	Select Security Zone
Wireless-	Select Security Zone
...-inside	Select Security Zone

Add SZ Auto-Create Save

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

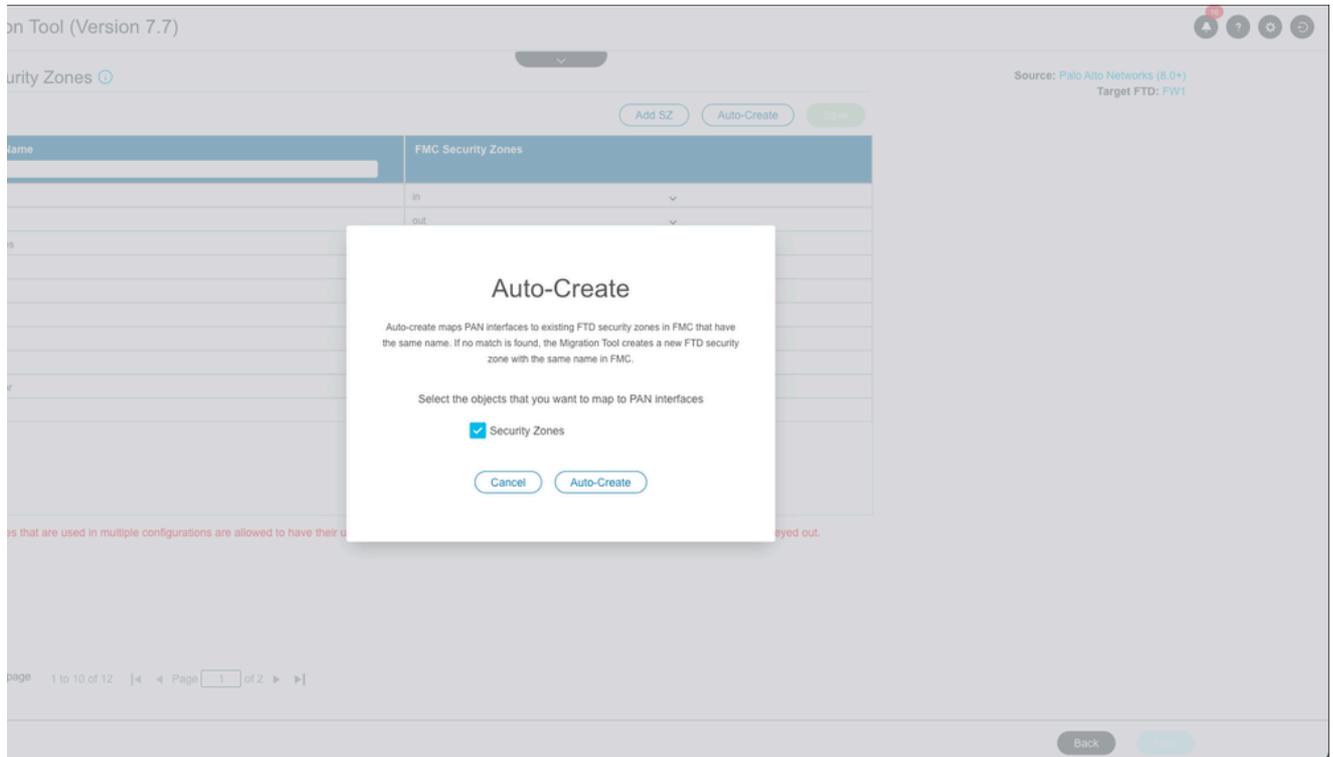
Back Next

Erstellung von Sicherheitszonen

Manuelle Erstellung von Sicherheitszonen:

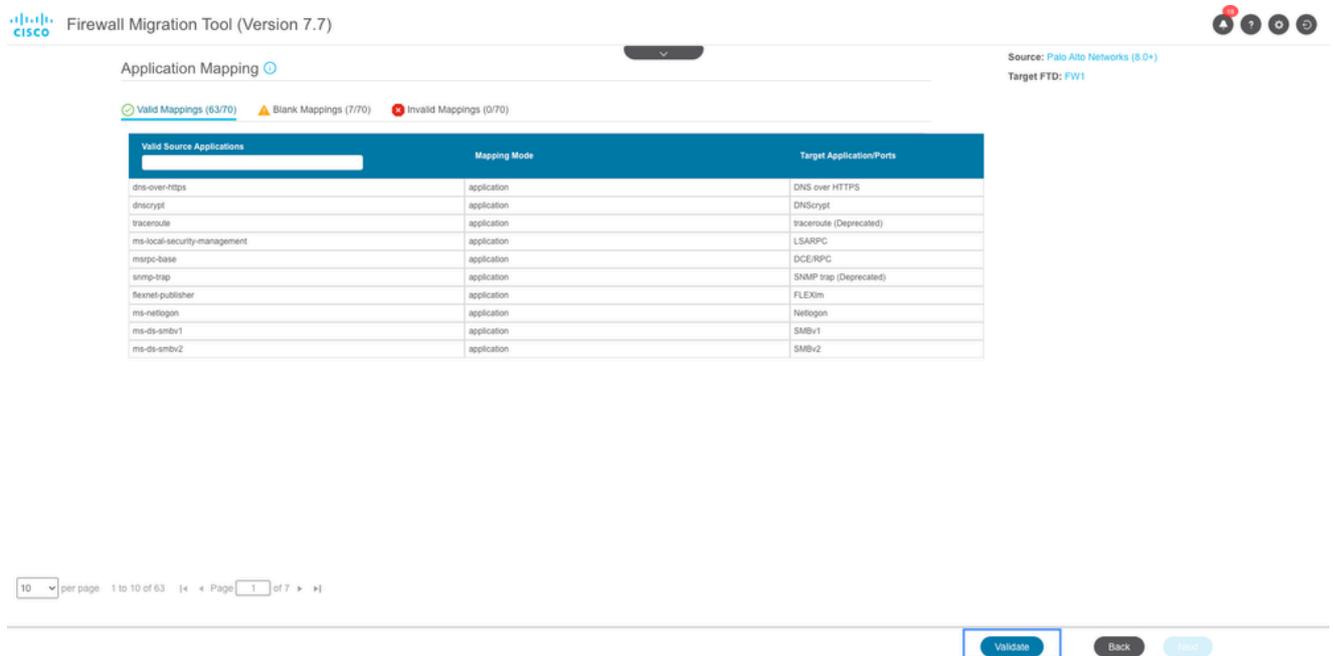
Manuelle Erstellung von Sicherheitszonen

Automatisches Erstellen von Sicherheitszonen:



Erstellung automatischer Sicherheitszonen

16. Sie können nun zum Abschnitt "Anwendungszuordnung" wechseln. Klicken Sie auf Validieren, um die Anwendungszuordnung zu validieren.



Anwendungszuordnung

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-securitymanagement	application	LSARPC
mrgc-base	application	DCE/RPC
snmp-trap	application	SNMP trap (Deprecated)
flexnet-publisher	application	FLEXim
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

Validierung der Anwendungszuordnung

Nach der Validierung listet FMT die leeren und ungültigen Zuordnungen auf. Ungültige Zuordnungen müssen korrigiert werden, bevor Sie fortfahren. Das Korrigieren von leeren Zuordnungen ist optional.

Klicken Sie erneut auf Validieren, um die korrigierten Zuordnungen zu validieren. Klicken Sie nach der erfolgreichen Validierung auf Weiter.

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

Leere und ungültige Anwendungszuordnung

- Die ACL kann bei Bedarf im nächsten Abschnitt optimiert werden. Überprüfen Sie die Konfiguration in den einzelnen Abschnitten, z. B. Zugriffskontrolle, Objekte, NAT, Schnittstellen, Routen und RAS-VPN. Klicken Sie nach dem Überprüfen der Konfigurationen auf Validieren.

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

Select all 195 entries Selected: 0 / 195

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

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

Optimize access control list and validate

Optimize ACL Validate

Validierung der Konfiguration

18. Nachdem die Validierung erfolgreich abgeschlossen wurde, wird eine Validierungsübersicht angezeigt. Klicken Sie auf Push Configuration, um die Konfiguration an das Ziel-FMC weiterzuleiten.

Validation Status

Successfully Validated

Validation Summary (Pre-push)

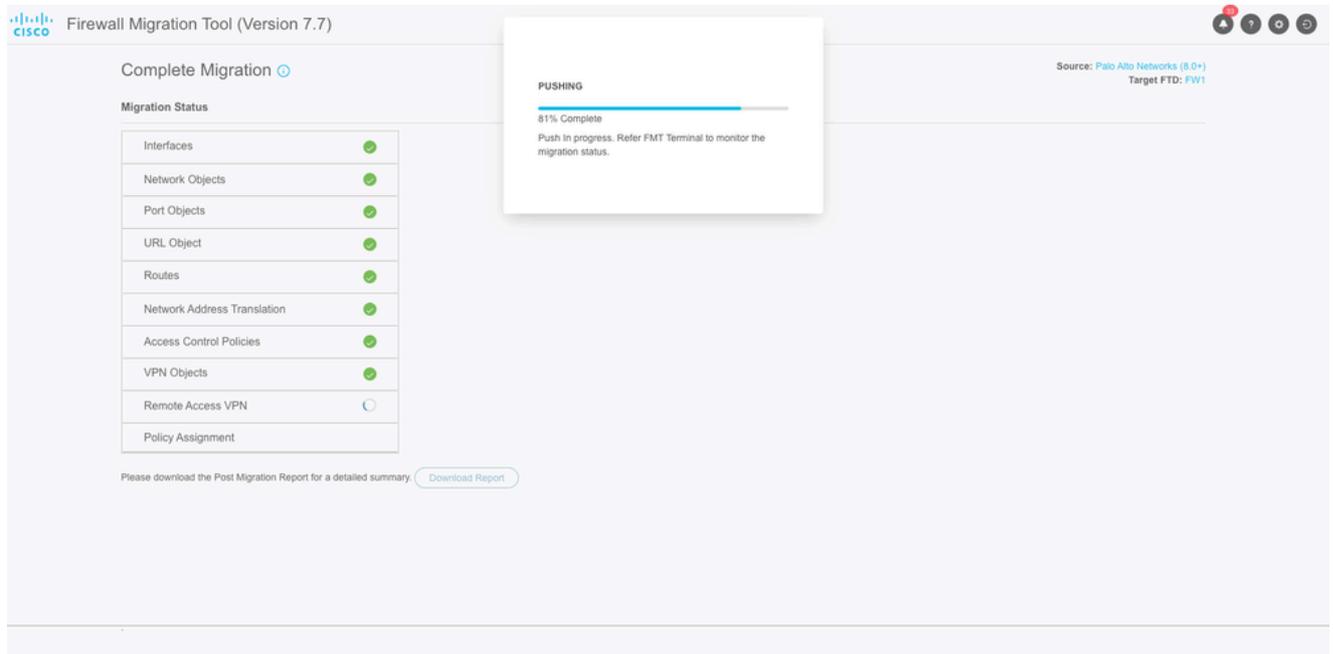
195	752	100	52	8
Access Control List Lines	Network Objects	Port Objects	Network Address Translation	Logical Interfaces
2	0	62	9	
Static Routes	Site-to-Site VPN Tunnels (Route Based)	Applications	Remote Access VPN (Global Protect Gateways)	

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

Push Configuration

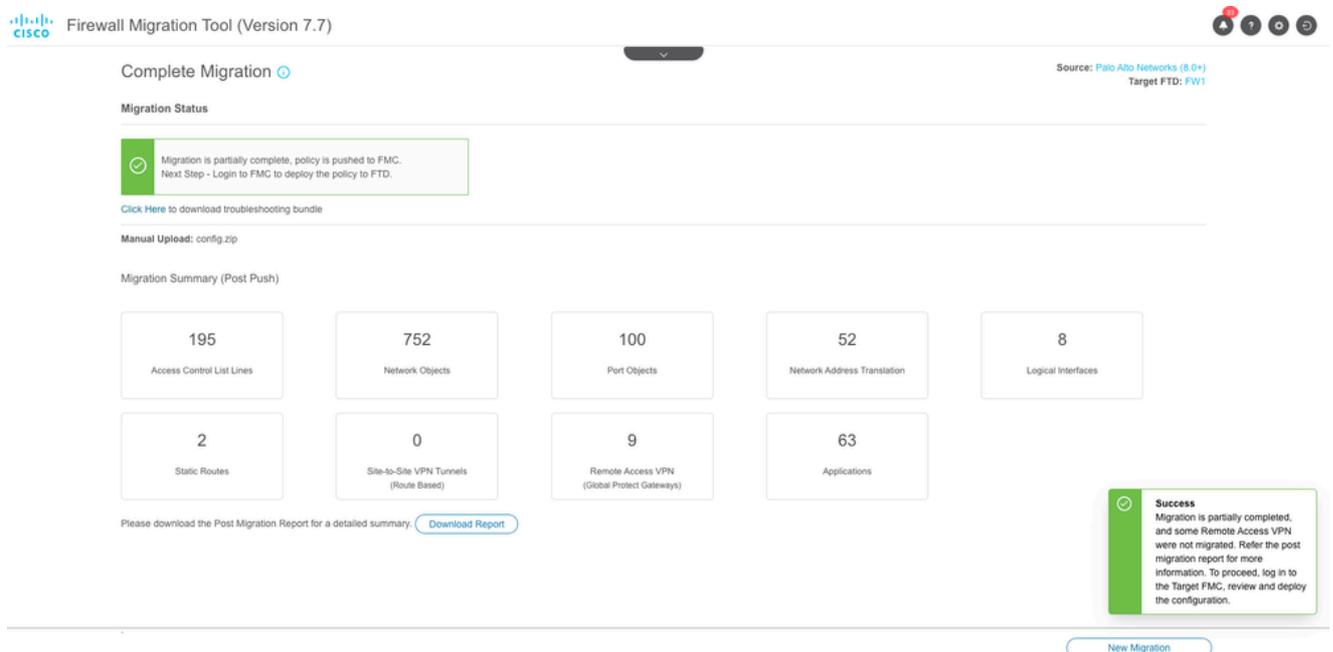
Zusammenfassung der Konfigurationsvalidierung

19. Der Fortschritt des Konfigurations-Pushvorgangs an FMC wird jetzt im Abschnitt "Migrationsstatus" angezeigt. Sie können das FMT-Terminalfenster auch zur Überwachung des Migrationsstatus verwenden.



## Migrationsstatus

20. Nach erfolgreicher Migration zeigt das Tool eine Migrationsübersicht an. Es werden auch teilweise migrierte Konfigurationen aufgeführt, falls vorhanden. Beispiel: Konfiguration des Remotezugriff-VPN in diesem Szenario aufgrund eines fehlenden Secure Client Package. Sie können auch den Bericht nach der Migration herunterladen, um die migrierten Konfigurationen zu überprüfen und festzustellen, ob Fehler oder Korrekturen erforderlich sind.



## Zusammenfassung der erfolgreichen Migration

21. Der letzte Schritt besteht darin, die migrierte Konfiguration von FMC zu überprüfen und die Konfiguration auf FTD bereitzustellen.
- So stellen Sie die Konfiguration bereit:
1. Melden Sie sich an der FMC-GUI an.
  2. Navigieren Sie zur Registerkarte Bereitstellen.

3. Wählen Sie die Bereitstellung aus, um die Konfiguration per Push an die Firewall weiterzuleiten.
4. Klicken Sie auf Bereitstellen.

## Fehlerbehebung

### Fehlerbehebung Secure Firewall Migration-Tool

Häufige Migrationsfehler:

- Unbekannte oder ungültige Zeichen in der PaloAlto-Konfigurationsdatei.
- Fehlende oder unvollständige Konfigurationselemente.
- Probleme mit der Netzwerkverbindung oder Latenz.
- Probleme beim Hochladen der PaloAlto-Konfigurationsdatei oder beim Übertragen der Konfiguration an das FMC.

Verwenden des Support-Pakets zur Fehlerbehebung:

- Klicken Sie im Bildschirm "Complete Migration" (Migration abschließen) auf die Schaltfläche Support.
- Wählen Sie Support Bundle und die herunterzuladenden Konfigurationsdateien aus.
- Protokoll- und DB-Dateien sind standardmäßig ausgewählt.
- Klicken Sie auf Herunterladen, um eine ZIP-Datei herunterzuladen.
- Extrahieren Sie die ZIP-Datei, um Protokolle, DB- und Konfigurationsdateien anzuzeigen.
- Klicken Sie auf Uns per E-Mail kontaktieren, um Fehlerdetails an das technische Team zu senden.
- Hängen Sie das Support-Paket an Ihre E-Mail an.
- Klicken Sie auf die Seite "TAC aufrufen", um ein Cisco TAC-Ticket zu erstellen.

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.