

Migrazione da Paloalto a Firepower Threat Defense tramite FMT

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica](#)

[Premesse](#)

[Ottenere il file zip di configurazione del firewall di Paloalto](#)

[Elenco di controllo pre-migrazione](#)

[Configurazione](#)

[Fasi della migrazione](#)

[Risoluzione dei problemi](#)

[Strumento di risoluzione dei problemi di migrazione Secure Firewall](#)

[Errori comuni di migrazione:](#)

[Utilizzo del pacchetto di supporto per la risoluzione dei problemi:](#)

Introduzione

In questo documento viene descritta la procedura per eseguire la migrazione da Paloalto Firewall a Cisco Firepower Threat Device.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Strumento di migrazione Firepower
- Firewall Paloalto
- Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Management Center (FMC)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

- Secure Firewall Threat Defense versione 7.4.2

Avvertenza: Le reti e gli indirizzi IP menzionati in questo documento non sono associati a singoli utenti, gruppi o organizzazioni. Questa configurazione è stata creata esclusivamente per l'uso in ambienti lab.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

I requisiti specifici per questo documento includono:

- PAN NGFW versione 8.4+ o successive
- Secure Firewall Management Center (FMCv) versione 6.2.3 o successiva

Lo strumento di migrazione del firewall supporta questo elenco di dispositivi:

- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) con FPS
- Cisco Secure Firewall Device Manager (7.2+)
- Punto di controllo (r75-r77)
- Punto di controllo (r80-r81)
- Fortinet (5.0+)
- Palo Alto Networks (8.0+)

Premesse

Prima di eseguire la migrazione della configurazione di Paloalto Firewall, eseguire le attività seguenti:

Ottenere il file zip di configurazione del firewall di Paloalto

- Paloalto Firewall deve essere versione 8.4+.
- Esporta la configurazione corrente dal firewall di Palo Alto (*.xml deve essere in formato xml).
- Accedere alla Cli di Paloalto Firewall per eseguire il comando show routing route e salvare l'output in formato testo (*.txt).
- Comprimere il file di configurazione in esecuzione (*.xml) e il file di routing (*.txt) con estensione *.zip.

Elenco di controllo pre-migrazione

- Accertarsi che l'FTD sia stato registrato nel CCP prima di iniziare il processo di migrazione.
- È stato creato un nuovo account utente con privilegi amministrativi nel CCP. Oppure è possibile utilizzare le credenziali di amministratore esistenti.
- Il file di configurazione .xml di Palo Alto esportato deve essere compresso con estensione .zip (seguire la procedura descritta nella sezione precedente).
- Il dispositivo Firepower deve avere lo stesso numero o più di interfacce fisiche o secondarie o di canali di porta rispetto alle interfacce Firewall di Paloalto.

Configurazione

Fasi della migrazione

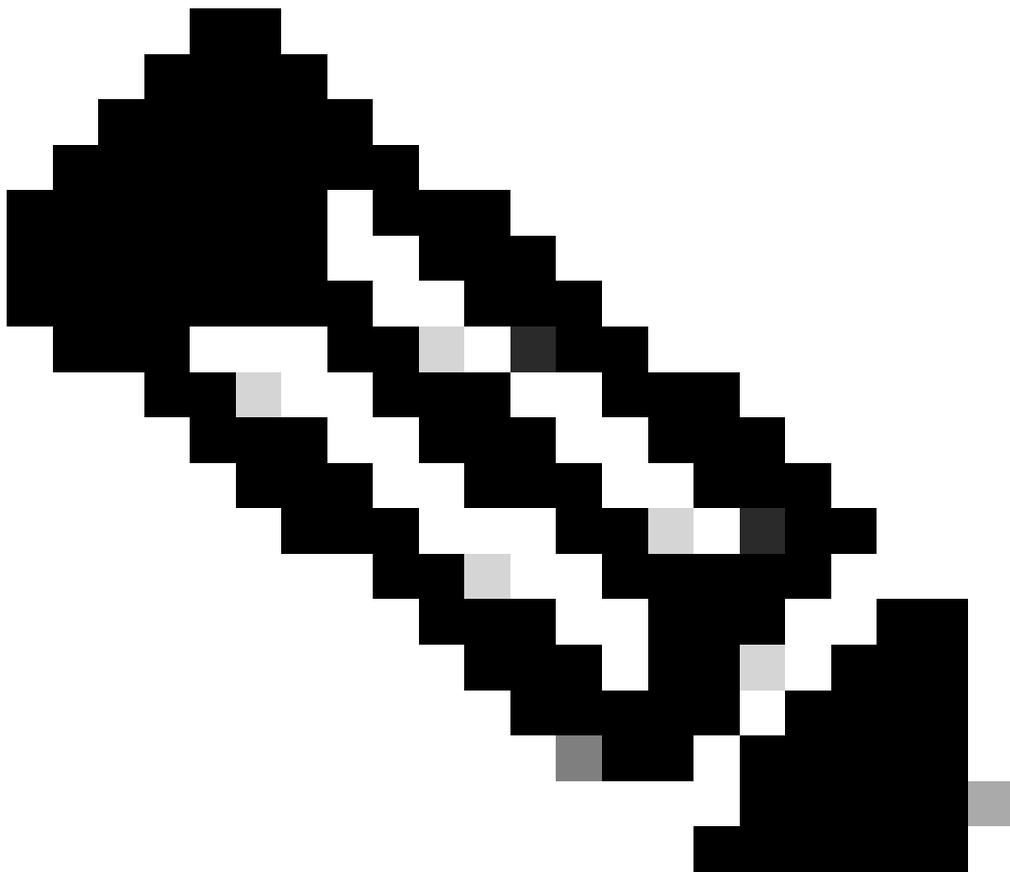
1. Scaricare lo strumento di migrazione Firepower più recente da Cisco Software Central compatibile con il computer:

The screenshot shows the Cisco Software Central interface for downloading the Secure Firewall Migration Tool (FMT) version 7.7.0. The page includes a search bar, navigation links, and a table of file information.

| 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 | ↓ 🛒 |

Download FMT

3. Aprire il file precedentemente scaricato sul computer.



Nota: Il programma si apre automaticamente e una console genera automaticamente il contenuto nella directory in cui è stato eseguito il file.

-
4. Dopo l'esecuzione del programma, viene aperto un browser Web che visualizza il Contratto di Licenza con l'utente finale.
 1. Selezionare la casella di controllo per accettare termini e condizioni.
 2. Fare clic su Procedi.
 5. Eseguire l'accesso con credenziali CCO valide per accedere all'interfaccia utente di FMT.



Security Cloud Sign On

Email

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

Or

[Other login options](#)

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

Prompt di accesso FMT

6. Selezionare il firewall di origine di cui eseguire la migrazione e fare clic su Avvia migrazione.

Firewall Migration Tool (Version 7.7)

Select Source Configuration

Source Firewall Vendor
Palo Alto Networks (8.0+)

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

GUI FMT

7. Viene visualizzata la sezione Metodi di estrazione, in cui è necessario caricare il file di configurazione Zip da Paloalto Firewall all'FMT.

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.

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

Caricamento guidato della configurazione

8. Il riepilogo della configurazione analizzata viene visualizzato dopo il caricamento del file di configurazione. Nel caso di VSYS, sono disponibili selezioni VSYS separate. Ciascuno di

essi deve essere analizzato e migrato in successione.
Convalidare il riepilogo analizzato e fare clic su Icona Successivo.

Extract Config Information Source: Palo Alto Networks (8.0+)

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

Riepilogo della convalida della configurazione

- In questa sezione è possibile scegliere il tipo di FMC. Fornire il proprio indirizzo IP di gestione e fare clic su Connect (Connetti). Viene visualizzato un popup in cui viene richiesto di fornire le credenziali FMC. Immettere le credenziali e fare clic su Login.

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
Connect

Choose FTD

Select Features >

Rule Conversion/ Process Config >

FMC Login

IP Address/Hostname/FQDN
10.225.107.99

Username
admin

Password

Login

Accesso a FMC

- Una volta completata la connessione a FMC, è possibile scegliere il dominio (se presente) e fare clic su Continua.

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

Selezione dominio

11. Scegliere l'FTD in cui si desidera eseguire la migrazione e fare clic su Continua.

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 ➤

Seleziona FTD di destinazione

12. Lo strumento ora elenca le funzionalità che verranno migrate. Fare clic su Continua.

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

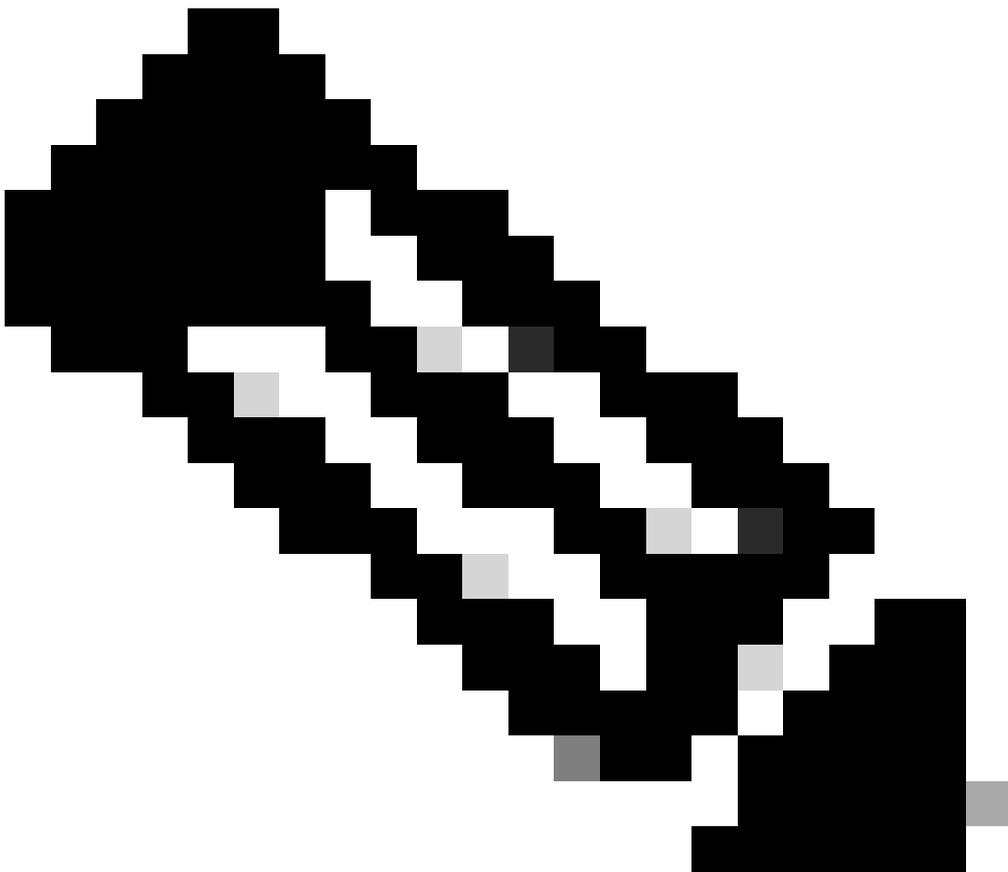
Select Features ⌵

| | | |
|--|---|---|
| Device Configuration <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Interfaces <input checked="" type="checkbox"/> Routes <input checked="" type="checkbox"/> Site-to-Site VPN Tunnels <ul style="list-style-type: none"> <input type="checkbox"/> Policy Based (Unsupported) ⓘ <input checked="" type="checkbox"/> Route Based (VTI) | Shared Configuration <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Access Control <ul style="list-style-type: none"> <input type="checkbox"/> Migrate policies with Application-default as Enabled ⓘ <input checked="" type="checkbox"/> Network Objects <input checked="" type="checkbox"/> Port Objects <input checked="" type="checkbox"/> Remote Access VPN | Advanced Configuration <ul style="list-style-type: none"> Optimization <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Migrate Only Referenced Objects Access Control Options <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Discovered Identities ⌵ ⓘ |
|--|---|---|

[Proceed](#)

Rule Conversion/ Process Config ➤

Selezione funzionalità



Nota: Tutte le feature sono selezionate per default. È possibile deselezionare qualsiasi configurazione che non deve essere migrata.

13. Fare clic su Start Conversion per convertire la configurazione.



Analisi della configurazione

Lo strumento analizza la configurazione e visualizza il riepilogo della conversione come mostrato nell'immagine. È inoltre possibile scaricare il Report pre-migrazione per convalidare la configurazione migrata in caso di errori o avvisi, se presenti. Passare alla pagina

successiva facendo clic su Avanti.

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

Riepilogo configurazione analizzata

14. Nella sezione Mappatura interfaccia è possibile definire la mappatura da Paloalto a FTD e modificare il nome di ciascuna interfaccia. Fare clic su Next (Avanti) dopo aver eseguito il mapping dell'interfaccia.

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

| PAN Interface Name | FTD Interface Name | Mapped Name |
|--------------------|--------------------|-------------|
| ethernet1/2 | Select Interface | ethernet_2 |
| ethernet1/3 | ✓ Ethernet1/1 | ethernet_3 |
| ethernet1/4 | Ethernet1/10 | ethernet_4 |
| ethernet1/5 | Ethernet1/11 | ethernet_5 |
| ethernet1/6 | Ethernet1/12 | ethernet_6 |
| ethernet1/7 | Ethernet1/13 | ethernet_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

Mappatura interfaccia

15. È possibile aggiungere l'area di protezione manualmente per ogni interfaccia oppure crearla automaticamente nella sezione Mapping dell'area di protezione. Fare clic su Avanti dopo aver creato e mappato le aree di protezione.

Map Security Zones

| PAN Zone Name | FMC Security Zones |
|---------------|----------------------|
| G...-inside | Select Security Zone |
| Outside | Select Security Zone |
| GP/PA- | Select Security Zone |
| ...ine | 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

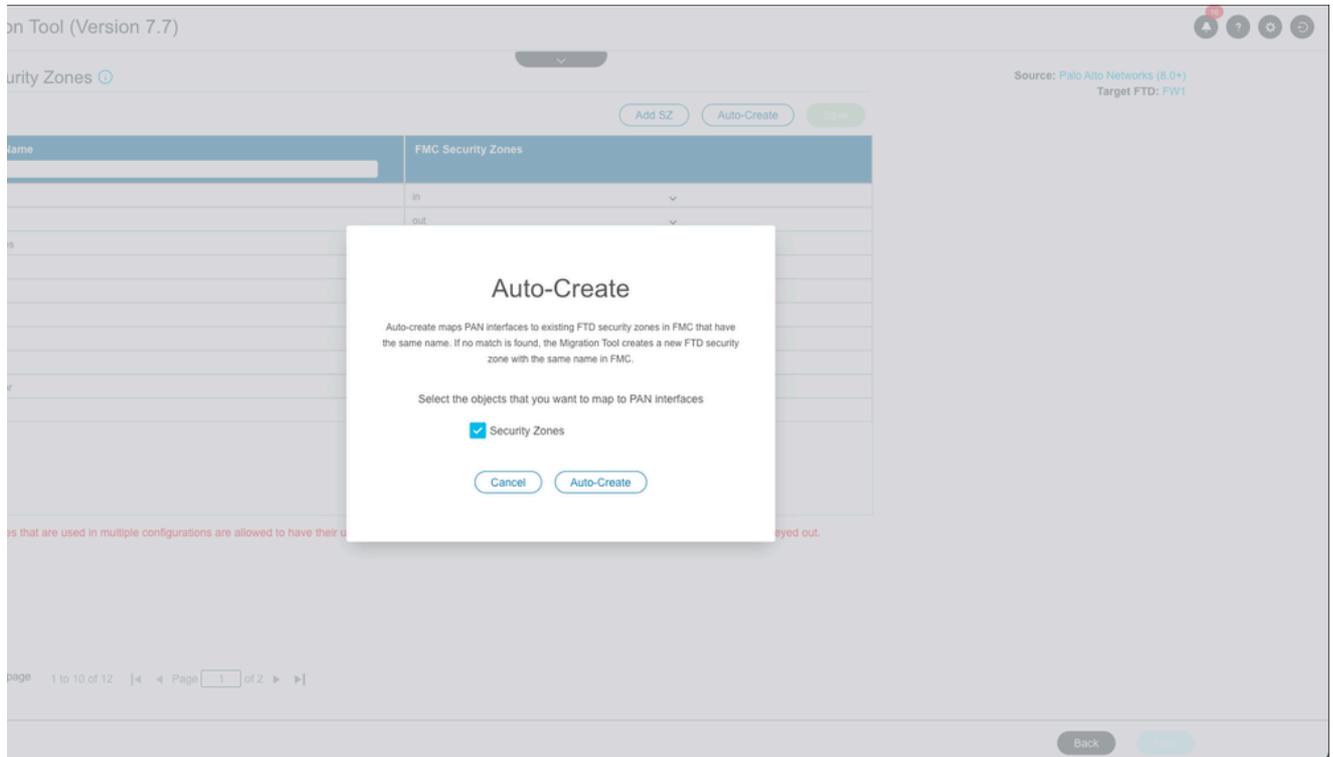
Creazione area di sicurezza

Creazione manuale delle aree di protezione:

The screenshot shows the 'Add SZ' dialog box. It has a title bar with a close button (X). Below the title, there is a section for 'Security Zones (SZ)' with an 'Add' button and a character limit warning: 'Max 48 characters for zone name. Allowed special characters are _.-+'. Below this is a table with columns for 'Security Zones', 'Type', and 'Actions'. The 'Security Zones' column contains the text 'DMZ'. The 'Type' column has a dropdown menu with 'ROUTED' selected and a checkmark. The 'Actions' column has a delete icon (X) and a confirm icon (checkmark). At the bottom of the dialog, there is a 'Close' button and a pagination indicator '0 - 0 of 0 Page 1 of 2'.

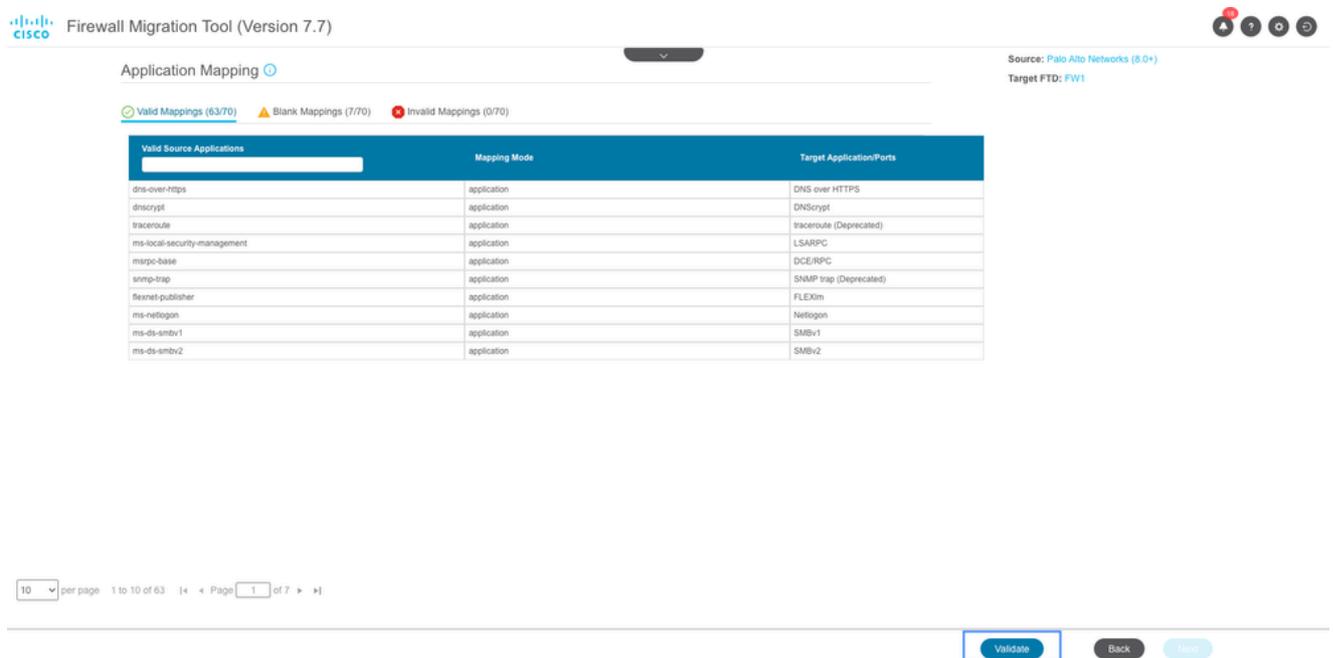
Creazione manuale area di sicurezza

Creazione automatica aree di protezione:



Creazione automatica area di sicurezza

- È ora possibile passare alla sezione Mapping applicazioni. Fare clic sul pulsante Convalida per convalidare il mapping dell'applicazione.



Mapping applicazione

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

Convalida mapping applicazioni

Al momento della convalida, FMT elenca i mapping vuoti e non validi. I mapping non validi devono essere corretti prima di procedere e la correzione dei mapping vuoti è facoltativa.

Fare di nuovo clic su Convalida per convalidare i mapping corretti. Fare clic su Avanti al termine della convalida.

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

Mapping applicazione vuoto e non valido

- Se necessario, è possibile ottimizzare gli ACL nella sezione successiva. Esaminare la configurazione in ciascuna sezione, ad esempio Controllo accesso, Oggetti, NAT, Interfacce, Route e VPN di accesso remoto. Fare clic su Validate dopo aver esaminato le configurazioni.

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 | | | ANY | NTP | NA | ✓ | Allow | None | |
| 3 | Allow Tm... | Df | GRP_ADDR... | ANY | ANY | | | ANY | NTP | NA | ✓ | Allow | None | |
| 4 | Allow DNS | Df | ANY | ANY | ANY | | | ANY | DNS, DNSCrypt, DN... | NA | ✓ | Allow | None | |
| 5 | Allow DNS | O | ANY | ANY | ANY | Inside | | ANY | DNS | NA | ✓ | Allow | None | |
| 6 | Allow API | Dc | 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 | O | ANY | ANY | ANY | Inside | | ANY | netmg-traceroute | NA | ✓ | Allow | None | |
| 10 | Allow ICM | O | ANY | ANY | ANY | Inside | | ANY | ICMPv4 | ANY | ✓ | Allow | None | |
| 11 | Allow DHC | O | ANY | ANY | ANY | Inside | | ANY | DHCP | NA | ✓ | Allow | None | |
| 12 | Allow NetE | O | ANY | ANY | ANY | Inside | | ANY | NetBIOS-ns, NetBIO... | NA | ✓ | Allow | None | |
| 13 | Allow DNS | O | ANY | ANY | ANY | Inside | | 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

Convalida configurazione

18. Al termine della convalida viene visualizzato un riepilogo di convalida. Fare clic su Push Configuration per eseguire il push della configurazione nel FMC di destinazione.

Validation Status

Successfully Validated

Validation Summary (Pre-push)

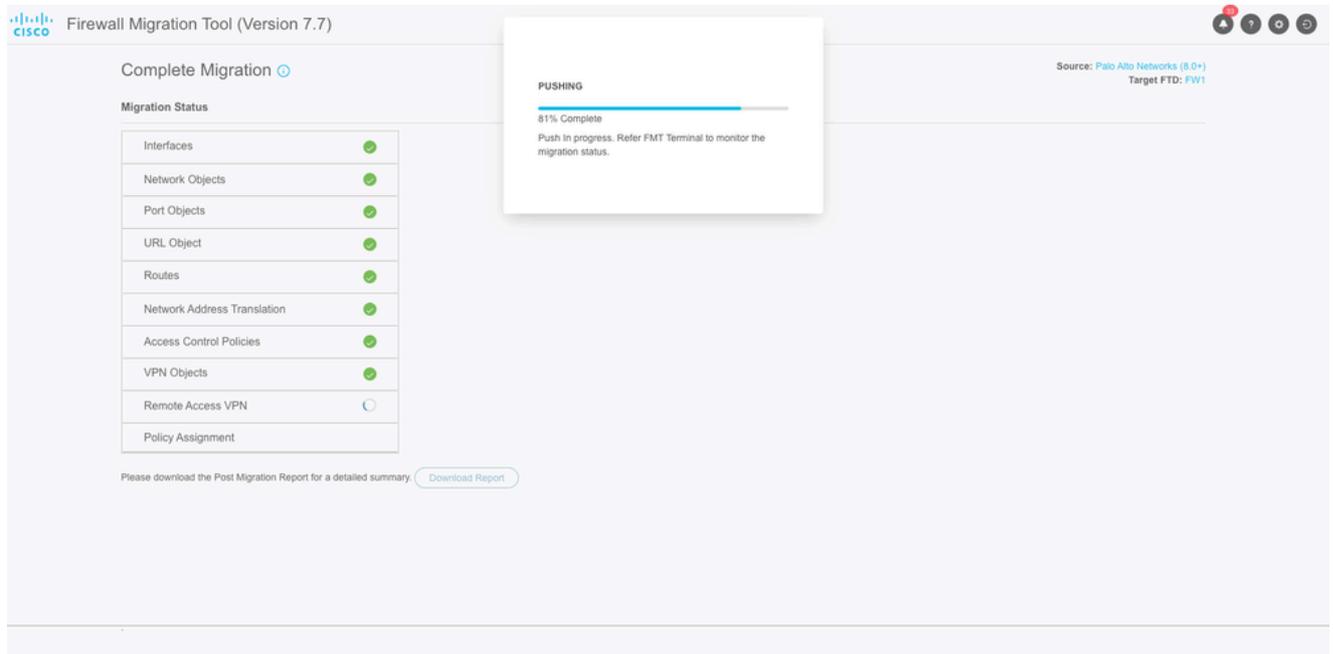
| | | | | |
|----------------------------------|---|---------------------|--|-------------------------|
| 195 Access Control List Lines | 752 Network Objects | 100 Port Objects | 52 Network Address Translation | 8 Logical Interfaces |
| 2 Static Routes | 0 Site-to-Site VPN Tunnels (Route Based) | 62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

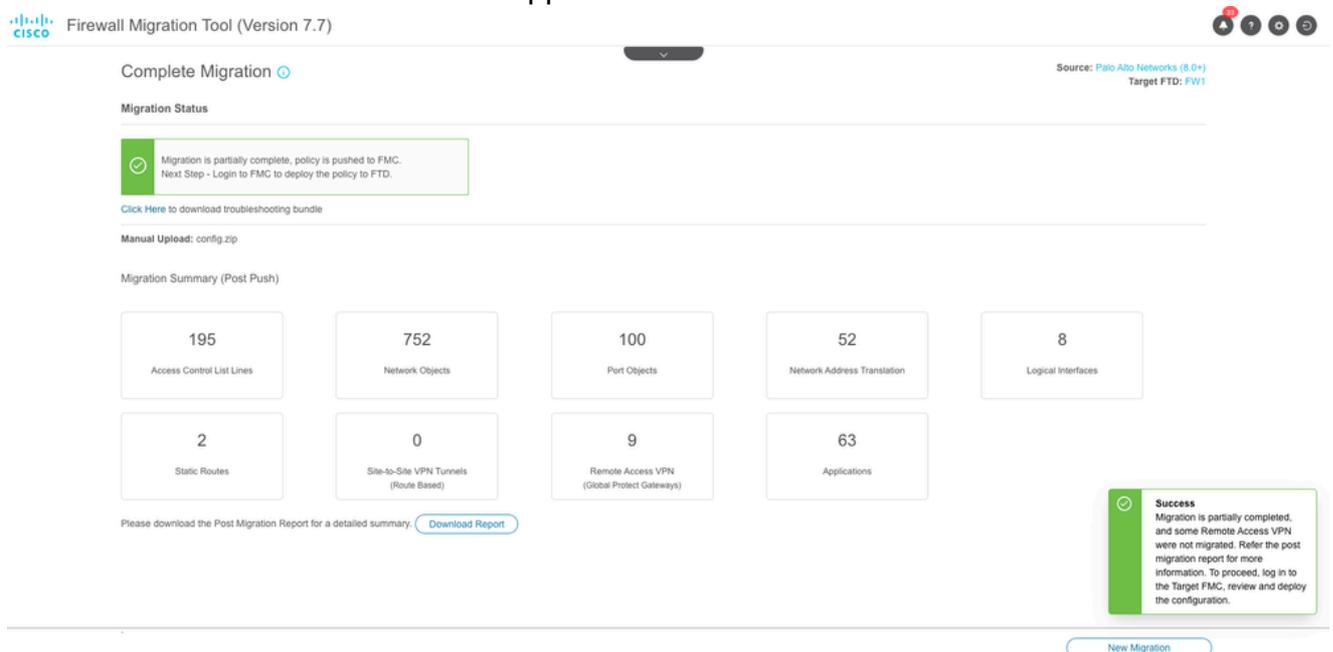
Riepilogo della convalida della configurazione

19. L'avanzamento del push della configurazione a FMC è ora visibile nella sezione relativa allo stato della migrazione. È possibile utilizzare la finestra del terminale FMT anche per monitorare lo stato della migrazione.



Stato migrazione

20. Un riepilogo della migrazione viene visualizzato dallo strumento al termine della migrazione. Vengono inoltre elencate le eventuali configurazioni di cui è stata eseguita una migrazione parziale. Ad esempio, la configurazione della VPN ad accesso remoto in questo scenario è dovuta alla mancanza del pacchetto Secure Client. È inoltre possibile scaricare il report post-migrazione per esaminare le configurazioni migrate e le eventuali correzioni o errori da apportare.



Riepilogo migrazione completata

21. L'ultimo passaggio consiste nell'esaminare la configurazione migrata da FMC e distribuire la configurazione in FTD.

Per distribuire la configurazione:

1. Accedere alla GUI del CCP.
2. Passare alla scheda Distribuisci.

3. Selezionare la distribuzione per eseguire il push della configurazione nel firewall.
4. Fare clic su Distribuisci.

Risoluzione dei problemi

Strumento di risoluzione dei problemi di migrazione Secure Firewall

Errori comuni di migrazione:

- Caratteri sconosciuti o non validi nel file di configurazione di PaloAlto.
- Elementi di configurazione mancanti o incompleti.
- Problemi di connettività di rete o latenza.
- Problemi durante il caricamento del file di configurazione di PaloAlto o durante il push della configurazione al FMC.

Utilizzo del pacchetto di supporto per la risoluzione dei problemi:

- Nella schermata "Complete Migration" (Completa migrazione), fare clic sul pulsante Support (Supporto).
- Selezionare Support Bundle e scegliere i file di configurazione da scaricare.
- I file log e DB sono selezionati per impostazione predefinita.
- Fare clic su Download per ottenere un file .zip.
- Estrarre il file .zip per visualizzare i log, il database e i file di configurazione.
- Fare clic su Invia e-mail per inviare i dettagli dell'errore al team tecnico.
- Allegare il pacchetto di supporto nell'e-mail.
- Per assistenza, fare clic su Visita la pagina TAC per creare una richiesta Cisco TAC.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).