

Configurazione dello strumento di migrazione Secure Firewall per la migrazione di ASA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Procedura di configurazione](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritta la procedura di migrazione di Cisco Adaptive Security Appliance (ASA) a Cisco Firepower.

Contributo di Ricardo Vera, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco Firewall Threat Defense (FTD) e Adaptive Security Appliance (ASA).

Componenti usati

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

- Windows PC con Firepower Migration Tool (FMT) versione 3.0.1
- Adaptive Security Appliance (ASA) v9.16.1
- Secure Firewall Management Center (FMCv) v7.0.1
- Secure Firewall Threat Defense Virtual (FTDv) v7.0.1

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.

Premesse

I requisiti specifici per questo documento includono:

- Cisco Adaptive Security Appliance (ASA) versione 8.4 o successive
- Secure Firewall Management Center (FMCv) versione 6.2.3 o successiva

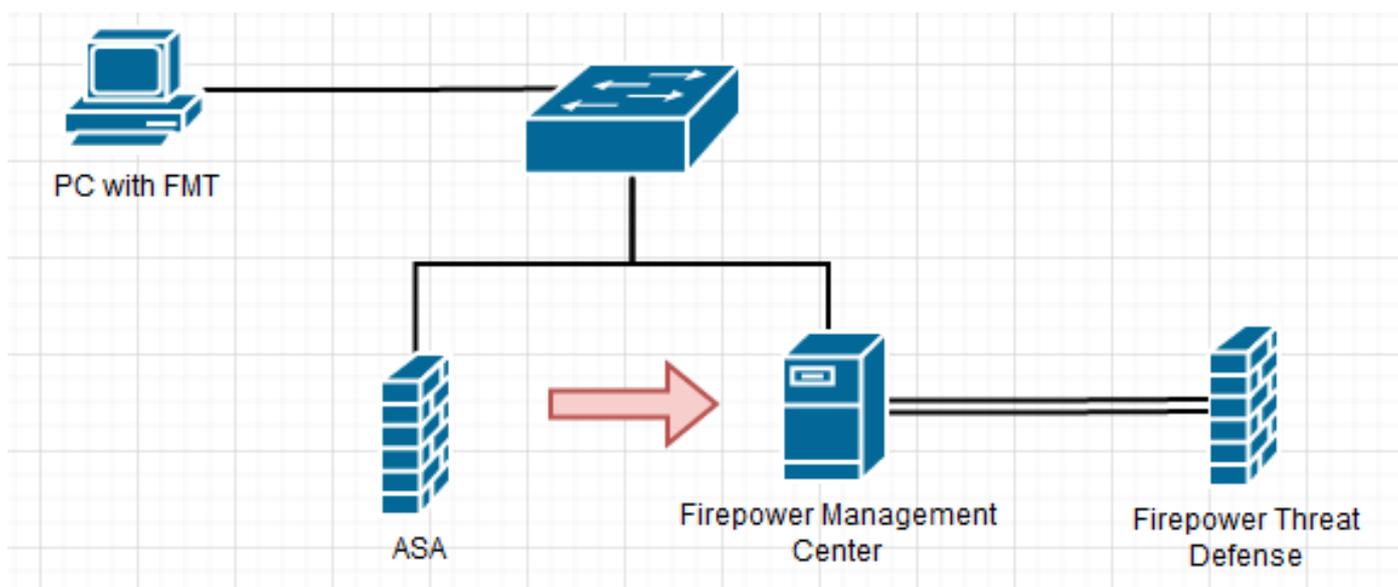
Lo strumento di migrazione del firewall supporta questo elenco di dispositivi:

- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) con FPS
- Punto di controllo (r75-r77)
- Punto di controllo (r80)
- Fortinet (5.0+)
- Palo Alto Networks (6.1+)

Prima di procedere con la migrazione, prendere in considerazione le [linee guida e le limitazioni per lo strumento di migrazione del firewall](#).

Configurazione

Esempio di rete



Procedura di configurazione

1. **Scarica** l'ultimo strumento di migrazione Firepower da Cisco Software Central:

Software Download

Downloads Home / Security / Firewalls / Next-Generation Firewalls (NGFW) / Secure Firewall Threat Defense Virtual / Firepower Migration Tool (FMT) - 3.0.1

Search...

Expand All Collapse All

Latest Release

- 3.0.1**
- 2.5.3

All Release

- 3
- 2

Secure Firewall Threat Defense Virtual

Release 3.0.1

My Notifications

Related Links and Documentation

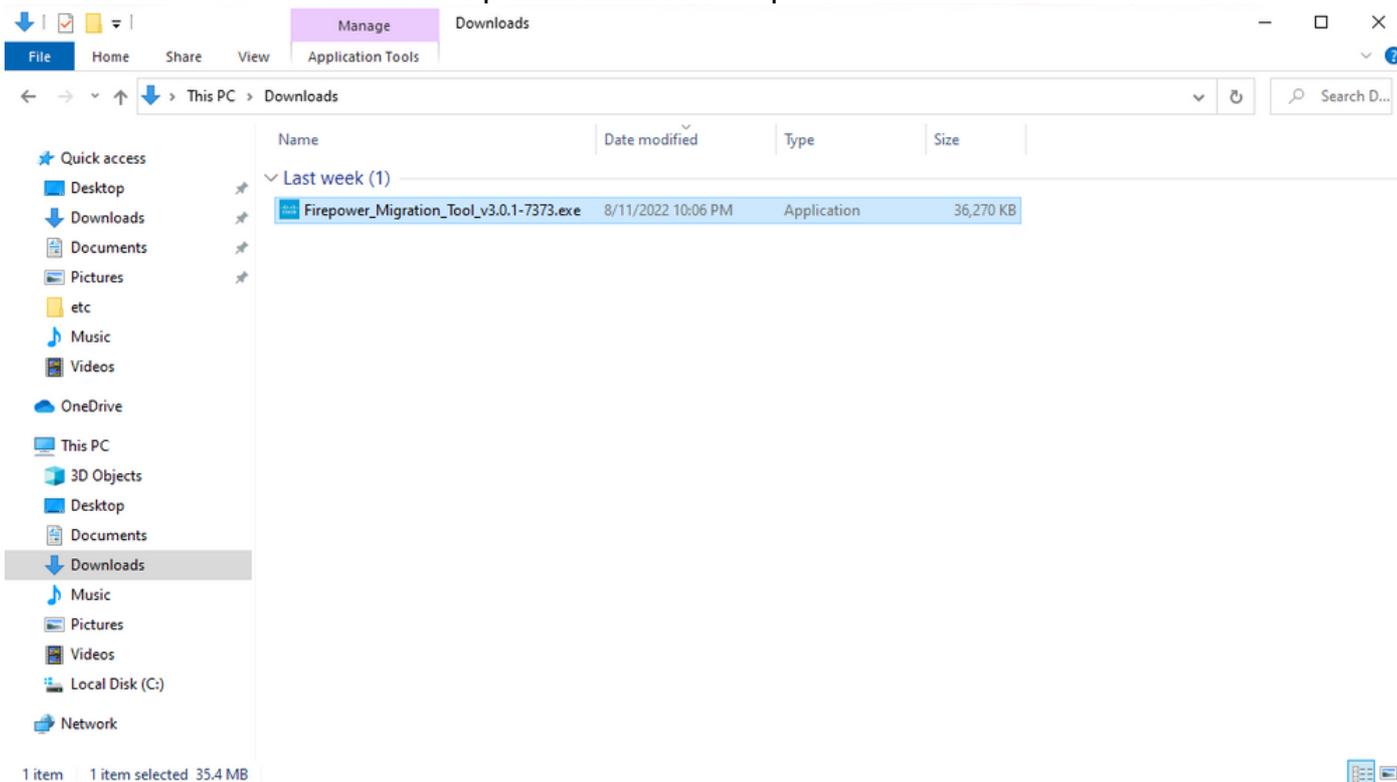
[Open Source](#)

[Release Notes for 3.0.1](#)

[Install and Upgrade Guides](#)

File Information	Release Date	Size	
The extractor will be used to extract checkpoint device-specific configurations which will be used as an input to Firepower Migration Tool. FMT-CP-Config-Extractor_v3.0.1-7373.exe Advisories	10-Aug-2022	9.83 MB	Download Shopping Cart Add to Favorites
Firepower Migration Tool 3.0.1 for Mac Firepower_Migration_Tool_v3.0.1-7373.command Advisories	10-Aug-2022	34.75 MB	Download Shopping Cart Add to Favorites
Firepower Migration Tool 3.0.1 for Windows Firepower_Migration_Tool_v3.0.1-7373.exe Advisories	10-Aug-2022	35.42 MB	Download Shopping Cart Add to Favorites

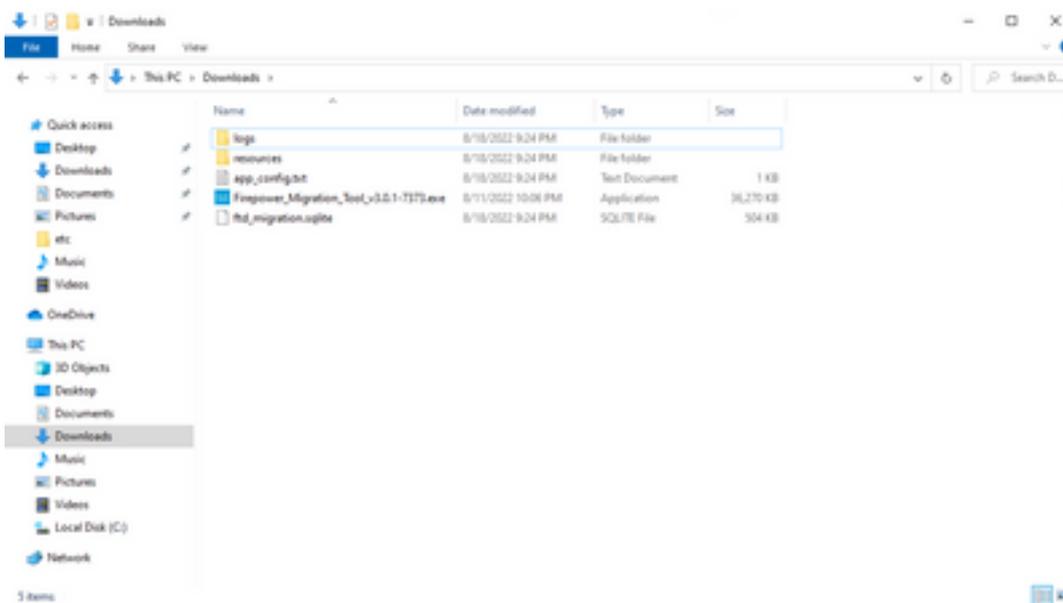
2. Fare clic sul file scaricato in precedenza sul computer.



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

```
C:\Users\cali\Downloads\Firepower_Migration_Tool_v1.0.1-7171.exe
2022-08-18 21:24:49,752 [INFO] __init__ > "Initializing..."
2022-08-18 21:24:49,767 [INFO] settings > "Settings:[global_suffix]"
2022-08-18 21:24:50,189 [INFO] tool_version > "ToolVersion:[0817373]"
2022-08-18 21:24:50,252 [INFO] __init__ > "Initializing..."
2022-08-18 21:24:51,252 [INFO] config > "loading settings"
2022-08-18 21:24:51,268 [INFO] client > "Getting ssl context for auth server"
2022-08-18 21:24:51,299 [INFO] tools > "Not verifying ssl certificates"
2022-08-18 21:24:51,299 [INFO] client > "No discovery url configured, all endpoints needs to be configured manually"

2022-08-18 21:24:51,314 [INFO] settings > "Disabled console quick edit mode"
2022-08-18 21:24:51,314 [DEBUG] common > "session table records count:1"
2022-08-18 21:24:51,314 [INFO] common > "Using port: 8888"
2022-08-18 21:24:51,799 [INFO] run > "***** Starting server at http://localhost:8888 *****"
 * Running on http://localhost:8888/ (Press CTRL+C to quit)
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /styles.a0d79d8031ca159b236f.bundle.css HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /inline.318b58c57b4eba3d437b.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /cui-font.880241c8aa87aa899c6a.woff2 HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /polyfills.76c2f23d4e2a1188f46c.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:56] "GET /main.777e77bd49fe82694a1a.bundle.js HTTP/1.1" 200 -
2022-08-18 21:24:57,075127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/cisco.svg HTTP/1.1" 200 -
[INFO] cco_login > "USA check for an user"
2022-08-18 21:24:57,704 [DEBUG] common > "session table records count:1"
127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:57] "GET /assets/icons/login.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [18/Aug/2022 21:24:58] "GET /favicon.ico HTTP/1.1" 200 -
```



3. Dopo l'esecuzione del programma, viene aperto un browser Web che visualizza il "Contratto di licenza con l'utente finale". Selezionare la casella di controllo per accettare i termini e le condizioni. Fare clic su **Continua**.

Select Source Configuration

Source Firewall Vendor

[Select Source]

- Cisco ASA (8.4+)
- Cisco ASA (9.2.2+) with FPS
- Check Point (775-777)
- Check Point (880)
- Fortinet (5.0+)
- Palo Alto Networks (6.1+)

Cisco ASA (8.4+) Pre-Migration Instructions

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

Acronyms used:

FMT: Firewall Migration Tool

FMC: Firepower Management Center

FTD: Firepower Threat Defense

Before you begin your Adaptive Security Appliance (ASA) to Firepower 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.
- **ASA Configuration Requirements:**
Export configuration file from ASA to .cfg or .txt format. Connect to live ASA to extract the configuration file for one or more contexts. To migrate following features in ASA:
 1. **Time Based ACLs:** FMC and FTD must be on 6.6 or later versions.
 2. **IP SLA Monitor:** FMC must be on 6.6 or later and FTD must be on 6.2.3 or later.
 3. **Object Group Search:** FMC and FTD must be on 6.6 or later versions.
 4. **ASA5505 Support:** FMC and FTD must be on 6.6 or later versions.
 5. **Remote Deployment:** FMC and FTD must be on 6.7 or later versions. If remote deployment is enabled, Firewall Migration Tool will only migrate ACLs, Network Object and Port Objects. Interface and Route configuration have to be migrated manually on to FMC.
 6. **Site-to-Site VPN Tunnels:** Policy Based (Crypto Map) VPN needs FMC and FTD to be on 6.6 or later. Route Based (VTI) Support, FMC and FTD to be on 6.7 or later. Ensure FTD must be added to FMC before migration. Firewall Migration Tool will migrate VPN tunnels as Point-to-Point network.

6. Selezionare il metodo di estrazione da utilizzare per ottenere la configurazione. Per il caricamento manuale è necessario caricare **Running Config** dell'ASA nel formato ".cfg" o ".txt". Collegare l'appliance ASA per estrarre le configurazioni direttamente dal firewall.

1 Extract ASA Information
 2 Select Target
 3 Map FTD Interface
 4 Map Security Zones & Interface Groups
 5 Optimize, Review & Validate
 6 Complete Migration

Extract Cisco ASA (8.4+) Information Source: Cisco ASA (8.4+)

Extraction Methods ▼

Manual Upload

- File format is '.cfg' or '.txt'.
- For Multi-context upload a show tech.
For Single-context upload show running.
- ⚠ Do not upload hand coded configurations.

Upload

Connect to ASA

- Enter the management IP address and connect using admin credentials.
- IP format should be: <IP>Port>.

ASA IP Address/Hostname

Connect

Context Selection >

Parsed Summary >

Back
Next

Nota: Per questo esempio, connettersi direttamente all'appliance ASA.

7. Un riepilogo della configurazione rilevata sul firewall viene visualizzato come dashboard. Fare clic su **Avanti**.

Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods >

ASA IP Address: 192.168.1.20

Context Selection >

Single Context Mode: Download config

Parsed Summary ▾

Collect Hitcounts: No



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

8. Selezionare il FMC di destinazione da utilizzare nella migrazione. Fornire l'indirizzo IP del CCP. Viene visualizzata una finestra popup in cui vengono richieste le credenziali di accesso del CCP.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management ▾

 On-Prem/Virtual FMC Cloud-delivered FMC

FMC IP Address/Hostname

192.168.1.18

Connect

1 FTD(s) Found

Proceed

✔️ Successfully connected to FMC

Choose FTD >

Select Features >

Rule Conversion/ Process Config >

9. (Facoltativo) Selezionare l'FTD di destinazione da utilizzare. Se si sceglie di eseguire la migrazione a un FTD, selezionare l'FTD che si desidera utilizzare. Se non si desidera utilizzare un FTD, è possibile compilare la casella di controllo Proceed without FTD

Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Select FTD Device Proceed without FTD

FTD (192.168.1.17) - VMWare (Native) v

Please ensure that the firewall mode configured on the target FTD device is the same as in the uploaded ASA configuration file. The existing configuration of the FTD device on the FMC is erased when you push the migrated configuration to the FMC.

Proceed

Select Features >

Rule Conversion/ Process Config >

Back

Next

10. Selezionare le configurazioni di cui si desidera eseguire la migrazione. Le opzioni vengono visualizzate negli screenshot.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management >

FMC IP Address/Hostname: 192.168.1.18

Choose FTD >

Selected FTD: FTD

Select Features >

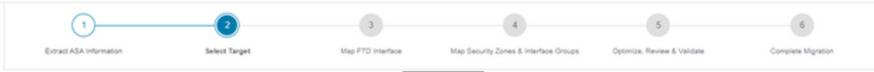
Device Configuration	Shared Configuration	Optimization
<input checked="" type="checkbox"/> Interfaces	<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Migrate Only Referenced Objects
<input checked="" type="checkbox"/> Routes	<input checked="" type="checkbox"/> Populate destination security zones	<input checked="" type="checkbox"/> Object Group Search
<input checked="" type="checkbox"/> Static	<input type="checkbox"/> Route-lookup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.	Inline Grouping
<input type="checkbox"/> BGP	<input checked="" type="checkbox"/> Migrate tunnelled rules as Prefilter	<input checked="" type="checkbox"/> CSM/ASDM
<input type="checkbox"/> EIGRP	<input type="checkbox"/> NAT (no data)	
<input type="checkbox"/> Site-to-Site VPN Tunnels (no data)	<input checked="" type="checkbox"/> Network Objects (no data)	
<input type="checkbox"/> Policy Based (Crypto Map)	<input type="checkbox"/> Port Objects (no data)	
<input type="checkbox"/> Route Based (VTI)	<input type="checkbox"/> Access List Objects(Standard, Extended)	
	<input type="checkbox"/> Time based Objects (no data)	
	<input type="checkbox"/> Remote Access VPN	
	<input type="checkbox"/> Remote Access VPN migration is supported on FMC/FTD 7.2 and above.	

Proceed

Back

Next

11. Avviare la conversione delle configurazioni da ASA a FTD.



Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

Back Next

12. Al termine della conversione, viene visualizzato un dashboard con il riepilogo degli oggetti da migrare (limitato alla compatibilità). È possibile fare clic su **Download Report** per ricevere un riepilogo delle configurazioni da migrare.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

0 parsing errors 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](#)

0 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/RAVP/NEIGRP)	1 Network Objects	0 Port Objects	0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
0 Network Address Translation	1 Logical Interfaces	1 Routes	0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)

Back Next

Esempio di report pre-migrazione, come mostrato nell'immagine:

Note: Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firepower Management Center to ensure that traffic is appropriately handled by Firepower Threat Defense after the configuration is successfully migrated.

I. Overall Summary:

A summary of the supported ASA configuration elements that can be successfully migrated to Firepower Threat Defense.

Collection Method	Connect ASA
ASA Configuration Name	aaalive_ciscoasa_2022-08-19_02-04-31.txt
ASA Firewall Context Mode Detected	single
ASA Version	9.16(1)
ASA Hostname	Not Available
ASA Device Model	ASA; 2048 MB RAM, CPU Xeon 4100 6100 8100 series 2200 Mhz
Hic Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	0
ACEs Migratable	0
Site to Site VPN Tunnels	0
FMC Type	On-Prem FMC
Logical Interfaces	1
Network Objects and Groups	1

13. Mappare le interfacce ASA con le interfacce FTD sullo strumento di migrazione.

Firewall Migration Tool

Map FTD Interface

Source: Cisco ASA (8.4+)
Target FTD: FTD

Refresh

ASA Interface Name	FTD Interface Name
Management0/0	GigabitEthernet0/0

20 per page 1 to 1 of 1 |< 4 Page 1 of 1 >|

Back Next

14. Creare le aree di sicurezza e i gruppi di interfacce per le interfacce sull'FTD

Map Security Zones and Interface Groups

Add SZ & IG Auto-Create

Source: Cisco ASA (8.4+)

Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	Select Security Zone	Select Interface Groups

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

Back Next

Le aree di sicurezza (SZ) e i gruppi di interfaccia (IG) vengono creati automaticamente dallo strumento, come mostrato nell'immagine:



Map Security Zones and Interface Groups

Add SZ & IG Auto-Create

Source: Cisco ASA (8.4+)

Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	management	management_ig (A)

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

Back Next

15. Rivedere e convalidare le configurazioni da migrare sullo strumento di migrazione. Se l'analisi e l'ottimizzazione delle configurazioni sono già state completate, fare clic su Validare.



Optimize, Review and Validate Configuration

Source: Cisco ASA (8.4+)
Target FTD: FTD

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

Access List Objects **Network Objects** Port Objects VPN Objects Dynamic-Route Objects

Select all 1 entries Selected: 0 / 1

#	Name	Validation State	Type	Value
1	obj-192.168.1.1	Will be created in FMC	Network Object	192.168.1.1

50 per page 1 to 1 of 1 Page 1 of 1

Note: Populate the areas highlighted in Yellow in EIGRP, Site to Site and Remote Access VPN sections to validate and proceed with migration

Validate

16. Se lo stato di convalida ha esito positivo, eseguire il push delle configurazioni nei dispositivi di destinazione.

Validation Status

Successfully Validated

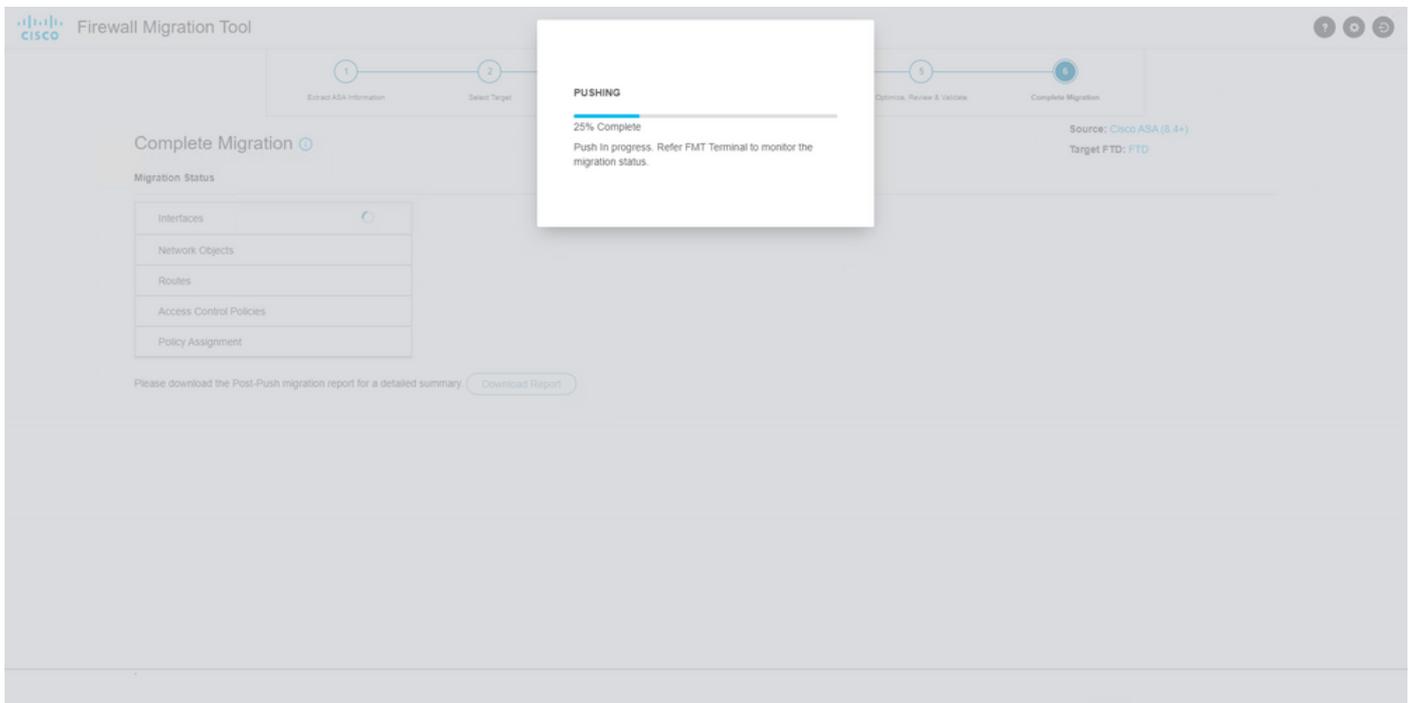
Validation Summary (Pre-push)

0	Not selected for migration	1	Not selected for migration	Not selected for migration
Access Control List Lines	Access List Objects (Standard, Extended used in BGP/RAV/EIGRP)	Network Objects	Port Objects	Dynamic-Route Objects (AS-Path, Community List, Policy List, Prefix List, Route-Map)
Not selected for migration	1	1	Not selected for migration	Not selected for migration
Network Address Transl...	Logical Interfaces	Routes	Site-to-Site VPN Tunnels	Remote Access VPN (Connection Profiles)

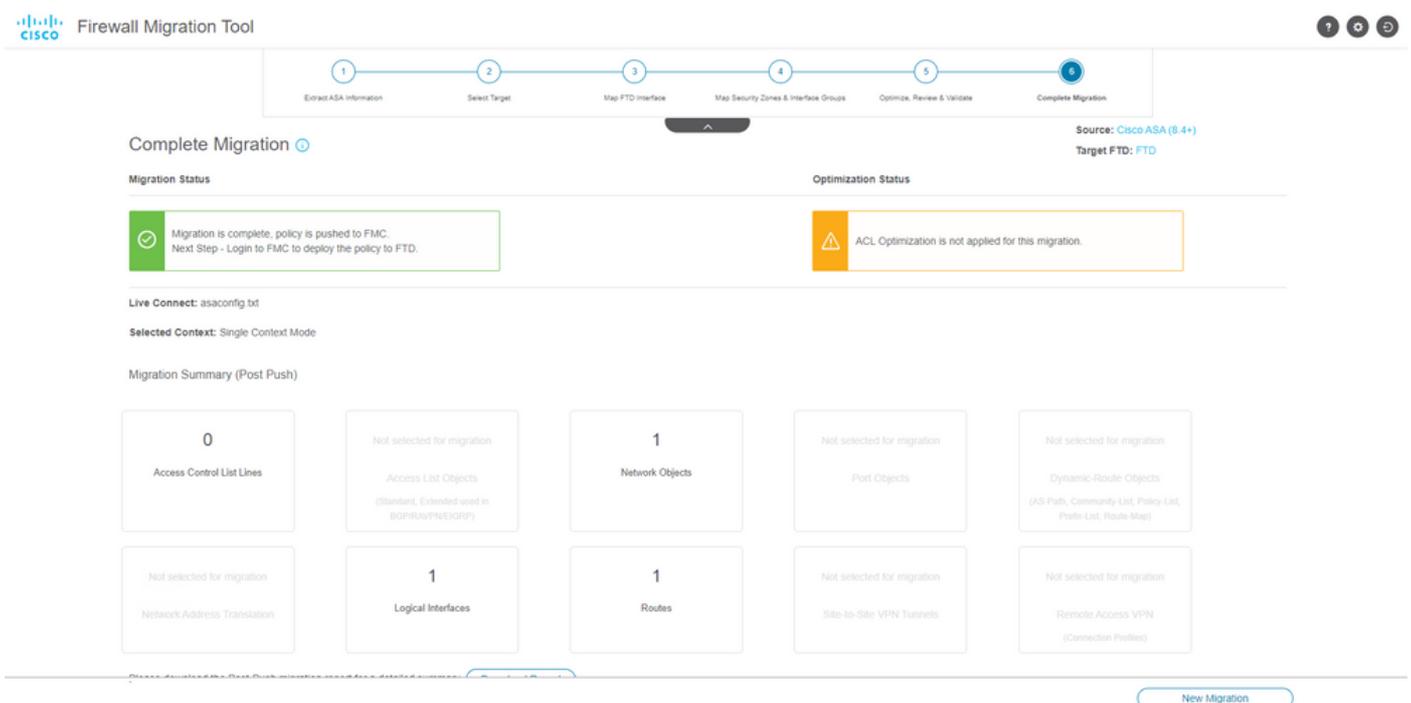
Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

Esempio di configurazione sottoposta a push tramite lo strumento di migrazione, come mostrato nell'immagine:



Esempio di migrazione riuscita, come mostrato nell'immagine:



17. (Facoltativo) Se si è scelto di eseguire la migrazione della configurazione a un FTD, è necessaria una distribuzione per eseguire il push della configurazione disponibile dal FMC al firewall, al fine di distribuire la configurazione: Accedere alla GUI del CCP. Passare alla Deploy. Selezionare la distribuzione per eseguire il push della configurazione nel firewall. Clic Deploy.

The screenshot displays the Cisco Firepower Management Center interface. At the top, the navigation menu includes Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The current page is titled "Deploy / Deployment" and features a "Deploy" button in the top right corner. A search bar is located at the top left, with the text "Search using device name, type, domain, group or status". Below the search bar is a table with the following columns: Device, Inspect Interruption, Type, Group, Last Deploy Time, Preview, and Status. The table contains one entry for "FTD" with a status of "Pending" and a last deploy time of "8/13/2022, 6:01:52 PM". To the left of the table is a sidebar menu with the following items: Device Configurations, Interface Policy, Advanced Settings, Routing Group, and IPv4 Static Route Policy. A "How To" button is located at the bottom center of the interface.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Verificare i log nella directory in cui è stato inserito il file dello strumento di migrazione di Firepower, ad esempio:

Firepower_Migration_Tool_v3.0.1-7373.exe/logs/log_2022-08-18-21-24-46.log

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).