Migrazione da ASA a Firepower Threat Defense (FTD) con FMT

Sommario

Introduzione

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

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:

- Mac OS con Firepower Migration Tool (FMT) versione 7.0.1
- Adaptive Security Appliance (ASA) v9.16(1)
- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.1

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.

Panoramica

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
- Cisco Secure Firewall Device Manager (7.2+)
- Punto di controllo (r75-r77)
- Punto di controllo (r80)
- Fortinet (5.0+)

· Palo Alto Networks (6.1+)

Premesse

Prima di migrare la configurazione ASA, eseguire le seguenti attività:

Recupero del file di configurazione ASA

Per eseguire la migrazione di un dispositivo ASA, usare il comando show running-config per un singolo contesto o show tech-support per la modalità multi-contesto per ottenere la configurazione, salvarla come file con estensione cfg o txt e trasferirla sul computer con lo strumento di migrazione Secure Firewall.

Esporta certificato PKI da ASA e importa in Management Center

Utilizzare questo comando per esportare il certificato PKI dalla CLI della configurazione ASA di origine con le chiavi in un file PKCS12:
ASA(config)#crypto può esportare <nome-trust-point> pkcs12 <passphrase>
Importare quindi il certificato PKI in un centro di gestione (Oggetti PKI Gestione oggetti). Per ulteriori informazioni, vedere Oggetti PKI nella Guida alla configurazione di Firepower Management Center.

Recupero di pacchetti e profili AnyConnect

I profili AnyConnect sono facoltativi e possono essere caricati tramite il centro di gestione o lo strumento di migrazione Secure Firewall.

Utilizzare questo comando per copiare il pacchetto richiesto dall'appliance ASA di origine su un server FTP o TFTP:

Copy <percorso file di origine:/nome file di origine> <destinazione>

ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <— Esempio di copia di Anyconnect Package.

ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <— Esempio di copia di un pacchetto del browser esterno.

ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <— Esempio di copia di Hostscan Package.

ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <— Esempio di copia di Dap.xml

ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <— Esempio di copia di Data.xml

ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <— Esempio di copia di un profilo Anyconnect.

Importare i pacchetti scaricati nel centro di gestione (Gestione oggetti > VPN > File AnyConnect).

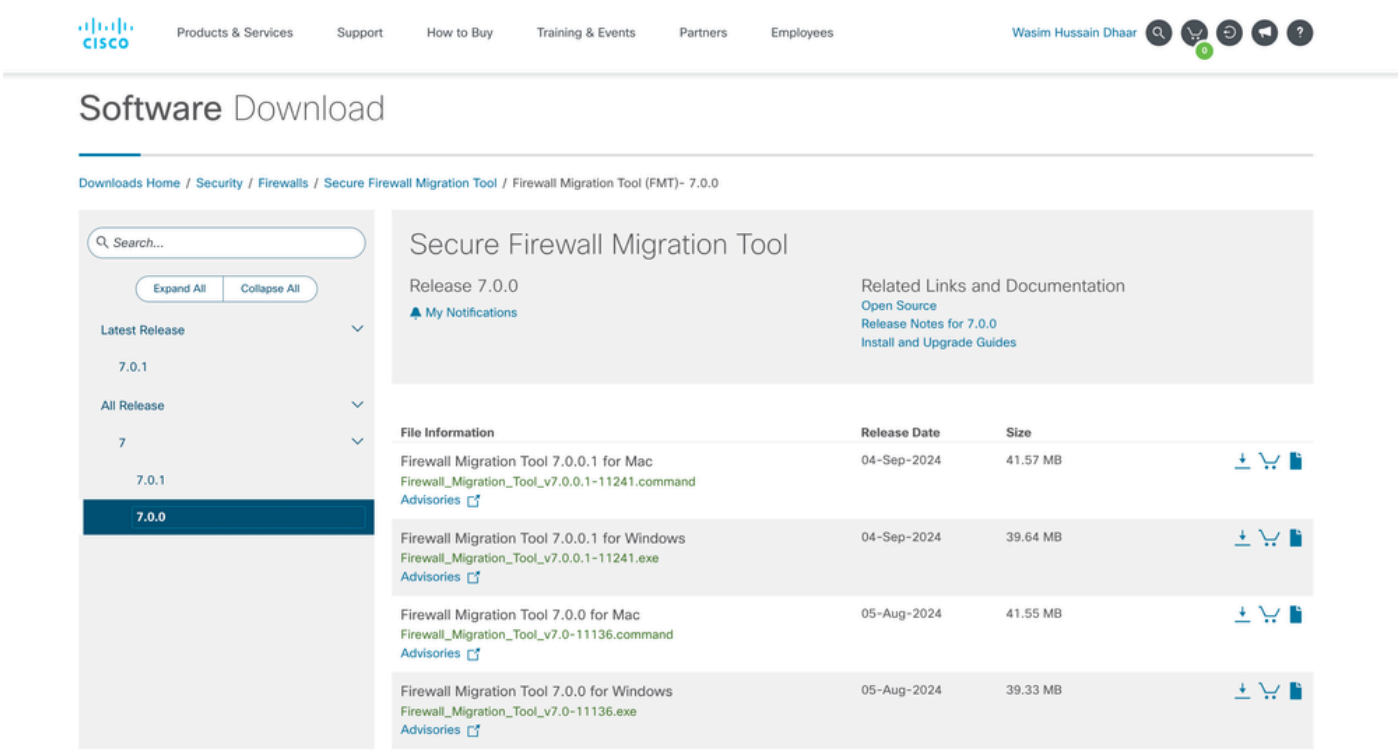
a-Dap.xml e Data.xml devono essere caricati nel centro di gestione dallo strumento di migrazione Secure Firewall nella sezione Verifica e convalida > VPN ad accesso remoto > File AnyConnect.

I profili b-AnyConnect possono essere caricati direttamente nel centro di gestione o tramite lo strumento di migrazione Secure Firewall nella sezione Revisione e convalida > VPN ad accesso remoto > File AnyConnect.

Configurazione

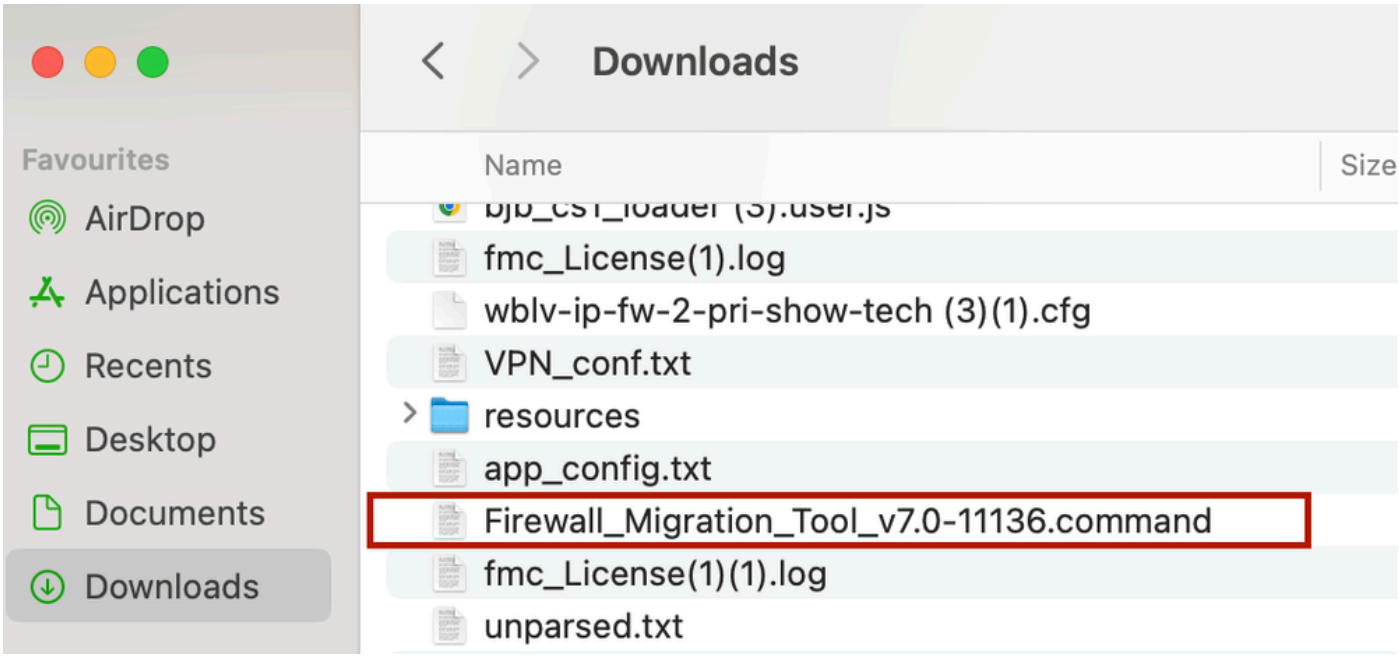
Procedura di configurazione:

1.Scarica l'ultima versione di Firepower Migration Tool da Cisco Software Central:

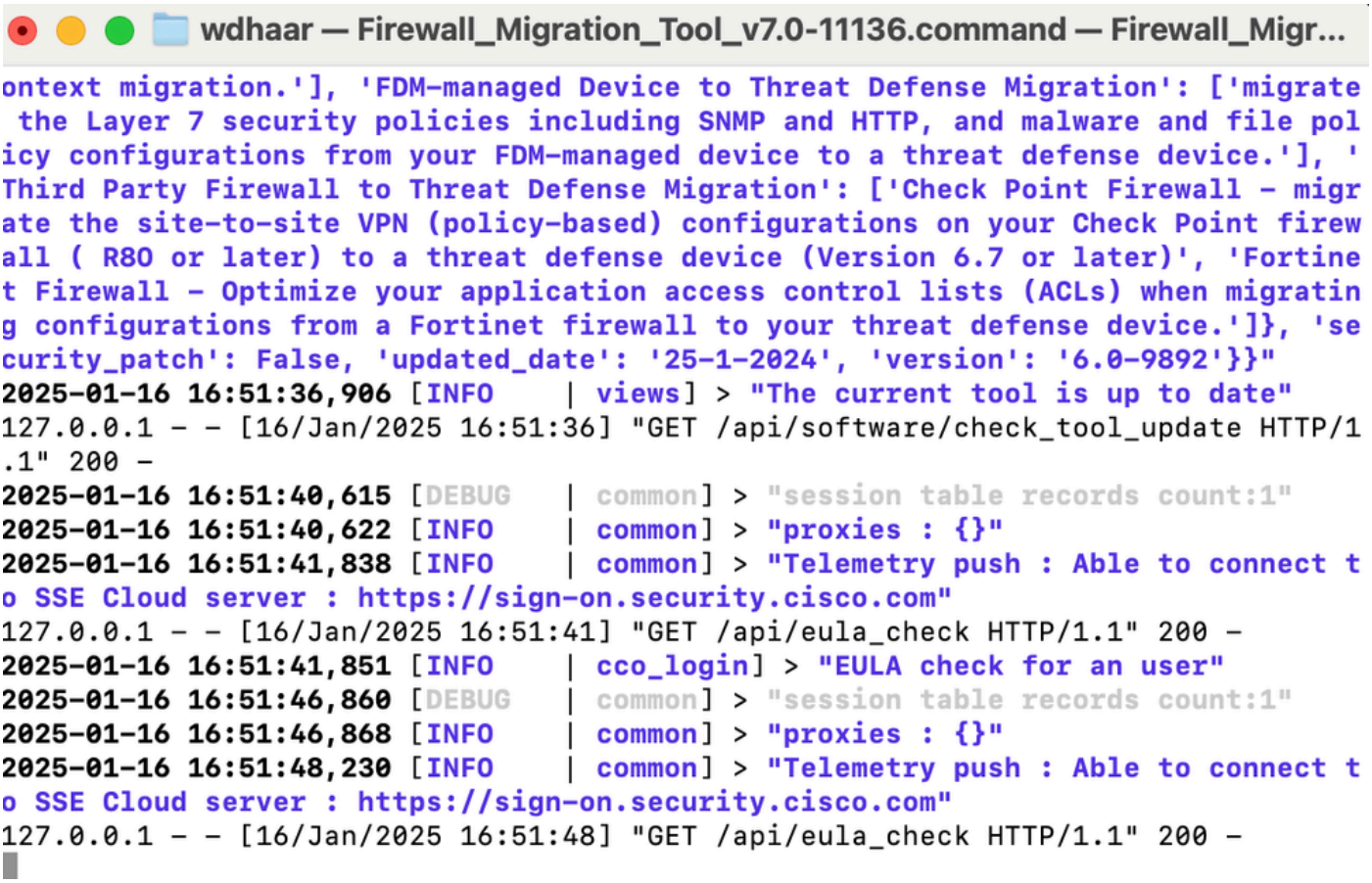


Download del software

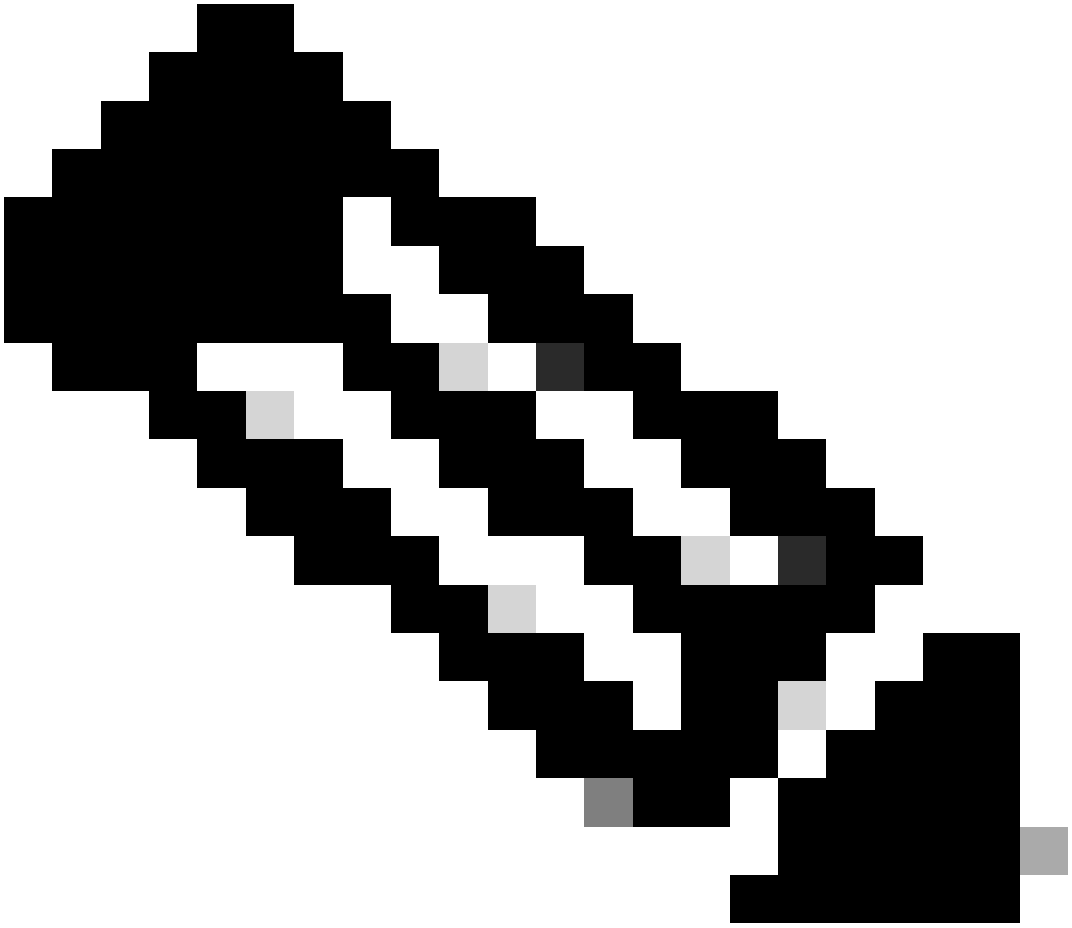
2. Fare clic sul file scaricato in precedenza sul computer.



Il file

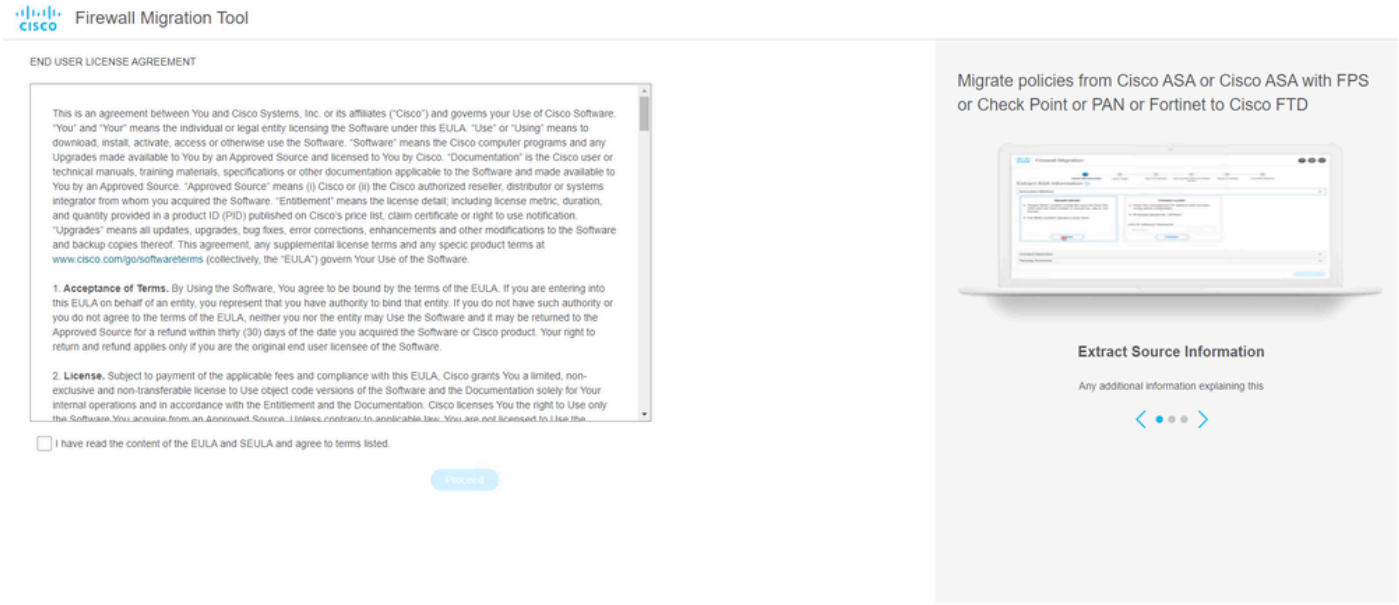


Registri console



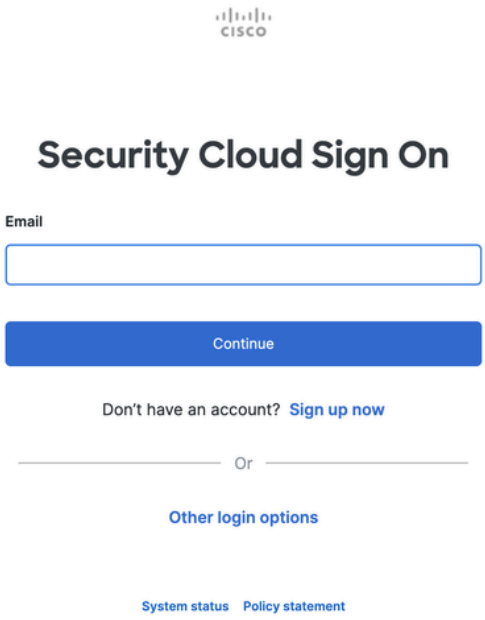
Nota: Il programma si apre automaticamente e una console genera automaticamente il contenuto nella directory in cui è stato eseguito il file.

3. 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 Continua.



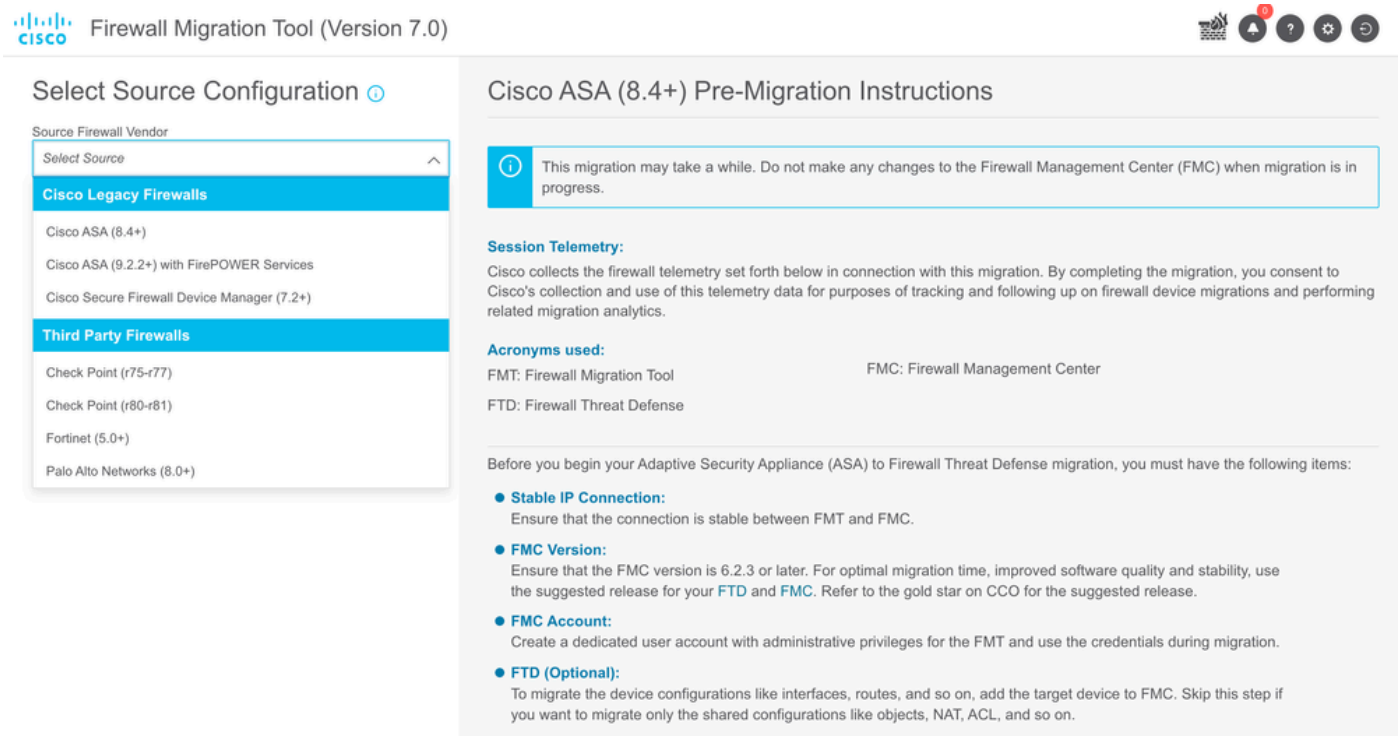
EULA

4. Effettuare l'accesso con un account CCO valido e l'interfaccia GUI FMT viene visualizzata sul browser Web.



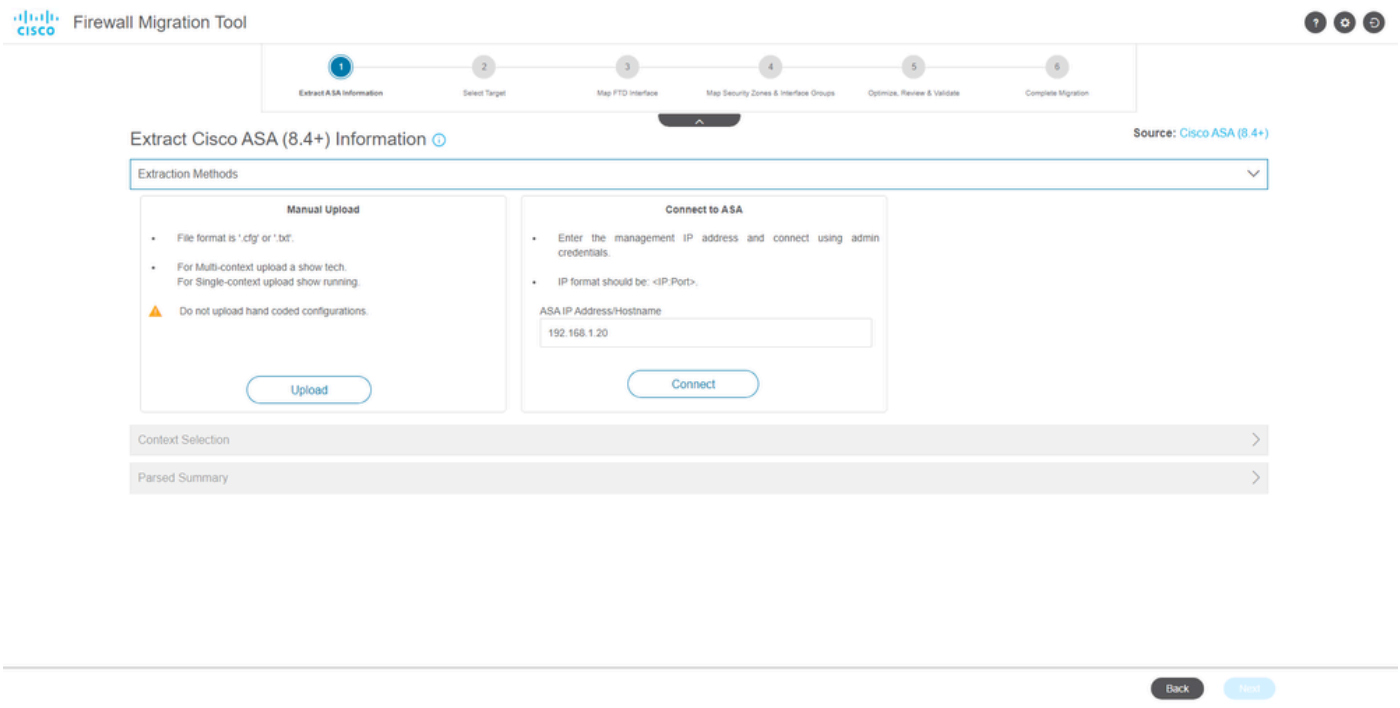
Accesso FMT

5. Selezionare il firewall di origine da migrare.

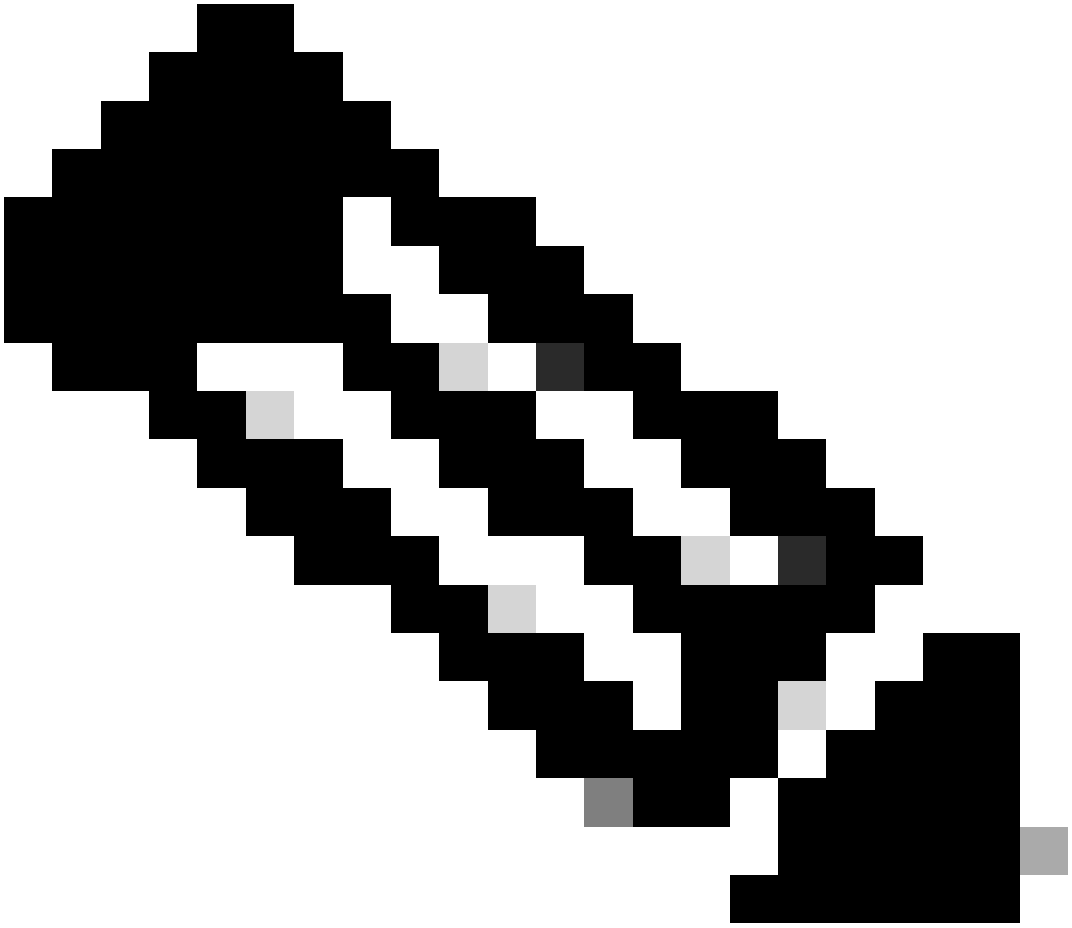


Firewall di origine

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

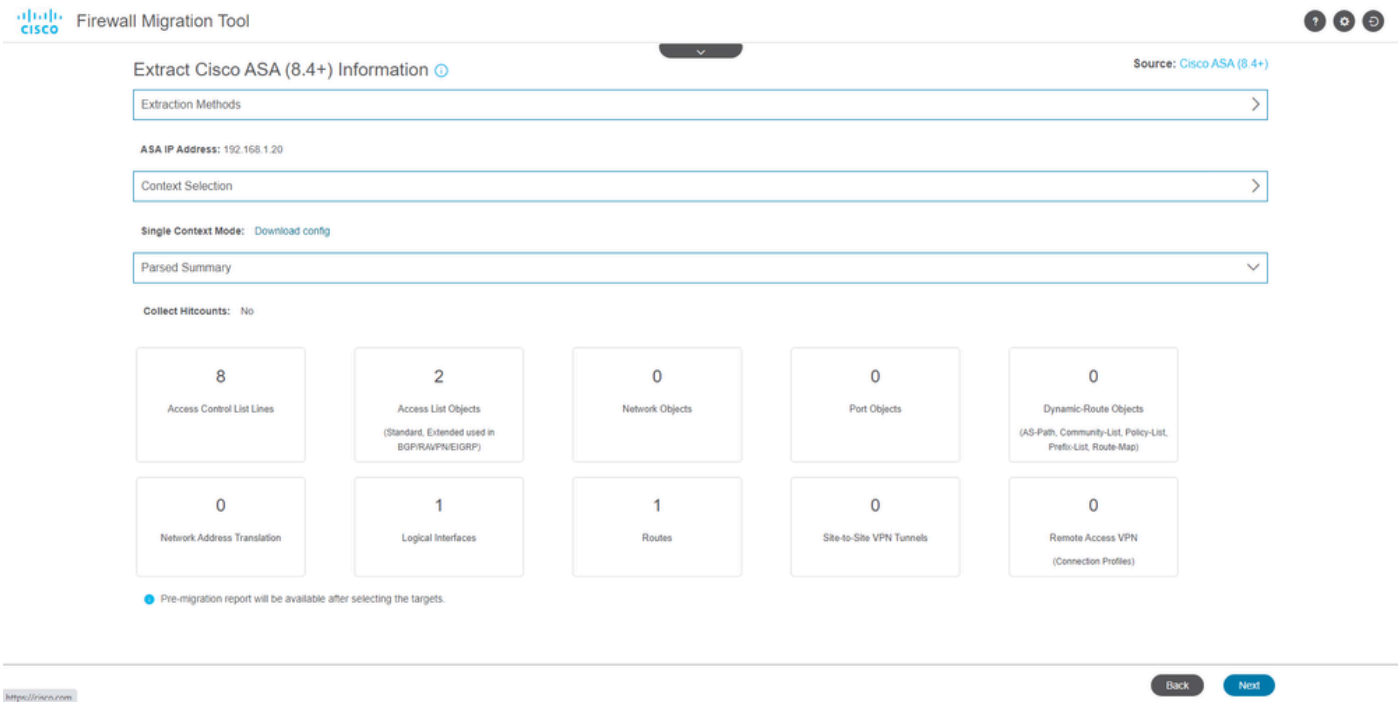


Estrazione



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

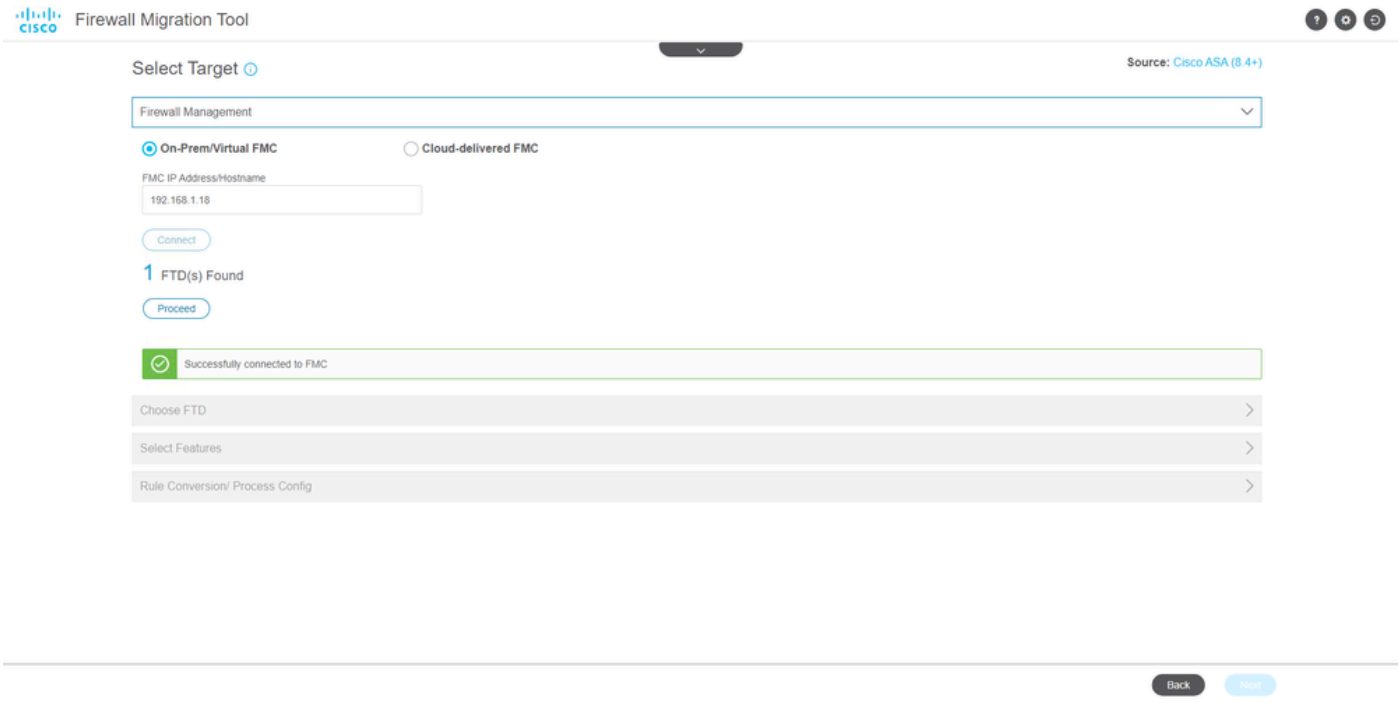
7. Un riepilogo della configurazione rilevata sul firewall viene visualizzato come dashboard. Fare clic su Avanti.



Riepilogo

8. Selezionare il CCP di destinazione da utilizzare per la migrazione.

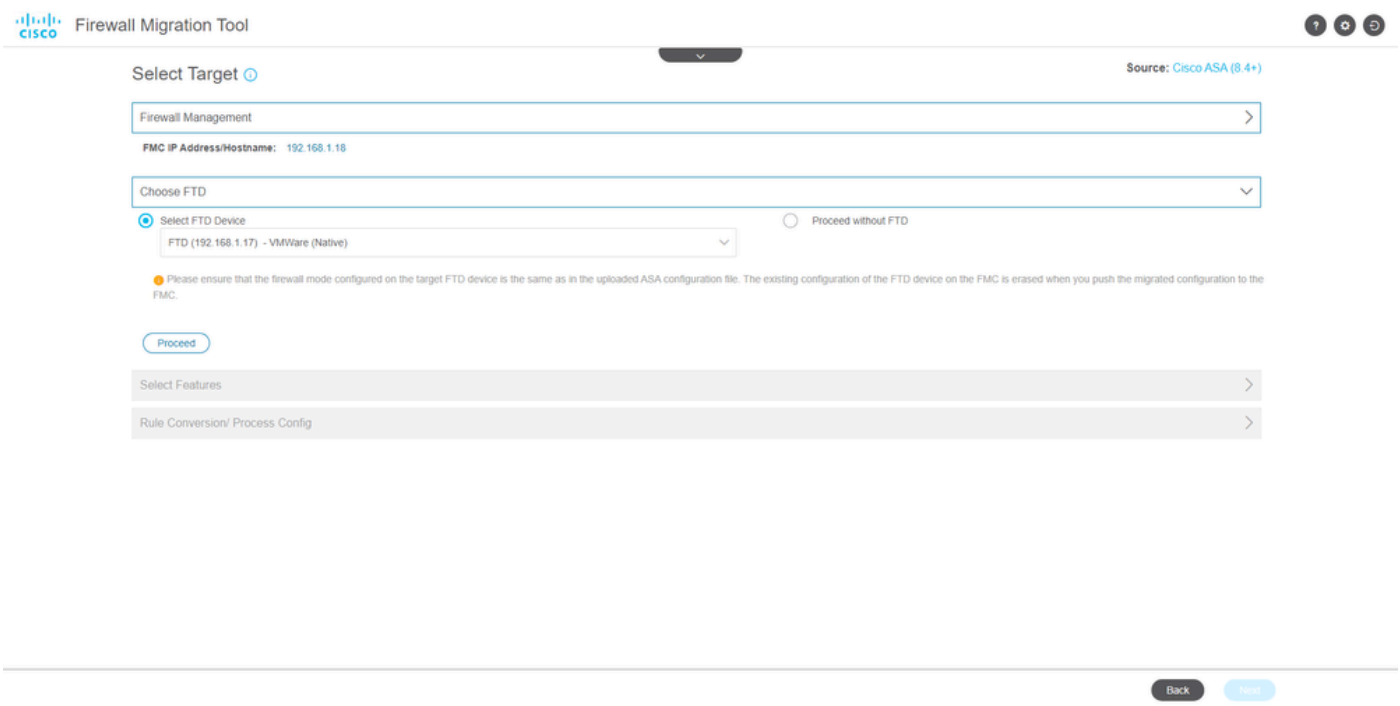
Fornire l'indirizzo IP del CCP.Verrà aperta una finestra popup in cui verranno richieste le credenziali di accesso del CCP.



IP FMC

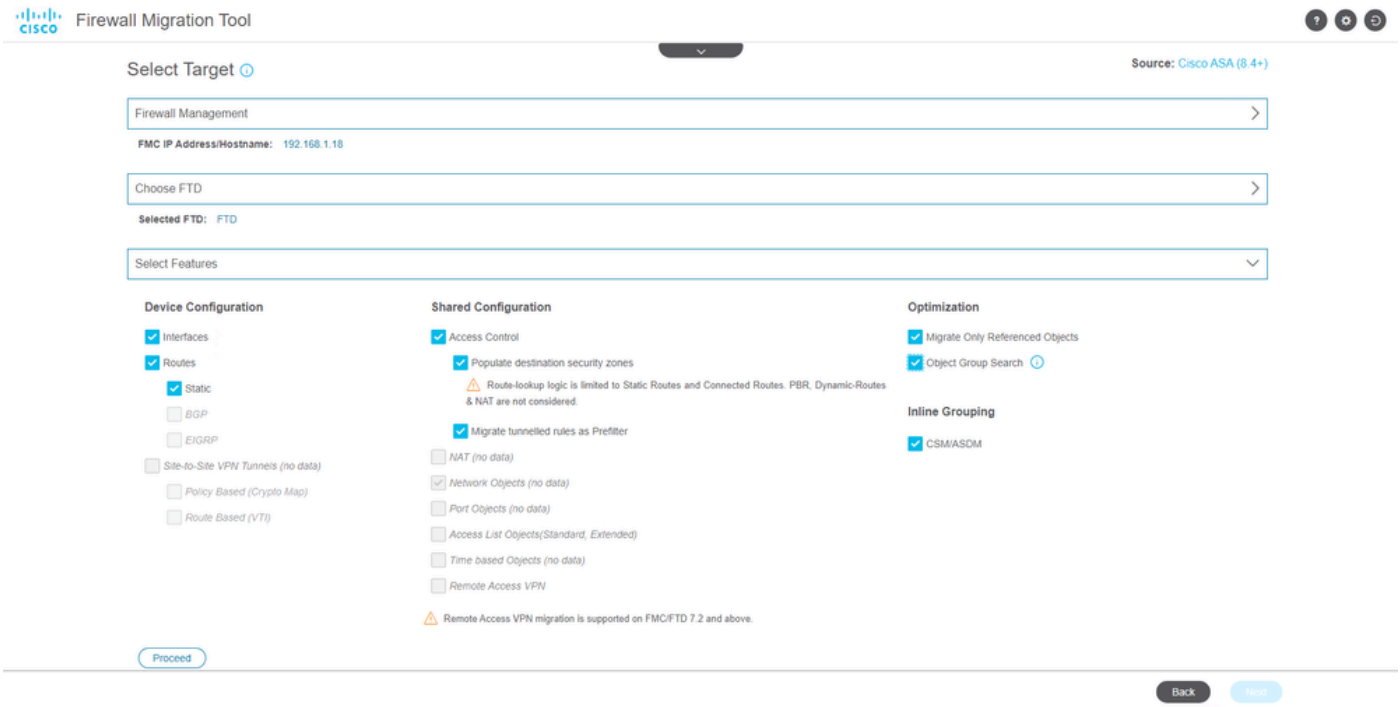
9. (Facoltativo) Selezionare l'FTD di destinazione che si desidera utilizzare.
    1. Se si sceglie di eseguire la migrazione a un FTD, selezionare l'FTD che si desidera utilizzare.
    2. Se non si desidera utilizzare un FTD, è possibile compilare la casella di controllo Proceed

without FTD



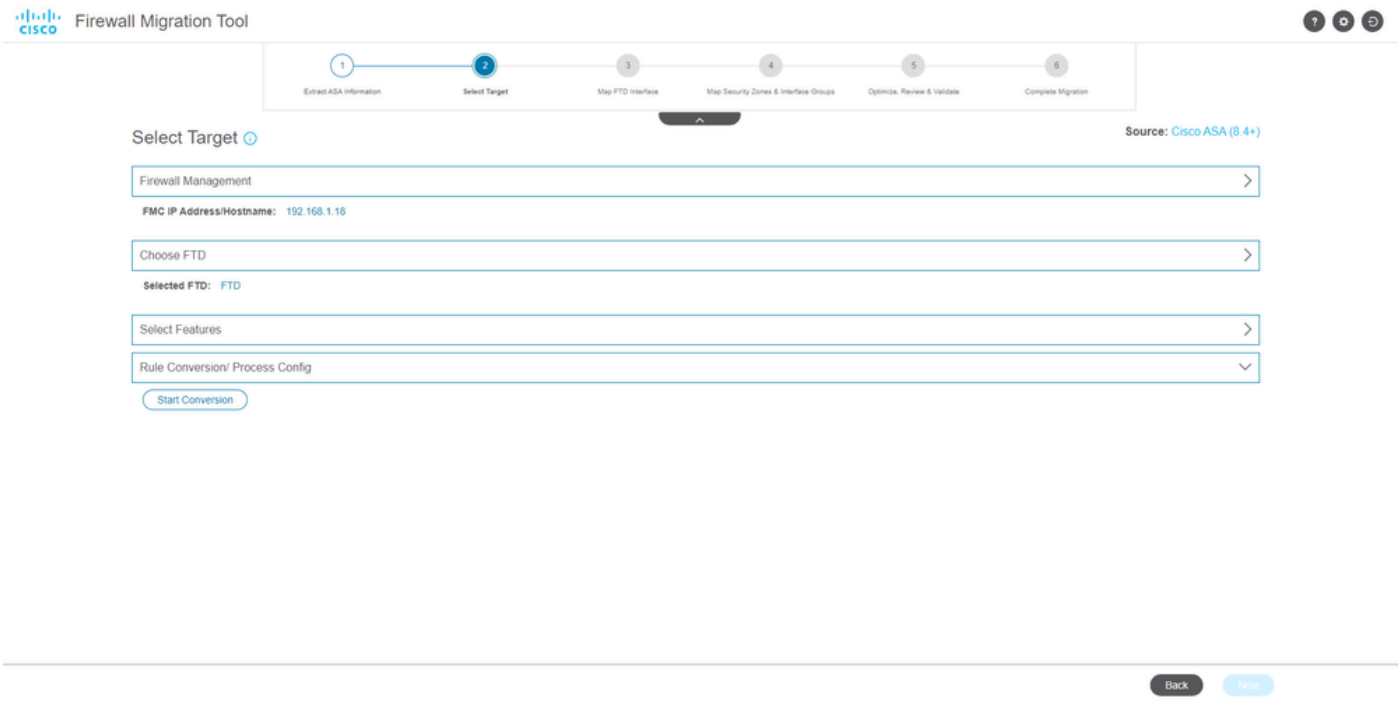
FTD destinazione

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



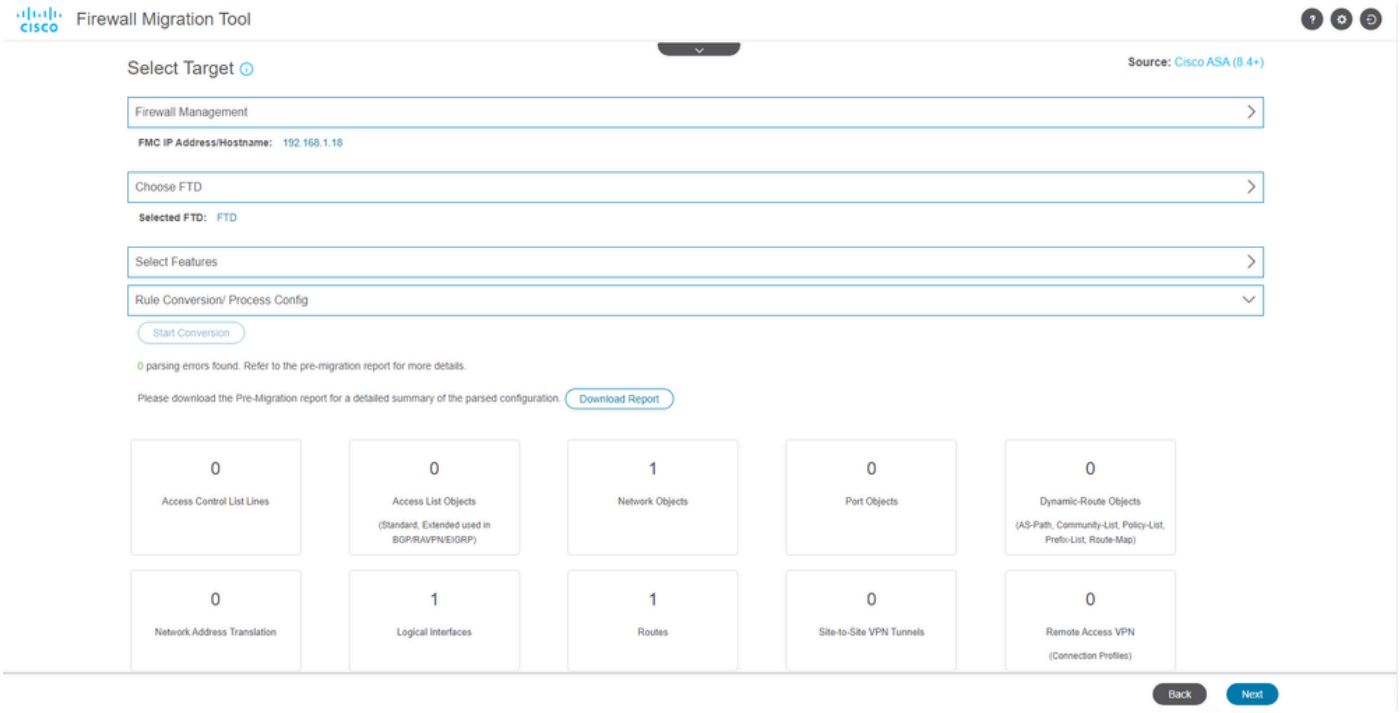
Configurazioni

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



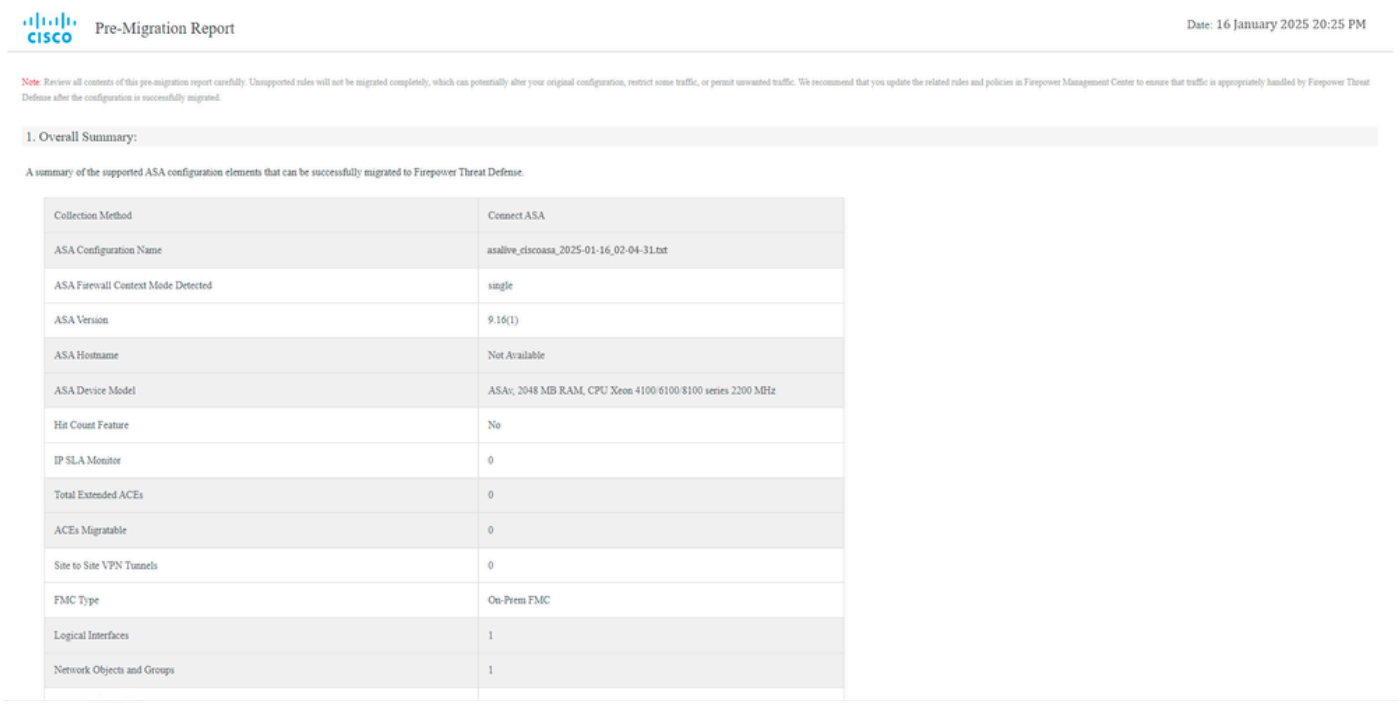
Avvia conversione

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



Scarica rapporto

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



Pre-Migration Report

Date: 16 January 2025 20:25 PM

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.

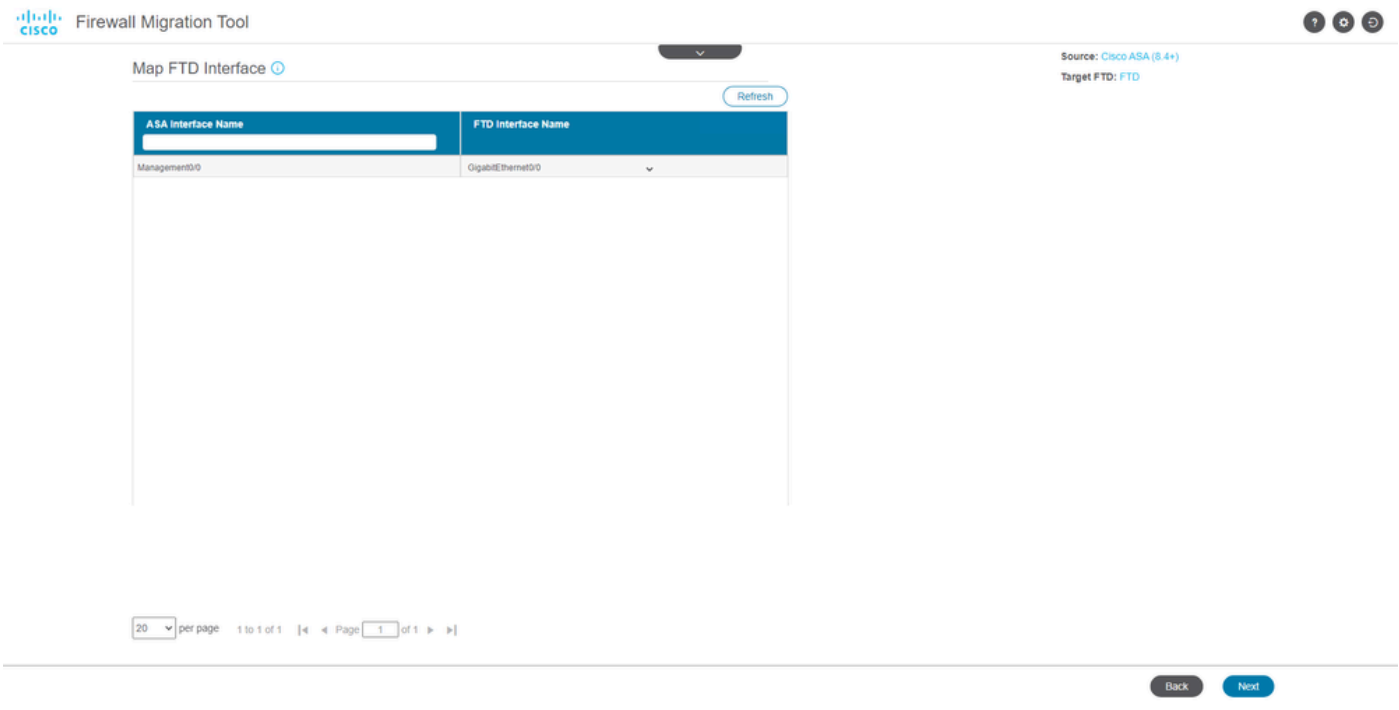
1. Overall Summary:

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

Collection Method	Connect ASA
ASA Configuration Name	asalive_ciscoasa_2025-01-16_02-04-31.txt
ASA Firewall Context Mode Detected	single
ASA Version	9.16(1)
ASA Hostname	Not Available
ASA Device Model	ASAv, 2048 MB RAM, CPU Xeon 4100/6100/8100 series 2200 MHz
Hit 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

Report pre-migrazione

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

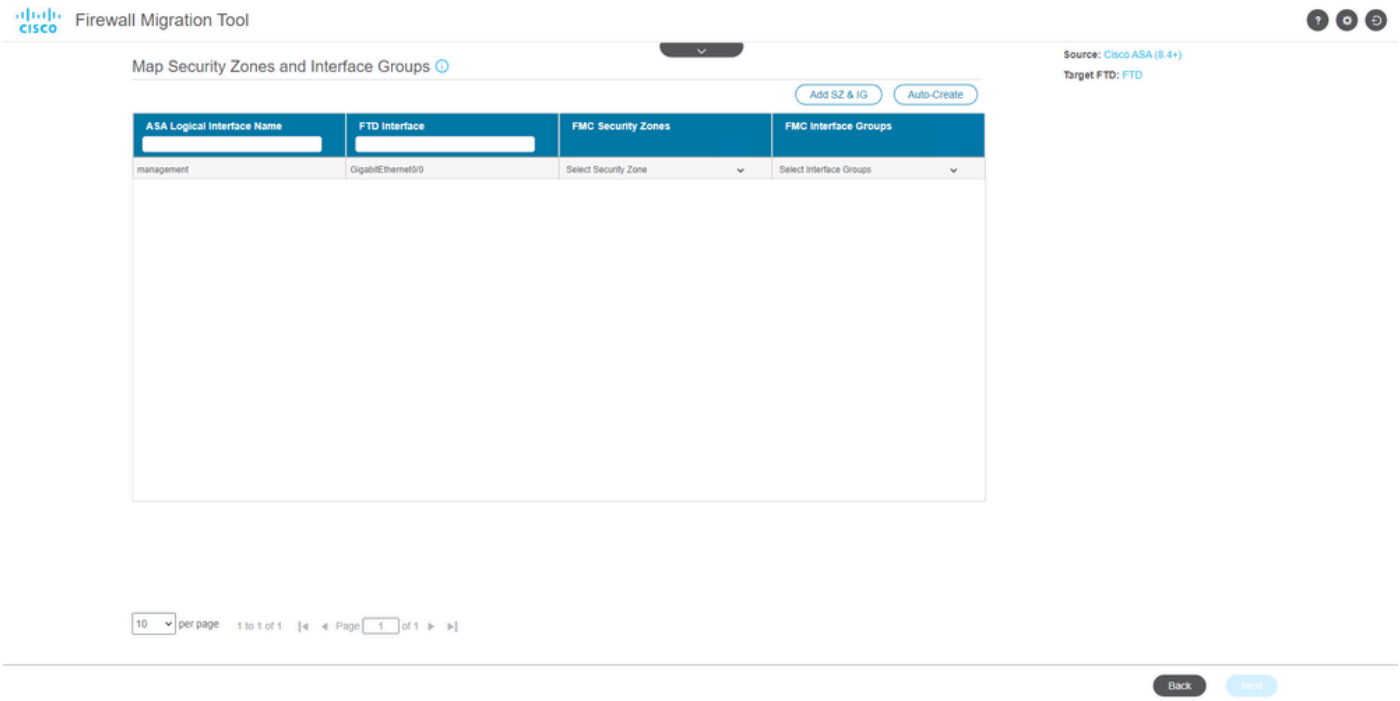
ASA Interface Name	FTD Interface Name
Management0/0	GigabitEthernet0/0

20 per page 1 to 1 of 1 Page 1 of 1

Back Next

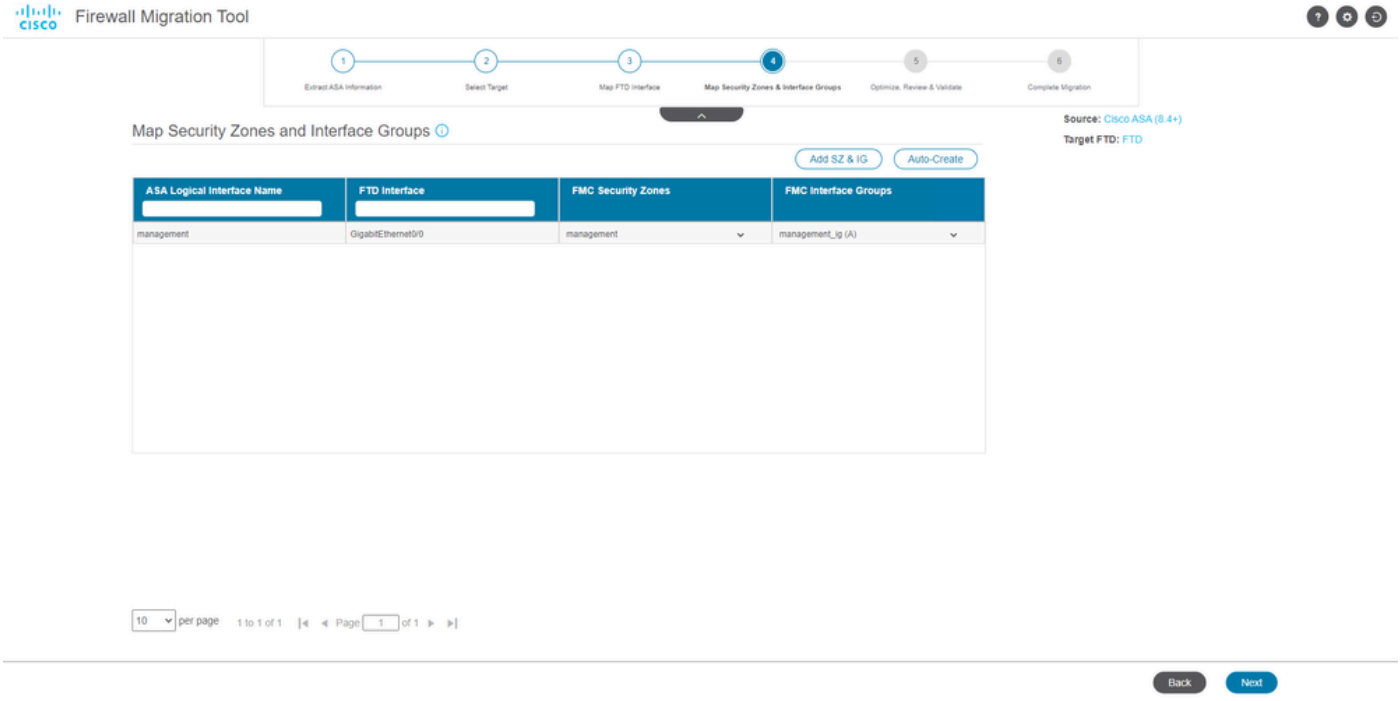
Mapping interfacce

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



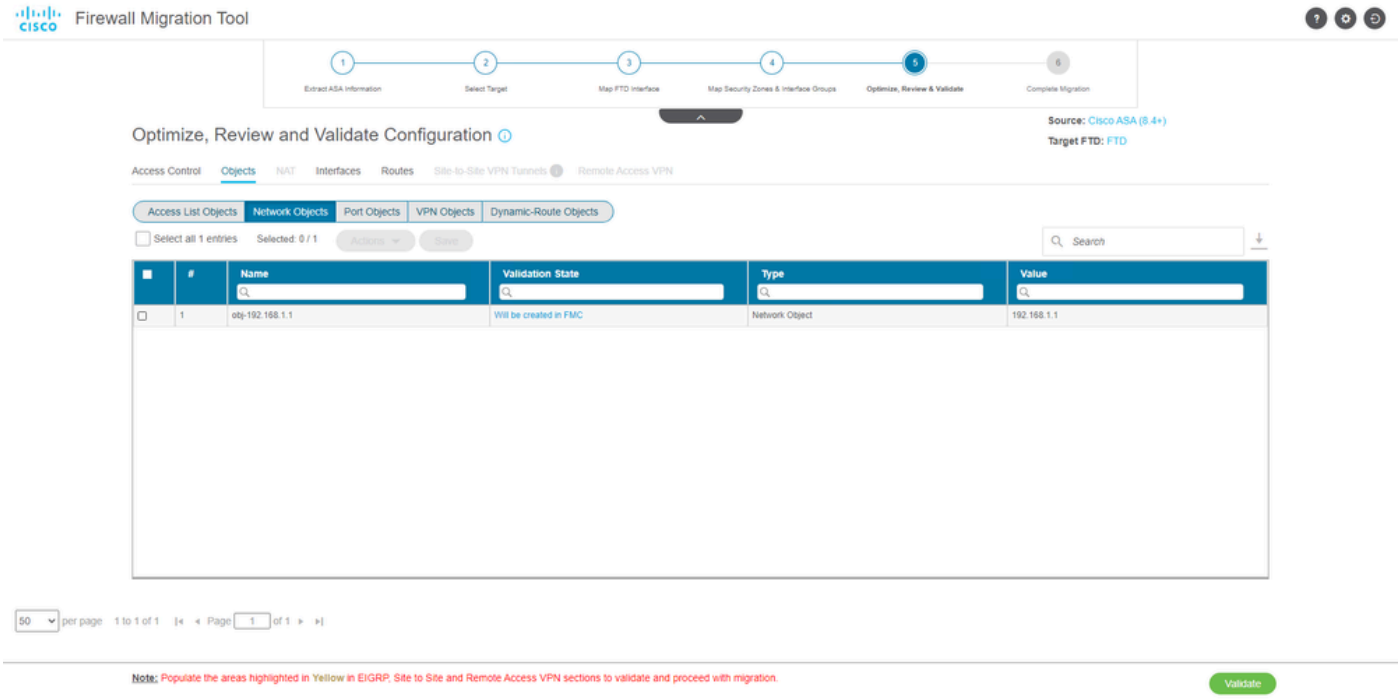
Aree di sicurezza e gruppi di interfaccia

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



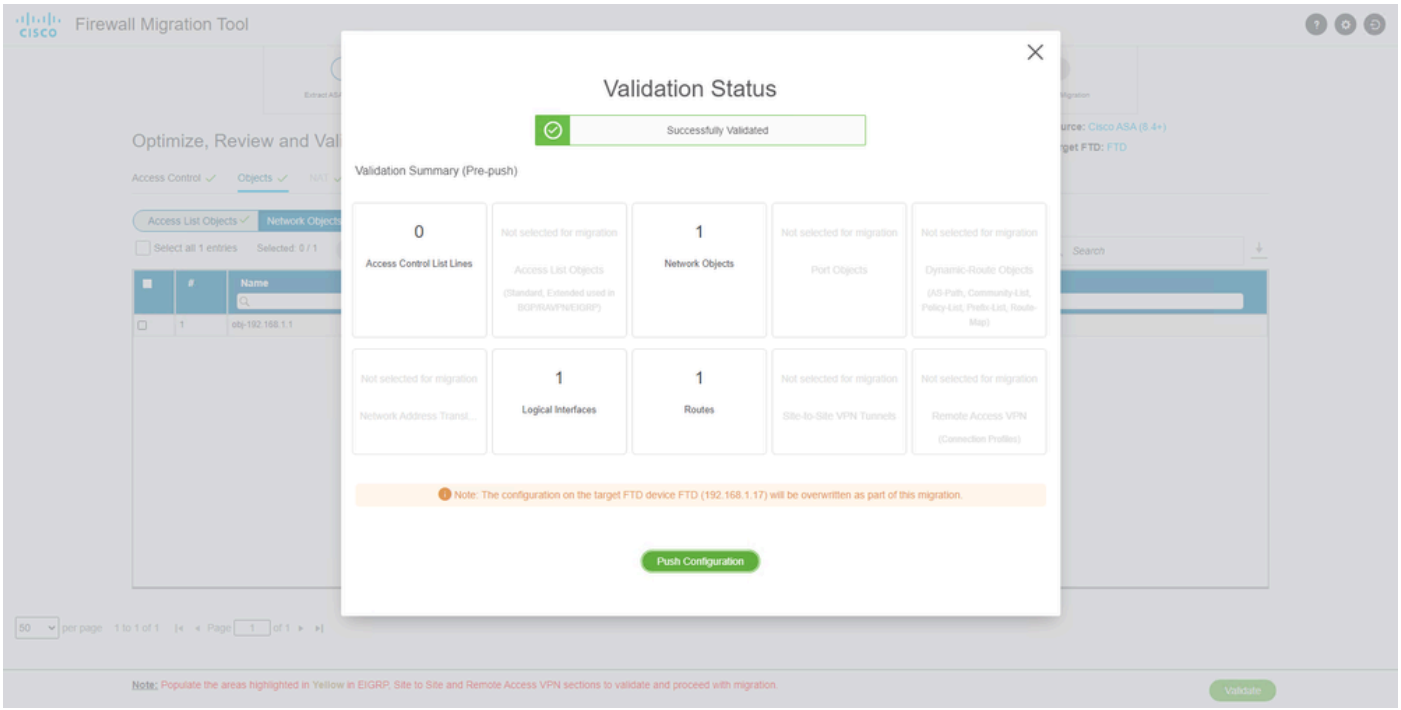
Crea automaticamente, strumento

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



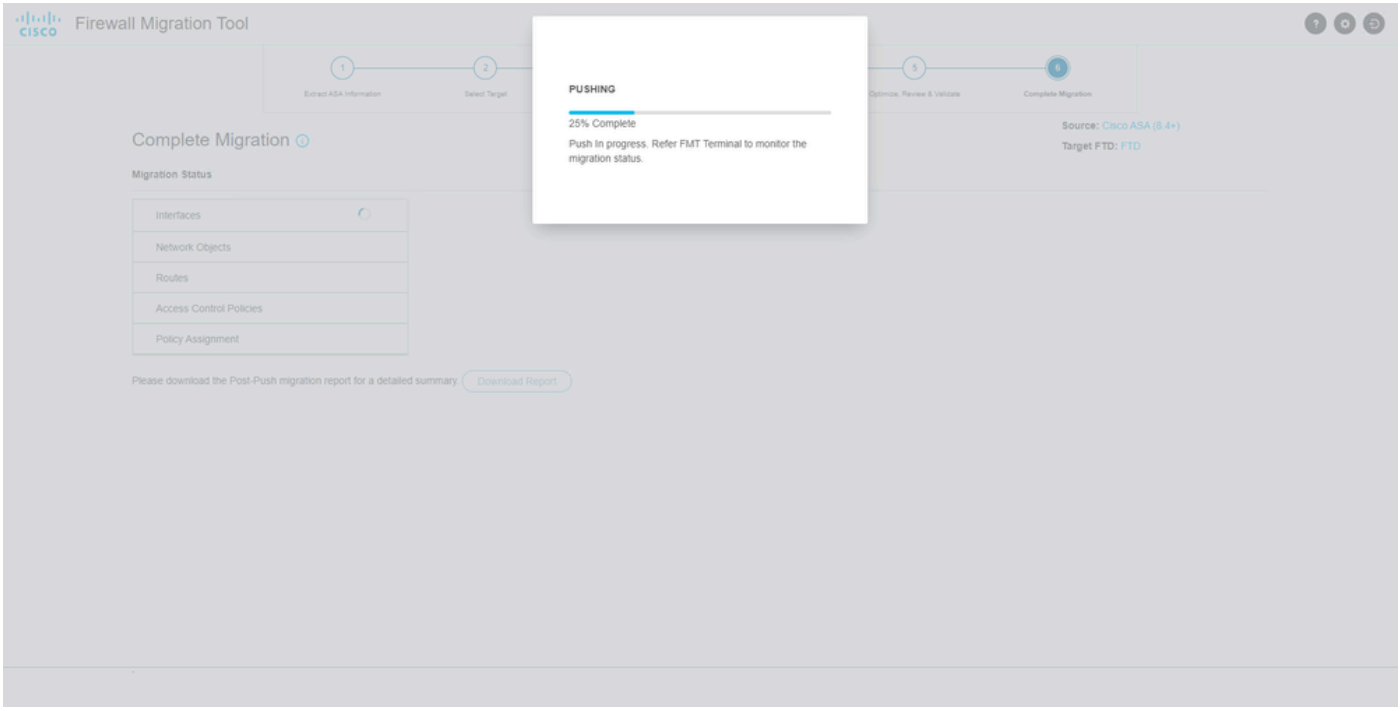
Verifica e convalida

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



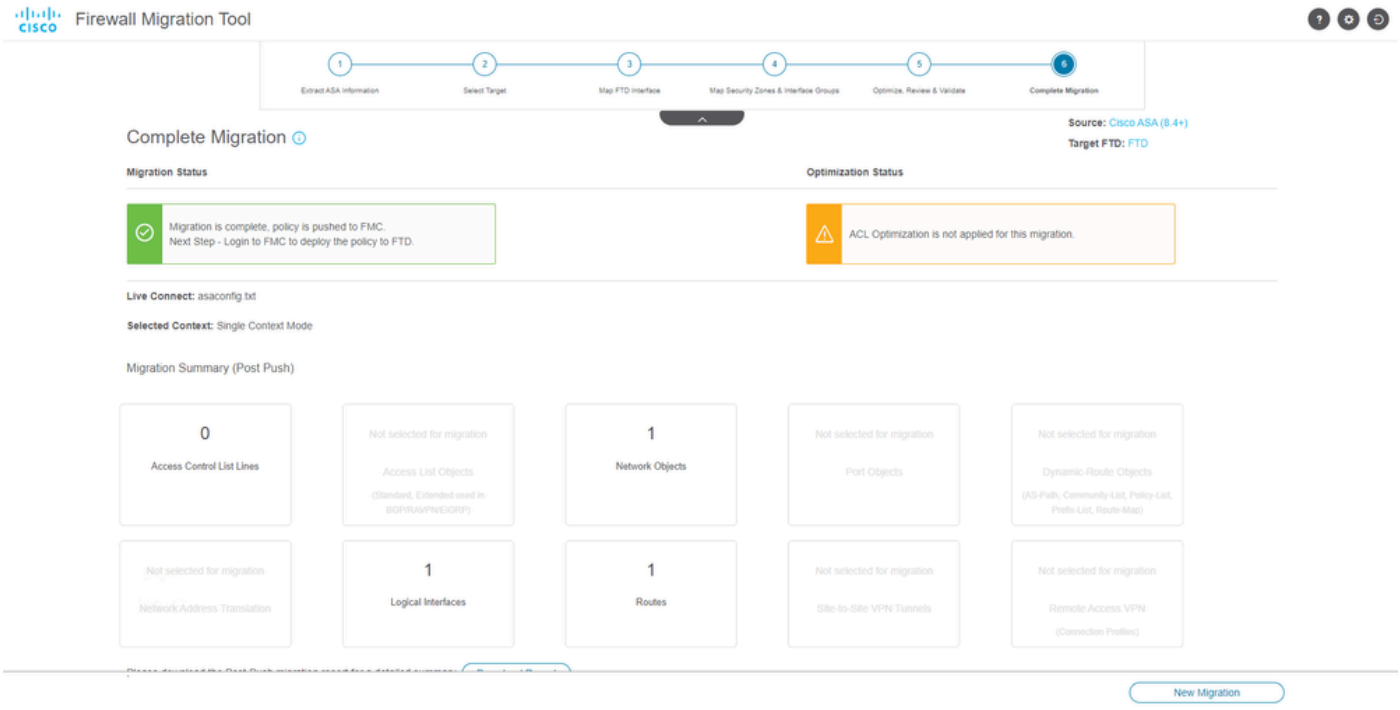
Convalida

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



Spingi

Esempio di migrazione riuscita, come mostrato nell'immagine:



Migrazione completata

(Facoltativo) Se si è scelto di eseguire la migrazione della configurazione in un FTD, è necessaria una distribuzione per eseguire il push della configurazione disponibile dal FMC al firewall.

Per distribuire la configurazione:

1. Accedere alla GUI del CCP.
2. Passare allaDeployscheda.

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

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 ASA.
    - Elementi di configurazione mancanti o incompleti.
    - Problemi di connettività di rete o latenza.
    - Problemi durante il caricamento del file di configurazione ASA o il push della configurazione al centro di gestione.
    - I problemi più comuni sono:
- 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 di 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.
    - Lo strumento consente di scaricare un bundle di supporto per i file di log, il database e i file di configurazione.
    - Passaggi da scaricare:
    - Per ulteriore supporto:

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).