Migrazione da Paloalto a Firepower Threat Defense tramite FMT

Sommario

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.

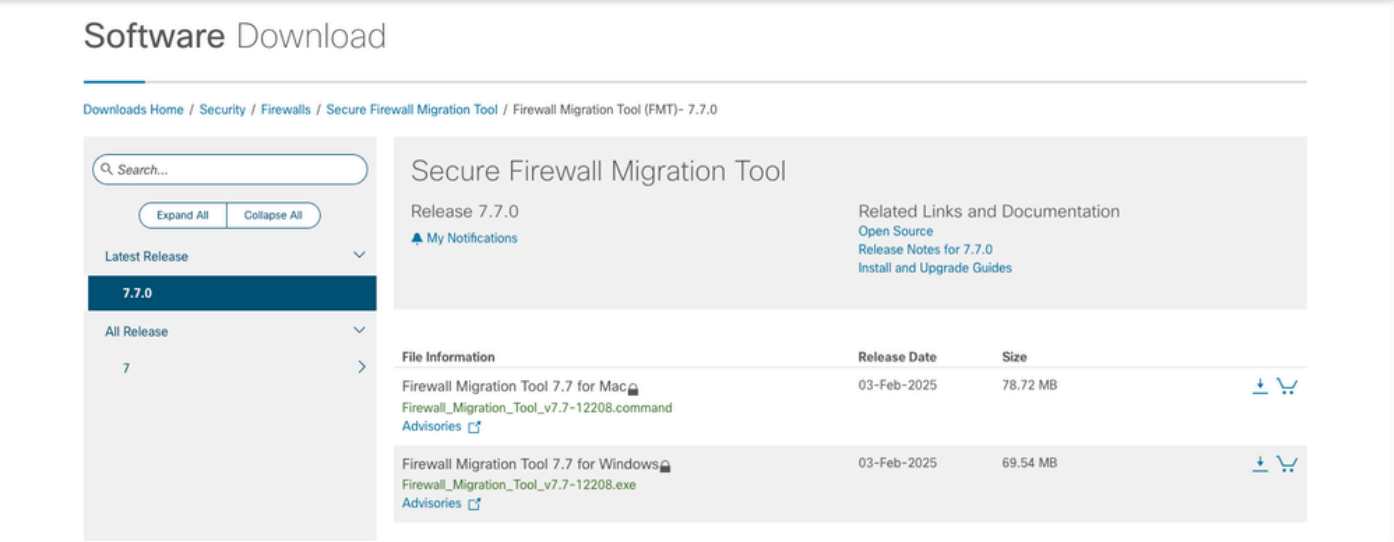
Elenco di controllo pre-migrazione

- 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

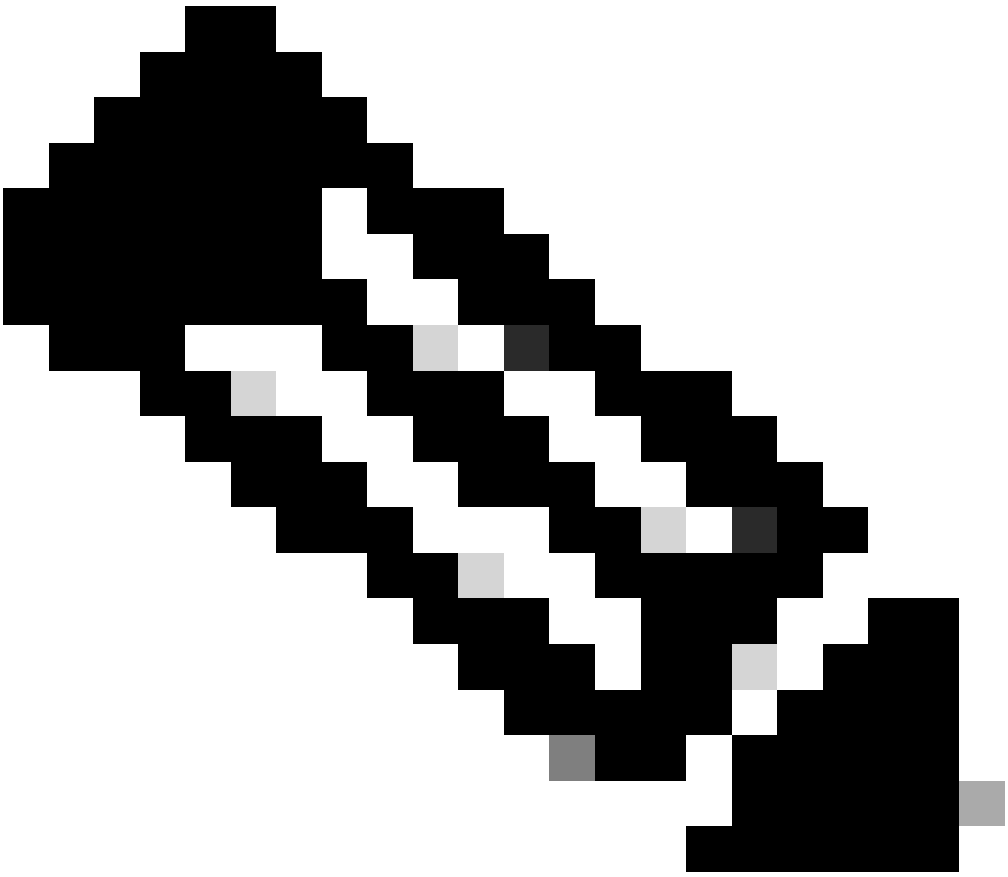
Fasi della migrazione

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



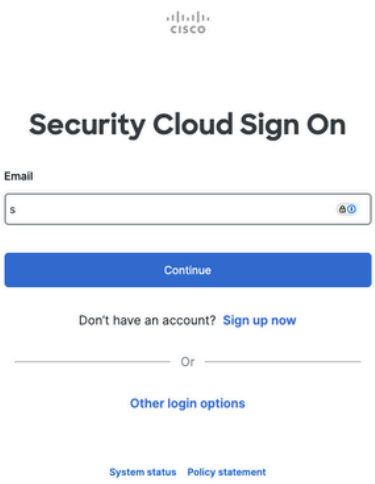
Download FMT

3. Aprire il file precedentemente scaricato sul computer.



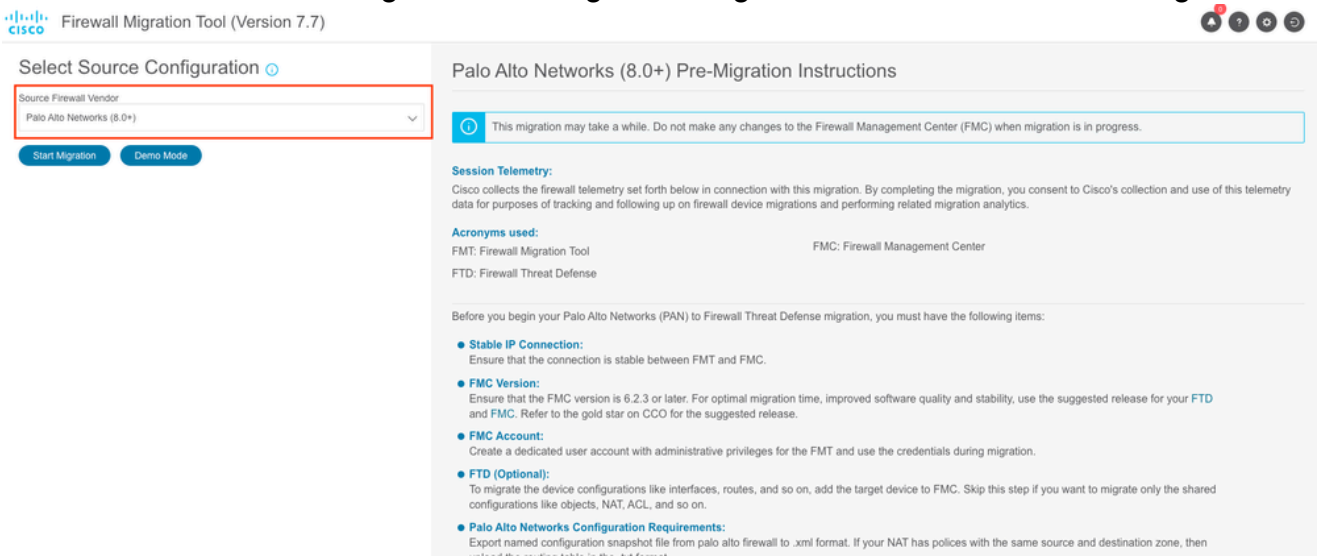
Nota: Il programma si apre automaticamente e una console genera automaticamente il contenuto nella directory in cui è stato eseguito il file.

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.



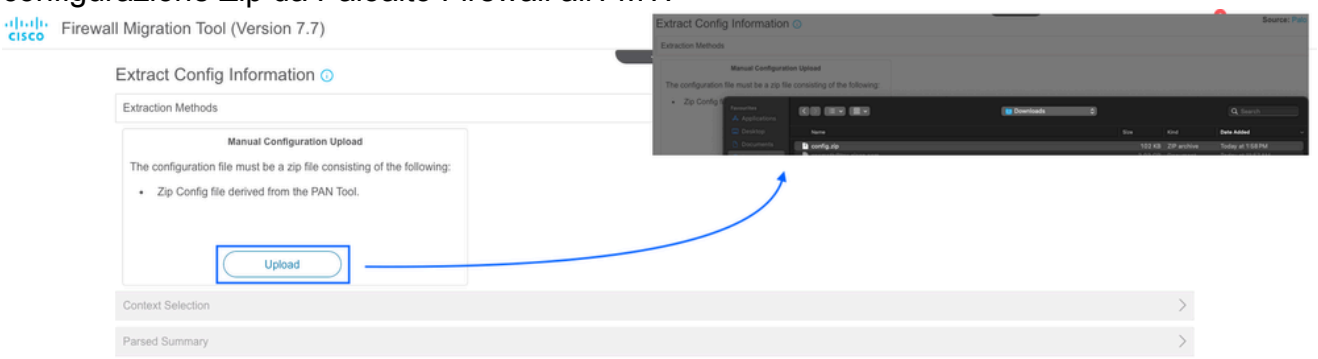
Prompt di accesso FMT

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



GUI FMT

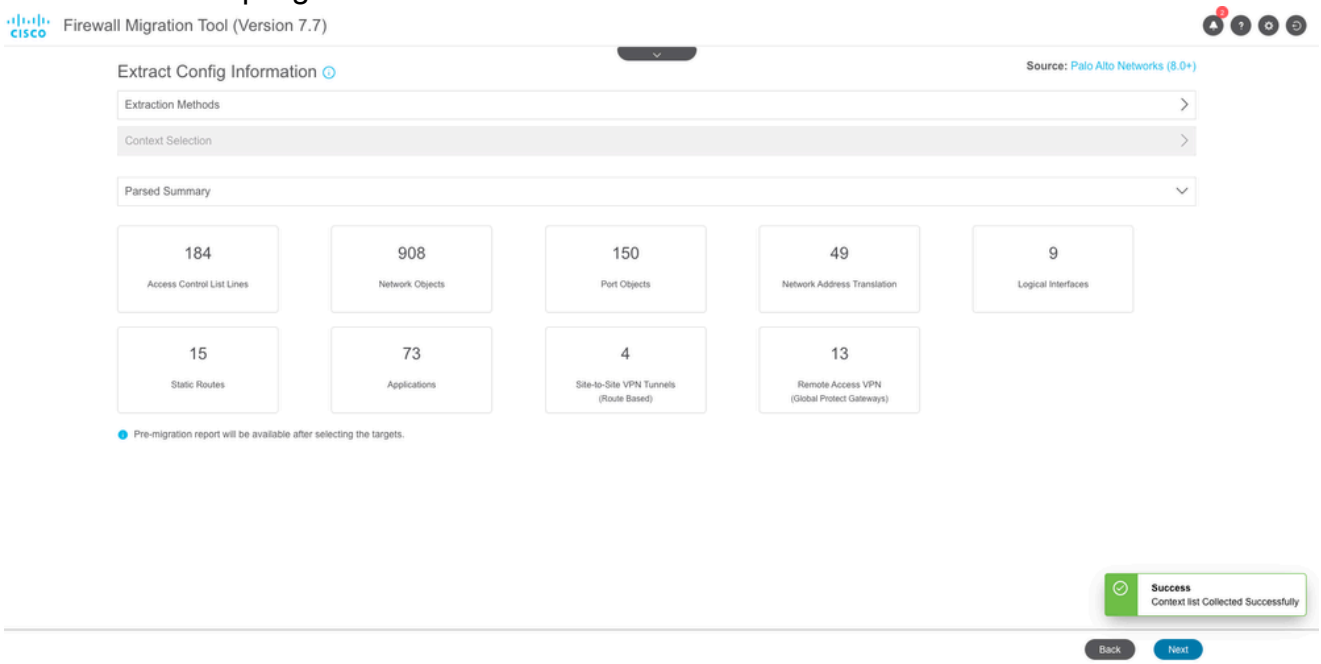
7. Viene visualizzata la sezione Metodi di estrazione, in cui è necessario caricare il file di configurazione Zip da Paloalto Firewall all'FMT.



Caricamento guidato della configurazione

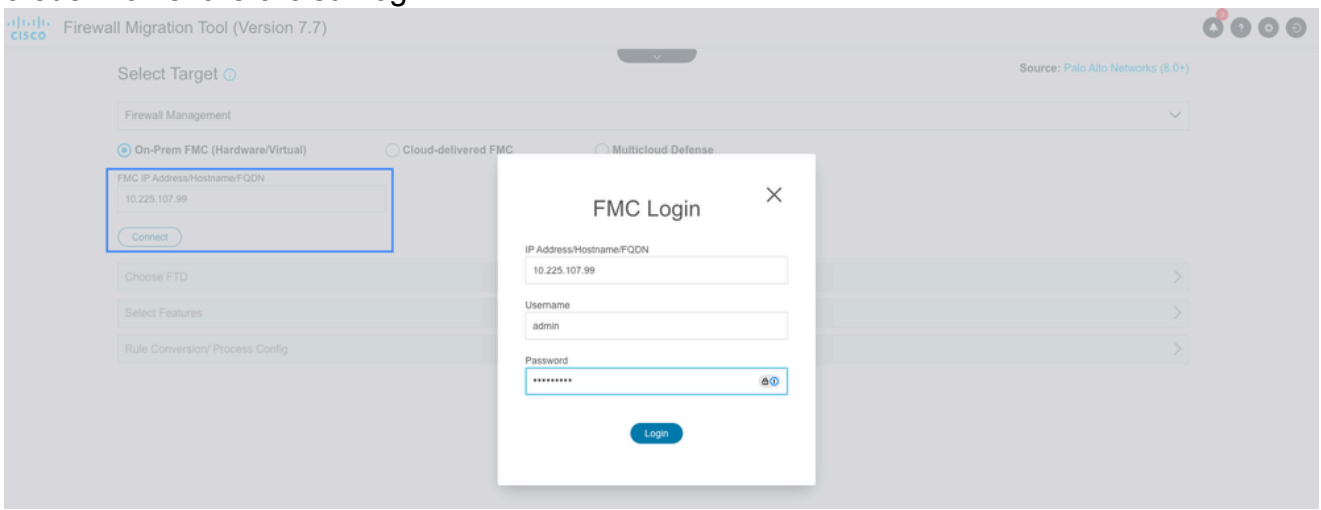
8. Il riepilogo della configurazione analizzata viene visualizzato dopo il caricamento del file di configurazione. Nel caso di VSYS, sono disponibili selezioni VSYS separate. Ciascuno di

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



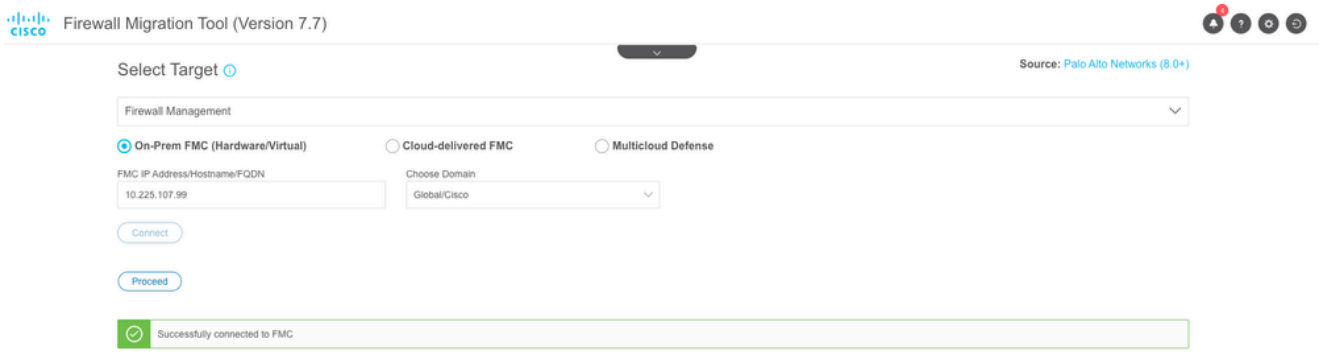
Riepilogo della convalida della configurazione

9. 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.



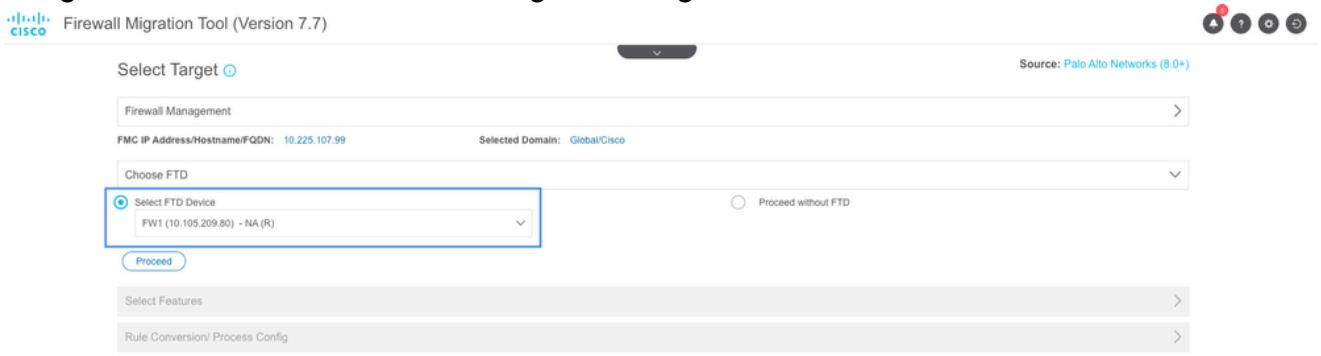
Accesso a FMC

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



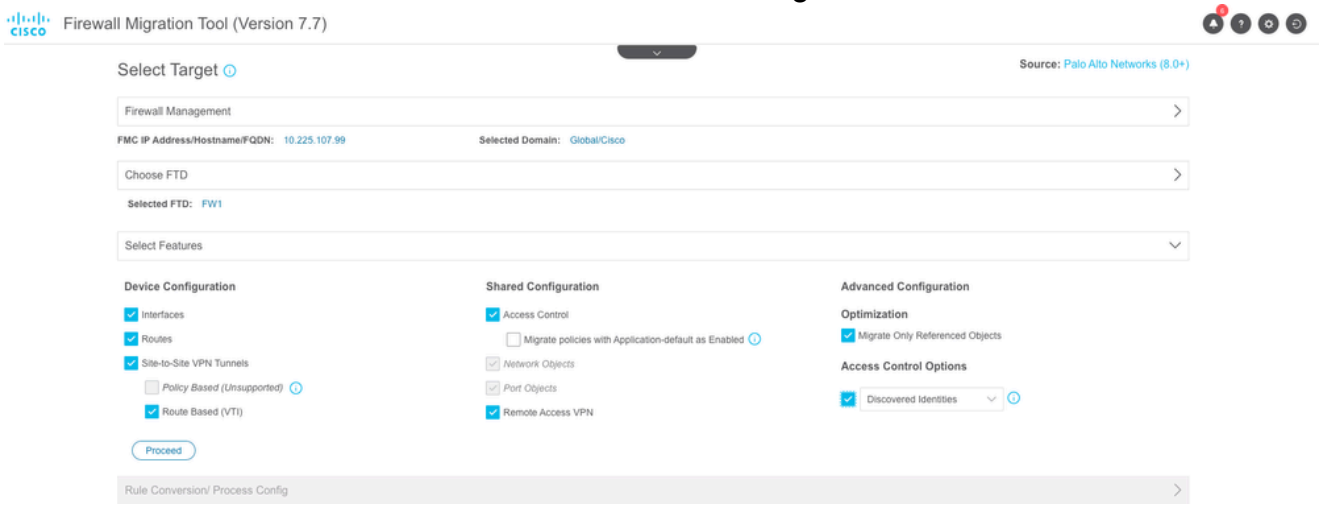
Selezione dominio

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

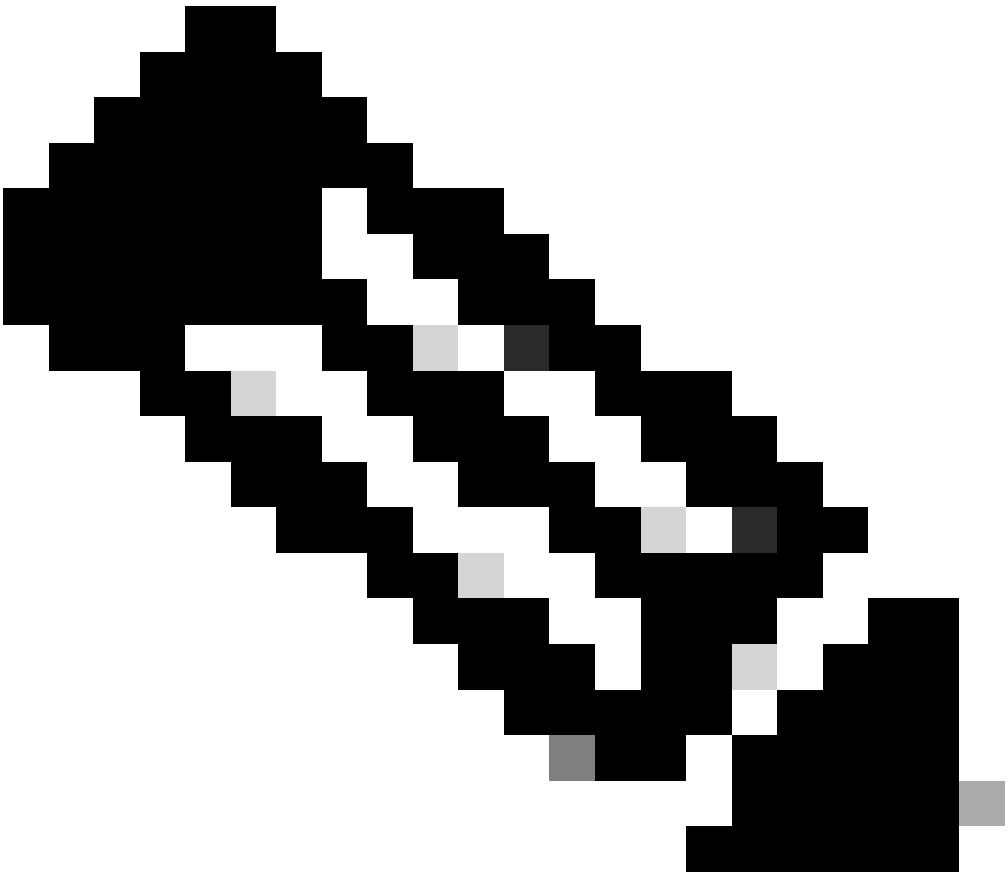


Seleziona FTD di destinazione

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

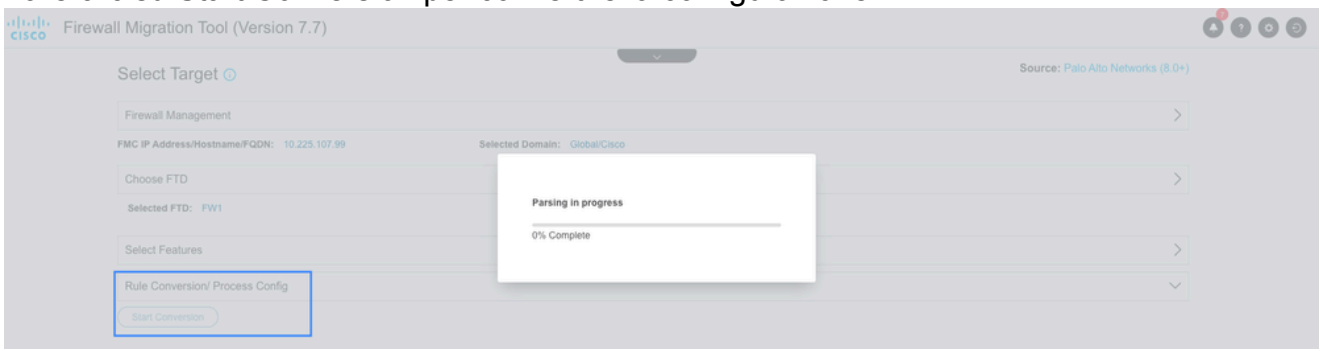


Selezione funzionalità



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

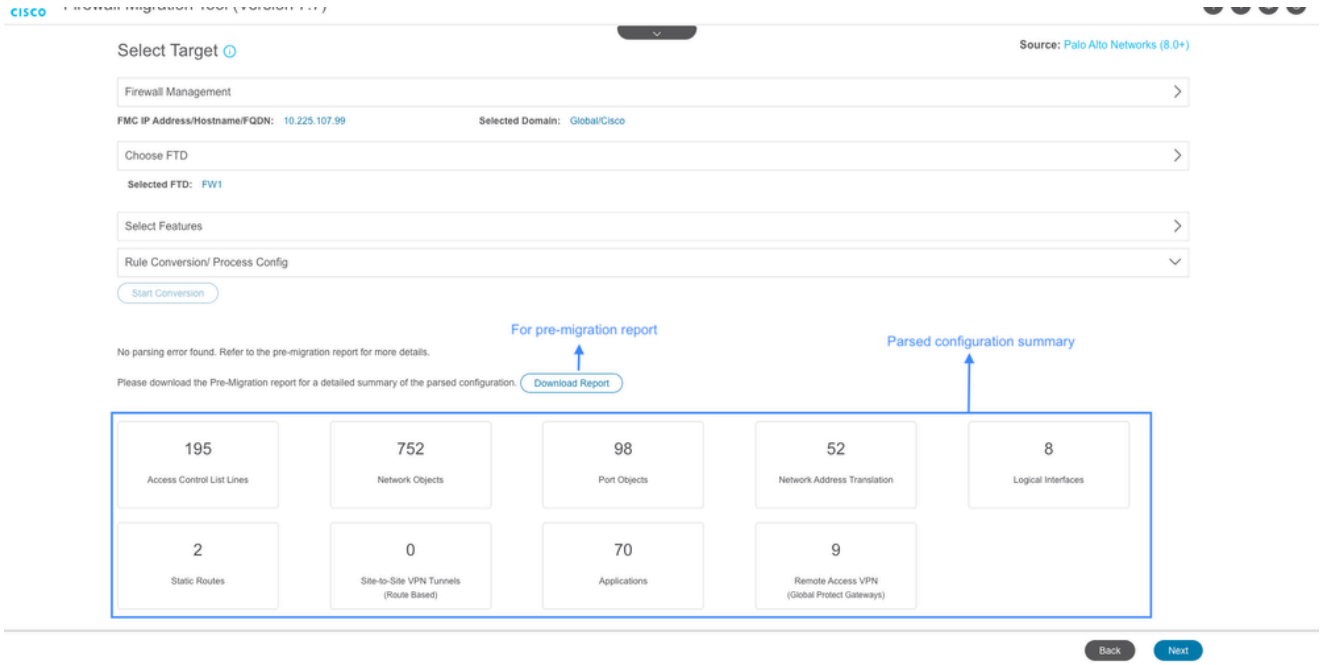
13. Fare clic su Start Conversion per convertire la configurazione.



Analisi della configurazione

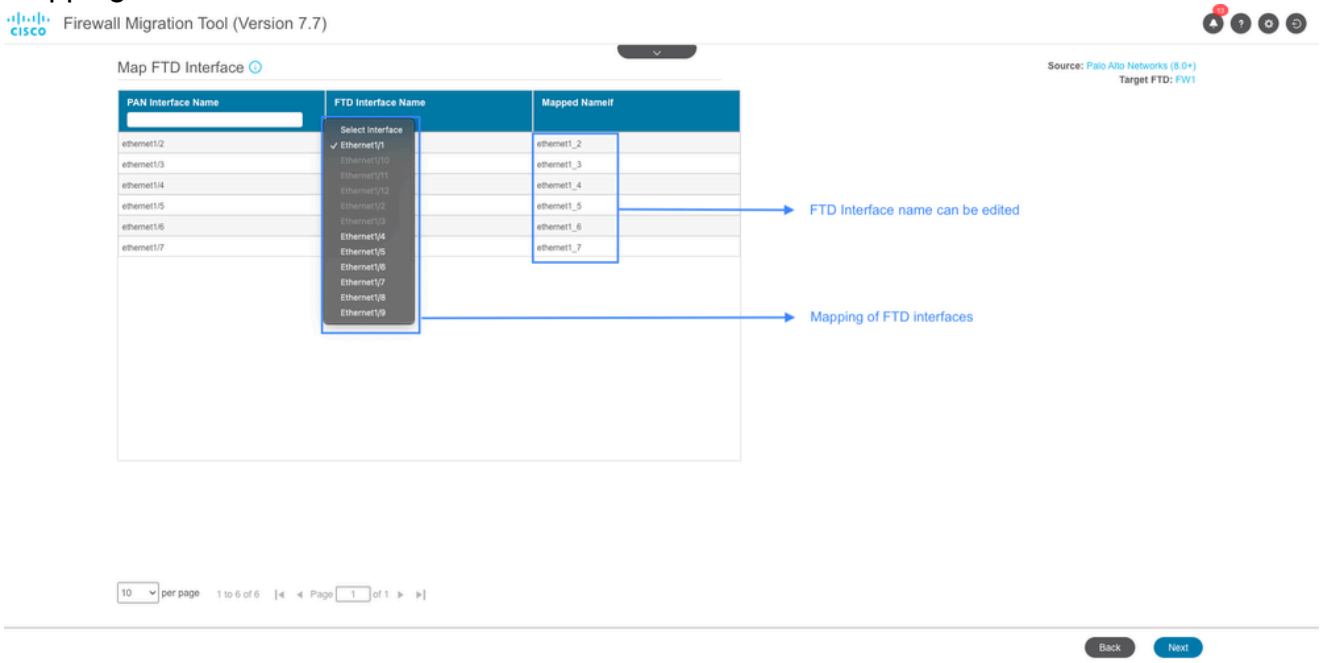
Lo strumento analizza la configurazione e visualizza il riepilogo della conversione come mostrato nell'immagine. È inoltre possibile scaricare il Report pre-migrazione per convalidare la configurazione migrata in caso di errori o avvisi, se presenti. Passare alla pagina

successiva facendo clic su Avanti.



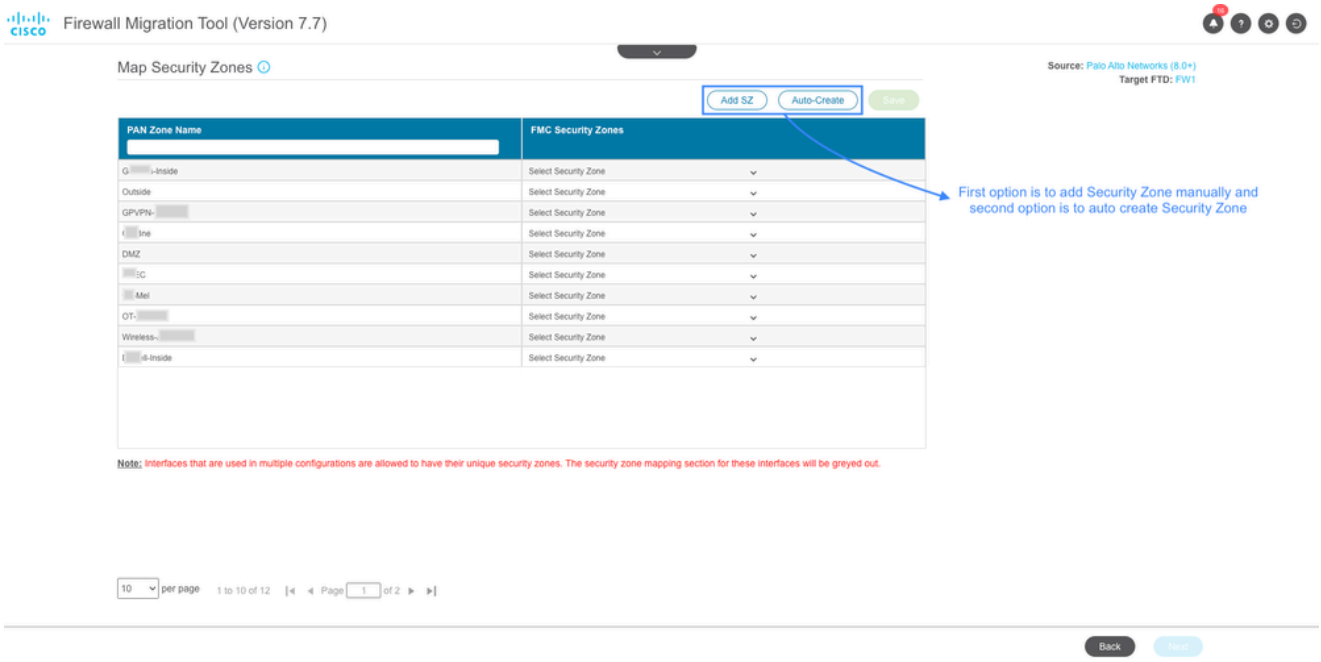
Riepilogo configurazione analizzata

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.



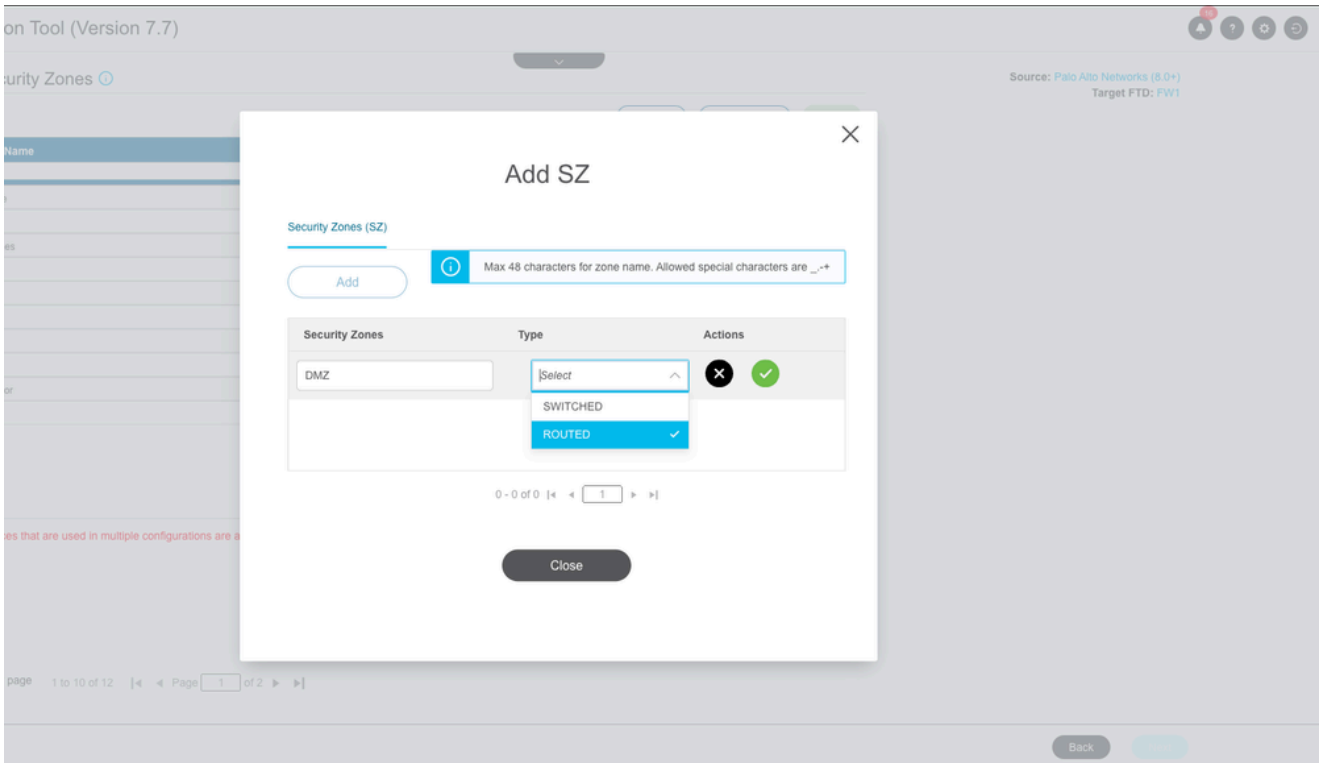
Mappatura interfaccia

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.



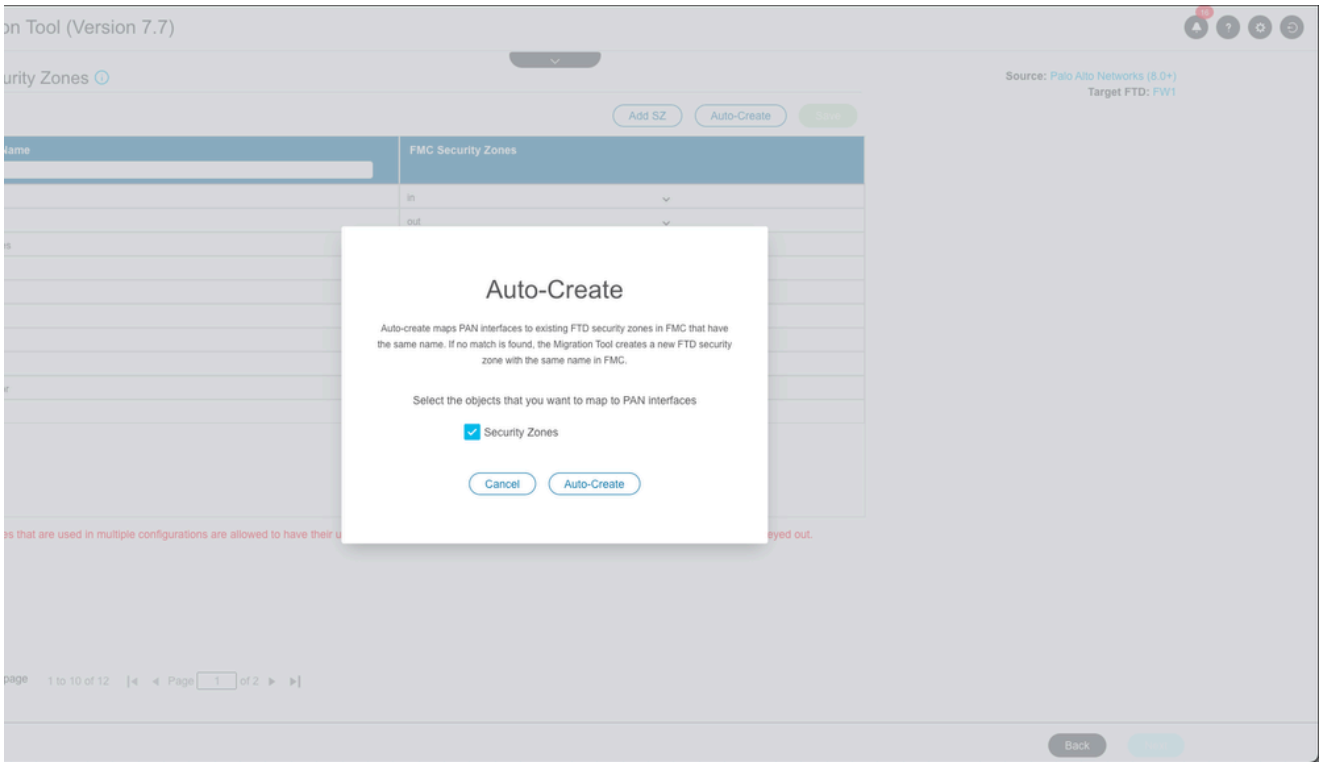
Creazione area di sicurezza

Creazione manuale delle aree di protezione:



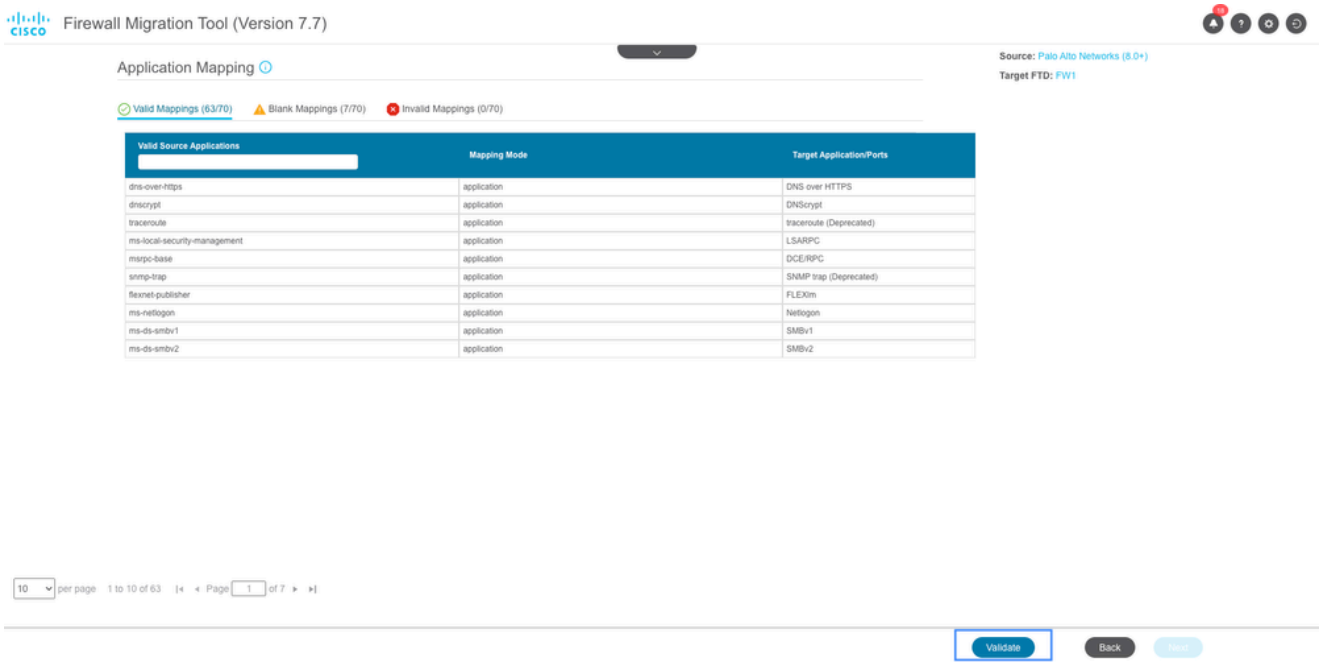
Creazione manuale area di sicurezza

Creazione automatica aree di protezione:

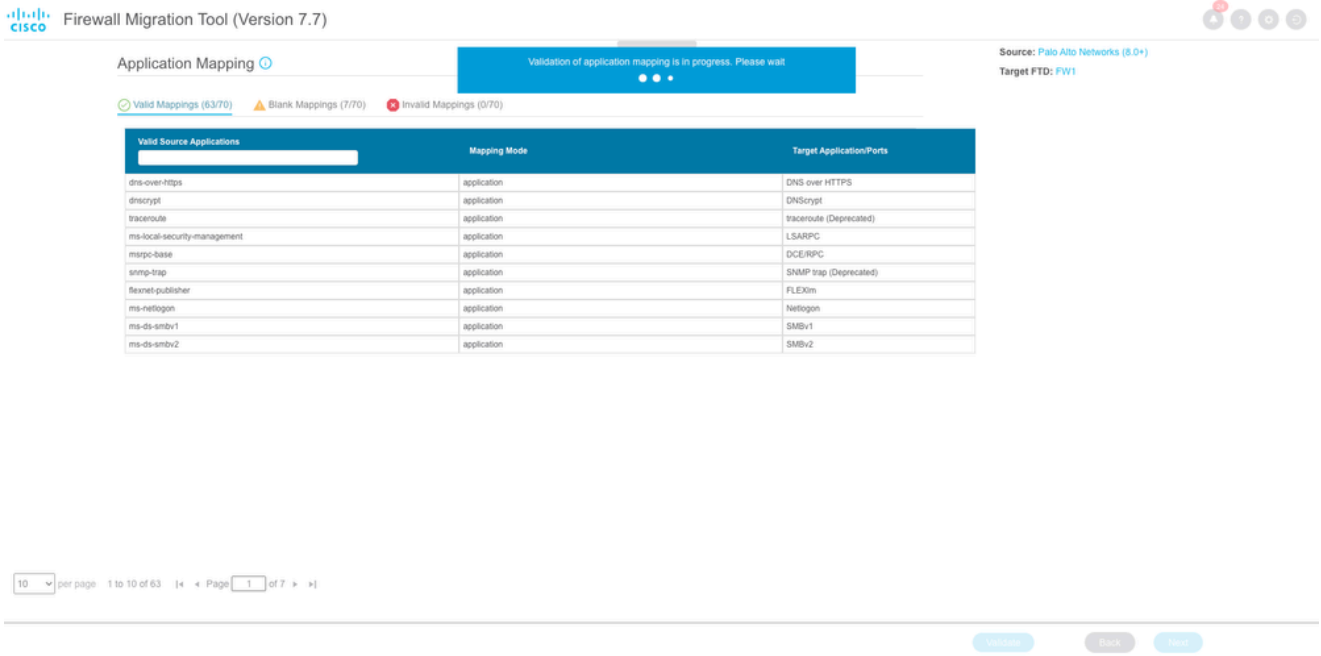


Creazione automatica area di sicurezza

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



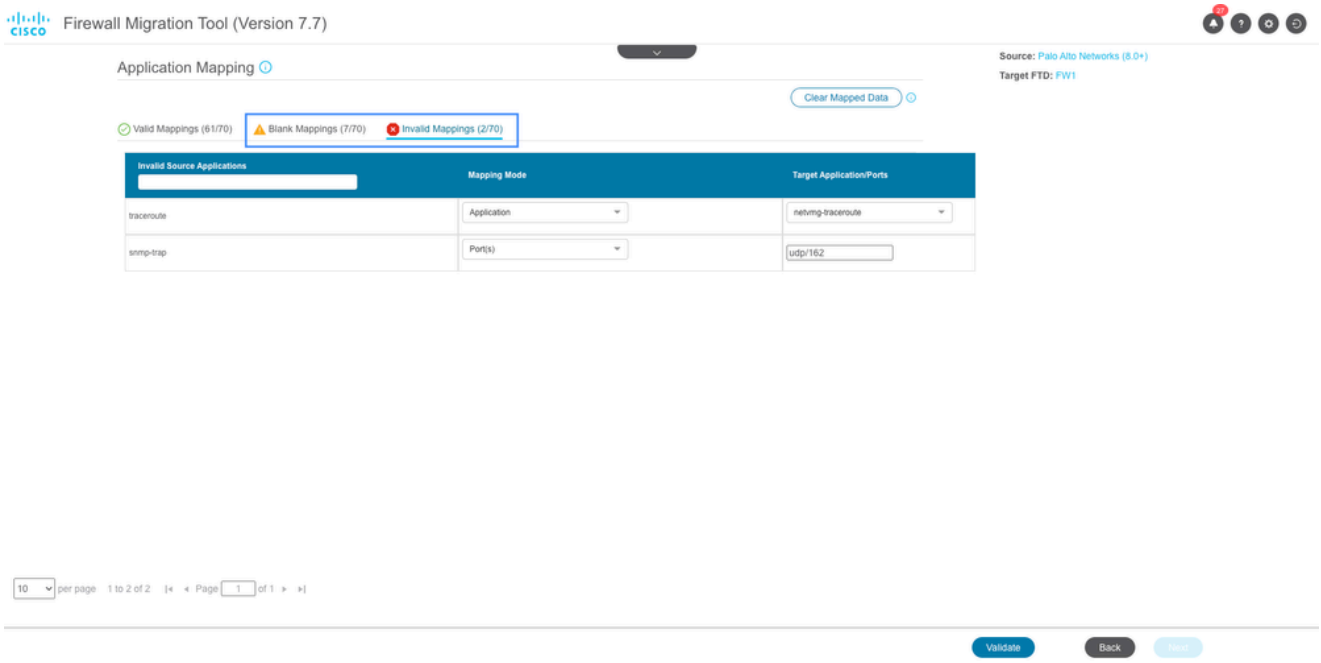
Mapping applicazione



Convalida mapping applicazioni

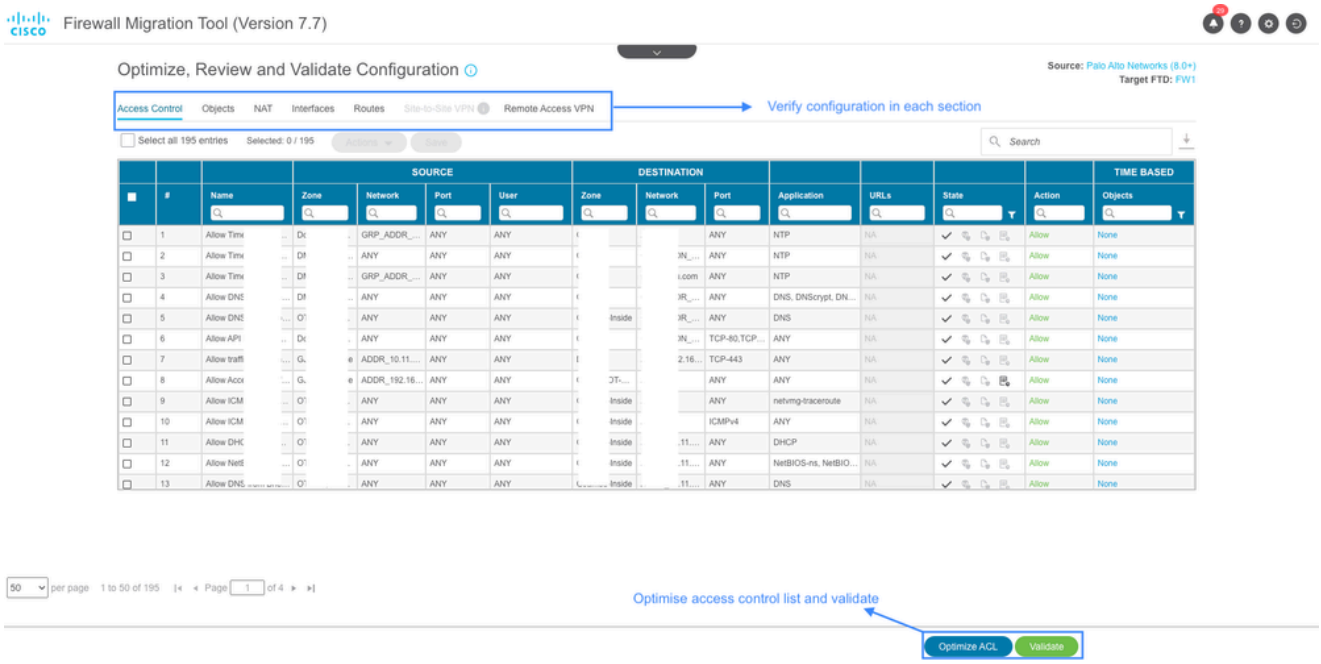
Al momento della convalida, FMT elenca i mapping vuoti e non validi. I mapping non validi devono essere corretti prima di procedere e la correzione dei mapping vuoti è facoltativa.

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



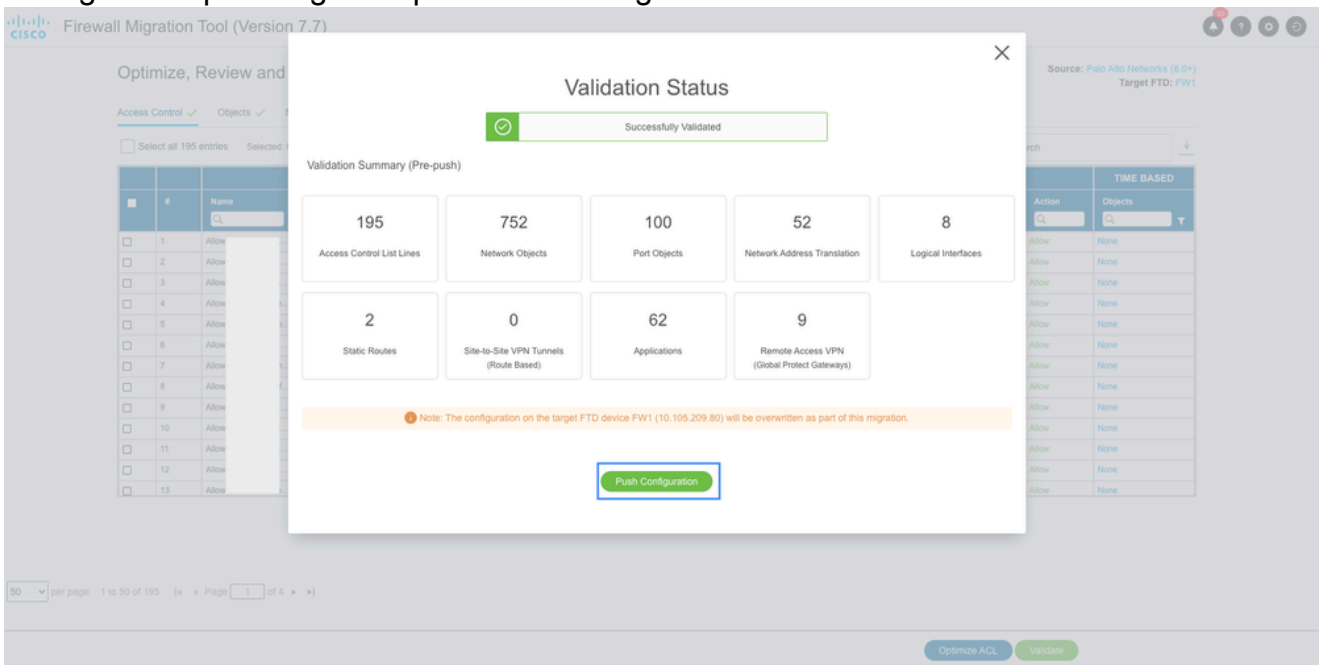
Mapping applicazione vuoto e non valido

17. 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.



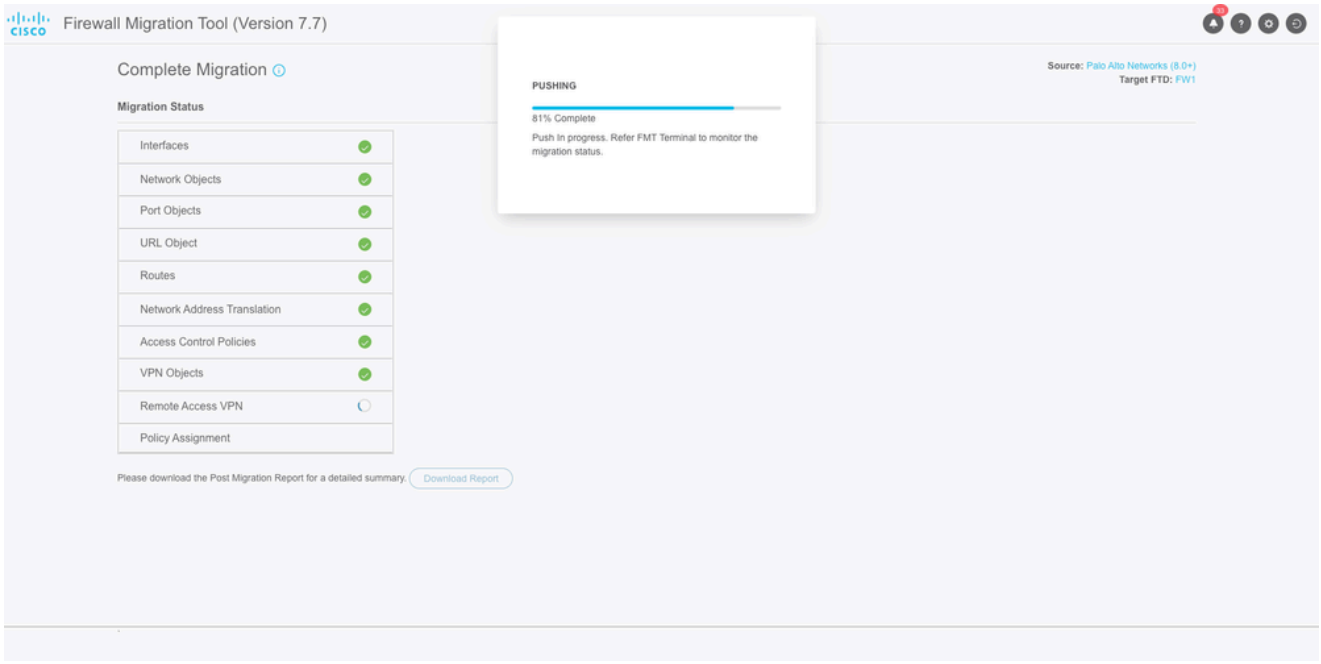
Convalida configurazione

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.



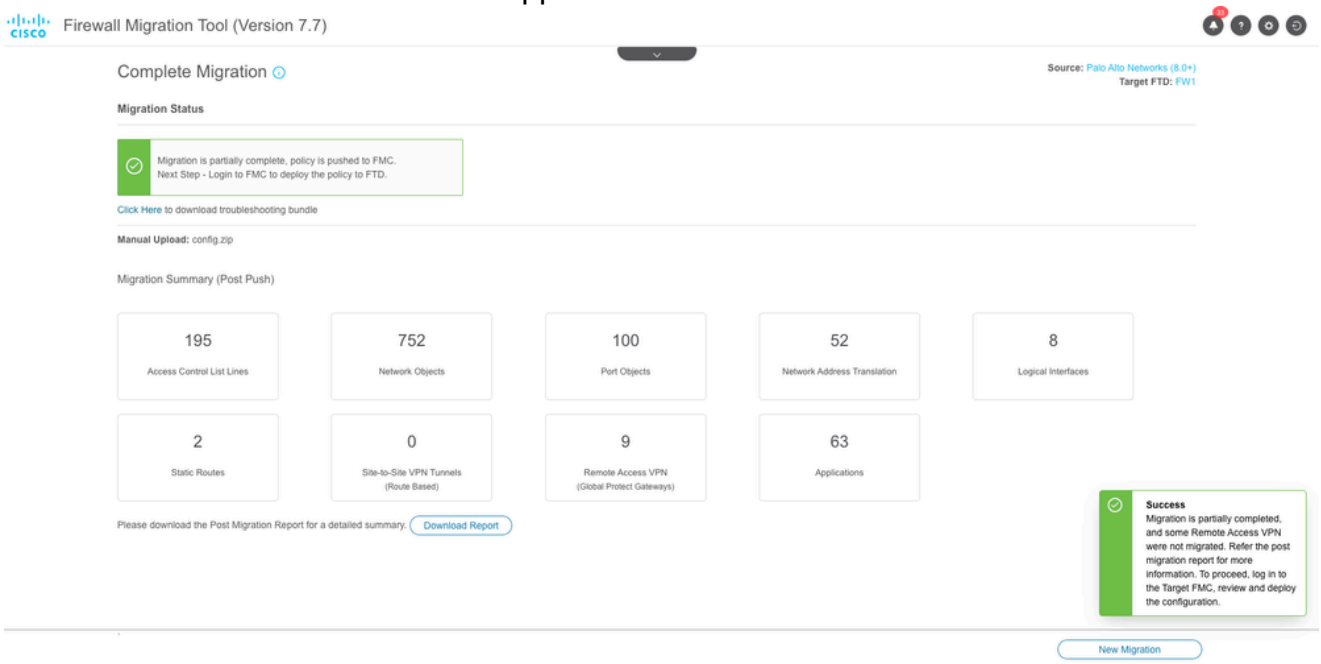
Riepilogo della convalida della configurazione

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).