Transizione perfetta: Migrazione da Palo Alto Firewall a Cisco FTD

Sommario

Introduzione

Questo documento descrive il processo di transizione da un firewall di Palo Alto a un sistema Cisco FTD utilizzando la versione 6.0 di FMT.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

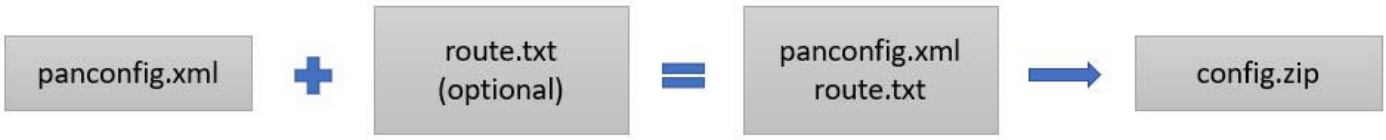
- Esportazione della configurazione corrente dal firewall di Palo Alto in formato XML (*.xml).
- Accesso alla CLI di Palo Alto Firewall ed esecuzione del comando show routing route, quindi salvataggio dell'output come file di testo (*.txt).
- Compressione del file di configurazione (*.xml) e del file di output di routing (*.txt) in un unico archivio ZIP (*.zip).

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Palo Alto Firewall versione 8.4.x

o successive.

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.



Firepower Migration Tool (FMT)

L'FMT aiuta i team di progettazione nella transizione dei firewall dei fornitori esistenti a Cisco Next-Generation Firewall (NGFW)/Firepower Threat Defense (FTD). Assicurarsi di utilizzare la versione più recente di FMT, scaricata dal sito Web Cisco.

Linee guida per la migrazione

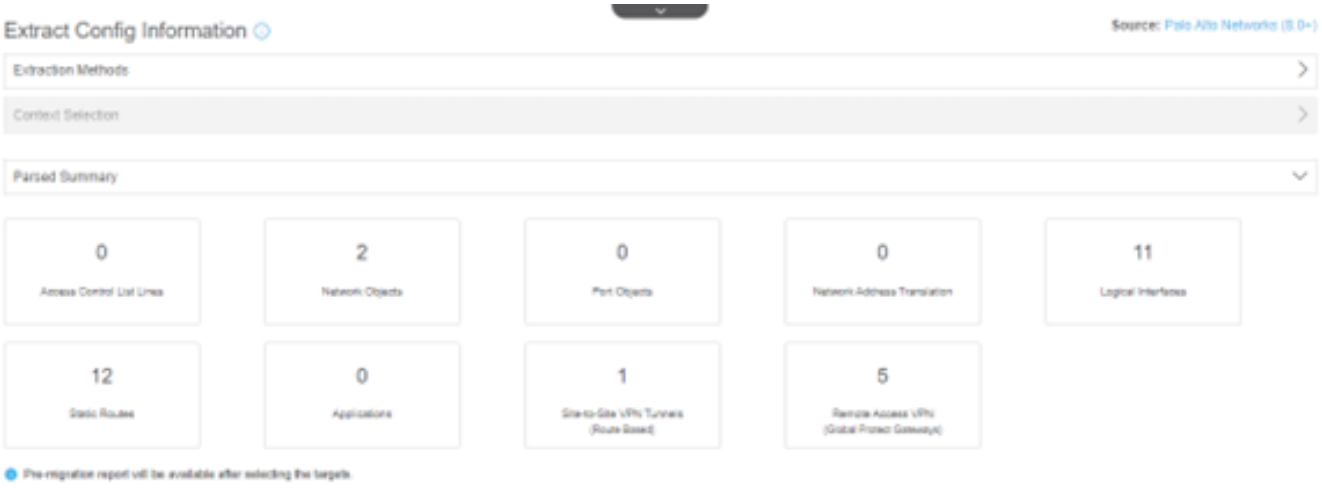
1. Elenco di controllo pre-migrazione

- Accertarsi che l'FTD sia stato aggiunto al CCP prima di iniziare il processo di migrazione.
- È stato creato un nuovo account utente con privilegi amministrativi nel CCP.
- Palo Alto esportato che esegue il file di configurazione.xml deve essere compresso con un'estensione di .zip.
- NGFW/FTD deve avere lo stesso numero di interfacce fisiche o secondarie o di canali di porta uguale alle interfacce firewall di Palo Alto.

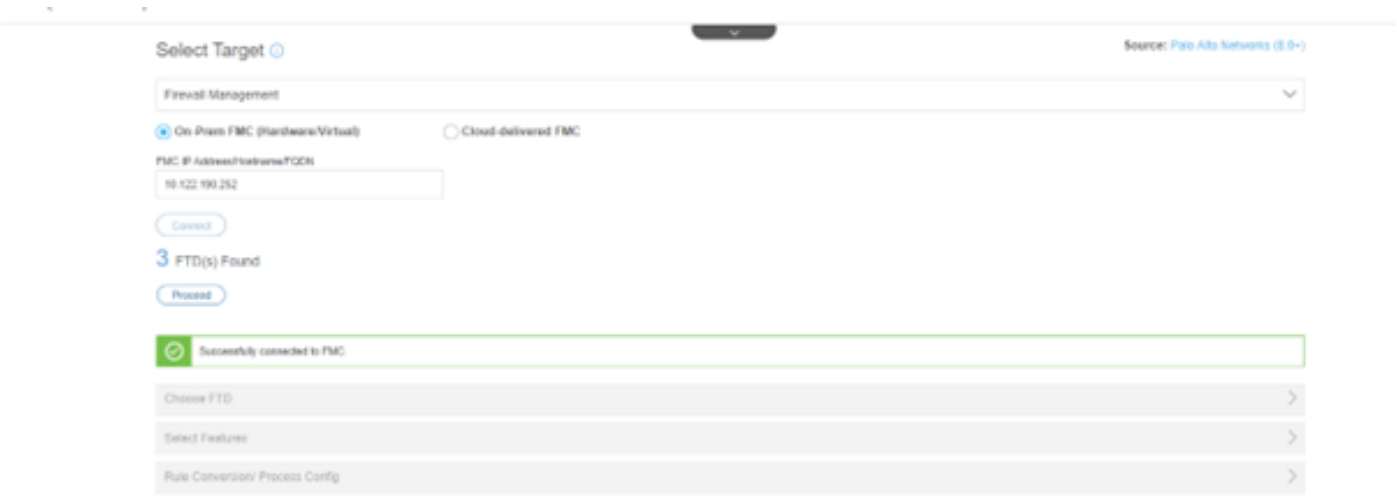
2. Utilizzo degli strumenti di migrazione

- Scaricare FMT tool .exe ed eseguirlo come amministratore.
- Per accedere a FMT, è necessario l'ID CEC o l'account utente cisco.
- Dopo aver eseguito correttamente l'accesso, lo strumento visualizza un dashboard in cui è possibile scegliere il fornitore del firewall e caricare il file *.zip corrispondente; fare riferimento all'immagine successiva.

- Leggere attentamente le istruzioni fornite a destra prima di procedere con la migrazione.
- Fare clic su Avvia migrazione quando si è pronti per iniziare.
- Caricare il file *.zip salvato che contiene le impostazioni di configurazione del firewall di Palo Alto.
- Una volta caricato il file di configurazione, sarà possibile visualizzare un Riepilogo analizzato del contenuto e fare clic su avanti; fare riferimento all'immagine successiva.

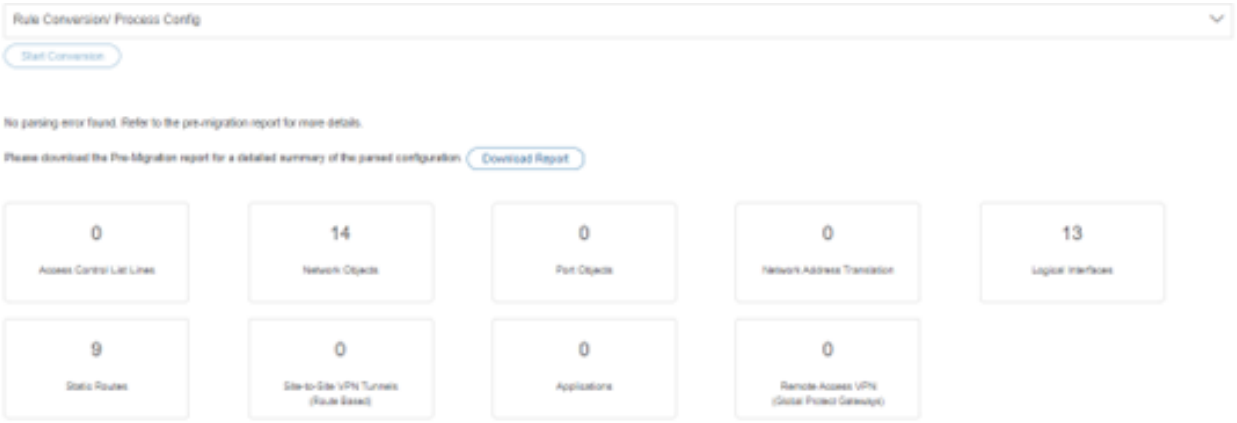


- Immettere l'indirizzo IP del CCP ed eseguire l'accesso.
- Lo strumento cercherà un FTD attivo registrato presso il CCP.
- Scegliere l'FTD di cui si desidera eseguire la migrazione e fare clic su Continua, come mostrato nell'immagine seguente.

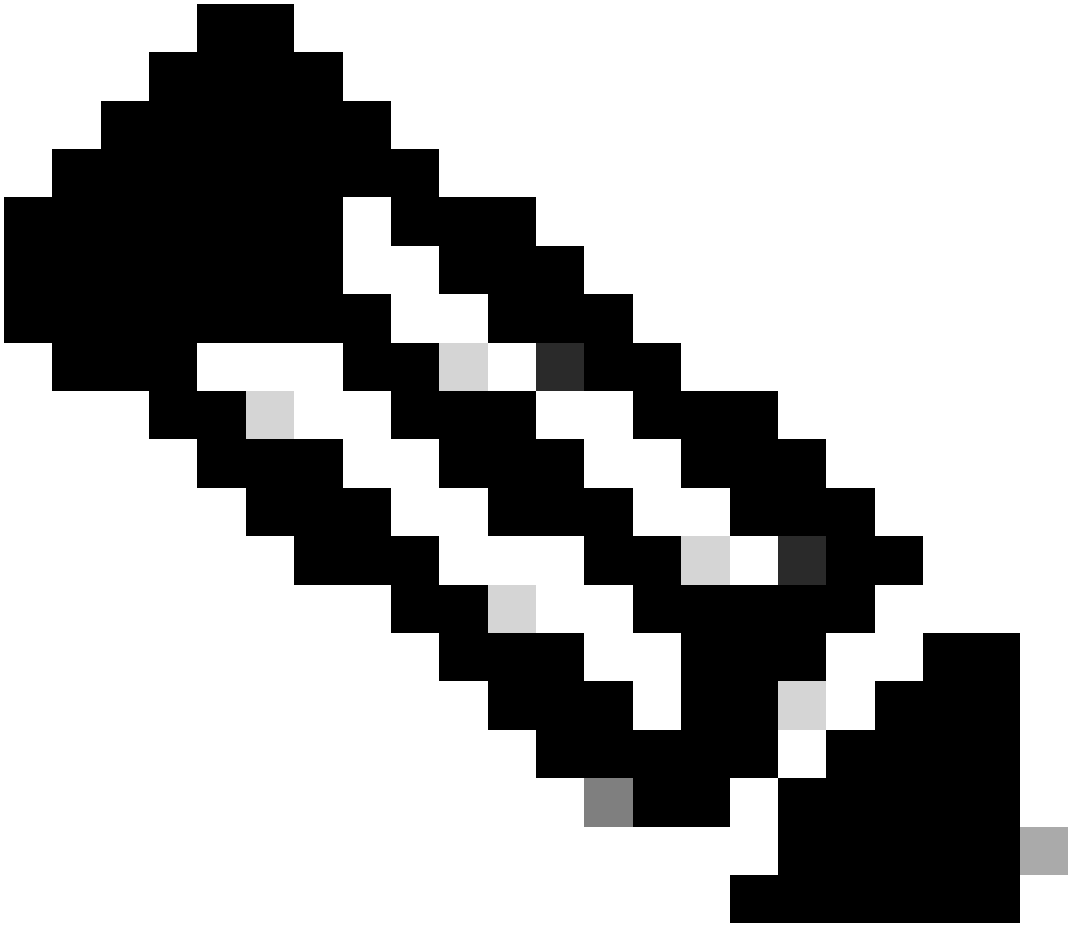


- Scegliere le funzionalità specifiche da migrare in base ai requisiti del cliente. Notate che i firewall di Palo Alto hanno un set di funzioni diverso rispetto a FTD.
- Fare clic su Continua e consultare l'immagine successiva come riferimento.

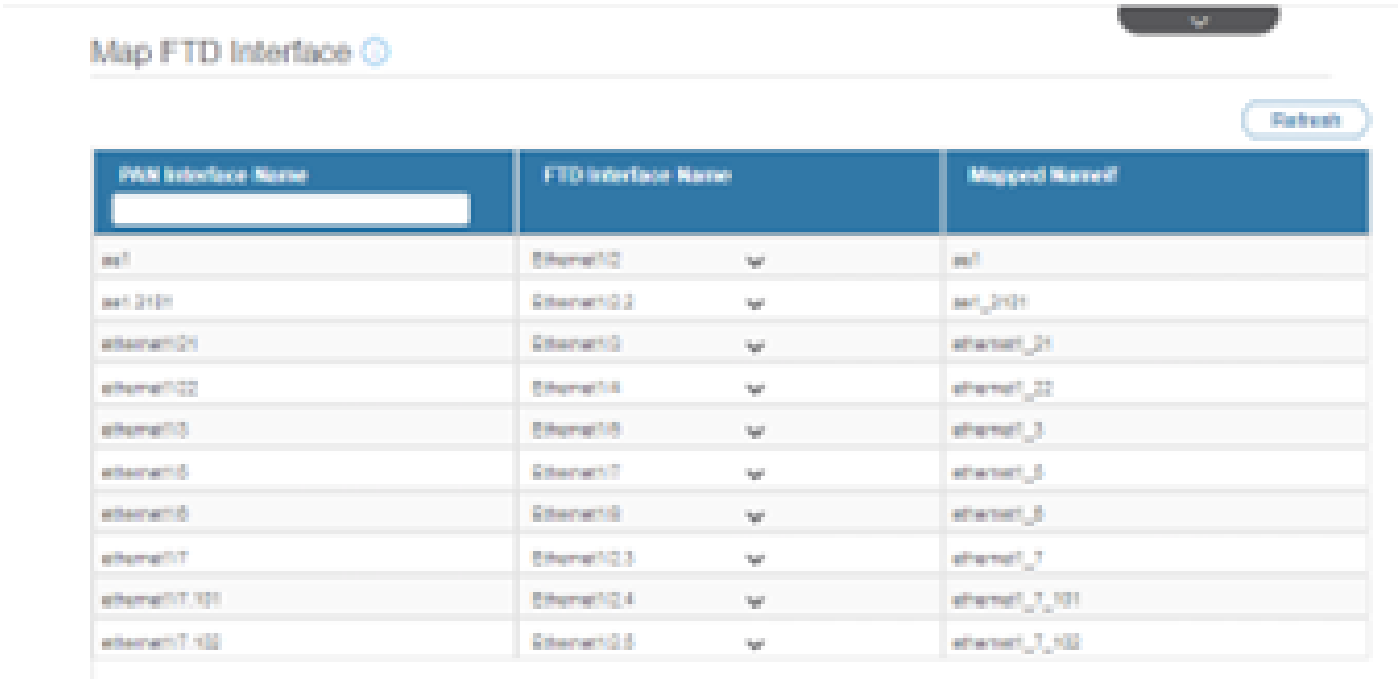
- FMT eseguirà la conversione in base alle selezioni effettuate. Esaminare le modifiche nel report di pre-migrazione, quindi fare clic su Continua. Per ulteriori informazioni, vedere l'immagine seguente.



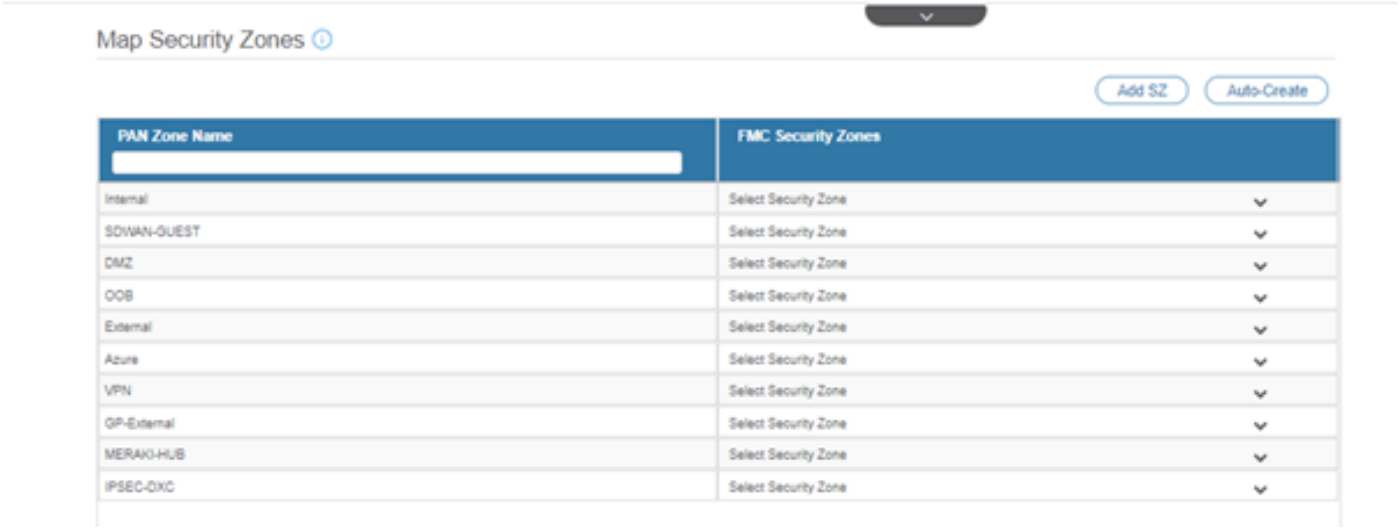
  - Mappare le interfacce dal firewall di Palo Alto a quelle sull'FTD. Per ulteriori informazioni, vedere l'immagine successiva.



Nota: NGFW/FTD deve avere lo stesso numero di interfacce fisiche o secondarie o di canali di porte uguale alle interfacce firewall di Palo Alto, incluse le sottointerfacce.



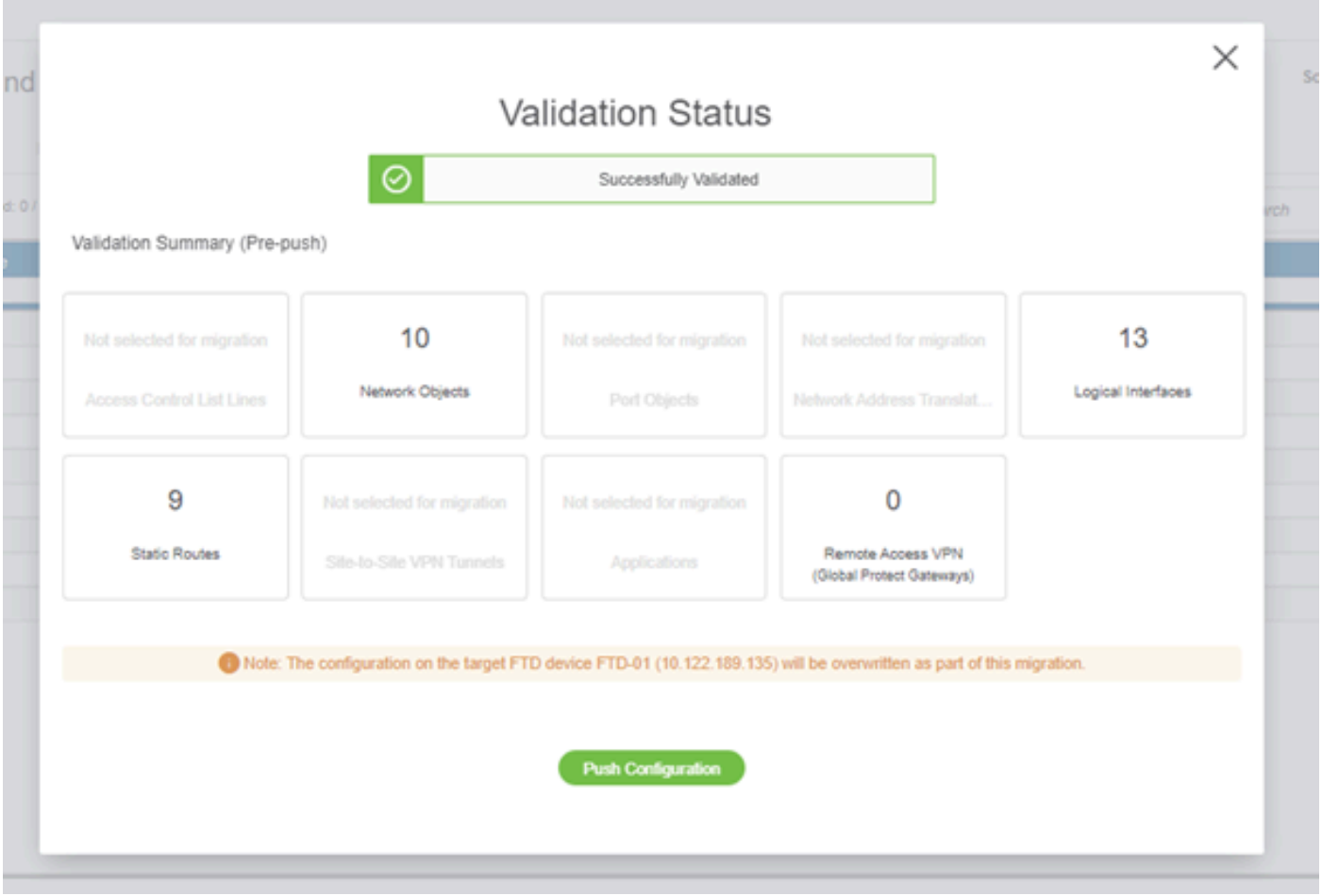
- Determinare la mappatura per le zone, che può essere eseguita manualmente o utilizzando la funzione di creazione automatica. Per la visualizzazione, fare riferimento all'immagine successiva.



- Assegnare il profilo di blocco dell'applicazione. Poiché si tratta di un dispositivo lab senza mappatura dell'applicazione, è possibile continuare con le impostazioni predefinite. Fare clic su Next (Avanti), quindi fare riferimento all'immagine fornita.

- Ottimizzare ACL, oggetti, interfacce e route in base alle esigenze. Poiché si tratta di un'installazione lab con configurazioni minime, è possibile procedere con le opzioni predefinite. Fare quindi clic su Convalida, facendo riferimento all'immagine successiva.

- Dopo la convalida, la configurazione è pronta per essere distribuita nell'FTD di destinazione. Per ulteriori istruzioni, vedere l'immagine successiva.



- La configurazione push consente di salvare le configurazioni migrate in FMC e di distribuirle automaticamente nell'FTD.
- In caso di problemi durante la migrazione, apri una richiesta TAC per ricevere ulteriore assistenza.

3. Convalida post - migrazione

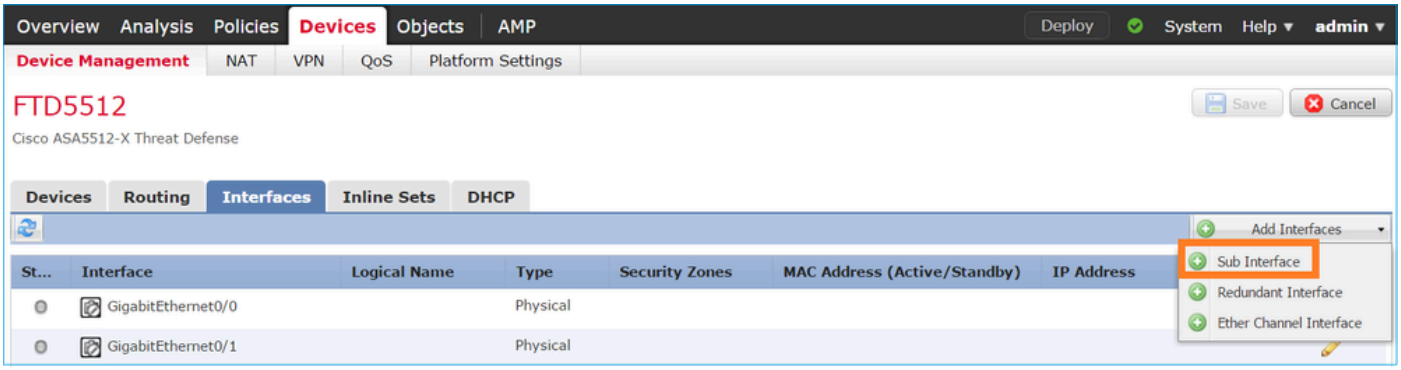
- Convalida della configurazione nell'FTD e nel FMC.
- Verifica degli ACL, dei criteri, della connettività e di altre funzionalità avanzate del dispositivo.
- Creare un punto di rollback prima di apportare qualsiasi modifica.
- Test della migrazione nell'ambiente lab prima dell'implementazione nell'ambiente di produzione.

Problemi noti

1. Interfacce mancanti su FTD

- Accedere alla CLI di Palo Alto ed eseguire il comando show interface all. È necessario avere un numero di interfacce uguale o superiore al numero di interfacce in FTD.
- Creare lo stesso numero o un numero maggiore di interfacce - sottointerfaccia, canale porta o interfaccia fisica tramite l'interfaccia GUI di FMC.
- Selezionare FMC GUI Device > Device Management, quindi fare clic sull'FTD in cui creare

l'interfaccia richiesta. In Sezione interfaccia (Interface section), dal menu a discesa nell'angolo destro selezionate Crea sottointerfaccia/BVI (Create Sub-interface/BVI) e create l'interfaccia e associate le interfacce corrispondenti. Salvare la configurazione e sincronizzare il dispositivo.



- Verificare che le interfacce siano state create su FTD eseguendo Show interface ip brief e procedere con la migrazione per la mappatura dell'interfaccia.

2. Tabella di routing

- Verificare la tabella di routing sul firewall di Palo Alto eseguendo Show routing route o Show routing route summary.
- Prima di eseguire la migrazione delle route a FTD, verificare la tabella e scegliere le route richieste in base alle esigenze del progetto.
- Convalidare la stessa tabella di routing nell'FTD tramite Mostra ciclo di lavorazione tutto e mostra riepilogo ciclo di lavorazione.

3. Ottimizza

- Il pannello Ottimizzazione oggetti è disattivato. A volte è necessario creare un oggetto manuale in FMC e mapparlo. Per visualizzare l'oggetto in FTD, utilizzare Mostra in esecuzione | negli oggetti e in Palo Alto, utilizzare Show address <nome oggetto>.
- La migrazione delle applicazioni richiede un controllo del firewall di Palo Alto prima della migrazione, FTD dispone di un dispositivo IPS dedicato oppure è possibile abilitare la funzione in FTD in modo da pianificare l'attività di migrazione delle applicazioni in base alle esigenze del cliente.
- La configurazione NAT del firewall di Palo Alto deve essere verificata tramite show running nat-policy e devi avere una policy NAT personalizzata in FTD, che può essere visualizzata in FTD tramite Show Running nat.

Conclusioni

La migrazione del firewall di Palo Alto all'FTD Cisco è stata completata con l'aiuto di FMT. In caso di problemi successivi alla migrazione con FTD e per la risoluzione dei problemi, aprire ulteriormente una richiesta 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).