Nahtloser Übergang: Migration von Palo Alto Firewall zu Cisco FTD

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

FirePOWER Migration-Tool (FMT)

Migrationsleitfaden

- 1. Checkliste vor der Migration
- 2. Verwendung des Migrationstools
- 3. Validierung nach der Migration

Bekannte Probleme

- 1. Fehlende Schnittstellen auf FTD
- 2. Routingtabelle
- 3. Optimierung

Schlussfolgerung

Einleitung

In diesem Dokument wird der Übergang von einer Palo Alto Firewall zu einem Cisco FTD-System unter Verwendung der FMT-Version 6.0 beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Exportieren der aktuellen Konfiguration von der Palo Alto Firewall im XML-Format (*.xml).
- Zugriff auf die Kommandozeile der Palo Alto Firewall und Ausführung des Befehls show routing route, Speichern der Ausgabe als Textdatei (*.txt).
- Komprimieren der Konfigurationsdatei (*.xml) und der Routing-Ausgabedatei (*.txt) in einem einzigen ZIP-Archiv (*.zip).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Palo Alto Firewall Version 8.4.x oder höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

FirePOWER Migration-Tool (FMT)

FMT unterstützt Technikerteams beim Übergang von vorhandenen Firewalls anderer Anbieter zu Cisco Next-Generation Firewall (NGFW)/Firepower Threat Defense (FTD). Stellen Sie sicher, dass Sie die neueste FMT-Version verwenden, die von der Cisco Website heruntergeladen wurde.

Migrationsleitfaden

1. Checkliste vor der Migration

- Vergewissern Sie sich, dass die FTD dem FMC hinzugefügt wurde, bevor Sie mit der Migration beginnen.
- Auf dem FMC wurde ein neues Benutzerkonto mit Administratorberechtigungen erstellt.
- Exportierte Palo Alto-Konfigurationsdatei .xml muss mit der Erweiterung .zip gezippt werden.
- NGFW/FTD müssen über dieselbe Anzahl physischer Schnittstellen, Subschnittstellen oder Port-Channels verfügen wie Palo Alto Firewall-Schnittstellen.

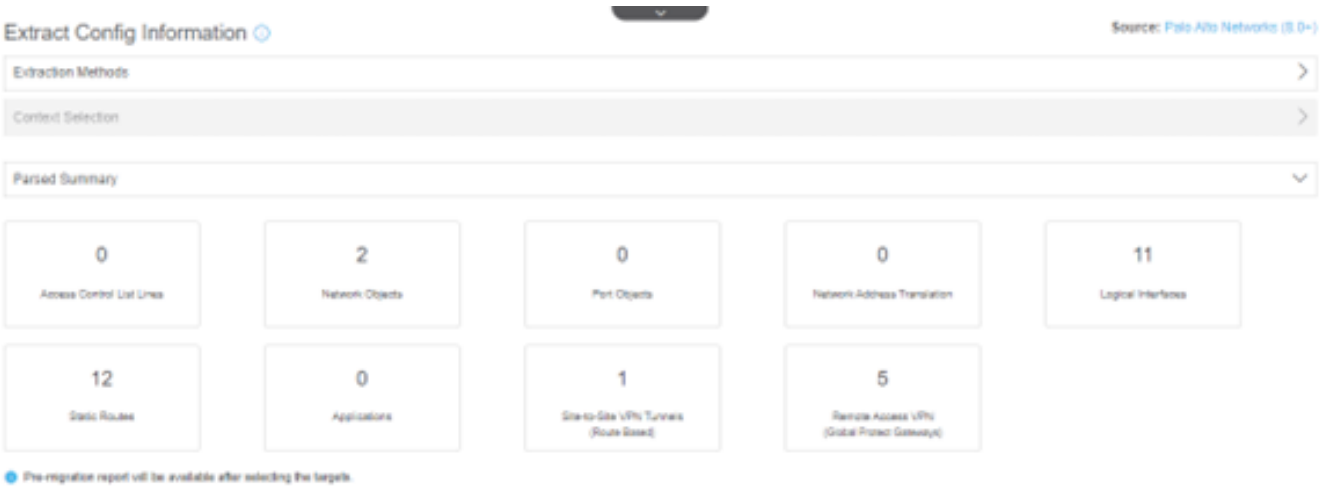
2. Verwendung des Migrationstools

- Laden Sie das FMT-Tool .exe herunter, und führen Sie es als Administrator aus.
- Für die Anmeldung bei FMT ist eine CEC-ID oder ein Cisco Benutzerkonto erforderlich.
- Nach erfolgreicher Anmeldung zeigt das Tool ein Dashboard an, auf dem Sie den Firewall-Anbieter auswählen und die entsprechende *.zip-Datei hochladen können. siehe nächstes Bild.

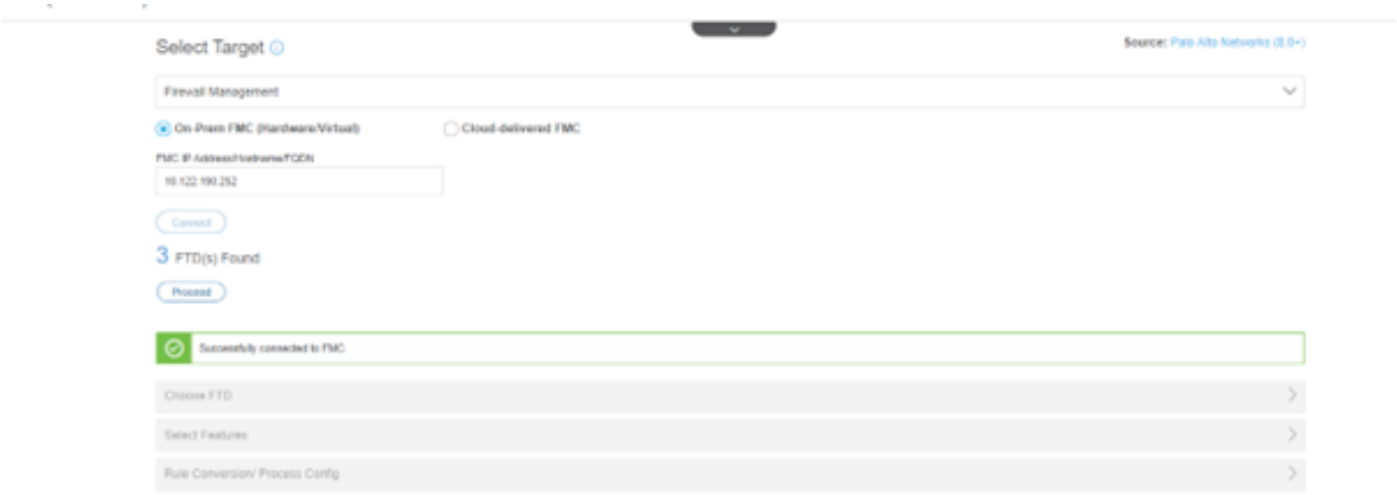
- Lesen Sie die Anweisungen auf der rechten Seite sorgfältig durch, bevor Sie mit der

Migration fortfahren.

- Klicken Sie auf Migration starten, sobald Sie bereit sind.
- Laden Sie die gespeicherte *.zip-Datei mit den Konfigurationseinstellungen von Ihrer Palo Alto-Firewall hoch.
- Sobald die Konfigurationsdatei hochgeladen wurde, wird eine analysierte Zusammenfassung des Inhalts angezeigt, und Sie können auf "Weiter" klicken. Weitere Informationen finden Sie im nächsten Bild.

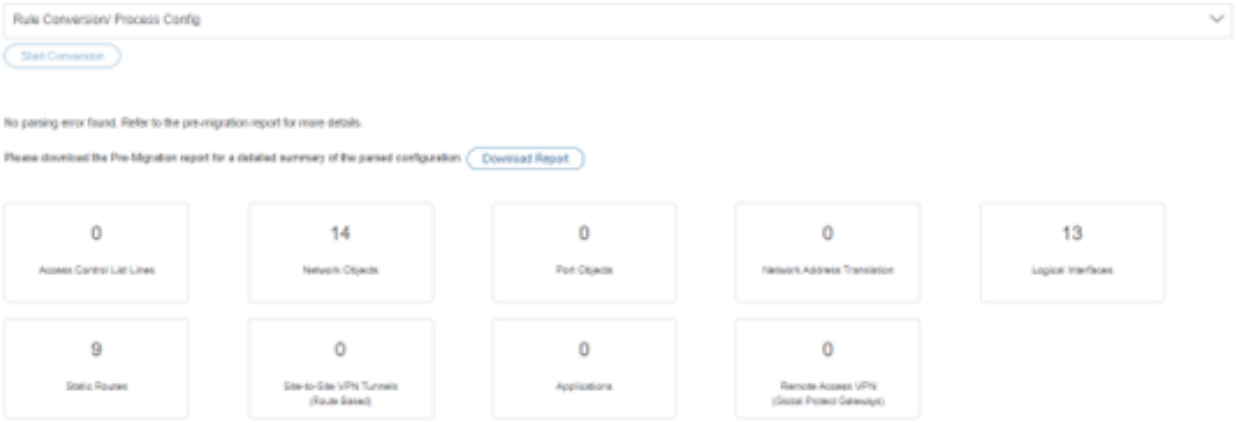


- Geben Sie die IP-Adresse des FMC ein, und melden Sie sich an.
- Das Tool sucht nach einer aktiven FTD, die beim FMC registriert wurde.
- Wählen Sie das FTD aus, das Sie migrieren möchten, und klicken Sie auf Proceed (Fortfahren), wie im nächsten Bild gezeigt.

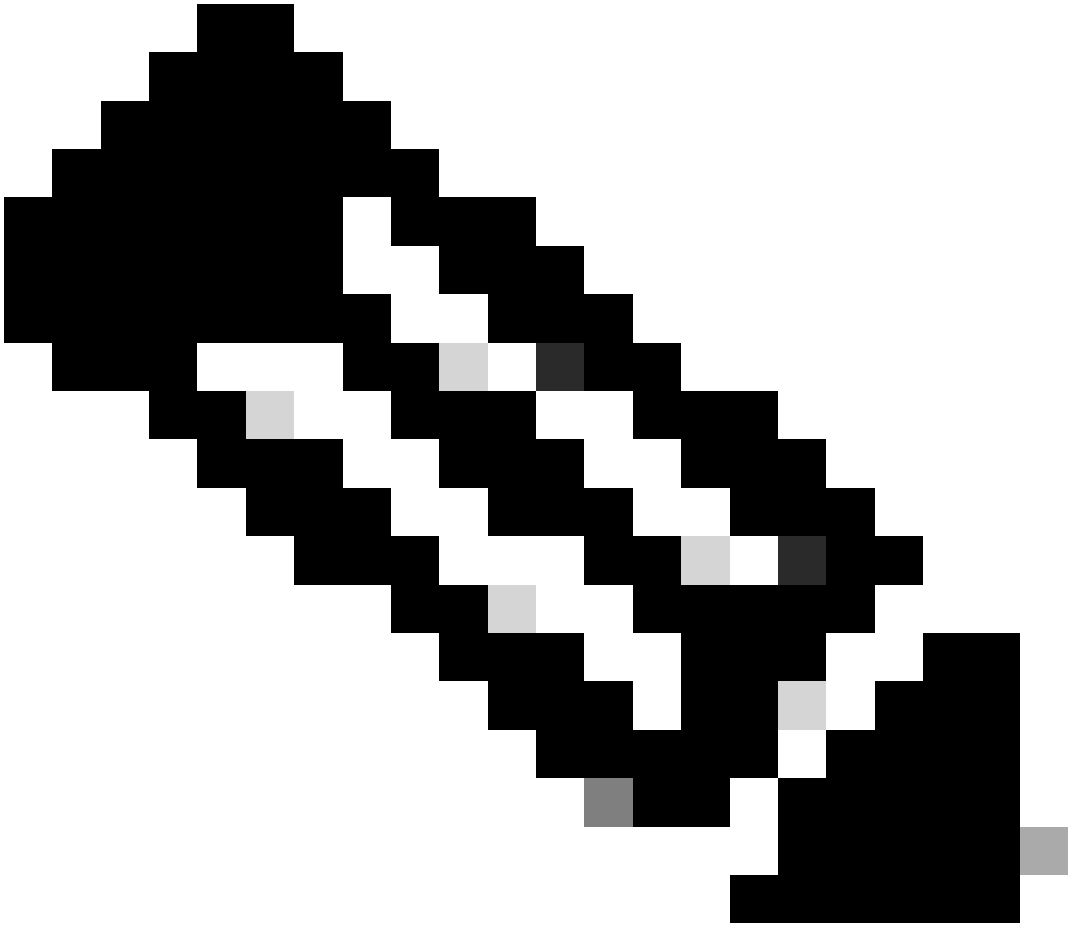


- Wählen Sie die spezifischen Funktionen aus, um je nach den Anforderungen des Kunden zu migrieren. Beachten Sie, dass Palo Alto Firewalls einen anderen Funktionsumfang haben als FTD.
- Klicken Sie auf Proceed (Fortfahren), und lesen Sie das nächste Bild.

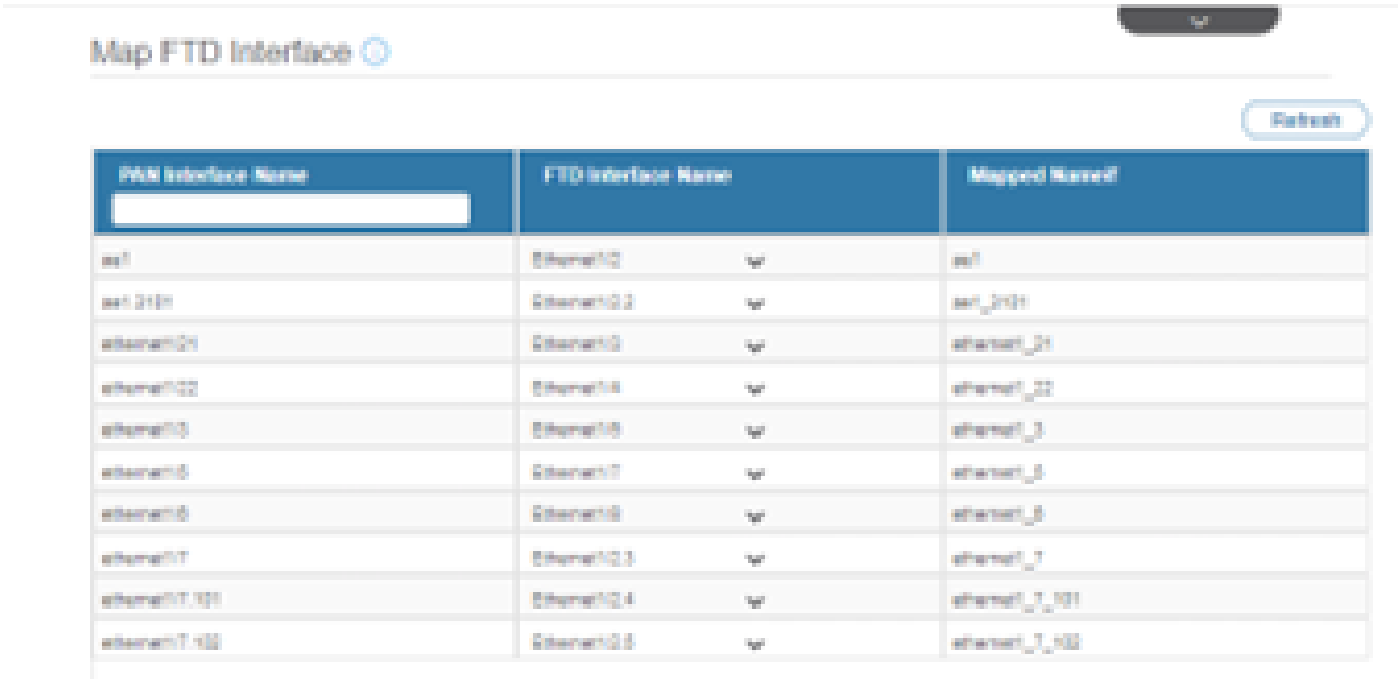
- Das FMT führt die Konvertierung entsprechend Ihrer Auswahl aus. Überprüfen Sie die Änderungen im Bericht vor der Migration, und klicken Sie dann auf Fortfahren. Sehen Sie sich das nächste Bild an.



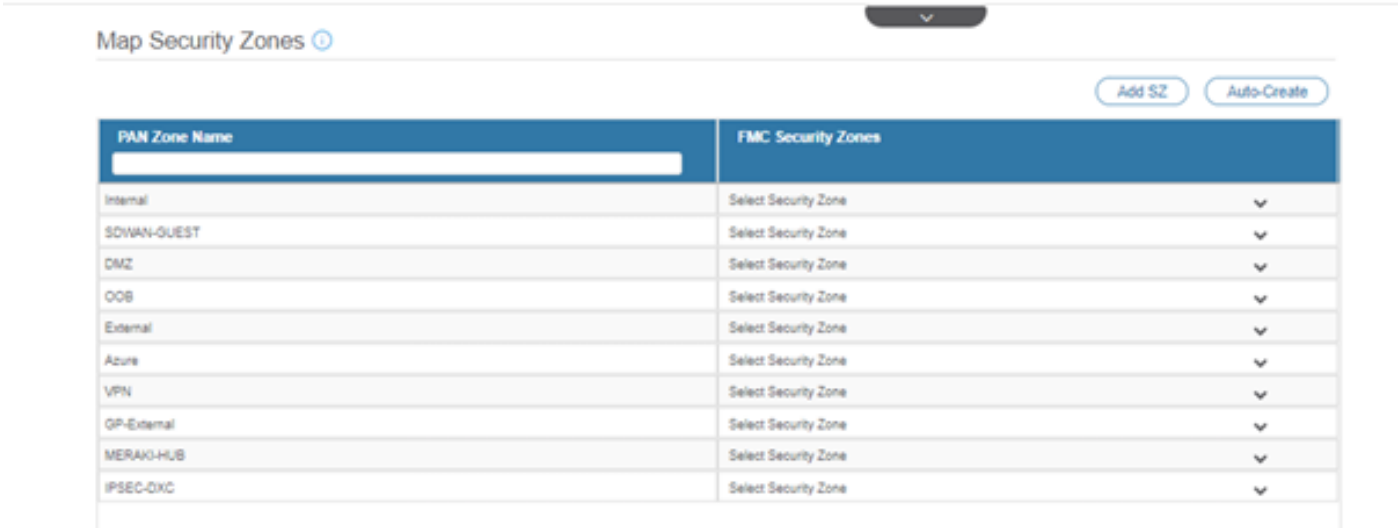
  - Ordnen Sie die Schnittstellen von der Palo Alto Firewall denen auf der FTD zu. Weitere Informationen finden Sie im nächsten Bild.



Anmerkung: NGFW/FTD muss über die gleiche Anzahl physischer Schnittstellen, Subschnittstellen oder Port-Channels verfügen wie Palo Alto Firewall-Schnittstellen, einschließlich Subschnittstellen.



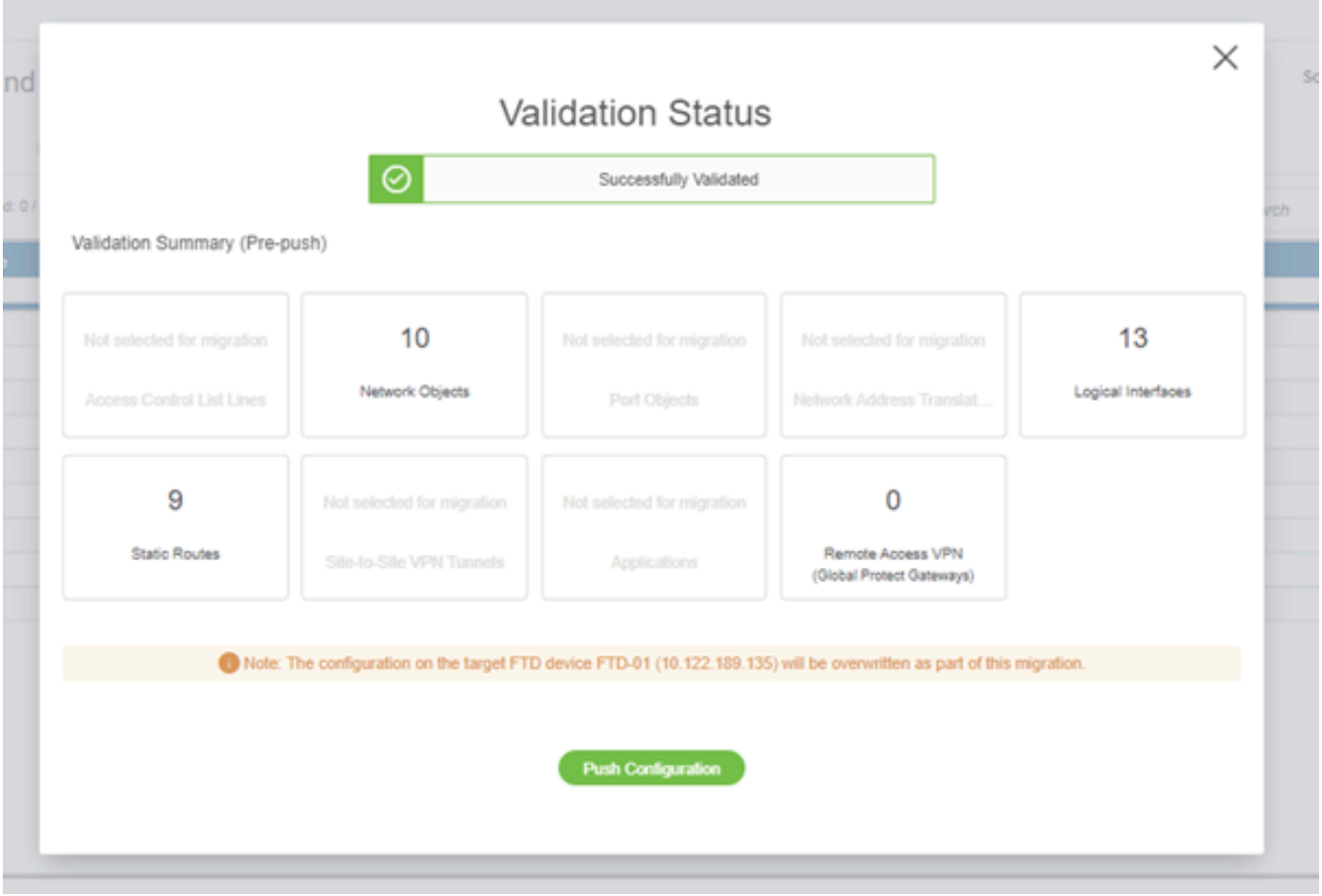
- Bestimmen Sie die Zuordnung für Zonen, die entweder manuell oder mithilfe der Funktion zum automatischen Erstellen durchgeführt werden kann. Weitere Informationen zur Visualisierung finden Sie im nächsten Bild.



- Weisen Sie Ihr Anwendungsblockierungsprofil zu. Da es sich um ein Übungsgerät ohne Anwendungszuordnung handelt, können Sie mit den Standardeinstellungen fortfahren. Klicken Sie auf Weiter, und verweisen Sie auf das bereitgestellte Bild.

- Optimierung von ACLs, Objekten, Schnittstellen und Routen nach Bedarf Da es sich hierbei um ein Lab-Setup mit minimalen Konfigurationen handelt, können Sie mit den Standardoptionen fortfahren. Klicken Sie anschließend auf Validieren, und verweisen Sie auf das nächste Bild.

- Nach erfolgreicher Validierung ist die Konfiguration für die geplante FTD bereit. Weitere Informationen finden Sie im nächsten Bild.



- Die Push-Konfiguration speichert die migrierten Konfigurationen im FMC und wird automatisch im FTD bereitgestellt.
- Bei Problemen während der Migration können Sie jederzeit ein TAC-Ticket erstellen, um weitere Unterstützung zu erhalten.

3. Validierung nach der Migration

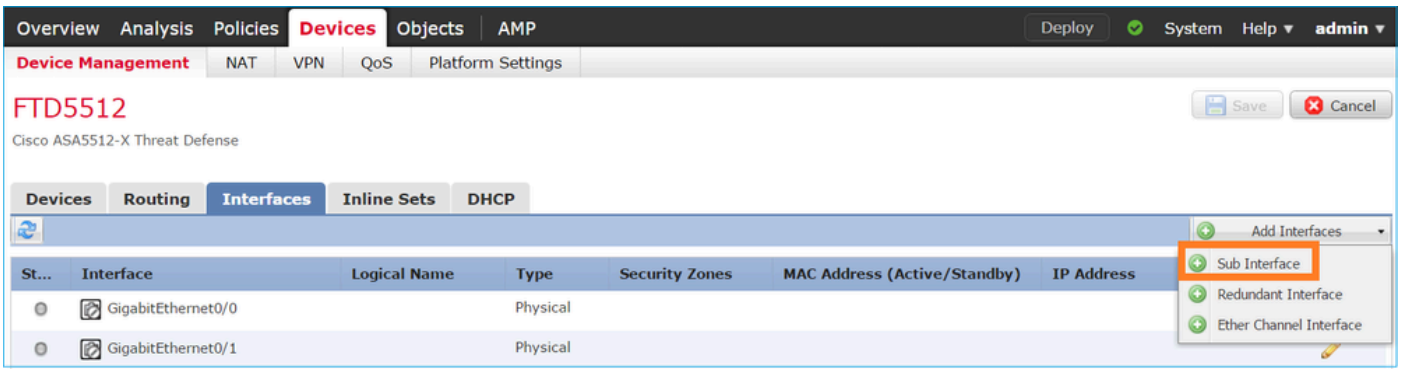
- Validierung der Konfiguration auf dem FTD und FMC
- Testen der Geräte-ACLs, Richtlinien, Verbindungen und anderer erweiterter Funktionen
- Erstellen Sie einen Rollbackpunkt, bevor Sie Änderungen vornehmen.
- Testen der Migration in der Laborumgebung vor der Einführung in die Produktionsumgebung

Bekannte Probleme

1. Fehlende Schnittstellen auf FTD

- Melden Sie sich bei Palo Alto CLI an, und führen Sie die Show-Schnittstelle all aus. Sie müssen die gleiche oder mehr Schnittstellen in FTD haben.
- Erstellen Sie die gleiche oder mehrere Schnittstellen - entweder Subschnittstelle, Port-Channel oder physische Schnittstelle über die FMC-GUI.
- Navigieren Sie zu FMC GUI Device > Device Management, und klicken Sie auf den FTD, in dem die erforderliche Schnittstelle erstellt werden soll. Wählen Sie im Dropdown-Menü in der rechten Ecke im Abschnitt Interface (Schnittstelle) die Option Create Sub-interface/BVI

(Subschnittstelle/BVI erstellen) entsprechend aus, und erstellen Sie die Schnittstelle, und ordnen Sie die entsprechenden Schnittstellen zu. Speichern Sie die Konfiguration, und führen Sie eine Synchronisierung mit dem Gerät durch.



- Überprüfen Sie, ob die Schnittstellen auf FTD erstellt wurden, indem Sie Show interface ip brief ausführen und mit der Migration für die Schnittstellenzuordnung fortfahren.

2. Routingtabelle

- Überprüfen Sie die Routing-Tabelle auf der Palo Alto Firewall, indem Sie Routing-Route anzeigen oder Routing-Routenübersicht anzeigen ausführen.
- Überprüfen Sie vor der Migration der Routen auf FTD die Tabelle, und wählen Sie die erforderlichen Routen gemäß den Projektanforderungen aus.
- Validieren Sie dieselbe Routing-Tabelle im FTD, indem Sie "Route All" (Alle Routen anzeigen) und "Route Summary" (Routenübersicht) anzeigen.

3. Optimierung

- Optimieren Objekte Panel ausgegraut, manchmal müssen Sie ein manuelles Objekt in FMC erstellen und es zuordnen. Um das Objekt in FTD anzuzeigen, verwenden Sie Show Running | in Objekten und in Palo Alto, Adresse anzeigen <Objektname> verwenden.
- Die Anwendungsmigration erfordert vor der Migration ein Audit der Palo Alto-Firewall, FTD verfügt über ein dediziertes IPS-Gerät oder Sie können die Funktion in FTD aktivieren, sodass Sie die Aufgabe der Anwendungsmigration entsprechend den Kundenanforderungen planen müssen.
- Die NAT-Konfiguration der Palo Alto Firewall muss durch show running nat-policy überprüft werden, und Sie müssen eine benutzerdefinierte NAT-Richtlinie in FTD haben, die in FTD durch Show Running nat angezeigt werden kann.

Schlussfolgerung

Die Palo Alto Firewall wurde mithilfe von FMT erfolgreich auf Cisco FTD migriert. Bei Problemen nach der Migration auf FTD und zur Fehlerbehebung können Sie ein TAC-Ticket erstellen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.