Migration von Palalto zu Firepower Threat Defense mit FMT

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Migration der Paloalto Firewall auf Cisco Firepower Threat Device beschrieben.

Voraussetzungen

Anforderungen

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

- FirePOWER Migrationstool
- Paloalto Firewall
- Sichere Firewall-Bedrohungsabwehr (FTD)
- Cisco Secure Firewall Management Center (FMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Mac OS mit Firepower Migration Tool (FMT) v7.7
- PAN NGFW Version 8.0+
- Secure Firewall Management Center (FMCv) v7.6

- Secure Firewall Threat Defense Version 7.4.2

Haftungsausschluss: Die in diesem Dokument erwähnten Netzwerke und IP-Adressen sind keinen einzelnen Benutzern, Gruppen oder Organisationen zugeordnet. Diese Konfiguration wurde exklusiv für den Einsatz in einer Laborumgebung erstellt.

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.

Überblick

Spezifische Anforderungen für dieses Dokument:

- PAN NGFW ab Version 8.4
- Secure Firewall Management Center (FMCv) Version 6.2.3 oder höher

Das Firewall Migration-Tool unterstützt diese Liste von Geräten:

- Cisco ASA (8,4+)
- Cisco ASA (9.2.2+) mit FPS
- Cisco Secure Firewall Device Manager (7.2+)
- Prüfpunkt (r75-r77)
- Prüfpunkt (r80-r81)
- Fortinet (5,0+)
- Palo Alto Networks (8.0+)

Hintergrundinformationen

Führen Sie vor der Migration Ihrer Paloalto Firewall-Konfiguration folgende Schritte aus:

Laden Sie die ZIP-Datei für die Palalto Firewall-Konfiguration herunter.

- Paloalto Firewall muss Version 8.4+ sein.
- Exportieren Sie die aktuelle Konfiguration von der Palo Alto Firewall (*.xml muss im XML-Format vorliegen).
- Melden Sie sich bei der Paloalto Firewall-CLI an, um die Show-Routing-Route auszuführen und die Ausgabe im TXT-Format (*.txt) zu speichern.
- Komprimieren Sie die aktuelle Konfigurationsdatei (*.xml) und die Routing-Datei (*.txt) mit der Erweiterung *.zip.

Checkliste vor der Migration

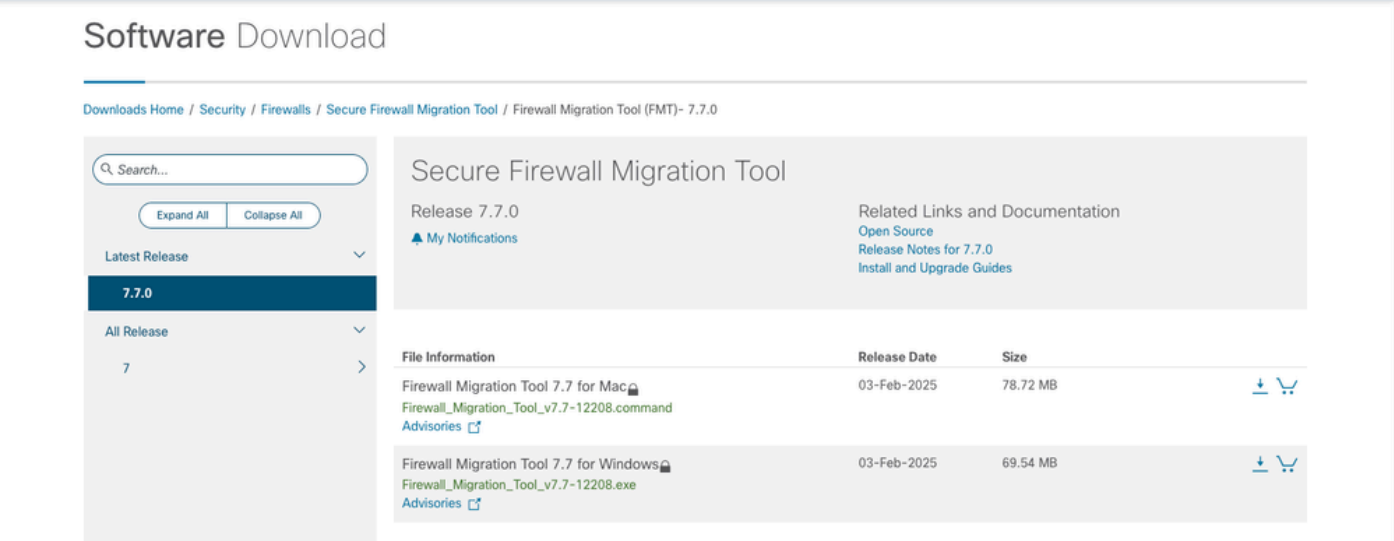
- Stellen Sie sicher, dass die FTD beim FMC registriert wurde, bevor Sie mit der Migration

beginnen.
- Auf dem FMC wurde ein neues Benutzerkonto mit Administratorberechtigungen erstellt. Sie können auch vorhandene Admin-Anmeldedaten verwenden.
- Exportierte Palo Alto-Konfigurationsdatei.xml muss mit der Erweiterung .zip gezippt werden (befolgen Sie die Prozedur, die im vorherigen Abschnitt erwähnt wurde).
- Das FirePOWER-Gerät muss im Vergleich zu den Paloalto Firewall-Schnittstellen die gleiche oder eine größere Anzahl von physischen Schnittstellen oder Subschnittstellen bzw. Port-Kanälen aufweisen.

Konfigurieren

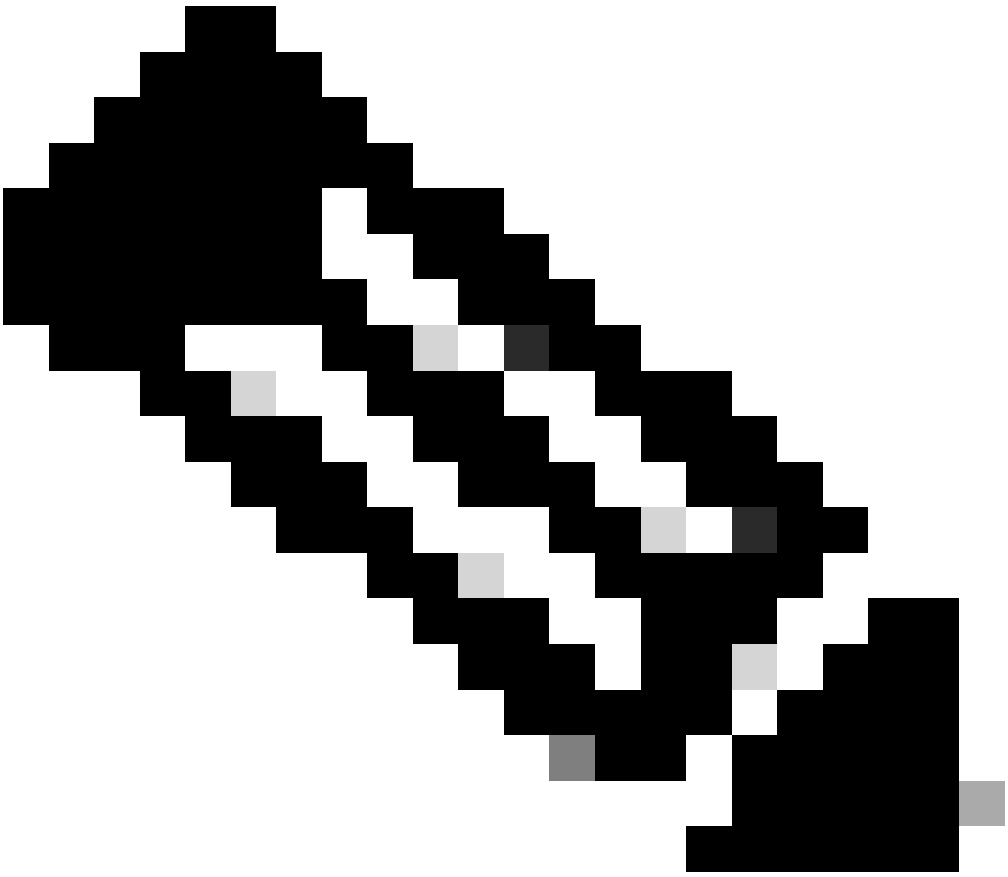
Migrationsschritte

1. Laden Sie das neueste Firepower Migration Tool von Cisco Software Central herunter, das mit Ihrem Computer kompatibel ist:



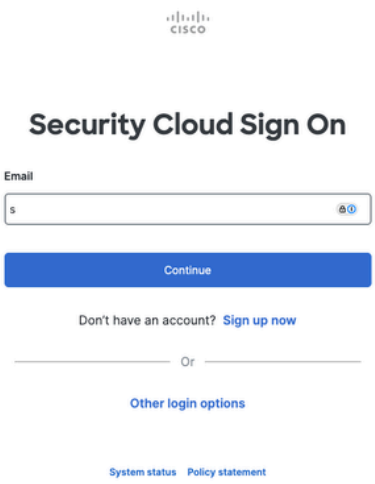
FMT-Download

3. Öffnen Sie die zuvor auf Ihren Computer heruntergeladene Datei.



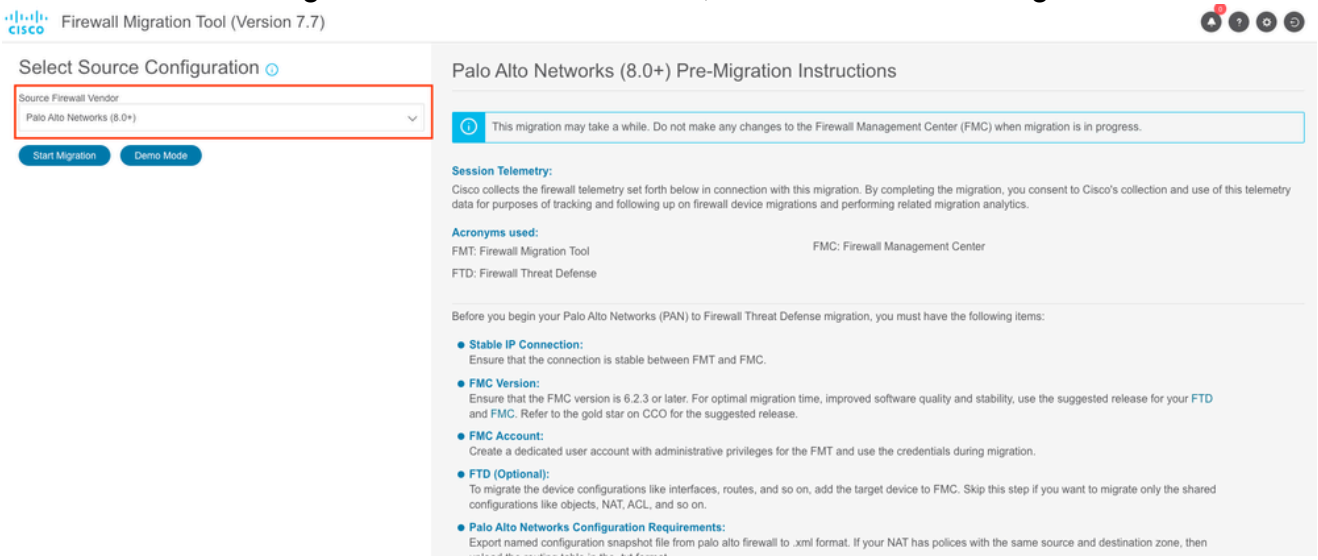
Anmerkung: Das Programm wird automatisch geöffnet, und eine Konsole generiert automatisch Inhalte für das Verzeichnis, in dem Sie die Datei ausgeführt haben.

4. Nach dem Ausführen des Programms wird ein Webbrowser geöffnet, in dem die Endbenutzer-Lizenzvereinbarung angezeigt wird.
    1. Aktivieren Sie das Kontrollkästchen, um die Geschäftsbedingungen zu akzeptieren.
    2. Klicken Sie auf Fortfahren.
5. Melden Sie sich mit gültigen CCO-Anmeldeinformationen an, um auf die FMT-GUI zuzugreifen.



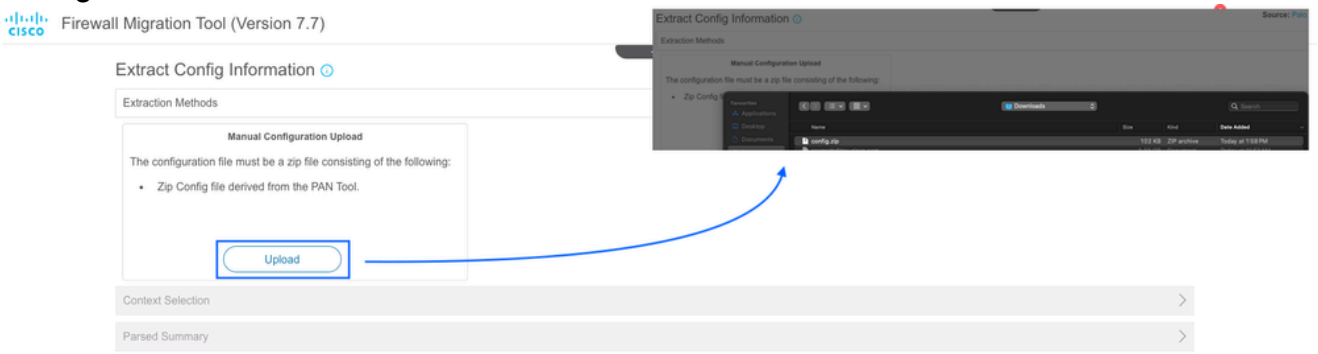
FMT-Anmeldeaufforderung

6. Wählen Sie die zu migrierende Quell-Firewall aus, und klicken Sie auf Migration starten.



FMT-GUI

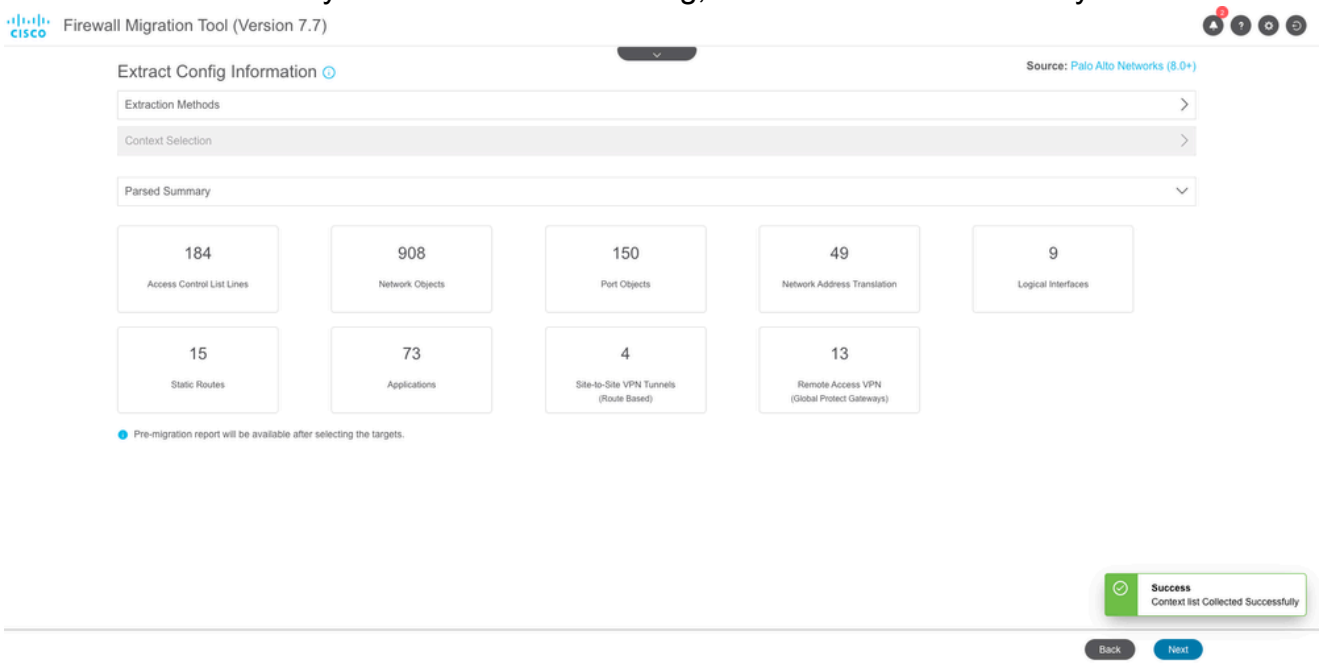
7. Der Abschnitt "Extraction Methods" wird nun angezeigt, in dem Sie die Zip-Konfigurationsdatei von Paloalto Firewall auf das FMT hochladen müssen.



Assistent zum Hochladen von Konfigurationen

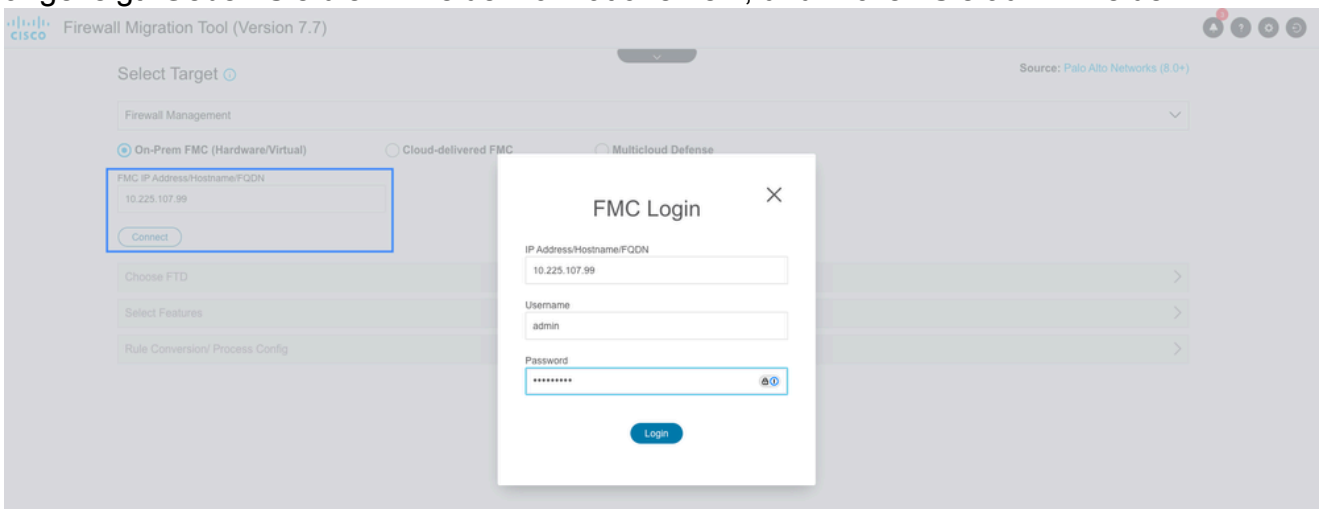
8. Die Zusammenfassung der analysierten Konfiguration wird jetzt angezeigt, nachdem die Konfigurationsdatei hochgeladen wurde. Im Fall von VSYS stehen separate VSYS-Optionen

zur Verfügung. Jeder von ihnen muss analysiert und nacheinander migriert werden. Validieren Sie die analysierte Zusammenfassung, und klicken Sie auf das Symbol Weiter.



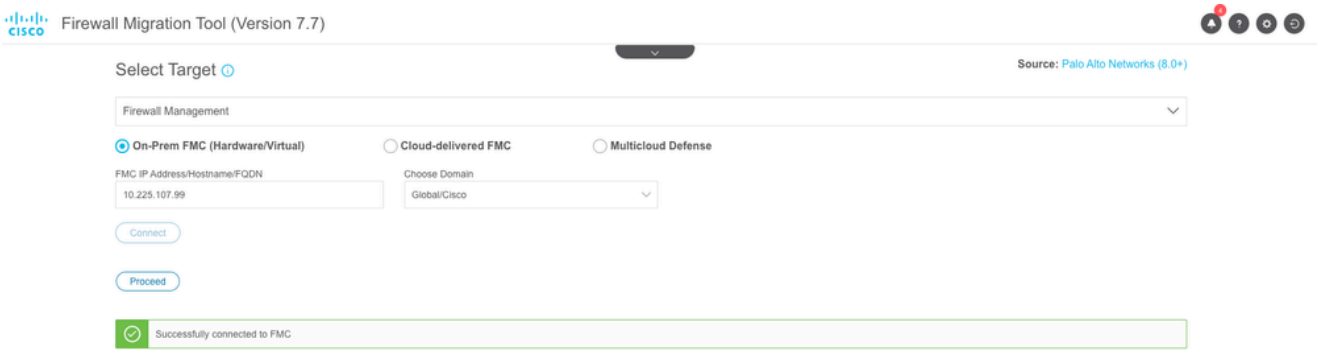
Zusammenfassung der Konfigurationsvalidierung

9. In diesem Abschnitt können Sie den Typ des FMC auswählen. Geben Sie die Management-IP-Adresse an, und klicken Sie auf Verbinden.
   Es wird ein Popup mit der Aufforderung zur Eingabe der FMC-Anmeldeinformationen angezeigt. Geben Sie die Anmeldeinformationen ein, und klicken Sie auf Anmelden.



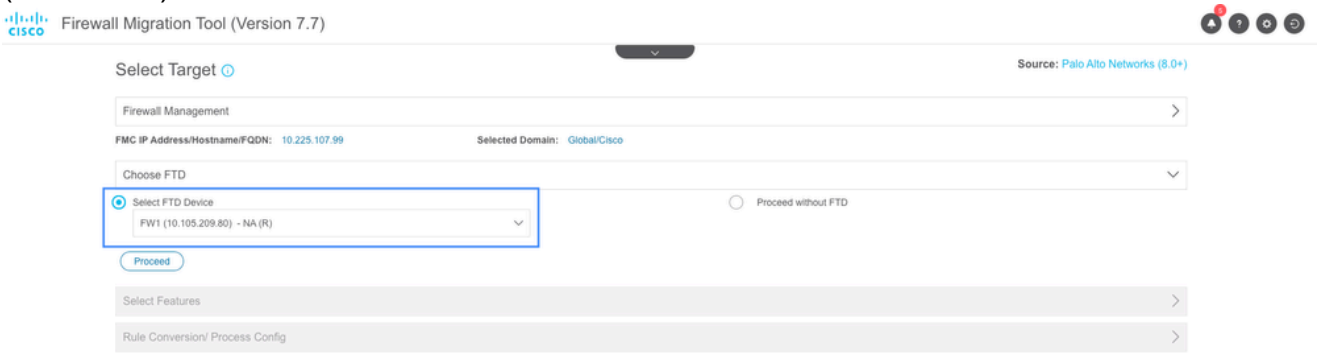
FMC-Anmeldung

10. Nach erfolgreicher Verbindung mit FMC können Sie jetzt die Domäne auswählen (falls vorhanden) und auf Proceed (Weiter) klicken.



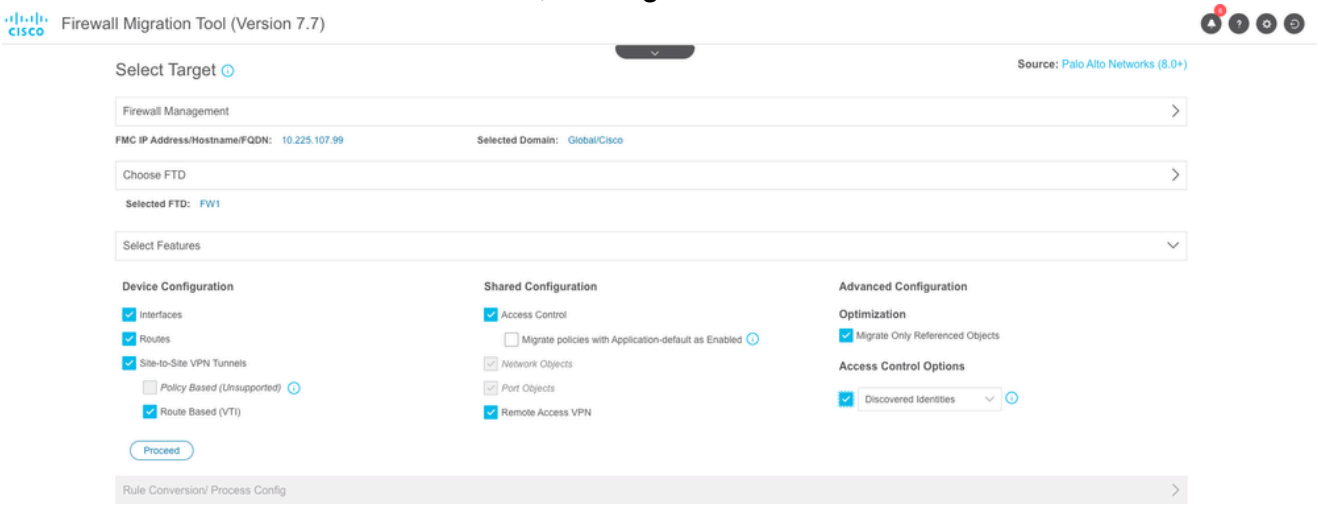
Domänenauswahl

11. Wählen Sie das FTD aus, zu dem Sie migrieren möchten, und klicken Sie auf Proceed (Fortfahren).

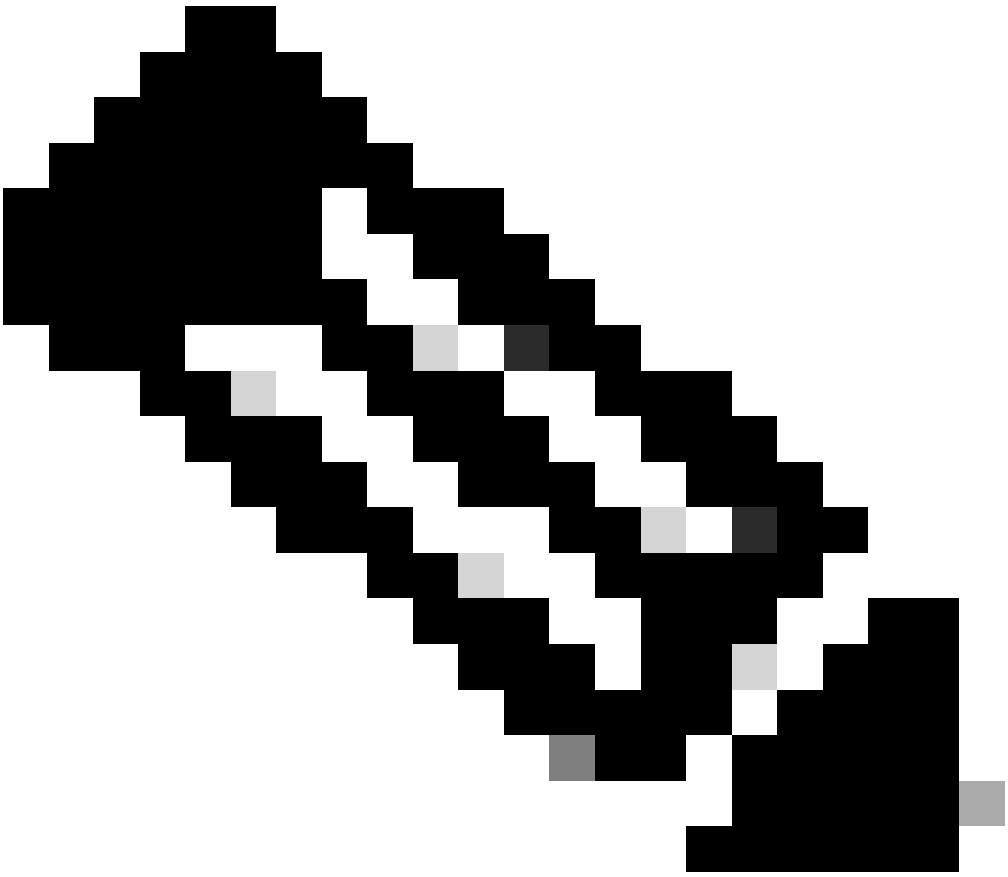


Ziel-FTD auswählen

12. Das Tool listet nun die Funktionen auf, die migriert werden sollen. Klicken Sie auf Fortfahren.

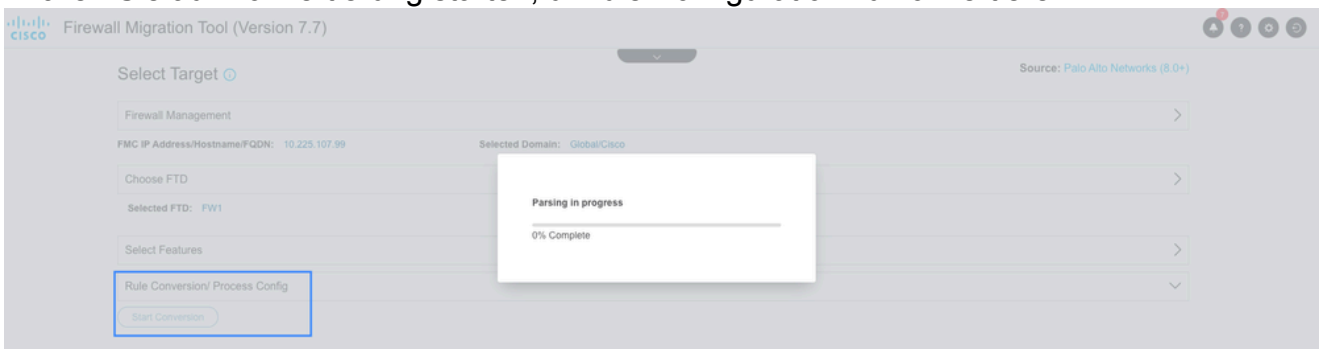


Funktionsauswahl



Anmerkung: Alle Funktionen sind standardmäßig ausgewählt. Sie können jede Konfiguration deaktivieren, die nicht migriert werden soll.

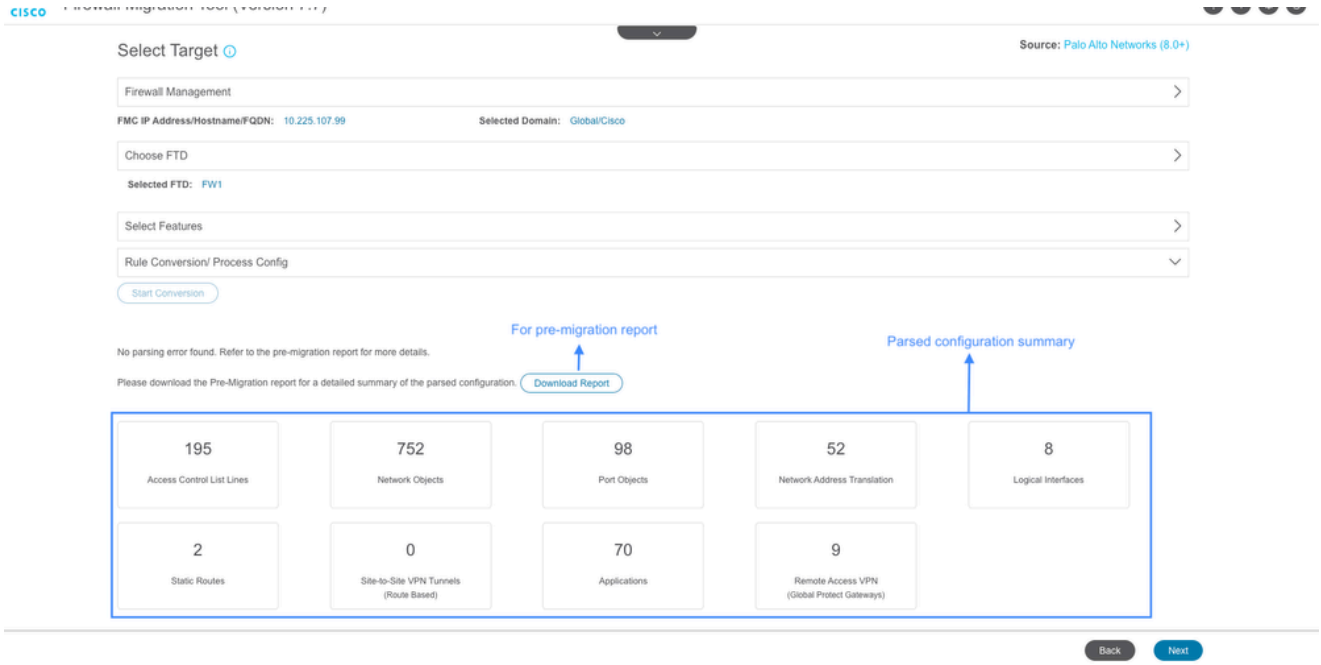
13. Klicken Sie auf Konvertierung starten, um die Konfiguration zu konvertieren.



Parsing-Konfiguration

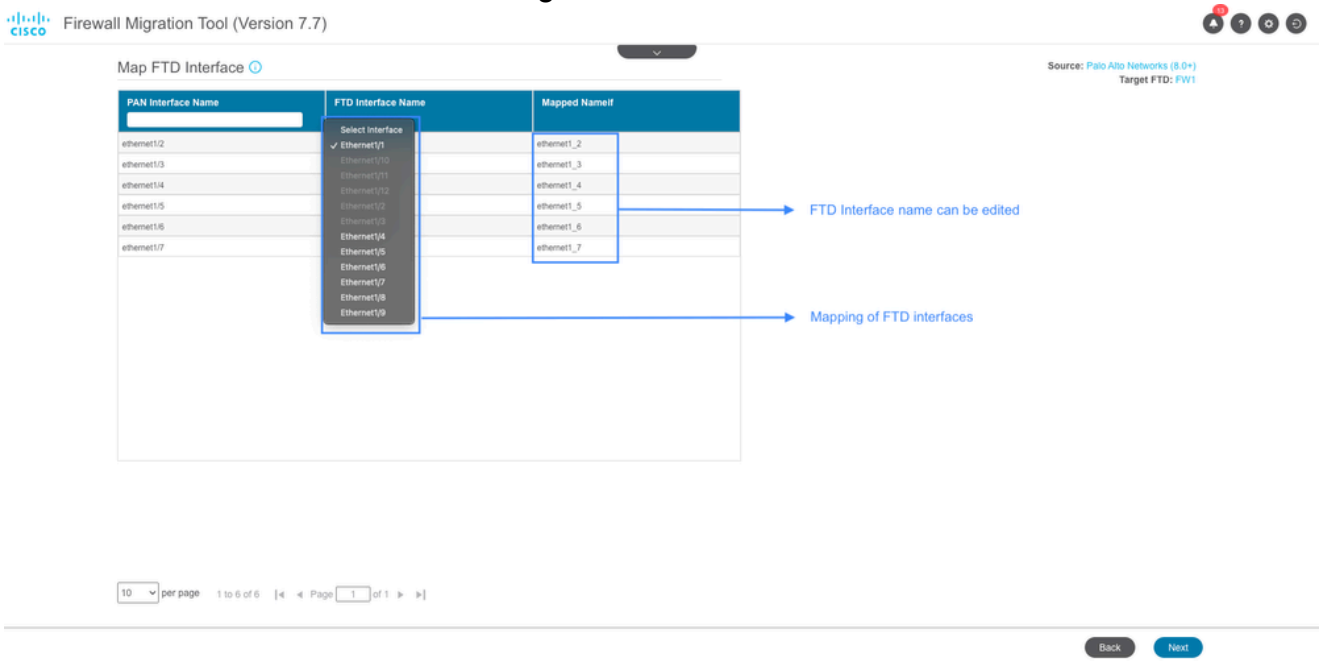
Das Tool analysiert die Konfiguration und zeigt die Konvertierungsübersicht an, wie im Bild dargestellt. Sie können auch den Bericht zur Vormigration herunterladen, um die migrierte Konfiguration auf Fehler oder Warnungen zu überprüfen. Navigieren Sie zur nächsten Seite,

indem Sie auf Weiter klicken.



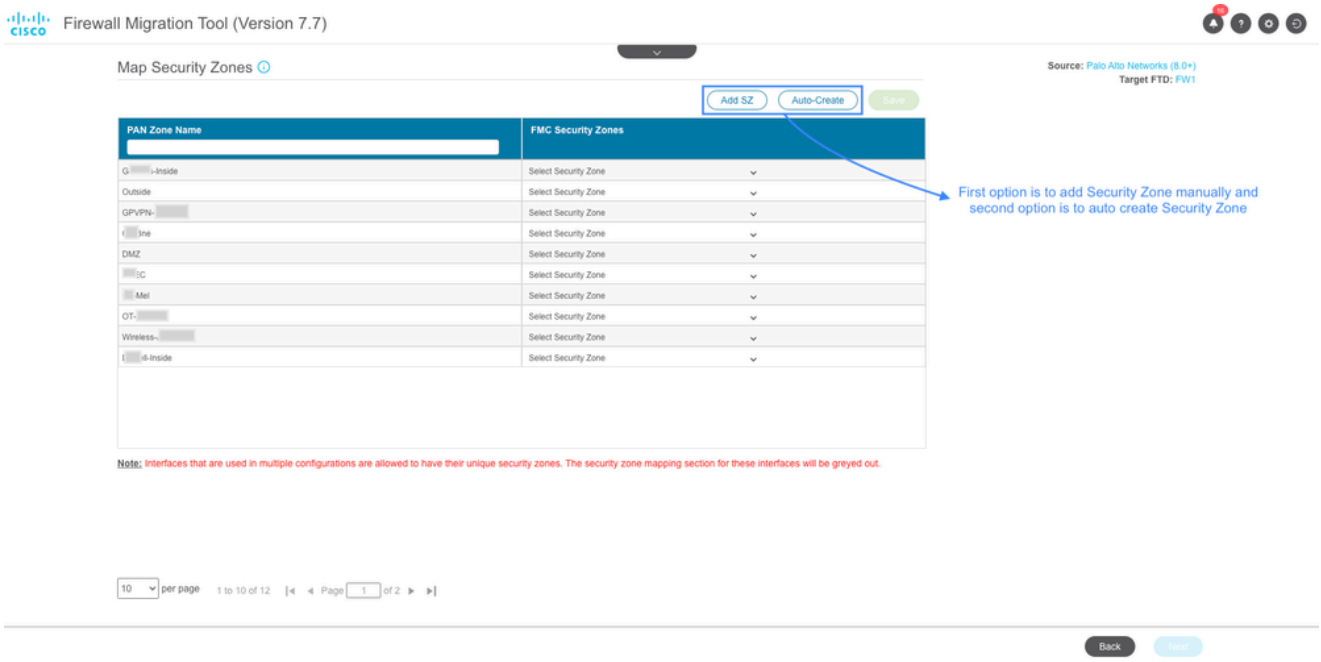
Zusammenfassung der analysierten Konfiguration

14. Im Schnittstellenzuordnungsabschnitt können Sie die Schnittstellenzuordnung von Paloalto zu FTD sowie den Schnittstellennamen für jede Schnittstelle bearbeiten. Klicken Sie nach Abschluss der Schnittstellenzuordnung auf Weiter.



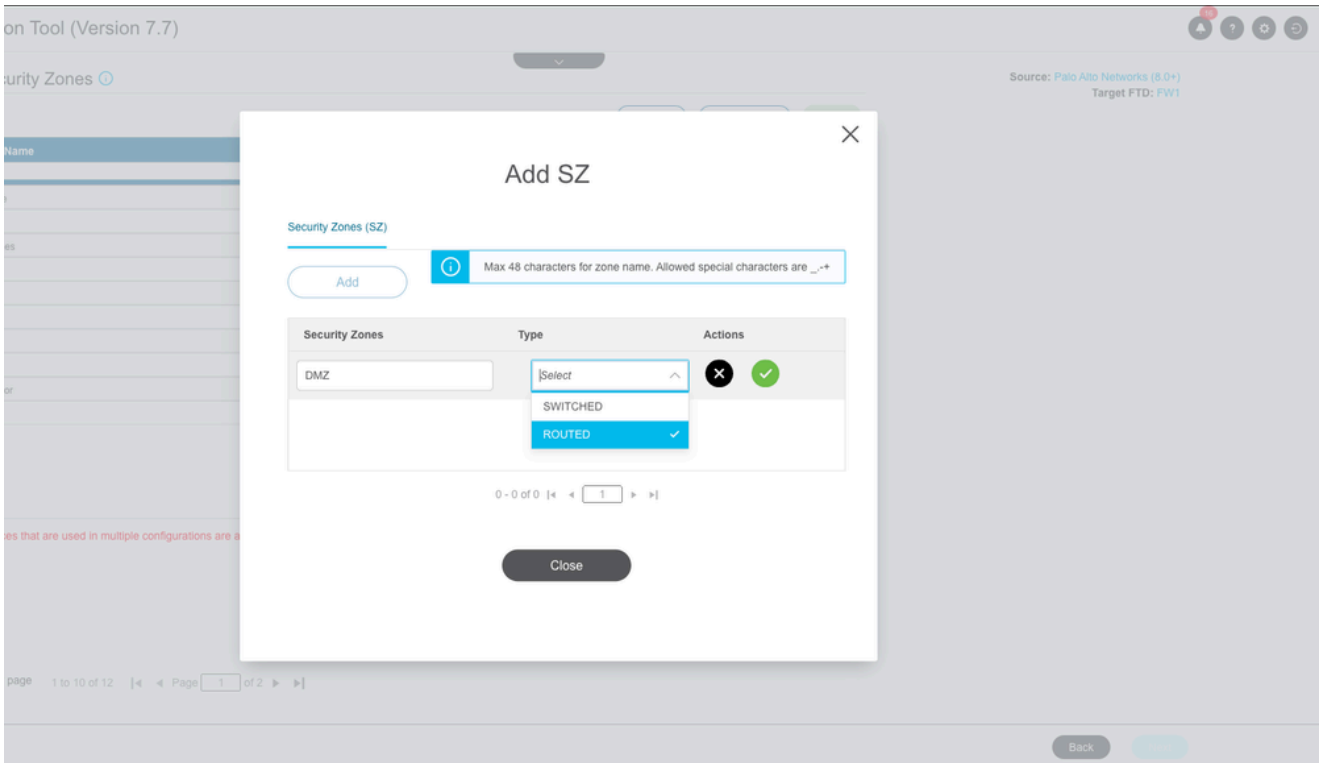
Schnittstellenzuordnung

15. Sie können die Sicherheitszone entweder manuell für jede Schnittstelle hinzufügen oder sie im Abschnitt Sicherheitszone zuordnen automatisch erstellen. Klicken Sie nach dem Erstellen und Zuordnen von Sicherheitszonen auf Weiter.



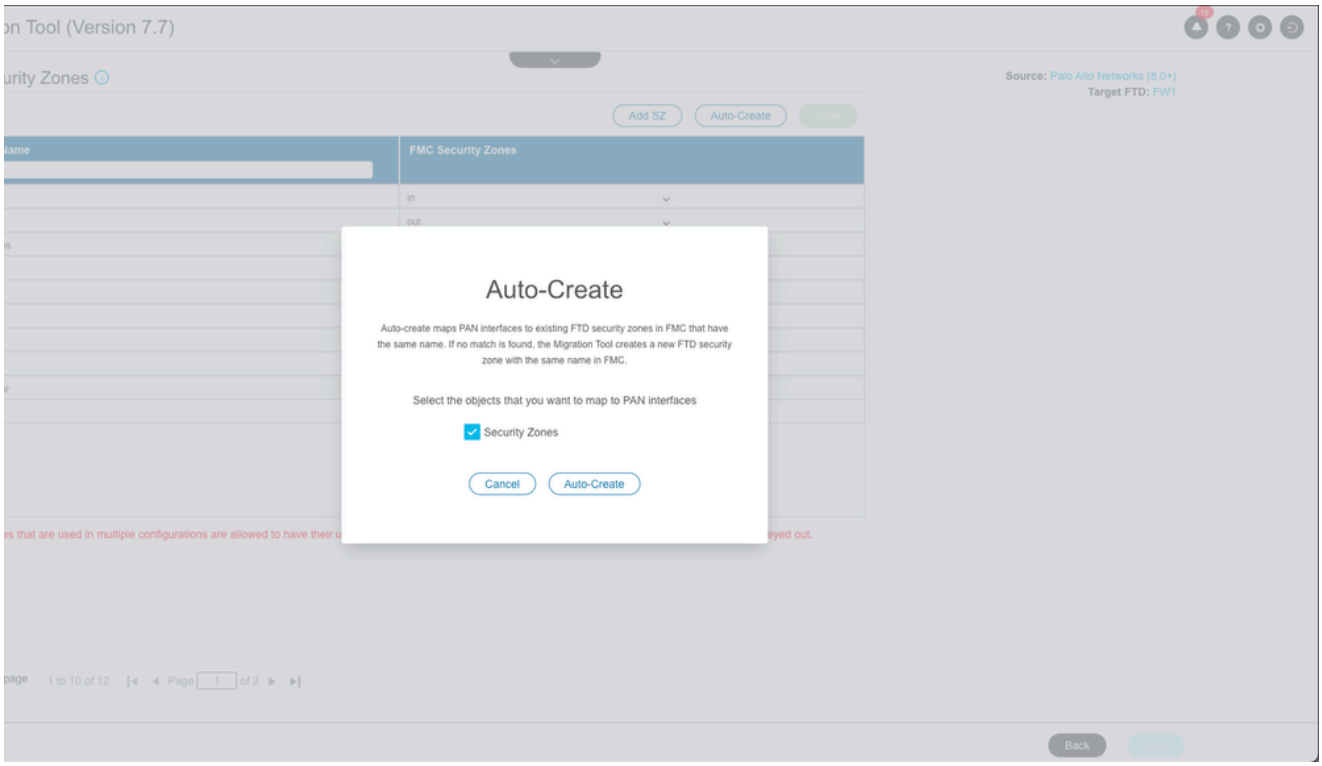
Erstellung von Sicherheitszonen

Manuelle Erstellung von Sicherheitszonen:



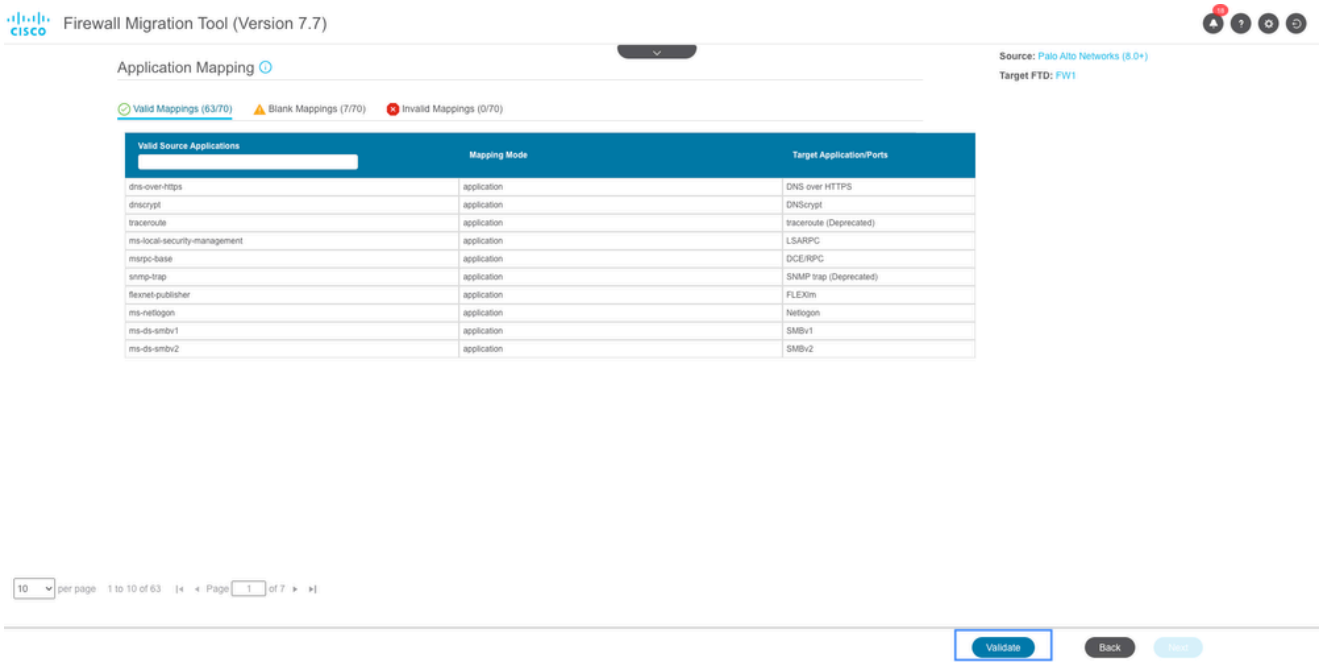
Manuelle Erstellung von Sicherheitszonen

Automatisches Erstellen von Sicherheitszonen:

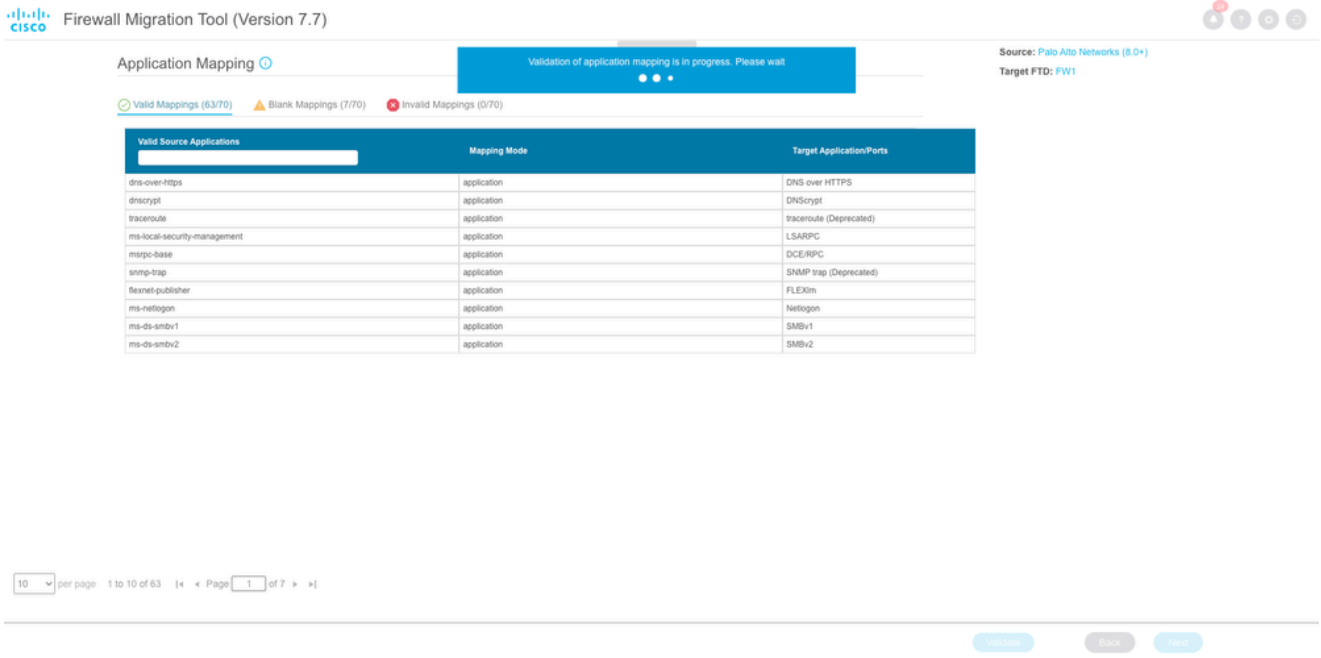


Erstellung automatischer Sicherheitszonen

16. Sie können nun zum Abschnitt "Anwendungszuordnung" wechseln. Klicken Sie auf Validieren, um die Anwendungszuordnung zu validieren.



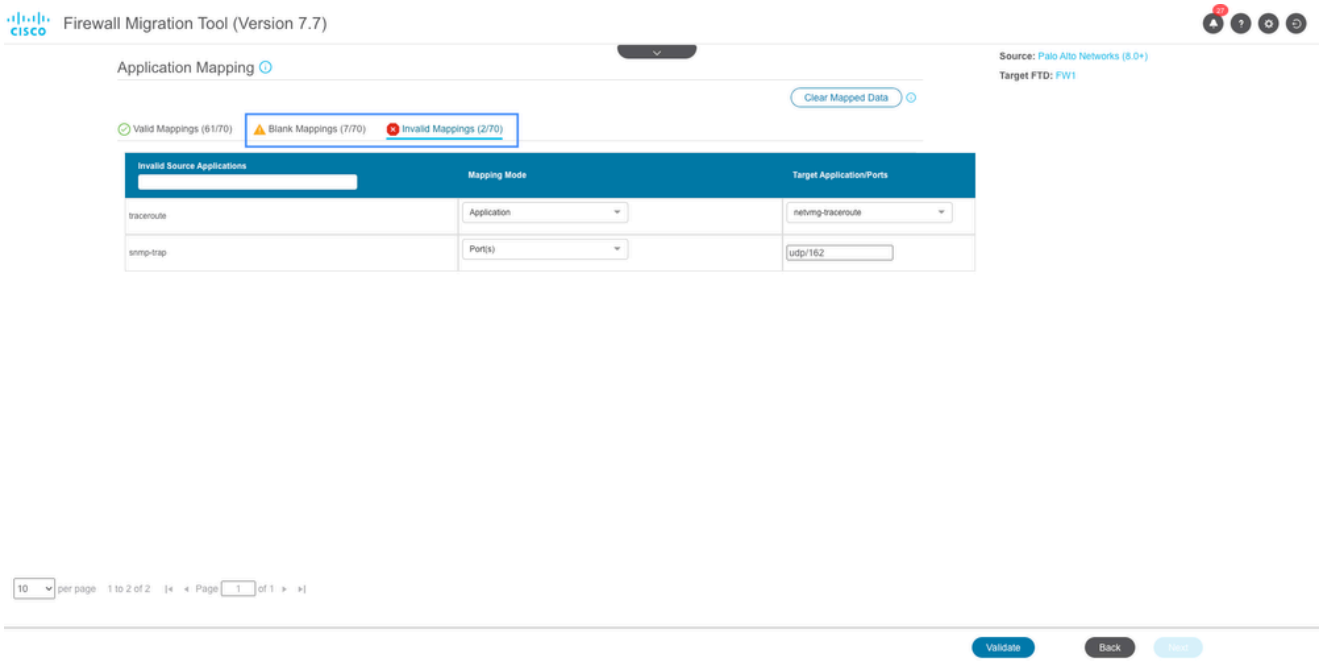
Anwendungszuordnung



Validierung der Anwendungszuordnung

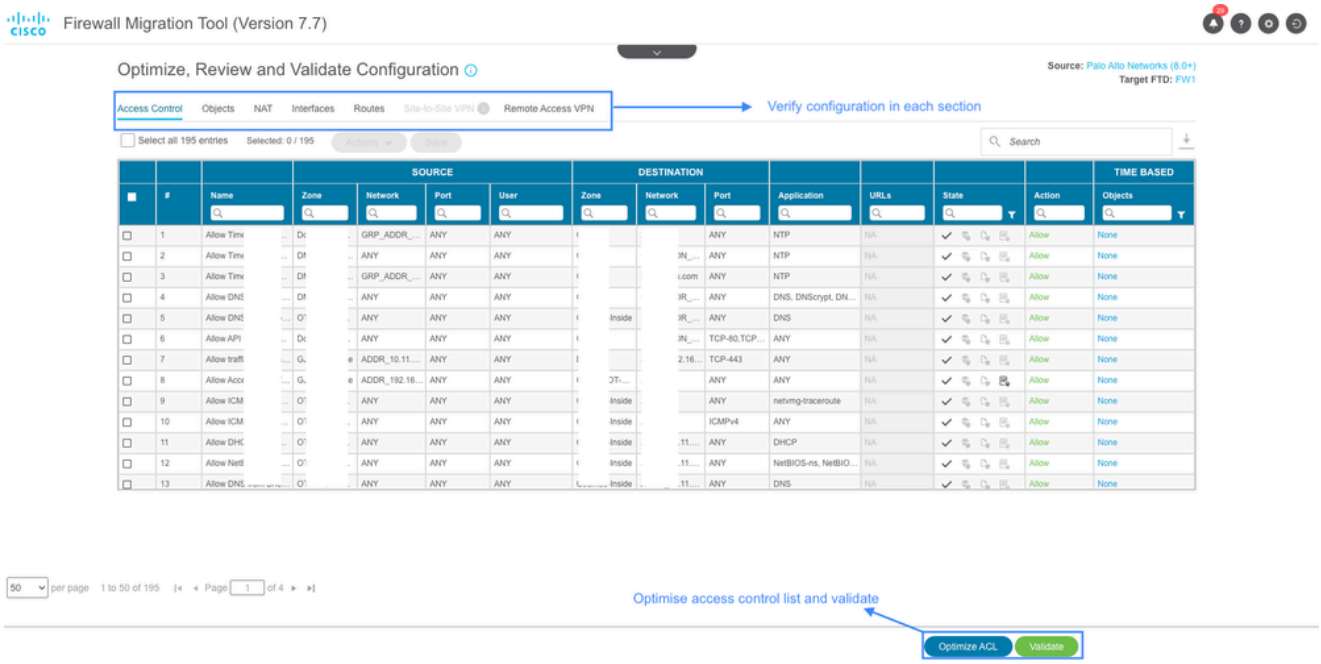
Nach der Validierung listet FMT die leeren und ungültigen Zuordnungen auf. Ungültige Zuordnungen müssen korrigiert werden, bevor Sie fortfahren. Das Korrigieren von leeren Zuordnungen ist optional.

Klicken Sie erneut auf Validieren, um die korrigierten Zuordnungen zu validieren. Klicken Sie nach der erfolgreichen Validierung auf Weiter.



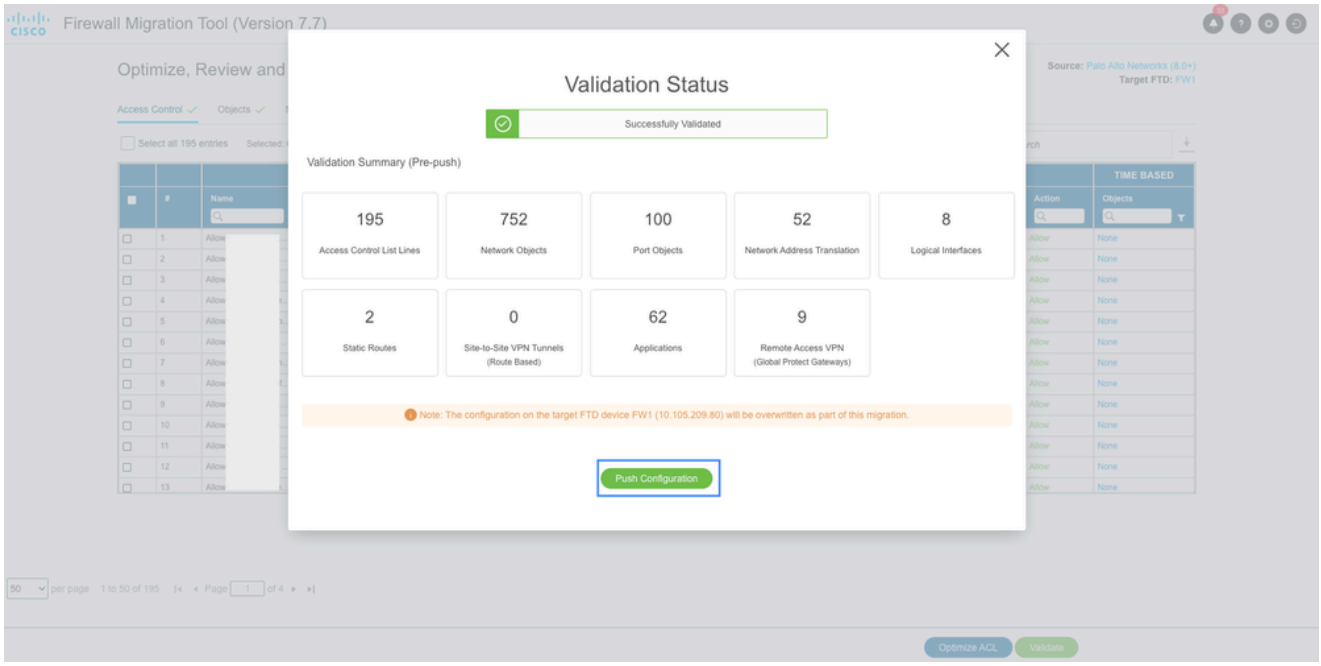
Leere und ungültige Anwendungszuordnung

17. Die ACL kann bei Bedarf im nächsten Abschnitt optimiert werden. Überprüfen Sie die Konfiguration in den einzelnen Abschnitten, z. B. Zugriffskontrolle, Objekte, NAT, Schnittstellen, Routen und RAS-VPN. Klicken Sie nach dem Überprüfen der Konfigurationen auf Validieren.



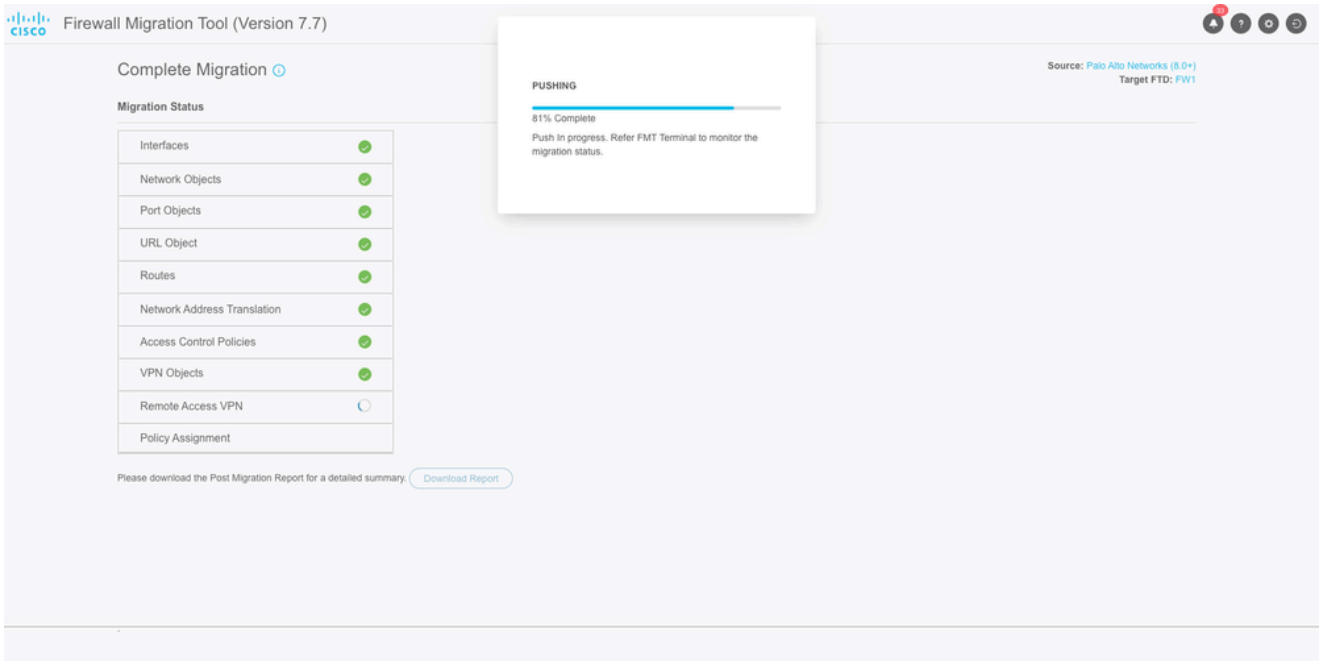
Validierung der Konfiguration

18. Nachdem die Validierung erfolgreich abgeschlossen wurde, wird eine Validierungsübersicht angezeigt. Klicken Sie auf Push Configuration, um die Konfiguration an das Ziel-FMC weiterzuleiten.



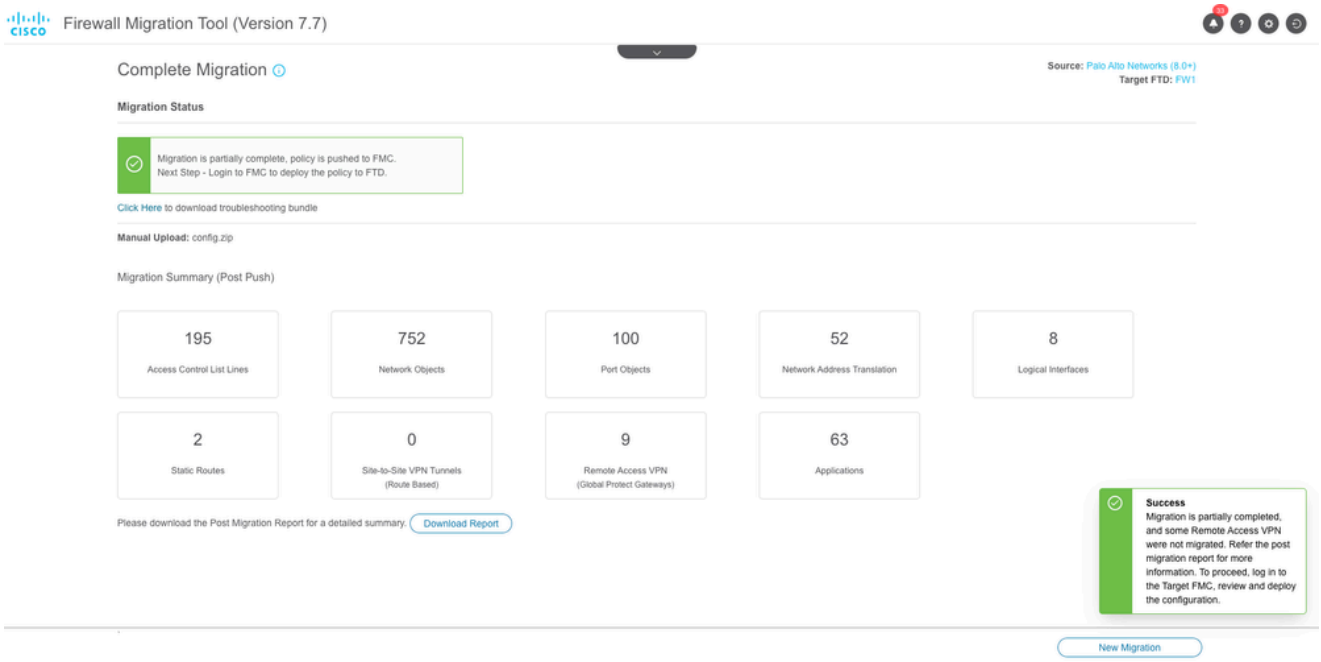
Zusammenfassung der Konfigurationsvalidierung

19. Der Fortschritt des Konfigurations-Pushvorgangs an FMC wird jetzt im Abschnitt "Migrationsstatus" angezeigt. Sie können das FMT-Terminalfenster auch zur Überwachung des Migrationsstatus verwenden.



Migrationsstatus

20. Nach erfolgreicher Migration zeigt das Tool eine Migrationsübersicht an. Es werden auch teilweise migrierte Konfigurationen aufgeführt, falls vorhanden. Beispiel: Konfiguration des Remotezugriff-VPN in diesem Szenario aufgrund eines fehlenden Secure Client Package. Sie können auch den Bericht nach der Migration herunterladen, um die migrierten Konfigurationen zu überprüfen und festzustellen, ob Fehler oder Korrekturen erforderlich sind.



Zusammenfassung der erfolgreichen Migration

21. Der letzte Schritt besteht darin, die migrierte Konfiguration von FMC zu überprüfen und die Konfiguration auf FTD bereitzustellen.
    So stellen Sie die Konfiguration bereit:
    1. Melden Sie sich an der FMC-GUI an.
    2. Navigieren Sie zur Registerkarte Bereitstellen.

3. Wählen Sie die Bereitstellung aus, um die Konfiguration per Push an die Firewall weiterzuleiten.
4. Klicken Sie auf Bereitstellen.

Fehlerbehebung

Fehlerbehebung Secure Firewall Migration-Tool

Häufige Migrationsfehler:

- Unbekannte oder ungültige Zeichen in der PaloAlto-Konfigurationsdatei.
- Fehlende oder unvollständige Konfigurationselemente.
- Probleme mit der Netzwerkverbindung oder Latenz.
- Probleme beim Hochladen der PaloAlto-Konfigurationsdatei oder beim Übertragen der Konfiguration an das FMC.

Verwenden des Support-Pakets zur Fehlerbehebung:

- Klicken Sie im Bildschirm "Complete Migration" (Migration abschließen) auf die Schaltfläche Support.
- Wählen Sie Support Bundle und die herunterzuladenden Konfigurationsdateien aus.
- Protokoll- und DB-Dateien sind standardmäßig ausgewählt.
- Klicken Sie auf Herunterladen, um eine ZIP-Datei herunterzuladen.
- Extrahieren Sie die ZIP-Datei, um Protokolle, DB- und Konfigurationsdateien anzuzeigen.
- Klicken Sie auf Uns per E-Mail kontaktieren, um Fehlerdetails an das technische Team zu senden.
- Hängen Sie das Support-Paket an Ihre E-Mail an.
- Klicken Sie auf die Seite "TAC aufrufen", um ein Cisco TAC-Ticket zu 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.