Migration von ASA zu Firepower Threat Defense (FTD) mit FMT

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Migration der Cisco Adaptive Security Appliance (ASA) auf Cisco Firepower Threat Device beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der Cisco Firewall Threat Defense (FTD)- und Adaptive Security Appliance (ASA)-Lösungen verfügen.

Verwendete Komponenten

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

- Mac OS mit Firepower Migration Tool (FMT) v7.0.1
- Adaptive Security Appliance (ASA) v9.16(1)
- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.1

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:

- Cisco Adaptive Security Appliance (ASA) Version 8.4 oder höher
- 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)
- Fortinet (5,0+)

· · Palo Alto Networks (6.1+)

Hintergrundinformationen

Führen Sie vor der Migration Ihrer ASA-Konfiguration die folgenden Aktivitäten aus:

Abrufen der ASA-Konfigurationsdatei

Um ein ASA-Gerät zu migrieren, verwenden Sie show running-config für einen einzelnen Kontext oder show tech-support für den Multi-Context-Modus, um die Konfiguration abzurufen, speichern sie als .cfg- oder .txt-Datei und übertragen sie mit dem Secure Firewall Migration Tool auf den Computer.

PKI-Zertifikat von ASA exportieren und in Management Center importieren

Verwenden Sie diesen Befehl, um das PKI-Zertifikat über die CLI aus der ASA-Quellkonfiguration mit den Schlüsseln in eine PKCS12-Datei zu exportieren:
ASA(config)#crypto kann <trust-point-name> pkcs12 <Passphrase> exportieren
Importieren Sie dann das PKI-Zertifikat in ein Verwaltungscenter (Object Management PKI Objects). Weitere Informationen finden Sie unter PKI-Objekte im Konfigurationsleitfaden für das FirePOWER Management Center.

Abrufen von AnyConnect-Paketen und -Profilen

AnyConnect-Profile sind optional und können über das Management Center oder das Secure Firewall Migration Tool hochgeladen werden.

Verwenden Sie diesen Befehl, um das erforderliche Paket von der Quell-ASA auf einen FTP- oder TFTP-Server zu kopieren:

Kopieren Sie <Quelldateispeicherort:/Quelldateiname> <Ziel>

ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Beispiel zum Kopieren von AnyConnect-Paketen.

ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Beispiel zum Kopieren eines externen Browserpakets.

ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Beispiel zum Kopieren des Hostscan-Pakets.

ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Beispiel zum Kopieren von Dap.xml

ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Beispiel zum Kopieren von Data.xml

ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Beispiel für das Kopieren von AnyConnect-Profil.

Importieren Sie die heruntergeladenen Pakete in das Management Center (Objektverwaltung > VPN > AnyConnect-Datei).

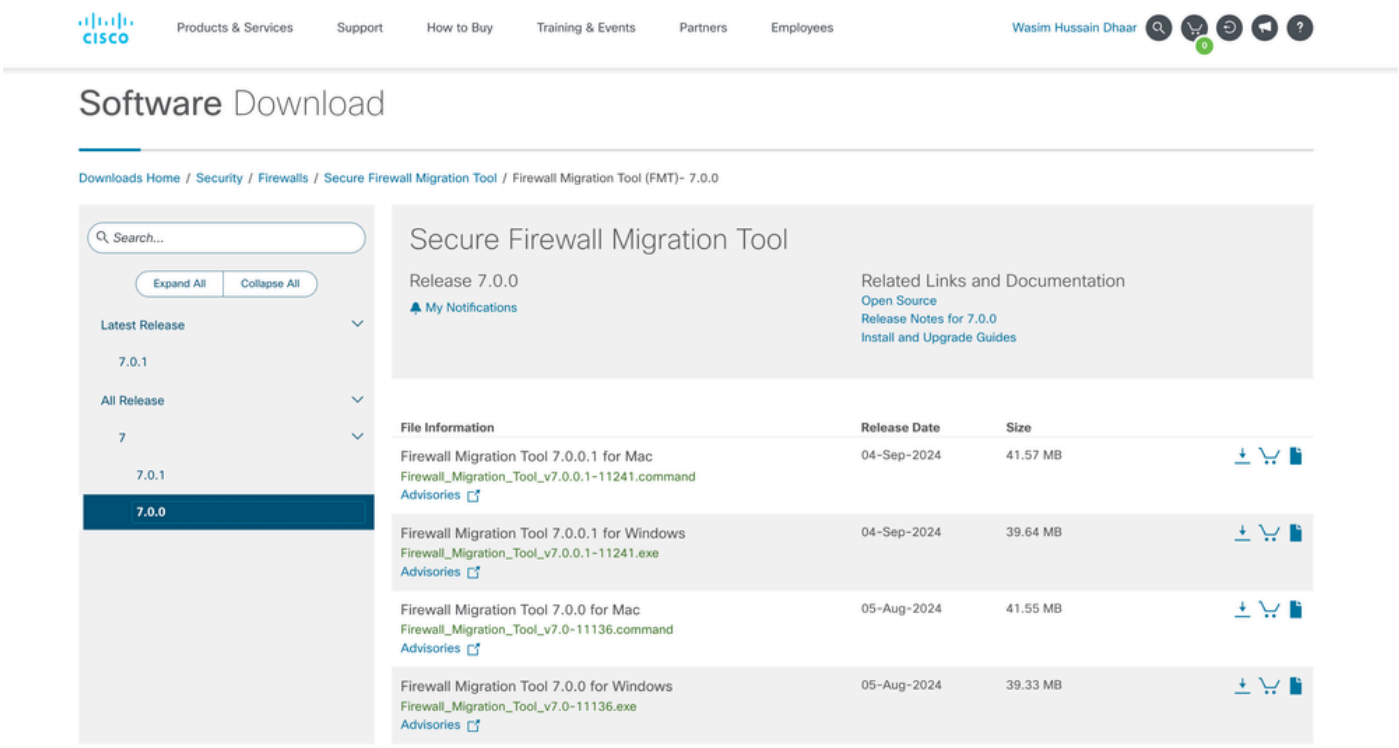
a-Dap.xml und Data.xml müssen über das Migrationstool für sichere Firewalls im Abschnitt Prüfen und validieren > Remotezugriff-VPN > AnyConnect-Datei in das Verwaltungscenter hochgeladen werden.

b-AnyConnect-Profile können direkt in das Management Center hochgeladen werden oder über das Migrationstool Secure Firewall im Abschnitt Prüfen und validieren > Remote Access VPN > AnyConnect-Datei.

Konfigurieren

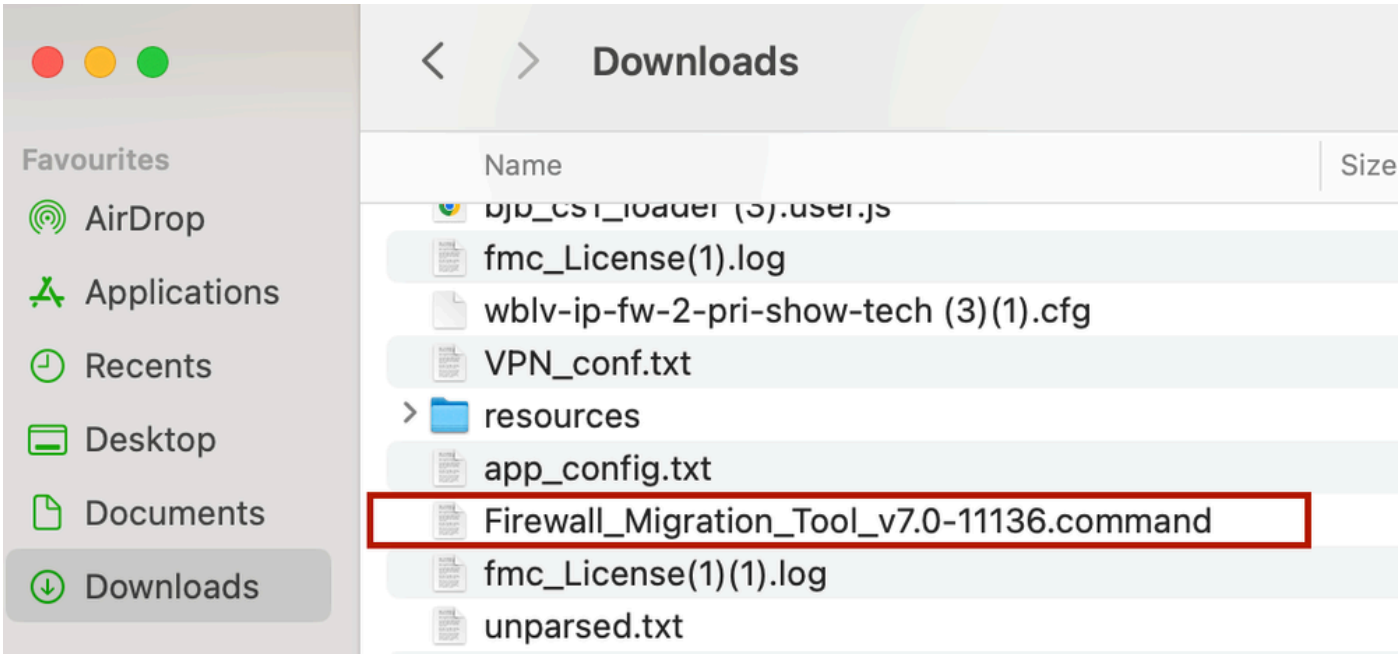
Konfigurationsschritte:

1.Herunterladen das neueste Firepower Migration Tool von Cisco Software Central:

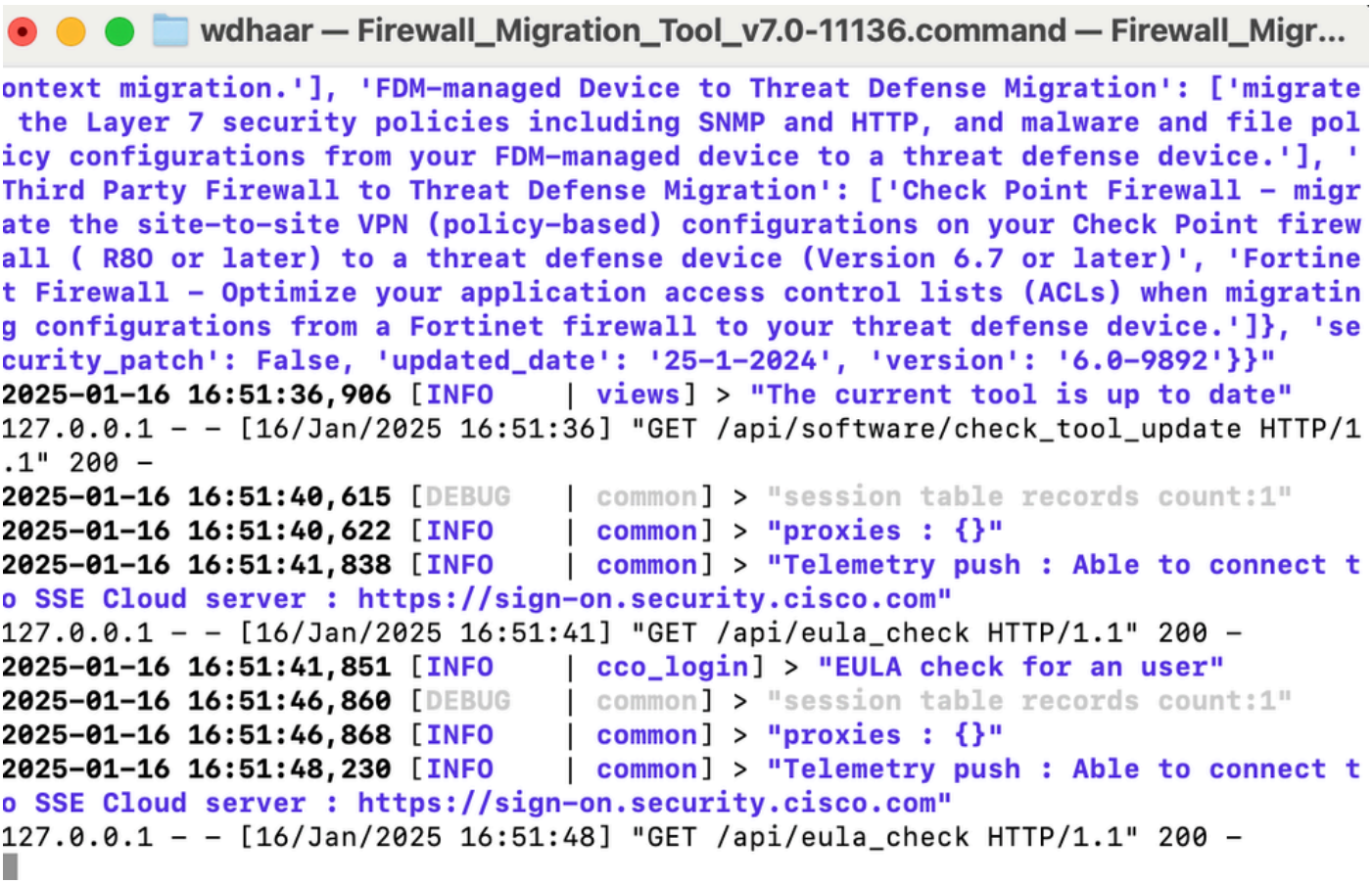


Software-Download

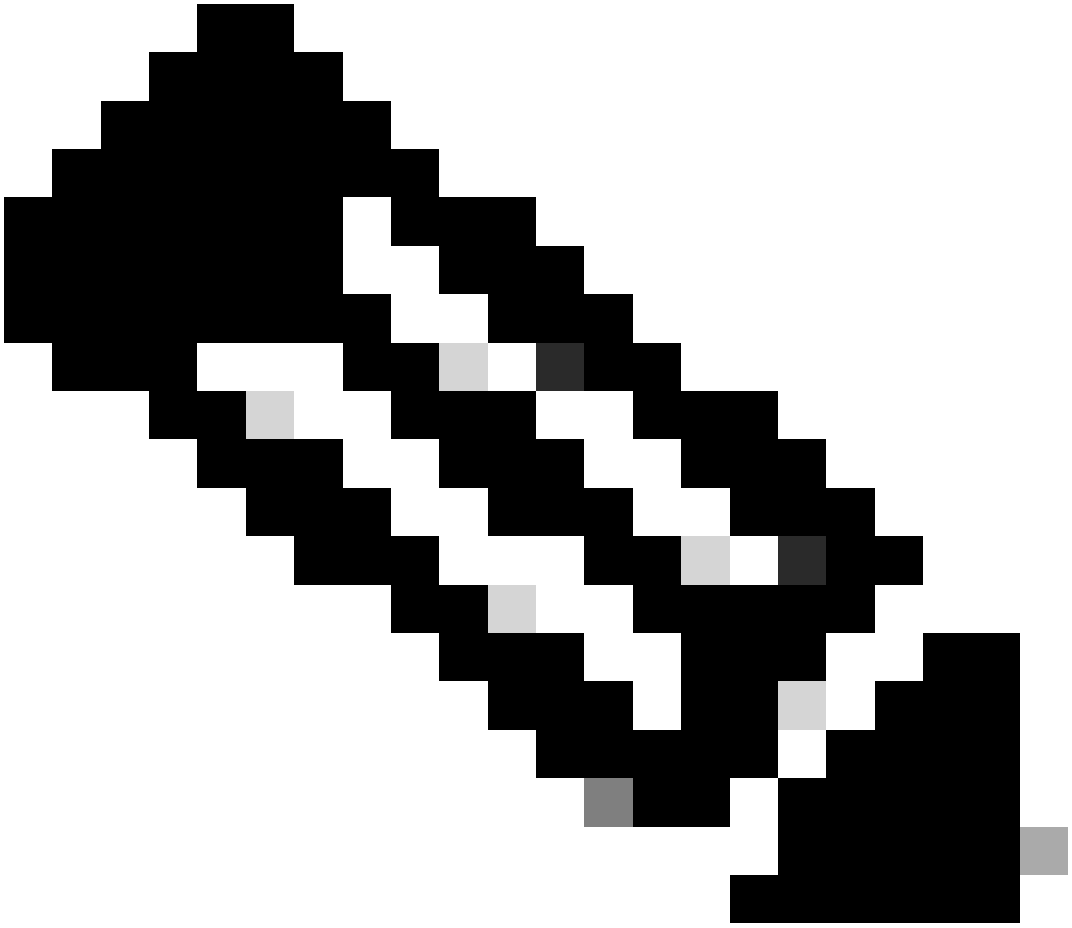
2. Klicken Sie auf die Datei, die Sie zuvor auf Ihren Computer heruntergeladen haben.



Die Datei

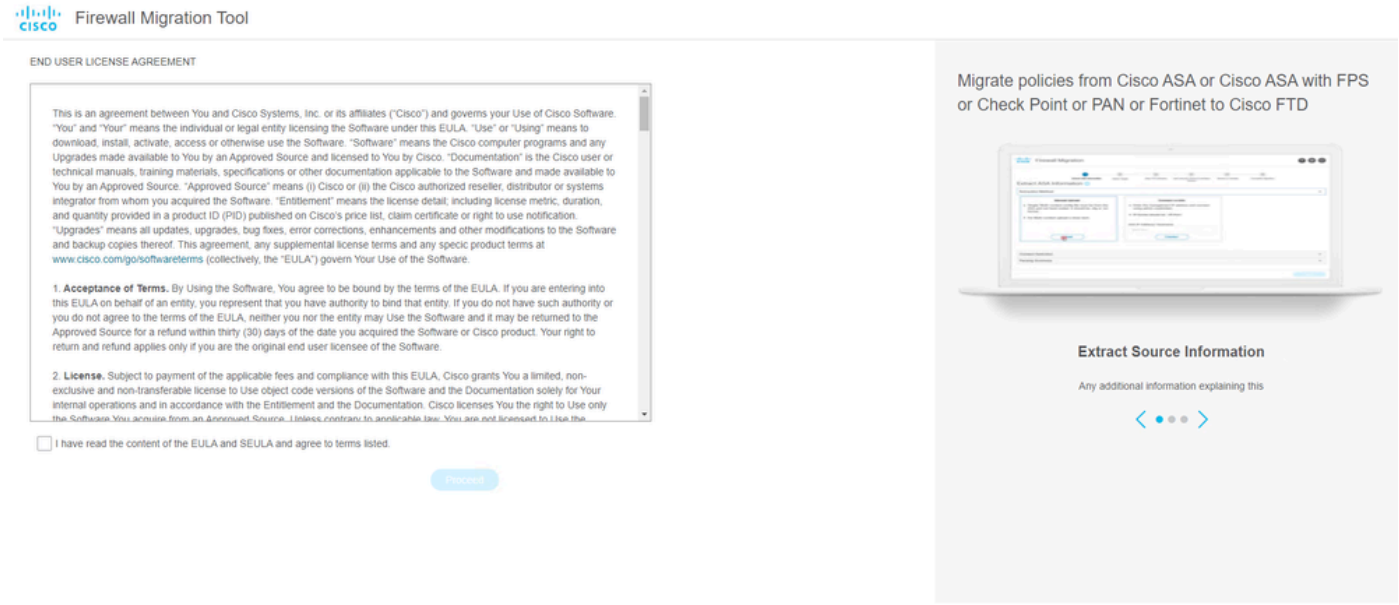


Konsolenprotokolle



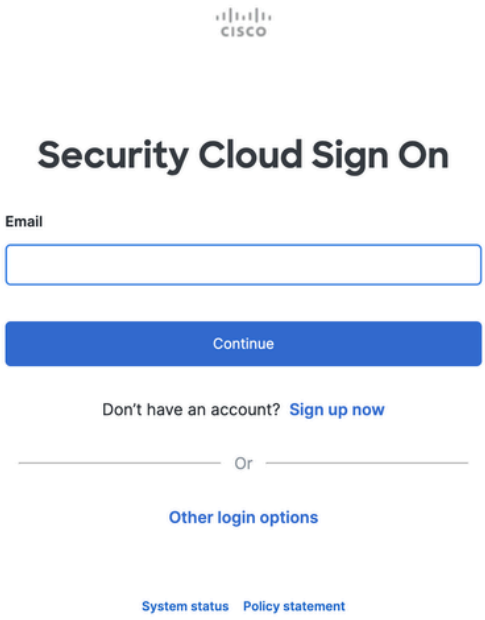
Anmerkung: Das Programm wird automatisch geöffnet, und eine Konsole generiert automatisch Inhalte für das Verzeichnis, in dem Sie die Datei ausgeführt haben.

3. Nachdem Sie das Programm ausgeführt haben, 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.



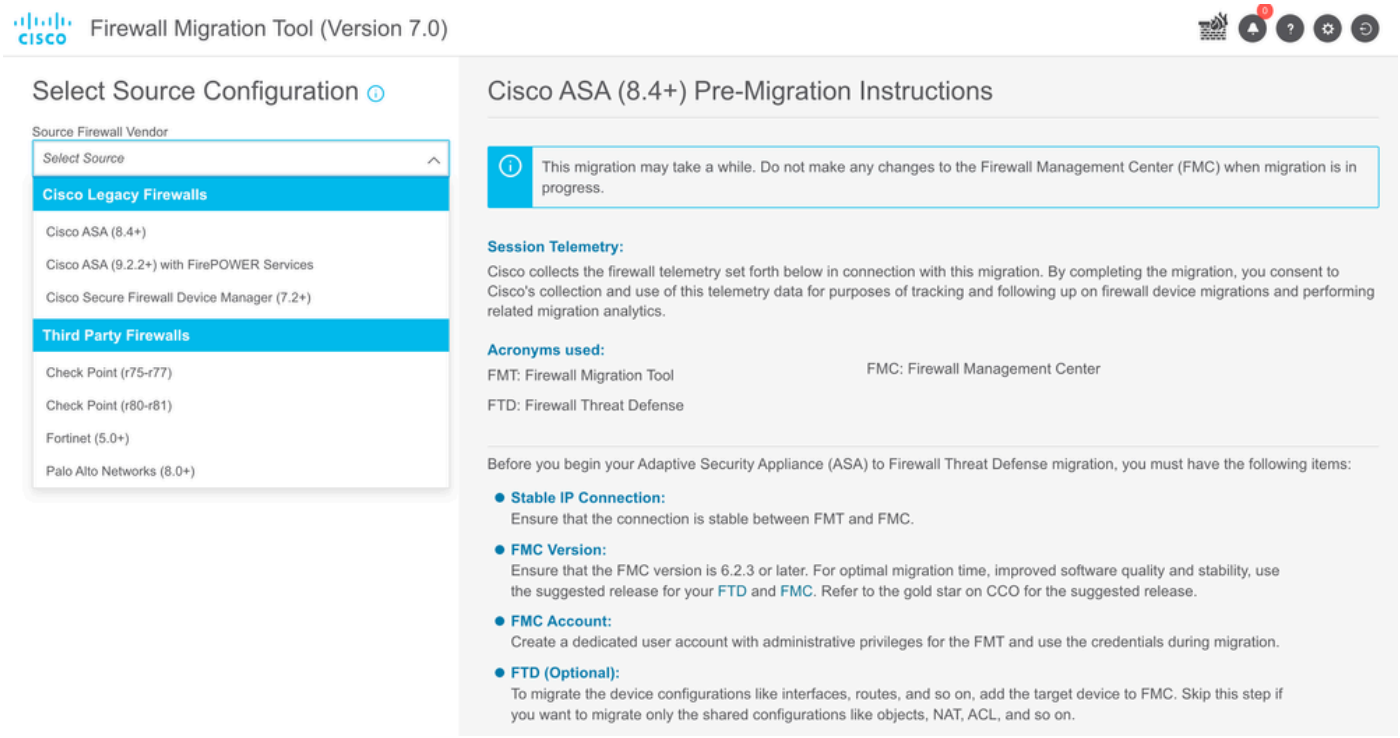
EULA

4. Melden Sie sich mit einem gültigen CCO-Konto an, und die grafische FMT-Benutzeroberfläche wird im Webbrowser angezeigt.



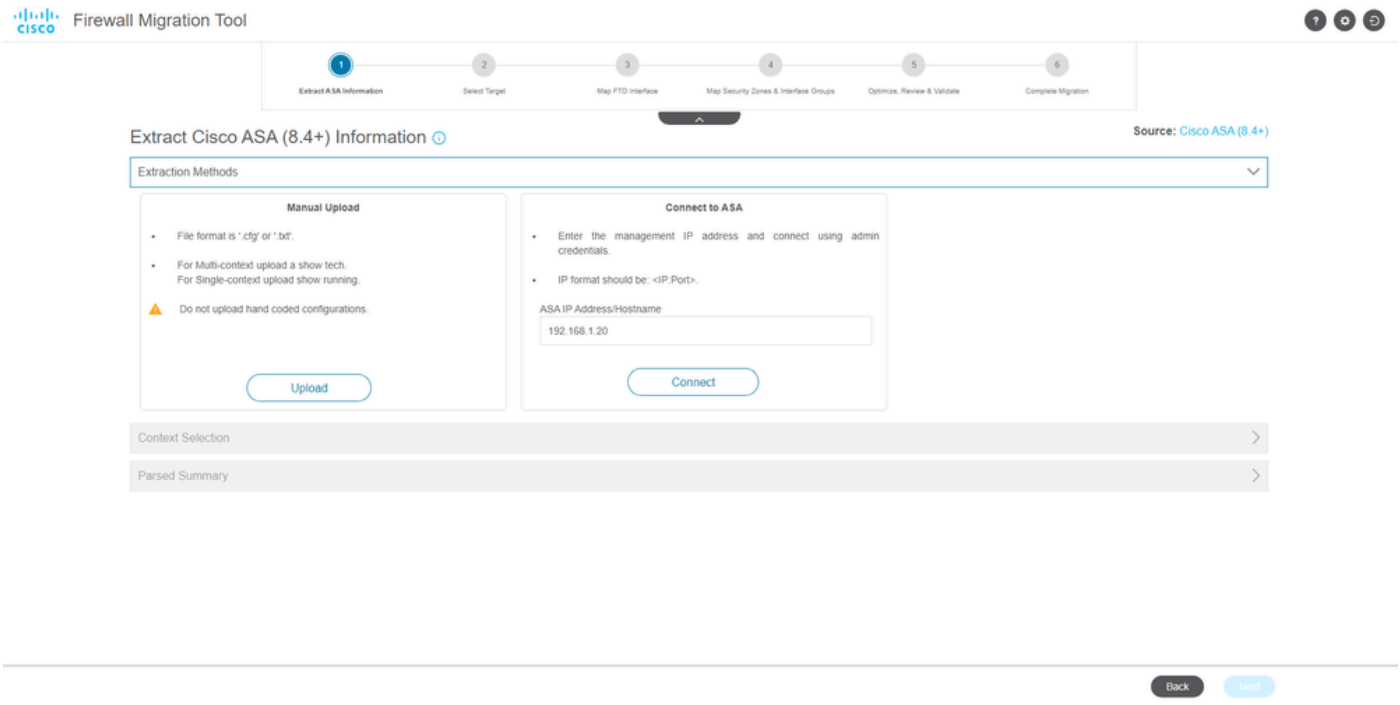
FMT-Anmeldung

5. Wählen Sie die zu migrierende Quell-Firewall aus.

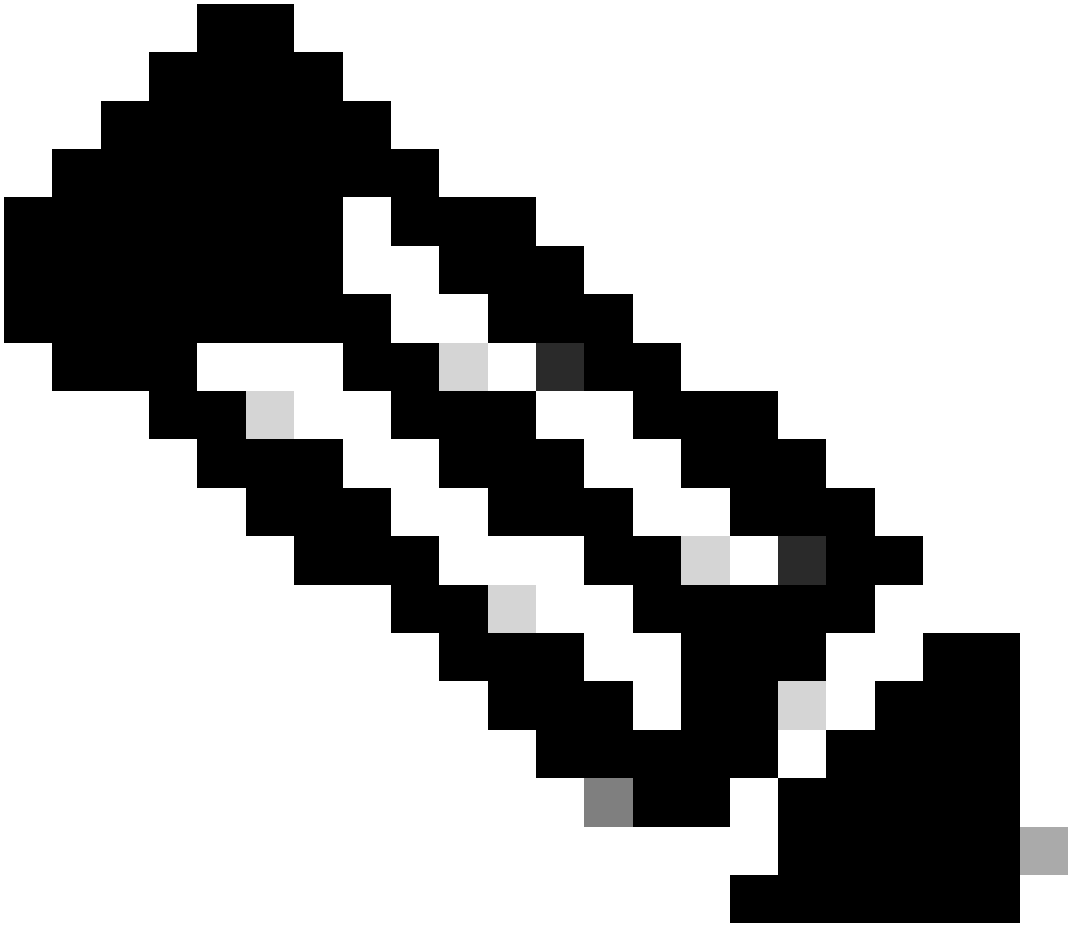


Quell-Firewall

6. Wählen Sie die Extraktionsmethode aus, die zum Abrufen der Konfiguration verwendet werden soll.
    1. Beim manuellen Hochladen müssen Sie die **Running Config** Datei der ASA im Format ".cfg" oder ".txt" hochladen.
    2. Stellen Sie eine Verbindung zur ASA her, um Konfigurationen direkt aus der Firewall zu extrahieren.

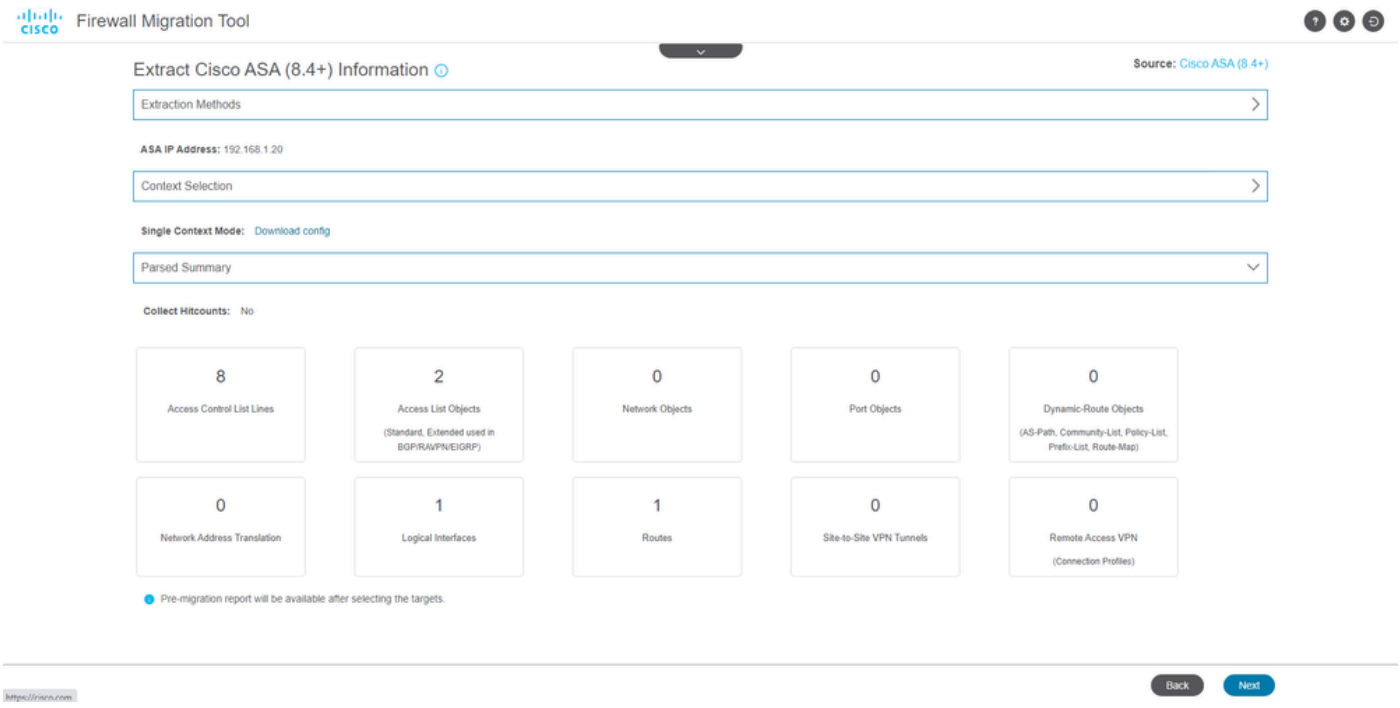


Extraktion



Anmerkung: In diesem Beispiel stellen Sie eine direkte Verbindung mit der ASA her.

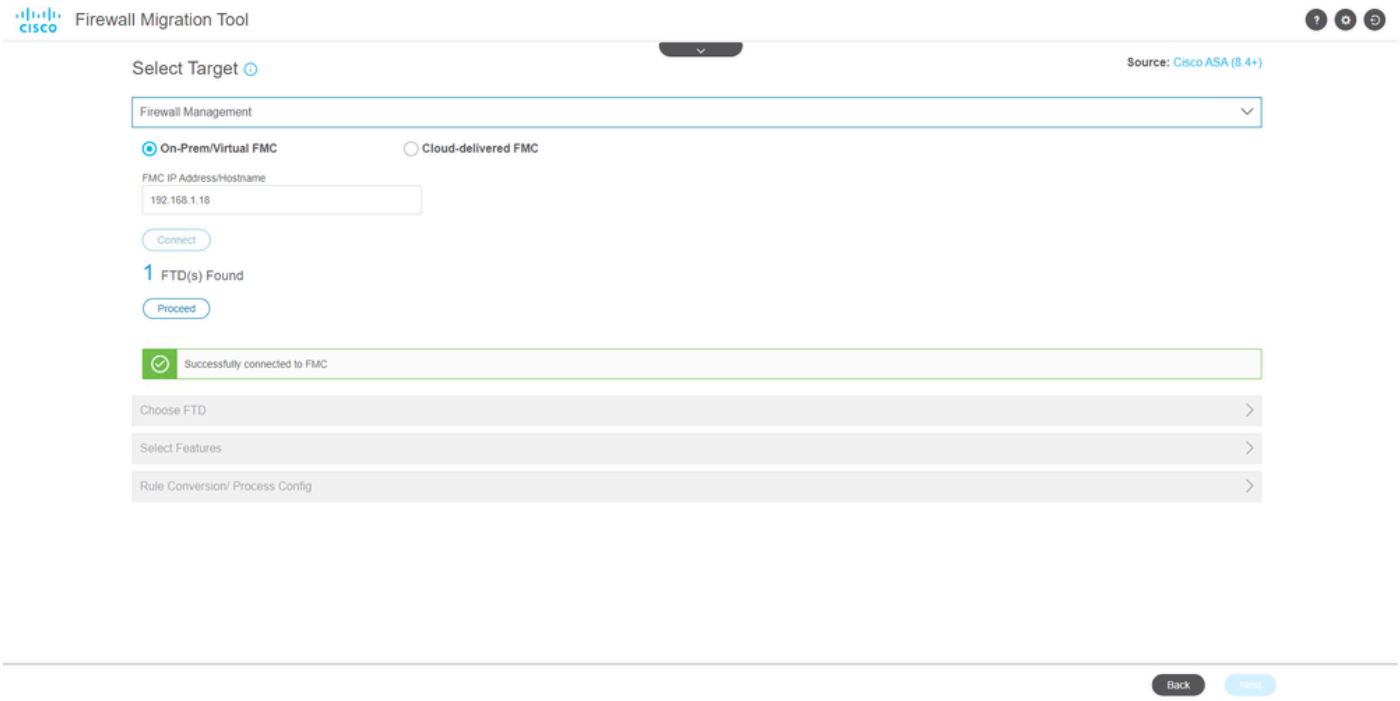
7. Eine Zusammenfassung der auf der Firewall gefundenen Konfiguration wird als Dashboard angezeigt. Klicken Sie auf "Weiter".



Zusammenfassung

8. Wählen Sie das Ziel-FMC, das für die Migration verwendet werden soll.

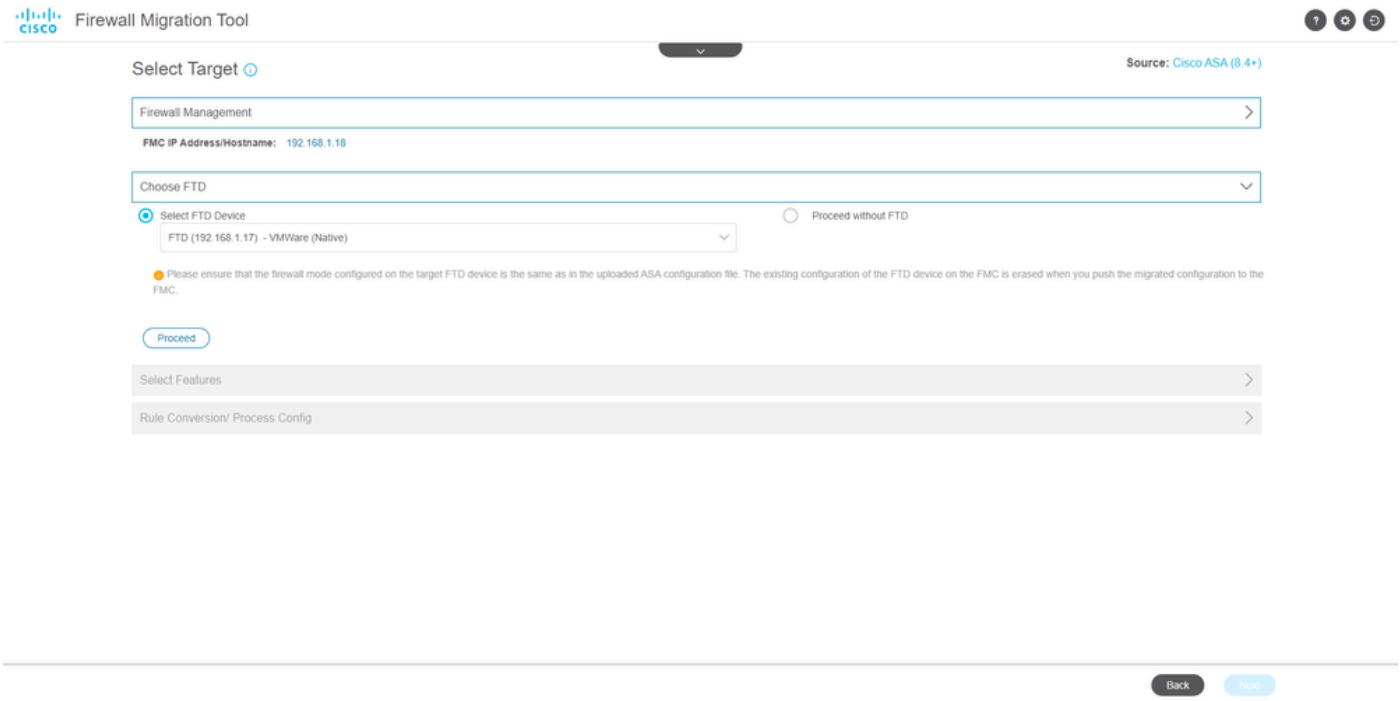
Geben Sie die IP-Adresse des FMC ein. Es öffnet ein Popup-Fenster, in dem Sie zur Eingabe der Anmeldeinformationen des FMC aufgefordert werden.



FMC-IP

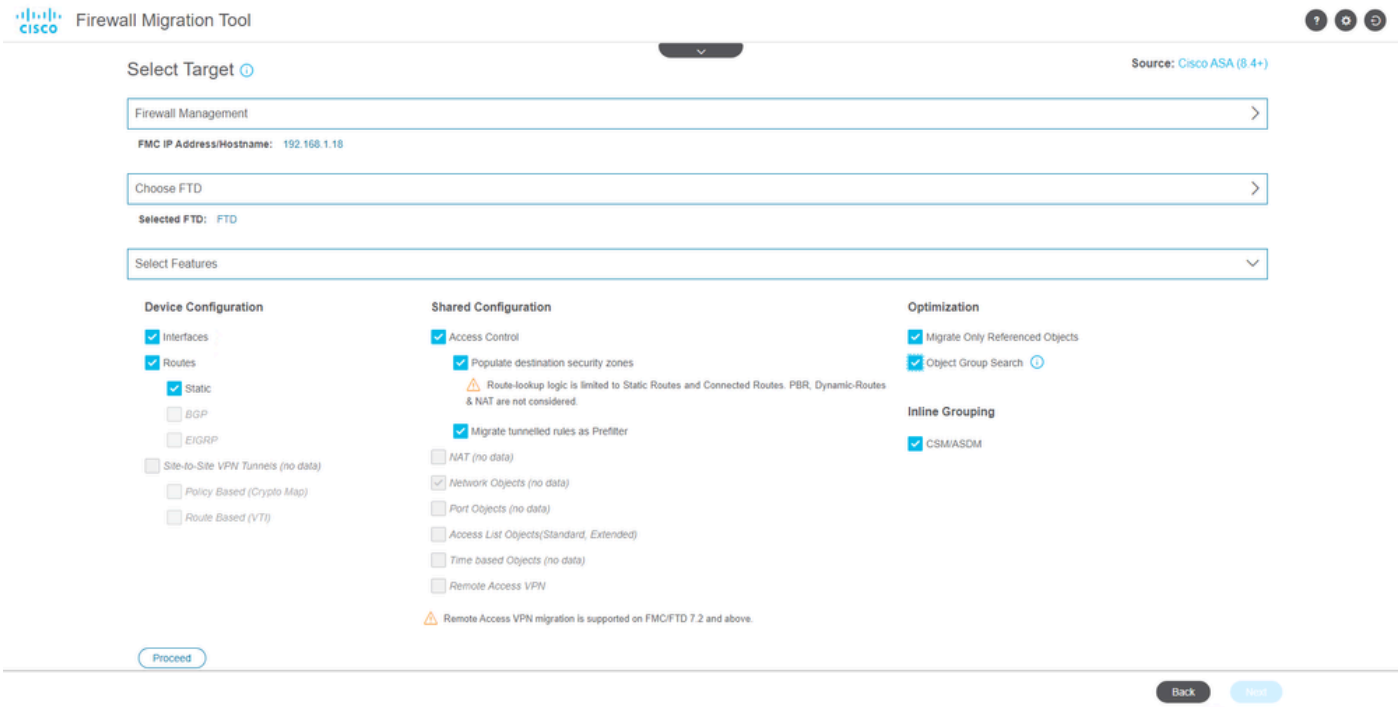
9. (Optional)Wählen Sie die FTD-Zielnummer aus, die Sie verwenden möchten.
    1. Wenn Sie zu einem FTD migrieren möchten, wählen Sie das FTD aus, das Sie verwenden möchten.
    2. Wenn Sie kein FTD verwenden möchten, können Sie das Kontrollkästchen aktivieren.

Proceed without FTD



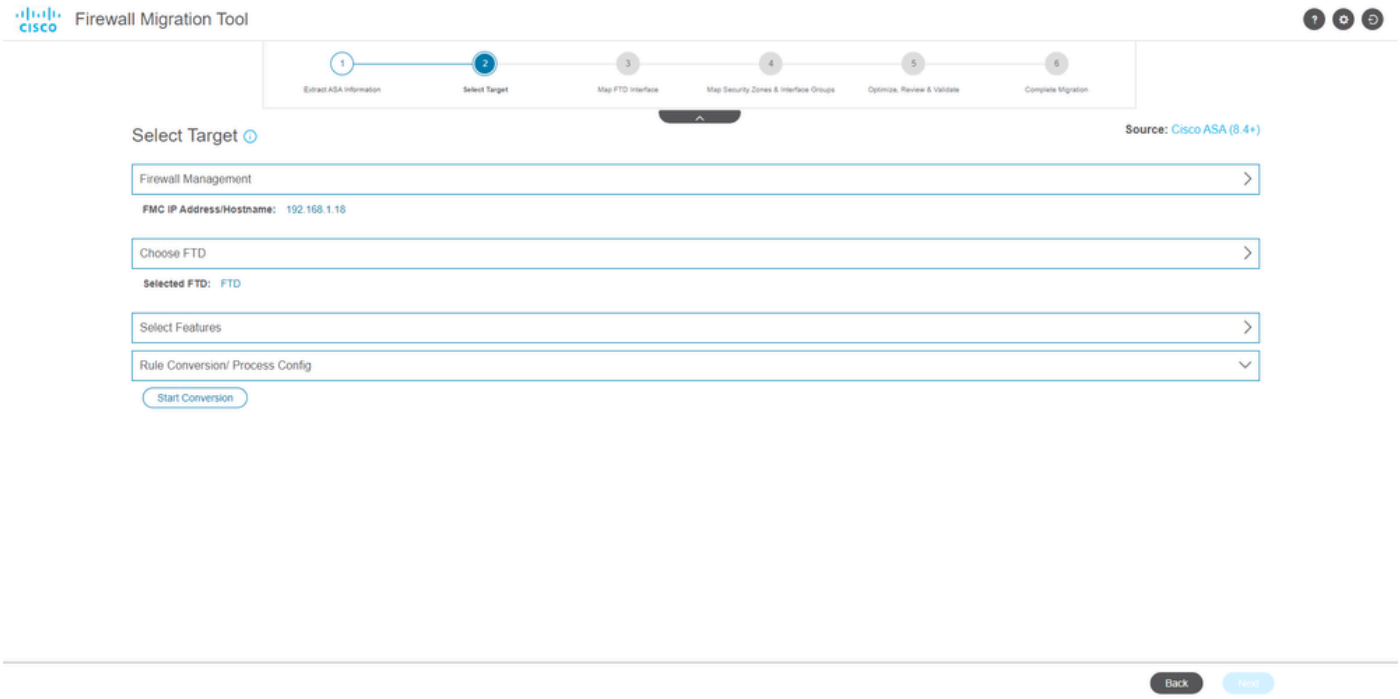
Ziel-FTD

10. Wählen Sie die Konfigurationen aus, die migriert werden sollen. Die Optionen werden in den Screenshots angezeigt.



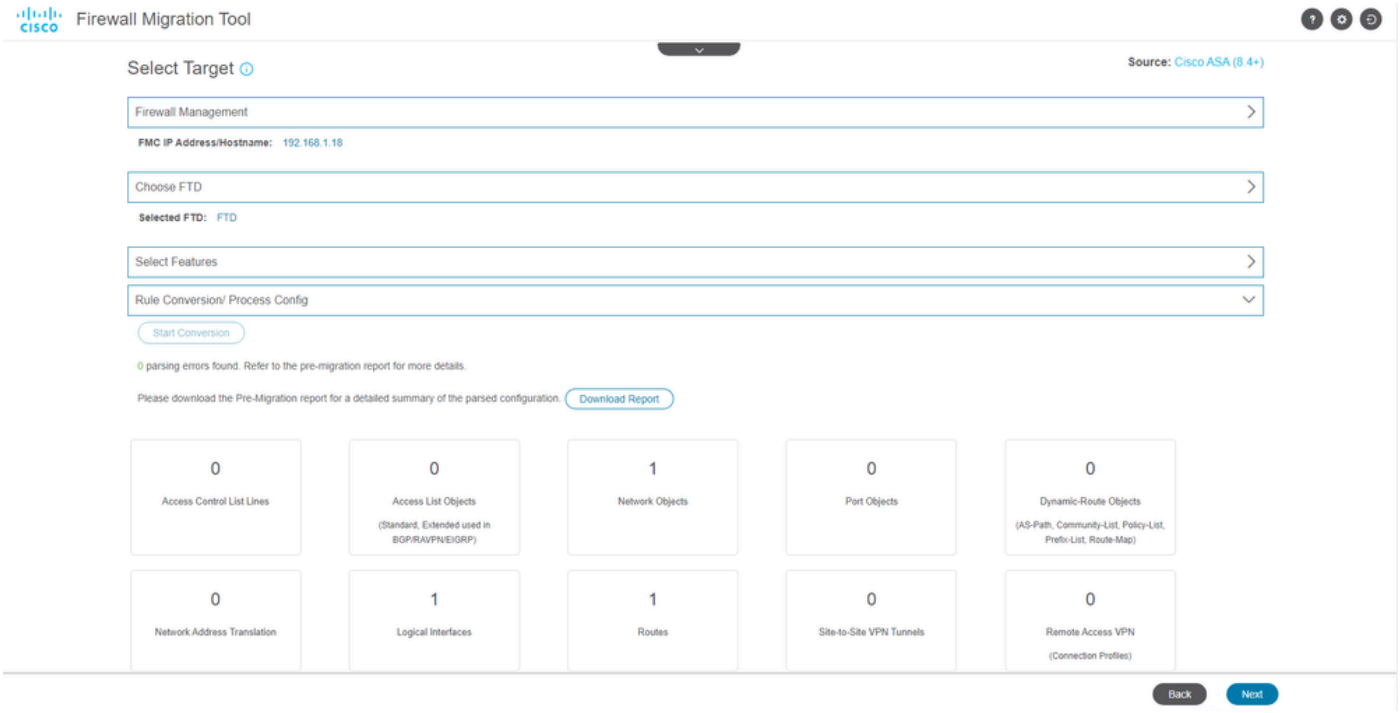
Konfigurationen

11. Starten Sie die Umwandlung der Konfigurationen von ASA in FTD.



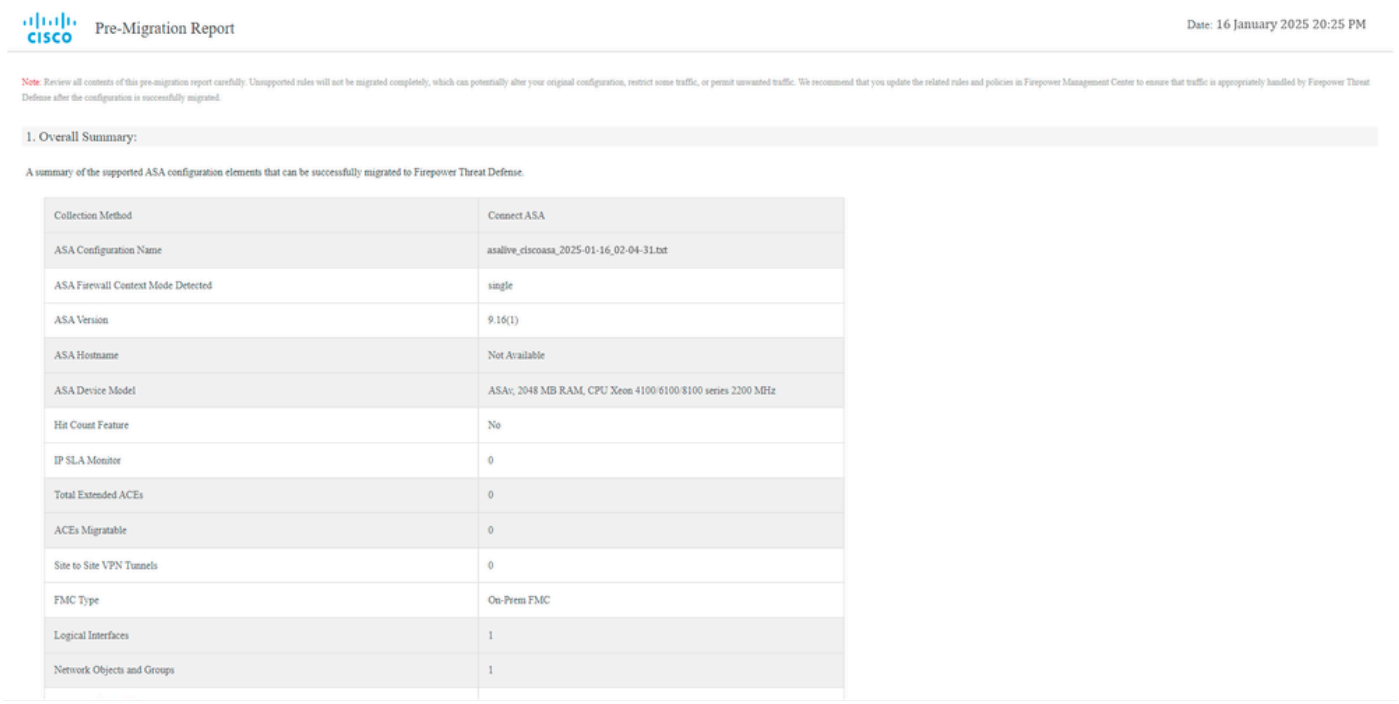
Konvertierung starten

12. Nach Abschluss der Konvertierung wird ein Dashboard mit der Zusammenfassung der zu migrierenden Objekte angezeigt (auf Kompatibilität beschränkt).
    1. Optional können Sie auf klicken**Download Report**, um eine Zusammenfassung der zu migrierenden Konfigurationen anzuzeigen.



Bericht herunterladen

Beispiel für einen Bericht vor der Migration, wie in der Abbildung dargestellt:



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.

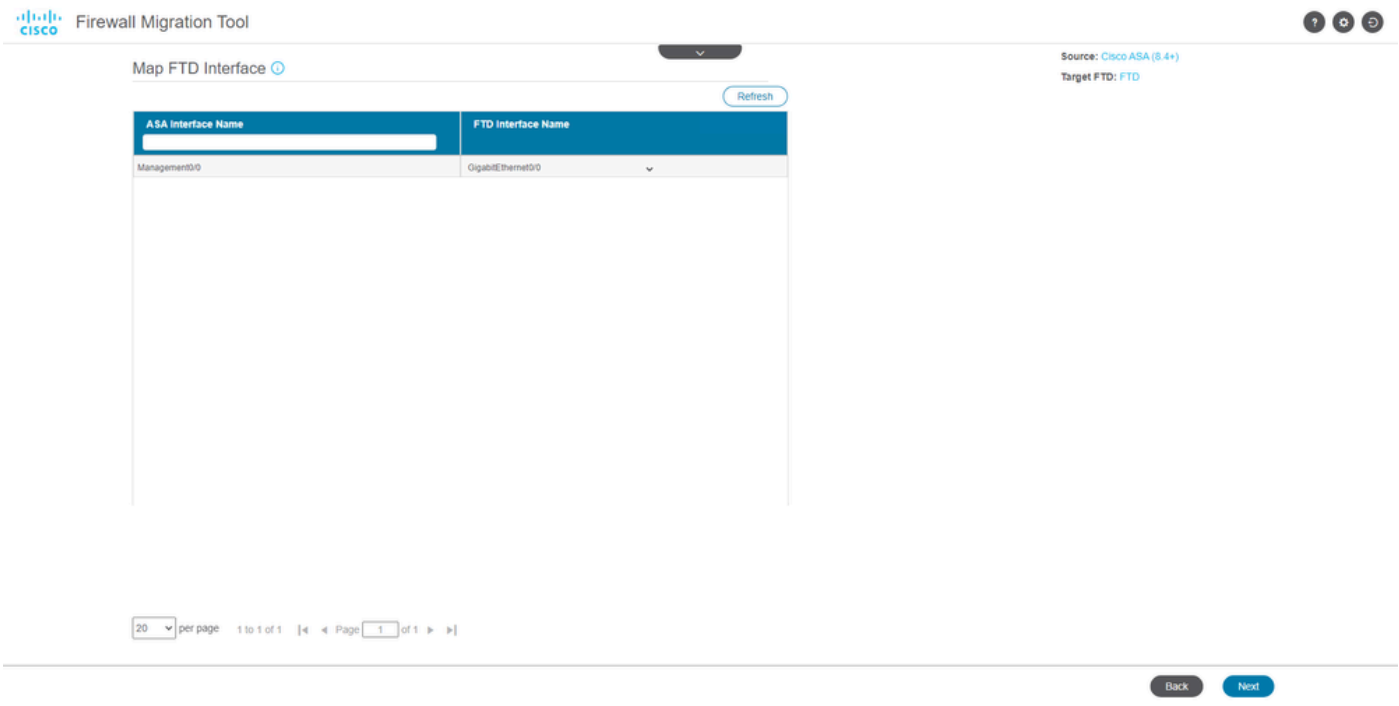
1. Overall Summary:

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

Bericht vor der Migration

13. Ordnen Sie die ASA-Schnittstellen den FTD-Schnittstellen des Migrations-Tools zu.



Firewall Migration Tool

Map FTD Interface

Source: Cisco ASA (8.4+)

Target FTD: FTD

Refresh

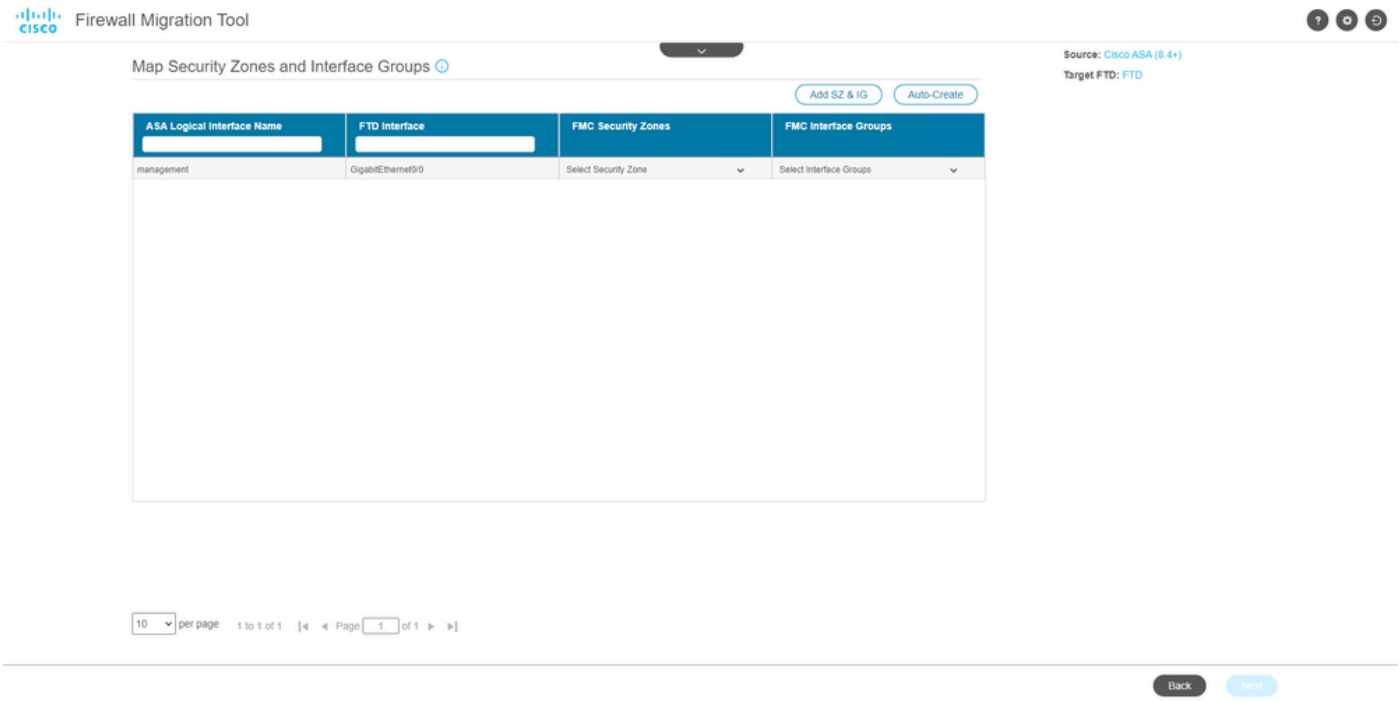
ASA Interface Name	FTD Interface Name
Management0/0	GigabitEthernet0/0

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

Back Next

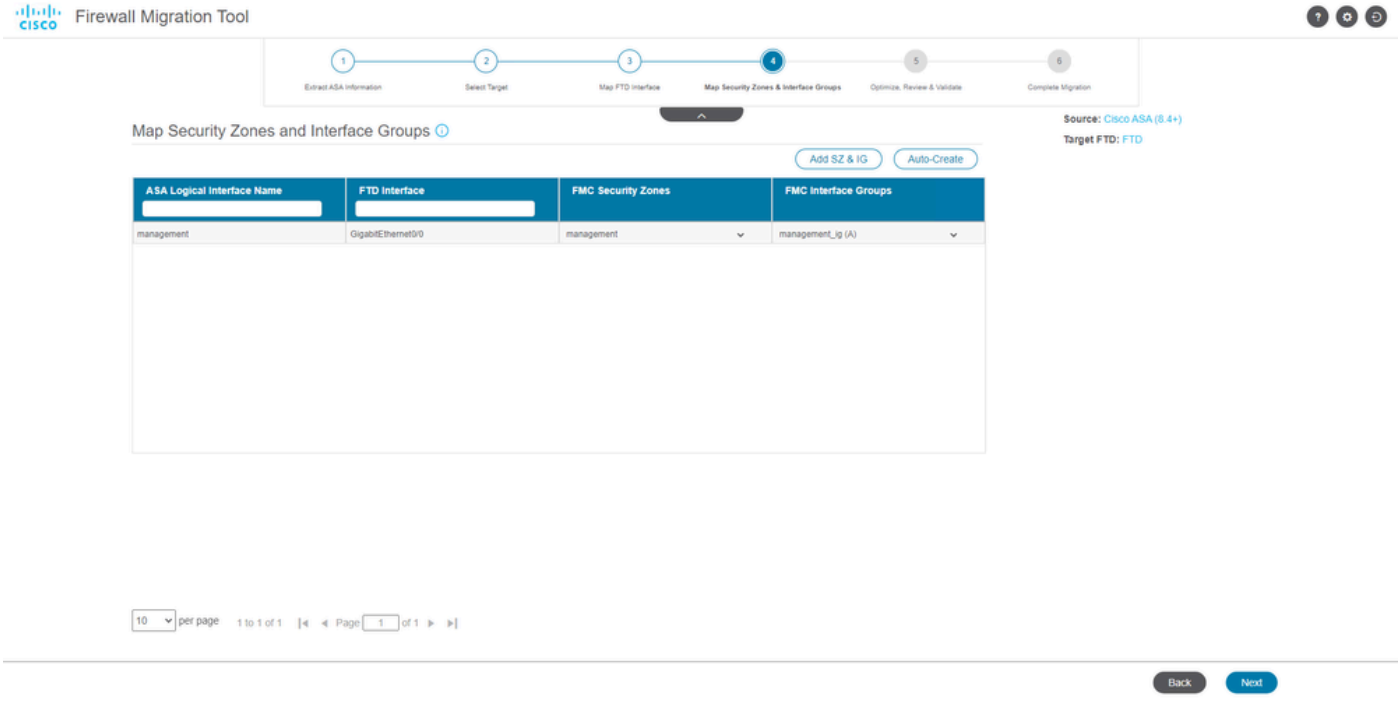
Schnittstellen zuordnen

14. Erstellen Sie die Sicherheitszonen und Schnittstellengruppen für die Schnittstellen auf dem FTD.



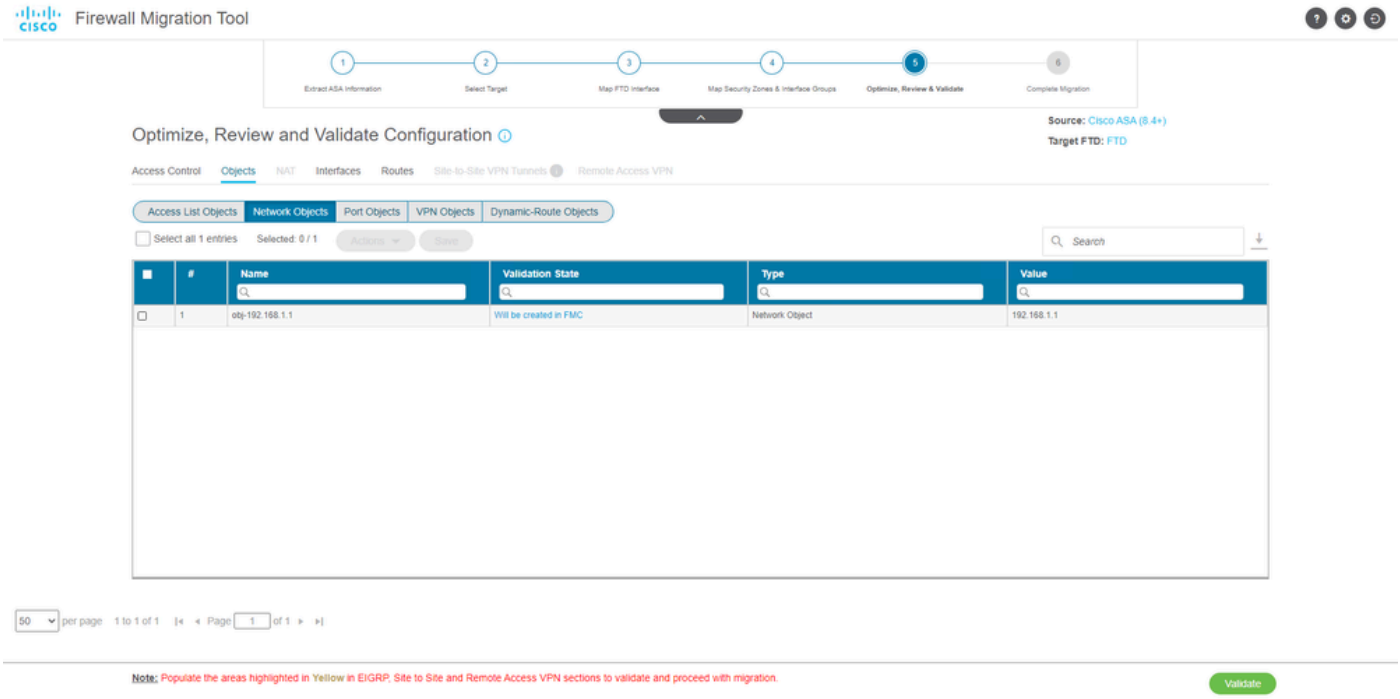
Sicherheitszonen und Schnittstellengruppen

Sicherheitszonen (SZ) und Schnittstellengruppen (IG) werden automatisch vom Tool erstellt, wie im Bild gezeigt:



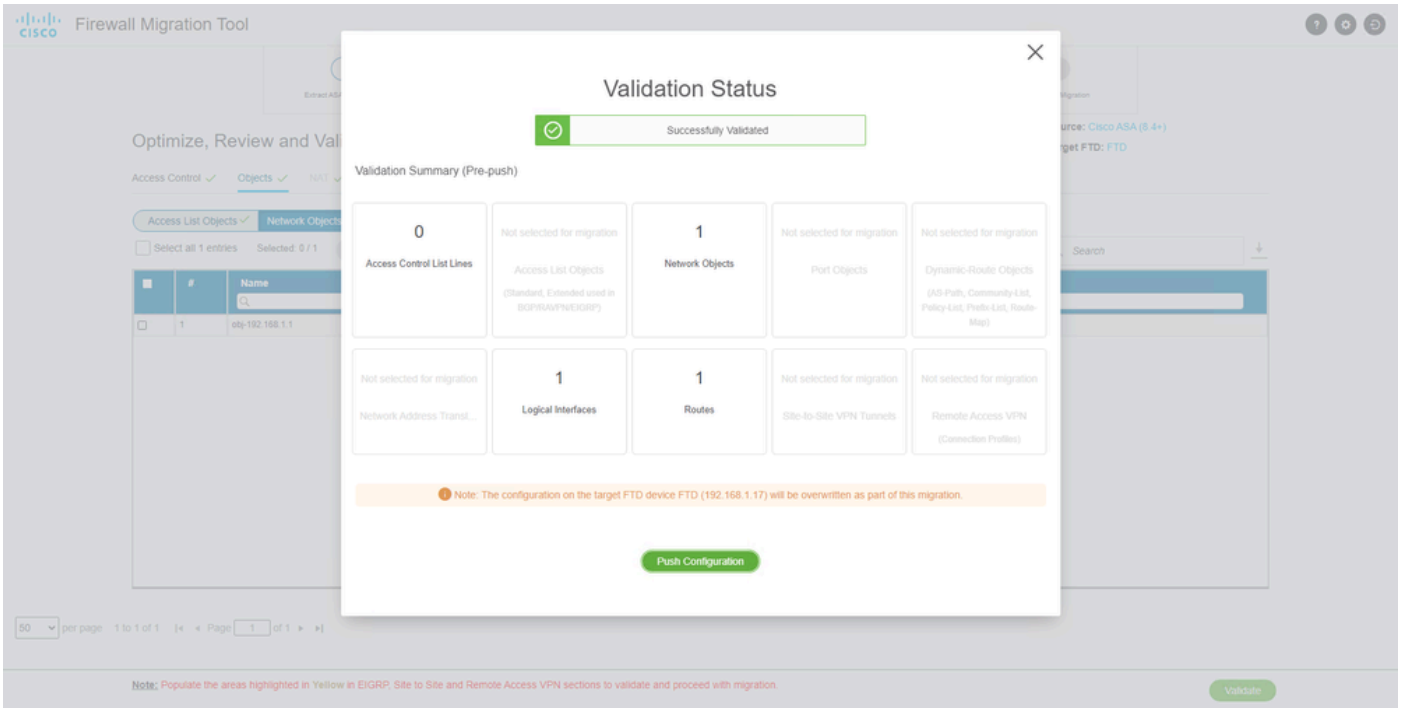
Tool zum automatischen Erstellen

15. Prüfen und validieren Sie die zu migrierenden Konfigurationen im Migrations-Tool.
    1. Wenn Sie die Überprüfung und Optimierung der Konfigurationen bereits abgeschlossen haben, klicken Sie auf Validate.



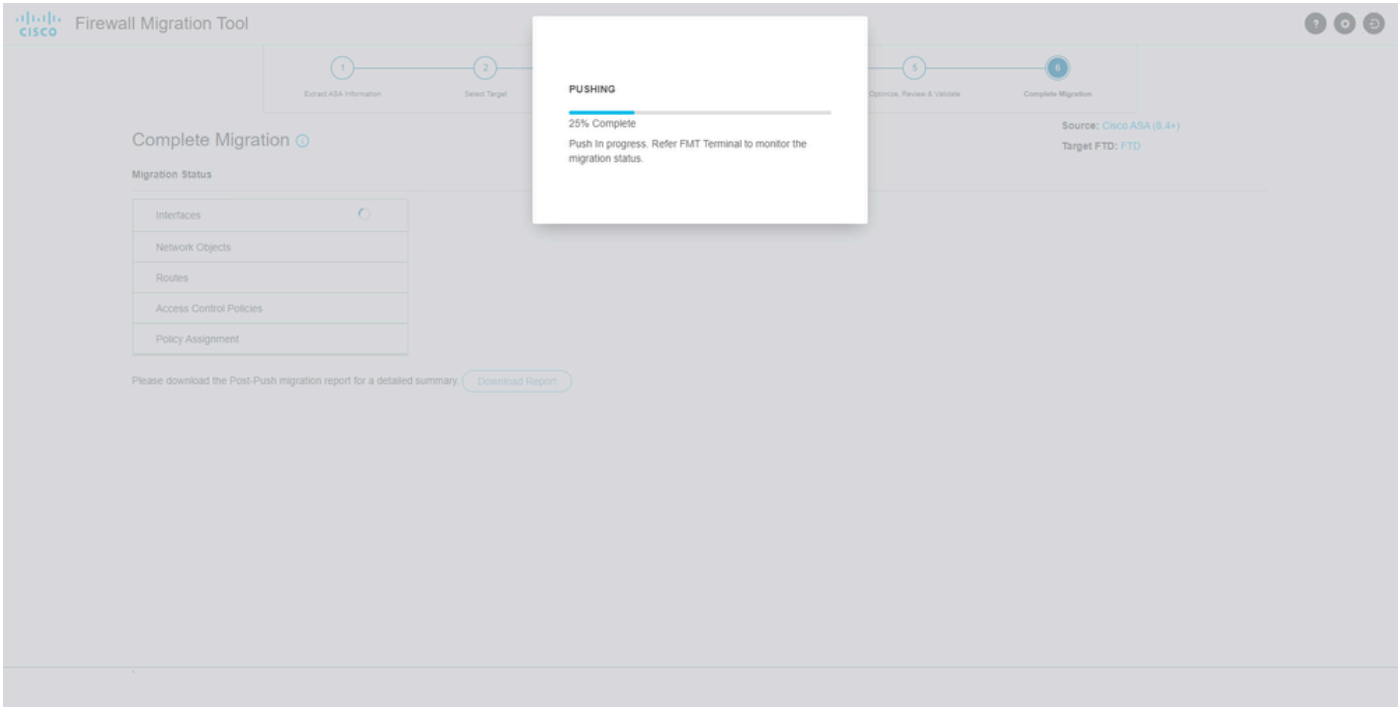
Prüfen und validieren

16. Wenn der Validierungsstatus erfolgreich ist, übertragen Sie die Konfigurationen auf die Zielgeräte.



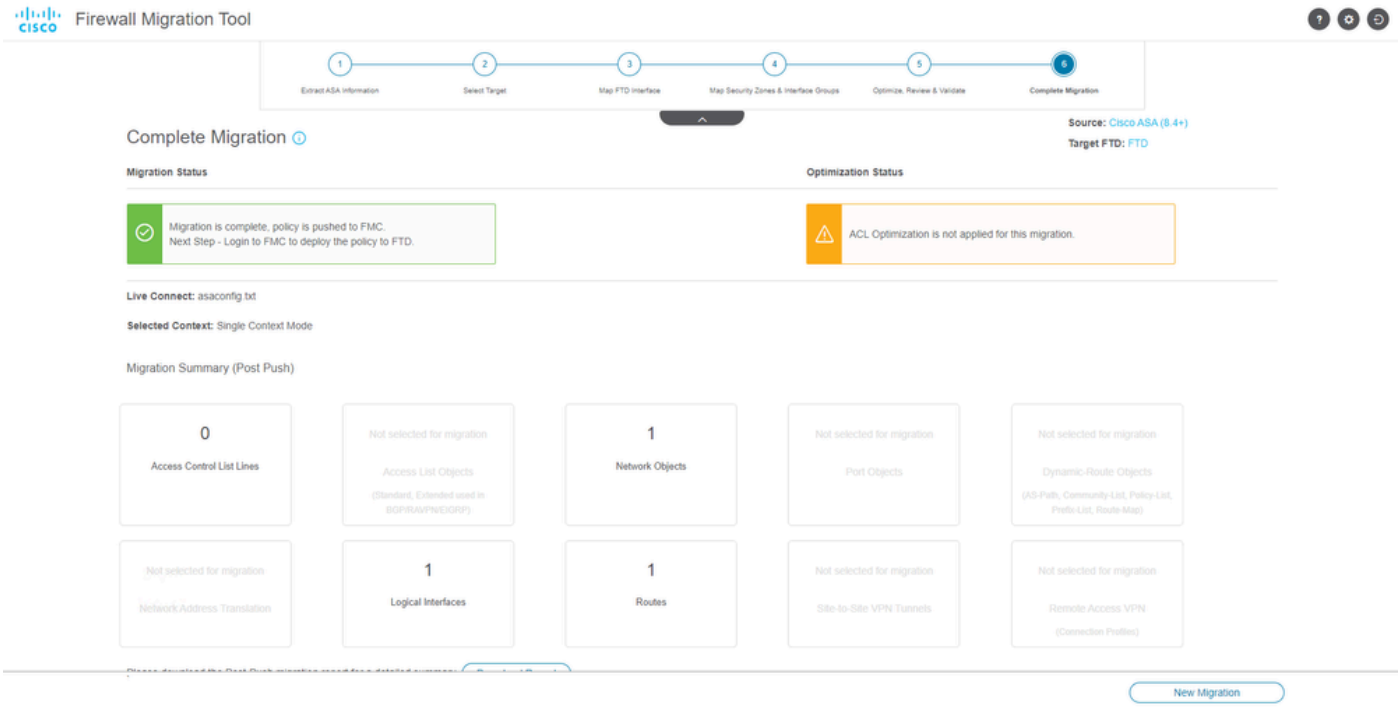
Validierung

Beispiel einer Konfiguration, die über das Migrations-Tool durchgeführt wird, wie in der Abbildung dargestellt:



Push

Beispiel einer erfolgreichen Migration, wie in der Abbildung dargestellt:



Erfolgreiche Migration

(Optional) Wenn Sie sich für die Migration der Konfiguration zu einem FTD entschieden haben, ist eine Bereitstellung erforderlich, um die verfügbare Konfiguration vom FMC auf die Firewall zu übertragen.

So stellen Sie die Konfiguration bereit:

1. Melden Sie sich an der FMC-GUI an.

2. Navigieren Sie zurDeployRegisterkarte.
3. Wählen Sie die Bereitstellung aus, um die Konfiguration per Push an die Firewall weiterzuleiten.
4. Klicken Sie auf . Deploy

Fehlerbehebung

Fehlerbehebung Secure Firewall Migration-Tool

- Häufige Migrationsfehler:
  - Unbekannte oder ungültige Zeichen in der ASA-Konfigurationsdatei.
  - Fehlende oder unvollständige Konfigurationselemente.
  - Probleme mit der Netzwerkverbindung oder Latenz.
  - Probleme beim Hochladen der ASA-Konfigurationsdatei oder beim Übertragen der Konfiguration an das Management Center.
  - Häufige Probleme sind:
- Verwendung 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.
  - Mit diesem Tool können Sie ein Support-Paket für Protokoll-, Datenbank- und Konfigurationsdateien herunterladen.
  - Herunterzuladende Schritte:
  - Weitere Unterstützung:

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.