

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

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Überblick](#)

[Hintergrundinformationen](#)

[Abrufen der ASA-Konfigurationsdatei](#)

[PKI-Zertifikat von ASA exportieren und in Management Center importieren](#)

[Abrufen von AnyConnect-Paketen und -Profilen](#)

[Konfigurieren](#)

[Konfigurationsschritte:](#)

[Fehlerbehebung](#)

[Fehlerbehebung Secure Firewall Migration-Tool](#)

---

## 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 Verwaltungszentrum (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-Profilen 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-ss0- 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 Verwaltungszentrum hochgeladen werden.

b-AnyConnect-Profilen 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 des neuesten Firepower Migration Tool von Cisco Software Central:

# Software Download

Downloads Home / Security / Firewalls / Secure Firewall Migration Tool / Firewall Migration Tool (FMT)- 7.0.0

Search...

Expand All Collapse All

Latest Release

7.0.1

All Release

7

7.0.1

7.0.0

## Secure Firewall Migration Tool

Release 7.0.0

[My Notifications](#)

Related Links and Documentation

[Open Source](#)

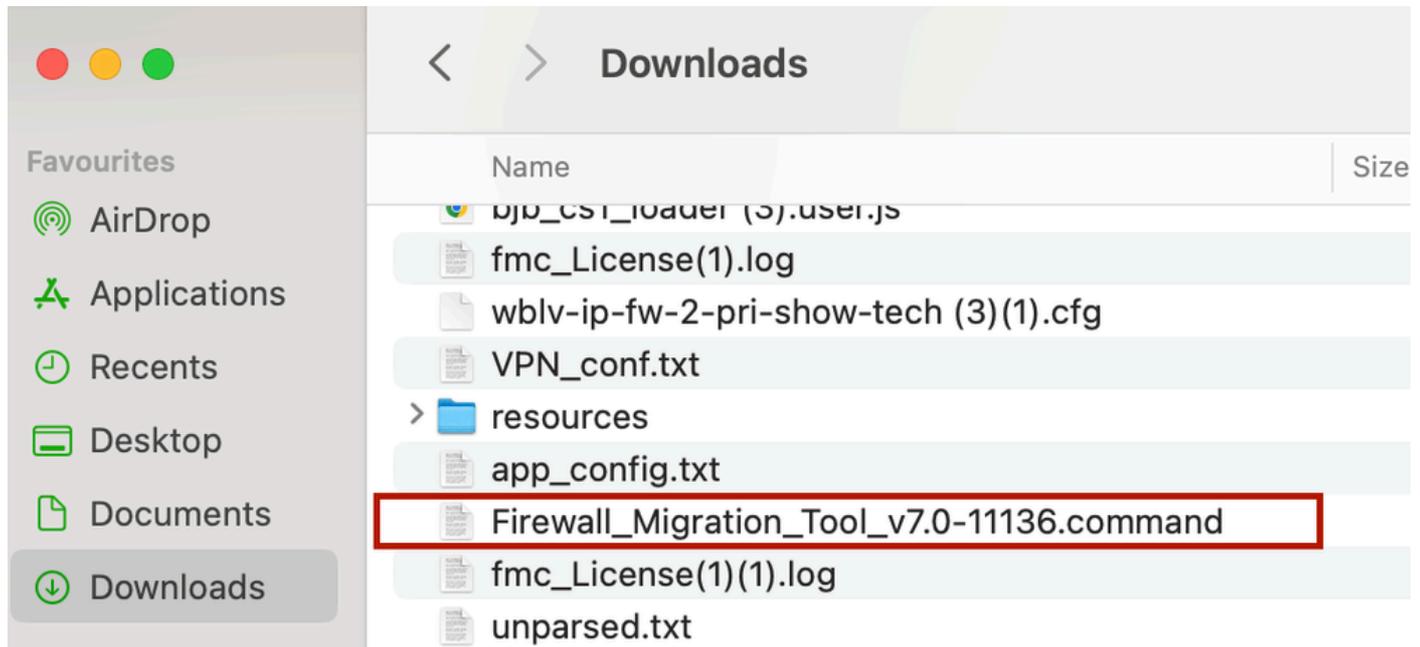
[Release Notes for 7.0.0](#)

[Install and Upgrade Guides](#)

File Information	Release Date	Size	
Firewall Migration Tool 7.0.0.1 for Mac Firewall_Migration_Tool_v7.0.0.1-11241.command <a href="#">Advisories</a>	04-Sep-2024	41.57 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
Firewall Migration Tool 7.0.0.1 for Windows Firewall_Migration_Tool_v7.0.0.1-11241.exe <a href="#">Advisories</a>	04-Sep-2024	39.64 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
Firewall Migration Tool 7.0.0 for Mac Firewall_Migration_Tool_v7.0-11136.command <a href="#">Advisories</a>	05-Aug-2024	41.55 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
Firewall Migration Tool 7.0.0 for Windows Firewall_Migration_Tool_v7.0-11136.exe <a href="#">Advisories</a>	05-Aug-2024	39.33 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>

Software-Download

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



Die Datei

```
ontext migration.'], 'FDM-managed Device to Threat Defense Migration': ['migrate
the Layer 7 security policies including SNMP and HTTP, and malware and file pol
icy configurations from your FDM-managed device to a threat defense device.'], '
Third Party Firewall to Threat Defense Migration': ['Check Point Firewall - migr
ate the site-to-site VPN (policy-based) configurations on your Check Point firew
all ( R80 or later) to a threat defense device (Version 6.7 or later)', 'Fortine
t Firewall - Optimize your application access control lists (ACLs) when migratin
g configurations from a Fortinet firewall to your threat defense device.']], 'se
curity_patch': False, 'updated_date': '25-1-2024', 'version': '6.0-9892'}}"
2025-01-16 16:51:36,906 [INFO      | views] > "The current tool is up to date"
127.0.0.1 - - [16/Jan/2025 16:51:36] "GET /api/software/check_tool_update HTTP/1
.1" 200 -
2025-01-16 16:51:40,615 [DEBUG    | common] > "session table records count:1"
2025-01-16 16:51:40,622 [INFO     | common] > "proxies : {}"
2025-01-16 16:51:41,838 [INFO     | common] > "Telemetry push : Able to connect t
o SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:41] "GET /api/eula_check HTTP/1.1" 200 -
2025-01-16 16:51:41,851 [INFO     | cco_login] > "EULA check for an user"
2025-01-16 16:51:46,860 [DEBUG    | common] > "session table records count:1"
2025-01-16 16:51:46,868 [INFO     | common] > "proxies : {}"
2025-01-16 16:51:48,230 [INFO     | common] > "Telemetry push : Able to connect t
o SSE Cloud server : https://sign-on.security.cisco.com"
127.0.0.1 - - [16/Jan/2025 16:51:48] "GET /api/eula_check HTTP/1.1" 200 -
```



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.

END USER LICENSE AGREEMENT

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail, including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof. This agreement, any supplemental license terms and any specific product terms at [www.cisco.com/go/software/terms](http://www.cisco.com/go/software/terms) (collectively, the "EULA") govern Your Use of the Software.

1. **Acceptance of Terms.** By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on behalf of an entity, you represent that you have authority to bind that entity. If you do not have such authority or you do not agree to the terms of the EULA, neither you nor the entity may Use the Software and it may be returned to the Approved Source for a refund within thirty (30) days of the date you acquired the Software or Cisco product. Your right to return and refund applies only if you are the original end user licensee of the Software.

2. **License.** Subject to payment of the applicable fees and compliance with this EULA, Cisco grants You a limited, non-exclusive and non-transferable license to Use object code versions of the Software and the Documentation solely for Your internal operations and in accordance with the Entitlement and the Documentation. Cisco licenses You the right to Use only the Software You acquire from an Approved Source. It makes no warranty, no applicable law. You are not licensed to Use the

I have read the content of the EULA and SEULA and agree to terms listed.

Proceed

Migrate policies from Cisco ASA or Cisco ASA with FPS or Check Point or PAN or Fortinet to Cisco FTD



Extract Source Information

Any additional information explaining this



EULA

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



## Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

[System status](#) [Policy statement](#)

FMT-Anmeldung

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





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".

## Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods &gt;

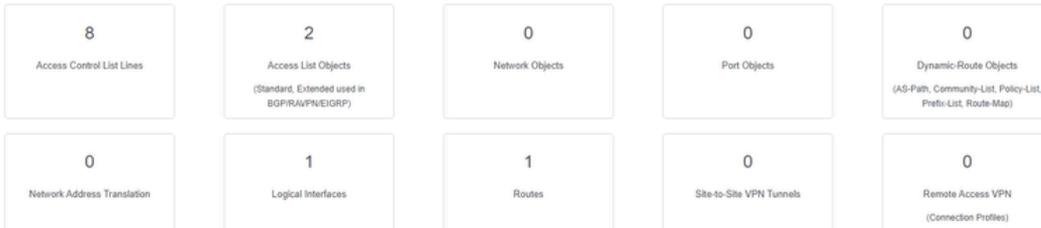
ASA IP Address: 192.168.1.20

Context Selection &gt;

Single Context Mode: Download config

Parsed Summary v

Collect Hitcounts: No



• Pre-migration report will be available after selecting the targets.

<https://cisco.com>

Back

Next

## 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.

## Select Target

Source: Cisco ASA (8.4+)

Firewall Management v

 On-Prem/Virtual FMC Cloud-delivered FMC

FMC IP Address/Hostname

192.168.1.18

Connect

1 FTD(s) Found

Proceed

Successfully connected to FMC

Choose FTD &gt;

Select Features &gt;

Rule Conversion/ Process Config &gt;

Back

Next

## 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

Firewall Migration Tool

Source: Cisco ASA (8.4+)

Select Target

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Select FTD Device  Proceed without FTD

FTD (192.168.1.17) - VMWare (Native)

Please ensure that the firewall mode configured on the target FTD device is the same as in the uploaded ASA configuration file. The existing configuration of the FTD device on the FMC is erased when you push the migrated configuration to the FMC.

Proceed

Select Features

Rule Conversion/ Process Config

Back Next

## Ziel-FTD

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

Firewall Migration Tool

Source: Cisco ASA (8.4+)

Select Target

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Device Configuration	Shared Configuration	Optimization
<input checked="" type="checkbox"/> Interfaces	<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Migrate Only Referenced Objects
<input checked="" type="checkbox"/> Routes	<input checked="" type="checkbox"/> Populate destination security zones	<input checked="" type="checkbox"/> Object Group Search
<input checked="" type="checkbox"/> Static	<input type="checkbox"/> NAT (no data)	<b>Inline Grouping</b>
<input type="checkbox"/> BGP	<input type="checkbox"/> Migrate tunnelled rules as Prefilter	<input checked="" type="checkbox"/> CSM/ASDM
<input type="checkbox"/> EIGRP	<input type="checkbox"/> Route-lockup logic is limited to Static Routes and Connected Routes. PBR, Dynamic-Routes & NAT are not considered.	
<input type="checkbox"/> Site-to-Site VPN Tunnels (no data)	<input type="checkbox"/> Remote Access VPN	
<input type="checkbox"/> Policy Based (Crypto Map)	<input type="checkbox"/> Remote Access VPN migration is supported on FMC/FTD 7.2 and above.	
<input type="checkbox"/> Route Based (VTI)		

Proceed

Back Next

## Konfigurationen

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



Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

Back Next

Konvertierung starten

12. Nach Abschluss der Konvertierung wird ein Dashboard mit der Zusammenfassung der zu migrierenden Objekte angezeigt (auf Kompatibilität beschränkt).

- Optional können Sie auf klicken **Download Report**, um eine Zusammenfassung der zu migrierenden Konfigurationen anzuzeigen.

Select Target

Source: Cisco ASA (8.4+)

Firewall Management

FMC IP Address/Hostname: 192.168.1.18

Choose FTD

Selected FTD: FTD

Select Features

Rule Conversion/ Process Config

Start Conversion

0 parsing errors found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration. [Download Report](#)

0 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/RAVP/VEIGRP)	1 Network Objects	0 Port Objects	0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
0 Network-Address Translation	1 Logical Interfaces	1 Routes	0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)

Back Next

Bericht herunterladen

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

**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	ASA; 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

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.

Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)  
Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	Select Security Zone	Select Interface Groups

10 per page 1 to 1 of 1 |< < Page 1 of 1 > >|

Back Next

Sicherheitszonen und Schnittstellengruppen

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



Map Security Zones and Interface Groups

Source: Cisco ASA (8.4+)  
Target FTD: FTD

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
management	GigabitEthernet0/0	management	management_lg (A)

10 per page 1 to 1 of 1 |< < Page 1 of 1 > >|

Back Next

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.



Optimize, Review and Validate Configuration

Source: Cisco ASA (8.4+)  
Target FTD: FTD

Access Control | **Objects** | NAT | Interfaces | Routes | Site-to-Site VPN Tunnels | Remote Access VPN

Access List Objects | **Network Objects** | Port Objects | VPN Objects | Dynamic-Route Objects

Select all 1 entries Selected: 0 / 1

#	Name	Validation State	Type	Value
1	obj-192.168.1.1	Will be created in FMC	Network Object	192.168.1.1

50 per page 1 to 1 of 1 Page 1 of 1

Note: Populate the areas highlighted in Yellow in EIGRP, Site to Site and Remote Access VPN sections to validate and proceed with migration

Validate

Prüfen und validieren

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

**Validation Status**

Successfully Validated

Validation Summary (Pre-push)

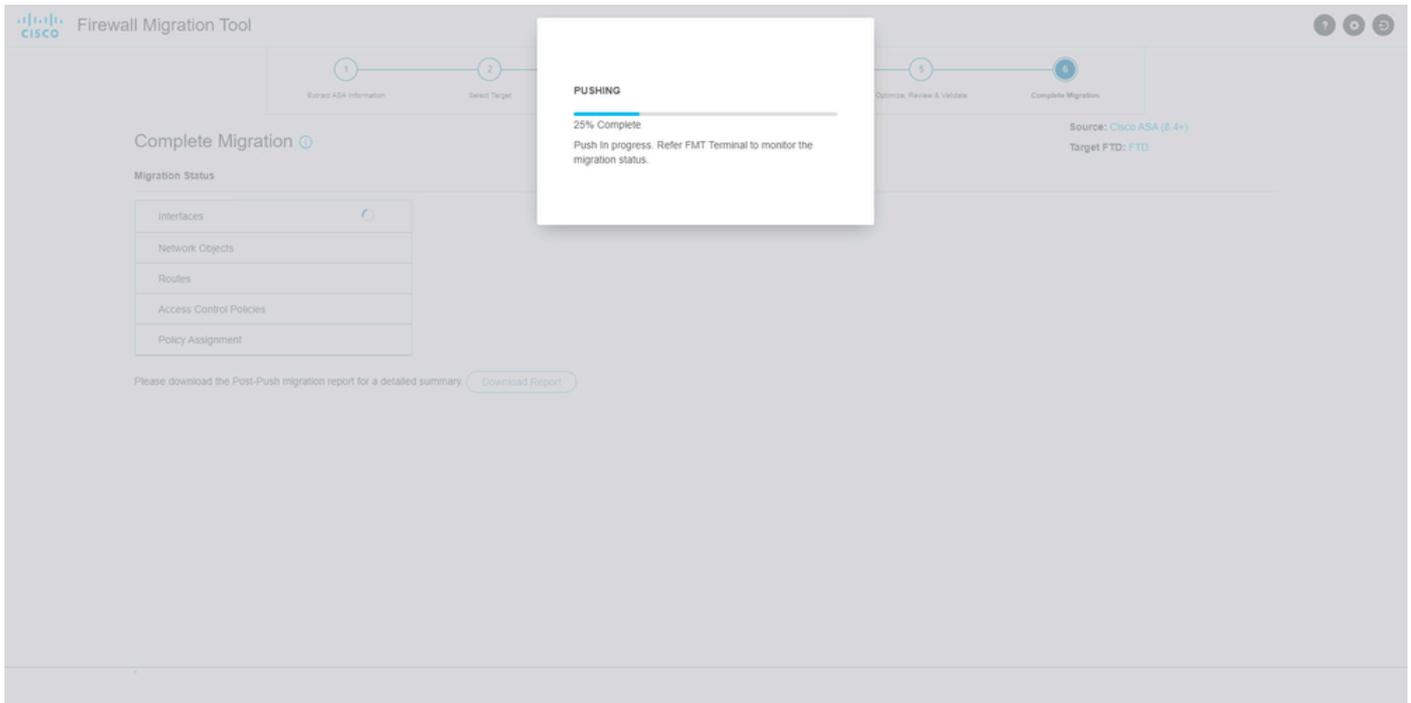
0	Not selected for migration	1	Not selected for migration	Not selected for migration
Access Control List Lines	Access List Objects (Standard, Extended used in BGP/HA/VPN/EIGRP)	Network Objects	Port Objects	Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
Not selected for migration	1	1	Not selected for migration	Not selected for migration
Network Address Transl...	Logical Interfaces	Routes	Site-to-Site VPN Tunnels	Remote Access VPN (Connection Profiles)

Note: The configuration on the target FTD device FTD (192.168.1.17) will be overwritten as part of this migration.

Push Configuration

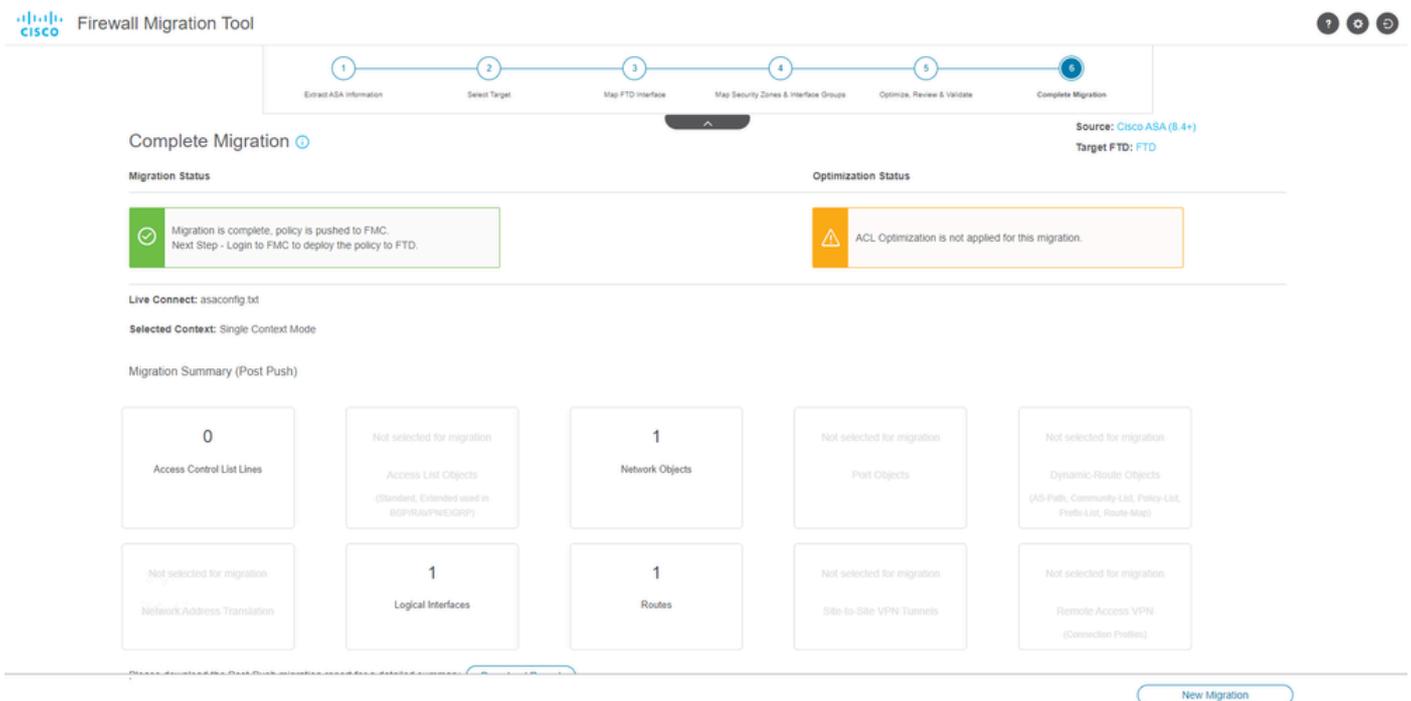
Validierung

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 zur `Deploy` Registerkarte.
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.