

FTD-Migration von einem FMC zu einem anderen FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Migration eines Cisco Firepower Threat Defense (FTD)-Geräts zwischen Firepower Management Centern beschrieben.

Voraussetzungen

Bevor Sie mit der Migration beginnen, stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Zugriff auf Quell- und Ziel-FMCs
- Administratorberechtigungen für FMC und FTD.
- Sicherung der aktuellen FMC-Konfiguration
- Stellen Sie sicher, dass auf den FTD-Geräten eine kompatible Softwareversion mit dem Ziel-FMC ausgeführt wird.
- Vergewissern Sie sich, dass das Ziel-FMC die gleiche Version wie das Quell-FMC hat.

Anforderungen

- Auf beiden FMCs müssen kompatible Softwareversionen ausgeführt werden.
- Netzwerkverbindung zwischen dem FTD-Gerät und beiden FMCs.
- Angemessener Speicher und Ressourcen auf dem Ziel-FMC für die Aufnahme des FTD-Geräts

Verwendete Komponenten

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

Cisco Firepower Threat Defense Virtual (FTDv) Version 7.2.5

FirePOWER Management Center Virtual (FMCv) Version 7.2.5

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.

Hintergrundinformationen

Die Migration eines FTD-Geräts von einem FMC zu einem anderen umfasst mehrere Schritte, darunter die Aufhebung der Registrierung des Geräts beim Quell-FMC, die Vorbereitung des Ziel-FMC und die erneute Registrierung des Geräts. Dieser Prozess stellt sicher, dass alle Richtlinien und Konfigurationen korrekt übertragen und angewendet werden.

Konfigurieren

Konfigurationen

1. Melden Sie sich beim Quell-FMC an.



Secure Firewall Management Center

Username

Password

Log In

2. Navigieren Sie zu Geräte > Geräteverwaltung, und wählen Sie das Gerät aus, das migriert werden soll.



View By:

All (1) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (1) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (1)

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	▼ Ungrouped (1)			
<input type="checkbox"/>	● 192.168.15.31 Snort 3 192.168.15.31 - Routed	FTDv for VMware	7.2.5	N/A

3. Navigieren Sie im Geräteabschnitt zum Gerät, und klicken Sie auf Exportieren, um Ihre Geräteeinstellungen zu exportieren.

FTD1

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

General



Name: FTD1
Transfer Packets: Yes
Mode: Routed
Compliance Mode: None
TLS Crypto Acceleration: Disabled

Device Configuration:

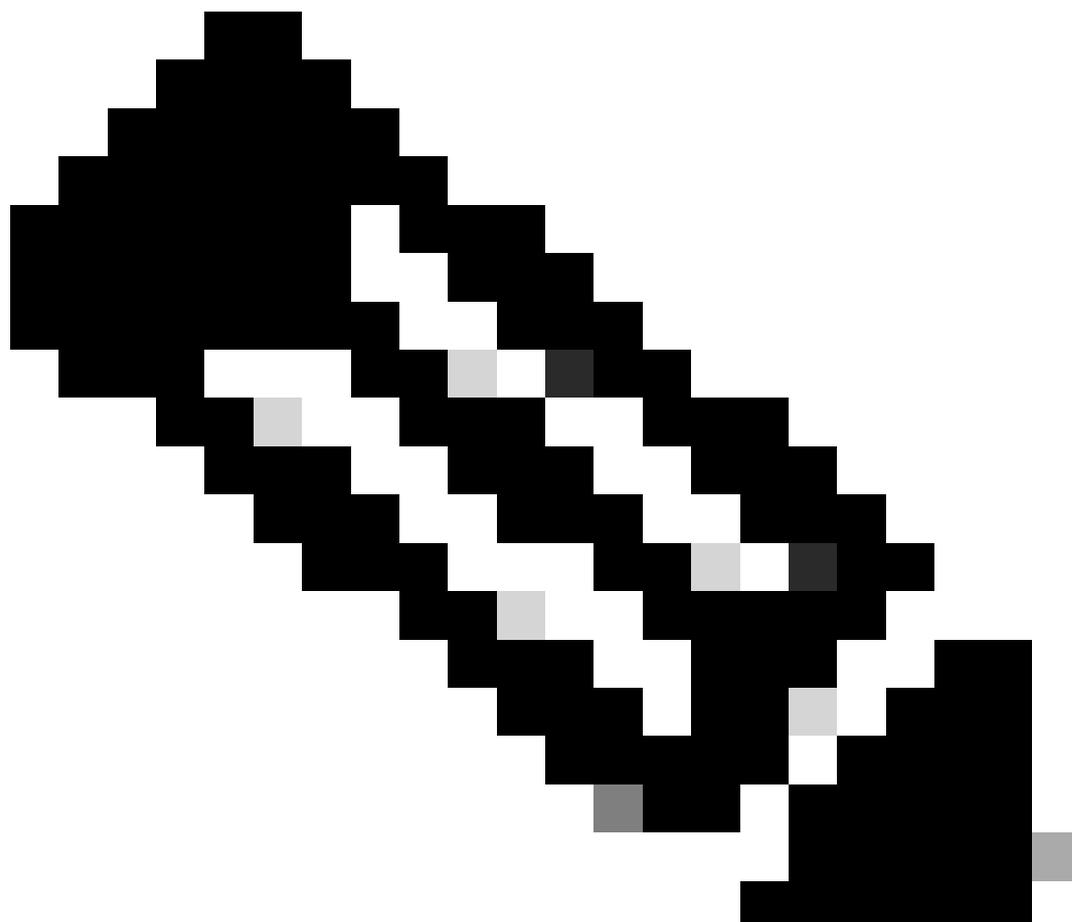
4. Nachdem die Konfiguration exportiert wurde, müssen Sie sie herunterladen.

Device Configuration Download

Backup taken on **14-Oct-2024 07:05 PM** is available.

[Click here to download the package](#)

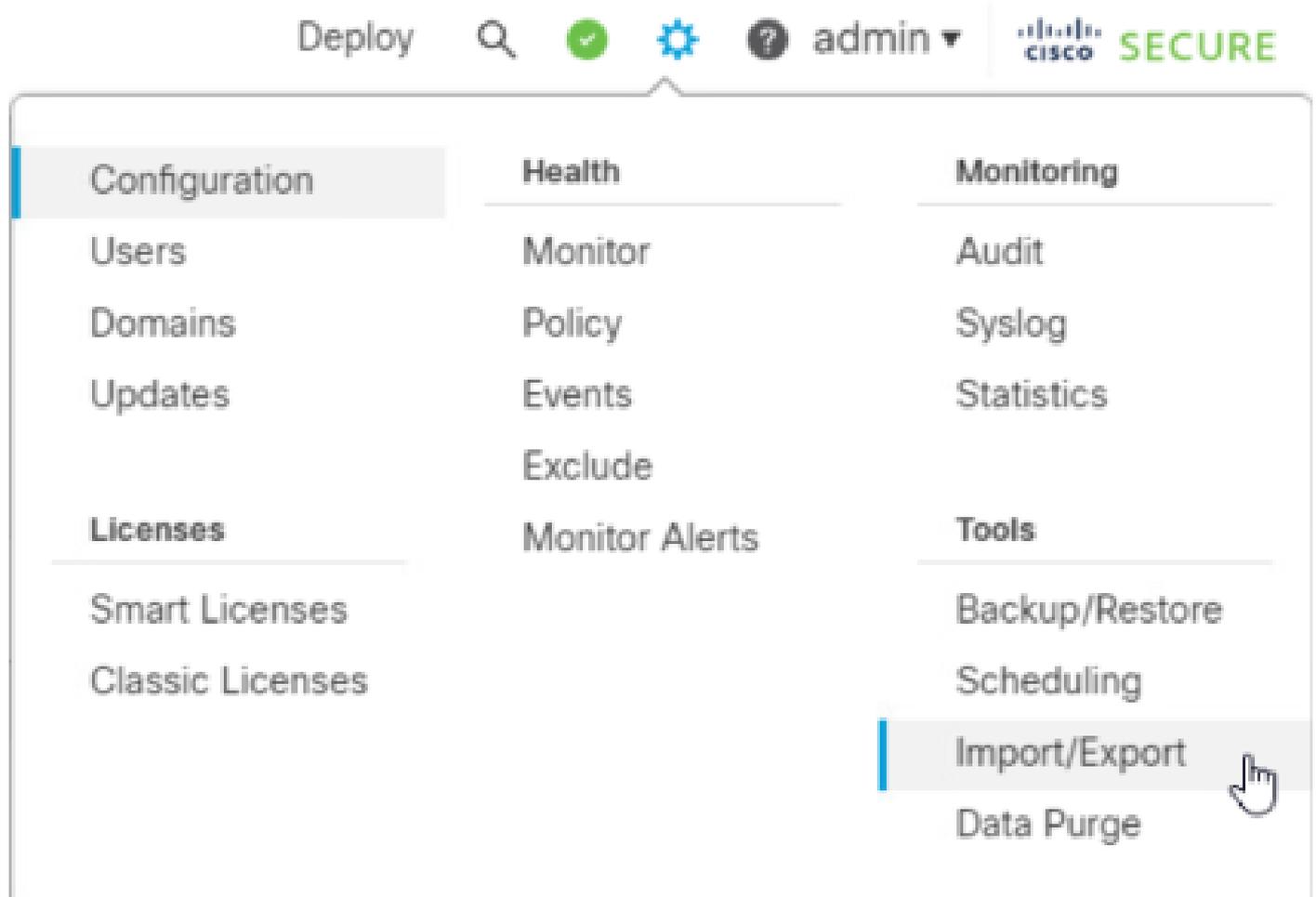
OK



Hinweis: Die heruntergeladene Datei muss die Erweiterung `.SFO` enthalten und enthält

Informationen zur Gerätekonfiguration wie IP-Adressen, Sicherheitszonen, statische Routen und andere Geräteeinstellungen.

5. Sie müssen die mit dem Gerät verknüpften Richtlinien exportieren, zu System > Tools > Import/Export navigieren, die Richtlinien auswählen, die Sie exportieren möchten, und auf Export klicken.



∨ Access Control Policy



test

Access Control Policy

> Contextual Cross-launch

> Custom Table View

> Custom Workflow

> Dashboard

> Health Policy

∨ NAT Threat Defense



NAT

NAT Threat Defense

∨ Platform Settings Threat Defense



test

Platform Settings Threat Defense

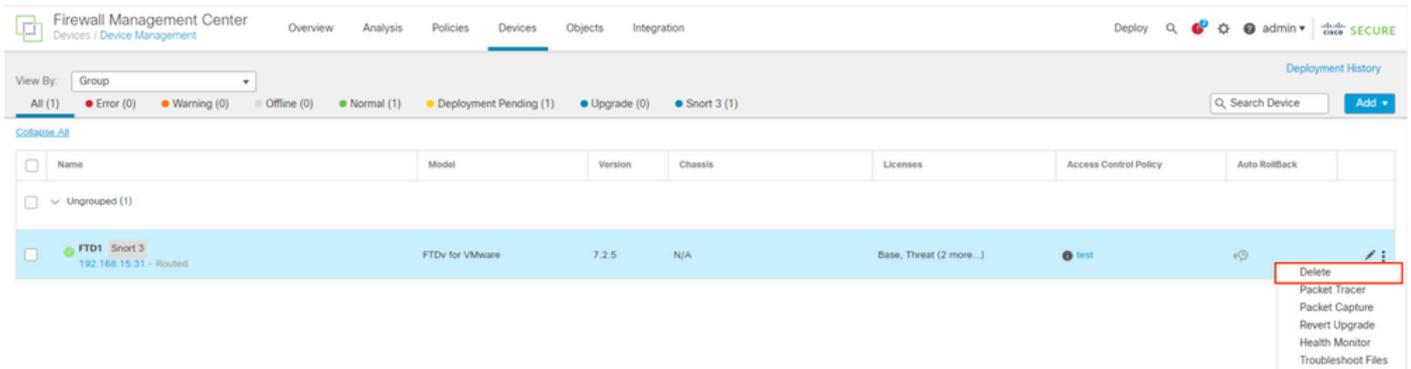
> Report Template

Export



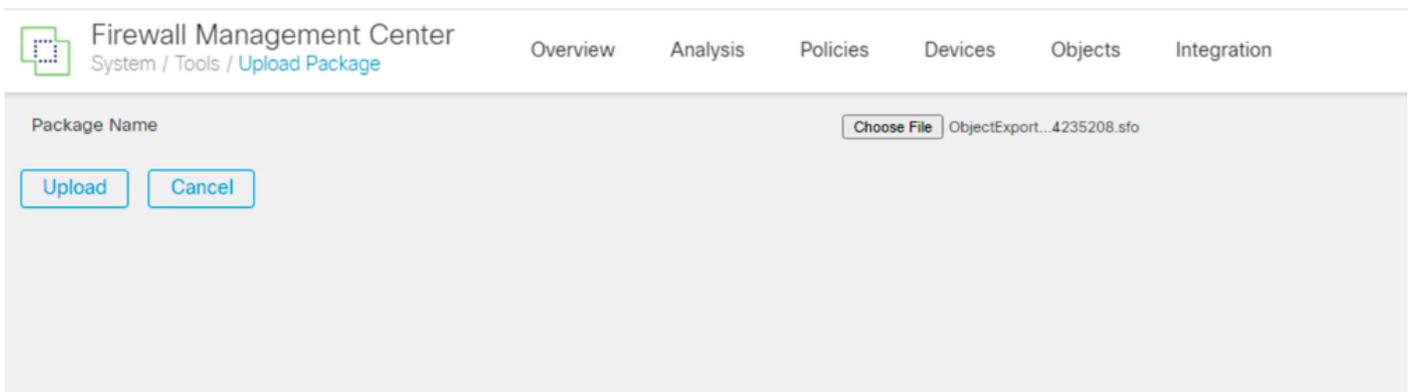
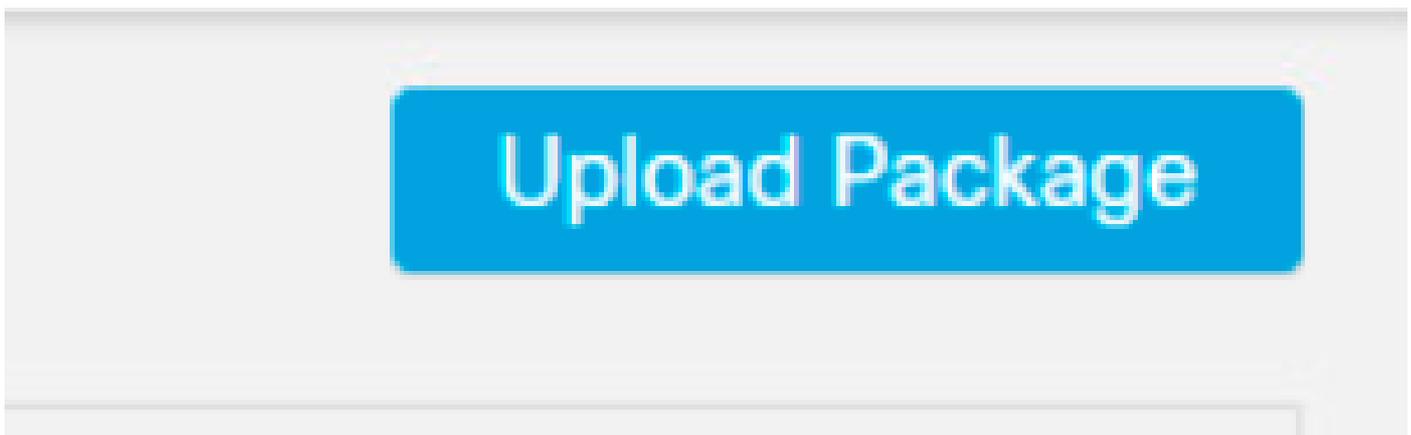
Hinweis: Stellen Sie sicher, dass die SFO-Datei erfolgreich heruntergeladen wurde. Der Download erfolgt automatisch nach dem Klicken auf Export. Diese Datei enthält die Zugriffskontrollrichtlinien, Plattformeinstellungen, NAT-Richtlinien und andere Richtlinien, die für die Migration unerlässlich sind, da sie nicht zusammen mit der Gerätekonfiguration exportiert werden und manuell auf das Ziel-FMC hochgeladen werden müssen.

6. Heben Sie die Registrierung des FTD-Geräts vom FMC auf, navigieren Sie zu Devices > Device Management, klicken Sie auf die drei vertikalen Punkte auf der rechten Seite, und wählen Sie Delete (Löschen) aus.



7. Vorbereiten des Ziel-FMC:

- Melden Sie sich beim Ziel-FMC an.
- Vergewissern Sie sich, dass das FMC das neue Gerät akzeptieren kann, indem Sie die in Schritt 5 heruntergeladenen FMC-Quellrichtlinien importieren. Navigieren Sie zu System > Tools > Import/Export, und klicken Sie auf Paket hochladen. Laden Sie die zu importierende Datei hoch, und klicken Sie auf Hochladen.



8. Wählen Sie die zu importierenden Richtlinien im Ziel-FMC aus.

test

Initial_Health_Policy 2024-09-29 18:25:54
 Initial Health Policy

NAT

test

9. Wählen Sie im Importmanifest eine Sicherheitszone aus, oder erstellen Sie eine neue Zone, die dem Schnittstellenobjekt zugewiesen werden soll, und klicken Sie auf Importieren.

Import Manifest
Network and Port objects will be reused if name and content matches with existing objects, in all other cases objects with duplicate names are imported as new objects with a number appended to the name.

test (Access Control Policy)
Initial_Health_Policy 2024-09-29 18:25:54 (Health Policy)
NAT (NAT Threat Defense)
test (Platform Settings Threat Defense)

dmz1 (Routed)

Access Control Policy: **test**
 Access Control Policy Rule: allowhttps (Source Zone) Access Control Policy Rule: allowssh (Source Zone)

NAT Policy: **NAT**
 NAT Policy Rule ID: # (Source Zone)

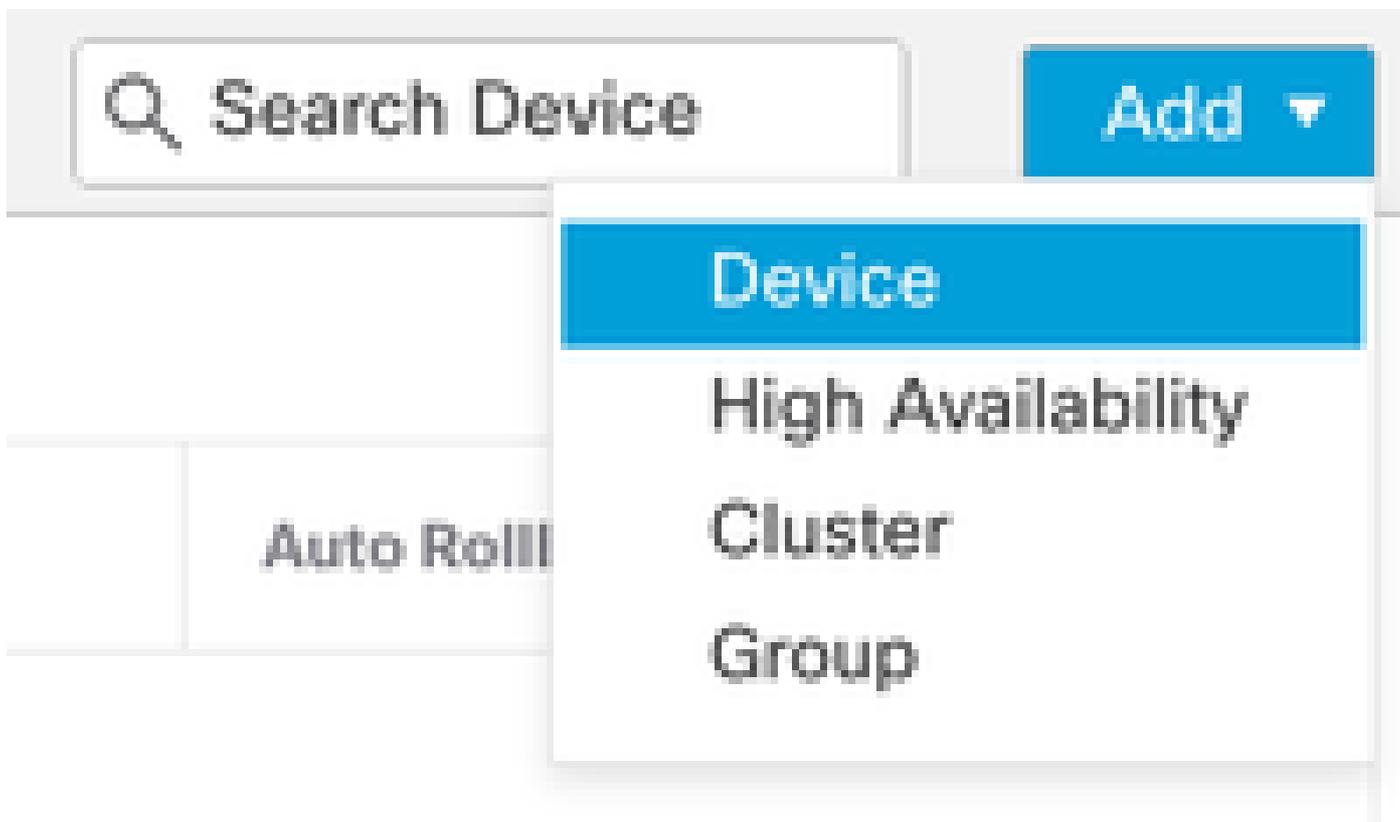
Security Zones:

labs (Routed)

Security Zones:

10. Registrieren Sie die FTD beim Ziel-FMC:

- Navigieren Sie auf dem Ziel-FMC zur Registerkarte Device > Management (Gerät > Verwaltung), und wählen Sie Add > Device (Hinzufügen > Gerät).
- Beenden Sie den Registrierungsprozess, indem Sie auf die Aufforderungen reagieren.



Add Device



CDO Managed Device

Host:†

Display Name:

Registration Key:*

Group:

Access Control Policy:*

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

- Malware
- Threat
- URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

† Either host or NAT ID is required.

Cancel

Register

Weitere Informationen finden Sie im Konfigurationsleitfaden für das Firepower Management Center unter [Hinzufügen von Geräten zum Firepower Management Center](#).

11. Navigieren Sie zu Gerät > Geräteverwaltung > wählen Sie FTD > Gerät aus, und klicken Sie auf Importieren. Eine Warnung wird angezeigt, die Sie zur Bestätigung auffordert, dass die Gerätekonfiguration ersetzt werden soll. Klicken Sie auf "Ja".

FTD1

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

General		  
Name:		FTD1
Transfer Packets:		Yes
Mode:		Routed
Compliance Mode:		None
TLS Crypto Acceleration:		Disabled
Device Configuration:	<input type="button" value="Import"/>	<input type="button" value="Export"/> <input type="button" value="Download"/>

Device Configuration Import

This will replace current device configuration with new configuration from imported file. Do you want to continue?

No

Yes

12. Wählen Sie die Importkonfigurationsdatei aus, die die Erweiterung .SFO sein muss, klicken Sie auf Upload, und es wird eine Meldung angezeigt, die angibt, dass der Import gestartet wurde.

The screenshot shows a Windows File Explorer window with the address bar set to 'Downloads'. The search bar contains 'Search Downloads'. The file list is as follows:

Name	Date modified	Type	Size
Yesterday (4)			
ObjectExport_20241014235208.sfo	10/14/2024 7:51 PM	SFO File	177 KB
exportconfig.sfo	10/14/2024 7:46 PM	SFO File	23 KB
DeviceExport-9fd9088e-7d04-11ef-a474-...	10/14/2024 7:18 PM	SFO File	23 KB
DeviceExport-bea34c00-8a80-11ef-88c6-...	10/14/2024 7:08 PM	SFO File	24 KB

Below the file list, a file selection dialog box is open. The text field contains 'exportconfig.sfo' and the file type dropdown is set to 'All Files'. The 'Open' button is highlighted in blue.

Device Configuration Import

Device configuration import task initiated. View the progress of task from Tasks view.

OK

Only:

13. Schließlich wird eine Warnmeldung angezeigt, und nach Abschluss des Imports wird automatisch ein Bericht erstellt, sodass Sie die importierten Objekte und Richtlinien überprüfen können.

The screenshot shows the Cisco Secure interface. At the top, there is a navigation bar with 'Deploy', a search icon, a notification icon with '2', a settings gear, a help icon, and the user 'admin'. The Cisco logo and 'SECURE' are on the right. Below the navigation bar, there are tabs for 'Deployments', 'Upgrades', 'Health', and 'Tasks'. The 'Tasks' tab is selected. To the right of the tabs is a 'Show Notifications' toggle switch. Below the tabs, there is a summary bar with '20+ total' (highlighted in blue), '0 waiting', '0 running', '0 retrying', '20+ success', and '1 failure'. A search box labeled 'Filter' is on the right. The main content area shows a notification for 'Device Configuration Import' with a green checkmark icon. The text reads 'Device configurations imported successfully' and includes a link 'View Import Report'. The notification is timestamped '6s' and has a close button 'X'.

Configuration Import Summary

Initiated by:
Initiated at: Tue Oct 15 00:40:18 2024

Policies

Policies imported: 3

Type	Name
PG.PLATFORM.AutomaticApplicationBypassPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.AutomaticApplicationBypassPage
PG.PLATFORM.PixInterface	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.PixInterface
PG.PLATFORM.NgfwInlineSetPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.NgfwInlineSetPage

Überprüfung

Überprüfen Sie nach Abschluss der Migration, ob das FTD-Gerät korrekt registriert wurde und mit dem Ziel-FMC funktioniert:

- Überprüfen Sie den Gerätestatus auf dem Ziel-FMC.
- Stellen Sie sicher, dass alle Richtlinien und Konfigurationen korrekt angewendet werden.
- Führen Sie einen Test durch, um sicherzustellen, dass das Gerät betriebsbereit ist.

Fehlerbehebung

Wenn während des Migrationsprozesses Probleme auftreten, sollten Sie folgende Schritte zur Fehlerbehebung in Betracht ziehen:

- Überprüfen der Netzwerkverbindung zwischen dem FTD-Gerät und beiden FMCs
- Vergewissern Sie sich, dass die Softwareversion auf beiden FMCs identisch ist.
- Überprüfen Sie die Warnungen auf beiden FMCs auf Fehlermeldungen oder Warnungen.

Zugehörige Informationen

- [Administratorleitfaden für Cisco Secure Firewall Management Center](#)
- [Konfiguration, Überprüfung und Fehlerbehebung bei der Registrierung von FirePOWER-Geräten](#)

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.