

# FTD HA-Upgrade von FDM verwaltet

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Überblick](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Schritt 1: Upgrade-Paket hochladen](#)

[Schritt 2: Überprüfen der Bereitschaft](#)

[Schritt 3: FTD in HA aktualisieren](#)

[Schritt 4: Aktiven Peer wechseln \(optional\)](#)

[Schritt 5: Finale Bereitstellung](#)

[Validieren](#)

---

## Einleitung

In diesem Dokument wird der Upgrade-Prozess für Cisco Secure Firewall Threat Defense in High Availability beschrieben, der von einem FirePOWER-Gerätemanager verwaltet wird.

## Voraussetzungen

### Anforderungen

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

- Hochverfügbarkeitskonzepte und -konfigurationen
- Cisco Secure FirePOWER Device Manager (FDM)-Konfiguration
- Konfiguration von Cisco Secure Firewall Threat Defense (FTD)

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Virtual Cisco FTD, Version 7.2.8.

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

Der FDM arbeitet, indem jeweils ein Peer aktualisiert wird. Zuerst der Standby-Modus und dann der Active-Modus, sodass ein Failover durchgeführt wird, bevor das Active-Upgrade gestartet wird.

## Hintergrundinformationen

Das Upgrade-Paket muss vor dem Upgrade von [software.cisco.com](https://software.cisco.com) heruntergeladen werden.

Führen Sie bei CLI-Aufruf den Befehl `show high-availability configim Active FTD` aus, um den HA-Status zu überprüfen.

```
> show high-availability config
```

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
```

```
Interface Poll frequency 5 seconds, holdtime 25 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 3 of 311 maximum
```

```
MAC Address Move Notification Interval not set
```

```
failover replication http
```

```
Version: Ours 9.18(3)53, Mate 9.18(3)53
```

```
Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C
```

```
Last Failover at: 11:57:26 UTC Oct 8 2024
```

```
    This host: Primary - Active
```

```
        Active time: 507441 (sec)
```

```
        slot 0: ASAv hw/sw rev (/9.18(3)53) status (Up Sys)
```

```
            Interface diagnostic (0.0.0.0): Normal (Waiting)
```

```
            Interface inside (192.168.45.1): Normal (Waiting)
```

```
            Interface outside (192.168.1.10): Normal (Waiting)
```

```
        slot 1: snort rev (1.0) status (up)
```

```
        slot 2: diskstatus rev (1.0) status (up)
```

```
    Other host: Secondary - Standby Ready
```

Active time: 8 (sec)

Interface diagnostic (0.0.0.0): Normal (Waiting)

Interface inside (0.0.0.0): Normal (Waiting)

Interface outside (0.0.0.0): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

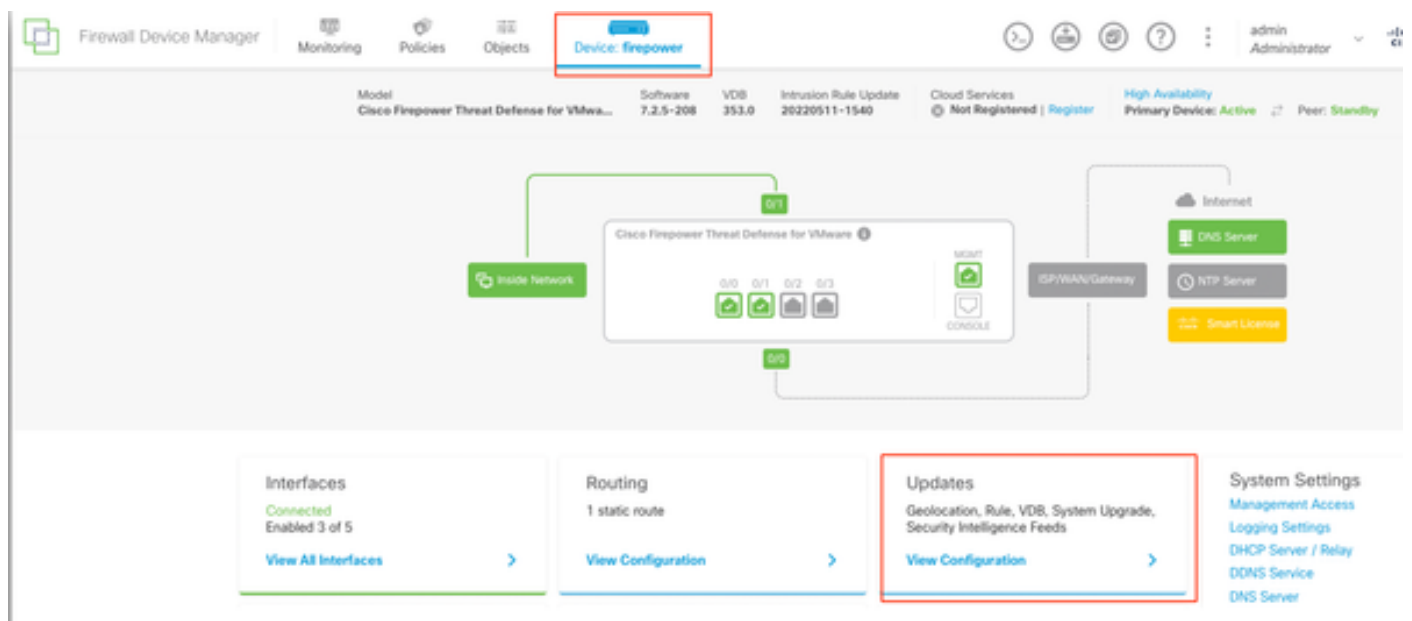
Wenn keine Fehler sichtbar sind, fahren Sie mit dem Upgrade fort.

## Konfigurieren

### Schritt 1: Upgrade-Paket hochladen

- Laden Sie das FTD-Upgrade-Paket über die grafische Benutzeroberfläche (GUI) auf den FDM hoch.

Diese muss zuvor basierend auf dem FTD-Modell und der gewünschten Version von der Cisco Software-Website heruntergeladen werden. Navigieren Sie zu Gerät > Updates > System Upgrade.



Updates

- Suchen Sie nach dem zuvor heruntergeladenen Image, und wählen Sie Hochladen aus.



Anmerkung: Laden Sie das Image auf aktive und Standby-Knoten hoch.

---

## System Upgrade

Current version 7.2.5-208

### **i** Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

*There are no software upgrades available on the system.*

*Upload an upgrade file to install.*

BROWSE

Bereitschaftsprüfung durchführen

## Schritt 2: Überprüfen der Bereitschaft

Die Bereitschaftsprüfungen bestätigen, ob die Appliances für die Aktualisierung bereit sind.


- Wählen Sie Upgrade Readiness Check ausführen aus.

## System Upgrade

Current version 7.2.5-208

### **i** Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco\_FTD\_Upgrade-7.2.8-25.sh.REL....**  [Replace file](#)  
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **Not Performed Yet** | [Run Upgrade Readiness Check](#)

UPGRADE NOW

**i** Reboot required

Bereitschaftsprüfung durchführen


### System Upgrade

Current version 7.2.5-208

---

**i Important**

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

|            |  |
|------------|--|
| File       | Cisco_FTD_Upgrade-7.2.8-25.sh.REL....    <a href="#">Replace file</a> |
|            | 14 Oct 2024 05:06 PM   |
| Upgrade to | 7.2.8-25   |

---


|                 |                   |   |
|-----------------|-------------------|---|
| Readiness Check | Not Performed Yet | <a href="#">Run Upgrade Readiness Check</a> |
|-----------------|-------------------|---|

**UPGRADE NOW** **i Reboot required**


Bereitschaftsprüfung durchführen

**i Important**

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

|            |  |
|------------|--|
| File       | Cisco_FTD_Upgrade-7.2.8-25.sh.REL....    <a href="#">Replace file</a> |
|            | 14 Oct 2024 05:06 PM   |
| Upgrade to | 7.2.8-25   |

---

|                 |   |
|-----------------|---|
| Readiness Check |  <b>Please Wait...</b> |
|-----------------|---|

**UPGRADE NOW** **i Reboot required**

Bereitschaftsprüfung durchführen


Der Fortschritt kann überprüft werden, indem Sie zu System > Upgrade navigieren.

## System Upgrade

Current version 7.2.5-208

### **i** Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco\_FTD\_Upgrade-7.2.8-25.sh.REL....**  | [Replace file](#)  
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **✓ Precheck Success** | [Run Upgrade Readiness Check](#)  
14 Oct 2024 05:51 PM

**UPGRADE NOW**

**i** Reboot required

Bereitschaftsprüfung durchführen

Das Upgrade kann durchgeführt werden, wenn die Bereitschaftsprüfung in FTD und das Ergebnis "Success" abgeschlossen ist.

### Schritt 3: FTD in HA aktualisieren

- Wählen Sie Standby FDM aus, und klicken Sie auf Jetzt aktualisieren.

## System Upgrade

Current version 7.2.5-208

### **i** Important

This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see [link](#)

File **Cisco\_FTD\_Upgrade-7.2.8-25.sh.REL....**  | [Replace file](#)  
14 Oct 2024 05:06 PM

Upgrade to **7.2.8-25**

Readiness Check **✔ Precheck Success** | [Run Upgrade Readiness Check](#)  
14 Oct 2024 05:51 PM

**UPGRADE NOW**

**i** Reboot required

Jetzt aktualisieren

Vor dem Upgrade:

1. Starten Sie eine Systemwiederherstellung nicht gleichzeitig mit einem System-Upgrade.
2. Starten Sie das System während der Aktualisierung nicht neu. Das System startet automatisch zum geeigneten Zeitpunkt während des Upgrades neu, wenn ein Neustart erforderlich ist.
3. Schalten Sie das Gerät während des Upgrades nicht aus. Wenn Sie das Upgrade unterbrechen, kann das System unbrauchbar werden.

Sie werden vom System abgemeldet, wenn die Aktualisierung beginnt.

Nach Abschluss der Installation wird das Gerät neu gestartet.



## Confirm System Upgrade



Before starting the upgrade:

1. Do not start a system restore at the same time as a system upgrade.
2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary.
3. **Do not power off the device** during the upgrade. Interrupting the upgrade can leave the system in an unusable state.

You will be logged out of the system when the upgrade begins.  
After the installation completes, the device will be rebooted.

### UPGRADE OPTIONS

- Automatically cancel on upgrade failure and roll back to the previous version

CANCEL

CONTINUE

Fortfahren



Anmerkung: Die Aktualisierung dauert ca. 20 Minuten pro FTD.

---

Auf CLI kann der Fortschritt im Upgrade-Ordner `/ngfw/var/log/sf` überprüft werden. in den Expertenmodus und den Enterroot-Zugriff wechseln.

```
> expert
```

```
admin@firepower:~$ sudo su
```

```
Password:
```

```
root@firepower:/home/admin# cd /ngfw/var/log/sf
```

```
root@firepower:/ngfw/var/log/sf# ls
```

```
Cisco_FTD_Upgrade-7.2.8.
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# ls -lrt
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# tail -f status.log
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/011_check_self.
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/015_verify_rpm.
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_check_dashb
```

```
ui: Upgrade in progress: ( 8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_get_snort_f
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/110_setup_upgra
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au
```

```
ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/152_save_etc_sf
```

```
ui: Upgrade in progress: (79% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zz_inst
```

```
ui: Upgrade in progress: (83% done. 4 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com
```

```
ui: Upgrade complete
```

```
ui: The system will now reboot.
```

```
ui: System will now reboot.
```

```
Broadcast message from root@firepower (Mon Oct 14 12:01:26 2024):
```

```
System will reboot in 5 seconds due to system upgrade.
```

```
Broadcast message from root@firepower (Mon Oct 14 12:01:31 2024):
```

```
System will reboot now due to system upgrade.
```

```
Broadcast message from root@firepower (Mon Oct 14 12:01:39 2024):
```

```
The system is going down for reboot NOW!
```

Aktualisieren Sie die zweite Einheit.

Wechseln Sie die Rollen, um dieses Gerät zu aktivieren: Wählen Sie Device > High Availability und dann Switch Mode aus dem Getriebemenü. Warten Sie, bis der Status des Geräts in "Aktiv" geändert wurde, und stellen Sie sicher, dass der Datenverkehr normal fließt. Dann melden Sie sich ab.

Upgrade: Wiederholen Sie die vorherigen Schritte, um sich beim neuen Standby-Gerät anzumelden, das Paket hochzuladen, das Gerät zu aktualisieren, den Fortschritt zu überwachen und den Erfolg zu überprüfen.

High Availability

Secondary Device: **Active**  Peer: **Standby**

Hohe Verfügbarkeit

High Availability

Primary Device: **Standby**  Peer: **Active**

Hohe Verfügbarkeit

Wechseln Sie auf der CLI zu LINA (system support diagnostic-CLI), und überprüfen Sie den Failover-Status auf der Standby-FTD mit dem Befehl show failover state.

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.
```

```
primary_ha> enable
```

```
Password:
```

```
primary_ha# show failover state
```

|              | State         | Last Failure Reason | Date/Time |
|--------------|---------------|---------------------|-----------|
| This host -  | Primary       |                     |           |
|              | Standby Ready | None                |           |
| Other host - | Secondary     |                     |           |
|              | Active        | None                |           |

====Configuration State====

Sync Skipped - STANDBY

====Communication State====

Mac set

primary\_ha#

Schritt 4: Aktiven Peer wechseln (optional)



Anmerkung: Wenn das sekundäre Gerät aktiv ist, hat es keine Auswirkungen auf den Betrieb.

---

Das primäre Gerät als aktiv und das sekundäre als Standby-Gerät zu konfigurieren, ist eine Best Practice, mit der Failover-Ereignisse nachverfolgt werden können.

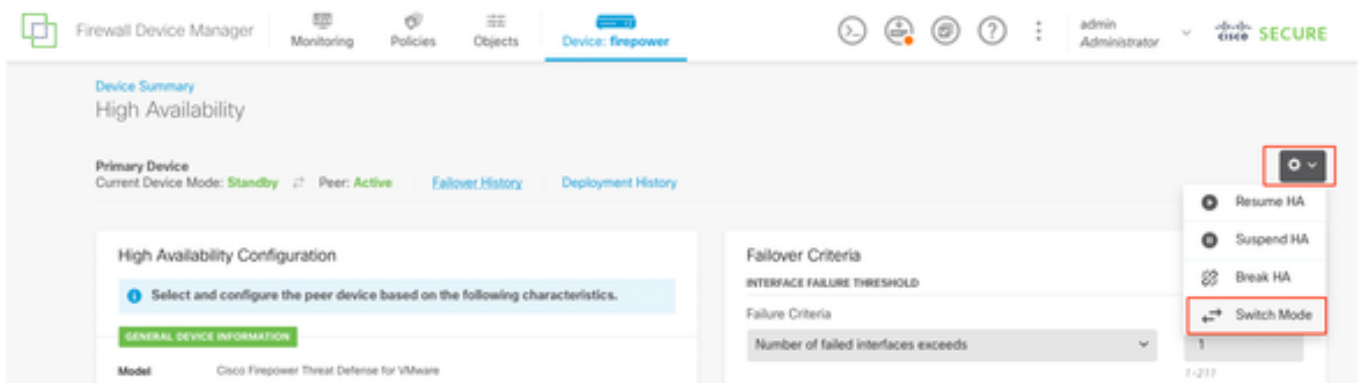
In diesem Fall ist "FTD Active" jetzt "Standby", und es kann ein manueller Failover verwendet werden, um den Status wieder auf "Active" zu setzen.

- Navigieren Sie zu Geräte > Hochverfügbarkeit.



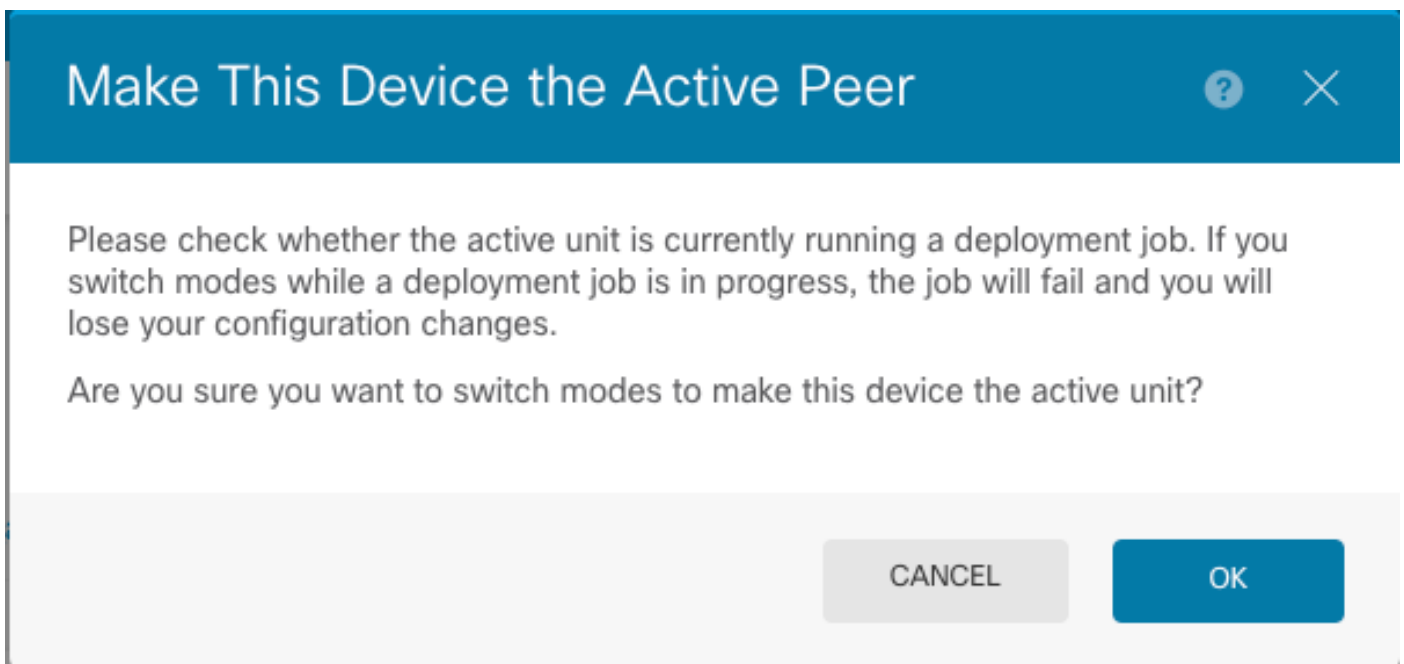
Hohe Verfügbarkeit

- Wählen Sie Switch Mode aus.



Switch-Modus

- Wählen Sie OK, um den Failover zu bestätigen.



Aktiver Peer

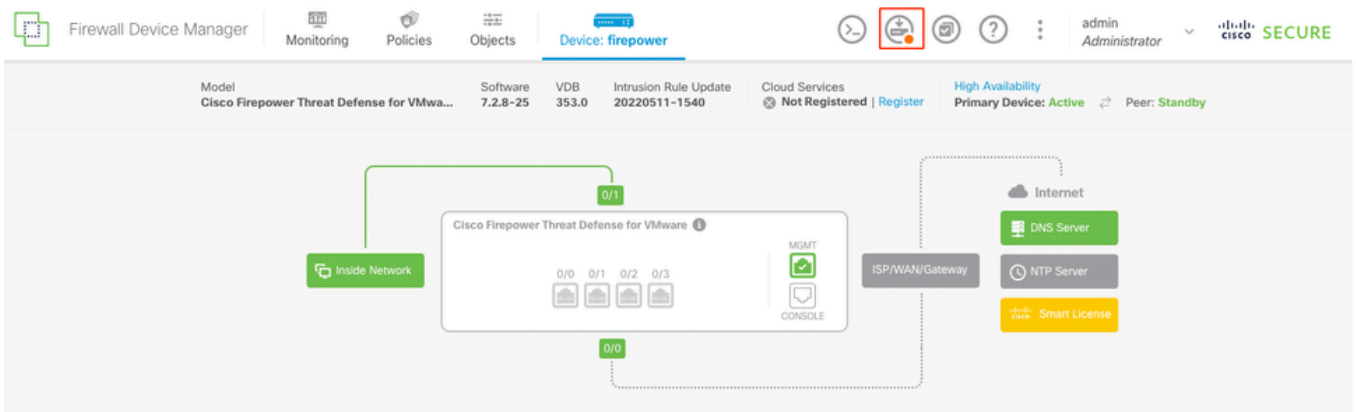
Validierung des HA-Status am Ende des Upgrades und Failover abgeschlossen.



Geräte

## Schritt 5: Finale Bereitstellung

- Stellen Sie die Richtlinie auf den Geräten bereit, indem Sie auf der Registerkarte "Bereitstellung" auf JETZT BEREITSTELLEN klicken.





## Pending Changes



✓ **Last Deployment Completed Successfully**  
14 Oct 2024 06:26 PM. [See Deployment History](#)

| Deployed Version (14 Oct 2024 06:26 PM)                                  | Pending Version                                       | LEGEND       |
|--|---|--------------|
| <b>Rule Update Version Edited: 20220511-1540</b>                         |   |              |
| lastSuccessSRUDate: 2024-10-08 06:15:04Z                                 | 2024-10-14 12:53:26Z                                  |              |
| -  | lspVersions[1]: 20220511-1540                         |              |
| <b>VDB Version Edited: 353</b>   |   |              |
| <b>+ Snort Version Added: 3.1.21.800-2</b>                               |   |              |
| -  | snortVersion: 3.1.21.800-2                            |              |
| -  | snortPackage: /ngfw/var/sf/snort-3.1.21.800-2/snor... |              |
| -  | name: 3.1.21.800-2                                    |              |
| <b>Data SSL Cipher Setting Edited: DefaultDataSSLCipherSetting</b>       |   |              |
| <b>SSL Cipher Edited: DefaultSSLCipher</b>                               |   |              |
| -  | protocolVersions[0]: TLSV1                            |              |
| -  | protocolVersions[1]: DTLSV1                           |              |
| -  | protocolVersions[2]: TLSV1_1                          |              |
| <b>Intrusion Policy Edited: Security Over Connectivity - Cisco Talos</b> |   |              |
| <b>Intrusion Policy Edited: Maximum Detection - Cisco Talos</b>          |   |              |
| MORE ACTIONS ▾   | CANCEL  | DEPLOY NOW ▾ |

Richtlinienbereitstellung

## Validieren

Um zu überprüfen, ob HA-Status und Upgrade abgeschlossen sind, müssen Sie den Status bestätigen:

Primary: Aktiv

Sekundär: Standby-fähig

Beide befinden sich unter der Version, die die kürzlich geänderte Version ist (in diesem Beispiel 7.2.8).



## Failover

- Überprüfen Sie den Failover-Status über den CLI-Click mithilfe der Befehle `show failover state` und `show failover`, um detailliertere Informationen zu erhalten.

Cisco FirePOWER Extensible Operating System (FX-OS) v2.12.1 (Build 73)  
 Cisco Firepower Threat Defense für VMware v7.2.8 (Build 25)

```
> show failover state
```

|              | State         | Last Failure Reason | Date/Time |
|--------------|---------------|---------------------|-----------|
| This host -  | Primary       |                     |           |
|              | Active        | None                |           |
| Other host - | Secondary     |                     |           |
|              | Standby Ready | None                |           |

```
====Configuration State====
```

```
    Sync Skipped
```

```
====Communication State====
```

```
    Mac set
```

```
> show failover
```

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
```

Reconnect timeout 0:00:00

Unit Poll frequency 1 seconds, holdtime 15 seconds

Interface Poll frequency 5 seconds, holdtime 25 seconds

Interface Policy 1

Monitored Interfaces 3 of 311 maximum

MAC Address Move Notification Interval not set

failover replication http

Version: Ours 9.18(4)210, Mate 9.18(4)210

Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C

Last Failover at: 14:13:56 UTC Oct 15 2024

This host: Primary - Active

Active time: 580 (sec)

slot 0: ASAv hw/sw rev (/9.18(4)210) status (Up Sys)

Interface diagnostic (0.0.0.0): Normal (Waiting)

Interface inside (192.168.45.1): Normal (Waiting)

Interface outside (192.168.1.10): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

Other host: Secondary - Standby Ready

Active time: 91512 (sec)

Interface diagnostic (0.0.0.0): Normal (Waiting)

Interface inside (0.0.0.0): Normal (Waiting)

Interface outside (0.0.0.0): Normal (Waiting)

slot 1: snort rev (1.0) status (up)

slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics

Link : failover-link GigabitEthernet0/2 (up)

| Stateful Obj | xmit  | xerr | rcv   | rerr |
|--------------|-------|------|-------|------|
| General      | 11797 | 0    | 76877 | 0    |

|                    |       |   |       |   |
|--------------------|-------|---|-------|---|
| sys cmd            | 11574 | 0 | 11484 | 0 |
| up time            | 0     | 0 | 0     | 0 |
| RPC services       | 0     | 0 | 0     | 0 |
| TCP conn           | 0     | 0 | 0     | 0 |
| UDP conn           | 176   | 0 | 60506 | 0 |
| ARP tbl            | 45    | 0 | 4561  | 0 |
| Xlate_Timeout      | 0     | 0 | 0     | 0 |
| IPv6 ND tbl        | 0     | 0 | 0     | 0 |
| VPN IKEv1 SA       | 0     | 0 | 0     | 0 |
| VPN IKEv1 P2       | 0     | 0 | 0     | 0 |
| VPN IKEv2 SA       | 0     | 0 | 0     | 0 |
| VPN IKEv2 P2       | 0     | 0 | 0     | 0 |
| VPN CTCP upd       | 0     | 0 | 0     | 0 |
| VPN SDI upd        | 0     | 0 | 0     | 0 |
| VPN DHCP upd       | 0     | 0 | 0     | 0 |
| SIP Session        | 0     | 0 | 0     | 0 |
| SIP Tx             | 0     | 0 | 0     | 0 |
| SIP Pinhole        | 0     | 0 | 0     | 0 |
| Route Session      | 1     | 0 | 0     | 0 |
| Router ID          | 0     | 0 | 0     | 0 |
| User-Identity      | 0     | 0 | 30    | 0 |
| CTS SGTNAME        | 0     | 0 | 0     | 0 |
| CTS PAC            | 0     | 0 | 0     | 0 |
| TrustSec-SXP       | 0     | 0 | 0     | 0 |
| IPv6 Route         | 0     | 0 | 0     | 0 |
| STS Table          | 0     | 0 | 0     | 0 |
| Umbrella Device-ID | 0     | 0 | 0     | 0 |
| Rule DB B-Sync     | 0     | 0 | 30    | 0 |
| Rule DB P-Sync     | 1     | 0 | 266   | 0 |
| Rule DB Delete     | 0     | 0 | 0     | 0 |

#### Logical Update Queue Information

|         | Cur | Max | Total  |
|---------|-----|-----|--------|
| Recv Q: | 0   | 31  | 123591 |
| Xmit Q: | 0   | 1   | 12100  |

Wenn beide FTDs dieselbe Version verwenden und der HA-Status "fehlerfrei" ist, ist das Upgrade abgeschlossen.

## 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.