FTD Multi-Instance-Hochverfügbarkeit auf Firepower 4100 konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Failover in FTD-Containerinstanzen (Multi-Instance) konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den Bereichen Firepower Management Center und Firewall Threat Defense verfügen.

Verwendete Komponenten

Cisco FirePOWER Management Center Virtual 7.2.5
Cisco FirePOWER 4145 NGFW-Appliance (FTD) 7.2.5
FirePOWER eXtensible Operating System (FXOS) 2.12 (0.498)
Windows 10

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.

Vor der Bereitstellung von FTD Multi-Instance ist es wichtig zu verstehen, wie sich dies auf die Systemleistung auswirken kann, und eine entsprechende Planung durchzuführen. Lesen Sie die offizielle Dokumentation von Cisco, oder wenden Sie sich an einen technischen Mitarbeiter von Cisco, um eine optimale Bereitstellung und Konfiguration sicherzustellen.

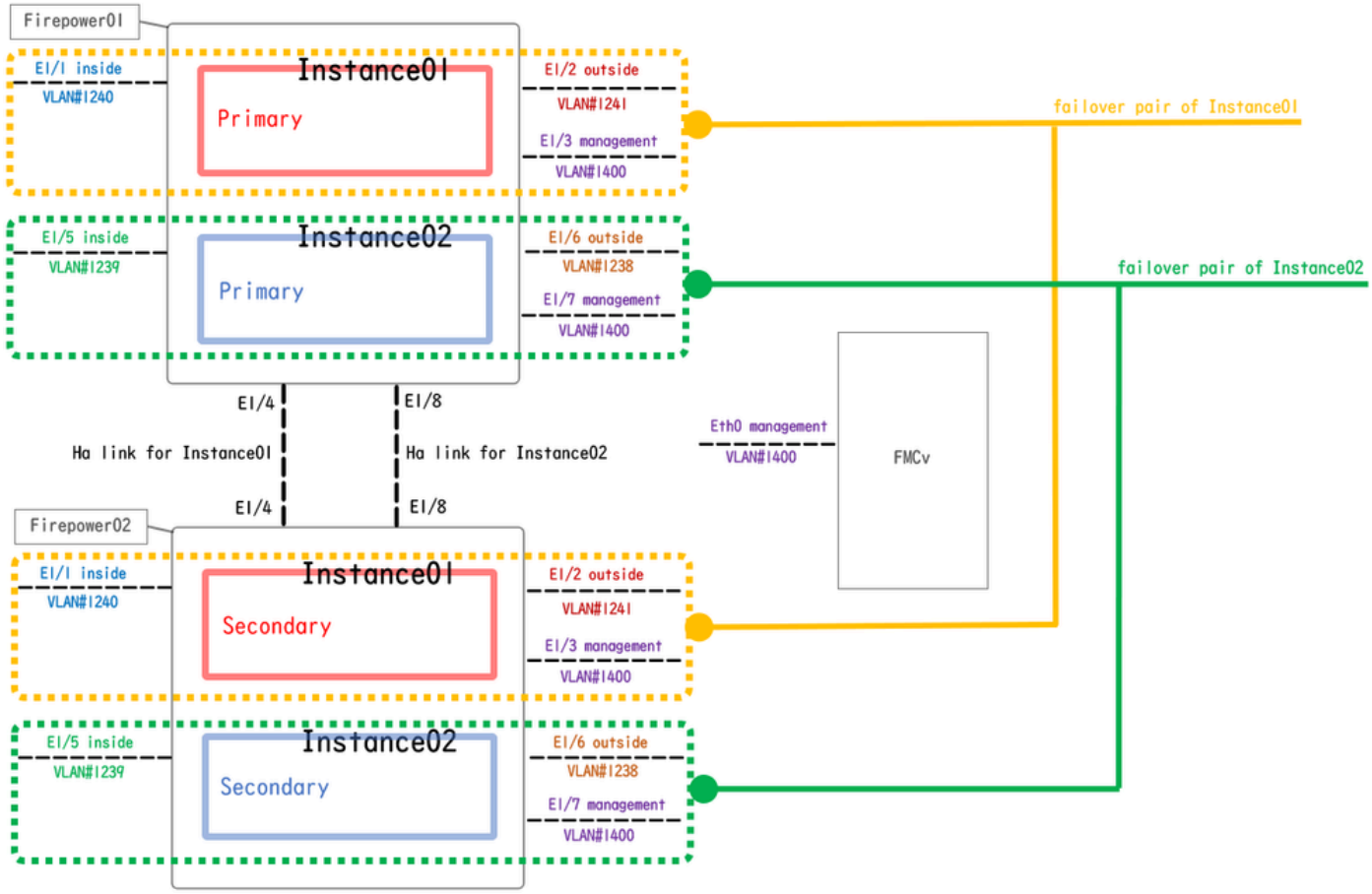
Hintergrundinformationen

Multi-Instance ist eine Funktion von FirePOWER Threat Defense (FTD), die dem ASA Multiple-Context-Modus ähnelt. Es ermöglicht Ihnen, mehrere separate Container-Instanzen von FTD auf einer einzigen Hardware auszuführen. Jede Container-Instanz ermöglicht die Trennung von Hardwareressourcen, ein separates Konfigurationsmanagement, separate Neuladevorgänge, separate Software-Updates und die Unterstützung der Funktionen zur umfassenden Bedrohungsabwehr. Dies ist besonders für Unternehmen nützlich, die unterschiedliche Sicherheitsrichtlinien für verschiedene Abteilungen oder Projekte benötigen, aber nicht in mehrere separate Hardware-Appliances investieren möchten. Die Multi-Instance-Funktion wird derzeit auf der Firepower 4100 und 9300 Series Security Appliance mit FTD 6.4 und höher unterstützt.

In diesem Dokument wird Firepower4145 verwendet, das maximal 14 Container-Instanzen unterstützt. Informationen zu den maximal in der FirePOWER-Appliance unterstützten Instanzen finden Sie unter Maximum Container Instances and Resources per Model.

Netzwerkdiagramm

In diesem Dokument wird die Konfiguration und Verifizierung für HA in Multi-Instance in diesem Diagramm vorgestellt.



Logisches Konfigurationsdiagramm

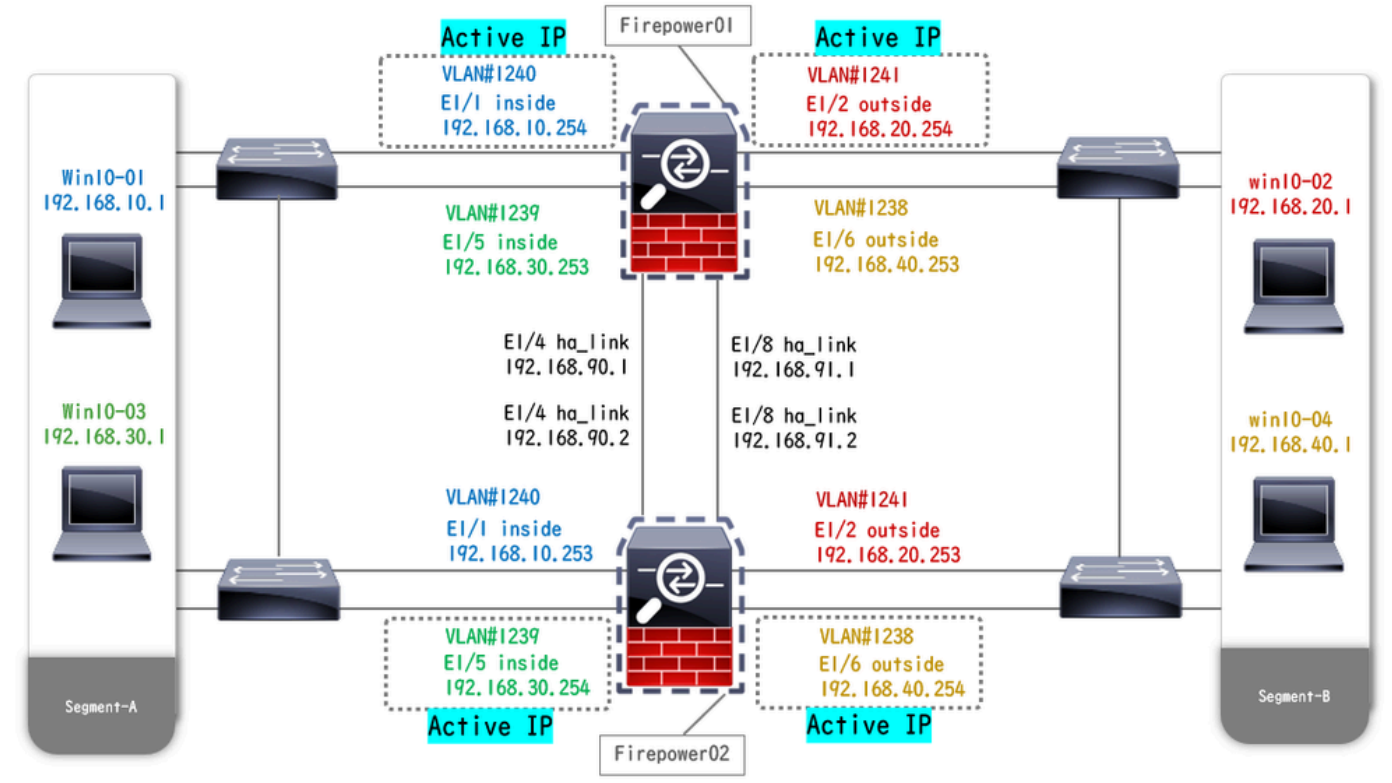
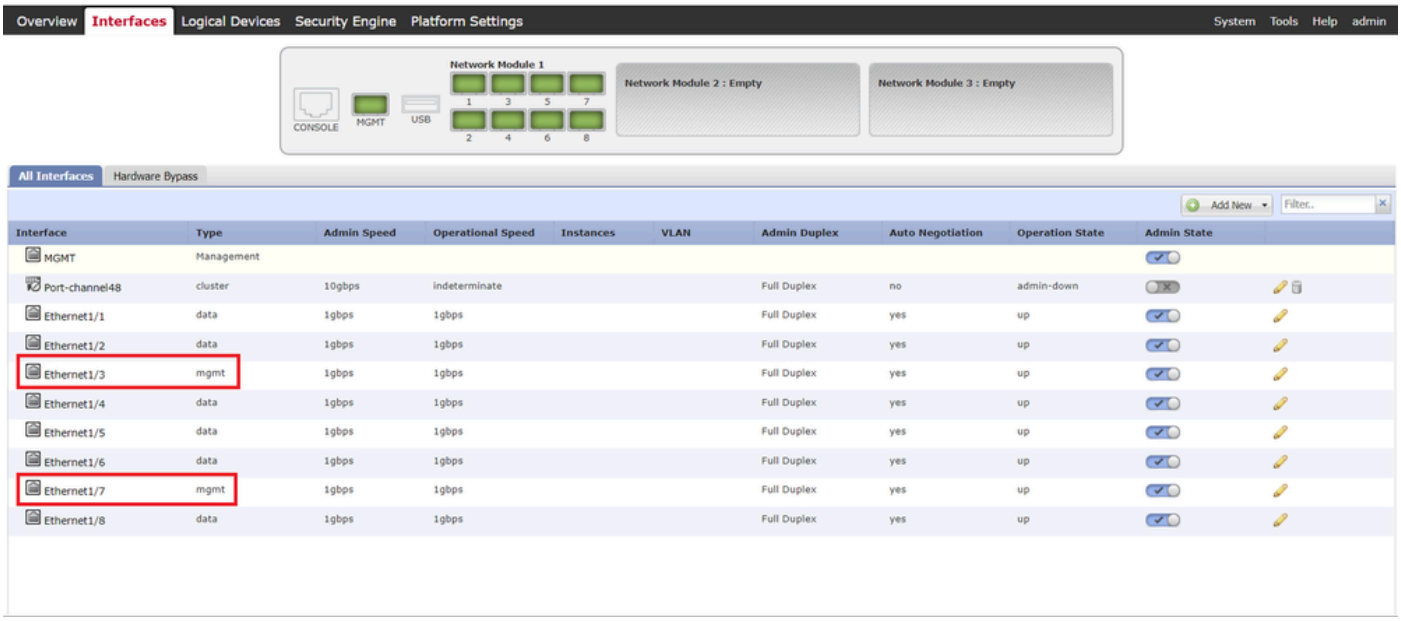


Diagramm der physischen Konfiguration

Konfigurationen

Schritt 1: Schnittstellen vorkonfigurieren

a. Navigieren Sie zu Schnittstellen in FCM. 2 Management-Schnittstellen festlegen. In diesem Beispiel Ethernet1/3 und Ethernet1/7.



Schnittstellen vorkonfigurieren

Schritt 2: Fügen Sie 2 Ressourcenprofile für Containerinstanzen hinzu.

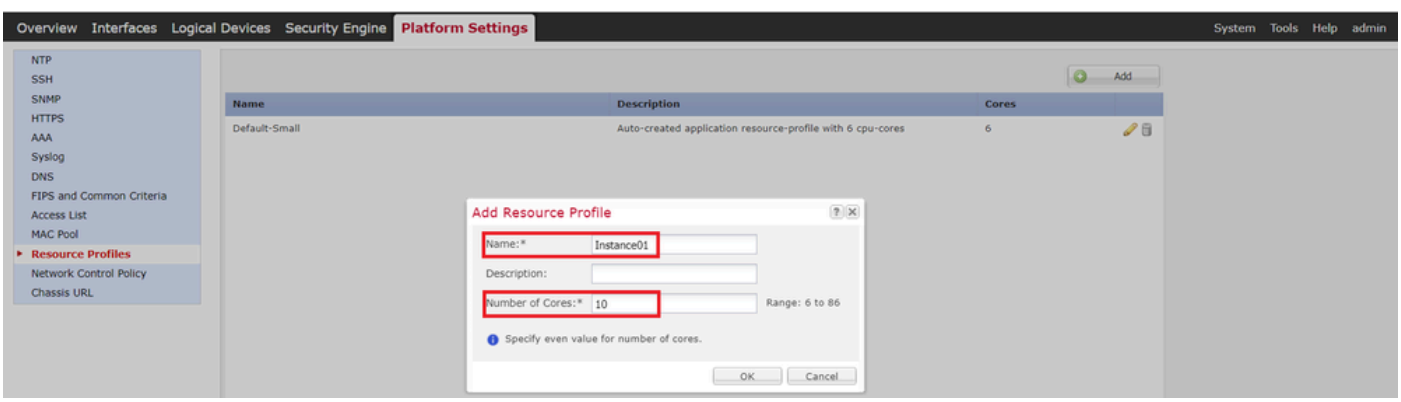
a. Navigieren Sie zu Plattformeinstellungen > Ressourcenprofile > Auf FCM hinzufügen. Erstes Ressourcenprofil festlegen.

In diesem Beispiel:
- Name: Instanz01
- Kernanzahl: 10

Hinweis: Für HA des Containerinstanzpaars müssen dieselben Ressourcenprofilattribute verwendet werden.

Legen Sie einen Profilnamen mit 1 bis 64 Zeichen fest. Beachten Sie, dass Sie den Namen dieses Profils nach dem Hinzufügen nicht mehr ändern können.

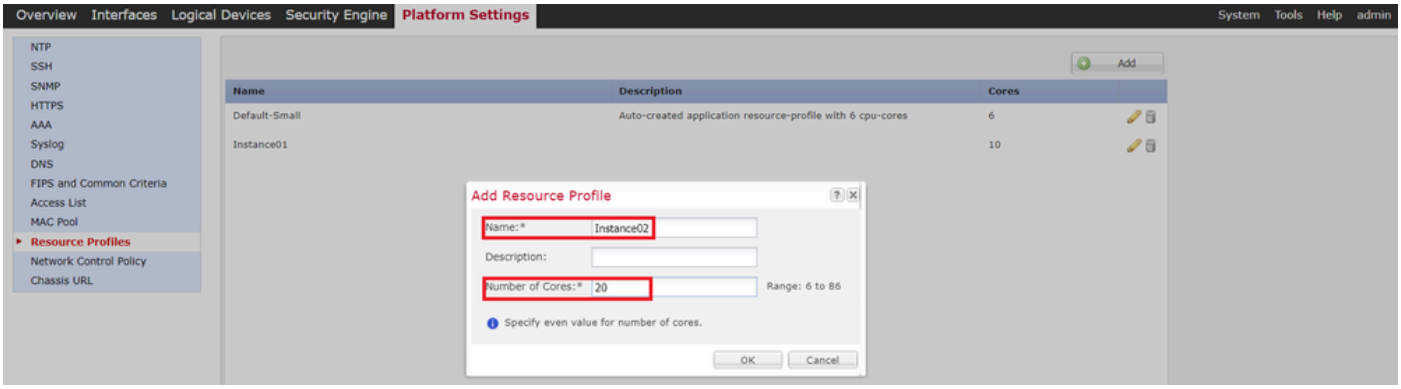
Legen Sie die Anzahl der Kerne für das Profil zwischen 6 und dem Maximum fest.



1. Ressourcenprofil hinzufügen

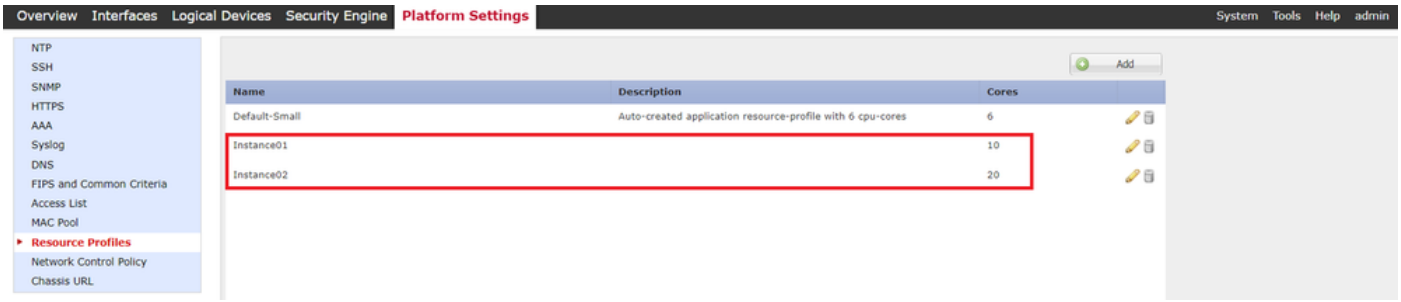
b. Wiederholen Sie a. in Schritt 2, um das zweite Ressourcenprofil zu konfigurieren.

In diesem Beispiel:
- Name: Instanz02
- Kernanzahl: 20



Zweites Ressourcenprofil hinzufügen

c. Überprüfen Sie, ob zwei Ressourcenprofile erfolgreich hinzugefügt wurden.



Ressourcenprofil bestätigen

Schritt 3: (Optional) Fügen Sie ein MAC-Pool-Präfix der virtuellen MAC-Adresse für Container-Instanzschnittstellen hinzu.

Sie können die virtuelle MAC-Adresse für die Active/Stanby-Schnittstelle manuell festlegen. Wenn für Multi-Instance-Funktionen keine virtuellen MAC-Adressen festgelegt wurden, generiert das Chassis automatisch MAC-Adressen für Instance-Schnittstellen und garantiert, dass eine gemeinsam genutzte Schnittstelle in jeder Instance eine eindeutige MAC-Adresse verwendet.

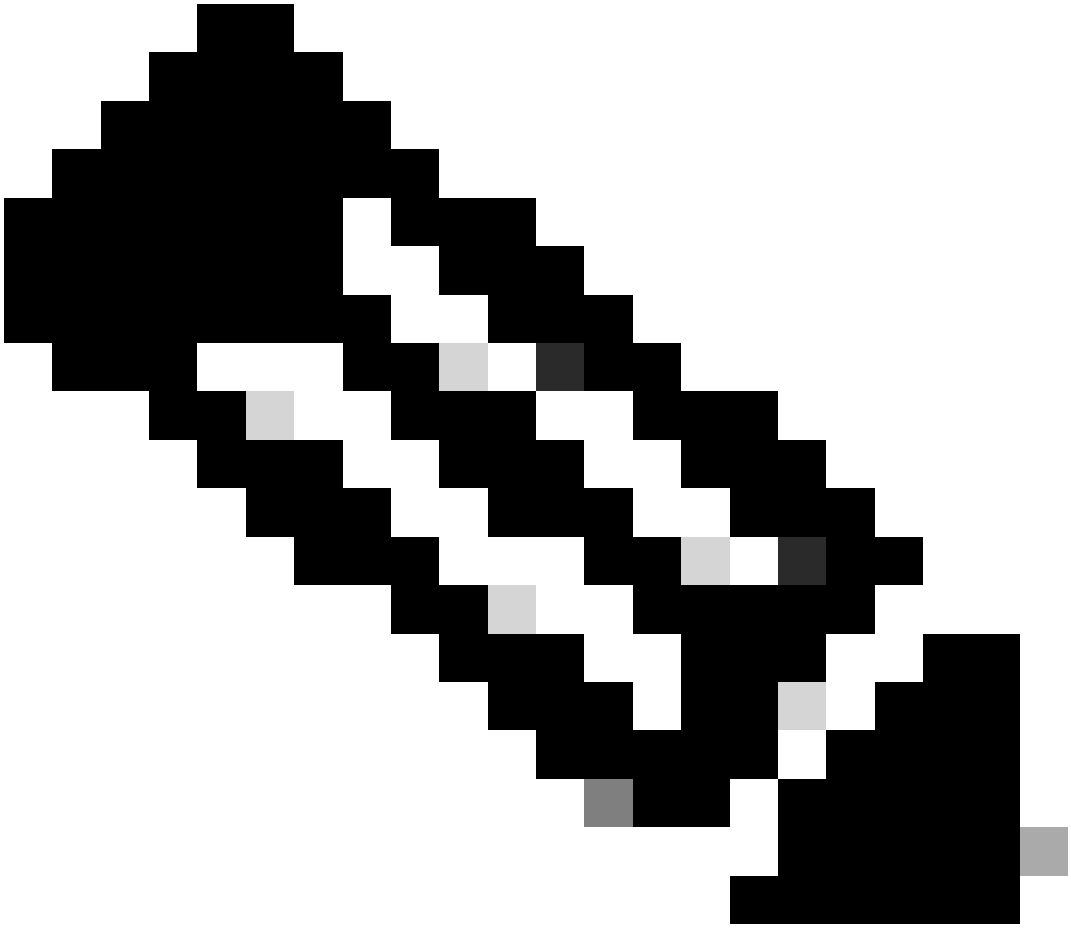
Weitere Informationen zur MAC-Adresse finden Sie unter Add a MAC Pool Prefix (MAC-Pool-Präfix hinzufügen) und View MAC Addresses for Container Instance Interfaces (MAC-Adressen für Containerinstanzschnittstellen anzeigen).

Schritt 4: Hinzufügen einer eigenständigen Instanz.

a. Navigieren Sie zu Logische Geräte > Eigenständig hinzufügen. Erste Instanz festlegen.

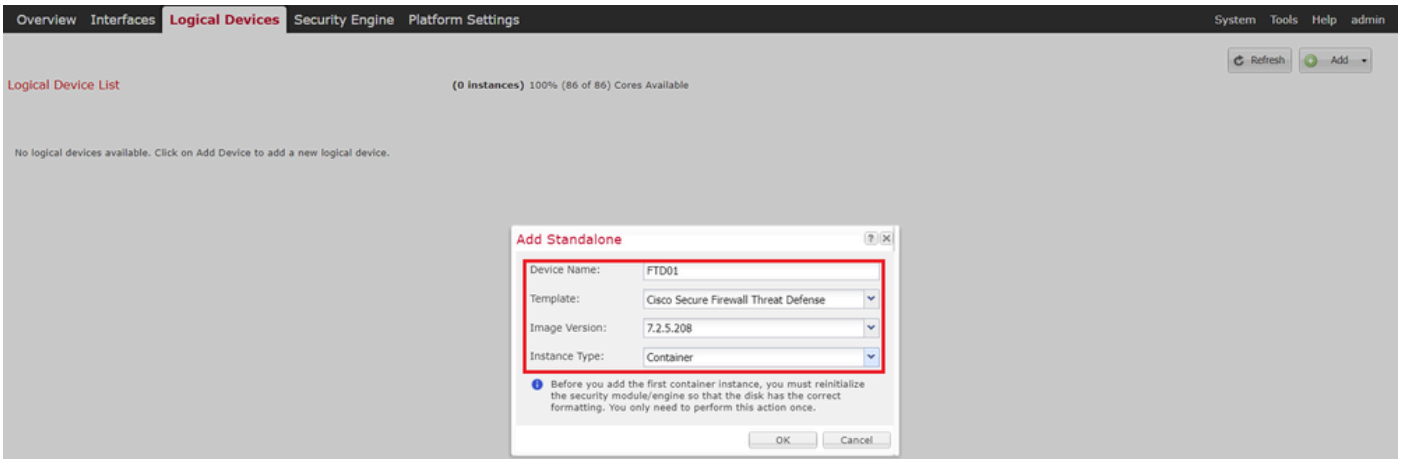
In diesem Beispiel:

- Gerätename: FTD01
- Instanztyp: Container



Hinweis: Die einzige Möglichkeit, eine Containeranwendung bereitzustellen, besteht darin, eine App-Instanz vorab bereitzustellen, wobei Instanztyp auf Container festgelegt ist. Stellen Sie sicher, dass Sie Container auswählen.

Sie können diesen Namen nicht mehr ändern, nachdem Sie das logische Gerät hinzugefügt haben.



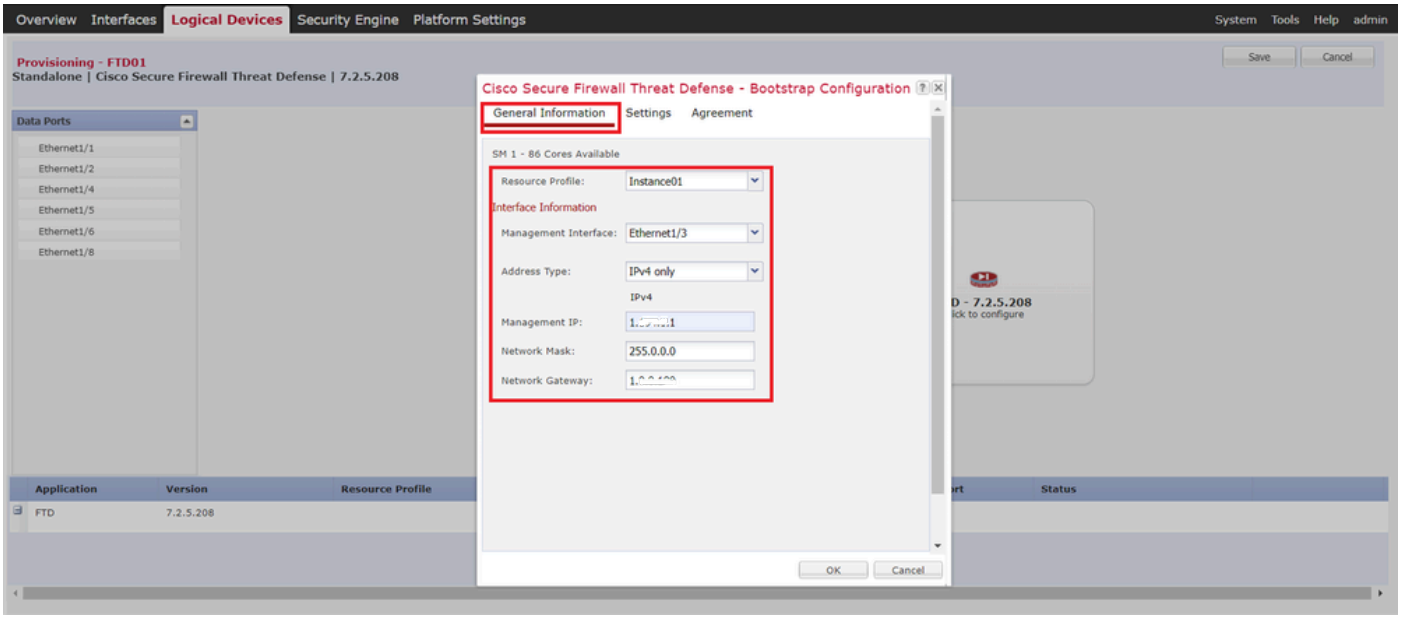
Instanz hinzufügen

Schritt 5: Schnittstellen konfigurieren

a. Legen Sie das Ressourcenprofil, die Verwaltungsschnittstelle und die Verwaltungs-IP für Instance01 fest.

In diesem Beispiel:

- Ressourcenprofil: Instanz01
- Management-Schnittstelle: Ethernet 1/3
- Management-IP: x.x.1.1



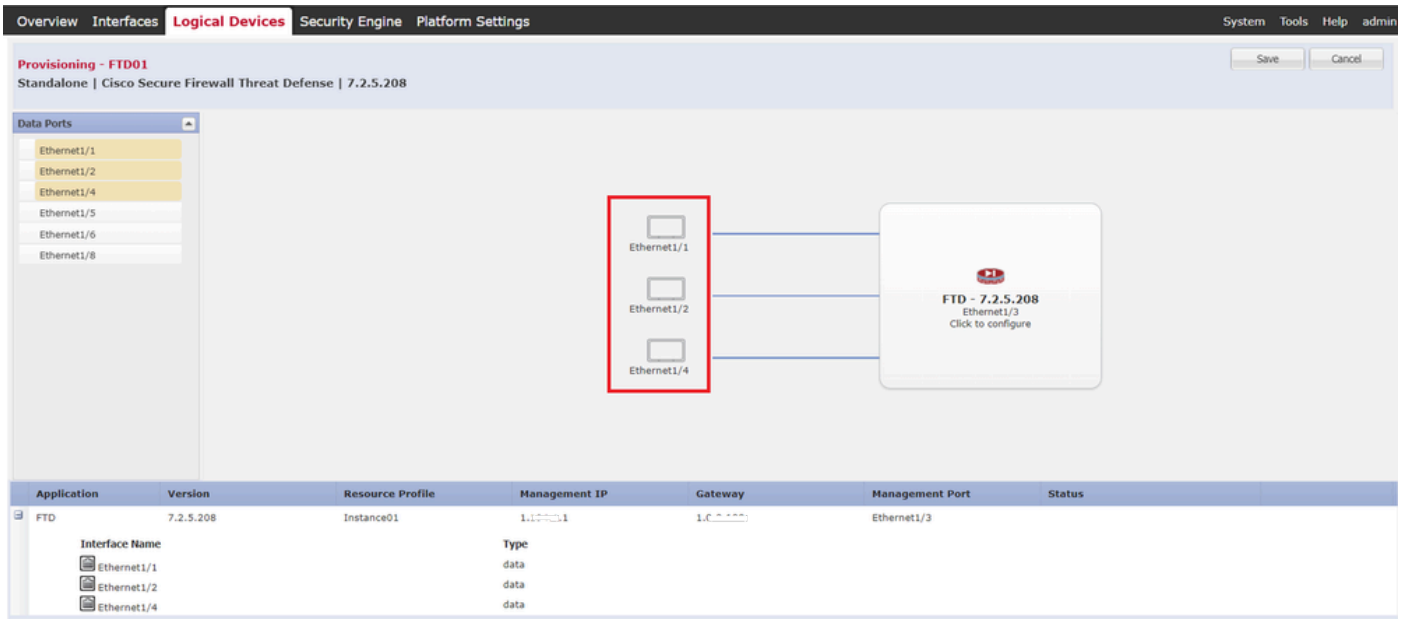
Profil/Management-Schnittstelle/Management-IP konfigurieren

b. Festlegen von Datenschnittstellen

In diesem Beispiel:

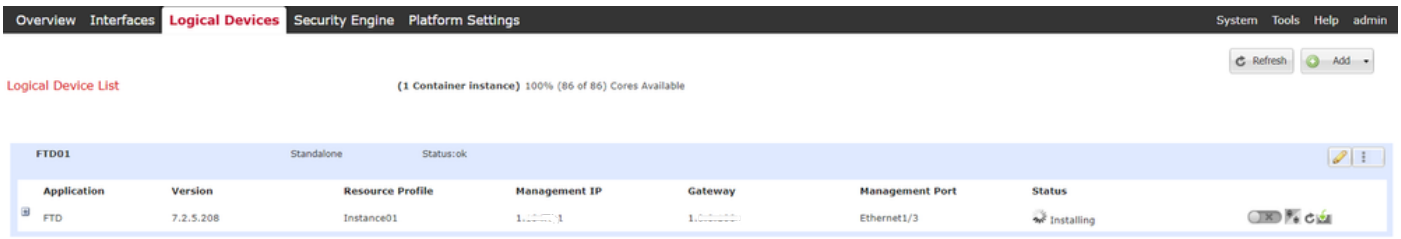
- Ethernet1/1 (für Innenbereiche verwendet)
- Ethernet1/2 (für Außenbereiche)

- Ethernet1/4 (für HA-Verbindung)



Festlegen von Datenschnittstellen

c. Navigieren Sie zu Logische Geräte. Warten auf Instanzstart.



Status von Instanz bestätigen01

d. Wiederholen Sie a. in Schritt 4.a und Schritt 5.a bis c, um eine 2. Instanz hinzuzufügen und Details dafür festzulegen.

In diesem Beispiel:

- Gerätename: FTD11
- Instanztyp: Container

- Ressourcenprofil: Instanz02
- Management-Schnittstelle: Ethernet1/7
- Management-IP: x.x.10.1

- Ethernet1/5 = innen

- Ethernet1/6 = außen

- Ethernet1/8 = HA-Verbindung

e. Bestätigen Sie, dass 2 Instanzen Online-Status auf FCM haben.

Instanzstatus im primären Gerät bestätigen

f. (Optional)Führen Sie scope ssa aus, **scope slot 1** und **show app-Instance** bestätigen Sie, dass 2 Instanzen in der Firepower-CLI den Status "Online" haben.

```
<#root>
```

FPR4145-ASA-K9#

```
scope ssa
 FPR4145-ASA-K9 /ssa #
scope slot 1
 FPR4145-ASA-K9 /ssa/slot #
show app-Instance
 Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deplo
Online
7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11
Online
7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online
```

g. Führen Sie die gleichen Schritte auf dem sekundären Gerät aus. Bestätigen Sie, dass 2 Instanzen den Status "Online" haben.

Instanzstatus im sekundären Gerät bestätigen

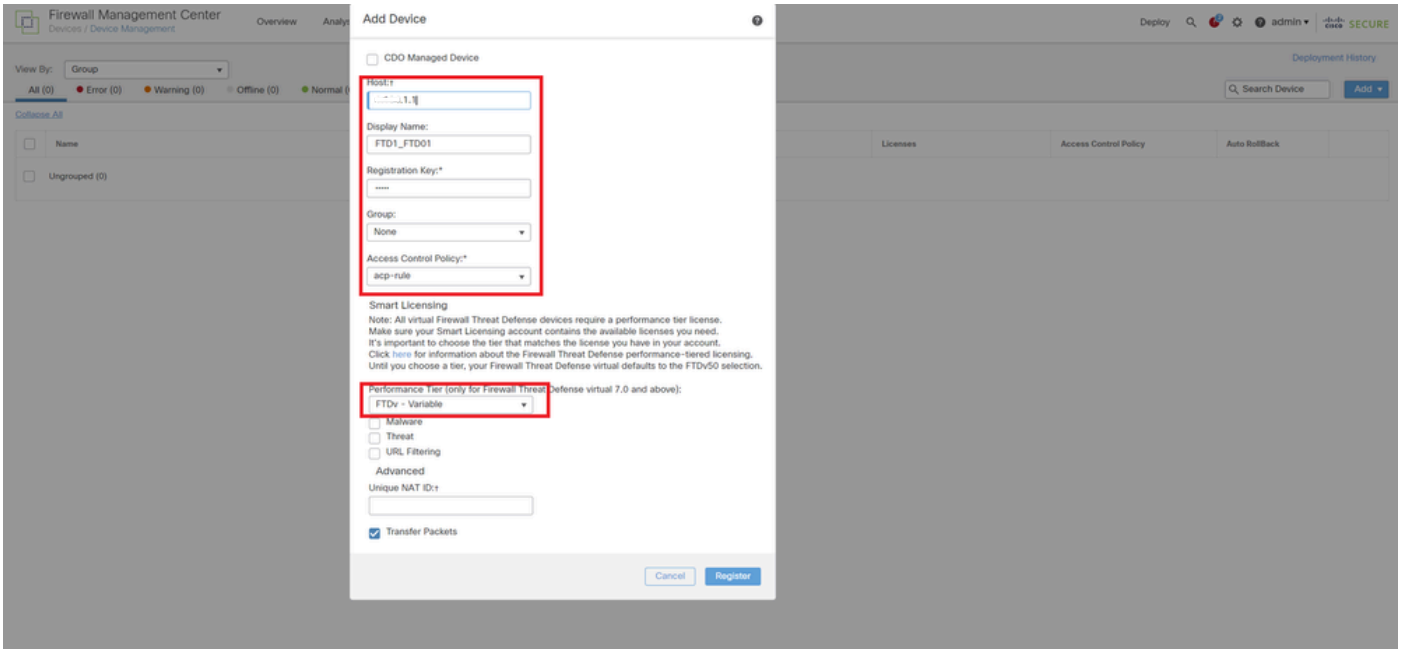
Schritt 6: Hochverfügbarkeitspaar für jede Instanz hinzufügen.

a. Navigieren Sie zu **Geräte** > **Gerät** auf FMC **hinzufügen**. Alle Instanzen zu FMC hinzufügen.

In diesem Beispiel:

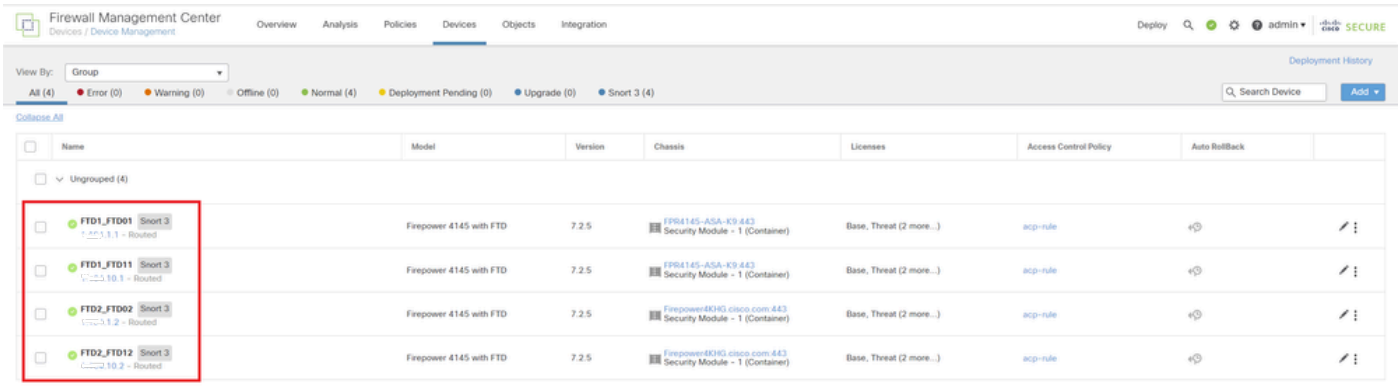
- Anzeigename für Instanz01 von FTD1: FTD1_FTD01
- Anzeigename für Instanz02 von FTD1: FTD1_FTD11
- Anzeigename für Instanz01 von FTD2: FTD2_FTD02
- Anzeigename für Instanz02 von FTD2: FTD2_FTD12

Dieses Bild zeigt die Einstellung für **FTD1_FTD01**.



FTD-Instanz zu FMC hinzufügen

b. Bestätigen Sie, dass alle Instanzen normal sind.



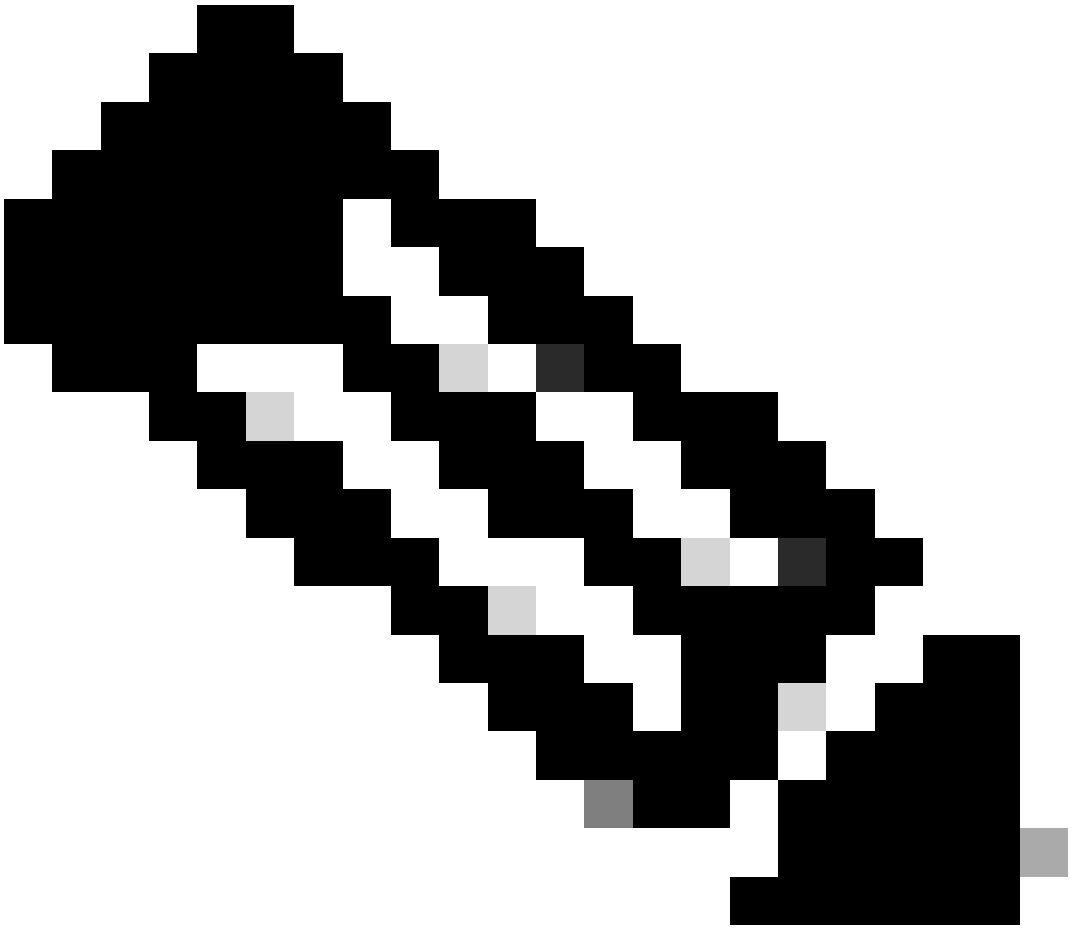
Instanzstatus in FMC bestätigen

c. Navigieren Sie zu **Geräte** > **Hochverfügbarkeit hinzufügen**. Erstes Failover-Paar einrichten.

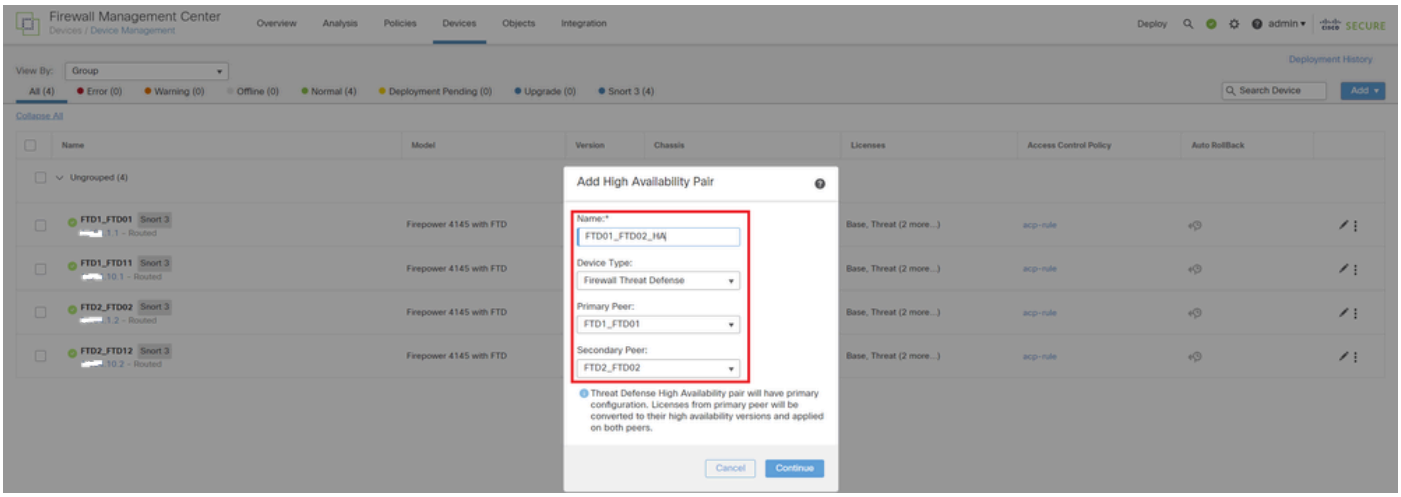
In diesem Beispiel:

- **Name: FTD01_FTD02_HA**
- **Primäre Gegenstelle: FTD1_FTD01**

- **Sekundärer Peer: FTD2_FTD02**



Hinweis: Wählen Sie die richtige Einheit als primäre Einheit aus.

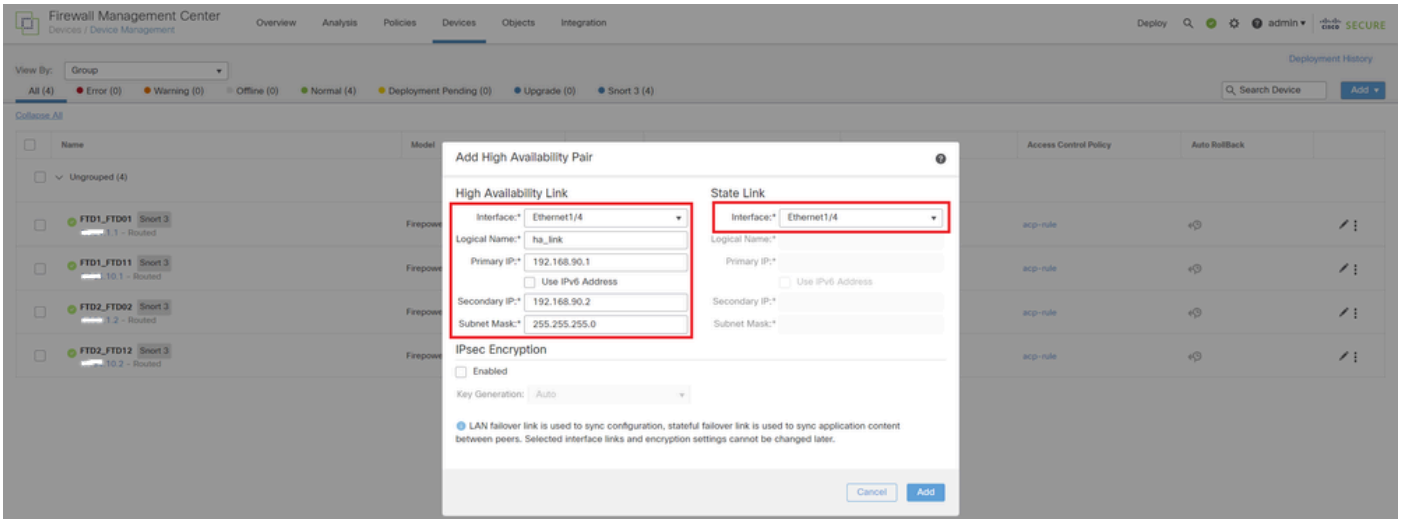


Erstes Failover-Paar hinzufügen

d. Einstellen der IP für die Failover-Verbindung im ersten Failover-Paar

In diesem Beispiel:

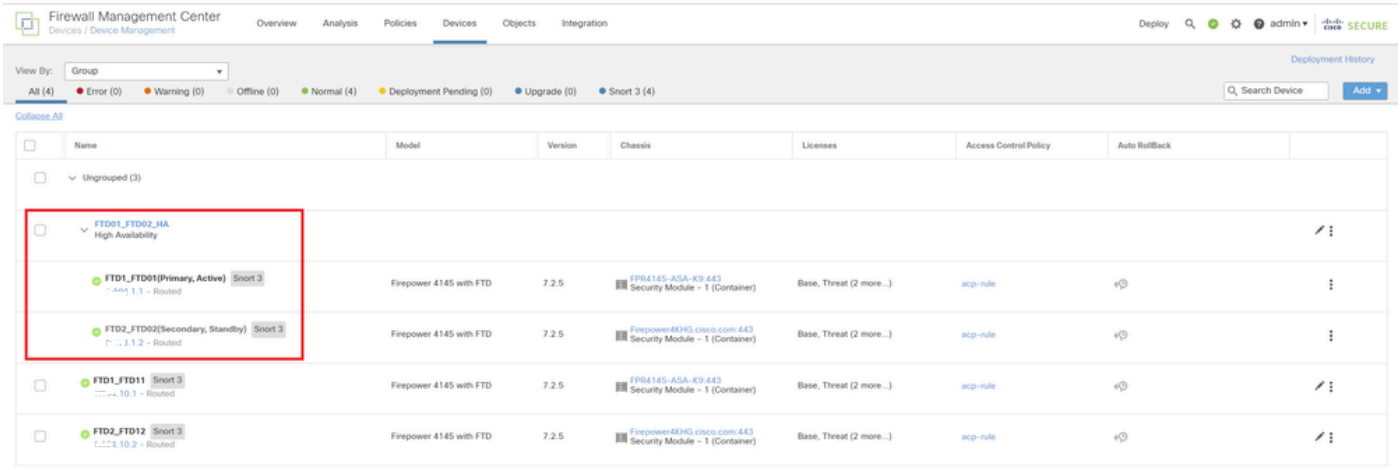
- **Hochverfügbarkeits-Link: Ethernet 1/4**
- **Zustandsverbindung: Ethernet 1/4**
- **Primäre IP: 192.168.90.1/24**
- **Sekundäre IP: 192.168.90.2/24**



HA-Schnittstelle und IP für das erste Failover-Paar einrichten

e. Den Failover-Status bestätigen

- **FTD1_FTD01 : Primär, Aktiv**
- **FTD2_FTD02 : Sekundär, Standby**



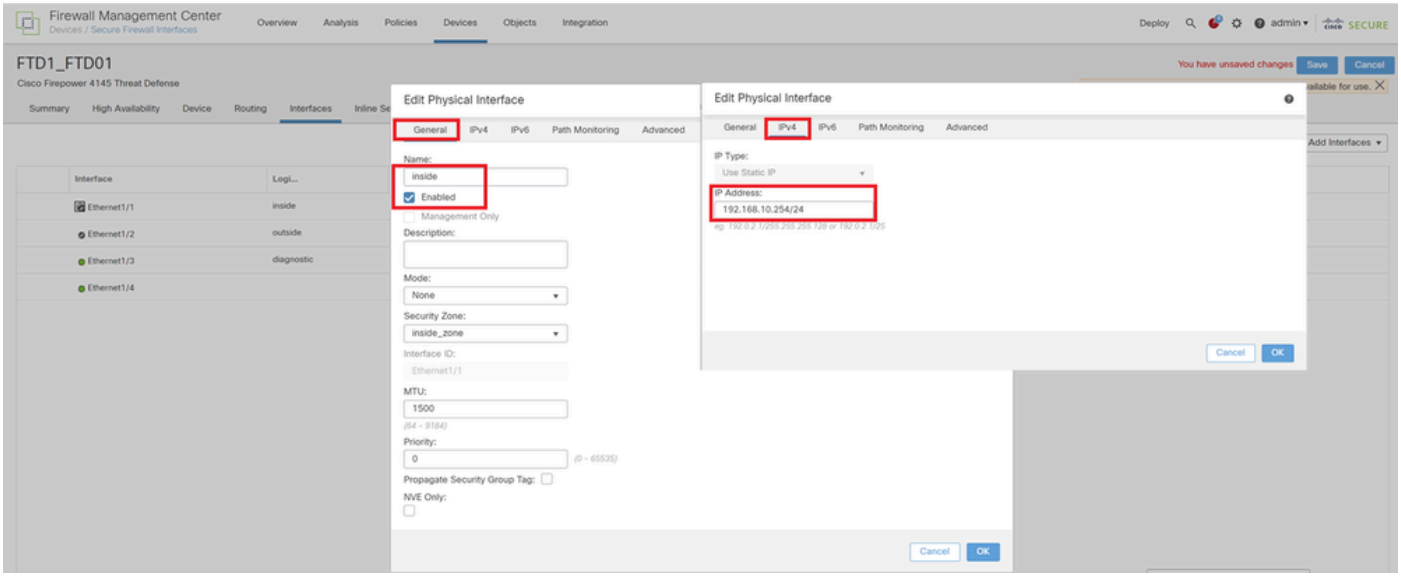
Status des ersten Failover-Paars bestätigen

f. Navigieren Sie zu **Geräte** > **Klicken Sie auf FTD01_FTD02_HA** (in diesem Beispiel) > **Schnittstellen.** Aktive IP für Datenschnittstelle festlegen.

In diesem Beispiel:

- Ethernet1/1 (innen): 192.168.10.254/24
- Ethernet1/2 (außen): 192.168.20.254/24
- Ethernet1/3 (Diagnose): 192.168.80.1/24

Dieses Bild zeigt die Einstellung für "Active IP" von **Ethernet1/1**.



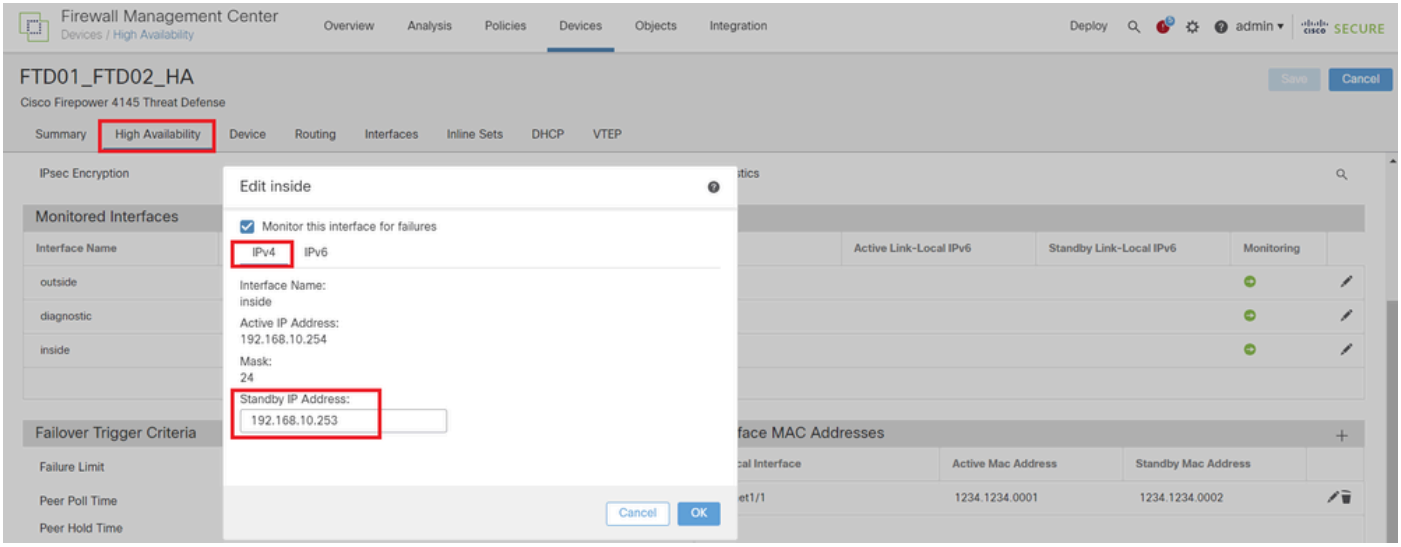
Aktive IP für Datenschnittstelle festlegen

g. Navigieren Sie zu **Devices** > **Klicken Sie auf FTD01_FTD02_HA** (in diesem Beispiel) > **High Availability.** Standby-IP für Datenschnittstelle festlegen.

In diesem Beispiel:

- Ethernet1/1 (innen): 192.168.10.253/24
- Ethernet1/2 (außen): 192.168.20.253/24
- Ethernet1/3 (Diagnose): 192.168.80.2/24

Dieses Bild zeigt die Einstellung für Standby-IP von **Ethernet1/1**.



Standby-IP für Datenschnittstelle festlegen

h. Wiederholen Sie die Schritte 6.c bis g, um das zweite Failover-Paar hinzuzufügen.

In diesem Beispiel:

- Name: FTD11_FTD12_HA
- Primäre Gegenstelle: FTD1_FTD11
- Sekundärer Peer: FTD2_FTD12

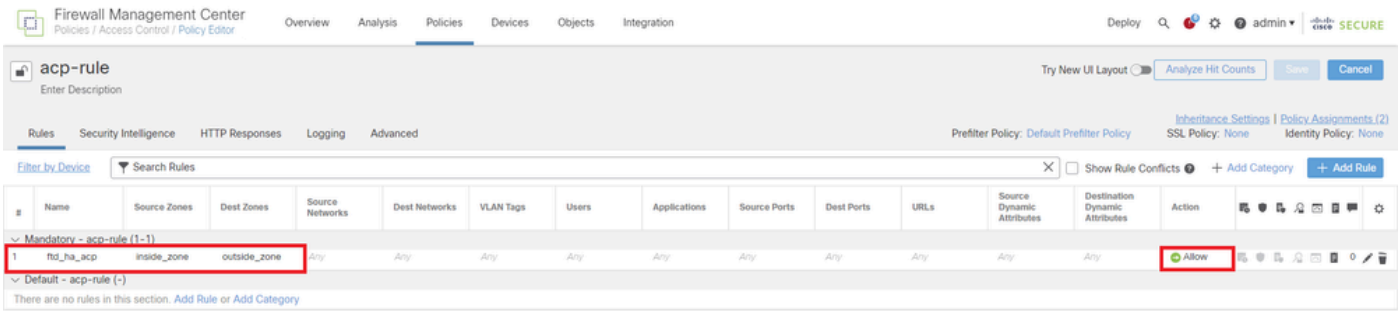
- Hochverfügbarkeits-Verbindung: Ethernet1/8
- State Link: Ethernet1/8
- Ethernet1/8 (ha_link Active): 192.168.91.1/24

- Ethernet1/5 (innen aktiv): 192.168.30.254/24
- Ethernet1/6 (außerhalb aktiv): 192.168.40.254/24
- Ethernet1/7 (Diagnose aktiv): 192.168.81.1/24

- Ethernet1/8 (ha_link Standby): 192.168.91.2/24

- Ethernet1/5 (im Standby-Modus): 192.168.30.253/24
- Ethernet1/6 (außerhalb von Standby): 192.168.40.253/24
- Ethernet1/7 (Diagnose-Standby): 192.168.81.2/24

i. Navigieren Sie zu **Logische Geräte** > **Eigenständige Geräte hinzufügen**. Legen Sie die ACP-Regel fest, um den Datenverkehr von innen nach außen zuzulassen.



AKP-Regel festlegen

j. Stellen Sie die Einstellung auf FTD bereit.

k. Bestätigen des HA-Status in CLI

Der HA-Status für jede Instanz wird auch in der Firepower-CLI bestätigt, die mit dem ASA-Standard identisch ist.

Ausführen **show running-config failover** und **show failover** Befehl zur Bestätigung des HA-Status von FTD1_FTD01 (primäre Instanz 01) .

```
<#root>

// confrim HA status of FTD1_FTD01 (Instance01 of Primary Device) >

show running-config failover

 failover failover lan unit primary failover lan interface ha_link Ethernet1/4 failover replication htt

show failover

 Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/4 (up) ...... This host: P
...... Other host: Secondary - Standby Ready <---- Instance01 of FPR02 is Standby Interface diagnostic
```

Ausführen **show running-config failover** und **show failover** Befehl zur Bestätigung des HA-Status von FTD1_FTD11 (primäre Instanz 02) .

```
<#root>

// confrim HA status of FTD1_FTD11 (Instance02 of Primary Device) >

show running-config failover

 failover failover lan unit primary failover lan interface ha_link Ethernet1/8 failover replication htt

show failover

 Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/8 (up) ...... This host: P
Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16
```

Ausführen **show running-config failover** und **show failover** Befehl zur Bestätigung des HA-Status von FTD2_FTD02 (sekundäre Instanz 01) .

```
<#root>

// confrim HA status of FTD2_FTD02 (Instance01 of Secondary Device) >

show running-config failover

 failover failover lan unit secondary failover lan interface ha_link Ethernet1/4 failover replication h

show failover

 Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) ...... This host:
Other host: Primary - Active <---- Instance01 of FPR01 is Active Active time: 31651 (sec) slot 0: UCSB-
```

Ausführung **show running-config failover** und **show failover** Befehl zur Bestätigung des HA-Status von FTD2_FTD12 (sekundäre Instanz 02) .

<#root>

// confrim HA status of FTD2_FTD12 (Instance02 of Secondary Device) >

show running-config failover

```
 failover failover lan unit secondary failover lan interface ha_link Ethernet1/8 failover replication h
Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-
```

l. Lizenznutzung bestätigen

Alle Lizenzen werden pro Sicherheits-Engine/Chassis genutzt, nicht pro Container-Instanz.

・ Grundlizenzen werden automatisch zugewiesen: eine pro Security Engine/Chassis.

・ Funktionslizenzen werden manuell jeder Instanz zugewiesen. Sie benötigen jedoch nur eine Lizenz pro Feature pro Sicherheits-Engine/-Chassis. Für eine spezielle Feature-Lizenz benötigen Sie nur eine Lizenz, unabhängig von der Anzahl der verwendeten Instanzen.

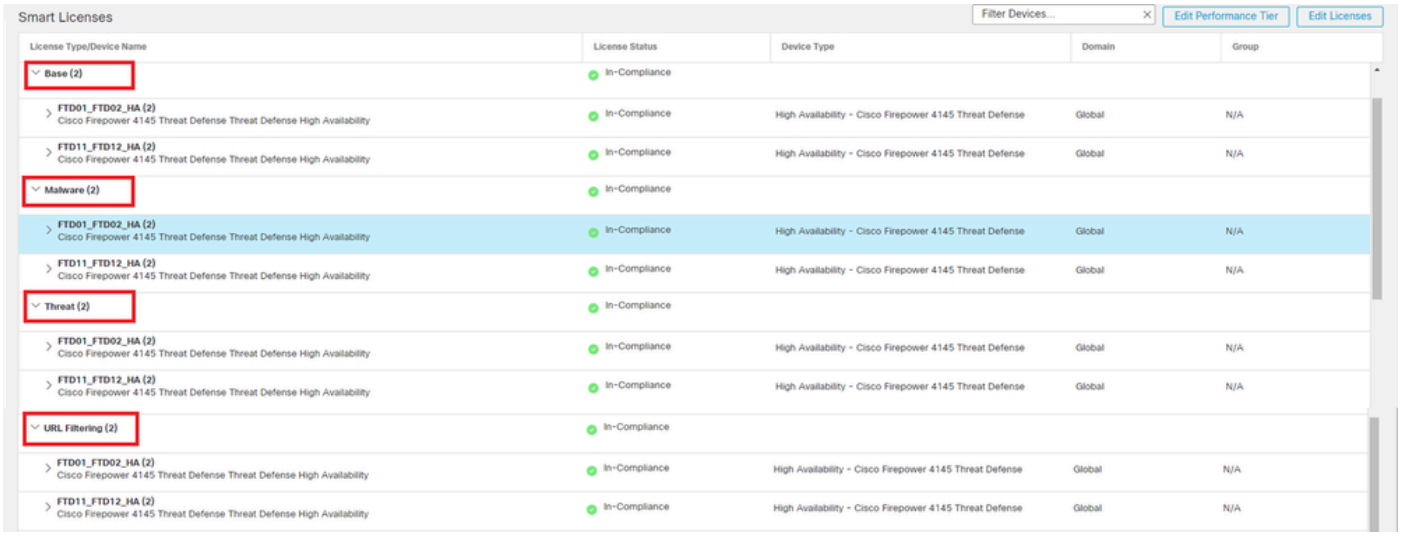
Diese Tabelle zeigt, wie die Lizenzen in diesem Dokument verwendet werden.

FPR01	Instanz 01	Basis, URL-Filterung, Malware, Bedrohung
	Instanz 02	Basis, URL-Filterung, Malware, Bedrohung
FPR02	Instanz 01	Basis, URL-Filterung, Malware, Bedrohung
	Instanz 02	Basis, URL-Filterung, Malware, Bedrohung

Gesamtzahl der Lizenzen

Basis	URL-Filterung	Malware	Bedrohung
2	2	2	2

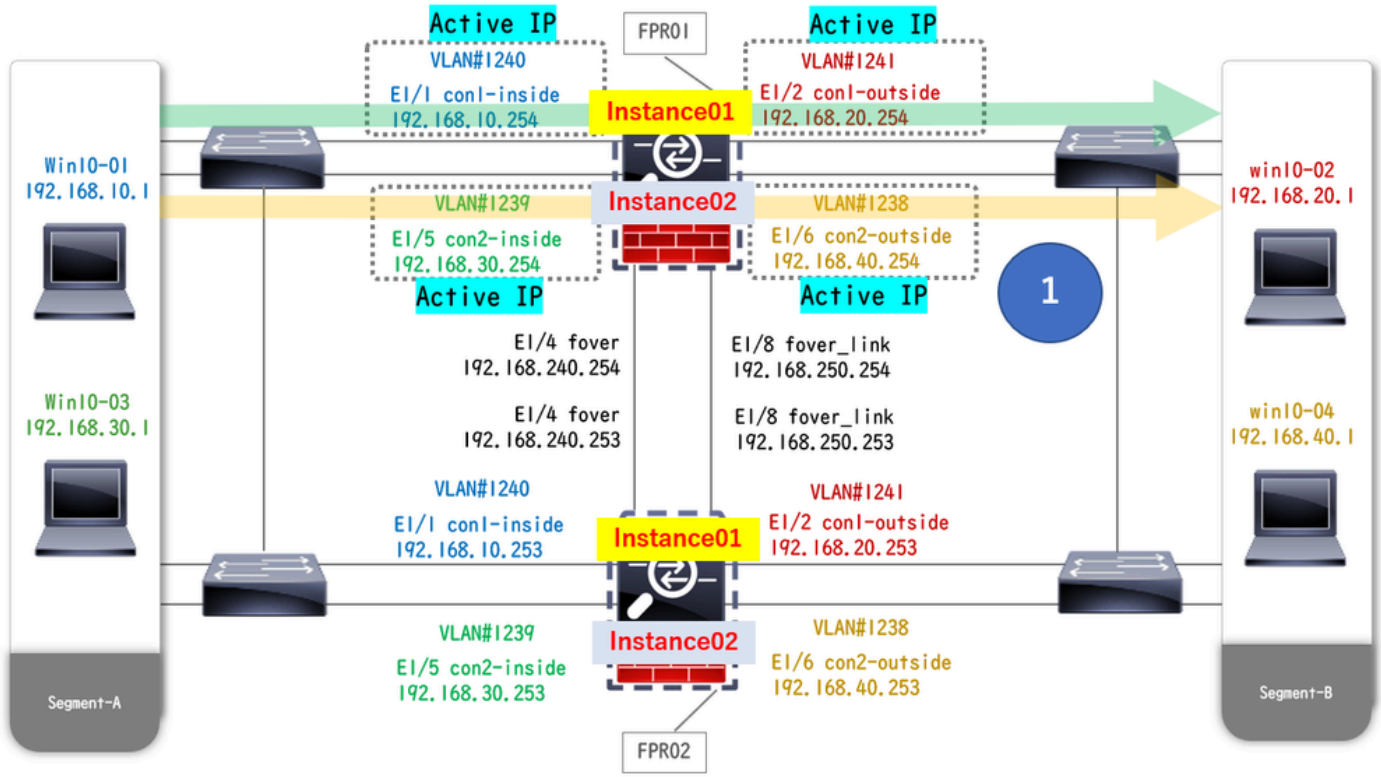
Bestätigen Sie die Anzahl der genutzten Lizenzen in der FMC-GUI.



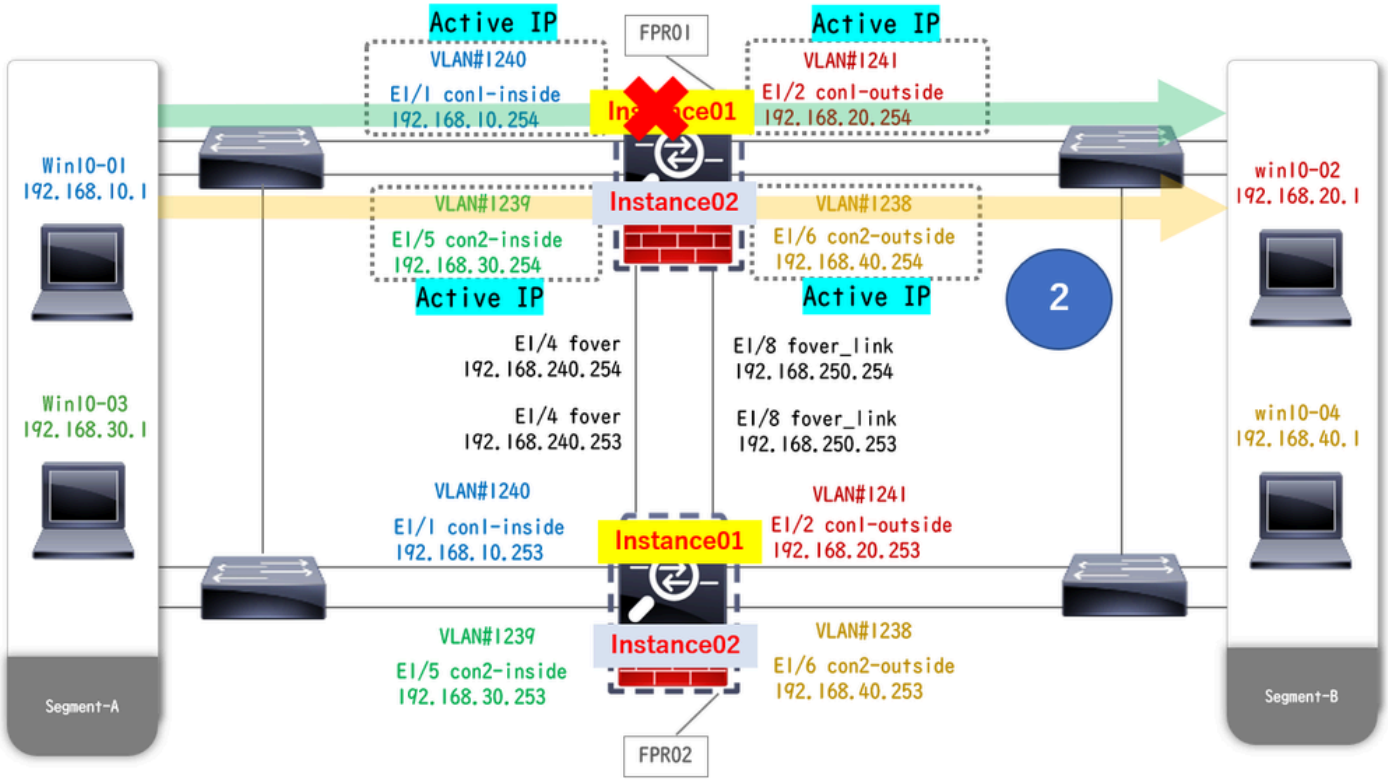
Genutzte Lizenzen bestätigen

Überprüfung

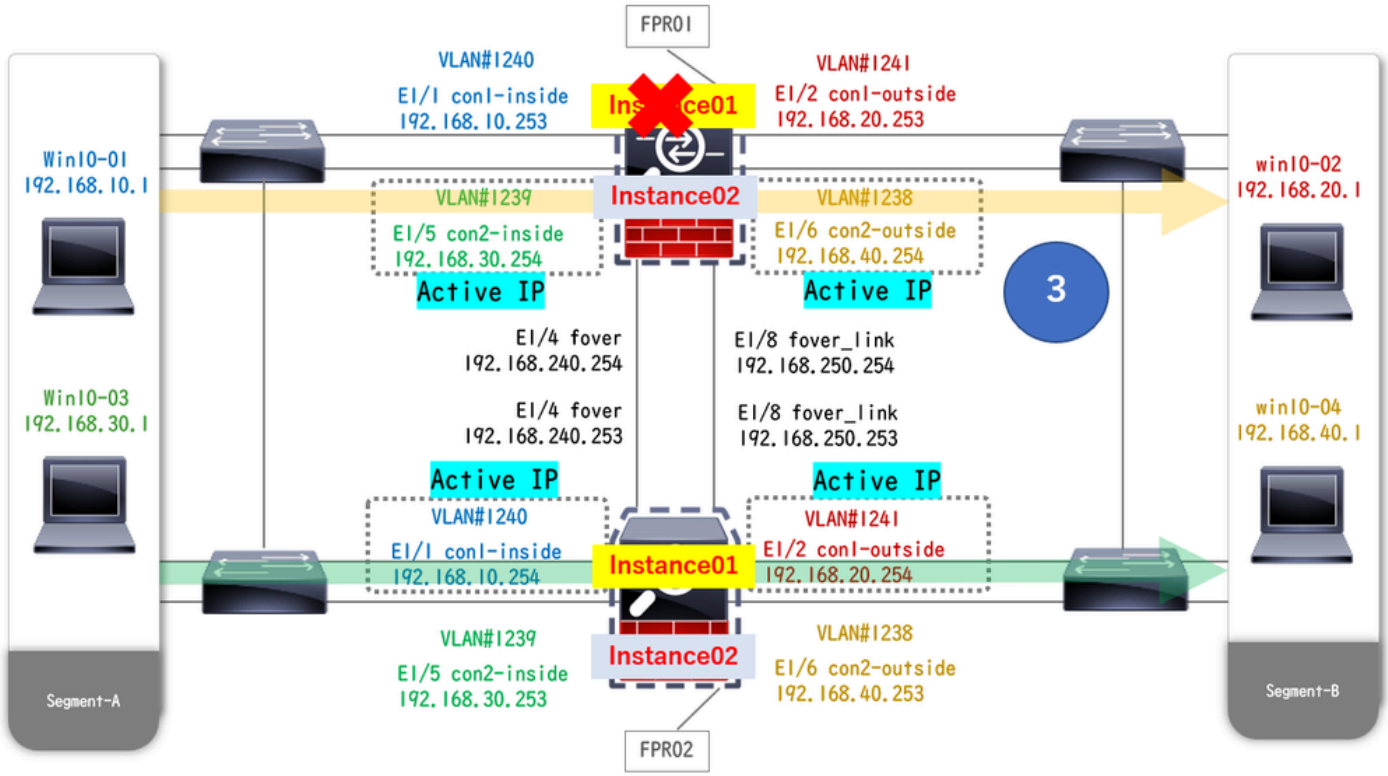
Bei einem Absturz auf FTD1_FTD01 (primäre Instanz01) wird das Failover von Instanz01 ausgelöst, und die Datenschnittstellen auf der Standby-Seite übernehmen die IP-/MAC-Adresse der ursprünglichen aktiven Schnittstelle, sodass der Datenverkehr (FTP-Verbindung in diesem Dokument) kontinuierlich von Firepower weitergeleitet wird.



Vor dem Absturz



Während des Absturzes



Failover wird ausgelöst

Schritt 1: Initiieren Sie eine FTP-Verbindung von Win10-01 zu Win10-02.

Schritt 2: Führen Sie einen show conn Befehl aus, um zu bestätigen, dass die FTP-Verbindung in beiden Instanzen hergestellt wurde.

<#root>

// Confirm the connection in Instance01 of FPR01 >

```
show conn
 TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm
show conn
 TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1
```

Schritt 3: Initiieren Sie eine FTP-Verbindung von Win10-03 zu Win10-04.

Schritt 4: Führen Sie einen **show conn** Befehl aus, um zu bestätigen, dass die FTP-Verbindung in beiden Instanzen hergestellt wurde.

<#root>

// Confirm the connection in Instance02 of FPR01 >

```
show conn
 TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm
show conn
 TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1
```

Schritt 5: Führen Sie einen Befehl connect ftd FTD01 und einen system support diagnostic-cli Befehl aus, um die ASA CLI zu starten. Führen Sie enable und **crashinfo force watchdog** Befehl aus, um den Absturz von Instance01 in der primären/aktiven Einheit zu erzwingen.

<#root>

Firepower-module1>

```
connect ftd FTD01
 >
system support diagnostic-cli
 FTD01>
enable
 Password: FTD01# FTD01#
crashinfo force watchdog
 reboot. Do you wish to proceed? [confirm]:
```

Schritt 6: Failover tritt in Instance01 auf, und die FTP-Verbindung wird nicht unterbrochen. Ausführen show failover und show conn Befehl zur Bestätigung des Status von Instance01 in FPR02.

<#root>

>

show failover

**Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) ..... This host:
Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside (**

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1

Schritt 7. Der Absturz in Instance01 hatte keine Auswirkungen auf Instance02. Führen Sie show failover und show conn Befehl aus, um den Status von Instance02 zu bestätigen.

<#root>

>

show failover

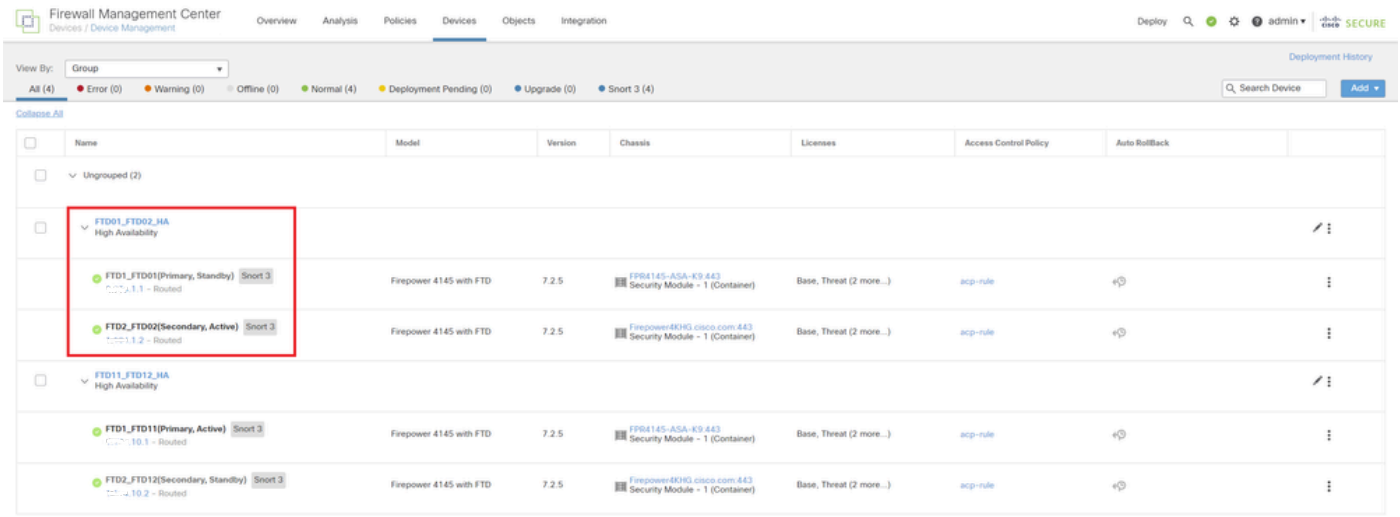
**Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host:
Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1**

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1

Schritt 8: Navigieren Sie zu **Geräte** > **Alle** auf FMC. Bestätigen Sie den HA-Status.

- **FTD1_FTD01 : Primär, Standby**
- **FTD2_FTD02 : Sekundär, Aktiv**

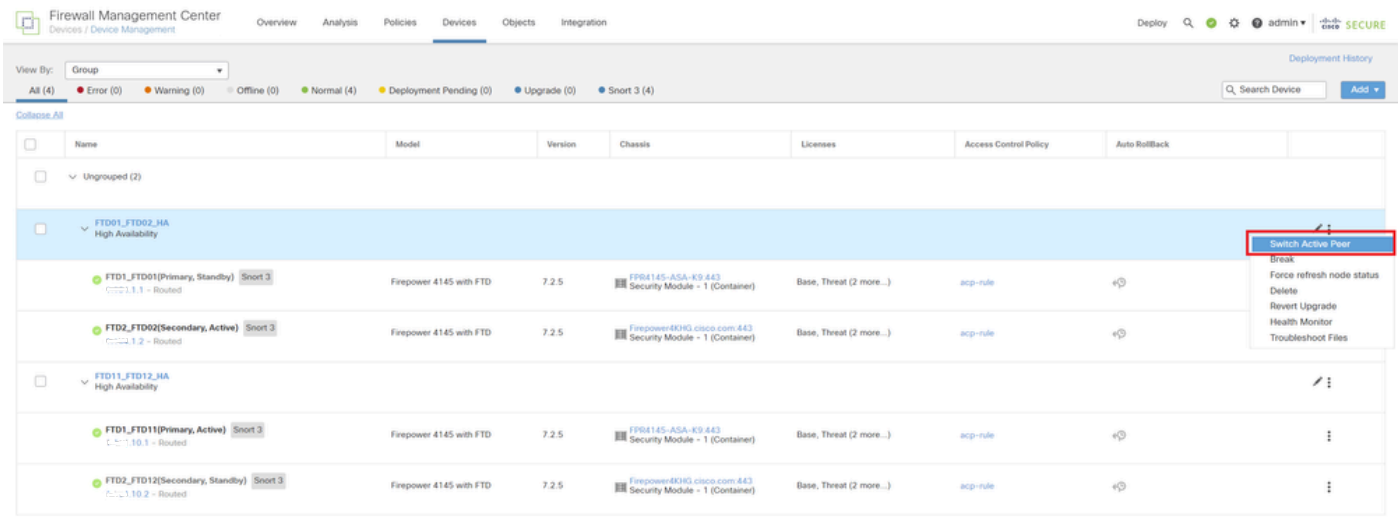


HA-Status bestätigen

Schritt 9. (Optional)Nachdem Instance01 von FPR01 auf normal zurückgesetzt wurde, können Sie den HA-Status manuell ändern. Dies kann

entweder über die FMC-GUI oder die FRP-CLI erfolgen.

Navigieren Sie auf FMC zu **Geräte** > **Alle**. Klicken Sie auf **Switch Active Peer** (**Switch Active Peer**), um den HA-Status für **FTD01_FTD02_HA zu ändern**.



HA-Status des Switches

Führen Sie in der Firepower-CLI den Befehl "Run connect ftd FTD01" und system support diagnostic-cli "command" aus, um die ASA-CLI aufzurufen. Führen Sie enable und **failover active** Befehl aus, um die hohe Verfügbarkeit für FTD01_FTD02_HA zu wechseln.

```
<#root>

Firepower-module1>

connect ftd FTD01

 >

system support diagnostic-cli

 Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of availab

enable

 firepower#

failover active
```

Fehlerbehebung

Um den Failover-Status zu überprüfen, führen Sie **show failover** und **show failover history** Befehl aus.

```
<#root>

>

show failover
```

```
 Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host:
Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1

>

show failover history

 ========================================================================== From State To State Reason =
```

Führen Sie den Befehl debug fover <option> aus, um das Fehlerbehebungsprotokoll für Failover zu aktivieren.

```
<#root>

>

debug fover

 auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution c
```

Referenz

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance_solution.html

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497

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.