Austausch defekter Einheiten bei hochverfügbarer Abwehr von Bedrohungen durch sichere Firewall

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie ein fehlerhaftes Secure Firewall Threat Defense-Modul ersetzen, das Teil einer HA-Konfiguration (High Availability) ist.

Voraussetzungen

Anforderungen

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

- Cisco Secure Firewall Management Center (FMC)
- Cisco FirePOWER Extensible Operating System (FXOS)
- Cisco Secure Firewall Threat Defense (FTD)

Verwendete Komponenten

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

- FirePOWER 4110 mit FXOS v2.12(0.498)
- Logisches Gerät führt Cisco Secure Firewall v7.2.5 aus
- Secure Firewall Management Center 2600 läuft v7.4
- Kenntnisse über Secure Copy Protocol (SCP)

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

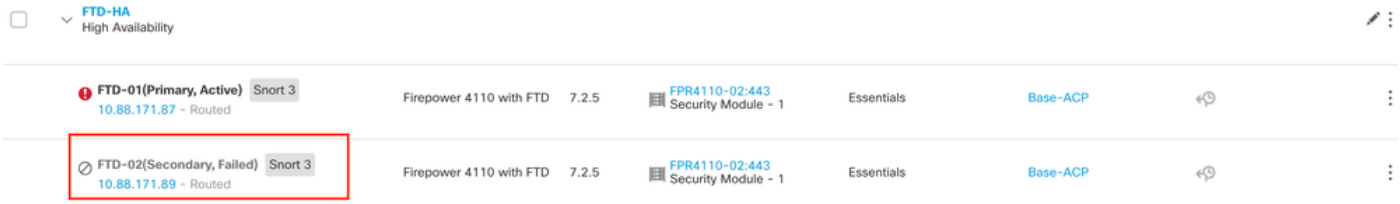
Dieses Verfahren wird auf folgenden Appliances unterstützt:

- Cisco Secure Firewall Appliances der Serie 1000
- Cisco Secure Firewall Appliances der Serie 2100
- Cisco Secure Firewall Appliances der Serie 3100
- Cisco Secure Firewall Appliances der Serie 4100
- Cisco Secure Firewall Appliances der Serie 4200
- Cisco Secure Firewall der Serie 9300
- Cisco Secure Firewall Threat Defense für VMware

Vorbereitungen

Für dieses Dokument muss das neue Gerät mit den gleichen FXOS- und FTD-Versionen konfiguriert sein.

Identifizieren der fehlerhaften Einheit

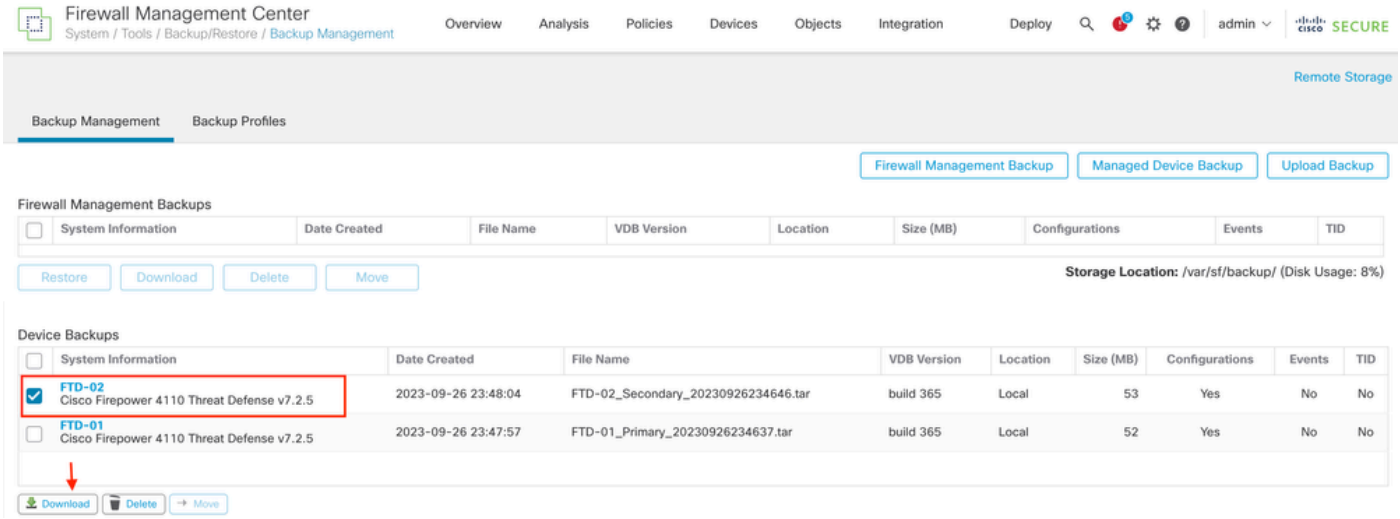


In diesem Szenario befindet sich die Sekundäreinheit (FTD-02) in einem fehlerhaften Zustand.

Ersetzen Sie eine fehlerhafte Einheit durch ein Backup.

Mit diesem Verfahren können Sie die primäre oder sekundäre Einheit ersetzen. Bei diesem Leitfaden wird davon ausgegangen, dass Sie über eine Sicherungskopie der fehlerhaften Einheit verfügen, die Sie ersetzen möchten.

Schritt 1: Laden Sie die Sicherungsdatei von FMC herunter. Navigieren Sie zu System > Tools > Restore > Device Backups, und wählen Sie die richtige Sicherung aus. Klicken Sie auf Herunterladen:



Schritt 2: Laden Sie die FTD-Sicherung in das Verzeichnis /var/sf/backup/ der neuen FTD hoch:

2.1 Laden Sie vom Test-PC (SCP-Client) die Sicherungsdatei in das FTD im Verzeichnis /var/tmp/ hoch:

```
@test-pc ~ % scp FTD-02_Secondary_20230926234646.tar cisco@10.88.243.90:/var/tmp/
```

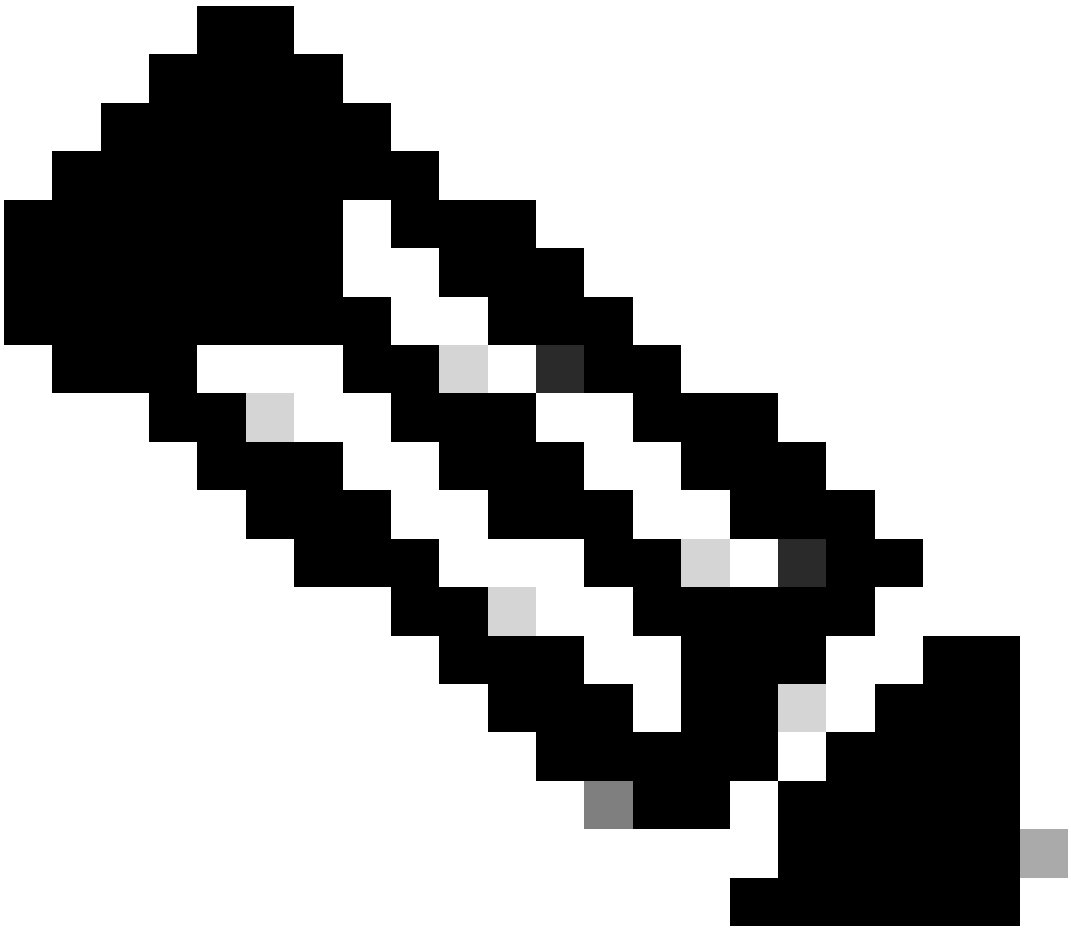
2.2 Verschieben Sie im FTD CLI Expert-Modus die Sicherungsdatei von /var/tmp/ nach /var/sf/backup/:

```
root@firepower:/var/tmp# mv FTD-02_Secondary_20230926234646.tar /var/sf/backup/
```

Schritt 3: Stellen Sie die FTD-02-Sicherung wieder her, indem Sie den nächsten Befehl aus dem Klischmodus anwenden:

```
>restore remote-manager-backup FTD-02_Secondary_20230926234646.tar

Device model from backup :: Cisco Firepower 4110 Threat Defense
This Device Model  :: Cisco Firepower 4110 Threat Defense
************************************************
Backup Details
************************************************
Model = Cisco Firepower 4110 Threat Defense
Software Version = 7.2.5
Serial = FLM22500791
Hostname = firepower
Device Name = FTD-02_Secondary
IP Address = 10.88.171.89
Role = SECONDARY
VDB Version = 365
SRU Version =
FXOS Version = 2.12(0.498)
Manager IP(s) = 10.88.243.90
Backup Date = 2023-09-26 23:46:46
Backup Filename = FTD-02_Secondary_20230926234646.tar
************************************************

******************** Caution ***************************
Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches versions from backup manifest be
Restore operation will overwrite all configurations on this device with configurations in backup.
If this restoration is being performed on an RMA device then ensure old device is removed from network
************************************************************
Are you sure you want to continue (Y/N)Y
Restoring device . . . . . .
Added table audit_log with table_id 1
Added table health_alarm_syslog with table_id 2
Added table dce_event with table_id 3
Added table application with table_id 4
Added table rna_scan_results_tableview with table_id 5
Added table rna_event with table_id 6
Added table ioc_state with table_id 7
Added table third_party_vulns with table_id 8
Added table user_ioc_state with table_id 9
Added table rna_client_app with table_id 10
Added table rna_attribute with table_id 11
Added table captured_file with table_id 12
Added table rna_ip_host with table_id 13
Added table flow_chunk with table_id 14
Added table rua_event with table_id 15
Added table wl_dce_event with table_id 16
Added table user_identities with table_id 17
Added table whitelist_violations with table_id 18
Added table remediation_status with table_id 19
Added table syslog_event with table_id 20
Added table rna_service with table_id 21
```

```
Added table rna_vuln with table_id 22
Added table SRU_import_log with table_id 23
Added table current_users with table_id 24

Broadcast message from root@firepower (Wed Sep 27 15:50:12 2023):

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

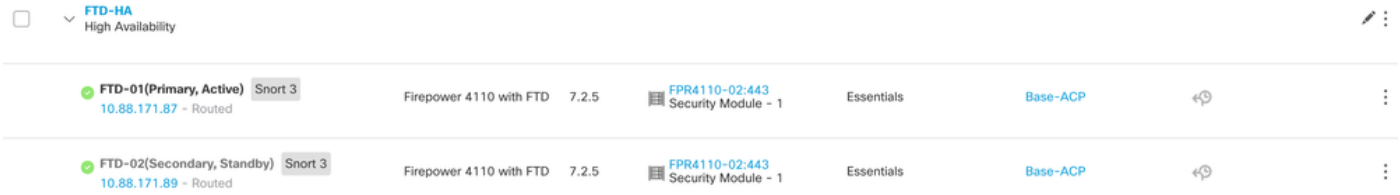


> Anmerkung: Wenn die Wiederherstellung abgeschlossen ist, meldet das Gerät Sie von der CLI ab, startet neu und stellt automatisch eine Verbindung mit dem FMC her. Zu diesem Zeitpunkt erscheint das Gerät veraltet.

Schritt 4: HA-Synchronisierung fortsetzen. Geben Sie über die FTD-CLI configure high-Availability Resume ein:

```
>configure high-availability resume
```

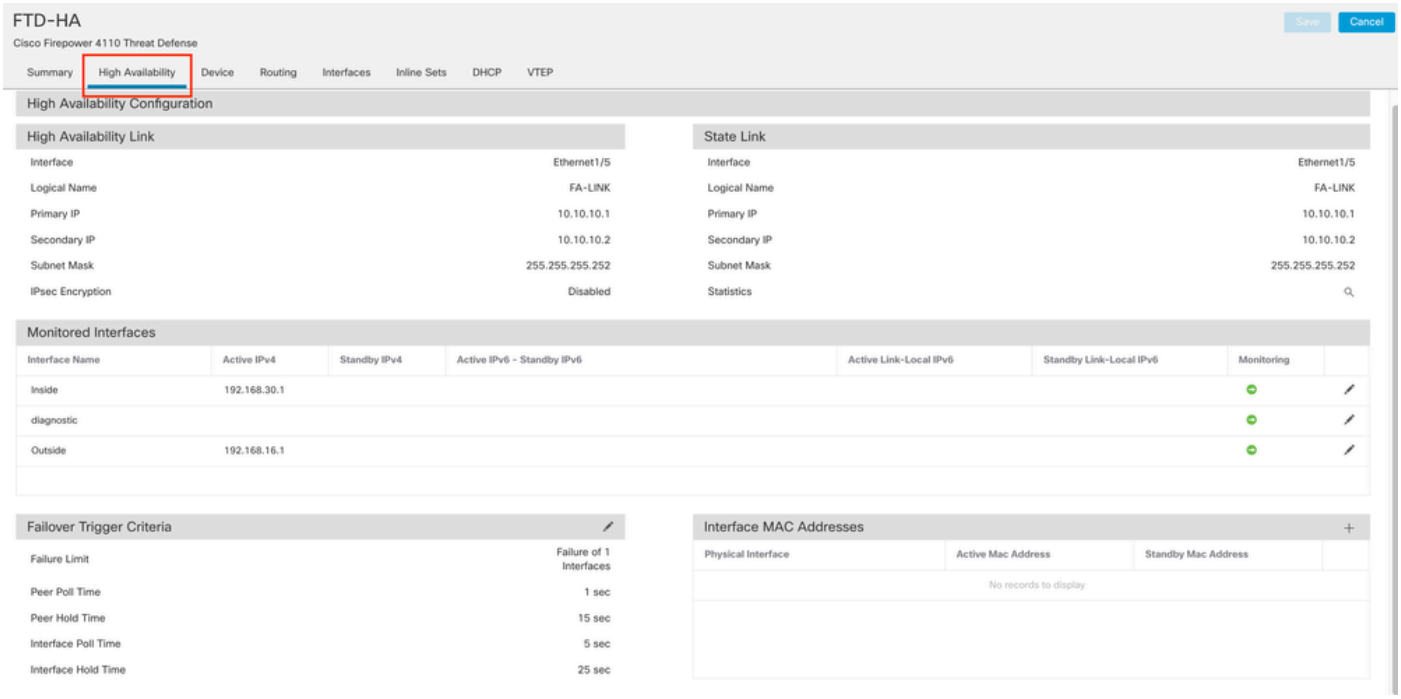
Die FTD-Hochverfügbarkeitskonfiguration ist jetzt abgeschlossen:



Ersetzen Sie eine fehlerhafte Einheit ohne Sicherung.

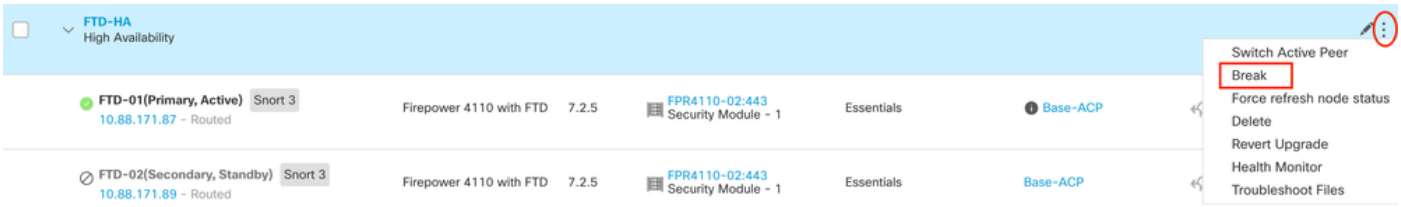
Wenn Sie keine Sicherung des ausgefallenen Geräts haben, können Sie mit diesem Leitfaden fortfahren. Sie können entweder die primäre oder sekundäre Einheit ersetzen, tDer Prozess hängt davon ab, ob es sich um ein primäres oder ein sekundäres Gerät handelt. Alle in dieser Anleitung beschriebenen Schritte dienen der Wiederherstellung einer fehlerhaften Sekundäreinheit. Wenn Sie eine fehlerhafte primäre Einheit wiederherstellen möchten, konfigurieren Sie in Schritt 5 die hohe Verfügbarkeit. Verwenden Sie dabei die vorhandene sekundäre/aktive Einheit als primäres Gerät und das Ersatzgerät als sekundäres/Standby-Gerät bei der Registrierung.

Schritt 1: Erstellen Sie einen Screenshot (Backup) der Hochverfügbarkeitskonfiguration, indem Sie zu Device > Device Management (Gerät > Gerätemanagement) navigieren. Bearbeiten Sie das richtige FTD HA-Paar (klicken Sie auf das Bleistiftsymbol), und klicken Sie dann auf die Option Hohe Verfügbarkeit:

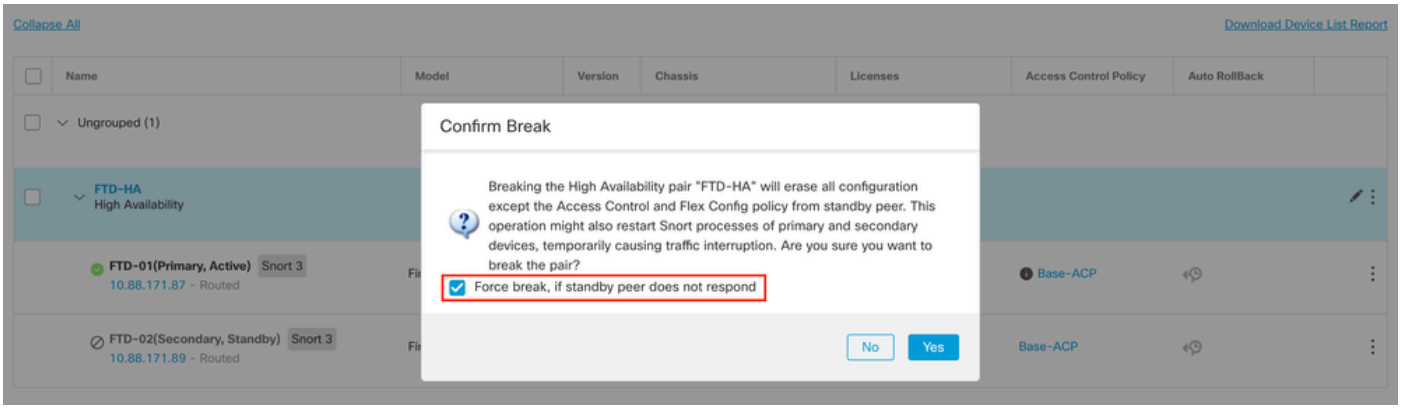


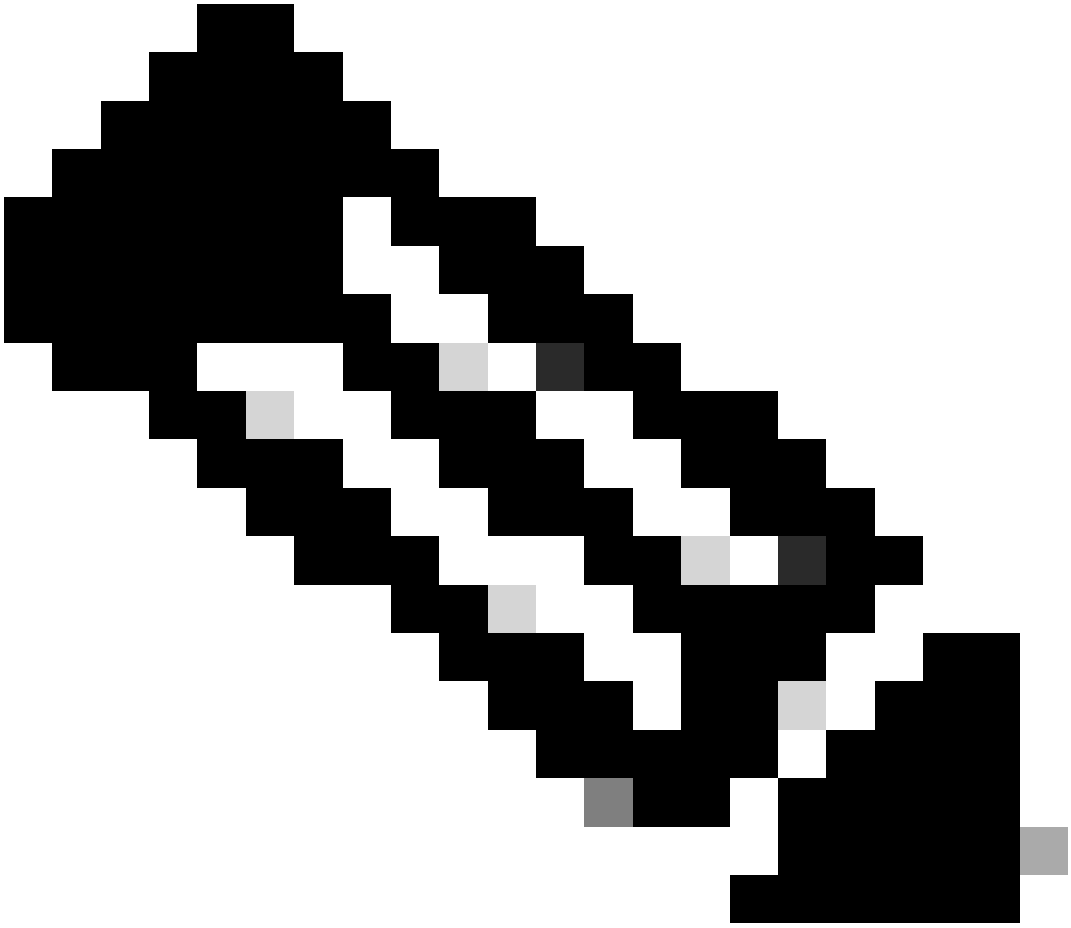
Schritt 2: Brechen Sie die HA.

2.1 Navigieren Sie zu Geräte > Geräteverwaltung, und klicken Sie dann auf das Menü mit den drei Punkten in der oberen rechten Ecke. Klicken Sie dann auf Break option:



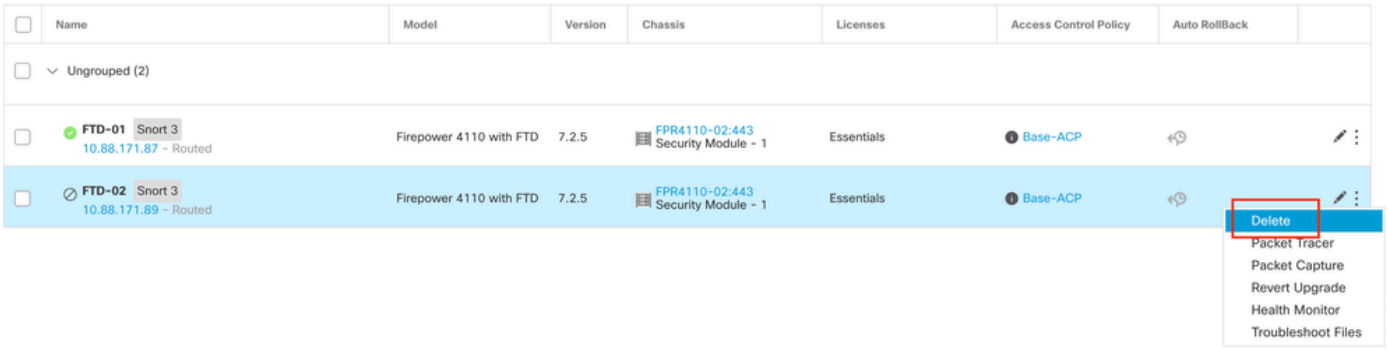
2.2. Wählen Sie die Option Unterbrechung erzwingen, wenn der Standby-Peer nicht reagiert:





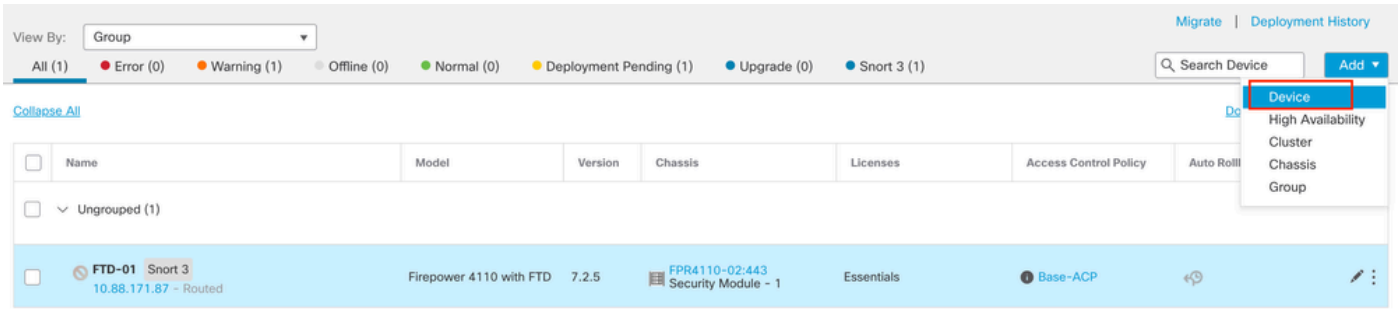
Anmerkung: Da die Einheit nicht reagiert, müssen Sie die Unterbrechung der HA erzwingen. Wenn Sie ein Hochverfügbarkeitspaar unterbrechen, behält das aktive Gerät die volle bereitgestellte Funktionalität bei. Das Standby-Gerät verliert seine Failover- und Schnittstellenkonfigurationen und wird zu einem eigenständigen Gerät.

Schritt 3: Löschen Sie fehlerhafte FTD. Identifizieren Sie die FTD, die ersetzt werden soll, und klicken Sie dann auf das Drei-Punkte-Menü. Klicken Sie auf Löschen:



Schritt 4: Fügen Sie den neuen FTD hinzu.

4.1. Navigieren Sie zu Geräte > Geräteverwaltung > Hinzufügen, und klicken Sie dann auf Gerät:



4.2. Wählen Sie die Bereitstellungsmethode, in diesem Fall Registrierungsschlüssel, konfigurieren Sie Host, Anzeigename, Registrierungsschlüssel. Konfigurieren Sie eine Zugriffssteuerungsrichtlinie, und klicken Sie auf Registrieren.

Add Device

Select the Provisioning Method:

(•) Registration Key ( ) Serial Number

[ ] CDO Managed Device

Host:†

10.88.171.89

Display Name:

FTD-02

Registration Key:*

••••••••

Group:

None

Access Control Policy:*

Base-ACP

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):

Select a recommended Tier

[ ] Carrier
[ ] Malware Defense
[ ] IPS
[ ] URL

Advanced

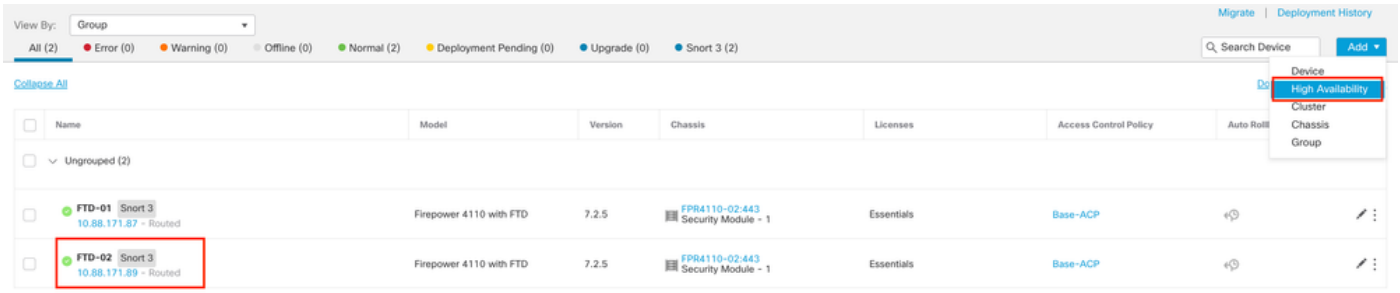
Unique NAT ID:†

[ ] Transfer Packets

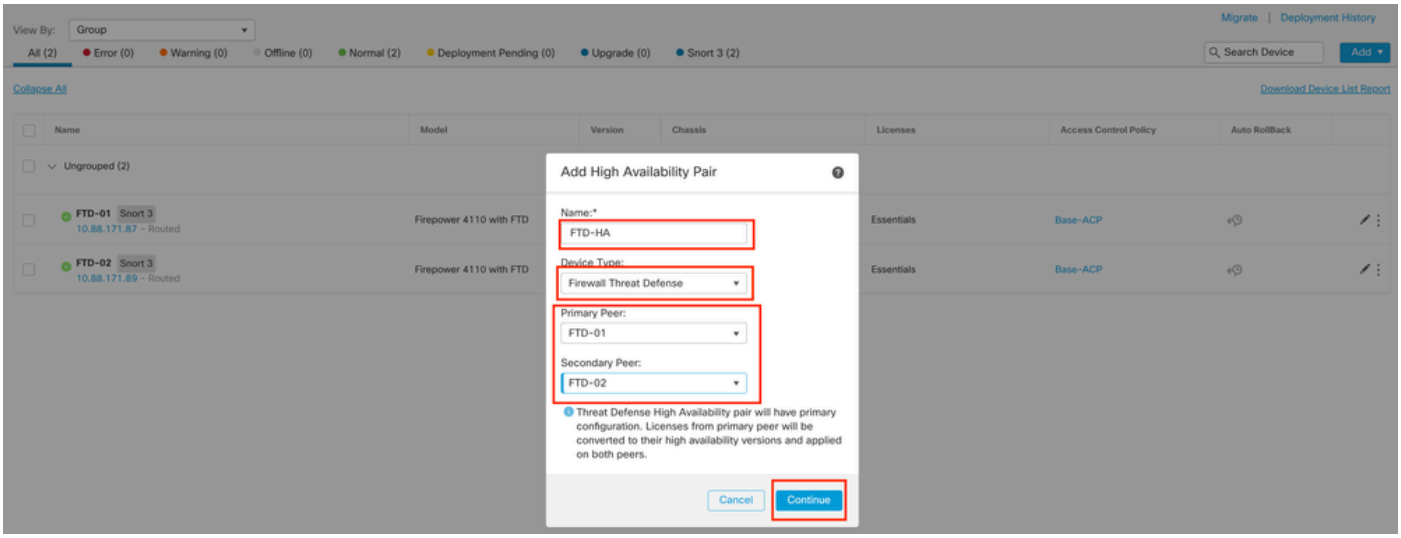
Cancel Register

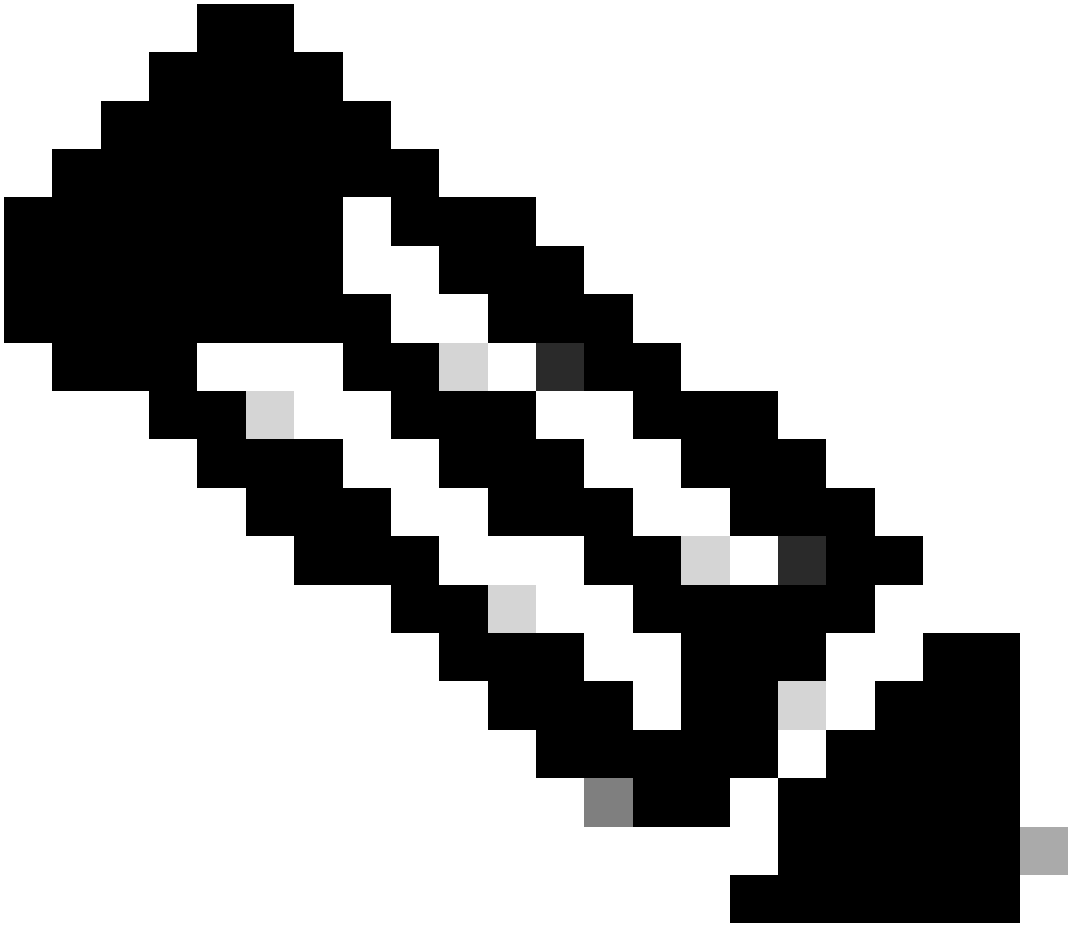
Schritt 5: Erstellen Sie die hohe Verfügbarkeit.

5.1 Navigieren Sie zu Devices > Device Management > Add, und klicken Sie auf High Availability (Hochverfügbarkeitsoption).



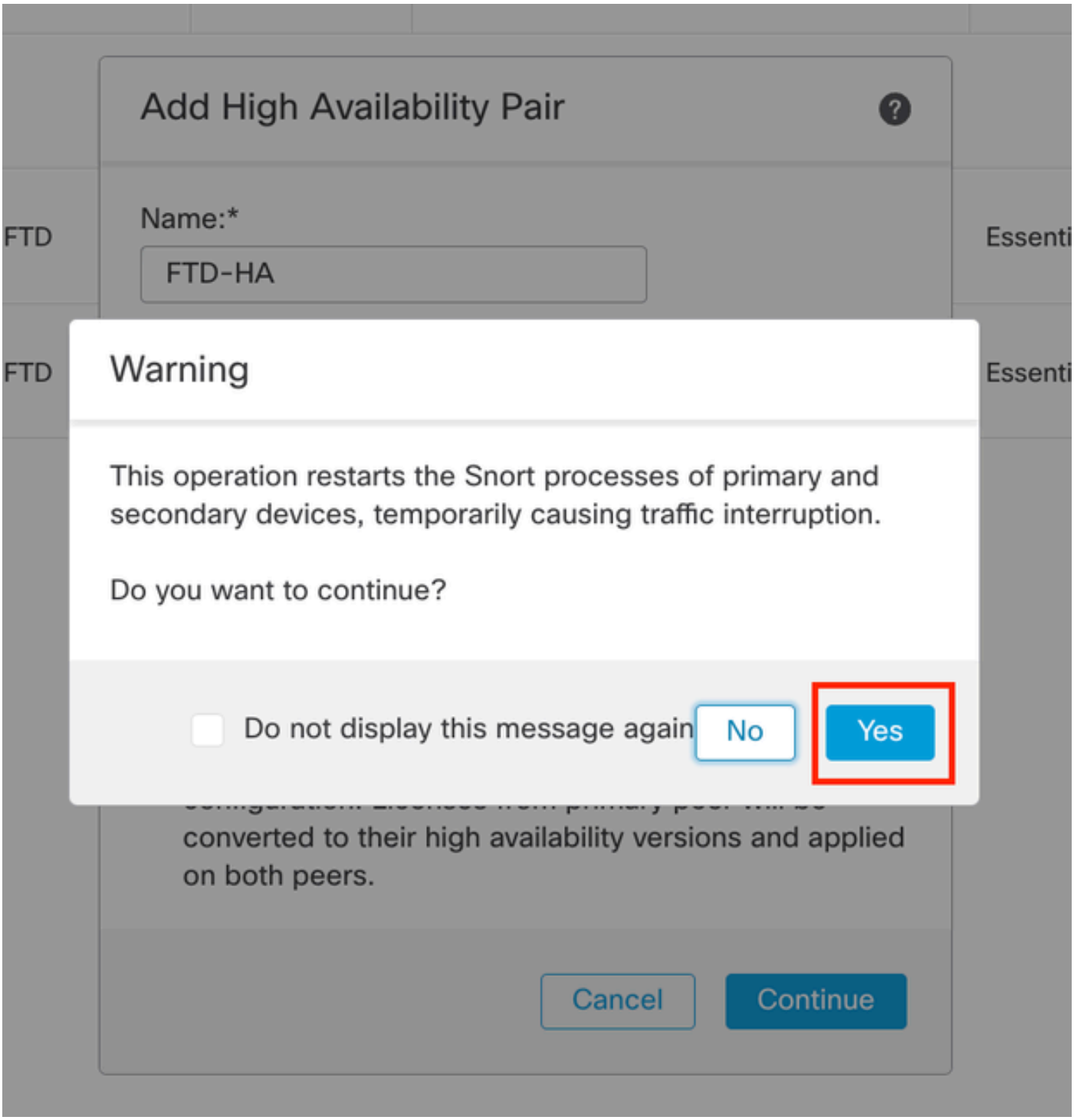
5.2. Konfigurieren Sie das Paar "Hohe Verfügbarkeit hinzufügen". Konfigurieren Sie den Namen, den Gerätetyp, wählen Sie FTD-01 als primären Peer und FTD-02 als sekundären Peer aus, und klicken Sie dann auf Weiter.

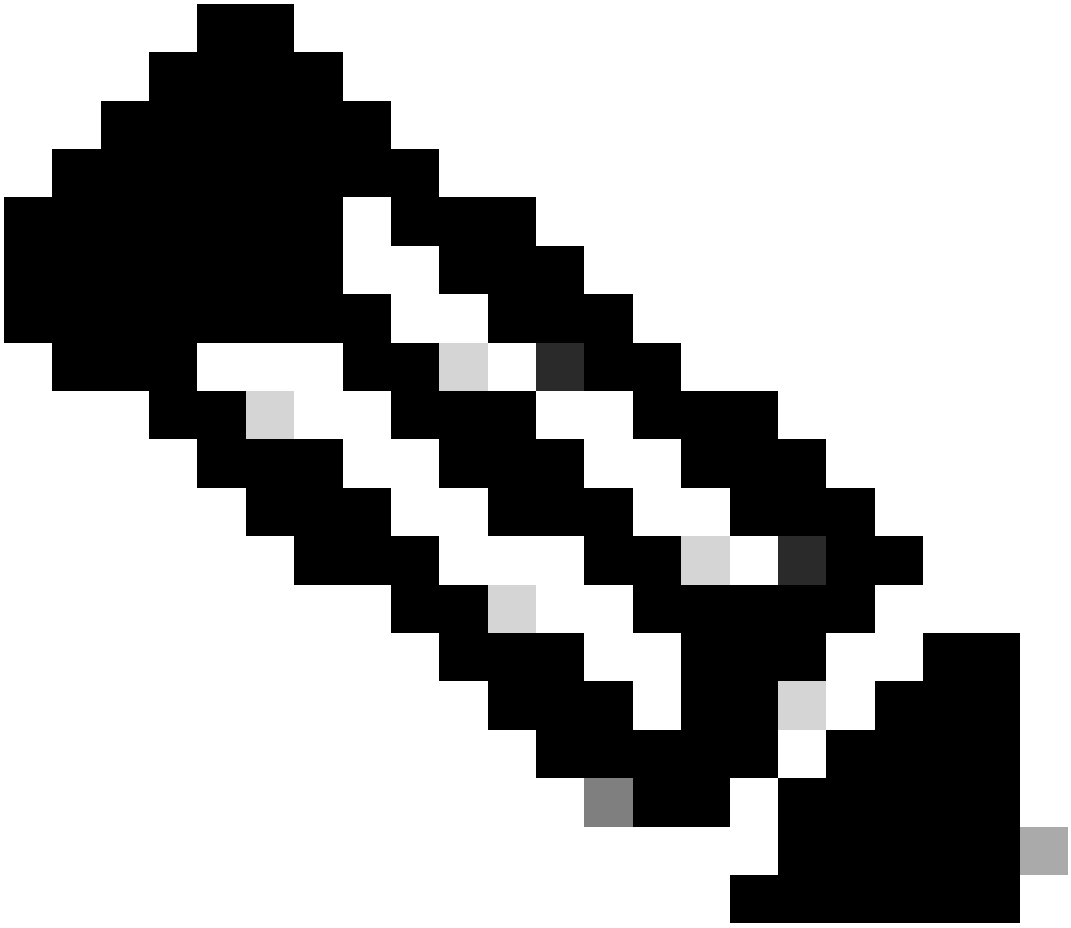




Anmerkung: Denken Sie daran, die primäre Einheit als Gerät auszuwählen, für das die Konfiguration noch verfügbar ist, in diesem Fall FTD-01.

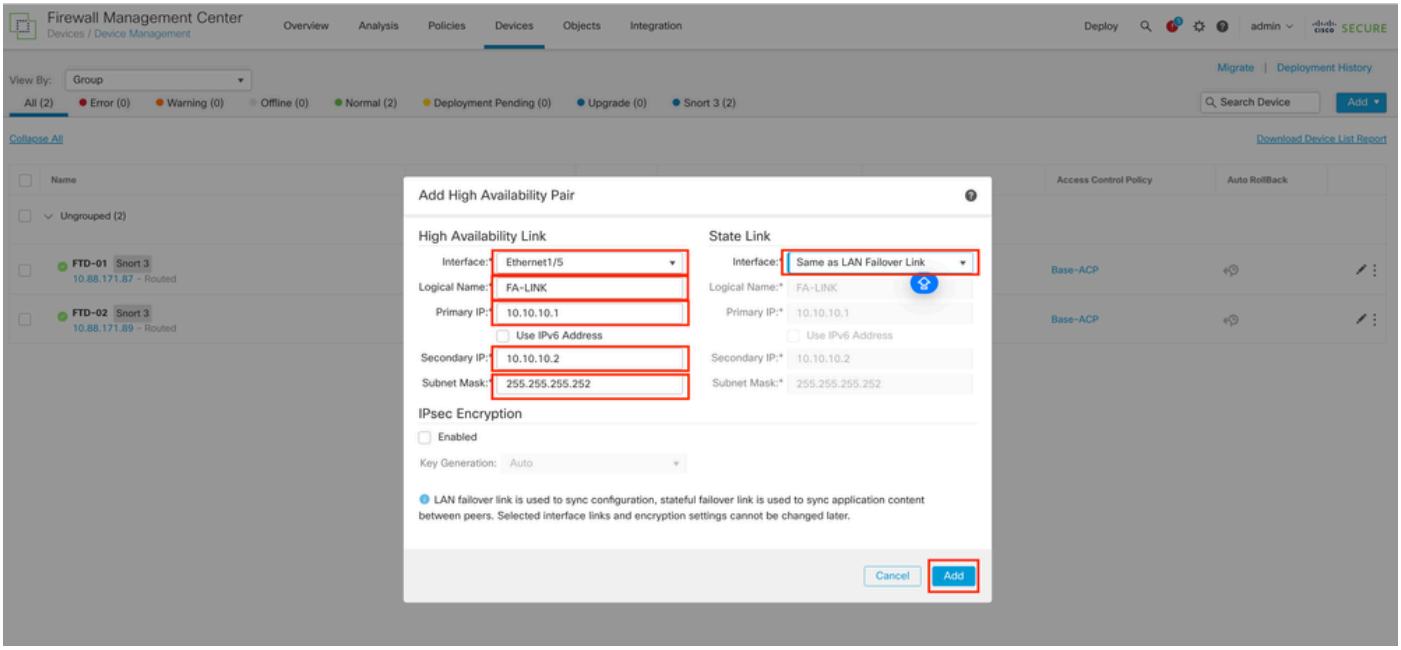
5.3. Bestätigen Sie die HA-Erstellung, und klicken Sie dann auf Ja.


Add High Availability Pair
Name:*
FTD-HA
FTD
Essenti
FTD
Essenti
Warning
This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption.
Do you want to continue?
Do not display this message again
No
Yes
converted to their high availability versions and applied on both peers.
Cancel
Continue

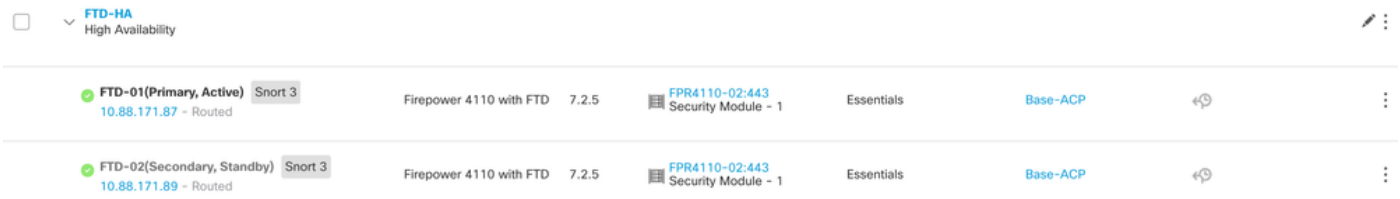


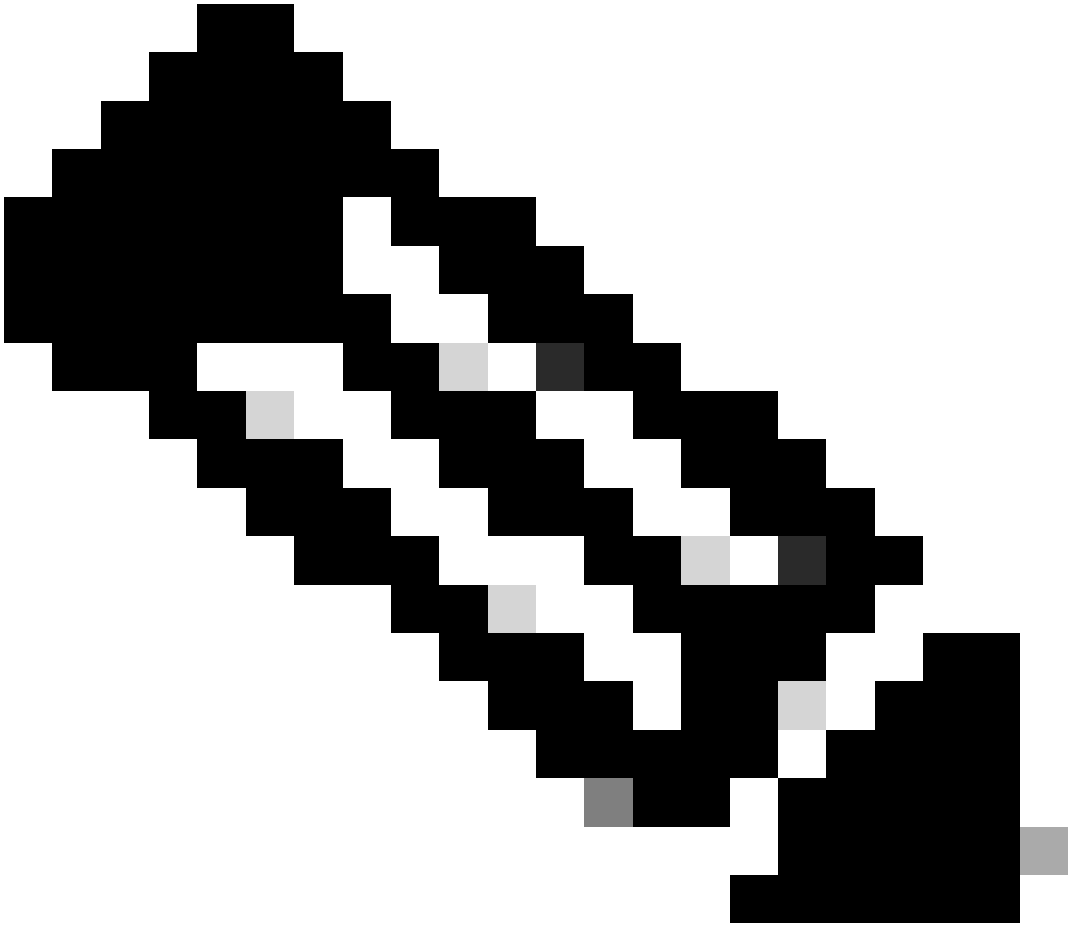
Anmerkung: Bei der Konfiguration der Hochverfügbarkeit wird die Snort-Engine beider Einheiten neu gestartet, was zu einer Unterbrechung des Datenverkehrs führen kann.

5.4. Konfigurieren Sie die Hochverfügbarkeitsparameter in Schritt 2, und klicken Sie dann auf die Option Hinzufügen:



6. Die FTD-Hochverfügbarkeitskonfiguration ist jetzt abgeschlossen:





Anmerkung: Wenn Sie keine virtuellen MAC-Adressen konfigurieren, müssen Sie die ARP-Tabellen der verbundenen Router löschen, um den Datenverkehrsfluss beim Austausch der primären Einheit wiederherzustellen. Weitere Informationen finden Sie unter MAC- und IP-Adressen in Hochverfügbarkeit.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

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.