

Vervang de Faulty Unit in Secure Firewall Threat Defence of High Availability

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Voordat u begint](#)

[Identificeer de defecte eenheid](#)

[Vervang een defecte eenheid door een back-up](#)

[Een defecte eenheid zonder back-up vervangen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een defecte Secure Firewall Threat Defense-module kunt vervangen die deel uitmaakt van een High Availability (HA)-installatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower eXtensible Operating System (FXOS)
- Cisco Secure Firewall Threat Defence (FTD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower 4110 draait op FXOS v2.12(0.498)
- Logisch apparaat voert Cisco Secure Firewall v7.2.5 uit
- Secure Firewall Management Center 2600 versie 7.4
- SCP-kennis (Secure Copy Protocol)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie







Deze procedure wordt op toestellen ondersteund:

- Cisco Secure Firewall 1000 Series-apparaten
- Cisco Secure Firewall 2100 Series-apparaten
- Cisco Secure Firewall 3100 Series-apparaten
- Cisco Secure Firewall 4100 Series-apparaten
- Cisco Secure Firewall 4200 Series-apparaten
- Cisco Secure Firewall 9300-apparaat
- Cisco Secure Firewall Threat Defense voor VMWare

Voordat u begint

Dit document vereist dat u de nieuwe eenheid hebt geconfigureerd met dezelfde FXOS- en FTD-versies.

Identificeer de defecte eenheid

FTD-HA High Availability							
 FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	 FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		
 FTD-02(Secondary, Failed) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	 FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		

In dit scenario is de secundaire eenheid (FTD-02) in een mislukte staat.

Vervang een defecte eenheid door een back-up

U kunt deze procedure gebruiken om de primaire of de secundaire eenheid te vervangen. In deze handleiding wordt ervan uitgegaan dat u een back-up hebt van de defecte eenheid die u gaat vervangen.

Stap 1. Download het reservebestand van FMC. Ga naar **Systeem > Gereedschappen > Terugzetten > Apparaatback-ups** en selecteer de juiste back-up. Klik op **Downloaden**:

The screenshot shows the Fire Management Center (FMC) interface. The breadcrumb navigation is **System / Tools / Backup/Restore / Backup Management**. The main navigation includes **Overview**, **Analysis**, **Policies**, **Devices**, **Objects**, **Integration**, **Deploy**, and **admin**. The **Backup Management** section is active, showing **Backup Management** and **Backup Profiles**. There are buttons for **Firewall Management Backup**, **Managed Device Backup**, and **Upload Backup**. Below this, the **Firewall Management Backups** section is visible, with a table of backups and buttons for **Restore**, **Download**, **Delete**, and **Move**. The **Storage Location** is **/var/sf/backup/ (Disk Usage: 8%)**. The **Device Backups** section shows a table with columns for **System Information**, **Date Created**, **File Name**, **VDB Version**, **Location**, **Size (MB)**, **Configurations**, **Events**, and **TID**. The table contains two entries: **FTD-02** (Cisco Firepower 4110 Threat Defense v7.2.5) and **FTD-01** (Cisco Firepower 4110 Threat Defense v7.2.5). The **FTD-02** entry is selected, and a red arrow points to the **Download** button below it.

System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
<input checked="" type="checkbox"/> FTD-02 Cisco Firepower 4110 Threat Defense v7.2.5	2023-09-26 23:48:04	FTD-02_Secondary_20230926234646.tar	build 365	Local	53	Yes	No	No
<input type="checkbox"/> FTD-01 Cisco Firepower 4110 Threat Defense v7.2.5	2023-09-26 23:47:57	FTD-01_Primary_20230926234637.tar	build 365	Local	52	Yes	No	No

Stap 2. Upload FTD back-up naar de **/var/sf/backup/** directory van de nieuwe FTD:

2.1 Upload vanuit de test-pc (SCP client) het back-upbestand naar het FTD onder de map **/var/tmp/**:

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

2.2 Verplaats het back-upbestand van FTD CLI expert mode van **/var/tmp/** naar **/var/sf/backup/**:

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

Stap 3. Zet de FTD-02 back-up terug door de volgende opdracht uit de clish-modus toe te passen:

>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!



Opmerking: Wanneer het herstel is voltooid, logt het apparaat u uit de CLI, start het opnieuw op en maakt het automatisch verbinding met het FMC. Op dit moment zal het apparaat verouderd lijken.

Stap 4. Hervat de HA-synchronisatie. Voer vanuit de FTD CLI de configuratie van een cv met hoge beschikbaarheid in:

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

De configuratie van de hoge beschikbaarheid van FTD is nu voltooid:

Device Name	Status	Model	Version	Security Module	Configuration	Actions
FTD-01(Primary, Active)	Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials Base-ACP	
FTD-02(Secondary, Standby)	Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials Base-ACP	

Een defecte eenheid zonder back-up vervangen

Als u geen back-up hebt van het defecte apparaat, kunt u deze handleiding gebruiken. U kunt de primaire of de secundaire eenheid vervangen, of het proces varieert afhankelijk van of het apparaat primair of secundair is. Alle stappen die in deze handleiding worden beschreven, zijn om een defecte secundaire eenheid te herstellen. Als u een defecte primaire eenheid wilt herstellen, moet u in Stap 5 hoge beschikbaarheid configureren met behulp van de bestaande secundaire/actieve eenheid als het primaire apparaat en het vervangende apparaat als het secundaire/stand-by apparaat tijdens de registratie.

Stap 1. Maak een screenshot (back-up) van de configuratie met hoge beschikbaarheid door te navigeren naar Apparaat > Apparaatbeheer. Bewerk het juiste FTD HA-paar (klik op het potloodpictogram) en klik vervolgens op de optie Hoge beschikbaarheid:

FTD-HA
Cisco Firepower 4110 Threat Defense

Summary **High Availability** Device Routing Interfaces Inline Sets DHCP VTEP

High Availability Configuration

High Availability Link		State Link	
Interface	Ethernet1/5	Interface	Ethernet1/5
Logical Name	FA-LINK	Logical Name	FA-LINK
Primary IP	10.10.10.1	Primary IP	10.10.10.1
Secondary IP	10.10.10.2	Secondary IP	10.10.10.2
Subnet Mask	255.255.255.252	Subnet Mask	255.255.255.252
IPsec Encryption	Disabled	Statistics	

Monitored Interfaces							
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	
Inside	192.168.30.1						
diagnostic							
Outside	192.168.16.1						

Failover Trigger Criteria	
Failure Limit	Failure of 1 Interfaces
Peer Poll Time	1 sec
Peer Hold Time	15 sec
Interface Poll Time	5 sec
Interface Hold Time	25 sec

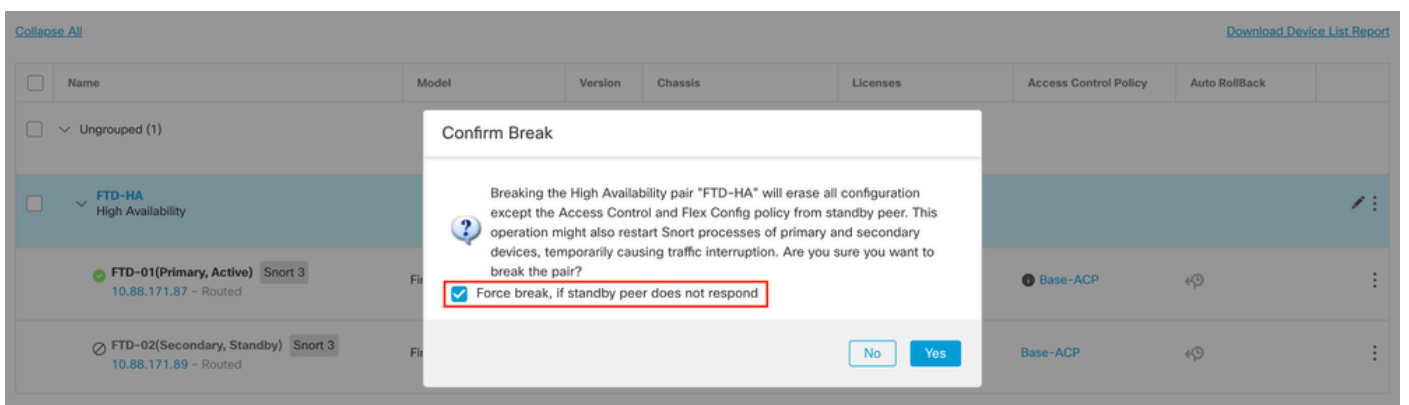
Interface MAC Addresses		
Physical Interface	Active Mac Address	Standby Mac Address
No records to display		

Stap 2. Breek de HA.

2.1 Navigeer naar Apparaten > Apparaatbeheer en klik vervolgens op het menu met drie punten in de rechterbovenhoek. Klik vervolgens op de optie Onderbreking:



2.2. Selecteer Force break als stand-by peer niet reageert optie:





Opmerking: Omdat de unit niet reageert, moet u de HA forceren. Wanneer u een high-Availability-paar breekt, behoudt het actieve apparaat de volledige geïmplementeerde functionaliteit. Het stand-by apparaat verliest zijn failover en interfaceconfiguraties en wordt een standalone apparaat.

Stap 3. Verwijdert defecte FTD. Identificeer het te vervangen FTD en klik vervolgens op het menu met drie punten. Klik op Verwijderen:

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
<input type="checkbox"/>	Ungrouped (2)							
<input type="checkbox"/>	FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		
<input type="checkbox"/>	FTD-02 Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		<ul style="list-style-type: none"> Delete Packet Tracer Packet Capture Revert Upgrade Health Monitor Troubleshoot Files

Stap 4. Voeg het nieuwe FTD toe.

4.1. Navigeer naar Apparaten > Apparaatbeheer > Toevoegen en klik vervolgens op Apparaat:

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Roll	
<input type="checkbox"/>	Ungrouped (1)							
<input type="checkbox"/>	FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP		<ul style="list-style-type: none"> Device High Availability Cluster Chassis Group

4.2. Selecteer de Provisioning Methode, in dit geval Registratiesleutel, configureer host, naam display, registratiesleutel. Configureer een toegangscontrolebeleid en klik op Registreren.

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

Stap 5. Maak de HA.

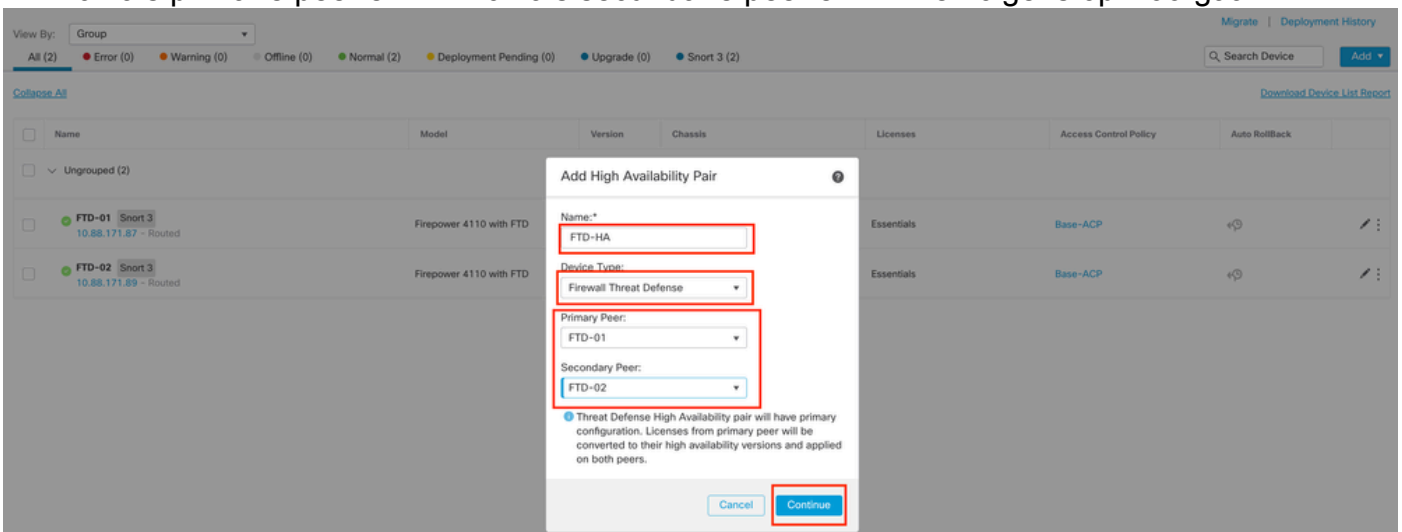
5.1 Navigeer naar Apparaten > Apparaatbeheer > Toevoegen en klik op High Availability.



The screenshot shows the Cisco ISE interface for device management. At the top, there are filters for 'View By: Group' and status indicators: All (2), Error (0), Warning (0), Offline (0), Normal (2), Deployment Pending (0), Upgrade (0), and Snort 3 (2). A search bar and an 'Add' button are visible. A dropdown menu is open from the 'Add' button, showing options: Device, High Availability (highlighted), Cluster, Chassis, and Group. Below the menu, a table lists devices. Two devices are highlighted with red boxes: 'FTD-01' (10.88.171.87) and 'FTD-02' (10.88.171.89), both with status 'Routed'.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Roll
FTD-01 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	EPR4110-02-443 Security Module - 1	Essentials	Base-ACP	
FTD-02 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	EPR4110-02-443 Security Module - 1	Essentials	Base-ACP	

5.2. Configureer het Add High Availability-paar. Configureer de naam, het apparaattype, selecteer FTD-01 als primaire peer en FTD-02 als secundaire peer en klik vervolgens op Doorgaan.



The screenshot shows the 'Add High Availability Pair' dialog box in the Cisco ISE interface. The dialog has the following fields and options:

- Name: FTD-HA
- Device Type: Firewall Threat Defense
- Primary Peer: FTD-01
- Secondary Peer: FTD-02

Below the fields, there is a note: "Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers." At the bottom of the dialog, there are 'Cancel' and 'Continue' buttons.



Opmerking: Vergeet niet om de primaire eenheid te selecteren als het apparaat dat nog steeds de configuratie heeft, in dit geval FTD-01.

5.3. Bevestig de HA-creatie en klik vervolgens op Ja.

Add High Availability Pair



Name:*

FTD-HA

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

Configuration changes from primary peer will be converted to their high availability versions and applied on both peers.

Cancel

Continue



Opmerking: Hoge beschikbaarheid configureren start de snormotor van beide eenheden opnieuw en dit kan verkeersonderbreking veroorzaken.

5.4. Configureer de High-Availability-parameters die zijn uitgevoerd in stap 2 en klik vervolgens op de Add-optie:

Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (0) Upgrade (0) Snort 3 (2)

Migrate | Deployment History

Search Device Add

Download Device List Report

Collaps All

Name

Ungrouped (2)

FTD-01 Snort 3
10.88.171.87 - Routed

FTD-02 Snort 3
10.88.171.89 - Routed

Access Control Policy Auto RollBack

Base-ACP

Base-ACP

Add High Availability Pair

High Availability Link	State Link
Interface: Ethernet1/5	Interface: Same as LAN Failover Link
Logical Name: FA-LINK	Logical Name: FA-LINK
Primary IP: 10.10.10.1	Primary IP: 10.10.10.1
<input type="checkbox"/> Use IPv6 Address	<input type="checkbox"/> Use IPv6 Address
Secondary IP: 10.10.10.2	Secondary IP: 10.10.10.2
Subnet Mask: 255.255.255.252	Subnet Mask: 255.255.255.252

IPsec Encryption

Enabled

Key Generation: Auto

LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.

Cancel Add

6. De configuratie van de hoge beschikbaarheid van de FTD is nu voltooid:

FTD-HA
High Availability

FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD 7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	⏪	⋮
FTD-02(Secondary, Standby) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD 7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	⏪	⋮



Opmerking: Als u geen virtuele MAC-adressen configureert, moet u de ARP-tabellen op verbonden routers wissen om de verkeersstroom te herstellen in het geval van vervanging van de primaire eenheid. Zie [MAC-adressen en IP-adressen in hoge beschikbaarheid voor](#) meer informatie.

Gerelateerde informatie

- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.