# FTD-Hochverfügbarkeit mit FDM konfigurieren

## Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Netzwerktopologie
Konfigurieren
Konfigurieren der primären Einheit für hohe Verfügbarkeit
Konfigurieren der Sekundäreinheit für hohe Verfügbarkeit
Überprüfung

### Einleitung

Dieses Dokument beschreibt die Einrichtung eines Aktiv/Standby-Hochverfügbarkeitspaars (HA) mit lokal verwaltetem Secure Firewall Threat Defense (FTD).

### Voraussetzungen

#### Anforderungen

Es wird empfohlen, über Kenntnisse in den folgenden Themen zu verfügen:

• Erstkonfiguration von Cisco Secure Firewall Threat Defense über die Benutzeroberfläche und/oder Shell.

#### Verwendete Komponenten

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

• FPR2110 Version 7.2.5, lokal verwaltet durch FirePOWER Device Manager (FDM)

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.

### Netzwerktopologie



Hinweis: Das in diesem Dokument beschriebene Beispiel ist eines von mehreren empfohlenen Netzwerkdesigns. Weitere Optionen finden Sie im Konfigurationsleitfaden <u>Avoiding Interrupted Failover and Data Links</u> (Vermeidung von Unterbrechungen durch Failover und Datenverbindungen).



### Konfigurieren

Konfigurieren der primären Einheit für hohe Verfügbarkeit

Schritt 1: Klicken Sie auf Device (Gerät), und drücken Sie die Taste Configure (Konfigurieren) oben rechts neben dem Status High Availability (Hohe Verfügbarkeit).



Schritt 2: Klicken Sie auf der Seite für hohe Verfügbarkeit auf das Feld Primärgerät.

Firewall Dev	vice Manager	题 Monitoring	Ø Policies	註王 Objects	Device: ftd-prim	ary		6.	٢	۲	?	:	admin Administrator	v	eisee SECURE
	Device Summary High Availa	bility													
	How High Ave	ailability Works												~	
Select the role for this device The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first. The secondary device remains in standby mode until the primary unit becomes unavailable.															
				P	trimary Device	(ar)	Secondary	Device	0						

Schritt 3: Konfigurieren Sie die Eigenschaften der Failoververbindung.

Wählen Sie die Schnittstelle aus, die Sie direkt mit Ihrer sekundären Firewall verbunden haben, und legen Sie die primäre und sekundäre IP-Adresse sowie die Subnetz-Netzmaske fest.

Aktivieren Sie das Kontrollkästchen Dieselbe Schnittstelle wie die Failover-Verbindung verwenden für die Stateful Failover-Verbindung.

Deaktivieren Sie das Feld IPSec-Verschlüsselungsschlüssel, und klicken Sie auf HA aktivieren, um die Änderungen zu speichern.

I have configuration of peer device in clipboard PASTE FROM CLIPBOARD	
FAILOVER LINK	STATEFUL FAILOVER LINK Use the same interface as the Failover Link
Interface	Interface
unnamed (Ethernet1/7) V	unnamed (Ethernet1/7) ~
Type IPv4 IPv6 Primary IP 10.1.1.1	Type IPv4 IPv6 Primary IP 10.1.1.1
e.g. 192.168.10.1	e.g. 192.168.11.1
Secondary IP 10.1.1.2 e.g. 192.168.10.2	Secondary IP 10.1.1.2 e.g. 192.168.11.2
Netmask	Netmask
255.255.255.252	255.255.255.252
e.g. 255.255.255.0 or 24	e.g. 255.255.255.0 or 24
IPSec Encryption Key (optional) For security purposes, the encryption key will not be included in the configuration copied to the clipboard when you activate HA. You will need to manually enter the key when you configure HA on the peer device.	IMPORTANT If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More
Before you activate HA, make sure both devices have the same Smart License and Cloud Regi	on. Otherwise HA will not work.
When you click Activate HA, these settings are automatically deployed to the dev momentary traffic loss. It might take a few minutes for deployment to finish.	ice. The deployment might restart inspection engines, which can result in the
Information is copied to the clipboard when deployment is done. You must allow the clipboard when deployment is done.	the browser to access your clipboard for the copy to be successful.





Tipp: Verwenden Sie ein Subnetz mit einer kleinen Maske, das nur für Failover-Datenverkehr vorgesehen ist, um Sicherheitslücken und/oder Netzwerkprobleme so weit wie möglich zu vermeiden.



Warnung: Das System stellt die Konfiguration sofort auf dem Gerät bereit. Sie müssen keinen Bereitstellungsauftrag starten. Wenn keine Meldung angezeigt wird, dass Ihre Konfiguration gespeichert wurde und die Bereitstellung ausgeführt wird, scrollen Sie zum Seitenanfang, um die Fehlermeldungen anzuzeigen. Die Konfiguration wird ebenfalls in die Zwischenablage kopiert. Sie können die Kopie verwenden, um die sekundäre Einheit schnell zu konfigurieren. Um die Sicherheit zu erhöhen, ist der Verschlüsselungsschlüssel (falls Sie einen Schlüssel festlegen) nicht in der Zwischenablage enthalten.

Schritt 4: Nach Abschluss der Konfiguration wird eine Meldung mit den nächsten Schritten angezeigt. Klicken Sie nach dem Lesen der Informationen auf Got It.

You have successfully deployed the HA configuration on the primary device. What's next?	×
Copy the HA configuration to the clipboard. Copied Click here to copy again	
<ul> <li>Paste it on the secondary device.</li> <li>Log into the secondary device and open the HA configuration page.</li> </ul>	
You are done! The devices should communicate and establish a high availability pair automatically.	
GOT IT	

Konfigurieren der Sekundäreinheit für hohe Verfügbarkeit

Schritt 1: Klicken Sie auf Device (Gerät), und drücken Sie die Taste Configure (Konfigurieren) oben rechts neben dem Status High Availability (Hohe Verfügbarkeit).

Firewall Device Manager Monitoring	Policies Objects	s 1	۵.	@ ? :	admin Administrator	cisco SECURE
Model Cisco Firepower 2110 Thr	Software eat Defense 7.2.5-208	VDB Intrusion Rule Update 370.0 20230925-1455	Cloud Services Connected   SEC TAC	High Availability 💮 Not Configured	CONFIGURE	
F Inside Network	Cisco Firepower 2110 The MGMT 1/1 CONSOLE 1/2	1/2 eat Defense 1/3 1/5 1/7 1/9 1/11 1/13 1/5 1/7 1/9 1/11 1/13 1/14 1/6 1/8 1/10 1/12 SFI 1/1	a 1/14 1/15 1/16	ISP/WAN/Gateway	DNS Server     DNS Server     NTP Server     Smart License	

Schritt 2: Klicken Sie auf der Seite für hohe Verfügbarkeit auf das Kästchen Sekundäres Gerät.

Firewall De	vice Manager	题 Monitoring	Policies	註玉 Objects	Device: ftd-secondary	0.	)	0	?	:	admin Administrator	v	eisco SECURE
	Device Summary High Availa	bility											
	How High Av	ailability Works										~	
Select the role for this device The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first. The secondary device remains in standby mode until the primary unit becomes unavailable.													
				6	Primary Device or	Secondary Dev							

Schritt 3: Konfigurieren Sie die Eigenschaften der Failoververbindung. Sie können die in der Zwischenablage gespeicherten Einstellungen nach der Konfiguration des primären FTD einfügen oder den Vorgang manuell fortsetzen.

Schritt 3.1: Um aus der Zwischenablage einzufügen, klicken Sie einfach auf die Schaltfläche Aus Zwischenablage einfügen, fügen Sie die Konfiguration ein (drücken Sie Strg+v gleichzeitig) und klicken Sie auf OK.

Select the role for this device									
The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first. The secondary device remains in standby mode until the primary unit becomes unavailable.									
Primary Device or Secondary Device									
I have configuration of peer device in clipboard PASTE FROM CLIPBOARD									

```
Paste here Peer Device Configuration
FAILOVER LINK CONFIGURATION
Interface: Ethernet1/7
Primary IP: 10.1.1.1/255.255.252
Secondary IP: 10.1.1.2/255.255.252
STATEFUL FAILOVER LINK CONFIGURATION
Interface: Ethernet1/7
Primary IP: 10.1.1.1/255.255.255.252
Secondary IP: 10.1.1.2/255.255.252
```

Schritt 3.2: Um manuell fortzufahren, wählen Sie die Schnittstelle aus, die Sie direkt mit Ihrer sekundären Firewall verbunden haben, und legen Sie die primäre und sekundäre IP-Adresse sowie die Subnetz-Netzmaske fest. Aktivieren Sie das Kontrollkästchen Dieselbe Schnittstelle wie die Failover-Verbindung verwenden für die Stateful Failover-Verbindung.

I have configuration of peer device in clipboard	PASTE FROM CLIPBOARD		
FAILOVER LINK		STATEFUL FAILOVER LINK	Use the same interface as the Fallover Link
Interface		Interface	
unnamed (Ethernet1/7)	~	unnamed (Ethernet1/7)	~
Type IPv4 IPv6 Primary IP 10.1.1.1		Type IPv4 IPv6 Primary IP 10.1.1.1	
e.g. 192.168.10.1		e.g. 192.168.11.1	
Secondary IP 10.1.1.2 e.g. 192.168.10.2		Secondary IP 10.1.1.2 e.g. 192.168.11.2	
Netmask		Netmask	
255.255.255.252		255.255.255.252	
e.g. 255.255.255.0 or 24		e.g. 255.255.255.0 or 24	
IPSec Encryption Key (optional) For security purposes, the encryption key will not be include clipboard when you activate HA. You will need to manually enter the key when you configure	td in the configuration copied to the HA on the peer device.	IMPORTANT If you configure an IPsec encryption k features, both devices will become ac	ey with inconsistent settings for export controlled tive after you activate HA. Learn More (2
<ul> <li>Before you activate HA, make sure both devices have</li> <li>When you click Activate HA, these settings ar momentary traffic loss. It might take a few might be a few mig</li></ul>	the same Smart License and Cloud Reginer automatically deployed to the devolutions for deployment to finish	ion. Otherwise HA will not work. vice. The deployment might restart insp	pection engines, which can result in the
momentary transcross, it might take a few mi	notes for deproyment to finish.		
Information is copied to the clipboard when d	leployment is done. You must allow	the browser to access your clipboard	for the copy to be successful.
	ACTIV	ИАТЕ НА	

Schritt 4: Deaktivieren Sie das Feld IPSec-Verschlüsselungsschlüssel, und klicken Sie auf HA aktivieren, um die Änderungen zu speichern.



Warnung: Das System stellt die Konfiguration sofort auf dem Gerät bereit. Sie müssen keinen Bereitstellungsauftrag starten. Wenn keine Meldung angezeigt wird, dass Ihre Konfiguration gespeichert wurde und die Bereitstellung ausgeführt wird, scrollen Sie zum Seitenanfang, um die Fehlermeldungen anzuzeigen.

Schritt 5: Nach Abschluss der Konfiguration erhalten Sie eine Meldung, in der die nächsten Schritte erläutert werden. Klicken Sie nach dem Lesen der Informationen auf Got It.

You have successfully deployed the HA configuration on the primary device. What's next?	×
<ul> <li>Copy the HA configuration to the clipboard.</li> <li>Copied Click here to copy again</li> <li>Paste it on the secondary device.</li> <li>Log into the secondary device and open the HA configuration</li> </ul>	
You are done! The devices should communicate and establish a high availability pair automatically.	
дот пт	

# Überprüfung

 Zu diesem Zeitpunkt zeigt Ihr Gerätestatus am ehesten an, dass es sich um das sekundäre Gerät auf der Seite für hohe Verfügbarkeit handelt. Wenn der Join zum primären Gerät erfolgreich war, beginnt das Gerät mit dem primären Gerät zu synchronisieren, und schließlich wird der Modus in Standby und der Peer in Active geändert.

	🕚 This device is part of a high availability (HA) pair and is currently in standby state. With few exceptions, you cannot edit the configuration for this device. To make any changes, please log into the active unit. Learn More 🖄										
Firewall Device Manager	Monitoring Policies Objects	Device: ftd-primary	admin dministrator disco SECURE								
	Model Cisco Firepower 2110 Threat	High Availability Secondary Device: Standby $\Rightarrow$ Peer: Active									
	Finalde Network	Internet									

 In der primären FTD wird meist auch der Hochverfügbarkeitsstatus angezeigt, jedoch als "Aktiv" und "Peer: Standby".



• Öffnen Sie eine SSH-Sitzung mit dem primären FTD, und geben Sie den Befehl show running-config failover ein, um die Konfiguration zu überprüfen.



• Validieren Sie den aktuellen Status des Geräts mit dem Befehl show failover state.

> show failover state									
This host -	State Primary	Last	Failure	Reason	Date/Time				
Other host -	Active Secondary	None							
	Standby Ready	None							
====Configuration State===									
Mac set									
>									

#### 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.