# FTD Multi-Instance-Hochverfügbarkeit auf Firepower 4100 konfigurieren

# Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Hintergrundinformationen
Netzwerkdiagramm
Konfigurationen
Schritt 1: Schnittstellen vorkonfigurieren
Schritt 2: Fügen Sie 2 Ressourcenprofile für Containerinstanzen hinzu.
Schritt 3: (Optional) Fügen Sie ein MAC-Pool-Präfix der virtuellen MAC-Adresse für Container- Instanzschnittstellen hinzu.
Schritt 4: Hinzufügen einer eigenständigen Instanz.
Schritt 5: Schnittstellen konfigurieren
Schritt 6: Hochverfügbarkeitspaar für jede Instanz hinzufügen.
Überprüfung
Fehlerbehebung
Referenz

# 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.

Overview Interface	Logical Devices	Security Engine	Platform Settings						Syste	m Tools Help	admin
			Network Module 1	5 7 5 8	Network Module 2 :	: Empty	Network Module 3 : En	pty			
All Interfaces Hardware	e Bypass										
to to de co		Adula forced	8					0	Add Ne	w Filter.	×
	Management	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State		
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down	(X)	a 🖉	
Ethernet1/1	data	1gbps	lgbps			Full Duplex	yes	up		ø	
Ethernet1/2	data	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/3	mgmt	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/4	data	1gbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/5	data	1gbps	1gbps			Full Duplex	yes	up		۵P	
Ethernet1/6	data	1gbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/7	mgmt	1gbps	lgbps			Full Duplex	yes	up		6P	
Ethernet1/8	data	1gbps	1gbps			Full Duplex	yes	up		P	

Schnittstellen vorkonfigurieren

Schritt 2: Fügen Sie 2 Ressourcenprofile für Containerinstanzen hinzu.

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

- 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.

Overview Interfaces Log	ical Devices Security Engine	Platform Settings			System Tools Help admin
NTP SSH				Add	
SNMP	Name	Description	Cores		
HTTPS AAA Syslog DNS	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	d ()	
FIPS and Common Criteria Access List MAC Pool		Add Resource Profile			
<ul> <li>Resource Profiles</li> <li>Network Control Policy</li> <li>Chassis URL</li> </ul>		Number of Cores:*     10     Range: 6 to 86       Specify even value for number of cores.			
		OK Cancel			

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

In diesem Beispiel:

- Name: Instanz02
- Kernanzahl: 20

Overview Interf	aces Logio	cal Devices Security Engir	Platform Settings			System Tools Help admin
NTP SSH					Add	
SNMP		Name	Description	Cores		
HTTPS		Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	/ 5	
Syslog		Instance01		10	/ 8	
DNS						
FIPS and Common	Criteria		Add Deserves Desfile			
Access List			Add Resource Profile			
MAC Pool			Name:* Instance02			
Resource Profiles						
Network Control Po	licy		Description:			
Chassis URL			Number of Cores:* 20 Range: 6 to 86			
			Specify even value for number of cores.			
			OK Cancel			

Zweites Ressourcenprofil hinzufügen

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

Ove	rview Interfaces Logi	ical	Devices Security Engine	Platform Settings						System	Tools	Help	admin
N	ΓP							0					
s	SH							·	NOU				
s	NMP		Name		Description		Cores						
н	TTPS		Default-Small		Auto-created application resource-profile with 6 cpu-	cores	6		28				
A	AA												
S	vslog		Instance01				10		a 🖓				
D	NS		Instance02				20		20				
F	PS and Common Criteria		1150010000				8.V		ø 0				
A	cess List												
M	AC Pool												
► R	esource Profiles												
N	etwork Control Policy												
c	nassis URL												

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

Schritt 4: Hinzufügen einer eigenständigen Instanz.

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

· 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.

Overview Interfaces Logical Devices Security Engine	Platform Settings			System Tools Help admin
Logical Device List	(0 instances) 100% (86 of 86) Cores	Available		C Refresh 💽 Add •
No logical devices available. Click on Add Device to add a new logical device.				
	Add Standalone		<u> 7 x</u>	
	Device Name:	FTD01		
	Template:	Cisco Secure Firewall Threat Defense	~	
	Image Version:	7.2.5.208	~	
	Instance Type:	Container	~	
	Before you add the the security modul formatting. You on	e first container instance, you must reiniti e/engine so that the disk has the correct ly need to perform this action once.	lize	
		ок	ancel	

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

Overview Interfaces Logical Devices Security Engine Platform	Settings	System Tools Help admin
Provisioning - FTD01 Standalone   Cisco Secure Firewall Threat Defense   7.2.5.208	Cisco Secure Firewall Threat Defense - Bootstrap Configuration 2 X	Save Cancel
Ethernet1/1 Ethernet1/2 Ethernet1/5 Ethernet1/6 Ethernet1/8	SH 1 - 86 Cores Available          Resource Profile:       Instance01         Interface Information         Management Interface:         Ethernet1/3         Address Type:         IPv4         Management IP:         I.I.ZZLI1         Network Mask:         255.0.0.0         Network Gateway:	
Application Version Resource Profile	irt Status	
G FTD 7.2.5.208		
4	OK Cancel	,

Profil/Management-Schnittstelle/Management-IP konfigurieren

## b. Festlegen von Datenschnittstellen

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

• Ethernet1/4 (für HA-Verbindung)

c	Overview Interfaces	Logical Devices	Security Engine Pla	atform Settings				System Tools Help admin
P S	Provisioning - FTD01 Standalone   Cisco Sec	ure Firewall Threat D	efense   7.2.5.208					Save Cancel
	Data Ports Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/6 Ethernet1/6				Ethernet1/1 Ethernet1/2 Ethernet1/2 Ethernet1/4	FTD	•- 7.2.5.208 themet1/3 k to configure	
	Application	Version	Resource Profile	n Management IP	Gateway	Management Por	t Status	
	FTD	7.2.5.208	Instance01	1.000001	1.0 0 000	Ethernet1/3		
	Interface Name		A CONTRACTOR A	Type data data data	**	Extracting a 2		

Festlegen von Datenschnittstellen

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

	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	js				System Tools Help admin
Lo	gical Devic	e List		c	1 Container instanc	e) 100% (86 of 86) Cores Avai	ilable			C Refresh Add •
	FTD01			Standalone	Status:ok					2 I
	Applicat	ion	Version	Resource F	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01		1	1	Ethernet1/3	🐝 Installing	0180 🎋 c 🖄

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.

- · 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.

Overview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logical Devic	ce List			2 Container instand	ces) 66% (56 of 86) Co	res Available			C Refresh 🕥 Add •
FTD11			Standalone	Status:ok					
Applica	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance02	]	10.1	1/20200	Ethernet1/7	Online	🕶 🕅 c 🖄
FTD01			Standalone	Status:ok					0 I.
Applica	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance01	]	Chilana	1.0	Ethernet1/3	Online	🕶 ) 🏹 🔍

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 Deplot 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.

Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	gs				System Tools Help admin
Logical Devic	ce List			2 Container instand	<b>xes)</b> 66% (56 of 86) Co	res Available			C Refresh 🕢 Add •
FTD12	]		Standalone	Status:ok					2 I
Applica	tion	Version	Resource I	rofile	Management IP	Gateway	Management Port	Status	
# FTD		7.2.5.208	Instance02		10.2	1.	Ethernet1/7	nline	🚾 🌃 c 🕍
FTD02			Standalone	Status:ok					01
Applica	tion	Version	Resource F	rofile	Management IP	Gateway	Management Port	Status	
# FTD		7.2.5.208	Instance01		1.2	1.6	Ethernet1/3	Online	💌 🏹 C 🕍

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.

Firewall Management Center Overview Analysis Poli	icies Devices Objects I	integration			Deploy	Q 📀 🔅 🚱 admin 🔹 :	dide SECURE
View By: Group						Deploye	ment History
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4) • De	eployment Pending (0)	(0) • Snort 3	(4)			Q, Search Device	Add 💌
Collapse All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)							
C FTD1_FTD01 Snort 3     C MOV.1.1 - Rovted	Firepower 4145 with FTD	7.2.5	ERATAS-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	1:
C PTD1_FTD11 Short 3 C 223 10.1 - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	43	11
FTD2_FTD02 Short 3	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	11
FTD2_FTD12 Snort 3     Circle 2.10.2 - Routed	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	11

Instanzstatus in FMC bestätigen

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

- · Name: FTD01\_FTD02\_HA
- · Primäre Gegenstelle: FTD1\_FTD01

#### · Sekundärer Peer: FTD2\_FTD02



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

Firewall Management Center Overview Analysis Process / Devices / Device Management	olicies Devices Objects I	ntegration			Deploy	Q 📀 🌣 🕑 admin 🔹	dide SECURE
View By: Group						Deploy	ment History
All (4) • Error (0) • Warning (0) = Offline (0) • Normal (4) • I	Deployment Pending (0)	(0) • Snort 3 (4)				Q, Search Device	Add 🔻
Collapse All							
Name	Model	Version Chase	ssis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)		Add High Availabi	ility Pair 🛛				
FTD1_FTD01 Snort 3	Firepower 4145 with FTD	Name:* FTD01_FTD02_HA		Base, Threat (2 more)	acp-rule	49	×1
FTD1_FTD11_Snort 3	Firepower 4145 with FTD	Device Type: Firewall Threat Defen	nse v	Base, Threat (2 more)	acp-rule	49	1
FTD2_FTD02_Short 3	Firepower 41.45 with FTD	Primary Peer: FTD1_FTD01	•	Base, Threat (2 more)	acp-rule	49	1
FTD2_FTD12 Snort 3	Firepower 4145 with FTD	Secondary Peer: FTD2_FTD02	Y	Base, Threat (2 more)	acp-rule	4Q	×1
		Threat Defense High configuration. Licen converted to their hi on both peers.	an Availability pair will have primary nees from primary peer will be high availability versions and applied				
			Cancel Continue				

Erstes Failover-Paar hinzufügen

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

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

Firewall Management Center Overview Devices / Device Management	ioy Q 🥝 🌣 📵 admin	dede SECURE				
View By: Group +					De	ployment History
All (4) • Error (0) • Warning (0) = Offline (0) • N	vormal (4) • Deployment P	rending (0)			Q, Search Device	Add •
Collacse All						
Name	Model	Add Migh Availability Pair		Access Control Policy	Auto RollBack	
Ungrouped (4)		And high Availability Fail				
		High Availability Link	State Link			
FTD1_FTD01 Snort 3	Firepowe	Interface:* Ethernet1/4 +	Interface:* Ethernet1/4 +	acp-rule	4(3)	11
		Logical Name:* ha_link	Logical Name:*			
FTD1_FTD11 Snort 3	Firepowe	Primary IP:* 192.168.90.1	Primary IP;*	acp-rule	4Q	11
		Use IPv6 Address	Use IPv6 Address			
FTD2_FTD02 Snort 3	Firepowe	Secondary IP:* 192.168.90.2	Secondary IP:*	acp-rule	4 <u>9</u>	11
The Province		Subnet Mask:* 255.255.255.0	Subnet Mask:*			
FTD2_FTD12 Snort 3	Firepowe	IPsec Encryption		acp-rule	4©	11
22.102 - Materia		Enabled				
		Key Generation: Auto v				
		LAN failover link is used to sync configuration, stated between peers. Selected interface links and encryption	ul failover link is used to sync application content settings cannot be changed later.			
			Cancel Add			

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

- e. Den Failover-Status bestätigen
- · FTD1\_FTD01 : Primär, Aktiv
- · FTD2\_FTD02 : Sekundär, Standby

C Dies	well Measurement Contex												
Devic	overview Analysis	Policies Devices Object	s Integration	1			Deploy Q 🕝	admin      admin      secon SECURE					
View By:	Group +							Deployment History					
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	pgrade (0)	Snort 3 (4)				Q, Search Device Add •					
Collapse All	Collecter Al												
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack						
0	V Ungrouped (3)												
	FTD01_FTD02_HA High Availability							1					
	FTD1_FTD01(Primary, Active) Snort 3 SAMA 1.1 - Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acpirule	<b>«</b> ۵	1					
_	· · · · · · · · · · · · · · · · · · ·												
	FTD2_FTD02(Secondary, Standby) Short 3 (*3.3.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢9	:					
	FTD1_FTD11 Snort 3     Tot=4.10.1 - Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-role	e9+	11					
	FTD2_FTD12 Snort 3     Ind2_Routed	Firepower 4145 with FTD	7.2.5	Firepower4XHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	ę۶	11					

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.

Firewall Management Center Devices / Secure Frewall Interfaces	Overview Analysis I	ilicies Devices Objects Integration		Deploy Q 🤣 🌣 🔕 admin 🔹 🐝 SECURE
FTD1_FTD01				You have unsaved changes Save Cancel
Summary High Availability Device Routing	g Interfaces Inline S	Edit Physical Interface Edit Physic	al Interface	ealiable for use. X
		General IPv4 IPv6 Path Monitoring Advanced General IP Type:	IPv4 IPv6 Path Monitoring Advanced	Add Interfaces +
Interface	Logi	inside Use Static I	· · ·	
Ethernet1/1	inside	Enabled     P Address:     192.168.10	254/24	
© Ethernet1/2	outside	Description:	5.255.255.128 or 192.0.2.1725	
Ethernet1/3	diagnostic			
Ethernet1/4		None v		
		Security Zone:		
		inside_zone *		
		Interface ID:		Cancel OK
		Ethernet1/1		
		MTU:		
		1500		
		(64 - 9184)		
		Phoney:		
		Descente Parado desce Texa		
		NVE Only:		
			Cancel	

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.

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy Q 🚱 🌣 @ admin 🕶 📩 SECURE											
FTD01_FTD02_HA Cisco Firepower 4145 Threat Defense Summary High Availability	e Device Routing Interfaces Inline Sets DHCP VTEP							Cancel			
IPsec Encryption	Edit inside	0	stics					٩			
Interface Name	Monitor this interface for failures IPv4 IPv6			Active Link-Local IPv6	Standby Link-	Local IPv6	Monitoring				
outside	Interface Name: inside						۰	1			
diagnostic	Active IP Address:		0					/			
inside	192.168.10.254 Mask:			٥	1						
	24 Standby IP Address: 192.168.10.253										
Failover Trigger Criteria			face MAC Addr	resses				+			
Failure Limit			cal Interface	Active Mac Add	Iress	Standby Ma	c Address				
Peer Poll Time		ancel OK	et1/1	1234.1234.000	1	1234.1234.	0002	/1			
Peer Hold Time											

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.

Ę	Firewall Ma Policies / Acce	anagement C ss Control / Policy	Center Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	Q 🗳 🌣	@ admin	• deade	SECU	RE
•	acp-rule Try New UI Layout ( Analyze Hit Counts Seeve Cancel Enter Description																		
P	Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy: Default Prefilter Policy: SSL Policy: None Identity Policy: None																		
Eib	er by Device	Search Rules											×	Show Rule Con	flicts 🛛 🕂	Add Categor	y +	Add Ru	le
	Name	Source Zones	Dest Zones	Source Networks	Der	st Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	15 O I.	<u>क</u> ा व		¢
$\sim M$	andatory - acp-rule	e (1-1)		_												_			
1	ftd_ha_acp	inside_zone	outside_zone	Any	,An		Any	Any	Any	Any	Any	Any	Any	Any	C Allow	E 0 E	2回	. • •	1
∼ D	✓ Default - acprule (-)																		
The	re are no rules in th	is section. Add Ru	le or Add Cate	gory															

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 <---- InstanceO1 of FPRO2 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.

Smart Licenses			Filter Devices	×	Edit Performance Tier	Edit Licenses
License Type/Device Name	License Status	Device Type		Domain	Group	
∨ Base (2)	In-Compliance					^
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	eat Defense	Global	N/A	_
FTD11_FTD12_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	eat Defense	Global	N/A	
✓ Malware (2)	In-Compliance					
FTD01_FTD02_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	eat Defense	Global	N/A	
FTD11_FTD12_HA (2)     Clsco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	eat Defense	Global	N/A	
✓ Threat (2)	In-Compliance					
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	eat Defense	Global	N/A	
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	eat Defense	Global	N/A	
✓ URL Fittering (2)	In-Compliance					- 1
FTD01_FTD02_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	

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.

// 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

Fir Dev	rewall Management Center Overview Analysis	Policies Devices Objec	ts Integratio	n			Deploy Q 🤇	admin • deale SECURE					
View By:	Group							Deployment History					
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	Deployment Pending (0)	lpgrade (0)	Snort 3 (4)				Q, Search Device Add +					
Collapse All	Al another a second secon												
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack						
	V Ungrouped (2)												
	FID01_FID02_HA High Availability							/:					
	FTD1_FTD01(Primary, Standby) Soort 3	Firepower 4145 with FTD	7.2.5	ERATIAS-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1					
	FTD2_FTD02(Secondary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1					
	✓ FTD11_FTD12_HA ∀ High Availability							11					
	FTD1_FTD11(Primary, Active) Short 3     Grammatic Structure Structure	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1					
	FTD2_FTD12(Secondary, Standby) Short 3     Tot.u. 10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com/443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	99	1					

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.

<b>C</b> 5	Firewall Management Center Overview Analysis Revices / Device Management	Policies Devices Objec	ts Integratio	n			Deploy Q 🥥	O admin      dealer SECURE					
View By:	Group							Deployment History					
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	Upgrade (0)	Snort 3 (4)				Q, Search Device Add 🔻					
Collapse A	Coffeese All												
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack						
	<ul> <li>Ungrouped (2)</li> </ul>												
	FTD01_FTD02_HA												
	Pign Avanaoury							Switch Active Peer					
	FTD1_FTD01(Primary, Standby) Snort 3     Control (Primary, Standby)	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	Force refresh node status Delete Revert Upgrade					
	FTD2_FTD02(Secondary, Active) Short 3     Control 1 2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢۹	Health Monitor Troubleshoot Files					
	V High Availability							11					
	C Strillo - Routed Snort 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:					
	FTD2_FTD12(Secondary, Standby) Short 3     Attp3.10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1					

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 available

firepower#

failover active

Fehlerbehebung

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

#### <#root>

>

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

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 of

#### 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.