# Configuración de FTD Multi-Instance High-Availability en Firepower 4100

# Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Diagrama de la red
Configuraciones
Paso 1. Preconfigurar interfaces
Paso 2. Agregue 2 perfiles de recursos para instancias de contenedor.
Paso 3. (Opcional) Agregue un prefijo de conjunto MAC de dirección MAC virtual para interfaces de instancia de contenedor.
Paso 4. Agregue una instancia independiente.
Paso 5. Configurar interfaces
Paso 6. Agregue Un Par De Alta Disponibilidad Para Cada Instancia.
Verificación
Troubleshoot
Referencia

# Introducción

Este documento describe cómo configurar la conmutación por fallas en instancias de contenedores de FTD (multiinstancia).

# Prerequisites

## Requirements

Cisco recomienda que conozca Firepower Management Center y Firewall Threat Defence.

## **Componentes Utilizados**

Cisco Firepower Management Center Virtual 7.2.5 Appliance de NGFW Cisco Firepower 4145 (FTD) 7.2.5 Sistema operativo extensible (FXOS) Firepower 2.12 (0.498) Windows 10

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antes de implementar FTD Multi-Instance, es importante entender cómo puede afectar el rendimiento de su sistema y planificar en consecuencia. Consulte siempre la documentación oficial de Cisco o consulte con un representante técnico de Cisco para garantizar una implementación y configuración óptimas.

# Antecedentes

Multi-Instance es una función de Firepower Threat Defence (FTD) que es similar al modo de contexto múltiple ASA. Permite ejecutar varias instancias de FTD de contenedor independientes en un único componente de hardware. Cada instancia de contenedor permite la separación de recursos físicos, la gestión de la configuración independiente, las recargas independientes, las actualizaciones de software independientes y la compatibilidad total con funciones de defensa frente a amenazas. Esto resulta especialmente útil para organizaciones que requieren diferentes políticas de seguridad para diferentes departamentos o proyectos, pero que no desean invertir en varios dispositivos de hardware independientes. Actualmente, la función de instancias múltiples es compatible con los appliances de seguridad Firepower de las series 4100 y 9300 que ejecutan FTD 6.4 y versiones posteriores.

Este documento utiliza Firepower4145, que admite un máximo de 14 instancias de contenedor. Para ver el número máximo de instancias admitidas en Firepower Appliance, consulte <u>Número</u> <u>máximo de instancias y recursos de contenedor por modelo.</u>

# Diagrama de la red

Este documento presenta la configuración y verificación para HA en Multi-Instance en este diagrama.



Diagrama de configuración lógica



Diagrama de configuración física

# Configuraciones

Paso 1. Preconfigurar interfaces

a. Navegue hasta Interfaces en FCM. Establezca 2 interfaces de gestión. En este ejemplo, Ethernet1/3 y Ethernet1/7.

Overview Interfac	es Logical Devices	Security Engine	Platform Settings						Syste	m Tools Help	admin
			Network Module 1 1 3 58 2 4 6	5 7 5 8	Network Module 2 :	: Empty	Network Module 3 : Em	pty			
All Interfaces Hardwa	re Bypass								1		
Interface	Turne	Admin Speed	Operational Speed	Instances	VIAN	Admin Duplay	Auto Negotiation	Operation State	Admin State	w • Filter.	×
MGMT	Management	Numin Speed	operational speed	Instances	VLAN	Admin Doplex	Auto Regulation	operation state			
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down	(IX)	J 🕄	
Ethernet1/1	data	1gbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/2	data	lgbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/3	mgmt	lgbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/4	data	1gbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/5	data	1gbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/6	data	1gbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/7	mgmt	lgbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/8	data	lgbps	1gbps			Full Duplex	yes	up		ø	

Preconfigurar interfaces

Paso 2. Agregue 2 perfiles de recursos para instancias de contenedor.

a. Navegue hasta Configuración de la plataforma > Perfiles de recursos > Agregar en FCM. Establecer el primer perfil de recursos.

En este ejemplo: ·Nombre: Instancia01 ·Número de núcleos: 10



Nota: Para el HA de un par de instancias de contenedor, deben utilizar los mismos atributos de perfil de recurso.

Establezca el nombre del perfil entre 1 y 64 caracteres. Tenga en cuenta que no puede cambiar el nombre de este perfil después de agregarlo.

Establezca el número de núcleos para el perfil, entre 6 y el máximo.

Overview	Interfaces Logic	cal Devices Security Engine	Platform Settings			System Tools Help admin
NTP SSH					Add	
SNMP		Name	Description	Cores		
AAA		Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	/ 🗊	
Syslog						
DNS						
FIPS and Co	mmon Criteria					
Access List			Add Resource Profile			
MAC Pool			Name:* Instance01			
Resource P	rofiles		andrandeva			
Network Cor	ntrol Policy		Description:			
Chassis URL			Number of Cores:* 10 Range: 6 to 86			
			Specify even value for number of cores.			
			OK Cancel			

b. Repita a. en el paso 2 para configurar el segundo perfil de recursos.

En este ejemplo: ·Nombre: Instancia02 ·Número de núcleos: 20

Overview Interfa	ices Logio	al Devices Security Engine	Platform Settings			System 1	fools He	lp admin
NTP SSH					Add			
SNMP		Name	Description	Cores				
AAA		Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	/ 8			
Syslog		Instance01		10	/ 8			
DNS FIPS and Common ( Access List MAC Pool • Resource Profiles Network Control Pol Chassis URL	Criteria		Add Resource Profile  Name:* Instance02 Description: Number of Cores:* 20 Range: 6 to 86 Sectify even value for number of cores.					
			OK Cancel					

Agregar 2º perfil de recursos

c. Compruebe que 2 perfiles de recursos se han agregado correctamente.

Ov	erview Interfaces Log	ical	Devices Security Engine	Platform Settings					System	Tools I	telp admin
	ITP						-				
3	SH						0	Add			
1	INMP		Name		Description	Cores					
,	ITTPS		Default-Small		Auto-created application resource-profile with 6 cpu-cores	6		28			
1	IAA										
5	syslog		Instance01			10		20			
1	WS		Instance02			20		28			
,	IPS and Common Criteria										
	ccess List										
	IAC Pool										
× 1	tesource Profiles										
1	letwork Control Policy										
(	hassis URL										

Confirmar perfil de recurso

Paso 3. (Opcional)Agregue un Prefijo de Pool MAC de la dirección MAC virtual para las Interfaces de Instancia de Contenedor.

Puede establecer manualmente la dirección MAC virtual para la interfaz activa/en espera. Si las Direcciones MAC Virtuales no están configuradas , para la capacidad de instancias múltiples, el chasis genera automáticamente direcciones MAC para las interfaces de instancia y garantiza que una interfaz compartida en cada instancia utilice una dirección MAC única.

Verifique <u>Agregar un Prefijo de Pool MAC y Ver Direcciones MAC para Interfaces de Instancia de</u> <u>Contenedor</u> para obtener más detalles sobre la dirección MAC.

Paso 4. Agregue una instancia independiente.

a. Navegue hasta Dispositivos lógicos > Agregar autónomo. Establecer primera instancia.

En este ejemplo: ·Nombre del dispositivo: FTD01

## ·Tipo de instancia: contenedor



Nota: La única forma de desplegar una aplicación contenedora es predesplegar una App-Instance con el Tipo de Instancia establecido en Contenedor. Asegúrese de seleccionar Contenedor.

No puede cambiar este nombre después de agregar el dispositivo lógico.

Overview Interfaces Logical Devices Security Engine	Platform Settings			S	ystem Tools Help admin
Logical Device List	(0 instances) 100% (86 of 86) Cor	res Available			C Refresh 🕢 Add •
No logical devices available. Click on Add Device to add a new logical device.					
	Add Standalone		() X		
	Device Name:	FTD01			
	Template:	Cisco Secure Firewall Threat Defense	<b>v</b>		
	Image Version:	7.2.5.208	¥		
	Instance Type:	Container	<b>*</b>		
	Before you add the security mo formatting. You	the first container instance, you must reinit dule/engine so that the disk has the correct only need to perform this action once.	lize		
		ок	ancel		

Agregar instancia

## Paso 5. Configurar interfaces

a. Establezca Resource Profile, Management Interface, Management IP para Instance01.

En este ejemplo: ·Perfil de recurso: Instancia01 ·Interfaz de gestión: Ethernet1/3 ·IP de gestión: x.x.1.1

Overview Interfaces Logical Devices Security Engine Platform S	Settings	System Tools Help admin
Provisioning - FTD01 Standalone   Cisco Secure Firewall Threat Defense   7.2.5.208	Cisco Secure Firewall Threat Defense - Bootstrap Configuration 💌	Save Cancel
Data Ports	General Information Settings Agreement	
EthernetJ/1 EthernetJ/2 EthernetJ/5 EthernetJ/6 EthernetJ/6	SM 1 - 86 Cores Available  Resource Profile: Instance01  Hanagement Interface: Ethernet1/3  Address Type: IPv4 only  IPv4 Hanagement IP: 1:::::1 Network Mask: 255.0.0 Network Gateway: 1.^	
Application Version Resource Profile	ort Status	
G FTD 7.2.5.208		
	OK Cancel	

Configurar perfil/interfaz de gestión/IP de gestión

b. Establecer interfaces de datos.

En este ejemplo:

·Ethernet1/1 (se utiliza para el interior)

·Ethernet1/2 (utilizado para el exterior)

·Ethernet1/4 (se utiliza para el enlace HA)

0	verview Interfaces	Logical Devices Secu	rity Engine Platform Set	tings				System Tools	Help admin
P S	rovisioning - FTD01 tandalone   Cisco Sec	ure Firewall Threat Defense	7.2.5.208					Save	Cancel
D	ata Ports	-							
	Ethernet1/1								
	Ethernet1/2								
	Ethernet1/5								
	Ethernet1/6								
	Ethernet1/8			Ethernet1/	1				
				Ethernet1/	4	FTD - 7.2.5.202 Ethernet1/3 Click to configure			
	Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
•	FTD	7.2.5.208	Instance01	1.1	1.0	Ethernet1/3			
	Interface Name			Туре					
	Ethernet1/1			data					
	Ethernet1/2			data					
	Ethernet1/4			data					

Establecer interfaces de datos

## c. Acceda a Dispositivos Lógicos. Esperando el inicio de la instancia.

(	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	s				System Tools Help admin
L	ogical Devic	e List			(1 Container instanc	e) 100% (86 of 86) Cores A	vailable			C Refresh Ads •
	FTD01			Standalone	Status:ok					2 I
	Applicat	ion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01		1	1.0.0.000	Ethernet1/3	🐝 Installing	(IR) 🎋 C 🕍

Confirmar estado de instancia01

d. Repita a. en los pasos 4.a y 5.a a c para agregar la 2ª instancia y definir los detalles correspondientes.

En este ejemplo:

•Nombre del dispositivo: FTD11 •Tipo de instancia: contenedor

·Perfil de recursos: instancia02
·Interfaz de gestión: Ethernet1/7
·IP de gestión: x.x.10.1

·Ethernet1/5 = interior

·Ethernet1/6 = externa

·Ethernet1/8 = enlace HA

e. Confirme que dos instancias están en línea en FCM.

Overview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logical Devi	ce List			2 Container instan	ces) 66% (56 of 86) C	ores 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	]		1/2-2-22	Ethernet1/7	Online	💌 🎘 c 🔬
FTD01			Standalone	Status:ok					Ø :
Applica	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
H FTD		7.2.5.208	Instance01	]	C ann	1.	Ethernet1/3	1 Online	🕶 🕅 c 🖾

Confirmar El Estado De La Instancia En El Dispositivo Principal

f. (Opcional)Ejecute scope ssa y scope slot 1 el show app-Instance comando para confirmar que las instancias 2 tienen el estado En línea en la CLI de Firepower.

# <#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. Haga lo mismo en el dispositivo secundario. Confirme que 2 instancias tengan el estado En línea.

¢	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	s				System Tools Help admin
Lo	gical Devio	e List			2 Container instanc	es) 66% (56 of 86) Cor	es Available			C Refresh 🖉 Add •
	FTD12			Standalone	Status:ok					
	Applicat	ion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance02	]		1.	Ethernet1/7	Online	💌 🕅 💌
	FTD02			Standalone	Status:ok					1
	Applicat	ion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01	]	1.2	1.0	Ethernet1/3	Online	💌 🕅 C 🖄

Confirmar Estado De Instancia En El Dispositivo Secundario

Paso 6. Agregue Un Par De Alta Disponibilidad Para Cada Instancia.

a. Navegue hasta **Dispositivos** > **Agregar dispositivo** en FMC. Agregar todas las instancias a FMC.

En este ejemplo:

Nombre de visualización de la instancia 01 de FTD1: FTD1\_FTD01
Nombre de visualización para la instancia 02 de FTD1: FTD1\_FTD11
Nombre de visualización de la instancia 01 de FTD2: FTD2\_FTD02
Nombre de visualización de la instancia 02 de FTD2: FTD2\_FTD12

Esta imagen muestra la configuración de FTD1\_FTD01.

Firewall Management Center Overview Analytic Devices / Device Management	Add Device	0	Deploy Q 🔮 🕸 🔕 admin 🕶 🖏 SECURE
View By: Group	CDO Managed Device		Deployment History Q, Search Device Add +
Name	Display Name: FTD1_FTD01	Licenses	Access Control Policy Auto RollBack
Ungrouped (0)	Registration Key:*         Group:         Once         Access Control Policy:*         acp-rule         Smart Licensing         Note: Al + units thread Thread Defense devices require a performance tier license.         It's important to choose the tier that matches the locense you have in your account.         Clickhees for information about the Firewall Thread Defense performance-tiered licensing.         Unit you choose the: you Freewall Thread Defense virtual 7.0 and above):         [Tory - virtuale)         Makese         Makese         Advanced         Unit_or         Unit_or         Transfer Packets	n.	
	Cancel Register		

Añadir instancia de FTD a FMC

#### b. Confirme que todas las instancias sean normales.

Firewall Management Center Overview Analysis	s Policies Devices Objects	Integration			Deploy	Q 🙆 🔅 🕲 admin•	dide SECURE					
View By: Group *	tw B): Group +											
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4)	) • Deployment Pending (0) • Upgrad	ie (0) • Snort 3	3 (4)			Q, Search Device	Add 🕶					
Collapse. All												
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack						
Ungrouped (4)												
FTD1_FTD01 Snort 3     t_Acts_1.1 = Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1:					
FTD1_FTD11 Short 3     Victo 10.1 - Routed	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	10	1					
FTD2_FTD02 Snort 3     Grave 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	40	1					
FTD2_FTD12 Short 3     Lings.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	11					

Confirmar estado de instancia en FMC

c. Vaya a **Devices** > **Add High Availability**. Establezca el primer par de conmutación por fallo.

En este ejemplo:

#### ·Nombre: FTD01\_FTD02\_HA

·Peer principal: FTD1\_FTD01



Nota: Asegúrese de seleccionar la unidad correcta como la unidad principal.

Firewall Management Center Overview Analysis Pol	licies Devices Objects I	ntegration			Deploy	Q 📀 🌣 \varTheta admin •	disto SECURE
View By: Group						Deploy	ment History
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4) • D	eployment Pending (0)	(0) • Snort 3 (4)				Q, Search Device	Add 🔻
Collarse All							
Name	Model	Version Chassis		Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)		Add High Availability	y Pair 🛛 🛛				
FTD1_FTD01_Snort.3	Firepower 4145 with FTD	Name:* FTD01_FTD02_HA		Base, Threat (2 more)	acp-rule	eçə	1
FTD1_FTD11_Snort.3	Firepower 4145 with FTD	Device Type: Firewall Threat Defense	*	Base, Threat (2 more)	acp-rule	49	1
FTD2_FTD02_Snort.3	Firepower 4145 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	•	Base, Threat (2 more)	acp-rule	45	1
		Threat Defense High Av configuration. Licenses converted to their high a on both peers.	wallability pair will have primary s from primary peer will be availability versions and applied				
			Cancel Continue				

Agregar primer par de conmutación por error

d. Establezca IP para el link de failover en el primer par de failover.

En este ejemplo:

·Enlace de alta disponibilidad: Ethernet1/4

·Enlace de estado: Ethernet1/4

·IP principal: 192.168.90.1/24

#### ·IP secundaria: 192.168.90.2/24

Firewall Management Center Overview Analysis Devices / Device Management	s Policies (	Devices Objects Integration		Deploy	९ 😑 🌣 😝 admin •	deades SECURE
Mexille Group					Depk	oyment History
All (4)   Error (0)  Warning (0)  Offline (0)  Normal (4)	Deployment F	Pending (0)			Q, Search Device	Add 🔻
Collarose Al						
Name Name	Model	Add High Availability Date		Access Control Policy	Auto RollBack	
Ungrouped (4)		Add high Availability Fail	0			
		High Availability Link	State Link			
FTD1_FTD01 Snort 3     I1 - Routed	Firepowe	Interface:* Ethernet1/4 +	Interface:* Ethernet1/4 +	acp-rule	«9	11
		Logical Name:* ha_link	Logical Name:*			
C FTD1_FTD1 Seet 3	Firepowe	Use IPv6 Address	Use IPv6 Address	acp-rule	*9	1
C FTD2_FTD02 Snort 3	Course of	Secondary IP:* 192.168.90.2	Secondary IP:*			
1.2 - Routed	Prepowe	Subnet Mask:* 255.255.255.0	Subnet Mask:*		42	1
FTD2_FTD12 Snort 3	Firepowe	IPsec Encryption		acp-rule	49	11
TO.2 - Housed		Enabled				
		Key Generation: Auto v				
		LAN failover link is used to sync configuration, stated	ful failover link is used to sync application content			
		between peers. Selected interface links and encryption	settings cannot be changed later.			
			Cancel Add			

Establecer la interfaz HA y la IP para el primer par de conmutación por fallo

e. Confirmar el estado de conmutación por fallas

#### ·FTD1\_FTD01: Principal, Activo

#### ·FTD2\_FTD02: Secundario, En espera

Fire Device	ewall Management Center Overview Analysis	Policies Devices Object	ts Integratio	n			Deploy Q 😋	O admin      duals      SE	ÉCURE
View By:	Group							Deployment Hist	tory
All (4)	Error (0)      Warning (0)      Offline (0)      Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	Ipgrade (0)	Snort 3 (4)				Q, Search Device	dd 🔻
Collapse All									
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack		
	<ul> <li>Ungrouped (3)</li> </ul>								
•	FID01_FID02_HA High Availability							/1	
	FTD1_FTD01(Primary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Ø	1	
	FTD2_FTD02(Secondary, Standby) Short 3 FT03.1.2 - Rosted	Firepower 4145 with FTD	7.2.5	Firepower4XHG cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	«Ø	I	
	FTD1_FTD11 Snort 3     Track 10.1 - Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢Ø	11	
	FTD2_FTD12 Snort 3     1	Firepower 4145 with FTD	7.2.5	Firepower4XHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	*Ø	11	

Confirmar estado del primer par de conmutación por error

f. Vaya a **Devices** > **Click FTD01\_FTD02\_HA** (en este ejemplo) > **Interfaces.** Establecer IP activa para interfaz de datos.

En este ejemplo:

·Ethernet1/1 (interno): 192.168.10.254/24

·Ethernet1/2 (exterior): 192.168.20.254/24

·Ethernet1/3 (diagnóstico): 192.168.80.1/24

#### Esta imagen muestra la configuración para la IP activa de Ethernet1/1.

Firewall Management Center Over Devices / Secure Firewall Interfaces	erview Analysis P	Policies Devices Objects Integration		Deploy Q 🧬 🌣 🔕 admin 🕶 📩 SECURE
FTD1_FTD01				You have unsaved changes Save Cancel
Cisco Firepower 4145 Threat Defense Summary High Availability Device Routing	Interfaces Inline Se	Edit Physical Interface	Edit Physical Interface	allable for use. ×
		General IPv4 IPv6 Path Monitoring Advance	g General IPv4 IPv6 Path Monitoring Advanced	Add Interfaces *
Interface	Logi	Name: inside	er syse: Use Static IP v ID Addeses	
Ethernet1/1	inside	Enabled     Management Only	192.108.10.254/24 = 192.2168.10.254/24 = 192.2168.21.255.26.26 192.02.125	
© Ethernet1/2 © Ethernet1/3	diagnostic	Description:		
Ethernet1/4		Mode: None		
		Security Zone: inside_zone		
		Interface ID: Ethernet1/1		Cancel
		MTU:		
		(64 - 9184) Priority:		
		0 (0 - 65535) Propagate Security Group Tag:		
		NVE Only:		
			Cancel	

Establecer IP activa para interfaz de datos

g. Vaya a Devices > Click FTD01\_FTD02\_HA (en este ejemplo) > High Availability. Establezca Standby IP for Data Interface.

En este ejemplo:

·Ethernet1/1 (interno): 192.168.10.253/24

·Ethernet1/2 (exterior): 192.168.20.253/24

·Ethernet1/3 (diagnóstico): 192.168.80.2/24

Esta imagen muestra la configuración para la IP en espera de Ethernet1/1.

Firewall Management Devices / High Availability	Center Overview Analysis Policies Devices	Objects Inte	gration		Deploy	९ 💕 🌣	admin 🕶	cisco SECURE
FTD01_FTD02_HA Cisco Firepower 4145 Threat Defense Summary High Availability	P Device Routing Interfaces Inline Sets DHCP VTI	EP						6 Cancel
IPsec Encryption	Edit inside	ø	itics					۹
Monitored Interfaces Interface Name	Monitor this interface for failures IPv4 IPv6			Active Link-Local IPv6	Standby Link-	Local IPv6	Monitoring	
outside	Interface Name: inside						0	/
diagnostic	Active IP Address: 192.168.10.254 Mask:						0	
	24 Standby IP Address: 192.168.10.253							
Failover Trigger Criteria			face MAC Addi	Active Mac Add	Iress	Standby Ma	c Address	+
Peer Poll Time Peer Hold Time		Cancel OK	et1/1	1234.1234.000	1	1234.1234.	0002	/1

Establecer IP en espera para la interfaz de datos

h. Repita los pasos 6.c a g, para agregar el segundo par de conmutación por fallas.

En este ejemplo:

Nombre: FTD11\_FTD12\_HAPar principal: FTD1\_FTD11Par secundario: FTD2\_FTD12

Enlace de alta disponibilidad: Ethernet1/8Enlace de estado: Ethernet1/8

·Ethernet1/8 (ha\_link activo): 192.168.91.1/24

·Ethernet1/5 (interna activa): 192.168.30.254/24

·Ethernet1/6 (fuera activo): 192.168.40.254/24

·Ethernet1/7 (diagnóstico activo): 192.168.81.1/24

·Ethernet1/8 (ha\_link Standby): 192.168.91.2/24

Ethernet1/5 (dentro del modo de espera): 192.168.30.253/24
Ethernet1/6 (fuera del modo de espera): 192.168.40.253/24
Ethernet1/7 (diagnóstico en espera): 192.168.81.2/24

i. Navegue hasta **Dispositivos lógicos** > **Agregar autónomo**. Establezca la regla ACP para permitir el tráfico desde el interior al exterior.

Ę	Firewall Ma Policies / Acces	anagement C ss Control / Policy	Center Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	Q 🗳 🕸	🛿 admir	• -dod 080	SECU	IRE
•	acp-rule     Try New UI Layout ( Analyze Hit Counts Save Cancel     Enter Description																		
	Rules Security Intelligence HTTP Responses Logging Advanced Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy: None Identity Policy: None																		
Eit	er by Device	Search Rules											×	Show Rule Con	flicts 🛛 +	Add Catego	y +	Add Ru	le
	Name	Source Zones	Dest Zones	Source Networks	De	est Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	15 O G	A 🗆		¢
$\sim N$	landatory - acp-rule	(1-1)		_															
1	ftd_ha_acp	inside_zone	outside_zone	Any	A		Any	Any	Any	Any	Any	Any	Any	(Any:	C Allow	15. V. D	20	<b>D</b> • ,	1
~ D	efault - acp-rule (-)	)																	
The	ere are no rules in this section, Add Rule or Add Category																		

j. Despliegue el ajuste en FTD.

k. Confirmar estado de HA en CLI

El estado de HA para cada instancia también se confirma en la CLI de Firepower, que es igual que ASA.

Ejecute show running-config failover el show failover comando y confirme el estado de HA de FTD1\_FTD01 (Instancia principal01).

#### <#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

Ejecute show running-config failover el show failover comando y confirme el estado de HA de FTD1\_FTD11 (Instancia principal02).

#### <#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

Ejecute show running-config failover el show failover comando y confirme el estado de HA de FTD2\_FTD02 (Instancia secundaria01).

#### <#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-

Ejecute show running-config failover el show failover comando y confirme el estado de HA de FTD2\_FTD12 (Instancia secundaria02).

#### <#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. Confirmar el consumo de licencias

Todas las licencias se consumen por chasis/motor de seguridad y no por instancia de contenedor.

·Las licencias base se asignan automáticamente: una por motor/chasis de seguridad.

·Las licencias de funciones se asignan manualmente a cada instancia, pero solo se consume una licencia por función según el motor/chasis de seguridad. Para una licencia de función específica, solo necesita un total de 1 licencia, independientemente del número de instancias en uso.

Esta tabla muestra cómo se consumen las licencias en este documento.

FPR01	Instancia01	Básico, filtrado de URL, malware y amenazas
	Instancia02	Básico, filtrado de URL, malware y amenazas
FPR02	Instancia01	Básico, filtrado de URL, malware y amenazas
	Instancia02	Básico, filtrado de URL, malware y amenazas

Número total de licencias

Base	Filtrado de URL	Malware	Amenaza
2	2	2	2

Confirme el número de licencias consumidas en la GUI de FMC.

Smart Licenses			Filter Devices	×	Edit Performance Tier	Edit Licenses
License Type/Device Name	License Status	Device Type		Domain	Group	
∨ Base (2)	<ul> <li>In-Compliance</li> </ul>					^
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	<ul> <li>In-Compliance</li> </ul>	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	<ul> <li>In-Compliance</li> </ul>	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	
V Mabware (2)	In-Compliance					
FTD01_FTD02_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	<ul> <li>In-Compliance</li> </ul>	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	<ul> <li>In-Compliance</li> </ul>	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	
✓ Threat (2)	In-Compliance					
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	<ul> <li>In-Compliance</li> </ul>	High Availability - Cisco Firepower 4145 Thr	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 Thr	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	

Confirmar licencias consumidas

#### Verificación

Cuando se produce un crash en FTD1\_FTD01 (Instancia Primaria01), se dispara el failover de la Instancia01 y las interfaces de datos en el lado en espera se hacen cargo de la dirección IP/MAC de la Interfaz Activa original, asegurando que el tráfico (conexión FTP en este documento) sea pasado continuamente por Firepower.



Antes del desperfecto



Durante el desperfecto



Failover Activado

Paso 1. Inicie la conexión FTP de Win10-01 a Win10-02.

Paso 2. El show conn comando Run para confirmar la conexión FTP se ha establecido en Instance01.

// 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

Paso 3. Inicie la conexión FTP de Win10-03 a Win10-04.

Paso 4. El show conn comando Run para confirmar la conexión FTP se ha establecido en Instance02.

#### <#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

Paso 5. Ejecute connect ftd FTD01 y system support diagnostic-cli el comando para entrar en la CLI de ASA. Ejecute enable y el **crashinfo force watchdog** comando para forzar la caída de la Instancia01 en la unidad Primaria/Activa.

#### <#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]:
```

Paso 6. La conmutación por fallo se produce en Instance01 y la conexión FTP no se interrumpe. Ejecute show failover y show conn el comando para confirmar el estado de Instance01 en 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

Paso 7. El desperfecto ocurrido en Instance01 no tuvo ningún efecto en Instance02. Ejecute show failover y show conn el comando para confirmar el estado de Instance02.

#### <#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
```

Paso 8. Vaya a Devices > All en FMC. Confirme el estado de HA.

### ·FTD1\_FTD01: Principal, En espera

#### ·FTD2\_FTD02: Secundario, Activo

Fin Dev	ewall Management Center Overview Analysis	Policies Devices Object	s Integration	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>	pgrade (0)	Snort 3 (4)				Q, Search Device Add •
Collapse All								
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	Ungrouped (2)							
	<ul> <li>FTD01_FTD02_HA</li> <li>High Availability</li> </ul>							1
	FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	ERATING Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Ø	:
	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	4Q+	:
	V FTD11_FTD12_HA High Availability							11
	FTD1_FTD11(Primary, Active) Short 3	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	:
	FTD2_FTD12(Secondary, Standby) Short 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp+rule	4Ø	:

Confirmar estado de HA

Paso 9. (Opcional)Después de que el Instance01 de FPR01 vuelva a la normalidad, puede cambiar manualmente el estado de HA. Esto se puede

En FMC, navegue hasta Devices > All. Haga clic en Switch Active Peer para cambiar el estado de HA para FTD01\_FTD02\_HA.

En Fi	rewall Management Center Overview Analysis vices / Device Management	Policies Devices Obje	octs Integration	n			Deploy Q 🥥	admin      dede SECURE
View By: All (4)	Group         •           • Error (0)         • Warning (0)         • Offline (0)         • Normal (4)	Deployment Pending (0)	Upgrade (0)	9 Snort 3 (4)				Deployment History Q, Search Device Add
Collapse Al								
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	✓ Ungrouped (2)							
	FTD01_FTD02_HA High Availability							Switch Active Peer
	FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	ER4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4D	Force refresh node status Delete Revert Upgrade
	FTD2_FTD02(Secondary, Active) Snort 3     Snort 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	¢۵	Health Monitor Troubleshoot Files
	FTD11_FTD12_HA High Availability							/1
	FTD1_FTD11(Primary, Active) Snort 3     C.5m1.0.1 - Routed	Firepower 4145 with FTD	7.2.5	E Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:
	FTD2_FTD12(Secondary, Standby) Snort 3     Entrol.10.2 - Routed	Firepower 4145 with FTD	7.2.5	Erepower401G cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1

Estado de HA del switch

En Firepower CLI, ejecute connect ftd FTD01 y system support diagnostic-cli el comando para entrar en ASA CLI. Ejecute enable el **failover** active comando y cambie el HA para FTD01\_FTD02\_HA.

#### <#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

enable

firepower#

failover active

Troubleshoot

Para validar el estado de failover, ejecute show failover y show failover history ordene.

#### <#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 (2

>

#### show failover history

Ejecute el comando debug fover <option> para habilitar el registro de debug de failover.

#### <#root>

>

#### debug fover

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

#### Referencia

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

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).