Configuración de alta disponibilidad de FTD mediante FDM

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Topología de red
Configurar
Configuración de la unidad principal para alta disponibilidad
Configuración de la unidad secundaria para alta disponibilidad
Verificación

Introducción

Este documento describe cómo configurar un par de alta disponibilidad (HA) activo/en espera de defensa frente a amenazas de firewall (FTD) gestionado localmente.

Prerequisites

Requirements

Se recomienda tener conocimiento de estos temas:

• Configuración inicial de Cisco Secure Firewall Threat Defence mediante GUI o shell.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

• FPR2110 versión 7.2.5 administrada localmente por Firepower Device Manager (FDM)

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.

Topología de red



Nota: El ejemplo descrito en este documento es uno de los varios diseños de red recomendados. Refiérase a la guía de configuración <u>Evitar Failover Interrumpido y</u> <u>Enlaces de Datos</u> para obtener más opciones.



Configurar

Configuración de la unidad principal para alta disponibilidad

Paso 1. Haga clic en Device y presione el botón Configure ubicado en la esquina superior derecha, junto al estado High Availability.



Paso 2. En la página Alta disponibilidad, haga clic en el cuadro Dispositivo principal.

Firewall De	vice Manager	Monitoring	Ø Policies	글고 Objects	Device: ftd-primary		(ک		۲	?	:	admin Administrator	Ý	cisco 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. Primary Device or Secondary Device														

Paso 3. Configure las propiedades Failover Link.

Seleccione la interfaz que ha conectado directamente a su firewall secundario y establezca la dirección IP primaria y secundaria, así como la máscara de red de subred.

Marque la casilla de verificación Use the same interface as the Failover Link para el Stateful Failover Link.

Desactive el cuadro Clave de cifrado IPSec y haga clic en Activar HA para guardar los cambios.

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 (2)
Before you activate HA, make sure both devices have the same Smart License and Cloud Regio	on. Otherwise HA will not work.
When you click Activate HA, these settings are automatically deployed to the devi momentary traffic loss. It might take a few minutes for deployment to finish.	ce. 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.





Sugerencia: utilice una pequeña subred de máscaras, dedicada únicamente al tráfico de conmutación por fallo para evitar en la medida de lo posible las infracciones de seguridad o los problemas de red.



Advertencia: el sistema implementa inmediatamente la configuración en el dispositivo. No es necesario iniciar un trabajo de implementación. Si no ve ningún mensaje que indique que la configuración se ha guardado y la implementación está en curso, desplácese a la parte superior de la página para ver los mensajes de error. La configuración también se copia en el portapapeles. Puede utilizar la copia para configurar rápidamente la unidad secundaria. Para mayor seguridad, la clave de cifrado (si la define) no se incluye en la copia del portapapeles.

Paso 4. Una vez finalizada la configuración, aparece un mensaje que explica los siguientes pasos. Haga clic en Got It después de leer la información.

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	
 Paste it on the secondary device. Log into the secondary device and open the HA configuration page. 	
You are done! The devices should communicate and establish a high availability pair automatically.	
GOT IT	

Configuración de la unidad secundaria para alta disponibilidad

Paso 1. Haga clic en Device y presione el botón Configure ubicado en la esquina superior derecha, junto al estado High Availability.

Firewall Device Manager Monitoring	Policies Object:	s Device: ftd-secondary		adr	nin 🗸 🖞 讨 SECURE
Model Cisco Firepower 2110 Thr	Software eat Defense 7.2.5-208	VDB Intrusion Rule Update 0 370.0 20230925-1455	Cloud Services	High Availability @ C	ONFIGURE
FC Inside Network	Cisco Firepower 2110 Thr MGMT 1/1 CONSOLE 1/2	12 est Defense 1/3 1/5 1/7 1/9 1/11 1/13 1/ 1/13 1/ 1/14 1/5 1/8 1/11 1/15 1/7 1/9 1/11	/14 1/15 1/16	SP/WAN/Gateway	Internet DNS Server NTP Server Smart License

Paso 2. En la página Alta disponibilidad, haga clic en el cuadro Dispositivo secundario.

Firewall De	vice Manager	题 Monitoring	Ø Policies	詳正 Objects	Device: ftd-secondary	(2		9 ?	:	admin Administrator	× ·	diala SECURE
	Device Summary High Availat	bility											
	How High Avai	lability 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	Secondary De	evice	0					

Paso 3. Configure las propiedades Failover Link. Puede pegar los parámetros almacenados en el portapapeles después de configurar el FTD principal, o puede continuar manualmente.

Paso 3.1. Para pegar desde el portapapeles simplemente haga clic en el botón Pegar desde el portapapeles, pegue la configuración (presione las teclas Ctrl+v simultáneamente) y haga clic en Aceptar.

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: 10.1.1.1/255.255.255.252
StATEFUL FAILOVER LINK CONFIGURATION
Interface: Ethernet1/7
Primary IP: 10.1.1.1/255.255.255.252
Secondary IP: 10.1.1.2/255.255.255.252
```

Paso 3.2. Para continuar manualmente, seleccione la interfaz que ha conectado directamente a su firewall secundario y establezca la dirección IP primaria y secundaria, así como la máscara de red de subred. Marque la casilla de verificación Use the same interface as the Failover Link para el Stateful Failover Link.

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 ka features, both devices will become ac	ey with inconsistent settings for export controlled tive after you activate HA. Learn More (2
 Before you activate HA, make sure both devices have When you click Activate HA, these settings at momentary traffic loss. It might take a few might take a few might be a few m	the same Smart License and Cloud Reginer re 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 deployment to finish.		
 Information is copied to the clipboard when one 	leployment is done. You must allow	the browser to access your clipboard	for the copy to be successful.
	ACTIV	ИАТЕ НА	

Paso 4. Desactive el cuadro Clave de cifrado IPSec y haga clic en Activar HA para guardar los cambios.



Advertencia: el sistema implementa inmediatamente la configuración en el dispositivo. No es necesario iniciar un trabajo de implementación. Si no ve ningún mensaje que indique que la configuración se ha guardado y la implementación está en curso, desplácese a la parte superior de la página para ver los mensajes de error.

Paso 5. Una vez finalizada la configuración, aparece un mensaje en el que se explican los siguientes pasos que debe realizar. Haga clic en Got It después de leer la información.

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	
 Paste it on the secondary device. Log into the secondary device and open the HA configuration page. 	
You are done! The devices should communicate and establish a high availability pair automatically.	
GOT IT	

Verificación

 En este momento, el estado del dispositivo indica que se trata del dispositivo secundario de la página Alta disponibilidad. Si la unión con el dispositivo principal se realizó correctamente, el dispositivo comienza a sincronizarse con el dispositivo principal y, finalmente, el modo cambia a En espera y el par a Activo.

	This device is part (of a high availability (HA) pair and is currently in standby state. With few exceptions, yo To make any changes, please log into the active unit. <u>Learn More</u>	ou cannot edit the configuration for this device. $t^{\rm C}$
Firewall Device Manager	Monitoring Policies Objects	Device: ftd-primary	admin v studio SECURE
	Model Cisco Firepower 2110 Threat	Software VDB Intrusion Rule Update Cloud Services Defense 7.2.5-208 370.0 20230925-1455 🥏 Connected SEC TAC	High Availability Secondary Device: Standby \vec{c}^2 Peer: Active
	Fairle Network	1/2 Cisco Firepower 2110 Threat Defense MGMT 1/1 1/3 1/5 1/7 1/9 1/11 MGMT 1/1 1/3 1/10 1/12 1/11 1/15 CONSOLE 1/2 1/10 1/12 SFP 1/11	Internet DNS Server ISP/WAN/Gateway Contro Server Category Smart License

• El FTD principal debe mostrar también el estado Alta disponibilidad, pero como Activo y Par: En espera.

Firewall Device Manager Monitori	ng Policies Objects Devi	ce: ftd-primary). 🖨 Ø	? : admin Administrator · the SECURE
	Model Cisco Firepower 2110 Threat Defense	Software VD8 Intrusion Rule Update 7.2.5-208 370.0 20230925-1455	Cloud Services High Ava Connected SEC TAC Primary I	lability Device: Active
	Cisco Fi	1/2 repower 2110 Threat Defense 0		Internet DNS Server
	toside Network	MOMT 1/1 1/2 1/5 1/7 1/9 1/11 Image: Console Image: Console <th< td=""><td>/13 1/14 1/15 1/16</td><td>N/Gateway NTP Server</td></th<>	/13 1/14 1/15 1/16	N/Gateway NTP Server
		171		

• Abra una sesión SSH al FTD primario y ejecute el comando show running-config failover para verificar la configuración.



• Valide el estado actual del dispositivo con el comando 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 se	t							
>								

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).