Configura elevata disponibilità FTD tramite FDM

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Topologia della rete
Configurazione
Configurare l'unità primaria per l'alta disponibilità
Configurare l'unità secondaria per l'alta disponibilità
Verifica

Introduzione

In questo documento viene descritto come configurare una coppia HA (High Availability) attiva/standby di Secure Firewall Threat Defense (FTD) gestita localmente.

Prerequisiti

Requisiti

È consigliabile conoscere i seguenti argomenti:

• Configurazione iniziale di Cisco Secure Firewall Threat Defense tramite GUI e/o shell.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

• FPR2110 versione 7.2.5 gestito localmente da Firepower Device Manager (FDM)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Topologia della rete



Nota: l'esempio descritto in questo documento è uno dei numerosi progetti di rete consigliati. Per ulteriori informazioni, consultare la guida alla configurazione per <u>evitare</u> <u>failover interrotto e collegamenti dati</u>.



Configurazione

Configurare l'unità primaria per l'alta disponibilità

Passaggio 1. Fare clic su Device (Dispositivo) e premere il pulsante Configure (Configura) situato nell'angolo in alto a destra, accanto allo stato High Availability (Alta disponibilità).



Passaggio 2. Nella pagina Alta disponibilità fare clic sulla casella Dispositivo principale.

Firewall Dev	ice Manager	Monitoring	Ø Policies	註王 Objects	Device: ftd-primary	_	(Σ)	٢	0	?	:	admin Administrator	Ý	eisco SECURE
	Device Summary High Availa	bility												
	How High Ava	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 or	Secondary	Device	0						

Passaggio 3. Configurare le proprietà Collegamento di failover.

Selezionare l'interfaccia connessa direttamente al firewall secondario e impostare l'indirizzo IP primario e secondario nonché la subnet netmask.

Selezionare la casella di controllo Utilizza la stessa interfaccia del collegamento di failover per il collegamento di failover stateful.

Deselezionare la casella Chiave di crittografia IPSec e fare clic su Attiva HA per salvare le modifiche.

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.





Suggerimento: utilizzare una subnet mask di piccole dimensioni, dedicata esclusivamente al traffico di failover per evitare violazioni della sicurezza e/o problemi di rete il più possibile.



Avviso: la configurazione viene distribuita immediatamente nel dispositivo. Non è necessario avviare un processo di distribuzione. Se non viene visualizzato un messaggio che indica che la configurazione è stata salvata e che la distribuzione è in corso, scorrere fino alla parte superiore della pagina per visualizzare i messaggi di errore. La configurazione viene copiata anche negli Appunti. È possibile utilizzare la copia per configurare rapidamente l'unità secondaria. Per una maggiore protezione, la chiave di crittografia (se ne è stata impostata una) non è inclusa nella copia negli Appunti.

Passaggio 4. Al termine della configurazione, viene visualizzato un messaggio in cui vengono illustrati i passaggi successivi. Fare clic su Scarica dopo aver letto le informazioni.

You have successfully deployed the HA configuration on the primary device. What's next? I need to configure Peer Device I configured both devices	×
1 Copy the HA configuration to the clipboard.	
 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	

Configurare l'unità secondaria per l'alta disponibilità

Passaggio 1. Fare clic su Device (Dispositivo) e premere il pulsante Configure (Configura) situato nell'angolo in alto a destra, accanto allo stato High Availability (Alta disponibilità).

Firewall Device Manager Monitoring	Policies Objects	Bevice: ftd-secondary	>	@ ? :	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	
Finiside Network	Cisco Firepower 2110 Three MONT 1/1 CONSOLE 1/2	172 sat Defense 1/3 1/5 1/7 1/9 1/11 1/4 1/6 1/8 1/10 1/12 St 1/4 1/6 1/8 1/10 1/12 St	13 1/14 1/15 1/16	ISP/WAN/Gateway	DNS Server DNS Server NTP Server dece Smart License	

Passaggio 2. Nella pagina Alta disponibilità fare clic sulla casella Periferica secondaria.

Firewall De	vice Manager	1回 Monitoring	Ø Policies	計正 Objects	Device: ftd-secondary	(96	0	?	:	admin Administrator	v ·	diala SECURE
	Device Summary High Availabil	lity											
	How High Availa	bility 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													

Passaggio 3. Configurare le proprietà Collegamento di failover. È possibile incollare le impostazioni memorizzate negli Appunti dopo aver configurato l'FTD principale oppure continuare manualmente.

Passaggio 3.1. Per incollare dagli Appunti, fare clic sul pulsante Incolla dagli Appunti, incollare nella configurazione (premere contemporaneamente i tasti Ctrl+v) e fare clic su 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: 10.1.1.1/255.255.255.252

Secondary IP: 10.1.1.2/255.255.255.252

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
```

Passaggio 3.2. Per procedere manualmente, selezionare l'interfaccia connessa direttamente al firewall secondario e impostare l'indirizzo IP primario e secondario nonché la subnet netmask. Selezionare la casella di controllo Utilizza la stessa interfaccia del collegamento di failover per il collegamento di failover stateful.

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		Type IPv4 IPv6	
Primary IP		Primary IP	
10.1.1.1		10.1.1.1	
Secondary IP 10.1.1.2		Secondary IP 10.1.1.2	
e.g. 192.168.10.2		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 includ clipboard when you activate HA. You will need to manually enter the key when you configure	ed 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 🕑
Before you activate HA, make sure both devices hav	e the same Smart License and Cloud Regi	ion. Otherwise HA will not work.	
when you click Activate HA, these settings a momentary traffic loss. It might take a few m	re automatically deployed to the dev nutes for deployment to finish.	vice. The deployment might restart insp	pection engines, which can result in the
Information is copied to the clipboard when a	deployment is done. You must allow	the browser to access your clipboard	for the copy to be successful.
	ACTIV	ATE HA	

Passaggio 4. Deselezionare la casella Chiave di crittografia IPSec e fare clic su Attiva HA per salvare le modifiche.



Avviso: la configurazione viene distribuita immediatamente nel dispositivo. Non è necessario avviare un processo di distribuzione. Se non viene visualizzato un messaggio che indica che la configurazione è stata salvata e che la distribuzione è in corso, scorrere fino alla parte superiore della pagina per visualizzare i messaggi di errore.

Passaggio 5. Al termine della configurazione, viene visualizzato un messaggio in cui vengono illustrati i passaggi successivi da eseguire. Fare clic su Scarica dopo aver letto le informazioni.

the	You have successfully deployed HA configuration on the primary device. What's next? eed to configure Peer Device I configured both devices	×
	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	
	GOT IT	

Verifica

 A questo punto lo stato del dispositivo indica che si tratta del dispositivo secondario nella pagina Alta disponibilità. Se l'unione con il dispositivo primario ha esito positivo, il dispositivo inizia a sincronizzarsi con il dispositivo primario e alla fine la modalità viene modificata in Standby e il peer in Attivo.

	1) 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 the SECURE
	High Availability Secondary Device: Standby 🛛 🤃 Peer: Active		
	Finiside Network	MARY 1/1 1/3 1/5 1/7 1/9 1/11 MARY 1/1 1/16 1/10 1/12 5FP COMBOLE 1/2 1/10 1/12 5FP	Internet

 L'FTD principale visualizza in genere anche lo stato Alta disponibilità, ma come Attivo e Peer: Standby.



• Aprire una sessione SSH sull'FTD primario e usare il comando show running-config failover per verificare la configurazione.



• Convalidare lo stato corrente del dispositivo con il 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 set									
>									

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).