FTD hoge beschikbaarheid configureren met FDM

Inhoud
Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Netwerktopologie
Configureren
De primaire eenheid voor hoge beschikbaarheid configureren
De secundaire eenheid configureren voor hoge beschikbaarheid
Verifiëren

Inleiding

In dit document wordt beschreven hoe u een actief/stand-by (HA) paar Secure Firewall Threat Defence (FTD) kunt instellen dat lokaal wordt beheerd.

Voorwaarden

Vereisten

Aanbevolen wordt kennis van deze onderwerpen te hebben:

• De eerste configuratie van Cisco Secure Firewall Threat Defence via GUI en/of shell.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

• FPR210 versie 7.2.5 lokaal beheerd door Firepower Device Manager (FDM)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerktopologie



Opmerking: het voorbeeld in dit document is een van de meerdere aanbevolen netwerkontwerpen. Raadpleeg de configuratiehandleiding <u>Onderbroken failover en</u> <u>datalink vermijden</u> voor meer opties.



Configureren

De primaire eenheid voor hoge beschikbaarheid configureren

Stap 1. Klik op Apparaat en druk op de knop Configureren rechtsboven, naast de status Hoge beschikbaarheid.



Stap 2. Klik op de pagina Hoge beschikbaarheid op het vakje Primair apparaat.

Firewall De	vice Manager	Monitoring	Ø Policies	章王 Objects	Device: ftd-primary	_	(>)	٢	0	?	:	admin Administrator	v	cisco SECU	RE
	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	rimary Device	Secondary	/ Device	0							

Stap 3. De eigenschappen van de failover link configureren.

Selecteer de interface die u rechtstreeks met uw secundaire firewall hebt verbonden en stel het primaire en secundaire IP-adres en het subnetmasker in.

Controleer Gebruik dezelfde interface als het aankruisvakje failover link voor de stateful failover link.

Schakel het vakje IPSec Encryption Key uit en klik op Activate HA om de wijzigingen op te slaan.

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.





Tip: gebruik een klein maskersubnetje, dat alleen bestemd is voor failover-verkeer om beveiligingslekken en/of netwerkproblemen zoveel mogelijk te voorkomen.



Waarschuwing: het systeem implementeert de configuratie onmiddellijk op het apparaat. U hoeft geen implementatietaak te starten. Als u geen bericht ziet dat aangeeft dat uw configuratie is opgeslagen en de implementatie is gestart, scrolt u naar de bovenkant van de pagina om de foutmeldingen te zien. De configuratie wordt ook naar het klembord gekopieerd. U kunt met deze kopie de secundaire eenheid snel configureren. Voor extra veiligheid is de coderingssleutel (als u deze instelt) niet opgenomen in het exemplaar van het klembord.

Stap 4. Nadat de configuratie is voltooid, ontvangt u een bericht waarin de volgende stappen worden uitgelegd. Klik na het lezen van de informatie op Got It.

t	he H	You have successfully deployed A configuration on the primary device. What's next?	×
(1	Copy the HA configuration to the clipboard.	
(2	Paste it on the secondary device. Log into the secondary device and open the HA configuration page.	
(\checkmark	You are done! The devices should communicate and establish a high availability pair automatically.	1
		бот п	

De secundaire eenheid configureren voor hoge beschikbaarheid

Stap 1. Klik op Apparaat en druk op de knop Configureren rechtsboven, naast de status Hoge beschikbaarheid.

Firewall Device Manager Monitoring	Ø [™]	1 Device: ftd-secondary	>	@ ? :	admin Administrator	cisco SECURE
Model Cisco Firepower 2110 Thr	Software V eat Defense 7.2.5-208 3	VDB Intrusion Rule Update 370.0 20230925-1455	Cloud Services Connected SEC TAC	High Availability () Not Configured	CONFIGURE	
FC Inside Network	Cisco Firepower 2110 Threat De MGMT 1/1 1/3 CONSOLE 1/2 1/4		a 1/14 1/15 1/16	ISP/WAN/Gateway	Internet DNS Server ONP Server down Smart License	

Stap 2. Klik op de pagina Hoge beschikbaarheid op het vakje Secundair apparaat.

Firewall De	vice Manager	题 Monitoring	Ø Policies	註王 Objects	Device: ftd-secondary	©.		0	?	:	admin Administrator	~ :	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												

Stap 3. De eigenschappen van de failover link configureren. U kunt de instellingen die zijn opgeslagen op uw klembord plakken na het configureren van de primaire FTD, of u kunt handmatig doorgaan.

Stap 3.1. Als u van het klembord wilt plakken, klikt u eenvoudig op de knop Plakken vanaf het klembord, plakt u in de configuratie (drukt u op toetsen Ctrl+v tegelijkertijd) en klikt u op 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
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
```

Stap 3.2. Om handmatig verder te gaan, selecteert u de interface die u rechtstreeks heeft verbonden met uw secundaire firewall en stelt u het primaire en secundaire IP-adres in evenals het subnetmasker Netmasker. Controleer Gebruik dezelfde interface als het aankruisvakje failover link voor de 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 Failover 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		Secondary IP					
10.1.1.2		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 include clipboard when you activate HA. You will need to manually enter the key when you configure	rd in the configuration copied to the HA on the peer device.	IMPORTANT If you configure an IPsec encryption ke features, both devices will become ac	iy with inconsistent settings for export controlled live after you activate HA. Learn More (2				
 Before you activate HA, make sure both devices have the same Smart License and Cloud Region. Otherwise HA will not work. When you click Activate HA, these settings are automatically deployed to the device. The deployment might restart inspection engines, which can result in the manual term in the manual term in the formal term in the formal term. 							
momentary tranic loss, it might take a few mi	notes for deproyment to finish.						
Information is copied to the clipboard when o	leployment is done. You must allow	the browser to access your clipboard	for the copy to be successful.				
	ACTIV	IATE HA					

Stap 4. Schakel het vakje IPSec Encryption Key uit en klik op Activate HA om de wijzigingen op te slaan.



Waarschuwing: het systeem implementeert de configuratie onmiddellijk op het apparaat. U hoeft geen implementatietaak te starten. Als u geen bericht ziet dat aangeeft dat uw configuratie is opgeslagen en de implementatie is gestart, scrolt u naar de bovenkant van de pagina om de foutmeldingen te zien.

Stap 5. Nadat de configuratie is voltooid, ontvangt u een bericht waarin de volgende stappen worden uitgelegd die u moet nemen. Klik na het lezen van de informatie op Got It.

You have successfully deployed the HA configuration on the primary device. What's next?	×
Copy the HA configuration to the clipboard. Copied Click here to copy again	
 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	

Verifiëren

 Op dit punt geeft uw apparaatstatus meestal aan dat dit het secundaire apparaat is op de pagina Hoge beschikbaarheid. Als de verbinding met het primaire apparaat succesvol was, begint het apparaat te synchroniseren met het primaire apparaat, en uiteindelijk wordt de modus veranderd in Standby en de peer in Active.

	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	Internet DNS Server ISP/WAN/Gateway Contro Server Category Smart License	

• De primaire FTD toont de status van hoge beschikbaarheid ook, maar als Active en Peer: Standby.

Firewall Device Manager	Monitoring Policies Objects	Device: ftd-primary) (7) : admin Administrator ~ "tisto SECURE
	Model Clsco Firepower 2110 Threat Def	Software VDB Intrusion Rule Update Cloud Services nse 7.2.5-208 370.0 20230925-1455 🥏 Connected SEC TAC	High Availability Primary Device: Active \vec{c}^2 Peer: Standby
	Co Inside Network	22 co Firepower 2110 Threat Defense © Moart 1/1 1/2 1/5 1/7 1/9 1/11 © 00NOOLE 1/2 1/4 1/15 1/16 [2] [2] [2] [2] [2] [2] [2] [2] [2] [2]	Internet DNS Server ISP/WAN/Gateway ONTP Server Control Smart License

• Open een SSH-sessie voor de primaire FTD en geef de opdracht show in werking steltconfiguratie failover om de configuratie te verifiëren.



• Valideren van de huidige status van het apparaat met de opdracht toont failover status.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.