Configurazione di FTD Multi-Instance Highavailability su Firepower 4100

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Esempio di rete
Configurazioni
Passaggio 1. Interfacce pre-configurate
Passaggio 2. Aggiungere 2 profili di risorse per le istanze del contenitore.
Passaggio 3. (Facoltativo) Aggiungere un prefisso del pool MAC dell'indirizzo MAC virtuale per le interfacce dell'istanza del contenitore.
Passaggio 4. Aggiungere un'istanza autonoma.
Passaggio 5. Configurazione interfacce
Passaggio 6. Aggiungere Una Coppia Di Disponibilità Elevata Per Ogni Istanza.
<u>Verifica</u>
Risoluzione dei problemi
Riferimento

Introduzione

In questo documento viene descritto come configurare il failover nelle istanze del contenitore FTD (a più istanze).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Firepower Management Center e Firewall Threat Defense.

Componenti usati

Cisco Firepower Management Center Virtual 7.2.5 Appliance Cisco Firepower 4145 NGFW (FTD) 7.2.5 Firepower eXtensible Operating System (FXOS) 2.12 (0.498) Windows 10

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.

Prima di distribuire FTD Multi-Instance, è importante capire come può influire sulle prestazioni del sistema e pianificare di conseguenza. Per garantire un'installazione e una configurazione ottimali, consultare sempre la documentazione ufficiale Cisco o un rappresentante tecnico Cisco.

Premesse

Multi-Instance è una funzione di Firepower Threat Defense (FTD) simile alla modalità a contesto multiplo ASA. Consente di eseguire più istanze di FTD di contenitori separati su un singolo componente hardware. Ogni istanza contenitore consente la separazione delle risorse hardware, la gestione di configurazione separata, ricaricamenti separati, aggiornamenti software separati e il supporto completo delle funzionalità di difesa dalle minacce. Ciò è particolarmente utile per le organizzazioni che richiedono criteri di sicurezza diversi per reparti o progetti diversi, ma che non desiderano investire in più appliance hardware separate. La funzione Multi-Instance è attualmente supportata sulle appliance di sicurezza Firepower serie 4100 e 9300 con FTD 6.4 e versioni successive.

In questo documento viene utilizzato Firepower4145, che supporta al massimo 14 istanze di contenitore. Per il numero massimo di istanze supportate in Firepower Appliance, vedere <u>Numero</u> <u>massimo di istanze del contenitore e di risorse per modello.</u>

Esempio di rete

Questo documento introduce la configurazione e la verifica di HA in istanze multiple in questo diagramma.



Diagramma di configurazione logica



Diagramma configurazione fisica

Configurazioni

Passaggio 1. Interfacce pre-configurate

a. Passare a Interfacce su FCM. Impostare 2 interfacce di gestione. Nell'esempio, Ethernet1/3 e Ethernet1/7.

Overview Interfac	es Logical Devices	Security Engine	Platform Settings						Syste	m Tools Help	admin
			Vetwork Module 1	5 7 5 8	ietwork Module 2 :	Empty	Network Module 3 : Em	spty			
All Interfaces Hardwa	ire Bypass								O Add Ne	w • Filter.	×
Interface	Туре	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State		
MGMT	Management										
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down	()X)	J 🗄	
Ethernet1/1	data	1gbps	lgbps			Full Duplex	yes	up		0	
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		ø	
Ethernet1/6	data	1gbps	1gbps			Full Duplex	yes	up		Ø	
Ethernet1/7	mgmt	1gbps	lgbps			Full Duplex	yes	up		ø	
Ethernet1/8	data	1gbps	1gbps			Full Duplex	yes	up		ø	

Interfacce pre-configurate

Passaggio 2. Aggiungere 2 profili di risorse per le istanze del contenitore.

a. Passare a Impostazioni piattaforma > Profili risorse > Aggiungi a FCM. Impostare il primo profilo risorsa.

Nell'esempio: ·Nome: Instance01 ·Numero di core: 10



Nota: per la disponibilità elevata della coppia di istanze del contenitore, è necessario che utilizzino gli stessi attributi del profilo della risorsa.

Impostare il nome del profilo tra 1 e 64 caratteri. Si noti che non è possibile modificare il nome di questo profilo dopo averlo aggiunto.

Impostare il numero di core per il profilo, tra 6 e il massimo.

Overview Interfaces Logi	cal Devices Security Engine	Platform Settings			System Tools Help admin
NTP SSH				O Add	
SNMP	Name	Description	Cores		
HTTPS AAA Syslog DNS FIPS and Common Criteria	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	<i>2</i> 3	
Access List		Add Resource Profile			
MAC Pool Resource Profiles		Name: * Instance01			
Network Control Policy Chassis URL		Description: Number of Cores:* 10 Range: 6 to 86 Specify even value for number of cores.			
		OK. Cancel			

b. Ripetere a. nel passo 2, per configurare il secondo profilo di risorsa.

Nell'esempio: ·Nome: Instance02 ·Numero di core: 20

Overview Interfaces Logic	al Devices Security Engine Pla	atform 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	48	
DNS					
FIPS and Common Criteria		Add Bessures Brofile			
Access List		Add Resource Profile			
MAC Pool		Name: * Instance02			
 Resource Profiles 		Description:			
Network Control Policy					
Chassis UKL		Number of Cores:* 20 Range: 6 to 86			
		Specify even value for number of cores.			
		OK Cancel			

Aggiungi secondo profilo risorse

c. Verificare che 2 profili di risorse siano stati aggiunti correttamente.

Over	view Interfaces Logi	al Devices	Security Engine	Platform Settings							S	stem	Tools I	telp a	idmin
NT	P														
SS	н								0	A00					
SN	MP	Name			Description			Cores							
HT	TPS	Default	-Small		Auto-created	application resource-profile with 6 cp	pu-cores	6		6					
Sv	slog	Instand	:e01					10		28					
DN	s														
FIF	S and Common Criteria	Instanc	eo2					20		6					
Acc	cess List														
MA	C Pool														
Re	source Profiles														
Ne	twork Control Policy														
Ch	assis URL														

Conferma profilo risorsa

Passaggio 3. (Facoltativo)Aggiungere un prefisso del pool MAC dell'indirizzo MAC virtuale per le interfacce dell'istanza del contenitore.

È possibile impostare manualmente l'indirizzo MAC virtuale per l'interfaccia attiva/standby. Se gli indirizzi MAC virtuali non sono impostati per la funzionalità multi-istanza, lo chassis genera automaticamente indirizzi MAC per le interfacce di istanza e garantisce che un'interfaccia condivisa in ciascuna istanza utilizzi un indirizzo MAC univoco.

Per ulteriori dettagli sull'indirizzo MAC, selezionare <u>Aggiungi prefisso pool MAC e Visualizza</u> <u>indirizzi MAC</u> per <u>interfacce istanze contenitore</u>.

Passaggio 4. Aggiungere un'istanza autonoma.

a. Selezionare Logical Devices > Add Standalone. Impostare la prima istanza.

Nell'esempio: ·Nome dispositivo: FTD01

·Tipo di istanza: contenitore



Nota: l'unico modo per distribuire un'applicazione contenitore consiste nella predistribuzione di un'istanza dell'applicazione con il tipo di istanza impostato su Container. Assicurarsi di selezionare Container.

Non è possibile modificare questo nome dopo aver aggiunto la periferica logica.

Overview Interfaces Logical Devices Security Er	gine Platform Settings			System Tools Help
Logical Device List	(0 instances) 100% (86 of 86) Co	ores Available		C Refresh Add
No logical devices available. Click on Add Device to add a new logical d	rice.			
	Add Standalone		(T)(X)	
	Device Name:	FTD01	_	
	Template:	Cisco Secure Firewall Threat Defense	*	
	Image Version:	7.2.5.208	¥	
	Instance Type:	Container	×	
	 Before you add the security my formatting. You 	the first container instance, you must reinit idule/engine so that the disk has the correct i only need to perform this action once.	lize	
		ок	ancel	

Aggiungi istanza

Passaggio 5. Configurazione interfacce

a. Impostare Resource Profile, Management Interface (Interfaccia di gestione), Management IP (IP di gestione) per Instance01.

Nell'esempio:

Profilo risorsa: istanza01
Interfaccia di gestione: Ethernet1/3
ManagementIP: 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 Firewali Threat Defense - Bootstrap Configuration 🖭	Save Cancel
Data Ports	General Information Settings Agreement	
EBhernet1/1 Ethernet1/2 Ethernet1/6 Ethernet1/6 Ethernet1/8	SM 1 - 86 Cores Available Resource Profile: Instance01 Interface Information Management Interface: Ethernet1/3 Address Type: IPv4 Management IP: If-0.100 Network Mask: 255.0.0.0 Network Gateway: I^^	
Application Version Resource Profile	irt Status	
➡ FTD 7.2.5.208		
	OK Cancel	

Configurazione profilo/interfaccia di gestione/IP di gestione

b. Interfacce dati set.

Nell'esempio:

·Ethernet1/1 (per l'interno)

```
·Ethernet1/2 (per uso esterno)
```

·Ethernet1/4 (utilizzato per il collegamento HA)

(Overview Interfaces	Logical Device	s Security Engine Platform S	ettings				System Tools Help admin
	Provisioning - FTD01 Standalone Cisco See	cure Firewall Threat	Defense 7.2.5.208					Save Cancel
	Data Ports Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/6 Ethernet1/8			Ether Ether	net1/1 net1/2 net1/4	FTD - 7.2.5.20 Ethernet1/3 Click to configure	8	
	Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status	
G	FTD Interface Name Ethernet1/1 Ethernet1/2	7.2.5.208	InstanceOl	1.1000 1 Type data data data	1.(Ethernet1/3		

Imposta interfacce dati

c. Passare a Dispositivi logici. In attesa dell'avvio dell'istanza.

(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 Avail	able			C Refresh 🖉 Add •
	FTD01			Standalone	Status:ok					2 I
	Applicat	tion	Version	Resource F	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01		1	1	Ethernet1/3	😽 Installing	💷 🎘 C 🕍

Conferma stato dell'istanza 01

d. Ripetere a. nel passo 4.a e dal passo 5.a al passo 5.c per aggiungere la seconda istanza e impostare i dettagli per essa.

Nell'esempio:

•Nome dispositivo : FTD11 •Tipo di istanza : Contenitore

Profilo risorse: Istanza02
Interfaccia di gestione : Ethernet1/7
ManagementIP : x.x.10.1

·Ethernet1/5 = interno

·Ethernet1/6 = esterno

·Ethernet1/8 = collegamento HA

e. Confermare che 2 istanze siano in linea su FCM.

Overview In	nterfaces Logical Devices	Security Engine	Platform Settings				System Tools Help admin
Logical Device	List	(3	2 Container instances) 66% (56 of 86) Cor	res Available			C Refresh 🔘 Add -
FTD11		Standalone	Status:ok				
Application	on Version	Resource Pr	rofile Management IP	Gateway	Management Port	Status	
I FTD	7.2.5.208	Instance02	.10.1	1/1.1.111	Ethernet1/7	Online	💌 🕅 C 🔬
FTD01		Standalone	Status: ok				2 I
Application	on Version	Resource Pr	rofile Management IP	Gateway	Management Port	Status	
FTD FTD	7.2.5.208	Instance01	Chitani	1.0	Ethernet1/3	Online	🚾) 🌆 c 🕍

Conferma Stato Istanza Nel Dispositivo Principale

f. (Facoltativo)Esegui scope ssa scope slot 1 e show app-Instance comando per confermare che 2 istanze sono in linea sulla CLI di 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 Deploy online 7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTDD1 Instance is Online ftd FTDD11 online 7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online

g. Eseguire la stessa operazione sul dispositivo secondario. Confermare che 2 istanze sono in linea.

0\	erview	Interfaces	Logical Devices	Security Engine	Platform Setting	gs				System Tools Help admin
Logi	cal Devio	e List			(2 Container instanc	xes) 66% (56 of 86) Cor	es Available			C Refresh 🕢 Add •
C	FTD12			Standalone	Status:ok					2 I
	Applicat	ion	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
۲	FTD		7.2.5.208	Instance02]		1.	Ethernet1/7	Online	💌 🕅 🐋
E	FTD02			Standalone	Status:ok					1
	Applicat	ion	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
۲	FTD		7.2.5.208	Instance01]		1.6	Ethernet1/3	Online	💌 🏹 C 🕍

Conferma stato istanza nel dispositivo secondario

Passaggio 6. Aggiungere Una Coppia Di Disponibilità Elevata Per Ogni Istanza.

a. Selezionare **Dispositivi** > **Aggiungi dispositivo** su FMC. Aggiungere tutte le istanze a FMC.

Nell'esempio:

Nome visualizzato per Instance01 di FTD1: FTD1_FTD01
Nome visualizzato per Instance02 of FTD1: FTD1_FTD11
Nome visualizzato per Instance01 di FTD2: FTD2_FTD02
Nome visualizzato per Instance02 of FTD2 : FTD2_FTD12

Nell'immagine è illustrata l'impostazione per FTD1_FTD01.

Firewall Management Center Overview Analyse Devices / Device Management	Add Device	0		Deploy Q 🌘	🖗 🐼 🙆 admin 🔹	esce SECURE
View By: Group ▼ All (0) ● Error (0) ● Warring (0) ■ Offine (0) ● Normal (Colleme All	CDO Managed Device				Deploy	ment History
Name	Display Name: FTD1_FTD01 Registration Key:*	ł	Licenses	Access Control Policy	Auto RollBack	
		n.				
	Cancel Register	•				

Aggiungi istanza FTD a FMC

b. Confermare che tutte le istanze siano normali.

Firewall Management Center Devices / Device Management	Overview Analysis Policies Devices Objects	Integration			Deploy	Q 🙆 🔅 🕲 admin 🔹	dede SECURE
View By: Group						Deploy	yment History
All (4) • Error (0) • Warning (0)	Offline (0) Normal (4) Deployment Pending (0) Upgr	ade (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	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acpinule	49	1
C PTD1_FTD11 Snort 3 Stats.10.1 + Routed	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1
FTD2_FTD02 Snort 3 Crru-0.1.2 - Routed	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4©	11
FTD2_FTD12 Snort 3	Firepower 4145 with FTD	7.2.5	Encycle Content (Container)	Base, Threat (2 more)	acp-rule	49	1:

Conferma stato istanza in FMC

c. Passare a **Dispositivi** > **Aggiungi alta disponibilità**. Impostare la prima coppia di failover.

Nell'esempio:

·Nome: FTD01_FTD02_HA

·Peer primario : FTD1_FTD01



Nota: assicurarsi di selezionare l'unità corretta come unità principale.

Firewall Management Center Overview Analysis Pr 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) • E	Deployment Pending (0)	(0) • Snort 3 (4)				Q, Search Device	Add 🔻
Collapse All							
Name	Model	Version Chass	ssis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)		Add High Availabil	ility Pair 🛛				
FTD1_FTD01 Secent 3	Firepower 4145 with FTD	Name:* FTD01_FTD02_H4		Base, Threat (2 more)	acp-rule	4Ç9	1
FTD1_FTD11_Snort 3	Firepower 4145 with FTD	Device Type: Firewall Threat Defense	nse v	Base, Threat (2 more)	acp-rule	43	1
FTD2_FTD02_Sect 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	4Ş	×1
		Threat Defense High configuration. Licens converted to their his on both peers.	h Availability pair will have primary nses from primary peer will be high availability versions and applied				
			Cancel Continue				

Aggiungi prima coppia di failover

d. Impostare IP per il collegamento di failover nella prima coppia di failover.

Nell'esempio:

·Collegamento ad alta disponibilità: Ethernet1/4

·Collegamento stato: Ethernet1/4

·IP primario: 192.168.90.1/24

·IP secondario: 192.168.90.2/24

Firewall Management Center Overview Analysis Devices / Device Management	s Policies (Devices Objects Integration		Deploy	९ 😑 🌣 😝 admin •	deades SECURE
Mexilia 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 Dale		Access Control Policy	Auto RollBack	
Ungrouped (4)		Add high Availability Fail	0			
		High Availability Link	State Link			
FTD1_FTD01 Snort 3 I 1 - 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		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			

Impostare l'interfaccia HA e l'indirizzo IP per la prima coppia di failover

e. Confermare lo stato del failover

·FTD1_FTD01: primario, attivo

·FTD2_FTD02: secondario, standby

Fire Device	ewall Management Center Overview Analysis ces / Device Management	Policies Devices Object	s Integration				Deploy Q 🥝	O admin duals cesce SE	CURE
View By:	Group +							Deployment Hist	tory
All (4)	Error (0) Warning (0) Offline (0) Normal (4)	 Deployment Pending (0) 	pgrade (0)	Snort 3 (4)				Q, Search Device	dd 🔻
Collapse All									
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack		
	Ungrouped (3)								
0	FIDD1_FIDD2_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	40	1	
	FTD2_FTD02(Secondary, Standby) Short 3 FT3.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	۹Ø	I	
	FTD1_FTD11 Short 3	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	Firepower4KHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	*Ø	11	

Confermare Lo Stato Della Prima Coppia Di Failover

f. Selezionare Devices > Click FTD01_FTD02_HA (in questo esempio) > Interfaces. Imposta IP attivo per interfaccia dati.

Nell'esempio:

·Ethernet1/1 (interna) : 192.168.10.254/24

·Ethernet1/2 (esterno) : 192.168.20.254/24

·Ethernet1/3 (diagnostica) : 192.168.80.1/24

L'immagine mostra l'impostazione per l'IP attivo di Ethernet1/1.

Firewall Management Center Ov Devices / Secure Frewall Interfaces	verview Analysis P	olicies Devices Objects Integration				Deploy Q 💕 🌣 🎯 ad	Imin • dede SECURE
FTD1_FTD01						You have unsaved chang	es Save Cancel
Cisco Firepower 4145 Threat Defense Summary High Availability Device Routing	Interfaces Inline Se	Edit Physical Interface		Edit Physical Interface			e vallable for use. X
		General IPv4 IPv6 Path Monitoring	Advanced	General IPv4 IPv6 Path Monitoring	Advanced		Add Interfaces +
Interface	Logi	Name:		IP Type: Use Static IP v			
Ethernet1/1	inside	Enabled Management Only:		IP Address: 192.168.10.254/24			
© Ethernet1/2	outside diagnostic	Description:		-eg. The out- outpoint and the out- outpoint			_
Ethernet1/4		Mode:					
		Security Zone:					
		Interface ID:				Cancel	3
		MTU:					
		(64 - 9184) Priority:					
		0 (0 - 65535) Decemente Securite Genera Terr					
		NVE Only:					
				Ca	ncel OK		

Imposta IP attivo per interfaccia dati

g. Passare a Dispositivi > Fare clic su FTD01_FTD02_HA (in questo esempio) > Alta disponibilità. Impostare Standby IP per Data Interface.

Nell'esempio:

·Ethernet1/1 (interna) : 192.168.10.253/24

·Ethernet1/2 (esterno) : 192.168.20.253/24

·Ethernet1/3 (diagnostica) : 192.168.80.2/24

Questa immagine mostra l'impostazione per Standby IP di Ethernet1/1.

Firewall Management Devices / High Availability	Center Overview Analysis Policies Device	es Objects Inte	gration		Deploy	९ 🔮 🔅	🗧 🕜 admin 🔻	cisco SECURE
FTD01_FTD02_HA Cisco Firepower 4145 Threat Defense Summary High Availability	e Device Routing Interfaces Inline Sets DHCP	VTEP						tve Cancel
IPsec Encryption	Edit inside	0	itics					٩
Monitored Interfaces	Monitor this interface for failures			Active Link-Local IPv6	Standby Link-	Local IPv6	Monitorin	9
outside	Interface Name:						٥	1
diagnostic	Active IP Address:						۰	1
inside	192.108.10.254 Mask:						۰	/
	24 Standby IP Address:							
Failover Trigger Criteria	192,100,10,255		face MAC Add	resses				+
Failure Limit			cal Interface	Active Mac Ad	ldress	Standby Ma	ac Address	
Peer Poll Time		Cancel	et1/1	1234.1234.00	01	1234.1234	.0002	/1
Peer Hold Time								

Imposta IP standby per interfaccia dati

h. Ripetere i passi da 6.c a g per aggiungere la seconda coppia di failover.

Nell'esempio:

Nome : FTD11_FTD12_HAPrimary Peer : FTD1_FTD11Peer secondario: FTD2_FTD12

·Collegamento ad alta disponibilità : Ethernet1/8 ·State Link : Ethernet 1/8

·Ethernet1/8 (ha_link attivo) : 192.168.91.1/24

·Ethernet1/5 (interno attivo) : 192.168.30.254/24

·Ethernet1/6 (esterno attivo) : 192.168.40.254/24

·Ethernet1/7 (diagnostica attiva) : 192.168.81.1/24

·Ethernet1/8 (ha_link Standby) : 192.168.91.2/24

·Ethernet1/5 (in standby) : 192.168.30.253/24

·Ethernet1/6 (fuori dallo standby) : 192.168.40.253/24

·Ethernet1/7 (diagnostic Standby) : 192.168.81.2/24

i. Passare a **Dispositivi logici** > **Aggiungi standalone**. Impostare la regola del provider di servizi di audioconferenza per consentire il traffico dall'interno all'esterno.

Ę	Policies / Acces	anagement C ss Control / Policy	enter Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	Q 🔮 🕸	🛿 admin	• obser	SECU	RE
•	acp-rule Enter Description												Try Ne	w UI Layout 🍽	Analyze Hit C	ounts	iave	Cance	
1	Rules Security Intelligence HTTP Responses Logging Advanced Prefitter Policy. Default Prefitter Policy. Default Prefitter Policy. Stationard Security Intelligence HTTP Responses Logging Advanced Prefitter Policy Responses Logging Advanced Prefitter Policy Responses Policy Policy Responses Policy Responses Policy Policy Policy Responses Policy Policy Policy Policy Policy Policy Policy Policy Polic																		
Eit	er by Device	Search Rules											×	Show Rule Con	ficts 🛛 🕂	Add Categor	y + 4	Add Ru	le
	Name	Source Zones	Dest Zones	Source Networks	De	st Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	15 O I.	201	-	¢
$\sim N$	landatory - acp-rule	e (1-1)		_												_			
1	1 ftd_ha_scp inside_zone outside_zone Any																		
$\sim D$	Nefault - acp-rule (-))																	
The	are are no rules in this section. Add Rule or Add Category																		

j. Distribuire l'impostazione su FTD.

k. Conferma stato HA nella CLI

Lo stato HA di ciascuna istanza è confermato anche nella CLI di Firepower, che è uguale allo stato di ASA.

Eseguire show running-config failover e show failover il comando per confermare lo stato HA di FTD1_FTD01 (istanza primaria01).

<#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

Eseguire show running-config failover e show failover il comando per confermare lo stato HA di FTD1_FTD11 (istanza primaria02).

<#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

Eseguire show running-config failover e show failover il comando per confermare lo stato HA di FTD2_FTD02 (istanza secondaria01).

<#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- Eseguire show running-config failover e show failover il comando per confermare lo stato HA di FTD2_FTD12 (Istanza secondaria02).

<#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. Conferma consumo licenza

Tutte le licenze vengono utilizzate per motore/chassis di sicurezza e non per istanza del contenitore.

·Le licenze di base vengono assegnate automaticamente: una per motore/chassis di sicurezza.

·Le licenze per le funzionalità vengono assegnate manualmente a ciascuna istanza, ma si utilizza solo una licenza per ogni motore/chassis di protezione delle funzionalità. Per una licenza per una funzionalità specifica, è sufficiente un totale di 1 licenza, indipendentemente dal numero di istanze in uso.

Nella tabella viene mostrato come usare le licenze in questo documento.

PR01	Istanza01	Base, filtro URL, malware, minaccia
	Istanza02	Base, filtro URL, malware, minaccia
PR02	Istanza01	Base, filtro URL, malware, minaccia
	Istanza02	Base, filtro URL, malware, minaccia

Numero totale di licenze

Base	Filtro URL	Malware	Minaccia
2	2	2	2

Confermare il numero di licenze utilizzate nell'interfaccia utente grafica di FMC.

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	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	
V Mabware (2)	In-Compliance					
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	
✓ 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	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	
✓ URL Filtering (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 Frepower 4145 Threat Defense Threat Defense High Availability	In+Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	

Conferma licenze usate

Verifica

Quando si verifica un crash su FTD1_FTD01 (Istanza primaria01), viene attivato il failover di Instance01 e le interfacce dati sul lato Standby rilevano l'indirizzo IP/MAC dell'interfaccia attiva originale, garantendo che il traffico (connessione FTP in questo documento) venga continuamente passato da Firepower.



Prima dell'arresto



Durante l'arresto anomalo



Failover Attivato

Passaggio 1. Avviare la connessione FTP da Win10-01 a Win10-02.

Passaggio 2. Il show conn comando Esegui per confermare la connessione FTP viene stabilita in entrambe le istanze di 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

Passaggio 3. Avviare la connessione FTP da Win10-03 a Win10-04.

Passaggio 4. Il show conn comando Esegui per confermare la connessione FTP viene stabilita in entrambe le istanze di 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

Passaggio 5. Eseguire connect ftd FTD01e system support diagnostic-cliil comando per accedere alla CLI di ASA. Eseguire enablee **crashinfo force watchdog** il comando per forzare l'arresto anomalo di Instance01 nell'unità primaria/attiva.

<#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]:
```

Passaggio 6. Il failover si verifica in Instance01 e la connessione FTP non viene interrotta. Eseguire show failovere show conn per confermare lo stato di 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

Passaggio 7. L'arresto anomalo si è verificato in Instance01 e non ha avuto alcun effetto su Instance02. Eseguire show failovere show conn per confermare lo stato di 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
```

Passaggio 8. Selezionare Dispositivi > Tutto in FMC. Confermare lo stato HA.

·FTD1_FTD01: primario, standby

·FTD2_FTD02: secondario, attivo

Fin Dev	ewall Management Center Overview Analysis	Policies Devices Object	s Integration	n			Deploy Q 🤇	admin • deale SECURE
View By:	Group							Deployment History
All (4)	Error (0) Warning (0) Offline (0) Normal (4)	 Deployment Pending (0) 	pgrade (0)	Snort 3 (4)				Q, Search Device Add •
Collapse All								
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	V Ungrouped (2)							
	FT001_FT002_HA High Availability							11
	FTD1_FTD01(Primary, Standby) Snort 3 http://discort.org/	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:
	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	*\$	1
	 FTD11_FTD12_MA High Availability 							11
	FTD1_FTD11(Primary, Active) Short 3 Control 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	:
	FTD2_FTD12(Secondary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	«Ø	1

Conferma stato HA

Passaggio 9. (Facoltativo)Dopo che Instance01 di FPR01 è tornata normale, è possibile modificare manualmente lo stato di HA. Questa

In FMC, selezionare Devices > All (Dispositivi > Tutti). Fare clic su Switch Active Peer per passare allo stato HA per FTD01_FTD02_HA.

C) 5	irewall Management Center Overview Analysis evices / Device Management	Policies Devices Objec	ts Integratio	n			Deploy Q 🥝	🔅 🚱 admin 🔹 🖂 dede SECURE
View By:	Group							Deployment History
All (4)	Error (0) Warning (0) Offline (0) Normal (4)	 Deployment Pending (0) 	Jpgrade (0)	Snort 3 (4)				Q, Search Device Add •
Collanse./	M							
	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	FPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	«Q	Force refresh node status Delete Revert Upgrade
	FTD2_FTD02(Secondary, Active) Snort 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	«Ø	Health Monitor Troubleshoot Files
	V FT011_FT012_HA High Availability							11
	FTD1_FTD11(Primary, Active) Snort 3 Legg 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	:
	FTD2_FTD12(Secondary, Standby) Snort 3 Elic(1.10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acpirule	+©	I

Stato switch HA

Dalla CLI di Firepower, eseguire connect ftd FTD01 il comando and system support diagnostic-cli per accedere alla CLI di ASA. Eseguire enablee **failover active** il comando per passare HA per 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

Risoluzione dei problemi

Per convalidare lo stato del failover, eseguire show failover e show failover history il comando.

<#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

Eseguire il comando debug fover <option> per abilitare il registro di debug del failover.

<#root>

>

debug fover

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

Riferimento

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

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).