Configurar a alta disponibilidade de várias instâncias de FTD no Firepower 4100

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Diagrama de Rede
Configurações
Etapa 1. Pré-configurar interfaces
Etapa 2. Adicione 2 perfis de recurso para instâncias de contêiner.
Etapa 3. (Opcional) Adicione um Prefixo de Pool MAC de endereço MAC virtual para Interfaces de Instância de Contêiner.
Etapa 4. Adicionar uma Instância Autônoma.
Etapa 5. Configurar interfaces
Etapa 6. Adicione O Par De Alta Disponibilidade Para Cada Instância.
Verificar
Troubleshooting
Referência

Introdução

Este documento descreve como configurar o Failover em Instâncias de Contêiner FTD (Várias Instâncias).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento do Firepower Management Center e do Firewall Threat Defense.

Componentes Utilizados

Cisco Firepower Management Center Virtual 7.2.5 Dispositivo de NGFW (FTD) 7.2.5 Cisco Firepower 4145 Firepower eXtensible Operating System (FXOS) 2.12 (0.498) Windows 10 As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Antes de implantar o FTD em várias instâncias, é importante entender como ele pode afetar o desempenho do sistema e planejar adequadamente. Sempre consulte a documentação oficial da Cisco ou consulte um representante técnico da Cisco para garantir a implantação e a configuração ideais.

Informações de Apoio

Várias instâncias são um recurso do Firepower Threat Defense (FTD) que é semelhante ao modo de contexto múltiplo do ASA. Ele permite executar várias instâncias de contêiner separadas do FTD em um único hardware. Cada Instância de contêiner permite a separação de recursos físicos, o gerenciamento de configuração separado, recarregamentos separados, atualizações de software separadas e suporte total ao recurso de defesa contra ameaças. Isso é particularmente útil para empresas que exigem políticas de segurança diferentes para departamentos ou projetos diferentes, mas que não desejam investir em vários dispositivos de hardware separados. O recurso de várias instâncias é atualmente suportado no dispositivo de segurança Firepower 4100 e 9300 Series que executa o FTD 6.4 e posterior.

Este documento usa o Firepower4145, que suporta no máximo 14 instâncias de contêiner. Para obter o máximo de instâncias aceitas no Firepower Appliance, consulte <u>Máximo de instâncias e</u> recursos de contêiner por modelo.

Diagrama de Rede

Este documento apresenta a configuração e a verificação de HA em várias instâncias neste diagrama.



Diagrama de configuração lógica



Diagrama de configuração física

Configurações

Etapa 1. Pré-configurar interfaces

a. Navegue até Interfaces no FCM. Defina 2 interfaces de gerenciamento. Neste exemplo, Ethernet1/3 e Ethernet1/7.

Overview Interfa	ces Logical Devices	Security Engine	Platform Settings						Syster	n Tools Help	admin
			Vetwork Module 1	5 7 5 8	ietwork Module 2 :	Empty	Network Module 3 : Em	pty			
All Interfaces Hardw	vare Bypass									Eilter	×
Interface	Туре	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State	T NOCE.	
MGMT	Management										
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down		a 🖉	
Ethernet1/1	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/2	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/3	mgmt	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/4	data	1gbps	1gbps			Full Duplex	yes	up	\frown	0	
Ethernet1/5	data	1gbps	1gbps			Full Duplex	yes	up	\frown	ø	
Ethernet1/6	data	1gbps	1gbps			Full Duplex	yes	up	\frown	ø	
Ethernet1/7	mgmt	1gbps	1gbps			Full Duplex	yes	up	\sim	6P	
Ethernet1/8	data	1gbps	1gbps			Full Duplex	yes	up	\frown	ø	

Pré-configurar interfaces

Etapa 2. Adicione 2 perfis de recurso para instâncias de contêiner.

a. Navegue até Platform Settings > Resource Profiles > Add no FCM. Defina o 1º perfil de recurso.

Neste exemplo: ·Nome: Instance01 ·Número de núcleos: 10



Observação: para HA do par de instâncias do contêiner, eles devem usar os mesmos atributos de perfil de recurso.

Defina o nome do perfil entre 1 e 64 caracteres. Observe que você não pode alterar o nome desse perfil depois de adicioná-lo.

Defina o número de núcleos para o perfil, entre 6 e o máximo.

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

b. Repita a. na Etapa 2, para configurar o 2º perfil de recurso.

Neste exemplo: ·Nome: Instance02 ·Número de núcleos: 20

Overview Interfaces Logica	al Devices Security Engine Platfor	rm 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	/ 8	
Syslog	Instance01		10	2 B	
DNS					
FIPS and Common Criteria		Add Persource Profile			
Access List					
MAC Pool		Name:* Instance02			
Resource Profiles		Description:			
Chargie UPI					
Chasara OKL		Number of Cores:* 20 Range: 6 to 86			
		Specify even value for number of cores.			
		OK Cancel			

Adicionar 2º Perfil de Recurso

c. Verifique se 2 perfis de recursos foram adicionados com êxito.

Overv	ew Interfaces	: Logi	cal Dev	ices	Security B	ingine	Platfor	m Settings	s										Syste	m 1	iools H	lelp	admin
NTP																							
SSH																	0	Add					
SNM			Ne	me						Descrip	ption				Cores								
нттр	5		De	fault-S	imall					Auto-cre	eated applic	ation resource	ce-profile with	6 cpu-cores	6			18					
AAA	-															•							
Sysic	9		Inc	stances	31										10	I		6					
FIPS	and Common Criter	ria	Inc	stance	02										20			J 🛙					
Acces	s List																						
MAC	Pool																						
Reso	urce Profiles																						
Netw	ork Control Policy																						
Chas	is URL																						

Confirmar perfil de recurso

Etapa 3. (Opcional)Adicione um Prefixo de Pool MAC de endereço MAC virtual para Interfaces de Instância de Contêiner.

Você pode definir manualmente o endereço MAC virtual para a interface Ativa/Em espera. Se os Endereços MAC Virtuais não estiverem definidos para o recurso de várias Instâncias, o chassi gerará automaticamente endereços MAC para interfaces de Instância e garantirá que uma interface compartilhada em cada Instância use um endereço MAC exclusivo.

Verifique <u>Add a MAC Pool Prefix e View MAC Addresses for Container Instance Interfaces</u> para obter mais detalhes sobre o endereço MAC.

Etapa 4. Adicionar uma Instância Autônoma.

a. Navegue até Dispositivos lógicos > Adicionar independente. Defina a 1ª instância.

Neste exemplo: ·Nome do dispositivo: FTD01

·Tipo de Instância: Contêiner



Observação: a única maneira de implantar um aplicativo de contêiner é pré-implantar uma App-Instance com Instance Type definido como Container. Certifique-se de selecionar Container.

Você não pode alterar esse nome depois de adicionar o dispositivo lógico.

Overview Interfaces Logical Devices Security Engine	Platform Settings		System Tools Help admin
Logical Device List	(0 instances) 100% (86 of 86) Cores A	vallable	C Refresh Add •
No logical devices available. Click on Add Device to add a new logical device.			
	Add Standalone		
	Device Name:	FTD01	
	Template:	Cisco Secure Firewall Threat Defense	
	Image Version: 7	*.2.5.208	
	Instance Type:	Container	
	Before you add the f the security module/ formatting. You only	irst container instance, you must reinitialize lengine so that the disk has the correct need to perform this action once.	
		OK Cancel	

Adicionar instância

Etapa 5. Configurar interfaces

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

Neste exemplo: ·Perfil de Recurso: Instance01 ·Interface de gerenciamento: 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 Firewall Threat Defense - Bootstrap Configuration 🖭	Save Cancel
Data Ports Ethernet1/1 Ethernet1/2 Ethernet1/3 Ethernet1/6 Ethernet1/8	General Information Settings Agreement SM 1 - 86 Cores Available Resource Profile: Instance01 Interface Information Management Interface: Ethernet1/3 IPv4 Management IP: Irva Network Mask: 255.0.0.0 Network Gateway: 1.^^tm	
Application Version Resource Profile	rt Status	
FTD 7.2.5.208		

Configurar perfil/interface de gerenciamento/IP de gerenciamento

b. Defina Interfaces de Dados.

Neste exemplo:

·Ethernet1/1 (usado para o interior)

·Ethernet1/2 (usado para fora)

·Ethernet1/4 (usado para link HA)

c	overview Interfaces	Logical Devices Secu	rity Engine Platform Set	tings				System Tools	Help admin
P S	rovisioning - FTD01 itandalone Cisco Sec	ure Firewall Threat Defense	7.2.5.208					Save	Cancel
	ata Ports Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/6 Ethernet1/6			Ethernet1] /1 /2] /4	FTD - 7.2.5.208 Etheretia Click to configure	3		
ļ	Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status		
•	FTD	7.2.5.208	Instance01	1.10001	1.0	Ethernet1/3			
	Interface Name Ethernet1/1 Ethernet1/2 Ethernet1/4			Type data data data					

Definir Interfaces de Dados

c. Navegue até Logical Devices. Aguardando a inicialização da Instância.

	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	s				System Tools Help admin
Lo	ogical Devic	e List		c	1 Container instanc	e) 100% (86 of 86) Cores Ava	ilable			C Refresh O Ads •
	FTD01			Standalone	Status:ok					₽ :
	Applicat	ion	Version	Resource F	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01		1	1.0-0-000	Ethernet1/3	🐝 Installing	💷 🎼 C 🕍

Confirmar Status da Instância01

d. Repita a. nas Etapas 4.a e 5.a a c para adicionar a 2ª Instância e definir detalhes para ela.

Neste exemplo:

•Nome do dispositivo: FTD11 •Tipo de Instância : Contêiner

·Perfil de Recurso: Instância02
·Interface de gerenciamento: Ethernet1/7
·IP de gerenciamento: x.x.10.1

·Ethernet1/5 = interno

·Ethernet1/6 = externo

·Ethernet1/8 = enlace HA

e. Confirme se 2 instâncias têm o status Online no FCM.

Overview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logical Devic	e List		c	2 Container instan	ces) 66% (56 of 86) C	ores Available			C Refresh 🔘 Add •
FTD11]		Standalone	Status:ok					
Applicat	tion	Version	Resource P	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance02]	10.1	1/2-2-22	Ethernet1/7	Online	💌 🎘 c 🔬
FTD01]		Standalone	Status:ok					/ :
Applicat	tion	Version	Resource P	Profile	Management IP	Gateway	Management Port	Status	
FTD FTD		7.2.5.208	Instance01]	C a.i.	1.0	Ethernet1/3	Online	💌 🕅 C 🖄

Confirmar Status Da Instância No Dispositivo Primário

f. (Opcional) Execute scope ssa o scope slot 1 e show app-Instance confirme se 2 instâncias estão com status on-line na CLI do 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 --> 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. Faça o mesmo no dispositivo secundário. Confirme se 2 instâncias têm o status Online.

¢	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	js				System Tools Help admin
Lo	gical Devic	e List			(2 Container instanc	es) 66% (56 of 86) Core	is Available			C Refresh 🕢 Add •
	FTD12			Standalone	Status:ok					2 I
	Applicat	ion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance02]		1.	Ethernet1/7	Online	💌 🎋 c 🚈
	FTD02			Standalone	Status:ok					1
	Applicat	ion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
1	FTD		7.2.5.208	Instance01		1.2	1.6	Ethernet1/3	Online	💌 🕅 C 💆

Confirmar Status Da Instância No Dispositivo Secundário

Etapa 6. Adicione O Par De Alta Disponibilidade Para Cada Instância.

a. Navegue até **Devices** > **Add Device** no FMC. Adicionar todas as instâncias ao FMC.

Neste exemplo:

·Nome para Exibição da Instância01 do FTD1: FTD1_FTD01
·Nome para Exibição da Instância02 do FTD1: FTD1_FTD11
·Nome para Exibição da Instância01 do FTD2: FTD2_FTD02
·Nome para Exibição da Instância02 do FTD2: FTD2_FTD12

Esta imagem mostra a configuração para FTD1_FTD01.

Firewall Management Center Overview Analyst 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		

Adicionar instância de FTD ao FMC

b. Confirme se todas as instâncias são normais.

Firewall Management Center Overview Analyski Devices / Device Management	s 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	Oeployment Pending (0) Upgrad	de (0) • Snort 3	1 (4)			Q, Search Device	Add 💌
Collapse All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)							
FTD1_FTD01 Snort 3 t_AC(1,1) = Routed	Firepower 4145 with FTD	7.2.5	ITR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	\$P	1:
C PTD1_FTD11 Smort 3 Victos 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 Emc0.1.2 - 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	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1

Confirmar Status da Instância no FMC

c. Navegue até **Devices** > **Add High Availability**. Defina o 1° par de failover.

Neste exemplo:

·Nome: FTD01_FTD02_HA

·Par Primário: FTD1_FTD01



Observação: certifique-se de selecionar a unidade correta como a unidade primária.

Firewall Management Center Overview Analysis Pro	olicies Devices Objects	Integration			Deploy	오. 🥥 🌣 🔞 admin 🔻	tinte SECURE
View By: Group						Deploy	ment History
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4) • E	Deployment Pending (0)	(0) • Snort 3	s (4)			Q, Search Device	Add 🔻
Collarse All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)		Add High A	wailability Pair				
FTD1_FTD01_Snort 3	Firepower 4145 with FTD	Name:* FTD01_FTD	02_H4	Base, Threat (2 more)	acp-rule	4Q	1
FTD1_FTD11 Short 3	Firepower 4145 with FTD	Device Type: Firewall Thre	at Defense 👻	Base, Threat (2 more)	acp-rule	49	1
FTD2_FTD02_Steet 3 FTD2_12 - Routed	Firepower 4145 with FTD	Primary Peer: FTD1_FTD0	•	Base, Threat (2 more)	acp-rule	49	1
FTD2_FTD12_Snort 3	Firepower 4145 with FTD	Secondary Pe FTD2_FTD0	or:	Base, Threat (2 more)	acp-rule	49	1
		Threat Deficient Configuration Configuration Converted to on both period.	ense High Availability pair will have primary or. Licenses from primary peer will be to their high availability versions and applied ers.				
			Cancel Continue				

Adicionar 1º par de failover

d. Defina o IP para o link de failover no primeiro par de failover.

Neste exemplo:

·Link de alta disponibilidade: Ethernet1/4

·Link de estado: Ethernet1/4

·IP primário: 192.168.90.1/24

·IP secundário: 192.168.90.2/24

Firewall Management Center Overview And Devices / Device Management	Nysis Policies D	Vevices Objects Integration		Deploy	오 📀 🌣 😝 admin •	-de-de- cisco SECURE
Mew By: Group					Depl	oyment History
All (4) • Error (0) • Warning (0) = Offline (0) • Norma	al (4) 🗢 Deployment P	rending (0) Upgrade (0) Snort 3 (4)			Q, Search Device	Add 🔻
Collapse-All						
Name	Model	Add High Availability Dair		Access Control Policy	Auto RollBack	
Ungrouped (4)		Ava high Availability Fail				
		High Availability Link	State Link			
FTD1_FTD01 Snort 3	Firepowe	Interface:* Ethernet1/4 +	Interface:* Ethernet1/4 +	acp-rule	4(9)	11
		Logical Name:* ha_link	Logical Name:*			
FTD1_FTD11 Snort 3	Firepowe	Primary IP:* 192.168.90.1	Primary IP:*	acp-rule	4Q	11
		Use IPv6 Address	Use IPv6 Address			
FTD2_FTD02_Snort 3	Firepowe	Secondary IP:* 192.168.90.2	Secondary IP:*	acp-rule	«Ģ	11
		Subnet Mask: 255.255.255.0	Subnet Mask;*			
FTD2_FTD12 Seet 3	Firepowe	IPsec Encryption		acp-rule	*©	11
		Enabled				
		Key Generation: Auto v				
		LAN failover link is used to sync configuration, statef between peers. Selected interface links and encryption	ul failover link is used to sync application content settings cannot be changed later.			
			Cancel Add			

Definir interface HA e IP para o primeiro par de failover

e. Confirme o status do failover

·FTD1_FTD01: Principal, Ativo

·FTD2_FTD02: Secundário, Em Espera

E Fire	ewall Management Center Overview Analysis ces / Device Management	Policies Devices Object	s Integration	1			Deploy Q 🥝	🔅 🕲 admin	cisco SECURE
View By:	Group +							De	oloyment 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		
	Ungrouped (3)								
	FID01_FID02_HA High Availability								11
	FTD1_FTD01(Primary, Active) Short 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40		I
	FTD2_FTD02(Secondary, Standby) Short 3 [1][3].1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower/KCHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q		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	Firepower4KHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	«Ø		1

Confirmar status do primeiro par de failover

f. Navegue até Devices > Clique em FTD01_FTD02_HA (neste exemplo) > Interfaces. Defina o IP ativo para a interface de dados.

Neste exemplo:

·Ethernet1/1 (interna): 192.168.10.254/24

·Ethernet1/2 (externo): 192.168.20.254/24

·Ethernet1/3 (diagnóstico): 192.168.80.1/24

Esta imagem mostra a configuração para IP Ativo de Ethernet1/1.

Firewall Management Center Overview Devices / Secure Firewall Interfaces	w Analysis Policies Devices Objects Integration		Deploy Q 🧬 🌣 🔕 admin 🛛 🎂 SECURE
FTD1_FTD01			You have unsaved changes Save Cancel
Summary High Availability Device Routing In	Interfaces Inline Se Edit Physical Interface	Edit Physical Interface	allable for use. X
Interface LogL Ethernet1/1 inside f(bernet1/2 outside)	Ceneral PV4 PV6 Path Montoring Adv Name: E inside E Enabled E Description:	anded Omman Pro Pain Homony Point Color IP Type: Use Static IP • IP Addrese: 192.166.10.254/24 rg 18/0.2.1/25255.55/18/07/18/0.2.1/25	Add Interfaces •
Ethernet1/3 diagn Ethernet1/4	None Security Zone:		
	Interface ID: IDharmet1/1 MTU: 1500 (id - 978d) Phothy: 0 (0 - 65535) Phopagate Security Group Tag: NUE Creby:		Cancel
		Cancel	



g. Navegue até **Devices** > **Clique em FTD01_FTD02_HA** (neste exemplo) > **High Availability.** Defina o IP de standby para a interface de dados.

Neste exemplo:

·Ethernet1/1 (interna): 192.168.10.253/24

·Ethernet1/2 (externo): 192.168.20.253/24

·Ethernet1/3 (diagnóstico): 192.168.80.2/24

Esta imagem mostra a configuração do IP em standby de Ethernet1/1.

Devices / High Availability	Center Overview Analysis Policies Device	s Objects Inte	gration		Deploy	९ 🗳 🌣	🕜 admin 🕶 👘	te SECURE
FTD01_FTD02_HA Cisco Firepower 4145 Threat Defense Summary High Availability	e Device Routing Interfaces Inline Sets DHCP N	/TEP						Cancel
IPsec Encryption	Edit inside	0	stics					٩
Monitored Interfaces	Monitor this interface for failures							
Interface Name	IPv4 IPv6			Active Link-Local IPv6	Standby Link	-Local IPv6	Monitoring	
outside	Interface Name:						٥	1
diagnostic	Active IP Address:						0	/
inside	192.168.10.254 Mask:						0	1
	24 Standby IP Address:							
Failover Trigger Criteria	192.168.10.253		face MAC Add	resses				+
Failure Limit			cal Interface	Active Mac	Address	Standby Mad	c Address	
Peer Poll Time		Cancel	et1/1	1234.1234	0001	1234.1234.0	0002	/1
Peer Hold Time								

Definir IP em Espera para Interface de Dados

h. Repita as etapas de 6.c a g para adicionar o segundo par de failover.

Neste exemplo:

Nome: FTD11_FTD12_HA
Par Principal: FTD1_FTD11
Par Secundário: FTD2_FTD12
Link de alta disponibilidade: Ethernet1/8

·Enlace: Ethernet1/8

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

·Ethernet1/5 (dentro Ativo) : 192.168.30.254/24

·Ethernet1/6 (Ativo externo): 192.168.40.254/24

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

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

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

•Ethernet1/6 (standby externo): 192.168.40.253/24

·Ethernet1/7 (Standby de diagnóstico): 192.168.81.2/24

i. Navegue até Logical Devices > Add Standalone. Defina a regra de ACP para permitir o tráfego de dentro para fora.

Ę	Firewall Ma Policies / Acces	anagement C ss Control / Policy	Center Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	Q 🗳 🌣	Ø ad	imin •	-de-de- cisco	SECU	JRE
•	acp-rule Try New UI Layout () Analyze Hit Counts Seve Cancel Enter Description																			
	Rules Security Intelligence HTTP Responses Logging Advanced Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy: SSL Policy: None Identity Policy: None																			
Eit	er by Device	Search Rules											×	Show Rule Con	flicts 🛛 +	Add Car	egory	+ /	Add Ri	ale
	Name	Source Zones	Dest Zones	Source Networks	Der	st Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	15 C	B , 2			¢
$\sim N$	landatory - acp-rule	e (1-1)		_																
1	1 ftd_ha_scp inside_zone outside_zone Any																			
∨ D	efault - acp-rule (-))																		
The	here are no rules in this section. Add Rule or Add Category																			

j. Implante a configuração no FTD.

k. Confirmar status de HA na CLI

O status de HA de cada instância também é confirmado na CLI do Firepower, que é igual ao ASA.

Execute **show running-config failover** e **show failover** execute o comando para confirmar o status de HA de FTD1_FTD01 (instância primária01).

<#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

Execute show running-config failover e show failover execute o comando para confirmar o status de HA de FTD1_FTD11 (Instância 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

Execute show running-config failover e show failover execute o comando para confirmar o status de HA de FTD2_FTD02 (Instância Secundária01).

<#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- Execute show running-config failover e show failover execute o comando para confirmar o status de HA de FTD2_FTD12 (Instância Secundária02).

<#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 consumo de licença

Todas as licenças são consumidas por mecanismo de segurança/chassi, e não por Instância de contêiner.

·As licenças básicas são atribuídas automaticamente: uma por mecanismo/chassi de segurança.

·As licenças de recursos são atribuídas manualmente a cada instância, mas você consome apenas uma licença por recurso por mecanismo/chassi de segurança. Para uma licença de recurso específico, você só precisa de um total de 1 licença, independentemente do número de instâncias em uso.

Esta tabela mostra como as licenças são consumidas neste documento.

FPR01	Instância01	Base, filtragem de URL, malware, ameaça
	Instância02	Base, filtragem de URL, malware, ameaça
FPR02	Instância01	Base, filtragem de URL, malware, ameaça
	Instância02	Base, filtragem de URL, malware, ameaça

Número total de licenças

Base	Filtragem de URL	Malware	Ameaça
2	2	2	2

Confirme o número de licenças consumidas na GUI do 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	
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					
FID01_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	
VURL Filtering (2)	In-Compliance					- 1
> FTD01_FTD02_HA (2) Cisco Frepower 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	

Confirmar licenças consumidas

Verificar

Quando ocorreu um travamento em FTD1_FTD01 (Instância principal01), o failover da Instância01 é acionado e as interfaces de dados no lado de standby assumem o endereço IP/MAC da interface ativa original, garantindo que o tráfego (conexão FTP neste documento) seja transmitido continuamente pelo Firepower.



Antes do travamento



Durante o travamento



O Failover É Disparado

Etapa 1. Iniciar conexão FTP de Win10-01 para Win10-02.

Etapa 2. Execute o show conn comando para confirmar se a conexão FTP foi estabelecida em ambos os casos de 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

Etapa 3. Iniciar conexão FTP de Win10-03 para Win10-04.

Etapa 4. Execute o show conn comando para confirmar se a conexão FTP foi estabelecida em ambos os casos de 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

Etapa 5. Execute o comando connect ftd FTD01 system support diagnostic-cli and para entrar no CLI do ASA. Execute enable e **crashinfo force watchdog** comando para forçar a falha Instance01 na unidade Principal/Ativa.

<#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]:
```

Etapa 6. O failover ocorre na Instance01 e a conexão FTP não é interrompida. Execute o comando show failover show conn and para confirmar o status da Instância01 no 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

Passo 7. A falha ocorreu na Instance01 não teve efeito na Instance02. Execute o comando show failover show conn and para confirmar o status 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

Etapa 8. Navegue até Devices > All no FMC. Confirme o status HA.

·FTD1_FTD01: Principal, Em Espera

·FTD2_FTD02: Secundário, Ativo

E Fin Dev	rewall Management Center Overview Analysis	Policies Devices Object	s Integratio	n			Deploy Q 📀	Costo 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	
	✓ Ungrouped (2)							
	FTD01_FTD02_HA High Availability							11
	FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	E Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1
	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	e2+	:
	✓ FTD11_FTD12_HA ✓ High Availability							/1
	FTD1_FTD11(Primary, Active) Snort 3 Ct. ** 10.1 - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:
	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	Ş	1

Confirmar status de HA

Etapa 9. (Opcional)Depois que a Instância01 de FPR01 voltar ao normal, você poderá alternar manualmente o status de HA. Isso pode ser feito

pela GUI do FMC ou pela CLI do FRP.

No FMC, navegue até Devices > All. Clique em Switch Ative Peer para alternar o status de HA para FTD01_FTD02_HA.

	irewall Management Center Overview Analysis evices / Device Management	Policies Devices Object	s 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) 	pgrade (0)	Snort 3 (4)				Q, Search Device Add •
Collapse.A	M.							
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	Ungrouped (2)							
	FTD01_FTD02_HA Hgh Availability							Switch Active Peer
	CTED1_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	4Q	Break Force refresh node status Delete Revert Upgrade
	C 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	«Ø	Health Monitor Troubleshoot Files
	V FT011_FT012_HA High Availability							11
	CET11_FTD11(Primary, Active) Snort 3 CET110.1 - Routed	Firepower 4145 with FTD	7.2.5	EFPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	«Ø	:
	FTD2_FTD12(Secondary, Standby) Snort 3 Entrol.10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower404G cisco.com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	+©	I

Status HA do switch

Na CLI do Firepower, execute os comandos connect ftd FTD01 e system support diagnostic-cli para entrar na CLI do ASA. Execute enable e failover active comando para comutar 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

Troubleshooting

Para validar o status do failover, execute show failover e show failover history execute o 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

Execute o comando debug fover <option> para habilitar o log de depuração de failover.

<#root>

>

debug fover

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

Referência

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.