Firepower 4100でのFTDマルチインスタンス高 可用性の設定

内容
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>ネットワーク図</u>
<u>コンフィギュレーション</u>
<u> ステップ 1:インターフェイスの事前設定</u>
<u> ステップ 2:コンテナインスタンスに2つのリソースプロファイルを追加します。</u>
<u>ステップ3:(オプション)コンテナインスタンスインターフェイスの仮想MACアドレスの</u> MACプールプレフィックスを追加します。
<u>ステップ4:スタンドアロンインスタンスを追加します。</u>
<u>ステップ 5 : インターフェイスの設定</u>
<u> 手順6:各インスタンスにハイアベイラビリティペアを追加します。</u>
トラブルシュート
<u>参考</u>

はじめに

このドキュメントでは、FTDコンテナインスタンス(マルチインスタンス)でフェールオーバー を設定する方法について説明します。

前提条件

要件

Firepower Management Center(FMC)およびファイアウォール脅威対策に関する知識があることが推奨されます。

使用するコンポーネント

Cisco Firepower Management Center(FMC)仮想7.2.5 Cisco Firepower 4145 NGFWアプライアンス(FTD)7.2.5 Firepower eXtensibleオペレーティングシステム(FXOS)2.12(0.498) Windows 10 このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

FTDマルチインスタンスを導入する前に、それがシステムのパフォーマンスに与える影響を理解 し、それに応じて計画を立てることが重要です。最適な導入と設定を行うには、必ずシスコの公 式文書を参照するか、シスコの技術担当者に相談してください。

背景説明

マルチインスタンスは、ASAマルチコンテキストモードと同様のFirepower Threat Defense(FTD)の機能です。これにより、単一のハードウェア上でFTDの複数の個別コンテナイン スタンスを実行できます。各コンテナインスタンスでは、リソースの分離、構成管理、リロード の分離、ソフトウェアアップデートの分離、脅威に対する防御機能の完全なサポートが可能です 。これは、部門やプロジェクトごとに異なるセキュリティポリシーを必要とするが、複数のハー ドウェアアプライアンスに個別に投資したくない組織に特に役立ちます。マルチインスタンス機 能は現在、FTD 6.4以降を実行するFirepower 4100および9300シリーズセキュリティアプライア ンスでサポートされています。

このドキュメントでは、最大14のコンテナインスタンスをサポートするFirepower4145を使用し ます。Firepowerアプライアンスでサポートされる最大インスタンス数については、「<u>モデルごと</u> <u>のコンテナインスタンスおよびリソースの最大数</u>」を参照してください。

ネットワーク図

このドキュメントでは、この図のマルチインスタンスのHAの設定と検証を紹介します。



論理構成図



物理構成図

コンフィギュレーション

ステップ1:インターフェイスの事前設定

a. FCMのインターフェイスに移動します。管理インターフェイスを2つ設定します。この例では、Ethernet1/3とEthernet1/7です。

Overview Interface	S Logical Devices	Security Engine	Platform Settings						Syste	n Tools Help	o admin
	<u></u>	CONSOLE MGMT	Network Module 1								
All Interfaces hardware	e bypass								Add Net	v • Filter.	×
Interface	Туре	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State		
М мбмт	Management								\frown		
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down	(IX)	J 6	
Ethernet1/1	data	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/2	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet 1/3	mgmt	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/4	data	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/5	data	1gbps	lgbps			Full Duplex	yes	up		1	
Ethernet1/6	data	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/7	mgmt	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/8	data	1gbps	lgbps			Full Duplex	yes	up		1	

インターフェイスの事前設定

ステップ2:コンテナインスタンスに2つのリソースプロファイルを追加します。

a. FCMで、Platform Settings > Resource Profiles > Addの順に移動します。1番目のリソースプロ ファイルを設定します。

- ・名前:Instance01
- ・コア数:10



注:コンテナインスタンスペアのHAの場合、同じリソースプロファイル属性を使用する 必要があります。

プロファイルの名前を1~64文字に設定します。このプロファイルを追加した後は、こ のプロファイルの名前を変更できないことに注意してください。

プロファイルのコアの数を6から最大の間で設定します。

Overview	Interfaces L	ogical (Devices Security Engine	Platform	Settings										System	Tools	Help	admin
NTP SSH													0	Add				
SNMP			Name				Descriptio	on			Co	res						
AAA			Default-Small				Auto-create	ed application r	resource-profile with 6 c	cpu-cores	6			0				
Syslog DNS																		
FIPS and Co	mmon Criteria																	
Access List					Add Resou	rce Profi	le		(?)×									
MAC Pool					Name:*	It	instance01											
 Resource P Network Cor 	ntrol Policy				Description	:												
Chassis URL					Number of	Cores:* 1	10		Range: 6 to 86									
					Specify	even value	for number of	cores.										
								c	OK Cancel									

b.ステップ2のa.を繰り返して、2番目のリソースプロファイルを設定します。

この例では、

- ・名前:Instance02
- ・コア数:20コア

Overview	v Interfaces L	ogical.	Devices Security Engine	Platform Settings	System 1	fools H	elp admin
NTP SSH				O Add			
SNMP			Name	Description Cores			
HTTPS			Default-Small	Auto-created application resource-profile with 6 cpu-cores 6 🥔 👸			
Syslog			Instance01	10 🥒 🖥			
DNS							
FIPS an	d Common Criteria			Add Passaurea Profile			
Access	List						
MAC Po	ol			Name:* Instance02			
Resource	ce Profiles						
Network	Control Policy			Description:			
Chassis	URL			Number of Cores:* 20 Range: 6 to 86			
				O Specify even value for number of cores.			
				OK Cancel			

2番目のリソースプロファイルの追加

c. 2つのリソースプロファイルが正常に追加されたことを確認します。

Overvi	ew Interfaces	Logica	al Devices	Security Engine	Platform Settings						System	Tools	Help	admin
NTP														
SSH			_						•	ADD				
SNM	-		Name			Description		Cores						
нттр	5		Default	Small		Auto-created application resource-profile with 6	6 cpu-cores	6		/ 6				
AAA	-													
Sysio	g		Instance	101				10		J 🛛				
EIDC	and Common Criteria		Instance	102				20		6				
Acces	and common criteria		_											
MAC	Pool													
Reso	urce Profiles													
Netw	ork Control Policy													
Chas	sis URL													

リソースプロファイルの確認

ステップ3:(オプション)コンテナインスタンスインターフェイスの仮想MACアド レスのMACプールプレフィックスを追加します。

アクティブ/スタンバイインターフェイスの仮想MACアドレスは手動で設定できます。マルチイン スタンス機能のために仮想MACアドレスが設定されていない場合(デフォルト)、シャーシは自 動的にインスタンスインターフェイスのMACアドレスを生成し、各インスタンスの共有インター フェイスが一意のMACアドレスを使用することを保証します。

MACアドレスの詳細については、「<u>MACプールプレフィックスの追加とコンテナインスタンスイ</u> <u>ンターフェイスのMACアドレスの表示</u>」を参照してください。

ステップ4:スタンドアロンインスタンスを追加します。

a. Logical Devices > Add Standaloneの順に移動します。第1インスタンスを設定します。

この例では、

・デバイス名:FTD01

・インスタンスタイプ:コンテナ



注:コンテナアプリケーションを導入する唯一の方法は、インスタンスタイプをコンテ ナに設定したアプリケーションインスタンスを事前導入することです。 Containerを選択 したことを確認します。

論理デバイスを追加した後で、この名前を変更することはできません。

Overview Interfaces Logical Devices Security Engine	Platform Settings		Si	stem Tools Help admin
Logical Device List	(0 instances) 100% (86 of 86) Cores Availabl	e		C Refresh 🕢 Add 🔸
No logical devices available. Click on Add Device to add a new logical device.				
	Add Standalone	(?) X		
	Device Name: FTD01			
	Template: Cisco Se	ecure Firewall Threat Defense		
	Image Version: 7.2.5.20	18		
	Instance Type: Contain	er 🗸 🗸		
	Before you add the first con the security module/engine formatting. You only need to	tainer instance, you must reinitialize so that the disk has the correct to perform this action once.		
		OK Cancel		

インスタンスの追加

ステップ5:インターフェイスの設定

a. Instance01のリソースプロファイル、管理インターフェイス、管理IPを設定します。

この例では、

- ・リソースプロファイル: Instance01
- ・管理インターフェイス: Ethernet1/3
- ・管理IP : x.x.1.1

Overview Interfaces Logical Devices Security Engine Platform S	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 Ethernet1/5 Ethernet1/6 Ethernet1/8	SH 1 - 86 Cores Available Resource Profile: Instance01 Interface Information Hanagement Interface: Ethernet1/3 Address Type: IPv4 only IPv4 Management IP: 1.1.1.1.1 Network Mask: 255.0.0.0 Network Gateway: 1.^	
Application Version Resource Profile	rt Status	
G FTD 7.2.5.208		
	OK Cancel	

プロファイル/管理インターフェイス/管理IPの設定

b.データインターフェイスを設定します。

- ・Ethernet1/1(内部で使用)
- ・Ethernet1/2(外部用)
- ・Ethernet1/4(HAリンクに使用)

0	verview Interfaces	Logical Devices Secu	rity Engine Platform Sett	ings				System Tools Help admin
Pi Si	rovisioning - FTD01 tandalone Cisco Sec	cure Firewall Threat Defense	e 7.2.5.208					Save Cancel
Di	ata Ports	-						
	Ethernet1/2							
	Ethernet1/4							
	Ethernet1/5							
	Ethernet1/6]	_		
	Ethernet1/8			Ethernet1	/1			
				Ethernet1]	FTD - 7.2.5.202 Ethernet1/3 Click to configure		
	Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status	
3	FTD	7.2.5.208	Instance01	1.10001	1.0	Ethernet1/3		
	Interface Name			Туре				
	Ethernet1/1			data				
	Ethernet1/2			data				
	Ethernet1/4			data				

データインターフェイスの設定

c. Logical Devicesに移動します。インスタンスのブートアップを待機しています。

Ove	rview	Interfaces	Logical Devices	Security Engine	Platform Setting	js				System Tools Help admin
Logic	al Device	e List		c	1 Container instanc	e) 100% (86 of 86) Cores A	wailable			C Refresh 🖉 Add •
	TD01			Standalone	Status:ok					2 I
	Applicati	ion	Version	Resource P	Profile	Management IP	Gateway	Management Port	Status	
۰	FTD		7.2.5.208	Instance01		1	1	Ethernet1/3	🐝 Installing	💷 🎘 c 🕍

Instance01のステータスの確認

d.手順4.aと手順5.a ~ cのa.を繰り返して2つ目のインスタンスを追加し、そのインスタンスの詳細を設定します。

- ・ デバイス名:FTD11
- ・ インスタンスタイプ:コンテナ
- ・リソースプロファイル: Instance02
- ・管理インターフェイス: Ethernet1/7
- ・ 管理IP:x.x.10.1
- ・Ethernet1/5 =内部
- ・Ethernet1/6 =外部
- ・Ethernet1/8 = HAリンク
- e. FCMで2つのインスタンスがオンライン状態であることを確認します。

Overview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logical Devie	ce List			(2 Container instan	ces) 66% (56 of 86) C	ores Available			C Refresh 🕥 Add •
FTD11			Standalone	Status:ok					
Applica	tion	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
H FTD		7.2.5.208	Instance02			1/2-2-222	Ethernet1/7	Online	🕶 🕅 c 🖄
FTD01			Standalone	Status:ok					01
Applica	tion	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance01]	C and	1.0	Ethernet1/3	Online	💌 🌾 c 🖾

プライマリデバイスのインスタンスステータスの確認

f. (オプション) scope ssaを実行し、 scope slot 1 および show app-Instance コマンドを実行して、2つのインスタンスが Firepower CLIでオンラインステータスであることを確認します。

<#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 Deplo 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.セカンダリデバイスでも同じ操作を行います。 2つのインスタンスがオンライン状態であることを確認します。

Overview	v Interfaces	Logical Devices	Security Engine	Platform Setting	gs				System Tools Help admin
Logical De	vice List			(2 Container instanc	xes) 66% (56 of 86) Core	ss Available			C Refresh 🖉 Add •
FTD12			Standalone	Status:ok					
Appl	cation	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
# FTD		7.2.5.208	Instance02]	10.2	1.	Ethernet1/7	Online	💌 🕅 c 🚾
FTD02			Standalone	Status:ok					/ I
Appl	cation	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
# FTD		7.2.5.208	Instance01]		1.6	Ethernet1/3	Online	💌 🏹 C 🕍

セカンダリデバイスのインスタンスステータスの確認

手順6:各インスタンスにハイアベイラビリティペアを追加します。

A. FMCで、Devices > Add Deviceの順に移動します。FMCにすべてのインスタンスを追加します。

この例では、

- ・FTD1のInstance01の表示名:FTD1_FTD01
- ・FTD1のInstance02の表示名:FTD1_FTD11
- ・FTD2のInstance01の表示名:FTD2_FTD02
- ・FTD2のInstance02の表示名:FTD2_FTD12

次の図にFTD1_FTD01の設定を示します。



FMCへのFTDインスタンスの追加

b.すべてのインスタンスが正常であることを確認します。

Firewall Management Center	teles Devices Objects						
Devices / Device Management Overview Analysis Po	ecies Devices Objects	integration			Deploy	d o o o aquin.	ONCE SECURE
View By: Group						Deploy	ment History
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4) • D	Peployment Pending (0)	(0) • Snort 3	(4)			Q, Search Device	Add 🕶
Collapse All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)							
FTD1_FTD01 Short 3 11 - Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1:
FTD1_FTD11 Scort 3 Victo 10.1 + Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1
FTD2_FTD02 Snort 3 Group 0.1.2 - Routed	Firepower 4145 with FTD	7.2.5	IIII Firepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	« ۵	1
FTD2_FTD12 Smort 3 Comp.10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1

FMCでのインスタンスステータスの確認

c. Devices > Add High Availabilityの順に移動します。1番目のフェールオーバーペアを設定します。

- ·名称:FTD01_FTD02_HA
- ・プライマリピア:FTD1_FTD01



注:正しいユニットをプライマリユニットとして選択してください。

Firewall Management Center Overview Analysis Po	olicies Devices Objects I	Integration		Deploy	오 📀 🌣 🙆 admin 🔻	tiste SECURE
View By: Group					Deploy	ment History
All (4) • Error (0) • Warning (0) = Offline (0) • Normal (4) • D	Deployment Pending (0)	(0) Snort 3 (4)			Q, Search Device	Add 🔻
Collarse Al						
Name	Model	Version Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)		Add High Availability Pair				
FTD1_FTD01 Smort 3	Firepower 4145 with FTD	Name:* FTD01_FTD02_HA	Base, Threat (2 more)	acp-rule	4Q	1
C FTD1_FTD11 Stent 3 10 1 - Routed	Firepower 4145 with FTD	Device Type: Firewall Threat Defense	Base, Threat (2 more)	acp-rule	4©	1
PTD2_FTD02_Secont_3 1.2 - Routed	Firepower 4145 with FTD	Primary Peer: FTD1_FTD01	Base, Threat (2 more)	acp-rule	4Q	1
FTD2_FTD12_Steat.3 N0.2 - Routed	Firepower 4145 with FTD	Secondary Peer: FTD2_FTD02 •	Base, Threat (2 more)	acp-rule	4Q	1
		Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.				
		Cancel Continue				

1番目のフェールオーバーペアの追加

- d.1番目のフェールオーバーペアのフェールオーバーリンクのIPを設定します。
- この例では、
- ・ハイアベイラビリティリンク:Ethernet1/4
- ・ステートリンク:Ethernet1/4
- ・プライマリIP:192.168.90.1/24

・セカンダリIP:192.168.90.2/24

Firewall Management Center Overview Analysis	Policies	Devices Objects Integration		Deploy	역 🙁 🌣 📵 admin 🕶	disco SECURE
View By: Group					Deplo	yment History
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4)	Deployment	Pending (0) Upgrade (0) Snort 3 (4)			Q, Search Device	Add •
Collacse All						
Name	Model	Add High Availability Dair		Access Control Policy	Auto RollBack	
Ungrouped (4)		Add high Availability Pail				
		High Availability Link	State Link			
FTD1_FTD01 Snort 3	Firepow	Interface:* Ethernet1/4 +	Interface:* Ethernet1/4 +	acp-rule	49	1:
		Logical Name:* ha_link	Logical Name:*			
FTD1_FTD11 Snort 3	Firepow	Primary IP:* 192.168.90.1	Primary IP:*	acp-rule	49	11
		Secondary IP:* 192.168.90.2	Secondary IP.*			
1.2 - Routed	Firepow	Subnet Mask:* 255.255.255.0	Subnet Mask:*	acp-rule	«9	11
FTD2_FTD12 Snort 3	Erenner	IPsec Encryption			40	1:
10.2 - Routed		Enabled				· :
		Key Generation: Auto +				
		LAN failover link is used to sync configuration, state between peers. Selected interface links and encryption	ful failover link is used to sync application content settings cannot be changed later.			
			Cancel			

1番目のフェールオーバーペア用のHAインターフェイスとIPの設定

e.フェールオーバーのステータスを確認します

・FTD1_FTD01:プライマリー、アクティブ

・FTD2_FTD02:セカンダリ、スタンバイ

Fire Devic	wall Management Center Overview Analysis	Policies Devices Object	s Integration	n			Deploy Q 📀 🔅	admin dealer secure			
Vew By: Group											
All (4)	All (4) • Error (0) • Warning (0) • Offine (0) • Deployment Pending (0) • Upgrade (0) • Snort 3 (4) Q. Search Device										
Collapse All	College Al										
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack				
	V Ungrouped (3)										
0	V FTD01_FTD02_HA							/ 1			
	FTD1_FTD01(Primary, Active) Short 3 Addy 1.1 - Routed	Firepower 4145 with FTD	7.2.5	ER4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	:			
	FTD2_FTD02(Secondary, Standby) Short 3 FTD1_12 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1			
	FTD1_FTD11 Snort 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	11			
	FTD2_FTD12 Snort 3 f_1_2_102 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	«Ø	11			

最初のフェールオーバーペアのステータスの確認

f. Devicesに移動し、FTD01_FTD02_HA(この例の場合)をクリックし、Interfacesをクリックします。 データインターフェイスの アクティブIPを設定します。

この例では、

- ・Ethernet1/1(内部):192.168.10.254/24
- ・Ethernet1/2(外部):192.168.20.254/24
- ・Ethernet1/3(診断):192.168.80.1/24

次の図に、Ethernet1/1のアクティブIPの設定を示します。

Firewall Management Center Devices / Secure Firewall Interfaces	Overview Analysis	Policies Devices Objects Integration		Deploy Q 🚱 🌣 🔕 admin 🔹 🕬 SECURE
FTD1_FTD01				You have unsaved changes Save Cancel
Cisco Firepower 4145 Threat Defense				valiable for use X
Summary High Availability Device Routin	ng Interfaces Inline S	Edit Physical Interface	Edit Physical Interface	•
		General IPv4 IPv6 Path Monitoring Advanced	General IPv4 IPv6 Path Monitoring Advanced	Arid Interfaces
		Namer	IP Type:	Plot interfaces *
Interface	Logi	inside	Use Static IP v	
Ethernet1/1	inside	Enabled	IP Address: 192.168.10.254/24	
© Ethernet1/2	outside	Description:	eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25	
Ethernet1/3	diagnostic			
Ethernet1/4		Mode:		
		Security Zone:		
		inside_zone v		
		Interface ID:		Cancel OK
		Ethernet1/1		
		MTU:		
		1500		
		(64 - 9184)		
		Priority:		
		0 (0 - 65535)		
		Propagate Security Group Tag:		
		NVE Only:		
		0		
			Cancel OK	

データインターフェイスのアクティブIPの設定

g. Devices > Click FTD01_FTD02_HA (この例の場合) > High Availabilityの順に移動します。 データインターフェイスのスタン バイIPを設定します。

- ・Ethernet1/1(内部):192.168.10.253/24
- ・Ethernet1/2(外部):192.168.20.253/24
- ・Ethernet1/3(診断):192.168.80.2/24

次の図に、Ethernet1/1のスタンバイIPの設定を示します。

Firewall Management Devices / High Availability	Center Overview Analysis Policies Device	es Objects Inte	gration		Deploy	९ 🗳 🔅	🕜 admin 🕶 谢	seco SECURE			
FTD01_FTD02_HA Cancel Clisco Firepower 4145 Threat Defense Cancel											
Summary High Availability	Device Routing Interfaces Inline Sets DHCP	VTEP									
IPsec Encryption	Edit inside	ø	itics					۹			
Monitored Interfaces	Monitor this interface for failures										
Interface Name	IPv4 IPv6			Active Link-Local IPv6	Standby Link-	Local IPv6	Monitoring				
outside	Interface Name:						0	1			
diagnostic	Active IP Address:						0	1			
inside	192.168.10.254						0	1			
	24										
	Standby IP Address: 192.168.10.253										
Failover Trigger Criteria			face MAC Add	resses				+			
Failure Limit			cal Interface	Active Mac Ad	dress	Standby Mac	Address				
Peer Poll Time		Cancel	et1/1	1234.1234.000	01	1234.1234.00	002	1			
Peer Hold Time		Ouncer OK									

データインターフェイスのスタンバイIPの設定

h.ステップ6.c~gを繰り返して、2番目のフェールオーバーペアを追加します。

この例では、

0

- ・ 名称 : FTD11_FTD12_HA
- ・ プライマリピア: FTD1_FTD11
- ・ セカンダリピア: FTD2_FTD12
- ・ ハイアベイラビリティリンク: Ethernet1/8
- ・ ステートリンク: Ethernet1/8
- ・Ethernet1/8(ha_linkアクティブ):192.168.91.1/24
- ・Ethernet1/5(内部アクティブ):192.168.30.254/24
- ・Ethernet1/6 (外部アクティブ):192.168.40.254/24
- ・Ethernet1/7 (診断アクティブ):192.168.81.1/24
- ・Ethernet1/8 (ha_linkスタンバイ):192.168.91.2/24
- ・Ethernet1/5(内部スタンバイ):192.168.30.253/24
- ・Ethernet1/6(外部スタンバイ):192.168.40.253/24
- ・Ethernet1/7 (診断スタンバイ):192.168.81.2/24

i. Logical Devices > Add Standaloneの順に移動します。内部から外部へのトラフィックを許可するようにACPルールを設定します

Firewall Management Center Policies / Access Control / Policy Editor	Analysis Policies	Devices	Objects Inte	egration					Deploy	Q 🔮 🌣	admin •	SECURE
Analyze Hit Counts Sove Cancel Enter Description												
Rules Security Intelligence HTTP Responses Logging Advanced Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy SSL Policy: None Identity Policy: None												
Eilter by Device Search Rules								×	Show Rule Cont	flicts 🛛 🕂	dd Category +	Add Rule
B Name Source Zones Dest Zones Source Network	Lest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	5 • 5 A 🗆 I	•
Mandatory - acp-rule (1-1)												
1 ftd_ha_acp inside_zone outside_zone Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	50500	0/1
✓ Default - acp-rule (-)												
There are no rules in this section. Add Rule or Add Category	There are no rules in this section. Add Rule or Add Category											

ACPルールの設定

j.設定をFTDに展開します。

k. CLIでのHAステータスの確認

各インスタンスのHAステータスは、ASAと同じFirepower CLIでも確認されます。

show running-config failover および show failover コマンドを実行して、FTD1_FTD01(プライマリインスタンス01)のHAステー タスを確認します。

<#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

show running-config failover および show failover コマンドを実行して、FTD1_FTD11のHAステータス(プライマリInstance02)を 確認します。

<#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

show running-config failover および show failover コマンドを実行して、FTD2_FTD02(セカンダリインスタンス01)のHAステー タスを確認します。

<#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-

show running-config failover および show failover コマンドを実行して、FTD2_FTD12(セカンダリInstance02)のHAステータスを 確認します。

<#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-

1.ライセンス消費の確認

すべてのライセンスは、コンテナインスタンスごとではなく、セキュリティエンジン/シャーシごとに消費されます。

・ベースライセンスは自動的に割り当てられます:セキュリティエンジン/シャーシごとに1つ。

・機能ライセンスは各インスタンスに手動で割り当てられますが、使用するライセンスは機能エンジン/シャーシあたり1つだけで す。特定の機能ライセンスで必要なライセンスは、使用中のインスタンスの数に関係なく、合計1つだけです。

次の表に、このドキュメントでライセンスがどのように消費されるかを示します。

FPR01	インスタンス01	ベース、URLフィルタリング、マルウェア、脅 威
	インスタンス02	ベース、URLフィルタリング、マルウェア、脅 威
FPR02	インスタンス01	ベース、URLフィルタリング、マルウェア、脅 威
	インスタンス02	ベース、URLフィルタリング、マルウェア、脅 威

ライセンスの総数

ベース	URL フィルタリング	マルウェア	脅威
2	2	2	2

FMC GUIで消費されたライセンス数を確認します。

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 Th	reat Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
$^{\sim}$ Mahware (2)	In-Compliance					
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
\checkmark Threat (2)	In-Compliance					
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	 In-Compliance 	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	reat Defense	Global	N/A	
✓ URL Filtering (2)	 In-Compliance 					
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	eat Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	eat Defense	Global	N/A	

使用したライセンスの確認

確認

FTD1_FTD01(プライマリインスタンス01)でクラッシュが発生すると、インスタンス01のフェールオーバーがトリガーされ、ス タンバイ側のデータインターフェイスが元のアクティブインターフェイスのIP/MACアドレスを引き継いで、トラフィック(この ドキュメントではFTP接続)がFirepowerによって継続的に渡されるようにします。



クラッシュ前



クラッシュ中



フェールオーバーがトリガーされる

ステップ1:Win10-01からWin10-02へのFTP接続を開始します。

ステップ2: show conn コマンドを実行して、Instance01の両方でFTP接続が確立されていることを確認します。

<#root>

// 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

ステップ3:Win10-03からWin10-04へのFTP接続を開始します。

ステップ4: show conn コマンドを実行して、FTP接続が両方のInstance02で確立されていることを確認します。

<#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

ステップ 5: connect ftd FTD01コマンドおよび system support diagnostic-cliコマンドを実行して、ASA CLIに入ります。 enableおよ び crashinfo force watchdog コマンドを実行して、プライマリ/アクティブ装置のInstance01を強制的にクラッシュさせます。

<#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]:

手順 6: Instance01でフェールオーバーが発生し、FTP接続は中断されません。 show failoverコマンドおよび show connコマンドを 実行して、FPR02でのInstance01のステータスを確認します。

<#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

手順7:Instance01で発生したクラッシュは、Instance02には影響を及ぼしませんでした。 show failoverコマンドおよび show connコ マンドを実行して、Instance02のステータスを確認します。

<#root>

>

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

ステップ8:FMCで、Devices > Allの順に移動します。HAステータスを確認します。

・FTD1_FTD01:プライマリ、スタンバイ

・FTD2_FTD02:セカンダリ、アクティブ

Fin Dev	ewall Management Center Overview Analysis	Policies Devices Object	ts Integratio	n			Deploy Q	admin • 付 SECURE			
View By:	View Dy: Group • Deployment History										
Collapse All											
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack				
	Ungrouped (2)										
	V FTD01_FTD02_HA Hgh Availability							11			
	FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	III Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4D	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	49	1			
	V FTD11_FTD12_HA High Availability							11			
	FTD1_FTD11(Primary, Active) Snort 3 Granulation - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1			
	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	\$	1			

HAステータスの確認

ステップ9:(オプション)FPR01のInstance01が通常に戻った後で、手動でHAのステータスを切り替えることができます。これは、FMC GUIまたはFRP CLIのいずれかによって実行できます。

FMCで、Devices > Allの順に移動します。Switch Active Peerをクリックして、FTD01_FTD02_HAのHAステータスをスイッチします。

E Fi	rewall Management Center Overview Analysis	Policies Devices Obje	cts Integration	n.			Deploy Q 🧔	admin dete SECURE
View By: All (4)	Group • • Error (0) • Warning (0) • Offline (0) • Normal (4)	Deployment Pending (0)	Upgrade (0)	▶ Snort 3 (4)				Deployment History Q, Search Device Add
Collapse Al								
	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	III Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	Q+	Force refresh node status Delete Revert Upgrade
	FTD2_FTD02(Secondary, Active) Short 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	45	Health Monitor Troubleshoot Files
	✓ FTD11_FTD12_HA High Availability							×1
	FTD1_FTD11(Primary, Active) Short 3 Committee 1 - Routed	Firepower 4145 with FTD	7.2.5	EREFERENCE FOR A Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	:
	FTD2_FTD12(Secondary, Standby) Short 3 Anto1.10.2 = Routed	Firepower 4145 with FTD	7.2.5	Erepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	<d< td=""><td>1</td></d<>	1

スイッチのHAステータス

Firepower CLIで、 connect ftd FTD01コマンドと system support diagnostic-cliコマンドを実行し、ASA CLIに入ります。 FTD01_FTD02_HAのHAをスイッチするために、 enableおよび failover active コマンドを実行します。

<#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

トラブルシュート

フェールオーバーのステータスを検証するには、 show failover コマンドと show failover history コマンドを実行します。

<#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

debug fover コマンドを実行して、フェールオーバーのデバッグログを有効にします。

<#root>

>

debug fover

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

参考

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 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。