# FDMを使用したFTDの高可用性の構成

内容

 はじめに

 前提条件

 要件

 使用するコンボーネント

 Network Topology

 設定

 ハイアベイラビリティのためのプライマリユニットの設定

 セカンダリユニットをハイアベイラビリティに設定する

 確認

## はじめに

このドキュメントでは、ローカルで管理されるセキュアファイアウォール脅威対策(FTD)のアク ティブ/スタンバイのハイアベイラビリティ(HA)ペアをセットアップする方法について説明します 。

#### 前提条件

#### 要件

次の項目に関する知識があることが推奨されます。

• Cisco Secure Firewall Threat Defenseの初期設定(GUIまたはシェル経由)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

• FPR2110バージョン7.2.5はFirepower Device Manager(FDM)によってローカルで管理され ます。

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。

### **Network Topology**



注:このドキュメントで説明している例は、複数の推奨ネットワーク設計のうちの1つで す。その他のオプションについては、設定ガイドの『フェールオーバーとデータリンク の中断の回避』を参照してください。



ハイアベイラビリティのためのプライマリユニットの設定

ステップ1: Deviceをクリックして、右上隅のHigh Availabilityステータスの横にあるConfigureボ タンを押します。



ステップ2: High Availabilityページで、Primary Deviceボックスをクリックします。

Firewall De	vice Manager	面 Monitoring	Ø Policies	識 Objects	Device: ftd-primary		6.	٢	0	?	:	admin Administrator	~	eisee SECURE
	Device Summary High Availa	bility												
	How High Av	ailability Works											~	
Select the role for this device The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first. The secondary device remains in standby mode until the primary unit becomes unavailable.														
				Ø P	rimary Device	Secondary	Device	0						

ステップ3:フェールオーバーリンクのプロパティを設定します。

セカンダリファイアウォールに直接接続したインターフェイスを選択し、プライマリおよびセカ ンダリのIPアドレスとサブネットネットマスクを設定します。

ステートフルフェールオーバーリンクの、Use the Same Interface as the Failover Linkチェックボックスをチェックします。

IPSec Encryption Keyボックスのチェックマークを外し、Activate HAをクリックして変更を保存 します。

I have configuration of peer device in clipboard PASTE FROM CLIPBOARD	
FAILOVER LINK	STATEFUL FAILOVER LINK Use the same interface as the Failover Link
Interface	Interface
unnamed (Ethernet1/7) V	unnamed (Ethernet1/7) ~
Type IPv4 IPv6 Primary IP 10.1.1.1	Type IPv4 IPv6 Primary IP 10.1.1.1
e.g. 192.168.10.1	e.g. 192.168.11.1
Secondary IP 10.1.1.2 e.g. 192.168.10.2	Secondary IP 10.1.1.2 e.g. 192.168.11.2
Netmask	Netmask
255.255.255.252	255.255.255.252
e.g. 255.255.255.0 or 24	e.g. 255.255.255.0 or 24
IPSec Encryption Key (optional) For security purposes, the encryption key will not be included in the configuration copied to the clipboard when you activate HA. You will need to manually enter the key when you configure HA on the peer device.	IMPORTANT If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More
Before you activate HA, make sure both devices have the same Smart License and Cloud Regi	on. Otherwise HA will not work.
When you click Activate HA, these settings are automatically deployed to the dev momentary traffic loss. It might take a few minutes for deployment to finish.	ice. The deployment might restart inspection engines, which can result in the
Information is copied to the clipboard when deployment is done. You must allow the clipboard when deployment is done.	the browser to access your clipboard for the copy to be successful.





ヒント:フェールオーバートラフィック専用の小さなマスクサブネットを使用して、セ キュリティ違反やネットワークの問題をできるだけ回避します。



警告:システムは即座に設定をデバイスに展開します。配置ジョブを開始する必要はあ りません。構成が保存され、展開が進行中であるというメッセージが表示されない場合 は、ページの上部までスクロールしてエラーメッセージを表示します。設定もクリップ ボードにコピーされます。コピーを使用すると、セカンダリユニットをすばやく設定で きます。セキュリティを強化するため、暗号化キー(設定されている場合)はクリップ ボードのコピーに含まれません。

ステップ 4:設定が完了すると、次の手順を説明するメッセージが表示されます。情報を読んだら、Got Itをクリックします。

the	You have successfully deployed HA configuration on the primary device. What's next? need to configure Peer Device I configured both devices	×
(1	Copy the HA configuration to the clipboard.	
2	Paste it on the secondary device. Log into the secondary device and open the HA configuration page.	
	You are done! The devices should communicate and establish a high availability pair automatically.	
	GOT IT	

#### セカンダリユニットをハイアベイラビリティに設定する

ステップ 1 : Deviceをクリックして、右上隅のHigh Availabilityステータスの横にあるConfigureボ タンを押します。

Firewall Device Manager Monitoring	Policies Objects	1 Device: ftd-secondary	admin Administrator
Model Cisco Firepower 2110 Thr	Software eat Defense 7.2.5-208	VDB Intrusion Rule Update Cloud Services 370.0 20230925-1455 Connected	SEC TAC Not Configured
FC Inside Network	Cisco Firepower 2110 Threat MMM 1/1 Console Console 1/2 1	1/2 Defense ● 1/3 1/5 1/7 1/9 1/11 ● ● ● ● ● ● ● ■ 1/13 1/14 1/15 1/16 ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	ISP/WAN/Gateway

#### ステップ2: High Availabilityページで、Secondary Deviceボックスをクリックします。

Firewall D	evice Manager 🕅 🎯	bies Objects Device: ftd-secondary	o 🖨 🗐 ?	admin Administrator	JRE				
	Device Summary High Availability								
	How High Availability Works			×					
Select the role for this device The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first. The secondary device remains in standby mode until the primary unit becomes unavailable.									
		Primary Device     or	Secondary Device						

ステップ3:フェールオーバーリンクのプロパティを設定します。プライマリFTDを設定した後、クリップボードに保存されている設定を貼り付けるか、手動で続行できます。

ステップ 3.1:クリップボードからペーストするには、Paste from Clipboardボタンをクリックし 、設定をペースト(Ctrl+Vを同時に押します)して、OKをクリックします。

Select the role for this device The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first.
The secondary device remains in standby mode until the primary unit becomes unavailable.
Primary Device     or     Secondary Device     G
I have configuration of peer device in clipboard PASTE FROM CLIPBOARD

```
Paste here Peer Device Configuration
```

FAILOVER LINK CONFIGURATION Interface: Ethernet1/7 Primary IP: 10.1.1.1/255.255.255.252 Secondary IP: 10.1.1.2/255.255.255.252

STATEFUL FAILOVER LINK CONFIGURATION Interface: Ethernet1/7 Primary IP: 10.1.1.1/255.255.255.252 Secondary IP: 10.1.1.2/255.255.255.252

(	CANCEL	ОК	

ステップ 3.2:手動で続行するには、セカンダリファイアウォールに直接接続したインターフェ イスを選択し、プライマリおよびセカンダリのIPアドレスとサブネットネットマスクを設定しま す。ステートフルフェールオーバーリンクの、Use the Same Interface as the Failover Linkチェッ クボックスをチェックします。

×

I have configuration of peer device in clipboard	PASTE FROM CLIPBOARD		
FAILOVER LINK		STATEFUL FAILOVER LINK	Use the same interface as the Failover Link
Interface		Interface	
unnamed (Ethernet1/7)	~	unnamed (Ethernet1/7)	~
Type IPv4 IPv6 Primary IP 10.1.1.1 e.g. 192.168.10.1		Type IPv4 IPv6 Primary IP 10.1.1.1 e.g. 192.168.11.1	
Secondary IP		Secondary IP	
10.1.1.2		10.1.1.2	
orge i san i son i son		e.g. rozrowiria	
Netmask		Netmask	
255.255.255.252		255.255.255.252	
e.g. 255.255.255.0 or 24		e.g. 255.255.255.0 or 24	
IPSec Encryption Key (optional) For security purposes, the encryption key will not be includ clipboard when you activate HA. You will need to manually enter the key when you configure	ed in the configuration copied to the HA on the peer device.	IMPORTANT If you configure an IPsec encryption ke features, both devices will become ac	ly with inconsistent settings for export controlled tive after you activate HA. Learn More 🖒
Before you activate HA, make sure both devices hav	e the same Smart License and Cloud Regi	ion. Otherwise HA will not work.	action annings, which can result in the
momentary traffic loss. It might take a few m	nutes for deployment to finish.	vice. The deployment might restart insp	voction engines, which can result in the
Information is copied to the clipboard when one of the clipboard wh	leployment is done. You must allow	the browser to access your clipboard	or the copy to be successful.
	ACTIV	ATE HA	

ステップ 4:IPSec Encryption Keyボックスのチェックマークを外し、Activate HAをクリックし て変更を保存します。



警告:システムは即座に設定をデバイスに展開します。配置ジョブを開始する必要はありません。構成が保存され、展開が進行中であるというメッセージが表示されない場合は、ページの上部までスクロールしてエラーメッセージを表示します。

ステップ 5:設定が完了すると、次に実行する必要がある手順を説明するメッセージが表示され ます。情報を読んだら、Got Itをクリックします。

the H	You have successfully deployed A configuration on the primary device. What's next? ed to configure Peer Device I configured both devices	×
1	Copy the HA configuration to the clipboard.	
2	Paste it on the secondary device. Log into the secondary device and open the HA configuration page.	
	You are done! The devices should communicate and establish a high availability pair automatically.	
	GOT IT	

## 確認

 この時点で、デバイスのステータスは、[ハイアベイラビリティ]ページでセカンダリデバイ スであることを示します。プライマリデバイスとの結合に成功すると、デバイスはプライマ リとの同期を開始し、最終的にモードがスタンバイに、ピアがアクティブに変更されます。



 プライマリFTDでは、ほとんどの場合、ハイアベイラビリティステータスが表示されますが 、アクティブおよびピア:スタンバイと表示されます。

Firewall Device Manager Monitoring	Policies Objects Devic	e: ftd-primary		administrator
	Model Cisco Firepower 2110 Threat Defense	Software         VDB         Intrusion Rule Update         C           7.2.5-208         370.0         20230925-1455         6	Cloud Services High Availability Connected   SEC TAC Primary Device: Active	Peer: Standby
				Internet
	Cisco Fin	epower 2110 Threat Defense MCMT 1/1 1/3 1/5 1/7 1/9 1/11		DNS Server
	Inside Network		1/14 1/15 1/16 ISP/WAN/Gateway	NTP Server
		11		

プライマリFTDとのSSHセッションを開き、show running-config failoverコマンドを発行して設定を確認します。



• show failover stateコマンドを使用して、デバイスの現在のステータスを検証します。

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

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。