# Configuration de la haute disponibilité FTD avec FDM

## Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Topologie du réseau
Configurer
Configuration de l'unité principale pour la haute disponibilité
Configuration de l'unité secondaire pour la haute disponibilité
Vérifier

# Introduction

Ce document décrit comment configurer une paire haute disponibilité (HA) active/de secours de défense contre les menaces de pare-feu (FTD) gérée localement.

# Conditions préalables

#### Exigences

Il est recommandé de connaître les sujets suivants :

• Configuration initiale de Cisco Secure Firewall Threat Defense via une interface utilisateur graphique et/ou un shell.

#### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• FPR2110 version 7.2.5 gérée localement par Firepower Device Manager (FDM)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

### Topologie du réseau



Remarque : l'exemple décrit dans ce document est l'une des multiples conceptions de réseau recommandées. Référez-vous au guide de configuration <u>Éviter le basculement</u> <u>interrompu et les liaisons de données</u> pour plus d'options.



# Configurer

Configuration de l'unité principale pour la haute disponibilité

Étape 1. Cliquez sur Device et appuyez sur le bouton Configure situé dans le coin supérieur droit, à côté de l'état High Availability.



Étape 2. Sur la page High Availability, cliquez sur la zone Primary Device.

Firewall Dev	vice Manager	Monitoring	Policies	章王 Objects	Device: ftd-primary		6	٢	۲	?	:	admin Administrator	×	eiseo 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.														
				P	trimary Device or	Secondary	Device	0						

Étape 3. Configurez les propriétés Failover Link.

Sélectionnez l'interface que vous avez connectée directement à votre pare-feu secondaire et définissez les adresses IP principale et secondaire ainsi que le masque de réseau de sous-réseau.

Cochez la case Utiliser la même interface que le lien de basculement pour le lien de basculement dynamique.

Décochez la case IPSec Encryption Key et cliquez sur Activate HA pour enregistrer les modifications.

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.





Conseil : utilisez un petit sous-réseau de masque, dédié au trafic de basculement uniquement pour éviter autant que possible les failles de sécurité et/ou les problèmes réseau.



Avertissement : le système déploie immédiatement la configuration sur le périphérique. Vous n'avez pas besoin de démarrer une tâche de déploiement. Si aucun message indiquant que votre configuration a été enregistrée et que le déploiement est en cours ne s'affiche, faites défiler la page jusqu'en haut pour afficher les messages d'erreur. La configuration est également copiée dans le Presse-papiers. Vous pouvez utiliser la copie pour configurer rapidement l'unité secondaire. Pour plus de sécurité, la clé de cryptage (si vous en définissez une) n'est pas incluse dans la copie du Presse-papiers.

Étape 4. Une fois la configuration terminée, vous obtenez un message expliquant les étapes suivantes. Cliquez sur Got It après avoir lu les informations.

You have successfully deployed the HA configuration on the primary device. What's next? I need to configure Peer Device I configured both devices	×
Copy the HA configuration to the clipboard. Copied Click here to copy again	
<ul> <li>Paste it on the secondary device.</li> <li>Log into the secondary device and open the HA configuration page.</li> </ul>	
You are done! The devices should communicate and establish a high availability pair automatically.	
GOT IT	

Configuration de l'unité secondaire pour la haute disponibilité

Étape 1. Cliquez sur Device et appuyez sur le bouton Configure situé dans le coin supérieur droit, à côté de l'état High Availability.

Firewall Device Manager Monitoring	Policies Object	IS 1 Device: ftd-secondary	۵.	@ ? :	admin Administrator	cisco SECURE
Model Cisco Firepower 2110 Thr	Software eat Defense 7.2.5-208	VDB Intrusion Rule Update 370.0 20230925-1455	Cloud Services Connected   SEC TAC	High Availability () Not Configured	CONFIGURE	
FC Inside Network	Cisco Firepower 2110 The MOMT 1/1 CONSOLE 1/2	1/3 1/5 1/7 1/9 1/11 1/3 1/5 1/7 1/9 1/11 1/13 1/13 1/13 1/13 1/13 1/13 1/13 1/13 1/13 1/13 1/13 1/13 1/13 1/15 1/13 1/15 1/13 1/15	3 1/14 1/15 1/16 p	ISP/WAN/Gateway	Internet     DNS Server     ONTP Server     ONTP Server     deale Smart License	

Étape 2. Sur la page Haute disponibilité, cliquez sur la zone Périphérique secondaire.

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

Étape 3. Configurez les propriétés Failover Link. Vous pouvez coller les paramètres stockés dans votre Presse-papiers après avoir configuré le FTD principal ou continuer manuellement.

Étape 3.1. Pour coller à partir du Presse-papiers, cliquez simplement sur le bouton Coller à partir du Presse-papiers, collez dans la configuration (touches Ctrl+v simultanément) et cliquez sur OK.

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

```
Paste here Peer Device Configuration
FAILOVER LINK CONFIGURATION
Interface: Ethernet1/7
Primary IP: 10.1.1.1/255.255.252
Secondary IP: 10.1.1.2/255.255.252
STATEFUL FAILOVER LINK CONFIGURATION
Interface: Ethernet1/7
Primary IP: 10.1.1.1/255.255.255.252
Secondary IP: 10.1.1.2/255.255.252
```

Étape 3.2. Pour continuer manuellement, sélectionnez l'interface que vous avez connectée directement à votre pare-feu secondaire et définissez les adresses IP principale et secondaire ainsi que le masque de réseau de sous-réseau. Cochez la case Utiliser la même interface que le lien de basculement dynamique.

I have configuration of peer device in clipboard	PASTE FROM CLIPBOARD		
FAILOVER LINK		STATEFUL FAILOVER LINK	Use the same interface as the Fallover Link
Interface		Interface	-
unnamed (Ethernet1/7)	~	unnamed (Ethernet1/7)	~
Type  IPv4 IPv6  Primary IP		Type IPv4 IPv6 Primary IP	
10.1.1.1		10.1.1.1	
e.g. 192.168.10.1		e.g. 192.168.11.1	
Secondary IP		Secondary IP	
10.1.1.2		10.1.1.2	
e.g. 192.168.10.2		e.g. 192.168.11.2	
Netmask		Netmask	
255.255.255.252		255.255.255.252	
e.g. 255.255.255.0 or 24		e.g. 255.255.255.0 or 24	
IPSec Encryption Key (optional) For security purposes, the encryption key will not be 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	ey with inconsistent settings for export controlled tive after you activate HA. Learn More (2
Before you activate HA, make sure both devices have     When you click Activate HA, these settings a	the same Smart License and Cloud Reginer results and Cloud Reginer results and Cloud Reginer results and the reginere resul	ion. Otherwise HA will not work. vice. The deployment might restart ins;	pection engines, which can result in the
momentary traffic loss. It might take a few mi	nutes for deployment to finish.		
Information is copied to the clipboard when a	leployment is done. You must allow	the browser to access your clipboard	for the copy to be successful.
	ACTIV	YATE HA	

Étape 4. Décochez la case IPSec Encryption Key et cliquez sur Activate HA pour enregistrer les modifications.



Avertissement : le système déploie immédiatement la configuration sur le périphérique. Vous n'avez pas besoin de démarrer une tâche de déploiement. Si aucun message indiquant que votre configuration a été enregistrée et que le déploiement est en cours ne s'affiche, faites défiler la page jusqu'en haut pour afficher les messages d'erreur.

Étape 5. Une fois la configuration terminée, vous obtenez un message expliquant les étapes suivantes à suivre. Cliquez sur Got It après avoir lu les informations.

You have successfully deployed the HA configuration on the primary device. What's next?	×
<ul> <li>Copy the HA configuration to the clipboard.</li> <li>Copied Click here to copy again</li> <li>Paste it on the secondary device.</li> <li>Log into the secondary device and open the HA configuration</li> </ul>	
page. You are done! The devices should communicate and establish a high availability pair automatically.	
<u>бот п</u>	

## Vérifier

 À ce stade, l'état de votre périphérique indique généralement qu'il s'agit du périphérique secondaire sur la page Haute disponibilité. Si la jonction avec le périphérique principal a réussi, le périphérique commence à se synchroniser avec le périphérique principal, et finalement le mode est changé en Standby et l'homologue en Active.

	This device is part of a high availability (HA) pair and is currently in standby state. With few exceptions, you cannot edit the configuration for this device. To make any changes, please log into the active unit. Learn More (2)										
Firewall Device Manager	Monitoring Policies Objects	Device: ftd-primary	admin dministrator disco SECURE								
	Model Cisco Firepower 2110 Threat	High Availability Secondary Device: Standby $\Rightarrow$ Peer: Active									
	Finalde Network	Internet									

• Le FTD principal doit également afficher l'état Haute disponibilité, mais aussi Actif et Homologue : En veille.



• Ouvrez une session SSH sur le FTD principal et exécutez la commande show running-config failover pour vérifier la configuration.



• Validez l'état actuel du périphérique à l'aide de la commande show failover state.

> 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								
>									

#### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.