Configuration de la haute disponibilité FTD avec FDM

Table des matières

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.

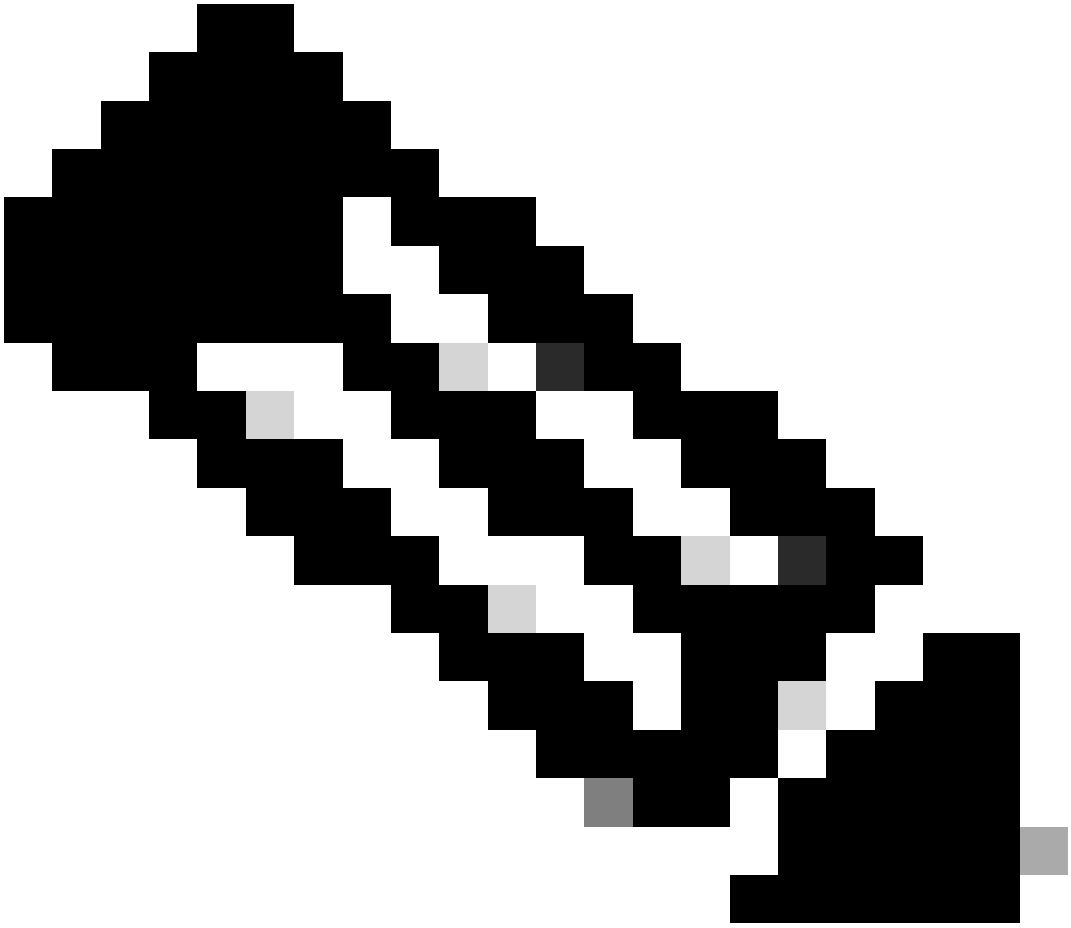
Composants utilisés

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

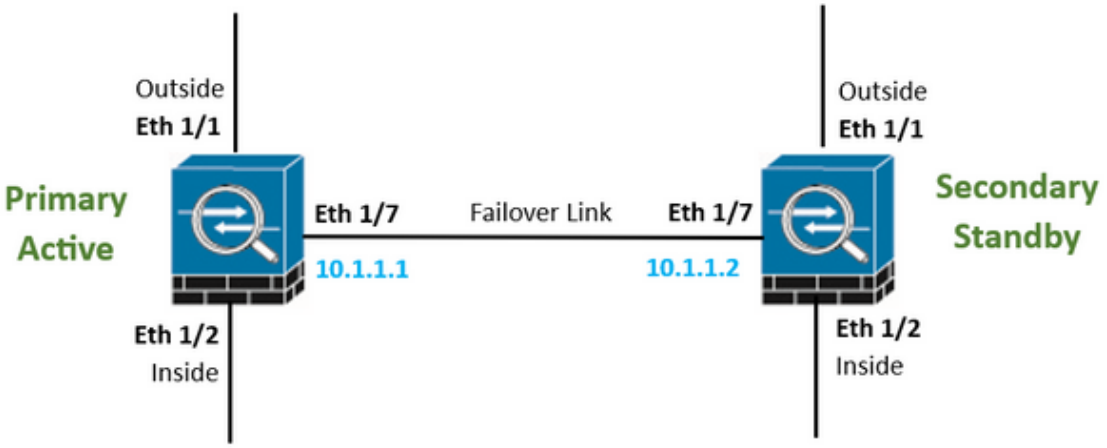
- FPR2110 version 7.2.5 gérée localement par Firepower Device Manager (FDM)

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



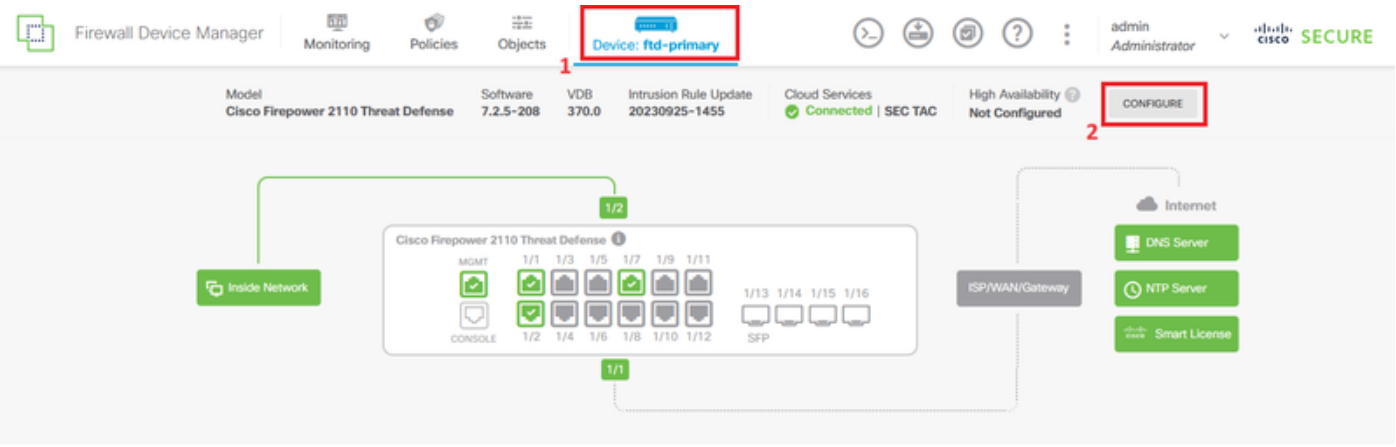
Remarque : l'exemple décrit dans ce document est l'une des multiples conceptions de réseau recommandées. Référez-vous au guide de configuration Éviter le basculement interrompu et les liaisons de données pour plus d'options.



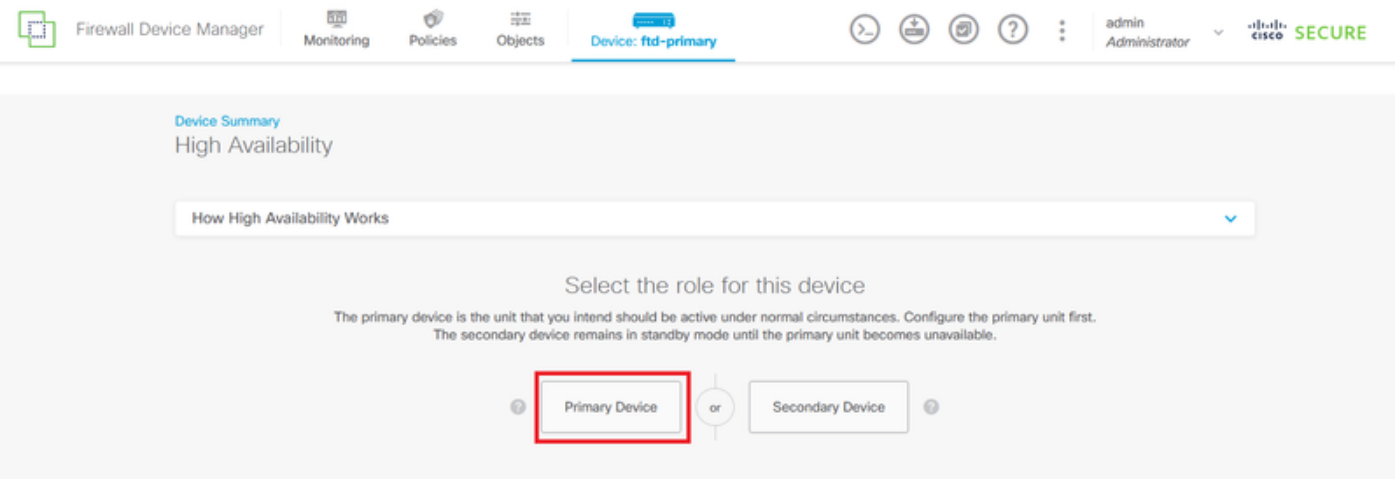
Configurer

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.



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

Interface

unnamed (Ethernet1/7)

Type

IPv4 IPv6

Primary IP

10.1.1.1

e.g. 192.168.10.1

Secondary IP

10.1.1.2

e.g. 192.168.10.2

Netmask

255.255.255.252

e.g. 255.255.255.0 or 24

STATEFUL FAILOVER LINK

Use the same interface as the Failover Link

Interface

unnamed (Ethernet1/7)

Type

IPv4 IPv6

Primary IP

10.1.1.1

e.g. 192.168.11.1

Secondary IP

10.1.1.2

e.g. 192.168.11.2

Netmask

255.255.255.252

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

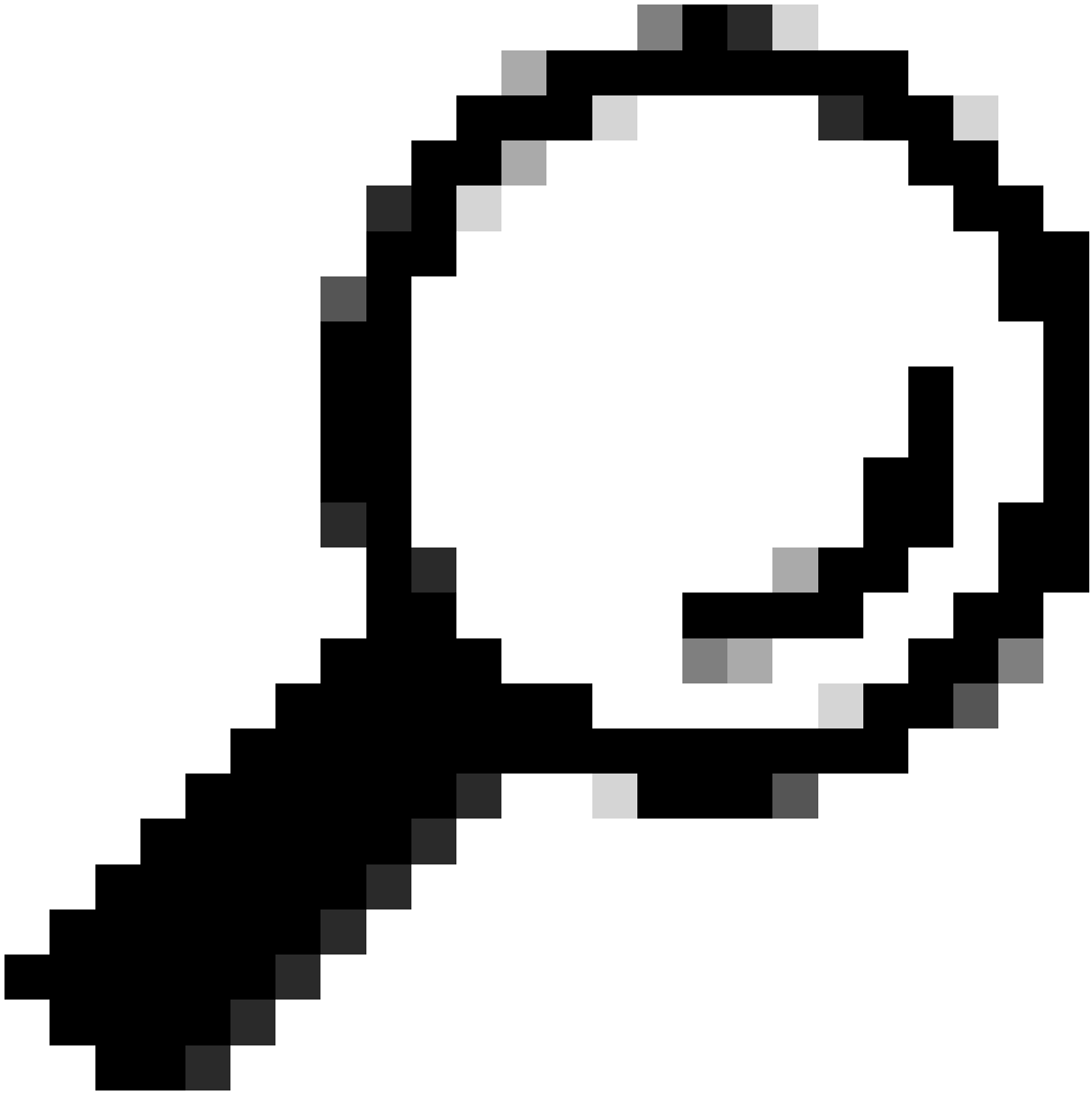
If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More

Before you activate HA, make sure both devices have the same Smart License and Cloud Region. Otherwise HA will not work.

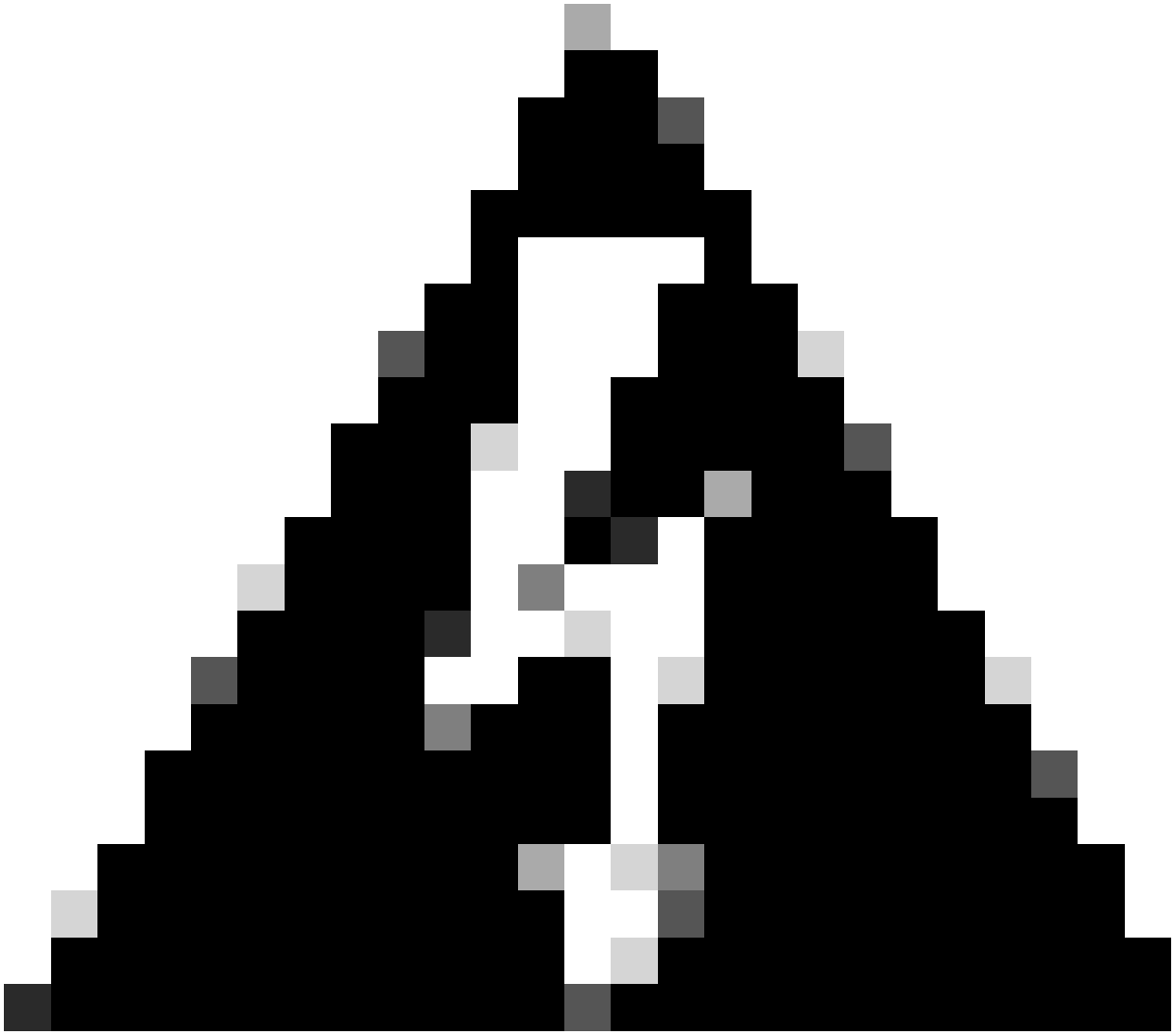
When you click Activate HA, these settings are automatically deployed to the device. The deployment might restart inspection engines, which can result in the momentary traffic loss. It might take a few minutes for deployment to finish.

Information is copied to the clipboard when deployment is done. You must allow the browser to access your clipboard for the copy to be successful.

ACTIVATE HA

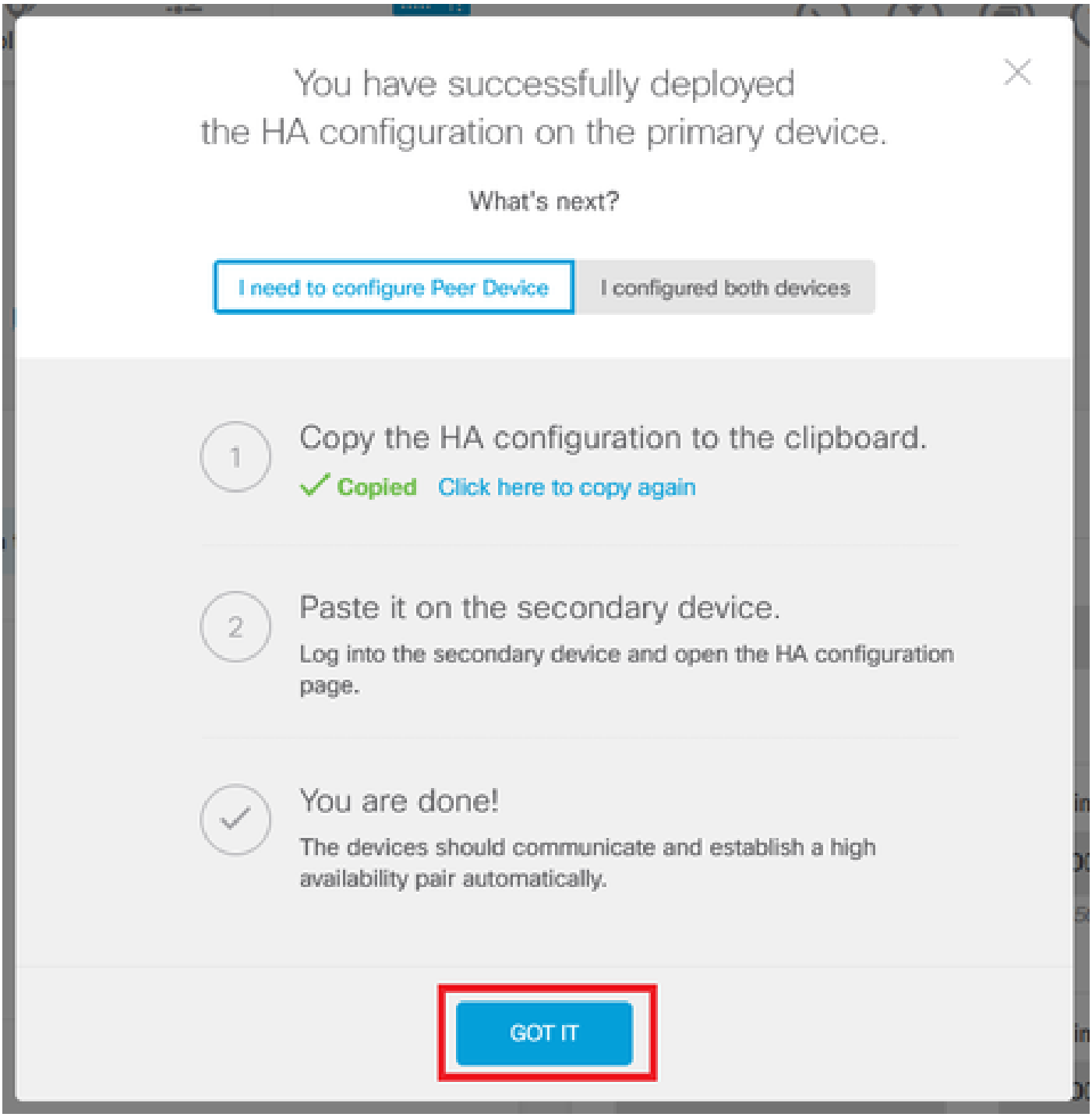


Conseil : utilisez un petit sous-réseau de masque, dédié au trafic de basculement uniquement pour éviter autant que possible les failles de sécurité et/ou les problèmes réseau.



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.

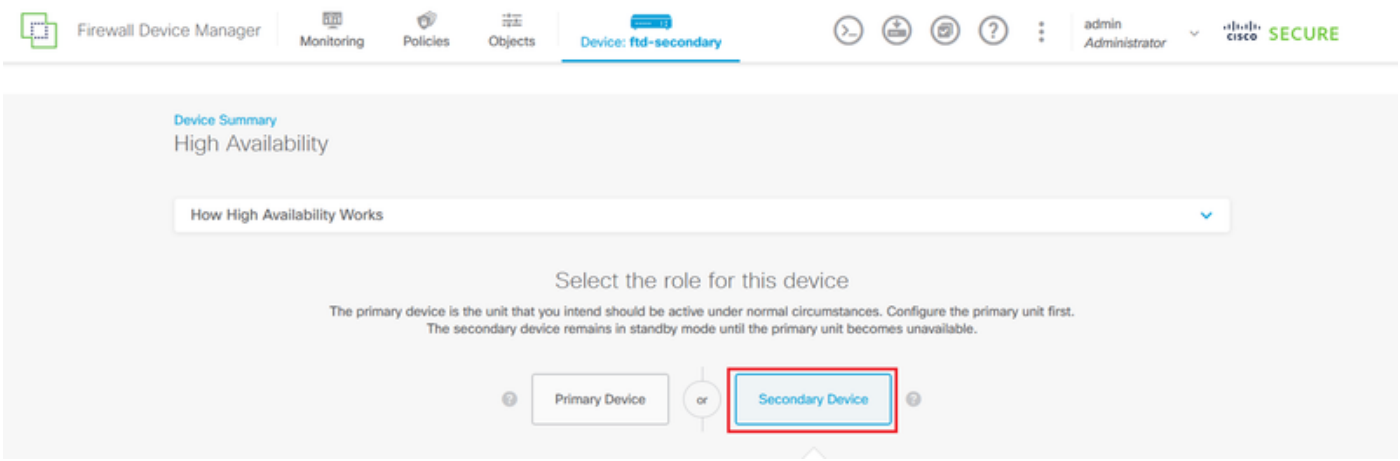
Étape 4. Une fois la configuration terminée, vous obtenez un message expliquant les étapes suivantes. Cliquez sur Got It après avoir lu les informations.



Configuration de l'unité secondaire pour la haute disponibilité

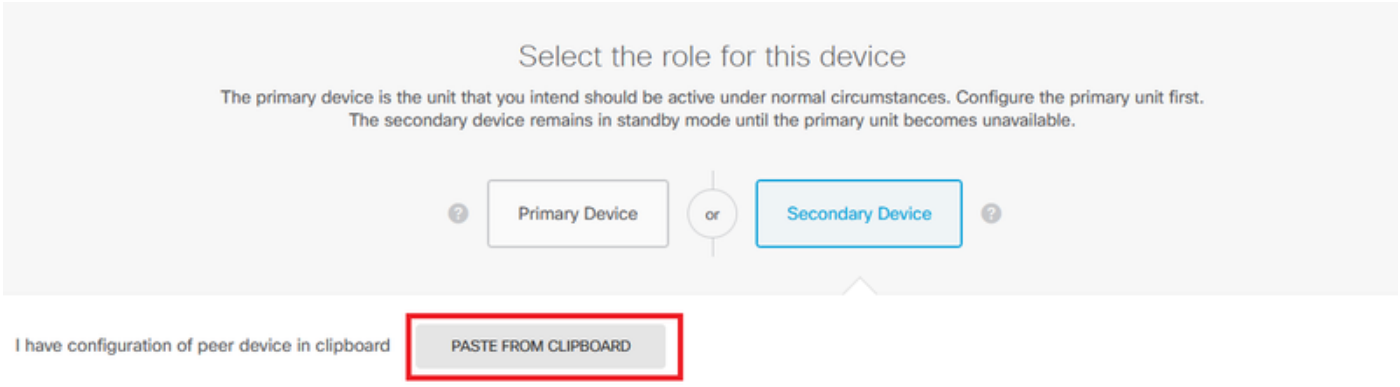
Étape 1. Cliquez sur Device et appuyez sur le bouton Configure situé dans le coin supérieur droit, à côté de l'état High Availability.

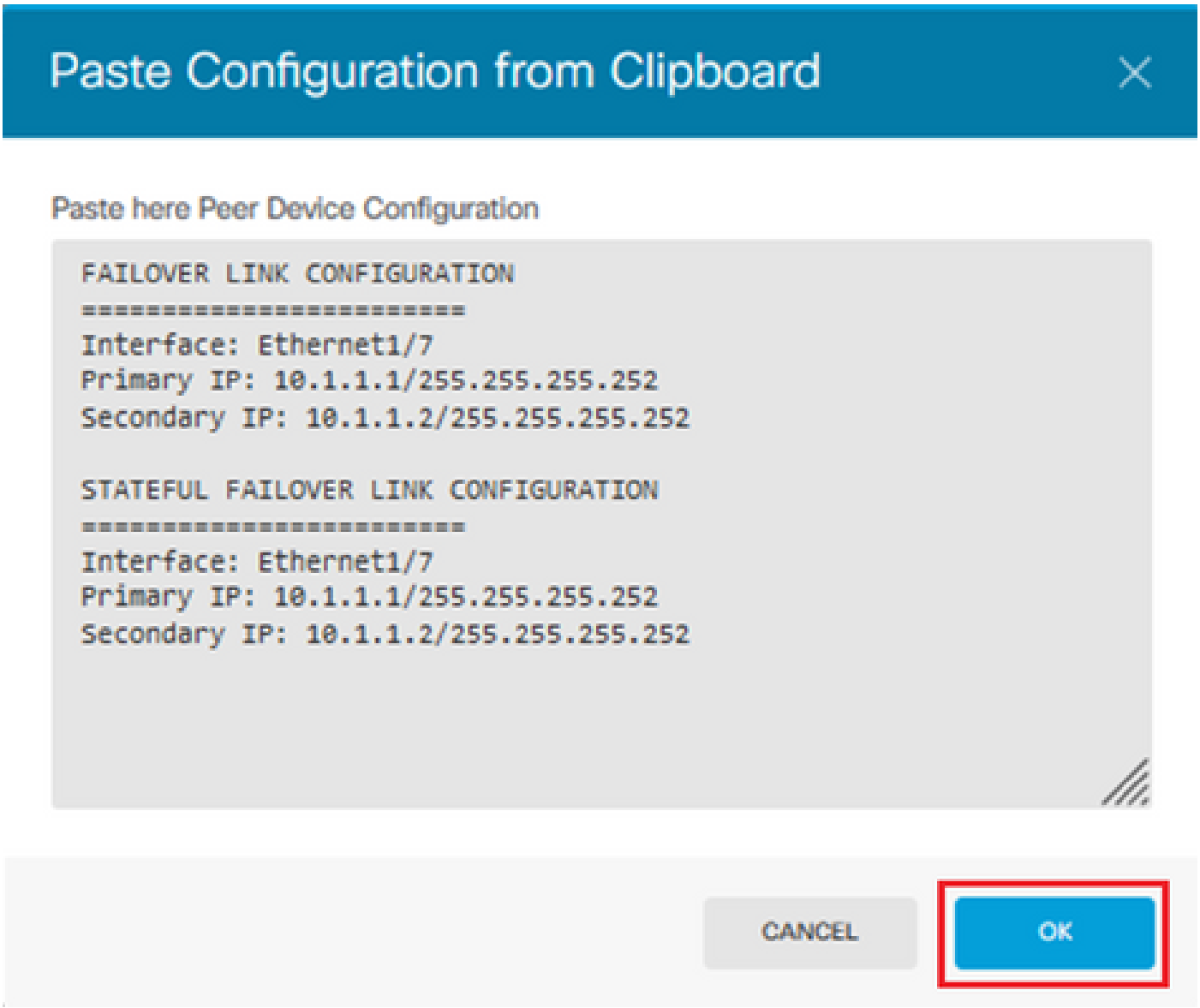
Étape 2. Sur la page Haute disponibilité, cliquez sur la zone Périphérique secondaire.



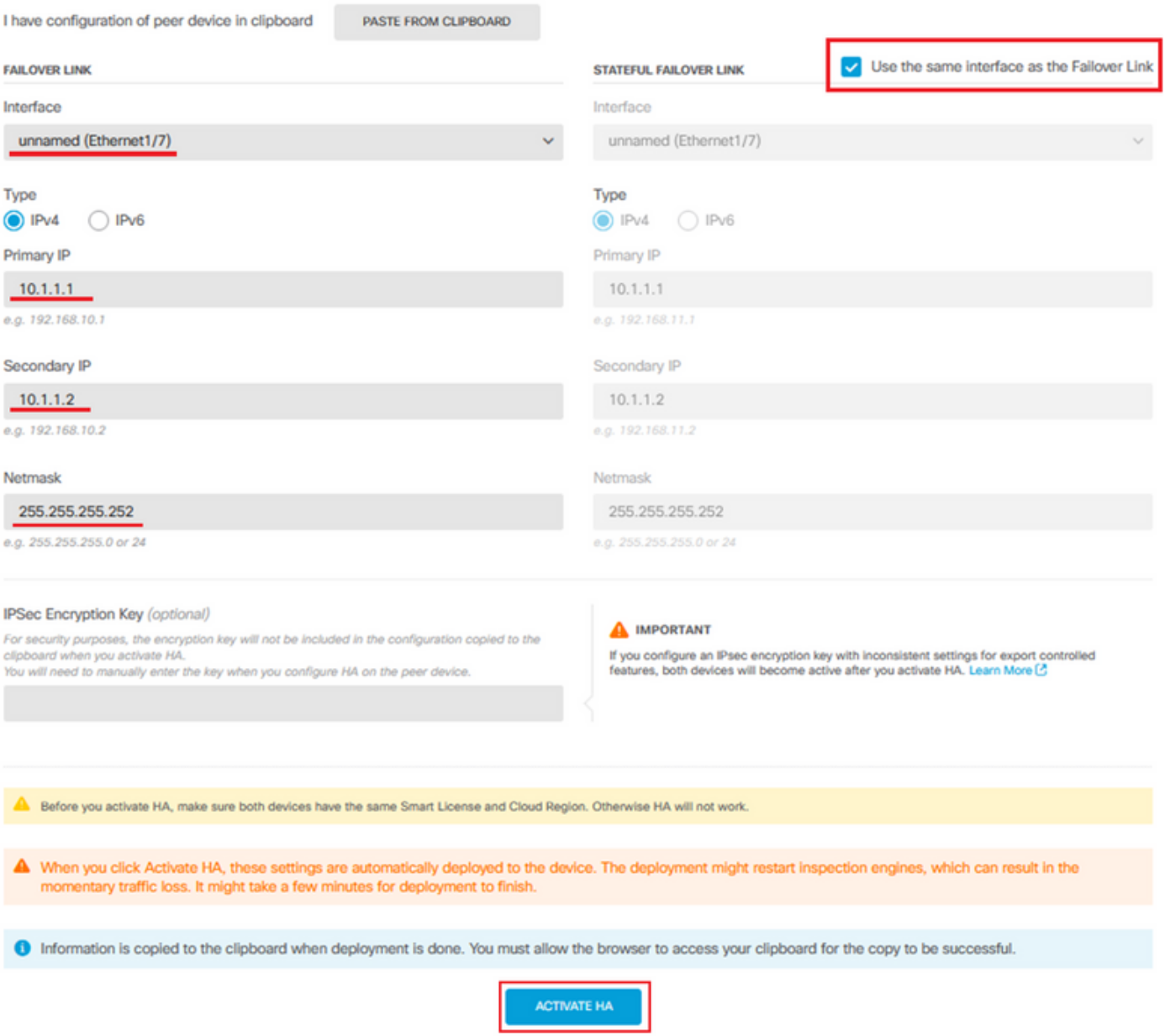
Étape 3. Configurez les propriétés Failover Link. Vous pouvez coller les paramètres stockés dans votre Presse-papiers après avoir configuré le FTD principal ou continuer manuellement.

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.

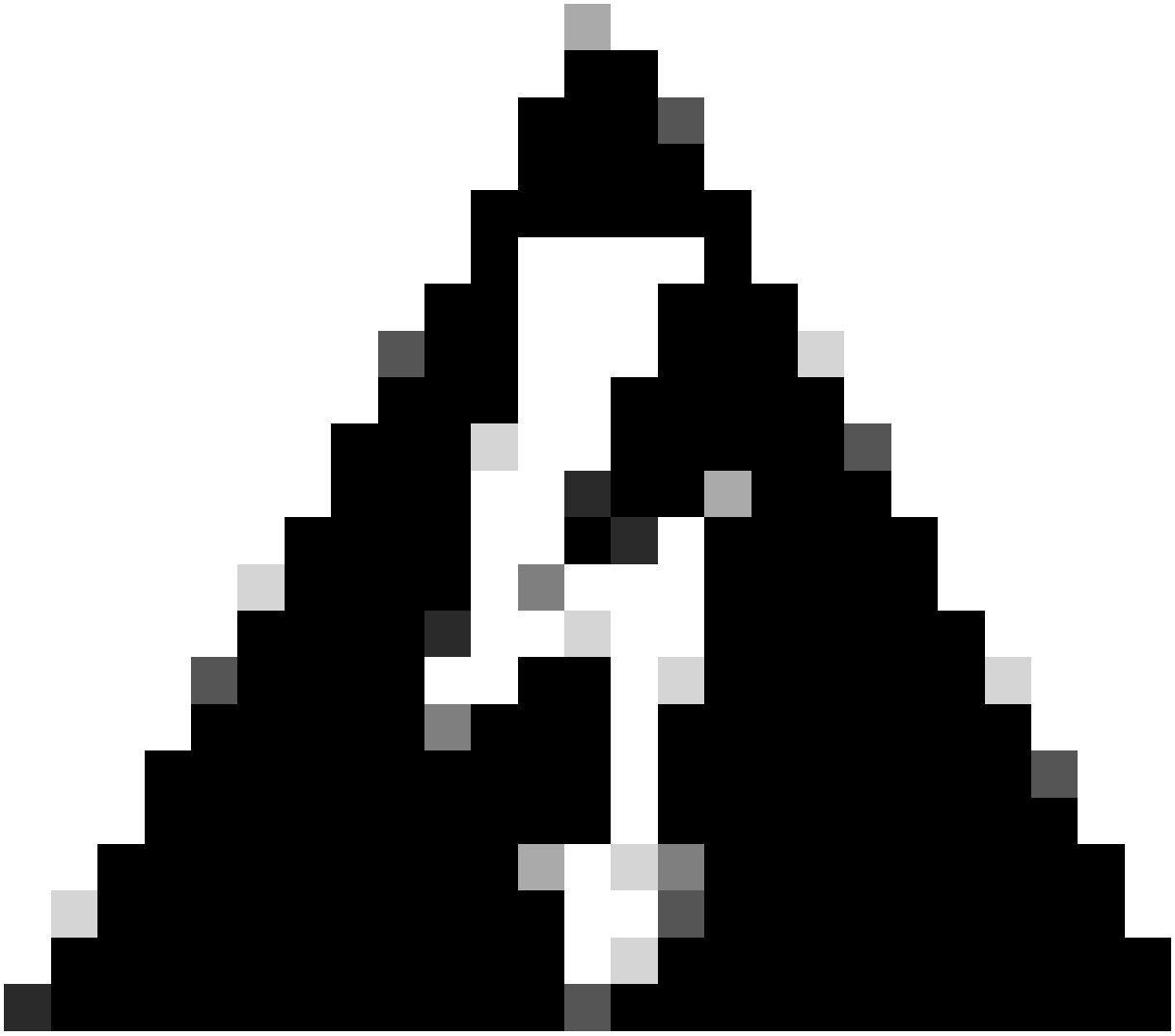




Étape 3.2. Pour continuer manuellement, sélectionnez l'interface que vous avez connectée directement à votre pare-feu secondaire et définissez les adresses IP principale et secondaire ainsi que le masque de réseau de sous-réseau. Cochez la case Utiliser la même interface que le lien de basculement pour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

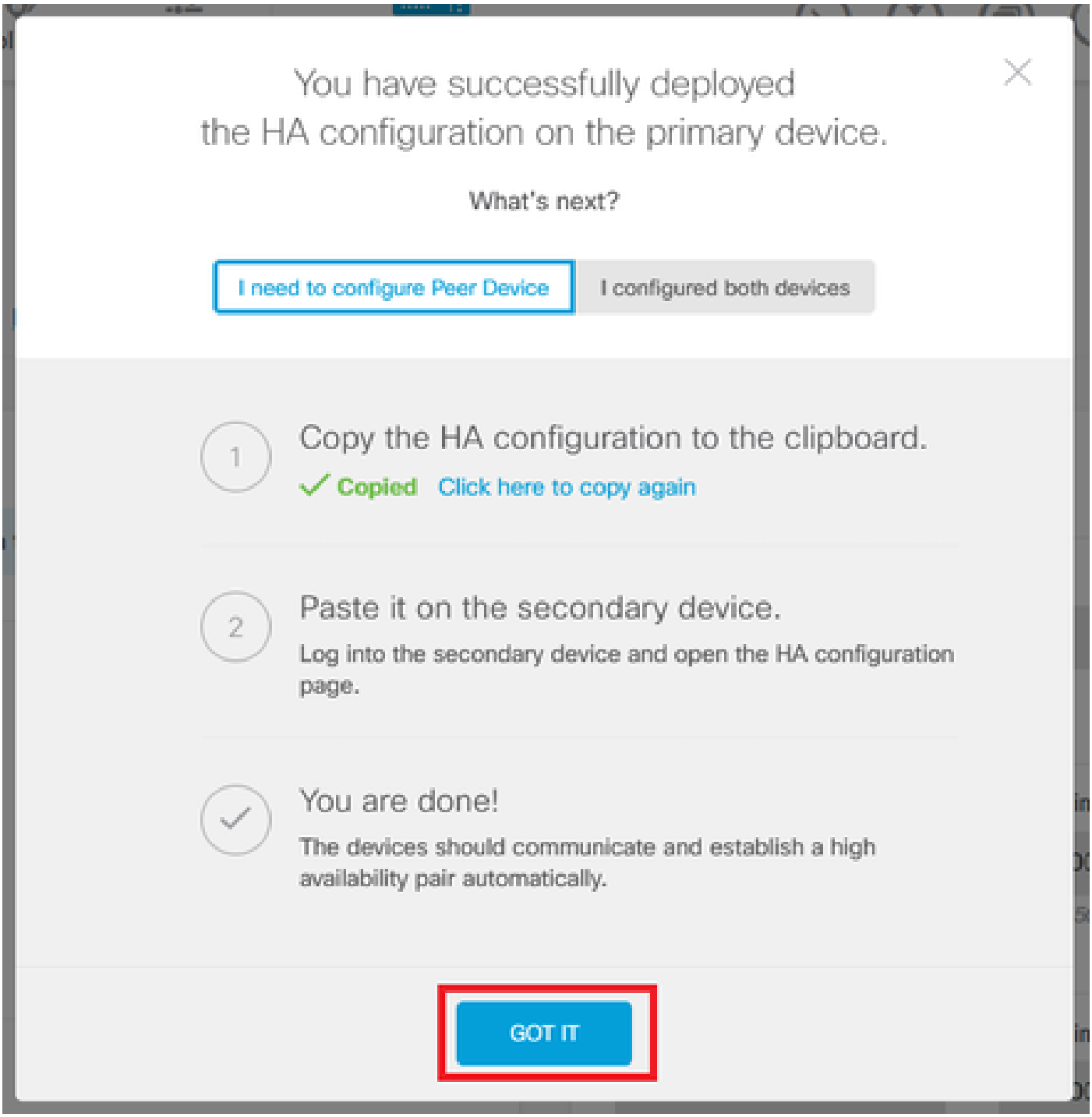


Étape 4. Décochez la case IPSec Encryption Key et cliquez sur Activate HA pour enregistrer les modifications.



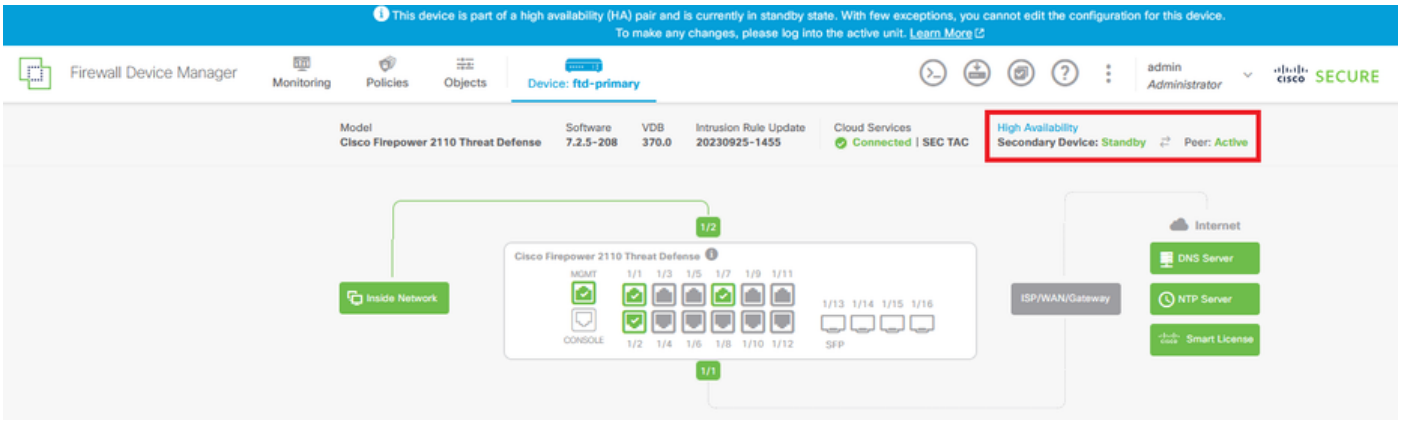
Avertissement : le système déploie immédiatement la configuration sur le périphérique. Vous n'avez pas besoin de démarrer une tâche de déploiement. Si aucun message indiquant que votre configuration a été enregistrée et que le déploiement est en cours ne s'affiche, faites défiler la page jusqu'en haut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

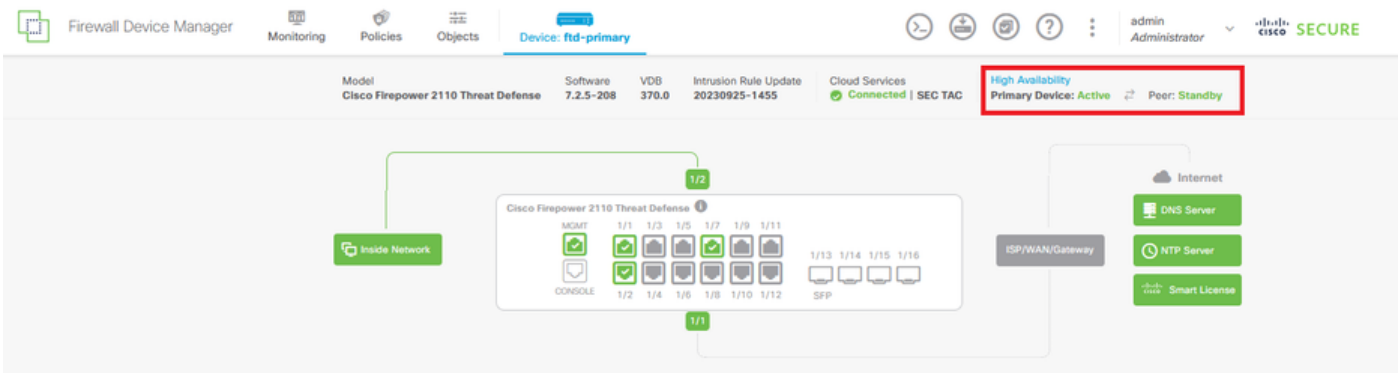


Vérifier

- 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.



- 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.

```
> show running-config failover
failover
failover lan unit primary
failover lan interface failover-link Ethernet1/7
failover replication http
failover link failover-link Ethernet1/7
failover interface ip failover-link 10.1.1.1 255.255.255.252 standby 10.1.1.2
```

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

```
> show failover state

              State          Last Failure Reason      Date/Time
This host  -  Primary
              Active         None
Other host -  Secondary
              Standby Ready  None

====Configuration State===
====Communication State===
        Mac set

>
```

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.