FTD hoge beschikbaarheid configureren met FDM

Inhoud

Inleiding

In dit document wordt beschreven hoe u een actief/stand-by (HA) paar Secure Firewall Threat Defence (FTD) kunt instellen dat lokaal wordt beheerd.

Voorwaarden

Vereisten

Aanbevolen wordt kennis van deze onderwerpen te hebben:

- De eerste configuratie van Cisco Secure Firewall Threat Defence via GUI en/of shell.

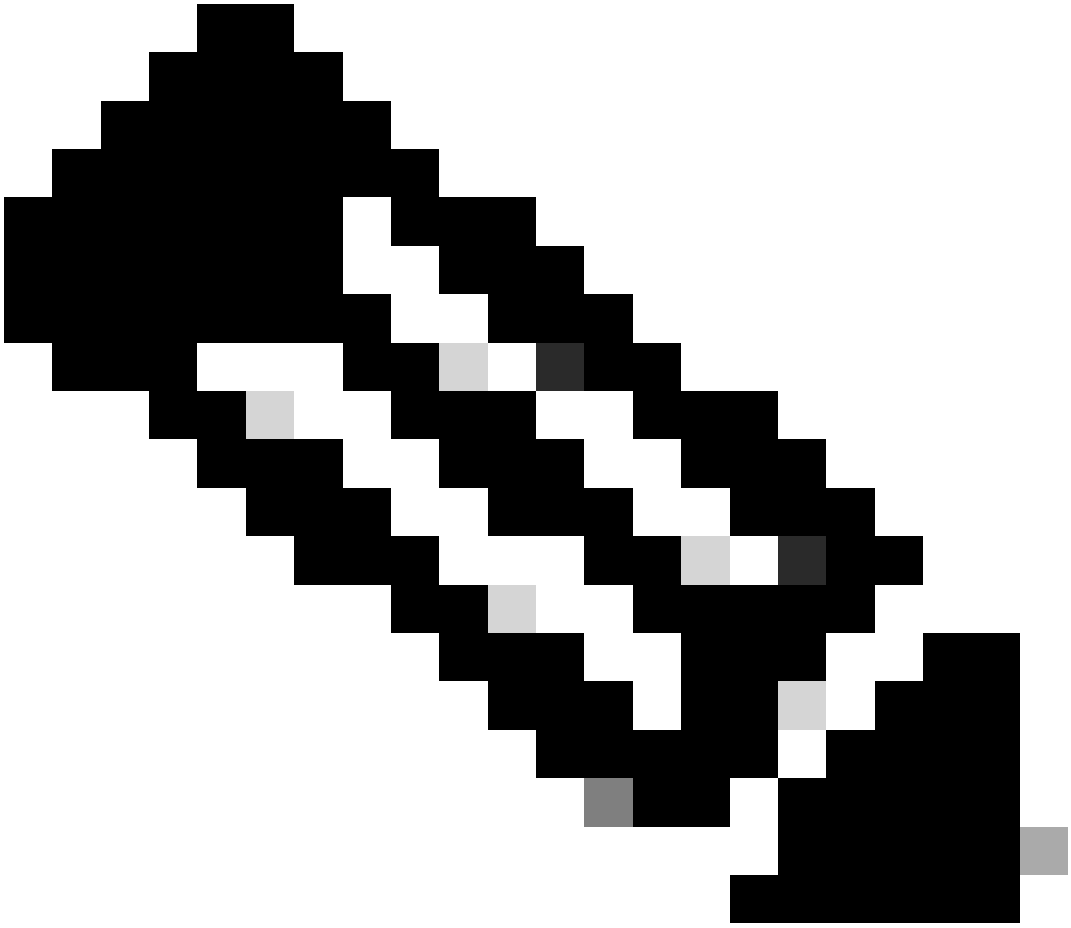
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

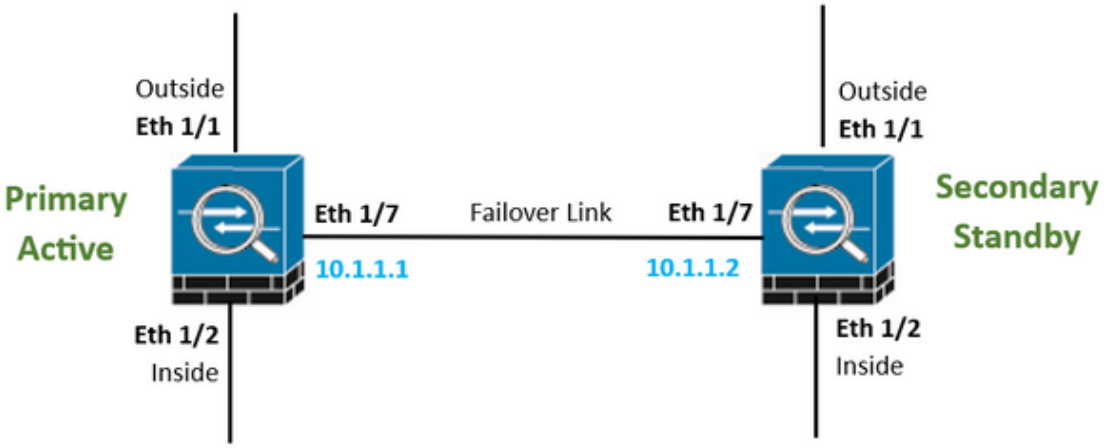
- FPR210 versie 7.2.5 lokaal beheerd door Firepower Device Manager (FDM)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Netwerktopologie



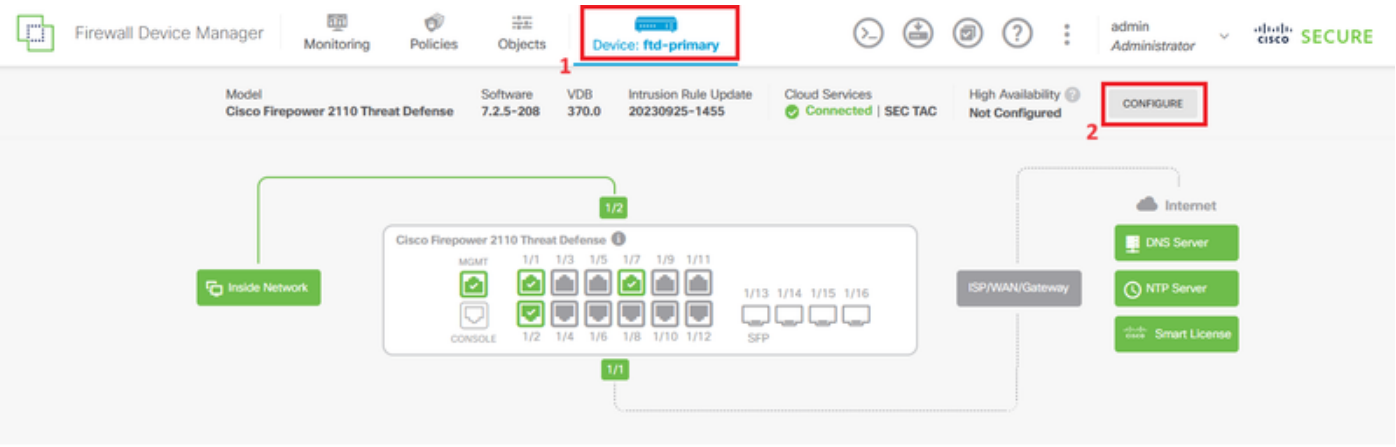
Opmerking: het voorbeeld in dit document is een van de meerdere aanbevolen netwerkontwerpen. Raadpleeg de configuratiehandleiding Onderbroken failover en datalink vermijden voor meer opties.



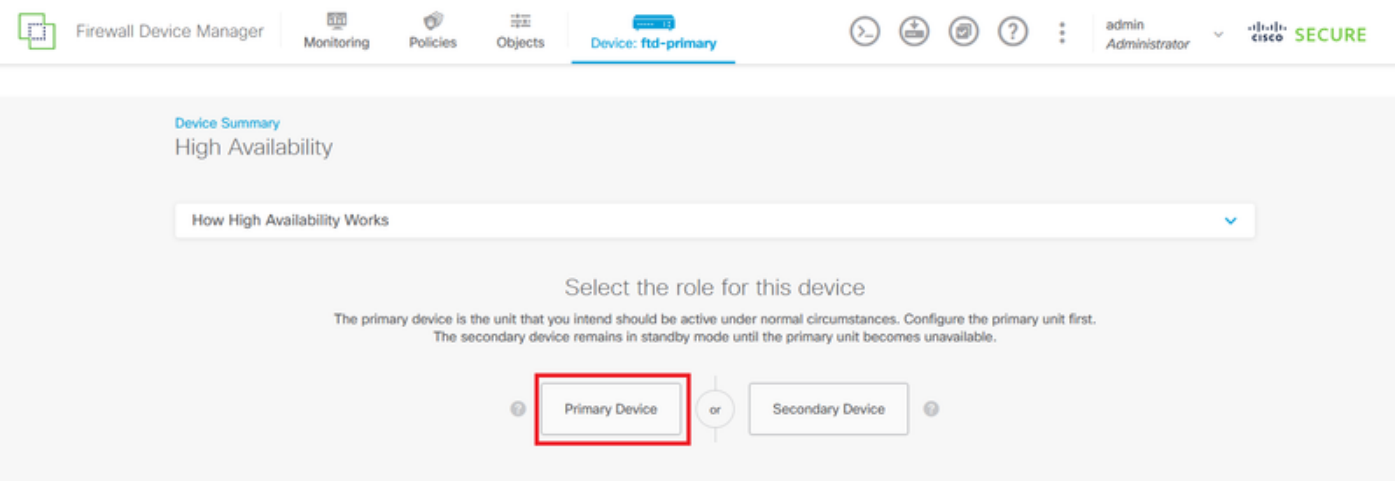
Configureren

De primaire eenheid voor hoge beschikbaarheid configureren

Stap 1. Klik op Apparaat en druk op de knop Configureren rechtsboven, naast de status Hoge beschikbaarheid.



Stap 2. Klik op de pagina Hoge beschikbaarheid op het vakje Primair apparaat.



Stap 3. De eigenschappen van de failover link configureren.

Selecteer de interface die u rechtstreeks met uw secundaire firewall hebt verbonden en stel het primaire en secundaire IP-adres en het subnetmasker in.

Controleer Gebruik dezelfde interface als het aankruisvakje failover link voor de stateful failover link.

Schakel het vakje IPSec Encryption Key uit en klik op Activate HA om de wijzigingen op te slaan.

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

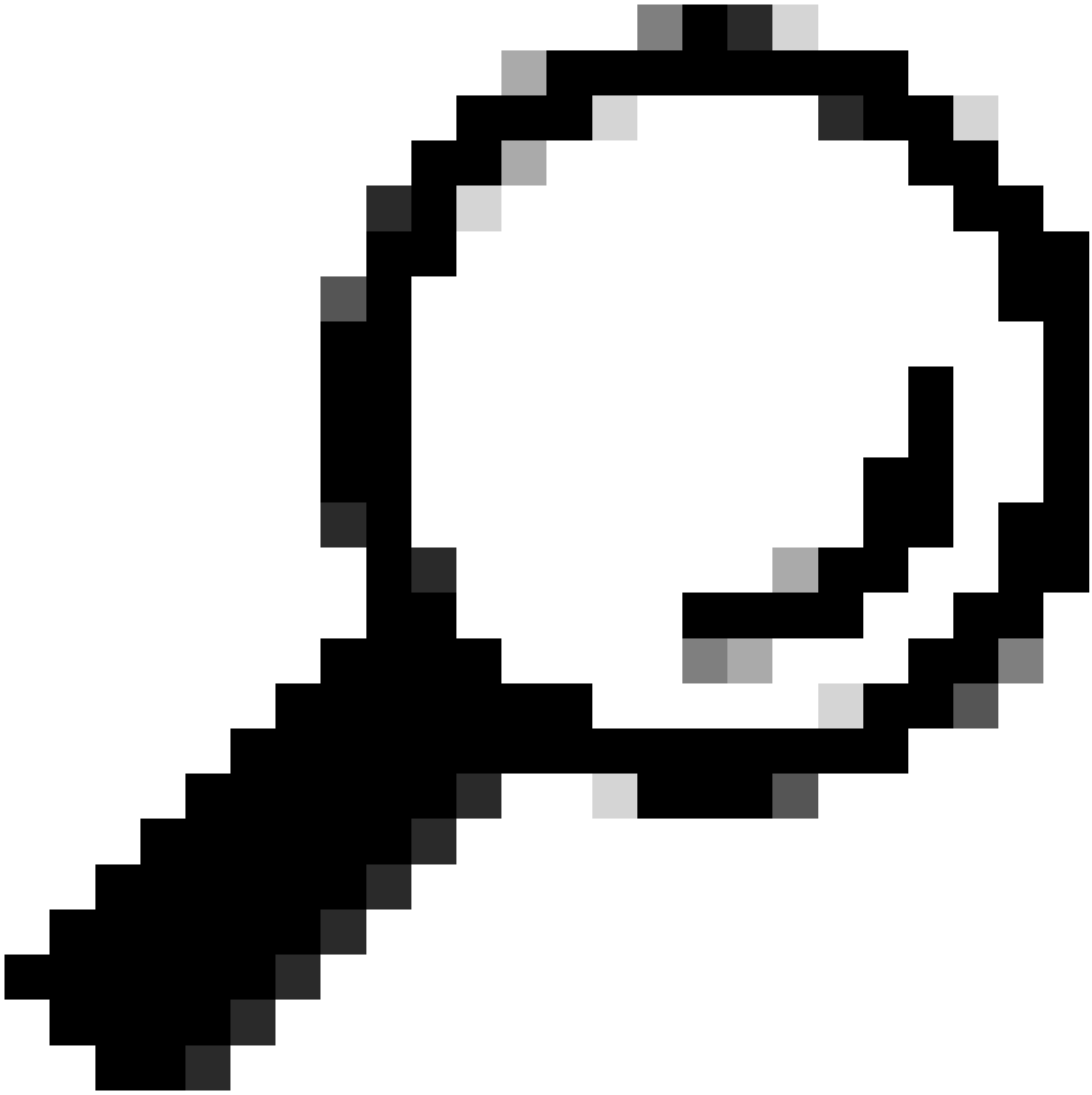
If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More

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

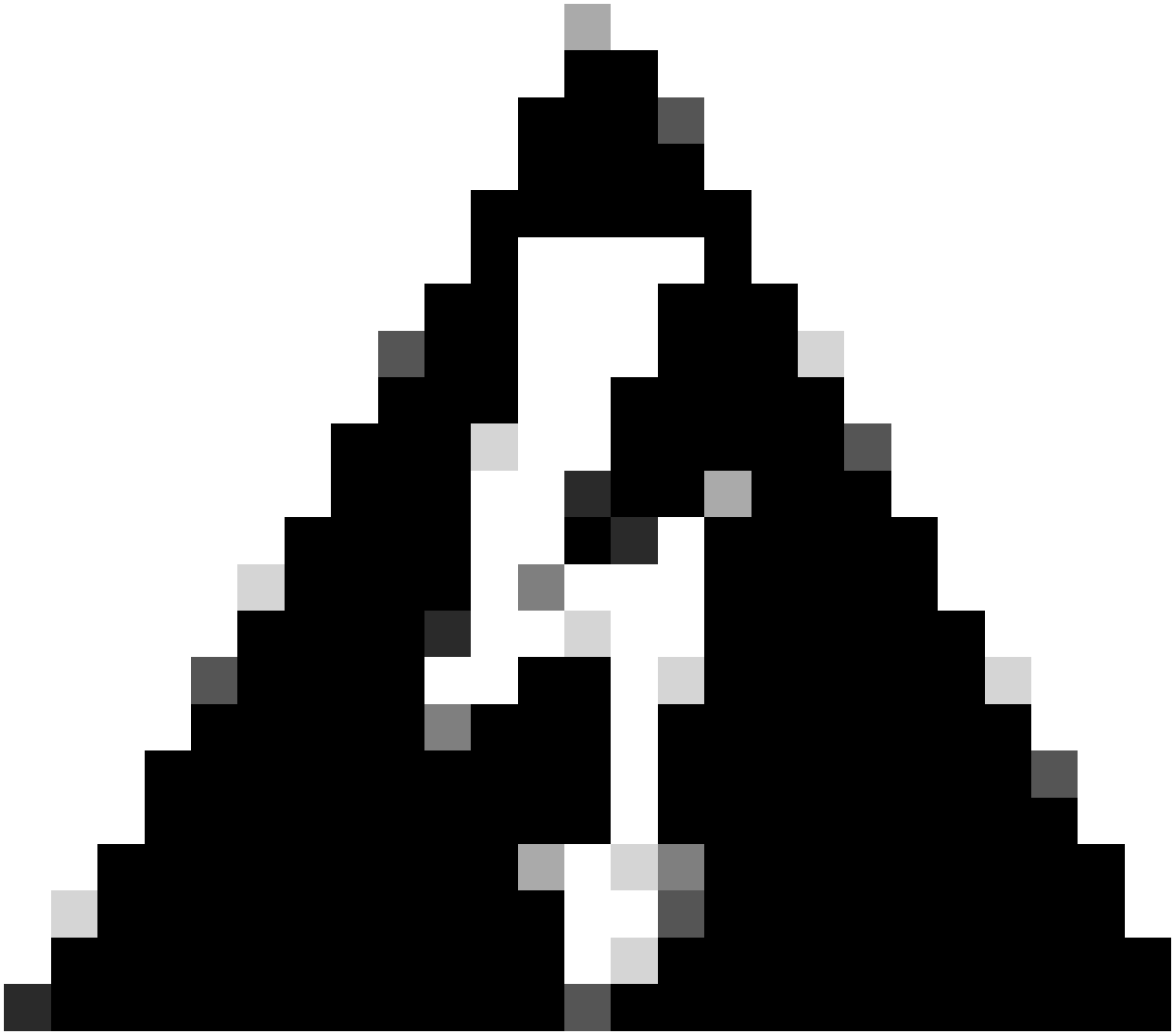
When you click Activate HA, these settings are automatically deployed to the device. The deployment might restart inspection engines, which can result in the momentary traffic loss. It might take a few minutes for deployment to finish.

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

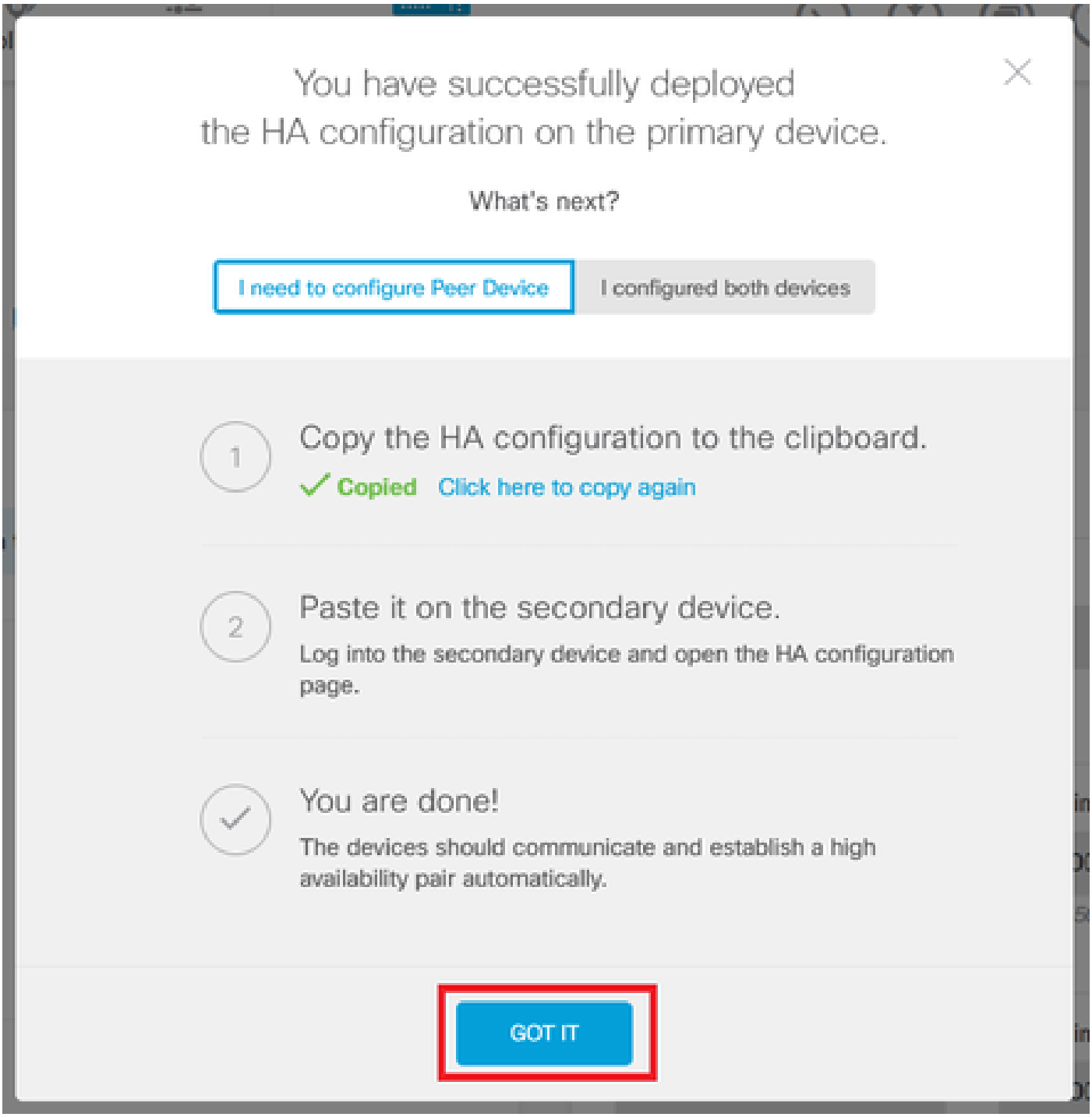


Tip: gebruik een klein maskersubnetje, dat alleen bestemd is voor failover-verkeer om beveiligingslekken en/of netwerkproblemen zoveel mogelijk te voorkomen.



Waarschuwing: het systeem implementeert de configuratie onmiddellijk op het apparaat. U hoeft geen implementatietaak te starten. Als u geen bericht ziet dat aangeeft dat uw configuratie is opgeslagen en de implementatie is gestart, scrolt u naar de bovenkant van de pagina om de foutmeldingen te zien. De configuratie wordt ook naar het klembord gekopieerd. U kunt met deze kopie de secundaire eenheid snel configureren. Voor extra veiligheid is de coderingssleutel (als u deze instelt) niet opgenomen in het exemplaar van het klembord.

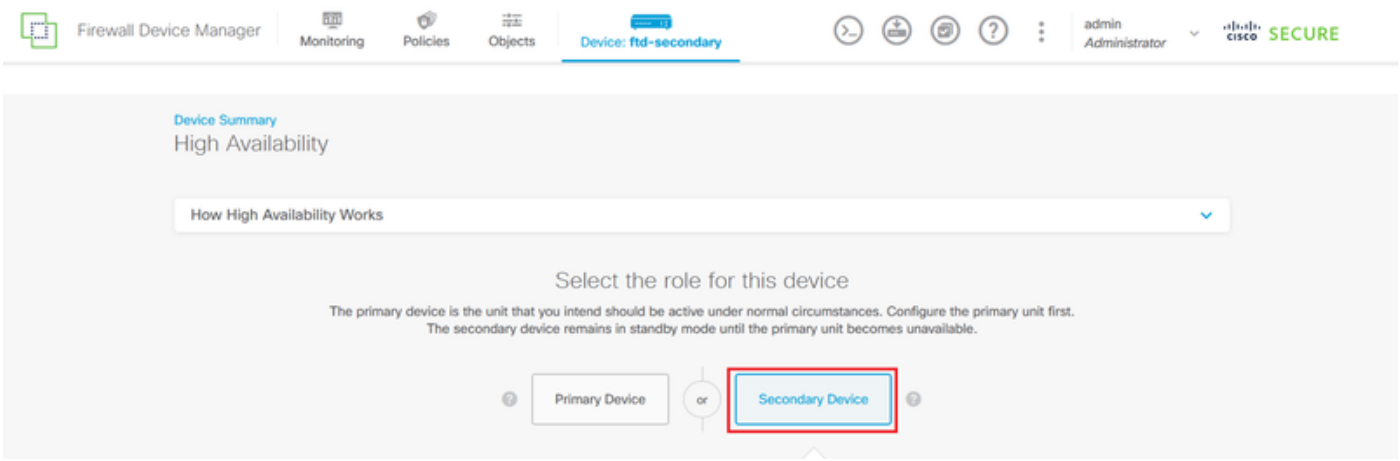
Stap 4. Nadat de configuratie is voltooid, ontvangt u een bericht waarin de volgende stappen worden uitgelegd. Klik na het lezen van de informatie op Got It.



De secundaire eenheid configureren voor hoge beschikbaarheid

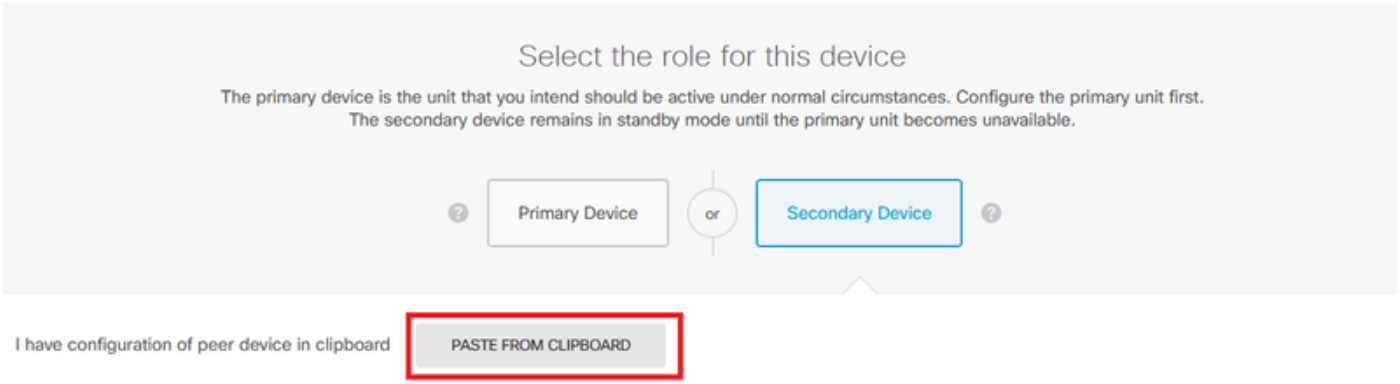
Stap 1. Klik op Apparaat en druk op de knop Configureren rechtsboven, naast de status Hoge beschikbaarheid.

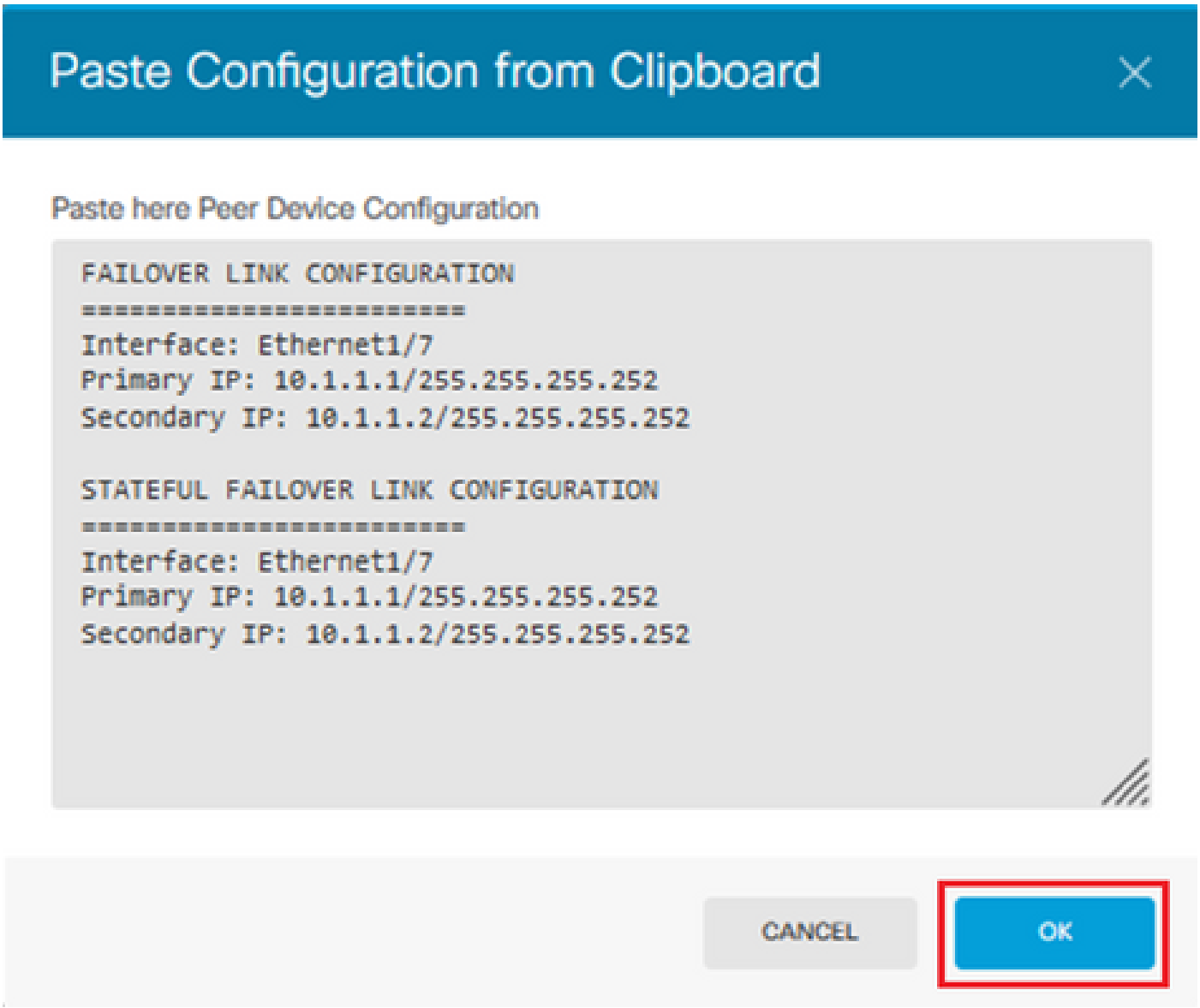
Stap 2. Klik op de pagina Hoge beschikbaarheid op het vakje Secundair apparaat.



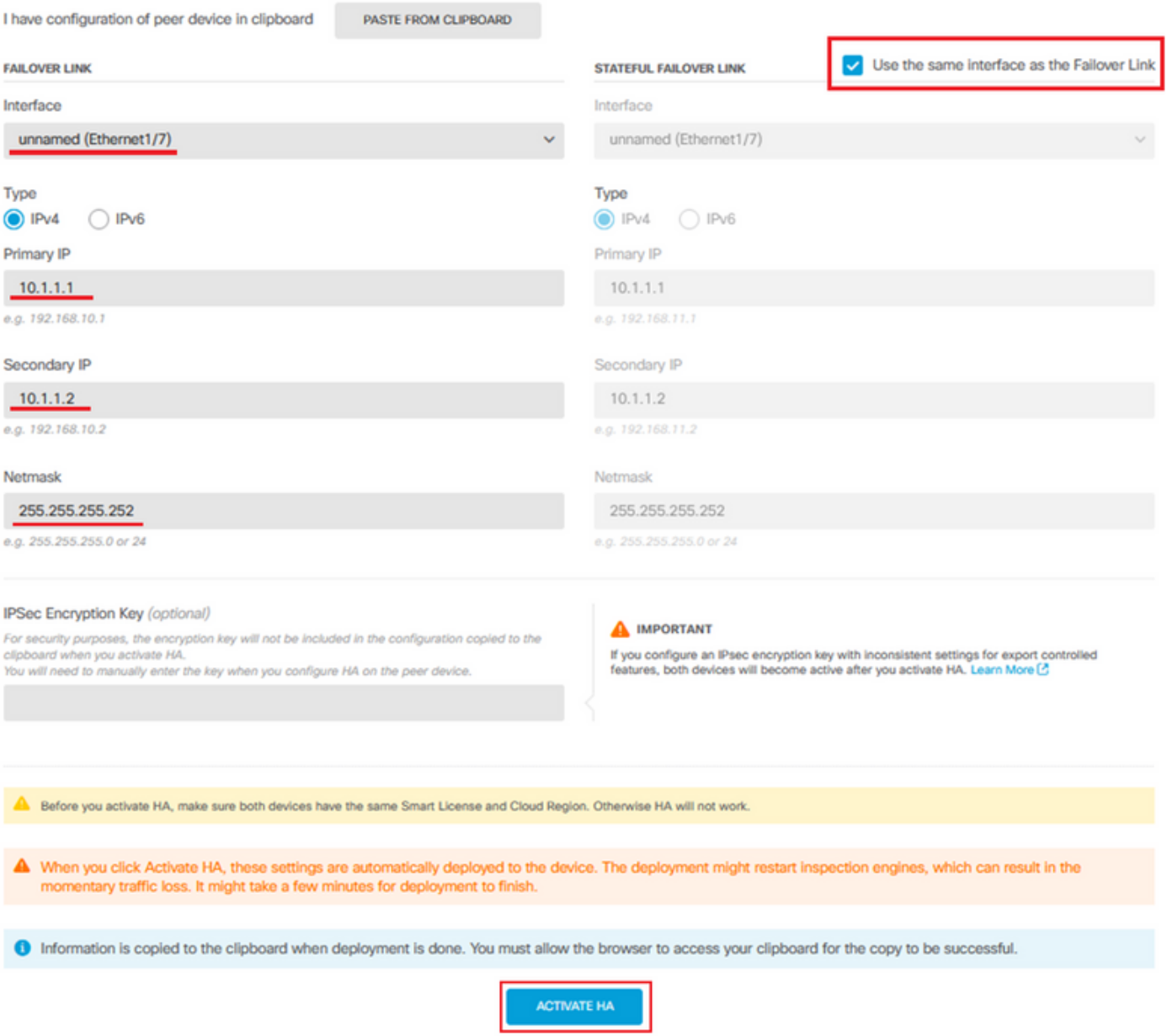
Stap 3. De eigenschappen van de failover link configureren. U kunt de instellingen die zijn opgeslagen op uw klembord plakken na het configureren van de primaire FTD, of u kunt handmatig doorgaan.

Stap 3.1. Als u van het klembord wilt plakken, klikt u eenvoudig op de knop Plakken vanaf het klembord, plakt u in de configuratie (drukt u op toetsen Ctrl+v tegelijkertijd) en klikt u op OK.

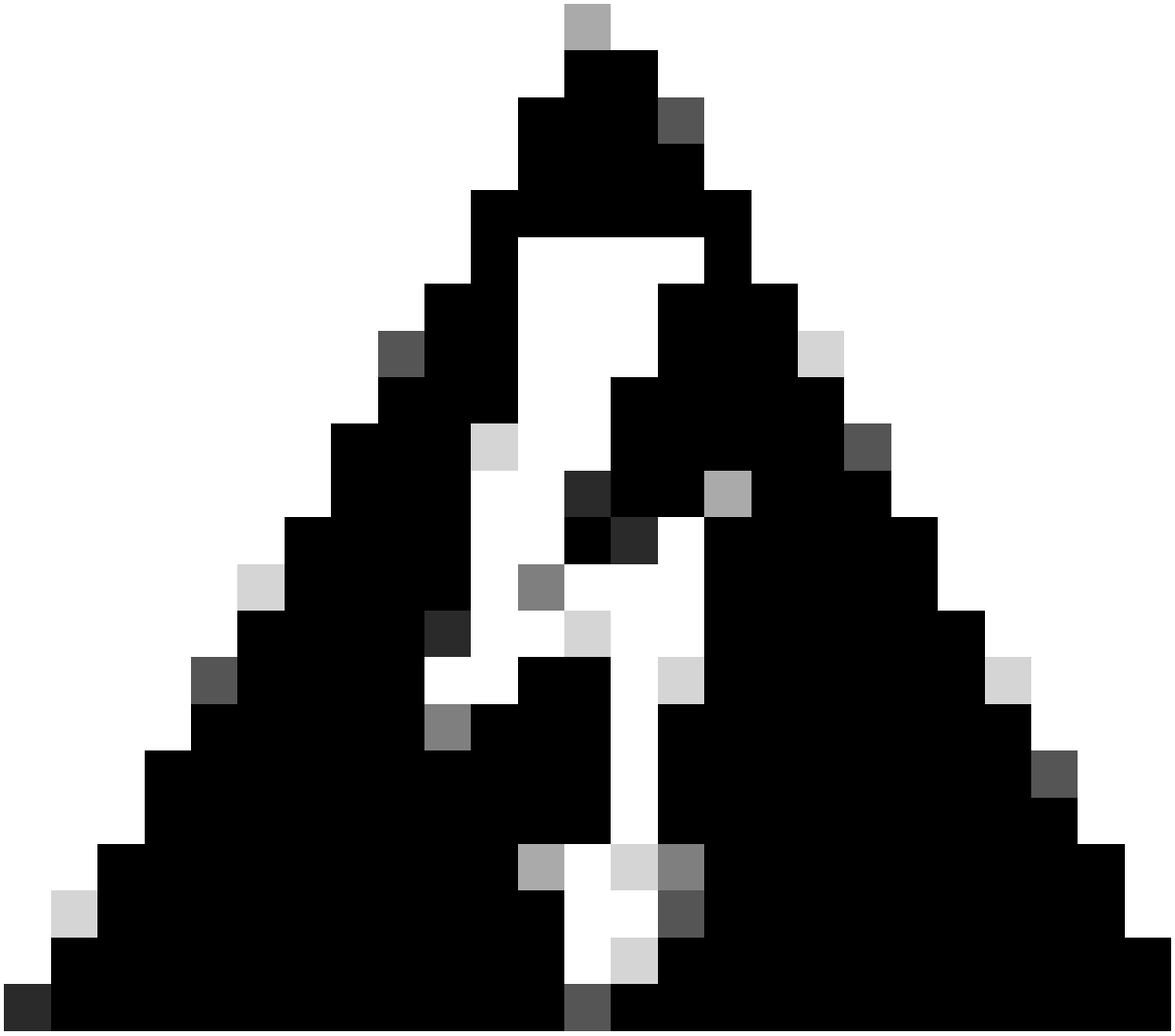




Stap 3.2. Om handmatig verder te gaan, selecteert u de interface die u rechtstreeks heeft verbonden met uw secundaire firewall en stelt u het primaire en secundaire IP-adres in evenals het subnetmasker Netmasker. Controleer Gebruik dezelfde interface als het aankruisvakje failover link voor de stateful failover link.

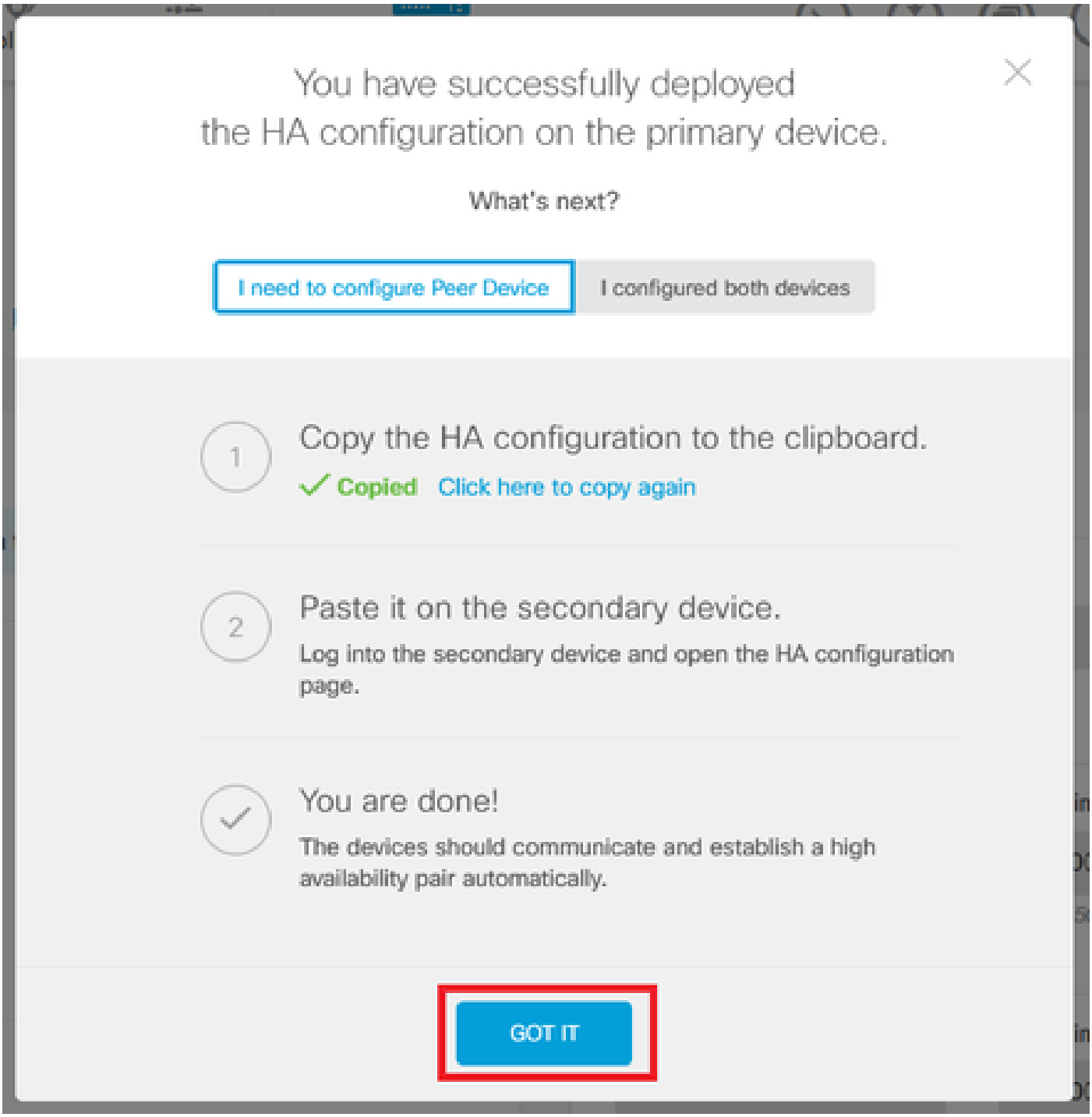


Stap 4. Schakel het vakje IPSec Encryption Key uit en klik op Activate HA om de wijzigingen op te slaan.



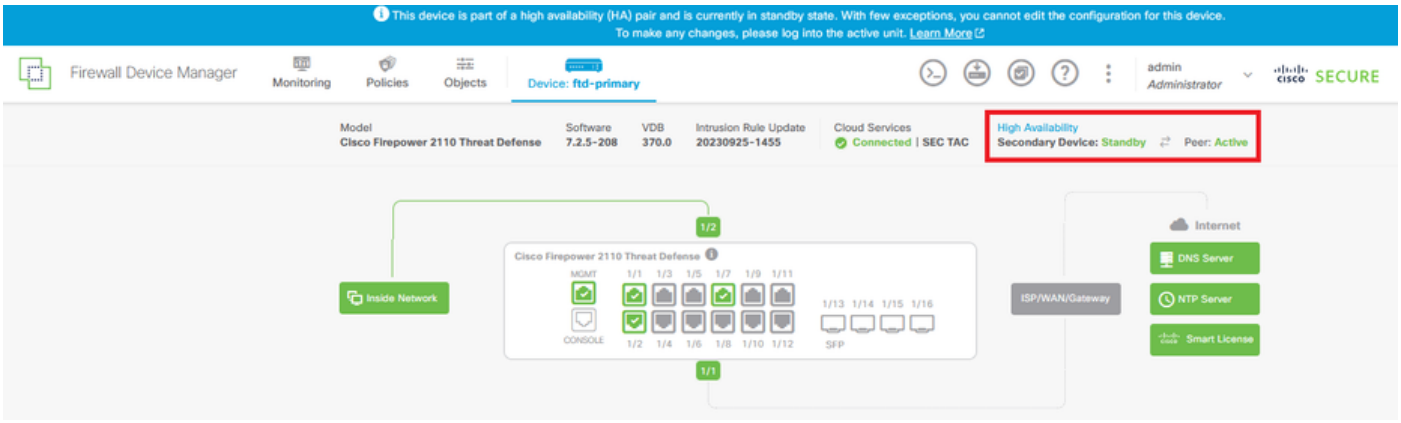
Waarschuwing: het systeem implementeert de configuratie onmiddellijk op het apparaat. U hoeft geen implementatietaak te starten. Als u geen bericht ziet dat aangeeft dat uw configuratie is opgeslagen en de implementatie is gestart, scrolt u naar de bovenkant van de pagina om de foutmeldingen te zien.

Stap 5. Nadat de configuratie is voltooid, ontvangt u een bericht waarin de volgende stappen worden uitgelegd die u moet nemen. Klik na het lezen van de informatie op Got It.

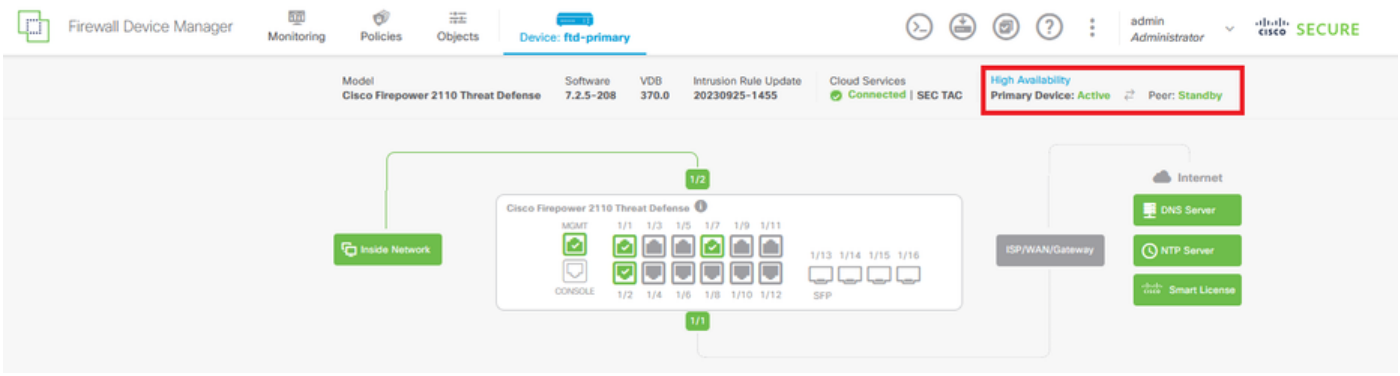


Verifiëren

- Op dit punt geeft uw apparaatstatus meestal aan dat dit het secundaire apparaat is op de pagina Hoge beschikbaarheid. Als de verbinding met het primaire apparaat succesvol was, begint het apparaat te synchroniseren met het primaire apparaat, en uiteindelijk wordt de modus veranderd in Standby en de peer in Active.



- De primaire FTD toont de status van hoge beschikbaarheid ook, maar als Active en Peer: Standby.



- Open een SSH-sessie voor de primaire FTD en geef de opdracht show in werking stelt-configuratie failover om de configuratie te verifiëren.

```
> 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
```

- Valideren van de huidige status van het apparaat met de opdracht toont failover status.

```
> 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

>
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.