FTD-Hochverfügbarkeit mit FDM konfigurieren

Inhalt

Einleitung

Dieses Dokument beschreibt die Einrichtung eines Aktiv/Standby-Hochverfügbarkeitspaars (HA) mit lokal verwaltetem Secure Firewall Threat Defense (FTD).

Voraussetzungen

Anforderungen

Es wird empfohlen, über Kenntnisse in den folgenden Themen zu verfügen:

- Erstkonfiguration von Cisco Secure Firewall Threat Defense über die Benutzeroberfläche und/oder Shell.

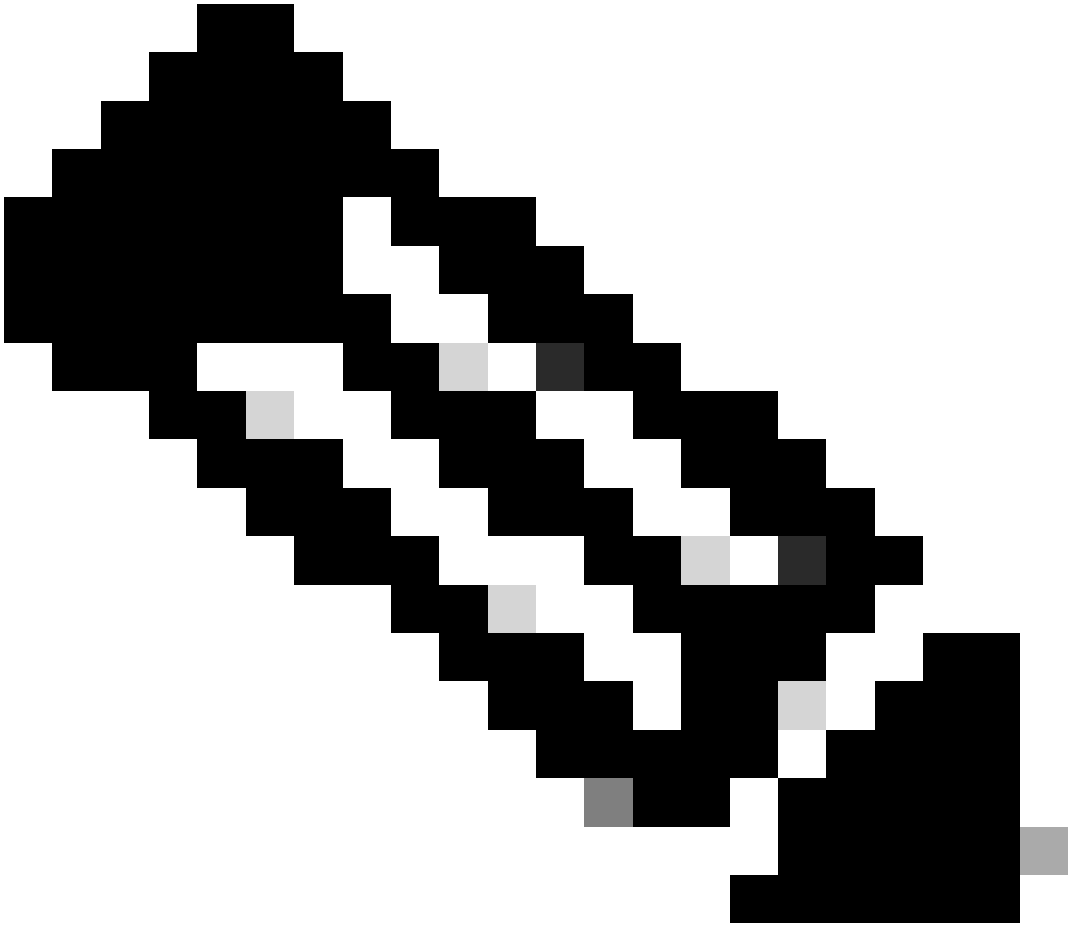
Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

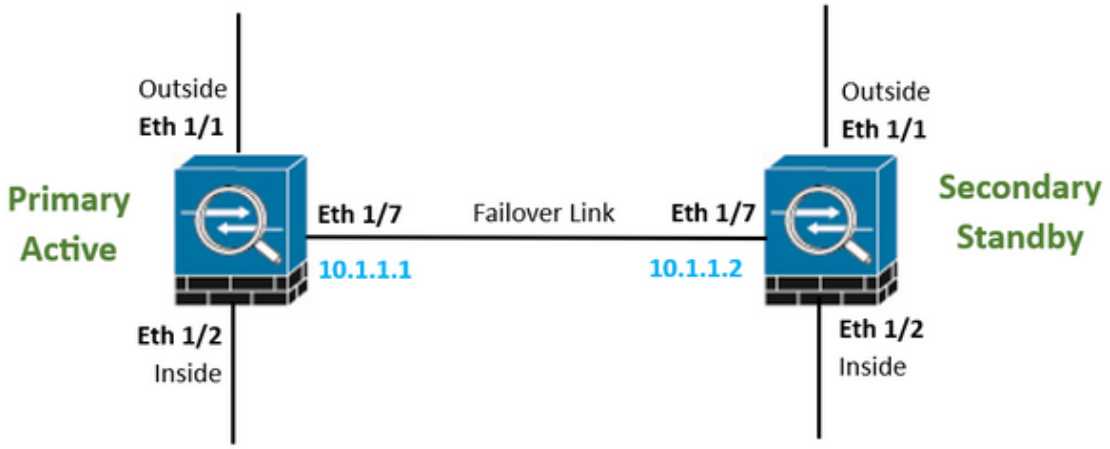
- FPR2110 Version 7.2.5, lokal verwaltet durch FirePOWER Device Manager (FDM)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerktopologie



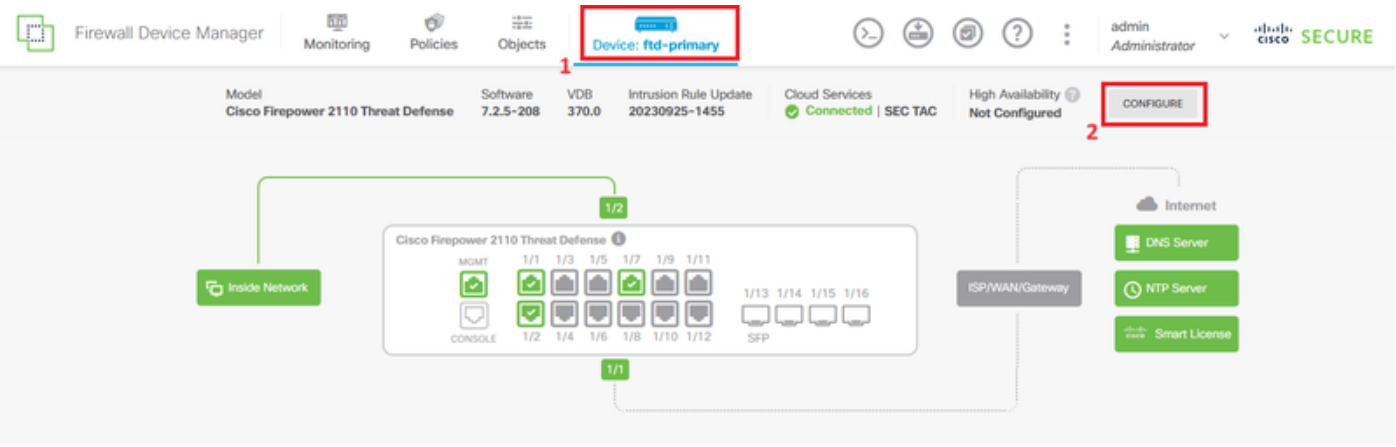
Hinweis: Das in diesem Dokument beschriebene Beispiel ist eines von mehreren empfohlenen Netzwerkdesigns. Weitere Optionen finden Sie im Konfigurationsleitfaden Avoiding Interrupted Failover and Data Links (Vermeidung von Unterbrechungen durch Failover und Datenverbindungen).



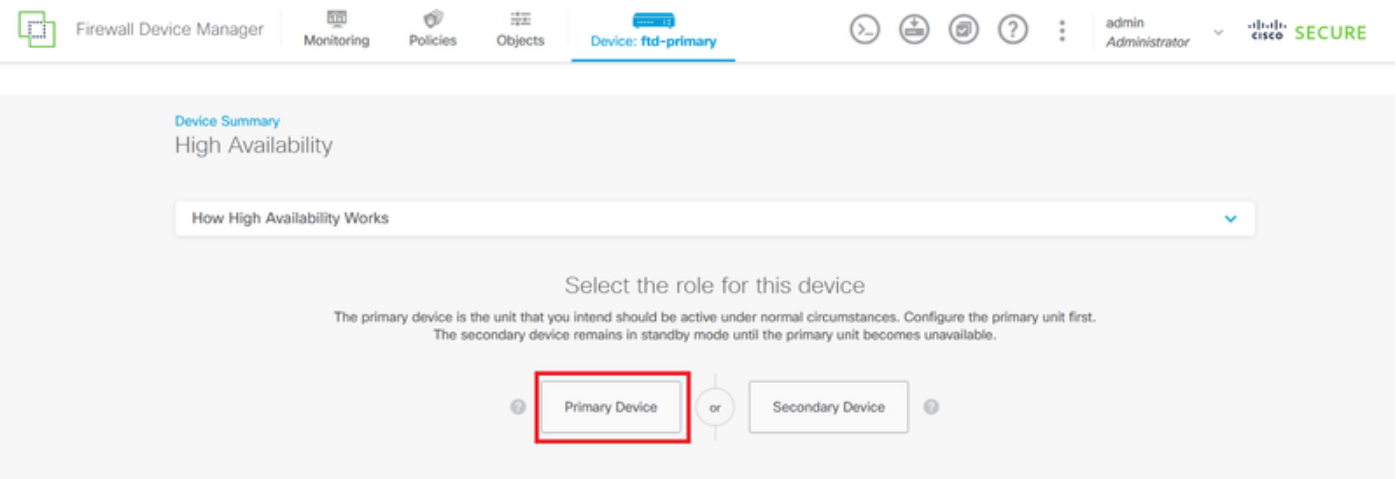
Konfigurieren

Konfigurieren der primären Einheit für hohe Verfügbarkeit

Schritt 1: Klicken Sie auf Device (Gerät), und drücken Sie die Taste Configure (Konfigurieren) oben rechts neben dem Status High Availability (Hohe Verfügbarkeit).



Schritt 2: Klicken Sie auf der Seite für hohe Verfügbarkeit auf das Feld Primärgerät.



Schritt 3: Konfigurieren Sie die Eigenschaften der Failoververbindung.

Wählen Sie die Schnittstelle aus, die Sie direkt mit Ihrer sekundären Firewall verbunden haben, und legen Sie die primäre und sekundäre IP-Adresse sowie die Subnetz-Netzmaske fest.

Aktivieren Sie das Kontrollkästchen Dieselbe Schnittstelle wie die Failover-Verbindung verwenden für die Stateful Failover-Verbindung.

Deaktivieren Sie das Feld IPSec-Verschlüsselungsschlüssel, und klicken Sie auf HA aktivieren, um die Änderungen zu speichern.

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

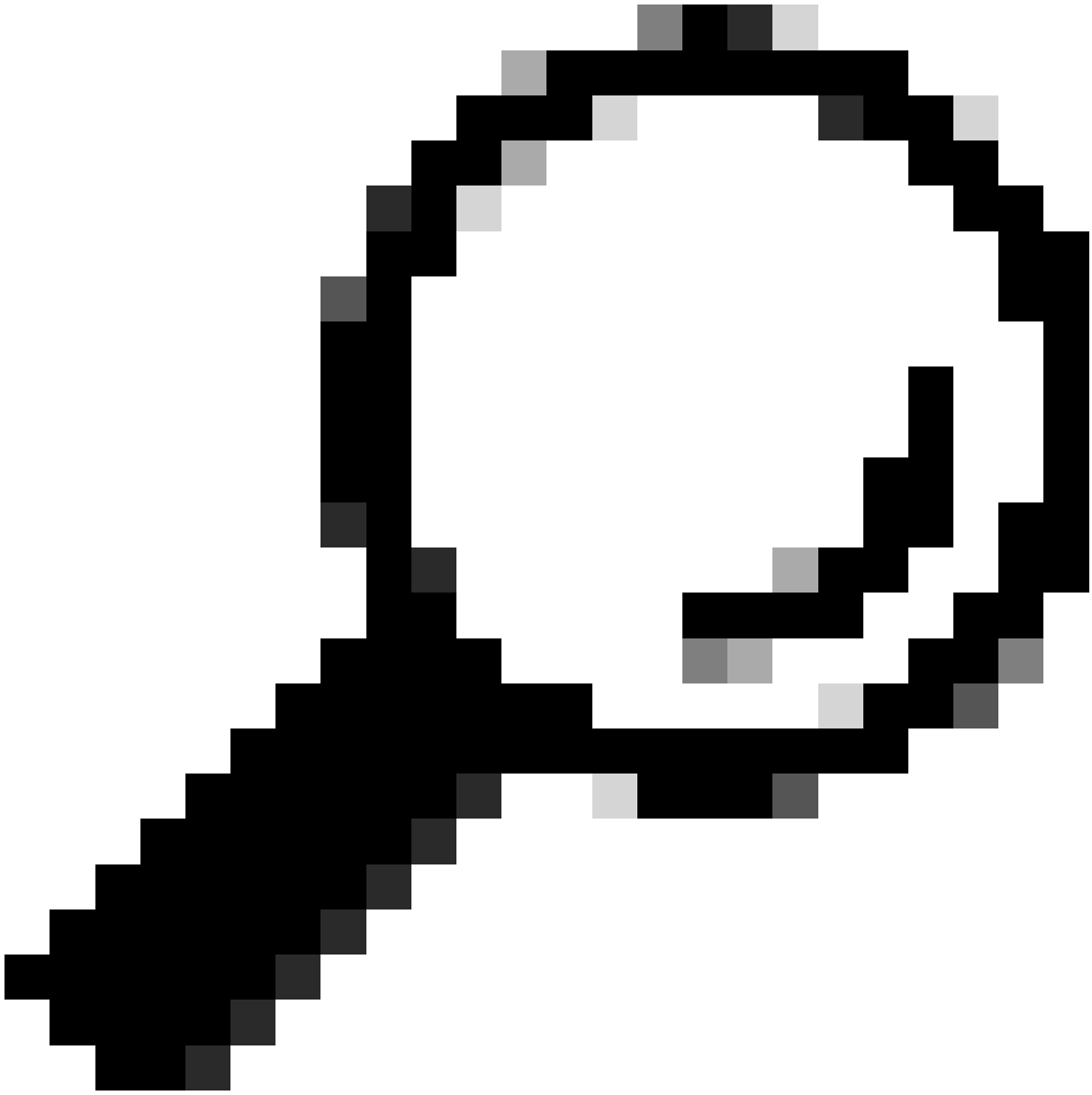
If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More

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

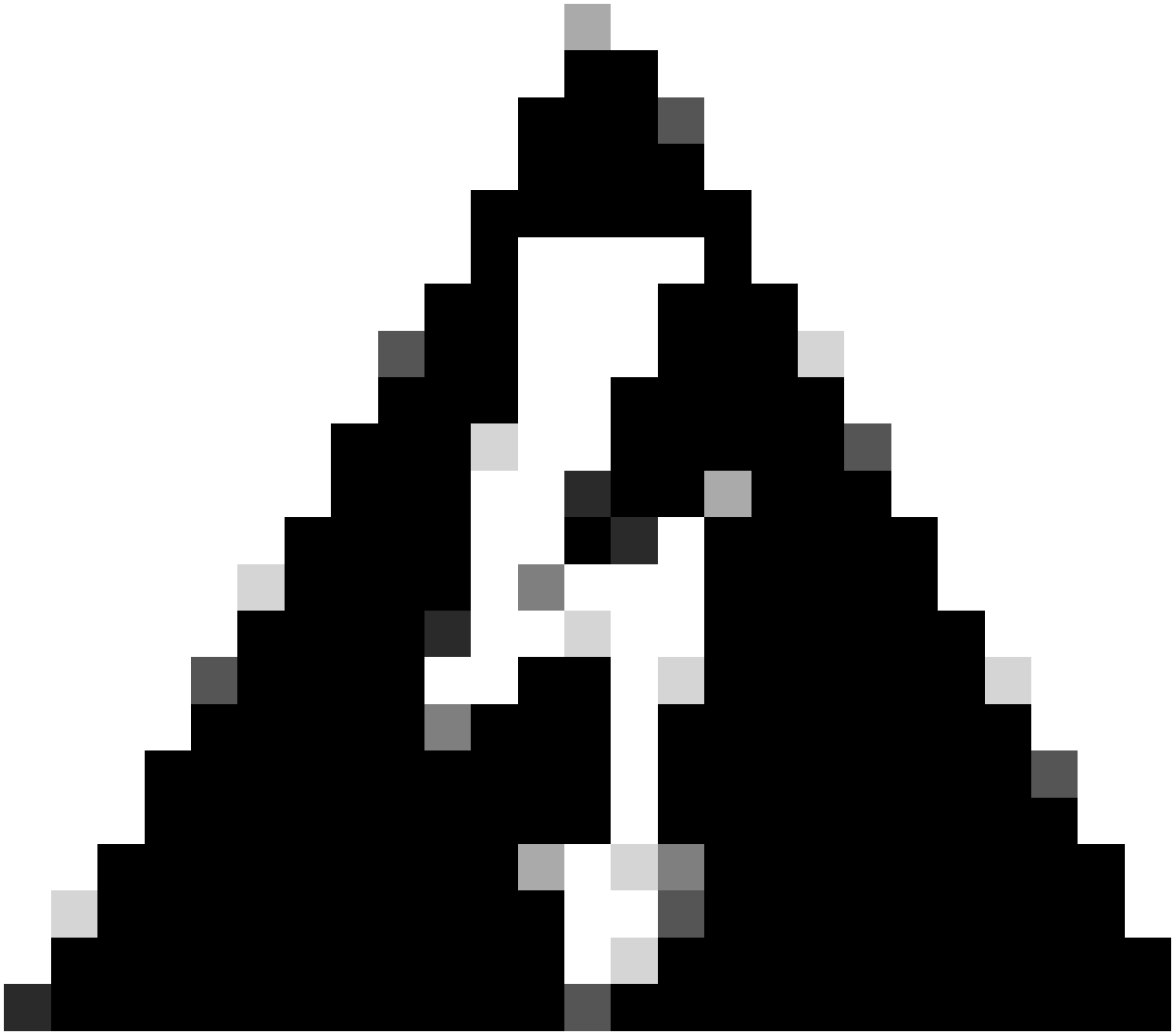
When you click Activate HA, these settings are automatically deployed to the device. The deployment might restart inspection engines, which can result in the momentary traffic loss. It might take a few minutes for deployment to finish.

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

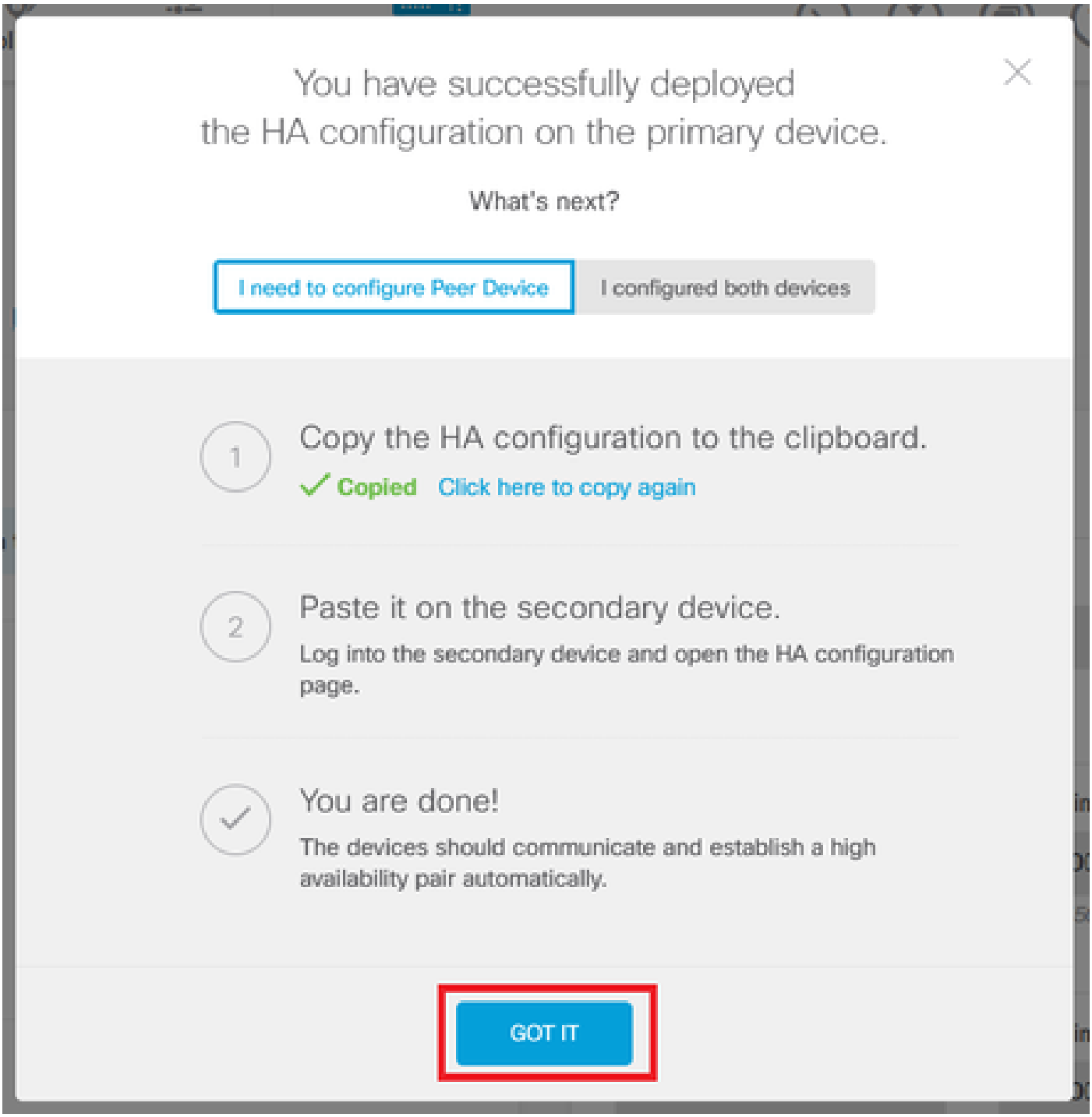


Tipp: Verwenden Sie ein Subnetz mit einer kleinen Maske, das nur für Failover-Datenverkehr vorgesehen ist, um Sicherheitslücken und/oder Netzwerkprobleme so weit wie möglich zu vermeiden.



Warnung: Das System stellt die Konfiguration sofort auf dem Gerät bereit. Sie müssen keinen Bereitstellungsauftrag starten. Wenn keine Meldung angezeigt wird, dass Ihre Konfiguration gespeichert wurde und die Bereitstellung ausgeführt wird, scrollen Sie zum Seitenanfang, um die Fehlermeldungen anzuzeigen. Die Konfiguration wird ebenfalls in die Zwischenablage kopiert. Sie können die Kopie verwenden, um die sekundäre Einheit schnell zu konfigurieren. Um die Sicherheit zu erhöhen, ist der Verschlüsselungsschlüssel (falls Sie einen Schlüssel festlegen) nicht in der Zwischenablage enthalten.

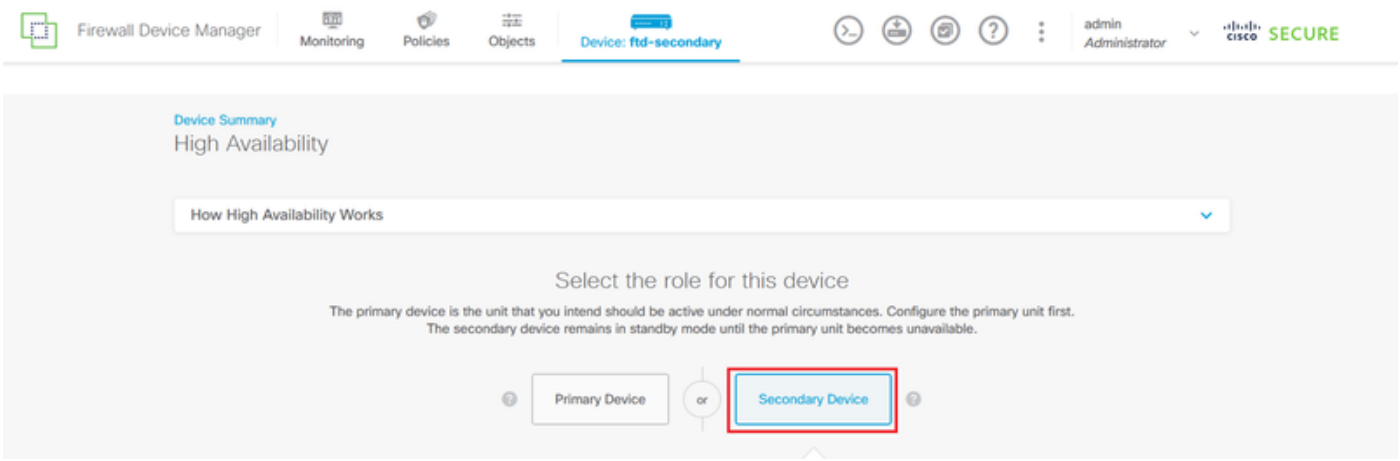
Schritt 4: Nach Abschluss der Konfiguration wird eine Meldung mit den nächsten Schritten angezeigt. Klicken Sie nach dem Lesen der Informationen auf Got It.



Konfigurieren der Sekundäreinheit für hohe Verfügbarkeit

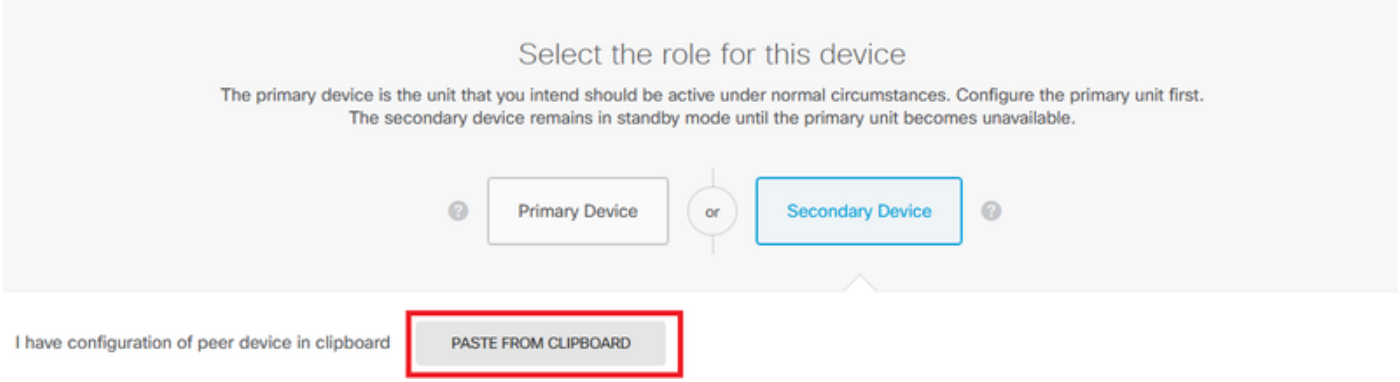
Schritt 1: Klicken Sie auf Device (Gerät), und drücken Sie die Taste Configure (Konfigurieren) oben rechts neben dem Status High Availability (Hohe Verfügbarkeit).

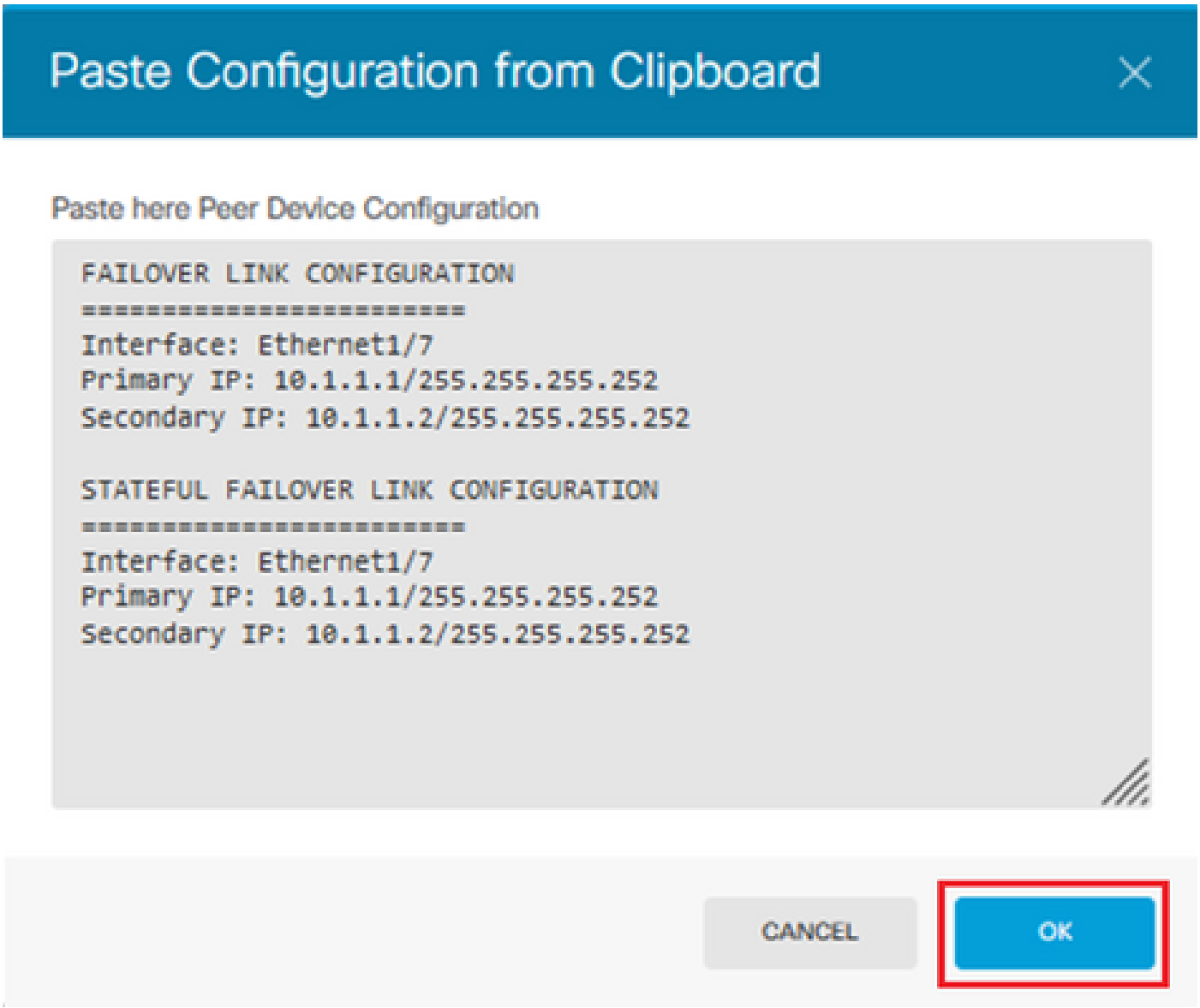
Schritt 2: Klicken Sie auf der Seite für hohe Verfügbarkeit auf das Kästchen Sekundäres Gerät.



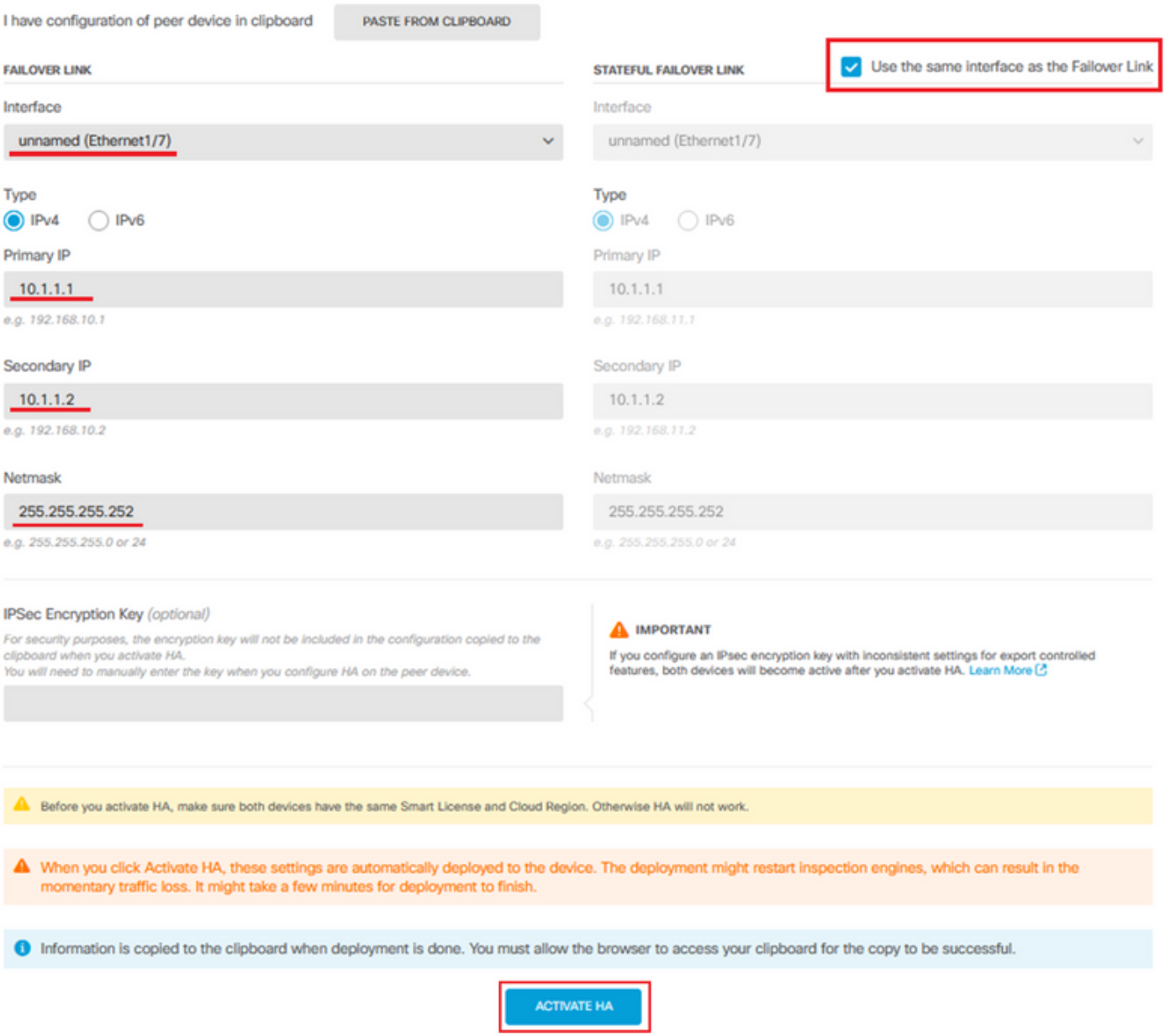
Schritt 3: Konfigurieren Sie die Eigenschaften der Failoververbindung. Sie können die in der Zwischenablage gespeicherten Einstellungen nach der Konfiguration des primären FTD einfügen oder den Vorgang manuell fortsetzen.

Schritt 3.1: Um aus der Zwischenablage einzufügen, klicken Sie einfach auf die Schaltfläche Aus Zwischenablage einfügen, fügen Sie die Konfiguration ein (drücken Sie Strg+v gleichzeitig) und klicken Sie auf OK.

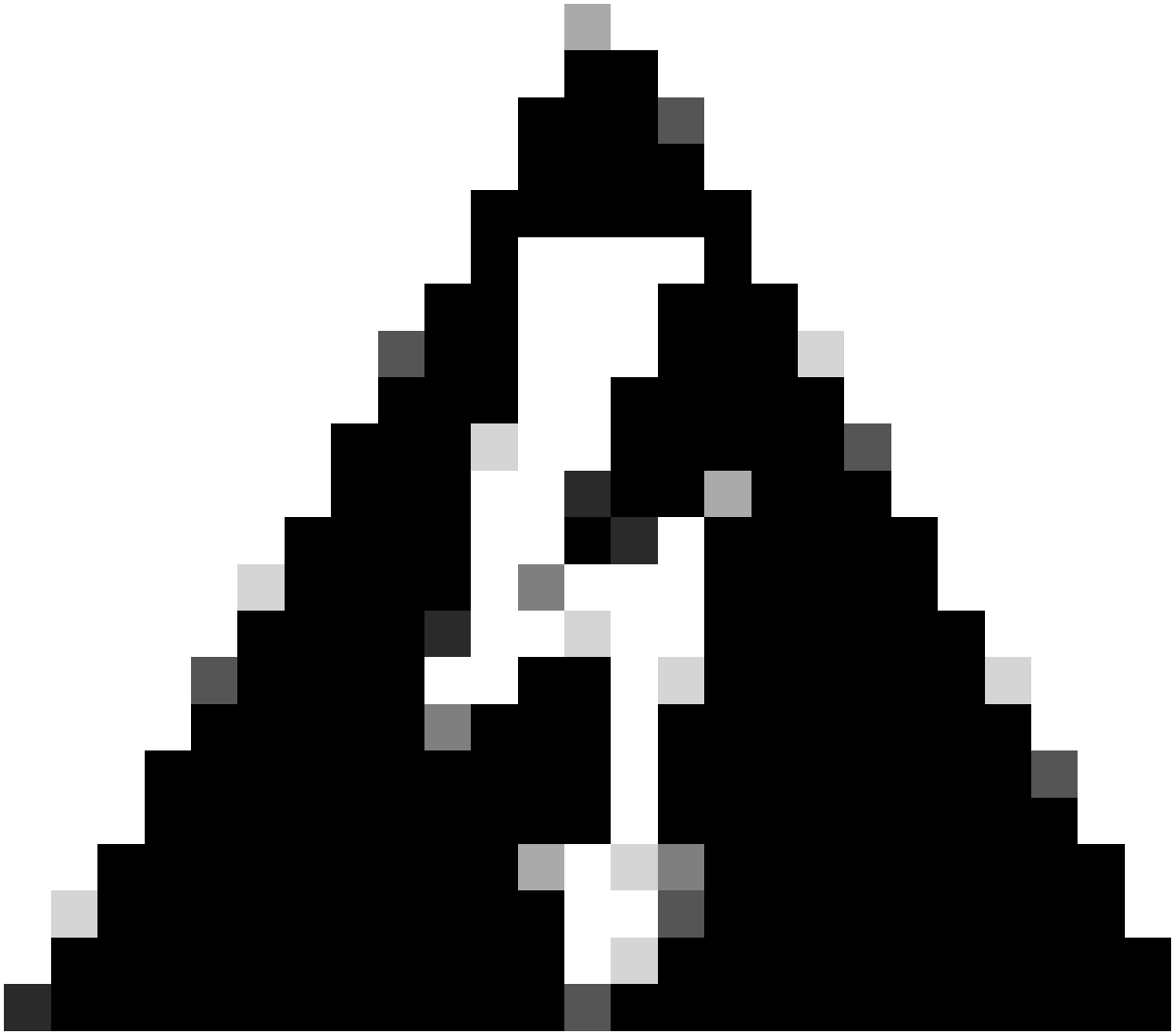




Schritt 3.2: Um manuell fortzufahren, wählen Sie die Schnittstelle aus, die Sie direkt mit Ihrer sekundären Firewall verbunden haben, und legen Sie die primäre und sekundäre IP-Adresse sowie die Subnetz-Netzmaske fest. Aktivieren Sie das Kontrollkästchen Dieselbe Schnittstelle wie die Failover-Verbindung verwenden für die Stateful Failover-Verbindung.

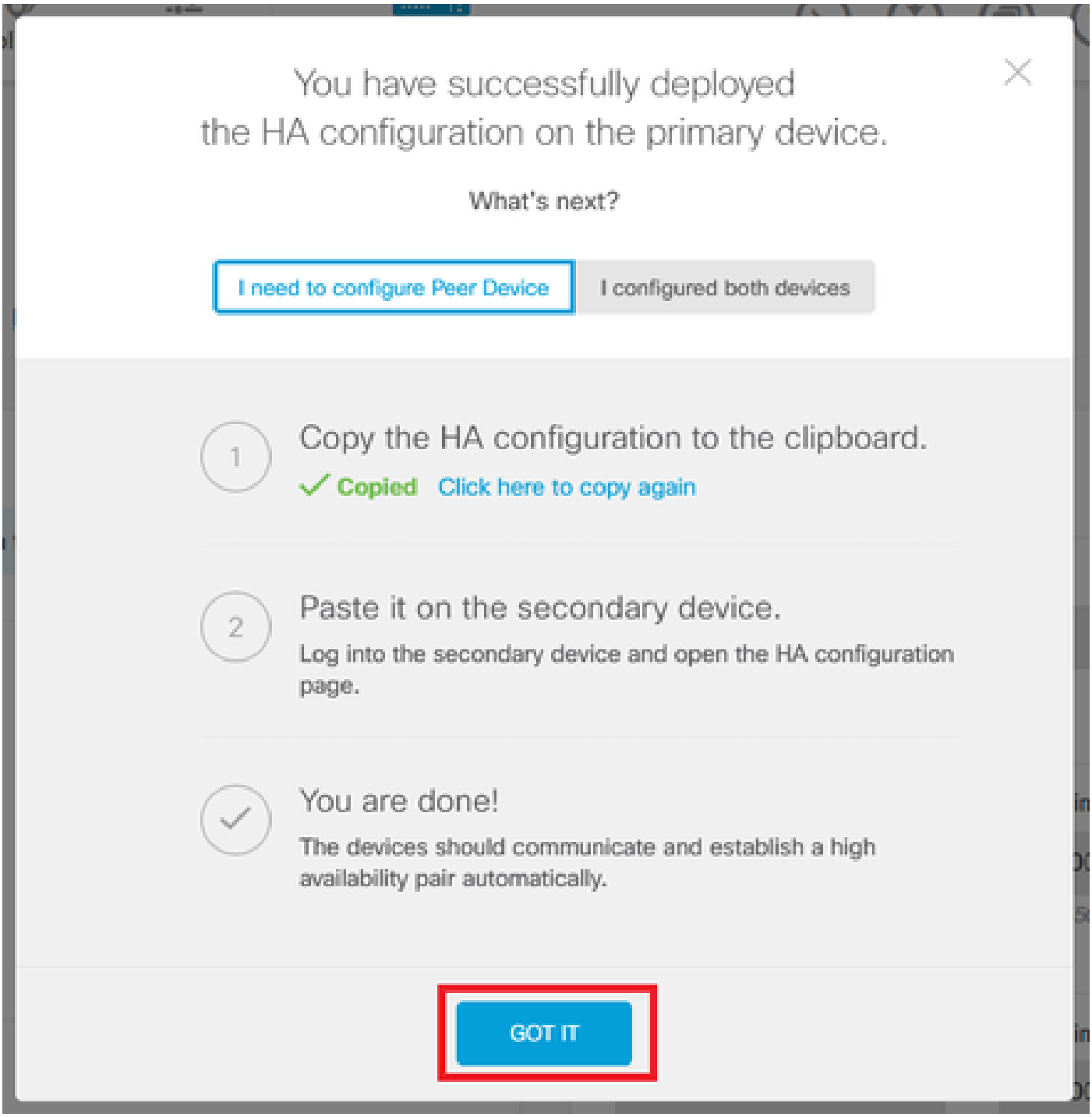


Schritt 4: Deaktivieren Sie das Feld IPSec-Verschlüsselungsschlüssel, und klicken Sie auf HA aktivieren, um die Änderungen zu speichern.



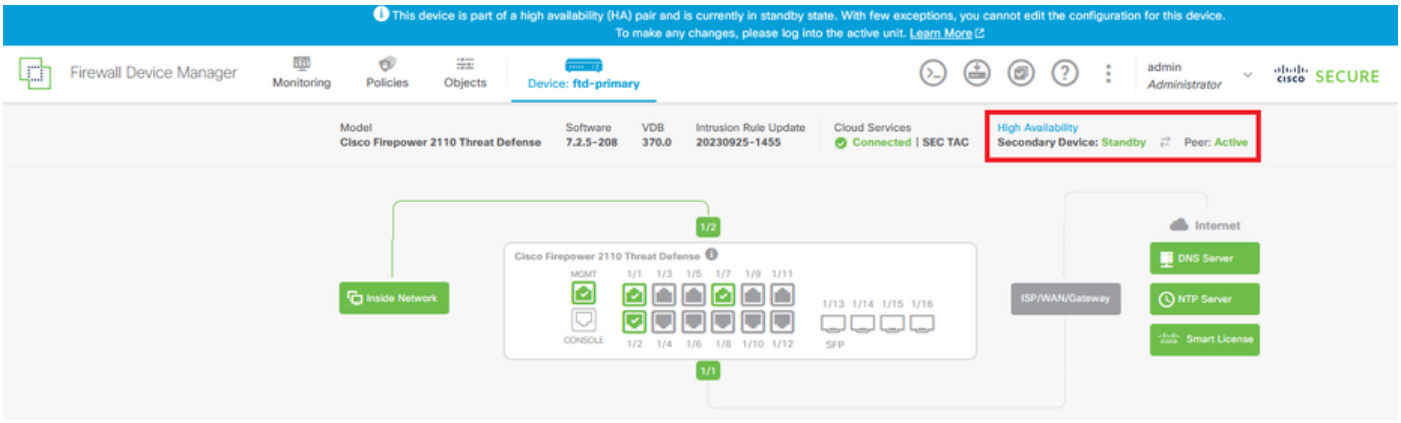
Warnung: Das System stellt die Konfiguration sofort auf dem Gerät bereit. Sie müssen keinen Bereitstellungsauftrag starten. Wenn keine Meldung angezeigt wird, dass Ihre Konfiguration gespeichert wurde und die Bereitstellung ausgeführt wird, scrollen Sie zum Seitenanfang, um die Fehlermeldungen anzuzeigen.

Schritt 5: Nach Abschluss der Konfiguration erhalten Sie eine Meldung, in der die nächsten Schritte erläutert werden. Klicken Sie nach dem Lesen der Informationen auf Got It.

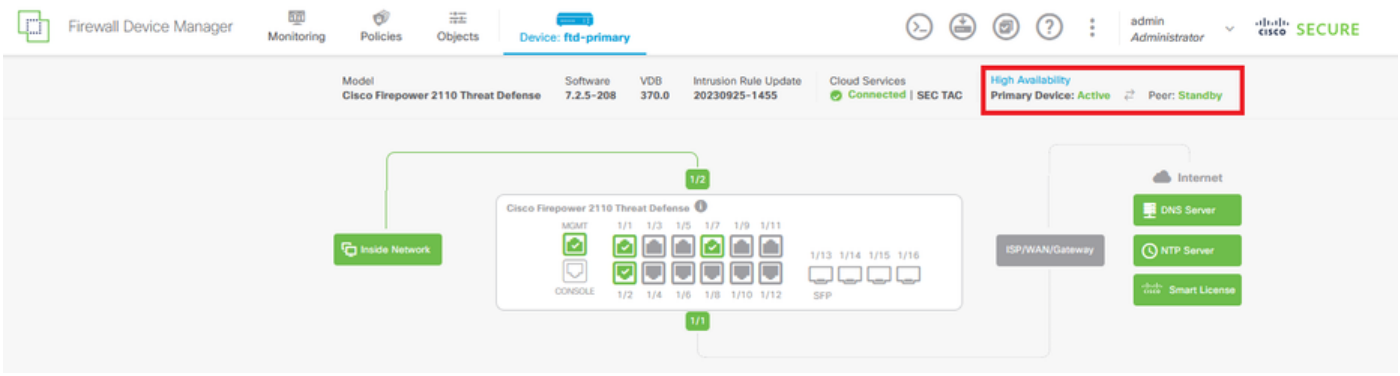


Überprüfung

- Zu diesem Zeitpunkt zeigt Ihr Gerätestatus am ehesten an, dass es sich um das sekundäre Gerät auf der Seite für hohe Verfügbarkeit handelt. Wenn der Join zum primären Gerät erfolgreich war, beginnt das Gerät mit dem primären Gerät zu synchronisieren, und schließlich wird der Modus in Standby und der Peer in Active geändert.



- In der primären FTD wird meist auch der Hochverfügbarkeitsstatus angezeigt, jedoch als "Aktiv" und "Peer: Standby".



- Öffnen Sie eine SSH-Sitzung mit dem primären FTD, und geben Sie den Befehl show running-config failover ein, um die Konfiguration zu überprüfen.

```
> 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
```

- Validieren Sie den aktuellen Status des Geräts mit dem Befehl 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

>
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.