Configura elevata disponibilità FTD tramite FDM

Sommario

Introduzione

In questo documento viene descritto come configurare una coppia HA (High Availability) attiva/standby di Secure Firewall Threat Defense (FTD) gestita localmente.

Prerequisiti

Requisiti

È consigliabile conoscere i seguenti argomenti:

- Configurazione iniziale di Cisco Secure Firewall Threat Defense tramite GUI e/o shell.

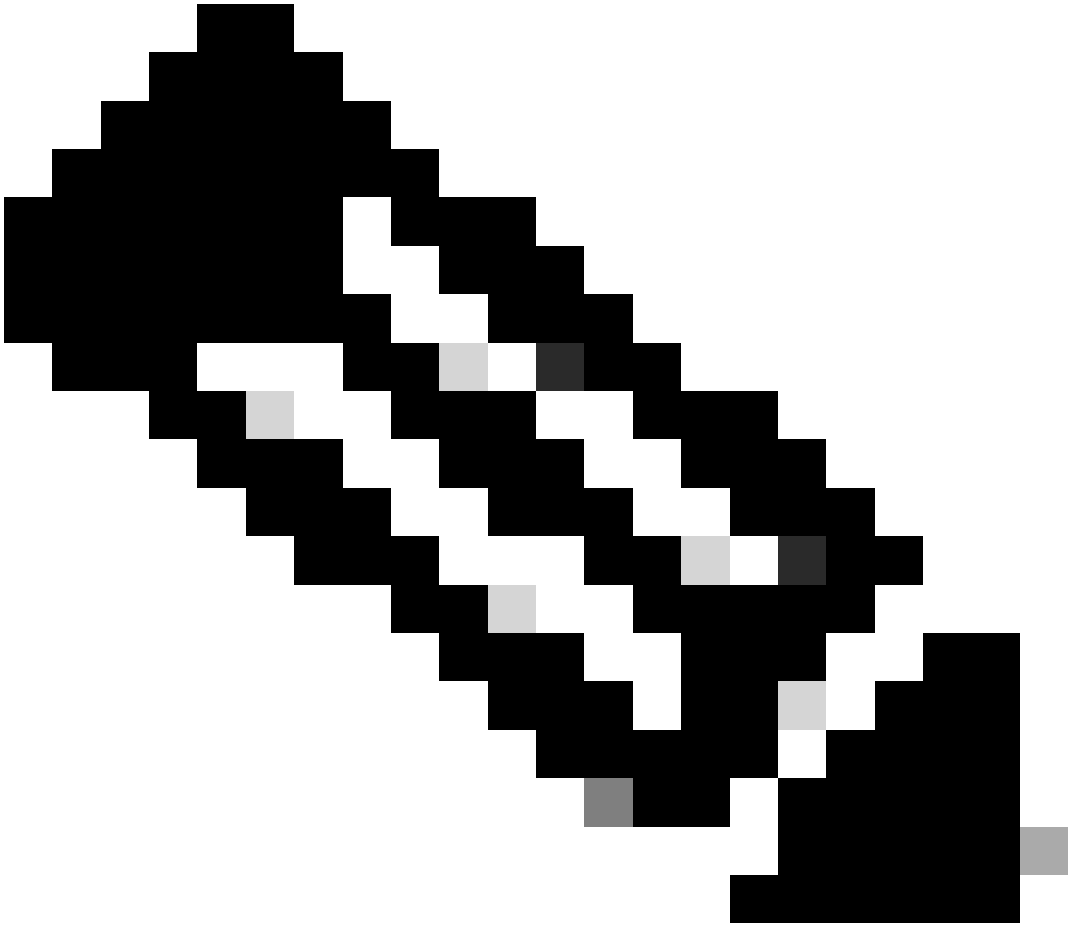
Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

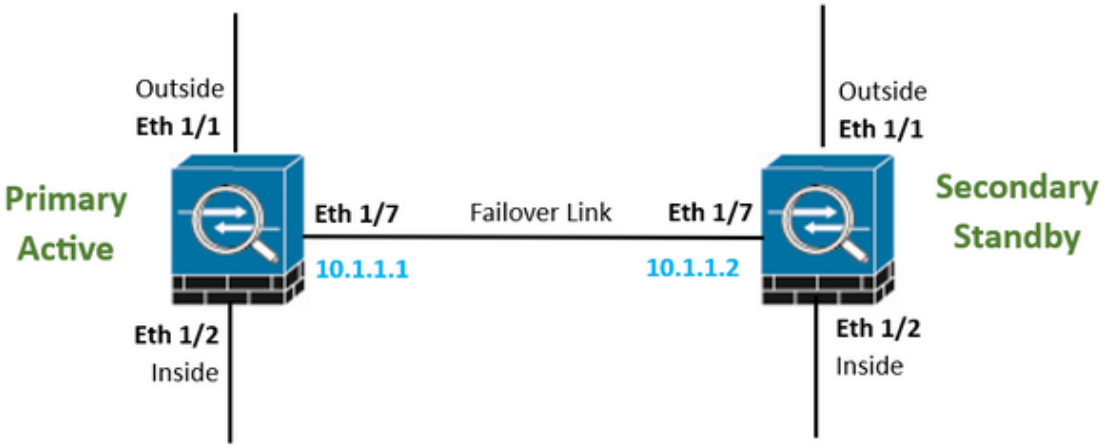
- FPR2110 versione 7.2.5 gestito localmente da Firepower Device Manager (FDM)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Topologia della rete



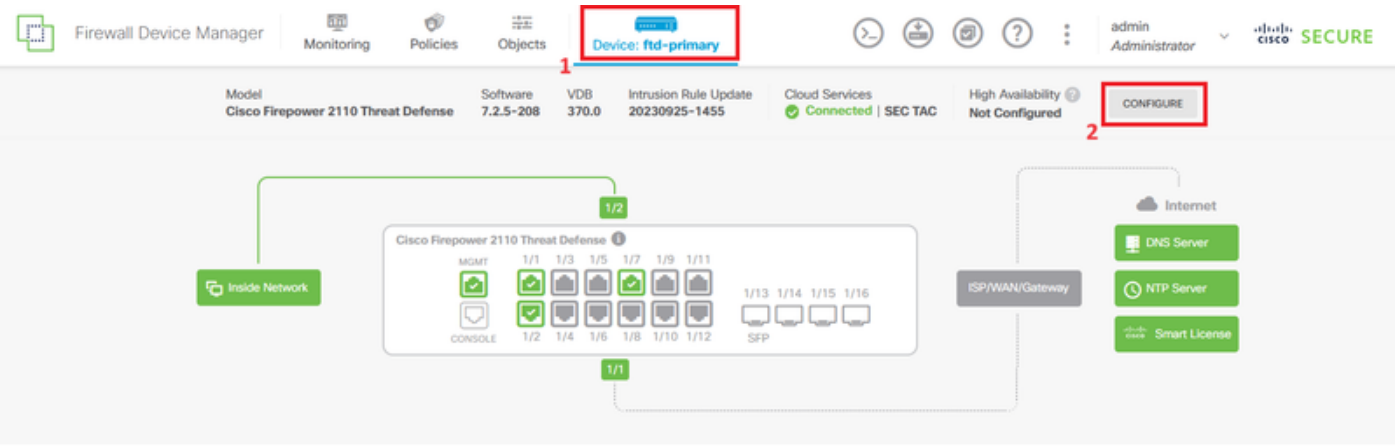
Nota: l'esempio descritto in questo documento è uno dei numerosi progetti di rete consigliati. Per ulteriori informazioni, consultare la guida alla configurazione per evitare failover interrotto e collegamenti dati.



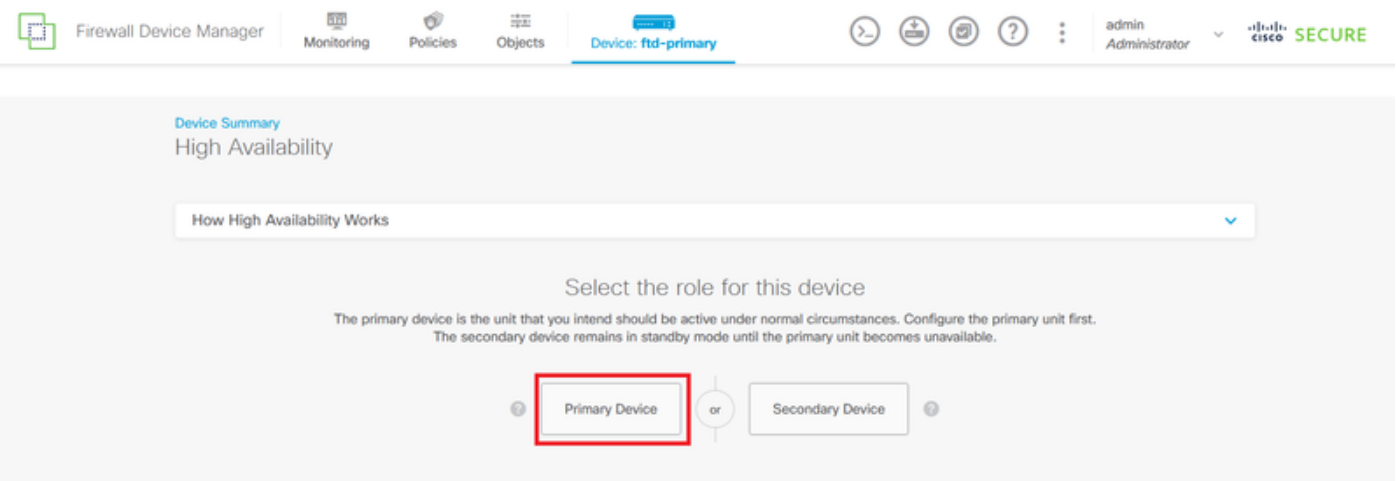
Configurazione

Configurare l'unità primaria per l'alta disponibilità

Passaggio 1. Fare clic su Device (Dispositivo) e premere il pulsante Configure (Configura) situato nell'angolo in alto a destra, accanto allo stato High Availability (Alta disponibilità).



Passaggio 2. Nella pagina Alta disponibilità fare clic sulla casella Dispositivo principale.



Passaggio 3. Configurare le proprietà Collegamento di failover.

Selezionare l'interfaccia connessa direttamente al firewall secondario e impostare l'indirizzo IP primario e secondario nonché la subnet netmask.

Selezionare la casella di controllo Utilizza la stessa interfaccia del collegamento di failover per il collegamento di failover stateful.

Deselezionare la casella Chiave di crittografia IPSec e fare clic su Attiva HA per salvare le modifiche.

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

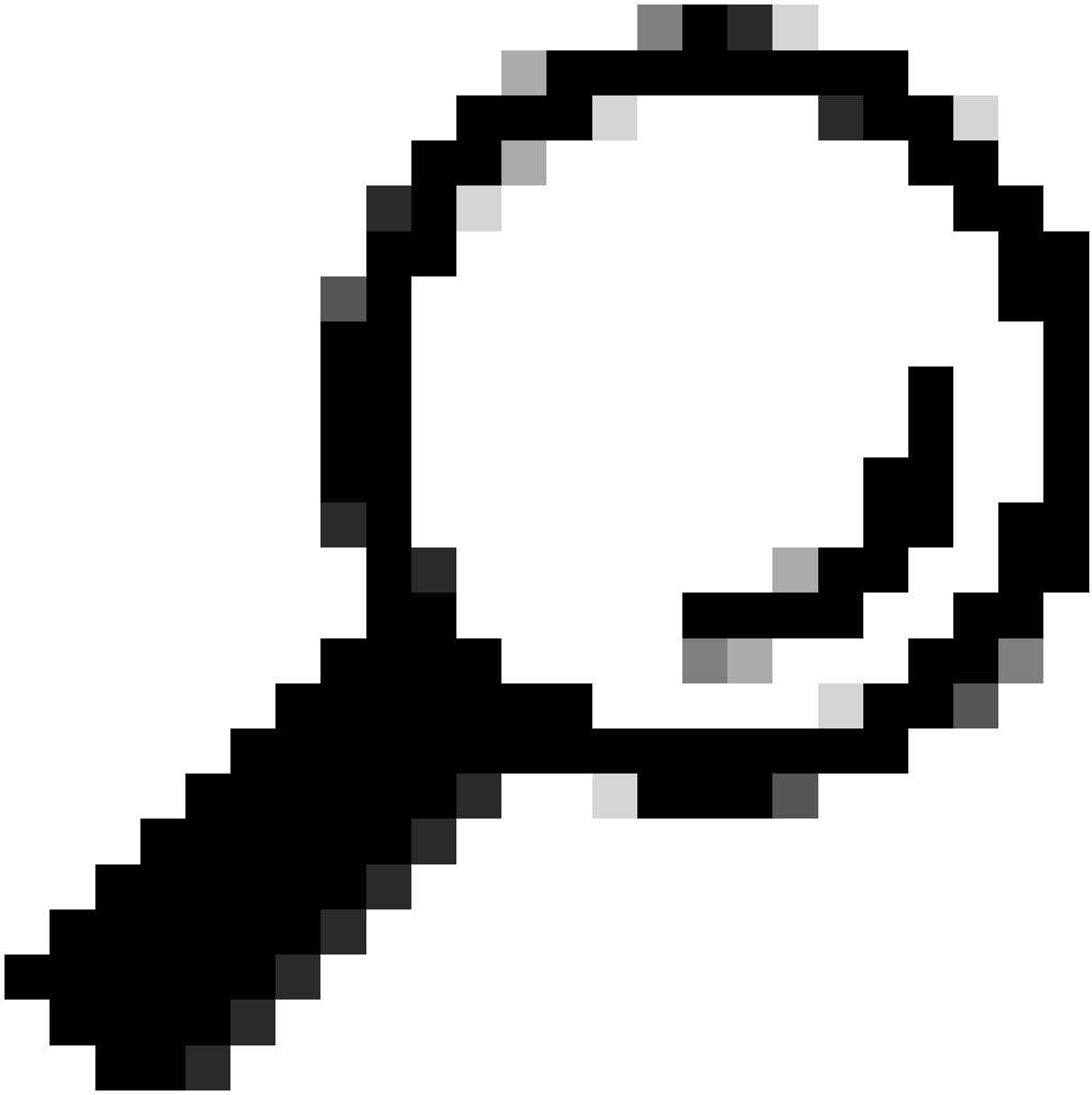
If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More

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

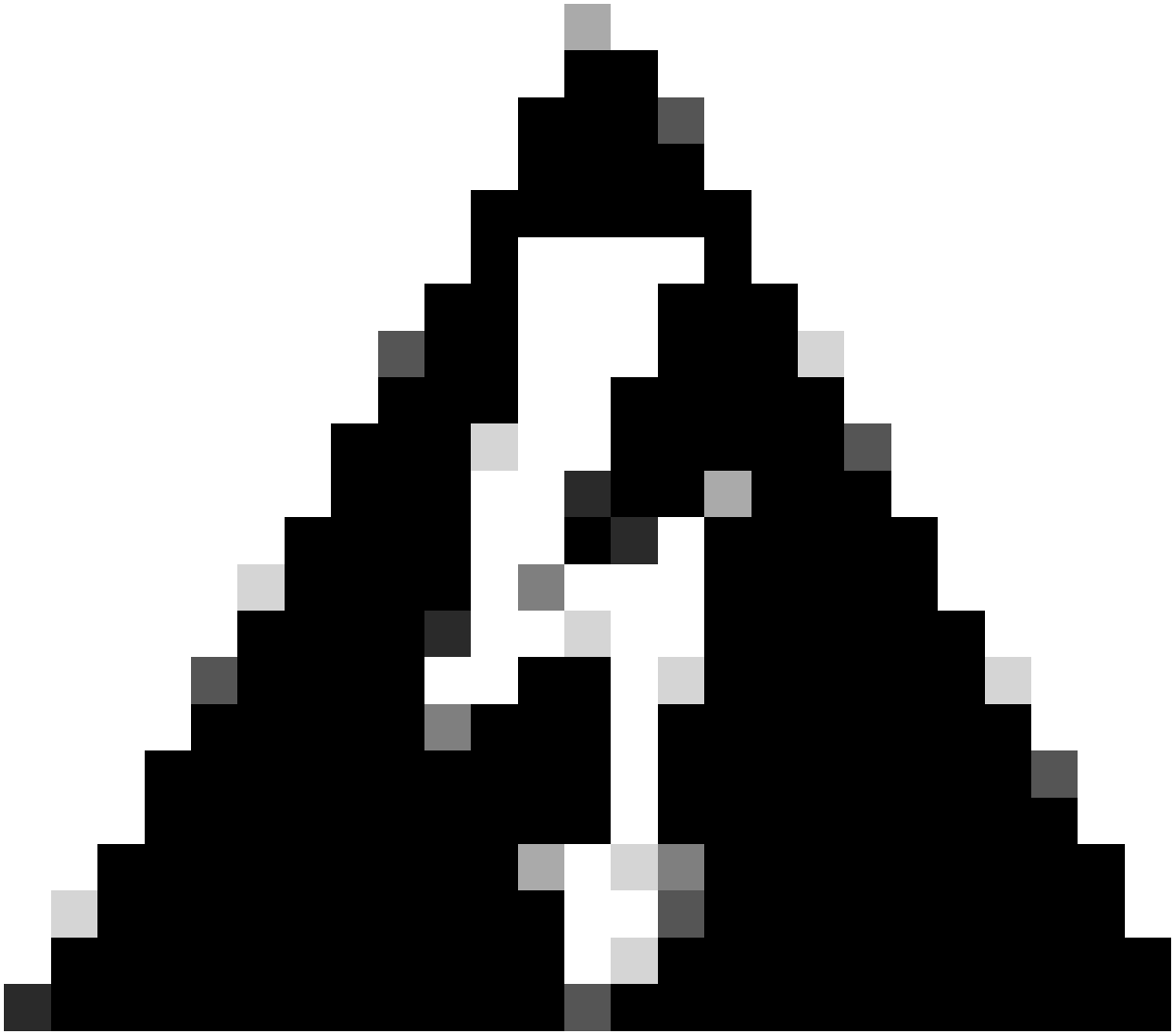
When you click Activate HA, these settings are automatically deployed to the device. The deployment might restart inspection engines, which can result in the momentary traffic loss. It might take a few minutes for deployment to finish.

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

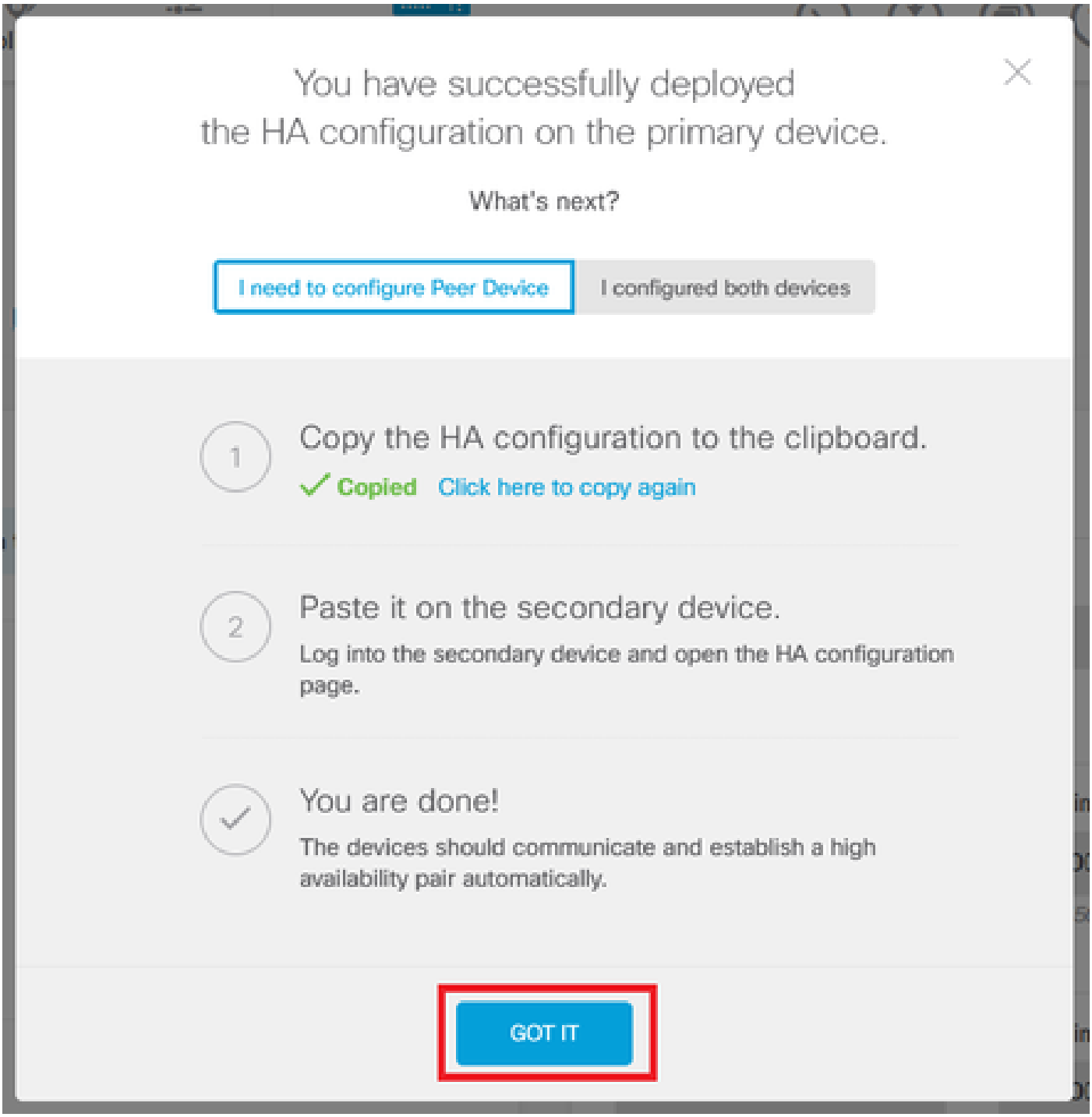


Suggerimento: utilizzare una subnet mask di piccole dimensioni, dedicata esclusivamente al traffico di failover per evitare violazioni della sicurezza e/o problemi di rete il più possibile.



Avviso: la configurazione viene distribuita immediatamente nel dispositivo. Non è necessario avviare un processo di distribuzione. Se non viene visualizzato un messaggio che indica che la configurazione è stata salvata e che la distribuzione è in corso, scorrere fino alla parte superiore della pagina per visualizzare i messaggi di errore. La configurazione viene copiata anche negli Appunti. È possibile utilizzare la copia per configurare rapidamente l'unità secondaria. Per una maggiore protezione, la chiave di crittografia (se ne è stata impostata una) non è inclusa nella copia negli Appunti.

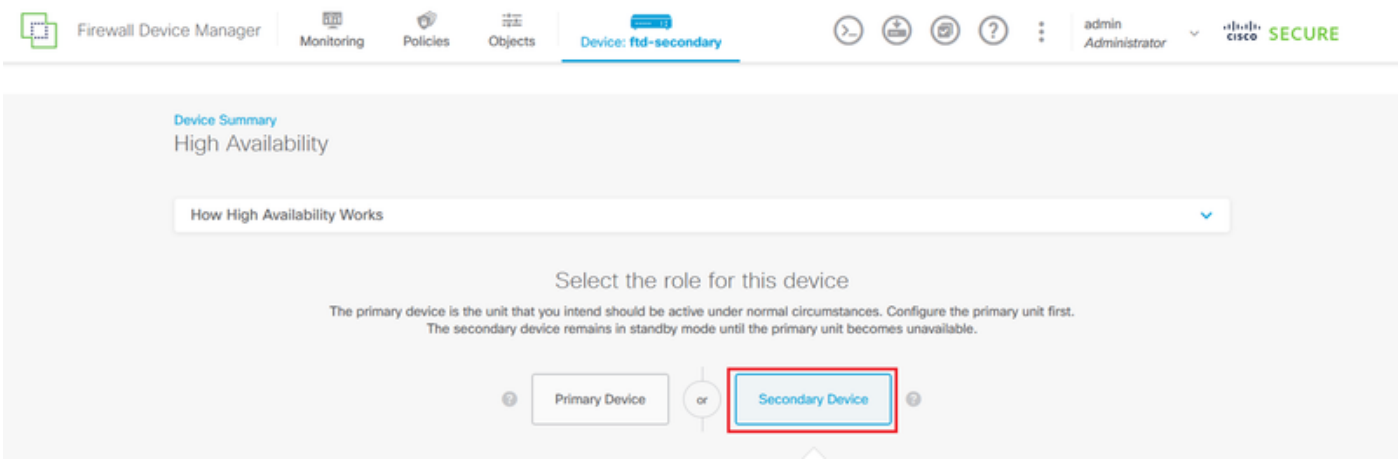
Passaggio 4. Al termine della configurazione, viene visualizzato un messaggio in cui vengono illustrati i passaggi successivi. Fare clic su Scarica dopo aver letto le informazioni.



Configurare l'unità secondaria per l'alta disponibilità

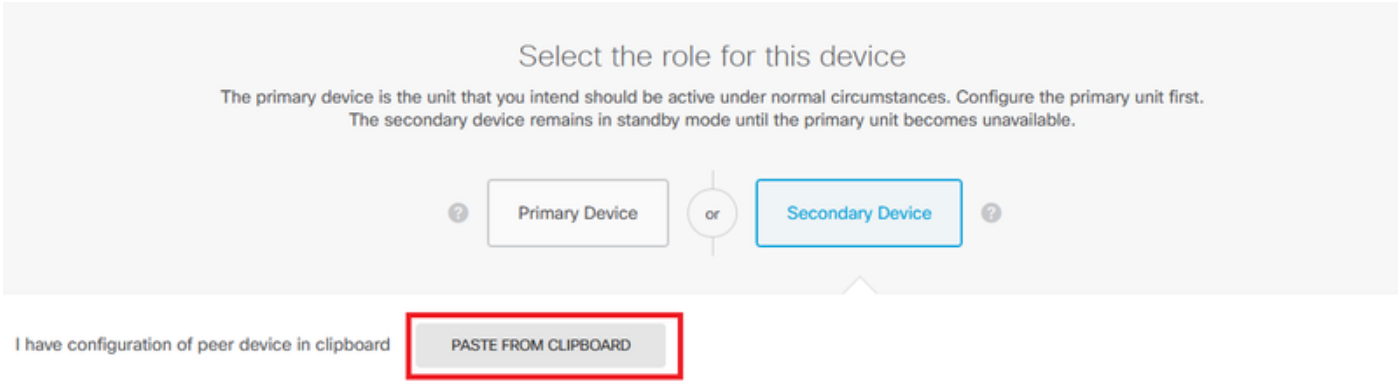
Passaggio 1. Fare clic su Device (Dispositivo) e premere il pulsante Configure (Configura) situato nell'angolo in alto a destra, accanto allo stato High Availability (Alta disponibilità).

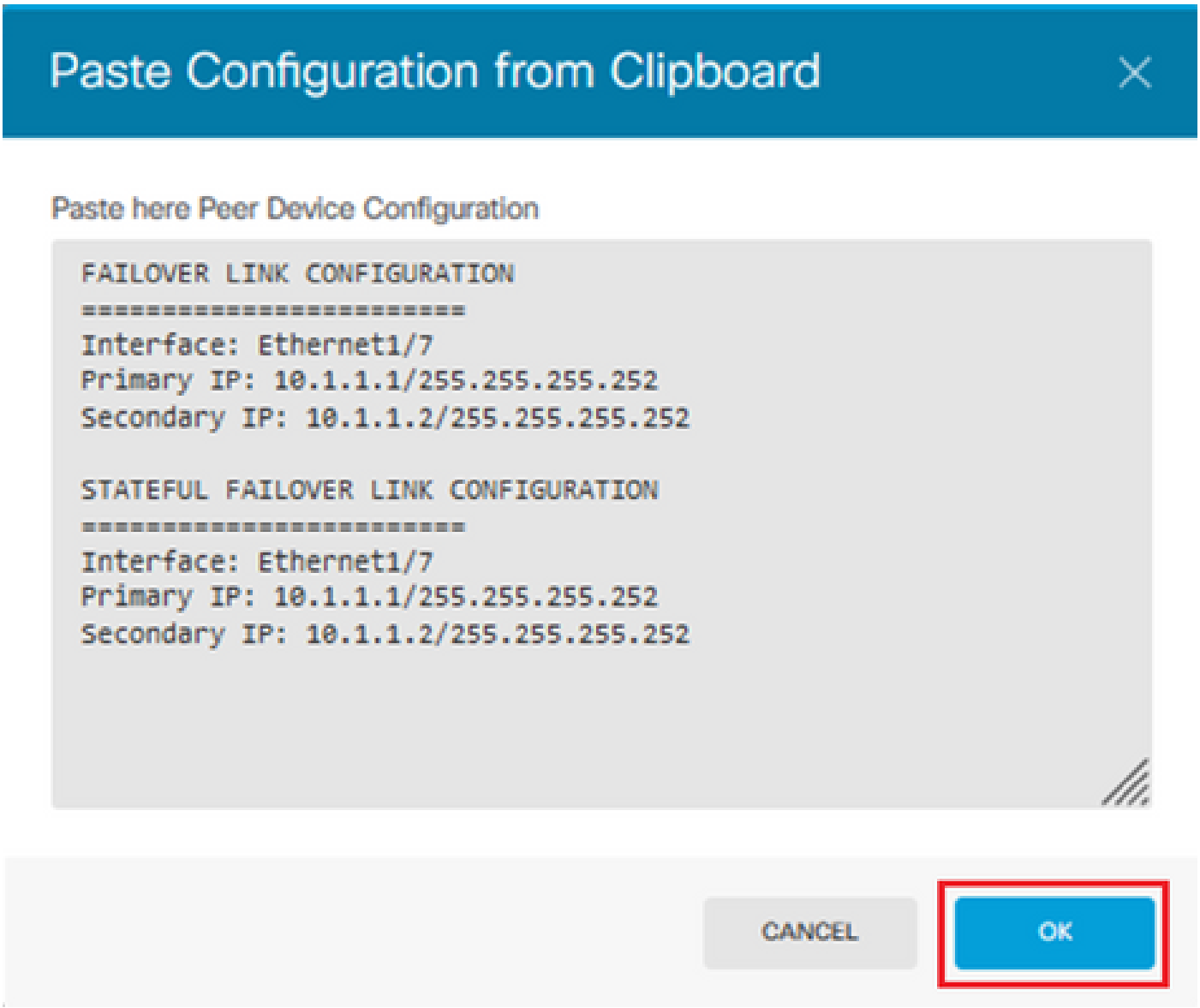
Passaggio 2. Nella pagina Alta disponibilità fare clic sulla casella Periferica secondaria.



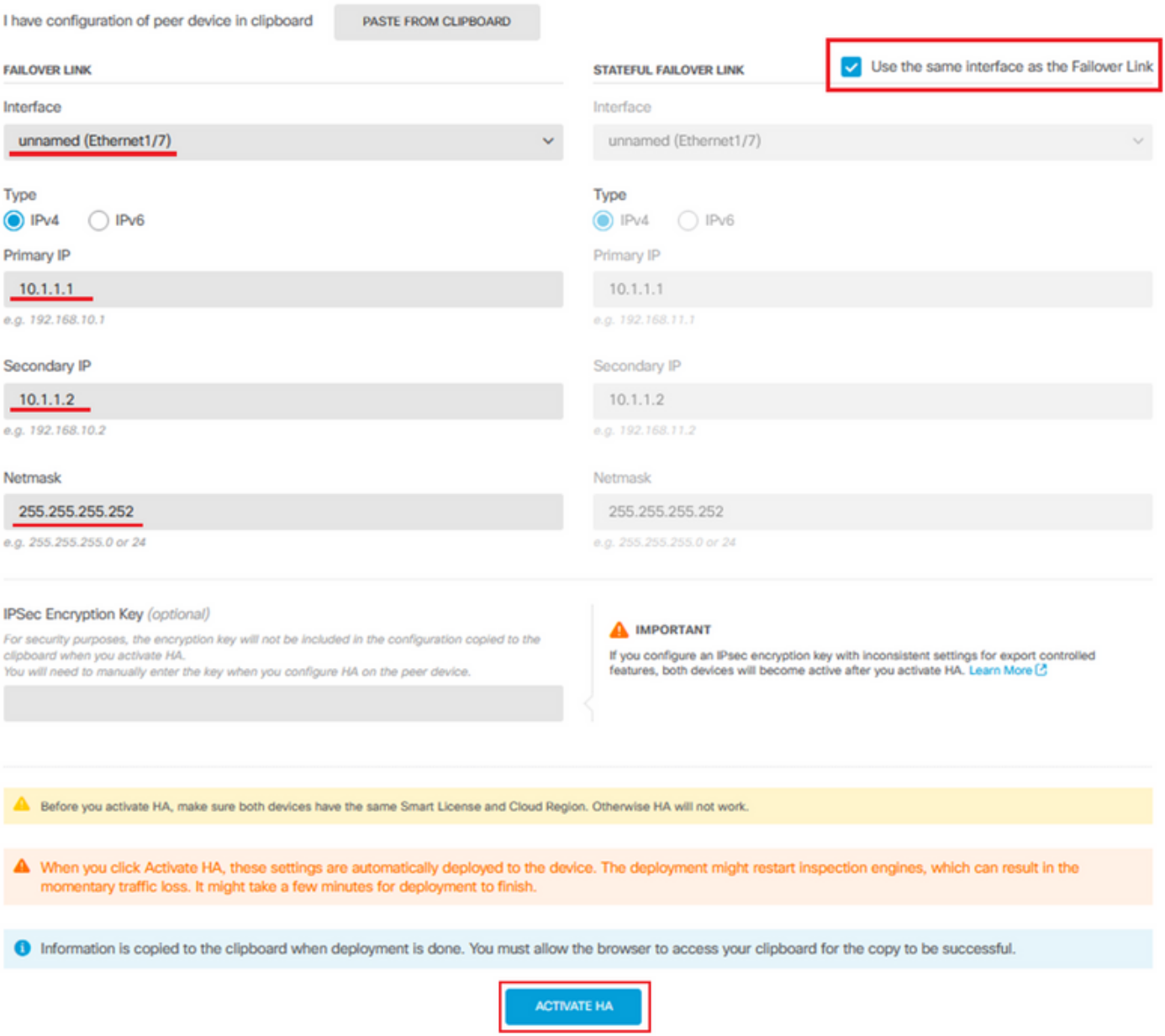
Passaggio 3. Configurare le proprietà Collegamento di failover. È possibile incollare le impostazioni memorizzate negli Appunti dopo aver configurato l'FTD principale oppure continuare manualmente.

Passaggio 3.1. Per incollare dagli Appunti, fare clic sul pulsante Incolla dagli Appunti, incollare nella configurazione (premere contemporaneamente i tasti Ctrl+v) e fare clic su OK.

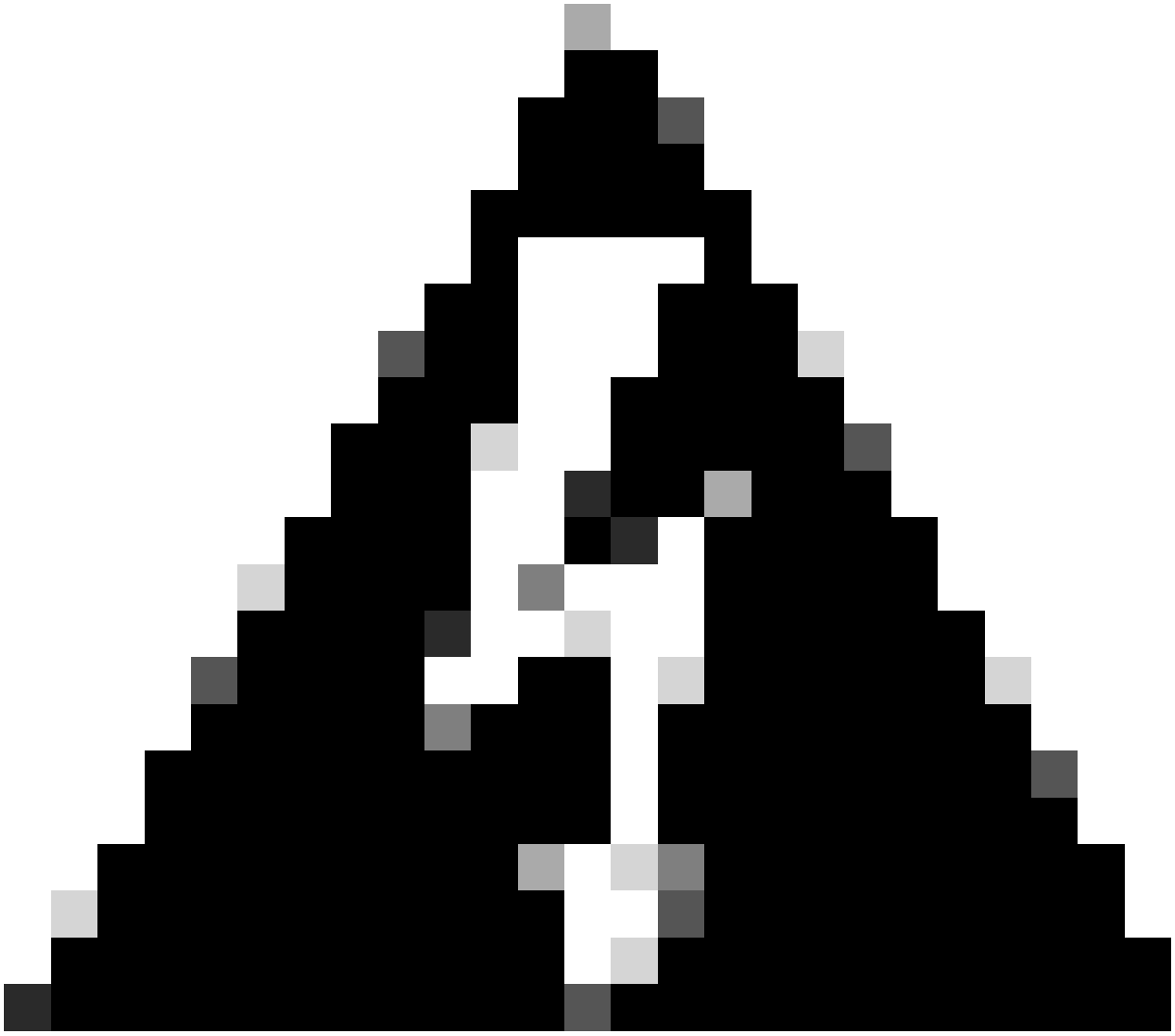




Passaggio 3.2. Per procedere manualmente, selezionare l'interfaccia connessa direttamente al firewall secondario e impostare l'indirizzo IP primario e secondario nonché la subnet netmask. Selezionare la casella di controllo Utilizza la stessa interfaccia del collegamento di failover per il collegamento di failover stateful.

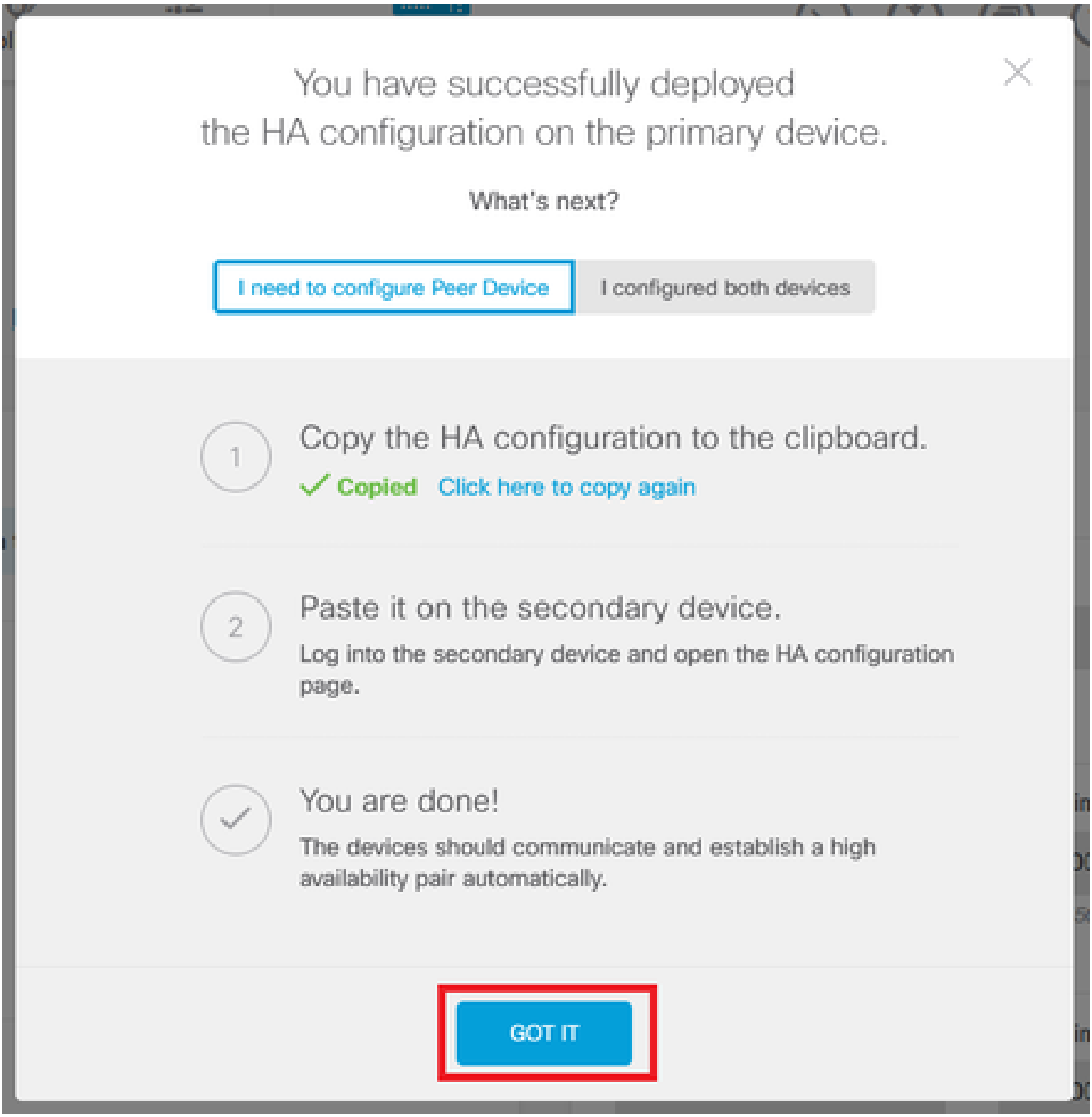


Passaggio 4. Deselezionare la casella Chiave di crittografia IPSec e fare clic su Attiva HA per salvare le modifiche.



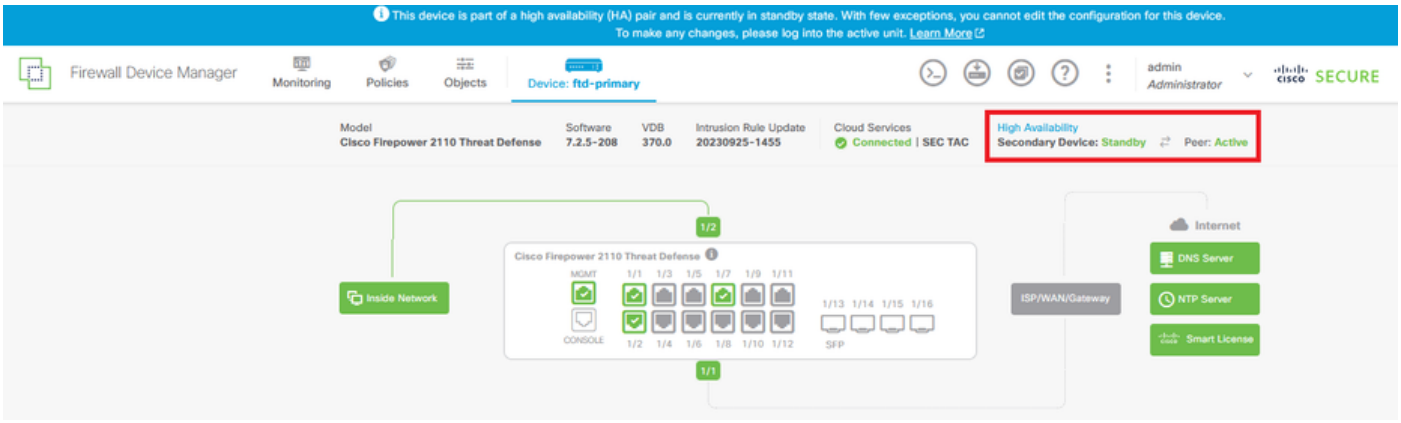
Avviso: la configurazione viene distribuita immediatamente nel dispositivo. Non è necessario avviare un processo di distribuzione. Se non viene visualizzato un messaggio che indica che la configurazione è stata salvata e che la distribuzione è in corso, scorrere fino alla parte superiore della pagina per visualizzare i messaggi di errore.

Passaggio 5. Al termine della configurazione, viene visualizzato un messaggio in cui vengono illustrati i passaggi successivi da eseguire. Fare clic su Scarica dopo aver letto le informazioni.

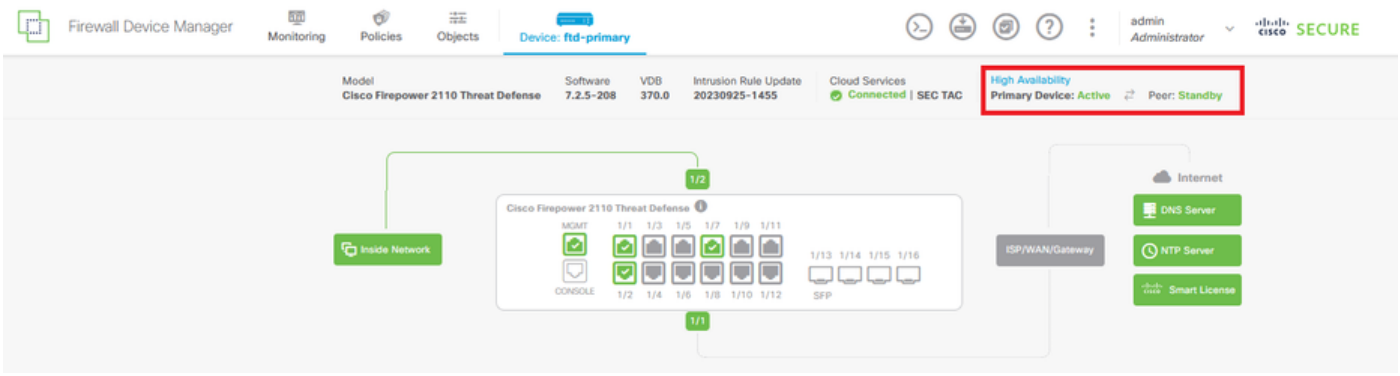


Verifica

- A questo punto lo stato del dispositivo indica che si tratta del dispositivo secondario nella pagina Alta disponibilità. Se l'unione con il dispositivo primario ha esito positivo, il dispositivo inizia a sincronizzarsi con il dispositivo primario e alla fine la modalità viene modificata in Standby e il peer in Attivo.



- L'FTD principale visualizza in genere anche lo stato Alta disponibilità, ma come Attivo e Peer: Standby.



- Aprire una sessione SSH sull'FTD primario e usare il comando show running-config failover per verificare la configurazione.

```
> 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
```

- Convalidare lo stato corrente del dispositivo con il comando 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

>
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).