

# 使用FDM配置FTD高可用性

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络拓扑](#)

[配置](#)

[配置主设备以实现高可用性](#)

[配置辅助设备以实现高可用性](#)

[验证](#)

---

## 简介

本文档介绍如何设置本地管理的安全防火墙威胁防御(FTD)的主用/备用高可用性(HA)对。

## 先决条件

### 要求

建议了解以下主题：

- 通过GUI和/或外壳进行的思科安全防火墙威胁防御初始配置。

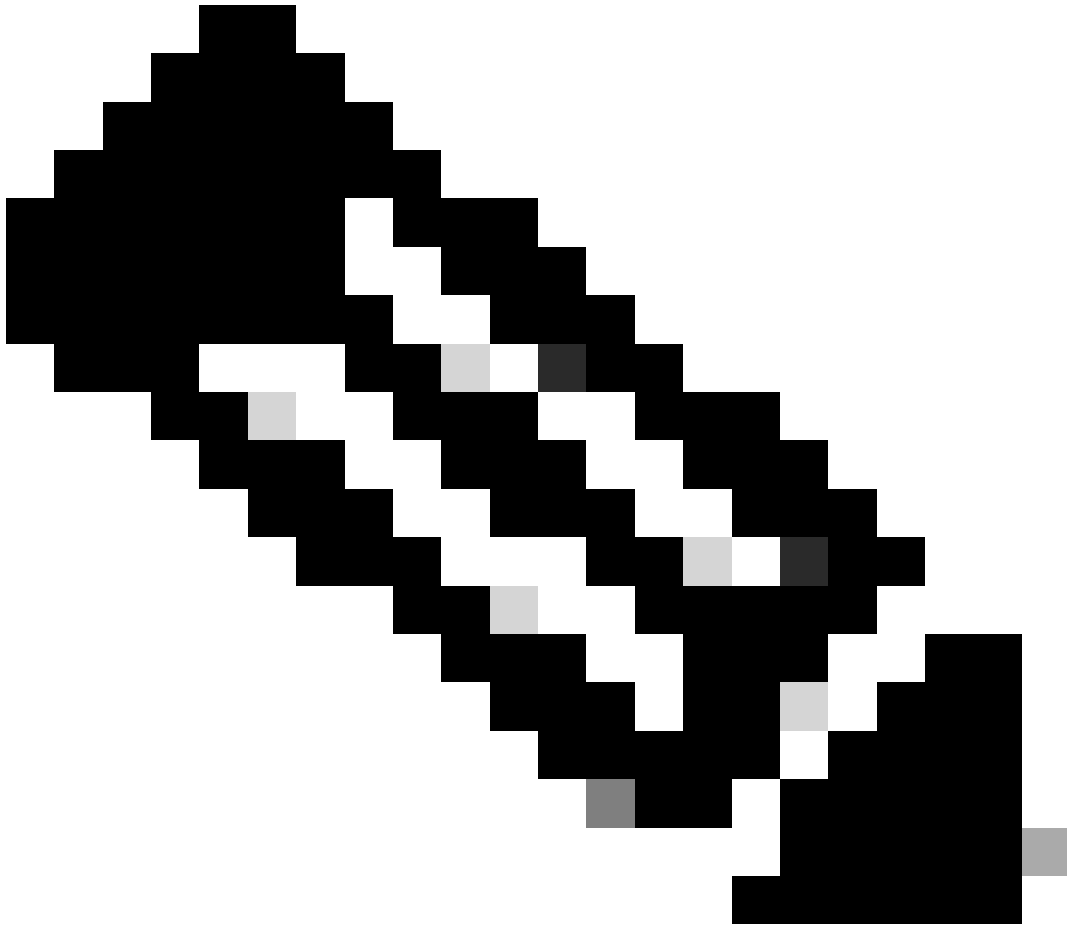
### 使用的组件

本文档中的信息基于以下软件和硬件版本：

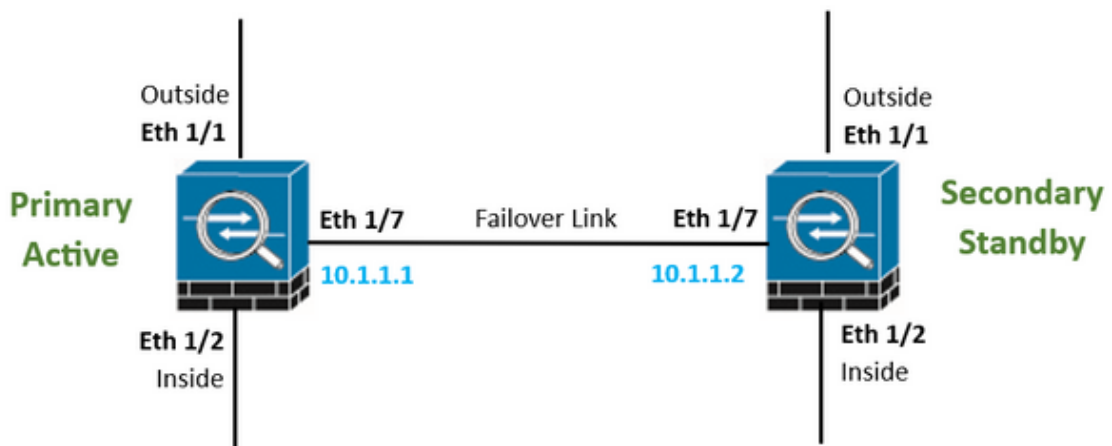
- FPR2110版本7.2.5由Firepower设备管理器(FDM)本地管理

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 网络拓扑



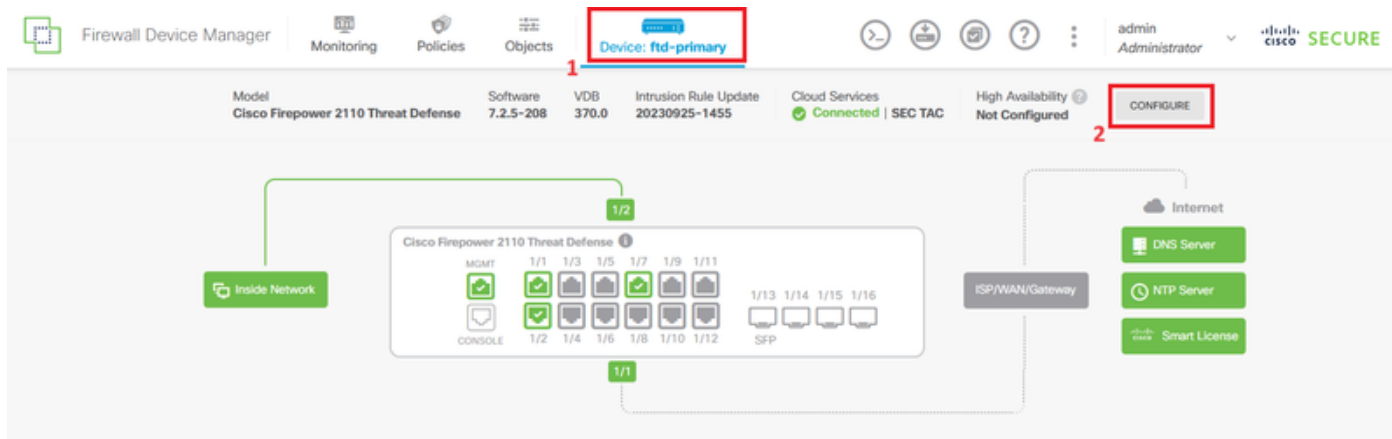
注意：本文档中介绍的示例是推荐的多种网络设计之一。有关更多选项，请参阅[避免中断故障切换和数据链路配置指南](#)。



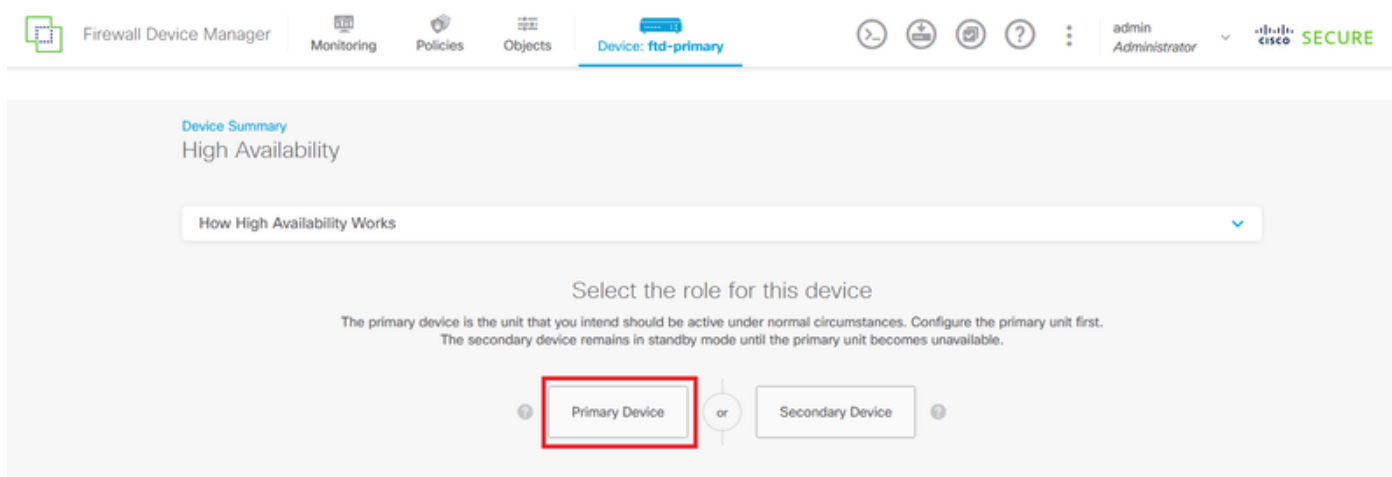
# 配置

## 配置主设备以实现高可用性

步骤1:单击Device，然后按下位于High Availability状态旁右上角的Configure按钮。



第二步：在“High Availability”页面上，单击Primary Device框。



第三步：配置故障切换链路属性。

选择已直接连接到辅助防火墙的接口，并设置主要和辅助IP地址以及子网网络掩码。

对于有状态故障切换链路，请选中Use the same interface as the Failover Link复选框。

清除“IPSec加密密钥”框，然后单击激活HA以保存更改。

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

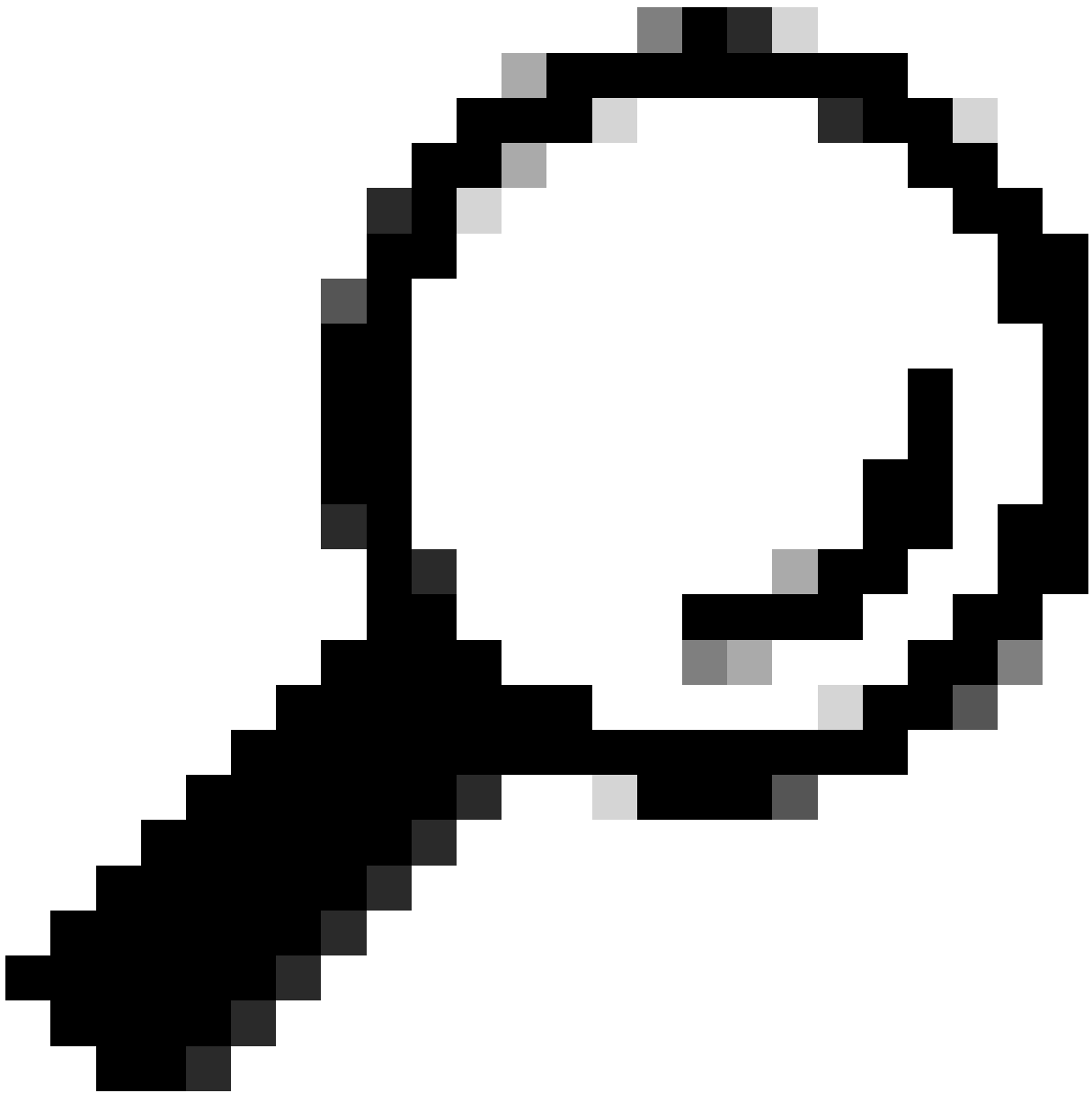
If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. [Learn More](#)

**⚠** 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.

**i** 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.

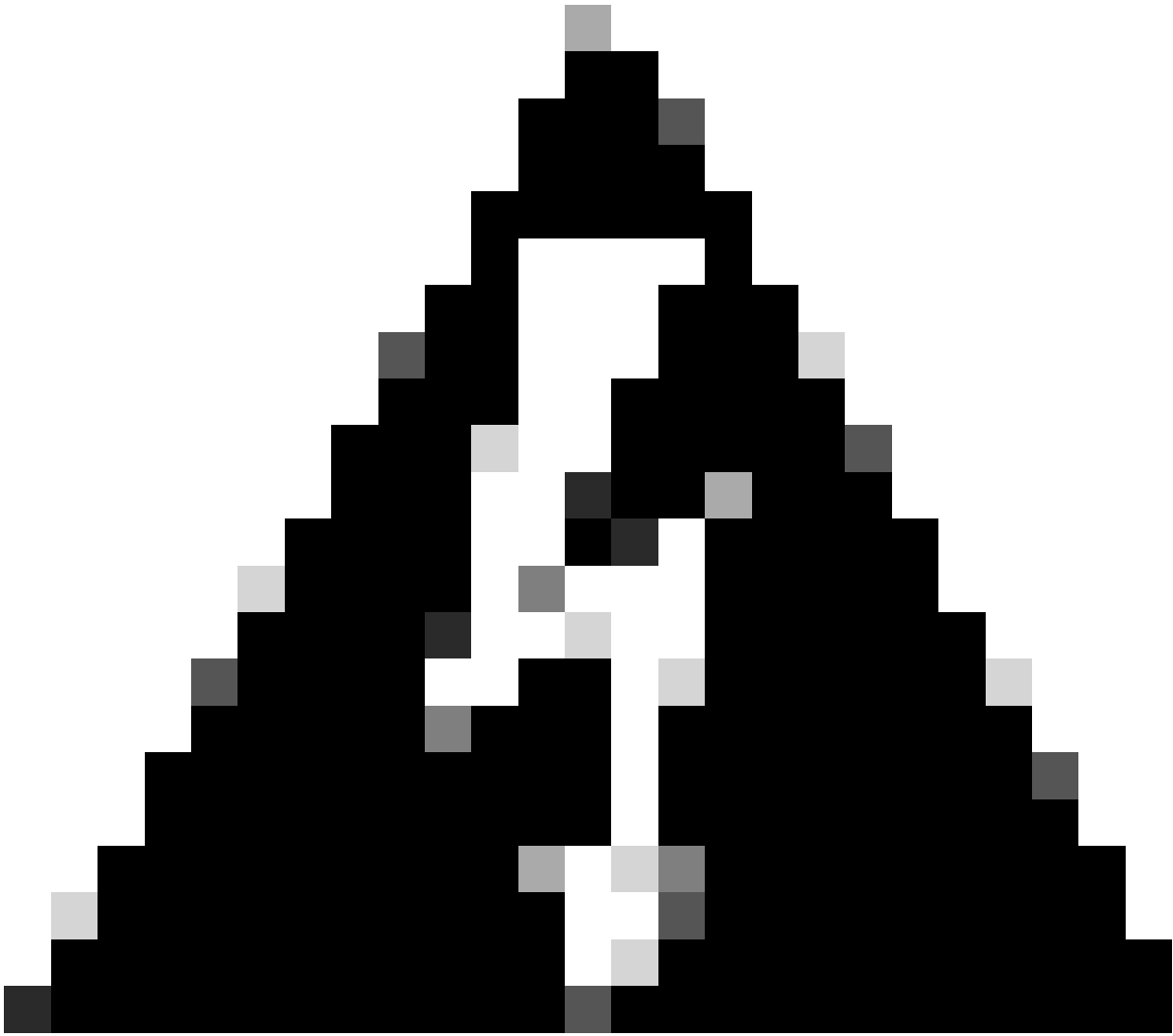
ACTIVATE HA



提示：使用专门用于故障切换流量的小型掩码子网，以尽可能避免安全漏洞和/或网络问题。

。

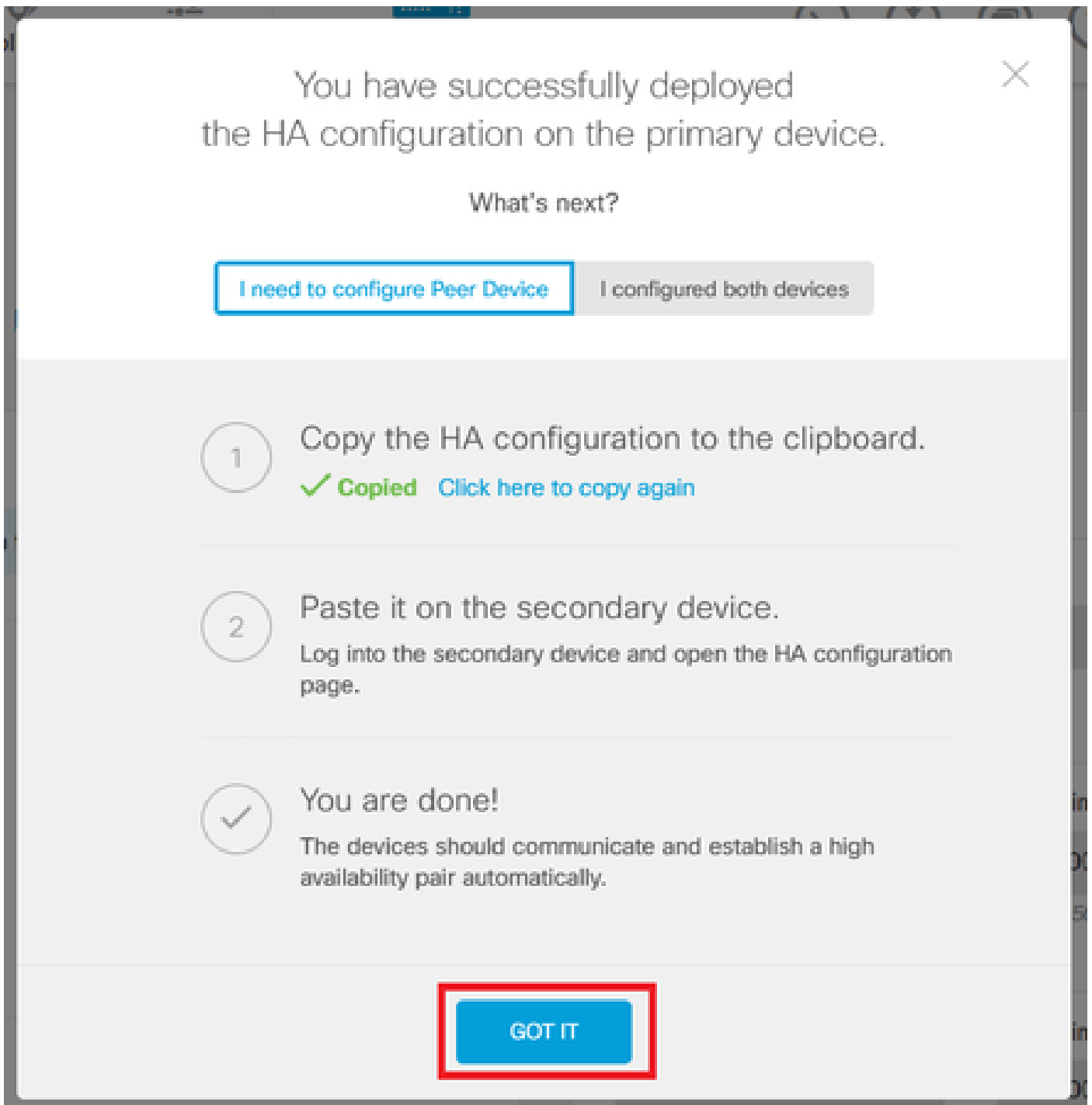
---



**警告：**系统立即将配置部署到设备。您无需启动部署作业。如果您没有看到表明配置已保存且部署正在进行中的消息，请滚动到页面顶部以查看错误消息。配置也会复制到剪贴板。您可以使用该副本快速配置辅助设备。为增强安全性，剪贴板副本中不包含加密密钥（如果已设置）。

---

**第四步：**配置完成后，您将收到一条消息，解释后续步骤。读取信息后，单击Get It。

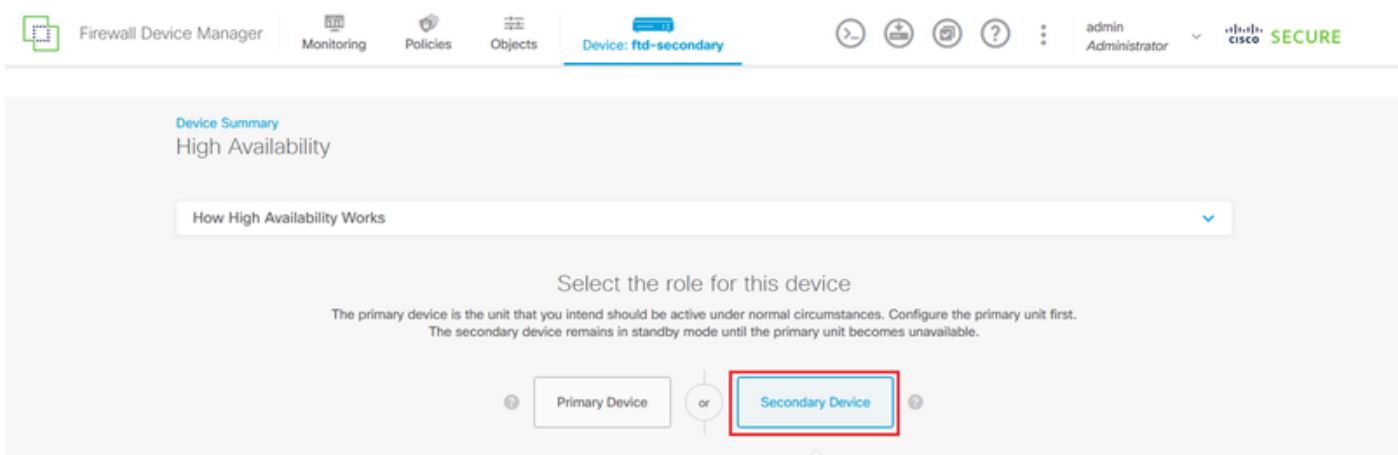


## 配置辅助设备以实现高可用性

步骤1:单击Device，然后按下位于High Availability状态旁右上角的Configure按钮。

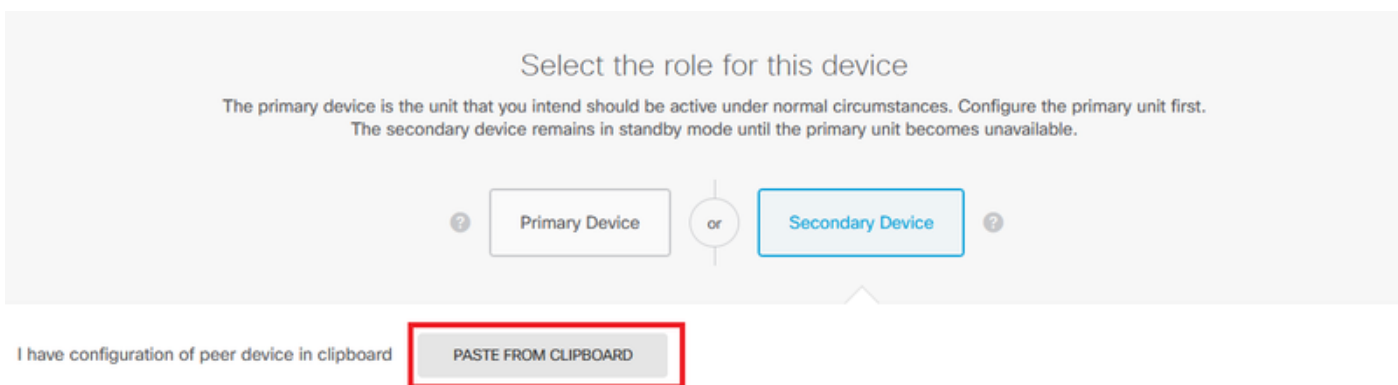


第二步：在“High Availability”页面上，单击Secondary Device框。



第三步：配置故障切换链路属性。配置主要FTD后，可以粘贴剪贴板中存储的设置，也可以手动继续。

步骤 3.1 要从剪贴板粘贴，只需单击Paste from Clipboard按钮，粘贴配置（同时按住Ctrl+v键）并单击OK。





## Paste Configuration from Clipboard



Paste here Peer Device Configuration

```
FAILOVER LINK CONFIGURATION
=====
Interface: Ethernet1/7
Primary IP: 10.1.1.1/255.255.255.252
Secondary IP: 10.1.1.2/255.255.255.252

STATEFUL FAILOVER LINK CONFIGURATION
=====
Interface: Ethernet1/7
Primary IP: 10.1.1.1/255.255.255.252
Secondary IP: 10.1.1.2/255.255.255.252
```

CANCEL

OK

步骤 3.2要手动继续，请选择已直接连接到辅助防火墙的接口，并设置主要和辅助IP地址以及子网网络掩码。对于有状态故障切换链路，请选中Use the same interface as the Failover Link复选框。

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](#)

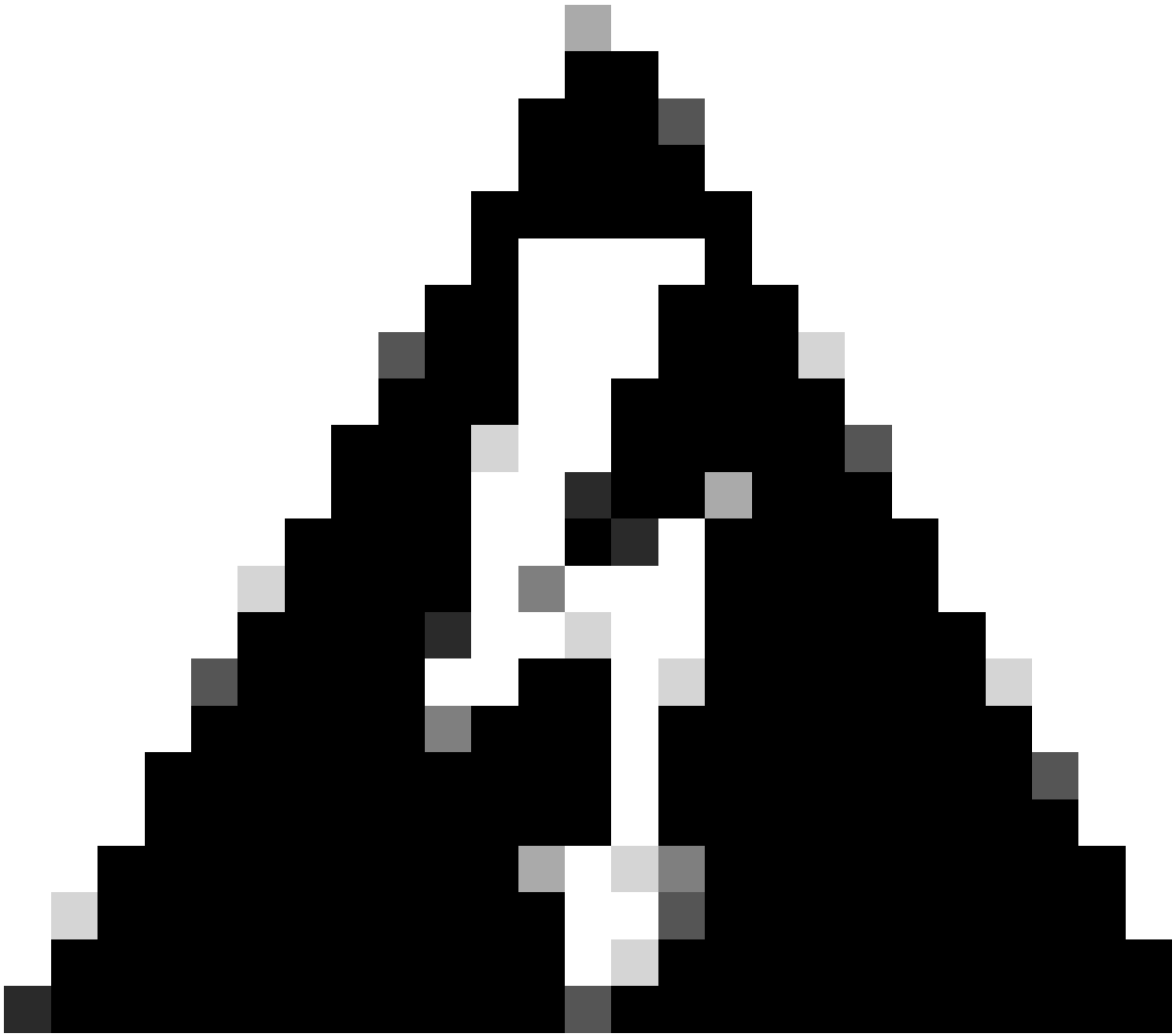
**⚠** Before you activate HA, make sure both devices have the same Smart License and Cloud Region. Otherwise HA will not work.

**⚠** 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.

**i** 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

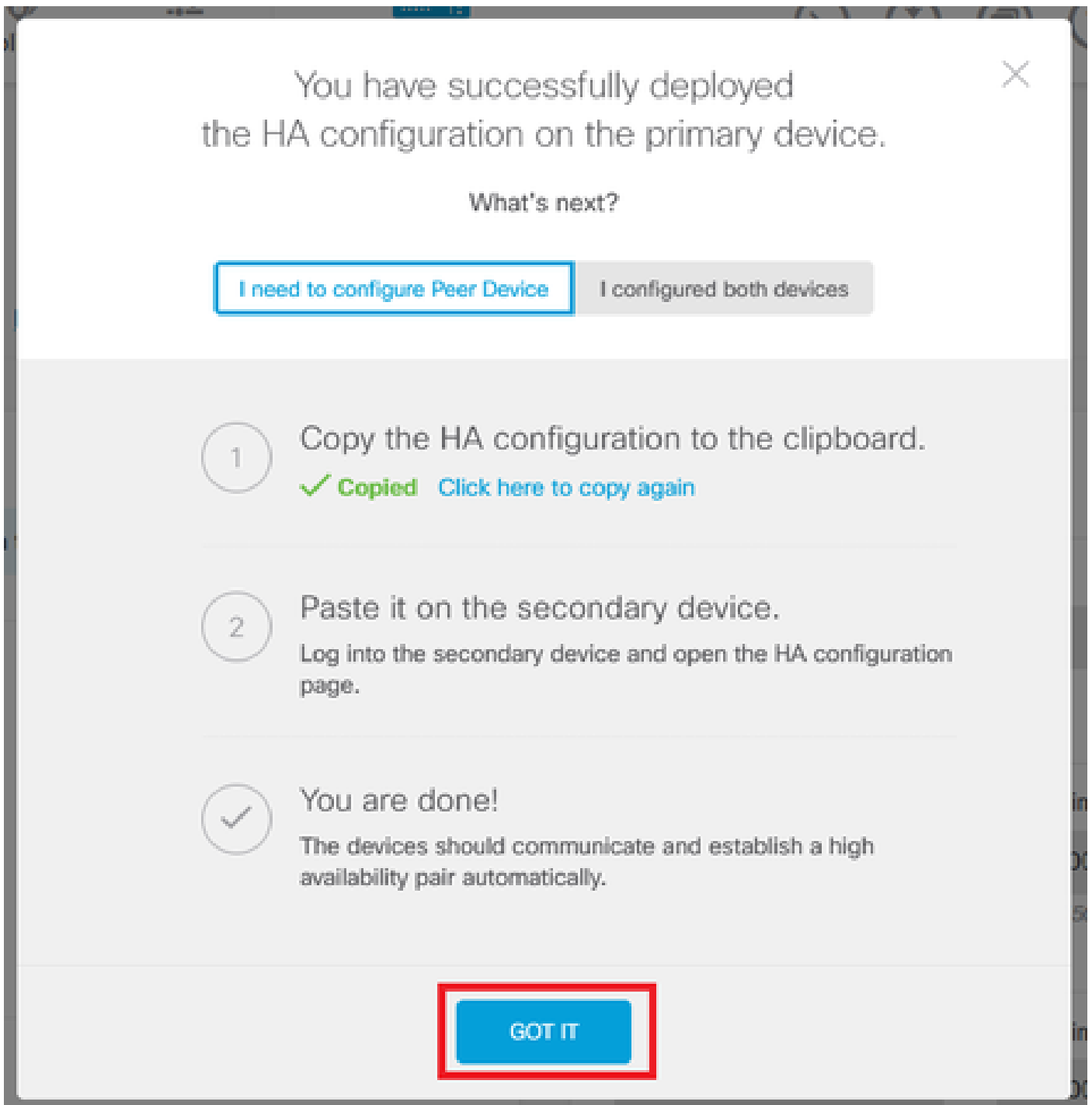
第四步：清除“IPSec加密密钥”框，然后单击激活HA以保存更改。



**警告：**系统立即将配置部署到设备。您无需启动部署作业。如果您没有看到表明配置已保存且部署正在进行中的消息，请滚动到页面顶部以查看错误消息。

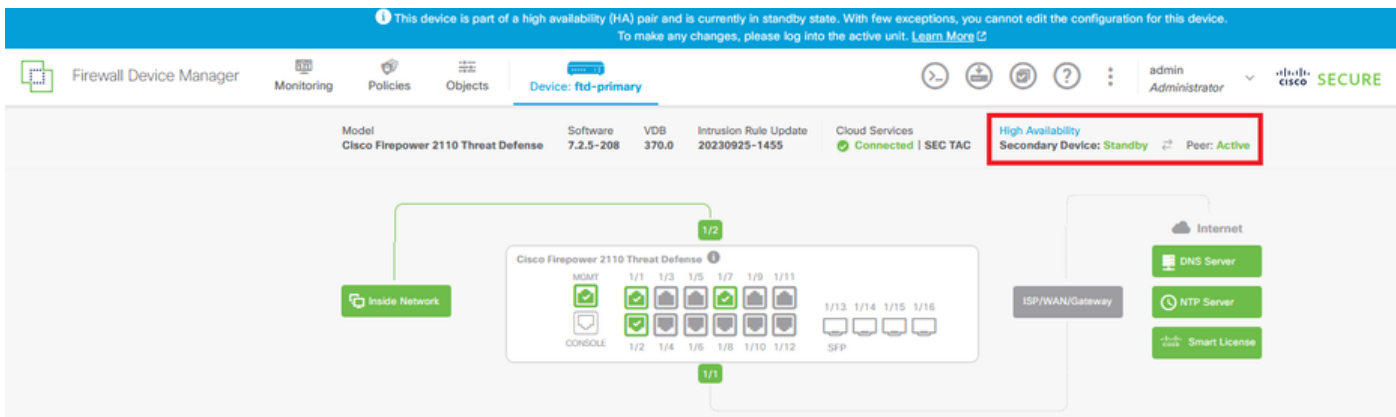
---

**第五步：**配置完成后，您将收到一条消息，说明您需要采取的后续步骤。读取信息后，单击Get It。

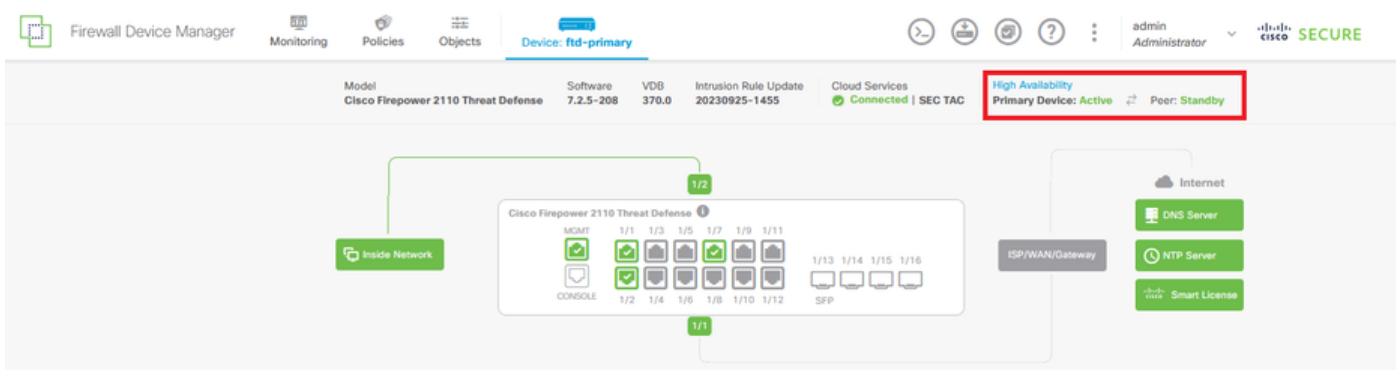


## 验证

- 此时，您的设备状态大部分指示这是High Availability页面上的辅助设备。如果与主设备的加入成功，设备将开始与主设备同步，最终模式更改为“备用”，对等设备更改为“活动”。



- 主FTD也大多数显示High Availability状态，但显示为Active和Peer：Standby。



- 打开与主FTD的SSH会话，并发出命令show running-config failover以验证配置。

```
> 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
```

- 使用命令show failover state验证设备的当前状态。

```
> 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

>
```

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。