

使用Firepower迁移工具从ASA配置文件配置FTD

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[验证](#)

[与Firepower迁移工具相关的已知错误](#)

[相关信息](#)

简介

本文档介绍自适应安全设备(ASA)到Firepower威胁防御(FTD)在FPR4145上迁移的示例。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA的基本知识
- Firepower管理中心(FMC)和FTD知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA 9.12(2) 版
- FTD版本6.7.0
- FMC版本6.7.0
- Firepower迁移工具版本2.5.0

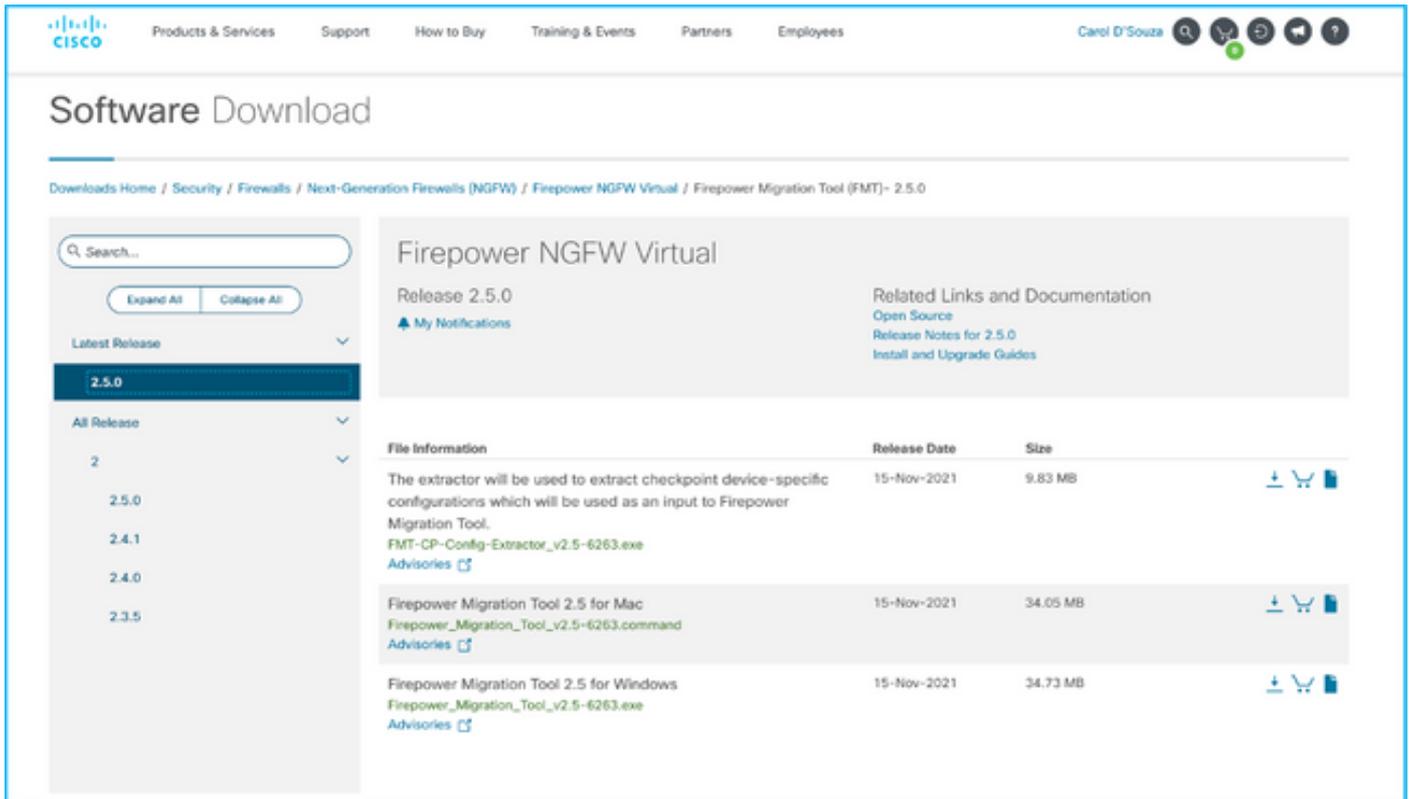
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

以.cfg或.txt格式导出ASA配置文件。FMC应部署为在其下注册的FTD。

配置

1.如图所示，从software.cisco.com下载Firepower迁移工具。



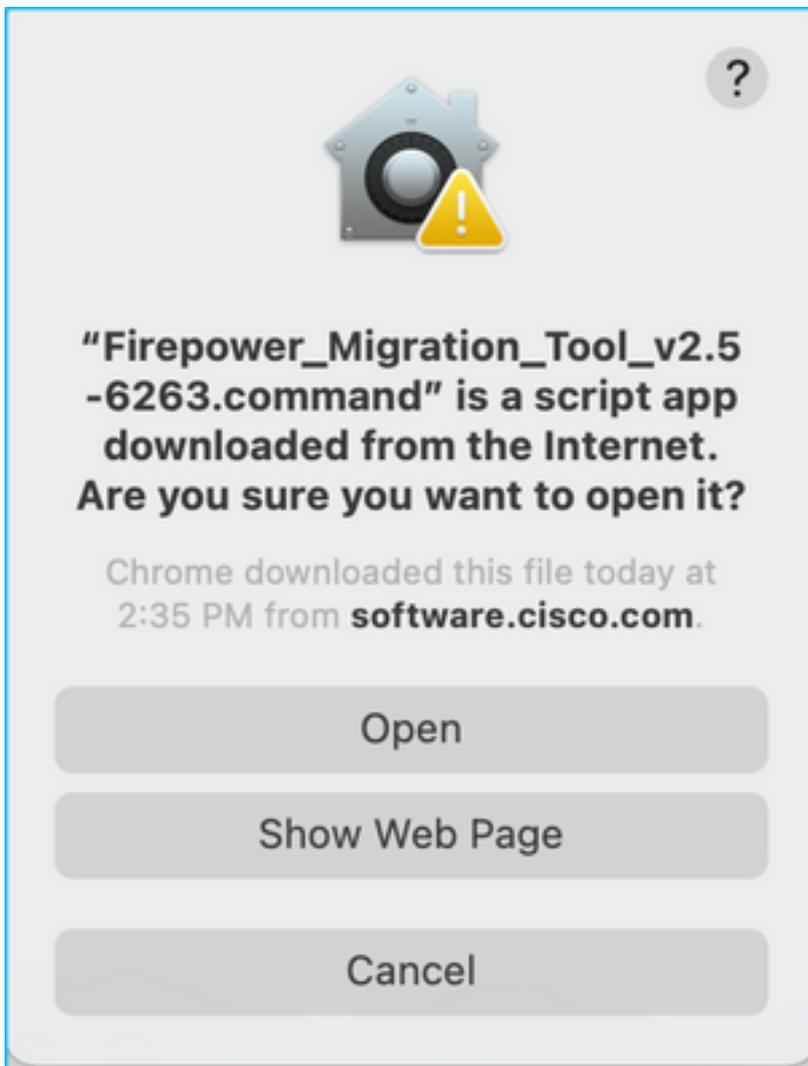
2.查看并验证“Firepower迁移工具的指南和限制”一节中的要求。

3.如果计划迁移大型配置文件，请配置睡眠设置，以便系统在迁移推送期间不进入睡眠状态。

3.1.对于Windows，导航至“控制面板”中的“电源选项”。单击当前电源计划旁边的更改计划设置。更改将计算机置于睡眠状态为“不”。单击“保存更改”。

3.2.对于MAC，导航至系统首选项>节能。勾选旁边的框，防止计算机在显示关闭时自动睡眠，并将滑块后的“关闭显示”拖动到“从不”。

注意：此警告，当MAC用户尝试打开下载的文件时，会弹出对话框。请忽略此警告，然后执行步骤4 A。



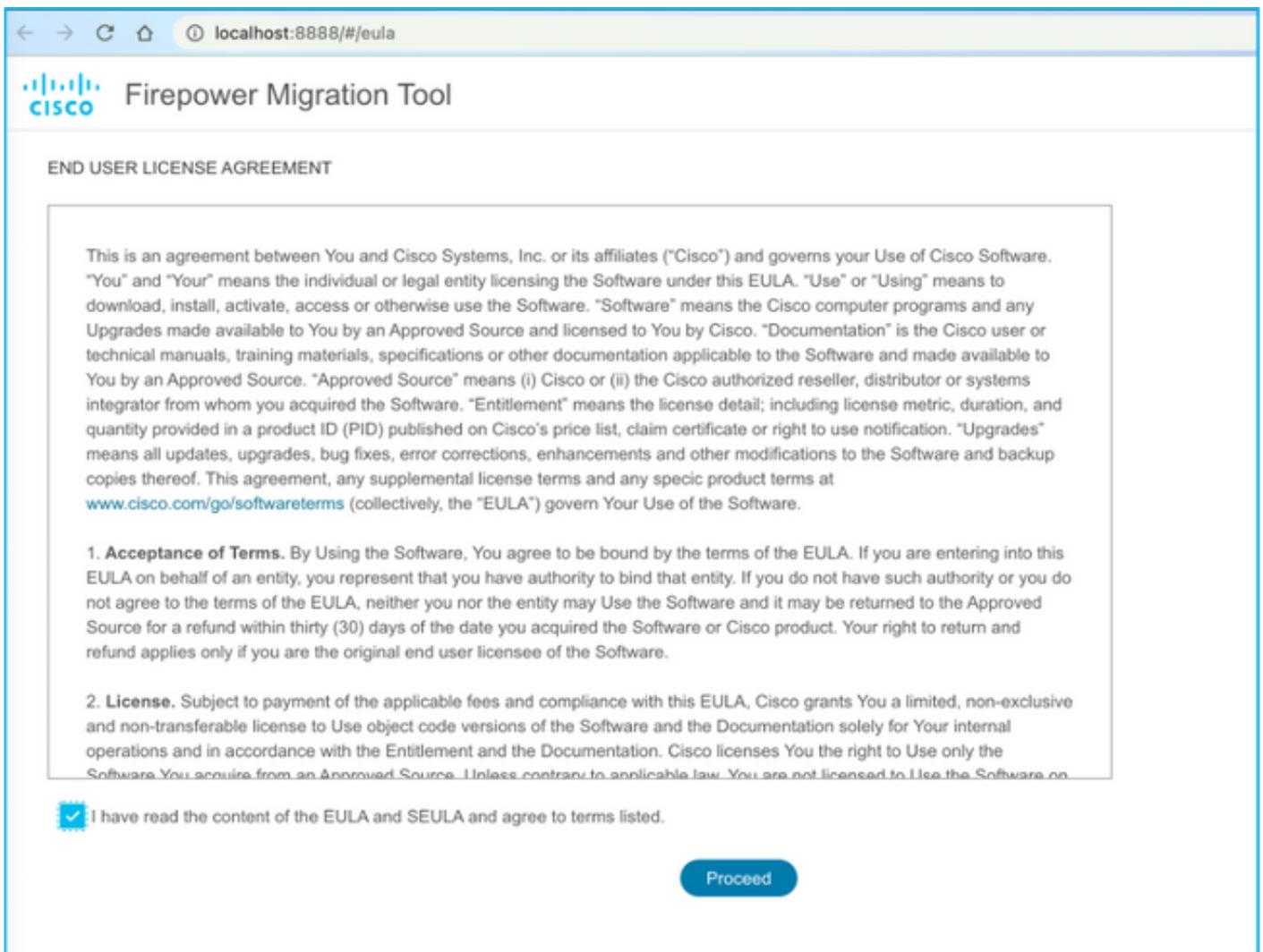
4. A.对于MAC — 使用终端并运行这些命令。

```
CAROLDSO-M-WGYT:~ caroldso$ cd Downloads/  
CAROLDSO-M-WGYT:Downloads caroldso$ chmod 750 Firepower_Migration_Tool_v2.5-6263  
.command  
CAROLDSO-M-WGYT:Downloads caroldso$ ./Firepower_Migration_Tool_v2.5-6263.command  
  
[75653] PyInstaller Bootloader 3.x  
[75653] LOADER: executable is /Users/caroldso/Downloads/Firepower_Migration_Tool  
_v2.5-6263.command  
[75653] LOADER: hompath is /Users/caroldso/Downloads  
[75653] LOADER: _MEIPASS2 is NULL  
[75653] LOADER: archivename is /Users/caroldso/Downloads/Firepower_Migration_Too  
l_v2.5-6263.command  
[75653] LOADER: Cookie found at offset 0x219AE08  
[75653] LOADER: Extracting binaries  
[75653] LOADER: Executing self as child
```

```
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /inline.318b50c57b4eba3d437b.bundle.js HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:47] "GET /cui-font.880241c0aa87aa899c6a.woff2 HTTP/1.1" 200 -
2021-11-23 14:49:47,999 [INFO      | cco_login] > "EULA check for an user"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/cisco.svg HTTP/1.1" 200 -
2021-11-23 14:49:48,013 [DEBUG     | common] > "session table records count:1"
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /api/eula_check HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/icons/login.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/1.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/3.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /assets/images/2.png HTTP/1.1" 200 -
127.0.0.1 - - [23/Nov/2021 14:49:48] "GET /favicon.ico HTTP/1.1" 200 -
```

4. B.对于Windows — 双击Firepower迁移工具，在Google Chrome浏览器中启动它。

5.接受许可证，如图所示。



6.在Firepower迁移工具的登录页面上，点击使用CCO登录链接，使用您的单点登录凭证登录Cisco.com帐户。

注意：如果您没有Cisco.com帐户，请在Cisco.com登录页上创建该帐户。使用以下默认凭证登录：用户名 — 管理员密码 — 管理员123。

Redirecting

You will be redirected to the Cisco login. Please login with your CCO credentials.

Do it later

Continue

7.选择源配置。在此场景中，它是Cisco ASA(8.4+)。

← → ↻ 🏠 ⓘ localhost:8888/#/home

 Firepower Migration Tool

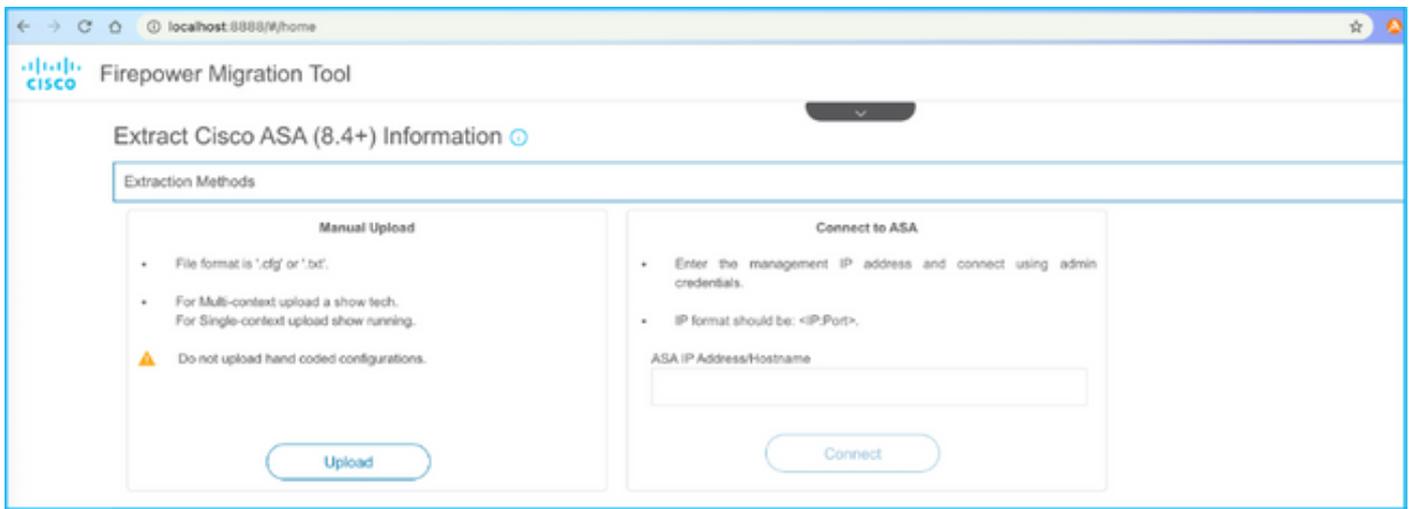
Select Source Configuration ⓘ

Source Firewall Vendor

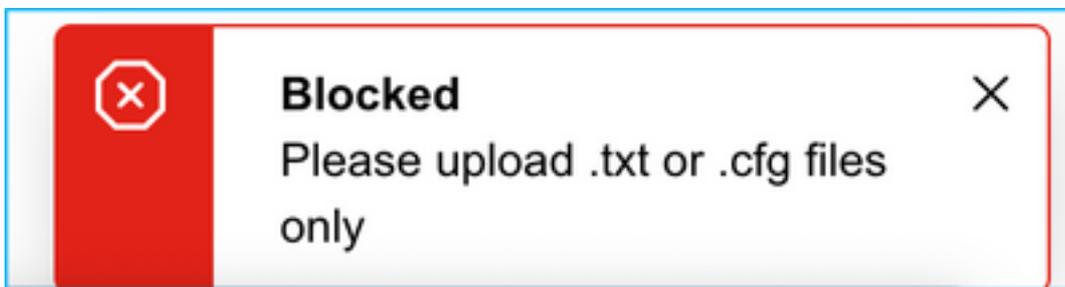
Select Source ^

- Cisco ASA (8.4+)
- Check Point (r75-r77)
- Check Point (r80)
- Palo Alto Networks (6.1+)
- Fortinet (5.0+)
- Cisco ASA (9.2.2+) with FPS

8.如果您没有与ASA的连接，请选择Manual Upload。否则，您可以从ASA检索运行配置并输入管理IP和登录详细信息。在我们的方案中，手动上传。

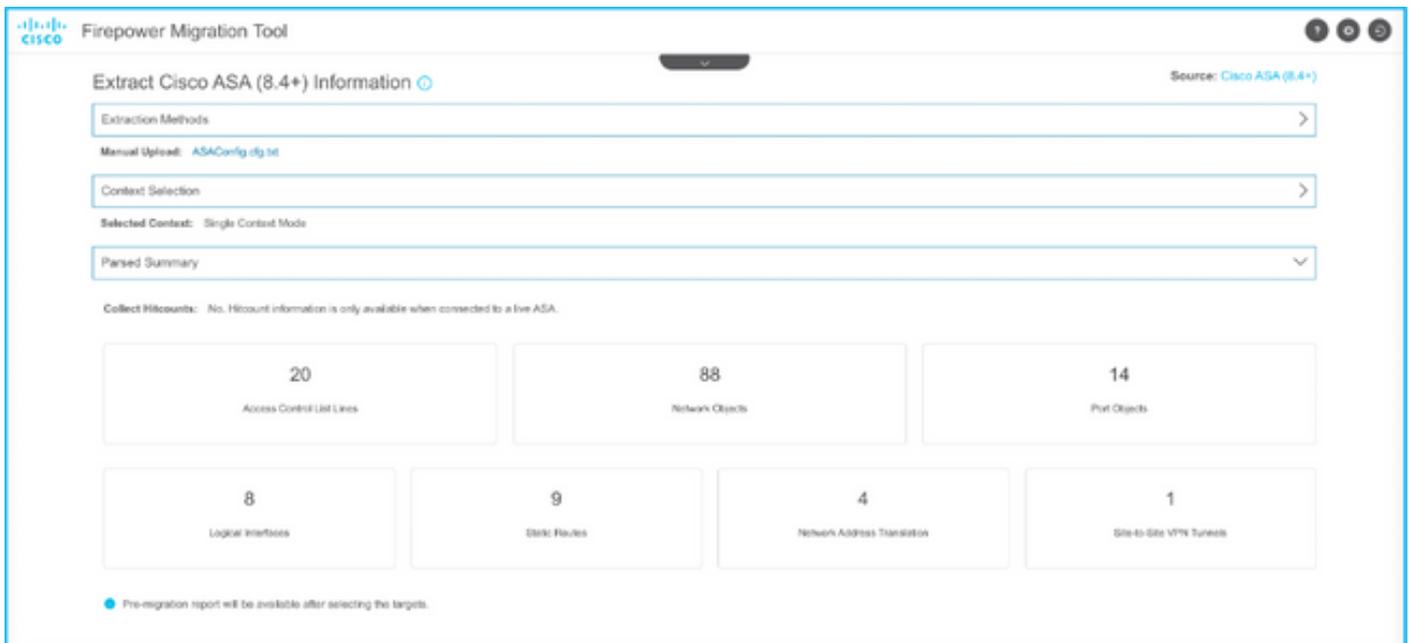


注意：如果文件不受支持，则会出现此错误。请确保将格式更改为纯文本。（尽管扩展名为.cfg，但仍会出现错误。）

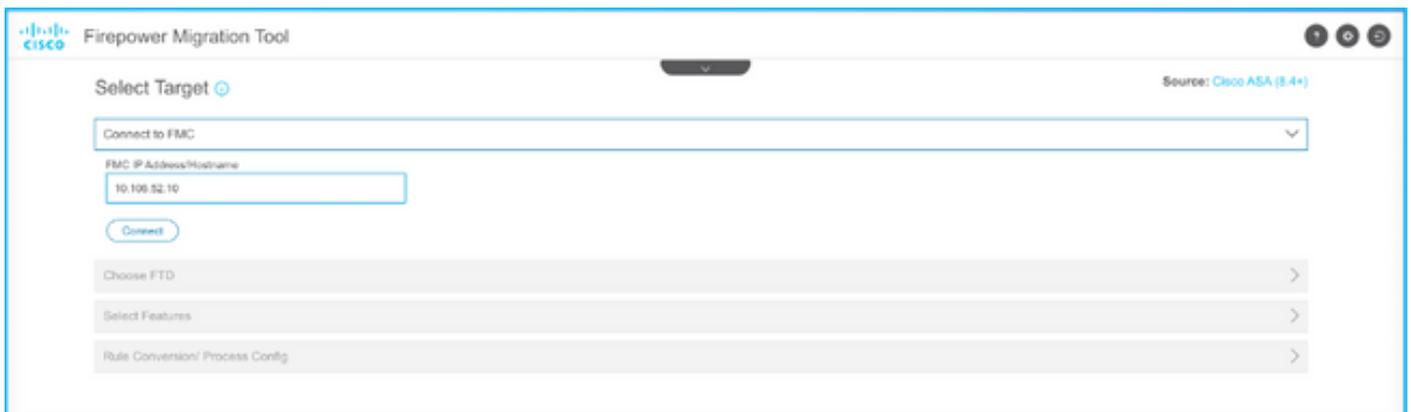


```
ASAConfig.cfg — Edited
asa# show running-config
: Saved
:
: Serial Number: FLM22160652
: Hardware: FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
:
ASA Version 9.12(2)
:
hostname asa
enable password ***** pbkdf2
:
license smart
feature tier standard
names
no mac-address auto
:
interface Ethernet1/1
no nameif
no security-level
no ip address
:
interface Ethernet1/2
nameif Inside
cts manual
security-level 0
no ip address
:
interface Ethernet1/3
nameif Outside
cts manual
security-level 0
no ip address
```

9.上传文件后，将解析元素，提供摘要，如图所示：



10. 输入ASA配置要迁移到的FMC IP和登录凭证。确保FMC IP可从您的工作站访问。



✕

FMC LOGIN

IP Address/Hostname

Username

Password

Login

11. FMC连接后，将显示其下的托管FTD。

Firepower Migration ToolSource: Cisco ASA (8.4+)

Gathering details

Select Target

Connect to FMC

FMC IP Address/Hostname

Connect

Successfully connected to FMC

Choose FTD

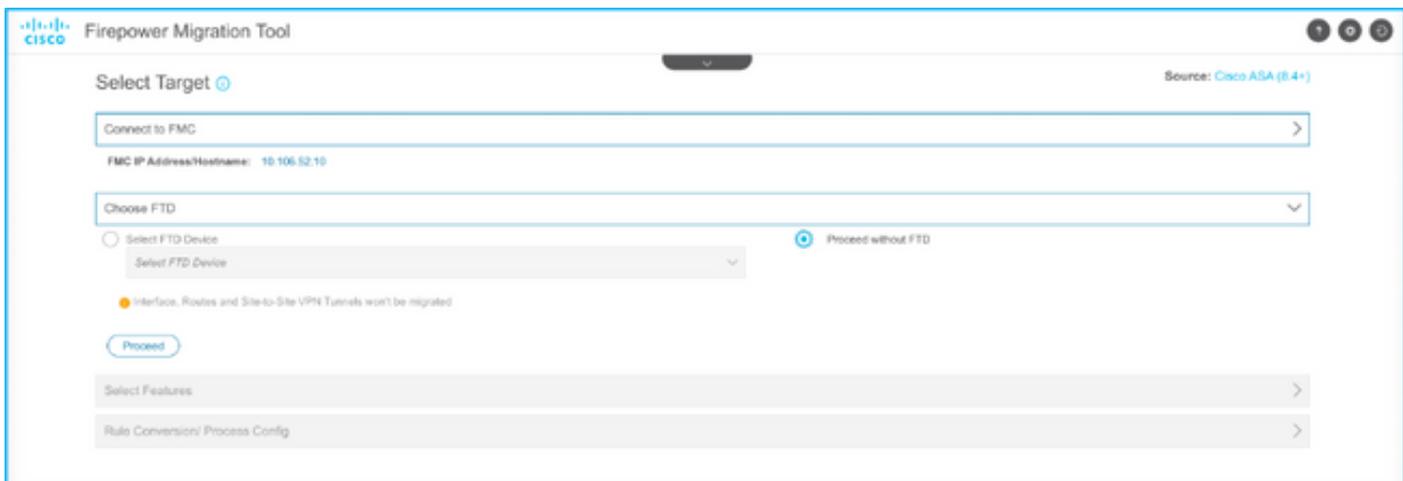
Select Features

Rule Conversion/ Process Config

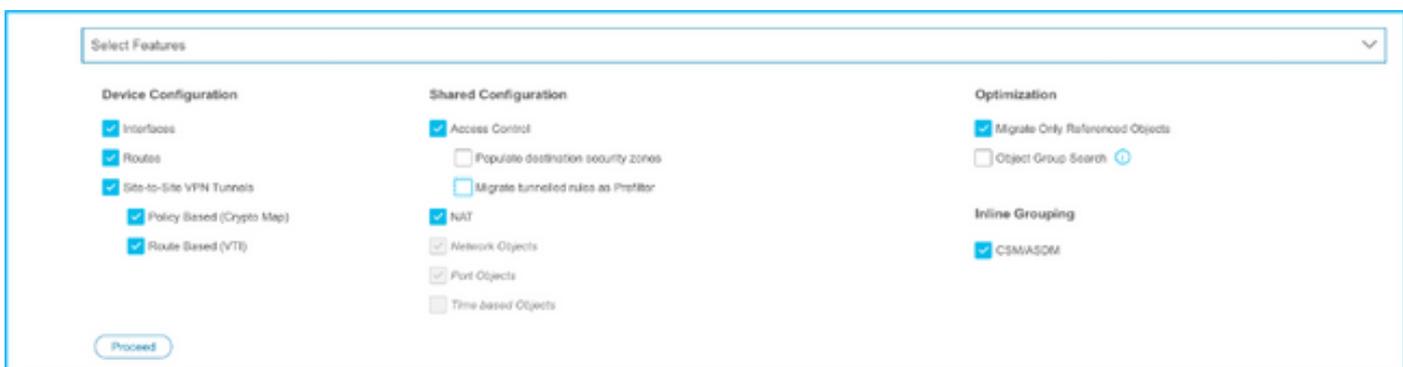
12.选择要向其执行ASA配置迁移的FTD。



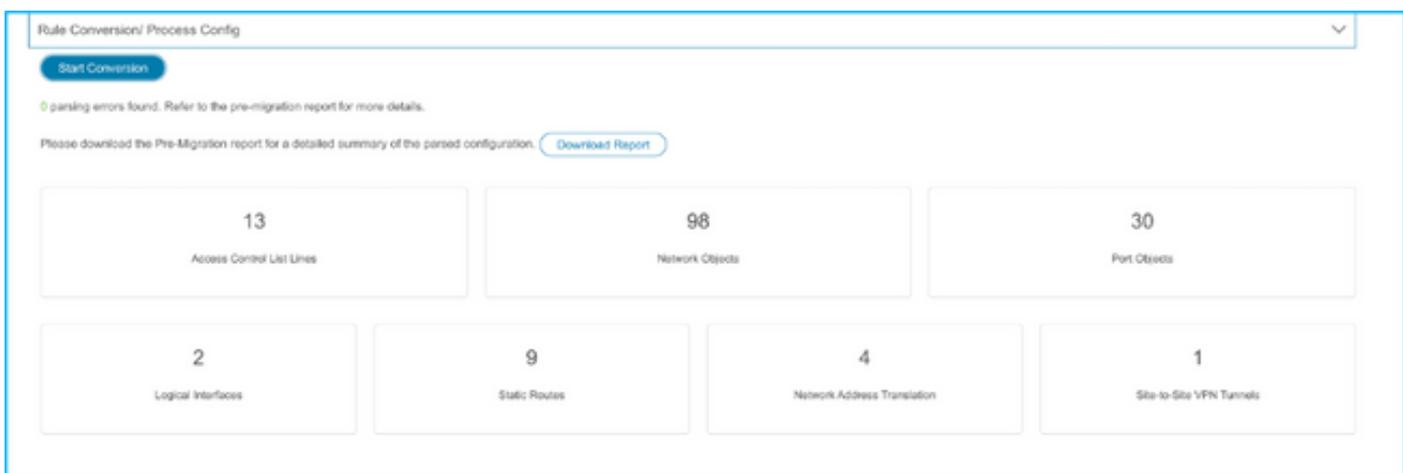
注意：建议选择FTD设备，否则接口、路由和站点到站点VPN配置必须手动完成。



13.选择需要迁移的功能，如图所示。



14.选择“开始转换”以启动预迁移，该迁移将填充与FTD配置有关的元素。



15.单击以前看到的“下载报告”，查看如图所示的迁移前报告。

The screenshot shows a web browser displaying a "Pre-Migration Report" from Cisco. The report title is "Pre-Migration Report" and the URL is "/Users/caroldso/Downloads/pre_migration_report_asa_2021-11-23_09-41-15.html". A note at the top states: "Review all contents of this pre-migration report carefully. Unsupported rules will not be migrated completely, which can potentially alter your original configuration, restrict some traffic, or permit unwanted traffic. We recommend you review the configuration by Firepower Threat Defense after the configuration is successfully migrated." The report is divided into sections, with the first being "1. Overall Summary:". Below this, a summary text reads: "A summary of the supported ASA configuration elements that can be successfully migrated to Firepower Threat Defense." A table follows, listing various configuration elements and their counts. The table has two columns: the element name and its count. The elements listed are: Collection Method (Manual), ASA Configuration Name (ASAConfig.cfg.txt), ASA Version (9.12(2)), ASA Hostname (asa), ASA Device Model (FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)), Hit Count Feature (No), IP SLA Monitor (0), Total Extended ACEs (13), ACEs Migratable (13), Site to Site VPN Tunnels (1), Logical Interfaces (2), Network Objects and Groups (98), Service Objects and Groups (30), Static Routes (9), and NAT Rules (4). A note at the bottom of the table states: "Note: ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored."

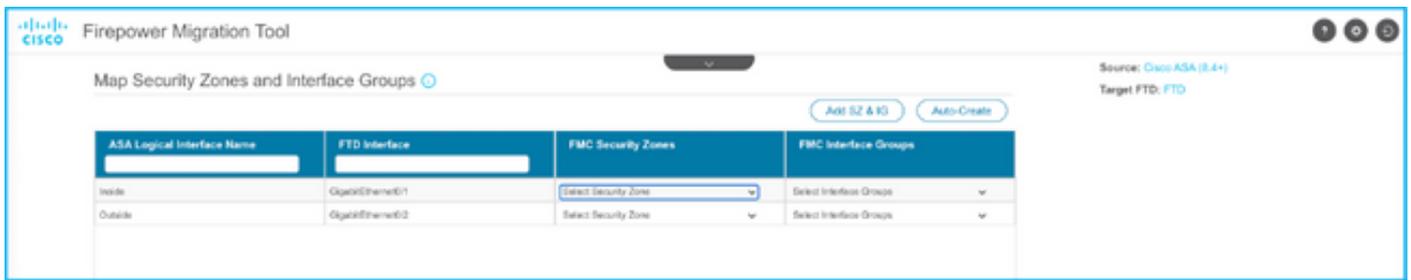
Collection Method	Manual
ASA Configuration Name	ASAConfig.cfg.txt
ASA Version	9.12(2)
ASA Hostname	asa
ASA Device Model	FPR4K-SM-12, 56533 MB RAM, CPU Xeon E5 series 2200 MHz, 1 CPU (24 cores)
Hit Count Feature	No
IP SLA Monitor	0
Total Extended ACEs	13
ACEs Migratable	13
Site to Site VPN Tunnels	1
Logical Interfaces	2
Network Objects and Groups	98
Service Objects and Groups	30
Static Routes	9
NAT Rules	4

Note: ACEs that are applied outbound or not attached to interfaces using the access-group command are ignored.

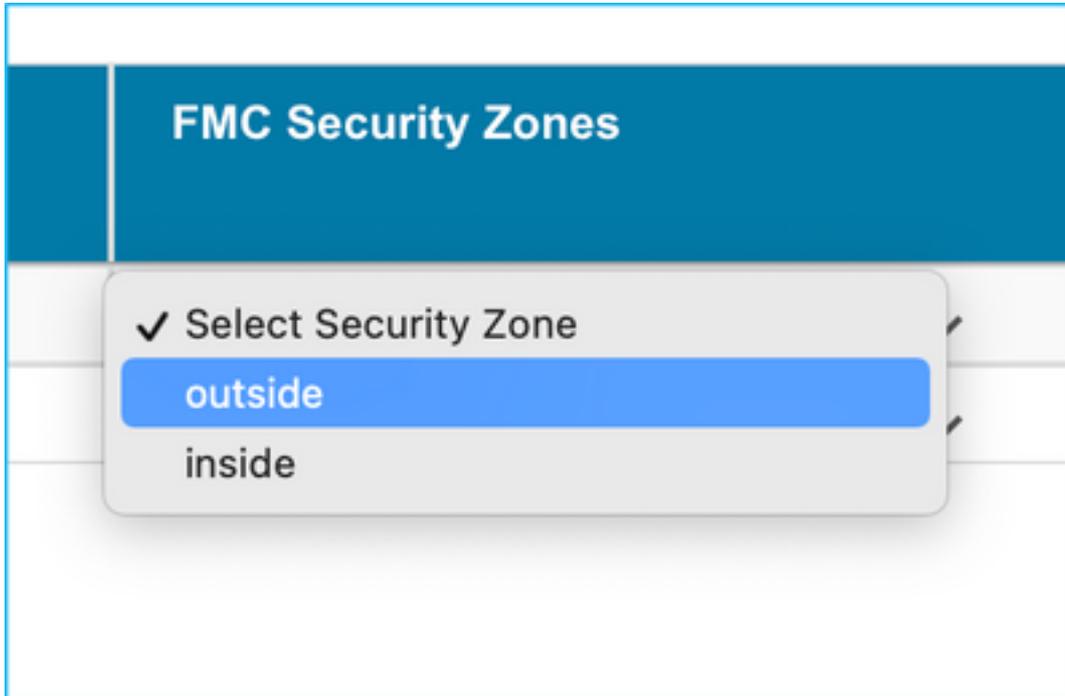
16.根据需要将ASA接口映射到FTD接口，如图所示。

The screenshot shows a configuration interface with a "Refresh" button in the top right corner. The interface is divided into two main sections: "ASA Interface Name" and "FTD Interface Name". Under "ASA Interface Name", there are two entries: "Ethernet1/2" and "Ethernet1/3". Under "FTD Interface Name", there is a dropdown menu with the following options: "Select Interface", "GigabitEthernet0/0", "GigabitEthernet0/1", and "GigabitEthernet0/2". The "GigabitEthernet0/2" option is selected, indicated by a checkmark and a blue highlight.

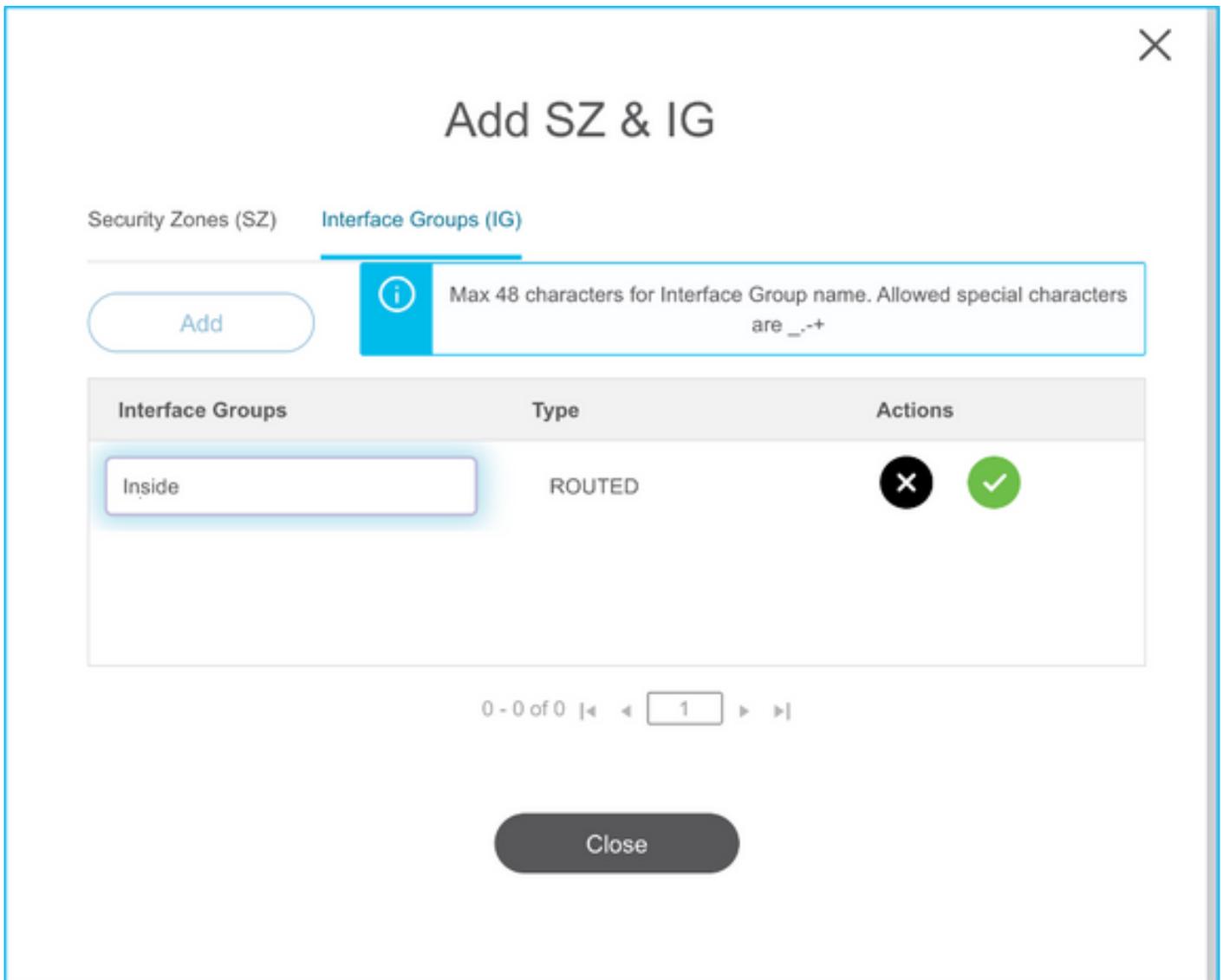
17.为FTD接口分配安全区域和接口组。



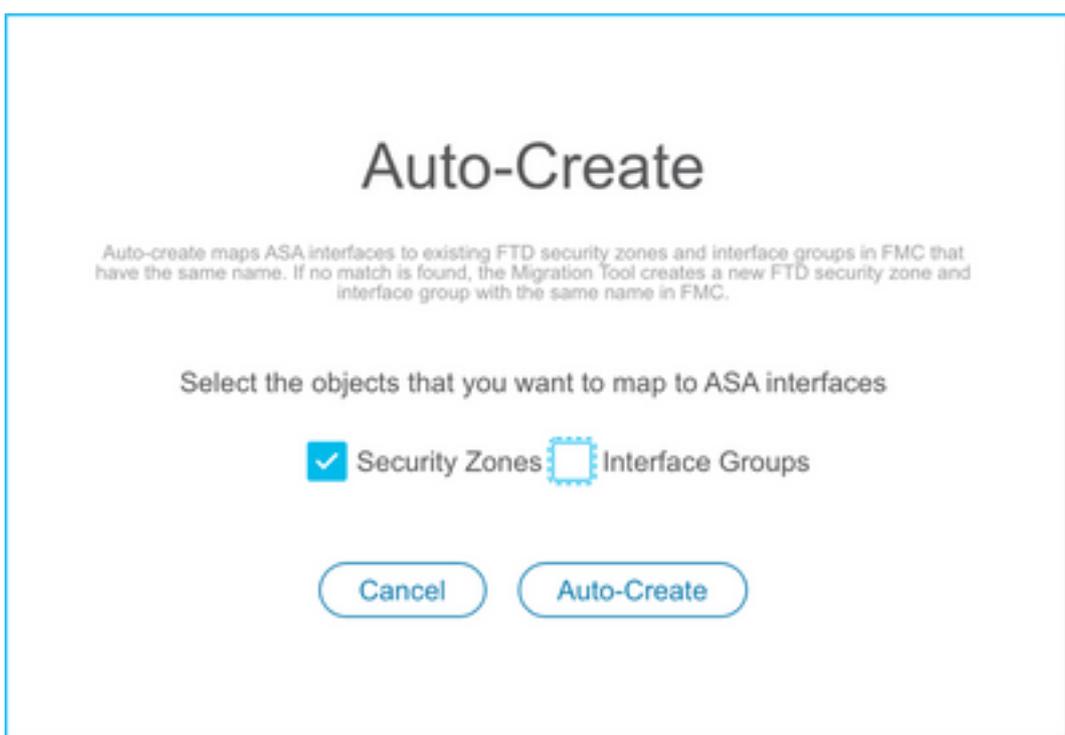
答：如果FMC已创建安全区域和接口组，您可以根据需要选择它们：

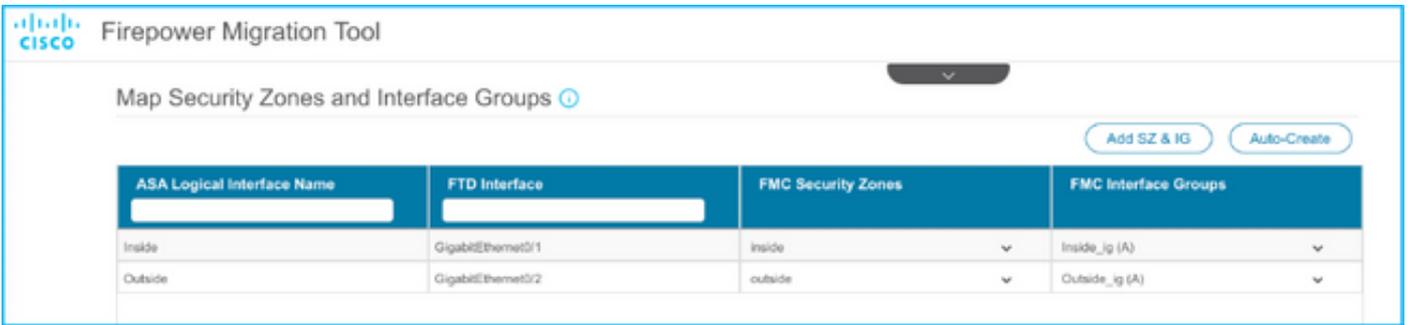


B.如果需要创建安全区域和接口组，请单击“添加SZ和IG”，如图所示。

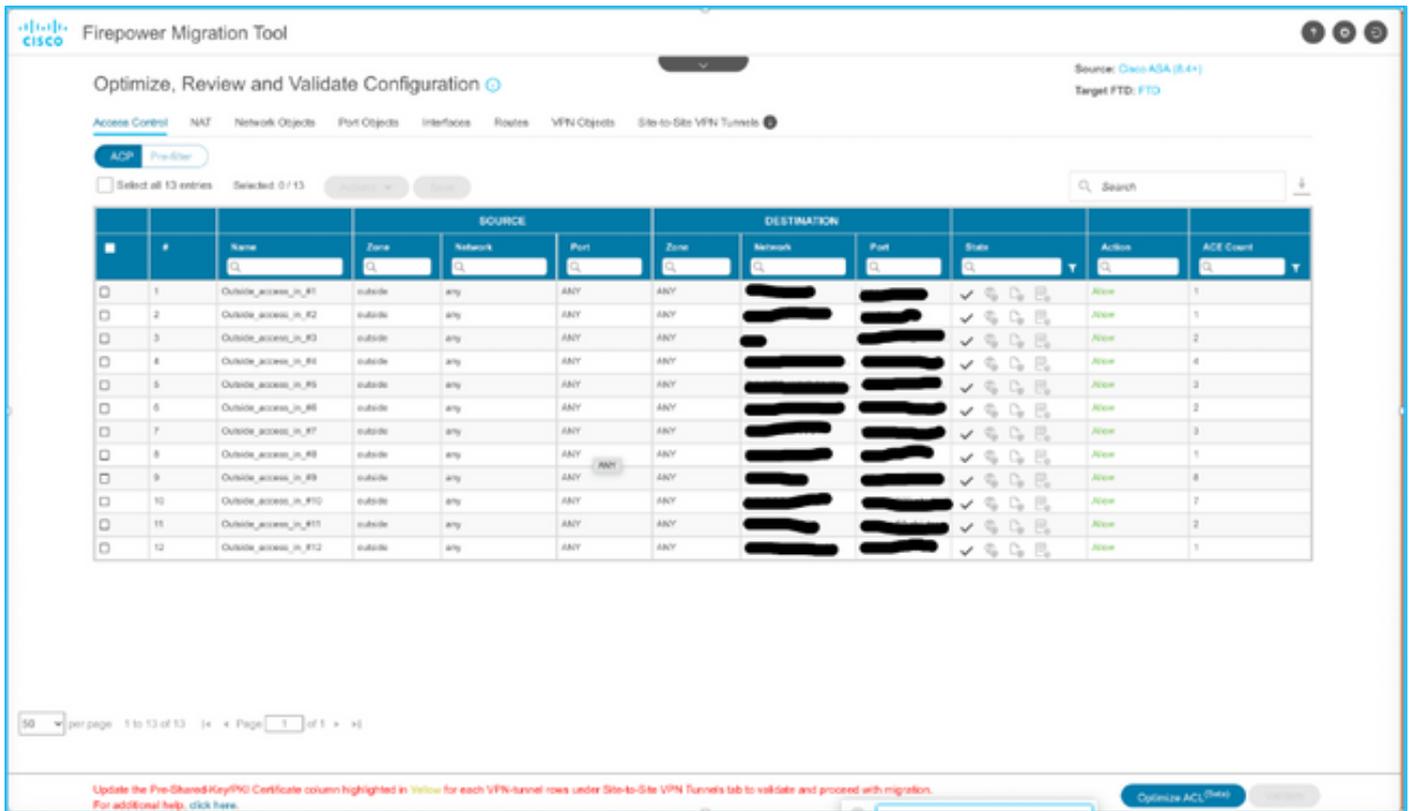


C. 否则，可以选择**Auto-Create**选项，该选项将分别创建名为**ASA逻辑接口_sz**和**ASA逻辑接口_ig**的安全区域和接口组。





18. 复查并验证创建的每个FTD元素。警报显示为红色，如图所示。



19. 如果要编辑任何规则，可以选择如图所示的迁移操作。添加文件和IPS策略的FTD功能可以在此步骤中完成。

ACP Pre-filter

Select all 13 entries Selected: 13 / 13 Actions Save

			MIGRATION ACTIONS	SOURCE
<input checked="" type="checkbox"/>	#	Name		
<input checked="" type="checkbox"/>	1	Outside_access_in_#1	Do not migrate	network
<input checked="" type="checkbox"/>	2	Outside_access_in_#2		
<input checked="" type="checkbox"/>	3	Outside_access_in_#3		
<input checked="" type="checkbox"/>	4	Outside_access_in_#4		
<input checked="" type="checkbox"/>	5	Outside_access_in_#5		
<input checked="" type="checkbox"/>	6	Outside_access_in_#6	outside	any

注意：如果FMC中已存在文件策略，则会按照图中所示填充它们。IPS策略和默认策略也适用。

✕

File Policy

Select File Policy *

eicar

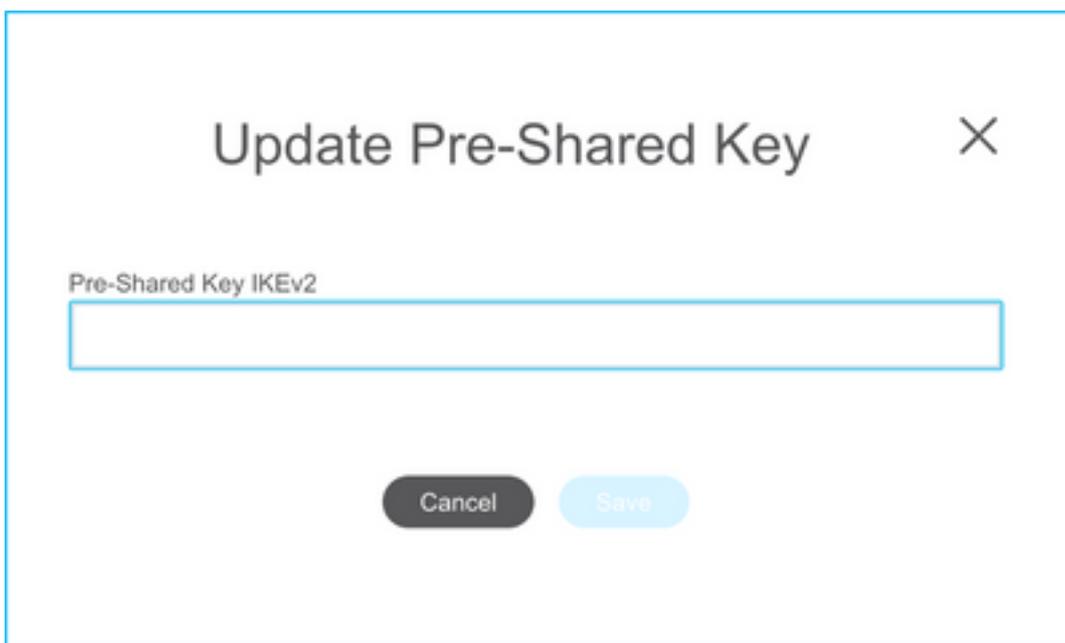
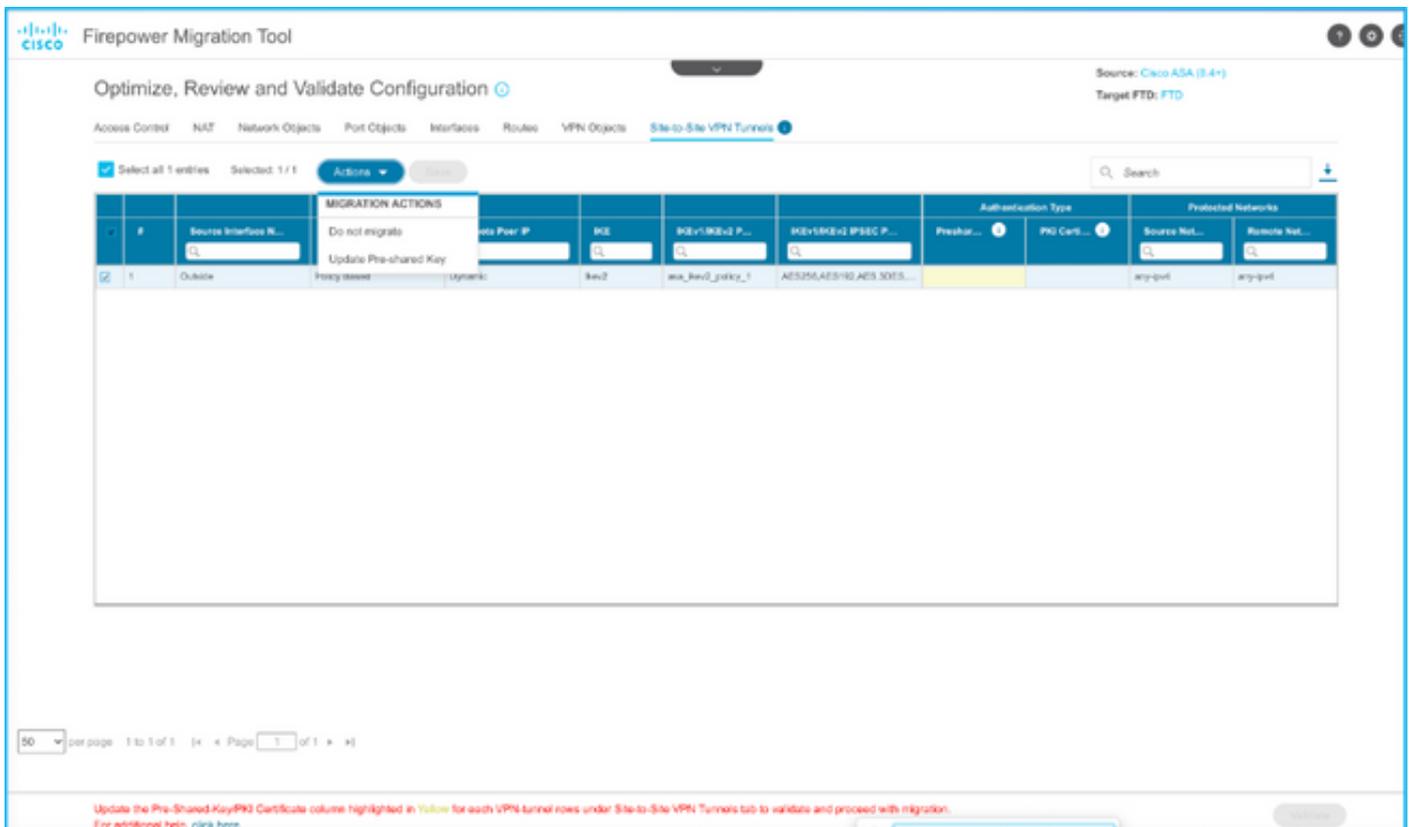
None

Cancel
Select

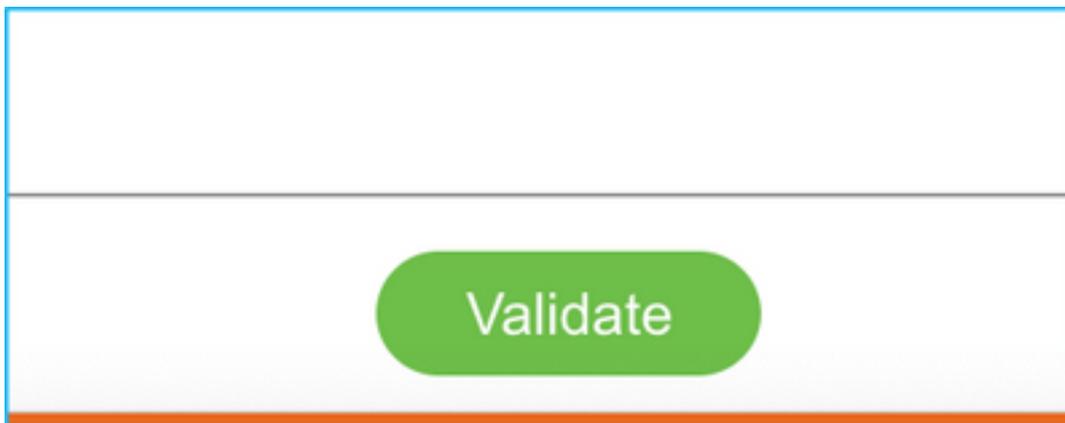
可以为所需规则完成日志配置。在此阶段，可以选择FMC上现有的系统日志服务器配置。

20.同样，您的配置中的NAT、网络对象、端口对象、接口、路由、VPN对象、站点到站点VPN隧道和其他元素也可以逐步查看。

注意：警报将通知如图所示更新预共享密钥，因为预共享密钥不会在ASA配置文件中复制。选择操作>更新预共享密钥以输入值。



21.最后，单击屏幕右下角的验证图标，如图所示。



22.验证成功后，单击“推送配置”，如图所示。

Validation Status

Successfully Validated

Validation Summary (Pre-push)

13 Access Control List Lines	37 Network Objects	14 Port Objects	
2 Logical Interfaces	9 Static Routes	4 Network Address Translation	1 Site-to-Site VPN Tunnels

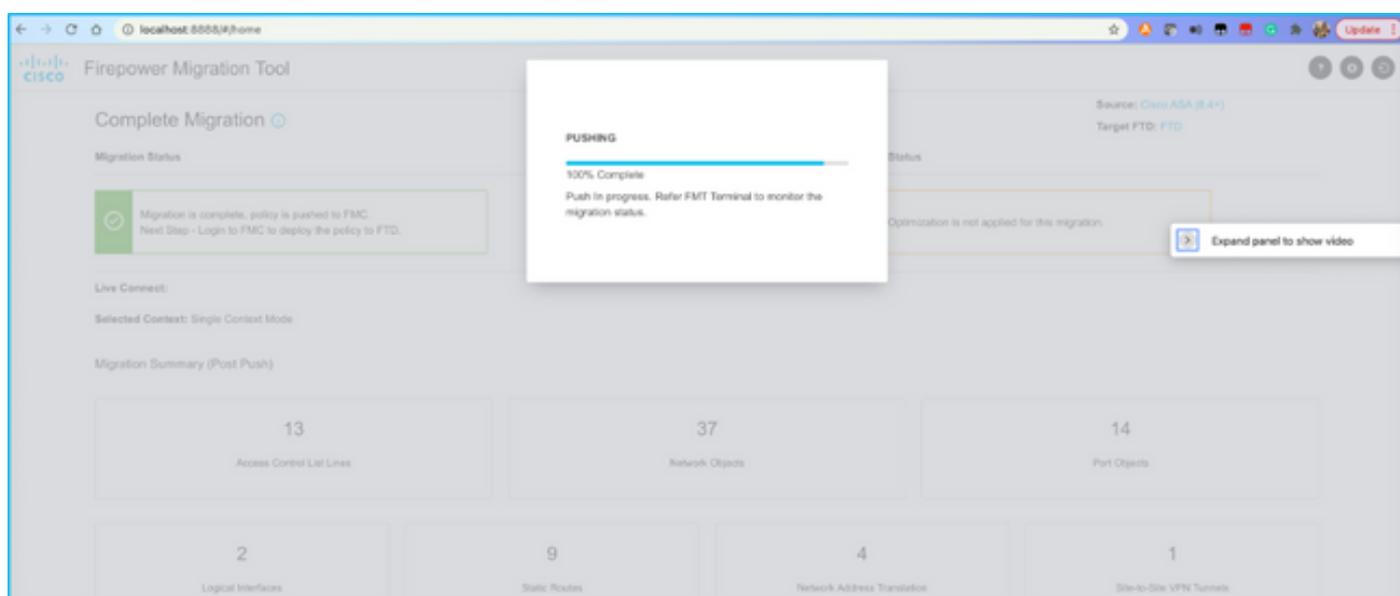
Note: The configuration on the target FTD device FTD (10.106.52.20) will be overwritten as part of this migration.

Push Configuration

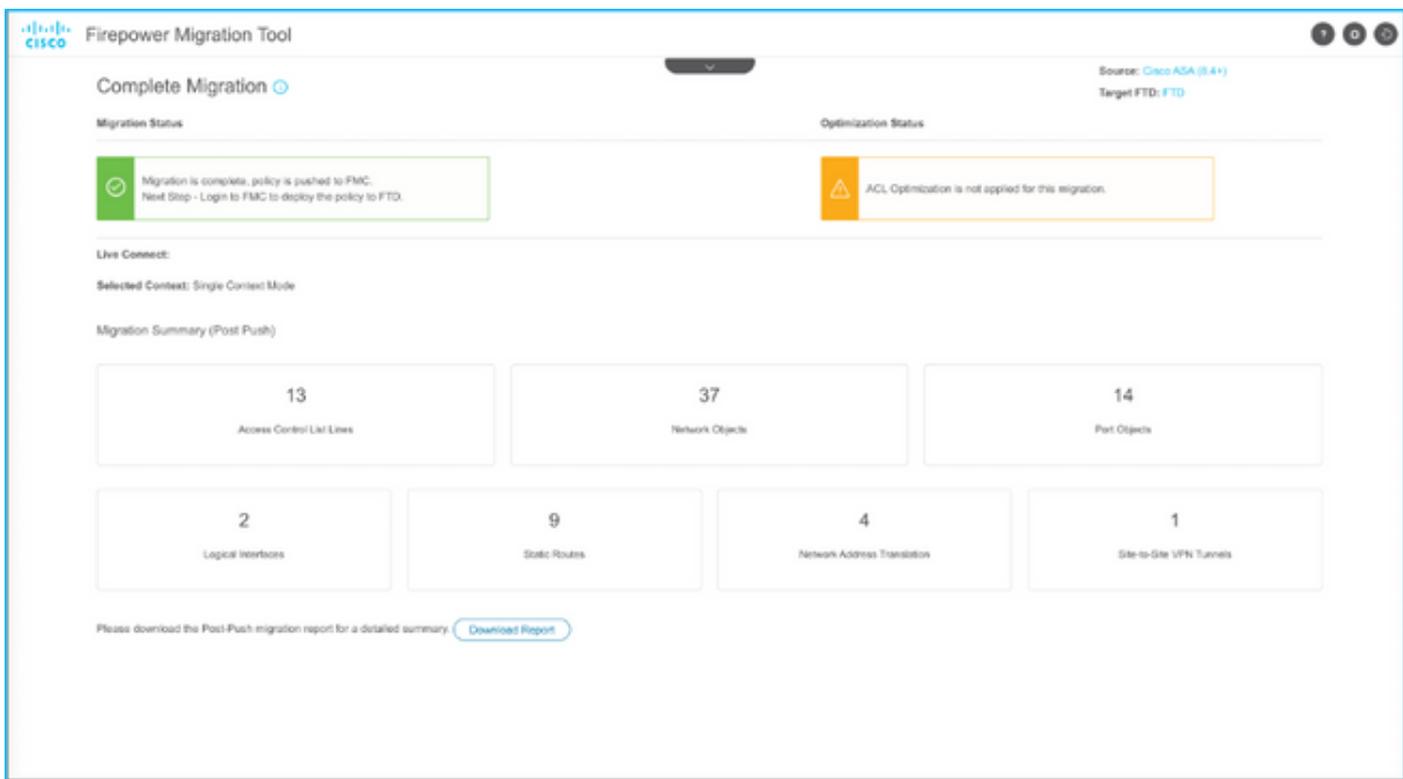
PUSHING

0% Complete

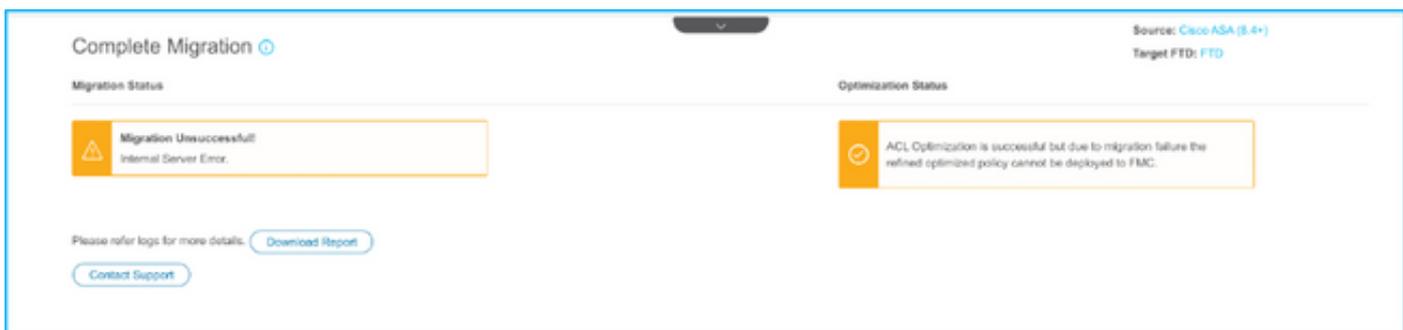
Push In progress. Refer FMT Terminal to monitor the migration status.



23. 迁移成功后，将显示的消息将显示在图中。



注意：如果迁移失败，请单击**Download Report**以查看迁移后报告。

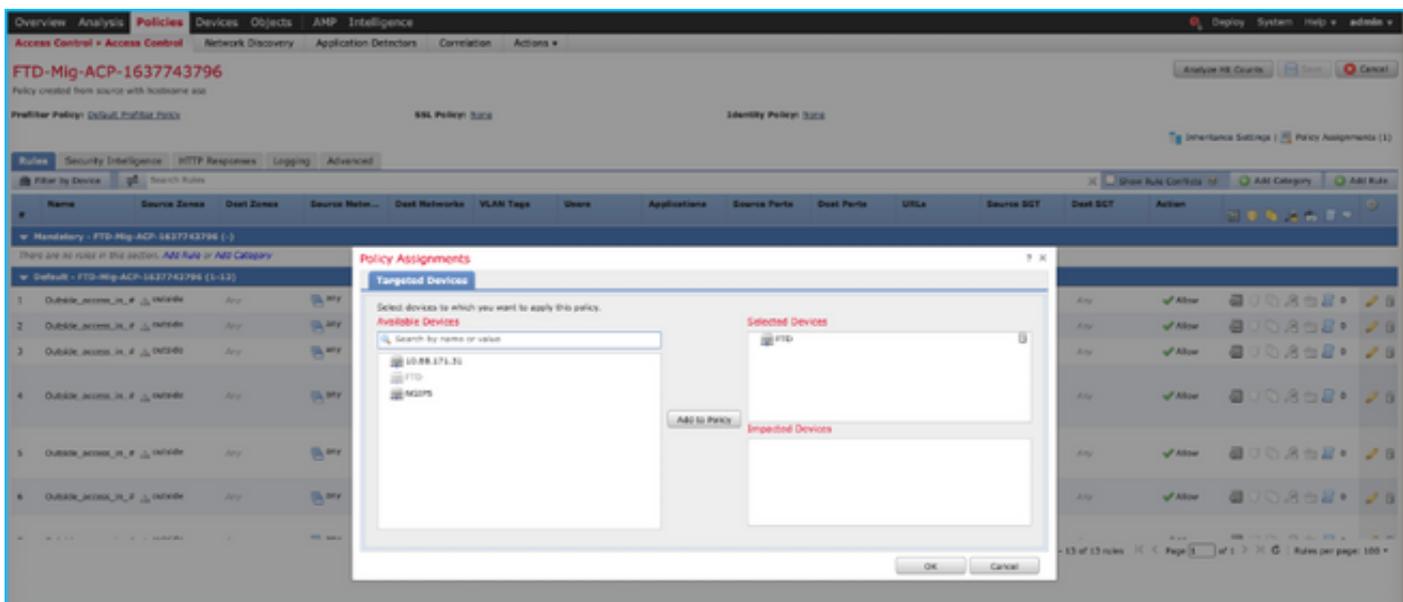


验证

使用本部分可确认配置能否正常运行。

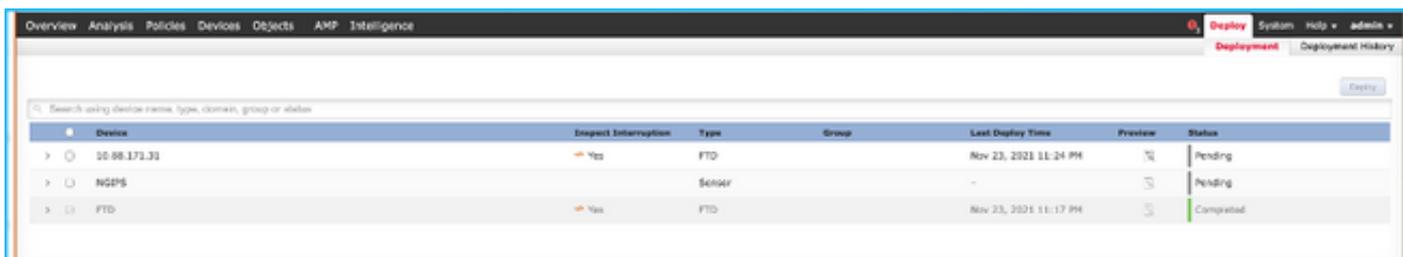
验证FMC。

1. 导航至**策略>访问控制>访问控制策略>策略分配**，以确认已填充选定的FTD。



注意：迁移访问控制策略的名称应具有前缀FTD-Mig-ACP。如果步骤2.8中未选择FTD，则需要要在FMC上选择FTD。

2.将策略推送到FTD。导航至**部署>部署> FTD名称>部署**，如图所示。



与Firepower迁移工具相关的已知错误

- Cisco Bug ID [CSCwa56374](#) - FMT工具挂起区域映射页，错误为内存使用率高
- Cisco Bug ID [CSCvz88730](#) - FTD端口通道管理接口类型的接口推送失败
- Cisco Bug ID [CSCvx21986](#) — 端口通道迁移到目标平台 — 不支持虚拟FTD
- Cisco Bug ID [CSCvy63003](#) — 如果FTD已是集群的一部分，迁移工具应禁用接口功能
- Cisco Bug ID [CSCvx08199](#) — 当应用引用超过50时，ACL需要拆分

相关信息

- [使用防火墙迁移工具将ASA防火墙迁移到威胁防御](#)
- [技术支持和文档 - Cisco Systems](#)