无缝过渡：从Palo Alto防火墙迁移到Cisco FTD

目录

简介

本文档介绍通过使用FMT 6.0版从Palo Alto防火墙过渡到Cisco FTD系统的过程。

先决条件

要求

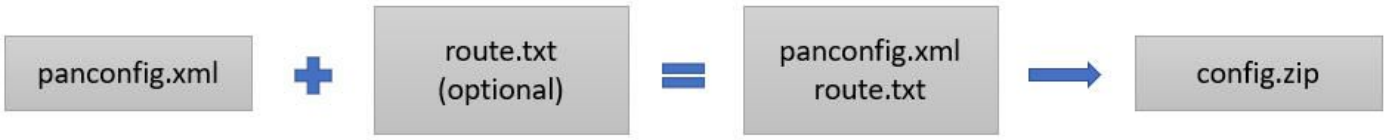
Cisco 建议您了解以下主题：

- 以XML格式(*.xml)从Palo Alto防火墙导出当前运行配置。
- 访问Palo Alto防火墙CLI并执行show routing route命令，然后将输出保存为文本文件(*.txt)。
- 将配置文件(*.xml)和路由输出文件(*.txt)压缩到单个ZIP存档(*.zip)。

使用的组件

本文档中的信息基于Palo Alto Firewall 8.4.x或更高版本。

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。



Firepower迁移工具(FMT)

FMT可帮助工程团队从任何现有供应商防火墙过渡到思科下一代防火墙(NGFW)/Firepower威胁防御(FTD)。 确保运行从思科网站下载的最新版本的FMT。

迁移指南

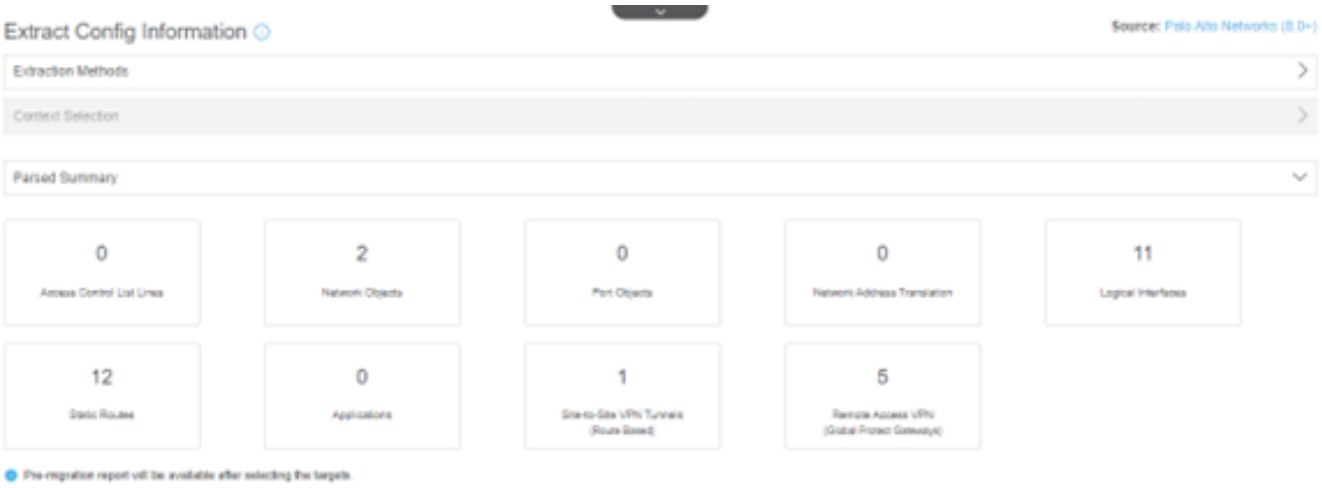
1.迁移前检查表

- 在开始迁移过程之前，确保FTD已添加到FMC。
- 已在FMC上创建具有管理权限的新用户帐户。
- 导出的Palo Alto运行配置文件.xml必须使用.zip的扩展名进行压缩。
- NGFW/FTD的物理或子接口或端口通道的数量必须与Palo Alto防火墙接口相同。

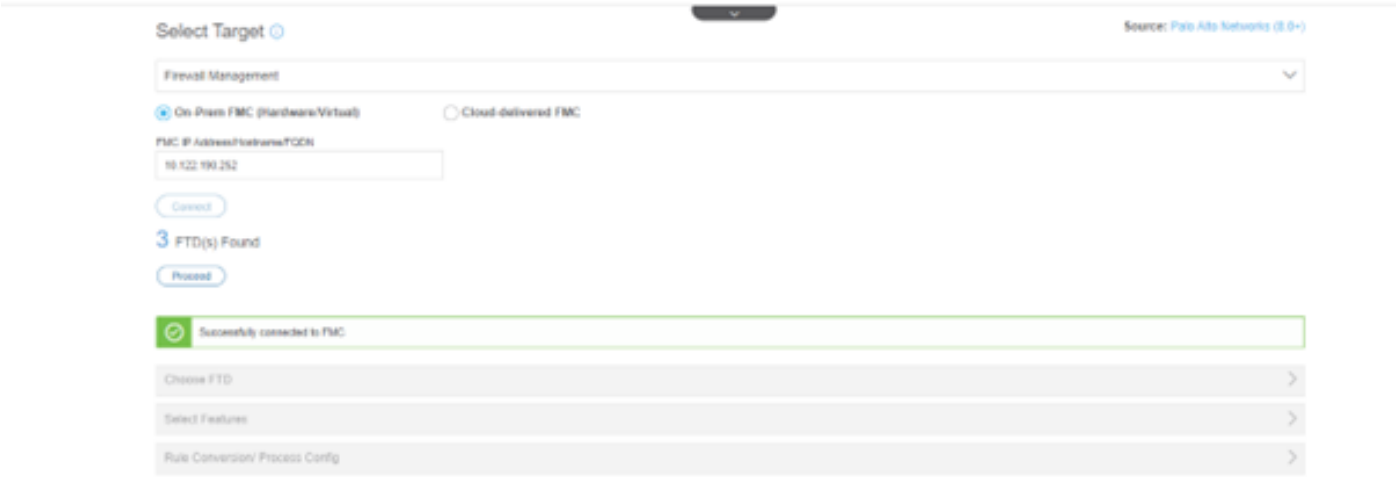
2.迁移工具使用情况

- 下载FMT工具.exe并以管理员身份运行。
- FMT需要CEC ID或思科用户帐户才能登录。
- 成功登录后，该工具将显示一个控制面板，您可以在其中选择防火墙供应商并上传相应的*.zip文件；请参阅下一张图片。

- 在继续迁移之前，请仔细查看右侧提供的说明。
- 准备开始后，单击Start Migration。
- 上传包含Palo Alto防火墙的配置设置的已保存的*.zip文件。
- 上传配置文件后，您将能够看到内容的Parsed Summary并点击next；请参阅下一个映像。



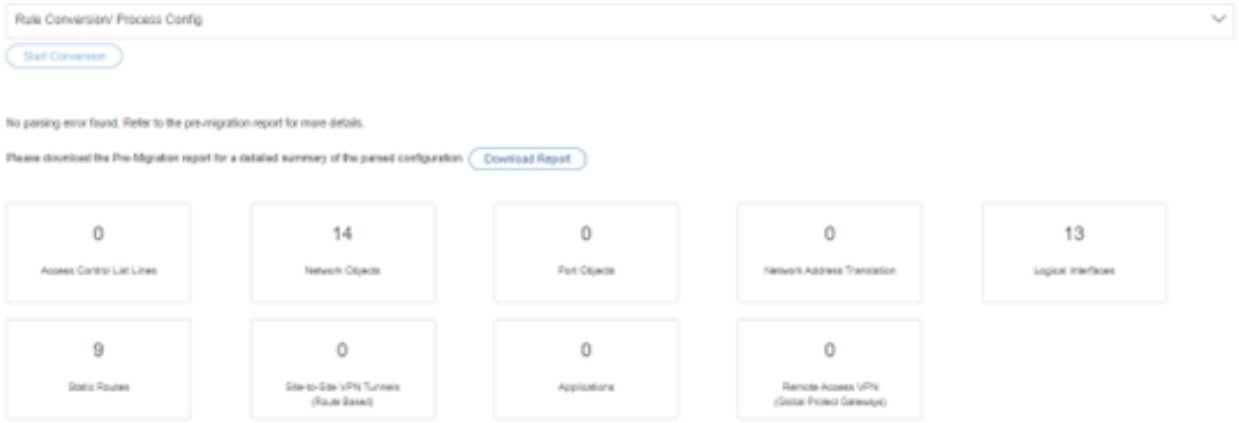
- 输入FMC的IP地址并登录。
- 该工具将搜索已向FMC注册的活动FTD。
- 选择要迁移的FTD，然后单击Proceed，如下图所示。



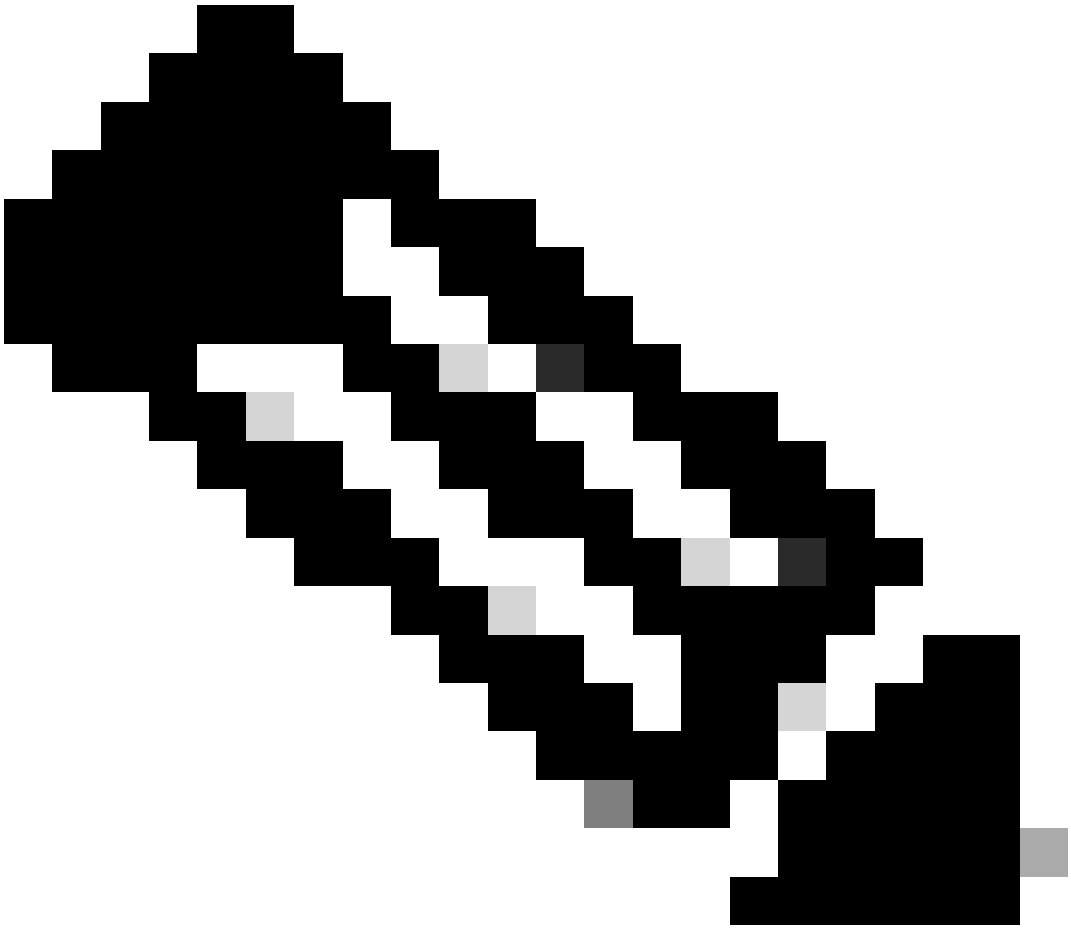
- 选择特定功能，以便根据客户要求进行迁移。请注意，与FTD相比，Palo Alto防火墙具有不同的功能集。
- 单击Proceed并查阅下一张图像以供参考。

- FMT将根据您的选择执行转换。查看“Pre-Migration Report”（迁移前报告）中的更改，然后单

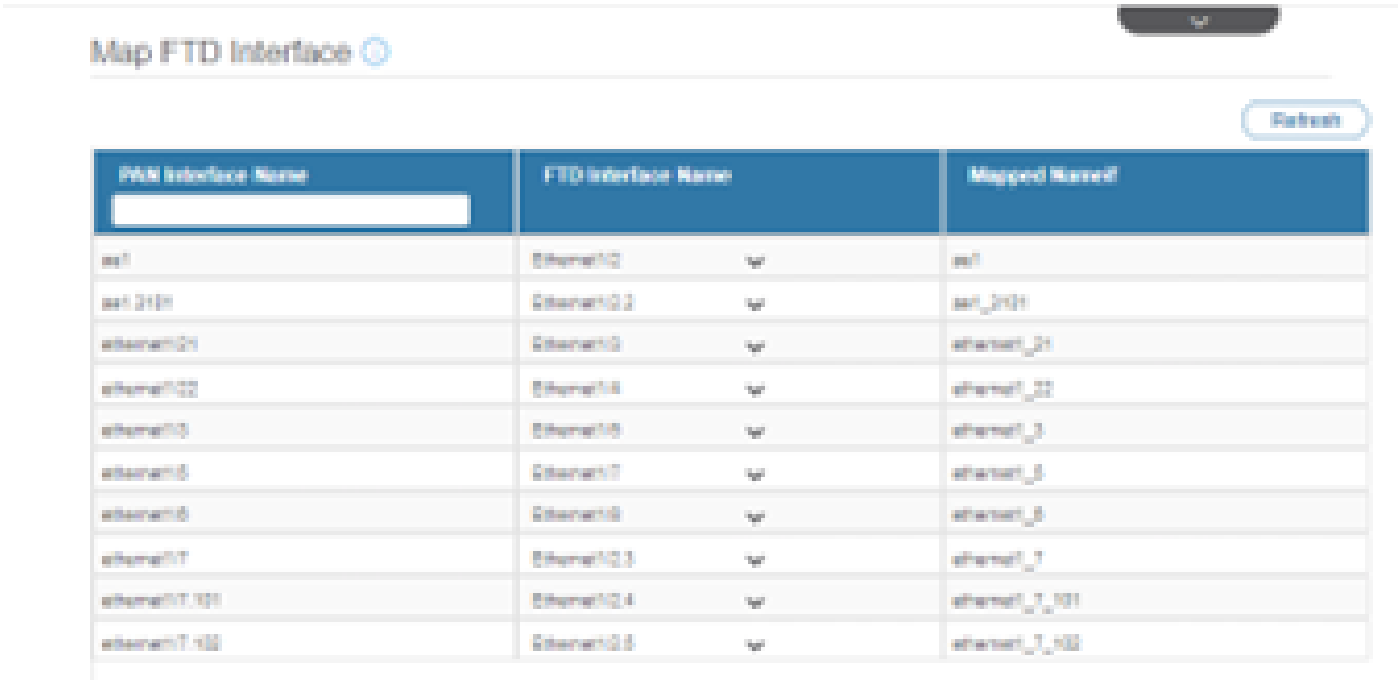
击Proceed。请参阅下一张图片以获取指导。



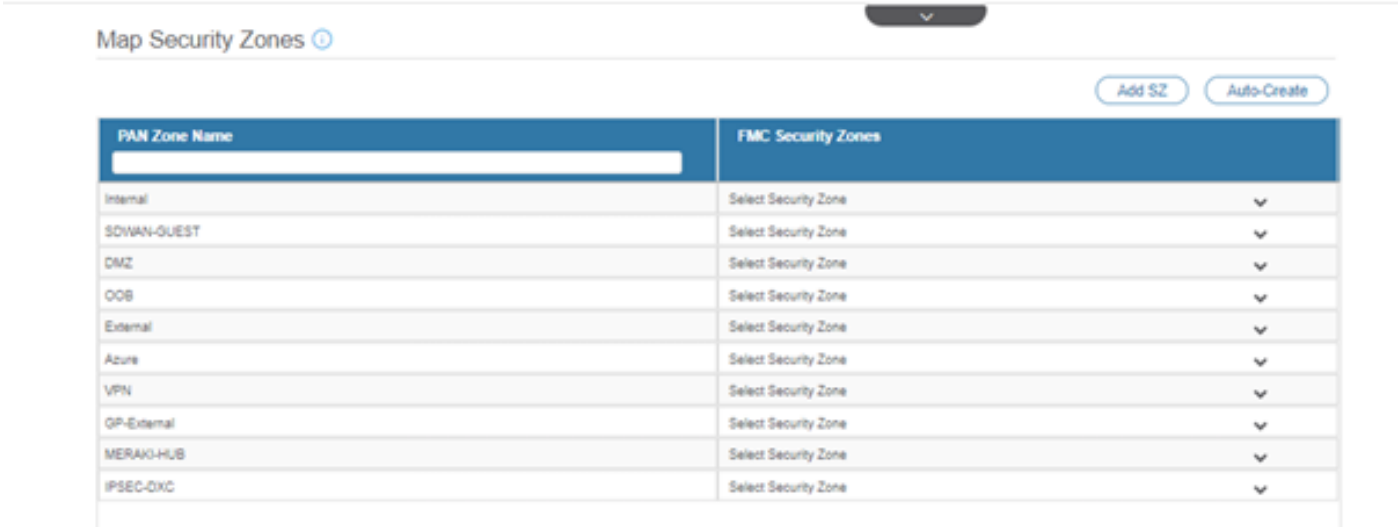
- 将接口从Palo Alto防火墙映射到FTD上的接口。有关详细信息，请参阅下一张图片。



注意：NGFW/FTD的物理或子接口数量或端口通道数量必须等于Palo Alto防火墙接口（包括子接口）。



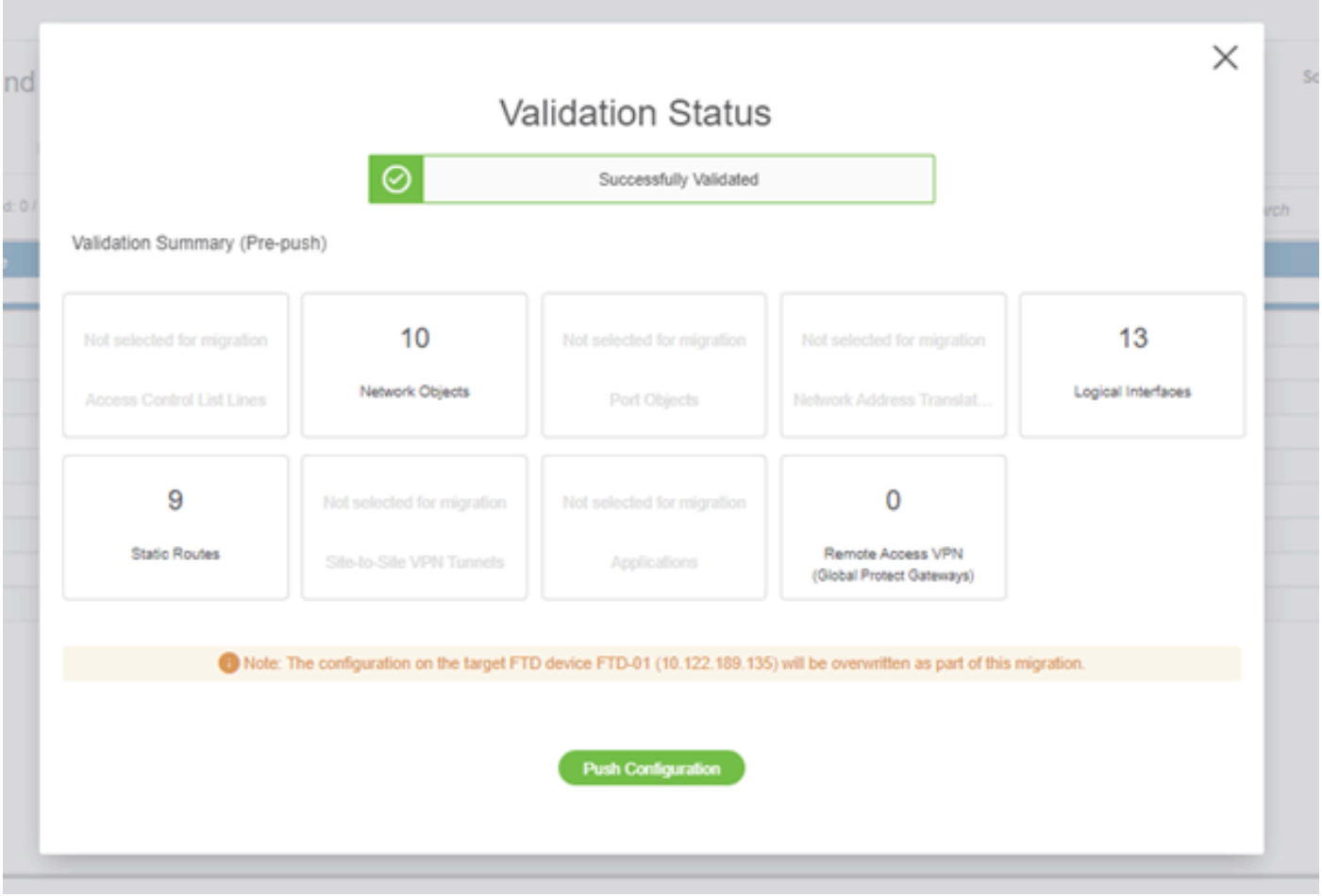
- 确定Zones的映射，可以手动完成，也可以使用Auto-create功能完成。有关可视化，请参阅下一张图片。



- 分配应用阻止配置文件。由于这是没有应用映射的实验设备，您可以继续使用默认设置。单击Next，并参阅提供的图像。

- 根据需要优化ACL、对象、接口和路由。由于这是具有最少配置的实验设置，您可以继续使用默认选项。然后单击Validate，引用下一个映像。

- 成功验证后，配置即可部署到目标FTD。有关进一步的说明，请参见下一个图像。



- 推送配置将在FMC中保存已迁移的配置，并将自动部署到FTD。
- 如果迁移过程中出现任何问题，请随时打开TAC案例以寻求进一步帮助。

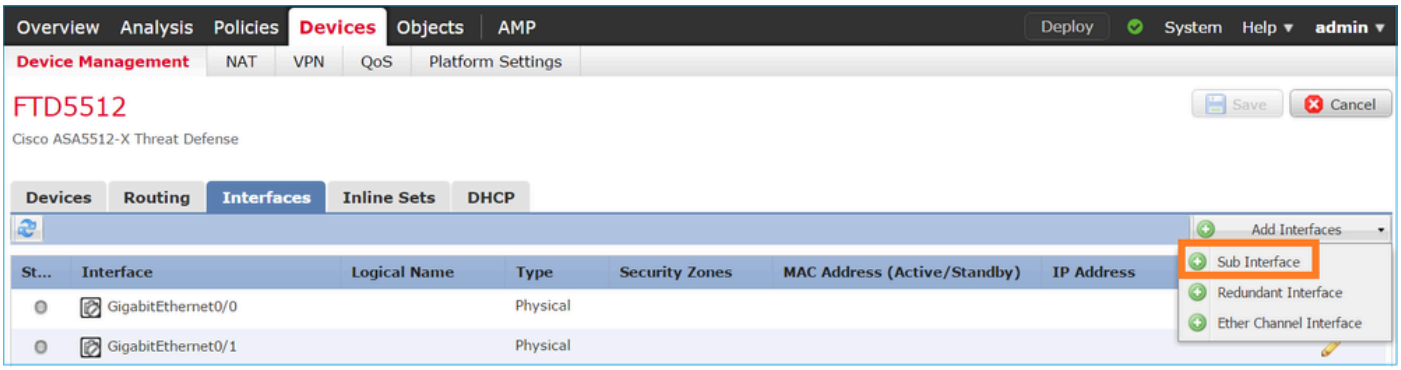
3.迁移后验证

- 验证FTD和FMC上的配置。
- 测试设备ACL、策略、连接和其他高级功能。
- 在执行任何更改之前创建回退点。
- 在生产环境中投入使用之前，先在实验室环境中测试迁移。

已知问题

1. FTD上缺少接口

- 登录Palo Alto CLI并执行show interface all。您必须拥有等于或大于FTD中的接口数。
- 通过FMC GUI创建相同或更多的接口 — 子接口、端口通道或物理接口。
- 导航到FMC GUI Device > Device Management，点击要在其中创建所需接口的FTD。在Interface部分下，从右角下拉菜单中选择Create Sub-interface/BVI，然后创建接口并关联相应的接口。保存配置并同步到设备。



- 通过执行Show interface ip brief检查接口是否在FTD上创建，并继续迁移接口映射。

2.路由表

- 通过执行Show routing route或Show routing route summary检验Palo Alto防火墙上的路由表。
- 在将路由迁移到FTD之前，请验证该表，并根据项目需要选择所需的路由。
- 在FTD中通过Show route all和show route summary验证相同的路由表。

3.优化

- “优化对象”(Optimizing objects)面板显示为灰色，有时您必须在FMC中创建手动对象并将其映射。要在FTD中查看对象，请使用Show Running |在对象和Palo Alto中，使用Show address <object name>。
- 应用迁移需要在迁移之前对Palo Alto防火墙进行审计，FTD具有专用的IPS设备，或者您可以在FTD中启用此功能，以便您根据客户要求规划应用迁移任务。
- Palo Alto防火墙的NAT配置必须通过show running nat-policy进行验证，并且您必须在FTD中具有自定义NAT策略，可以在FTD中通过Show Running nat进行查看。

结论

在FMT的帮助下，Palo Alto防火墙已成功迁移至思科FTD。在FTD上迁移后发生任何问题，为了排除故障，请进一步打开TAC案例。

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）。