# 使用FMT将Paloalto迁移到Firepower威胁防御

## 目录



## 简介

本文档介绍将Paloalto防火墙迁移到Cisco Firepower威胁设备的过程。

### 先决条件

### 要求

Cisco 建议您了解以下主题：

- Firepower迁移工具
- Paloalto防火墙
- 安全防火墙威胁防御(FTD)
- 思科安全防火墙管理中心(FMC)

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带Firepower迁移工具(FMT)v7.7的Mac OS
- PAN NGFW版本8.0+
- 安全防火墙管理中心(FMCv)v7.6
- 安全防火墙威胁防御版本7.4.2

免责声明：本文档中引用的网络和IP地址未与任何单个用户、组或组织关联。此配置专为实验环境而创建。

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。

### 概述

本文档的具体要求包括：

- PAN NGFW版本8.4+或更高版本
- 安全防火墙管理中心(FMCv)版本6.2.3或更高版本

防火墙迁移工具支持以下设备列表：

- 思科ASA(8.4+)
- 带FPS的Cisco ASA(9.2.2+)
- 思科安全防火墙设备管理器(7.2+)
- 检查点(r75-r77)
- 检查点(r80-r81)
- Fortinet(5.0+)
- Palo Alto Networks(8.0+)

## 背景信息

在迁移Paloalto防火墙配置之前，请执行以下活动：

获取Paloalto防火墙配置zip文件

- Paloalto防火墙的版本必须为8.4+。
- 从Palo Alto防火墙导出当前运行配置（*.xml必须采用xml格式）。
- 登录到Paloalto Firewall Cli以执行show routing route并以txt格式(*.txt)保存输出。
- 压缩扩展名为*.zip的运行配置文件(*.xml)和路由文件(*.txt)。

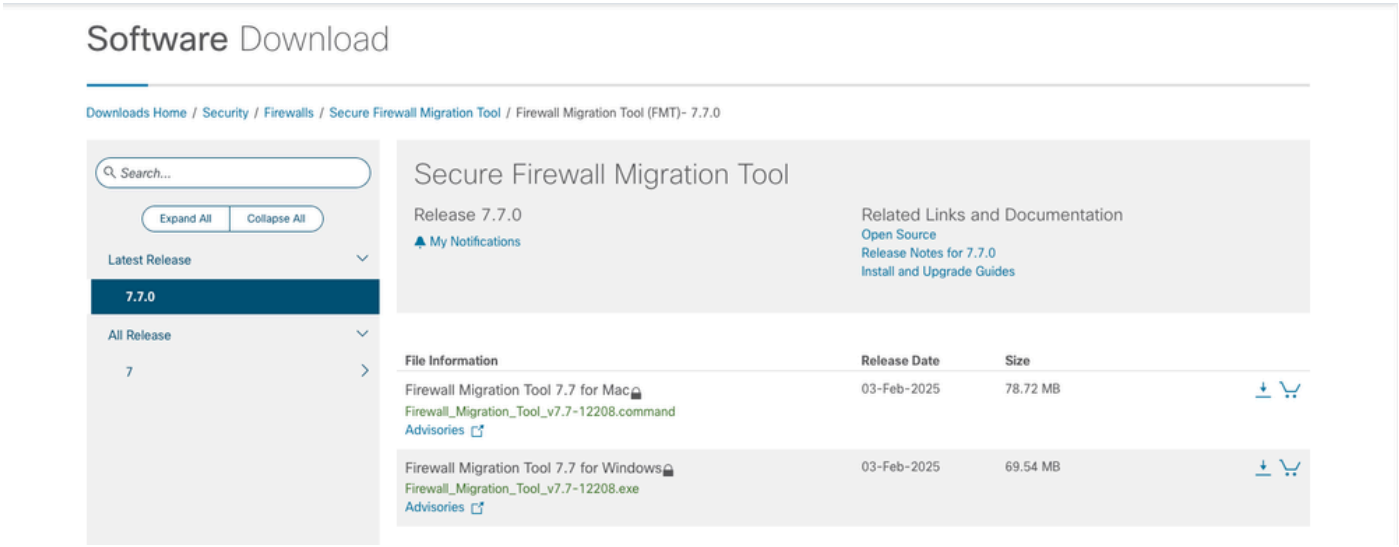
迁移前检查表

- 在开始迁移过程之前，确保FTD已注册到FMC。
- 已在FMC上创建具有管理权限的新用户帐户。或者可以使用现有的管理员凭证。
- 导出的Palo Alto运行配置文件.xml必须使用.zip扩展名进行压缩（请遵循上一节中提到的步骤）。
- 与Paloalto防火墙接口相比，Firepower设备的物理或子接口或端口通道的数量必须相同或更多。

### 配置

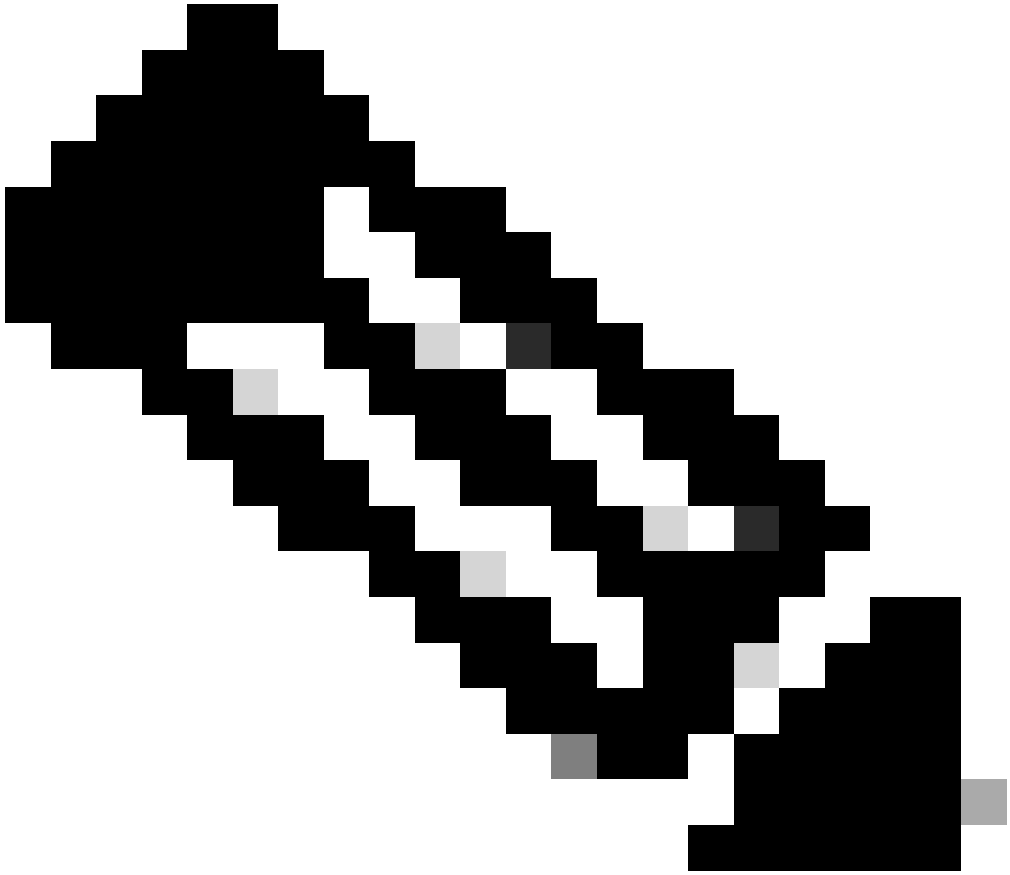
### 迁移步骤

1.从Cisco Software Central下载与您的计算机兼容的最新Firepower迁移工具：



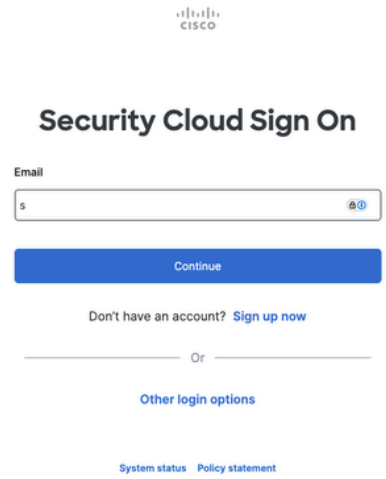

FMT下载

3. 打开之前下载到计算机的文件。



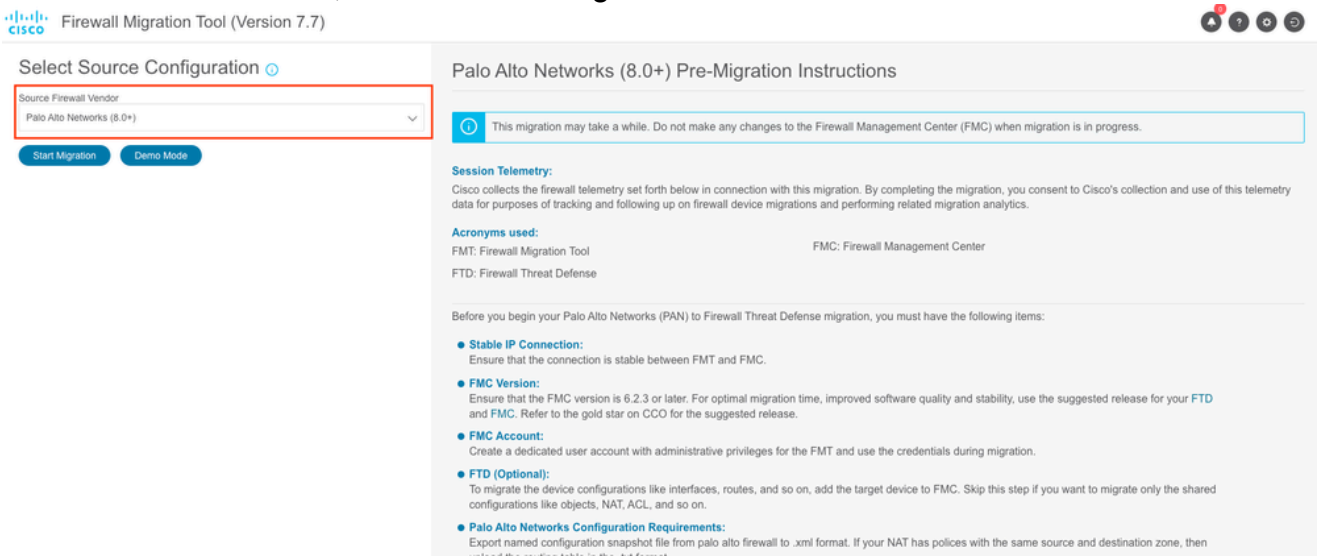
注意：该程序会自动打开，控制台会在您运行文件的目录上自动生成内容。

4. 运行该程序后，它会打开一个Web浏览器，其中显示End User License Agreement。
    1. 选中此复选框以接受条款和条件。
    2. 点击Proceed。
5. 使用有效的CCO凭证登录，以访问FMT GUI。



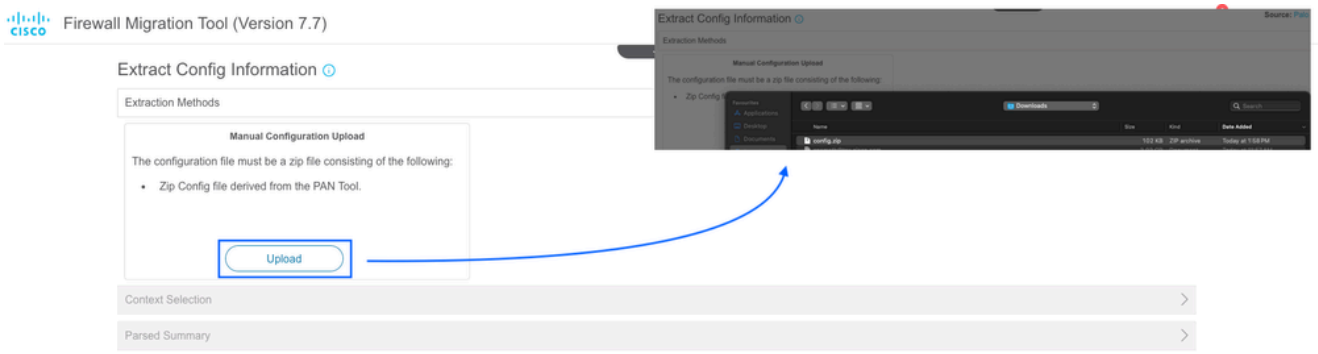

FMT登录提示

6. 选择要迁移的源防火墙，然后单击Start Migration。



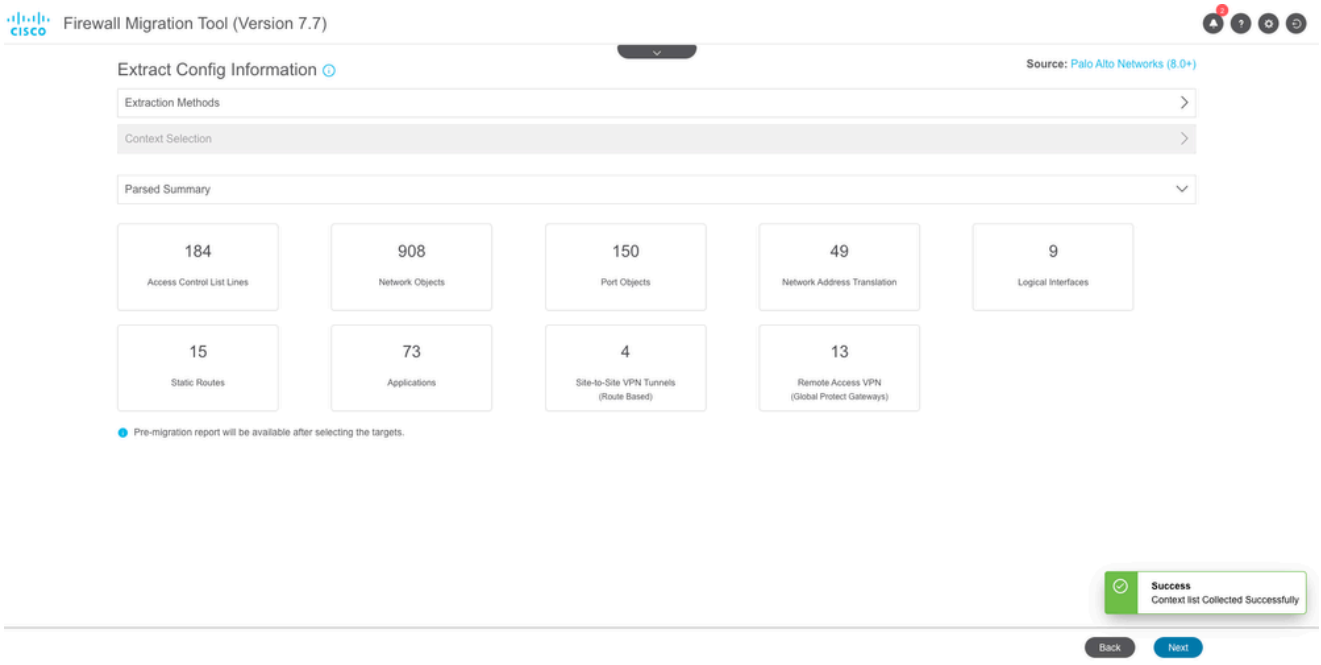

FMT GUI

7. 此时将显示“提取方法”部分，您必须从Paloalto防火墙将Zip配置文件上传到FMT。



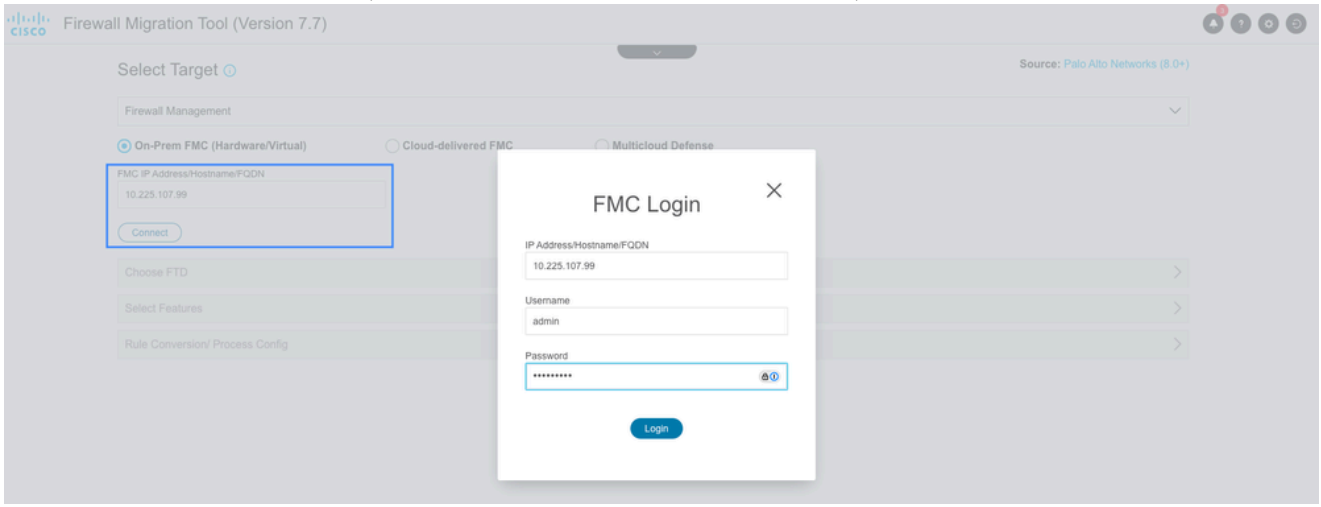

配置上传向导

8. 上传配置文件后，将显示解析的配置摘要。对于VSYS，可以使用单独的VSYS选择。必须逐个解析和迁移它们。
   验证解析的摘要并点击下一步图标。



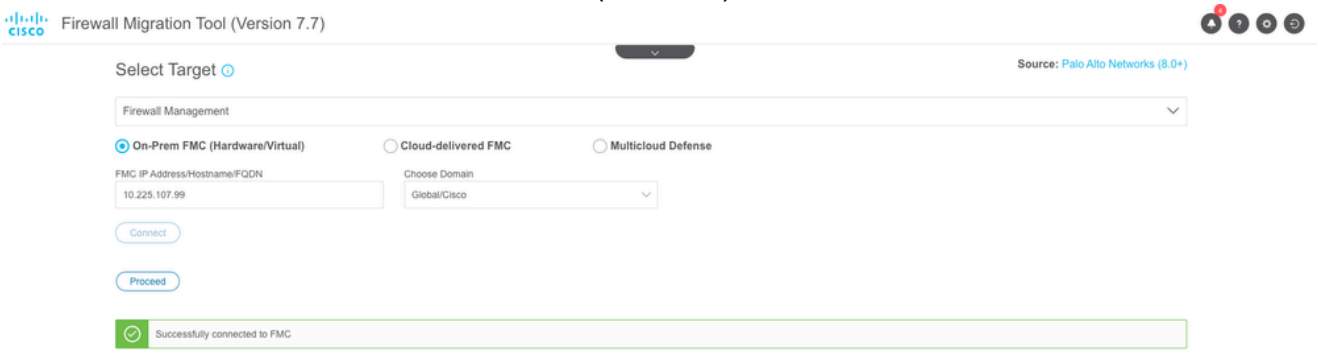

配置验证摘要

9. 您可以在此部分选择FMC的类型。提供其管理IP地址，然后单击Connect。
   系统将显示一个弹出窗口，提示您提供FMC凭证。输入凭证，然后单击登录。



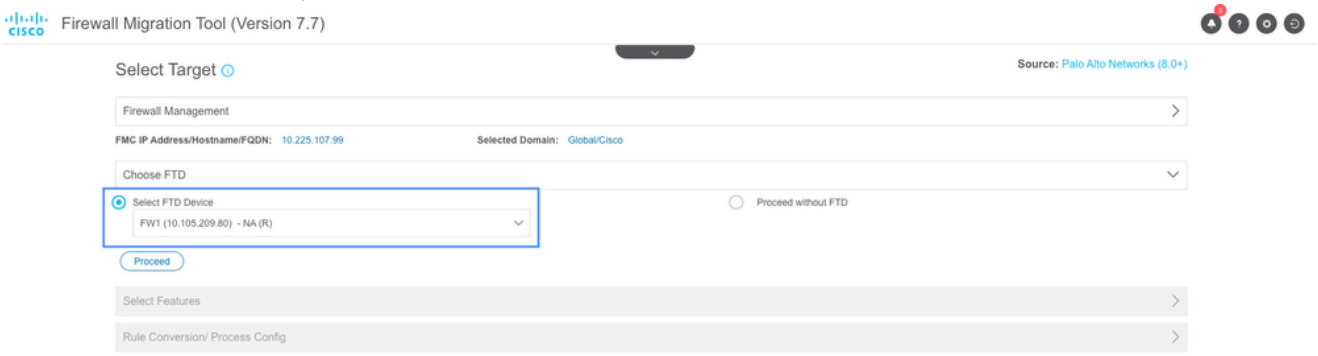
FMC登录

10. 在成功连接到FMC后，您现在可以选择域（如果有）并点击继续。



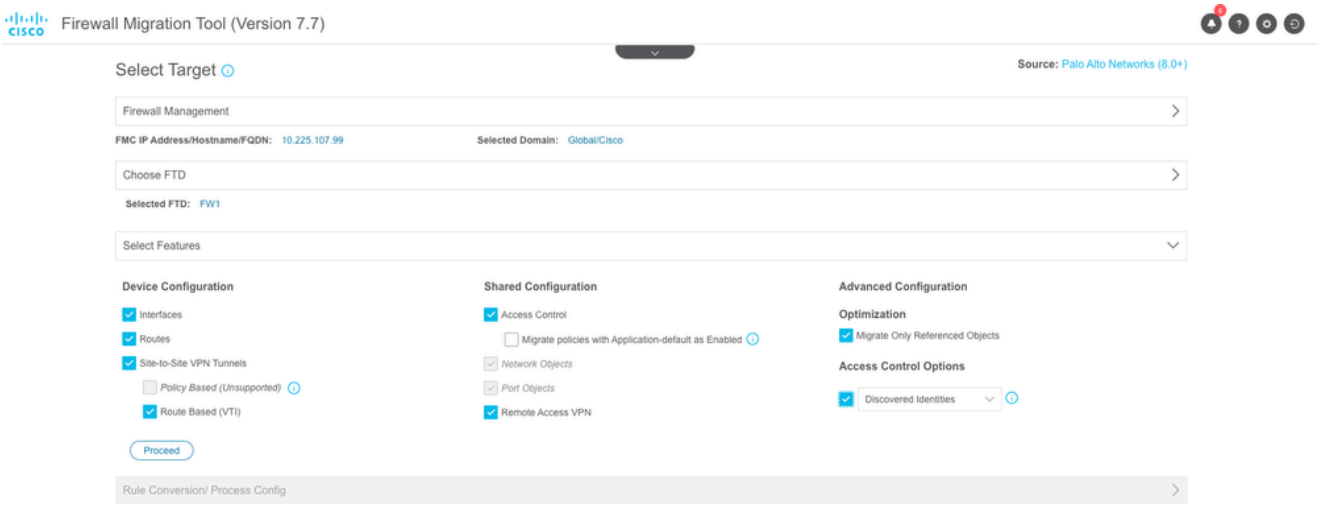

域选择

11. 选择要迁移到的FTD，然后单击Proceed。




选择目标FTD

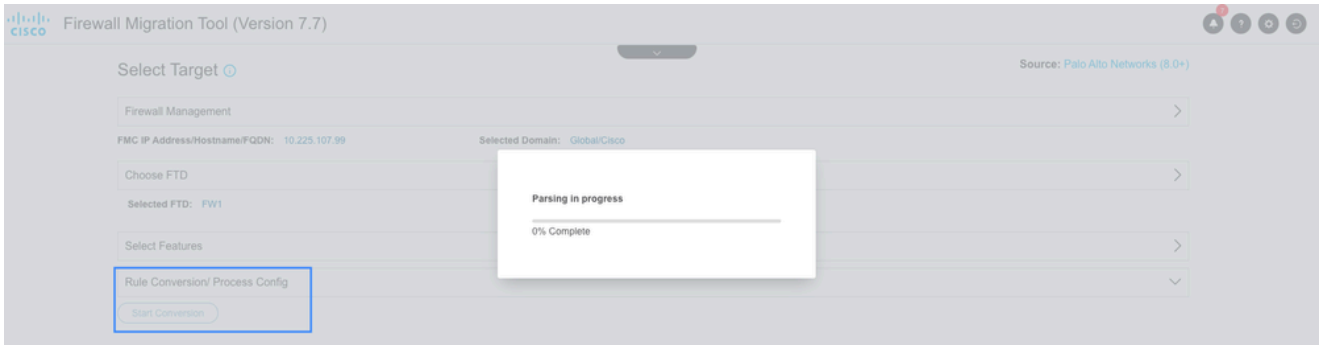
12. 该工具现在列出了要迁移的功能。单击Proceed。




功能选择

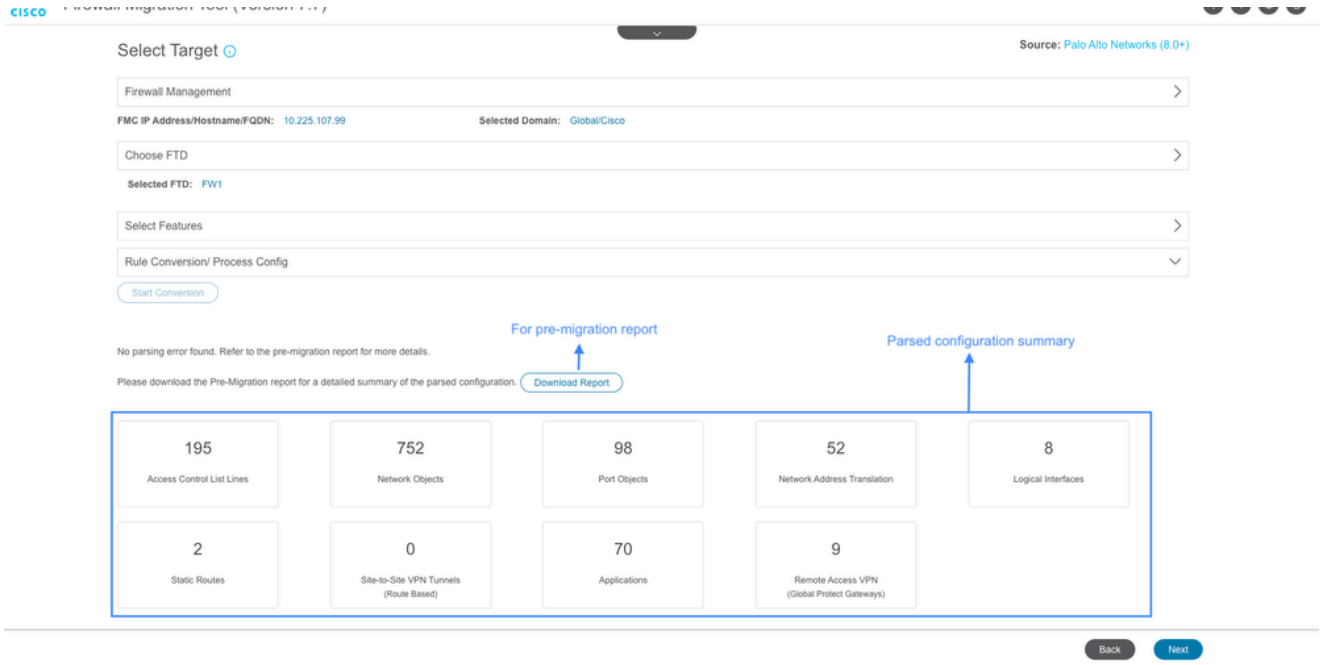
注意：默认情况下会选取所有功能。您可以取消选择任何不迁移的配置。

13. 单击Start Conversion转换配置。



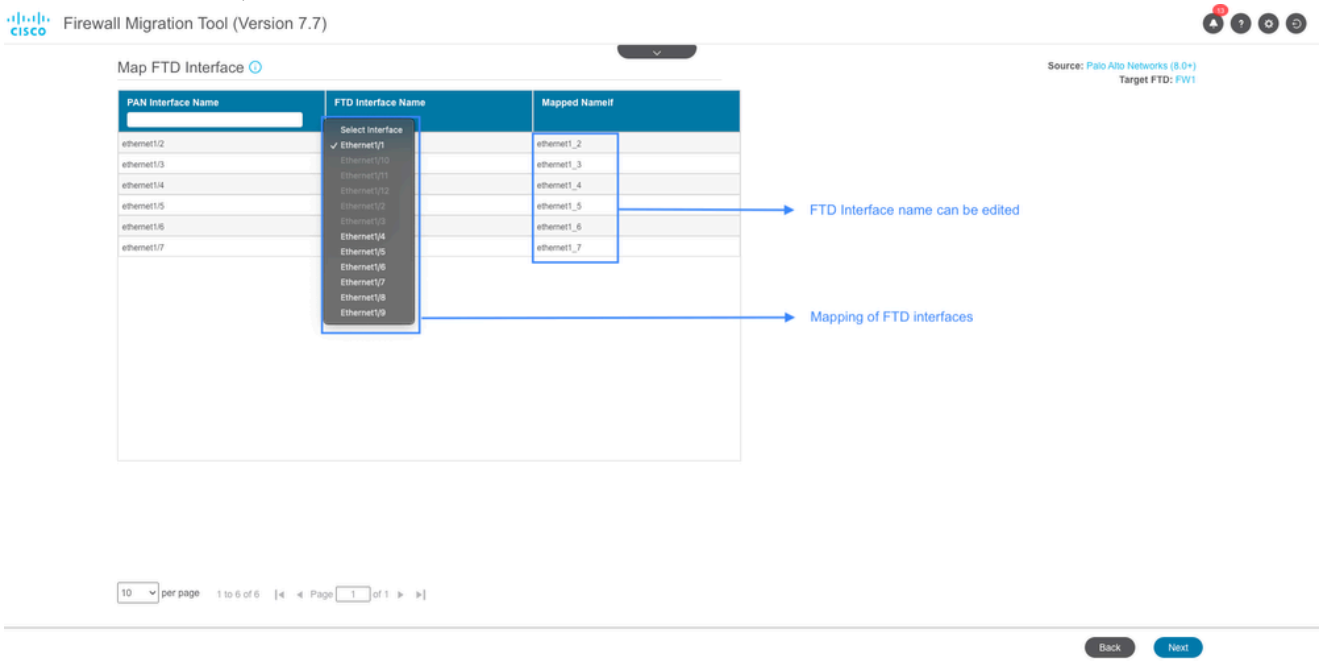

正在分析配置

该工具解析配置并显示转换摘要，如图所示。您也可以下载迁移前报告，以验证任何错误或警告（如果有）的迁移配置。 单击Next导航到下一页。



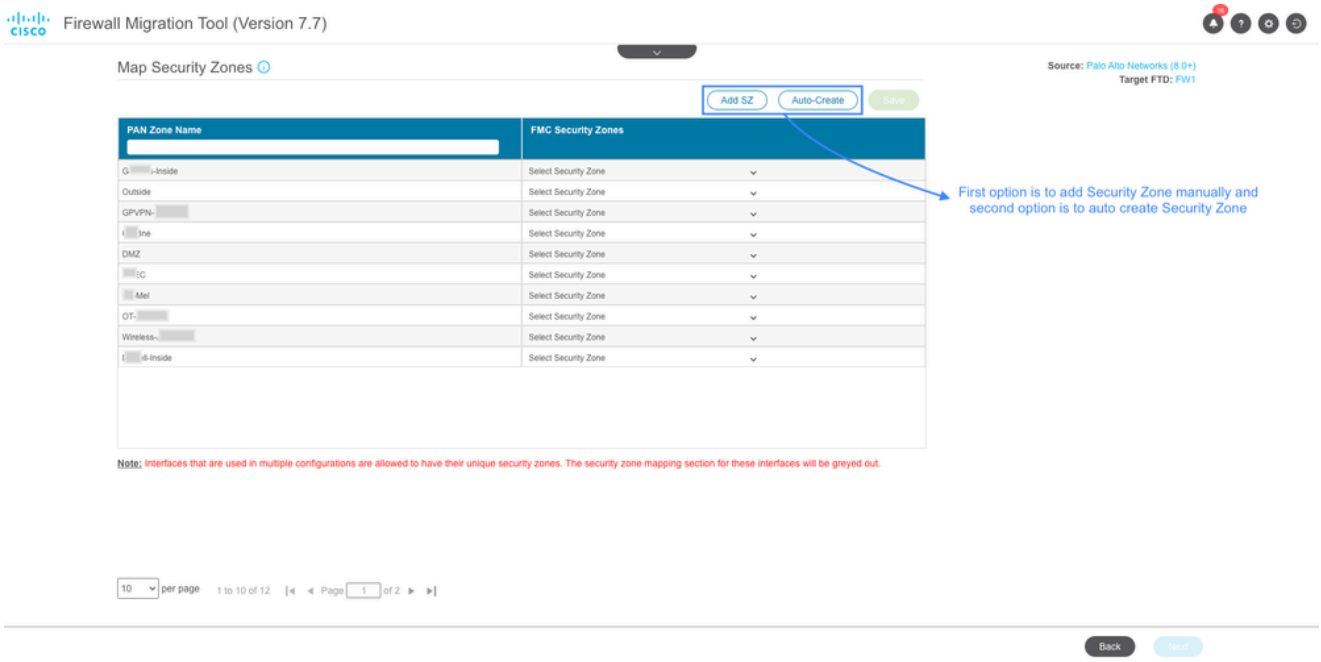

解析的配置摘要

14. 您可以在Interface Mapping部分定义Paloalto到FTD接口映射以及编辑每个接口的接口名称。完成接口映射后，单击下一步。



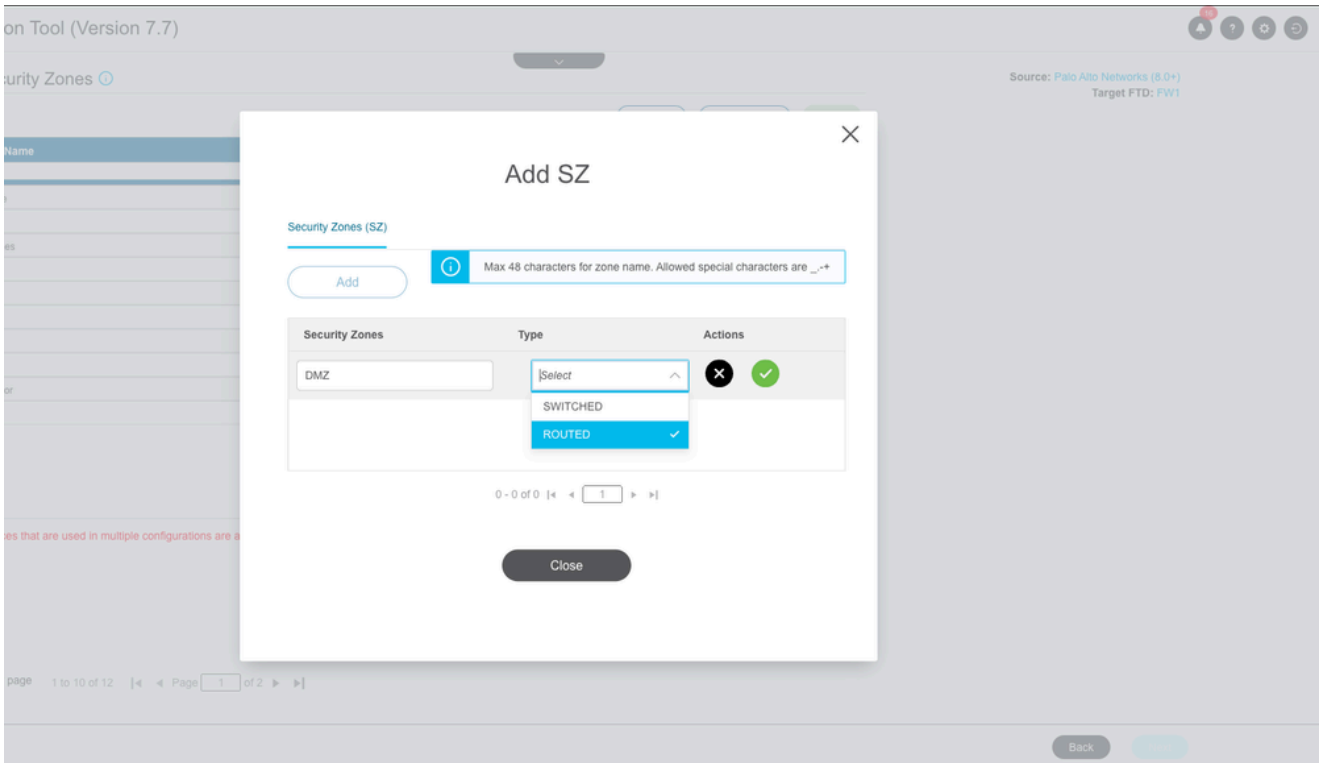

接口映射

15. 您可以为每个接口手动添加安全区域，也可以在映射安全区域部分中自动创建安全区域。创建并映射安全区域后，单击Next。



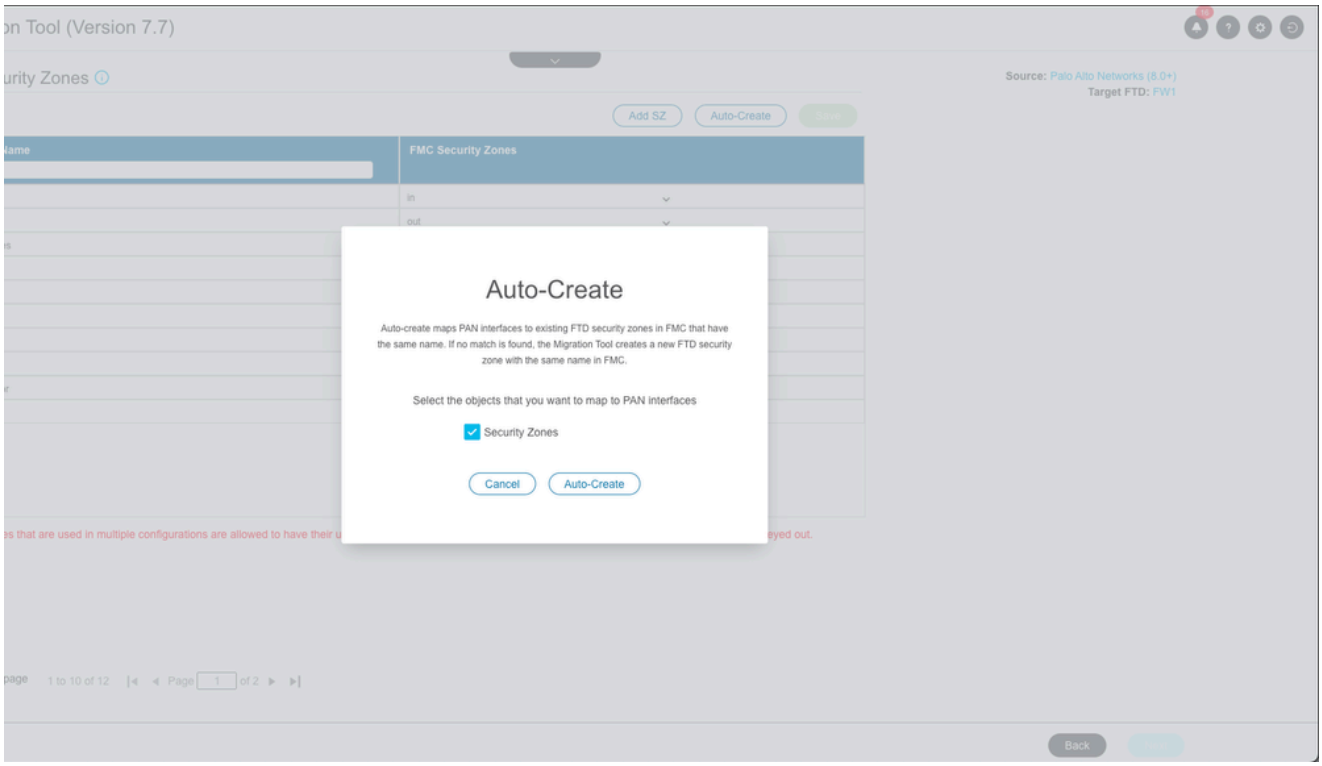

安全区域创建

## 手动创建安全区域：



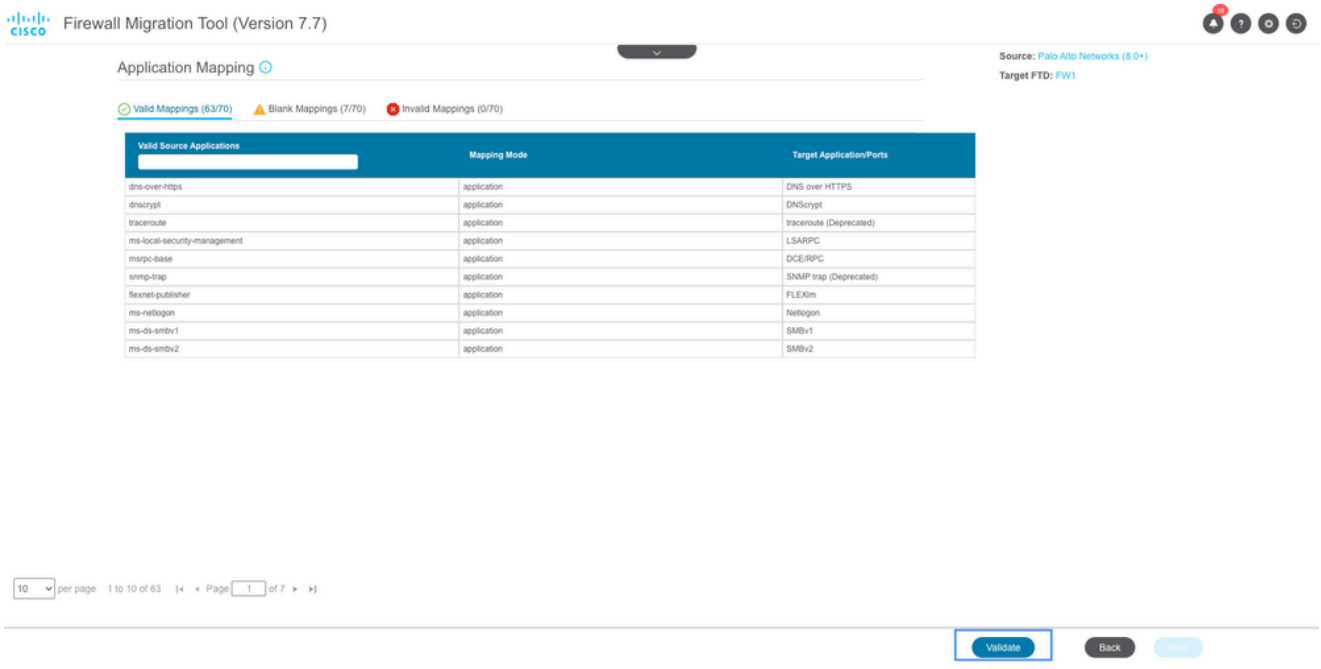

手动创建安全区域

## 自动创建安全区域：

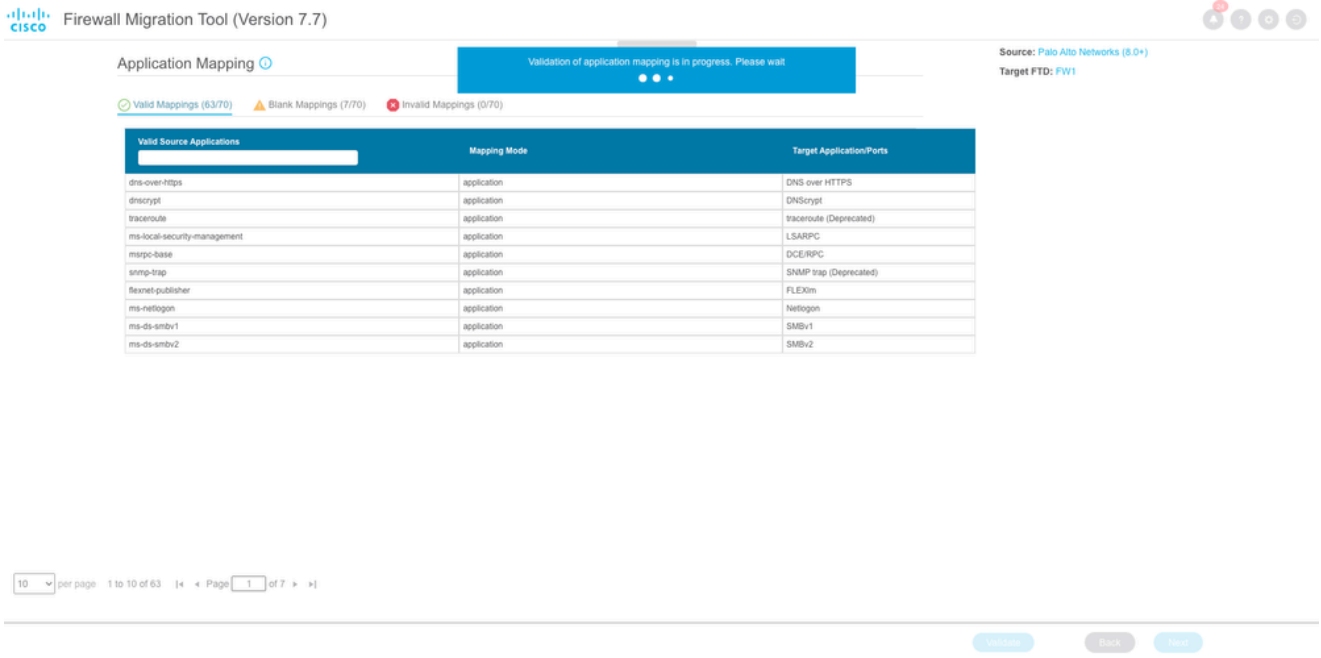



自动安全区域创建

16. 现在您可以转到“应用程序映射”部分。单击Validate按钮验证应用程序映射。



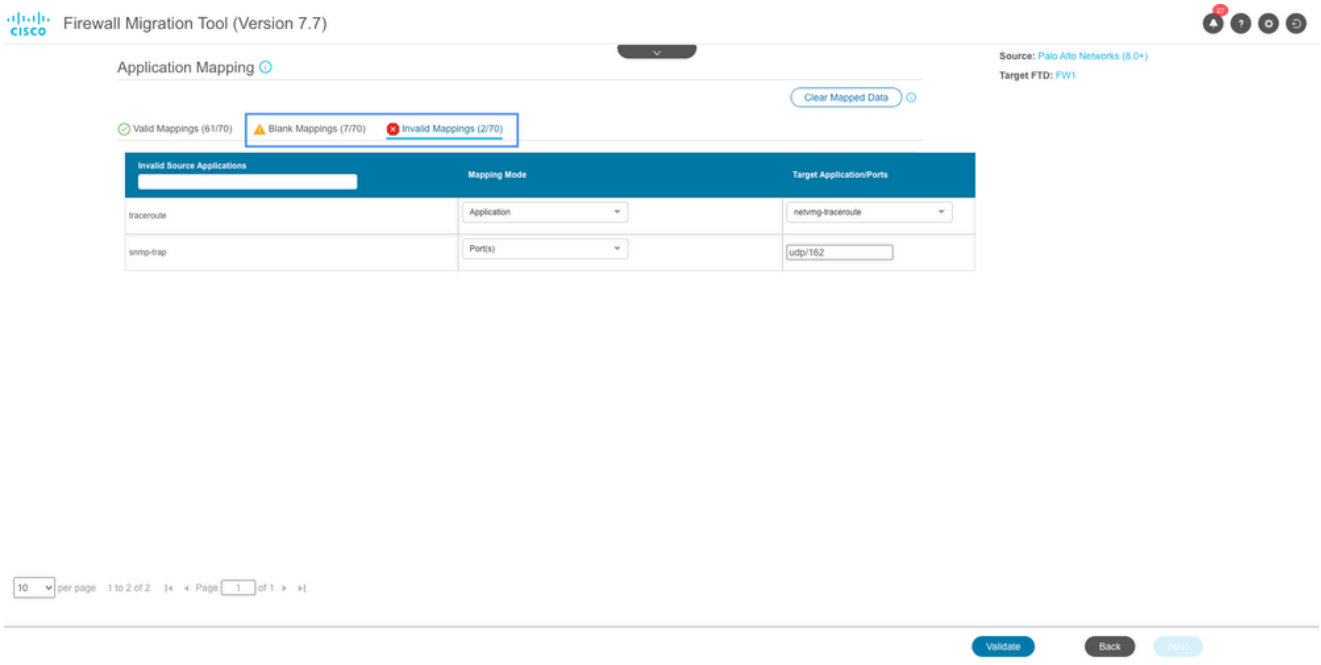

应用映射




应用程序映射验证

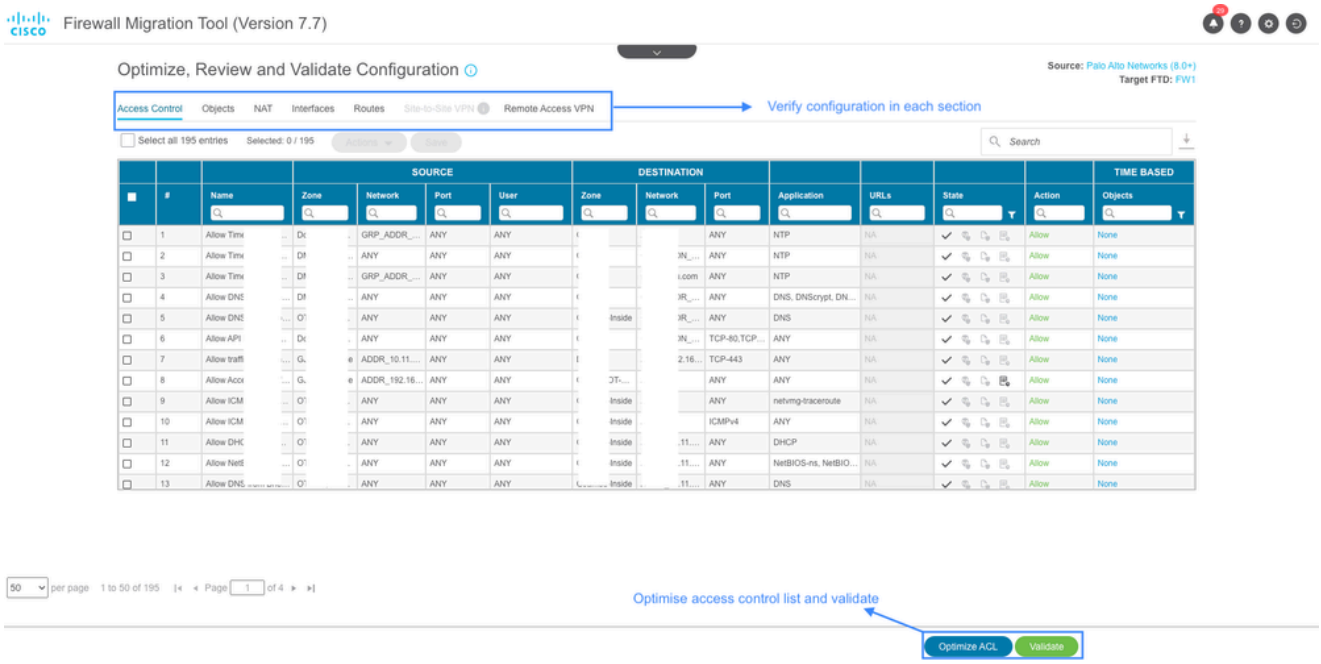
验证后，FMT将列出空白和无效映射。在继续进一步之前必须更正无效映射，并且更正空白映射是可选操作。

再次单击Validate以验证更正的映射。验证成功后，单击Next。



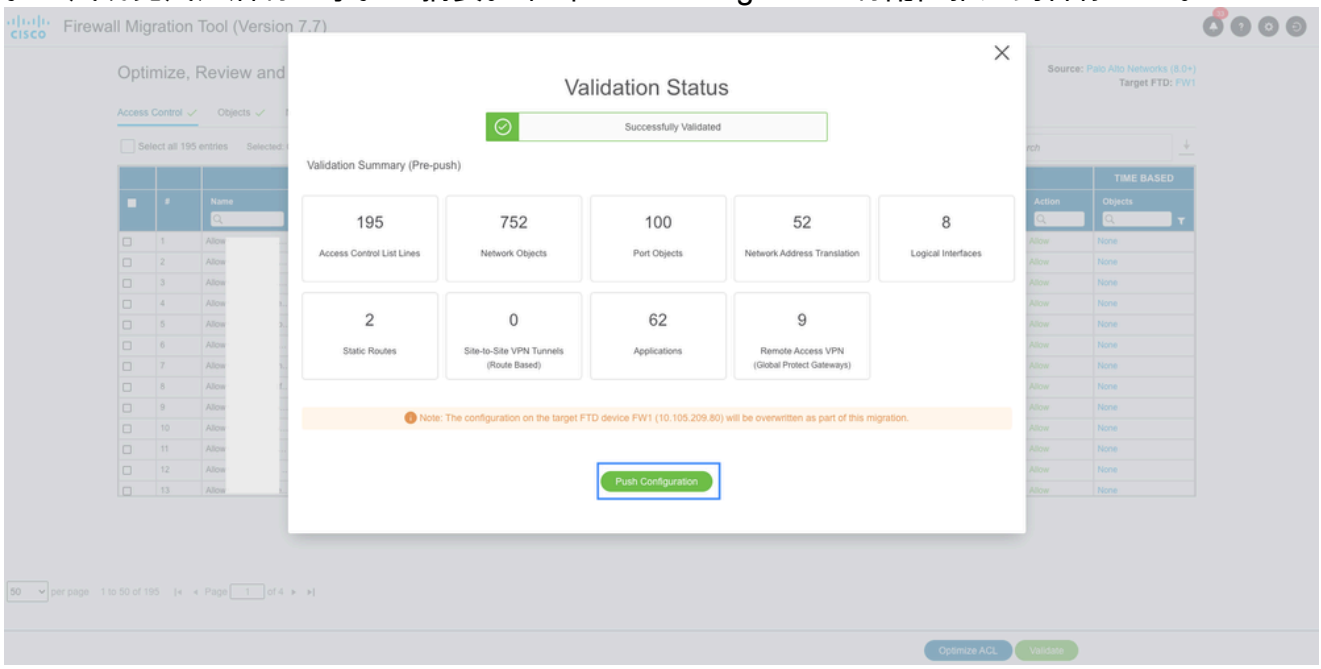

空白和无效应用程序映射

17. 如果需要，可以在下一节中优化ACL。查看每个部分的配置，例如访问控制、对象、NAT、接口、路由和远程访问VPN。查看配置后，单击Validate。



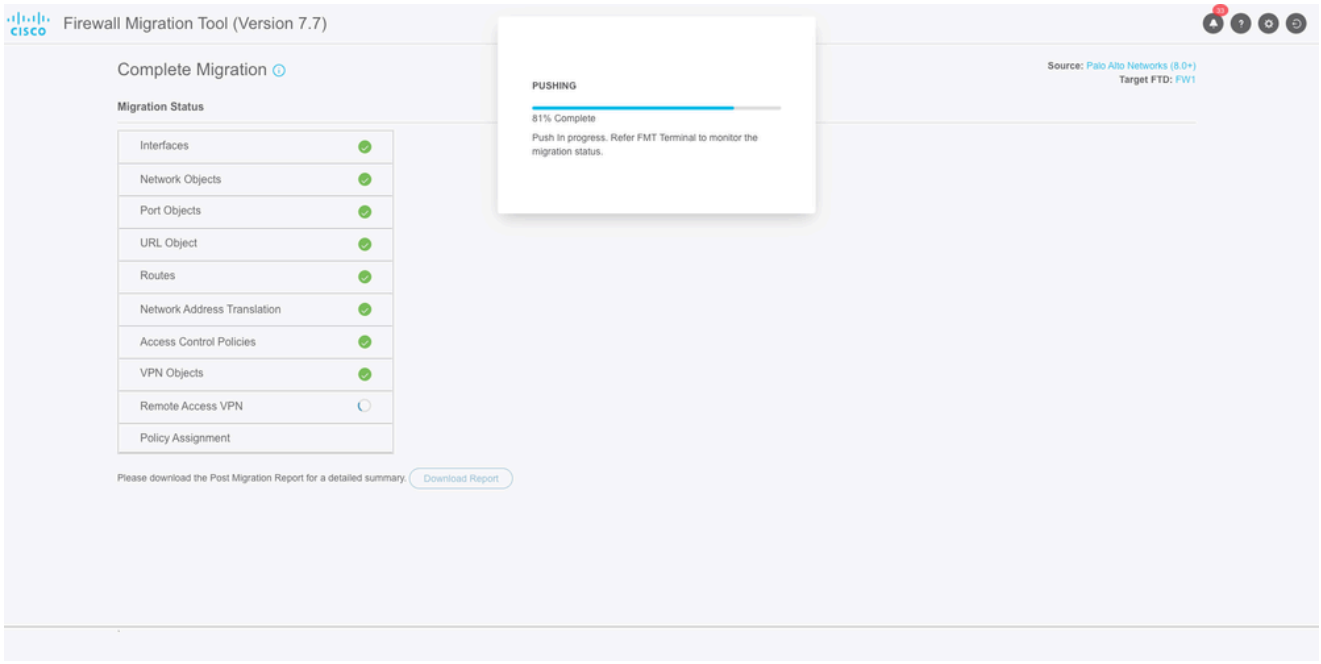

配置验证

18. 验证成功完成之后将显示验证摘要。单击Push Configuration将配置推送到目标FMC。



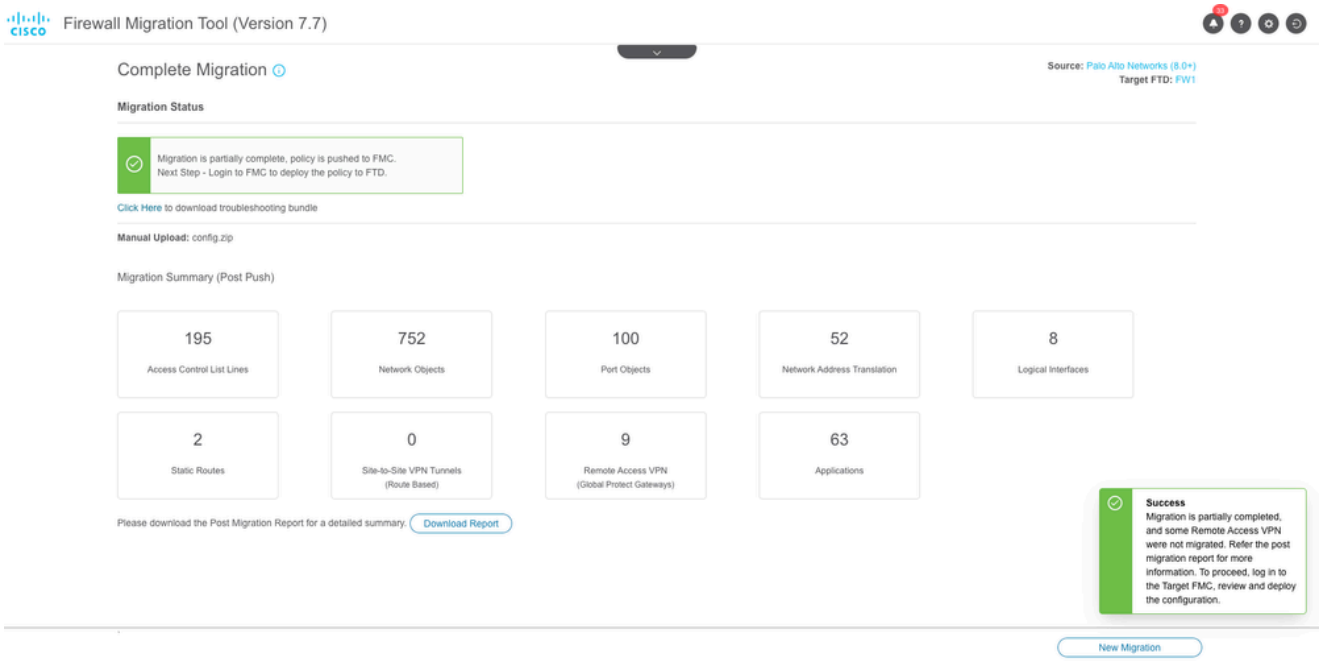

配置验证摘要

19. 配置推送到FMC的进度现在显示在Migration Status部分。您也可以使用FMT terminal窗口监控迁移状态。




迁移状态

20. 迁移摘要由工具在成功迁移时显示。它还列出部分迁移的配置（如果有）。例如，由于缺少安全客户端软件包，此场景中的远程访问VPN配置。
    您还可以下载迁移后报告来检查迁移的配置以及是否有任何错误或需要更正的配置。




成功迁移摘要

21. 最后一步是查看从FMC迁移的配置和将配置部署到FTD。
    要部署配置，请执行以下操作：
    1. 登录到FMC GUI。
    2. 导航到部署选项卡。
    3. 选择要将配置推送到防火墙的部署。
    4. 单击Deploy。

# 故障排除

## 安全防火墙迁移工具故障排除

常见迁移失败：

- PaloAlto配置文件中未知或无效的字符。
- 配置元素缺失或不完整。
- 网络连接问题或延迟。
- 在PaloAlto配置文件上传期间或将配置推送到FMC时出现问题。

使用支持捆绑包进行故障排除：

- 在“Complete Migration”（完成迁移）屏幕上，单击Support按钮。
- 选择Support Bundle并选择要下载的配置文件。
- 默认情况下会选择日志和数据库文件。
- 单击Download获取.zip文件。
- 解压缩.zip以查看日志、数据库和配置文件。
- 单击Email us将故障详细信息发送给技术团队。
- 在邮件中附加支持捆绑包。
- 单击访问TAC页面以创建思科TAC案例以获取帮助。

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）。