配置由单个FMC管理的FTD之间的VPN迁移

目录

简介

本文档介绍将站点到站点VPN从一个FTD迁移到由同一FMC管理的另一个FTD，同时保持与路由器的VPN连接。

先决条件

要求

为有效实施迁移流程，思科建议熟悉以下主题：
· FTD向FMC注册：了解如何向Firepower管理中心(FMC)注册Firepower威胁防御(FTD)设备。
·站点到站点VPN配置：在FMC管理的FTD设备上配置站点到站点VPN的经验。

使用的组件

本文档基于给定的软件和硬件版本：
·Firepower威胁防御虚拟(FTDv):运行7.3.1版的两个实例。
· Firepower管理中心(FMC):7.4.0 版.

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。

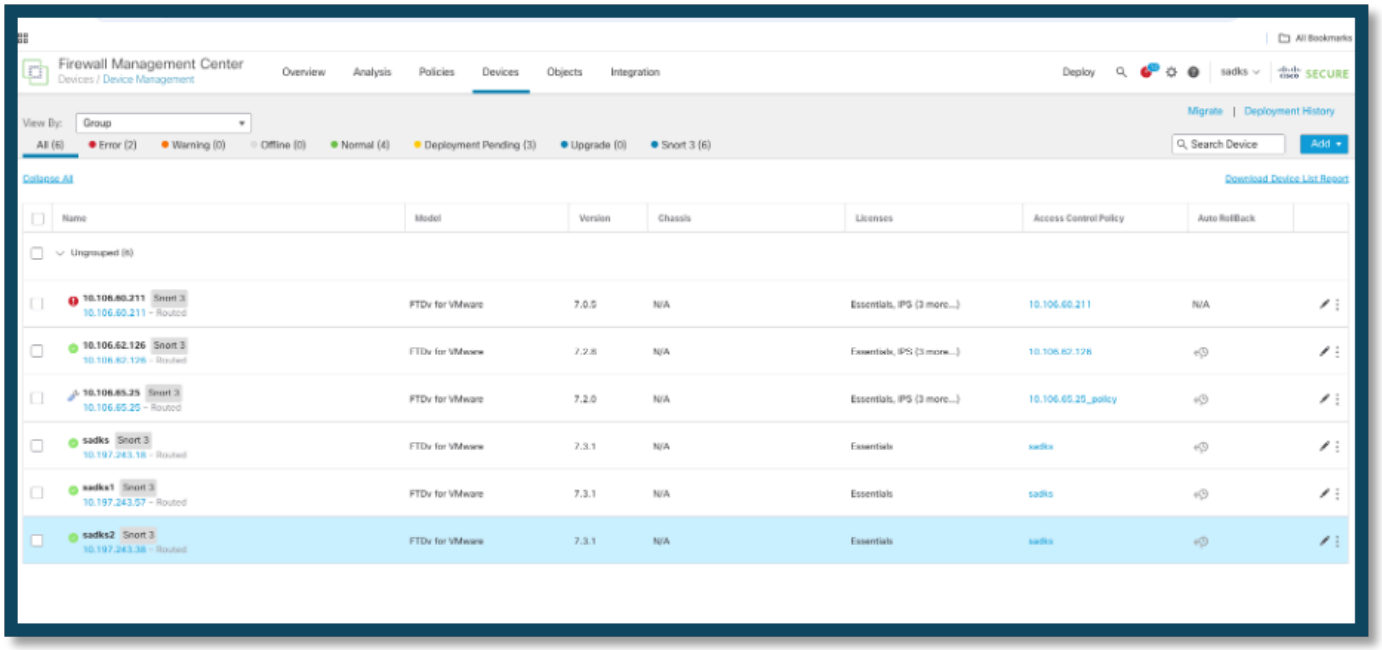
配置

步骤

1.向FMC注册新的FTD:
·首先在Firepower管理中心(FMC)的Devices > Device Management下注册新的Firepower威胁防

御(FTD)设备。

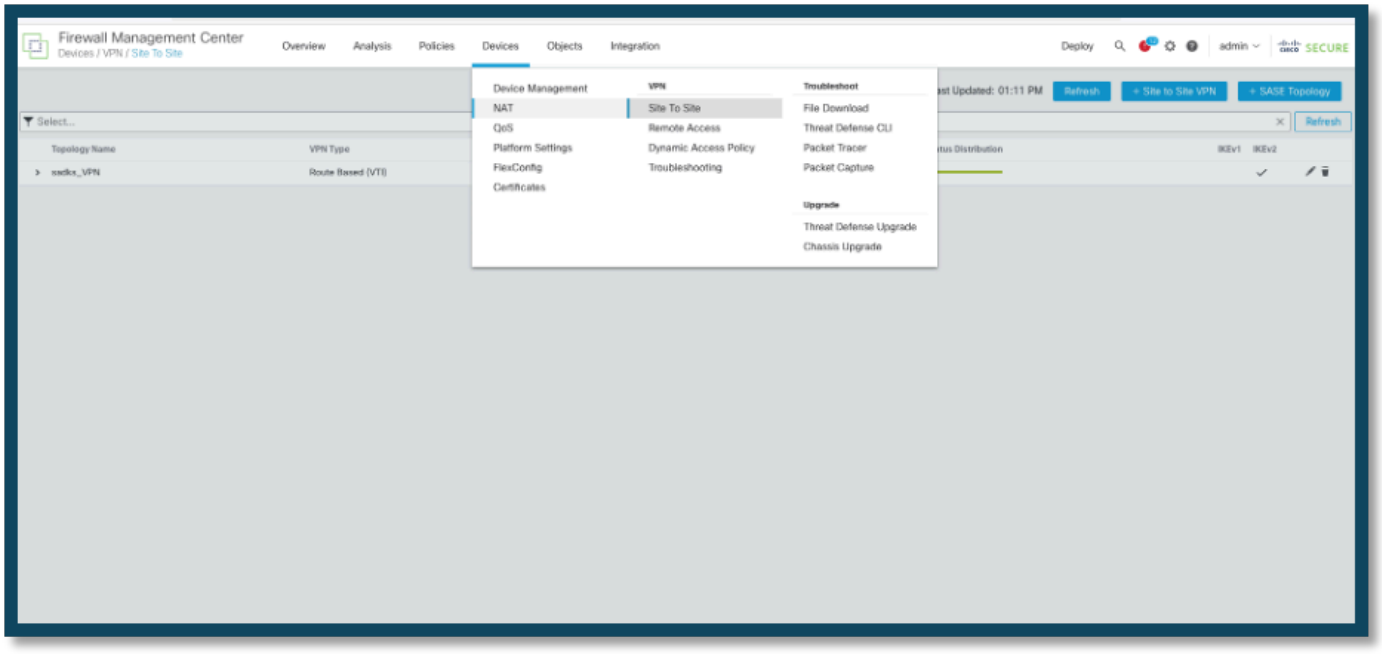
·在本示例中，注册的新设备名为“sadks2”。



新注册的FTD

2. 访问站点到站点隧道配置：

·转到FMC界面中的Devices > Site to Site，导航到站点到站点隧道设置。

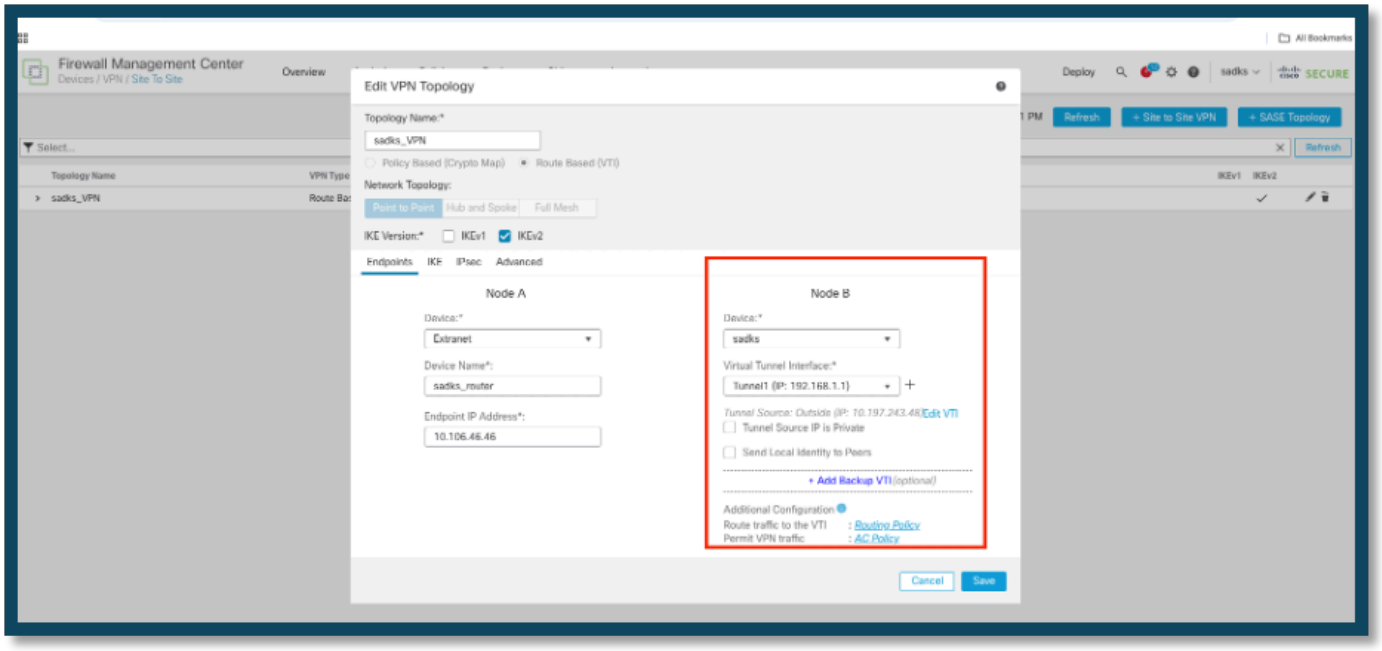


导航到VPN配置

3.修改VPN配置：

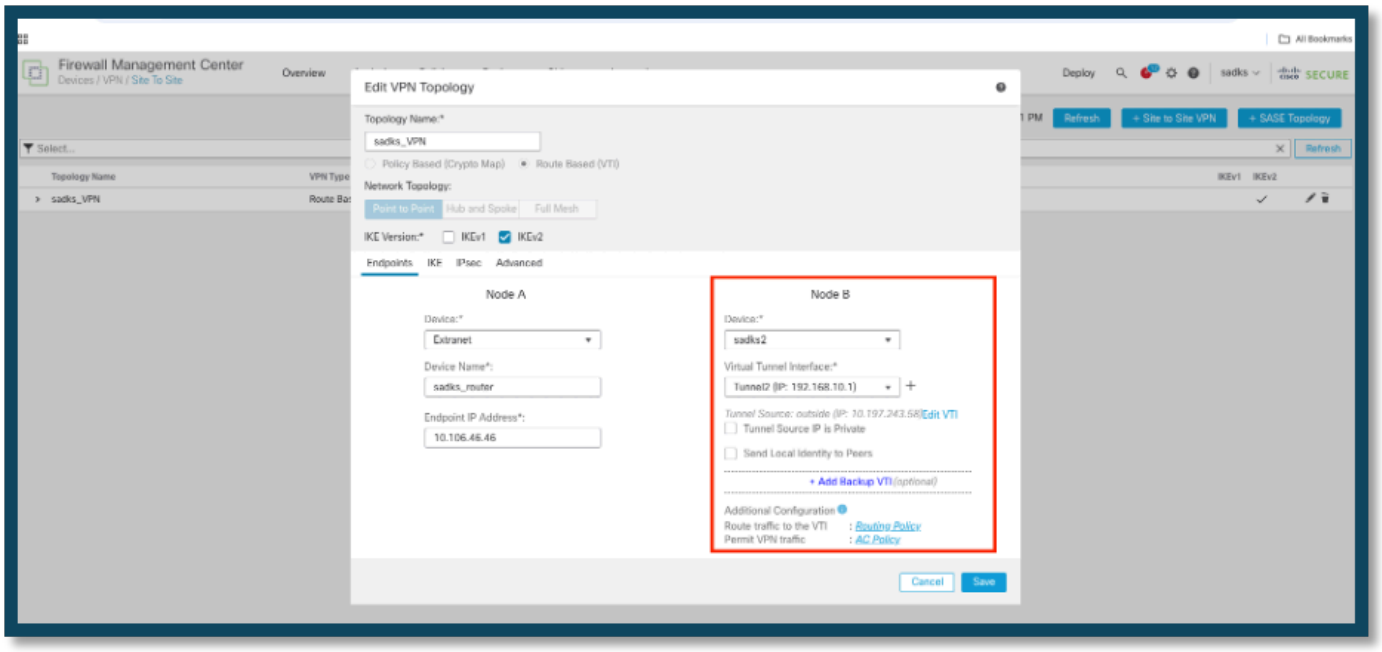
·选择要更新的VPN配置。

•示例：在此场景中，VPN配置涉及FTD设备和路由器。此处，节点B代表FTD设备，并且已更新配置以将设备关联从“sadks”更改为“sadks2”。



旧FTD设备

到



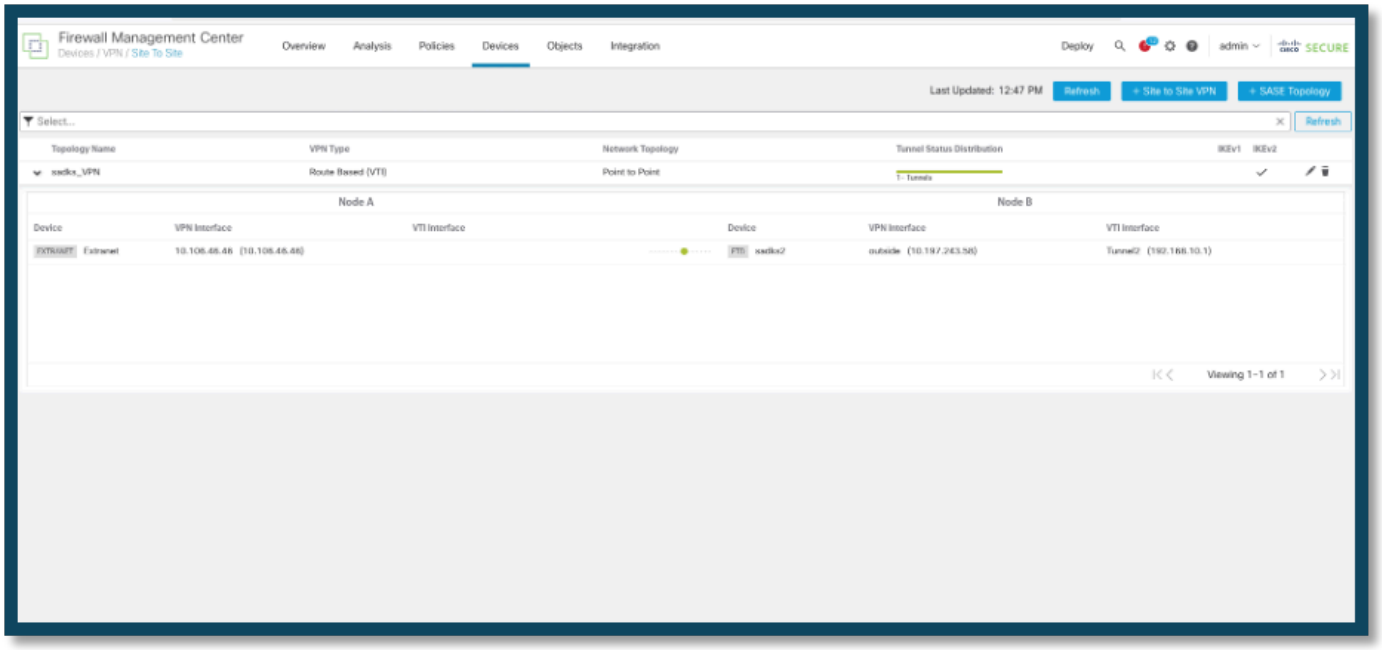
新FTD设备

4.保存并部署配置：

·进行必要的更改后，保存配置并部署以激活更新。

验证

隧道在部署后启动。



通道状态

故障排除

初始连接问题

构建VPN时，需要双方协商隧道。因此，当您排除任何类型的隧道故障时，最好获取会话的两端。有关如何调试IKEv2隧道的详细指南可以在此处找到：如何调试IKEv2 VPN

隧道故障的最常见原因是连接问题。确定这一点的最佳方法是在设备上捕获数据包。使用此命令在设备上捕获数据包捕获：

<#root>

```
capture capout interface outside match ip host 10.106.46.46 host 10.197.243.58
```

捕获到位后，尝试通过VPN发送流量并检查数据包捕获中的双向流量。

使用以下命令检查数据包捕获：

<#root>

show cap capout

特定流量问题

您遇到的常见流量问题包括：

- FTD后的路由问题 — 内部网络无法将数据包路由回分配的IP地址和VPN客户端。
- 访问控制列表阻止流量。
- VPN流量未绕过网络地址转换。

有关FMC管理的FTD上的VPN的详细信息，您可以在此处找到完整配置指南：由FMC管理的FTD配置指南

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）。