在FDM管理的FTD上配置远程访问VPN

目录

简介

先决条件

- 要求
- 使用的组件
- 许可

背景信息

配置

- 网络图
- 验证FTD上的许可
- 定义受保护的网络
- 创建本地用户
- 添加证书
- 配置远程访问VPN

验证

故障排除

- AnyConnect客户端问题
- 初始连接问题
- 特定流量问题

简介

本文档介绍如何配置在运行版本6.5.0及更高版本的机上管理器FDM管理的FTD上的RAVPN部署。

先决条件

要求

思科建议您了解Firepower设备管理器(FDM)上的远程访问虚拟专用网络(RAVPN)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：

- 运行版本6.5.0-115的思科Firepower威胁防御(FTD)
- Cisco AnyConnect Secure Mobility Client 版本 4.7.01076

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。

许可

- Firepower威胁防御在启用导出控制功能的智能许可门户中注册（以便允许启用RAVPN配置选项卡）
- 任何已启用的AnyConnect许可证（APEX、Plus或仅VPN）

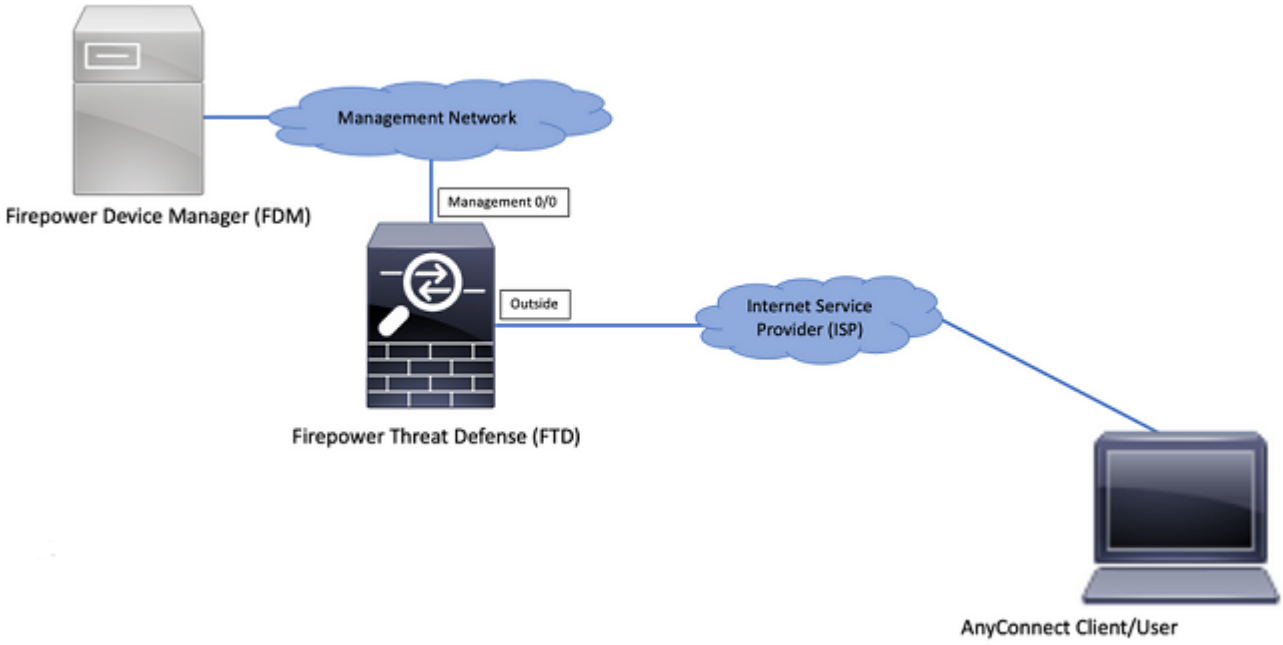
背景信息

通过FDM配置FTD时，当您尝试通过外部接口为AnyConnect客户端建立连接时，如果通过同一接口访问管理，则会遇到困难。这是FDM的已知限制。已针对此问题提交增强请求Cisco Bug ID CSCvm76499。

配置

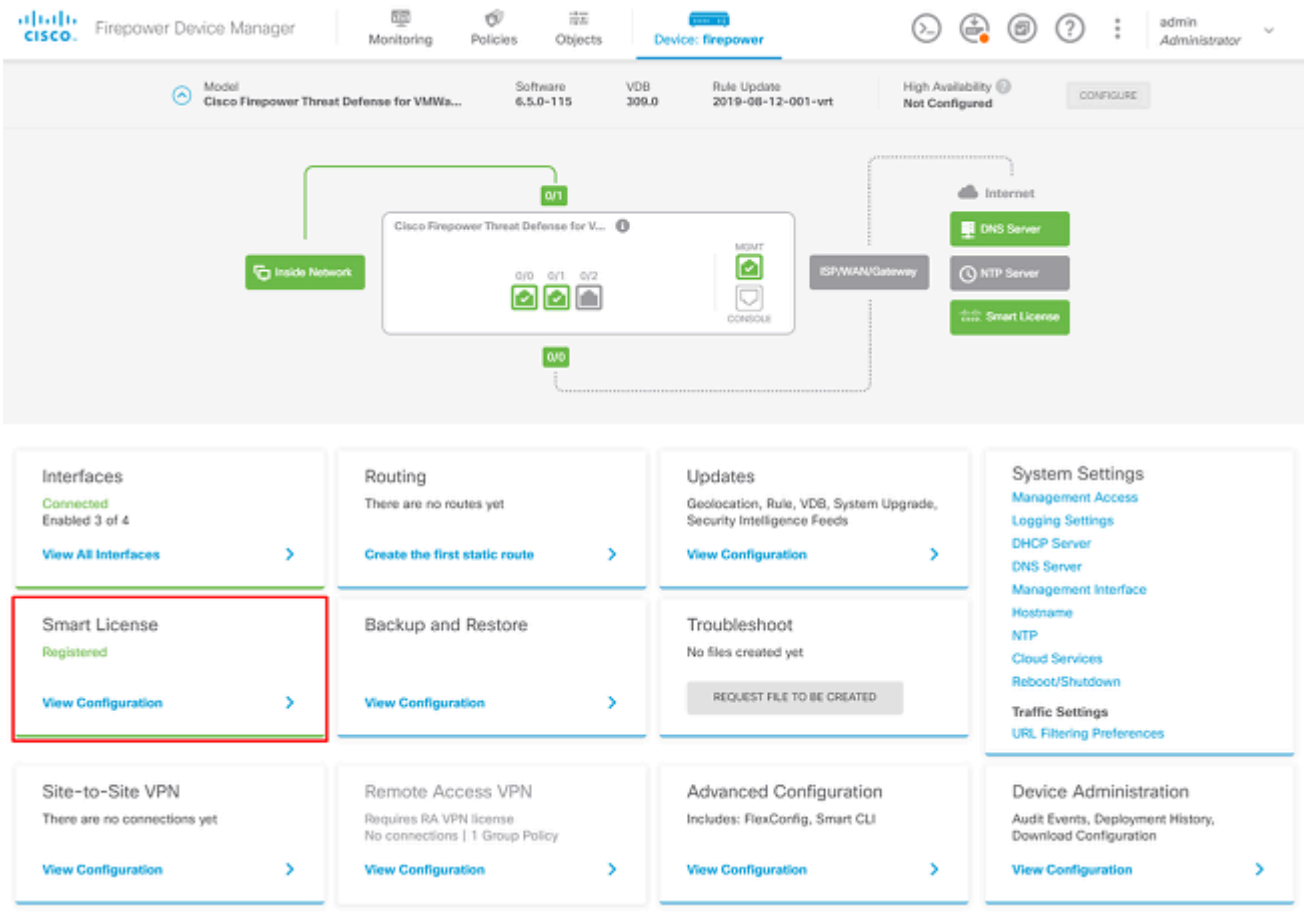
网络图

AnyConnect Client Authentication with use of Local（AnyConnect客户端身份验证使用本地）。

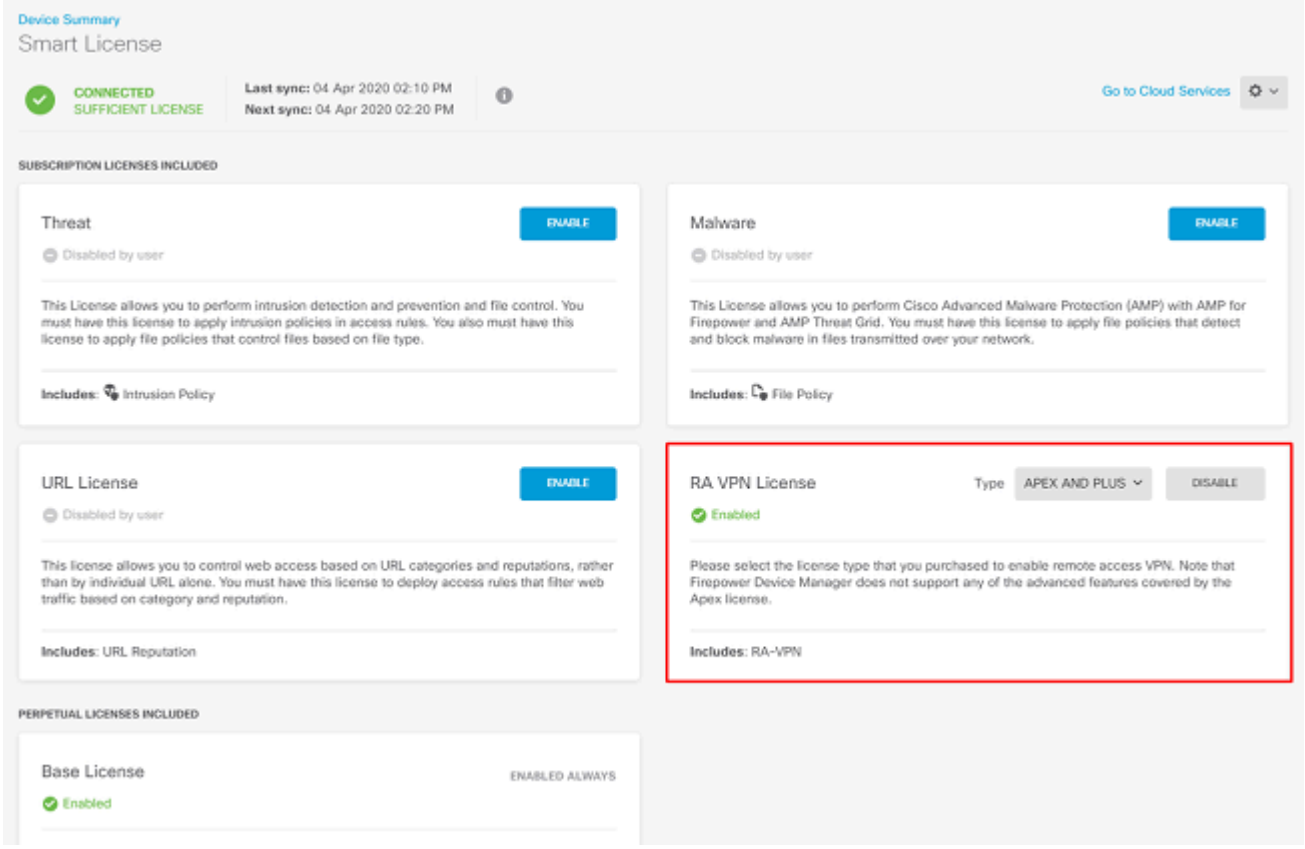


验证FTD上的许可

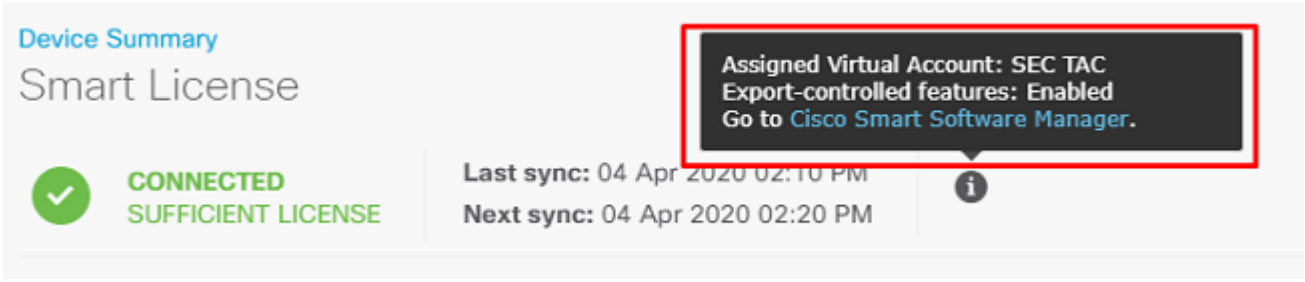
步骤1.确认设备已注册到智能许可，如图所示。



步骤2.验证设备上是否启用了AnyConnect许可证，如图所示。

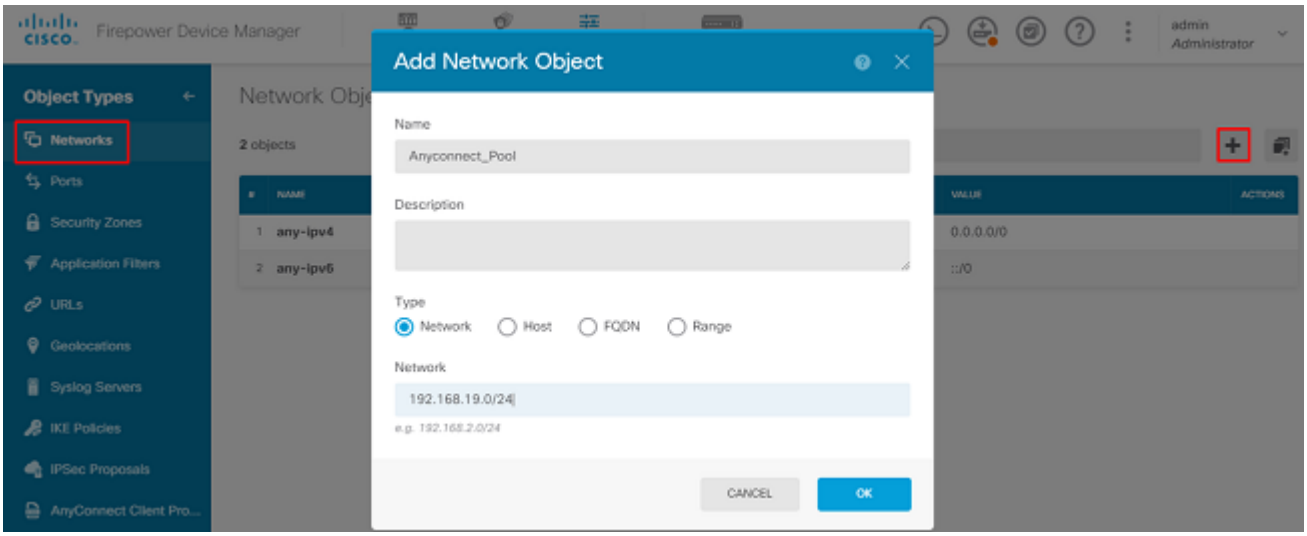


步骤3.验证导出控制功能在令牌中是否已启用，如图所示。

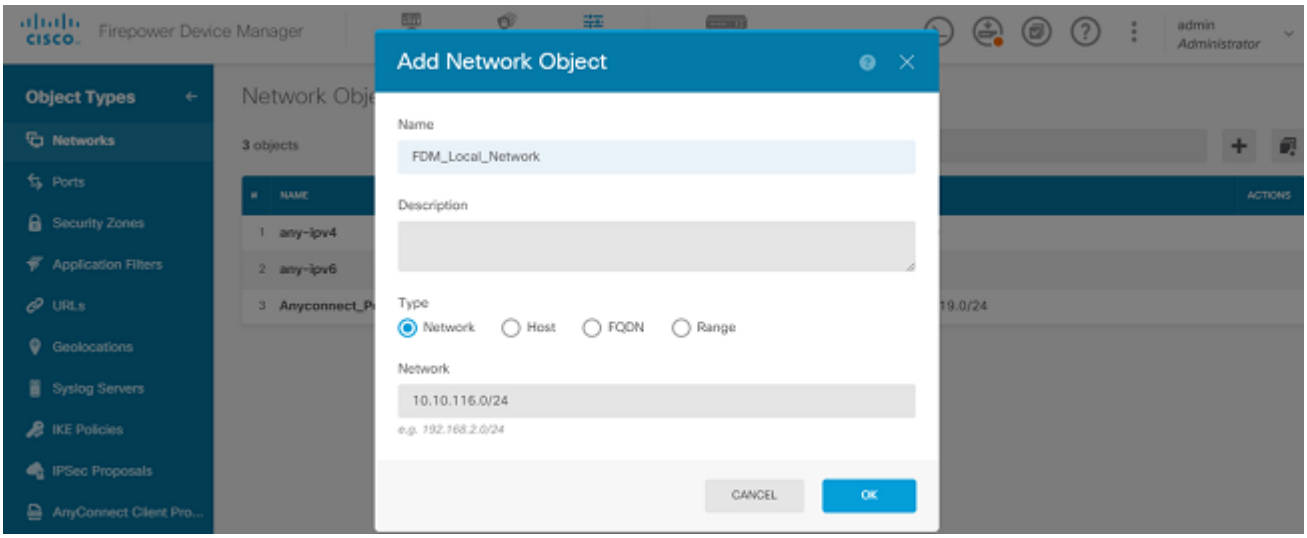


定义受保护的网络

导航至。Objects > Networks > Add new Network从FDM GUI配置VPN Pool和LAN Networks。创建VPN Pool以用于AnyConnect用户的本地地址分配，如图所示。

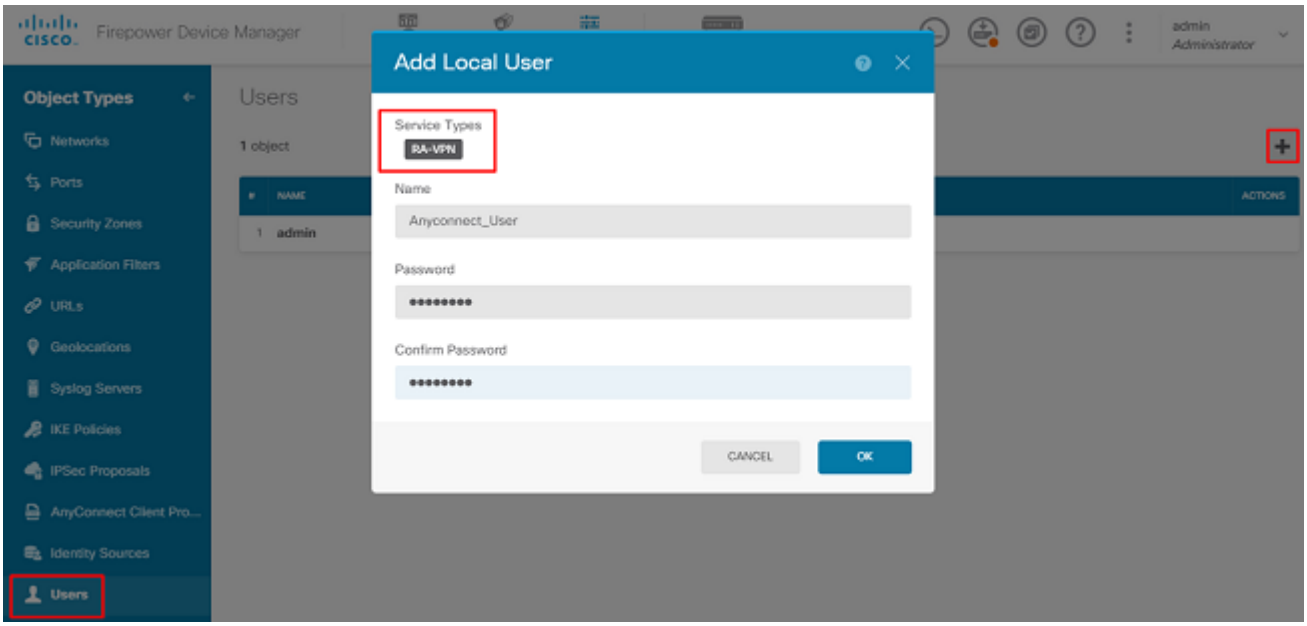


为FDM设备后面的本地网络创建对象，如图所示。



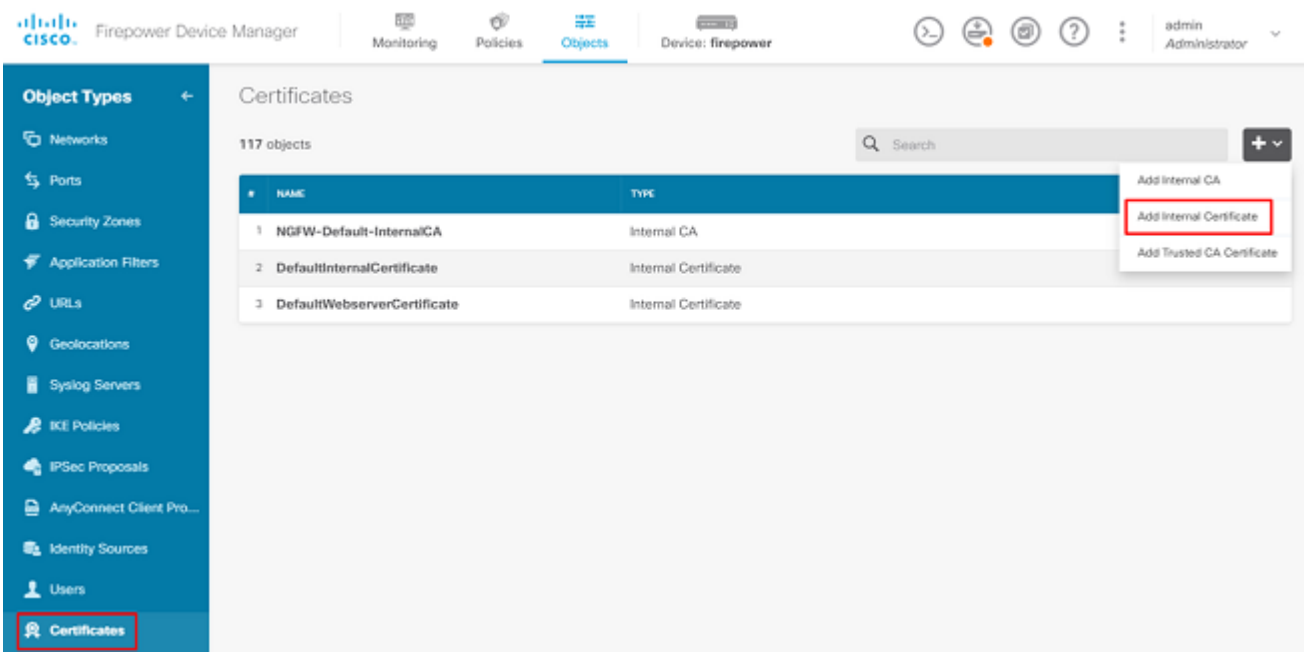
创建本地用户

导航至。Objects > Users > Add User添加通过AnyConnect连接到FTD的VPN 本地用户。如图所示，创建本地用户。

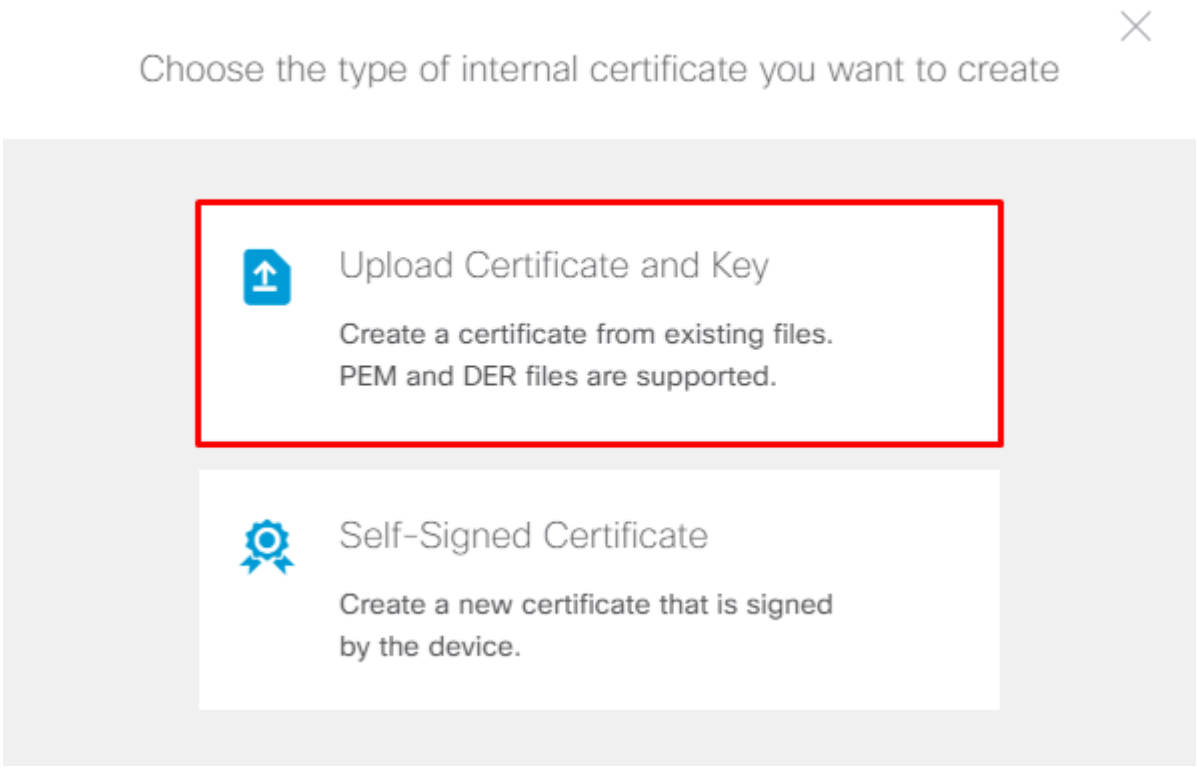


添加证书

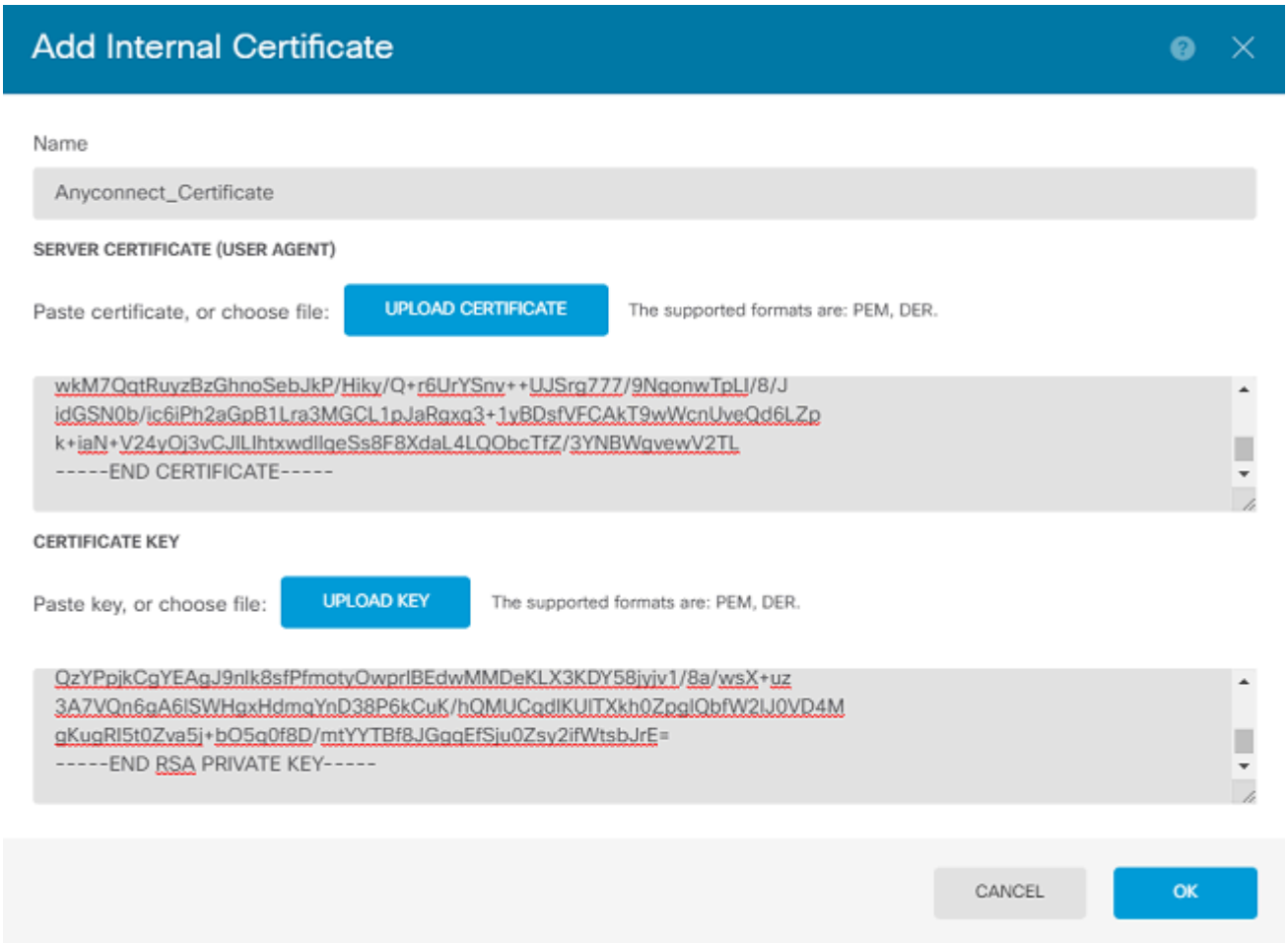
导航至Objects > Certificates > Add Internal Certificate。配置证书，如图所示。



上传证书和私钥（如图所示）。

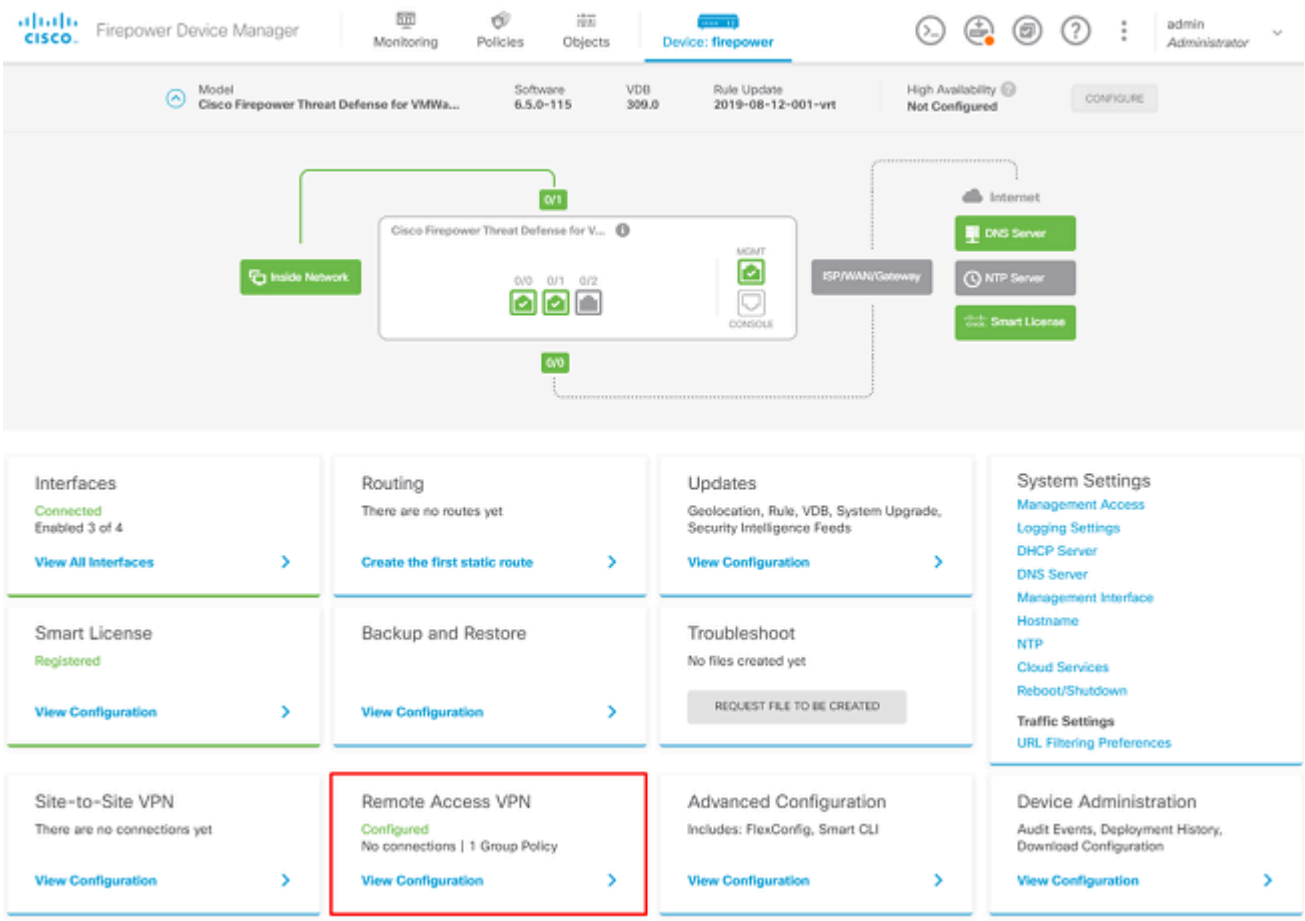


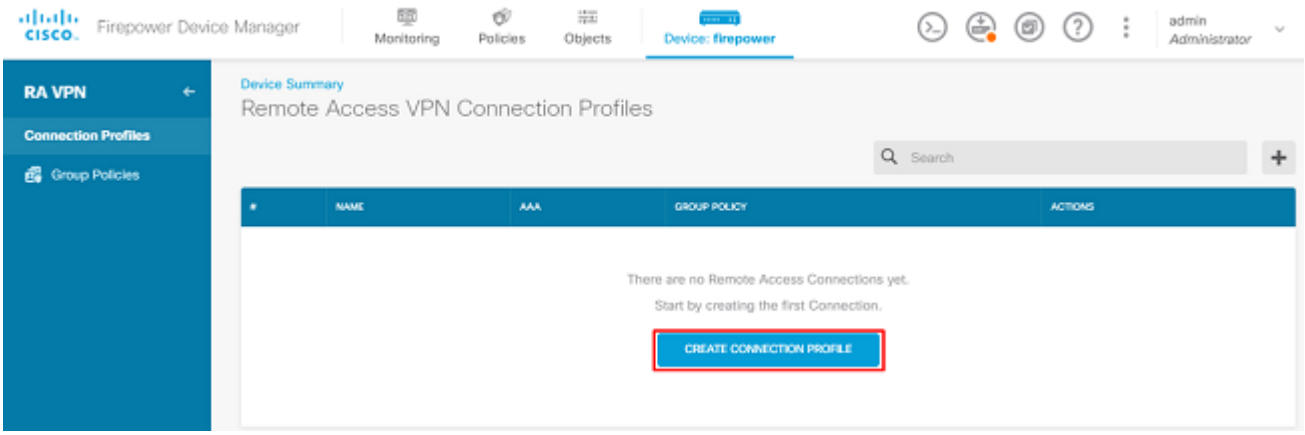
证书和密钥可以通过复制和粘贴或每个文件的上传按钮上传，如图所示。



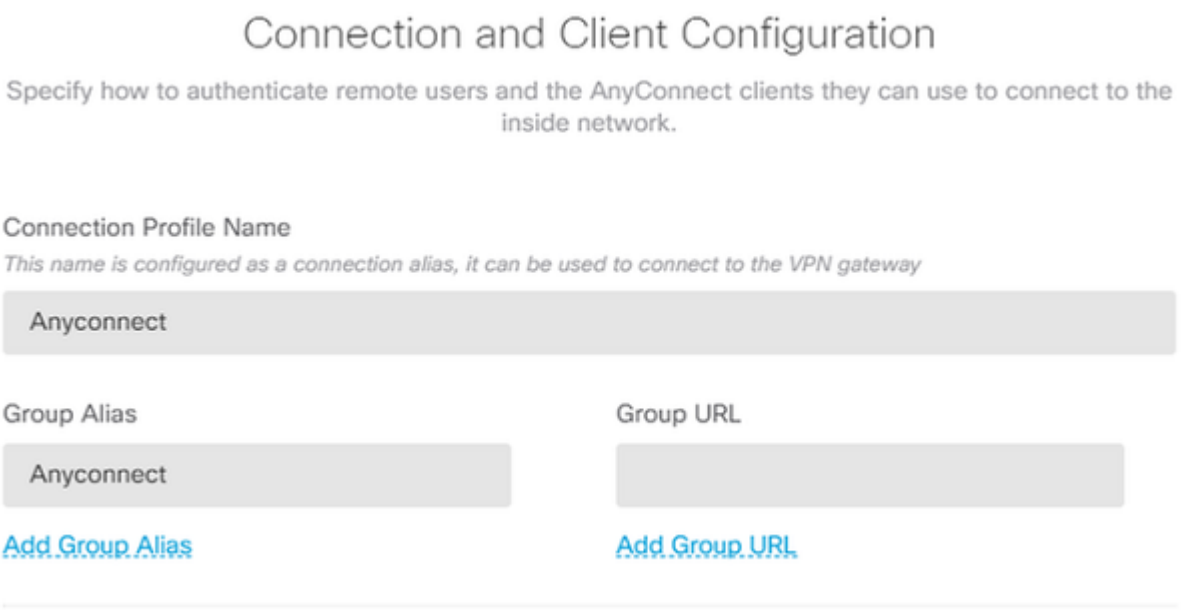
配置远程访问VPN

导航到Remote Access VPN > Create Connection Profile。在FDM上浏览RA VPN向导，如图所示。

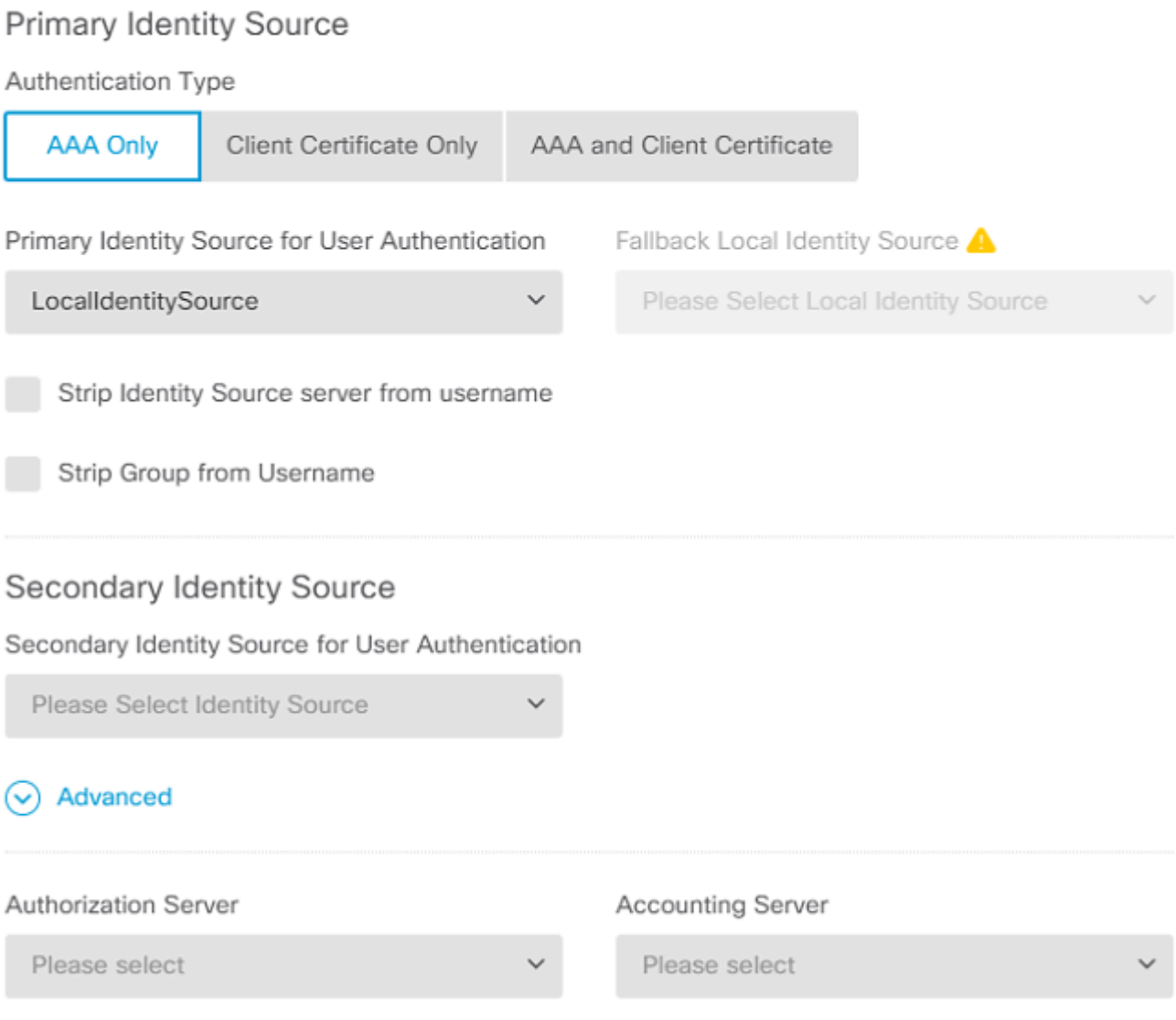




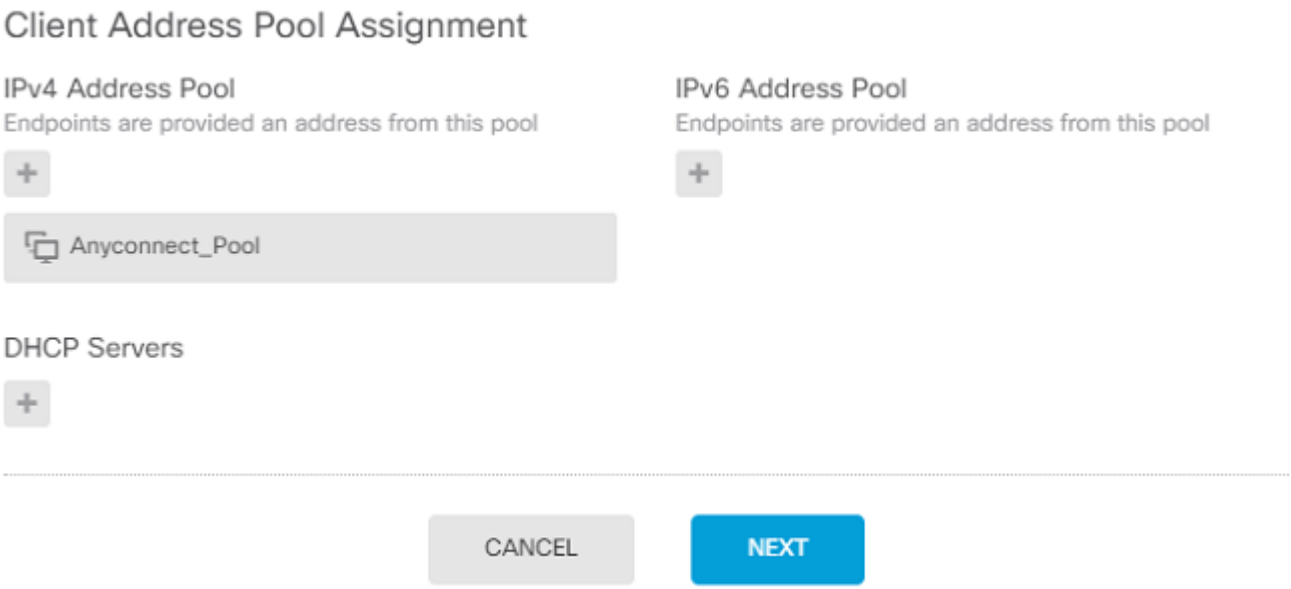
创建连接配置文件并启动配置，如图所示。



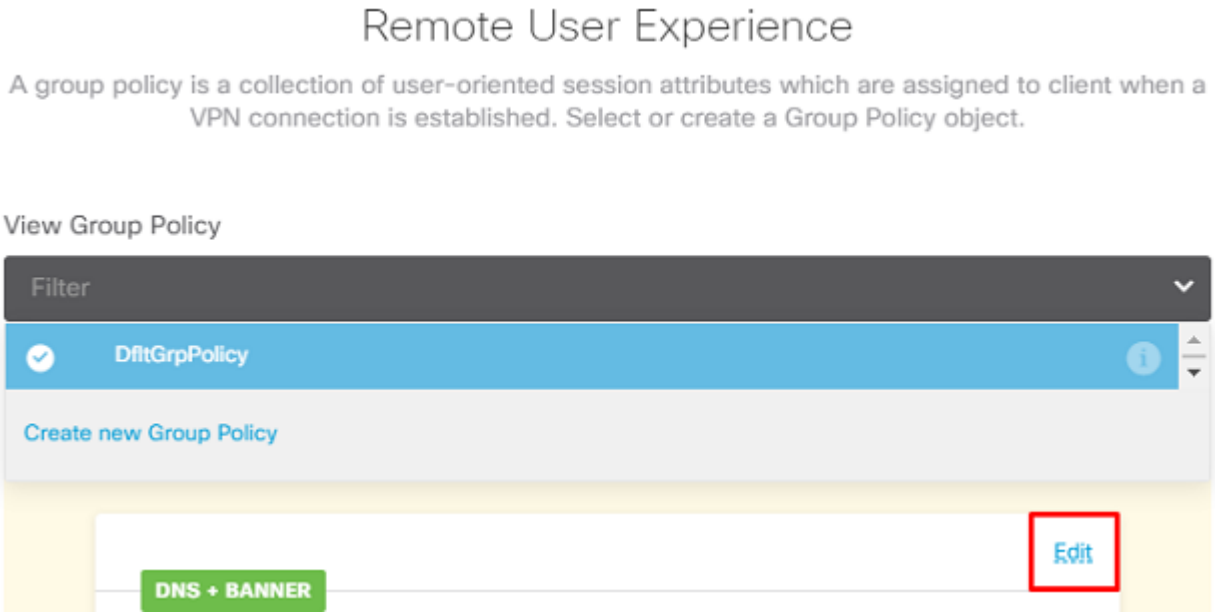
选择身份验证方法，如图所示。本指南使用本地身份验证。



选择Anyconnect_Pool（如图所示）对象。



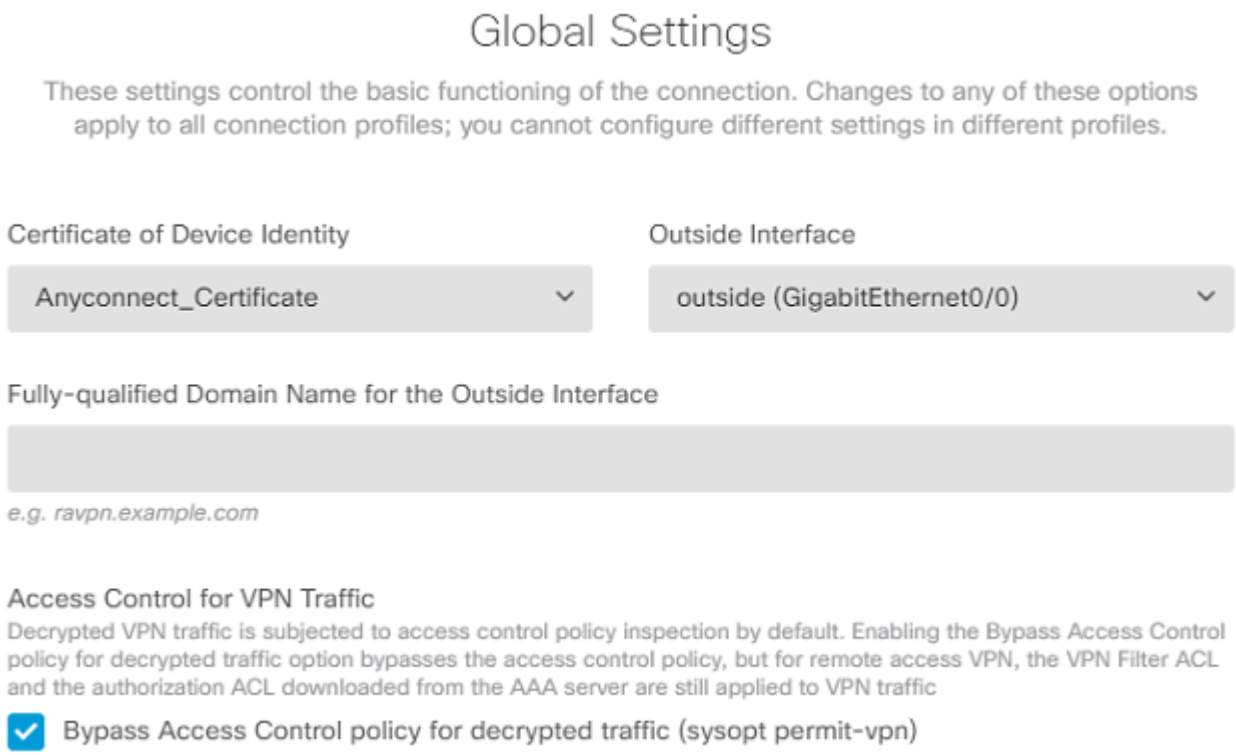
默认组策略的摘要显示在下一页上。当您点击下拉菜单并选择选项时，可以创建新的组策略Create a new Group Policy。在本指南中，使用默认组策略。选择策略顶部的edit选项，如图所示。



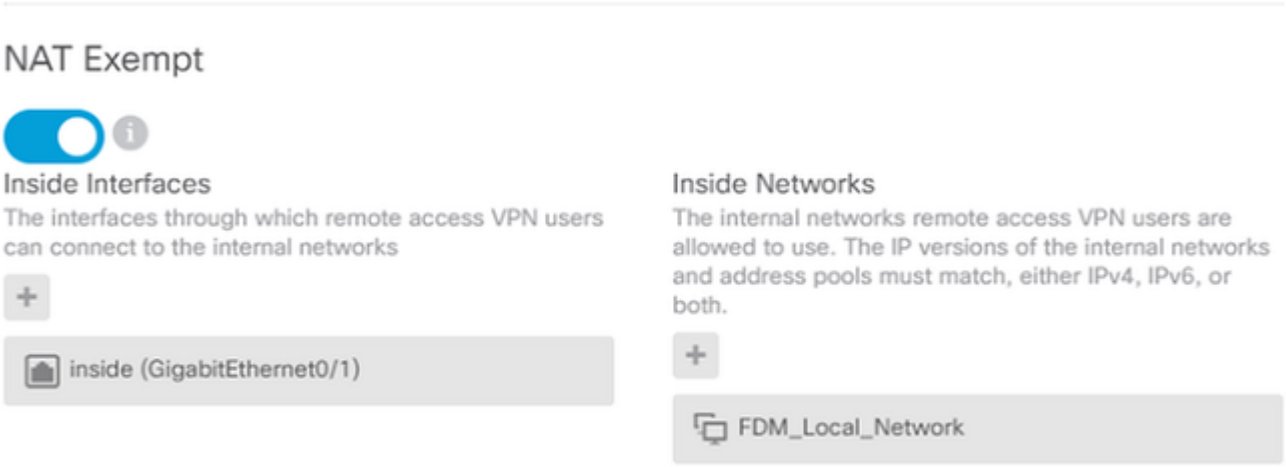
在组策略中，添加Split tunneling，以便连接到AnyConnect的用户仅通过AnyConnect客户端发送发往内部FTD网络的流量，而所有其他流量均流出用户的ISP连接，如图所示。



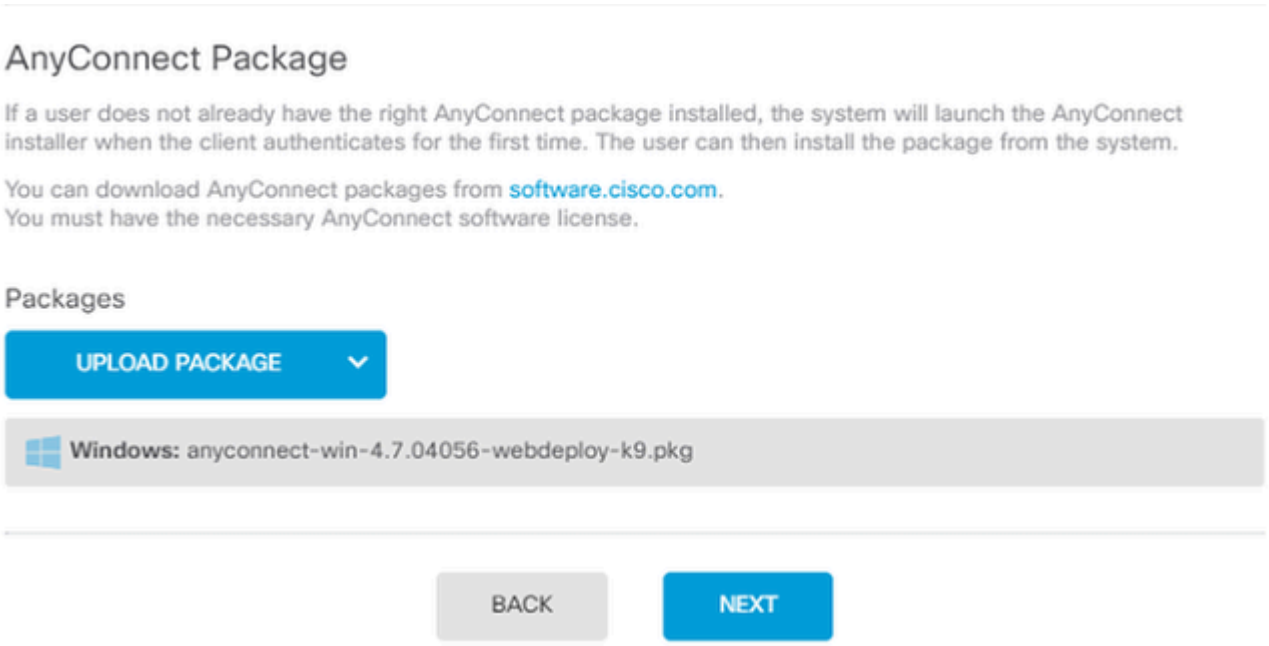
在下一页上，选择证书部分中添加的Anyconnect_Certificate。下一步，选择FTD侦听AnyConnect连接的接口。选择Bypass Access Control策略用于解密的流量(sysopt permit-vpn)。 如果未选择，则这是一sysopt permit-vpn个可选命令。必须创建访问控制策略，以允许来自AnyConnect客户端的流量访问内部网络，如图所示。



可以在下手动配置NAT免除Policies > NAT，也可以由向导自动配置。选择内部接口和网络,AnyConnect客户端需要这些网络才能访问，如图所示。



为用户可以连接的每个操作系统(Windows/Mac/Linux)选择AnyConnect软件包，如图所示。

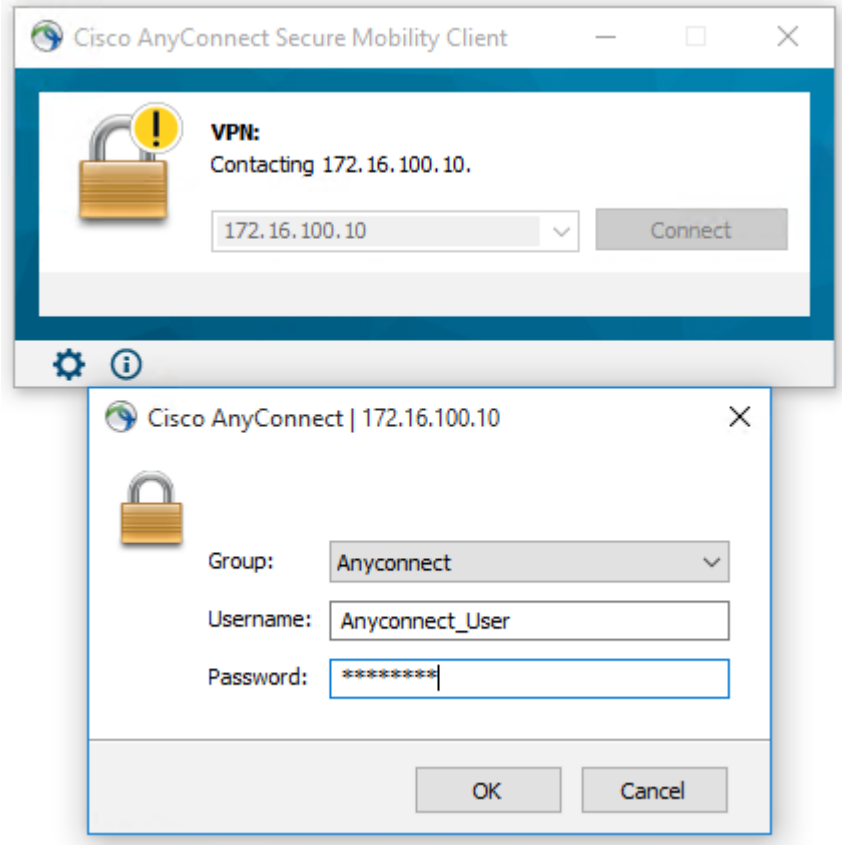


最后一页提供了整个配置的摘要。确认已设置正确的参数，然后点击Finish按钮并Deploy新配置。

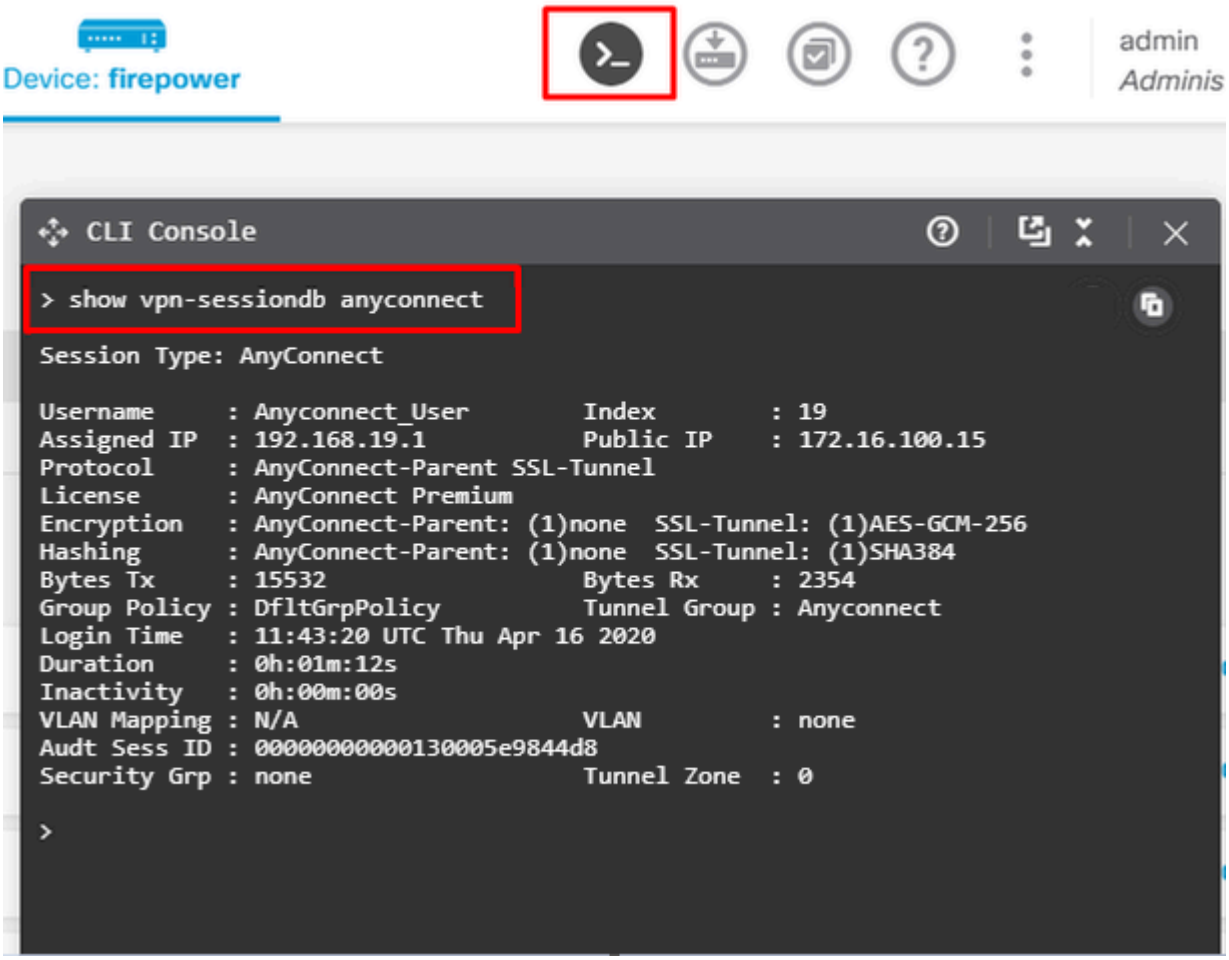
验证

使用本部分可确认配置能否正常运行。

部署配置后，尝试连接。如果您的FQDN解析为FTD的外部IP，请在AnyConnect连接框中输入它。在本示例中，使用FTD的外部IP地址。使用在FDM的对象部分中创建的用户名/密码，如图所示。



从FDM 6.5.0开始，无法通过FDM GUI监视AnyConnect用户。唯一的选项是通过CLI监控AnyConnect用户。FDM GUI的CLI控制台也可用于验证用户是否已连接。使用此命令， Show vpn-sessiondb anyconnect.



同一命令可以直接从CLI运行。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Anyconnect_User        Index        : 15
Assigned IP  : 192.168.19.1           Public IP    : 172.16.100.15
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 38830                  Bytes Rx     : 172
Group Policy : DfltGrpPolicy          Tunnel Group : Anyconnect
Login Time   : 01:08:10 UTC Thu Apr 9 2020
Duration     : 0h:00m:53s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000f0005e8e757a
Security Grp : none                   Tunnel Zone  : 0
```

故障排除

本节提供可用于对配置进行故障排除的信息。

如果用户无法通过SSL连接到FTD，请执行以下步骤以隔离SSL协商问题：

1. 验证可以通过用户的计算机ping FTD以外的IP地址。
2. 使用外部嗅探器验证TCP三次握手是否成功。

AnyConnect客户端问题

本部分提供了对两个最常见的AnyConnect VPN客户端问题进行故障排除的指南。有关AnyConnect客户端的故障排除指南，请参阅AnyConnect VPN客户端故障排除指南。

初始连接问题

如果用户存在初始连接问题，请在FTD上启用debug webvpn AnyConnect并分析调试消息。调试必须在FTD的CLI上运行。使用命令debug webvpn anyconnect 255。从客户端计算机收集DART捆绑包，以便从AnyConnect获取日志。有关如何收集DART捆绑包的说明，请参阅以下内容：收集DART捆绑包。

特定流量问题

如果连接成功，但流量在SSL VPN隧道上失败，请查看客户端上的流量统计信息，以验证客户端正在接收和传输流量。详细的客户端统计信息在AnyConnect的所有版本中均可用。如果客户端显示正在发送和接收流量，请检查FTD中是否有已接收和已传输的流量。如果FTD应用过滤器，则会显示过滤器名称，您可以查看ACL条目以检查您的流量是否被丢弃。用户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。

有关由FDM管理的FTD上的远程访问VPN的详细信息，请在此找到完整配置指南：由FDM管理的远程访问FTD。

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）。