在FTD上配置安全客户端(AnyConnect)远程访问VPN

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 1.必备条件
  - a)导入SSL证书
  - b)配置RADIUS服务器
  - c)为VPN用户创建地址池
  - d)创建XML配置文件
  - e)上传AnyConnect映像
- 2.远程访问向导

连接

限制

安全考虑

- a)启用uRPF
- b)启用sysopt connection permit-vpnOption

相关信息

简介

本文档介绍在安全防火墙威胁防御上配置安全客户端(AnyConnect)远程访问VPN。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本VPN、TLS和IKEv2知识
- 基本身份验证、授权和记帐(AAA)以及RADIUS知识

- 使用安全防火墙管理中心的经验

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全防火墙威胁防御(SFTD)7.2.5
- 安全防火墙管理中心(SFMC)7.2.9
- 安全客户端(AnyConnect)5.1.6

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

本文档提供了安全防火墙威胁防御(FTD)版本7.2.5及更高版本的配置示例，允许远程访问VPN使用传输层安全(TLS)和Internet密钥交换版本2(IKEv2)。 作为客户端，可以使用安全客户端(AnyConnect)，这可在多个平台上受支持。

配置

1.先决条件

要通过Secure Firewall Management Center中的Remote Access（远程访问）向导，请执行以下操作：

- 创建用于服务器身份验证的证书。
- 配置RADIUS或LDAP服务器以进行用户身份验证。
- 为VPN用户创建地址池。
- 上传不同平台的AnyConnect映像。

a)导入SSL证书

配置安全客户端时，证书至关重要。证书必须具有DNS名称和/或IP地址的主题备用名称扩展名以避

免在Web浏览器中出错。

> 注意：只有注册的思科用户才能访问内部工具和漏洞信息。

手动证书注册存在限制：

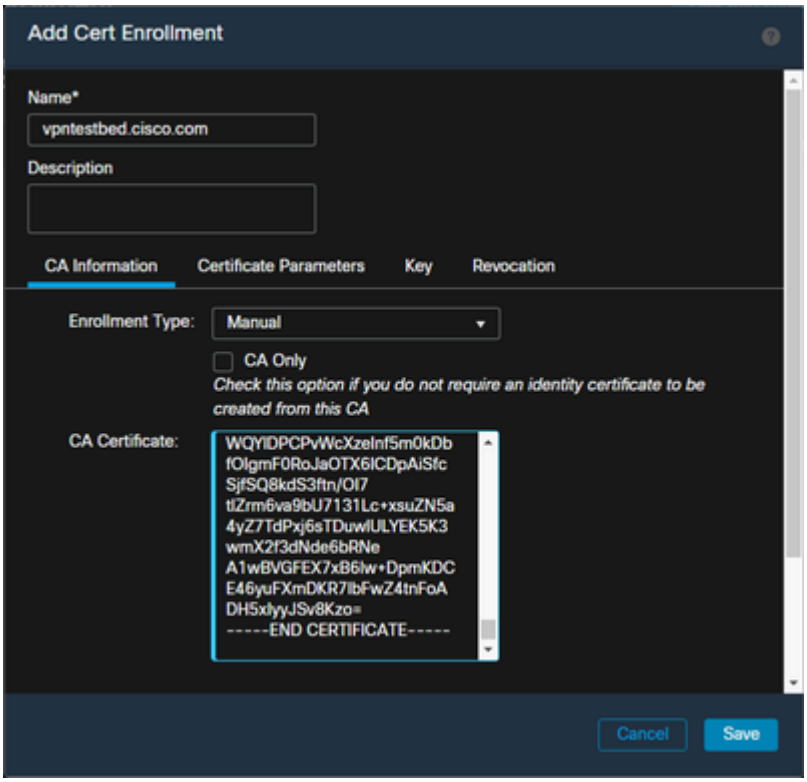
- 在SFTD上，在生成CSR之前需要CA证书。
- 如果CSR是在外部生成的，则手动方法会失败，因此必须使用其他方法(PKCS12)。

在SFTD设备上获取证书有多种方法，但安全且简单的方法是创建证书签名请求(CSR)，使用证书颁发机构(CA)对其进行签名，然后导入CSR中针对公钥颁发的证书。

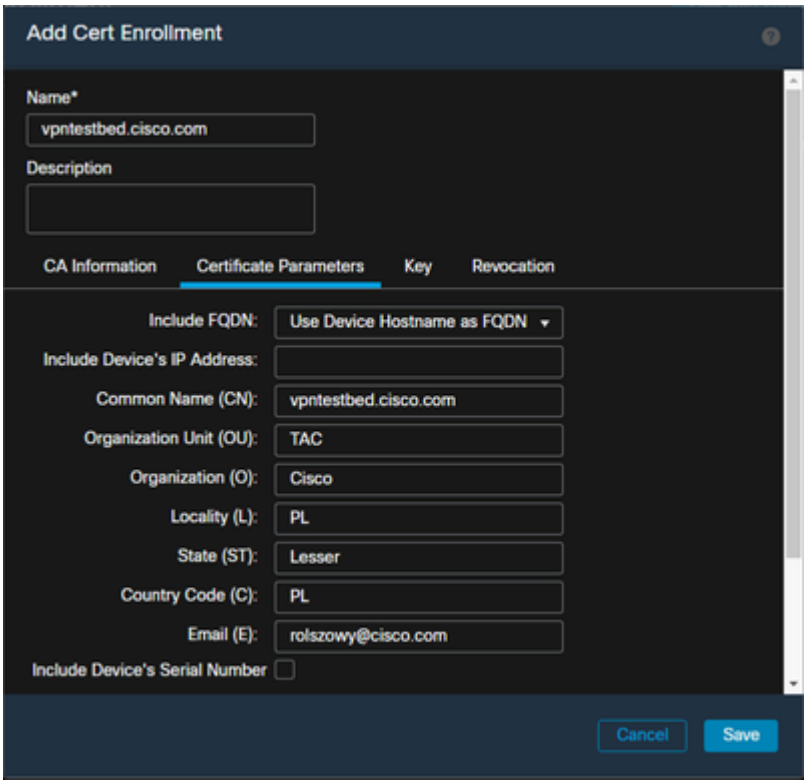
要完成的步骤：

- 导航到Objects > Object Management > PKI > Cert Enrollment，然后单击Add Cert Enrollment。

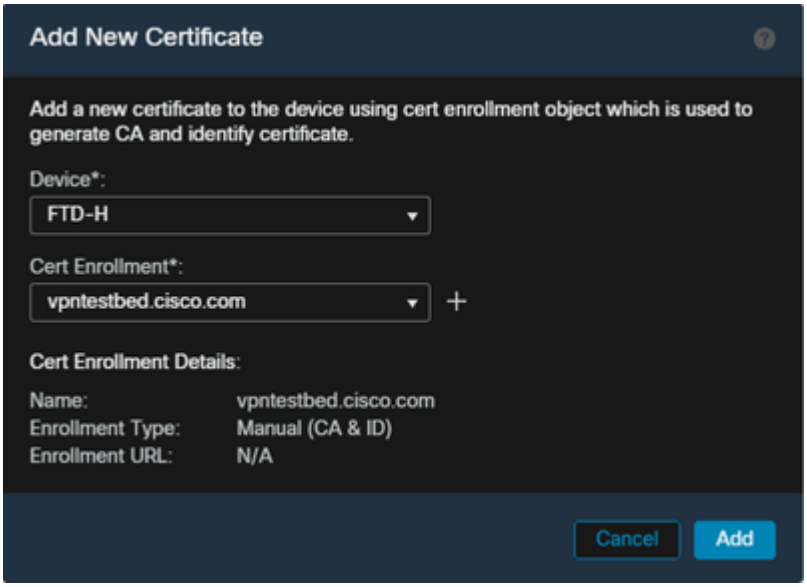
- 选择Enrollment Type并粘贴Certificate Authority(CA)证书（用于签署CSR的证书）。



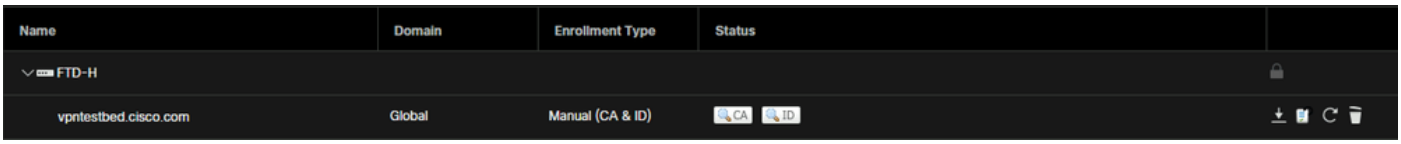
- 然后，转到第二个选项卡，选择Custom FQDN并填写所有必要的字段，例如：



- 在第三个选项卡上，选择Key Type，选择name和size。对于RSA，最少2048位。
- 单击Save并导航到Devices > Certificates > Add。
- 然后选择Device，在Cert Enrollment下，选择您刚刚创建的信任点，然后单击Add:

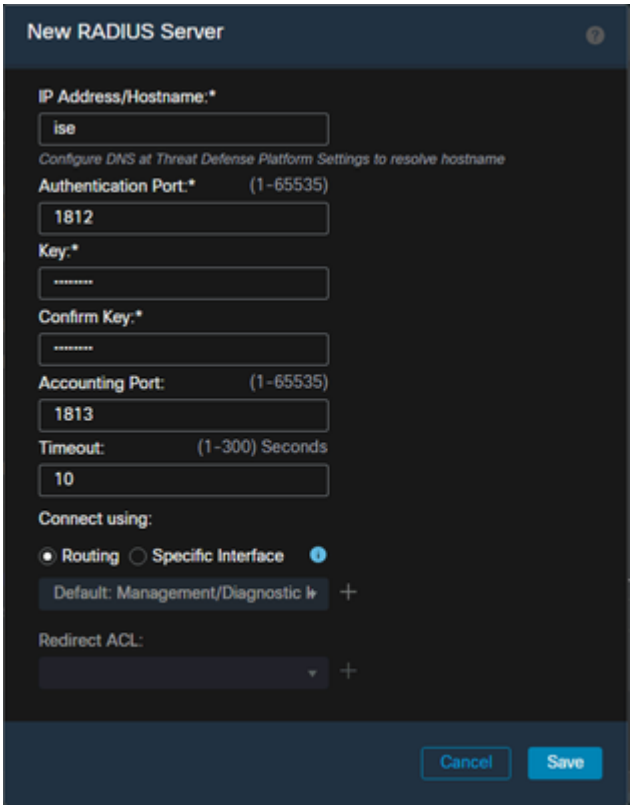


- 之后，点击信任点名称旁边的 ID 图标，然后是，之后将CSR复制到CA并签名。证书的属性必须与普通HTTPS服务器相同。
- 从CA收到base64格式的证书后，选择Browse Identity Certificate，从磁盘中进行选择，然后单击Import。当此操作成功时，您会看到：



b)配置RADIUS服务器

- 导航到Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group > +。
- 填写名称并添加IP地址以及共享密钥，然后单击保存:

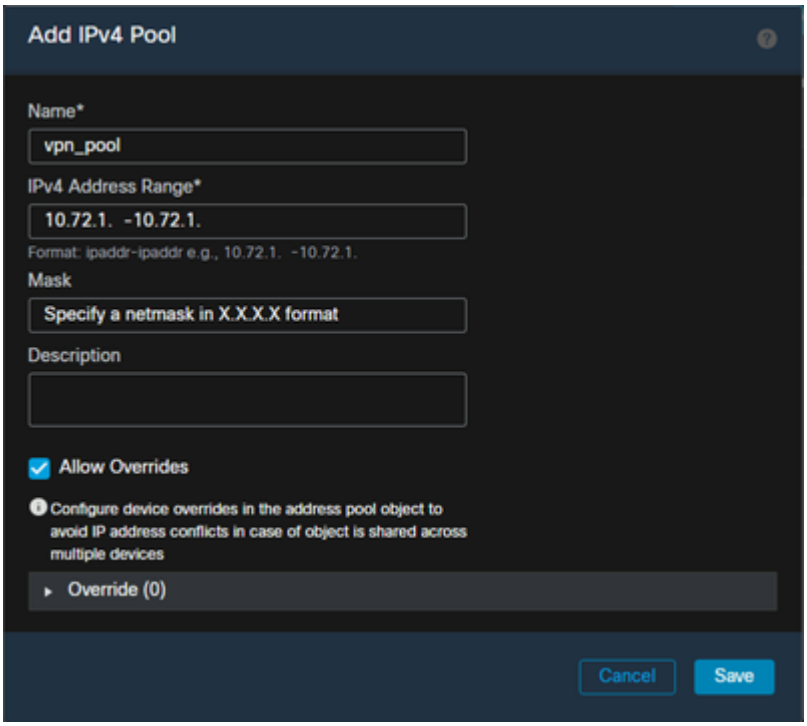


- 之后，您可以在列表中看到服务器：



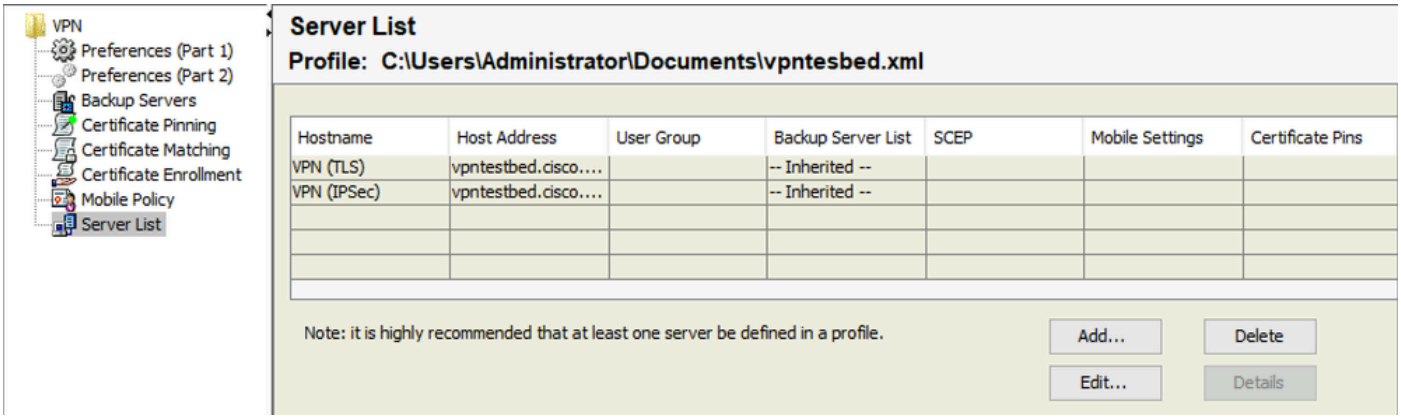
c)为VPN用户创建地址池

- 导航到Objects > Object Management > Address Pools > IPv4 Pools > Add IPv4 Pools。
- 输入名称和范围，不需要掩码：



d)创建XML配置文件

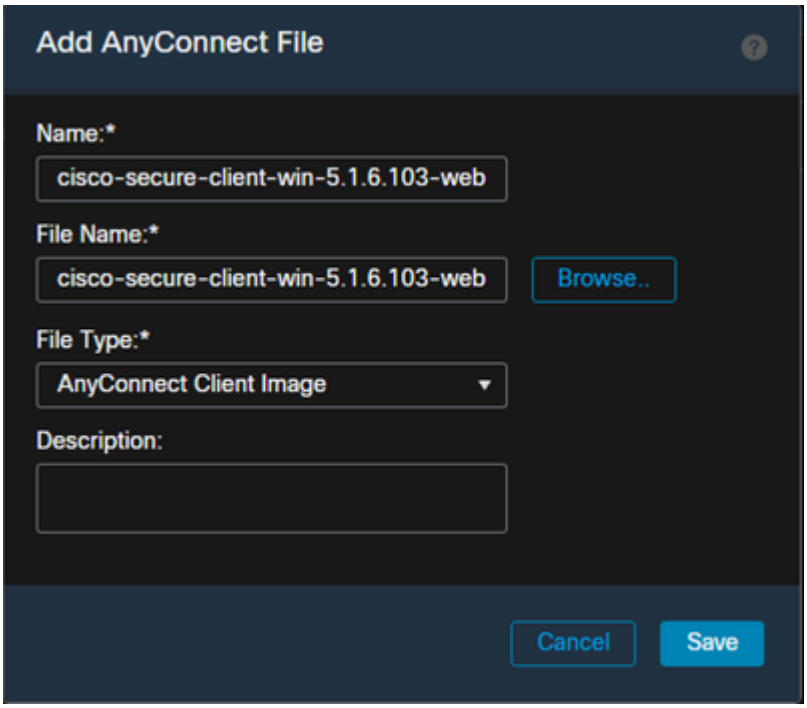
- 从思科站点下载配置文件编辑器并打开它。
- 导航到服务器列表>添加……
- 输入Display Name和FQDN。您可以在服务器列表中看到以下条目：



- 单击OK和File > Save as...

e)上传AnyConnect映像

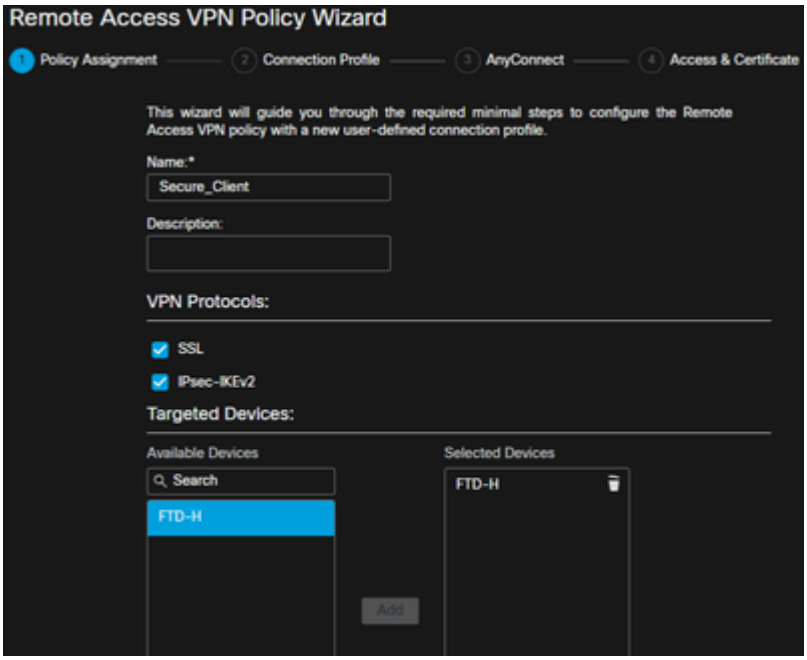
- 从思科站点下载软件包映像。
- 导航到Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。
- 键入名称并从磁盘中选择PKG文件，然后单击Save:



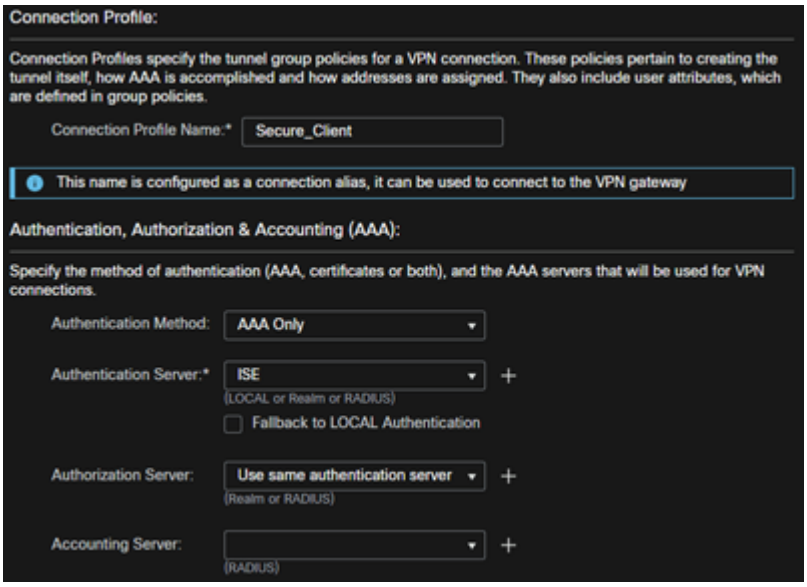
- 根据您自己的要求添加更多软件包。

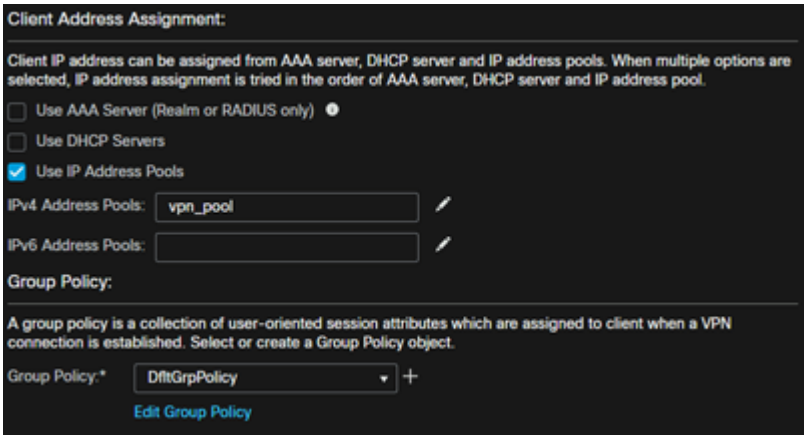
2.远程访问向导

- 导航到设备 > VPN > 远程访问 > 添加新配置。
- 为配置文件命名并选择FTD设备:

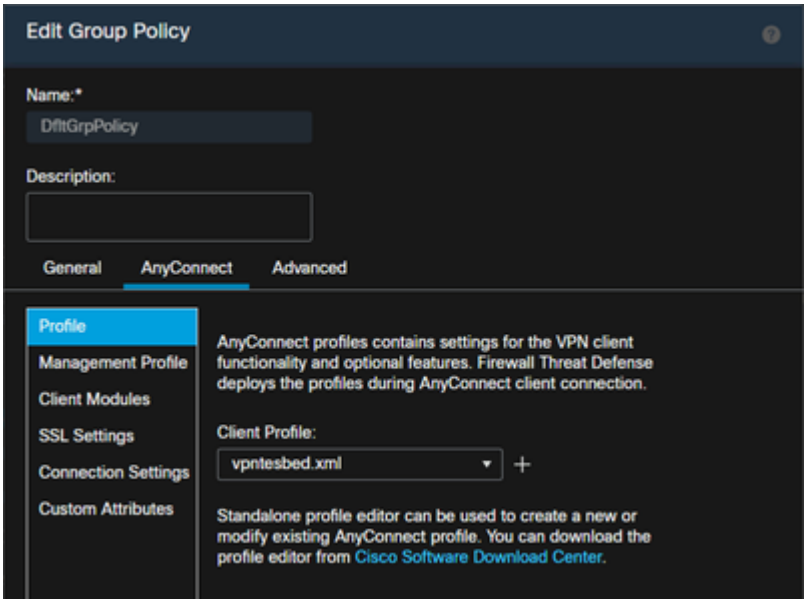


- 在Connection Profile步骤中，键入Connection Profile Name，选择之前创建的Authentication Server和Address Pools:

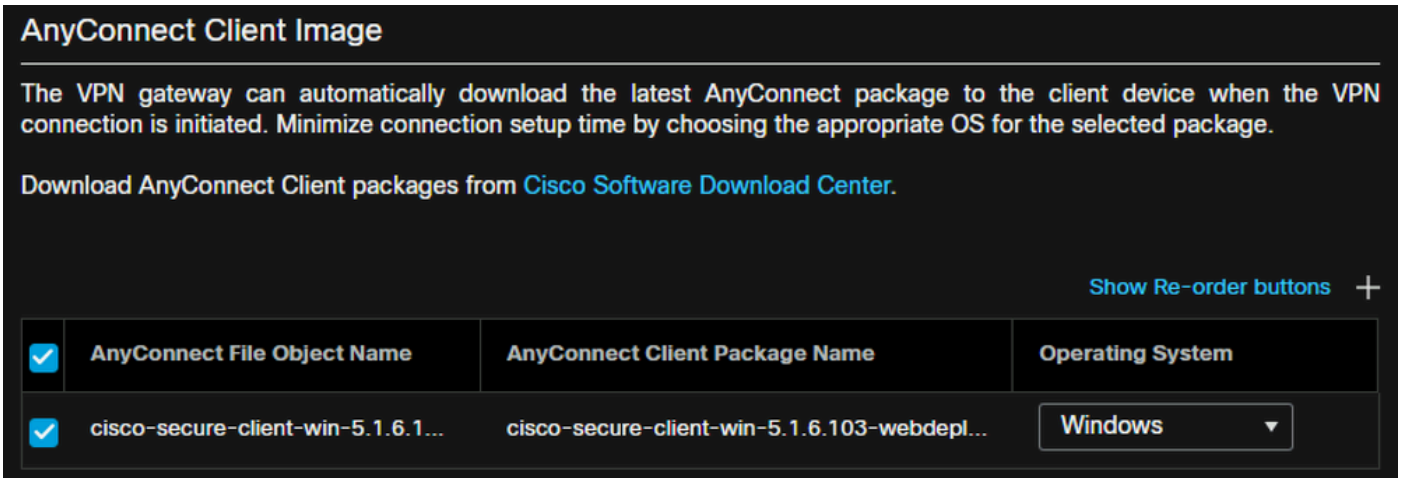




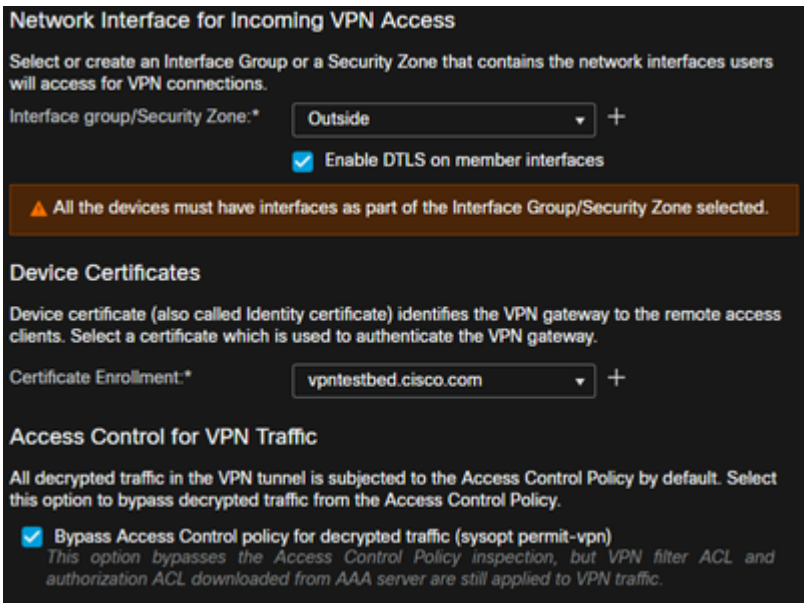
- 单击Edit Group Policy，然后在AnyConnect选项卡上选择Client Profile，然后单击Save:



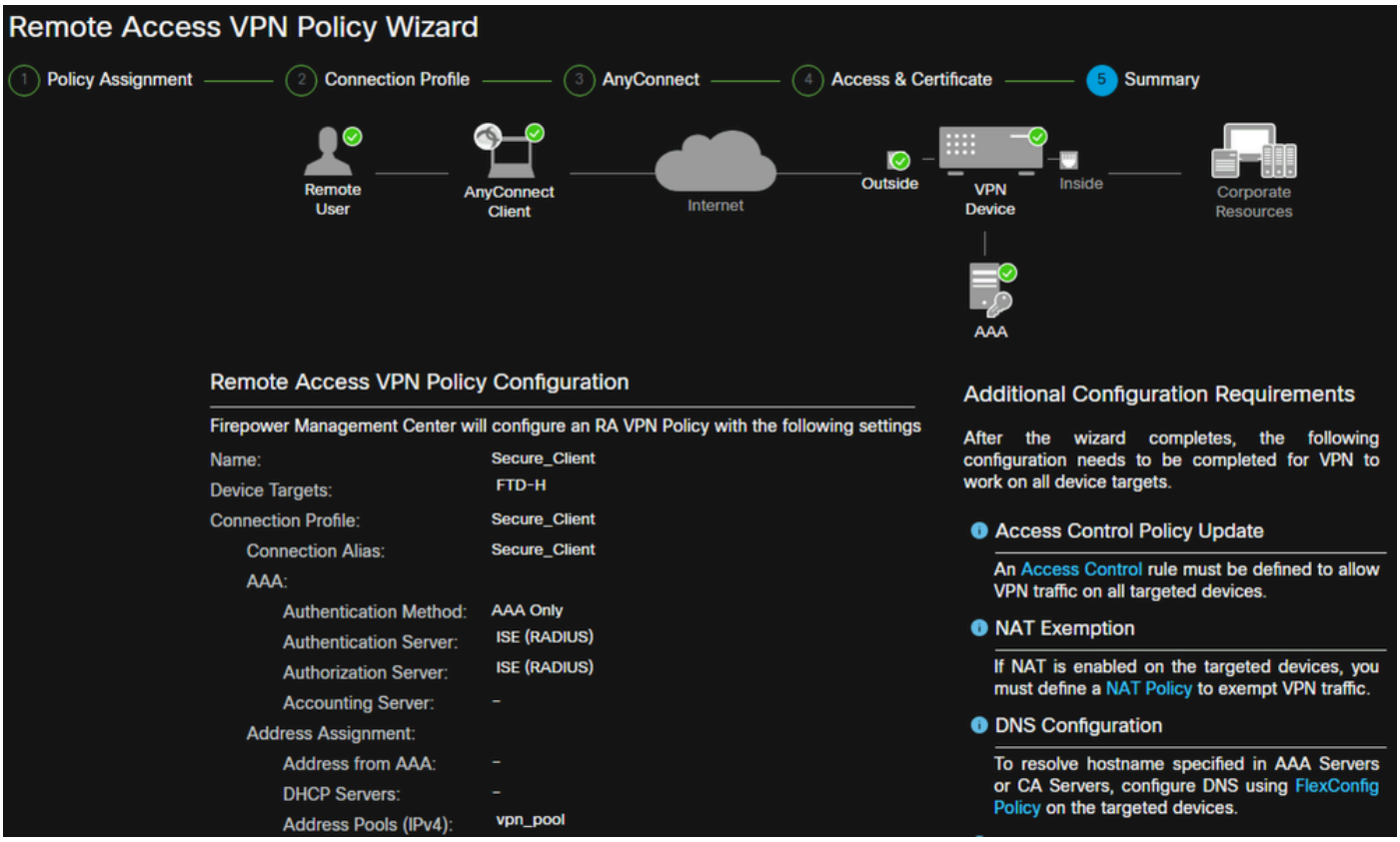
- 在下一页上，选择AnyConnect Images，然后单击Next。



- 在下一个屏幕上，选择Network Interface and Device Certificates:



- 当所有配置都正确时，可以单击Finish，然后单击Deploy:



- 这会将整个配置、证书和AnyConnect软件包复制到FTD设备。

连接

要连接到FTD，必须打开浏览器，键入指向外部接口的DNS名称或IP地址。然后，使用RADIUS服务器中存储的凭据登录，并在屏幕上执行这些步骤。安装AnyConnect后，必须在AnyConnect窗口中输入相同的地址，然后单击Connect。

限制

目前，在FTD上不受支持，但在ASA上可用：

- FTDposture VPN不支持通过动态授权或RADIUS授权更改(CoA)进行组策略更改

- AnyConnect自定义(增强功能：Cisco bug ID CSCvq87631)
- AnyConnect脚本(增强功能：Cisco Bug ID CSCvt58044)
- AnyConnect本地化
- WSA集成
- RA和L2L VPN同步IKEv2动态加密映射(增强功能：Cisco Bug ID CSCvr52047)
- TACACS、Kerberos - KCD身份验证和RSA SDI(增强功能：Cisco Bug ID CSCvx55859)
- 浏览器代理

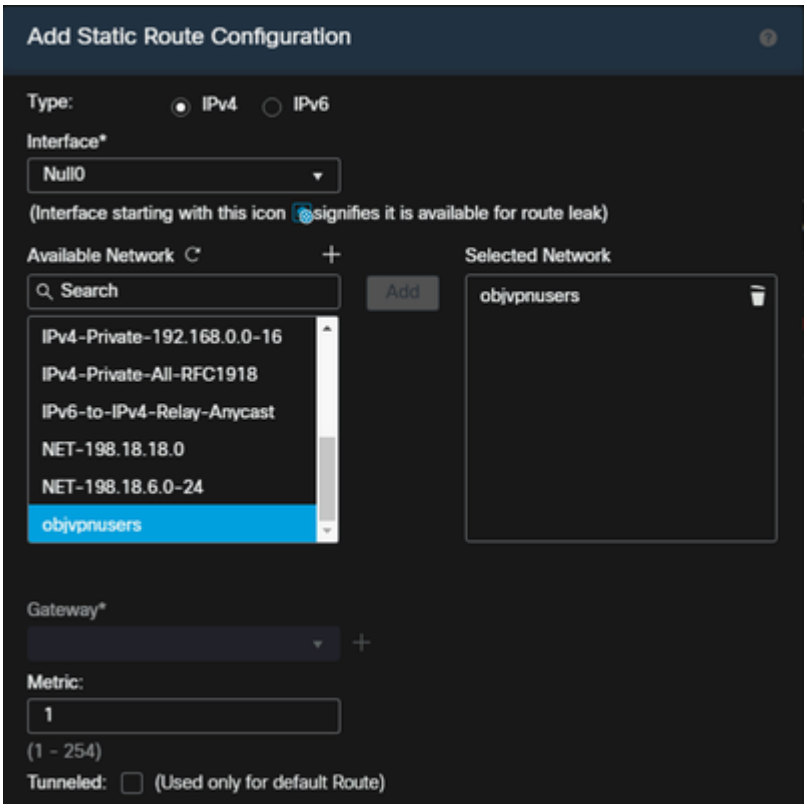
安全考虑

默认情况下，sysopt connection permit-vpnoption处于禁用状态。这意味着必须允许来自外部接口上的地址池的流量通过访问控制策略。虽然添加预过滤器或访问控制规则以仅允许VPN流量，但如果明文流量与规则条件匹配，则会错误地允许该流量。

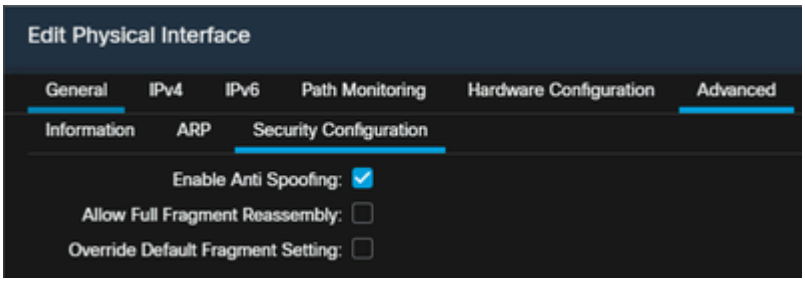
有两种方法可以解决此问题。首先，TAC推荐的选项是为外部接口启用反欺骗（在ASA上称为单播反向路径转发 — uRPF）；其次，启用sysopt connection permit-vpn以完全绕过Snort检查。第一个选项允许对进出VPN用户的流量进行正常检查。

a)启用uRPF

- 为C部分中定义的用于远程访问用户的网络创建空路由。导航到Devices > Device Management > Edit > Routing > Static Route，然后选择Add route。



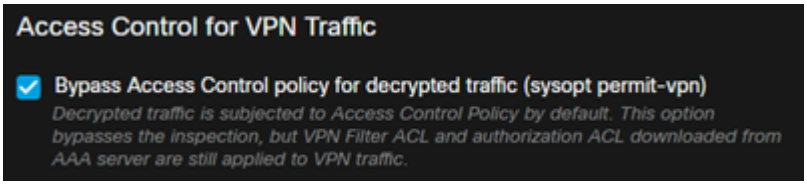
- 接下来，在VPN连接终止的接口上启用uRPF。要查找此信息，请导航到Devices > Device Management > Edit > Interfaces > Edit > Advanced > Security Configuration > Enable Anti Spoofing。



当用户连接时，路由表中会为该用户安装32位路由。来自uRFP丢弃的池中其他未使用IP地址的明文流量。要查看反欺骗的说明，请参阅[在防火墙威胁防御上设置安全配置参数。]

b)启用sysopt connection permit-vpn选项

- 在向导或设备(Devices)> VPN >远程访问(Remote Access)> VPN配置文件(VPN Profile)>访问接口(Access Interfaces)下，有一个选项可以完成。



相关信息

- 思科技术支持和下载

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）。