在安全防火墙上配置安全客户端VPN管理隧道

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 限制

配置

- 配置
  - 步骤1.创建AnyConnect管理VPN配置文件
  - 步骤2.创建AnyConnect VPN配置文件
  - 步骤3.将AnyConnect管理VPN配置文件和AnyConnect VPN配置文件上传到FMC
  - 步骤4.创建组策略
  - 步骤5.创建新的AnyConnect配置
  - 步骤6.创建URL对象
  - 步骤7.定义URL别名

验证

故障排除

简介

本文档介绍如何在Cisco FMC管理的安全防火墙威胁防御上配置安全客户端VPN管理隧道。

先决条件

要求

Cisco 建议您了解以下主题：

- 客户端证书身份验证
- Cisco AnyConnect配置文件编辑器
- 通过防火墙管理中心(FMC)配置SSL AnyConnect

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FMC版本6.7.0（内部版本65）
- 思科防火墙威胁防御(FTD)版本6.7.0（内部版本65）
- Cisco AnyConnect 4.9.01095安装在Windows 10计算机上

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

在本示例中，安全套接字层(SSL)用于在FTD和Windows 10客户端之间创建虚拟专用网络(VPN)。

从版本6.7开始，Cisco FTD支持AnyConnect管理隧道的配置。此修复以前打开的增强请求Cisco bug ID CSCvs78215。

AnyConnect管理功能允许您在终端完成启动后立即创建VPN隧道。用户无需手动启动AnyConnect应用。一旦系统通电，AnyConnect VPN代理服务将检测管理VPN功能，并使用主机条目（在AnyConnect管理VPN配置文件的服务器列表中定义）启动AnyConnect会话。

限制

- 仅支持客户端证书身份验证。
- Windows客户端仅支持计算机证书存储区。
- Cisco Firepower设备管理器(FDM)Cisco Bug ID CSCvx90058不支持。
- 不支持Linux客户端。

Cisco Secure Client Administrator Guide，Release 5中所述的全部限制。

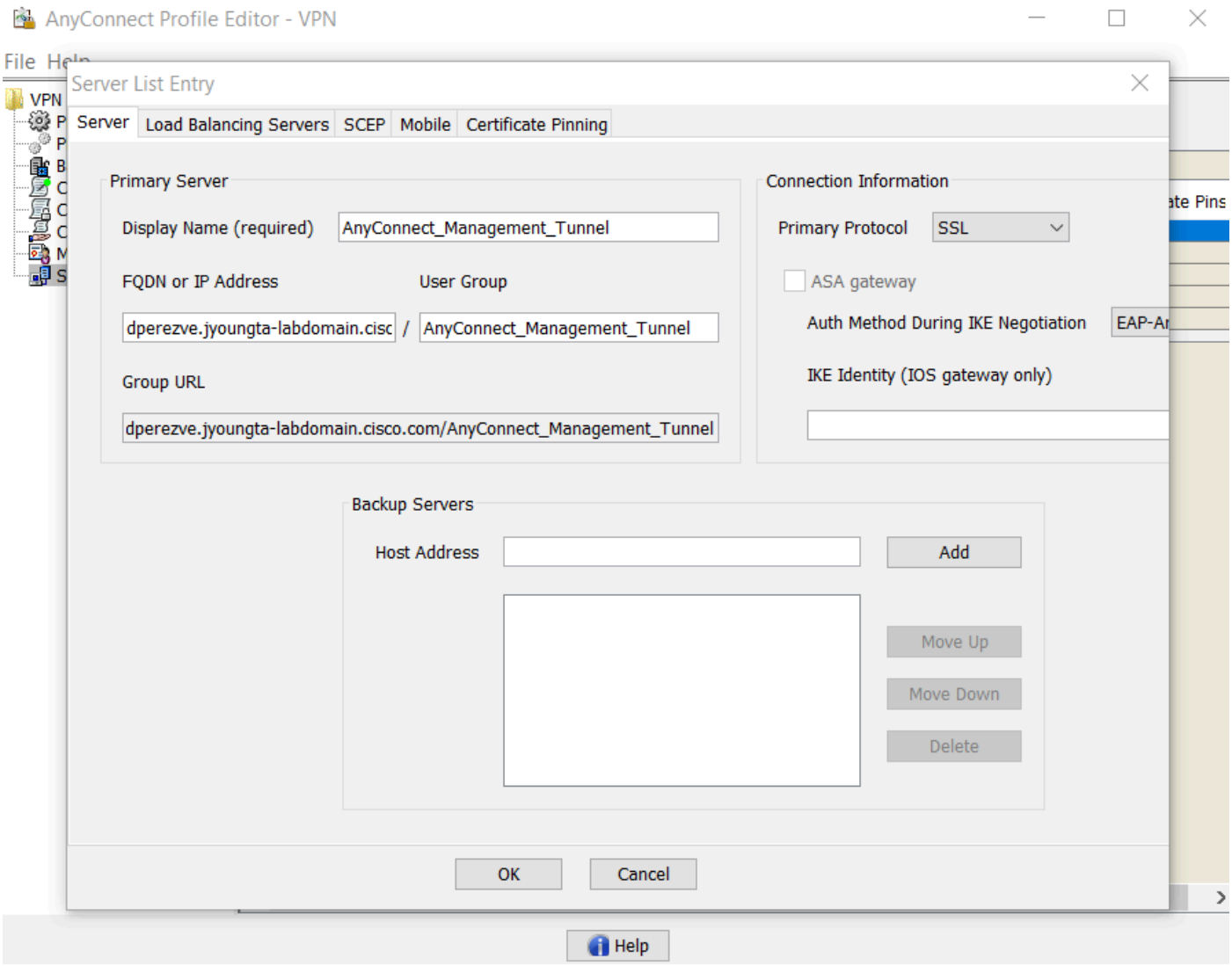
配置

配置

步骤1.创建AnyConnect管理VPN配置文件

打开AnyConnect配置文件编辑器以创建AnyConnect管理VPN配置文件。管理配置文件包含终端启动后用于建立VPN隧道的所有设置。

1.在本示例中，定义了“服务器列表”条目指向完全限定域名(FQDN)dperezve.jyoungta-labdomain.cisco.com，并且选择SSL作为主要协议。要添加服务器列表，请导航到服务器列表，然后选择添加按钮。填写必填字段并保存更改。

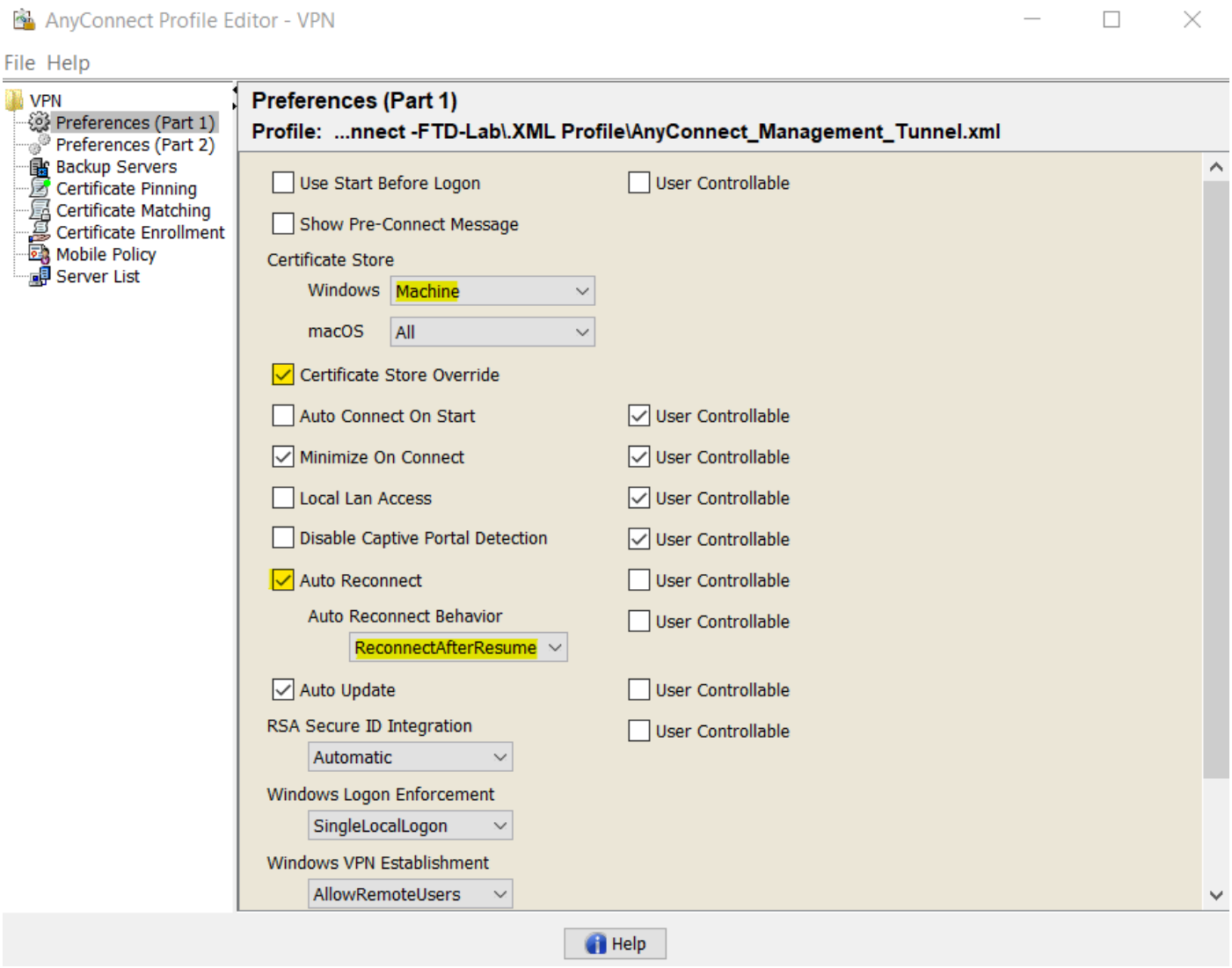


2.除服务器列表外，管理VPN配置文件还必须包含一些强制性首选项：

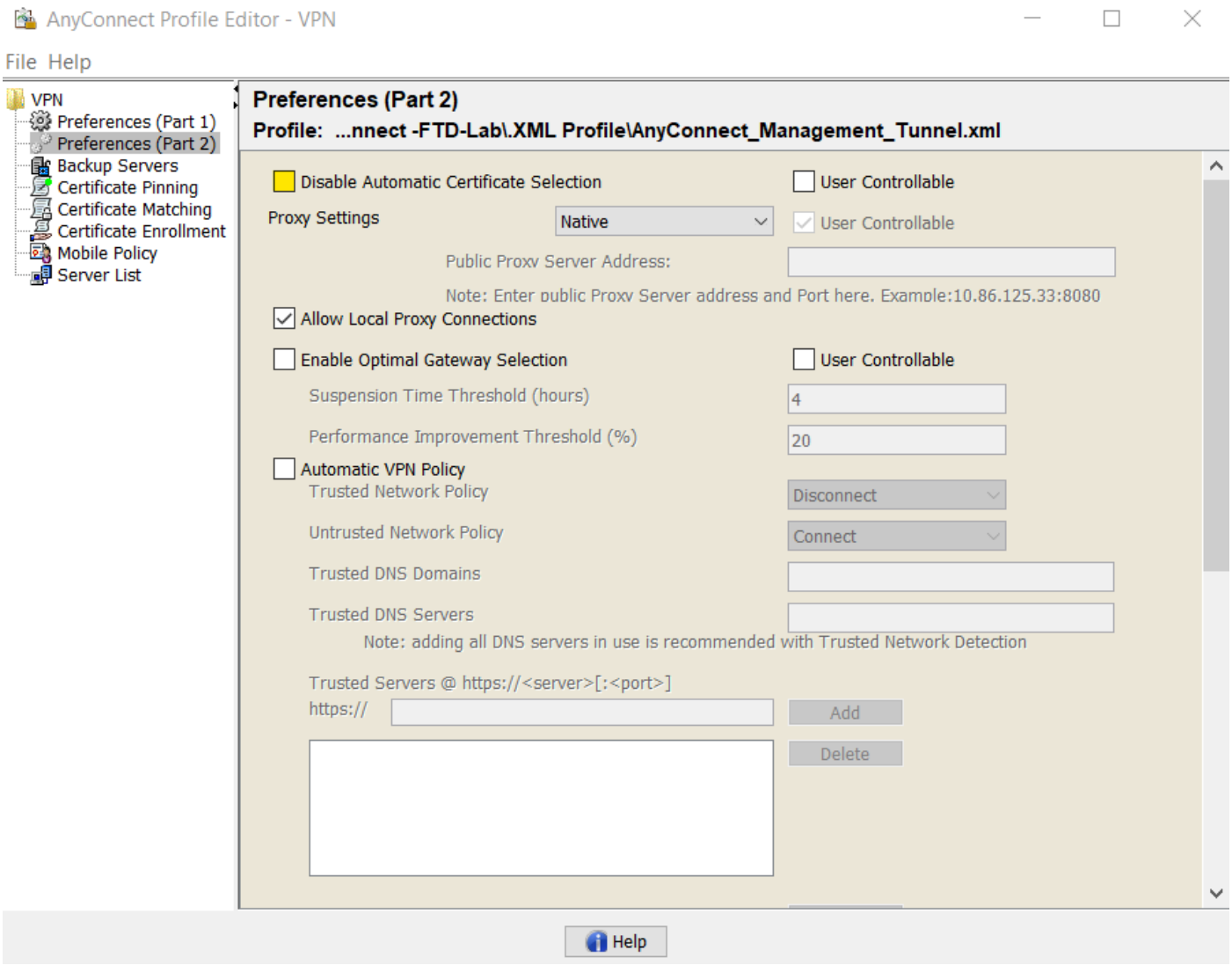
- AutomaticCertSelection必须设置为true。
- AutoReconnect必须设置为true。
- 必须为ReconnectAfterResume配置AutoReconnectBehavior。
- AutoUpdate必须设置为false。
- BlockUntrustedServers必须设置为true。
- 必须为MachineStore配置CertificateStore。

- CertificateStoreOverride必须设置为true。
- EnableAutomaticServerSelection必须设置为false。
- EnableScripting必须设置为false。
- RetainVPNOnLogoff必须设置为true。

3.在AnyConnect配置文件编辑器中，导航到首选项(第1部分)，然后调整设置，如图所示：



4.定位至首选项（第2部分）并取消选定禁用自动证书选择选项。



步骤2.创建AnyConnect VPN配置文件

作为管理VPN配置文件的补充，必须配置常规AnyConnect VPN配置文件。AnyConnect VPN配置文件用于第一次连接尝试。在此会话期间，会从FTD下载管理VPN配置文件。

使用AnyConnect配置文件编辑器创建AnyConnect VPN配置文件。在这种情况下，两个文件都包含相同的设置，因此可以使用相同的过程。

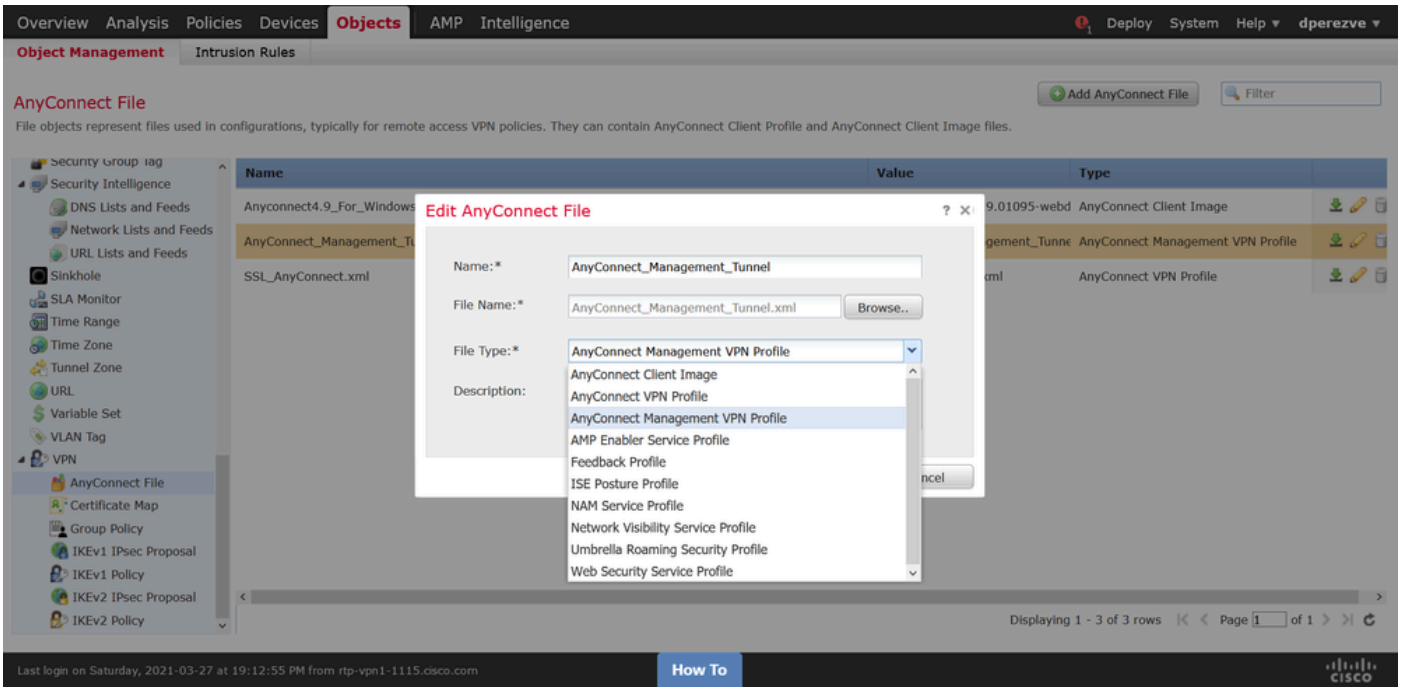
步骤3.将AnyConnect管理VPN配置文件和AnyConnect VPN配置文件上传到FMC

1.创建配置文件后，将这些配置文件作为AnyConnect文件对象上传到FMC。

2.要将新的AnyConnect管理VPN配置文件上传到FMC，请导航到对象>对象管理，然后从目录中选

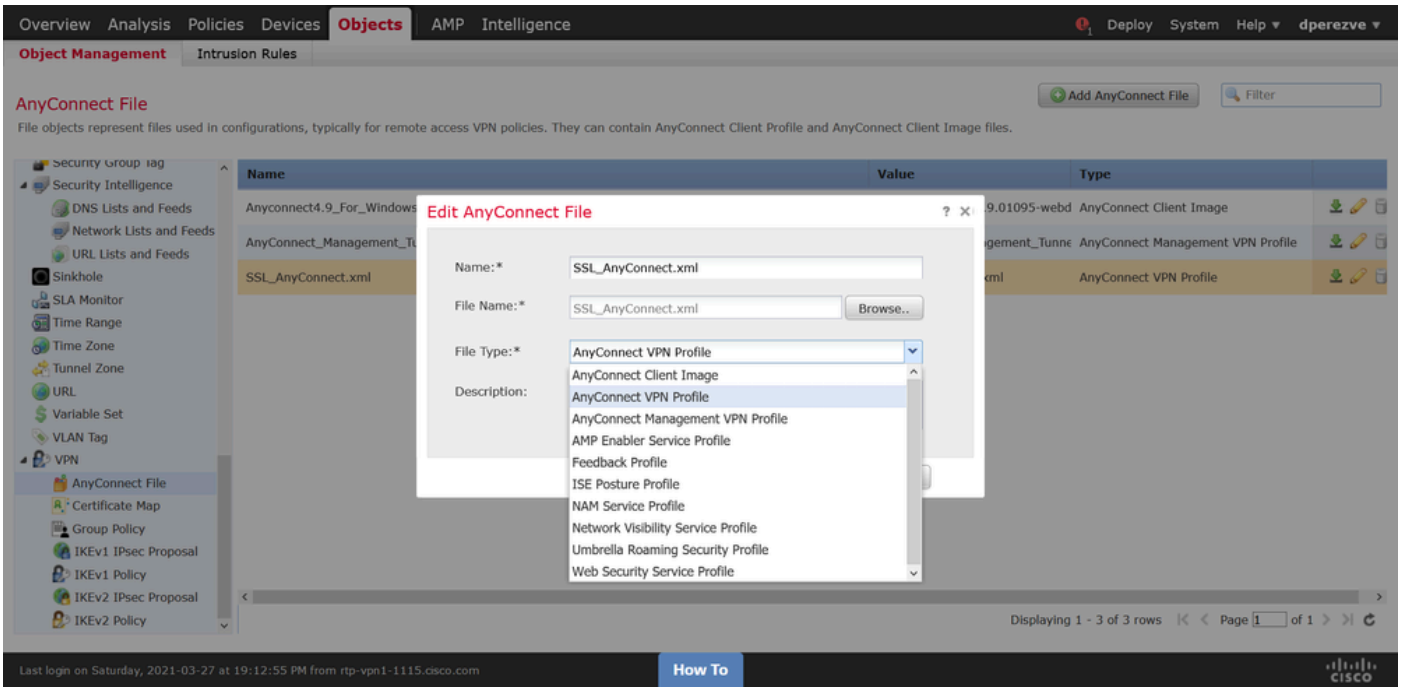
择VPN选项。选择Add AnyConnect File按钮。

3.提供文件的名称。选择AnyConnect Management VPN Profile作为文件类型并保存对象。

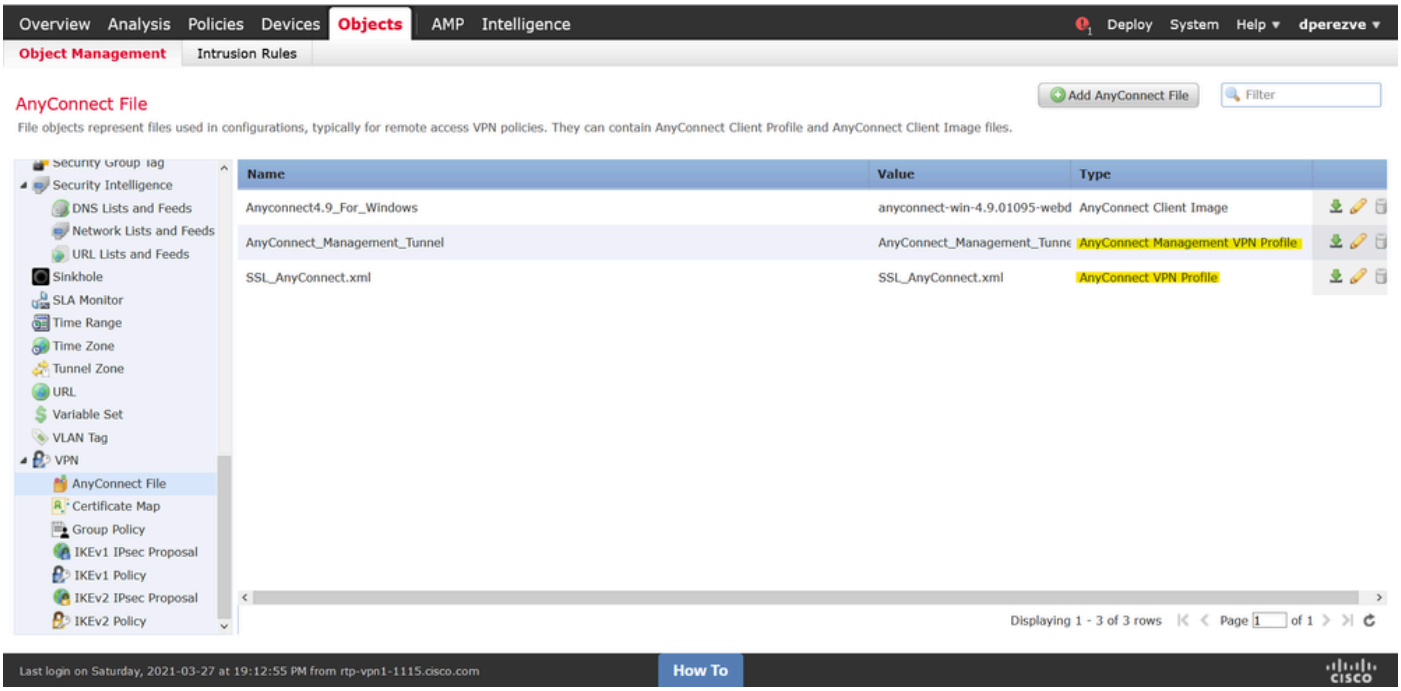


4.要上传AnyConnect VPN配置文件，请导航到对象>对象管理，然后从目录中选择VPN选项。选择Add AnyConnect File按钮。

5.提供文件的名称，此时，选择AnyConnect VPN配置文件作为文件类型并保存新对象。



6.必须将配置文件添加到对象列表，并分别标记为AnyConnect管理VPN配置文件和AnyConnect VPN配置文件。

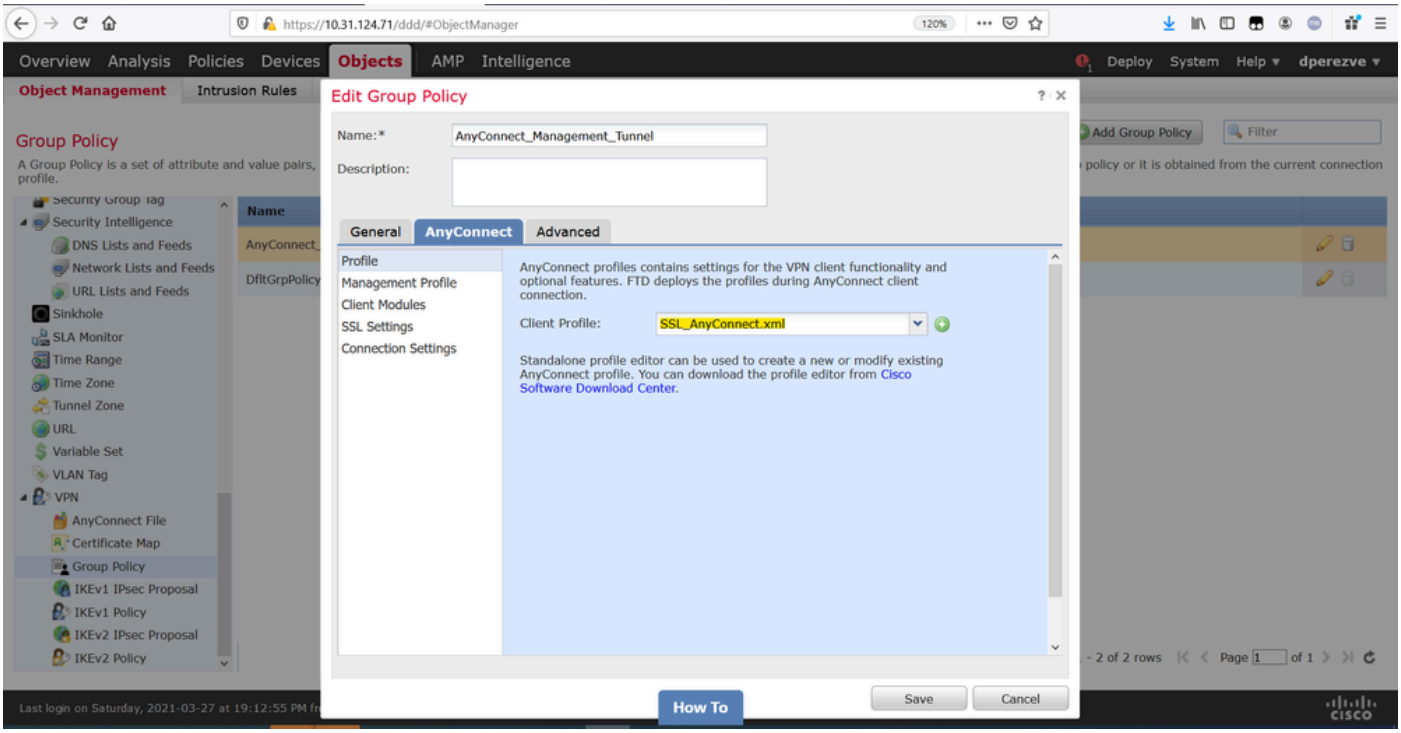


步骤4.创建组策略

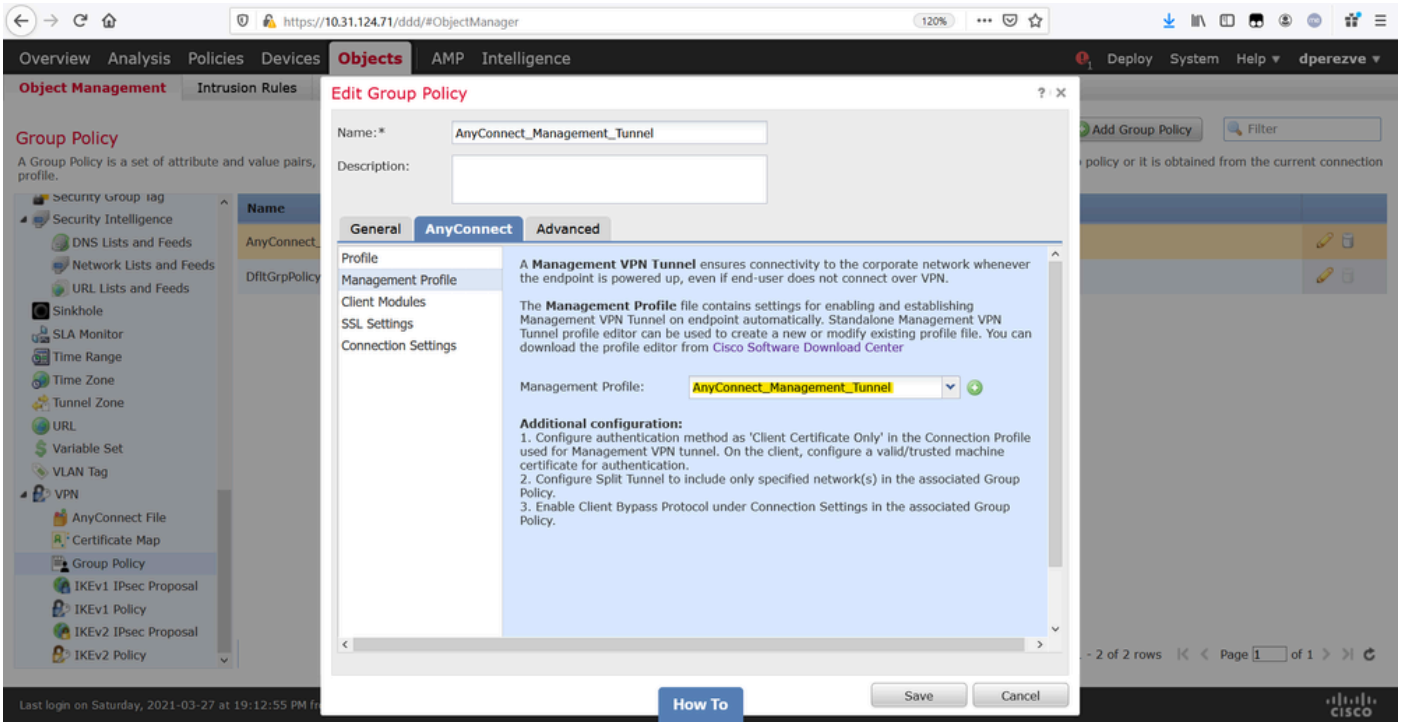
1.要创建新的组策略，请导航到对象>对象管理，然后从目录中选择VPN选项。选择Group Policy，然后单击Add Group Policy按钮。

2.打开添加组策略窗口后，分配名称并定义AnyConnect池，然后打开AnyConnect选项卡。

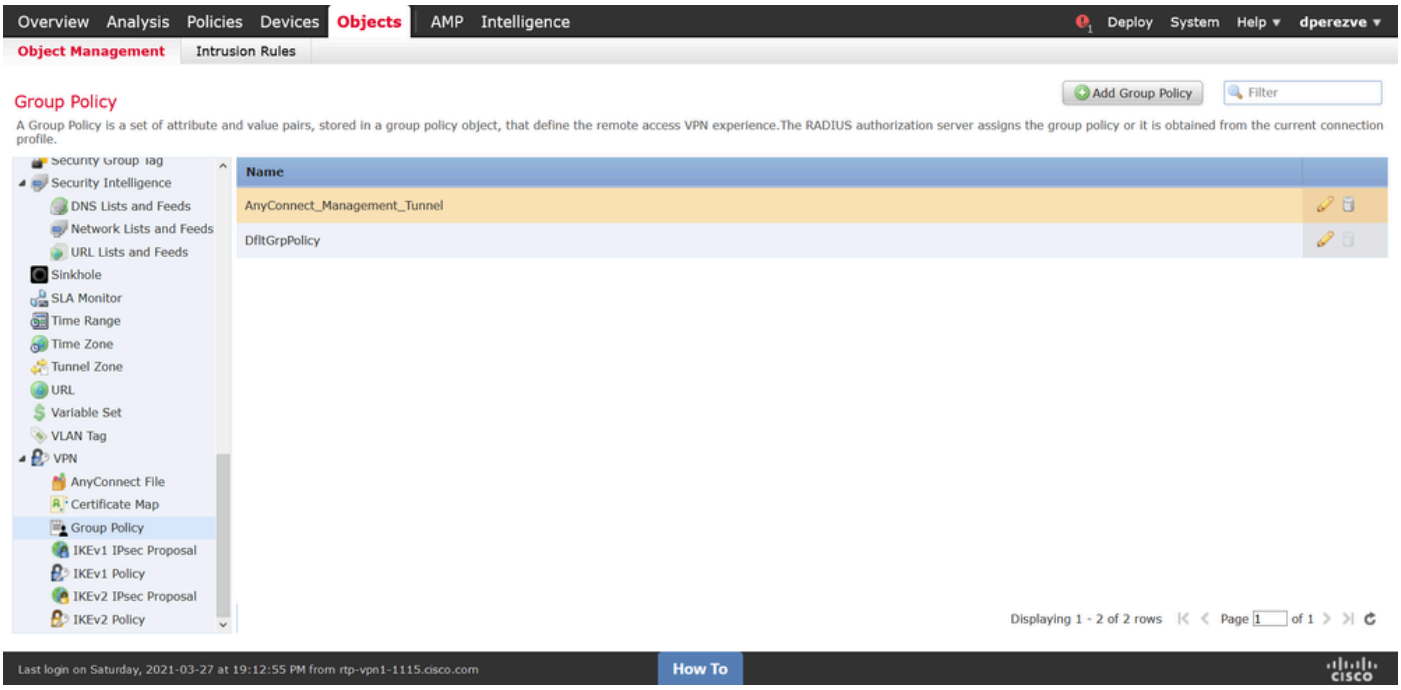
3.导航至Profile，然后在Client Profile下拉菜单中选择代表常规AnyConnect VPN配置文件的对象。



4.定位至“管理配置文件”标签，然后在“管理配置文件”下拉菜单中选择包含管理VPN配置文件的对象。



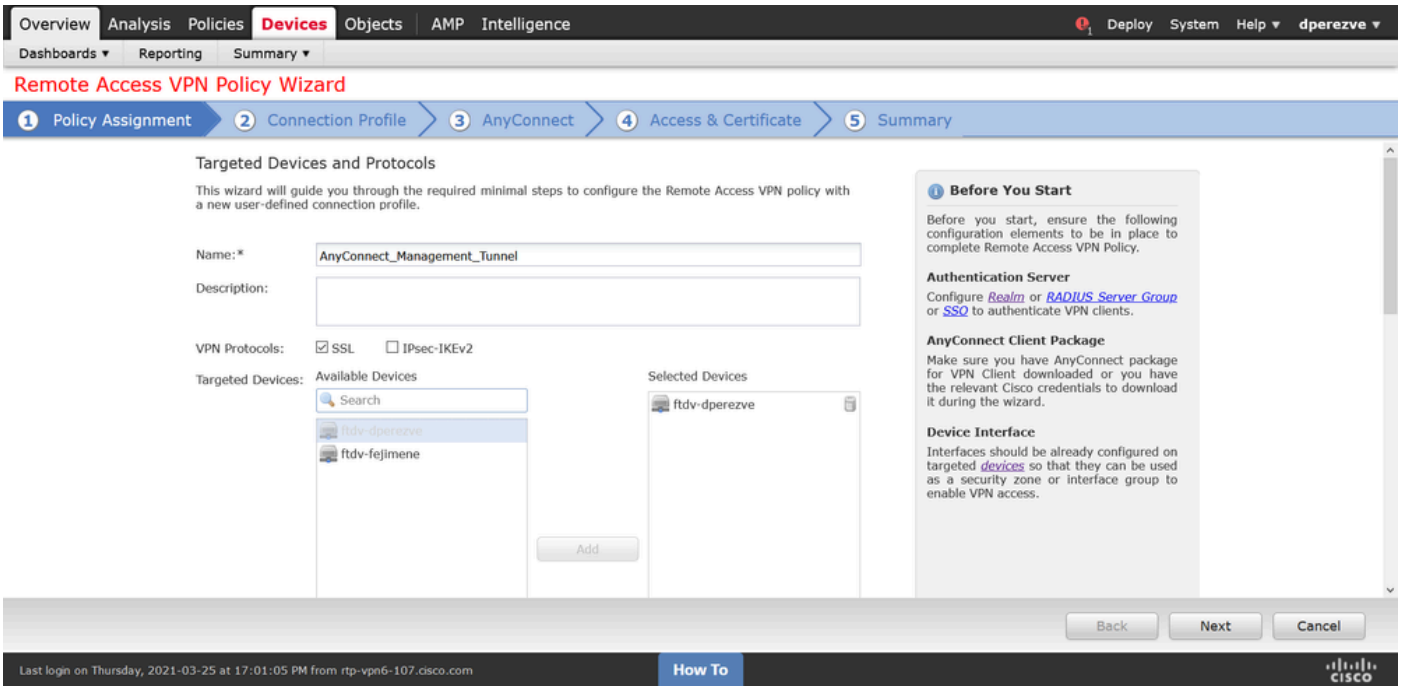
5.保存更改，以将新对象添加到现有组策略。



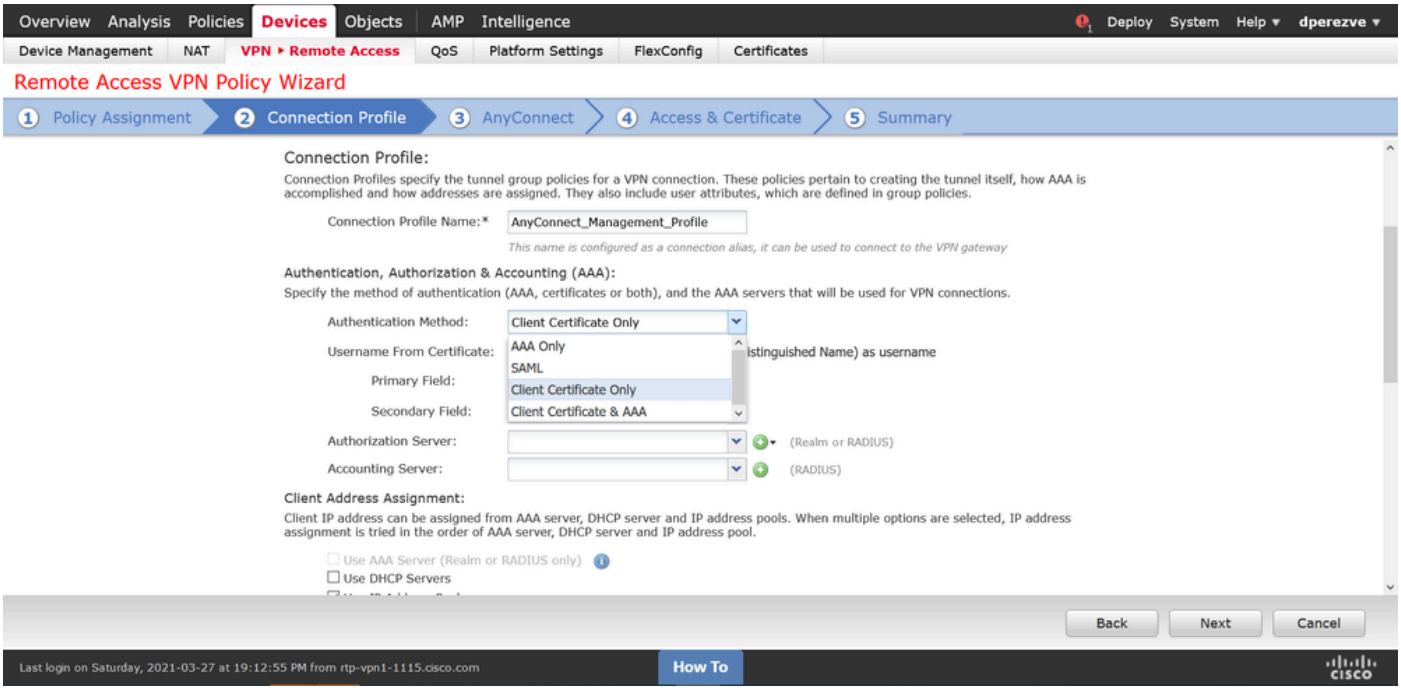
步骤5.创建新的AnyConnect配置

1.在FMC中配置SSL AnyConnect包括4个不同的步骤。要配置AnyConnect，请导航到设备> VPN >远程访问，然后选择添加按钮。此操作必须打开远程访问VPN策略向导。

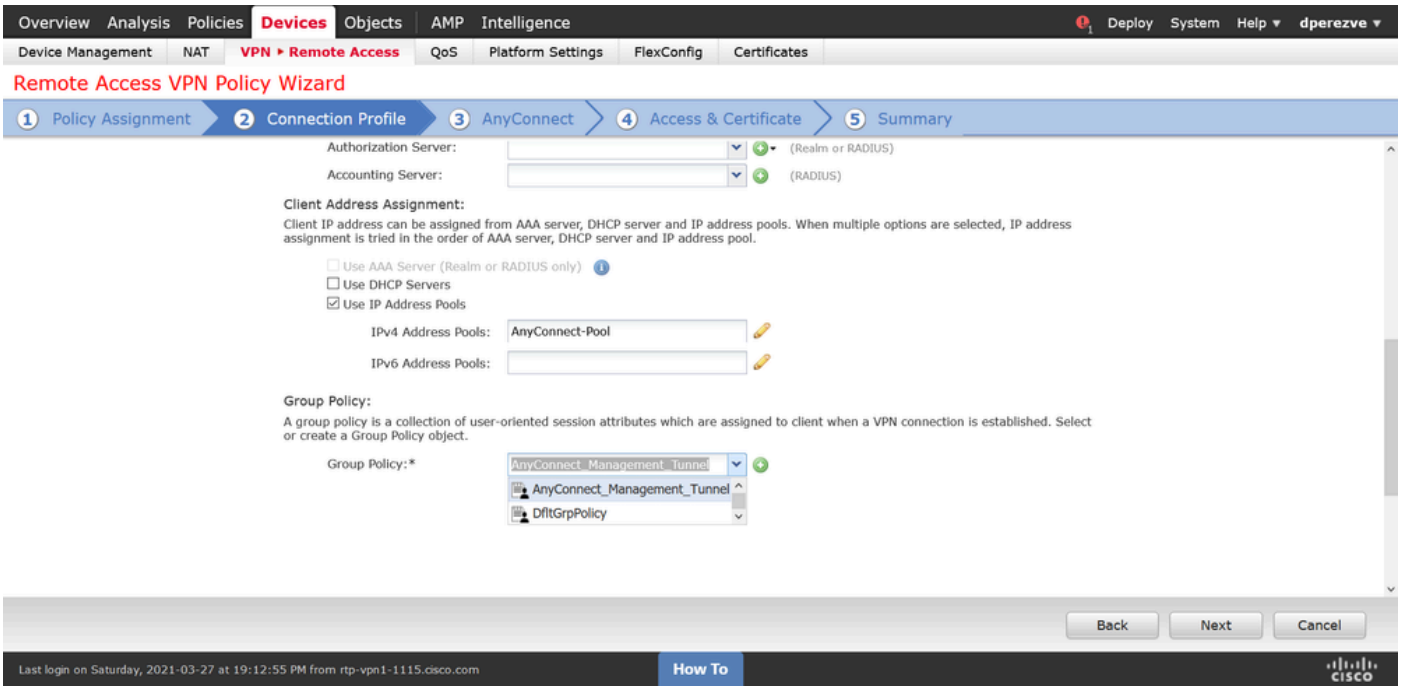
2.在Policy Assignment选项卡上，选择手边的FTD设备，定义连接配置文件的名称，然后选中SSL复选框。



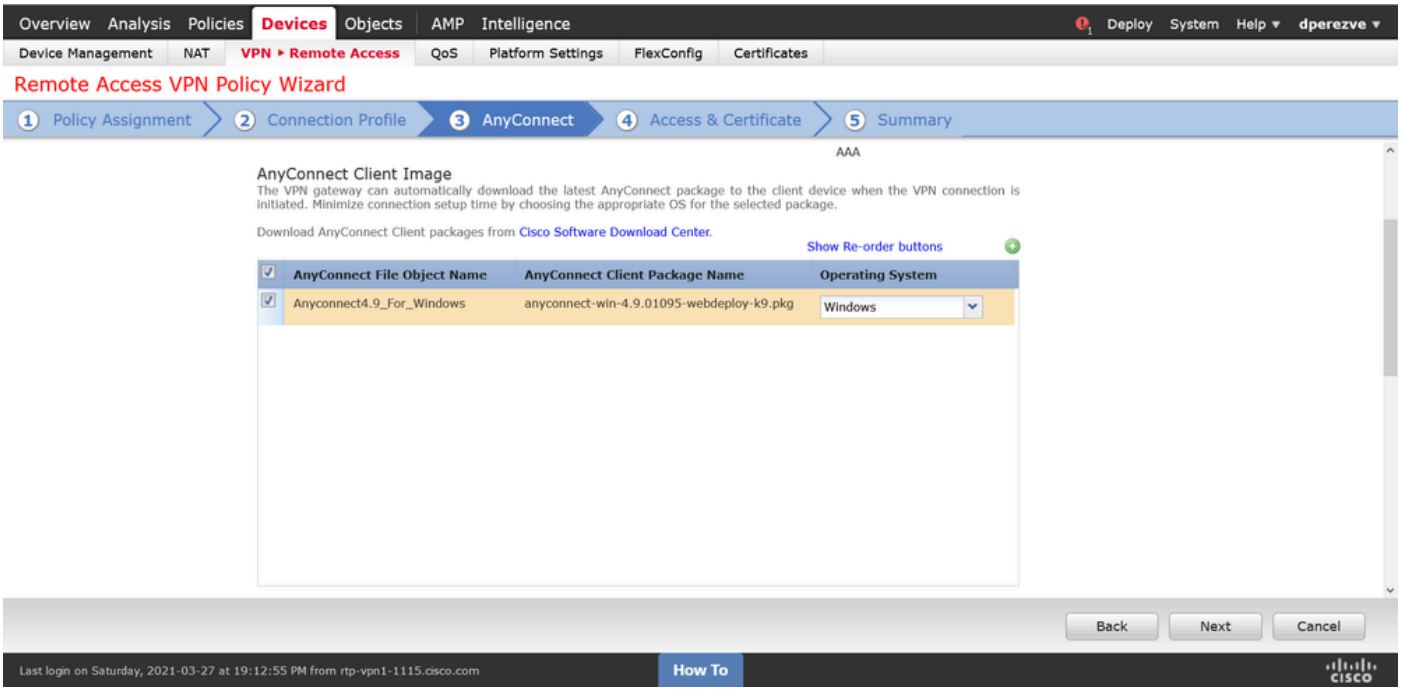
2.在Connection Profile上，选择Client Certificate Only作为身份验证方法。这是该功能支持的唯一身份验证。



3.然后，在“组策略”下拉菜单中，选择在步骤3中创建的组策略对象。



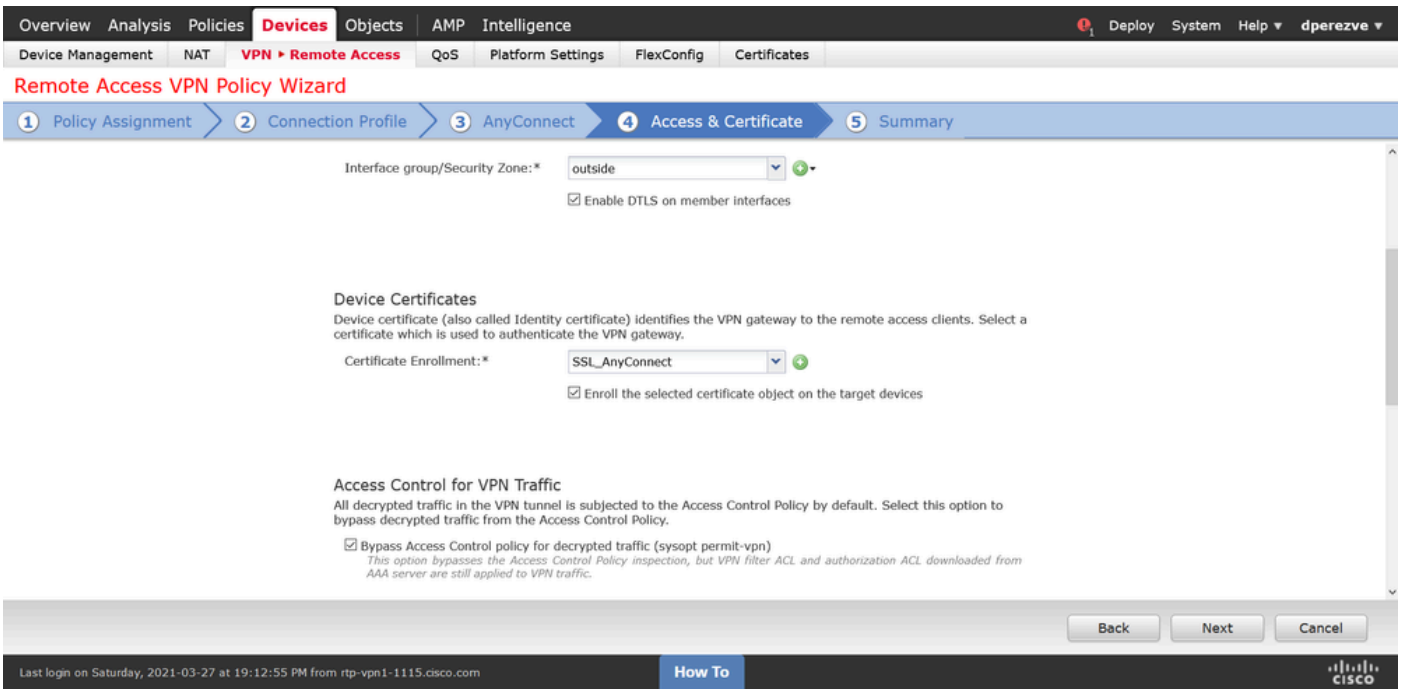
4.在AnyConnect选项卡上，根据终端上的操作系统(OS)选择AnyConnect File Object。



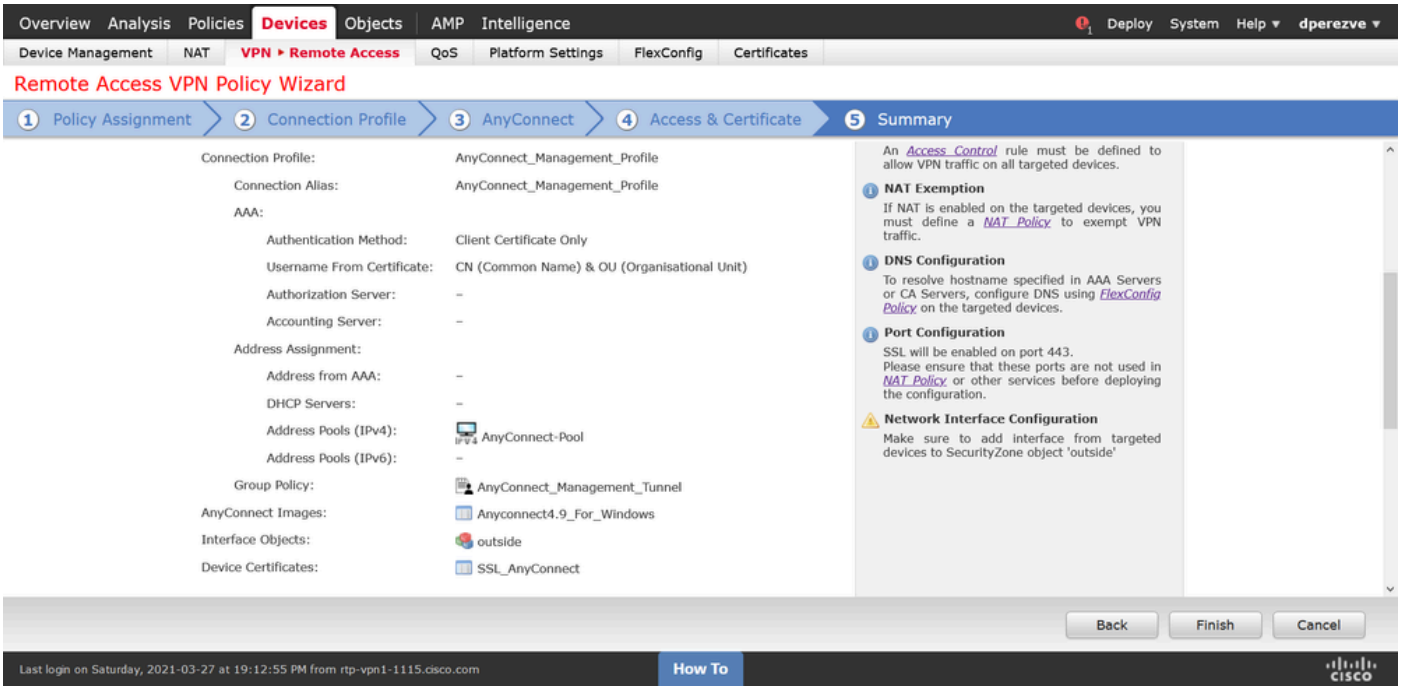
5.在Access & Certificate上，指定FTD必须使用的证书，以向Windows客户端探测其身份。

注意：由于用户在使用管理VPN功能时无法与AnyConnect应用交互，因此证书必须完全受信任，且不得打印任何警告消息。

注意：为防止证书验证错误，证书的使用者名称中包含的公用名称(CN)字段必须与XML配置文件服务器列表（第1步和第2步）中定义的FQDN匹配。



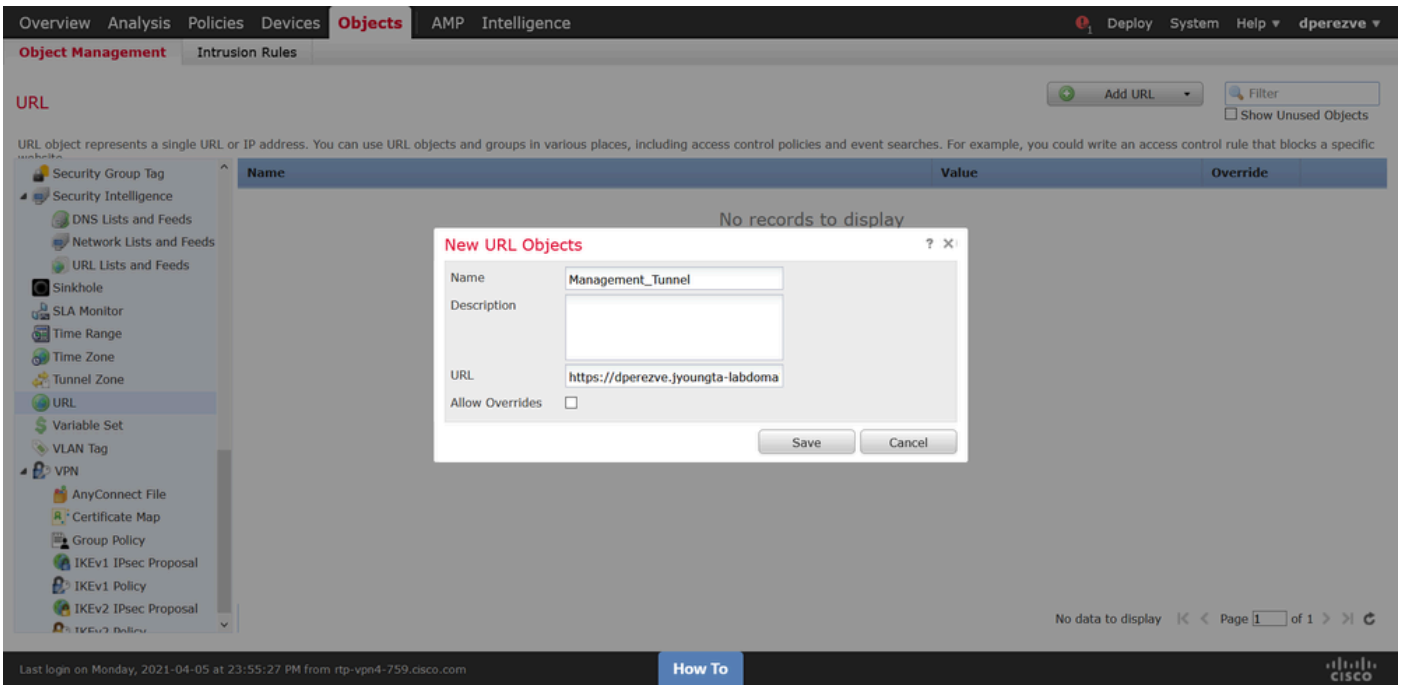
6.最后，选择摘要选项卡上的完成按钮以添加新的AnyConnect配置。



步骤6.创建URL对象

1.定位至“对象”>“对象管理”，然后从目录中选择URL。然后，在Add URL下拉菜单中选择Add Object。

2.为对象提供名称，并使用管理VPN配置文件服务器列表中指定的FQDN/用户组定义URL（第2步）。 在本示例中，URL必须是dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel。

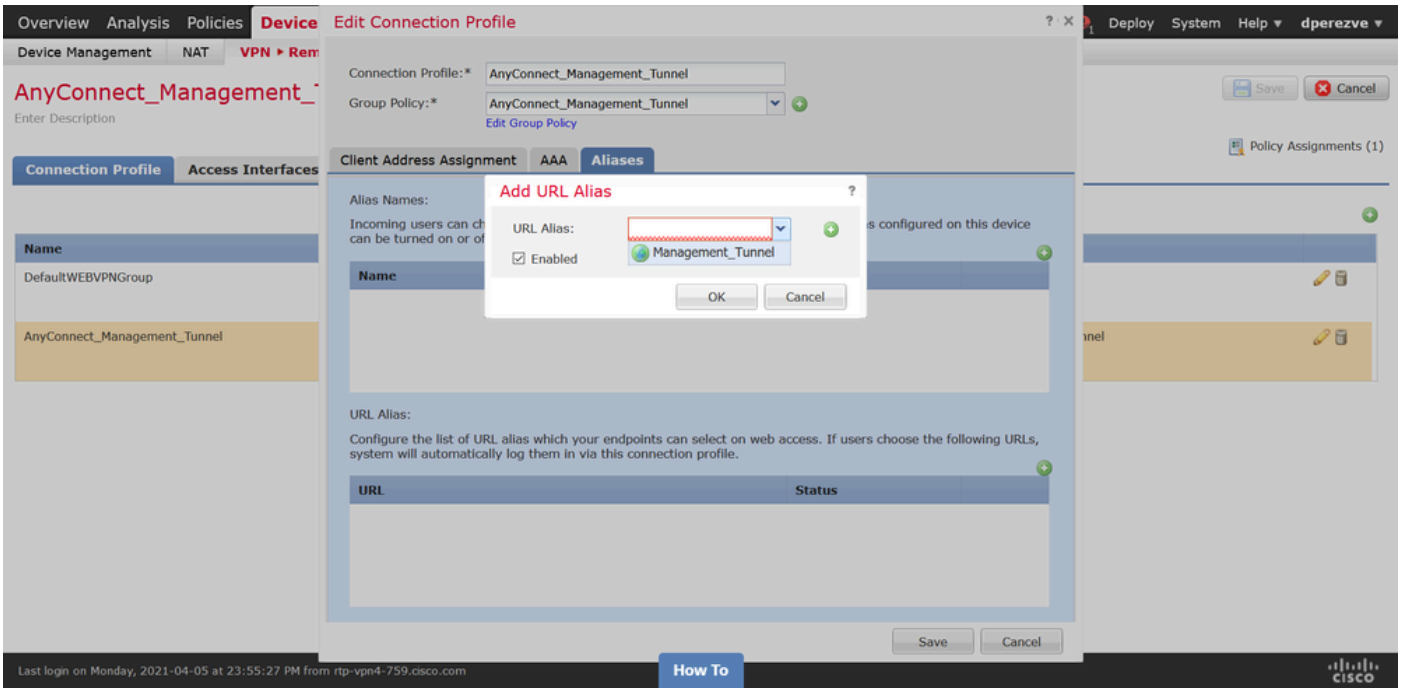


3.保存更改以将对象添加到对象列表。

步骤7.定义URL别名

1.要在AnyConnect配置中启用URL别名，请导航到设备> VPN >远程访问，然后单击铅笔图标进行编辑。

2.在“连接配置文件”选项卡上，选择手头的配置，导航到别名，然后单击添加按钮。然后，在URL别名下拉菜单中选择URL对象。确保选中Enabled复选框。



3.保存更改并将配置部署到FTD。

验证

部署完成后，需要与AnyConnect VPN配置文件建立第一个手动的AnyConnect连接。在此连接期间，管理VPN配置文件从FTD下载并存储在C:\ProgramData\Cisco\Cisco AnyConnect安全移动客户端\Profile\MgmtTun中。从此，后续连接必须通过管理VPN配置文件启动，无需任何用户交互。

故障排除

对于证书验证错误：

- 确保证书颁发机构(CA)的根证书安装在FTD上。
- 确保在Windows计算机存储上安装由同一CA签名的身份证书。
- 确保CN字段包含在证书中，并且与管理VPN配置文件的服务器列表中定义的FQDN和URL别名中定义的FQDN相同。

对于未启动的管理隧道：

- 确保管理VPN配置文件已下载并存储在C:\ProgramData\Cisco\Cisco AnyConnect安全移动客

户端\Profile\MgmtTun中。
- 确保管理VPN配置文件的名称为VpnMgmtTunProfile.xml。

对于连接问题，请收集DART捆绑包并联系思科TAC进行进一步研究。

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）。