远程访问 VPN

远程访问虚拟专用网络 (VPN) 允许个人用户使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备，从远程位置连接到您的网络。这样，移动员工就可以从家庭网络或公共 Wi-Fi 网络进行连接。

以下主题介绍如何为您的网络配置远程访问 VPN。

远程访问 VPN 概述

您可以使用 设备管理器，配置通过 SSL 借助 Secure Client 软件实现的远程访问 VPN。

Secure Client 与 威胁防御 设备协商 SSL VPN 连接时，会使用传输层安全 (TLS) 或数据报传输层安全 (DTLS) 进行连接。DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。客户端与 威胁防御 设备协商要使用的 TLS/DTLS 版本。如果客户端支持 DTLS，则使用 DTLS。

各设备型号的最大并发 VPN 会话数量

根据设备型号，设备上允许的并发远程访问 VPN 会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程访问 VPN 会话数
Firepower 1010	75
Firepower 1120	150

设备型号	最大并发远程访问 VPN 会话数
Firepower 1140	400
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Secure Firewall 3110	3000
Secure Firewall 3120	6000
Secure Firewall 3130	15,000
Secure Firewall 3140	20,000
Firepower 4100 系列，所有型号	10,000
Firepower 9300 设备，所有型号	20,000
Threat Defense Virtual：FTDv5	50
Threat Defense Virtual： FTDv10、FTDv20、FTDv30	250
Threat Defense Virtual：FTDv50	750
Threat Defense Virtual：FTDv100	10,000
ISA 3000	25

下载 Secure Client 软件

在配置远程访问 VPN 之前，必须将 Secure Client 软件下载到您的工作站。定义 VPN 时，您需要上传这些软件包。

您应该下载最新的 Secure Client 版本，以确保获得最新的功能、漏洞修复和安全补丁。请定期更新威胁防御设备上的软件包。

注释 可以为以下每个操作系统上传一个 Secure Client 软件包：Windows、Mac 和 Linux。无法为特定操作系统类型上传多个版本。

从 software.cisco.com 获取 Secure Client 软件包。您需要下载客户端的“完全安装软件包”版本。

用户如何安装 Secure Client 软件

要完成 VPN 连接，您的用户必须安装 Secure Client 软件。可以使用现有的软件分发方法直接安装该软件。或者，可以让用户直接从威胁防御设备安装 Secure Client 。

用户必须对其工作站具有管理员权限才能安装软件。

安装 Secure Client 后，如果您将新的 Secure Client 版本上传到系统，Secure Client 将在用户进行下一个VPN连接时检测到新版本。系统将自动提示用户下载并安装更新的客户端软件。这种自动化可为您和您的客户端简化软件分发。

如果您决定让用户一开始从 威胁防御设备安装软件，请告诉用户执行以下步骤。

注释 Android 和 iOS 用户应从相应的应用商店下载 Secure Client。

过程

步骤 1 使用 Web 浏览器，打开 **https://***ravpn-address*，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。

您在配置远程访问 VPN 时确定此接口。系统提示用户登录。

如果更改了远程访问 VPN 连接的端口，则用户必须在 URL 中包含该自定义端口。例如，如果将端口更改为 4443，则 URL 应为 https://ravpn.example.com:4443

步骤 2 登录到网站。

用户使用为远程访问 VPN 配置的目录服务器进行身份验证。登录成功后可继续操作。

如果登录成功，系统将确定用户是否已具有所需的 Secure Client版本。如果用户的计算机上没有 Secure Client ，或者客户端的版本较低，系统将自动开始安装 Secure Client 软件。

安装后，Secure Client 会完成远程访问 VPN 连接。

使用 RADIUS 和组策略控制用户权限和属性

您可以将用户授权属性（也称为用户权利或权限）应用于来自外部 RADIUS 服务器或 威胁防御设备上定义的组策略的 RA VPN 连接。如果 威胁防御 设备从与组策略上配置的属性冲突的外部 AAA 服务器接收属性，则来自 AAA 服务器的属性始终优先。

威胁防御设备按照以下顺序应用属性：

1. 外部 AAA 服务器上的用户属性 - 该服务器在用户身份验证或授权成功后返回这些属性。

2. 在 威胁防御设备上配置的组策略 - 如果 RADIUS 服务器为用户返回 RADIUS CLASS 属性 IETF-Class-25 (OU=group-policy) 值，威胁防御设备会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。
3. 连接配置文件分配的组策略 - 连接配置文件包含该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。连接至 威胁防御设备的所有用户最初都属于此组，这可以提供 AAA 服务器返回的用户属性或分配给用户的组策略中缺失的所有属性。

威胁防御设备支持供应商 ID 为 3076 的 RADIUS 属性。如果使用的 RADIUS 服务器没有定义这些属性，您必须手动定义它们。要定义属性，请使用属性名称或编号、类型、值和供应商代码 (3076)。

以下主题根据属性值是在 RADIUS 服务器中定义的还是由系统发送到 RADIUS 服务器的来介绍受支持的属性。

发送到 RADIUS 服务器的属性

RADIUS 属性 146 和 150 由 威胁防御 发送到 RADIUS 服务器，用于身份验证请求和授权请求。以下所有属性都是由 威胁防御设备发送到 RADIUS 服务器，用于记账开始请求、临时更新请求和停止请求。

表 *1:* 发送到 *RADIUS* 的属性 威胁防御

属性	属性编号	语法、类型	单值或多值	说明或值
客户端类型	150	整数	单值	连接到 VPN 的客户端类型： 2 = Secure Client SSL VPN
会话类型	151	整数	单值	连接类型： 1 = Secure Client SSL VPN
隧道组名称	146	字符串	单值	用于建立会话的连接配置文件名称，如 威胁防御设备上的定义。此名称可以包含 1-253 个字符。

从 RADIUS 服务器接收的属性

以下用户授权属性由 RADIUS 服务器发送到 威胁防御设备。

表 *2:* 发送到 威胁防御 的 *RADIUS* 属性

属性	属性编号	语法、类型	单值或多值	说明或值
Access-List-Inbound	86	字符串	单值	这两个访问列表属性都使用 威胁防御 设备上配置的 ACL 名称。使用 Smart CLI 扩展访问列表对象类型创建 ACL（依次选择**设备** > **高级配置** > **Smart CLI** > **对象**）。 此类 ACL 用于控制入站流量（流量进入 威胁防御设备）或出站流量（流量离开 威胁防御 设备）。
Access-List-Outbound	87	字符串	单值	

属性	属性编号	语法、类型	单值或多值	说明或值
Address-Pools	217	字符串	单值	威胁防御 设备上定义的网络对象名称，用于识别将作为地址池供客户端连接 RA VPN 时使用的子网。在**对象 (Objects)** 页面上定义网络对象。
Banner1	15	字符串	单值	用户登录时显示的横幅。
Banner2	36	字符串	单值	用户登录时显示的横幅的第二部分。横幅 2 附加到横幅 1。
Group-Policy	25	字符串	单值	要在连接中使用的组策略。必须在 RA VPN **组策略 (Group Policy)** 页面上创建组策略。您可以使用以下其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
Simultaneous-Logins	2	整数	单值	允许用户建立的独立并发连接的数量，0 - 2147483647。
VLAN	140	整数	单值	限制用户连接的 VLAN，0 - 4094。还必须在 威胁防御设备的子接口上配置此 VLAN。

双因素身份验证

可以为RA VPN配置双因素身份验证。配置了双因素身份验证时，用户必须提供用户名、静态密码，以及一个额外项，如RSA 令牌或Duo密码等。双因素身份验证不同于使用第二个身份验证源，双因素是在单个身份验证源中配置的，其与 RSA/Duo 服务器的关系绑定到主身份验证源。例外情况是 Duo LDAP，它将“Duo LDAP 服务器”配置为辅助身份验证源。

在双因素身份验证过程中，第一个因素是 RADIUS 或 AD 服务器，与之配合使用的第二个因素是推送到移动设备的 RSA 令牌和 Duo 密码，正是使用此令牌和密码来检测系统，

RSA 双因素身份验证

可以使用以下方法之一配置 RSA。有关 RSA 端配置的信息，请参阅 RSA 文档。

- 直接在 设备管理器 中将 RSA 服务器定义为 RADIUS 服务器，并将此服务器用作 RA VPN 中的主身份验证源。

  使用此方法时，用户必须使用 RSA RADIUS 服务器上配置的用户名进行身份验证，并使用一次性临时 RSA 令牌连接密码，用逗号分隔密码和令牌：密码,令牌。

  在此配置中，通常会使用单独的 RADIUS 服务器 （例如，Cisco ISE 提供的 RADIUS 服务器) 提供授权服务。将第二个 RADIUS 服务器配置为授权、配置或记账服务器。

- 将 RSA 服务器与支持直接集成的 RADIUS 或 AD 服务器集成，并配置 RA VPN，将非 RSA RADIUS 或 AD 服务器用作主要身份验证源。在这种情况下，RADIUS/AD 服务器使用 RSA-SDI 在客户端和 RSA 服务器之间代理和安排双因素身份验证。

  使用此方法时，用户必须使用非 RSA RADIUS 或 AD 服务器上配置的用户名进行身份验证，并使用一次性临时 RSA 令牌连接密码，用逗号分隔密码和令牌：密码,令牌。

  在此配置中，也会将第二个非 RSA RADIUS 服务器用作授权和记账（可选）服务器。

使用 RADIUS 的 Duo 双因素身份验证

可以将 Duo RADIUS 服务器配置为主要身份验证源。此方法使用 Duo RADIUS 身份验证代理。

有关配置 Duo 的详细步骤，请参阅 https://duo.com/docs/cisco-firepower。

然后，配置 Duo，以转发定向到代理服务器的身份验证请求，并将另一台 RADIUS 服务器或 AD 服务器用作第一个身份验证因素，将 Duo 云服务用作第二个因素。

使用此方法时，用户必须使用 Duo 身份验证代理和关联的 RADIUS/AD 服务器上配置的用户名，以及 RADIUS/AD 服务器中配置的用户名对应的密码进行身份验证，其后紧随以下其中一个 Duo 代码：

- *Duo-passcode*。例如，*my-password*,**12345**。
- **push**。例如，*my-password*,**push**。使用 **push** 告知 Duo 向用户应该已经安装并注册的 Duo 移动应用发送推送身份验证。
- **sms**。例如，*my-password*,**sms**。使用 **sms** 告知 Duo 向用户的移动设备发送包含新一批密码的 SMS 消息。使用 **sms** 时，用户的身份验证尝试将会失败。用户必须重新进行身份验证，并输入新密码作为辅助因素。
- **phone**。例如，*my-password*,**phone**。使用 **phone** 告知 Duo 执行电话回叫身份验证。

如果用户名/密码已经过验证，Duo 身份验证代理会联系 Duo 云服务，后者将核实该请求是来自有效配置的代理设备，然后按照指示将临时密码推送到用户的移动设备。当用户接受此密码时，Duo 会将会话标记为已验证，同时 RA VPN 成功创建。

使用 LDAP 的 Duo 双因素身份验证

可以将 Duo LDAP 服务器作为辅助身份验证源与作为主要源的 Microsoft Active Directory (AD) 或 RADIUS 服务器结合使用。使用 Duo LDAP 时，辅助身份验证使用 Duo 密码、推送通知或电话呼叫验证主要身份验证。

威胁防御设备使用通过端口 TCP/636 的 LDAPS 与 Duo LDAP 通信。

请注意，Duo LDAP 服务器仅提供身份验证服务，不提供身份服务。因此，如果将 Duo LDAP 作为主要身份验证源，则在任何控制面板中都将看不到与 RA VPN 连接关联的用户名，且将无法为这些用户编写访问控制规则。

使用此方法时，用户必须使用 RADIUS/AD 服务器和 Duo LDAP 服务器上配置的用户名进行身份验证。系统提示通过 Secure Client 登录时，用户应在主**密码**字段中提供 RADIUS/AD 密码，对于**辅助密码**，可以提供以下选项之一来使用 Duo 进行身份验证。有关详细信息，请参阅 https://guide.duo.com/anyconnect。

- *Duo* 密码 - 使用密码进行身份验证，密码将由 Duo Mobile 生成、通过 SMS 发送、由硬件令牌生成或由管理员提供。例如，1234567。
- **推送** - 如果已安装并激活 Duo Mobile 应用，请将登录请求推送至您的手机。查看请求并点击**批准**以登录。
- **电话** - 使用电话呼叫进行身份验证。
- **短信** - 以短信消息请求 Duo 密码。登录尝试失败。使用新密码重新登录。

有关使用 Duo LDAP 的详细说明和示例，请参阅如何使用 Duo LDAP 配置双因素身份验证，第 37 页。

远程访问 VPN 的许可要求

您的基本设备许可证必须满足出口要求，您才能配置远程访问 VPN。注册设备时，必须使用启用了出口控制功能的智能软件管理器账户。您也不能使用评估许可证配置该功能。

此外，您需要购买并启用远程访问 VPN 许可证，请选择以下任一项：Secure Client Advantage、Secure Client Premier 或 仅限 Secure Client VPN。即使这些许可证被设计为在与基于 ASA 软件的头端一起使用时允许不同的功能集，它们对于 威胁防御 设备都同等处理。

要启用许可证，请依次选择**设备** > **智能许可证** > **查看配置**，然后在远程访问 RA VPN 许可证组中选择正确的许可证。您需要在智能软件管理器账户中提供许可证。有关启用许可证的详细信息，请参阅启用或禁用可选许可证。

有关详细信息，请参阅《思科 *AnyConnect* 订购指南》http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf。另外，http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.html 中还提供了其他数据表。

远程访问 VPN 的准则和限制

配置 RA VPN 时，请时刻注意以下准则和限制。

- 对于同一个 TCP 端口，无法在同一接口上同时配置 设备管理器 访问（管理访问列表中的 HTTPS 访问）和远程访问 SSL VPN。例如，如果在外部接口上配置远程访问 SSL VPN，则也无法在端口 443 上打开 HTTPS 连接的外部接口。如果在同一接口上配置这两个功能，请确保至少更改其中一项服务的 HTTPS 端口，以避免冲突。
- RA VPN 外部接口是全局设置。不能在不同的接口上配置不同的连接配置文件。
- 无法在 NAT 规则的源地址和远程访问 VPN 地址池中使用重叠地址。
- 如果您使用 RADIUS 和 RSA 令牌配置双因素身份验证，则在大多数情况下，12 秒的默认身份验证超时太短，无法实现成功的身份验证。您可以通过创建自定义 Secure Client 配置文件并将其应用到 RA VPN 连接配置文件，来增加身份验证超时值，如 配置并上传客户端配置文件，第 9 页中所述。建议身份验证超时时间最短为 60 秒，以便用户有足够的时间进行身份验证并粘贴 RSA 令牌，以及进行令牌往返验证。

- 不直接支持对 RA VPN 前端发出命令（例如 **curl** ），并且可能不会产生所需的结果。例如，前端不响应 HTTP HEAD 请求。

配置远程访问 VPN

要为客户端启用远程访问 VPN，需要配置许多单独的项目。以下步骤程序介绍了端到端流程。

过程

步骤 1 配置许可证。

需要启用两个许可证：

- 注册设备时，必须使用启用了出口控制功能的智能软件管理器账户。基本许可证必须符合出口控制要求，然后才能配置远程访问 VPN。您也不能使用评估许可证配置该功能。有关注册设备的步骤程序，请参阅注册设备。
- 远程访问 VPN 许可证。有关详细信息，请参阅远程访问 VPN 的许可要求，第 7 页。要启用该许可证，请参阅启用或禁用可选许可证。

步骤 2 配置证书。

对客户端与设备之间的 SSL 连接进行身份验证需要使用证书。您可以将预定义的 DefaultInternalCertificate 用于 VPN，也可以自行创建证书。

如果对用于身份验证的目录领域使用加密连接，则必须上传受信任的 CA 证书。

有关证书及其上传方法的详细信息，请参阅配置证书。

步骤 3 （可选。）配置 TLS/SSL 设置。

默认情况下，系统将允许远程用户使用系统支持的任何 TLS 版本和加密密码连接到远程访问 VPN。但是，您可以限制允许使用的 TLS/DTLS 版本、密码和 Diffie-Hellman 组以执行更安全的连接。请参阅配置 TLS/SSL 密码设置。

步骤 4 （可选。） 配置并上传客户端配置文件，第 9 页。

步骤 5 配置用于对远程用户进行身份验证的身份源。

您可以对允许登录远程访问 VPN 的用户账户使用以下源。或者，可以使用客户端证书进行身份验证，可单独使用，也可与身份源配合使用。

- Active Directory 身份领域 - 作为主要身份验证源。在 Active Directory AD 服务器中定义用户账户。请参阅配置 AD 身份领域。
- RADIUS 服务器组 - 充当主要或辅助身份验证源，并用于授权和记账。请参阅配置 RADIUS 服务器组。

- LocalIdentitySource（本地用户数据库）- 作为主要或回退源。您可以直接在设备上定义用户，不使用外部服务器。如果您使用本地数据库作为回退源，请确保您定义与外部服务器中定义的相同用户名/密码。请参阅配置本地用户。
- Duo LDAP 服务器 - 作为主要或辅助身份验证源。虽然您可以使用 Duo LDAP 服务器作为主要源，但这并不是常规配置。通常将其用作辅助源以便与主 Active Directory 或 RADIUS 服务器结合提供双因素身份验证。有关详细信息，请参阅如何使用 Duo LDAP 配置双因素身份验证，第 37 页。

步骤 6 （可选。）为 RA VPN 配置组策略，第 21 页

组策略定义用户相关的属性。可以配置组策略，根据组成员身份提供差异化的资源访问权限。或者，可以对所有连接使用默认策略。

步骤 7 配置 RA VPN 连接配置文件，第 14 页。

步骤 8 允许流量通过远程访问 VPN，第 12 页。

步骤 9 验证远程访问 VPN 配置，第 12 页。

如果在完成连接时遇到问题，请参阅远程访问 VPN 故障排除，第 27 页。

步骤 10 （可选。）启用身份策略并配置被动身份验证规则。

如果启用被动用户验证，通过远程访问VPN登录的用户将显示在控制面板上，他们也可以用作策略中的流量匹配条件。如果不启用被动身份验证，只有当远程访问 VPN 用户匹配主动身份验证策略时，这些用户才可用。必须启用身份策略以在控制面板中获取任何用户名信息，或将其用于流量匹配。

配置并上传客户端配置文件

Secure Client 配置文件随 Secure Client 软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及是否允许最终用户更改 Secure Client 首选项和高级设置中的选项。

如果在配置远程访问 VPN 连接时为外部接口配置完全限定主机名 (FQDN)，系统将为您创建一个客户端配置文件。此配置文件启用默认设置。只有在需要非默认行为时，才需要创建和上传客户端配置文件。请注意，客户端配置文件是可选的：如果您不上传， Secure Client 将对所有配置文件控制选项使用默认设置。

注释 必须将 威胁防御 设备的外部接口添加到 VPN 配置文件的服务器列表中，以便 Secure Client 在第一次连接时显示所有用户可控的设置。如果您不将地址或 FQDN 添加为配置文件中的主机条目，则系统不会向会话应用过滤器。例如，如果您创建了一个证书匹配，且证书与条件正确匹配，但您未将设备添加为该配置文件中的主机条目，那么证书匹配将被忽略。

您可以为 Secure Client 以及可以选择性地与 Secure Client 一起使用的各种模块（例如 AMP 启用程序）创建配置文件。虽然您可以为任何这些模块上传配置文件，但 设备管理器 仅支持创建 Secure Client 配置文件。但是，您可以通过 设备管理器上传任何类型的配置文件，然后使用 威胁防御 API（来自 API Explorer）更改对象的配置文件类型。配置文件页面显示所有类型的所有配置文件，但列表不指示配置文件类型。以下程序说明如何完成此任务。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在编辑配置文件属性时，点击对象列表中所示的**创建新的 Secure Client 配置文件 (Create New Secure Client Profile)** 链接来创建 Secure Client 配置文件对象。

开始之前

在上传客户端配置文件之前，必须先执行以下操作。

- 下载并安装独立版 Secure Client“配置文件编辑器 - Windows/独立版安装程序 (MSI)”。此安装文件仅适用于 Windows，文件名为 anyconnect-profileeditor-win-<version>-k9.msi，其中 <version> 是 Secure Client 版本（文件名可能会有所不同）。例如，anyconnect-profileeditor-win-4.3.04027-k9.msi。您还必须在安装配置文件编辑器之前安装 Java JRE 1.6（或更高版本）。从 software.cisco.com 获取 Secure Client 配置文件编辑器。请注意，此软件包包含所有配置文件编辑器，而不只是 VPN 客户端的一个配置文件编辑器。
- 使用配置文件编辑器创建所需的配置文件。您应在配置文件中指定外部接口的主机名或 IP 地址。有关详细信息，请参阅编辑器的在线帮助。

过程

步骤 1 选择**对象**，然后从目录中选择**Secure Client 配置文件 (Secure Client Profiles)**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑某个对象，请点击该对象的编辑图标 ( )。
- 要下载与对象关联的配置文件，请点击对象的下载图标 ( )。

要删除未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 3 为对象输入名称和（可选）说明。

如果要上传模块配置文件，请使用对象名称指示模块类型，以便更轻松地将其与 Secure Client 配置文件区分开来。

步骤 4 点击**上传**并选择使用配置文件编辑器创建的文件。

步骤 5 点击**打开**上传配置文件。

步骤 6 点击**确定**添加对象。

步骤 7 如果您创建的配置文件实际上是与 Secure Client 配置文件不同的类型，请完成以下步骤来更改对象的配置文件类型。

a) 点击“更多选项”按钮 (⋮) 并选择 **API Explorer**。

系统会在单独的选项卡或窗口中打开 API Explorer，具体取决于您的浏览器设置。

b) 打开 AnyConnectClientProfile 资源。

c) 选择 GET /object/anyconnectclientprofiles 方法，然后点击**试用！**按钮。

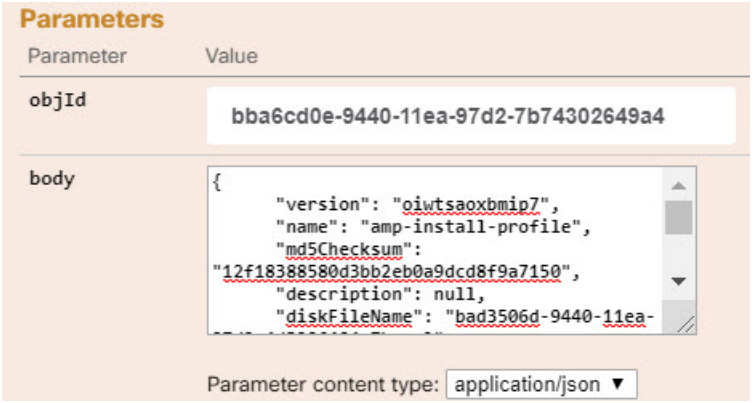
每个配置文件对象将如下所示。突出显示的属性是您需要更改的属性。

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile",
      "links": {
        "self": "https://10.89.5.38/api/fdm/v6/object/
anyconnectclientprofiles/bba6cd0e-9440-11ea-97d2-7b74302649a4"
      }
```

d) 在输出中找到您的对象，选择代码，按住 Ctrl 的同时点击将其复制到剪贴板。

e) 选择 PUT /object/anyconnectclientprofiles/{objId} 方法，并将内容粘贴到**正文**字段中。

f) 复制 **id** 值并将其粘贴到正文上方的 **objId** 编辑框中。您还可以在 “self” URL 的末尾找到对象 ID。



g) 在对象正文中，找到 **anyConnectModuleType** 字段，并将该值替换为您的配置文件类型的值。从 DART、FEEDBACK、WEB_SECURITY、ANY_CONNECT_CLIENT_PROFILE、AMP_ENABLER、NETWORK_ACCESS_MANAGER、NETWORK_VISIBILITY、START_BEFORE_LOGIN、ISE_POSTURE、UMBRELLA 中进行选择。

h) 再次在**正文**中，删除**链接**属性，在**类型**值后面添加逗号。

此对象正文应如下所示：

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
```

```
"diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
"anyConnectModuleType": "AMP_ENABLER",
"id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
"type": "anyconnectclientprofile"
}
```


i) 点击**试用！**按钮检查响应以验证对象是否已正确修改。您应获得响应代码200和回应更改的响应正文。您可以使用 GET 方法进一步验证结果。

允许流量通过远程访问 VPN

可以使用以下方法之一来启用远程访问 VPN 隧道中的流量。

- 配置 **sysopt connection permit-vpn** 命令，此命令会使匹配 VPN 连接的流量免受访问控制策略的限制。此命令的默认值是 **no sysopt connection permit-vpn**，这意味着 VPN 流量还必须获得访问控制策略的允许。

  外部用户无法在远程访问 VPN 地址池中伪造 IP 地址，因此这种允许 VPN 流量的方法较为安全。但它的缺点是，VPN流量得不到检测，也就是说不会对流量应用入侵和文件保护、URL过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。

  要配置此命令，请在 RA VPN 连接配置文件中选择**为已解密的流量绕过访问控制策略**选项。

- 创建访问控制规则以允许来自远程访问 VPN 地址池的连接。此方法可确保对 VPN 流量进行检测，并将高级服务应用于连接。但它的缺点是，有可能造成外部用户伪造IP地址，进而获得访问　内部网络的权限。

验证远程访问 VPN 配置

在配置远程访问 VPN 并将该配置部署到设备后，请确认是否可以进行远程连接。

如果遇到问题，请阅读故障排除主题以帮助查明和更正问题。请参阅远程访问 VPN 故障排除，第 27 页。

过程

步骤 1 在外部网络中，使用 Secure Client建立 VPN 连接。

使用 Web 浏览器，打开 **https://***ravpn-address*，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。如有必要，安装客户端软件并完成连接。请参阅用户如何安装 Secure Client 软件，第 3 页。

如果更改了远程访问 VPN 连接的端口，则必须在 URL 中包含该自定义端口。例如，如果将端口更改为 4443，则 URL 应为 https://ravpn.example.com:4443

如果配置了组 URL，也可尝试这些 URL。

步骤 2 登录到设备 CLI，如登录命令行界面 (CLI)中所述。 或者，打开 CLI 控制台。

步骤 3 使用 **show vpn-sessiondb** 命令查看有关当前 VPN 会话的摘要信息。

统计信息应显示您的活动 Secure Client 会话以及有关累积会话、峰值并发会话数量和非活动会话的信息。以下是该命令的输出示例。

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ----------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
  SSL/TLS/DTLS              :      1 :         49 :           3 :        0
Clientless VPN              :      0 :          1 :           1
  Browser                   :      0 :          1 :           1
--------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     50
Device Total VPN Capacity   :  10000
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
Clientless                  :      0 :          1 :               1
AnyConnect-Parent           :      1 :         49 :               3
SSL-Tunnel                  :      1 :         46 :               3
DTLS-Tunnel                 :      1 :         46 :               3
--------------------------------------------------------------------------------
Totals                      :      3 :        142
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
IPv6 Usage Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
AnyConnect SSL/TLS/DTLS     :        :           :
  Tunneled IPv6             :      1 :         20 :           2
--------------------------------------------------------------------------------
```

步骤 4 使用 **show vpn-sessiondb anyconnect** 命令查看有关当前 VPN 会话的详细信息。

详细信息包括使用的加密方式、传输和接收的字节数及其他统计信息。如果使用VPN连接，随着您重新发出命令，您应可看到传输/接收的字节数会变化。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : priya                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
```

```
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                 Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy        Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                  Tunnel Zone  : 0
```

管理远程访问 VPN 配置

远程访问 VPN 连接配置文件定义了一些特征，这些特征允许外部用户使用 Secure Client与系统建立 VPN 连接。每个配置文件都定义了用于用户身份验证的 AAA 服务器和证书、分配用户 IP 地址的地址池，以及定义各种面向用户的属性的组策略。

如果需要为不同的用户组提供可变的服务，或者有不同的身份验证源，您将创建多个配置文件。例如，如果您的组织与使用不同身份验证服务器的组织合并，您可以为使用这些身份验证服务器的新组创建配置文件。

过程

步骤 1 点击**设备** > **远程访问 VPN** 组中的**查看配置**。

该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

步骤 2 点击目录中的**连接配置文件**（如果未将其选定）。

步骤 3 执行以下任一操作：

- 点击 + 按钮创建新的连接配置文件。有关详细说明，请参阅配置 RA VPN 连接配置文件，第 14 页。
- 点击查看按钮()，打开连接配置文件和连接说明的摘要。在摘要中，可以点击**编辑**以进行更改。
- 点击删除按钮 ()，删除不再需要的连接配置文件。
- 选择目录中的**组策略**，定义连接配置文件面向用户的属性。请参阅为 RA VPN 配置组策略，第 21 页。

配置 RA VPN 连接配置文件

您可以创建远程访问VPN连接配置文件，允许用户在外部网络（例如其家庭网络）上时连接到您的内部网络。创建单独的配置文件，以适应不同的身份验证方法。

开始之前

在配置远程访问 (RA) VPN 连接之前：

- 从 software.cisco.com 将所需的 Secure Client 软件包下载到您的工作站。
- 外部接口（作为远程访问 VPN 连接终端的外部接口）也不能具有允许相同端口上的 HTTPS 连接的管理访问列表。为管理访问配置其他端口（请参阅在数据接口上配置用于管理访问的HTTPS端口），或者为连接配置文件配置其他端口。这两项服务都默认使用 443，因此其中一项必须更改。

过程

步骤 1 点击**设备** > **远程访问 VPN** 组中的**查看配置**。

该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

步骤 2 点击目录中的**连接配置文件**（如果未将其选定）。

步骤 3 执行以下操作之一：

- 点击 + 按钮创建新的连接配置文件。
- 点击查看按钮()，打开连接配置文件和连接说明的摘要。在摘要中，可以点击**编辑**以进行更改。

步骤 4 配置基本连接属性。

- **连接配置文件名称** - 此连接的名称，最多 50 个字符，不能含空格。例如，MainOffice。不能将 IP 地址用作名称。

  注释 您在此输入的名称将是用户在 Secure Client 客户端的连接列表中看到的名称。选择一个对您的用户来说有意义的名称。

- **组别名、组 URL** - 别名包含特定连接配置文件的备用名称或URL。在连接到威胁防御 设备时，VPN 用户可以在连接列表中的 Secure Client 客户端中选择别名。连接配置文件名称会自动添加为组别名。别名最多可包含 31 个字符。

  您还可以配置组 URL 列表，在发起远程访问 VPN 连接时您的终端可以从该列表中进行选择。如果用户使用组 URL 进行连接，系统将自动使用与 URL 匹配的连接配置文件。此 URL 供尚未安装 Secure Client 客户端的客户使用。

  按需要添加组别名和 URL。在设备上定义的所有连接配置文件中，这些别名和 URL 必须是唯一的。组 URL 必须以 **https://** 开头。

  例如，您可能有别名承包商和组 URL https://ravpn.example.com/contractor。安装 Secure Client 客户端后，用户只需在连接的 Secure Client VPN 下拉列表中选择组别名。

步骤 5 配置主身份源和辅助身份源（可选）。

这些选项确定设备如何对远程用户进行身份验证，以启用远程访问VPN连接。最简单的方法是仅使用 AAA，然后选择 AD 领域或使用 LocalIdentitySource。根据**身份验证类型**，您可以使用以下方法：

- **仅 AAA** - 根据用户名和密码对用户进行身份验证和授权。有关详细信息，请参阅为连接配置文件配置 AAA，第 18 页。
- **仅客户端证书** - 根据客户端设备身份证书进行用户身份验证。有关详细信息，请参阅为连接配置文件配置证书身份验证，第 20 页。
- **AAA 和 ClientCertificate** - 同时使用用户名/密码和客户端设备身份证书。
- **SAML** - 在主身份验证时使用 SAML 服务器。使用 SAML 时，不能配置回退或辅助身份验证源。有关详细信息，请参阅为连接配置文件配置 AAA，第 18 页。

步骤 6 配置客户端的地址池。

地址池定义了远程客户端在建立 VPN 连接时，系统可以分配给它们的 IP 地址。有关详细信息，请参阅为 RA VPN 配置客户端寻址，第 21 页。

步骤 7 点击**下一步 (Next)**。

步骤 8 选择要用于此配置文件的**组策略**。

组策略在建立隧道后设置用户连接的条款。系统包含名为 DfltGrpPolicy 的默认组策略。您可以创建其他组策略，以提供您所需的服务。

选择组策略时，您会看到组特征的摘要。在摘要中，点击**编辑 (Edit)** 可进行更改。

如果您需要的组策略尚不存在，请在下拉列表中点击**创建新的组策略 (Create New Group Policy)**。

有关组策略的详细信息，请参阅为 RA VPN 配置组策略，第 21 页。

步骤 9 点击**下一步 (Next)**。

步骤 10 配置全局设置。

这些选项适用于每个连接配置文件。在创建第一个连接配置文件后，后续的每个配置文件都会预配置这些选项。如果您做出了更改，则每个已配置的连接配置文件都会更改。

- **设备身份证书** - 选择用于建立设备身份的内部证书。客户端必须接受此证书才能完成安全的VPN连接。如果您还没有证书，请点击下拉列表中的**创建新内部证书 (Create New Internal Certificate)**。您必须配置证书。
- **外部接口** - 用户在进行远程访问 VPN 连接时连接的接口。请选择您支持的设备与最终用户之间的任何接口，虽然这通常是外部（面向互联网的）接口。
- **外部接口的完全限定域名** - 接口的名称，例如 ravpn.example.com。如果指定名称，系统可以为您创建一个客户端配置文件。

  注释 您要确保 VPN 中和客户端使用的 DNS 服务器可以将此名称解析为外部接口的 IP 地址。将 FQDN 添加到相关 DNS 服务器。

- **端口** - 用于 RA VPN 连接的 TCP 端口。默认值为 443。如果需要在用于 RA VPN 的同一接口上连接到 设备管理器 ，则必须更改连接配置文件或 设备管理器的端口号。这两项服务都默认使用 443。请注意，如果更改远程访问 VPN 连接的端口，用户必须在 URL 中包含该端口号。
- **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** -是否要让 VPN 流量受访问控制策略的限制。默认情况下已解密VPN流量受制于访问控制策略检查。启用**为已解密的流量绕过访问控制策略**选项会使流量绕过访问控制策略，但对于远程访问 VPN 而言，从 AAA 服务器下载的 VPN 过滤器 ACL 和授权 ACL 仍然适用于 VPN 流量。

  请注意，如果选择此选项，系统会配置 **sysopt connection permit-vpn** 命令，此为全局设置。这也会影响站点间VPN连接的行为。此外，就此选项而言，您无法为各连接配置文件采取不同的设置：此功能对所有的配置文件而言，要么都设为开启，要么都设为关闭。

  如果不选择此选项，外部用户可能会骗取远程访问 VPN 地址池中的 IP 地址，从而获取访问您网络的权限。这种情况可能会发生，因为您创建的访问控制规则需要允许地址池访问内部资源。如果您使用访问控制规则，请考虑使用用户说明来控制访问，而不是只使用源 IP 地址。

  选择此选项的弊端在于，VPN 流量将不会被检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。
- **NAT 豁免** - 启用 NAT 豁免，使进出远程访问 VPN 终端的流量免于执行 NAT 转换。如果不豁免 VPN 流量执行 NAT，请确保外部和内部接口的现有 NAT 规则不适用于 RA VPN 地址池。NAT 豁免规则是给定源/目标接口和网络组合的手动静态身份 NAT 规则，但它们不会反映在 NAT 策略中，它们是隐藏起来的。如果启用 NAT 豁免，还必须进行以下配置。

  请注意，这是一个全局选项；它会应用于所有连接配置文件。因此，请仅添加接口和内部网络，而不要替换它们，否则您将会改变已定义的所有其他连接配置文件的 NAT 豁免设置。

  - **内部接口** - 选择远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
  - **内部网络** - 选择代表远程用户将访问的内部网络的网络对象。网络列表必须包含与您支持的地址池相同的 IP 类型。

- **Secure Client 软件包** - RA VPN 连接上将支持的 Secure Client 完整安装软件映像。对于每个软件包，文件名（包括扩展名）不能超过 60 个字符。可以为 Windows、Mac 和 Linux 终端上传单独的软件包。但是，无法为不同的连接配置文件配置不同的软件包。如果已为另一个配置文件配置软件包，则会预先选中此软件包。对此配置的更改将会应用于所有配置文件。

  从 software.cisco.com 下载该软件包。如果终端尚未安装正确的软件包，系统会提示用户在用户验证后下载并安装软件包。

步骤 11 点击**下一步**。

步骤 12 审核摘要。

首先，验证摘要是否正确。

然后，点击 **说明** 查看最终用户初步安装 Secure Client 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击**复制 (Copy)** 将这些说明复制到剪贴板，然后分发给您的用户。

步骤 13 点击**完成 (Finish)**。

下一步做什么

确保 VPN 隧道中允许流量，如允许流量通过远程访问 VPN，第 12 页中所述。

为连接配置文件配置 AAA

身份验证、授权和记账(AAA)服务器使用用户名和密码来确认是否允许用户访问远程访问VPN。如果使用 RADIUS 服务器，则可以区分已验证用户的授权级别，从而提供对受保护资源的差异化访问权限。还可以使用 RADIUS 记账服务来跟踪使用情况。

在配置AAA时，您必须配置主身份源。辅助源和备用源是可选的。如果想要实施双重身份验证，请使用辅助源，例如，RSA 令牌或 DUO。

主身份源选项

- **用户身份验证的主身份源** - 用于对远程用户进行身份验证的主要身份源。必须在此源或可选的回退源中定义最终用户，才能完成 VPN 连接。选择以下一个选项：
  - Active Directory (AD) 身份领域。如果所需的领域尚不存在，请点击**创建新身份领域**。
  - RADIUS 服务器组。
  - LocalIdentitySource（本地用户数据库）- 您可以直接在设备上定义用户，而不使用外部服务器。
  - Duo LDAP 服务器。但是，这最好用作辅助身份验证源，以提供双因素身份验证，如如何使用 Duo LDAP 配置双因素身份验证，第 37 页中所述。如果将其用作主要源，则不会获取用户身份信息，而且在控制面板中也看不到用户信息，也不能编写基于用户的访问控制规则。
  - SAML 服务器。如果使用 SAML 服务器，则无法配置回退或辅助身份验证源。可以将RADIUS用作授权服务器，但必须配置RADIUS服务器，以便不需要身份验证。也就是说，在 SAML 对连接进行身份验证后，RADIUS 服务器将提供授权信息。
- **SAML 登录体验** - 如果选择 SAML 作为主身份验证源，您需要选择使用哪个客户端浏览器来完成 Web 身份验证：
  - **VPN 客户端嵌入式浏览器** - VPN 客户端使用其嵌入式浏览器进行 Web 身份验证，因此该身份验证仅适用于 VPN 连接。这是默认浏览器，无需进一步配置。
  - **默认操作系统浏览器** - VPN 客户端使用系统的默认浏览器进行 Web 身份验证。此选项可在您的 VPN 身份验证和其他企业登录之间启用单点登录 (SSO)。如果您想要支持无法在嵌入式浏览器中执行的 Web 身份验证方法（例如生物特征身份验证），也可选择此选项。

    您必须上传一个软件包，在浏览器中启用 Web 身份验证。从 software.cisco.com 获取软件包。请注意，所有使用 SAML 和默认操作系统浏览器的连接配置文件都使用您上传的数据； 这些数据包是全局的，而不是特定于连接配置文件的。

- **回退本地身份源** - 如果主要源是一个外部服务器，您可以选择 LocalIdentitySource 作为回退源，以防主服务器不可用。如果使用本地数据库作为回退源，请确保您定义的本地用户名/密码与外部服务器中的定义的用户名/密码相同。

高级选项 - 点击**高级**链接并配置以下选项：

- **删除选项** - 领域是管理域。启用以下选项将允许仅基于用户名进行身份验证。您可以启用这些选项的任意组合。但是，如果服务器无法分析分隔符，则必须选中这两个复选框。
  - **从用户名删除身份源服务器** - 在将用户名传递到 AAA 服务器之前，是否要从用户名删除身份源名称。例如，如果选择此选项且用户输入域\用户名作为用户名，则该域将从用户名中删除，并发送到 AAA 服务器进行身份验证。默认情况下，此选项处于取消选中状态。
  - **从用户名删除组** - 在将用户名传递到 AAA 服务器之前，是否要从用户名删除组名称。此选项适用于 username@domain 格式中给定的名称；此选项会剥离域和 @ 符号。默认情况下，此选项处于取消选中状态。
- **启用密码管理** - 是否允许用户在密码过期时更改密码。如果不选择此选项，当用户的密码过期时，Secure Client 将拒绝连接，用户必须前往 AAA 服务器更改密码。如果选择此选项，Secure Client 会在密码过期时提示用户更改密码，这对用户来说要方便得多。请选择以下其中一个选项。此外，请确保在 AAA 服务器上启用 MSCHAPv2。
  - **在密码过期前 x 天通知用户**（仅限 LDAP）- 从您指定的天数开始，警告用户密码即将过期。您可以将警告设置为 1-180 天，默认值为 14。
  - **在密码过期当天通知用户** - 不会警告用户，但在密码过期时仍会提示用户更改密码。即使您设置了警告期，RADIUS 用户也始终会出现此行为。

辅助身份源

- **用于用户授权的辅助身份源** - 可选的第二个身份源。如果用户成功使用主要源进行身份验证，则系统会提示其使用辅助源进行身份验证。可以选择 AD 领域、RADIUS 服务器组、Duo LDAP 服务器或本地身份源。
- **高级选项** - 点击**高级**链接并配置以下选项：
  - **辅助源的备用本地身份源** - 如果辅助源为外部服务器，您可以选择 LocalIdentitySource 作为备用源，以防辅助服务器不可用。如果使用本地数据库作为备用源，请确保您定义的本地用户名/密码与辅助外部服务器中定义的用户名/密码相同。
  - **使用主要用户名进行辅助登录** - 默认情况下，使用辅助身份源时，系统将提示输入辅助源的用户名和密码。如果选择此选项，系统将仅提示您输入辅助密码，并使用与主身份源相同的用户名来进行辅助源身份验证。如果您在主身份源和辅助身份源中配置了相同的用户名，请选择此选项。
  - **会话服务器用户名** - 身份验证成功后，用户名将显示在事件和统计控制面板中，用于确定基于用户或组的 SSL 解密和访问控制规则之间的匹配关系，并用于记账。由于使用了两个身份验证源，因此您需要告诉系统是使用主用户名还是辅助用户名作为用户身份。默认情况下，使用主用户名。

- **密码类型** - 如何获取辅助服务器的密码。仅当您选择 **AAA 和客户端证书**作为身份验证类型时，此字段才适用，并且对于证书选项，您选择**在用户登录窗口预填证书中的用户名**以及**在登录窗口隐藏用户名**。默认值为**提示**，这表明系统将提示用户输入密码。

  选择**主身份源密码**，自动使用用户在主服务器中进行身份验证时输入的密码。

  选择**公用密码**，为每个用户使用相同的密码，然后在**公用密码**字段中输入该密码。

其他选项

- **授权服务器** - 已配置为授权远程访问 VPN 用户的 RADIUS 服务器组。

  身份验证完成后，授权将控制对每个经过身份验证的用户都可用的服务和命令。授权通过组合一组描述用户被授权执行的操作、其实际功能和限制的属性来工作。如果您不使用授权，则单独的身份验证将为所有经过身份验证的用户提供相同的访问权限。有关配置 RADIUS 授权的信息，请参阅使用 RADIUS 和组策略控制用户权限和属性，第 3 页。

  请注意，如果系统从 RADIUS 服务器获取的授权属性与组策略中定义的属性重叠，则 RADIUS 属性将覆盖组策略属性。

- **记账服务器** -（可选。）用于为远程访问 VPN 会话记账的 RADIUS 服务器组。

  记账会跟踪用户正在访问的服务以及他们正在使用的网络资源量。威胁防御 设备向 RADIUS 服务器报告用户活动。记账信息包括每个会话的开始和停止时间、用户名、会话时通过设备的字节数、使用的服务以及每个会话的持续时间。然后，您可分析该数据，以进行网络管理、客户端计费或审核。您可以单独使用记账功能，也可以将其与身份验证和授权功能配合使用。

为连接配置文件配置证书身份验证

可以使用客户端设备安装的证书对远程访问VPN连接进行身份验证。使用证书身份验证时，请确保用于验证远程访问用户连接的受信任 CA 证书包括用于**验证使用**的 **SSL 客户端**选项。

使用客户端证书时，仍可以配置辅助身份源、备用源，以及授权和记账服务器。这些是AAA选项；有关详细信息，请参阅为连接配置文件配置 AAA，第 18 页。

以下是证书特定的属性。您可以为主身份源和辅助身份源单独配置这些属性。配置辅助源为可选操作。

- **从证书中获取的用户名** - 选择以下选项之一：
  - **映射特定字段** - 按照**主要字段**和**辅助字段**的顺序使用证书元素。默认值为 CN（公用名）和 OU（组织单位）。选择适用于您的组织的选项。这些字段组合在一起用于提供用户名，此名称用于事件和控制面板中，并出于匹配的目的，在 SSL 解密和访问控制规则中使用。
  - **使用完整 DN（可分辨名称）作为用户名** - 系统自动从 DN 字段派生出用户名。
- **高级选项 (Advanced options)** - 点击**高级 (Advanced)** 链接并配置以下选项：
  - **在用户登录窗口预填证书中的用户名** - 在提示用户进行身份验证时，是否在用户名字段填写检索到的用户名。

- **在登录窗口隐藏用户名** - 如果选择**预填充**选项，则可以隐藏用户名，这意味着用户无法编辑密码提示中的用户名。

为 RA VPN 配置客户端寻址

系统必须可以通过某种方法向连接到远程访问 VPN 的终端提供 IP 地址。这些地址可以由 AAA 服务器、DHCP 服务器、组策略中配置的 IP 地址池，或连接配置文件中配置的 IP 地址池提供。系统会按照以上顺序尝试使用这些资源，并在获取一个可用地址后停止尝试，然后将此地址分配给客户端。因此，您可以配置多个选项，以便在并发连接数异常多的情况下，可保障系统能获取地址。

使用下列一个或多个方法配置连接配置文件的地址池。

- **AAA 服务器**- 首先，在 威胁防御 设备上配置网络对象，用于指定地址池的子网。然后，在 RADIUS 服务器中，使用对象名称配置用户的地址池 (217) 属性。此外，还要在连接配置文件中指定用于身份验证的 RADIUS 服务器。
- **DHCP** - 首先，使用一个或多个 IPv4 地址范围为 RA VPN 配置 DHCP 服务器（您无法使用 DHCP 配置 IPv6 池）。然后，使用 DHCP 服务器的 IP 地址创建主机网络对象。随后，便可以在连接配置文件的 **DHCP 服务器 (DHCP Servers)**属性中选择此对象。您最多可以配置 10 个 DHCP 服务器。

  如果 DHCP 服务器有多个地址池，则可以在与连接配置文件关联的组策略中使用 **DHCP 作用域**属性，选择要使用的池。使用池的网络地址创建主机网络对象。例如，如果 DHCP 池包含 192.168.15.0/24 和 192.168.16.0/24，将 DHCP 范围设置为 192.168.16.0 可确保从 192.168.16.0/24 子网中选择地址。
- **本地 IP 地址池** - 首先，创建最多六个网络对象，用于指定子网。可以为 IPv4 和 IPv6 单独配置池。然后，在组策略或者连接配置文件的 **IPv4 地址池**和 **IPv6 地址池**选项中，选择这些对象。无需同时配置 IPv4 和 IPv6，只需配置您想要支持的地址方案即可。

  也不需要同时在组策略和连接配置文件中配置池。组策略会覆盖连接配置文件的设置，因此如果您在组策略中配置了池，则请将连接配置文件中的选项留空。

  请注意，系统按照您列出的顺序使用地址池。

为 RA VPN 配置组策略

组策略是针对远程访问 VPN 连接的一组面向用户的属性/值对。连接配置文件使用组策略，在建立隧道后设置用户连接的条款。通过组策略可将整组属性应用于用户或用户组，而不必为每个用户单独指定每个属性。

系统包含名为 DfltGrpPolicy 的默认组策略。您可以创建其他组策略，以提供您所需的服务。

过程

步骤 1 点击**设备** > **远程访问 VPN** 组中的**查看配置**。

该组显示有关当前已配置多少连接配置文件和组策略的摘要信息。

步骤 2 点击目录中的**组策略**。

步骤 3 执行以下任一操作：

- 点击 + 按钮，创建新组。有关组策略页面上的属性的说明，请参阅以下主题：
  - 常规属性，第 22 页
  - 会话设置属性，第 23 页
  - 地址分配属性，第 23 页
  - 分割隧道属性，第 24 页
  - Secure Client 属性，第 24 页
  - 流量过滤器属性，第 25 页
  - Windows 浏览器代理属性，第 26 页
- 点击编辑按钮 ( )，编辑现有组策略。
- 点击删除按钮 ( )，删除不再需要的组。当前，该组不能用于连接配置文件。

常规属性

组策略的常规属性定义组名称和一些其他基本设置。“名称”属性是唯一必需的属性。

- **名称** - 组策略的名称。此名称最多可包含 64 个字符，允许使用空格。
- **说明** - 组策略的说明。说明最多可以有 1,024 个字符。
- **DNS 服务器** - 选择定义连接到 VPN 时，DNS 服务器客户端应用于域名解析的 DNS 服务器组。如果所需的组尚不存在，请点击**创建 DNS 组 (Create DNS Group)** 并立即创建组。
- **横幅**- 登录时向用户显示的横幅文本或欢迎消息。默认无横幅。最多 496 字符。这种 Secure Client 支持部分 HTML。为确保向远程用户正确地显示横幅，请使用
 标记表示换行。
- **默认域** - RA VPN 中用户的默认域名。例如 example.com。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。
- **安全客户端配置文件** - 点击 + 并选择要用于该组的 Secure Client 配置文件。如果为外部接口（在连接配置文件中）配置的是完全限定域名，则系统将会为您创建默认配置文件。或者，您可上传您自己的客户端配置文件。使用独立的 Secure Client 配置文件编辑器创建这些配置文件，您可以从 software.cisco.com 下载和安装该编辑器。如果不选择客户端配置文件， Secure Client 将为所有选项使用默认值。此列表中的项目是 Secure Client 配置文件对象，而不是配置文件本身。您可以通过点击下拉列表中的**创建新的 Secure Client 配置文件 (Create New Secure Client Profile)**，创建（和上传）新配置文件。

  除了 Secure Client 配置文件，您还可以选择 Secure Client 模块配置文件，例如 AMP 启用程序。您可以为每个模块类型选择一个配置文件。

会话设置属性

组政策会话设置控制用户可以连接到 VPN 的时长和可以创建的独立连接的数量。

- **最长连接时间** - 在不注销和重新连接的情况下，允许用户持续连接到 VPN 的最大时间长度（以分钟为单位），范围为 1 到 4473924 或留空。默认值为无限（留空），但空闲超时仍适用。
- **连接时间警报间隔** - 如果您指定了最大连接时间，则警报间隔定义，在达到最长时间之前，向用户显示即将自动断开连接警告的时间。用户可以选择结束连接并重新连接，以重新启动计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **空闲时间** - VPN 连接在自动关闭之前可以闲置的时间长度（以分钟为单位），范围为 1 到 35791394。如果在此时间段内此连接上无通信活动，则系统会终止连接。默认值为 30 分钟。
- **空闲时间警报间隔** - 在达到空闲时间之前，向用户显示因闲置会话而即将自动断开连接的警报的时间。任何活动都会重置计时器。默认值为 1 分钟。可以指定 1 到 30 分钟。
- **每个用户的同时登录数** - 允许用户执行的最多同时登录数。默认值为 3。可以指定 1 到 2147483647 个连接。允许大量同时连接可能会危害安全性并影响性能。

地址分配属性

组策略的地址分配属性定义组的 IP 地址池。此处定义的地址池将覆盖使用此组的任何连接配置文件中定义的池。如果您希望使用连接配置文件中定义的池，请将这些设置留空。

- **IPv4 地址池**、**IPv6 地址池** - 这些选项定义远程终端的地址池。根据客户端用于建立 VPN 连接的 IP 版本，从这些池为客户端分配地址。选择一个网络对象，定义要支持的每个 IP 类型的子网。如果您不想支持该 IP 版本，则可以空着列表。例如，可以将 IPv4 池定义为 10.100.10.0/24。地址池不能与外部接口的 IP 地址位于同一子网。

  可以指定包含最多六个地址池的列表，用于本地地址分配。地址池的指定顺序非常重要。系统按照地址池出现的顺序分配这些地址池中的地址。

- **DHCP 范围** - 如果在连接配置文件中为地址池配置了 DHCP 服务器，DHCP 作用域会标识要用于此组的地址池的子网。DHCP 服务器的地址还必须来自此作用域标识的同一个子网。作用域允许您选择 DHCP 服务器中定义的部分地址池，用于此特定组。

  如未定义网络范围，则 DHCP 服务器将按地址池配置顺序分配 IP 地址。它将检查各个池，直到发现未分配的地址为止。

  要指定范围，请选择包含与所需池位于同一子网上但不在池内的可路由地址的网络对象。DHCP 服务器确定此 IP 地址所属的子网并从该地址池分配 IP 地址。

  建议尽可能将接口的 IP 地址用于路由目的。例如，如果池为 10.100.10.2-10.100.10.254，接口地址为 10.100.10.1/24，则使用 10.100.10.1 作为 DHCP 范围。请不要使用网络编号。如果对象尚不存在，请点击**创建新网络 (Create New Network)**。DHCP 仅可用于 IPv4 寻址。如果您选择的地址不是接口地址，可能需要为范围地址创建静态路由。

分割隧道属性

组策略的分割隧道属性定义系统如何处理用于内部网络的流量和流向外部的流量。分割隧道引导一些网络流量通过 VPN 隧道（加密），将剩下的网络流量引导至 VPN 隧道外部（未加密或以明文形式）。

- **IPv4 分割隧道、IPv6 分割隧道** - 可以根据流量是使用 IPv4 寻址还是 IPv6 寻址来指定不同的选项，但每个流量的选项都相同。如果想要启用分割隧道，指定其中一个要求您选择网络对象的选项。
  - **允许所有流量通过隧道** - 不分割隧道。一旦用户建立 RA VPN 连接，用户的所有流量都会通过受保护隧道。这是默认值。这也被视为最安全的选项。
  - **允许指定流量通过隧道** - 选择定义目标网络和主机地址的网络对象。前往这些目标的所有流量都会通过受保护隧道。客户端会将前往其他目标的流量路由至隧道外部（例如，本地 Wi-Fi 或网络连接）。
  - **排除以下指定网络** - 选择定义目标网络或主机地址的网络对象。客户端将前往这些目标的所有流量路由至隧道外部的连接。前往其他目标的流量都会通过隧道。
- **分割 DNS** - 您可以配置系统通过安全连接发送某些 DNS 请求，同时允许客户端将其他 DNS 请求发送到客户端上配置的 DNS 服务器。您可以配置以下 DNS 行为：
  - **根据分割隧道策略发送 DNS 请求** - 使用此选项时，系统将按照与定义分割隧道选项相同的方式处理 DNS 请求。如果启用分割隧道，则会根据目标地址发送 DNS 请求。如果未启用分割隧道，所有 DNS 请求都会通过受保护的连接。
  - **始终通过隧道发送 DNS 请求** - 如果启用了分割隧道，但想要通过受保护连接将所有 DNS 请求发送到为该组定义的 DNS 服务器上，则可选择此选项。
  - **仅通过隧道发送指定的域** - 如果想要让受保护的 DNS 服务器仅解析特定域的地址，则可选择此选项。然后，指定这些域，用逗号分隔域名。例如，example.com, example1.com。如果想要让内部 DNS 服务器解析内部域的名称，同时让外部 DNS 服务器处理所有其他互联网流量，请使用此选项。

Secure Client 属性

组策略的 Secure Client 属性定义 Secure Client 客户端用于远程访问 VPN 连接的某些 SSL 和连接设置。

SSL 设置

- **启用数据报传输层安全 (DTLS)**-是否允许 Secure Client 使用两个同步隧道：SSL 隧道和 DTLS 隧道。使用 DTLS 可避免某些 SSL 连接带来的延迟和带宽问题，并可改进对数据包延迟敏感的实时应用的性能。如果不启用 DTLS，Secure Client 用户在建立 SSL VPN 连接时仅与 SSL 隧道连接。
- **DTLS 压缩** - 是否使用 LZS 为此组压缩数据报传输层安全 (DTLS) 连接。默认情况下会禁用 DTLS 压缩。

- **SSL 压缩** - 是否启用数据压缩，如启用，则设置要使用的数据压缩方法：**Deflate** 或 **LZS**。默认情况下会**禁用** SSL 压缩。数据压缩加快了传输速率，但也增加了每个用户会话的内存需求和 CPU 使用率。因此，SSL 压缩会降低设备的整体吞吐量。
- **SSL 重新生成密钥方法**、**SSL 重新生成密钥间隔** - 客户端能够为 VPN 连接重新生成密钥，重新协商加密密钥和初始化向量，从而提高连接的安全性。选择**无**可禁用重新生成密钥。要启用重新生成密钥，请选择**新隧道 (New Tunnel)**来创建新的隧道。（**现有隧道**选项导致的操作与**新隧道**的相同。）如果启用重新生成密钥，还需设置重新生成密钥间隔，默认间隔为 4 分钟。可以将间隔设置为 4 到 10080 分钟（1 周）。

连接设置

- **忽略 DF（不分片）位** - 是否忽略需要分片的数据包内的“不分片” (DF) 位。选择此选项会允许强制将已设置 DF 位的数据包分片，从而使这些数据包能够通过隧道。
- **客户端绕行协议** - 允许您配置安全网关管理 IPv4 流量（安全网关仅允许 IPv6 流量时）或管理 IPv6 流量（安全网关仅允许 IPv4 流量时）的方式。

  当 Secure Client 建立与头端的 VPN 连接时，头端可以为客户端分配 IPv4 和/或 IPv6 地址。如果头端对 Secure Client 连接仅分配一个 IPv4 地址或一个 IPv6 地址，则您可以配置 Client Bypass Protocol 以丢弃头端尚未分配 IP 地址（默认、已禁用、未检查）的网络流量，或允许该流量绕过头端并从客户端以未加密或“明文形式”发送（已启用、已检查）。

  例如，假设安全网关只将一个 IPv4 地址分配给 Secure Client 连接，且终端为双协议栈。当终端尝试访问 IPv6 地址时，如果禁用客户端旁路协议，则会丢弃 IPv6 流量；但是，如果启用客户端旁路协议，则会从客户端以明文形式发送 IPv6 流量。
- **MTU** - Secure Client 为 SSL VPN 连接建立的最大传输单位 (MTU) 大小。默认值为 1406 字节。范围为 576 至 1462 字节。
- **Secure Client 和 VPN 网关之间的保持连接消息** - 是否在对等体之间交换保持连接消息，以证明它们可用于在隧道中发送和接收数据。保持连接消息以设置的时间间隔传输。默认间隔为 20 秒，有效范围为 15 到 600 秒。
- **网关端 DPD 间隔**、**客户端 DPD 间隔** - 启用失效对等体检测 (DPD)，确保 VPN 网关或 VPN 客户端快速检测对等体不再响应的时间。您可以单独启用网关或客户端 DPD。发送 DPD 消息的默认间隔为 30 秒。时间间隔可以是 5 到 3600 秒。

流量过滤器属性

组策略的流量过滤器属性定义您想要对分配到该组的用户设置的限制。您可以使用这些属性（而非创建策略规则）根据主机或子网地址和协议或 VLAN 来限制 RA VPN 用户仅可访问特定资源。

默认情况下，RA VPN 用户不会受到组策略的限制，可以访问受保护网络上的任何目标。

- **访问列表过滤器** - 使用扩展的访问控制列表 (ACL) 限制访问权限。选择 Smart CLI 扩展 ACL 对象，或点击**创建扩展访问列表**并立即创建。

  扩展 ACL 允许您基于源地址、目标地址和协议（例如 IP 或 TCP）进行过滤。ACL 评估遵循自上而下、“先匹配的规则先应用”原则，因此，请确保特定规则放在一般规则之前。ACL 末尾

不包含隐式“deny any”语句，因此如果您只是想要拒绝对几个子网的访问，同时允许其他访问，请确保在 ACL 末尾加上“permit any”规则。VPN 过滤器仅适用于初始连接。它不适用于因应用检查操作而打开的辅助连接，例如 SIP 媒体连接。

由于您无法在编辑扩展的 ACL Smart CLI 对象时创建网络对象，因此您应在编辑组策略之前创建 ACL。否则，您可能需要先创建对象，然后再返回来创建网络对象，最后创建您需要的所有访问控制条目。要创建 ACL，请转至**设备** > **高级配置** > **Smart CLI** > **对象**，创建对象，并选择**扩展访问列表**作为对象类型。有关示例，请参阅如何通过组控制 RA VPN 访问，第 60 页。

- **限制 VPN 到 VLAN** - 也称为“VLAN 映射”，此属性指定该组策略应用到的会话的出口 VLAN 接口。系统将该组中的所有流量都转发到所选 VLAN。

  使用此属性向组策略分配 VLAN 以简化访问控制。向此属性赋值是在会话中使用 ACL 过滤流量的替代方法。确保您指定了在设备子接口上定义的 VLAN 编号。值的范围为 1 到 4094。

Windows 浏览器代理属性

组策略的 Windows 浏览器代理属性确定用户浏览器上定义的代理是否运行以及如何运行。

可以为 **VPN 会话期间浏览器代理**选择以下值之一：

- **终端设置无变化** - 允许用户配置（或不配置）浏览器代理或HTTP，并在已配置的情况下使用代理。
- **禁用浏览器代理** - 不使用为浏览器定义的代理（如有）。浏览器连接不会通过该代理。
- **自动检测设置** - 在客户端设备的浏览器中启用自动代理服务器检测。
- **使用自定义设置** - 定义所有客户端设备应对 HTTP 流量使用的代理。配置以下设置：
  - **代理服务器 IP 或主机名、端口** - 代理服务器的 IP 地址或主机名，以及代理服务器用于代理连接的端口。主机和端口总共不能超过 100 个字符。
  - **浏览器例外列表** - 与例外列表中的主机/端口的连接不通过代理。添加不应使用代理的所有目标的主机/端口值。例如，www.example.com port 80。点击**添加 (Add)** 链接以将项目添加到列表。点击垃圾桶图标可删除项目。整个代理例外列表（包括所有地址和端口）不能超过 255 个字符。

监控远程访问 VPN

要对远程访问 VPN 进行监控和故障排除，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。

- **show vpn-sessiondb** 显示有关 VPN 会话的信息。您可以使用 **clear vpn-sessiondb** 命令重置这些统计信息。
- **show webvpn** *keyword* 显示的是远程访问 VPN 配置相关信息，包括统计信息和安装的 AnyConnect 映像。输入 **show webvpn ?** 查看可用关键字。
- **show aaa-server** 可显示用于远程访问 VPN 的目录服务器的统计信息。

远程访问 VPN 故障排除

远程访问 VPN 连接问题可能源自客户端或 威胁防御设备配置。以下主题介绍您可能会遇到的主要故障排除问题。

SSL 连接问题故障排除

如果用户无法对外部 IP 地址进行初始非 Secure Client 连接以下载 Secure Client，请执行以下操作：

1. 如果为远程访问 VPN 连接配置文件配置了非默认端口，请确保用户在 URL 中包含该端口号。例如：https://ravpn.example.com:4443
2. 从客户端工作站，验证能否对外部接口的 IP 地址执行 ping 命令。如果不能，请确定从用户工作站到该地址无路由的原因。
3. 从客户端工作站，验证能否对外部接口（即远程访问 [RA] VPN 连接配置文件中定义的接口）的完全限定域名 (FQDN) 执行 ping 操作。如果能够 ping 通 IP 地址但 ping 不通 FQDN，则需要更新客户端和 RA VPN 连接配置文件使用的 DNS 服务器，添加该 FQDN 到 IP 地址的映射。
4. 验证用户是否接受外部接口提供的证书。用户应该永久接受该证书。
5. 检查 RA VPN 连接配置，并验证您是否选择了正确的外部接口。一个常见错误是选择了面向内部网络的内部接口，而不是面向 RA VPN 用户的外部接口。
6. 如果正确配置了 SSL 加密，请使用外部嗅探器来验证 TCP 三次握手是否成功。

Secure Client AnyConnect 下载和安装问题故障排除

如果用户可以与外部接口建立 SSL 连接，但无法下载和安装 Secure Client 软件包，请考虑以下方面：

- 确保您已上传客户端操作系统适用的 Secure Client 软件包。例如，如果用户的工作站运行的是 Linux，但您没有上传 Linux Secure Client 映像，就没有可安装的软件包。
- 对于 Windows 客户端，用户必须获有管理员权限才能安装软件。
- 对于 Windows 客户端，工作站必须启用 ActiveX 或安装 Java JRE 1.5 或更高版本，推荐使用 JRE 7。
- 对于 Safari 浏览器，必须启用 Java。
- 请尝试不同的浏览器，一种浏览器失败不意味着其他浏览器也会失败。

Secure Client 连接问题故障排除

如果用户能够连接到外部接口、下载并安装 Secure Client，然后却无法使用 Secure Client 完成连接，请考虑以下方面：

- 如果使用 DHCP 向客户端提供 IP 地址，并且客户端无法获取地址，请检查 NAT 规则。适用于 RA VPN 网络的任何 NAT 规则都应包括路由查找选项。路由查找可以帮助确保 DHCP 请求通过适当的接口发送到 DHCP 服务器。
- 如果身份验证失败，请检验用户输入的用户名和密码是否正确，该用户名在身份验证服务器中的定义是否正确。身份验证服务器还必须可以通过一个数据接口使用。

注释 如果身份验证服务器在外部网络，则需要配置与该外部网络的站点间 VPN 连接，并将远程访问 VPN 接口地址包括在 VPN 中。有关详细信息，请参阅如何通过远程访问 VPN 使用外部网络上的目录服务器，第 47 页。

- 如果在远程访问 (RA) VPN 连接配置文件中为外部接口配置了完全限定域名 (FQDN)，请验证能否从客户端设备 ping 通该 FQDN。如果能够 ping 通 IP 地址但 ping 不通 FQDN，则需要更新客户端和 RA VPN 连接配置文件使用的 DNS 服务器，添加该 FQDN 到 IP 地址的映射。如果使用的是为外部接口指定 FQDN 时生成的默认 Secure Client 配置文件，用户需要编辑服务器地址才能使用 IP 地址，直到 DNS 被更新。
- 验证用户是否接受外部接口提供的证书。用户应该永久接受该证书。
- 如果用户的 Secure Client 包括多个连接配置文件，请检验其选择的连接配置文件是否正确。
- 如果客户端似乎一切正常，请与 威胁防御设备建立 SSH 连接，并输入 **debug webvpn** 命令。检查尝试连接期间发出的消息。

RA VPN 流量问题故障排除

如果用户可以进行安全远程访问 (RA) VPN 连接，但无法发送和接收流量，请执行以下操作：

1. 使客户端断开连接，然后重新连接。有时此方法会消除问题。
2. 在 Secure Client中，请检查流量统计信息以确定发送和接收的数据包计数器是否在增加。如果接收的数据包计数保持为零，则 威胁防御设备未返回任何流量。这种情况下，威胁防御配置可能存在问题。常见问题包括：
   - 访问规则在阻止流量。检查访问控制策略是否包含阻止内部网络与 RA VPN 地址池之间传递流量的规则。如果您的默认操作是阻止流量，则可能需要创建一个显式“允许”规则。
   - VPN 过滤器会阻止流量。检查连接配置文件的组策略中配置的 ACL 流量过滤器或 VLAN 过滤器。您可能需要在 ACL 中进行调整或更改 VLAN，具体取决于您如何 （或是否）根据组策略过滤流量。
   - RA VPN 流量没有绕过 NAT 规则。确保为每个内部接口的 RA VPN 连接配置 NAT 豁免。或者，确保 NAT 规则不会阻止内部网络和接口与 RA VPN 地址池和外部接口之间的通信。
   - 路由配置错误。确保定义的所有路由有效并在正常工作。例如，如果您为外部接口定义了静态 IP 地址，请确保路由表包含默认路由（对于 0.0.0.0/0 和 ::/0）。

- 确保为 RA VPN 配置的 DNS 服务器和域名正确，并且客户端系统使用的是正确的 DNS 服务器和域名。验证 DNS 服务器是否可访问。
- 如果在 RA VPN 中启用分割隧道，请检查到指定内部网络的流量是否通过该隧道，而所有其他流量则绕过该隧道（以使 威胁防御设备看不到）。

3. 与 威胁防御设备建立 SSH 连接，并验证是否在为远程访问 VPN 发送和接收流量。使用以下命令。
   - **show webvpn anyconnect**
   - **show vpn-sessiondb**

远程访问 VPN 示例

以下是配置远程访问 VPN 的示例。

如何实施 RADIUS 授权更改

RADIUS 授权更改 (CoA)，也称为动态授权，为 威胁防御远程访问 VPN 提供终端安全。RA VPN 的一个主要挑战是保护　内部网络免遭受攻击终端感染，并在终端受病毒或恶意软件感染时，在终端上采取补救措施来保护终端。有必要在所有阶段（即，在 RA VPN 会话之前、过程中和之后）保护终端和内部网络。RADIUS CoA 功能有助于实现此目标。

如果使用思科身份服务引擎 (ISE) RADIUS 服务器，则可以配置授权更改策略实施。

ISE 授权更改功能提供一种机制，以在建立身份验证、授权和记账 (AAA) 会话后更改其属性。当 AAA 中的用户或用户组的策略发生更改时，ISE 会向 威胁防御 设备发送 CoA 消息，以重新初始化身份验证并应用新策略。不需要内联安全状态实施点 (IPEP) 来为与 威胁防御设备建立的每个 VPN 会话应用访问控制列表 (ACL)。

在 CoA 期间可以更改的属性包括重定向 URL、重定向 ACL 和安全组标记。

以下主题介绍 CoA 的运行方式和配置方法。

授权更改系统流程

Cisco ISE 拥有客户端安全状态代理，用于评估终端对条件的合规性，例如主机上安装的进程、文件、注册表项、防病毒保护、反间谍软件防护和防火墙软件。管理员可以限制网络访问权限直至终端合规，或者提高本地用户的权限，使其可以制定补救措施。ISE 终端安全评估可执行客户端评估。客户端从 ISE 获得终端安全评估要求策略、执行终端安全评估数据收集、将结果与策略进行比较，并将评估结果发送回 ISE。

以下是 威胁防御 设备、ISE 和 RA VPN 客户端之间的授权更改 (CoA) 处理流程。

1. 远程用户使用 Secure Client向 威胁防御 设备发起 RA VPN 会话。
2. 威胁防御 设备为此用户向 ISE 服务器发送 RADIUS 访问-请求消息。

3. 由于此时的客户端安全状态是未知的，因此ISE会将用户与为未知安全状态配置的授权策略进行匹配。此策略定义以下 cisco-av-pair 选项，ISE 将在 RADIUS 访问-接受响应中发送到 威胁防御 。

   - **url-redirect-acl=***acl_name*，其中 *acl_name* 是 威胁防御 设备上配置的扩展 ACL 的名称。此 ACL 定义哪些用户流量应重定向到 ISE 服务器，即 HTTP 流量。例如：

     ```
     url-redirect-acl=redirect
     ```

   - **url-redirect=***url*，其中，URL 是流量应重定向到的目标位置。例如：

     ```
     url-redirect=https://ise2.example.com:8443/guestportal/gateway?sessionId=xx&action=cpp
     ```

   您必须为数据接口配置 DNS，以便可以解析主机名。如果在连接配置文件的组策略中还配置流量过滤，请确保客户端池可以通过端口（在示例中为 TCP/8443）到达 ISE 服务器。

4. 威胁防御 设备发送 RADIUS 记账 - 请求开始数据包并接收来自 ISE 的响应。记账请求包含会话的所有详细信息，包括会话 ID、VPN 客户端的外部 IP 地址和 威胁防御 设备的 IP 地址。ISE 使用会话ID来识别会话。威胁防御 设备还会定期发送临时账户信息，其中最重要的属性是 威胁防御 设备分配给客户端的 IP 地址的 Framed-IP-Address 属性。

5. 在未知安全状态的情况下，威胁防御 设备会将流量从匹配重定向 ACL 的客户端重定向至重定向 URL。ISE 确定客户端是否具有所需的安全状态合规性模块，并在必要时提示用户安装。

6. 在客户端设备上安装代理后，代理会自动执行ISE终端安全评估策略中配置的检查。客户端直接与 ISE 通信。它向 ISE 发送终端安全评估报告，其中可以包含使用 SWISS 协议和 8905 TCP/UDP 端口进行的多个交换。

7. 当ISE收到代理发送的终端安全评估报告时，它会再次处理授权规则。这次，终端安全状态是已知的，会有另一个不同的规则与客户端会匹配。ISE 发送 RADIUS CoA 数据包，其中包括适用于兼容或不合规终端的可下载的 ACL (DACL)。例如，合规 DACL 可能允许所有访问，而不合规 DACL 会拒绝所有访问。DACL 内容由 ISE 管理员决定。

8. 威胁防御设备会删除重定向。如果没有缓存DACL，则必须发送访问-请求才可从ISE下载它们。此特定 DACL 与 VPN 会话关联；不会成为设备配置的一部分。

9. 当 RA VPN 用户再次尝试访问网页时，用户可以访问 威胁防御 设备上为此会话安装的 DACL 允许的资源。

注释 如果端点无法满足所有强制性要求，且需要手动采取补救措施时， Secure Client会打开一个补救窗口，显示需要操作的项目。补救窗口在后台运行，以保证网络活动更新不会弹出，引起干扰或中断。用户可以在 Secure Client 的 ISE 终端安全评估图块部分，点击**详细信息**，查看检测到的内容和您加入网络前所需的更新。

在 威胁防御 设备上配置授权更改

大多数授权更改策略是在 ISE 服务器中配置的。但是，您必须将 威胁防御 设备配置为正确连接到 ISE。以下程序介绍如何配置此配置的 威胁防御 端。

开始之前

如果在任何对象中使用了主机名，请确保配置可用于数据接口的DNS服务器，如为数据流量和管理流量配置 DNS中所述。通常，您仍然需要配置 DNS，才可获得功能齐全的系统。

过程

步骤 1 配置扩展的访问控制列表 (ACL)，用于将初始连接重定向到 ISE。

重定向 ACL 的目的是向 ISE 发送初始流量，以便 ISE 可以评估客户端安全状态。ACL 应向 ISE 发送 HTTPS 流量，而非已设定发往 ISE 的流量或被定向到域名解析 DNS 服务器的流量。重定向 ACL 的示例如下所示：

```
access-list redirect extended deny ip any host <ISE server IP>
access-list redirect extended deny ip any host <DNS server IP>
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

但是，请注意，ACL 包含隐式“deny any any”作为最后一个访问控制条目 (ACE)。在此示例中，与 TCP 端口 www（即端口 80）匹配的最后一个 ACE 将不会匹配与前 3 个 ACE 匹配的任何流量，因此这些 ACE 是冗余的。您只需使用最后一个 ACE 创建 ACL 即可获得相同的结果。

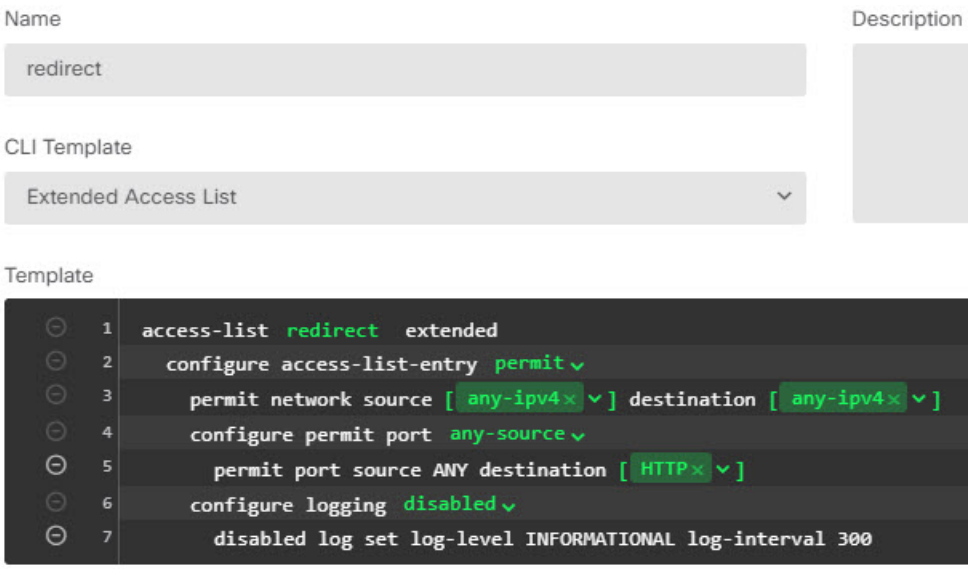
请注意，在重定向 ACL 中，允许和拒绝操作只会确定哪些流量与 ACL 匹配，系统会允许匹配的流量并拒绝不匹配的流量。实际上，系统并不会丢弃任何流量，被拒绝的流量只是未重定向至 ISE。

要创建重定向 ACL，您需要配置 Smart CLI 对象。

a) 选择**设备** > **高级配置** > **Smart CLI** > **对象**。
b) 点击 + 创建新对象。
c) 输入 ACL 的名称。例如，**重定向**。
d) 对于 **CLI 模板**，选择**扩展访问列表**。
e) 在**模板**正文中进行以下配置：

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = any-ipv4
- configure permit port = any-source
- destination-port = HTTP
- configure logging = disabled

ACE 应如下所示：



f) 点击**确定 (OK)**。

在下次部署更改时会配置此 ACL。无需在任何其他策略中使用此对象来强制部署。

注释 此 ACL 仅适用于 IPv4。如果您还想要支持 IPv6，除了要为源和目标网络选择 any-ipv6 外，只需再添加一个拥有所有相同属性的 ACE 即可。您还可以添加其他 ACE，以确保前往 ISE 或 DNS 服务器的流量未被重定向。您首先需要创建主机网络对象，以保留这些服务器的 IP 地址。

步骤 2 配置用于动态授权的 RADIUS 服务器组。

要启用授权更改（也称为动态授权），您必须在 RADIUS 服务器和服务器组对象中正确选择几个关键选项。以下步骤将重点介绍这些属性。有关这些对象的详细信息，请参阅 RADIUS 服务器和组。

a) 依次选择**对象** > **身份源**。

b) 点击 + > **RADIUS 服务器**。

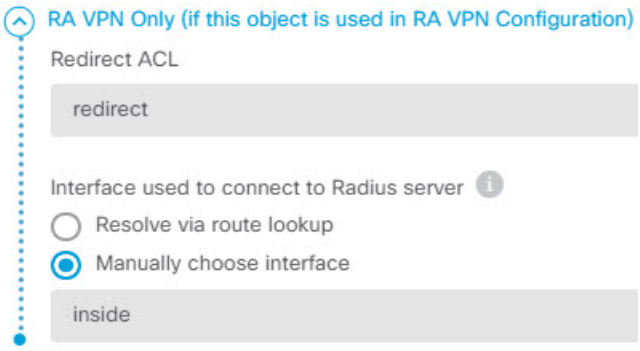
c) 输入服务器名称、ISE RADIUS 服务器的主机名/IP 地址、身份验证端口和服务器上配置的密钥。如果需要，可调整超时。这些选项不直接与动态授权相关。

d) 点击“仅 RA VPN”链接并配置以下选项：

- **重定向 ACL** - 选择您创建的用于重定向的扩展 ACL。在此示例中，ACL 命名为重定向。
- **用于连接 Radius 服务器的接口** - 选择**手动选择接口**，并选择通过其可以访问服务器的接口。您必须选择特定接口，以便系统可以正确启用接口上的 CoA 侦听程序。

  如果此服务器还用于 设备管理器 管理访问，则此接口将被忽略。系统始终通过管理 IP 地址对管理访问尝试进行身份验证。

以下示例展示了为内部接口配置的选项。



e) 点击**确定**保存服务器对象。

如果您设置了冗余，拥有多个相同的 ISE RADIUS 服务器，则请为每个服务器创建服务器对象。

f) 点击 **+** > **RADIUS 服务器组**。

g) 输入服务器组的名称，并根据需要调整空载时间和最大尝试次数。

h) 选择**动态授权**选项，如果 ISE 服务器配置为使用不同的端口，还需要更改端口号。端口 1700 用于侦听 CoA 数据包的默认端口。

i) 如果 RADIUS 服务器配置为使用 AD 服务器对用户进行身份验证，请选择**支持 RADIUS 服务器的领域**，指定与此RADIUS 服务器结合使用的 AD 服务器。如果尚不存在此领域，请点击列表底部的**创建新身份领域**立即配置。

j) 在 **RADIUS 服务器**下，点击 **+** 并选择您为 RA VPN 创建的服务器对象。

k) 点击**确定**保存服务器组对象。

步骤 3 依次选择**设备** > **RA VPN** > **连接配置文件**，并创建使用此 RADIUS 服务器组的连接配置文件。

使用**AAA 身份验证**（单独使用或与证书结合使用），并在**用户身份验证主身份源**、**授权**和**记账**选项中选择服务器组。

请根据组织的需要，配置所有其他选项。

注释 如果通过 VPN 网络访问 DNS 服务器，请编辑连接配置文件中使用的组策略，在分割隧道属性页面上配置**分割 DNS (Split DNS)** 选项。

在 ISE 中配置授权更改

大多数授权更改配置是在ISE服务器中完成的。ISE 具有安全状况评估代理，其在终端设备上运行，ISE 直接与要确定安全状况的设备进行通信。实质上，威胁防御设备会等待 ISE 发出指令，指示其如何处理给定的最终用户。

对配置安全状况评估策略的完整讨论不在本文档的范围之内。但是，以下程序介绍了一些基本配置。可以此为起点来配置 ISE。请注意，各版本中的具体命令路径、页面名称和属性名称可能会发生更改。您使用的 ISE 版本可能使用不同的术语或组织。

支持的最低 ISE 版本为 2.2 补丁 1。

开始之前

此程序假定您已在 ISE RADIUS 服务器中配置用户。

过程

步骤 1 依次选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **网络设备 (Network Devices)**，将 威胁防御 设备添加到“ISE 网络设备”(ISE Network Device) 清单，并配置 RADIUS 设置。

选择 **RADIUS 身份验证设置**，并配置与 威胁防御 RADIUS 服务器对象中配置的共享密钥相同的 **共享密钥** 。如果需要，可更改 **CoA 端口** 号，并确保在 威胁防御 RADIUS 服务器组对象中配置相同的端口。

步骤 2 依次选择**策略** > **策略元素** > **结果** > **授权** > **可下载的 ACL**。

创建 2 个可下载的 ACL (DACL)，一个供合规终端使用，另一个供不合规终端使用。

例如，您可能允许对合规终端 (permit ip any any) 的全部访问，同时拒绝对不合规终端 (deny ip any any) 的全部访问。您可以根据需要调整 DACL 的复杂程度，以根据用户的合规状态为其提供确切的访问权限。您将在授权配置文件中使用这些 DACL。

步骤 3 依次选择**策略** > **策略元素** > **结果** > **授权** > **授权配置文件**并配置所需的配置文件。

您需要适用于以下状态的配置文件。下文列出了每个配置文件至少应具备的属性。

- **未知** - 未知终端安全评估配置文件是默认的终端安全评估配置文件。在初次建立 RA VPN 连接时，每个终端都与此策略匹配。此规则的要点在于，要应用重定向 ACL 和 URL，且如果终端上未安装终端安全评估代理时，还需下载此代理。如果未安装代理或安装失败，终端可以保持与此配置文件关联。否则，在评估终端安全状况后，终端将移至合规或不合规的配置文件。

  至少应具备的属性包括：

  - **名称** - 例如，PRE_POSTURE。
  - **访问类型** - 选择 **ACCESS_ACCEPT**。
  - **常见任务**- 选择 **Web 重定向**（**CWA**、**MDM**、**NSP**、**CPP**），然后选择 **客户端调配**（**安全状况**），并输入您在 威胁防御 设备上配置的重定向 ACL 的名称。在**值**中，选择**客户端调配门户**（如果未选中此选项）。
  - **属性详细信息**应显示两个 cisco-av-pair 值，分别用于 url-redirect-acl 和 url-redirect。ISE 会将此数据发送到 威胁防御 设备，其会将此条件应用于 RA VPN 用户会话。

- **合规** - 终端安全评估完成后，如果终端符合为其配置的所有要求，则客户端被视为合规并可获取此配置文件。通常，您会给予此客户端完全访问权限。

  至少应具备的属性包括：

  - **名称** - 例如，FULL_ACCESS。
  - **访问类型** - 选择 **ACCESS_ACCEPT**。

- **常见任务** - 选择 **DACL 名称**，然后选择适用于合规用户的可下载 ACL，例如 PERMIT_ALL_TRAFFIC。ISE 会将此 ACL 发送到 威胁防御 设备，设备会将其应用于用户会话。此 DACL 将替换用于用户会话的初始重定向 ACL。

- **不合规** - 如果安全状况评估确定终端不符合所有要求，客户端可在一个倒计时时间内让终端符合规范，例如，通过安装所需的更新使终端符合规范。 Secure Client 通知用户合规性问题。在倒计时期间，终端始终处于未知合规状态。如果倒计时完毕后，终端仍不符合规范，则会话会被标记为不合规，并获得不合规配置文件。通常，您将阻止此终端的所有访问，或至少以某种方式限制访问权限。

  至少应具备的属性包括：

  - **名称** - 例如，Non_Compliant。
  - **访问类型** - 选择 **ACCESS_ACCEPT**。
  - **常见任务** - 选择 **DACL 名称**，然后选择适用于不合规用户的可下载 ACL，例如 DENY_ALL_TRAFFIC。ISE 会将此 ACL 发送到 威胁防御 设备，设备会将其应用于用户会话。此 DACL 将替换用于用户会话的初始重定向 ACL。

步骤 4 依次选择**策略** > **策略元素** > **结果** > **客户端调配** > **资源**并配置以下资源：

- **AnyConnect 软件包** - 从 software.cisco.com 下载的头端包文件。支持的客户端平台需要使用单独的软件包，因此您可能需要配置多个类型，例如 AnyConnectDesktopWindows。
- **ISE 安全状况配置文件**（**类型：AnyConnectProfile**）- 此配置文件定义合规性模块用于评估最终用户设备的设置。此文件还定义用户必须在多长时间内使不合规设备变为合规。
- **合规性模块软件包**（**类型：ComplianceModule**） - Secure Client 合规性模块文件是将推送到已安装的 AnyConnect 软件包，用于检查终端合规性的文件。使用**从思科站点添加资源**命令下载此文件。确保根据已配置的 Secure Client 软件包下载正确的模块，否则用户将会下载失败。您还可以在 ISEComplianceModule 文件夹中 Secure Client 列表内的 software.cisco.com 上找到这些文件。
- **AnyConnect 配置文件**（**类型：AnyConnectConfig**）- 这些 Secure Client 版本特定的设置定义要应用的 **AnyConnect 软件包**、**合规性模块**和 **ISE 安全状况**。由于每个操作系统都有各自适用的软件包，因此请为将支持的每个客户端操作系统（例如，Windows、MAC、Linux）创建单独的配置文件。

步骤 5 依次选择**策略** > **客户端调配**并配置客户端调配策略。

为需要实施 CoA 的每个操作系统创建新的规则，例如，使用 CoA_ClientProvisionWin 等名称。为规则选择适当的操作系统，并在**结果**中，选择您为操作系统创建的作为**代理**的 Secure Client 配置文件。

禁用已更换的默认操作系统特定的规则。

步骤 6 配置安全评估策略。

在此步骤中，您制定对组织有意义的终端安全评估要求。

- 依次选择**策略**>**策略元素**>**条件**>**终端安全评估**，并定义需要满足的基本安全评估条件。例如，您可能需要用户已安装特定应用。
- 依次选择**策略** > **策略元素** > **结果** > **终端安全评估** > **要求**，并定义终端的合规性模块要求。
- 依次选择**策略** > **终端安全评估** > **终端安全评估策略**，并配置适用于受支持操作系统的策略。

步骤 7 依次选择**策略** > **策略集** > **默认** > **授权策略**，并创建策略。

为每个合规条件添加规则。这些示例值是基于上一步骤中的示例。

- 未知，用于在安全评估前和安全评估中下载。
  - 名称 - 例如，PRE_POSTURE
  - 条件 -“Session-PostureStatus EQUALS Unknown”和“Radius-NAS-Port-Type EQUALS Virtual”
  - 配置文件 - 例如，PRE_POSTURE
- 合规，适用于符合安全评估要求的客户端。
  - 名称 - 例如，FULL_ACCESS
  - 条件 -“Session-PostureStatus EQUALS Compliant”和“Radius-NAS-Port-Type EQUALS Virtual”
  - 配置文件 - 例如，FULL_ACCESS
- 不合规，适用于不符合安全评估要求的客户端。
  - 名称 - 例如，NON-COMPLIANT
  - 条件 -“Session-PostureStatus EQUALS NonCompliant”和“Radius-NAS-Port-Type EQUALS Virtual”
  - 配置文件 - 例如，Non_Compliant

步骤 8 （可选。）依次选择**管理** > **设置** > **终端安全评估** > **重新评估**，并启用终端安全重新评估。

默认情况下，仅在连接时评估终端安全状况。您可以启用终端安全重新评估，以便定期检查已连接终端的安全状况。您可以设置重新评估间隔，以执行此操作的频率。

如果系统重新评估失败，您可以定义系统应如何做出响应。您可以允许用户继续操作（保持连接），将用户注销，或要求用户修复系统。

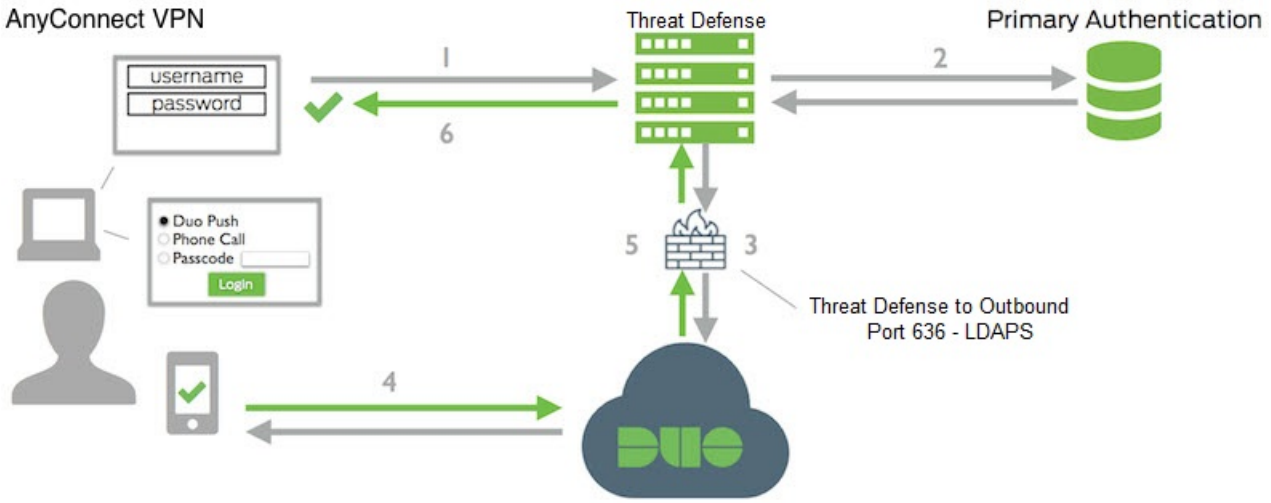
如何使用 Duo LDAP 配置双因素身份验证

可以将 Duo LDAP 服务器作为辅助身份验证源与作为主要源的 Microsoft Active Directory (AD) 或 RADIUS 服务器结合使用。使用 Duo LDAP 时，辅助身份验证使用 Duo 密码、推送通知或电话呼叫验证主要身份验证。

以下主题详细说明这种类型的高级配置。

Duo LDAP 辅助身份验证系统流程

下图显示的是 威胁防御 如何和 Duo 共同发挥作用，以使用 LDAP 提供双因素身份验证。



以下是系统流程的说明：

1. 用户对 威胁防御 设备进行远程访问 VPN 连接，并提供用户名和密码。
2. 威胁防御 使用主身份验证服务器（可能是 Active Directory 或 RADIUS）对此主要身份验证尝试进行身份验证。
3. 如果主身份验证正常工作， 威胁防御 会将辅助身份验证请求发送至 Duo LDAP 服务器。
4. 然后，通过推送通知、带密码的短信消息或电话呼叫单独对用户进行身份验证。用户必须成功完成此身份验证。
5. Duo 响应 威胁防御 设备，以指示用户是否已成功进行身份验证。
6. 如果辅助身份验证成功，则 威胁防御 设备会与用户的 Secure Client建立远程访问 VPN 连接。

配置 Duo LDAP 辅助身份验证

以下操作步骤介绍配置双因素身份验证的端到端过程，使用 Duo LDAP 作为辅助身份验证源，用于远程访问 VPN。请注意，必须拥有一个 Duo 账户，并从 Duo 获取一些信息，才能完成此配置。

过程

步骤 1 创建 Duo 账户并获取集成密钥、密钥和 API 主机名。

以下是对此过程的概述。有关详细信息，请参阅 Duo 网站 https://duo.com。

a) 注册 Duo 账户。
b) 登录到 Duo 管理面板并导航至**应用**，
c) 点击**保护应用**并在应用列表中找到思科 SSL VPN。点击**保护此应用**以获取您的集成密钥、密钥和 API 主机名。如需帮助，请参阅《Duo 入门指南》https://duo.com/docs/getting-started。

步骤 2 创建用于 Duo LDAP 服务器的 Duo LDAP 身份源。

必须使用 威胁防御 API 创建 Duo LDAP 对象，而不可使用 设备管理器创建该对象。可以使用 API Explorer 或编写自己的客户端应用来创建对象。以下步骤介绍如何使用 API Explorer 创建对象。

a) 请登录 设备管理器，点击“更多选项”按钮 ( )，然后选择 **API Explorer**。

系统会在单独的选项卡或窗口中打开 API Explorer，具体取决于您的浏览器设置。

b) （可选。）获取识别系统应用于连接至 Duo LDAP 服务器的接口所需的值。

如果不指定接口，系统将使用路由表。如有必要，可以创建用于Duo LDAP服务器的静态路由。或者，也可以指定要在Duo LDAP对象中使用的接口。如果要指定接口，请使用接口组中的各种 GET 方法获取所需值。可以使用物理接口、子接口、EtherChannel 接口或 VLAN 接口。例如，要获取物理接口的值，请使用 GET/devices/default/interfaces 方法并查找需要使用的接口的对象。需要从接口对象获得以下值：

- id
- type
- version
- name

c) 点击 **DuoLDAPIdentitySource** 标题以打开组。
d) 点击 **POST /object/duoldapidentitysources** 方法。
e) 在**参数**标题下，对于 **body** 元素，点击右侧**数据类型**列中的**示例值**显示框。此操作会将示例加载至正文值编辑框中。
f) 在**正文值**编辑框中，执行以下操作：

- 删除以下属性行：**version**、**id**。（这些属性是 PUT 调用而不是 POST 调用所需的属性。）
- 对于 **name**，请输入对象名称，例如，Duo-LDAP-server。
- 对于 **description**，要么输入对象的有意义说明以供参考，要么删除该属性行。
- 对于 **apiHostname**，请输入您从 Duo 账户中获取的 API 主机名。主机名应如下所示，X 替换为您的唯一值：API-XXXXXXXX.DUOSECURITY.COM。无需大写。

- 对于 **port**，请输入用于 LDAPS 的 TCP 端口。这应该是 636，除非 Duo 通知您使用不同端口。请注意，必须确保访问控制列表允许通过此端口流向 Duo LDAP 服务器的流量。
- 对于 **timeout**，请输入连接到 Duo 服务器所采用的超时时间（以秒为单位）。值可以是 1-300 秒。默认值为 120。要使用默认值，请输入 120 或删除该属性行。
- 对于 **integrationKey**，请输入从您的 Duo 账户获取的集成密钥。
- 对于 **secretKey**，输入从您的 Duo 账户获取的密钥。此密钥随后将被屏蔽。
- 对于 **interface**，请输入要用于连接到 Duo LDAP 服务器的接口的 ID、类型、版本和名称值，或删除用于定义接口属性的 6 行，包括尾部的右大括号。
- 对于 **type**，将值保留为 duoldapidentitysource。

例如，对象正文可能如下所示，其中系统会对 apiHostname 和 integrationKey 进行模糊处理，但会显示故意伪造的密钥：

```
{
  "name": "Duo-LDAP-server",
  "description": "Duo LDAP server for RA VPN",
  "apiHostname": "API-XXXXXXXX.DUOSECURITY.COM",
  "port": 636,
  "timeout": 120,
  "integrationKey": "XXXXXXXXXXXXXXXXXXXX",
  "secretKey": "123456789",
  "type": "duoldapidentitysource"
}
```

g) 点击**试用！**按钮。

系统将发出 **curl** 命令，以将对象发布至设备配置。系统将显示 curl 命令、响应正文和响应代码。如果创建的正文有效，则在**响应代码**字段中应该会看到 **200** 。

如果发生错误，请查看响应正文了解错误消息。可以更正正文值，然后重试。

h) 点击顶部菜单中的 **设备** ，返回至 设备管理器 。

i) 点击**对象**，然后点击目录中的**身份源**。

您的 Duo LDAP 对象应显示在列表中。如未显示，请返回 API Explorer，然后再次尝试创建对象。可以使用 GET 方法检查其是否确实已创建。

请注意，可以使用 设备管理器删除该对象，但不能对其进行编辑或查看其内容。必须使用 API 执行这些操作。相关方法显示在 **DuoLDAPIdentitySource** 组中。

步骤 3 将 Duo 网站的受信任 CA 证书上传至 设备管理器。

威胁防御 系统必须具有验证与 Duo LDAP 服务器的连接所需的证书。可以使用此程序获取并上传证书，该过程已通过 Google Chrome 浏览器完成。适用于您的浏览器的确切步骤可能有所不同。或者，也可以直接转至 https://www.digicert.com/digicert-root-certificates.htm 并下载证书，但以下程序是通用的，可以用其获取任何站点的根受信任 CA 证书。

a) 在浏览器中打开 https://duo.com。

b) 点击浏览器 URL 字段中的站点信息链接，然后点击**证书**链接。此操作将打开“证书信息”对话框。

c) 点击**证书路径**选项卡，并选择路径的根（顶部）级别。在本例中为 DigiCert。

d) 选择 DigiCert，然后点击**查看证书**。此操作将打开一个新的“证书”对话框，“常规”选项卡应指示其已发布给 DigiCert High Assurance EV 根 CA。这是需要上传至 设备管理器的根 CA 证书。

e) 点击**详细信息**选项卡，然后点击**复制到文件**按钮以启动证书下载向导。

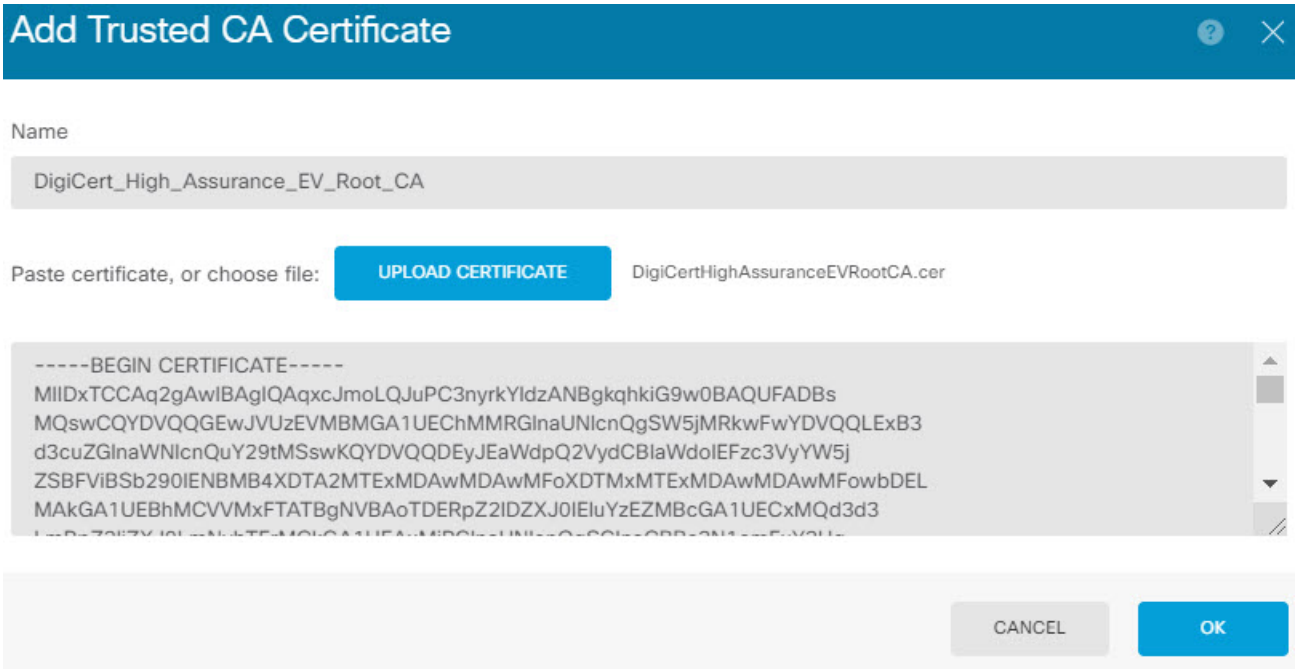
f) 使用该向导将证书下载至您的工作站。使用默认 DER 格式下载。

g) 在 设备管理器中，选择 **对象** > **证书**。

h) 依次点击 + > **添加受信任 CA 证书**。

i) 输入证书名称，例如，DigiCert_High_Assurance_EV_Root_CA。（不允许使用空格。）

j) 点击**上传证书**，然后选择下载的文件。



k) 点击**确定**。

步骤 4 使用 Secure Client 配置文件编辑器创建配置文件，将身份验证超时值指定为 60 秒或更长时间。

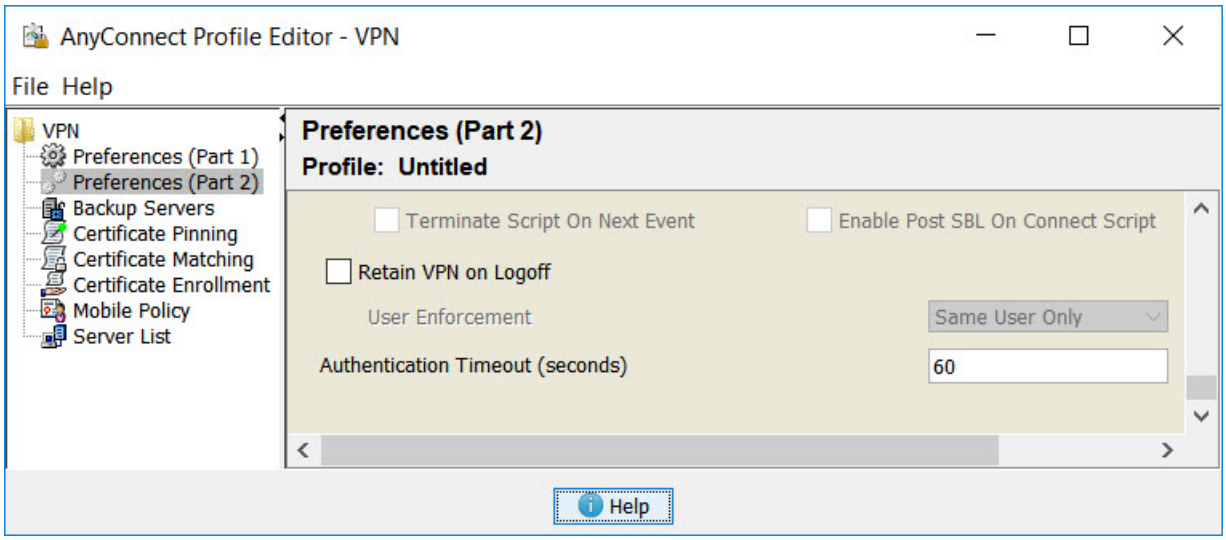
需要为用户提供额外的时间来获取 Duo 密码并完成辅助身份验证。我们建议将此时间设置为至少 60 秒。

有关创建并上传 Secure Client 配置文件的详细信息，请参阅 配置并上传客户端配置文件，第 9 页。以下操作步骤介绍如何仅配置身份验证超时，然后将配置文件上传至 威胁防御。如果要更改其他设置，现在就可以进行更改。

a) 如果尚未执行此操作，请下载并安装 Secure Client 配置文件编辑器软件包。可以在思科软件中心 (software.cisco.com) 相应 Secure Client 版本文件夹内找到此软件包。

b) 打开 Secure Client **VPN 配置文件编辑器 (VPN Profile Editor)**。

c) 在目录中选择**首选项（第 2 部分）**，滚动至页面末尾，并将**身份验证超时**更改为 60（或更大值）。以下是来自 AnyConnect 4.7 VPN 配置文件编辑器的图像；先前或后续版本可能不同。



d) 选择**文件 (File)** > **保存 (Save)**，将配置文件 XML 文件保存至您的工作站，并使用适当名称（例如，duo-ldap-profile.xml）。

现在，可以关闭 VPN 配置文件编辑器应用。

e) 在 设备管理器 中，选择**对象 (Objects)** > **Secure Client 配置文件 (Secure Client Profiles)**。

f) 点击 + 创建新的配置文件对象。

g) 为对象输入**名称**。例如，Duo-LDAP-profile。

h) 点击**上传**，选择创建的 XML 文件。

i) 点击**确定**。

步骤 5 创建组策略，并在策略中选择 Secure Client 配置文件。

分配给用户的组策略控制连接的许多方面。以下操作步骤介绍如何将配置文件 XML 文件分配到组。有关可以使用组策略执行哪些操作的更多详细信息，请参阅为 RA VPN 配置组策略，第 21 页。

a) 在**设备 (Device)** > **远程访问 VPN (Remote Access VPN)** 中点击**查看配置 (View Configuration)**。

b) 选择目录中的**组策略**。

c) 编辑 DfltGrpPolicy，或者点击 + 并创建新的组策略。例如，如果您需要适用于所有用户的单个远程访问 VPN 连接配置文件，则宜编辑默认组策略。

d) 在“常规”(General) 页面上，配置以下属性：

- **名称** - 对于新的配置文件，请输入名称。例如，Duo-LDAP-group。
- **Secure Client 配置文件** - 点击 + 并选择创建的 Secure Client 配置文件对象。

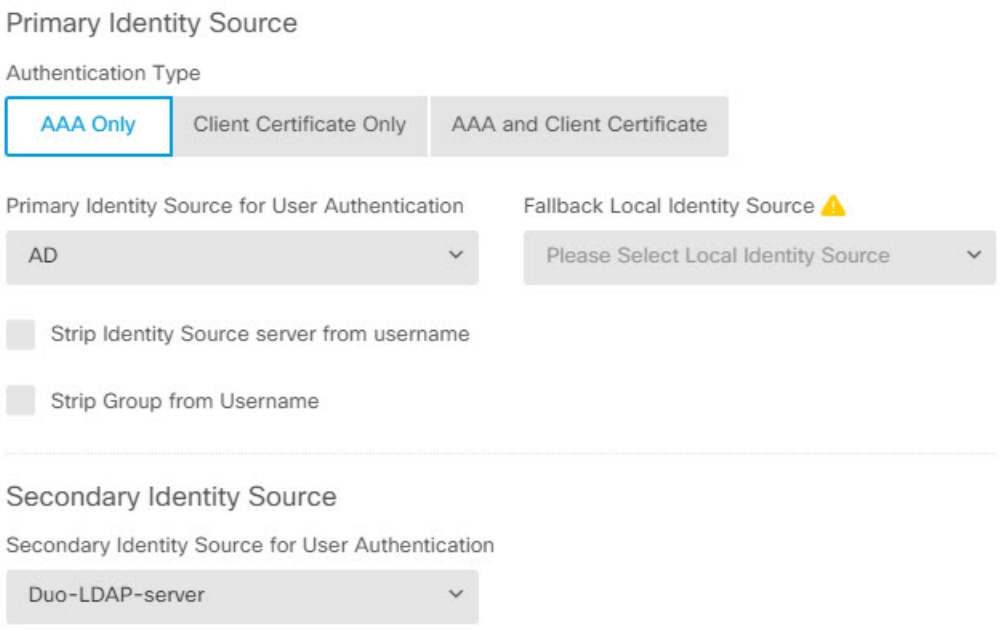
e) 点击**确定**保存组配置文件。

步骤 6 创建或编辑用于 Duo-LDAP 辅助身份验证的远程访问 VPN 连接配置文件。

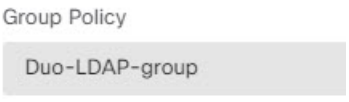
配置连接配置文件有很多步骤，详见配置 RA VPN 连接配置文件，第 14 页。以下操作过程仅介绍将 Duo-LDAP 启用为辅助身份验证源并应用 Secure Client 配置文件所需执行的密钥更改。对于新连接配置文件，必须配置其余必填字段。对于此操作过程，我们假设您正在编辑现有连接配置文件，而且您只需更改这两个设置。

a) 在 RA VPN 页面上，选择目录中的**连接配置文件 (Connection Profiles)**。
b) 编辑现有配置文件或创建新的配置文件。
c) 在主身份源下，配置以下内容：

- **身份验证类型** - 选择**仅 AAA** 或 **AAA 和客户端证书**。除非使用 AAA，否则无法配置双因素身份验证。
- **用于用户身份验证的主要身份源** - 选择主 Active Directory 或 RADIUS 服务器。请注意，可以选择一个 Duo-LDAP 身份源作为主要源。然而，Duo-LDAP 仅提供身份验证服务，而不提供身份服务，因此，如果将其作为主要身份验证源，则在任何控制面板中都将看不到与 RA VPN 连接关联的用户名，且将无法为这些用户编写访问控制规则。（如有需要，可将回退配置为本地身份源。）
- **辅助身份源** - 选择 Duo-LDAP 身份源。



d) 点击**下一步**。
e) 在“远程用户体验”(Remote User Experience) 页面上，选择您创建或编辑的**组策略 (Group Policy)**。



f) 点击此页面上的**下一步 (Next)** 和下一页上的“全局设置”(Global Settings)。
g) 点击**完成**，将更改保存至连接配置文件。

步骤 7 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

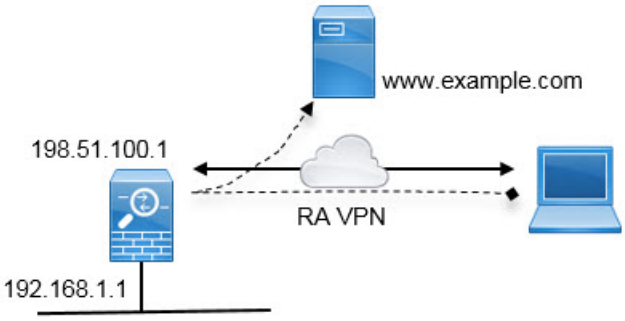
b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

如何在外部接口上为远程访问 VPN 用户提供互联网访问权限（发夹方法）

在远程访问VPN中，您可能希望远程网络用户通过您的设备访问互联网。不过，这些远程用户进入设备所用的接口与访问互联网所用的接口（外部接口）相同，因此需要使互联网流量从外部接口退出。这种技术有时候称为发夹方法。

下图展示了一个示例。外部接口 198.51.100.1 上配置了一个远程访问 VPN。您想要拆分远程用户的 VPN 隧道，以使退出的互联网流量重新回到外部接口，而流向内部网络的流量仍然流经设备。因此，如果远程用户想要访问互联网上的某个服务器（例如 www.example.com），连接会首先通过 VPN，然后从 198.51.100.1 接口路由回到互联网。



以下程序介绍如何配置此服务。

开始之前

此示例假定您已经注册设备、应用远程访问 VPN 许可证并上传 Secure Client 映像。同时还假定您已配置身份领域，并且此领域也用于身份策略。

过程

步骤 1 配置远程访问 VPN 连接。

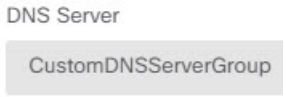
除连接配置文件外，配置还需要自定义的组策略。由于发夹为常见配置，且组策略中所需的设置通常是可用的，因此，在此示例中，我们将编辑默认组策略，而非创建新的组策略。您可以使用任一种方法。

a) 点击**设备** > **远程访问 VPN** 组中的**查看配置**。

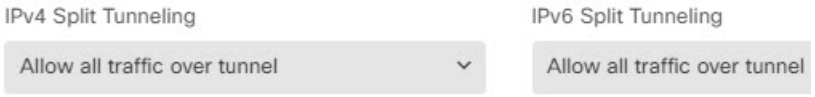
b) 点击目录中的**组策略**，然后点击 DfltGrpPolicy 对象的编辑图标 ( ) 。

c) 对默认组策略进行以下更改：

- 在 **DNS 服务器 (DNS Server)** 的**常规 (General)** 页面，选择定义服务器 VPN 终端在解析域名时应使用的 DNS 服务器组。



- 在**分割隧道 (Split Tunneling)** 页面上，为 **IPv4** 和 **IPv6 分割隧道 (IPv6 Split Tunneling)** 选择**允许所有流量通过隧道选项 (Allow all traffic over tunnel option)**。这是默认设置，因此它可能已正确配置。



注释 **此设置对启用发夹至关重要**。您希望所有流量都通过 VPN 网关，而分割隧道这种方法允许远程客户端直接访问 VPN 外部的本地或互联网站点。

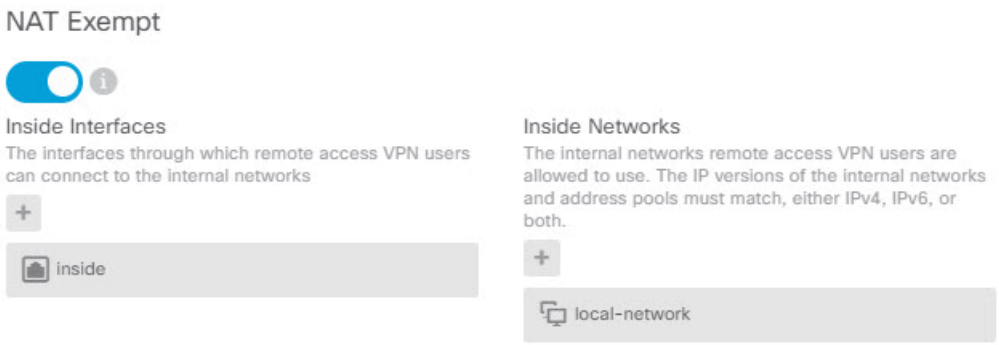
d) 点击**确定**，保存对默认组策略的更改。

e) 点击**连接配置文件**，编辑现有配置文件或创建新的配置文件。

f) 在连接配置文件中，就像配置任何其他 RA VPN 配置一样，按照向导程序操作并配置所有选项。但是，您必须正确配置以下选项才可启用发夹：

- 第 2 步中的**组策略**。选择需要为发夹自定义的组策略。

- 第 3 步中的 **NAT 豁免**。启用此功能。选择内部接口，然后选择定义内部网络的网络对象。在本示例中，该对象应指定 192.168.1.0/24。流向内部网络的 RA VPN 流量不会进行地址转换。但是，应用发夹方法的流量通过外部接口传出，因此这些流量仍会进行 NAT，因为 NAT 豁免仅适用于内部接口。请注意，如果您定义了其他连接配置文件，则需要将其添加到现有设置中，因为此配置适用于所有连接配置文件。



注释　**NAT 豁免**选项是另一个对发夹配置十分重要的设置。

g) （可选。）在**全局设置**步骤中，选择**为已解密流量绕过访问控制策略 (sysopt permit-vpn)** 选项。

选择此选项，则无需再配置访问控制规则以允许来自 RA VPN 地址池的流量通过。此选项可提供更好的安全性（外部用户无法骗取池中的地址），但会使得 RA VPN 流量不再会接受检查，包括 URL 过滤和入侵保护。请充分考虑此选项的优缺点再决定是否需要选择。

h) 查看远程访问 VPN 配置，然后点击**完成**。

步骤 2 将 NAT 规则配置为将外部接口发出的所有连接转换到外部 IP 地址上的端口（接口 PAT）。

完成初始设备配置后，系统将创建名为 InsideOutsideNatRule 的 NAT 规则。此规则将接口 PAT 应用于任意接口上通过外部接口流出设备的 IPv4 流量。由于外部接口包含在“任何”源接口中，因此，此规则已经存在，除非您对所需的规则进行编辑或将其删除。

以下程序介绍如何创建所需的规则。

a) 依次点击**策略** > **NAT**。

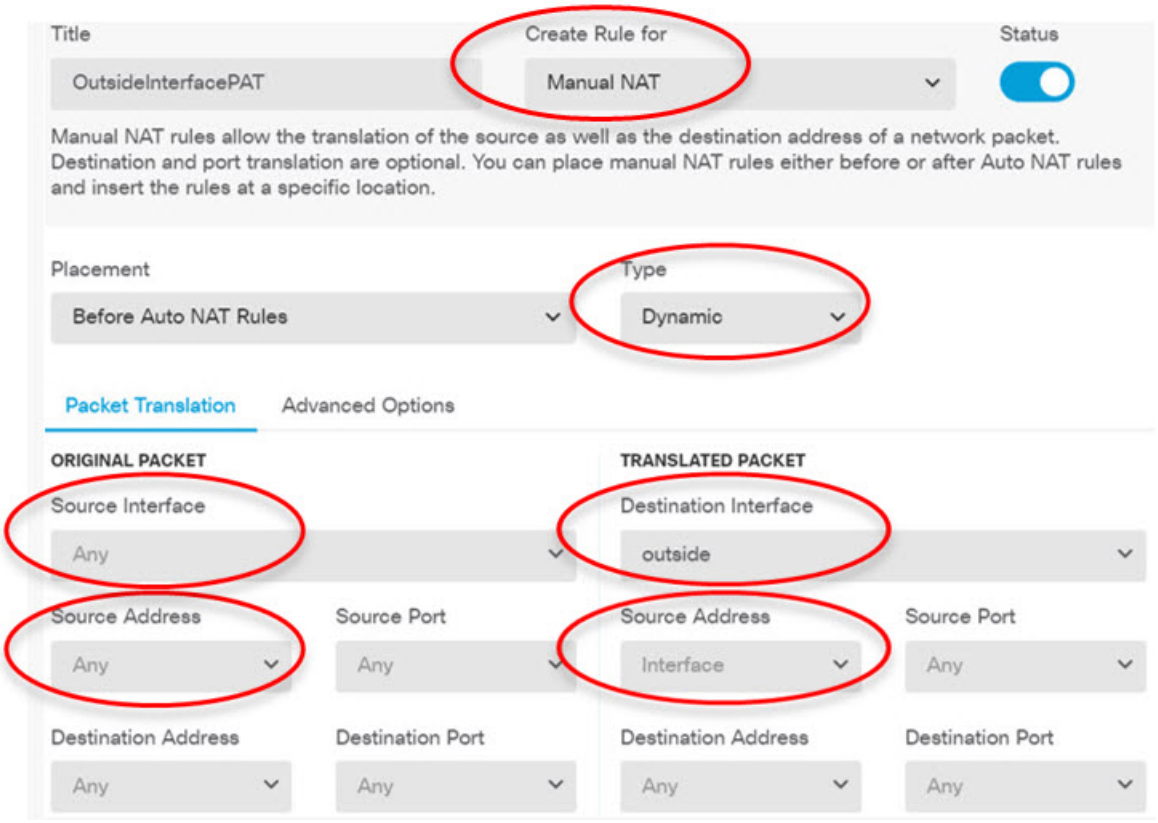
b) 执行以下操作之一：

- 要编辑 InsideOutsideNatRule，请将鼠标指针悬停在**操作**列上，然后点击编辑图标 ( )。
- 要创建新规则，请点击 **+**。

c) 配置规则的以下属性：

- **名称** - 为新规则输入一个有意义且不含空格的名称。例如，OutsideInterfacePAT。
- **创建规则用于** - **手动 NAT**。
- **位置** - **自动 NAT 规则之前**（默认）。
- **类型** - **动态**。
- **原始数据包** - 对于**源地址**，请选择“任何”或 any-ipv4。对于**源接口**，请确保选择“任何”（默认值）。对于所有其他“原始数据包”选项，请保留默认值“任何”。
- **已转换的数据包** - 对于**目标接口**，请选择外部接口。对于**已转换的地址**，请选择**接口**。对于所有其他“已转换的数据包”选项，请保留默认值“任何”。

下图展示了选择“任何”作为源地址时的简单情况。



d) 点击**确定**。

步骤 3 （如果不在连接配置文件中配置**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)**。）配置访问控制规则，以允许从远程访问 VPN 地址池进行访问。

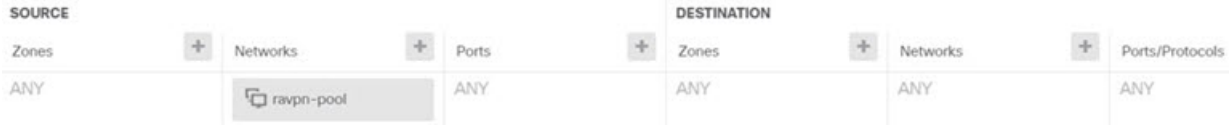
如果在连接配置文件中选择**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)**，则来自 RA VPN 池地址的流量会绕过访问控制策略。您无法编写将应用于此流量的访问控制规则。仅当禁用此选项时，才需要编写规则。

在以下示例中，允许来自地址池的流量流至任何目标。您可以根据自己的具体要求调整此选项。也可以在此规则之前添加阻止规则，过滤掉不必要的流量。

a) 依次点击**策略** > **访问控制**。
b) 点击 + 创建新规则。
c) 配置规则的以下属性：

- **顺序** - 在策略中选择一个位置，此位置应位于可能会匹配并阻止这些连接的任何其他规则之前。默认情况下，会将该规则添加到策略的末尾。如果稍后需要重新调整规则的位置，可以编辑此选项，也可以直接将规则拖放到表格中相应的位置。
- **名称** - 输入一个有意义且不含空格的名称。例如，RAVPN-address-pool。
- **操作** - **允许**。如果不希望对此流量执行协议违规检测或入侵检测，可以选择“信任”。

- **源/目标**选项卡 - 对于**源** > **网络**，请选择在远程访问 VPN 连接配置文件中用于地址池的同一对象。对于所有其他“源”和“目标”选项，请保留默认值“任何”。



- **应用**、**URL** 和**用户**选项卡 - 保留这些选项卡的默认设置，即不做任何选择。
- **入侵**、**文件**选项卡 -（可选）您可以选择入侵或文件策略，以进行威胁或恶意软件检测。
- **日志记录**选项卡 -（可选）您可以选择启用连接日志记录。

d) 点击**确定 (OK)**。

步骤 4 确认您的更改。

a) 点击网页右上角的**部署更改**图标。

b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

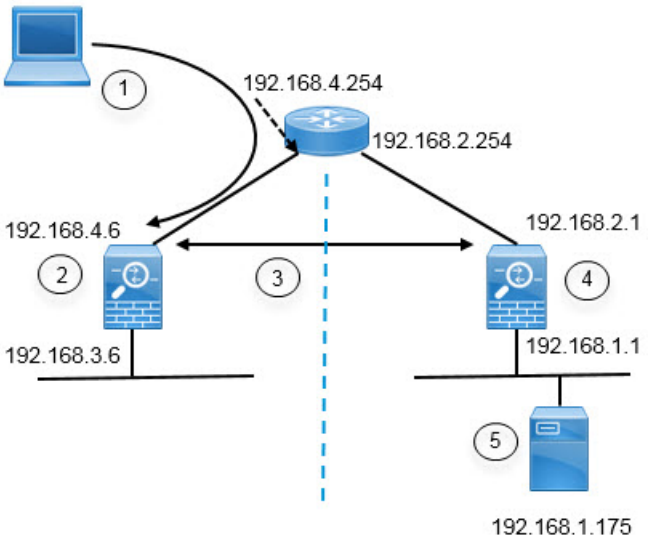
如何通过远程访问 VPN 使用外部网络上的目录服务器

您可以配置远程访问 VPN，以便移动员工和远程办公人员安全地连接到内部网络。此连接的安全性取决于您的目录服务器，该目录服务器对用户连接进行身份验证，以确保仅授权用户才能登录。

如果您的目录服务器位于外部网络而非内部网络上，则需要配置从外部接口到包含目录服务器的网络的站点间 VPN 连接。**站点间 VPN 配置有一个诀窍**：您必须将远程访问 VPN 设备的外部接口地址包括在站点间VPN连接的“内部”网络内，还必须将其包括在目录服务器所在设备的远程网络中。后续程序会对此加以说明。

注释 如果使用数据接口作为虚拟管理接口的网关，此配置还允许将目录用于身份策略。如果不使用数据接口作为管理网关，请确保存在从管理网络到参与站点间 VPN 连接的内部网络的路由。

此使用案例实施以下网络场景。



图中标注	说明
1	与 192.168.4.6 建立 VPN 连接的远程访问主机。客户端将在 172.18.1.0/24 地址池中获得一个地址。
2	站点 A，托管远程访问 VPN。
3	站点 A 和站点 B 威胁防御 设备的外部接口之间的站点间 VPN 隧道。
4	站点 B，托管目录服务器。
5	目录服务器，位于站点 B 的内部网络上。

开始之前

此使用案例假定您按照设备安装向导进行了正常的基准配置。具体包括：

- 有一条 Inside_Outside_Rule 访问控制规则，允许（或信任）从 inside_zone 到 outside_zone 的流量。
- inside_zone 和 outside_zone 安全区（分别）包含内部和外部接口。
- 有一个 InsideOutsideNATRule，对从内部接口到外部接口的所有流量执行接口 PAT。对于默认情况下使用内部网桥组的设备，可能存在多个接口 PAT 规则。
- 存在 0.0.0.0/0 的一条静态 IPv4 路由，指向外部接口。此示例假定您对外部接口使用静态 IP 地址，但也可以使用 DHCP 动态获取静态路由。在本示例中，我们假定采用以下静态路由：
  - 站点 A：外部接口，网关为 192.168.4.254。
  - 站点 B：外部接口，网关为 192.168.2.254。

过程

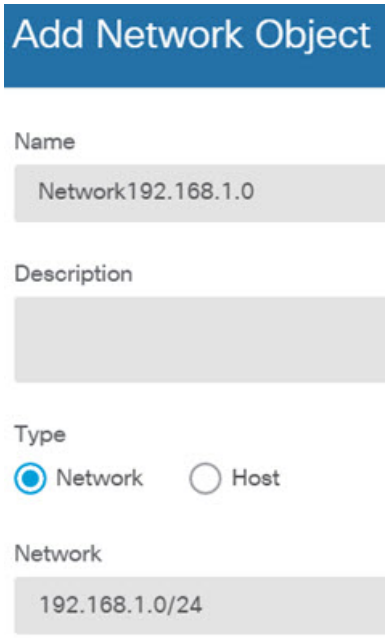
步骤 1 配置**站点 B**（托管目录服务器）上的站点间 VPN 连接。

a) 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。

b) 点击 + 按钮。

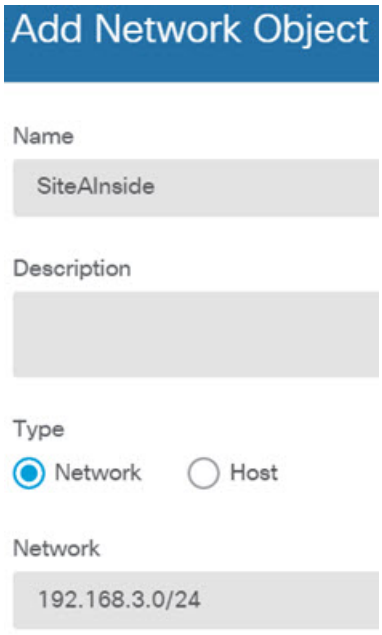
c) 为**终端设置**配置以下选项。

- **连接配置文件名称** - 输入名称，例如 SiteA（表示连接到站点 A）。
- **本地站点** - 这些选项定义本地终端。
  - **本地 VPN 访问接口** - 选择**外部**接口（图表中地址为 192.168.2.1 的那一个接口）。
  - **本地网络** - 点击 + 并选择标识应参与 VPN 连接的本地网络的网络对象。由于目录服务器在此网络上，因此可以参与站点间VPN。假定该对象尚不存在，点击**创建新网络**并为 192.168.1.0/24 网络配置对象。在保存对象后，在下拉列表中选择它并点击**确定**。

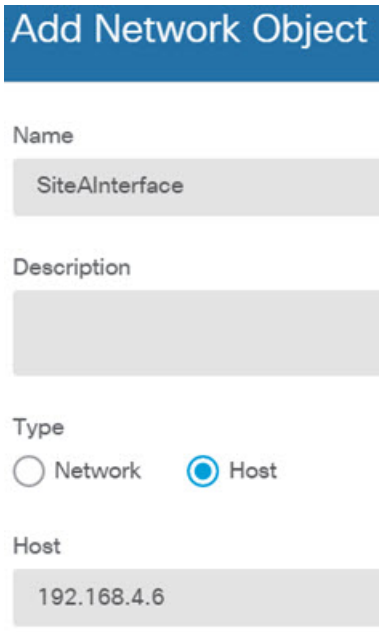


- **远程站点** - 这些选项定义远程终端。
  - **远程 IP 地址** - 输入 192.168.4.6，这是将托管 VPN 连接的远程 VPN 对等体接口的 IP 地址。
  - **远程网络** - 点击 + 并选择标识应参与 VPN 连接的远程网络的网络对象。点击**创建新网络**，配置以下对象，然后在列表中选择它们。

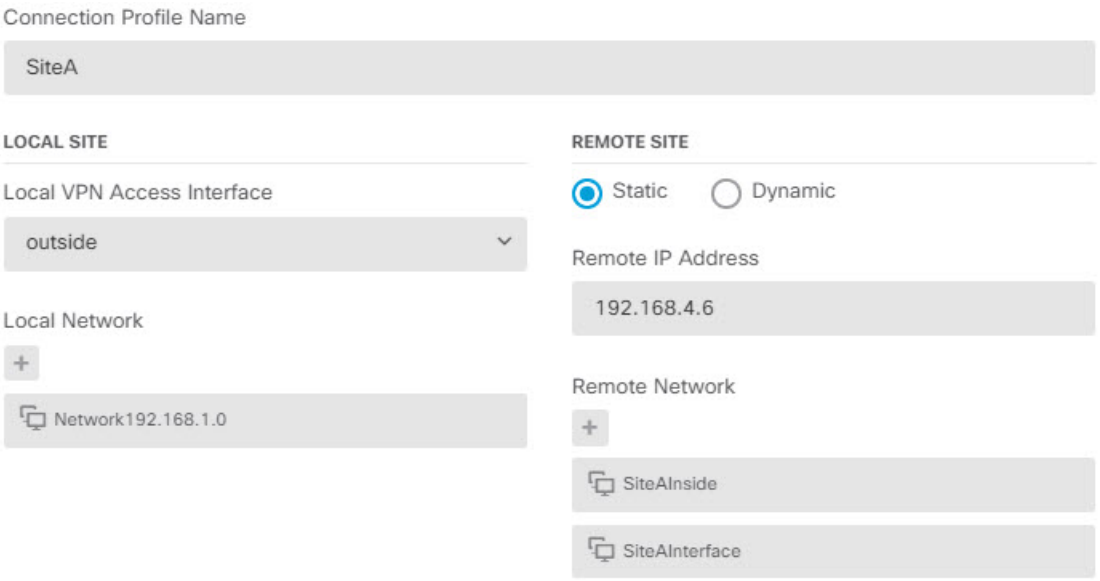
    1. SiteAInside，网络，192.168.3.0/24。



2. SiteAInterface，主机，192.168.4.6。这是关键：您必须将远程访问 **VPN** 连接点地址作为站点间 **VPN** 连接的远程网络的一部分，以便该接口上托管的 **RA VPN** 可以使用目录服务器。



完成后，终端设置应如下所示：



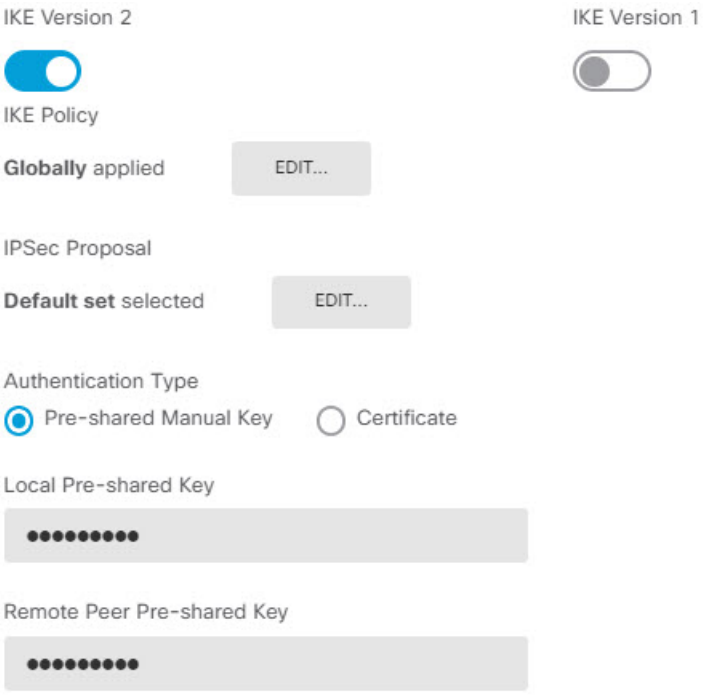
d) 点击**下一步**。

e) 定义 VPN 的隐私配置。

在本使用案例中，我们假定您符合出口控制功能的要求，允许使用强加密。调整这些示例设置以满足您的需求和许可证合规性。

- **IKE 版本 2**、**IKE 版本 1** - 保留默认设置，启用 **IKE 版本 2**，禁用 **IKE 版本 1**。
- **IKE 策略** - 点击**编辑**并启用 **AES-GCM-NULL-SHA** 和 **AES-SHA-SHA**，禁用 **DES-SHA-SHA**。
- **IPsec 提议** - 点击**编辑**。在“选择 IPSec 提议”对话框中，点击 **+**，然后点击**设置默认值**以选择默认 AES-GCM 提议。
- **本地预共享密钥**、**远程对等体预共享密钥** - 输入此设备和远程设备上为 VPN 连接定义的密钥。这些密钥在 IKEv2 中可能不同。该密钥可以有 1 至 127 个字母数字字符。**记住这些密钥，因为在站点 A 设备上创建站点间 VPN 连接时，必须配置相同的字符串**。

IKE 策略应如下所示：



f) 配置**其他选项**。

- **NAT 豁免** - 选择托管内部网络的接口，在本示例中为**内部**接口。通常，您不希望站点间 VPN 隧道中的流量转换其 IP 地址。此选项仅在本地网络驻留在单个路由接口（而非网桥组成员）后时有用。如果本地网络位于多个路由接口或一个或多个网桥组成员之后，则必须手动创建 NAT 豁免规则。有关手动创建所需规则的信息，请参阅使站点间 VPN 流量豁免 NAT。
- **完美前向保密的 Diffie-Hellman 组** - 选择**第 19 组**。此选项决定是否使用完美前向保密 (PFS) 为每个加密交换生成和使用唯一会话密钥。唯一会话密钥可保护交换免于后续解密，即使整个交换已被记录且攻击者已经获得终端设备使用的预共享密钥或私钥。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组。

该选项应如下所示：

g) 点击**下一步**。

h) 查看摘要并点击**完成**。

摘要信息将复制到剪贴板。您可以将这些信息粘贴到文档中，并使用它来帮助您配置远程对等体，或将其发送到负责配置对等体的一方。

i) 点击网页右上角的**部署更改**图标。

j) 点击**立即部署**按钮，并等待部署成功完成。

现在，站点 B 设备已准备好托管站点间 VPN 连接的一端。

步骤 2 注销**站点 B** 设备并登录**站点 A** 设备。

步骤 3 配置**站点 A**（托管远程访问 VPN）上的站点间 VPN 连接。

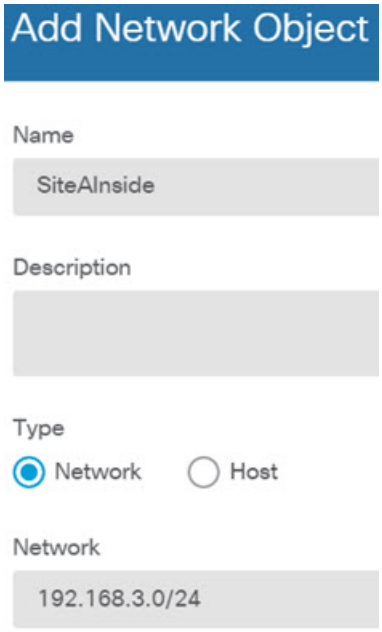
a) 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。

b) 点击 + 按钮。

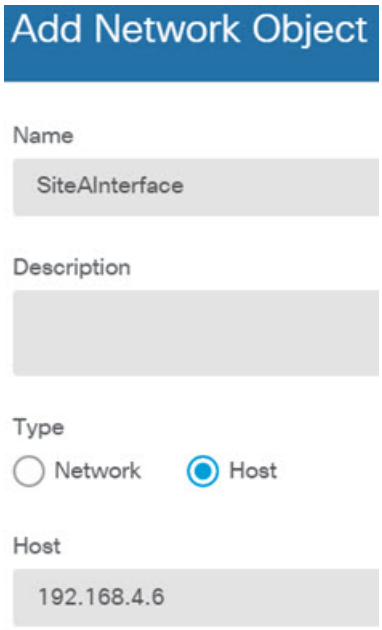
c) 为**终端设置**配置以下选项。

- **连接配置文件名称** - 输入名称，例如 SiteB（表示连接到站点 B）。
- **本地站点** - 这些选项定义本地终端。
  - **本地 VPN 接入接口** - 选择**外部**接口（图表中地址为 192.168.4.6 的那一个接口）。
  - **本地网络** - 点击 + 并选择标识应参与 VPN 连接的本地网络的网络对象。点击**创建新网络**，配置以下对象，然后在列表中选择它们。**注意，您已在站点 B 设备中创建相同的对象，但是您必须在站点 A 设备中重新创建它们。**

1. SiteAInside，网络，192.168.3.0/24。

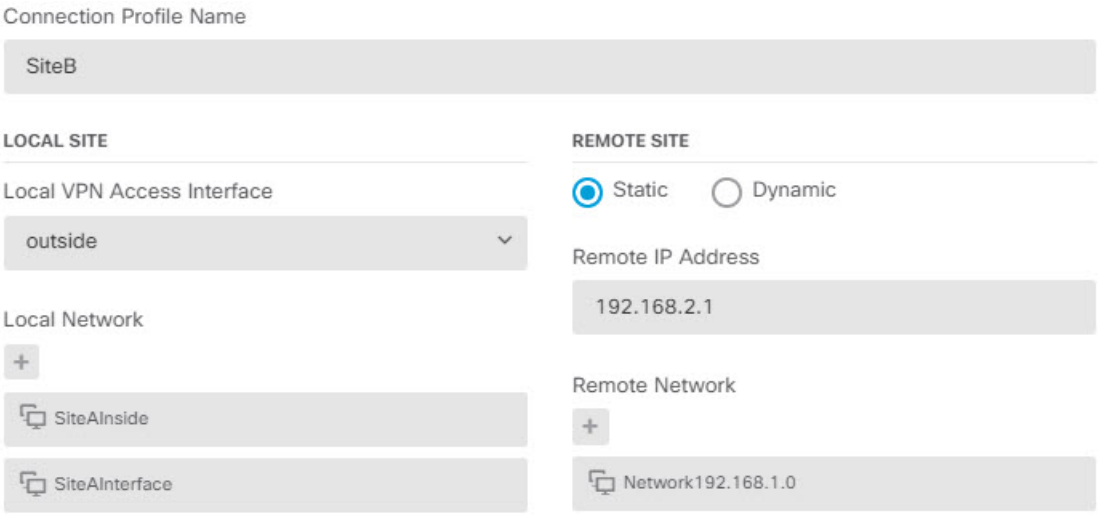


2. SiteAInterface，主机，192.168.4.6。**这是关键：您必须将远程访问 VPN 连接点地址作为站点间 VPN 连接的内部网络的一部分，以便该接口上托管的 RA VPN 可以使用远程网络上的目录服务器。**



- **远程站点** - 这些选项定义远程终端。
  - **远程 IP 地址** - 输入 192.168.2.1，这是将托管 VPN 连接的远程 VPN 对等体接口的 IP 地址。
  - **远程网络** - 点击 + 并选择标识应该参与 VPN 连接的远程网络的网络对象（包含目录服务器的 VPN 连接）。点击**创建新网络**并为 192.168.1.0/24 网络配置对象。在保存对象后，在下拉列表中选择它并点击**确定**。**注意，您已在站点 B 设备中创建相同的对象，但是您必须在站点 A 设备中重新创建它。**

完成后，终端设置应如下所示。请注意，与站点 B 设置相比，本地/远程网络是相反的。点对点连接的两端看起来应始终是这样的。

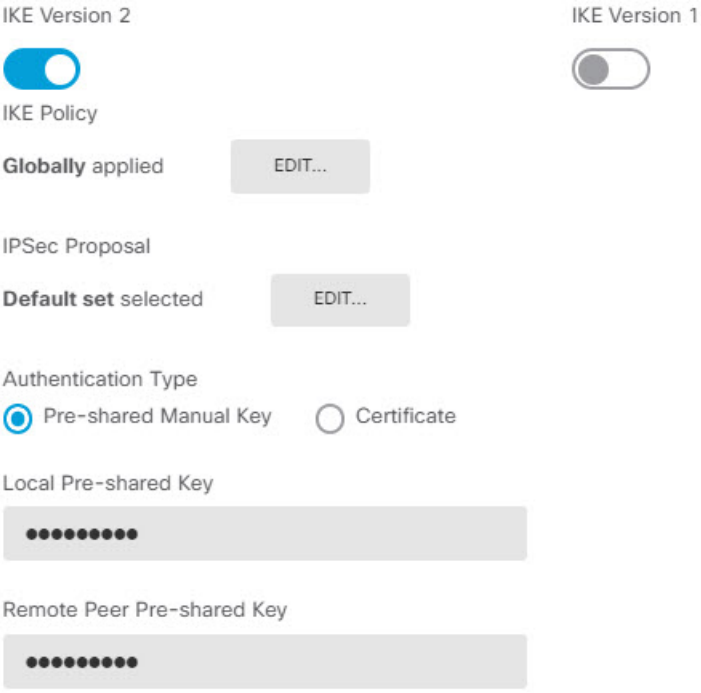


d) 点击**下一步**。

e) 定义 VPN 的隐私配置。

与站点 B 连接一样，配置相同的 IKE 版本、策略和 IPsec 提议，以及相同的预共享密钥，**但请确保调换本地和远程预共享密钥**。

IKE 策略应如下所示：



f) 配置**其他选项**。

- **NAT 豁免** - 选择托管内部网络的接口，在本示例中为**内部**接口。通常，您不希望站点间 VPN 隧道中的流量转换其 IP 地址。此选项仅在本地网络驻留在单个路由接口（而非网桥组成员）后时有用。如果本地网络位于多个路由接口或一个或多个网桥组成员之后，则必须手动创建 NAT 豁免规则。有关手动创建所需规则的信息，请参阅使站点间 VPN 流量豁免 NAT。
- **完美前向保密的 Diffie-Hellman 组** - 选择**第 19 组**。

该选项应如下所示：

g) 点击**下一步**。
h) 查看摘要并点击**完成**。
i) 点击网页右上角的**部署更改**图标。

j) 点击**立即部署**按钮，并等待部署成功完成。

现在，站点 A 设备已准备好托管站点间 VPN 连接的另一端。由于站点 B 已经配置了兼容设置，因此两台设备应该协商 VPN 连接。

您可以登录设备 CLI 并对目录服务器进行 ping 测试，从而确认连接。您也可以使用 **show ipsec sa** 命令查看会话信息。

步骤 4 在**站点 A** 上配置目录服务器。点击**测试**验证是否有连接。

a) 选择**对象**，然后从目录中选择**身份源**。
b) 点击 **+** > **AD**。
c) 配置基本领域属性。

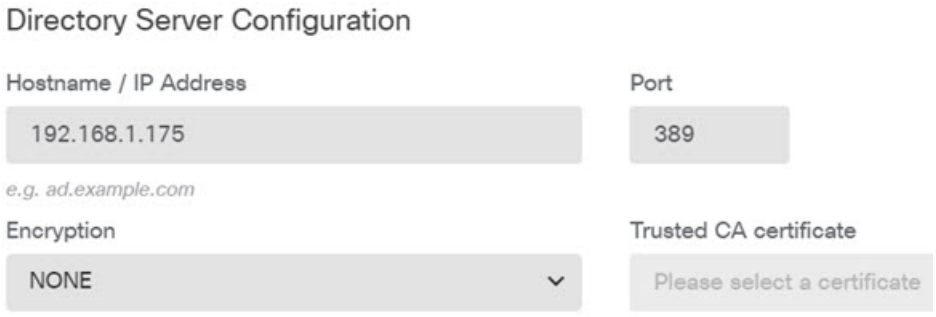
- **名称** - 目录领域的名称。例如，AD。
- **类型** - 目录服务器的类型。Active Directory 是唯一支持的类型，所以无法更改此字段。
- **目录用户名**、**目录密码** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

  注释 系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=adminisntrator、cn=users、dc=example、dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准 DN** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如，cn=users,dc=example,dc=com。有关查找基准 DN 的信息，请参阅确定目录基准标识名。
- **AD 主域** - 设备应加入的 Active Directory 完全限定域名。例如 example.com。

d) 配置目录服务器属性。

- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。在本例中，输入 192.168.1.175。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。在本例中，保留 389。
- **加密** - 使用加密连接下载用户和组信息。系统默认为**无**，也就是说以明文形式下载用户和组信息。对于 RA VPN，您可以使用 **LDAPS**，即基于 SSL 的 LDAP。如果选择此选项，则使用端口 636。RA VPN 不支持 STARTTLS。对于此示例，选择**无**。
- **受信任的 CA 证书** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 192.168.1.175 作为 IP 地址，但证书中的地址为 ad.example.com，则连接会失败。



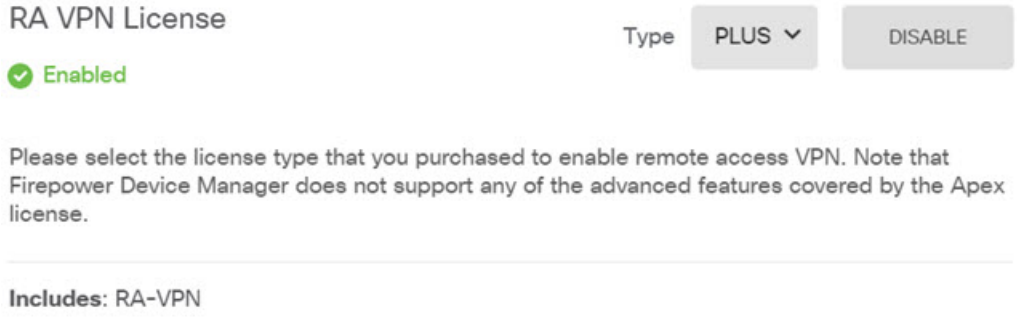
e) 点击**测试**按钮验证系统是否可以与服务器通信。

系统使用单独的进程访问服务器，因此您可能会收到错误通知，指出连接适用于一种用途而不适用于另一种用途，例如可用于身份策略，但不可用于远程访问 VPN。如果无法访问服务器，请确认 IP 地址和主机名正确、DNS 服务器具有该主机名的条目等。另外，验证站点间 VPN 连接是否正常工作，并且您在 VPN 中包含了站点 A 的外部接口地址，并且 NAT 不会转换目录服务器的流量。您可能还需要为服务器配置静态路由。

f) 点击**确定**。

步骤 5 依次点击**设备** > **智能许可证** > **查看配置**，然后启用 RA VPN 许可证。

启用 RA VPN 许可证时，请选择您购买的许可证类型：Plus、Apex（或两者）或仅 VPN。有关详细信息，请参阅远程访问 VPN 的许可要求，第 7 页。

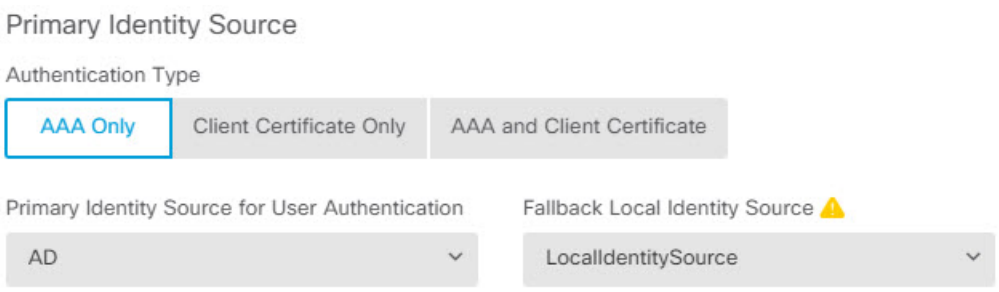


步骤 6 在站点 A 上配置远程访问 VPN。

a) 点击**设备** > **远程访问 VPN** 组中的**查看配置**。确保您位于**连接配置文件 (Connection Profiles)** 页面。

b) 创建或编辑连接配置文件。

c) 在向导的第一步中，设置配置文件名称，然后选择 AD 领域作为主身份验证源。或者，您可以选择本地数据库作为备用身份源。



d) 配置地址池。

对于本示例，点击 +，然后在 IPv4 地址池中选择**创建新的网络**，并为 172.18.1.0/24 网络创建一个对象，然后选择此对象。从该地址池中为客户端分配地址。将 IPv6 池留空。地址池不能与外部接口的 IP 地址位于同一子网。

该对象应如下所示：

该地址池规范应如下所示：

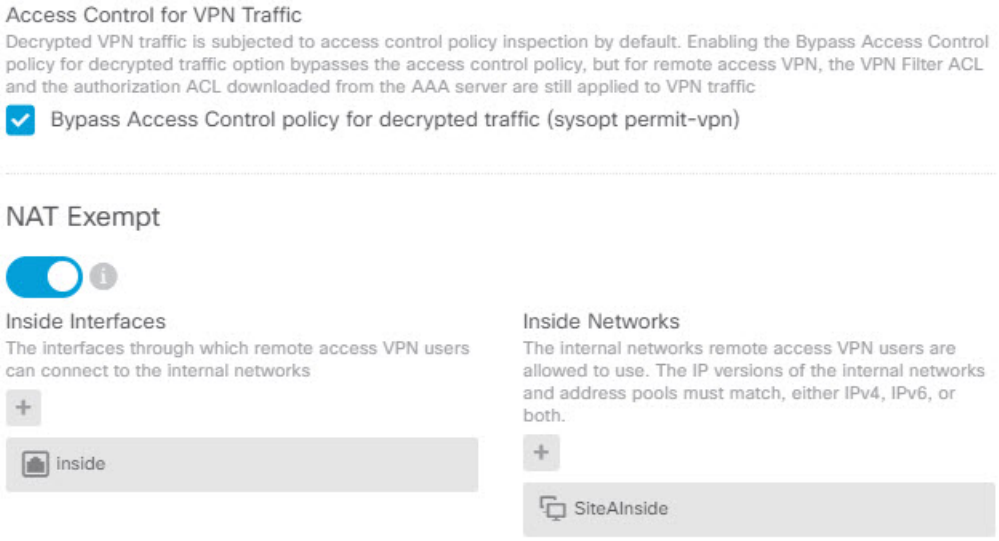
e) 点击**下一步**，然后选择适当的组策略。

选中您选择的策略的摘要信息。确保已配置 DNS 服务器。如果未配置，请立即编辑策略并配置 DNS。

f) 点击**下一步**，并在全局设置中，选择**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** 选项，并配置 **NAT 豁免**选项。

对于 **NAT 豁免**，您需要配置以下选项。请注意，如果您定义了其他连接配置文件，则需要将其添加到现有设置中，因为此配置适用于所有连接配置文件。

- **内部接口** - 选择**内部**接口。这些是远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
- **内部网络** - 选择 SiteAInside 网络对象。这些是代表远程用户将访问的内部网络的网络对象。



g) 上传适用于受支持平台的 Secure Client 软件包。

h) 点击**下一步**并验证设置。

首先，验证摘要是否正确。

然后，点击 **说明** 查看最终用户初步安装 Secure Client 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击**复制**以将这些说明复制到剪贴板，然后将它们粘贴在文本文件或邮件中。

i) 点击**完成**。

步骤 7 点击网页右上角的**部署更改**图标。

步骤 8 点击**立即部署**按钮，并等待部署成功完成。

现在，站点 A 设备已准备好接受 RA VPN 连接。让外部用户安装 Secure Client 客户端并完成 VPN 连接。

您可以登录设备 CLI 并使用 **show vpn-sessiondb anyconnect** 命令查看会话信息，从而确认连接。

如何通过组控制 RA VPN 访问

您可以配置远程访问VPN连接配置文件，以根据组策略提供对内部资源的差异化访问权限。例如，如果您想要向员工提供不受限制的访问权限，但仅向承包商提供单个　内部网络的访问权限，则可以使用组策略来定义不同的 ACL，以适当地限制访问。

以下示例展示了如何为应只能访问 192.168.2.0/24 内部子网的承包商设置 RA VPN 连接。对于常规员工，您可以使用默认组策略，其中没有为VPN定义流量过滤器。如果您想要对这些用户设置限制，并应用按照以下方法构建的 ACL，则可以编辑默认组策略。

开始之前

此程序假定您已创建要用于承包商的身份源。此身份源可能不同于您用于常规员工的身份源。由于此身份源并非与限制访问严格相关，因此我们可以在本示例中忽略它。

此示例还假设“inside2”接口配置为托管 192.168.2.0/24 子网，其 IP 地址为 192.168.2.1（子网上的任何其他地址也是可接受的）。

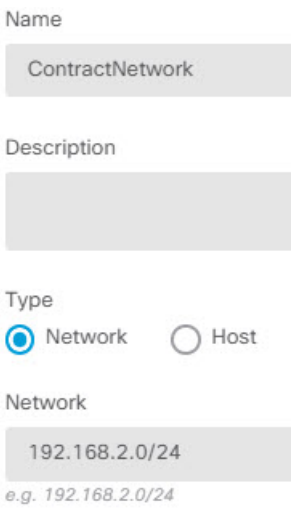
过程

步骤 1 配置扩展访问控制列表 (ACL)，以限制 RA VPN 流量。

您需要先配置定义目标 192.168.2.0/24 的网络对象，然后创建 Smart CLI 对象，定义此访问列表。由于 ACL 在末尾包含隐式拒绝语句，因此您需要仅允许对子网的访问，且定向至子网外部任何 IP 地址的流量将被拒绝。此示例仅适用于 IPv4；您还可以配置对象，来限制对特定子网的 IPv6 访问。只需创建网络对象并将基于 IPv6 的 ACE 添加到相同的 ACL。

a) 依次选择**对象** > **网络**，并创建所需的对象。

例如，将对象命名为 ContractNetwork。此对象应与以下所示类似：

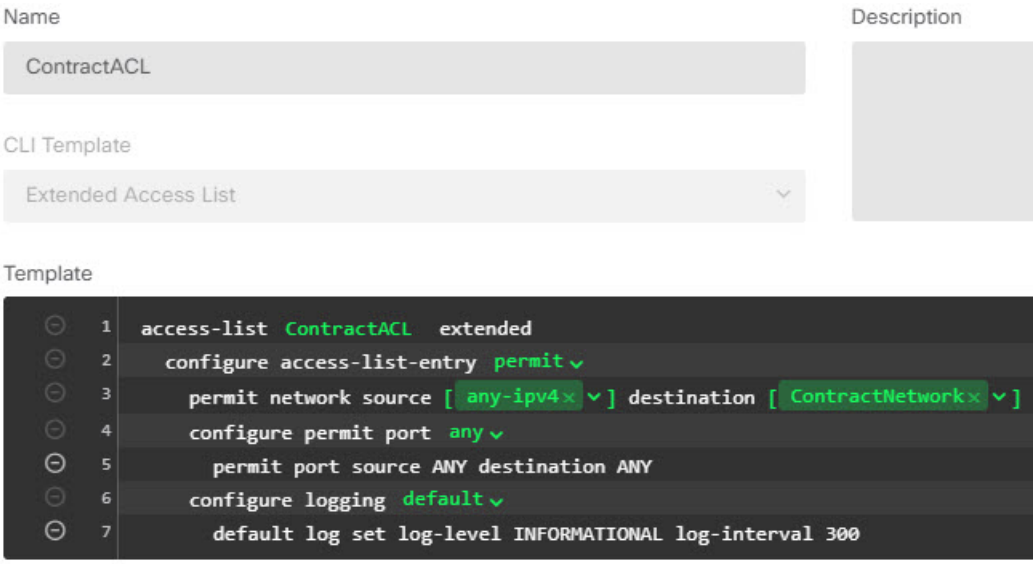


b) 选择**设备** > **高级配置** > **Smart CLI** > **对象**。
c) 点击 **+** 创建新对象。
d) 输入 ACL 的名称。例如，**ContractACL**。
e) 对于 **CLI 模板**，选择**扩展访问列表**。
f) 在**模板**正文中进行以下配置：

- configure access-list-entry action = permit
- source-network = any-ipv4
- destination-network = ContractNetwork object
- configure permit port = any

- configure logging = default

ACE 应如下所示：



g) 点击**确定 (OK)**。

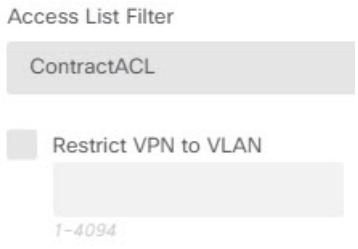
在下次部署更改时会配置此 ACL。无需在任何其他策略中使用此对象来强制部署。

步骤 2 创建使用此 ACL 的组策略。

您至少还需要为组策略配置DNS服务器。您可以根据需要配置其他选项。以下步骤重点介绍与此使用案例相关的一个设置。

a) 依次选择**设备** > **RA VPN** > **组策略**。
b) 点击+，创建新的组策略。
c) 在**常规 (General)**页面中，输入策略名称，例如 **ContractGroup**。
d) 点击目录中的**流量过滤器**。
e) 对于**访问列表过滤器**，选择 ContractACL 对象。

对于本示例，将 VLAN 选项留空。请注意，您也可以设置一个 VLAN 用于过滤，并为 VLAN 配置子接口。



f) 点击**确定**保存组策略。

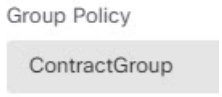
步骤 3 配置适用于承包商的连接配置文件。

a) 在 RA VPN 页面上，点击目录中的**连接配置文件 (Connection Profiles)**。
b) 点击 **+**，创建新的连接配置文件。
c) 完成向导的第 1 步，然后点击**下一步**。

输入配置文件的名称，例如，Contractors。

按照惯常做法配置其余选项。包括为承包商选择适当的身份验证源和定义地址池。

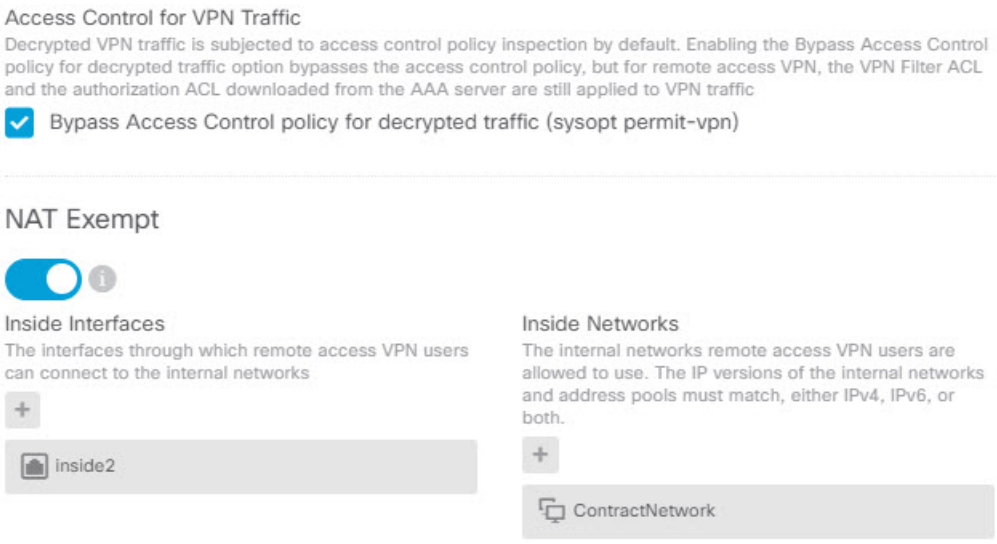
d) 选择为承包商配置的组策略，然后点击**下一步**。



e) 在全局设置中，选择**为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** 选项，并配置 **NAT 豁免**选项。

对于 **NAT 豁免**，您需要配置以下选项。请注意，如果您定义了其他连接配置文件，则需要将其添加到现有设置中，因为此配置适用于所有连接配置文件。

- **内部接口** - 选择 **inside2** 接口。这些是远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
- **内部网络** - 选择 ContractNetwork 网络对象。这些是代表远程用户将访问的内部网络的网络对象。



f) 上传适用于受支持平台的 Secure Client 软件包。
g) 点击**下一步**并验证设置。

首先，验证摘要是否正确。

然后，点击 **说明** 查看最终用户初步安装 Secure Client 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击**复制**以将这些说明复制到剪贴板，然后将它们粘贴在文本文件或邮件中。

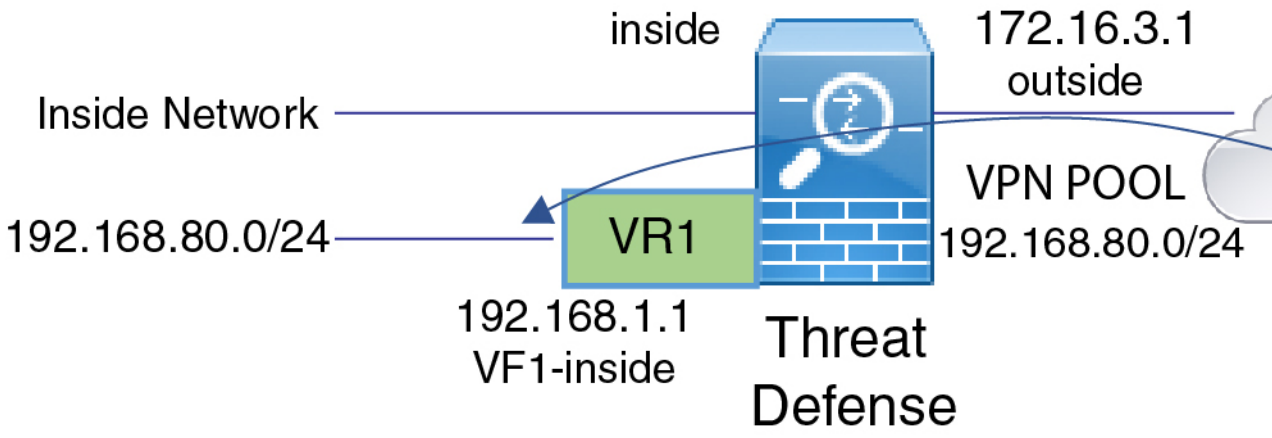
h) 点击**完成**。

如何对不同虚拟路由器中的内部网络进行 RA VPN 访问

如果在设备上配置多个虚拟路由器，则必须在全局虚拟路由器中配置 RA VPN。不能在分配给自定义虚拟路由器的接口上配置 RA VPN。

由于虚拟路由器的路由表是独立的，因此，如果RA VPN用户需要访问属于不同虚拟路由器的网络，则必须创建静态路由。

请考虑以下示例。在这种情况下，RA VPN 用户连接到地址为 172.16.3.1 的外部接口，并在 192.168.80.0/24 池中获得IP地址。此时，该用户可以访问连接到全局虚拟路由器的内部网络。但是，该用户无法访问属于虚拟路由器 VR1 的 192.168.1.0/24 网络。要允许 VR1 网络和 RA VPN 用户之间的流量传输，必须配置双向静态路由。



开始之前

此示例假设您已配置 RA VPN，定义虚拟路由器，配置接口并将其分配给相应的虚拟路由器。

过程

步骤 1 配置从全局虚拟路由器到 VR1 的路由泄漏。

此路由允许在 VPN 池中分配 IP 地址的 Secure Client访问 VR1 虚拟路由器中的 192.168.1.0/24 网络。

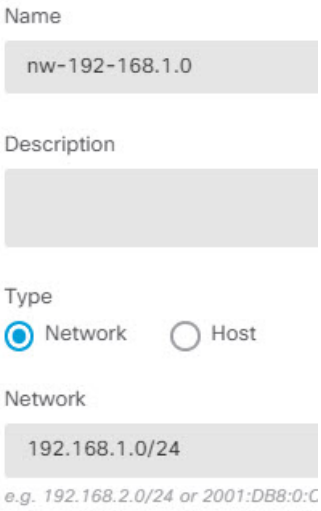
a) 依次选择**设备** > **路由** > **查看配置**。

b) 点击全局虚拟路由器的查看图标 ( )。

c) 在全局路由器的**静态路由**选项卡上，点击 + 并配置路由：

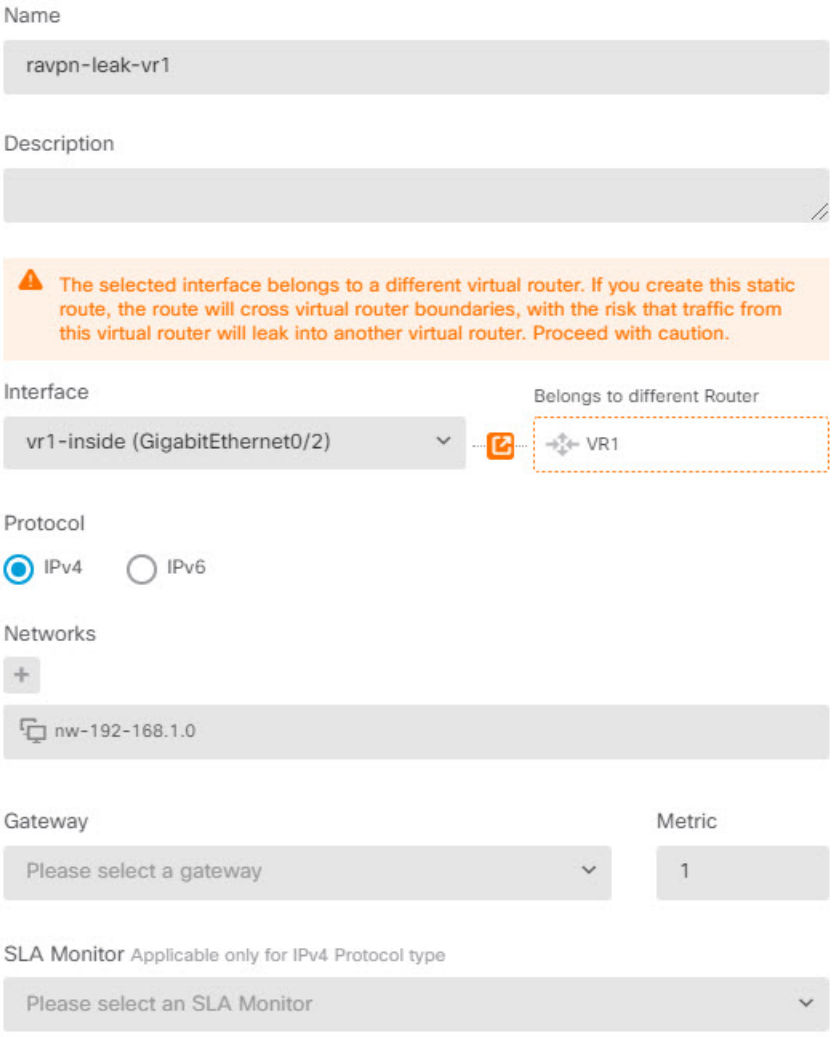
- **名称** - 可以使用任何名称，例如 **ravpn-leak-vr1**。
- **接口** - 选择 **vr1-inside**。

- **协议** - 选择 **IPv4**。
- **网络** - 选择定义 192.168.1.0/24 网络的对象。如有需要，请点击**创建新网络**立即创建对象。



- **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

对话框应如下所示：



d) 点击**确定**。

步骤 2 配置从 VR1 到全局虚拟路由器的路由泄漏。

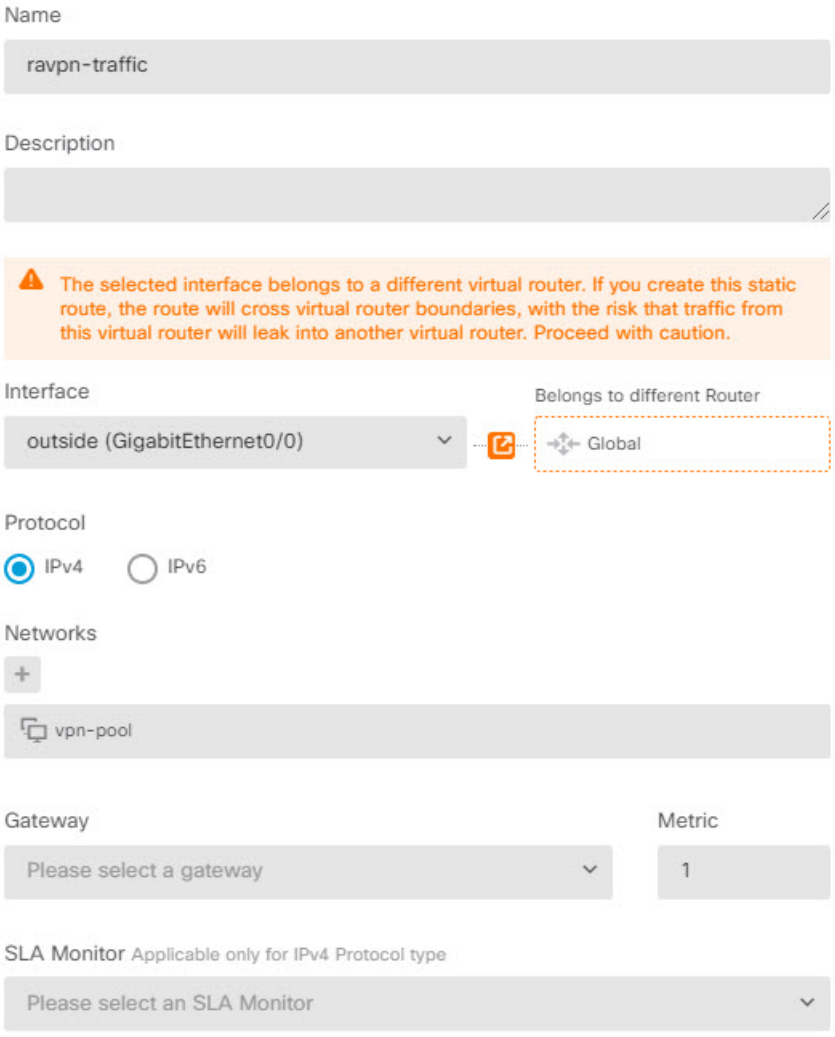
此路由允许 192.168.1.0/24 网络上的终端向在 VPN 池中分配 IP 地址的 Secure Client发起连接。

a) 从虚拟路由器下拉列表中选择 **VR1**，以切换至 VR1 配置。

b) 在 VR1 虚拟路由器的**静态路由**选项卡上，点击 **+** 并配置路由：

- **名称** - 可以使用任何名称，例如 **ravpn-traffic**。
- **接口** - 选择 **outside**。
- **协议** - 选择 **IPv4**。
- **网络** - 选择为 VPN 池创建的对象，例如 **vpn-pool**。
- **网关** - 将此项目留空。将路由泄漏到另一个虚拟路由器时，您不必选择网关地址。

对话框应如下所示：



c) 点击**确定 (OK)**。

下一步做什么

如果 RA VPN 地址池与自定义虚拟路由器中的 IP 地址之间存在重叠，则还必须对 IP 地址使用静态 NAT 规则，以启用正确的路由。但是，更简单的方法是，直接更改 RA VPN 地址池，使其不存在重叠。

如何自定义 Secure Client 图标和徽标

您可以在 Windows 和 Linux 客户端计算机上自定义 Secure Client 应用的图标和徽标。图标的名称是预定义的，并且对您上传的图像的文件类型和大小有特定限制。

虽然您在部署自己的可执行文件以自定义 GUI 时可以使用任何文件名，但本示例假设您只是在不部署完全自定义框架的情况下交换图标和徽标。

您可以替换许多图像，其文件名因平台而异。有关自定义选项、文件名、类型和大小的完整信息，请参阅 *Cisco* 安全客户端管理员指南中有关自定义和本地化 Secure Client 和安装程序的章节。例如，在以下位置可以找到 4.8 客户端的相应章节：

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html

开始之前

在本示例中，我们将替换 Windows 客户端的以下图像。请注意，如果图像的大小与最大值不同，系统会自动将其调整为最大值，并在必要时扩展图像。

- app_logo.png

  此应用徽标图像是应用图标，最大大小为 128 x 128 像素。

- company_logo.png

  此公司徽标图像显示在托盘浮出控件左上角和“高级”对话框中。最大大小为 97 x 58 像素。

- company_logo_alt.png

  “关于”对话框右下角显示备用公司徽标图像。最大大小为 97 x 58 像素。

要上传这些文件，必须将其放置在 威胁防御 设备可以访问的服务器上。您可以使用 TFTP、FTP、HTTP、HTTPS 或 SCP 服务器。根据服务器设置的要求，从这些文件获取图像的 URL 可以包括路径和用户名/密码。此示例将使用 TFTP。

过程

步骤 1 将图像文件上传到充当 RA VPN 头端且应使用自定义图标和徽标的每个 威胁防御 设备。

a) 使用 SSH 客户端登录设备 CLI。

b) 在 CLI 中，输入 **system support diagnostic-cli** 命令以进入诊断 CLI 模式。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv1>
```

注释 阅读消息！您必须按 **Ctrl+a，然后按 d**，才能退出诊断 CLI 并返回正常的 威胁防御 CLI 模式。

c) 请注意命令提示符。普通 CLI 仅使用 >，而诊断 CLI 的用户执行模式使用主机名加 >。在本例中为 ftdv1>。您需要进入特权执行模式，该模式使用 **#** 作为结束字符，例如 ftdv1#。如果提示符已包含 **#**，请跳过此步骤。否则，请输入 enable 命令，并在密码提示时按 Enter 键，而不输入密码。

```
ftdv1> enable
Password:
ftdv1#
```

d) 使用 **copy** 命令将每个文件从托管服务器复制到 威胁防御 设备的 disk0。您可以将它们放在子目录中，例如 disk0:/anyconnect-images/。您可以使用 **mkdir** 命令创建新文件夹。

例如，如果 TFTP 服务器的 IP 地址为 10.7.0.80，并且您想要创建新目录，则命令将类似于以下内容。请注意，第一个示例后省略了对 **copy** 命令的响应。

```
ftdv1# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images

ftdv1# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)

ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo.png
disk0:/anyconnect-images/company_logo.png
ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

步骤 2 在诊断 CLI 中使用 **import webvpn** 命令指示 AnyConnect 在客户端计算机上安装 Secure Client 时下载这些图像。

import webvpn AnyConnect-customization type resource platform win name *filename* **disk0:/***directoryname/filename*

此命令适用于 Windows。对于 Linux，请根据您的客户端的需要，将 **win** 关键字替换为 **linux** 或 **linux-64**。

例如，要导入上一步中上传的文件，假设我们仍在诊断 CLI 中：

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

步骤 3 确认配置：

- 要验证导入的文件，请在诊断 CLI 特权执行模式下使用 **show import webvpn AnyConnect-customization** 命令。
- 要验证图像是否已下载到客户端，这些图像应在用户运行客户端时显示。您还可以在 Windows 客户端上检查以下文件夹，其中 %PROGRAMFILES% 通常解析为 c:\Program Files。

  %PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res

下一步做什么

如果要恢复默认图像，请对自定义的每个图像使用 **revert webvpn** 命令（在诊断 CLI 特权执行模式下）。命令为：

revert webvpn AnyConnect-customization type resource platform win name *filename*

与 **import webvpn** 一样，如果您已自定义这些客户端平台，请将 **win** 替换为 **linux** 或 **linux-64**，并为导入的每个图像文件名单独发出该命令。例如：

```
ftdv1# revert webvpn AnyConnect-customization type resource platform win
name app_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。