站点间 VPN

虚拟专用网络 (VPN) 是一种网络连接，通过诸如互联网或其他网络之类的公共资源在远程对等体之间建立安全隧道。VPN 使用隧道来封装正常 IP 数据包内的数据包，以在基于 IP 的网络上转发。它们使用加密来确保隐私和身份验证，以确保数据的完整性。

VPN 基础知识

借助隧道，可以使用互联网等公共TCP/IP网络在远程用户与企业专用网络之间创建安全连接。每个安全连接都称为一个隧道。

基于 IPSec 的 VPN 技术通过互联网安全关联和密钥管理协议（ISAKMP 或 IKE）以及 IPSec 隧道标准来建立和管理隧道。ISAKMP 和 IPSec 将完成以下操作：

- 协商隧道参数。
- 建立隧道。
- 验证用户和数据。
- 管理安全密钥。
- 加密和解密数据。
- 管理隧道中的数据传输。
- 作为隧道终端或路由器管理入站和出站数据传输。

VPN 中的设备可用作双向隧道终端。它可以从专用网络接收明文数据包，将其封装，创建隧道，然后发送到隧道的另一端，随后解封并发送到最终目标。它也会从公用网络接收封装数据包，将其解封，然后发送给其在专用网络上的最终目标。

建立站点间 VPN 连接之后，本地网关后的主机可通过安全 VPN 隧道连接至远程网关后的主机。一个连接由以下部分组成：这两个网关的 IP 地址和主机名、这两个网关后的子网，以及这两个网关用来进行相互身份验证的方法。

互联网密钥交换 (IKE)

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用提议。

IKE 策略是一组算法，供两个对等体用于保护它们之间的 IKE 协商。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数保护后续 IKE 协商。对于 IKE 版本 1 (IKEv1)，IKE 策略包含单个算法集和模数组。与 IKEv1 不同，在 IKEv2 策略中，您可以选择多个算法和模数组，对等体可以在第 1 阶段协商期间从中进行选择。可创建单个 IKE 策略，尽管您可能需要不同的策略来向最需要的选项赋予更高优先级。对于站点间 VPN，您可以创建单个 IKE 策略。

要定义 IKE 策略，请指定：

- 唯一优先级（1 至 65,543，其中 1 为最高优先级）。
- 一种 IKE 协商加密方法，用于保护数据并确保隐私。
- 散列消息身份验证代码 (HMAC) 方法（在 IKEv2 中称为完整性算法），用于确保发送人身份，以及确保消息在传输过程中未被修改。
- 对于 IKEv2，使用单独的伪随机函数 (PRF) 作为派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法。这些选项与用于散列算法的选项相同。
- Diffie-Hellman 组，用于确定 encryption-key-determination 算法的强度。设备使用此算法派生加密密钥和散列密钥。
- 是否启用额外的后量子密钥交换。通过后量子密码 (PQC) 算法，利用额外密钥交换提升安全性。
- 身份验证方法，用于确保对等体的身份。
- 在更换加密密钥前，设备可使用该加密密钥的时间限制。

当 IKE 协商开始时，发起协商的对等体将其启用的所有策略发送到远程对等体，然后远程对等体按优先级顺序搜索其自己的策略的匹配项。如果 IKE 策略具有相同的加密、散列（完整性和用于 IKEv2 的 PRF）、身份验证和 Diffie-Hellman 值，而且 SA 生命周期小于或等于发送的策略中的生命周期，则它们之间存在匹配。如果生命周期不同，则会应用较短的生命周期（来自远程对等体）。默认情况下，使用 DES 的简单 IKE 策略是唯一启用的策略。您可以启用更高优先级的其他 IKE 策略来协商更强的加密标准，但 DES 策略应确保成功协商。

VPN 加密与性能

配置 VPN 隧道加密时，请提供充分的保护，并通过平衡安全性和性能来维持效率。

由于VPN隧道通常流经公共网络（最可能是互联网），因此您需要对连接进行加密以保护流量。您可以通过 IKE 策略和 IPsec 提议来定义加密及其他安全技术。使用更强的隧道加密可能会降低系统性能。

如果您的设备许可证允许使用强加密，您可以从丰富的加密算法、散列算法和Diffie-Hellman组中进行选择。本文档不提供关于具体选项选择的指导。如果您在大型公司或其他组织执行运营，可能已有需要满足的指定标准。如果没有，请花些时间研究各个选项。

为 VPN 策略决定加密算法

在决定用于 IKE 策略或 IPsec 提议的加密算法时，您的选择仅限于 VPN 中的设备所支持的算法。

- 对于 IKEv2，您可以配置多个加密算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。
- 对于 IKEv1，仅可以选择一个选项。
- 对于 IPsec 提议，该算法用于封装安全协议 (ESP)，该协议提供身份验证、加密和防重放服务。ESP 为 IP 协议类型 50。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀。

如果设备许可证符合强加密要求，可以从可用的加密算法中选择。如果不符合强加密要求，则只能选择 DES。

强加密许可证注意事项

注释 如果符合强加密要求，在从评估许可证升级到智能许可证之前，请检查并更新加密算法以实现更强的加密，从而使 VPN 配置正常工作。选择基于 AES 的算法。如果您使用支持强加密的帐户注册，则不支持 DES。注册后，在删除对 DES 的所有使用之前，您无法部署更改。

可用的加密算法：

- AES-GCM — （仅限 IKEv2）Galois/计数器模式下的高级加密标准是一种分组密码模式，提供机密性和数据源身份验证。它比 AES 提供更高的安全性。

  AES-GCM 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。较长的密钥可提高安全性，但会降低性能。NSA Suite B 是一组加密算法，设备必须支持该算法集以满足联邦密码强度标准，其要求使用 GCM。

- AES - 高级加密标准是一种对称密码算法，提供比 DES 更高的安全性，在计算上比 3DES 更高效。AES 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。较长的密钥可提高安全性，但会降低性能。
- DES - 数据加密标准，使用 56 位密钥进行加密，是一种对称密钥块算法。如果您的许可证帐户不符合导出控制要求，这将是您唯一的选择。
- Null、ESP-Null - 空加密算法提供无加密的身份验证。此方法不安全，请自行决定是否使用。

决定使用哪些散列算法

在 IKE 政策中，散列算法创建消息摘要，用于确保消息的完整性。在 IKEv2 中，您可以选择一个散列算法用于完整性，另一个用于伪随机函数 (PRF)。

在 IPsec 提议中，封装安全协议 (ESP) 使用散列算法进行身份验证。在 IKEv2 IPsec 提议中，这称为完整性散列。在 IKEv1 IPsec 提议中，算法名称包含 ESP- 前缀和 -HMAC 后缀。

系统将按安全性从高到低的顺序排列您的设置，并按此顺序与对等体进行协商。对于 IKEv1，请仅选择一个选项。

选择满足安全和性能需求的散列算法：

- SHA（安全散列算法）— 生成 160 位摘要的标准 SHA (SHA1)。

  这些 SHA-2 选项提供更高的安全性，且可用于 IKEv2 配置。如果需要 NSA Suite B 密码学合规，请选择其中之一。

  - SHA256 - 指定具有 256 位摘要的安全散列算法 SHA 2。
  - SHA384 - 指定具有 384 位摘要的安全散列算法 SHA 2。
  - SHA512 - 指定具有 512 位摘要的安全散列算法 SHA 2。

- 空或无（NULL、ESP-NONE）—（仅限 IPsec 提议）仅将空散列算法用于测试目的。如果您选择其中一个 AES-GCM/GMAC 选项作为加密算法，则应选择空完整性算法。对于这些加密标准，即使您选择非空选项，完整性散列也会被忽略。

决定要使用的 Diffie-Hellman 模数组

您可使用 Diffie-Hellman 密钥推导算法生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数越大安全性越高，但所需处理时间也越长。两个对等体上必须具有一个匹配的模数组。

若使用 AES 加密，应选用 Diffie-Hellman (DH) 组 5 或更高以支持 AES 所需的大密钥长度。IKEv1 策略不支持所有的组。

要实施 NSA Suite B 加密规范，请使用 IKEv2 并选择椭圆曲线 Diffie-Hellman (ECDH) 的一个选项：19、20 或 21。使用 2048 位模数的椭圆曲线选项和组较不易受 Logjam 等攻击。

要使用后量子密码算法实现额外的密钥交换，请包含一个或多个模块格组。

对于 IKEv2，您可以配置多个组。系统将按安全性从高到低的顺序对设置进行排序，然后使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

- 14 - Diffie-Hellman 组 14：2048 位模幂算法 (MODP) 组。被认为可以良好地保护 192 位密钥。
- 15 - Diffie-Hellman 组 15：3072 位 MODP 组。
- 16 - Diffie-hellman 组 16：4096 位 MODP 组。
- 19 - Diffie-Hellman 组 19：美国国家标准与技术研究所 (NIST) 256 位椭圆曲线取素数 (ECP) 组。
- 20 - Diffie-Hellman 组 20： NIST 384 位 ECP 组。
- 21 - Diffie-Hellman 组 21： NIST 521 位 ECP 组。

- 31 - Diffie-Hellman 组 31：椭圆曲线 25519 256 位 EC 组。
- ML35 - 模块网格组 35（NIST 512 位 KYBER 组）。
- ML36 - 模块网格组 36（NIST 768 位 KYBER 组）。
- ML37 - 模块网格组 37（NIST 1024 位 KYBER 组）
- NONE - 组 0（转换 ID NONE）。可在额外密钥交换轮次中配合其他组使用 NONE 作为回退。若系统无法协商任何其他组，可使用先前已协商的组完成连接。

确定使用哪种身份验证方法

可以使用以下方法对站点间 VPN 连接中的对等体进行身份验证。

预共享密钥

预共享密钥是在连接中的每个对等体上配置的加密密钥字符串。这些密钥由 IKE 在身份验证阶段使用。对于 IKEv1，您必须在每个对等体上配置相同的预共享密钥。对于 IKEv2，您可以在每个对等体上配置唯一密钥。

与证书相比，预共享密钥的扩展性相对逊色。如果需要配置大量的站点间VPN连接，请使用证书而非预共享密钥。

证书

数字证书使用 RSA 密钥对为 IKE 密钥管理消息进行签名和加密。在配置站点间 VPN 连接的两端时，请选择本地设备的身份证书，以便远程对等体可以对本地对等体进行身份验证。

要使用证书方法，您需要执行以下操作：

1. 使用证书颁发机构 (CA) 注册本地对等体并获取设备身份证书。将证书上传到设备。有关详细信息，请参阅上传内部证书和内部 CA 证书。

   如果您也负责远程对等体，还需注册此对等体。虽然对这些对等体使用同一CA比较方便，但并非必须要这么做。

   无法使用自签证书来建立 VPN 连接。必须使用证书颁发机构来注册设备。

   如果使用 Windows 证书颁发机构 (CA) 创建用于站点间 VPN 终端的证书，则必须使用为应用策略扩展指定 IP 安全终端系统的证书。可以在证书“属性”对话框中的“扩展”选项卡上（在 Windows CA 服务器上）找到此内容。此扩展的默认值为“IP 安全 IKE 中间”，对于使用 防火墙设备管理器配置的站点间 VPN 不起作用。

2. 上传用于签署本地对等体身份证书的受信任 CA 证书。如果使用了中间 CA，请上传完整的证书链，包括根证书和中间证书。有关详细信息，请参阅上传受信任的 CA 证书。

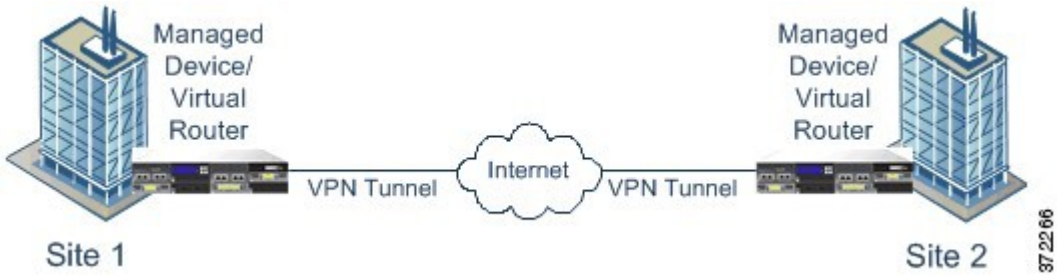
3. 如果使用了不同的 CA 注册远程对等体，还需上传用于签署远程对等体身份证书的受信任 CA 证书。从控制远程对等体的组织获取证书。如果他们使用了中间 CA，请上传完整的证书链，包括根证书和中间证书。

4. 在配置站点间 VPN 连接时，请选择证书方法，然后选择本地对等体的身份证书。连接的每一端会指定连接本地端的证书；您无需指定远程对等体的证书。

VPN 拓扑

只能使用 防火墙设备管理器来配置点对点 VPN 连接。虽然所有连接都是点对点的，但您可以通过定义设备参与的每个隧道，链接到更大的中心辐射型或网状 VPN。

下图显示了典型的点对点 VPN 拓扑。在点对点 VPN 拓扑中，两个终端彼此直接通信。将两个终端配置为对等体设备，任一台设备均可启动安全连接。



与动态寻址对等体建立站点间 VPN 连接

即使不知道对等体的 IP 地址，您也可以创建到此对等体的站点间 VPN 连接。此功能在以下情况下非常有用：

- 对等体使用 DHCP 获取它的地址时，您不能使用具有特定静态 IP 地址的远程终端。
- 设备在中心辐射型拓扑中充当控制中心，允许与其建立连接的远程对等体的数量不确定。

需要与动态寻址对等体 B 建立安全连接时，您需要确保连接端点 A 拥有静态 IP 地址。随后，在 A 上创建连接时，请指明对等体具有动态地址。但是，在对等体 B 上配置连接时，请确保输入 A 的 IP 地址作为远程对等地址。

当系统建立站点间 VPN 连接时，任何包含具有动态地址的对等体的连接都处于仅响应状态。换言之，必须由远程对等体发起连接。在远程对等体尝试建立连接时，设备会使用您在连接中定义的方法（预共享密钥或证书）验证连接。

由于只有在远程对等体发起连接之后才会建立VPN连接，因此在连接建立之前，系统会丢弃与允许流量通过 VPN 隧道的访问控制规则匹配的出站流量。这可确保数据不会在未采取适当加密和 VPN 保护措施的情况下离开您的网络。

虚拟隧道接口和基于路由的 VPN

传统上，您通过定义通过 VPN 隧道加密的特定本地和远程网络来配置站点间 VPN 连接。这些在 VPN 连接配置文件的加密映射中定义。这种类型的站点间 VPN 称为基于策略的 VPN。

或者，您还可以配置基于路由的站点间 VPN。在这种情况下，您可以创建虚拟隧道接口 (VTI)，即与特定物理接口（通常是外部接口）关联的虚拟接口。然后，使用带有静态和动态路由的路由表将所需流量定向到 VTI。通过 VTI（出口）路由的所有流量都通过您为 VTI 配置的 VPN 隧道进行加密。

因此，使用基于路由的站点间 VPN，只需更改路由表即可管理给定 VPN 连接中的受保护网络，而完全无需更改 VPN 连接配置文件。您无需跟踪远程网络并更新 VPN 连接配置文件，以考虑这些更改。这简化了云运营商和大型企业的 VPN 管理。

此外，您可以为 VTI 创建访问控制规则，以调整隧道中允许的流量类型。例如，您可以应用入侵检测以及 URL 和应用过滤。

配置基于路由的 VPN 的过程概述

简言之，设置基于路由的站点间 VPN 的过程包括以下步骤：

过程

步骤 1 为本地终端创建 IKEv1/2 策略和 IPsec 提议。

步骤 2 创建与面向远程对等体的物理接口关联的虚拟隧道接口 (VTI)。

步骤 3 创建使用 VTI、IKE 策略和 IPsec 提议的站点间 VPN 连接配置文件。

步骤 4 在远程对等体、远程 VTI 和指定此本地 VTI 作为远程终端的站点间 VPN 连接配置文件上创建与远程终端相同的 IKE 和 IPsec 提议（从远程对等体的角度来看）。

步骤 5 在两个对等体上创建路由和访问控制规则，以通过隧道发送相应流量。

确保每个终端上的路由和访问控制相互镜像，以允许流量在两个方向上流动。

静态路由具有以下一般特征：

- **接口** - 虚拟隧道接口 (VTI) 名称。
- **网络** - 定义受远程终端保护的远程网络的网络对象。
- **网关** - 定义 VPN 隧道的远程终端 IP 地址的网络对象。

虚拟隧道接口和基于路由的 VPN 准则

IPv6 准则

虚拟隧道接口仅支持 IPv4 地址。无法在 VTI 上配置 IPv6 地址。

其他准则

- 最多可以创建 1024 个 VTI。
- 不能在 VTI 基于路由的 VPN 上配置静态或动态反向路由注入。（只能使用 Firewall Threat Defense API 配置反向路由注入。）
- 选择 VTI 作为本地接口时，无法配置动态对等体地址。
- 选择 VTI 作为本地接口时，无法配置远程备份对等体。

- 不能为分配给自定义虚拟路由器的源接口创建 VTI。使用虚拟路由器时，只能在全局虚拟路由器中的接口上配置 VTI。
- 无论隧道中的数据流量如何，IKE 和 IPsec 安全关联都将不断重新生成密钥。这可确保 VTI 隧道始终处于活动状态。
- 不能在基于路由的连接配置文件上同时配置 IKEv1 和 IKEv2：必须仅配置一个 IKE 版本。
- 只要加密映射中配置的对等体地址与 VTI 的隧道目的地不同，就可以在同一个物理接口上使用不同的 VTI 和基于策略的（加密映射）配置。
- 在 VTI 上仅支持 BGP 路由协议。
- 如果系统终接 IOS IKEv2 VTI 客户端，请禁用 IOS 上的配置交换请求，因为系统无法为由 IOS VTI 客户端发起的会话检索 mode-CFG 属性。
- 基于路由的站点间 VPN 配置为双向，这意味着 VPN 隧道的任一终端都可以发起连接。创建连接配置文件后，您可以将此终端更改为唯一发起方 (INITIATE_ONLY) 或唯一响应方 (RESPOND_ONLY)。确保将远程终端修改为使用补充连接类型。要进行此更改，您必须转到 API Explorer 并使用 GET /devices/default/s2sconnectionprofiles 查找连接配置文件。然后，您可以将正文内容复制/粘贴到 PUT /devices/default/s2sconnectionprofiles/{objId} 方法中，更新 **connectionType** 以指定所需类型，并运行该方法。

IPsec 流分流

IPsec 流卸载是一项性能优化功能：

- 初始建立后，将 IPsec 连接卸载至现场可编程门阵列 (FPGA) 或专用硬件组件
- 通过在硬件中处理预解密、解密、预加密和加密来提升设备性能，并且
- 在支持的设备型号上默认启用，系统软件仍处理内层流安全策略。

IPsec 流卸载特性

初始设置 IPsec 站点间 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)。此过程可提高设备性能。在 Cisco Secure Firewall 1200 系列上，IPsec 连接被分流到Marvell 加密加速器 (CPT)，以提高设备性能。

卸载操作包括入向和出向的预解密及解密处理。系统软件对内层流应用安全策略。

IPsec 流卸载适用于以下设备类型：

- Cisco Secure Firewall 1200
- Cisco Secure Firewall 3100

默认情况下，系统在支持的設備型号上启用 IPsec 流卸载。要更改配置，请使用 FlexConfig 实施 **flow-offload-ipsec** 命令。有关详细信息，请参阅 ASA 命令参考。

管理站点间 VPN

虚拟专用网络 (VPN) 是一种网络连接，通过诸如互联网或其他网络之类的公共资源在远程对等体之间建立安全隧道。VPN 使用隧道来封装正常 IP 数据包内的数据包，以在基于 IP 的网络上转发。它们使用加密来确保隐私和身份验证，以确保数据的完整性。

您可以与对等体设备创建VPN连接。所有连接都是点对点连接，但您可以通过配置所有相关连接，将设备连接到更大的中心辐射型或网格 VPN 中。

开始之前

以下事实控制可重新创建的站点间 VPN 连接的类型和数量：

- VPN 连接使用加密技术保护网络隐私。您可以使用的加密算法取决于您的基本许可证是否允许强加密。而控制这一点的，则是您在向思科智能许可证管理器注册时是否选择了允许在设备上使用出口控制功能的选项。如果您使用的是评估许可证，或者您没有启用出口控制功能，则无法使用强加密。
- 您最多可以创建 20 个唯一性 IPsec 配置文件。唯一性取决于 IKEv1/v2 提议和证书、连接类型、DH 组和 SA 生命周期的组合。您可以重复使用现有配置文件。因此，如果对所有站点间 VPN 连接使用相同的设置，则只有一个唯一性 IPsec 配置文件。一旦达到 20 个唯一性 IPsec 配置文件的限制，就无法创建新的站点间VPN连接，除非使用与现有连接配置文件相同的属性组合。

过程

步骤 1 点击**设备**，然后点击站点间 VPN 组中的**查看配置 (View Configuration)**。

此操作将打开“站点间 VPN”(Site-to-Site VPN) 页面，其中列出了您已配置的所有连接。

步骤 2 执行以下任一操作。

- 要创建新的站点间 VPN 连接，请点击 + 按钮。请参阅配置站点间 VPN 连接，第 10 页。

  如果尚无连接，也可以点击**创建站点间连接**按钮。

- 要编辑现有连接，请点击该连接的编辑图标 ( )。请参阅配置站点间 VPN 连接，第 10 页。
- 要将连接配置的摘要复制到剪贴板，请点击该连接的复制图标 ( )。您可以将此信息粘贴到文档中发送给远程设备的管理员，帮助完成连接另一端的配置。
- 要删除不再需要的连接，请点击该连接的删除图标 ( )。

配置站点间 VPN 连接

假定获得了远程设备所有者的合作与权限，您可以创建点对点VPN连接，将您的设备链接到另一台设备。虽然所有连接都是点对点的，但您可以通过定义设备参与的每个隧道，链接到更大的中心辐射型或网状 VPN。

开始之前

您可以为每个本地网络/远程网络组合创建单个 VPN 连接。但是，如果远程网络在每个连接配置文件中是唯一的，则可以为本地网络创建多个连接。

如果远程网络重叠，请务必先创建限制更严格的连接配置文件。系统将按照您创建连接配置文件的顺序创建隧道，而不是按其显示顺序（即字母顺序）创建隧道。

例如，如果您希望从192.16.0.0/16到10.91.0.0/16的一个隧道通向远程终端A，但希望隧道192.16.0.0/24通过远程终端 B 通向 10.0.0.0/8 的其余部分，则必须为 A 创建连接配置文件，然后再为 B 创建连接配置文件。

注释 若创建多条策略型站点间 VPN 连接，各配置文件中须指定相同接口为本地 VPN 访问接口。FDM 不支持为多个接口创建策略型站点间 VPN。

过程

步骤 1 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。

步骤 2 执行以下任一操作：

- 要创建新的站点间 VPN 连接，请点击 + 按钮。

  如果尚无连接，也可以点击**创建站点间连接**按钮。

- 要编辑现有连接，请点击该连接的编辑图标 ( )。

要删除不再需要的连接，请点击该连接的删除图标 ( )。

步骤 3 定义点对点 VPN 连接的终端。

- **连接配置文件名称** - 此连接的名称，最多 64 个字符，不含空格。例如，MainOffice。不能将 IP 地址用作名称。
- **类型** - 如何识别应通过 VPN 隧道发送的流量。选择以下一个选项：
  - **基于路由 (VTI)** - 您将使用路由表（主要是静态路由）定义应参与隧道的本地和远程网络。如果选择此选项，则必须选择虚拟隧道接口 (VTI) 作为本地 VPN 接入接口。您还必须为隧道的远程端使用静态 IP 地址。确保在创建 VPN 连接配置文件后为 VTI 配置适当的静态路由和访问控制规则。

- **基于策略** - 您将直接在站点间 VPN 连接配置文件中指定本地和远程网络。这是定义哪些流量应受 VPN 隧道保护的经典方法。

- **本地站点** - 这些选项定义本地终端。
  - **本地 VPN 访问接口** - 选择远程对等体可连接的接口。这通常是外部接口。该接口不能是网桥组的成员。
  - **本地网络** -（仅基于策略。）点击 **+** 并选择标识应参与 VPN 连接的本地网络的网络对象。这些网络上的用户将能够通过该连接访问远程网络。

  注释
  您可以为这些网络使用 IPv4 或 IPv6 地址，但必须在连接的每一侧都具有匹配的地址类型。例如，本地 IPv4 网络的 VPN 连接必须至少有一个远程 IPv4 网络。您可以在单个连接的两端结合 IPv4 和 IPv6。终端受保护的网络不能重叠。

- **远程站点** - 这些选项定义远程终端。
  - **静态/动态** - 远程对等体的 IP 地址是以静态还是动态的方式定义的（例如，通过 DHCP 定义）。如果选择**静态**，请输入远程对等体的 IP 地址。如果选择**动态**，仅远程对等体可以发起此 VPN 连接。

    对于基于路由的 VPN，您可以仅选择**静态**。
  - **远程 IP 地址**（仅限于静态寻址。）- 输入将用于托管 VPN 连接的远程 VPN 对等体接口的 IP 地址。
  - **远程备用对等体** -（可选，仅基于策略的连接。）点击**添加对等体**为远程终端添加备用对等体。如果主终端不可用，系统会尝试与其中一个备用对等体重新建立VPN连接。您可以添加多个备用对等体。

    配置每个备用对等体时，您可以配置要用于该对等体的预共享密钥和证书。使用您为主远程对等体配置的相同技术。将这些设置留空可使用为连接配置文件配置的相同值。

    配置第一个备用对等体后，您可以通过点击**添加另一个对等体**来添加另一个对等体，或删除对等体，或点击**编辑**更改对等体的设置。

    如果备用对等体可通过主对等体之外的其他接口访问，请确保在**本地 VPN 访问接口**下选择所需接口。
  - **远程网络** -（仅基于策略。）点击 **+** 并选择标识应参与 VPN 连接的远程网络的网络对象。这些网络上的用户将能够通过连接访问本地网络。

步骤 4 点击**下一步 (Next)**。

步骤 5 定义 VPN 的隐私配置。

注释
您的许可证决定您可以选择哪些加密协议。您必须符合强加密的条件，即满足导出管制条件，才能选择除最基本选项以外的任何其他选项。

- **IKE 版本 2**，**IKE 版本 1** - 选择在互联网密钥交换 (IKE) 协商期间使用的 IKE 版本。对于基于策略的连接，可以选择其中一项或两项；对于基于路由的连接，只能选择其中一项。当设备尝试与另一个对等体协商连接时，它使用您允许且该对等体接受的任何版本。如果这两个版本都允许，而对于最初选择的版本的协商不成功，则设备将自动回退到另一个版本。如果配置了 IKEv2，则系统将始终首先尝试它。两个对等体必须都支持 IKEv2 才能在协商中使用它。

- **IKE 策略** - 互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。这是一个全局策略：您启用的对象应用于所有 VPN。点击**编辑**以检查每个 IKE 版本当前全局启用的策略，并启用和创建新的策略。有关详细信息，请参阅配置全局 IKE 策略，第 14 页。

- **IPsec 提议** - IPsec 提议定义确保 IPsec 隧道中流量安全的安全协议和算法的组合。点击**编辑**并为每个 IKE 版本选择提议。选择要允许的所有提议。点击**设置默认值**以简单选择系统默认值，这根据您的出口合规性而有所不同。系统与对等体协商，从最强到最弱的提议，直到约定一个匹配项。有关详细信息，请参阅配置 IPsec 提议，第 19 页。

- **身份验证类型** - 您想要如何对 VPN 连接中的对等体进行身份验证，**预共享手动密钥**或**证书**中的任一种方法。您还需要根据您的选择填写以下字段。对于 IKEv1，您的选择必须与连接配置的 IKEv1 策略对象中选择的身份验证方式匹配。有关这些选项的详细信息，请参阅确定使用哪种身份验证方法，第 5 页。

  - （IKEv2）**本地预共享密钥**，**远程对等预共享密钥** - 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。

  - （IKEv1）**预共享密钥** - 本地和远程设备上均定义的密钥。该密钥可以有 1 至 127 个字母数字字符。

  - **证书** - 本地对等体的设备身份证书。必须是通过证书颁发机构 (CA) 获取的证书；不能使用自签证书。如果尚未上传证书，请点击**创建新对象**链接。您还需要上传用于签署身份证书的根证书和所有中间受信任的 CA 证书。确保将上传的证书的**验证使用**设置为包括 **IPsec 客户端**。如果尚未上传这些证书，可以在完成向导后执行此操作。

- **IPsec 设置** - 安全关联的生存期。达到生存期后，系统会重新协商安全关联。当系统收到对等体发来的协商请求时，它会使用对等体提出的生存期值或本地配置的生存期值（取较小者）作为新安全关联的生存期。有两个生存期：“定时”生存期和“流量”生存期。只要到达这两个生存期之一（无论先到达哪一个），安全关联就会到期。

  - **生存期持续时间** - 安全关联在到期前可以存续的秒数。范围为 120 到 214783647 秒。全局默认值为 28,800 秒（8 小时）。

  - **生存期大小** - 使用特定安全关联的对等体之间在该安全关联到期前可通过的流量（以千字节为单位）。范围为 10 到 2147483647 千字节或留空。全局默认值为 4,608,000 千字节。将该字段留空可删除基于大小的限制，并使用持续时间作为唯一限制。

- **NAT 豁免** -（仅基于策略。）是否从本地 VPN 访问接口的 NAT 策略中豁免 VPN 流量。如果不想将 NAT 规则应用于本地网络，请选择托管本地网络的接口。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，第 24 页。

- **完美前向保密的 Diffie-Hellman 组** - 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。要启用完美前向保密，请选择在模数组列表中生成 PFS 会话密钥时使用的 Diffie-Hellman 密钥导出算法。如果同时启用 IKEv1 和 IKEv2，则选项仅限于 IKEv1 支持的那些。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组，第 4 页。

步骤 6 点击**下一步 (Next)**。

步骤 7 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。

您必须执行一些附加步骤，才能允许 VPN 隧道中的流量，如允许流量通过站点间 VPN，第 14 页中所述。

部署配置后，登录到设备 CLI 并使用 **show ipsec sa** 命令确认终端是否建立了安全关联。请参阅验证站点间 VPN 连接，第 21 页。

配置虚拟隧道接口

您只能在基于路由的站点间 VPN 连接配置文件中使用虚拟隧道接口 (VTI)。VTI 与物理接口相关联，通过该物理接口与远程对等体建立 VPN 连接。使用虚拟接口，您可以简化站点间 VPN 连接并使用静态和动态路由控制流量，而无需在连接配置文件中为 VPN 指定本地和远程网络。

过程

步骤 1 点击**设备**，然后点击“接口”摘要中的链接，再点击**虚拟隧道接口**。

步骤 2 执行以下任一操作：

- 点击 + 或**创建虚拟隧道接口**以创建新接口。
- 点击现有接口的编辑图标 ()。

如果不再需要某个子接口，请点击其删除图标 ()。您必须先删除使用该接口的任何站点间连接配置文件，然后才能将其删除。

步骤 3 配置以下选项：

- **名称** - 接口的名称，最多 48 个字符。如果更改现有接口的名称，系统会在包含该接口的所有策略和对象中自动更改该接口。不得在名称中使用大写字母。
- **状态** - 将滑块点击为启用状态  。
- **说明** -（可选。）一行说明最多可包含 200 个字符（不包括回车符）。

- **隧道 ID** - 介于 0-10413 之间的编号。此编号附加到 Tunnel 一词后面，构成接口的硬件名称。您必须选择尚未用于其他 VTI 的编号。例如，输入 1 可创建接口 Tunnel1。
- **隧道源** - 选择与此 VTI 关联的接口。隧道源是虚拟隧道接口上定义的站点间 VPN 用于连接到远程终端的接口。选择可以访问远程终端的接口，例如外部接口。源接口可以是物理接口、子接口或 EtherChannel，并且必须具有名称。该接口不能是网桥虚拟接口 (BVI) 的成员。
- **IP 地址和子网掩码** - IPv4 地址和关联的子网掩码。例如，192.168.1.1/24 或 /255.255.255.0。此地址无需与隧道源接口的地址位于同一子网上。但是，如果在源接口上配置远程访问 (RA) VPN，则 VTI IP 地址不能处于为 RA VPN 配置的地址池中。

步骤 4 点击**确定**。

允许流量通过站点间 VPN

可以使用以下方法之一来启用站点间 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。

  由于外部用户无法在远程受保护网络中伪造 IP 地址，因此这是一种允许流量通过 VPN 的较为安全的方法。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。

  配置此命令的首选方法是创建远程访问 VPN 配置文件，其中您选择**为已解密的流量绕过访问控制策略**选项。如果您不想要配置 RA VPN，或您无法配置 RA VPN，则可以使用 FlexConfig 配置命令。

注释 此方法不适用于在虚拟隧道接口 (VTI) 上配置的基于路由的 VPN 连接。您必须始终为基于路由的 VPN 配置访问控制规则。

- 创建访问控制规则以允许来自远程网络的连接。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。

配置全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时

均使用提议。IKE 提议是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象”(Objects) 页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的**编辑**，来启用、禁用和创建策略。

注释 您最多可以启用 20 个 IKE 策略。

过程

步骤 1 从目录中选择**对象**，然后选择 **IKE 策略**。

IKEv1 和 IKEv2 的策略显示在不同列表中。

步骤 2 为每个 IKE 版本启用您希望允许的 IKE 策略。

a) 在对象表上方选择 **IKEv1** 或 **IKEv2**，以显示该版本的策略。

b) 点击**状态**开关以启用适当的对象并禁用不符合要求的对象。

如果您的一些安全要求没有反映在现有对象中，请定义新的对象以实施您的要求。有关详情，请参阅以下主题：

- 配置 IKEv1 策略，第 16 页
- 配置 IKEv2 策略，第 17 页

c) 验证相对优先级是否符合您的要求。

如果您需要更改策略的优先级，请进行编辑。如果策略为预定义的系统策略，则需要创建您自己的策略版本来更改优先级。

优先级是相对的，而非绝对的。例如，优先级 80 高于 160。如果 80 是您启用的最高优先级对象，则它将成为您的首选策略。但如果您随后启用了优先级为 25 的策略，那它将成为您的首选策略。

d) 如果同时使用两个 IKE 版本，使用另一个版本时，请重复相同的过程。

配置 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv1 策略有多个。如果哪个符合您的需求，只需点击**状态**开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在 VPN 连接中编辑 IKEv1 设置时，点击对象列表中所示的**创建新 IKE 策略**链接来创建 IKEv1 策略对象。

过程

步骤 1 从目录中选择**对象**，然后选择 **IKE 策略**。

步骤 2 选择对象表上方的 **IKEv1**，以显示 IKEv1 策略。

步骤 3 如果任何系统定义的策略符合您的要求，请点击**状态**旋钮以启用它们。

也可使用**状态**开关禁用不需要的策略。相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。

步骤 4 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 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 5 配置 IKEv1 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **名称** - 对象的名称，最多 128 个字符。
- **状态** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **身份验证 (Authentication)** - 在两个对等体之间使用的身份验证方法。有关详细信息，请参阅确定使用哪种身份验证方法，第 5 页。
  - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。
  - **证书 (Certificate)** - 使用对等体的设备身份证书来识别彼此。必须通过在证书颁发机构中注册每个对等体来获取这些证书。还须上传用于签署每个对等体的身份证书的受信任 CA 根

证书和中间 CA 证书。对等体可以注册到相同或不同的 CA 中。对于任一对等体，都不能使用自签证书。

- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请参阅为 VPN 策略决定加密算法，第 3 页。
- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数越大，安全性越高，但需要的处理时间更长。两个对等体必须具有匹配的模数组。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组，第 4 页。
- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请参阅决定使用哪些散列算法，第 4 页。
- **使用时间** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 6 点击**确定**，保存更改。

配置 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击**状态**开关便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。另外，您还可以在编辑 VPN 连接中的 IKEv2 设置时，点击对象列表中所示的**创建新 IKE 策略 (Create New IKE Policy)** 链接来创建 IKEv2 策略。

过程

步骤 1 从目录中选择**对象**，然后选择 **IKE 策略**。

步骤 2 选择对象表上方的 **IKEv2** 以显示 IKEv2 策略。

步骤 3 如果任何系统定义的策略符合您的要求，请点击**状态**旋钮以启用它们。

也可使用**状态**开关禁用不需要的策略。相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。

步骤 4 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 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 5 配置 IKEv2 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **名称** - 对象的名称，最多 128 个字符。
- **状态** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密 (Encryption)** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要求选择完整性散列，而混合模式禁止选择单独的完整性散列。) 系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅为 VPN 策略决定加密算法，第 3 页。
- **Diffie-Hellman 组 (Diffie-Hellman Group)** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数越大，安全性越高，但需要的处理时间更长。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的说明，请参阅决定要使用的 Diffie-Hellman 模数组，第 4 页。
- **后量子密钥交换** — 最多可配置 7 次额外的密钥交换，以协商更多密钥。通过结合使用 Diffie-Hellman、椭圆曲线 Diffie-Hellman 和后量子模格算法进行多次密钥交换，您可以设定最低安全级别，同时支持更高级别的安全配置。初始密钥交换是 DH/ECDH 密码；后续交换可以包括 PQC 算法。可以包含空白行。请注意，每次交换都必须成功才能最终建立连接，因此您可以在交换中使用 NONE 作为回退选项，以防同组内的其他选项无法协商。（NONE 与空白不同；您不能在交换中单独使用 NONE。）
- **完整性散列 (Integrity Hash)** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请参阅决定使用哪些散列算法，第 4 页。
- **伪随机函数 (PRF) 散列** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法，第 4 页。
- **使用时间** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 6 点击**确定**，保存更改。

配置 IPsec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本（IKEv1 或 IKEv2），存在不同的 IPsec 提议对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。

注释 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议。

为 IKEv1 配置 IPsec 提议

使用 IKEv1 IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

有几个预定义的IKEv1 IPsec提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IPsec 提议**链接来创建 IKEv1 IPsec 提议对象。

过程

步骤 1 选择**对象**，然后从目录中选择 **IPsec 提议**。

步骤 2 选择对象表上方的 **IKEv1** 显示 IKEv1 IPsec 提议。

步骤 3 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 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 配置 IKEv1 IPsec 提议属性。

- **名称** - 对象的名称，最多 128 个字符。
- **模式** - IPSec 隧道的运行模式。
  - **隧道**模式封装整个 IP 数据包。IPSec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPSec。
  - **传输**模式只封装 IP 数据包的上层协议。IPSec 报头被插入到 IP 报头和上层协议报头（例如 TCP）之间。传输模式要求源和目的主机都支持 IPSec，并且只有在隧道的目的对等体是 IP 数据包的最终目的时才可使用。通常只有在保护第 2 层或第 3 层隧道协议（例如 GRE、L2TP 和 DLSW）时，才会使用传输模式。
- **ESP 加密** - 此提议的封装安全协议 (ESP) 加密算法。有关选项的说明，请参阅为 VPN 策略决定加密算法，第 3 页。
- **ESP 散列** - 要用于身份验证的散列或完整性算法。有关选项的说明，请参阅决定使用哪些散列算法，第 4 页。

步骤 5 点击**确定**，保存更改。

为 IKEv2 配置 IPsec 提议

使用 IKEv2 IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

有几个预定义的 IKEv2 IPsec 提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”(Objects) 页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时，点击对象列表中所示的**创建新 IPsec 提议**链接来创建 IKEv2 IPsec 提议对象。

过程

步骤 1 选择**对象**，然后从目录中选择 **IPsec 提议**。

步骤 2 选择对象表上方的 **IKEv2** 显示 IKEv2 IPsec 提议。

步骤 3 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 ( )。

要删除某个未引用的对象，请点击该对象的垃圾桶图标 ( )。

步骤 4 配置 IKEv2 IPsec 提议属性。

- **名称** - 对象的名称，最多 128 个字符。
- **加密** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅为 VPN 策略决定加密算法，第 3 页。
- **完整性散列 (Integrity Hash)** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请参阅决定使用哪些散列算法，第 4 页。

  注释
  如果选择其中一个 AES-GCM/GMAC 选项作为加密算法，则应该选择空完整性算法。即使您选择非空选项，这些加密标准也不会使用完整性散列算法。

步骤 5 点击**确定**，保存更改。

验证站点间 VPN 连接

在配置站点间 VPN 连接并将该配置部署到设备后，请确认系统是否与远程设备建立了安全关联。

如果无法建立连接，请在设备 CLI 中使用 **ping interface** *interface_name remote_ip_address* 命令，以确保路径通过 VPN 接口连接到远程设备。如果没有连接通过配置的接口，可停用 **interface** *interface_name* 关键字并确定连接是否通过其他接口。您可能选错了用于连接的接口：必须选择面对远程设备的接口，而不是面对受保护网络的接口。

如果存在网络路径，请检查两个终端配置和支持的 IKE 版本和密钥，并根据需要调整 VPN 连接。确保没有访问控制规则或 NAT 规则会阻止连接。

过程

步骤 1 登录到设备 CLI，如登录命令行界面 (CLI)中所述。

步骤 2 使用 **show ipsec sa** 命令可确认是否建立了 IPsec 安全关联。

您应可看到设备（**本地地址**）与远程对等体 (**current_peer**) 之间建立了 VPN 连接。随着您通过该连接发送流量，数据包 (pkts) 计数应会而增加。访问列表应显示该连接的本地和远程网络。

例如，以下输出显示 IKEv2 连接。

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
      #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CD22739C
      current inbound spi : 52D2F1E4

    inbound esp sas:
      spi: 0x52D2F1E4 (1389556196)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4285434/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xCD22739C (3441587100)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4055034/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

以下输出显示 IKEv1 连接。

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6
```

```
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
    path mtu 1500, ipsec overhead 74(44), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: 077D72C9
    current inbound spi : AC146DEC

  inbound esp sas:
    spi: 0xAC146DEC (2887020012)
       SA State: active
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
       slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
       sa timing: remaining key lifetime (kB/sec): (3914999/28567)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x000007FF
  outbound esp sas:
    spi: 0x077D72C9 (125661897)
       SA State: active
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
       slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
       sa timing: remaining key lifetime (kB/sec): (3914999/28567)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
```

步骤 3 使用 **show isakmp sa** 命令可验证 IKE 安全关联。

您可以使用不带 **sa** 关键字的命令（或改用 **stats** 关键字）查看 IKE 统计信息。

例如，以下输出显示 IKEv2 安全关联。

```
> show isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local             Remote            Status   Role
592216161 192.168.2.15/500  192.168.4.6/500   READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
```

```
          ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

以下输出显示 IKEv1 安全关联。

```
> show isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.4.6
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
```

监控站点间 VPN

要对站点间 VPN 连接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 ipsec sa** 显示 VPN 会话（安全关联）。您可以使用 **clear ipsec sa counters** 命令重置这些统计信息。
- **show ipsec** *keyword* 显示的是 IPsec 运行数据和统计信息。输入 **show ipsec ?** 查看可用关键字。
- **show isakmp** 显示 ISAKMP 运行数据和统计信息。

站点间 VPN 示例

以下是配置站点间 VPN 的示例。

使站点间 VPN 流量豁免 NAT

当您在某个接口上定义了站点间 VPN 连接并且还对该接口实施了 NAT 规则时，可以选择使该 VPN 上的流量豁免 NAT 规则。如果 VPN 连接的远端可以处理您的内部地址，则可能要执行此操作。

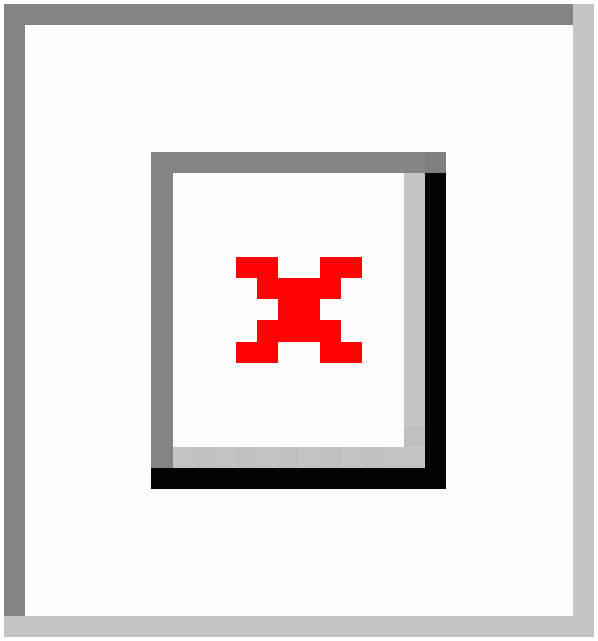
创建 VPN 连接时，可以选择 **NAT 豁免**选项自动创建 NAT 豁免规则。不过，此操作仅在通过单个路由接口（而非网桥组成员）连接本地受保护网络时才奏效。相反，如果该连接中的本地网络位于两个或多个路由接口之后或者一个或多个网桥组成员之后，则需要手动配置 NAT 豁免规则。

要使 VPN 流量豁免 NAT 规则，需要为目的是远程网络时的本地流量创建身份手动 NAT 规则。然后，将 NAT 应用于目的是其他网络（例如互联网）时的流量。如果本地网络有多个接口，请为每个接口分别创建规则。也可以考虑以下建议：

- 如果连接中有多个本地网络，请创建一个网络对象组用于容纳定义这些网络的对象。
- 如果 VPN 中同时包括 IPv4 和 IPv6 网络，请为其各创建一个单独的身份 NAT 规则。

下例显示连接博尔德办公室和圣荷西办公室的站点间隧道。对于要发送到互联网的流量（例如，从博尔德办公室中的 10.1.1.6 到 www.example.com），需要利用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口 PAT 规则。然而，对于要穿过 VPN 隧道的流量（例如，从博尔德办公室中的 10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份 NAT 规则来豁免此流量。身份 NAT 只能将地址转换为其相同的地址。

图 *1:* 用于站点间 *VPN* 的接口 *PAT* 和身份 *NAT*



以下示例说明 Firewall1（博尔德办公室）的配置。该示例假定内部接口是网桥组，因此需要为每个成员接口编写规则。如果有一个或多个路由内部接口，其过程相同。

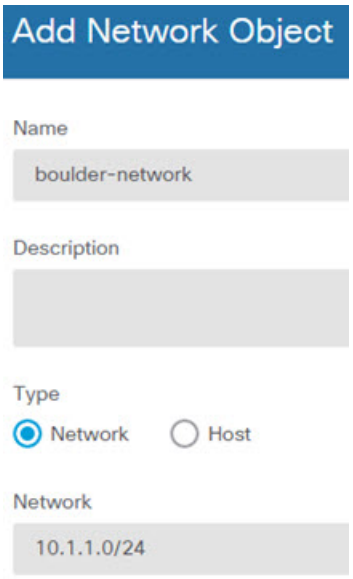
注释 此示例假定只包括 IPv4 网络。如果该 VPN 还包括 IPv6 网络，请为 IPv6 创建并行规则。请注意，由于无法实施 IPv6 接口 PAT，因此需要使用唯一 IPv6 地址创建主机对象用于 PAT。

过程

步骤 1 创建对象来定义各种网络。

a) 选择**对象**。
b) 从目录中选择**网络**，然后点击 +。
c) 找到博尔德办公室内部网络。

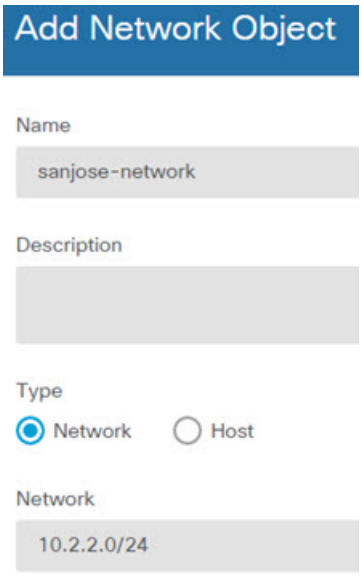
为网络对象命名（例如，boulder-network），选择**网络**，然后输入网络地址 10.1.1.0/24。



d) 点击**确定**。

e) 点击 + 并定义内部圣荷西办公室网络。

为网络对象命名（例如，sanjose-network），选择**网络**，然后输入网络地址 10.2.2.0/24。



f) 点击**确定**。

步骤 2 在Firewall1（博尔德办公室）上，为博尔德办公室网络配置经过VPN连接到圣荷西办公室时的手动身份 NAT。

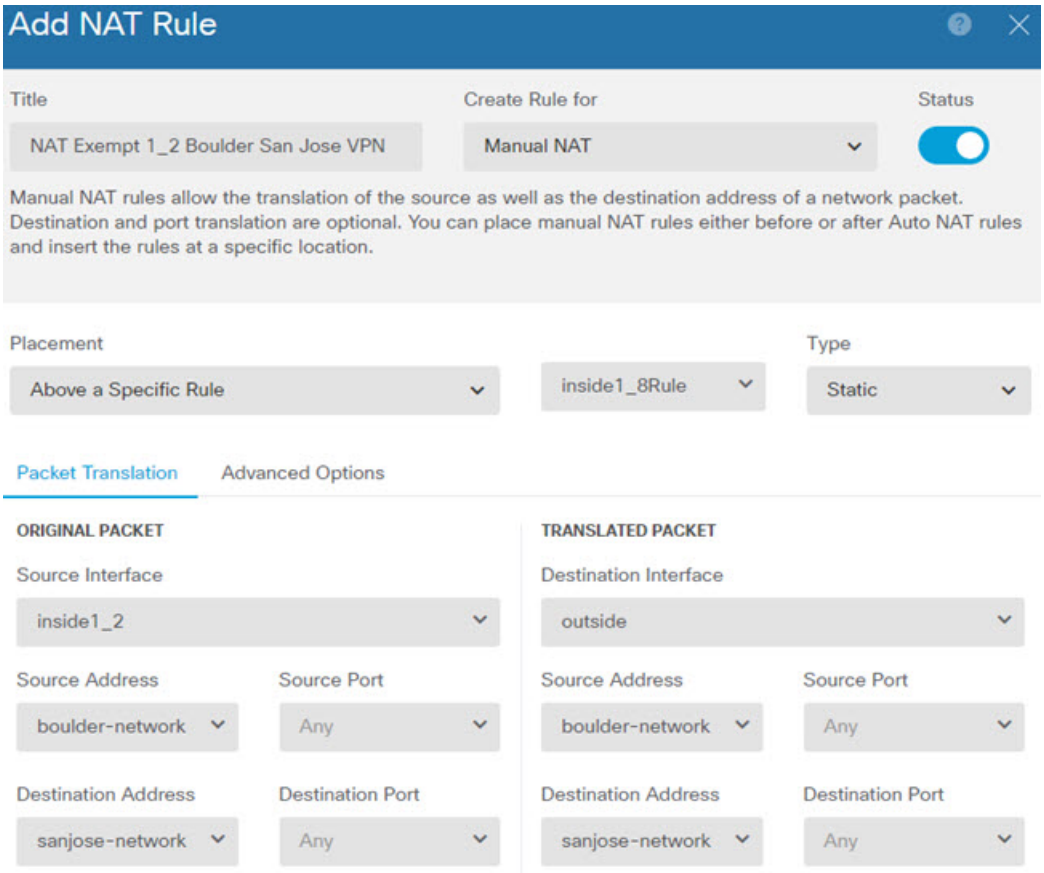
a) 依次选择**策略** > **NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- **标题** = NAT Exempt 1_2 Boulder San Jose VPN（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **位置** = **特定规则之上**，然后在“手动 NAT 在自动 NAT 之前”部分选择第一条规则。需要确保此规则在目标接口的任何常规接口 PAT 规则之前。否则，该规则可能不会应用于正确的流量。
- **类型** = 静态。
- **源接口** = inside1_2。
- **目标接口** = 外部。
- **原始源地址** = boulder-network 网络对象。
- **转换后的源地址** = boulder-network 网络对象。
- **原始目标地址** = sanjose-network 网络对象。
- **转换后的目标地址** = sanjose-network 网络对象。

  注释
  由于您不需要转换目标地址，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。此规则为源和目标配置身份 NAT。



d) 在**高级**选项卡中，选择**不在目标接口上使用代理 ARP**。

e) 点击**确定**。

f) 重复此过程，为每个其他内部接口创建相应规则。

步骤 3 在 Firewall1（博尔德办公室）上，为内部博尔德办公室网络配置接入互联网时的手动动态接口 PAT。

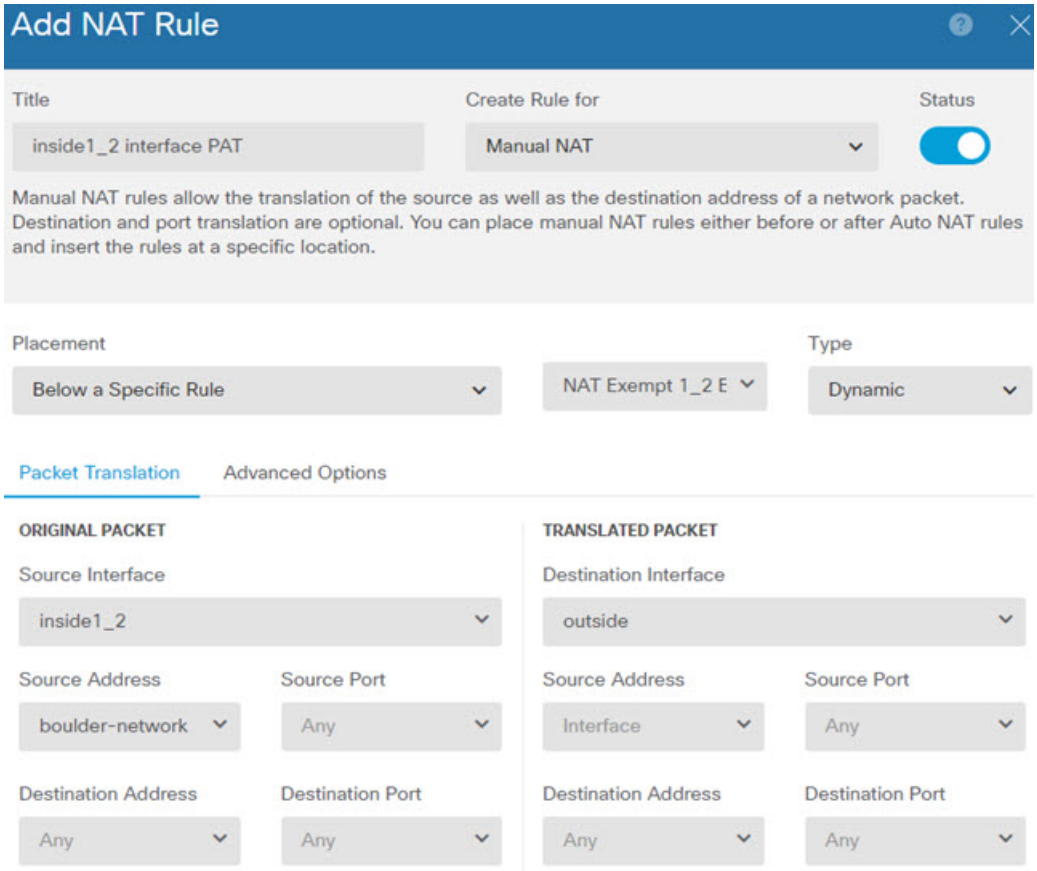
注释
内部接口可能已经配置了将所有 IPv4 流量包括在内的动态接口 PAT 规则，因为初始配置过程中会默认创建这些规则。不过，为完整起见，此处仍显示了这些配置。完成这些步骤之前，请检查是否已经存在将内部接口和网络包括在内的规则，如有则跳过此步骤。

a) 点击 + 按钮。

b) 配置以下属性：

- **标题** = inside1_2 接口 PAT（或您选择的其他名称）。
- **创建规则用于** = 手动 NAT。
- **位置** = **特定规则之下**，然后在“手动 NAT 在自动 NAT 之前”部分选择您在上面为此接口创建的规则。由于此规则将应用于所有目标地址，使用 sanjose-network 作为目标的规则必须在此规则之前，否则 sanjose-network 规则永远没有匹配项。默认设置是将新的手动 NAT 规则放到“NAT 规则在自动 NAT 之前”部分的末尾，此设置也已足够。

- **类型** = 动态。
- **源接口** = inside1_2。
- **目标接口** = 外部。
- **原始源地址** = boulder-network 网络对象。
- **转换后的源地址** = **接口**。此选项配置使用目标接口的接口 PAT。
- **原始目标地址** = 任何。
- **转换后的目标地址** = 任何。



c) 点击**确定**。

d) 重复此过程，为每个其他内部接口创建相应规则。

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。

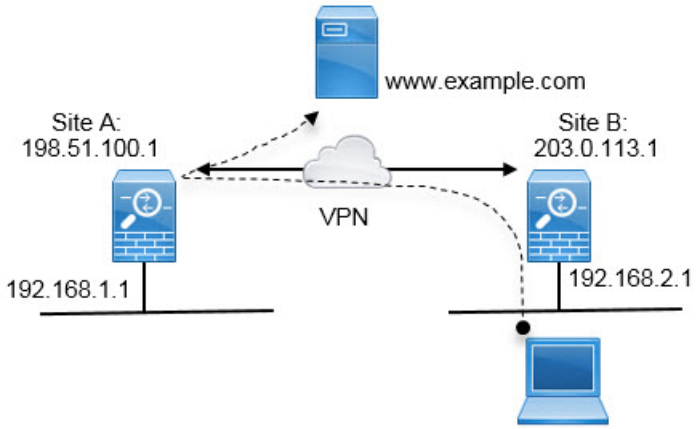
步骤 5 如果您也管理着 Firewall2（圣荷西办公室），您可以为该设备配置类似的规则。

- 当目标是 boulder-network 时，手动身份 NAT 规则将用于 sanjose-network。为 Firewall2 内部和外部网络创建新的接口对象。
- 当目标是“任何”时，手动动态接口 PAT 规则将用于 sanjose-network。

如何在外部接口上为外部站点间VPN用户提供互联网访问（发夹方法）

在站点间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。在 198.51.100.1（在主站点上，站点 A）与 203.0.113.1（远程站点，站点 B）之间配置了一个站点间 VPN 隧道。从网络内部的远程站点 192.168.2.0/24 流出的所有用户流量均通过此 VPN 隧道。因此，如果该网络上的用户想要访问互联网上的某个服务器（例如 www.example.com），连接会首先通过此 VPN 隧道，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。首先，需要配置 VPN 隧道的两个终端。

开始之前

此程序假定您使用了允许 VPN 流量的默认设置，使 VPN 流量受访问控制策略的限制。在运行配置中，这由 **no sysopt connection permit-vpn** 命令表示。如果您通过 FlexConfig 启用 **sysopt connection permit-vpn**，或者在 RA VPN 连接配置文件中选择了**为已解密流量绕过访问控制策略**选项，则无需执行配置访问控制规则的步骤。

过程

步骤 1 （站点 A，主站点。）配置到远程站点 B 的站点间 VPN 连接。

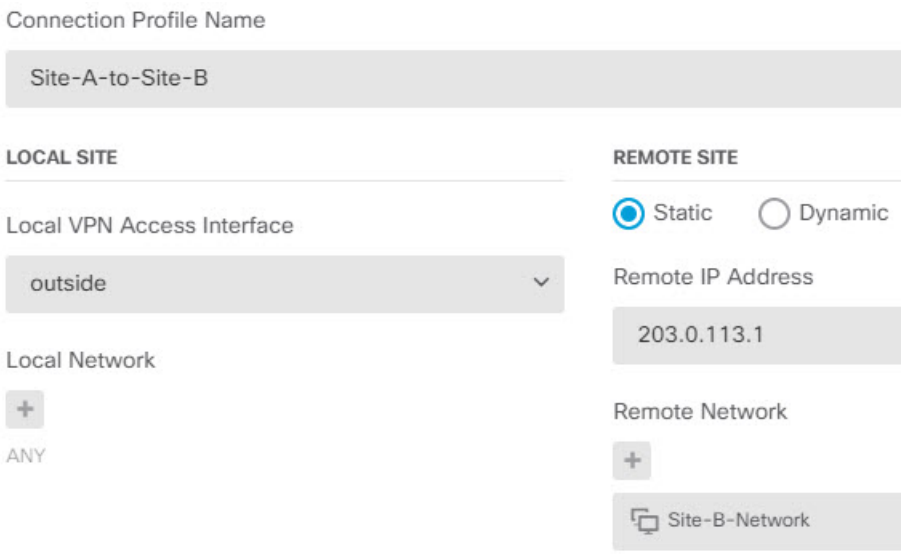
a) 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。

b) 点击 + 添加新连接。

c) 按如下所述定义终端，然后点击**下一步 (Next)**：

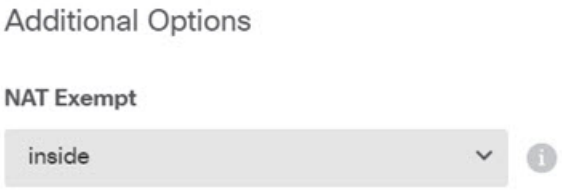
- **连接配置文件名称** - 为连接指定一个有意义的名称，例如 Site-A-to-Site-B。
- **本地 VPN 接入接口** - 选择外部接口。
- **本地网络** - 保留默认值“任何”。
- **远程 IP 地址** - 输入远程对等体外部接口的 IP 地址。在本示例中，此地址为 203.0.113.1。
- **远程网络** - 点击 +，然后选择定义远程对等体的受保护网络的网络对象。在本示例中，此对象为 192.168.2.0/24。可以点击**创建新网络**立即创建对象。

下图展示了第一步操作对应的界面。



d) 定义隐私配置，然后点击**下一步 (Next)**。

- **IKE 策略** - IKE 设置对发夹方法没有影响。选择满足安全需求的 IKE 版本、策略和提议即可。请记下您输入的本地和远程预共享密钥：配置远程对等体时会用到这些信息。
- **NAT 豁免** - 选择内部接口。



- **完美前向保密的 Diffie-Hellman 组** - 此设置对发夹方法没有影响。可以根据需要配置此设置。

e) 点击**完成**。

连接摘要信息将会复制到剪贴板。您可以将这些信息粘贴到文本文件或其他文档，帮助您配置远程对等体。

步骤 2 （站点 A，主站点。）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。

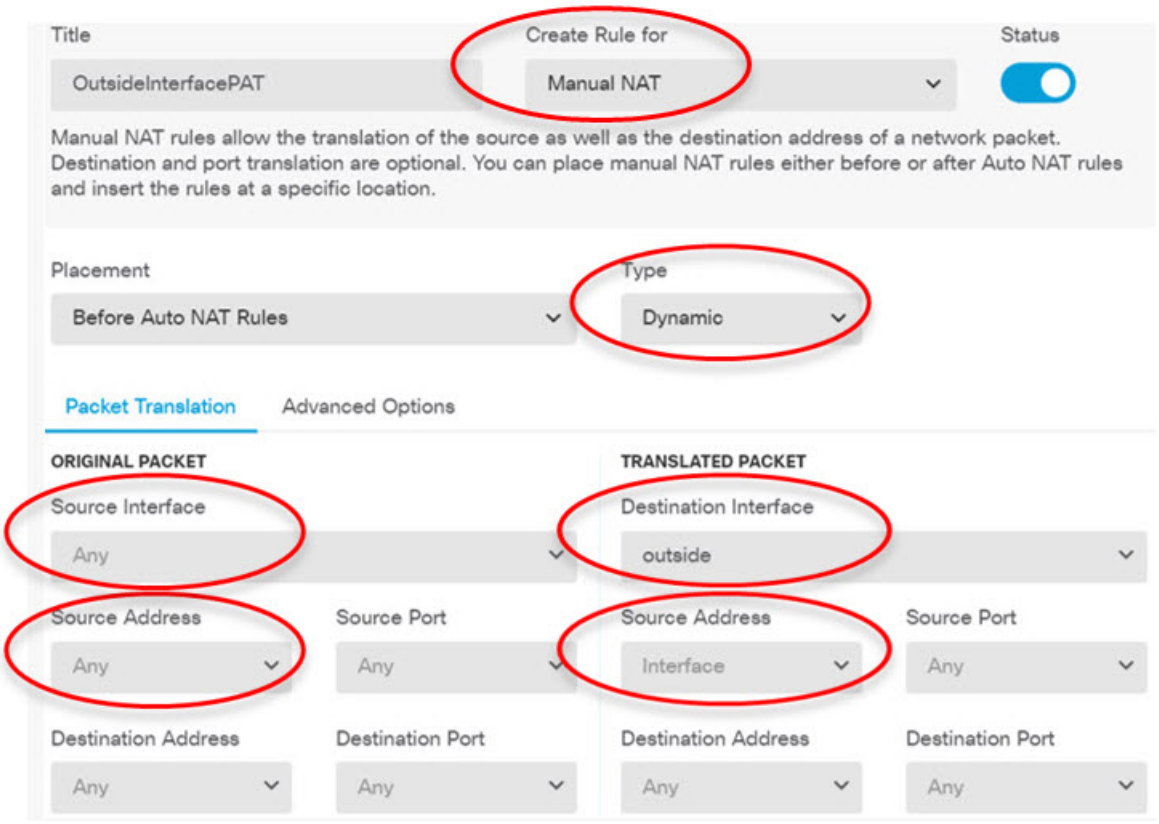
a) 依次点击**策略** > **NAT**。
b) 执行以下操作之一：

- 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 （站点 A，主站点。）配置访问控制规则，以允许访问站点 B 上的受保护网络。

仅仅创建 VPN 连接不会自动允许通过 VPN 上的流量。还需要确保您的访问控制策略允许流量通过远程网络。

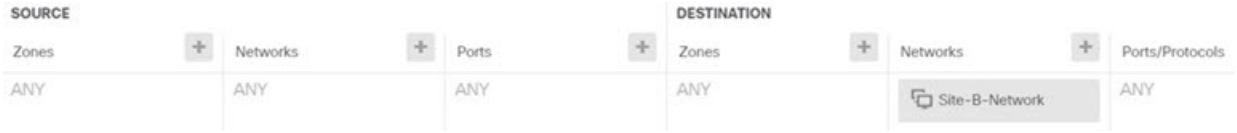
以下程序展示了如何添加远程网络专用的规则。是否需要其他规则取决于您现有的规则。

a) 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，Site-B-Network。
- **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**目标** > **网络**，请选择您在 VPN 连接配置文件中用于远程网络的同一对象。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**。

步骤 4 （站点 A，主站点。）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。如果保持窗口打开，那么成功部署后，窗口中将指示没有待处理的更改。

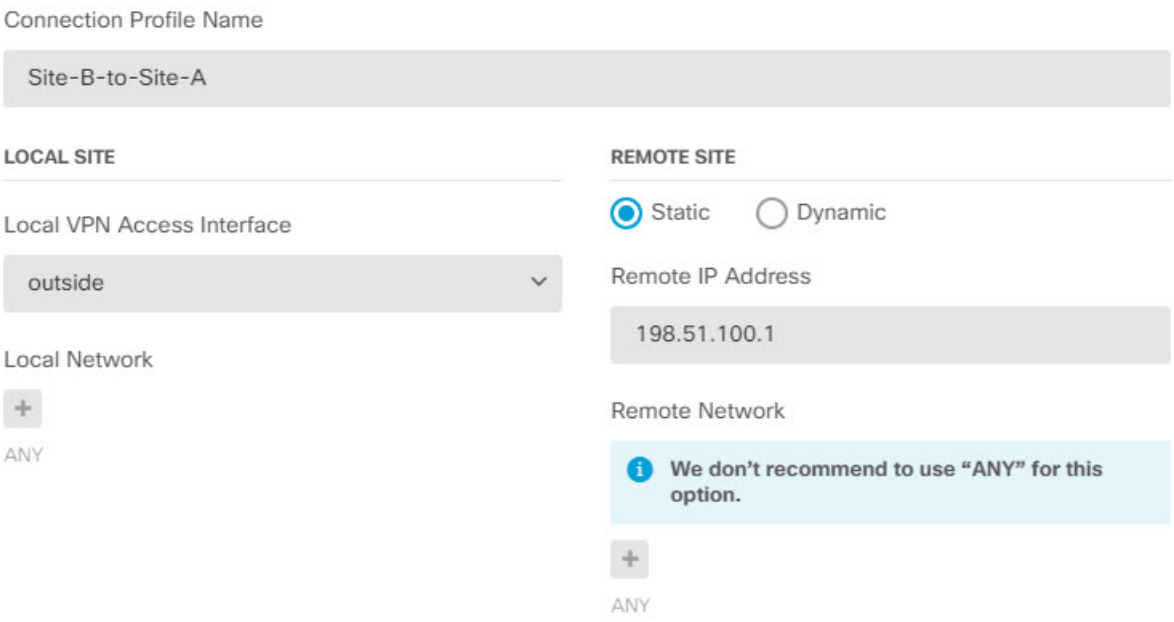
步骤 5 （站点 B，远程站点。）登录到远程站点设备，并配置到站点 A 的站点间 VPN 连接。

借助从站点 A 设备配置获取的连接摘要来配置连接的站点 B 端。

a) 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。
b) 点击 + 添加新连接。
c) 按如下所述定义终端，然后点击**下一步 (Next)**：

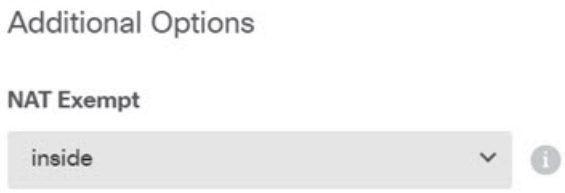
- **连接配置文件名称** - 为连接指定一个有意义的名称，例如，Site-B-to-Site-A。
- **本地 VPN 接入接口** - 选择外部接口。
- **本地网络** - 点击 +，然后选择定义本地受保护网络的网络对象。在本示例中，此对象为 192.168.2.0/24。可以点击**创建新网络**立即创建对象。
- **远程 IP 地址** - 输入主站点的外部接口的 IP 地址。在本示例中，此地址为 198.51.100.1。
- **远程网络** - 保留默认值“任何”。请忽略警告；此警告与本使用案例无关。

下图展示了第一步操作对应的界面。



d) 定义隐私配置，然后点击**下一步 (Next)**。

- **IKE 策略** - IKE 设置对发夹方法没有影响。配置与 VPN 连接的站点 A 端相同或兼容的选项。必须正确配置预共享密钥：按照站点 A 设备上的配置交换本地和远程密钥（适用于 IKEv2）。对于 IKEv1，只有一个密钥，此密钥在两个对等体上必须相同。
- **NAT 豁免** - 选择内部接口。



- **完美前向保密的 Diffie-Hellman 组** - 此设置对发夹方法没有影响。匹配 VPN 连接的站点 A 端使用的设置。

e) 点击**完成**。

步骤 6 （站点 B，远程站点。）删除受保护网络的所有 NAT 规则，以便离开此站点的所有流量都必须流经 VPN 隧道。

由于站点 A 设备会执行地址转换，因此无需在此设备上执行 NAT。但还是请根据自己的具体情况具体分析。如果您有多个内部网络，而且不是所有这些网络都参与此 VPN 连接，则请勿删除这些网络所需的 NAT 规则。

a) 依次点击**策略** > **NAT**。
b) 执行以下操作之一：

- 要删除规则，请将鼠标指针悬停在“操作”列上，然后点击删除图标 ( )。

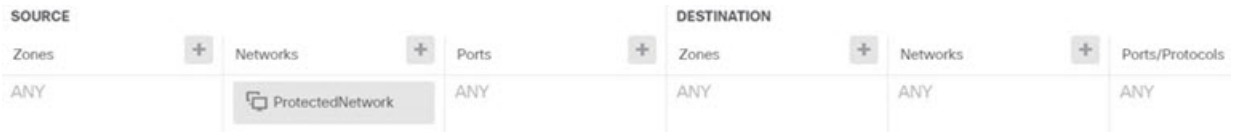
- 要编辑规则，使其不再应用于受保护的网络，请将鼠标指针悬停在“操作”列上，然后点击编辑图标 ( )。

步骤 7 （站点 B，远程站点。）配置访问控制规则，以允许从受保护网络访问互联网。

以下示例允许受保护网络中的流量通过任何目标。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。还有另外一种方法，就是在站点 A 设备上配置阻止规则。

a) 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，Protected-Network-to-Any。
- **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 VPN 连接配置文件中用于本地网络的同一对象。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**。

步骤 8 （站点 B，远程站点。）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，并等待部署完成。

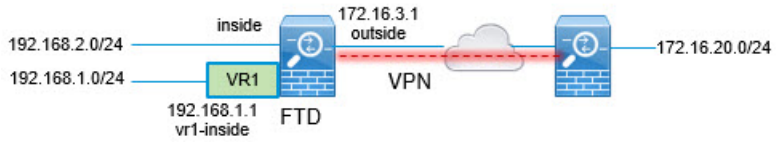
您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。如果保持窗口打开，那么成功部署后，窗口中将指示没有待处理的更改。

如何通过站点间 VPN 保护来自多个虚拟路由器的网络流量

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站点间 VPN。不能在分配给自定义虚拟路由器的接口上配置站点间 VPN。

由于虚拟路由器的路由表是独立的，因此，如果需要通过站点间VPN来保护往返托管在自定义虚拟路由器内的网络的连接，必须创建静态路由。您还需要更新站点间VPN连接，以包括这些额外的网络。

请考虑以下示例。在这种情况下，站点间 VPN 在 172.16.3.1 的外部接口上定义。此 VPN 可以包括内部网络 192.168.2.0/24，而无需进行额外配置，因为内部接口也是全局虚拟路由器的一部分。但是，如果您需要为 192.168.1.0/24 网络（其为 VR1 虚拟路由器的一部分）提供站点间 VPN 服务，则必须配置双向静态路由，并将网络添加到站点间 VPN 配置中。



开始之前

此示例假设您已在本地网络 192.168.2.0/24 与外部网络 172.16.20.0/24 之间配置站点间 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。

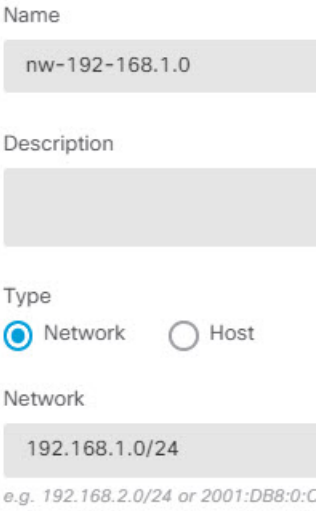
此路由允许受站点间 VPN 的外部（远程）终端保护的终端访问 VR1 虚拟路由器中的 192.168.1.0/24 网络。

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 ( )。

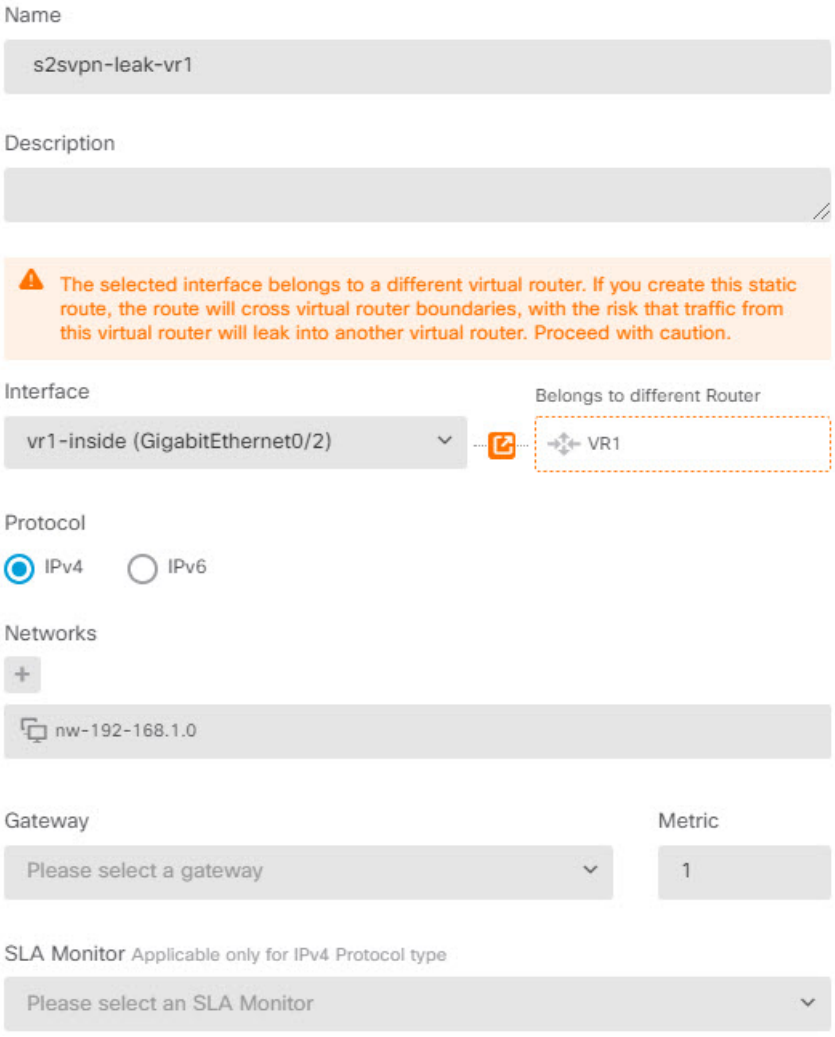
c) 在全局路由器的**静态路由**选项卡上，点击 + 并配置路由：

- **名称** - 可以使用任何名称，例如 **s2svpn-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。

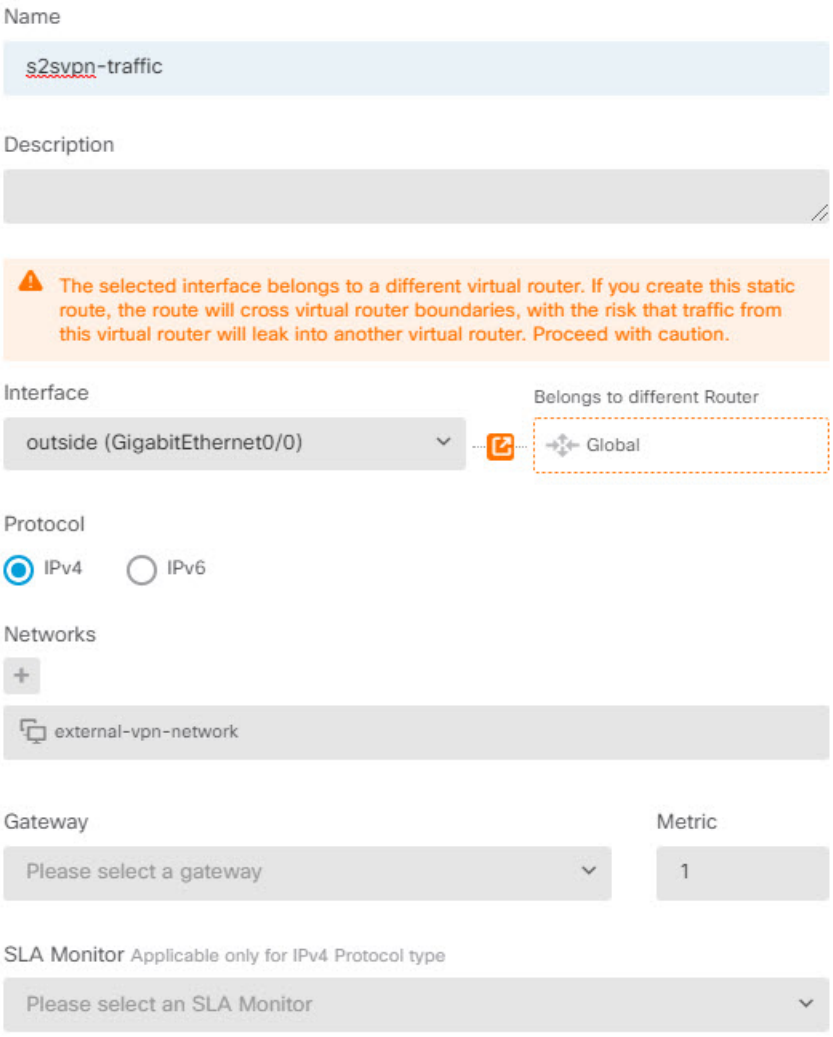
此路由允许 192.168.1.0/24 网络上的终端发起流经站点间 VPN 隧道的连接。在本示例中，远程终端正在保护 172.16.20.0/24 网络。

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 **s2svpn-traffic**。
- **接口** - 选择 **outside**。
- **协议** - 选择 **IPv4**。
- **网络** - 选择为远程终端的受保护网络创建的对象，例如 **external-vpn-network**。
- **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：



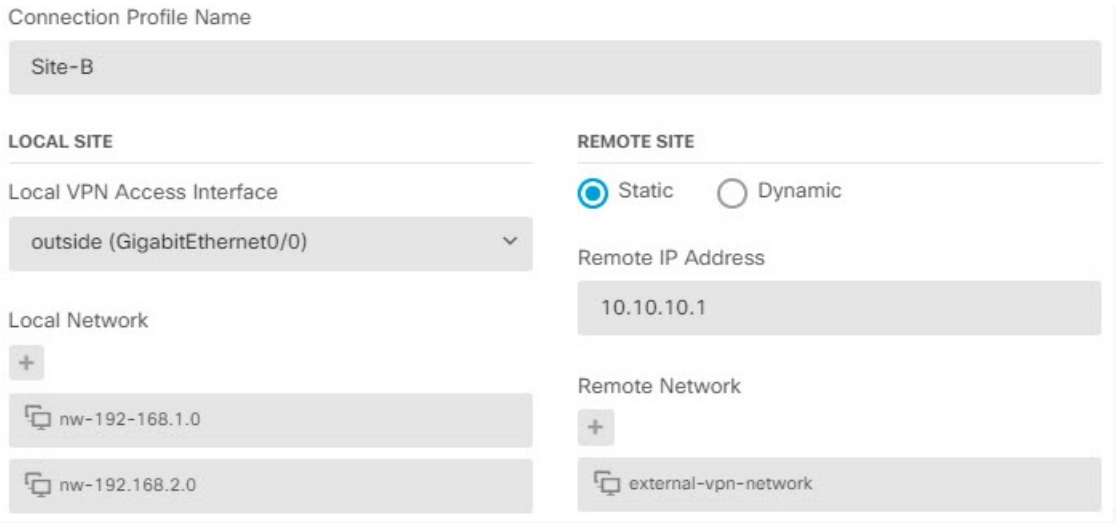
c) 点击**确定**。

步骤 3 将 192.168.1.0/24 网络添加到站点间 VPN 连接配置文件中。

a) 依次选择**设备** > **站点间 VPN** > **查看配置**。

b) 点击连接配置文件的编辑图标 ( )。

c) 在向导的第一页上，点击**本地网络**下的 +，然后为 192.168.1.0/24 网络添加对象。


Connection Profile Name
Site-B
LOCAL SITE
Local VPN Access Interface
outside (GigabitEthernet0/0)
Local Network
nw-192-168.1.0
nw-192.168.2.0
REMOTE SITE
Static
Dynamic
Remote IP Address
10.10.10.1
Remote Network
external-vpn-network

d) 完成向导。

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。

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。

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。

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。