站点到站点 VPN

关于站点间 VPN

Cisco Secure Firewall Threat Defense站点到站点 VPN 支持以下功能：

- IPsec IKEv1 和 IKEv2 协议。
- 用于身份验证的证书和自动或手动预共享密钥。
- IPv4 和 IPv6。支持内部和外部的所有组合。
- IPsec IKEv2 站点间 VPN 拓扑提供符合安全认证的配置设置。
- 静态和动态接口。
- 支持 管理中心和 威胁防御 HA 环境。
- 当隧道关闭时，VPN 会发出警报。
- 可使用 威胁防御统一 CLI 获得的隧道统计信息。
- 点对点外联网和中心辐射型 VPN 的 IKEv1 和 IKEv2 备份对等体配置。

- “中心辐射型”部署中作为中心的外联网设备。
- 与“点对点”部署中外联网设备配对的托管终端的动态 IP 地址。
- 作为终端的外联网设备的动态 IP 地址。
- “中心辐射型”部署中作为外联网设备的中心。

VPN 拓扑

要创建一个新的站点到站点VPN拓扑，必须为其指定一个唯一名称，指定拓扑类型，选择用于IPsec IKEv1 和/或 IKEv2 的 IKE 版本。此外，确定您的身份验证方法。配置完毕后，可以将拓扑部署到威胁防御设备。Cisco Secure Firewall Management Center仅在 威胁防御设备上配置站点到站点 VPN。

您可以从三种拓扑类型中进行选择，包括一个或多个 VPN 隧道：

- 点对点 (PTP) 部署在两个终端之间建立 VPN 隧道。
- 中心辐射型部署会建立一组 VPN 隧道，将中心终端连接到一组分支节点。
- 全网状部署会在一组终端之间建立一组 VPN 隧道。

IPsec 和 IKE

在 Cisco Secure Firewall Management Center中，站点到站点 VPN 是根据分配给 VPN 拓扑的 IKE 策略和 IPsec 建议配置的。策略和建议是定义站点到站点 VPN 的特性的参数集，例如用于在 IPsec 隧道中保护流量安全的安全协议和算法。可能需要多种策略类型来定义可以分配给VPN拓扑的完整配置映像。

身份验证

要对VPN连接进行身份验证，请在拓扑中配置预共享密钥，或在每个设备上配置信任点。预共享密钥允许在两个对等体之间共享安全密钥，该共享密钥在 IKE 身份验证阶段使用。信任点包含 CA 的身份、CA 特定的参数，以及与一个已注册身份证书的关联。

外部网设备

每种拓扑类型都可以包括外部网设备，即不在 管理中心中管理的设备。其中包括：

- Cisco Secure Firewall Management Center 支持但您的组织不负责的思科设备。例如，由您公司内的其他部门管理的网络中的分支，或者与服务提供商或合作伙伴的网络的连接。
- 非思科设备。不能使用 Cisco Secure Firewall Management Center 创建配置以及将配置部署到非思科设备。

将非思科设备或未由 Cisco Secure Firewall Management Center管理的思科设备作为“外联网”设备添加到 VPN 拓扑。此外，还指定每个远程设备的 IP 地址。

Cisco Secure Firewall Threat Defense站点到站点 VPN 指南和限制

- 站点间 VPN 支持 ECMP 区域接口。
- 必须为拓扑中的所有节点配置加密 ACL 或受保护的网络。不可在一个节点上为拓扑配置加密 ACL，而在另一个节点上配置受保护的网络。
- 您可以通过对不在当前域中的终端使用外联网对等体，在域之间建立 VPN 连接。
- 您可以使用 管理中心 备份来备份 威胁防御 VPN。
- IKEv1 不支持 CC/UCAPL 兼容设备。我们建议您对这些设备使用 IKEv2。
- 不能在域之间移动 VPN 拓扑。
- VPN 中不支持具有 “range” 选项的网络对象。
- 威胁防御 VPN 当前不支持 PDF 导出和策略比较。
- 对于 威胁防御 VPN，没有按隧道或按设备的编辑选项，只能编辑整个拓扑。
- 选择加密 ACL 时， 管理中心 不会验证传输模式的设备接口地址。
- 不支持自动镜像 ACE 生成。在任一端，对等设备的镜像 ACE 生成都是手动过程。
- 使用加密 ACL 时， 管理中心 仅支持点对点 VPN，不支持隧道运行状况事件。
- 只要使用的是 IKE 端口 500/4500，或者有一些 PAT 转换处于活动状态，则无法在同一端口上配置站点间 VPN，因为无法在这些端口上启动服务。
- 隧道状态不会实时更新，但是在 管理中心中以五分钟为间隔进行更新。
- 您无法使用字符 "（双引号）作为预共享密钥的一部分。如果您在预共享密钥中使用了 "，请确保更改该字符。

站点间 VPN 的要求和必备条件

型号支持

威胁防御

支持的域

枝叶

用户角色

管理员

管理站点间 VPN

“站点间 VPN”(Site to Site VPN) 页面提供站点间 VPN 隧道的快照。您可以查看隧道的状态，并根据设备、拓扑或隧道类型来过滤隧道。该页面每页列出20个拓扑，您可以在页面之间导航，以便查看更多拓扑详细信息。您可以点击单个 VPN 拓扑，以便展开并查看终端的详细信息。

开始之前

对于站点间 VPN 的证书身份验证，您必须通过按照证书中的说明分配信任点来准备设备。

过程

选择**设备 > VPN > 站点到站点**管理您的 Firepower 威胁防御站点到站点 VPN 配置和部署。

该页面列出了站点间 VPN 拓扑，并使用颜色代码来指示隧道的状态：

- 活动（绿色）-存在活动的 IPsec 隧道。
- 未知（琥珀色）-未从设备收到隧道建立事件。
- 关闭（红色）-不存在活动的 IPsec 隧道。
- 待部署 - 设备上尚未部署拓扑。

从以下选项中选择：

- **刷新**-查看 VPN 的更新状态。
- **添加**-创建新的策略型或路由型站点间 VPN。
- **编辑**-修改现有 VPN 拓扑的设置。

  注释 在最初保存拓扑类型之后，不能对其进行编辑。要更改拓扑类型，应删除该拓扑并新建一个拓扑。

  两个用户不应 同时编辑同一拓扑；然而，Web 界面不会阻止同时编辑。

- **删除 (Delete)** - 要删除 VPN 部署，请点击 **删除**（ ）。
- 部署 - 选择**部署 > 部署**；请参阅部署配置更改。

  注释 一些 VPN 设置仅在部署期间进行验证。请务必确认部署已经成功。

配置策略型站点间 VPN

过程

步骤 1 选择**设备 > VPN > 站点到站点**。然后，选择**添加 VPN > Firepower 威胁防御设备**，或编辑列出的 VPN 拓扑。。

步骤 2 输入唯一的**拓扑名称**。我们建议命名您的拓扑以指示它是一个威胁防御VPN，并指定其拓扑类型。

步骤 3 点击**策略型（加密映射）(Policy Based [Crypto Map])** 以配置站点间 VPN。

步骤 4 选择此 VPN 的**网络拓扑**。

步骤 5 选择要在 IKE 协商期间使用的 IKE 版本。**IKEv1** 或 **IKEv2**。

默认值是 IKEv2。根据需要选择一个或两个选项；如果拓扑中的任何设备不支持 IKEv2，请选择 IKEv1。

您也可以为点对点外联网 VPN 配置备份对等体。有关详细信息，请参阅威胁防御 VPN 终端选项，第 6 页。

步骤 6 必需： 通过点击拓扑中每个节点的 **添加**（+），为该 VPN 部署添加终端。

按照威胁防御 VPN 终端选项， 第 6 页中的描述配置每个终端字段。

- 对于“点到点”，配置**节点 A** 和**节点 B**。
- 对于“中心辐射型”，配置 **中心节点**和**分支节点**
- 对于“全网格”，配置多个**节点**

步骤 7 （可选） 按照描述为该部署指定非默认 IKE 选项 威胁防御 VPN IKE 选项， 第 9 页

步骤 8 （可选） 按照描述为该部署指定非默认 IPsec 选项 威胁防御 VPN IPSec 选项， 第 11 页

步骤 9 （可选） 按照威胁防御高级站点到站点 VPN 部署选项， 第 13 页中的描述为该部署指定非默认高级选项。

步骤 10 单击**保存**。
终端将添加到您的配置中。

下一步做什么

部署配置更改；请参阅部署配置更改。

注释 一些 VPN 设置仅在部署期间进行验证。请务必确认部署已经成功。

如果您收到 VPN 隧道处于非活动状态的警报，即使 VPN 会话已启动，请按照 VPN 故障排除说明来验证并确保 VPN 处于活动状态。有关详细信息，请参阅 VPN 监控和故障排除 和 VPN 故障排除。

威胁防御 VPN 终端选项

导航路径

设备 > VPN > 站点到站点。然后，**添加 VPN > Firepower 威胁防御设备**，或编辑列出的 VPN 拓扑。打开**终端**选项卡。

字段

设备

为您的部署选择一个终端节点：

- 由此 管理中心管理的 威胁防御设备
- 由此 管理中心管理的 威胁防御高可用性容器
- **外部网**设备，并非由此 管理中心 管理的任意设备（思科或第三方设备）。

设备名称

仅对于外部网设备，为该设备提供一个名称。我们建议其命名可将其识别为非托管设备。

接口

如果选择受管设备作为其终端，请在该受管设备上选择一个接口。

对于“点对点”部署，您还可以配置具有动态接口的终端。具有动态接口的终端只能与外联网设备配对，无法与具有托管设备的终端配对。

您可以在**设备** > **设备管理** > **添加/编辑设备** > **接口**下配置设备接口。

IP 地址

- 如果选择外联网设备（**不**由 管理中心管理的设备），请为终端指定一个 IP 地址。

  对于外联网设备，选择**静态**并指定一个 IP 地址，或选择**动态**以允许动态外联网设备。

- 如果选择托管设备作为终端，则从下拉列表中选择一个 IPv4 地址或多个 IPv6 地址。这些 IP 地址已分配给托管设备上的此接口。
- 拓扑中的所有终端都必须具有相同的 IP 寻址方案。IPv4 隧道可以传输 IPv6 流量，反之亦然。受保护的网络定义隧道流量将使用的寻址方案。
- 如果受管设备是高可用性容器，请从接口列表中进行选择。

此 IP 为私有 IP

如果终端驻留在带网络地址转换 (NAT) 的防火墙后面，请选中此复选框。

注释 仅当对等体由同一个管理中心管理时才使用此选项，如果对等体是外联网设备，则不要使用此选项。

公有 IP 地址

如果选中了**此 IP 为私有 IP** 复选框，请为防火墙指定公共 IP 地址。如果终端为响应方，则必须指定此值。

连接类型

将允许的协商指定为双向、只应答或只发起。受支持的连接类型组合有：

表 *1:* 受支持的连接类型组合

远程节点	中心节点
只发起	只应答
双向	只应答
双向	双向

证书映射

选择预配置的证书映射对象，或点击 **添加**（+） 以添加证书映射对象。证书地图定义在接收的客户端证书中需要哪些信息才能使其对 VPN 连接有效。有关详细信息，请参阅 证书映射对象。

受保护网络

⚠

注意 中心辐射型拓扑 - 为避免动态加密映射的流量丢弃，请确保不要为两个终端选择 任何 受保护的网络。

如果受保护的网络配置为 任何，则不会在两个终端上生成适用于隧道的加密 ACL。

定义受此 VPN 终端保护的网络。通过选择定义这些网络（受此终端保护的网络）的子网/IP 地址列表来选择网络。点击 **添加**（+） 可选择可用的网络对象，或添加新的网络对象。请参阅 创建网络对象。访问控制列表会由此处所做的选择生成。

- **子网/IP 地址（网络）** - VPN 终端不能有相同的 IP 地址，并且 VPN 终端对中的受保护网络不能重叠。如果一个终端的受保护网络包含 IPv4 或 IPv6 条目，另一个终端的受保护网络必须至少包含一个相同类型的条目（IPv4 或 IPv6）。否则，另一个终端的 IP 地址必须为相同类型，且不会与受保护网络中的条目重叠。（对于 IPv4，使用 /32 CIDR 地址块；对于 IPv6 使用 /128 CIDR 地址块）。如果以上两种检查均失败，则此终端对无效。

注释 Cisco Secure Firewall Management Center中默认 **启用反向路由注入** 。

子网/IP 地址（**网络**） 将保持默认选择。

如果已为“受保护的网络”选择 任何 并观察到默认路由流量被丢弃，请禁用反向路由注入。选择 **VPN**> **站点间 (Site to Site)** > 编辑 VPN > **IPsec** > **启用反向路由注入 (Enable Reverse Route Injection)**。部署配置更改，以便从加密映射配置中删除 set reverse-route（反向路由注入），并删除导致反向隧道流量被丢弃的 VPN 通告反向路由。

- **访问列表（扩展）(Access List [Extended])** - 扩展访问列表提供控制此终端可接受的流量类型（例如GRE或OSPF流量）的功能。流量可通过地址或端口加以限制。点击 **添加**（+）可添加访问控制列表对象。

注释 访问控制列表仅适用于点对点拓扑。

高级设置

启用动态反向路由注入 (Enable Dynamic Reverse Route Injection) - 反向路由注入 (RRI) 可让路由自动插入到受远程隧道终端保护的网络和主机的路由进程中。仅在成功建立 IPsec 安全关联 (SA) 后才会创建动态 RRI 路由。

注释
- 动态 RRI 仅在 IKEv2 上支持，在 IKEv1 或 IKEv1 + IKEv2 上不支持。
- 只发起对等体、全网状拓扑和外联网对等体不支持动态 RRI。
- 在点对点中，只有一个对等体可以启用动态 RRI。
- 在中心和分支之间，只有一个终端可以启用动态 RRI。
- 动态 RRI 不能与动态加密映射配合使用。

将本地身份发送到对等体 (Send Local Identity to Peers) - 选择此选项可将本地身份信息发送到对等设备。从列表中选择以下**本地身份配置 (Local Identity Configuration)** 之一并配置本地身份：

- **IP 地址 (IP address)** - 对身份使用接口的 IP 地址。
- **自动 (Auto)** - 对预共享密钥使用 IP 地址并对基于证书的连接使用证书 DN。
- **电邮 ID**- 指定要用于身份的邮件 ID。电邮 ID 最多可以包含 127 个字符。
- **主机名 (Hostname)** - 使用完全限定主机名。
- **密钥 ID (Key ID)** - 指定用于身份的密钥 ID。密钥 ID 必须少于 65 个字符。

本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。唯一身份允许 威胁防御 在 NAT 后面有多个 IPsec 隧道，以便连接到 Cisco Umbrella 安全互联网网关 (SIG)。

有关在 Umbrella 上配置唯一隧道 ID 的信息，请参阅 **Cisco Umbrella SIG 用户指南**。

VPN 过滤器 (VPN Filter) - 从列表中选择扩展访问列表，或点击**添加 (Add)** 以创建新的扩展访问列表对象，以过滤站点间 VPN 流量。

VPN 过滤器使用扩展访问列表来提供额外的安全性并过滤站点间 VPN 数据。通过为 VPN 过滤器选择的扩展访问列表对象，您可以在进入 VPN 隧道之前过滤预加密流量和离开 VPN 隧道的已解密流量。如果启用了 **sysopt permit-vpn** 选项，将对来自 VPN 隧道的流量绕过访问控制策略规则。如果启用了 **sysopt permit-vpn** 选项，VPN 过滤器有助于识别和过滤站点间 VPN 流量。

注释 只有点对点和中心辐射型拓扑支持 VPN 过滤器。它在网状拓扑上不支持。

对于中心辐射型拓扑，您可以选择覆盖分支终端上的中心 VPN 过滤器，以免需要在特定隧道上启用不同的 VPN 过滤器。

选择**覆盖中心上的 VPN 过滤器 (Override VPN Filter on the Hub)** 选项以覆盖辐射点上的集线器 VPN 过滤器。选择**远程 VPN 过滤器 (Remote VPN Filter)** 扩展访问列表对象或创建要覆盖的访问列表。

注释 对于作为分支的外联网设备，只有 **覆盖中心上的 VPN 过滤器** 选项可用。

有关 sysopt permit-VPN 的详细信息，请参阅威胁防御 高级站点间 VPN 隧道选项，第 15 页。

威胁防御 VPN IKE 选项

对于您为此拓扑选择的 IKE 版本，请指定 **IKEv1/IKEv2 设置 (IKEv1/IKEv2 Settings)**。

注释 此对话框中的设置适用于整个拓扑、所有隧道和所有受管设备。

导航路径

设备 > VPN > 站点到站点。然后，**添加 VPN > Firepower 威胁防御设备**，或编辑列出的 VPN 拓扑。打开 **IKE** 选项卡。

字段

策略

从预定义列表中选择 IKEv1 或 IKEv2 策略对象，或者创建新的对象以供使用。您可以选择多个 IKEv1 和 IKEv2 策略。IKEv1 和 IKEv2 最多支持 20 个 IKE 策略，每个都有不同的值集。为您创建的每个策略分别分配一个唯一的优先级。优先级数值越低，优先级就越高。

有关详细信息，请参阅 威胁防御 IKE 策略

身份验证类型

站点间VPN支持两种身份验证方法：预共享密钥和证书。有关这两种方法的说明，请参阅确定使用哪种身份验证方法。

注释 在支持 IKEv1 的 VPN 拓扑中，所选 IKEv1 策略对象中指定的**身份验证方法**会成为 IKEv1 **身份验证类型**设置的默认设置。这些值必须匹配，否则，您的配置将出错。

- **预共享自动密钥** - 管理中心 会自动定义此 VPN 的预共享密钥。指定**预共享密钥长度 (Pre-shared Key Length)**，即密钥中的字符数（1-27 个）。

  不支持将字符 "（双引号）作为预共享密钥的一部分。如果您在预共享密钥中使用了 "，请确保在升级到 Cisco Secure Firewall Threat Defense 6.30 或更高版本后更改该字符。

- **预共享手动密钥** - 手动分配此VPN的预共享密钥。指定 **密钥**，然后重新输入以 **确认密钥**。

  在为IKEv2选择此选项后，将显示 **仅执行基于十六进制的预共享密钥** 复选框，如果需要则将其选中。如果已经执行，则必须使用数字0-9或A-F，为该密钥输入一个有效的十六进制值（它是一个 2-256 个字符的偶数）。

- **证书 (Certificate)** - 当您将证书用作 VPN 连接的身份验证方法时，对等体从 PKI 基础设施中的 CA 服务器获取数字证书，并用其相互进行身份验证。

  在 **证书** 字段中，选择预配置的证书注册对象。此注册对象可在受管设备上生成同名的信任点。证书注册对象应与设备关联并安装在设备上，之后注册过程完成，然后会创建一个信任点。

  信任点表示 CA 或身份对。信任点包括 CA 的身份、CA 特定配置参数，以及与一个注册的身份证书的关联。

  在选择此选项之前，请注意以下事项：

  - 确保你已经在拓扑结构中的所有端点上注册了一个证书注册对象 - 证书登记对象包含创建证书签名请求 (CSR) 以及从指定的证书颁发机构 (CA) 获取身份证书所需的 CA 服务器信息和注册参数。证书注册对象用于将受管设备注册到 PKI 基础设施中，并在支持 VPN 连接的设备上创建信任点（CA 对象）。有关创建证书注册对象的说明，请参阅添加证书注册对象；有关在终端上注册对象的说明，请参阅以下适用内容之一：

    - 使用自签注册安装证书
    - 使用 EST 注册安装证书
    - 使用 SCEP 注册安装证书

- 使用手动注册安装证书
- 使用 PKCS12 文件安装证书

注释 对于站点间 VPN 拓扑，请确保在拓扑中的所有终端中注册相同的证书注册对象。有关详细信息，请参阅下表。

- 请参阅下表，了解不同场景的注册要求。某些场景会要求您覆盖特定设备的证书注册对象。请参阅管理对象覆盖以了解如何覆盖对象。

证书注册类型	所有终端的设备身份证书均来自同一 CA		所有终端的设备身份证书均来自不同 CA
	未在证书注册对象中指定设备特定参数	在证书注册对象中指定了设备特定的参数	
手动	无需覆盖	需要覆盖	需要覆盖
EST	无需覆盖	需要覆盖	需要覆盖
SCEP	无需覆盖	需要覆盖	需要覆盖
PKCS	需要覆盖	需要覆盖	需要覆盖
自签名	不适用	不适用	不适用

- 了解 Cisco Secure Firewall Threat Defense VPN 证书指南和限制中提到的 VPN 证书限制。

注释 如果使用 Windows 证书颁发机构（CA），则默认应用策略扩展名为 **IP 安全 IKE 中间**。如果使用此默认设置，则必须在 **PKI 证书注册** 对话框的 **密钥** 选项卡的“高级设置”部分中为所选对象选择 **忽略 IPsec 密钥使用** 选项。否则，终端无法完成站点间 VPN 连接。

威胁防御 VPN IPSec 选项

注释 此对话框中的设置适用于整个拓扑、所有隧道和所有受管设备。

加密映射类型

加密映射整合了设置 IPsec 安全关联 (SA) 所需的所有组件。当两个对等体尝试建立 SA 时，每个对等体均必须至少有一个兼容的加密映射项。IPsec 安全协商使用加密映射条目中定义的提议来保护该加密映射的 IPsec 规则所指定的数据流。为此部署的加密映射选择静态或动态模式：

- **静态** - 在点对点或全网状 VPN 拓扑中使用静态加密映射。
- **动态** - 动态加密映射实质上创建了一个不配置所有参数的加密映射项。稍后将动态配置缺少的参数（作为 IPsec 协商的结果）以满足远程对等体的要求。

  动态加密映射策略适用于中心辐射型以及点对点VPN拓扑。要应用这些策略，请为拓扑中的一个对等体指定动态 IP 地址，同时确保在此拓扑上启用动态加密映射。在全网格 VPN 拓扑中，只能应用静态加密映射策略。

IKEv2 模式

仅限于 IPsec IKEv2，请指定将 ESP 加密和身份验证应用于隧道的封装模式。此字段确定原始 IP 数据包的哪个部分已应用 ESP。

- **隧道模式** -（默认）封装模式设置为隧道模式。隧道模式将 ESP 加密和身份验证应用至整个原始 IP 数据包（IP 报头和数据），隐藏最终的源主机和目标地址，并成为新 IP 数据包中的负载。

  隧道模式的主要优势是不需要修改终端系统即可获得IPsec的优势。此模式允许路由器等网络设备用作IPsec代理。也就是说，路由器代表主机执行加密。源路由器加密数据包并将其沿 IPsec 隧道转发。目标路由器解密原始 IP 数据报并将其转发到目标系统。隧道模式还可以防止流量分析；利用隧道模式，攻击者只能确定隧道终端，而无法确定通过隧道传送的数据包的真正源和目标，即使其与隧道终点一样也无法确定。

- **传输首选**-封装模式设置为传输模式，且可选择在对等体不支持时回退到隧道模式。在传输模式下，仅加密 IP 负载，原始 IP 报头保持不变。因此，管理员必须选择与 VPN 接口 IP 地址相匹配的受保护网络。

  此模式的优势是每个数据包只需增加几个字节并且允许公共网络上的设备查看数据包的最终源和目标。在传输模式下，可以根据 IP 报头中的信息在中间网络上启用特殊处理（例如 QoS）。然而，第 4 层报头将被加密，这就限制了对数据包的检查。

- **传输必要**-封装模式设置为仅传输模式，允许回退到隧道模式。如果因一个端点不支持，端点无法成功协商传输模式，将不进行 VPN 连接。

计划书

点击 **编辑**（✎），以便为所选 IKEv1 或 IKEv2 方法指定提议。从可用的 **IKEv1 Ipsec 提议** 或 **IKEv2 Ipsec 提议** 对象中进行选择，或创建一个新的对象并选择该对象。请阅参配置 IKEv1 IPsec 方案对象和配置 IKEv2 IPsec 方案对象了解详情。

启用安全关联 (SA) 强度实施

启用此选项可确保子 IPsec SA 使用的加密算法不比父 IKE SA 更强 (根据密钥中的位数)。

启用反向路由注入

启用反向路由注入 (RRI) 支持静态路由自动插入到受远程隧道终端保护的网络和主机的路由进程中。

启用完全向前保密

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或私有密

钥。如果选择此选项，也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。

模块组

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。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。 有关选项的完整说明，请参阅决定要使用的 Diffie-Hellman 模数组。

生命周期持续时间

安全关联在过期之前存在的秒数。默认值为 28,800 秒。

寿命大小

使用特定安全关联的Ipsec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）。默认值为 4,608,000 千字节。不允许使用无限数据。

ESPv3 设置

验证传入 ICMP 错误消息

选择是否验证通过 IPsec 隧道接收，并发往专用网络上的内部主机的 ICMP 错误消息。

启用“不分段”策略

定义 IPsec 子系统如何处理大型数据包，这些数据包在 IP 报头中设置了不分片 (DF) 位。

策略

- Copy DF bit - 保持 DF 位。
- Clear DF bit - 忽略 DF 位。
- Set DF bit - 设置并使用 DF 位。

启用数据流机密性 (TFC) 数据包

启用虚拟TFC数据包，这些数据包会通过隧道，用于屏蔽流量配置文件。可以使用**Burst**、**Payload Size** 和 **Timeout** 参数生成穿过指定 SA 的随机长度的数据包。

注释 您可以按照任意长度和间隔对 IPsec 安全关联 (SA) 启用虚拟流量机密性 (TFC) 数据包。您必须在启用 TFC 之前设置 IKEv2 IPsec 提议。

启用 TFC 数据包可防止 VPN 隧道处于空闲状态。因此，如果启用了 TFC 数据包，则组策略中配置的 VPN 空闲超时不会按预期工作。

威胁防御高级站点到站点 VPN 部署选项

以下部分介绍在站点间VPN部署中可以指定的高级选项。这些设置适用于整个拓扑、所有隧道和所有受管设备。

威胁防御 VPN 高级 IKE 选项

高级 > IKE > ISAKAMP 设置

IKE 保持连接

启用或禁用 IKE 保持连接。您可以将此选项设置为 EnableInfinite，以便设备从不会启动保持连接来监控自身。

阈值

指定 IKE 保持连接置信间隔。该间隔是允许对等体在开始保持连接监控之前空闲的秒数。最小间隔值为 10 秒（默认值）；最大间隔值为 3600 秒。

重试间隔

指定在 IKE 保持连接重试之间等待的秒数。默认值为 2 秒；最大值为 10 秒。

发送至对等体的身份：

选择对等体将在 IKE 协商期间用于标识自身的身份：

- **autoOrDN**（默认值）- 按连接类型确定 IKE 协商：用于预共享密钥的 IP 地址或用于证书身份验证的证书 DN（不受支持）。
- **ipAddress** - 使用交换 ISAKMP 身份信息的主机的 IP 地址。
- **hostname** - 使用交换 ISAKMP 身份信息的主机的完全限定域名。此名称包含主机名和域名。

注释 为所有 VPN 连接启用或禁用此选项。

启用激进模式

如果 IP 地址未知，并且 DNS 解析在设备上可能不可用，请选择此协商方法来交换密钥信息。协商基于主机名和域名。

在隧道断开连接时启用通知

当 SA 上接收的入站数据包与该 SA 的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。默认情况下会禁用发送此通知。

高级 > IKE > IVEv2 安全关联 (SA) 设置

IKE v2 可使用其他会话控制，限制打开的 SA 的数量。默认情况下，打开的 SA 的数量没有限制。

Cookie 质询

是否向对等体设备发送 Cookie 质询，以响应 SA 发起数据包，这可以帮助阻止拒绝服务 (DoS) 攻击。默认情况下，当 50% 的可用 SA 正在协商时使用 Cookie 质询。选择以下选项之一：

- 自定义
- 从不（默认）
- 始终

质询传入 Cookie 的阈值
正在协商的允许的 SA 总数的百分比。这将对未来的任何 SA 协商都触发 Cookie 质询。范围为 0 到 100%。

协商中允许的 SA 数
限制可以随时协商的 SA 的最大数量。如果与 Cookie 质询配合使用，可以配置低于此限制的 Cookie 质询阈值，以便实现有效的交叉检查。

允许的最大 SA 数
限制允许的 IKEv2 连接数。默认值为不受限制。

在隧道断开连接时启用通知
当SA上接收的入站数据包与该SA的流量选择器不匹配时，允许管理员启用或禁用向对等体发送 IKE 通知。默认情况下禁用发送此通知。

威胁防御 VPN高级 IPsec 选项

高级 > IPsec > IPsec 设置

加密前启用分段
此选项允许流量通过不支持 IP 分片的 NAT 设备。这不影响支持 IP 分片的 NAT 设备的运行。

路径最大传输单元老化
选中以启用“路径最大传输单元 (PMTU) 时效”，即重置安全关联 (SA) 的 PMTU 的间隔时间。

值重置间隔
输入SA的PMTU值重置为其原始值的分钟数。有效范围是10到30分钟，默认值为不受限制。

威胁防御 高级站点间 VPN 隧道选项

导航路径

设备 > VPN > 站点到站点，然后，选择**添加 VPN > Firepower 威胁防御设备**，或编辑列出的 VPN 拓扑。打开**高级**选项卡，然后在导航窗格中选择**隧道**。

隧道选项

仅可用于中心辐射型拓扑和全网状拓扑。对于点对点配置，不会显示此部分。

- **使辐射间连接通过中心** - 默认情况下将被禁用。选择此字段将使辐射每一端上的设备将其连接通过中心节点扩展到另一台设备。

NAT 设置

- **保持连接消息穿越** - 选择是否启用 NAT 保持连接消息穿越。NAT 遍历保持连接用于在 VPN 连接的中心和分支之间存在设备（中间设备）并且该设备对 IPsec 流执行 NAT 时，传输保持连接消息时。

  如果选择此选项，请配置在辐射与中间设备之间发送两次保持连接信号（以指示会话处于活动状态）之间的**间隔**（以秒为单位）。此值可以介于 5 到 3600 秒之间。默认值为 20 秒。

VPN 流量访问控制

- **为已解密的流量绕过访问控制策略 (sysopt permit-vpn)** - 默认情况下，威胁防御 会在解密的流量上应用访问控制策略检查。启用此选项可绕过 ACL 检查。威胁防御 仍会将从 AAA 服务器下载的 VPN 过滤器 ACL 和授权 ACL 应用于 VPN 流量。

  启用或禁用所有VPN连接的选项。如果禁用此选项，请确保访问控制策略或预过滤器策略允许流量。

证书映射设置

- **使用在终端中配置的证书映射来确定隧道**-如果启用（选中）此选项，则将通过匹配已收到证书的内容与在终端节点中配置的证书对象的内容，来确定隧道。
- **使用证书 OU 字段来确定隧道**- 如果选择此选项，将指示如果无法根据已配置的映射确定节点（上面的选项），则将使用已收到证书的使用者可分辨名称 (DN) 中组织单位 (OU) 的值来确定隧道。
- **使用 IKE 身份来确定隧道**- 如果选择此选项，将指示如果无法根据规则匹配确定或通过 OU 获取节点（上面的选项），则会根据 phase1 IKE ID 的内容，将基于证书的 IKE 会话映射到隧道。
- **使用对等体 IP 地址来确定隧道**-如果选择此选项，将指示如果无法根据规则匹配确定或通过OU或 IKE ID 方法获取节点（上面的选项），则将使用已建立的对等体 IP 地址。

关于 Virtual Tunnel Interface

管理中心 支持称为虚拟隧道接口 (VTI) 的可路由逻辑接口。VTI 不需要将 IPsec 会话静态映射到物理接口。IPsec 隧道终端与虚拟接口关联。您可以像使用其他接口一样使用这些接口，并应用静态和动态路由策略。

作为策略型 VPN 的替代方案，您可以在 VTI 的对等体之间创建 VPN 隧道。VTI 可通过将 IPSec 配置文件连接到每个隧道的端部，为基于 VPN 的路由提供支持。VTI 会使用静态或动态路由。设备加密或解密来自或到达隧道接口的流量，并根据路由表将其转发。这可以简化部署，而且 VTI 通过动态路由协议支持路由型VPN，还能满足虚拟私有云的诸多要求。管理中心 让您能够从基于密码图的 VPN 配置轻松迁移到基于 VTI 的 VPN。

您可以使用站点到站点 VPN 向导为静态 VTI 配置基于路由的 VPN。使用静态路由或 BGP 加密流量。

您可以创建路由安全区，向其添加 VTI 接口，然后为通过 VTI 隧道为解密的流量控制定义访问控制规则。

您可以在以下对象之间创建基于 VTI 的 VPN：

- 两台 威胁防御 设备。
- 一个威胁防御和公共云。
- 一个威胁防御和另一个具有运营商冗余的威胁防御。

- 一个威胁防御以及任何其他带有 VTI 接口的设备。

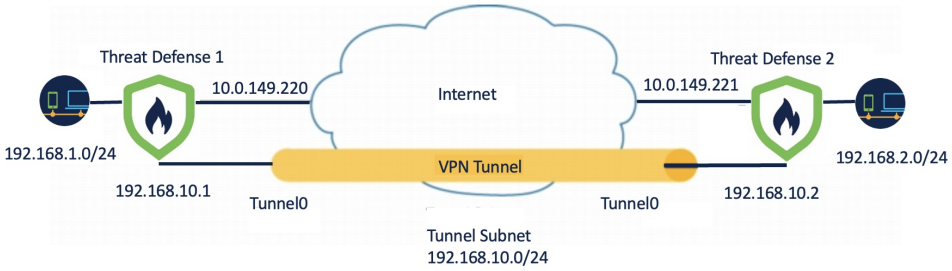
有关详细信息，请参阅 静态 VTI，第 17 页。

威胁防御功能历史记录

静态 VTI

静态 VTI 使用隧道接口在两个站点之间创建始终在线的隧道。对于静态 VTI，您必须将物理接口定义为隧道源。每个设备最多可以关联 1024 个 VTI。要在管理中心创建静态 VTI 接口，请参阅添加 VTI 接口，第 20 页。

下图显示了使用静态 VTI 的 VPN 拓扑。



关于威胁防御 1：

- 静态 VTI IP 地址为 192.168.10.1
- 隧道源为 10.0.149.220
- 隧道目的地为 10.0.149.221

关于威胁防御 2：

- 静态 VTI IP 地址为 192.168.10.2
- 隧道源为 10.0.149.221
- 隧道目的地为 10.0.149.220

优势

- 最大限度地减少和简化配置。

  您不必跟踪加密映射访问列表的所有远程子网，也不必配置复杂的访问列表或加密映射。

- 提供可路由接口。

  支持 BGP、 等 IP 路由协议和静态路由。

- 支持备份 VPN 隧道
- 支持使用 ECMP 进行负载均衡。

- 支持虚拟路由器。
- 为 VPN 流量提供差分访问控制。

  您可以为 VTI 配置安全区域，并将其用于 AC 策略。该配置：

  - 允许您对 VPN 流量与明文流量进行分类和区分，并选择性地允许 VPN 流量。
  - 为跨不同 VPN 隧道的 VPN 流量提供差分访问控制。

Virtual Tunnel Interfaces 准则和限制

IPv6 支持

- VTI 支持 IPv6。
- 隧道源接口可以有一个 IPv6 地址，并且同样的地址可以用作隧道终端。
- 管理中心 支持以下 VTI IP（或内部网络 IP 版本）与公共 IP 版本的组合：
  - IPv6 over IPv6
  - 基于 IPv6 的 IPv4
  - IPv4 over IPv4
  - 基于 IPv4 的 IPv6
- VTI 支持将静态和动态 IPv6 地址作为隧道源和目的地址。
- 隧道源接口可以有一个 IPv6 地址，并且您可以将隧道终端地址。如果不指定地址， 威胁防御使用列表中的第一个 IPv6 全局地址会被默认为隧道终端。

BGP IPv6 支持

VTI 支持 IPv6 BGP。

多实例和群集

- 多实例中支持 VTI。
- VTI 不支持群集。

防火墙模式

仅在路由模式中支持 VTI。

静态 VTI 的限制

- 仅支持 20 个唯一的 IPSec 配置文件。

- 不支持动态 VTI、OSPF 和 QoS。
- 在策略型路由中，您只能将 VTI 配置为出口接口。

静态VTI 的一般配置准则

- VTI 只有在 IPsec 模式下才可配置。
- 可以将 BGP 或静态路由用于使用这种隧道接口的流量。
- 在具有动态路由的 HA 配置中，备用设备无法通过 VTI 隧道访问已知子网，因为这些隧道是使用活动 IP 地址创建的。
- 您最多可以在一台设备上配置 1024 个静态 VTI。在计算 VTI 计数时，请考虑以下事项：
  - 包括 nameif 子接口，以便得出可在设备上配置的 VTI 总数。
  - 您不能在端口通道的成员接口上配置 nameif。因此，隧道计数只会随实际主端口通道接口的数量减少，而不会随其任何成员接口的数量减少。
  - 平台上的 VTI 计数限于该平台上可配置的 VLAN 数量。例如，Firepower 1120 支持 512 个 VLAN，隧道计数为 512 减去 配置的物理接口数。
- 如果要在高可用性设置中的设备上配置超过 400 个 VTI，您必须将 45 秒配置为 威胁防御 HA 的设备保持时间。
- VTI 的 MTU 将根据底层物理接口自动设置。
- 静态 VTI 支持 IKE 版本 v1 和 v2，并使用 IPsec 在隧道的源地址与目标地址之间收发数据。
- 如果必须应用 NAT，则将 IKE 和 ESP 数据包封装在 UDP 报头中。
- 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。
- 隧道组名称必须与对等体作为其 IKEv1 或 IKEv2 身份发送的内容相符。
- 对于 LAN 间隧道组中的 IKEv1，仅当隧道身份验证方法为数字证书和/或对等体配置为使用积极模式时，才能使用非 IP 地址的名称。
- 只要加密映射中配置的对等体地址与 VTI 的隧道目的地址不同，VTI 和加密映射配置就可以在同一个物理接口上共存。
- 默认情况下，所有通过 VTI 发送的流量都会被加密。
- 可以在 VTI 接口上应用访问规则来控制通过 VTI 的流量。
- 您可以将 VTI 接口与 ECMP 区域关联，同时配置 ECMP 静态路由以实现以下目的：
  - 负载均衡（主用/主用 VTI）- 连接可以通过任何并行 VTI 隧道进行传输。
  - 无缝连接迁移 - 当 VTI 隧道无法访问时，流会被无缝迁移到同一区域中配置的另一个 VTI 接口。

- 非对称路由 - 通过一个 VTI 接口转发流量，并通过另一个 VTI 接口配置反向流量。

有关配置 ECMP 的信息，请参阅配置等价静态路由。

备份 VTI 的准则和限制

- 不支持跨隧道故障转移的流恢复能力。例如，明文 TCP 连接在隧道故障切换后丢失，而您需要重新启动故障转移期间发生的任何 FTP 传输。
- 备份 VTI 中不支持证书身份验证。

相关主题

环回接口的准则和限制

创建基于路由的站点间 VPN，第 21 页

添加 VTI 接口

要配置基于路由的站点间 VPN，您必须在 VTI 隧道的两个节点上的设备上创建 VTI 接口。

过程

步骤 1 选择**设备 > 设备管理**。

步骤 2 点击要创建 VTI 接口的设备旁边的**编辑**图标。

步骤 3 选择 **添加接口 > 虚拟隧道接口**。

步骤 4 输入接口的名称和说明。默认情况下，接口处于启用状态。

确保指定的名称不超过 28 个字符。

步骤 5 （可选）从 **安全区域** 下拉列表中选择一个安全区域，以便以将静态 VTI 接口添加到该区域。

如果要在安全区域的基础上执行流量检查，请将 VTI 接口添加到安全区域并配置访问控制 (AC) 规则。要允许 VPN 流量通过隧道，您需要添加一条将此安全区域作为源区域的 AC 规则。

步骤 6 在 **优先级** 字段中输入在多个 VTI 之间对流量进行负载均衡的优先级。

范围是从 0 到 65535。最小的数字具有最高优先级。此选项不适用于动态 VTI。

步骤 7 对于静态 VTI，请在 **隧道 ID** 字段中输入 0 到 10413 范围内的唯一隧道 ID。

步骤 8 从 **隧道源** 下拉列表中选择隧道源接口。

VPN 隧道在此接口（物理 接口）处终止。从下拉列表中选择接口的 IP 地址。无论 IPsec 隧道模式如何，您都可以选择 IP 地址。如果有多个 IPv6 地址，请选择要用作隧道终端的地址。

步骤 9 在 **IPSec 隧道模式**下，点击 **IPv4** 或 **IPv6** 单选按钮以指定通过 IPsec 隧道的流量类型。

步骤 10 在 **IP 地址 (IP Address)** 字段中，输入要用于隧道终端的 IP 地址和子网。基于路由的 VPN 的两个终端的 VTI IP 地址必须都位于同一子网中。

注释　我们建议使用 169.254.x.x/16 范围内的 IP，不包括 威胁防御 保留范围 (169.254.1.x/24)。此外，请使用 /30 作为网络掩码，以便最好在 VTI 隧道的两端仅使用两个地址。例如，169.254.100.1/30。

步骤 11　点击**确定 (OK)**。

步骤 12　单击**保存**。

创建基于路由的站点间 VPN

您可以为以下两种拓扑配置基于路由的站点间 VPN：

- **点对点**：在隧道的两个节点上配置 VTI，并使用向导配置 VPN。
- **中心辐射型**：在中心和分支上配置 VTI。

您可以将外联网设备配置为集线器，并将托管设备配置为分支。您可以配置多个中心和分支，也可以配置备份中心和分支。

- 对于外联网中心和分支，您可以将多个 IP 配置为备份。
- 对于托管分支，您可以配置备份静态 VTI 接口以及主 VTI 接口。

有关 VTI 的详细信息，请参阅关于 Virtual Tunnel Interface，第 16 页。

过程

步骤 1　选择**设备 > 站点间**。

步骤 2　在**添加 VPN (Add VPN)** 下拉菜单中，选择 **Firepower 威胁防御设备 (Firepower Threat Defense Device)**。

步骤 3　选择**添加**。

步骤 4　在 **拓扑名称** 字段中，输入 VPN 拓扑的名称。

步骤 5　选择 **基于路由 (VTI)** 并执行以下操作之一：

- 选择 **点对点** 作为网络拓扑。要为路由型 **点对点** 拓扑配置终端，请参阅为点对点拓扑配置终端，第 22 页。
- 选择 **中心辐射型** 作为网络拓扑。要为路由型**中心辐射型**拓扑配置终端，请参阅为中心辐射型拓扑配置终端，第 24 页。

步骤 6　（可选）为部署指定 **IKE** 选项，如威胁防御 VPN IKE 选项，第 9 页中所述。

步骤 7　（可选）为部署指定 **IPsec** 选项，如威胁防御 VPN IPSec 选项，第 11 页中所述。

步骤 8　（可选）为部署指定 **高级** 选项，如威胁防御高级站点到站点 VPN 部署选项，第 13 页中所述。

步骤 9 单击**保存**。

下一步做什么

在两台设备上配置 VTI 接口和 VTI 隧道后，您必须配置：

- 用于通过 VTI 隧道在设备之间路由 VTI 流量的路由策略。有关详细信息，请参阅为 VTI 配置路由和 AC 策略，第 28 页。
- 用于允许已加密的流量的访问控制规则。选择 **策略 > 访问控制**。

为点对点拓扑配置终端

配置以下参数，为 **点对点** 拓扑节点为路由型站点间 VPN 配置终端：

开始之前

在基于路由的 VPN 中配置点对点拓扑的基本参数，如 创建基于路由的站点间 VPN，第 21 页 中所述，然后点击 **终端** 选项卡。

过程

步骤 1 在 **节点 A** 下，从 **设备** 下拉菜单中选择要用作 VTI 隧道第一个终端的已注册设备 (威胁防御) 或外联网的名称。

对于外联网对等体，请指定以下参数：

1. 指定设备的名称。
2. 在 **终端 IP 地址** 中输入主 IP 地址。如果配置备份 VTI，请添加一个逗号，然后指定备份 IP 地址。
3. 点击**确定 (OK)**。

为外联网集线器配置上述参数后，请在 **IKE** 选项卡中指定外联网的预共享密钥。

注释 AWS VPC 会将 **AES-GCM-NULL-SHA-LATEST** 作为默认策略。如果远程对等体连接到 AWS VPC，请从 **策略** 下拉列表中选择 **AES-GCM-NULL-SHA-LATEST** 以建立 VPN 连接，而无需更改 AWS 中的默认值。

步骤 2 对于已注册的设备，您可以从 **虚拟隧道接口** 下拉列表中指定节点 A 的 VTI 接口。

所选隧道接口是节点 A 的源接口，并且它将成为节点 B 的隧道目的接口。

如果要在节点 A 上创建一个新接口，请点击 + 图标并配置字段，如添加 VTI 接口，第 20 页中所述。

如果要编辑现有 VTI 的配置，请在**虚拟隧道接口 (Virtual Tunnel Interface)** 下拉字段中选择 VTI，然后点击**编辑 VTI (Edit VTI)**。

步骤 3 如果您的节点 A 设备位于 NAT 设备后面，请选中**隧道源 IP 为专用 (Tunnel Source IP is Private)** 复选框。在**隧道源公共 IP 地址 (Tunnel Source Public IP Address)** 字段中，输入隧道源公共 IP 地址。

步骤 4 **将本地身份发送到对等体 (Send Local Identity to Peers)** - 选择此选项可将本地身份信息发送到对等设备。从列表中选择以下**本地身份配置 (Local Identity Configuration)** 之一并配置本地身份：

- **IP 地址 (IP address)** - 对身份使用接口的 IP 地址。
- **自动 (Auto)** - 对预共享密钥使用 IP 地址并对基于证书的连接使用证书 DN。
- **电邮 ID**- 指定要用于身份的邮件 ID。电邮 ID 最多可以包含 127 个字符。
- **主机名 (Hostname)** - 使用完全限定主机名。
- **密钥 ID (Key ID)** - 指定用于身份的密钥 ID。密钥 ID 必须少于 65 个字符。

本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。唯一身份允许 威胁防御 在 NAT 后面有多个 IPsec 隧道，以便连接到思科 Umbrella 安全互联网网关 (SIG)。

有关在 Umbrella 上配置唯一隧道 ID 的信息，请参阅 **Cisco Umbrella SIG 用户指南**。

步骤 5 （可选）点击 **添加备份 VTI** 以指定其他 VTI 接口作为备份接口。

注释 确保两个拓扑对等体的备份 VTI 具有不同的隧道源。一台设备不能有两个具有相同隧道源和隧道目标的 VTI；因此，请配置唯一的隧道源和隧道目标组合。

虽然虚拟隧道接口是在备用 VTI 下指定的，但路由配置决定了哪个隧道会被用作主隧道或备用隧道。

步骤 6 在**连接类型 (Connection Type)** 下拉菜单中，选择**仅应答 (Answer Only)** 或**双向 (Bidirectional)**。如果已将 IKE 协议版本选择为 IKEv1，则其中一个节点必须为 **仅应答**。

仅应答：设备只能在对等设备发起连接时做出响应，不能发起任何连接。

双向：设备可以发起或响应连接。这是默认选项。

步骤 7 在**其他配置 (Additional Configuration)** 下，执行以下操作：

- 要将流量路由到 VTI，请点击**路由策略 (Routing Policy)**。管理中心 会显示**设备 (Devices)** > **路由 (Routing)** 页面。

  您可以为 VPN 流量配置静态或 BGP 路由。

- 要允许 VPN 流量，请点击 **AC 策略 (AC Policy)**。管理中心 会显示设备的访问控制策略页面。继续添加用于指定 VTI 安全区域的允许/阻止规则。配置备份 VTI 时，请确保包含与主 VTI 相同的安全区域的备份隧道。AC 策略页面中的备份 VTI 不需要特定的设置。

步骤 8 对节点 B 重复上述程序。

步骤 9 点击**确定 (OK)**。

下一步做什么

- （可选）为部署指定 **IKE** 选项，如 威胁防御 VPN IKE 选项，第 9 页中所述。
- （可选）为部署指定 **IPsec** 选项，如 威胁防御 VPN IPSec 选项，第 11 页中所述。
- （可选）为部署指定 **高级** 选项，如 威胁防御高级站点到站点 VPN 部署选项，第 13 页中所述。
- 单击**保存**。
- 要将流量路由到 VTI，请依次选择 **设备 > 设备管理**，编辑威胁防御设备，然后点击 **路由** 选项卡。

  您可以为 VPN 流量配置静态或 BGP 路由。
- 要允许 VPN 流量，请依次选择 **策略 > 访问控制**。。添加用于指定 VTI 安全区域的规则。对于备份 VTI，请确保包含与主 VTI 相同的安全区域的备份 VTI。

为中心辐射型拓扑配置终端

配置以下参数，为 **中心辐射型** 拓扑节点配置路由型站点间 VPN 终端：

开始之前

在基于路由的 VPN 中配置中心辐射型拓扑的基本参数，如 创建基于路由的站点间 VPN，第 21 页中所述，然后点击 **终端** 选项卡。

过程

步骤 1 添加集线器节点：

a) 在**中心节点 (Hub Nodes)** 下，点击**添加 (+) (Add [+])**。
b) 在**设备名称 (Device Name)** 字段中输入设备名称。
c) 在**终端 IP 地址 (Endpoint IP address)**中，输入主 IP 地址。如果要配置备份中心，请输入一个逗号，然后指定备份 IP 地址。
d) 点击 **IKE** 选项卡并指定外联网上提供的预共享密钥。
e) 单击**确定 (OK)**。

添加分支节点：

- 对于外联网分支，配置参数与集线器类似。
- 对于托管分支节点，请配置类似于点对点节点的参数。

a) 在**分支节点 (Spoke Nodes)** 下，点击**添加 (+) (Add [+])**。
b) 在**设备 (Device)** 下拉菜单中，选择已注册设备的名称 (威胁防御).
c) 指定接口设置：

- 在 **静态虚拟隧道接口** 下拉菜单中，选择您在已选为 VTI 终端的 威胁防御 设备上创建的 VTI 接口。
- 如果要创建新接口，请点击 + 图标并填写相关字段，如添加 VTI 接口，第 20 页中所述。
- 如果要编辑现有 VTI 的配置，请在**静态虚拟隧道接口 (Static Virtual Tunnel Interface)** 下拉字段中选择 VTI，然后点击**编辑 VTI (Edit VTI)**。

步骤 2 如果您的终端设备位于 NAT 设备后面，请选中 **隧道源 IP 为专用** 复选框。在**隧道源公共 IP 地址 (Tunnel Source Public IP Address)** 字段中，输入隧道源公共 IP 地址。

步骤 3 **将本地身份发送到对等体 (Send Local Identity to Peers)** - 选择此选项可将本地身份信息发送到对等设备。从列表中选择以下**本地身份配置 (Local Identity Configuration)** 之一并配置本地身份：

- **IP 地址 (IP address)** - 对身份使用接口的 IP 地址。
- **自动 (Auto)** - 对预共享密钥使用 IP 地址并对基于证书的连接使用证书 DN。
- **电邮 ID**- 指定要用于身份的邮件 ID。电邮 ID 最多可以包含 127 个字符。
- **主机名 (Hostname)** - 使用完全限定主机名。
- **密钥 ID (Key ID)** - 指定用于身份的密钥 ID。密钥 ID 必须少于 65 个字符。

本地身份用于为每个 IKEv2 隧道配置唯一身份，而不是为所有隧道配置一个全局身份。唯一身份允许 威胁防御 在 NAT 后面有多个 IPsec 隧道，以便连接到 Cisco Umbrella 安全互联网网关 (SIG)。

有关在 Umbrella 上配置唯一隧道 ID 的信息，请参阅 **Cisco Umbrella SIG 用户指南**。

步骤 4 （可选）点击**添加备份 VTI (Add Backup VTI)** 以指定其他 VTI 作为备份接口。

注释 确保两个拓扑对等体均未在同一隧道源上配置备份 VTI。例如，如果对等体 A 的两个 VTI（主和备份）配置了一个隧道源接口，例如 10.10.10.1/30，则对等体 B 的 2 个 VTI 也不能使用一个隧道源 IP，例如 20.20 .20.1/30。

注释 虽然虚拟隧道接口是在备用 VTI 下指定的，但路由配置决定了哪个隧道会被用作主隧道或备用隧道。

可以执行以下操作：

- 要创建新的备份接口，请使用 + 图标。
- 要编辑现有备份 VTI 的配置，请使用**编辑 VTI (Edit VTI)**。

注释 如果设备位于 NAT 设备后面，请选中 **隧道源 IP 为专用** 复选框。在**隧道源公共 IP 地址 (Tunnel Source Public IP Address)** 字段中，输入隧道源公共 IP 地址。

步骤 5 扩展 **高级设置** 并在 **连接类型** 下拉菜单中，选择 **仅应答** 或 **双向**。如果已将 IKE 协议版本选择为 IKEv1，则其中一个节点必须为 **仅应答**。

步骤 6 对于外联网分支，请指定以下参数：

1. 在**设备名称 (Device Name)** 字段中输入设备名称。

2. 在**终端 IP 地址 (Endpoint IP address)**中，输入主 IP 地址。如果要配置备份 VTI，请输入一个逗号，然后指定备份 IP 地址。
3. 点击 **IKE** 选项卡并指定外联网上提供的预共享密钥。

   注释　AWS VPC 会将 **AES-SHA-SHA-LATEST** 作为默认策略。因此，如果远程对等体连接到 AWS VPC，请从**策略 (Policy)** 下拉列表中选择 **AES-SHA-SHA-LATEST** 以建立 VPN 连接，而无需更改 AWS 中的默认值。

步骤 7 重复上述程序以配置其他分支节点。

步骤 8 点击**确定 (OK)**。

下一步做什么

- （可选）为部署指定 **IKE** 选项，如 威胁防御 VPN IKE 选项，第 9 页中所述。
- （可选）为部署指定 **IPsec** 选项，如 威胁防御 VPN IPSec 选项，第 11 页中所述。
- （可选）为部署指定 **高级** 选项，如 威胁防御高级站点到站点 VPN 部署选项，第 13 页中所述。
- 单击**保存**。

通过备用 VTI 隧道路由流量

Cisco Secure Firewall Threat Defense 支持为基于路由的 (VTI) VPN 配置备份隧道。当主 VTI 无法路由流量时，VPN 中的流量会通过备用 VTI 传送。

您可以在以下场景中部署备份 VTI 隧道：

- 两个对等体都有服务提供商冗余备份。

  在这种情况下有两个物理接口，可充当对等体的两个 VTI 的隧道源。

- 只有一个对等体具有服务提供商冗余备份。

  在这种情况下，只有对等体的一端有一个接口备份，而另一端只有一个隧道源接口。

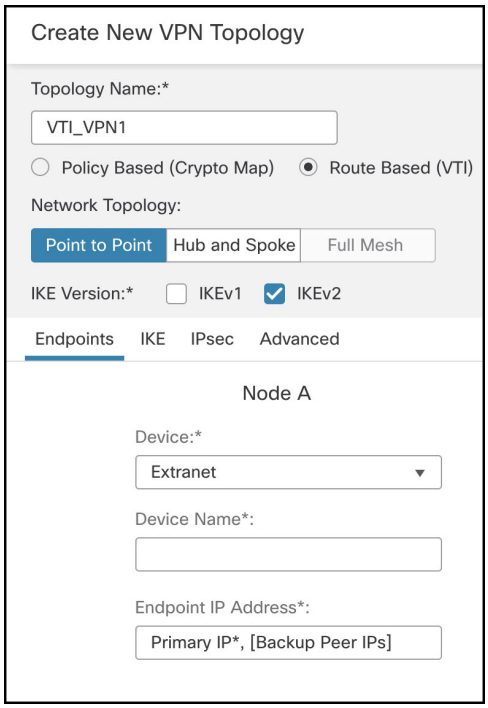
步骤	相应操作	更多信息
1	查看准则和限制。	Virtual Tunnel Interfaces 准则和限制，第 18 页
2	创建 VTI 接口。	添加 VTI 接口，第 20 页
3	在 **创建新 VPN 拓扑向导** 的 **添加终端** 对话框中，点击 **添加备份 VTI**，为每个对等体配置相应的备份接口。	• 为点对点拓扑配置终端，第 22 页 • 为中心辐射型拓扑配置终端，第 24 页

步骤	相应操作	更多信息
4	配置路由策略。	• 依次选择 **设备 > 设备管理**，并且编辑威胁防御设备。 • 点击**路由**。
5	配置访问控制策略。	• 选择 **策略 > 访问控制**。

配置备份 VTI 隧道的准则

- 对于外联网对等体，您可以在托管的对等体上指定备用接口的隧道源 IP 地址并配置隧道目标 IP。

  您可以在 **创建新的 VPN 拓扑** 向导的 **终端 IP 地址** 字段中指定备份对等体 IP 地址。



- 在配置备份接口后，请为路由流量配置路由策略和访问控制策略。

  虽然主 VTI 和备用 VTI 始终可用，但流量只会通过路由策略中配置的隧道来传输。有关详细信息，请参阅为 VTI 配置路由和 AC 策略，第 28 页。

- 配置备份 VTI 时，请确保包含与主 VTI 相同的安全区域的备份隧道。AC 策略页面中的备份 VTI 不需要特定的设置。

- 当为 VPN 配置了备用隧道，请配置具有不同指标的静态路由，以便处理通过备用隧道的流量的故障转移。

为 VTI 配置路由和 AC 策略

在两台设备上配置 VTI 接口和 VTI 隧道后，您必须配置：

- 用于通过 VTI 隧道在设备之间路由 VTI 流量的路由策略。
- 用于允许已加密的流量的访问控制规则。

VTI 的路由配置

对于 VTI 接口，可以配置静态路由或路由协议，例如 BGP。

1. 依次选择 **设备 > 设备管理**，并且编辑 威胁防御 设备。
2. 点击**路由**。
3. 配置静态路由或 BGP。

路由	参数	更多信息
Static Route	• **接口**-选择 VTI 接口。对于备份隧道，请选择备份 VTI 接口。 • **所选网络**-远程对等体的受保护网络。 • **网关**-远程对等体的隧道接口 IP 地址。对于备用隧道，请选择远程对等体的备用隧道接口 IP 地址。 • **指标**-对于备用隧道，请配置不同指标，以便处理通过备用隧道的流量的故障转移。	添加静态路由

路由	参数	更多信息

BGP	• 在 **常规设置** > **BGP** 下启用 BGP，提供本地设备的 AS 编号，并添加路由器 ID（如果您选择手动）。
	• 在 **BGP**下，启用 IPv4/IPv6 并点击 **邻居** 选项卡以配置邻居。
	  • **IP 地址**-远程对等体的 VTI 接口 IP 地址。对于备用隧道，则还要添加具有远程对等体的备用 VTI 接口 IP 地址的邻居。
	  • **远程 AS**-远程对等体的 AS 编号。
	• 点击 **重新分发** 选项卡，将 **源协议** 选择为“已连接”，以便启用连接的路由重新分发。
		配置 BGP

AC 策略规则

将访问控制规则添加到设备上的访问控制策略，以便允许使用以下设置在 VTI 隧道之间加密流量：

1. 通过“允许”操作来创建规则。
2. 选择本地设备的VTI安全区域作为源区域，然后选择远程对等体的VTI安全区域作为目标区域。
3. 选择远程对等体的VTI安全区域作为源区域，然后选择本地设备的VTI安全区域作为目标区域。

有关配置访问控制规则的详细信息，请参阅创建和编辑访问控制规则。

监控站点间 VPN

Cisco Secure Firewall Management Center 提供站点间 VPN 隧道的快照 以便确定站点间 VPN 隧道的状态。您可以查看对等设备之间的隧道列表以及每个隧道的状态：活动、非活动或无活动数据。您可以根据拓扑结构、设备和状态来过滤表中的数据。监控控制面板中的表格会显示实时数据，您可以配置为按指定的时间间隔来刷新数据。该表显示了基于加密映射的VPN的点对点、中心辐射型以及全网状拓扑。隧道信息还包含路由型 VPN 或虚拟隧道接口 (VTI) 的数据。

您可以使用此数据：

- 确定有问题的 VPN 隧道并进行故障排除。
- 验证站点间 VPN 对等设备之间的连接。

- 监控 VPN 隧道的运行状况，以便在站点间提供不间断的 VPN 连接。

有关配置基于加密映射的站点间 VPN 的信息，请参阅配置策略型站点间 VPN，第 5 页。

有关 VTI 的信息，请参阅 关于 Virtual Tunnel Interface，第 16 页。

有关 威胁防御 VPN 监控和故障排除的信息，请参阅VPN 监控和故障排除。

准则和限制

- 该表会显示已部署的站点间VPN 的列表。它不会显示已创建但未部署的隧道。
- 该表不会显示有关基于策略的 VPN 和备份 VTI 的备份隧道的信息。
- 对于集群部署，该表不会显示实时数据中的导向器更改。它只会显示部署VPN时存在的导向器信息。只有在更改后重新部署了隧道 AM，导向器更改才会在表中体现出来。

站点间 VPN 监控控制面板

站点间 VPN 监控控制面板显示站点间 VPN 隧道的以下构件：

- **隧道状态表 (Tunnel Status Table)** - 列出使用 管理中心 配置的站点间 VPN 的表
- **隧道状态分布图 (Tunnel Status Distribution Chart)** - 以环状图来显示隧道的聚合状态。
- **拓扑摘要列表**- 按拓扑来汇总的隧道状态。

VPN 隧道的状态

站点间监控控制面板会列出以下状态的 VPN 隧道：

- **非活动 (Inactive)** - 如果所有 IPSec 隧道都关闭，则策略型（基于加密映射）的 VPN 隧道将处于非活动状态。如果 VTI 或 隧道遇到任何配置或连接问题，则该隧道将关闭。
- **活动 (Active)** - 在 管理中心 中，站点间 VPN 是根据分配给 VPN 拓扑的 IKE 策略和 IPsec 建议来配置的。如果 管理中心 在部署后通过隧道识别出需要关注的流量，则策略型 VPN 隧道将处于活动状态。只有当至少有一个 IPsec 隧道正常运行时，IKE 隧道才会正常运行。

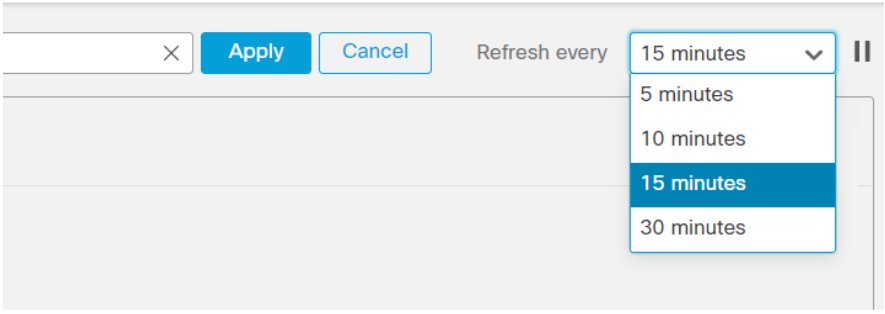
  路由型 VPN (VTI) 隧道不需要所关注的流量处于活动状态。如果它们的配置和部署没有错误，则它们将处于活动状态。
- **无活动数据 (No Active Data)** - 策略型 VPN 隧道会保持“无活动数据”(No Active Data) 状态，直到第一次有流量事件通过隧道。“无活动数据”(No Active Data) 状态还会列出已部署但出错的策略型和路由型 VPN。

自动数据刷新

表中的站点间 VPN 数据会定期刷新。您可以配置为以特定间隔刷新 VPN 监控数据，或者关闭自动数据刷新。

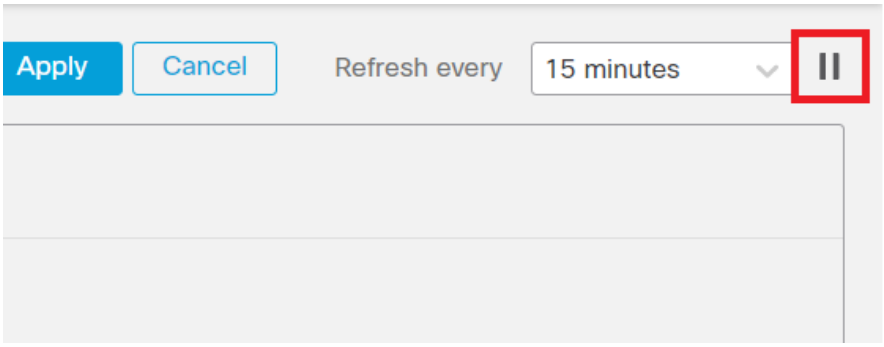
点击**刷新 (Refresh)** 间隔下拉列表，从可用的间隔时间中选择以刷新表中的数据。

图 *1:* 刷新隧道数据



点击**暂停 (Pause)** 可根据需要停止自动数据刷新。您可以点击同一按钮继续刷新隧道数据。

图 *2:* 暂停定期数据刷新



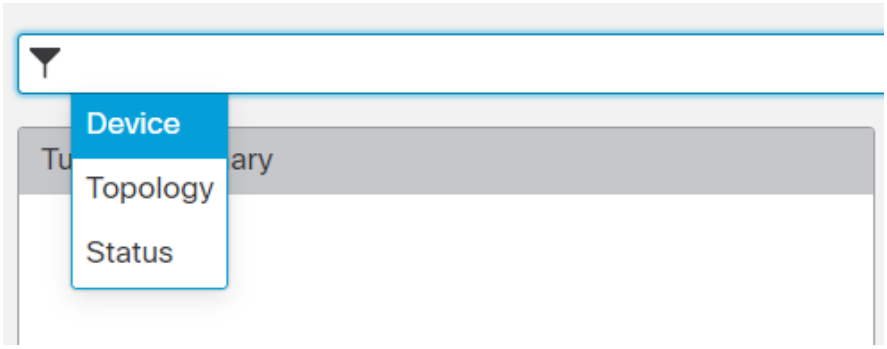
对站点间 VPN 监控数据进行过滤和排序

您可以按拓扑、设备和状态来过滤和查看 VPN 监控表中的数据。

例如，您可以查看特定拓扑中处于关闭状态的隧道。

在过滤器框中点击选择过滤条件，然后指定要过滤的值。

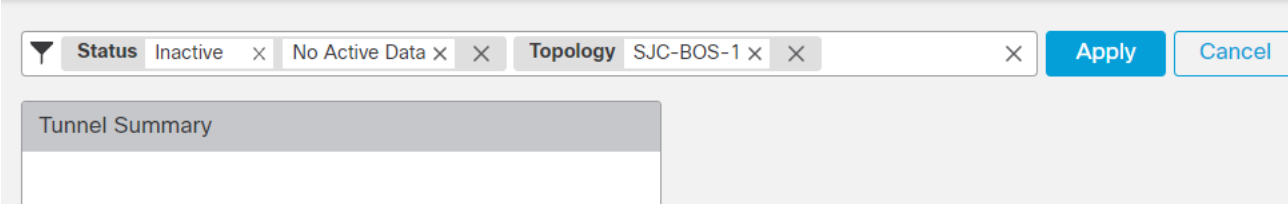
图 *3:* 过滤隧道数据



您可以根据需要使用多个过滤条件来查看数据。

例如，您可以选择只查看处于“开启”(Up) 和“关闭”(Down) 状态的隧道，并忽略处于“未知”(Unknown) 状态的隧道。

图 4: 示例：过滤隧道数据



排序数据 (Sort the data) - 要按列对数据进行排序，请点击列标题。

相关主题

关于站点间 VPN，第 1 页
关于 Virtual Tunnel Interface，第 16 页

站点间 VPN 的历史记录

特性	Version	详细信息
IPsec 流分流	7.2	在 Secure Firewall 3100上，默认情况下会分流 IPsec 流。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)，这应该会提高设备性能。 您可以使用 FlexConfig 和 **flow-offload-ipsec** 命令更改配置。
站点间 VPN 过滤器	7.1	添加了控制策略，以控制站点间 VPN 流量。
本地隧道 ID 支持	7.1	对于站点间 VPN 上的每个终端，您可以配置要与对等体共享的唯一隧道 ID。
多 IKE 策略支持	7.1	您可以为每个终端添加多个 IKEv1 和 IKEv2 策略对象。
站点间 VPN 监控控制面板	7.1	使用站点间 VPN 监控控制面板，查看和监控站点间 VPN 隧道的状态。
备份基于路由的站点间 VPN 的虚拟隧道接口 (VTI) 。	7.0	配置使用虚拟隧道接口的站点间 VPN 时，可以为隧道选择备份 VTI。指定备用 VTI 可提供恢复能力，以便在主连接断开时，备用连接可能仍能正常工作。例如，可以将主 VTI 指向一个服务提供商的终端，将备用 VTI 指向其他服务提供商的终端。 通过选择基于路由作为点对点连接的 VPN 类型，您可以在站点间 VPN 向导中添加备份 VTI。
将 VTI 数量从每个接口 100 个增加到每个设备 1024 个	7.0	支持的最大 VTI 数量从每个物理接口 100 个增强到每个设备 1024 个 VTI。

特性	Version	详细信息
IPv6 支持	7.0	您可以配置 IPv6 寻址的 VTI。虽然仅支持静态 IPv6 地址作为隧道源和目的地址，但不支持 VTI 上的 IPv6 BGP。
删除和弃用弱密码	6.7	已删除对不太安全的密码的支持。我们建议您在升级到 威胁防御 6.70 以支持 DH 和加密算法之前更新 VPN 配置，以确保 VPN 正常工作。 更新 IKE 提议和 IPSec 策略以匹配 威胁防御 6.70 中支持的策略，然后再部署配置更改。 从 威胁防御 6.70 开始，以下安全性较低的密码已被删除或弃用： • 已弃用 IKEv1 的 **Diffie-Hellman GROUP 5**，并已为 IKEv2 将其删除 • Diffie-Hellman 组 2 和 24 已被删除。 • **加密算法**：3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256 已被删除。 **注释** 在评估模式下或对不满足强加密导出控制要求的用户继续支持**DES** 。 **NULL** 在 IKEv2 策略中已已删除，但在 IKEv1 和 IKEv2 IPsec 转换集中仍支持。
动态 RRI 支持	6.7	基于 IKEv2 的静态加密映射支持动态反向路由。
面向站点间 VPN 的备用对等体	6.6	您可以使用 管理中心 将备份对等体添加到站点间 VPN 连接。例如，如果您有两个 ISP，则可以将 VPN 连接配置为故障转移到备用 ISP（如果与第一个 ISP 的连接不可用）。

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。