VPN 概述

虚拟专用网络 (VPN) 连接在使用公共网络（如互联网）的终端之间建立安全隧道。

本章适用于 Cisco Secure Firewall Threat Defense 设备上的 远程访问和 站点到站点 VPN。它描述了互联网协议安全 (IPsec)、互联网安全关联和密钥管理协议（ISAKMP 或 IKE）以及用于构建站点到站点 和远程接入 VPN 的 SSL 标准。

VPN 类型

管理中心 支持以下几种类型的 VPN 配置：

- 威胁防御设备上的远程接入 VPN。

  远程接入 VPN 是远程用户和您公司的专用网络之间的安全、加密连接或隧道。连接由 VPN 终端设备组成，该设备是具有VPN客户端功能的工作站或移动设备，以及在企业专用网络边缘的 VPN 前端设备或安全网关。

  Cisco Secure Firewall Threat Defense设备可以配置为通过 管理中心支持 SSL 或 IPsec IKEv2 上的远程接入 VPN。它们作为此功能中的安全网关，将对远程用户进行身份验证、授权访问以及加密数据，以提供与网络的安全连接。由 管理中心管理的其他任何类型的设备都不支持远程接入 VPN 连接。

  Cisco Secure Firewall Threat Defense安全网关支持 AnyConnect 安全移动客户端完整隧道客户端。为远程用户提供安全的 SSL IPsec IKEv2 连接需要此客户端。此客户端为远程用户提供了客户端所带来的好处，而不需要网络管理员在远程计算机上安装和配置客户端，因为它可以在连接时部署到客户端平台。它是终端设备上唯一受支持的客户端。

- 威胁防御设备上的站点到站点 VPN

  站点到站点VPN可连接不同地理位置的网络。您可以在受管设备之间以及受管设备与其他符合所有相关标准的思科或第三方对等体之间创建站点到站点的IPsec连接。这些对等体可以采用内部和外部 IPv4 和 IPv6 地址的任意组合。站点到站点隧道使用 Internet Protocol Security (IPsec) 协议套件和 IKEv1 或 IKEv2 构建。建立 VPN 连接之后，本地网关后台的主机可通过安全 VPN 隧道连接至远程网关后台的主机。

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 IKE 策略。IKEv1 和 IKEv2 最多分别支持 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。

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。
- 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。如果生命周期不相同，则应用远程对等体策略中较短的生命周期。默认情况下，Cisco Secure Firewall Management Center会为所有 VPN 终端部署优先级最低的 IKEv1 策略，以确保成功协商。

IPSec

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 隧道的流量由安全协议和算法组合保护。

Ipsec 提议策略定义 IPsec 隧道所需的设置。Ipsec 提议是应用于设备上 VPN 接口的一个或多个加密映射的集合。加密映射整合了设置 IPsec 安全关联所需的所有元素，包括：

- 提议（或转换集）是确保 IPsec 隧道中流量安全的安全协议和算法的组合。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体上相同的提议。找到后，提议将用于创建一个 SA，以保护该加密映射的访问列表中的数据流，从而保护 VPN 中的流量。IKEv1 和 IKEv2 有单独的 Ipsec 提议。在 IKEv1 提议（或转换集）中，对于每个参数都设置一个值。对于 IKEv2 提议，您可以为单个提议配置多个加密和集成算法。
- 加密映射整合了设置 Ipsec 安全关联 (SA) 所需的所有元素，包括 IPsec 规则、提议、远程对等体以及定义 IPsec SA 所需的其他参数。当两个对等体尝试建立 SA 时，必须至少有一个兼容的加密映射项。

当未知的远程对等体尝试启动与本地中心的 IPsec 安全关联时，站点到站点 VPN 中将使用动态加密映射策略。中心不能是安全关联协商的发起者。动态加密策略允许远程对等体与本地中心交换 Ipsec 流量，即使中心不知道远程对等体的身份。动态加密映射策略实质上创建了一个没有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。要应用动态加密映射策略，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。请注意，在全网格 VPN 拓扑中，只能应用静态加密映射策略。

注释 对于 Firepower 威胁防御 (FTD) 上的远程访问和站点间 VPN，同一接口不支持同时使用 IKEv2 动态加密映射。

VPN 数据包流

在威胁防御设备上，默认情况下，不允许任何流量没有显式权限而通过访问控制。VPN 隧道流量也不会中继到终端，直到它通过 Snort 为止。传入隧道数据包经过解码后才发送到 Snort 进程。Snort 在加密前将处理传出数据包。

识别 VPN 隧道每个终端节点的受保护网络的访问控制可以确定允许通过 威胁防御设备并访问终端的流量。对于远程接入 VPN 流量，必须将组策略过滤器或访问控制规则配置为允许 VPN 流量。

此外，在隧道关闭时，系统不向公共资源发送隧道流量。

IPsec 流分流

您可以将支持的设备型号配置为使用 IPsec 数据流分流。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。

分流操作特别涉及入口上的预解密和解密处理，以及出口上的预加密和加密处理。系统软件处理内部流以应用安全策略。

默认情况下启用 IPsec 数据流分流，并应用于以下设备类型：

- Secure Firewall 3100

IPsec 流分流的限制

不分流以下 IPsec 流：

- IKEv1 隧道。仅 IKEv2 隧道将被分流。IKEv2 支持更强的密码。
- 配置了基于卷的密钥更新的流。

- 已配置压缩的流。
- 传输模式流。仅会分流隧道模式流。
- AH 格式。仅支持 ESP/NAT-T 格式。
- 已配置后分段的流。
- 防重放窗口大小不是 64 位且防重放的流不会被禁用。
- 已启用防火墙过滤器的流。

配置 IPsec 数据流分流

默认情况下，在支持该功能的硬件平台上启用 IPsec 数据流分流。要更改配置，请使用 FlexConfig 实施 **flow-offload-ipsec** 命令。有关命令的详细信息，请参阅 ASA 命令参考。

VPN 许可

没有用于启用 Cisco Secure Firewall Threat Defense VPN 的特定许可，该 VPN 默认情况下是可用的。

管理中心根据智能许可服务器提供的属性，确定是允许还是阻止在 威胁防御 设备上使用强加密。

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。

如果你用评估许可证创建了你的VPN配置，并将你的许可证从评估许可证升级为具有出口控制功能的智能许可证，请检查并更新你的加密算法，以加强加密，使 VPN 正常工作。不再支持基于 DES 的加密。

VPN 连接应具有多高的安全性？

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。可以使用 IKE 策略和 IPsec 提议定义要应用的加密和其他安全技术。

如果您的设备许可证允许应用较强的加密，则有大量的加密和散列算法以及Diffie-Hellman组供您选择。然而，通常情况下，应用于隧道的加密越强，系统性能越差。您要在安全性和性能之间实现平衡，在提供充分保护的同时不牺牲效率。

我们无法就选择哪些选项提供具体指导。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。

下面的主题介绍了几个可用选项。

遵守安全认证要求

许多VPN设置都有允许您遵守各种安全认证标准的选项。查看您的认证要求和可用选项以规划VPN配置。

决定使用哪个加密算法

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，可以从以下加密算法中选择。如果不符合强加密要求，则只能选择 DES。

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账户注册，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。

- AES-GCM - （仅 IKEv2。）Galois/Counter 模式中的高级加密标准是提供机密性和数据源身份验证的分组加密操作模式，并且提供比 AES 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。密钥越长，其提供的安全性就越高，但性能会随之降低。GCM 是支持 NSA Suite B 所需的 AES 模式。NSA Suite B 是一套加密算法，设备必须支持这套算法才能满足密码强度的联邦标准。.
- 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。密钥越长，其提供的安全性就越高，但性能会随之降低。
- 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。如果您的许可证账户不符合导出控制要求，这将是您唯一的选择。
- Null、ESP-Null - 不使用加密。空加密算法提供不加密的身份验证。这通常仅用于测试目的。但是，它在许多平台上根本不起作用，包括虚拟和 Firepower 2100。

决定使用哪些散列算法

在 IKE 策略中，散列算法创建消息摘要，用于确保消息的完整性。在 IKEv2 中，散列算法分成两个选项，一个用于完整性算法，一个用于伪随机函数 (PRF)。

在 IPsec 提议中，散列算法由封装安全协议 (ESP) 用于身份验证。在 IKEv2 IPsec 提议中，这称为完整性散列。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀，并且还有 -HMAC 后缀（代表“散列方法身份验证代码”）。

对于 IKEv2，您可以配置多个散列算法。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。

您可以选择以下散列算法：

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

以下 SHA-2 选项更加安全，可用于 IKEv2 配置。如果要实施 NSA Suite B 加密规范，请选择以下选项之一。

- 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。）空散列算法；这通常仅用于测试目的。但是，如果选择 AES-GCM 选项之一作为加密算法，则应选择空完整性算法。即使选择非空选项，这些加密标准也会忽略完整性散列。

决定要使用的 Diffie-Hellman 模数组

您可以使用以下 Diffie-Hellman 密钥导出算法生成 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，但需要的处理时间更长。两个对等体上必须具有一个匹配的模数组。

如果选择 AES 加密，要支持 AES 所需的大型密钥长度，应使用 Diffie-Hellman (DH) 组 5 或更高组。IKEv1 策略不支持下面列出的所有组。

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少遭受 Logjam 等攻击。

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，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。

- 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。

确定使用哪种身份验证方法

VPN 可用的身份验证方法是预共享密钥和数字证书。

站点到站点、IKEv1 和 IKEv2 VPN 连接都可以使用这两种方法。

仅使用 SSL 和 IPsec IKEv2 的远程访问仅支持数字证书身份验证。

在身份验证阶段，预共享密钥允许密钥在两个对等体之间共享并由 IKE 使用。必须在每个对等体上配置相同的共享密钥，否则无法建立 IKE SA。

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。证书规定两个对等体之间通信的不可否认性，这意味着可以证明通信已实际发生。使用此身份验证方法时，您需要定义一个公共密钥基础设施 (PKI)，以便对等体可以从证书颁发机构 (CA) 获得数字证书。CA 管理证书请求并向参与网络设备颁发证书，从而为所有参与设备提供集中密钥管理。

预共享密钥不能很好地扩展，使用 CA 可以提高 IPsec 网络的易管理性和可扩展性。使用 CA，不需要在所有加密设备之间配置密钥。相反，每个参与设备都向 CA 注册，并从 CA 请求证书。每个具有其自己的证书和 CA 公共密钥的设备都可以在给定 CA 的域内为其他各个设备进行身份验证。

预共享密钥

预共享密钥使您能够在两个对等体之间共享密钥。 IKE 在身份验证阶段使用此密钥。必须在每个对等体上配置相同的共享密钥，否则无法建立 IKE SA。

要配置预共享密钥，请选择是使用手动还是自动生成的密钥，然后指定IKEv1/IKEv2选项中的密钥。然后，在部署配置时，将在拓扑中的所有设备上配置该密钥。

PKI 基础设施和数字证书

公共密钥基础架构

PKI 为参与的网络设备提供集中密钥管理。它是一组定义的策略、程序和角色，通过生成、验证和撤销公钥证书（通常称为数字证书）支持公钥加密。

在公钥加密中，连接的每个终端均具有包含公钥和私钥的密钥对。密钥对被VPN终端用于消息签名和加密。这对密钥相互补充，用其中一个密钥加密的任何内容都可用另一个密钥解密，保证了连接上数据流的安全性。

生成一个用于签名和加密的通用RSA、ECDSA或EDDSA密钥对，也可以为每种用途生成单独的密钥对。单独的签名和加密密钥有助于降低泄露密钥的风险。SSL 使用密钥进行加密而非签名，但是，IKE 使用密钥进行签名而非加密。通过为每种用途使用单独的密钥，泄露密钥的风险降至最低。

数字证书或标识证书

当将数字证书用作 VPN 连接的身份验证方法时，系统将对等体配置为从证书颁发机构 (CA) 获取数字证书。CA 是“签署”证书以验证其真实性，从而确保设备或用户的身份的可信颁发机构。

作为公共密钥基础设施 (PKI) 的一部分，CA 服务器会管理公共 CA 证书请求并为参与的网络设备颁发证书，此活动称为证书注册。这些数字证书（又称为身份证书）包含：

- 所有者用于身份验证的数字识别信息，例如名称、序列号、公司、部门或 IP 地址。
- 向证书所有者发送和从证书所有者接收加密数据所需要的公钥。
- CA 的安全数字签名。

此外，证书还规定两个对等体之间通信的不可否认性，这意味着它们可以证明通信已实际发生。

证书注册

使用PKI可提高VPN的可管理性和可扩展性，因为您无需配置所有加密设备之间的预共享密钥。您需使用 CA 服务器单独注册每个参与设备，该 CA 服务器明确受信任进行设备身份验证和身份证书的创建。完成注册后，每个参与的对等体将其身份证书发送给另一个对等体，以使用证书中包含的公钥验证身份并建立加密会话。有关注册 威胁防御设备的详细信息，请参阅证书注册对象。

证书颁发机构证书

为了验证对等体的证书，每个参与设备都必须从服务器检索CA证书。CA证书用于签署其他证书。它是自签名证书，也称为根证书。此证书包含CA的公钥，用于解密和验证收到的对等体证书的CA数字签名和内容。CA 证书可通过以下方式获得：

- 使用简单证书注册协议（SCEP） 或安全传输注册（EST） 从 CA 服务器检索 CA 的证书
- 从另一个参与的设备手动复制 CA 证书

信任点

完成注册后，会在受管设备上创建信任点。它是 CA 及关联证书的对象代表。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。

PKCS#12 文件

PKCS#12或PFX文件将服务器证书、任何中间证书和私钥保存在一个加密文件中。这种类型的文件可以直接导入到设备中以创建信任点。

撤销检查

CA 还可以为不再参与网络的对等体撤销证书。撤销的证书由联机证书状态协议 (OCSP) 服务器管理，或在存储于 LDAP 服务器上的证书撤销列表 (CRL) 中列出。对等体可以在从其他对等体接受证书之前对证书进行检查。

删除或弃用的散列算法、加密算法和Diffie-Hellman模数组

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 和 IKEv2 的 **Diffie-Hellman GROUP 5** 。
- 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。

VPN 拓扑选项

在创建新的VPN拓扑时，您必须至少为其提供唯一名称，指定拓扑类型，然后选择IKE版本。您可以从三种拓扑类型中进行选择，每种类型都包括一组 VPN 隧道。

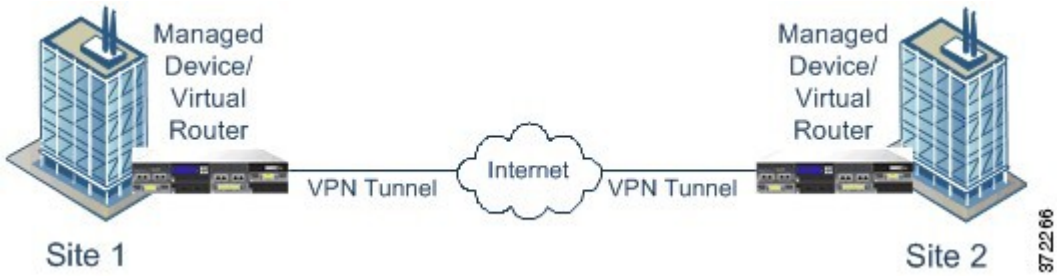
- 点到点 (PTP) 拓扑会在两个终端之间建立 VPN 隧道。
- 中心辐射型拓扑会建立一组 VPN 隧道，将中心终端连接到一组分支终端。
- 全网状拓扑会在一组终端之间建立一组 VPN 隧道。

手动或自动为 VPN 身份验证定义预共享密钥，没有默认密钥。如果选择自动，Cisco Secure Firewall Management Center会生成预共享密钥并将其分配给拓扑中的所有节点。

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。

下图显示了典型的点对点 VPN 拓扑。

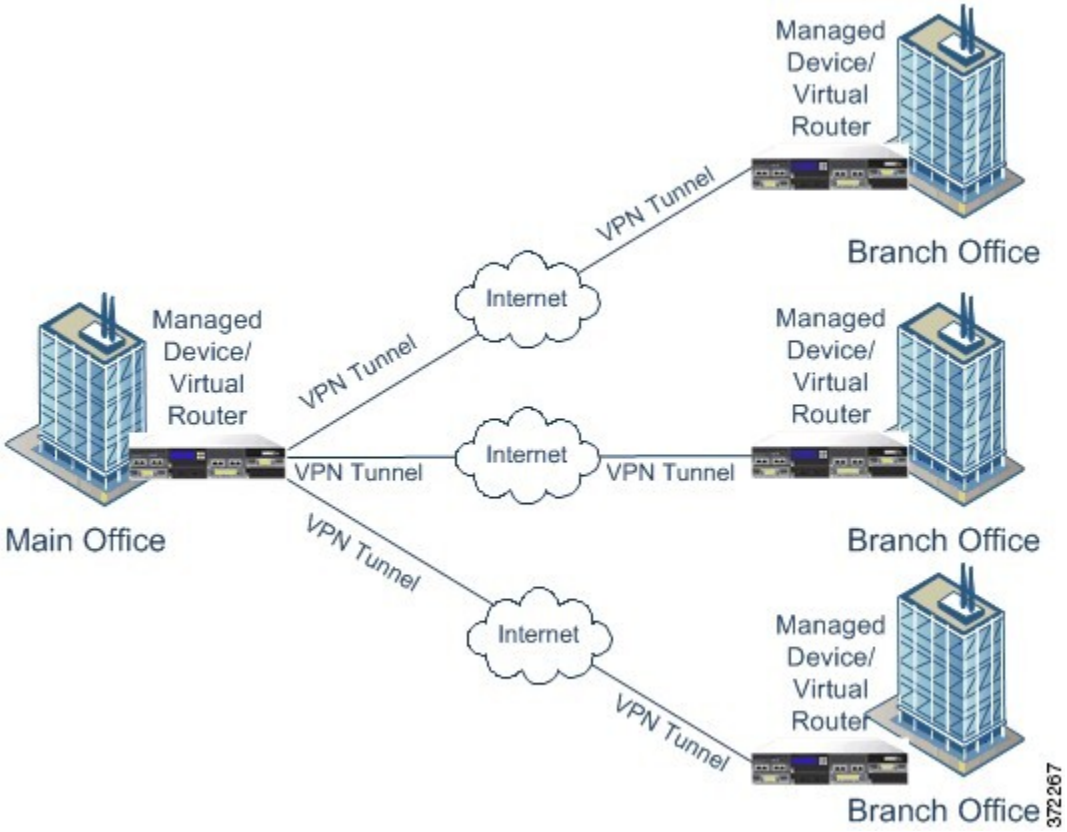


集中星型 VPN 拓扑

在集中星型VPN拓扑中，中心终端（集线器节点）与多个远程终端（辐射节点）连接。集线器节点与每个辐射终端之间的每条连接均为独立VPN隧道。任何辐射节点后台的主机均可通过集线器节点相互通信。

集中星型拓扑通常代表通过互联网或其他第三方网络建立安全连接，将公司总部和分公司相连的VPN。这些部署为所有员工提供对公司网络的受控访问权。通常，集线器节点位于总部。辐射节点位于分支机构并启动大部分流量。

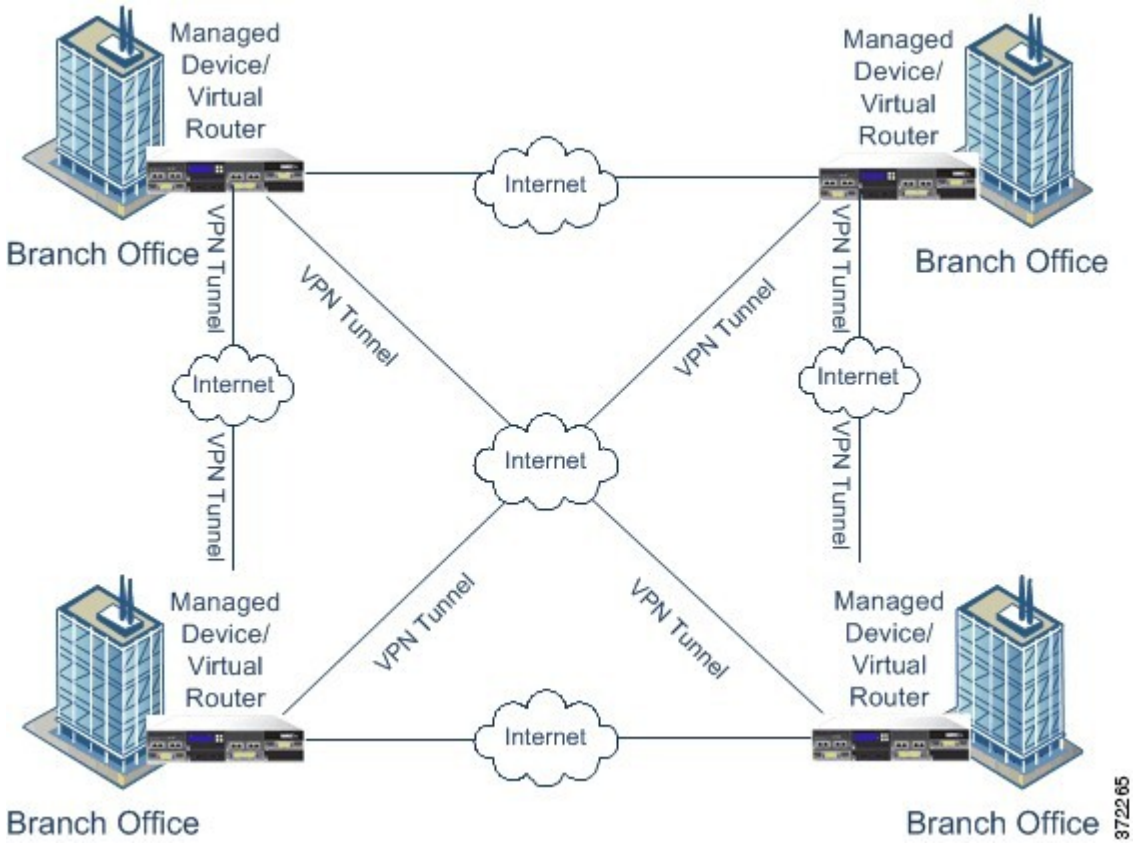
下图显示了典型的集中星型 VPN 拓扑。



全网状 VPN 拓扑

在全网状 VPN 部署中，所有终端均可通过单个 VPN 隧道与每个其他终端进行通信。这种拓扑可提供冗余，以便在某个终端出现故障时，其他终端仍然能够相互通信。它通常代表连接一组分散式分公司地点的 VPN。在此配置中，所部署的支持 VPN 的受管设备数量取决于所需的冗余级别。

以下图表显示了典型的全网状 VPN 拓扑。



隐式拓扑

除了三种主要的VPN拓扑以外，还可通过这些拓扑的组合形式创建其他更复杂的拓扑。具体包括：

- 部分网状结构 - 一种网络结构，其中部分设备按照全网状拓扑加以组织，而其他设备则形成中心辐射型结构，或与某些全网状设备的点对点连接。部分网状结构不能提供全网状拓扑那样的冗余度，但其实施成本相对较低。部分网状拓扑用于连接到全网状主干的外围网络。
- 分层中心辐射型结构 - 一种中心辐射型拓扑网络结构，其中某一设备可在一种或多种拓扑中作为中心设备，而在其他拓扑中作为辐射设备。允许从辐射组到其最直接中心的流量。
- 联合中心辐射型结构 - 两种连接起来形成点对点隧道的拓扑的组合（中心辐射型、点对点或全网状）。例如，联合中心辐射型拓扑可能包含两种中心辐射型拓扑，它们的中心充当点对点拓扑中的对等设备。

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。