安全连接概览

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 站点间 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）以及用于构建站点间 和远程访问 VPN 的 SSL 标准。

- VPN 类型， 第 1 页
- VPN 基础知识， 第 2 页
- VPN 数据包流， 第 5 页
- IPsec 流分流， 第 5 页
- VPN 许可， 第 6 页
- VPN 加密与性能， 第 6 页
- 已弃用的哈希算法、加密算法和 Diffie-Hellman 模数组， 第 11 页
- VPN 拓扑， 第 12 页

VPN 类型

VPN 类型是一种网络连接类别，

- 在远程位置和专用网络之间提供安全、加密的连接
- 支持部署模式，包括远程访问和站点到站点配置，以及
- 使用各种协议（包括 SSL 和 IPsec）建立安全隧道。

支持的 VPN 连接类型

防火墙管理中心 支持这些类型的 VPN 配置：

- Firewall Threat Defense 设备上的远程接入 VPN。

  远程接入VPN提供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。这些连接使用两种设备：一种是 VPN 终端设备，它具有 VPN 客户端功能的工作站或移动设备；一种是位于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 防火墙管理中心支持 SSL 或 IPsec IKEv2 上的远程接入 VPN。这些设备作为安全网关，可以验证远程用户身份、授权访问并加密数据，从而为您的网络提供安全连接。仅这些设备支持由 防火墙管理中心 管理的远程访问 VPN 连接。

Cisco Secure Firewall Threat Defense安全网关支持 安全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。在建立连接后，系统会自动安装此客户端，因此网络管理员无需在远程计算机上手动安装或配置此客户端。它是终端设备上唯一受支持的客户端。

- Firewall Threat Defense 设备上的站点间 VPN。

  站点间VPN可连接不同地理位置的网络。您可以在托管设备之间以及托管设备与其他思科或第三方对等体之间创建站点间的 IPsec 连接。这些对等体可以使用 IPv4 和 IPv6 地址。站点间隧道使用 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

VPN 是一种安全的网络技术，

- 利用隧道技术在公共TCP/IP网络（如互联网）上建立远程用户与企业专用网络之间的安全连接
- 采用基于 IPsec 的技术（符合 ISAKMP [IKE] 和 IPsec 隧道标准）来构建和管理隧道，并
- 通过封装和解封装数据包的隧道端点实现双向数据传输。

VPN 隧道管理功能

ISAKMP 和 IPsec 实现以下隧道管理功能：

- 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。

VPN 部署使用两种主要设备类型：

- 中心：实现与一个或多个远程分支设备或分支之间的安全VPN连接的设备。中心还充当分支相互通信的网关。
- 分支：通过VPN连接到中心设备，以安全访问中心设备背后的企业资源的设备。分支通过中心相互通信。

互联网密钥交换 (IKE)

互联网密钥交换 (IKE) 是一种关键管理协议，可以

- 对 IPsec 对等体进行身份验证
- 协商并分发 IPsec 加密密钥，并且
- 自动建立 IPsec 安全关联 (SA)。

IKE 协商阶段和政策

IKE 协商包括两个阶段：

- 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。

每个阶段都使用提议来协商连接。

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。当每个对等体同意一个共同的 IKE 策略时，IKE 协商开始。此策略定义了保护后续 IKE 协商的安全参数。IKEv1 策略包含一组算法和一个模数组。在 IKEv2 策略中，您可以选择多个算法和模数组供对等体在第一阶段协商期间选择。您可以创建单个 IKE 策略，或创建多个策略以优先考虑首选选项。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。较低的优先级数字表示较高的策略优先级。

要定义 IKE 策略，请指定：

- 唯一的优先级（1 到 65,543，1 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。
- 一种散列消息身份验证代码 (HMAC) 方法（在 IKEv2 中称为完整性算法），用于验证发送方的身份，并确认消息在传输过程中未被更改。
- 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，用于确定加密密钥确定算法的强度。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，发起对等体将其所有策略发送到远程对等体。远程对等体按优先级顺序搜索与其自身策略的匹配项。如果两个对等体使用相同的加密、散列（IKEv2 中的完整性和 PRF）、身份验证和 Diffie-Hellman 值，则 IKE 策略匹配。SA 生存期必须小于或等于发送的策略中的生存期。如果生存期不完全相同，则采用远程对等体策略中的较短值。默认情况下，为确保所有VPN终端协商成功，Secure Firewall Management Center 会为所有 VPN 终端部署具有最低优先级的 IKEv1 策略。

IPSec

IPsec 是一种用于设置 VPN 的安全方法：

- 提供 IP 数据包级别的数据加密，
- 通过隧道在公共网络上传输数据，隧道是两个对等体之间安全的逻辑通信路径，并且
- 通过安全协议和算法的组合来保护进入 IPsec 隧道的流量。

使用 IPsec，数据通过隧道在公共网络上传输。

IPsec 提议策略组件

IPsec 提议策略定义了 IPsec 隧道的设置。IPsec 提议包含一个或多个加密映射，这些映射应用于设备中的 VPN 接口。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）结合了安全协议和算法，以保护 IPsec 隧道中的流量。在 IPsec 安全关联 (SA) 协商过程中，对等方会寻找匹配的提议。应用所选的提议以创建安全关联 (SA)，保护加密映射访问列表中的数据流并确保 VPN 流量的安全。IKEv1 和 IKEv2 有单独的 Ipsec 提议。在 IKEv1 提议（或转换集）中，每个参数都需要设置一个值。在 IKEv2 提议中，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，站点间 VPN 中将使用动态加密映射策略。中心不会发起安全关联协商。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。动态加密映射策略会在配置所有参数之前创建加密映射条目。IPsec 协商随后动态配置缺失的参数，以满足远程对等方的要求。

  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。在全网格 VPN 拓扑中，只能应用静态加密映射策略。

注释 对于 Firewall Threat Defense 设备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

VPN 数据包流是一个安全过程，

- 在允许流量通过之前，需要通过访问控制获得明确的权限，
- 在将传入的隧道数据包发送到 Snort 进程之前对其进行解密。
- 在加密之前，通过 Snort 处理传出的数据包，并且
- 隧道关闭时，阻断通往公共水源的隧道交通。

访问控制要求

访问控制识别 VPN 隧道中每个终端节点的受保护网络，并确定哪些流量允许通过 Firewall Threat Defense 设备并到达终端。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。

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。Cisco Secure Firewall 6100 系列中，IPsec 连接卸载至 Kintex 7 (KC400) FPGA。该 FPGA 内置加密引擎，支持 AES-GCM-128 和 AES-GCM-256 加解密。

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
- Cisco Secure Firewall 4200
- Cisco Secure Firewall 6100

启用设备的 VTI 环回接口时，也会使用 IPsec 数据流分流。

对于集群分布式站点间 VPN 模式中的不对称流量，IPsec 流分流可让流量所有者在硬件中解密通过集群控制链路转发的 IPsec 流量。此功能不可配置，且在启用 IPsec 流卸载时始终可用。

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。

VPN 许可

您不需要特定的许可证即可在 Firewall Threat Defense 设备上启用 VPN，该功能默认可用。

防火墙管理中心会根据设备中的出口管制功能来决定允许还是阻止在 Firewall Threat Defense 设备中使用强加密。在注册思科智能软件管理器时，可启用此功能。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。选择 **管理** > **许可证** > **智能许可证** 以便在 防火墙管理中心 中验证此功能。

如果您使用评估许可证创建了VPN配置，后来将许可证升级为具有出口管制功能的智能许可证，请检查并更新您的加密算法以使用更强的加密，确保 VPN 正常运行。请勿使用基于 DES 的加密，因为它不受支持。

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。

符合安全认证要求

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

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 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。

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。

决定 VPN 身份验证方法

VPN 身份验证方法是一种安全机制，它会

- 验证 VPN 连接中对等体的身份
- 实现网络设备之间的安全通信，并且
- 确保只有授权的设备才能建立 VPN 连接。

可用的身份验证方法

VPN 支持两种主要的身份验证方法：

- **预共享密钥**：在对等体之间共享的密钥，由 IKE 在身份验证阶段使用。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。证书提供两个对等体之间通信的证明。

VPN 类型支持因身份验证方法而异。

表 *1: VPN* 身份验证方法支持

VPN 类型	**预共享密钥**	**数字证书**
站点到站点 IKEv1 和 IKEv2	支持	支持
远程访问（SSL 和 IPsec IKEv2）	不支持	支持

使用数字证书身份验证时，您需要为对等体定义公钥基础设施 (PKI)，以便从证书颁发机构 (CA) 获取数字证书。CA 管理证书请求并向参与的网络设备颁发证书，从而为所有参与设备提供集中式密钥管理。

预共享密钥难以在大型网络中管理。CA 使管理和扩展 IPsec 网络更加容易。使用 CA，不需要在所有加密设备之间配置密钥。向 CA 注册每个设备以请求其证书。拥有自己的证书和 CA 公钥的设备可以验证 CA 域内其他设备。

预共享密钥

预共享密钥是一种密钥，

- 使您可以在两个对等体之间共享身份验证凭证
- 由 IKE 在身份验证阶段使用，以及
- 必须在每个对等体上进行完全相同的配置，否则无法建立 IKE SA。

密钥配置选项

要配置预共享密钥，请选择手动密钥或自动生成的密钥。在 IKEv1 或 IKEv2 选项中指定此密钥。在部署配置时，将在拓扑中的所有设备上配置该密钥。

PKI 基础设施与数字证书

PKI 基础设施是一种集中式密钥管理系统，

- 提供已定义的策略、流程和角色，以支持公钥密码学
- 生成、验证和撤销公钥证书（通常称为数字证书），以及
- 管理由 VPN 端点公钥和私钥组成的密钥对，用于对消息进行签名和加密。

公钥密码学与证书组件

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。

生成通用的RSA、ECDSA或EDDSA密钥对，用于签名和加密。或者，为每种用途分别生成独立的密钥对。独立的签名密钥和加密密钥有助于降低密钥泄露风险。SSL 使用密钥进行加密，而 IKE 使用密钥进行签名。每种用途使用独立的密钥可最大限度地减少暴露风险。

证书还能通过提供两个对等体之间发生过通信的证明来确保不可否认性。

您可以通过以下方式获取 CA 证书：

- 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

信任点是CA及其关联证书的对象表示。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。

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。

数字证书或身份证书

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。

数字证书包含以下组件：

- 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。

证书注册流程包括以下步骤：

1. 作为 PKI 的一部分，CA 服务器管理公共 CA 证书请求，并为参与的网络设备颁发证书。
2. 每个参与设备需使用 CA 服务器单独注册，该服务器负责验证身份并创建设备的身份证书。
3. 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。

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。您只需使用 CA 服务器注册每个参与设备，该服务器负责验证身份并创建设备的身份证书。注册完成

后，每个参与的对等体将其身份证书发送给对方，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 Firewall Threat Defense 设备证书的详细信息，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 数字签名及其内容。

要获取 CA 证书，请执行以下操作：

- 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，会在托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 特定参数以及一个已注册的身份证书。

PKCS#12 文件

PKCS#12 文件或 PFX 文件将服务器证书、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。

已弃用的哈希算法、加密算法和 Diffie-Hellman 模数组

请先更新您的 VPN 配置，以使用受支持的 DH 和加密算法，然后再升级到 Firewall Threat Defense 6.70 或更高版本。

- 更新您的 IKE 提议和 IPSec 策略，使其与 Firewall Threat Defense 6.70 或更高版本支持的策略相匹配。
- 请在更新为支持的算法后部署配置更改。

从 Firewall Threat Defense 6.70 版本开始，已移除对这些安全性较低的加密算法的支持：

- 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 和 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

在创建新的VPN拓扑时，您必须为其提供唯一名称，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。

VPN 身份验证没有默认的预共享密钥。您必须手动定义预共享密钥或让系统自动生成该密钥。如果选择自动，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。

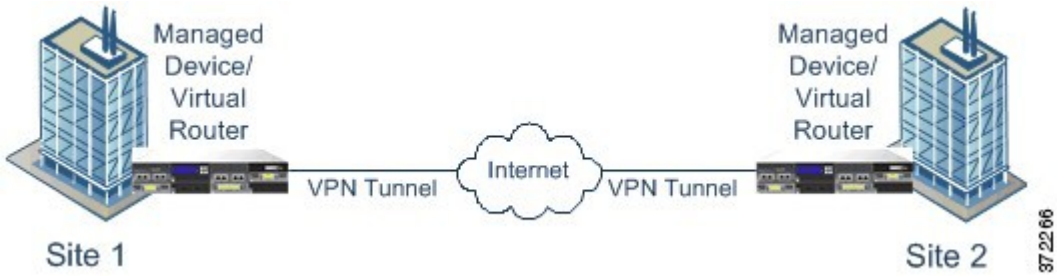
点对点 VPN 拓扑

点对点 VPN 拓扑是一种网络配置，

- 使两个终端能够直接相互通信
- 允许您将两个终端配置为对等设备，并且
- 允许任一设备启动安全连接。

此图显示了典型的点对点 VPN 拓扑。

图 *1:* 点对点 *VPN* 拓扑



中心辐射型 VPN 拓扑

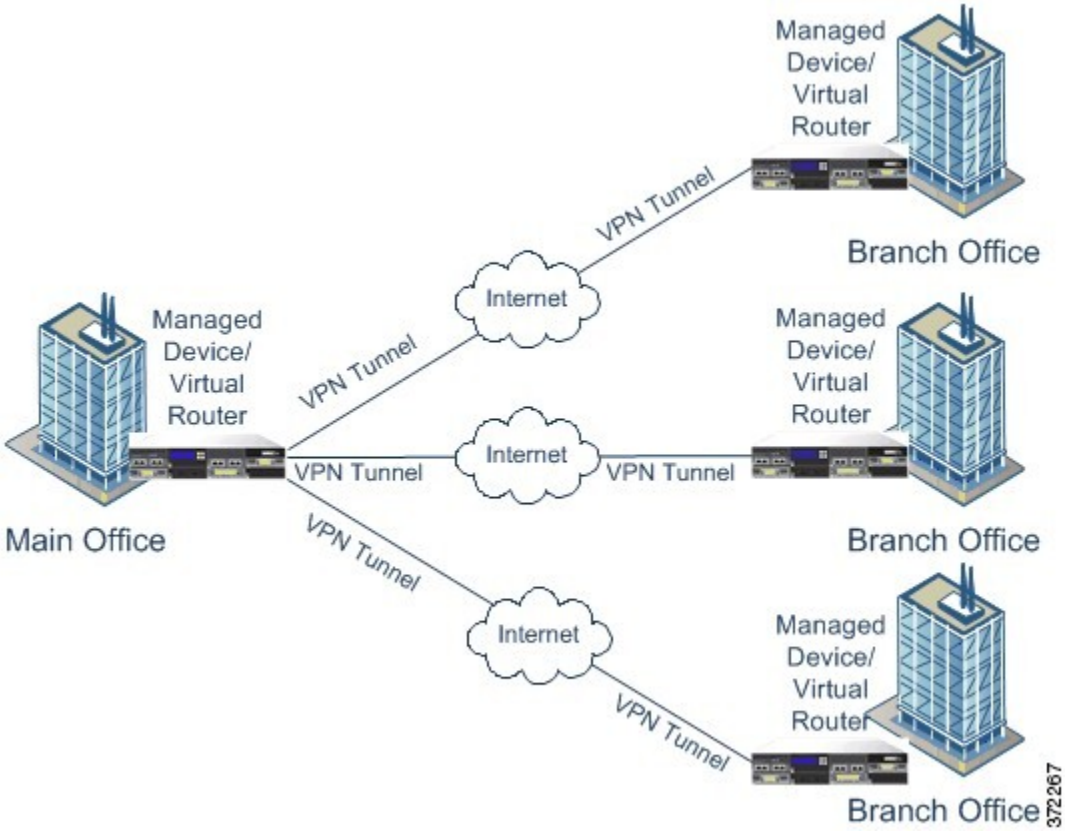
中心辐射型 VPN 拓扑是一种网络架构，

- 将中心终端（中心节点）与多个远程终端（分支节点）连接起来
- 将中心节点与各个分支节点之间的每个连接都建立为一个独立的 VPN 隧道，并且
- 使任何分支节点后面的主机都能通过中心节点相互通信。

中心辐射型拓扑结构通常代表 VPN，它使用互联网或其他第三方网络上的安全连接将组织的总部和分支机构连接起来。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。

此图展示了一种典型的中心辐射型 VPN 拓扑结构。

图 *2:* 中心辐射型 *VPN* 拓扑图



全网状 VPN 拓扑

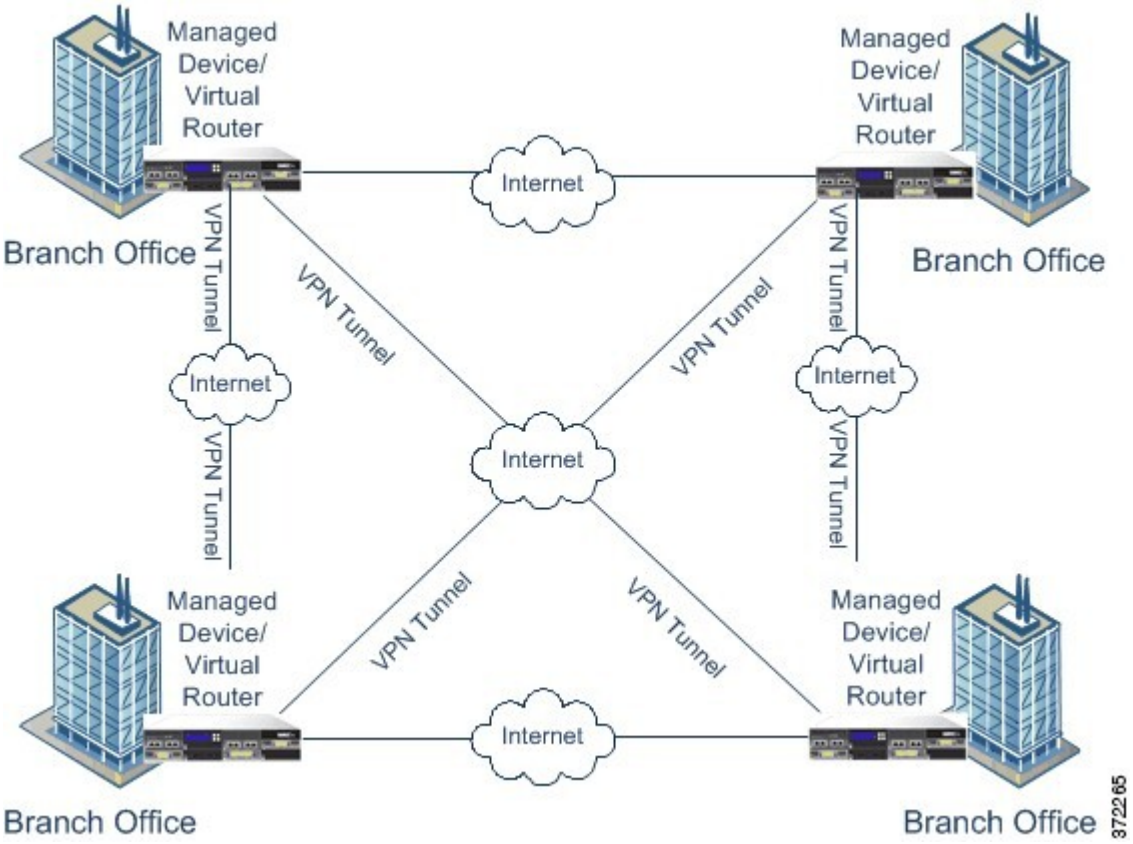
全网状 VPN 拓扑是一种网络配置，

- 允许所有终端通过独立的 VPN 隧道与其他所有终端通信。
- 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，以及
- 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 的托管设备数量取决于所需的冗余级别。

此图展示了一个典型的全网状 VPN 拓扑结构。

图 *3:* 全网状 *VPN* 拓扑



隐式拓扑

隐式拓扑是一种复杂的 VPN 网络配置，

- 结合了三种主要 VPN 拓扑（全网状、中心辐射型和点对点）的元素
- 创建比单个拓扑类型更高级的网络架构，以及
- 提供满足特定网络要求的定制连接解决方案。

隐式拓扑类型

- **部分网状结构**：一种网络，其中部分设备采用全网状拓扑结构，而其他设备则与部分全网状设备形成中心辐射型拓扑或点对点连接。部分网状不提供全网状结构的冗余，但实施成本较低。外围网络采用部分网状拓扑结构连接到全网状骨干网。
- **分层中心辐射型结构**：一种中心辐射型拓扑网络，其中设备在某些拓扑结构中充当中心设备，而在另一些拓扑结构中充当分支设备。分支组可以将流量发送到最近的中心。

- **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。

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。