paloalto TECHDOCS

IPsec VPN 管理

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

June 9, 2023

Table of Contents

IPSec VPN 基础知识 5

IPsec VPN 6

IPSec 隧道模式 7

IPSec VPN 类型 8

IPSec VPN 隧道 9

VPN 部署 11

VPN 的 Internet 密钥交换 (IKE) 13

IKE 网关 13

IKE 阶段 1 14

IKE 阶段 2 15

IKEv2 17

IPSec VPN（站点到站点）入门 21

站点到站点 VPN 概述 22

隧道接口 22

隧道监控 23

IPSec VPN 的代理 ID 24

规划 IPSec VPN 隧道设置 26

配置 IPSec VPN 隧道（站点到站点） 27

设置 IKE 网关 28

导出对等设备的证书以使用哈希和 URL 进行访问 32

导入证书以进行 IKEv2 网关验证 32

更改 IKEv2 的密钥有效期或身份验证间隔 33

更改 IKEv2 的 Cookie 激活阈值 34

配置 IKEv2 流量选择器 34

定义加密配置文件 36

定义 IKE 加密配置文件 36

定义 IPSec 加密配置文件 37

建立 IPSec 隧道 38

设置 IPsec 隧道（隧道模式） 38

设置 IPsec 隧道（传输模式） 39

监控 IPSec VPN 隧道 41

定义隧道监控配置文件 42

查看隧道状态 43
启用、禁用、刷新或重启 IKE 网关或 IPsec 隧道 46
启用或禁用 IKE 网关或 IPSec 隧道 46
刷新或重新启动 IKE 网关或 IPSec 隧道 46
站点到站点 VPN 配置示例 49
使用静态路由的站点到站点 VPN 50
使用 OSPF 的站点与站点 VPN 56
使用静态和动态路由的站点到站点 VPN 63
故障排除 71
排查 IPSec VPN 隧道连接问题 72
测试 VPN 连接 72
解释 VPN 错误消息 73
使用 CLI 解决站点到站点 VPN 问题 76
Show 命令 76
清除命令 77
测试命令 77
调试命令 78

IPSec VPN 基础知识

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

通过虚拟专用网络 (VPN) 创建隧道可让用户和系统在公共网络上安全地进行连接，如同在局域网 (LAN) 上进行连接。要建立 VPN 隧道，需要两台可以相互进行身份验证的设备，并且能够加密它们之间的信息流。此类设备可以是两个 Palo Alto Networks 防火墙，或是一个 Palo Alto Networks 防火墙和一个其他供应商提供的具备 VPN 功能的设备。

了解 VPN 的基本概念：

- IPsec VPN
- IPSec 隧道模式
- IPSec VPN 类型
- IPSec VPN 隧道
- VPN 部署
- VPN 的 Internet 密钥交换 (IKE)

IPsec VPN

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

IPSec VPN 通过公共网络基础设施（例如互联网）提供私有且安全的 IP 通信。利用这项技术，不同地理区域的不同站点或用户可以通过网络进行通信，从而安全地使用其资源。IPSec 提供数据机密性和完整性，包括身份验证、完整性检查和加密。

IPSec VPN 是两种常见 VPN 协议之一，或者是用于建立 VPN 连接的标准集。在 IP 层，IPSec 提供对整个网络（而不仅仅是单个设备）的安全远程访问。

IPSec VPN 有两种类型：

- 隧道模式
- 传输模式

IPSec 与 **VPN** 之间的区别

IP 安全 **(IPSec)**	**VPN**
为 IP 主机提供对 IP 网络上发送的数据进行加密和验证的方法。	使用加密来隐藏 VPN 客户端和服务器之间发送的所有数据。
通过使用 IPSec，拥有 IP 地址的实体可以创建安全隧道。	许多类型的 VPN 协议提供不同级别的安全性和其他功能。VPN 行业中最常用的隧道协议是点对点隧道协议 (PPTP)、第二层隧道协议 (L2TP) 或 IPSec、安全套接字隧道协议 (SSTP) 和 OpenVPN。

IPSec 隧道模式

在何处可以使用？	需要提供什么？
• Prisma Access（Prisma Access 尚不支持 IPSec 隧道传输模式） • PAN-OS	无需许可证

IPSec 标准定义了两种不同的 IPSec 操作模式：隧道模式和传输模式。传输模式和隧道模式之间的主要区别在于应用策略规则的位置。虽然在隧道模式下，原始数据包被封装在另一个 IP 标头中，但在任一模式下，数据包都可以通过身份验证标头 (AH)、封装安全负载 (ESP) 来提供保护，或者同时使用两者。

- *AH* 不能与 *NAT* 一起使用，因为完整性是通过使用 *IP* 标头的某些字段来计算的。原因是 *AH* 在基于哈希的消息身份验证代码 *(HMAC)* 计算中包含外部 *IP* 标头，导致 *NAT* 会将其破坏。
- *IPSec* 传输模式用于端到端通信，例如客户端和服务器之间，或者工作站和网关（如果网关被视为主机）之间。一个很好的例子是从工作站到服务器的加密 *Telnet* 或远程桌面会话。
- 虽然 *PAN-OS* ® 默认支持隧道模式，但传输模式是 *PAN-OS 11.0* 版本才开始引入的新选项。

IPSec VPN 类型

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

站点到站点（或网关到网关）VPN 和远程访问（客户端到站点）VPN 是两种不同类型的 VPN。客户端到站点 VPN 代表单个用户连接，而站点到站点 VPN 则处理整个网络之间的远程连接。

在站点到站点 VPN 中，IPSec 安全方法用于创建从一个客户网络到客户远程站点的加密隧道。Palo Alto Networks VPN 隧道也可以在合作伙伴之间使用。

站点到站点 VPN 不允许多个端点。

在远程访问 VPN 中，各个端点连接到专用网络以远程访问该专用网络的服务和资源。远程访问 VPN 最适合企业和家庭用户，因为它允许多个端点。

IPSec VPN 隧道

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

创建 IPSec 隧道的过程首先开始建立加密和安全的预备隧道，然后在该安全隧道内协商 IPSec 隧道的加密密钥和参数。

VPN 协商分两个定义的阶段进行：阶段 1 和阶段 2。阶段 1 的主要目的是建立一个安全的加密通道，两个对等设备可以通过该通道进行协商。当阶段 1 成功完成后，对等设备迅速进入阶段 2 的协商。

如果隧道接口所在的区域与流量发出或离开的区域不同，则定义一条策略规则以允许流量从源区域流向包含隧道接口的区域。在隧道接口上配置 IP 地址是可选的。如果您打算在隧道接口上运行动态路由协议，则需要此 IP 地址。

虽然 IPSec 融合了许多组件技术并提供多种加密选项，但基本操作包括以下五个主要过程：

- 感兴趣的流量或按需 — IPSec 隧道策略规则和路由表确定哪种类型的流量是“感兴趣”的流量，或需要“按需”捕获的流量，从而提供保护。PAN-OS VPN 安全策略的实施方式取决于设备平台。访问列表解释 IPSec 策略规则以确定哪些流量将受 IPSec 保护。

  仅当将感兴趣的流量发往该隧道时，IPSec 隧道才会启动。如需手动启动隧道，请参考 使用 CLI 排除站点到站点 VPN 问题检查隧道状态并清除隧道。
- **IKE** 阶段 **1** — IKE 是与 IPSec 一起使用的密钥管理协议标准。IKE 对 IPSec 会话中的每个对等设备进行身份验证，自动协商两级 SA，并处理分两个阶段完成的会话密钥交换：阶段 1 和阶段 2。

  IKE 阶段 1 的主要目的是对 IPSec 对等设备进行身份验证并在对等设备之间建立安全通道。
- **IKE** 阶段 **2**— IKE 在对等设备之间协商更严格的 IPSec 安全关联 (SA) 参数。
- **IPSec** 数据传输 — 合格数据在 IPSec 对等设备之间传输。根据定义感兴趣流量的方法，通过 IPSec 会话交换信息。数据包在 IPSec 对等设备处使用 IPSec SA 中指定的任何加密进行加密和解密。
- **IPSec** 隧道会话终止 — IPSec 会话可能会终止，因为流量结束且 IPSec SA 已删除，或者 SA 可能根据任一 SA 有效期设置超时。SA 超时可以是在达到指定的秒数后，或者达到通过连接传递的指定字节数后。

  当 SA 终止时，密钥将被丢弃，从而要求 IKE 执行新的阶段 2，并可能执行新的阶段 1 协商。新的 SA 可以在当前 SA 到期之前建立，从而保持不间断的数据流。

  IPSec 会话因删除或超时而终止。

Palo Alto Networks 下一代防火墙上的 **IPSec** 隧道策略规则实施

封装数据包以在网络上安全传输是通过 IPsec 协议完成的。例如，在站点到站点 VPN 的情况下，网络中的源主机传输 IP 数据包。当该数据包到达网络边缘时，它会与 VPN 网关联系。与该网络对应的 VPN 网关对专用 IP 数据包进行加密，并通过 ESP 隧道将其中继到下一个网络边缘的对等 VPN 网关，该网关对数据包进行解密并将其传送到目标主机。

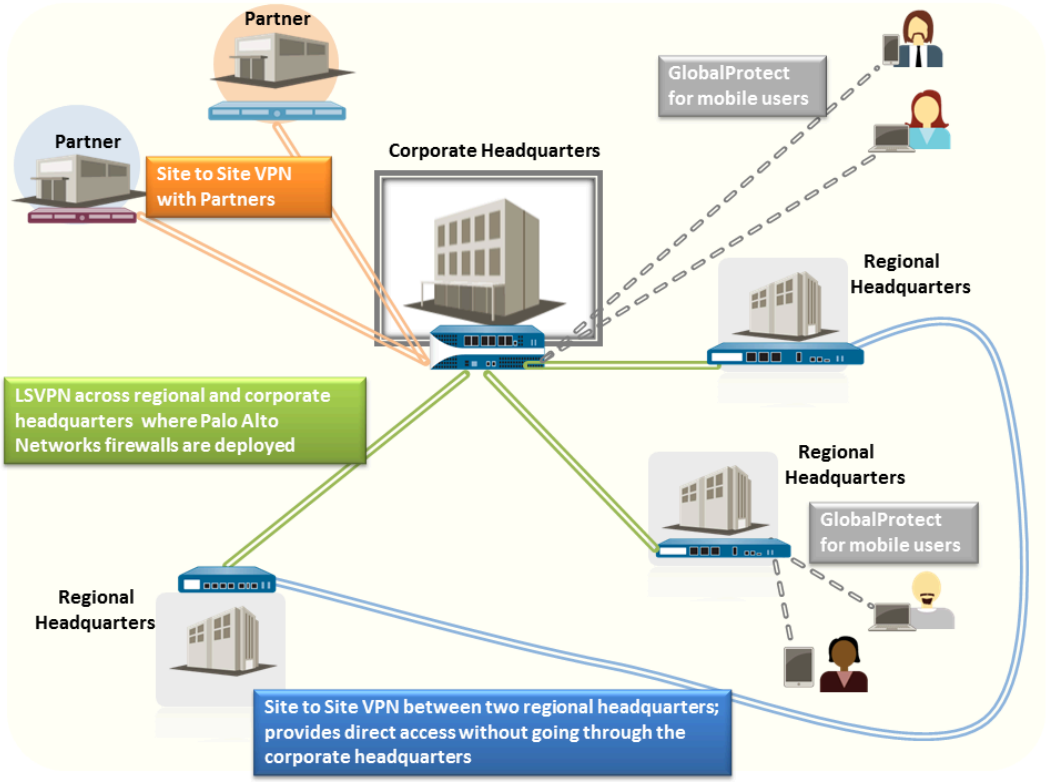
基于策略的 VPN 具有特定的安全规则、策略规则或访问列表（例如源地址、目标地址和端口），这些规则被配置为允许感兴趣的流量通过 IPSec 隧道。这些规则在快速模式（或 IPSec 阶段 2）期间被引用，并且在第一或第二消息中作为代理 ID 进行交换。如果 Palo Alto Networks 防火墙未配置代理 ID 设置，则防火墙将代理 ID 设置为默认值（source ip = 0.0.0.0/0、destination ip = 0.0.0.0/0、application:any），并在快速模式的第一条或第二条消息期间与对等设备交换。

VPN 部署

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

Palo Alto Networks 防火墙支持以下 VPN 部署：

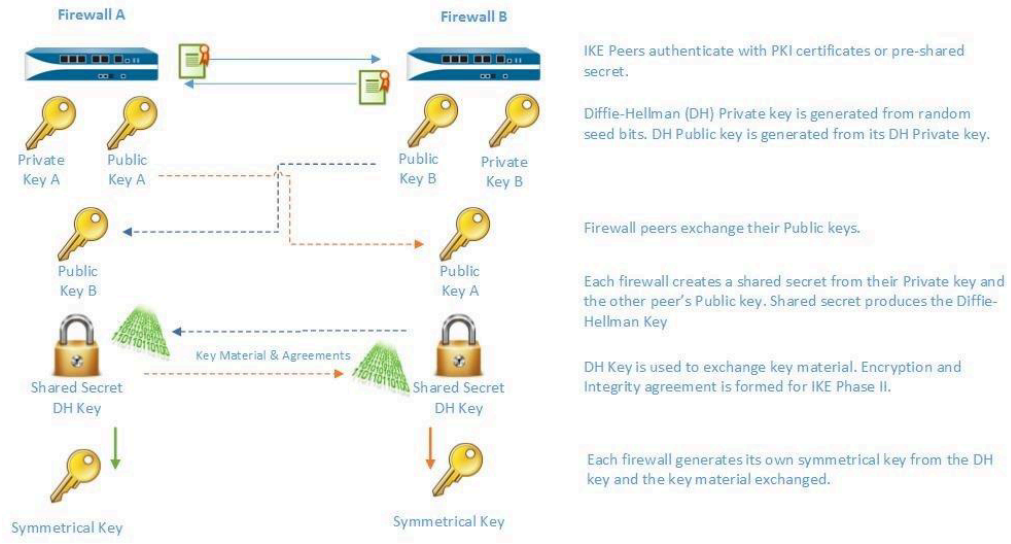
- 站点到站点 **VPN** — 连接中心站点和远程站点的简单 VPN，或者连接中心站点和多个远程站点的星型 VPN。防火墙使用 Internet 协议安全 (IPSec) 协议组为两个站点之间的流量建立安全隧道。请参阅站点到站点 VPN 概述。
- 远程用户到站点 **VPN** — 使用 GlobalProtect 代理允许远程用户通过防火墙建立安全连接的解决方案。此解决方案使用 SSL 和 IPSec 在用户和站点之间建立安全连接。请参阅《GlobalProtect 管理员指南》。
- 大规模 **VPN** — Palo Alto Networks GlobalProtect 大规模 VPN (LSVPN) 提供了在最多 1,024 个卫星办公室部署可扩展星型 VPN 的简化机制。该解决方案需要在每个中心和每个星型拓扑中对 Palo Alto Networks 防火墙进行解密。它使用证书对设备进行身份验证、使用 SSL 在所有组件之间进行安全通信并使用 IPSec 保护数据。请参阅大规模 VPN (LSVPN)。
- 远程站点 **VPN** — 远程站点使用 IPSec 隧道来保护远程网络位置的用户和设备。此外，使用 GlobalProtect 保护的移动用户和远程站点的用户使用 IPSec 隧道（用于服务连接或 ZTNA 连接器）或 GRE 隧道（用于 Colo-Connect 连接）访问私有应用程序。



VPN 的 Internet 密钥交换 (IKE)

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

IKE 过程允许位于隧道两端的 VPN 对等设备使用双方商定的加密的密钥或证书和方法对数据包进行加密和解密。IKE 过程在两个阶段会出现：IKE 阶段 1 和 IKE 阶段 2。每个阶段都可使用利用加密配置文件（即 IKE 加密配置文件和 IPSec 加密配置文件）定义的密钥和加密算法，并且 IKE 协商的结果为安全关联 (SA)。SA 是一组双方商定的密钥和算法，VPN 对等设备用来允许在 VPN 隧道之间传输数据。下图显示了建立 VPN 隧道的密钥交换过程：



IKE 网关

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

在两个网络之间发起和终止 VPN 连接的 Palo Alto Networks 防火墙或防火墙和其他安全设备称为 IKE 网关。要建立 VPN 隧道并在 IKE 网关之间发送流量，每个对等设备必须拥有 IP 地址（静态或动态）或 FQDN。VPN 对等设备使用预共享密钥或证书进行相互身份验证。

对等设备还必须在 IKE 阶段 1 中协商用于建立 VPN 隧道的主模式或主动模式和 SA 生命周期。主模式保护对等设备的身份且更安全，因为在建立隧道时会交换多个数据包。主模式是为 IKE 协商推荐的模式，如果两个对等设备都支持该模式。主动模式使用少量数据包建立 VPN 隧道，因此速度较快，但用来建立 VPN 隧道的安全性较低。

有关配置的详细信息，请参阅设置 IKE 网关。

IKE 阶段 1

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

在本阶段中，防火墙使用在 IKE 网关配置和 IKE 加密配置文件中定义的参数相互进行身份验证，并建立安全控制通道。IKE 阶段支持使用预共享密钥或数字证书（使用公钥基础设施 (PKI)）对对等设备进行相互身份验证。预共享密钥是用于保护小型网络的简单解决方案，因为它们不需要支持 PKI 基础设施。数字证书需要更强的身份验证安全，因此保护大型网络或实施起来更方便。

使用证书时，请确保两个网关对等设备信任 CA 签发的证书，并且证书链中证书的最大长度为 5 或更少。在启用 IKE 碎片后，防火墙可以最多使用证书链中的 5 个证书重编 IKE 消息，并成功建立 VPN 隧道。

IKE 加密配置文件用于定义在 IKE SA 协商中使用的以下选项：

- Diffie-Hellman (DH) 组为 IKE 生成对称密钥。

  Diffie-Hellman 算法使用一方的私钥和另一方的公钥创建共享机密，即两个 VPN 隧道对等设备共享的加密密钥。在防火墙上支持的 DH 组为：

组号	位数
组 1	768 位
组 2	1024 位（默认）
组 5	1,536 比特
组 14	2048 位
组 15	（PAN-OS 10.2.0 及更高版本）3072 位模块化指数组
组 16	（PAN-OS 10.2.0 及更高版本）4096 位模块化指数组
组 19	256 位椭圆曲线组
组 20	384 位椭圆曲线组
组 21	（PAN-OS 10.2.0 及更高版本）512 位随机椭圆曲线组

- 身份验证算法 - sha1、sha 256、sha 384、sha 512 或 md5。

- 加密算法 — aes-256-gcm、aes-128-gcm、3des、aes-128-cbc、aes-192-cbc、aes-256-cbc 或 des。

  - *PAN-OS 10.0.3* 及更高版本支持 *aes-256-gcm* 和 *aes-128-gcm* 算法。
  - *PAN-OS 10.1.0* 及更早版本支持 *des* 加密算法。

IKE 阶段 2

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

在保护和验证隧道后，在阶段 2 中，通道可用来进一步保护在网络之间传输数据。IKE 阶段 2 使用在该过程的阶段 1 和 IPSec 加密配置文件中创建的密钥，定义在 IKE 阶段 2 的 SA 中使用的 IPSec 协议和密钥。

IPSec 使用以下协议来实现安全通信：

- 封装安全负载 (ESP) — 可让您对整个 IP 数据包进行加密，对数据包源进行身份验证并验证数据完整性。虽然 ESP 需要您对数据包进行加密和身份验证，但可以选择通过将加密选项设置为 Null 只加密或只进行身份验证；使用加密不会影响身份验证。
- 身份验证头 (AH) — 对数据包源进行身份验证和验证数据完整性。AH 不会对数据负载进行加密，且不适合用于数据隐私非常重要的部署。AH 常用于验证对等设备的合法性，并且不需要数据隐私。

表 **1: IPSec** 身份验证和加密支持的算法

ESP	**AH**
支持 **Diffie-Hellman (DH)** 交换选项	
• 组 1 — 768 位 • 组 2 — 1024 位（默认） • 组 5 — 1536 位 • 组 14 — 2048 位 • （PAN-OS 10.2.0 及更高版本）第 15 组 — 3072 位模块化指数组 • （PAN-OS 10.2.0 及更高版本）第 16 组 — 4096 位模块化指数组 • 组 19 — 256 位椭圆曲线组 • 组 20 —384 位椭圆曲线组 • （PAN-OS 10.2.0 及更高版本）第 21 组 — 512 位随机椭圆曲线组 • no-pfs — 默认情况下，完全正向保密处于启用状态，这表示 IKE 阶段 2 会使用上述所列组之一生成新 DH 密钥。该密钥独立于 IKE 阶段 1 中交换的密钥，可提供更好的数据传输安全。	

ESP	AH
如果您选择 no-pf，则不会续订在阶段 1 中创建的 DH 密钥，且 IPSec SA 协商只需使用一个密钥。必须同时为 PFS 启用或禁用两个 VPN 对等设备。	
支持的加密算法	
• des	（PAN-OS 10.1.0 及更早版本）具有 56 位安全强度的数据加密标准 (DES)。
• 3des	安全强度为 112 位的三重数据加密标准 (3DES)。
• aes-128-cbc	使用密码块链 (CBC) 的高级加密标准 (AES)，安全强度为 128 位。
• aes-192-cbc	使用密码强度为 192 位的 CBC 的 AES。
• aes-256-cbc	使用密码强度为 256 位的 CBC 的 AES。
• aes-128-ccm	使用密码强度为 128 位的 Counter with CBC-MAC (CCM) 的 AES。
• aes-128-gcm	使用密码强度为 128 位的 Galois/Counter Mode (GCM) 的 AES。
• aes-256-gcm	使用密码强度为 256 位的 GCM 的 AES。
支持的身份验证算法	
• md5	• md5
• sha 1	• sha 1
• sha 256	• sha 256
• sha 384	• sha 384
• sha512	• sha 512

保护 **IPSec VPN** 隧道的方法（**IKE** 阶段 **2**）

可以使用手动密钥和自动密钥保护 IPSec VPN 隧道。此外，IPSec 配置选项包括密钥协议的 Diffie-Hellman 组，以及加密算法和消息身份验证的哈希算法。

- 手动密钥 — 如果 Palo Alto Networks 防火墙使用旧设备建立 VPN 隧道，或者如果想要减少生成会话密钥的开销，通常使用手动密钥。如果使用手动密钥，必须在两个对等设备上配置同一密钥。

  不建议使用手动密钥建立 VPN 隧道，因为在中断对等设备之间的密钥信息时可能会影响会话密钥；如果该密钥受到影响，则数据传输不再安全。
- 自动密钥 — 自动密钥可让您根据在 IPSec 加密配置文件中定义的算法自动生成用于建立和维护 IPSec 隧道的密钥。

IKEv2

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

IPSec VPN 网关使用 IKEv1 或 IKEv2 协商 IKE 安全关联 (SA) 和 IPSec 隧道。IKEv2 在 RFC 5996 内定义。

与使用阶段 1 SA 和阶段 2 SA 的 IKEv1 不同，IKEv2 使用封装式安全措施负载 (ESP) 或身份验证标头 (AH) 的子 SA，该 SA 与 IKE SA 一起设置。

如果位于两个网关之间的设备上出现 NAT，您需要在两个网关上启用 NAT 遍历 (NAT-T)。一个网关只能查看 NAT 设备的公共（全局可路由）IP 地址。

与 IKEv1 相比，IKEv2 具备以下优势：

- 隧道端点交换较少的消息即可建立隧道。IKEv2 使用四个消息；IKEv1 使用九个消息（在主要模式下）或六个消息（在主动模式下）。
- 内置 NAT-T 功能提升了供应商之间的兼容性。
- 如果隧道关闭，内置运行状况检查可自动重建隧道。活性检查取代了 IKEv1 中使用的失效对等设备检测。
- 支持流量选择器（每个交换一个）。流量选择器用在 IKE 协商中，用于控制哪些流量可以访问此隧道。
- 支持哈希和 URL 证书交换来减少碎片。
- 通过提高对等设备验证来抵御 Dos 攻击。超过半开 SA 数量可以触发 Cookie 验证。

在配置 IKEv2 之前，您应该先熟悉以下概念：

- 活性检查
- Cookie 激活阈值和严格 Cookie 验证
- 流量选择器
- 哈希和 URL 证书交换
- SA 密钥有效期和重新验证间隔

在设置 IKE 网关后，如果您选择 IKEv2，请根据环境需要执行下列与 IKEv2 相关的可选任务：

- 导出对等设备的证书以使用哈希和 URL 进行访问
- 导入证书以进行 IKEv2 网关验证
- 更改 IKEv2 的密钥有效期或身份验证间隔
- 更改 IKEv2 的 Cookie 激活阈值
- 配置 IKEv2 流量选择器

活性检查

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

IKEv2 的活性检查类似于失效对等设备检测 (DPD)，IKEv1 使用此检测作为确定对等设备是否仍可用的方式。

在 IKEv2 中，网关以可配置的时间间隔（默认为 5 秒）向对等设备发送任意 IKEv2 包传输或空的参考消息来实现活性检查。如果需要，发送者会尝试重新传输，最多尝试 10 次。如果得不到响应，发送方会关闭并删除 IKE_SA 和对应的 CHILD_SA。发送方会发出另一个 IKE_SA_INIT 消息来从头开始。

Cookie 激活阈值和严格 **Cookie** 验证

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

始终为 IKEv2 启用 Cookie 验证；这有助于防御半开 SA DoS 攻击。您可以配置将触发 Cookie 验证的半开 SA 全局阈值数。您还可以配置各 IKE 网关来为每个新 IKEv2 SA 执行 Cookie 验证。

- **Cookie Activation Threshold**（**Cookie** 激活阈值）是全局 VPN 会话设置，用于限制同步半开 IKE SA（默认为 500）的数量。如果半开 IKE SA 数量超过 **Cookie Activation Threshold**（**Cookie** 激活阈值），响应者将会请求 Cookie，且发起者必须使用包含 Cookie 的 IKE_SA_INIT 进行响应以对此连接进行验证。如果 Cookie 验证成功，可以启动其他 SA。值为 0 表示 Cookie 验证应始终开启。

  发起者返回 Cookie 之前，响应者不会维护发起者的状态，也不会执行 Diffie-Hellman 密钥交换。IKEv2 Cookie 验证可减少试图保留大量连接半开放的攻击。

  Cookie Activation Threshold（**Cookie** 激活阈值）必须低于 **Maximum Half Opened SA**（最大半开 **SA**）设置。如果更改 IKEv2 的 Cookie 激活阈值 为非常大的数字（例如，65534），而 **Maximum Half Opened SA**（最大半开 **SA**）设置保留默认值 65535，则基本上会禁用 cookie 验证。

- 如果无论全局阈值如何，您都想为网关收到的每个新 IKEv2 SA 执行 Cookie 验证，您可以启用 **Strict Cookie Validation**（严格 **Cookie** 验证）。**Strict Cookie Validation**（严格 **Cookie** 验证）只影响要配置的 IKE 网关，默认情况下处于禁用状态。禁用 **Strict Cookie Validation**（严格 **Cookie** 验证）时，系统将使用 **Cookie Activation Threshold**（**Cookie** 激活阈值）确定是否需要 Cookie。

流量选择器

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

在 IKEv1 中，具备基于路由的 VPN 的防火墙需要使用本地和远程代理 ID 才能设置 IPSec 隧道。每个对等设备将自己的代理 ID 与收到的数据包进行比较，以成功协商 IKE 阶段 2。IKE 阶段 2 说的是协商 SA 来设置 IPSec 隧道。（有关代理 ID 的详细信息，请参阅隧道接口。）

在 IKEv2 中，您可以配置 IKEv2 流量选择器，此选择器是 IKE 协商期间使用的网络流量的组件。流量选择器在 CHILD_SA（隧道创建）阶段 2 期间用以设置隧道和确定允许哪些流量通过此隧道。这两个 IKE 网关对等设备必须协商并在流量选择器上达成一致；否则，其中一侧对等设备会缩小地址范围来达成一致。一个 IKE 连接可以有多个隧道；例如，您可以为各部门分配不同的隧道来隔离流量。流量分离还允许实施 QoS 之类的功能。

IPv4 和 IPv6 流量选择器有：

- 源 **IP** 地址 — 网络前缀、地址范围、特定主机或通配符。
- 目标 **IP** 地址 — 网络前缀、地址范围、特定主机或通配符。
- 协议 — 传输协议，如 TCP 或 UDP。
- 源端口 — 产生此数据包的端口。
- 目标端口 — 数据包的目标端口。

在 IKE 协商期间，不同的网络和协议可以有多个流量选择器。例如，发起者可能指示要通过隧道将 TCP 数据包从 172.168.0.0/16 发送到其对等设备，目标为 198.5.0.0/16。同时希望通过同一隧道将 UDP 数据包从 172.17.0.0/16 发送到同一网关，目标为 0.0.0.0（任意网络）。对等设备网关必须与这些流量选择器保持一致才能知道会发生什么操作。

有可能一个网关将使用流量选择器（比其它网关的 IP 地址更加具体的 IP 地址）开始协商。

- 例如，网关 A 提供源 IP 地址 172.16.0.0/16 和目标 IP 地址 192.16.0.0/16。但是网关 B 配置为使用 0.0.0.0（任意源）作为源地址，使用 0.0.0.0（任意目标）作为目标 IP 地址。因此，网关 B 会将其源 IP 地址缩小到 192.16.0.0/16，将目标地址缩小到 172.16.0.0/16。因此，缩小将适应网关 A 的地址，并且这两个网关的流量选择器将一致。
- 如果网关 B（配置了源 IP 地址 0.0.0.0）是发起者，而不是响应者，网关 A 将使用其更为具体的 IP 地址进行响应，网关 B 将缩小其地址以达成一致。

哈希和 URL 证书交换

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

IKEv2 支持在 SA 的 IKEv2 协商期间使用的哈希和 URL 证书交换。将证书存储在由 URL 指定的 HTTP 服务器上。对等设备从接收指向服务器的 URL 的服务器获取证书。哈希用于检查证书的内容是否有效。因此，这两个对等设备会与 HTTP CA 交换证书，而不是互相交换证书。

哈希和 URL 的哈希部分可减少消息大小，因此哈希和 URL 是一种在 IKE 阶段减少数据包碎片的方法。对等设备收到所需的证书和哈希，说明 IKE 阶段 1 已对对等设备进行验证。减少碎片发生有助于防御 DoS 攻击。

在配置 IKE 网关时，通过选择 **HTTP Certificate Exchange**（**HTTP** 证书交换）并输入 **Certificate URL**（证书 **URL**）可以启用哈希和 URL 证书交换。对等设备也必须使用哈希和 URL 证书交换才能使交换成功。如果对等设备不能使用哈希和 URL，将以在 IKEv1 中交换哈希和 URL 证书的类似方式交换 X.509 证书。

如果您启用哈希和 URL 证书交换，如果证书服务器中尚无此证书，必须将此证书导出到证书服务器。在您导出证书时，文件格式应为 **Binary Encoded Certificate (DER)**（二进制编码证书 **(DER)**）。请参阅导出对等设备的证书以使用哈希和 URL 进行访问。

SA 密钥有效期和重新验证间隔

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

IKEv2 中有两个 IKE 加密配置文件值用于控制 IKEv2 IKE SA 的建立，分别为 **Key Lifetime**（密钥有效期）和 **IKEv2 Authentication Multiple**（**IKEv2** 身份验证倍数）。密钥有效期是协商 IKE SA 密钥保持有效的时间长度。在密钥有效期到期之前，必须重新为 SA 生成密钥；否则，一旦到期，SA 必须开始新的 IKEv2 IKE SA 密钥更新。默认值为 8 小时。

重新身份验证间隔等于 **Key Lifetime**（密钥有效期）乘以 **IKEv2 Authentication Multiple**（**IKEv2** 身份验证倍数）。认证倍数默认为 0，即禁用重认证功能。

身份验证倍数范围为 0-50。因此，例如您将身份验证倍数设置为 20，则系统会每隔 20 次密钥更新执行一次重新验证，即每 160 个小时执行一次。这表示须向 IKE 进行重新验证以从头重建 IKE SA 之前，网关有 160 小时的时间执行子 SA 创建。

在 IKEv2 中，发起者和响应者网关都有自己的密钥有效期，而密钥有效期较短的网关是要求更新 SA 密钥的网关。

IPSec VPN（站点到站点）入门

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

VPN 连接可提供两个或多个站点之间的信息的安全访问。要提供资源和可靠连接的安全访问，VPN 连接需要以下组件：IKE 网关、隧道接口、隧道监控、VPN 的互联网密钥交换 (IKE) 和 IKEv2。

在规划 IPSec VPN 隧道设置之前，了解以下内容非常重要：

- 隧道接口
- 隧道监控
- IPSec VPN 的代理 ID

站点到站点 VPN 概述

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

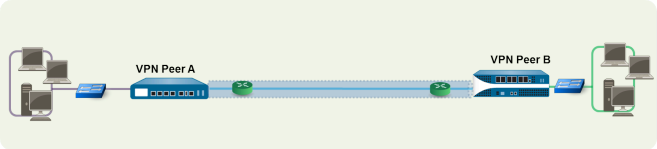
可让您连接两个局域网 (LAN) 的 VPN 连接称为站点到站点 VPN。您可以配置基于路由的 VPN，以连接位于两个站点的 Palo Alto Networks 防火墙，或者将 Palo Alto Networks 防火墙与其他位置的第三方安全设备进行连接。防火墙还可以与基于第三方的 VPN 设备进行互操作；Palo Alto Networks 防火墙支持基于路由的 VPN。

Palo Alto Networks 防火墙可建立基于路由的 VPN，其中防火墙可根据目标 IP 地址做出路由决策。如果通过 VPN 隧道将流量路由到特定目标，则会将该流量作为 VPN 流量进行处理。

可以使用 Internet 协议安全 (IPSec) 协议组为 VPN 流量建立安全隧道，并保护 TCP/IP 数据包中的信息（如果隧道类型为 ESP，则加密）。在其他 IP 负载中嵌入 IP 数据包（标头和负载），并应用新标头，然后通过 IPSec 隧道发送。新标头中的源 IP 地址是本地 VPN 对等设备的源 IP 地址，目标 IP 地址是隧道远端 VPN 对等设备的目标 IP 地址。当数据包到达远程 VPN 对等设备（隧道远端的防火墙）后，将会移除外部标头，并将原始数据包发送到其目的地。

要建立 VPN 隧道，首先需要对对等设备进行身份验证。在身份验证成功后，对等设备协商加密机制和算法来保护通信。Internet 密钥交换 (IKE) 过程用来对 VPN 对等设备进行身份验证，并在隧道的每一端定义 IPSec 安全关联 (SA) 保护 VPN 通信。IKE 使用数字证书或预共享密钥，以及 Diffie Hellman 密钥为 IPSec 隧道建立 SA。SA 指定安全传输所需的所有参数 — 包括安全参数索引 (SPI)、安全协议、加密密钥和目标 IP 地址 — 加密、数据身份验证、数据完整性和端点身份验证。

下图显示了两个站点之间的 VPN 隧道。如果受 VPN 对等设备 A 保护的客户端需要位于其他站点的服务器的内容，则 VPN 对等设备 A 向 VPN 对等设备 B 发起连接请求。如果安全策略允许进行连接，VPN 对等设备 A 使用 IKE 加密配置文件参数（IKE 阶段 1）建立安全连接，并对 VPN 对等设备 B 进行身份验证。然后，VPN 对等设备 A 使用 IPSec 加密配置文件建立 VPN 隧道，该配置文件用来定义 IKE 阶段 2 参数以允许在两个站点之间安全传输数据。



隧道接口

在何处可以使用？	需要提供什么？
• Prisma Access	无需许可证

在何处可以使用？	需要提供什么？
• PAN-OS	

要建立 VPN 隧道，每个端点的第 3 层接口都必须拥有逻辑隧道接口用来连接到防火墙并建立 VPN 隧道。隧道接口是用来在两个端点之间传输流量的逻辑（虚拟）接口。如果配置任何代理 ID，代理 ID 将计入任何 IPSec 隧道容量。

隧道接口必须属于安全区域才能应用策略规则，并且必须将其分配给虚拟路由器才能使用现有路由基础设施。务必确保将隧道接口和物理接口分配给同一虚拟路由器，这样防火墙才可执行路由查找并确定要使用的相应隧道。

通常，连接到隧道接口的第 3 层接口属于外部区域，如不信任区域。尽管隧道接口可以位于与物理接口相同的安全区域，但为了增加安全性和更好地了解，可以为隧道接口创建单独区域。如果为隧道接口创建单独区域（即 VPN 区域），则需创建安全策略以便使得流量能够在 VPN 区域和信任区域之间流动。

要在站点之间路由流量，隧道接口不需要 IP 地址。如果要启用隧道监控，或者使用动态路由协议在隧道之间路由流量，则只需要 IP 地址。使用动态路由，可将隧道 IP 地址用作路由到 VPN 隧道的流量的下一个跃点 IP 地址。

如果使用 VPN 对等设备配置 Palo Alto Networks 防火墙执行基于策略的 VPN，则必须在建立 IPSec 隧道时配置本地和远程代理 ID。每个对等设备与数据包中收到的内容进行配置的代理 ID 比较，以允许成功的 IKE 阶段 2 协商。如果需要多个隧道，可以为每个隧道接口配置唯一的代理 ID；一个隧道接口最多可以拥有 250 个代理 ID。每个代理 ID 对于防火墙的 IPSec VPN 隧道容量非常重要，并且隧道容量根据防火墙型号而有所不同。

有关配置的详细信息，请参阅建立 IPSec 隧道。

隧道监控

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

对于 VPN 隧道，可以检查整个隧道的目标 IP 地址连接。防火墙上的网络监控配置文件可让您验证目标 IP 地址连接（使用 ICMP）或指定轮询间隔的下一个跃点，并指定在发生故障后访问监控的 IP 地址要采取的操作。

如果无法访问目标 IP 地址，可以配置防火墙等待隧道恢复或配置自动故障转换至另一个隧道。在这两种情况下，防火墙生成系统日志提醒您隧道发生故障，并重新协商 IPSec 密钥加快恢复。

有关配置的详细信息，请参阅监控 IPSec VPN 隧道。

IPSec VPN 的代理 ID

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

代理身份或代理 ID 是指属于 IPSec VPN 的一组流量，该流量受对等设备之间协商的 SA（或在协商成功后进行设置）的约束。

它允许识别，然后引导流量：

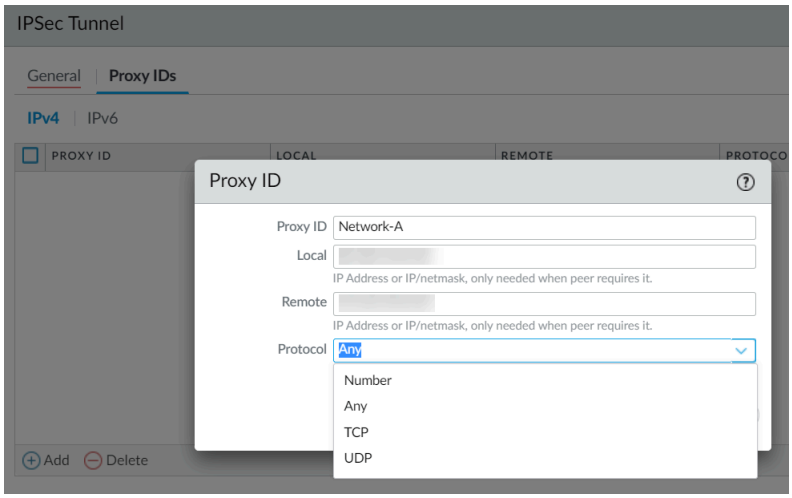
- 到适当的隧道，其中多个隧道在共享同一 IKE 网关的相同两个对等设备之间共存。
- 允许具有不同参数的唯一 SA 和共享 SA 共存。

在相同的两个对等设备之间设置 *VPN* 隧道的配置中使用代理 *ID*。

代理 ID 有助于识别哪些流量属于特定的 IPSec VPN。这允许操作系统安装适当的挂钩，以定向与代理 ID（客户端 ID）中的源地址和目标地址匹配的流量，并将其定向到匹配的 IPSec SA 中，或者传入和传出匹配的 IPSec SA 的 VPN 中。

设置代理 **ID**

Palo Alto Networks是其他一些使用代理 ID 的供应商之一。下图显示了 Palo Alto Networks 代理 ID 窗口及其选项。



选择 **Network**（网络） > **IPSec Tunnels**（**IPSec** 隧道） > **Proxy IDs**（代理 **ID**）。输入代理 ID 名称、本地 IP 地址、远程 IP 地址（如果对等设备需要）、协议类型及其本地和远程端口号。

每个代理 *ID* 都被视为一个 *VPN* 隧道，因此计入防火墙的 *IPSec VPN* 隧道容量。例如，站点到站点 *IPSec VPN* 隧道的最大限制为：*PA-3020* 为 *1000*、*PA-2050* 为 *100*，*PA-200* 为 *25*。

代理 ID 的行为与 IKE 版本不同：

- **IKEv1** — Palo Alto Networks 设备仅支持代理 ID 完全匹配。如果对等设备的代理 ID 不匹配，则 VPN 无法正常工作。
- **IKEv2** — 当两个 VPN 网关上的代理 ID 设置不同时，支持流量选择器缩小范围。

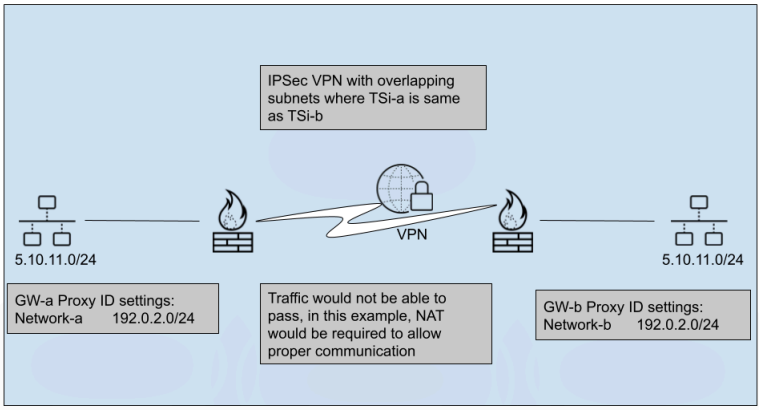
使用代理编号

以下示例显示了两个 VPN 网关：A 和 B。

IKE 协商由 VPN GW-az 启动，i=initiator、r=responder。VPN GW-a 定义流量选择器 TSi-a/TSr-a，VPN GW-b 指定流量选择器 TSi-b/TSr-b。虽然 TSr-a 与 TSr-b 相同，因此可以忽略，但 TSi-a 可以不同于 TSi-b。

在这种情况量无法通过 VPN 隧道路由，因为隧道的两端存在相同的网络。

但是，如下所示，解决此问题的唯一方法是让两个对等网关创建 NAT，以将新的、唯一的网络子网转换为内部网络，否则一端必须更改子网 IP。



这样，任何一端的所有流量都将发往新的 NAT 地址，而不是其他类似的网络。两个网关都必须执行 NAT 才能正常工作，以消除有关哪个网络位于哪一侧的混淆。

为 **Palo Alto** 网络防火墙配置 **IPSec VPN**

如果隧道的另一端是第三方 VPN 设备，否则是非 PAN-OS 防火墙，则需要指定匹配的本地代理 ID 和远程代理 ID：通常是本地和远程 LAN 子网。

配置 IPSec 隧道代理标识以标识 NAT 流量的本地和远程 IP 网络时，必须使用 NAT 后 IP 网络信息配置 IPSec 隧道的代理标识配置。这样做的原因是代理 ID 信息定义了 IPSec 配置允许通过两端隧道的网络。

规划 IPSec VPN 隧道设置

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

在设置 IPSec 隧道之前，确定以下因素并规划成功设置 IPSec 隧道非常重要。

STEP 1 | 决定 **VPN** 类型：站点到站点或远程访问

站点到站点 VPN 允许使用 IPSec 安全方法创建从一个客户网络到客户远程站点的加密隧道。但是，远程访问 VPN 允许个人用户连接到专用网络以访问其服务和资源。

STEP 2 | 为 **VPN** 选择安全方法

在站点到站点 VPN 中，IPSec 安全方法用于创建从一个客户网络到客户远程站点的加密隧道。

在远程访问 VPN 中，个人用户连接到专用网络。

STEP 3 | 决定 **VPN** 客户端

站点到站点 VPN 不需要在每个客户端上进行设置。远程访问 VPN 可能需要也可能不需要在每个客户端上进行设置。

STEP 4 | 决定 **VPN** 隧道设置

站点到站点 VPN 不需要每个用户都启动 VPN 隧道设置。远程访问 VPN 要求每个远程访问用户启动 VPN 隧道设置。

STEP 5 | 决定安全技术

站点到站点 VPN 支持 IPSec 技术，而远程访问 VPN 支持 SSL 和 IPSec 技术。

STEP 6 | 决定是单个用户还是多个用户需要 **VPN**

在站点到站点 VPN 中，不允许多个用户；然而，在远程访问 VPN 中，允许多个用户。

配置 IPSec VPN 隧道（站点到站点）

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

要设置站点到站点 VPN：

- 请确保以太网接口、虚拟路由器和区域均已正确配置。有关更多信息，请参阅 配置接口和区域。
- 创建隧道接口。理想的情况是，将隧道接口放在一个单独区域，以便隧道流量可以使用不同的策略。
- 设置静态路由或指定路由协议，以将流量重定向到 VPN 隧道。要支持动态路由协议（支持 OSPF、BGP、RIP），必须为隧道接口分配 IP 地址。
- 定义 IKE 网关在 VPN 隧道各端的对等设备之间建立通信；还定义加密配置文件指定用于标识、身份验证和加密的协议和算法，用来在 IKEv1 阶段 1 中建立 VPN 隧道。请参阅设置 IKE 网关和定义 IKE 加密配置文件。
- 配置建立 IPSec 连接在整个 VPN 隧道传输数据所需的参数；请参阅 建立 IPSec 隧道。对于 IKEv1 阶段 2，请参阅定义 IPSec 加密配置文件。
- （可选）指定防火墙监控 IPSec 隧道的方式。请参阅监控 IPSec VPN 隧道 。
- 定义筛选和检查流量的安全策略。

如果安全规则库的结尾是拒绝规则，则除非另行允许，否则阻止区域内通信。必须在拒绝规则上方显式包括允许 *IKE* 和 *IPSec* 应用程序的规则。

如果您的 *VPN* 流量通过（不是始发或终止）*PA-7000* 系列或 *PA-5200* 系列防火墙，请配置双向安全策略规则以允许 *ESP* 或 *AH* 流量在两个方向流动。

完成这些任务后，便可使用隧道。发往在策略规则中定义的区域/地址的流量根据路由表中的目标路径自动正常路由，并作为 VPN 流量进行处理。有关站点到站点 VPN 的几个示例，请参阅站点到站点 VPN 配置示例。

设置 IKE 网关

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

要建立 VPN 隧道，VPN 对等设备或网关必须使用预共享密钥或数字证书进行相互身份验证，并在其中建立安全通道以协商用于保护各端主机之间流量的 IPSec 安全关联 (SA)。

STEP 1 | 定义 IKE 网关。

1. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateways**（**IKE** 网关）， **Add**（添加）网关，然后输入网关 **Name**（名称）（**General**（常规）选项卡）。
2. 设置 **Version**（版本）为 **IKEv1 only mode**（仅 **IKEv1** 模式）、**IKEv2 only mode**（仅 **IKEv2** 模式）或 **IKEv2 preferred mode**（**IKEv2** 首选模式）。IKE 网关将在此处指定的模式下开始与对等设备的协商。如果您选择 **IKEv2 preferred mode**（**IKEv2** 首选模式），这两个对等设备将使用 IKEv2，但远程对等设备要支持 IKEv2，否则它们将使用 IKEv1。

   选中的 **Version**（版本）还决定了您可以使用 **Advanced Options**（高级选项）选项卡上的哪些选项。

STEP 2 | 建立隧道（网关）的本地端点。

1. 选择 **Address Type**（地址类型）：**IPv4** 或 **IPv6**。
2. 在本地网关所在的防火墙上选择物理出站 **Interface**（接口）。
3. 从 **Local IP Address**（本地 **IP** 地址）列表中选择 VPN 连接将用作端点的 IP 地址；这是面向外部的接口，且具有防火墙上公开路由 IP 地址。

STEP 3 | 在隧道（网关）远端建立对等设备。

从 **Peer IP Address Type**（对端 **IP** 地址类型）选择以下其中一个并输入对端的相应信息：

- **IP** — 输入 **Peer Address**（对端地址）作为 IPv4 或 IPv6 地址，或输入 IPv4 或 IPv6 地址的地址对象。
- **FQDN** — 输入 **Peer Address**（对端地址）作为 FQDN 字符串或是使用 FQDN 字符串的地址对象。如果 FQDN 或 FQDN 地址对象解析为多个 IP 地址，则防火墙将从与 IKE 网关的地址类型（IPv4 或 IPv6）匹配的一组地址中选择首选地址，如下所示：
  - 如果未协商 IKE 安全关联 (SA)，则首选地址为具有最小值的 IP 地址。
  - 如果 IKE 网关使用返回地址集中的地址，则防火墙选择此地址（无论其是否是集中最小的地址）。
  - 如果 IKE 网关使用非返回地址集中的地址，则防火墙选择一个新地址，这是集中最小的地址。
- **Dynamic**（动态） — 如果对端 IP 地址或 FQDN 值未知，请选择 **Dynamic**（动态），此后，对等设备将启动协商。

使用 *FQDN* 或 *FQDN* 地址对象可以减少对端受动态 *IP* 地址变更影响的环境中的问题（否则，需要您重新配置此 *IKE* 网关对端地址）。

STEP 4 | 指定验证对等设备的方式：

选择 **Authentication**（身份验证）方法：**Pre-Shared Key**（预共享密钥）或 **Certificate**（证书）。如果您选择预共享密钥，请前进至下一步。如果选择证书，请跳到步骤 6：配置基于证书的身份验证。

STEP 5 | 配置预共享密钥。

1. 输入一个 **Pre-shared Key**（预共享密钥）作为整个隧道内身份验证的安全密钥。重新将此值输入到 **Confirm Pre-shared Key**（确认预共享密钥）。最多使用 255 个 ASCII 或非 ASCII 字符。

   生成一个字典式攻击很难破解的密钥；如有必要，请使用预共享密钥生成器。

2. 对于 **Local Identification**（本地标识），请从以下类型中进行选择，然后输入您确定的值：**FQDN (hostname)**（主机名）、**IP address**（**IP** 地址）、**KEYID (binary format ID string in HEX)**（以十六进制表示的二进制格式 **ID** 字符串）、和**User FQDN (email address)**（用户 **FQDN**（电子邮件地址））。本地标识用于定义本地网关的格式和标识。如果没有指定值，则将使用本地 IP 地址作为本地标识值。
3. 对于 **Peer Identification**（对端标识），请从以下类型中进行选择，然后输入您确定的值：**FQDN (hostname)**（主机名）、**IP address**（**IP** 地址）、**KEYID (binary format ID string in HEX)**（以十六进制表示的二进制格式 **ID** 字符串）、和**User FQDN (email address)**（用户 **FQDN**（电子邮件地址））。对等设备标识用于定义对等设备网关的格式和标识。如果没有指定值，则将使用对端 IP 地址作为对等设备标识值。
4. 执行步骤 7（配置网关的高级选项）。

STEP 6 | 配置基于证书的身份验证。

如果您选择 **Certificate**（证书）作为对隧道另一端对等设备网关进行身份验证的方法，请执行此过程的剩余步骤。

1. 选择防火墙上已存在的 **Local Certificate**（本地证书），**Import**（导入）证书，或 **Generate**（生成）新证书。
   - 如果您需要 **Import**（导入）证书，则首先请导入证书以对 IKEv2 网关进行身份验证，然后返回到此任务。
   - 如果您想 **Generate**（生成）新证书，则首先请在防火墙上生成证书，然后返回到此任务。
2. （可选）启用（选择）**HTTP Certificate Exchange**（**HTTP** 证书交换） 以配置哈希和 URL（仅限 IKEv2）。对于 HTTP 证书交换，请输入 **Certificate URL**（证书 **URL**）。有关更多信息，请参阅哈希和 URL 证书交换。
3. 选择 **Local Identification**（本地身标识）类型 — **Distinguished Name (Subject) FQDN (hostname)**（可分辨名称（主题）**FQDN**（主机名）、**IP address**（**IP** 地址）或 **User FQDN (email address)**（用户 **FQDN**（电子邮件地址）），然后输入值。本地标识用于定义本地网关的格式和标识。
4. 选择 **Peer Identification**（对等设备标识）类型 — **Distinguished Name (Subject) FQDN (hostname)**（可分辨名称（主题）**FQDN**（主机名）、**IP address**（**IP** 地址）或 **User FQDN (email address)**（用户 **FQDN**（电子邮件地址）），然后输入值。对等设备标识用于定义对等设备网关的格式和标识。
5. 选择 **Peer ID Check**（对等设备 **ID** 检查）类型：
   - **Exact**（精确）— 确保本地设置和对等设备 IKE ID 有效内容精确匹配。
   - **Wildcard**（通配符）— 允许对等设备标识只匹配通配符 (*) 之前的每个字符。通配符后面的字符不需要匹配。
6. （可选）即使对等设备标识与证书中的对等设备标识不匹配，IKE SA 仍成功，请单击 **Permit peer identification and certificate payload identification mismatch**（允许对等设备标识和证书有效内容标识不匹配）。
7. 创建 **Certificate Profile**（证书配置文件）。证书配置文件包含有关如何验证对等设备网关的信息。
8. （可选）要严格控制密钥的使用方式，请单击 **Enable strict validation of peer’s extended key use**（启用对等设备扩展密钥使用的严格验证）。

STEP 7 | 配置网关的高级选项。

1. （可选）在公共选项（**Advanced Options**（高级选项））中**Enable Passive Mode**（启用被动模式），以指定防火墙仅响应 IKE 连接请求，但不启用。
2. 如果您的设备在网关之间执行 NAT，请 **Enable NAT Traversal**（启用 **NAT** 遍历），以在 IKE 和 UDP 协议中使用 UDP 封装，从而使这些协议直接通过中间 NAT 设备。
3. 如果已在步骤 1 中配置 **IKEv1 only mode**（仅 **IKEv1** 模式），请在 IKEv1 选项卡上进行以下配置：
   - 选择 **Exchange Mode**（交换模式）：**auto**（自动）、**aggressive**（主动）或**main**（主要）。将防火墙设置为使用 **auto**（自动）交换模式时，可以接受 **main**（主要）模式和 **aggressive**（主动）模式的协商请求；但是，只要有可能，该防火墙便会在 **main**（主要）模式进行交换。

     如果交换模式没有设置为 ***auto***（自动），则必须使用同一交换模式配置两个对等设备，以允许每个对等设备接受协商请求。
   - 选择现有配置文件或保留 **IKE Crypto Profile**（**IKE** 加密配置文件）列表中的默认配置文件。必要时，您可以定义 IKE 加密配置文件。
   - （只有当使用基于证书的身份验证且尚未将交换模式设置为主动模式时）单击 **Enable Fragmentation**（启用碎片）以便使防火墙能够使用 IKE 碎片。
   - 单击 **Dead Peer Detection**（失效对等设备检测），然后输入 **Interval**（间隔）（范围为 2-100 秒）。对于 **Retry**（重试），请指定与 IKE 对等设备断开连接之前允许的重试次数（范围为 2 到 100）。失效对等设备检测通过将 IKE 阶段 1 通知负载发送到对等设备并等待确认来确定处于非活动状态或不可用的 IKE 对等设备。
4. 如果在步骤 1 中已配置 **IKEv2 only mode**（仅 **IKEv2** 模式）或 **IKEv2 preferred mode**（**IKEv2** 首选模式），请在 IKEv2 选项卡上进行以下配置：
   - 选择 **IKE Crypto Profile**（**IKE** 加密配置文件），此配置文件可配置 IKE 阶段 1 选项，如 DH 组、哈希算法和 ESP 身份验证。有关 IKE 加密配置文件的信息，请参阅 IKE 阶段 1。
   - （可选）启用 **Strict Cookie Validation**（严格 **Cookie** 验证） Cookie 激活阈值和严格 Cookie 验证。
   - （可选）如果您希望网关向其网关对等设备发送消息请求以请求响应，请单击 **Enable Liveness Check**（启用活性检查）并输入 **Interval (sec)**（间隔（秒））（默认为 5 秒）。如果需要，发起者最多会尝试 10 次活性检查。如果得不到响应，发起者会关闭并删除 IKE_SA 和 CHILD_SA。发起者会发出另一个 IKE_SA_INIT 消息来从头开始。

STEP 8 | 单击 **OK**（确定）并 **Commit**（提交）更改。

导出对等设备的证书以使用哈希和 URL 进行访问

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

IKEv2 支持 哈希和 URL 证书交换 作为隧道远端的对等设备从已导入此证书的服务器获取证书的方法。执行此任务以将证书导出到该服务器。您必须已使用 **Device**（设备） > **Certificate Management**（证书管理）创建证书。

STEP 1 | 选择 **Device**（设备） > **Certificates**（证书），并且如果您的平台支持多虚拟系统，您可以为 **Location**（位置）选择相应的虚拟系统。

STEP 2 | 在 **Device Certificates**（设备证书）选项卡上，选择要 **Export**（导出）到服务器的证书。

证书的状态应为有效，并且未到期。防火墙不会阻止您导出无效证书。

STEP 3 | 对于 **File Format**（文件格式），请选择 **Binary Encoded Certificate (DER)**（二进制编码证书 **(DER)**）。

STEP 4 | 保留 **Export private key**（导出私钥）的未选中状态。无需为哈希和 URL 导出私钥。

STEP 5 | 单击 **OK**（确定）。

导入证书以进行 IKEv2 网关验证

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

如果您要对 IKEv2 网关的对等设备进行身份验证，并且防火墙上没有使用过本地证书，或者您想从其他位置导入证书，请执行此任务。

此任务假设您已选择 **Network**（网络） > **IKE Gateways**（**IKE** 网关），已添加网关，并已为 **Local Certificate**（本地证书）单击 **Import**（导入）。

STEP 1 | 导入证书。

1. 选择 **Network**（网络） > **IKE Gateways**（**IKE** 网关），**Add**（添加）网关，然后在 **General**（常规）选项卡上为 **Authentication**（身份验证）选择 **Certificate**（证书）。对于 **Local Certificate**（本地证书），请单击 **Import**（导入）。
2. 在“导入证书”窗口中，为您要导入的证书输入 **Certificate Name**（证书名称）。
3. 如果要在多个虚拟系统间共享该证书，请选择 **Shared**（共享）。
4. 对于 **Certificate File**（证书文件），请单击 **Browse**（浏览）找到此证书文件。单击文件名并单击 **Open**（打开），此操作可填充 **Certificate File**（证书文件）字段。
5. 对于 **File Format**（文件格式），请选择下列其中一种：
   - **Base64** 编码证书 **(PEM)** — 包含证书，但不含密钥。这是明文的。
   - 加密私钥和证书 **(PKCS12)** — 包含证书和密钥。
6. 如果密钥所在文件与证书文件不是同一文件，请选择 **Import private key**（导入私钥）。密钥可选，但以下情况例外：
   - 如果将 **File Format**（文件格式）设置为 **PEM**，请导入密钥。通过单击 **Browse**（浏览）并浏览到要导入的密钥文件来输入 **Key file**（密钥文件）。
   - 输入 **Passphrase**（密码）和 **Confirm Passphrase**（确认密码）。
7. 单击 **OK**（确定）。

STEP 2 | 继续下一个任务。

步骤配置基于证书的身份验证。

更改 IKEv2 的密钥有效期或身份验证间隔

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

此任务为可选任务，IKEv2 IKE SA 密钥更新生命周期的默认设置为 8 小时。IKEv2 身份验证倍数的默认设置为 0，表示禁用重新验证功能。有关详细信息，请参阅 SA 密钥有效期和重新验证间隔。

要更改默认值，请执行以下任务。先决条件是已存在 IKE 加密配置文件。

STEP 1 | 更改 IKE 加密配置文件的 SA 密钥有效期或身份验证间隔

1. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Crypto**（**IKE** 加密），然后选择适用于本地网关的 IKE 加密配置文件。
2. 对于 **Key Lifetime**（密钥有效期），请选择单位（**Seconds**（秒）、**Minutes**（分钟）、**Hours**（小时）或 **Days**（天））并输入值。最短时间为 3 分钟。
3. 对于 **IKE Authentication Multiple**（**IKE** 身份验证倍数），请输入一个值，此值乘以生命周期可确定重新验证间隔。

STEP 2 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

更改 IKEv2 的 Cookie 激活阈值

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

如果需要 Cookie 验证前，您希望防火墙的阈值不同于 500 半开 SA 会话数的默认设置，请执行以下任务。有关 Cookie 验证的详细信息，请参阅 Cookie 激活阈值和严格 Cookie 验证。

STEP 1 | 更改 Cookie 激活阈值。

1. 选择 **Device**（设备） > **Setup**（设置） > **Session**（会话），然后编辑 VPN 会话设置。对于 **Cookie Activation Threshold**（**Cookie** 激活阈值），请输入响应者从发起者请求 Cookie 之前允许的最大半开 SA 数量（范围为 0-65,535，默认为 500）。
2. 单击 **OK**（确定）。

STEP 2 | 提交更改。

单击 **OK**（确定）和 **Commit**（提交）。

配置 IKEv2 流量选择器

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

在 IKEv2 中，您可以配置流量选择器，这是 IKE 协商期间使用的网络流量的组件。流量选择器在 CHILD_SA（隧道创建）阶段 2 期间用以设置隧道和确定允许哪些流量通过此隧道。这两个 IKE 网关对等设备必须协商并在流量选择器上达成一致；否则，其中一侧对等设备会缩小地址范围来达成一致。一个 IKE 连接可以有多个隧道；例如，您可以为各部门分配不同的隧道来隔离流量。流量分离还允许实施 QoS 之类的功能。使用以下工作流可配置流量选择器。

STEP 1 | 选择 **Network**（网络） > **IPSec Tunnels**（**IPSec** 隧道） > **Proxy IDs**（代理 **ID**）。

STEP 2 | 选择 **IPv4** 或 **Ipv6** 选项卡。

STEP 3 | 单击 **Add**（添加），然后在 **Proxy ID**（代理 **ID**）字段中输入 **Name**（名称）。

STEP 4 | 在 **Local**（本地）字段中，输入 **Source IP Address**（源 **IP** 地址）。

STEP 5 | 在 **Remote**（远程）字段中输入 **Destination IP Address**（目标 **IP** 地址）。

STEP 6 | 在 **Protocol**（协议）字段中，选择传输协议（**TCP** 或 **UDP**）。

STEP 7 | 单击 **OK**（确定）。

定义加密配置文件

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

加密配置文件指定用于在两个 IKE 对等设备之间进行身份验证和/或加密的密码，以及密钥有效期。每个再协商之间的时间段称为生命周期；当指定的时间段到期后，防火墙重新协商一组新的密钥。

为了保护 VPN 隧道之间的通信，防火墙需要 IKE 和 IPSec 加密配置文件来分别完成 IKE 阶段 1 和阶段 2 协商。防火墙包含现成的默认 IKE 加密配置文件和默认 IPSec 加密配置文件。

- 定义 IKE 加密配置文件
- 定义 IPSec 加密配置文件

定义 IKE 加密配置文件

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

IKE 加密配置文件用于设置在 IKE 阶段 1 的密钥交换过程中使用的加密和身份验证算法，密钥有效期指定密钥的有效时间长度。要调用配置文件，必须将其附加到 IKE 网关配置。

将 *IKE* 网关的 ***Peer IP Address Type***（对等 ***IP*** 地址类型）配置为 ***Dynamic***（动态），且已应用 *IKEv1* 主模式或 *IKEv2* 时，同一接口或本地 *IP* 地址上配置的所有 *IKE* 网关均必须使用相同的加密配置文件。如果网关上的加密配置文件相同，尽管初始连接可能在不同的网关上启动，但当交换预共享密钥或证书和对等 *ID* 时，连接将转移到正确的网关。

无论您的 VPN 对等设备是否来自同一供应商，VPN 对等设备都必须配置相同的 IKE 参数才能成功执行 IKE 协商。

成功的 IKE 协商需要匹配以下参数：

- 密钥交换 DH 组
- 加密算法
- 认证算法

例如，如果您已将 VPN 对等设备 1 配置为使用 **group20** 作为 DH 组，使用 **sha384** 进行身份验证，并使用 **aes-256-gcm** 进行加密。然后，要与其建立 IPSec 隧道的 VPN 对等设备 2 也应配置相同的值。

- PAN-OS 10.1 及更高版本和 Prisma Access（Panorama 管理）
- #unique_39

定义 IPSec 加密配置文件

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

IPSec 加密配置文件在 IKE 阶段 2 中调用。它指定了当使用自动密钥 IKE 自动为 IKE SA 生成密钥时如何保护隧道内的数据。

无论您的 VPN 对等设备是否来自同一供应商，VPN 对等设备都必须配置相同的 IPSec 参数才能成功执行 IPSec 协商。

当 VPN 对等设备之间以下参数匹配时，IPSec 协商将成功：

- IPSec 协议（ESP 或 AH）
- 用于密钥交换的 DH 组（或 PFS）
- 加密算法
- 认证算法

例如，如果您已将 VPN 对等设备 1 配置为使用 **ESP** 作为 IPSec 协议，使用 **group20** 作为 DH 组，使用 **sha384** 进行身份验证，使用 **aes-256-gcm** 进行加密。然后，要与其建立 IPSec 隧道的 VPN 对等设备 2 也应配置完全相同的值。

默认情况下，IPSec 隧道上启用完美前向保密 (PFS) 以生成更加随机的密钥。PFS 通过在 IPSec SA 协商期间执行额外的密钥交换来实现此目的，生成新的共享密钥并将其组合到新的 IPSec SA 密钥中。配置 PFS 时，请确保两个 VPN 对等设备具有相同的 PFS 配置。IPSec SA 协商失败将导致 IPSec 隧道建立失败。

- PAN-OS 10.1 及更高版本和 Prisma Access（Panorama 管理）
- Prisma Access（云管理）

建立 IPSec 隧道

在何处可以使用？	需要提供什么？
• Prisma Access（Prisma Access 尚不支持 IPSec 隧道传输模式） • PAN-OS	无需许可证

IPSec 是一套用于保护对等设备之间通信的协议。在 IPSec 中，您可以配置各种设置，例如加密和身份验证算法以及安全关联超时。其中一种这样的配置是 IPSec 模式 — 隧道模式或传输模式。

配置 IPSec 隧道时，可以选择 IPSec 模式为隧道模式或传输模式来建立安全连接。这意味着，您可以选择在隧道模式或传输模式下加密或验证数据包。默认情况下，PAN-OS® 支持隧道模式，在数据（IP 数据包）穿过隧道时对数据（IP 数据包）进行身份验证或加密。从 PAN OS 11.0.0 开始，您可以使用运输模式。

隧道模式和传输模式的差异

隧道模式	传输模式
加密整个数据包，包括 IP 标头。加密后，会向数据包添加一个新 IP 标头。	仅加密负载，同时保留原始 IP 标头。
隧道监控机制使用隧道接口 IP 地址。	隧道监控机制自动使用物理接口的 IP 地址（网关接口 IP 地址），而忽略隧道接口 IP 地址。
支持双重封装。	不支持双重封装。
此模式通常用于点对点通信。	此模式通常用于主机间的通信。

设置 IPsec 隧道（隧道模式）

在何处可以使用？	需要提供什么？
• Prisma Access • PAN-OS	无需许可证

IPSec 隧道配置可让您对遍历隧道的数据（IP 数据包）进行身份验证和/或加密。

如果设置防火墙使用支持基于策略的 VPN 的对等设备，必须定义代理 ID。支持基于策略的 VPN 的设备使用特定安全规则/策略或访问列表（源地址、目标地址和端口），允许感兴趣的流量通过 IPSec 隧道。在快速模式或 IKE 阶段 2 协商过程中会引用这些规则，并且在该过程的第一或第二条消息中将其作为代理 ID 进行交换。因此，如果配置防火墙使用基于策略的 VPN 对等设备，对于成功的阶段 2 协商，必须定义代理 ID，以便使两个对等设备上的设置相同。如果尚未配置代理 ID，由于防火墙支持基于策略的 VPN，因此用作代理 ID 的默认值为源 IP 地址：0.0.0.0/0，目标 IP 地址：0.0.0.0/0，应用领域：任何领域；并且，当与对等设备交换这些值时，它会导致无法建立 VPN 连接。

要成功建立 IPSec 隧道，IKE 和 IPSec 协商都应该成功：

- 仅当两个 VPN 对等设备交换配置的相同 IKE 参数时，IKE 协商才会成功。
- 只有当两个 VPN 对等设备交换配置的相同 IPSec 参数时，IPSec 协商才会成功。
- PAN-OS 10.1 及更高版本
- #unique_43
- #unique_44

设置 IPsec 隧道（传输模式）

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

传输模式是从 PAN-OS 11.0.0 版本开始的新功能，支持：

- 仅 IPv4 地址。
- 仅封装安全负载 (ESP) 协议。
- 仅 IKEv2。
- DH 组 20，用于 Diffie-Hellman (DH) 组和 PFS。
- 仅 GCM 模式下采用 256 位密钥的 AES。

您可以根据自己的网络需求选择 IPsec 模式：

- 如果要加密在下一代防火墙和隧道端点之间交换的管理平面协议（例如 BGP）数据包，则必须配置 IPSec 传输模式。传输模式允许您使用最可靠的协议对控制流量（例如路由协议和信号化消息）进行加密。利用传输模式，您可以加密属于防火墙 IP 地址的点对点流量。
- 如果要加密在下一代防火墙和隧道端点之间交换的数据平面流量，则必须配置 IPSec 隧道模式。

启用传输模式之前的注意事项：

- 启用 NAT-T 时，无法选择传输模式。
- 您无法在环路接口上配置具有传输模式的 IPSec 隧道的 IKE 网关。

- IPSec 传输模式不使用代理 ID 设置进行协商。因此，您无法在传输模式下配置代理 ID。如果您尝试通过任何其他方法配置代理 ID，它将自动替换为 0.0.0.0/0。
- 您只能通过 **auto-key** 密钥交换方式使用传输模式。
- 如果您配置没有 IPsec 隧道的 IKE 网关，则在默认情况下，IKE 会协商隧道模式的子安全关联 (SA)。
- 在没有 GRE 封装的 IPSec 传输模式下，不要通过关联的隧道接口路由用户流量。在物理接口（例如以太网 1/1）而不是隧道接口上配置控制协议（如 BGP 对等会话）。虽然 BGP 路由的 IPsec 隧道模式适用于隧道接口，但 BGP 路由的 IPsec 传输模式仅适用于物理接口。
- IPsec 隧道默认以 **Tunnel**（隧道）模式运行。
- 应在 **Transport**（传输）模式下启用 **Add GRE Encapsulation**（添加 **GRE** 封装），以封装组播数据包。

由于 PAN-OS 10.2 及更早版本不支持传输模式，因此降级到先前版本会导致兼容性问题。降级之前，必须手动删除任何传输模式隧道或切换到隧道模式。否则，降级将导致发生故障。

- PAN-OS 11.0 及更高版本

监控 IPSec VPN 隧道

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

要提供不间断的 VPN 服务，可以在防火墙上使用失效对等设备检测功能和隧道监控功能。还可以监控隧道的状态。这些监控任务在下面几个部分进行介绍：

- 定义隧道监控配置文件
- 查看隧道状态

为了排除故障，您可以启用/禁用，刷新或重新启动 IKE 网关或 IPSec 隧道。

定义隧道监控配置文件

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

隧道监控配置文件可让您验证 VPN 对等设备之间的连接；您可以配置隧道接口以指定的时间间隔 Ping 目标 IP 地址，并指定隧道之间通信中断后要采取的操作。

STEP 1 | 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **Monitor**（监控）。可以使用默认隧道监控配置文件。

STEP 2 | 单击 **Add**（添加），然后输入配置文件的 **Name**（名称）。

STEP 3 | 选择无法访问目标 IP 地址时应采取的 **Action**（操作）。

- **Wait Recover**（等待恢复）— 防火墙等待隧道恢复。隧道将继续在路由决策中使用隧道接口，就像隧道仍处于活动状态。
- **Fail Over**（故障转移）— 强制流量转移到备份路径（如可用）。防火墙禁用隧道接口，从而禁用路由表中的任何路由使用接口。

在这两种情况下，防火墙尝试通过协商新的 IPSec 密钥加快恢复。

STEP 4 | 指定触发指定操作的 **Interval (sec)**（间隔（秒））和 **Threshold**（阈值）。

- **Threshold**（阀值）指定在执行指定操作之前等待的检测信号数（范围为 2-100；默认为 5）。
- **Interval (sec)**（间隔（秒））指定检测信号之间的时间（范围为 2-10，默认为 3）。

STEP 5 | 将监控配置文件附加到 IPSec 隧道配置。请参阅启用隧道监控。

查看隧道状态

在何处可以使用？	需要提供什么？
• PAN-OS • Cloud Management	❑ 无需许可证 ❑ NGFW Premium 许可证的 AIOps

隧道状态可让您知道是否已建立有效的 IKE 阶段 1 和阶段 2 SA，以及隧道接口是否已启用且是否可用于传递流量。

由于隧道接口是逻辑接口，因此它不能表示物理链路状态。因此，必须启用隧道监控，使隧道接口可以验证到 IP 地址的连接，并确定路径是否仍然可用。如果 IP 地址无法访问，防火墙将等待隧道恢复或故障转移。当执行故障转移时，现有的隧道断开，并触发路由更改建立新的隧道和重定向流量。

- PAN-OS
- 云端管理

查看 IPSec VPN 隧道状态

STEP 1 | 选择**Network**（网络） > **IPSec Tunnels**（**IPSec** 隧道）。

STEP 2 | 查看 **Tunnel Status**（隧道状态）。

- 绿色表示 IPSec SA 隧道有效。
- 红色表示 IPSec SA 不可用或已过期。

STEP 3 | 查看 **IKE Gateway Status**（**IKE** 网关状态）。

- 绿色表示 IKE 阶段 1 SA 有效。
- 红色表示该 IKE 阶段 1 SA 不可用或已过期。

STEP 4 | 查看 **Tunnel Interface Status**（隧道接口状态）。

- 绿色表示隧道接口已打开。
- 红色表示隧道接口已关闭，因为隧道监控已启用且状态为 DOWN。

要对尚未启动的 VPN 隧道进行故障排除，请参阅 解释 VPN 错误消息。

查看 IPSec VPN 隧道状态

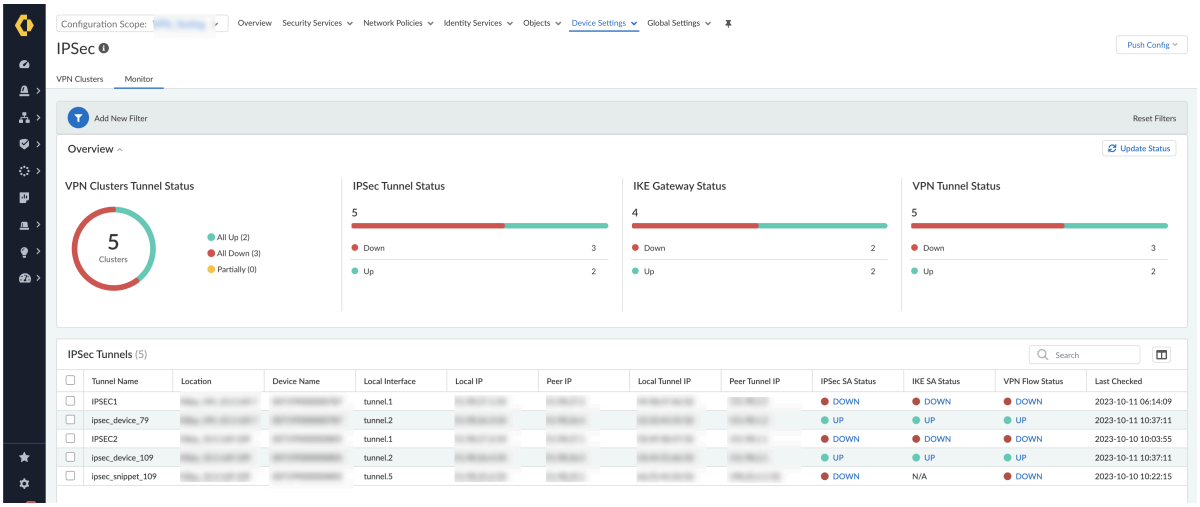
STEP 1 | 登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理）> **Configuration**（配置）> **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）> **Device Settings**（设备设置）> **IPSec Tunnels**（**IPSec** 隧道），然后选择 **Monitor**（监控）。

STEP 3 | 选择 **Configuration Scope**（配置范围）以查看 IPSec VPN 隧道状态。您可以从 **Folders**（文件夹）中选择文件夹或防火墙来监控在防火墙上创建的 IPSec VPN 隧道：

- 要查看所有防火墙上 IPSec 隧道的状态，请选择 **All Firewalls**（所有防火墙）文件夹。
- 要查看与文件夹关联的防火墙组的 IPSec 隧道的状态，请选择特定文件夹。
- 要查看特定防火墙上 IPSec 隧道的状态，请选择该防火墙。

- 如果您使用 *AutoVPN* 创建 *VPN* 集群，则无法监控这些防火墙的 *IPSec* 隧道状态。
- 您只能监控本地防火墙，而不能监控 *Prisma Access* 管理的组件。
- 在全局和片段级别禁用监视。因此，您可以在全局或片段配置范围内创建 *IPSec* 隧道，但只能在文件夹或防火墙级别监控 *IPSec* 隧道。



STEP 4 | 查看 **VPN Cluster Tunnel Status**（**VPN** 集群隧道状态），该界面会以图形方式显示启动的隧道数量、关闭的隧道数量以及部分启动的隧道数量。

STEP 5 | 在 **IPSec Tunnels**（**IPSec** 隧道）中查看 **IPSec SA Status**（**IPSec SA** 状态）。

- 绿色 **(UP)** 表示有效的 IPSec SA 隧道。选择 **UP** 可以查看 IPSec 隧道的详细信息。
- 红色 **(DOWN)** 表示 IPSec SA 不可用或已过期。选择 **DOWN** 可查看解释失败原因的详细信息。

STEP 6 | 在 **IPSec Tunnels**（**IPSec** 隧道）中查看 **IKE SA Status**（**IKE SA** 状态）。

- 绿色 (**UP**) 表示 IKE 阶段 1 SA 有效。选择 **UP** 可查看有关 IKE 网关的详细信息。
- 红色 (**DOWN**) 表示该 IKE 阶段 1 SA 不可用或已过期。选择 **DOWN** 可查看解释失败原因的详细信息。

STEP 7 | 查看 **VPN Flow Status**（**VPN** 流状态）以获取 **IPSec Tunnels**（**IPSec** 隧道）中的 VPN 流量信息。

- 绿色 (**UP**) 表示 IPSec 隧道已启动。选择 **UP** 可查看有关 VPN 流量的详细信息。
- 红色 (**DOWN**) 表示 IPSec 隧道已关闭。选择 **DOWN** 可查看解释失败原因的详细信息。

STEP 8 | 选择 **Add New Filter**（添加新过滤器），然后选择字段以查看基于所选字段的结果。例如，通过从列表中选择 **Device Name**（设备名称） 可 **Add New Filter**（添加新过滤器），以查看所选设备的 IPSec 隧道状态。

选择 **Reset Filters**（重置过滤器）Reset Filters可删除一个或多个过滤器。

STEP 9 | 选择 **Update Status**（更新状态）可更新该级别（防火墙、文件夹或所有防火墙）中存在的所有 IPSec 隧道监控数据。

启用、禁用、刷新或重启 IKE 网关或 IPsec 隧道

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

您可以启用、禁用、刷新或重新启动 IKE 网关或 VPN 隧道来简化故障诊断。

- 启用或禁用 IKE 网关或 IPSec 隧道
- 刷新或重新启动 IKE 网关或 IPSec 隧道

启用或禁用 IKE 网关或 IPSec 隧道

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

您可以启用或禁用 IKE 网关或 IPSec 隧道来简化故障诊断。

启用或禁用 IKE 网关。

1. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateways**（**IKE** 网关），然后选择您要启用或禁用的网关。
2. 在屏幕底部单击 **Enable**（启用）或 **Disable**（禁用）。

启用或禁用 IPSec 隧道。

1. 选择 **Network**（网络） > **IPSec Tunnels**（**IPSec** 隧道），然后选择您要启用或禁用的隧道。
2. 在屏幕底部单击 **Enable**（启用）或 **Disable**（禁用）。

刷新或重新启动 IKE 网关或 IPSec 隧道

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

您可以刷新或重新启动 IKE 网关或 IPSec 隧道。IKE 网关和 IPSec 隧道的刷新和重新启动行为如下所示：

阶段	刷新	重新启动
IKE 网关（IKE 阶段 1）	为所选 IKE 网关更新屏幕上的统计信息。 等同于在 CLI 中发送第二个 `show` 命令（在初始 `show` 命令之后）。	重新启动所选 IKE 网关。 **IKEv2**：同时重新启动所有关联的子 IPSec 安全关联 (SA)。 **IKEv1**：不重新启动关联的 IPSec SA。 重新启动会干扰所有现有会话。 等同于在 CLI 中发送 **`clear`**、**`test`**、**`show`** 命令序列。
IPSec 隧道（IKE 阶段 2）	为所选 IPSec 隧道更新屏幕上的统计信息。 等同于在 CLI 中发送第二个 `show` 命令（在初始 `show` 命令之后）。	重新启动 IPSec 隧道。 重新启动会干扰所有现有会话。 等同于在 CLI 中发送 **`clear`**、**`test`**、**`show`** 命令序列。

请注意，重新启动 IKE 网关的结果取决于它是 IKEv1 还是 IKEv2。

刷新或重新启动 IKE 网关。

1. 选择 **Network**（网络）> **IPSec Tunnels**（**IPSec** 隧道），然后为您要刷新或重新启动的网关选择隧道。
2. 在针对该隧道的行内，在“状态”列中单击 **IKE Info**（**IKE** 信息）。
3. 在 IKE 信息屏幕的底部，单击您想执行的操作：
   - **Refresh**（刷新）— 更新屏幕上的统计信息。
   - **Restart**（重新启动）— 清除 SA，因此 IKE 协商重新开始和隧道重新创建前会丢弃流量。

刷新或重新启动 IPSec 隧道。

因为使用隧道监视器监控隧道状态，或使用外部网络监视器监控通过 IPSec 隧道的网络连接，因此您可以确定隧道需要刷新或重新启动。

1. 选择 **Network**（网络）> **IPSec TunnelsIPSec** 隧道），然后选择您要刷新或重新启动的隧道。
2. 在针对该隧道的行内，在“状态”列中单击 **Tunnel Info**（隧道信息）。
3. 在隧道信息屏幕的底部，单击您想执行的操作：
   - **Refresh**（刷新）— 更新屏幕上的统计信息。
   - **Restart**（重新启动）— 清除 SA，因此 IKE 协商重新开始和隧道重新创建前会丢弃流量。

站点到站点 VPN 配置示例

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

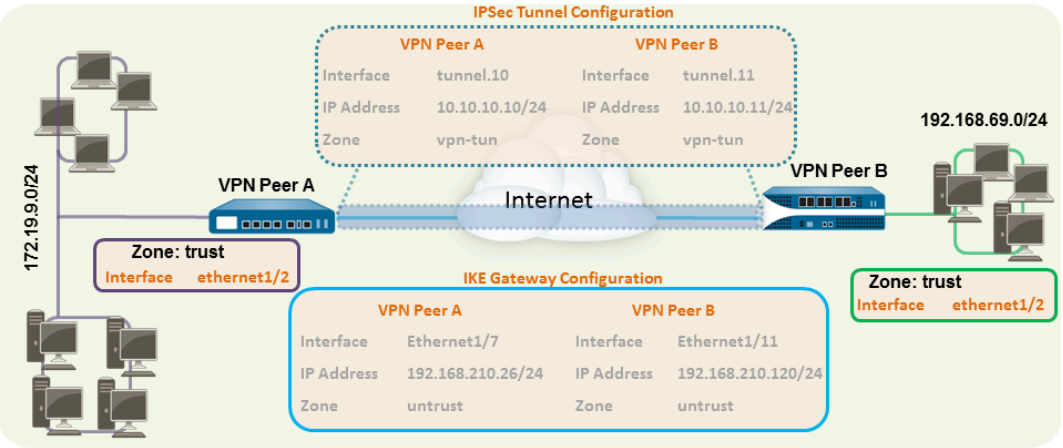
以下部分提供了配置一些常见 VPN 部署的说明：

- 使用静态路由的站点到站点 VPN
- 使用 OSPF 的站点与站点 VPN
- 使用静态和动态路由的站点到站点 VPN

使用静态路由的站点到站点 VPN

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

下例显示了使用静态路由的两个站点之间的 VPN 连接。不使用动态路由，VPN 对等设备 A 和 VPN 对等设备 B 上的隧道接口不需要 IP 地址，因为防火墙自动将隧道接口用作在站点之间路由流量的下一个跃点。但是，要启用隧道监控，要为每个隧道接口分配一个静态 IP 地址。



STEP 1 | 配置第 3 层接口。

此接口用于 IKE 阶段 1 隧道。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后选择要为 VPN 配置的接口。
2. 从 **Interface Type**（接口类型）中选择 **Layer3**（第三层） 。
3. 在 **Config**（配置）选项卡上，选择接口所属的 **Security Zone**（安全区域）：
   - 接口必须可从信任网络以外的区域访问。考虑创建专用的 VPN 区域以便深入了解和控制 VPN 流量。
   - 如果尚未创建区域，可从 **Security Zone**（安全区域）中选择 **New Zone**（新建区域），并定义新区域的 **Name**（名称），然后单击 **OK**（确定）。
4. 选择要使用的 **Virtual Router**（虚拟路由器）。
5. 若要向接口分配 IP 地址，请选择 **IPv4** 选项卡，单击 IP 部分中的**Add (**添加**)**，然后输入要分配给接口的 IP 地址和网络掩码，例如 192.168.210.26/24。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：
   - **Interface**（接口）— ethernet1/7
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 192.168.210.26/24

   VPN 对等设备 B 配置如下：
   - **Interface**（接口）— ethernet1/11
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 192.168.210.120/24

STEP 2 | 创建隧道接口，并将其附加到虚拟路由器和安全区域。

1. 选择 **Network**（网络 ） > **Interfaces**（接口） > **Tunnel**（隧道），并单击 **Add**（添加）。
2. 在 **Interface Name**（接口名称）字段中，指定数字后缀；例如 **.1**。
3. 在 **Config**（配置）选项卡中，按下列方法展开 **Security Zone**（安全区域）以定义区域：
   - 要将信任区域用作隧道的终止点，请选择该区域。
   - （推荐）要为 VPN 隧道终止创建单独区域，请单击 **New Zone**（新区域）。在“区域”对话框中，定义新区域的 **Name**（名称）（如 *vpn-tun*），然后单击 **OK**（确定）。
4. 选择 **Virtual Router**（虚拟路由器）。
5. （可选）要向隧道接口分配 IP 地址，选择 **IPv4** 或 **IPv6** 选项卡，单击 IP 部分中的 **Add**（添加），然后输入要分配给接口的 IP 地址和网络掩码。

   使用静态路由，隧道接口不需要 IP 地址。对于发往指定子网/IP 地址的流量，隧道接口将自动成为下一个跃点。如果要启用隧道监控，请考虑添加 IP 地址。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：
   - **Interface**（接口）— tunnel.10
   - **Security Zone**（安全区域）— vpn_tun
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 172.19.9.2/24

   VPN 对等设备 B 配置如下：
   - **Interface**（接口）— tunnel.11
   - **Security Zone**（安全区域）— vpn_tun
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 192.168.69.2/24

STEP 3 | 在虚拟路由器上，将静态路由配置为目标子网。

1. 选择 **Network**（网络） > **Virtual Router**（虚拟路由器）并单击在上述步骤中定义的路由器。
2. 选择 **Static Route**（静态路由），并单击 **Add**（添加），然后输入新路由以访问子网（位于隧道的另一端）。

   在本例中，VPN 对等设备 A 配置如下：

   - **Destination**（目标）— 192.168.69.0/24
   - **Interface**（接口）— tunnel.10

   VPN 对等设备 B 配置如下：

   - **Destination**（目标） — 172.19.9.0/24
   - **Interface**（接口）— tunnel.11

STEP 4 | 设置加密配置文件（IKE 加密配置文件用于阶段 1 和 IPSec 加密配置文件用于阶段 2）。

在两个对等设备上完成此任务，并确保设置相同的值。

1. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Crypto**（**IKE** 加密）。在本例中，我们使用默认配置文件。
2. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IPSec Crypto**（**IPSec** 加密）。在本例中，我们使用默认配置文件。

STEP 5 | 设置 IKE 网关。

1. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateway**（**IKE** 网关）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：

   - **Interface**（接口）— ethernet1/7
   - **Local IP address**（本地 **IP** 地址）— 192.168.210.26/24
   - **Peer IP type/address**（对等设备 **IP** 类型/地址）— static/192.168.210.120
   - **Preshared keys**（预共享密钥）— 输入一个值
   - **Local identification**（本地标识）— 无；这意味着将使用本地 IP 地址作为本地标识值。
   - VPN 对等设备 B 配置如下：
   - **Interface**（接口）— ethernet1/11
   - **Local IP address**（本地 **IP** 地址）— 192.168.210.120/24
   - **Peer IP type/address**（对等设备 **IP** 类型/地址）— 静态/192.168.210.26
   - **Preshared keys**（预共享密钥）— 输入与对等设备 A 相同的值
   - **Local identification**（本地标识）— 无
3. 选择 **Advanced Phase 1 Options**（高级阶段 **1** 选项），然后选择先前创建用于 IKE 阶段 1 的 IKE 加密配置文件。

STEP 6 | 建立 IPSec 隧道。

1. 选择**Network**（网络） > **IPSec Tunnels**（**IPSec** 隧道）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：

   - **Tunnel Interface**（隧道接口） — tunnel.10
   - **Type**（类型）— 自动密钥
   - **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
   - **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在步骤 4 中定义的 IPSec 加密配置文件。

   VPN 对等设备 B 配置如下：

   - **Tunnel Interface**（隧道接口） — tunnel.11
   - **Type**（类型）— 自动密钥
   - **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
   - **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在步骤 4 中定义的 IPSec 加密。
3. （可选）选择 **Show Advanced Options**（显示高级选项），并选择 **Tunnel Monitor**（隧道监控），然后指定为验证连接要 ping 的目标 IP 地址。通常，使用 VPN 对等设备的隧道接口 IP 地址。
4. （可选）要定义在建立连接失败后要采取的操作，请参阅定义隧道监控配置文件。

STEP 7 | 创建策略规则以允许站点之间的通信（子网）。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. 创建规则以允许不可信区域与 vpn-tun 区域，以及 vpn-tun 区域与不可信区域之间的流量，流量来源于指定的源和目标 IP 地址。

STEP 8 | 提交任何挂起的配置更改。

单击 **Commit**（提交）。

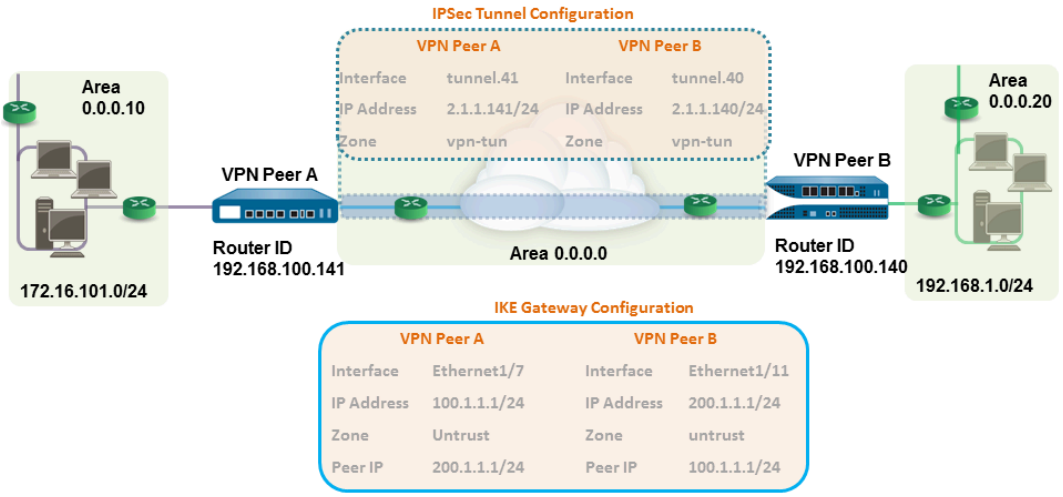
STEP 9 | 测试 VPN 连接.

另请参阅 查看隧道状态。

使用 OSPF 的站点与站点 VPN

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

在本例中，每个站点都使用 OSPF 动态路由流量。静态分配每个 VPN 对等设备的隧道 IP 地址，并用作在两个站点之间路由流量的下一个跃点。



STEP 1 | 在每个防火墙上配置第 3 层接口。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后选择要为 VPN 配置的接口。
2. 从 **Interface Type**（接口类型）列表中选择 **Layer3**（第三层） 。
3. 在 **Config**（配置）选项卡上，选择接口所属的 **Security Zone**（安全区域）：
   - 接口必须可从信任网络以外的区域访问。考虑创建专用的 VPN 区域以便深入了解和控制 VPN 流量。
   - 如果尚未创建区域，可从 **Security Zone**（安全区域）列表中选择 **New Zone**（新建区域），并定义新区域的 **Name**（名称），然后单击 **OK**（确定）。
4. 选择要使用的 **Virtual Router**（虚拟路由器）。
5. 若要向接口分配 IP 地址，请选择 **IPv4** 选项卡，单击 IP 部分中的**Add (**添加**)**，然后输入要分配给接口的 IP 地址和网络掩码，例如 192.168.210.26/24。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：
   - **Interface**（接口）— ethernet1/7
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 100.1.1.1/24

   VPN 对等设备 B 配置如下：
   - **Interface**（接口）— ethernet1/11
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 200.1.1.1/24

STEP 2 | 创建隧道接口，并将其附加到虚拟路由器和安全区域。

1. 选择 **Network**（网络 ） > **Interfaces**（接口） > **Tunnel**（隧道），并单击 **Add**（添加）。
2. 在 **Interface Name**（接口名称）字段中，指定数字后缀；例如 **.11**。
3. 在 **Config**（配置）选项卡中，按下列方法展开 **Security Zone**（安全区域）以定义区域：
   - 要将信任区域用作隧道的终止点，请选择该区域。
   - （推荐）要为 VPN 隧道终止创建单独区域，请单击 **New Zone**（新区域）。在“区域”对话框中，定义新区域的 **Name**（名称）（如 vpn-tun），然后单击 **OK**（确定）。
4. 选择 **Virtual Router**（虚拟路由器）。
5. 要向隧道接口分配 IP 地址，请选择 **IPv4** 或 **IPv6** 选项卡，单击 IP 部分中的 **Add**（添加），然后输入要分配给接口的 IP 地址和网络掩码/前缀，如 172.19.9.2/24。

   使用此 IP 地址作为将流量路由到隧道的下一个跃点 IP 地址，且也可用于监控隧道的状态。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：
   - **Interface**（接口）— tunnel.41
   - **Security Zone**（安全区域）— vpn_tun
   - **Virtual Router**（虚拟路由器）— 默认
   - **Ipv4** — 2.1.1.141/24

   VPN 对等设备 B 配置如下：
   - **Interface**（接口）—tunnel.40
   - **Security Zone**（安全区域）— vpn_tun
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** （IPv4）— 2.1.1.140/24

STEP 3 | 设置加密配置文件（IKE 加密配置文件用于阶段 1 和 IPSec 加密配置文件用于阶段 2）。

在两个对等设备上完成此任务，并确保设置相同的值。

1. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Crypto**（**IKE** 加密）。在本例中，我们使用默认配置文件。
2. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IPSec Crypto**（**IPSec** 加密）。在本例中，我们使用默认配置文件。

STEP 4 | 在虚拟路由器上设置 OSPF 配置，并将 OSPF 区域连接到防火墙的相应接口。

有关防火墙上可用 OSPF 选项的详细信息，请参阅配置 OSPF。

当两个以上的 OSPF 路由器需要交换路由信息时，可将广播用作链路类型。

1. 选择 **Network**（网络） > **Virtual Routers**（ 虚拟路由器），然后选择默认路由器或添加新路由器。
2. 选择 **OSPF**（对于 IPv4）或 **OSPFv3**（对于 Ipv6），然后选择 **Enable**（启用）。
3. 在本例中，VPN 对等设备 A 的 OSPF 配置如下：
   - **Router ID**（路由器 **ID**）：192.168.100.141
   - **Area ID**（区域 **ID**）：0.0.0.0，分配给 tunnel.1 接口，链路类型：p2p
   - **Area ID**（区域 **ID**）：0.0.0.10，分配给接口 Ethernet1/1，链路类型：广播

   VPN 对等设备 B 的 OSPF 配置如下：
   - **Router ID**（路由器 **ID**）：192.168.100.140
   - **Area ID**（区域 **ID**）：0.0.0.0，分配给 tunnel.1 接口，链路类型：p2p
   - **Area ID**（区域 **ID**）：0.0.0.20，分配给接口 Ethernet1/15，链路类型：广播

STEP 5 | 设置 IKE 网关。

本示例对于两个 VPN 对等设备使用静态 IP 地址。通常，企业办公室使用静态配置的 IP 地址，分支机构使用的 IP 地址可以是动态 IP 地址；动态 IP 地址最不适合用于配置稳定服务，如 VPN。

1. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateway**（**IKE** 网关）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：
   - **Interface**（接口）— ethernet1/7
   - **Local IP address**（本地 **IP** 地址）— 100.1.1.1/24
   - **Peer IP address**（对等设备 IP 地址）— 200.1.1.1/24
   - **Preshared keys**（预共享密钥）— 输入一个值

   VPN 对等设备 B 配置如下：
   - **Interface**（接口）— ethernet1/11
   - **Local IP address**（本地 **IP** 地址）— 200.1.1.1/24
   - **Peer IP address**（对等设备 **IP** 地址）— 100.1.1.1/24
   - **Preshared keys**（预共享密钥）— 输入与对等设备 A 相同的值
3. 选择先前创建用于 IKE 阶段 1 的 IKE 加密配置文件。

STEP 6 | 建立 IPSec 隧道。

1. 选择**Network**（网络） > **IPSec Tunnels**（**IPSec** 隧道）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：

   - **Tunnel Interface**（隧道接口）—tunnel.41
   - **Type**（类型）— 自动密钥
   - **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
   - **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在上文定义的 IKE 网关。

   VPN 对等设备 B 配置如下：

   - 隧道接口 — tunnel.40
   - **Type**（类型）— 自动密钥
   - **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
   - **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在上文定义的 IKE 网关。
3. 选择 **Show Advanced Options**（显示高级选项），并选择 **Tunnel Monitor**（隧道监控），然后指定为验证连接要 ping 的目标 IP 地址。
4. 要定义在建立连接失败后要采取的操作，请参阅定义隧道监控配置文件。

STEP 7 | 创建策略规则以允许站点之间的通信（子网）。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. 创建规则以允许不可信区域与 vpn-tun 区域，以及 vpn-tun 区域与不可信区域之间的流量，流量来源于指定的源和目标 IP 地址。

STEP 8 | 验证 OSPF 邻接并从 CLI 路由。

验证两个防火墙可以相互看作完整状态的邻居。同时确认 VPN 对等设备的隧道接口的 IP 地址和 OSPF 路由器 ID。在每个 VPN 对等设备上使用以下 CLI 命令。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface          next-AS
2.1.1.0/24              0.0.0.0                 10   Oi       6760  tunnel.41
172.16.101.0/24         0.0.0.0                 10   Oi       6854  ethernet1/1
192.168.1.0/24          2.1.1.140               20 A Oo       6754  tunnel.40
total routes shown: 3
    admin@FW-B> show routing route type ospf

    flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
           Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


    VIRTUAL ROUTER: vr1 (id 1)
      ==========
    destination             nexthop             metric flags      age   interface
    2.1.1.0/24              0.0.0.0                 10   Oi       20033 tunnel.40
    172.16.101.0/24         2.1.1.141               20   AOo      6896  tunnel.40
    192.168.1.0/24          0.0.0.0                 10   Oi       8058  ethernet1/15
    total routes shown: 3
```

STEP 9 | 测试 VPN 连接.

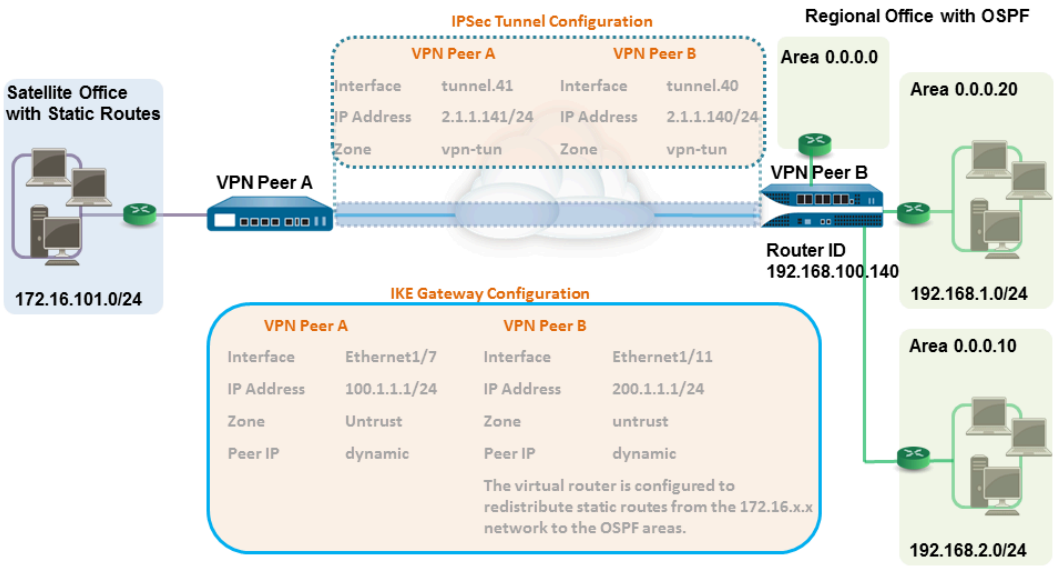
请参阅设置隧道监控和 查看隧道状态。

使用静态和动态路由的站点到站点 VPN

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

在本例中，一个站点使用静态路由，另一个站点使用 OSPF。当两个位置之间的路由协议不相同时，必须使用静态 IP 地址配置每个防火墙上的隧道接口。然后，要允许交换路由信息，必须使用重新分发配置文件配置同时参与静态和动态路由过程的防火墙。配置重新分发配置文件，启用虚拟路由器重新分发和筛选协议之间的路由 — 静态路由、连接路由和主机 — 从静态自治系统到 OSPF 自治系统。如果不配置此重新分发配置文件，则其拥有各项协议功能，并且不会与在同一虚拟路由器上运行的其他协议交换任何路由信息。

在本例中，卫星办公室拥有静态路由，且会将发往 192.168.x.x 网络的所有流量路由到 tunnel.41。VPN 对等设备 B 上的虚拟路由器同时参与静态和动态路由过程，并使用重新分发配置文件进行配置，以将静态路由传播（导出）到 OSPF 自治系统。



STEP 1 | 在每个防火墙上配置第 3 层接口。

1. 选择 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网），然后选择要为 VPN 配置的接口。
2. 从 **Interface Type**（接口类型）中选择 **Layer3**（第三层） 。
3. 在 **Config**（配置）选项卡上，选择接口所属的 **Security Zone**（安全区域）：
   - 接口必须可从信任网络以外的区域访问。考虑创建专用的 VPN 区域以便深入了解和控制 VPN 流量。
   - 如果尚未创建区域，可从 **Security Zone**（安全区域）中选择 **New Zone**（新建区域），并定义新区域的 **Name**（名称），然后单击 **OK**（确定）。
4. 选择要使用的 **Virtual Router**（虚拟路由器）。
5. 若要向接口分配 IP 地址，请选择 **IPv4** 选项卡，单击 IP 部分中的**Add (**添加**)**，然后输入要分配给接口的 IP 地址和网络掩码，例如 192.168.210.26/24。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：
   - **Interface**（接口）— ethernet1/7
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 100.1.1.1/24

   VPN 对等设备 B 配置如下：
   - **Interface**（接口）— ethernet1/11
   - **Security Zone**（安全区域）— 不可信
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** — 200.1.1.1/24

STEP 2 | 设置加密配置文件（IKE 加密配置文件用于阶段 1 和 IPSec 加密配置文件用于阶段 2）。

在两个对等设备上完成此任务，并确保设置相同的值。

1. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Crypto**（**IKE** 加密）。在本例中，我们使用默认配置文件。
2. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IPSec Crypto**（**IPSec** 加密）。在本例中，我们使用默认配置文件。

STEP 3 | 设置 IKE 网关。

使用预共享密钥，要在建立 IKE 阶段 1 隧道时添加身份验证检查，可以设置本地和对等设备标识属性，以及在 IKE 协商过程中匹配的相应值。

1. 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateway**（**IKE** 网关）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：

   - **Interface**（接口）— ethernet1/7
   - **Local IP address**（本地 **IP** 地址）— 100.1.1.1/24
   - **Peer IP type**（对等设备 **IP** 类型）— 动态
   - **Preshared keys**（预共享密钥）— 输入一个值
   - **Local identification**（本地标识）— 选择 **FQDN(hostname)**（主机名），然后输入 VPN 对等设备 A 的值。
   - **Peer identification**（对等设备标识）— 选择 **FQDN(hostname)**（主机名），然后输入 VPN 对等设备 B 的值。

   VPN 对等设备 B 配置如下：

   - **Interface**（接口）— ethernet1/11
   - **Local IP address**（本地 **IP** 地址）— 200.1.1.1/24
   - **Peer IP address**（对等设备 **IP** 地址）— 动态
   - **Preshared keys**（预共享密钥）— 输入与对等设备 A 相同的值
   - **Local identification**（本地标识）— 选择 **FQDN(hostname)**（主机名），然后输入 VPN 对等设备 B 的值
   - **Peer identification**（对等设备标识）— 选择 **FQDN(hostname)**（主机名），然后输入 VPN 对等设备 A 的值
3. 选择先前创建用于 IKE 阶段 1 的 IKE 加密配置文件。

STEP 4 | 创建隧道接口，并将其附加到虚拟路由器和安全区域。

1. 选择 **Network**（网络 ） > **Interfaces**（接口） > **Tunnel**（隧道），并单击 **Add**（添加）。
2. 在 **Interface Name**（接口名称）字段中，指定数字后缀，如 **.41**。
3. 在 **Config**（配置）选项卡中，按下列方法展开 **Security Zone**（安全区域）以定义区域：
   - 要将信任区域用作隧道的终止点，请选择该区域。
   - （推荐）要为 VPN 隧道终止创建单独区域，请单击 **New Zone**（新区域）。在“区域”对话框中，定义新区域的 **Name**（名称）（如 *vpn-tun*），然后单击 **OK**（确定）。
4. 选择 **Virtual Router**（虚拟路由器）。
5. 要向隧道接口分配 IP 地址，请选择 **IPv4** 或 **IPv6** 选项卡，单击 IP 部分中的 **Add**（添加），然后输入要分配给接口的 IP 地址和网络掩码/前缀，如 172.19.9.2/24。

   使用此 IP 地址将流量路由到隧道，并监控隧道的状态。
6. 要保存接口配置，请单击 **OK**（确定）。

   在本例中，VPN 对等设备 A 配置如下：
   - **Interface**（接口）— tunnel.41
   - **Security Zone**（安全区域）— vpn_tun
   - **Virtual Router**（虚拟路由器）— 默认
   - **Ipv4** — 2.1.1.141/24

   VPN 对等设备 B 配置如下：
   - **Interface**（接口）— tunnel.42
   - **Security Zone**（安全区域）— vpn_tun
   - **Virtual Router**（虚拟路由器）— 默认
   - **IPv4** （IPv4）— 2.1.1.140/24

STEP 5 | 指定在 192.168.x.x 网络中将流量路由到目标的接口。

1. 在 VPN 对等设备 A 上，选择虚拟路由器。
2. 选择 **Static Routes**（静态路由），然后 **Add**（添加）tunnel.41 作为在 192.168.x.x 网络中将流量路由到 **Destination**（目标）的**Interface**（接口）。

STEP 6 | 在虚拟路由器上设置静态路由和 OSPF 配置，并将 OSPF 区域连接到防火墙的相应接口。

1. 在 VPN 对等设备 B 上，选择 **Network**（网络） > **Virtual Routers**（虚拟路由器），然后选择默认路由器或添加新路由器。
2. 选择 **Static Routes**（静态路由），然后 **Add**（添加）隧道 IP 地址作为在 172.168.x.x. 网络中路由流量的下一个跃点。

   分配所需的路由跃点数；使用较低的值，使得转发表中的路由选择具有更高的优先级。
3. 选择 **OSPF**（对于 IPv4）或 **OSPFv3**（对于 Ipv6），然后选择 **Enable**（启用）。
4. 在本例中，VPN 对等设备 B 的 OSPF 配置如下：
   - 路由器 ID：192.168.100.140
   - 区域 ID：0.0.0.0，分配给接口接口 Ethernet 1/12，链路类型：广播
   - 区域 ID：0.0.0.10，分配给接口 Ethernet1/1，链路类型：广播
   - 区域 ID：0.0.0.20，分配给接口 Ethernet1/15，链路类型：广播

STEP 7 | 创建重新分发配置文件以便将静态路由插入 OSPF 自治系统。

1. 在 VPN 对等设备 B 上创建重新分发配置文件。
   1. 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器），然后选择上面使用的路由器。
   2. 选择 **Redistribution Profiles**（重新分发配置文件），然后单击 **Add**（添加）。
   3. 输入配置文件的名称，并选择 **Redist**（重新分发），然后指定 **Priority**（优先级）值。如果已配置多个配置文件，则首先匹配优先级值最低的配置文件。
   4. 将 **Source Type**（源类型）设置为 **static**（静态），然后单击 **OK**（确定）。在步骤 6 中定义的静态路由将用于重新分发。
2. 将静态路由注入 OSPF 系统。
   1. 选择 **OSPF** > **Export Rules**（导出规则）（对于 IPv4）或 **OSPFv3** > **Export Rules**（导出规则）（对于 IPv6）。
   2. 单击 **Add**（添加），然后选择创建的重新分发配置文件。
   3. 选择将外部路由插入 OSPF 系统的方式。默认选项 **Ext2** 仅使用外部跃点数计算路由的总成本。要同时使用内部和外部 OSPF 跃点数，请使用 **Ext1**。
   4. 为插入 OSPF 系统的路由分配 **Metric**（跃点数）（成本值）。此选项可让您在将路由插入 OSPF 系统时更改跃点数。
   5. 单击 **OK**（确定）。

STEP 8 | 建立 IPSec 隧道。

1. 选择**Network**（网络） > **IPSec Tunnels**（**IPSec** 隧道）。
2. 单击 **Add**（添加），然后配置 **General**（常规）选项中的选项。

   在本例中，VPN 对等设备 A 配置如下：

   - **Tunnel Interface**（隧道接口）—tunnel.41
   - **Type**（类型）— 自动密钥
   - **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
   - **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在上文定义的 IKE 网关。

   VPN 对等设备 B 配置如下：

   - 隧道接口 — tunnel.40
   - **Type**（类型）— 自动密钥
   - **IKE Gateway**（**IKE** 网关）— 选择上文定义的 IKE 网关。
   - **IPSec Crypto Profile**（**IPSec** 加密配置文件）— 选择在上文定义的 IKE 网关。
3. 选择 **Show Advanced Options**（显示高级选项），并选择 **Tunnel Monitor**（隧道监控），然后指定为验证连接要 ping 的目标 IP 地址。
4. 要定义在建立连接失败后要采取的操作，请参阅定义隧道监控配置文件。

STEP 9 | 创建策略规则以允许站点之间的通信（子网）。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. 创建规则以允许不可信区域与 vpn-tun 区域，以及 vpn-tun 区域与不可信区域之间的流量，流量来源于指定的源和目标 IP 地址。

STEP 10 | 验证 OSPF 邻接并从 CLI 路由。

验证两个防火墙可以相互看作完整状态的邻居。同时确认 VPN 对等设备的隧道接口的 IP 地址和 OSPF 路由器 ID。在每个 VPN 对等设备上使用以下 CLI 命令。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route**

以下是每个 VPN 对等设备上的输出示例。

```
VPN PeerA

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          2.1.1.141       20      A S             tunnel.41
192.168.2.0/24          2.1.1.141       20      A S             tunnel.41
172.16.101.0/24         0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24            2.1.1.141       20      A S             tunnel.41

VPN PeerB

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          0.0.0.0         10      A Oo            ethernet1/1
192.168.2.0/24          0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24         2.1.1.140       20      A H             tunnel.40
2.1.1.141/24            2.1.1.140       10      A C             tunnel.40
```

STEP 11 | 测试 VPN 连接.

请参阅设置隧道监控和 查看隧道状态。

故障排除

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

本章分享了测试 VPN 连接和解释 VPN 错误消息（如果遇到）的任务。使用 CLI 命令监视站点到站点 VPN 连接并对其进行故障排除。

- 排查 IPSec VPN 隧道连接问题
- 使用 CLI 排查站点到站点 IPSec VPN 隧道问题

排查 IPSec VPN 隧道连接问题

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

测试 IPSec VPN 连接并对其进行故障排除，以获得最佳性能：

- 测试 VPN 连接
- 解释 VPN 错误消息

测试 VPN 连接

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

执行此任务以测试 VPN 连接。

STEP 1 | 通过 Ping 隧道间的某台主机或使用以下 CLI 命令启动 IKE 阶段 1：

```
test vpn ike-sa gateway <gateway_name>
```

STEP 2 | 输入以下命令测试 IKE 阶段 1 是否已设置：

```
show vpn ike-sa gateway <gateway_name>
```

在输出中，检查是否显示安全关联。如果没有显示，请查看系统日志消息以解释失败的原因。

STEP 3 | 通过 Ping 隧道间的某台主机或使用以下 CLI 命令启动 IKE 阶段 2：

```
test vpn ipsec-sa tunnel <tunnel_name>
```

STEP 4 | 输入以下命令测试 IKE 阶段 2 是否已设置：

```
show vpn ipsec-sa tunnel <tunnel_name>
```

在输出中，检查是否显示安全关联。如果没有显示，请查看系统日志消息以解释失败的原因。

STEP 5 | 要查看 VPN 流量流信息，请使用以下命令：

```
show vpn flow total tunnels configured:            1 filter - type
 IPSec, state any total IPSec tunnel configured:       1 total
 IPSec tunnel shown:                1 name                    id
      state      local-ip       peer-ip       tunnel-i/f
 ------------------------------------------------------------------------
 vpn-to-siteB       5       active
    100.1.1.1     200.1.1.1     tunnel.41
```

解释 VPN 错误消息

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

下表列出了系统日志中记录的一部分常见的 VPN 错误消息。

表 **2: VPN** 问题的 **Syslog** 错误消息

如果错误如下：	请尝试以下操作：

`IKE phase-1 negotiation is failed as initiator, main mode.Failed SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 due to timeout.`
或者
`IKE phase 1 negotiation is failed.Couldn’ t find configuration for IKE phase-1 request for peer IP x.x.x.x[1929]`
	• 确认 IKE 网关配置中每个 VPN 对等设备的公共 IP 地址准确。
	• 确认可以 ping IP 地址且路由问题不会导致连接出现故障。

`Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored...`
或者
`IKE phase-1 negotiation is failed.Unable to process peer’ s SA payload.`
	检查 IKE 加密配置文件配置，确认两端都建议进行常用加密、身份验证和 DH 组建议。

`pfs group mismatched:my:2peer:0` 或者	检查 IPSec 加密配置文件配置以确认：

如果错误如下：	请尝试以下操作：
`IKE phase-2 negotiation failed when processing SA payload.No suitable proposal found in peer' s SA payload.`	• 在两个 VPN 对等设备上已启用或禁用 PFS • 每个对等设备建议的 DH 组至少拥有一个共同的 DH 组
`IKE phase-2 negotiation failed when processing Proxy ID.Received local id x.x.x.x/x type IPv4 address protocol 0 port 0, received remote id y.y.y.y/y type IPv4 address protocol 0 port 0.`	其中一端的 VPN 对等设备使用基于策略的 VPN。必须在 Palo Alto Networks 防火墙上配置代理 ID。请参阅创建代理 ID 以标识 VPN 对等设备。
提交错误：`Tunnel interface tunnel.x multiple binding limitation (xx) reached.`	您必须已达到防火墙支持的最大代理 ID。在建立 IPSec 隧道之前，请检查防火墙上支持的最大代理 ID。 我们建议您在为 VPN 对等设备配置代理 ID 之前检查防火墙支持的最大代理 ID。如果您有一个用例，想要实施的 IPSec VPN 隧道超过防火墙支持的最大代理 ID，请执行以下步骤： • 配置具有相同阶段 1 和阶段 2 配置的另一个隧道。 • 代理 ID 的 SuperNet IP 地址。例如，不要使用 10.1.0.0/16、10.2.0.0/16，而是将范围的 supernet 设置为 10.0.0.0/8 以避免多个条目。
识别代号不匹配	代理 ID 不匹配将导致无法建立站点到站点 IPSec VPN 隧道。因此，请在两个 VPN 对等设备上配置相同的代理 ID，以成功建立站点到站点 IPSec VPN 隧道。 例如：在站点到站点 IPSec 隧道配置中，如果一个 VPN 对等设备配置了网络掩码 /32 的 IP 地址，而远程 VPN 对等设备配置了相同的 IP 地址，但使用不同的网络掩码 /16，则会导致建立 VPN 隧道失败。

如果错误如下：	请尝试以下操作：
	其他防火墙供应商的代理 *ID* 称为访问列表或访问控制列表 *(ACL)*。 VPN 对等设备中的代理 ID 应该是彼此的精确镜像（即相反），但不匹配。 用于建立 IPSec VPN 隧道的 VPN 对等设备的代理 ID 配置示例： 如果 VPN 防火墙 1 将 192.0.2.0/24 配置为本地 ID，将 192.0.2.25/24 配置为对等 ID。那么，必须将 VPN 防火墙 2 配置为 192.0.2.25/24 作为本地 ID，将 192.0.2.0/24 配置为对等 ID。

使用 CLI 解决站点到站点 VPN 问题

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

使用以下 CLI 命令对第 1 阶段和第 2 阶段站点到站点 VPN 问题进行故障排除：

- Show 命令
- 清除命令
- 测试命令
- 调试命令

Show 命令

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

如果您要...	请使用...
• 显示所有 VPN 通道的基本统计信息	`> show running tunnel flow info`
• 显示给定网关的 IKE SA	`> show vpn ike-sa gateway <gateway> | match <x.x.x.x/Y>`
• 显示给定隧道的 IKE SA	`> show vpn ike-sa tunnel <tunnel>`
• 显示 IPSec 计数器	`> show vpn flow`
• 显示所有 IPSec 网关及其配置的列表	`> show vpn gateway`
• 显示 IKE 阶段 1 SA	`> show vpn ike-sa`

如果您要...	请使用...
• 显示 IKE 阶段 2 SA	`> show vpn ipsec-sa`
• 显示自动密钥 IPSec 隧道配置列表	`>  show vpn tunnel`

清除命令

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

如果您要...	请使用...
• 删除给定网关的 IKEv1 IKE SA	`> clear vpn ike-sa gateway <gateway>`
• 删除给定隧道的 IKEv1 IKE SA	`> clear vpn ike-sa tunnel <tunnel>`
• 删除给定隧道的 IKEv1 IPSec SA	`> clear vpn ipsec-sa tunnel <tunnel>`

测试命令

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

如果您要...	请使用...
• 与指定网关发起 IKE 协商	`> test vpn ike-sa gateway <gateway>`
• 为指定隧道发起 IPSec 协商	`> test vpn ipsec-sa tunnel <tunnel>`

调试命令

在何处可以使用？	需要提供什么？
• PAN-OS	无需许可证

如果您要...	请使用...
• 打开调试以查看详细的日志记录和状态	`> debug ike global on debug less mp-log ikemgr.log debug ike stat`
• 数据包捕获用于查看和捕获主要、积极和快速模式协商。	`> debug ike pcap on view-pcap no-dns-lookup yes no-port-lookup yes debug-pcap ikemgr.pcap`
• 关闭调试	`> debug ike pcap off`