aws

用户指南

AWS Site-to-Site VPN

AWS Site-to-Site VPN: 用户指南

Table of Contents

什么是 AWS Site-to-Site VPN？

默认情况下，您在 Amazon VPC 中启动的实例无法与本地 (AWS Cloud) 网络和远程设备通信，例如，这可能是站点或本地设备。您可以创建 AWS Site-to-Site VPN (VP Site-to-Site N) 连接并配置路由以通过该连接传递流量，从而允许从 VPC 访问您的远程设备。

尽管 VPN 连接是一个通用术语，但在本文档中，VPN 连接是指您的 VPC 和您自己的本地网络之间的连接。 Site-to-SiteVPN 支持互联网协议安全 (IPsec) VPN 连接。

内容

概念

以下是 Site-to-Site VPN 的关键概念：

- VPN 连接：您的本地设备与您的设备之间的安全连接 VPCs。
- VPN 隧道：用于在客户网络和 AWS之间传输数据的加密链接。

  每个 VPN 连接均包括两条 VPN 隧道，可以同时使用这两条隧道来实现高可用性。
- 客户网关：一种向您的客户网关设备提供 AWS 相关信息的 AWS 资源。
- 客户网关设备： Site-to-SiteVPN 连接您一侧的物理设备或软件应用程序。
- 目标网关：VP Site-to-Site N 连接的 Amazon 端点的通用术语。
- 虚拟私有网关：虚拟私有网关是 VPN 连接的 Amazon 端的 Site-to-Site VPN 终端节点，可以连接到单个 VPC。
- 传输网关：一个传输中心，可用于互连多个 VPCs 本地网络，也可用作 VPN 连接的 Amazon 端点的 V Site-to-Site PN 终端节点。

Site-to-Site VPN 功能

AWS Site-to-Site VPN 连接支持以下功能：

- 互联网密钥交换版本 2 (IKEv2)
- NAT 遍历
- 适用于虚拟专用网关（VGW）配置的 4 字节 ASN，范围为 1 至 2147483647。请参阅您的 AWS Site-to-Site VPN 连接的客户网关选项了解更多信息。
- 适用于客户网关（CGW）的 2 字节 ASN，范围为 1 至 65535。请参阅您的 AWS Site-to-Site VPN 连接的客户网关选项了解更多信息。
- CloudWatch 指标
- 您的客户网关的可重用 IP 地址。
- 其他加密选项，包括 AES 256 位加密、SHA-2 哈希，以及其他 Diffie-Hellman 组
- 可配置的隧道选项
- BGP 会话的 Amazon 端的自定义专用 ASN
- 来自下属 CA 的私有证书 AWS Private Certificate Authority
- 支持 IPv6 传输网关上的 VPN 连接流量

Site-to-Site VPN 限制

V Site-to-Site PN 连接有以下限制。

- IPv6 虚拟专用网关上的 VPN 连接不支持流量。
- AWS VPN 连接不支持路径 MTU 发现。

此外，在使用 Site-to-Site VPN 时，请考虑以下几点。

- 将您 VPCs 连接到常见的本地网络时，我们建议您在网络中使用不重叠的 CIDR 块。

Site-to-Site VPN 资源

您可以使用以下任何接口创建、访问和管理 Site-to-Site VPN 资源：

- AWS Management Console— 提供可用于访问您的 Site-to-Site VPN 资源的 Web 界面。

- AWS Command Line Interface (AWS CLI) — 为包括 Amazon VPC 在内的各种 AWS 服务提供命令，并在 Windows、macOS 和 Linux 上受支持。 AWS Site-to-Site VPN 命令行包含在较大的命令行参考中 EC2
  - 有关命令行界面的一般信息，请参见AWS Command Line Interface。
  - 有关可用 EC2 命令的列表，包括 Site-to-Site VPN 命令，请参阅EC2 命令行参考。

    > **Note**
    >
    > 命令行参考没有区分 Site-to-Site VPN 命令和较大的 EC2 命令集

- AWS SDKs— 提供特定语言 APIs 并处理许多连接细节，例如计算签名、处理请求重试和错误处理。有关更多信息，请参阅 AWS SDKs。
- 查询 API — 提供您使用 HTTPS 请求调用的低级别 API 操作。使用查询 API 是用于访问 Amazon VPC 的最直接方式，但需要您的应用程序处理低级别详细信息，例如生成哈希值以签署请求以及进行错误处理。有关更多信息，请参阅 Amazon EC2 API 参考。

定价

您需要为预置并且可用的 VPN 连接按 VPN 连接小时数付费。有关更多信息，请参阅加AWS Site-to-Site VPN 速 Site-to-Site VPN 连接定价。

您需要支付从 Amazon EC2 向互联网传输数据的费用。有关更多信息，请参阅 Amazon EC2 按需定价页面上的数据传输。

当您创建加速 VPN 连接时，我们将代表您创建和管理两个加速器。您需要按小时为每个加速器付费，并支付数据传输费。有关更多信息，请参阅AWS Global Accelerator 定价。

如何 AWS Site-to-Site VPN 运作

Site-to-SiteVPN 连接由以下组件组成：

- 虚拟私有网关或中转网关
- 客户网关设备
- 客户网关

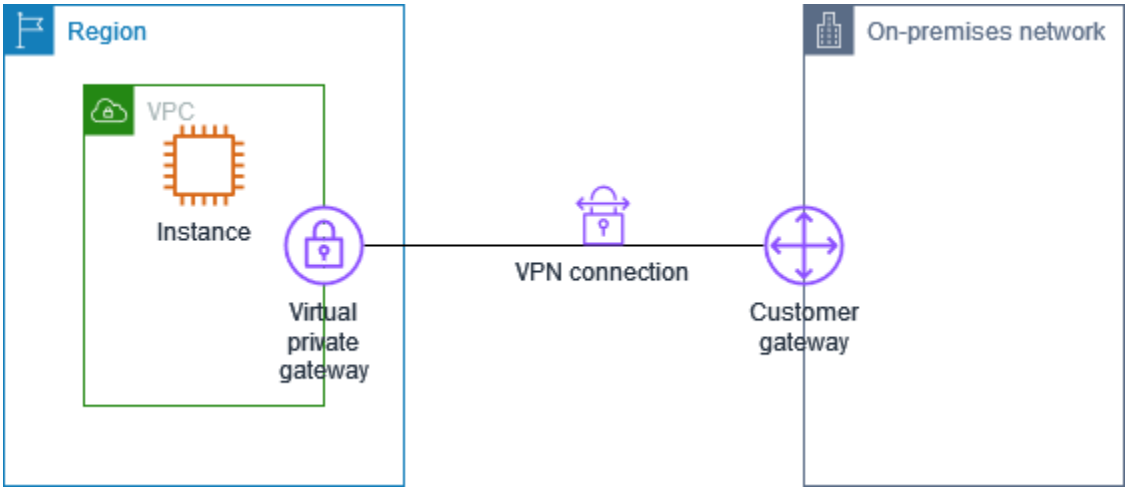
VPN 连接在侧面的虚拟专用网关或传输网关与本地 AWS 端的客户网关之间提供两条 VPN 隧道。

有关 Site-to-Site VPN 配额的更多信息，请参阅AWS Site-to-Site VPN 配额。

虚拟专用网关

虚拟专用网关是 VPN 连接的 Amazon 端的 Site-to-Site VPN 集中器。您创建虚拟私有网关并将其连接到虚拟私有云 (VPC)，其资源必须访问 Site-to-Site VPN 连接。

下图显示了 VPC 和本地网络之间使用虚拟私有网关的 VPN 连接。

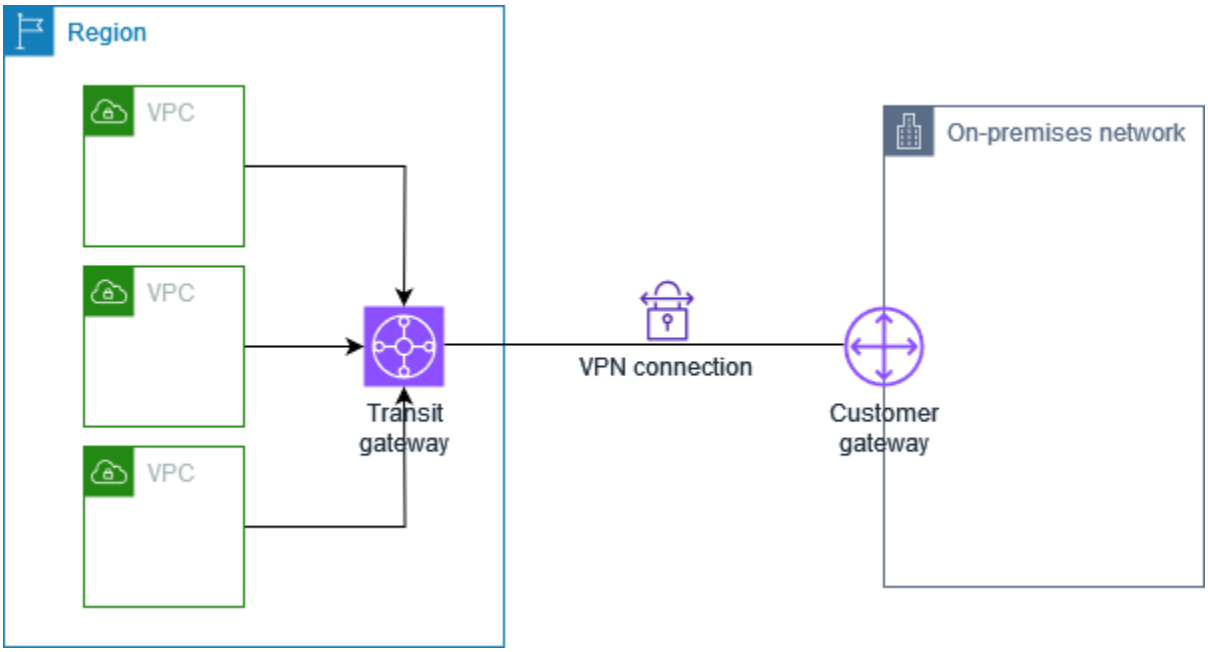


创建虚拟专用网关时，可以为网关的 Amazon 端指定专用自治系统编号 (ASN)。如果不指定 ASN，则会使用默认 ASN (64512) 创建虚拟专用网关。创建虚拟专用网关后，无法更改 ASN。要查看您的虚拟私有网关的 ASN，请在 Amazon VPC 控制台的虚拟私有网关页面中查看其详细信息，或使用describe-vpn-gateways AWS CLI 命令。

Transit Gateway

公交网关是一个交通枢纽，可用于将您的本地网络 VPCs 与您的本地网络互连。有关更多信息，请参阅 Amazon VPC 中转网关。您可以在传输网关上创建 Site-to-Site VPN 连接作为附件。

下图显示了使用传输网关在多个网络 VPCs 和您的本地网络之间的 VPN 连接。中转网关有三个 VPC 挂载和一个 VPN 挂载。



您在传输网关上的 Site-to-Site VPN 连接可以支持 VPN 隧道内的 IPv4 IPv6流量或 VPN 隧道内的流量。有关更多信息，请参阅 IPv4 还有进 IPv6 来的交通 AWS Site-to-Site VPN。

您可以将 Site-to-Site VPN 连接的目标网关从虚拟专用网关修改为传输网关。有关更多信息，请参阅 the section called “修改 VPN 连接的目标网关”。

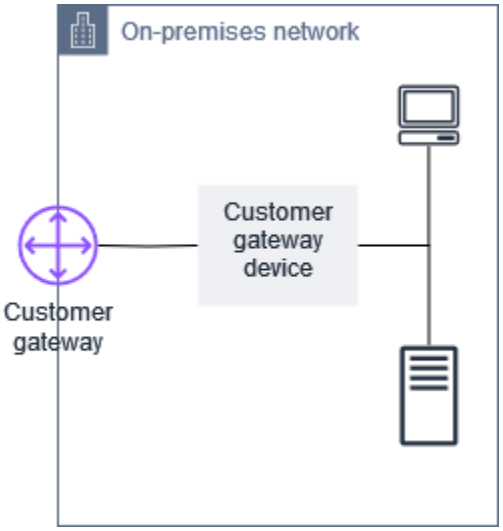
客户网关设备

客户网关设备是 Site-to-Site VPN 连接中您一侧的物理设备或软件应用程序。您可以将设备配置为使用 Site-to-Site VPN 连接。有关更多信息，请参阅 AWS Site-to-Site VPN 客户网关设备。

默认情况下，您的客户网关设备必须通过生成流量和启动 Internet 密钥交换 (IKE) 协商过程来开通 Site-to-Site VPN 连接的隧道。您可以将 Site-to-Site VPN 连接配置为指定 AWS 必须改为启动 IKE 协商进程。有关更多信息，请参阅 AWS Site-to-Site VPN 隧道启动选项。

客户网关

客户网关 是您在 AWS 中创建的资源，它表示本地网络中的客户网关设备。创建客户网关时，您需要向提供有关您的设备的信息 AWS。有关更多信息，请参阅 the section called “客户网关选项”。

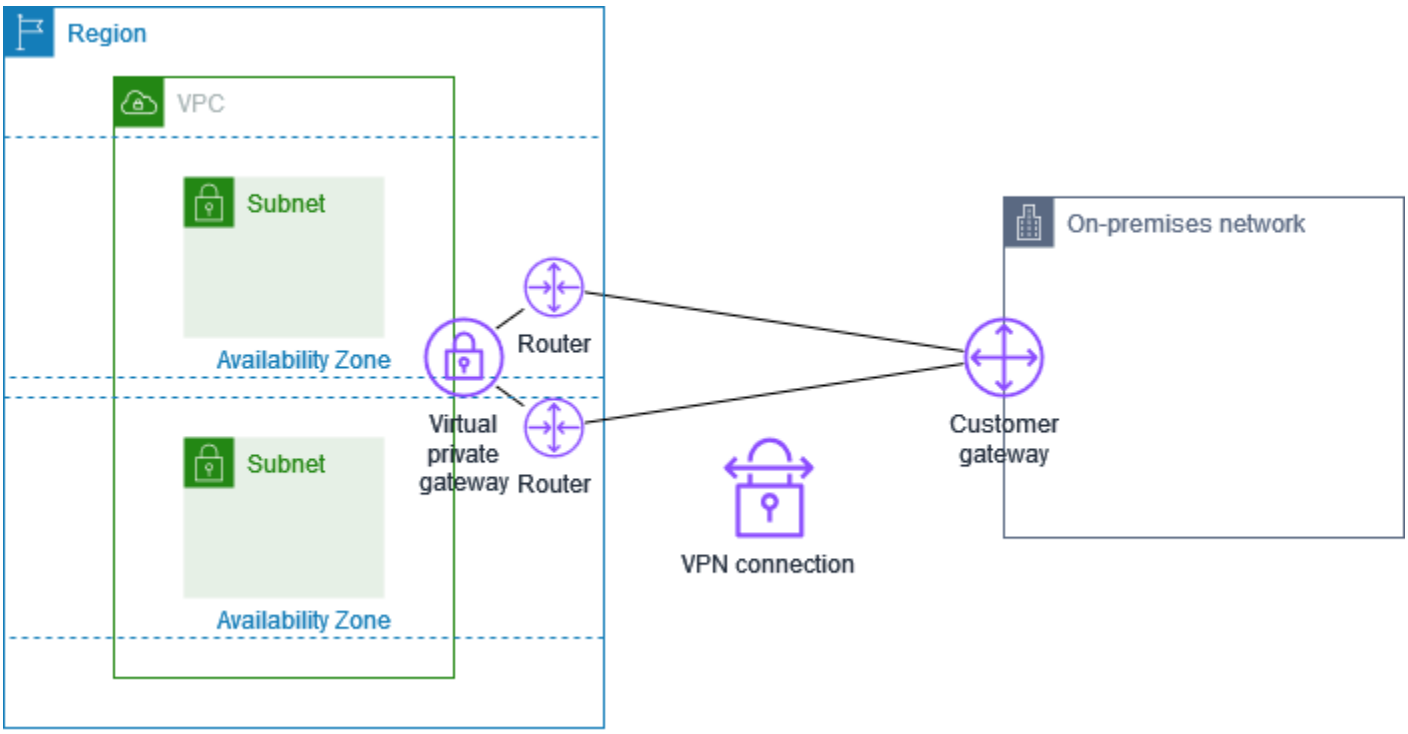


要将 Amazon VPC 与 Site-to-Site VPN 连接配合使用，您或您的网络管理员还必须在远程网络中配置客户网关设备或应用程序。当您创建 Site-to-Site VPN 连接时，我们会为您提供所需的配置信息，您的网络管理员通常会执行此配置。有关客户网关要求和配置的信息，请参阅AWS Site-to-Site VPN 客户网关设备。

您的 AWS Site-to-Site VPN 连接的隧道选项

您可以使用 Site-to-Site VPN 连接将您的远程网络连接到 VPC。每个 Site-to-Site VPN 连接都有两条隧道，每条隧道使用唯一的公有 IP 地址。配置两条隧道以提供冗余能力是重要的步骤。当一条隧道不可用（例如，因维护而关闭）时，网络流量会自动路由到该特定 Site-to-Site VPN 连接的可用隧道。

下图展示了 VPN 连接的两条隧道。每条隧道在不同的可用区终止，以提供更高的可用性。从本地网络到的流量 AWS 使用两条隧道。来自本地网络 AWS 的流量优先选择其中一条隧道，但如果 AWS 侧面出现故障，则可以自动故障转移到另一条隧道。



创建 Site-to-Site VPN 连接时，需要下载特定于您的客户网关设备的配置文件，其中包含配置设备的信息，包括配置每条隧道的信息。创建 Site-to-Site VPN 连接时，您可以选择自己指定一些隧道选项。否则， AWS 会提供默认值。

> **Note**
>
> Site-to-Site 无论客户网关的提案顺序如何，VPN 隧道端点都会从下面列表中的最低配置值开始评估来自客户网关的提案。您可以使用`modify-vpn-connection-options`命令来限制 AWS 端点将接受的选项列表。有关更多信息，请参阅 Amazon EC2 命令行参考modify-vpn-connection-options中的。

以下是您可以配置的隧道选项。

> **Note**
>
> 某些隧道选项有多个默认值。例如，IKE 版本有两个默认隧道选项值：`ikev1` 和 `ikev2`。如果您不选择特定值，则所有默认值都将与该隧道选项相关联。单击删除您不希望与隧道选项相关联的任何默认值。例如，如果您只想使用 `ikev1` 作为 IKE 版本，请单击 `ikev2` 将其删除。

失效对端检测 (DPD) 超时

发生 DPD 超时之后的秒数。DPD 超时为 30 秒意味着 VPN 端点将在第一次保持连接失败 30 秒后认为对等体已死亡。您可以指定 30 或更高值。

原定设置值：40

DPD 超时操作

发生失效对端检测 (DPD) 超时后采取的操作。您可以指定：

- `Clear`：当发生 DPD 超时时结束 IKE 会话（停止隧道并清除路由）
- `None`：当发生 DPD 超时时不采取任何操作
- `Restart`：当发生 DPD 超时时重新启动 IKE 会话

有关更多信息，请参阅AWS Site-to-Site VPN 隧道启动选项。

默认值：`Clear`

VPN 日志记录选项

使用 Site-to-Site VPN 日志，您可以访问有关 IP 安全 (IPsec) 隧道建立、互联网密钥交换 (IKE) 协商和失效对等体检测 (DPD) 协议消息的详细信息。

有关更多信息，请参阅 AWS Site-to-Site VPN 日志。

可用的日志格式：`json`、`text`

IKE 版本

VPN 隧道允许的 IKE 版本。您可以指定一个或多个默认值。

默认值：`ikev1`、`ikev2`

隧道内部 IPv4 CIDR

VPN 隧道的内部（内部）IPv4 地址范围。您可以指定 `169.254.0.0/16` 范围中大小为 /30 的 CIDR 块。在使用相同虚拟专用网关的所有 Site-to-Site VPN 连接中，CIDR 块必须是唯一的。

> **Note**
>
> 对于一个中转网关上的所有连接，CIDR 块无需唯一。但如果它们不唯一，则可能会在客户网关上造成冲突。在传输网关的多个 Site-to-Site VPN 连接上重复使用相同的 CIDR 块时，请谨慎行事。

以下 CIDR 块由系统保留，不能使用：

- 169.254.0.0/30
- 169.254.1.0/30
- 169.254.2.0/30
- 169.254.3.0/30
- 169.254.4.0/30
- 169.254.5.0/30
- 169.254.169.252/30

默认：该范围内大小为 /30 的 IPv4 CIDR 块。169.254.0.0/16

预共享密钥存储

预共享密钥的存储类型：

- 标准-预共享密钥直接存储在 Site-to-Site VPN 服务中。
- S@@ ecrets Manager — 使用 AWS Secrets Manager存储预共享密钥。有关 Secrets Manager 的更多信息，请参阅使用 Secrets Manager 增强安全功能。

隧道内部 IPv6 CIDR

（仅IPv6 限 VPN 连接）VPN 隧道的内部（内部） IPv6 地址范围。您可以指定本地 fd00::/8 范围内的大小为 /126 的 CIDR 块。在使用相同传输网关的所有 Site-to-Site VPN 连接中，CIDR 块必须是唯一的。

默认：本地fd00::/8范围内大小为 /126 的 IPv6 CIDR 块。

本地 IPv4 网络 CIDR

（仅IPv4 限 VPN 连接）在 IKE 第 2 阶段协商期间为 VPN 隧道的客户（本地）端使用的 CIDR 范围。此范围用于建议路由，但不强制实施流量限制，因为仅 AWS 使用基于路径的路由 VPNs 。不支持基于策略 VPNs ，因为它们会限制 AWS“支持动态路由协议和多区域架构的能力”。这应包括本地网络中需要通过 VPN 隧道进行通信的 IP 范围。应使用正确的路由表配置和安全组来控制实际流量。 NACLs

默认：0.0.0.0/0

远程 IPv4 网络 CIDR

（仅IPv4 限 VPN 连接）在 IKE 第 2 阶段协商期间为 VPN 隧道 AWS 一侧使用的 CIDR 范围。此范围用于建议路由，但并不强制执行流量限制，因为 AWS 仅使用基于路径的路由 VPNs。AWS 不支持基于策略， VPNs 因为它们缺乏复杂路由场景所需的灵活性，并且与传输网关和 VPN 等价多

路径 (ECMP) 等功能不兼容。对于 VPCs，这通常是您的 VPC 的 CIDR 范围。对于中转网关，这可能包括来自连接网络 VPCs 或其他网络的多个 CIDR 范围。

默认：0.0.0.0/0

本地 IPv6 网络 CIDR

（仅IPv6 限 VPN 连接）允许通过 VPN 隧道进行通信的客户网关（本地）端的 IPv6 CIDR 范围。

默认值：::/0

远程 IPv6 网络 CIDR

（仅限 IPv6 VPN 连接）允许通过 VPN 隧道进行通信 AWS 的一侧的 IPv6 CIDR 范围。

默认值：::/0

阶段 1 Diffie-Hellman (DH) 组编号

对于 VPN 隧道的阶段 1 IKE 协商，允许的 DH 组编号。您可以指定一个或多个默认值。

默认值：2、14、15、16、17、18、19、20、21、22、23、24

阶段 2 Diffie-Hellman (DH) 组编号

对于 VPN 隧道的阶段 2 IKE 协商，允许的 DH 组编号。您可以指定一个或多个默认值。

默认值：2、5、14、15、16、17、18、19、20、21、22、23、24

阶段 1 加密算法

对于 VPN 隧道的阶段 1 IKE 协商，允许的加密算法。您可以指定一个或多个默认值。

默认值： AES128、、 AES128-GCM- AES256 16、-GCM-16 AES256

阶段 2 加密算法

对于 VPN 隧道的阶段 2 IKE 协商，允许的加密算法。您可以指定一个或多个默认值。

默认值： AES128、、 AES128-GCM- AES256 16、-GCM-16 AES256

阶段 1 完整性算法

对于 VPN 隧道的阶段 1 IKE 协商，允许的完整性算法。您可以指定一个或多个默认值。

默认值： SHA1、 SHA2 -256、- SHA2 384、-512 SHA2

阶段 2 完整性算法

对于 VPN 隧道的阶段 2 IKE 协商，允许的完整性算法。您可以指定一个或多个默认值。

默认值： SHA1、 SHA2 -256、- SHA2 384、-512 SHA2

阶段 1 生命周期

> **Note**
>
> AWS 使用第 1 阶段生命周期和第 2 阶段生命周期字段中设置的时间值启动重新生成密钥。如果此生命周期与协商的握手值不同，则可能会中断隧道连接。

IKE 协商的阶段 1 的生命周期，以秒为单位。您可以指定 900 到 28800 之间的数字。

默认值：28800（8 小时）

阶段 2 生命周期

> **Note**
>
> AWS 使用第 1 阶段生命周期和第 2 阶段生命周期字段中设置的时间值启动重新生成密钥。如果此生命周期与协商的握手值不同，则可能会中断隧道连接。

IKE 协商的阶段 2 的生命周期，以秒为单位。您可以指定 900 到 3600 之间的数字。您指定的数字必须小于阶段 1 生命周期的秒数。

默认值：3600（1 小时）

预共享密钥 (PSK)

预共享密钥 (PSK)，用于在目标网关和客户网关之间建立初始 Internet 密钥交换 (IKE) 安全关联。

PSK 的长度必须在 8 到 64 个字符之间，而且不能以零 (0) 开头。允许的字符是字母数字字符、句点 (.) 和下划线 (_)。

默认值：32 个字符的字母数字字符串。

更改密钥模糊值

在其中随机选择更改密钥时间的更改密钥窗口的百分比（由更改密钥容许时间确定）

您可以指定介于 0 到 100 之间的百分比值。

默认值：100

更改密钥容许时间

第 1 阶段和第 2 阶段生命周期到期之前的空闲时间（以秒为单位），在此期间 VPN 连接 AWS 端执行 IKE 重新密钥。

您可以指定一个介于 60 和阶段 2 生命周期值一半之间的数字。

更改密钥的确切时间基于更改密钥模糊值随机选择。

原定设置：270（4.5 分钟）

回放窗口大小的数据包

IKE 回放窗口中的数据包数。

您可以指定 64 到 2048 之间的值。

默认值：1024

启动操作

为 VPN 连接建立隧道时要执行的操作。您可以指定：

- `Start`: AWS 启动 IKE 协商以开启隧道。仅当您的客户网关配置了 IP 地址时才支持。
- `Add`：您的客户网关设备必须启动 IKE 协商才能启动隧道。

有关更多信息，请参阅AWS Site-to-Site VPN 隧道启动选项。

默认值：`Add`

隧道端点生命周期控制

隧道端点生命周期控制提供对端点替换计划的控制。

有关更多信息，请参阅 AWS Site-to-Site VPN 隧道端点生命周期控制。

默认值：`Off`

您可以在创建 Site-to-Site VPN 连接时指定隧道选项，也可以修改现有 VPN 连接的隧道选项。有关更多信息，请参阅以下主题：

- 步骤 5：创建 VPN 连接
- 修改 AWS Site-to-Site VPN 隧道选项

AWS Site-to-Site VPN 隧道身份验证选项

您可以使用预共享密钥或证书对 Site-to-Site VPN 隧道端点进行身份验证。

预共享密钥

预共享密钥 (PSK) 是 VP Site-to-Site N 隧道的默认身份验证选项。创建隧道时，您可以指定自己的 PSK，也可以 AWS 允许自动生成一个 PSK。PSK 使用以下方法之一进行存储：

- 直接在 Site-to-Site VPN 服务中。有关更多信息，请参阅 Site-to-Site VPN 客户网关设备。
- AWS Secrets Manager 为了增强安全性。有关使用 Secrets Manager 存储 PSK 的更多信息，请参阅使用 Secrets Manager 增强安全功能。

然后，在配置客户网关设备时使用 PSK 字符串。

来自的私有证书 AWS Private Certificate Authority

如果您不想使用预先共享的密钥，则可以使用来自 AWS Private Certificate Authority 的私有证书对 VPN 进行身份验证。

您必须使用 AWS Private Certificate Authority (AWS 私有 CA)，通过从属 CA 创建私有证书 要对 ACM 从属 CA 签名，您可以使用 ACM 根 CA 或外部 CA。有关创建私有证书的更多信息，请参阅《AWS Private Certificate Authority 用户指南》中的创建和管理私有 CA。

您必须创建服务相关角色才能生成和使用 Site-to-Site VPN 隧道端点 AWS 一侧的证书。有关更多信息，请参阅 the section called “服务相关角色”。

> **Note**
>
> 为了便于无缝的证书轮换，任何与 `CreateCustomerGateway` API 调用中最初指定的证书具有相同证书颁发机构链的证书都足以建立 VPN 连接。

如果您不指定客户网关设备的 IP 地址，我们将不检查 IP 地址。此操作允许您将客户网关设备移动到不同的 IP 地址，而无需重新配置 VPN 连接。

Site-to-Site 当您创建证书 VPN 时，VPN 会对客户网关证书执行证书链验证。除了基本的 CA 和有效性检查外， Site-to-SiteVPN 还会检查 X.509 扩展是否存在，包括授权密钥标识符、主题密钥标识符和基本约束。

AWS Site-to-Site VPN 隧道启动选项

默认情况下，您的客户网关设备必须通过生成流量和启动 Internet 密钥交换 (IKE) 协商过程来开通 Site-to-Site VPN 连接的隧道。您可以将 VPN 隧道配置为指定 AWS 必须改为启动或重新启动 IKE 协商进程。

VPN 隧道 IKE 启动选项

以下 IKE 启动选项可用。您可以为 Site-to-Site VPN 连接中的一条或两条隧道实施其中一个或两个选项。有关这些设置和其他隧道选项设置的更多详细信息，请参阅VPN 隧道选项。

- 启动操作：为新的或修改的 VPN 连接建立 VPN 隧道时要执行的操作。默认情况下，您的客户网关设备启动 IKE 协商过程以启动隧道。您可以指定 AWS 必须改为启动 IKE 协商进程。
- DPD 超时操作：发生失效对端检测 (DPD) 超时后要采取的操作。默认情况下，IKE 会话停止，隧道关闭，路由将被移除。您可以指定在 DPD 超时发生时 AWS 必须重新启动 IKE 会话，也可以指定在 DPD 超时发生时 AWS 不得采取任何操作。

规则和限制

以下规则和限制适用：

- 要启动 IKE 协商， AWS 需要您的客户网关设备的公有 IP 地址。如果您为 VPN 连接配置了基于证书的身份验证，并且在中创建客户网关资源时未指定 IP 地址 AWS，则必须创建新的客户网关并指定 IP 地址。然后，修改 VPN 连接并指定新的客户网关。有关更多信息，请参阅 更改 AWS Site-to-Site VPN 连接的客户网关。
- IKEv2 仅支持从 VPN 连接 AWS 侧启动 IKE（启动操作）。
- 如果从 VPN 连接 AWS 侧使用 IKE 初始化，则不包括超时设置。它会不断尝试建立连接，直到建立连接。此外，当 VPN 连接 AWS 端收到来自您的客户网关的 delete SA 消息时，它将重新启动 IKE 协商。
- 如果您的客户网关设备位于防火墙或其他使用网络地址转换 (NAT) 的设备后面，则必须配置身份 (IDr)。有关的更多信息 IDr，请参阅 RFC 7296。

如果您没有从 AWS 侧面为 VPN 隧道配置 IKE 初始化，并且 VPN 连接有一段空闲时间（通常为 10 秒，具体取决于您的配置），则隧道可能会中断。为防止发生此问题，您可以使用网络监控工具来生成 keepalive Ping。

使用 VPN 隧道启动选项

有关使用 VPN 隧道启动选项的更多信息，请参阅以下主题：

- 要创建新的 VPN 连接并指定 VPN 隧道启动选项，请执行以下操作：步骤 5：创建 VPN 连接
- 要修改现有 VPN 连接的 VPN 隧道启动选项，请执行以下操作：修改 AWS Site-to-Site VPN 隧道选项

AWS Site-to-Site VPN 隧道端点替换

您的 Site-to-Site VPN 连接由两个 VPN 隧道组成，用于实现冗余。有时，在 AWS 执行隧道更新或修改 VPN 连接时，会替换一个或两个 VPN 隧道端点。在隧道端点替换期间，在预置新的隧道端点时，通过该隧道的连接可能会中断。

主题

- 客户发起的端点替换
- AWS 托管式端点替换
- AWS Site-to-Site VPN 隧道端点生命周期控制

客户发起的端点替换

在您修改 VPN 连接的以下组件时，将替换隧道端点中的一个或两个。

修改	API 操作	隧道影响
修改 VPN 连接的目标网关	ModifyVpnConnection	在预置新的隧道终端节点时，两个隧道都不可用。
更改 VPN 连接的客户网关	ModifyVpnConnection	在预置新的隧道终端节点时，两个隧道都不可用。
修改 VPN 连接选项	ModifyVpnConnectionOptions	在预置新的隧道终端节点时，两个隧道都不可用。
修改 VPN 隧道选项	ModifyVpnTunnelOptions	修改的隧道在更新期间不可用。

AWS 托管式端点替换

AWS Site-to-Site VPN 是一项托管服务，会定期向您的 VPN 隧道端点应用更新。进行这些更新的原因有多种，包括以下几点：

- 应用常规升级，例如补丁、恢复能力改进和其他增强功能
- 停用底层硬件
- 当自动监控确定 VPN 隧道端点运行状况不佳时

AWS 一次将隧道端点更新应用到 VPN 连接的一个隧道。在隧道端点更新期间，您的 VPN 连接可能会出现短暂的冗余丢失。因此，在 VPN 连接中配置两个隧道以实现高可用性非常重要。

AWS Site-to-Site VPN 隧道端点生命周期控制

隧道端点生命周期控制可以控制端点更换时间表，并且可以帮助最大限度地减少 AWS 托管隧道端点更换期间的连接中断。借助此功能，您可以选择在最适合您业务的时间接受隧道端点的 AWS 托管更新。如果您有短期业务需求或每个 VPN 连接只能支持单个隧道，请使用此功能。

> **Note**
>
> 在极少数情况下，即使启用了隧道端点生命周期控制功能，也 AWS 可能会立即对隧道端点应用关键更新。

主题

隧道端点生命周期控制的工作原理

为 VPN 连接中的各个隧道开启隧道端点生命周期控制功能。可以在创建 VPN 时启用此功能，也可以通过修改现有 VPN 连接的隧道选项来启用此功能。

启用隧道端点生命周期控制后，您将通过两种方式进一步了解即将到来的隧道维护事件：

- 您将收到即将更换隧道端点的 AWS Health 通知。
- 使用 get-vpn-tunnel-replacement- AWS CLI status命令可以在 AWS Management Console 或中查看待维护的状态，以及应用后自动维护和上次维护应用的时间戳。

当隧道端点维护可用时，在之后自动应用维护时间戳之前，您将有机会在方便的时间接受更新。

如果您没有在维护自动应用日期之后应用更新，则 AWS 将在不久之后自动执行隧道端点更换，这是常规维护更新周期的一部分。

启用 AWS Site-to-Site VPN 隧道端点生命周期控制

可以在现有或新的 VPN 连接上启用端点生命周期控制。这可以使用 AWS Management Console 或来完成 AWS CLI。

> **Note**
>
> 原定设置情况下，当您为现有 VPN 连接启用该功能时，将同时发起隧道端点替换。如果您想开启该功能，但不想立即发起隧道端点替换，则可以使用跳过隧道替换选项。

Existing VPN connection

以下步骤演示如何在现有 VPN 连接上启用隧道端点生命周期控制。

使用 AWS Management Console启用隧道端点生命周期控制

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在左侧导航栏中，选择 Site-to-Site VPN 连接。
3. 在 VPN 连接下选择适当的连接。
4. 依次选择操作和修改 VPN 隧道选项。
5. 通过选择适当的 VPN 隧道外部 IP 地址，选择要修改的特定隧道。
6. 在隧道端点生命周期控制下，选中启用复选框。
7. （可选）选择跳过隧道替换。
8. 选择 Save changes（保存更改）。

使用 AWS CLI启用隧道端点生命周期控制

使用modify-vpn-tunnel-options命令开启隧道端点生命周期控制。

New VPN connection

以下步骤演示如何在创建新的 VPN 连接期间启用隧道端点生命周期控制。

要在创建新 VPN 连接期间启用隧道端点生命周期控制，请使用 AWS Management Console

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN Connections。
3. 选择创建 VPN 连接。
4. 在隧道 1 选项和隧道 2 选项所对应的部分中，在隧道端点生命周期控制下，选择启用。
5. 选择 Create VPN Connection（创建 VPN 连接）。

要在创建新 VPN 连接期间启用隧道端点生命周期控制，请使用 AWS CLI

使用create-vpn-connection命令开启隧道端点生命周期控制。

验证是否启用了 AWS Site-to-Site VPN 隧道端点生命周期控制

您可以使用 AWS Management Console 或 CLI 验证是否在现有 VPN 隧道上启用了隧道端点生命周期控制。

- 如果禁用了隧道端点生命周期控制，并且您希望启用它，请参阅启用 隧道端点生命周期控制。
- 如果启用了隧道端点生命周期控制，并且您希望禁用它，请参阅关闭 隧道端点生命周期控制。

使用 AWS Management Console验证是否启用了隧道端点生命周期控制

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在左侧导航栏中，选择 Site-to-Site VPN 连接。
3. 在 VPN 连接下选择适当的连接。
4. 选择隧道详细信息选项卡。
5. 在隧道详细信息中，查找隧道端点生命周期控制，它将报告该功能是启用还是禁用。

使用 AWS CLI验证是否启用了隧道端点生命周期控制

使用describe-vpn-connections命令验证隧道端点生命周期控制是否已启用。

检查可用的 AWS Site-to-Site VPN 隧道更新

启用隧道端点生命周期控制功能后，您可以使用 AWS Management Console 或 CLI 查看 VPN 连接是否有可用的维护更新。检查可用的 Site-to-Site VPN 隧道更新不会自动下载和部署更新。您可以选择何时部署。有关下载和部署更新的步骤，请参阅接受维护更新。

要检查可用更新，请使用 AWS Management Console

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在左侧导航栏中，选择 Site-to-Site VPN 连接。
3. 在 VPN 连接下选择适当的连接。
4. 选择隧道详细信息选项卡。
5. 查看待维护列。状态将为可用或无。

要检查可用更新，请使用 AWS CLI

使用 get-vpn-tunnel-replacement-status 命令检查是否有可用的更新。

接受 AWS Site-to-Site VPN 隧道维护更新

当维护更新可用时，您可以使用 AWS Management Console 或 CLI 接受该更新。您可以选择在方便的时间接受 Site-to-Site VPN 隧道维护更新。在您接受维护更新后，系统便会部署该更新。

> **Note**
>
> 如果您不接受维护更新， AWS 将在常规维护更新周期中自动部署它。

要接受可用的维护更新，请使用 AWS Management Console

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在左侧导航栏中，选择 Site-to-Site VPN 连接。
3. 在 VPN 连接下选择适当的连接。
4. 选择操作，然后选择替换 VPN 隧道。
5. 通过选择适当的 VPN 隧道外部 IP 地址，选择要替换的特定隧道。

6. 选择替换。

要接受可用的维护更新，请使用 AWS CLI

使用replace-vpn-tunnel命令接受可用的维护更新。

关闭 AWS Site-to-Site VPN 隧道端点生命周期控制

如果您不想再使用隧道终端节点生命周期控制功能，则可以使用 AWS Management Console 或将其关闭 AWS CLI。当您关闭此功能时， AWS 将定期自动部署维护更新，这些更新可能会在您的工作时间内发生。为避免任何业务影响，我们强烈建议您在 VPN 连接中配置这两个隧道以实现高可用性。

> **Note**
>
> 虽然有可用的待维护，但在关闭该功能时无法指定跳过隧道替换选项。您可以随时关闭该功能，而无需使用跳过隧道替换选项，但 AWS 会通过立即启动隧道端点替换来自动部署可用的待维护更新。

使用关闭隧道端点生命周期控制 AWS Management Console

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在左侧导航栏中，选择 Site-to-Site VPN 连接。
3. 在 VPN 连接下选择适当的连接。
4. 依次选择操作和修改 VPN 隧道选项。
5. 通过选择适当的 VPN 隧道外部 IP 地址，选择要修改的特定隧道。
6. 要关闭隧道端点生命周期控制，请在隧道端点生命周期控制下，清除启用复选框。
7. （可选）选择跳过隧道替换。
8. 选择 Save changes（保存更改）。

使用关闭隧道端点生命周期控制 AWS CLI

使用modify-vpn-tunnel-options命令关闭隧道端点生命周期控制。

您的 AWS Site-to-Site VPN 连接的客户网关选项

下表描述了在 AWS中创建客户网关资源所需的信息

Item	描述
（可选）名称标签。	创建具有“名称”键以及您指定的值的标签。
（仅动态路由）客户网关的边界网关协议 (BGP) 自治系统编号 (ASN)。	支持 1 到 4,294,967,295 范围内的 ASN。您可以使用为您的网络分配的现有公有 ASN，但以下情况除外： • 7224 - 在所有区域保留 • 9059 - 在 `eu-west-1` 区域保留 • 10124 - 在 `ap-northeast-1` 区域保留 • 17943 - 在 `ap-southeast-1` 区域保留 如果您没有公有 ASN，则可以使用私有 ASN（在 64512 至 65534 或 4200000000 至 4294967294 范围内）。默认 ASN 是 64512。有关路由的更多信息，请参阅 AWS Site-to-Site VPN 路由选项。
客户网关设备的外部接口的 IP 地址。	该 IP 地址必须是静态的。 如果您的客户网关设备位于网络地址转换 (NAT, Network Address Translation) 设备的后面，请使用 NAT 设备的 IP 地址。此外，请确保允许端口 500（如果使用 NAT 遍历，则还要允许端口 4500）上的 UDP 数据包在您的网络和端点之间传输。 AWS Site-to-Site VPN 有关更多信息，请参阅防火墙规则。 当您使用来自 AWS Private Certificate Authority 的私有证书和公有 VPN 时，不需要 IP 地址。
（可选）使用 AWS Certificate Manager (ACM) 从属 CA 获得的私有证书。	如果您要使用基于证书的身份验证，请提供将在客户网关设备上使用的 ACM 私有证书的 ARN。

Item	描述
	创建客户网关时，可以将客户网关配置为使用 AWS Private Certificate Authority 私有证书对 Site-to-Site VPN 进行身份验证。 当您选择使用此选项时，您将创建一个完全 AWS托管的私有证书颁发机构 (CA)，供组织内部使用。根 CA 证书和从属 CA 证书均由存储和管理 AWS 私有 CA。 在创建客户网关之前，您可以使用从属 CA 创建私有证书 AWS Private Certificate Authority，然后在配置客户网关时指定证书。有关创建私有证书的信息，请参阅《AWS Private Certificate Authority 用户指南》中的创建和管理私有 CA。
（可选）设备。	与此客户网关关联的客户网关设备的名称。

加速 AWS Site-to-Site VPN 连接

您可以选择为 Site-to-Site VPN 连接启用加速。加速 Site-to-Site VPN 连接（加速 VPN 连接）用于 AWS Global Accelerator 将流量从您的本地网络路由到离您的客户网关设备最近的 AWS 边缘站点。AWS Global Accelerator 优化网络路径，使用无拥塞的 AWS 全球网络将流量路由到提供最佳应用程序性能的端点（有关更多信息，请参阅）。AWS Global Accelerator您可以使用加速 VPN 连接来避免通过公共 Internet 路由流量时可能发生的网络中断。

当您创建加速 VPN 连接时，我们将代表您创建和管理两个加速器（每个 VPN 隧道一个）。您无法使用 AWS Global Accelerator 控制台或自己查看或 APIs管理这些加速器。

有关支持加速 VPN 连接的 AWS 区域的信息，请参阅AWS 加速 Site-to-Site VPN FAQs。

启用加速

默认情况下，当您创建 Site-to-Site VPN 连接时，加速处于禁用状态。在传输网关上创建新的 Site-to-Site VPN 连接时，您可以选择启用加速。有关更多信息和步骤，请参阅创建公交网关 AWS Site-to-Site VPN 附件。

加速 VPN 连接使用单独的 IP 地址池作为隧道端点 IP 地址。两个 VPN 隧道的 IP 地址选自两个独立的网络区域。

规则和限制

要使用加速的 VPN 连接，应遵循以下规则：

- 只有连接到传输网关的 Site-to-Site VPN 连接才支持加速。虚拟私有网关不支持加速 VPN 连接。
- 加速 Site-to-Site VPN 连接不能与 AWS Direct Connect 公共虚拟接口一起使用。
- 您无法为现有 Site-to-Site VPN 连接开启或关闭加速。相反，您可以根据需要创建开启或关闭加速功能的新 Site-to-Site VPN 连接。然后，将您的客户网关设备配置为使用新的 Site-to-Site VPN 连接并删除旧的 Site-to-Site VPN 连接。
- NAT-遍历 (NAT-T) 是加速 VPN 连接所需的，并且默认情况下处于启用状态。如果您从 Amazon VPC 控制台下载了配置文件，请检查 NAT-T 设置并根据需要对其进行调整。
- 必须从客户网关设备启动加速 VPN 隧道的 IKE 协商。影响此行为的两个隧道选项是 `Startup Action` 和 `DPD Timeout Action`。有关更多信息，请参阅 VPN 隧道选项 和 VPN 隧道启动选项。
- Site-to-Site 由于全球加速器中对数据包分段的支持有限 AWS Global Accelerator，因此使用基于证书的身份验证的 VPN 连接可能与不兼容。有关更多信息，请参阅 AWS Global Accelerator 的工作原理。如果您需要使用基于证书的身份验证的加速 VPN 连接，您的客户网关设备必须支持 IKE 分段。否则，请勿启用 VPN 加速。

AWS Site-to-Site VPN 路由选项

AWS 建议发布特定的 BGP 路由，以影响虚拟专用网关中的路由决策。请查阅供应商文档，了解您的设备特有的命令。

创建多个 VPN 连接后，虚拟专用网关将使用静态分配的路由或 BGP 路由通告将网络流量发送到适当的 VPN 连接。使用哪一个路由取决于配置 VPN 连接的方式。在虚拟专用网关中存在相同路由的情况下，优先选择静态分配的路由，而非 BGP 通告路由。如果选择使用 BGP 通告的选项，则无法指定静态路由。

有关路由优先级的更多信息，请参阅路由表和路由优先级。

创建 Site-to-Site VPN 连接时，必须执行以下操作：

- 指定您计划使用的路由的类型（动态或静态）
- 更新子网的路由表

可添加到路由表的路由数有配额。有关更多信息，请参阅《Amazon VPC 用户指南》的 Amazon VPC 限额中的“路由表”部分。

主题

中的静态和动态路由 AWS Site-to-Site VPN

您选择的路由类型可由您的客户网关设备品牌和型号决定。如果您的客户网关设备支持边界网关协议 (BGP)，请在配置 Site-to-Site VPN 连接时指定动态路由。如果您的客户网关设备不支持 BGP，请指定静态路由。

如果您使用支持 BGP 广告的设备，则无需指定 Site-to-Site VPN 连接的静态路由，因为该设备使用 BGP 向虚拟专用网关通告其路由。如果您的设备不支持 BGP 通告，则必须选择静态路由，并输入您的网络的路由 (IP 前缀)，以便与虚拟私有网关建立通信。

我们建议您在适用的情况下使用支持 BGP 的设备，因为 BGP 协议可提供稳健的活性探测检查，可以在第一条隧道出现故障时协助对第二条 VPN 隧道进行失效转移。不支持 BGP 的设备也可执行健康检查，以便在需要时协助失效转移到第二条隧道。

您必须将客户网关设备配置为将流量从本地网络路由到 Site-to-Site VPN 连接。配置取决于设备的品牌和型号。有关更多信息，请参阅 AWS Site-to-Site VPN 客户网关设备。

路由表和 AWS Site-to-Site VPN 路由优先级

路由表决定了将网络流量从您的 VPC 定向到何处。在您的 VPC 路由表中，您必须为您的远程网络添加路由，并将虚拟私有网关指定为目标。这将使从 VPC 传送到您的远程网络的流量能够通过虚拟专用网关和其中一个 VPN 隧道进行路由。您可以为路由表启用路由传播，从而自动将您的网络路由传播到表。

我们使用路由表中与流量匹配的最具体的路由来判断数据流的路由方式 (最长前缀匹配)。如果路由表具有重叠或匹配的路由，则应用以下规则：

- 如果来自 Site-to-Site VPN 连接或 AWS Direct Connect 连接的传播路由与您的 VPC 的本地路由重叠，则即使传播的路由更具体，也最好使用本地路由。

- 如果来自 Site-to-Site VPN 连接或 AWS Direct Connect 连接的传播路由与其他现有静态路由具有相同的目标 CIDR 块（不能应用最长前缀匹配），则我们会优先考虑目标为 Internet 网关、虚拟专用网关、网络接口、实例 ID、VPC 对等连接、NAT 网关、传输网关或网关 VPC 终端节点的静态路由。

例如，以下路由表具有指向互联网网关的静态路由和指向虚拟私有网关的传播路由。这两条路由的目的地均为 `172.31.0.0/24`。在这种情况下，目标为 `172.31.0.0/24` 的所有流量均路由到互联网网关，这是静态路由，因此，其优先级高于传播路由。

目的地	目标
10.0.0.0/16	本地
172.31.0.0/24	vgw-11223344556677889（传播）
172.31.0.0/24	igw-12345678901234567（静态）

只有虚拟私有网关已知的 IP 前缀可接收来自您的 VPC 的数据流量，无论是通过 BGP 通告还是静态路由条目。虚拟专用网关不路由任何不以收到的 BGP 通告、静态路由条目或其附加 VPC CIDR 为目标的其他流量。虚拟专用网关不支持 IPv6 流量。

在虚拟私有网关收到路由信息时，它使用路径选择来决定如何路由流量。如果所有端点都运行正常，则最长前缀匹配适用。隧道端点的运行状况优先于其他路由属性。此优先级适用于 VPNs 虚拟专用网关和传输网关。如果前缀相同，则虚拟私有网关按照以下方式对路由进行优先排序：

- BGP 从连接传播路由 AWS Direct Connect

  黑洞路由不会通过 BGP 传播到 Site-to-Site VPN 客户网关。
- 为 Site-to-Site VPN 连接手动添加静态路由
- BGP 从 VPN 连接传播路由 Site-to-Site
- 要匹配每个 Site-to-Site VPN 连接使用 BGP 的前缀，将比较 AS 路径，首选 AS 路径最短的前缀。

> **Note**
>
> AWS 强烈建议使用支持非对称路由的客户网关设备。
> 对于支持非对称路由的客户网关设备，我们不建议使用 AS 路径前加，以确保两个隧道具有相同的 AS 路径。这有助于确保 multi-exit discriminator 使用我们在 VPN 隧道终端节点更新期间在隧道上设置的 (MED) 值来确定隧道优先级。

对于不支持非对称路由的客户网关设备，可以使用 AS PATH 前加和本地首选项，从而使某个隧道优先于另一个隧道。但是，当出口路径发生变化时，这可能会导致流量下降。

- 当 AS 的长度 PATHs 相同时，如果 AS_SEQUENCE 中的第一个 AS 在多条路径上相同，multi-exit discriminators (MEDs) 进行比较。首选具有最低 MED 值的路径。

在 VPN 隧道端点更新期间，路由优先级受到影响。

在 Site-to-Site VPN 连接上， AWS 选择两条冗余隧道中的一条作为主出口路径。此选择有时可能会更改，我们强烈建议您配置这两个隧道以实现高可用性并允许非对称路由。隧道端点的运行状况优先于其他路由属性。此优先级适用于 VPNs 虚拟专用网关和传输网关。

对于虚拟专用网关，将选择一条穿过网关上所有 Site-to-Site VPN 连接的隧道。要使用多个隧道，我们建议您探索等价多路径 (ECMP)，传输网关上的 Site-to-Site VPN 连接支持此功能。有关更多信息，请参阅 Amazon VPC 中转网关 中的中转网关。虚拟专用网关上的 Site-to-Site VPN 连接不支持 ECMP。

对于使用 BGP 的 VP Site-to-Site N 连接，主隧道可以通过以下方式标识 multi-exit discriminator (MED) 值标识。我们建议通告更为具体的 BGP 路由，以影响路由决策。

对于使用静态路由的 Site-to-Site VPN 连接，可以通过流量统计数据或指标来识别主隧道。

VPN 隧道终端节点更新期间的路由

Site-to-SiteVPN 连接由客户网关设备和虚拟专用网关或传输网关之间的两条 VPN 隧道组成。建议您配置两个隧道以实现冗余。 AWS 还会不时对您的 VPN 连接进行例行维护，这可能会短暂禁用 VPN 连接的两个隧道中的一个。有关更多信息，请参阅 隧道端点替换通知。

当我们在一条 VPN 隧道上执行更新时，我们会在另一条隧道上 multi-exit discriminator 设置一个较低的出站 (MED) 值。如果您已将客户网关设备配置为使用两个隧道，则 VPN 连接在隧道端点更新过程中使用另一条（上行）隧道。

Note

- 要确保首选具有较低 MED 的上行隧道，请确保您的客户网关设备对两个隧道使用相同的“权重和本地首选项”值（“权重和本地首选项”的优先级高于 MED）。

IPv4 还有进 IPv6 来的交通 AWS Site-to-Site VPN

您在传输网关上的 Site-to-Site VPN 连接可以支持 VPN 隧道内的 IPv4 IPv6流量或 VPN 隧道内的流量。默认情况下， Site-to-SiteVPN 连接支持 VPN 隧道内的 IPv4 流量。您可以配置新的 Site-to-Site VPN 连接以支持 VPN 隧道内的 IPv6 流量。然后，如果您的 VPC 和本地网络配置为寻 IPv6 址，则可以通过 VPN 连接发送 IPv6 流量。

如果您为 VPN 连接启 IPv6 用 VP Site-to-Site N 隧道，则每个隧道都有两个 CIDR 块。一个是大小为 /30 的 IPv4 CIDR 块，另一个是大小为 /126 IPv6 的 CIDR 块。

以下规则适用：

- IPv6 只有 VPN 隧道的内部 IP 地址支持地址。 AWS 终端节点的外部隧道 IP IPv4 地址是地址，您的客户网关的公有 IP 地址必须是 IPv4地址。
- Site-to-Site 不支持虚拟专用网关上的 VPN 连接 IPv6。
- 您无法启用对现有 Site-to-Site VPN 连接的 IPv6 支持。
- Site-to-SiteVPN 连接不能同时支持 IPv4 和 IPv6 流量。

有关创建 VPN 连接的更多信息，请参阅步骤 5：创建 VPN 连接。

开始使用 AWS Site-to-Site VPN

使用以下步骤来建立 AWS Site-to-Site VPN 连接。在创建过程中，您将指定虚拟私有网关、中转网关或“未关联”作为目标网关类型。如果您指定 “未关联”，则可以稍后选择目标网关类型，也可以将其用作 AWS Cloud WAN 的 VPN 附件。本教程帮助您使用虚拟私有网关创建 VPN 连接。该教程假定您的现有 VPC 具有一个或多个子网。

要使用虚拟私有网关设置连接，请完成以下步骤：

任务

- 先决条件
- 步骤 1：创建客户网关
- 步骤 2：创建目标网关
- 步骤 3：配置路由
- 步骤 4：更新安全组
- 步骤 5：创建 VPN 连接
- 步骤 6：下载配置文件
- 步骤 7：配置客户网关设备

相关任务

- 要为 AWS 云广域网创建 VPN 连接，请参阅创建云 WAN VPN 连接。
- 要在中转网关上创建 VPN 连接，请参阅创建中转网关 VPN 连接。

先决条件

您需要以下信息来设置和配置 VPN 连接的组件。

Item	信息
客户网关设备	VPN 连接在您一端的物理或软件设备。您需要供应商（例如 Cisco）、平台（例如 ISR 系列路由器）和软件版本（例如 IOS 12.4）。

Item	信息
客户网关	要在中创建客户网关资源 AWS，您需要以下信息： • 设备外部接口的可在 Internet 上路由的 IP 地址 • 路由类型：静态或动态 • 对于动态路由，为边界网关协议 (BGP) 自治系统编号 (ASN)。 • （可选）用于验证您的 VPN AWS Private Certificate Authority 的私有证书 有关更多信息，请参阅 客户网关选项。
（可选）BGP 会话 AWS 一侧的 ASN	您可以在创建虚拟私有网关或中转网关时指定此项。如果您未指定值，则会应用默认 ASN。有关更多信息，请参阅虚拟专用网关。
VPN 连接	要创建 VPN 连接，您需要以下信息： • 对于静态路由，为您的私有网络的 IP 前缀。 • （可选）每个 VPN 隧道的隧道选项。有关更多信息，请参阅 您的 AWS Site-to-Site VPN 连接的隧道选项。

步骤 1：创建客户网关

客户网关提供 AWS 有关您的客户网关设备或软件应用程序的信息。有关更多信息，请参阅 客户网关。

如果您计划使用私有证书对 VPN 进行身份验证，请使用从属 CA 创建私有证书 AWS Private Certificate Authority。有关创建私有证书的信息，请参阅《AWS Private Certificate Authority 用户指南》中的创建和管理私有 CA。

> **Note**
>
> 您必须指定 IP 地址，或者指定私有证书的 Amazon 资源名称。

使用控制台创建客户网关

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择客户网关。
3. 选择创建客户网关。
4. （可选）对于 Name tag（名称标签），为您的客户网关输入名称。这样做可创建具有 Name 键以及您指定的值的标签。
5. 对于 BGP ASN，输入您的客户网关的边界网关协议 (BGP) 自治系统编号 (ASN)。
6. 对于 IP address（IP 地址），输入客户网关设备的静态 Internet 可路由 IP 地址。如果您的客户网关设备位于为 NAT-T 而启用的 NAT 设备后面，请使用 NAT 设备的公有 IP 地址。
7. （可选）如果您想要使用私有证书，对于 Certificate ARN (证书 ARN)，请选择私有证书的 Amazon 资源名称。
8. （可选）对于设备，输入与此客户网关关联的客户网关设备的名称。
9. 选择创建客户网关。

使用命令行或 API 创建客户网关

- CreateCustomerGateway（亚马逊 EC2 查询 API）
- create-customer-gateway (AWS CLI)
- New-EC2CustomerGateway (AWS Tools for Windows PowerShell)

步骤 2：创建目标网关

要在您的 VPC 和本地网络之间建立 VPN 连接，您必须在连接 AWS 侧创建目标网关。目标网关可以是虚拟私有网关或中转网关。

创建虚拟专用网关

创建虚拟私有网关时，可以为网关的 Amazon 端指定自定义的私有自治系统编号 (ASN)，或使用 Amazon 原定设置 ASN。此 ASN 必须与您为客户网关指定的 ASN 不同。

创建虚拟专用网关后，必须将其连接到您的 VPC。

创建虚拟专用网关并将其连接到您的 VPC

1. 在导航窗格中，选择虚拟私有网关。
2. 选择 Create virtual private gateway（创建虚拟私有网关）。
3. （可选）对于名称标签，输入虚拟私有网关的名称。这样做可创建具有 Name 键以及您指定的值的标签。
4. 对于自治系统号（ASN），保留原定设置选择 Amazon 原定设置 ASN，以使用原定设置 Amazon ASN。否则，选择自定义 ASN并输入一个值。对于 16 位 ASN，该值必须在 64512 到 65534 范围内。对于 32 位 ASN，该值必须在 4200000000 到 4294967294 范围内。
5. 选择 Create virtual private gateway（创建虚拟私有网关）。
6. 选择您已创建的虚拟私有网关，然后依次选择 Actions（操作）和 Attach to VPC（挂载到 VPC）。
7. 对于可用 VPCs，选择您的 VPC，然后选择附加到 VPC。

使用命令行或 API 创建虚拟专用网关

- CreateVpnGateway（亚马逊 EC2 查询 API）
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

使用命令行或 API 将虚拟专用网关连接到 VPC

- AttachVpnGateway（亚马逊 EC2 查询 API）
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

创建中转网关

有关创建中转网关的更多信息，请参阅 Amazon VPC 中转网关 中的中转网关。

步骤 3：配置路由

要使您 VPC 中的实例可以访问您的客户网关，您必须配置路由表以包含您的 VPN 连接所使用的路由，并将它们指向您的虚拟私有网关或中转网关。

（虚拟私有网关）在路由表中启用路由传播

您可以为路由表启用路由传播，以自动传播 Site-to-Site VPN 路由。

对于静态路由，您为 VPN 配置指定的静态 IP 前缀会在 VPN 连接状态为 UP 时传播到路由表。同样，对于动态路由，来自客户网关的通告 BGP 路由会在 VPN 连接的状态为 UP 时传播到路由表。

> **Note**
>
> 如果您的连接中断但 VPN 连接保持在 UP 状态，您的路由表中的任何已传播路由将不会自动删除。请注意这一点，例如在您想将流量失效转移到静态路由时。在这种情况下，您可能必须禁用路由传播才能删除传播的路由。

使用控制台启用路由传播

1. 在导航窗格中，选择 Route tables（路由表）。
2. 选择与子网关联的路由表。
3. 在路由传播选项卡上，选择编辑路由传播。选择您在之前过程中创建的虚拟私有网关，然后选择保存。

> **Note**
>
> 如果您没有启用路由传播，则必须手动输入 VPN 连接使用的静态路由。为此，请选择您的路由表，然后依次选择 Routes（路由）、Edit（编辑）。在目的地中，添加您的 Site-to-Site VPN 连接使用的静态路由。对于 Target，选择虚拟专用网关 ID，然后选择 Save。

使用控制台禁用路由传播

1. 在导航窗格中，选择 Route tables（路由表）。
2. 选择与子网关联的路由表。
3. 在路由传播选项卡上，选择编辑路由传播。清除虚拟私有网关的传播复选框。

4. 选择保存。

使用命令行或 API 启用路由传播

- EnableVgwRoutePropagation（亚马逊 EC2 查询 API）
- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

使用命令行或 API 禁用路由传播

- DisableVgwRoutePropagation（亚马逊 EC2 查询 API）
- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

（中转网关）向路由表添加路由

如果您为中转网关启用了路由表传播，则 VPN 连接的路由将传播到中转网关路由表。有关更多信息，请参阅 Amazon VPC 中转网关 中的路由。

如果您将 VPC 连接到中转网关，并且您希望允许 VPC 中的资源能够访问您的客户网关，则必须向子网路由表添加路由以指向中转网关。

向 VPC 路由表中添加路由

1. 在导航窗格中，选择路由表。
2. 选择与 VPC 关联的路由表。
3. 在 Routes (路由) 选项卡上，选择 Edit routes (编辑路由)。
4. 选择 Add route (添加路由)。
5. 对于目标，输入目标 IP 地址范围。对于目标，选择中转网关。
6. 选择保存更改。

步骤 4：更新安全组

要允许从您的网络访问 VPC 中的实例，您必须更新安全组规则以启用入站 SSH、RDP 和 ICMP 访问。

向安全组添加规则以启用访问

1. 在导航窗格中，选择安全组。
2. 选择 VPC 中要允许访问的实例的安全组。
3. 在 Inbound Rules (入站规则) 选项卡上，选择 Edit inbound rules (编辑入站规则)。
4. 添加规则，这些规则允许从您的网络进行入站 SSH、RDP 和 ICMP 访问，然后选择保存规则。有关更多信息，请参阅《Amazon VPC 用户指南》中的使用安全组规则。

步骤 5：创建 VPN 连接

将客户网关与您之前创建的虚拟私有网关或中转网关结合使用，以创建 VPN 连接。

创建 VPN 连接

1. 在导航窗格中，选择 Site-to-Site VPN 连接。
2. 选择创建 VPN 连接。
3. （可选）对于名称标签，为您的 VPN 连接输入名称。这样做可创建具有 Name 键以及您指定的值的标签。
4. 对于 Target gateway type（目标网关类型），选择 Virtual private gateway（虚拟私有网关）或 Transit gateway（中转网关）。然后，选择您之前创建的虚拟私有网关或中转网关。
5. 对于客户网关，选择现有，然后从客户网关 ID 中选择之前创建的客户网关。
6. 根据您的客户网关设备是否支持边界网关协议 (BGP)，选择其中一个路由选项：
   - 如果您的客户网关设备支持 BGP，请选择动态（需要 BPG）。
   - 如果您的客户网关设备不支持 BGP，请选择静态。对于 Static IP Prefixes，为您的 VPN 连接的专用网络指定各自的 IP 前缀。
7. 选择预共享密钥存储类型：
   - 标准-预共享密钥直接存储在 Site-to-Site VPN 服务中。
   - S@@ ecrets Manager — 使用 AWS Secrets Manager存储预共享密钥。有关 Secrets Manager 的更多信息，请参阅使用 Secrets Manager 增强安全功能。
8. 如果您的目标网关类型是传输网关，则对于 IP 内部隧道版本，请指定 VPN 隧道是否支持 IPv4 或 IPv6流量。 IPv6 只有传输网关上的 VPN 连接才支持流量。
9. 如果您在 IP 版本内指定IPv4隧道，则可以选择为客户网关和允许通过 VPN 隧道进行通信的 AWS 端指定 IPv4 CIDR 范围。默认值为 `0.0.0.0/0`。

如果您在 IP 版本内指定IPv6隧道，则可以选择为客户网关和允许通过 VPN 隧道进行通信的 AWS 端指定 IPv6 CIDR 范围。这两个范围的默认值均为 `::/0`。

10. 对于外部 IP 地址类型，保留默认选项 PublicIpv4。
11. （可选）对于隧道选项，您可以选择为每个隧道指定以下信息：
    - 内部隧道 IPv4 地址`169.254.0.0/16`范围 IPv4 中的 CIDR 块大小为 /30。
    - 如果您在 IP 版本内IPv6为 Tunnel 指定，则内部隧道地址的`fd00::/8`范围中会有 /126 IPv6 CIDR 块。 IPv6
    - IKE 预共享密钥（PSK）。支持以下版本： IKEv1 或 IKEv2。
    - 要编辑隧道的高级选项，请选择编辑隧道选项。有关更多信息，请参阅 VPN 隧道选项。
12. 选择创建 VPN 连接。创建 VPN 连接可能需要几分钟时间。

使用命令行或 API 创建 VPN 连接

- CreateVpnConnection（亚马逊 EC2 查询 API）
- create-vpn-connection (AWS CLI)
- New-EC2VpnConnection (AWS Tools for Windows PowerShell)

步骤 6：下载配置文件

创建 VPN 连接后，您可以下载示例配置文件用于配置客户网关设备。

> **Important**
>
> 配置文件仅为示例，可能与您的目标 VPN 连接设置完全不符。它规定了大多数地区的 AES128 SHA1、和 Diffie-Hellman 组 2 的 VPN 连接的最低要求，以及 AWS 区域中的 AES128 SHA2、和 Diffie-Hellman 组 14 的最低要求。 AWS GovCloud 它还指定用于身份验证的预共享密钥。您必须修改示例配置文件以利用其他安全算法、Diffie-Hellman 组、私有证书和流量。 IPv6
>
> 我们在配置文件中引入了对许多常用客户网关设备的 IKEv2 支持，并将随着时间的推移继续添加其他文件。有关 IKEv2 支持的配置文件列表，请参阅AWS Site-to-Site VPN 客户网关设备。

权限

要从正确加载下载配置屏幕 AWS Management Console，您必须确保您的 IAM 角色或用户拥有以下 Amazon 的权限 EC2
APIs：`GetVpnConnectionDeviceTypes`和`GetVpnConnectionDeviceSampleConfiguration`。

使用控制台下载配置文件

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择您的 VPN 连接，然后选择下载配置。
4. 选择与您的客户网关设备对应的供应商、平台和软件和 IKE 版本。如果您的设备未列出，请选择 Generic (通用)。
5. 选择 Download（下载）。

使用命令行或 API 下载配置文件示例

- GetVpnConnectionDeviceTypes（亚马逊 EC2 API）
- GetVpnConnectionDeviceSampleConfiguration（亚马逊 EC2 查询 API）
- get-vpn-connection-device-类型 ()AWS CLI
- get-vpn-connection-device-示例配置 ()AWS CLI

步骤 7：配置客户网关设备

使用示例配置文件配置客户网关设备。客户网关设备是 VPN 连接在您这一端的实体设备或软件设备。有关更多信息，请参阅 AWS Site-to-Site VPN 客户网关设备。

AWS Site-to-Site VPN 建筑场景

在以下方案中，您将创建具有一个或多个客户网关设备的多个 VPN 连接。

使用同一客户网关设备的多个 VPN 连接

您可以使用相同的客户网关设备创建从您的本地位置到其他VPCs 位置的其他 VPN 连接。您可以为这些 VPN 连接中的每一个重复使用相同的客户网关 IP 地址。

将多个客户网关设备连接到单个虚拟专用网关 (AWS VPN CloudHub)

您可以从多个客户网关建立多个 VPN 连接到单个虚拟私有网关。这使您可以将多个位置连接到 AWS VPN CloudHub。有关更多信息，请参阅 使用 VPN 在 AWS Site-to-Site VPN 连接之间进行安全通信 CloudHub。您在多个地理位置布置了客户网关设备后，各个设备应通告该位置专有的唯一 IP 地址集。

使用第二个客户网关设备的冗余 VPN 连接

如需避免因您的客户网关设备不可用而造成连接中断，您可以使用第二个客户网关设置第二个 VPN 连接。有关更多信息，请参阅 用于故障转移的冗余 AWS Site-to-Site VPN 连接。在单个位置建立了冗余客户网关设备后，两个设备均会通告相同的 IP 地址。

以下是常见的 Site-to-Site VPN 架构：

- 单个和多个 VPN 连接
- the section called “冗余 VPN 连接”
- 使用 VPN 在 VPN 连接之间进行安全通信 CloudHub

AWS Site-to-Site VPN 单一和多个 VPN 连接示例

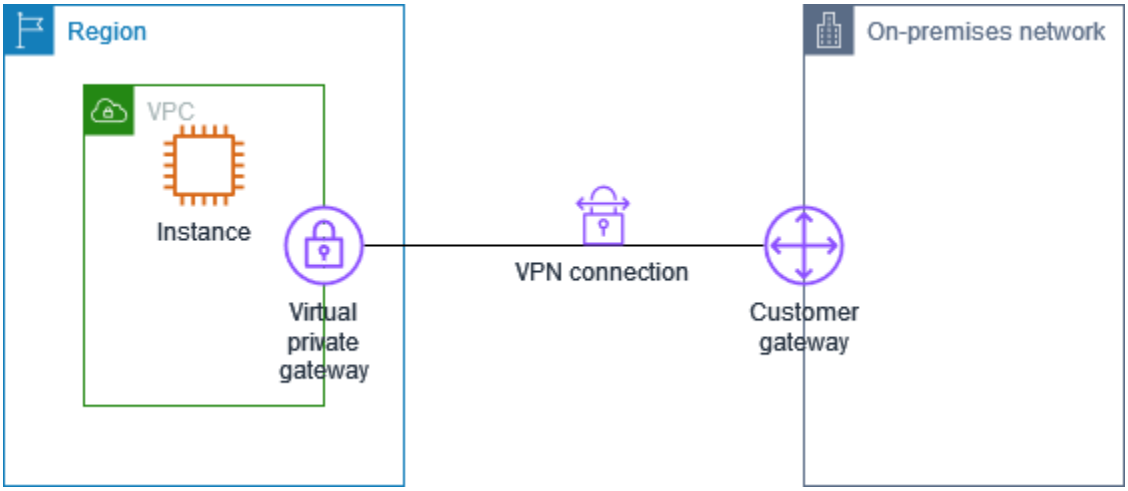
下图说明了单个和多个 Site-to-Site VPN 连接。

示例

- 单个 Site-to-Site VPN 连接
- 与传输网关的单个 Site-to-Site VPN 连接
- 多个 Site-to-Site VPN 连接
- 通过传输网关进行多个 Site-to-Site VPN 连接
- Site-to-Site 与 VPN 的连接 AWS Direct Connect
- 私有 IP Site-to-Site VPN 连接与 AWS Direct Connect

单个 Site-to-Site VPN 连接

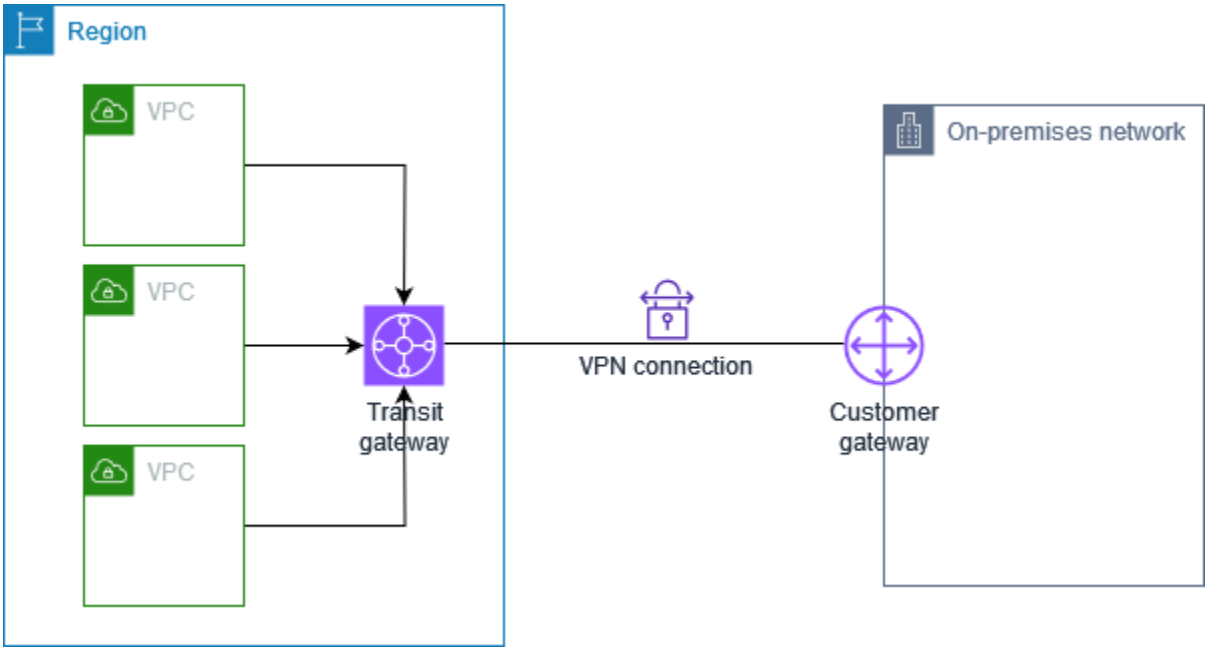
VPC 具有挂载的虚拟私有网关，您的本地（远程）网络内包括一个客户网关设备，您必须配置该设备以启用 VPN 连接。必须更新 VPC 路由表，以使从 VPC 通向网络的任何流量可以转至虚拟私有网关。



有关设置此方案的步骤，请参阅开始使用 AWS Site-to-Site VPN。

与传输网关的单个 Site-to-Site VPN 连接

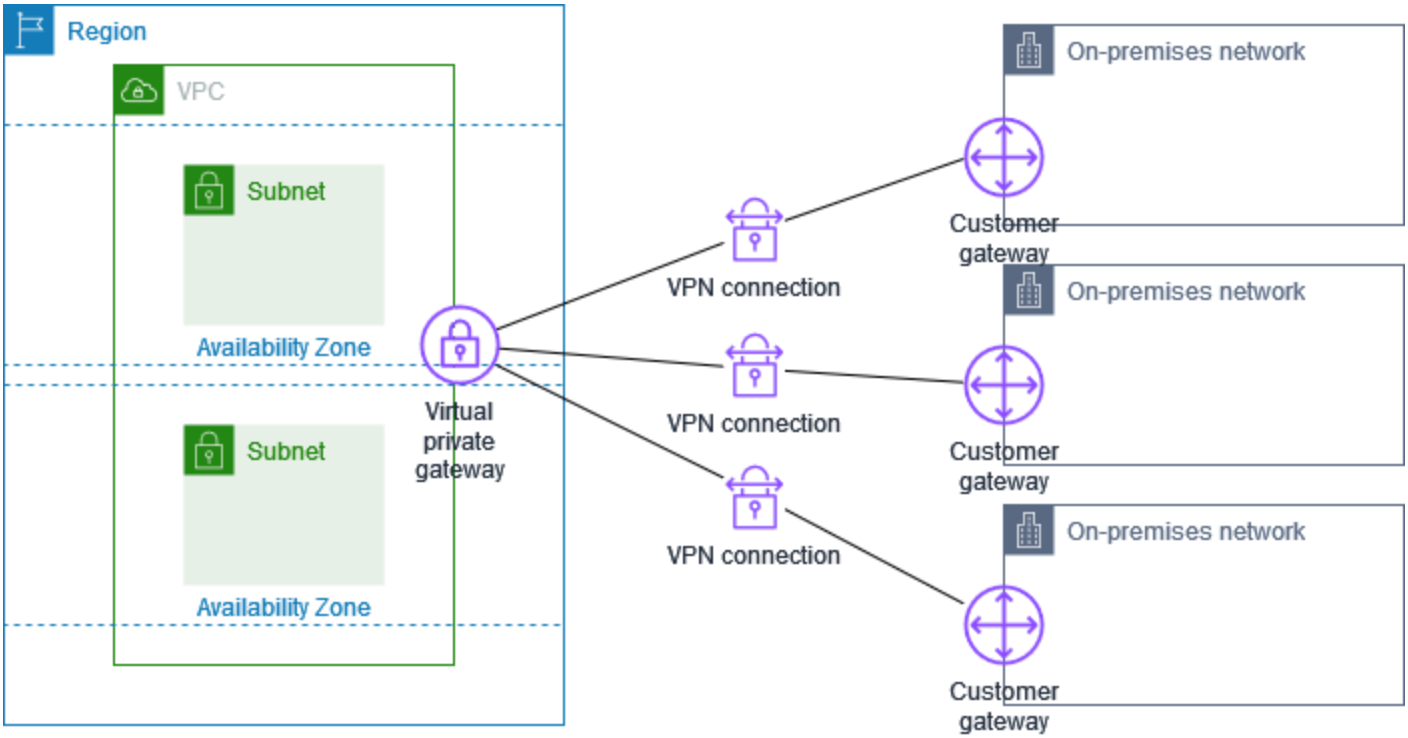
VPC 具有挂载的中转网关，您的本地（远程）网络内包括一个客户网关设备，您必须配置该设备以启用 VPN 连接。必须更新 VPC 路由表，以使从 VPC 通向网络的任何流量可以转至中转网关。



有关设置此方案的步骤，请参阅开始使用 AWS Site-to-Site VPN。

多个 Site-to-Site VPN 连接

VPC 有一个连接的虚拟专用网关，并且您有多个 Site-to-Site VPN 连接到多个本地位置。您可以设置路由，以使从您的 VPC 通向您的网络的数据流可以被路由到虚拟专用网关中。

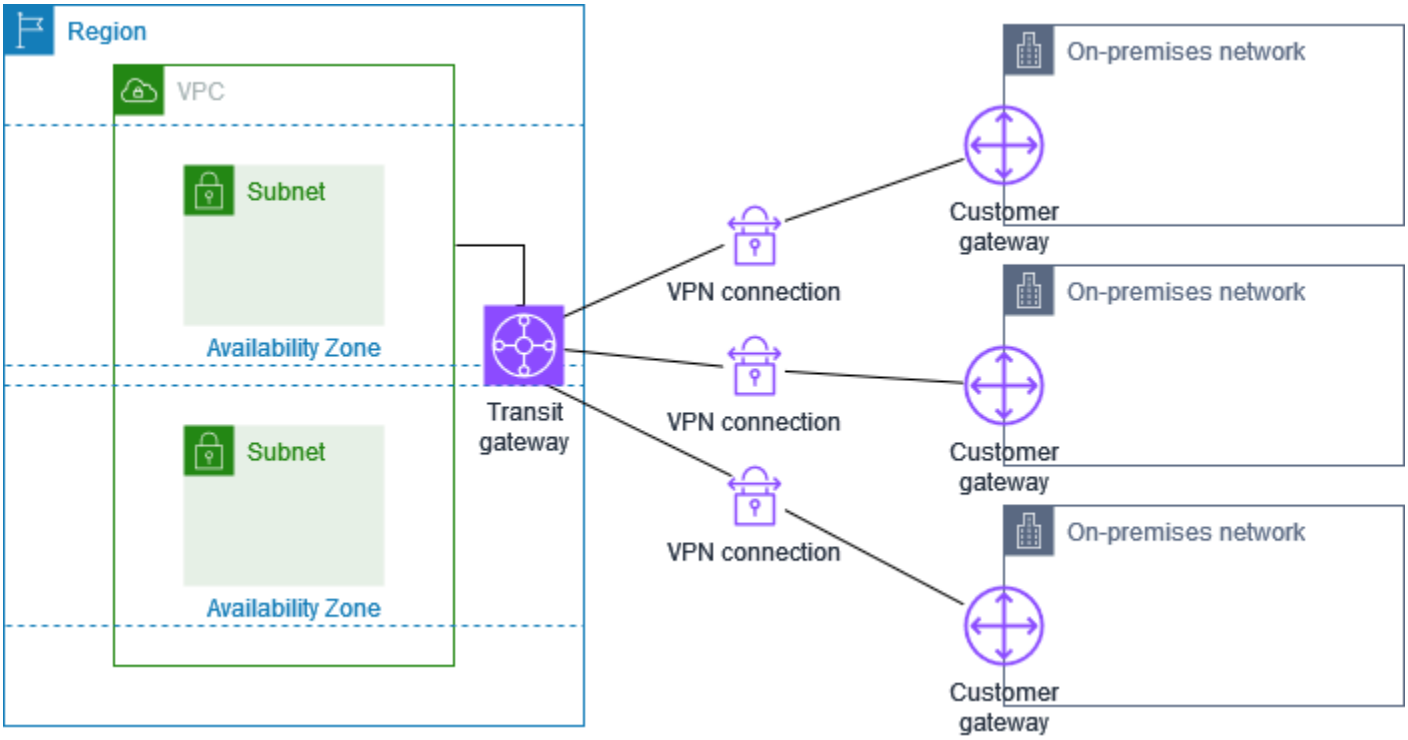


当您创建到单个 Site-to-Site VPC 的多个 VPN 连接时，您可以配置第二个客户网关以创建到同一外部位置的冗余连接。有关更多信息，请参阅 用于故障转移的冗余 AWS Site-to-Site VPN 连接。

您还可以使用此场景创建到多个地理位置的 Site-to-Site VPN 连接，并在站点之间提供安全的通信。有关更多信息，请参阅 使用 VPN 在 AWS Site-to-Site VPN 连接之间进行安全通信 CloudHub。

通过传输网关进行多个 Site-to-Site VPN 连接

VPC 有连接的传输网关，并且您有多个 Site-to-Site VPN 连接到多个本地位置。您可以设置路由，以使从 VPC 发往您的网络的任何流量都路由到中转网关中。

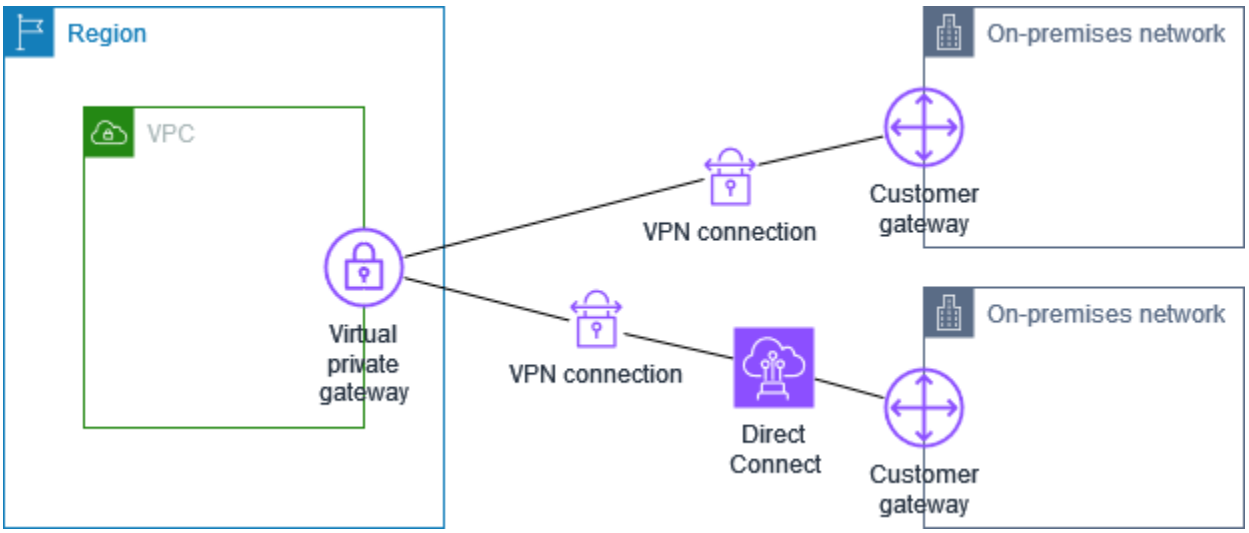


当您创建与单个中转网关的多个 Site-to-Site VPN 连接时，您可以配置第二个客户网关以创建到同一外部位置的冗余连接。

您还可以使用此场景创建到多个地理位置的 Site-to-Site VPN 连接，并在站点之间提供安全的通信。

Site-to-Site 与 VPN 的连接 AWS Direct Connect

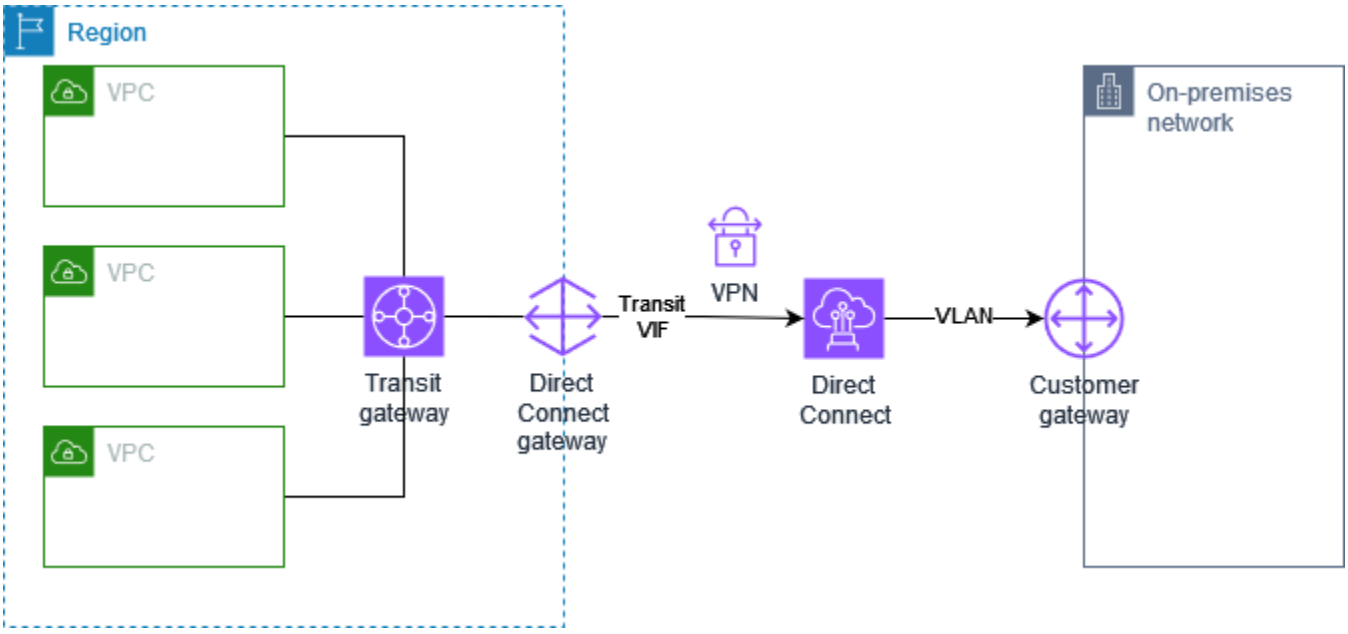
VPC 已连接虚拟专用网关，并通过连接到您的本地（远程）网络 AWS Direct Connect。您可以配置 AWS Direct Connect 公共虚拟接口，通过虚拟专用网关在您的网络与公共 AWS 资源之间建立专用的网络连接。您可以设置路由，以便所有来自您网络的 VPC 流量都路由到虚拟私有网关和 AWS Direct Connect 连接。



在同一个虚拟专用网关上同时设置 AWS Direct Connect 和 VPN 连接时，添加或删除对象可能会导致虚拟专用网关进入 “正在连接” 状态。这表示正在对内部路由进行更改，该更改将在 AWS Direct Connect 和 VPN 连接之间切换，以最大限度地减少中断和数据包丢失。此操作完成后，虚拟私有网关将返回到“已附加”状态。

私有 IP Site-to-Site VPN 连接与 AWS Direct Connect

使用私有 IP Site-to-Site VPN，您 AWS 无需使用公有 IP 地址即可加密本地网络之间的 AWS Direct Connect 流量。Private IP VPN AWS Direct Connect 可确保 AWS 与本地网络之间的流量既安全又私密，从而使客户能够遵守监管和安全规定。



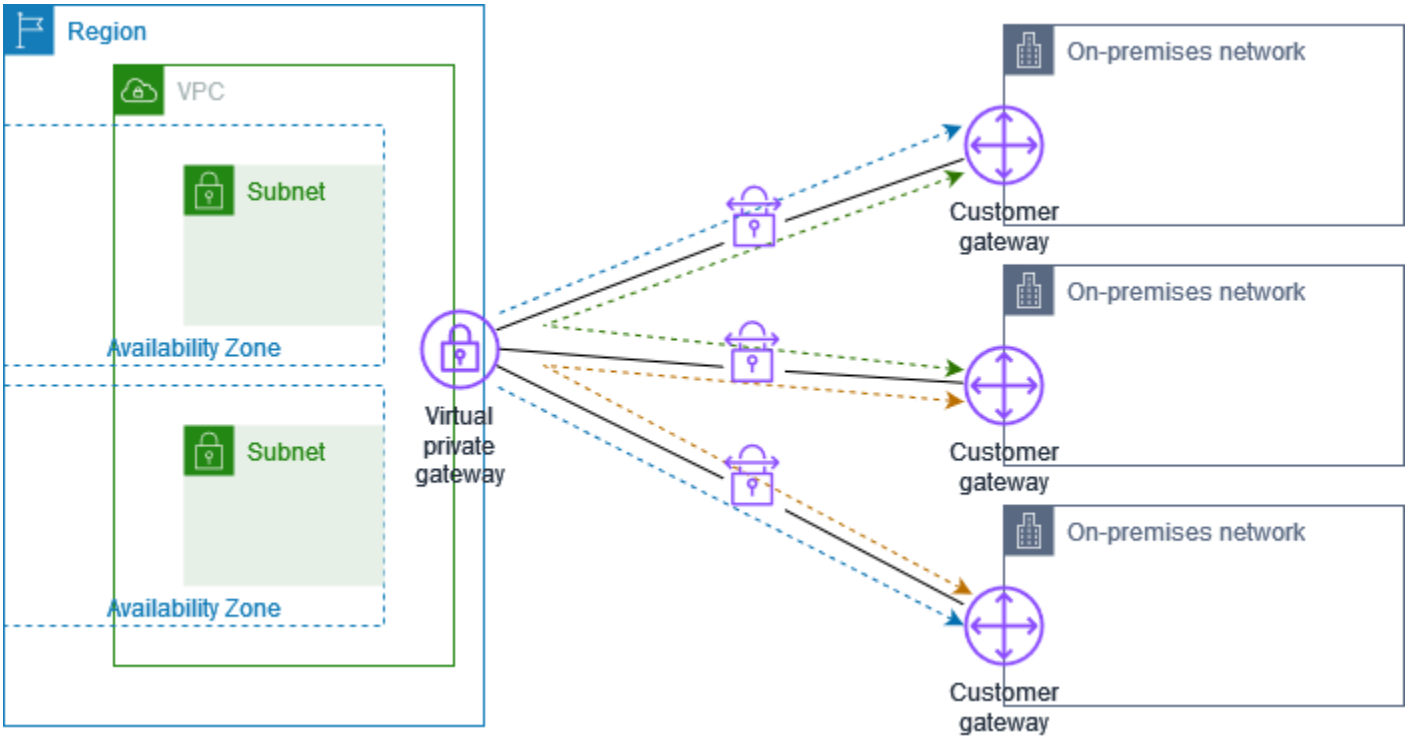
有关更多信息，请参阅以下博客文章：AWS Site-to-Site VPN 私有 IP 简介 VPNs。

使用 VPN 在 AWS Site-to-Site VPN 连接之间进行安全通信 CloudHub

如果您有多个 AWS Site-to-Site VPN 连接，则可以使用 AWS VPN 在站点之间提供安全的通信 CloudHub。这可使您的站点彼此进行通信，而不只是与 VPC 中的资源进行通信。VPN 的 CloudHub 运行 hub-and-spoke模式很简单，无论是否有 VPC，您都可以使用。如果您有多个分支机构和现有的互联网连接，并且希望为这些站点之间的主连接或备用连接实施一种方便、可能低成本的 hub-and-spoke模式，则此设计非常适合。

概览

下图显示了 VPN CloudHub 架构。虚线显示远程站点之间通过 VPN 连接路由的网络流量。站点的 IP 范围不得重叠。



对于此场景，请执行以下操作：

1. 创建单个虚拟私有网关。
2. 创建多个客户网关，每个网关都使用该网关的公有 IP 地址。您必须为每个客户网关使用唯一的边界网关协议 (BGP) 自治系统编号 (ASN)。
3. 创建从每个客户网关到公共虚拟专用网关的动态路由 Site-to-Site VPN 连接。

4. 配置客户网关设备以向虚拟私有网关通告特定于站点的前缀（例如 10.0.0.0/24、10.0.1.0/24）。路由通告会被每个 BGP 对等体接收并重新通告，使每个站点都可以向其他站点发送或接受数据。这是使用 VPN 连接的 VPN 配置文件中的网络语句完成的 Site-to-Site。根据您使用的路由类型，网络声明可能会有稍许不同。
5. 在子网路由表中配置路由以使 VPC 中的实例能够与站点通信。有关更多信息，请参阅（虚拟私有网关）在路由表中启用路由传播。您可以在路由表中配置聚合路由（例如，10.0.0.0/16）。在客户网关设备和虚拟私有网关之间使用更具体的前缀。

使用虚拟专用网关 AWS Direct Connect 连接的站点也可以成为 AWS VPN 的一部分 CloudHub。例如，您在纽约的公司总部可以与 VPC 建立 AWS Direct Connect 连接，而您的分支机构可以使用 Site-to-Site VPN 连接到 VPC。洛杉矶和迈阿密的分支机构可以相互发送和接收数据，也可以与您的公司总部发送和接收数据，所有这些都使用 AWS VPN CloudHub。

定价

要使用 AWS VPN CloudHub，您需要支付典型的亚马逊 V Site-to-Site PC VPN 连接费率。您需要按小时承担 VPN 与虚拟专用网关的连接费用。当您使用 AWS VPN 将数据从一个站点发送到另一个站点时 CloudHub，将数据从您的站点发送到虚拟专用网关是免费的。对于从虚拟私有网关转继到您的端点的数据，您仅需支付标准 AWS 数据传输费用即可。

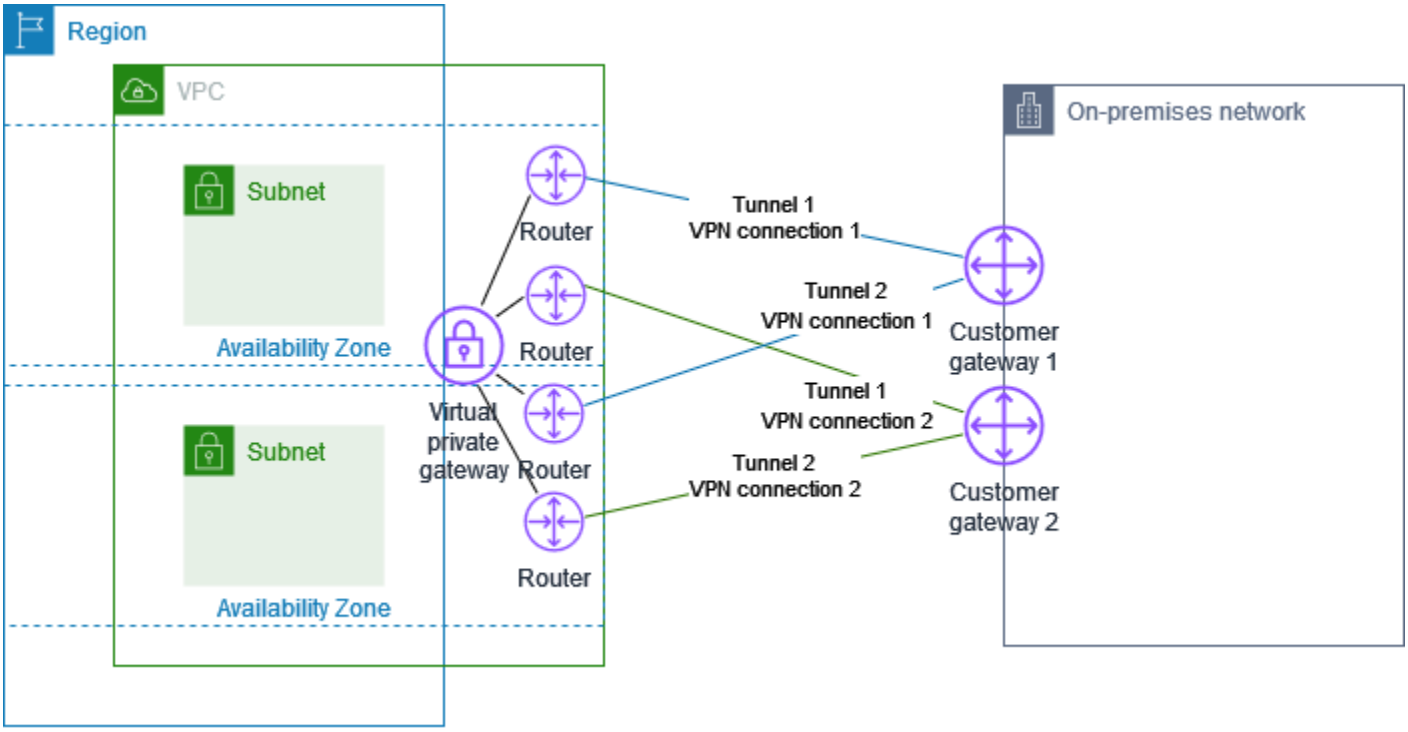
例如，如果您在洛杉矶有一个站点，在纽约有一个站点，并且两个站点都与虚拟专用网关有 Site-to-Site VPN连接，则您需要为每个 Site-to-Site VPN 连接支付每小时费率（因此，如果费率为每小时 0.05 美元，则总共为每小时 0.10 美元）。您还需要为通过每个 Site-to-Site VPN 连接从洛杉矶发送到纽约（反之亦然）的所有数据支付标准 AWS 数据传输费率。通过 Site-to-Site VPN 连接发送到虚拟专用网关的网络流量是免费的，但是通过 Site-to-Site VPN 连接从虚拟专用网关发送到终端节点的网络流量按标准 AWS 数据传输费率计费。

有关更多信息，请参阅 Site-to-Site VPN 连接定价。

用于故障转移的冗余 AWS Site-to-Site VPN 连接

为了在您的客户网关设备不可用时防止连接中断，您可以通过添加第二台客户网关设备来设置与您的 VPC 和虚拟专用网关的第二个 V Site-to-Site PN 连接。通过使用冗余 VPN 连接和客户网关设备，您可以在对其中一个设备进行维护时，保证数据流量可以继续流经第二个 VPN 连接。

下图演示了两个 VPN 连接。每个 VPN 连接都有其自己的隧道和其自己的客户网关。



对于此场景，请执行以下操作：

- 通过使用相同的虚拟 Site-to-Site专用网关并创建新的客户网关来设置第二个 VPN 连接。第二个 Site-to-Site VPN 连接的客户网关 IP 地址必须可公开访问。
- 配置第二个客户网关设备。两个设备都应向虚拟私有网关通告相同的 IP 范围。我们使用 BGP 路由确定流量的路径。如果一个客户网关设备发生故障，则虚拟私有网关会将所有流量定向到正常工作的客户网关设备。

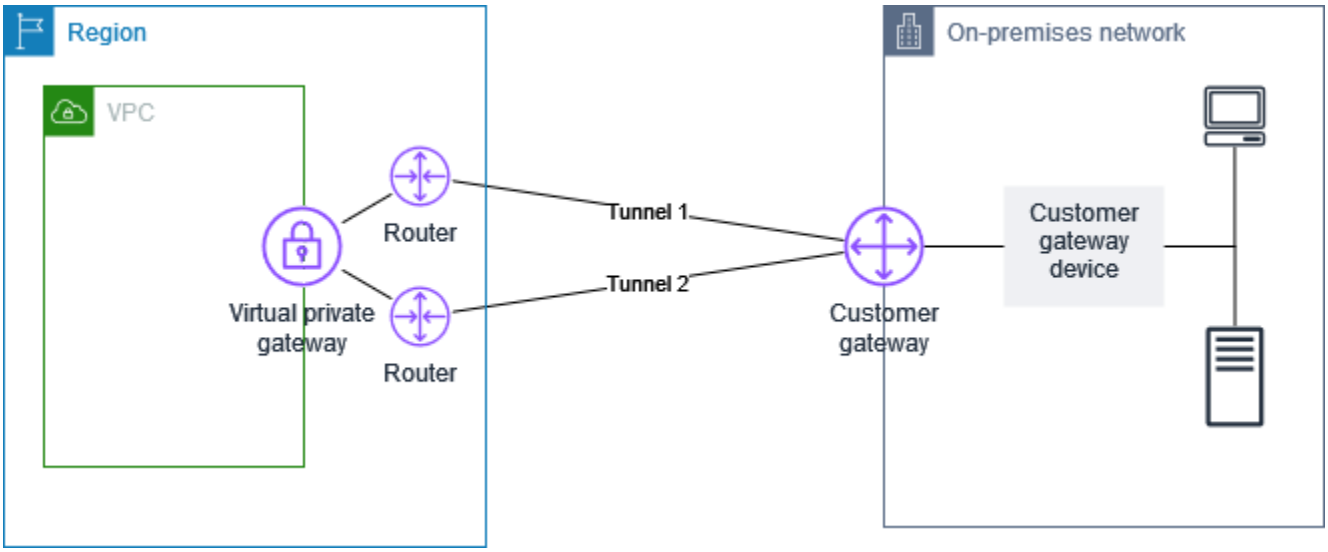
动态路由的 Site-to-Site VPN 连接使用边界网关协议 (BGP) 在您的客户网关和虚拟专用网关之间交换路由信息。静态路由的 Site-to-Site VPN 连接要求您在客户网关的您一侧输入远程网络的静态路由。通告 BGP 和静态输入的路由信息可以帮助两端的网关在出现故障时判断可用隧道，进而重新路由流量。我们建议您配置您的网络，使其使用 BGP 提供的路由信息 (若适用) 以选择可用路径。精确配置取决于您的网络架构。

有关创建和配置客户网关和 Site-to-Site VPN 连接的更多信息，请参阅开始使用 AWS Site-to-Site VPN。

AWS Site-to-Site VPN 客户网关设备

客户网关设备是您在本地网络中拥有或管理的物理设备或软件设备（在 Site-to-Site VPN 连接的您这边）。您或您的网络管理员必须将设备配置为使用 Site-to-Site VPN 连接。

下面的示意图显示您的网络、客户网关设备以及通往虚拟私有网关（挂载到您的 VPC）的 VPN 连接。客户网关和虚拟私有网关之间的两条线代表 VPN 连接的隧道。如果里面有设备故障 AWS，你的 VPN 连接会自动故障转移到第二条隧道，这样你的访问就不会中断。 AWS 还会不时对 VPN 连接执行例行维护，这可能会短暂禁用 VPN 连接的两个隧道中的一个。有关更多信息，请参阅 AWS Site-to-Site VPN 隧道端点替换。因此，当您配置客户网关设备时，务必将设备配置为使用这两条隧道。



有关设置 VPN 连接的步骤，请参阅开始使用 AWS Site-to-Site VPN。在此过程中，您可以在中创建客户网关资源 AWS，该资源可向您的设备提供 AWS 有关您的设备的信息，例如其面向公众的 IP 地址。有关更多信息，请参阅 您的 AWS Site-to-Site VPN 连接的客户网关选项。中的客户网关资源 AWS 不配置或创建客户网关设备。您必须自行配置设备。

您还可以在 AWS Marketplace 上查找软件 VPN 设备。

AWS Site-to-Site VPN 客户网关设备的要求

AWS 支持许多 Site-to-Site VPN 客户网关设备，我们为这些设备提供了可下载的配置文件。有关支持的设备列表以及下载配置文件的步骤，请参阅静态和动态路由配置文件。

如果您的设备不在支持的设备列表中，则下一节将介绍该设备建立 Site-to-Site VPN 连接必须满足的要求。

客户网关设备的配置有四个主要部分。以下符号表示配置的各个部分。

IKE	Internet 密钥交换 (IKE) 安全关联。这是交换用于建立 IPsec 安全关联的密钥所必需的。
IPsec	IPsec 安全关联。此项用于处理隧道的加密、身份验证等。
Tunnel	隧道接口。此项用于接收来往隧道的流量。
BGP	（可选）建立边界网关协议 (BGP) 对等体。对于使用 BGP 的设备，这会在客户网关设备和虚拟私有网关之间交换路由。

下表列出了对客户网关设备的要求、相关的 RFC（用于参考）和有关该要求的备注。

每个 VPN 连接由两条单独的隧道构成。每个隧道都包含一个 IKE 安全关联、一个 IPsec 安全关联和 BGP 对等连接。每条隧道只能有一个唯一的安全关联 (SA) 对（一个入站和一个出站），因此两条隧道（四个）总共只能有两个唯一的安全关联 (SA SAs) 对。有些设备使用基于策略的 VPN 并创建任意多 SAs 个 ACL 条目。因此，可能需要合并您的规则，然后再进行筛选，以使您不允许多余的流量通过。

默认情况下，当生成流量并且从 VPN 连接的一端启动 IKE 协商时，VPN 隧道将启动。您可以将 VPN 连接配置为改为从连接 AWS 端启动 IKE 协商。有关更多信息，请参阅 AWS Site-to-Site VPN 隧道启动选项。

VPN 端点支持重新加密，如果客户网关设备没有发送任何重新商通信，则当阶段 1 即将到期时，可以启动谈判。

要求	RFC	评论
建立 IKE 安全关联 IKE	RFC 2409 RFC 7296	首先使用预共享密钥或 AWS Private Certificate Authority 用作身份验证器的私有证书在虚拟专用网关和客户网关设备之间建立 IKE 安全关联。建立后，IKE 即协商临时密钥，以便对将来的 IKE 消息进行保密。参数之间必须完全一致，包括加密和身份验证参数。 在中创建 VPN 连接时 AWS，您可以为每个隧道指定自己的预共享密钥，也可以让它为您 AWS 生成一个预共享密钥。或者，您可以使用指定用于客户网关设备的私有证书。 AWS Private Certificate Authority 有关配置

要求	RFC	评论
		VPN 隧道的更多信息，请参阅 您的 AWS Site-to-Site VPN 连接的隧道选项。 支持以下版本： IKEv1 和 IKEv2。 我们仅支持主模式 IKEv1。 Site-to-SiteVPN 服务是一种基于路由的解决方案。如果您使用的是基于策略的配置，则必须将配置限制为单个安全关联 (SA)。
在隧道模式下建立 IPsec 安全关联 IPsec	RFC 4301	使用 IKE 临时密钥，在虚拟专用网关和客户网关设备之间建立密钥以形成 IPsec 安全关联 (SA)。网关间的流量使用该 SA 进行加密和解密。IKE 会定期自动轮换用于加密 IPsec SA 内部流量的临时密钥，以确保通信的机密性。
使用 AES 128 位加密或 AES 256 位加密功能	RFC 3602	加密功能用于确保 IKE 和 IPsec 安全关联的隐私。
使用 SHA-1 或 SHA-2 (256) 哈希函数	RFC 2404	此哈希函数用于对 IKE 和 IPsec安全关联进行身份验证。
使用 Diffie-Hellman Perfect Forward Secrecy。	RFC 2409	IKE 使用 Diffie-Hellman 建立临时密钥，确保客户网关设备和虚拟私有网关之间的所有通讯安全可靠。 支持以下组： • 第 1 阶段组：2、14-24 • 第 2 阶段组：2、5、14-24
（动态路由 VPN 连接）使用失效对等体检测 IPsec	RFC 3706	失效对端检测的运用让 VPN 设备能够快速识别网络条件阻止数据包经由 Internet 传送的情况。发生此情况时，网关将删除该安全关联并尝试建立新关联。在此过程中，如果可能，将使用备用 IPsec 隧道。

要求	RFC	评论
（动态路由 VPN 连接）将隧道绑定到逻辑接口（基于路由的 VPN） 	无	您的设备必须能够将 IPsec 隧道绑定到逻辑接口。该逻辑接口包含用来向虚拟私有网关建立 BGP 对等体的 IP 地址。该逻辑接口不应执行额外的封装（例如：GRE 或 IP 中的 IP）。应将接口最大传输单位 (MTU) 设置为 1399 字节。
（动态路由 VPN 连接）建立 BGP 对等体 	RFC 4271	对于使用 BGP 的设备，BGP 用于在客户网关设备和虚拟私有网关间交换路由。所有 BGP 流量都经过加密并通过 IPsec 安全协会传输。两个网关都需要 BGP 才能交换可通过 SA 访问的 IP 前缀。 IPsec

AWS VPN 连接不支持 Path MTU 发现 (RFC 1 191)。

如果您的客户网关设备和 Internet 之间有防火墙，请参阅AWS Site-to-Site VPN 客户网关设备的防火墙规则。

AWS Site-to-Site VPN 客户网关设备的最佳实践

使用 IKEv2

我们强烈建议使用您 IKEv2 的 Site-to-Site VPN 连接。 IKEv2 是一种比现在更简单、更强大、更安全的协议 IKEv1。只有当您的客户网关设备不支持时，才应使用 IKEv1 IKEv2。有关 IKEv1 和之间区别的更多详细信息 IKEv2，请参阅的附录 A RFC7296。

重设数据包上的“Don't Fragment (DF)”标记

部分数据包带有一个标记，称为 Don't Fragment (DF) 标记，表示该数据包不应分片。若数据包带有该标记，网关就会生成一条“ICMP Path MTU Exceeded”消息。部分情况中，应用程序不含可处理这些 ICMP 消息和减少每个数据包数据传输量的充分机制。部分 VPN 设备可以忽略该 DF 标记并按要求无条件分片数据包。如果您的客户网关设备拥有该功能，我们建议您酌情使用。有关更多详细信息，请参阅 RFC 791。

加密前分片 IP 数据包

如果通过 Site-to-Site VPN 连接发送到的数据包超过 MTU 大小，则必须对其进行分段。为避免性能降低，我们建议您将客户网关设备配置为在数据包加密之前对其进行分段。 Site-to-Site然后，VPN

将重新组装所有分段的数据包，然后将其转发到下一个目的地，以实现更高的 AWS 网络 packet-per-second流量。有关更多详细信息，请参阅 RFC 4459。

确保数据包大小不超过目标网络的 MTU

由于 Site-to-Site VPN 在转发到下一个目的地之前会重新组合从您的客户网关设备收到的任何分段数据包，因此请记住，对于接下来转发这些数据包的目标网络，例如通过或使用某些协议（例如 Radius），可能会考虑数据包大小/MTU。 AWS Direct Connect

根据使用的算法调整 MTU 和 MSS 大小

TCP 数据包通常是 IPsec 隧道中最常见的数据包类型。 Site-to-SiteVPN 支持的最大传输单元 (MTU) 为 1446 字节，相应的最大分段大小 (MSS) 为 1406 字节。但加密算法的标头大小各异，可能会导致无法实现这些最大值。要通过避免碎片化获得最佳性能，我们建议您特别根据所使用的算法设置 MTU 和 MSS。

使用下表来设置 MTU/MSS 以避免碎片化问题并实现最佳性能：

加密算法	哈希算法	NAT 遍历	MTU	MSS () IPv4	MSS (IPv6-in-IPv4)
AES-GCM-16	不适用	disabled	1446	1406	1386
AES-GCM-16	不适用	已启用	1438	1398	1378
AES-CBC	SHA1/SHA2-256	disabled	1438	1398	1378
AES-CBC	SHA1/SHA2-256	已启用	1422	1382	1362
AES-CBC	SHA2-384	disabled	1422	1382	1362
AES-CBC	SHA2-384	已启用	1422	1382	1362
AES-CBC	SHA2-512	disabled	1422	1382	1362
AES-CBC	SHA2-512	已启用	1406	1366	1346

> **Note**
>
> AES-GCM 算法涵盖加密和身份验证，因此不存在会影响 MTU 的明确身份验证算法选择。

禁用 IKE 唯一 IDs

一些客户网关设备支持的设置可确保每个隧道配置最多存在一个第 1 阶段安全关联。此设置可能导致 VPN 对等网络之间的第 2 阶段状态不一致。如果您的客户网关设备支持此设置，建议将其禁用。

AWS Site-to-Site VPN 客户网关设备的防火墙规则

您必须有一个静态 IP 地址才能用作将您的客户网关设备连接到端点的 IPsec隧道的 AWS Site-to-Site VPN 终端节点。如果在您的客户网关设备 AWS 之间设置了防火墙，则必须遵守下表中的规则才能建立 IPsec 隧道。 AWS-side 的 IP 地址将在配置文件中。

传入（从 Internet）

输入规则 I1	
源 IP	Tunnel1 外部 IP
目的 IP	客户网关
协议	UDP
源端口	500
目的地	500
输入规则 I2	
源 IP	Tunnel2 外部 IP
目的 IP	客户网关
协议	UDP
源端口	500
目的地端口	500

输入规则 I3

源 IP	Tunnel1 外部 IP
目的 IP	客户网关
协议	IP 50（ESP）

输入规则 I4

源 IP	Tunnel2 外部 IP
目的 IP	客户网关
协议	IP 50（ESP）

传出（向 Internet）

输出规则 O1

源 IP	客户网关
目的 IP	Tunnel1 外部 IP
协议	UDP
源端口	500
目的地端口	500

输出规则 O2

源 IP	客户网关
目的 IP	Tunnel2 外部 IP
协议	UDP
源端口	500
目的地端口	500

输出规则 O3	
源 IP	客户网关
目的 IP	Tunnel1 外部 IP
协议	IP 50（ESP）
输出规则 O4	
源 IP	客户网关
目的 IP	Tunnel2 外部 IP
协议	IP 50（ESP）

规则 I1、I2、O1、和 O2 启用 IKE 数据包的传输。规则 I3、I4、O3 和 O4 允许传输包含加密 IPsec 网络流量的数据包。

> **Note**
>
> 如果您在设备上使用 NAT 穿越 (NAT-T)，请确保也允许端口 4500 上的 UDP 流量在您的网络和端点之间传输。 AWS Site-to-Site VPN 检查您的设备是否通告 NAT-T。

AWS Site-to-Site VPN 客户网关设备的静态和动态配置文件

创建 VPN 连接后，您还可以选择从 Amazon VPC 控制台或使用 EC2 API 下载 AWS提供的示例配置文件。请参阅步骤 6：下载配置文件了解更多信息。还可以从各个页面下载专门用于静态和动态路由的配置的 .zip 文件示例。

AWS提供的示例配置文件包含特定于您的 VPN 连接的信息，您可以使用这些信息来配置您的客户网关设备。这些设备特定的配置文件仅适用于 AWS 测试过的设备。如果未列出您的特定客户网关设备，您可以下载一个通用配置文件以开始使用。

> **Important**
>
> 配置文件仅为示例，可能与您预期的 Site-to-Site VPN 连接设置不完全匹配。它规定了大多数地区的 AES128 SHA1、和 Diffie-Hellman 组 2 的 Site-to-Site VPN 连接的最低要求，以及

AWS 区域中的 AES128 SHA2、和 Diffie-Hellman 组 14 的最低要求。 AWS GovCloud 它还指定用于身份验证的预共享密钥。您必须修改示例配置文件以利用其他安全算法、Diffie-Hellman 组、私有证书和流量。 IPv6

> **Note**
>
> 这些设备特定的配置文件由尽 AWS 力提供。虽然它们已经过测试 AWS，但这种测试是有限的。如果您遇到配置文件问题，可能需要与特定供应商联系以获得更多支持。

下表包含设备列表，这些设备具有可供下载的示例配置文件，该文件已更新为支持 IKEv2。我们在配置文件中引入了对许多常用客户网关设备的 IKEv2 支持，并将随着时间的推移继续添加其他文件。随着更多示例配置文件的添加，此列表将更新。

Vendor	平台	软件
检查点	Gaia	R80.10+
Cisco Meraki	MX 系列	15.12+ (WebUI)
Cisco Systems, Inc。	ASA 5500 系列	ASA 9.7+ VTI
Cisco Systems, Inc。	CSRv AMI	IOS 12.4+
Fortinet	Fortigate 40+ 系列	FortiOS 6.4.4+ (GUI)
Juniper Networks, Inc。	J 系列路由器	JunOS 9.5+
Juniper Networks, Inc。	SRX 路由器	JunOS 11.0+
Mikrotik	RouterOS	6.44.3
Palo Alto Networks	PA 系列	PANOS 7.0+
SonicWall	NSA、TZ	OS 6.5
Sophos	Sophos 防火墙	v19+
Strongswan	Ubuntu 16.04	Strongswan 5.5.1+

Vendor	平台	软件
Yamaha	RTX 路由器	Rev.10.01.16+

AWS Site-to-Site VPN 客户网关设备的可下载静态路由配置文件

要下载包含特定于您的 Site-to-Site VPN 连接配置值的示例配置文件，请使用 Amazon VPC 控制台、AWS 命令行或 Amazon EC2 API。有关更多信息，请参阅 步骤 6：下载配置文件。

您也可以下载不包含特定于您的 Site-to-Site VPN 连接配置值的静态路由的通用示例配置文件：static-routing-examples. zip

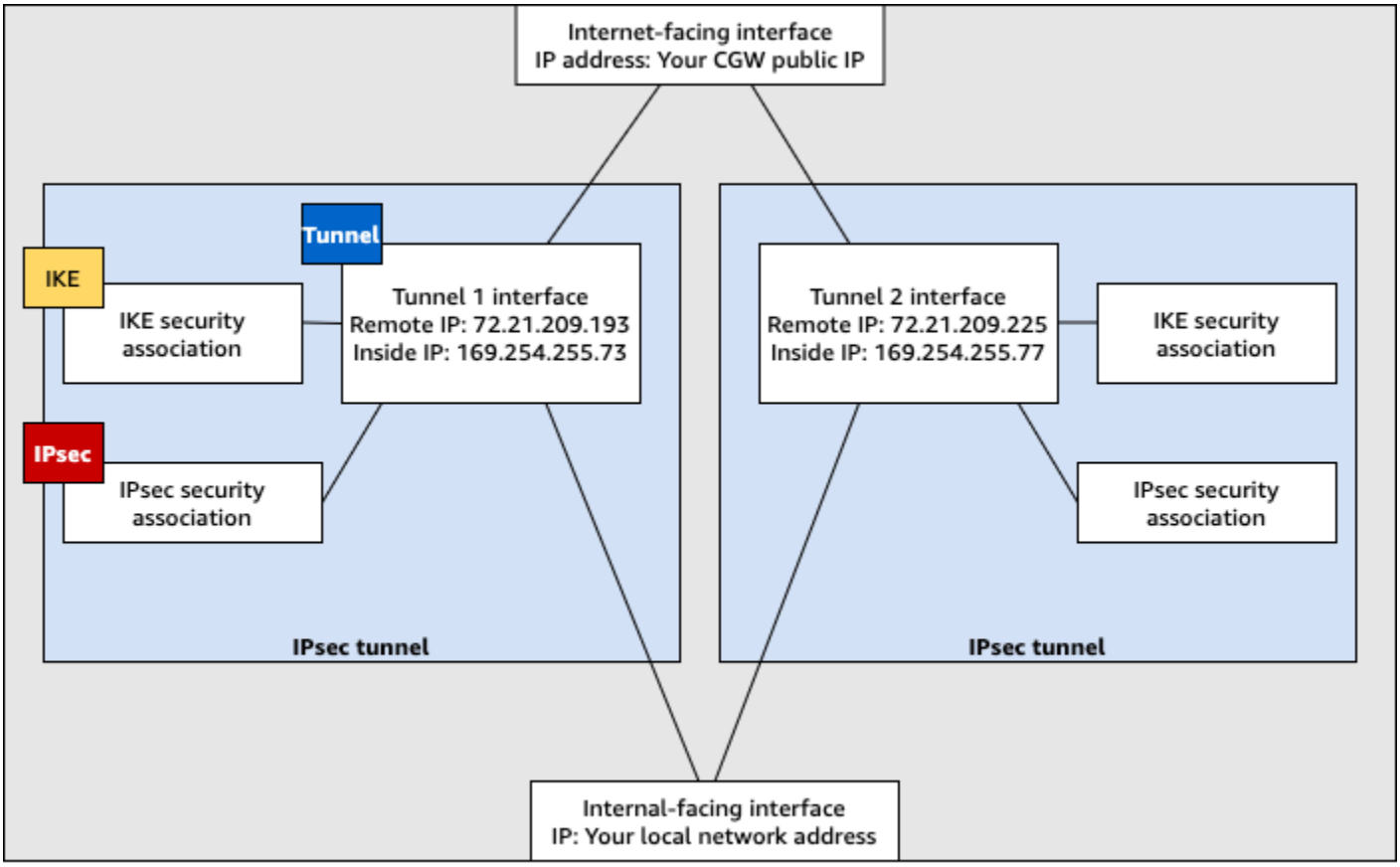
这些文件对某些组件使用占位符值。例如，它们使用：

- VPN 连接 ID、客户网关 ID 和虚拟私有网关 ID 的示例值
- 远程（外部）IP 地址 AWS 端点的占位符（*AWS_ENDPOINT_1*和*AWS_ENDPOINT_2*）
- 客户网关设备上可路由互联网的外部接口 IP 地址的占位符 () *your-cgw-ip-address*
- 预共享密钥值的占位符 () pre-shared-key
- IP 地址内的隧道的示例值。
- MTU 设置的示例值。

> **Note**
>
> 示例配置文件中提供的 MTU 设置仅供示例之用。有关根据自己的情况设置最佳 MTU 值的信息，请参阅AWS Site-to-Site VPN 客户网关设备的最佳实践。

除了提供占位符值外，这些文件还指定了大多数地区的、和 Diffie-Hellman 组 2 的 Site-to-Site VPN 连接的最低要求，以及 AWS 区域中的 AES128 SHA1 AES128 SHA2、和 Diffie-Hellman 组 14 的最低要求。 AWS GovCloud它们还指定用于身份验证的预共享密钥。您必须修改示例配置文件以利用其他安全算法、Diffie-Hellman 组、私有证书和流量。 IPv6

下图概述了在客户网关设备上配置的各种组件。它包括隧道接口 IP 地址的示例值。



为 AWS Site-to-Site VPN 客户网关设备配置静态路由

以下是使用客户网关设备的用户界面（如果可用）配置该设备的一些示例过程。

Check Point

如果您的设备是运行 R77.10 或更高版本的 Check Point Security Gateway 设备，则使用 Gaia 操作系统和 Check Point 配置客户网关设备的步骤。 SmartDashboard你也可以参阅 Check Point 支持中心上的 Check Point Secur IPsec ity Gateway VPN to Amazon Web Services VPC 的文章。

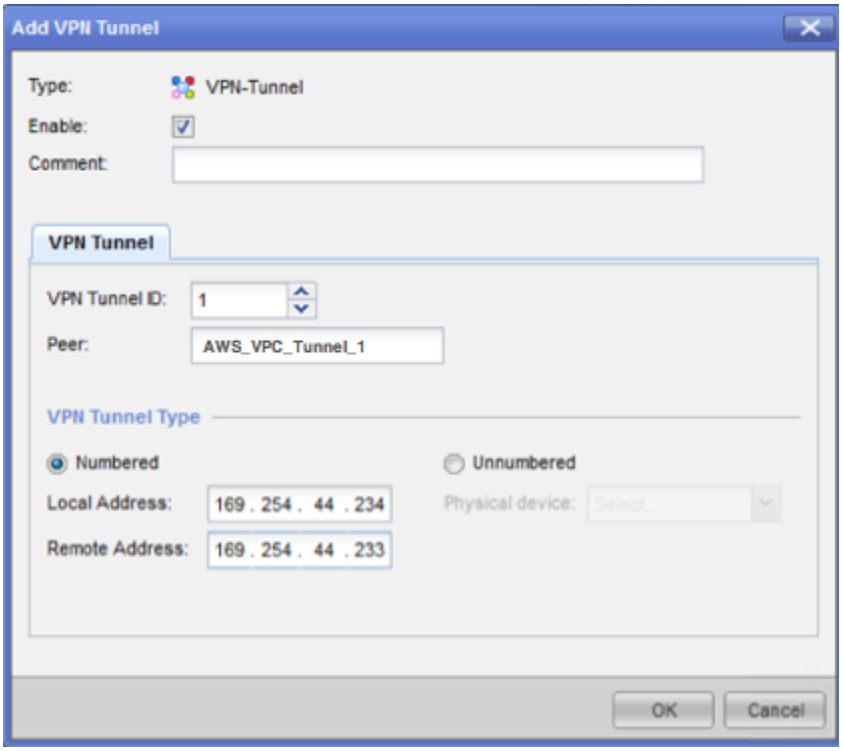
配置隧道接口

第一步是创建 VPN 隧道并为每条隧道提供客户网关和虚拟专用网关的私有（内部）IP 地址。要创建第一条隧道，请使用配置文件的 `IPSec Tunnel #1` 部分下提供的信息。要创建第二条隧道，请使用配置文件的 `IPSec Tunnel #2` 部分中提供的值。

1. 打开检查点安全网关设备的 Gaia 门户。
2. 选择 Network Interfaces、Add、VPN tunnel。

3. 在对话框中，配置如下设置，然后在配置完成后选择 OK：

   - 对于 VPN Tunnel ID，输入任何唯一值，例如 1。
   - 对于 Peer，输入隧道的唯一名称，例如 `AWS_VPC_Tunnel_1` 或 `AWS_VPC_Tunnel_2`。
   - 确保已选择 Numbered (编号)，对于 Local Address (本地地址)，输入配置文件中为 `CGW Tunnel IP` 指定的 IP 地址，例如，`169.254.44.234`。
   - 对于 Remote Address，输入配置文件中为 `VGW Tunnel IP` 指定的 IP 地址，例如，`169.254.44.233`。



4. 通过 SSH 连接到您的安全网关。如果您使用的是非默认 Shell，请通过运行以下命令来更改为 clish：`clish`
5. 对于隧道 1，请运行以下命令。

```
set interface vpnt1 mtu 1436
```

   对于隧道 2，请运行以下命令。

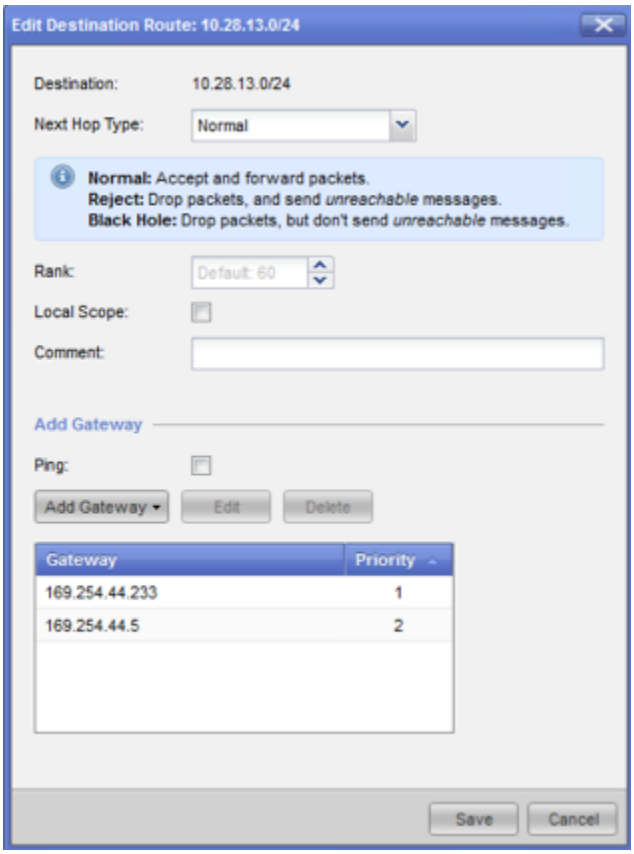
```
set interface vpnt2 mtu 1436
```

6. 重复这些步骤以使用配置文件的 `IPSec Tunnel #2` 部分下的信息创建另一条隧道。

配置静态路由

在此步骤中，将为每条隧道指定到 VPC 中子网的静态路由以便能够通过隧道接口发送流量。第二条隧道在第一条隧道出现问题时将启用失效转移。如果检测到问题，将从路由表中删除基于策略的静态路由，并激活第二个路由。您还必须允许检查点网关对隧道的另一端执行 Ping 操作以检查隧道是否已启动。

1. 在 Gaia 门户中，选择IPv4 静态路由，添加。
2. 指定您的子网的 CIDR，例如，`10.28.13.0/24`。
3. 选择 Add Gateway、IP Address。
4. 输入配置文件中为 `VGW Tunnel IP` 指定的 IP 地址 (例如，`169.254.44.233`)，并指定优先级为 1。
5. 选择 Ping。
6. 使用配置文件的 `VGW Tunnel IP` 部分下的 `IPSec Tunnel #2` 值，对第二条隧道重复步骤 3 和 4。指定优先级为 2。



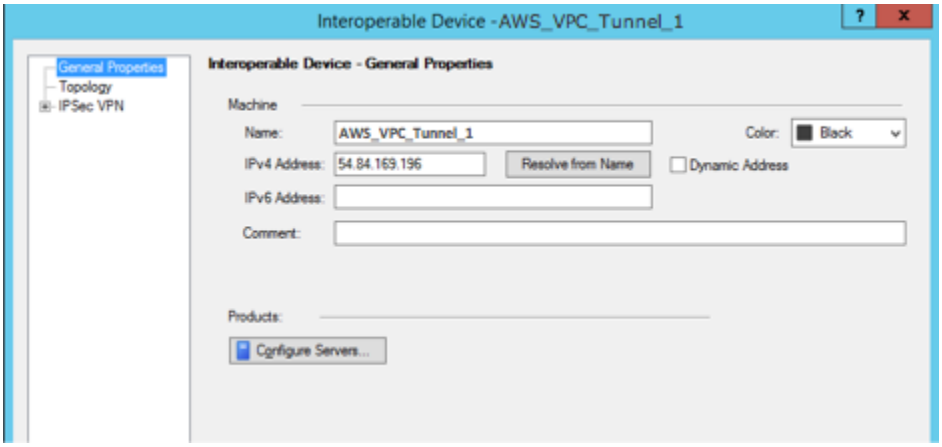
7. 选择保存。

如果您使用的是集群，请对集群的其他成员重复上述步骤。

定义新的网络对象

在此步骤中，您将为每条 VPN 隧道创建一个网络对象，并指定虚拟专用网关的公有 (外部) IP 地址。您稍后将这些网络对象作为 VPN 社区的卫星网关进行添加。您还需要创建一个空组以用作 VPN 域的占位符。

1. 打开检查点 SmartDashboard。
2. 对于 Groups，打开上下文菜单并选择 Groups、Simple Group。您可以对每个网络对象使用相同的组。
3. 对于 Network Objects，打开上下文 (右键单击) 菜单并选择 New、Interoperable Device。
4. 对于 Name (名称)，输入您为隧道提供的名称，例如，`AWS_VPC_Tunnel_1` 或 `AWS_VPC_Tunnel_2`。
5. 对于IPv4 地址，请输入配置文件中提供的虚拟专用网关的外部 IP 地址，例如`54.84.169.196`。保存您的设置并关闭对话框。



6. 在中 SmartDashboard，打开您的网关属性，然后在类别窗格中，选择拓扑。
7. 要检索接口配置，请选择 Get Topology。
8. 在 VPN Domain (VPN 域) 部分中，选择 Manually defined (手动定义)，然后浏览找到并选择您在步骤 2 中创建的空组。选择确定。

> **Note**
>
> 您可以保留已配置的任何现有 VPN 域。但是，请确保新的 VPN 连接使用或提供的主机和网络未在该 VPN 域中声明，尤其是在 VPN 域自动派生的情况下。

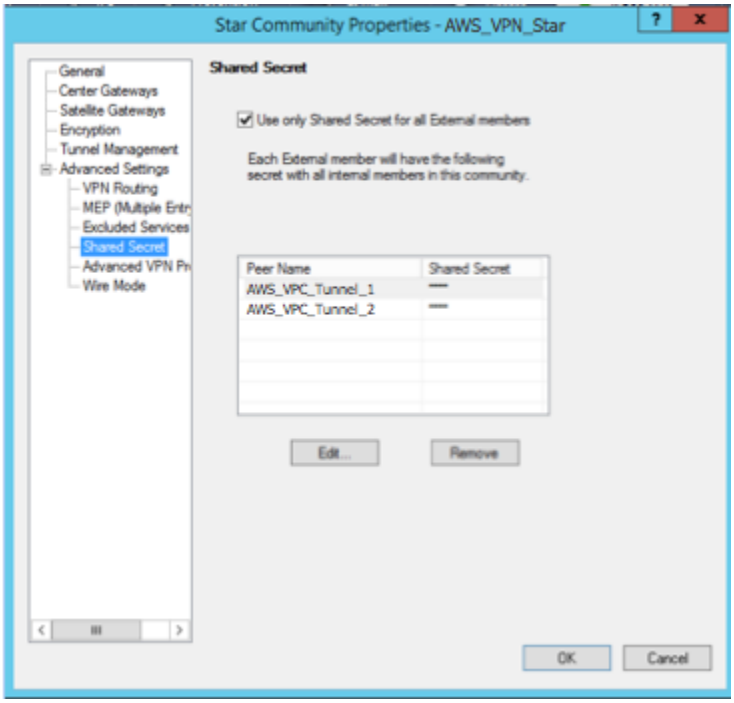
9. 重复这些步骤以使用配置文件的 `IPSec Tunnel #2` 部分下的信息创建另一个网络对象。

> **Note**
>
> 如果您使用的是集群，请编辑拓扑并将接口定义为集群接口。使用配置文件中指定的 IP 地址。

创建和配置 VPN 社区、IKE 和 IPsec设置

在此步骤中，您将在检查点网关上创建一个 VPN 社区 (为每条隧道将网络对象 (可互操作设备) 添加到该社区)。您还可以配置互联网密钥交换 (IKE) 和 IPsec设置。

1. 在网关属性中，在类别窗格中选择 IPSecVPN。
2. 选择 Communities、New、Star Community。
3. 为您的社区提供名称 (例如，`AWS_VPN_Star`)，然后选择类别窗格中的 Center Gateways。
4. 选择 Add，并将您的网关或集群添加到参与者网关列表。
5. 在类别窗格中，依次选择 Satellite Gateways (卫星网关) 和 Add (添加)，然后将您之前创建的可互操作设备（`AWS_VPC_Tunnel_1` 和 `AWS_VPC_Tunnel_2`）添加到参与者网关列表。
6. 在类别窗格中，选择 Encryption。在 “加密方法” 部分中，IKEv1 仅选择。在 Encryption Suite 部分中，选择 Custom、Custom Encryption。
7. 在对话框中，配置如下加密属性，并在完成后选择 OK：
   - IKE 安全关联 (第 1 阶段) 属性：
     - Perform key exchange encryption with：AES-128
     - Perform data integrity with：SHA-1
   - IPsec 安全关联（第 2 阶段）属性：
     - 使用以下 IPsec 命令执行数据加密：AES-128
     - Perform data integrity with：SHA-1
8. 在类别窗格中，选择 Tunnel Management。选择 Set Permanent Tunnels、On all tunnels in the community。在 VPN Tunnel Sharing 部分中，选择 One VPN tunnel per Gateway pair。
9. 在类别窗格中，展开 Advanced Settings，然后选择 Shared Secret。
10. 选择第一条隧道的对等名称，再选择 Edit (编辑)，然后输入配置文件的 `IPSec Tunnel #1` 部分中指定的预共享密钥。
11. 选择第二条隧道的对等名称，再选择 Edit (编辑)，然后输入配置文件的 `IPSec Tunnel #2` 部分中指定的预共享密钥。



12. 仍然在 Advanced Settings (高级设置) 类别中，选择 Advanced VPN Properties (高级 VPN 属性)，配置如下属性，然后在完成后选择 OK (确定)：

    - IKE (第 1 阶段)：
      - Use Diffie-Hellman group (使用 Diffie-Hellman 组)：`Group 2`
      - Renegotiate IKE security associations every `480` minutes
    - IPsec （第 2 阶段）：
      - 选择 Use Perfect Forward Secrecy
      - Use Diffie-Hellman group (使用 Diffie-Hellman 组)：`Group 2`
      - 每**`3600`**秒钟重新协商一次 IPsec 安全关联

创建防火墙规则

在此步骤中，您将配置一个具有防火墙规则和定向匹配规则的策略，这些规则允许 VPC 和本地网络之间的通信。然后在网关上安装该策略。

1. 在中 SmartDashboard，为您的网关选择全局属性。在类别窗格中，展开 VPN，然后选择 Advanced。
2. 选择 Enable VPN Directional Match in VPN Column，并保存您的更改。
3. 在中 SmartDashboard，选择防火墙，然后使用以下规则创建策略：

- 允许 VPC 子网通过所需协议与本地网络进行通信。
- 允许本地网络通过所需协议与 VPC 子网进行通信。

4. 打开 VPN 列中的单元格的上下文菜单，并选择 Edit Cell。
5. 在 VPN Match Conditions 对话框中，选择 Match traffic in this direction only。通过为以下每个定向匹配规则选择 Add 来创建该规则，并在完成后选择 OK：
   - `internal_clear` > VPN 社区（您先前创建的 VPN 星级社区，例如，`AWS_VPN_Star`）
   - VPN 社区 > VPN 社区
   - VPN 社区 > `internal_clear`
6. 在中 SmartDashboard，选择策略，安装。
7. 在对话框中，选择您的网关并选择 OK 以安装策略。

修改 tunnel_keepalive_method 属性

您的检查点网关可使用失效对端检测 (DPD) 来标识 IKE 关联中断的时间。要为永久隧道配置 DPD，必须在 AWS VPN 社区中配置永久隧道（请参阅步骤 8）。

默认情况下，VPN 网关的 `tunnel_keepalive_method` 属性设置为 `tunnel_test`。您必须将该值更改为 dpd。VPN 社区中每个需要 DPD 监控的 VPN 网关都必须使用 `tunnel_keepalive_method` 属性进行配置，包括任何第三方 VPN 网关。您不能为同一网关配置不同的监控机制。

您可以使用 Gui DBedit 工具更新该`tunnel_keepalive_method`属性。

1. 打开检查点 SmartDashboard，然后选择安全管理服务器、域管理服务器。
2. 选择 File 和 Database Revision Control...，然后创建修订快照。
3. 关闭所有 SmartConsole 窗口，例如、“ SmartDashboard SmartView 跟踪器” 和 “ SmartView 监视器”。
4. 启动 Gui BDedit 工具。有关更多信息，请参阅检查点支持中心上的文章检查点数据库工具。
5. 依次选择 Security Management Server 和 Domain Management Server。
6. 在左上窗格中，依次选择 Table、Network Objects 和 network_objects。
7. 在右上窗格中，依次选择相关的 Security Gateway 和 Cluster 对象。
8. 按 Ctrl+F，或者使用 Search 菜单搜索以下内容：`tunnel_keepalive_method`。

9. 在下方窗格中，打开 tunnel_keepalive_method 的上下文菜单，并选择 Edit... (编辑...)。选择 dpd，然后选择 OK (确定)。
10. 对属于 AWS VPN 社群的每个网关重复步骤 7 到步骤 9。
11. 依次选择 File 和 Save All。
12. 关闭 Gui DBedit 工具。
13. 打开检查点 SmartDashboard，然后选择安全管理服务器、域管理服务器。
14. 在相关的 Security Gateway 和 Cluster 对象上安装策略。

有关更多信息，请参阅检查点支持中心上的文章 R77.10 中的新增 VPN 特征。

启用 TCP MSS 固定

TCP MSS 固定减小了 TCP 数据包的最大段大小以防止数据包分段。

1. 导航到以下目录：C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\。
2. 通过运行 GuiDBEdit.exe 文件打开检查点数据库工具。
3. 选择 Table、Global Properties、properties。
4. 对于 fw_clamp_tcp_mss，选择 Edit。将值更改为 true 并选择 OK。

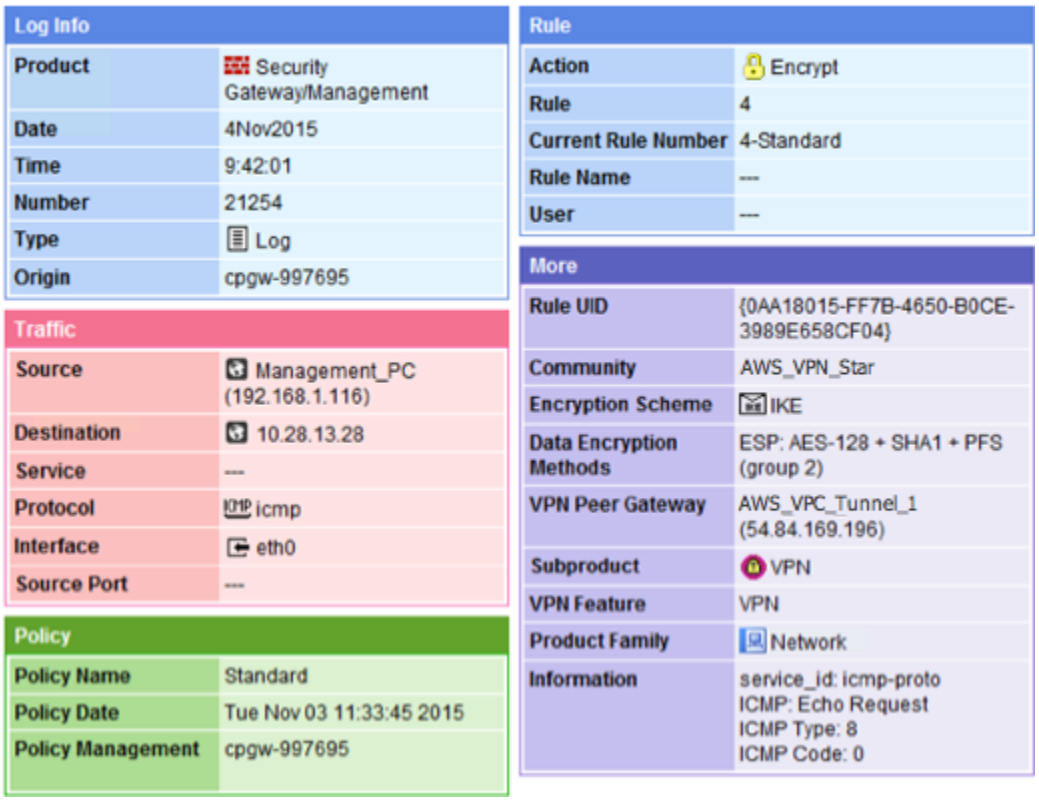
验证隧道状态

您可以通过在专家模式下从命令行工具运行以下命令来验证隧道状态。

```
vpn tunnelutil
```

在显示的选项中，选择 1 以验证 IKE 关联，选择 2 以验证 IPsec关联。

您也可以使用检查点智能跟踪器日志来验证通过连接传输的数据包是否已加密。例如，以下日志指示数据包通过隧道 1 发送到 VPC 并且已加密。



SonicWALL

以下过程演示如何使用 SonicOS 管理界面在 SonicWALL 设备上配置 VPN 隧道。

配置隧道

1. 打开 SonicWALL SonicOS 管理界面。
2. 在左窗格中，依次选择 VPN、Settings。在 VPN Policies 下方，选择 Add...。
3. 在 General 选项卡上的 VPN 策略窗口中，填写以下信息：
   - 策略类型：选择隧道接口。
   - Authentication Method：选择 IKE using Preshared Secret。
   - Name：输入 VPN 策略的名称。建议使用配置文件中提供的 VPN ID 名称。
   - IPsec 主网关名称或地址：输入配置文件中提供的虚拟专用网关的 IP 地址（例如`72.21.209.193`）。
   - IPsec 辅助网关名称或地址：保留默认值。
   - Shared Secret：输入配置文件中提供的预共享密钥，然后在 Confirm Shared Secret 中再次输入。
   - 本地 IKE ID：输入客户网关（SonicWall 设备）IPv4 的地址。

- 对等 IKE ID：输入虚拟专用网关 IPv4 的地址。

4. 在 Network 选项卡上，填写以下信息：

   - 在 Local Networks 下方，选择 Any address。建议使用此选项防止本地网络出现连接问题。
   - 在 Remote Networks 下方，选择 Choose a destination network from list。在 AWS中使用您的 VPC 的 CIDR 创建一个地址对象。

5. 在 Proposals (提案) 选项卡上，填写以下信息：

   - 在 IKE (Phase 1) Proposal 下方，执行以下操作：
     - Exchange：选择 Main Mode。
     - DH Group (DH 组)：输入 Diffie-Hellman 组的值（例如 2）。
     - Encryption：选择 AES-128 或 AES-256。
     - 身份验证：选择SHA1或SHA256。
     - Life Time：输入 28800。
   - 在 IKE (Phase 2) Proposal 下方，执行以下操作：
     - Protocol：选择 ESP。
     - Encryption：选择 AES-128 或 AES-256。
     - 身份验证：选择SHA1或SHA256。
     - 选中 Enable Perfect Forward Secrecy 复选框，然后选择 Diffie-Hellman 组。
     - Life Time：输入 3600。

   > **Important**
   >
   > 如果您在 2015 年 10 月之前创建了虚拟专用网关，则必须为两个阶段指定 Diffie-Hellman 组 2、AES-128 和两个阶段。 SHA1

6. 在 Advanced 选项卡上，填写以下信息：

   - 选择 Enable Keep Alive。
   - 选择 Enable Phase2 Dead Peer Detection 并输入以下内容：
     - 对于 Dead Peer Detection Interval，输入 60 (这是 SonicWALL 设备接受的最小值)。
     - 对于 Failure Trigger Level，输入 3。
   - 对于 VPN Policy bound to，选择 Interface X1。这是通常为公有 IP 地址指定的接口。

7. 选择确定。在 Settings 页面上，隧道的 Enable 复选框默认应处于选中状态。绿点表示隧道已启动。

Cisco 设备：其他信息

某些 Cisco ASAs 仅支持活动/待机模式。使用这些 Cisco 时 ASAs，一次只能有一个活动隧道。仅在第一个隧道不可用的情况下，备用隧道才可用。借助该冗余度，您应该始终可以通过其中一个隧道连接到您的 VPC。

Cis ASAs co 9.7.1 及更高版本支持主动/主动模式。使用这些 Cisco 时 ASAs，可以同时激活两条隧道。借助该冗余度，您应该始终可以通过其中一个隧道连接到您的 VPC。

对于 Cisco 设备，您必须执行以下操作：

- 配置外部接口。
- 确保 Crypto ISAKMP 策略序列号具有唯一性。
- 确保 Crypto 列表策略序列号具有唯一性。
- 确保加密 IPsec 转换集和加密 ISAKMP 策略序列与设备上配置的任何其他 IPsec 隧道保持一致。
- 确保 SLA 监控号具有唯一性。
- 对在客户网关设备和您的本地网络之间传输流量的所有路由选择进行配置。

AWS Site-to-Site VPN 客户网关设备的可下载动态路由配置文件

要下载包含特定于您的 Site-to-Site VPN 连接配置值的示例配置文件，请使用 Amazon VPC 控制台、AWS 命令行或 Amazon EC2 API。有关更多信息，请参阅 步骤 6：下载配置文件。

您也可以下载不包含特定于您的 Site-to-Site VPN 连接配置值的动态路由的通用示例配置文件：dynamic-routing-examples. zip

这些文件对某些组件使用占位符值。例如，它们使用：

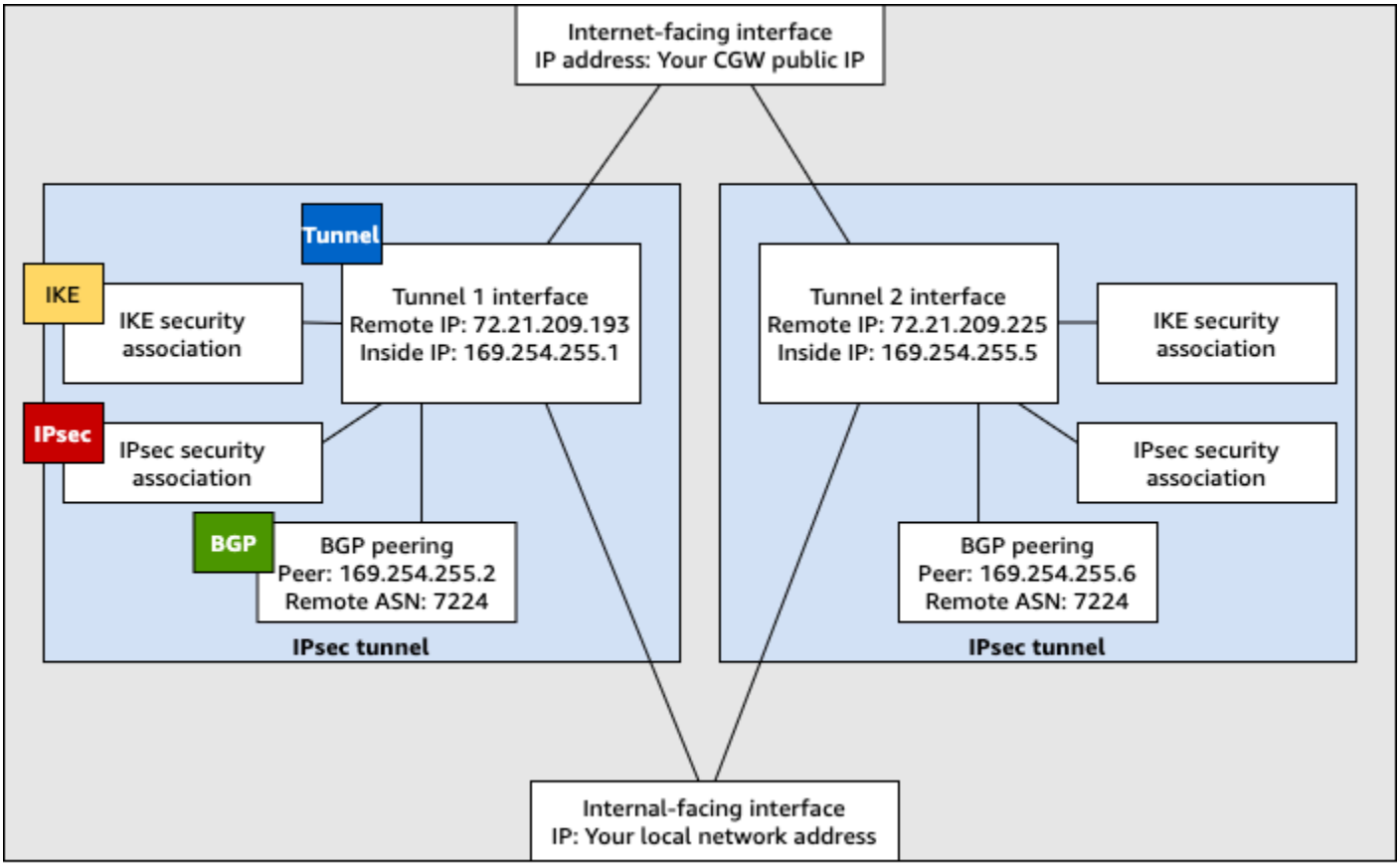
- VPN 连接 ID、客户网关 ID 和虚拟私有网关 ID 的示例值
- 远程（外部）IP 地址 AWS 端点的占位符（*AWS_ENDPOINT_1*和*AWS_ENDPOINT_2*）
- 客户网关设备上可路由互联网的外部接口 IP 地址的占位符 () *your-cgw-ip-address*
- 预共享密钥值的占位符 () pre-shared-key
- IP 地址内的隧道的示例值。

- MTU 设置的示例值。

> **Note**
>
> 示例配置文件中提供的 MTU 设置仅供示例之用。有关根据自己的情况设置最佳 MTU 值的信息，请参阅AWS Site-to-Site VPN 客户网关设备的最佳实践。

除了提供占位符值外，这些文件还指定了大多数地区的、和 Diffie-Hellman 组 2 的 Site-to-Site VPN 连接的最低要求，以及 AWS 区域中的 AES128 SHA1 AES128 SHA2、和 Diffie-Hellman 组 14 的最低要求。 AWS GovCloud它们还指定用于身份验证的预共享密钥。您必须修改示例配置文件以利用其他安全算法、Diffie-Hellman 组、私有证书和流量。 IPv6

下图概述了在客户网关设备上配置的各种组件。它包括隧道接口 IP 地址的示例值。



Customer gateway device

为 AWS Virtual Private Network 客户网关设备配置动态路由

以下是使用客户网关设备的用户界面（如果可用）配置该设备的一些示例过程。

Check Point

以下是使用 Gaia 门户网站和 Check Point 配置运行 R77.10 或更高版本的 Check Point Security Gateway 设备的步骤。 SmartDashboard您也可以参考检查点支持中心的 Amazon Web Services VPN BGP 一文。

配置隧道接口

第一步是创建 VPN 隧道并为每条隧道提供客户网关和虚拟专用网关的私有（内部）IP 地址。要创建第一条隧道，请使用配置文件的 IPSec Tunnel #1 部分下提供的信息。要创建第二条隧道，请使用配置文件的 IPSec Tunnel #2 部分中提供的值。

1. 通过 SSH 连接到您的安全网关。如果您使用的是非默认 Shell，请通过运行以下命令来更改为 clish：clish
2. 通过运行以下命令来设置客户网关 ASN（在中创建客户网关时提供的 ASN AWS）。

```
set as 65000
```

3. 使用配置文件的 IPSec Tunnel #1 部分下提供的信息，为第一条隧道创建隧道接口。为您的隧道提供唯一名称，例如 AWS_VPC_Tunnel_1。

```
add vpn tunnel 1 type numbered local 169.254.44.234 remote 169.254.44.233
 peer AWS_VPC_Tunnel_1
set interface vpnt1 state on
set interface vpnt1 mtu 1436
```

4. 重复这些命令以使用配置文件的 IPSec Tunnel #2 部分下提供的信息创建第二条隧道。为您的隧道提供唯一名称，例如 AWS_VPC_Tunnel_2。

```
add vpn tunnel 1 type numbered local 169.254.44.38 remote 169.254.44.37
 peer AWS_VPC_Tunnel_2
set interface vpnt2 state on
set interface vpnt2 mtu 1436
```

5. 设置虚拟私有网关 ASN。

```
set bgp external remote-as 7224 on
```

6. 使用配置文件的 IPSec Tunnel #1 部分中提供的信息为第一条隧道配置 BGP。

```
set bgp external remote-as 7224 peer 169.254.44.233 on
```

```
set bgp external remote-as 7224 peer 169.254.44.233 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.233 keepalive 10
```

7. 使用配置文件的 IPSec Tunnel #2 部分中提供的信息为第二条隧道配置 BGP。

```
set bgp external remote-as 7224 peer 169.254.44.37 on
set bgp external remote-as 7224 peer 169.254.44.37 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.37 keepalive 10
```

8. 保存配置。

```
save config
```

创建 BGP 策略

接下来，创建一个 BGP 策略，该策略允许导入 AWS公布的路由。然后，将您的客户网关配置为将其本地路由公布到 AWS。

1. 在 Gaia WebUI 中，选择 Advanced Routing、Inbound Route Filters。选择 Add，然后选择 Add BGP Policy (Based on AS)。
2. 对于 Add BGP Policy (添加 BGP 策略)，在第一个字段中选择一个介于 512 和 1024 之间的值，然后在第二个字段中输入虚拟私有网关 ASN（例如，7224）。
3. 选择保存。

传播本地路由

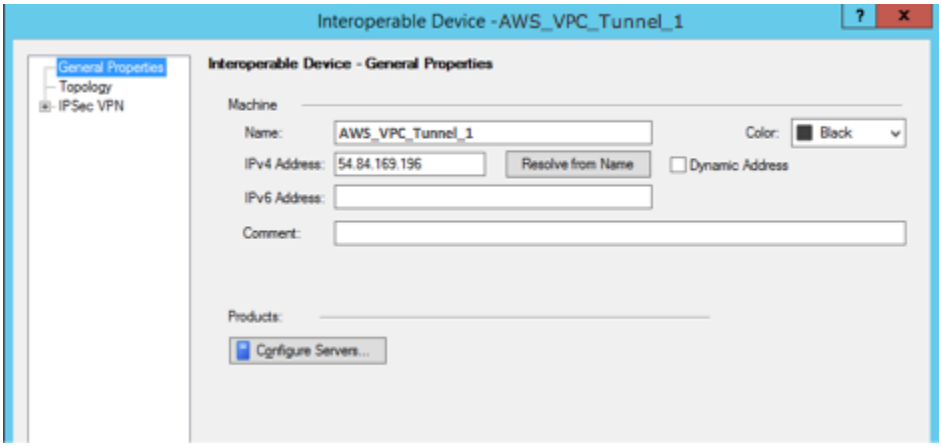
以下步骤适用于分配本地接口路由。您也可以从不同的源重新分配路由（例如，静态路由或通过动态路由协议获取的路由）。有关更多信息，请参阅 Gaia 高级路由 R77 版本管理指南。

1. 在 Gaia WebUI 中，选择 Advanced Routing、Routing Redistribution。选择 Add Redistribution From (添加重新分配源)，然后选择 Interface (接口)。
2. 对于 To Protocol (目标协议)，选择虚拟私有网关 ASN（例如，7224）。
3. 对于 Interface，选择一个内部接口。选择保存。

定义新的网络对象

接下来，为每条 VPN 隧道创建一个网络对象，并指定虚拟私有网关的公有（外部）IP 地址。您稍后将这些网络对象作为 VPN 社区的卫星网关进行添加。您还需要创建一个空组以用作 VPN 域的占位符。

1. 打开检查点 SmartDashboard。
2. 对于 Groups，打开上下文菜单并选择 Groups、Simple Group。您可以对每个网络对象使用相同的组。
3. 对于 Network Objects，打开上下文 (右键单击) 菜单并选择 New、Interoperable Device。
4. 对于 Name (名称)，输入您在步骤 1 中为隧道提供的名称，例如，`AWS_VPC_Tunnel_1` 或 `AWS_VPC_Tunnel_2`。
5. 对于IPv4 地址，请输入配置文件中提供的虚拟专用网关的外部 IP 地址，例如`54.84.169.196`。保存您的设置并关闭对话框。



6. 在左侧类别窗格中，选择 Topology。
7. 在 VPN Domain (VPN 域) 部分中，选择 Manually defined (手动定义)，然后浏览找到并选择您在步骤 2 中创建的空组。选择确定。
8. 重复这些步骤以使用配置文件的 `IPSec Tunnel #2` 部分下的信息创建另一个网络对象。
9. 转到您的网关网络对象，打开您的网关或集群对象，然后选择 Topology。
10. 在 VPN Domain (VPN 域) 部分中，选择 Manually defined (手动定义)，然后浏览找到并选择您在步骤 2 中创建的空组。选择确定。

> **Note**
>
> 您可以保留已配置的任何现有 VPN 域。但是，请确保新的 VPN 连接使用或提供的主机和网络未在该 VPN 域中声明，尤其是在 VPN 域自动派生的情况下。

> **Note**
>
> 如果您使用的是集群，请编辑拓扑并将接口定义为集群接口。使用配置文件中指定的 IP 地址。

创建和配置 VPN 社区、IKE 和 IPsec设置

接下来，在检查点网关上创建一个 VPN 社区（为每条隧道将网络对象（可互操作设备）添加到该社区）。您还可以配置互联网密钥交换 (IKE) 和 IPsec设置。

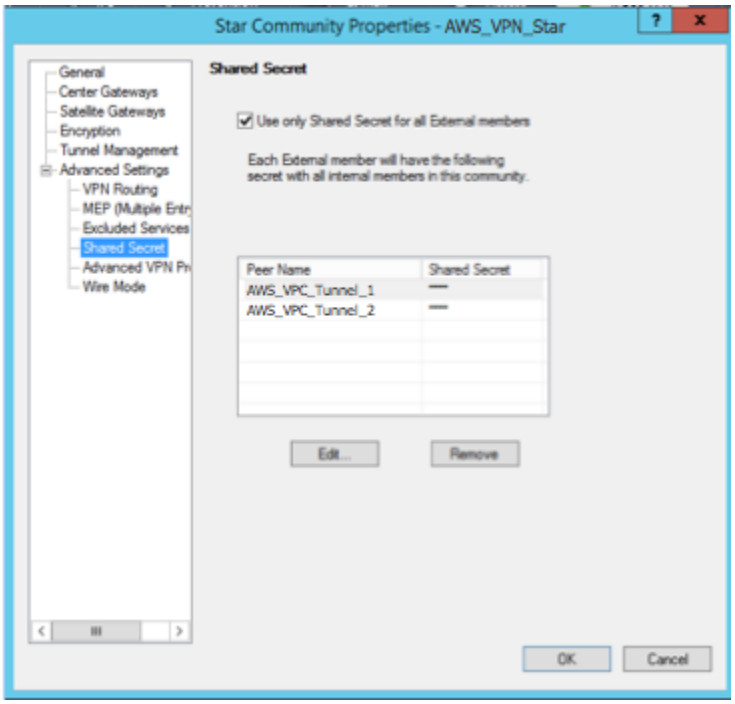
1. 在网关属性中，在类别窗格中选择 IPSecVPN。
2. 选择 Communities、New、Star Community。
3. 为您的社区提供名称 (例如，`AWS_VPN_Star`)，然后选择类别窗格中的 Center Gateways。
4. 选择 Add，并将您的网关或集群添加到参与者网关列表。
5. 在类别窗格中，选择 Satellite Gateways (卫星网关)、Add (添加)，然后将您之前创建的可互操作设备（`AWS_VPC_Tunnel_1` 和 `AWS_VPC_Tunnel_2`）添加到参与者网关列表。
6. 在类别窗格中，选择 Encryption。在 “加密方法” 部分，选择 “IKEv1 IPv4 和 IKEv2 ” IPv6。在 Encryption Suite 部分中，选择 Custom、Custom Encryption。

   > **Note**
   >
   > 必须选择 for IPv4 和 IKEv1 f IKEv2 or IPv6 选项才能 IKEv1 使用功能。

7. 在对话框中，配置如下加密属性，然后在完成后选择 OK (确定)：
   - IKE 安全关联 (第 1 阶段) 属性：
     - Perform key exchange encryption with：AES-128
     - Perform data integrity with：SHA-1
   - IPsec 安全关联（第 2 阶段）属性：

- 使用以下 IPsec 命令执行数据加密：AES-128
- Perform data integrity with：SHA-1

8. 在类别窗格中，选择 Tunnel Management。选择 Set Permanent Tunnels、On all tunnels in the community。在 VPN Tunnel Sharing 部分中，选择 One VPN tunnel per Gateway pair。
9. 在类别窗格中，展开 Advanced Settings，然后选择 Shared Secret。
10. 选择第一条隧道的对等名称，再选择 Edit (编辑)，然后输入配置文件的 `IPSec Tunnel #1` 部分中指定的预共享密钥。
11. 选择第二条隧道的对等名称，再选择 Edit (编辑)，然后输入配置文件的 `IPSec Tunnel #2` 部分中指定的预共享密钥。



12. 仍然在 Advanced Settings (高级设置) 类别中，选择 Advanced VPN Properties (高级 VPN 属性)，配置如下属性，然后在完成后选择 OK (确定)：

- IKE (第 1 阶段)：
  - Use Diffie-Hellman group (使用 Diffie-Hellman 组)：`Group 2 (1024 bit)`
  - Renegotiate IKE security associations every `480` minutes
- IPsec （第 2 阶段）：
  - 选择 Use Perfect Forward Secrecy
  - Use Diffie-Hellman group (使用 Diffie-Hellman 组)：`Group 2 (1024 bit)`
  - 每**3600**秒钟重新协商一次 IPsec 安全关联

创建防火墙规则

接下来，配置一个具有防火墙规则和定向匹配规则的策略，这些规则允许 VPC 和本地网络之间的通信。然后在网关上安装该策略。

1. 在中 SmartDashboard，为您的网关选择全局属性。在类别窗格中，展开 VPN，然后选择 Advanced。
2. 选择 Enable VPN Directional Match in VPN Column，然后选择 OK。
3. 在中 SmartDashboard，选择防火墙，然后使用以下规则创建策略：
   - 允许 VPC 子网通过所需协议与本地网络进行通信。
   - 允许本地网络通过所需协议与 VPC 子网进行通信。
4. 打开 VPN 列中的单元格的上下文菜单，并选择 Edit Cell。
5. 在 VPN Match Conditions 对话框中，选择 Match traffic in this direction only。通过为以下每个定向匹配规则选择 Add (添加) 来创建该规则，然后在完成后选择 OK (确定)：
   - `internal_clear` > VPN 社区（您先前创建的 VPN 星级社区，例如，`AWS_VPN_Star`）
   - VPN 社区 > VPN 社区
   - VPN 社区 > `internal_clear`
6. 在中 SmartDashboard，选择策略，安装。
7. 在对话框中，选择您的网关并选择 OK 以安装策略。

修改 tunnel_keepalive_method 属性

您的检查点网关可使用失效对端检测 (DPD) 来标识 IKE 关联中断的时间。要为永久隧道配置 DPD，必须在 AWS VPN 社区中配置永久隧道。

默认情况下，VPN 网关的 `tunnel_keepalive_method` 属性设置为 `tunnel_test`。您必须将该值更改为 dpd。VPN 社区中每个需要 DPD 监控的 VPN 网关都必须使用 `tunnel_keepalive_method` 属性进行配置，包括任何第三方 VPN 网关。您不能为同一网关配置不同的监控机制。

您可以使用 Gui DBedit 工具更新该`tunnel_keepalive_method`属性。

1. 打开检查点 SmartDashboard，然后选择安全管理服务器、域管理服务器。
2. 选择 File 和 Database Revision Control...，然后创建修订快照。

3. 关闭所有 SmartConsole 窗口，例如、“ SmartDashboard SmartView 跟踪器” 和 “ SmartView 监视器”。
4. 启动 Gui BDedit 工具。有关更多信息，请参阅检查点支持中心上的文章检查点数据库工具。
5. 依次选择 Security Management Server 和 Domain Management Server。
6. 在左上窗格中，依次选择 Table、Network Objects 和 network_objects。
7. 在右上窗格中，依次选择相关的 Security Gateway 和 Cluster 对象。
8. 按 Ctrl+F，或者使用 Search 菜单搜索以下内容：`tunnel_keepalive_method`。
9. 在下方窗格中，打开 `tunnel_keepalive_method` 的上下文菜单，并选择 Edit...。依次选择 dpd 和 OK (确定)。
10. 对属于 AWS VPN 社群的每个网关重复步骤 7 到步骤 9。
11. 依次选择 File 和 Save All。
12. 关闭 Gui DBedit 工具。
13. 打开检查点 SmartDashboard，然后选择安全管理服务器、域管理服务器。
14. 在相关的 Security Gateway 和 Cluster 对象上安装策略。

有关更多信息，请参阅检查点支持中心上的文章 R77.10 中的新增 VPN 特征。

启用 TCP MSS 固定

TCP MSS 固定减小了 TCP 数据包的最大段大小以防止数据包分段。

1. 导航到以下目录：`C:\Program Files (x86)\CheckPoint\SmartConsole \R77.10\PROGRAM\`。
2. 通过运行 `GuiDBEdit.exe` 文件打开检查点数据库工具。
3. 选择 Table、Global Properties、properties。
4. 对于 `fw_clamp_tcp_mss`，选择 Edit。将值更改为 `true`，然后选择 OK (确定)。

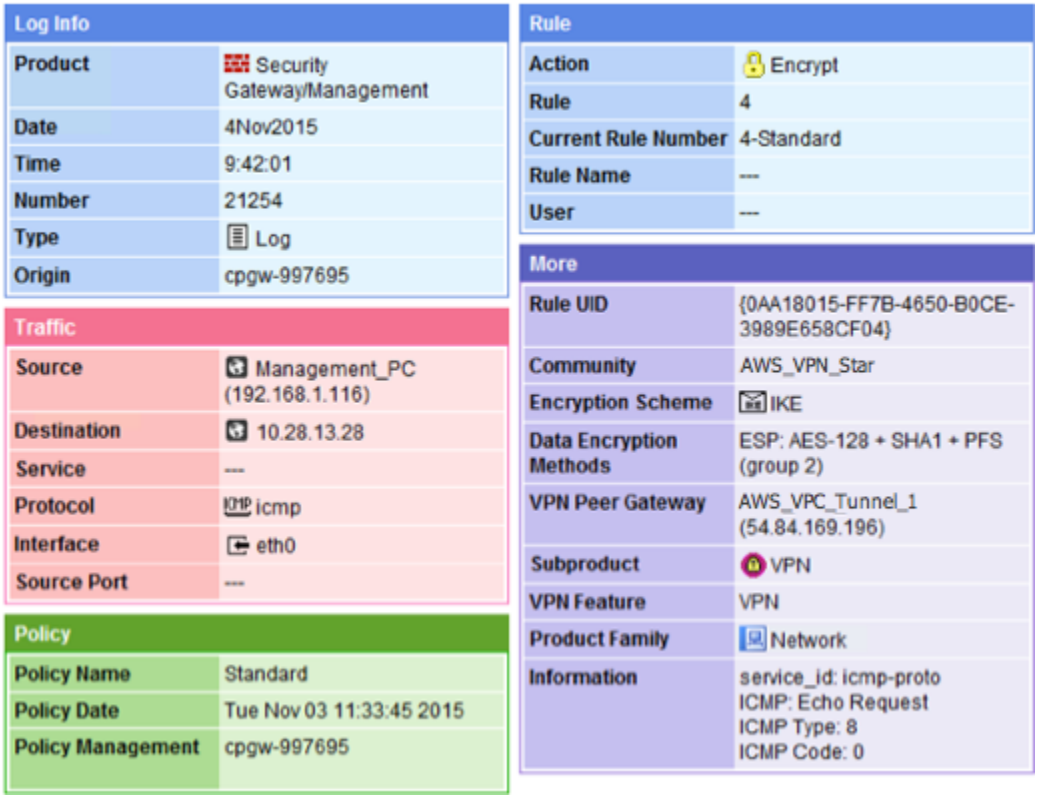
验证隧道状态

您可以通过在专家模式下从命令行工具运行以下命令来验证隧道状态。

```
vpn tunnelutil
```

在显示的选项中，选择 1 以验证 IKE 关联，选择 2 以验证 IPsec关联。

您也可以使用检查点智能跟踪器日志来验证通过连接传输的数据包是否已加密。例如，以下日志指示数据包通过隧道 1 发送到 VPC 并且已加密。



SonicWALL

您可以使用 SonicOS 管理界面配置 SonicWALL 设备。有关配置隧道的更多信息，请参阅为 AWS Site-to-Site VPN 客户网关设备配置静态路由。

您无法使用管理接口配置此设备的 BGP。请改用示例配置文件中名为 BGP 的部分中提供的命令行指令进行配置。

Cisco 设备：其他信息

某些 Cisco ASAs 仅支持活动/待机模式。使用这些 Cisco 时 ASAs，一次只能有一个活动隧道。仅在第一个隧道不可用的情况下，备用隧道才可用。借助该冗余度，您应该始终可以通过其中一个隧道连接到您的 VPC。

Cis ASAs co 9.7.1 及更高版本支持主动/主动模式。使用这些 Cisco 时 ASAs，可以同时激活两条隧道。借助该冗余度，您应该始终可以通过其中一个隧道连接到您的 VPC。

对于 Cisco 设备，您必须执行以下操作：

- 配置外部接口。
- 确保 Crypto ISAKMP 策略序列号具有唯一性。
- 确保 Crypto 列表策略序列号具有唯一性。
- 确保加密 IPsec 转换集和加密 ISAKMP 策略序列与设备上配置的任何其他 IPsec 隧道保持一致。
- 确保 SLA 监控号具有唯一性。
- 对在客户网关设备和您的本地网络之间传输流量的所有路由选择进行配置。

Juniper 设备：其他信息

以下信息适用于 Juniper J 系列 和 SRX 客户网关设备的示例配置文件。

- 外部接口被称为*ge-0/0/0.0*。
- 隧道接口 IDs 称为*st0.1*和*st0.2*。
- 确保您识别上行链路接口的安全区（配置信息使用默认的“untrust”区）。
- 确保您识别内部接口的安全区（配置信息使用默认的“trust”区）。

将 Windows 服务器配置为 AWS Site-to-Site VPN 客户网关设备

您可以将一台运行 Windows Server 的服务器配置为 VPC 的客户网关设备。无论你是在 VPC 中的 EC2 实例上运行 Windows Server，还是在自己的服务器上运行 Windows Server，都要使用以下流程。以下过程适用于 Windows Server 2012 R2 及更高版本。

内容

配置您的 Windows 实例

如果您要在从 Windows AMI 启动的 EC2 实例上配置 Windows 服务器，请执行以下操作：

- 禁用实例的源/目标检查：
  1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
  2. 选择您的 Windows 实例，然后依次选择 Actions（操作）、Networking（网络）、Change source/destination check（更改源/目标检查）。选择 Stop（停止），然后选择 Save（保存）。
- 更新适配器设置，以便您可以路由来自其他实例的流量：
  1. 连接到您的 Windows 实例。有关更多信息，请参阅连接到您的 Windows 实例。
  2. 打开控制面板，启动设备管理器。
  3. 展开网络适配器节点。
  4. 选择网络适配器（根据实例类型，可能是 Amazon Elastic Network Adapter 或 Intel 82599 虚拟功能），然后选择 Action（操作）、Properties（属性）。
  5. 在 “高级” 选项卡上，禁用 “IPv4校验和卸载”、“TCP 校验和卸载” (IPv4) 和 “UDP 校验和卸载 (IPv4)” 属性，然后选择 “确定”。
- 向您的账户分配弹性 IP 地址并将该地址与实例关联。有关更多信息，请参阅 Amazon EC2 用户指南中的弹性 IP 地址。记下这个地址——创建客户网关时需要这个地址。
- 确保实例的安全组规则允许出站 IPsec 流量。默认情况下，安全组允许所有出站流量。但是，如果安全组的出站规则已从其原始状态进行了修改，则必须为 IPsec 流量创建以下出站自定义协议规则：IP 协议 50、IP 协议 51 和 UDP 500。

记下您的 Windows 实例所在网络的 CIDR 范围，例如，`172.31.0.0/16`。

步骤 1：创建 VPN 连接并配置您的 VPC

要从您的 VPC 创建 VPN 连接，请执行以下操作：

1. 创建虚拟私有网关并将其连接到您的 VPC。有关更多信息，请参阅 创建虚拟专用网关。
2. 创建 VPN 连接和新的客户网关。对于客户网关，请指定 Windows Server 的公有 IP 地址。对于 VPN 连接，请选择静态路由，然后输入 Windows Server 所在网络的 CIDR 范围，例如 `172.31.0.0/16`。有关更多信息，请参阅 步骤 5：创建 VPN 连接。

创建 VPN 连接后，请将 VPC 配置为启用通过 VPN 连接进行通信。

配置您的 VPC

- 在 VPC 中创建私有子网（如果您还没有），以启动要与 Windows Server 通信的实例。有关更多信息，请参阅在 VPC 中创建子网。

> **Note**
>
> 私有子网是不路由到 Internet 网关的子网。下一个项目中描述了此子网的路由。

- 更新您的 VPN 连接的路由表：
  - 向私有子网的路由表添加路由，以虚拟私有网关作为目标，以 Windows Server 的网络（CIDR 范围）作为目的地。有关更多信息，请参阅《Amazon VPC 用户指南》中的从路由表添加和删除路由。
  - 为虚拟专用网关启用路由传播。有关更多信息，请参阅（虚拟私有网关）在路由表中启用路由传播。
- 为您的实例创建安全组，以允许在 VPC 与您的网络之间进行通信：
  - 添加允许来自您的网络的入站 RDP 或 SSH 访问的规则。这样，您可以从您的网络连接到 VPC 中的实例。例如，要允许您的网络中的计算机访问您的 VPC 中的 Linux 实例，请创建一个 SSH 类型、源设置为您的网络的 CIDR 范围（如 `172.31.0.0/16`）的入站规则。有关更多信息，请参阅 Amazon VPC 用户指南中的您的 VPC 的安全组。
  - 添加允许来自您的网络的入站 ICMP 访问的规则。这样，通过从 Windows Server 对 VPC 中的实例执行 ping 操作，可以测试您的 VPN 连接。

步骤 2：下载 VPN 连接的配置文件

您可以使用 Amazon VPC 控制台为您的 VPN 连接下载 Windows Server 配置文件。

下载配置文件

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN Connections。
3. 选择您的 VPN 连接，然后选择 Download Configuration（下载配置）。
4. 选择 Microsoft 作为供应商，Windows Server 作为平台，2012 R2 作为软件。选择下载。您可以打开或保存文件。

配置文件中包含一部分与以下示例相似的信息。您会看到这些信息出现两次，每条隧道一次。

```
vgw-1a2b3c4d Tunnel1
-----------------------------------------------------------------
Local Tunnel Endpoint:       203.0.113.1
```

```
Remote Tunnel Endpoint:      203.83.222.237
Endpoint 1:                  [Your_Static_Route_IP_Prefix]
Endpoint 2:                  [Your_VPC_CIDR_Block]
Preshared key:               xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE
```

`Local Tunnel Endpoint`

在您创建 VPN 连接时，您为客户网关指定的 IP 地址。

`Remote Tunnel Endpoint`

虚拟专用网关的两个 IP 地址之一，用于终止连接 AWS 侧的 VPN 连接。

`Endpoint 1`

在您创建 VPN 连接时，您指定作为静态路由的 IP 前缀。您的网络中的这些 IP 地址被允许使用 VPN 连接访问您的 VPC。

`Endpoint 2`

连接到虚拟私有网关的 VPC 的 IP 地址范围（CIDR 块，例如 10.0.0.0/16）。

`Preshared key`

用于在`Local Tunnel Endpoint`和`Remote Tunnel Endpoint`之间建立 IPsec VPN 连接的预共享密钥。

我们建议您将两条隧道配置为 VPN 连接的一部分。在 VPN 连接的 Amazon 一端，每条隧道均连接到单独的 VPN 集线器。尽管每次只可使用一条隧道，但第二条隧道会在第一条隧道出现故障时自动建立连接。配备冗余隧道可确保在设备故障时连续可用。由于一次仅一条隧道可用，Amazon VPC 控制台指示一条隧道处于关闭状态。这是预期行为，因此无需您采取任何操作。

配置了两条隧道后，如果其中出现设备故障 AWS，您的 VPN 连接将在几分钟内自动故障转移到虚拟专用网关的第二条隧道。在您配置客户网关设备时，务必配置两条隧道。

> **Note**
>
> 不时对虚拟专用网关 AWS 执行例行维护。这项维护可能会在短时间内禁用您的 VPN 连接的两条隧道中的一条。当我们执行维护任务时，您的 VPN 连接会自动失效转移到第二条隧道。

下载的配置文件中提供了有关互联网密钥交换 (IKE) 和 IPsec 安全关联 (SA) 的其他信息。

```
MainModeSecMethods:         DHGroup2-AES128-SHA1
MainModeKeyLifetime:        480min,0sess
QuickModeSecMethods:        ESP:SHA1-AES128+60min+100000kb
QuickModePFS:               DHGroup2
```

`MainModeSecMethods`

IKE SA 的加密和身份验证算法。这些是 VPN 连接的建议设置，也是 Windows 服务器 IPsec VPN 连接的默认设置。

`MainModeKeyLifetime`

IKE SA 密钥使用期限。 这是 VPN 连接的建议设置，也是 Windows 服务器 IPsec VPN 连接的默认设置。

`QuickModeSecMethods`

IPsec SA 的加密和身份验证算法。这些是 VPN 连接的建议设置，也是 Windows 服务器 IPsec VPN 连接的默认设置。

`QuickModePFS`

我们建议您在会话中使用主密钥完全向前保密 (PFS)。IPsec

步骤 3：配置 Windows Server

在设置 VPN 隧道之前，您必须在 Windows Server 上安装并配置路由和远程访问服务。这将允许远程用户访问您的网络上的资源。

要安装路由和远程访问服务

1. 登录您的 Windows Server。
2. 转到开始菜单，然后选择服务器管理器。
3. 安装路由和远程访问服务：
   a. 从管理菜单中，选择添加角色和功能。
   b. 在开始之前页面中，确认您的服务器满足先决条件，然后选择下一步。
   c. 选择基于角色或基于功能的安装，然后选择下一步。
   d. 选择 Select a server from the server pool（从服务器池中选择一个服务器），选择 Windows Server，然后选择 Next（下一步）。

e. 在列表中选择网络策略和访问服务。在显示的对话框中选择添加功能以确认此角色所需的功能。

f. 在同一列表中，依次选择远程访问、下一步。

g. 在选择功能页面上，选择下一步。

h. 在网络策略和访问服务 页面中，选择下一步。

i. 在远程访问页面上，选择下一步。在下一页上，选择DirectAccess 和 VPN (RAS)。在显示的对话框中选择添加功能以确认此角色服务所需的功能。在同一列表中，选择路由，然后选择下一步。

j. 在 Web 服务器角色(IIS) 页面上，选择下一步。保留默认选择，然后选择下一步。

k. 选择安装。安装完成后，选择关闭。

配置和启用路由和远程访问服务器。

1. 在仪表板上，选择通知 (旗帜图标)。此时应该还有一项任务是完成部署后配置。选择打开开始向导链接。
2. 选择仅部署 VPN。
3. 在 Routing and Remote Access (路由和远程访问) 对话框中，选择服务器名称，选择 Action (操作)，然后选择 Configure and Enable Routing and Remote Access (配置并启用路由和远程访问)。
4. 在路由和远程访问服务器安装向导的第一个页面上，选择下一步。
5. 在 Configuration (配置) 页面上，选择 Custom Configuration (自定义配置)、Next (下一步)。
6. 依次选择 LAN 路由、下一步和完成。
7. 当出现路由和远程访问对话框提示时，选择启动服务。

步骤 4：设置 VPN 隧道

通过运行所下载的配置文件中的 netsh 脚本，或者使用 Windows Server 用户界面，可以配置 VPN 隧道。

> **Important**
>
> 我们建议您在会话中使用主密钥完全向前保密 (PFS)。 IPsec 如果您选择运行 netsh 脚本，它会包含一个用于启用 PFS () qmpfs=dhgroup2 的参数。您不能使用 Windows 用户界面启用 PFS，而是必须使用命令行来启用。

选项

- 选项 1：运行 netsh 脚本
- 选项 2：使用 Windows Server 用户界面

选项 1：运行 netsh 脚本

复制已下载配置文件中的 Netsh 脚本，并更换变量。以下为示例脚本。

```
netsh advfirewall consec add rule Name="vgw-1a2b3c4d Tunnel 1" ^
Enable=Yes Profile=any Type=Static Mode=Tunnel ^
LocalTunnelEndpoint=Windows_Server_Private_IP_address ^
RemoteTunnelEndpoint=203.83.222.236 Endpoint1=Your_Static_Route_IP_Prefix ^
Endpoint2=Your_VPC_CIDR_Block Protocol=Any Action=RequireInClearOut ^
Auth1=ComputerPSK Auth1PSK=xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE ^
QMSecMethods=ESP:SHA1-AES128+60min+100000kb ^
ExemptIPsecProtectedConnections=No ApplyAuthz=No QMPFS=dhgroup2
```

Name：您可以用自己选择的名称替换建议名称(vgw-1a2b3c4d Tunnel 1)。

LocalTunnelEndpoint：输入您网络上的 Windows 服务器的私有 IP 地址。

Endpoint1：Windows Server 所在网络的 CIDR 块，例如 172.31.0.0/16。用双引号 (") 将此值括起来。

Endpoint2：您的 VPC 或 VPC 中的子网的 CIDR 块，例如，10.0.0.0/16。用双引号 (") 将此值括起来。

在 Windows Server 上的命令提示行窗口中运行已更新的脚本。(^可让您剪切和粘贴命令行中的折叠文本)。要设置此 VPN 连接的第二条 VPN 隧道，请使用配置文件中的第二个 Netsh 脚本重复该过程。

完成后，请转到 配置 Windows 防火墙。

有关 netsh 参数的更多信息，请参阅 Microsoft 库中的 Netsh AdvFirewall Consec 命令。 TechNet

选项 2：使用 Windows Server 用户界面

您还可以使用 Windows Server 用户界面以设置 VPN 隧道。

> **Important**
>
> 您无法使用 Windows Server 用户界面启用主密钥完美前向保密 (PFS)。您必须如启用主密钥完全向前保密所述使用命令行启用 PFS。

任务

- 为 VPN 隧道配置安全规则
- 确认隧道配置
- 启用主密钥完全向前保密
- 配置 Windows 防火墙

为 VPN 隧道配置安全规则

在这部分中，将在 Windows Server 上配置安全规则以创建 VPN 隧道。

为 VPN 隧道配置一个安全规则

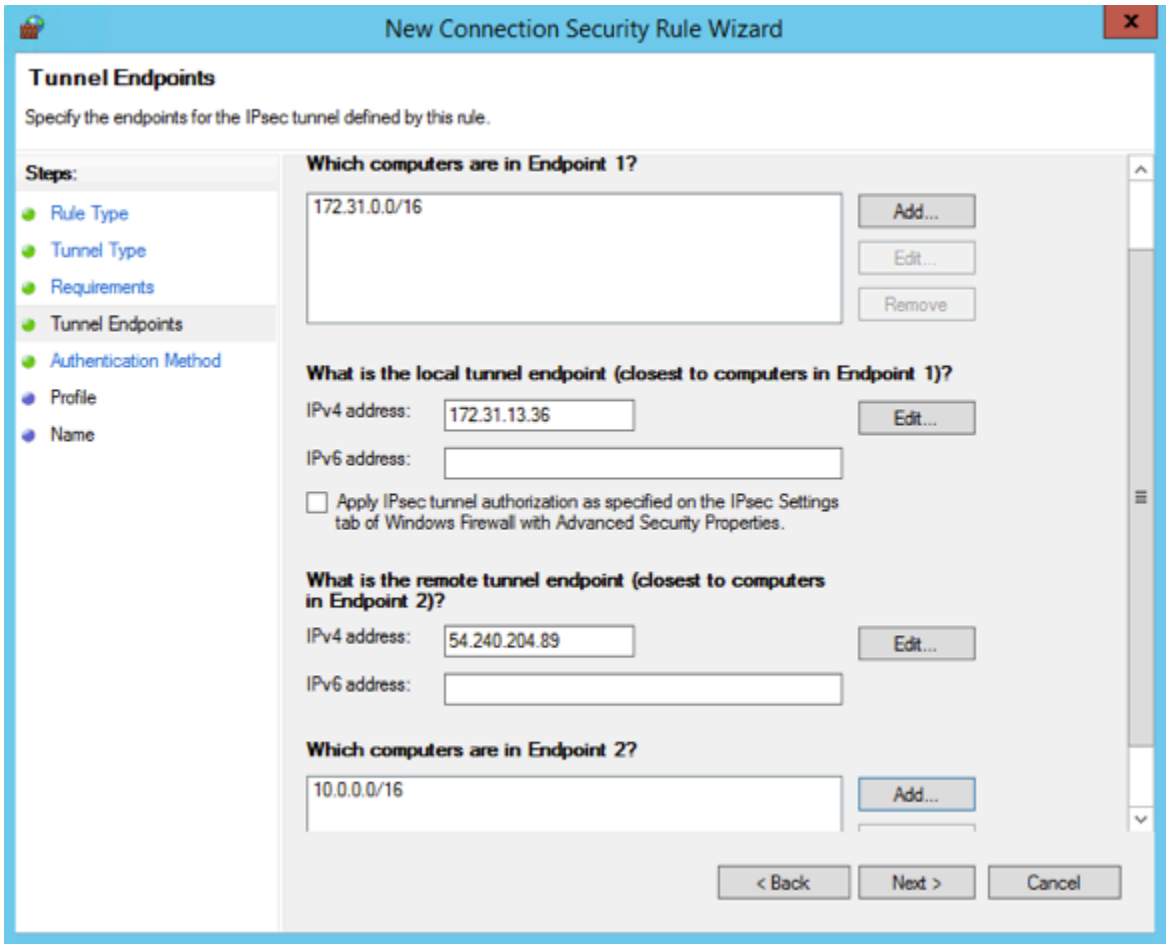
1. 打开服务器管理器，选择 Tools（工具），然后选择Windows Defender Firewall with Advanced Security（高级安全 Windows Defender 防火墙）。
2. 选择连接安全规则、操作和新建规则。
3. 在新建连接安全规则向导中的规则类型页面上，选择隧道，然后选择下一步。
4. 在 Tunnel Type (隧道类型) 页面中的 What type of tunnel would you like to create (您希望创建什么类型的隧道) 下，选择 Custom Configuration (自定义配置)。在 “是否要将 IPsec受保护的连接从该隧道中排除出来” 下，保留默认值为选中状态（否。 通过隧道发送与该连接安全规则匹配的所有网络流量），然后选择 “下一步”。
5. 在要求页面中，选择要求对入站连接进行身份验证。不要为出站连接建立隧道，然后选择下一步。
6. 在隧道端点页面上，在端点 1 中的计算机下，选择添加。输入您的网络的 CIDR 范围（在 Windows Server 客户网关设备之后，例如 `172.31.0.0/16`），然后选择 OK（确定）。该范围可以包含您的客户网关设备的 IP 地址。
7. 在什么是本地隧道终结点(最接近终结点 1 中的计算机) 下，选择编辑。在IPv4 地址字段中，输入您的 Windows 服务器的私有 IP 地址，然后选择确定。

8. 在什么是远程隧道终结点(最接近终结点 2 中的计算机) 下，选择编辑。在IPv4 地址字段中，输入配置文件中隧道 1 的虚拟专用网关的 IP 地址（参见Remote Tunnel Endpoint），然后选择确定。

> **Important**
>
> 如果您正在对隧道 2 重复此步骤，请确保选择隧道 2 的端点。

9. 在终结点 2 中的计算机下，选择添加。在此 IP 地址或子网字段中，输入您的 VPC 的 CIDR 块，然后选择确定。

> **Important**
>
> 您必须在此对话框中进行滚动，直至您找到端点 2 中的计算机为止。在完成此步骤之前请勿单击下一步，否则您将无法连接到您的服务器。



10. 确认您指定的所有设置都正确，然后选择 Next (下一步)。
11. 在身份验证方法页面上，选择高级，然后选择自定义。
12. 在第一身份验证方法下，选择添加。
13. 选择 Preshared key (预共享密钥)，输入配置文件中的预共享密钥值，然后选择 OK (确定)。

> **Important**
>
> 如果要对隧道 2 重复此步骤，请确保选择隧道 2 的预共享密钥。

14. 确保未选中第一身份验证可选，然后选择确定。
15. 选择下一步。
16. 在 Profile (配置文件) 页面上，选中所有三个复选框：Domain (域)、Private (私有) 和 Public (公有)。选择下一步。
17. 在名称页面中，为您的连接规则输入名称；例如 `VPN to Tunnel 1`，然后选择 Finish (完成) 。

重复以上过程，从配置文件中指定隧道 2 的数据。

完成后，您的 VPN 连接即配置了两条隧道。

确认隧道配置

确认隧道配置

1. 打开服务器管理器，选择工具，选择高级安全 Windows 防火墙，然后选择连接安全规则。
2. 验证两条隧道的以下设置：

   - Enabled (已启用) 为 `Yes`
   - 终结点 1 是您的网络的 CIDR 块
   - 终结点 2 是您的 VPC 的 CIDR 块
   - Authentication mode (身份验证模式) 是 `Require inbound and clear outbound`
   - Authentication method (身份验证方法) 为 `Custom`
   - 端点 1 端口为 `Any`
   - 端点 2 端口为 `Any`
   - Protocol (协议) 为 `Any`

3. 选择第一个规则，然后选择属性。
4. 在 Authentication (身份验证) 选项卡上的 Method (方法) 下，选择 Customize (自定义)。确认 First authentication methods (第一身份验证方法) 包含隧道配置文件中的正确预共享密钥，然后选择 OK (确定)。
5. 在 Advanced (高级) 选项卡中，验证 Domain (域)、Private (私有) 和 Public (公有) 都已被选定。
6. 在 “IPsec 隧道传输” 下，选择 “自定义”。验证以下 IPsec 隧道设置，然后再次选择 “确定” 和 “确定” 以关闭对话框。
   - 已选择 “使用 IPsec 隧道”。
   - 本地隧道端点（最接近端点 1）包含 Windows Server 的 IP 地址。如果您的客户网关设备是 EC2 实例，则这是该实例的私有 IP 地址。
   - Remote tunnel endpoint (closest to Endpoint 2) (本地隧道端点 (最接近端点 2)) 中包含此隧道的虚拟专用网关的 IP 地址。
7. 打开您的第二条隧道的属性。对此隧道重复第 4 步到第 7 步。

启用主密钥完全向前保密

您可以使用命令行启用主密钥完全向前保密。此功能不能通过用户界面启用。

启用主密钥完全向前保密

1. 在您的 Windows Server 中打开新的命令提示符窗口。
2. 输入以下命令，并将 `rule_name` 替换为您为第一个连接规则提供的名称。

```
netsh advfirewall consec set rule name="rule_name" new QMPFS=dhgroup2
 QMSecMethods=ESP:SHA1-AES128+60min+100000kb
```

3. 对第二条隧道重复执行步骤 2，这次使用您为第二个连接规则提供的名称替换 `rule_name`。

配置 Windows 防火墙

在服务器上设置安全规则后，请配置一些基本IPsec 设置以使用虚拟专用网关。

配置 Windows 防火墙

1. 打开 Server Manager（服务器管理器），依次选择 Tools（工具）、Windows Defender Firewall with Advanced Security（高级安全 Windows Defender 防火墙）和 Properties（属性）。

2. 在 “IPsec 设置” 选项卡的 “IPsec豁免” 下，确认 “豁免 ICMP” 是否IPsec为 “否”（默认）。验证IPsec 隧道授权是否为 “无”。
3. 在IPsec 默认值下，选择自定义。
4. 在密钥交换(主模式) 下，选择高级，然后选择自定义。
5. 在 Customize Advanced Key Exchange Settings (自定义高级密钥交换设置) 中的 Security methods (安全方式) 下，验证第一个条目是否使用了以下默认值。

   - 完整性：SHA-1
   - 加密术：AES-CBC 128
   - 密钥交换算法：Diffie-Hellman Group 2
   - 在“Key lifetimes”选项下，验证“Minutes”为480，并且“Sessions”为0。

   以下设置与配置文件中的条目对应。

   ```
   MainModeSecMethods: DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1
   MainModeKeyLifetime: 480min,0sec
   ```

6. 在密钥交换选项下，选择将 Diffie-Hellman 用于增强的安全性，然后选择确定。
7. 在数据保护(快速模式)下，选择高级，然后选择自定义。
8. 选择要求所有使用这些设置的连接安全规则使用加密。
9. 在 Data integrity and encryption (数据完整性和加密算法) 选项下，保留默认值：

   - 协议：ESP
   - 完整性：SHA-1
   - 加密术：AES-CBC 128
   - 使用期限：60 分钟

   这些值与配置文件中的以下条目对应。

   ```
   QuickModeSecMethods:
   ESP:SHA1-AES128+60min+100000kb
   ```

10. 选择 “确定” 返回 “自定义IPsec 设置” 对话框，然后再次选择 “确定” 以保存配置。

步骤 5：启用失效网关检测

接下来，配置 TCP，以删除无法使用的网关。也可以修改注册表键以完成此操作：HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters。在完成前面的部分之前，不要执行此步骤。在您更改注册密钥之后，您必须重新启动服务器。

启用失效网关检测

1. 在 Windows 服务器上，启动命令提示符或 PowerShell 会话，然后输入 regedit 以启动注册表编辑器。
2. 展开 HKEY_LOCAL_ MACHINE，展开 SYSTE M，展开，展开 “服务” CurrentControlSet，展开 Tcpi p，然后展开 “参数”。
3. 从编辑菜单中，选择新建，然后选择 DWORD (32-位)值。
4. 输入名称 EnableDeadGWDetect。
5. 选择EnableDeadGWDetect并选择 “编辑”、“修改”。
6. 在值数据中，输入 1，然后选择确定。
7. 关闭注册表编辑器，并重新启动服务器。

有关更多信息，请参阅 Microsoft TechNet 资源库EnableDeadGWDetect中的。

步骤 6：测试 VPN 连接

要测试 VPN 连接是否正常工作，请在 VPC 中启动一个实例，并确保该实例没有 Internet 连接。启动实例后，从您的 Windows Server 对该实例的私有 IP 地址执行 ping 操作。从客户网关设备生成流量时，VPN 隧道将出现。因此，ping 命令也将启动 VPN 连接。

有关测试 VPN 连接的步骤，请参阅测试 AWS Site-to-Site VPN 连接。

如果 ping 命令失败，请检查以下信息：

- 确保您配置了安全组规则以允许 ICMP 流向您的 VPC 中的实例。如果您的 Windows 服务器是一个 EC2 实例，请确保其安全组的出站规则允许 IPsec 流量。有关更多信息，请参阅 配置您的 Windows 实例。
- 确保您向其发送 ping 命令的实例上的操作系统已配置为响应 ICMP。我们建议您使用其中一款亚马逊 Linux AMIs。
- 如果您要执行 ping 操作的实例是 Windows 实例，请连接到该实例并在 Windows 防火墙 ICMPv4 上启用入站功能。

- 确保为您的 VPC 或子网正确配置了路由表。有关更多信息，请参阅 步骤 1：创建 VPN 连接并配置您的 VPC。
- 如果您的客户网关设备是 EC2 实例，请确保已禁用该实例的源/目标检查。有关更多信息，请参阅配置您的 Windows 实例。

在 Amazon VPC 控制台的 VPN Connections 页面上，选择 VPC 连接。第一条隧道处于 UP 状态。第二条隧道应同时配置，但除非第一条隧道出现故障，否则第二条隧道将无法使用。稍候几分钟，以建立加密隧道。

对 AWS Site-to-Site VPN 客户网关设备进行故障排除

排查客户网关设备故障时，请务必采用结构化方法。本节的前两个主题提供了通用流程图，分别用于排查在使用配置为动态路由的设备（启用 BGP）和配置为静态路由的设备（未启用 BGP）时出现的问题。这些主题之后是针对 Cisco、Juniper 和 Yamaha 客户网关设备的特定设备故障排除指南。

除了本节中的主题外，启用 AWS Site-to-Site VPN 日志对于排查和解决 VPN 连接问题也非常有用。有关一般测试说明，另请参阅测试 AWS Site-to-Site VPN 连接。

主题

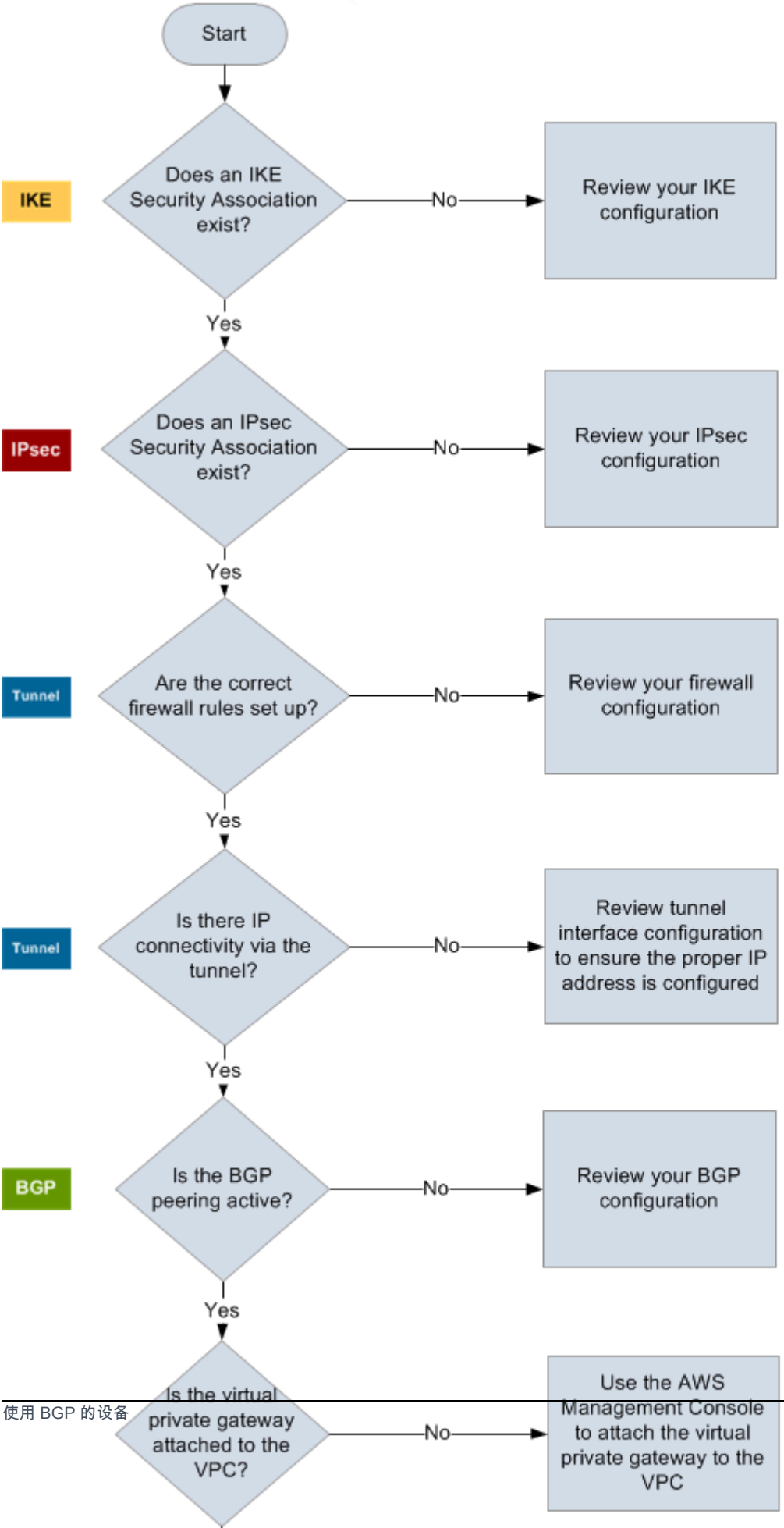
- 使用边界网关协议时排除 AWS Site-to-Site VPN 连接故障
- 在没有边界网关协议的情况下排除 AWS Site-to-Site VPN 连接故障
- 排除与 Cisco ASA 客户网关设备的 AWS Site-to-Site VPN 连接故障
- 排除与 Cisco IOS 客户网关设备的 AWS Site-to-Site VPN 连接故障
- 排除与不使用边界网关协议的 Cisco IOS 客户网关设备的 AWS Site-to-Site VPN 连接故障
- 使用瞻博网络 JunoS 客户网关设备排除 AWS Site-to-Site VPN 连接故障
- 使用瞻博网络 ScreenOS 客户网关设备进行 AWS Site-to-Site VPN 连接故障排除
- 对 Yamaha 客户网关设备的 AWS Site-to-Site VPN 连接进行故障排除

其他资源

- Amazon VPC 论坛
- 如何排查 Amazon VPC 的 VPN 隧道连通性问题？

使用边界网关协议时排除 AWS Site-to-Site VPN 连接故障

以下示意图和表提供了有关排查使用边界网关协议 (BGP) 的客户网关设备的问题的一般指导。此外，建议您启用设备的调试特征。详情请咨询您的网关设备供应商。

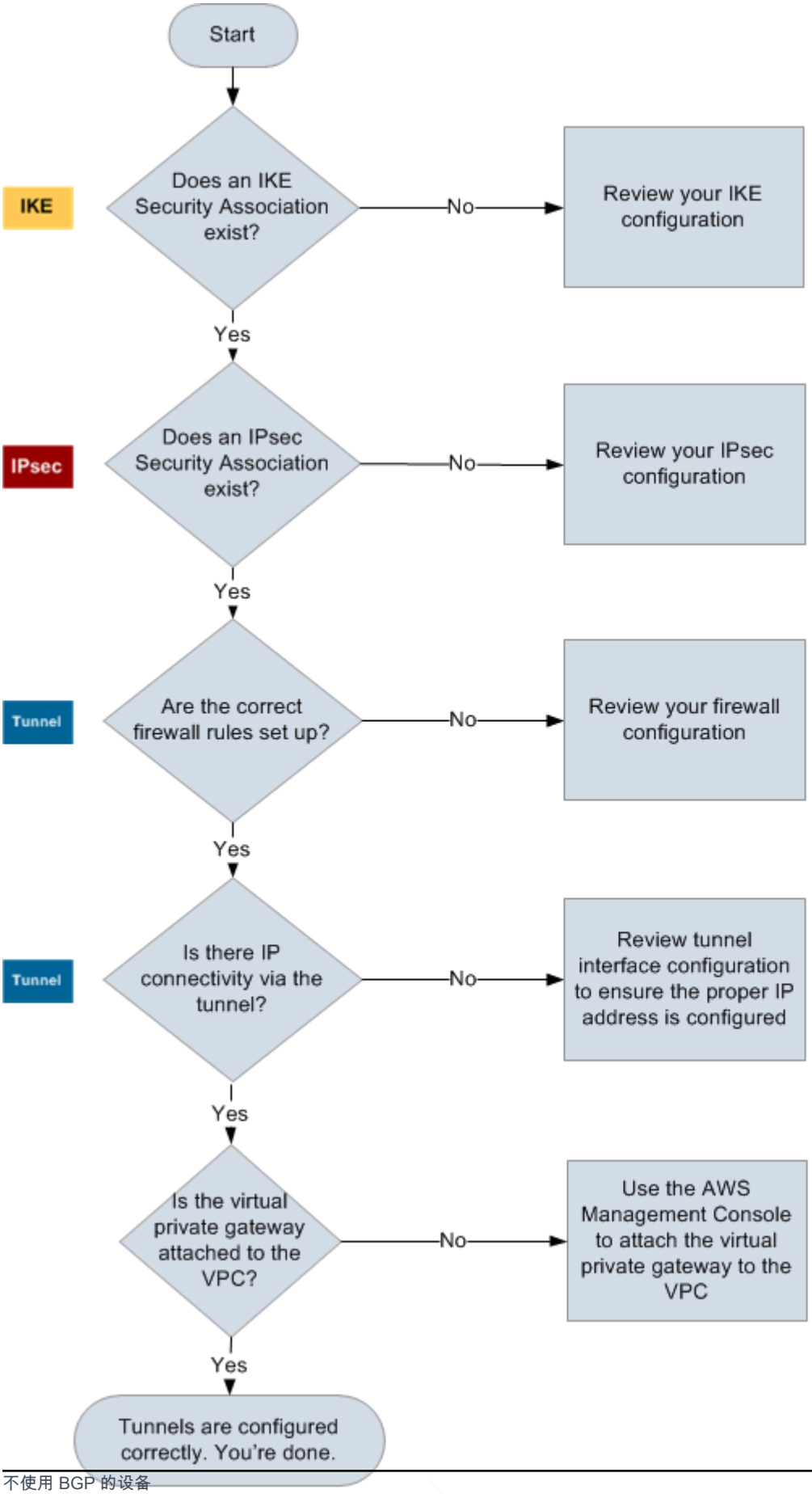

Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
BGP
Is the BGP peering active?
No
Review your BGP configuration
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC

IKE	确定 IKE 安全关联是否存在。 交换用于建立安全关联的密钥需要 IKE IPsec 安全关联。 如果 IKE 安全关联不存在，请核查您的 IKE 配置设置。您必须按配置文件中所列内容来配置加密、身份验证、完全向前保密和模式参数。 如果存在 IKE 安全关联，请转到 “IPsec”。
IPsec	确定是否存在 IPsec 安全关联 (SA)。 S IPsec A 就是隧道本身。查询您的客户网关设备以确定 S IPsec A 是否处于活动状态。确保您按配置文件中所列内容来配置加密、身份验证、完全向前保密和模式参数。 如果不存在 IPsec SA，请检查您的 IPsec 配置。 如果 S IPsec A 存在，请前往 “隧道”。
隧道	确认所需的防火墙规则是否已设置（如需规则列表，请参见 AWS Site-to-Site VPN 客户网关设备的防火墙规则）。如果存在，请继续配置。 确定是否存在通过该隧道的 IP 连通性。 隧道每一端均有如配置文件指定的 IP 地址。虚拟专用网关地址用作 BGP 邻系统的地址。从您的客户网关设备向该地址发出 ping，以确定 IP 流量是否正确加密和解密。 如果 ping 不成功，请核查您的隧道接口配置以确保配置了正确的 IP 地址。 如果 ping 成功，请继续配置“BGP”。
BGP	确定 BGP 对等会话是否活动。 对于每条隧道，请执行以下操作： • 在您的客户网关设备上，确定 BGP 状态是否为 `Active` 或 `Established` 。BGP 对等体可能需要 30 分钟的时间才能转为活跃。 • 确保客户网关设备正在向虚拟私有网关通告默认路由 (0.0.0.0/0)。 若隧道不处于此状态，请核查您的 BGP 配置。

	如果 BGP 对等已建立，并且您正在接收和通告前缀，您的隧道即已正确配置。请确保两条隧道均处于该状态。

在没有边界网关协议的情况下排除 AWS Site-to-Site VPN 连接故障

以下示意图和表提供了有关排除不使用边界网关协议 (BGP) 的客户网关设备的一般指导。此外，建议您启用设备的调试特征。详情请咨询您的网关设备供应商。


Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC
Yes
Tunnels are configured correctly. You're done.

IKE	确定 IKE 安全关联是否存在。 交换用于建立安全关联的密钥需要 IKE IPsec 安全关联。 如果 IKE 安全关联不存在，请核查您的 IKE 配置设置。您必须按配置文件中所列内容来配置加密、身份验证、完全向前保密和模式参数。 如果存在 IKE 安全关联，请转到 “IPsec”。
IPsec	确定是否存在 IPsec 安全关联 (SA)。 S IPsec A 就是隧道本身。查询您的客户网关设备以确定 S IPsec A 是否处于活动状态。确保您按配置文件中所列内容来配置加密、身份验证、完全向前保密和模式参数。 如果不存在 IPsec SA，请检查您的 IPsec 配置。 如果 S IPsec A 存在，请前往 “隧道”。
隧道	确认所需的防火墙规则是否已设置（如需规则列表，请参见 AWS Site-to-Site VPN 客户网关设备的防火墙规则）。如果存在，请继续配置。 确定是否存在通过该隧道的 IP 连通性。 隧道每一端均有如配置文件指定的 IP 地址。虚拟专用网关地址用作 BGP 邻系统的地址。从您的客户网关设备向该地址发出 ping，以确定 IP 流量是否正确加密和解密。 如果 ping 不成功，请核查您的隧道接口配置以确保配置了正确的 IP 地址。 如果 ping 成功，请继续配置“静态路由”。
静态路由	对于每条隧道，请执行以下操作： • 验证您已将隧道作为下一路程段，向 VPC CIDR 添加了一条静态路由。 • 验证您是否已在 Amazon VPC 控制台添加了一条静态路由，以告知虚拟私有网关将流量路由回您的内部网络。 如果隧道不处于该状态，请核查您的设备配置。 确保两条隧道均处于该状态，然后您就完成了。

排除与 Cisco ASA 客户网关设备的 AWS Site-to-Site VPN 连接故障

对 Cisco 客户网关设备的连接进行故障排除时，请考虑 IKE IPsec、和路由。您可以按任何次序对这些方面进行故障排除，不过建议您从 IKE 开始（位于网络堆栈的底部）并依次向上排除。

> **Important**
>
> 某些 Cisco ASAs 仅支持活动/待机模式。使用这些 Cisco 时 ASAs，一次只能有一个活动隧道。仅在第一个隧道不可用的情况下，其他备用隧道才可用。备用隧道可能在您的日志文件中生成以下错误，您可以忽略该错误：`Rejecting IPSec tunnel: no matching crypto map entry for remote proxy 0.0.0.0/0.0.0.0/0/0 local proxy 0.0.0.0/0.0.0.0/0/0 on interface outside`。

IKE

使用以下命令。响应显示带正确配置的 IKE 的客户网关设备。

```
ciscoasa# show crypto isakmp sa
```

```
   Active SA: 2
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1   IKE Peer: AWS_ENDPOINT_1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

您应该可以看到包含隧道中所指定远程网关的 `src` 值的一行或多行。`state` 值应为 `MM_ACTIVE`，`status` 应为 `ACTIVE`。任何项的缺乏或任何项处于其他状态均表示 IKE 未正确配置。

如需进一步排除故障，请运行下面的命令以启用可提供诊断信息的日志消息。

```
router# term mon
router# debug crypto isakmp
```

要禁用调试，请使用下面的命令。

```
router# no debug crypto isakmp
```

IPsec

使用以下命令。响应显示 IPsec配置正确的客户网关设备。

```
ciscoasa# show crypto ipsec sa
```

```
interface: outside
    Crypto map tag: VPN_crypto_map_name, seq num: 2, local addr: 172.25.50.101

      access-list integ-ppe-loopback extended permit ip any vpc_subnet subnet_mask
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (vpc_subnet/subnet_mask/0/0)
      current_peer: integ-ppe1

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

      local crypto endpt.: 172.25.50.101, remote crypto endpt.: AWS_ENDPOINT_1

      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 6D9F8D3B
      current inbound spi : 48B456A6

    inbound esp sas:
      spi: 0x48B456A6 (1219778214)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x6D9F8D3B (1839172923)
```

```
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, PFS Group 2, }
        slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
        sa timing: remaining key lifetime (kB/sec): (4374000/3593)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
        0x00000000 0x00000001
```

对于每个隧道接口，您应该可以看到 `inbound esp sas` 和 `outbound esp sas`。这假设已列出一个 SA（例如`spi: 0x48B456A6`），并且配置 IPsec 正确。

在 Cisco ASA 中， IPsec 只有在发送相关流量（应加密的流量）之后才会出现。为了始终保持 IPsec 活动状态，我们建议配置 SLA 监视器。SLA 监控器继续发送感兴趣的流量，使流量保持 IPsec活动状态。

您也可以使用以下 ping 命令强制开始协商并继续协商。 IPsec

```
ping ec2_instance_ip_address
```

```
Pinging ec2_instance_ip_address with 32 bytes of data:

Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

如需进一步排除故障，请使用下面的命令启用调试。

```
router# debug crypto ipsec
```

要禁用调试，请使用下面的命令。

```
router# no debug crypto ipsec
```

路由

向隧道的另一端发出 ping。如果这行得通，那么你 IPsec 应该被确定下来。如果这不起作用，请检查您的访问列表，并参考上一 IPsec 节。

如果您无法访问实例，请核查以下信息。

1. 验证是否已将访问列表配置为允许与保密图关联的流量。

   您可以使用下面的命令进行这项操作。

   ```
   ciscoasa# show run crypto
   ```

   ```
   crypto ipsec transform-set transform-amzn esp-aes esp-sha-hmac
   crypto map VPN_crypto_map_name 1 match address access-list-name
   crypto map VPN_crypto_map_name 1 set pfs
   crypto map VPN_crypto_map_name 1 set peer AWS_ENDPOINT_1 AWS_ENDPOINT_2
   crypto map VPN_crypto_map_name 1 set transform-set transform-amzn
   crypto map VPN_crypto_map_name 1 set security-association lifetime seconds 3600
   ```

2. 使用以下命令检查访问列表。

   ```
   ciscoasa# show run access-list access-list-name
   ```

   ```
   access-list access-list-name extended permit ip any vpc_subnet subnet_mask
   ```

3. 验证访问列表是否正确。以下示例访问列表允许所有流向 VPC 子网 10.0.0.0/16 的内部流量。

   ```
   access-list access-list-name extended permit ip any 10.0.0.0 255.255.0.0
   ```

4. 从 Cisco ASA 设备运行 traceroute，看看它是否到达了 Amazon 路由器（例如，*AWS_ENDPOINT_1*/ ）。*AWS_ENDPOINT_2*

   如果能访问 Amazon 路由器，则检查您在 Amazon VPC 控制台中添加的静态路由，同时检查特定实例的安全组。

5. 如需进一步排查问题，请核查配置。

反弹隧道接口

如果隧道看起来已开通，但流量无法正常流动，则反弹（禁用和重新启用）隧道接口通常可以解决连接问题。要反弹 Cisco ASA 上的隧道接口，请执行以下操作：

1. 运行以下命令：

```
ciscoasa# conf t
ciscoasa(config)# interface tunnel X  (where X is your tunnel ID)
ciscoasa(config-if)# shutdown
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# end
```

   或者，你可以使用单行命令：

```
ciscoasa# conf t ; interface tunnel X ; shutdown ; no shutdown ; end
```

2. 恢复接口后，检查 VPN 连接是否已重新建立，以及流量现在是否正常流动。

排除与 Cisco IOS 客户网关设备的 AWS Site-to-Site VPN 连接故障

对 Cisco 客户网关设备的连接进行故障排除时，请考虑四件事：IKE IPsec、隧道和 BGP。您可以按任何次序对这些方面进行故障排除，不过建议您从 IKE 开始（位于网络堆栈的底部）并依次向上排除。

IKE

使用以下命令。响应显示带正确配置的 IKE 的客户网关设备。

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.37.160  72.21.209.193   QM_IDLE           2001    0 ACTIVE
192.168.37.160  72.21.209.225   QM_IDLE           2002    0 ACTIVE
```

您应该可以看到包含隧道中所指定远程网关的 `src` 值的一行或多行。`state` 应为 `QM_IDLE`，`status` 应为 `ACTIVE`。任何项的缺乏或任何项处于其他状态均表示 IKE 未正确配置。

如需进一步排除故障，请运行下面的命令以启用可提供诊断信息的日志消息。

```
router# term mon
router# debug crypto isakmp
```

要禁用调试，请使用下面的命令。

```
router# no debug crypto isakmp
```

IPsec

使用以下命令。响应显示 IPsec配置正确的客户网关设备。

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.37.160

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.225
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
      spi: 0x6ADB173(112046451)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE
```

```
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB8357C22(3090512930)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Tunnel2
     Crypto map tag: Tunnel2-head-0, local addr 174.78.144.73

     protected vrf: (none)
     local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     current_peer 72.21.209.193 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
     #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.193
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xF59A3FF6(4120526838)

     inbound esp sas:
      spi: 0xB6720137(3060924727)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
       sa timing: remaining key lifetime (k/sec): (4387273/3492)
       IV size: 16 bytes
```

```
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xF59A3FF6(4120526838)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4387273/3492)
      IV size: 16 bytes
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

对于每个隧道接口，您应该可以看到 `inbound esp sas` 和 `outbound esp sas`。假设 SA 已列出（`spi: 0xF95D2F3C`例如）`ACTIVE`，`Status`并且配置 IPsec 正确。

如需进一步排除故障，请使用下面的命令启用调试。

```
router# debug crypto ipsec
```

使用下面的命令禁用调试。

```
router# no debug crypto ipsec
```

隧道

首先，检查必要的防火墙规则是否已布置到位。有关更多信息，请参阅 AWS Site-to-Site VPN 客户网关设备的防火墙规则。

如果您的防火墙规则设置正确，则请使用下面的命令继续排除故障。

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.255.2/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 72.21.209.225
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

确保 `line protocol` 已运行。检查隧道源 IP 地址、源接口和目的地分别匹配客户网关设备外部 IP 地址、接口和虚拟私有网关外部 IP 地址的隧道配置。确保 `Tunnel protection via IPSec` 已存在。在两个隧道接口上运行命令。要解决任何问题，请查看配置并检查与客户网关设备的物理连接。

另外请使用下面的命令，将 169.254.255.1 替换为您的虚拟专用网关的内部 IP 地址。

```
router# ping 169.254.255.1 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.255.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

您应该可以看到五个感叹号。

如需进一步排查问题，请核查配置。

BGP

使用以下命令。

```
router# show ip bgp summary
```

```
BGP router identifier 192.168.37.160, local AS number 65000
BGP table version is 8, main routing table version 8
2 network entries using 312 bytes of memory
2 path entries using 136 bytes of memory
3/1 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 948 total bytes of memory
BGP activity 4/1 prefixes, 4/1 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
169.254.255.1   4  7224     363     323        8    0    0 00:54:21        1
169.254.255.5   4  7224     364     323        8    0    0 00:00:24        1
```

两个邻系统均已列出。对于每个系统，您应看到 State/PfxRcd 值为 1。

如果 BGP 对等体已运行，请验证您的客户网关设备正在向 VPC 通告默认路由 (0.0.0.0/0)。

```
router# show bgp all neighbors 169.254.255.1 advertised-routes
```

```
For address family: IPv4 Unicast
BGP table version is 3, local router ID is 174.78.144.73
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
     r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

Network             Next Hop            Metric   LocPrf Weight Path
*> 10.120.0.0/16    169.254.255.1          100        0   7224    i

Total number of prefixes 1
```

另外，请确保您正在从虚拟专用网关接收对应于您的 VPC 的前缀。

```
router# show ip route bgp
```

```
 10.0.0.0/16 is subnetted, 1 subnets
B       10.255.0.0 [20/0] via 169.254.255.1, 00:00:20
```

如需进一步排查问题，请核查配置。

排除与不使用边界网关协议的 Cisco IOS 客户网关设备的 AWS Site-to-Site VPN 连接故障

对 Cisco 客户网关设备的连接进行故障排除时，请考虑三件事：IKE IPsec、和隧道。您可以按任何次序对这些方面进行故障排除，不过建议您从 IKE 开始（位于网络堆栈的底部）并依次向上排除。

IKE

使用以下命令。响应显示带正确配置的 IKE 的客户网关设备。

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
174.78.144.73 205.251.233.121 QM_IDLE           2001    0 ACTIVE
174.78.144.73 205.251.233.122 QM_IDLE           2002    0 ACTIVE
```

您应该可以看到包含隧道中所指定远程网关的 `src` 值的一行或多行。`state` 应为 `QM_IDLE`，`status` 应为 `ACTIVE`。任何项的缺乏或任何项处于其他状态均表示 IKE 未正确配置。

如需进一步排除故障，请运行下面的命令以启用可提供诊断信息的日志消息。

```
router# term mon
router# debug crypto isakmp
```

要禁用调试，请使用下面的命令。

```
router# no debug crypto isakmp
```

IPsec

使用以下命令。响应显示 IPsec配置正确的客户网关设备。

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 174.78.144.73

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.121
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
      spi: 0x6ADB173(112046451)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB8357C22(3090512930)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
```

```
       Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Tunnel2
     Crypto map tag: Tunnel2-head-0, local addr 205.251.233.122

     protected vrf: (none)
     local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     current_peer 72.21.209.193 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
     #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.122
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xF59A3FF6(4120526838)

     inbound esp sas:
      spi: 0xB6720137(3060924727)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
       sa timing: remaining key lifetime (k/sec): (4387273/3492)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xF59A3FF6(4120526838)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
```

```
        sa timing: remaining key lifetime (k/sec): (4387273/3492)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:
```

对于每个隧道接口，您均应看到传入 `esp sas` 和传出 `esp sas`。这假设 SA 已列出（例如`spi: 0x48B456A6`），状态为`ACTIVE`，并且配置 IPsec 正确。

如需进一步排除故障，请使用下面的命令启用调试。

```
router# debug crypto ipsec
```

要禁用调试，请使用下面的命令。

```
router# no debug crypto ipsec
```

隧道

首先，检查必要的防火墙规则是否已布置到位。有关更多信息，请参阅 AWS Site-to-Site VPN 客户网关设备的防火墙规则。

如果您的防火墙规则设置正确，则请使用下面的命令继续排除故障。

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.249.18/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 205.251.233.121
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
```

```
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

确保 line protocol 已运行。检查隧道源 IP 地址、源接口和目的地分别匹配客户网关设备外部 IP 地址、接口和虚拟私有网关外部 IP 地址的隧道配置。确保 Tunnel protection through IPSec 已存在。在两个隧道接口上运行命令。要解决任何问题，请查看配置并检查与客户网关设备的物理连接。

您也可以使用下面的命令，将 169.254.249.18 替换为您的虚拟专用网关的内部 IP 地址。

```
router# ping 169.254.249.18 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.249.18, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

您应该可以看到五个感叹号。

路由

要查看您的静态路由表，请使用下面的命令。

```
router# sh ip route static
```

```
     1.0.0.0/8 is variably subnetted
S       10.0.0.0/16 is directly connected, Tunnel1
is directly connected, Tunnel2
```

您应该可以看到通过两个隧道的 VPC CIDR 静态路由存在。如果它不存在，请添加静态路由，如下所示。

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100
```

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200
```

检查 SLA 监视器

```
router# show ip sla statistics 100
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

```
router# show ip sla statistics 200
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 200
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

`Number of successes` 的值指示 SLA 监视器是否已成功设置。

如需进一步排查问题，请核查配置。

使用瞻博网络 JunoS 客户网关设备排除 AWS Site-to-Site VPN 连接故障

对瞻博网络客户网关设备的连接进行故障排除时，请考虑四件事：IKE IPsec、隧道和 BGP。您可以按任何次序对这些方面进行故障排除，不过建议您从 IKE 开始（位于网络堆栈的底部）并依次向上排除。

IKE

使用以下命令。响应显示带正确配置的 IKE 的客户网关设备。

```
user@router> show security ike security-associations
```

```
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
4       72.21.209.225   UP     c4cd953602568b74  0d6d194993328b02  Main
3       72.21.209.193   UP     b8c8fb7dc68d9173  ca7cb0abaedeb4bb  Main
```

您应该可以看到包含隧道中所指定远程网关的远程地址的一行或多行。State 应为 UP。任何项的缺失或任何项处于其他状态（例如 DOWN）均表示 IKE 未正确配置。

如需进一步进行问题排查，请启用 IKE 跟踪选项，如示例配置信息中所推荐。然后运行下面的命令，将各种调试信息打印到屏幕上。

```
user@router> monitor start kmd
```

从外部主机上，您可以使用下面的命令检索整个日志文件。

```
scp username@router.hostname:/var/log/kmd
```

IPsec

使用以下命令。响应显示 IPsec配置正确的客户网关设备。

```
user@router> show security ipsec security-associations
```

```
Total active tunnels: 2
ID      Gateway        Port  Algorithm        SPI      Life:sec/kb Mon vsys
<131073 72.21.209.225  500   ESP:aes-128/sha1 df27aae4 326/ unlim   -   0
>131073 72.21.209.225  500   ESP:aes-128/sha1 5de29aa1 326/ unlim   -   0
<131074 72.21.209.193  500   ESP:aes-128/sha1 dd16c453 300/ unlim   -   0
>131074 72.21.209.193  500   ESP:aes-128/sha1 c1e0eb29 300/ unlim   -   0
```

具体来说，每个网关地址您至少应该看到两行（对应远程网关）。每行开头的插入符号 (< >) 表示特定项的流量方向。在输出内容中，入站流量（“<”，从虚拟私有网关到此客户网关设备的流量）和出站流量（“>”）分别占据单独的行。

如需进一步排查问题，请启用 IKE 跟踪选项 (如需更多信息请参阅前面有关 IKE 的部分)。

隧道

首先，请反复检查必要的防火墙已布置到位。有关规则列表，请参阅AWS Site-to-Site VPN 客户网关设备的防火墙规则。

如果您的防火墙规则设置正确，则请使用下面的命令继续排除故障。

```
user@router> show interfaces st0.1
```

```
Logical interface st0.1 (Index 70) (SNMP ifIndex 126)
   Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
   Input packets : 8719
   Output packets: 41841
   Security: Zone: Trust
   Allowed host-inbound traffic : bgp ping ssh traceroute
   Protocol inet, MTU: 9192
     Flags: None
     Addresses, Flags: Is-Preferred Is-Primary
     Destination: 169.254.255.0/30, Local: 169.254.255.2
```

确保 Security: Zone 正确，并且 Local 地址匹配客户网关设备隧道的内部地址。

下一步，请使用下面的命令，将 169.254.255.1 替换为您的虚拟专用网关的内部 IP 地址。您得到的结果看上去应该如此处所示。

```
user@router> ping 169.254.255.1 size 1382 do-not-fragment
```

```
PING 169.254.255.1 (169.254.255.1): 1410 data bytes
64 bytes from 169.254.255.1: icmp_seq=0 ttl=64 time=71.080 ms
64 bytes from 169.254.255.1: icmp_seq=1 ttl=64 time=70.585 ms
```

如需进一步排查问题，请核查配置。

BGP

运行以下命令。

```
user@router> show bgp summary
```

```
Groups: 1 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0                 2          1          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|
#Active/Received/Accepted/Damped...
169.254.255.1          7224          9         10       0       0        1:00 1/1/1/0
            0/0/0/0
169.254.255.5          7224          8          9       0       0          56 0/1/1/0
            0/0/0/0
```

如需进一步排查问题，请使用下面的命令，将 169.254.255.1 替换为您的虚拟专用网关的内部 IP 地址。

```
user@router> show bgp neighbor 169.254.255.1
```

```
Peer: 169.254.255.1+179 AS 7224 Local: 169.254.255.2+57175 AS 65000
  Type: External    State: Established    Flags: <ImportEval Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Export: [ EXPORT-DEFAULT ]
  Options: <Preference HoldTime PeerAS LocalAS Refresh>
  Holdtime: 30 Preference: 170 Local AS: 65000 Local System AS: 0
  Number of flaps: 0
  Peer ID: 169.254.255.1    Local ID: 10.50.0.10       Active Holdtime: 30
  Keepalive Interval: 10         Peer index: 0
  BFD: disabled, down
  Local Interface: st0.1
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 120
  Stale routes from peer are kept for: 300
  Restart time requested by this peer: 120
  NLRI that peer supports restart for: inet-unicast
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer supports 4 byte AS extension (peer-as 7224)
  Table inet.0 Bit: 10000
    RIB State: BGP restart is complete
    Send state: in sync
```

```
    Active prefixes:              1
    Received prefixes:            1
    Accepted prefixes:            1
    Suppressed due to damping:    0
    Advertised prefixes:          1
Last traffic (seconds): Received 4    Sent 8    Checked 4
Input messages:  Total 24     Updates 2       Refreshes 0     Octets 505
Output messages: Total 26     Updates 1       Refreshes 0     Octets 582
Output Queue[0]: 0
```

在此处，您应看到 Received prefixes 和 Advertised prefixes 逐个列出。上述内容应该在 Table inet.0 部分中。

如果 State 不是 Established，请检查 Last State 和 Last Error，了解纠正问题所需的详细信息。

如果 BGP 对等体已运行，请验证您的客户网关设备正在向 VPC 通告默认路由 (0.0.0.0/0)。

```
user@router> show route advertising-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 0.0.0.0/0               Self                                    I
```

另外，请确保您正在从虚拟私有网关接收对应于您的 VPC 的前缀。

```
user@router> show route receive-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.110.0.0/16           169.254.255.1        100                7224 I
```

使用瞻博网络 ScreenOS 客户网关设备进行 AWS Site-to-Site VPN 连接故障排除

对基于瞻博网络 ScreenOS 的客户网关设备的连接进行故障排除时，请考虑四件事：IKE IPsec、隧道和 BGP。您可以按任何次序对这些方面进行故障排除，不过建议您从 IKE 开始（位于网络堆栈的底部）并依次向上排除。

IKE 和 IPsec

使用以下命令。响应显示带正确配置的 IKE 的客户网关设备。

```
ssg5-serial-> get sa
```

```
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000002<   72.21.209.225  500 esp:a128/sha1 80041ca4  3385 unlim A/-    -1 0
00000002>   72.21.209.225  500 esp:a128/sha1 8cdd274a  3385 unlim A/-    -1 0
00000001<   72.21.209.193  500 esp:a128/sha1 ecf0bec7  3580 unlim A/-    -1 0
00000001>   72.21.209.193  500 esp:a128/sha1 14bf7894  3580 unlim A/-    -1 0
```

您应该可以看到包含隧道中所指定远程网关的远程地址的一行或多行。Sta 值应为 A/-，而 SPI 应为 00000000 以外的十六进制数。处于其他状态的项表示 IKE 未正确配置。

如需进一步进行问题排查，请启用 IKE 跟踪选项（如示例配置文件中所推荐）。

隧道

首先，请反复检查必要的防火墙已布置到位。有关规则列表，请参阅AWS Site-to-Site VPN 客户网关设备的防火墙规则。

如果您的防火墙规则设置正确，则请使用下面的命令继续排除故障。

```
ssg5-serial-> get interface tunnel.1
```

```
  Interface tunnel.1:
  description tunnel.1
  number 20, if_info 1768, if_index 1, mode route
  link ready
  vsys Root, zone Trust, vr trust-vr
  admin mtu 1500, operating mtu 1500, default mtu 1500
  *ip 169.254.255.2/30
  *manage ip 169.254.255.2
  route-deny disable
  bound vpn:
    IPSEC-1

  Next-Hop Tunnel Binding table
  Flag Status Next-Hop(IP)    tunnel-id  VPN
```

```
  pmtu-v4 disabled
  ping disabled, telnet disabled, SSH disabled, SNMP disabled
  web disabled, ident-reset disabled, SSL disabled

  OSPF disabled  BGP enabled  RIP disabled  RIPng disabled  mtrace disabled
  PIM: not configured  IGMP not configured
  NHRP disabled
  bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
             configured ingress mbw 0kbps, current bw 0kbps
             total allocated gbw 0kbps
```

确保您可以看到 `link:ready`，并且 IP 地址匹配客户网关设备隧道的内部地址。

下一步，请使用下面的命令，将 169.254.255.1 替换为您的虚拟专用网关的内部 IP 地址。您得到的结果看上去应该如此处所示。

```
ssg5-serial-> ping 169.254.255.1
```

```
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 169.254.255.1, timeout is 1 seconds
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=32/32/33 ms
```

如需进一步排查问题，请核查配置。

BGP

运行以下命令。

```
ssg5-serial-> get vrouter trust-vr protocol bgp neighbor
```

```
Peer AS Remote IP       Local IP          Wt Status   State     ConnID Up/Down
------------------------------------------------------------------------------
   7224 169.254.255.1   169.254.255.2    100 Enabled  ESTABLISH     10 00:01:01
   7224 169.254.255.5   169.254.255.6    100 Enabled  ESTABLISH     11 00:00:59
```

两个 BGP 对等体的状态均为 ESTABLISH，这表示与虚拟私有网关的 BGP 连接是活动的。

如需进一步排查问题，请使用下面的命令，将 169.254.255.1 替换为您的虚拟专用网关的内部 IP 地址。

```
ssg5-serial-> get vr trust-vr prot bgp neigh 169.254.255.1
```

```
peer: 169.254.255.1,  remote AS: 7224, admin status: enable
type: EBGP, multihop: 0(disable), MED: node default(0)
connection state: ESTABLISH, connection id: 18 retry interval: node default(120s), cur
 retry time 15s
configured hold time: node default(90s), configured keepalive: node default(30s)
configured adv-interval: default(30s)
designated local IP: n/a
local IP address/port: 169.254.255.2/13946, remote IP address/port: 169.254.255.1/179
router ID of peer: 169.254.255.1, remote AS: 7224
negotiated hold time: 30s, negotiated keepalive interval: 10s
route map in name: , route map out name:
weight: 100 (default)
self as next hop: disable
send default route to peer: disable
ignore default route from peer: disable
send community path attribute: no
reflector client: no
Neighbor Capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:  advertised and received
force reconnect is disable
total messages to peer: 106, from peer: 106
update messages to peer: 6, from peer: 4
Tx queue length 0, Tx queue HWM: 1
route-refresh messages to peer: 0, from peer: 0
last reset 00:05:33 ago, due to BGP send Notification(Hold Timer Expired)(code 4 :
 subcode 0)
number of total successful connections: 4
connected: 2 minutes 6 seconds
Elapsed time since last update: 2 minutes 6 seconds
```

如果 BGP 对等体已运行，请验证您的客户网关设备正在向 VPC 通告默认路由 (0.0.0.0/0)。该命令适用于 ScreenOS 6.2.0 和更高版本。

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 advertised
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
--------------------------------------------------------------------------------
```

```
>i          0.0.0.0/0          0.0.0.0 32768    100      0   IGP
Total IPv4 routes advertised: 1
```

另外，确保您正在从虚拟私有网关接收对应于您的 VPC 的前缀。该命令适用于 ScreenOS 6.2.0 和更高版本。

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 received
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix          Nexthop     Wt   Pref    Med Orig    AS-Path
-------------------------------------------------------------------------------
>e*     10.0.0.0/16    169.254.255.1    100    100    100  IGP    7224
Total IPv4 routes received: 1
```

对 Yamaha 客户网关设备的 AWS Site-to-Site VPN 连接进行故障排除

对雅马哈客户网关设备的连接进行故障排除时，请考虑四件事：IKE、 IPsec、隧道和 BGP。您可以按任何次序对这些方面进行故障排除，不过建议您从 IKE 开始（位于网络堆栈的底部）并依次向上排除。

> **Note**
>
> IKE 的第 2 阶段中使用的 `proxy ID` 设置在 Yamaha 路由器上默认处于禁用状态。这可能会导致连接到 Site-to-Site VPN 时出现问题。如果您的路由器上未配置，请查看 AWS提供的 Yamaha 示例配置文件以进行正确设置。`proxy ID`

IKE

运行以下命令。响应显示带正确配置的 IKE 的客户网关设备。

```
# show ipsec sa gateway 1
```

```
sgw  flags local-id                      remote-id        # of sa
-------------------------------------------------------------------------
1    U K   YOUR_LOCAL_NETWORK_ADDRESS     72.21.209.225    i:2 s:1 r:1
```

您应该可以看到包含隧道中所指定远程网关的 `remote-id` 值的行。您可以通过省略隧道号来列出所有安全关联 (SAs)。

如需进一步排查问题，请运行下面的命令，启用可提供诊断信息的 DEBUG 级日志消息。

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

要取消记录项，请运行下面的命令。

```
# no ipsec ike log
# no syslog debug on
```

IPsec

运行以下命令。响应显示 IPsec配置正确的客户网关设备。

```
# show ipsec sa gateway 1 detail
```

```
SA[1] Duration: 10675s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit

SPI: 6b ce fd 8a d5 30 9b 02 0c f3 87 52 4a 87 6e 77
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[2] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: send
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: a6 67 47 47
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[3] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: receive
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: 6b 98 69 2b
```

```
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[4] Duration: 10681s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit
SPI: e8 45 55 38 90 45 3f 67 a8 74 ca 71 ba bb 75 ee
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
```

对于每个隧道接口，您应该可以看到 `receive sas` 和 `send sas`。

如需进一步排除故障，请使用下面的命令启用调试。

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

运行下面的命令以禁用调试。

```
# no ipsec ike log
# no syslog debug on
```

隧道

首先，检查必要的防火墙规则是否已布置到位。有关规则列表，请参阅AWS Site-to-Site VPN 客户网关设备的防火墙规则。

如果您的防火墙规则设置正确，则请使用下面的命令继续排除故障。

```
# show status tunnel 1
```

```
TUNNEL[1]:
Description:
  Interface type: IPsec
  Current status is Online.
  from 2011/08/15 18:19:45.
  5 hours 7 minutes 58 seconds  connection.
  Received:    (IPv4) 3933 packets [244941 octets]
               (IPv6) 0 packet [0 octet]
  Transmitted: (IPv4) 3933 packets [241407 octets]
```

```
                (IPv6) 0 packet [0 octet]
```

确保current status值在线，也Interface type就是说 IPsec。确保在两个隧道接口上运行命令。如需在此解决任何问题，请核查配置。

BGP

运行以下命令。

```
# show status bgp neighbor
```

```
BGP neighbor is 169.254.255.1, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.1, Foreign port: 0

BGP neighbor is 169.254.255.5, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.5, Foreign port:
```

两个邻系统均已列出。对于每个系统，您应看到 BGP state 值为 Active。

如果 BGP 对等体已运行，请验证您的客户网关设备正在向 VPC 通告默认路由 (0.0.0.0/0)。

```
# show status bgp neighbor 169.254.255.1 advertised-routes
```

```
Total routes: 1
*: valid route
```

```
  Network             Next Hop        Metric LocPrf Path
* default             0.0.0.0              0        IGP
```

另外，确保您正在从虚拟私有网关接收对应于您的 VPC 的前缀。

```
# show ip route
```

```
Destination         Gateway          Interface       Kind  Additional Info.
default             ***.***.***.***   LAN3(DHCP)    static
10.0.0.0/16         169.254.255.1    TUNNEL[1]       BGP  path=10124
```

与... 一起工作 AWS Site-to-Site VPN

您可以使用 Amazon Site-to-Site VPC 控制台或使用 VPN 资源 AWS CLI。

内容

为 AWS 云广域网创建 AWS Site-to-Site VPN 附件

您可以使用以下步骤为 AWS Cloud WAN 创建 Site-to-Site VPN 附件。按照以下步骤为云 WAN 创建 VPN 连接。有关 VPN 附件和云广域网的更多信息，请参阅云广域网用户指南中的 AWS 云广域网中的 Site-to-site AWS VPN 附件。

使用控制台为 AWS Cloud WAN 创建 VPN 连接

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择创建 VPN 连接。
4. （可选）对于名称标签，输入连接的名称。这样做可创建具有 Name 键以及您指定的值的标签。
5. 对于 Target gateway type（目标网关类型），请选择 Not associated（未关联）。
6. 对于客户网关，执行以下操作之一：
   - 要使用现有的客户网关，请选择现有，然后选择客户网关。

- 要创建客户网关，请选择新建。对于 IP address（IP 地址），请输入静态公有 IP 地址。对于证书 ARN，请选择私有证书的 ARN（如果使用基于证书的身份验证）。对于 BGP ASN，输入您的客户网关的边界网关协议（BGP）自治系统编号（ASN）。有关更多信息，请参阅客户网关选项。

7. 对于路由选项，选择动态或静态。
8. 对于 IP 内的 Tunnel 版本，请选择IPv4或IPv6。
9. （可选）对于启用加速，选中复选框可启用加速。有关更多信息，请参阅 加速的 VPN 连接。

   如果您启用加速，我们将创建两个加速器以供您的 VPN 连接使用。将收取额外费用。
10. （可选）对于本地 IPv4 网络 CIDR，请指定允许通过 VPN 隧道进行通信的客户网关（本地）端的 IPv4 CIDR 范围。默认为 `0.0.0.0/0`。

    对于远程 IPv4 网络 CIDR，请指定允许通过 VPN 隧道进行通信 AWS 的一侧的 IPv4 CIDR 范围。默认为 `0.0.0.0/0`。

    如果您在 IP 版本内指定IPv6隧道，则在允许通过 VPN 隧道进行通信的客户网关端和 AWS 端指定允许通过 VPN 隧道进行通信的 IPv6 CIDR 范围。这两个范围的默认值均为 `::/0`。
11. （可选）对于隧道选项，您可以选择为每个隧道指定以下信息：

    - 内部隧道 IPv4 地址`169.254.0.0/16`范围 IPv4 中的 CIDR 块大小为 /30。
    - 如果您在 IP 版本内IPv6为 Tunnel 指定，则内部隧道地址`fd00::/8`范围中会有 /126 IPv6 CIDR 块。 IPv6
    - IKE 预共享密钥（PSK）。支持以下版本： IKEv1 或 IKEv2。
    - 要编辑隧道的高级选项，请选择编辑隧道选项。有关更多信息，请参阅 VPN 隧道选项。
12. 选择创建 VPN 连接。

使用命令行或 API 创建 Site-to-Site VPN 连接

- CreateVpnConnection（亚马逊 EC2 查询 API）
- create-vpn-connection (AWS CLI)

创建公交网关 AWS Site-to-Site VPN 附件

要在中转网关上创建 VPN 挂载，您必须指定中转网关和客户网关。在执行此过程之前，需要创建中转网关。有关创建中转网关的更多信息，请参阅 Amazon VPC 中转网关 中的中转网关。

使用控制台在中转网关上创建 VPN 挂载

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择创建 VPN 连接。
4. （可选）对于名称标签，输入连接的名称。这样做可创建具有 Name 键以及您指定的值的标签。
5. 对于目标网关类型，选择中转网关，然后选择中转网关。
6. 对于客户网关，执行以下操作之一：
   - 要使用现有的客户网关，请选择现有，然后选择客户网关。

     如果您的客户网关位于为 NAT 遍历（NAT-T）而启用的网络地址转换（NAT）设备后面，请使用您的 NAT 设备的公有 IP 地址，并调整防火墙规则以取消阻止 UDP 端口 4500。
   - 要创建客户网关，请选择新建。对于 IP Address（IP 地址），请输入静态公有 IP 地址。对于证书 ARN，请选择私有证书的 ARN（如果使用基于证书的身份验证）。对于 BGP ASN，输入您的客户网关的边界网关协议（BGP）自治系统编号（ASN）。有关更多信息，请参阅客户网关选项。
7. 对于路由选项，选择动态或静态。
8. 对于 IP 版本内的隧道，指定 VPN 隧道是否支持 IPv4 或 IPv6 流量。 IPv6 只有传输网关上的 VPN 连接才支持流量。
9. （可选）对于启用加速，选中复选框可启用加速。有关更多信息，请参阅 加速的 VPN 连接。

   如果您启用加速，我们将创建两个加速器以供您的 VPN 连接使用。将收取额外费用。
10. （可选）对于本地 IPv4 网络 CIDR，请指定允许通过 VPN 隧道进行通信的客户网关（本地）端的 IPv4 CIDR 范围。默认为 `0.0.0.0/0`。

    对于远程 IPv4 网络 CIDR，请指定允许通过 VPN 隧道进行通信 AWS 的一侧的 IPv4 CIDR 范围。默认为 `0.0.0.0/0`。

    如果您在 IP 版本内指定IPv6隧道，则在允许通过 VPN 隧道进行通信的客户网关端和 AWS 端指定允许通过 VPN 隧道进行通信的 IPv6 CIDR 范围。这两个范围的默认值均为 `::/0`。
11. （可选）对于隧道选项，您可以选择为每个隧道指定以下信息：
    - 内部隧道 IPv4 地址`169.254.0.0/16`范围 IPv4 中的 CIDR 块大小为 /30。
    - 如果您在 IP 版本内IPv6为 Tunnel 指定，则内部隧道地址`fd00::/8`范围中会有 /126 IPv6 CIDR 块。 IPv6
    - IKE 预共享密钥（PSK）。支持以下版本： IKEv1 或 IKEv2。

- 要编辑隧道的高级选项，请选择编辑隧道选项。有关更多信息，请参阅 VPN 隧道选项。

12. 选择创建 VPN 连接。

使用创建 VPN 附件 AWS CLI

使用create-vpn-connection命令并为该`--transit-gateway-id`选项指定传输网关 ID。

测试 AWS Site-to-Site VPN 连接

创建 AWS Site-to-Site VPN 连接并配置客户网关后，您可以启动实例并通过 ping 实例来测试连接。

在您开始之前，确保完成以下操作：

- 使用可以响应 Ping 请求的 AMI。我们建议您使用其中一款亚马逊 Linux AMIs。
- 在您的 VPC 中配置过滤实例流量的任意安全组或网络 ACL，以允许入站和出站 ICMP 流量。这使实例能够接收 `ping` 请求。
- 如果您使用的是运行 Windows Server 的实例，请连接到该实例并在 Windows 防火墙 ICMPv4 上启用入站功能，以便 ping 该实例。
- （静态路由）确保客户网关设备具有指向 VPC 的静态路由，并且您的 VPN 连接具有静态路由，这样流量可以返回到您的客户网关设备。
- （动态路由）确保在客户网关设备上建立了 BGP 状态。建立 BGP 对等会话大约需要 30 秒时间。确保路由通过 BGP 正确通告并显示在子网路由表中，以便流量能够返回到您的客户网关。请确保两个隧道都配置了 BGP 路由。
- 确保您已在子网路由表中为 VPN 连接配置了路由。

测试连接

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在控制面板上，选择启动实例。
3. （可选）对于名称，为您的实例输入一个描述性名称。
4. 对于应用程序和操作系统映像（Amazon 机器映像），选择快速启动，然后为您的实例选择操作系统。
5. 对于密钥对名称，选择现有密钥对或新建一个密钥对。
6. 对于网络设置，选择选择现有安全组，然后选择您配置的安全组。

7. 在 Summary（摘要）面板中，选择 Launch instance（启动实例）。
8. 当实例开始运行后，获取其私有 IP 地址 (例如 10.0.0.4)。Amazon EC2 控制台将地址显示为实例详细信息的一部分。
9. 对于在您的网络中、位于客户网关设备背后的计算机，您可以使用 ping 命令侦测实例的私有 IP 地址。

   ```
   ping 10.0.0.4
   ```

   成功的响应与以下内容类似。

   ```
   Pinging 10.0.0.4 with 32 bytes of data:

   Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
   Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
   Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

   Ping statistics for 10.0.0.4:
   Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

   Approximate round trip times in milliseconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
   ```

   为测试隧道失效转移，您可临时禁用客户网关设备上的隧道之一，然后重复此步骤。您无法禁用 VPN 连接的 AWS 端的隧道。
10. 要测试从 AWS 您的本地网络的连接，您可以使用 SSH 或 RDP 从您的网络连接到您的实例。然后，您可以使用网络中另一台计算机的私有 IP 地址运行 ping 命令，以验证连接的两端是否可以启动和接收请求。

    有关如何连接到 Linux 实例的更多信息，请参阅亚马逊 EC2 用户指南中的连接到您的 Linux 实例。有关如何连接到 Windows 实例的更多信息，请参阅亚马逊 EC2 用户指南中的连接到您的 Windows 实例。

删除 AWS Site-to-Site VPN 连接和网关

如果您不再需要 AWS Site-to-Site VPN 连接，可以将其删除。当您删除 Site-to-Site VPN 连接时，我们不会删除与 VP Site-to-Site N 连接关联的客户网关或虚拟专用网关。如果您不再需要相关的客户网关和虚拟私有网关，可以将其删除。

> **Warning**
>
> 如果您删除了 Site-to-Site VPN 连接然后创建了新连接，则必须下载新的配置文件并重新配置客户网关设备。

任务

- 删除 AWS Site-to-Site VPN 连接
- 删除 AWS Site-to-Site VPN 客户网关
- 在中分离和删除虚拟专用网关 AWS Site-to-Site VPN

删除 AWS Site-to-Site VPN 连接

删除 Site-to-Site VPN 连接后，它会在短时间内保持可见状态，状态为`deleted`，然后该条目会自动删除。

使用控制台删除 VPN 连接

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择 VPN 连接，然后依次选择操作和删除 VPN 连接。
4. 提示进行确认时，输入 **`delete`**，然后选择 Delete（删除）。

使用命令行或 API 删除 VPN 连接

- DeleteVpnConnection（亚马逊 EC2 查询 API）
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

删除 AWS Site-to-Site VPN 客户网关

如果您不再需要某一客户网关，可以将其删除。您无法删除 Site-to-Site VPN 连接中使用的客户网关。

使用控制台删除客户网关

1. 在导航窗格中，选择客户网关。

2. 选择客户网关，然后依次选择操作和删除客户网关。
3. 提示进行确认时，输入 **delete**，然后选择 Delete（删除）。

使用命令行或 API 删除客户网关

- DeleteCustomerGateway（亚马逊 EC2 查询 API）
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (AWS Tools for Windows PowerShell)

在中分离和删除虚拟专用网关 AWS Site-to-Site VPN

如果您不再需要 VPC 的某一虚拟私有网关，可以将其与 VPC 断开。

使用控制台断开虚拟私有网关

1. 在导航窗格中，选择虚拟私有网关。
2. 选择相应的虚拟私有网关，然后选择 Actions、Detach from VPC。
3. 选择分离虚拟私有网关。

如果不再需要某一断开的虚拟私有网关，可将其删除。您无法删除仍与 VPC 关联的虚拟私有网关。虚拟私有网关删除之后，它会在短时间内保持可见，状态为 `deleted`，然后该条目将被自动删除。

使用控制台删除虚拟私有网关

1. 在导航窗格中，选择虚拟私有网关。
2. 选择虚拟私有网关，然后依次选择操作和删除虚拟私有网关。
3. 提示进行确认时，输入 **delete**，然后选择 Delete（删除）。

使用命令行或 API 断开虚拟私有网关

- DetachVpnGateway（亚马逊 EC2 查询 API）
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway (AWS Tools for Windows PowerShell)

使用命令行或 API 删除虚拟私有网关

- DeleteVpnGateway（亚马逊 EC2 查询 API）
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

修改 AWS Site-to-Site VPN 连接的目标网关

您可以修改 AWS Site-to-Site VPN 连接的目标网关。以下迁移选项可用：

- 现有虚拟私有网关到中转网关
- 到另一个虚拟专用网关的现有虚拟专用网关
- 现有中转网关到另一个中转网关
- 现有中转网关到虚拟私有网关

修改目标网关后，在我们配置新的终端节点期间，您的 Site-to-Site VPN 连接将在短时间内暂时不可用。

以下任务可帮助您完成迁移到新网关的过程。

任务

- 步骤 1：创建新的目标网关
- 步骤 2：删除您的静态路由（有条件）
- 步骤 3：迁移到新网关
- 步骤 4：更新 VPC 路由表
- 步骤 5：更新目标网关路由（有条件）
- 步骤 6：更新客户网关 ASN（有条件）

步骤 1：创建新的目标网关

在执行向新目标网关的迁移之前，您必须先配置新的网关。有关添加虚拟专用网关的信息，请参阅the section called “创建虚拟专用网关”。有关添加中转网关的更多信息，请参阅 Amazon VPC 中转网关 中的创建中转网关。

如果新的目标网关是传输网关，请将 VPCs 连接到传输网关。有关 VPC 挂载的信息，请参阅 Amazon VPC 中转网关 中的 VPC 的中转网关挂载。

在将目标从虚拟私有网关修改为中转网关时，您可以选择将中转网关 ASN 设置为与虚拟私有网关 ASN 相同的值。如果您选择使用其他 ASN，则必须将客户网关设备上的 ASN 设置为中转网关 ASN。有关更多信息，请参阅 the section called “步骤 6：更新客户网关 ASN（有条件）”。

步骤 2：删除您的静态路由（有条件）

当您从具有静态路由的虚拟私有网关迁移到中转网关时，此步骤是必需的。

您必须先删除静态路由，然后再迁移到新的网关。

> **Tip**
>
> 保留一份静态路由，然后将其删除。在 VPN 连接迁移完成后，您需要将这些路由重新添加到中转网关。

从路由表中删除路由

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Route tables（路由表），然后选择路由表。
3. 在路由选项卡上，选择编辑路由。
4. 对于到虚拟私有网关的静态路由，选择删除。
5. 选择保存更改。

步骤 3：迁移到新网关

更改目标网关

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择 VPN 连接，然后依次选择操作和修改 VPN 连接。
4. 对于目标类型，选择网关类型。

    a. 如果新目标网关为虚拟私有网关，则选择 VPN 网关。

b. 如果新目标网关为中转网关，则选择中转网关。

5. 选择 Save changes（保存更改）。

使用命令行或 API 修改 Site-to-Site VPN 连接

- ModifyVpnConnection（亚马逊 EC2 查询 API）
- modify-vpn-connection (AWS CLI)

步骤 4：更新 VPC 路由表

迁移到新的网关后，您可能需要修改您的 VPC 路由表。有关更多信息，请参阅《Amazon VPC 用户指南》中的路由表。

下表说明了有关修改 VPN 网关目标后要进行的 VPC 路由表更新。

现有网关	新网关	VPC 路由表更改
使用传播路由的虚拟专用网关	Transit Gateway	添加包含中转网关 ID 的路由。
使用传播路由的虚拟专用网关	使用传播路由的虚拟专用网关	无需操作。
使用传播路由的虚拟专用网关	使用静态路由的虚拟专用网关	添加一个路由，其中包含新的虚拟私有网关的 ID。
使用静态路由的虚拟专用网关	Transit Gateway	将包含虚拟私有网关 ID 的路由更新为包含中转网关的 ID。
使用静态路由的虚拟专用网关	使用静态路由的虚拟专用网关	将包含虚拟私有网关 ID 的路由更新为包含新的虚拟私有网关的 ID。
使用静态路由的虚拟专用网关	使用传播路由的虚拟专用网关	删除包含虚拟私有网关 ID 的路由。
Transit Gateway	使用静态路由的虚拟专用网关	将包含中转网关 ID 的路由更新为包含虚拟私有网关的 ID。
Transit Gateway	使用传播路由的虚拟专用网关	删除包含中转网关 ID 的路由。

现有网关	新网关	VPC 路由表更改
Transit Gateway	Transit Gateway	将包含中转网关 ID 的路由更新为包含新的中转网关的 ID。

步骤 5：更新目标网关路由（有条件）

当新网关是传输网关时，修改传输网关路由表以允许 VPC 和 VP Site-to-Site N 之间的流量。有关更多信息，请参阅 Amazon VPC Transit Gateway中的中转网关路由表。

如果您删除了 VPN 静态路由，则必须将这些静态路由添加到中转网关路由表中。

与虚拟私有网关不同，中转网关将为一个 VPN 挂载上的所有隧道设置相同的多出口标识（MED）值。如果要从虚拟私有网关迁移到中转网关，并依据 MED 值进行隧道选择，我们建议您更改路由以避免连接问题。例如，您可以在中转网关上公布更具体的路由。有关更多信息，请参阅 路由表和 AWS Site-to-Site VPN 路由优先级。

步骤 6：更新客户网关 ASN（有条件）

当新网关具有与旧网关不同的 ASN 时，您必须更新客户网关设备上的 ASN 以指向新 ASN。参阅 您的 AWS Site-to-Site VPN 连接的客户网关选项 了解更多信息。

修改 AWS Site-to-Site VPN 连接选项

您可以修改 Site-to-Site VPN 连接的连接选项。您可以修改以下选项：

- IPv4 CIDR 范围位于可通过 VPN 隧道进行通信的 VPN 连接的本地（客户网关）端和远程 (AWS) 端。对于这两个范围，默认值为 `0.0.0.0/0`。
- IPv6 CIDR 范围位于可通过 VPN 隧道进行通信的 VPN 连接的本地（客户网关）和远程 (AWS) 端。对于这两个范围，默认值为 `::/0`。

修改 VPN 连接选项时， AWS 侧面的 VPN 端点 IP 地址不会更改，隧道选项也不会更改。在 VPN 连接更新过程中，您的 VPN 连接将在短时间内暂时不可用。

使用控制台修改 VPN 连接选项

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。

2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择您的 VPN 连接，然后依次选择操作和修改 VPN 连接选项。
4. 根据需要输入新的 CIDR 范围。
5. 选择 Save changes（保存更改）。

使用命令行或 API 修改 VPN 连接选项

- modify-vpn-connection-options (AWS CLI)
- ModifyVpnConnectionOptions（亚马逊 EC2 查询 API）

修改 AWS Site-to-Site VPN 隧道选项

您可以修改 VPN 连接中的 VPN 隧道的隧道选项。 Site-to-Site可以一次修改一个 VPN 隧道。

> **Important**
>
> 在修改 VPN 隧道时，该隧道上的连接会被中断长达几分钟。确保您为预期的停机时间做了计划。

使用控制台修改 VPN 隧道选项

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择 Site-to-Site VPN 连接，然后选择操作、修改 VPN 隧道选项。
4. 对于 VPN 隧道外部 IP 地址，选择 VPN 隧道的隧道端点 IP。
5. 根据需要为隧道选项选择或输入新值。有关隧道选项的更多信息，请参阅 VPN 隧道选项。

   > **Note**
   >
   > 某些隧道选项有多个默认值。单击可删除任何默认值。然后，系统将从隧道选项中删除该默认值。

6. 选择 Save changes（保存更改）。

使用命令行或 API 修改 VPN 隧道选项

- (AWS CLI) describe-vpn-connections用于查看当前隧道选项和modify-vpn-tunnel-options修改隧道选项。
- （Amazon EC2 Query API）用于DescribeVpnConnections查看当前隧道选项和ModifyVpnTunnelOptions修改隧道选项。

编辑 AWS Site-to-Site VPN 连接的静态路由

对于配置为静态路由的虚拟专用网关上的 Site-to-Site VPN 连接，您可以在 VPN 配置中添加或删除静态路由。

使用控制台添加或删除静态路由

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择 VPN 连接。
4. 选择编辑静态路由。
5. 根据需要添加或删除路由。
6. 选择 Save changes（保存更改）。
7. 如果您尚未为路由表启用路由传播，则必须手动更新您的路由表中的路由以在 VPN 连接中反映更新的静态 IP 前缀。有关更多信息，请参阅（虚拟私有网关）在路由表中启用路由传播。
8. 对于中转网关上的 VPN 连接，您可以在中转网关路由表中添加、修改或删除静态路由。有关更多信息，请参阅 Amazon VPC Transit Gateway中的中转网关路由表。

使用命令行或 API 添加静态路由

- CreateVpnConnectionRoute（亚马逊 EC2 查询 API）
- create-vpn-connection-route (AWS CLI)
- New-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

使用命令行或 API 删除静态路由

- DeleteVpnConnectionRoute（亚马逊 EC2 查询 API）
- delete-vpn-connection-route (AWS CLI)

- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

更改 AWS Site-to-Site VPN 连接的客户网关

您可以使用 Amazon Site-to-Site VPC 控制台或命令行工具更改 VPN 连接的客户网关。

更改客户网关后，在我们预调配新端点时，您的 VPN 连接将在短时间内暂时不可用。

使用控制台更改客户网关

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择 VPN 连接。
4. 依次选择操作和修改 VPN 连接。
5. 对于目标类型，选择客户网关。
6. 对于目标客户网关，选择新的客户网关。
7. 选择 Save changes（保存更改）。

使用命令行或 API 更高客户网关

- ModifyVpnConnection（亚马逊 EC2 查询 API）
- modify-vpn-connection (AWS CLI)

替换已泄露的 AWS Site-to-Site VPN 连接凭证

如果您认为 Site-to-Site VPN 连接的隧道凭证已被泄露，则可以更改 IKE 预共享密钥或更改 ACM 证书。您使用的方法取决于您用于 VPN 隧道的身份验证选项。有关更多信息，请参阅 AWS Site-to-Site VPN 隧道身份验证选项。

更改 IKE 预共享密钥

您可以修改 VPN 连接的隧道选项，并为每个隧道指定新的 IKE 预共享密钥。有关更多信息，请参阅修改 AWS Site-to-Site VPN 隧道选项。

或者，您可以删除 VPN 连接。有关更多信息，请参阅 删除 VPN 连接和网关。您不需要删除 VPC 或虚拟专用网关。然后，使用相同的虚拟私有网关创建一个新的 VPN 连接，并在您的客户网关设备中配

置新的密钥。您可以为隧道指定自己的预共享密钥，也可以让您 AWS 生成新的预共享密钥。有关更多信息，请参阅创建 VPN 连接。重新创建 VPN 连接时，隧道的内部和外部地址可能会发生变化。

更改隧道端点 AWS 一侧的证书

轮换证书。有关更多信息，请参阅 轮换 VPN 隧道端点证书。

更改客户网关设备上的证书

1. 创建新证书。有关信息，请参阅《AWS Certificate Manager 用户指南》中的发布和管理证书。
2. 将证书添加到客户网关设备。

轮换 AWS Site-to-Site VPN 隧道端点证书

您可以使用 Amazon VPC 控制台在 AWS 侧面的隧道终端节点上轮换证书。当隧道端点的证书即将到期时，使用服务相关角色 AWS 自动轮换证书。有关更多信息，请参阅 the section called “服务相关角色”。

使用控制台轮换 Site-to-Site VPN 隧道端点证书

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择 Site-to-Site VPN 连接，然后选择操作、修改 VPN 隧道证书。
4. 选择隧道端点。
5. 选择保存。

要轮换 Site-to-Site VPN 隧道端点证书，请使用 AWS CLI

使用 modify-vpn-tunnel-certificate 命令。

带有的私 AWS Site-to-Site VPN 有 IP AWS Direct Connect

借助私有 IP VPN，您可以通过部署 IPsec VPN AWS Direct Connect，加密本地网络和本地网络之间的流量 AWS，而无需使用公有 IP 地址或其他第三方 VPN 设备。

私有 IP VPN 的主要用例之一 AWS Direct Connect 是帮助金融、医疗保健和联邦行业的客户实现监管和合规目标。Private IP VPN AWS Direct Connect 可确保 AWS 与本地网络之间的流量既安全又私密，从而使客户能够遵守其监管和安全规定。

私有 IP VPN 的好处

- 简化的网络管理和操作：如果没有私有 IP VPN，客户必须部署第三方 VPN 和路由器来实现 AWS Direct Connect 网络私 VPNs 有化。利用私有 IP VPN 功能，客户无需部署和管理自己的 VPN 基础结构。这可以简化网络运营并降低成本。
- 改善安全状况：以前，客户必须使用公共 AWS Direct Connect 虚拟接口 (VIF) 来加密流量 AWS Direct Connect，这需要为 VPN 端点提供公有 IP 地址。公开使用 IPs 会增加外部 (DOS) 攻击的可能性，这反过来又迫使客户部署额外的安全设备来保护网络。此外，公共 VIF 开放了所有 AWS 公共服务和客户本地网络之间的访问权限，从而增加了风险的严重性。私有 IP VPN 功能允许通过 AWS Direct Connect 传输进行加密 VIFs（而不是公共 VIFs），并能够配置私有 IPs。除了加密之外，这还提供 end-to-end私有连接，从而改善了整体安全状况。
- 更高的路由规模：私有 IP VPN 连接提供更高的路由限制（5000 条出站路由和 1000 条入站路由），而 AWS Direct Connect 单独连接目前限制为 200 条出站路由和 100 条入站路由。

私有 IP VPN 的工作原理

私有 IP Site-to-Site VPN 通过 AWS Direct Connect 传输虚拟接口 (VIF) 运行。它使用 AWS Direct Connect 网关和传输网关将您的本地网络与 AWS VPCs之互连。私有 IP VPN 连接在 AWS 侧面的传输网关和本地端的客户网关设备上都有终止点。您必须为 IPsec 隧道的传输网关和客户网关设备端分配私有 IP 地址。您可以使用任一地址范围内的私有 IP 地址， RFC1918 也可以使用 RFC6598 私有 IPv4 地址范围。

您将私有 IP VPN 连接附加到中转网关。然后，您可以在 VPN 连接和也连接到传输网关的任何 VPCs（或其他网络）之间路由流量。您可以通过将路由表与 VPN 连接关联来实现此目标。相反，您可以使用与关联的路由表，将流量从您的路由 VPCs 到私有 IP VPN 附件 VPCs。

与 VPN 连接关联的路由表可以与底层 AWS Direct Connect 连接关联的路由表相同或不同。这使您能够在本地网络和本地网络之间同时路由加密 VPCs和未加密的流量。

有关离开 VPN 的流量路径的更多详细信息，请参阅《AWS Direct Connect 用户指南》中的私有虚拟接口和中转虚拟接口路由策略。

任务

- 通过创建私有 AWS Site-to-Site VPN IP AWS Direct Connect

通过创建私有 AWS Site-to-Site VPN IP AWS Direct Connect

要使用创建私有 IP VPN， AWS Direct Connect 请按照以下步骤操作。在通过 Direct Connect 创建私有 IP VPN 之前，您需要确保首先创建中转网关和 Direct Connect 网关。在创建这两个网关后，需要在两个网关之间创建关联。下表描述了这些先决条件。在创建并关联这两个网关后，应使用该关联创建 VPN 客户网关和连接。

先决条件

下表描述了通过 Direct Connect 创建私有 IP VPN 之前需要满足的先决条件。

Item	步骤	信息
为 Site-to-Site VPN 准备传输网关。	使用 Amazon Virtual Private Cloud (VPC) 控制台或使用命令行或 API 创建传输网关。 请参阅《Amazon VPC 中转网关指南》中的中转网关。	传输网关是一个网络中转枢纽，可用于将您的网络 VPCs 和本地网络互连。您可以创建新的中转网关，也可以使用现有中转网关来建立私有 IP VPN 连接。在创建中转网关或修改现有中转网关时，可以为连接指定私有 IP CIDR 块。 **Note** 在指定要与私有 IP VPN 关联的中转网关 CIDR 块时，请确保 CIDR 块不会与中转网关上的任何其他网络连接的任何 IP 地址重叠。如果任何 IP CIDR 块发生了重叠，可能会导致客户网关设备出现配置问题。

Item	步骤	信息
为 Site-to-Site VPN 创建 AWS Direct Connect 网关。	使用 Direct Connect 控制台、命令行或 API 创建 Direct Connect 网关。 请参阅《AWS Direct Connect 用户指南》中的创建 AWS Direct Connect 网关。	Direct Connect 网关允许您跨多个 AWS 区域连接虚拟接口 (VIFs)。此网关用于连接到您的 VIF。
为 Site-to-Site VPN 创建传输网关关联。	使用 Direct Connect 控制台、命令行或 API 创建 Direct Connect 网关和中转网关之间的关联。 请参阅《AWS Direct Connect 用户指南》中的关联或取消 AWS Direct Connect 与公交网关的关联。	创建 AWS Direct Connect 网关后，为网关创建中转 AWS Direct Connect 网关联。为之前在允许的前缀列表中确定的中转网关指定私有 IP CIDR。

为 Site-to-Site VPN 创建客户网关和连接

客户网关是您在中创建的资源 AWS。它表示本地网络中的客户网关设备。创建客户网关时，您需要向提供有关您的设备的信息 AWS。有关更多详细信息，请参阅 客户网关。

使用控制台创建客户网关

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择客户网关。
3. 选择创建客户网关。
4. （可选）对于 Name tag（名称标签），为您的客户网关输入名称。这样做可创建具有 Name 键以及您指定的值的标签。
5. 对于 BGP ASN，输入您的客户网关的边界网关协议（BGP）自治系统编号（ASN）。
6. 对于 IP address（IP 地址），输入您的客户网关设备的私有 IP 地址。

> **Important**
>
> 配置 AWS 私有 IP 时 AWS Site-to-Site VPN，必须使用 RFC 1918 地址指定自己的隧道端点 IP 地址。请勿使用 point-to-point IP 地址在您的客户网关路由器和终端节点之间进行 eBGP 对等。 AWS Direct Connect AWS 建议使用客户网关路由器上的环回或 LAN 接口作为源地址或目标地址，而不是 point-to-point连接。
> 有关 RFC 1918 的更多信息，请参阅私有互联网的地址分配。

7. （可选）对于 Device（设备），输入托管此客户网关的设备的名称。
8. 选择创建客户网关。
9. 在导航窗格中，选择 Site-to-Site VPN 连接。
10. 选择创建 VPN 连接。
11. （可选）在名称标签中，输入您的 Site-to-Site VPN 连接的名称。这样做可创建具有 Name 键以及您指定的值的标签。
12. 对于 Target gateway type（目标网关类型），选择 Transit gateway（中转网关）。然后，选择您之前确定的中转网关。
13. 对于 Customer gateway（客户网关），选择 Existing（现有）。然后，选择您之前创建的客户网关。
14. 根据您的客户网关设备是否支持边界网关协议（BGP），选择一个路由选项：
    - 如果您的客户网关设备支持 BGP，请选择动态（需要 BPG）。
    - 如果您的客户网关设备不支持 BGP，请选择静态。
15. 对于 IP 版本内的隧道，指定 VPN 隧道是否支持 IPv4 或 IPv6 流量。
16. （可选）如果您在 IP 版本内指定了隧道，则可以选择为客户网关和允许通过 VPN 隧道进行通信的 AWS 端指定 IPv4 CIDR 范围。IPv4默认值为 `0.0.0.0/0`。

    如果您在 IP 版本内指定IPv6隧道，则可以选择为客户网关和允许通过 VPN 隧道进行通信的 AWS 端指定 IPv6 CIDR 范围。这两个范围的默认值均为 `::/0`。
17. 对于外部 IP 地址类型，请选择 PrivateIpv4。
18. 对于传输附件 ID，请为相应网关选择传输 AWS Direct Connect 网关附件。
19. 选择创建 VPN 连接。

> **Note**
>
> Enable acceleration（启用加速）选项不适用于 AWS Direct Connect上的 VPN 连接。

使用命令行或 API 创建客户网关

- CreateCustomerGateway（亚马逊 EC2 查询 API）
- create-customer-gateway (AWS CLI)

AWS Site-to-Site VPN 中的安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 AWS Site-to-Site VPN 的合规性计划，请参阅AWS 按合规计划划分的范围内AWS 服务按合规计划。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 Site-to-Site VPN 时如何应用分担责任模型。以下主题向您展示如何配置 Site-to-Site VPN 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Site-to-Site VPN 资源。

内容

使用 Secrets Manager 增强 AWS Site-to-Site VPN 安全功能

AWS Site-to-Site VPN 的 Security Rebase 功能提供了增强的安全功能，可让您更好地控制和了解自己的 VPN 连接。一项关键改进是能够将预共享密钥 (PSKs) 存储在 VPN 服务中， AWS Secrets Manager 而不是直接存储在 Site-to-Site VPN 服务中，从而实现更好的机密管理并符合安全最佳实践。该功能还包括一个 `GetActiveVpnTunnelStatus` API，可实时查看活动 VPN 隧道中使用的安全参数，包括两个 IKE 阶段的加密算法、完整性算法和 Diffie-Hellman 组。此外，您现在可以生成推荐的安全配置，通过排除传统选项（例如）来强制使用现代协议 IKEv1。如果您的组织需要保持严格的安全标准，需要对您的VPN配置进行详细的审计跟踪，或者想要确保您的VPN连接使用最安全的可用协议，则这些增强功能特别有价值。

内容

在中更改 Secrets Manager 的预共享密钥 AWS Site-to-Site VPN

如果在 Secrets Manager 中无法访问您的隧道，则可以更改该隧道的预共享密钥。

> **Note**
>
> - 更改预共享密钥时，请确保您拥有两个 Secrets Manager 服务所必需的 IAM 权限。
> - 更改 VPN 隧道的预共享密钥后，连接最多会中断几分钟。确保为预期的停机时间做好计划。

更改 VPN 隧道的 Secrets Manager 预共享密钥

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择 Site-to-Site VPN 连接，然后选择操作、修改 VPN 隧道选项。
4. 对于 VPN 隧道外部 IP 地址，选择 VPN 隧道的隧道端点 IP。
5. 在新的预共享密钥中，选择新的预共享密钥。

   > **Note**
   >
   > 此选项仅适用于存储在 Secrets Manager 中的密钥。

6. 选择保存更改。
7. 对任何其他隧道重复这些步骤。

在中更改预共享密钥存储模式 AWS Site-to-Site VPN

更改现有 VPN 隧道的预共享密钥存储模式。

> **Note**
>
> - 更改存储模式时，请确保您拥有 Site-to-Site VPN 和 Secrets Manager 服务所必需的 IAM 权限。
> - 更改 VPN 隧道的存储模式后，连接最多会中断几分钟。确保为预期的停机时间做好计划。

更改预共享密钥存储模式

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 选择 Site-to-Site VPN 连接，然后选择操作、修改 VPN 隧道选项。
4. 对于 VPN 隧道外部 IP 地址，选择 VPN 隧道的隧道端点 IP。
5. 在 “预共享密钥存储” 下，选择以下预共享密钥存储类型之一。
   - 标准-预共享密钥直接存储在 Site-to-Site VPN 服务中。
   - S@@ ecrets Manager — 使用 AWS Secrets Manager存储预共享密钥。有关 Secrets Manager 的更多信息，请参阅使用 Secrets Manager 增强安全功能。
6. 选择保存更改。

将存储模式从 Secrets Manager 更改为标准存储模式时：

- 预共享密钥将从 Secrets Manager 中移除并移至 Site-to-Site VPN 服务。
- 隧道的条目已从 Secrets Manager 密钥中删除。

将存储模式从标准模式更改为 Secrets Manager 时：

- 预共享密钥已从 Site-to-Site VPN 服务中删除
- 如果一个新的 Secrets Manager 密钥尚不存在，则会创建该密钥。
- 新的预共享密钥存储在 Secrets Manager 中。

AWS Site-to-Site VPN 中的数据保护

分 AWS 担责任模型适用于 AWS Site-to-Site VPN 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API 或 AWS 服务 使用 Site-to-Site VPN 或其他方式时 AWS SDKs。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

互联网络流量隐私

Site-to-SiteVPN 连接以私密方式将您的 VPC 连接到您的本地网络。在 VPC 与您网络之间传输的数据通过加密的 VPN 连接路由，以保护动态数据的机密性和完整性。Amazon 支持互联网协议安全 (IPsec) VPN 连接。 IPsec 是一种协议套件，用于通过对数据流中的每个 IP 数据包进行身份验证和加密来保护 IP 通信。

每个 Site-to-Site VPN 连接都由两条加密的 IPsec VPN 隧道组成， AWS 用于连接您的网络。每个隧道中的流量都可以使用 AES128 或进行加密， AES256 并使用Diffie-Hellman组进行密钥交换，从而提供完美的向前保密。 AWS 使用 SHA1 或 SHA2 哈希函数进行身份验证。

您的 VPC 中的实例不需要公有 IP 地址即可连接到 Site-to-Site VPN 连接另一端的资源。实例可以通过 Site-to-Site VPN 连接将其互联网流量路由到您的本地网络。然后，实例可以通过您的现有出站流量点以及网络安全和监控设备访问 Internet。

请参阅以下主题了解更多信息：

- 您的 AWS Site-to-Site VPN 连接的隧道选项：提供有关每个隧道可用的 IPsec 和互联网密钥交换 (IKE) 选项的信息。
- AWS Site-to-Site VPN 隧道身份验证选项：提供 VPN 隧道端点的身份验证选项的相关信息。
- AWS Site-to-Site VPN 客户网关设备的要求：提供 VPN 连接在您一端的客户网关设备要求的相关信息。
- 使用 VPN 在 AWS Site-to-Site VPN 连接之间进行安全通信 CloudHub：如果您有多个 Site-to-Site VPN 连接，则可以使用 VP AWS N 在本地站点之间提供安全的通信 CloudHub。

AWS Site-to-Site VPN 的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 Site-to-Site VPN 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- AWS Site-to-Site VPN 如何与 IAM 配合使用
- VPN 基于身份的策略示例 AWS Site-to-Site
- AWS Site-to-Site VPN 身份和访问疑难解答
- AWS Site-to-SiteVPN 的托管策略
- 为 Site-to-Site VPN 使用服务相关角色

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Site-to-Site VPN 中所做的工作。

服务用户-如果您使用 Site-to-Site VPN 服务完成工作，则您的管理员会为您提供所需的凭据和权限。当你使用更多的 Site-to-Site VPN 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Site-to-Site VPN 中的某项功能，请参阅AWS Site-to-Site VPN 身份和访问疑难解答。

服务管理员 — 如果您负责公司的 Site-to-Site VPN 资源，则可能拥有对 Site-to-Site VPN 的完全访问权限。您的工作是确定您的服务用户应访问哪些 Site-to-Site VPN 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解贵公司如何将 IAM 与 Site-to-Site VPN 结合使用，请参阅AWS Site-to-Site VPN 如何与 IAM 配合使用。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 Site-to-Site VPN 的访问权限。要查看您可以在 IAM 中使用的基于身份的 Site-to-Site VPN 策略示例，请参阅。VPN 基于身份的策略示例 AWS Site-to-Site

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的AWS 签名版本 4。

无论使用何种身份验证方法，您都可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的 IAM 中的AWS 多重身份验证。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建帐户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 IAM 用户指南中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅 AWS IAM Identity Center 用户指南中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 AWS Management Console，您可以从用户切换到 IAM 角色（控制台）。您可

以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 AWS WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs) — SCPs 是 JSON 策略，用于指定中组织或组织单位 (OU) 的最大权限 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有账户。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

AWS Site-to-Site VPN 如何与 IAM 配合使用

在使用 IAM 管理对 Site-to-Site VPN 的访问之前，请先了解有哪些 IAM 功能可用于 Site-to-Site VPN。

您可以在 AWS Site-to-Site VPN 中使用的 IAM 功能

IAM 特征	Site-to-Site VPN 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACLs	否
ABAC（策略中的标签）	否
临时凭证	是
主体权限	是
服务角色	是
服务相关角色	是

要全面了解 Site-to-Site VPN 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

VPN 基于身份的策略 Site-to-Site

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

VPN 基于身份的策略示例 Site-to-Site

要查看基于 Site-to-Site VPN 身份的策略示例，请参阅。VPN 基于身份的策略示例 AWS Site-to-Site

VPN 中 Site-to-Site基于资源的策略

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

Site-to-SiteVPN 的政策行动

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Site-to-Site VPN 操作列表，请参阅《服务授权参考》中的 AWS Site-to-Site VPN 定义的操作。

Site-to-SiteVPN 中的策略操作在操作前使用以下前缀：

```
ec2
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

要查看基于 Site-to-Site VPN 身份的策略示例，请参阅。VPN 基于身份的策略示例 AWS Site-to-Site

Site-to-SiteVPN 的策略资源

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Site-to-Site VPN 资源类型及其列表 ARNs，请参阅《服务授权参考》中的 AWS Site-to-Site VPN 定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 VPN 定义的 AWS Site-to-Site 操作。

要查看基于 Site-to-Site VPN 身份的策略示例，请参阅。VPN 基于身份的策略示例 AWS Site-to-Site

Site-to-SiteVPN 的策略条件密钥

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Site-to-Site VPN 条件密钥列表，请参阅《服务授权参考》中的 AWS Site-to-Site VPN 条件密钥。要了解可以使用条件密钥的操作和资源，请参阅 AWS Site-to-Site VPN 定义的操作。

要查看基于 Site-to-Site VPN 身份的策略示例，请参阅。VPN 基于身份的策略示例 AWS Site-to-Site

ACLs 在 Site-to-Site VPN 中

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

带有 VPN 的 ABA Site-to-Site C

支持 ABAC（策略中的标签）：否

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）和许多 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

在 Site-to-Site VPN 中使用临时证书

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

VPN 的跨服务主体 Site-to-Site权限

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Site-to-SiteVPN 的服务角色

支持服务角色：是

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 Site-to-Site VPN 功能。仅当 Site-to-Site VPN 提供相关指导时才编辑服务角色。

VPN 的 Site-to-Site服务相关角色

支持服务相关角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的AWS 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

VPN 基于身份的策略示例 AWS Site-to-Site

默认情况下，用户和角色无权创建或修改 Site-to-Site VPN 资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 Site-to-Site VPN 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》中的 AWS Site-to-Site VPN 操作、资源和条件密钥。 ARNs

主题

- 策略最佳实践
- 使用 Site-to-Site VPN 控制台
- 描述特定的 Site-to-Site VPN 连接
- 创建和描述 AWS Site-to-Site VPN 连接所需的资源

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 Site-to-Site VPN 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管式策略或工作职能的AWS 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 Site-to-Site VPN 控制台

要访问 AWS Site-to-Site VPN 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 Site-to-Site VPN 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Site-to-Site VPN 控制台，还要将 Site-to-Site VPN `AmazonVPCFullAccess` 或`AmazonVPCReadOnlyAccess` AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

描述特定的 Site-to-Site VPN 连接

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpnConnections"
         ],
         "Resource": ["*"]
      }
   ]
}
```

创建和描述 AWS Site-to-Site VPN 连接所需的资源

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
         "ec2:DescribeVpnConnections",
         "ec2:DescribeVpnGateways",
         "ec2:DescribeCustomerGateways",
         "ec2:CreateCustomerGateway",
         "ec2:CreateVpnGateway",
         "ec2:CreateVpnConnection"
         ],
         "Resource": [
            "*"
         ]
      },
   {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/s2svpn.amazonaws.com/
AWSServiceRoleForVPCS2SVPNInternal",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName":"s2svpn.amazonaws.com"
            }
```

```
        }
      }
   ]
}
```

AWS Site-to-Site VPN 身份和访问疑难解答

使用以下信息来帮助您诊断和修复在使用 Site-to-Site VPN 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Site-to-Site VPN 中执行操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人 AWS 账户 访问我的 Site-to-Site VPN 资源

我无权在 Site-to-Site VPN 中执行操作

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 ec2:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 ec2:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到错误消息，提示您无权执行iam:PassRole操作，则必须更新您的策略以允许您将角色传递给 Site-to-Site VPN。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户marymajor尝试使用控制台在 Site-to-Site VPN 中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 Site-to-Site VPN 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Site-to-Site VPN 是否支持这些功能，请参阅AWS Site-to-Site VPN 如何与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

AWS Site-to-SiteVPN 的托管策略

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些政策涵盖常见用例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管式策略添加额外权限以支持新特征。此类更新会影响附加策略的所有身份（用户、组和角色）。当启

动新特征或新操作可用时，服务最有可能会更新 AWS 托管式策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，`ReadOnlyAccess` AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动一项新功能时， AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的AWS 托管式策略。

AWS 托管策略： AWSVPCS2SVpnServiceRolePolicy

您可以将 `AWSVPCS2SVpnServiceRolePolicy` 策略附加到 IAM 身份。此策略允许 Site-to-Site VPN 管理 V Site-to-Site PN 中的 AWS Secrets Manager 密钥。有关更多信息，请参阅 the section called “使用服务相关角色”。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AWSVPCS2SVpnServiceRolePolicy。

Site-to-Site AWS 托管策略的 VPN 更新

查看自该服务于 2025 年 5 月开始追踪 Site-to-Site VPN AWS 托管政策变更以来这些更新的详细信息。

更改	描述	日期
AWSVPCS2SVpnServiceRolePolicy-更新了政策。	策略中添加了新的权限，允许 Site-to-Site VPN 管理 VPN 连接的 AWS Secrets Manager `s2svpn`托管密钥。	2025 年 5 月 14 日

为 Site-to-Site VPN 使用服务相关角色

AWS Site-to-Site VPN 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色，直接关联到 Site-to-Site VPN。服务相关角色由 Site-to-Site VPN 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置 Site-to-Site VPN 变得更加容易，因为您不必手动添加必要的权限。 Site-to-SiteVPN 定义其服务相关角色的权限，除非另有定义，否则只有 Site-to-Site VPN 可以担任其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在首先删除相关资源后，您才能删除服务相关角色。这样可以保护您的 Site-to-Site VPN 资源，因为您不会无意中删除访问这些资源的权限。

VPN 的服务相关角色权限 Site-to-Site

Site-to-Site VPN 使用名为 AWSServiceRoleForVPCS2SVPN 的服务相关角色——允许 Site-to-Site VPN 创建和管理与您的 VPN 连接相关的资源。

S AWSService RoleFor VPCS2 VPN 服务相关角色信任以下服务来代入该角色：

- `s2svpn.amazonaws.com`

此服务相关角色使用托管策略 AWSVPCS2SVpnServiceRolePolicy 对指定资源完成以下操作：

- 在 VPN 连接中使用证书身份验证时，请 AWS Site-to-Site VPN 导出 VPN 隧道 AWS Certificate Manager 证书以在 VPN 隧道端点上使用。
- 在 VPN 连接中使用证书身份验证时， AWS Site-to-Site VPN 管理 VPN 隧道 AWS Certificate Manager 证书的续订。
- 在 VPN 连接中使用 SecretsManager 预共享密钥存储时， AWS Site-to-Site VPN 管理 VPN 连接的 AWS Secrets Manager s2svpn 托管密钥。

要查看此策略的权限，请参阅《AWS 托管式策略参考》中的 AWSVPCS2SVpnServiceRolePolicy。

为 VPN 创建服务相关角色 Site-to-Site

您无需手动创建服务相关角色。当您在 AWS Management Console、或 AWS API 中创建带有关联的 ACM 私有证书的客户网关时 AWS CLI， Site-to-SiteVPN 会为您创建服务相关角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您使用关联的 ACM 私有证书创建客户网关时， Site-to-SiteVPN 会再次为您创建服务相关角色。

编辑 VPN 的服务相关角色 Site-to-Site

Site-to-Site VPN 不允许您编辑 AWSService RoleFor VPCS2 SVPN 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色描述。

删除 VPN 的服务相关角色 Site-to-Site

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果您尝试删除资源时 Site-to-Site VPN 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 S Site-to-Site VPN 使用的 AWSService RoleFor VPCS2 VPN 资源

只有在删除具有关联 ACM 私有证书的所有客户网关之后，您才能删除此服务相关角色。这样可以确保您不会无意中移除 VPN 连接正在使用的 ACM 证书的访问权限。 Site-to-Site

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSService RoleFor VPCS2 SVPN 服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

韧性在 AWS Site-to-Site VPN

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础结构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础设施外， Site-to-SiteVPN 还提供多种功能来帮助支持您的数据弹性和备份需求。

每个 VPN 连接两条隧道

Site-to-SiteVPN 连接由两条隧道组成，每条隧道终止于不同的可用区，以提高您的 VPC 的可用性。如果里面有设备故障 AWS，你的 VPN 连接会自动故障转移到第二条隧道，这样你的访问就不会中断。AWS 还会不时对您的 VPN 连接进行例行维护，这可能会短暂禁用 VPN 连接的两个隧道中的一个。有关更多信息，请参阅 AWS Site-to-Site VPN 隧道端点替换。因此，在您配置客户网关时，务必配置这两条隧道。

冗余

为了在您的客户网关不可用时防止连接中断，您可以设置第二个 Site-to-Site VPN 连接。有关更多信息，请参阅以下文档：

- 用于故障转移的冗余 AWS Site-to-Site VPN 连接
- Amazon Virtual Private Cloud Connectivity Options
- 构建可扩展且安全的多 vPC AWS 网络基础架构

AWS Site-to-Site VPN 中的基础设施安全

作为一项托管服务， AWS Site-to-Site VPN 受到 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Site-to-Site VPN。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

监控 AWS Site-to-Site VPN 连接

监控是维护 AWS Site-to-Site VPN 连接的可靠性、可用性和性能的重要组成部分。您应从 解决方案的所有部分收集监控数据，以便更轻松地调试出现的多点故障。但是，在开始监控 Site-to-Site VPN 连接之前，您应该制定一份包含以下问题答案的监控计划：

- 监控目的是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

下一步，通过在不同时间和不同负载条件下测量性能，在您的环境中建立正常 VPN 性能的基准。监控 VPN 时，将历史监控数据存储起来，以便可以与当前性能数据进行比较，确定正常性能模式和异常性能表现，并设计出问题解决方法。

要建立基准，您应监控以下各项：

- 您的 VPN 隧道的状态
- 传入隧道中的数据
- 从隧道传出的数据

主题

监控工具

AWS 提供了可用于监控 Site-to-Site VPN 连接的各种工具。您可以配置其中的一些工具来为您执行监控任务，但有些工具需要手动干预。建议您尽可能实现监控任务自动化。

自动监控工具

您可以使用以下自动监控工具来监视 Site-to-Site VPN 连接并在出现问题时进行报告：

- A CloudWatch mazon Alarms — 在您指定的时间段内观察单个指标，并根据该指标在多个时间段内相对于给定阈值的值执行一项或多项操作。该操作是发送给 Amazon SNS 主题的通知。CloudWatch 警报不会仅仅因为它们处于特定状态就调用操作；该状态必须已更改并保持了指定的时间段。有关更多信息，请参阅 使用 Amazon 监控 AWS Site-to-Site VPN 隧道 CloudWatch。
- AWS CloudTrail 日志监控-在账户之间共享日志文件，通过将 CloudTrail 日志文件发送到 “日志” 来实时监控 CloudWatch 日志文件，用 Java 编写日志处理应用程序，并验证您的日志文件在传送后是否未更改 CloudTrail。有关更多信息，请参阅《Amazon API 参考》 AWS CloudTrail中的 “使用记录 EC2 API 调用” 和 “AWS CloudTrail 用户指南” 中的 “使用 CloudTrail 日志文件”。
- AWS Health 事件-接收与 Site-to-Site VPN 隧道运行状况变化、最佳实践配置建议或接近扩展限制时相关的警报和通知。使用 Personal Health Dashboard 上的事件来触发自动失效转移、缩短故障排除时间或优化连接以实现高可用性。有关更多信息，请参阅 AWS Health 和 AWS Site-to-Site VPN 事件。

手动监控工具

监控 Site-to-Site VPN 连接的另一个重要部分是手动监控 CloudWatch 警报未涵盖的项目。Amazon VPC 和 CloudWatch 控制台控制面板提供您的 AWS 环境状态 at-a-glance视图。

> **Note**
>
> 在 Amazon VPC 控制台中， Site-to-SiteVPN 隧道状态参数（例如 “状态” 和 “上次状态更改”）可能无法反映瞬态状态变化或隧道瞬间抖动。建议使用 CloudWatch 指标和日志进行精细的隧道状态更改更新。

- Amazon VPC 控制面板显示：
  - 服务运行状况（按区域）
  - Site-to-Site VPN 连接
  - VPN 隧道状态（在导航窗格中，选择 Site-to-Site VPN 连接，选择 Site-to-Site VPN 连接，然后选择隧道详细信息）
- CloudWatch 主页显示：
  - 当前告警和状态

- 告警和资源图表
- 服务运行状况

此外，您还可以使用 CloudWatch 执行以下操作：

- 创建自定义控制面板以监控您关心的服务
- 绘制指标数据图，以排除问题并弄清楚趋势
- 搜索和浏览您的所有 AWS 资源指标
- 创建和编辑告警以接收问题通知

AWS Site-to-Site VPN 日志

AWS Site-to-Site VPN 日志可让您更深入地了解 Site-to-Site VPN 部署。使用此功能，您可以访问 Site-to-Site VPN 连接日志，这些日志提供有关 IP 安全 (IPsec) 隧道建立、互联网密钥交换 (IKE) 协商和失效对等体检测 (DPD) 协议消息的详细信息。

Site-to-Site VPN 日志可以发布到 Amazon CloudWatch 日志。此功能为客户提供了一种统一的方式来访问和分析其所有 Site-to-Site VPN 连接的详细日志。

主题

Site-to-SiteVPN 日志的好处

- 简化的 VP Site-to-Site N 故障排除：VPN 日志可帮助您查明与您的客户网关设备之间的 AWS 配置不匹配情况，并解决初始 VPN 连接问题。VPN 连接可能由于设置配置错误（例如超时调整不当）而随时间推移发生间歇性抖动，底层传输网络中可能存在问题（例如互联网天气），或者路由更改或路径故障可能导致通过 VPN 的连接中断。此功能可让您准确地诊断间歇性连接故障的原因，并微调低级别隧道配置以实现可靠运行。

- 集中 AWS Site-to-Site VPN 可见性： Site-to-SiteVPN 日志可以提供 VP Site-to-Site N 连接的所有不同方式的隧道活动日志：虚拟网关、Transit Gateway CloudHub，以及同时使用互联网和 AWS Direct Connect 作为传输方式。此功能为客户提供了一种统一的方式来访问和分析其所有 Site-to-Site VPN 连接的详细日志。
- 安全与合规：可以将 Site-to-Site VPN 日志发送到 Amazon CloudWatch Logs，以便对一段时间内的 VPN 连接状态和活动进行回顾性分析。这可以帮助您满足合规性和法规要求。

Amaz CloudWatch on Logs 资源策略大小限制

CloudWatch 日志资源策略限制为 5120 个字符。当 CloudWatch Logs 检测到策略接近此大小限制时，它会自动启用以开头的日志组`/aws/vendedlogs/`。启用日志记录后， Site-to-SiteVPN 必须使用您指定的日志组更新您的 CloudWatch 日志资源策略。为避免达到 CloudWatch 日志资源策略大小限制，请在日志组名称前加上`/aws/vendedlogs/`。

Site-to-Site VPN 日志内容

Site-to-SiteVPN 隧道活动日志中包含以下信息。日志流文件名使用 VpnConnection ID 和 TunnelOutsideIPAddress。

字段	描述
VpnLogCreationTimestamp (`event_timestamp`)	日志创建时间戳，采用用户可读格式。
隧道 DPDEnabled (`dpd_enabled`)	失效对端检测协议启用状态（True/False）。
隧道CGWNATTDetection状态 (`nat_t_detected`)	在客户网关设备上检测到 NAT-T（True/False）。
隧道IKEPhase1状态 (`ike_phase1_state`)	IKE 第 1 阶段协议状态（已建立 | 正在重新生成密钥 | 正在协商 | 关闭）。
隧道IKEPhase2状态 (`ike_phase2_state`)	IKE 第 2 阶段协议状态（已建立 | 正在重新生成密钥 | 正在协商 | 关闭）。
VpnLogDetail (`details`)	IKE 和 DPD IPsec 协议的详细消息。

内容

IKEv1 错误消息

消息	说明
对等方无响应 - 宣布对等方终止	对等方未响应 DPD 消息，强制执行 DPD 超时操作。
AWS 由于预共享密钥无效，隧道有效载荷解密失败	需要在两个 IKE 对等方上配置相同的预共享密钥。
未找到与之匹配的提案 AWS	AWS VPN 端点（例如 3DES）不支持第 1 阶段（加密、哈希和 DH 组）的提议属性。
未找到匹配的提案。使用“No proposal chosen”（未选择任何提案）进行通知	在对等方之间交换“No proposal chosen”（未选择任何提案）错误消息，以告知必须在 IKE 对等方上为第 2 阶段配置正确的提案/策略。
AWS 带有 SPI 的第 2 阶段 SA 的隧道已收到删除:xxxx	CGW 已发送第 2 阶段的 delete_SA 消息。
AWS 隧道收到了来自 CGW 的 IKE_SA 的 DELETE	CGW 已发送第 1 阶段的 delete_SA 消息。

IKEv2 错误消息

消息	说明
AWS 隧道 DPD 在 {retry_count} 重新传输后超时	对等方未响应 DPD 消息，强制执行 DPD 超时操作。
AWS 隧道收到了来自 CGW 的 IKE_SA 的 DELETE	Peer 已向 Parent/IKE_SA 发送了 delete_SA 消息。

消息	说明
AWS 带有 SPI 的第 2 阶段 SA 的隧道已收到删除:xxxx	Peer 已为 CHILD_SA 发送了 Delete_SA 消息。
AWS 隧道检测到 (CHILD_REKEY) 冲突为 CHILD_DELETE	CGW 已为活动 SA 发送了 Delete_SA 消息，目前正在更改密钥。
AWS 由于检测到冲突，正在删除隧道 (CHILD_SA) 冗余 SA	由于冲突，如果生成冗余 SAs ，Peer 节点将在按照 RFC 匹配随机数值后关闭冗余 SA。
AWS 隧道第 2 阶段在保持第 1 阶段时无法建立	由于协商错误（例如提议不正确），对等方无法建立 CHILD_SA。
AWS：流量选择器：TS_UNACCEPTABLE：接收自响应方	对等方提议了错误的流量选择器/加密域。Peer 节点的配置应完全相同且正确 CIDRs。
AWS 隧道正在发送身份验证_失败作为响应	对等方无法通过验证 IKE_AUTH 消息的内容来对对等方进行身份验证
AWS 隧道检测到与 cgw 的预共享密钥不匹配 :xxxx	需要在两个 IKE 对等方上配置相同的预共享密钥。
AWS 隧道超时：使用 cgw 删除未建立的第 1 阶段 IKE_SA: xxxx	以对等方身份删除半打开的 IKE_SA 尚未开始协商
未找到匹配的提案。使用“No proposal chosen”（未选择任何提案）进行通知	在对等方之间交换“No proposal chosen”（未选择任何提案）错误消息，以告知必须在 IKE 对等方上配置正确的提案。
未找到与之匹配的提案 AWS	AWS VPN Endpoint 不支持第 1 阶段或第 2 阶段（加密、哈希和 DH 组）的建议属性，3DES例如。

IKEv2 谈判消息

消息	说明
AWS CREATE_CHILD_SA 的隧道处理请求 (id=xxx)	AWS 已收到来自 CGW 的 CREATE_CHILD_SA 请求。
AWS 隧道正在发送 CREATE_CHILD_SA 的响应 (id=xxx)	AWS 正在向 CGW 发送 CREATE_CHILD_SA 响应。
AWS 隧道正在发送 CREATE_CHILD_SA 的请求 (id=xxx)	AWS 正在向 CGW 发送 CREATE_CHILD_SA 请求。
AWS CREATE_CHILD_SA 的隧道处理响应 (id=xxx)	AWS 已收到来自 CGW 的 CREATE_CHILD_SA 回复。

发布到 CloudWatch 日志的 IAM 要求

为了使日志记录功能正常运行，附加到用于配置该功能的 IAM 主体的 IAM policy 必须至少包含以下权限。更多详情也可以在《Amazon L og CloudWatch s 用户指南》的 “启用某些 AWS 服务的日志记录” 部分中找到。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "S2SVPNLogging"
    },
```

```
    {
      "Sid": "S2SVPNLoggingCWL",
      "Action": [
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

查看 AWS Site-to-Site VPN 日志配置

查看 Site-to-Site VPN 连接的活动日志。在这里，您可以查看有关配置的详细信息，例如加密算法或者是否已启用隧道 VPN 日志。还可以查看隧道状态。这有助于更好地跟踪 VPN 连接可能遇到的任何问题或冲突。

查看当前隧道日志记录设置

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 从 VPN connections（VPN 连接）列表中选择要查看的 VPN 连接。
4. 选择 Tunnel details（隧道详细信息）选项卡。
5. 展开 Tunnel 1 options（隧道 1 选项）和 Tunnel 2 options（隧道 2 选项）部分，以查看所有隧道配置详细信息。
6. 您可以在 Tunn el VPN 日志下查看日志功能的当前状态，也可以在 CloudWatch日志组下查看当前配置的CloudWatch 日志组（如果有）。

使用 AWS 命令行或 API 查看 Site-to-Site VPN 连接上的当前隧道日志记录设置

- DescribeVpnConnections（亚马逊 EC2 查询 API）
- describe-vpn-connections (AWS CLI)

启用 AWS Site-to-Site VPN 日志

启用 Site-to-Site VPN 日志以记录 VPN 活动，例如隧道状态和其他详细信息。您可以对新连接启用日志记录功能，也可以修改现有连接以开始日志记录活动。如果您希望对连接禁用日志记录，请参阅禁用 Site-to-Site VPN 日志。

> **Note**
>
> 当您为现有 Site-to-Site VPN 连接隧道启用 VPN 日志时，该隧道上的连接可能会中断几分钟。但是，每个 VPN 连接都提供两条隧道以实现高可用性，因此，您可以一次对一条隧道启用日志记录，同时保持通过此隧道的连接不被修改。有关更多信息，请参阅 AWS Site-to-Site VPN 隧道端点替换。

在创建新 VPN 连接期间启用 Site-to-Site VPN 日志记录

按照步骤 5：创建 VPN 连接过程操作。在步骤 9 Tunnel Options（隧道选项）期间，您可以指定要用于这两条隧道的所有选项，包括 VPN logging（VPN 日志记录）选项。有关这些选项的详细信息，请参阅您的 AWS Site-to-Site VPN 连接的隧道选项。

使用 AWS 命令行或 API 在新 Site-to-Site VPN 连接上启用隧道日志记录

- CreateVpnConnection（亚马逊 EC2 查询 API）
- create-vpn-connection (AWS CLI)

在现有 Site-to-Site VPN 连接上启用隧道日志记录

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN 连接。
3. 从 VPN connections（VPN 连接）列表中选择要修改的 VPN 连接。
4. 依次选择 Actions（操作）、Modify VPN tunnel options（修改 VPN 隧道选项）。
5. 通过从 VPN tunnel outside IP address（VPN 隧道外部 IP 地址）列表中选择适当的 IP 地址，选择要修改的隧道。
6. 在 Tunnel activity log（隧道活动日志）下，选择 Enable（启用）。
7. 在 Amazon CloudWatch 日志组下，选择要将日志发送到的亚马逊 CloudWatch 日志组。
8. （可选）在 Output format（输出格式）下，选择日志输出的所需格式：json 或 text（文本）。
9. 选择 Save changes（保存更改）。

10. （可选）如果需要，对其它隧道重复步骤 4 到 9。

使用 AWS 命令行或 API 在现有 Site-to-Site VPN 连接上启用隧道日志记录

- ModifyVpnTunnelOptions（亚马逊 EC2 查询 API）
- modify-vpn-tunnel-options (AWS CLI)

禁用 AWS Site-to-Site VPN 日志

如果您不再希望跟踪某个连接上的任何活动，请对该连接禁用 VPN 日志记录。此操作仅禁用日志记录，不会影响该连接的任何其他活动。要对连接启用或重新启用日志记录，请参阅启用 Site-to-Site VPN 日志。

在 Site-to-Site VPN 连接上禁用隧道日志记录

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 Site-to-Site VPN Connections。
3. 从 VPN connections（VPN 连接）列表中选择要修改的 VPN 连接。
4. 依次选择 Actions（操作）、Modify VPN tunnel options（修改 VPN 隧道选项）。
5. 通过从 VPN tunnel outside IP address（VPN 隧道外部 IP 地址）列表中选择适当的 IP 地址，选择要修改的隧道。
6. 在 Tunnel activity log（隧道活动日志）下，清除 Enable（启用）。
7. 选择 Save changes（保存更改）。
8. （可选）如果需要，对其它隧道重复步骤 4 到 7。

使用 AWS 命令行或 API 禁用 Site-to-Site VPN 连接上的隧道日志记录

- ModifyVpnTunnelOptions（亚马逊 EC2 查询 API）
- modify-vpn-tunnel-options (AWS CLI)

使用 Amazon 监控 AWS Site-to-Site VPN 隧道 CloudWatch

您可以使用监控 VPN 隧道 CloudWatch，它收集来自 VPN 服务的原始数据并将其处理为可读的近乎实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。VPN 指标数据可用 CloudWatch 时会自动发送到。

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

内容

VPN 指标和维度

以下 CloudWatch 指标可用于您的 Site-to-Site VPN 连接。

指标	描述
TunnelState	隧道的状态。对于静态 VPNs，0 表示向下，1 表示向上。对于 BGP VPNs，1 表示已建立，0 表示所有其他状态。对于这两种类型 VPNs，介于 0 和 1 之间的值表示至少有一条隧道未开启。 单位：介于 0 和 1 之间的小数值
TunnelDataIn †	连接 AWS 侧通过 VPN 隧道从客户网关接收的字节。每个指标数据点代表在前一数据点后接收的字节数。使用 Sum 统计数据显示在此期间收到的总字节数。 该指标对解密后的数据进行计数。 单位：字节
TunnelDataOut †	从连接 AWS 侧通过 VPN 隧道发送到客户网关的字节。每个指标数据点代表在前一数据点后发送的字节数。使用 Sum 统计数据显示在此期间发送的总字节数。 该指标对加密前的数据进行计数。 单位：字节

† 即使隧道关闭，这些指标也可以报告网络使用情况。这是因为系统会定期检查隧道状态，以及后台 ARP 和 BGP 请求。

要筛选指标数据，请使用以下维度。

维度	描述
VpnId	按 Site-to-Site VPN 连接 ID 筛选指标数据。
TunnelIpAddress	按虚拟专用网关隧道的 IP 地址筛选指标数据。

查看 Amazon CloudWatch Logs 的指标 AWS Site-to-Site VPN

当您创建 Site-to-Site VPN 连接时，VPN 服务会在可用时向其 CloudWatch发送有关您的 VPN 连接的指标。您可以按如下方式查看 VPN 连接的指标。

使用 CloudWatch 控制台查看指标

指标的分组首先依据服务命名空间，然后依据每个命名空间内的各种维度组合。

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择指标。
3. 在 All metrics 下，选择 VPN 指标命名空间。
4. 选择指标维度以查看指标（例如，VPN 隧道指标）。

> **Note**
>
> 在您正在查看的 AWS 区域中创建 Site-to-Site VPN 连接后，VPN 命名空间才会出现在 CloudWatch 控制台中。

要查看指标，请使用 AWS CLI

在命令提示符处输入下面的命令：

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

创建 Amazon CloudWatch 警报以监控 AWS Site-to-Site VPN 隧道

您可以创建一个 CloudWatch 警报，当警报状态发生变化时，该警报会发送 Amazon SNS 消息。警报会每隔一段时间（间隔由您指定）监控一个指标，并根据指标值与给定阈值的相对关系每隔若干个时间段向 Amazon SNS 主题发送一个通知。

例如，您可以创建警报来监控单个 VPN 隧道的状态，并在隧道状态在 15 分钟内的 3 个数据点为 DOWN 时发送通知。

创建单个隧道状态的警报

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，展开警报，然后选择所有警报。
3. 选择创建警报，然后选择选择指标。
4. 选择 VPN，然后选择 VPN 隧道指标。
5. 选择所需隧道的 IP 地址，与TunnelState指标位于同一行。选择选择指标。
6. 因为无论何时 TunnelState 是... ，选择 L ow er，然后在 th an... 下的输入字段中输入 “1” 。
7. 在其他配置下，对于要发出警报的数据点，将输入设置为“三取三”。
8. 选择下一步。
9. 在向以下 SNS 主题发送通知下，选择一个现有的通知列表或创建一个新的通知列表。
10. 选择下一步。
11. 输入警报的名称。选择下一步。
12. 检查警报的设置，然后选择创建警报。

您可以创建监控 Site-to-Site VPN 连接状态的警报。例如，您可以创建一个警报，以在一条或两条隧道的状态在一个 5 分钟的时段内为 DOWN 时发送通知。

为 Site-to-Site VPN 连接状态创建警报

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，展开警报，然后选择所有警报。
3. 选择创建警报，然后选择选择指标。
4. 选择 VPN，然后选择 VPN 连接指标。
5. 选择您的 Site-to-Site VPN 连接和TunnelState指标。选择选择指标。
6. 对于统计数据，指定最大。

或者，如果您已将 Site-to-Site VPN 连接配置为两条隧道都处于开启状态，则可以将统计数据指定为 “最小”，以便在至少一条隧道关闭时发送通知。

7. 对于 Whenever（每当），选择 Lower/Equal（小于/等于，(<=)）并输入 0（或当至少有一个隧道处于关闭状态时，为 0.5）。选择 Next (下一步)。
8. 在选择 SNS 主题下，选择现有通知列表或选择新建列表，创建一个新列表。选择下一步。
9. 为您的警报输入名称和描述。选择下一步。
10. 检查警报的设置，然后选择创建警报。

您还可以创建警报来监控进入或离开 VPN 隧道的流量。例如，下面的警报监控从您的网络进入 VPN 隧道的流量，当字节数在 15 分钟内达到阈值 5000000 时发送通知。

创建传入网络流量警报

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，展开警报，然后选择所有警报。
3. 选择创建警报，然后选择选择指标。
4. 选择 VPN，然后选择 VPN 隧道指标。
5. 选择 VPN 隧道的 IP 地址和TunnelDataIn指标。选择选择指标。
6. 对于统计数据，指定总和。
7. 对于时段，选择 15 分钟。
8. 对于 Whenever（每当），选择 Greater/Equal（大于/等于，>=），然后输入 5000000。选择下一步。
9. 在选择 SNS 主题下，选择现有通知列表或选择新建列表，创建一个新列表。选择下一步。
10. 为您的警报输入名称和描述。选择下一步。
11. 检查警报的设置，然后选择创建警报。

下面的警报监控离开 VPN 隧道进入您的网络的流量，当字节数在 15 分钟内少于 1000000 时发送通知。

创建传出网络流量警报

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，展开警报，然后选择所有警报。

3. 选择创建警报，然后选择选择指标。
4. 选择 VPN，然后选择 VPN 隧道指标。
5. 选择 VPN 隧道的 IP 地址和TunnelDataOut指标。选择选择指标。
6. 对于统计数据，指定总和。
7. 对于时段，选择 15 分钟。
8. 对于每当，选择小于/等于 (<=)，然后输入 1000000。选择下一步。
9. 在选择 SNS 主题下，选择现有通知列表或选择新建列表，创建一个新列表。选择下一步。
10. 为您的警报输入名称和描述。选择下一步。
11. 检查警报的设置，然后选择创建警报。

有关创建警报的更多示例，请参阅亚马逊 CloudWatch 用户指南中的创建亚马逊 CloudWatch 警报。

AWS Health 和 AWS Site-to-Site VPN 事件

AWS Site-to-Site VPN 自动向. 发送通知AWS Health Dashboard。此仪表板无需设置，可供经过身份验证的 AWS 用户使用。您可以通过 AWS Health Dashboard配置多个操作来响应事件通知。

AWS Health Dashboard 为您的 VPN 连接提供以下类型的通知：

- 隧道端点替换通知
- 单隧道 VPN 通知

隧道端点替换通知

当您的 VPN 连接中的一个或两个 VPN 隧道端点被替换 AWS Health Dashboard 时，您会收到隧道端点更换通知。当 AWS 执行隧道更新时或当您修改 VPN 连接时，会替换隧道端点。有关更多信息，请参阅 AWS Site-to-Site VPN 隧道端点替换。

隧道端点替换完成后，通过 AWS Health Dashboard 事件 AWS 发送隧道端点替换通知。

单隧道 VPN 通知

Site-to-SiteVPN 连接由两条用于冗余的隧道组成。我们强烈建议您配置两个隧道以实现高可用性。如果您的 VPN 连接有一个隧道开启，但另一个隧道每天关闭超过一个小时，您将通过 AWS Health Dashboard 事件收到每月 的 VPN single tunnel notification（VPN 单隧道通知）。此事件将每天更

新，检测到的任何新 VPN 连接均为单一隧道，每周发送通知。每个月都会创建一个新事件，该事件将清除所有不再被检测为单一隧道的 VPN 连接。

AWS Site-to-Site VPN 配额

您的 AWS 账户具有以下与 Site-to-Site VPN 相关的配额（以前称为限制）。除非另有说明，否则，每个限额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。

要请求增加可调配额，请选择 Adjustable（可调）列中的 Yes（是）。有关更多信息，请参阅《Service Quotas 用户指南》中的请求增加配额。

Site-to-Site VPN 资源

名称	默认值	可调整
每个区域的客户网关数	50	是
每个区域的虚拟私有网关数	5	是
Site-to-Site 每个区域的 VPN 连接数	50	是
Site-to-Site 每个虚拟专用网关的 VPN 连接数	10	是
每个区域的加速 Site-to-Site VPN 连接数	10	是
每个区域的未关联 Site-to-Site的 VPN 连接	10	是

> **Note**
>
> 加速连接和非关联连接均计入每个区域的 Site-to-Site VPN 连接总配额。

您一次能将一个虚拟专用网关连接到 VPC。要将同一 Site-to-Site VPN 连接连接到多个 VPN 连接 VPCs，我们建议您改用中转网关进行探索。有关更多信息，请参阅 Amazon VPC 中转网关 中的中转网关。

Site-to-Site 传输网关上的 VPN 连接受传输网关连接总数限制的约束。有关更多信息，请参阅 Transit Gateway 配额。

路线

通告的路由源包括 VPC 路由、其他 VPN 路由和来自 AWS Direct Connect 虚拟接口的路由。通告的路由来自与 VPN 挂载关联的路由表。

> **Note**
>
> 如果您使用的是虚拟专用网关，并且在您的 VPC 路由表上启用了路由传播，则会自动为您的 VPN 连接添加动态和静态路由，但不超过 VPC 路由表的限制。有关更多详细信息，请参阅《Amazon VPC 用户指南》中的 Amazon VPC 限额。

名称	默认值	可调整
从客户网关设备通告到虚拟专用网关上的 Site-to-Site VPN 连接的动态路由	100	否
从虚拟专用网关上的 Site-to-Site VPN 连接通告到客户网关设备的路由	1000	否
从客户网关设备通告到中转网关上的 Site-to-Site VPN 连接的动态路由	1000	否
从中转网关上的 Site-to-Site VPN 连接通告到客户网关设备的路由	5000	否
从客户网关设备到虚拟专用网关上的 Site-to-Site VPN 连接的静态路由	100	否

带宽和吞吐量

有许多因素会影响通过 Site-to-Site VPN 连接实现的带宽，包括但不限于：数据包大小、流量组合 (TCP/UDP)、中间网络的整形或限制策略、互联网天气以及特定的应用程序要求。

名称	默认值	可调整
每个 VPN 隧道的最大带宽	最高 1.25 Gbps	否

名称	默认值	可调整
每个 VPN 隧道的最大每秒数据包数 (PPS)	最高 14 万	否

对于传输网关上的 Site-to-Site VPN 连接，您可以使用 ECMP 通过聚合多个 VPN 隧道来获得更高的 VPN 带宽。要使用 ECMP，必须配置 VPN 连接以进行动态路由。在使用静态路由的 VPN 连接上不支持 ECMP。有关更多信息，请参阅中转网关。

最大传输单元 (MTU)

Site-to-Site VPN 支持的最大传输单元 (MTU) 为 1446 字节，相应的最大分段大小 (MSS) 为 1406 字节。但某些使用较大 TCP 报头的算法可能会实际上降低该最大值。为避免碎片化，我们建议您根据选择的算法设置 MTU 和 MSS。有关 MTU、MSS 和最佳值的更多详细信息，请参阅AWS Site-to-Site VPN 客户网关设备的最佳实践。

不支持巨型帧。有关更多信息，请参阅 Amazon EC2 用户指南中的巨型帧。

Site-to-SiteVPN 连接不支持路径 MTU 发现。

其他配额资源

有关与中转网关相关的配额，包括中转网关上的挂载数量，请参阅 Amazon VPC 中转网关指南 中的中转网关的配额。

有关其他 VPC 配额，请参阅 Amazon VPC 用户指南 中的 Amazon VPC 配额。

Site-to-SiteVPN 用户指南的文档历史记录

下表描述了《 AWS Site-to-Site VPN 用户指南》的更新。

变更	说明	日期
更新了 AWSVPCS2S VpnServiceRolePolicy AWS 托管策略	向 AWS 托管策略添加了新的权限，允许 Site-to-Site VPN 管理 VPN 连接的 AWS Secrets Manager 托管密钥。	2025 年 5 月 27 日
更新了预共享密钥存储选项	Site-to-Site VPN 现在 AWS Secrets Manager 支持存储预共享密钥。	2025 年 5 月 27 日
已删除 Classic VPN 信息	从指南中删除了有关 Classic VPN 的信息。	2023 年 1 月 19 日
VPN 日志示例消息	为 Site-to-Site VPN 连接添加了示例日志。	2022 年 12 月 9 日
更新了下载配置实用工具	Site-to-Site VPN 客户可以为兼容的客户网关 (CGW) 设备生成配置模板，从而更轻松地创建 VPN 连接。 AWS 此更新增加了对许多流行的 CGW 设备的 Internet Key Exchange 版本 2 (IKEv2) 参数的支持，并包括两个新的 APIs — GetVpnConnectionDeviceTypes 和。 GetVpnConnectionDeviceSampleConfiguration	2021 年 9 月 21 日
VPN 连接通知	Site-to-Site VPN 会自动将有关您的 VPN 连接的通知发送到 AWS Health Dashboard。	2020 年 10 月 29 日

VPN 隧道启动	您可以配置您的 VPN 隧道 AWS 以打开隧道。	2020 年 8 月 27 日
修改 VPN 连接选项	您可以修改 Site-to-Site VPN 连接的连接选项。	2020 年 8 月 27 日
其他安全算法	您可以将其他安全算法应用到 VPN 隧道。	2020 年 8 月 14 日
IPv6 支持	您的 VPN 隧道可以支持隧道内的 IPv6 流量。	2020 年 8 月 12 日
合并 AWS Site-to-Site VPN 指南	此版本将《 AWS Site-to-Site VPN 网络管理员指南》的内容合并到本指南中。	2020 年 3 月 31 日
加速 AWS Site-to-Site VPN 连接	您可以为 AWS Site-to-Site VPN 连接启用加速。	2019 年 12 月 3 日
修改 AWS Site-to-Site VPN 隧道选项	您可以修改 AWS Site-to-Site VPN 连接中 VPN 隧道的选项。还可以配置其他隧道选项。	2019 年 8 月 29 日
AWS Private Certificate Authority 私有证书支持	您可以使用中的私有证书对您的 VPN AWS Private Certificate Authority 进行身份验证。	2019 年 8 月 15 日
全新 Site-to-Site VPN 用户指南	此版本将 AWS Site-to-Site VPN （以前称为 AWS 托管 VPN ）内容与 Amazon VPC 用户指南分开。	2018 年 12 月 18 日
修改目标网关	您可以修改 AWS Site-to-Site VPN 连接的目标网关。	2018 年 12 月 18 日
自定义 ASN	创建虚拟专用网关时，可以为网关的 Amazon 端指定专用自治系统编号（ASN）。	2017 年 10 月 10 日

VPN 隧道选项	您可以为 VPN 隧道指定隧道内部 CIDR 块和自定义预共享密钥。	2017 年 10 月 3 日
VPN 指标	您可以查看 VPN 连接的 CloudWatch 指标。	2017 年 5 月 15 日
VPN 增强功能	现在，VPN 连接在连接的第 1 和第 2 阶段支持 AES 256 位加密功能、SHA-256 哈希函数、NAT 遍历及其他 Diffie-Hellman 组。此外，您现可为使用同一个客户网关设备的每个 VPN 连接使用相同的客户网关 IP 地址。	2015 年 10 月 28 日
VPN 连接使用静态路由配置。	您可以使用静态路由配置创建与 Amazon VPC 的 VP IPsec N 连接。之前，VPN 连接要求使用边界网关协议（BGP）。现在，我们支持两种类型的连接，您可以与不支持 BGP 的设备建立连接，包括 Cisco ASA 和 Microsoft Windows Server 2008 R2。	2012 年 9 月 13 日
自动路由传播	现在，您可以配置来自您的 VPN 的路由和 AWS Direct Connect 指向 VPC 路由表的链接的自动传播。	2012 年 9 月 13 日
AWS VPN CloudHub 和冗余的 VPN 连接	无论是否通过 VPC，您都可以在两个站点之间安全通信。您可以使用冗余 VPN 连接为您的 VPC 提供容错连接。	2011 年 9 月 29 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。