AWS Site-to-Site VPN

用户指南

AWS Site-to-Site VPN: 用户指南

Table of Contents

AWS Site-to-Site VPN 是什么？

默认情况下，您在 Amazon VPC 中启动的实例无法与您自己的（远程）网络进行通信。通过在 VPC 中附加虚拟专用网关、创建自定义路由表、更新您的安全组规则并创建 AWS Site-to-Site VPN (Site-to-Site VPN) 连接，您可以启用从 VPC 访问您远程网络的权限。

尽管术语 VPN 连接 是一项泛指性术语，但是在此文档中，“VPN 连接”是指在您的 VPC 和您自己的内部网络之间的连接。Site-to-Site VPN 支持 Internet 协议安全 (IPsec) VPN 连接。

您的 Site-to-Site VPN 连接可以是 AWS Classic VPN 或 AWS VPN。有关更多信息，请参阅 AWS Site-to-Site VPN 类别 (p. 2)。

> **Important**
>
> 我们目前不支持通过 Site-to-Site VPN 连接的 IPv6 流量。

内容

Site-to-Site VPN 的组成部分

Site-to-Site VPN 连接由以下部分组成。有关 Site-to-Site VPN 限制的更多信息，请参阅 Amazon VPC 用户指南 中的 Amazon VPC 限制。

虚拟专用网关

虚拟专用网关是 Site-to-Site VPN 连接在 Amazon 一端的 VPN 集线器。您可以创建虚拟专用网关，并将其附加到要从中创建 Site-to-Site VPN 连接的 VPC。

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。要检查虚拟专用网关的 ASN，请在 Amazon VPC 控制台中的虚拟专用网关屏幕上查看其详细信息，或者使用 describe-vpn-gateways AWS CLI 命令。

> **Note**
>
> 如果您在 2018-06-30 以前创建虚拟专用网关，则默认 ASN 在 亚太区域（新加坡）区域中是 17493，在 亚太区域（东京）区域中是 10124，在 欧洲（爱尔兰）区域中是 9059，在所有其他区域中是 7224。

AWS Transit Gateway

您可以将 AWS Site-to-Site VPN 连接的目标网关从虚拟专用网关修改为 中转网关。中转网关 是一个中转中心，您可用它来互连 Virtual Private Cloud (VPC) 和本地网络。有关更多信息，请参阅修改Site-to-Site VPN 连接的目标网关 (p. 18)。

客户网关

客户网关是指 Site-to-Site VPN 连接在您这一端的实体设备或软件应用程序。

要创建 AWS 连接，您必须在 Site-to-Site VPN 中创建一个客户网关资源，用以向 AWS 提供有关您的客户网关设备的信息。下表描述了创建客户网关资源所需的信息。

项目	描述
客户网关外部接口的 Internet 可路由 IP 地址 (静态)	公有 IP 地址值必须是静态地址。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。
路由类型 — 静态或动态。	有关更多信息，请参阅 Site-to-Site VPN 路由选项 (p. 7)。
(仅动态路由) 客户网关的边界网关协议 (BGP) 自治系统编号 (ASN)。	您可以使用指定给您的网络的现有 ASN。如果您没有 ASN，您可以使用专用 ASN (在 64512–65534 范围内)。 如果您在控制台中使用 VPC 向导来设置您的 VPC，我们会自动使用 65000 作为 ASN。

如需通过 Site-to-Site VPN 连接使用 Amazon VPC，您或您的网络管理员还必须配置远程网络中的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 Amazon VPC 网络管理员指南中的您的客户网关。

当流量从您的 Site-to-Site VPN 连接端生成时，VPN 隧道出现。虚拟专用网关不是启动程序；您的客户网关必须启动隧道。如果 Site-to-Site VPN 连接经历一段空闲时间（通常为 10 秒，具体取决于配置），隧道就会关闭。为防止发生这种情况，您可以使用网络监控工具（如使用 IP SLA）来生成保持连接 Ping 信号。

有关已经过 Amazon VPC 测试的客户网关的列表，请参阅 Amazon Virtual Private Cloud 常见问题。

AWS Site-to-Site VPN 类别

您的 Site-to-Site VPN 连接可以是 AWS Classic VPN 连接或 AWS VPN 连接。您新建的所有 Site-to-Site VPN 连接都是 AWS VPN 连接。仅有 AWS VPN 连接支持以下功能：

- Internet 密钥交换版本 2 (IKEv2)
- NAT 遍历
- 4 字节 ASN (除 2 字节 ASN 之外)
- 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

您可以通过使用 Amazon VPC 控制台或命令行工具，查明 Site-to-Site VPN 连接的类别。

使用控制台确定 Site-to-Site VPN 类别

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

2. 在导航窗格中，选择 Site-to-Site VPN Connections (站点到站点 VPN 连接)。
3. 选择 Site-to-Site VPN 连接，在详细信息窗格中检查 Category (类别) 的值。值 `VPN` 表示 AWS VPN 连接。值 `VPN-Classic` 表示 AWS Classic VPN 连接。

使用命令行工具确定 Site-to-Site VPN 类别

- 您可以使用 describe-vpn-connections AWS CLI 命令。在返回的输出中，记下`Category` 值。值 `VPN` 表示 AWS VPN 连接。值 `VPN-Classic` 表示 AWS Classic VPN 连接。

  在下面的示例中，Site-to-Site VPN 连接是 AWS VPN 连接。

```
aws ec2 describe-vpn-connections --vpn-connection-ids vpn-1a2b3c4d
```

```
{
    "VpnConnections": [
        {
            "VpnConnectionId": "vpn-1a2b3c4d",

            ...

            "State": "available",
            "VpnGatewayId": "vgw-11aa22bb",
            "CustomerGatewayId": "cgw-ab12cd34",
            "Type": "ipsec.1",
            "Category": "VPN"
        }
    ]
}
```

或者，使用以下命令之一：

- DescribeVpnConnections (Amazon EC2 查询 API)
- Get-EC2VpnConnection (Windows PowerShell 工具)

从 AWS Classic VPN 迁移到 AWS VPN

如果您现有的 Site-to-Site VPN 连接是 AWS Classic VPN 连接，则可以通过创建新的虚拟专用网关和 Site-to-Site VPN 连接，将旧的虚拟专用网关从您的 VPC 中断开，并将新的虚拟专用网关连接到 VPC，来迁移到 AWS VPN 连接。

如果现有的虚拟专用网关与多个 Site-to-Site VPN 连接关联，则必须为新的虚拟专用网关重新创建各自的 Site-to-Site VPN 连接。如果有多个 AWS Direct Connect 专用虚拟接口连接到虚拟专用网关，您必须为新的虚拟专用网关重新创建各自的专用虚拟接口。有关更多信息，请参阅 AWS Direct Connect 用户指南 中的创建虚拟接口。

如果现有的 Site-to-Site VPN 连接是 AWS VPN 连接，则您无法迁移到 AWS Classic VPN 连接。

> **Note**
>
> 在此过程中，如果您禁用路由传播并将旧的虚拟专用网关与您的 VPC 分离，通过当前 VPC 连接进行的连接会中断。当新的虚拟专用网关连接到您的 VPC 并且新的 Site-to-Site VPN 连接处于活动状态时，将会恢复连接。确保您为预期的停机时间做了计划。

迁移到 AWS VPN 连接

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

2. 在导航窗格中，依次选择 Virtual Private Gateways (虚拟专用网关)、Create Virtual Private Gateway (创建虚拟专用网关)，然后创建虚拟专用网关。
3. 在导航窗格中，依次选择 Site-to-Site VPN 连接、创建 VPN 连接。指定以下信息，然后选择是，创建。
   - 虚拟专用网关：选择您在上一步中创建的虚拟专用网关。
   - 客户网关：选择现有，然后选择当前 AWS Classic VPN 连接的现有客户网关。
   - 根据需要指定路由选项。
4. 选择新的 Site-to-Site VPN 连接，然后选择下载配置。为您的客户网关设备下载适当的配置文件。
5. 使用配置文件在客户网关设备上配置 VPN 隧道。例如，请参阅 Amazon VPC 网络管理员指南。还不要启用隧道。如果需要一直禁用新配置的隧道，请与供应商联系获得指导。
6. (可选) 创建测试 VPC 并将虚拟专用网关连接到测试 VPC。根据需要更改加密域/源目标地址，并测试从本地网络中的主机到测试 VPC 中的测试实例的连接性。
7. 如果您正在对路由表使用路由传播，请在导航窗格中选择 Route Tables。为您的 VPC 选择路由表，然后依次选择 Route Propagation、Edit。清除旧的虚拟专用网关的复选框，然后选择保存。

   Note

   从此步骤开始，连接将被中断，直到与新的虚拟专用网关连接，并且新的 Site-to-Site VPN 连接处于活动状态为止。
8. 在导航窗格中，选择虚拟专用网关。选择旧的虚拟专用网关，然后依次选择 Actions (操作)、Detach from VPC (与 VPC 分离) 和 Yes, Detach (是，分离)。选择新的虚拟专用网关，然后选择操作、附加到 VPC。为您的 Site-to-Site VPN 连接指定 VPC，然后选择是，请连接。
9. 在导航窗格中，选择路由表。为您的 VPC 选择路由表，然后执行下列操作之一：
   - 如果您正在使用路由传播，请依次选择 Route Propagation、Edit。选择与 VPC 连接的新虚拟专用网关，然后选择 Save。
   - 如果您正在使用静态路由，请依次选择 Routes、Edit。将路由修改为指向新的虚拟专用网关，然后选择 Save。
10. 在客户网关设备上启用新隧道，并禁用旧隧道。要开启隧道，则必须从本地网络启动连接。

    请检查路由表以确保路由正被传播 (如果适用)。当 VPN 隧道的状态为 `UP` 时，路由会传播到路由表。

    Note

    如果需要恢复到以前的配置，请断开新的虚拟专用网关，然后执行步骤 8 和 9 以重新连接旧的虚拟专用网关并更新您的路由。
11. 如果您不再需要 AWS Classic VPN 连接，并且不想继续为其付费，请从客户网关设备中删除以前的隧道配置，然后删除该 Site-to-Site VPN 连接。要执行此操作，请转到 Site-to-Site VPN 连接，选择 Site-to-Site VPN 连接，然后选择删除。

    Important

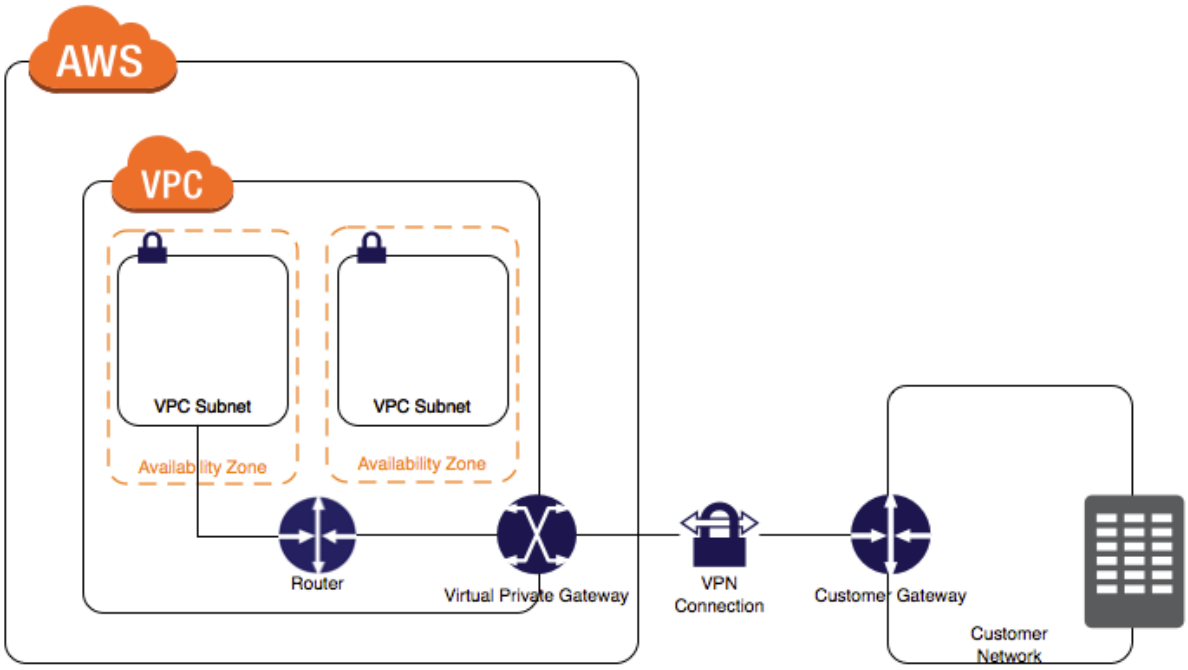
    删除 AWS Classic VPN 连接后，便不能将新的 AWS VPN 连接恢复为或迁移回 AWS Classic VPN 连接。

Site-to-Site VPN 配置示例

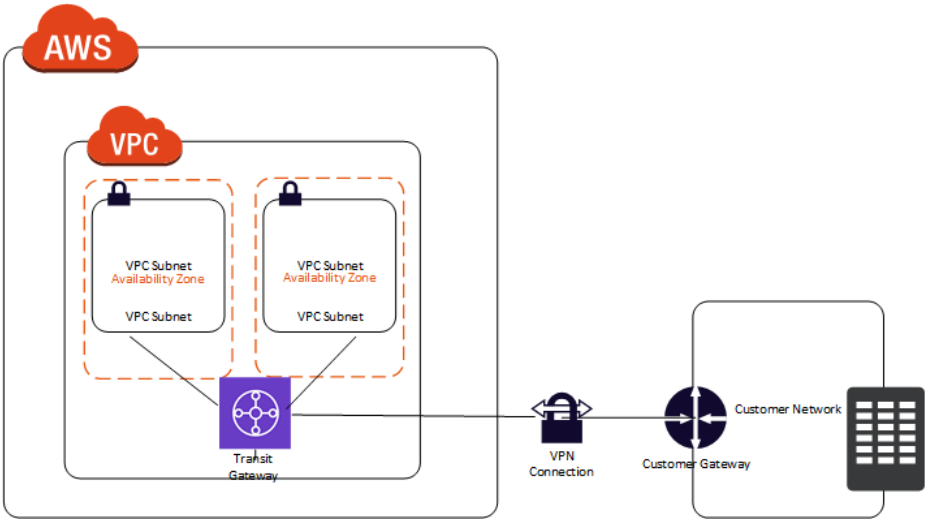
下图展示的是单一和多 Site-to-Site VPN 连接。VPC 附加了虚拟专用网关，您的远程网络内包括一个客户网关，您必须配置该网关以启用 Site-to-Site VPN 连接。您可以设置路由，以使从您的 VPC 通向您的网络的数据流可以被路由到虚拟专用网关中。

当您为单一 VPC 创建多项 Site-to-Site VPN 连接时，您可以配置第二客户网关，以创建到同一外部地点的冗余连接。您还可以使用它来创建到多个地理位置的 Site-to-Site VPN 连接。

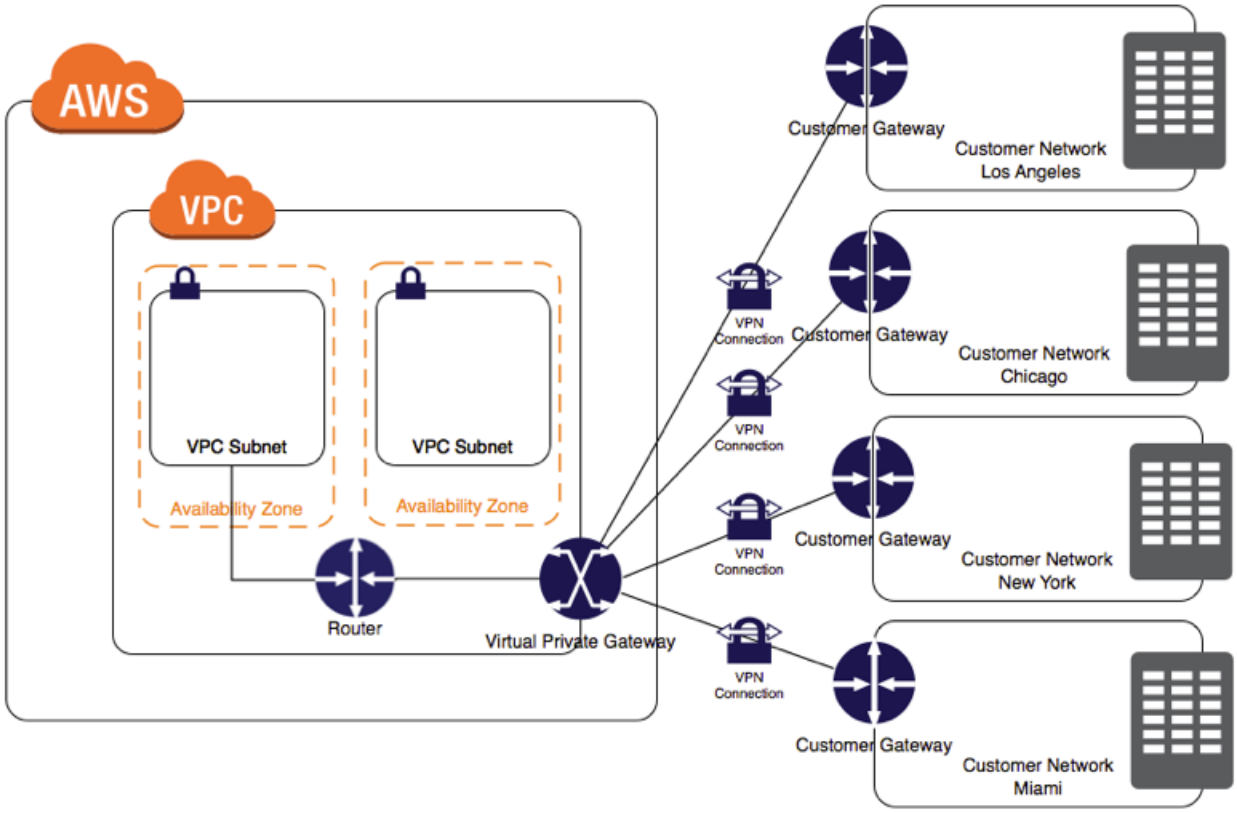
单一 Site-to-Site VPN 连接



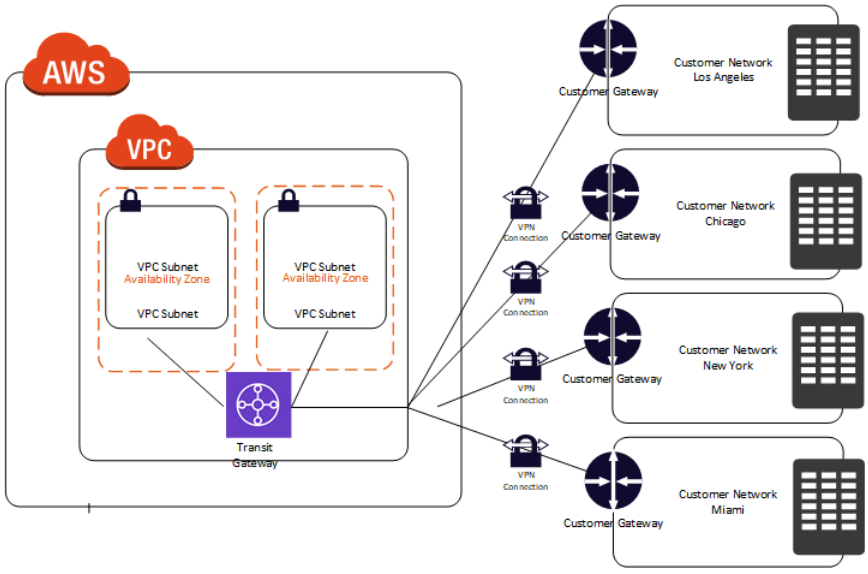
使用中转网关的单一 Site-to-Site VPN 连接



多个 Site-to-Site VPN 连接



使用一个中转网关的多个 Site-to-Site VPN 连接



Site-to-Site VPN 路由选项

在创建 Site-to-Site VPN 连接时，您必须执行以下操作：

- 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限制。有关更多信息，请参阅 Amazon VPC 用户指南 中 Amazon VPC 限制的“路由表”部分。

静态和动态路由

您选择的路由类型可由您的 VPN 设备构造和型号决定。如果您的 VPN 支持边界网关协议 (BGP)，您可以在配置 Site-to-Site VPN 连接时指定动态路由方式。如果您的设备不支持 BGP，您便需要指定静态路由。有关已经过 Amazon VPC 测试的静态和动态路由设备的列表，请参阅 Amazon Virtual Private Cloud 常见问题。

当您使用 BGP 设备时，您不需要为 Site-to-Site VPN 连接指定静态路由，因为设备会使用 BGP 将其路由通告虚拟专用网关。如果您的设备支持 BGP 广告，则您无法指定静态路由；如果您的设备不支持 BGP，您必须选择静态路由，并输入您的网络的路由（IP 前缀），以便与虚拟专用网关建立通信。

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 隧道进行故障转移。不支持 BGP 的设备也可执行健康检查，以便在需要时协助故障转移到第二条隧道。

路由表和 VPN 路由优先级

路由表决定了将网络流量定向到何处。在您的路由表中，您必须为您的远程网络添加路由，并将虚拟专用网关指定为目标。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。

只有虚拟专用网关已知的 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。

在虚拟专用网关收到路由信息时，它使用路径选择来决定如何将流量路由到您的远程网络。将应用最长前缀匹配；否则，将应用以下规则：

- 如果来自 Site-to-Site VPN 连接或 AWS Direct Connect 连接的任何传播路由与 VPC 的本地路由重叠，则本地路由的优先级最高，即使传播路由更特定也是如此。
- 如果来自 Site-to-Site VPN 连接或 AWS Direct Connect 连接的任何传播路由的目标 CIDR 块与其他现有静态路由的相同（无法应用最长前缀匹配），我们将设置其目标为 Internet 网关、虚拟专用网关、网络接口、实例 ID、VPC 对等连接、NAT 网关或 VPC 终端节点的静态路由的优先级。

如果 Site-to-Site VPN 连接内存在重叠路由，且最长前缀匹配不适用，则我们在 Site-to-Site VPN 连接内按以下规则排序路由，从最高优先级到最低优先级：

- 来自 AWS Direct Connect 连接的 BGP 传播路由
- 为 Site-to-Site VPN 连接手动添加的静态路由
- 来自 Site-to-Site VPN 连接的 BGP 传播路由

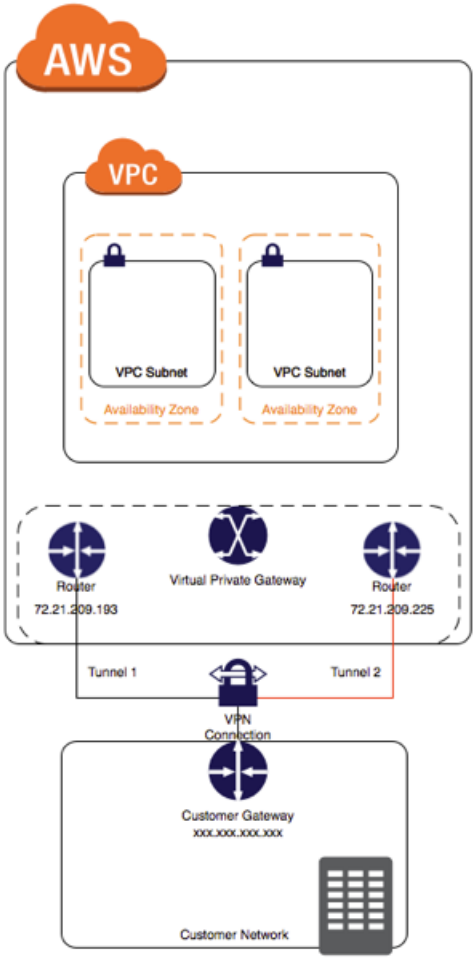
在该示例中，路由表包含一条到 Internet 网关（您手动添加的）的静态路由和一条到虚拟专用网关的传播路由。这两条路由的目的地均为 `172.31.0.0/24`。在这种情况下，目的地为 `172.31.0.0/24` 的所有流量均路由到 Internet 网关 — 这是静态路由，因此，其优先级高于传播路由。

目的地	目标
10.0.0.0/16	本地
172.31.0.0/24	vgw-1a2b3c4d (传播)
172.31.0.0/24	igw-11aa22bb

为您的 Site-to-Site VPN 连接配置 VPN 隧道

您使用 Site-to-Site VPN 连接以将您的远程网络连接到 VPC。每项 Site-to-Site VPN 连接都有两条隧道，每条隧道都会使用一个独特的虚拟专用网关公有 IP 地址。配置两条隧道以提供冗余能力是重要的步骤。当一条隧道无法使用时（例如，因维护而关闭），网络流量会自动路由到指定 Site-to-Site VPN 连接的其他可用隧道。

下图展示了 Site-to-Site VPN 连接的两条隧道。



当您创建 Site-to-Site VPN 连接时，将会下载一个特定于客户网关设备的配置文件，其中包含有关配置设备的信息，包括有关配置每个隧道的信息。在创建 Site-to-Site VPN 连接时，您可以选择自己指定某些隧道选项。否则，AWS 会提供默认值。

下表描述了您可以配置的隧道选项。

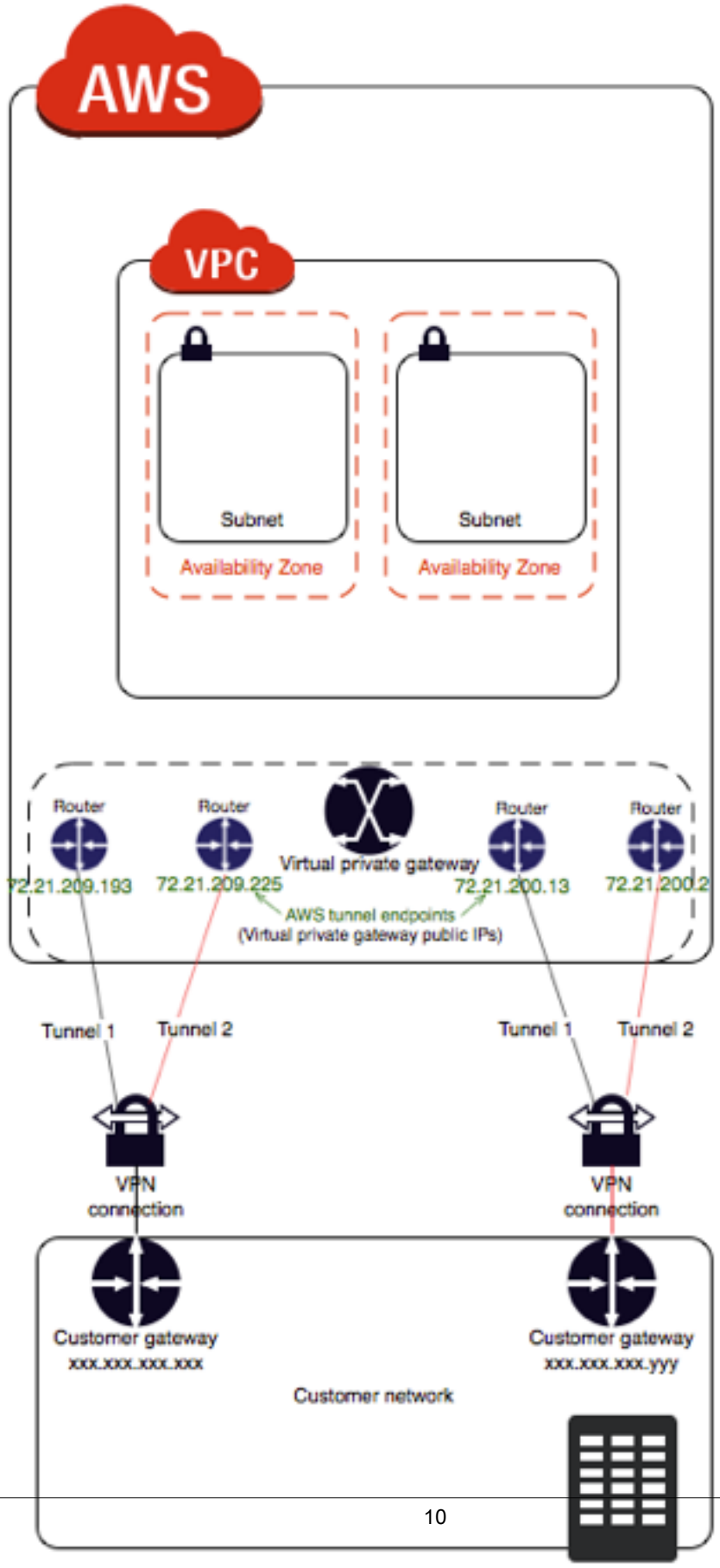
项目	描述	AWS 提供的默认值
隧道内部 CIDR	VPN 隧道的内部 IP 地址范围。您可以指定 `169.254.0.0/16` 范围中大小为 /30 的 CIDR 块。对于使用同一虚拟专用网关的所有 Site-to-Site VPN 连接，CIDR 块必须是唯一的。 以下 CIDR 块由系统保留，不能使用： • `169.254.0.0/30` • `169.254.1.0/30` • `169.254.2.0/30` • `169.254.3.0/30` • `169.254.4.0/30` • `169.254.5.0/30` • `169.254.169.252/30`	`169.254.0.0/16` 范围中大小为 /30 的 CIDR 块。
预共享密钥 (PSK)	预共享密钥 (PSK)，用于在虚拟专用网关和客户网关之间建立初始 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 (_)。	32 个字符的字母数字字符串。

创建 Site-to-Site VPN 连接后，便无法修改隧道选项。要更改现有连接的隧道内部 IP 地址或 PSK，必须删除 Site-to-Site VPN 连接并创建一个新连接。您无法为 AWS Classic VPN 连接配置隧道选项。

使用冗余 Site-to-Site VPN 连接以提供故障转移

如上所述，Site-to-Site VPN 连接配有两条隧道以帮助确保连接性，以防止出现其中一个 Site-to-Site VPN 连接不可用的情况。要避免因您的客户网关不可用而造成连接中断，您可使用第二个客户网关来为您的 VPC 和虚拟专用网关设置另一个 Site-to-Site VPN 连接。通过使用冗余 Site-to-Site VPN 连接和网关，您可以在对其中一个客户网关进行维护时保证数据流量可以继续流经第二个客户网关的 Site-to-Site VPN 连接。如需在您的远程网络中建立冗余 Site-to-Site VPN 连接和客户网关，您需要设置第二项 Site-to-Site VPN 连接。第二个 Site-to-Site VPN 连接的客户网关 IP 地址必须可以公开访问。

下图展示了每个 Site-to-Site VPN 连接的两条隧道和两个客户网关。


AWS
VPC
Subnet
Availability Zone
Subnet
Availability Zone
Router
Router
Virtual private gateway
Router
Router
72.21.209.193
72.21.209.225
72.21.200.13
72.21.200.2
AWS tunnel endpoints
(Virtual private gateway public IPs)
Tunnel 1
Tunnel 2
Tunnel 1
Tunnel 2
VPN
connection
VPN
connection
Customer gateway
xxx.xxx.xxx.xxx
Customer gateway
xxx.xxx.xxx.yyy
Customer network

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 连接要求您输入在您这一端的客户网关的远程网络静态路由。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。

入门

按照以下过程手动设置 AWS Site-to-Site VPN 连接。或者，您也可以让 VPC 创建向导为您完成其中的许多步骤。有关使用 VPC 创建向导以设置虚拟专用网关的更多信息，请参阅 Amazon VPC 用户指南 中的场景 3：带有公有子网和私有子网的 VPC 和 AWS Site-to-Site VPN 访问或场景 4：仅带有私有子网的 VPC 和 AWS Site-to-Site VPN 访问。

要设置 Site-to-Site VPN 连接，您需要完成以下步骤：

- 步骤 1: 创建客户网关 (p. 12)
- 步骤 2: 创建虚拟专用网关 (p. 12)
- 步骤 3: 在您的路由表中启用路由传播 (p. 13)
- 步骤 4: 更新您的安全组 (p. 14)
- 步骤 5: 创建 Site-to-Site VPN 连接并配置客户网关 (p. 14)

这些过程假定您的 VPC 具有一个或多个子网。

创建客户网关

客户网关向 AWS 提供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 (p. 1)。

使用控制台创建客户网关

1. 打开 Amazon VPC 控制台 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Customer Gateways，然后选择 Create Customer Gateway。
3. 填写以下信息，然后选择 Create Customer Gateway：
   - (可选) 对于 Name，为您的客户网关键入名称。这样做可创建具有 `Name` 键以及您指定的值的标签。
   - 对于 Routing，选择路由类型。
   - 对于动态路由，为 BGP ASN 键入边界网关协议 (BGP) 自治系统编号 (ASN)。
   - 对于 IP Address，为您的客户网关设备键入静态、可在 Internet 上路由的 IP 地址。如果您的客户网关位于为 NAT-T 而启用的 NAT 设备后面，请使用 NAT 设备的公有 IP 地址。

使用命令行或 API 创建客户网关

- CreateCustomerGateway (Amazon EC2 查询 API)
- create-customer-gateway (AWS CLI)
- New-EC2CustomerGateway (适用于 Windows PowerShell 的 AWS 工具)

创建虚拟专用网关

创建虚拟专用网关时，可以选择为网关的 Amazon 端指定专用自治系统编号 (ASN)。ASN 必须与为客户网关指定的 BGP 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，依次选择 Virtual Private Gateways、Create Virtual Private Gateway。
2. (可选) 为虚拟专用网关键入名称。这样做可创建具有 `Name` 键以及您指定的值的标签。
3. 对于 ASN，保留默认选择以使用默认的 Amazon ASN。否则，选择 Custom ASN 并键入一个值。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。
4. 选择 Create Virtual Private Gateway。
5. 选择您已创建的虚拟专用网关，然后依次选择 Actions、Attach to VPC。
6. 从列表中选择您的 VPC ，然后选择 Yes, Attach。

使用命令行或 API 创建虚拟专用网关

- CreateVpnGateway (Amazon EC2 查询 API)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (适用于 Windows PowerShell 的 AWS 工具)

使用命令行或 API 将虚拟专用网关连接到 VPC

- AttachVpnGateway (Amazon EC2 查询 API)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (适用于 Windows PowerShell 的 AWS 工具)

在您的路由表中启用路由传播

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 Site-to-Site VPN 连接所使用的路由并将它们指向您的虚拟专用网关。您可以为路由表启用路由传播，从而自动将这些路由传播到表。

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

> **Note**
>
> 如果您的连接中断，您的路由表中的任何已传播路由将不会自动删除。您可能必须禁用路由传播以删除已传播的路由；例如，如果您希望流量故障转移至某个静态路由。

使用控制台启用路由传播

1. 在导航窗格中，选择 Route Tables，然后选择与子网关联的路由表；默认情况下，该路由表为 VPC 的主路由表。
2. 在详细信息窗格中的路由传播选项卡上，选择编辑，选择您在上一步骤中创建的虚拟专用网关，然后选择 保存。

> **Note**
>
> 对于静态路由，如果您没有启用路由传播，则您必须手动输入您的 Site-to-Site VPN 连接使用的静态路由。为此，请选择您的路由表，然后依次选择路由、编辑。对于目的地，添加您的 Site-to-Site VPN 连接使用的静态路由。对于目标，选择虚拟专用网关 ID，然后选择保存。

使用控制台禁用路由传播

1. 在导航窗格中，选择 Route Tables，然后选择与子网关联的路由表。
2. 依次选择 Route Propagation、Edit。清除虚拟专用网关的 Propagate 复选框，然后选择 Save。

使用命令行或 API 启用路由传播

- EnableVgwRoutePropagation（Amazon EC2 查询 API）
- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (适用于 Windows PowerShell 的 AWS 工具)

使用命令行或 API 禁用路由传播

- DisableVgwRoutePropagation（Amazon EC2 查询 API）
- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (适用于 Windows PowerShell 的 AWS 工具)

更新您的安全组

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入站 SSH、RDP 和 ICMP 访问

1. 在导航窗格中，选择 Security Groups，然后选择 VPC 的默认安全组。
2. 在详细信息窗格中的入站选项卡上，添加规则，该规则允许您的网络进行入站 SSH、RDP 和 ICMP 访问，然后选择保存。有关添加入站规则的更多信息，请参阅 Amazon VPC 用户指南 中的添加、删除和更新规则。

有关使用 AWS CLI 处理安全组的更多信息，请参阅 Amazon VPC 用户指南 中的您的 VPC 的安全组。

创建 Site-to-Site VPN 连接并配置客户网关

创建 Site-to-Site VPN 连接后，请下载配置信息并使用它来配置客户网关设备或软件应用程序。

创建 Site-to-Site VPN 连接并配置客户网关

1. 在导航窗格中，依次选择 Site-to-Site VPN 连接、创建 VPN 连接。
2. 填写以下信息，然后选择创建 VPN 连接：
   - （可选）对于名称标签，为您的 Site-to-Site VPN 连接键入名称。这样做可创建具有 `Name` 键以及您指定的值的标签。
   - 选择您之前创建的虚拟专用网关。
   - 选择您之前创建的客户网关。
   - 根据您的 VPN 路由器是否支持边界网关协议 (BGP)，选择一个路由选项：
     - 如果您的 VPN 路由器支持 BGP，请选择 Dynamic (requires BGP)。
     - 如果您的 VPN 路由器不支持 BGP，请选择静态。对于静态 IP 前缀，为您的 Site-to-Site VPN 连接的专用网络指定各自的 IP 前缀。
   - 在隧道选项下面，您可以选择为每个隧道指定以下信息：
     - 隧道内部 IP 地址的 `169.254.0.0/16` 范围中大小为 /30 的 CIDR 块。

- IKE 预共享密钥 (PSK)。支持以下版本：IKEv1 或 IKEv2。

有关这些选项的详细信息，请参阅 为您的 Site-to-Site VPN 连接配置 VPN 隧道 (p. 8)。

创建 Site-to-Site VPN 连接可能需要几分钟的时间。准备就绪之后，选择该连接，然后选择下载配置。

3. 在下载配置对话框中，选择与客户网关设备或软件对应的供应商、平台和软件，然后选择是，请下载。
4. 为您的网络管理员提供配置文件和指南：Amazon VPC 网络管理员指南。在网络管理员配置客户网关之后，Site-to-Site VPN 连接便已可以操作。

使用命令行或 API 创建 Site-to-Site VPN 连接

- CreateVpnConnection（Amazon EC2 查询 API）
- create-vpn-connection (AWS CLI)
- New-EC2VpnConnection (适用于 Windows PowerShell 的 AWS 工具)

编辑 Site-to-Site VPN 连接的静态路由

对于静态路由，您可以添加、修改或删除您的 VPN 配置的静态路由。

添加、修改或删除静态路由

1. 打开 Amazon VPC 控制台 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Site-to-Site VPN Connections (站点到站点 VPN 连接)。
3. 依次选择静态路由、编辑。
4. 修改现有静态 IP 前缀或选择 Remove 将其删除。选择 Add Another Rule 以向您的配置添加新的 IP 前缀。完成此操作后，选择保存。

Note

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 Site-to-Site VPN 连接中反映更新的静态 IP 前缀。有关更多信息，请参阅 在您的路由表中启用路由传播 (p. 13)。

使用命令行或 API 添加静态路由

- CreateVpnConnectionRoute（Amazon EC2 查询 API）
- create-vpn-connection-route (AWS CLI)
- New-EC2VpnConnectionRoute (适用于 Windows PowerShell 的 AWS 工具)

使用命令行或 API 删除静态路由

- DeleteVpnConnectionRoute（Amazon EC2 查询 API）
- delete-vpn-connection-route (AWS CLI)
- Remove-EC2VpnConnectionRoute (适用于 Windows PowerShell 的 AWS 工具)

替换受损的凭证

如果您认为 Site-to-Site VPN 连接的隧道凭证已经受损，您可以更改 IKE 预共享密钥。为此，删除 Site-to-Site VPN 连接，使用相同的虚拟专用网关创建一项新的凭证，并在您的客户网关中配置新的密钥。您可以在

创建 Site-to-Site VPN 连接时指定自己的预共享密钥。您还需要确认隧道的内部和外部地址可以相互匹配，因为在您重新建立 Site-to-Site VPN 连接时这些地址可能也会随之更改。在您执行此步骤时，与您的 VPC 实例的通信将会停止，但实例仍会继续不受干扰地运行。在网络管理员执行新配置信息之后，您的 Site-to-Site VPN 连接便可使用新凭证，而到您的 VPC 实例的网络连接也将恢复正常。

Important

此步骤要求您的网络管理员组的协助。

更改 IKE 预共享密钥

1. 删除 Site-to-Site VPN 连接。有关更多信息，请参阅删除 Site-to-Site VPN 连接 (p. 21)。您不需要删除 VPC 或虚拟专用网关。
2. 创建新的 Site-to-Site VPN 连接并为隧道指定您自己的预共享密钥，或者让 AWS 为您生成新的预共享密钥。有关更多信息，请参阅创建 Site-to-Site VPN 连接并配置客户网关 (p. 14)。
3. 下载新的配置文件。

测试 Site-to-Site VPN 连接

创建 AWS Site-to-Site VPN 连接并配置客户网关后，您可以启动一个实例并通过 ping 通实例来测试连接。您需要使用响应 ping 请求的 AMI，而且需要确保您实例的安全组配置为启用入站 ICMP。建议您使用一个 Amazon Linux AMI。如果您使用的实例在 Windows Server 中运行，您将需要登录实例，并在 Windows 防火墙中启用 ICMPv4，方可检测实例。

> **Important**
>
> 您必须对 VPC 中负责过滤实例流量的任何安全组或网络 ACL 进行配置，以允许入站和出站 ICMP 流量。

测试端到端连接

1. 打开 Amazon EC2 控制台 https://console.aws.amazon.com/ec2/。
2. 在控制面板上，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页上，选择某个 AMI，然后选择 Select。
4. 选择实例类型，然后选择 Next: Configure Instance Details。
5. 在 Configure Instance Details 页面上，为 Network 选择您的 VPC。对于 Subnet，选择您的子网。选择 Next，直至到达 Configure Security Group 页面。
6. 选择 Select an existing security group (选择现有安全组) 选项，然后选择您之前修改的默认组。选择 Review and Launch。
7. 检视您已经选择的设置。执行所需的任何更改，然后选择 Launch 以选择一个密钥对并启动实例。
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 控制台显示的地址是实例详细信息的一部分。
9. 对于在您的网络中、位于客户网关背后的计算机，您可以使用`ping`命令侦测实例的私有 IP 地址。成功响应的形式与下方类似：

```
ping 10.0.0.4
```

```
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
```

您现在可以使用 SSH 或 RDP 来连接您 VPC 中的实例。有关如何连接 Linux 实例的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的 Connect to Your Linux Instance。有关如何连接 Windows 实例的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的连接到您的 Windows 实例。

修改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：

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

以下任务可帮助您完成迁移到新网关的过程。

任务

步骤 1：创建中转网关

在执行迁移到新网关的过程之前，您必须配置新的网关。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” (p. 12)。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。

如果新目标网关是中转网关，则将 VPC 附加到中转网关。有关附加 VPC 的信息，请参阅 Amazon VPC 中转网关 中的中转网关附加到 VPC。

步骤 2：删除您的静态路由（对于迁移到中转网关的静态 VPN 连接，这是必需步骤）

当您从具有静态路由的虚拟专用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 Amazon VPC 控制台 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择路由表，然后选择路由表。

3. 在 Routes (路由) 选项卡中，选择 Edit (编辑)，然后对于到虚拟专用网关的静态路由，选择 Remove (删除)。
4. 完成后选择 Save (保存)。

步骤 3：迁移到新网关

1. 打开 Amazon VPC 控制台 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Site-to-Site VPN Connections (站点到站点 VPN 连接)。
3. 选择Site-to-Site VPN 连接，然后依次选择操作、修改 VPN 连接。
4. 在 Change Target (更改目标) 下，执行以下操作：

   a. 对于 Target Type (目标类型)，选择网关类型。

   b. 配置连接目标：

   [虚拟专用网关] 对于 Target VPN Gateway ID (目标 VPN 网关 ID)，选择虚拟专用网关 ID。

   [中转网关] 对于Target 中转网关 ID (目标中转网关 ID)，选择中转网关 ID。
5. 选择 Save (保存)。

使用命令行或 API 修改Site-to-Site VPN 连接

- ModifyVpnConnection (Amazon 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。下表提供了有关您要采取的操作的信息。有关更新 VPC 路由表的信息，请参阅 Amazon VPC 用户指南 中的路由表。

修改 VPN 网关目标需要更新 VPC 路由表

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	中转网关	添加指向中转网关 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网关	使用静态路由的虚拟专用网关	添加一个条目，其中包含新的虚拟专用网关 ID。
使用静态路由的虚拟网关	中转网关	更新 VPC 路由表，并将包含虚拟专用网关 ID 的条目更改为包含中转网关 ID。
使用静态路由的虚拟网关	使用静态路由的虚拟专用网关	将指向虚拟专用网关 ID 的条目更新为指向新的虚拟专用网关 ID。
使用静态路由的虚拟网关	使用传播路由的虚拟专用网关	删除包含虚拟专用网关 ID 的条目。
中转网关	使用静态路由的虚拟专用网关	将包含中转网关的条目更新为包含虚拟专用网关 ID。

现有网关	新网关	VPC 路由表更改
中转网关	使用传播路由的虚拟专用网关	删除包含中转网关 ID 的条目。
中转网关	中转网关	将包含中转网关 ID 的条目更新为包含新的中转网关 ID。

步骤 5：更新中转网关路由（当新网关是中转网关时，此步骤是必需的）

当新网关是中转网关时，修改中转网关路由表以允许 VPC 和Site-to-Site VPN 之间的流量。有关中转网关路由的信息，请参阅 Amazon VPC 中转网关 中的中转网关路由表。

Important

如果您删除了 VPN 静态路由，您必须将这些静态路由添加到中转网关路由表。

删除 Site-to-Site VPN 连接

若您不再需要某一 AWS Site-to-Site VPN 连接，则可将其删除。

> **Important**
>
> 如果您删除了 Site-to-Site VPN 连接并创建了一个新连接，则需要下载新配置信息，然后让您的网络管理员重新配置客户网关。

使用控制台删除 Site-to-Site VPN 连接

1. 打开 Amazon VPC 控制台 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Site-to-Site VPN Connections (站点到站点 VPN 连接)。
3. 选择 Site-to-Site VPN 连接，然后依次选择操作、删除。
4. 选择删除。

若您不再需要某一客户网关，则可将其删除。您无法删除正在 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 Customer Gateways。
2. 选择要删除的客户网关，然后选择 Actions、Delete Customer Gateway.
3. 选择是，删除。

如果您不再需要 VPC 的某一虚拟专用网关，则可将其断开。

使用控制台断开虚拟专用网关

1. 在导航窗格中，选择虚拟专用网关。
2. 选择相应的虚拟专用网关，然后选择 Actions、Detach from VPC。
3. 选择 Yes, Detach。

如果不再需要某一断开的虚拟专用网关，可将其删除。您无法删除仍与 VPC 关联的虚拟专用网关。

使用控制台删除虚拟专用网关

1. 在导航窗格中，选择虚拟专用网关。
2. 选择要删除的虚拟专用网关，然后选择 Actions、Delete Virtual Private Gateway。
3. 选择是，删除。

使用命令行或 API 删除 Site-to-Site VPN 连接

- DeleteVpnConnection（Amazon EC2 查询 API）
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection（适用于 Windows PowerShell 的 AWS 工具）

使用命令行或 API 删除客户网关

- DeleteCustomerGateway（Amazon EC2 查询 API）

- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway（适用于 Windows PowerShell 的 AWS 工具）

使用命令行或 API 断开虚拟专用网关

- DetachVpnGateway（Amazon EC2 查询 API）
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway（适用于 Windows PowerShell 的 AWS 工具）

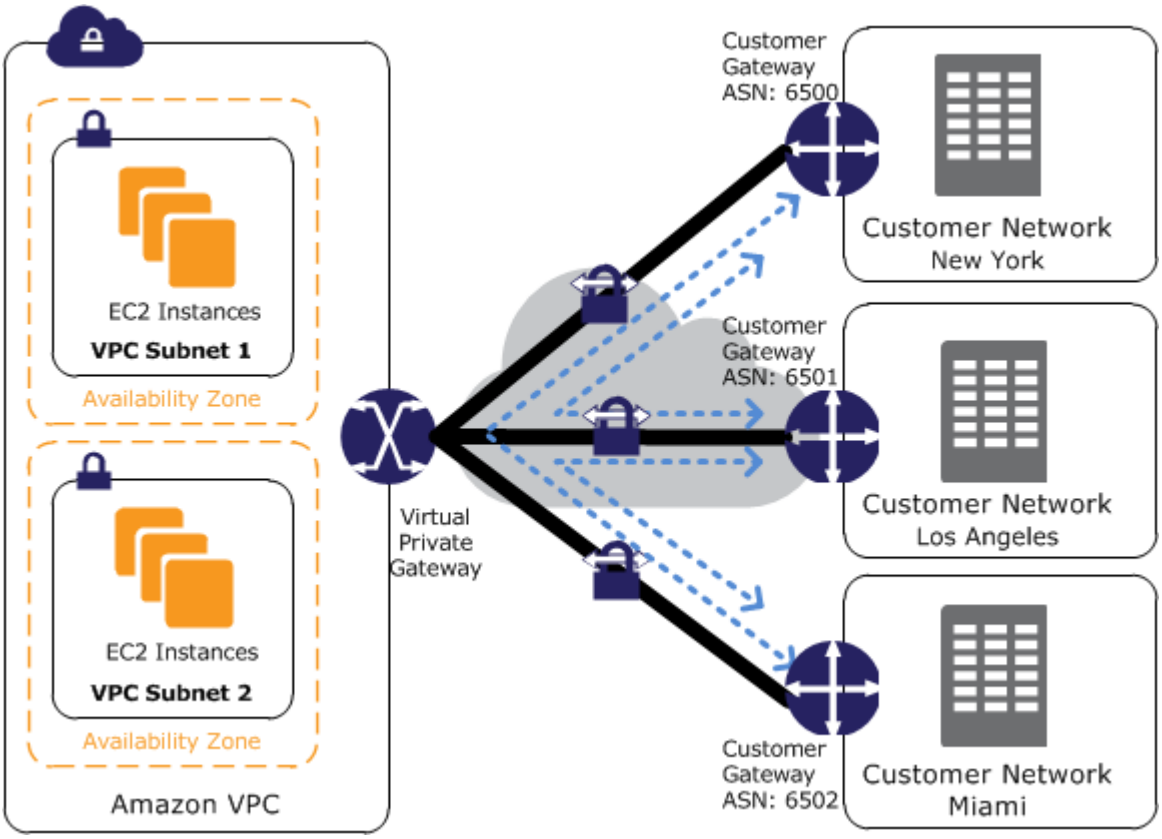
使用命令行或 API 删除虚拟专用网关

- DeleteVpnGateway（Amazon EC2 查询 API）
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (适用于 Windows PowerShell 的 AWS 工具)

使用 VPN CloudHub 在各个站点之间提供安全的通信

如果您有多个 AWS Site-to-Site VPN 连接，您可以使用 AWS VPN CloudHub 在各个站点之间提供安全的通信。这可使您的远程站点彼此进行通信，而不只是与 VPC 进行通信。VPN CloudHub 在简单的星型拓扑连接模型上操作，您可以在使用或不使用 VPC 的情况下操作 VPN CloudHub。这种设计适合有多间分公司和现有 Internet 连接的客户，帮助他们实施方便、潜在低成本的星型拓扑连接模型，以便在这些远程办公室之间建立主要或备用连接。

下图展示了 VPN CloudHub 架构，蓝色虚线表明远程站点之间的网络流量（通过 Site-to-Site VPN 连接路由）。



要使用 AWS VPN CloudHub，必须创建具有多个客户网关的虚拟专用网关。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)。客户网关可通过它们的 Site-to-Site VPN 连接传播适当的路由（BGP 前缀）。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。站点的 IP 范围不得重叠。每个站点还可以发送和从 VPC 接收数据（与使用标准 Site-to-Site VPN 连接的方式相同）。

使用 AWS Direct Connect 连接来连接虚拟专用网关的站点也可以是 AWS VPN CloudHub 的一部分。例如，您在纽约的公司总部有到 VPC 的 AWS Direct Connect 连接，您的分公司可以使用 Site-to-Site VPN 连接以连接 VPC。洛杉矶和迈阿密的分公司可以使用 AWS VPN CloudHub 在彼此以及您的公司总部之间发送和接收数据。

如需配置 AWS VPN CloudHub，您可以使用 AWS 管理控制台创建多个客户网关，每个网关都有网关公有 IP 地址和 ASN。接下来，您可以创建从每个客户网关到通用虚拟专用网关的 Site-to-Site VPN 连接。每个 Site-to-Site VPN 连接都必须传播其指定的 BGP 路由。您可以使用 Site-to-Site VPN 连接的 VPN 配置文件内的网络声明完成此操作。根据您使用的路由类型，网络声明可能会有稍许不同。

在使用 AWS VPN CloudHub 时，您需要支付标准的 Amazon VPC Site-to-Site VPN 连接费用。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 CloudHub 从一个站点向另一个站点发送数据，从您的站点向虚拟专用网关发送数据不会产生任何费用。对于从虚拟专用网关转继到您的终端节点的数据您仅需支付标准 AWS 数据传输费用即可。例如，如果您在洛杉矶设有一个站点、在纽约设有第二个站点，并且两个站点都有通向虚拟专用网关的 Site-to-Site VPN 连接，您应为每个 Site-to-Site VPN 连接支付每小时 0.05 美元的费用（总费用为每小时 0.10 美元）。您还需要为所有经过每条 Site-to-Site VPN 连接从洛杉矶发送到纽约（或从纽约发送到洛杉矶）的数据支付标准 AWS 数据传输费用；通过 Site-to-Site VPN 连接发送到虚拟专用网关的数据流量不会产生任何费用，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将按照标准 AWS 数据传输费用产生相应的费用。有关更多信息，请参阅 Site-to-Site VPN 连接定价。

监控您的 Site-to-Site VPN 连接

监控是保持 AWS Site-to-Site VPN 连接的可靠性、可用性和性能的重要部分。您应从 AWS 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。不过，在开始监控 Site-to-Site VPN 连接之前，您应制定一个监控计划并在计划中回答下列问题：

- 您的监控目标是什么？
- 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

内容

监控工具

AWS 为您提供了各种可以用来监控 Site-to-Site VPN 连接的工具。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化监控工具来监控 Site-to-Site VPN 连接并在出现错误时报告：

- Amazon CloudWatch 警报 – 按您指定的时间段观察单个指标，并根据相对于给定阈值的指标值在若干时间段内执行一项或多项操作。操作是发送通知到 Amazon SNS 主题。CloudWatch 警报将不会仅因为其处于特定状态而调用操作；该状态必须已改变并在指定的若干个时间段内保持不变。有关更多信息，请参阅使用 Amazon CloudWatch 监控 VPN 隧道 (p. 26)。
- AWS CloudTrail 日志监控 – 在账户间共享日志文件，通过将 CloudTrail 日志文件发送到 CloudWatch Logs 对它们进行实时监控，使用 Java 编写日志处理应用程序，以及验证您的日志文件是否在由 CloudTrail 传送后未发生更改。有关更多信息，请参阅 Amazon EC2 API Reference 中的使用 AWS CloudTrail 记录 API 调用和 AWS CloudTrail User Guide 中的使用 CloudTrail 日志文件。

手动监控工具

监控 Site-to-Site VPN 连接时的另一个重要环节是手动监控 CloudWatch 警报未涵盖的那些项。Amazon VPC 和 CloudWatch 控制台控制面板提供您的 AWS 环境状态的概览视图。

- 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，选择一个 Site-to-Site VPN 连接，然后选择隧道详细信息）
- CloudWatch 主页将显示以下内容：
  - 当前警报和状态
  - 警报和资源的图表
  - 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
  - 搜索并浏览您所有的 AWS 资源指标
  - 创建和编辑警报以接收有关问题的通知

使用 Amazon CloudWatch 监控 VPN 隧道

您可以使用 CloudWatch 监控 VPN 隧道，此工具可从 VPN 服务收集原始数据，并将数据处理为便于读取的近乎实时的指标。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。一旦 VPN 指标数据变为可用，便会自动发送到 CloudWatch。

> **Important**
>
> AWS Classic VPN 连接不支持 CloudWatch 指标。有关更多信息，请参阅AWS Site-to-Site VPN 类别 (p. 2)。

有关更多信息，请参阅 Amazon CloudWatch 用户指南。

VPN 隧道指标和维度

以下指标可用于 VPN 隧道。

指标	描述
`TunnelState`	隧道的状态。对于静态 VPN，0 表示关闭，1 表示运行。对于 BGP VPN，1 表示已建立，0 用于所有其他状态。 单位：布尔值
`TunnelDataIn`	通过 VPN 隧道接收的字节数。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

指标	描述
TunnelDataOut	通过 VPN 隧道发送的字节数。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

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 VPN 隧道 CloudWatch 指标

当您创建新的 Site-to-Site VPN 连接时，一旦有关您的 VPN 隧道的下列指标变为可用，VPN 服务便会将其发送给 CloudWatch。您可以按照以下方法查看 VPN 隧道的各项指标。

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. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择 Metrics。
3. 在全部指标下，选择 VPN 指标命名空间。
4. 选择指标维度以查看指标（例如，对于 Site-to-Site VPN 连接）。

使用 AWS CLI 查看指标

在命令提示符处，输入以下命令：

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

创建 CloudWatch 警报以监控 VPN 隧道

您可以创建 CloudWatch 警报，用于在警报改变状态时发送 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，并根据相对于给定阈值的指标值每隔若干个时间段向 Amazon SNS 主题发送一个通知。

例如，您可以创建一个警报来监控 VPN 隧道的状态，并在隧道状态在连续 3 个 5 分钟时间段内为 DOWN 时发送通知。

创建隧道状态警报

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，依次选择警报和创建警报。
3. 选择 VPN Tunnel Metrics。

4. 选择 VPN 隧道的 IP 地址以及 TunnelState 指标。选择 Next (下一步)。
5. 按如下所示配置警报，然后在完成后选择创建警报：

   - 在 Alarm Threshold 下，输入警报的名称和说明。对于每当，选择 <= 并输入 0。输入 3 作为连续周期数。
   - 在 Actions 下，选择现有通知列表，或者选择 New list 以创建一个新的通知列表。
   - 在警报预览下，选择 5 分钟的周期并指定最大值的统计数据。

您可以创建一个监控 Site-to-Site VPN 连接状态的警报。例如，当两条隧道的状态在一个连续 5 分钟的周期内均为关闭时，以下警报将会发送通知。

创建 Site-to-Site VPN 连接状态的警报

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，依次选择警报和创建警报。
3. 选择 VPN Connection Metrics (VPN 连接指标)。
4. 选择您的 Site-to-Site VPN 连接以及 TunnelState 指标。选择 Next (下一步)。
5. 按如下所示配置警报，然后在完成后选择创建警报：

   - 在 Alarm Threshold 下，输入警报的名称和说明。对于每当，选择 <= 并输入 0。输入 1 作为连续周期数。
   - 在 Actions 下，选择现有通知列表，或者选择 New list 以创建一个新的通知列表。
   - 在警报预览下，选择 5 分钟的周期并指定最大值的统计数据。

     或者，如果您已将 Site-to-Site VPN 连接配置为两个隧道都开启，则可以指定最小值统计信息，以便在至少一个隧道关闭时发送通知。

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. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，依次选择警报和创建警报。
3. 选择 VPN Tunnel Metrics。
4. 选择 VPN 隧道的 IP 地址以及 TunnelDataIn 指标。选择 Next (下一步)。
5. 按如下所示配置警报，然后在完成后选择创建警报：

   - 在 Alarm Threshold 下，输入警报的名称和说明。对于每当，选择 >= 并输入 5000000。输入 1 作为连续周期数。
   - 在 Actions 下，选择现有通知列表，或者选择 New list 以创建一个新的通知列表。
   - 在 Alarm Preview 下，选择 15 分钟的周期并指定 Sum 的统计数据。

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. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，依次选择警报和创建警报。
3. 选择 VPN Tunnel Metrics。
4. 选择 VPN 隧道的 IP 地址以及 TunnelDataOut 指标。选择 Next (下一步)。
5. 按如下所示配置警报，然后在完成后选择创建警报：

- 在 Alarm Threshold 下，输入警报的名称和说明。对于每当，选择 <= 并输入 1000000。输入 1 作为连续周期数。
- 在 Actions 下，选择现有通知列表，或者选择 New list 以创建一个新的通知列表。
- 在 Alarm Preview 下，选择 15 分钟的周期并指定 Sum 的统计数据。

有关创建警报的更多示例，请参阅 Amazon CloudWatch 用户指南 中的创建 Amazon CloudWatch 警报。

文档历史记录

下表介绍 AWS Site-to-Site VPN 用户指南更新。

更改	描述	日期
您可以修改 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。有关更多信息，请参阅修改Site-to-Site VPN 连接的目标网关 (p. 18)。	2018 年 12 月 18 日
首次发布	此版本将 AWS Site-to-Site VPN（先前称为 AWS 托管 VPN）的内容与 Amazon VPC 用户指南分开。	2018 年 12 月 18 日