AWS 白皮书

Amazon Virtual Private Cloud Connectivity Options

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Virtual Private Cloud Connectivity Options: AWS 白皮书

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

摘要 1
摘要 1
简介 2
Network-to-Amazon VPC 连接选项 4
AWS Site-to-Site VPN 6
其他资源 8
AWS Transit Gateway Site-to-Site + ... 8
其他资源 11
AWS Direct Connect 11
其他资源 14
AWS Direct Connect + AWS Transit Gateway 15
其他资源 15
AWS Direct Connect + AWS Site-to-Site VPN 16
其他资源 16
AWS Direct Connect AWS Transit Gateway + AWS Site-to-Site VPN 17
其他资源 18
AWS VPN CloudHub 18
其他资源 19
AWS Transit Gateway + 软件定义广域网解决方案 19
其他资源 21
软件 VPN 22
其他资源 23
亚马逊 VPC-to-Amazon VPC 连接选项 24
VPC 对等连接 25
其他资源 23
AWS Transit Gateway 27
其他资源 28
AWS PrivateLink 29
访问控制 AWS PrivateLink 29
其他资源 30
软件 VPN 30
其他资源 31
软件 VPN-to-AWS Site-to-Site VPN 32
其他资源 33

软件远程 access-to-Amazon VPC 连接选项 34
AWS Client VPN 34
其他资源 35
软件客户端 VPN 35
其他资源 37
传输 VPC 38
其他资源 38
AWS 云广域网 39
需知信息 39
其他资源 40
结论 41
附录 A：软件 VPN 实例的高级高可用架构 42
VPN 监控 42
贡献者 44
文档修订 45
版权声明 46
..... xlvii

Amazon Virtual Private Cloud Connectivity Options

发布日期：2023 年 4 月 5 日 (文档修订)

摘要

Amazon Virtual Private Cloud（亚马逊 VPC）允许客户配置亚马逊网络服务 (AWS) 云的私有隔离部分，在那里他们可以使用客户定义的 IP 地址范围在虚拟网络中启动 AWS 资源。Amazon VPC 为客户提供了多种将其 AWS 虚拟网络与其他远程网络连接起来的选项。本文档描述了可供我们的客户使用的几种常见网络连接选项。其中包括用于将远程客户网络与 Amazon VPC 集成以及将多个 Amazon VPCs 连接到连续虚拟网络的连接选项。

本白皮书适用于想要查看可用连接选项的企业网络架构师和工程师或 Amazon VPC 管理员。它概述了促进网络连接讨论的各种选项，并提供了指向其他文档和资源的指针，以及更详细的信息或示例。

简介

Amazon VPC 提供多种网络连接选项供您使用，具体取决于您当前的网络设计和要求。这些连接选项包括使用互联网或 AWS Direct Connect 连接作为网络主干，以及终止与 AWS 或用户管理的网络终端节点的连接。此外，借助 AWS，您可以选择如何利用 AWS 服务或用户管理的网络设备和路由，在 Amazon VPC 和您的网络之间传送网络路由。本白皮书考虑了以下选项，并对每个选项进行了概述和高级比较：

- Network-to-Amazon VPC 连接选项
  - AWS Site-to-Site VPN — 介绍如何建立从远程网络上的网络设备到 Amazon VPC 的托管 VP IPsec N 连接。
  - AWS Transit Gateway + AWS IPsec VP Site-to-Site N — 介绍使用建立从远程网络上的网络设备到亚马逊 VPCs区域网络中心的托管 VPN 连接 AWS Transit Gateway。
  - AWS Direct Connect-介绍如何使用建立从您的远程网络到 Amazon VPC 的私有逻辑连接 AWS Direct Connect。
  - AWS Direct Connect + AWS Transit Gateway— 介绍如何使用 AWS Direct Connect 和建立从您的远程网络到 Amazon VPCs 区域网络中心的私有逻辑连接 AWS Transit Gateway。
  - AWS Direct Connect + AWS Site-to-Site VPN — 介绍如何使用 AWS Direct Connect 和 AWS VPN 建立从您的远程网络到 Amazon V Site-to-Site PC 的私有加密连接。
  - AWS Direct ConnectAWS Transit Gateway + AWS Site-to-Site VPN— 介绍如何使用 AWS Direct Connect 和建立从您的远程网络到 Amazon VPCs 区域网络中心的私有加密连接 AWS Transit Gateway。
  - AWS VPN CloudHub— 描述建立连接远程分支机构的 hub-and-spoke模型。
  - 软件 VPN— 介绍如何建立从远程网络上的设备到 Amazon VPC 内运行的用户管理的软件 VPN 设备的 VPN 连接。
  - AWS Transit Gateway + 软件定义广域网解决方案-介绍软件定义广域网 (SD-WAN) 解决方案的集成，该解决方案使用 AWS 主干网或互联网作为传输网络 VPCs，将多个远程位置互连到 Amazon 的区域网络中心。
- 亚马逊 VPC-to-Amazon VPC 连接选项
  - VPC 对等连接— 介绍如何使用 Amazon VPC 对等互连功能在区域 VPCs 内和跨区域连接亚马逊。
  - AWS Transit Gateway— 描述在 hub-and-spoke模型中使用 AWS Transit Gateway 在区域 VPCs 内和跨区域连接 Amazon。

  - AWS PrivateLink— 介绍如何将 Amazon VPCs 与 VPC 接口终端节点和 VPC 终端节点服务连接起来。
  - 软件 VPN— 介绍如何 VPCs 使用在每个 Amazon VPC 内部运行的用户管理的软件 VPN 设备之间建立的 VPN 连接连接亚马逊。
  - 软件 VPN-to-AWS Site-to-Site VPN— 介绍通过在一个亚马逊 VPCs VPC 中的用户管理的软件 VPN 设备和连接到另一个亚马逊 VPC 的 V AWS Site-to-Site PN 之间建立的 VPN 连接来连接亚马逊。
- 软件远程 access-to-Amazon VPC 连接选项
  - AWS Client VPN— 介绍如何利用 AWS Client VPN 将软件远程访问连接到亚马逊 VPC。
  - 软件客户端 VPN— 介绍如何利用用户管理的软件 VPN 设备将软件远程访问连接到 Amazon VPC。
- 传输 VPC-介绍如何将软件 VPN 与 AWS 托管的 VPN 结合使用，在 AWS 上建立全球传输网络。
- AWS 云广域网-介绍如何建立托管广域网 (WAN)，以便轻松构建、管理和监控 Amazon 资源 VPCs、数据中心和远程分支机构之间的全球互连。

Network-to-Amazon VPC 连接选项

本节提供将远程网络与您的 Amazon VPC 环境连接起来的设计模式。这些选项可用于通过将您的内部网络扩展到 AWS 云来将 AWS 资源与您现有的现场服务（例如监控、身份验证、安全、数据或其他系统）集成。此网络扩展还允许您的内部用户无缝连接到 AWS 上托管的资源，就像任何其他面向内部的资源一样。

为每个连接的网络使用非重叠的 IP 范围时，最好实现 VPC 与远程客户网络的连接。例如，如果您想将一个或多个 VPCs 连接到公司网络，请确保它们配置了唯一的无类域间路由 (CIDR) 范围。我们建议为每个 VPC 分配一个连续、不重叠的 CIDR 块。有关 Amazon VPC 路由和限制的更多信息，请参阅亚马逊 VPC 常见问题解答。

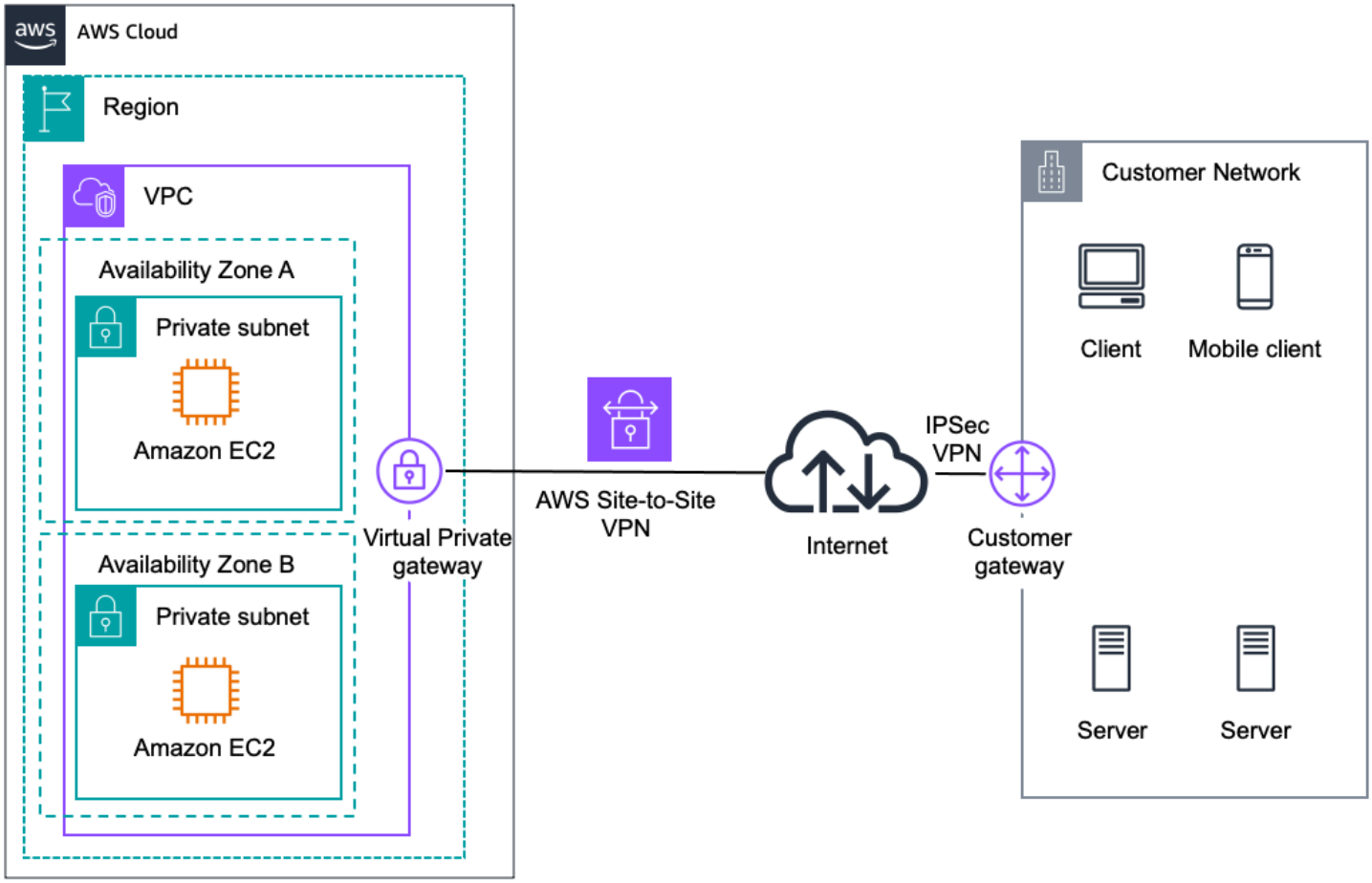
选项	使用场景	优点	限制
AWS Site-to-Site VPN	AWS 托管 IPsec VPN 通过互联网连接到单个 VPC	重复使用现有的 VPN 设备和流程 重复使用现有的互联网连接 AWS 托管的高可用性 VPN 服务 支持静态路由或动态边界网关协议 (BGP) 对等和路由策略	网络延迟、可变性和可用性取决于互联网条件 您负责实现冗余和故障转移（如果需要） 远程设备必须支持单跳 BGP（利用 BGP 进行动态路由时）
AWS Transit Gateway + AW Site-to-Site S	AWS 托管 IPsec VPN 通过互联网连接到多个区域路由器 VPCs	与上一个选项相同 AWS 管理了高可用性和可扩展性的区域网络中心，最多可容纳 5,000 个附件	与上一个选项相同
AWS Direct Connect	通过专线进行专用网络连接	更可预测的网络性能 降低带宽成本	可能需要额外的电信和托管服务提供商关系或配置新的网络线路

选项	使用场景	优点	限制
		支持 BGP 对等和路由策略	
AWS Direct Connect + AWS Transit Gateway	通过专线连接到多个区域路由器的专用网络连接 VPCs	与上一个选项相同 AWS 管理了高可用性和可扩展性的区域网络中心，最多可容纳 5,000 个附件	与之前的选项相同
AWS Direct Connect + AWS Site-to-Site VPN	IPsec 通过私人线路进行的 VPN 连接	更可预测的网络性能 降低带宽成本 支持 BGP 对等和路由策略 AWS Direct Connect 重复使用现有的 VPN 设备和流程 AWS 托管的高可用性 VPN 服务 在 VPN 连接上支持静态路由或动态边界网关协议 (BGP) 对等和路由策略	可能需要额外的电信和托管服务提供商关系或配置新的网络电路 您负责实现冗余和故障转移（如果需要） 远程设备必须支持单跳 BGP（利用 BGP 进行动态路由时）
AWS Direct ConnectAWS Transit Gateway + AWS Site-to-Site VPN	IPsec 通过专线与区域路由器进行多个 VPN 连接 VPCs	与之前的选项相同 AWS 管理了高可用性和可扩展性的区域网络中心，最多可容纳 5,000 个附件	与之前的选项相同

选项	使用场景	优点	限制
AWS VPN CloudHub	以主连接或备份连接 hub-and-spoke模式连接远程分支机构	重复使用现有的互联网连接和 AWS VPN 连接 AWS 托管的高可用性 VPN 服务 支持 BGP 用于交换路由和路由优先级	网络延迟、可变性和可用性取决于互联网 用户管理的分支机构端点负责实现冗余和故障转移（如果需要）
AWS Transit Gateway + 软件定义广域网解决方案	使用 AWS 主干网或互联网作为传输网络，将远程分支机构和办公室与软件定义的广域网连接起来。	支持更多的 SD-WAN 供应商、产品和协议 一些供应商解决方案已与 AWS 原生服务集成。	如果将 SD-WAN 设备放置在 Amazon VPC 中，则您有责任实现高可用性（高可用性）。
软件 VPN	通过互联网进行基于软件设备的 VPN 连接	支持更多的 VPN 供应商、产品和协议 完全由客户管理的解决方案	您负责为所有 VPN 端点实施 HA（高可用性）解决方案（如果需要）

AWS Site-to-Site VPN

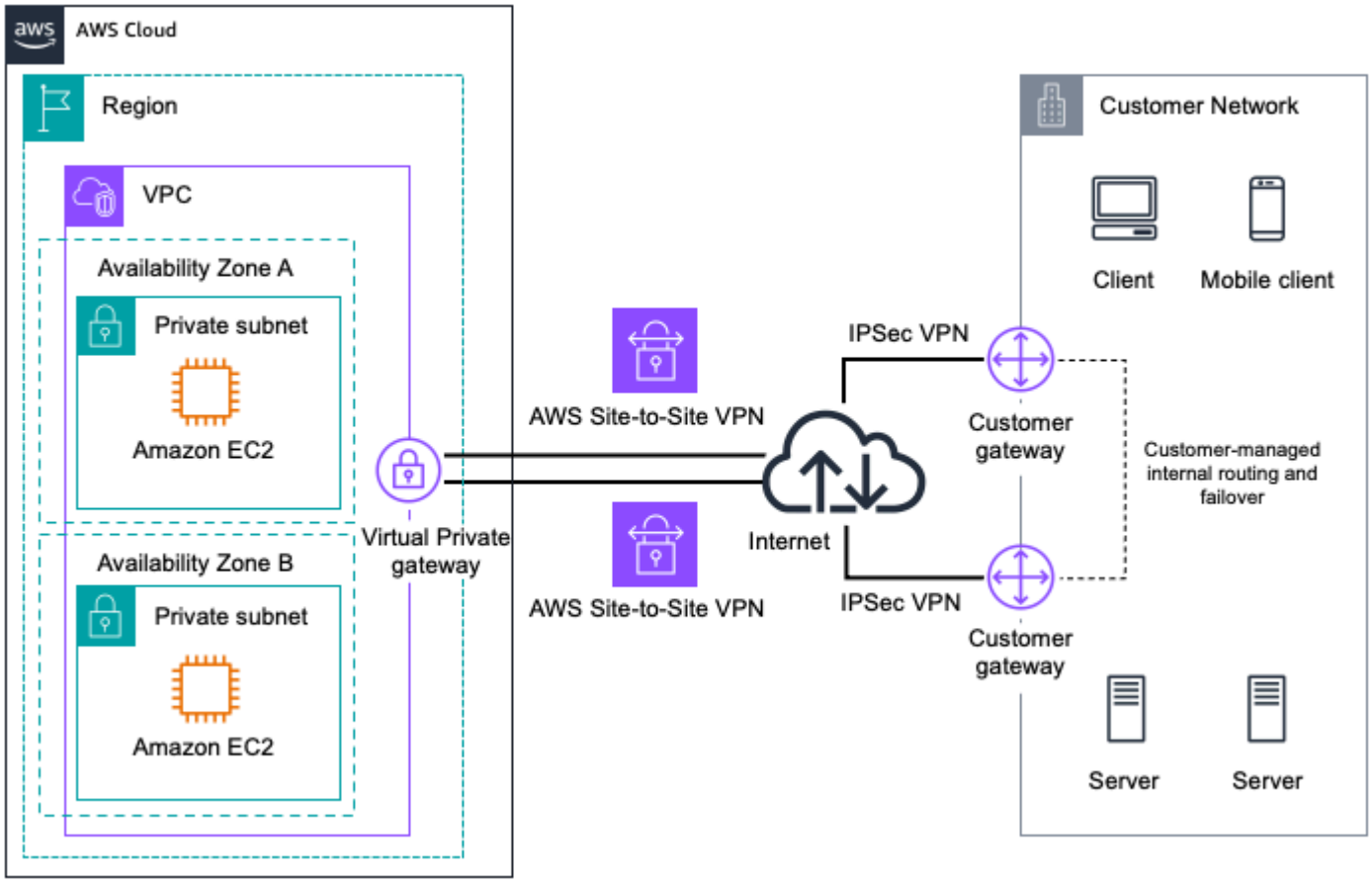
Amazon VPC 提供了通过互联网在您的远程网络和 Amazon VPC 之间创建 VP IPsec N 连接的选项，如下图所示。



AWS Managed VPN

如果您想利用 AWS 托管的 VPN 终端节点，该终端节点包括 VPN 连接的 AWS 端内置的自动冗余和故障转移，请考虑采用这种方法。

虚拟专用网关还支持并鼓励使用多个用户网关连接，以便您可以在 VPN 连接的自己端实现冗余和故障转移，如下图所示。



Redundant AWS Site-to-Site VPN Connections

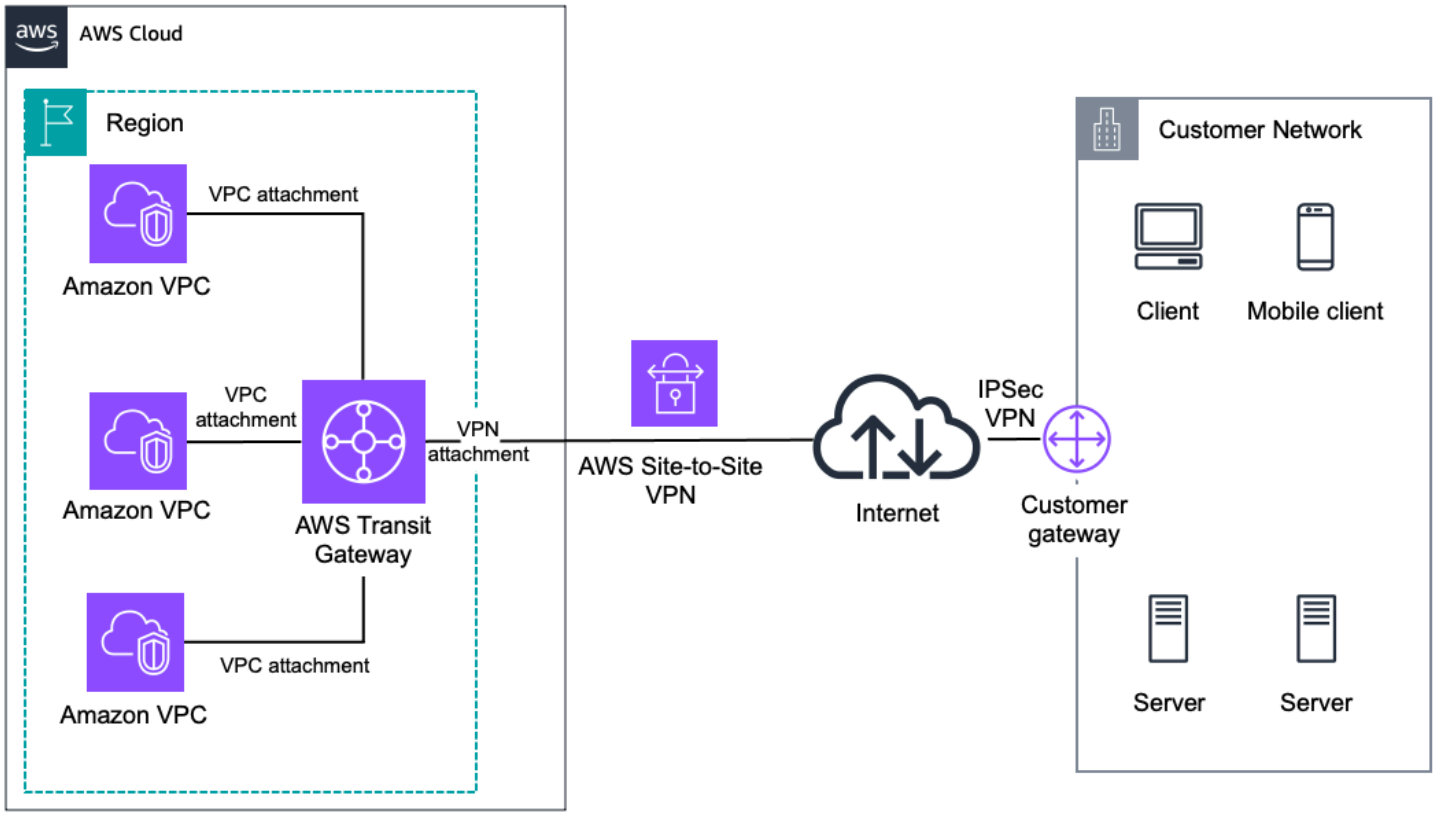
提供了动态和静态路由选项，使您的路由配置更加灵活。动态路由使用 BGP 对等互连在 AWS 和这些远程终端节点之间交换路由信息。借助动态路由，您还可以在 BGP 广告中指定路由优先级、策略和权重（指标），并影响您的网络与 AWS 之间的网络路径。请务必注意，使用 BGP 时， IPsec 和 BGP 会话必须在同一个用户网关设备上终止，因此它必须能够终止两者 IPsec 和 BGP 会话。

其他 资源

- AWS Site-to-Site VPN 用户指南
- 对客户网关设备的要求
- 使用 Amazon VPC 测试的客户网关设备

AWS Transit Gateway + AW Site-to-Site S

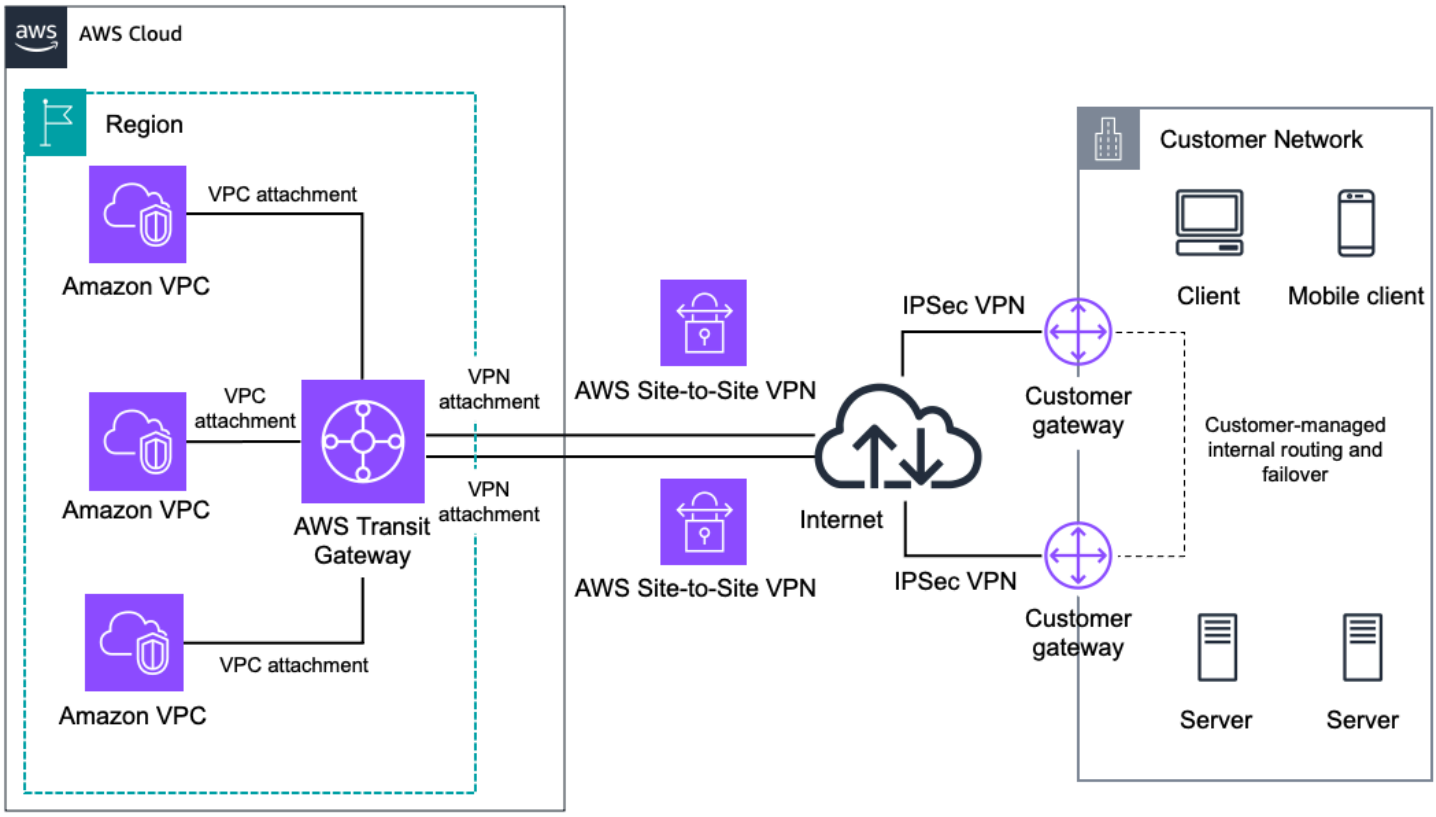
AWS Transit Gateway 是一个 AWS 托管的高可用性和可扩展性的区域网络中转中心，用于互连 VPCs 和客户网络。使用 Transit Gatewa y VPN 附件的 AWS Tr ansit Gateway + IPsec VPN 提供了通过互联网在远程网络和 Transit Gateway 之间创建 VPN 连接的选项，如下图所示。



AWS Transit Gateway and AWS Site-to-Site VPN

如果您想利用 AWS 托管的 VPN 终端节点连接到同一地区的多个 VPN 终端节点，而无需支付额外费用，也无需管理多个 VPCs Amazon 的多个 IPsec VPN 连接，则可以考虑使用这种方法。 VPCs

AWS Transit Gateway 还支持并鼓励使用多个用户网关连接，这样您就可以在 VPN 连接的自己端实现冗余和故障转移，如下图所示。

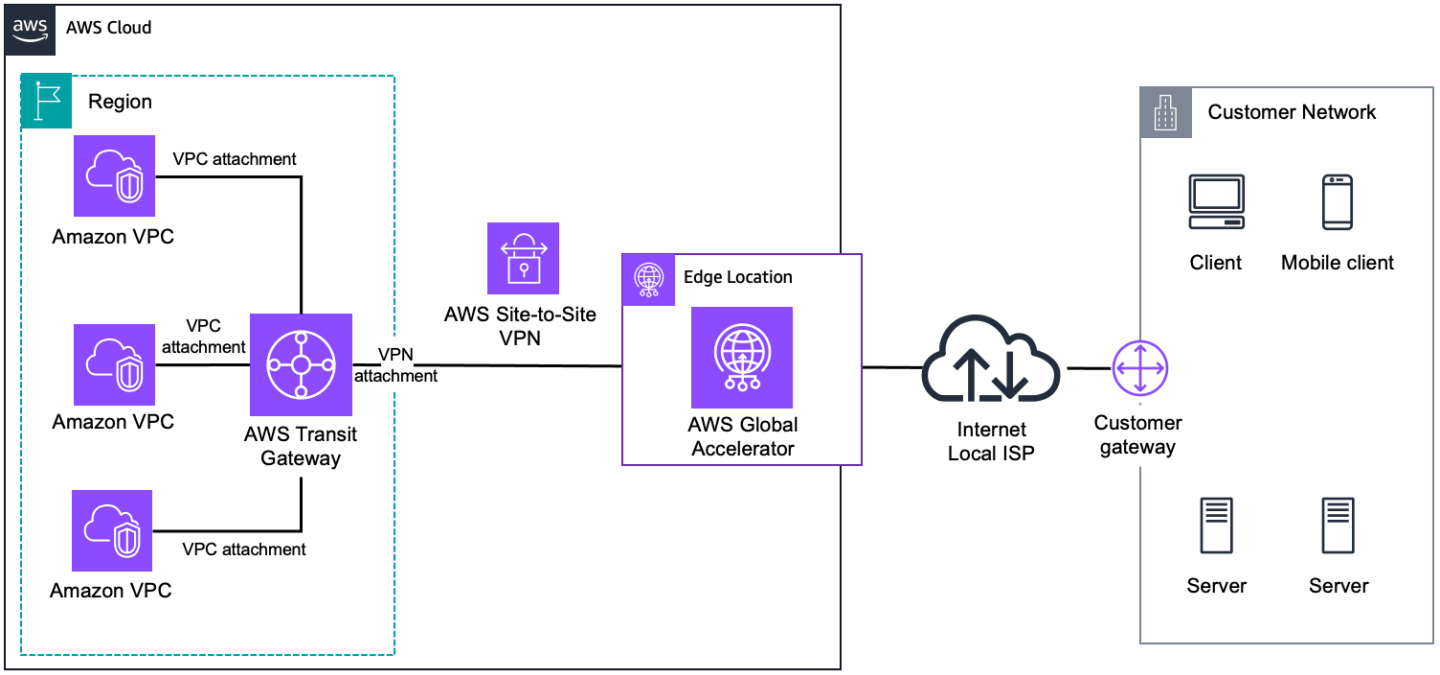


AWS Transit Gateway and Redundant VPN

提供了动态和静态路由选项，使您可以灵活地在 Transit Gateway VPN IPsec 连接上进行路由配置。动态路由使用 BGP 对等互连在 AWS 和这些远程终端节点之间交换路由信息。借助动态路由，您还可以在 BGP 广告中指定路由优先级、策略和权重（指标），并影响您的网络与 AWS 之间的网络路径。请务必注意，使用 BGP 时， IPsec 和 BGP 会话必须在同一个用户网关设备上终止，因此它必须能够终止两者 IPsec 和 BGP 会话。

每个 VPN 连接可以实现 1.25 Gbps 的吞吐量和每秒 140,000 个数据包。在 Transit Gateway 中终止 VPN 连接时，您可以使用等价多路径 (ECMP) 路由，通过聚合多个 VPN 隧道来获得更高的 VPN 带宽。要使用 ECMP，您需要在 VPN 连接中配置动态路由 — 使用静态路由不支持 ECMP。

此外，您还可以在 AWS Site-to-Site VPN 连接中启用加速。加速 VPN 连接使用 AWS Global Accelerator 将流量从您的网络路由到离您的客户网关设备最近的 AWS 边缘站点。您可以使用此选项来避免在通过公共 Internet 路由流量时可能发生的网络中断。只有连接到 Transit Gateway 的 VPN 连接才支持加速，如下图所示：



Accelerated AWS Site-to-Site VPN

最后，关于 IP 寻址、 AWS Transit Gateway 支持的 Site-to-Site VPN 连接 IPv4 和 IPv6 流量。以下规则适用：

- IPv6 仅支持 VPN 隧道的内部 IP 地址。 AWS 端点的外部 IP 地址是公有 IPv4 地址。客户网关 IP 地址应为公共 IPv4 地址。
- Site-to-SiteVPN 连接不能同时支持 IPv4 和 IPv6 流量。如果您的混合连接需要双栈通信，则应为 IPv4 和 IPv6 流量创建不同的 VPN 隧道。

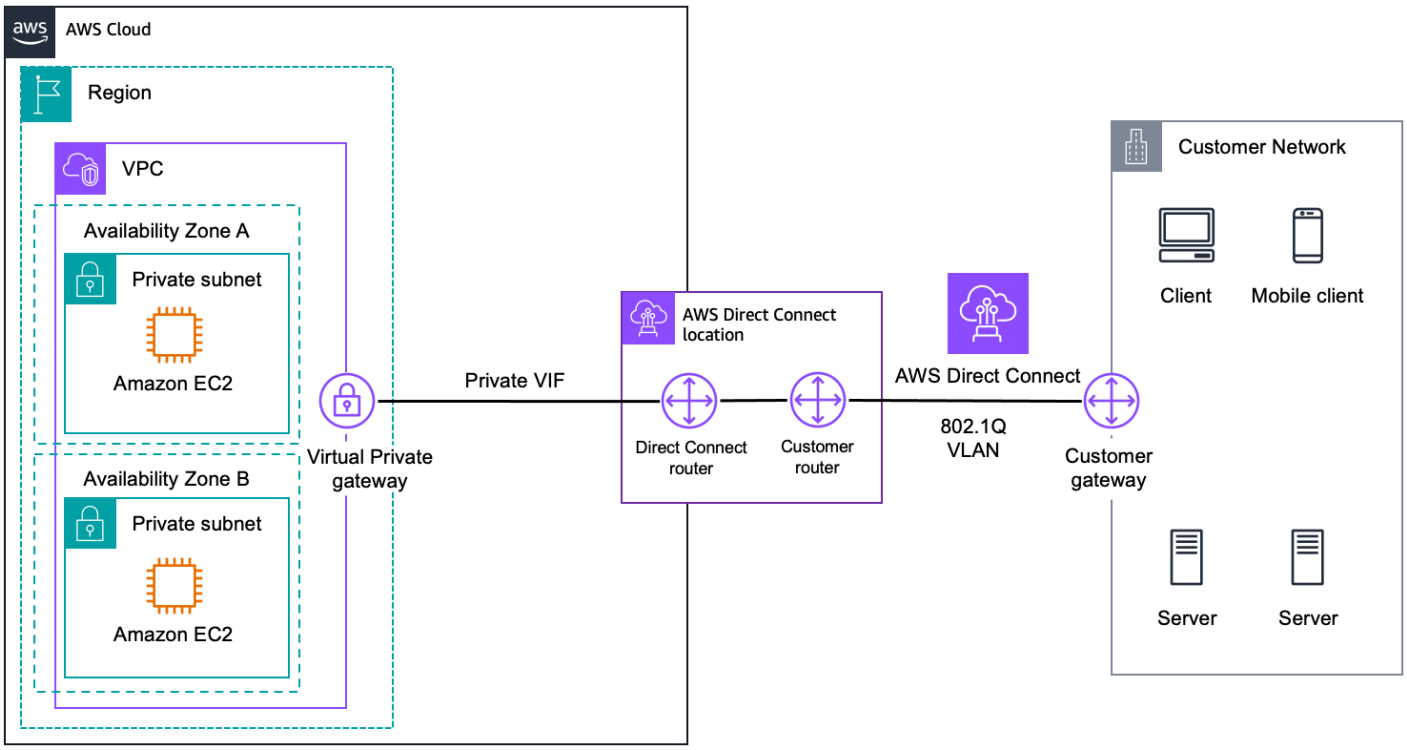
其他 资源

- 中转网关 VPN 附件
- 客户网关
- 使用 Site-to-Site VPN
- 加速 Site-to-Site VPN 连接

AWS Direct Connect

AWS Direct Connect可以轻松建立从本地网络到一个或多个本地网络的专用连接 VPCs。 AWS Direct Connect 可以降低网络成本、增加带宽吞吐量，并提供比基于 Internet 的连接更稳定的网络体验。它使用行业标准 802.1Q 通过私有 VLANs IP 地址连接亚马逊 VPC。使用虚拟接口 (VIFs) 进行配置，您可以配置三种不同的类型 VIFs： VLANs

- 公共虚拟接口-在 AWS 公共端点与您的数据中心、办公室或托管环境之间建立连接。
- Transit 虚拟接口-在您的数据中心、办公室或托管环境之间 AWS Transit Gateway 建立私有连接。此连接选项将在本节中介绍???。
- 私有虚拟接口-在 Amazon VPC 资源与您的数据中心、办公室或托管环境之间建立私有连接。私 VIFs 有化的用法如下图所示。



AWS Direct Connect

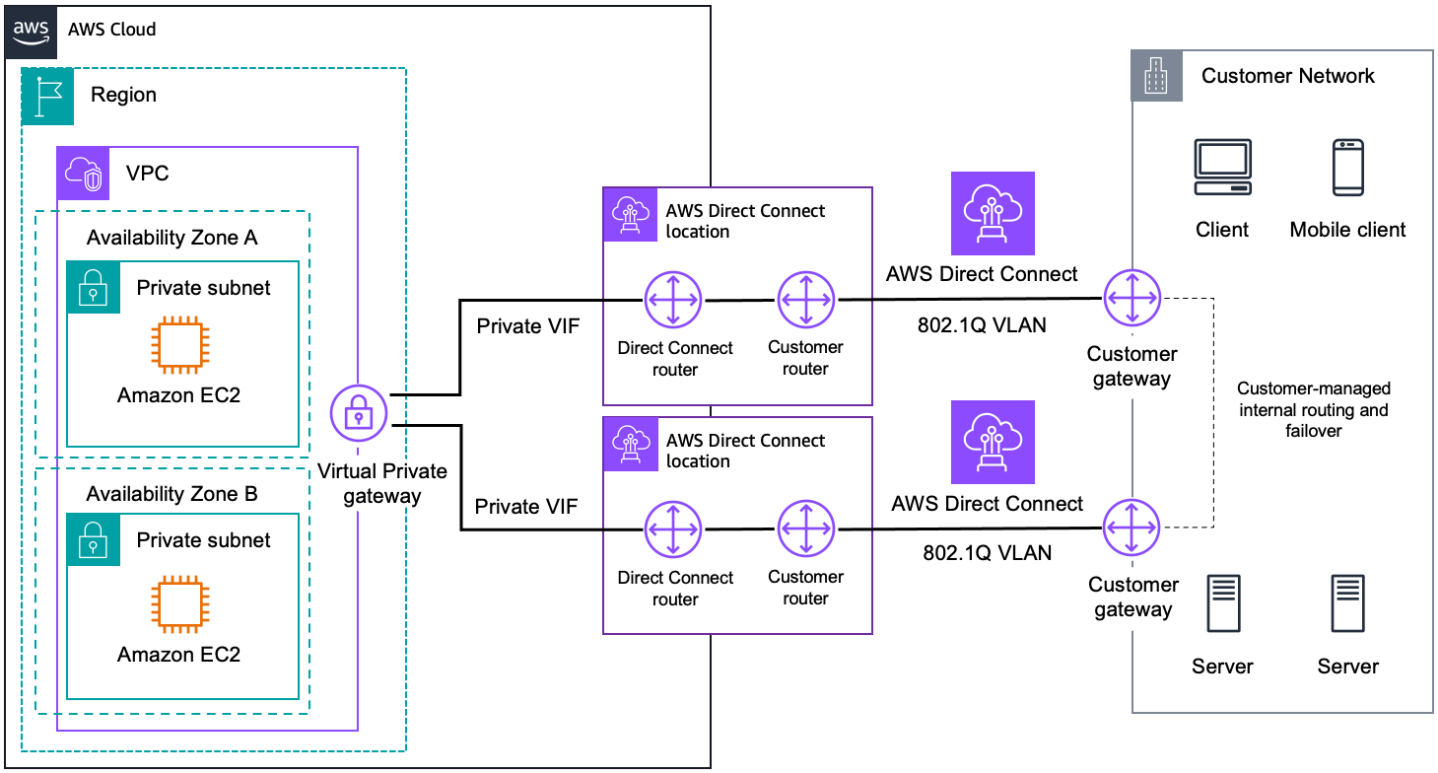
您可以 AWS Direct Connect 通过在 Direct Connect 位置建立与 Di rect Connect 位置的 AWS 设备的交叉连接来建立与 AWS 主干网的连接。您可以从我们的任何 Direct Connect 网点（中国除外）访问任何 AWS 区域。如果您在某个地点没有设备，则可以从 WAN 服务提供商生态系统中进行选择，将您的 AWS Direct Connect 终端节点与远程网络集成。 AWS Direct Connect

使用 AWS Direct Connect，您有两种类型的连接：

- 专用连接，其中物理以太网连接与单个客户关联。您可以订购 1、10 或 100 Gbps 的端口速度。您可能需要与合作伙伴计划中的合作伙伴合作，以帮助您在 AWS Direct Connect 连接与数据中心、办公室或托管环境之间建立网络回路。 AWS Direct Connect
- 托管连接，其中物理以太网连接由 AWS Direct Connect 合作伙伴配置并与您共享。您可以订购介于 50 Mbps 和 10 Gbps 之间的端口速度。您与合作伙伴在他们建立的 AWS Direct Connect 连接以及连接与您的数据中心、办公室或托管环境之间的网络电路 AWS Direct Connect 方面进行合作。

对于专用连接，您还可以使用链路聚合组 (LAG) 在单个 AWS Direct Connect 终端节点上聚合多个连接。您可以将它们视为单一的托管连接。您最多可以聚合四个 1 或 10-Gbps 的连接，以及最多两个 100-Gbps 的连接。

在中讨论高可用性时 AWS Direct Connect，我们建议使用其他 AWS Direct Connect 连接。R AWS Direct Connect esiliency Toolkit 为在数据中心、办公室或托管环境之间 AWS 建立高弹性的网络连接提供了指导。下图显示了高弹性连接选项的示例，其中两个连接在两个 AWS Direct Connect 不同的 AWS Direct Connect 位置终止。

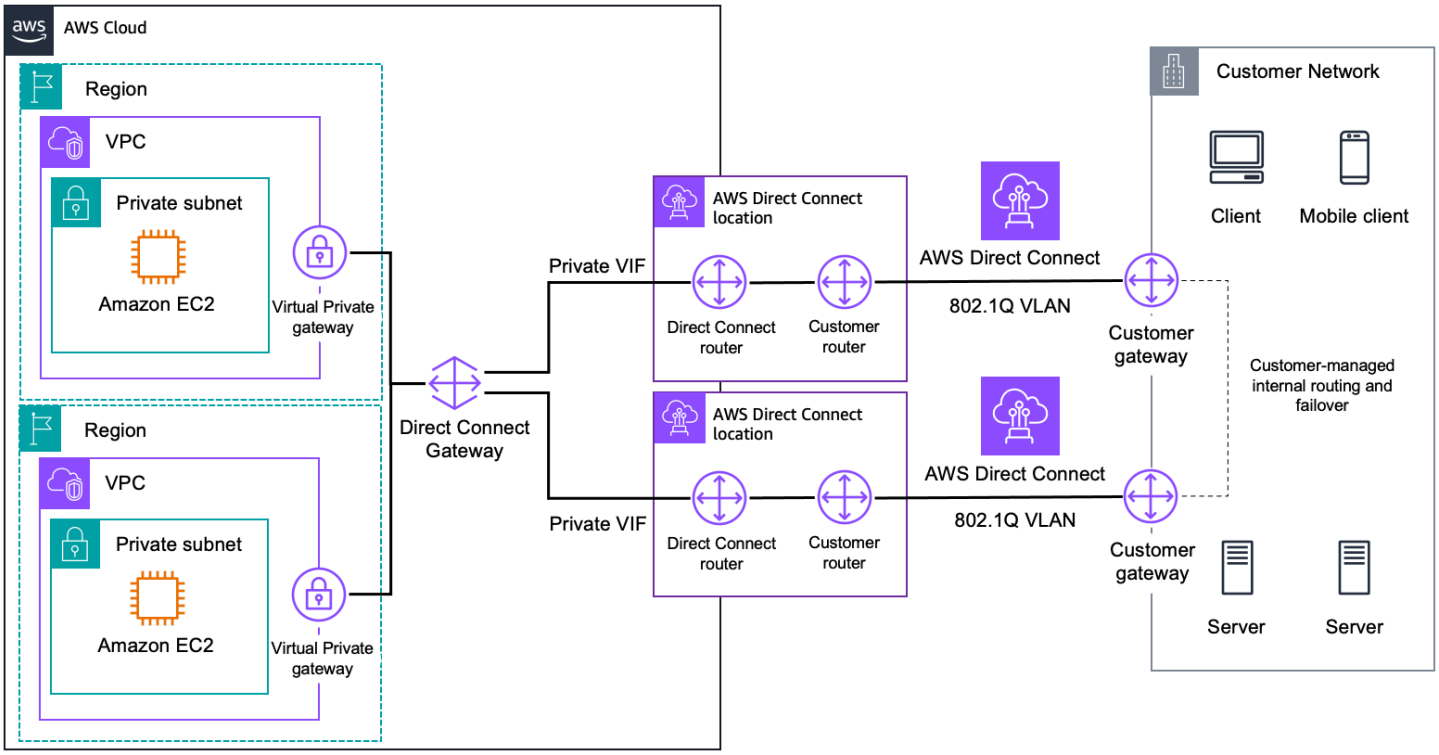


冗余 AWS Direct Connect

AWS Direct Connect 默认情况下未加密。对于 10 或 100 Gbps 的专用连接，您可以使用 MAC 安全 (MACsec) 作为加密选项。对于 1 Gbps 或更低的连接，您可以在连接之上创建 VPN 隧道——此选

项将在AWS Direct Connect + AWS Site-to-Site VPN和AWS Direct ConnectAWS Transit Gateway + AWS Site-to-Site VPN章节中介绍。

其中一项重要资源 AWS Direct Connect 是 Direct Connect 网关，它是一种全球可用的资源，可以跨不同地区或 AWS 账户连接到多个 Amazon VPCs 或 Transit Gateway。该资源还允许您从一个私有 VIF 或中转 VIF 连接到任何参与的 VPC 或 Transit Gateway，从而减少 AWS Direct Connect 管理，如下图所示。



AWS Direct Connect Gateway

关于 IP 寻址， AWS Direct Connect 虚拟接口同时支持双栈 IPv4 操作和 IPv6 BGP 会话。

- 私有和传输 VIFs IPv4 配置使用 AWS 生成 IPv4 的地址或由您配置的地址。对于公共 VIFs IPv4 BGP 对等互连，您必须指定自己拥有的唯一公共 /31 IPv4 CIDR（或提交请求以分配 CIDR 块）。
- 对于所有类型的 VIFs IPv6 BGP 对等互连，AWS 会分配一个 /125 CIDR，这是不可配置的。

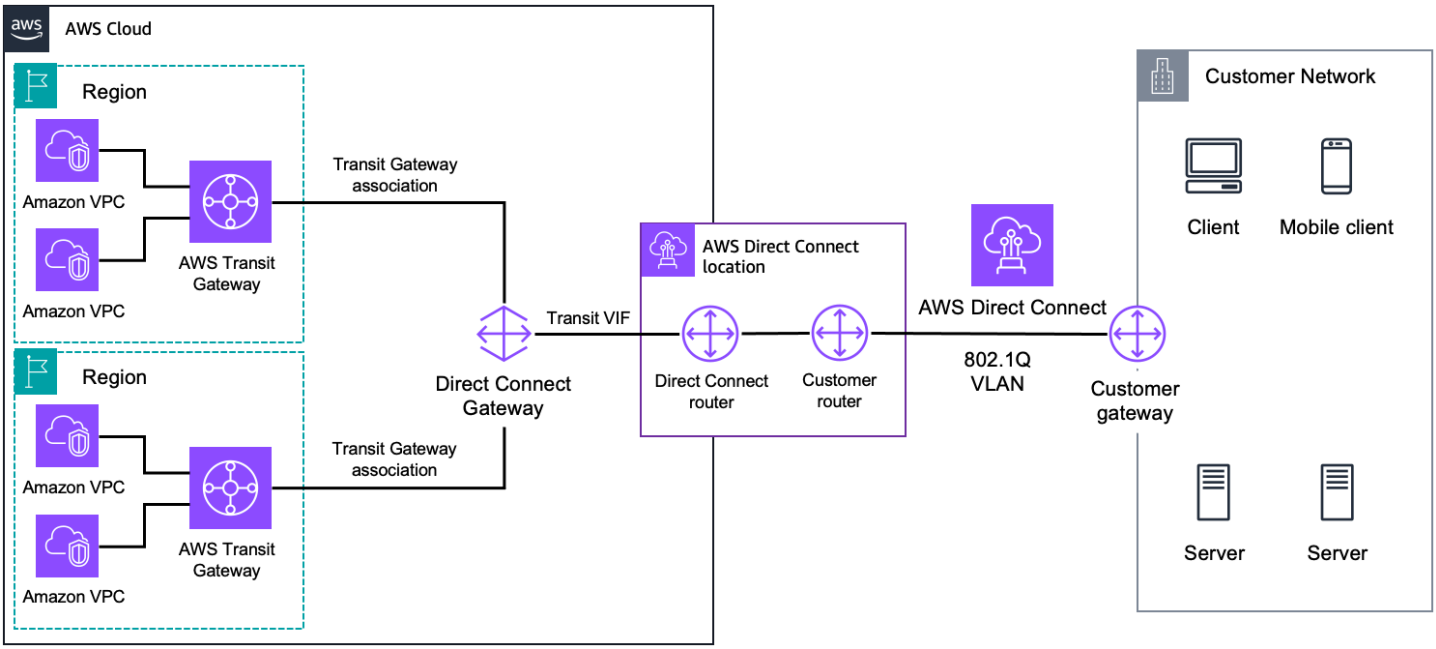
其他 资源

- AWS Direct Connect 用户指南
- AWS Direct Connect 虚拟接口
- AWS Direct Connect 网关

- AWS Direct Connect 弹性工具包
- AWS Direct Connect MAC 安全
- AWS Direct Connect 地点
- AWS Direct Connect 配送合作伙伴

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect+ AWS Transit Gateway，使用与 Di rect Connect 网关的传输 VIF 连接，使您的网络能够通过专用连接连接多个区域集中式路由器。下图显示了连接到两台路由器的情况。



AWS Direct Connect and AWS Transit Gateway

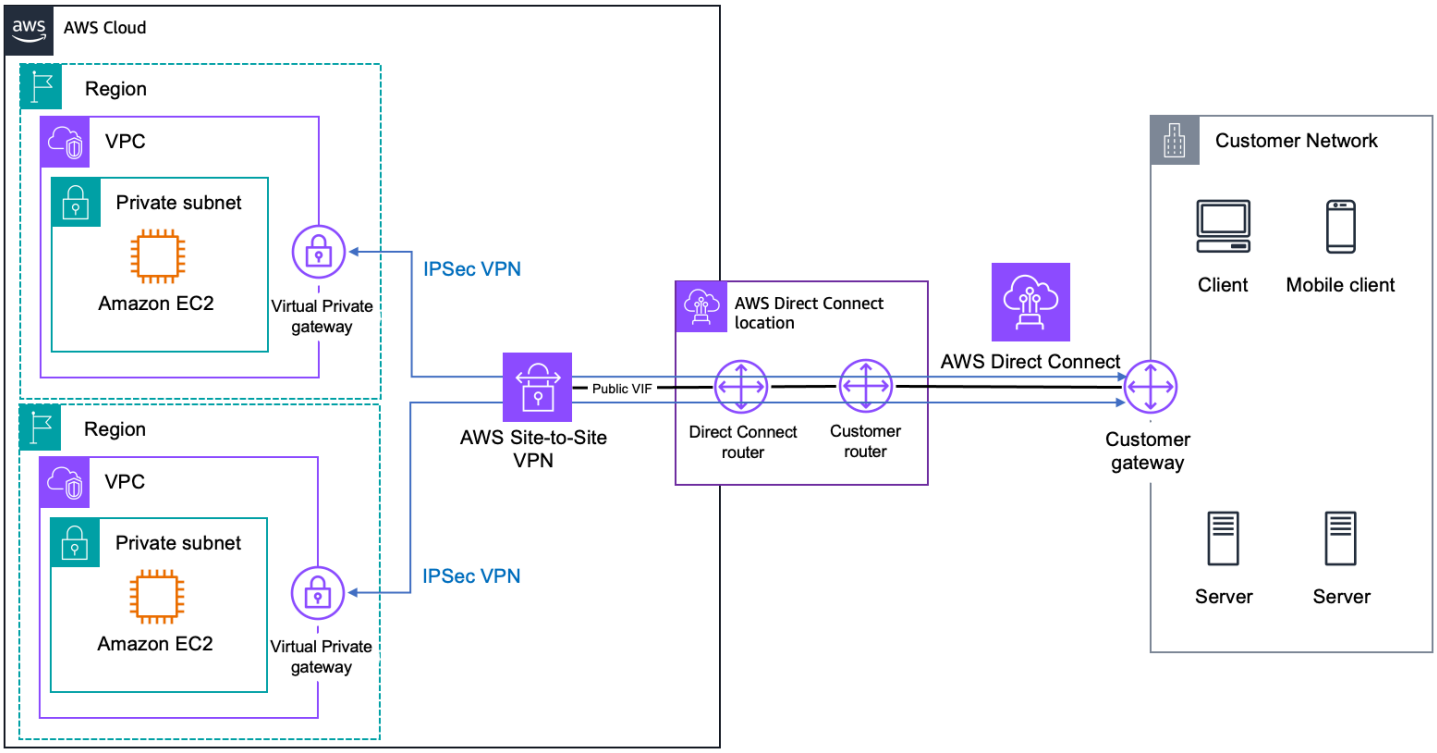
每个都 AWS Transit Gateway 是一个网络 VPCs 中转枢纽，可在同一区域内互连，将 Amazon VPC 路由配置整合到一个地方。该解决方案简化了 Amazon VPC 与您的网络之间通过私有连接的连接的管理，与基于互联网的连接相比，可以降低网络成本、增加带宽吞吐量并提供更稳定的网络体验。

其他 资源

- AWS Direct Connect 用户指南
- 中的链路聚合组 AWS Direct Connect
- 博客文章：将低于 1 Gbps 的托管连接与 AWS Transit Gateway 集成

AWS Direct Connect + AWS Site-to-Site VPN

使用 AWS Direct Connect+ AWS Site-to-Site VPN，您可以将 AWS Direct Connect 连接与 AWS 托管的 VPN 解决方案相结合。 AWS Direct Connect pub VIFs lic 在您的网络和公有 AWS 资源（例如 AWS Site-to-Site VPN 终端节点）之间建立专用的网络连接。建立与服务的连接后，您可以创建与相应的 Amazon VPC 虚拟私有网关的 IPsec 连接。下图说明了此选项。



AWS Direct Connect and AWS Site-to-Site VPN

该解决方案将 end-to-end安全 IPsec 连接的优势与低延迟和更高的带宽相结合，可提供比基于互联网的 VPN 连接更稳定的网络体验。 AWS Direct Connect 在公共 VIF 上与您的路由器 AWS Direct Connect 之间建立 BGP 连接会话。将在 VP IPsec N 隧道上的虚拟专用网关和您的路由器之间建立另一个 BGP 会话或静态路由。

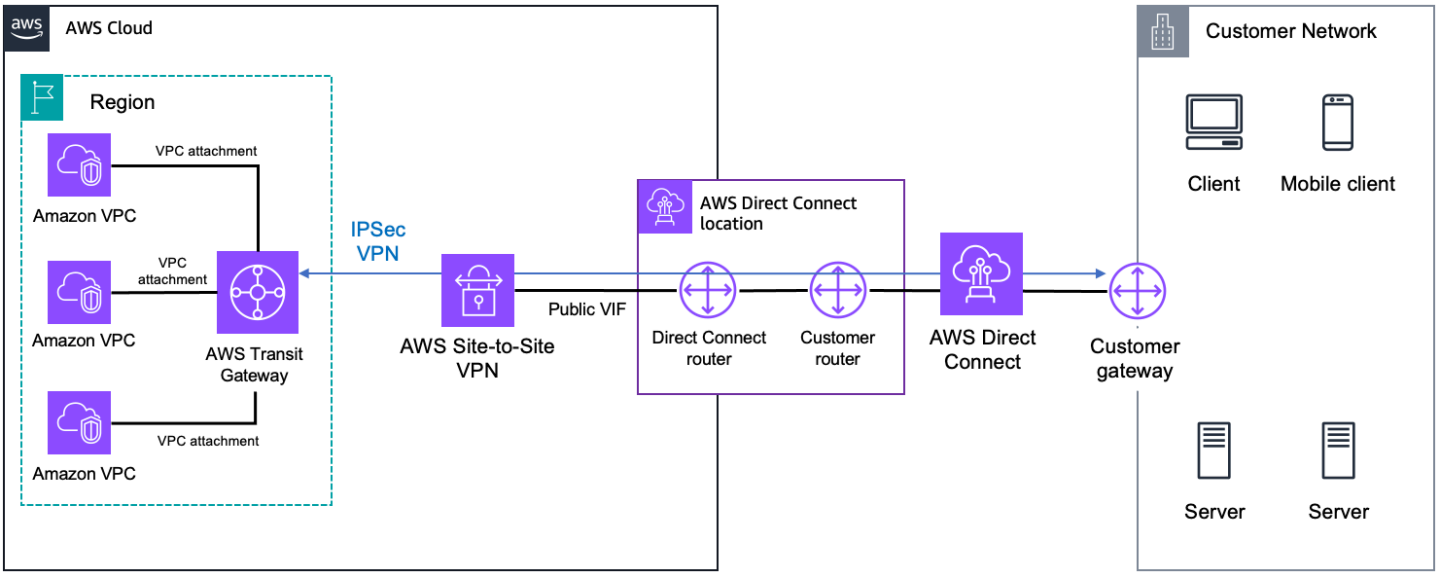
其他 资源

- AWS Direct Connect
- AWS Direct Connect 虚拟接口
- AWS Site-to-Site VPN 用户指南

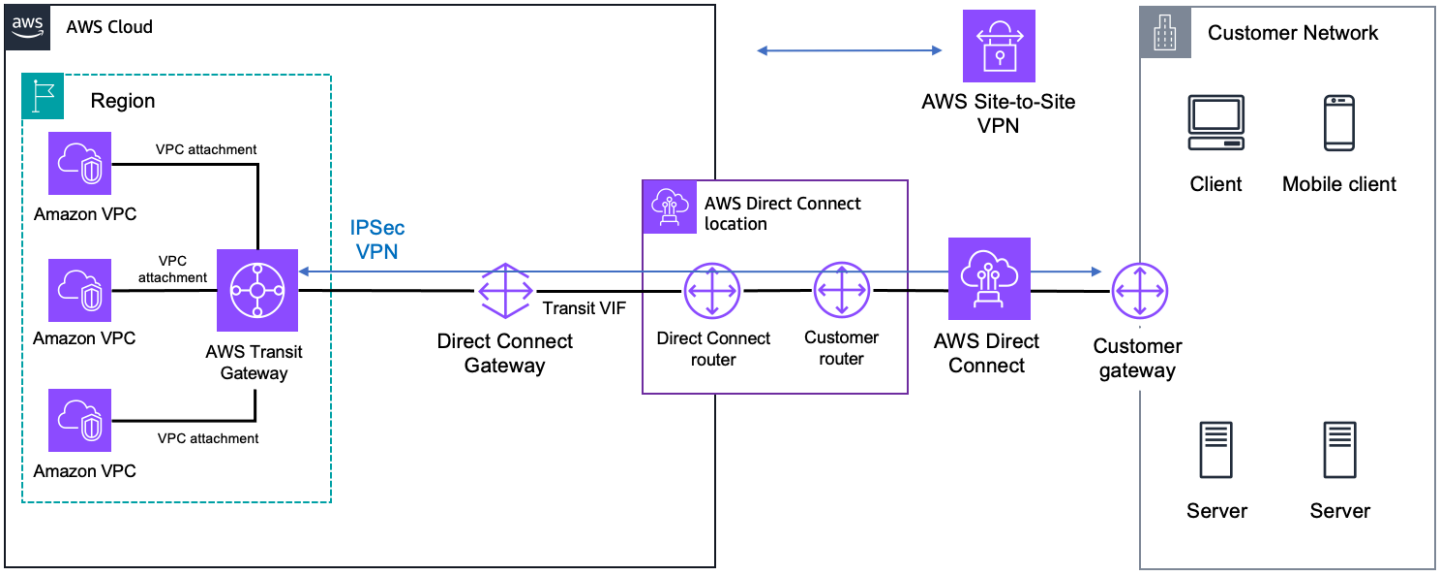
AWS Direct ConnectAWS Transit Gateway + AWS Site-to-Site VPN

使用 AWS Direct Connect+ AWS Transit Gateway+ AWS Site-to-Site VPN，您可以通过私有专用连接在您的网络和 Amazon VPCs 的区域集中式路由器之间启用 end-to-end IPsec加密连接。

您可以先使用 AWS Direct Connect 公共 VIFs 在您的网络与公有 AWS 资源（例如 AWS Site-to-Site VPN 终端节点）之间建立专用的网络连接。建立此连接后，您可以创建 IPsec 与的连接 AWS Transit Gateway。下图说明了此选项。



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (public VIF)



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (transit VIF)

当您想要简化管理并最大限度地降低与同一地区多个 Amazon VPCs 的 IPsec VPN 连接的成本时，可以考虑采用这种方法，同时通过基于互联网的 VPN 使用私有专用连接具有低延迟和一致的网络体验优势。使用公共或中转 VIF 在路由器 AWS Direct Connect 与您的路由器之间建立 BGP 会话。将在 VP IPsec N 隧道上与您的路由器之间 AWS Transit Gateway 建立另一个 BGP 会话或静态路由。

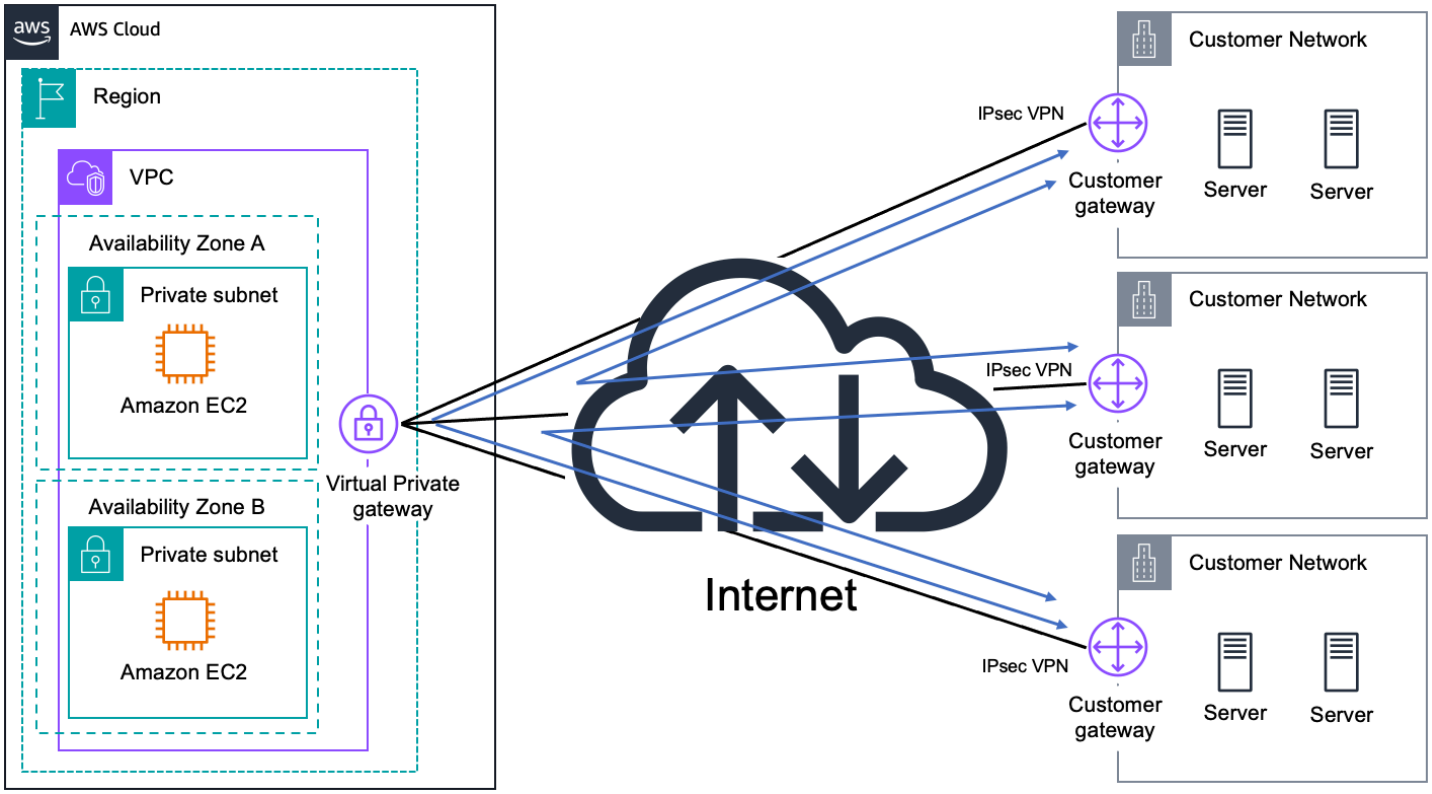
其他 资源

- AWS Direct Connect 虚拟接口
- 中转网关 VPN 附件
- 对客户网关设备的要求
- 使用 Amazon VPC 测试的客户网关设备
- AWS Site-to-Site VPN — 私有 IP VPN 带有 AWS Direct Connect

AWS VPN CloudHub

基于前面介绍的 AWS 托管 VPN 选项，您可以使用安全地从一个站点与另一个站点进行通信 AWS VPN CloudHub。在一个简单 hub-and-spoke模型上 AWS VPN CloudHub 运行，无论是否有 VPC，您都可以使用该模型。如果您有多个分支机构和现有的互联网连接，并且希望为这些远程办公室之间的主连接或备份连接实施一种方便、可能低成本的 hub-and-spoke模式，请使用这种方法。

下图显示了 AWS VPN CloudHub 架构，其中的线条表示远程站点之间的网络流量通过其 AWS VPN 连接进行路由。



AWS VPN CloudHub

AWS VPN CloudHub 使用带有多个客户网关的 Amazon VPC 虚拟私有网关，每个网关使用唯一的 BGP 自治系统编号 (ASNs)。远程站点的 IP 范围不得重叠。您的网关通过其 VPN 连接通告相应的路由（BGP 前缀）。这些路由通告会被接收并重新通告给每个 BGP 对等体，以便每个站点都可以向其他站点发送数据和从其他站点接收数据。

其他 资源

- 使用 VPN 在站点之间提供安全的通信 CloudHub
- AWS Site-to-Site VPN 用户指南
- 对客户网关设备的要求
- 使用 Amazon VPC 测试的客户网关设备

AWS Transit Gateway + 软件定义广域网解决方案

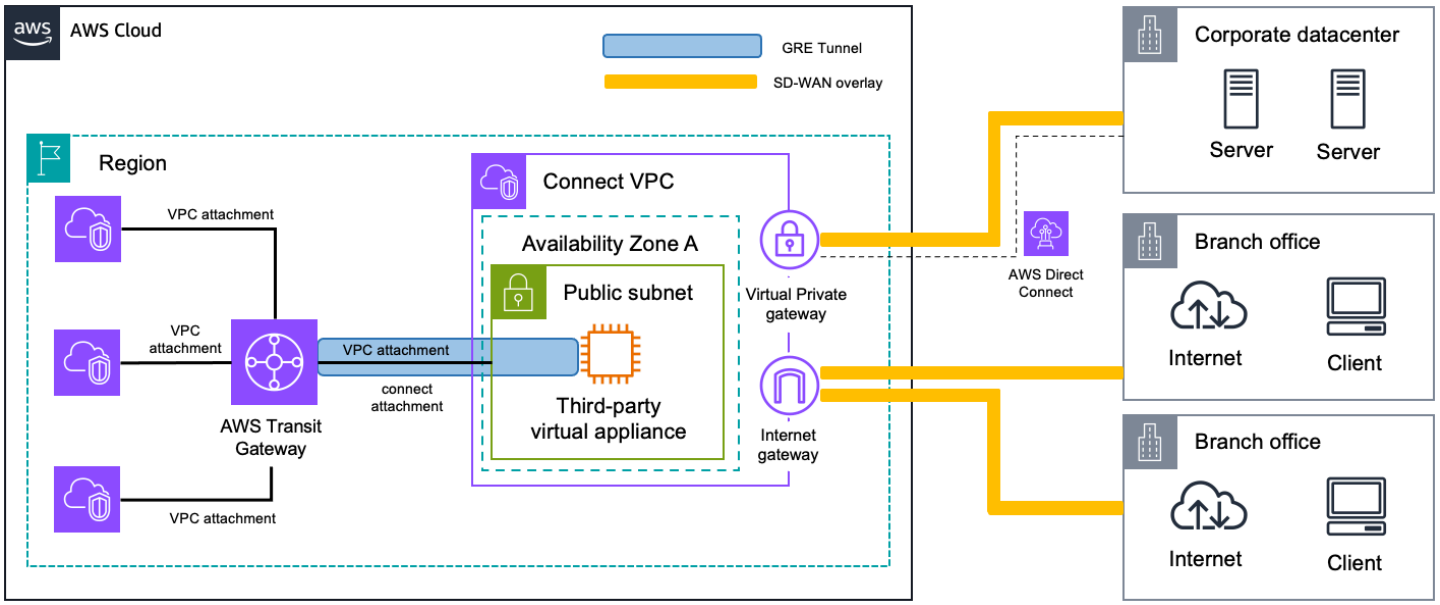
软件定义的广域网 (SD-WANs) 用于通过不同的传输网络（例如使用公共互联网、MPLS 网络或 AWS 主干网络）连接您的数据中心、办公室或托管环境，根据网络条件、应用程序类型或服务质量 (QoS AWS Direct Connect) 要求，在最合适、最有效的路径上自动动态地管理流量。

如果您的网络拓扑很复杂，有多个数据中心、办公室或托管环境需要相互通信以及与 AWS 进行通信，请使用这种方法。SD-WAN 解决方案可以帮助您高效管理此类网络。

在谈论 SD-WAN 网络与 AWS 的连接时， AWS Transit Gateway 提供了一个托管的、高度可用且可扩展的区域网络传输中心，用于互连 VPCs 您的 SD-WAN 网络。Transit Gateway 连接附件提供了一种将您的 SD-WAN 基础设施和设备与 AWS 连接的原生方式。这使得无需进行设置即可轻松将软件定义广域网扩展到 AWS。 IPsec VPNs

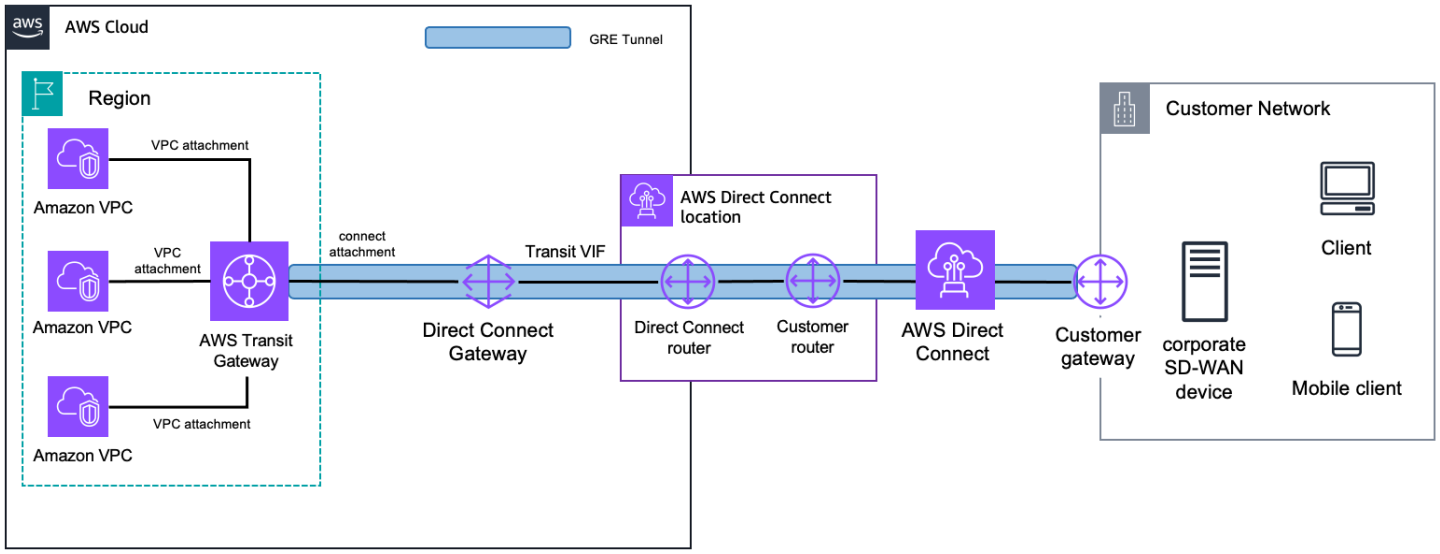
Transit Gateway 连接附件支持通用路由封装 (GRE)，与 VPN 连接相比，带宽性能更高。它支持用于动态路由的边界网关协议 (BGP)，并且无需配置静态路由。这简化了网络设计并降低了相关的运营成本。此外，它与 T ransit Gateway Network Manager 的集成通过全球网络拓扑、连接级别性能指标和遥测数据提供了高级可见性。

使用连接附件将 SD-WAN 网络集成到 Transit Gateway 时，有两种常见的模式。第一个是将 SD-WAN 网络的虚拟设备放在 AWS 内的 VPC 中。然后，您可以使用 VPC 附件作为虚拟设备和 Transit Gateway 之间的 Transit Gateway 连接连接的底层传输，如下图所示。



SD-WAN connectivity with AWS Transit Gateway (virtual appliance in AWS)

或者，您无需添加额外的基础设施即可将您的 SD-WAN 流量扩展到 AWS 并将其分段。您可以使用连接作为底层传输来创建 Transit Gateway AWS Direct Connect 连接附件，如下图所示。



SD-WAN connectivity with AWS Transit Gateway (Direct Connect as transport)

使用 Transit Gateway 连接附件时，需要注意一些注意事项：

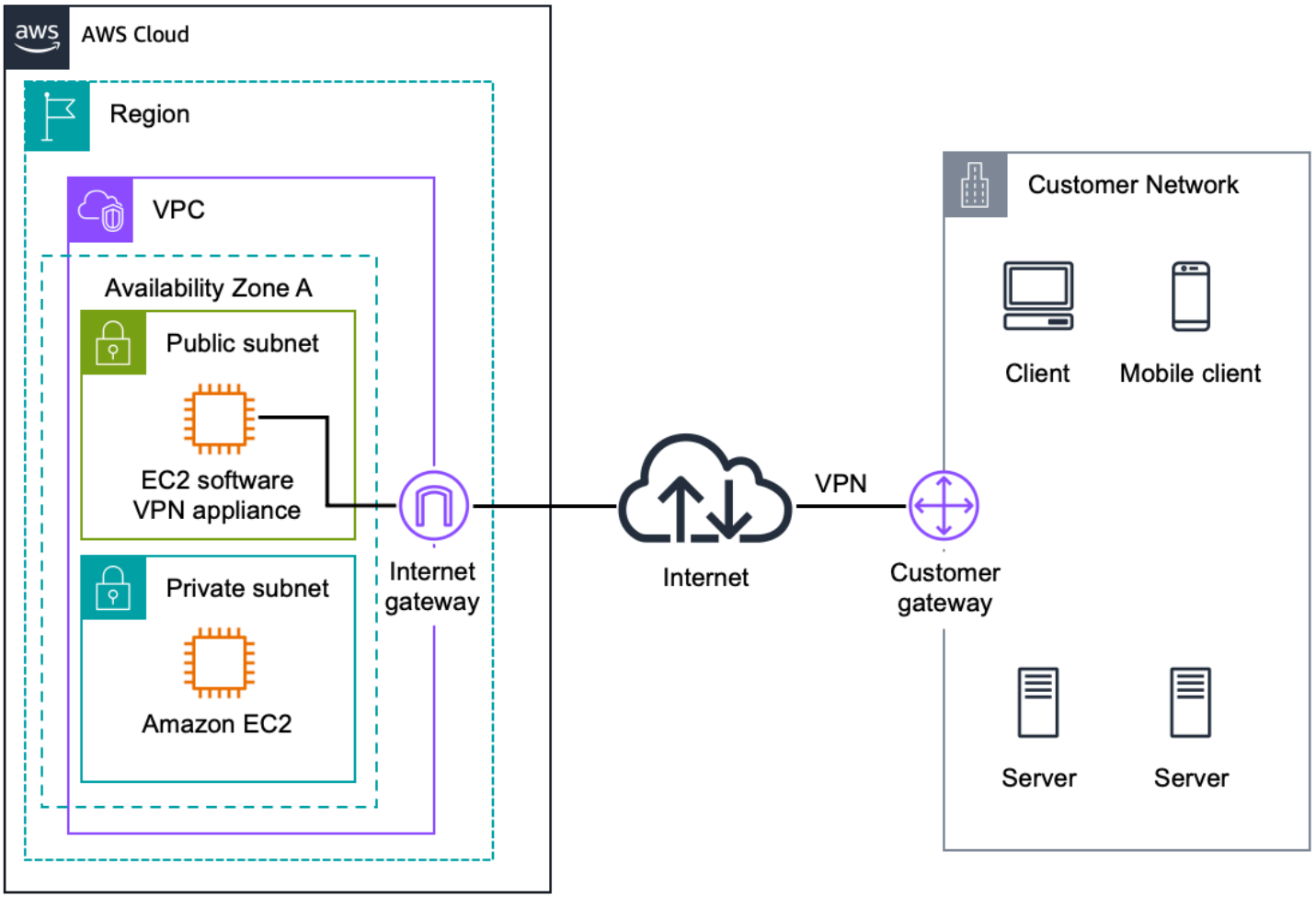
- 您可以在现有公交网关上创建连接附件。
- 第三方设备必须配置 GRE 隧道，才能使用连接附件发送和接收来自 Transit Gateway 的流量。设备必须配置 BGP 才能进行动态路由更新和运行状况检查。
- Connect 附件不支持静态路由。
- Transit Gateway 连接附件支持每个 GRE 隧道的最大带宽为五 Gbps。通过在多个 Connect 对等体（GRE 隧道）上为同一 Connect 附件通告相同的前缀，可以实现高于 5 Gbps 的带宽。
- 每个连接连接最多支持四个 Connect 对等体。
- Transit Gateway 通过 BGP 的多协议扩展（MBGP 或 MP-BGP）连接附件支持 IPv6 和动态路由通告。

其他 资源

- 中转网关对等连接挂载
- 要求和注意事项
- 博客文章：使用 AWS Transit Gateway Connect 简化软件定义广域网连接

软件 VPN

Amazon VPC 允许您在远程网络和亚马逊 VPC 网络中运行的软件 VPN 设备之间创建 VPN 连接，从而灵活地全面管理 Amazon VPC 连接的两端。如果您必须管理 VPN 连接的两端，无论是出于合规目的，还是为了利用 Amazon VPC 的 VPN 解决方案目前不支持的网关设备，则建议使用此选项。下图显示了此选项。



软件 Site-to-Site VPN

您可以从多个合作伙伴和开源社区组成的生态系统中进行选择，这些社区生产了在亚马逊上运行的软件 VPN 设备 EC2。除此选择外，您还必须负责管理软件设备，包括配置、补丁和升级。

请注意，此设计在网络设计中引入了潜在的单点故障，因为软件 VPN 设备运行在单个 Amazon EC2 实例上。有关更多信息，请参阅软件 VPN 实例的附录 A：软件 VPN 实例的高级高可用架构架构。

其他 资源

- 中提供的 VPN 设备 AWS Marketplace
- 技术简介-将 Cisco ASA 连接到 VPC EC2 实例 (IPsec)
- 技术简报-将多个 EC2 实例 VPCs 与实例连接 (IPsec)
- 技术简报-将多个 EC2 实例 VPCs 与实例连接 (SSL)

亚马逊 VPC-to-Amazon VPC 连接选项

当您想将多个 Amazon VPCs 集成到更大的虚拟网络中时，请使用这些设计模式。如果您 VPCs 出于安全、计费、在多个区域的存在或内部退款要求而需要多个，以便更轻松地在 Amazon 之间集成 AWS 资源，则此功能非常有用。 VPCs您还可以将这些模式与网络到 Amazon VPC 的连接选项相结合，以创建跨越远程网络和多个网络的公司网络。 VPCs

当对所连接的每个 VPC 使用非重叠的 IP 范围时，最好实现 VPC 之间的 VPCs 连接。例如，如果您想连接多个 VPC VPCs，请确保每个 VPC 都配置了唯一的无类域间路由 (CIDR) 范围。因此，我们建议您为每个 VPC 分配一个连续、不重叠的 CIDR 块。有关 Amazon VPC 路由和限制的更多信息，请参阅 Amazon VPC 常见问题解答。

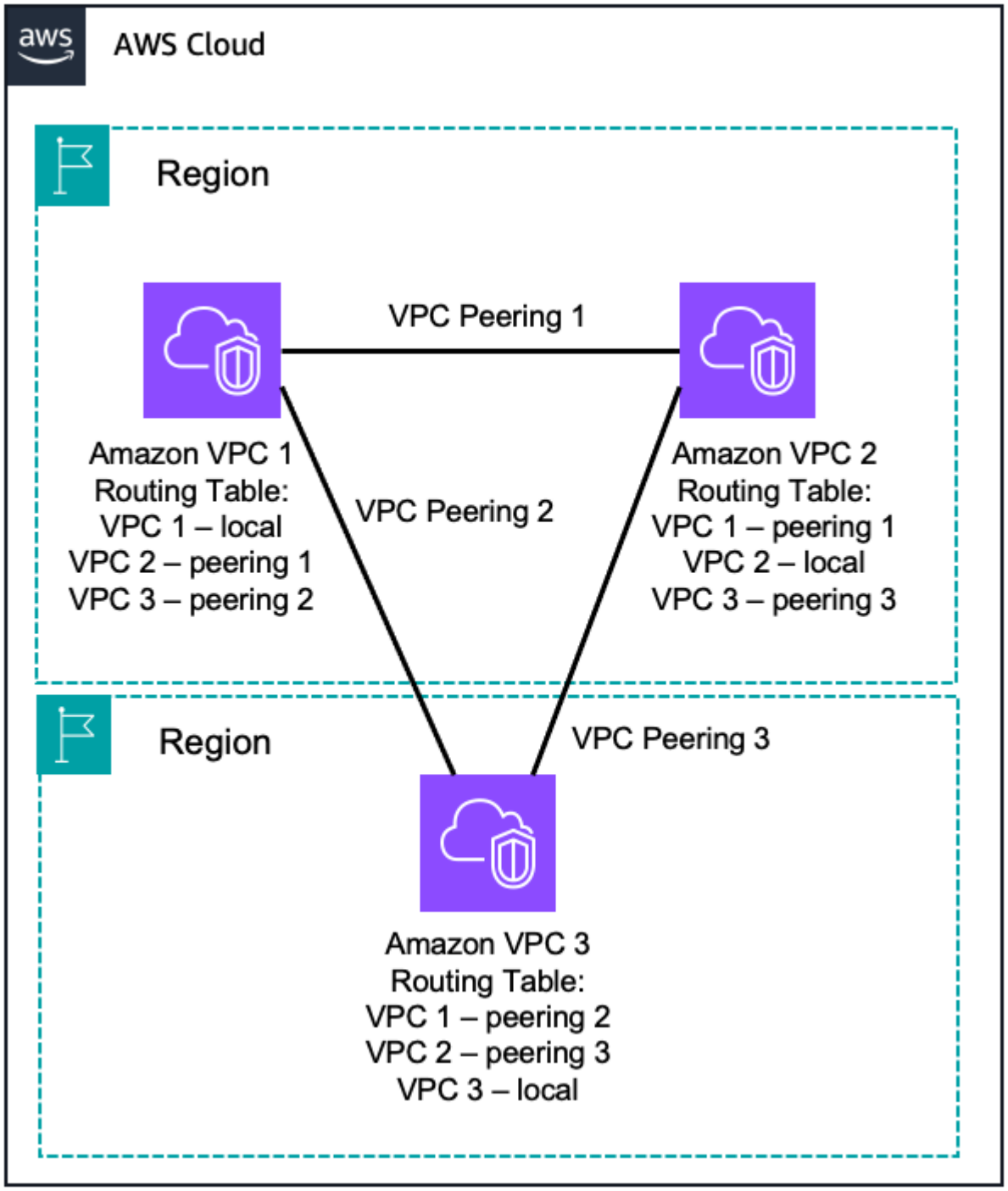
选项	使用场景	优点	限制
VPC 对等连接	AWS 提供的两者之间的网络连接。 VPCs	利用 AWS 托管的可扩展网络基础设施	VPC 对等互连不支持可传递的对等关系 难以大规模管理
AWS Transit Gateway	AWS 提供的区域路由器连接 VPCs	AWS 托管的高可用性和可扩展性服务 区域网络中心，可容纳多达 5,000 个附件	Transit Gateway 对等连接仅支持静态路由
AWS PrivateLink	AWS VPCs 使用接口端点在两者之间提供的网络连接	利用 AWS 托管的可扩展网络基础设施	VPC 终端节点服务仅在创建它们的 AWS 区域中可用
软件 VPN	之间基于软件设备的 VPN 连接 VPCs	支持各种 VPN 供应商、产品和协议 完全由您管理	您负责为所有 VPN 端点实施 HA 解决方案（如果需要） VPN 实例可能会成为网络瓶颈
软件 VPN-to-AWS Site-to-Site VPN	软件设备到 VPN 之间的连接 VPCs	AWS 托管的高可用性 VPC VPN 连接	您负责为软件设备 VPN 端点实施 HA 解决方案（如果需要）

选项	使用场景	优点	限制
		支持由您管理的各种 VPN 供应商和产品 支持静态路由和动态 BGP 对等和路由策略	VPN 实例可能会成为网络瓶颈 IPsec 仅适用于 AWS 托管 VPN 的 VPN 协议

VPC 对等连接

VPC 对等连接是两者之间的网络连接 VPCs ，它允许使用每个 VPC 的私有 IP 地址进行路由，就像它们在同一个网络中一样。可以在您自己的 VPC 之间 VPCs 或与其他 AWS 账户中的 VPC 之间创建 VPC 对等连接。VPC 对等互连还支持区域间对等。

使用区域间 VPC Peering 的流量始终保持在全球 AWS 主干上，并且永远不会穿越公共互联网，从而减少了威胁载体，例如常见漏洞利用和 S 攻击。 DDo



VPC-to-VPC Peering

AWS 使用 VPC 的现有基础设施创建 VPC 对等连接，并且不依赖单独的物理硬件。因此，它们不会在两者之间 VPCs引入潜在的单点故障或网络带宽瓶颈。此外，可以利用 VPC 路由表、安全组和网络访问控制列表来控制哪些子网或实例能够利用 VPC 对等连接。

Amazon VPCs 不支持传递对等互连，这意味着您无法使用第三个 VPC 作为传输 VPCs ，与两个未直接对等互连的用户进行通信。如果您希望所有人使用 VPC VPCs 对等互连相互通信，则需要在他们每个人之间创建 1:1 的 VPC 对等连接。或者，您可以使用 AWS Transit Gateway 或 AWS Cloud WAN 充当网络传输中心。

VPC 对等连接同时支持 IPv4 和 IPv6 流量。但是，如果两个主要 IPv4 CIDR 块重叠，则无论使用哪个辅助地址块 IPv4 或 IPv6 CIDR 块，都 VPCs 无法对等互连。 VPCs 如果您计划在主网段之间使用 VPC 对等连接，请在为它们分配主 CIDR 块时考虑这一点。

其他 资源

- 亚马逊 VPC 对等互连
- 什么是 VPC 对等互连？

AWS Transit Gateway

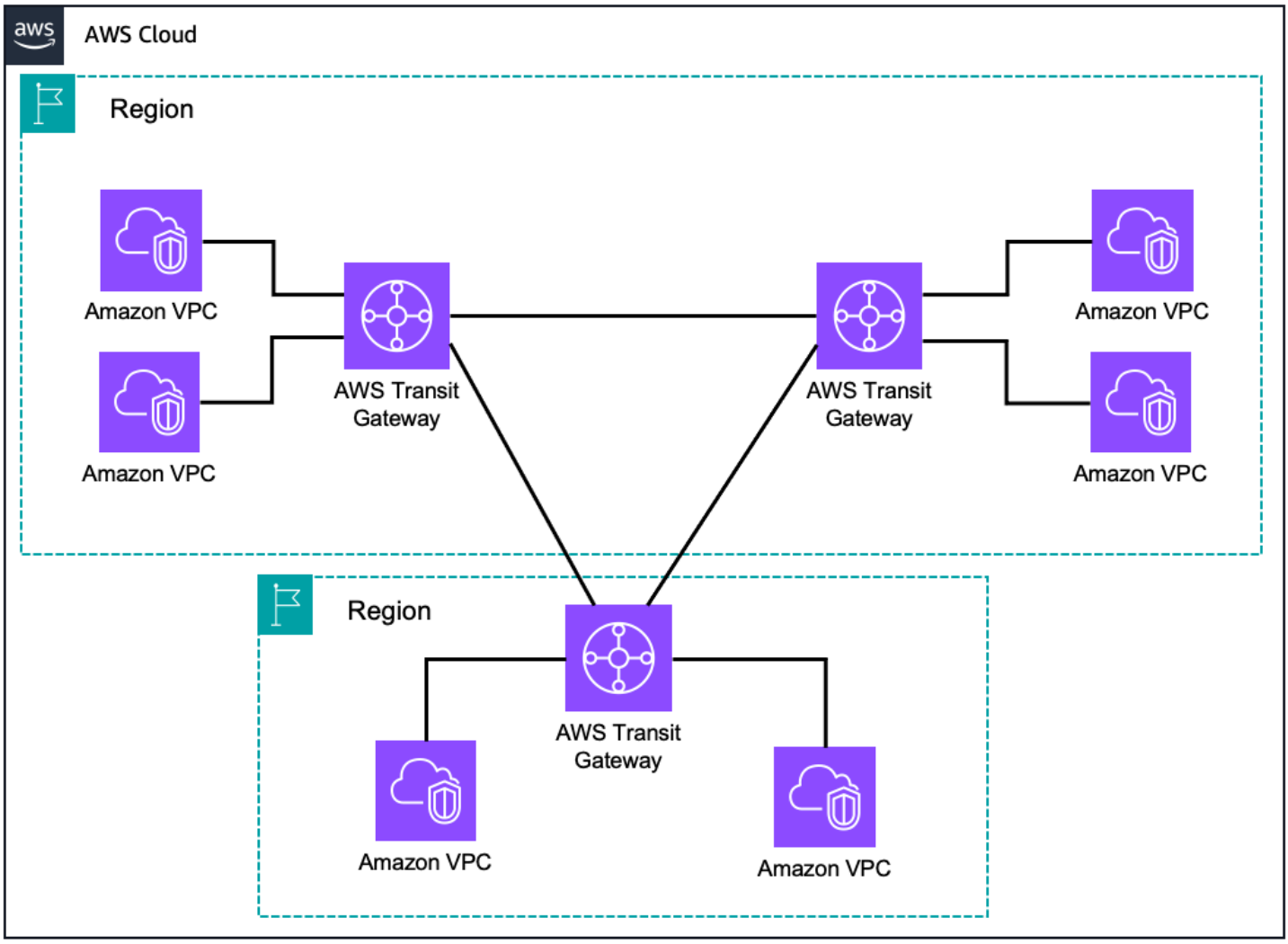
AWS Transit Gateway 是一项高度可用且可扩展的服务，用于整合具有 hub-and-spoke架构的区域的 AWS VPC 路由配置。每个分支 VPC 只需要连接到 Transit Gateway 即可访问其他连接的 VPC VPCs。中同时支持 IPv4 和 IPv6 流量 AWS Transit Gateway。

您可以利用多个 Transit Gateway 路由表、关联和传播在同一 Transit Gateway 内对流量进行分段。您将能够从单一管理点管理不同的路由域（例如生产和非生产流量），从而确保这些路由域无法相互通信。

您还可以利用 Transit Gateway 创建的 hub-and-spoke架构来集中访问共享服务，例如流量检查、接口 VPC 终端节点访问或通过 NAT 网关或 NAT 实例的出口流量。这种集中化简化了将这些资源分成几个管理的复杂性 VPCs，并且可以更好地控制您在 AWS 中的足迹。

Transit Gateways 可以在同一 AWS 区域内或不同的 AWS 区域之间相互对等。 AWS Transit Gateway 流量始终保持在全球 AWS 主干上，从不穿越公共互联网，从而减少了常见漏洞和 DDo S 攻击等威胁载体。

Transit Gateway 拥有大量的 VPCs，可通过 VPC 对等互连提供更简单的 VPC-to-VPC通信管理，如下图所示。



AWS Transit Gateway

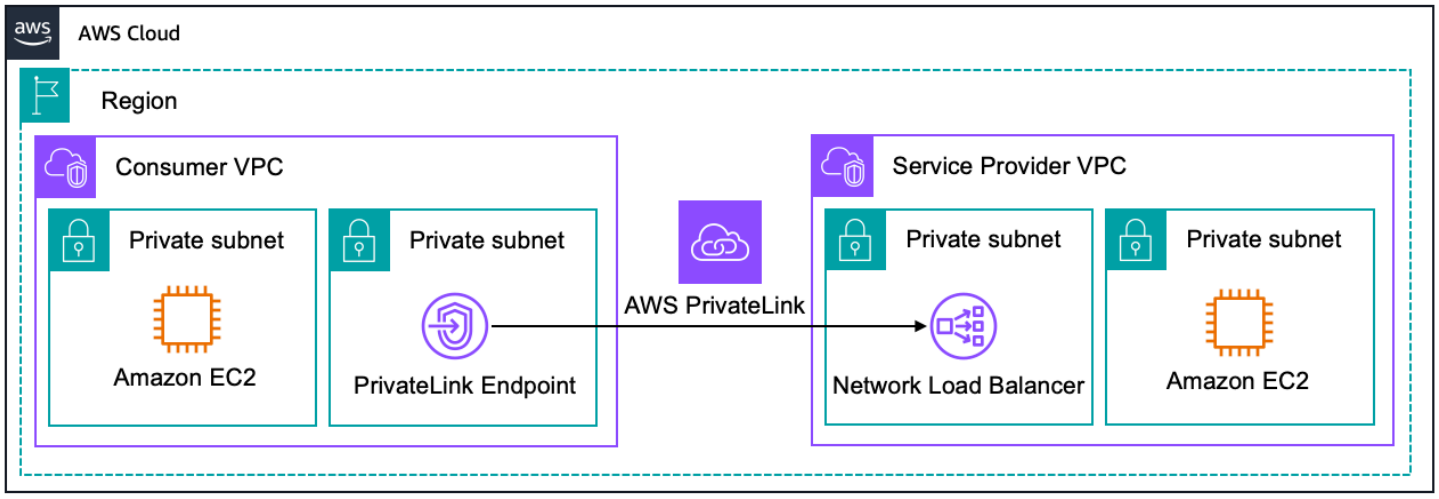
要集中查看进出您的传输网关的 IP 流量，您可以将 Transit Gateway 流日志发布到 Amazon Lo CloudWatch gs 和 Amazon S3。流日志数据是在网络流量路径之外收集的，因此不会影响网络吞吐量或延迟。

其他 资源

- 亚马逊 VPC 传输网关
- 中转网关对等连接挂载
- 使用公交网关
- 使用 Transit Gateway 流日志记录网络流量

AWS PrivateLink

AWS PrivateLink 允许您通过 VPC 中的私有 IP 地址连接到某些 AWS 服务、由其他 AWS 账户托管的服务（称为终端节点服务）以及支持的 AWS Marketplace 合作伙伴服务。接口终端节点直接在您的 VPC 内部创建，使用弹性网络接口和 VPC 子网中的 IP 地址。这意味着可以使用 VPC 安全组来管理对终端节点的访问。



AWS PrivateLink

如果您想在 AWS 网络中使用私有 IP 地址安全地使用其他 VPC 提供的服务，我们建议您采用这种方法。或者，当 IP 地址重叠时， VPCs 也 AWS PrivateLink 是一个不错的解决方案。

AWS PrivateLink 完全支持 IPv6，但必须启用或修改目标 VPCs、VPC 子网、Network Load Balancer 和 DNS 名称才能使用双堆栈。满足这些先决条件后， IPv6 可以在终端节点的服务配置中启用。

访问控制 AWS PrivateLink

接口终端节点是使用弹性网络接口和 VPC 子网中的 IP 地址直接在您的 VPC 内部创建的。这意味着可以使用 VPC 安全组来管理对终端节点的网络访问。

创建接口终端节点或网关终端节点时，还可以附加终端节点策略。终端节点策略控制哪些 AWS 委托人（AWS 账户、IAM 用户和角色）可以使用 VPC 终端节点访问终端节点服务。

您不能将多个策略附加到一个端点。但是，您可以随时修改端点策略。

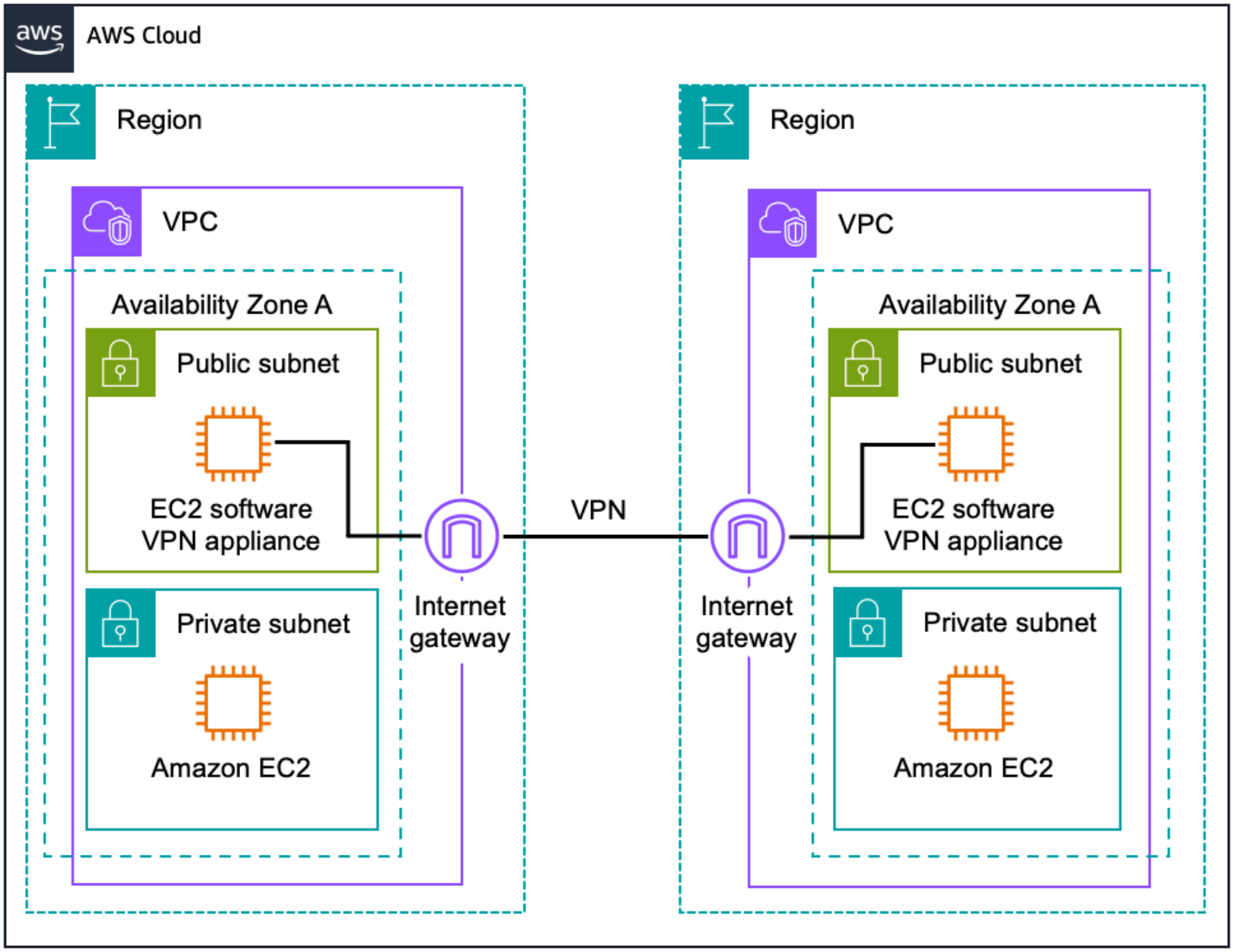
终端节点策略不会覆盖或取代 IAM 用户策略或特定于服务的策略（例如 Amazon S3 存储桶策略）。如果您使用接口终端节点连接到 Amazon S3，则还可以使用 Amazon S3 存储桶策略来控制从特定终端节点或特定 VPCs终端节点访问存储桶。

其他 资源

- 接口 VPC 终端节点 (AWS PrivateLink)
- VPC 终端节点服务 (AWS PrivateLink)
- 博客文章： IPv6 通过 PrivateLink 服务和端点加快您的采用速度
- 博客文章：连接 IP 范围重叠的网络
- AWS PrivateLink 合作伙伴

软件 VPN

Amazon VPC 提供了灵活的网络路由。这包括能够在两个或多个软件 VPN 设备之间创建安全 VPN 隧道， VPCs 将多个设备连接到更大的虚拟专用网络，以便每个 VPC 中的实例可以使用私有 IP 地址无缝地相互连接。如果您想使用首选的 VPN 软件提供商管理 VPN 连接的两端，则建议使用此选项。此选项使用连接到每个 VPC 的互联网网关来促进软件 VPN 设备之间的通信。



Software Site-to-Site VPN VPC-to-VPC Routing

您可以从多个合作伙伴和开源社区组成的生态系统中进行选择，这些社区生产了在 Amazon 上运行的软件 VPN 设备 EC2。除了这种选择外，您还有责任管理软件设备，包括配置、补丁和升级。

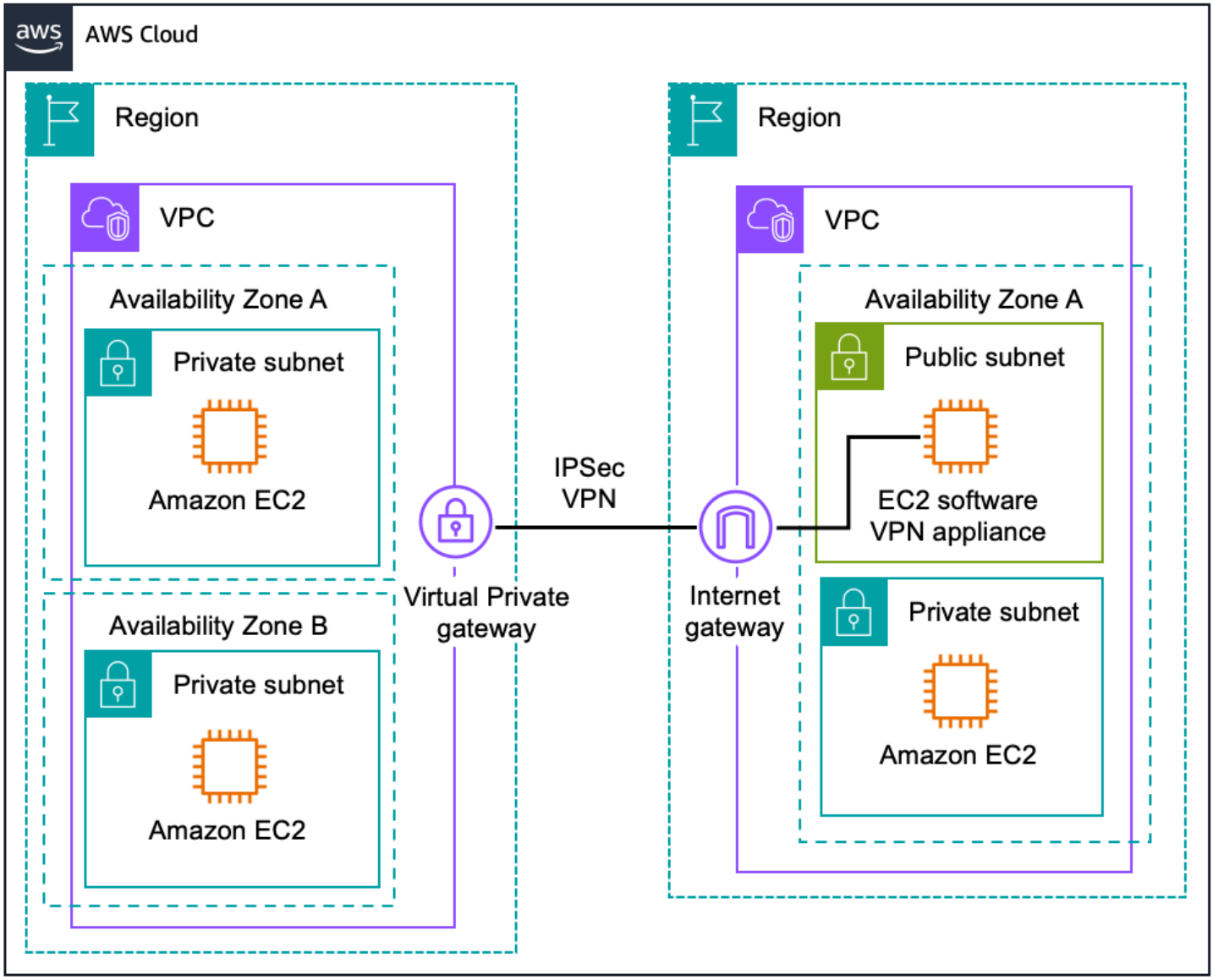
请注意，此设计在网络设计中引入了潜在的单点故障，因为软件 VPN 设备在单个 Amazon EC2 实例上运行。有关更多信息，请参阅 附录 A：软件 VPN 实例的高级高可用架构。

其他 资源

- VPN 设备可从中获得 AWS Marketplace
- 技术简报-将多个 EC2 实例 VPCs 与实例连接 (IPsec)
- 技术简报-将多个 EC2 实例 VPCs 与实例连接 (SSL)

软件 VPN-to-AWS Site-to-Site VPN

Amazon VPC 允许灵活地将 AWS 托管 VPN 和软件 VPN 选项组合在一起以连接多个选项 VPCs。通过这种设计，您可以在软件 VPN 设备和虚拟专用网关之间创建安全 VPN 隧道，从而允许每个 VPC 中的实例使用私有 IP 地址无缝地相互连接。此选项使用一个 Amazon VPC 中的虚拟私有网关，在另一个 Amazon VPC 中使用互联网网关和软件 VPN 设备的组合，如下图所示。



Software VPN to AWS Site-to-Site VPN VPC-to-VPC Routing

请注意，此设计在网络设计中引入了潜在的单点故障。有关更多信息，请参阅 附录 A：软件 VPN 实例的高级高可用架构。

其他 资源

- VPN 设备可从中获得 AWS Marketplace
- AWS Site-to-Site VPN 用户指南
- 对客户网关设备的要求

软件远程 access-to-Amazon VPC 连接选项

借助软件远程访问 VPN，您可以利用低成本、弹性和安全的服务来实施远程访问解决方案，同时还能提供与 AWS 托管资源的无缝连接。远程网络不那么广泛或尚未为员工构建和部署远程访问解决方案的小型公司通常更喜欢这种选择。

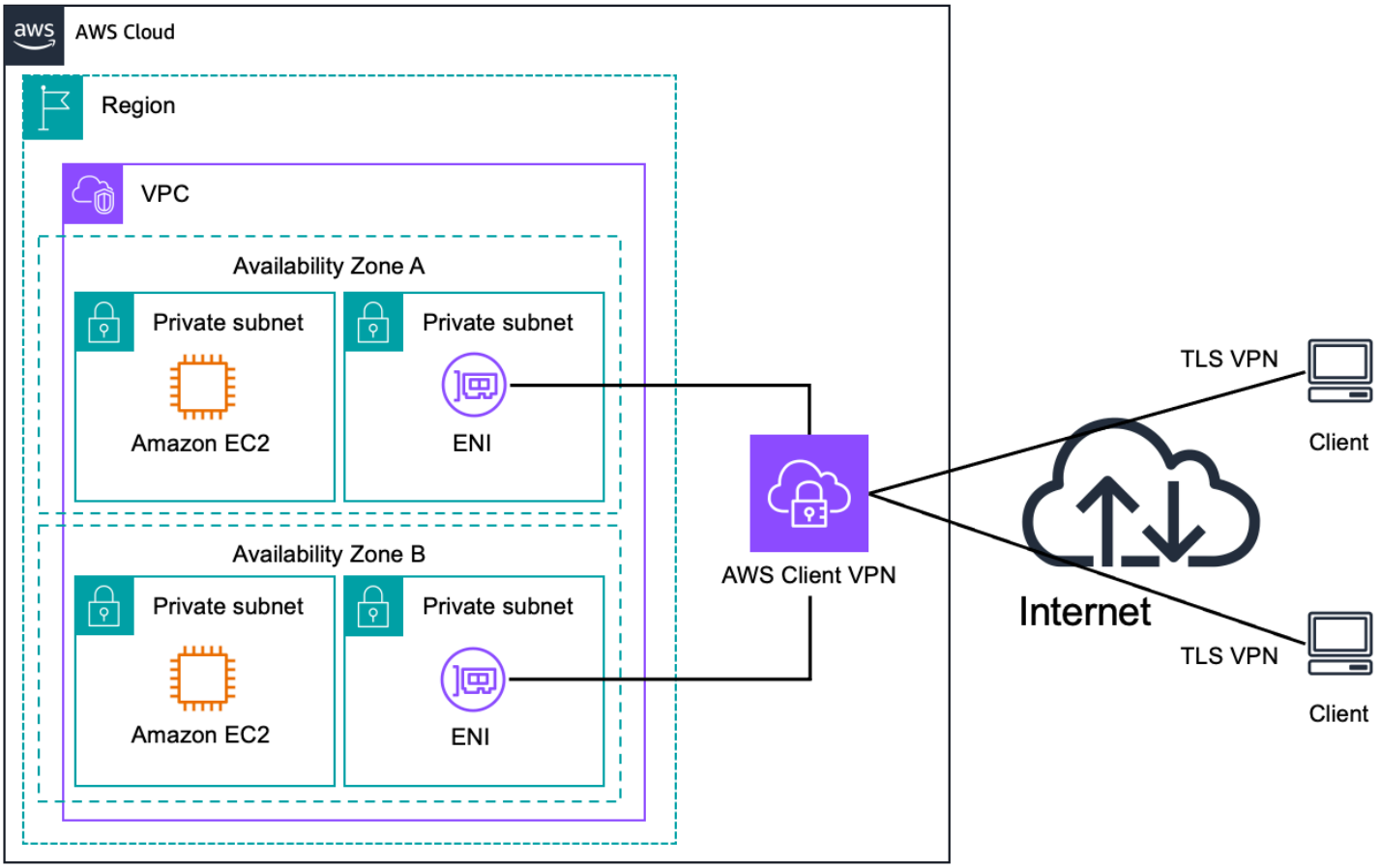
您可以将这些模式与Network-to-Amazon VPC 连接选项连接选项结合起来亚马逊 VPC-to-Amazon VPC 连接选项，创建一个跨越远程网络和多个 VPCs网络的网络。

下表概述了这些选项的优点和局限性。

选项	使用场景	优点	限制
AWS Client VPN	AWS 托管的 Amazon VPC 和/或内部网络的远程访问解决方案	AWS 托管的高可用性和可扩展性服务	仅限 OpenVPN 客户端
软件客户端 VPN	软件 VPN 设备远程访问亚马逊 VPC 和/或内部网络的解决方案	支持更多的 VPN 供应商、产品和协议 完全由客户管理的解决方案	你负责实施 HA 解决方案

AWS Client VPN

AWS Client VPN 是一项 AWS 托管的高可用性和可扩展性服务，可实现安全的软件远程访问。它提供了在远程客户端和您的 Amazon 之间创建安全 TLS 连接的选项 VPCs，以便通过互联网安全地访问 AWS 资源和本地资源，如下图所示。



AWS Client VPN Remote Access

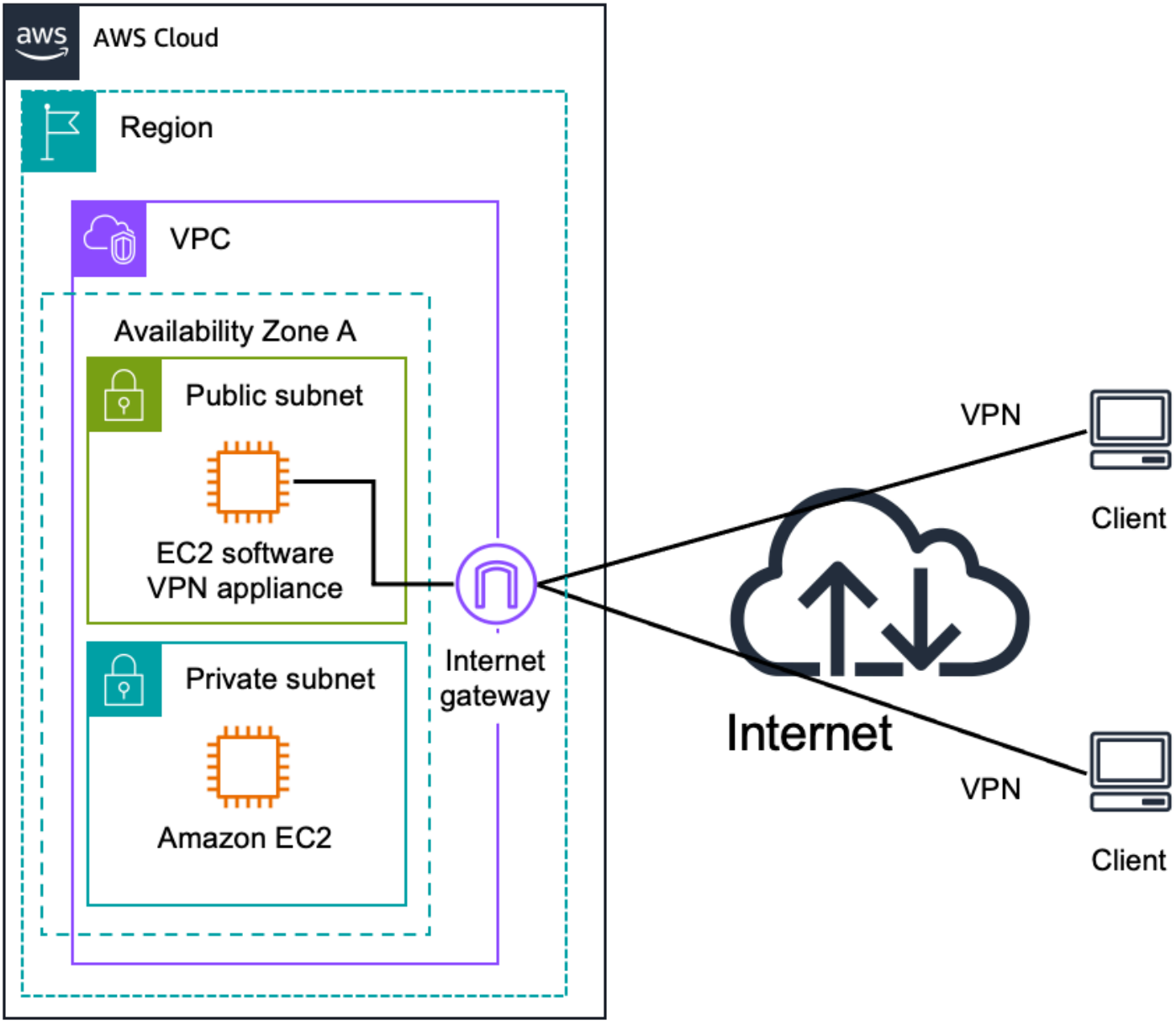
远程客户端可以是适用于桌面的 AWS Client VPN 客户端，也可以是第三方 OpenVPN VPN 客户端，通过活动目录或相互证书身份验证进行身份验证。

其他 资源

- AWS Client VPN 管理员指南

软件客户端 VPN

您可以从多个合作伙伴和开源社区组成的生态系统中进行选择，这些社区开发了在 Amazon 上运行的远程访问解决方案。 EC2这些解决方案为远程访问您的 Amazon VPCs、安全访问 AWS 资源和通过互联网在本地安全访问 AWS 资源提供了极大的灵活性，如下图所示。



Software Client VPN Remote Access

远程访问解决方案的复杂性各不相同，支持多个客户端身份验证选项（包括多因素身份验证），并且可以与 Amazon VPC 或远程托管的身份和访问管理解决方案（利用其中一个 VP network-to-Amazon C 选项）集成，例如 Microsoft Active Directory 或其他 LDAP/多因素身份验证解决方案。

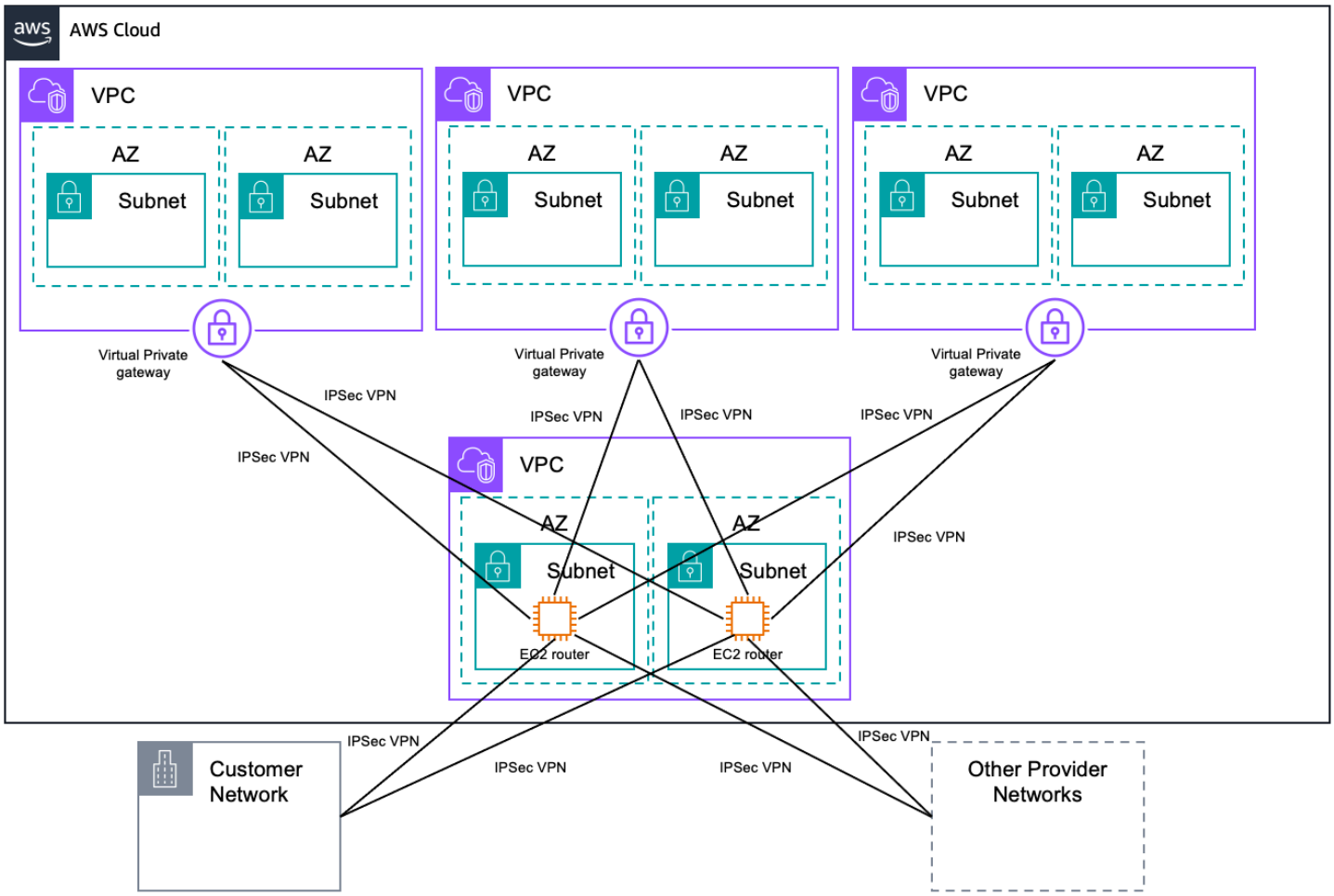
您负责管理远程访问软件，包括用户管理、配置、补丁和升级。这种设计在网络设计中引入了潜在的单点故障，因为远程访问服务器在单个 Amazon EC2 实例上运行。有关更多信息，请参阅 附录 A：软件 VPN 实例的高级高可用架构。

其他 资源

- VPN 设备可从中获得 AWS Marketplace
- OpenVPN 接入服务器快速入门指南

传输 VPC

基于上述软件 VPN 设计，您可以在 AWS 上创建全球传输网络。传输 VPC 是一种常用策略，用于连接多个地理上分散 VPCs 的远程网络，从而创建全球网络传输中心。中转 VPC 简化了网络管理，并最大限度地减少了连接多个 VPCs 和远程网络所需的连接数量。下图说明了这种设计。



Transit VPC

除了在本地网络 VPCs 之间提供直接的网络路由外，该设计还使中转 VPC 能够实施更复杂的路由规则，例如重叠网络范围之间的网络地址转换，或者添加额外的网络级数据包过滤或检查。Transit VPC 设计可用于支持重要的用例，例如私有网络、共享连接和跨账户 AWS 使用。

其他 资源

- AWS Transit Gateway
- 适用于 SD-WAN 和路由的 Cisco Catalyst 8000V AWS Marketplace

AWS 云广域网

AWS Cloud WAN 是一种以意图为导向的托管广域网 (WAN)，由您定义的策略进行描述，该策略将您的数据中心、分支机构和 AWS 网络统一起来。虽然您可以通过跨区域互连多个公交网关来创建自己的全球网络，但 Cloud WAN 提供了内置的自动化、分段和配置管理功能，专为基于您的核心网络策略构建和运营全球网络而设计。Cloud WAN 增加了诸如自动 VPC 附件、集成性能监控和集中配置等功能。

核心网络策略以声明性语言编写，用于定义分段、AWS 区域路由以及附件应如何映射到分段。通过核心网络策略，您可以描述您的访问控制和流量路由意图，而 AWS Cloud WAN 则负责处理网络配置细节。

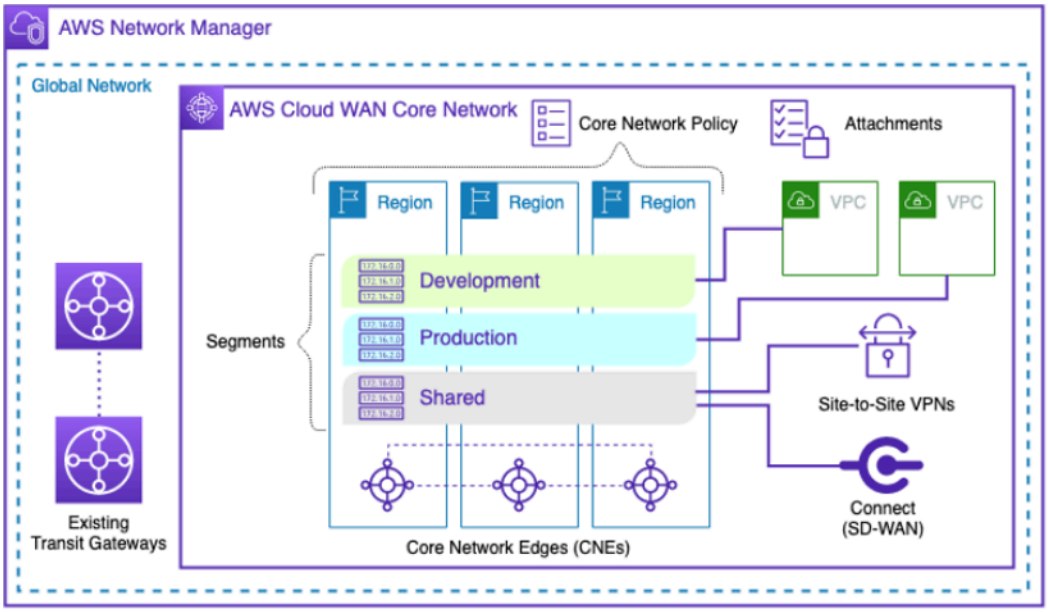
Cloud WAN 在 AWS Network Manager 中进行管理，这使您能够在 AWS 账户、区域和本地位置集中管理和可视化您的云广域网核心网络和 Transit Gateway 网络。Network Manager 为您提供多种仪表板可视化效果，帮助您查看和监控全球网络的各个方面。一些仪表板包括：

- 精确定位网络资源（例如边缘位置、设备和附件）所在位置的世界地图。
- 监控使用 CloudWatch 事件来跟踪 15 个月的统计数据，让您可以更好地了解网络的表现。
- 事件跟踪可将实时事件流式传输到事件仪表板。
- 您的中转网关网络和中转网关的拓扑图和逻辑图。

Transit Gateway 和 Cloud WAN 都允许在本地 VPCs 和本地位置之间进行集中连接。Transit Gateway 是一个区域网络连接中心，最适合在某些 AWS 区域开展业务、想要管理自己的对等互连和路由配置，或者更喜欢使用自己的自动化系统的客户。Cloud WAN 最适合希望通过策略定义其全球网络并让服务自动实现底层组件的客户。

需知信息

- CNE（核心网络边缘）继承了许多 Transit Gateway 特征，例如每个 VPC 连接的吞吐量。
- 云 WAN 同时支持 IPv4 和 IPv6。
- 对于具有许多更改的大型网络，可以考虑创建一个单独的开发和测试全球网络，以便您可以验证更改。



AWS Cloud WAN

其他 资源

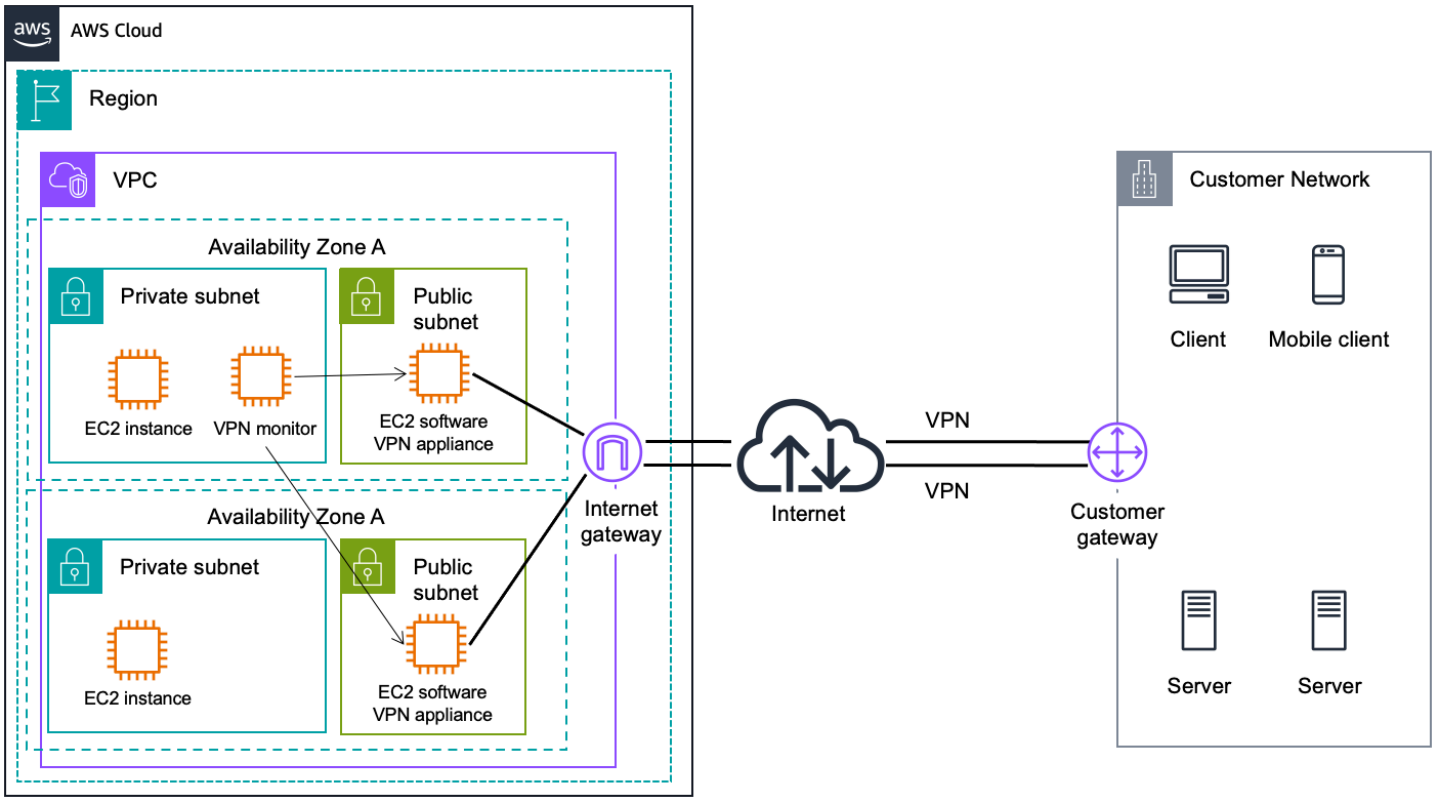
- AWS 云广域网文档
- 博客文章：AWS Cloud WAN 和 AWS Transit Gateway 迁移和互操作性模式

结论

AWS 提供了许多高效、安全的连接选项，帮助您在将远程网络与 Amazon VPC 集成时充分利用 AWS。本白皮书中提供的选项重点介绍了客户成功集成远程网络或多个 Amazon VPC 网络时使用的几种连接选项和模式。您可以使用此处提供的信息来确定最合适的机制，用于连接运营业务所需的基础架构，无论其实际位于何处或托管在哪里。

附录 A：软件 VPN 实例的高级高可用架构

为软件 VPN 实例创建完全弹性的 VPC 连接需要设置和配置多个 VPN 实例和一个监控实例来监控 VPN 连接的运行状况。



高级软件 VPN HA

我们建议将您的 VPC 路由表配置为同时利用所有 VPN 实例，方法是将来自一个可用区内所有子网的流量引导到同一可用区内相应的 VPN 实例。然后，每个 VPN 实例都为共享相同可用区的实例提供 VPN 连接。

VPN 监控

要监控基于软件的 VPN 设备，您可以创建 VPN 监控器。VPN 监控器是运行 VPN 监控脚本所需的自定义实例。此实例旨在运行和监控 VPN 连接和 VPN 实例的状态。如果 VPN 实例或连接出现故障，监控器需要停止、终止或重启 VPN 实例，同时还需要将流量从受影响的子网重新路由到正常运行的 VPN 实例，直到两个连接都恢复正常运行。由于客户要求各不相同，AWS 目前不提供设置此监控实例的规范性指导。但是，可以将在 NAT 实例之间启用 HA 的示例脚本用作为软件 VPN 实例创建 HA 解决方案的起点。我们建议您仔细考虑必要的业务逻辑，以便在 VPN 连接失败时提供通知或尝试自动修复网络连接。

此外，您可以使用 Amazon CloudWatch 指标监控 AWS 托管 VPN 隧道，该指标将来自 VPN 服务的数据点收集为可读的近乎实时的指标。每个 VPN 连接都会收集各种隧道指标并将其发布到 Amazon CloudWatch。这些指标允许您监控隧道运行状况、活动并创建自动操作。

贡献者

本文档的贡献者包括：

- Daniel Yu，AWS Enterprise Support 高级技术客户经理
- Garvit Singh，解决方案构建器，AWS 解决方案架构
- Steve Morad，AWS 解决方案架构解决方案构建者高级经理
- Sohaib Tahir，解决方案架构师，AWS 解决方案架构
- Fiona Armada，AWS 解决方案架构首席解决方案架构师
- Pablo Sánchez Carmona，网络专家解决方案架构师，AWS 解决方案架构
- Tony Hawke，AWS Enterprise Support 高级网络专家技术客户经理

文档修订

如需获取有关该白皮书更新的通知，请订阅 RSS 信息源。

变更	说明	日期
已更新白皮书	自始至终添加了 AWS Cloud WAN 和 Transit Gateway 连接附件选项、更新的图表和信息。	2023 年 4 月 5 日
已更新白皮书	添加了 AWS Transit Gateway 和 AWS Client VPN 选项，自始至终更新了图表和信息。	2020年6月6日
次要更新	对修复对软件 VPN 设备的引用进行了微小的更改。	2020 年 5 月 20 日
已更新白皮书	自始至终都更新了信息。重点介绍以下设计/功能：传输 VPC、Direct Connect 网关和。 AWS PrivateLink	2018年1月1日
初次发布	亚马逊虚拟私有云 Virtual Private Cloud 连接选项已发布。	2014 年 7 月 1 日

版权声明

客户有责任对本文档中的信息进行单独评测。本文档：(a) 仅供参考；(b) 代表当前提供的 AWS 产品和实操，如有更改，恕不另行通知；并且 (c) AWS 及其附属机构、供应商或许可方不做任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户承担的责任和义务受 AWS 协议制约，本文档不是 AWS 与客户直接协议的一部分，也不构成对该协议的修改。

© 2020，Amazon Web Services, Inc. 或其附属公司。保留所有权利。

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。