Amazon 虚拟专有云连接选项

Steve Morad

2014 年 7 月

目录

摘要

Amazon Virtual Private Cloud (即 Amazon 虚拟专有云，简称 Amazon VPC) 允许客户配置一套专有的隔离型 Amazon Web Services（简称 AWS）云分区，并在其中利用客户定义的 IP 地址范围立足虚拟网络启动 AWS 资源。Amazon VPC 为客户提供多种选项，用于将其 AWS 虚拟网络同其它远程网络进行连接。本份白皮书将阐述适合客户实际需求的几类常见连接选项，其中包括将远程客户网络与 Amazon VPC 加以结合，以及多套 Amazon VPC 利用一套连续虚拟网络彼此对接。

本份白皮书旨在面向企业网络架构师与工程师，或者 Amazon VPC 管理员等希望了解可用连接选项的群体。其中对多种选项加以概述，从而以综合方式对网络连接进行讨论，同时亦指向其它文档及资源中更为详尽的信息或示例。

简介

Amazon VPC 为大家提供多种网络连接选项，具体选择取决您的现有网络设计及实际要求。这些连接选项包括利用互联网或者 AWS Direct Connect 连接作为网络“主干”，而其终端则接入 AWS 或者由用户管理的网络端点。另外，利用 AWS 大家能够选择网络的具体路由方式，引导流量在 Amazon VPC 以及自有网络间的传输路径，同时利用 AWS 或者用户管理的网络设备及路由机制。本份白皮书将对以下选项做出概述，同时进行高层级比较：

用户网络到 Amazon VPC 连接选项

硬件 VPN	在远程网络上的客户网络设备与 AWS 管理的网络设备之间建立一条硬件 VPN 连接，并将其附加至您的 Amazon VPC 处。
AWS Direct Connect	在您的远程网络与 Amazon VPC 之间一条专有逻辑连接，且利用 AWS Direct Connect 实现。
AWS Direct Connect+ VPN	在您的远程网络与 Amazon VPC 之间建立一条专有加密连接，并利用 AWS Direct Connect 实现。
AWS VPN CloudHub	建立一套中枢与辐射模型，用于连接各远程分支办公环境
软件 VPN	Describes establishing a VPN connection from your equipment on a remote network toa user-managed software VPN appliance running inside an Amazon VPC.

Amazon VPC 到 Amazon VPC 连接选项

VPC 对等网络	AWS 推荐方案，利用 Amazon VPC 的对等特性将多套位于同一服务区内的 Amazon VPC 彼此对接。
软件 VPN	利用 VPN 对多套 Amazon VPC 彼此对接，此 VPN 由运行在各 Amazon VPC 之内的用户管理软件 VPN 方案负责建立。
软件到硬件 **VPN**	利用 VPN 连接对接多套 Amazon VPC，此 VPN 由单一 Amzon VPC 内的用户管理软件 VPN 方案与附加至另一 Amazon VPC 的 AWS 管理网络设备负责建立。
硬件 VPN	用于连接多套 Amazon VPC，利用用户远程网络与各 Amazon VPC 之间的多条硬件 VPN 连接。
AWS Direct Connect	用于连接多套 Amazon VPC，利用客户管理的 AWS Direct Connect 路由器建立逻辑连接。

互联网用户到 Amazon VPC 连接选项

软件远程访问 VPN	除了利用客户网络到 Amazon VPC 连接选项以对接远程用户与 VPC 资源，此选项利用远程接入解决方案为最终用户提供接入 Amazon VPC 的 VPN 连接。

网络到 Amazon VPC 连接选项

本章节将向大家阐述由远程网络接入 Amazon VPC 环境的设计模式。相关选项适用于通过将内部网络扩展至 AWS 云，从而将 AWS 资源与您的现有内部服务（例如监控、验证、安全、数据或者其它系统）相结合的用例场景。这一网络扩展机制亦允许大家的内部用户以无缝化方式接入由 AWS 托管的资源，且具体方式与接入其它面向内部的资源基本一致。

VPC 与远程客户网络间的连接最好通过非覆盖 IP 范围以单独接入各网络的方式实现。举例来说，如果大家希望将一套或者多套 VPC 接入您的内部网络，请确保它们皆以惟一的无类别域间路由（简称 CIDR）范围进行配置。我们建议大家分配单一、连续且无覆盖的 CIDR 块以供各 VPC 使用。欲了解更多与 Amazon VPC 路由及限制相关的细节信息，请参阅 Amazon VPC 常见问题解答。[1]

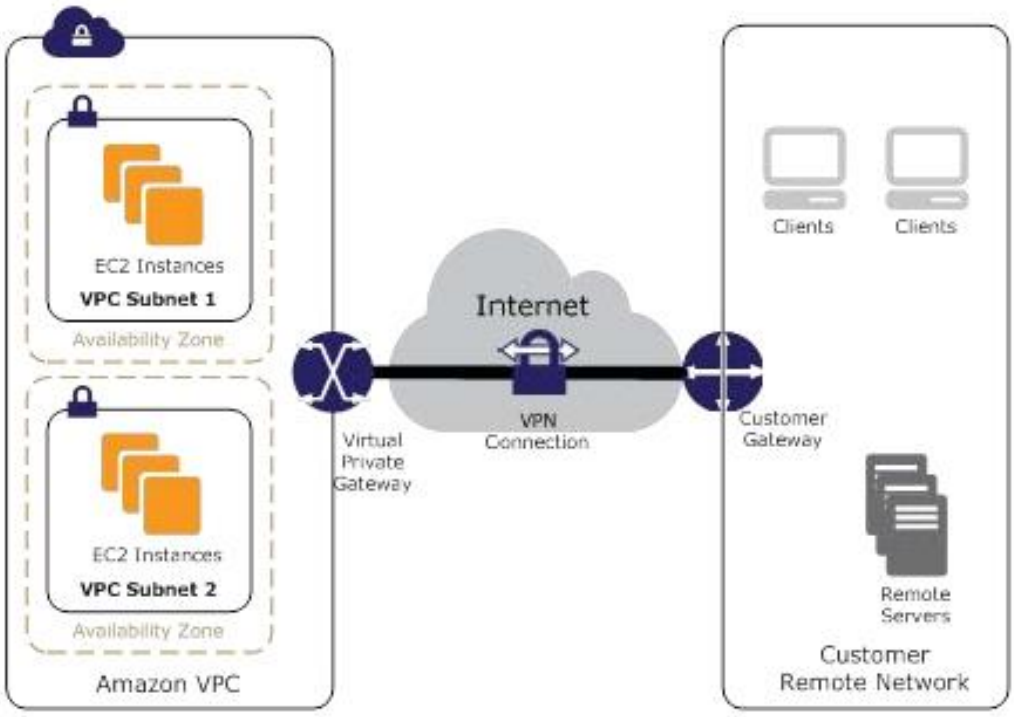
选项	用例	优势	局限
硬件 VPN	基于硬件且经由互联网实现的 IP 安全 VPN 连接	复用现有 VPN 设备与流程 复用现有互联网连接 AWS 管理端点包括多数据中心冗余与自动故障转移机制 支持静态或动态路由边界网关协议(简称 BGP)的对等与路由策略	网络的延迟水平、变化性以及可用性取决于互联网状态 客户管理端点负责实现冗余及故障转移（如果需要）
AWS Direct Connect	经由专有路线实现的专用网络连接	更具可预测性的网络性能 降低传输带宽使用成本 1 或 10 Gbps 配置连接 支持 BGP 对等及路由策略	客户设备必须支持单跳 BGP（当使用 GBP 动态路由机制时） 可能要求与电信及托管服务供应商建立额外合作或者利用新的网络链路以实现配置

[1] http://aws.amazon.com/vpc/faqs/

选项	用例	优势	局限
软件 VPN	基于软件方案且经由互联网实现的 VPN 连接	支持多种 VPN 供应方、产品及协议 完全客户管理解决方案	客户负责为全部 VPN 端点实现 HA（即高可用性）解决方案
AWS Direct Connect + VPN	经由专有线路实现的基于硬件 IP 安全 VP	与上一选项相同，但新增安全 IP 安全 VPN 连接	与上一选项相同，但增加部分额外 VPN 复杂性
AWS VPN CloudHub	在中枢与辐射模式中实现远程分支办公环境连接，用于实现一级或者备份连接	复用现有互联网连接与 AWS VPN 连接（例如网络延迟、变化性与可用性取决于互联网自身状态使用 AWS VPN CLoudHub 作为指向第三方 MPLS 网络的备份连接） AWS 管理虚拟专有网关包含多数据中心冗余与自动故障转移机制 支持 BGP 以实现交换路由及路由策略（例如首选 MPLS 连接而非备份 AWS VPN 连接）	用户管理的远程办公端点负责实现冗余与故障转移功能（如果需要）

硬件 VPN

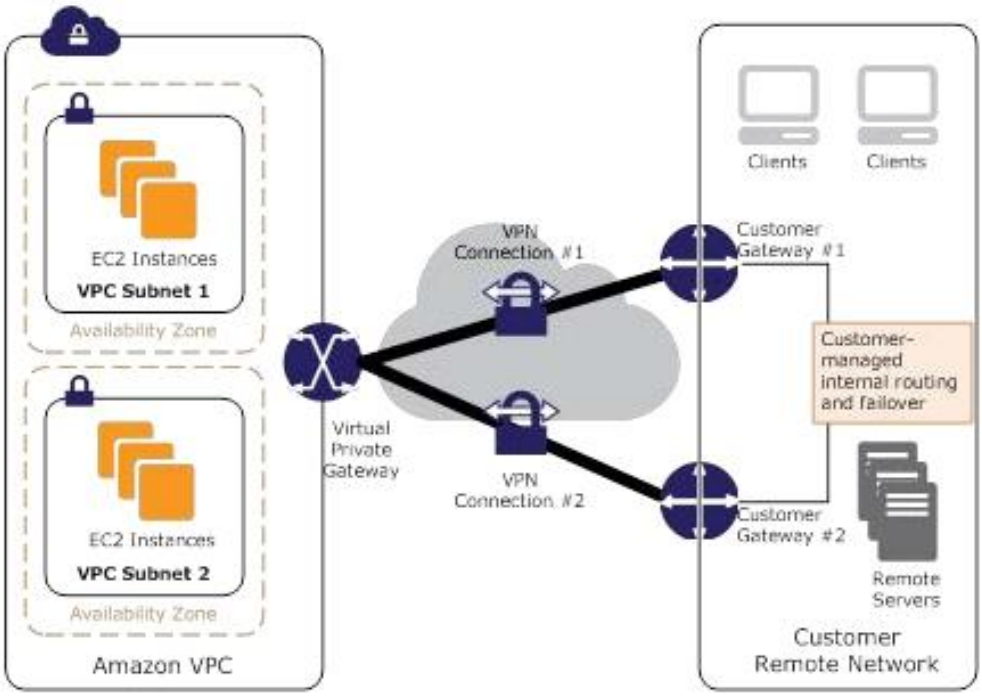
Amazon VPC 提供选项以创建一条经由互联网用于连接远程客户网络与其 Amazon VPC 的 IP 安全硬件 VPN 连接，具体如图一所示。如果希望充分发挥 AWS 管理 VPN 端点提供的各项优势，包括多数据中心冗余以及 VPN 连接中 AWS 端的内置故障转移能力，则应当考虑使用这一选项。尽管示意图中并未表现，但 Amazon 虚拟专有网关（简称 VGW）负责区分两个 VPN 端点，同时使用物理隔离的两座数据中心以提升 VPN 连接的可用性水平。



图一：硬件 VPN

VGW 还支持并鼓励使用多用户网关连接，这意味着大家可以如图二所示在自己的 VPN 端实现冗余与故障转移。其同时提供动态与静态路由选项，帮助大家灵活地进行路由配置。动态路由利用 BGP 对等机制以在 AWS 与其远程端点之间交换路由信息。利用动态路由，大家亦能够指定路由优先级、策略并在 BGP 广播内应用加权（指标），同时变更自有网络与 AWS 之间的网络路径。

另外需要强调的是，当使用 BGP 时，IPsec 与 BGP 连接必须终止于同一用户网关设备，因此其必须能够终止 IPsec 与 BGP 连接。



图二：冗余硬件 VPN 连接

扩展阅读

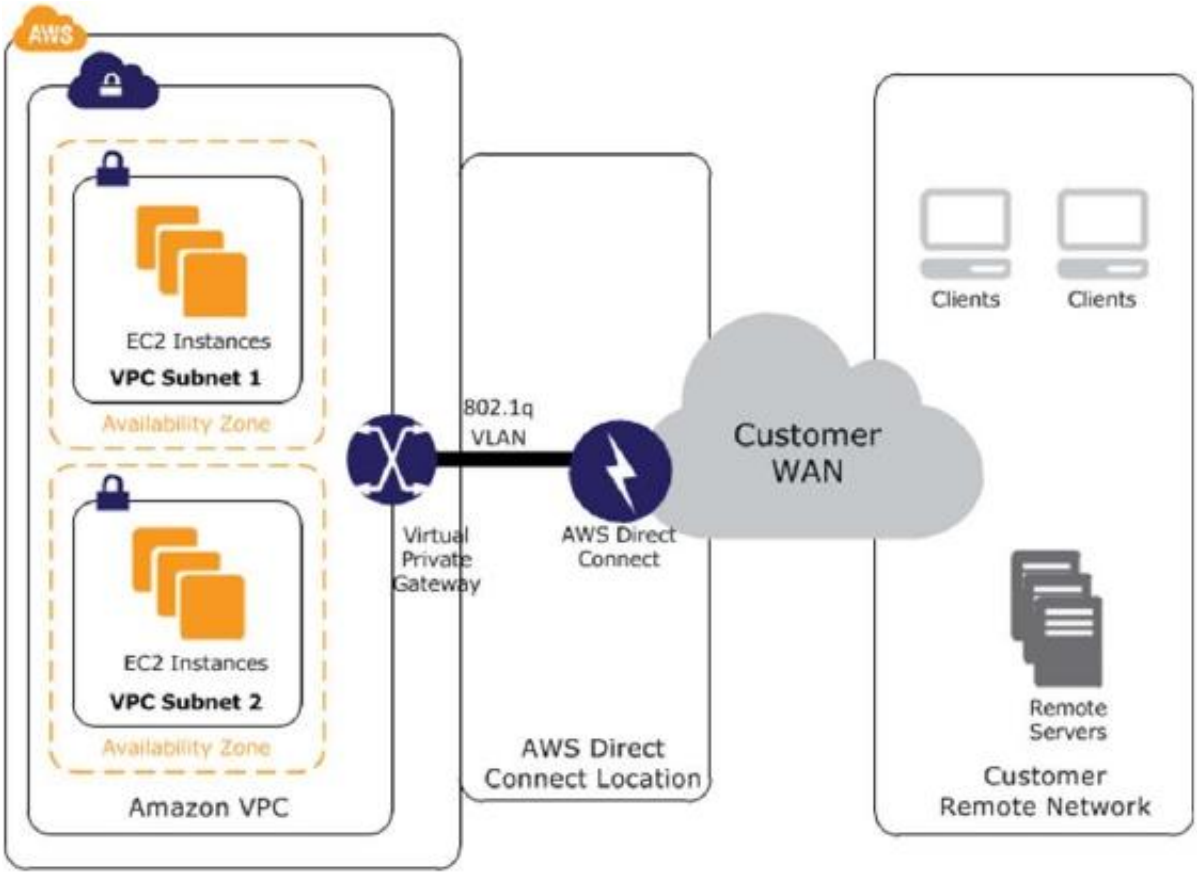
- 为您的 VPC 添加硬件虚拟专有网关 [2]
- 客户网关设备最低要求 [3]
- 已知可与 Amazon VPC 协作的客户网关设备 [4]

AWS Direct Connect

AWS Direct Connect 能够轻松在内部网络与 Amazon VPC 之间建立起一条专用连接。利用 AWS Direct Connect，大家可以在 AWS 与您的数据中心、办公环境或者异地环境间建立起专有连接。这条专有连接可降低网络使用成本，提升传输带宽通量，同时提供较互联网连接更具一致性的网络使用体验。

AWS Direct Connect 允许大家建立起 1 Gbps 或者 10 Gbps 专用网络连接（或者多条连接），用于对接 AWS 网络与 AWS Direct Connect 位置之一。其利用行业标准 VLAN 以利用专有 IP 地址接入运行在 Amazon VPC 当中的 Amazon Elastic Compute Cloud（即 Amazon 弹性计算云，简称 Amazon EC2）实例。大家可以从一整套 WAN 服务供应商生态系统当选取对应方案，从而将自己的 AWS Direct Connect 端点与远程网络进行整合。图三所示即为这一模式。

[2] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
[3] http://aws.amazon.com/vpc/faqs/#C8
[4] http://aws.amazon.com/vpc/faqs/#C9



图三：AWS Direct Connect

扩展阅读

- AWS Direct Connect 产品页面 [5]
- AWS Direct Connect 各可选位置 [6]
- AWS Direct Connect 常见问题解答 [7]
- AWS Direct Connect 上手指南 [8]

[5] http://aws.amazon.com/directconnect/

[6] http://aws.amazon.com/directconnect/#details

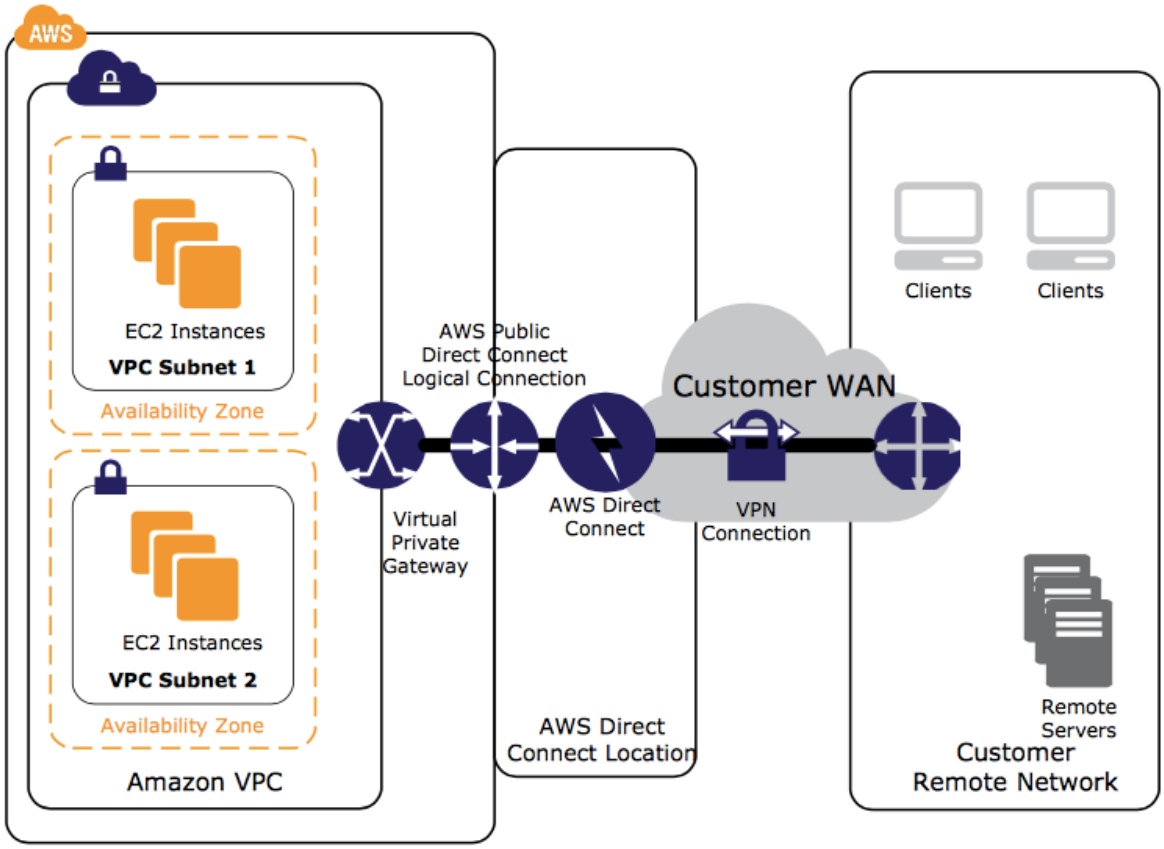
[7] http://aws.amazon.com/directconnect/faqs/

[8] http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Welcome.html

AWS Direct Connect + VPN

利用 AWS Direct Connect + VPN，大家可以将一条或者多条 AWS Direct Connect 专用网络连接同 Amazon VPC 硬件 VPN 加以结合。这一结合能够实现 IP 安全加密专有连接，从而降低网络使用成本、提升传输带宽通量并提供较互联网 VPN 连接更具一致性的网络使用体验。

大家可以利用 AWS Direct Connect 在您的内部网络与公共 AWS 资源（例如 Amazon VGW IPsec 端点）之间建立起专用逻辑网络连接。这套解决方案将 AWS 管理的硬件 VPN 解决方案与 AWS Direct Connect 解决方案的低延迟、传输带宽提升以及低一致性等优势进行结合，共同建立起一套端到端安全 IPsec 连接。图四所示即为这一选项。



图四：AWS Direct Connect + VPN

扩展阅读

- AWS Direct Connect 产品页面 [9]
- AWS Direct Connect 常见问题解答 [10]
- 为您的 VPC 添加硬件虚拟专用网关

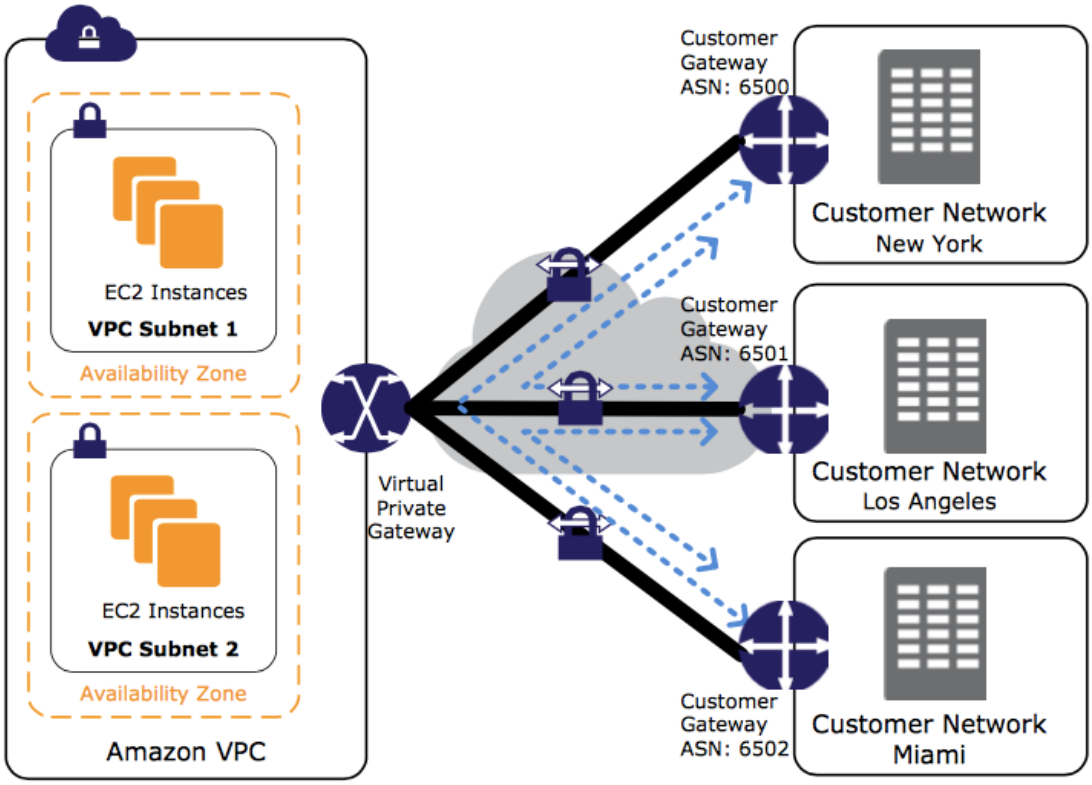
[9] http://aws.amazon.com/directconnect/

[10] http://aws.amazon.com/directconnect/faqs/

AWS VPN CloudHub

立足于之前提到的硬件 VPN 与 AWS Diret Connect 选项，大家可以安全地利用 AWS VPN CLoudHub 在不同站点之间实现通信。AWS VPN CloudHub 负责建立一套简单的中枢与辐射模式，大家可以利用其配合 VPC 或者单独使用。利用这套设计，如果大家拥有多个分支办公环境及现有互联网连接，则能够利用这一便捷的低成本中枢与辐射模式支撑各远程办公环境之间的首要或者备份连接。

图五所示即为 AWS VPN CloudHub 架构，其中蓝色虚线指示了各远程站点之间经由其 AWS VPN 连接实现路由的网络流量。



图五：AWS VPN CloudHub

AWS VPN CloudHub 利用一套 Amazon VPC 虚拟专有网关配合多套网关，各网关拥有惟一的 BGP 自治系统编号（简称 ASN）。大家的网关会经由其 VPN 连接进行对应路由（BGP 前缀）通告。这些路由通告将由各 BGP 对等点进行接收与读取，从而确保各站点都能够向其它站点发出数据及接收后者发来的数据。各辐射位置的远程网络前缀必须包含惟一 ASN，且各站点绝对不可包含覆盖 IP 范围。每个站点亦能够面向 VPC 利用标准 VPN 连接进行数据发送与接收。

此选项可与 AWS Direct Connect 或者其它硬件 VPN 选项相结合（例如每站点多网关以实现冗余或者主干路由），具体取决于您的实际要求。

扩展阅读

- AWS VPN CloudHub[11]
- Amazon VPC VPN 指南
- 客户端设备最低要求 [12]
- 已知能够与 Amazon VPC 协作的客户网关设备 [13]
- AWS Direct Connect 产品页面 [14]

[11] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html

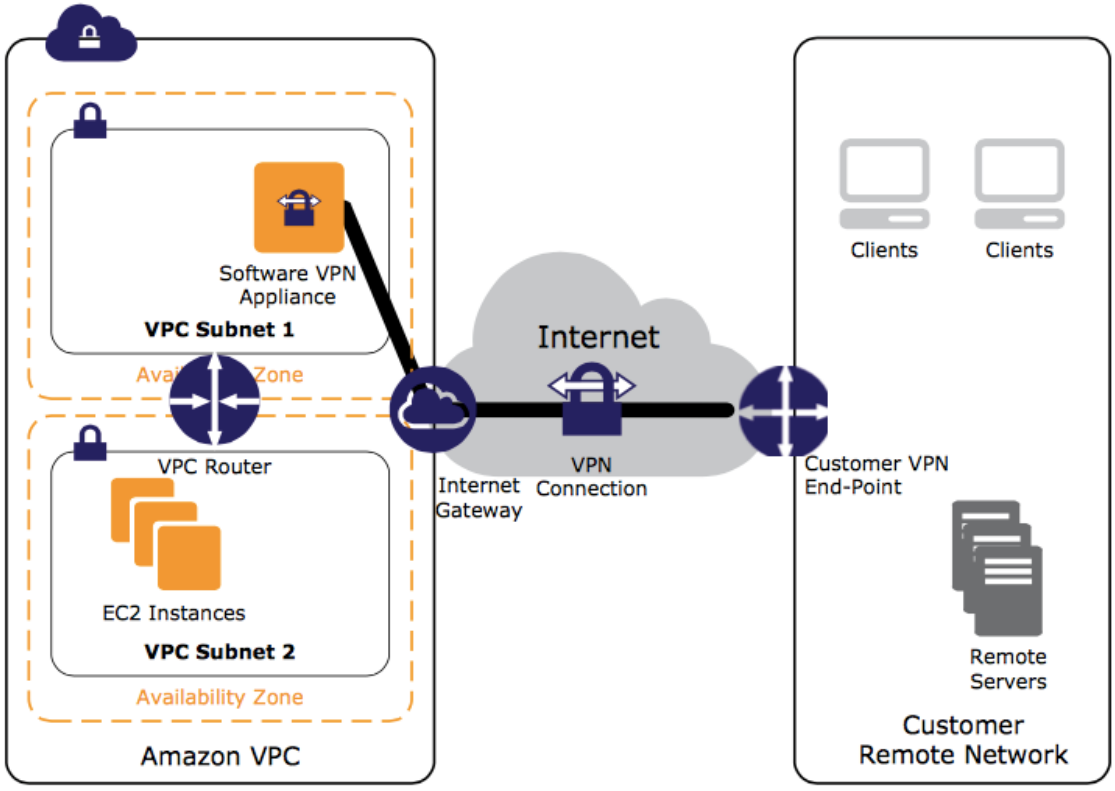
[12] http://aws.amazon.com/vpc/faqs/#C8

[13] http://aws.amazon.com/vpc/faqs/#C9

[14] http://aws.amazon.com/directconnect/

软件 VPN

Amazon VPC 能够为大家提供出色的灵活性，用于通过在远程网络与运行在 Amazon VPC 网络内的软件 VPN 方案间创建 VPN 连接以全面管理 Amazon VPC 连接的两端。如果大家需要管理 VPN 连接两端以满足合规性要求或者使用目前 Amazon VPC 硬件 VPN 解决方案尚不支持的网关设备，则建议大家使用这一选项。图六所示即为这一选项.



图六：软件 VPN

大家可以选择一套多合作伙伴以及开源社区生态系统，并由其提供运行在 Amazon EC2 上的 VPN 方案。其中包括来自各知名安全厂商的产品，包括 Check Point、Astaro、OpenVPN Technologies 以及微软等，同时亦包括 OpenVPN、Openswan 以及 IPsec-Tools 等知名开源工具。除此之外，这些选择还将为大家带来对应的软件方案管理责任，包括对其进行配置、补丁安装与升级等。

需要注意的是，这一设计方案可能会给网络设计带来潜在的单点故障可能性，这是因为该软件 VPN 方案运行在单一 Amazon EC2 之上。请参阅附录一：软件 VPN 实例高级高可用性架构内容以获取更多细节信息。

扩展阅读

- 由 AWS Marketplace 提供的 VPN 方案[15]
- 技术简介——将思科 ASA 接入 VPC EC2 实例（IPsec）[16]
- 技术简介——将多套 VPC 接入 EC2 实例（IPsec）[17]
- 技术简介——将多套 VPC 接入 EC2 实例（SSL）[18]

[15] https://aws.amazon.com/marketplace/search/results/ref=brs_navgno_search_box?searchTerms=vpn

[16] http://aws.amazon.com/articles/8800869755706543

[17] 尽管这些指南专门用于解决接入多 Amazon VPC 的需求，但其同样适用于利用接入 Amazon VPC 内 IPsec 或者 SSL 软件 VPN 方案的内部 VPN 设备替换其中一套 VPC 的网络配置用例。

[18] http://aws.amazon.com/articles/0639686206802544

Amazon VPC 到 Amazon VPC 连接选项

如果大家希望立足于单一大规模虚拟网络实现多套 Amazon VPC 之间的彼此对接，则应当使用此类设计模式。这类方案适合需要以安全性、低成本方式在多个位置或者基于内部退单要求轻松在不同 Amazon VPC 间实现 AWS 资源整合的业务场景。大家也可以将这些模式与客户网络到 Amazon VPC 连接选项加以结合，从而建立起能够涵盖远程网络及多套 VPC 的企业网络。

各 VPC 间的 VPC 连接最好利用采取非覆盖 IP 范围的各 VPC 连接方式实现。举例来说，如果大家希望将多套 VPC 加以对接，则需要确保每套 VPC 皆配置以惟一无类别域间路由（简称 CIDR）范围。因此，我们建议大家为各 VPC 分配单一的连续非覆盖 CIDR 块。欲了解更多与 Amazon VPC 路由及限制相关的细节信息，请参阅 Amazon VPC 常见问题解答：

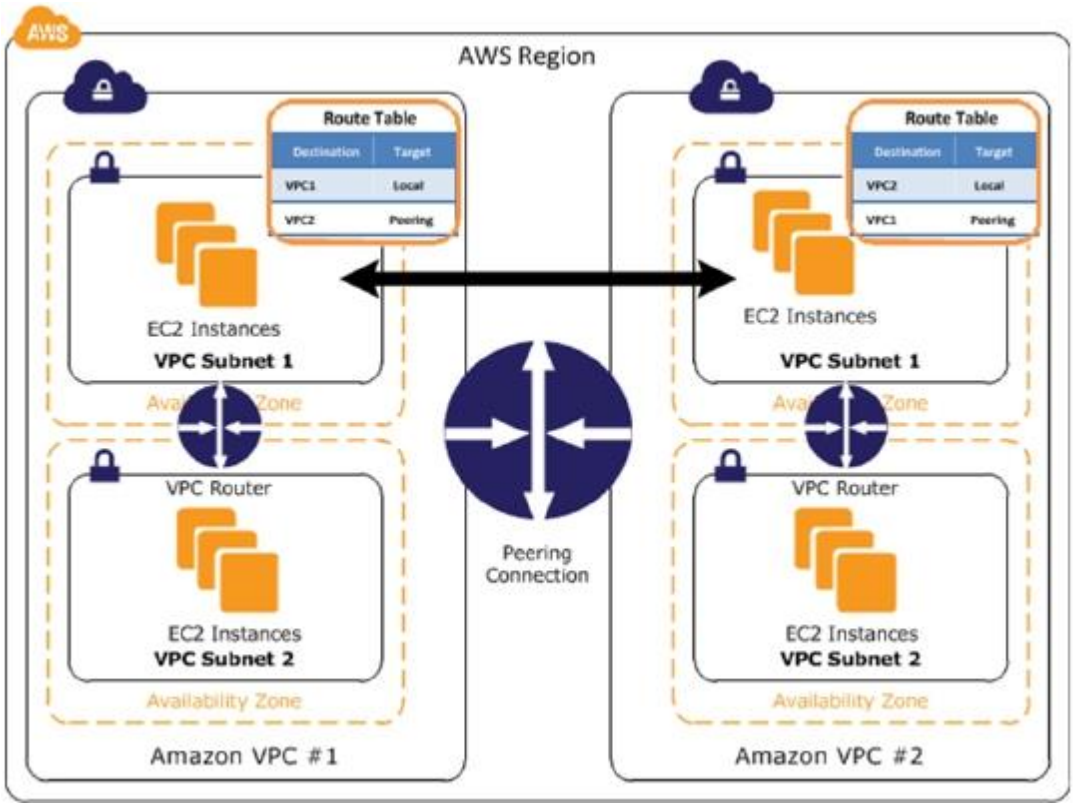
http://aws.amazon.com/vpc/faqs/

选项	用例	优势	局限
VPC 对等网络	AWS 提供的，用于对接同一服务区内两套 VPC 的网络连接。	• 利用同一服务区内的 AWS 网络基础设施。 • 不依赖于 VPN 实例或者其它物理硬件。 • 不存在单点故障可能性。 • 不存在传输带宽瓶颈。	• 对等连接目前仅支持同一服务区内两位置的对接。
软件 VPN	各 VPC 之间基于软件方案的 VPN 连接。	• 利用同一服务区内的 AWS 网络方案及各服务区间的互联网通道。 • 支持一系列 VPN 供应方、产品及协议。 • 由用户进行全面管理。	• 大家需要负责全部 VPN 端点的高可用性保障（如果需要）。 • VPN 实例可能成为网络性能瓶颈。
软件到硬件 **VPN**	各 VPC 之间利用由软件方案到硬件 VPN 的连接方式。	• 利用同一服务区内的 AWS 网络方案及各服务区间的互联网通道。 • AWS 管理的端点包含多数据中心冗余与自动故障转移机制。	• 大家需要负责全部软件方案 VPN 端点的高可用性保障（如果需要）. • VPN 实例可能成为网络性能瓶颈.

选项	用例	优势	局限
硬件 VPN	VPC 到 VPC 路由由用户利用基于硬件的 IPsec VPN 连接进行重，此 VPN 由客户设备及互联网共同实现。	• 复用现有 Amazon VPC VPN 连接。 • AWS 管理的端点包括多数据中心冗余与自动故障转移机制。 • 支持静态路由与动态 BGP 对等及路由策略。	• 网络延迟、变化性及可用性取决于互联网状态。 • 您需要负责管理端点的冗余与故障转移（如果需要）。
AWS Direct Connect	VPC 到 VPC 路由由您利用 AWS Direct Connect 位置的自有设备与专有线路进行管理。	• 统一的网络性能水平。 • 降低传输带宽使用成本。 • 1 或 10 Gbps 配置连接。 • 支持静态与 BGP 对等及路由策略	• 可能需要与电信及托管服务供应商建立额外合作

VPC 对等网络

VPC 对等连接属于建立于两套 VPC 之间的网络连接，其利用各 VPC 的专有 IP 地址实现路由，且要求二者处于同一网络当中。AWS 建议大家对于处于同一服务区内的 VPC 使用此连接方法。VC 对等连接可在大家的自有 VPC 之间或者与同一 AWS 服务区内其它 AWS 账户下的 VPC 间建立。



图七：VPC 到 VPC 对等连接

AWS 利用现有 VPC 基础设施创建 VPC 对等连接。这些连接要么属于网关，要么属于 VPN 连接，且不依赖于其它物理硬件。因此，其不会带来潜在的单点故障可能性，亦不会在 VPC 之间导致网络传输带宽瓶颈。另外，VPC 路由表、安全组以及网络访问控制列表皆可用于控制子网或者实例对 VPC 对等连接的使用。

VPC 对等连接能够帮助大家在不同 VPC 之间实现数据传输。大家可以利用其对接多个 AWS 账户下的各套 VPC，从而将管理或者共享服务 VPC 接入特定应用或者客户 VPC，亦可以无缝化方式接入合作伙伴的 VPC。欲了解更多适合应用 VPC 对等连接的场景示例，请参阅 Amazon VPC 对等连接指南。[19]

扩展阅读

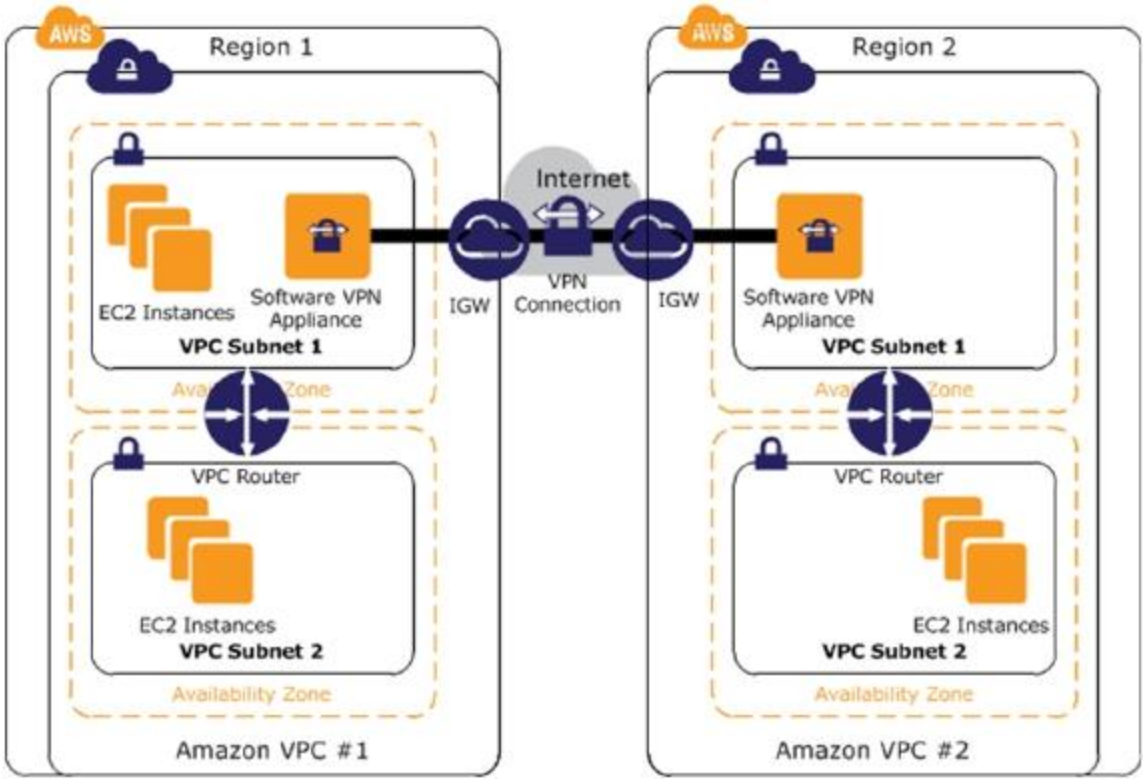
- Amazon VPC 用户指南 [20]
- Amazon VPC 对等连接指南

[19] http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/

[20] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html

软件 VPN

Amazon VPC 提供出色的网络路由灵活性。其中包括在两套甚至更多软件 VPN 方案之间创建安全 VPN 通道，旨在连接同属于单一大规模虚拟专有网络的多套 VPC，从而确保各 VPC 中的实例能够以无缝化方式利用专有 IP 地址彼此对接。这一选项适用于需要跨越多个 AWS 服务区实现 VPC 连接，同时利用现有 VPN 软件方案管理 VPN 连接两端的用户。此选项利用一套附加至每套 VPC 的互联网网关以实现各软件 VPN 方案间的连接。



图八：服务区间 VPC 到 VPC 路由

大家可以从多家合作伙伴与开源社区构成的生态系统当中选择适合自己的软件 VPN 方案，并将其运行在 Amazon EC2 之上。其中包含来自众多知名安全厂商的方案，例如 Check Point、Sophos、OpenVPN Technologies 以及微软等，亦包含 OpenVPN、Openswan 以及 IPsec-Tools 等高人气开源工具。不过在使用这些软件方案的同时，大家需要自行负担部分管理责任，包括对其进行配置、补丁安装及升级等。

需要注意的是，这一设计方案会给网络体系带来潜在的单点故障，这是因为软件 VPN 方案运行在单一 Amazon EC2 实例之上。参阅附录一：软件 VPN 实例高级高可用性架构以了解更多细节信息。

扩展阅读

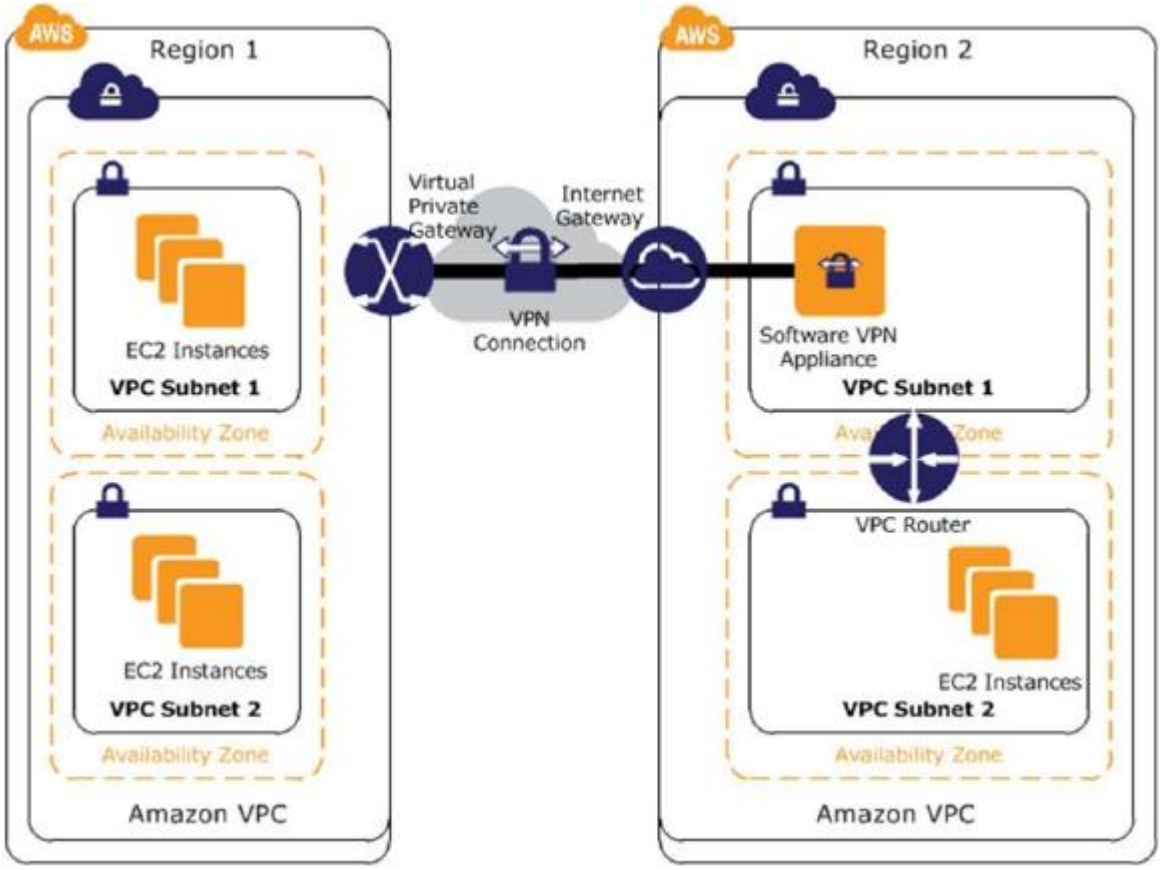
- 来自 AWS Marketplace 的各 VPN 方案
- 技术简介——将多套 VPC 与 EC2 实例对接（IPsec）[21]
- 技术简介——将多套 VPC 与 EC2 实例对接（SSL）[22]

软件到硬件 VPN

Amazon VPC 提供出色的灵活性，允许大家将硬件 VPN 与软件 VPN 选项加以结合，从而实现多套 VPC 的彼此互连。利用这一设计，大家能够在软件 VPN 方案与虚拟专有网关之间建立起安全 VPN 通道，从而接入归属于同一大型虚拟专有网络中的多套 VPC，且允许各 VPC 中的实例以无缝化方式利用专有 IP 地址进行彼此对接。对于希望跨越多个 AWS 服务区且需要发挥 AWS 管理硬件 VPN 端点提供的自动化多数据中心冗余及故障转移等 VPN 连接中 VGW 端内置优势的客户，我们推荐大家使用此选项。这套方案在单一 Amazon VPC 当中利用一套虚拟专有网关，同时配合存在于另一 Amazon VPC 内的虚拟专有网关及互联网网关的结合体，具体如图九所示。

[21] http://aws.amazon.com/articles/5472675506466066

[22] http://aws.amazon.com/articles/0639686206802544



图九：服务区间 VPC 到 VPC 路由

需要注意的是，这套设计方案会给网络系统带来潜在的单点故障可能性，这是因为 Astaro Security Gateway 运行在单一 Amazon EC2 实例之上。请参阅附录一：软件 VPN 实例高级高可用性架构以了解更多细节信息。

扩展阅读

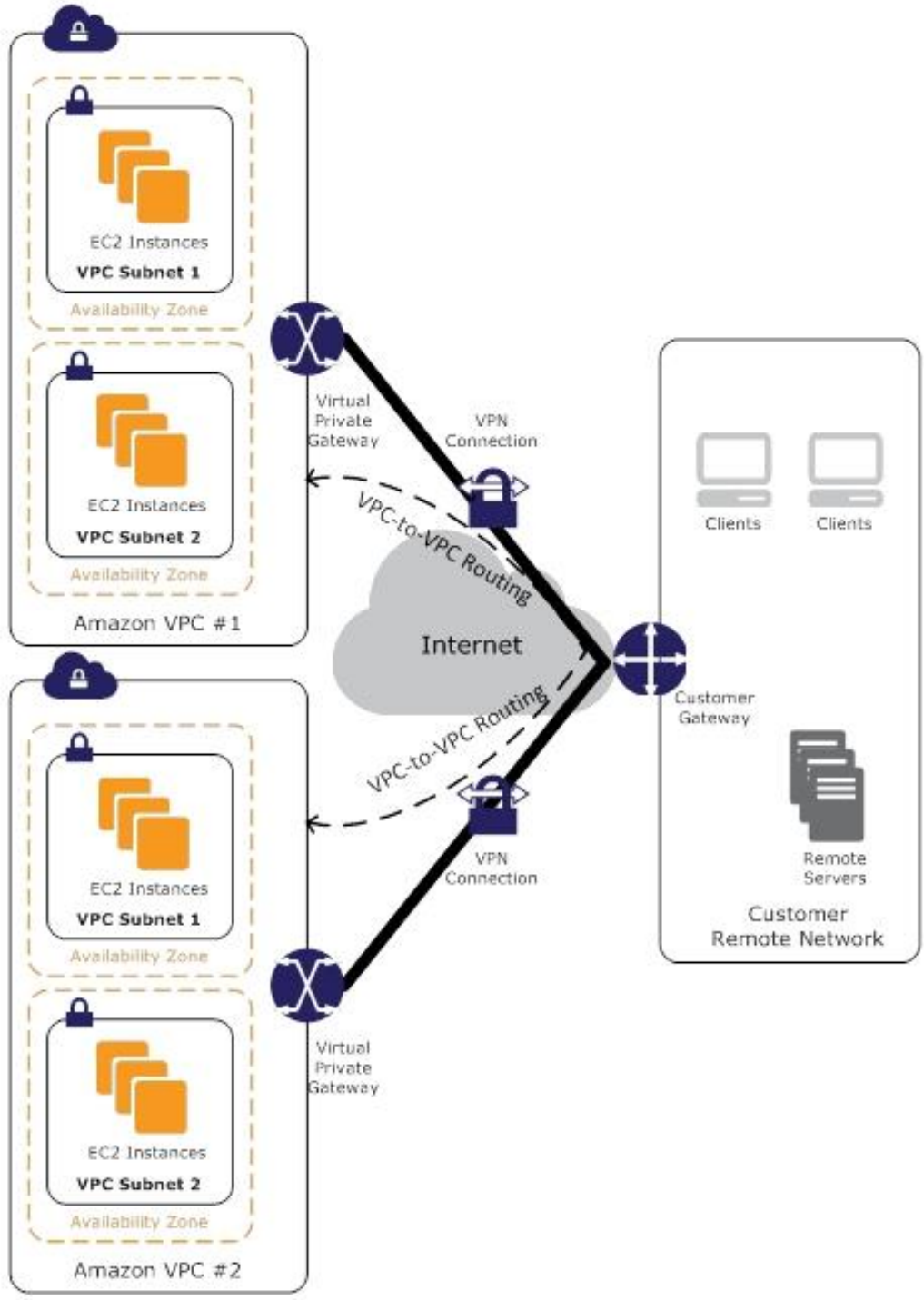
- 技术简介——利用 Sophos Security Gateway 连接多套 VPC[23]
- 配置 Windows Server 2008 R2 作为 Amazon 虚拟专有云的客户网关[24]

[23] http://aws.amazon.com/articles/1909971399457482

[24] http://docs.amazonwebservices.com/AmazonVPC/latest/UserGuide/CustomerGateway-Windows.html

硬件 VPN

Amazon VPC 提供此选项以创建一套硬件 IPsec VPN，用于将您的远程网络通过互联网与 Amazon VPC 进行对接。大家亦可利用多条硬件 VPN 连接在各 Amazon VPC 之间实现流量路由，具体如图十所示。



图十：在多套 VPC 间进行流量路由

对于希望跨越多个 AWS 服务区且需要发挥 AWS 管理硬件 VPN 端点提供的自动化多数据中心冗余及故障转移等 VPN 连接中 VGW 端内置优势的客户，我们推荐大家使用此选项。尽管上图中没有体现，但 Amazon VGW 会标明两个不同 VPN 端点，其位于两座物理隔离的数据中心当中以增加各 VPN 连接的可用性。

Amazon VGW 同时支持多客户网关连接（参照前文中‘客户网络到 Amazon VPC 选项’与‘硬件 VPN’章节，以及图二所示），允许大家在 VPN 连接的内部端实现冗余与故障转移机制。这套解决方案还允许大家利用 BGP 对等机制在 AWS 与各远程端点之间进行路由信息交换。大家可以在 BGP 通告当中指定路由优先级、策略以及加权（指标），从而对往来于自有网络及 AWS 间的流量进行网络路径调整。

这套方案从路由角度来看并不理想，因为流量必须经由互联网方可实现往来，但其能够帮助大家更为灵活地控制并管理本地与远程网络间的路由机制，同时可提供对硬件 VPN 连接的潜在复用能力。

扩展阅读

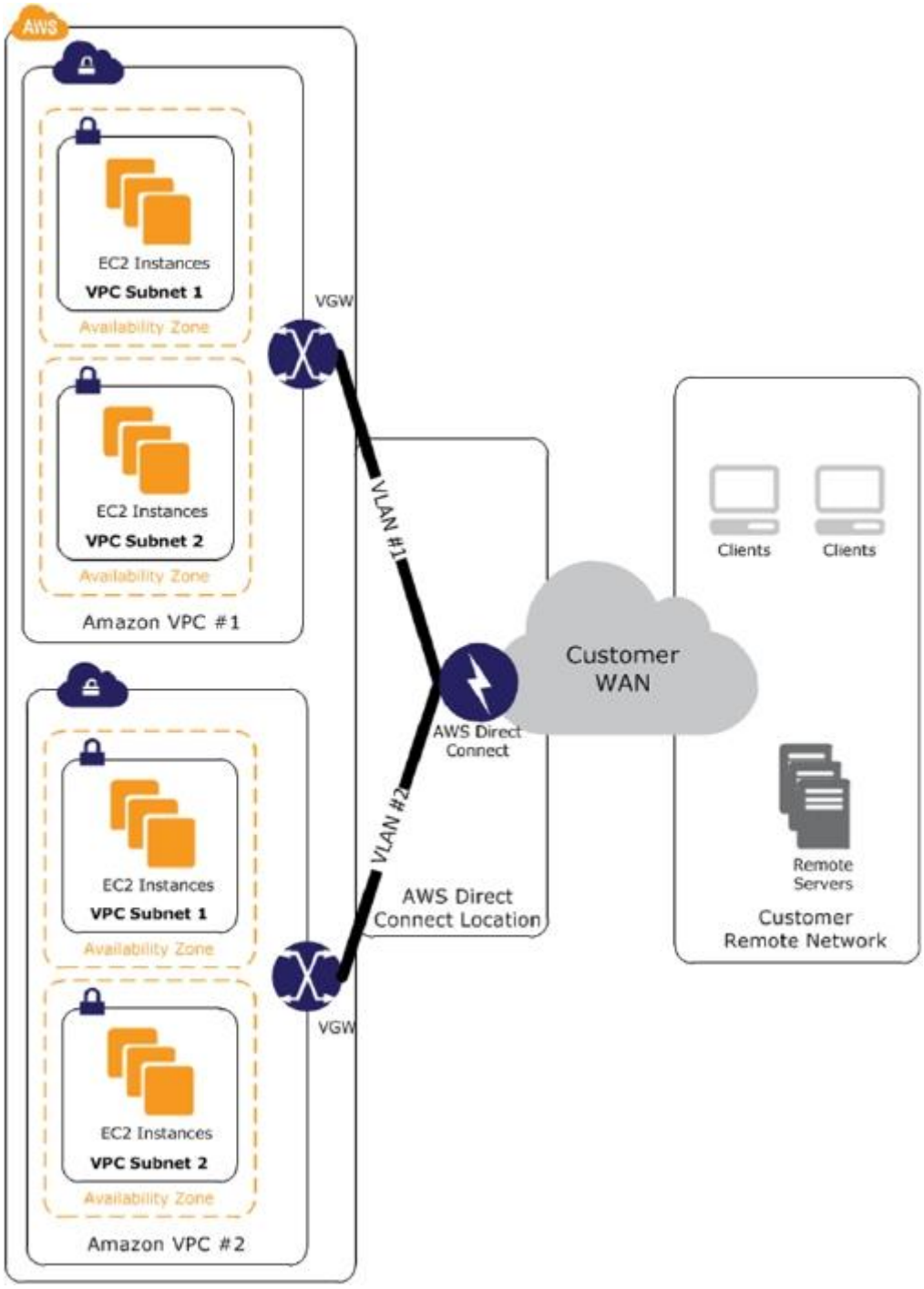
- Amazon VPC 用户指南
- 客户网关设备最低要求
- 已知可与 AMazon VPC 协作的各客户网关设备
- 技术简介——将单一路由器与多套 VPC 对接 [25]

AWS Direct Connect

AWS Direct Connect 能够显著降低由内部设施到 Amazon VPC，或者多套 Amazon VPC 之间的专有网络连接建立流程。此选项能够潜在降低网络使用成本，提升传输带宽通量并提供较其它 VPC 到 VPC 连接选项更具一致性的网络使用体验。

大家可以将单一物理 AWS Direct Connect 连接拆分为多条逻辑连接，且每条分配给一套 VPC。大家随后能够利用这些逻辑连接在各 VPC 之间实现流量路由，如图十一所示。除了实现服务区间路由，大家还能够利用现有 WAN 供应商将 AWS Direct Connect 位置接入其它服务区，并利用 AWS Direct Connect 经由 WAN 主干网络在各服务区间实现流量路由。

[25] http://aws.amazon.com/articles/5458758371599914



图十一：利用 AWS Direct Connect 实现服务区间 VPC 到 VPC 路由

如果大家已经在使用 AWS Direct Connect 或者希望利用 AWS Direct Connect 降低网络成本、提升传输带宽通量并实现更为一致的网络使用体验，那么我们建议您使用这一选项。AWS Direct Connect 能够提供非常高效的路由效果，因为流量可经由附加至各服务区内 AWS 网络的 1 GB 或者 10 GB 光纤连接。另外，这项服务还能够帮助大家更为灵活地控制并管理本地及远程网络的路由机制，同时为 AWS Direct Connect 连接带来潜在的复用能力。

扩展阅读

- AWS Direct Connect 产品页面 [26]
- AWS Direct Connect 位置 [27]
- AWS Direct Connect 常见问题解答 [28]
- AWS Direct Connect 上手指南 [29]

[26] http://aws.amazon.com/directconnect/

[27] http://aws.amazon.com/directconnect/#details

[28] http://aws.amazon.com/directconnect/faqs/

[29] http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Welcome.html

内部用户到 Amazon VPC 连接选项

内部用户要访问 Amazon VPC 资源，通常需要使用客户网络到 Amazon VPC 选项或者使用软件远程接入 VPN 以将内部用户接入至 VPC 资源。利用上述选项，大家可以复用自己的现有内部及远程访问解决方案，从而管理最终用户访问同时保证其拥有指向 AWS 托管资源的无缝化连接体验。更多立足内部环境接入远程访问解决方案的细节信息不在本文的讨论范围之内，大家可参阅“客户网络到 Amazon VPC 选项”以了解部分相关内容。

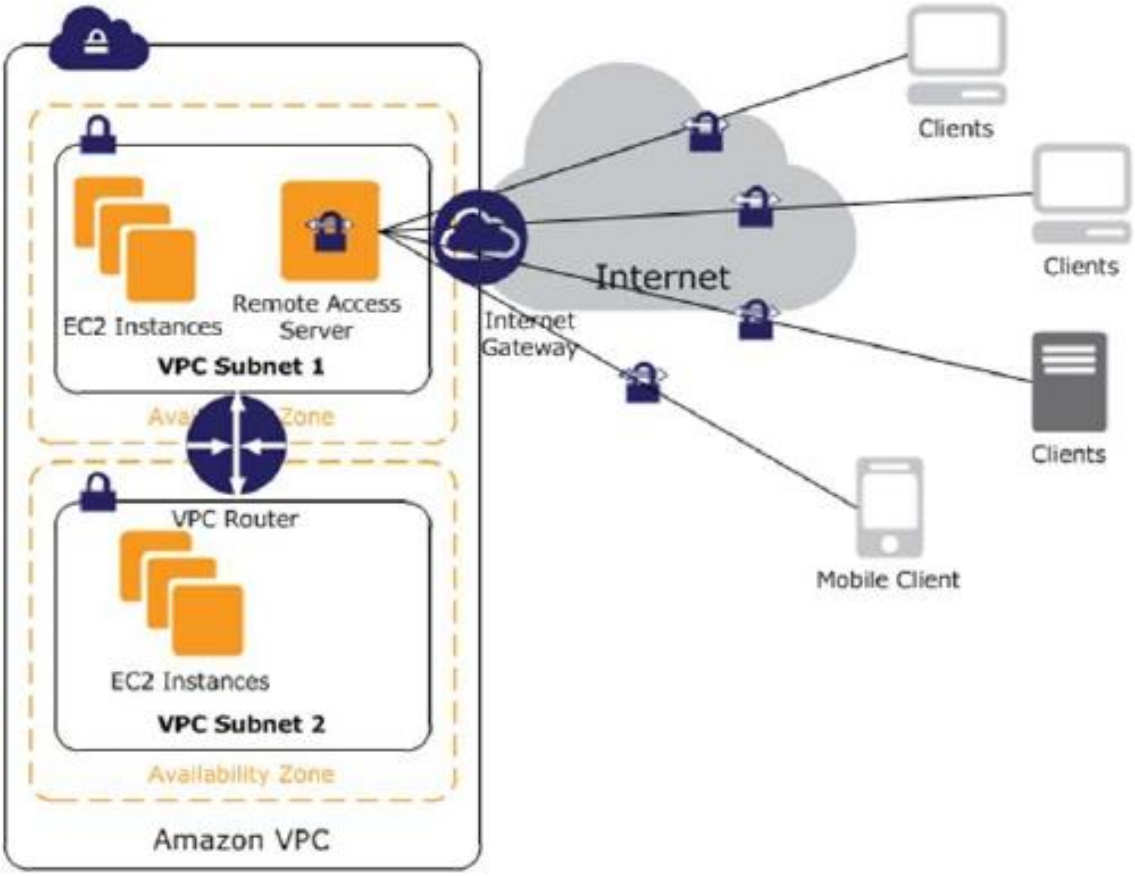
利用软件远程接入 VPN，大家可以利用低成本、弹性且安全的 Amazon Web Services 以实现远程访问解决方案，同时继续提供指向 AWS 托管资源的无缝化访问体验。另外，大家也可以将软件远程接入 VPN 与您的内部网络到 Amazon VPC 选项加以结合，从而提供指向内部网络的远程访问。此选项特别适合那些远程网络体系不太发达的小型企业，或者尚未为员工构建并部署远程访问解决方案的客户。

以下表格概述了上述选项的优势与局限。

选项	用例	优势	局限
用户网络到 Amazon VPC 选项	将数据中心虚拟延伸至 AWS	利用现有最终用户内部及远程接入策略与技术	要求现有最终用户拥有内部及远程接入条件
软件远程接入 VPN	基于云的远程接入解决方案，指向 Amazon VPC 以及/或者内部网络	利用由 AWS 提供的低成本、弹性且安全网络服务实现远程接入解决方案	如果已经具备内部及远程接入实现方案，则具备冗余效果

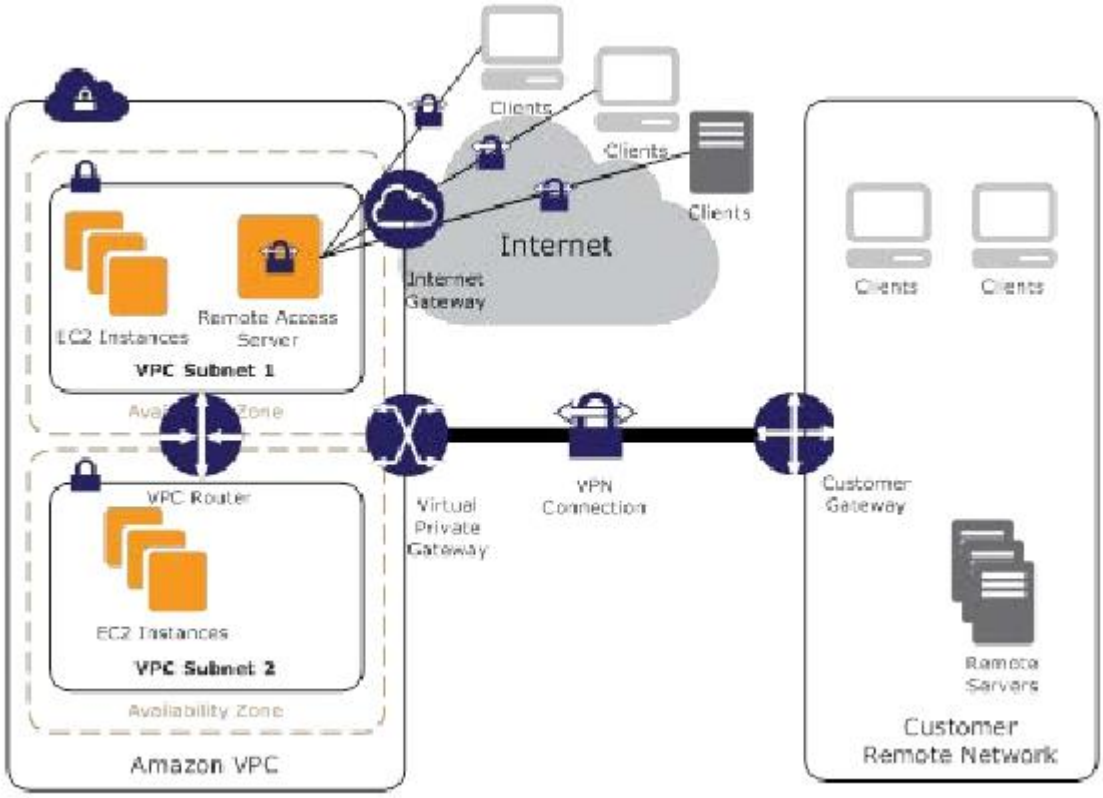
软件远程接入 VPN

大家可以从多家合作伙伴及开源社区构成的生态系统中选择可运行在 Amazon EC2 上的远程接入解决方案。其中包含来自众多知名安全厂商的方案，例如 Check Point、Sophos、OpenVPN Technologies 以及微软等。图十二所示为利用内部远程用户数据库建立的简单远程接入解决方案。



图十二：远程接入解决方案

远程接入解决方案包括高复杂性、支持多种客户端验证机制的选项（例如多因素验证），亦可与 Amazon VPC 或者远程托管身份与访问管理解决方案（利用内部网络到 Amazon VPC 选项之一）——例如微软 Active Directory 或者其它 LDAP/多因素验证解决方案——相集成。图十三所示为这一结合成果，允许远程接入服务器在必要时利用内部访问管理解决方案。



图十三：综合性远程接入解决方案

利用软件 VPN 选项，客户需要负责对远程访问软件进行管理，包括用户管理、配置、补丁安装与升级等等。另外，需要注意的是这一设计可能会给网络系统带来单点故障可能性，因为远程接入服务器运行在单一 Amazon EC2 实例之上。请参阅附录一：软件 VPN 实例高级高可用性架构以了解更多细节信息。

扩展阅读

- 来自 AWS Marketplace 的 VPN 方案
- OpenVPN 接入服务器快速上手指南 [30]

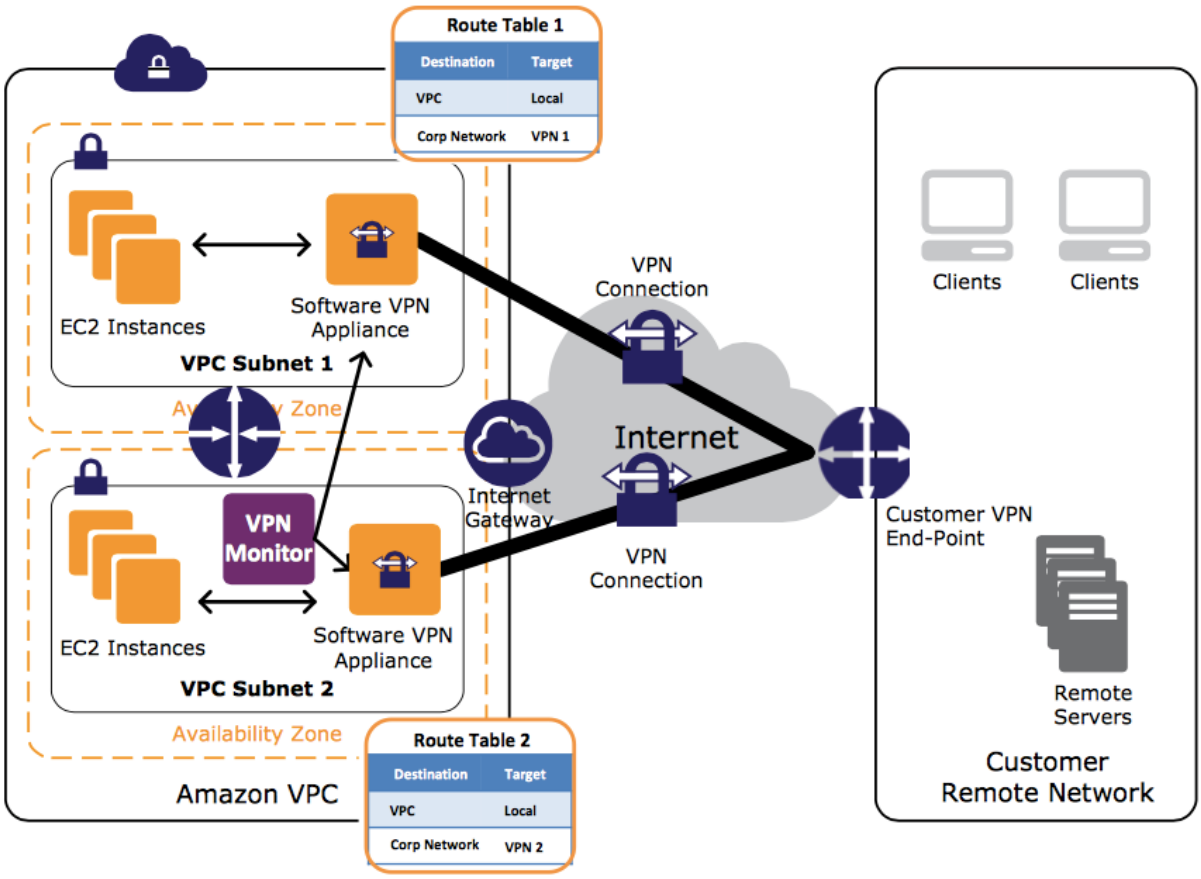
[30] http://docs.openvpn.net/how-to-tutorialsguides/virtual-platforms/amazon-ec2-appliance-ami-quick-start-guide/

总结

AWS 提供多种高效且安全的连接选项，可帮助大家通过将远程网络与 Amazon VPC 相结合以最大程度发挥 AWS 潜在优势。本份白皮书提及的各选项已经为多家企业所使用，并成功将其远程网络或者多套 Amazon VPC 加以对接。我们希望这些选项能够帮助大家顺利满足基础设施连接需求，并确保位于或者托管于任意位置的业务实现顺畅运行。

附录一：软件 VPN 实例高级高可用性架构

创建一条指向软件 VPN 实例的完全弹性 VPC 连接，要求大家设置并配置多个 VPN 实例并利用一个监控实例全程监督各 VPN 连接的运行情况。



图十四：高级高可用性设计

我们建议大家配置自己的 VPC 路由表以并发利用全部 VPN 实例，即立足对应可用区内的各 VPN 实例将来自全部子网的流量进行路由。各个 VPN 实例随后会为共享同一可用区的各实例提供 VPN 连接。

VPN 监控实例

VPN 监控一种定制化实例，大家需要利用其创建并开发监控脚本且加以执行。此类实例旨在运行并监控各 VPN 连接与 VPN 实例的运行状况。如果某一 VPN 实例或者连接发生故障，该监控机制需要停止、终止或者重启该 VPN 实例，同时继续将来自受影响子网的流量重新路由至正常运作的 VPN 实例时，直到两条连接再次恢复正常。由于客户需求多种多样，因此 AWS 目前并不提供设置监控实例的具体方法。不过，大家可以参阅 NAT 实例间的高可用性一文作为起点，用于为软件 VPN 实例构建高可用性解决方案。一旦 VPN 连接发生故障，大家应当考虑利用必要的业务逻辑发出通知以及/或者尝试自动修复网络连接。