AWS 白皮書

Amazon Virtual Private Cloud 連線選項

Amazon Virtual Private Cloud 連線選項: AWS 白皮書

Table of Contents

Amazon Virtual Private Cloud 連線選項

出版日期：二零二三年四月五日 () 文件修訂

摘要

Amazon Virtual Private Cloud (Amazon VPC) 可讓客戶佈建 Amazon Web Services (AWS) 雲端的私有隔離區段，讓他們可以使用客戶定義的 IP 地址範圍在虛擬網路中啟動 AWS 資源。Amazon VPC 為客戶提供多種選項，讓他們將 AWS 虛擬網路與其他遠端網路連線。本文件說明我們客戶可以使用的幾種常見網路連線選項。其中包括用於將遠端客戶網路與 Amazon VPC 整合，以及將多個 Amazon VPC 連接到連續虛擬網路的連線選項。

本白皮書適用於想要檢視可用連線選項的企業網路架構師和工程師或 Amazon VPC 管理員。它提供了各種選項的概觀，以促進網絡連接討論，以及指向更多詳細信息或示例的其他文檔和資源的指針。

簡介

Amazon VPC 提供多種網路連線選項供您使用，具體取決於您目前的網路設計和需求。這些連線選項包括使用網際網路或AWS Direct Connect連線做為網路骨幹，以及終止與 AWS 或使用者管理網路端點的連線。此外，透過 AWS，您可以選擇使用 AWS 服務或使用者管理的網路設備和路由，在 Amazon VPC 和網路之間交付網路路由的方式。本白皮書考慮了以下選項，其中包括概述和每個選項的高層次比較：

- 網路到 Amazon VPC 連線選項
  - AWS Site-to-Site VPN — 描述建立從遠端網路上的網路設備到 Amazon VPC 的受管 IPSec VPN 連線。
  - AWS Transit Gateway + AWS Site-to-Site VPN — 描述使用建立從遠端網路上的網路設備到 Amazon VPC 區域網路中樞的受管 IPSec VPN 連線。AWS Transit Gateway
  - AWS Direct Connect-描述使AWS Direct Connect用建立從遠端網路到 Amazon VPC 的私有邏輯連線。
  - AWS Direct Connect + AWS Transit Gateway— 說明使用AWS Direct Connect和AWS Transit Gateway建立從遠端網路到 Amazon VPC 區域網路中樞的私有邏輯連線。
  - AWS Direct Connect+ AWS Site-to-Site VPN — 描述使用AWS Direct Connect和 AWS 網站對站 Site-to-Site VPN 建立從遠端網路到 Amazon VPC 的私有加密連線。
  - AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN— 說明使用AWS Direct Connect和AWS Transit Gateway建立從遠端網路到 Amazon VPC 區域網路中樞的私有加密連線。
  - AWS VPN CloudHub— 說明建立連線遠端分公司的 hub-and-spoke 模型。
  - VPN 軟體— 說明從遠端網路上的設備與 Amazon VPC 內執行的使用者管理軟體 VPN 設備建立 VPN 連線。
  - AWS Transit Gateway + SD-WAN 解決方案-說明軟體定義廣域網路 (SD-WAN) 解決方案的整合，以使用AWS骨幹或網際網路做為傳輸網路，將數個遠端位置與 Amazon VPC 的區域網路中樞互連。
- Amazon 虛擬私人雲端到 Amazon VPC 連接選項
  - VPC 對等互連— 說明使用 Amazon VPC 對等功能在區域內和區域之間連接 Amazon VPC。
  - AWS Transit Gateway— 說明使用 hub-and-spoke模型AWS Transit Gateway在區域內和跨區域連接 Amazon VPC。
  - AWS PrivateLink— 說明將 Amazon VPC 與虛擬私人雲端介面端點和 VPC 點服務連線。

  - VPN 軟體— 說明使用在每個 Amazon VPC 內執行的使用者受管軟體 VPN 設備之間建立的 VPN 連線來連接 Amazon VPC。
  - 軟體 VPN 到 AWS Site-to-Site VPN— 說明將 Amazon VPC 與在一個 Amazon VPC 中的使用者管理軟體 VPN 設備和連接到另一個 Amazon VPC 的 AWS Site-to-Site VPN 之間建立的 VPN 連線連接。
- 軟體遠端存取 Amazon VPC 連線選項
  - AWS Client VPN— 說明利用 AWS Client VPN 將軟體遠端存取連線到 Amazon VPC。
  - 軟體用戶端 VPN— 說明利用使用者管理的軟體 VPN 設備，將軟體遠端存取連線至 Amazon VPC。
- 交通 VPC-說明使用軟體 VPN 搭配 AWS 管理的 VPN，在 AWS 上建立全球傳輸網路。
- AWS 雲端廣域網路-描述建立受管廣域網路 (WAN)，以便輕鬆建立、管理和監控 Amazon VPC、資料中心和遠端分支機構中資源之間的全域互連。

網路到 Amazon VPC 連線選項

本節提供連接遠端網路與 Amazon VPC 環境的設計模式。這些選項對於將 AWS 資源與現有的現場服務 (例如監控、身分驗證、安全、資料或其他系統) 整合非常有用，方法是將內部網路延伸到 AWS 雲端。此網路延伸模組也可讓您的內部使用者順暢地連線至 AWS 上託管的資源，就像任何其他內部資源一樣。

針對每個連線的網路使用非重疊 IP 範圍時，最佳實現遠端客戶網路的 VPC 連線。例如，如果您想要將一或多個 VPC 連線到公司網路，請確定 VPC 設定為唯一的無類別網域間路由 (CIDR) 範圍。我們建議您配置單一、連續、非重疊的 CIDR 區塊，以供每個 VPC 使用。如需有關 Amazon VPC 路由和約束的其他資訊，請參閱 Amazon VPC 常見問答集。

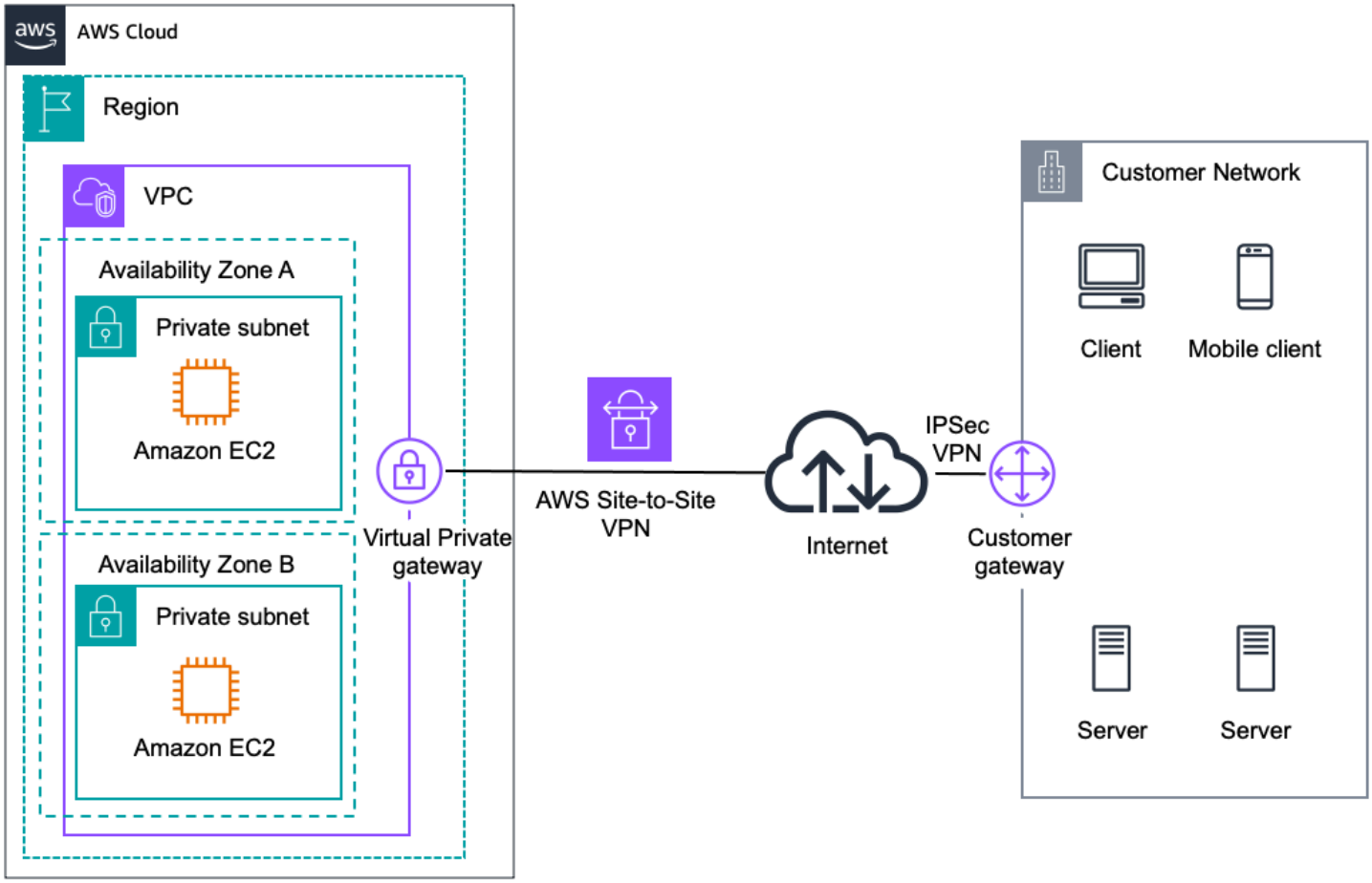
選項	使用案例	優點	限制
AWS Site-to-Site VPN	透過網際網路與個別虛擬私人 VPC 端的 AWS 受管 IPSec VPN 連線	重複使用現有的 VPN 設備和流程 重複使用現有的互聯 AWS 受管的高可用性 VPN 服務 支援靜態路由或動態邊界閘道通訊協定 (BGP) 對等與路由原則	網路延遲、變動性和可用性取決於網際網路狀況 您有責任實施冗餘和故障轉移 (如果需要) 遠端裝置必須支援單跳 BGP (利用 BGP 進行動態路由時)
AWS Transit Gateway + AWS Site-to-Site VPN	AWS 受管 IPSec VPN 透過網際網路連線到多個 VPC 的區域路由器	與上一個選項相同 AWS 管理的高可用性和可擴展性區域網路中樞，最多可容納 5,000 個附件	與上一個選項相同
AWS Direct Connect	透過私人線路連接專用網絡	更可預測的網路效能 降低頻寬成本	可能需要配置額外的電信和託管服務提供商關係或新的網絡電路

選項	使用案例	優點	限制
		支援 BGP 對等互連和路由原則	
AWS Direct Connect + AWS Transit Gateway	透過私人線路與多個 VPC 的區域路由器進行專用網路連線	與上一個選項相同 AWS 管理的高可用性和可擴展性區域網路中樞，最多可容納 5,000 個附件	與上一個選項相同
AWS Direct Connect + AWS Site-to-Site VPN	透過私人線路進行 IPsec VPN 連線	更可預測的網路效能 降低頻寬成本 支援 BGP 對等互連和路由原則 AWS Direct Connect 重複使用現有的 VPN 設備和流程 AWS 受管的高可用性 VPN 服務 支援 VPN 連線上的靜態路由或動態邊界閘道通訊協定 (BGP) 對等與路由原則	可能需要配置額外的電信和託管服務提供商關係或新的網絡電路 您有責任實施冗餘和故障轉移（如果需要） 遠端裝置必須支援單跳 BGP (利用 BGP 進行動態路由時)
AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN	透過私人線路與多個虛擬私人電腦的區域路由器進行 IPsec VPN 連線	與上一個選項相同 AWS 管理的高可用性和可擴展性區域網路中樞，最多可容納 5,000 個附件	與上一個選項相同

選項	使用案例	優點	限制
AWS VPN CloudHub	以 hub-and-spoke 模型 Connect 遠端分公司，以獲得主要或備份連線	重用現有的互聯網連接和 AWS VPN 連接 AWS 受管的高可用性 VPN 服務 支持 BGP 交換路由和路由優先級	網路延遲、變動性和可用性取決於網際網路 使用者管理的分公司端點負責實作備援和容錯移轉 (如有需要)
AWS Transit Gateway + SD-WAN 解決方案	透過軟體定義的廣域網路，使用 AWS 骨幹或網際網路做為傳輸網路，Connect 遠端分公司和辦公室。	支援更廣泛的 SD-WAN 廠商、產品和通訊協定 部分廠商解決方案與 AWS 原生服務整合。	如果 SD-WAN 設備放置在 Amazon VPC 中，您必須負責實作這些設備的 HA (高可用性)。
VPN 軟體	透過網際網路進行軟體設備的 VPN 連線	支援更廣泛的 VPN 廠商、產品和通訊協定 完全客戶管理的解決	您有責任為所有 VPN 端點實作 HA (高可用性) 解決方案 (如有需要)

AWS Site-to-Site VPN

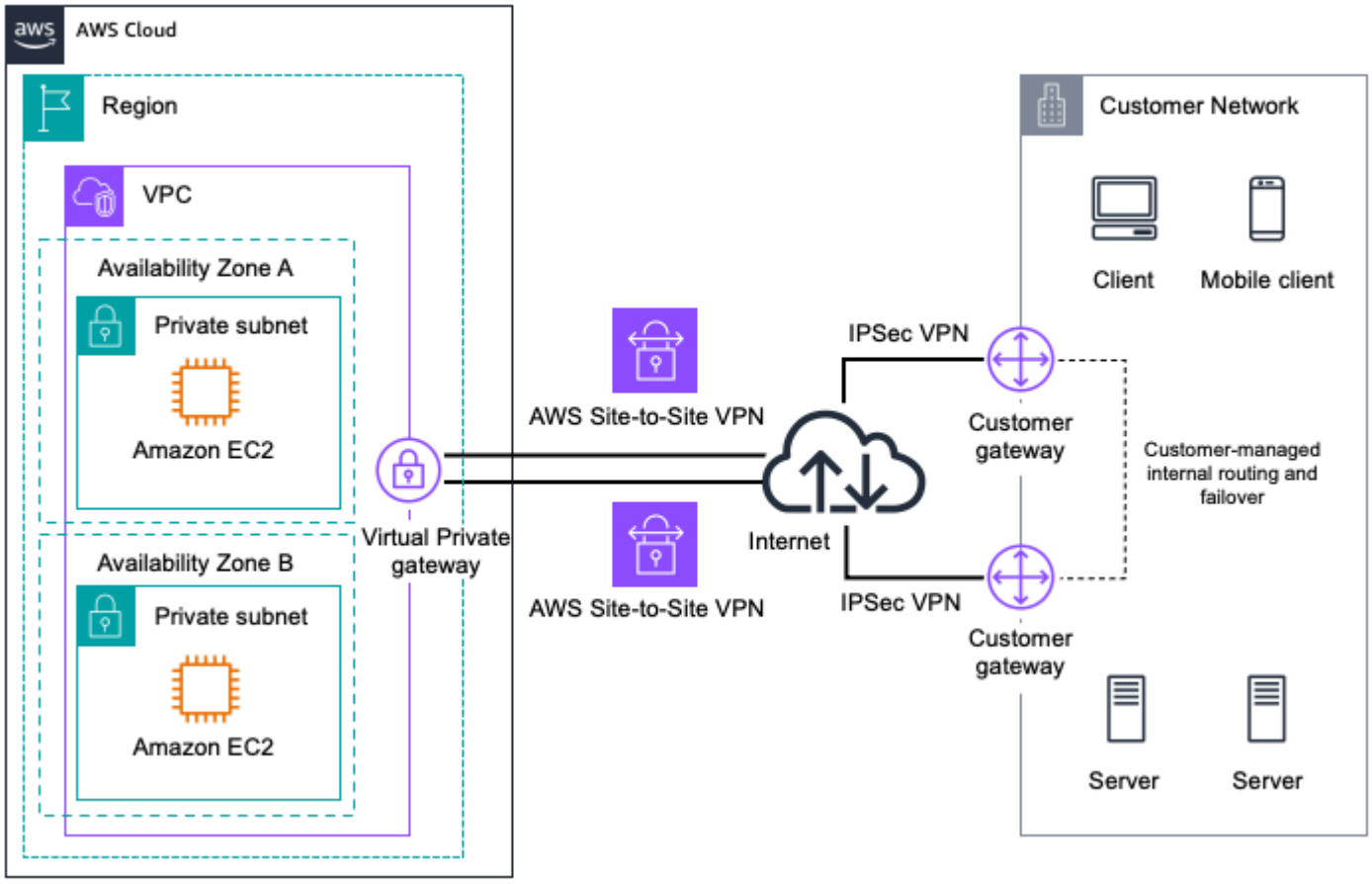
Amazon VPC 提供透過網際網路在遠端網路和 Amazon VPC 之間建立 IPsec VPN 連線的選項，如下圖所示。



AWS Managed VPN

如果您想要利用 AWS 管理的 VPN 端點，其中包含內建於 VPN 連線 AWS 端點的自動備援和容錯移轉，請考慮採用此方法。

虛擬私有閘道也支援並鼓勵多個使用者閘道連線，以便您可以在 VPN 連線端實作備援和容錯移轉，如下圖所示。



Redundant AWS Site-to-Site VPN Connections

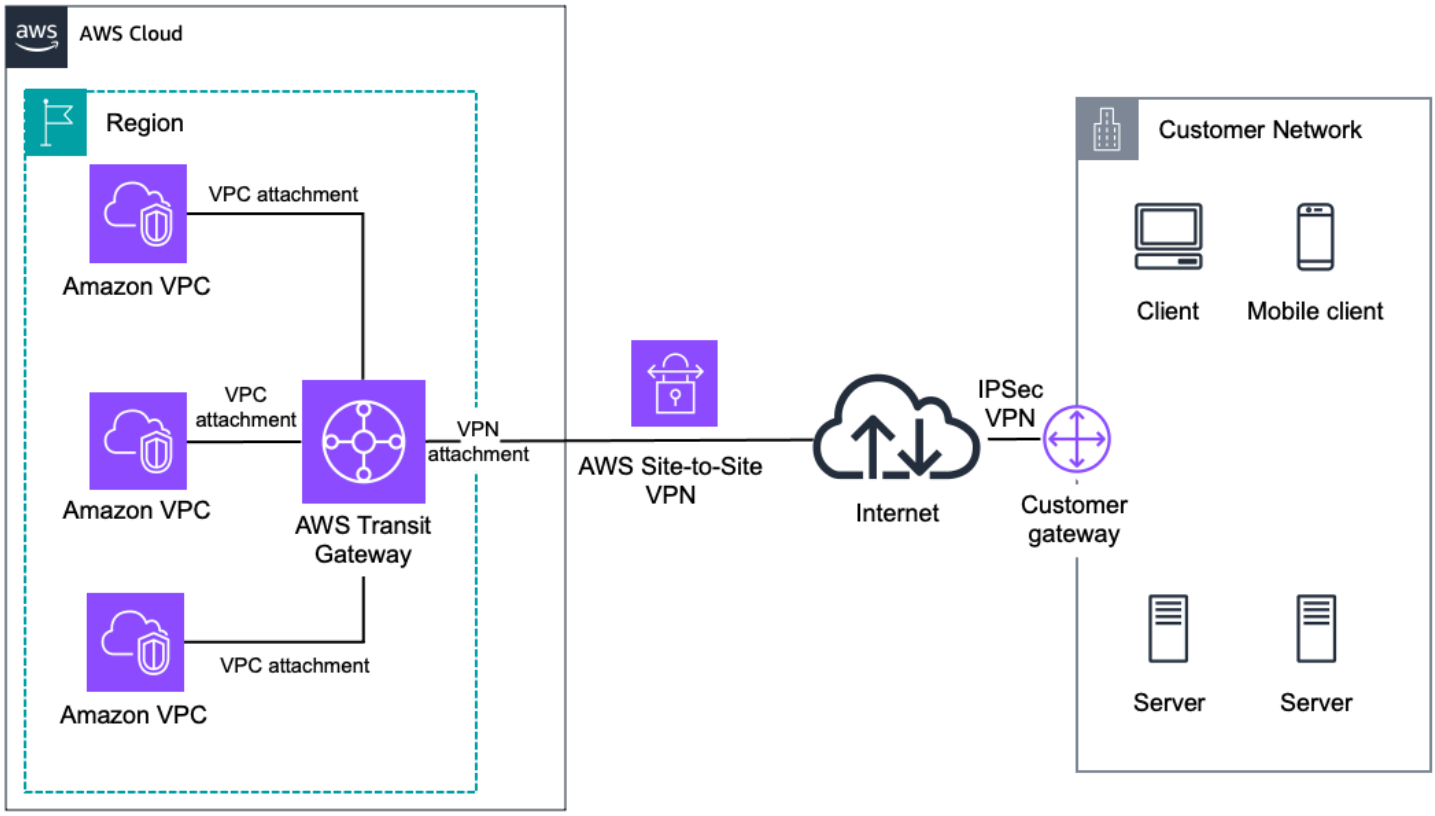
提供動態和靜態路由選項，讓您在路由設定上具有彈性。動態路由使用 BGP 對等互連，在 AWS 和這些遠端端點之間交換路由資訊。使用動態路由，您也可以在 BGP 廣告中指定路由優先順序、政策和權重 (指標)，並影響網路和 AWS 之間的網路路徑。請務必注意，當您使用 BGP 時，IPsec 和 BGP 工作階段都必須在相同的使用者閘道裝置上終止，因此必須能夠終止 IPsec 和 BGP 工作階段。

其他資源

- AWS Site-to-Site VPN 使用者指南
- 客戶閘道裝置的需求
- 透過 Amazon VPC 測試的客戶閘道裝置

AWS Transit Gateway + AWS Site-to-Site VPN

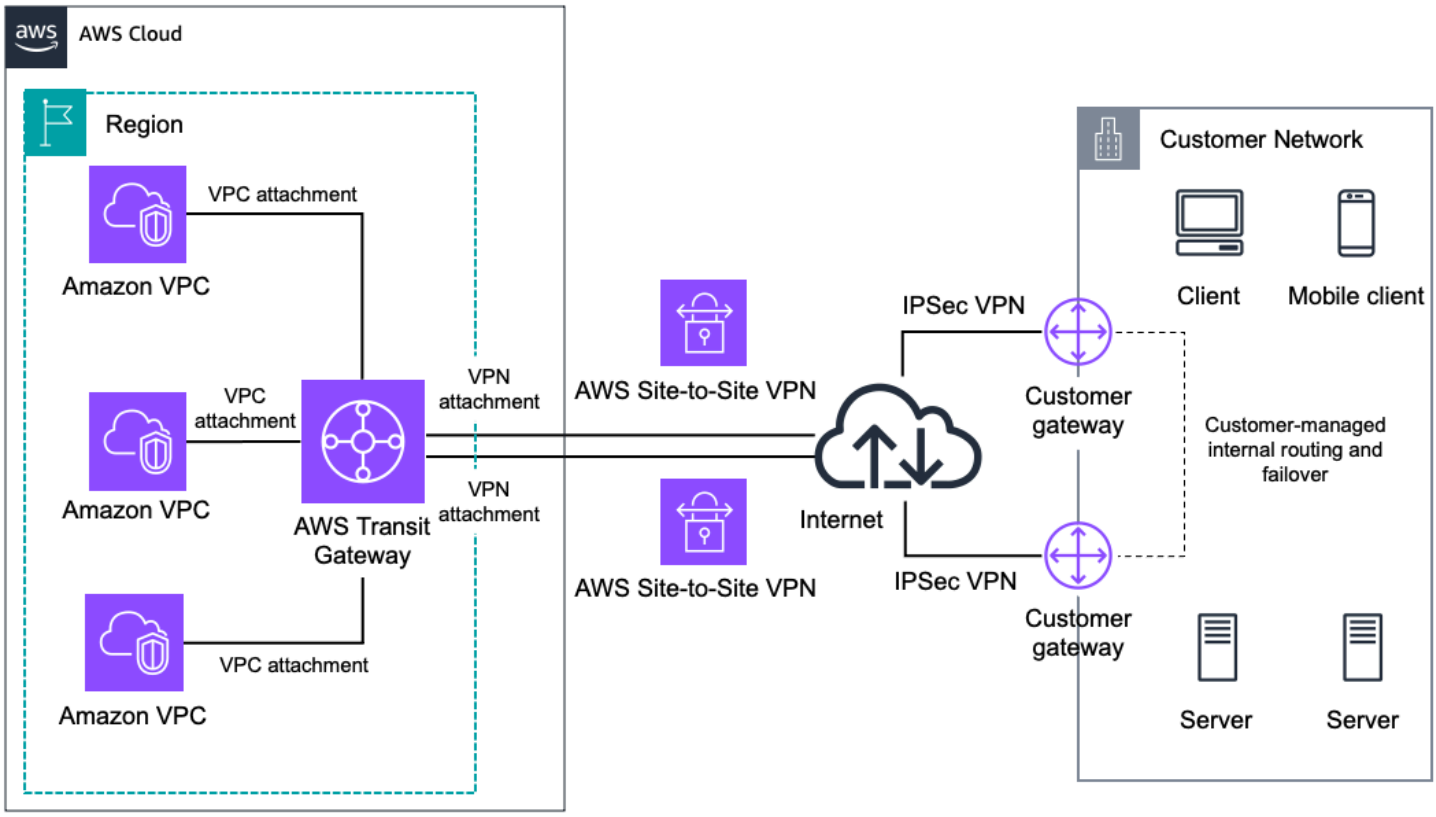
AWS Transit Gateway 是 AWS 受管的高可用性和可擴展性區域網路傳輸中樞，用於互連 VPC 和客戶網路。AWS Transit Gateway + VPN 使用 Transit Gateway VPN 附件，提供在遠端網路和透過網際網路 Transit Gateway 之間建立 IPsec VPN 連線的選項，如下圖所示。



AWS Transit Gateway and AWS Site-to-Site VPN

當您想要利用 AWS 管理的 VPN 端點連線到同一區域中的多個 VPC，而不需要額外成本和管理多個 Amazon VPC 的多個 IPsec VPN 連線，請考慮使用此方法。

AWS Transit Gateway 也支援並鼓勵多個使用者閘道連線，以便您可以在 VPN 連線端實作備援和容錯移轉，如下圖所示。

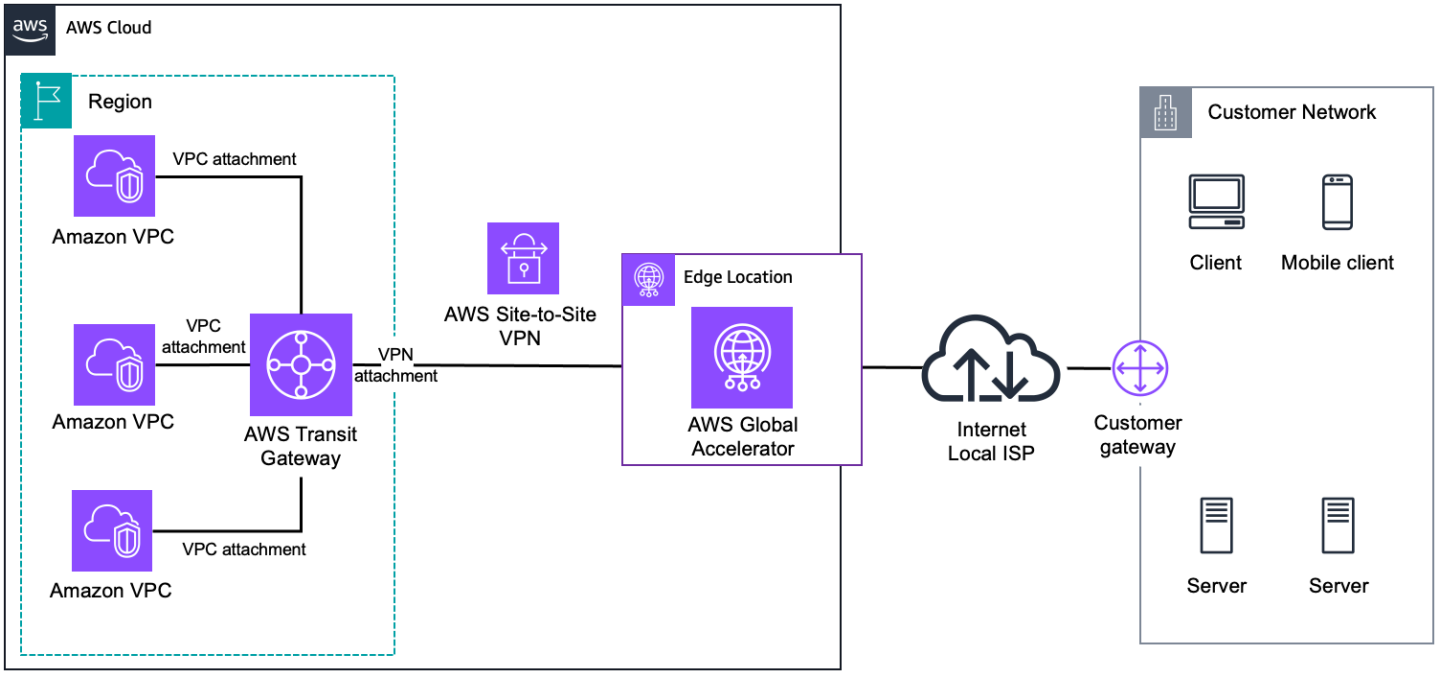


AWS Transit Gateway and Redundant VPN

提供動態和靜態路由選項，可讓您在 Transit Gateway VPN IPsec 附件上彈性進行路由設定。動態路由使用 BGP 對等互連，在 AWS 和這些遠端端點之間交換路由資訊。使用動態路由，您也可以在 BGP 廣告中指定路由優先順序、政策和權重 (指標)，並影響網路和 AWS 之間的網路路徑。請務必注意，當您使用 BGP 時，IPsec 和 BGP 工作階段都必須在相同的使用者閘道裝置上終止，因此必須能夠終止 IPsec 和 BGP 工作階段。

每個 VPN 連線，您可以達到 1.25 Gbps 的輸送量和每秒 14 萬個封包。終止 Transit Gateway 道中的 VPN 連線時，您可以使用同等成本多重路徑 (ECMP) 路由，透過彙總多個 VPN 通道來取得更高的 VPN 頻寬。若要使用 ECMP，您需要在 VPN 連線中設定動態路由 — 使用靜態路由不支援 ECMP。

此外，您可以在 AWS 站 Site-to-Site VPN 連接中啟用加速。加速 VPN 連線使用 AWS Global Accelerator 將流量從您的網路路由到最靠近客戶閘道裝置的 AWS 節點。您可以使用此選項來避免在透過公用網際網路路由傳送流量時可能發生的網路中斷。只有連接到 Transit Gateway 的 VPN 連線才支援加速，如下圖所示：



Accelerated AWS Site-to-Site VPN

最後，關於 IP 定址，上的 Site-to-Site VPN 連接同時 AWS Transit Gateway 支持 IPv4 和 IPv6 流量。適用的規定如下：

- IPv6 僅支援 VPN 通道的內部 IP 位址。 AWS 端點的外部 IP 位址是公用 IPv4 位址。客戶閘道 IP 位址應為公用 IPv4 位址。
- 站台對站台 VPN 連接不能同時支援 IPv4 和 IPv6 流量。如果您的混合式連線需要雙堆疊通訊，您應該為 IPv4 和 IPv6 流量建立不同的 VPN 通道。

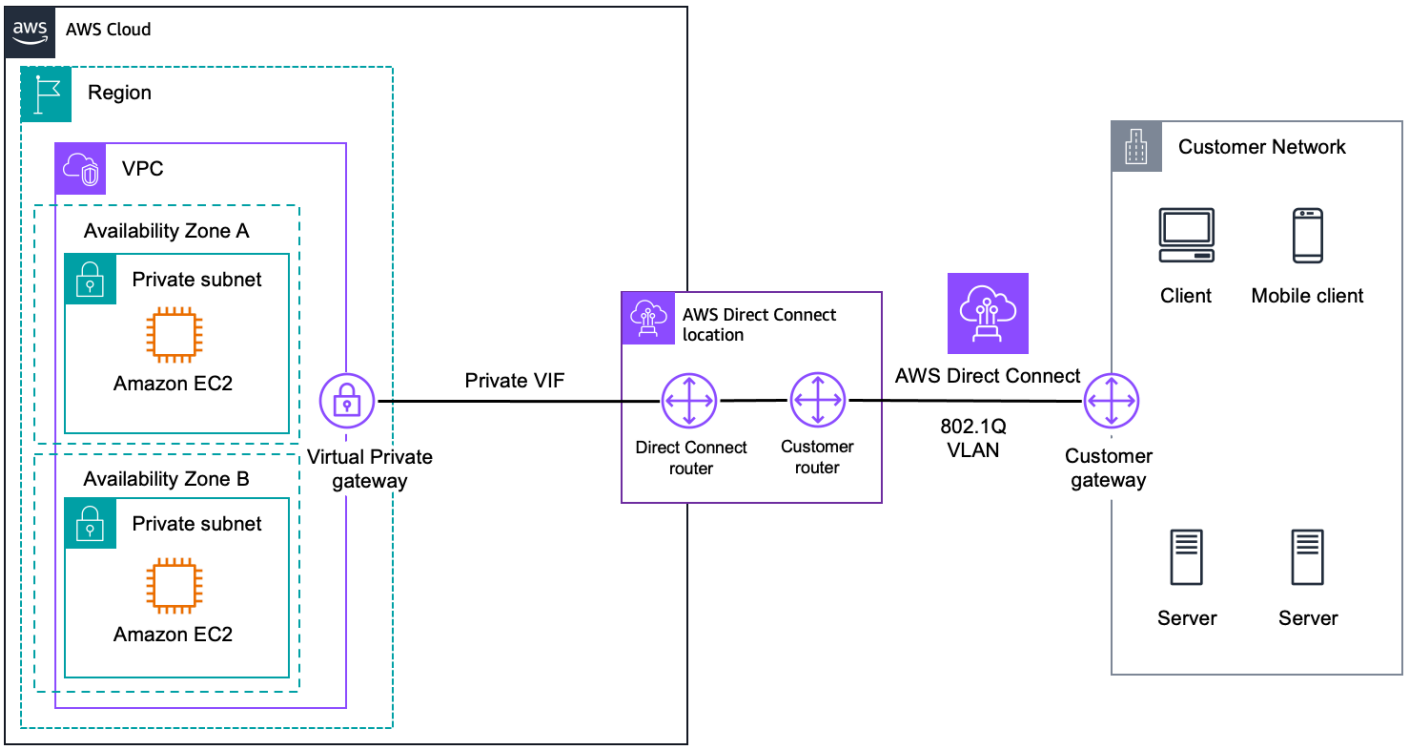
其他資源

- 交通閘道 VPN 附件
- 客戶閘道
- 使用 Site-to-Site VPN
- 加速 Site-to-Site VPN 連線

AWS Direct Connect

AWS Direct Connect可讓您輕鬆建立從內部部署網路到一或多個 VPC 的專用連線。 AWS Direct Connect 可降低網路成本、增加頻寬輸送量，並提供比網際網路連線更一致的網路體驗。它使用業界標準 802.1Q VLAN，使用私有 IP 地址連接到 Amazon VPC 私人雲端。VLAN 使用虛擬介面 (VIF) 進行設定，您可以設定三種不同類型的 VIF：

- 公共虛擬界面-在 AWS 公共端點與您的數據中心，辦公室或託管環境之間建立連接。
- 傳輸虛擬界面-在資料中心、辦公室或主機託管環境之間 AWS Transit Gateway 建立私有連接。本節涵蓋此連線選項???。
- 私有虛擬界面-在 Amazon VPC 資源與您的資料中心、辦公室或主機託管環境之間建立私有連線。下圖顯示了私有 VIF 的使用。



AWS Direct Connect

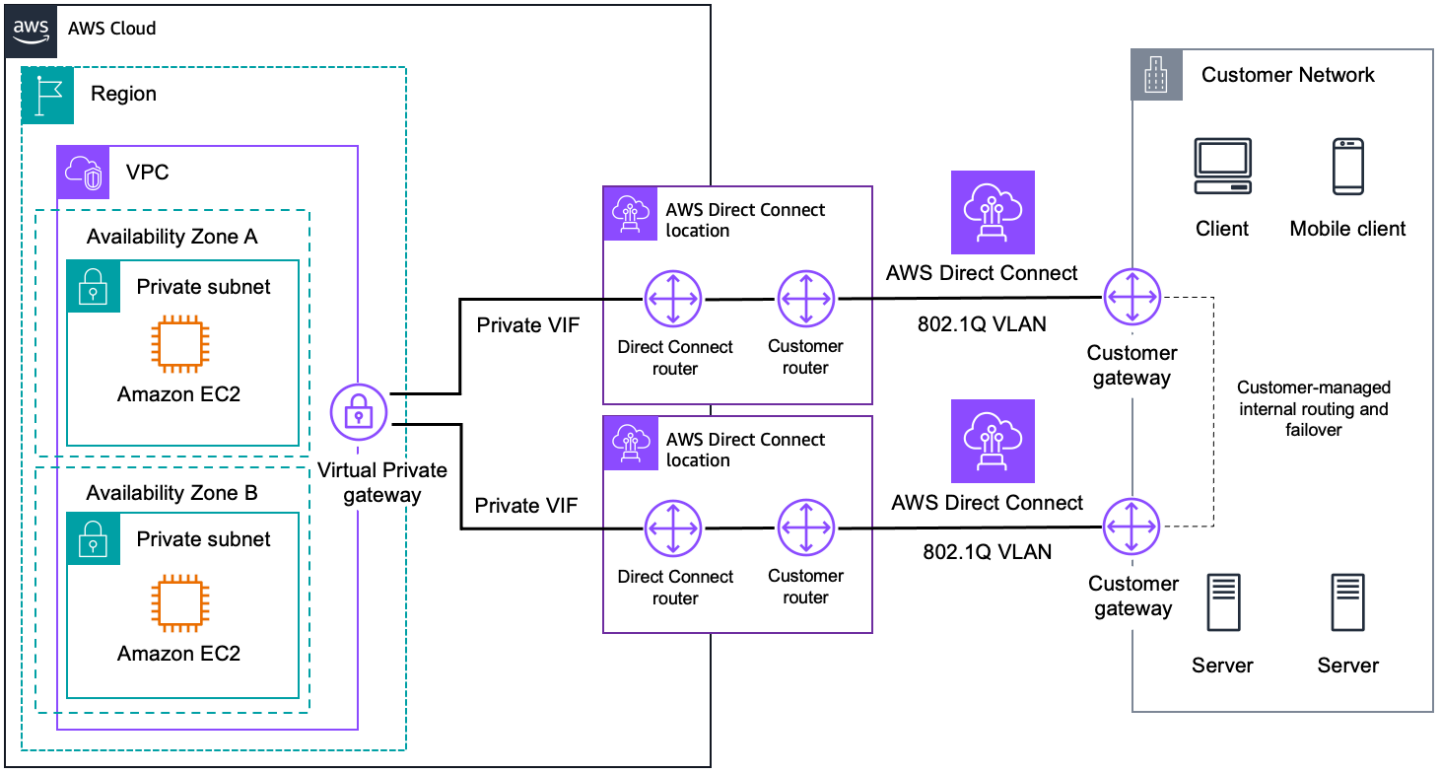
您可以使 AWS Direct Connect 用在「直接 AWS 連線」位置建立與 AWS 裝置的交叉連線，以建立與骨幹的 Connect 線。您可以從我們的任何直接 Connect AWS 地點進入任何地區（中國除外）。如果您在某個地點沒有設備，則可以從 WAN 服務供應商的生態系統中進行選擇，將您的 AWS Direct Connect 端點與遠端網路整合在一個 AWS Direct Connect 位置。

使用 AWS Direct Connect，您有兩種類型的連接：

- 專用連線，其中實體乙太網路連線與單一客戶相關聯。您可以訂購 1、10 或 100 Gbps 的連接埠速度。您可能需要與合作夥伴計畫中的合作 AWS Direct Connect 夥伴合作，協助您在 AWS Direct Connect 連線與資料中心、辦公室或主機託管環境之間建立網路電路。
- 託管連線，其中實體乙太網路連線由 AWS Direct Connect 合作夥伴佈建並與您共用。您可以訂購介於 50 兆比特和 10 Gbps 之間的連接埠速度。您可以在合作夥伴建立的連線以及 AWS Direct Connect 連線與資料中心、辦公室或主機代管環境之間的網路電路中與合作夥伴合作。 AWS Direct Connect

對於專用連線，您也可以使用連結彙總群組 (LAG) 在單一 AWS Direct Connect 端點彙總多個連線。您可以將它們視為單一的受管理連線。您最多可以彙總四個 1 或 10-Gbps 連線，以及最多兩個 100-Gbps 連線。

在中討論高可用性時 AWS Direct Connect，建議您使用其他 AWS Direct Connect 連線。AWS Direct Connect 彈性工具組提供指引，協助您在資料中心、辦公室或主機託管環境之間 AWS 建立高度彈性的網路連線。下圖顯示高彈性連線選項的範例，其中兩個 AWS Direct Connect 連線終止在兩個不同 AWS Direct Connect 的位置。

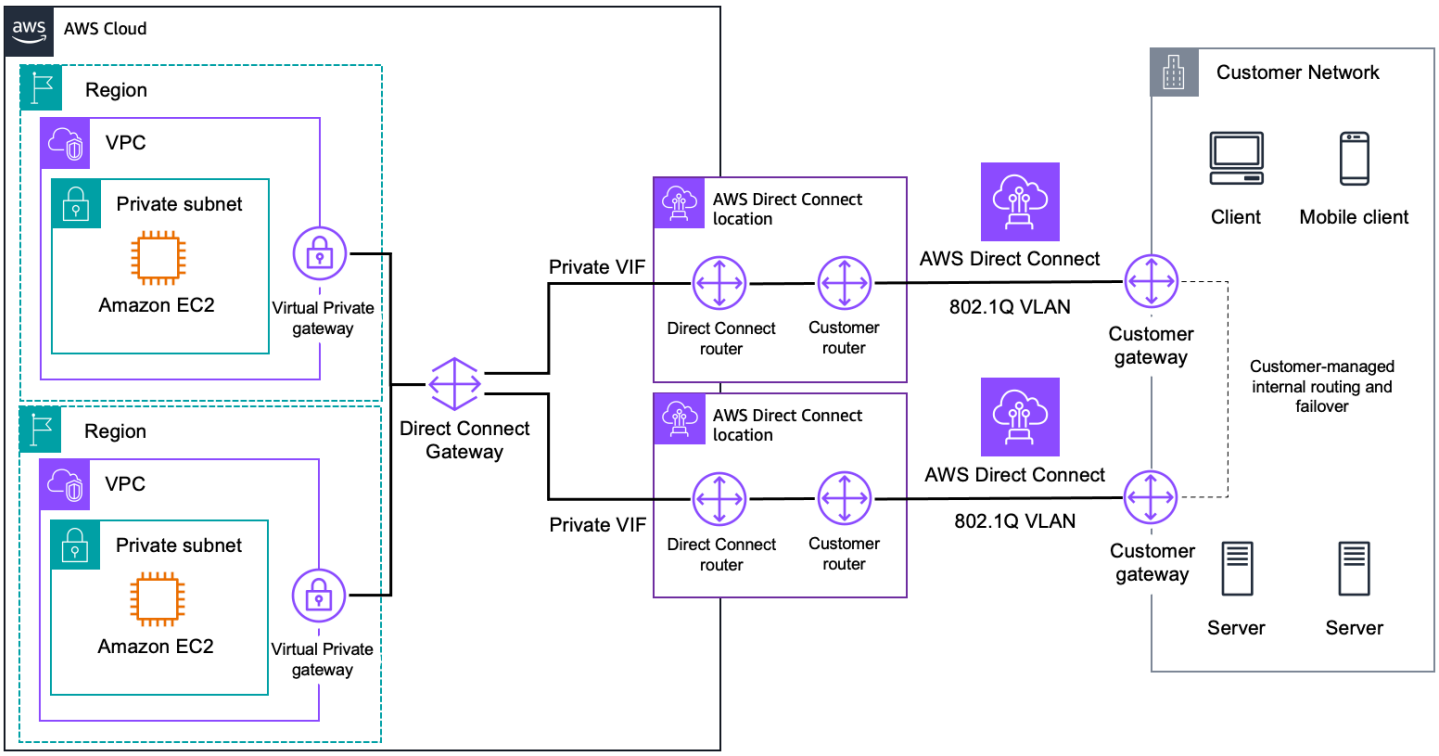


冗餘 AWS Direct Connect

AWS Direct Connect 默認情況下不加密。對於 10 或 100 Gbps 的專用連接，您可以使用 MAC 安全性（MacSec）作為加密選項。對於 1 Gbps 或更小的連線，您可以在連線上方建立 VPN 通道，這個選項

涵蓋在AWS Direct Connect + AWS Site-to-Site VPN和AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN章節中。

其中一個重要資源 AWS Direct Connect 是 Direct Connect 閘道，這是一種全球可用的資源，可讓您連接到多個 Amazon VPC 或跨不同區域或 AWS 帳戶的傳輸閘道。此資源還允許您從一個私有 VIF 或傳輸 VIF 連接到任何參與的 VPC 或傳輸閘道，從而減少 AWS Direct Connect 管理，如下圖所示。



AWS Direct Connect Gateway

在 IP 位址方面， AWS Direct Connect 虛擬介面同時支援 IPv4 和 IPv6 BGP 工作階段，以進行雙堆疊作業。

- 私人和傳輸 VIF IPv4 設定會使用 AWS 產生的 IPv4 位址或您設定的位址。對於公用 VIF IPv4 BGP 對等互連，您必須指定您擁有的唯一公用 /31 IPv4 CIDR (或提交要求以指派 CIDR 區塊)。
- 對於所有類型的 VIF IPv6 BGP 對等互連，AWS 會指派一個無法設定的 /125 CIDR。

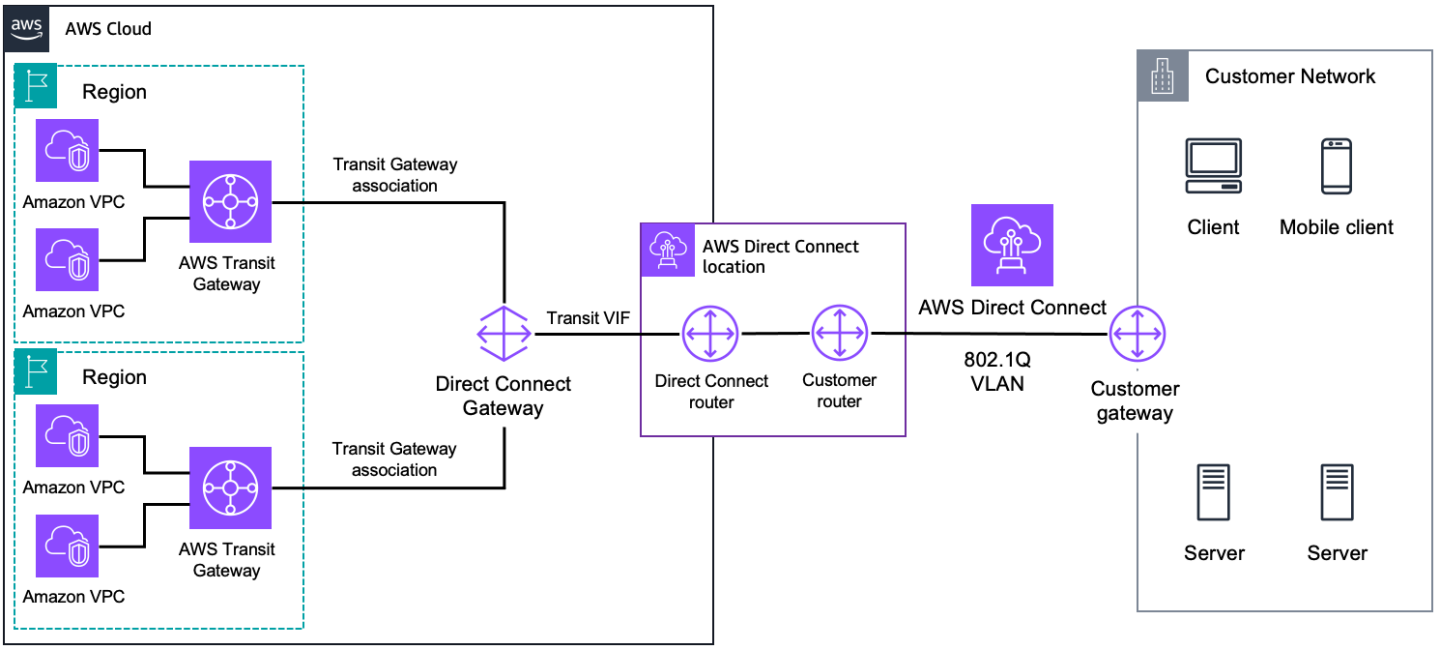
其他資源

- AWS Direct Connect 使用者指南
- AWS Direct Connect 虛擬介面
- AWS Direct Connect 閘道器

- AWS Direct Connect 彈性工具包
- AWS Direct Connect MAC 安全性
- AWS Direct Connect 位置
- AWS Direct Connect 送餐夥伴

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect+ AWS Transit Gateway，使用傳輸 VIF 附件到 Direct Connect 閘道，使您的網絡能夠通過私人專用連接連接多個區域集中式路由器連接。下圖顯示了連接到兩個路由器。



AWS Direct Connect and AWS Transit Gateway

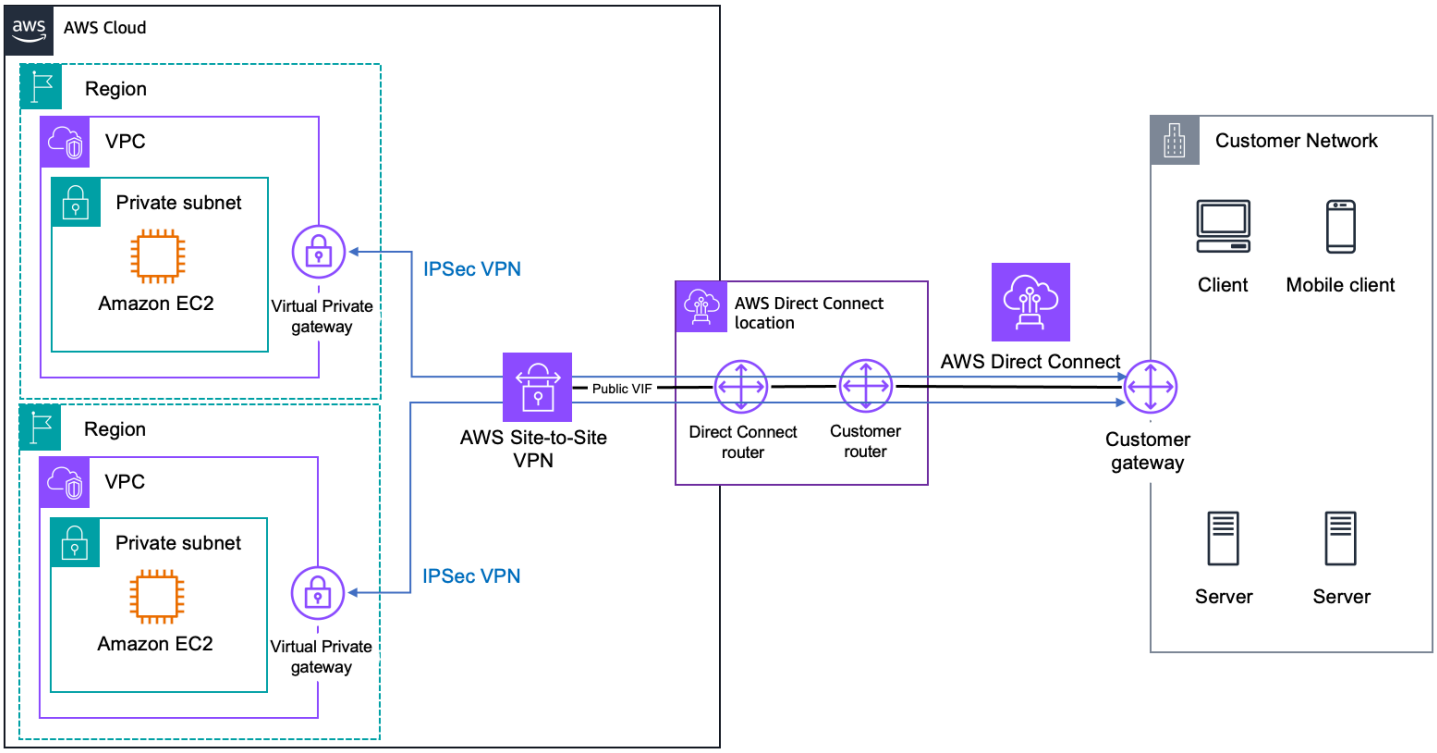
每個都 AWS Transit Gateway 是網路傳輸中樞，可將相同區域中的 VPC 互連，將 Amazon VPC 路由組態整合在一個位置。此解決方案可簡化透過私有連線管理 Amazon VPC 與網路之間的連線，進而降低網路成本、增加頻寬輸送量，並提供比網際網路連線更一致的網路體驗。

其他資源

- AWS Direct Connect 使用者指南
- 連結彙總群組 AWS Direct Connect
- 部落格文章：整合小於 1 Gbps 的託管連線與 AWS Transit Gateway

AWS Direct Connect + AWS Site-to-Site VPN

使用 AWS Direct Connect+ AWS Site-to-Site VPN，您可以將 AWS Direct Connect 連接與 AWS 管理的 VPN 解決方案結合使用。 AWS Direct Connect 公有 VIF 會在您的網路和公有 AWS 資源 (例如 AWS 站點對站點 VPN 端點) 之間建立專用網路連線。建立與服務的連線後，您可以建立與對應的 Amazon VPC 虛擬私有閘道的 IPsec 連線。下圖說明此選項。



AWS Direct Connect and AWS Site-to-Site VPN

此解決方案將 end-to-end 安全 IPsec 連線的優點與低延遲和更高的頻寬相結合，提供比網際網路 VPN 連線更一致的網路體驗。 AWS Direct Connect BGP 連線工作階段會在 AWS Direct Connect 與您的路由器之間建立在公用 VIF 上。另一個 BGP 工作階段或靜態路由器會在虛擬私有閘道與 IPsec VPN 通道上的路由器之間建立。

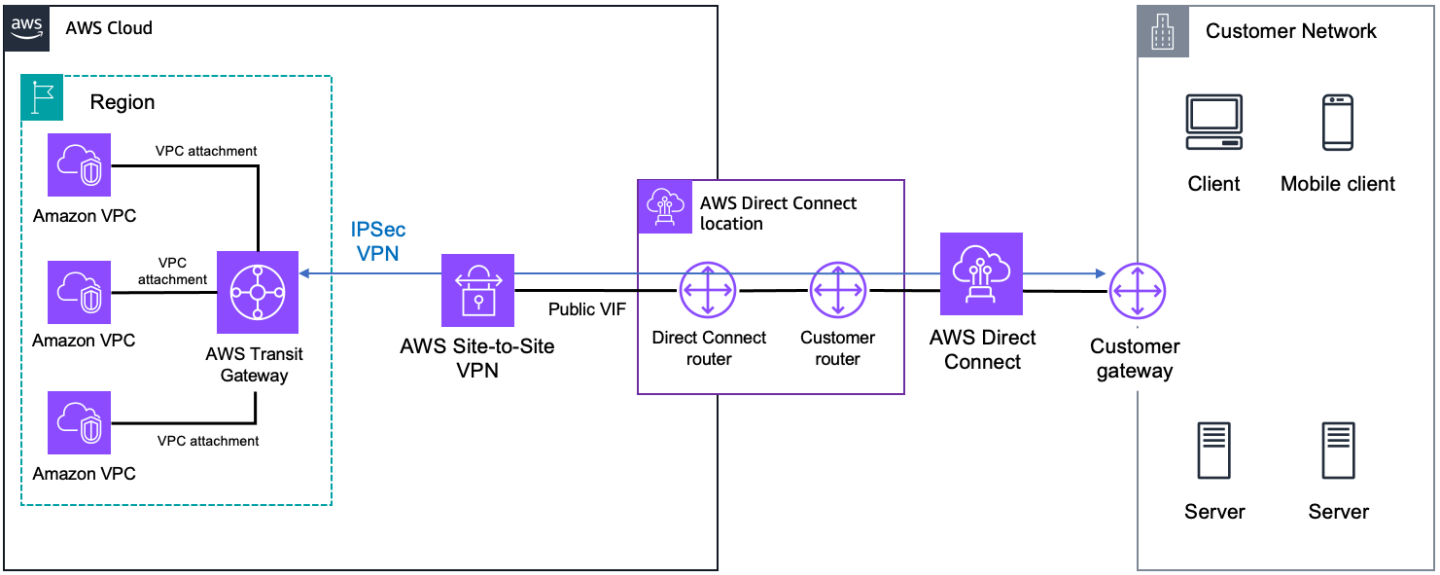
其他資源

- AWS Direct Connect
- AWS Direct Connect 虛擬介面
- AWS Site-to-Site VPN 使用者指南

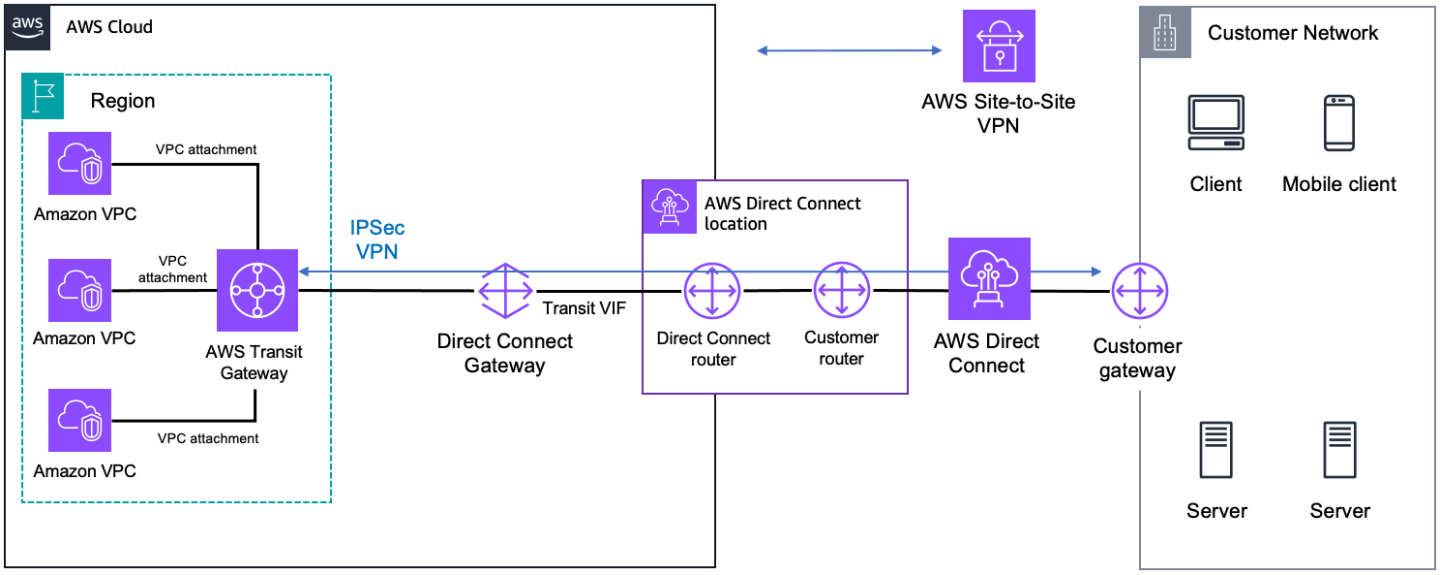
AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN

使用 AWS Direct Connect+ AWS Transit Gateway+ AWS Site-to-Site VPN，您可以透過私有專用連線為 Amazon VPC 啟用網路和區域集中式路由器之間的 end-to-end IPSec 加密連線。

您可以使用 AWS Direct Connect 公有 VIF，先在網路與公有 AWS 資源 (例如 AWS 站點對站點 VPN 端點) 之間建立專用網路連線。建立此連線之後，您可以建立與的 IPsec 連線。 AWS Transit Gateway 下圖說明此選項。



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)

當您想要簡化管理，並將 IPsec VPN 連線到同一區域中多個 Amazon VPC 的成本降至最低時，請考慮採用這種方法，以及透過網際網路 VPN 進行私人專用連線所帶來的低延遲和一致的網路體驗優勢。BGP 工作階段會使用公用或傳輸 VIF 在路由器 AWS Direct Connect 和路由器之間建立。另一個 BGP 工作階段或靜態路由器會在 IPsec VPN 通道上 AWS Transit Gateway 與您的路由器之間建立。

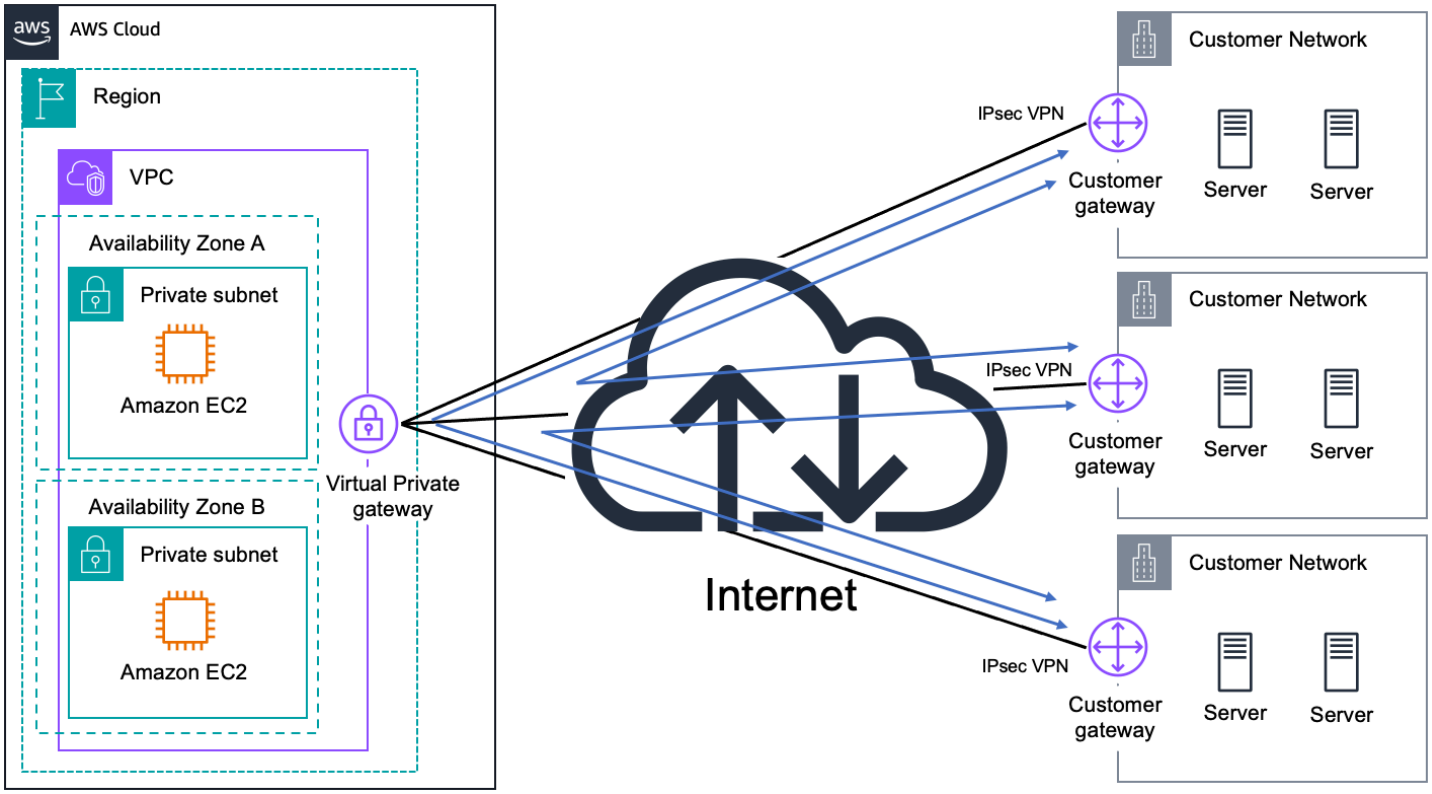
其他資源

- AWS Direct Connect 虛擬界面
- 交通閘道 VPN 附件
- 客戶閘道裝置的需求
- 透過 Amazon VPC 測試的客戶閘道裝置
- AWS Site-to-Site VPN — 具有私有 IP VPN AWS Direct Connect

AWS VPN CloudHub

在先前描述的 AWS 受管 VPN 選項上進行建置，您可以使用安全地從一個網站到另一個網站通訊 AWS VPN CloudHub。在一個簡單的 hub-and-spoke 模型上 AWS VPN CloudHub 運行，您可以在 VPC 上使用或不使用 VPC。如果您有多個分公司和現有的網際網路連線，並且想要為這些遠端辦公室之間的主要或備份連線實作便利且可能低成本的 hub-and-spoke 模式，請使用此方法。

下圖顯示 AWS VPN CloudHub 架構，其中含有線條表示透過其 AWS VPN 連線路由之遠端站台之間的網路流量。



AWS VPN CloudHub

AWS VPN CloudHub 使用具有多個客戶閘道的 Amazon VPC 虛擬私有閘道，每個閘道都使用唯一的 BGP 自主系統編號 (ASN)。遠端站台的 IP 範圍不得重疊。您的閘道會透過其 VPN 連線公告適當的路由 (BGP 前置詞)。這些路由通告會接收並重新通告給每個 BGP 對等，以便每個站台都可以向其他網站傳送資料並從其他網站接收資料。

其他資源

- 使用 VPN 在站點之間提供安全通信 CloudHub
- AWS Site-to-Site VPN 使用者指南
- 客戶閘道裝置的需求
- 透過 Amazon VPC 測試的客戶閘道裝置

AWS Transit Gateway + SD-WAN 解決方案

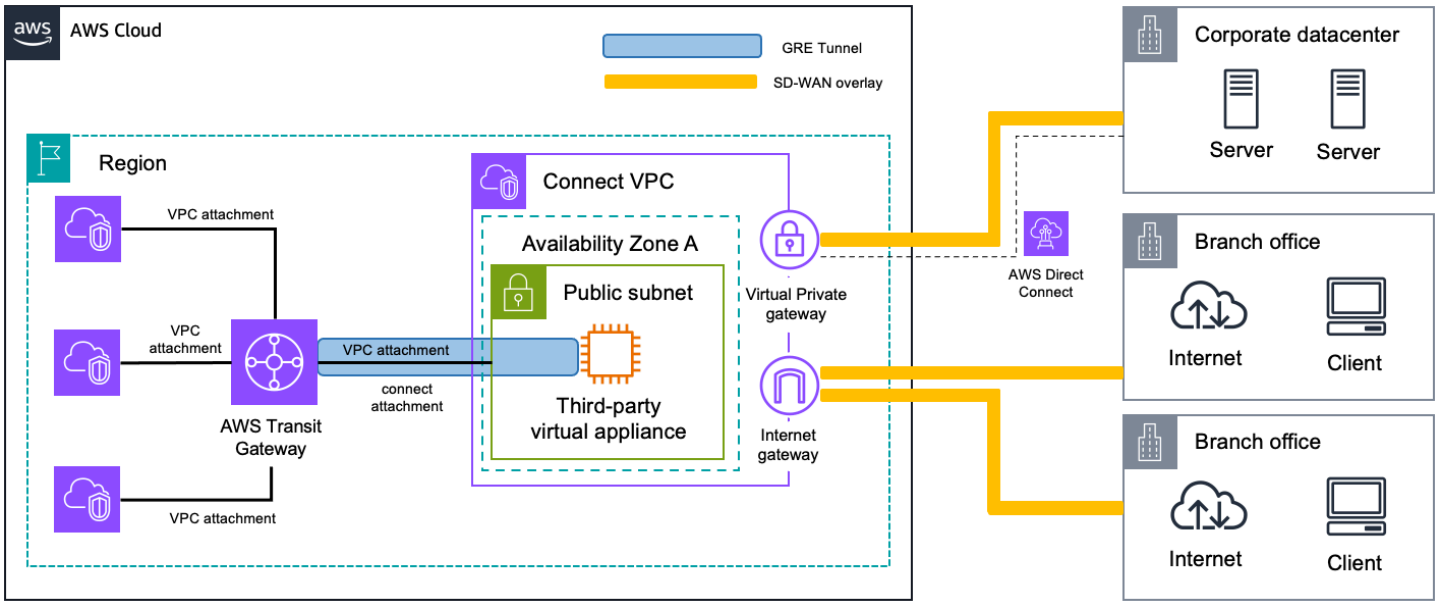
軟體定義的廣域網路 (SD-WAN) 可用來透過不同傳輸網路 (例如公用網際網路、MPLS 網路或 AWS 骨幹) 連接資料中心、辦公室或主機代管環境，並根據網路條件、應用程式類型或服務品質 (QoS AWS Direct Connect) 要求，自動和動態管理最合適且有效率的路徑上的流量。

如果您擁有複雜的網路拓撲，且有數個資料中心、辦公室或主機託管環境需要在本身與 AWS 之間進行通訊，請使用此方法。SD-WAN 解決方案可以幫助您有效地管理這種類型的網絡。

在討論 SD-WAN 網路與 AWS 的連線時， AWS Transit Gateway 提供受管高可用性且可擴展的區域網路傳輸中樞，以互連 VPC 和 SD-WAN 網路。Transit Gateway 連接附件提供原生方式，將 SD-WAN 基礎設施和設備與 AWS 連接。如此一來，您就可以輕鬆地將 SD-WAN 擴充至 AWS，而不需要設定 IPsec VPN。

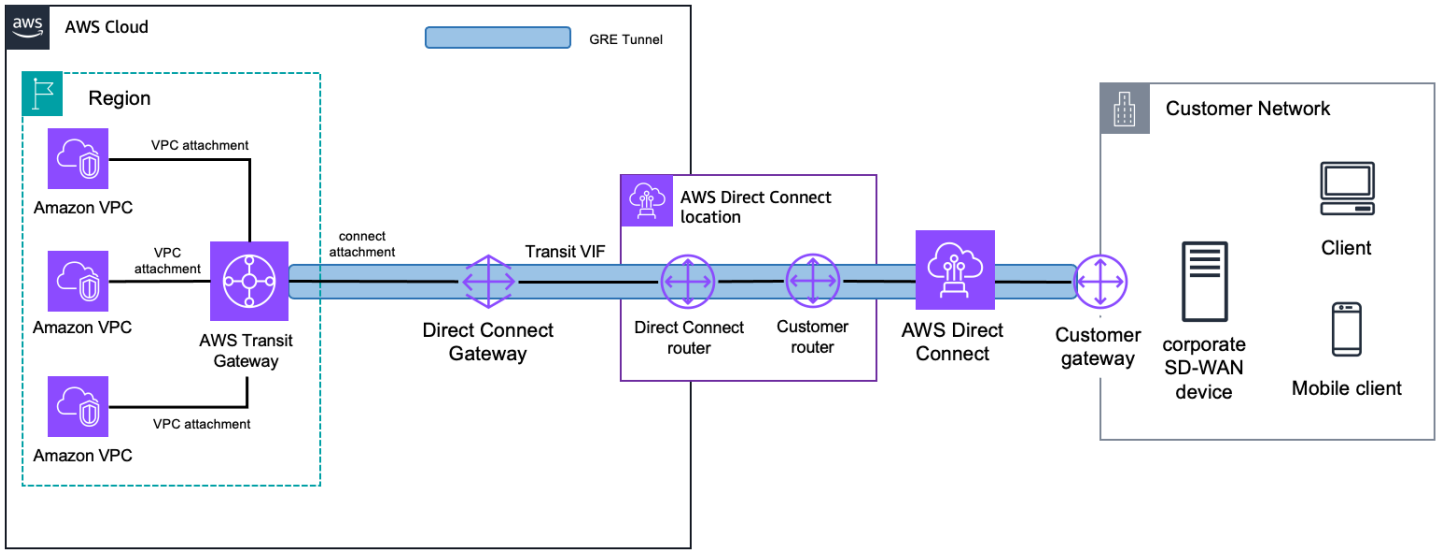
Transit Gateway 連線附件支援一般路由封裝 (GRE)，相較於 VPN 連線，可提供更高的頻寬效能。它支持邊界網關協議（BGP）進行動態路由，並且無需配置靜態路由。這樣可簡化網路設計，並降低相關的營運成本。此外，它與 Transit Gateway 網路管理員的整合可透過全域網路拓撲、附件層級效能指標和遙測資料提供進階能見度。

使用連接附件將 SD-WAN 網絡集成到 Transit Gateway 時，您有兩種常見的模式。第一個是將 SD-WAN 網路的虛擬設備放置在 AWS 內的 VPC 中。然後，您可以使用 VPC 附件作為 Transit Gateway 的基礎傳輸連接虛擬應用裝置和 Transit Gateway 之間的附件，如下圖所示。



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

或者，您可以將 SD-WAN 流量擴展和區段到 AWS，而無需新增額外的基礎設施。您可以使用 AWS Direct Connect 連線作為基礎傳輸來建立 Transit Gateway 連接附件，如下圖所示。



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

使用 Transit Gateway 連線附件時，需注意一些注意事項：

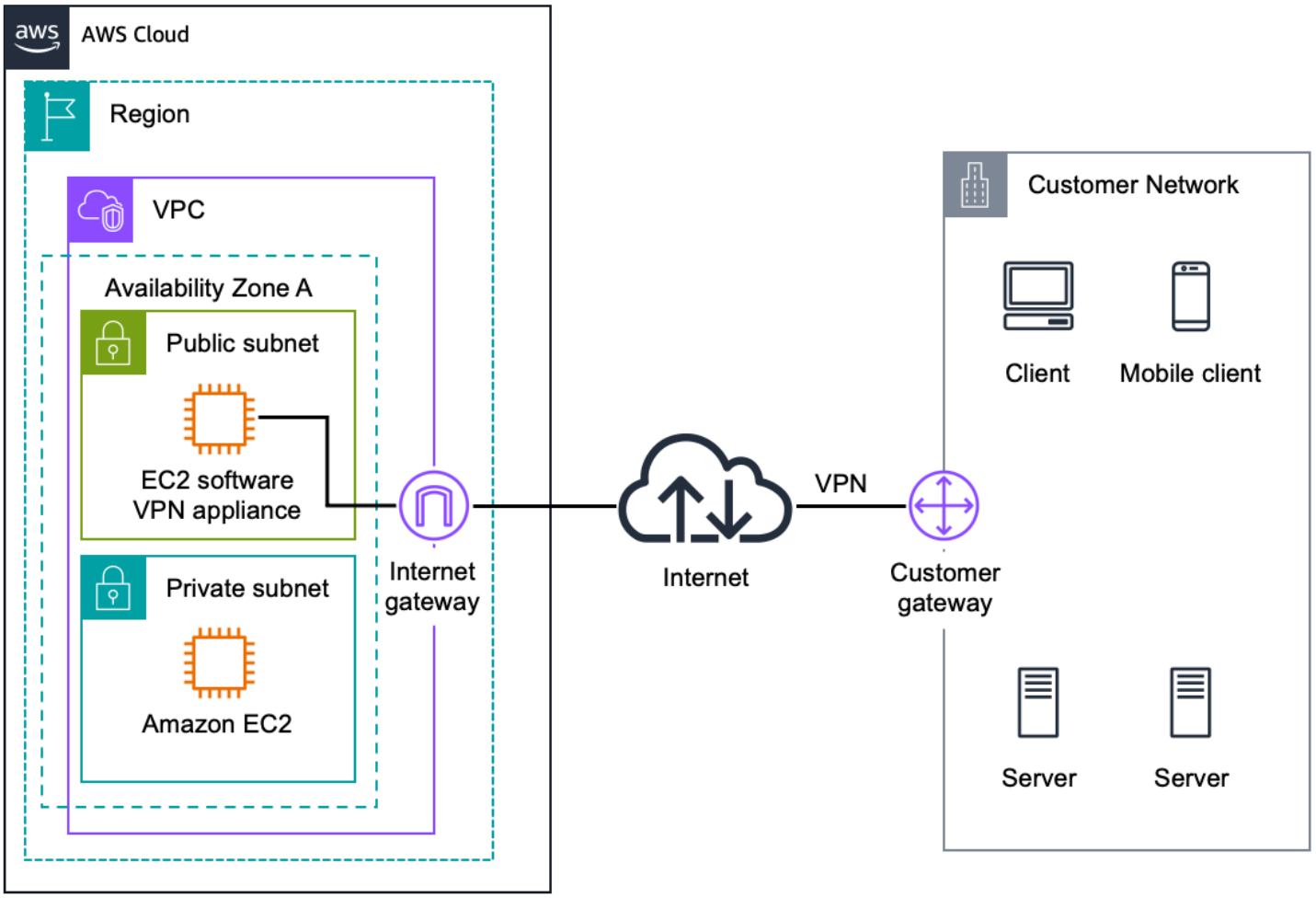
- 您可以在現有的交通閘道上建立連線附件。
- 協力廠商應用裝置必須設定 GRE 通道，才能使用連線附件從傳 Transit Gateway 道傳送和接收流量。設備必須使用 BGP 設定，才能進行動態路由更新和健康狀態檢查。
- Connect 附件不支持靜態路由。
- Transit Gateway 道連線附件可支援每個 GRE 通道的最大頻寬為 5 Gbps。頻寬高於 5 Gbps 可以通過在相同的 Connect 附件的多個 Connect 對等（GRE 通道）上廣告相同的前綴來實現。
- 每個連線附件最多可支援四個 Connect 對等。
- Transit Gateway 連線附件可透過 BGP (MBGP 或 MP-BGP) 的「多重通訊協定延伸」來支援 IPv6 和動態路由廣告。

其他資源

- 傳輸閘道對等連接附件
- 需求和考量
- 部落格文章：透 AWS Transit Gateway 連線簡化 SD-WAN 連線

VPN 軟體

Amazon VPC 透過在遠端網路和 Amazon 虛擬私人雲端網路中執行的軟體 VPN 設備之間建立 VPN 連接，讓您能夠靈活地完全管理 Amazon VPC 連線的兩端。如果您必須管理 VPN 連線的兩端 (不論是為了合規目的或是利用目前不受 Amazon VPC VPN 解決方案支援的閘道裝置)，建議使用此選項。下圖顯示此選項。



軟體 Site-to-Site VPN

您可以從多個合作夥伴和開放原始碼社群的生態系統中進行選擇，這些社群已產生在 Amazon EC2 上執行的軟體 VPN 設備。除了此選擇之外，您還必須負責管理軟體應用裝置，包括組態、修補程式和升級。

請注意，由於軟體 VPN 設備在單一 Amazon EC2 執行個體上執行，因此此設計會在網路設計中引入可能的單一故障點。如需詳細資訊，請參閱軟體 VPN 執行個體的附錄 A：軟體 VPN 執行個體的高階 HA 架構架構。

其他資源

- 中提供的 VPN 設備 AWS Marketplace
- 技術簡介-將思科 ASA 連接至 VPC EC2 執行個體 (IPsec)
- 技術簡介-將多個 VPC 連接至 EC2 執行個體 (IPsec)
- 技術簡介-將多個 VPC 與 EC2 執行個體 (SSL) 連接

Amazon 虛擬私人雲端到 Amazon VPC 連接選項

當您想要將多個 Amazon VPC 整合到更大的虛擬網路時，請使用這些設計模式。如果您因為安全性、帳單、多個區域存在或內部退款要求而需要多個 VPC，以便更輕鬆地在 Amazon VPC 之間整合 AWS 資源，此功能非常有用。您也可以將這些模式與網路到 Amazon VPC 連線選項結合使用，以建立跨遠端網路和多個 VPC 的企業網路。

針對連線的每個 VPC 使用非重疊 IP 範圍時，VPC 之間的 VPC 連線最佳化。例如，如果您想要連接多個 VPC，請確定每個 VPC 都設定了唯一的無類別網域間路由 (CIDR) 範圍。因此，我們建議您配置單一、連續、非重疊的 CIDR 區塊，以供每個 VPC 使用。如需有關 Amazon VPC 路由和約束的其他資訊，請參閱 Amazon VPC 常見問答集。

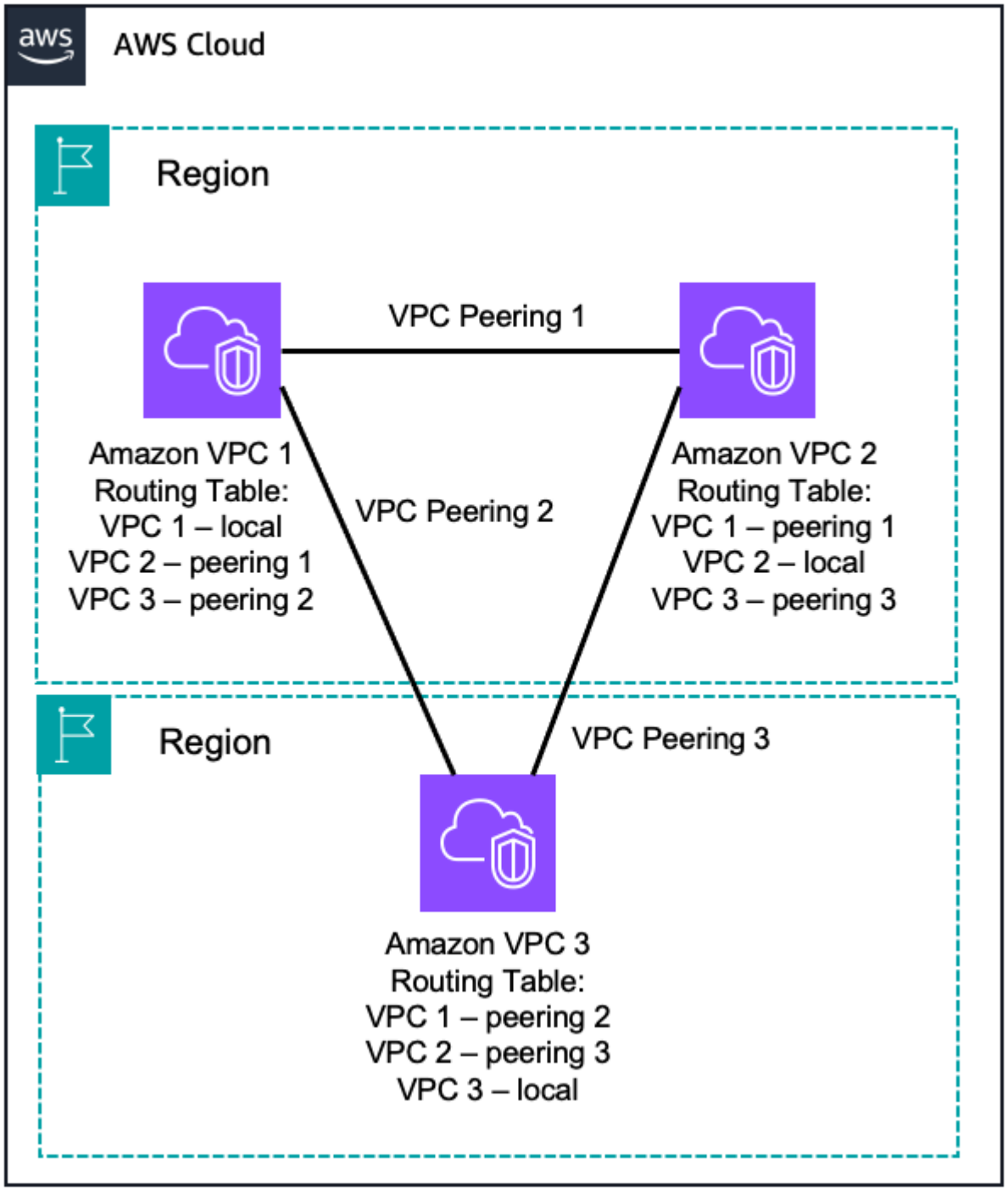
選項	使用案例	優點	限制
VPC 對等互連	AWS 在兩個 VPC 之間提供的網路連線能力。	利用 AWS 受管的可擴展聯網基礎設施	VPC 對等互連不支援轉移對等關係 難以大規模管理
AWS Transit Gateway	AWS 為 VPC 提供的區域性路由器連線	AWS 受管的高可用性和可擴展性服務 區域網路中樞，最多可容納 5,000 個附件	Transit Gateway 對等互連僅支援靜態路由
AWS PrivateLink	AWS 使用介面端點在兩個 VPC 之間提供的網路連線	利用 AWS 受管的可擴展聯網基礎設施	VPC 端點服務僅適用於建立這些服務的 AWS 區域
VPN 軟體	VPC 之間以軟體裝置為基礎的 VPN 連線	支援各種 VPN 廠商、產品和通訊協定 完全由您管理	您有責任為所有 VPN 端點實作 HA 解決方案 (如有需要) VPN 執行個體可能會成為網路瓶頸
軟體 VPN 到 AWS Site-to-Site VPN	軟體設備與 VPC 之間的 VPN 連線	AWS 受管的高可用性虛擬私人雲端 VPN 連線	您有責任為軟體應用裝置 VPN 端點實作

選項	使用案例	優點	限制
		支援各種由您管理的 VPN 廠商和產品 支援靜態路由和動態 BGP 對等和路由原則	HA 解決方案 (如有需要) VPN 執行個體可能會成為網路瓶頸 IPSec VPN 通訊協定僅適用於 AWS 受管 VPN

VPC 對等互連

VPC 對等互連連線是兩個 VPC 間的聯網連線，允許使用每個 VPC 的私有 IP 地址進行路由，就好像他們位於相同的網路。您可以在自己的 VPC 之間建立 VPC 對等連線，或使用其他 AWS 帳戶中的 VPC 建立。VPC 對等互連也支援區域間對等。

使用區域間 VPC 對等互連的流量始終保留在全球 AWS 骨幹網上，而且永遠不會穿越公有網際網路，進而減少常見漏洞攻擊和 DDoS 攻擊等威脅媒介。



VPC-to-VPC Peering

AWS 使用 VPC 的現有基礎設施來建立 VPC 對等連線，不需要依賴單獨的實體硬體。因此，它們不會在 VPC 之間引入潛在的單點故障或網路頻寬瓶頸。此外，您還可以利用 VPC 路由表、安全群組和網路存取控制清單來控制哪些子網路或執行個體能夠利用 VPC 對等連線。

Amazon VPC 不支援傳遞對等，這表示您無法通訊使用第三個 VPC 作為傳輸未直接對等的兩個 VPC。如果您希望所有 VPC 使用 VPC 對等互連進行通訊，則需要在每個 VPC 之間建立 1:1 VPC 對等連線。或者，您可以使用AWS Transit Gateway或 AWS 雲端 WAN 做為網路傳輸中樞。

VPC 擬私人雲端對等連線同時支援 IPv4 和 IPv6 流量。但是，如果兩個 VPC 的主要 IPv4 CIDR 區塊重疊，則無法對等，而不論使用的次要 IPv4 或 IPv6 CIDR 區塊為何。如果您打算在 VPC 之間使用 VPC 對等連接，在將主要 CIDR 區塊指派給 VPC 時，請考慮這一點。

其他資源

- Amazon VPC 對等互連
- 什麼是 VPC 對等互連？

AWS Transit Gateway

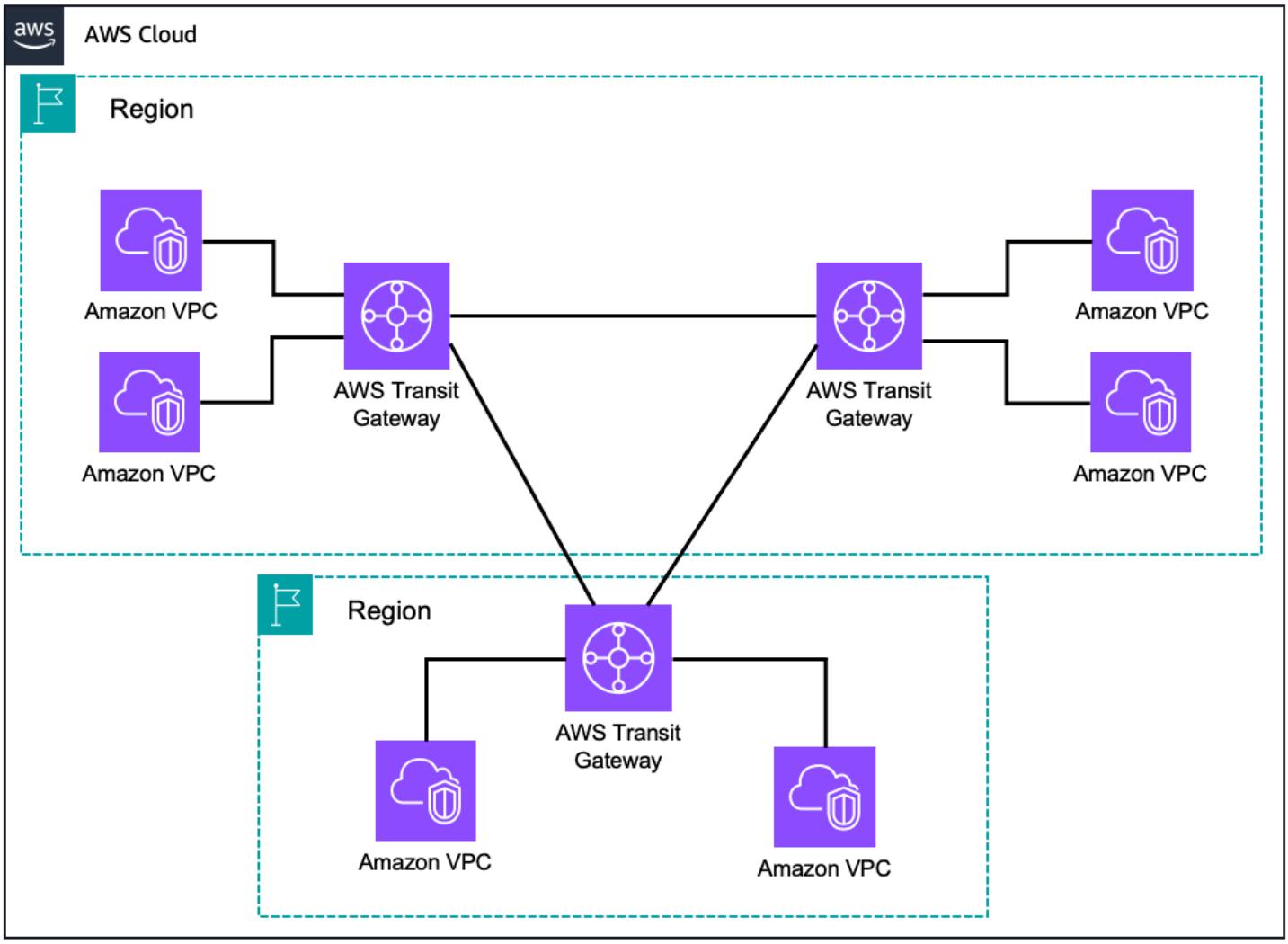
AWS Transit Gateway是一種高可用性和可擴展的服務，用於整合具有 hub-and-spoke 架構的區域的 AWS VPC 路由組態。每個支點 VPC 只需要連接到 Transit Gateway 即可存取其他連接的 VPC。在 AWS Transit Gateway中同時支援 IPv4 和 IPv6 流量。

您可以利用多個「傳 Transit Gateway」路由表、關聯和傳輸，在同一個「傳 Transit Gateway」中區段流量。您可以從單一管理點管理不同的路由網域 (例如生產和非生產流量)，確保這些路由網域無法彼此通訊。

您也可以利用 Transit Gateway 建立的 hub-and-spoke 架構，集中存取共用服務，例如流量檢查、介面 VPC 端點存取，或透過 NAT 閘道或 NAT 執行個體輸出流量。這種集中化可簡化在數個 VPC 中管理這些資源的複雜性，並在擴展 AWS 的使用空間時提供更好的控制。

傳輸閘道可以在相同 AWS 區域內或不同 AWS 區域之間彼此對等。 AWS Transit Gateway流量始終保持在全球 AWS 骨幹網上，而且永遠不會遍歷公共網際網路，進而減少常見漏洞攻擊和 DDoS 攻擊等威脅媒介。

傳 Transit Gateway 具有大量的 VPC，可透過 VPC 對等互連，提供更簡單的 VPC 至 VPC 通訊管理，如下圖所示。



AWS Transit Gateway

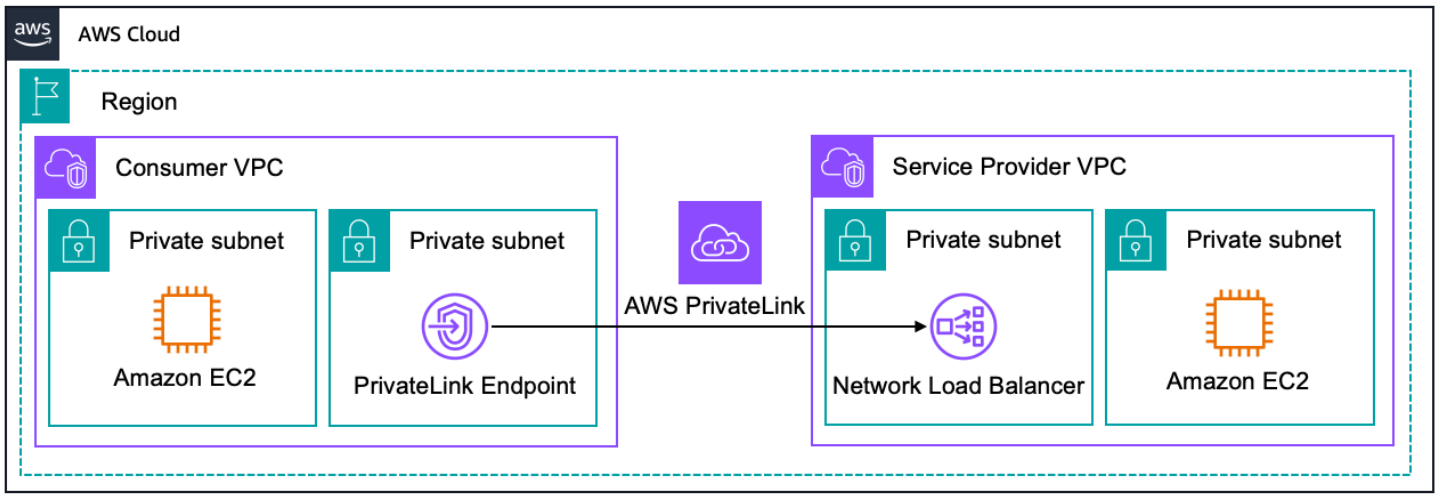
如需進出傳輸閘道的 IP 流量的集中能見度，您可以將 Transit Gateway 道流程日誌發佈到 Amazon CloudWatch 日誌和 Amazon S3。流量日誌資料是在網路流量路徑之外收集，因此不會影響網路輸送量或延遲。

其他資源

- Amazon VPC 傳輸閘道
- 傳輸閘道對等連接附件
- 使用交通閘道
- 使用 Transit Gateway 流程記錄記錄網路流量

AWS PrivateLink

AWS PrivateLink可讓您透過 VPC 中的私有 IP 地址連接到某些 AWS 服務、由其他 AWS 帳戶託管的服務 (稱為端點服務) 以及支援的AWS Marketplace合作夥伴服務。介面端點是直接在 VPC 內建立的，使用 VPC 子網路中的彈性網路介面和 IP 位址。這表示 VPC 安全群組可用於管理端點的存取。



AWS PrivateLink

如果您想要使用私有 IP 地址在 AWS 網路中安全地使用其他 VPC 提供的服務，我們建議您使用此方法。或者，當 VPC 具有重疊 IP 地址時，AWS PrivateLink這是一個很好的解決方案。

AWS PrivateLink完全支援 IPv6，但必須啟用或修改目的地 VPC、VPC 子網路、Network Load Balancer 和 DNS 名稱才能使用雙堆疊。符合這些先決條件後，即可在端點的服務組態中啟用 IPv6。

存取控制 AWS PrivateLink

透過 VPC 子網路中的彈性網路介面和 IP 位址，直接在 VPC 內建立介面端點。這表示 VPC 安全群組可用於管理端點的網路存取。

建立介面端點或閘道端點時，也可以附加端點策略。端點政策控制哪些 AWS 主體 (AWS 帳戶、IAM 使用者和角色) 可以使用 VPC 端點存取端點服務。

您無法將一個以上的政策連接至端點。但是，您可以隨時修改端點政策。

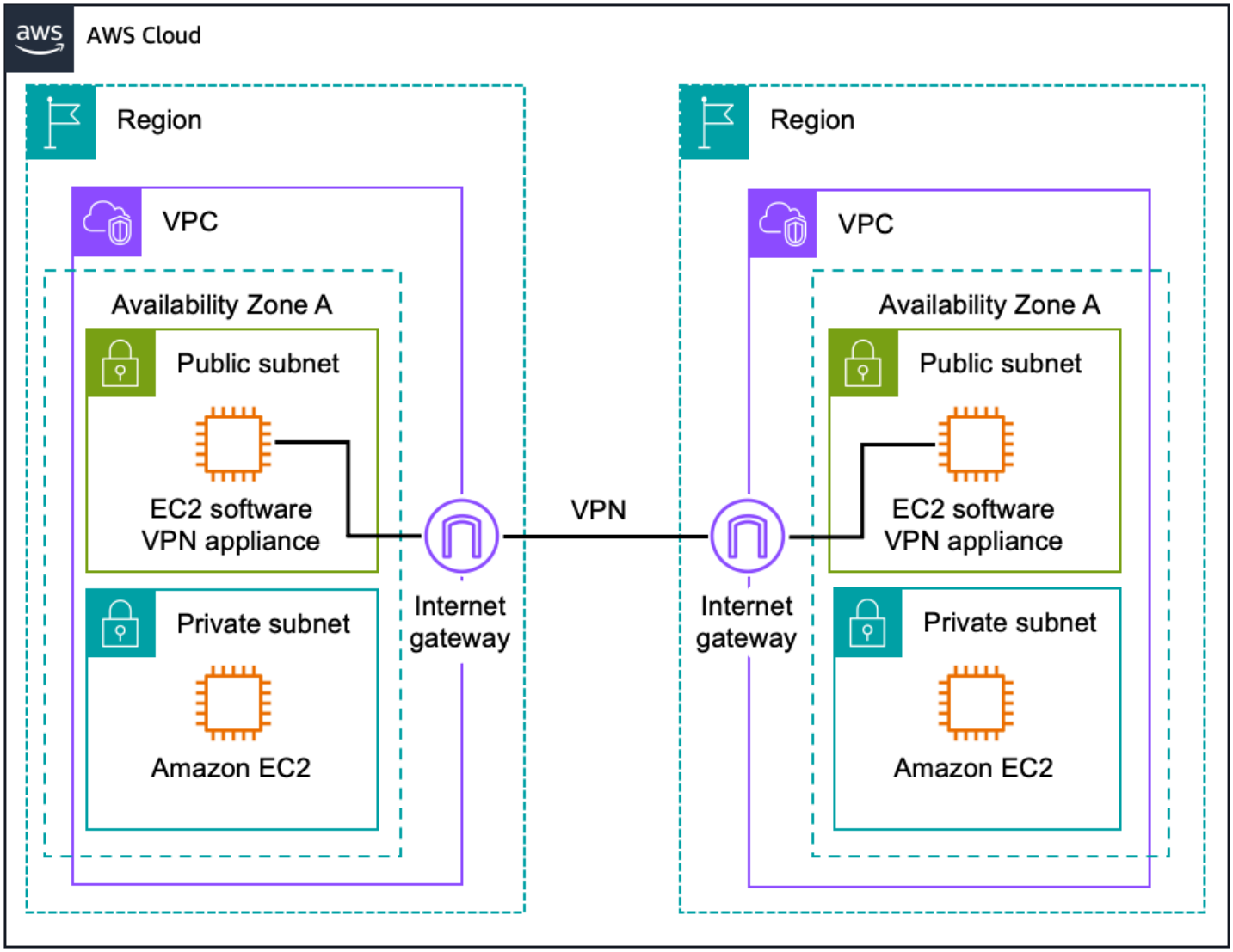
端點政策不會覆寫或取代 IAM 使用者政策或服務特定政策 (例如 Amazon S3 儲存貯體政策)。如果您使用介面端點連接至 Amazon S3，您也可使用 Amazon S3 儲存貯體政策來控制特定端點或特定 VPC 對儲存貯體的存取。

其他資源

- 介面 VPC 端端點 () AWS PrivateLink
- VPC 端端點服務 () AWS PrivateLink
- 部落格文章：透過 PrivateLink 服務和端點加快 IPv6 採用
- 部落格文章：連接具有重疊 IP 範圍的網路
- AWS PrivateLink夥伴

VPN 軟體

Amazon VPC 提供網路路由彈性。這包括在兩個或多個軟體 VPN 設備之間建立安全 VPN 通道的能力，以便將多個 VPC 連接到更大的虛擬私人網路，以便每個 VPC 中的執行個體可以使用私有 IP 地址無縫連接到彼此。當您想要使用偏好的 VPN 軟體供應商管理 VPN 連線的兩端時，建議使用此選項。此選項使用連接到每個 VPC 的網際網路閘道，以促進軟體 VPN 設備之間的通訊。



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

您可以從多個合作夥伴和開放原始碼社群的生態系統中進行選擇，這些社群已產生可在 Amazon EC2 上執行的軟體 VPN 設備。除了此選擇之外，您還負責管理軟體應用裝置，包括組態、修補程式和升級。

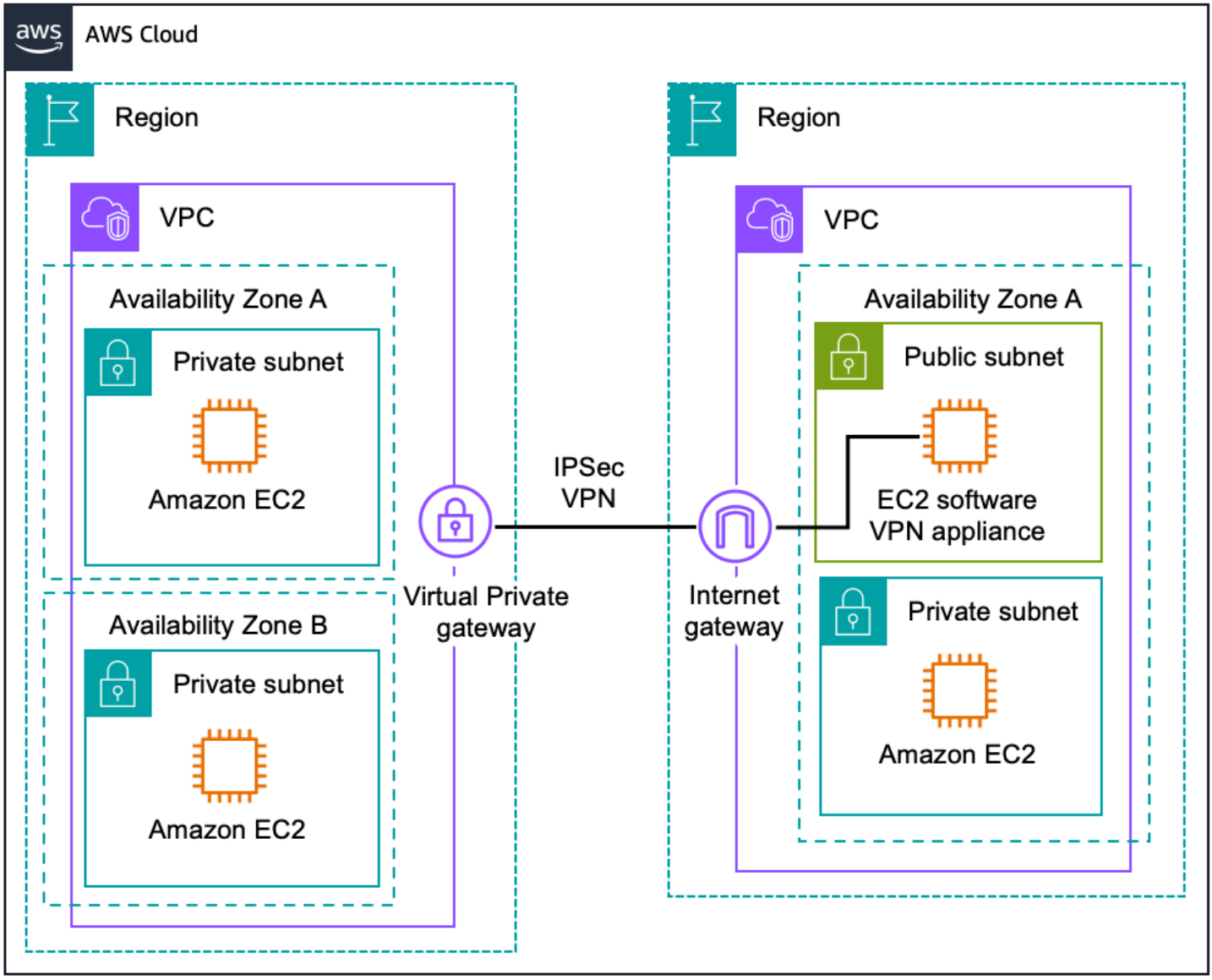
請注意，由於軟體 VPN 設備在單一 Amazon EC2 執行個體上執行，因此此設計會在網路設計中引入可能的單點故障。如需其他資訊，請參閱 附錄 A：軟體 VPN 執行個體的高階 HA 架構。

其他資源

- VPN 設備可從 AWS Marketplace
- 技術簡介-將多個 VPC 連接至 EC2 執行個體 (IPsec)
- 技術簡介-將多個 VPC 與 EC2 執行個體 (SSL) 連接

軟體 VPN 到 AWS Site-to-Site VPN

Amazon VPC 提供了結合 AWS 受管 VPN 和軟體 VPN 選項的彈性，以連接多個 VPC。透過此設計，您可以在軟體 VPN 應用裝置和虛擬私有閘道之間建立安全的 VPN 通道，讓每個 VPC 中的執行個體都能使用私有 IP 位址無縫連接彼此。此選項在一個 Amazon VPC 中使用虛擬私有閘道，以及另一個 Amazon VPC 中的網際網路閘道和軟體 VPN 設備的組合，如下圖所示。



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

請注意，此設計會在網路設計中引入可能的單一故障點。如需其他資訊，請參閱 附錄 A：軟體 VPN 執行個體的高階 HA 架構。

其他資源

- VPN 設備可從 AWS Marketplace
- AWS Site-to-Site VPN 使用者指南
- 客戶閘道裝置的需求

軟體遠端存取 Amazon VPC 連線選項

透過軟體遠端存取 VPN，您可以利用低成本、彈性且安全的服務來實作遠端存取解決方案，同時提供連線至 AWS 託管資源的順暢體驗。此選項通常適用於具有較不廣泛遠端網路的規模較小的公司，或尚未為員工建置和部署遠端存取解決方案的公司。

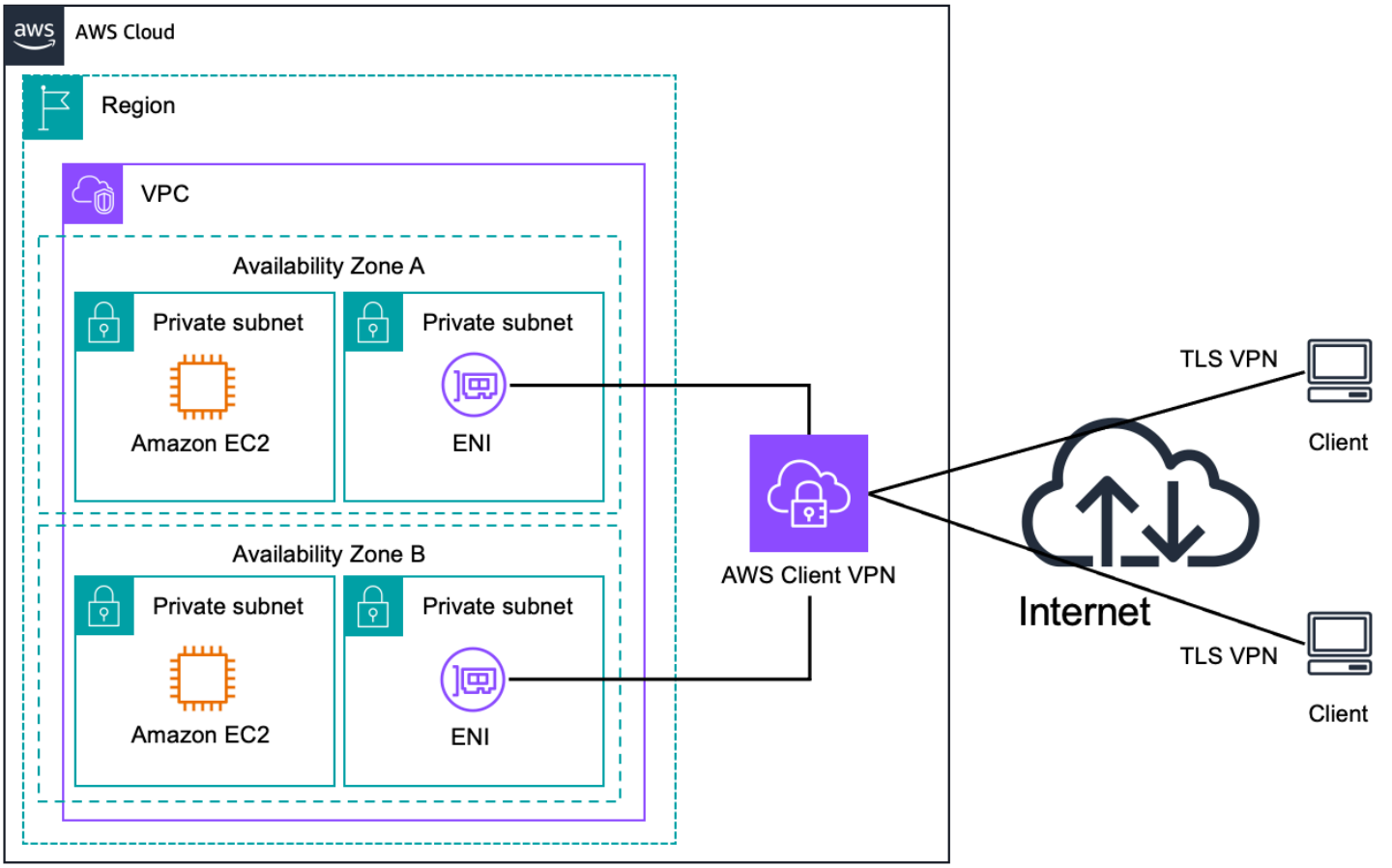
您可以將這些模式與網路到 Amazon VPC 連線選項連線選項結合在一起，並Amazon 虛擬私人雲端到 Amazon VPC 連接選項建立跨越遠端網路和多個 VPC 的網路。

下表概述了這些選項的優點和限制。

選項	使用案例	優點	限制
AWS Client VPN	AWS 對Amazon VPC 和/或內部網路的受管遠端存取解決方案	AWS 受管的高可用性和可擴展性服務	僅限 OpenVPN 用戶端
軟體用戶端 VPN	軟體VPN 裝置遠端存取Amazon VPC 和/或內部網路的解決方案	支援更廣泛的 VPN 廠商、產品和通訊協定 完全客戶管理的解決	您有責任實施醫管局解決方案

AWS Client VPN

AWS Client VPN 是 AWS 受管的高可用性和可擴展性服務，支援安全的軟體遠端存取。它提供在遠端用戶端和 Amazon VPC 之間建立安全 TLS 連線的選項，以便透過網際網路安全地存取 AWS 資源和現場部署，如下圖所示。



AWS Client VPN Remote Access

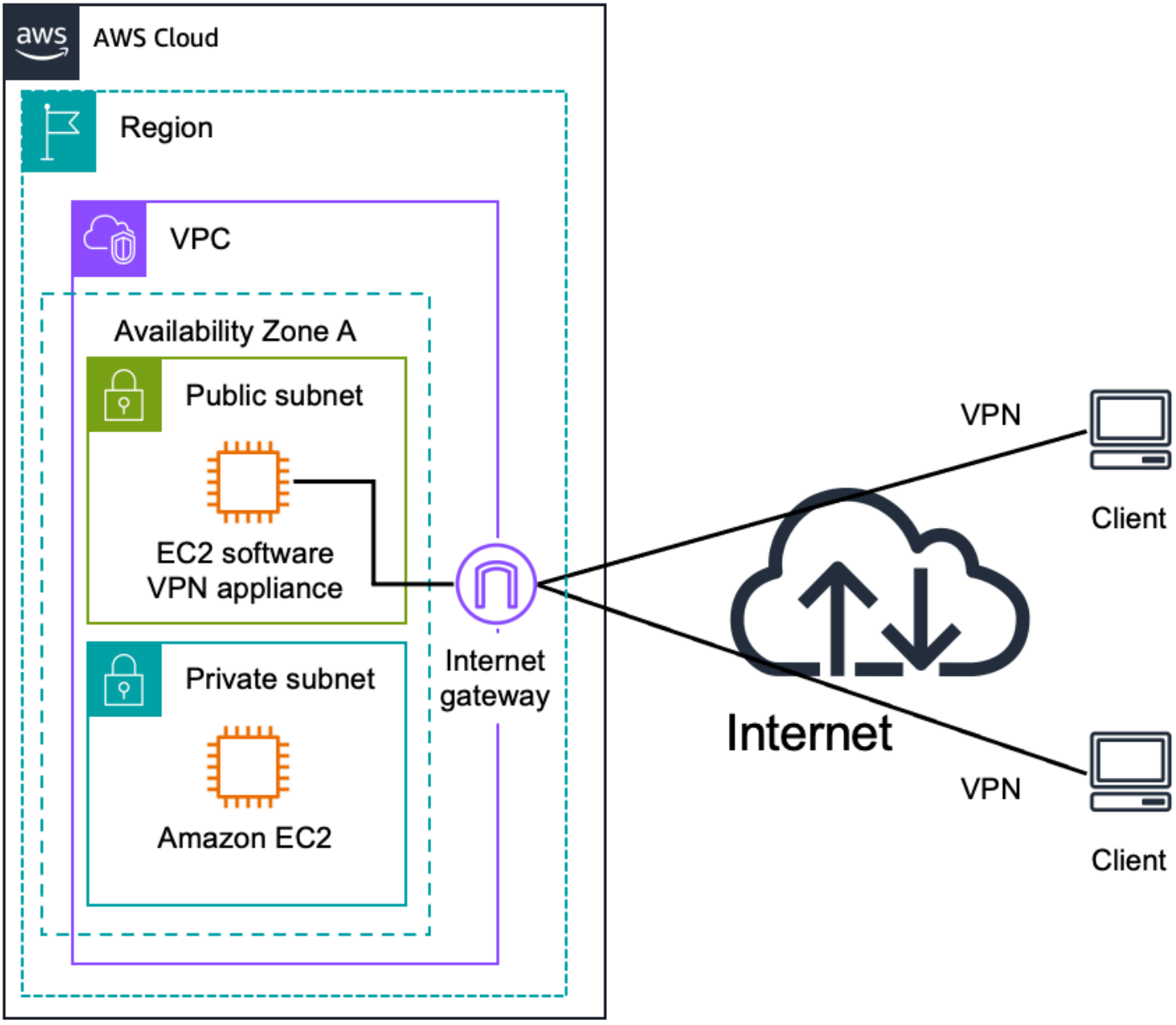
遠端用戶端可以是桌面版 AWS Client VPN，也可以是第三方 OpenVPN 用戶端，透過使用中目錄或相互憑證身份驗證進行身份驗證。

其他資源

- AWS Client VPN 管理員指南

軟體用戶端 VPN

您可以從多個合作夥伴和開放原始碼社群的生態系統中進行選擇，這些社群已產生可在 Amazon EC2 上執行的遠端存取解決方案。這些解決方案在遠端存取 Amazon VPC 的安全協定上提供了極大的彈性，以及透過網際網路安全存取 AWS 資源和現場部署，如下圖所示。



Software Client VPN Remote Access

遠端存取解決方案複雜，支援多種用戶端身份驗證選項 (包括多重要素身份驗證)，並且可以與 Amazon VPC 或遠端託管的身分和存取管理解決方案 (利用其中一個網路到 Amazon VPC 選項) 整合，例如 Microsoft Active Directory 或其他 LDAP/多因素身份驗證解決方案。

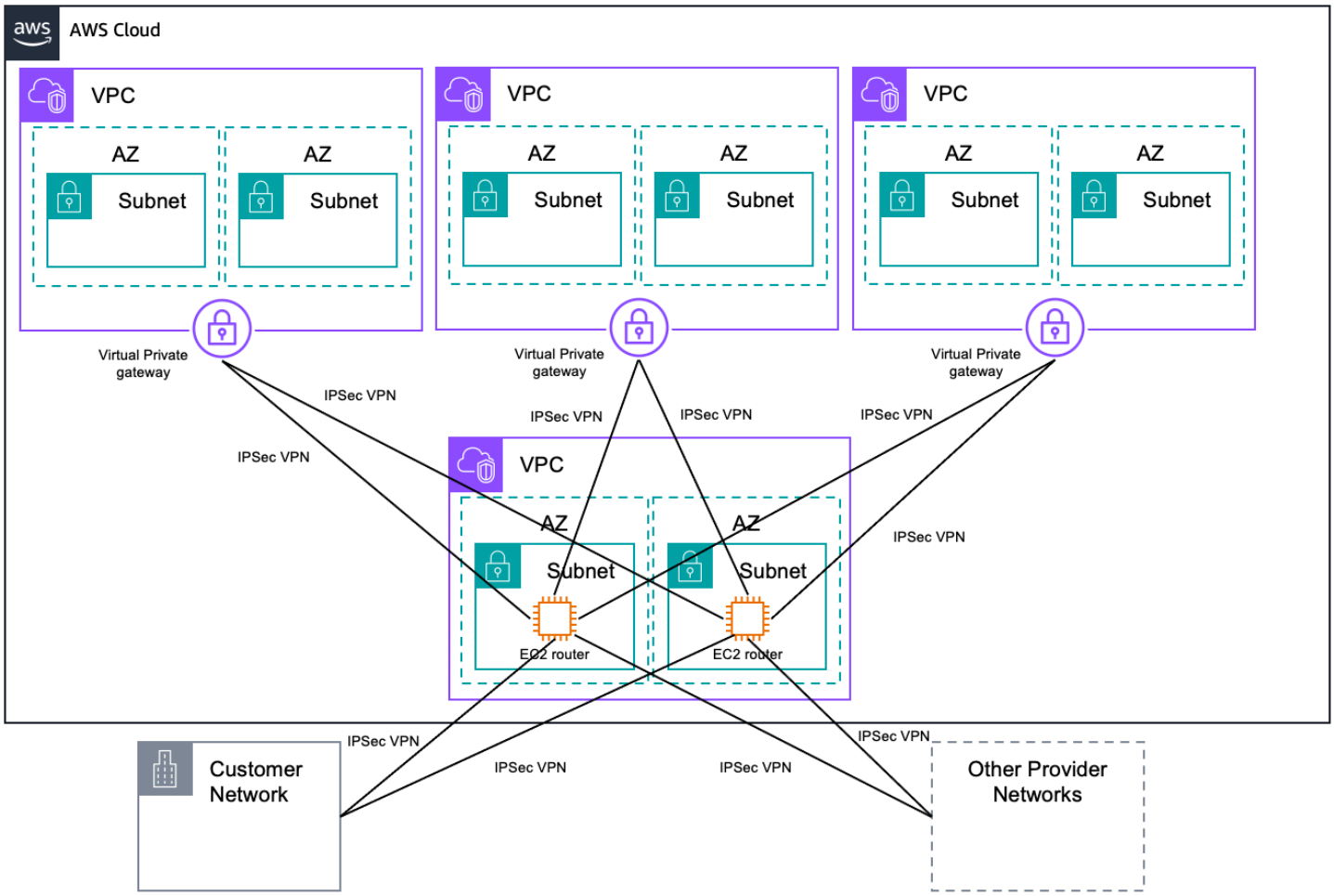
您負責管理遠端存取軟體，包括使用者管理、組態、修補程式和升級。當遠端存取伺服器在單一 Amazon EC2 執行個體上執行時，此設計會在網路設計中引入可能的單一故障點。如需其他資訊，請參閱 附錄 A：軟體 VPN 執行個體的高階 HA 架構。

其他資源

- VPN 設備可從 AWS Marketplace
- 開放式 VPN 存取伺服器快速入門指南

交通 VPC

以上述軟體 VPN 設計為基礎，您可以在 AWS 上建立全球傳輸網路。傳輸 VPC 是連接多個分散各地的 VPC 和遠端網路，以建立全球網路傳輸中心的常見策略。傳輸 VPC 會簡化網路管理，並最大程度減少連線多個 VPC 和遠端網路所需的連線數。下圖說明此設計。



Transit VPC

除了在 VPC 和內部部署網路之間提供直接的網路路由，此設計還可讓傳輸 VPC 實作更複雜的路由規則，例如重疊網路範圍之間的網路位址轉譯，或新增額外的網路層級封包篩選或檢查。傳輸 VPC 設計可用於支援重要的使用案例，例如私有聯網、共用連線和跨帳戶 AWS 使用。

其他資源

- AWS Transit Gateway
- 適用於 SD-WAN 和路由的思科催化劑 8000V AWS Marketplace

AWS 雲端廣域網路

AWS Cloud WAN 是意向驅動的受管廣域網路 (WAN)，由您定義的政策描述，以統一您的資料中心、分支機構和 AWS 網路。雖然您可以透過跨地區的多個 Transit Gateway 互連，建立自己的全球網路，但 Cloud WAN 提供內建的自動化、分段和組態管理功能，專為建立和操作全球網路而設計，可根據您的核心網路政策進行設計。Cloud WAN 新增了自動化 VPC 附件、整合式效能監控和集中式設定等功能。

核心網路政策以宣告式語言撰寫，用來定義區段、AWS 區域路由，以及附件應如何對應至區段。透過核心網路政策，您可以描述存取控制和流量路由的意圖，而 AWS Cloud WAN 則會處理網路組態詳細資訊。

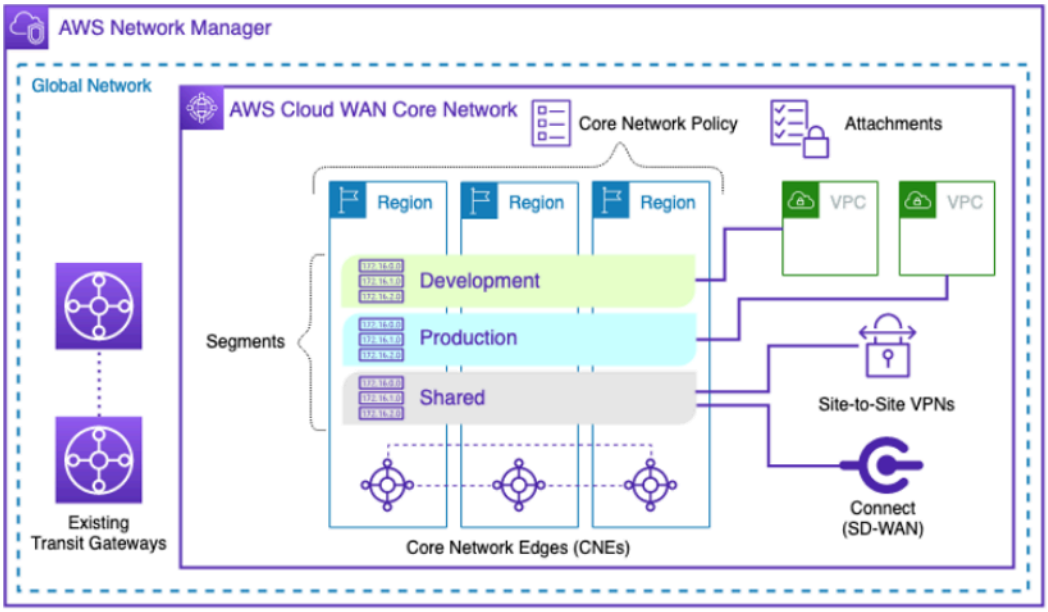
雲端 WAN 在 AWS Network Manager 中管理，可讓您集中管理和視覺化跨 AWS 帳戶、區域和現場部署位置的雲端 WAN 核心網路和 Transit Gateway 網路。Network Manager 提供多種儀表板視覺效果，可協助您檢視和監控全球網路的所有層面。一些儀表板包括：

- 世界地圖可精確找出網路資源 (例如節點位置、裝置和附件) 所在的位置。
- 使用 E CloudWatch vents 追蹤 15 個月統計資料的監控功能，讓您更清楚瞭解網路的效能。
- 將即時事件串流至事件儀表板的事件追蹤。
- 運輸閘道網路和交通閘道的拓撲和邏輯圖。

Transit Gateway 和雲端 WAN 都允許 VPC 和內部部署位置之間的集中連線。Transit Gateway 是區域網路連線中樞，對於在少數 AWS 區域中運作、想要管理自己的對等和路由組態或偏好使用自己的自動化的客戶而言，是最佳選擇。Cloud WAN 最適合想要透過原則定義全球網路，並讓服務自動實作基礎元件的客戶。

須知事項

- CNE (核心網路邊緣) 會繼承許多傳 Transit Gateway 特性，例如每個 VPC 附件的輸送量。
- 雲端廣域網路支援 IPv4 和 IPv6。
- 目前雲端 WAN 本身不支援AWS Direct Connect附件。若要AWS Direct Connect搭配 Cloud WAN 使用，您需要將 Transit Gateway 連接至AWS Direct Connect閘道，然後將 Transit Gateway 對等至 Cloud WAN。
- 對於具有許多變更的大型網路，請考慮建立個別的開發並測試全域網路，您可以在其中驗證變更。



AWS Cloud WAN

其他資源

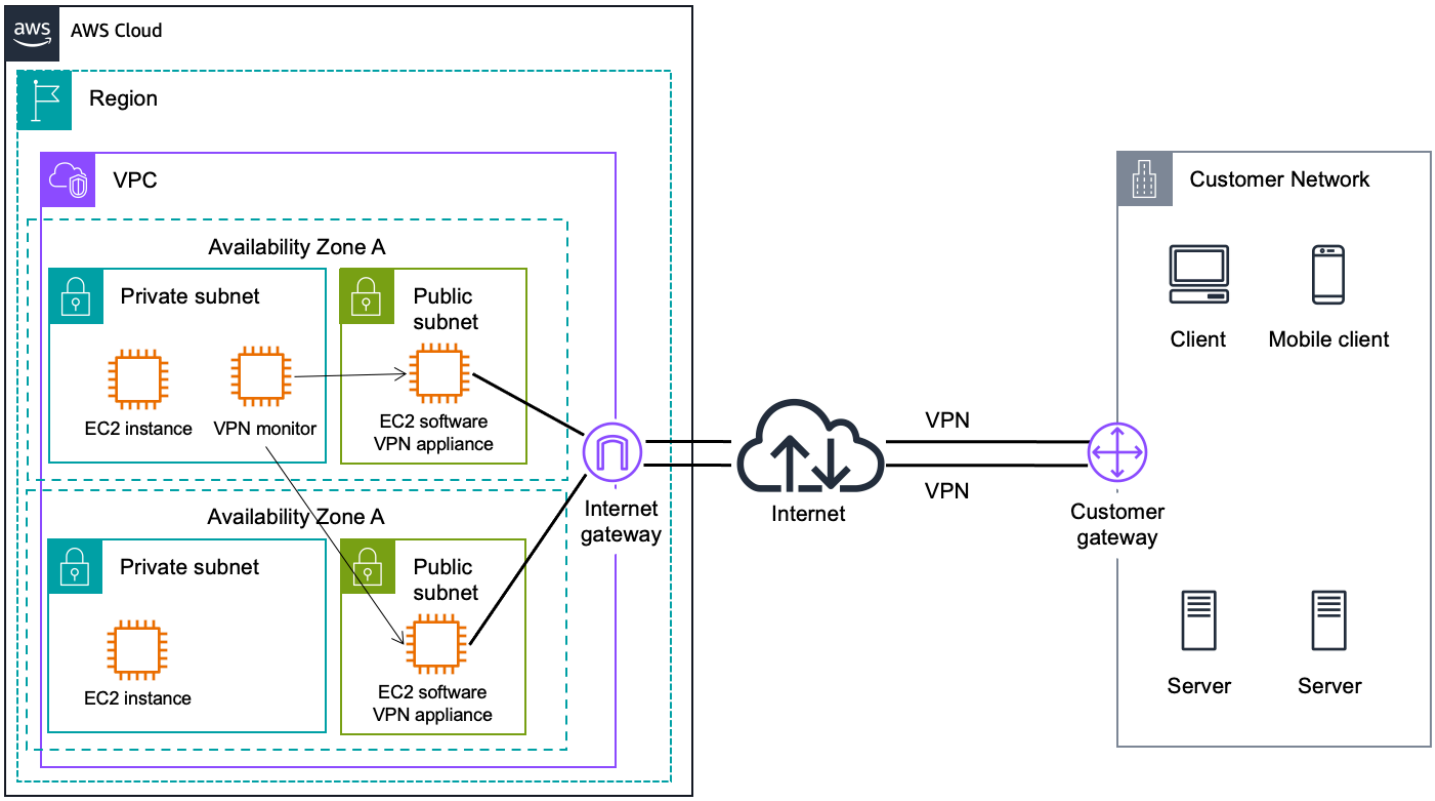
- AWS 雲端廣域網路文件
- 部落格文章：AWS 雲端 WAN 和 AWS Transit Gateway 遷移和互通性模式

結論

AWS 提供了許多高效、安全的連接選項，以幫助您在將遠端網路與 Amazon VPC 整合時充分利用 AWS。本白皮書中提供的選項重點介紹了客戶用於成功整合遠端網路或多個 Amazon VPC 網路的一些連接選項和模式。您可以使用此處提供的資訊來確定對於連接執行業務所需的基礎設施而言最合適的機制，無論基礎設施的實體位置或託管位置在何處。

附錄 A：軟體 VPN 執行個體的高階 HA 架構

為軟體 VPN 執行個體建立完全彈性的 VPC 連線，需要設定和設定多個 VPN 執行個體以及監控執行個體，才能監控 VPN 連線的健康狀態。



高階軟體 VPN HA

建議您將 VPC 路由表設定為同時利用所有 VPN 執行個體，方法是將來自一個可用區域中所有子網路的流量導向至相同可用區域中的個別 VPN 執行個體。然後，每個 VPN 執行個體都會為共用相同可用區域的執行個體提供 VPN 連線。

VPN 監控

要監視基於軟件的 VPN 設備，您可以創建一個 VPN 監視器。VPN 監視器是您需要執行 VPN 監控指令碼的自訂執行個體。此執行個體旨在執行和監控 VPN 連線和 VPN 執行個體的狀態。如果 VPN 執行個體或連線中斷，監視器就必須停止、終止或重新啟動 VPN 執行個體，同時也會將流量從受影響的子網路重新路由到運作中的 VPN 執行個體，直到兩個連線都能正常運作為止。由於客戶需求各不相同，AWS 目前不提供設定此監控執行個體的規範指導。不過，在 NAT 執行個體之間啟用 HA 的範例指令碼可以做為為軟體 VPN 執行個體建立 HA 解決方案的起點。我們建議您透過必要的業務邏輯來提供通知，或在 VPN 連線失敗時嘗試自動修復網路連線。

此外，您可以使用 Amazon CloudWatch 指標監控 AWS 受管 VPN 通道，這些指標會將 VPN 服務的資料點收集到可讀的近即時指標中。每個 VPN 連線都會收集各種隧道指標，並將其發佈到 Amazon CloudWatch。這些指標可讓您監視隧道健康狀況、活動並建立自動化動作。

貢獻者

本文件的貢獻者包括：

- AWS 企業 Support 資深技術客戶經理 Yu
- 解決方案建置工具、AWS 解決方案架構
- AWS 解決方案架構解決方案建置者資深經理 Steve Morad
- 解決方案架構師，AWS 解決方案架構師
- Fiona Armada，AWS 解決方案架構首席解決方案架構師
- 巴勃羅·桑切斯·卡莫納，AWS 解決方案架構的網絡專家解決方案架構師
- 托尼·霍克，AWS 企業 Support 資深聯網專家技術客戶經理

文件修訂

若要收到有關此白皮書更新的通知，請訂閱 RSS 摘要。

變更	描述	日期
白皮書已更新	新增 AWS 雲端 WAN 和 Transit Gateway 連接附件選項、更新的圖表和資訊。	2023 年 4 月 5 日
白皮書已更新	新增 AWS Transit Gateway 和 AWS Client VPN 選項、更新的圖表和資訊。	二零二零年六月六日
次要更新	修復對軟件 VPN 設備的引用的細微更改。	2020 年 5 月 20 日
白皮書已更新	更新了整個信息。專注於以下設計/功能：傳輸 VPC，直接 Connect 網關和. AWS PrivateLink	二 ○ 一八年一月一日
初次出版	Amazon Virtual Private Cloud 連接選項已發布。	2014 年 7 月 1 日

聲明

客戶應負責對本文件中的資訊自行進行獨立評估。本文件：(a) 僅供參考之用，(b) 代表目前的 AWS 產品供應與實務，如有變更恕不另行通知，以及 (c) 不構成 AWS 及其附屬公司、供應商或授權人的任何承諾或保證。AWS 產品或服務以「現況」提供，不提供任何明示或暗示的擔保、主張或條件。AWS 對其客戶之責任與義務，應受 AWS 協議之約束，且本文件並不屬於 AWS 與其客戶間之任何協議的一部分，亦非上述協議之修改。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。