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

發佈日期：2023 年 4 月 5 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，讓客戶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 為客戶提供數種選項，可將 AWS 虛擬網路與其他遠端網路連線。本文件說明可供客戶使用的幾個常見網路連線選項。其中包括將遠端客戶網路與 Amazon VPC 整合的連線選項，以及將多個 Amazon VPCs 連接到連續虛擬網路。

此白皮書適用於希望檢閱可用連線選項的公司網路架構師和工程師或 Amazon VPC 管理員。它提供各種選項的概觀，以促進網路連線討論，以及提供更多詳細資訊或範例的其他文件和資源的指標。

簡介

Amazon VPC 會根據您目前的網路設計和需求，提供多個網路連線選項供您使用。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 或使用者受管網路端點的連線。此外，透過 AWS，您可以利用 AWS 服務或使用者管理的網路設備和路由，選擇 Amazon VPC 與網路之間的網路路由交付方式。本白皮書會考慮下列選項，並概述每個選項的高階比較：

- Network-to-Amazon VPC 連線選項
  - AWS Site-to-Site VPN – 說明從遠端網路上的網路設備建立受管 IPsec VPN 連線至 Amazon VPC。
  - AWS Transit Gateway + AWS Site-to-Site VPN – 說明如何使用 從遠端網路上的網路設備建立受管 IPsec VPN 連線，以連接至 Amazon VPCs 的區域網路中樞 AWS Transit Gateway。
  - AWS Direct Connect - 描述使用 從遠端網路建立與 Amazon VPC 的私有邏輯連線 AWS Direct Connect。
  - AWS Direct Connect + AWS Transit Gateway – 說明使用 AWS Direct Connect 和 ，從遠端網路建立私有邏輯連線至 Amazon VPCs 的區域網路中樞 AWS Transit Gateway。
  - AWS Direct Connect + AWS Site-to-Site VPN – 說明使用 Direct Connect 和 AWS Site-to-Site VPN，從遠端網路建立與 Amazon VPC 的私有加密連線。
  - AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN – 說明使用 Direct Connect 和 ，從遠端網路建立私有加密連線，以連線至 Amazon VPCs 的區域網路中樞 AWS Transit Gateway。
  - Site-to-Site VPN CloudHub – 說明建立用於連接遠端分支辦公室的hub-and-spoke模型。
  - 軟體 VPN – 描述從遠端網路上的設備建立 VPN 連線，以連線到在 Amazon VPC 內執行的使用者受管軟體 VPN 設備。
  - AWS Transit Gateway + SD-WAN 解決方案 - 描述整合軟體定義的廣域網路 (SD-WAN) 解決方案，以使用 AWS 骨幹或網際網路做為傳輸網路，將多個遠端位置互連至 Amazon VPCs 的區域網路中樞。
- Amazon VPC-to-Amazon VPC 連線選項
  - VPC 對等互連 – 描述使用 Amazon VPCs 對等互連功能在區域內和區域間連線 Amazon VPC。
  - AWS Transit Gateway – 描述在hub-and-spoke模型 AWS Transit Gateway 中使用 在區域內和區域間連接 Amazon VPCs。
  - AWS PrivateLink – 描述將 Amazon VPCs 與 VPC 介面端點和 VPC 端點服務連線。

  - 軟體 VPN – 描述使用在每個 Amazon VPCs 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-to-AWS Site-to-Site VPN – 說明將 Amazon VPCs 與使用者受管軟體 VPN 設備之間建立的 VPN 連線連線，該連線位於一個 Amazon VPC 和連接至另一個 Amazon VPC AWS 的 Site-to-Site VPN 之間。
- 軟體access-to-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至 Amazon VPC。
  - 軟體用戶端 VPN – 說明如何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。
- 傳輸 VPC - 描述使用軟體 VPN 搭配 AWS 受管 VPN 在 AWS 上建立全域傳輸網路。
- AWS 雲端 WAN - 描述建立受管廣域網路 (WAN)，以輕鬆建置、管理和監控 Amazon VPCs、資料中心和遠端分支中資源之間的全域互連。

Network-to-Amazon VPC 連線選項

本節提供將遠端網路與您的 Amazon VPC 環境連線的設計模式。這些選項有助於透過將內部網路擴展到 AWS 雲端，將 AWS 資源與您現有的現場服務（例如監控、身分驗證、安全性、資料或其他系統）整合。此網路延伸還允許您的內部使用者無縫連接到 AWS 上託管的資源，就像任何其他內部面向的資源一樣。

為每個連線的網路使用非重疊 IP 範圍時，最好實現遠端客戶網路的 VPC 連線。例如，如果您想要將一或多個 VPCs 連線到您的公司網路，請確定它們已設定唯一的無類別網域間路由 (CIDR) 範圍。我們建議為每個 VPC 配置單一、連續、不重疊的 CIDR 區塊。如需 Amazon VPC 路由和限制條件的其他資訊，請參閱 Amazon VPC 常見問答集。

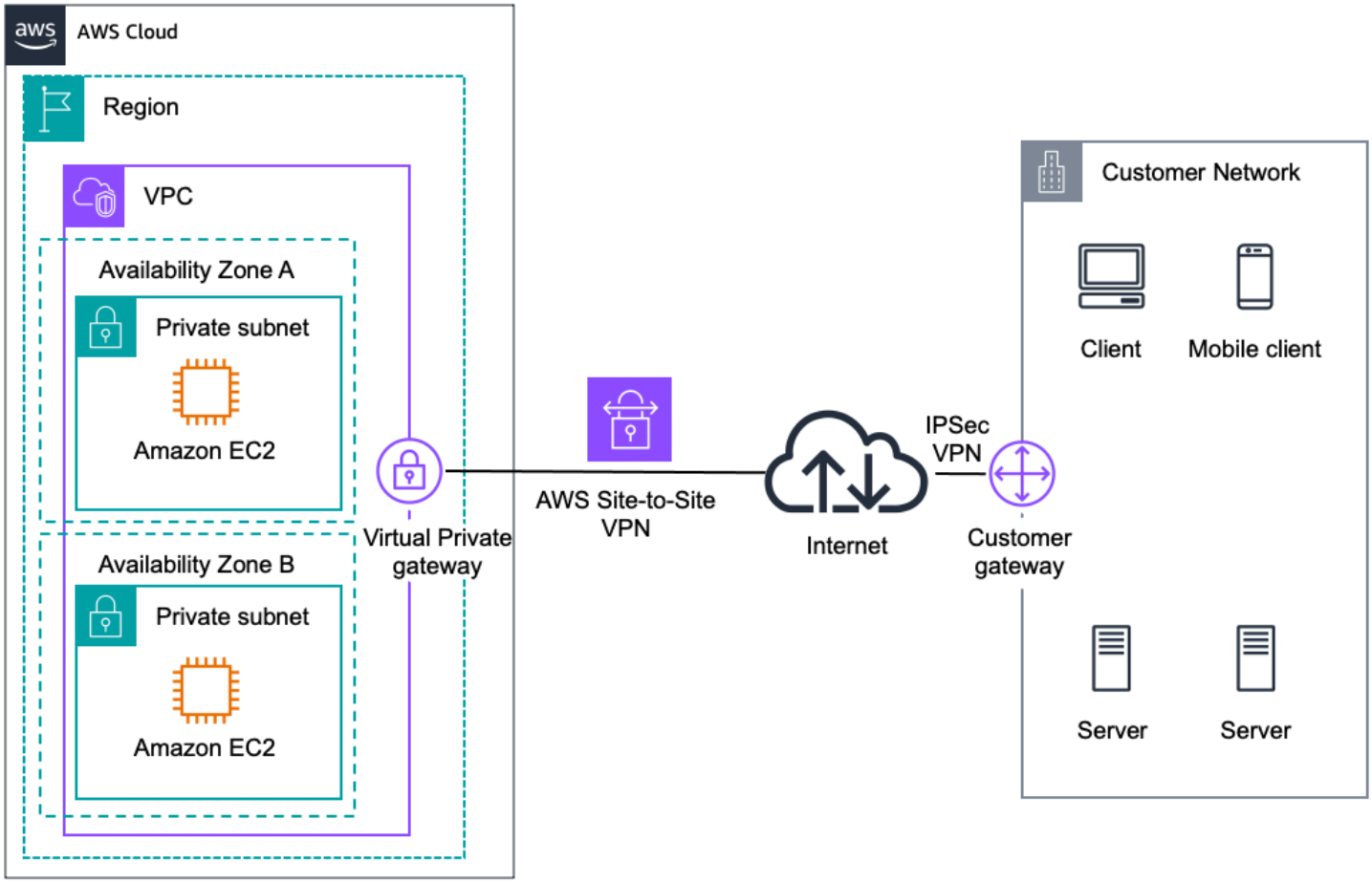
選項	使用案例	優點	限制
AWS Site-to-Site VPN	AWS 受管 IPsec VPN 透過網際網路連線至個別 VPC	重複使用現有的 VPN 設備和程序 重複使用現有的網際網路連線 AWS 受管高可用性 VPN 服務 支援靜態路由或動態邊界閘道協定 (BGP) 對等和路由政策	網路延遲、變異性和可用性取決於網際網路條件 您負責實作備援和容錯移轉（如果需要） 遠端裝置必須支援單一躍點 BGP（在利用 BGP 進行動態路由時）
AWS Transit Gateway + AWS Site-to-Site VPN	AWS 受管 IPsec VPN 透過網際網路連線至多個 VPCs的區域路由器	與上一個選項相同 AWS 受管的高可用性和可擴展性區域網路中樞，最多可連接 5，000 個附件	與上一個選項相同
AWS Direct Connect	透過私有線路的專用網路連線	更可預測的網路效能 降低頻寬成本	可能需要佈建額外的電信和託管供應商關係或新的網路電路

選項	使用案例	優點	限制
		支援 BGP 對等互連和路由政策	
AWS Direct Connect + AWS Transit Gateway	透過私有線路的專用網路連線到多個 VPCs 的區域路由器	與上一個選項相同 AWS 受管的高可用性和可擴展性區域網路中樞，最多可連接 5，000 個附件	與上一個選項相同
AWS Direct Connect + AWS Site-to-Site VPN	透過私有線路的 IPsec VPN 連接	更可預測的網路效能 降低頻寬成本 在 上支援 BGP 對等互連和路由政策 AWS Direct Connect 重複使用現有的 VPN 設備和程序 AWS 受管高可用性 VPN 服務 支援 VPN 連線上的靜態路由或動態邊界閘道協定 (BGP) 對等和路由政策	可能需要佈建額外的電信和託管供應商關係或新的網路線路 您負責實作備援和容錯移轉（如果需要） 遠端裝置必須支援單一躍點 BGP（在利用 BGP 進行動態路由時）
AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN	IPsec VPN 透過私有線路連線至多個 VPCs 的區域路由器	與上一個選項相同 AWS 受管的高可用性和可擴展性區域網路中樞，最多可連接 5，000 個附件	與上一個選項相同

選項	使用案例	優點	限制
Site-to-Site VPN CloudHub	在hub-and-spoke模型中連接遠端分支辦公室，以進行主要或備份連線	重複使用現有的網際網路連線和 Site-to-Site VPN 連線 AWS 受管高可用性 VPN 服務 支援 BGP 交換路由和路由優先順序	網路延遲、變異性和可用性取決於網際網路 使用者受管分支辦公室端點負責實作備援和容錯移轉（如果需要）
AWS Transit Gateway + SD-WAN 解決方案	使用 AWS 骨幹或網際網路做為傳輸網路，以軟體定義的廣域網路連接遠端分支和辦公室。	支援更廣泛的 SD-WAN 廠商、產品和通訊協定 有些廠商解決方案與 AWS 原生服務整合。	如果 SD-WAN 設備放置在 Amazon VPC 中，您需負責實作這些設備的 HA（高可用性）。
軟體 VPN	軟體設備型 VPN 透過網際網路連線	支援更廣泛的 VPN 廠商、產品和通訊協定 完全客戶受管的解決方案	您負責為所有 VPN 端點（如果需要）實作 HA（高可用性）解決方案

AWS Site-to-Site VPN

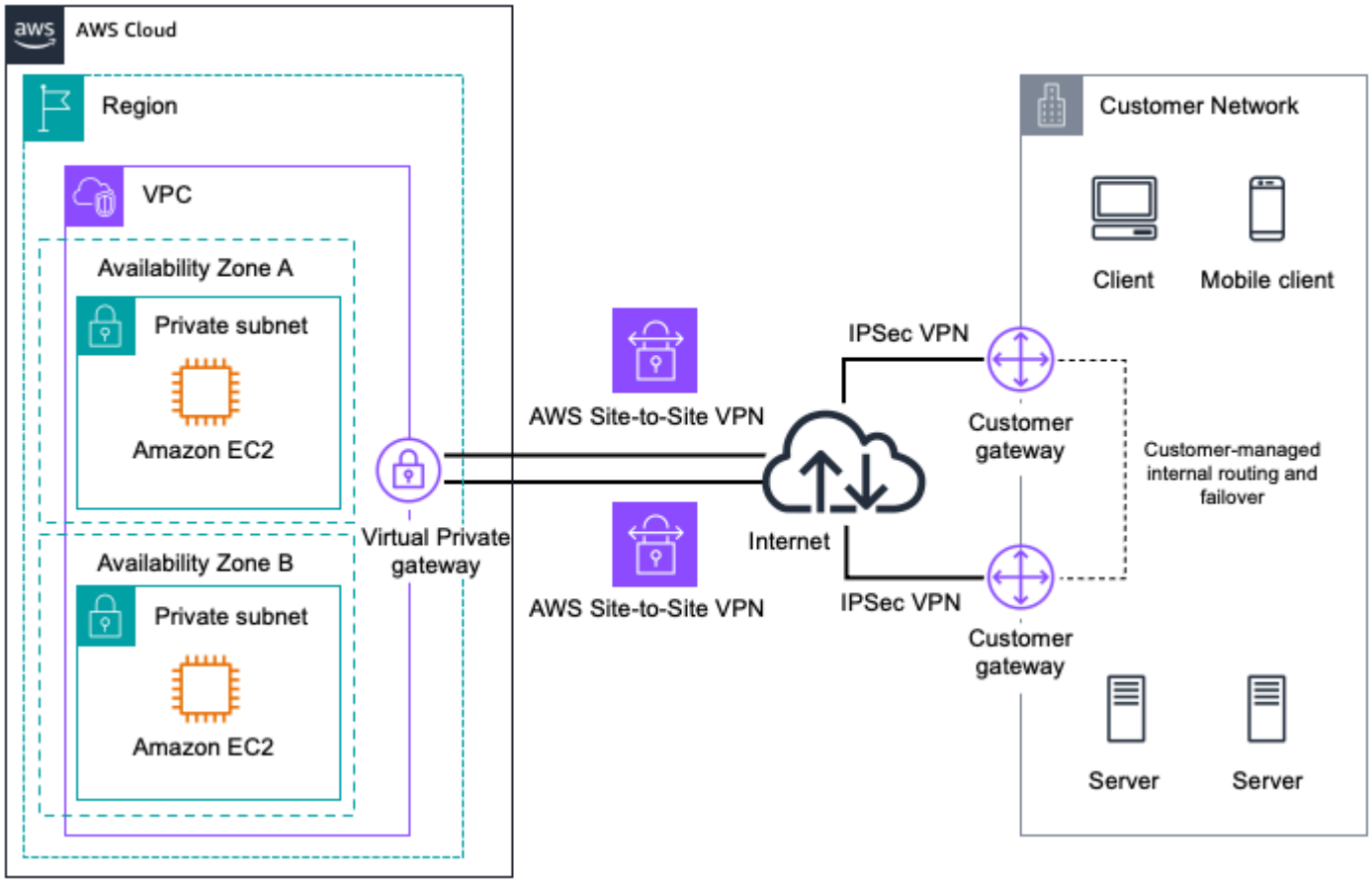
Amazon VPC 提供在遠端網路與 Amazon VPC 之間透過網際網路建立 IPsec VPN 連線的選項，如下圖所示。



AWS Managed VPN

當您想要利用內建於 VPN 連線 AWS 端的自動備援和容錯移轉的 AWS 受管 VPN 端點時，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，因此您可以在 VPN 連線的 端實作備援和容錯移轉，如下圖所示。



Redundant AWS Site-to-Site VPN Connections

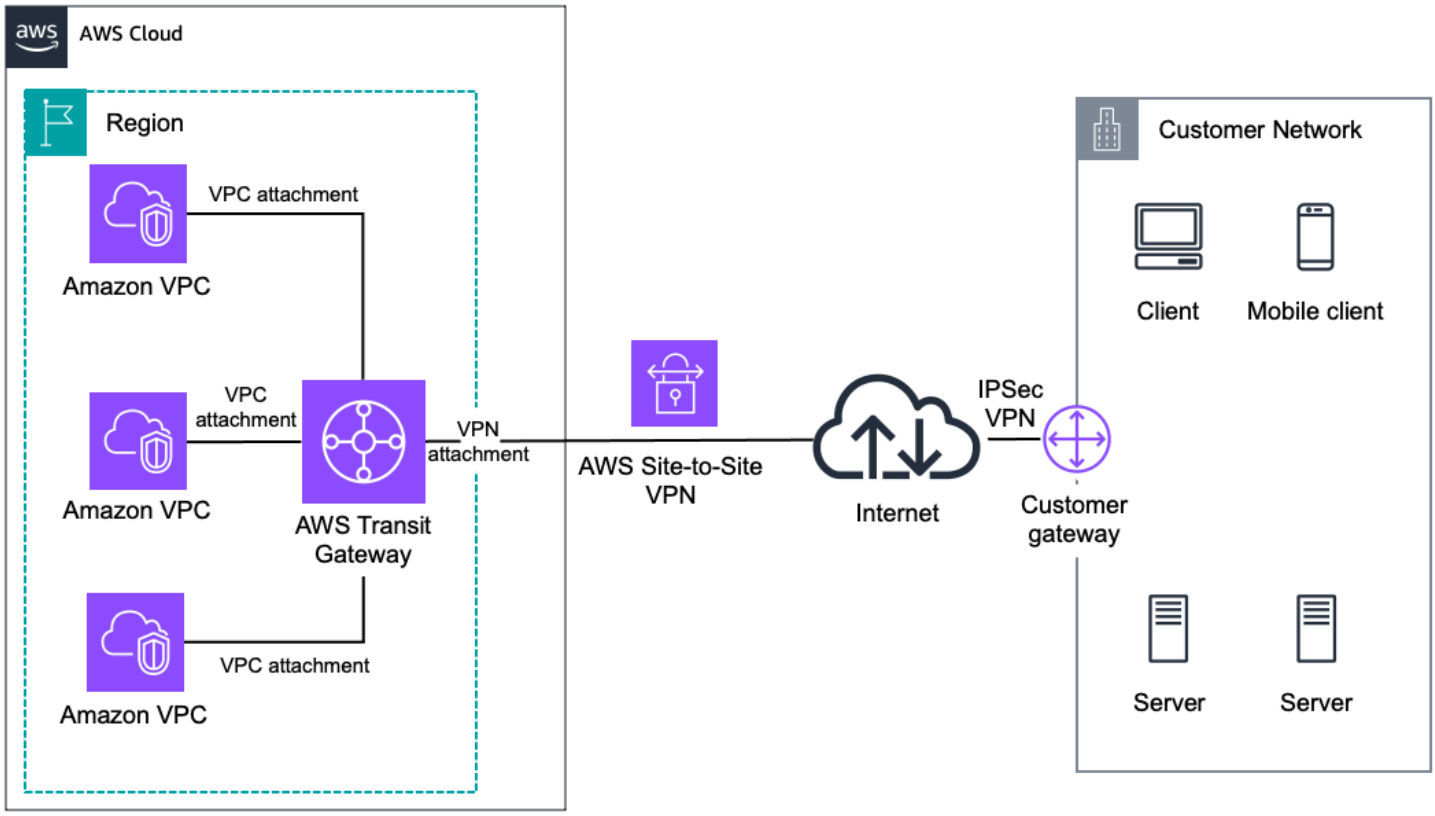
動態和靜態路由選項皆提供，讓您在路由組態中保有彈性。動態路由使用 BGP 對等互連，在 AWS 和這些遠端端點之間交換路由資訊。透過動態路由，您也可以在 BGP 公告中指定路由優先順序、政策和權重（指標），並影響網路和 AWS 之間的網路路徑。請務必注意，當您使用 BGP 時，必須在相同的使用者閘道裝置上同時終止 IPsec 和 BGP 工作階段，因此必須能夠同時終止 IPsec 和 BGP 工作階段。

其他資源

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

AWS Transit Gateway + AWS Site-to-Site VPN

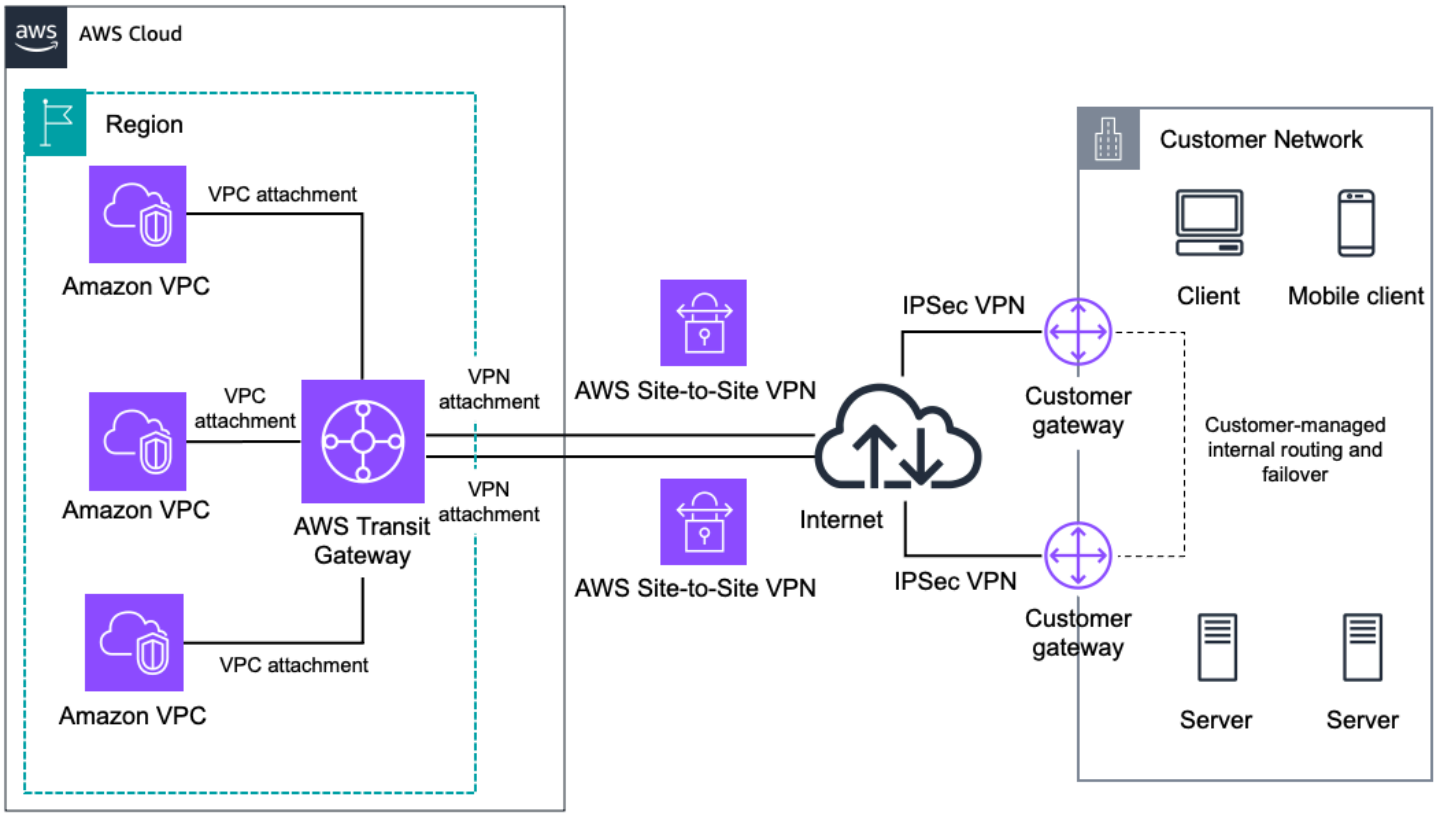
AWS Transit Gateway 是 AWS 受管的高可用性和可擴展性區域網路傳輸中樞，用於互連 VPCs和客戶網路。AWS Transit Gateway + VPN 使用 Transit Gateway VPN 連接，提供在遠端網路與透過網際網路的 Transit Gateway 之間建立 IPsec VPN 連線的選項，如下圖所示。



AWS Transit Gateway and AWS Site-to-Site VPN

當您想要利用 AWS 受管 VPN 端點連線到相同區域中VPCs 時，請考慮使用此方法，而無需額外成本和管理多個 Amazon VPCs 的多個 IPsec VPN 連線。

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

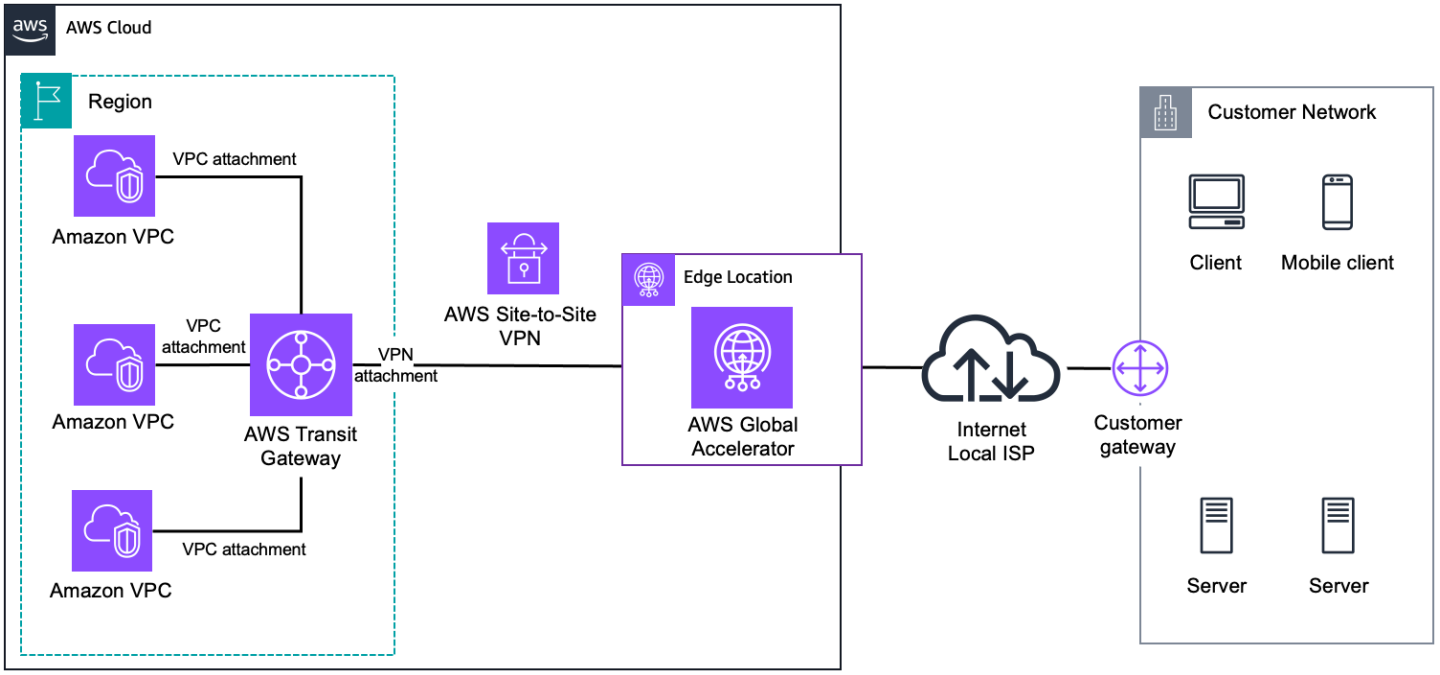


AWS Transit Gateway and Redundant VPN

動態和靜態路由選項都提供，讓您在 Transit Gateway VPN IPsec 連接上的路由組態中具有靈活性。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。透過動態路由，您也可以在 BGP 公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，必須在相同的使用者閘道裝置上同時終止 IPsec 和 BGP 工作階段，因此必須能夠同時終止 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 140，000 個封包。在 Transit Gateway 中終止 VPN 連線時，您可以使用等於成本多路徑 (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 – 不支援使用靜態路由的 ECMP。

此外，您可以在 AWS Site-to-Site VPN 連線中啟用加速。加速的 VPN 連接使用 AWS Global Accelerator 將流量從您的網路路由到最接近您客戶閘道裝置的 AWS 節點。您可以使用此選項，以避免流量透過公有網際網路路由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， AWS Transit Gateway 上的Site-to-Site連線支援 IPv4 和 IPv6 流量。適用的規定如下：

- 只有 VPN 通道的內部 IP 地址才支援 IPv6。 AWS 端點的外部 IP 地址是公有 IPv4 地址。客戶閘道 IP 地址應為公有 IPv4 地址。
- 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。

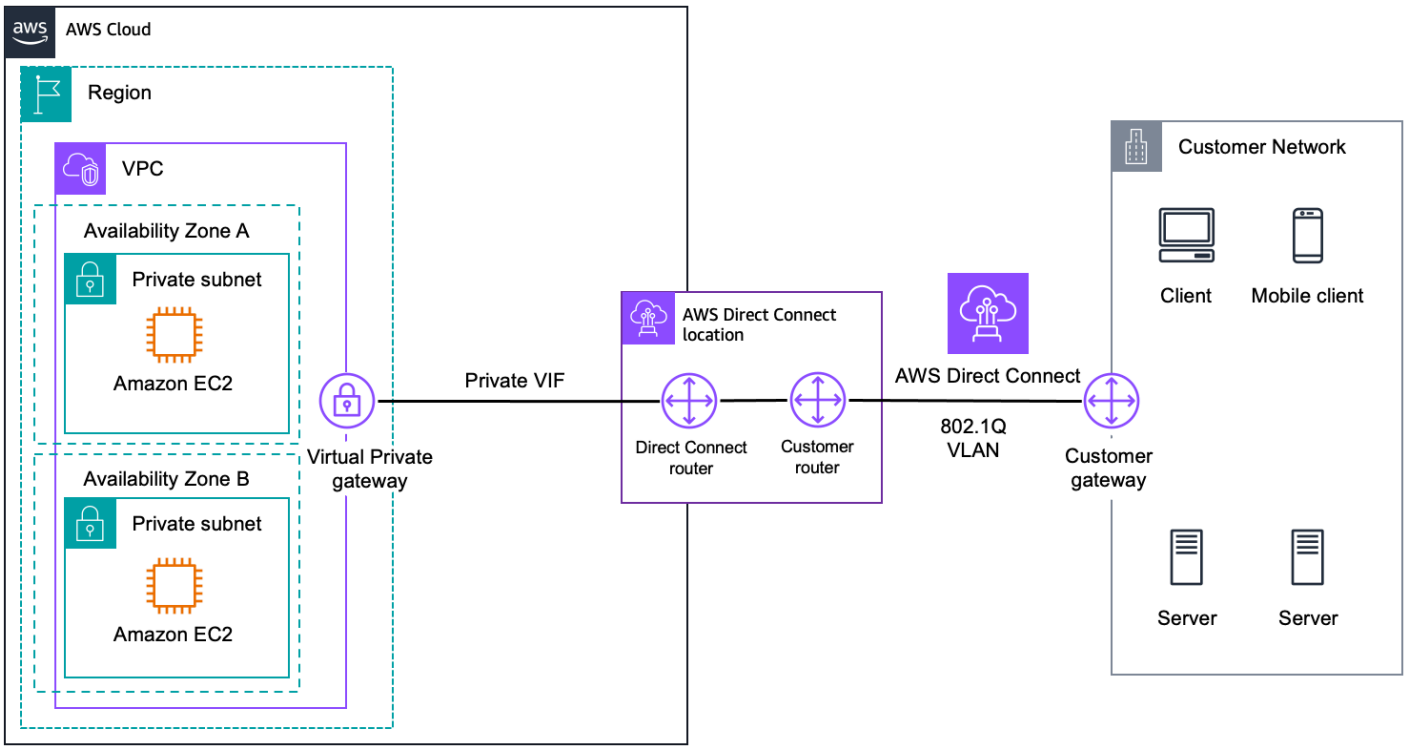
其他資源

- 傳輸閘道 VPN 連接
- 客戶閘道
- 使用Site-to-Site VPN
- 加速Site-to-Site連線

AWS Direct Connect

AWS Direct Connect 可讓您輕鬆地建立從內部部署網路到一或多個 VPCs專用連線。 Direct Connect 可以降低網路成本、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。它使用業界標準的 802.1Q VLANs，使用私有 IP 地址連線至 Amazon VPC。VLANs 是使用虛擬介面 (VIFs設定，您可以設定三種不同類型的 VIFs：

- 公有虛擬介面 - 建立 AWS 公有端點與資料中心、辦公室或主機代管環境之間的連線。
- 傳輸虛擬介面 - 在 AWS Transit Gateway 與資料中心、辦公室或主機代管環境之間建立私有連線。此連線選項涵蓋在 區段中???。
- 私有虛擬介面 - 在 Amazon VPC 資源與資料中心、辦公室或主機代管環境之間建立私有連線。下圖顯示私有 VIFs 的使用。



AWS Direct Connect

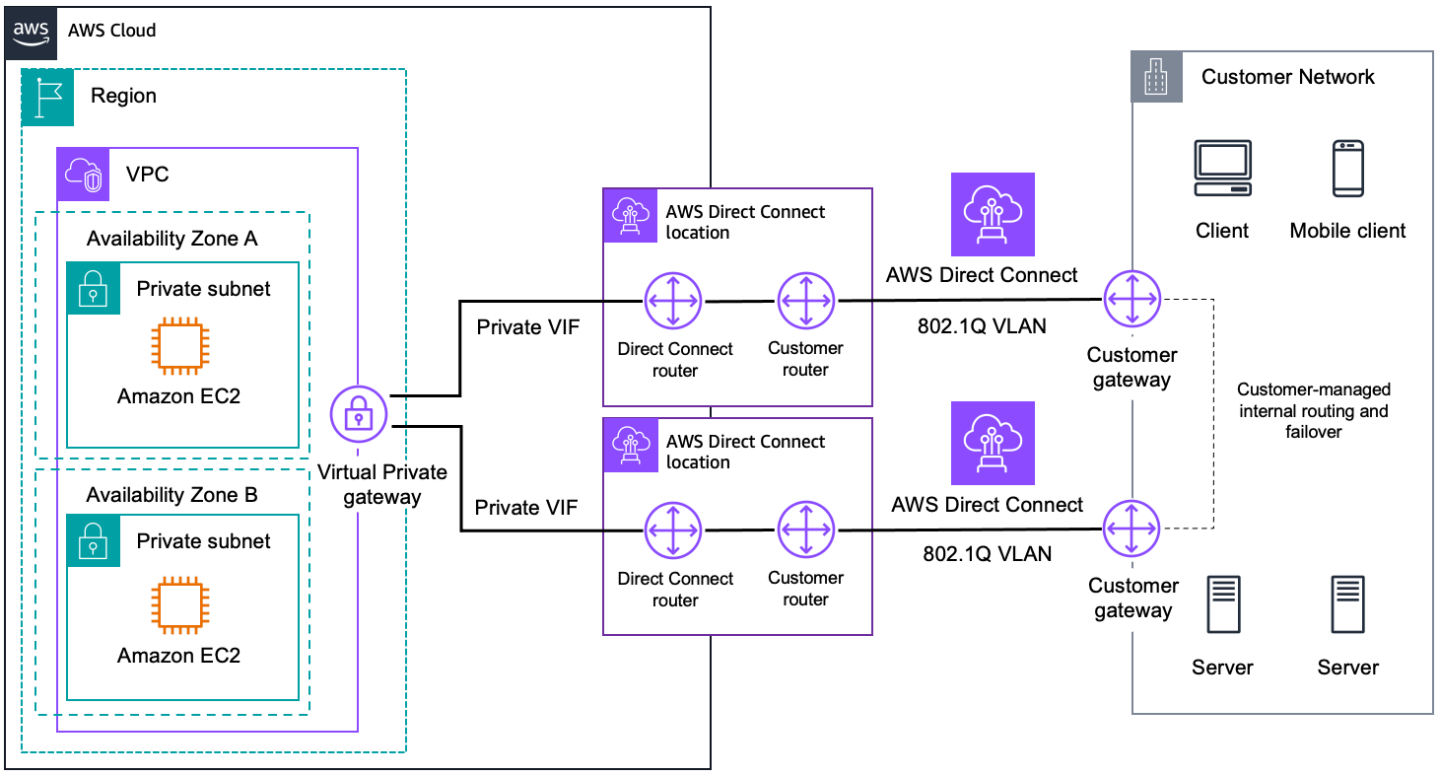
您可以使用 建立與 Direct Connect 位置中 AWS 裝置的交叉連線， AWS Direct Connect 以建立 AWS 與骨幹的連線。您可以從我們的任何 Direct Connect 位置 （ 中國除外 ） 存取任何 AWS 區域。如果您在某個位置沒有設備，您可以從 WAN 服務供應商的生態系統中進行選擇，以將 AWS Direct Connect 端點整合到與遠端網路的 AWS Direct Connect 位置。

使用 時 AWS Direct Connect，您有兩種連線類型：

- 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劃中的 AWS Direct Connect 合作夥伴合作，以協助您在 AWS Direct Connect 連線與資料中心、辦公室或主機代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是由 AWS Direct Connect 合作夥伴佈建並與您共用。您可以訂購介於 50 Mbps 到 10 Gbps 之間的連接埠速度。您在合作夥伴建立的 Direct Connect 連線和 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，都與合作夥伴合作。

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受管連線。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。

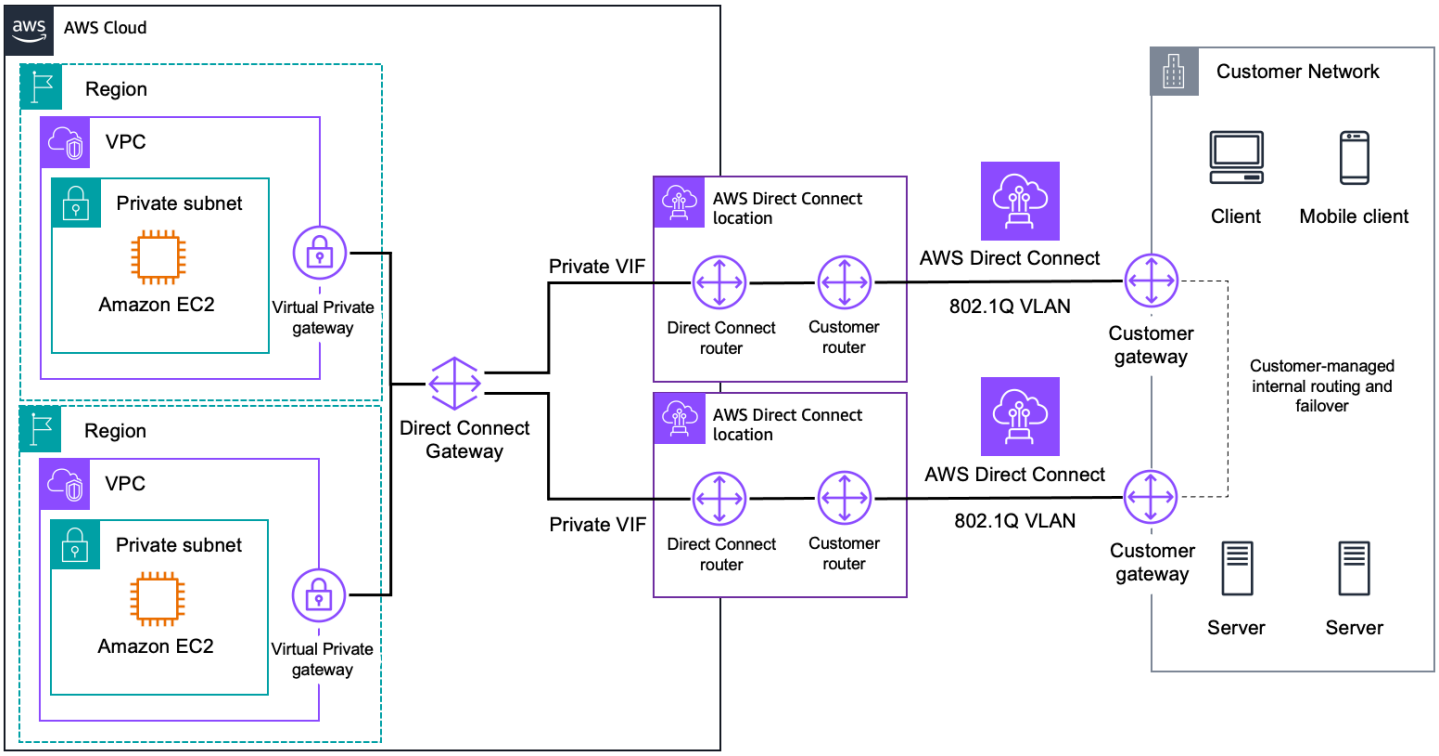
在 中討論高可用性時 AWS Direct Connect，建議使用其他 Direct Connect 連線。Direct Connect 彈性工具組提供在 AWS 與資料中心、辦公室或主機代管環境之間建立高度彈性網路連線的指引。下圖顯示高彈性連線選項的範例，其中兩個 Direct Connect 連線終止於兩個不同的 Direct Connect 位置。



備援 AWS Direct Connect

AWS Direct Connect 預設不會加密。對於 10 或 100 Gbps 的專用連線，您可以使用 MAC 安全性 (MACsec) 作為加密選項。對於 1 Gbps 或以下的連線，您可以在連線上方建立 VPN 通道 – 此選項涵蓋在 AWS Direct Connect + AWS Site-to-Site VPN和 AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN區段中。

中的一個重要資源 AWS Direct Connect 是 Direct Connect 閘道，這是一個全球可用的資源，可跨不同區域或 AWS 帳戶啟用與多個 Amazon VPCs 或 Transit Gateway 的連線。此資源也可讓您從一個私有 VIF 或傳輸 VIF 連線到任何參與的 VPC 或 Transit Gateway，減少 AWS Direct Connect 管理，如下圖所示。



AWS Direct Connect Gateway

關於 IP 定址， AWS Direct Connect 虛擬介面支援 IPv4 和 IPv6 BGP 工作階段進行雙堆疊操作。

- 私有和傳輸 VIFs IPv4 組態會使用 AWS 產生的 IPv4 地址或您設定的地址。對於公有 VIFs IPv4 BGP 對等互連，您必須指定您擁有的唯一公有 /31 IPv4 CIDR （或提交請求以指派 CIDR 區塊）。
- 對於所有類型的 VIFs IPv6 BGP 對等互連，AWS 會指派無法設定的 /125 CIDR。

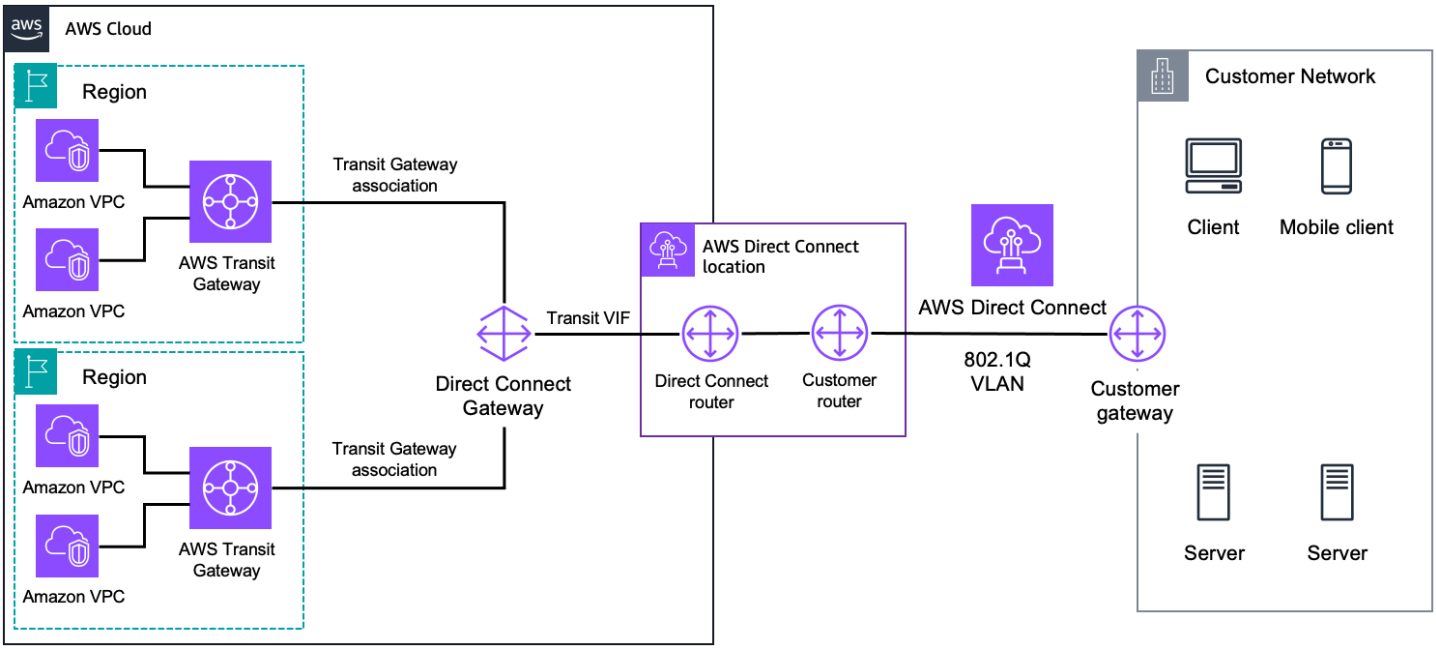
其他資源

- AWS Direct Connect 使用者指南
- AWS Direct Connect 虛擬介面
- AWS Direct Connect 閘道
- AWS Direct Connect 彈性工具組
- AWS Direct Connect MAC 安全性
- AWS Direct Connect 位置

- AWS Direct Connect 交付合作夥伴

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect + AWS Transit Gateway使用 Direct Connect 閘道的傳輸 VIF 連接，讓您的網路能夠透過私有專用連線連接多個區域性集中式路由器。下圖顯示連線至兩個路由器。



AWS Direct Connect and AWS Transit Gateway

每個 AWS Transit Gateway 都是網路傳輸中樞，可將相同區域中VPCs 互連，將 Amazon VPC 路由組態整合在一個位置。此解決方案透過私有連線簡化 Amazon VPC 與網路之間的連線管理，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。

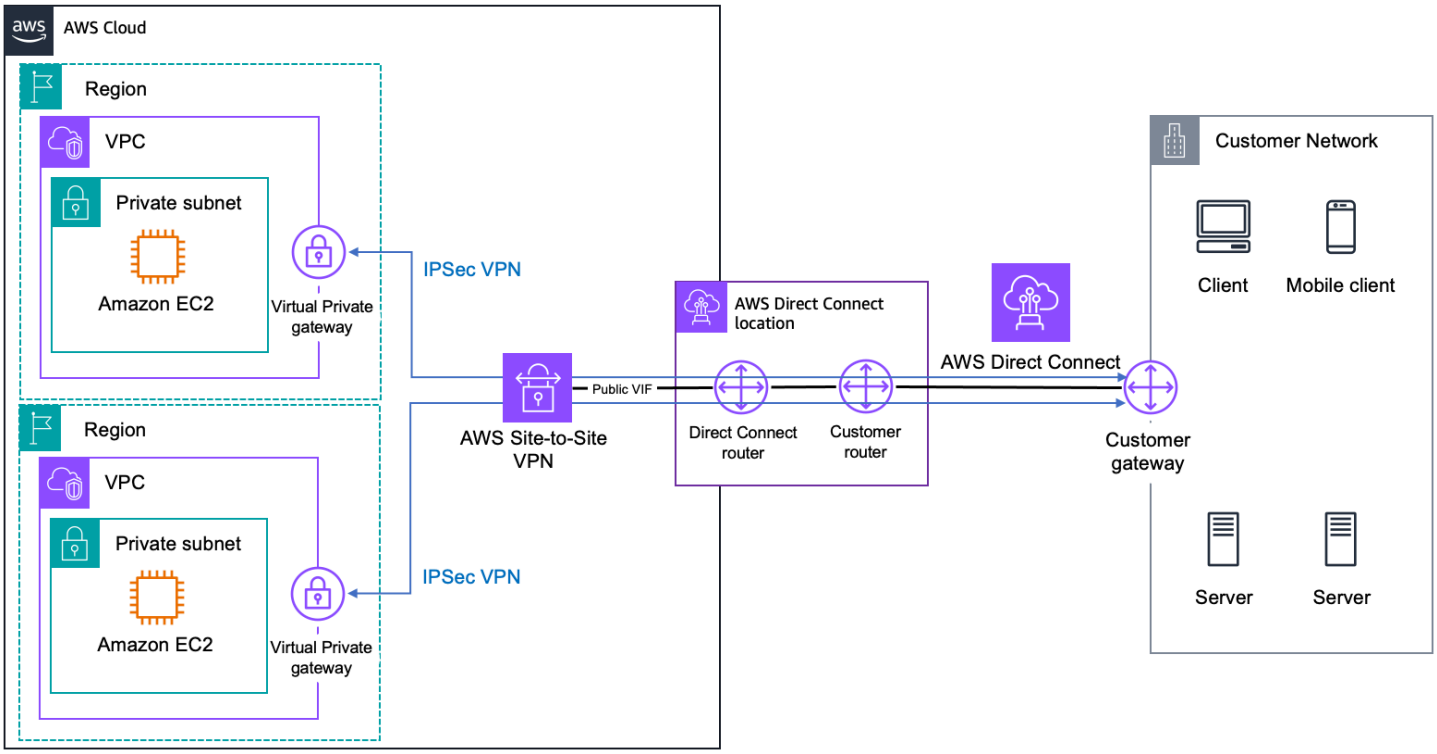
其他資源

- AWS Direct Connect 使用者指南
- 在 中連結彙總群組 AWS Direct Connect
- 部落格文章：整合 sub-1 Gbps 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 連線與 AWS 受管 VPN 解決方案結合。 AWS Direct Connect 公有 VIFs會在您的網路與公有 AWS 資源之間建立專用網

路連線，例如 AWS Site-to-Site VPN 端點。建立與服務的連線後，您就可以建立與對應 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

此解決方案結合了end-to-end安全 IPsec 連線的優點，以及低延遲和增加的 頻寬 AWS Direct Connect ，可提供比網際網路 VPN 連線更一致的網路體驗。BGP 連線工作階段是在公有 VIF 上的 AWS Direct Connect 與路由器之間建立。另一個 BGP 工作階段或靜態路由將在 IPsec VPN 通道上的虛擬私有閘道和路由器之間建立。

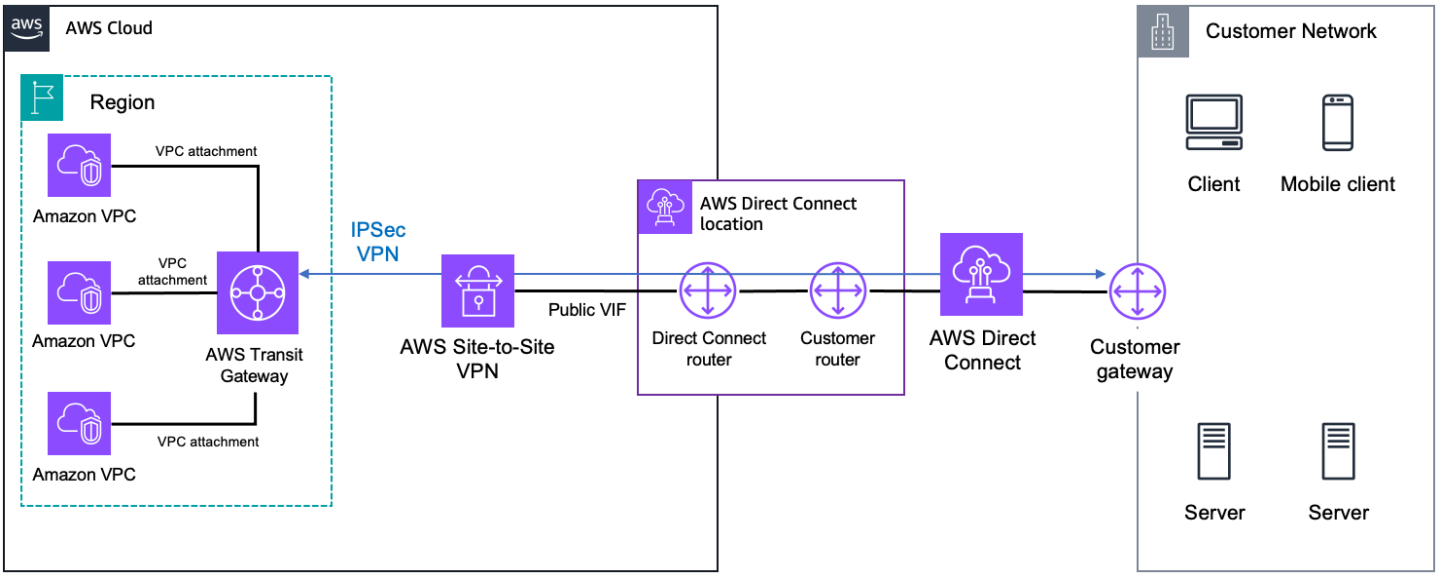
其他資源

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

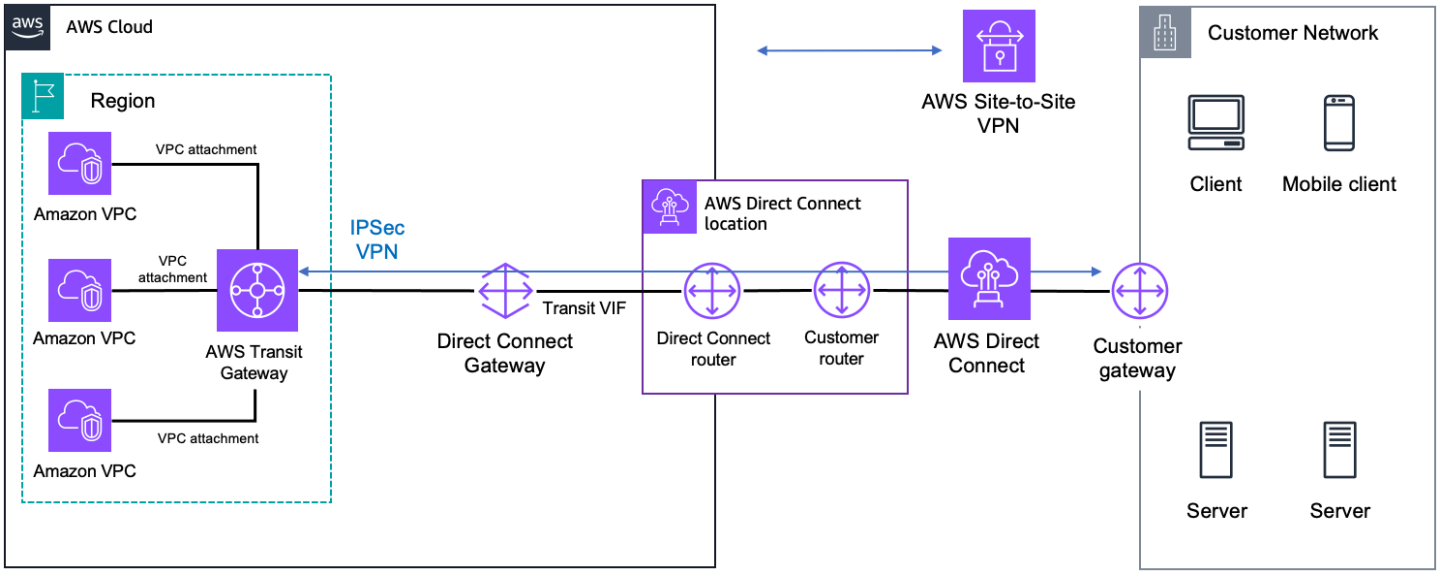
AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN

使用 AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN，您可以透過私有專用連線，在網路與 Amazon VPCs 的區域集中式路由器之間啟用end-to-end IPsec 加密連線。

您可以使用 AWS Direct Connect 公有 VIFs，先在您的網路與公有 AWS 資源之間建立專用網路連線，例如 AWS Site-to-Site VPN 端點。一旦建立此連線，您就可以建立 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，並將相同區域中多個 Amazon VPCs 的 IPsec VPN 連線成本降至最低時，請考慮採用此方法，並透過網際網路式 VPN 提供私有專用連線的低延遲和一致的網路體驗優勢。BGP 工作階段是在 AWS Direct Connect 與路由器之間使用公有或傳輸 VIF 建立的。另一個 BGP 工作階段或靜態路由將在 IPsec VPN 通道上的 AWS Transit Gateway 路由器之間建立。

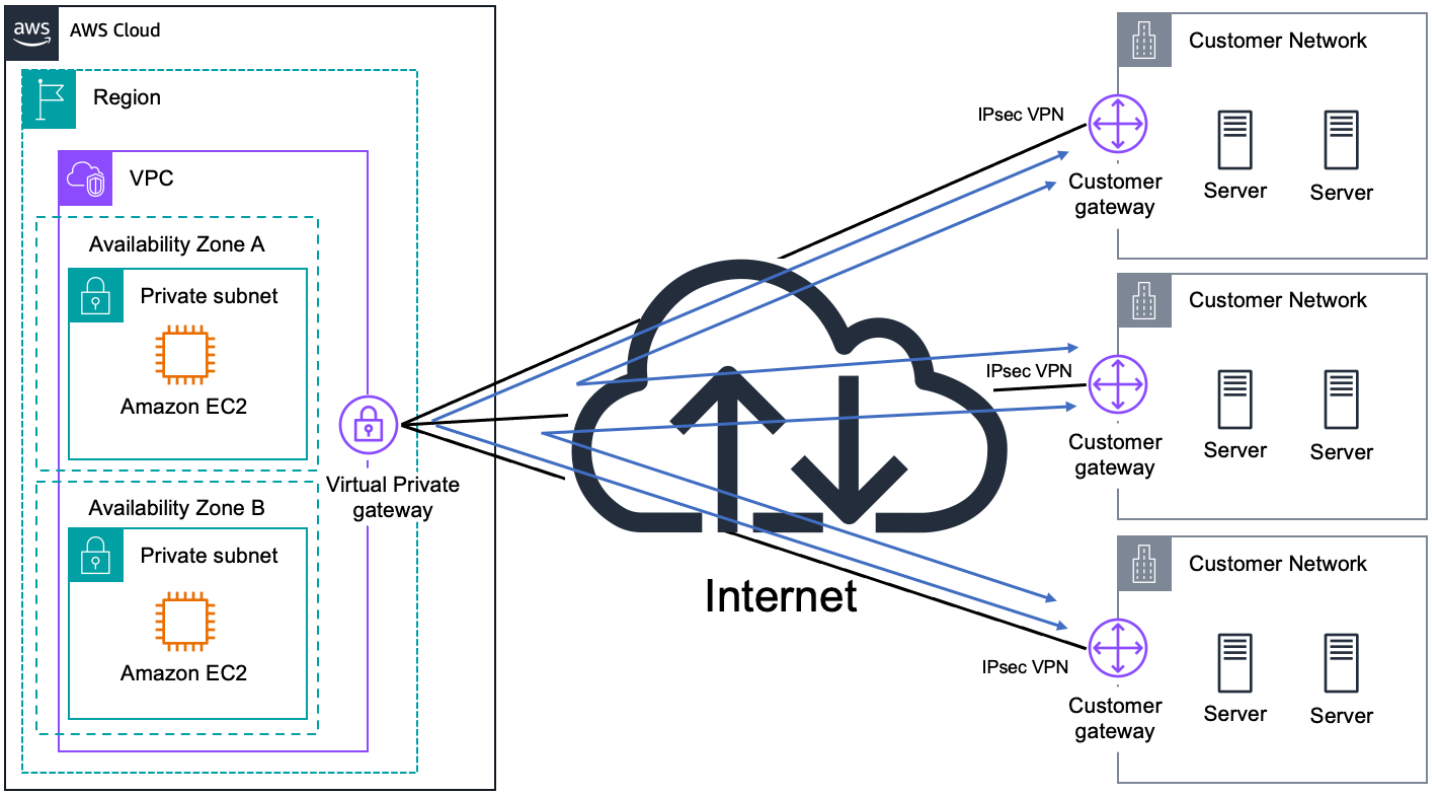
其他資源

- AWS Direct Connect 虛擬介面
- 傳輸閘道 VPN 連接
- 客戶閘道裝置的需求
- 使用 Amazon VPC 測試的客戶閘道裝置
- AWS Site-to-Site VPN – 使用 的私有 IP VPN AWS Direct Connect

Site-to-Site VPN CloudHub

在上述 AWS 受管 VPN 選項的基礎上，您可以使用 Site-to-Site VPN CloudHub 安全地從一個網站與另一個網站通訊。 Site-to-Site VPN CloudHub 會在簡單的hub-and-spoke模型上運作，您可以搭配或不搭配 VPC 使用。如果您有多個分支辦公室和現有的網際網路連線，並想要實作便利、可能低成本的hub-and-spoke模型，在這些遠端辦公室之間進行主要或備份連線，請使用此方法。

下圖顯示 Site-to-Site VPN CloudHub 架構，其中行指出透過其 Site-to-Site VPN 連線路由之遠端站台之間的網路流量。



Site-to-Site VPN CloudHub

Site-to-Site 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 自治系統編號 (ASNs)。遠端站台不得有重疊的 IP 範圍。您的閘道會透過其 VPN 連線公告適當的路由 (BGP 字首）。這些路由公告會接收並重新公告到每個 BGP 對等，以便每個網站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 CloudHub 在網站之間提供安全通訊
- AWS Site-to-Site VPN 使用者指南
- 客戶閘道裝置的需求
- 使用 Amazon VPC 測試的客戶閘道裝置

AWS Transit Gateway + SD-WAN 解決方案

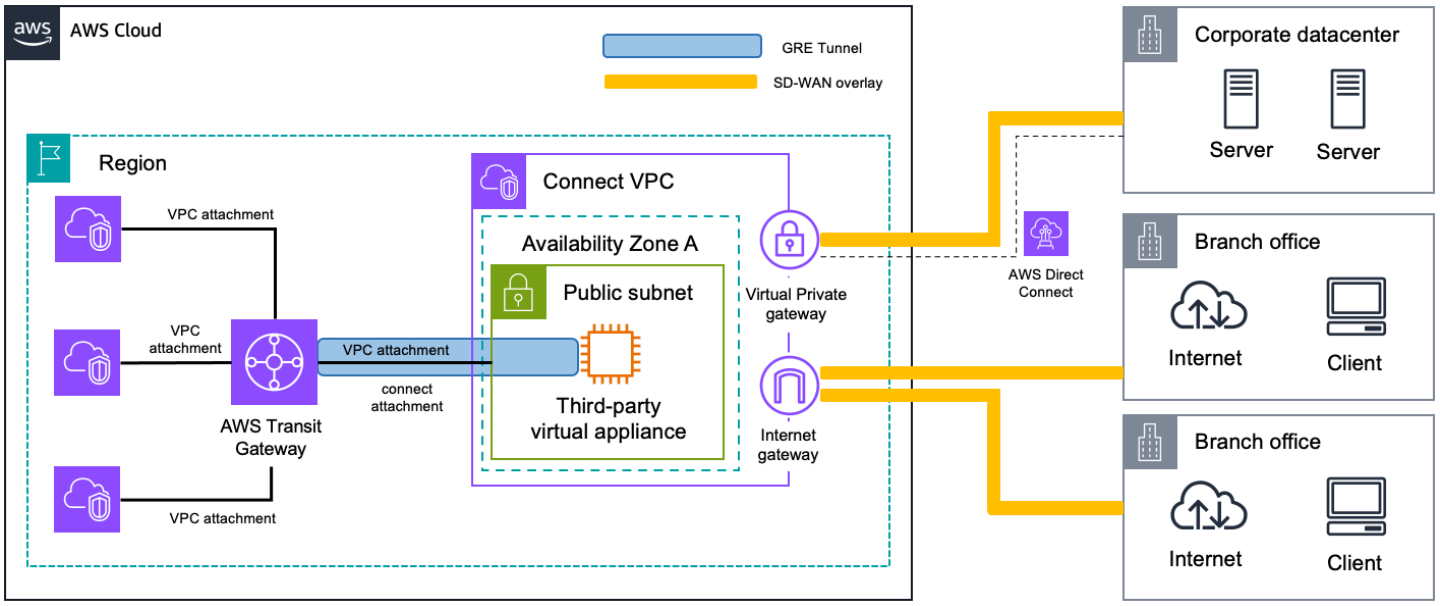
軟體定義的廣域網路 (SD-WANs) 用於透過不同的傳輸網路（例如公有網際網路、MPLS 網路或 AWS 骨幹 AWS Direct Connect使用）連接您的資料中心、辦公室或主機代管環境，根據網路條件、應用程式類型或服務品質 (QoS) 需求，自動且動態地跨最適當且最有效率的路徑管理流量。

如果您有複雜的網路拓撲，具有數個資料中心、辦公室或主機代管環境，需要自行與 AWS 通訊，請使用此方法。SD-WAN 解決方案可協助您有效率地管理這類網路。

討論 SD-WAN 網路與 AWS 的連線時， AWS Transit Gateway 提供受管、高可用性和可擴展的區域網路傳輸中樞，以互連 VPCs 和 SD-WAN 網路。Transit Gateway 連線附件提供將 SD-WAN 基礎設施和設備與 AWS 連線的原生方式。這可讓您輕鬆地將 SD-WAN 擴展到 AWS，而無需設定 IPsec VPNs。

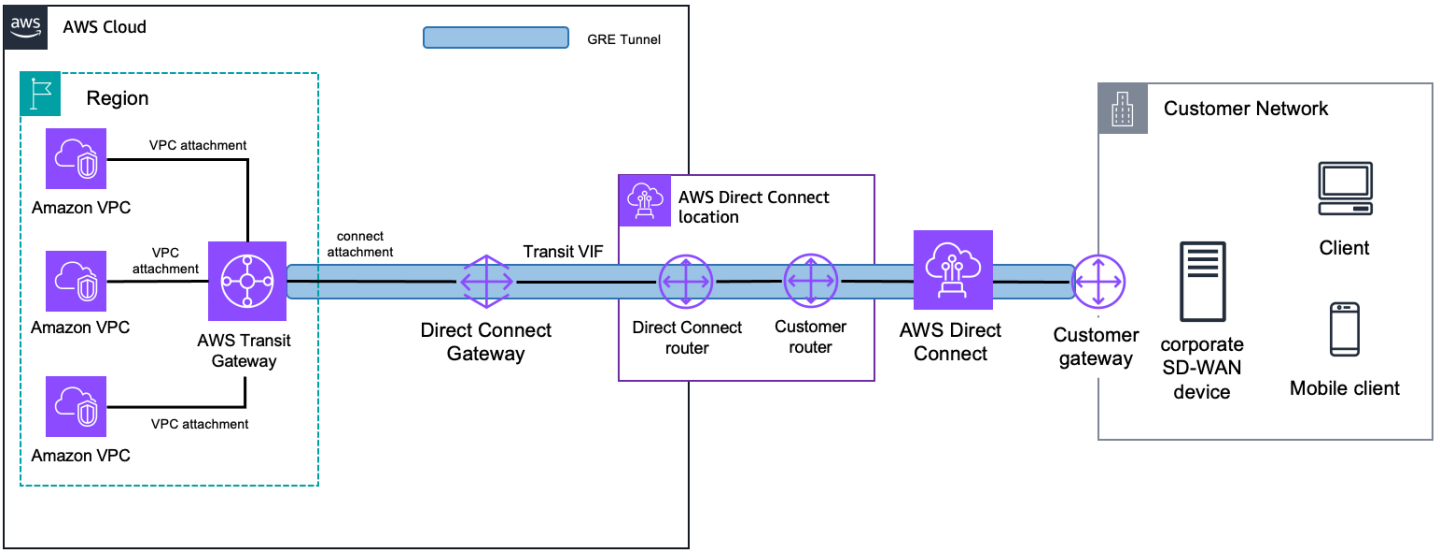
傳輸閘道連線附件支援一般路由封裝 (GRE)，可提供比 VPN 連線更高的頻寬效能。它支援動態路由的邊界閘道協定 (BGP)，並不需要設定靜態路由。這可簡化網路設計並降低相關聯的營運成本。此外，它與 Transit Gateway Network Manager 的整合透過全球網路拓撲、連接層級效能指標和遙測資料提供進階可見性。

使用連線附件將 SD-WAN 網路整合到 Transit Gateway 時，您有兩種常見模式。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 連接做為虛擬設備與 Transit Gateway 之間 Transit Gateway 連接連接的基礎傳輸，如下圖所示。



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

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



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

使用 Transit Gateway Connect 附件時需要注意一些考量：

- 您可以在現有的 Transit Gateway 上建立連線附件。
- 第三方設備必須使用 GRE 通道設定，以便使用連線附件從 Transit Gateway 傳送和接收流量。設備必須使用 BGP 設定，以進行動態路由更新和運作狀態檢查。
- 連線附件不支援靜態路由。

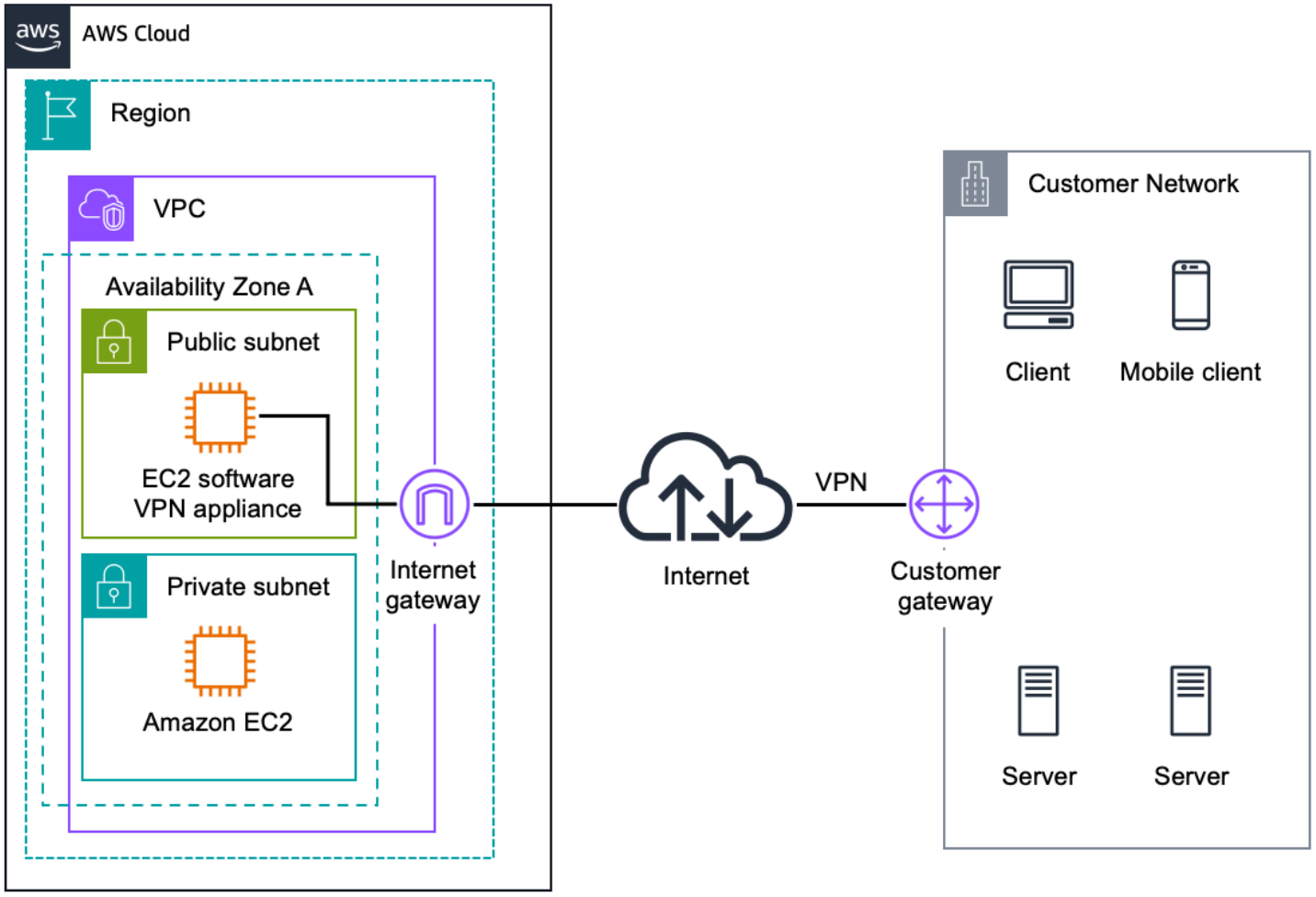
- Transit Gateway 連線附件支援每個 GRE 通道最多 5 Gbps 的頻寬。高於 5 Gbps 的頻寬可以透過在多個 Connect 對等 (GRE 通道） 中為相同的 Connect 連接公告相同的字首來實現。
- 每個連線附件最多支援四個 Connect 對等。
- Transit Gateway 連線附件支援透過 BGP 的多協定延伸 (MBGP 或 MP-BGP) 進行 IPv6 和動態路由公告。

其他資源

- 傳輸閘道對等互連附件
- 需求和考量事項
- 部落格文章：使用 AWS Transit Gateway Connect 簡化 SD-WAN 連線

軟體 VPN

Amazon VPC 可讓您在遠端網路與在 Amazon VPC 網路中執行的軟體 VPN 設備之間建立 VPN 連線，藉此靈活地完整管理 Amazon VPC 連線的兩側。如果您為了合規目的或利用 Amazon VPC VPN 解決方案目前不支援的閘道裝置，必須管理 VPN 連接的兩端，建議使用此選項。下圖顯示此選項。



軟體Site-to-Site VPN

您可以從由多個合作夥伴和開放原始碼社群組成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。除了此選項之外，您還必須負責管理軟體設備，包括組態、修補程式和升級。

請注意，此設計會在網路設計中引入潛在的單一故障點，因為軟體 VPN 設備會在單一 Amazon EC2 執行個體上執行。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

- 中可用的 VPN 設備 AWS Marketplace
- 技術簡介 - 將 Cisco ASA 連線至 VPC EC2 執行個體 (IPsec)
- 技術簡介 - 使用 EC2 執行個體連接多個 VPCs (IPsec)
- 技術簡介 - 使用 EC2 執行個體 (SSL) 連接多個 VPCs

Amazon VPC-to-Amazon VPC 連線選項

當您想要將多個 Amazon VPCs 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、多個區域中的存在或內部收費要求而需要多個 VPCs，這非常有用，以便更輕鬆地在 Amazon VPCs 之間整合 AWS 資源。您也可以將這些模式與 Network-to-Amazon VPC 連線選項結合，以建立跨越遠端網路和多個 VPCs的公司網路。

對要連接的每個 VPCs 使用非重疊 IP 範圍時，最好在 VPC 之間實現 VPC 連線。例如，如果您想要連接多個 VPCs，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、不重疊的 CIDR 區塊，以供每個 VPC 使用。如需 Amazon VPC 路由和限制條件的其他資訊，請參閱 Amazon VPC 常見問答集。

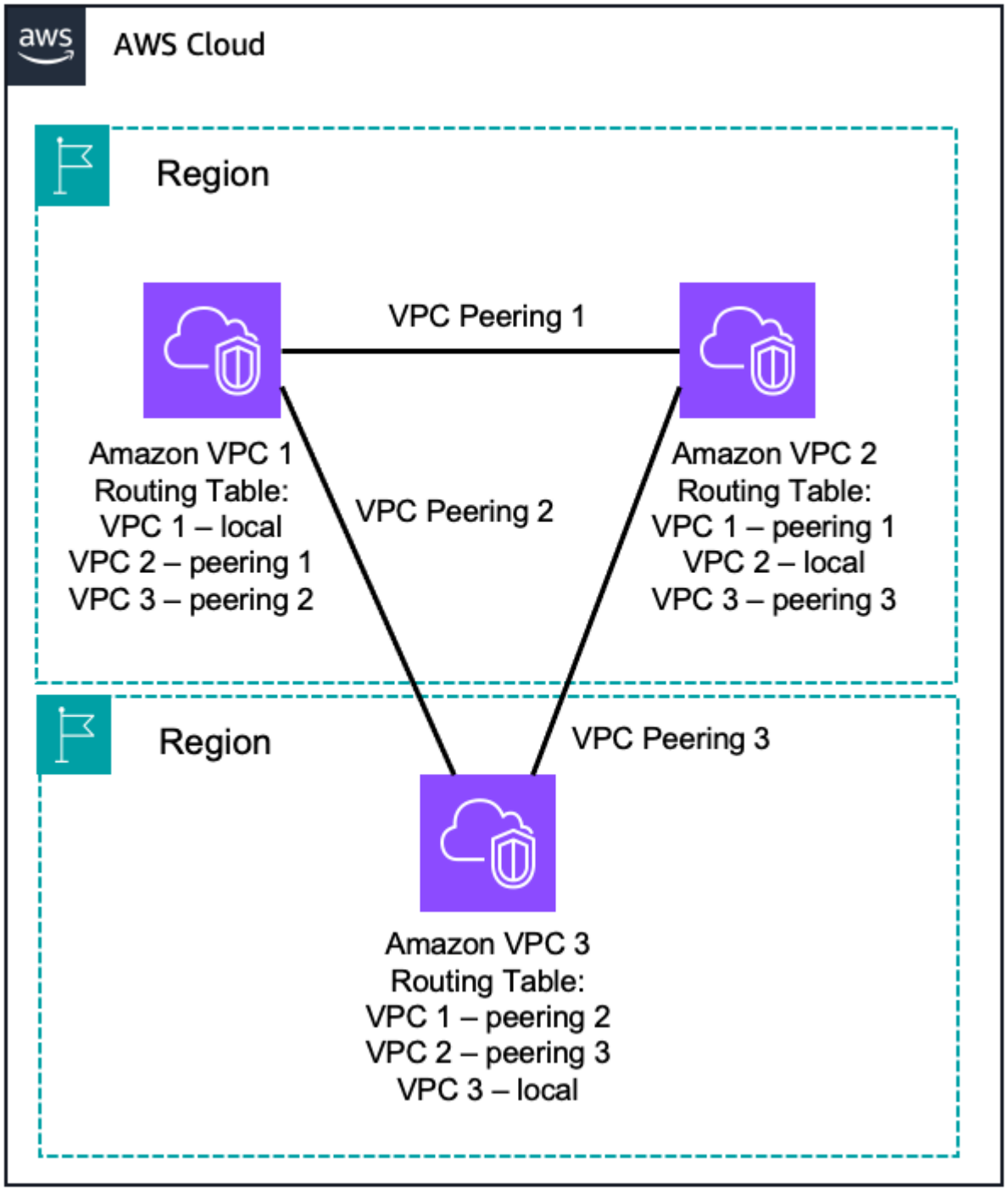
選項	使用案例	優點	限制
VPC 對等互連	兩個 VPCs 之間的 AWS 提供的網路連線。	利用 AWS 受管的可擴展聯網基礎設施	VPC 對等互連不支援傳輸對等互連關係 難以大規模管理
AWS Transit Gateway	AWS 為 VPCs 提供的區域路由器連線	AWS 受管高可用性和可擴展性服務 區域網路中樞，最多可連接 5，000 個附件	Transit Gateway 對等僅支援靜態路由
AWS PrivateLink	使用介面端點VPCs 之間的 AWS 提供的網路連線	利用 AWS 受管的可擴展聯網基礎設施	VPC 端點服務僅適用於建立它們的 AWS 區域
軟體 VPN	VPCs 之間的軟體設備型 VPN 連線	支援各種 VPN 廠商、產品和通訊協定 完全由您管理	您負責為所有 VPN 端點實作 HA 解決方案（如果需要） VPN 執行個體可能會成為網路瓶頸
軟體 VPN-to-AWS Site-to-Site VPN	VPCs 之間的軟體設備與 VPN 連線	AWS 受管高可用性 VPC VPN 連接	您負責為軟體設備 VPN 端點實作 HA 解決方案（如果需要）

選項	使用案例	優點	限制
		支援由您管理的各種 VPN 廠商和產品 支援靜態路由和動態 BGP 對等互連和路由政策	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 Managed 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。可以在您自己的 VPCs 之間或另一個 AWS 帳戶中的 VPC 建立 VPC 對等互連。VPC 對等互連也支援區域間對等互連。

使用區域間 VPC 對等互連的流量一律維持在全域 AWS 骨幹上，絕不會周遊公有網際網路，從而減少威脅媒介，例如常見的入侵和 DDoS 攻擊。



VPC-to-VPC Peering

AWS 使用 VPC 的現有基礎設施來建立 VPC 互連連線，而且不依賴單獨的實體硬體。因此，它們不會在 VPCs 之間引入潛在的單點故障或網路頻寬瓶頸。此外，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 對等互連。

Amazon VPCs不支援傳輸對等互連，這表示您無法使用第三個 VPCs作為傳輸直接對等互連的兩個 VPC 進行通訊。如果您希望所有 VPCs使用 VPC 對等互連彼此通訊，則需要在它們之間建立 1：1 VPC 對等互連。或者，您可以使用 AWS Transit Gateway 或 AWS Cloud WAN 做為網路傳輸中樞。

VPC 對等互連連線支援 IPv4 和 IPv6 流量。不過，如果兩個 VPCs 的主要 IPv4 CIDR 區塊重疊，則無法對等互連，無論使用的次要 IPv4 或 IPv6 CIDR 區塊為何。如果您打算在 VPCs 之間使用 VPC 對等互連，則在將主要 CIDR 區塊指派給 VPC 時請考量這一點。

其他資源

- Amazon VPC 對等互連
- 什麼是 VPC 對等互連？

AWS Transit Gateway

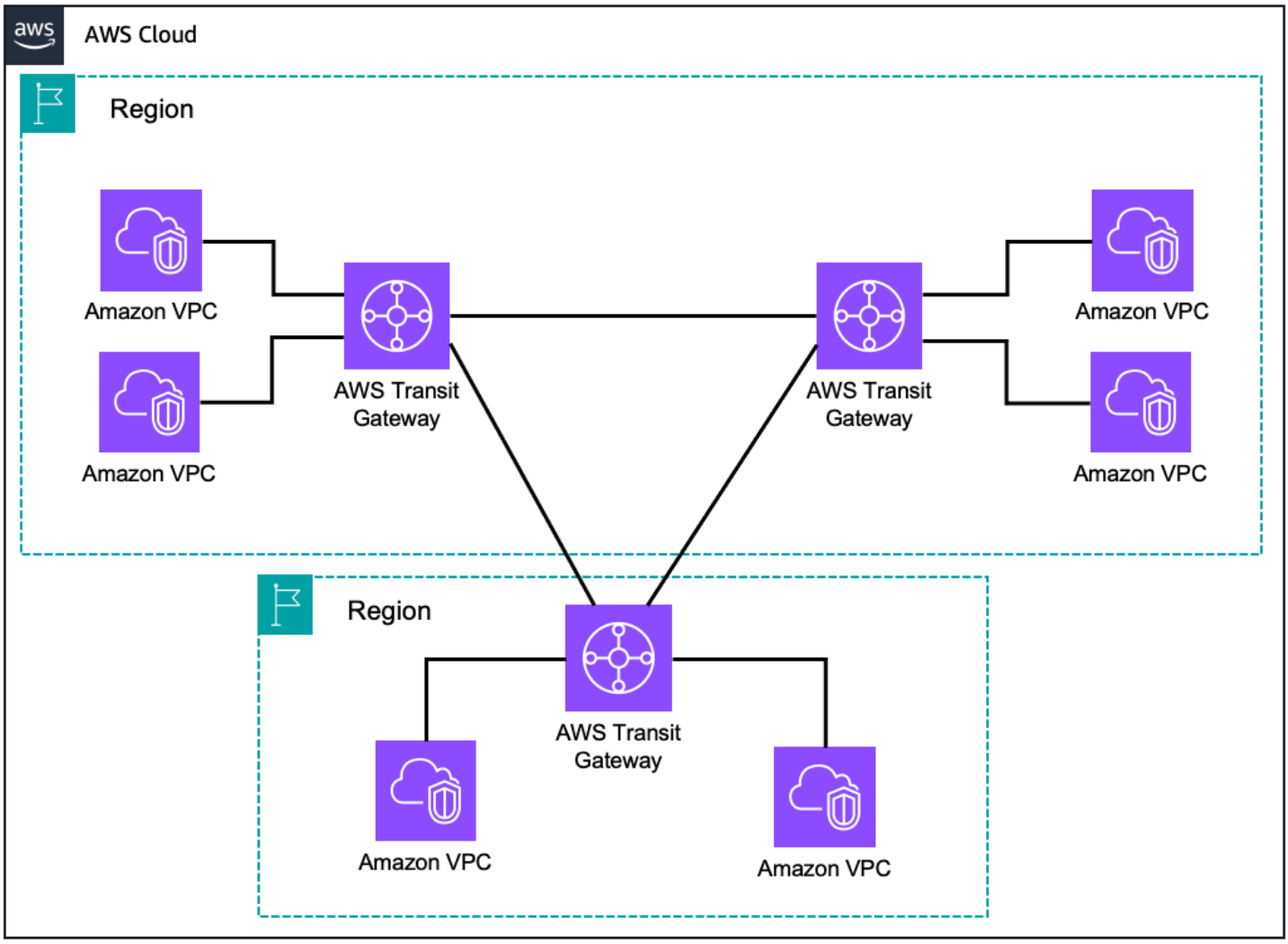
AWS Transit Gateway 是一種高可用性和可擴展的服務，可將區域的 AWS VPC 路由組態與hub-and-spoke式架構合併。每個語音 VPC 只需要連接到 Transit Gateway 即可存取其他連線VPCs。支援 IPv4 和 IPv6 流量 AWS Transit Gateway。

您可以利用數個 Transit Gateway 路由表、關聯和傳播，將流量分割在相同的 Transit Gateway 中。您將能夠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式架構，集中存取共用服務，例如流量檢查、界面 VPC 端點存取，或透過 NAT 閘道或 NAT 執行個體傳出流量。此集中化可簡化在多個 VPCs 中管理這些資源的複雜性，並可讓您在 AWS 中擴展您的足跡時獲得更好的控制。

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 流量一律保留在全域 AWS 骨幹上，絕不會周遊公有網際網路，進而減少常見的入侵和 DDoS 攻擊等威脅媒介。

使用大量 VPCs，Transit Gateway 可透過 VPC-to-VPC 通訊管理，如下圖所示。



AWS Transit Gateway

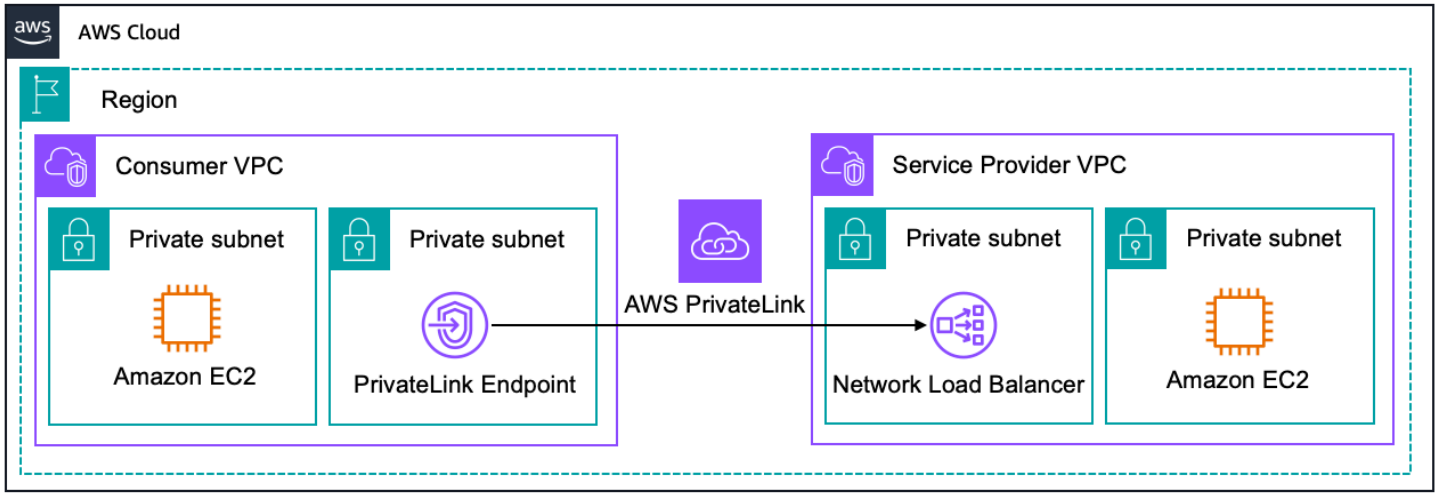
若要集中了解進出傳輸閘道的 IP 流量，您可以將傳輸閘道流量日誌發佈至 Amazon CloudWatch Logs 和 Amazon S3。流量日誌資料是在網路流量路徑之外收集，因此不會影響網路輸送量或延遲。

其他資源

- Amazon VPC 傳輸閘道
- 傳輸閘道對等連接
- 使用傳輸閘道
- 使用傳輸閘道流量日誌記錄網路流量

AWS PrivateLink

AWS PrivateLink 可讓您透過 VPC 中的私有 IP 地址，連線至某些 AWS 服務、其他 AWS 帳戶託管的服務（稱為端點服務) 和支援的 AWS Marketplace 合作夥伴服務。界面端點是直接在 VPC 內部建立，使用 VPC 子網路中的彈性網路界面和 IP 地址。這表示 VPC 安全群組可用來管理對端點的存取。



AWS PrivateLink

如果您想要使用私有 IP 地址，在 AWS 網路中安全地使用另一個 VPC 提供的服務，建議您使用此方法。或者， AWS PrivateLink 當 VPCs有重疊的 IP 地址時， 是理想的解決方案。

AWS PrivateLink 完全支援 IPv6，但必須啟用或修改目的地 VPCs、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。

的存取控制 AWS PrivateLink

界面端點是直接在 VPC 內部建立，方法是使用 VPC 子網路中的彈性網路界面和 IP 地址。這表示 VPC 安全群組可用來管理端點的網路存取。

當您建立介面端點或閘道端點時，您也可以連接端點政策。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。

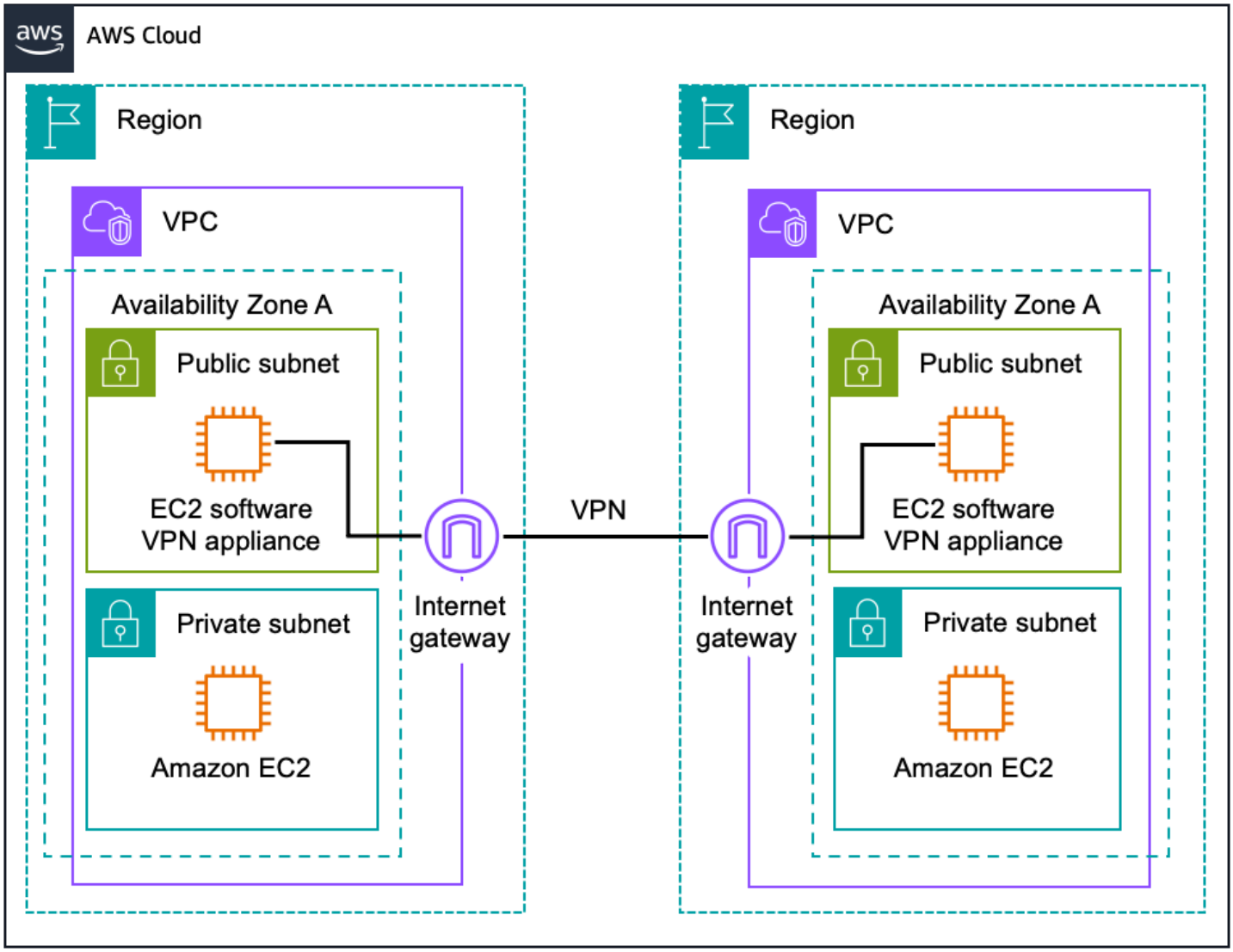
端點政策不會覆寫或取代 IAM 使用者政策或服務特定政策 （例如 Amazon S3 儲存貯體政策）。如果您使用介面端點連接至 Amazon S3，您也可使用 Amazon S3 儲存貯體政策來控制特定端點或特定 VPC 對儲存貯體的存取。

其他資源

- 介面 VPC 端點 (AWS PrivateLink)
- VPC 端點服務 (AWS PrivateLink)
- 部落格文章：使用 PrivateLink 服務和端點加速採用 IPv6
- 部落格文章：使用重疊 IP 範圍連接網路
- AWS PrivateLink 合作夥伴

軟體 VPN

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，以將多個 VPCs 連接到更大的虛擬私有網路，以便每個 VPC 中的執行個體可以使用私有 IP 地址無縫地互相連接。當您想要使用偏好的 VPN 軟體提供者來管理 VPN 連接的兩端時，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

您可以從由多個合作夥伴和開放原始碼社群組成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。除了這項選擇之外，您也必須負責管理軟體設備，包括組態、修補程式和升級。

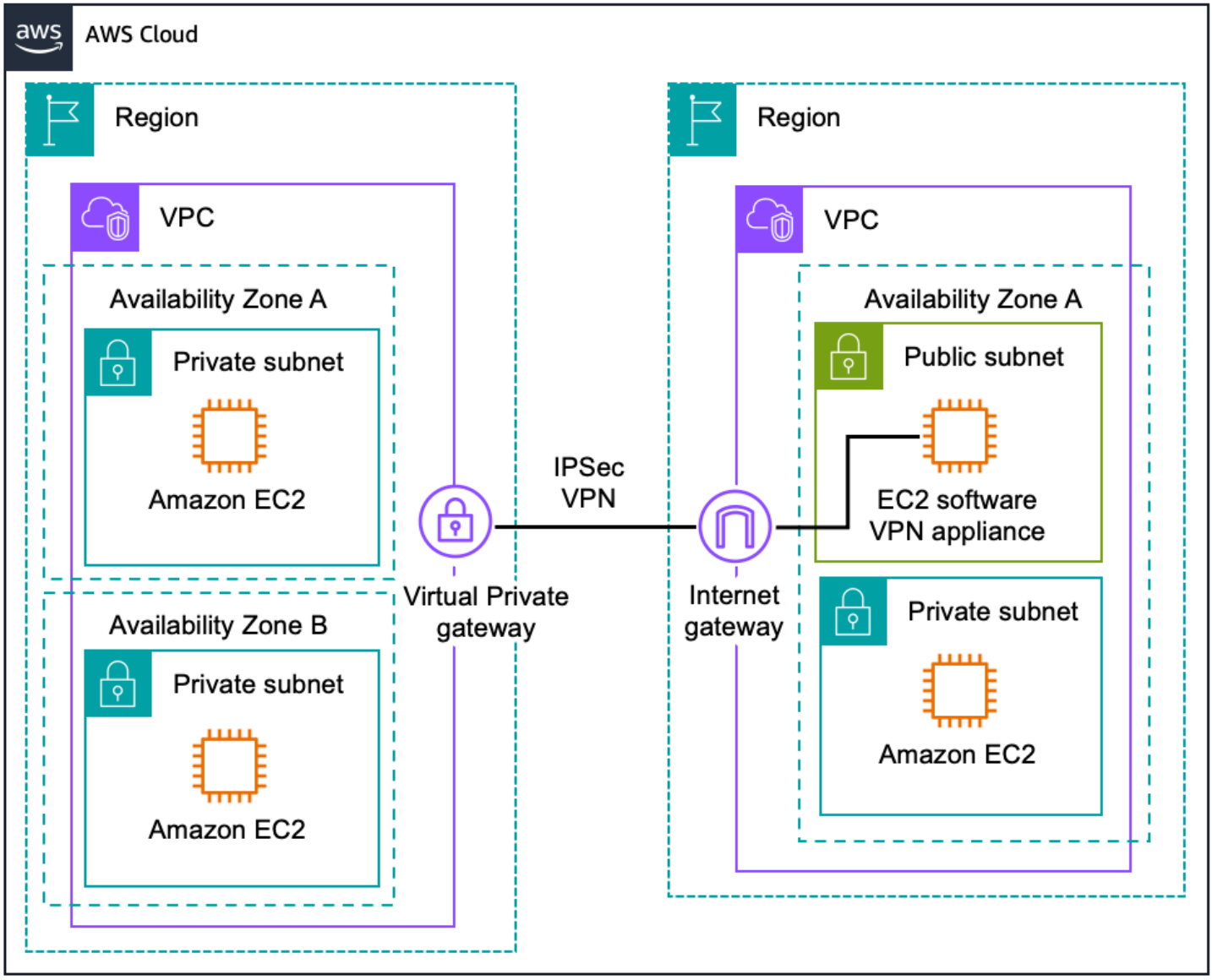
請注意，此設計會在軟體 VPN 設備在單一 Amazon EC2 執行個體上執行時，將潛在的單點故障引入網路設計。如需其他資訊，請參閱 附錄 A：軟體 VPN 執行個體的高階 HA 架構。

其他資源

- 可從 取得的 VPN 設備 AWS Marketplace
- 技術簡介 - 使用 EC2 執行個體連接多個 VPCs (IPsec)
- 技術簡介 - 使用 EC2 執行個體 (SSL) 連接多個 VPCs

軟體 VPN-to-AWS Site-to-Site VPN

Amazon VPC 提供結合 AWS 受管 VPN 和軟體 VPN 選項以連接多個 VPCs彈性。透過此設計，您可以在軟體 VPN 設備與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 地址無縫地互相連接。此選項在一個 Amazon VPC 中使用虛擬私有閘道，並在另一個 Amazon VPC 中使用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潛在的單點故障。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

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

軟體access-to-Amazon VPC 連線選項

透過軟體遠端存取 VPN，您可以利用低成本、彈性和安全的 服務來實作遠端存取解決方案，同時提供無縫的連線 AWS 託管資源體驗。擁有較不廣泛遠端網路，或尚未為員工建置和部署遠端存取解決方案的小型公司通常偏好此選項。

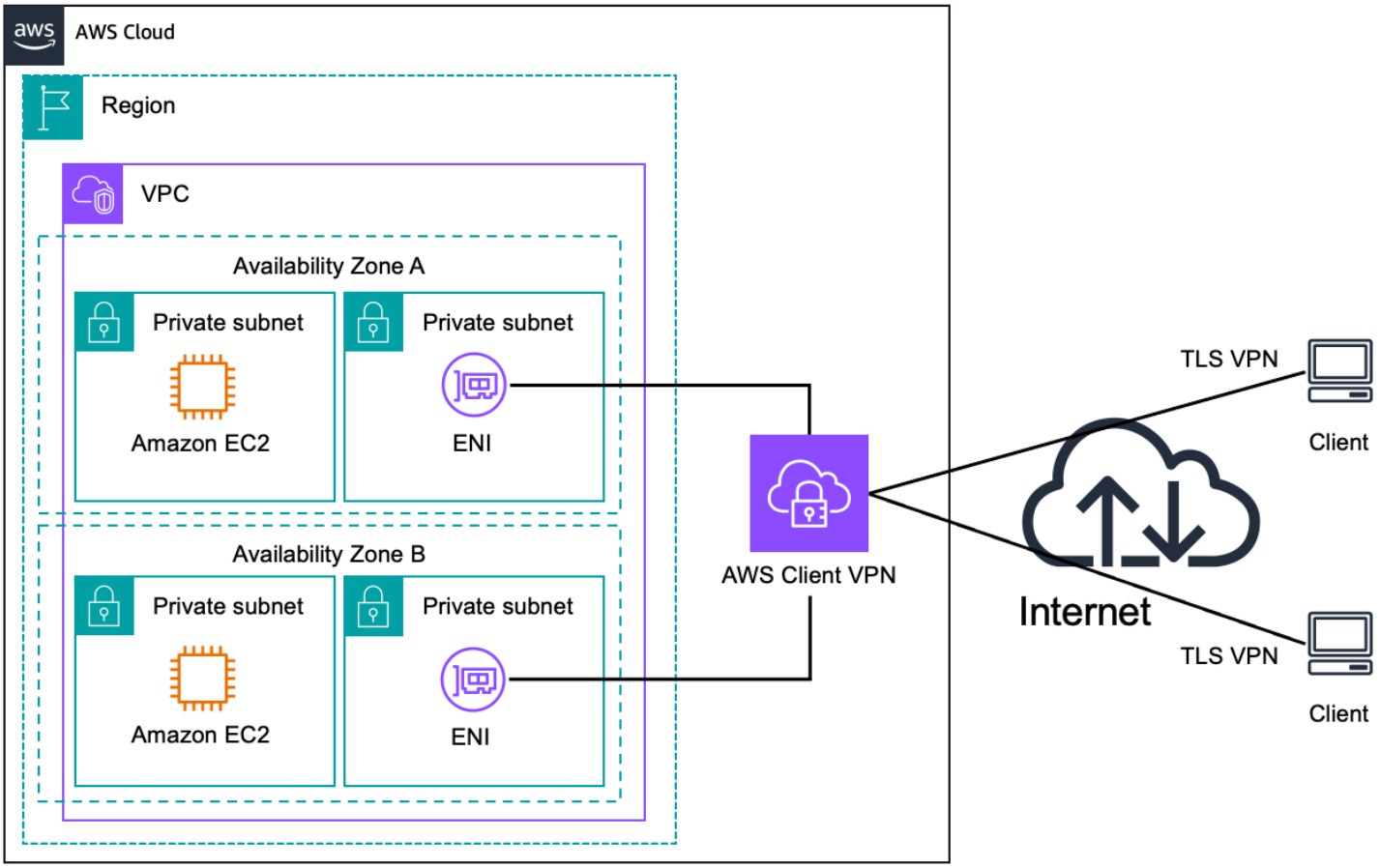
您可以結合這些模式與Network-to-Amazon VPC 連線選項連線選項Amazon VPC-to-Amazon VPC 連線選項，並建立跨越遠端網路和多個 VPCs的網路。

下表概述這些選項的優點和限制。

選項	使用案例	優點	限制
AWS Client VPN	Amazon VPC 和/或內部網路的 AWS 受管遠端存取解決方案	AWS 受管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 設備對 Amazon VPC 和/或內部網路的遠端存取解決方案	支援更廣泛的 VPN 廠商、產品和通訊協定 完全客戶受管的解決方案	您負責實作 HA 解決方案

AWS Client VPN

AWS Client VPN 是一種 AWS 受管的高可用性和可擴展性服務，可實現安全的軟體遠端存取。它提供在遠端用戶端和 Amazon VPCs 之間建立安全 TLS 連線的選項，以安全地透過網際網路存取 AWS 資源和內部部署，如下圖所示。



AWS Client VPN Remote Access

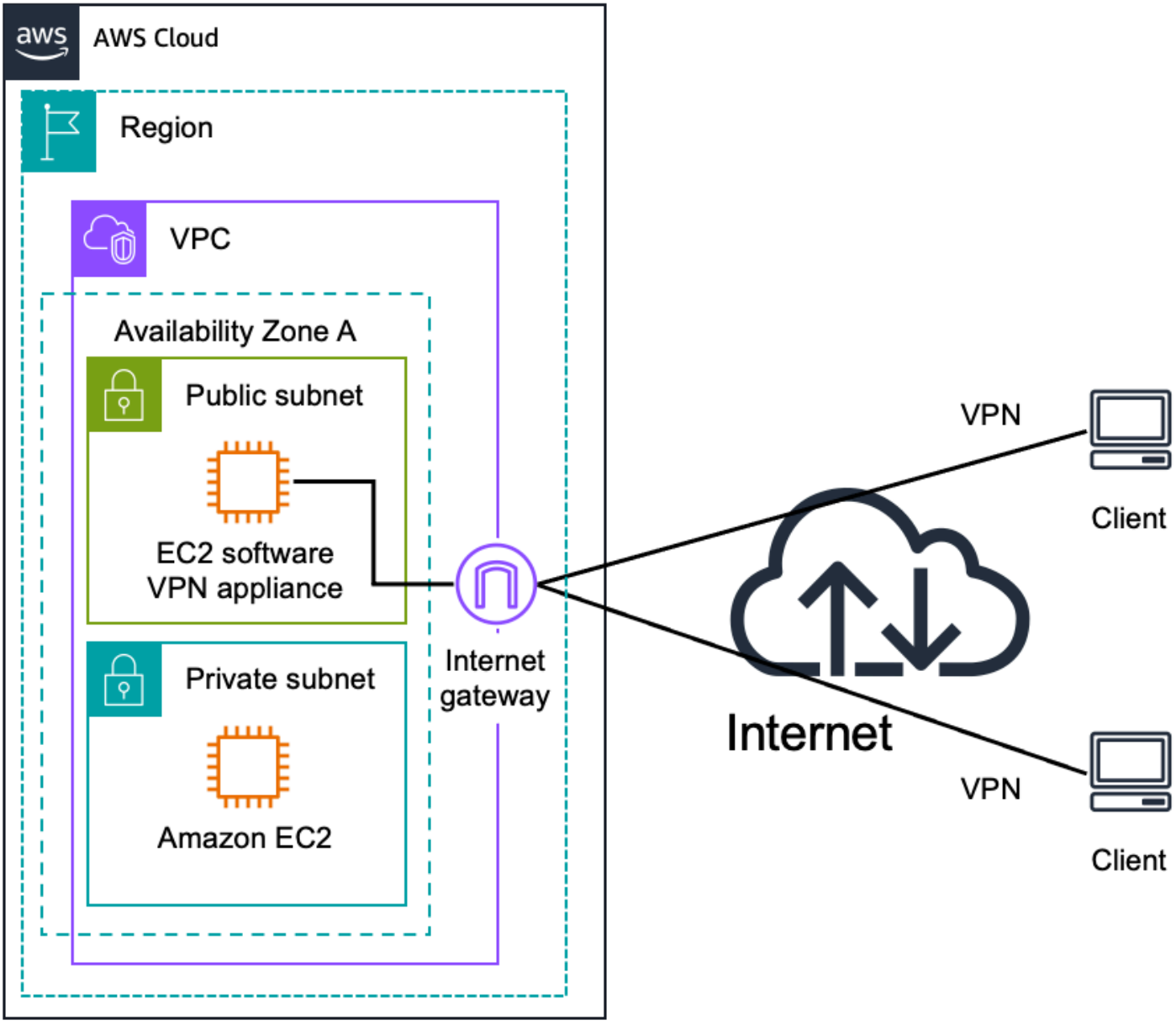
遠端用戶端可以是 AWS Client VPN for Desktop 或第三方 OpenVPN VPN 用戶端，透過 Active Directory 或交互憑證身分驗證進行身分驗證。

其他資源

- AWS Client VPN 管理員指南

軟體用戶端 VPN

您可以從由多個合作夥伴和開放原始碼社群組成的生態系統中進行選擇，這些社群已產生在 Amazon EC2 上執行的遠端存取解決方案。這些解決方案可為遠端存取 Amazon VPCs 的安全通訊協定提供極大的靈活性，以便透過網際網路安全地存取 AWS 資源和內部部署，如下圖所示。



Software Client VPN Remote Access

遠端存取解決方案的複雜性範圍、支援多個用戶端身分驗證選項（包括多重要素驗證），並且可以與 Amazon VPC 或遠端託管身分和存取管理解決方案（利用其中一個network-to-Amazon VPC 選項）整合，例如 Microsoft Active Directory 或其他 LDAP/多重要素身分驗證解決方案。

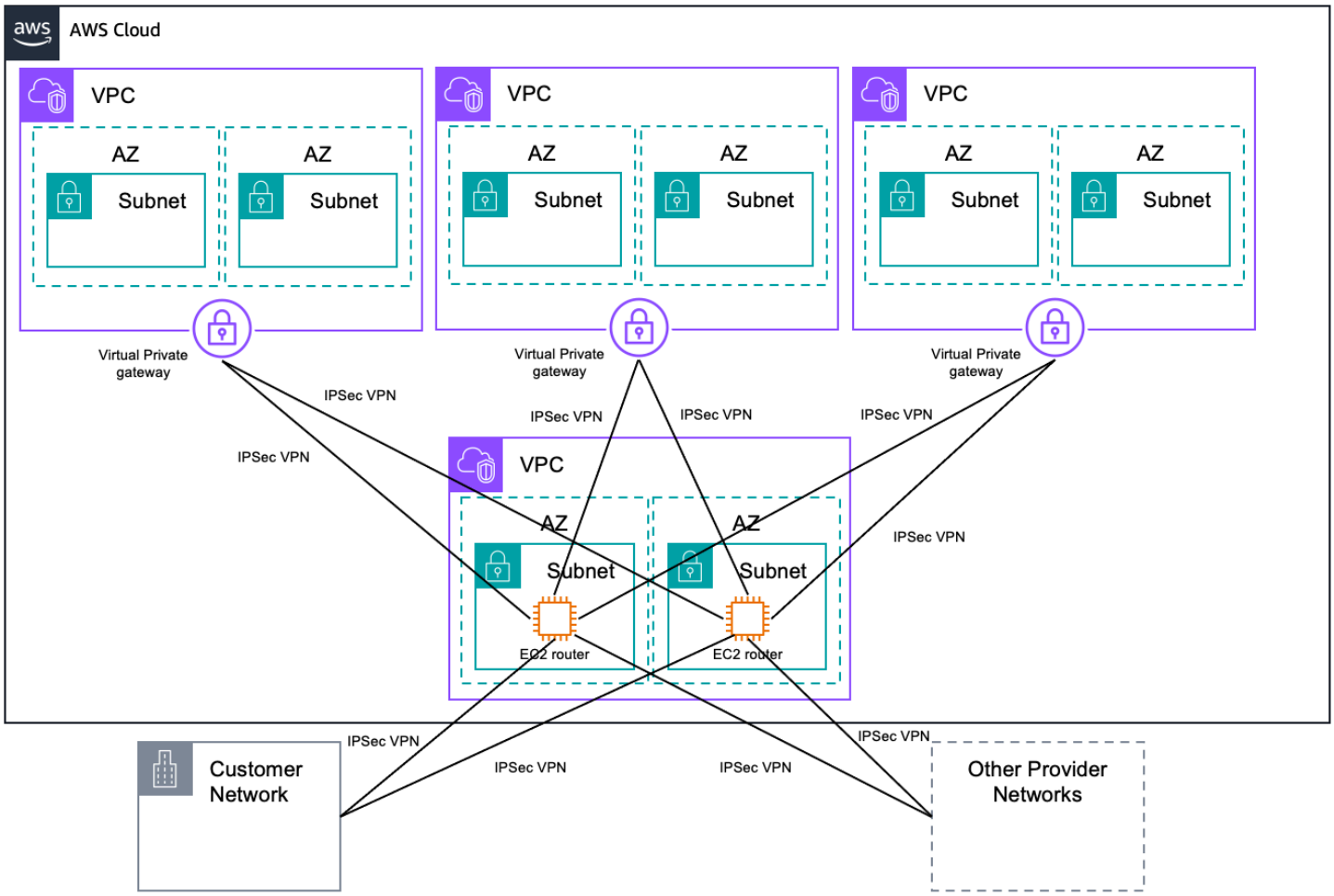
您負責管理遠端存取軟體，包括使用者管理、組態、修補程式和升級。當遠端存取伺服器在單一 Amazon EC2 執行個體上執行時，此設計會在網路設計中引入潛在的單點故障。如需其他資訊，請參閱 附錄 A：軟體 VPN 執行個體的高階 HA 架構。

其他資源

- 可從 取得的 VPN 設備 AWS Marketplace
- OpenVPN Access Server 快速入門指南

傳輸 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 是連接多個分散地理的 VPCs 和遠端網路的常見策略，以建立全球網路傳輸中心。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 VPCs和內部部署網路之間提供直接網路路由之外，此設計也可讓傳輸 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 用量。

其他資源

- AWS Transit Gateway
- 在 中用於 SD-WAN 和路由的 Cisco Catalyst 8000V AWS Marketplace

AWS 雲端 WAN

AWS Cloud WAN 是意圖驅動型受管廣域網路 (WAN)，由您定義的政策描述，該政策會統一您的資料中心、分支和 AWS 網路。雖然您可以透過跨區域互連多個傳輸閘道來建立自己的全球網路，但 Cloud WAN 會根據您的核心網路政策，提供專為建置和操作全球網路而設計的內建自動化、分割和組態管理功能。Cloud WAN 新增了自動化 VPC 連接、整合式效能監控和集中式組態等功能。

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

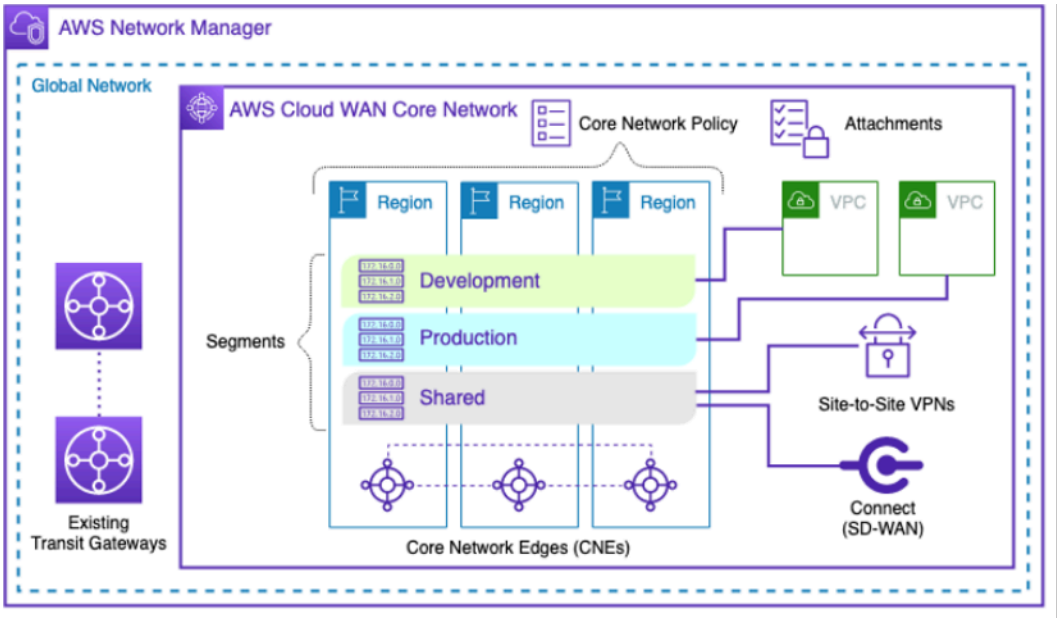
Cloud WAN 是在 AWS Network Manager 中管理，可讓您集中管理和視覺化 AWS 帳戶、區域和內部部署位置之間的 Cloud WAN 核心網路和 Transit Gateway 網路。Network Manager 為您提供數個儀表板視覺化，協助您檢視和監控全球網路的所有層面。某些儀表板包括：

- 世界地圖可精確定位您的網路資源，例如節點、裝置和附件。
- 使用 CloudWatch Events 追蹤 15 個月統計資料的監控，讓您更清楚網路效能。
- 將即時事件串流至事件儀表板的事件追蹤。
- 傳輸閘道網路和傳輸閘道的拓撲和邏輯圖。

Transit Gateway 和 Cloud WAN 允許 VPCs和內部部署位置之間的集中式連線。Transit Gateway 是區域網路連線中樞，最適合在幾個 AWS 區域中操作、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。Cloud WAN 最適合希望透過政策定義其全球網路，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） 繼承許多傳輸閘道特性，例如每個 VPC 連接的輸送量。
- Cloud WAN 同時支援 IPv4 和 IPv6。
- 對於具有許多變更的大型網路，請考慮建立單獨的開發和測試全域網路，以便驗證變更。



AWS Cloud WAN

其他資源

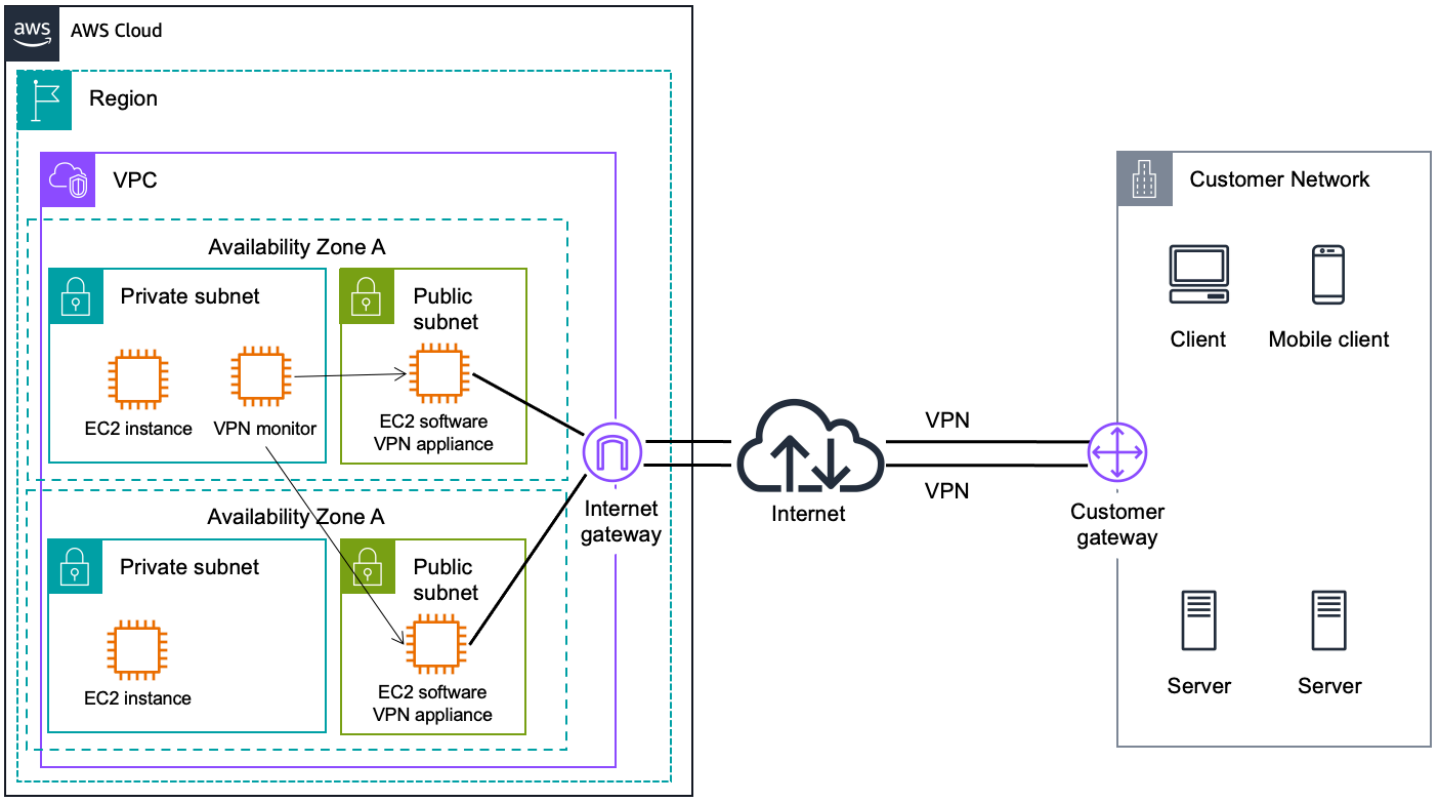
- AWS Cloud WAN 文件
- 部落格文章：AWS Cloud WAN 和 AWS Transit Gateway 遷移和互通性模式

結論

AWS 提供多種有效率且安全的連線選項，可協助您在整合遠端網路與 Amazon VPC 時充分利用 AWS。本白皮書提供的選項重點介紹客戶用來成功整合其遠端網路或多個 Amazon VPC 網路的數個連線選項和模式。您可以使用此處提供的資訊來判斷最適當的機制，以連接執行業務所需的基礎設施，無論其實際位置或託管位置為何。

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 連線需要設定和組態多個 VPN 執行個體和監控執行個體，以監控 VPN 連線的運作狀態。



高階軟體 VPN HA

我們建議您設定 VPC 路由表，透過相同可用區域中的個別 VPN 執行個體，將來自某個可用區域中所有子網路的流量引導至該區域，以同時利用所有 VPN 執行個體。然後，每個 VPN 執行個體會為共用相同可用區域的執行個體提供 VPN 連線。

VPN 監控

若要監控軟體型 VPN 設備，您可以建立 VPN 監控。VPN 監控是您需要執行 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，監視器需要停止、終止或重新啟動 VPN 執行個體，同時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，直到兩個連線再次運作為止。由於客戶需求不同，AWS 目前不提供設定此監控執行個體的規範性指引。不過，在 NAT 執行個體之間啟用 HA 的範例指令碼可以用作建立 Software VPN 執行個體 HA 解決方案的起點。我們建議您仔細考慮必要的商業邏輯，以便在 VPN 連線失敗時提供通知或嘗試自動修復網路連線。

此外，您可以使用 Amazon CloudWatch 指標來監控 AWS Managed VPN 通道，該指標會將 VPN 服務的資料點收集為可讀且近乎即時的指標。每個 VPN 連接都會收集各種通道指標並將其發佈至 Amazon CloudWatch。這些指標可讓您監控通道運作狀態、活動，並建立自動化動作。

貢獻者

本文件的貢獻者包括：

- Daniel Yu，AWS Enterprise Support 資深技術客戶經理
- Garvit Singh，AWS 解決方案架構解決方案建置器
- Steve Morad，AWS 解決方案架構解決方案建置者資深經理
- Sohaib Tahir，解決方案架構師，AWS 解決方案架構
- Fiona Armada，AWS 解決方案架構首席解決方案架構師
- Pablo Sánchez Carmona，聯網專家解決方案架構師，AWS 解決方案架構
- Tony Hawke，AWS Enterprise Support 資深聯網專家技術客戶經理

文件修訂

若要收到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	新增了 AWS Cloud WAN 和 Transit Gateway 連接連接選項、更新了圖表和資訊。	2023 年 4 月 5 日
白皮書已更新	新增了 AWS Transit Gateway 和 AWS Client VPN 選項、更新了圖表和資訊。	2020 年 6 月 6 日
次要更新	修正軟體 VPN 設備的參考的次要變更。	2020 年 5 月 20 日
白皮書已更新	更新整體資訊。專注於下列設計/功能：傳輸 VPC、Direct Connect 閘道和 AWS PrivateLink。	2018 年 1 月 1 日
初次出版	Amazon Virtual Private Cloud 連線選項已發佈。	2014 年 7 月 1 日

注意

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件：(a) 僅供參考，(b) 代表目前的 AWS 產品產品和實務，這些產品和實務如有變更，恕不另行通知，且 (c) 不會從 AWS 及其附屬公司、供應商或授權方建立任何承諾或保證。AWS 產品或服務「原樣」提供，不做任何明示或暗示的保證、表示或條件。AWS 對其客戶的責任與義務應由 AWS 協議管轄，本文並非 AWS 與其客戶之間的任何協議的一部分，也並非上述協議的修改。

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。