AWS 白皮书

建立可擴充且安全的多重VPC AWS 網路基礎架構

建立可擴充且安全的多重VPC AWS 網路基礎架構: AWS 白皮书

Table of Contents

建立可擴充且安全的多重 VPC AWS 網路基礎

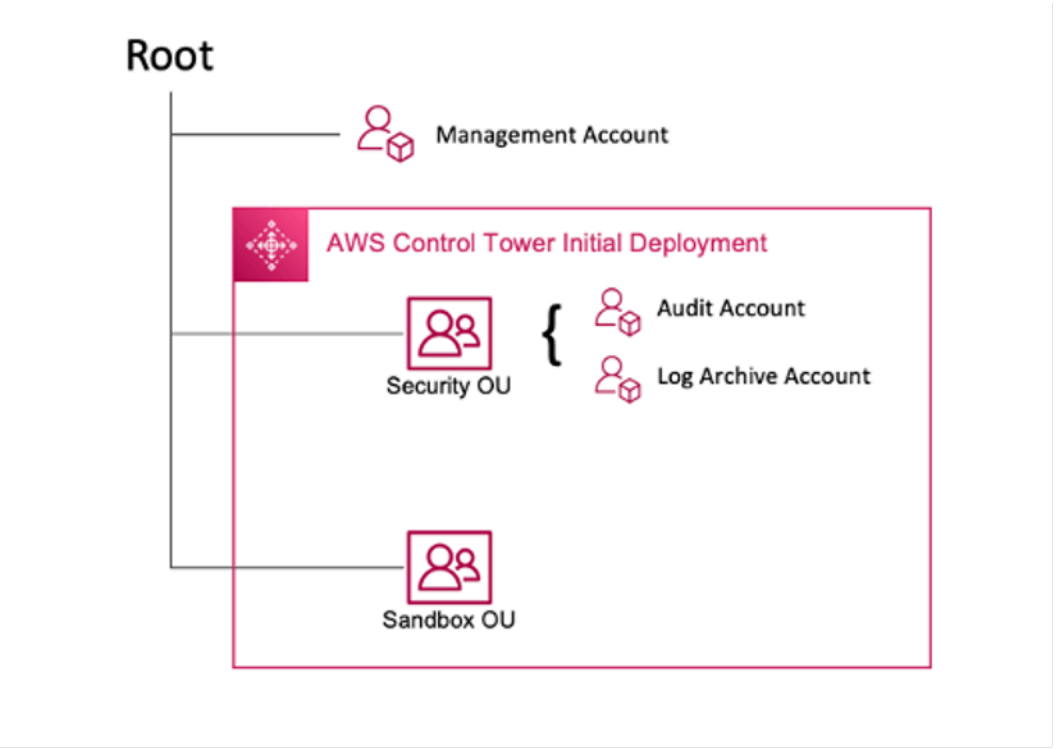
出版日期：二零二四年四月十七日（ ）文件歷史紀錄

Amazon Web Services (AWS) 客戶通常依賴數百個帳戶和虛擬私有雲 (VPC) 來區隔工作負載並擴大其足跡。此級別的規模通常會在資源共用、VPC 間連線以及現場部署設施到 VPC 連線方面帶來挑戰。

本白皮書說明使用 Amazon 虛擬私有雲 (Amazon VPC)、、、AWS Transit Gateway閘道 Load Balancer 和 Amazon R ou te 53 等 AWS 服務在大型網路中建立可擴展且安全網路架構的最佳實務。AWS PrivateLinkAWS Direct ConnectAWS Network Firewall它展示了管理不斷增長的基礎架構的解決方案 — 確保可擴展性、高可用性和安全性，同時保持較低的間接成本。

簡介

AWS 客戶首先在一個帳戶中構建資源，該 AWS 帳戶代表了一個管理界限，該界限分割權限，成本和服務。然而，隨著客戶組織的成長，需要更大的服務細分來監控成本、控制存取，以及提供更輕鬆的環境管理。多帳戶解決方案可針對組織內的 IT 服務和使用者提供特定帳戶，藉此解決這些問題。 AWS 提供數種工具來管理和設定此基礎結構，包括 AWS Control Tower.



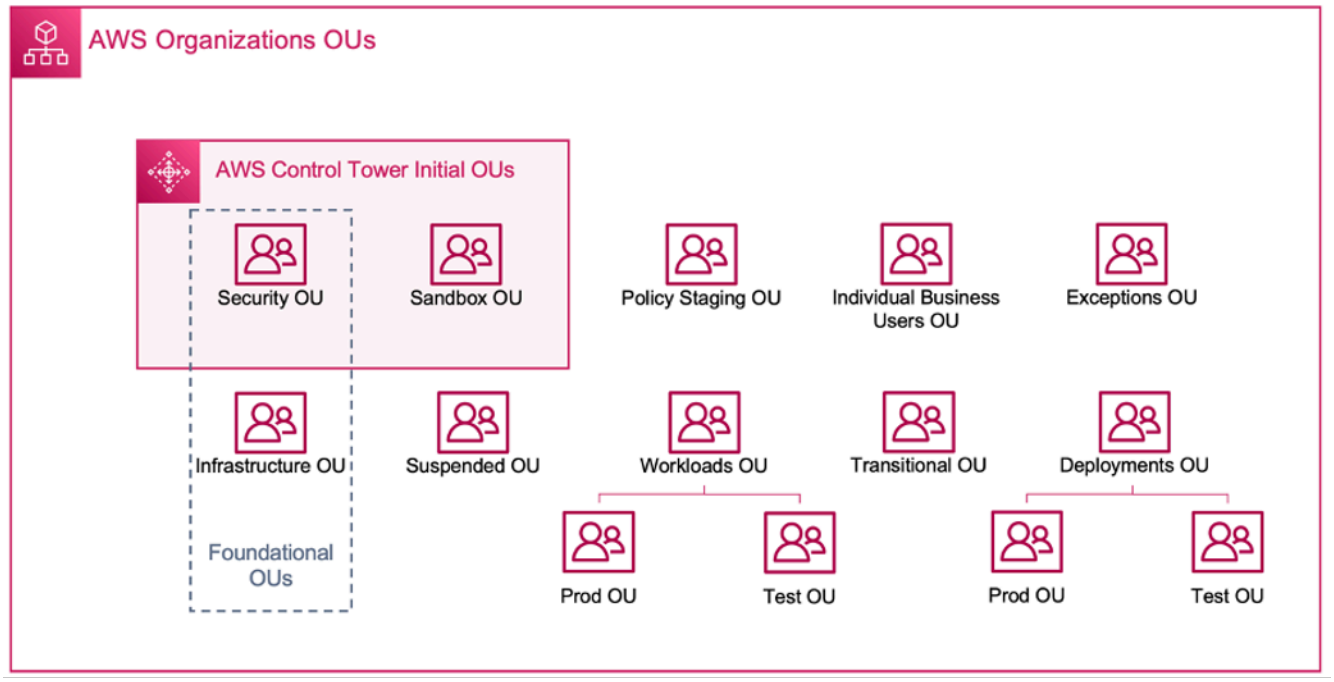
AWS Control Tower 初始部署

當您使用設定多帳戶環境時 AWS Control Tower，它會建立兩個組織單位 (OU)：

- 安全性 OU — 在此 OU 中， AWS Control Tower 建立兩個帳戶：
- 日誌存檔
- 稽核 (此帳戶對應於先前在指南中討論的安全性工具帳戶。)
- 沙箱 OU — 此 OU 是在其中建立之帳戶的預設目的地 AWS Control Tower。它包含帳戶，您的建築商可以在其中探索和試驗 AWS 服務以及其他工具和服務，這取決於您的團隊可接受的使用政策。

AWS Control Tower 可讓您建立、註冊和管理其他 OU，以擴充初始環境以實作指引。

下圖顯示最初部署的 OU AWS Control Tower。您可以擴充 AWS 環境以實作圖表中包含的任何建議 OU，以符合您的需求。



AWS 組織 OU

如需使用多帳戶環境的詳細資訊 AWS Control Tower，請參閱使用多帳戶組織 AWS 環境白皮書中的附錄 E。

> **Note**
>
> 在本白皮書中，「Control Tower」是您部署工作負載的可擴充、安全且高效能的多帳戶/多 VPC 人雲端設定的廣泛術語。此設置可以使用不同的工具來構建。您可以在使用多帳戶組織 AWS 環境白皮書中找到有關多帳戶雲端基礎的最佳實務、設計原則和優點的詳細資訊。

大多數客戶從幾個 VPC 開始部署他們的基礎架構。客戶建立的 VPC 數量通常與其帳戶、使用者和階段環境 (生產、開發、測試等) 的數量有關。隨著雲端使用量的增加，客戶與之互動的使用者、業務單位、應用程式和區域數量也會增加，從而導致建立新的 VPC。

隨著 VPC 數量的增加，跨 VPC 管理對於客戶雲端網路的運作變得至關重要。本白皮書涵蓋跨 VPC 和混合式連線三個特定領域的最佳實務：

- 網路連線 — 大規模互連 VPC 與內部部署網路。
- 網路安全性 — 建立集中式出口點以存取網際網路和端點，例如網路位址轉譯 (NAT) 閘道、VPC 端點和閘道負載平衡器。AWS PrivateLinkAWS Network Firewall
- DNS 管理 — 解析控制中心內的 DNS 和混合式 DNS。

IP 位址規劃與管理

為了構建可擴展的多帳戶多 VPC 網絡設計，IP 地址規劃和管理至關重要。良好的 IP 定址方案需要考慮您目前和 future 的網路需求。您的 IP 位址配置 IP 需要涵蓋內部部署工作負載、雲端工作負載，並且還應該允許 future 的擴充 (例如 AWS 區域，新增業務單位，以及併購)。這也應該可以防止您的團隊無意中建立重疊的 IP CIDR。如果需要重疊 IP CIDR，例如隔離或中斷連接的工作負載，則此決策必須有意識，並應考慮對路由、安全性和成本的影響。您可能還需要考慮為此類例外建立必要的核准處理。良好的 IP 位址配置也有助於簡化您的網路設計和路由配置。

關鍵考量事項：

- 預先規劃您的 IP 位址配置 (包括公有和私有 IP)，並選取 IP 位址管理工具，以配置、管理及追蹤所有工作負載的 IP 位址使用情況。
- 使用階層式和摘要的 IP 位址配置。
- 根據環境、組織或業務單位 AWS 區域，規劃一致的 IP 指派。
- 為內部部署和雲端網路指定不同的 IP CIDR (IPv4 和 IPv6)。
- 主動防止和追蹤 IP CIDR 重疊。
- 適當調整 IP CIDR 的大小，以實現擴展和 future 的成長。
- 為您的工作負載啟用 IPv6 或雙堆疊相容性，以減少 IP 衝突並解決 IPv4 空間耗盡的問題。

您可以使用 Amazon VPC IP 位址管理員 (IPAM) 來簡化工作負載的公有和私有 IP 地址的規劃、追蹤和監控。 AWS IPAM 允許您組織，分配，監視和共享多個 AWS 區域 和之間的 IP 地址空間。 AWS 帳戶它還有助於使用特定商業規則將 CIDR 自動分配給 VPC。

如需部落格文章，請參閱 Amazon VPC IP 地址管理員最佳實務、使用 Amazon VPC IP 地址管理員跨 VPC 和區域管理 IP 集區，以及如何使用 IPAM 管理跨 VPC 和 IP 地址管理 IP 集區的 AWS Control Tower部落格文章。 AWS 區域 AWS Control Tower

你是否 Well-Architected？

AWS Well-Architected 的架構可協助您瞭解在雲端中建置系統時所做決策的優缺點。Framework 的六大支柱可讓您學習如何設計和操作可靠、安全、高效、符合成本效益且可持續發展的系統的架構最佳實務。使用中免費提供的 AWS Well-Architected ToolAWS Management Console，您可以針對每個支柱回答一組問題，根據這些最佳實務來檢閱工作負載。

如需雲端架構的更多專家指導和最佳實務 (參考架構部署、圖表和白皮書)，請參閱架構中心。AWS

VPC 到虛擬私人 VPC 的連接

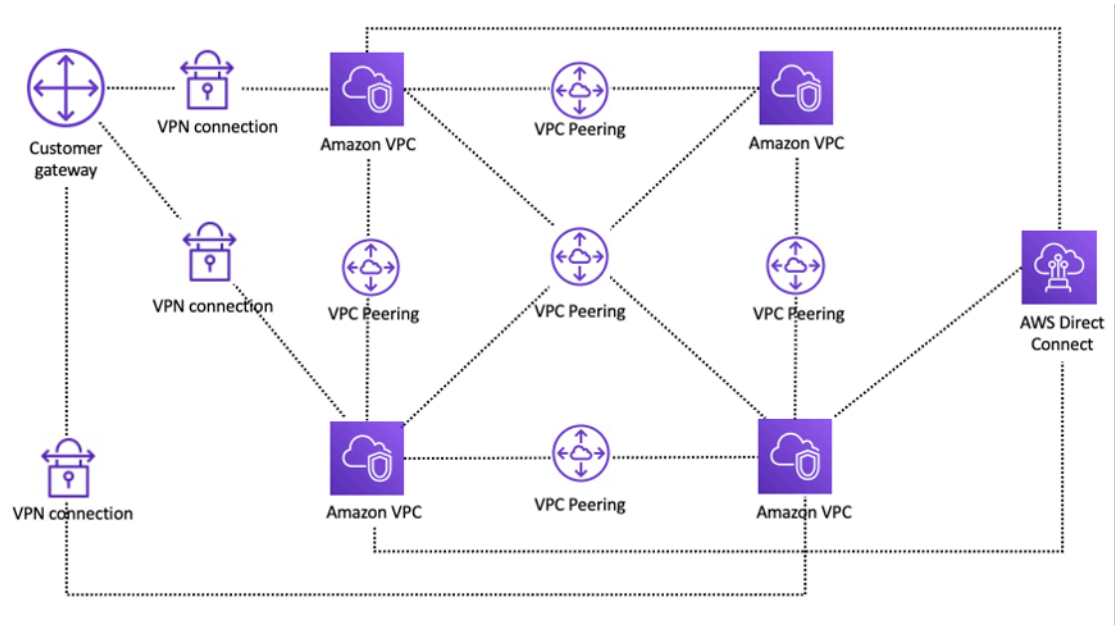
客戶可以使用兩種不同的 VPC 連線模式來設定多虛擬私人雲端環境：多對多，或集線器和支點。在此 many-to-many 方法中，每個 VPC 之間的流量會在每個 VPC 之間個別管理。在 hub-and-spoke 模型中，所有 VPC 間流量都會流經中央資源，該資源會根據已建立的規則路由流量。

VPC 對等互連

連接兩個 VPC 的第一種方式是使用 VPC 對等。在此設定中，連線會啟用 VPC 之間的完整雙向連線。此對等連線可用來路由 VPC 之間的流量。 不同帳戶和 AWS 區域中的 VPC 也可以對等。透過 VPC 對等連線保持在可用區域內的所有資料傳輸都是免費的。透過跨可用區域的 VPC 對等連線進行的所有資料傳輸，均以標準區域內資料傳輸費率計費。如果 VPC 跨區域對等，則會收取標準區域間資料傳輸費用。

VPC 對等互 point-to-point 連是連線能力，不支援傳遞路由。例如，如果您在 VPC A 和 VPC B 之間以及 VPC A 和 VPC C 之間有 VPC 對等連線，則 VPC B 中的執行個體無法透過 VPC A 傳輸到達 VPC C。若要在 VPC B 和 VPC C 之間路由封包，您必須建立直接 VPC 對等連線。

在規模上，當您有數十或數百個 VPC 時，將它們與對等互連接可能會產生數百或數千個對等連接的網格。大量連線可能難以管理和擴充。例如，如果您有 100 個 VPC，並且想要在它們之間設定完整網格對等，則需要 4,950 個對等連線 [n(n-1)/2]，其中n是 VPC 的總數。每個 VPC 的作用中對等連線上限上限為 125 個。



使用 VPC 對等互連進行網路設定

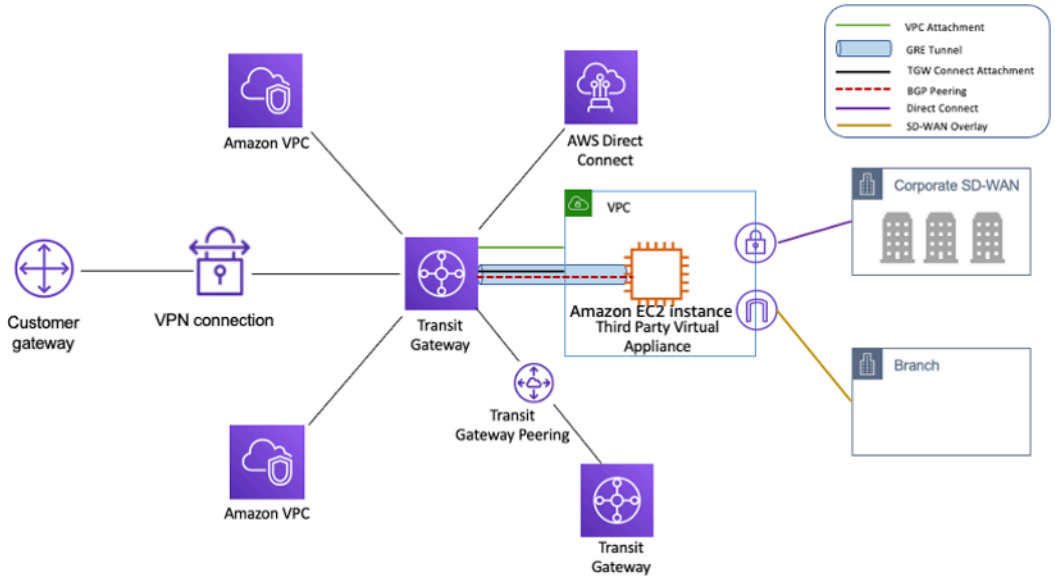
如果您使用 VPC 對等互連，則必須對每個 VPC 進行內部部署連線 (VPN 和/或直接連線)。VPC 中的資源無法使用對等 VPC 的混合式連線存取內部部署，如上圖所示。

當一個 VPC 中的資源必須與另一個 VPC 中的資源通訊、兩個 VPC 的環境都受到控制和保護，且要連線的 VPC 數目少於 10 (以允許個別管理每個連線) 時，最適合使用 VPC 對等互連。與 VPC 間的其他選項相比，VPC 對等互連可提供最低的整體成本和最高的彙總效能。

AWS Transit Gateway

AWS Transit Gateway提供中樞和支點設計，可將 VPC 和內部部署網路連接為完全受控的服務，而無需佈建第三方虛擬應用裝置。不需要 VPN 覆蓋，並可 AWS 管理高可用性和可擴展性。

Transit Gateway 可讓客戶連接數千個 VPC。您可以將所有混合式連線 (VPN 和 Direct Connect 連線) 連接到單一閘道，在單一位置合併和控制組織的整個 AWS 路由設定 (請參閱下圖)。傳 Transit Gateway 控制如何使用路由表在所有已連接的分支網路之間路由流量。此 hub-and-spoke 模型可簡化管理並降低營運成本，因為 VPC 只會連線到 Transit Gateway 執行個體來存取連線的網路。



集線器和輻條設計 AWS Transit Gateway

Transit Gateway 是一種區域資源，可以在同 AWS 區域一個資源中連接數千個 VPC。您可以透過單一「直接連線」連線來 Connect 多個閘道，以進行混合式連線 通常，您只能使用一個 Transit Gateway 執行個體來連接指定區域中的所有 VPC 執行個體，並使用 Transit Gateway 路由表將它們隔離到需要的地方。請注意，您不需要額外的傳輸閘道即可獲得高可用性，因為傳輸閘道在設計上具有高度可用性；如需備援，請在每個區域中使用單一閘道。不過，建立多個閘道的有效案例可以限制設定錯誤的爆炸半徑、隔離控制平面作業和管理。 ease-of-use

使用 Transit Gateway 對等互連，客戶可以在相同或多個區域內對等其 Transit Gateway 執行個體，並在它們之間路由流量。它使用與 VPC 對等互連相同的基礎結構，因此經過加密。如需詳細資訊，請參閱使用 AWS Transit Gateway 區域間對等建立全球網路和 AWS Transit Gateway 現在支援區域內對等互連。

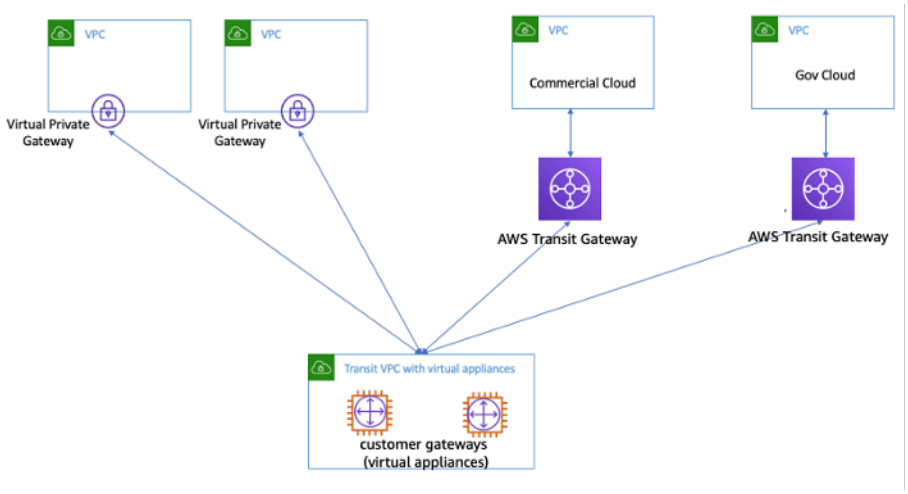
將組織的 Transit Gateway 執行個體置於其網路服務帳戶中。這可讓管理網路服務帳戶的網路工程師集中管理。使用 AWS Resource Access Manager (RAM) 共用 Transit Gateway 執行個體，以便在同一區域內的 AWS 組織中跨多個帳戶連接 VPC。AWS RAM 可讓您輕鬆安全地與 AWS AWS 組織內的任何 AWS 帳戶人共用資源。如需詳細資訊，請參閱中央帳戶部落格文章中的傳輸閘道自動化 AWS Transit Gateway 附件。

Transit Gateway 還允許您在 SD-WAN 基礎架構之間建立 Connect，並 AWS 使用 Transit Gateway 連接。使用具有邊界閘道通訊協定 (BGP) 的傳輸閘道 Connect 附件以進行動態路由，使用一般路由封裝 (GRE) 通道通訊協定以達到高效能，每個 Connect 附件最多可提供 20 Gbps 的總頻寬 (每個 Connect 附件最多可提供四個傳 Transit Gateway 道 Connect 對等)。透過使用傳 Transit Gateway Connect，您可以透過 VPC 附件或附件，將內部部署 SD-WAN 基礎結構或 SD-WAN 應用裝置整合為基礎傳輸層。AWS Direct Connect 有關參考架構和詳細配置，請參閱使用 AWS Transit Gateway Connect 簡化 SD-WAN 連接。

交通 VPC 解決方案

傳輸 VPC 可以透過與 VPC 對等不同的方式在 VPC 之間建立連線，方法是針對 VPC 間連線引入集線器和支點設計。在傳輸虛擬私人雲端網路中，一個中央虛擬私人雲端 (集線器 VPC) 透過 VPN 連線，通常透過 IPsec 利用 BGP 連線與其他所有 VPC (支點虛擬私人雲端) 連線。中央 VPC 包含 Amazon 彈性運算雲端 (Amazon EC2) 執行個體，該執行軟體設備可使用 VPN 覆蓋將傳入流量路由到目的地。傳輸 VPC 對等具有下列優點：

- 使用覆蓋 VPN 網路啟用傳遞路由，允許集線器和支點設計。
- 在集線器傳輸 VPC 中的 EC2 執行個體上使用第三方廠商軟體時，可以使用圍繞進階安全性 (第 7 層防火牆/入侵防禦系統 (IPS)/入侵偵測系統 (IDS)) 的廠商功能。如果客戶在內部部署使用相同的軟體，他們將受益於統一的操作/監控體驗。
- 傳輸 VPC 架構可提供某些使用案例所需的連線能力。例如，您可以將 AWS GovCloud 執行個體和商業區域 VPC 或 Transit Gateway 執行個體連接到傳輸 VPC，並啟用兩個區域之間的 VPC 間連線。考慮此選項時，請評估您的安全性和合規性需求。為了提高安全性，您可以使用本白皮書稍後所述的設計模式來部署集中式檢查模型。



使用虛擬應用裝置的傳輸 VPC

Transit VPC 面臨各自的挑戰，例如根據執行個體大小/系列在 EC2 上執行第三方廠商虛擬設備的成本較高、每個 VPN 連線的輸送量有限 (每個 VPN 通道最高 1.25 Gbps)，以及額外的設定、管理和彈性開銷 (客戶負責管理執行第三方廠商虛擬設備的 EC2 執行個體的 HA 和 EC2 執行個體備援)。

VPC 對等互連與傳輸 VPC 與 Transit Gateway

表 1 — 連線能力比較

條件	VPC 對等互連	交通 VPC	轉換閘道	PrivateLink	雲端廣域網	VPC Lattice
範圍	區域/全球	區域性	區域性	區域性	全球服務	區域性
架構	全網格	基於 VPN 的 hub-and-spoke	以附件為基礎 hub-and-spoke	提供者或消費者模型	以附件為基礎，多區域	應用程式對應用連線
擴展	125 個主動同行器/虛VPC	取決於虛擬路由器/EC2	每個區域 5000 個附件	沒有限制	每個核心網路 5000 個附件	每項服務 500 個 VPC 關聯
區隔	安全群組	客戶管理	Transit Gateway 路由表	無分割	客群	服務和服務網絡政策

條件	VPC 對等互連	交通 VPC	轉換閘道	PrivateLink	雲端廣域網	VPC Lattice
Latency (延遲)	最低	額外的，由於 VPN 加密開銷	其他 Transit Gateway 躍點	流量停留在 AWS 骨幹上，客戶應進行測試	使用與交通網關相同的數據 Transit Gateway	流量停留在 AWS 骨幹上，客戶應進行測試
頻寬限制	每個執行個體限制，無彙總限制	依據大小/系列而定的 EC2 執行個體頻寬限制	最高可達 100 Gbps (爆發)/附件	每個可用區域 10 Gbps，可自動擴充高達 100 Gbps	最高可達 100 Gbps (爆發)/附件	每個可用區域 10 Gbps
Visibility	VPC 流量日誌	VPC 流程記錄和 CloudWatch 指標	Transit Gateway 網路管理員、VPC 流程記錄、CloudWatch 指標	CloudWatch 度量	網路管理員、VPC 流程記錄、CloudWatch 指標	CloudWatch 存取記錄
安全群組 交互參考	支援	不支援	不支援	不支援	不支援	不適用
IPv6 支援	支援	取決於虛擬應用裝置	支援	支援	支援	支援

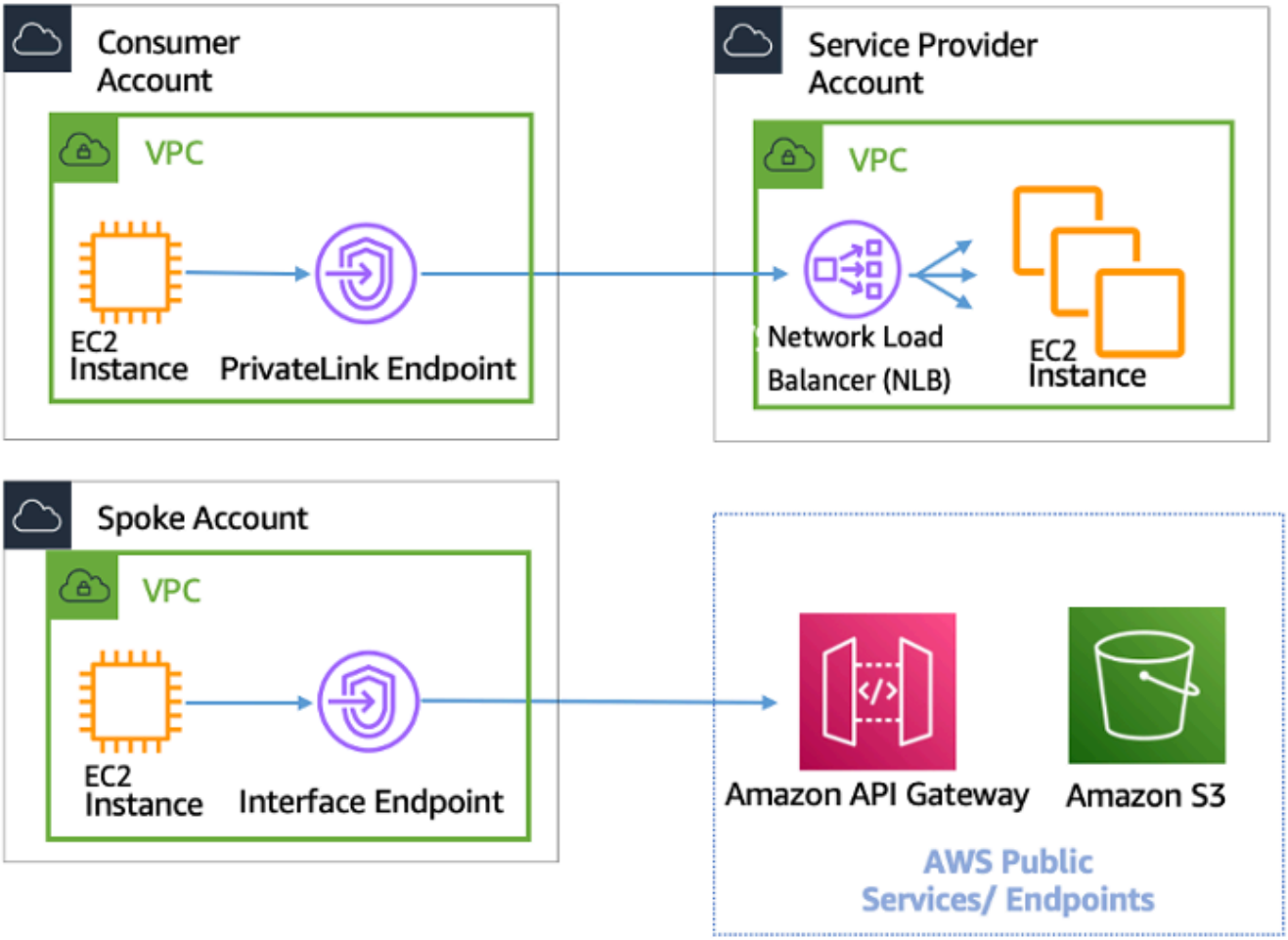
AWS PrivateLink

AWS PrivateLink在 VPC、AWS 服務和現場部署網路之間提供私有連線，而不會將流量暴露到公用網際網路。由 VPC 端點提供支援的介面 AWS PrivateLink，可讓您輕鬆地跨不同帳戶 AWS 和 VPC 連線到其他服務，大幅簡化您的網路架構。這可讓想要將位於某 AWS 區域 個 VPC (服務提供者) 中的服

務/應用程式公開給其他 VPC (消費者) 的客戶，以便只有取用者 VPC 啟動與服務提供者 VPC 連線的方式。其中一個例子是您的私有應用程序訪問服務提供商 API 的能力。

若要使用 AWS PrivateLink，請在 VPC 中為您的應用程式建立 Network Load Balancer，並建立指向該負載平衡器的 VPC 端點服務組態。然後，服務取用者會為您的服務建立介面端點。這會在消費者子網路中建立一個 elastic network interface (ENI)，其私有 IP 位址可做為目的地服務之流量的入口點。消費者和服務不需要位於相同的 VPC 中。如果 VPC 不同，取用者和服務提供者 VPC 可能具有重疊的 IP 位址範圍。除了建立介面 VPC 端點以存取其他 VPC 中的服務之外，您還可以建立介面 VPC 端點，透過以下方式私有存取支援的 AWS 服務 AWS PrivateLink，如下圖所示。

使用 Application Load Balancer (ALB) 做為 NLB 的目標，您現在可以將 ALB 進階路由功能與. AWS PrivateLink如需參考架構和詳細設定，請參閱 Network Load Balancer 的應用程式負載平衡器類型目標群組。



AWS PrivateLink 用於連線到其他 VPC 和 AWS 服務

Transit Gateway、VPC 對等互連之間的選擇取決 AWS PrivateLink 於連線能力。

- AWS PrivateLink— AWS PrivateLink 當您設定用戶端/伺服器時，要允許一或多個取用者 VPC 單向存取特定服務或服務提供者 VPC 或特定服務中的一組執行個體時使用。 AWS 只有在取用者 VPC 中具有存取權的用戶端可以起始與服務提供者 VPC 或 AWS 服務中的服務連線。當兩個 VPC 中的用戶端和伺服器具有重疊的 IP 位址時，這也是一個不錯的選擇，因為在 AWS PrivateLink 用戶端 VPC 內以確保與服務提供者沒有 IP 衝突的方式使用 ENI。您可以透過 VPC 對等互連、VPN、Transit Gateway、雲 AWS PrivateLink 端 WAN 和. AWS Direct Connect
- VPC 對等互連和 Transit Gateway — 當您想要在 VPC 之間啟用第 3 層 IP 連線時，請使用 VPC 對等互連和 Transit Gateway 道。

  您的架構將包含這些技術的混合，以滿足不同的使用案例。所有這些服務都可以相互組合並運行。例如， AWS PrivateLink 處理 API 樣式的用戶端與伺服器連線、用於處理直接連線需求的 VPC 對等互連需求 (在區域或區域間連線可能仍需要放置群組)，以及 Transit Gateway 可簡化大規模 VPC 的連線，以及混合式連線的邊緣整合。

VPC 共享

如果群組之間的網路隔離不需要由 VPC 擁有者嚴格管理，但帳戶層級的使用者和權限必須是，則共用 VPC 非常有用。使用共用 VPC 時，多個 AWS 帳戶會在共用的集中管理 Amazon VPC 中建立其應用程式資源 (例如 Amazon EC2 執行個體)。在此模型中，擁有 VPC (擁有者) 的帳戶與其他帳戶 (參與者) 共用一或多個子網路。共用子網路後，參與者可以檢視、建立、修改及刪除與其共用之子網路中的應用程式資源。參與者無法檢視、修改或刪除屬於其他參與者或 VPC 擁有者的資源。共用 VPC 中資源之間的安全性是使用安全性群組、網路存取控制清單 (NACL) 或子網路之間的防火牆來管理。

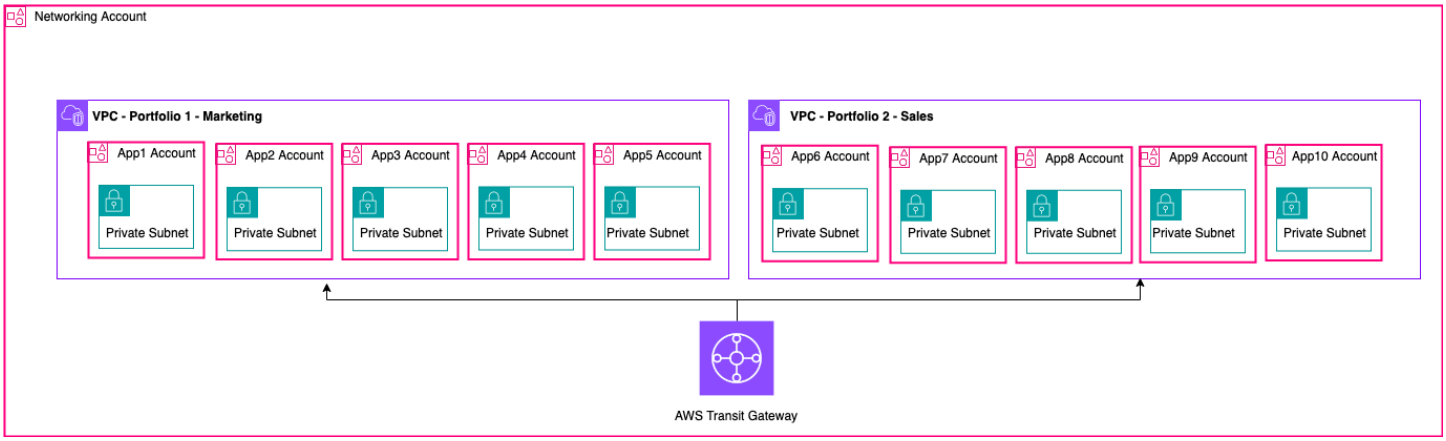
VPC 共享的好處：

- 簡化的設計 — 虛擬私人雲端間的連線沒有複雜性
- 減少受管理的 VPC
- 網絡團隊和應用程序所有者之間的職責劃分
- 更好的 IPv4 位址使用率
- 降低成本 — 屬於相同可用區域內不同帳戶的執行個體之間無需支付資料傳輸費用

> **Note**
>
> 當您與多個帳戶共用子網路時，您的參與者應該有一定程度的合作，因為他們共用 IP 空間和網路資源。如有必要，您可以選擇為每個參與者帳戶共用不同的子網路。每個參與者一個子網路可讓網路 ACL 除了安全群組之外提供網路隔離。

大多數客戶架構將包含多個 VPC，其中許多 VPC 將與兩個以上的帳戶共用。Transit Gateway 和 VPC 對等可用於連接共用 VPC。例如，假設您有 10 個應用程式。每個應用程式都需要自己的 AWS 帳戶。這些應用程式可分為兩個應用程式組合 (相同產品組合中的應用程式具有類似的網路需求，「行銷」中的應用程式 1-5，「銷售」中的應用程式 6-10)。

每個應用程式產品組合可以有一個 VPC (總共兩個 VPC)，而且 VPC 會與該產品組合中的不同應用程式擁有者帳戶共用。應用程式擁有者將應用程式部署到其各自的共用 VPC 中 (在這種情況下，在不同的子網路中，使用 NACL 進行網路路由分割和隔離)。這兩個共用 VPC 透過 Transit Gateway 進行連接。透過此設定，您可以從必須將 10 個 VPC 連線到只有兩個 VPC，如下圖所示。

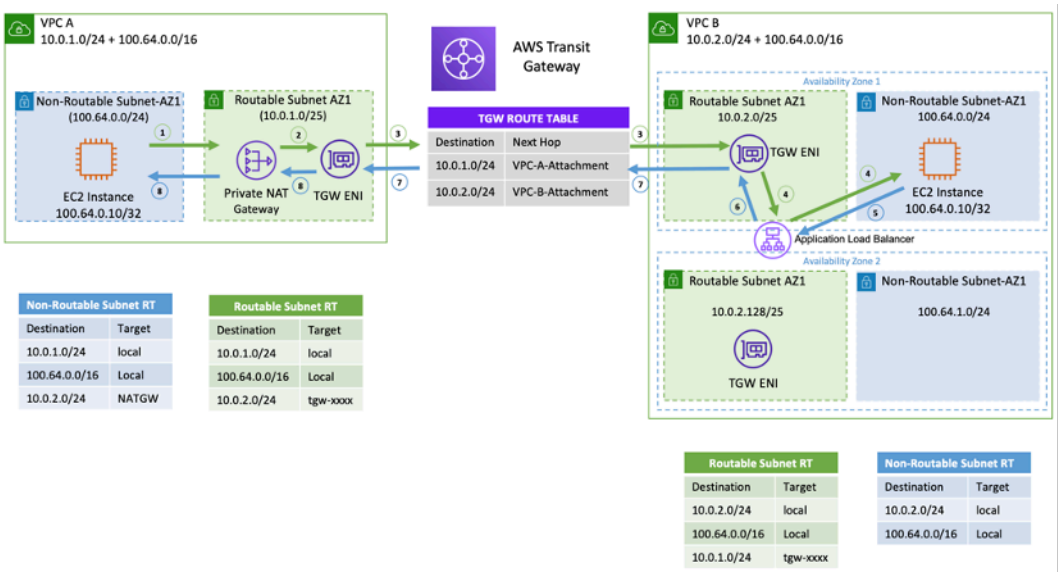


設定範例 — 共用 VPC

> **Note**
>
> VPC 共用參與者無法在共用子網路中建立所有 AWS 資源。如需詳細資訊，請參閱 VPC 共用說明文件中的限制一節。
>
> 如需 VPC 共用的主要考量事項和最佳做法的詳細資訊，請參閱 VPC 共用：重要考量事項和最佳做法部落格文章。

私有 NAT 閘道

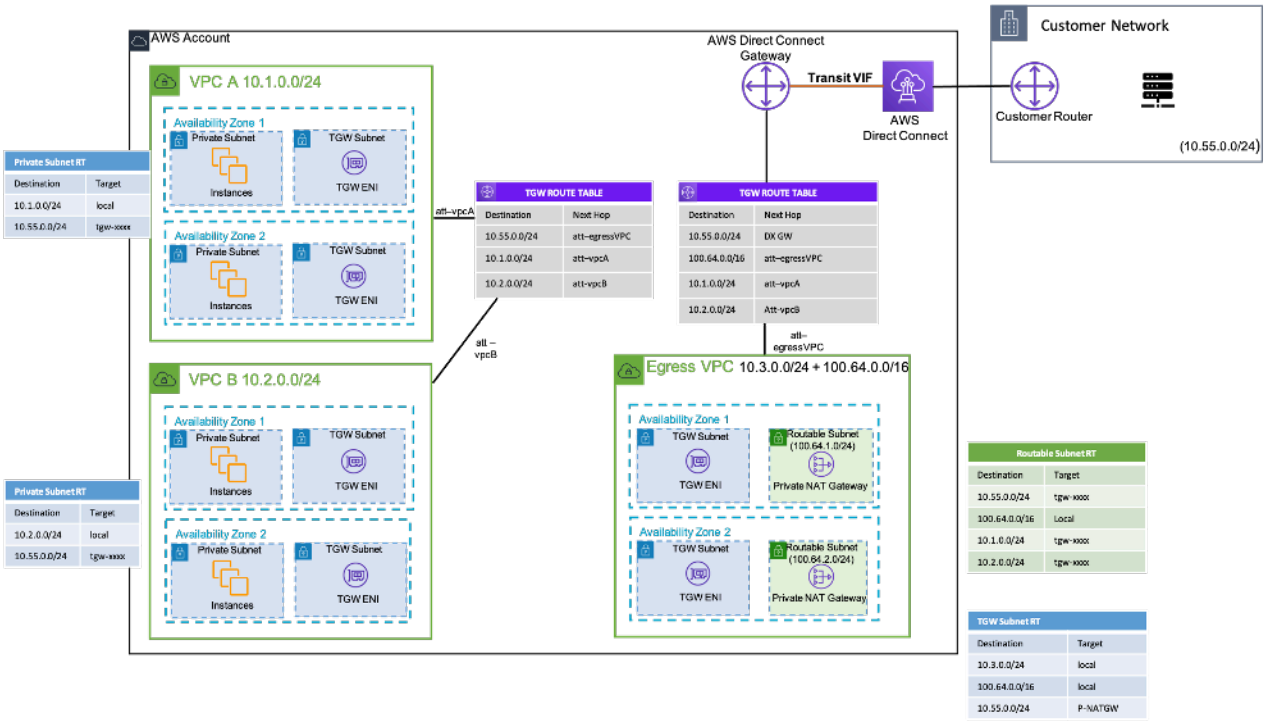
團隊通常獨立工作，他們可能會為項目創建一個新的 VPC，該項目可能具有重疊的無類別域間路由（CIDR）塊。為了進行整合，他們可能想要啟用具有重疊 CIDR 的網路之間的通訊，這是無法透過 VPC 對等互連和傳 Transit Gateway 等功能來實現的。私有 NAT 閘道可協助解決此使用案例。私有 NAT 閘道會使用唯一的私有 IP 位址來為重疊的來源 IP 位址執行來源 NAT，ELB 會針對重疊的目的地 IP 位址執行目的地 NAT。您可以使用傳輸閘道或虛擬私有閘道，將流量從私人 NAT Transit Gateway 由到其他 VPC 或內部部署網路。



設定範例 — 私人 NAT 閘道

上述條件顯示 VPC A 和 B 中兩個不可路由的子網路 (重疊的 CIDR、100.64.0.0/16) 子網路。若要在它們之間建立連線，您可以分別將次要非重疊/路由的 CIDR (可路由子網路和) 新增至 VPC A 和 B。10.0.1.0/24 10.0.2.0/24可路由的 CIDR 應由負責 IP 分配的網路管理小組分配。私有 NAT 閘道會新增至 VPC A 中的10.0.1.125可路由子網路，IP 位址為。私有 NAT 閘道會針對來自 VPC A (100.64.0.10) 非路由子網路中執行個體的要求，如私有 NAT 閘道的 ENI 一樣10.0.1.125，執行來源網路位址轉譯。現在，流量可以指向分配給 VPC B () 中的 Application Load Balancer（ALB）的可路由 IP 地址，其目標為。10.0.2.10 100.64.0.10流量是透過公共 Transit Gateway 路由傳送 傳回流量會由私有 NAT 閘道處理回到要求連線的原始 Amazon EC2 執行個體。

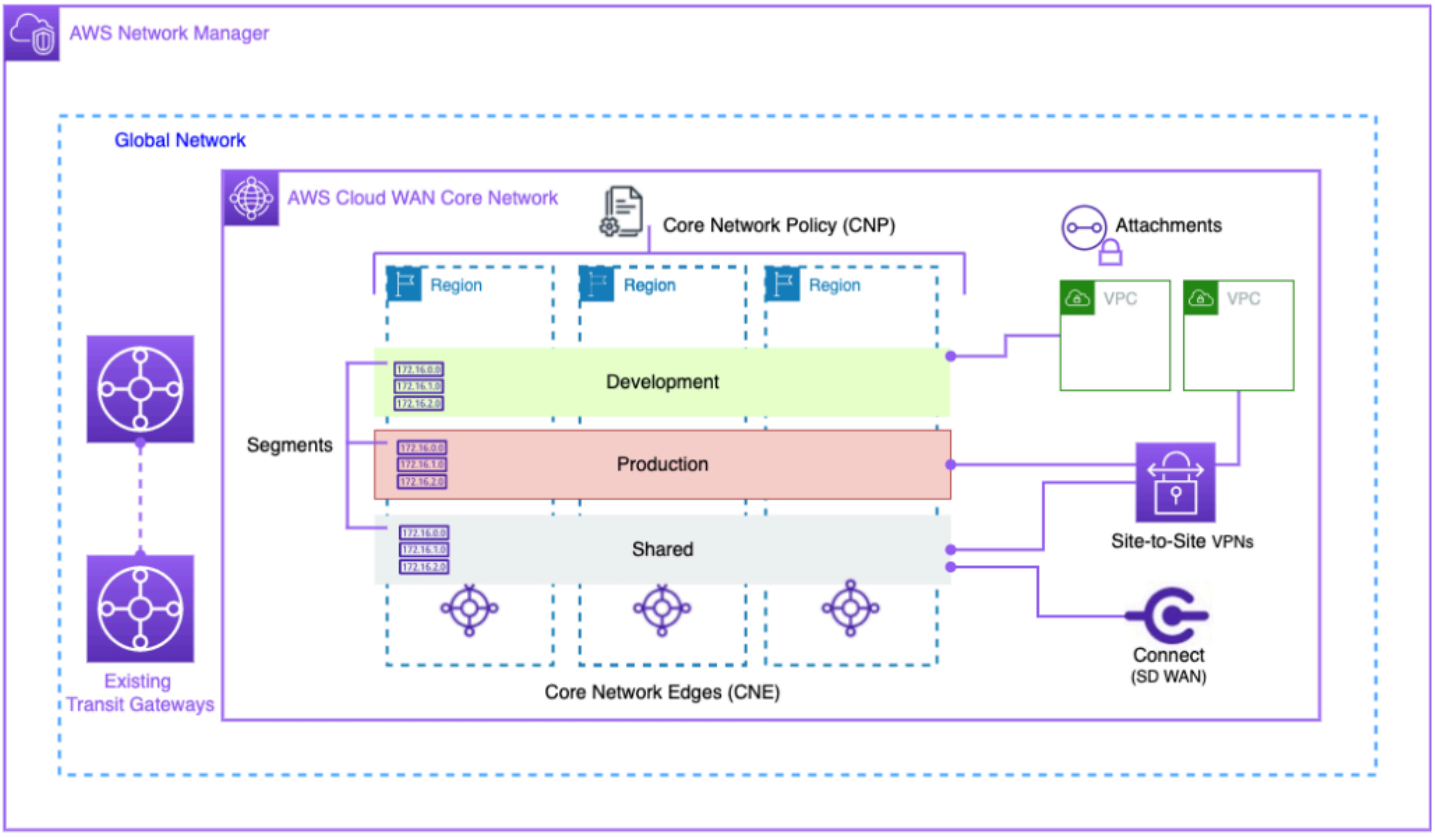
當您的內部部署網路限制對核准 IP 的存取時，也可以使用私有 NAT 閘道。少數客戶的內部部署網路只需透過客戶擁有的有限連續核准 IP 區塊，才能與私人網路 (無 IGW) 進行通訊。您可以使用私有 NAT 閘道，在每個允許列出的 IP 後面的 AWS VPC 上執行大型工作負載，而不是將每個執行個體分配給區塊的獨立 IP。如需詳細資訊，請參閱如何使用私有 NAT 解決方案解決私有 IP 耗盡問題部落格文章。



設定範例 — 如何使用私人 NAT 閘道為內部部署網路提供核准的 IP

AWS 雲端廣域網

AWS 雲端 WAN 是將網路連接在一起的新方式，我們之前可以透過傳輸閘道、VPC 對等互連和 IPSEC VPN 通道進行連接。之前，您可以設定一或多個 VPC，將它們與先前的其中一個方法連接在一起，然後使用 IPSEC VPN 或連線 AWS Direct Connect 到內部部署網路。您可以在一個位置定義網路和安全狀態結構，而在另一個位置定義您的網路。Cloud WAN 可讓您將所有這些結構集中在單一位置。透過原則，您可以細分網路，以判斷誰可以與誰交談，並透過這些區段將生產流量與開發或測試工作負載或內部部署網路隔離開來。



雲端廣域網路框圖

透過網路管理員使用者介面和 API 管理您的全球 AWS 網路。全球網路是所有網路物件的根層級容器；核心網路是 AWS 管理的全球網路的一部分。核心網路原則 (CNP) 是單一版本化的原則文件，可定義核心網路的所有層面。附件是您要新增至核心網路的任何連線或資源。核心網路邊緣 (CNE) 是符合原則之附件的本機連線點。網路區段是路由網域，依預設，僅允許區段內的通訊。

若要使用雲端廣域網路：

1. 在 AWS 網路管理員中，建立全球網路和關聯的核心網路。
2. 建立 CNP，定義要用來附加至區段的區段 AWS 區域 、出貨預先通知範圍及標記。
3. 套用網路原則。
4. 使用資源存取管理員與您的使用者、帳戶或組織共用核心網路。
5. 建立並標記附件。
6. 更新連接 VPC 中的路由以包含核心網路。

雲端 WAN 旨在簡化 AWS 基礎設施在全球連接的程序。它可讓您使用集中式權限原則來區隔流量，並在公司位置使用現有的基礎結構。雲端 WAN 也會連接您的 VPC、SD 廣域網、用戶端 VPN、防火

牆、VPN 和資料中心資源，以連線至雲端 WAN。如需詳細資訊，請參閱 AWS 雲端 WAN 部落格文章。

AWS 雲端 WAN 可提供連接雲端和現場部署環境的統一網路。Organizations 使用新一代防火牆 (NGFW) 和入侵預防系統 (IPSS) 來確保安全性。AWS Cloud WAN 和 Transit Gateway 遷移和互通性模式部落格文章描述了用於集中管理和檢查 Cloud WAN 網路 (包括單一區域和多區域網路) 中輸出網路流量的架構模式，以及設定路由表。這些架構可確保資料和應用程式保持安全，同時維護安全的雲端環境。

如需雲端 WAN 的詳細資訊，請參閱 AWS 雲端 WAN 中的集中式對外檢查架構部落格文章。

Amazon VPC Lattice

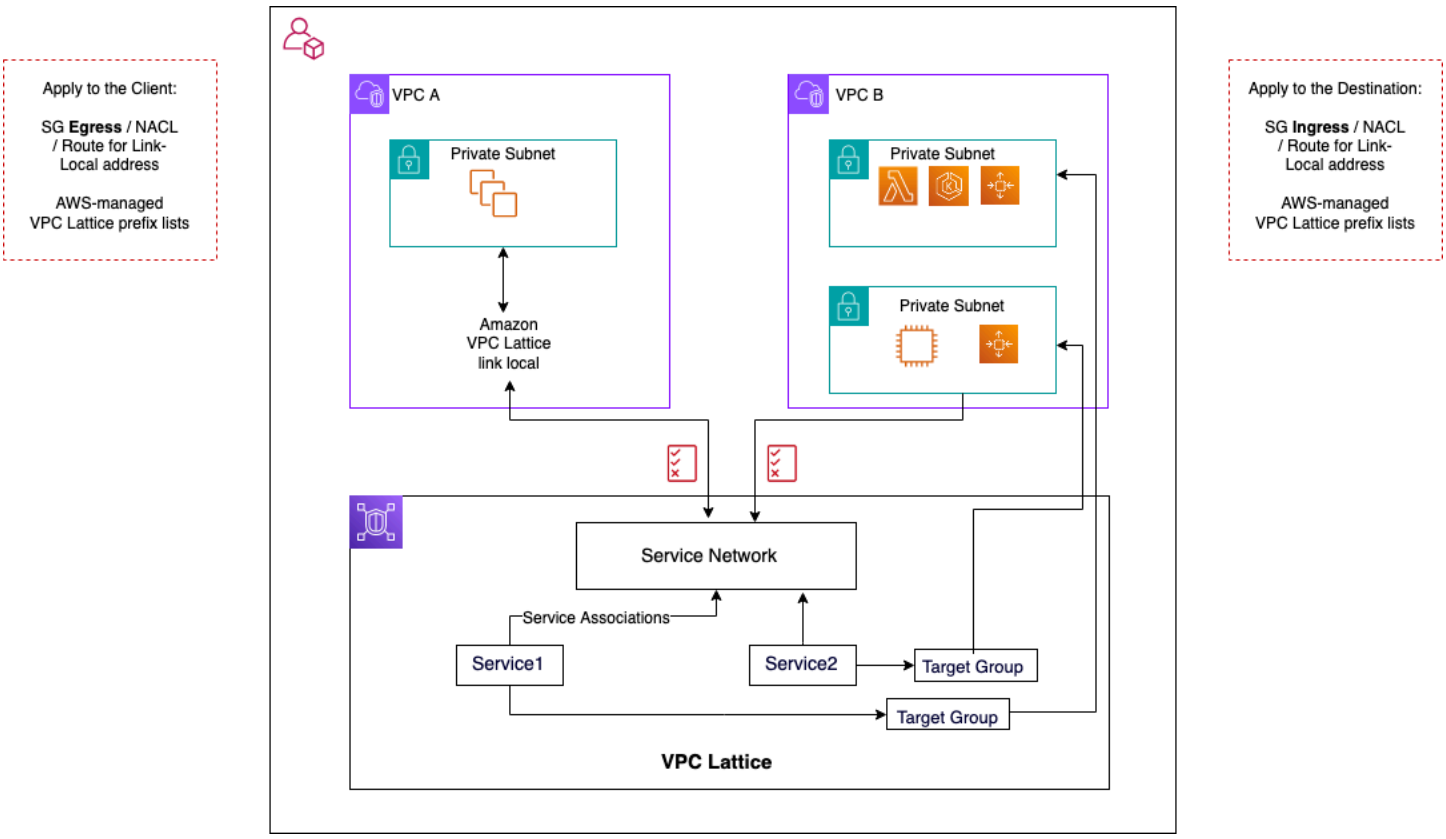
Amazon VPC Ladess 是一種全受管的應用程式聯網服務，可用來連接、監控和保護各種帳戶和虛擬私有雲之間的服務。VPC 萊迪思有助於在邏輯邊界內互連服務，以便您可以有效地管理和發現它們。

VPC 晶格元件包括：

- 服務-這是在實例，容器或 Lambda 函數上運行的應用程序的單元，由監聽器，規則和目標組組成。
- 服務網絡-這是用於自動實現服務發現和連接，並將通用訪問和觀察政策應用於服務集合的邏輯界限。
- 驗證政策-可與服務網路或個別服務相關聯的 IAM 資源政策，以支援請求層級身份驗證和內容特定授權。
- 服務目錄-集中檢視您擁有或透過 AWS Resource Access Manager 與您共用的服務。

VPC 格子使用步驟：

1. 建立服務網路。服務網路通常位於網路管理員擁有完整存取權的網路帳戶上。服務網路可以在組織內的多個帳戶之間共用。共享可以在個別服務或整個服務帳戶上執行。
2. 將 VPC 連接到服務網路以啟用每個 VPC 的應用程式網路，以便不同的服務可以開始使用在網路中註冊的其他服務。安全群組會套用來控制流量。
3. 開發人員定義服務，這些服務會填入服務目錄中，並註冊到服務網路中。VPC 萊迪斯包含所有已配置服務的地址簿。開發人員也可以定義路由原則以使用藍/綠部署。安全性是在定義身份驗證和授權政策的服務網絡級別以及實施 IAM 訪問政策的服務級別進行管理。



VPC 晶格通訊流程

更多詳細信息可以在 VPC 萊迪斯用戶指南中找到。

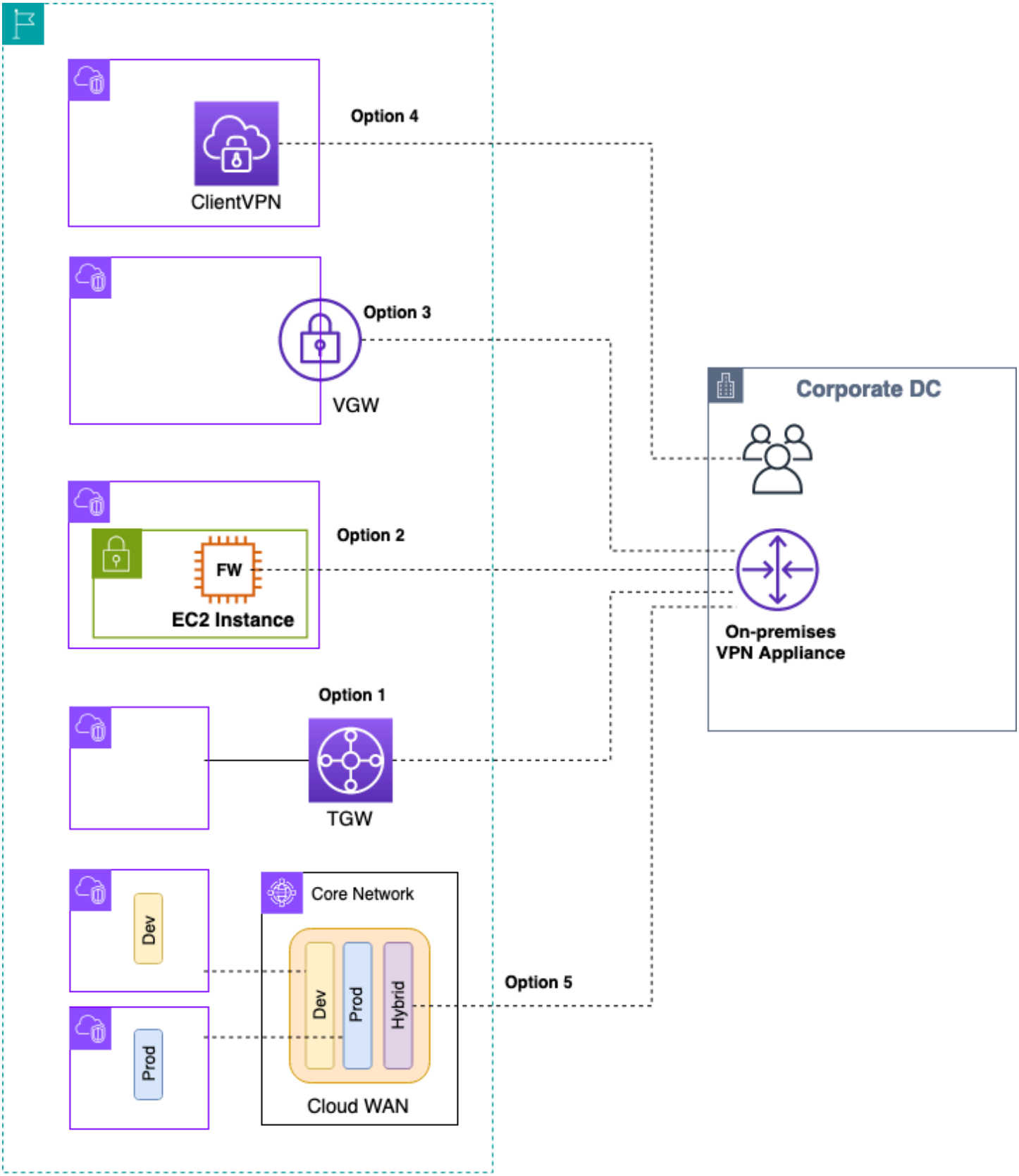
混合式連線

本節著重於安全地連接雲端資源與內部部署資料中心。啟用混合式連線的方法有三種：

- O ne-to-one 連線 — 在此設定中，會為每個 VPC 建立 VPN 連線和/或直接連線私有VIF。這是透過使用虛擬私有閘道 (VGW) 來完成的。此選項非常適合少量 VPC，但隨著客戶擴展 VPC 的規模，管理每個 VPC 的混合連線可能會變得困難。
- 邊緣整合 — 在此設定中，客戶可在單一端點整合多個 VPC 的混合式 IT 連線。所有 VPC 都共用這些混合式連線。這是通過使用 AWS Transit Gateway 和 AWS Direct Connect 網關來完成的。
- 完整網狀混合式整合 — 在此設定中，客戶可使用內建的 CloudWAN 在單一端點整合多個 VPC 的連線能力。 AWS Transit Gateway這是一種完整的原則型方法，可在一或多個 AWS 帳戶中進行聯網，以程式碼表示。目前，使用邊緣連線需要 AWS Direct Connect 對等 Transit Gateway 至 CloudWAN。

VPN

有多種方式可以將 VPN 設定到 AWS：

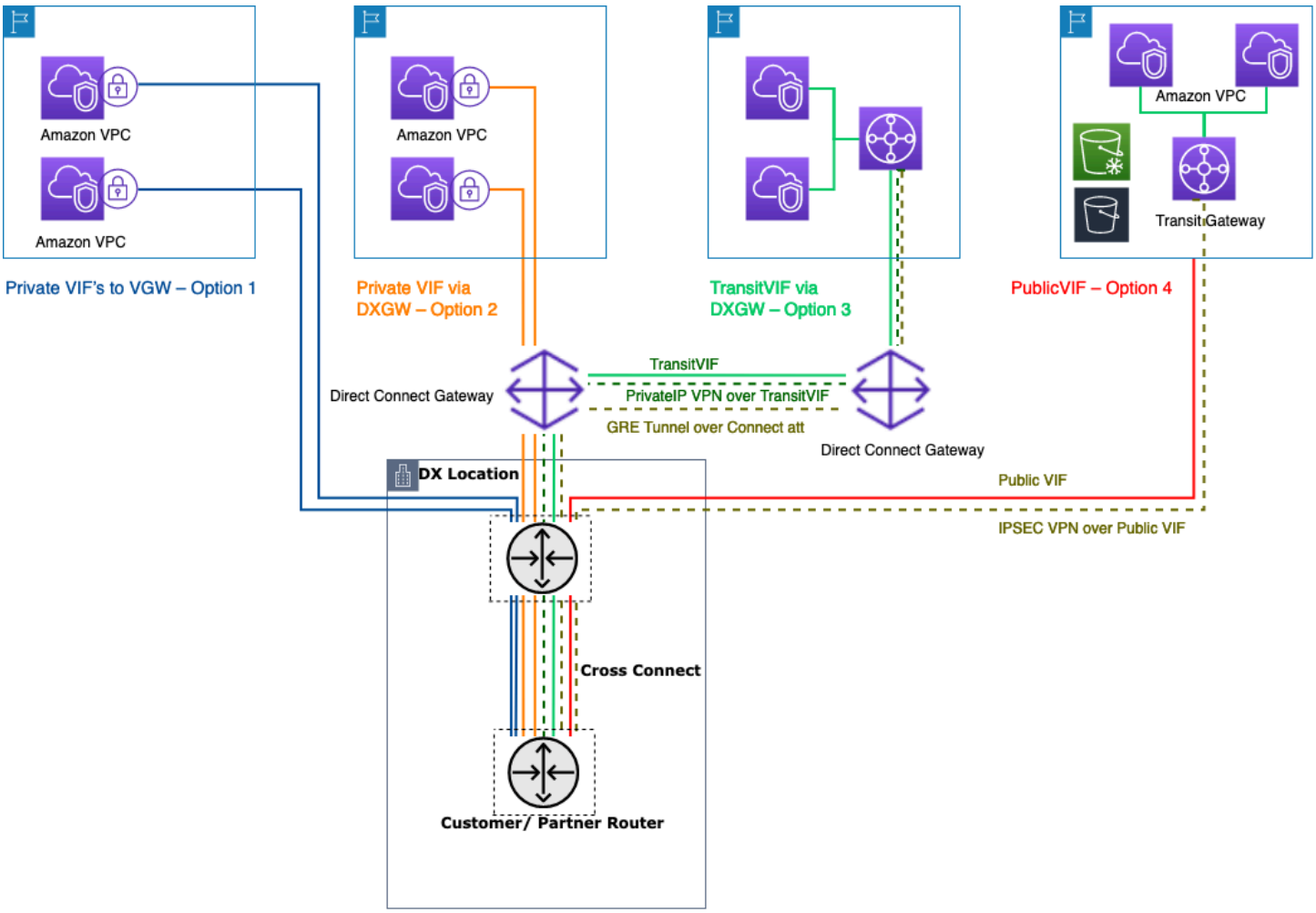

Option 4
ClientVPN
Option 3
VGW
Corporate DC
Option 2
FW
EC2 Instance
On-premises
VPN Appliance
Option 1
TGW
Dev
Core Network
Dev
Prod
Hybrid
Option 5
Prod
Cloud WAN

AWS VPN 選項

- 選項 1：整合 Transit Gateway 上的 VPN 連線 — 此選項會利用 Transit Gateway 上的 Transit Gateway VPN 附件。Transit Gateway 支持 IPsec 終止 site-to-site VPN。客戶可以建立通往 Transit Gateway 的 VPN 通道，並可存取連接到它的 VPC。傳輸閘道同時支援靜態和 BGP 式動態 VPN 連線。Transit Gateway 也支援 VPN 附件上的同等成本多路徑 (ECMP)。每個 VPN 連線每個通道的輸送量上限為 1.25-Gbps。啟用 ECMP 可讓您彙總 VPN 連線的輸送量，以便擴充超過 1.25 Gbps 的預設最大限制。在此選項中，您需要支付 Transit Gateway 定價和定AWS VPN 價。AWS 建議使用此選項進行 VPN 連線。如需詳細資訊，請參閱使用 AWS 傳輸閘道的擴展 VPN 輸送量部落格文章。
- 選項 2：終止 Amazon EC2 執行個體上的 VPN — 當客戶需要特定廠商軟體功能集 (例如思科 DMVPN 或一般路由封裝 (GRE)) 時，客戶可利用此選項，或想要跨各種 VPN 部署的操作一致性。您可以使用傳輸 VPC 設計進行邊緣整合，但請務必記住，傳輸 VPC VPC 到虛擬私人 VPC 的連接部分的所有關鍵考量都適用於混合式 VPN 連線。您必須負責管理高可用性，並支付 EC2 執行個體以及任何廠商軟體授權和支援費用。
- 選項 3：在虛擬私有閘道 (VGW) 上終止 VPN — 此 AWS 站 Site-to-Site VPN 服務選項可讓您在每個 one-to-one VPC 建立一個 VPN 連線 (包含一對備援 VPN 通道) 的連線設計。這是開始使用 VPN 連接到 AWS 的好方法，但是隨著您擴展 VPC 數量，管理越來越多的 VPN 連接可能會變得具有挑戰性。因此，利用 Transit Gateway 的邊緣整合設計最終將是一個更好的選擇。VGW 的 VPN 輸送量限制為每個通道 1.25 Gbps，而且不支援 ECMP 負載平衡。從定價的角度來看，您只需支付 AWS VPN 定價費用，執行 VGW 不需要任何費用。如需詳細資訊，請參閱AWS VPN 定價和AWS VPN 虛擬私有閘道。
- 選項 4：終止用戶端 VPN 端點上的 VPN 連線 — AWS Client VPN 是受管用戶端型 VPN 服務，可讓您安全地存取現場部署網路中的 AWS 資源和資源。透過 Client VPN，您可以使用 OpenVPN 或 AWS 提供的 VPN 用戶端，從任何位置存取您的資源。透過設定 Client VPN 端點，用戶端和使用者可以連線以建立傳輸層安全性 (TLS) VPN 連線。如需詳細資訊，請參閱 AWS Client VPN 文件。
- 選項 5：整合 AWS 雲端 WAN 上的 VPN 連線 — 此選項與此清單中的第一個選項類似，但是它使用 CloudWAN 網狀架構透過網路政策文件以程式設計方式設定 VPN 連線。

AWS Direct Connect

雖然透過網際網路 VPN 是開始使用的絕佳選擇，但是網際網路連線對於生產流量來說可能不可靠。由於這種不可靠性，許多客戶選擇AWS Direct Connect。 AWS Direct Connect 是一種聯網服務，提供使用網際網路連線到 AWS 的替代方法。使用時 AWS Direct Connect，先前透過網際網路傳輸的資料會透過設施和 AWS 之間的私有網路連線傳送。在許多情況下，私人網路連線可以降低成本、增加頻寬，並提供比網際網路連線更一致的網路體驗。有數種方式可用 AWS Direct Connect 來連線至 VPC：



連接內部部署資料中心的方式 AWS Direct Connect

- 選項 1：建立 Connect 到 VPC 的 VGW 的私有虛擬介面 (VIF) — 您可以為每個直接連線連線建立 50 個 V IF，最多可連線至 50 個 VPC (一個 VIF 提供連線至一個 VPC)。每個 VPC 都有一個 BGP 對等互連。此設定中的連線僅限於直 Connect 線位置所在的 AWS 區域。VIF 對 one-to-one 映至 VPC (以及缺乏全域存取權)，使其成為在著陸區存取 VPC 的最不偏好的方式。
- 選項 2：建立私有 VIF 至與多個 VGW 相關聯的直接連線閘道 (每個 VGW Connect 至 VPC) — 直 Connect 閘道是全球可用的資源。您可以在任何地區建立 Direct Connect 閘道，並從所有其他地區存取該閘道，包括 GovCloud （中國除外）。直接 Connect 閘道可透過單一私有 VIF 在任何 AWS 帳戶中連線至全球最多 20 個 VPC (透過 VGW)。如果「著陸區」由少量 VPC（十個或更少的 VPC）組成，並且/或您需要全域存取，則這是一個很好的選擇。每個直接連線連線的每個直 Connect Connect 線閘道都有一個 BGP 對等工作階段。直 Connect 線閘道僅適用於南北流量，不允許 VPC 到 VPC 的連線。如需詳細資訊，請參閱 AWS Direct Connect 文件中的虛擬私有閘道關聯。使用此選項，連線不僅限於直 Connect 線位置所在的 AWS 區域。 AWS Direct Connect 閘道僅適用

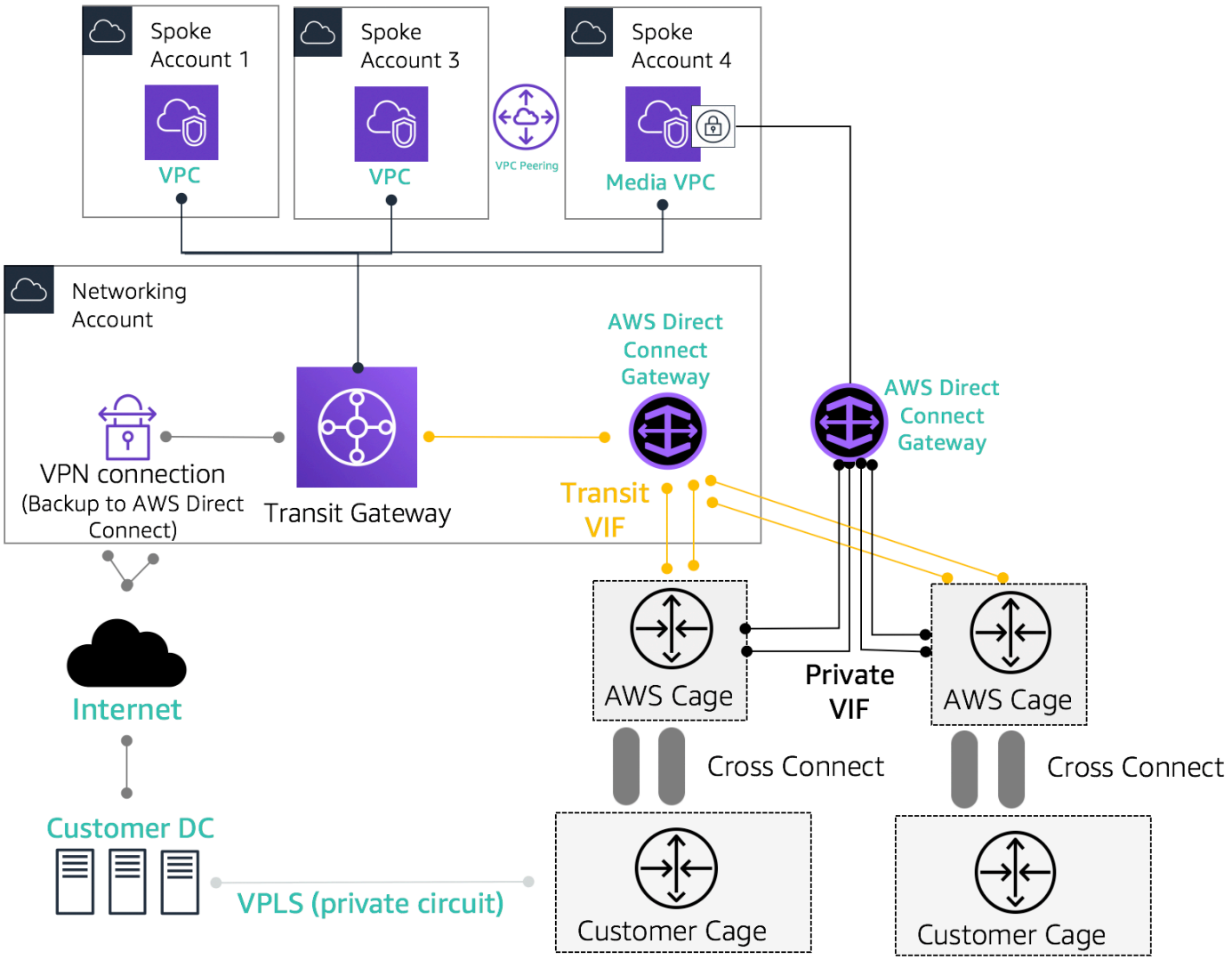
於北/南交通，不允許虛擬私人雲端到虛擬私人 VPC 的連線。此規則的例外情況是，當超級網路在兩個或多個 VPC 上公告，這些 VPC 具有與相同 AWS Direct Connect 閘道和相同虛擬界面相關聯的連接 VGW。在此情況下，VPC 可透過 AWS Direct Connect 端點彼此通訊。如需詳細資訊，請參閱 AWS Direct Connect 閘道文件。

- 選項 3：建立傳輸 VIF 至與傳輸閘道相關聯的直 Connect Transit Gateway — 您可以使用 Transit VIF 將傳輸閘道執行個體與直 Connect 閘道相關聯。 AWS Direct Connect 現在支援所有連接埠速度的 Transit Gateway 連線，在不需要高速連線 (大於 1Gbps) 時，為 Transit Gateway 使用者提供更具成本效益的選擇。這使您能夠以 50、100、200、300、400 和 500 Mbps 的速度使用直接 Connect，連接到 Transit Gateway。傳輸 VIF 可讓您透過單一 Transit Gateway VIF 和 BGP 對等，將現場部署資料中心連接至每個 AWS Direct Connect 閘道最多六個傳輸閘道執行個體 (可連線至數千個 VPC)。這是大規模連接多個 VPC 的選項中最簡單的設置，但是您應該注意 Transit Gateway 配額。需要注意的一個重要限制是，您只能透過傳輸 VIF 將 200 個字首從傳 Transit Gateway 公告到內部部署路由器。使用先前的選項，您需要支付直 Connect 定價的費用。對於此選項，您還需要支付 Transit Gateway 附件和資料處理費用。如需詳細資訊，請參閱直 Connect 上的 Transit Gateway 關聯說明文件。
- 選項 4：建立透過直 Connect 連線公用 VIF Transit Gateway 的 VPN 連線 — 公用 VIF 可讓您使用公有 IP 地址存取所有 AWS 公有服務和端點。在 Transit Gateway 上建立 VPN 附件時，AWS 端點會取得兩個 VPN 端點的公用 IP 位址。這些公用 IP 可透過公用 VIF 存取。您可以透過公用 VIF 建立任意多個 Transit Gateway 執行個體的 VPN 連線。當您透過公有 VIF 建立 BGP 對等互連時，AWS 會向您的路由器通告整個 AWS 公有 IP 範圍。為確保您僅允許某些流量（例如，僅允許流量進入 VPN 終止端點），建議您使用 FIREWER 內部部署設施。此選項可用於在網路層加密您的直 Connect。
- 選項 5： AWS Direct Connect 使用私有 IP VPN 建立與 Transit Gateway 的 VPN 連線 — 私有 IP VPN 是一項功能，可讓客戶使用私有 IP 地址透過直 Connect 連線部署 AWS Site-to-Site VPN 連線。使用此功能，您可以透過 Direct Connect 連線加密現場部署網路和 AWS 之間的流量，而不需要公有 IP 地址，進而同時增強安全性和網路隱私。私有 IP VPN 部署在 Transit VIF 之上，因此可讓您以更安全、私密且可擴充的方式，使用 Transit Gateway 集中管理客戶的 VPC 和內部部署網路的連線。
- 選項 6：透過傳輸 VIF 建立 GRE 通道至公共 Transit Gateway —「Transit Gateway Connect」附件類型支援 GRE。使用 Transit Gateway Connect，SD-WAN 基礎設施可以原生連接到 AWS，而無需在 SD-WAN 網路虛擬設備和 Transit Gateway 之間設定 IPSec VPN。GRE 通道可透過傳輸 VIF 建立，並將「傳 Transit Gateway 道 Connect 線」做為附件類型，相較於 VPN 連線，可提供更高的頻寬效能。如需詳細資訊，請參閱使用 Connect 簡化 SD-WAN AWS Transit Gateway 連線的部落格文章。

「將 VIF 傳輸至直 Connect 線閘道」選項似乎是最佳選項，因為它可讓您使用每個直接連線的單一 BGP 工作階段， AWS 區域 在單一點 (Transit Gateway) 合併指定的所有內部部署 Connect 線；不過，圍繞此選項的一些限制和考量，可能會導致您在結合使用私有傳輸 VIF 以滿足著陸區域連線需求。

下圖說明使用 Transit VIF 做為連線 VPC 的預設方法的範例設定，而私有 VIF 則用於必須從內部部署資料中心傳輸到媒體 VPC 的邊緣使用案例。私有 VIF 用於避免 Transit Gateway 資料處理費用。最佳作法是在兩個不同的「直 Connect 連線」位置至少有兩個連線，以獲得最大的備援能力 — 總共四個連線。您可以為每個連線建立一個 VIF，總共四個私人 VIF 和四個傳輸 VIF。您也可以建立 VPN 做為連線的備份 AWS Direct Connect 連線。

透過「透過傳輸 VIF 建立 GRE 通道到傳輸閘道」選項，您就能以原生方式將 SD-WAN 基礎設施與 AWS 連接。它不需要在 SD-WAN 網路虛擬設備和 Transit Gateway 之間設定 IPsec VPN。



混合式連線參考架構範例

使用網路服務帳戶來建立直 Connect 資源，以便劃分網路管理界限。直 Connect 連線連線、直 Connect 線閘道和傳輸閘道都可以位於網路服務帳戶中。要與您的著陸區共享 AWS Direct Connect 連接，只需通過 AWS RAM 其他帳戶共享公共 Transit Gateway 即可。

直 Connect 連線連線的 MacSec 安全性

客戶可以在特定位置使用 MAC 安全標準 (MacSEC) 加密 (IEEE 802.1AE) 與其直 Connect 連線連線，提供 10 Gbps 和 100 Gbps 專用連線。透過此功能，客戶可以在第 2 層保護資料安全，而直 Connect 則提供 point-to-point 加密功能。若要啟用直 Connect MacSec 功能，請確定符合 MacSec 的先決條件。因為 MacSec 會保護連結的 hop-by-hop基礎上，因此您的裝置必須與我們的直接 Connect 裝置具有直接第 2 層的鄰接。您的最後一哩提供商可以幫助您驗證您的連接是否可以與 MacSec 一起使用。如需詳細資訊，請參閱將 MacSec 安全性新增至 AWS Direct Connect 連線。

AWS Direct Connect 彈性建議

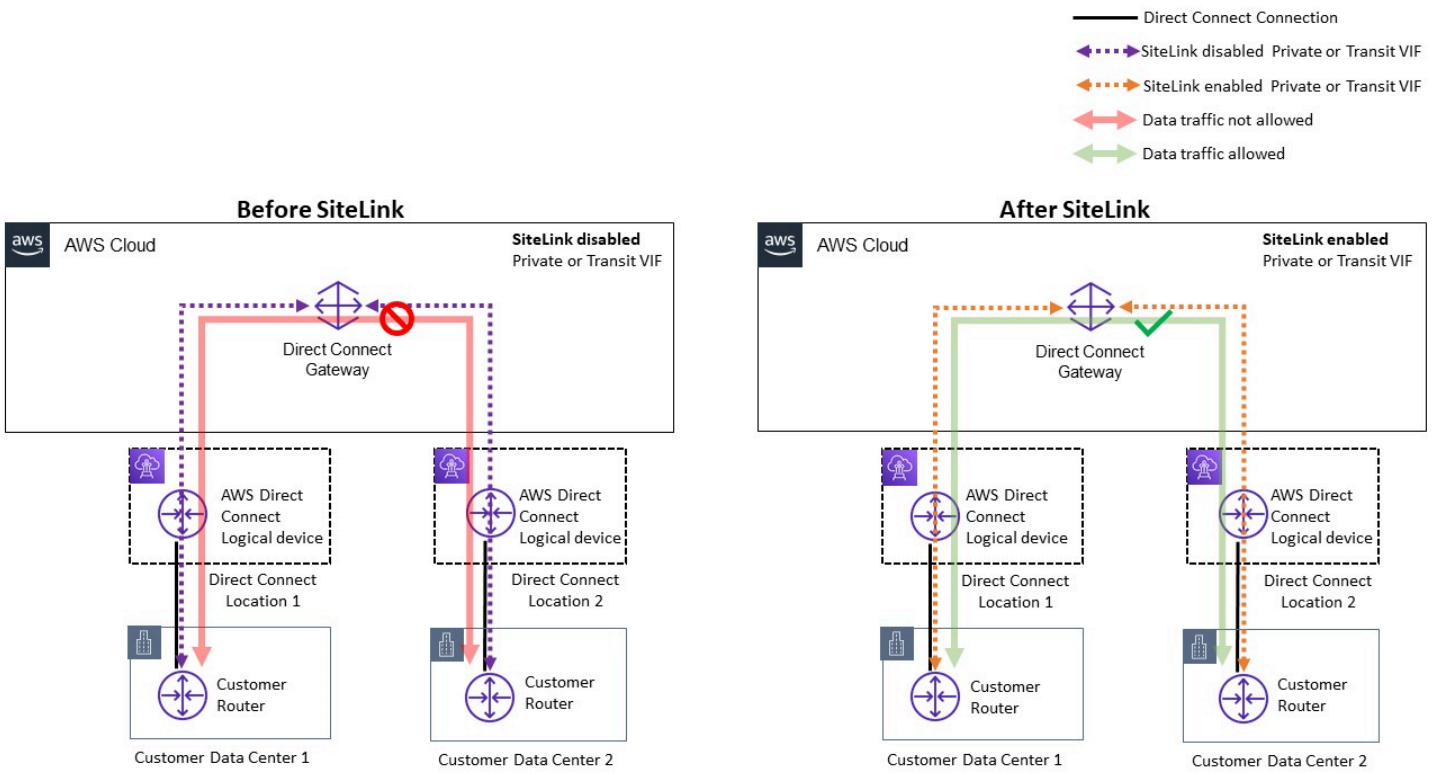
客戶可以透過現場部署網路 AWS Direct Connect，在 Amazon VPC 和 AWS 資源中實現高度彈性的連線能力。最佳做法是客戶從多個資料中心進行連線，以消除任何單點實體位置故障。根據工作負載類型的不同，客戶也建議使用多個直 Connect 連線連線來進行備援。

AWS 也提供 AWS Direct Connect 彈性工具組，可為客戶提供具有多種備援模型的連線精靈；協助客戶判斷哪種模型最適合其服務等級協定 (SLA) 要求，並相應地使用 Direct Connect 連線設計混合式連線。如需詳細資訊，請參閱AWS Direct Connect 復原建議。

AWS Direct Connect SiteLink

過去，只有透過暗光纖或其他技術、IPSEC VPN 使用直接電路建置，或是透過採用 MPLS 或傳統 T1 電路等技術的協力廠商電路供應商，才能設定內部部署網路的 site-to-site 連結。 MetroEthernet隨著的出現 SiteLink，客戶現在可以為在某 AWS Direct Connect 個位置終止的內部部署位置啟用直接 site-to-site 連線。使用您的直接 Connect 電路提供 site-to-site 連接，而無需通過 VPC 路由流量，完全繞過 AWS 區域。

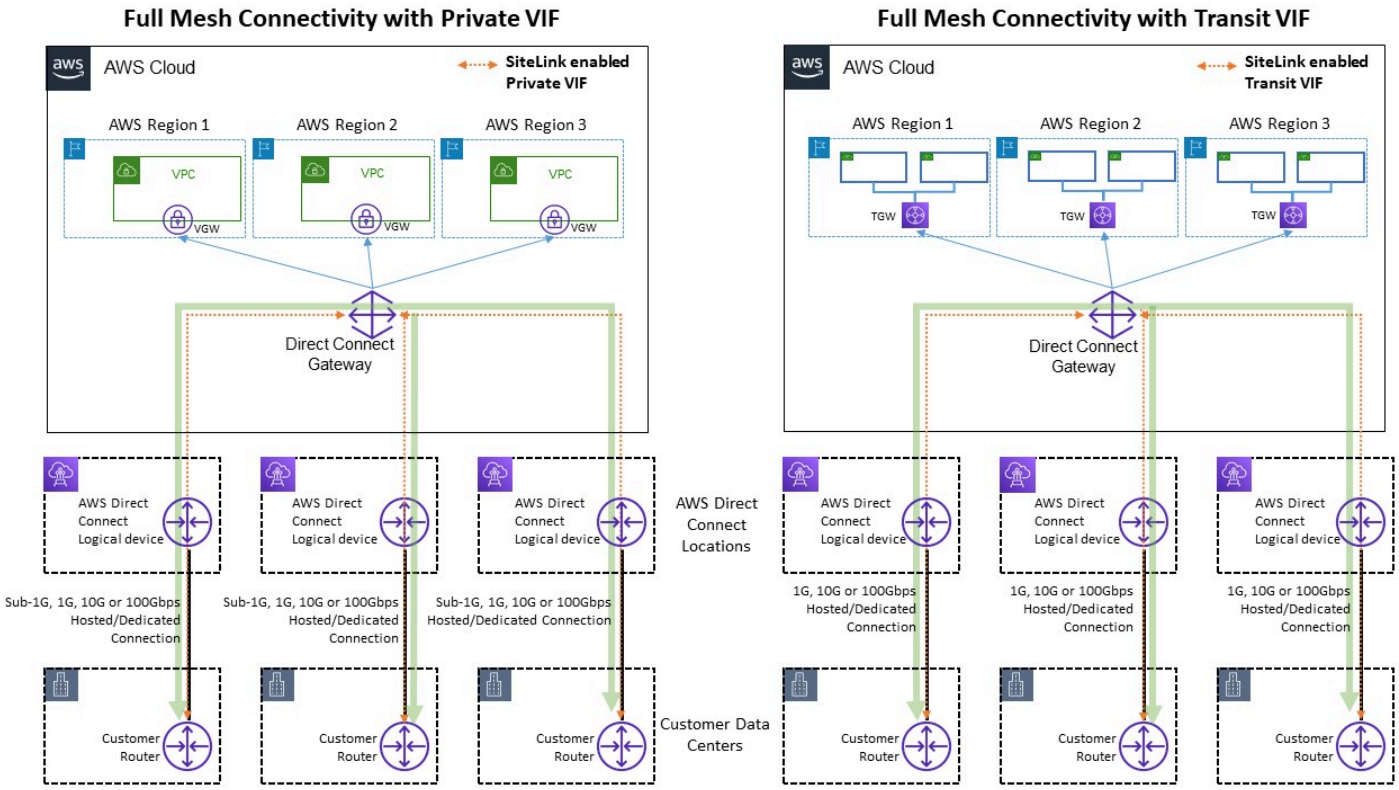
現在，您可以透過 AWS Direct Connect 位置之間最快的路徑傳送資料，在全球網路中的辦公室和資料中心之間建立全域、可靠且 pay-as-you-go 連線。



範例參考架構 AWS Direct Connect SiteLink

使用時 SiteLink，您首先將現場部署網路連接到全球 100 多個 AWS Direct Connect 位置的 AWS。然後，在這些連線上建立虛擬介面 (VIF) 並啟用 SiteLink。將所有 VIF 連接到同一個 AWS Direct Connect 閘道 (DXGW) 後，您就可以開始在它們之間傳送資料。您的資料使用快速、安全且可靠的 AWS 全球網路，遵循不同 AWS Direct Connect 位置到目的地之間的最短路徑。你不需要有任何資源在任 AWS 區域 何使用 SiteLink。

透過 SiteLink 啟用的 VIF SiteLink，DXGW 會從路由器學習 IPv4/IPv6 前置詞、執行 BGP 最佳路徑演算法、更新屬性 (例如 NextHop 和 AS_Path)，並將這些 BGP 前置碼重新公告至與該 DXGW 相關聯的已啟用 VIF 的其餘部分。 SiteLink如果您在 VIF SiteLink 上停用，DXGW 將不會透過此 VIF 將學到的內部部署首碼公告給其他已啟用的 VIF。 SiteLink SiteLink 停用 VIF 的現場部署前置詞僅會廣告至 DXGW 閘道關聯，例如 AWS 虛擬私有閘道 (VGW) 或與 DXGW 相關聯的傳 Transit Gateway 道 (TGW) 執行個體。



網站連結允許流量範例

SiteLink 允許客戶使用 AWS 全球網路，做為遠端位置之間的主要或次要/備份連線，具有高頻寬和低延遲，並透過動態路由來控制哪些位置可以相互通訊以及與 AWS 區域資源通訊。

如需詳細資訊，請參閱簡介 AWS Direct Connect SiteLink。

集中輸出至網際網路

當您在多帳戶環境中部署應用程式時，許多應用程式將需要僅限輸出的網際網路存取 (例如，下載程式庫、修補程式或作業系統更新)。這對於IPv4和IPv6流量都可以實現。因此IPv4，您可以透過NAT閘道 (建議使用NAT) 形式的網路位址轉譯 ()，或者透過在 Amazon EC2 執行個體上執行的自我管理NAT執行個體來達成，作為所有輸出網際網路存取的方式。內部應用程式位於私有子網路中，而NAT閘道和 Amazon EC2 NAT 執行個體則位於公有子網路中。

AWS建議您使用NAT閘道，因為它們提供更好的可用性和頻寬，而且您需要較少的 eort 來管理。如需詳細資訊，請參閱比較NAT閘道和NAT執行個體。

對於IPv6流量，可以將出口流量設定為以分散方式VPC透過僅出口網際網路閘道離開每個流量，也可以將其設定為VPC使用NAT執行個體或 Proxy 執行個體集中傳送至集中式。IPv6模式將在中討論集中式輸出 IPv6。

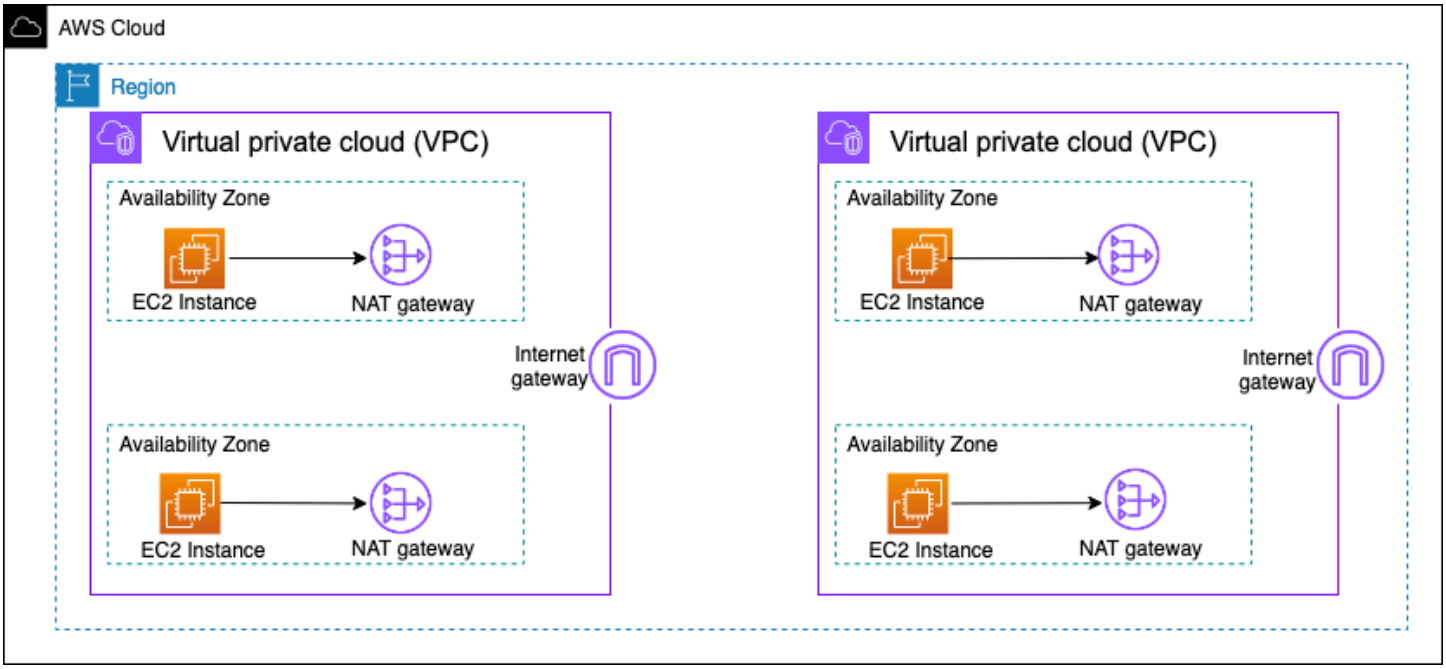
主題

- 使用NAT閘道進行集中式IPv4輸出
- 將NAT閘道與集中式IPv4輸 AWS Network Firewall 出搭配使用
- 將NAT閘道和閘道 Load Balancer 與 Amazon EC2 執行個體搭配使用集中IPv4輸出
- 集中式輸出 IPv6

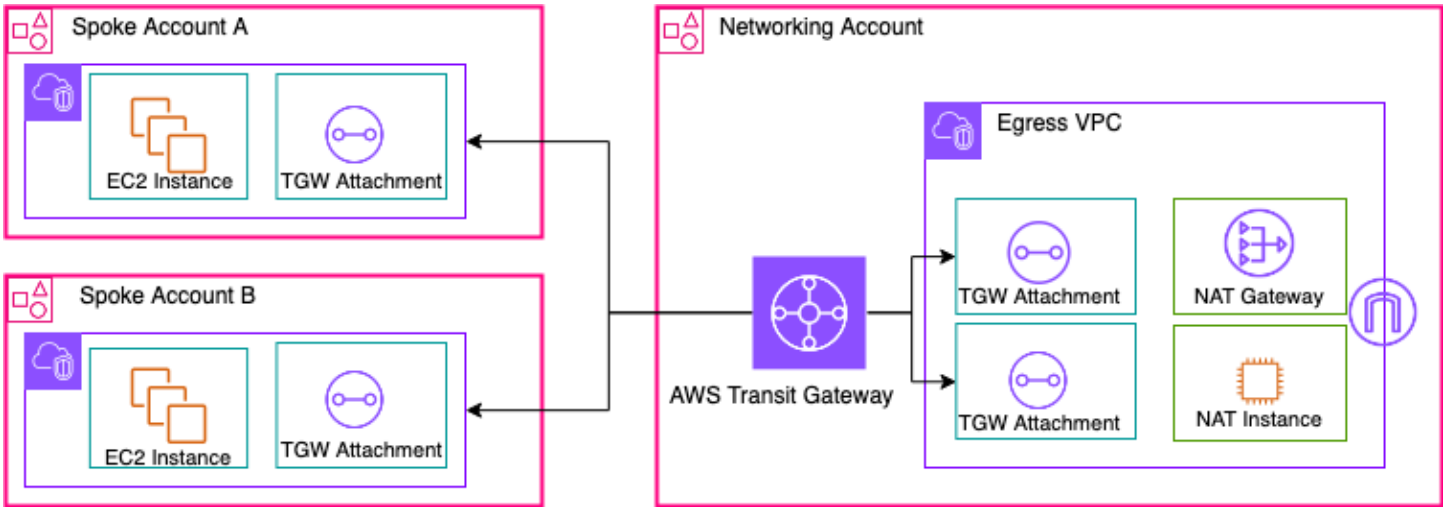
使用NAT閘道進行集中式IPv4輸出

NAT閘道是一種受管理的網路位址轉譯服務。在每個網輻中部署NAT閘道VPC可能會變得高昂成本，因為您需要為部署的每個NAT閘道支付小時費用 (請參閱 Amazon VPC 定價)。集中NAT閘道是降低成本的可行選擇。若要集中化，您可以VPC在網路服務帳戶中建立個別的輸出、在出口中部署NAT閘道 VPC，然後VPC使用 Transit Gateway 或 Cloud 將所有出口流量從網點路由傳送VPCs至出口中的NAT閘道WAN，如下圖所示。

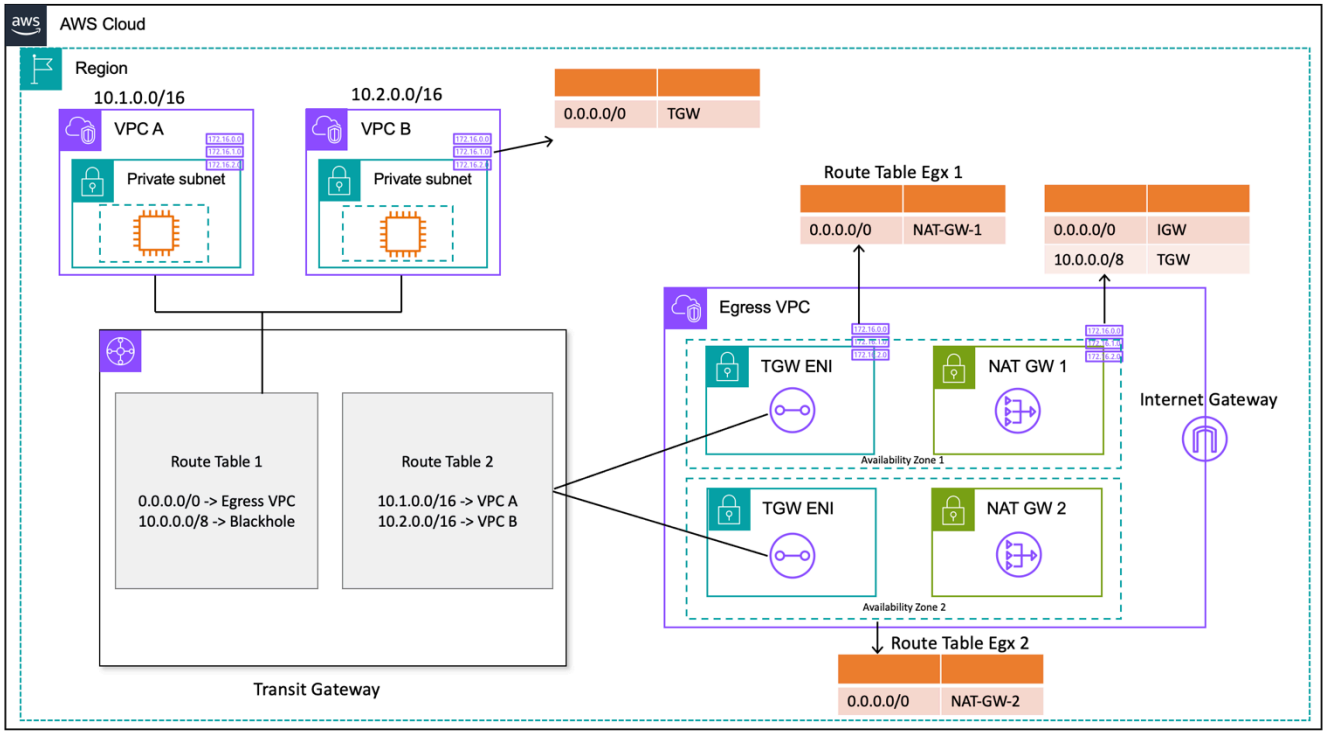
> **Note**
>
> 當您使用 Transit Gateway 集中化NAT閘道時，您需要支付額外的 Transit Gateway 資料處理費用 — 與在每VPC個網關中執行NAT閘道的分散式方法相比。在某些邊緣情況下，當您透過NAT閘道傳送大量資料時VPC，將NAT本機保留在中VPC以避免 Transit Gateway 資料處理費用可能更具成本效益。



分散式高可用性NAT閘道架構



使用傳輸NAT閘道的集中式閘道 (概觀)



使用傳輸NAT閘道的集中式閘道（路由表設計）

在此設定中，輪輻VPC附件與 Route Table 1 (RT1) 相關聯，並會傳播至「路由表格 2」(RT2)。有一條黑洞路線可以禁止兩VPCs人相互溝通。如果您想要允許間VPC通訊，您可以從中移除`10.0.0.0/8 -> Blackhole`路由項目RT1。這可讓他們透過傳輸閘道進行通訊。您也可以將分支VPC附件傳播到RT1（或者，您可以使用一個路由表並將所有內容關聯/傳播到該表），從而在使用 Transit Gateway 之間啟用直接流量。VPCs

您可以在將所有流量RT1指向出口VPC時新增靜態路由。由於這種靜態路由，Transit Gateway 會透過其ENIs在出口VPC處傳送所有網際網路流量。進入出口後VPC，流量會遵循子網路路由表格中找到的路由，而這些 Transit Gateway ENIs 所在的路由。您可以在子網路路由表中新增路由，將所有流量指向相同可用區域中的個別NAT閘道，以最小化跨可用區域 (AZ) 流量。NAT閘道子網路路由表具有網際網路閘道 (IGW) 做為下一個躍點。若要將流量傳回至「傳輸閘道」，您必須在NAT閘道子網路路由表格中新增靜態路由表項目，將所有輻條VPC繫結流量指向 Transit Gateway 作為下一個躍點。

高可用性

為了達到高可用性，您應該使用多個NAT閘道 (每個可用區域中有一個閘道)。如果NAT閘道無法使用，流量可能會丟棄在穿越受影響NAT閘道的可用區域中。如果有一個可用區域無法使用，Transit Gateway 端點以及該可用區域中的NAT閘道將會失敗，且所有流量都會透過另一個可用區域中的Transit NAT Gateway 道和閘道端點流動。

安全

您可以仰賴來源執行個體的安全群組、Transit Gateway 路由表中的黑洞路由，以及NAT閘道所在子網ACL路的網路。例如，客戶可以在NAT閘道公用子網路ACLs上使用，以允許或封鎖來源或目的地 IP 位址。或者，您也可以將 G NAT ateway 與用 AWS Network Firewall 於下一節所述的集中式輸出，以滿足此需求。

可擴展性

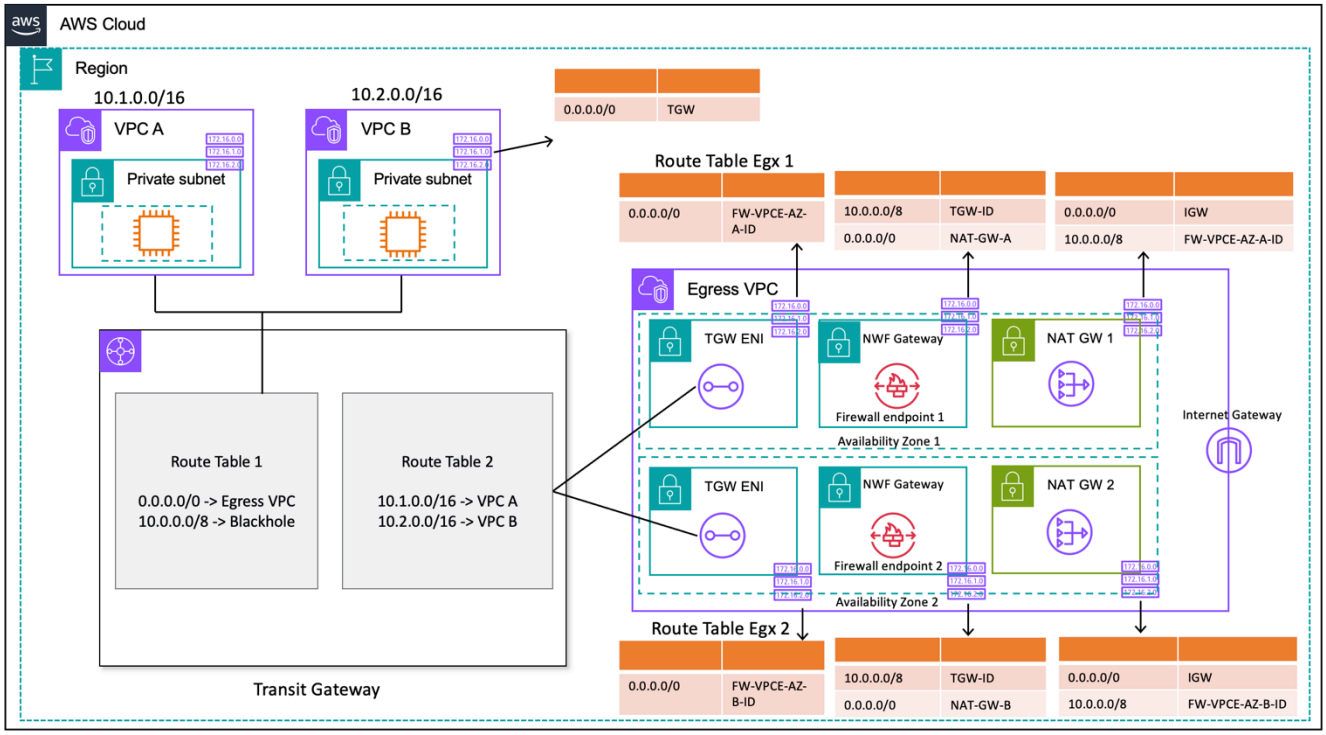
單一NAT閘道每個指派的 IP 位址最多可支援 55,000 個同時連線至每個唯一目的地。您可以要求調整配額，以允許最多八個指派的 IP 位址，允許 440,000 個同時連線至單一目的地 IP 和連接埠。NAT閘道器提供 5 Gbps 的頻寬，並自動擴充至 100 Gbps。Transit Gateway 通常不會做為負載平衡器，也不會將流量平均分配到多個可用區域中的NAT閘道之間。如果可能，跨越 Transit Gateway 的流量將保持在可用區域內。如果 Amazon EC2 執行個體起始流量位於可用區域 1 中，流量將從輸出中相同可用區域 1 的 Transit Gateway 彈性網路界面中脫離，VPC並根據 elastic network interface 所在的子網路路由表格移至下一個躍點。如需規則的完整清單，請參閱 Amazon Virtual Private Cloud 文件中的NAT閘道。

如需詳細資訊，請參閱從多個VPCs使用 AWS Transit Gateway 建立單一網際網路出口點部落格文章。

將NAT閘道與集中式IPv4輸 AWS Network Firewall 出搭配使用

如果您想要檢查和篩選輸出流量，可以在集中式輸出架構中結合 AWS Network Firewall 與NAT閘道。AWS Network Firewall 是一項託管服務，可讓您輕鬆為您VPCs的所有. 它為您的整個VPC第 3-7 層網絡流量提供控制和可見性。您可以執行URL/網域名稱、IP 位址和內容型輸出流量篩選，以阻止可能的資料遺失、協助符合法規要求，並封鎖已知的惡意程式通訊。 AWS Network Firewall 支援數千條規則，這些規則可以過濾掉已知錯誤 IP 位址或錯誤網域名稱的網路流量。您也可以透過匯入開放原始碼IPS規則集或使用 Suricata 規則語法撰寫您自己的入侵預防系統 (IPS) 規則，將 Suricata 規則用作 AWS Network Firewall 服務的一部分。 AWS Network Firewall 還允許您導入來自AWS合作夥伴的兼容規則。

在具有檢查的集中式出口架構中， AWS Network Firewall 端點是輸出的傳輸閘道附件子網路路由表中的預設路由表目標。VPC輻條VPCs和互聯網之間的流量使用 AWS Network Firewall 如下圖所示進行檢查。



具有 AWS Network Firewall 和NAT閘道的集中式出口（路由表設計）

對於具有 Transit Gateway 的集中式部署模式，AWS建議在多個可用區域中部署 AWS Network Firewall 端點。客戶執行工作負載的每個可用區域中應該有一個防火牆端點，如上圖所示。最佳作法是，防火牆子網路不應包含任何其他流量，因 AWS Network Firewall 為無法檢查來自防火牆子網路內的來源或目的地的流量。

與先前的設定類似，輻條VPC附件與 Route Table 1 (RT1) 相關聯，並傳播至「路由表 2」(RT2)。明確添加了黑洞路由，以禁止兩VPCs者相互通信。

繼續使用預設路由將所有流量RT1指向出口VPC。Transit Gateway 會將所有流量轉送至出口VPC中兩個可用區域的其中一個。一旦流量到達輸出中的其ENIs中一個 Transit GatewayVPC，您就會點選預設路由，該路由會將流量轉送至其個別可用區域中的其中一個 AWS Network Firewall 端點。 AWS Network Firewall 接著會根據您設定的規則檢查流量，然後再使用預設路由將流量轉送至NAT閘道。

這種情況不需要 Transit Gateway 設備模式，因為您不會在附件之間傳送流量。

> **Note**
>
> AWS Network Firewall 不會為您執行網路位址轉譯，此功能會在通過流量檢查之後由NAT閘道處理 AWS Network Firewall。在此情況下，不需要輸入路由，因為NATGWIPs依預設，傳回流量會轉送至。

因為您使用的是 Transit Gateway，因此我們可以在NAT網關之前放置防火牆。在此模型中，防火牆可以看到 Transit Gateway 後面的來源 IP。

如果您在單一執行此操作VPC，我們可以使用VPC路由增強功能，以便您檢查相同VPC子網路之間的流量。如需詳細資訊，請參閱AWS Network Firewall 具有VPC路由增強功能的部署模型部落格文章。

可擴展性

AWS Network Firewall 可以根據流量負載自動擴展或縮減防火牆容量，以維持穩定、可預測的效能，將成本降至最低。 AWS Network Firewall 專為支援數萬個防火牆規則而設計，每個可用區域最多可擴充 100 Gbps 輸送量。

關鍵考量

- 每個防火牆端點可處理約 100 Gbps 的流量，如果您需要更高的突發或持續輸送量，請聯絡AWS支援部門。
- 如果您選擇在AWS帳戶中建立NAT閘道以及 Network Firewall，則可免除標準NAT閘道處理和每小時的使用費，而且每 GB 的處理次數和防火牆收取的使用時數。 one-to-one
- 您也可以考慮透過 AWS Firewall Manager 沒有 Transit Gateway 的分散式防火牆端點。
- 在將防火牆規則移至生產環境之前先測試防火牆規則，類似於網路存取控制清單，視訂單很重要。
- 需要先進的蘇里卡塔規則才能進行更深入的檢查。網路防火牆支援入口和出口流量的加密流量檢查。
- HOME_NET規則群組變數定義了可在狀態引擎中進行處理的來源 IP 範圍。使用集中式處理，您必須將所有附加到 Transit Gateway 的VPCCIDRs附加內容，以使其符合處理資格。如需HOME_NET規則群組變數的詳細資訊，請參閱 Network Firewall 文件。
- 請考慮VPC在個別的網路服務帳戶中部署 Transit Gateway 和出口，以根據職責委派來隔離存取；例如，只有網路管理員可以存取網路服務帳戶。
- 為了簡化此模型 AWS Network Firewall 中的部署和管理， AWS Firewall Manager 可以使用。Firewall Manager 可讓您自動將您在集中式位置建立的保護套用至多個帳戶，藉此集中管理不同的防火牆。Firewall Manager 員支援 Network Firewall 的分散式和集中式部署模式。若要深入了解，請參閱部落格文章如何 AWS Network Firewall 使用 AWS Firewall Manager.

將NAT閘道和閘道 Load Balancer 與 Amazon EC2 執行個體搭配使用集中IPv4輸出

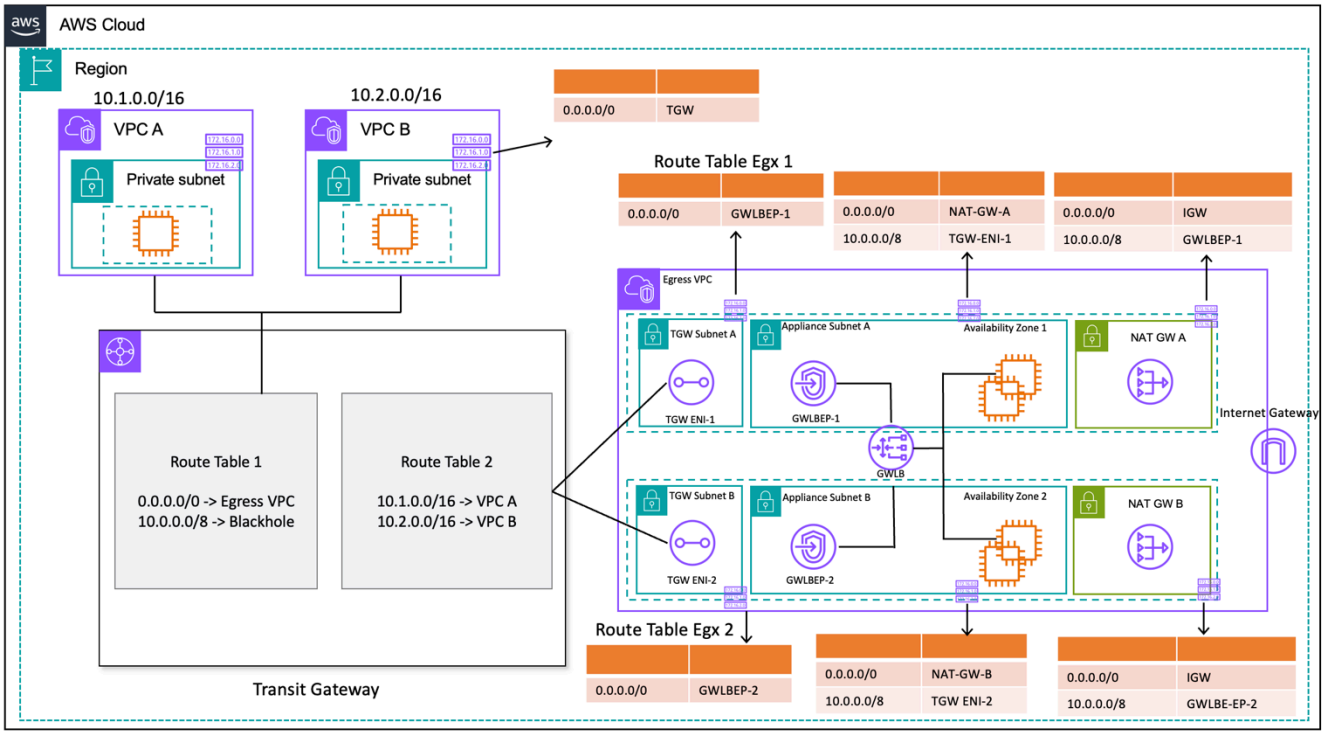
從 AWS Marketplace 和作為退出點使用以軟體 AWS Partner Network 為基礎的虛擬設備 (在 Amazon 上EC2) 與NAT閘道設定類似。如果您想要使用各種廠商產品的進階第 7 層網路/入侵防護/偵測系統 (IPS/IDS)，以及深度封包檢測功能，可以使用此選項。

在下圖中，除了閘道之外，您還可以使用NAT閘道 Load Balancer (GWLB) 後方的EC2執行個體部署虛擬應用裝置。在此設定中，閘道 Load Balancer 端點 (GWLBE)、虛擬應用裝置和NAT閘道會部署在集中式VPC，並使用VPC附件連接至 Transit Gateway 道。GWLB輻條VPCs也使用VPC附件連接到 Transit Gateway。由於GWLBEs是可路由的目標，因此您可以將流量路由傳 Transit Gateway 之間的流量傳送至設定為後方目標的虛擬應用裝置叢集GWLB。GWLB充當 bump-in-the-wire 並透明地將所有第 3 層流量通過第三方虛擬設備，因此流量的來源和目的地不可見。因此，此架構可讓您集中檢查透過 Transit Gateway 穿越的所有出口流量。

如需有關流量如何從應用程式流向網際網路並透過此設定傳回的詳細資訊，請參閱使用AWS閘道 Load Balancer 的集中式檢查架構和 AWS Transit Gateway。VPCs

您可以在 Transit Gateway 上啟用設備模式，以維持透過虛擬設備的流量對稱。這表示在流程的生命週期內，雙向流量會透過相同應用裝置和可用區域進行路由。此設定對於執行深度封包檢查的狀態防火牆尤其重要。啟用設備模式不再需要複雜的因應措施，例如來源網路位址轉譯 (SNAT)，以強制流量返回正確的應用裝置以維持對稱性。如需詳細資訊，請參閱部署閘道 Load Balancer 的最佳作法。

也可以在沒有 Transit Gateway 的情況下以分散式方式部署GWLB端點，以啟用出口檢查。若要深入瞭解此架構模式，請參閱AWS閘道 Load Balancer 簡介：支援的架構模式部落格文章。



使用閘道 Load Balancer 和EC2執行個體集中輸出 (路由表設計)

高可用性

AWS建議在多個可用區域中部署閘道負載平衡器和虛擬應用裝置，以提高可用性。

閘道 Load Balancer 可執行健康狀態檢查以偵測虛擬應用裝置故障 如果是運作狀況不佳的設備，請將新流程GWLB重新路由至健康的設備。無論目標的健全狀況狀態為何，現有流程一律會移至相同的目標。這可讓連線排出，並因應設備CPU尖峰造成的健康狀態檢查失敗。如需詳細資訊，請參閱部落格文章部署閘道 Load Balancer 的最佳做法中的第 4 節：瞭解應用裝置和可用區域失敗案例。閘道 Load Balancer 可以使用 auto 資源調度群組做為目標 這項優勢消除了管理應用裝置叢集的可用性和可擴充性的繁重工作。

優點

閘道 Load Balancer 和閘道 Load Balancer 端點由其提供支援 AWS PrivateLink，可讓您安全地跨VPC界線交換流量，而無需周遊公用網際網路。

Gateway Load Balancer 是一項受管理服務，可消除管理、部署和擴展虛擬安全應用裝置的無差別繁重工作，讓您可以專注於重要的事情。閘道 Load Balancer 可將防火牆堆疊公開為端點服務，供客戶訂閱使用 AWS Marketplace. 這就是所謂的防火牆即服務 (FWaaS)；它引入了簡化的部署，無需依賴BGP和分配流量ECMP到多個 Amazon EC2 執行個體。

關鍵考量

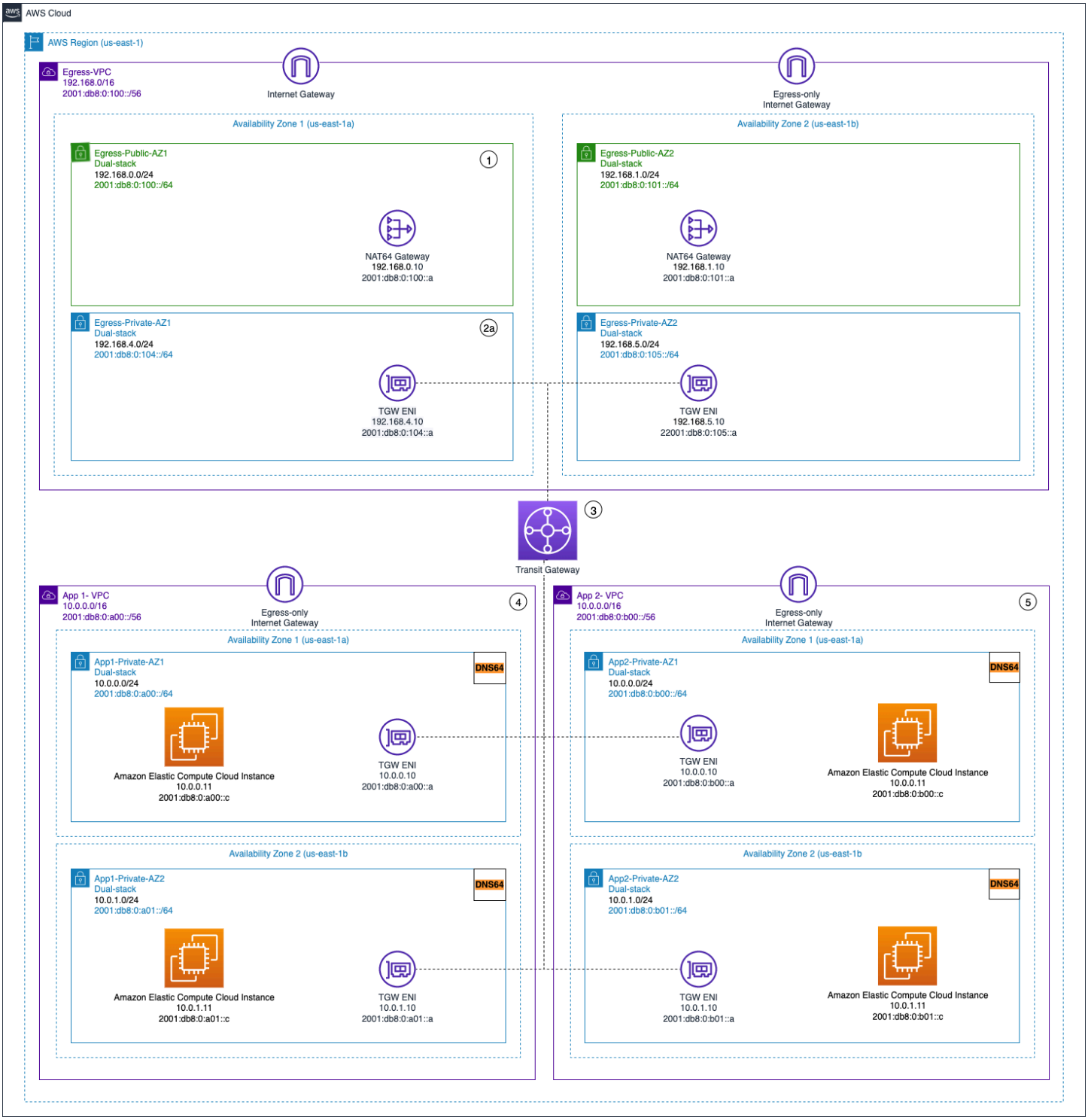
- 這些設備需要支持 Geneve 封裝協議進行集成。GWLB
- 某些協力廠商設備可支援SNAT並覆蓋路由 (雙臂模式)，因此無需建立NAT閘道以節省成本。但是，在使用此模式之前，請諮詢您選擇的AWS合作夥伴，因為這取決於供應商的支持和實施。
- 記下GWLB閒置逾時。這可能會導致用戶端上的連線逾時。您可以在客戶端，服務器，網絡牆和操作系統級別上調整超時以避免這種情況。如需詳細資訊，請參閱部署閘道 Load Balancer 部落格文章中的第 1 節：調整TCP保持活動或逾時值以支援長壽TCP命值。
- GWLBE由供電 AWS PrivateLink，因此將 AWS PrivateLink 收取費用。您可以在AWS PrivateLink 定價頁面了解更多信息。如果您將集中式模型與 Transit Gateway 搭配使用，則需支付TGW資料處理費用。
- 請考慮在個別的網路服務帳戶VPC中部署 Transit Gateway 和出口，以根據職責委派來隔離存取，例如只有網路系統管理員可以存取網路服務帳戶。

集中式輸出 IPv6

若要在具有集中式IPv6輸出的雙堆疊部署中支援IPv4輸出，必須選擇下列其中一種模式：

- 具有分散IPv6式IPv4出口的集中式出口
- 集中式IPv4出口和集中IPv6輸出

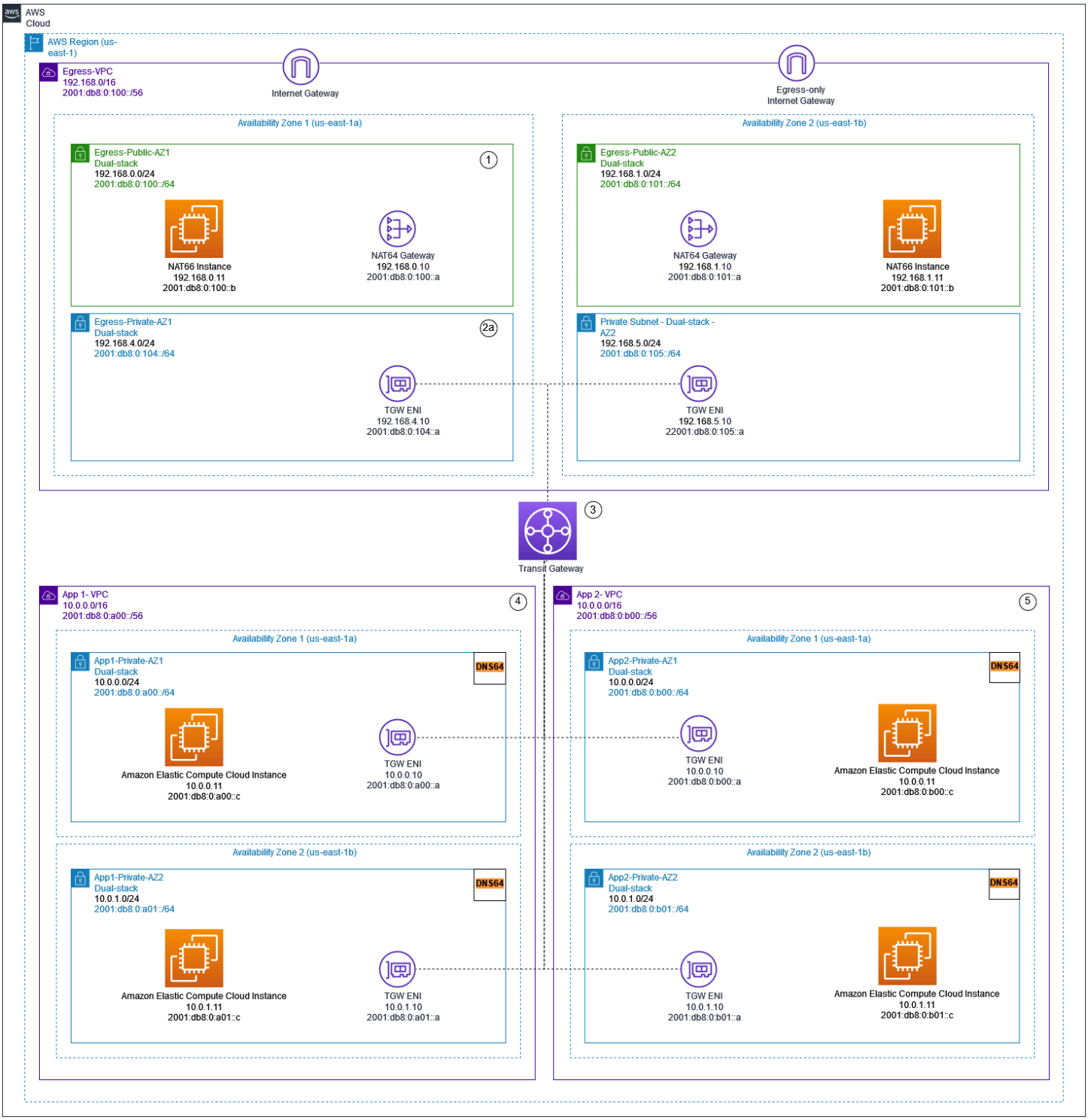
在下圖所示的第一個模式中，每個網輻中都會部署僅限輸出的網際網路閘道。VPC僅限 EGRES 的網際網路閘道是水平擴充、冗餘且高可用性的閘道，允許IPv6從您內部的執行個體傳出通訊。VPC它們可防止網際網路啟動與執行個體的IPv6連線。僅限輸出的網際網路閘道不收費。在此部署模型中，IPv6流量會從每個閘道的僅限輸出網際網路閘道流出，VPC而流量則會IPv4流過部署的集中式NAT閘道。



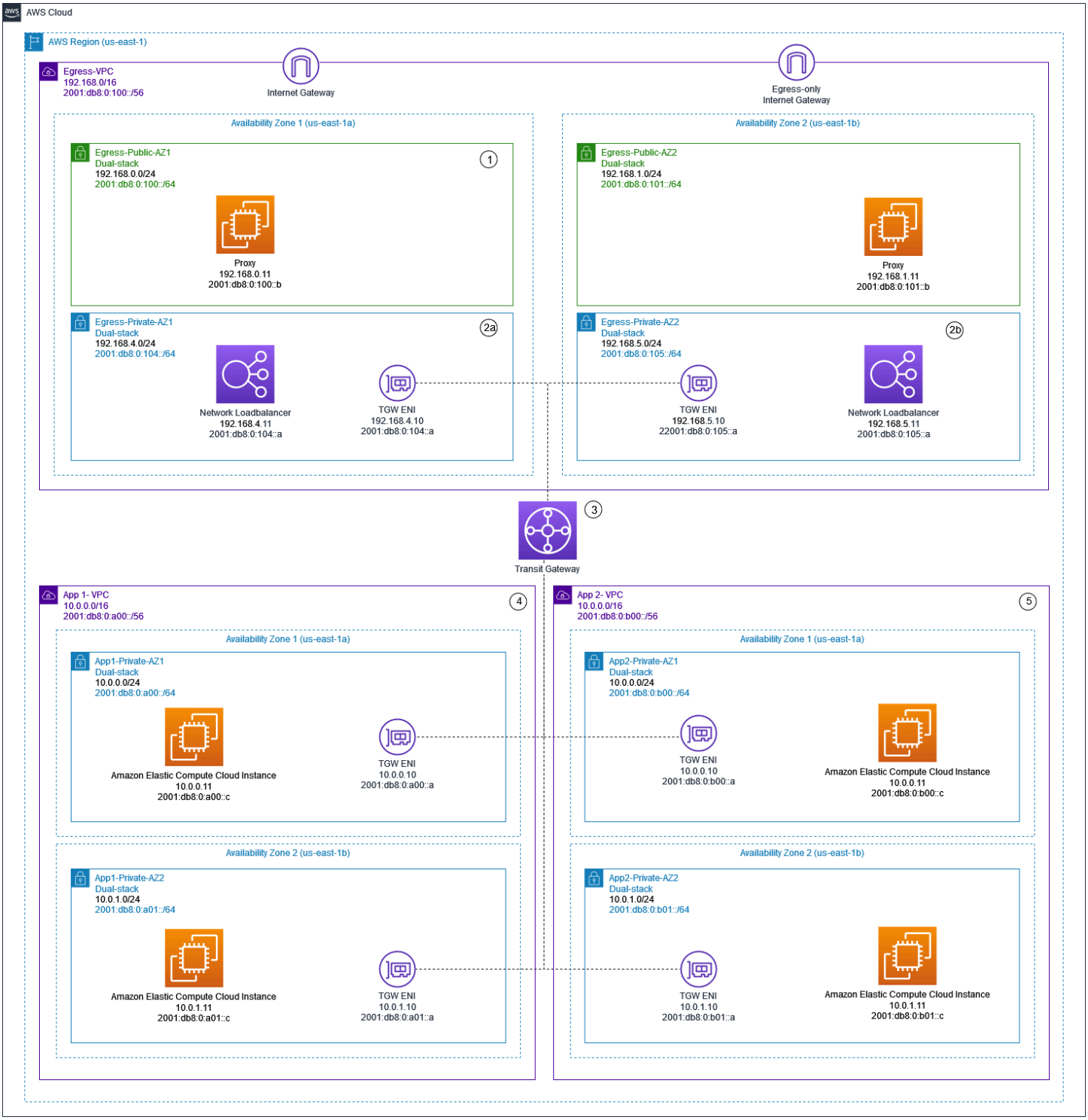
集中式IPV4出口和僅IPv6分散式輸出

在下圖所示的第二個模式中，會將執行個體的輸出IPv6流量傳送至集中VPC式。這可以透過在NAT66執行個體和NAT閘道上使用 IPv6-to-IPv6 網路前綴轉譯 (NPTv6)，或使用 Proxy 執行個體和 Network

Load Balancer 來完成。如果需要對輸出流量進行集中式流量檢查，且無法在每個網輻中執行此模式，則適用此模式VPC。



使用IPv6NAT閘道和NAT66執行個體集中輸出



使用 Proxy 執行個體IPv4和 Network Load Balancer 進行集中和IPv6輸出

AWS白皮書說明集中式IPv6出口模式。IPv6出IPv6口模式將在部落格中詳細討論雙堆疊的集中式輸出網際網路流量 IPv6VPCs，以IPv4及特殊考量、範例解決方案和圖表。

針對虛擬私人雲端到 VPC 以及內部部署至 VPC 流量的集中式網路安全性

在某些情況下，客戶可能會想要在其多帳戶環境中實作第 3-7 層的網路 /IP/ID，以檢查 VPC 之間 (東西流量) 或內部部署資料中心與 VPC (南北流量) 之間的交通。這可以實現不同的方式，具體取決於用例和要求。例如，您可以合併閘道 Load Balancer、Network Firewall、傳輸 VPC，或使用集中式架構搭配傳輸閘道。這些案例將在下一節中討論。

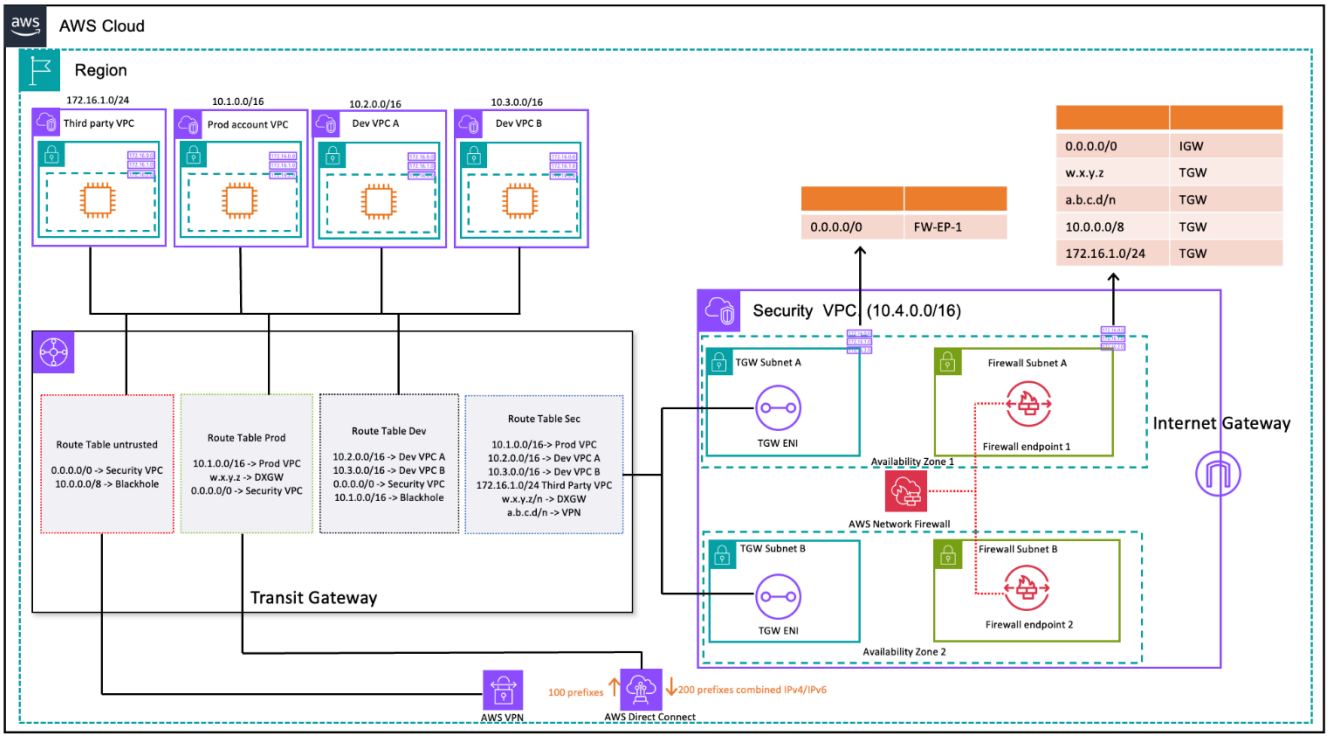
使用集中式網路安全性檢查模型的考量

若要降低成本，您應該選擇透過 AWS Network Firewall 或閘道 Load Balancer 傳遞的流量。繼續進行的方法之一是定義安全區域並檢查不受信任區域之間的流量。不受信任的區域可以是由協力廠商管理的遠端網站、您不控制/信任的廠商 VPC，或是沙箱 /dev VPC，與您的其他環境相比，其安全規則更寬鬆。此範例中有四個區域：

- 不受信任區域 — 這適用於來自「VPN 到遠端不受信任網站」或第三方廠商 VPC 的任何流量。
- 生產 (產品) 區域 — 包含來自生產 VPC 和內部部署客戶 DC 的流量。
- 開發 (開發) 區域 — 包含來自兩個開發 VPC 的流量。
- 安全性 (秒) 區域 — 包含我們的防火牆元件 Network Firewall 或閘道 Load Balancer。

此設定有四個安全性區域，但您可能會有更多安全性區域。您可以使用多個路由表和黑洞路由來實現安全隔離和最佳流量。選擇正確的區域集取決於您的整體著陸區設計策略（帳戶結構，VPC 設計）。您可以擁有區域來啟用業務單位 (BUS)、應用程式、環境等之間的隔離。

如果您想要檢查和篩選虛擬私人雲端到虛擬私人雲端、區域間流量和 VPC 人雲端內部部署流量，您可以在集中式架構中與 Transit Gateway 合併 AWS Network Firewall 。藉由具有的 hub-and-spoke 模型 AWS Transit Gateway，可以實現集中式部署模型。會部署 AWS Network Firewall 在單獨的安全性 VPC 中。單獨的安全 VPC 提供了一種簡化和集中的方法來管理檢查。這樣的 VPC 架構可提供 AWS Network Firewall 來源和目標 IP 的可見性。來源和目標 IP 都會保留。此安全性 VPC 由每個可用區域中的兩個子網路組成；其中一個子網路專用於 AWS Transit Gateway 附件，而另一個子網路則專用於防火牆端點。此 VPC 中的子網路應該只包含 AWS Network Firewall 端點，因為 Network Firewall 無法檢查與端點位於相同子網路中的流量。當您使用 Network Firewall 集中檢查流量時，它可以對輸入流量執行深度封包檢查 (DPI)。DPI 模式在本 paper 的「集中式入站檢查」一節中進行了擴展。



使用 Transit Gateway 和 (路由表設計) 檢查 VPC 到 VPC 以及內部部署至 VPC 流量檢查 AWS Network Firewall

在具有檢查功能的集中式架構中，Transit Gateway 子網路需要個別的 VPC 路由表，以確保流量會轉送至相同可用區域內的防火牆端點。對於回程流量，會設定包含通往 Transit Gateway 的預設路由的單一 VPC 路由表。通過 AWS Network Firewall檢查流量之後，流量會返回到相同的可用區域 AWS Transit Gateway 中。這是可能的，由於 Transit Gateway 的設備模式功能。Transit Gateway 的設備模式功能也有助 AWS Network Firewall 於在安全 VPC 內部具有狀態流量檢查功能。

在傳輸閘道上啟用設備模式後，它會在連線的整個生命週期內使用流程雜湊演算法選取單一網路介面。傳輸閘道對傳回流量使用相同的網路界面。這可確保雙向流量會對稱路由，在流量的存留期內透過 VPC 連接中相同的可用區域路由傳送。如需有關設備模式的詳細資訊，請參閱 Amazon VPC 文件中的可設定狀態設備和設備模式。

如需使用 AWS Network Firewall 和 Transit Gateway 的安全 VPC 的不同部署選項，請參閱 AWS Network Firewall 部落格文章的部署模型。

使用閘道 Load Balancer 搭配 Transit Gateway 來實現集中式網路

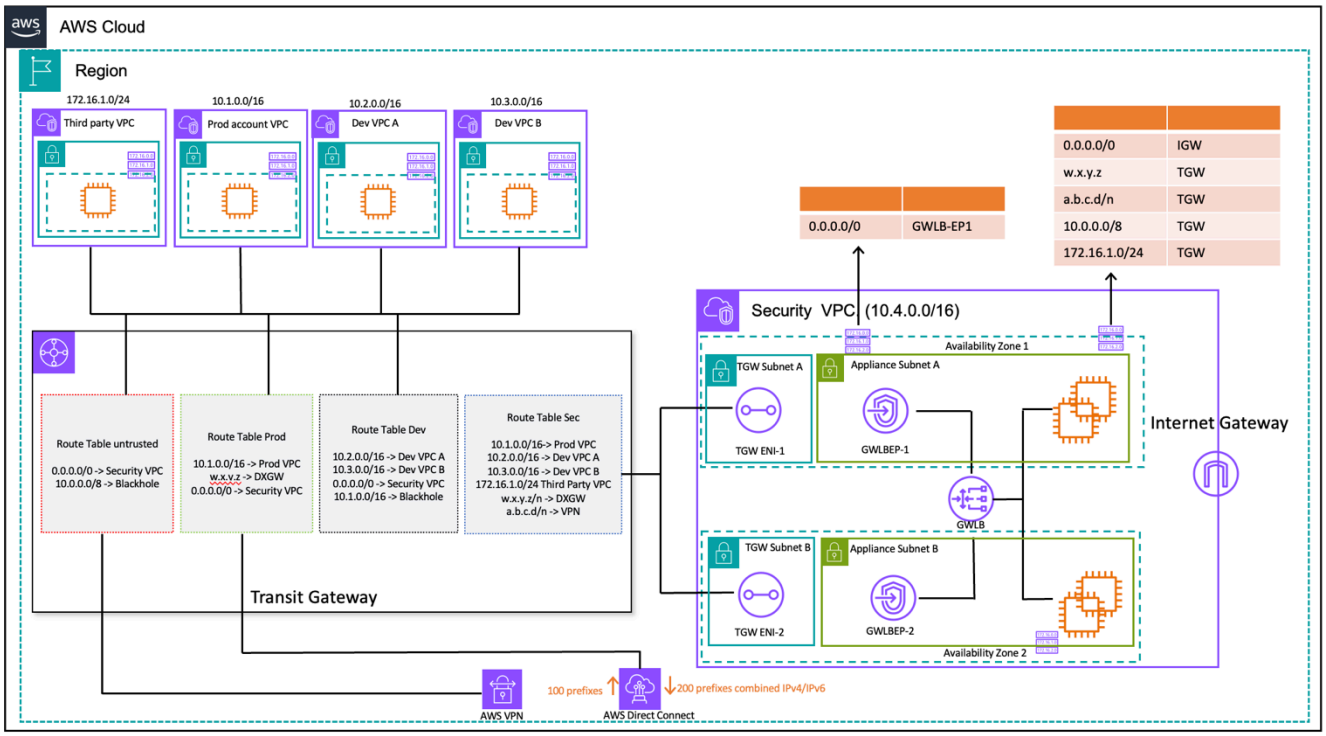
客戶通常會希望整合虛擬應用裝置來處理流量篩選，並提供安全性檢查功能。在這種使用案例中，他們可以整合閘道 Load Balancer、虛擬應用裝置和 Transit Gateway，以部署集中式架構以檢查 VPC 到 VPC 和 VPC 流量。to-on-premises

閘道 Load Balancer 與虛擬應用裝置一起部署在單獨的安全性 VPC 中。將檢查流量的虛擬應用裝置設定為閘道 Load Balancer 後方的目標。由於閘道 Load Balancer 端點是可路由的目標，因此客戶可以將流量路由傳 Transit Gateway 移至虛擬應用裝置叢集。為確保流量對稱，Transit Gateway 上已啟用設備模式。

每個網輻 VPC 都有一個與 Transit Gateway 相關聯的路由表，該表格具有通往 Security VPC 附件的預設路由作為下一個躍點。

集中式安全性 VPC 由每個可用區域中的應用裝置子網路組成，這些子網路具有閘道 Load Balancer 端點和虛擬應用裝置。它也在每個可用區域中都有 Transit Gateway 附件的子網路，如下圖所示。

如需使用閘道 Load Balancer 和傳輸閘道進行集中式安全檢查的詳細資訊，請參閱 AWS 閘道 Load Balancer 的集中式檢查架構和 AWS Transit Gateway部落格文章。



使用傳輸閘道和 AWS 閘道 Load Balancer (路由表設計) 進行 on-premises-to VPC 到 VPC 和-VPC 流量檢查

AWS Network Firewall 和 AWS 閘道 Load Balancer 的重要考量

- 執行東西向檢查時，應在 Transit Gateway 上啟用設備模式。
- 您可以 AWS 區域 使用「AWS Transit Gateway」區域間對等，部署相同的模型，以檢查其他流量。
- 根據預設，部署在可用區域中的每個閘道 Load Balancer 只會將流量分配到相同可用區域內的已註冊目標。這稱為可用性區域相似性。如果啟用跨區域負載平衡，閘道 Load Balancer 會在所有已啟用的

可用區域中，將流量分散到所有已註冊且運作良好的目標。如果所有可用區域中的所有目標運作狀況不良，則閘道 Load Balancer 會失敗開啟。如需詳細資訊，請參閱部署閘道 Load Balancer 部落格文章中的第 4 節：瞭解應用裝置和可用區域失敗案例。

- 對於多區域部署， AWS 建議您在個別的本機區域中設定個別的檢查 VPC，以避免區域間的相依性並降低相關的資料傳輸成本。您應該檢查當地區域的流量，而不是將檢查集中到另一個區域。
- 在多區域部署中執行額外以 EC2 為基礎的高可用性 (HA) 對的成本可能會增加。如需詳細資訊，請參閱部署閘道 Load Balancer 的最佳做法部落格文章。

AWS Network Firewall 與閘道 Load Balancer

表 2 — AWS Network Firewall 與閘道 Load Balancer

條件	AWS Network Firewall	Gateway Load Balancer
使用案例	具有狀態的託管網絡防火牆，具有入侵檢測和預防服務功能，與 Suricata 兼容。	託管服務可輕鬆部署、擴展和管理第三方虛擬設備
复杂性	AWS 託管服務。 AWS 處理服務的可擴展性和可用性。	AWS 受管服務。 AWS 將處理閘道 Load Balancer 服務的延展性和可用性。客戶負責管理閘道 Load Balancer 後方虛擬應用裝置的擴展和可用性。
比例	AWS Network Firewall 端點由提供電源 AWS PrivateLink。Network Firewall 每個防火牆端點最多支援 100 Gbps 的網路流量。	閘道 Load Balancer 端點支援每個端點最高 100 Gbps 的頻寬
成本	AWS Network Firewall 端點成本 + 資料處理費	閘道 Load Balancer + 閘道 Load Balancer 端點 + 虛擬應用裝置 + 資料處理費用

集中式入境檢查

面向 Internet 的應用程序本質上具有更大的攻擊面，並且暴露於大多數其他類型的應用程序不必面對的威脅類別。擁有必要的保護，以免對這些類型的應用程序的攻擊，並最大程度地減少影響表面積，是任何安全策略的核心部分。

當您在著陸區部署應用程式時，使用者會透過公用網際網路存取許多應用程式 (例如，透過內容傳遞網路 (CDN) 或透過公開的網路應用程式)，透過公用負載平衡器、API 閘道或直接透過網際網路閘道存取。在這種情況下，您可以使用 AWS Web 應用程式防火牆 (AWS WAF) 進行入站應用程式檢查，或者使用閘道 Load Balancer 或 IDS/IPS 入站檢查來保護工作負載和應用程式。 AWS Network Firewall

當您繼續在著陸區域部署應用程式時，您可能需要檢查傳入的網際網路流量。您可以通過多種方式實現這一目標，使用分散式、集中式或組合檢測架構，使用 Gateway Load Balancer 執行您的第三方防火牆應 AWS Network Firewall 用裝置，或透過使用開放原始碼 Suricata 規則提供進階 DPI 和 IDS/IPS 功能。本節涵蓋閘道 Load Balancer 和集 AWS Network Firewall 中式部署，使用 AWS Transit Gateway 作為路由流量的中央中樞。

AWS WAF 並檢 AWS Firewall Manager 查來自互聯網的入站流量

AWS WAF 是一種 Web 應用程式防火牆，可協助保護您的 Web 應用程式或 API，以防止可能影響可用性、危害安全性或耗用過多資源的常見 Web 入侵程式和機器人。 AWS WAF 讓您能夠建立安全規則來控制機器人流量並封鎖常見攻擊模式，例如 SQL 插入或跨網站指令碼 (XSS)，讓您控制流量到達應用程式的方式。您也可以自訂篩選出特定流量模式的規則。

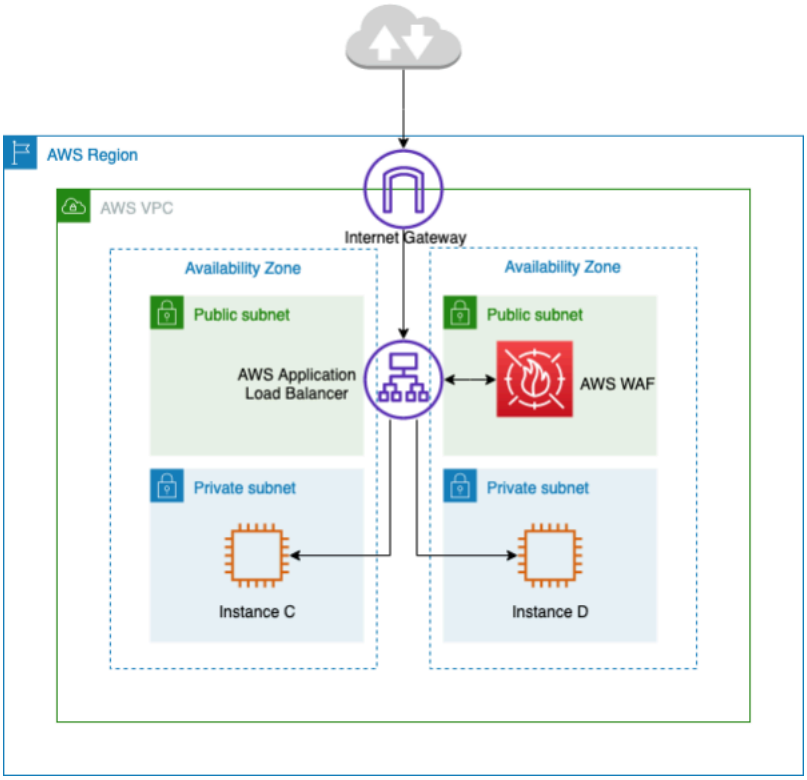
您可以 AWS WAF 在 Amazon 上部署 CloudFront 作為 CDN 解決方案的一部分、在網路伺服器前端的 Application Load Balancer 器、REST API 的 Amazon API 閘道，或 AWS AppSync 針對 GraphQL API API 進行部署。

部署之後 AWS WAF，您就可以使用視覺化規則產生器、JSON 中的程式碼、由維護的受管規則建立自己的流量篩選規則 AWS，或者您也可以從 AWS Marketplace. 這些規則可以根據指定的模式評估流量，以過濾掉不需要的流量。您可以進一步使 CloudWatch 用 Amazon 監控傳入流量指標和記錄。

若要集中管理中的所有帳戶和應用程式 AWS Organizations，您可以使用 AWS Firewall Manager。AWS Firewall Manager 是一項安全管理服務，可讓您集中配置和管理防火牆規則。建立新應用程式時， AWS Firewall Manager 透過強制執行一組通用的安全規則，輕鬆地將新的應用程式和資源納入法規遵循。

使用時 AWS Firewall Manager，您可以輕鬆地為應用程式負載平衡器、API Gateway 執行個體和 Amazon CloudFront 分發推出 AWS WAF 規則。 AWS Firewall Manager 與 in 整 AWS 受管規則 合

AWS WAF，可讓您在應用程式上部署預先設定的策劃 AWS WAF 規則的簡單方法。如需集中管理 AWS WAF 的詳細資訊 AWS Firewall Manager，請參閱集中管理 AWS WAF (API v2) AWS 受管規則以及使用 AWS Firewall Manager.



使用集中式入站流量檢查 AWS WAF

在先前的架構中，應用程式在私有子網路中多個可用區域的 Amazon EC2 執行個體上執行。Amazon EC2 執行個體前面部署了一個面向公開的應用程式負載平衡器 (ALB)，用於平衡不同目標之間的請求。與 AWS WAF ALB 相關聯。

優點

- 透過 AWS WAF Bot Control，您可以掌握和控制應用程式的常見和普遍的機器人流量。
- 使用的受管規則 AWS WAF，您可以快速開始使用，並保護您的 Web 應用程式或 API 免受常見威脅。您可以從許多規則類型中進行選擇，例如解決問題的規則類型，例如開放 Web 應用程式安全性專案 (OWASP) 十大安全風險、內容管理系統 (CMS) (例如 WordPress Joomla) 的特定威脅，甚至是新興的常見弱點和曝光 (CVE)。受管規則會在新問題出現時自動更新，因此您可以花更多時間建置應用程式。
- AWS WAF 是受管理的服務，在此架構中檢查不需要任何設備。此外，它還透過 Amazon 資料 Firehose 提供近乎即時的日誌。 AWS WAF 提供近乎即時的網路交易可見性，您可以使用這些交易在 Amazon 中建立新規則或警示。 CloudWatch

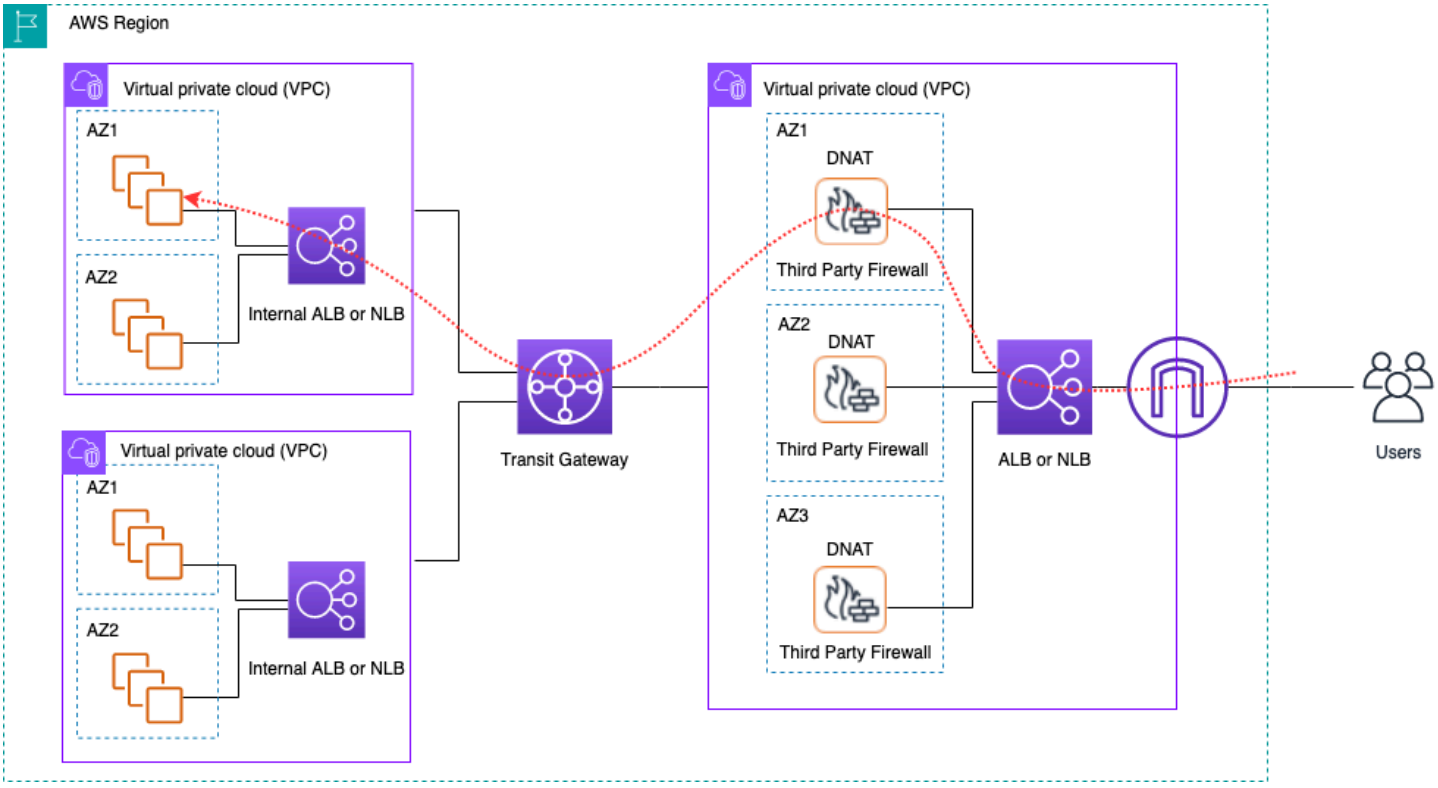
關鍵考量

- 此架構最適合用於 HTTP 標頭檢查和分散式檢測，因 AWS WAF 為整合在每個 ALB、散 CloudFront 發和 API Gateway 上。 AWS WAF 不記錄請求主體。
- 進入第二組 ALB（如果存在）的流量可能不會被相同的 AWS WAF 實例檢查; 因為將對第二組 ALB 發出新的請求。

使用第三方設備進行集中檢查

在此架構設計模式中，您可以在 Amazon EC2 上跨 Elastic Load Balancer (ELB) 後面的多個可用區域 (例如應用程式/Network Load Balancer) 在個別的檢驗 VPC 中部署第三方防火牆設備。

檢測 VPC 以及其他輻條 VPC 會透過 Transit Gateway 作為 VPC 附件連接在一起。輻條 VPC 中的應用程式是內部 ELB 的前端，視應用程式類型而定，可以是 ALB 或 NLB。透過網際網路的用戶端會連線至檢查 VPC 中的外部 ELB 的 DNS，該檢查 VPC 會將流量路由傳送至其中一個防火牆應用裝置。防火牆會檢查流量，然後使用內部 ELB 的 DNS，透過 Transit Gateway 將流量路由至支點 VPC，如下圖所示。如需使用第三方設備進行入站安全檢查的詳細資訊，請參閱如何將第三方防火牆設備整合到 AWS 環境部落格文章。



使用第三方設備和 ELB 集中進入流量檢查

優點

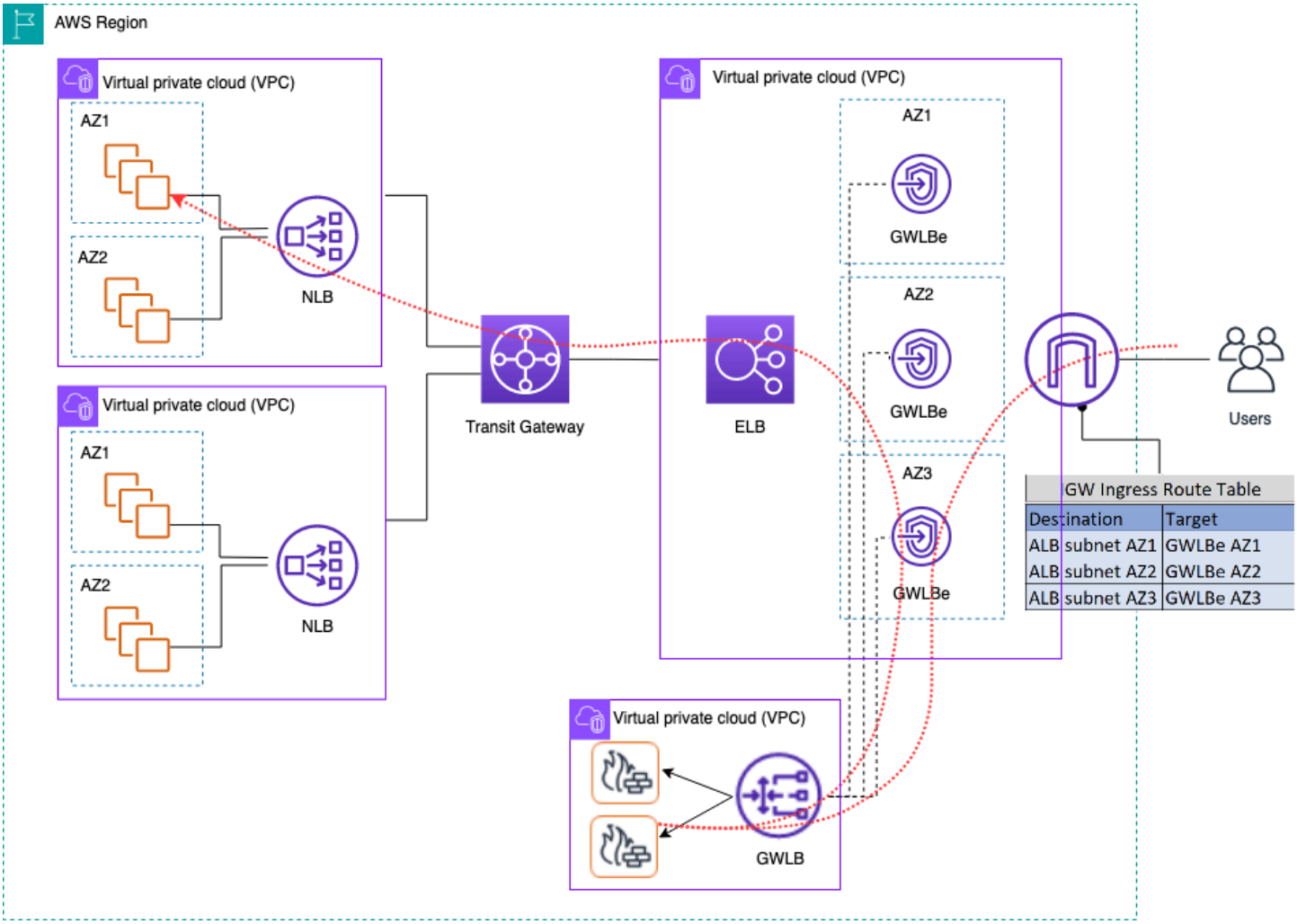
- 此架構可支援透過協力廠商防火牆設備提供的任何應用程式類型的檢測和進階檢測功能。
- 此病毒碼支援從防火牆應用裝置到支點 VPC 的 DNS 路由，這可讓網輻 VPC 中的應用程式在 ELB 之後獨立擴充。
- 您可以將 Auto Scaling 與 ELB 搭配使用，以擴展檢測 VPC 中的防火牆應用裝置。

關鍵考量

- 您需要跨可用區域部署多個防火牆應用裝置，以獲得高可用性。
- 防火牆必須設定並執行來源 NAT，才能維持流程對稱性，這表示應用程式將看不到用戶端 IP 位址。
- 請考慮在網路服務帳戶中部署 Transit Gateway 和檢查 VPC。
- 其他協力廠商防火牆授權/支援費用。Amazon EC2 費用取決於執行個體類型。

使用防火牆應用裝置與閘道 Load Balancer 檢查來自網際網路的輸入流

客戶使用第三方新世代防火牆 (NGFW) 和入侵防禦系統 (IPS) 作為其深度防禦策略的一部分。 傳統上，這些通常是專用的硬件或軟件/虛擬設備。您可以使用閘道 Load Balancer 水平擴展這些虛擬應用裝置，以檢查來自 VPC 和傳送至 VPC 的流量，如下圖所示。



使用防火牆應用裝置搭配閘道 Load Balancer 進行集中式輸入

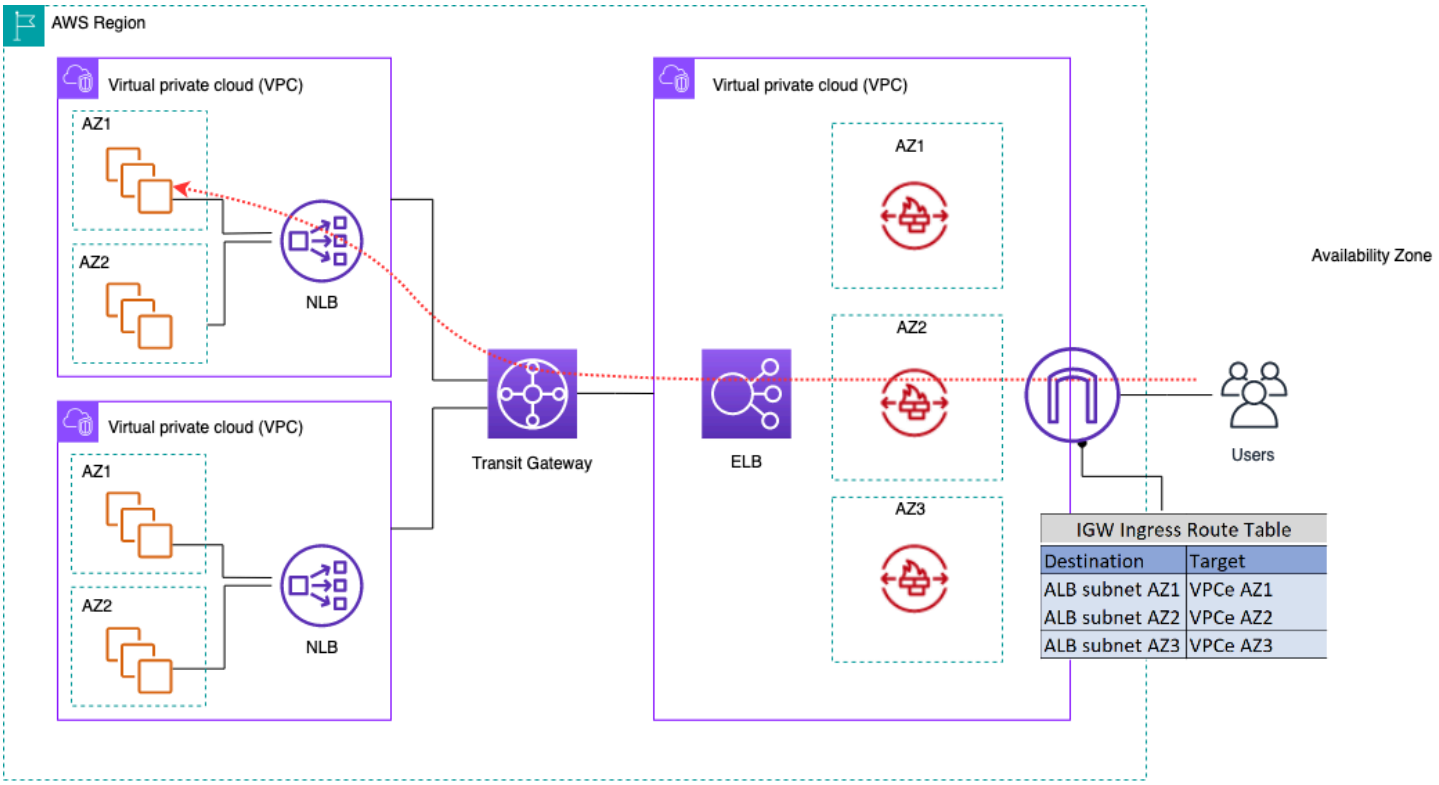
在先前的架構中，閘道 Load Balancer 端點會部署到個別邊緣 VPC 中的每個可用區域。新一代防火牆、入侵防護系統等部署在集中式設備 VPC 中的閘道 Load Balancer 後方。此設備 VPC 可以位於與支點 VPC 相同的 AWS 帳戶或不同的 AWS 帳戶。虛擬應用裝置可以設定為使用 Auto Scaling 群組，並自動向閘道 Load Balancer 註冊，以便自動調整安全層。

這些虛擬應用裝置可透過 Internet Gateway (IGW) 存取其管理介面，或使用應用裝置 VPC 中的防禦主機設定來管理。

使用 VPC 輸入路由功能，邊緣路由表會更新，以將來自網際網路的輸入流量路由到閘道 Load Balancer 後方的防火牆應用裝置。已檢查的流量會透過閘道 Load Balancer 端點路由至目標 VPC 執行個體。如需各種使用AWS 閘道 Load Balancer 方式的詳細資訊，請參閱閘道 Load Balancer 簡介：支援的架構模式部落格文章。

使用集 AWS Network Firewall 中式輸入

在此架構中，入口流量會在到達 VPC 的其餘部分 AWS Network Firewall 之前進行檢查。在此設定中，流量會在 Edge VPC 中部署的所有防火牆端點之間分割。您可以在防火牆端點和 Transit Gateway 子網路之間部署公用子網路。您可以使用 ALB 或 NLB，其中包含您的分支 VPC 中的 IP 目標，同時為其後面的目標處理 Auto Scaling。

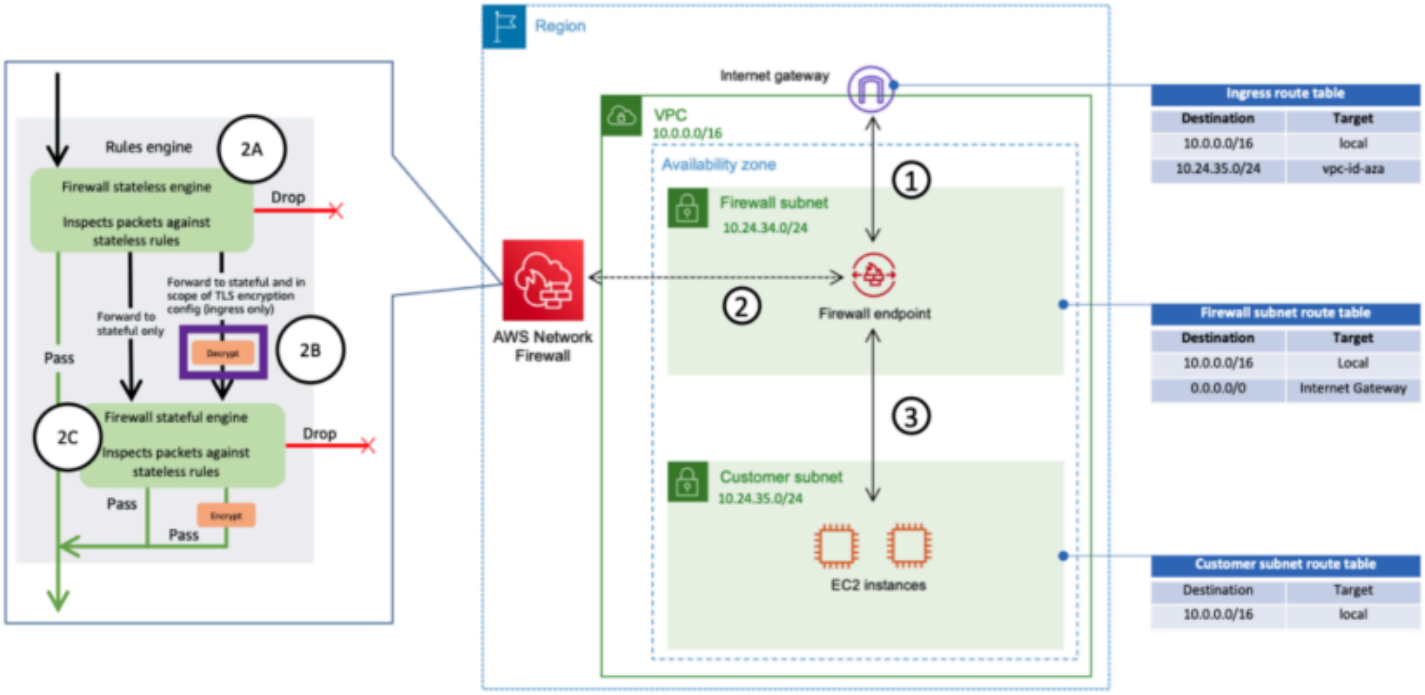


使用 AWS Network Firewall 進行入口流量檢查

為了簡化此模型 AWS Network Firewall 中的部署和管理， AWS Firewall Manager 可以使用。Firewall Manager 可讓您自動將您在集中式位置建立的保護套用至多個帳戶，藉此集中管理不同的防火牆。Firewall Manager 員支援 Network Firewall 的分散式和集中式部署模式。部落格文章如何使用部署 AWS Network Firewall 提 AWS Firewall Manager供有關模型的更多詳細資訊。

深度封包檢測 (DPI) 搭配 AWS Network Firewall

Network Firewall 可以對輸入流量執行深度封包檢查 (DPI)。使用儲存在 (ACM) 中的傳輸層安全性 AWS Certificate Manager (TLS) 憑證，Network Firewall 可以解密封包、執行 DPI，以及重新加密封包。使用 AnetWork 防火牆設定 DPI 時，有幾個注意事項。首先，受信任的 TLS 憑證必須儲存在 ACM 中。其次，Network Firewall 規則必須設定為正確傳送封包以進行解密和重新加密。如需詳細資訊，請參閱部落格文章 TLS 檢查設定以瞭 AWS Network Firewall解加密流量。



使用具有 DPI 的 Network Firewall 進行入口流量檢查

集中式輸入 AWS Network Firewall 架構中的關鍵考量

- Edge VPC 中的 Elastic Load Balancing 只能將 IP 位址作為目標類型，而不能使用主機名稱。在上圖中，目標是網輻 VPC 中 Network Load Balancer 的專用 IP。在邊緣 VPC 中使用 ELB 後面的 IP 目標會導致遺失 Auto Scaling。
- 請考慮 AWS Firewall Manager 將防火牆端點當作單一窗格使用。
- 此部署模型會在進入邊緣 VPC 時使用流量檢查，因此有可能降低檢測架構的整體成本。

DNS

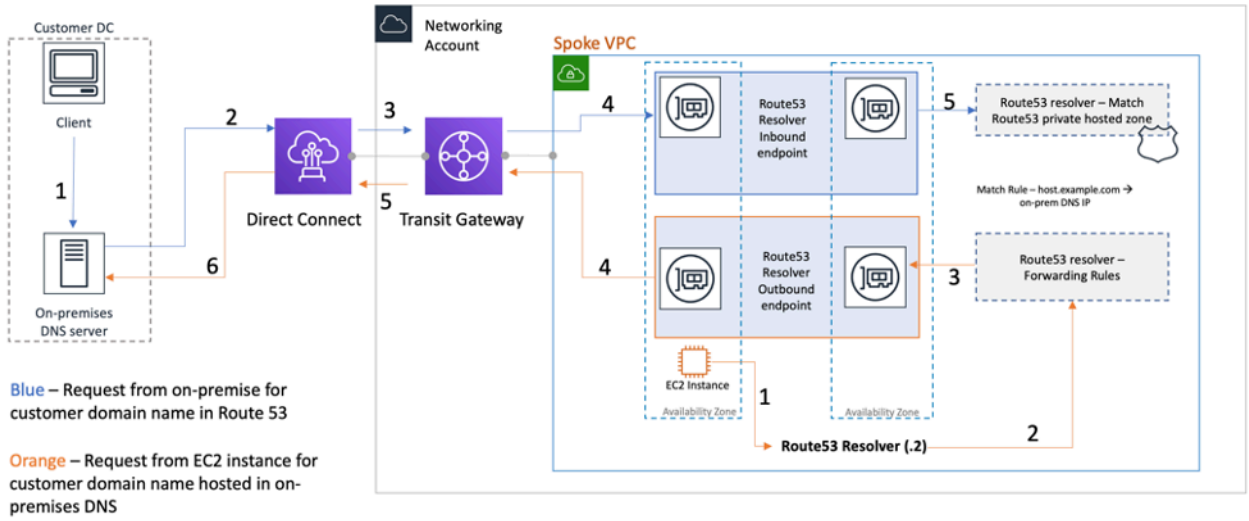
當您將執行個體啟動到 VPC (不包括預設 VPC) 時，會根據您為 VPC 指定的 DNS 屬性以及執行個體是否具有公用 IPv4 位址，為執行個體 AWS 提供私人 DNS 主機名稱 (可能是公用 DNS 主機名稱)。當enableDnsSupport屬性設定為時true，您可以從路由 53 解析器 (VPC CIDR 的 IP 偏移量 +2) 取得 VPC 內的 DNS 解析。根據預設，Route 53 解析器會回答 VPC 網域名稱的 DNS 查詢，例如 EC2 執行個體的網域名稱或 Elastic Load Balancing 負載平衡器。透過 VPC 對等互連，只要啟用此功能的選項，一個 VPC 中的主機就可以將公用 DNS 主機名稱解析為對等 VPC 中執行個體的私有 IP 位址。這同樣適用於透過 AWS Transit Gateway連接的 VPC。如需詳細資訊，請參閱啟用 VPC 對等連線的 DNS 解析 Support。

如果您想將執行個體對應至自訂網域名稱，可以使用 Amazon Route 53 建立自訂 DNS 到 IP 對應記錄。Amazon Route 53 託管區域是一個容器，其中包含您希望 Amazon Route 53 如何回應網域及其子網域的 DNS 查詢的相關資訊。公用託管區域包含可透過公用網際網路解析的 DNS 資訊，而私有託管區域則是特定的實作，僅向已附加至特定私有託管區域的 VPC 顯示資訊。在您擁有多個 VPC 或帳戶的登陸區域設定中，您可以將單一私有託管區域與 AWS 帳戶和跨區域的多個 VPC 建立關聯 (僅適用於 SD K/CLI I/API)。VPC 中的最終主機會使用其各自的路由 53 解析器 IP (VPC CIDR 位移 +2) 做為 DNS 查詢的名稱伺服器。VPC 中的 Route 53 解析器僅接受來自 VPC 內資源的 DNS 查詢。

混合式 DNS

DNS 是任何基礎結構的重要組成部分，無論是混合或其他方式，因為它提供了應用程序依賴的主機名稱到 IP 地址解析。實作混合式環境的客戶通常已經有 DNS 解析系統，而且他們想要能與目前系統配合運作的 DNS 解決方案。無法使用 VPN 或從內部部署網路存取原生路由 53 解析程式 (基礎 VPC CIDR 設定 +2 個)。 AWS Direct Connect因此，當您將 AWS 區域中 VPC 的 DNS 與網路的 DNS 整合時，您需要 Route 53 解析器入埠端點 (適用於您要轉寄至 VPC 的 DNS 查詢) 和 Route 53 解析器輸出端點 (適用於從 VPC 轉送至網路的查詢)。

如下圖所示，您可以設定輸出解析器端點，將其從 VPC 中的 Amazon EC2 執行個體接收的查詢轉寄到網路上的 DNS 伺服器。若要將選取的查詢轉寄至內部部署網路，請建立 Route 53 解析器規則，以指定您要轉寄之 DNS 查詢的網域名稱 (例如 example.com)，以及您網路上要轉寄查詢的 DNS 解析器 IP 位址。對於從內部部署網路到 Route 53 託管區域的輸入查詢，網路上的 DNS 伺服器可以將查詢轉送至特定 VPC 中的輸入解析器端點。

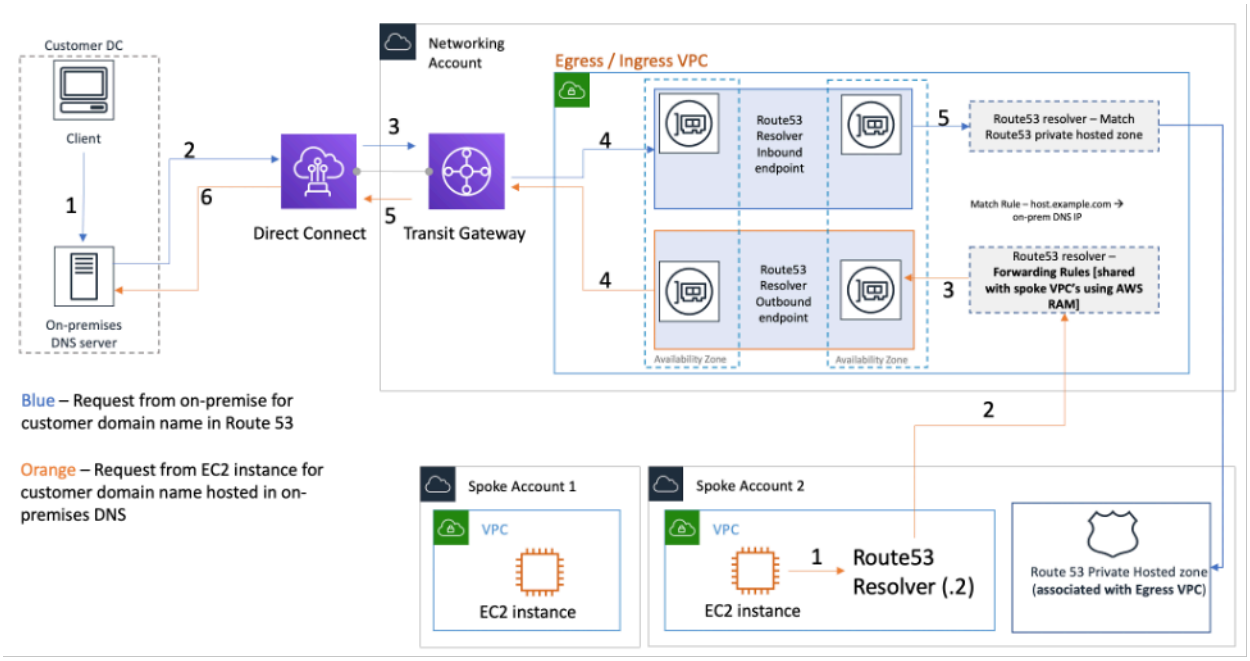


使用路由 53 解析器的混合式 DNS 解析

這可讓您的現場部署 DNS 解析器輕鬆解析 AWS 資源的網域名稱，例如 Amazon EC2 執行個體或 Route 53 私有託管區域中與該 VPC 相關聯的記錄。此外，Route 53 解析器端點每秒最多可處理 10,000 個查詢，因此可以輕鬆擴展到更大的 DNS 查詢量。如需詳細資訊，請參閱 Amazon Route 53 文件中的解析程式的最佳實務。

不建議您在著陸區的每個 VPC 中建立 Route 53 解析器端點。將它們集中在中央輸出 VPC (位於網路服務帳戶中)。這種方法可以提供更好的管理性，同時保持低成本（為您創建的每個輸入/出站解析器端點收取小時費用）。您可以與著陸區的其餘部分共用集中式的入站和出站端點。

- 輸出解析 — 使用網路服務帳戶來撰寫解析器規則 (根據哪些 DNS 查詢將轉送至內部部署 DNS 伺服器)。使用 Resource Access Manager (RAM)，與多個帳號共用這些 Route 53 解析器規則 (並與帳號中的 VPC 建立關聯)。支點 VPC 中的 EC2 執行個體可以傳送 DNS 查詢至 Route 53 解析器，而 Route 53 解析器服務會透過輸出 VPC 中的輸出 Route 53 解析器端點將這些查詢轉送至現場部署 DNS 伺服器。 您不需要將對等式支點 VPC 與出口 VPC，也不需要透過 Transit Gateway 連接它們。請勿使用輸出解析程式端點的 IP 做為支點 VPC 中的主要 DNS。網輻 VPC 應該在其 VPC 中使用路由 53 解析器 (以偏移 VPC CIDR)。



在入口/出口VPC 中集中路由 53 解析器端點

- 輸入 DNS 解析 — 在集中式 VPC 中建立 Route 53 解析器入埠端點，並將著陸區中的所有私有託管區域與此集中式 VPC 建立關聯。如需詳細資訊，請參閱將更多 VPC 與私有託管區域產生關聯。與 VPC 關聯的多個私人託管區域 (PHZ) 不能重疊。如上圖所示，此 PHZ 與集中式 VPC 的關聯可讓內部部署伺服器使用集中式 VPC 中的輸入端點，解析任何私有託管區域 (與中央 VPC 相關聯) 中任何項目的 DNS。 如需有關混合式 DNS 設定的詳細資訊，請參閱使用 Amazon Route 53 的混合雲集中式 DNS 管理和適用於 Amazon VPC 的 AWS Transit Gateway 和混合雲 DNS 選項。

Route 53 DNS 防火牆

Amazon Route 53 Resolver DNS 防火牆有助於篩選和管理 VPC 的輸出 DNS 流量。DNS 防火牆的主要用途是透過定義網域名稱允許清單 (允許 VPC 中的資源僅針對組織信任的網站提出輸出 DNS 要求)，協助防止資料外洩。它還可讓客戶為不希望 VPC 內的資源透過 DNS 與之通訊的網域建立封鎖清單。 Amazon Route 53 Resolver DNS 防火牆具有以下功能：

客戶可以建立規則來定義 DNS 查詢的回應方式。可針對網域名稱定義的動作包括`NODATA`、`OVERRIDE`和`NXDOMAIN`。

客戶可以為允許清單和拒絕清單建立警示，以監視規則活動。當客戶想要在將規則移至生產環境之前先測試規則時，這可能會派上用場。

如需詳細資訊，請參閱如何開始使用適用於 Amazon VPC 的 Amazon Route 53 Resolver DNS 防火牆部落格文章。

集中存取VPC私有端點

VPC端點可讓您以私密方式連線VPC至支援的AWS服務，而不需要網際網路閘道、NAT裝置、VPN連線或 AWS Direct Connect 連線。因此，您不VPC會暴露在公共互聯網上。您中的執行個體VPC不需要公用 IP 位址即可與具有此介面端點的AWS服務端點通訊。您VPC與其他服務之間的流量不會離開AWS網路骨幹。VPC端點是虛擬裝置。它們是水平縮放、備援和高可用性的VPC元件。目前可佈建兩種端點類型：介面端點 (由支援 AWS PrivateLink) 和閘道端點。閘道端點可用於私下存取 Amazon S3 和亞馬遜 DynamoDB 服務。使用閘道端點不需額外付費。需支付標準數據傳輸與資源使用費。

界面 VPC 端點

介面端點由一或多個具有私有 IP 位址的彈性網路介面組成，該網路介面可做為目標至支援 AWS 服務之流量的進入點。佈建介面端點時，會產生端點每小時執行的費用以及資料處理費用。根據預設，您可以在每VPC一個您想要存取 AWS 服務的介面端點中建立介面端點。在客戶希望跨多個特定AWS服務進行互動的著陸區設置中，這可能是成本高昂且具有挑戰性的。VPCs為了避免這種情況，您可以在集中託管接口端點VPC。所有支點都VPCs會透過 Transit Gateway 使用這些集中式端點。

當您建立 AWS 服務的VPC端點時，您可以啟用私有DNS。啟用時，此設定會建立AWS受管理的 Route 53 私有託管區域 (PHZ)，以便將公用 AWS 服務端點解析為介面端點的私有 IP。受管理PHZ僅適VPC用於介面端點。在我們的設置中，當我們希VPCs望輻條能夠解決集中DNS託管的VPC端點時VPC，託管將PHZ無法正常工作。若要解決這個問題，請停用在建立介面端點DNS時自動建立私有的選項。接下來，手動建立與服務端點名稱相符的 Route 53 私有託管區域，並新增具有完整 AWS 服務端點名稱指向介面端點的別名記錄。

1. 登入 AWS Management Console 並瀏覽至路線 53。
2. 選取私人託管區域，然後導覽至「建立記錄」。
3. 填入「記錄名稱」欄位，選取「記錄類型」作為 A，然後啟用「別名」。

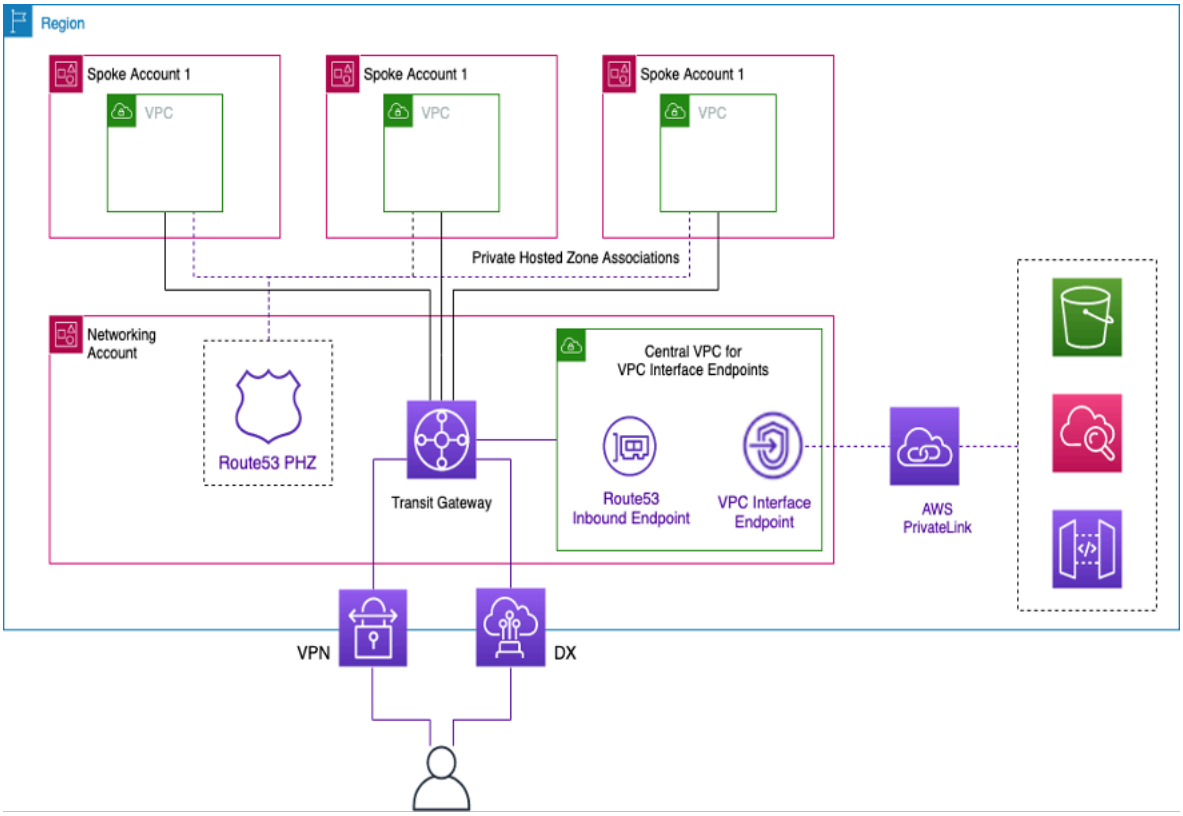
   請注意，某些服務 (例如 Docker 和用OCI戶端端點 (`dkr.ecr`)，需要使用萬用字元別名 (*) 作為記錄名稱。
4. 在將流量路由到部分下，選擇流量應發送到的服務，然後從下拉列表中選擇區域。
5. 選取適當的路由原則，並啟用評估目標健全狀況的選項。

您可以將此私人託管區域與著陸區VPCs內的其他區域建立關聯。此組態允許分支VPCs將全方位服務端點名稱解析為在集中式介面端點VPC。

> **Note**
>
> 若要存取共用私有託管區域，支點中的主機VPCs應使用其的 Route 53 解析程式 IP。VPC介面端點也可透過 VPN「直 Connect」從內部部署網路存取。使用條件式轉送規則，將全方位服務端點名稱的所有DNS流量傳送至 Route 53 Resolver 入埠端點，這會根據私有託管區域解決DNS要求。

在下圖中，Transit Gateway 會啟用從支點VPCs到集中式介面端點的流量流量。在網絡服務帳戶中為其創建VPC端點和私有託管區域，並與支點帳戶VPCs中的支點共享。如需與其他人共用端點資訊的詳細資訊VPCs，請參閱整合 AWS Transit Gateway AWS PrivateLink 與 Amazon Route 53 解析器部落格文章。

> **Note**
>
> 一種分散式VPC端點方法，即每個端點VPC允許您在VPC端點上套用最低權限策略。透過集中式方法，您可以針對單一端點上的所有分支VPC存取套用和管理原則。隨著數量的增加VPCs，使用單一政策文件維持最低權限的複雜性可能會增加。單一原則文件也會產生較大的爆炸半徑。您也受到政策文件的大小限制 (20,480 個字元)。



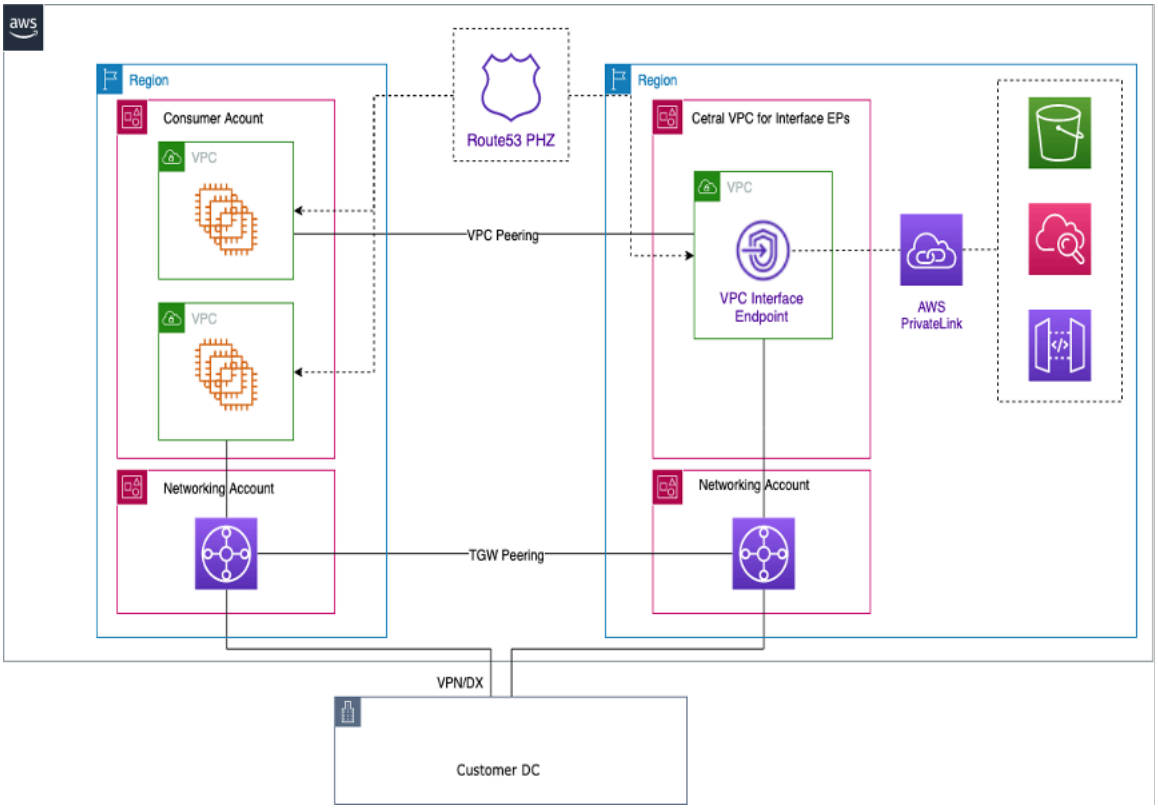
集中化介面端VPC點

跨區域端點存取

如果您想要在共用通用VPC端點的不同區域中進行多個VPCs設定，請使用先前所述的「」。PHZ每個區域VPCs中的兩者都將PHZ與端點的別名相關聯。為了在多區域架構VPCs中路由流量，每個區域的 Transit Gateway 都需要對等。如需詳細資訊，請參閱此部落格：針對跨帳戶多區域架構使用 Route 53 私有託管區域。

VPCs您可以使用「傳輸閘道」或「VPC對等互連」將來自不同區域的路由到另一個區域。請使用下列文件來進行對等傳輸閘道：傳輸閘道對等連接附件。

在此範例中，VPC`us-west-1`區域中的 Amazon EC2 執行個體將使用取PHZ得`us-west-2`區域中端點的私有 IP 地址，並VPC透過 Transit Gateway 對等或VPC對等互連將流量路由至`us-west-2`區域。使用此架構時，流量會保留在AWS網路內，讓EC2執行個體安全地存`us-west-1`取VPC服務，`us-west-2`而無需透過網際網路。



多區域端點 VPC

> **Note**
>
> 存取跨區域的端點時，需要支付區域間資料傳輸費用。

參照上圖，在區域中建立端點服us-west-2務。VPC此端點服務可讓您存取該區域中的AWS服務。為了讓其他區域中的執行個體 (例如us-east-1) 存取us-west-2區域中的端點，您需要在中建立位址記錄，並在中建立PHZ具有所需VPC端點的別名。

首先，請確定每個區域VPCs中的與您建立的區域PHZ相關聯。

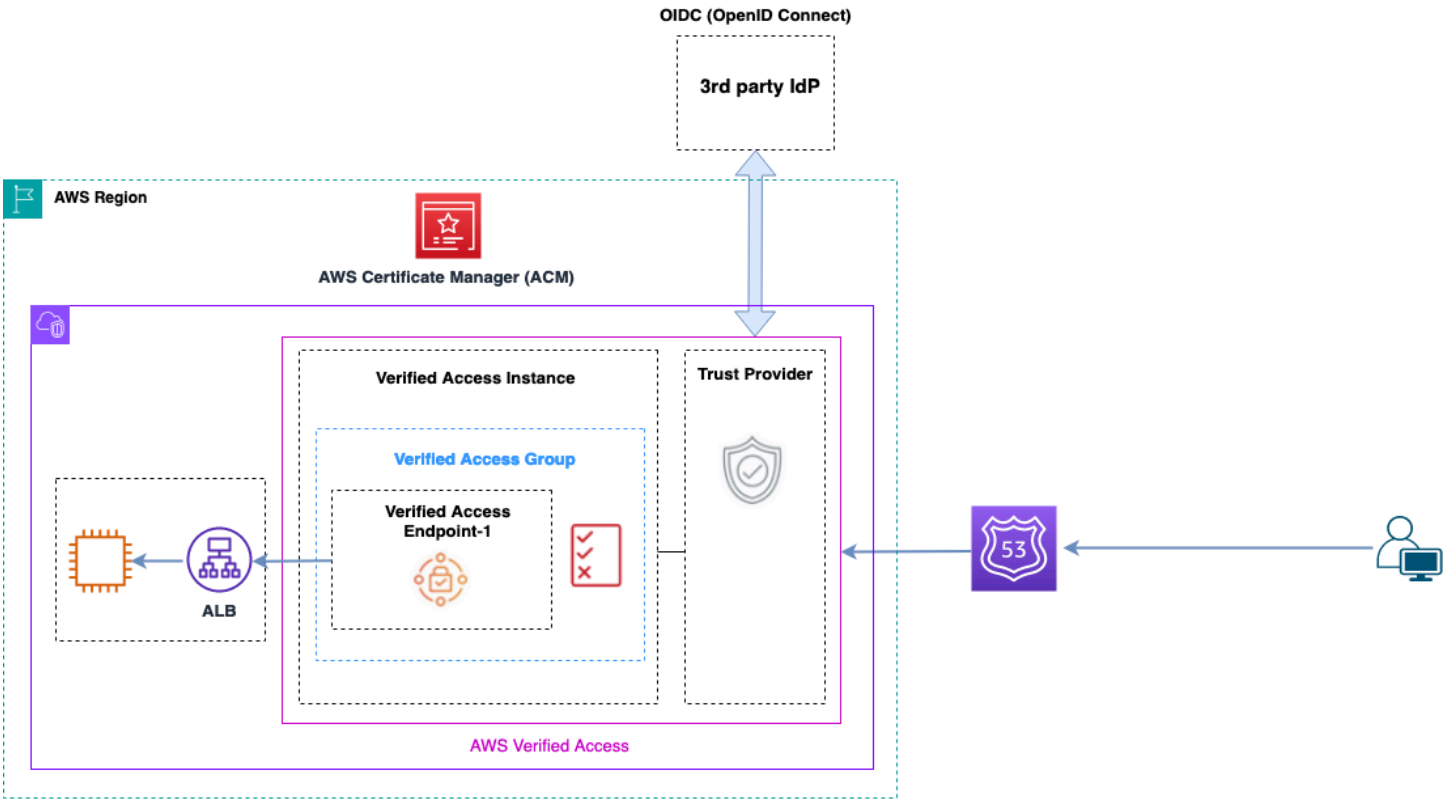
在多個可用區域中部署端點時，傳回來源端點的 IP 位址DNS將來自已配置之可用區域中的任何子網路。

呼叫端點時，請使用中的完整網域名稱 (FQDN)。PHZ

AWS Verified Access

AWS Verified Access 在私人網路中提供對應用程式的安全存取，而無需VPN. 它可以實時評估請求，例如身份，設備和位置。該服務授予基於應用程序的策略訪問，並通過提高組織的安全性連接用戶。驗證存取權可做為身分識別感知的反向 Proxy，提供對私有應用程式的存取。在將流量路由到應用程式之前，會先執行使用者身分和裝置健康狀況 (如果適用

下圖提供「已驗證存取權」的高階概觀。使用者傳送存取應用程式的要求。「已驗證存取」會根據群組和任何應用程式特定端點原則的存取原則來評估要求。如果允許存取，則會透過端點將要求傳送至應用程式。



已驗證存取概觀

在一個 AWS Verified Access 體系結構的主要組成部分是：

- 驗證存取執行個體 — 執行個體會評估應用程式要求，並僅在符合安全性需求時授予存取權。
- 已驗證存取端點 — 每個端點代表一個應用程式。端點可以是NLB，也可以ALB是網絡接口。
- 已驗證存取群組 — 已驗證存取端點的集合。建議您針對具有類似安全性需求的應用程式將端點分組，以簡化原則管理。
- 存取原則 — 一組使用者定義的規則，可決定是否允許或拒絕存取應用程式。

- 信任提供者 —「已驗證存取」是一項有助於管理使用者身分識別和裝置安全性狀態的服務。它與 AWS 和第三方信任提供者相容，要求每個「已驗證存取」執行個體至少附加一個信任提供者。每個執行個體都可以包含單一身分信任提供者以及多個裝置信任提供者。
- 信任資料 — 每次收到應用程式要求時，信任提供者傳送至「已驗證存取」的安全性資料，例如使用者的電子郵件地址或其所屬群組，都會根據您的存取原則進行評估。

更多詳細資訊可在驗證存取權部落格文章中找到。

結論

當您在 AWS 著陸區擴展應用程式的使用量 AWS 和部署時，VPC 和網路元件的數量也會增加。本白皮書說明如何管理這種不斷成長的基礎架構，確保可擴展性、高可用性和安全性，同時保持低成本。在使用傳輸閘道、共用 VPC、VPC 端點、閘道 Load Balancer AWS Direct Connect、Amazon Route 53 和第三方軟體設備等服務時 AWS Network Firewall，做出正確的設計決策變得至關重要。了解每種方法的關鍵考量因素，並根據您的需求向後進行分析，並分析哪種選項或選項組合最適合您是非常重要的。

貢獻者

以下人員為本文件做出了貢獻：

- 塔希爾, 解決方案架構師, Amazon Web Services
- 希林，解決方案架構師，Amazon Web Services
- 庫納爾潘薩里, 解決方案架構師, Amazon Web Services
- 埃里克·瓦斯克斯，解決方案架構師，Amazon Web Services
- 圖莎賈格代爾, 解決方案架構師, Amazon Web Services
- 阿米爾·謝里夫，解決方案架構師，Amazon Web Services
- 格倫·戴維斯，解決方案架構師，Amazon Web Services
- 尼克·克尼維頓，解決方案架構師，Amazon Web Services
- 賽達多·喬漢，首席解決方案架構師，Amazon Web Services

文件歷史記錄

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
重大更新	在白皮書中更新 CloudWAN、Amazon VPC 格子、ENA 快遞、混合式連線、 AWS Direct Connect 網站連結、深度封包檢測和. AWS Verified Access	2024年4月17日
次要更新	更新了圖表，使其更新後的 DX 連接選項更加一致，包括私有 IP VPN 以及整個過程中的許多微小更改。	2023 年 7 月 6 日
次要更新	更新 AWS Control Tower 資訊、反映各種服務的新輸送量限制、更新的 NAT 閘道圖表、集中輸出的更新安全性區段。	2023 年 4 月 4 日
次要更新	新增區段：跨區域端點存取。	2022 年 7 月 19 日
重大更新	更新了「Transit Gateway」部分，其中包含「傳輸 Transit Gateway Connect」，更新了「傳輸 VPC AWS Direct Connect 」部分；更新了 MacSec 和彈性建議的部分；更新部分。 AWS PrivateLink 新增 VPC 對等互連與傳輸 VPC 與傳 Transit Gateway 比較表；新增集中式傳入檢查區段；更新 VPC 到 VPC 和 VPC 內部部署到 VPC 的集中式網路安全性，以及使用閘道 Load	2022 年 2 月 22 日

	Balancer 設計模式集中輸出至網際網路；新增私有 NAT 閘道 AWS Network Firewall 和 Amazon Route 53 DNS 防火牆區段。	
次要更新	更新了 Transit Gateway 與 VPC 對等部分	2021 年 4 月 2 日
白皮書已更新	更正文字以符合 [圖 7] 中所示的選項	2020 年 6 月 10 日
初次出版	白皮書已發佈。	2019 年 11 月 15 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 及其關係企業、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。