AWS 白皮書

建置可擴展且安全的多 VPC AWS 網路基礎設施

建置可擴展且安全的多 VPC AWS 網路基礎設施: AWS 白皮書

Table of Contents

摘要和介紹 1
簡介 1
IP 地址規劃和管理 3
您是 Well-Architected 嗎？ 3
VPC 到 VPC 連線 5
VPC 對等互連 5
AWS Transit Gateway 6
傳輸 VPC 解決方案 7
VPC 互連 vs. Transit VPC vs. Transit Gateway 8
AWS PrivateLink 9
VPC 共享 11
私有 NAT 閘道 13
AWS 雲端 WAN 14
Amazon VPC Lattice 16
混合連線 18
VPN 18
Direct Connect 20
Direct Connect 連線上的 MACsec 安全性 24
Direct Connect 彈性建議 24
Direct Connect SiteLink 24
集中輸出至網際網路 27
使用 NAT 閘道進行集中式 IPv4 輸出 27
高可用性 29
安全 30
可擴展性 30
使用 NAT 閘道搭配 AWS Network Firewall 進行集中式 IPv4 輸出 30
可擴展性 32
關鍵考量 32
將 NAT 閘道和 Gateway Load Balancer 與 Amazon EC2 執行個體搭配使用，以進行集中式 IPv4 輸出 33
高可用性 34
優點 34
關鍵考量 35
IPv6 的集中式輸出 35

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 39
使用集中式網路安全性檢查模型的考量 39
使用閘道 Load Balancer 搭配 Transit Gateway 來實現集中式網路 40
AWS Network Firewall 和 AWS 閘道 Load Balancer 的關鍵注意事項 41
集中式傳入檢查 43
AWS WAF 和 AWS Firewall Manager 用於檢查來自網際網路的傳入流量 43
優點 44
關鍵考量 45
使用第三方設備集中檢查傳入 45
優點 46
關鍵考量 46
使用防火牆設備搭配 Gateway Load Balancer 檢查來自網際網路的傳入流量 47
使用 AWS Network Firewall 進行集中式輸入 48
使用 進行深度封包檢查 (DPI) AWS Network Firewall 49
集中式輸入架構 AWS Network Firewall 中 的主要考量事項 49
DNS 50
混合 DNS 50
Route 53 DNS 防火牆 52
集中存取 VPC 私有端點 54
介面 VPC 端點 54
跨區域端點存取 56
AWS Verified Access 57
結論 60
貢獻者 61
文件歷史紀錄 62
注意 64
..... lxv

建置可擴展且安全的多 VPC AWS 網路基礎設施

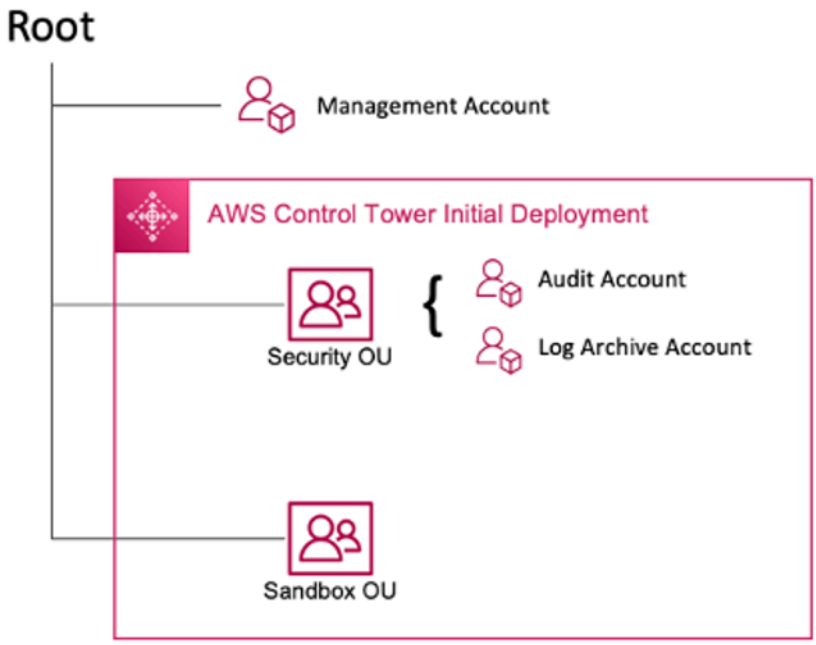
發佈日期：2024 年 4 月 17 日 (文件歷史紀錄)

Amazon Web Services (AWS) 客戶通常依賴數百個帳戶和虛擬私有雲端 (VPCs) 來分割工作負載並擴展其足跡。這種規模通常會在 VPC 連線的資源共用、VPC 間連線和內部部署設施方面造成挑戰。

本白皮書說明使用 Amazon Virtual Private Cloud (Amazon VPC)、AWS Transit Gateway、、AWS PrivateLinkDirect Connect、Gateway Load Balancer、 AWS Network Firewall和 Amazon Route 53 等 AWS 服務，在大型網路中建立可擴展且安全的網路架構的最佳實務。它示範了管理不斷增長的基礎設施的解決方案 - 確保可擴展性、高可用性和安全性，同時保持低成本。

簡介

AWS 客戶從在代表管理界限的單一 AWS 帳戶中建置資源開始，以區隔許可、成本和服務。不過，隨著客戶的組織成長，為了監控成本、控制存取，以及提供更輕鬆的環境管理，需要更多的服務區隔。多帳戶解決方案透過為組織中的 IT 服務和使用者提供特定帳戶來解決這些問題。 AWS 提供多種工具來管理和設定此基礎設施，包括 AWS Control Tower。



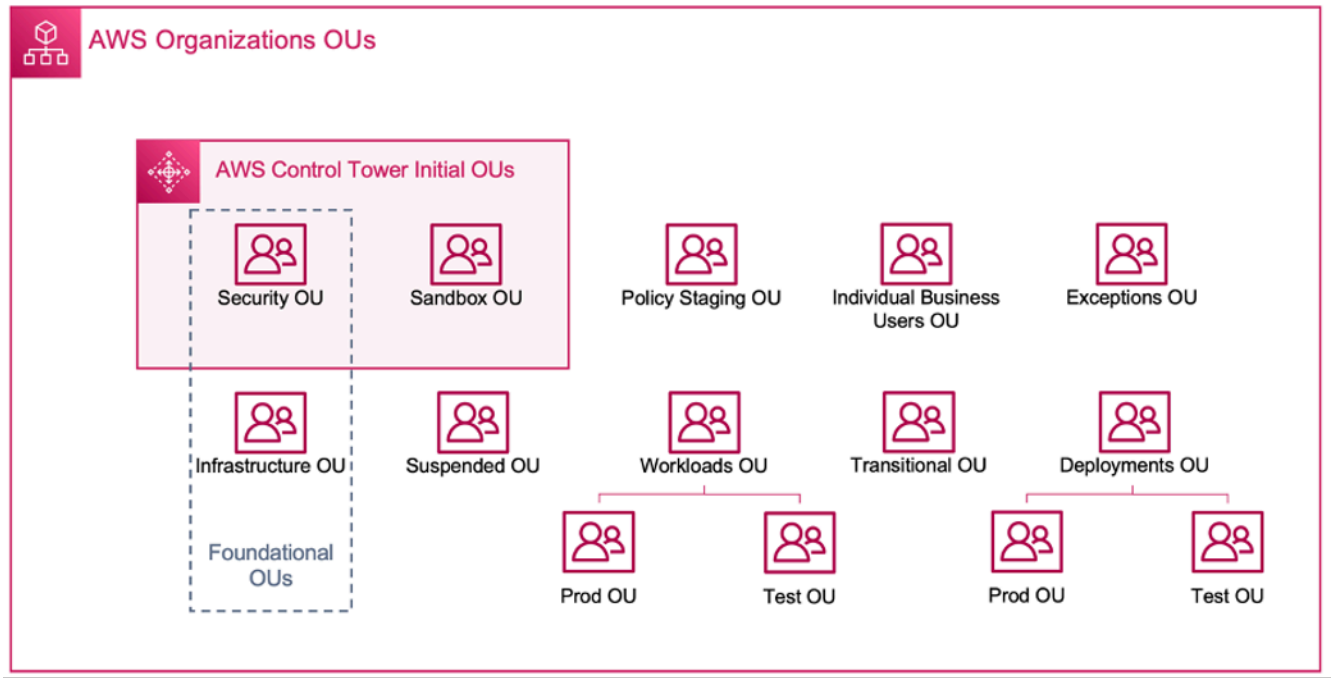
AWS Control Tower 初始部署

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 (OUs)：

- 安全性 OU – 在此 OU 中， 會 AWS Control Tower 建立兩個帳戶：
- 日誌存檔
- 稽核 （此帳戶對應至本指南先前討論的安全工具帳戶。）
- 沙盒 OU – 此 OU 是其中建立之帳戶的預設目的地 AWS Control Tower。它包含您的建置器可以在其中探索和試驗 AWS 服務以及其他工具和服務的帳戶，但需遵守您團隊的可接受使用政策。

AWS Control Tower 可讓您建立、註冊和管理其他 OUs，以擴展初始環境來實作指引。

下圖顯示最初部署的 OUs AWS Control Tower。您可以擴展您的 AWS 環境來實作圖表中包含的任何建議 OUs，以符合您的需求。



AWS 組織 OUs

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

大多數客戶都從幾個 VPCs 開始部署其基礎設施。客戶建立VPCs 數量通常與其帳戶、使用者和暫存環境 （生產、開發、測試等） 的數量相關。隨著雲端用量的增加，與客戶互動的使用者、業務單位、應用程式和區域數量也會增加，進而建立新的 VPCs。

隨著 VPCs 數量的增加，跨 VPC 管理對於客戶雲端網路的操作至關重要。本白皮書涵蓋跨 VPC 和混合連線三個特定領域的最佳實務：

- 網路連線 – 大規模互連 VPCs 和內部部署網路。

- 網路安全 – 建置存取網際網路和端點的集中式輸出點，例如網路位址轉譯 (NAT) 閘道、VPC 端點 AWS PrivateLink 、、 AWS Network Firewall 和 Gateway Load Balancer。
- DNS 管理 – 解析 Control Tower 內的 DNS 和混合式 DNS。

IP 地址規劃和管理

為了建置可擴展的多帳戶多 VPC 網路設計，IP 地址規劃和管理是必要的。良好的 IP 定址機制需要考慮您目前和未來的聯網需求。您的 IP 地址方案 IP 需要涵蓋您的內部部署工作負載、雲端工作負載，也應該允許未來擴展（例如，新增 AWS 區域、業務單位和合併或收購）。它還應該防止您的團隊不小心建立重疊CIDRs。如果需要重疊的 IP CIDR，例如隔離或中斷連線的工作負載，則此決策需要有意識，並應考量對路由、安全性和成本的影響。您可能還需要考慮為此類例外狀況建立必要的核准程序。良好的 IP 定址機制也有助於簡化網路設計和路由組態。

關鍵考量事項：

- 事先規劃您的 IP 定址機制（包括公有和私有 IPs)，然後選取 IP 地址管理工具，以配置、管理和追蹤所有工作負載的 IP 地址用量。
- 使用階層式和摘要 IP 定址機制。
- 根據環境 AWS 區域、組織或業務單位，規劃一致的 IP 指派。
- 為內部部署和雲端網路指定不同的 IP CIDRs (IPv4 和 IPv6)。
- 主動防止和追蹤重疊CIDRs。
- 適當調整 IP CIDRs的大小，以實現擴展和未來成長。
- 啟用工作負載以實現 IPv6 或雙堆疊相容性，以減少 IP 衝突並解決 IPv4 空間耗盡。

您可以使用 Amazon VPC IP Address Manager (IPAM) 來簡化 AWS 工作負載的公有和私有 IP 地址規劃、追蹤和監控。IPAM 可讓您跨多個 和 組織、配置、監控 AWS 區域 和共用 IP 地址空間 AWS 帳戶。它還有助於使用特定業務規則將 CIDRs 自動配置到 VPCs。

請參閱 Amazon VPC IP Address Manager 最佳實務、使用 Amazon VPC IP Address Manager 管理 VPCs 和區域的 IP 集區，以及部落格文章的 IP 地址管理 AWS Control Tower，以了解 IP 定址最佳實務，以及如何使用 IPAM 管理跨 VPCs IP 集區 AWS 區域，以及 AWS Control Tower。

您是 Well-Architected 嗎？

AWS Well-Architected Framework 可協助您了解在雲端建置系統時所做決策的優缺點。架構的六大支柱可讓您學習架構最佳實務，以設計和操作可靠、安全、有效率、經濟實惠且永續的系統。使用 AWS

Well-Architected Tool免費提供的 AWS 管理主控台，您可以透過回答每個支柱的一組問題，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引和最佳實務，參考架構部署、圖表和白皮書，請參閱AWS 架構中心。

VPC 到 VPC 連線

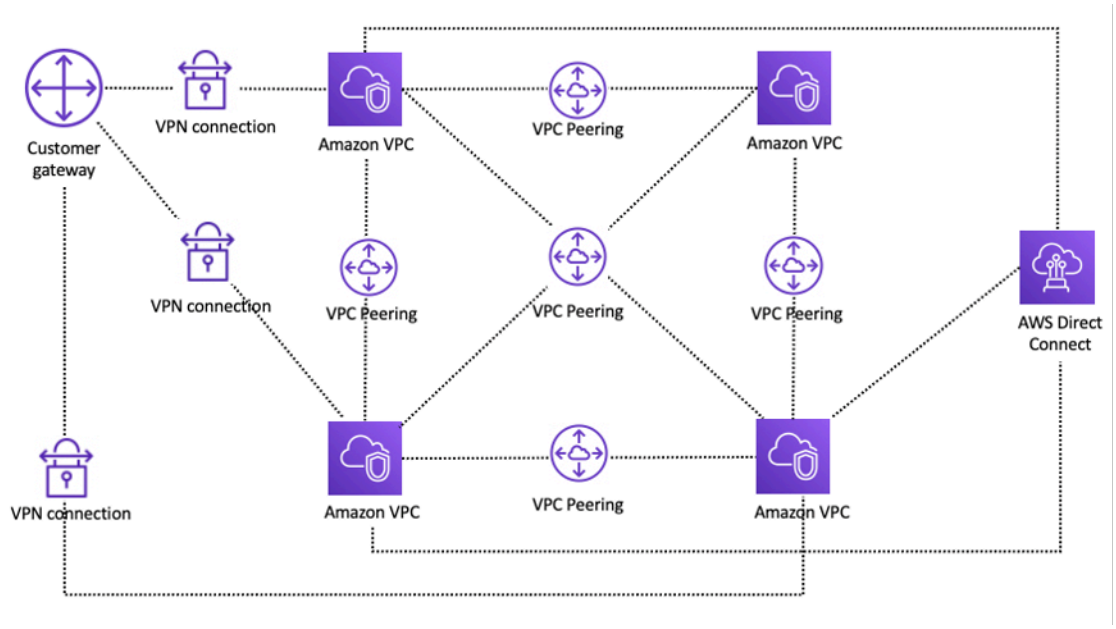
客戶可以使用兩種不同的 VPC 連線模式來設定多 VPC 環境：許多到許多，或中樞和輪輻。在many-to-many方法中，每個 VPC 之間的流量會在每個 VPC 之間個別管理。在中hub-and-spoke模型中，所有 VPC 間流量都會流經中央資源，而中央資源會根據已建立的規則路由流量。

VPC 對等互連

連接兩個 VPCs 的第一個方法是使用 VPC 對等互連。在此設定中，連線可在 VPCs 之間啟用完整雙向連線。此對等連線用於路由 VPCs 之間的流量。不同帳戶和 AWS 區域中的 VPCs 也可以對等互連。透過保持在可用區域內的 VPC 對等互連連線進行的所有資料傳輸都是免費的。透過跨可用區域的 VPC 對等互連進行的所有資料傳輸，都會以標準區域內資料傳輸費率計費。如果 VPCs 跨區域對等，則會收取標準區域間資料傳輸費用。

VPC 對等互連是point-to-point連線，不支援傳輸路由。例如，如果您在 VPC A 和 VPC B 之間以及 VPC A 和 VPC C 之間具有 VPC 對等互連，則 VPC B 中的執行個體無法透過 VPC A 傳輸以到達 VPC C。若要在 VPC B 和 VPC C 之間路由封包，您需要建立直接的 VPC 對等互連連線。

大規模地，當您有數十或數百VPCs 時，將它們與對等互連可能會導致數百或數千個對等互連的網格。大量連線可能難以管理和擴展。例如，如果您有 100 VPCs，而且想要在它們之間設定完整的網格對等互連，則需要 4，950 個對等互連 【n(n-1)/2】 ，其中 n是 VPCs 的總數。每個 VPC 最多有 125 個作用中對等互連。



使用 VPC 對等互連的網路設定

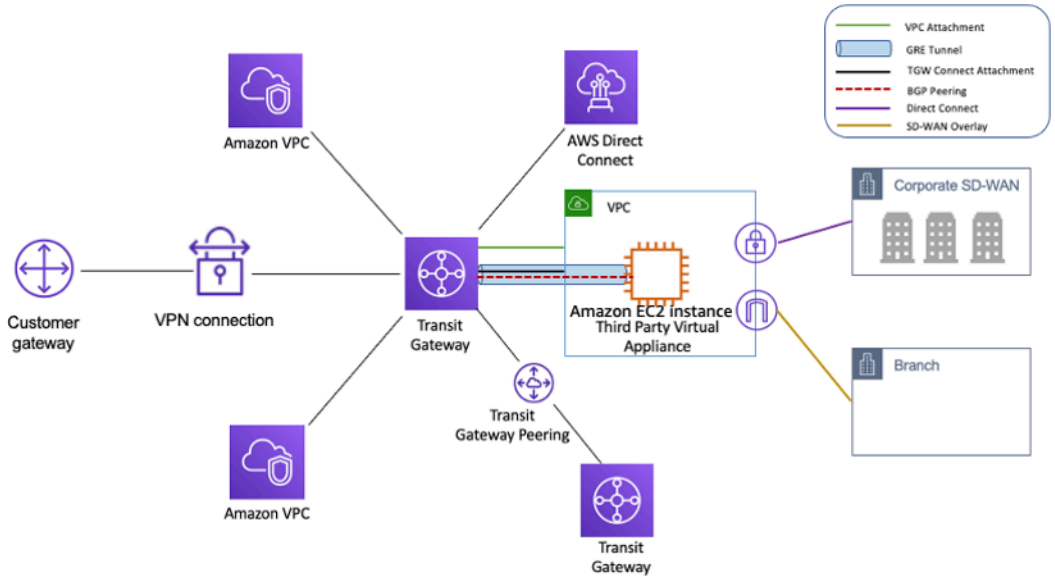
如果您使用 VPC 對等互連，則必須對每個 VPC 建立內部部署連線 (VPN 和/或 Direct Connect)。VPC 中的資源無法使用對等 VPC 的混合連線到達內部部署，如上圖所示。

當一個 VPC 中的資源必須與另一個 VPC 中的資源通訊、兩個 VPCs的環境受到控制和保護，且要連線的 VPCs 數量少於 10 時，最好使用 VPC 對等互連（以允許每個連線的個別管理）。與其他 VPC 互連選項相比，VPC 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 提供中樞和輻條設計，可將 VPCs 和內部部署網路作為全受管服務進行連接，而無需您佈建第三方虛擬設備。不需要 VPN 浮水印，並 AWS 管理高可用性和可擴展性。

Transit Gateway 可讓客戶連接數千個 VPCs。您可以將所有混合連線 (VPN 和 Direct Connect 連線）連接到單一閘道，在一個位置整合和控制組織的整個 AWS 路由組態（請參閱下圖）。Transit Gateway 會使用路由表，控制流量在所有連接的輻條網路之間路由的方式。此hub-and-spoke模型可簡化管理並降低營運成本VPCs 只會連線至 Transit Gateway 執行個體，以取得連線網路的存取權。



使用 的中樞和輻條設計 AWS Transit Gateway

Transit Gateway 是區域性資源，可以在相同的 中連接數千個 VPCs AWS 區域。您可以透過單一 Direct Connect 連線連接多個閘道，以進行混合連線。一般而言，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，並在需要時使用 Transit Gateway 路由表來隔離它們。請注意，您不需要額外的傳輸閘道來實現高可用性，因為傳輸閘道的設計非常可用；對於備援，請在每個區域中使用單一閘道。不過，有一個有效的案例可以建立多個閘道，以限制設定錯誤的爆量半徑、隔離控制平面操作和管理ease-of-use。

透過 Transit Gateway 對等互連，客戶可以在相同或多個區域中對等 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基礎設施，因此會加密。如需詳細資訊，請參閱使用 AWS Transit Gateway 區域間對等互連建置全球網路和 AWS Transit Gateway 現在支援區域間對等互連。

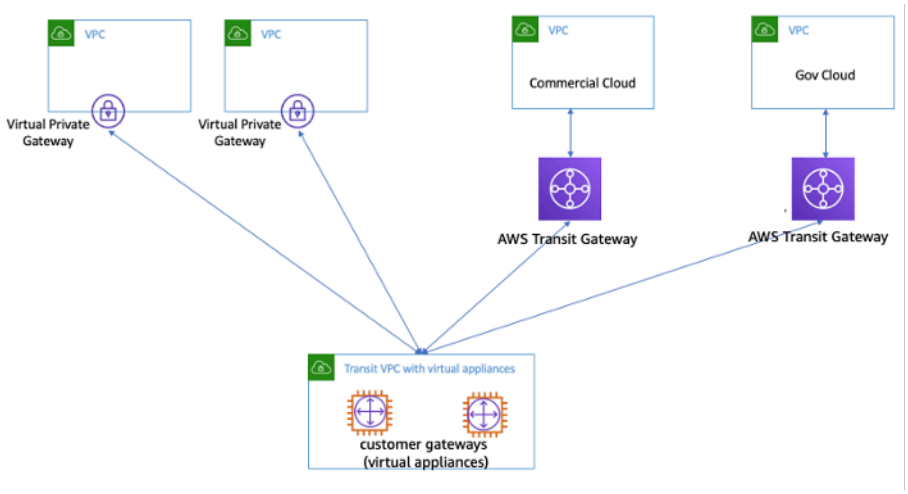
將組織的 Transit Gateway 執行個體放在其 Network Services 帳戶中。這可讓管理 Network Services 帳戶的網路工程師集中管理。使用 AWS Resource Access Manager (RAM) 來共用 Transit Gateway 執行個體，以便在相同區域內的 AWS Organization 中多個帳戶之間連接 VPCs。AWS RAM 可讓您輕鬆安全地與任何 AWS Organization 內 AWS 帳戶或 AWS Organization 共用 AWS 資源。如需詳細資訊，請參閱中央帳戶部落格文章中的自動化 AWS Transit Gateway 連接至傳輸閘道。

Transit Gateway 也可讓您在 SD-WAN 基礎設施與 AWS 使用 Transit Gateway Connect 之間建立連線。將 Transit Gateway Connect 連接與邊界閘道通訊協定 (BGP) 搭配使用，以用於動態路由，並將一般路由封裝 (GRE) 通道通訊協定搭配使用，以實現高效能，為每個 Connect 連接提供高達 20 Gbps 的總頻寬 （每個 Connect 連接最多四個 Transit Gateway Connect 對等）。透過使用 Transit Gateway Connect，您可以透過 VPC 連接或連接來整合在雲端中執行的內部部署 SD-WAN 基礎設施或 Direct Connect SD-WAN 設備，做為基礎傳輸層。如需參考架構和詳細組態，請參閱使用 AWS Transit Gateway Connect 簡化 SD-WAN 連線。

傳輸 VPC 解決方案

傳輸 VPCs可以採用與 VPC 對等互連不同的方式，在 VPCs 之間建立連線，方法是引入中樞和輻條設計，以實現 VPC 間連線。在傳輸 VPC 網路中，一個中央 VPC （中樞 VPC) 會透過 VPN 連線與所有其他 VPC （輻 VPC) 連線，通常透過 IPsec 利用 BGP。中央 VPC 包含執行軟體設備的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體，使用 VPN 浮水印將傳入流量路由至目的地。傳輸 VPC 對等互連具有下列優點：

- 使用覆蓋 VPN 網路啟用暫時性路由 — 允許中心和輻條設計。
- 在中樞傳輸 VPC 的 EC2 執行個體上使用第三方廠商軟體時，可以使用進階安全性 （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，則受益於統一的操作/監控體驗。
- Transit VPC 架構可啟用某些使用案例中可能需要的連線。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 Transit VPC，並在兩個區域之間啟用 VPC 間連線。考慮此選項時，請評估您的安全和合規要求。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。



使用虛擬設備傳輸 VPC

Transit VPC 本身就面臨挑戰，例如根據執行個體大小/系列在 EC2 上執行第三方供應商虛擬設備的成本較高、每個 VPN 連線的輸送量有限（每個 VPN 通道高達 1.25 Gbps），以及額外的組態、管理和彈性額外負荷（客戶負責管理執行第三方供應商虛擬設備的 EC2 執行個體的 HA 和備援）。

VPC 互連 vs. Transit VPC vs. Transit Gateway

表 1 — 連線能力比較

條件	VPC 對等互連	傳輸 VPC	轉換閘道	PrivateLink	雲端 WAN	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	以 VPN 為基礎的中 hub-and-spoke	以附件為基礎的中hub-and-spoke	提供者或消費者模型	以附件為基礎的多區域	應用程式對應用程式連線
擴展	125 個作用中的對等/VPC	取決於虛擬路由器/EC2	每個區域 5000 個附件	無限制	每個核心網路 5000 個附件	每個服務 500 個 VPC 關聯
區隔	安全群組	客戶受管	Transit Gateway 路由表	無分割	客群	Servie 和服務網路政策

條件	VPC 對等互連	傳輸 VPC	轉換閘道	PrivateLink	雲端 WAN	VPC Lattice
Latency (延遲)	最低	額外，由於 VPN 加密額外負荷	其他 Transit Gateway 跳轉	流量會保留在 AWS 骨幹上，客戶應該測試	使用與 Transit Gateway 相同的資料平面	流量會保留在 AWS 骨幹上，客戶應該測試
頻寬限制	每個執行個體限制，無彙總限制	根據大小/家庭，受限於 EC2 執行個體頻寬限制	最高 100 Gbps（爆量）/連接	每個可用區域 10 Gbps，自動擴展至 100 Gbps	最高 100 Gbps（爆量）/連接	每個可用區域 10 Gbps
Visibility	VPC 流量日誌	VPC 流程日誌和 CloudWatch 指標	Transit Gateway Network Manager、VPC 流程日誌、CloudWatch 指標	CloudWatch Metrics	Network Manager、VPC 流程日誌、CloudWatch 指標	CloudWatch 存取日誌
安全群組 交叉參考	支援	不支援	不支援	不支援	不支援	不適用
IPv6 支援	支援	取決於虛擬設備	支援	支援	支援	支援

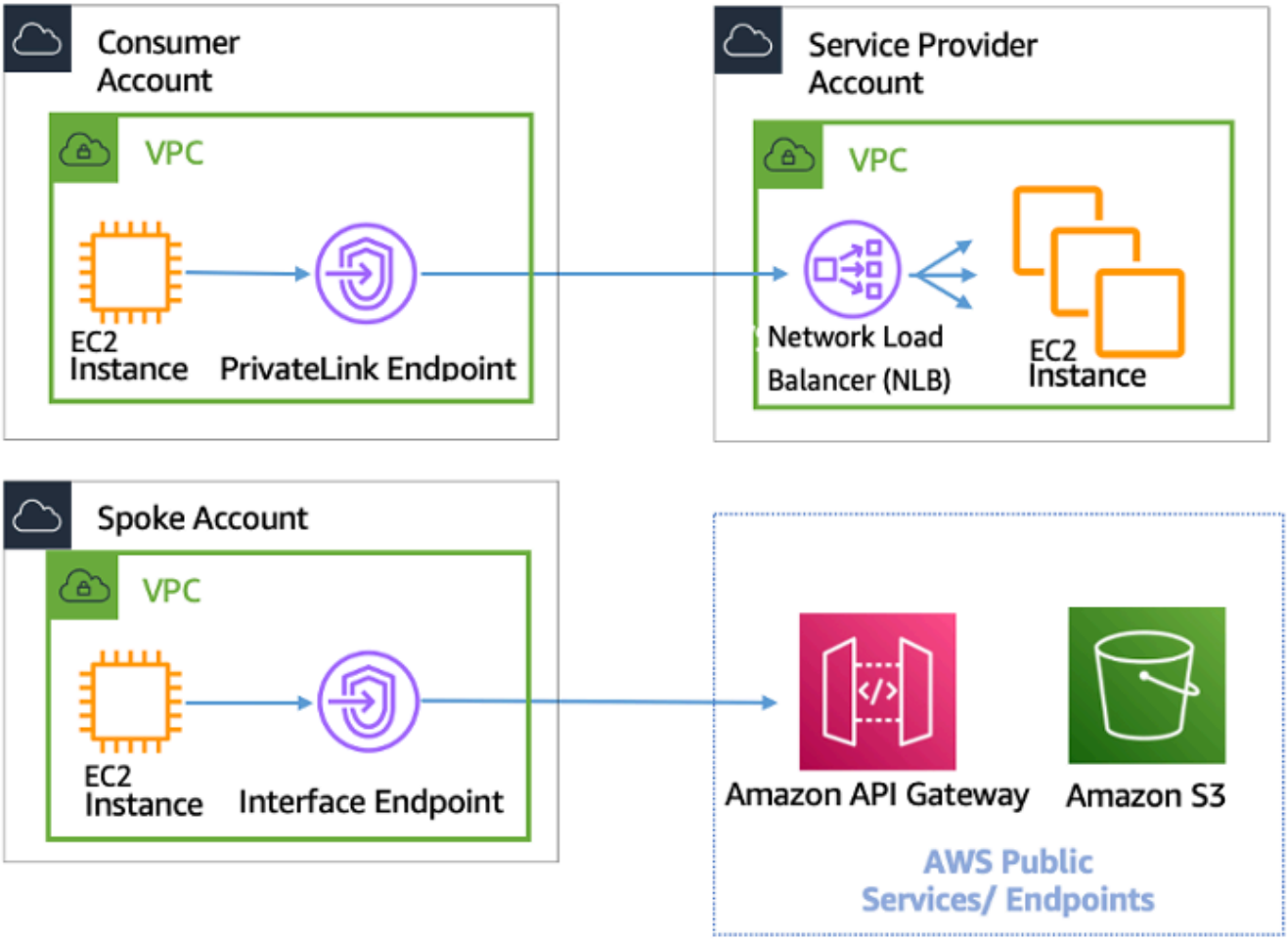
AWS PrivateLink

AWS PrivateLink 提供 VPCs、AWS 服務和內部部署網路之間的私有連線，而不會將您的流量暴露到公有網際網路。採用 技術的界面 VPC 端點 AWS PrivateLink可讓您輕鬆地跨不同帳戶 AWS 和 VPCs 連線至 和其他 服務，以大幅簡化您的網路架構。這可讓可能想要以僅消費者 VPCs 啟動與服務提供者

VPC 之連線 AWS 區域 的方式，將某個 VPC （服務提供者） 中的服務/應用程式私下公開給 內的其他 VPCs（消費者）。例如，您的私有應用程式可存取服務提供者 APIs。

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，服務消費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彈性網路介面 (ENI)，其私有 IP 地址可做為目的地為 服務的流量進入點。消費者和服務不需要位於相同的 VPC 中。如果 VPC 不同，消費者和服務提供者 VPCs可以有重疊的 IP 地址範圍。除了建立介面 VPC 端點以存取其他 VPCs中的服務之外，您還可以建立介面 VPC 端點，透過 私下存取支援的 AWS 服務 AWS PrivateLink，如下圖所示。

使用 Application Load Balancer (ALB) 作為 NLB 的目標，您現在可以將 ALB 進階路由功能與 結合 AWS PrivateLink。如需參考架構和詳細組態，請參閱適用於 Network Application Load Balancer Load Balancer 類型目標群組。



AWS PrivateLink 與其他 VPCs

Transit Gateway、VPC 對等互連和 之間的選擇 AWS PrivateLink 取決於連線。

- AWS PrivateLink — 當您有用戶端/伺服器設定，而您想要允許一或多個消費者 VPCs 單向存取特定服務或服務提供者 VPC 或特定 AWS 服務中的一組執行個體 AWS PrivateLink 時，請使用 。只有具有取用者 VPC 中存取權的用戶端，才能在服務提供者 VPC 或服務中啟動對服務的連線 AWS 。當兩個 VPCs具有重疊的 IP 地址時，這也是不錯的選擇，因為 AWS PrivateLink 會在用戶端 VPC 中使用 ENIs，以確保 不會與服務提供者發生 IP 衝突。您可以透過 VPC 對等互連、VPN、傳輸閘道、雲端 WAN 和 存取 AWS PrivateLink 端點 AWS Direct Connect。
- VPC 對等互連和傳輸閘道 — 當您想要在 VPC 之間啟用 layer-3 IP 連線時VPCs 對等互連和傳輸閘道。

  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互相組合和操作。例如， AWS PrivateLink 處理 API 樣式用戶端伺服器連線、處理直接連線需求的 VPC 對等互連，其中可能需要在區域內或區域間連線的置放群組，以及 Transit Gateway 簡化大規模 VPCs 的連線，以及用於混合連線的邊緣整合。

VPC 共享

當團隊之間的網路隔離不需要由 VPCs 擁有者嚴格管理，但帳戶層級使用者和許可必須如此時，共用 VPC 非常有用。透過共用 VPC，多個 AWS 帳戶會在共用、集中管理的 Amazon VPCs 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 的帳戶 （擁有者） 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 VPCs中資源之間的安全，是使用安全群組、網路存取控制清單 (NACLs) 或透過子網路之間的防火牆進行管理。

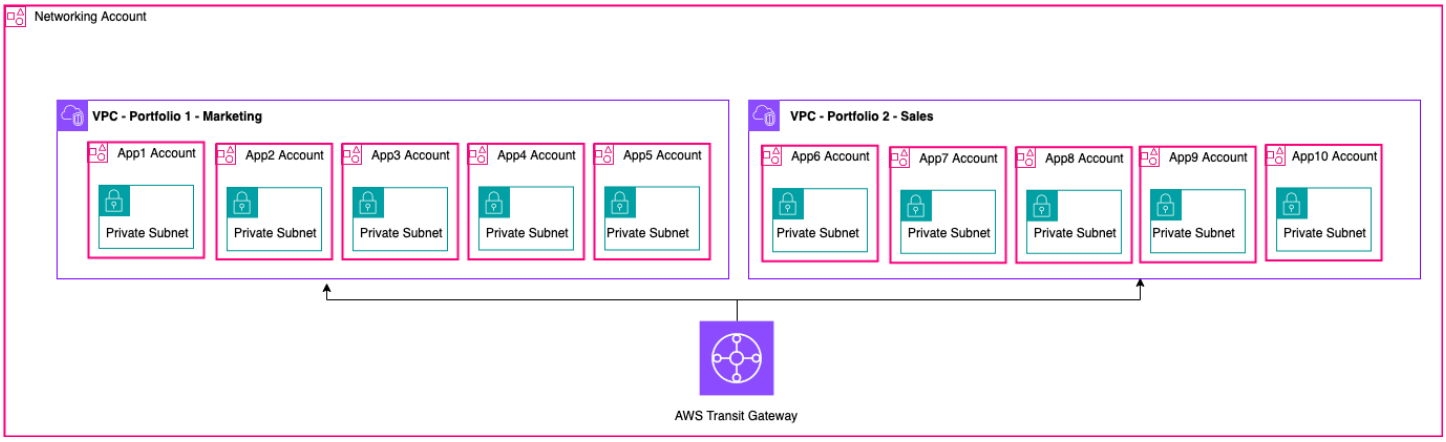
VPC 共用優點：

- 簡化設計：VPC 間連線不複雜
- 受管 VPCs 較少
- 網路團隊和應用程式擁有者之間的職責劃分
- 更好的 IPv4 地址使用率
- 降低成本 — 屬於相同可用區域內不同帳戶的執行個體之間不收取資料傳輸費用

> **Note**
>
> 當您與多個帳戶共用子網路時，參與者應該有一定程度的合作，因為他們正在共用 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 除了提供安全群組之外，還提供網路隔離。

大多數客戶架構將包含多個 VPCs，其中許多 VPC 會與兩個或多個帳戶共用。Transit Gateway 和 VPC 對等互連可用來連接共用 VPCs。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產品組合（相同產品組合內的應用程式具有類似的聯網需求，即「行銷」中的應用程式 1–5 和「銷售」中的應用程式 6–10)。

您可以為每個應用程式產品組合有一個 VPC（總共兩個 VPCs)，而 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（在此情況下，在不同的子網路中，使用 NACLs 進行網路路由分割和隔離）。這兩個共用 VPCs 是透過 Transit Gateway 連接。透過此設定，您可以將 10 VPCs，如下圖所示。

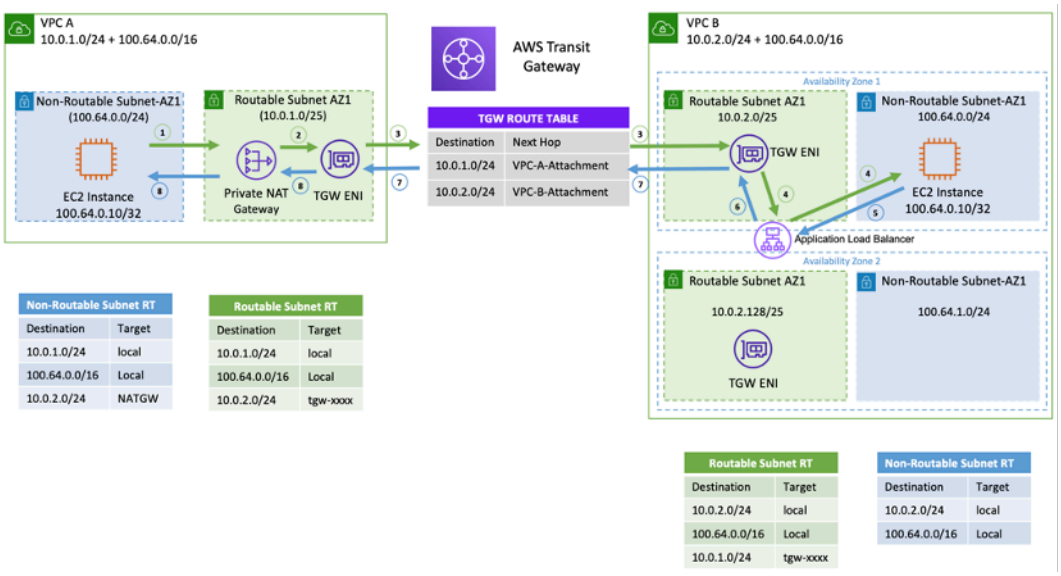


設定範例 – 共用 VPC

> **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 共用文件中的限制一節。
> 如需 VPC 共用的重要考量和最佳實務的詳細資訊，請參閱 VPC 共用：重要考量和最佳實務部落格文章。

私有 NAT 閘道

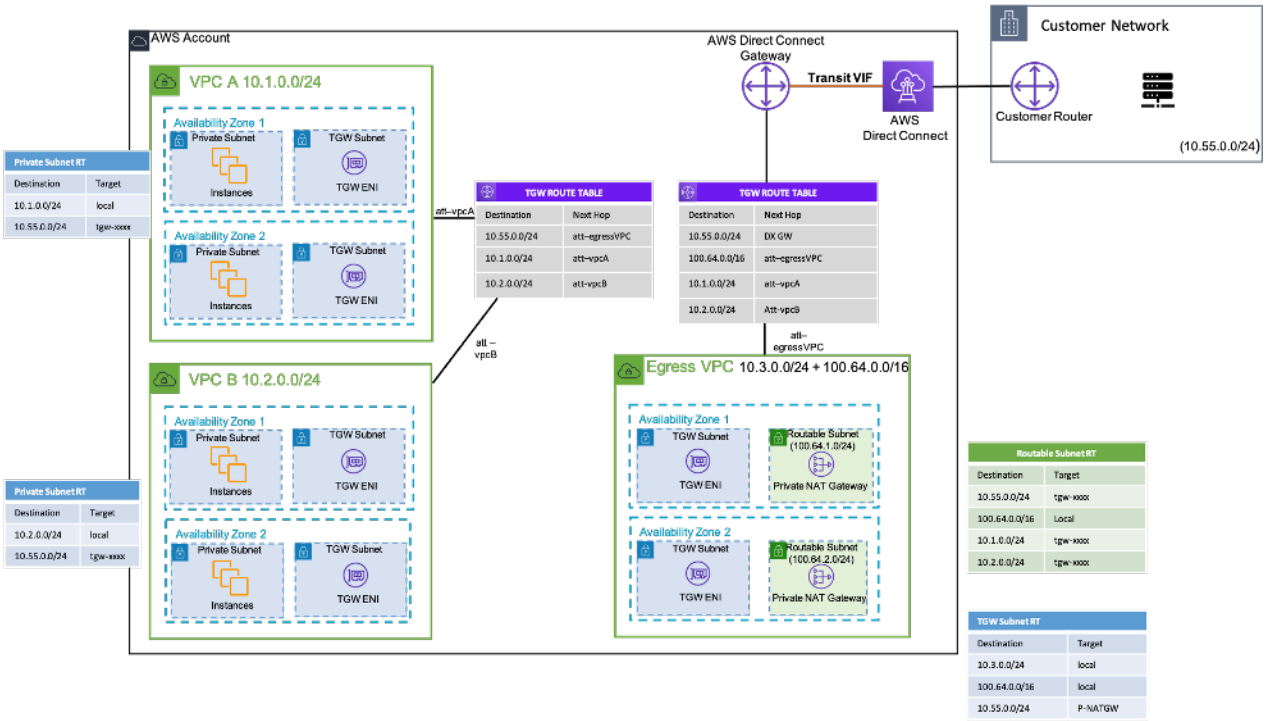
團隊通常獨立運作，而且他們可能會為專案建立新的 VPC，這可能具有重疊的無類別網域間路由 (CIDR) 區塊。為了進行整合，他們可能想要啟用具有重疊 CIDRs的網路之間的通訊，這些 CIDR 無法透過 VPC 對等互連和 Transit Gateway 等功能實現。私有 NAT 閘道可協助處理此使用案例。私有 NAT 閘道使用唯一的私有 IP 地址來執行重疊來源 IP 地址的來源 NAT，而 ELB 則會執行重疊目的地 IP 地址的目的地 NAT。您可以使用 Transit Gateway 或虛擬私有閘道，將流量從私有 NAT 閘道路由到其他 VPCs 或內部部署網路。



設定範例 – Private NAT 閘道

上圖顯示 VPC A 和 B 中的兩個不可路由（重疊 CIDRs，100.64.0.0/16) 子網路。若要在它們之間建立連線，您可以分別將次要不可重疊/可路由 CIDRs（可路由子網路，10.0.1.0/24和 10.0.2.0/24) 新增至 VPC A 和 B。可路由 CIDRs 應由負責 IP 配置的網路管理團隊配置。私有 NAT 閘道會新增至 VPC A 中 IP 地址為 的可路由子網路10.0.1.125。私有 NAT 閘道會在 VPC A (100.64.0.10) 不可路由子網路中的執行個體請求上執行來源網路地址轉譯10.0.1.125，做為私有 NAT 閘道的 ENI。現在可將流量指向指派給 VPC B () 中 Application Load Balancer (ALB10.0.2.10) 的可路由 IP 地址，其目標為 100.64.0.10。流量會透過 Transit Gateway 路由。傳回流量會由私有 NAT 閘道處理，再傳回請求連線的原始 Amazon EC2 執行個體。

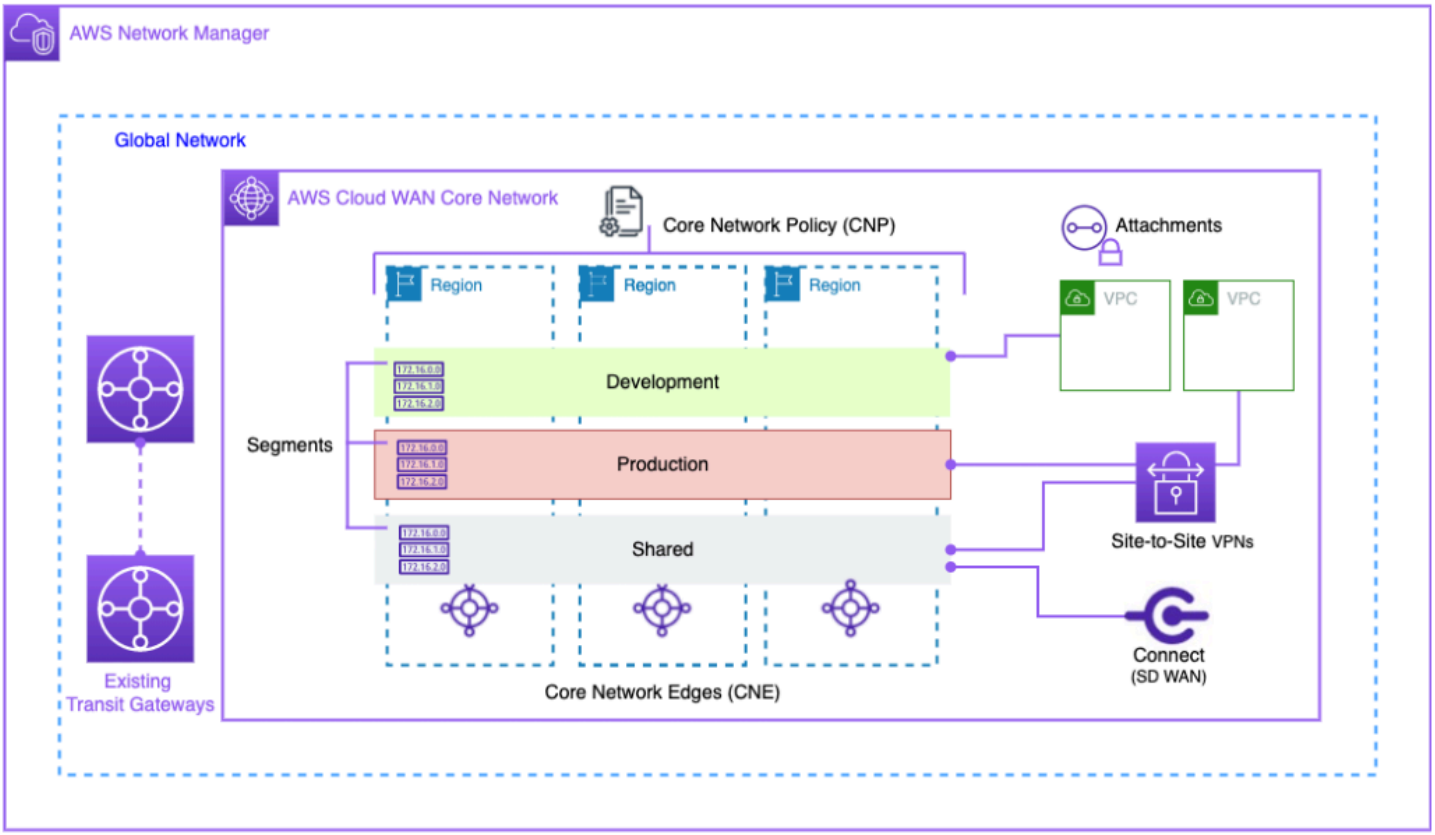
當您的內部部署網路限制存取核准的 IPs 時，也可以使用私有 NAT 閘道。合規部門要求少數客戶的內部部署網路只能透過客戶擁有的有限連續 IPs 區塊與私有網路（非 IGW) 通訊。您可以使用私有 NAT 閘道在每個允許清單 IP 後面的 AWS VPCs 上執行大型工作負載，而不是將每個執行個體與區塊分開配置。如需詳細資訊，請參閱如何使用私有 NAT 解決方案解決私有 IP 耗盡部落格文章。



設定範例 – 如何使用 Private NAT 閘道為內部部署網路提供核准的 IPs

AWS 雲端 WAN

AWS Cloud WAN 是將網路連接在一起的新方法，我們之前可以使用 Transit Gateways、VPC Peering 和 IPSEC VPN 通道。您先前會設定一或多個 VPCs、使用上述其中一種方法將它們連接在一起，並使用 IPSEC VPN 或 Direct Connect 連線到內部部署網路。您可以在一個位置定義您的網路和安全狀態建構，並在另一個位置定義您的網路。Cloud WAN 可讓您將所有這些建構集中在單一位置。根據政策，您可以分割您的網路，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。



Cloud WAN 區塊圖

透過 AWS Network Manager 使用者介面和 APIs管理您的全球網路。全域網路是所有網路物件的根層級容器；核心網路是 AWS 管理的全域網路的一部分。核心網路政策 (CNP) 是定義核心網路所有層面的單一版本控制政策文件。附件是您想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 政策之附件的本機連接點。根據預設，網路區段是路由網域，僅允許區段內的通訊。

若要使用 CloudWAN：

1. 在 AWS Network Manager 中，建立全域網路和相關聯的核心網路。
2. 建立 CNP，以定義區段、ASN 範圍 AWS 區域 和要用來連接至區段的標籤。
3. 套用網路政策。
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. 建立和標記附件。
6. 更新連接 VPCs中的路由，以包含核心網路。

Cloud WAN 旨在簡化全球連接 AWS 基礎設施的程序。它可讓您使用集中式許可政策來分割流量，並使用您公司據點的現有基礎設施。Cloud WAN 也會連接您的 VPCs、SD-WANs、用戶端 VPNs、防火

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

AWS Cloud WAN 可啟用統一的網路連接雲端和內部部署環境。組織使用新一代防火牆 (NGFWs) 和入侵預防系統 IPSs) 來確保安全。AWS Cloud WAN 和 Transit Gateway 遷移和互通性模式部落格文章描述了架構模式，用於集中管理和檢查 Cloud WAN 網路中的傳出網路流量，包括單一區域和多區域網路，並設定路由表。這些架構可確保資料和應用程式安全，同時維護安全的雲端環境。

如需 Cloud WAN 的詳細資訊，請參閱 AWS Cloud WAN 部落格文章中的集中式傳出檢查架構。

Amazon VPC Lattice

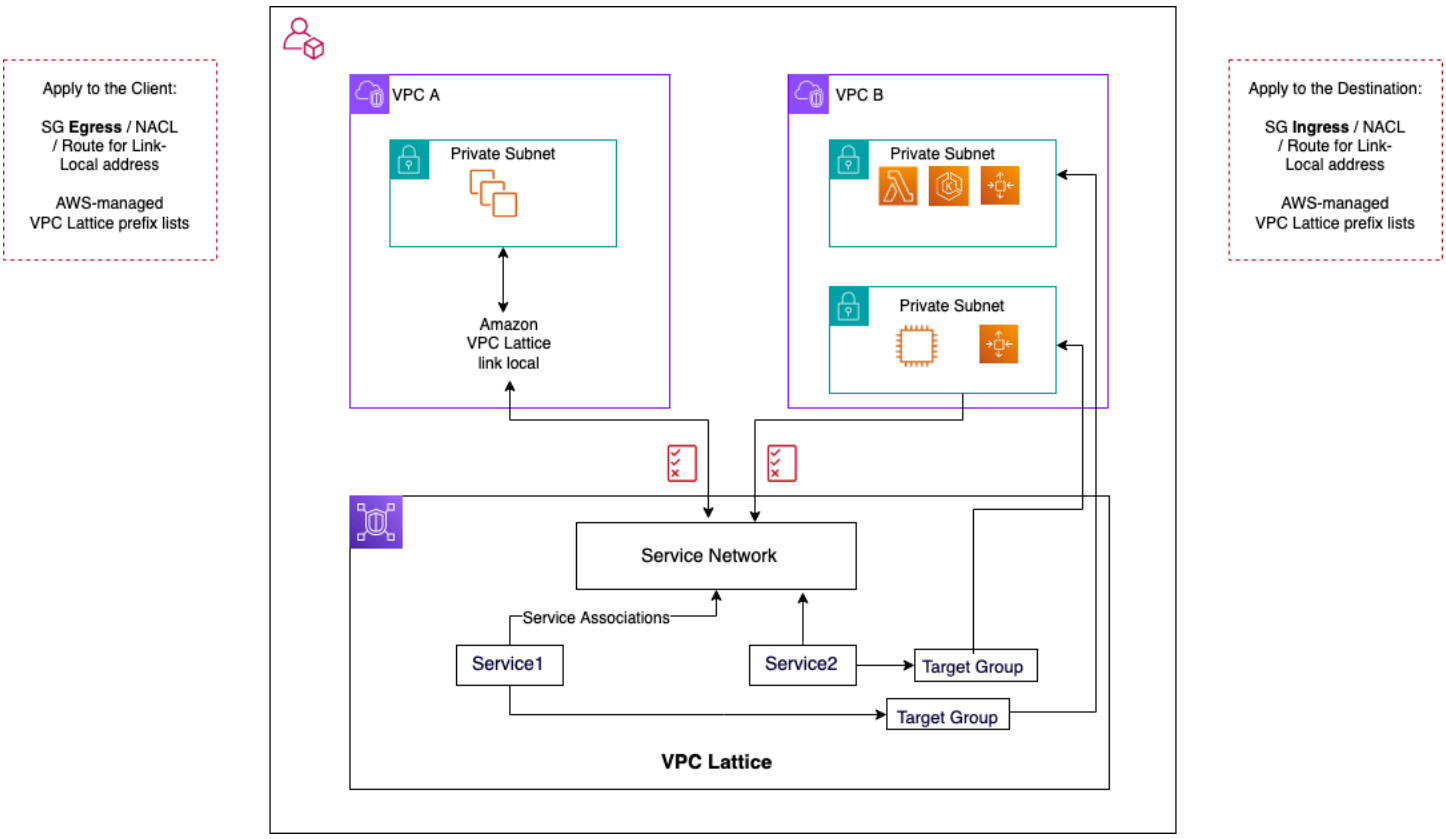
Amazon VPC Lattice 是一種全受管應用程式聯網服務，用於跨各種帳戶和虛擬私有雲端來連接、監控和保護服務。VPC Lattice 有助於在邏輯界限內互連服務，讓您可以有效率地管理和探索這些服務。

VPC Lattice 元件包含：

- 服務 - 這是在執行個體、容器或 Lambda 函數上執行的應用程式單位，由接聽程式、規則和目標群組組成。
- 服務網路 - 這是邏輯界限，用於自動實作服務探索和連線，並將常見的存取和可觀測性政策套用至服務集合。
- 驗證政策 - 可與服務網路或個別服務相關聯的 IAM 資源政策，以支援請求層級身分驗證和內容特定授權。
- 服務目錄 - 您擁有或透過 AWS Resource Access Manager 與您共用之服務的集中式檢視。

VPC Lattice 使用步驟：

1. 建立服務網路。服務網路通常位於網路管理員具有完整存取權的網路帳戶中。服務網路可以在組織中的多個帳戶之間共用。共用可以在個別服務或整個服務帳戶上執行。
2. 將 VPCs連接至服務網路，以啟用每個 VPC 的應用程式聯網，讓不同的服務可以開始耗用網路中註冊的其他 服務。會套用安全群組來控制流量。
3. 開發人員會定義 服務，這些服務會填入服務目錄中並註冊至服務網路。VPC Lattice 包含所有已設定服務的通訊錄。開發人員也可以定義路由政策以使用藍/綠部署。安全性是在定義身分驗證和授權政策的服務網路層級，以及在實作 IAM 存取政策的服務層級進行管理。



VPC Lattice 通訊流程

如需更多詳細資訊，請參閱 VPC Lattice 使用者指南。

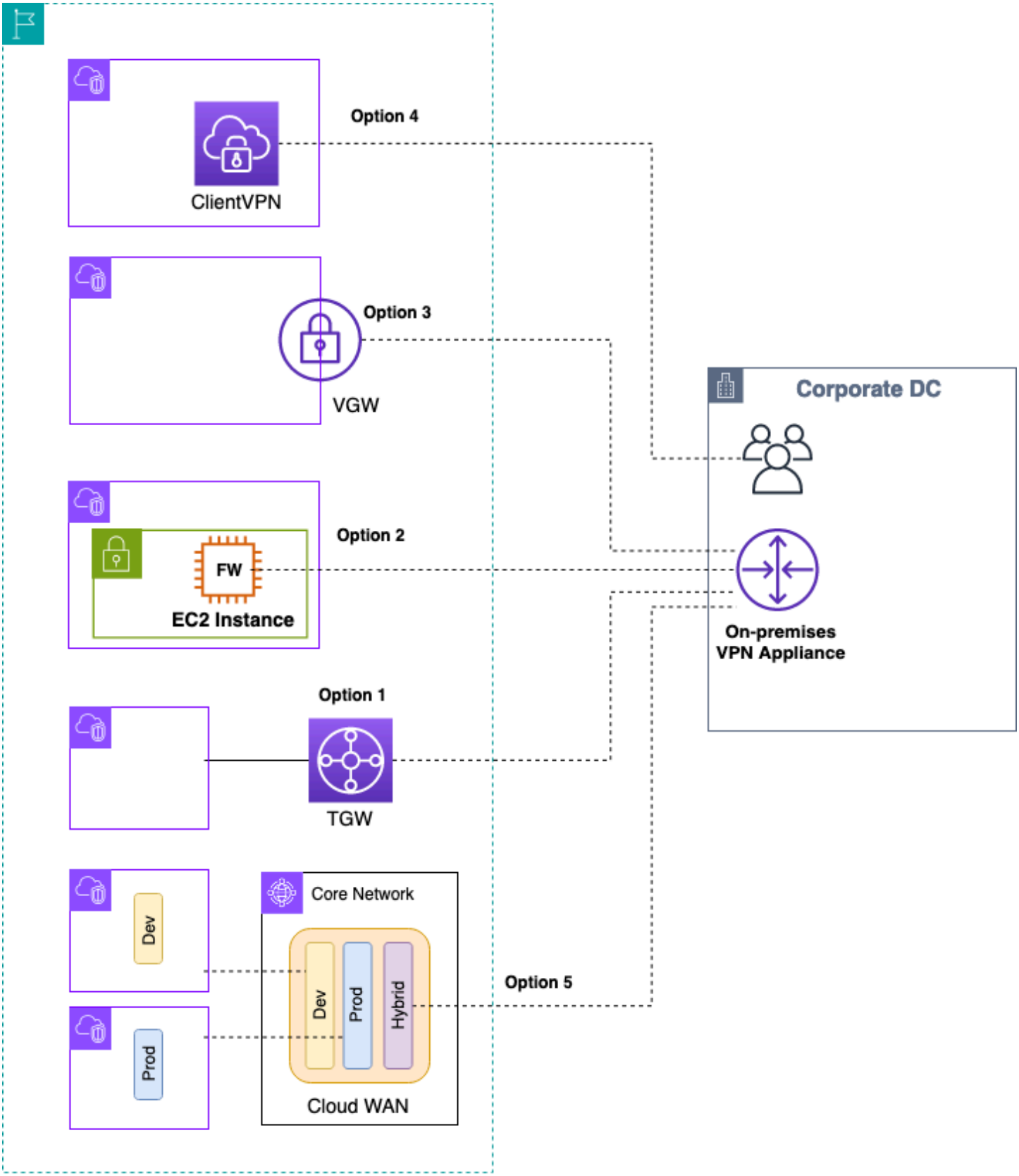
混合連線

本節著重於將雲端資源與內部部署資料中心安全地連線。啟用混合連線的方法有三種：

- One-to-one連線：在此設定中，會為每個 VPC 建立 VPN 連線和/或 Direct Connect 私有 VIF。這是使用虛擬私有閘道 (VGW) 來完成的。此選項適用於少量 VPCs，但隨著客戶擴展其 VPCs，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，客戶會將多個 VPCs的混合 IT 連線整合在單一端點。所有 VPCs共用這些混合連線。這是使用 AWS Transit Gateway 和 Direct Connect 閘道來完成的。
- 全網格混合整合：在此設定中，客戶使用建置於 的 CloudWAN，在單一端點整合多個 VPCs 的連線 AWS Transit Gateway。這是在一或多個 AWS 帳戶中聯網的完整政策型方法，以程式碼表示。目前，使用 Direct Connect 進行邊緣連線需要將 Transit Gateway 互連至 CloudWAN。

VPN

設定 VPN 到 AWS 的方式有多種：

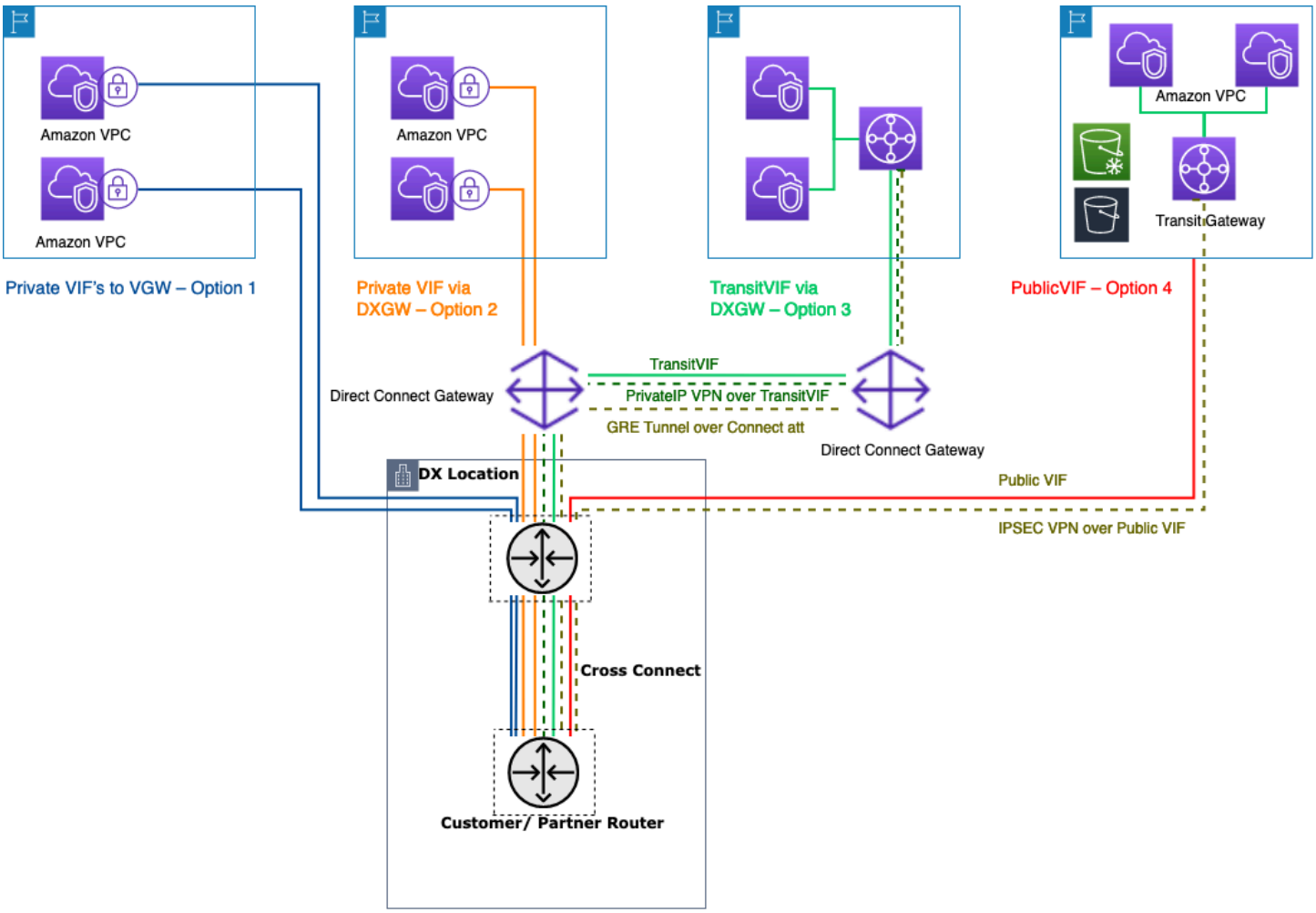


Site-to-Site VPN 選項

- 選項 1：整合 Transit Gateway 上的 VPN 連線 — 此選項利用 Transit Gateway 上的 Transit Gateway VPN 連接。Transit Gateway 支援site-to-site的 IPsec 終止。客戶可以建立連至 Transit Gateway 的 VPN 通道，並可以存取連到它的 VPCs。Transit Gateway 支援靜態和 BGP 型動態 VPN 連線。Transit Gateway 也支援 VPN 連接上的等價多路徑 (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，進而擴展到超過預設的 1.25 Gbps 上限。在此選項中，您需要支付 Transit Gateway 定價和Site-to-Site VPN 定價的費用。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 Transit Gateway 部落格文章擴展 VPN 輸送量。
- 選項 2：在 Amazon EC2 執行個體上終止 VPN — 當客戶想要特定廠商軟體功能集（例如 Cisco DMVPN 或一般路由封裝 (GRE)），或想要跨各種 VPN 部署運作一致性時，客戶會利用此選項。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 VPC 連線區段中的所有關鍵考量事項都適用於混合 VPN 連線。您負責管理高可用性，並支付 EC2 執行個體以及任何廠商軟體授權和支援成本的費用。
- 選項 3：在虛擬私有閘道 (VGW) 上終止 VPN — 此 AWS Site-to-Site VPN 服務選項可啟用one-to-one連線設計，您可以在其中為每個 VPC 建立一個 VPN 連線（由一對備援 VPN 通道組成）。 這是開始使用 VPN 連線至 AWS 的好方法，但隨著您擴展 VPCs 數量，管理不斷增加的 VPN 連線數量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成為更好的選項。VGW 的 VPN 輸送量限制為每個通道 1.25 Gbps，不支援 ECMP 負載平衡。從定價角度來看，您只需支付 AWS VPN 定價，執行 VGW 無需付費。如需詳細資訊，請參閱 Site-to-Site VPN 定價和Site-to-Site VPN 虛擬私有閘道上的 。
- 選項 4：終止用戶端 VPN 端點上的 VPN 連線 — AWS Client VPN 是一種受管的用戶端型 VPN 服務，可讓您安全地存取內部部署網路中的 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 Transport Layer Security (TLS) VPN 連線。如需詳細資訊，請參閱 AWS Client VPN 文件。
- 選項 5：在 AWS Cloud WAN 上合併 VPN 連線 — 此選項類似於此清單中的第一個選項，但它使用 CloudWAN 結構透過網路政策文件以程式設計方式設定 VPN 連線。

Direct Connect

雖然透過網際網路的 VPN 是入門的絕佳選擇，但網際網路連線對於生產流量可能不可靠。由於這種不可靠性，許多客戶選擇 Direct Connect。 Direct Connect 是一種聯網服務，提供使用網際網路連線到 AWS 的替代方案。使用 時 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來傳遞。在許多情況下，私有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。有幾種方法可以使用 Direct Connect 連線到 VPCs：



使用 連線現場部署資料中心的方法 Direct Connect

- 選項 1：建立連接到 VPC 之 VGW 的私有虛擬介面 (VIF)：每個 Direct Connect 連線可以建立 50 VIFs，讓您最多連接到 50 VPCs（一個 VIF 提供與一個 VPC 的連線）。每個 VPC 有一個 BGP 對等互連。此設定中的連線僅限於 Direct Connect 位置所在的 AWS 區域。VIF 對 VPC 的one-to-one 映射（且缺乏全域存取）使得存取登陸區域中VPCs 成為最不理想的方法。
- 選項 2：建立私有 VIF 到與多個 VGWs相關聯的 Direct Connect 閘道（每個 VGW 都連接到 VPC) — Direct Connect 閘道是全球可用的資源。您可以在任何區域中建立 Direct Connect 閘道，並從所有其他區域存取，包括 GovCloud（中國除外）。Direct Connect Gateway 可透過單一私有 VPCs（透過 VGWs)。如果登陸區域包含少量 VPCs（十個或更少VPCs) 和/或您需要全域存取，這是很好的選擇。每個 Direct Connect 連線的每個 Direct Connect Gateway 都有一個 BGP 對等互連工作階段。Direct Connect 閘道僅適用於北/南流量流程，不允許 VPC-to-VPC連線。如需詳細資訊，請參閱 Direct Connect 文件中的虛擬私有閘道關聯。使用此選項時，連線不限於 Direct Connect 位置所在的 AWS 區域。 Direct Connect gateway 僅適用於北/南流量流程，不允許 VPC-to-VPC的連

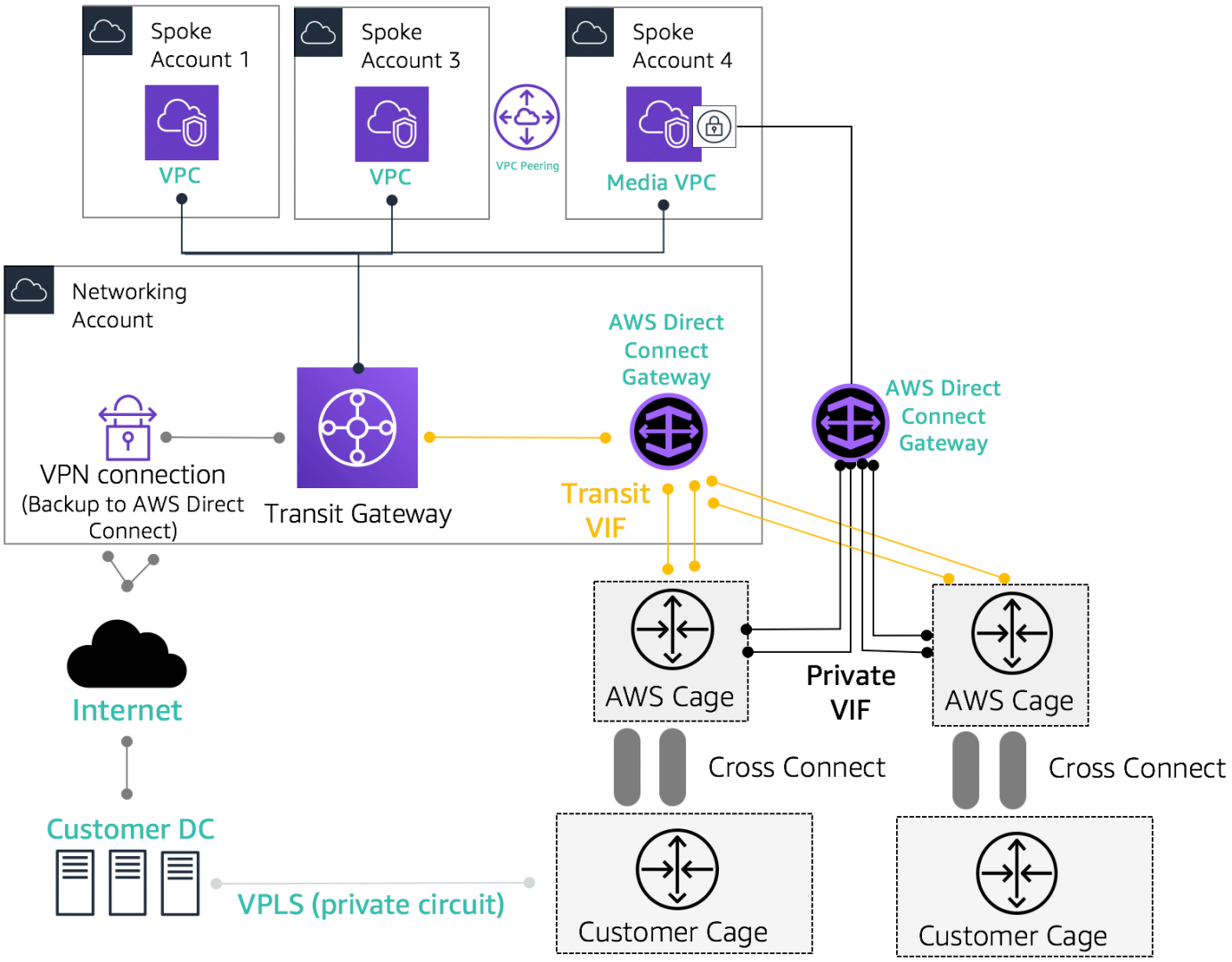
線。此規則的例外狀況是，當超級網路在兩個或多個 VPCs 之間進行公告，而這兩個 VPC 的連接 VGWs與相同 Direct Connect 閘道相關聯，且位於相同的虛擬介面上。在這種情況下，VPCs 可以透過 Direct Connect 端點彼此通訊。如需詳細資訊，請參閱Direct Connect 閘道文件。

- 選項 3：建立傳輸 VIF 至與 Transit Gateway 相關聯的 Direct Connect 閘道 — 您可以使用 Transit VIF 將 Transit Gateway 執行個體與 Direct Connect 閘道建立關聯。 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。這可讓您以 50、100、200、300、400 和 500 Mbps 的速度使用 Direct Connect 連線至 Transit Gateway。Transit VIF 可讓您透過單一傳輸 VIF 和 BGP 對等互連，將內部部署資料中心連接至每個 Direct Connect 閘道最多六個 Transit Gateway 執行個體（可連接至數千個 VPCs)，跨不同 AWS 區域和 AWS 帳戶。這是大規模連接多個 VPCs的選項中最簡單的設定，但您應該注意 Transit Gateway 配額。要注意的一個關鍵限制是，您只能透過傳輸 VIF，將 200 個字首從 Transit Gateway 公告到內部部署路由器。使用先前的選項，您需為 Direct Connect 定價付費。對於此選項，您還需要支付 Transit Gateway 連接和資料處理費用。如需詳細資訊，請參閱 Direct Connect 上的 Transit Gateway Associations 文件。
- 選項 4：透過 Direct Connect 公有 VIF 建立與 Transit Gateway 的 VPN 連線 — 公有 VIF 可讓您使用公有 IP 地址存取所有 AWS 公有服務和端點。當您在 Transit Gateway 上建立 VPN 連接時，您會在 AWS 端取得兩個 VPN 端點的公有 IP 地址。這些公有 IPs可透過公有 VIF 存取。您可以透過公有 VIF 建立任意數目的 VPN 連線至任意數目的 Transit Gateway 執行個體。當您透過公有 VIF 建立 BGP 對等互連時，AWS 會將整個 AWS 公有 IP 範圍公告至您的路由器。為了確保您只允許特定流量（例如，只允許流向 VPN 終止端點的流量），建議您使用防火牆內部部署設施。此選項可用於在網路層加密 Direct Connect。
- 選項 5： Direct Connect 使用私有 IP VPN 建立對 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 Direct Connect 部署 AWS Site-to-Site VPN 連線。使用此功能，您可以透過 Direct Connect 連線來加密內部部署網路與 AWS 之間的流量，而不需要公有 IP 地址，因此可同時提高安全性和網路隱私權。私有 IP VPN 部署在 Transit VIFs之上，因此可讓您使用 Transit Gateway 以更安全、私密和可擴展的方式，集中管理客戶的 VPCs 和內部部署網路的連線。
- 選項 6：透過傳輸 VIF 建立 GRE 通道至 Transit Gateway – Transit Gateway Connect 連接類型支援 GRE。透過 Transit Gateway Connect，SD-WAN 基礎設施可以原生連接到 AWS，而無需在 SD-WAN 網路虛擬設備與 Transit Gateway 之間設定 IPsec VPNs。GRE 通道可透過傳輸 VIF 建立，以 Transit Gateway Connect 做為連接類型，提供比 VPN 連線更高的頻寬效能。如需詳細資訊，請參閱使用 AWS Transit Gateway Connect 簡化 SD-WAN 連線部落格文章。

「將 VIF 傳輸到 Direct Connect 閘道」選項似乎是最佳選項，因為它可讓您使用每個 Direct Connect 連線的單一 BGP 工作階段，在 AWS 區域 單一點 （傳輸閘道） 整合給定的所有內部部署連線；不過，此選項的一些限制和考量可能會導致您使用私有和傳輸 VIFs，以符合您的登陸區域連線需求。

下圖說明的範例設定，其中 Transit VIF 用作連線至 VPCs的預設方法，而私有 VIF 用於邊緣使用案例，其中必須從現場部署資料中心將非常大量的資料傳輸到媒體 VPC。私有 VIF 用於避免 Transit Gateway 資料處理費用。最佳實務是，您應該在兩個不同的 Direct Connect 位置有至少兩個連線，才能達到最大備援，總共四個連線。您為每個連線建立一個 VIF，總共四個私有 VIFs和四個傳輸 VIFs。您也可以建立 VPN 做為 Direct Connect 連線的備份連線。

使用「透過傳輸 VIF 建立 GRE 通道到傳輸閘道」選項，您可以原生連接 SD-WAN 基礎設施與 AWS。它不需要在 SD-WAN 網路虛擬設備與 Transit Gateway 之間設定 IPsec VPNs。



混合連線的範例參考架構

使用 Network Services 帳戶來建立 Direct Connect 資源，以分隔網路管理界限。Direct Connect 連線、Direct Connect 閘道和 Transit Gateways 都可以位於 Network Services 帳戶中。若要與您的登陸區域共用 Direct Connect 連線，只需透過 AWS RAM 與其他帳戶共用 Transit Gateway。

Direct Connect 連線上的 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) 搭配 10 Gbps 和 100 Gbps 專用連線的 Direct Connect 連線。透過此功能，客戶可以在第 2 層保護其資料，而 Direct Connect 則提供point-to-point加密。若要啟用 Direct Connect MACsec 功能，請確定符合 MACsec 先決條件。由於 MACsec 會hop-by-hop連結，因此您的裝置必須具有我們的 Direct Connect 裝置的直接第 2 層相鄰。您的最後一哩提供者可協助您驗證連線是否適用於 MACsec。如需詳細資訊，請參閱將 MACsec 安全性新增至 AWS Direct Connect 連線。

Direct Connect 彈性建議

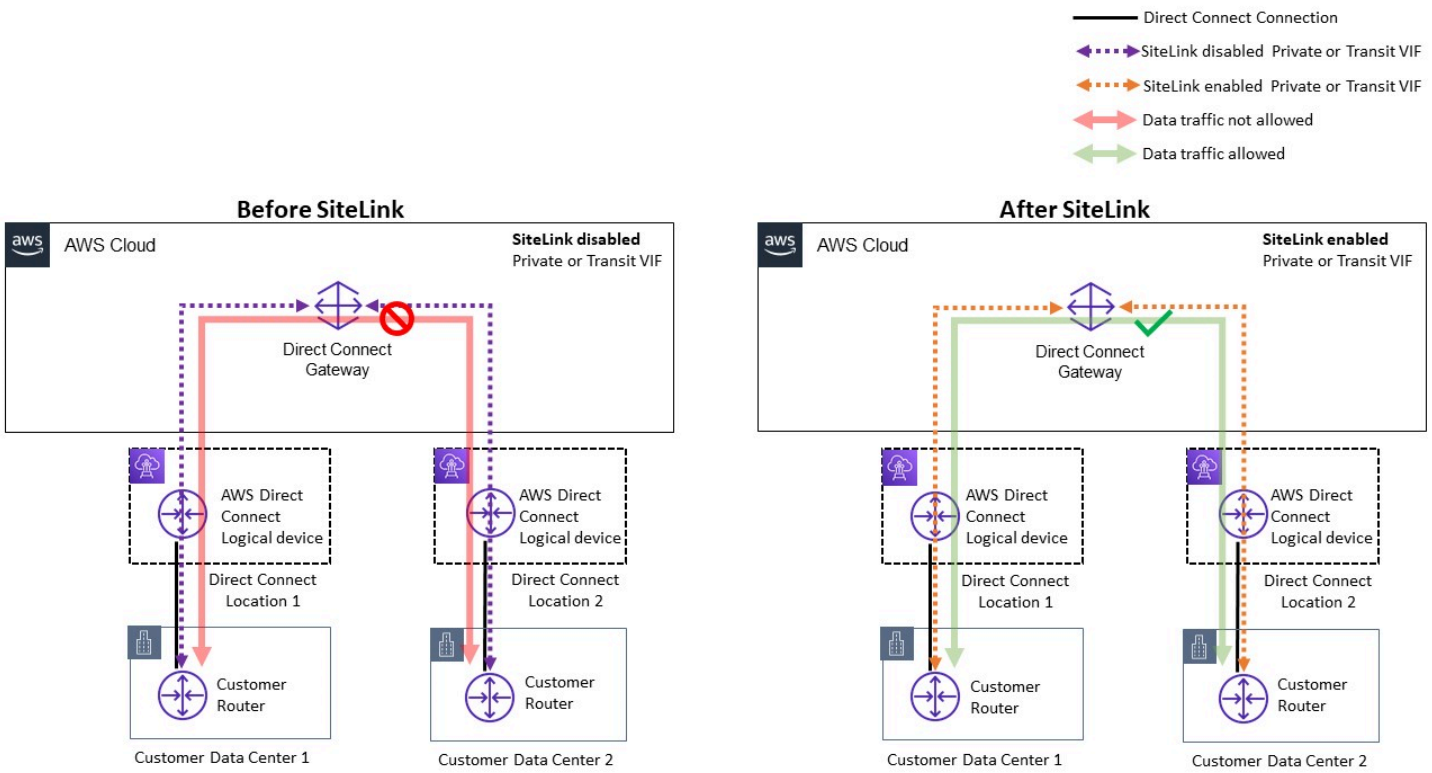
使用 Direct Connect，客戶可以從內部部署網路實現對 Amazon VPCs和 AWS 資源的高度彈性連線。最佳實務是客戶從多個資料中心連線，以消除任何單點實體位置故障。建議客戶根據工作負載類型，使用多個 Direct Connect 連線進行備援。

AWS 也提供 Direct Connect 彈性工具組，可為客戶提供具有多個備援模型的連線精靈；協助他們判斷哪個模型最適合其服務層級協議 (SLA) 需求，並使用 Direct Connect 連線相應地設計其混合連線。如需詳細資訊，請參閱Direct Connect 彈性建議。

Direct Connect SiteLink

先前，只有透過深色光纖或其他技術、IPSEC VPNs 使用直接電路建置，或使用第三方電路供應商搭配 MPLS、MetroEthernet 或舊版 T1 電路等技術，才能為您的內部部署網路設定site-to-site站台連結。隨著 SiteLink 的到來，客戶現在可以為其內部部署位置啟用直接site-to-site連線，而這些連線會在某個 Direct Connect 位置終止。使用您的 Direct Connect 電路提供site-to-site的連線，而無需透過 VPCs路由流量，完全繞過 AWS 區域。

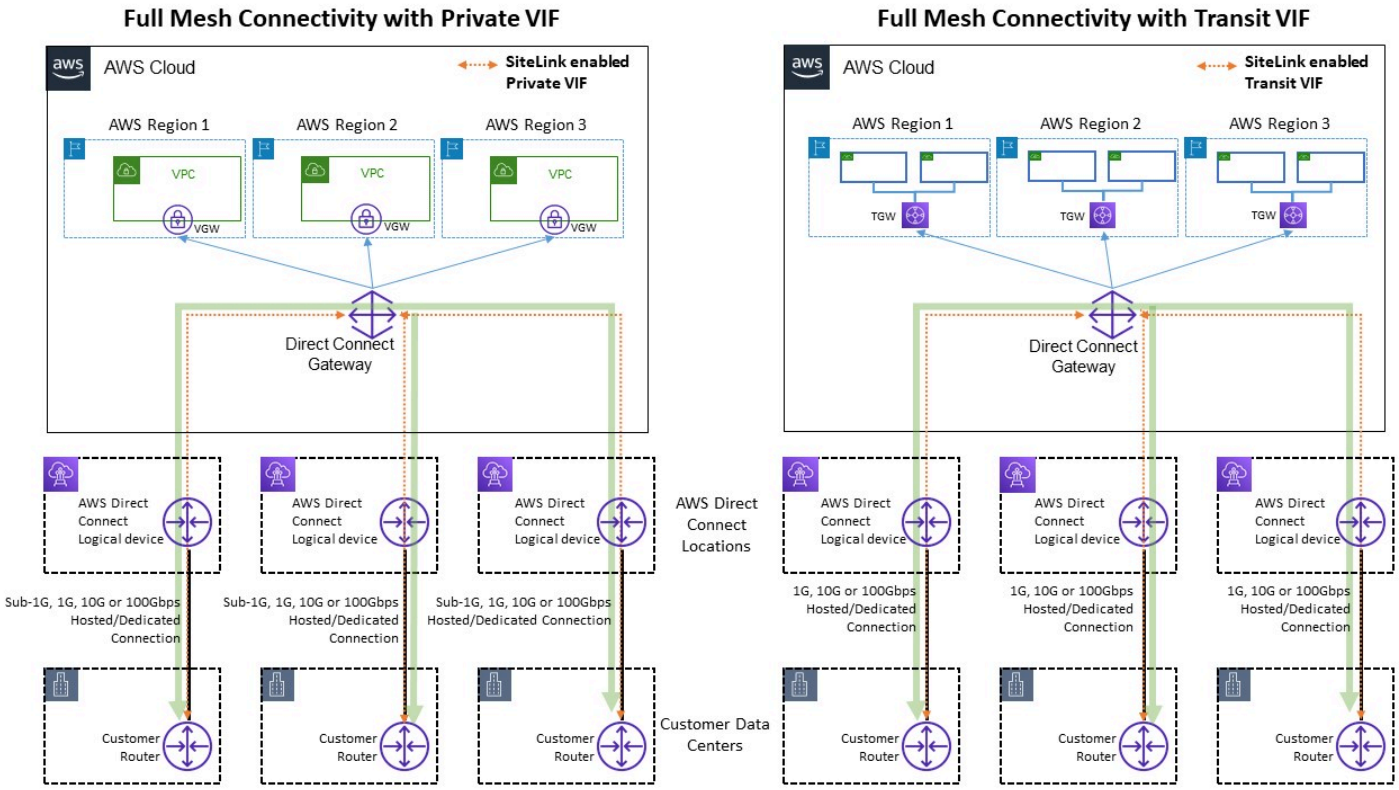
現在，您可以透過 Direct Connect 位置之間的最快路徑傳送資料，在 全球網路的辦公室和資料中心之間建立全球、可靠且pay-as-you-go的連線。



for Direct Connect SiteLink 的範例參考架構

使用 SiteLink 時，您首先會將內部部署網路連接到全球超過 100 個 Direct Connect 位置的 AWS。然後，您可以在這些連線上建立虛擬介面 VIFs)，並啟用 SiteLink。一旦所有 VIFs都連接到相同的 Direct Connect 閘道 (DXGW)，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 Direct Connect 位置到目的地之間的最短路徑。您不需要有任何資源 AWS 區域 ，即可使用 SiteLink。

使用 SiteLink，DXGW 會透過啟用 SiteLink VIFs 從您的路由器學習 IPv4/IPv6 字首、執行 BGP 最佳路徑演算法、更新 NextHop 和 AS_Path 等屬性，並將這些 BGP 字首重新公告至與該 DXGW 相關聯的其他啟用 SiteLink VIFs。如果您在 VIF 上停用 SiteLink，DXGW 不會將此 VIF 上學到的內部部署字首公告給其他已啟用 SiteLink VIFs。SiteLink 停用 VIF 的內部部署字首只會公告至 DXGW Gateway 關聯，例如與 DXGW 相關聯的 AWS Virtual Private Gateways (VGWs) 或 Transit Gateway (TGW) 執行個體。



Sitelink 允許流量流程範例

SiteLink 可讓客戶使用 AWS 全域網路，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，並搭配動態路由來控制哪些位置可以彼此通訊，以及與 AWS 區域資源通訊。

如需詳細資訊，請參閱 Introducing 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傳出限定網際網路存取（例如，下載程式庫、修補程式或作業系統更新）。這可以同時針對 IPv4 和 IPv6 流量達成。對於 IPv4，這可以透過 NAT 閘道（建議）形式的網路位址轉譯 (NAT) 實現，或者，在 Amazon EC2 執行個體上執行的自我管理 NAT 執行個體，作為所有輸出網際網路存取的方法。內部應用程式位於私有子網路中，而 NAT Gateway 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，因為它們提供了更好的可用性和頻寬，並且需要您更輕鬆進行管理。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，輸出流量可以設定為以分散式方式透過僅輸出網際網路閘道離開每個 VPC，也可以設定為使用 NAT 執行個體或代理執行個體傳送至集中式 VPC。IPv6 模式會在 中討論IPv6 的集中式輸出。

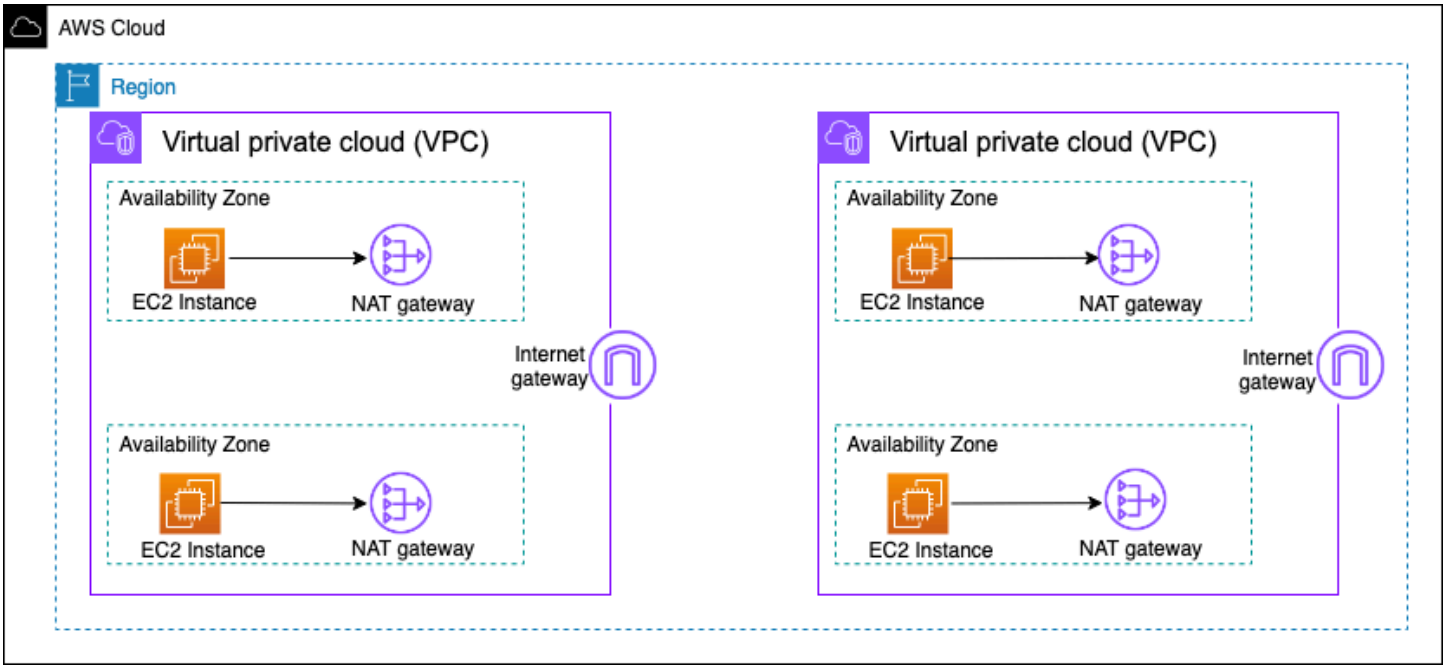
主題

- 使用 NAT 閘道進行集中式 IPv4 輸出
- 使用 NAT 閘道搭配 AWS Network Firewall 進行集中式 IPv4 輸出
- 將 NAT 閘道和 Gateway Load Balancer 與 Amazon EC2 執行個體搭配使用，以進行集中式 IPv4 輸出
- IPv6 的集中式輸出

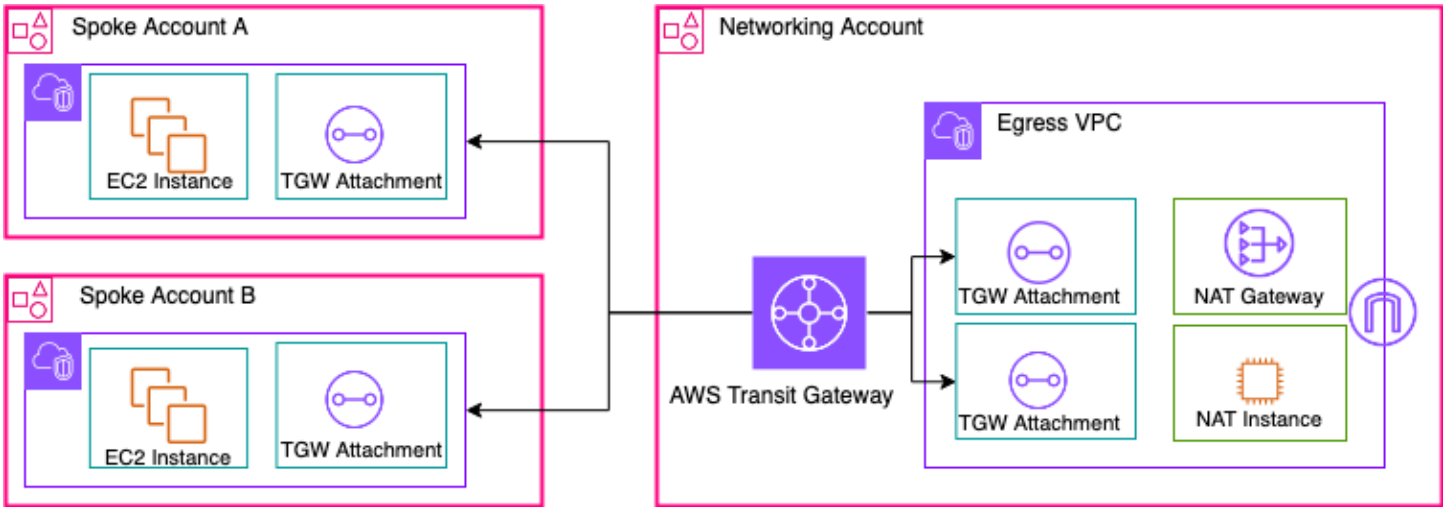
使用 NAT 閘道進行集中式 IPv4 輸出

NAT 閘道是受管網路地址轉譯服務。在每個語音 VPC 中部署 NAT 閘道可能會成本過高，因為您要為部署的每個 NAT 閘道支付每小時費用（請參閱 Amazon VPC 定價）。集中 NAT 閘道是降低成本的可行選項。若要集中，您可以在網路服務帳戶中建立個別的輸出 VPC、在輸出 VPC 中部署 NAT 閘道，並使用 Transit Gateway 或 CloudWAN 將所有來自輻 VPCs輸出流量路由到位於輸出 VPC 中的 NAT 閘道，如下圖所示。

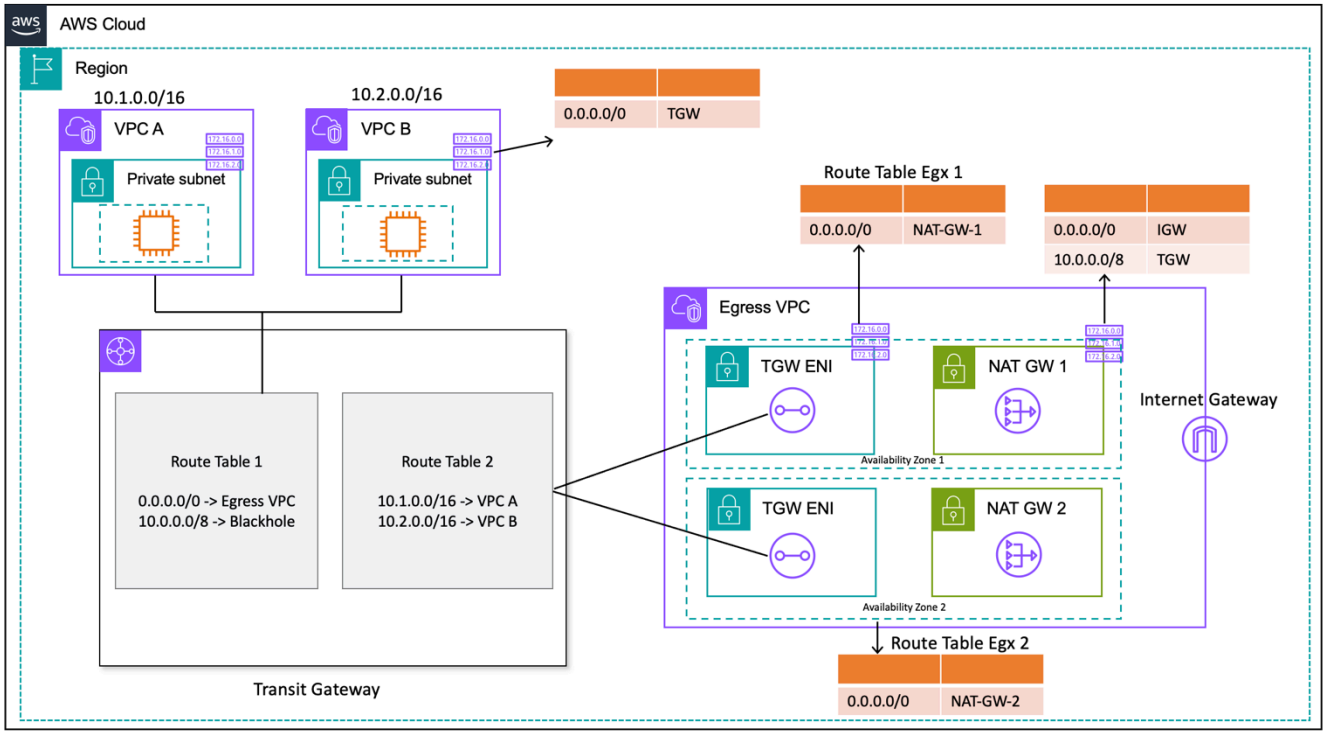
> **Note**
>
> 當您使用 Transit Gateway 集中 NAT 閘道時，您需要支付額外的 Transit Gateway 資料處理費用，相較於在每個 VPC 中執行 NAT 閘道的分散式方法。在某些情況下，當您透過 NAT 閘道從 VPC 傳送大量資料時，將 NAT 本機保留在 VPC 中以避免傳輸閘道資料處理費用可能是更具成本效益的選項。



分散式高可用性 NAT 閘道架構



使用 Transit Gateway 的集中式 NAT 閘道 （概觀）



使用 Transit Gateway 的集中式 NAT 閘道 （路由表設計）

在此設定中，輻 VPC 連接與路由表 1 (RT1) 相關聯，並傳播至路由表 2 (RT2)。有一個 Blackhole 路由不允許兩個 VPCs彼此通訊。如果您想要允許 VPC 間通訊，您可以從 RT1 移除`10.0.0.0/8 -> Blackhole`路由項目。這可讓它們透過傳輸閘道進行通訊。您也可以將語音 VPC 連接傳播到 RT1（或者，您可以使用一個路由表，並將一切關聯/傳播到其中），使用 Transit Gateway 在 VPCs之間啟用直接流量流程。

您可以在 RT1 中新增靜態路由，將所有流量指向輸出 VPC。由於此靜態路由，Transit Gateway 會透過輸出 VPC 中的 ENIs 傳送所有網際網路流量。在輸出 VPC 中，流量會遵循這些 Transit Gateway ENIs所在的子網路路由表中定義的路由。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，以將跨可用區域 (AZ) 流量降至最低。NAT 閘道子網路路由表具有網際網路閘道 (IGW) 作為下一個躍點。若要傳回流量回傳，您必須在 NAT 閘道子網路路由表中新增靜態路由表項目，將所有輻條 VPC 繫結流量指向 Transit Gateway 做為下一個躍點。

高可用性

為了獲得高可用性，您應該使用多個 NAT 閘道 （每個可用區域各一個）。如果 NAT 閘道無法使用，流量可能會捨棄在周遊受影響 NAT 閘道的可用區域中。如果某個可用區域無法使用，傳輸閘道端點和該可用區域中的 NAT 閘道將會失敗，而且所有流量都會流經另一個可用區域中的傳輸閘道和 NAT 閘道端點。

安全

您可以依賴來源執行個體上的安全群組、傳輸閘道路由表中的黑洞路由，以及 NAT 閘道所在子網路的網路 ACL。例如，客戶可以使用 NAT Gateway 公有子網路上的 ACLs（允許或封鎖來源或目的地 IP 地址）。或者，您可以使用 NAT Gateway 搭配 AWS Network Firewall 進行下一節所述的集中式輸出，以滿足此需求。

可擴展性

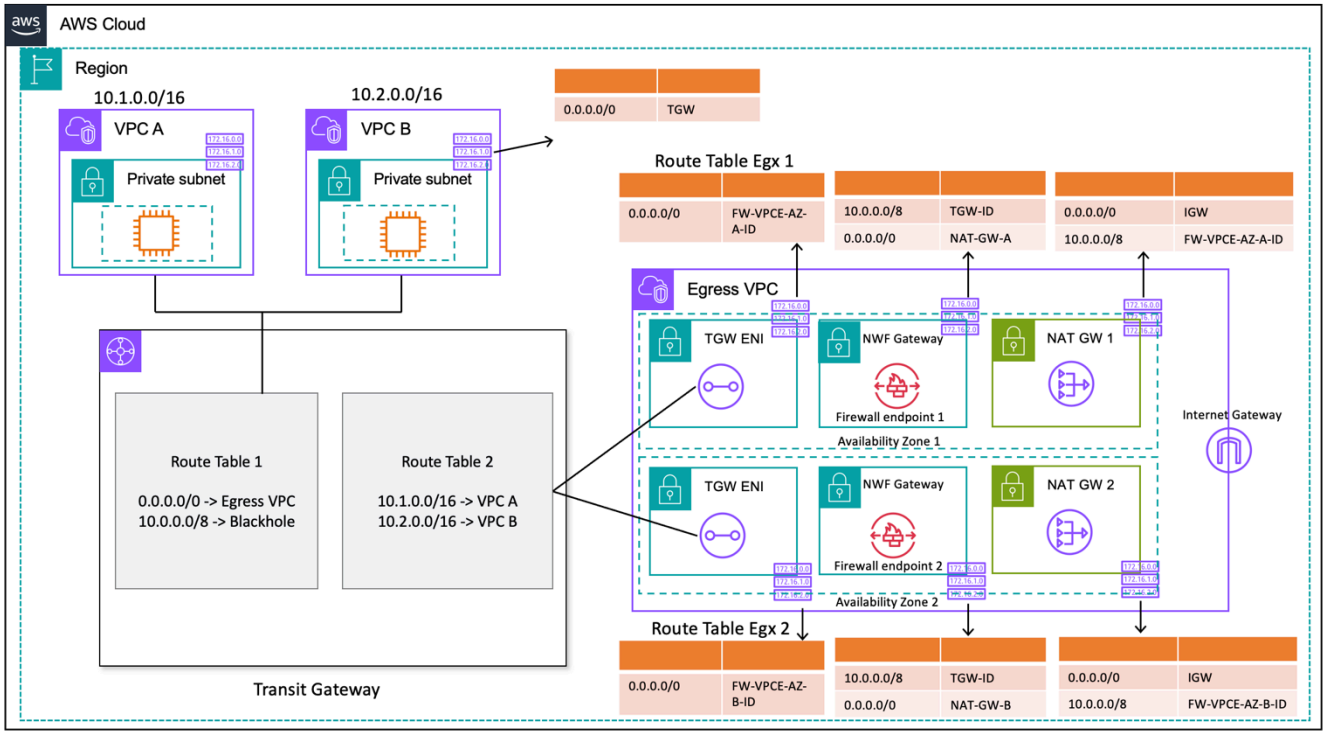
單一 NAT 閘道最多可支援每個指派 IP 地址與每個唯一目的地的 55，000 個同時連線。您可以請求配額調整，以允許最多八個指派的 IP 地址，允許 440，000 個同時連線到單一目的地 IP 和連接埠。NAT 閘道提供 5 Gbps 的頻寬，並自動擴展至 100 Gbps。Transit Gateway 通常不會充當負載平衡器，也不會將流量平均分配到多個可用區域中的 NAT 閘道。如果可能，跨 Transit Gateway 的流量將保持在可用區域內。如果啟動流量的 Amazon EC2 執行個體位於可用區域 1，流量會流出輸出 VPC 中相同可用區域 1 中的 Transit Gateway 彈性網路介面，並根據彈性網路介面所在的子網路路由表，流向下一個躍點。如需完整的規則清單，請參閱 Amazon Virtual Private Cloud 文件中的 NAT 閘道。

如需詳細資訊，請參閱使用 AWS Transit Gateway 從多個 VPCs 建立單一網際網路結束點部落格文章。

使用 NAT 閘道搭配 AWS Network Firewall 進行集中式 IPv4 輸出

如果您想要檢查和篩選傳出流量，您可以將 AWS Network Firewall 與 NAT 閘道整合到集中式輸出架構中。 AWS Network Firewall 是一種受管服務，可讓您輕鬆為所有 VPCs 部署基本網路保護。它可為整個 VPC 提供 Layer 3-7 網路流量的控制和可見性。您可以執行 URL/網域名稱、IP 地址和內容型傳出流量篩選，以停止可能的資料遺失、協助符合合規要求，以及封鎖已知的惡意軟體通訊。 AWS Network Firewall 支援數千個規則，可篩選出目的地為已知不良 IP 地址或不良網域名稱的網路流量。您也可以匯入開放原始碼規則集或使用 Suricata 規則語法編寫自己的入侵預防系統 (IPS) 規則，以使用 Suricata IPS 規則做為 AWS Network Firewall 服務的一部分。 AWS Network Firewall 也可讓您匯入來自 AWS 合作夥伴的相容規則。

在具有檢查的集中式輸出架構中， AWS Network Firewall 端點是輸出 VPC 傳輸閘道連接子網路路由表中的預設路由表目標。使用 檢查輪輻 VPCs 和網際網路之間的流量 AWS Network Firewall ，如下圖所示。



使用 AWS Network Firewall 和 NAT 閘道的集中輸出（路由表設計）

對於使用 Transit Gateway 的集中式部署模型，AWS 建議在多個可用區域中部署 AWS Network Firewall 端點。在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。根據最佳實務，防火牆子網路不應包含任何其他流量，因為 AWS Network Firewall 無法檢查來自防火牆子網路內來源或目的地的流量。

與先前的設定類似，語音 VPC 連接與路由表 1 (RT1) 相關聯，並傳播到路由表 2 (RT2)。系統會明確新增 Blackhole 路由，以禁止兩個 VPCs 彼此通訊。

繼續在 RT1 中使用預設路由，將所有流量指向輸出 VPC。Transit Gateway 會將所有流量轉送到輸出 VPC 中的兩個可用區域之一。一旦流量到達輸出 VPC 中的其中一個 Transit Gateway ENIs，您就會到達預設路由，該路由會將流量轉送至其各自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，再使用預設路由將流量轉送至 NAT 閘道。

此案例不需要 Transit Gateway 設備模式，因為您未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，此函數會在透過 進行流量檢查後由 NAT 閘道處理 AWS Network Firewall。在此情況下，不需要輸入路由，因為傳回流量預設會轉送至 NATGW IPs。

因為您使用的是 Transit Gateway，所以我們可以在 NAT 閘道之前放置防火牆。在此模型中，防火牆可以看到 Transit Gateway 後方的來源 IP。

如果您在單一 VPC 中執行此操作，我們可以使用 VPC 路由增強功能，讓您檢查相同 VPC 中子網路之間的流量。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，以將成本降至最低。 AWS Network Firewall 旨在支援數萬個防火牆規則，並可為每個可用區域擴展高達 100 Gbps 的輸送量。

關鍵考量

- 每個防火牆端點都可以處理大約 100 Gbps 的流量，如果您需要更高的高載或持續輸送量，請聯絡 AWS 支援。
- 如果您選擇在 AWS 帳戶中建立 NAT 閘道以及 Network Firewall，標準 NAT 閘道處理和每小時使用費會因每 GB 的處理和防火牆的使用時數而one-to-one免除。
- 您也可以在沒有 Transit Gateway AWS Firewall Manager 的情況下，透過 考慮分散式防火牆端點。
- 將防火牆規則移至生產環境之前，請先測試防火牆規則，與順序很重要的網路存取控制清單類似。
- 需要進階 Suricata 規則才能進行更深入的檢查。網路防火牆支援輸入和輸出流量的加密流量檢查。
- `HOME_NET` 規則群組變數定義了有資格在具狀態引擎中處理的來源 IP 範圍。使用集中式方法，您必須新增連接到 Transit Gateway 的所有其他 VPC CIDRs，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。
- 考慮在單獨的 Network Services 帳戶中部署 Transit Gateway 和輸出 VPC，以根據職責委派來隔離存取權；例如，只有網路管理員可以存取 Network Services 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位置建立的保護套用至多個帳戶，以集中管理不同的

防火牆。Firewall Manager 支援 Network Firewall 的分散式和集中式部署模型。若要進一步了解，請參閱部落格文章如何使用 部署 AWS Network FirewallAWS Firewall Manager。

將 NAT 閘道和 Gateway Load Balancer 與 Amazon EC2 執行個體搭配使用，以進行集中式 IPv4 輸出

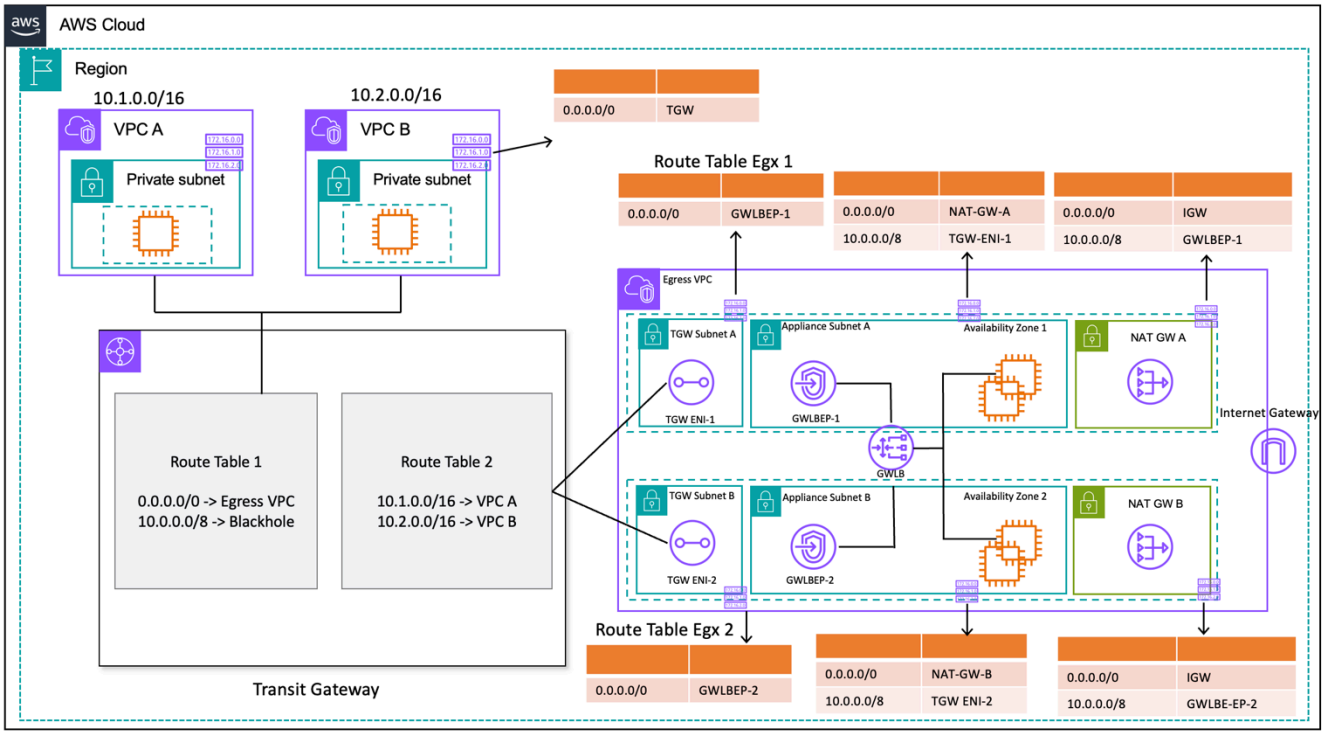
從 AWS Marketplace 和 使用軟體型虛擬設備 （ 在 Amazon EC2 上 ） AWS Partner Network 做為結束點，類似於 NAT 閘道設定。如果您想要使用各種廠商方案的進階 layer 7 防火牆/入侵防護/偵測系統 (IPS/IDS) 和深度封包檢查功能，則可使用此選項。

在下圖中，除了 NAT 閘道之外，您還可以使用 Gateway Load Balancer (GWLB) 後方的 EC2 執行個體部署虛擬設備。在此設定中，GWLB、Gateway Load Balancer Endpoint (GWLBE)、虛擬設備和 NAT 閘道會部署在使用 VPC 連接連接到 Transit Gateway 的集中式 VPC 中。語音 VPCs 也會使用 VPC Attachment 連接到 Transit Gateway。由於 GWLBEs是可路由的目標，因此您可以將往返 Transit Gateway 的流量路由到設定為 GWLB 後方目標的虛擬設備機群。GWLB 充當bump-in-the-wire，並透明地透過第三方虛擬設備傳遞所有第 3 層流量，因此流量的來源和目的地看不到。因此，此架構可讓您集中檢查透過 Transit Gateway 周遊的所有輸出流量。

如需流量如何從 VPCs 中的應用程式流向網際網路及透過此設定傳回的詳細資訊，請參閱使用 AWS Gateway Load Balancer 和 的集中式檢查架構 AWS Transit Gateway。

您可以在 Transit Gateway 上啟用設備模式，以透過虛擬設備維持流程對稱。這表示雙向流量會在流程生命週期內透過相同的設備與可用區域路由。此設定對於執行深度封包檢查的狀態防火牆特別重要。啟用設備模式不需要複雜的解決方法，例如來源網路位址轉譯 (SNAT)，即可強制流量返回正確的設備以維持對稱性。如需詳細資訊，請參閱部署 Gateway Load Balancer 的最佳實務。

您也可以在沒有 Transit Gateway 的情況下以分散式方式部署 GWLB 端點，以啟用輸出檢查。請參閱簡介 AWS Gateway Load Balancer：支援的架構模式部落格文章，進一步了解此架構模式。



使用 Gateway Load Balancer 和 EC2 執行個體的集中式輸出 （路由表設計）

高可用性

AWS 建議在多個可用區域中部署 Gateway Load Balancer 和虛擬設備，以提高可用性。

Gateway Load Balancer 可以執行運作狀態檢查，以偵測虛擬設備故障。如果發生運作狀態不佳的設備，GWLB 會將新的流程重新路由至運作狀態良好的設備。無論目標的運作狀態為何，現有流程一律會移至相同的目標。這可讓連線耗盡，並因應設備上 CPU 峰值所造成的運作狀態檢查失敗。如需詳細資訊，請參閱部落格文章中第 4 節：了解設備與可用區域故障案例部署 Gateway Load Balancer 的最佳實務。Gateway Load Balancer 可以使用自動擴展群組作為目標。此優點會讓管理設備機群的可用性和可擴展性變得繁重。

優點

Gateway Load Balancer 和 Gateway Load Balancer 端點採用 技術 AWS PrivateLink，可安全地跨 VPC 邊界交換流量，而無需周遊公有網際網路。

Gateway Load Balancer 是一項受管服務，可減輕管理、部署、擴展虛擬安全設備的繁重工作，讓您可以專注於重要的事項。Gateway Load Balancer 可以將防火牆堆疊公開為端點服務，讓客戶可以使用訂閱 AWS Marketplace。這稱為 Firewall as a Service (FWaaS)；它引入了簡化的部署，並不需要依賴 BGP 和 ECMP 在多個 Amazon EC2 執行個體之間分配流量。

關鍵考量

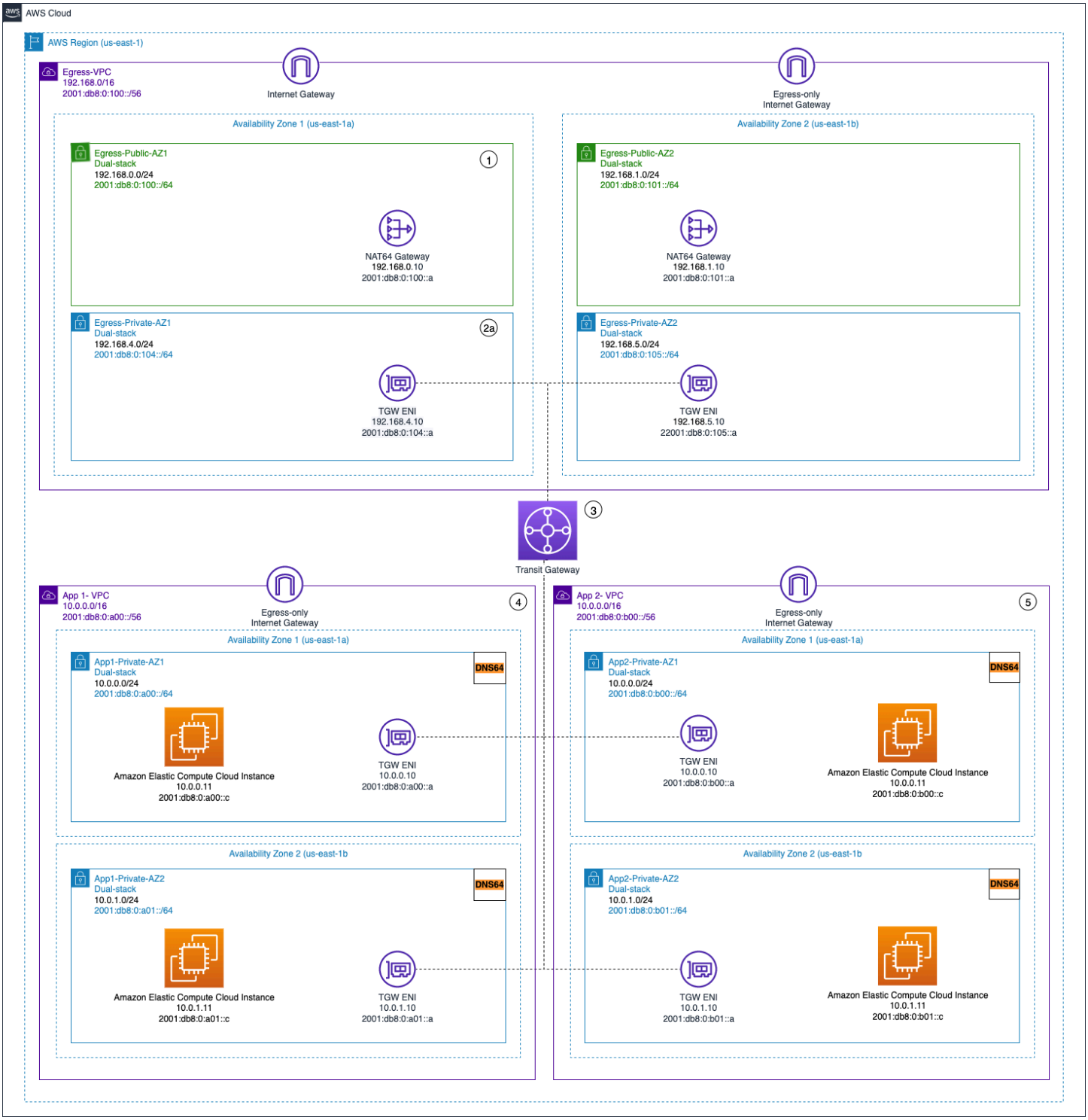
- 設備需要支援 Geneve 封裝通訊協定，才能與 GWLB 整合。
- 某些第三方設備可以支援 SNAT 和覆蓋路由 (雙臂模式)，因此不需要建立 NAT 閘道來節省成本。不過，使用此模式之前，請先諮詢您選擇的 AWS 合作夥伴，因為這取決於廠商支援和實作。
- 請記下 GWLB 閒置逾時。這可能會導致用戶端的連線逾時。您可以在用戶端、伺服器、防火牆和作業系統層級上調整逾時，以避免這種情況。如需詳細資訊，請參閱Load Balancer部署 Gateway Load Balancer 最佳實務部落格文章中的調整 TCP 保持連線或逾時值，以支援長期 TCP 流程。
- GWLBE 採用 技術 AWS PrivateLink，因此會產生 AWS PrivateLink 費用。您可以在 AWS PrivateLink 定價頁面中進一步了解。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。
- 考慮在單獨的 Network Services 帳戶中部署 Transit Gateway 和輸出 VPC，以根據職責委派來隔離存取權，例如只有網路管理員可以存取 Network Services 帳戶。

IPv6 的集中式輸出

若要在具有集中式 IPv4 輸出的雙堆疊部署中支援 IPv6 輸出，必須選擇兩種模式之一： IPv4

- 具有分散式 IPv6 輸出的集中式 IPv4 輸出 IPv6
- 集中式 IPv4 輸出和集中式 IPv6 輸出

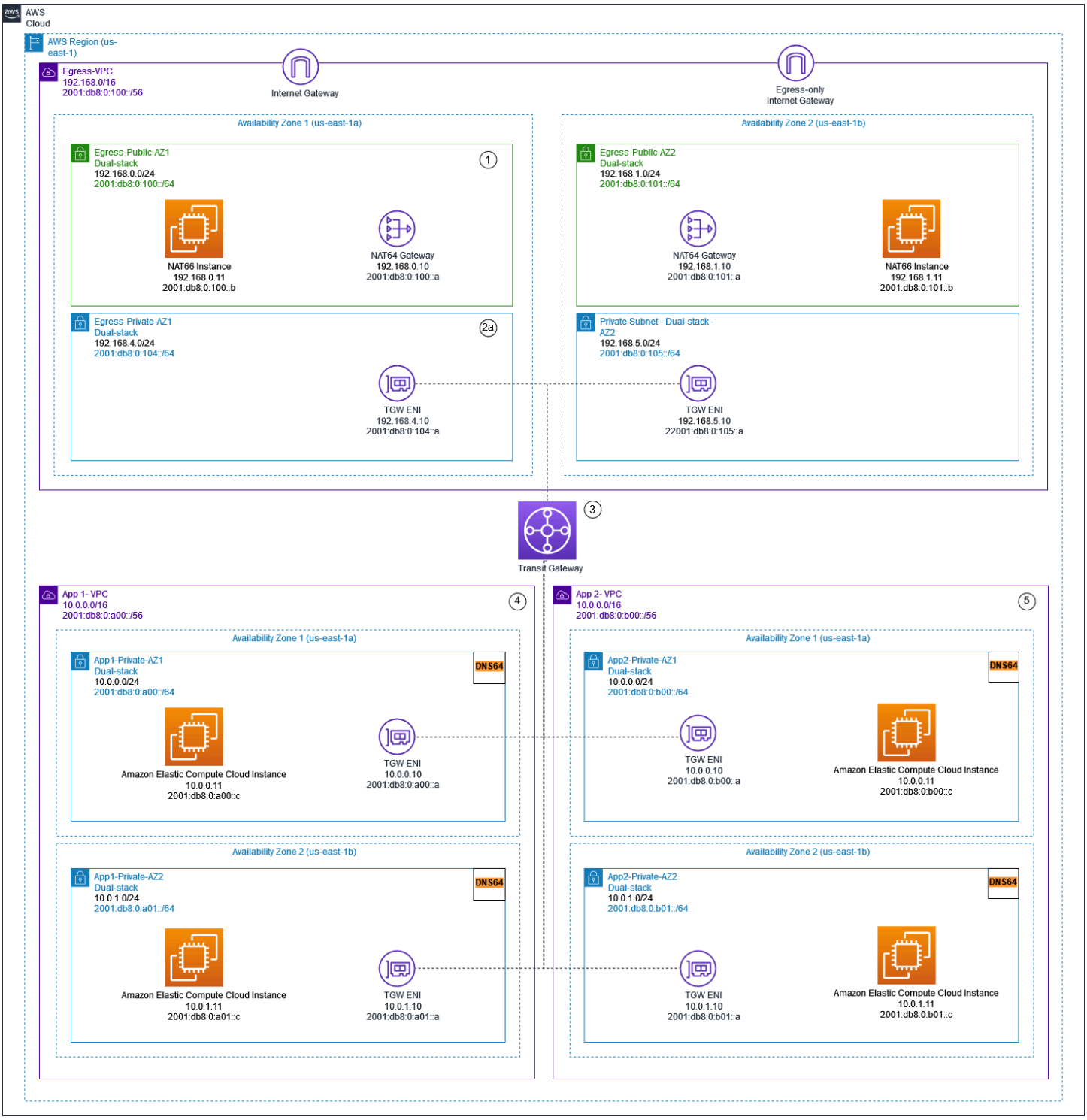
在下圖所示的第一個模式中，輸出限定網際網路閘道會部署在每個輪輻 VPC 中。僅輸出網際網路閘道是水平擴展、備援和高可用性的閘道，允許透過 IPv6 從 VPC 內的執行個體進行傳出通訊。它們可防止網際網路啟動與執行個體的 IPv6 連線。僅限輸出的網際網路閘道不收費。在此部署模型中，IPv6 流量會從每個 VPC 中的輸出限定網際網路閘道流出，而 IPv4 流量會透過部署的集中式 NAT 閘道流出。



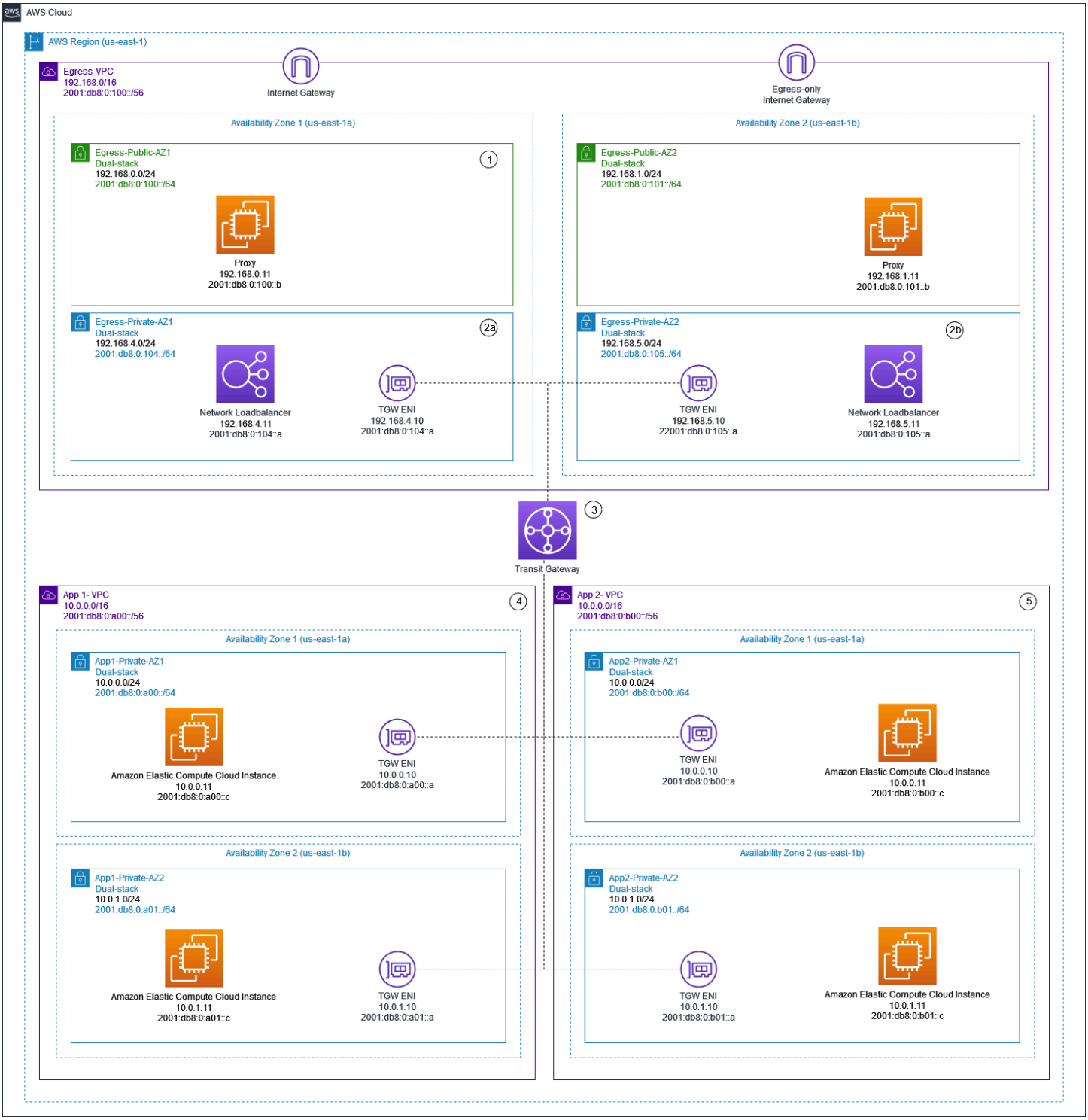
集中 IPV4 輸出和僅分散式傳出 IPv6 輸出

在第二個模式中，如下圖所示，來自執行個體的輸出 IPv6 流量會傳送至集中式 VPC。這可以透過搭配使用 IPv6-to-IPv6 網路字首轉譯 (NPTv6) 與 NAT66 執行個體和 NAT 閘道，或使用 Proxy 執行個體和

Network Load Balancer 來完成。如果需要針對傳出流量進行集中流量檢查，且無法在每個輪輻 VPC 中執行，則此模式適用。



使用 NAT 閘道和 NAT66 執行個體的集中式 IPv6 輸出 NAT66



使用代理執行個體和 Network Load Balancer 的集中式 IPv4 和 IPv6 輸出

AWS 上的 IPv6 白皮書說明集中式 IPv6 輸出模式。IPv6 輸出模式會在部落格中更詳細地討論雙堆疊 IPv4 和 IPv6 VPCs 的集中式傳出網際網路流量，以及特殊考量、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。

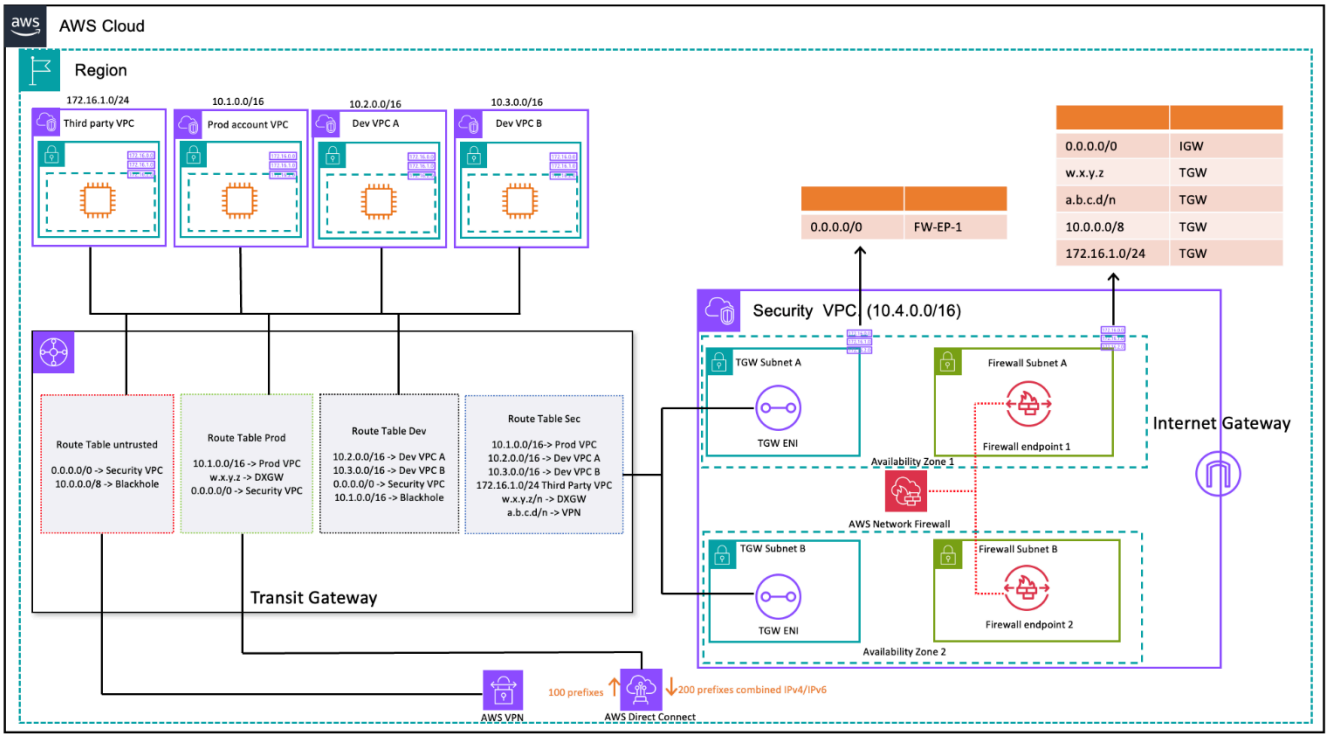
使用集中式網路安全性檢查模型的考量

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

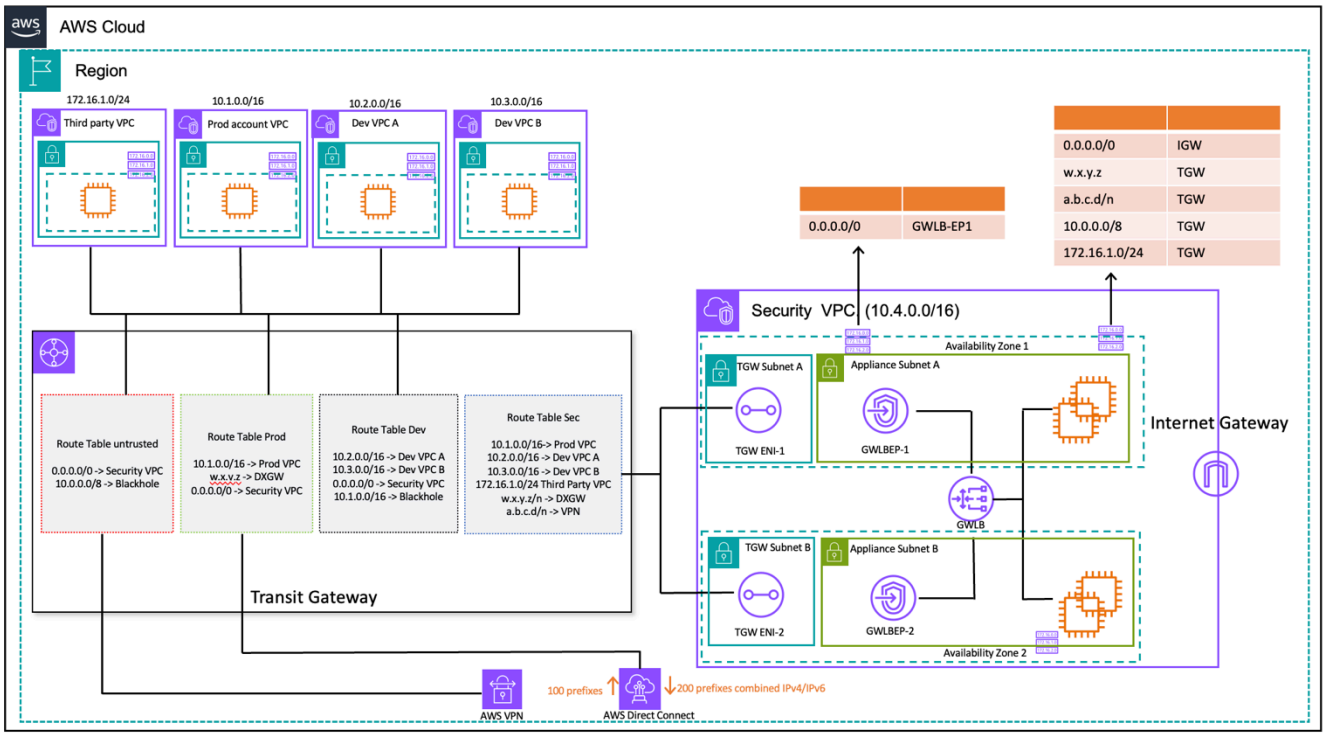
客戶通常會希望整合虛擬應用裝置來處理流量篩選，並提供安全性檢查功能。在這種使用案例中，他們可以整合閘道 Load Balancer、虛擬應用裝置和 Transit Gateway，以部署集中式架構以檢查 VPC 到 VPC 和 VPC 流量。to-on-premises

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

集中式傳入檢查

面向網際網路的應用程式本質上具有較大的攻擊面，並且暴露於大多數其他類型的應用程式不需要面對的威脅類別。擁有對這些類型應用程式進行攻擊的必要保護，並將影響表面積降至最低，是任何安全策略的核心部分。

當您在登陸區域中部署應用程式時，使用者將透過公有網際網路（例如，透過內容交付網路 (CDN)，或透過面向公有的 Web 應用程式），透過面向公有的負載平衡器、API 閘道或直接透過網際網路閘道存取許多應用程式。在這種情況下，您可以使用 AWS Web Application Firewall (AWS WAF) 進行傳入應用程式檢查，或使用 Gateway Load Balancer 或 進行 IDS/IPS 傳入檢查，來保護工作負載和應用程式 AWS Network Firewall。

當您繼續在登陸區域中部署應用程式時，您可能需要檢查傳入網際網路流量。您可以使用執行第三方防火牆設備的 Gateway Load Balancer，或透過使用開放原始碼 Suricata 規則 AWS Network Firewall 搭配進階 DPI 和 IDS/IPS 功能，以多種方式使用分散式、集中式或合併的檢查架構。本節涵蓋 Gateway Load Balancer 和 AWS Network Firewall 集中式部署，使用 AWS Transit Gateway 做為路由流量的中央中樞。

AWS WAF 和 AWS Firewall Manager 用於檢查來自網際網路的傳入流量

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 APIs 不受可能影響可用性、危及安全性或消耗過多資源的常見 Web 入侵和機器人影響。可讓您建立安全規則來控制流量到達應用程式 AWS WAF 的方式，以控制機器人流量並封鎖常見的攻擊模式，例如 SQL Injection 或跨網站指令碼 (XSS)。您也可以自訂篩選出特定流量模式的規則。

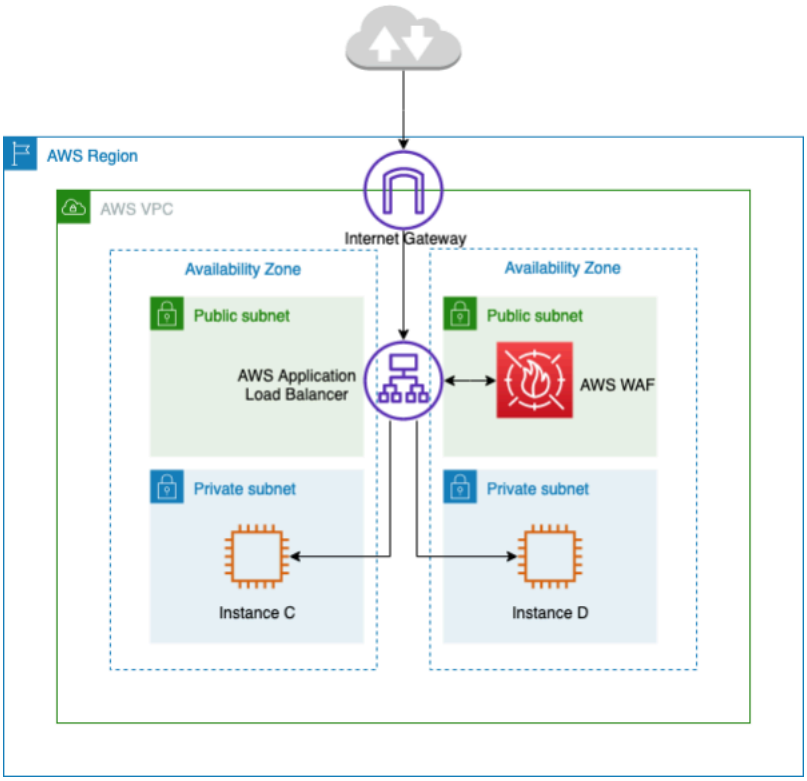
您可以在 Amazon CloudFront AWS WAF 上部署 做為 CDN 解決方案的一部分、面向 Web 伺服器的 Application Load Balancer、適用於 REST APIs Amazon API Gateway，或 AWS AppSync 適用於 GraphQL APIs。

部署之後 AWS WAF，您可以使用視覺化規則建置器、JSON 中的程式碼、由 維護的受管規則，或是從 訂閱第三方規則 AWS，來建立自己的流量篩選規則 AWS Marketplace。這些規則可以透過根據指定的模式評估流量來篩選掉不需要的流量。您可以進一步使用 Amazon CloudWatch 來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 是一種安全管理服務，可讓您集中設定和管理防火牆規則。當您建立新的應用

程式時， 會強制執行一組常見的安全規則， AWS Firewall Manager 讓新的應用程式和資源輕鬆符合規範。

使用 AWS Firewall Manager，您可以輕鬆推出 Application Load Balancer、API Gateway 執行個體和 Amazon CloudFront 分佈的 AWS WAF 規則。 與 AWS Firewall Manager 整合 AWS 受管規則 AWS WAF，可讓您輕鬆地在應用程式上部署預先設定、策劃的 AWS WAF 規則。如需 AWS WAF 使用 集中管理的詳細資訊 AWS Firewall Manager，請參閱集中管理 AWS WAF (API v2) AWS 受管規則 和大規模管理 AWS Firewall Manager。



使用 的集中傳入流量檢查 AWS WAF

在上述架構中，應用程式會在私有子網路中多個可用區域中的 Amazon EC2 執行個體上執行。在 Amazon EC2 執行個體前面部署了面向公有的 Application Load Balancer (ALB)，負載平衡不同目標之間的請求。與 AWS WAF ALB 相關聯。

優點

- 使用AWS WAF 機器人控制，您可以掌握和控制應用程式常用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 APIs免受常見威脅。您可以從許多規則類型中進行選擇，例如解決開放式 Web 應用程式安全專案 (OWASP) 前 10 個安全風險、WordPress 或 Joomla 等內容管理系統 (CMS) 特定威脅，甚至是新興的常見漏洞與暴

露 (CVE) 等問題的規則類型。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 是一項受管服務，在此架構中檢查不需要任何設備。此外，它透過 Amazon Data Firehose. AWS WAF gives 提供近乎即時的日誌，近乎即時的 Web 流量可見性，您可以用來在 Amazon CloudWatch 中建立新的規則或提醒。

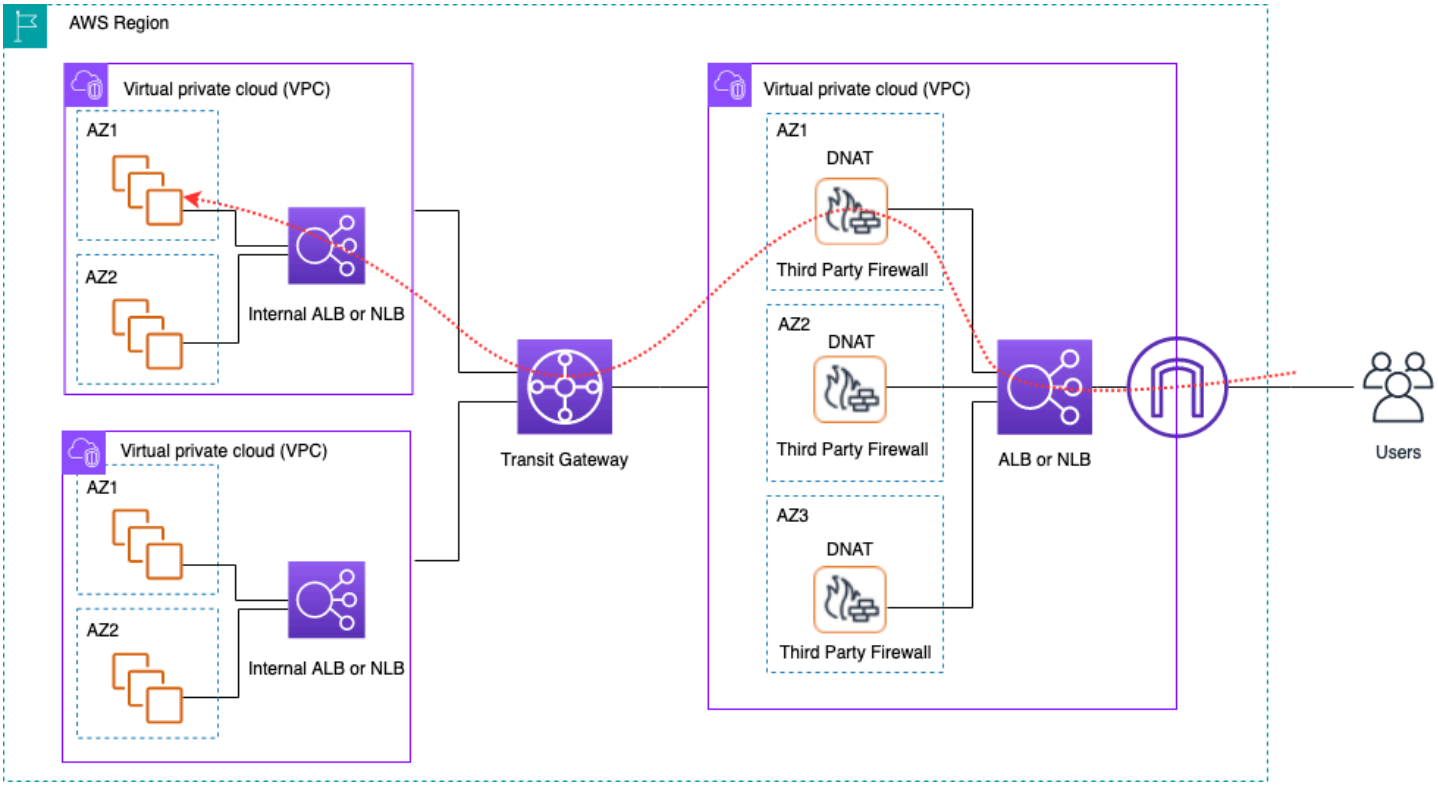
關鍵考量

- 此架構最適合 HTTP 標頭檢查和分散式檢查，因為 AWS WAF 整合在每個 ALB、CloudFront 分佈和 API Gateway 上。 AWS WAF 不會記錄請求內文。
- 前往第二組 ALB （如果有） 的流量可能無法由相同的 AWS WAF 執行個體檢查；因為會向第二組 ALB 提出新的請求。

使用第三方設備集中檢查傳入

在此架構設計模式中，您會在 Amazon EC2 上跨 Elastic Load Balancer (ELB) 後方的多個可用區域部署第三方防火牆設備，例如獨立檢測 VPC 中的 Application/Network Load Balancer。

檢查 VPC 和其他輻 VPCs 透過 Transit Gateway 做為 VPC 連接連接在一起。輸換 VPCs 中的應用程式由內部 ELB 做為前端，其可以是 ALB 或 NLB，視應用程式類型而定。透過網際網路的用戶端會連線至檢查 VPC 中外部 ELB 的 DNS，該 VPC 會將流量路由到其中一個防火牆設備。防火牆會檢查流量，然後使用內部 ELB 的 DNS 將流量路由至透過 Transit Gateway 的 Spoke VPC，如下圖所示。如需使用第三方設備進行傳入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。



使用第三方設備與 ELB 進行集中式輸入流量檢查

優點

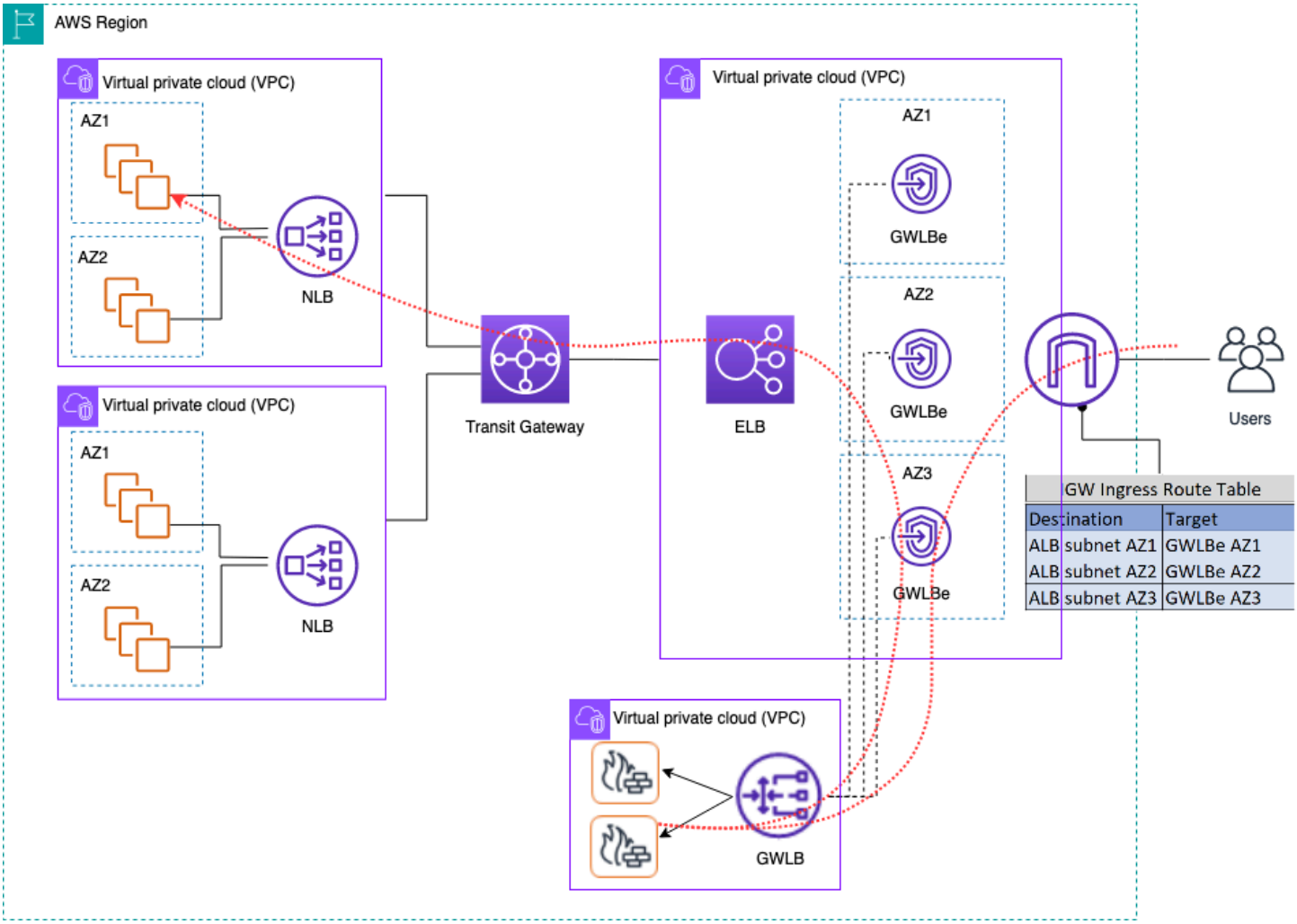
- 此架構可支援透過第三方防火牆設備提供的任何檢查和進階檢查功能應用程式類型。
- 此模式支援從防火牆設備進行 DNS 型路由以發言 VPCs，這可讓發言 VPCs中的應用程式在 ELB 後方獨立擴展。
- 您可以使用 Auto Scaling 搭配 ELB 來擴展檢測 VPC 中的防火牆設備。

關鍵考量

- 您需要跨可用區域部署多個防火牆設備，以獲得高可用性。
- 防火牆需要使用 設定並執行來源 NAT，以維護流程對稱性，這表示應用程式看不到用戶端 IP 地址。
- 請考慮在 Network Services 帳戶中部署傳輸閘道和檢查 VPC。
- 其他第三方供應商防火牆授權/支援成本。Amazon EC2 費用取決於執行個體類型。

使用防火牆設備搭配 Gateway Load Balancer 檢查來自網際網路的傳入流量

客戶使用第三方新一代防火牆 (NGFW) 和入侵預防系統 (IPS) 作為深度防禦策略的一部分。 傳統上，這些通常是專用硬體或軟體/虛擬設備。您可以使用 Gateway Load Balancer 水平擴展這些虛擬設備，以檢查進出 VPC 的流量，如下圖所示。



使用防火牆設備搭配 Gateway Load Balancer 的集中式傳入流量檢查

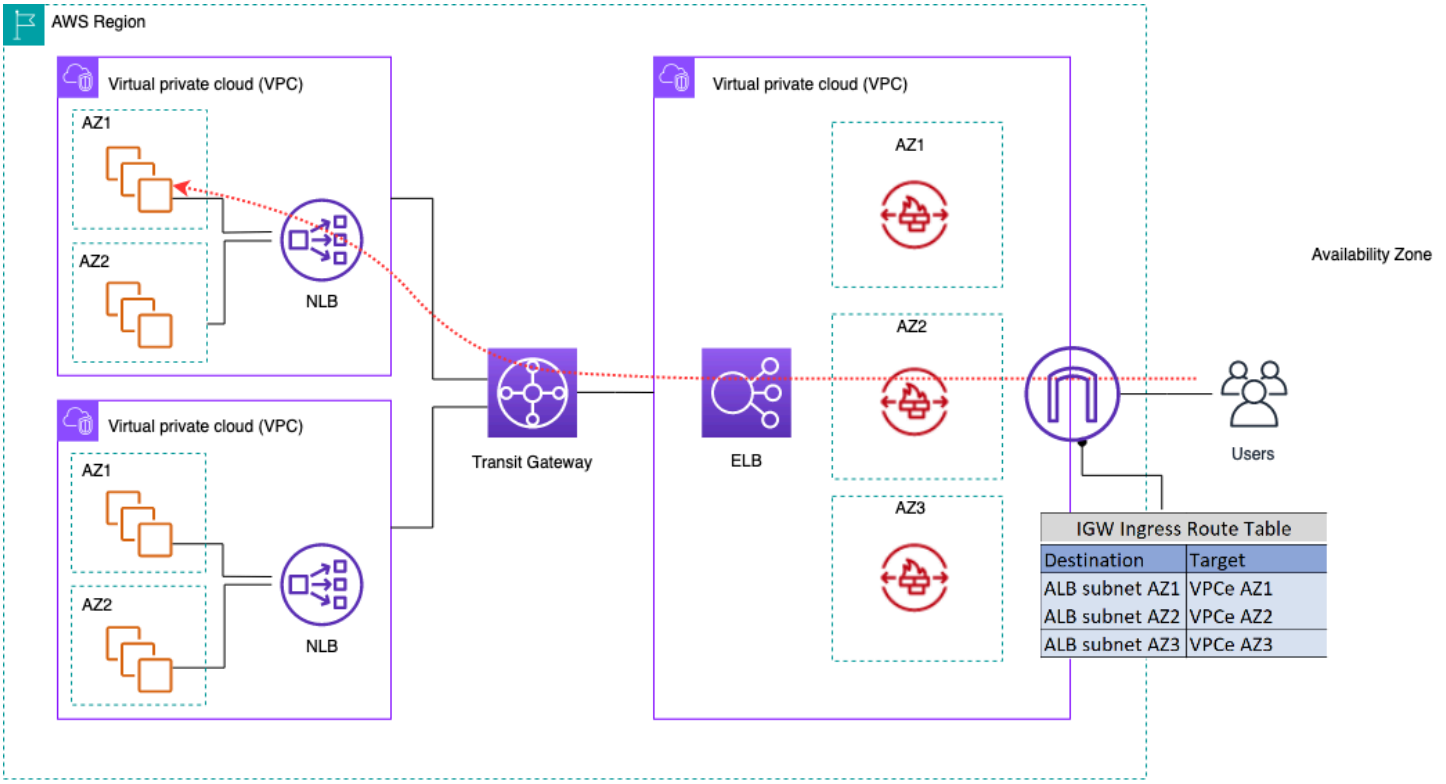
在上述架構中，Gateway Load Balancer 端點會部署到個別邊緣 VPC 中的每個可用區域。新一代防火牆、入侵防護系統等會部署在集中式設備 VPC 的 Gateway Load Balancer 後方。此裝置 VPC 可以位於與語音 VPCs 或不同 AWS 帳戶相同的 AWS 帳戶中。虛擬設備可設定為使用 Auto Scaling 群組，並自動向 Gateway Load Balancer 註冊，允許自動擴展安全層。

這些虛擬設備可以透過網際網路閘道 (IGW) 存取其管理介面，或使用設備 VPC 中的堡壘主機設定來管理。

使用 VPC 傳入路由功能，邊緣路由表會更新，以將傳入流量從網際網路路由到 Gateway Load Balancer 後方的防火牆設備。檢查的流量會透過 Gateway Load Balancer 端點路由至目標 VPC 執行個體。如需各種 AWS Gateway Load Balancer 使用方式的詳細資訊，請參閱簡介 Gateway Load Balancer：支援的架構模式部落格文章。 Load Balancer

使用 AWS Network Firewall 進行集中式輸入

在此架構中，傳入流量會在到達其餘 VPCs AWS Network Firewall 之前由 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 子網路之間部署公有子網路。您可以使用 ALB 或 NLB，其中包含語音 VPCs中的 IP 目標，同時處理背後目標的 Auto Scaling。



使用 AWS Network Firewall 進行傳入流量檢查

若要簡化此模型 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位置建立的保護套用至多個帳戶，以集中管理不同的防火牆。Firewall Manager 支援 Network Firewall 的分散式和集中式部署模型。部落格文章如何使用 部署 AWS Network FirewallAWS Firewall Manager 提供模型的詳細資訊。

使用 進行深度封包檢查 (DPI) AWS Network Firewall

Network Firewall 可以對輸入流量執行深度封包檢查 (DPI)。使用存放在 (ACM) 中的 Transport Layer Security AWS Certificate Manager (TLS) 憑證，Network Firewall 可以解密封包、執行 DPI 並重新加密封包。使用 Network Firewall 設定 DPI 有幾個考量。首先，信任的 TLS 憑證必須存放在 ACM 中。其次，網路防火牆規則必須設定為正確傳送封包以進行解密和重新加密。如需加密流量和詳細資訊，請參閱部落格文章的 TLS 檢查組態 AWS Network Firewall。

集中式輸入架構 AWS Network Firewall 中 的主要考量事項

- Edge VPC 中的 Elastic Load Balancing 只能將 IP 地址做為目標類型，而非主機名稱。在上圖中，目標為輪換 VPC 中 Network Load Balancer 的私有 IPs。 VPCs 在邊緣 VPC 中使用 ELB 後方的 IP 目標會導致 Auto Scaling 遺失。
- 考慮使用 AWS Firewall Manager 做為防火牆端點的單一玻璃窗格。
- 此部署模型會在進入邊緣 VPC 時使用流量檢查，因此有可能降低檢查架構的整體成本。

DNS

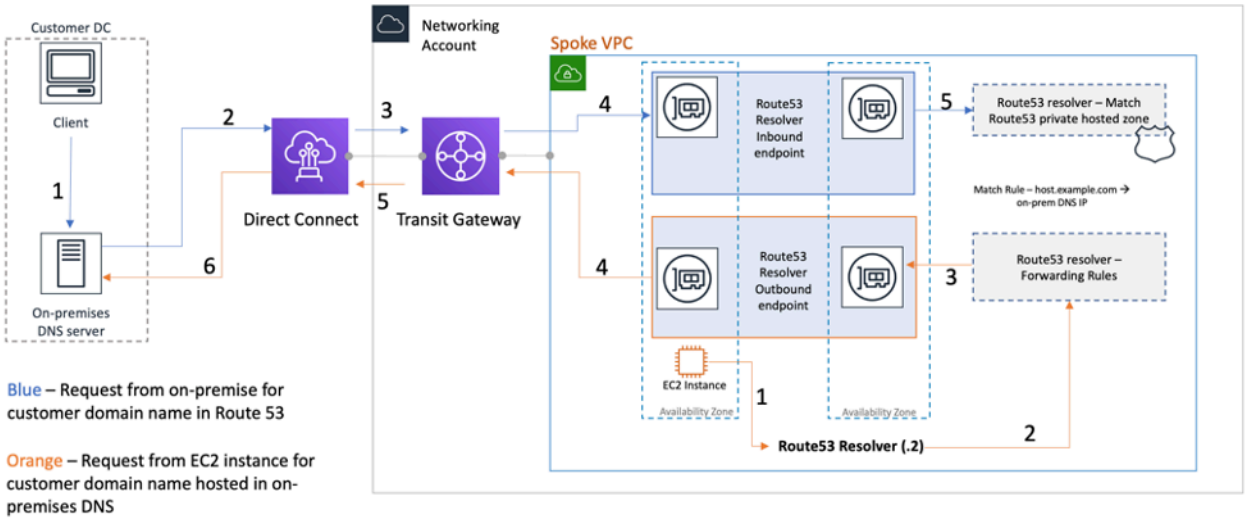
當您在 VPC 中啟動執行個體時，除了預設 VPC 之外， 會根據您為 VPC 指定的 DNS 屬性 ，以及執行個體是否具有公有 IPv4 地址，為執行個體 AWS 提供私有 DNS 主機名稱 （以及可能的公有 DNS 主機名稱）。當enableDnsSupport屬性設定為 時true，您可以從 Route 53 Resolver 取得 VPC 內的 DNS 解析 (+2 IP 偏移至 VPC CIDR)。根據預設，Route 53 Resolver 會回應 VPC 網域名稱的 DNS 查詢，例如 EC2 執行個體或 Elastic Load Balancing 負載平衡器的網域名稱。使用 VPC 對等互連時，一個 VPC 中的主機可以將公有 DNS 主機名稱解析為對等 VPCs 中執行個體的私有 IP 地址，前提是已啟用此選項。同樣適用於透過 連線VPCs AWS Transit Gateway。如需詳細資訊，請參閱啟用 VPC 對等連線的 DNS 解析支援。

如果您想要將執行個體映射至自訂網域名稱，您可以使用 Amazon Route 53 建立自訂 DNS-to-IP-mapping記錄。Amazon Route 53 託管區域是容器，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。公有託管區域包含可透過公有網際網路解析的 DNS 資訊，而私有託管區域是僅向已連接至特定私有託管區域的 VPCs 提供資訊的特定實作。在擁有多個 VPCs或帳戶的登陸區域中，您可以將單一私有託管區域與跨 AWS 帳戶和跨區域的多個 VPCs 建立關聯 （只能使用 SDK/CLI/API 進行）。VPCs 中的終端主機會使用其各自的 Route 53 Resolver IP (+2 偏移 VPC CIDR) 做為 DNS 查詢的名稱伺服器。VPC 中的 Route 53 Resolver 僅接受來自 VPC 內資源的 DNS 查詢。

混合 DNS

DNS 是任何基礎設施的關鍵元件，混合式或其他方式，因為它提供應用程式依賴的hostname-to-IP-address解析。實作混合環境的客戶通常已經有 DNS 解析系統，而且他們希望 DNS 解決方案與其目前的系統一起運作。原生 Route 53 解析程式 （基本 VPC CIDR 的 +2 位移） 無法使用 VPN 或 從內部部署網路連接 Direct Connect。因此，當您將 AWS 區域中 VPCs的 DNS 與網路的 DNS 整合時，您需要 Route 53 Resolver 傳入端點 （適用於轉送至 VPCs的 DNS 查詢） 和 Route 53 Resolver 傳出端點（適用於從 VPCs至網路的查詢）。

如下圖所示，您可以設定傳出解析程式端點，將其從 VPCs 中的 Amazon EC2 執行個體接收的查詢轉送到您網路上的 DNS 伺服器。若要將選取的查詢從 VPC 轉送至內部部署網路，請建立 Route 53 Resolver 規則，指定您要轉送之 DNS 查詢的網域名稱 （例如 example.com)，以及您要轉送查詢之網路上 DNS 解析程式的 IP 地址。對於從內部部署網路到 Route 53 託管區域的傳入查詢，您網路上的 DNS 伺服器可以將查詢轉送到指定 VPC 中的傳入解析程式端點。

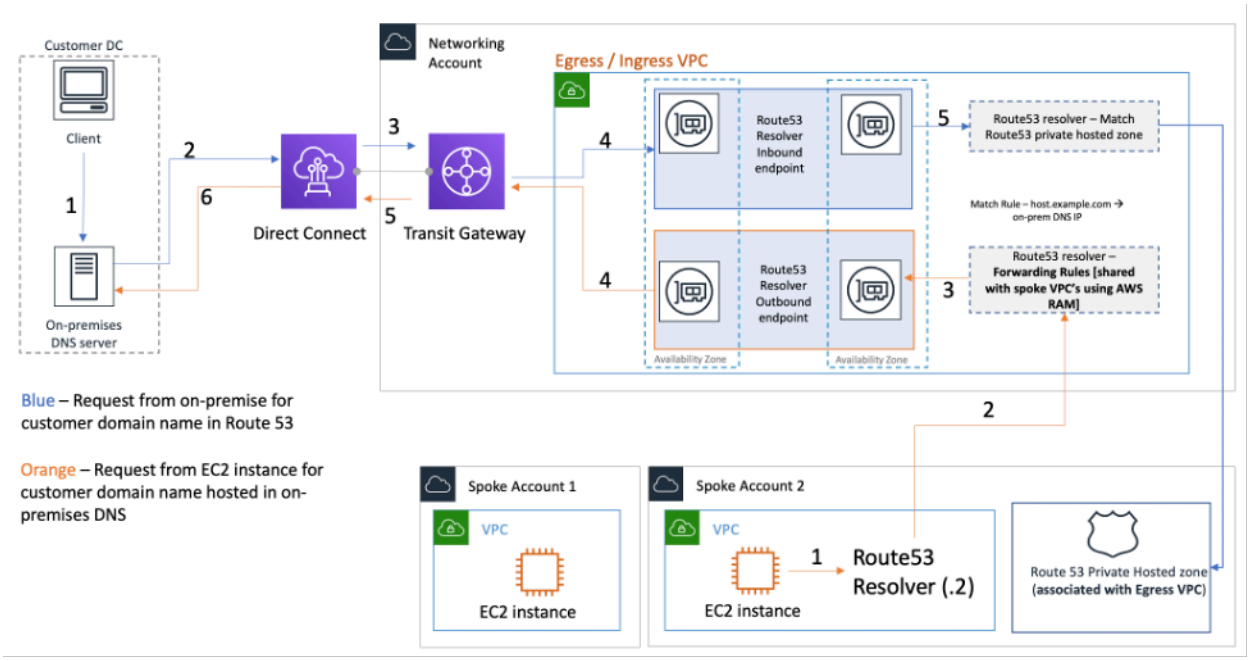


使用 Route 53 Resolver 的混合 DNS 解析

這可讓您的內部部署 DNS 解析程式輕鬆解析 AWS 資源的網域名稱，例如 Amazon EC2 執行個體或與 VPC 相關聯的 Route 53 私有託管區域中的記錄。此外，Route 53 Resolver 端點每秒最多可以處理每個 ENI 大約 10，000 個查詢，因此可以輕鬆擴展到更大的 DNS 查詢磁碟區。如需詳細資訊，請參閱 Amazon Route 53 文件中的解析程式最佳實務。

不建議您在登陸區域的每個 VPC 中建立 Route 53 Resolver 端點。將它們集中在中央輸出 VPC 中（在網路服務帳戶中）。此方法可提高可管理性，同時降低成本（針對您建立的每個傳入/傳出解析程式端點，需支付每小時費用）。您與其他登陸區域共用集中式傳入和傳出端點。

- 傳出解析 — 使用 Network Services 帳戶寫入解析程式規則（根據 DNS 查詢將轉送到內部部署 DNS 伺服器）。使用 Resource Access Manager (RAM)，與多個帳戶共用這些 Route 53 Resolver 規則（並與帳戶中VPCs 建立關聯）。輪換 VPCs中的 EC2 執行個體可以將 DNS 查詢傳送至 Route 53 Resolver，Route 53 Resolver Service 會透過輸出 VPC 中的傳出 Route 53 Resolver 端點，將這些查詢轉送至內部部署 DNS 伺服器。 您不需要將語音 VPCs對等至輸出 VPC，或透過 Transit Gateway 連接它們。請勿使用傳出解析程式端點的 IP 做為語音 VPCs中的主要 DNS。呼叫 VPCs應該在其 VPC 中使用 Route 53 Resolver（以偏移 VPC CIDR)。



在輸入/輸出 VPC 中集中 Route 53 Resolver 端點

- 傳入 DNS 解析 – 在集中式 VPC 中建立 Route 53 Resolver 傳入端點，並將登陸區域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 VPCs 與私有託管區域建立關聯。與 VPC 相關聯的多個私有託管區域 (PHZ) 無法重疊。如上圖所示，PHZ 與集中式 VPC 的這種關聯將使內部部署伺服器能夠使用集中式 VPC 中的傳入端點解析任何私有託管區域（與中央 VPC 關聯）中任何項目的 DNS。 如需混合 DNS 設定的詳細資訊，請參閱使用 Amazon Route 53 和 AWS Transit Gateway 的混合雲端的集中式 DNS 管理以及 Amazon VPC 的混合雲端 DNS 選項。

Route 53 DNS 防火牆

Amazon Route 53 Resolver DNS 防火牆可協助篩選和調節 VPCs傳出 DNS 流量。DNS 防火牆的主要用途是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發出傳出 DNS 請求，以協助防止資料洩漏。它也讓客戶能夠為他們不希望 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 防火牆具有下列功能：

客戶可以建立規則來定義 DNS 查詢的回答方式。可以為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提醒，以監控規則活動。當客戶想要在將規則移至生產環境之前測試規則時，這可以派上用場。

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 端點可讓您將 VPC 私下連線至支援的 AWS 服務，而不需要網際網路閘道或 NAT 裝置、VPN 連線或 Direct Connect 連線。因此，VPC 不會公開至公有網際網路。VPC 中的執行個體不需要公有 IP 地址，即可使用此介面端點與 AWS 服務端點通訊。您的 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。這些端點是水平擴展、冗餘且高度可用的 VPC 元件。目前可佈建兩種類型的端點：介面端點 （ 由 提供支援AWS PrivateLink) 和閘道端點。閘道端點可用來私下存取 Amazon S3 和 Amazon 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。

介面 VPC 端點

界面端點包含一或多個彈性網路介面，其具有私有 IP 地址，可做為目的地為受 AWS 支援服務之流量的進入點。當您佈建介面端點時，端點與資料處理費用一起執行的每小時都會產生成本。根據預設，您會在您要存取 AWS 服務的每個 VPC 中建立介面端點。這在客戶想要跨多個 VPCs。若要避免這種情況，您可以在集中式 VPC 中託管介面端點。所有發言 VPCs 將透過 Transit Gateway 使用這些集中式端點。

當您建立服務 VPC 端點時 AWS ，您可以啟用私有 DNS。啟用時，設定會建立 AWS 受管 Route 53 私有託管區域 (PHZ)，讓公有 AWS 服務端點能夠解析為介面端點的私有 IP。受管 PHZ 只能在具有介面端點的 VPC 內運作。在我們的設定中，當我們希望發言 VPCs 能夠解析集中式 VPC 中託管的 VPC 端點 DNS 時，受管 PHZ 將無法運作。若要克服此問題，請停用在建立介面端點時自動建立私有 DNS 的選項。接下來，手動建立符合服務端點名稱的 Route 53 私有託管區域，並將具有指向介面端點之完整 AWS 服務 端點名稱的別名記錄新增。 https://docs.aws.amazon.com/general/latest/gr/aws-service-information.html

1. 登入 AWS 管理主控台 並導覽至 Route 53。
2. 選取私有託管區域，然後導覽至建立記錄。
3. 填入記錄名稱欄位，選取記錄類型為 A，然後啟用別名。

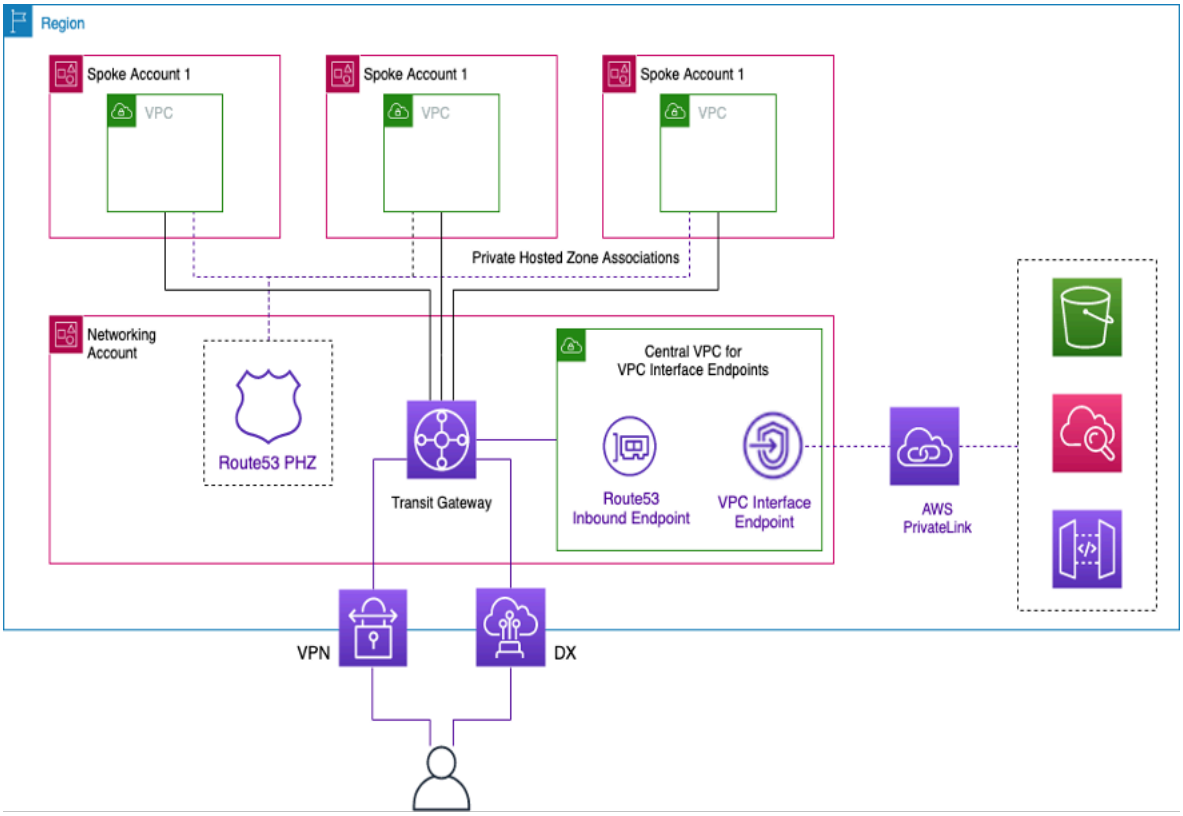
   請注意，某些 服務，例如 Docker 和 OCI 用戶端端點 (`dkr.ecr`)，需要針對記錄名稱使用萬用字元別名 (*)。
4. 在路由流量到區段下，選取流量應傳送到的服務，然後從下拉式清單中選取區域。
5. 選取適當的路由政策，並啟用評估目標運作狀態的選項。

您可以將此私有託管區域與登陸區域中的其他 VPCs建立關聯。此組態允許發言 VPCs 將完整服務端點名稱解析為集中式 VPC 中的界面端點。

> **Note**
>
> 若要存取共用私有託管區域，發言 VPCs 中的主機應使用其 VPC 的 Route 53 Resolver IP。界面端點也可以透過 VPN 和 Direct Connect 從內部部署網路存取。使用條件式轉送規則，將完整服務端點名稱的所有 DNS 流量傳送至 Route 53 Resolver 傳入端點，這會根據私有託管區域解析 DNS 請求。

在下圖中，Transit Gateway 會啟用從輪輻 VPCs到集中式介面端點的流量流程。在 Network Services 帳戶中建立 VPC 端點和私有託管區域，並與發言帳戶中VPCs 共用。如需與其他 VPCs 共用端點資訊的詳細資訊，請參閱整合 AWS Transit Gateway 與 AWS PrivateLink 和 Amazon Route 53 Resolver 部落格文章。

> **Note**
>
> 分散式 VPC 端點方法，即每個 VPC 的端點可讓您在 VPC 端點上套用最低權限政策。在集中式方法中，您將套用和管理單一端點上所有發言 VPC 存取的政策。隨著 VPCs 數量的增加，使用單一政策文件維持最低權限的複雜性可能會增加。單一政策文件也會產生較大的爆量半徑。政策文件的大小也會受到限制 (20，480 個字元）。



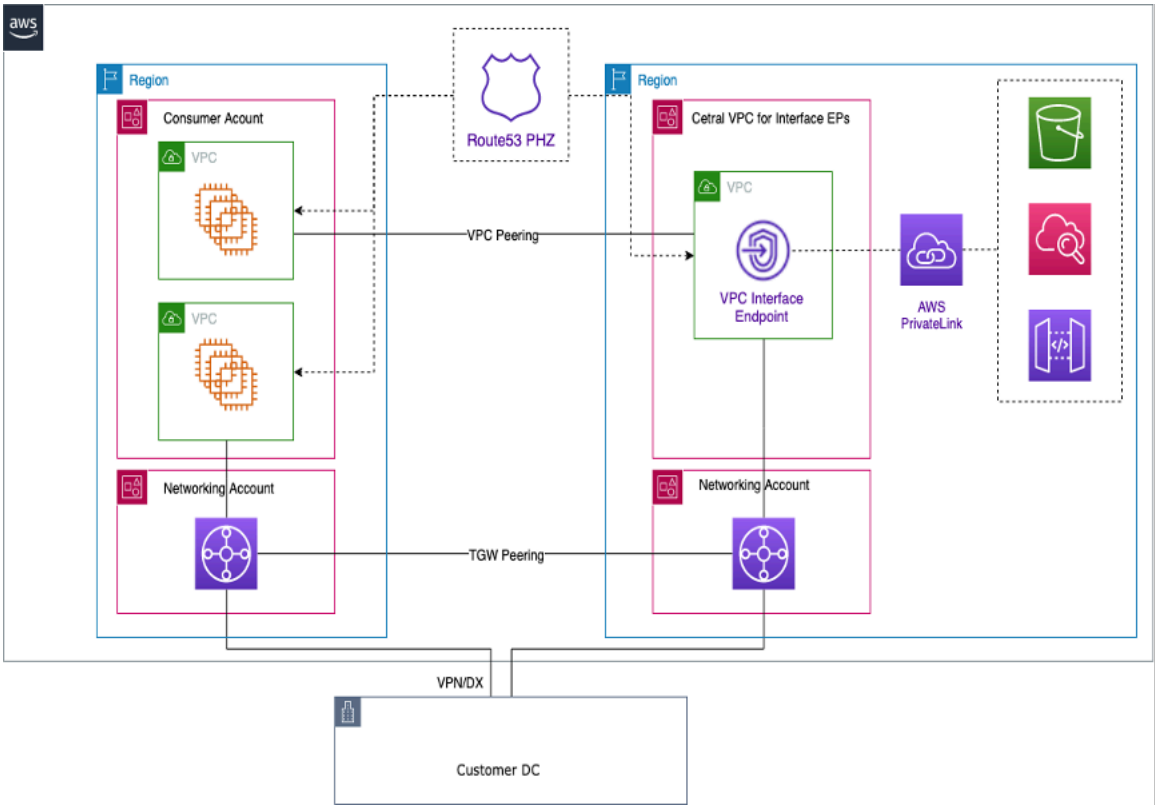
集中界面 VPC 端點

跨區域端點存取

當您想要在不同區域設定多個共用常見 VPCs 端點的 VPC 時，請使用 PHZ，如先前所述。每個區域中 VPCs 都會與 PHZ 和端點的別名建立關聯。為了在多區域架構中路由 VPCs之間的流量，每個區域中的 Transit Gateway 都必須對等。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。

來自不同區域的 VPCs 可以使用 Transit Gateways 或 VPC Peering 彼此路由。使用下列文件對 Transit Gateways 進行對等互連：Transit Gateway 對等互連附件。

在此範例中，VPC `us-west-1`區域中的 Amazon EC2 執行個體將使用 PHZ 取得區域中端點的私有 IP 地址，`us-west-2`並透過 Transit Gateway 對等互連或 VPC 對等互連將流量路由至`us-west-2`區域 VPC。使用此架構，流量會保留在 AWS 網路中，安全地允許 中的 EC2 執行個體`us-west-1`存取 中的 VPC 服務，`us-west-2`而無需透過網際網路。



多區域 VPC 端點

> **Note**
>
> 跨區域存取端點時，會收取區域間資料傳輸費用。

請參閱上圖，在 us-west-2 區域的 VPC 中建立端點服務。此端點服務可讓您存取該區域中的 AWS 服務。為了讓另一個區域中的執行個體（例如 us-east-1) 存取us-west-2該區域中的端點，您需要在 PHZ 中建立地址記錄，並使用別名來存取所需的 VPC 端點。

首先，請確定每個區域中VPCs 與您建立的 PHZ 相關聯。

在多個可用區域中部署端點時，從 DNS 傳回端點的 IP 地址將來自配置的可用區域中的任何子網路。

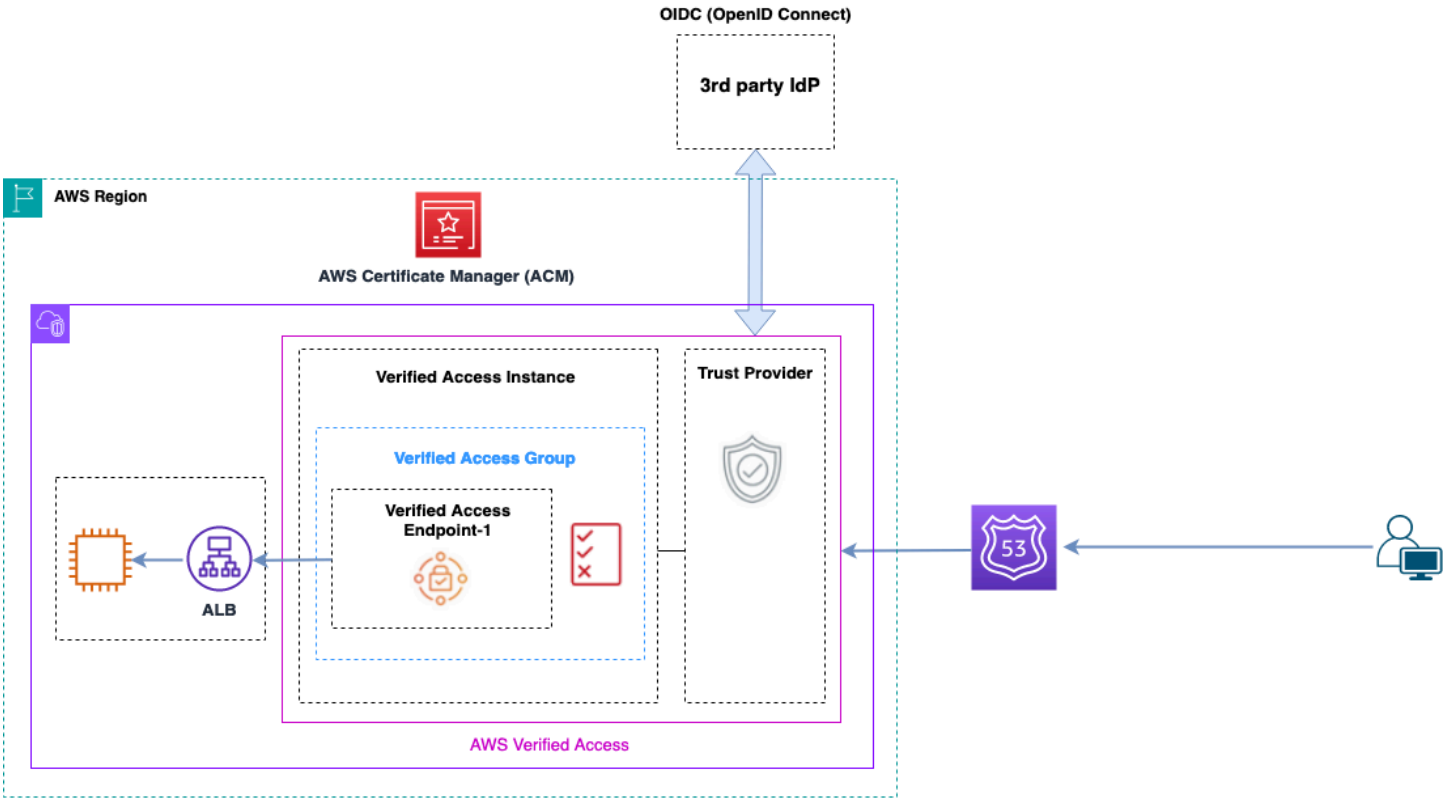
叫用端點時，請使用 PHZ 中的完整網域名稱 (FQDN)。

AWS Verified Access

AWS Verified Access 可在沒有 VPN 的情況下，安全地存取私有網路中的應用程式。它可即時評估請求，例如身分、裝置和位置。此服務會根據應用程式的政策授予存取權，並透過提高組織的安全性來連

接使用者。已驗證存取透過做為身分感知反向代理來提供對私有應用程式的存取。使用者身分和裝置運作狀態，如果適用的話，會在將流量路由至應用程式之前執行。

下圖提供 Verified Access 的高階概觀。使用者傳送存取應用程式的請求。Verified Access 會根據群組的存取政策以及任何應用程式特定的端點政策來評估請求。如果允許存取，請求會透過端點傳送至應用程式。



驗證存取概觀

AWS Verified Access 架構中的主要元件為：

- 已驗證存取執行個體 – 執行個體會評估應用程式請求，並只在符合您的安全需求時授予存取權。
- 已驗證存取端點 – 每個端點代表應用程式。端點可以是 NLB、ALB 或網路介面。
- Verified Access 群組 – Verified Access 端點的集合。我們建議您將具有類似安全需求的應用程式的端點分組，以簡化政策管理。
- 存取政策 – 一組使用者定義的規則，可決定是否允許或拒絕對應用程式的存取。
- 信任提供者 – Verified Access 是一項服務，可協助管理使用者身分和裝置安全狀態。它與 AWS 和第三方信任提供者相容，要求每個 Verified Access 執行個體至少連接一個信任提供者。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 – 每次收到應用程式請求時，您的信任提供者傳送至 Verified Access 的安全資料，例如使用者的電子郵件地址或所屬群組，都會根據您的存取政策進行評估。

您可以在 Verified Access 部落格文章中找到更多詳細資訊。

結論

當您在 AWS 登陸區域中擴展 AWS 和部署應用程式的用量時，VPCs 和聯網元件的數量會增加。本白皮書說明如何管理不斷增長的基礎設施，以確保可擴展性、高可用性和安全性，同時降低成本。在使用 Transit Gateway、Shared VPC、 Direct Connect、VPC 端點、Gateway Load Balancer AWS Network Firewall、Amazon Route 53 和第三方軟體設備等服務時，做出正確的設計決策變得至關重要。請務必了解每種方法的關鍵考量，並從您的需求向後工作，並分析最適合您的選項或選項組合。

貢獻者

下列個人對本文件有所貢獻：

- Sohaib Tahir，Amazon Web Services 解決方案架構師
- Shirin Bhambhani，Amazon Web Services 解決方案架構師
- Amazon Web Services 解決方案架構師 Kunal Pansari
- Eric Vasquez，Amazon Web Services 解決方案架構師
- Tushar Jagdale，Amazon Web Services 解決方案架構師
- Ameer Shariff，Amazon Web Services 解決方案架構師
- Glenn Davis，Amazon Web Services 解決方案架構師
- Nick Kniveton，Amazon Web Services 解決方案架構師
- Sidhartha Chauhan，Amazon Web Services 首席解決方案架構師

文件歷史記錄

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
主要更新	整份白皮書的更新，包括 CloudWAN、Amazon VPC Lattice、ENA Express、混合連線、 Direct Connect Sitelink、Deep Packet Inspection 和 的變更 AWS Verified Access。	2024 年 4 月 17 日
次要更新	更新圖表以更一致地更新 DX 連線選項，以包含私有 IP VPN，並在整個過程中進行許多次要變更。	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、更新後的 NAT 閘道圖表、更新的安全區段以集中輸出。	2023 年 4 月 4 日
次要更新	新增章節：跨區域端點存取。	2022 年 7 月 19 日
主要更新	已更新 Transit Gateway 區段與 Transit Gateway Connect，已更新 Transit VPC 區段；已更新 MACsec Direct Connect 區段與彈性建議；已更新 AWS PrivateLink 區段。新增了 VPC 對等互連與 Transit VPC 與 Transit Gateway 比較表；新增了集中式傳入檢查區段；將 VPC-to-VPC和VPC-on-	2022 年 2 月 22 日

	premises 的集中式網路安全更新為 VPC，並使用 AWS Network Firewall 和 Gateway Load Balancer 設計模式集中輸出至網際網路；新增了私有 NAT 閘道和 Amazon Route 53 DNS 防火牆區段。	
次要更新	已更新 Transit Gateway 與 VPC 對等互連章節	2021 年 4 月 2 日
白皮書已更新	更正文字以符合圖 7 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

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，這些產品和實務可能隨時變更，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 產品或服務的提供方式是「原樣」，不提供任何明示或暗示的保證、陳述或條件。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。