AWS 白皮書

混合連線

混合連線: AWS 白皮書

Table of Contents

混合式連線

出版日期：二零二三年七月六日 () 文件修訂

許多組織需要連接其內部部署資料中心、遠端站台和雲端。混合式網路可連接這些不同的環境。本白皮書描述 AWS 建置區塊，以及在決定適合您的混合連線模型時應考慮的關鍵要求。為了幫助您確定最適合您的業務和技術需求的解決方案，我們提供決策樹來指導您完成邏輯選擇過程。

簡介

現代化的組織會使用大量的 IT 資源。在過去，在內部部署資料中心或主機代管設施中託管這些資源很常見。隨著雲端運算的採用日益增加，組織透過網路連線交付和使用雲端服務供應商的 IT 資源。Organizations 可以選擇將部分或全部現有 IT 資源遷移到雲端。在任何一種情況下，都需要一個通用網絡來連接內部部署和雲端資源。內部部署和雲端資源的共存稱為混合雲，連接它們的通用網路稱為混合式網路。即使您的組織將所有 IT 資源保留在雲端，仍可能需要與遠端站台的混合式連線。

有幾種連接模式可供選擇。雖然選擇增加了靈活性，但選擇最佳選項需要分析業務和技術需求，並消除不適合的選項。您可以將需求分組在一起，包括安全性、部署時間、效能、可靠性、通訊模型、延展性等考量。一旦他們仔細收集、分析並考慮了需求，網路和雲端架構師就可以識別適用的AWS混合式網路建置區塊和解決方案。為了識別和選擇最佳模型，建築師必須了解每個模型的優缺點。還有一些技術限制可能導致排除其他適合的模型。

為了簡化選擇過程，本白皮書指導您按照邏輯順序完成每個關鍵考慮因素。在每個考慮之下，都有用於收集要求的問題。確定每個設計決策的影響以及潛在的解決方案。白皮書提供了一些考慮因素的決策樹，作為一種幫助決策過程，消除選項並了解每個決策後果的方法。它以涵蓋混合使用案例的場景結束，應用 end-to-end連接模型選擇和設計。您可以使用這個範例來瞭解如何在實際範例中執行本白皮書中規定的程序。

本白皮書旨在幫助您選擇和設計最佳的混合連接模式。本白皮書的結構如下所示：

- 混合式連線建置區塊：用於混合式連線的AWS服務概觀。
- 連接性選擇和設計考量 — 每種連接模型的定義，每種模型如何影響設計決策，需求識別問題，解決方案和決策樹。
- 客戶使用案例-如何在實踐中應用考慮因素和決策樹的例子。

你是否 Well-Architected？

AWSWell-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

AWS混合式連線建置區塊

混合式網路連線架構有三個建置區塊：

- 混合式網路連線：連線服務與內部部署客戶閘道裝置之間AWS的連線類型。
- AWS混合式連線AWS服務：提供客戶基礎架構與AWS.
- 內部部署客戶閘道裝置：客戶現有網路中的裝置，該裝置是混合式網路連線的內部部署端點。下列各節目的討論這些裝置的不同技術需求不同。

混合式網路連線

有幾種方式可在內部部署設備和AWS. 本白皮書著重於如何將這些不同的方式結合到整體架構中，但提供了不同選項（AWS Direct Connect站對站虛擬私人網路和 Transit Gateway Connect）的簡要概述。

AWS Direct Connect

AWS Direct Connect是建立從您的場所到的專用網路連線的服務AWS。如需詳細資訊，請參閱 AWS Direct Connect。

有兩種類型的AWS Direct Connect連接：專用和託管連接。專用連線是裝置與內部部署AWS裝置之間的直接連結，而代管連線則由可為您處理連線詳細資料的AWS合作夥伴支援。如需詳細資訊，請參閱AWS Direct Connect連線。

直 Connect 連線連線使用虛擬介面 (VIF) 來隔離不同的流量流量。多個 VIF 可以使用相同的直 Connect 結，並以 VLAN (802.1q) 標籤隔開。提供AWS網路連線的 VIF 有三種類型。如需詳細資訊，請參閱AWS Direct Connect虛擬介面。這三種類型如下：

- 私有 VIF：私有 VIF 是裝置與內部資源之間的私人連線。AWS這些會直接AWS在虛擬私有閘道 (VGW) 上終止 (支援單一 VPC)，或透過直接連 Connect 閘道 (然後連線至多個 VGW) 終止。
- 公用 VIF：公用 VIF 可連線至任何公用AWS資源，例如 S3、DynamoDB 和公有 EC2 IP 範圍。雖然公有 VIF 無法直接存取網際網路，但任何 Amazon 公有資源都可以存取該資源 (包括其他客戶的公有 EC2 執行個體)，客戶在安全規劃期間應考慮這些資源。
- 傳輸 VIF：傳輸 VIF 是您的裝置與透過直 Connect 連線閘道之間的私人連線。AWS Transit Gateway速度小於 1 Gbps 的連結現在支援傳輸 VIF-如需詳細資訊，請參閱上市公告。

> **Note**
>
> 託管虛擬界面（託管 VIF）是一種私有 VIF 類型，其中 VIF 被指定給與擁有AWS Direct Connect連接的AWS 帳戶AWS 帳戶不同（可以包括合作夥伴）。AWS Direct Connect AWS 不再允許新的合作夥伴提供此模型。如需詳細資訊，請參閱建立託管虛擬介面。

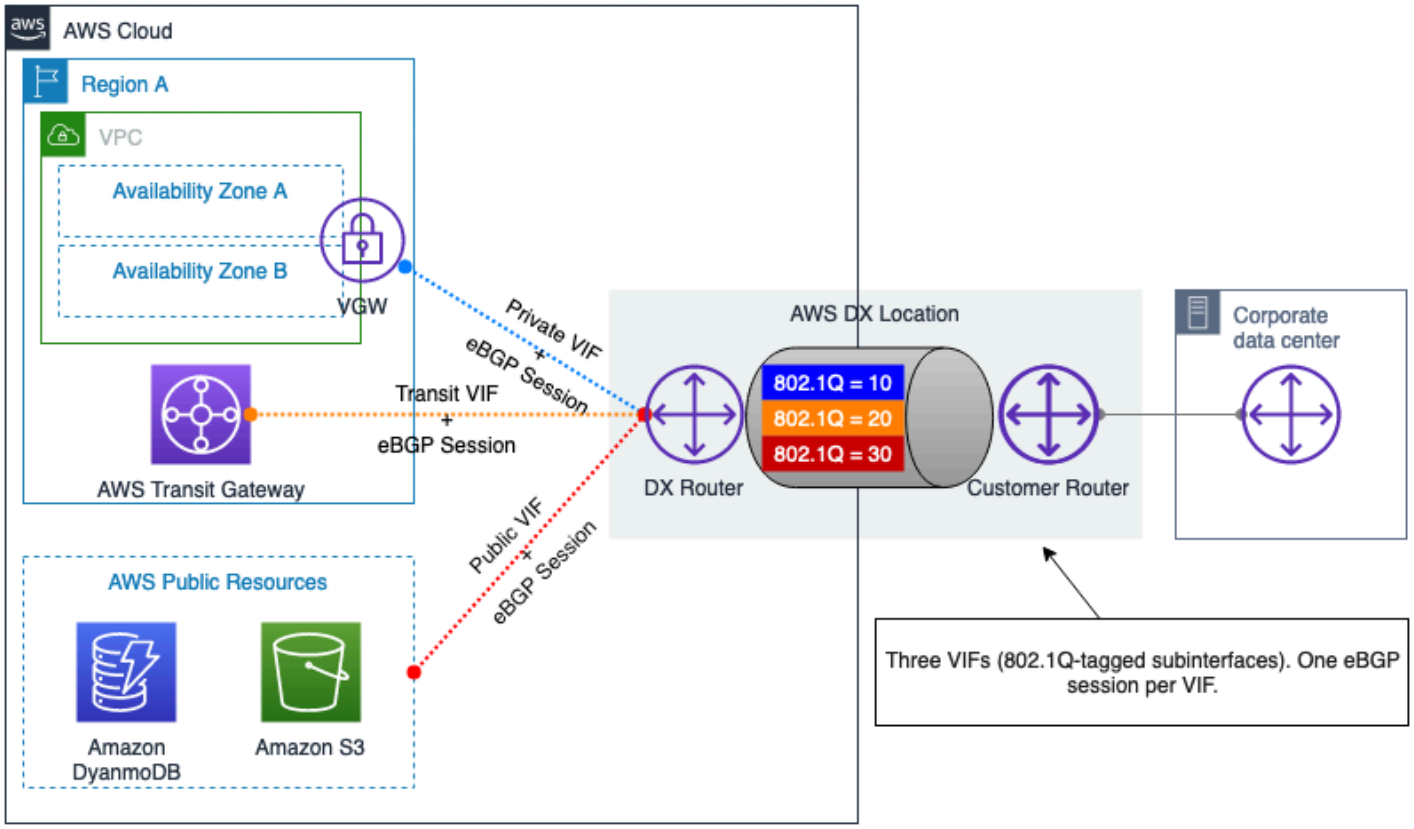

圖 1 — AWS Direct Connect 私人和公共 VIF

網站對站台虛擬私人網路 (VPN)

site-to-site VPN 可讓兩個網路安全通訊，而且可透過不受信任的傳輸 (例如網際網路) 使用。客戶可以透過兩個選項，在現場部署網站和 Amazon 虛擬私人雲端 (Amazon VPC) 之間建立 VPN 連線：

- AWS託管 Site-to-Site VPN（AWSS2S VPN）：這是一種使用 IPSec 的全受管和高可用性 VPN 服務。AWS Site-to-Site VPN如需詳細資訊，請參閱「什麼」。您可以選擇為站台對站台 VPN 連接啟用加速。如需詳細資訊，請參閱加速 Site-to-Site VPN 連線。S2S VPN 還可以使用直接 Connect 傳輸 VIF，以避免流量遍歷互聯網，從而降低成本並允許使用私有 IP 地址。如需詳細資訊，請參閱使用 AWS Direct Connect.

- 軟體 Site-to-Site VPN (客戶管理 VPN)：使用此 VPN 連線選項，您必須負責佈建和管理整個 VPN 解決方案，通常是在 EC2 執行個體上執行 VPN 軟體。如需詳細資訊，請參閱軟體 Site-to-Site VPN。

這兩種選項都需要客戶閘道裝置的支援，才能終止 VPN 通道的內部部署結束。這個裝置可以是實體裝置或軟體設備。如需有關所測試之網路裝置的詳細資訊AWS，請參閱已測試的客戶閘道裝置清單。

Transit Gateway Connect（TGW Connect）

Transit Gateway 道 Connect 會使用內部部署閘道裝置AWS Transit Gateway與內部部署閘道裝置之間的 BGP 用於 TGW Connect 之上以啟用動態路由。請注意，TGW Connect 未加密。如需詳細資訊，請參閱 Transit Gateway Connect。

AWS混合式連線服務

AWS混合式連線服務提供可高度擴充、高可用性的網路元件。它們在建置混合式網路解決方案中扮演著重要角色。撰寫本白皮書時，有三個主要服務端點：

- AWS虛擬私有閘道 (VGW) 是一種區域性的高度備援服務，可在 VPC 層級提供 IP 路由和轉送，做為 VPC 與客戶閘道裝置通訊的閘道。VGW 可以終止 AWS S2S VPN 連線和AWS Direct Connect私有 VIF。
- AWS Transit Gateway(TGW) 是一種區域性、高可用性和可擴充性的服務，可讓您使用單一集中式閘道，透過 Site-to-Site VPN 和/或直接連線，透過網站對站台 VPN 和/或直接連線來 Connect 多個 VPC，以及您的內部部署網路。從概念上講，一個AWS Transit Gateway充當高可用性和冗餘的虛擬雲路由器。 AWS Transit Gateway通過多個直接 Connect Connect，VPN 通道或 TGW 連接對等支持同等成本的多路徑（ECMP）路由。Transit Gateway 可以在相同區域和跨區域中彼此對等，從而允許其連接的資源透過對等連結進行通訊。如需詳細資訊，請參閱AWS Transit Gateway案例。
- AWS 雲端WAN 提供中央儀表板，可讓您在分公司、資料中心和 Amazon VPC 之間建立連線，只要按幾下滑鼠即可建立全球網路。您可以使用網路原則，在一個位置自動化網路管理和安全性工作。如需詳細資訊，請參閱 AWS 雲端WAN 文件。
- 直接 Connect 閘道 (DXGW) 是一項全球可用的服務，可將路由資訊分配到其連線中，其行為與傳統網路中的 BGP 路由反射器類似。資料不會通過 DXGW，它只會處理路由資訊。您可以在任意位置中建立 DXGW，AWS 區域並從所有其他方式存取 DXGW。AWS 區域您可以將直接 Connect VIF 連接到 DXGW，然後將 DXGW 與 VGW 相關聯 (使用私有 VIF) 或 (使用傳輸 VIF)。AWS Transit Gateway如需詳細資訊，請參閱直 Connect 閘道。您不需要為備援建立多個 DXGW，因為它是全球可用性服務。但是，您可以選擇使用多個 DxGW 來分隔路由網域，例如您想要保持完全隔離的生產環境和測試網路。

混合式連線類型和設計考量

白皮書的本節涵蓋了在選擇混合式網路以連接內部部署環境時，會影響您選擇的考量因素。AWS它遵循邏輯思維過程，以支持您選擇最佳的混合連接解決方案。影響設計的考量分為影響連線類型的考量，以及影響連線設計的考量。連線類型考量將支援您決定使用以網際網路為基礎的 VPN 或直 Connect 線。連線設計考量可協助您決定如何設定連線。

涵蓋影響連線類型的下列考量事項：部署時間、安全性、SLA、效能和成本。檢閱這些考量事項以及它們如何影響您的設計選擇之後，您將能夠決定是否建議使用以網際網路為基礎的連線或直 Connect 連線來滿足您的需求。

涵蓋影響連線設計的下列考量事項：可擴充性、通訊模型、可靠性和協力廠商 SD-WAN 整合。在審閱了這些考量以及它們如何影響您的設計選擇之後，您將能夠決定建議的最佳邏輯設計以滿足您的需求。

以下結構用於討論和分析每個選擇和設計考慮因素：

- 定義-什麼是考慮的簡要定義。
- 關鍵問題-提供一組問題，可讓您收集與考量相關的需求。
- 要考慮的能力-解決與考慮相關要求的解決方案。
- 決策樹-基於某些考量或一組考量，提供決策樹來幫助您選擇最佳的混合式網路解決方案。

影響混合式網路設計的考量會依序涵蓋，其中一個考量的輸出是輸入的一部分，以供後續考量。如 [圖 2] 所示，第一個步驟是決定連接類型，然後依照設計選取的考量細化它。

[圖 2] 示範兩個考量項目類別、個別考量，以及後續子章節中涵蓋考量的邏輯順序。這些都是做出混合式網路設計決策時的重要考量因素。如果目標設計不需要所有這些考量，您可以專注於適用於您需求的考量。

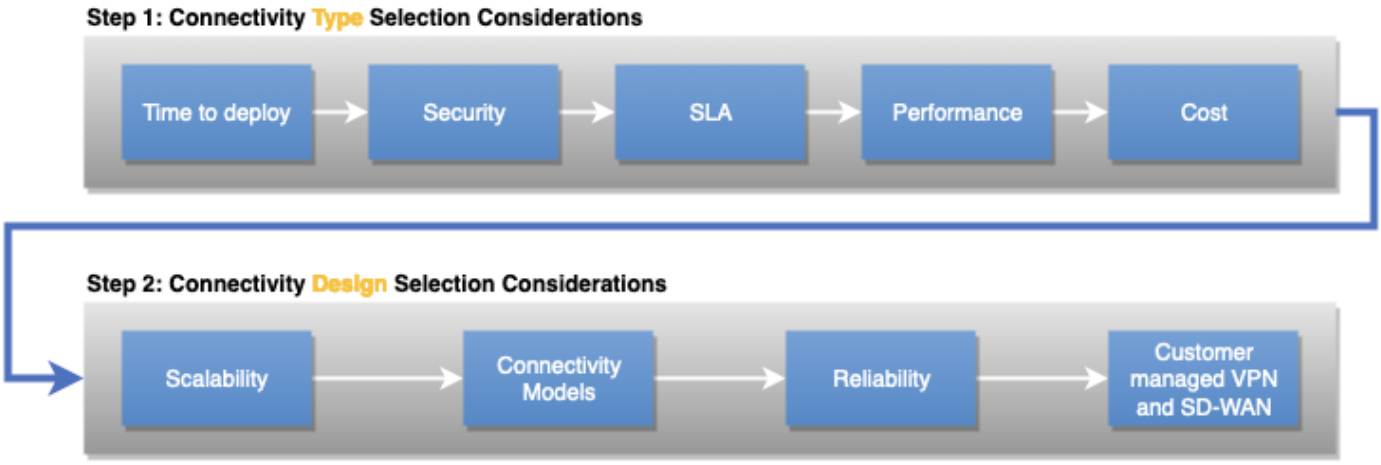

圖 2-考慮類別，個別考慮因素以及它們之間的邏輯順序

連接類型選擇

本節涵蓋了影響您為工作負載選取的連線類型的考量。這包括部署時間、安全性、SLA、效能和成本。

考量事項

- 部署時間
- 安全性
- 服務等級協議 (SLA)
- 效能
- 費用

部署時間

定義

部署時間可能是為工作負載選取合適連線類型的重要因素。視連線類型和內部部署位置而定，可在數小時內建立連線能力，但如果必須安裝其他電路，可能需要數週或數月的時間。這會影響您決定使用以網際網路為基礎的連線、私人專用連線，或由AWS Direct Connect合作夥伴作為管理服務提供的私人託管連線。

關鍵問題

- 部署所需的時間表為何？小時、天數、週數或幾個月？

- 連接需要多長時間-這是一個短暫的項目還是永久性的基礎設施？

需要考慮的能力

如果您需要在數小時或數天內AWS連線，您很可能需要使用現有的網路連線。這通常意味著通AWS過公共互聯網建立 VPN 連接。如果現有的 AWS DX 合作夥伴為您提供私人AWS連線，則可在數小時內佈建新的託管連線。

當您有數天到數週的時間時，您可以與AWS Direct Connect合作夥伴合作建立私有連線AWS。 AWS Direct Connect合作夥伴可協助您建立位AWS Direct Connect置與資料中心、辦公室或主機代管環境之間的網路連線。某些AWS Direct Connect合作夥伴已獲准提供直 Connect 線託管連線。託管連線的佈建速度通常比專用連線更快。 AWS Direct Connect合作夥伴將使用連接至AWS骨幹的現有基礎結構佈建每個託管連線。

當您有數週到幾個月的時間時，您可以調查與建立專用的私人連線AWS。服務提供商和AWS Direct Connect合作夥伴促進AWS Direct Connect專用連接。服務供應商通常會在客戶的場所安裝網路設備，以促進直 Connect 線專用連線。視服務供應商、網站的位置以及其他實體因素而定，直 Connect 連線專用連線的安裝可能需要數週到幾個月的時間。

如果您已將網路設備安裝在該位置所在的相同主機代管設施中，則可以透過主機代管站台的交叉連線快速建立AWS Direct Connect專用連線。AWS Direct Connect請求連接後，AWS請向您提供授權書和連接設施分配（LOA-CFA）以供您下載，或通過電子郵件向您發送更多信息請求。LOA-CFA 是連接到的授權AWS，您的網絡提供商需要為您訂購交叉連接。

表 1 — 成本效益比較

	網際網路連線	DX 專用連接（DX 位置內的現有設備）	DX 專用連接（淨新）	DX 託管連線 (DX 合作夥伴的現有連接埠)	DX 託管連線 (淨新)
佈建時間	小時到天	天	幾個星期至幾個月	小時到天	幾天到幾週到幾個月

> **Note**
>
> 提供的佈建時間指南基於真實世界的觀察，僅作為說明。考慮到您的站點位置、與直接連線位置的距離以及預先存在的基礎結構時，都會影響佈建時間。您的AWS Direct Connect合作夥伴會針對精確的佈建時間提供建議。

安全性

定義

安全性需求會影響您的混合式連線類型。這些考量因素包括：

- 傳輸類型 — 互聯網或私人網絡連接
- 加密要求

關鍵問題

- 您的安全要求和政策是否允許使用互聯網上的加密連接來連接AWS，還是要求使用私人網絡連接？
- 利用私人網路連線時，網路層是否必須在傳輸過程中提供加密？

技術方案

您的安全性需求和原則可能允許使用網際網路，或需要在AWS與貴公司網路之間使用私人網路連線。它們還會影響網絡是否必須在傳輸過程中提供加密，或者如果在應用程序層執行加密是可接受的決定。

如果您可以利用網際網路，則AWS Site-to-Site VPN可用於在您的網路和 Amazon VPC 之間建立加密通道，或AWS Transit Gateway透過網際網路。如果您利用以網際網路為基礎的連線，您也可以選擇透AWS過網際網路將 SD-WAN 解決方案延伸至網際網路。本白皮書稍後的客戶管理 VPN 和 SD-WAN 一節涵蓋了 SD-WAN 的特定考量。

如果您需要AWS與公司網路之間的私人網路連線，AWS建議您使用AWS Direct Connect專用連線或託管連線。如果需要透過私人網路連線進行加密，您應該透過直 Connect 線 (透過公用 VIF 或傳輸 VIF) 建立 VPN，或考慮在 10Gbps 或 100Gbps 專用連線上使用 MacSec。

表 2-示例汽車公司連接類型要求

	站台對站台 VPN	Direct Connect
傳輸	網際網路	私人網路連線
傳輸中加密	是	需要透過 DX 進行 S2S VPN、透過傳輸 VIF 的 S2S VPN，或在 10Gbps 或 100 Gbps 的專用連線上使用 Macsec

服務等級協議 (SLA)

定義

企業組織通常需要服務提供者來滿足組織消耗的每個服務的 SLA。該組織反過來在頂部建立自己的服務，並可能為自己的消費者提供 SLA。SLA 很重要，因為它描述了服務的提供和操作方式，並且通常包含特定的可衡量特性，例如可用性。如果服務違反定義的 SLA，服務提供者通常會提供協議所指定的財務補償。SLA 定義度量的類型、需求和測量週期。例如，請參閱 AWS Direct ConnectSLA 下的正常運行時間目標定義。

關鍵問題

- 是否需要含服務點數的混合式連線連線 SLA？
- 整個混合式網路是否需要遵守正常執行時間目標？

需要考慮的能力

連線類型：網際網路連線可能無法預測。雖然使AWS用不同的 ISP 集合來處理多個連結，但網際網路的管理只不在AWS或單一供應商的管理網域之外。一旦流量離開其網路邊界，雲端供應商可以對路由工程和流量造成的影響數量有限。也就是說，有一個 AWS Site-to-Site VPNSLA 可為AWS Site-to-Site VPN端點提供可用性目標。

AWSDirect Connect 提供正式的 SLA，其中包含服務積分，計算方式為您針對未符合 SLA 的每月帳單週期無法使用的適用連線支付的連接AWS Direct Connect埠時數總費用的百分比計算。如果需要 SLA，建議使用這種傳輸方式。 AWS Direct Connect列出每個執行時間目標的特定最低組態需求，例如AWS Direct Connect位置數目、連線數目及其他組態詳細資料。未能滿足需求意味著如果服務中斷定義的 SLA，則無法提供服務點數。

重要的是，即使選擇提供混合式連線的服務設定為符合 SLA 需求，網路的其餘部分也可能無法提供相同等級的 SLA。AWS責任在AWS Direct Connect連接埠的AWS Direct Connect位置結束。一AWS且將流量轉移到您組織的網路，就不再是負責AWS。如果您在內部部署網路之間AWS使用服務提供者，則連線會受到您與服務供應商之間的 SLA (如果適用) 的約束。請記住，在設計混合式連接時，整個混合網絡與其中最薄弱的部分一樣好。

AWS Direct Connect合作夥伴提供AWS Direct Connect連接。合作夥伴可以根據其產品提供的服務點數提供 SLA，直到分界點為止。AWS應該直接與 APN 合作夥伴評估該選項並進一步研究。 AWS會發佈經過驗證的外送夥伴清單。

邏輯設計：除了連接類型之外，您還必須將其他構建塊視為整體設計的一部分。作為一個例子，AWS Transit Gateway有自己的 SLA，AWSS2S VPN 也是如此。出AWS Transit Gateway於安全原因，您可能會使用擴展和 AWS S2S VPN，但是您必須以與每個 SLA 一致的方式進行設計，才有資格獲得每個個別服務的服務點數。

檢閱AWS Direct Connect彈性建議和復原工具組。

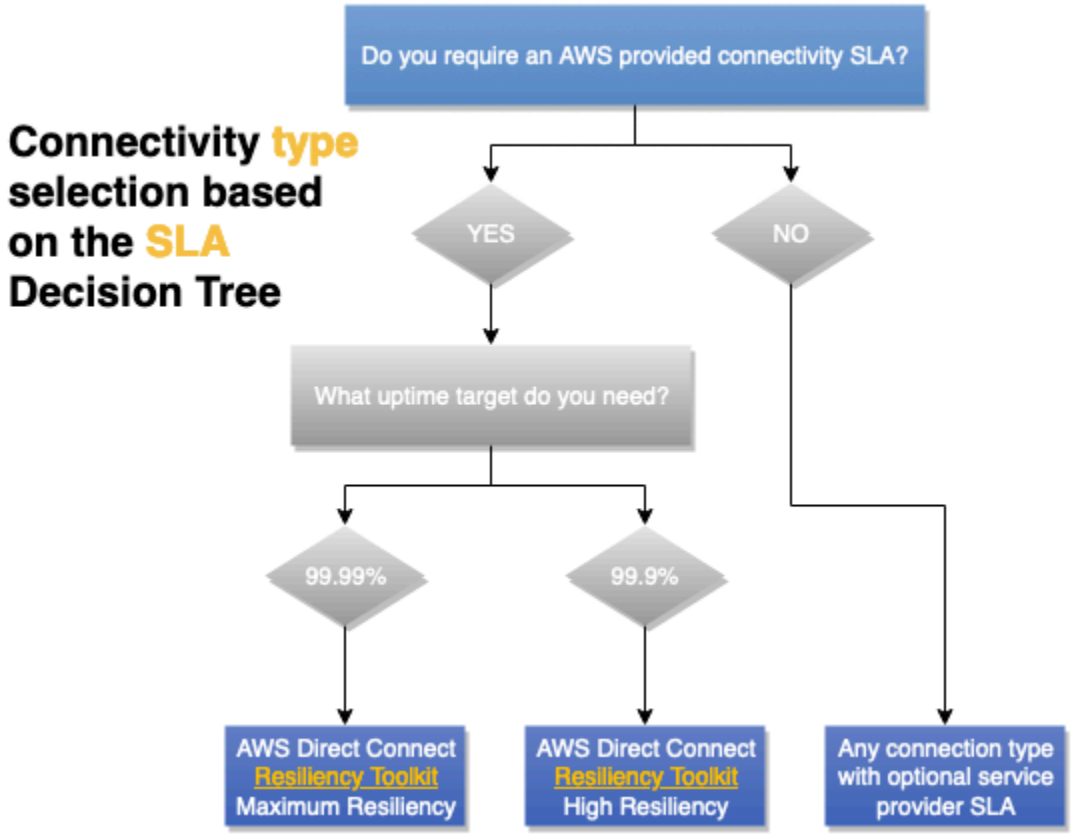

圖 3 — SLA 考量決策樹

效能

定義

影響網路效能的因素有很多，例如延遲、封包遺失、抖動和頻寬。根據應用需求，每個因素的重要性可能會有所不同。

關鍵問題

根據您的應用程式需求，您必須找出影響應用程式行為和使用者體驗的網路效能因素，並排定優先順序。

頻寬

頻寬是指連線的資料傳輸速率，通常以每秒位元數 (bps) 為單位。每秒兆比特（Mbps）和每秒千兆位（Gbps）是常見的縮放比例，並且是基數 10（每秒 100 萬位 = 1 Mbps），而不是其他地方看到的基數 2（2 ^ 10）。

評估應用程式的頻寬需求時，請記住頻寬需求可能會隨著時間而改變。初始部署到雲端、一般作業、新工作負載和容錯移轉案例都可能有不同的頻寬需求。

應用程式可以有自己的頻寬考量。某些應用程式可能需要透過高頻寬連線的確定性效能，而其他應用程式則需要確定性效能和高頻寬。如果應用程式達到每個流量流量頻寬限制，應用程式可能需要特殊的組態才能 parallel 使用多個流量流量 (有時稱為串流或通訊端)，以允許其使用更多連線的頻寬。VPN 可以限制輸送量，因為隧道開銷、更低的 MTU 限制或硬體頻寬限制。

Latency (延遲)

延遲是封包透過網路連線從來源到目的地所需的時間，通常以毫秒 (ms) 為單位測量，低延遲需求有時以微秒 (µs) 表示。延遲是光速的函數，因此延遲會隨距離而增加。

應用程式延遲需求可採用不同的形式。高度互動的應用程式 (例如虛擬桌面) 可以有一個延遲目標，從使用者執行輸入到使用者看到虛擬桌面對該輸入做出反應為止。網路電話 (VoIP) 應用程式可能具有類似的需求。需要考慮的第二種工作負載類型是具有高度交易性的工作負載，需要伺服器回應才能繼續。資料庫或其他形式的索引鍵/值存放區可能受到網路延遲增加的影響。

Jitter (抖動)

抖動測量網絡延遲的一致性，並且像延遲一樣，通常以毫秒（毫秒）為單位進行測量。

應用程式抖動需求通常可在即時串流應用程式中找到，包括視訊和語音傳遞。這些應用程式通常要求其資料流程保持一致的速率和延遲，而且緩衝區較小，以修正少量抖動。

封包遺失

封包遺失是指未傳送的網路流量百分比的測量值。由於高流量突發，容量減少，網絡設備故障和其他原因，所有網絡有時都會出現某種程度的數據包丟失。因此，應用程式必須有一定的封包遺失容許度，但是，它們可以容忍的程度可能因應用程式而有所不同。

使用 TCP 傳輸其流量的應用程式可以透過重新傳輸修正封包遺失的能力。在 IP 之上使用 UDP 或他們自己的協議的應用程序需要實現自己的處理數據包丟失的方法，並且可能對它非常敏感。IP 語音應用程式可以簡單地將靜音插入有封包遺失的通話部分，而不是嘗試重新傳輸。有些 VPN 解決方案包含自己的機制，用於從用來承載流量的網路上的封包遺失中復原。

需要考慮的能力

當需要可預測的延遲和輸送量時，AWS Direct Connect建議選擇，因為它可提供確定性的效能。頻寬可以根據輸送量需求來選擇。 AWS建議您在需要比以網際網路為基礎的連線提供更一致的網路體驗AWS Direct Connect時使用。私有 VIF 和傳輸 VIF 支援 Jumbo 框架，可減少透過網路的封包數量，並可因為減少額外負荷而改善輸送量。 AWS Direct ConnectSiteLink允許使用AWS骨幹在您的位置之間提供連接，並且可以根據需要啟用。使用的頻寬 SiteLink 應考慮您的直 Connect 頻寬選擇。

透過使用 VPN AWS Direct Connect 會增加加密。不過，它會減少 MTU 大小，進而降低輸送量。AWS受管理的網站對站台 (S2S) VPN 功能可以在文件中找到。AWS Site-to-Site VPN如果透過連線加密是主要的加密需求，則許多直接連線位置都支援 MacSec。MacSec 沒有相同的 MTU 或 Site-to-Site VPN 連線的潛在輸送量考量。 AWS Transit Gateway允許客戶水平擴展 VPN 連接數量，並相應地提高輸送量同等成本的多路徑路由 (ECMP)。 AWS的受管 Site-to-Site VPN 支持使用直接 Connect 傳輸 VIF 進行私有連接-有關詳細信息，請參閱私有 AWS Direct Connect IP VPN。

另一種選擇是透過網際網路使用AWS受管理的 Site-to-Site VPN。由於成本低，它可能是一個有吸引力的選擇，並且廣泛使用。但是，請記住，在互聯網上的性能是最好的努力。互聯網天氣事件，擁塞和延遲時間增加可能無法預測。 AWS提供了AWS加速 S2S VPN 的解決方案，可以減輕使用互聯網路徑的一些缺點。加速 S2S VPN 使用AWS全域加速器，可讓 VPN 流量儘早進入AWS網路，並儘可能靠近客戶閘道裝置。這會使用不壅塞的AWS全球網路將網路路徑最佳化，將流量路由到能夠提供最佳效能的端點。您可以使用加速 VPN 連線，避免網路路由到網路上的網路會造成網路中斷。

費用

定義

在雲端中，混合式連線的成本包括佈建資源和使用量的成本。佈建資源的成本是以時間單位來衡量，通常是每小時一次。資料傳輸和處理的使用量通常以 GB 為單位。其他成本包括連線至AWS網路存在點

的成本。如果您的網路位於相同的主機代管設施中，則可能與交叉連線的成本一樣低。如果您的網路位於不同的位置，則需要支付服務供應商或 APN Direct Connect 合作夥伴的費用。

關鍵問題

- 您預計AWS每月會從您的設施和網際網路傳送到多少資料？
- 您預計AWS每月會傳送多少資料到您的設施和網際網路？
- 這些金額多久會改變一次？
- 失敗案例中有哪些變化？

需要考慮的能力

如果您有需要執行頻寬繁重的工作負載AWS，AWS Direct Connect可以透過兩種方式降低進出網路成本。AWS首先，通過AWS直接傳輸數據，您可以降低支付給互聯網服務提供商的帶寬成本。其次，透過專用連線傳輸的所有資料都會以降低的AWS Direct Connect資料傳輸費率收費，而非網際網路資料傳輸費率，詳情請參閱 Direct Connect 定價頁面。

AWS Direct Connect允許使用AWS Direct Connect SiteLink 來互連您的網站使用AWS骨幹-有關更多信息，請參閱 SiteLink 啟動博客。利用此功能會產生一般的直 Connect 資料傳輸成本，並啟用每小時的費 SiteLink 用。您可以 SiteLink 隨選啟用和停用，對於涉及網際網路或私人網路連線的故障情況，這可能是一個不錯的選擇。

如果您使用網路服務供應商在內部部署和 Direct Connect 位置之間進行連線，則您的能力和變更頻寬承諾所需的時間取決於您與服務供應商的合約。

AWS骨幹可以從任何AWS網絡存在點將您的流量傳遞到中國以AWS 區域外的任何地方。與使用網際網路存取遠端相比，此功能具有許多技術優勢AWS 區域，但需要付出代價 — 如需詳細資訊，請參閱 EC2 資料傳輸定價頁面。如果流量路徑AWS Transit Gateway中有一個，則會增加每 GB 的資料處理成本，但是如果在兩個 Transit Gateway 之間使用區域間對等，則只需支付 Transit Gateway 資料處理的一次費用。

最佳的應用程式設計可將資料處理保持在內，AWS並將不必要的資料輸出費 資料輸入AWS是免費的。

> **Note**
>
> 作為整體連接解決方案的一部分，除了AWS連接成本之外，您還應該考慮 end-to-end 連接的成本，包括 DX 位置內的服務提供者成本，交叉連接，機架和設備（如果需要）。

如果您不確定是否應該使用互聯網或私人連接，請計算一個盈虧平衡點，其中比使用互聯網AWS Direct Connect更便宜。如果數據量意AWS Direct Connect味著成本更低，並且您需要永久連接，則AWS Direct Connect是最佳的連接選擇。

如果連接是暫時的，並且互聯網滿足其他要求，則由於互聯網的彈性，在互聯網上使用 AWS S2S VPN 可能會更便宜。請注意，您必須從內部部署網路擁有足夠的網際網路連線能力。

如果您位於具有的設施內AWS Direct Connect（該列表可在 Direct Connect 網站上找到），則可以建立交叉連接到AWS。這意味著在 1,10 或 100 Gbps 的速度使用專用連接。 AWS Direct Connect合作夥伴提供更多頻寬選項和更小的容量，這可能會最佳化您的連線成本。例如，您可以從 50 Mbps 的託管連線開始，而不是 1 Gbps 專用連線。

使用AWS Transit Gateway，您可以與許多 VPC 共用 VPN 和直 Connect 連線連線。雖然您需要支付AWS Transit Gateway每小時連線的數量以及流通的流量計費AWS Transit Gateway，但它可以簡化管理並減少所需的 VPN 連線和 VIF 數量。降低營運開銷的優點和成本節省，可輕鬆地超過資料處理的額外成本。或者，您可以考慮一種設計，其中位於大多數 VPC 的流量路徑中，但不AWS Transit Gateway是全部。這種方法可避免您需要將大量AWS Transit Gateway資料傳入的使用案例所產生的資料處理費用AWS。有關此設計的更多詳細信息，請參閱「連接模型」部分。另一種方法是通過互聯網將 AWS S2S VPN AWS Direct Connect 作為備份/故障轉移路徑結合為主要路徑。雖然技術上可行且非常符合成本效益，但此解決方案存在技術上的缺點 (請參閱本白皮書的「可靠性」一節中討論)，而且管理起來更加困難。 AWS對於高度關鍵或重要的工作負載，不建議這樣做。

最後一種方法是部署在 Amazon EC2 執行個體中的客戶管理 VPN 或 SD-WAN。與 AWS S2S VPN 相比，如果有數十到數百個站點，則規模上可能會更便宜。但是，需要考慮每個虛擬設備的管理開銷、授權成本和 EC2 資源成本。

決策矩陣

表 3 — 範例公司汽車連接設計輸入

類別	由客戶管理的 VPN 或 SD-WAN	AWSS2S 網路 VPN	AWS加速的 S2S 網路 VPN	AWS Direct Connect託管連線	AWS Direct Connect專用連接
需要網路連線	是	是	是	否	否
佈建的資源成本	EC2 執行個體和軟體授權	AWSS2S 網路 VPN	AWSS2S VPN 和AWS全球加速器	港口成本的適用容量	專用連接埠成本

類別	由客戶管理的 VPN 或 SD-WAN	AWSS2S 網路 VPN	AWS加速的 S2S 網路 VPN	AWS Direct Connect託管連線	AWS Direct Connect專用連接
資料傳輸成本	網路費率	網際網路費率或直 Connect 費率	互聯網與數據傳輸溢價	直接 Connect 速率	直接 Connect 速率
轉換閘道	選用	選用	必要	選用	選用
AWS資料處理成本	N/A	只有搭配 AWS Transit Gateway	是	只有搭配 AWS Transit Gateway	只有搭配 AWS Transit Gateway
可以過度使用 AWS Direct Connect嗎？	是	是	否	N/A	N/A

連線設計選擇

白皮書的本節涵蓋影響連線設計選擇的考量事項。連線設計包括邏輯層面，以及如何設計和最佳化您的混合連線可靠性。

將涵蓋下列考量事項：可擴展性、連線模式、可靠性，以及客戶受管VPN和 SD-WAN。

考量事項

- 可擴展性
- 連線模式
- 可靠性
- 客戶受管VPN和 SD-WAN

可擴展性

定義

可擴展性是指您的連線解決方案隨著時間的推移而成長和發展的能力。

設計解決方案時，您需要考慮目前的規模以及預期的成長。這種成長可以是有機成長，也可能與快速擴展有關，例如在合併和收購類型案例中。

注意：根據目標解決方案架構，並非所有上述元素都需要納入考量。不過，它們可以作為基礎元素，以識別最常見的混合網路解決方案的可擴展性要求。本白皮書著重於混合式連線選擇和設計。建議您也考慮與VPC網路架構相關的混合連線規模。如需詳細資訊，請參閱建置可擴展且安全的多VPC AWS 網路基礎設施白皮書。

關鍵問題

- 目前和預期的需要VPCs連線至內部部署網站的數量是多少？
- 是否VPCs部署在單一 AWS 區域 或多個區域中？
- 需要將多少個內部部署站台連線到 AWS？
- 每個需要連線至 的網站有多少個客戶閘道裝置 （通常是路由器或防火牆） AWS？
- 預計要向 Amazon 公告多少路由VPCs，以及從 AWS 側面接收的預期路由數量是多少？
- AWS 是否需要隨著時間增加頻寬至 ？

考量的能力

規模是混合連線設計的重要因素。此時，後續章節會將規模納入目標連線模型設計的一部分。

以下是將混合網路連線設計的規模複雜性降至最低的建議最佳實務：

- 應使用路由摘要來減少向 公告並從 接收的路由數量 AWS。因此，IP 定址方案需要設計為最大限度地使用路由摘要。流量工程是重要的整體考量。如需流量工程的詳細資訊，請參閱可靠性一節中的流量工程子節。
- DXGW 搭配 VGW或 使用 將BGP對等工作階段數量降至最低 AWS Transit Gateway，其中單一BGP工作階段可提供與多個 的連線VPCs。
- 當多個和 AWS 區域 內部部署站台需要連接在一起WAN時，請考慮 Cloud。

連線模式

定義

連線模式是指 （內部部署） 網路與雲端資源之間的通訊模式 AWS。您可以在單一 AWS 區域 或多個VPCs區域VPC內部署 Amazon 內的雲端資源，以及在 AWS 單一或多個 中具有公有端點的服務 AWS 區域，例如 Amazon S3 和 DynamoDB

關鍵問題

- 是否有在 區域內和跨 區域之間進行通訊VPC的需求？
- 是否需要直接從內部部署存取 AWS 公有端點？
- 是否需要使用內部部署的VPC端點存取 AWS 服務？

考量的能力

以下是一些最常見的連線模型案例。每個連線模型涵蓋需求、屬性和考量事項。

注意：如先前所強調，此白皮書著重於內部部署網路與 之間的混合連線 AWS。如需互連 設計的詳細資訊VPCs，請參閱建置可擴展且安全的多VPC AWS 網路基礎設施白皮書。

模型

- AWS 加速 VPN – Site-to-Site AWS Transit Gateway，單一 AWS 區域
- AWS DX – DXGW使用 VGW，單一區域
- AWS DX – DXGW使用 VGW、多區域和 AWS 公有對等
- AWS DX – DXGW使用 AWS Transit Gateway、多區域和 AWS 公有對等
- AWS DX – DXGW使用 AWS Transit Gateway，多區域（超過 3 個）

AWS 加速 VPN – Site-to-Site AWS Transit Gateway，單一 AWS 區域

此模型由以下項目構成：

- 單一 AWS 區域。
- AWS 與 的受管 Site-to-SiteVPN連線 AWS Transit Gateway。
- 加速VPN已啟用。

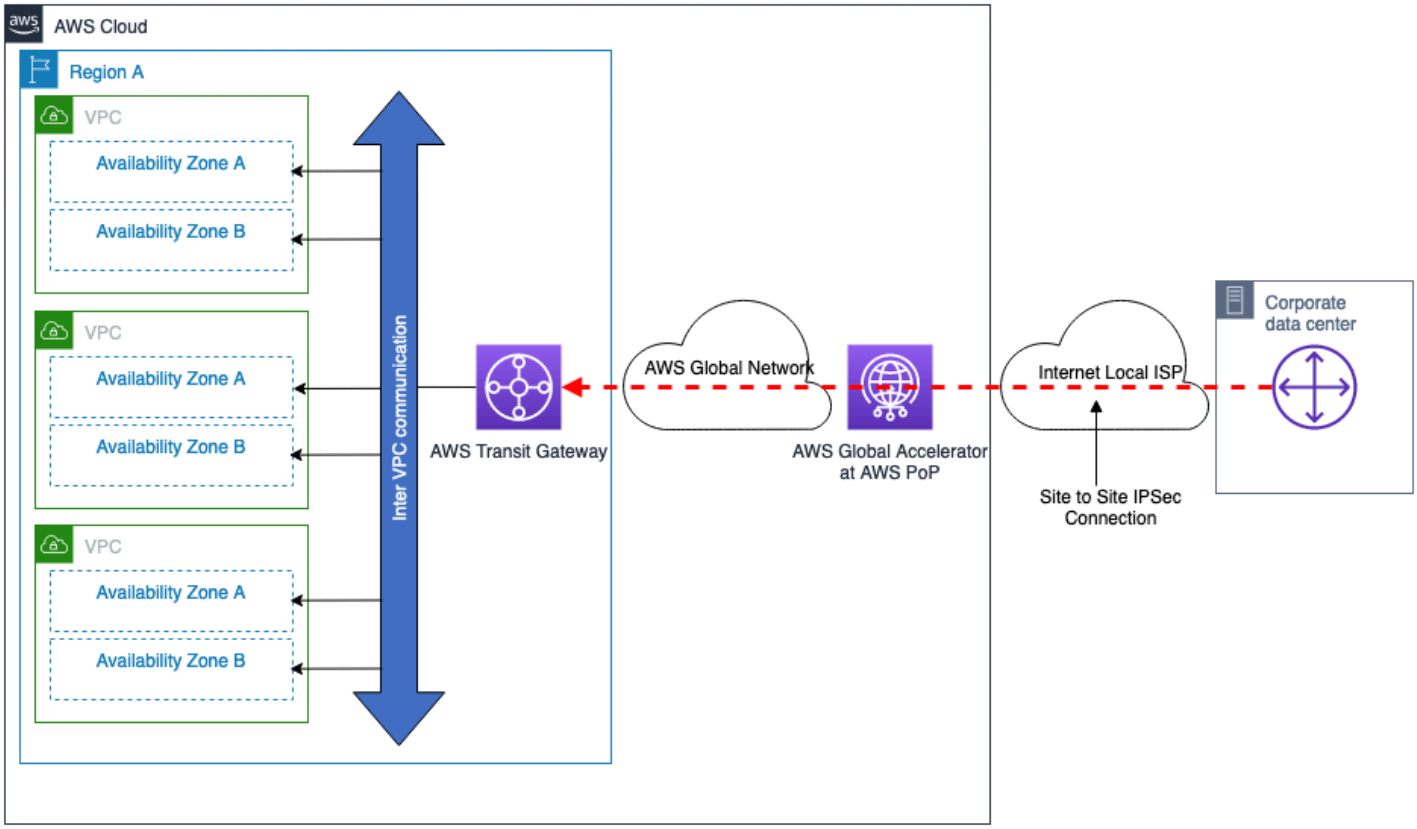

圖 4 – 受 AWS 管 VPN – AWS Transit Gateway，單一 AWS 區域

連線模型屬性：

- 透過使用加速VPN連線 ，提供透過公有網際網路建立最佳化連線的能力。 AWS Site-to-Site VPN
- 透過使用 設定多個VPN通道，提供實現更高VPN連線頻寬的能力ECMP。
- 可用於從多個遠端站台進行連線。
- 提供具有動態路由 （ BGP ） 的自動容錯移轉。
- 在 AWS Transit Gateway 連線至 的情況下VPCs，所有連接的 VPCs都可以使用相同的VPN連線。您也可以控制 之間所需的通訊模型VPCs，如需詳細資訊，請參閱 Transit Gateways 的運作方式。
- 提供靈活的設計選項，以將第三方安全和 SD-WAN 虛擬設備與 整合 AWS Transit Gateway。請參閱流量 和內部部署對VPC流量 的 VPC-to-VPC集中式網路安全。

規模考量：

- 最多 50 Gbps 的頻寬，並ECMP設定多個IPsec通道 （ 每個流量將限制為每個VPN通道的最大頻寬 ）。

- 每 VPCs可以連接數千個 AWS Transit Gateway。
- 請參閱其他規模限制的Site-to-Site VPN配額，例如路由數量。

其他考量事項：

- 內部部署資料中心與 之間資料傳輸的額外 AWS Transit Gateway 處理成本 AWS。
- 遠端 的安全群組VPC無法在 中參考 AWS Transit Gateway – 不過，這由VPC對等支援。

AWS DX – DXGW使用 VGW，單一區域

此模型由以下項目構成：

- 單一 AWS 區域。
- 與獨立 DX 位置的雙重 AWS Direct Connect 連線。
- AWS DXGW VPCs使用 直接連接至 VGW。
- AWS Transit Gateway 用於 通訊間的VPC選用用途。

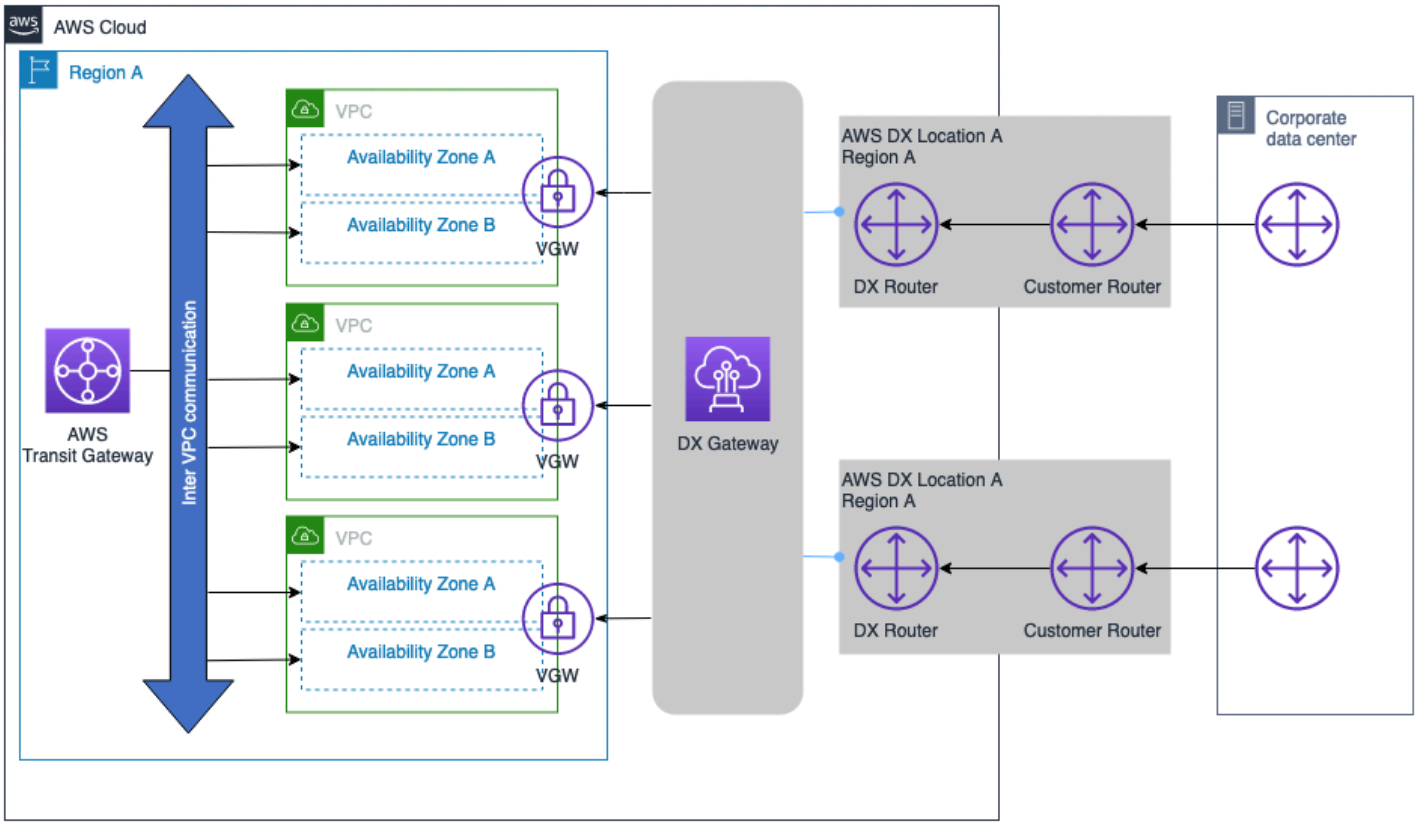

圖 5 – AWS DX – DXGW使用 VGW，單一 AWS 區域

連線模型屬性：

- 提供未來在其他 區域中連線至 VPCs和 DX 連線的功能。
- 提供具有動態路由（BGP）的自動容錯移轉。
- 透過 AWS Transit Gateway ，您可以在 之間控制所需的通訊模型VPCs。如需詳細資訊，請參閱傳輸閘道的運作方式。

規模考量：

如需其他規模限制AWS Direct Connect的詳細資訊，例如支援的字首數目、VIFs每個 DX 連線類型的數目（專用、託管）。一些關鍵考量事項：

- 私有的BGP工作階段VIF最多可為 IPv4和 公告 100 個路由IPv6。
- 透過DXGW單一BGP工作階段，每個工作階段VPCs最多可連接 20 個。如果需要超過 20 個 VPCs，DXGWs可以新增額外的 ，以促進大規模的連線，或考慮使用 Transit Gateway 整合。
- 可視需要新增其他 AWS Direct Connect。

其他考量事項：

- 不會產生 與內部部署網路之間 AWS 資料傳輸 AWS Transit Gateway 的相關處理成本。
- VPC 無法參考遠端 的安全群組 AWS Transit Gateway （需要VPC對等）。
- VPC 對等可用來取代 AWS Transit Gateway 促進 之間的通訊VPCs，但這會增加操作複雜性，以大規模建立和管理大量VPC point-to-point對等。
- 如果不需要通訊VPC間，則此連線模型不需要 AWS Transit Gateway 或 VPC互連。

AWS DX – DXGW使用 VGW、多區域和 AWS 公有對等

此模型由以下項目構成：

- 多個內部部署資料中心具有與 的雙重連線 AWS。
- 與獨立 DX 位置的雙重 AWS Direct Connect 連線。
- AWS DXGW VPCs使用 直接連接至超過 10 VGW個，VPCs使用 最多可連接至 20 個VGW。
- 用於區域VPC間和區域間通訊 AWS Transit Gateway 的選用 。

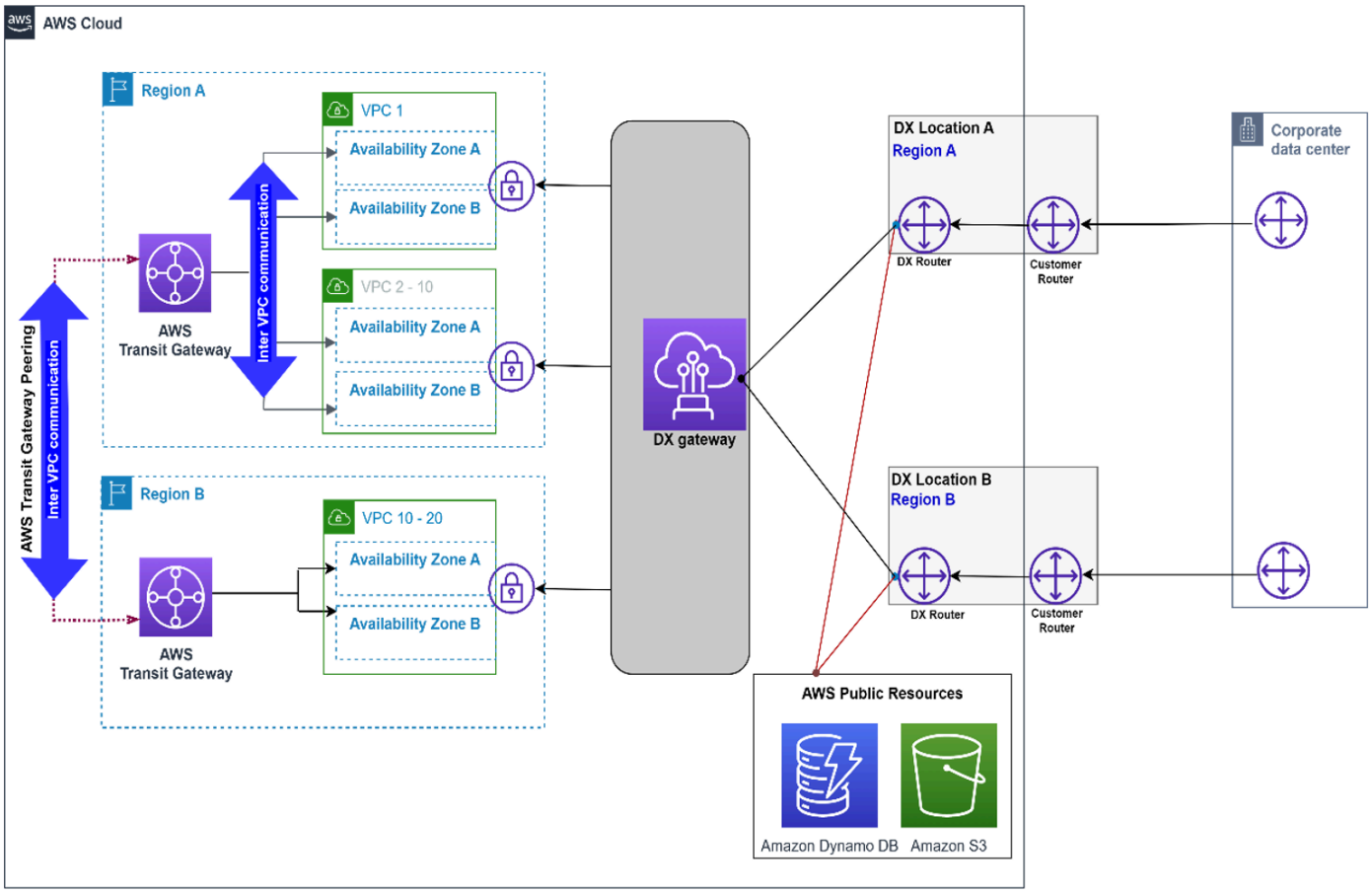

圖 6 – AWS DX – DXGW搭配 VGW、多區域和公有 VIF

連線模型屬性：

- AWS DXGW VPCs使用 直接連接至超過 10 個，VGW最多 VPCs 20 個VGW。
- AWS DX public VIF 用於直接透過 AWS DX 連線存取 AWS 公有服務，例如 Amazon S3。
- 提供未來在其他 區域中連線至 VPCs和 DX 連線的功能。
- 由 VPC和 Transit Gateway 互連促進的跨區域 AWS Transit Gateway 和跨區域VPC通訊。

規模考量：

如需其他規模限制AWS Direct Connect的詳細資訊，例如支援的字首數目、VIFs每個 DX 連線類型的數目（專用、託管）。一些關鍵考量事項：

- 私有的BGP工作階段VIF最多可為 IPv4和 公告 100 個路由IPv6。
- 每個私有 上的DXGW單一BGP工作階段VPCs最多可連接 20 VIF個，VIFs每個 最多可連接 30 個私有DXGW。

- 可視需要新增其他 AWS Direct Connect。

其他考量事項：

- 不會產生 和內部部署網路之間 AWS 資料傳輸 AWS Transit Gateway 的相關處理成本。
- VPC 無法由 參考遠端 的安全群組 AWS Transit Gateway （需要VPC對等）。
- VPC 對等化可以用來取代 AWS Transit Gateway 促進 之間的通訊VPCs，但這會增加操作複雜性，以大規模建立和管理大量VPC point-to-point對等化。
- 如果不需要通訊VPC間，則此連線模型不需要 AWS Transit Gateway 或 VPC互連。

AWS DX – DXGW使用 AWS Transit Gateway、多區域和 AWS 公有對等

此模型由以下項目構成：

- 多個 AWS 區域。
- 與獨立 DX 位置的雙重 AWS Direct Connect 連線。
- 單一內部部署資料中心，具有與 的雙重連線 AWS。
- AWS DXGW 使用 AWS Transit Gateway。
- VPCs 每個區域大規模 。

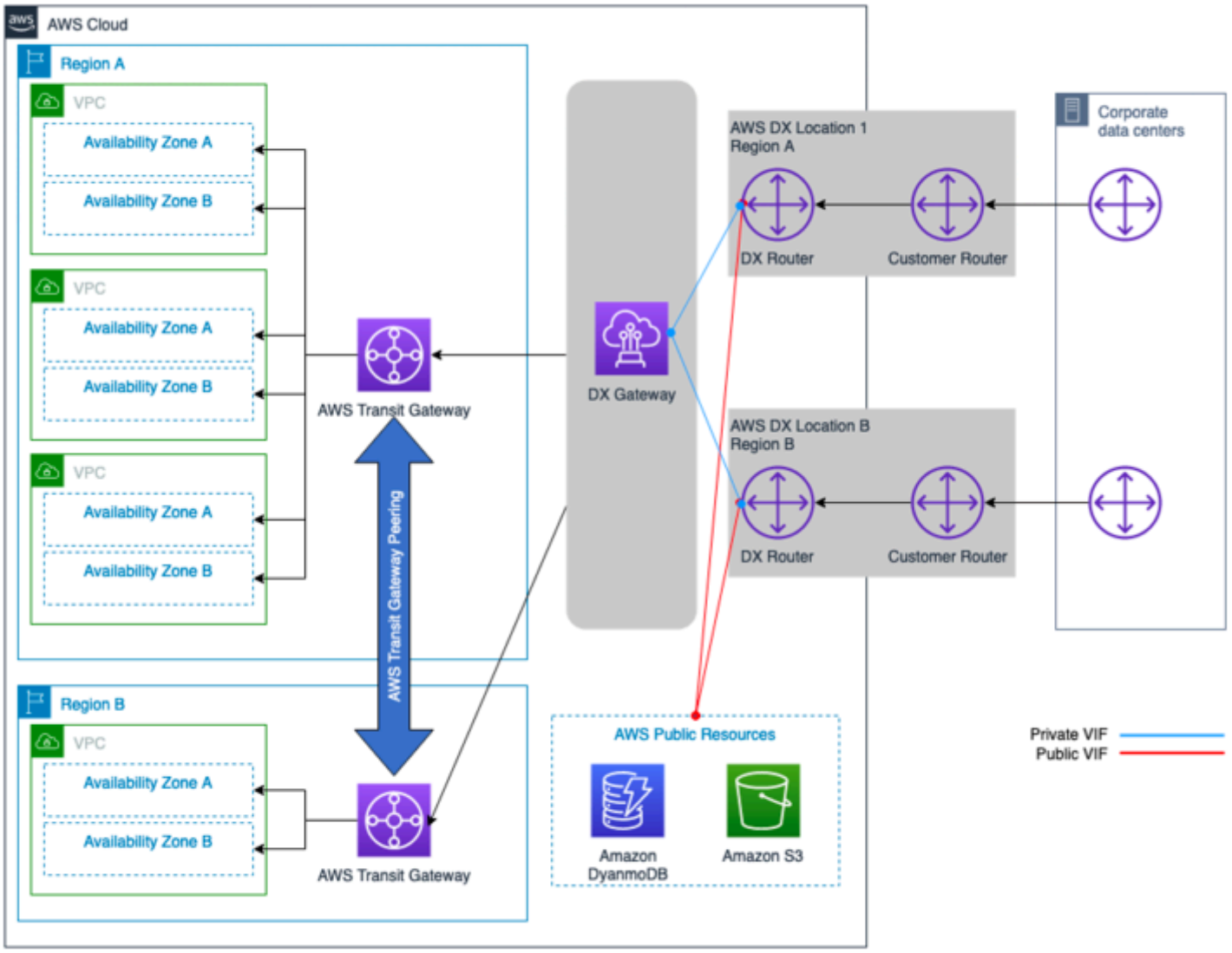

圖 7 – AWS DX – DXGW搭配 AWS Transit Gateway、多區域和 AWS 公有 VIF

連線模型屬性：

- AWS DX public VIF 用於直接透過 AWS DX 連線存取 S3 等 AWS 公有資源。
- 提供未來在其他 區域中連線至 VPCs 和/或 DX 連線的功能。
- AWS Transit Gateway 連線至 時VPCs，可以在 之間實現全部或部分網格連線VPCs。
- AWS Transit Gateway 互連促進的跨區域VPC和跨區域VPC通訊。
- 提供靈活的設計選項，以整合第三方安全和SDWAN虛擬設備與 AWS Transit Gateway。請參閱：流量 VPC-to-VPC 和內部部署的集中式網路安全VPC。

規模考量：

- 往返的路由數量限制 AWS Transit Gateway 為透過 Transit 支援的最大路由數量 VIF（傳入和傳出號碼不同）。如需規模限制和支援的路由數 和 的詳細資訊，請參閱AWS Direct Connect 配額VIFs。
- VPCs 每個 AWS Transit Gateway BGP工作階段最多可擴展數千個。
- VIF 每個 AWS DX 的單一傳輸。
- 可視需要新增其他 AWS DX 連線。

其他考量事項：

- 產生 AWS 和內部部署站台之間資料傳輸的額外 AWS Transit Gateway 處理成本。
- VPC 無法由 參考遠端 的安全群組 AWS Transit Gateway （需要VPC對等）。
- VPC 對等化可以用來取代 AWS Transit Gateway 促進 之間的通訊VPCs，但這會增加操作複雜性，以大規模建立和管理大量VPC point-to-point對等化。

AWS DX – DXGW使用 AWS Transit Gateway，多區域 （超過 3 個）

此模型由以下項目構成：

- 多個 AWS 區域 （超過 3 個）。
- 雙內部部署資料中心。
- 每個區域跨 至獨立 DX 位置的雙重 AWS Direct Connect 連線。
- AWS DXGW 使用 AWS Transit Gateway。
- VPCs 每個區域大規模 。
- 在 之間互連的完整網格 AWS Transit Gateway。

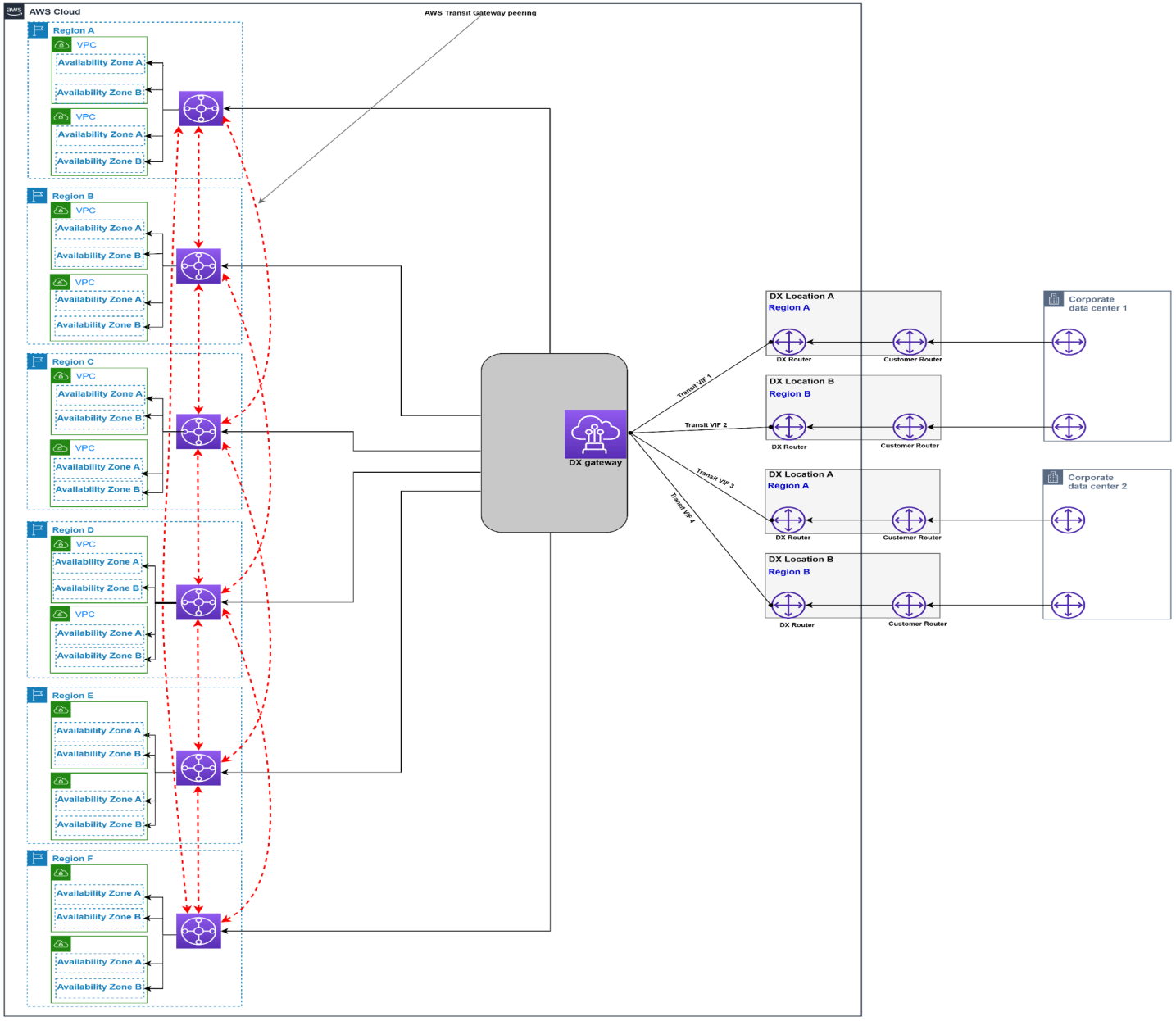

圖 8 – AWS DX – DXGW使用 AWS Transit Gateway、多區域 （超過三個 ）

連線模型屬性：

- 最低的操作開銷。
- AWS DX public VIF 用於直接透過 AWS DX 連線存取 AWS 公有資源，例如 S3。
- 提供未來在其他 區域中連線至 VPCs和 DX 連線的功能。
- AWS Transit Gateway 連線至 時VPCs，可以在 之間實現全部或部分網格連線VPCs。
- 區域間VPC通訊由 AWS Transit Gateway 對等促進。

- 提供靈活的設計選項，以整合第三方安全和SDWAN虛擬設備與 AWS Transit Gateway。請參閱：流量 VPC-to-VPC和內部部署的集中網路安全VPC。

規模考量：

- 往返的路由數量限制 AWS Transit Gateway 為透過 Transit 支援的最大路由數量 VIF（傳入和傳出號碼不同）。如需規模限制的詳細資訊，請參閱AWS Direct Connect 配額。如果需要減少路由數量，請考慮路由摘要。
- 每個BGP工作階段VPCs在每個工作階段 AWS Transit Gateway 上擴展到數千個 DXGW（假設佈建的 AWS DX 連線提供的效能足夠）。
- 每個 AWS Transit Gateway最多可連接六個 DXGW。
- 如果需要使用 連接三個以上的區域 AWS Transit Gateway，則需要額外的 DXGWs。
- VIF 每個 AWS DX 的單一傳輸。
- 可視需要新增其他 AWS DX 連線。

其他考量事項：

- 在內部部署站台與 之間進行資料傳輸時，會產生額外的 AWS Transit Gateway 處理成本 AWS。
- VPC 無法由 參考遠端 的安全群組 AWS Transit Gateway （需要VPC對等）。
- VPC 對等可用來取代 AWS Transit Gateway 促進 之間的通訊VPCs，但這會增加操作複雜性，以大規模建立和管理大量VPC point-to-point對等。

下列決策樹涵蓋可擴展性和通訊模型考量：

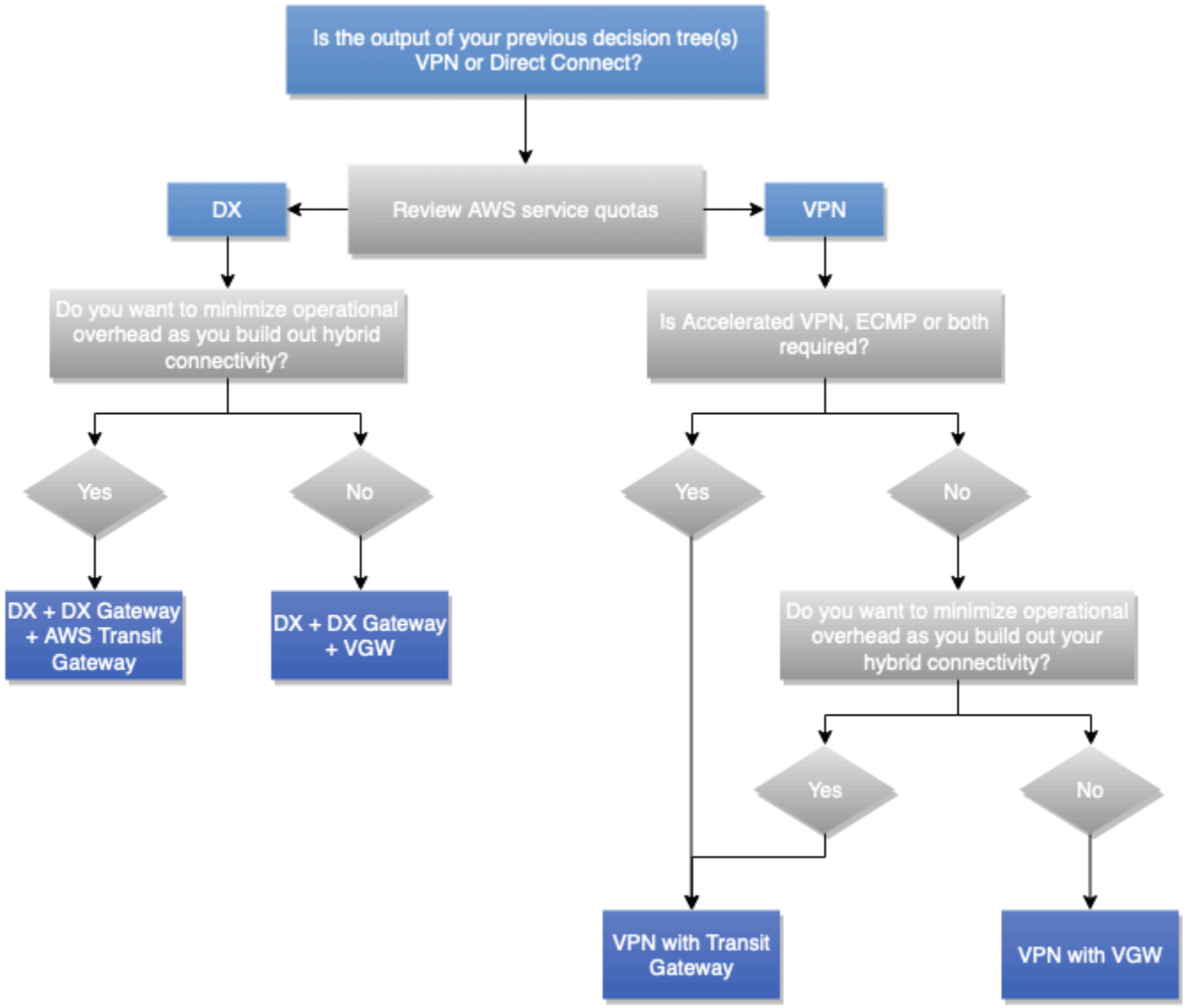

圖 9 – 可擴展性和通訊模型決策樹

> **Note**
>
> 如果選取的連線類型為 VPN，通常在效能考量時，應決定VPN終止點是 AWS VGW還是 AWS Transit Gateway AWS S2S VPN連線。如果尚未完成，您可以考慮 之間所需的通訊模型，VPC以及連線到VPN連線VPC所需的 （數目），以協助您做出決策。

可靠性

定義

可靠性是指服務或系統在必要時執行其預期功能的能力。系統可靠性可以透過其在指定時間範圍內的操作品質水準來測量。與彈性形成對比，彈性是指系統從基礎設施或服務中斷中動態且可靠地復原的能力。

如需如何使用可用性和彈性來測量可靠性的詳細資訊，請參閱 AWS Well-Architected Framework 的可靠性支柱。

關鍵問題

可用性

可用性是工作負載可供使用的時間百分比。常見目標包括 99%（每年允許 3.65 天的停機時間）、99.9%（8.77 小時）和 99.99%（52.6 分鐘），其中一小部分是百分比中的九位數（99% 為「二九」，99.9% 為「三九」等）。 AWS 與內部部署資料中心之間的聯網解決方案可用性可能與整體解決方案或應用程式可用性不同。

網路解決方案可用性的關鍵問題包括：

- 如果我的 AWS 資源無法與我的內部部署資源通訊，是否可以繼續運作？ 反之亦然？
- 我應該將計劃維護的排程停機時間視為包含在可用性指標中或排除在可用指標之外嗎？
- 與整體應用程式運作狀態分開，我如何衡量聯網層的可用性？

Well-Architected Framework Reliability Pillar 的可用性區段提供計算可用性的建議和公式。

彈性

彈性是工作負載在以下方面的能力：從基礎架構或服務中斷恢復、動態取得運算資源以符合需求，以及緩解中斷狀況 (例如，設定錯誤或暫時性網路問題)。如果備援網路元件（連結、網路裝置等）沒有足夠的可用性自行提供預期的函數，則其對故障的恢復能力較低。結果是使用者體驗不佳和降級。

網路解決方案彈性的關鍵問題包括：

- 我應該允許多少次同時發生、分散的故障？
- 如何透過連線解決方案和內部網路來減少單一故障點？
- 分散式拒絕服務（DDoS）事件的漏洞是什麼？

技術解決方案

首先，請務必注意，不是每個混合網路連線解決方案都需要高水準的可靠性，而且提高可靠性水準會相應增加成本。在某些情況下，主要站台可能需要可靠（備援和彈性）連線，因為停機時間對業務的影響較高，而區域站台可能因為發生故障事件時對業務的影響較低，而不需要相同層級的可靠性。建議參考AWS Direct Connect 復原建議，因為它說明了確保高復原性的 AWS 最佳實務 AWS Direct Connect 。

為了在恢復能力的情況下實現可靠的混合網路連線解決方案，設計需要考慮以下方面：

- 備援：旨在消除混合網路連線路徑中的任何單一故障點，包括但不限於網路連線、邊緣網路裝置、跨可用區域和 DX 位置的備援 AWS 區域，以及裝置電源、光纖路徑和作業系統。為了本白皮書的目的和範圍，備援著重於網路連線、邊緣裝置（例如，客戶閘道裝置）、 AWS DX 位置和 AWS 區域（適用於多區域架構）。
- 可靠的容錯移轉元件：在某些情況下，系統可能正常運作，但無法在所需的層級執行其功能。在單一故障事件期間，這種情況很常見，其中發現規劃的備援元件以非備援方式運作，因為使用量，其網路負載沒有其他位置可前往，導致整個解決方案的容量不足。
- 容錯移轉時間：容錯移轉時間是次要元件完全接管主要元件角色所需的時間。容錯移轉時間有多個因素：偵測失敗所需的時間、啟用次要連線所需的時間，以及通知網路其餘部分變更所需的時間。可以使用VPN連結的失效對等偵測（DPD）和 AWS Direct Connect 連結的雙向轉送偵測（BFD）來改善故障偵測。啟用次要連線的時間可能非常短（如果這些連線一律處於作用中狀態）、可能是短時間時段（如果需要啟用預先設定的VPN連線）或更長的時間（如果需要移動實體資源或設定新資源）。通知網路的其餘部分通常透過客戶網路內的路由通訊協定進行，每個通訊協定都有不同的收斂時間和組態選項 – 這些組態超出了本白皮書的範圍。
- 流量工程：彈性混合網路連線設計的流量工程旨在解決正常和失敗情況下，流量應如何通過多個可用連線。建議遵循故障設計概念 ，其中您需要查看解決方案在不同故障情況下的運作方式，以及業務是否接受。本節討論一些常見的流量工程使用案例，旨在增強混合網路連線解決方案的整體彈性。AWS Direct Connect 有關路由和討論幾個流量工程選項來影響流量流的章節 BGP（社群、BGP本機偏好設定、AS Path 長度）。若要設計有效的流量工程解決方案，您需要充分了解每個 AWS 網路元件在路由評估和選擇方面如何處理 IP 路由，以及影響路由選擇的潛在機制。其詳細資訊超出本文件的範圍。如需詳細資訊，請參閱視需要的 Transit Gateway Route Evaluation Order、Site-to-Site VPNRoute Priority 和 Direct Connect Routing 和BGP文件。

> **Note**
>
> 在VPC路由表中，您可以參考具有其他路由選擇規則的字首清單。如需此使用案例的詳細資訊，請參閱字首清單的路由優先順序。 AWS Transit Gateway 路由表也支援字首清單，但一旦套用，它們就會擴展到特定的路由項目。

具有更特定路由的雙 Site-to-SiteVPN連線範例

此案例是以小型內部部署站台為基礎，透過網際網路連接至 的單一 AWS 區域 備援VPN連線 AWS Transit Gateway。圖 10 中描述的流量工程設計顯示，透過流量工程，您可以透過以下方式影響提高混合連線解決方案可靠性的路徑選擇：

- 彈性混合連線：備援VPN連線各提供相同的效能容量，使用動態路由通訊協定 （BGP） 支援自動容錯移轉，並使用VPN無效對等偵測加快連線失敗偵測。
- 效能效率：在兩個VPN連線ECMP之間設定 ， AWS Transit Gateway 有助於最大化整體VPN連線頻寬。或者，透過廣告不同的更具體路由以及網站摘要路由，可以管理兩個VPN連線之間的負載獨立性

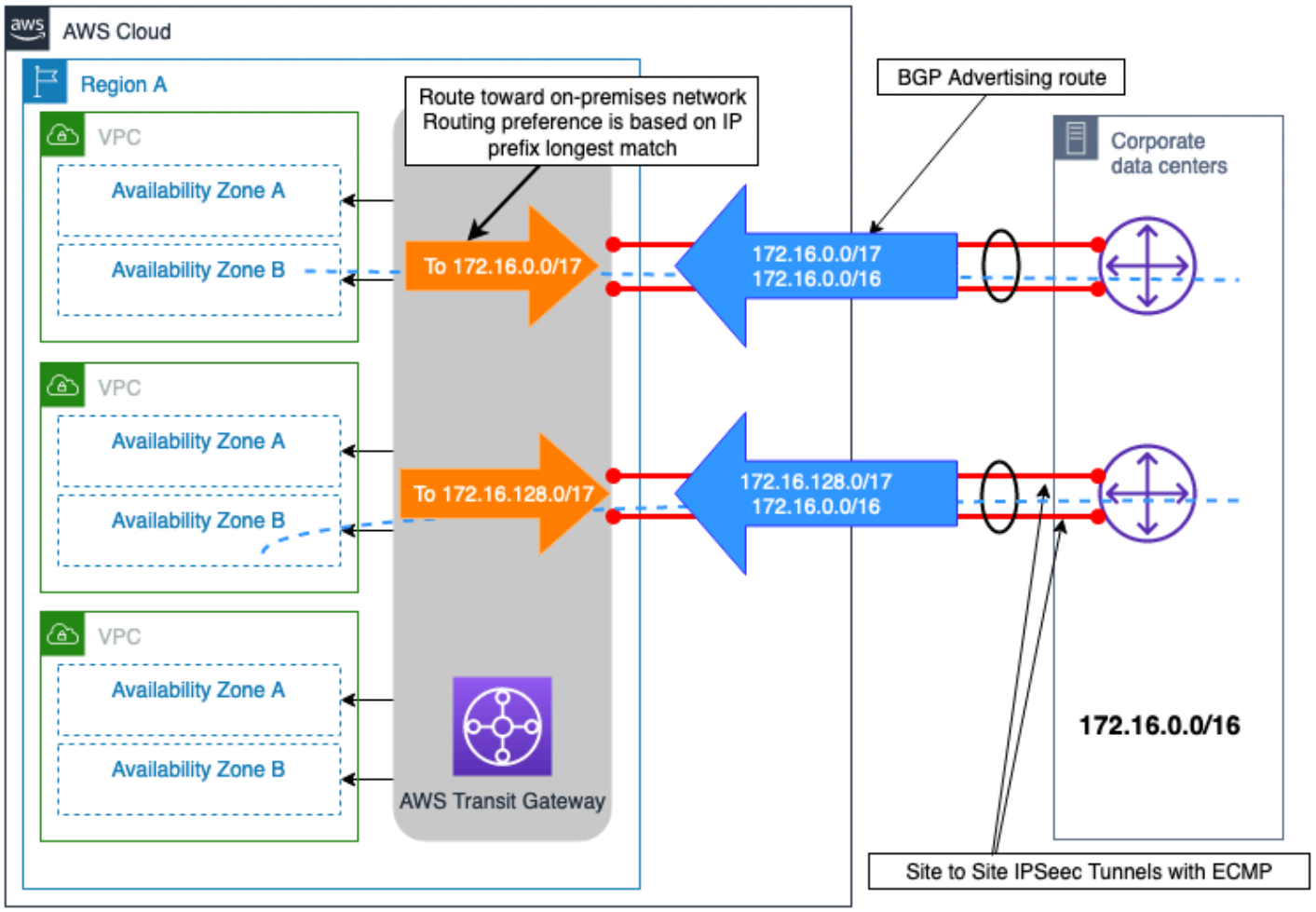

圖 10 – 具有更特定路由的雙 Site-to-SiteVPN連線範例

具有多個 DX 連線的雙內部部署站台範例

圖 11 中所示的案例顯示位於不同地理區域的兩個內部部署資料中心網站，並使用 AWS Direct Connect 搭配 DXGW和 AWS 使用 的最大恢復能力連線模型（如 AWS Direct Connect 恢復力建議 所述）來連線至 VGW。這兩個內部部署站台會透過資料中心互連（DCI）連結彼此互連。屬於遠端分支站台的內部部署 IP 字首（192.168.0.0/16）會從兩個內部部署資料中心站台公告。此字首的主要路徑應為資料中心 1。如果資料中心 1 或兩個 DX 位置發生故障，往返遠端分支站台的流量將容錯移轉至資料中心 2。此外，每個資料中心都有一個網站特定的 IP 字首。這些字首需要直接到達，如果兩個 DX 位置都失敗，則需要透過其他資料中心網站。

透過將BGP社群屬性與通告 的路由建立關聯 AWS DXGW，您可以影響來自 AWS DXGW 端的輸出路徑選擇。這些社群屬性會控制指派給公告路由 AWS的 BGP 本機偏好設定屬性。如需詳細資訊，請參閱 AWS DX Routing 政策和BGP社群 。

為了最大限度地提高 AWS 區域 連線層級的可靠性，每對 AWS DX 連線都會進行設定，ECMP以便可以同時將兩者用於每個內部部署站台與 之間的資料傳輸 AWS。

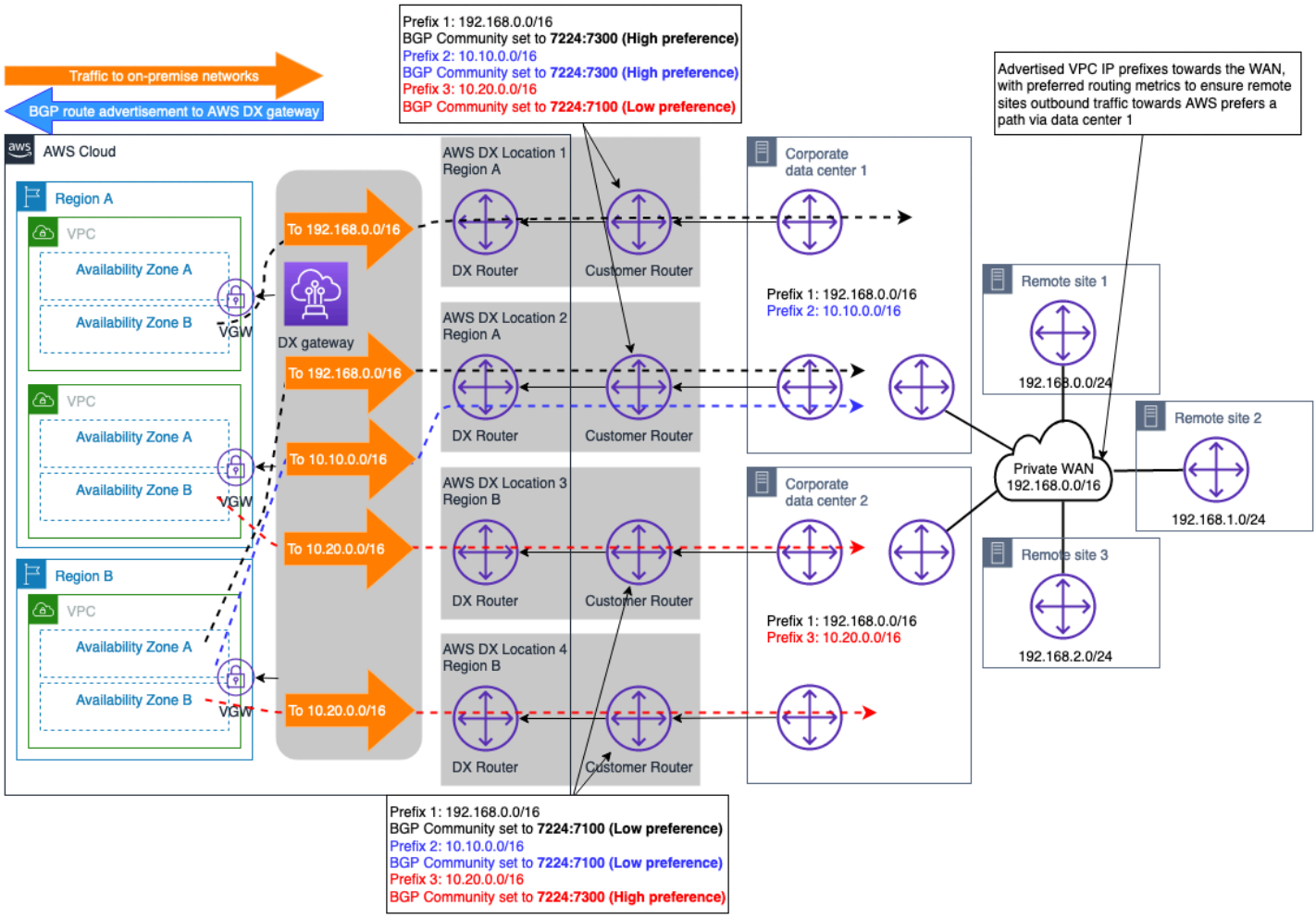

圖 11 – 具有多個 DX 連線的雙內部部署站台範例

透過此設計，目的地為內部部署網路（具有相同的公告字首長度和BGP社群）的流量將使用 分散到每個站台的雙 DX 連線ECMP。不過，如果 DX 連線ECMP不需要 ，則可以使用先前討論的相同概念，並在路由政策和BGP社群文件中描述，進一步在 DX 連線層級設計路徑選擇。

注意：如果內部部署資料中心內的路徑中存在安全裝置，則需要設定這些裝置，以允許流量透過一個 DX 連結離開，並從相同資料中心網站內的另一個 DX 連結（兩個連結都與 搭配使用ECMP）離開。

VPN 連線作為 DX AWS 連線的備份範例

VPN 可以選取 以提供備份網路連線至 AWS Direct Connect 連線。一般而言，這種類型的連線模式是由成本所驅動，因為它因為網際網路上的效能不確定，而為整體混合連線解決方案提供較低程度的可靠

性，而且無法透過公有網際網路SLA取得連線。這是有效且符合成本效益的連線模型，當成本是最高優先順序考量且預算有限時，或可能作為臨時解決方案使用，直到可以佈建次要 DX 為止。圖 12 說明此連線模式的設計。此設計的一個關鍵考量因素是， VPN和 DX 連線都在 終止 AWS Transit Gateway，相較於可透過連接至 的 DX 連線公告的路由，VPN連線可以公告更多路由 AWS Transit Gateway。這可能會導致路由狀況欠佳。解決此問題的選項是在客戶閘道裝置 （CGW） 設定從VPN連線接收路由的路由篩選，僅允許接受摘要路由。

注意：若要在 上建立摘要路由 AWS Transit Gateway，您需要指定路由表中任意連接的靜態 AWS Transit Gateway 路由，以便沿著更具體的路由傳送摘要。

從 AWS Transit Gateway 路由表的角度來看，內部部署字首的路由會從 AWS DX 連線 （透過 DXGW） 和 從 接收VPN，字首長度相同。在 的路由優先順序邏輯之後 AWS Transit Gateway，透過 Direct Connect 接收的路由比透過 Site-to-Site 接收的路由具有更高的偏好設定VPN，因此透過 的路徑 AWS Direct Connect 將優先於到達內部部署網路 （in-premise network）。

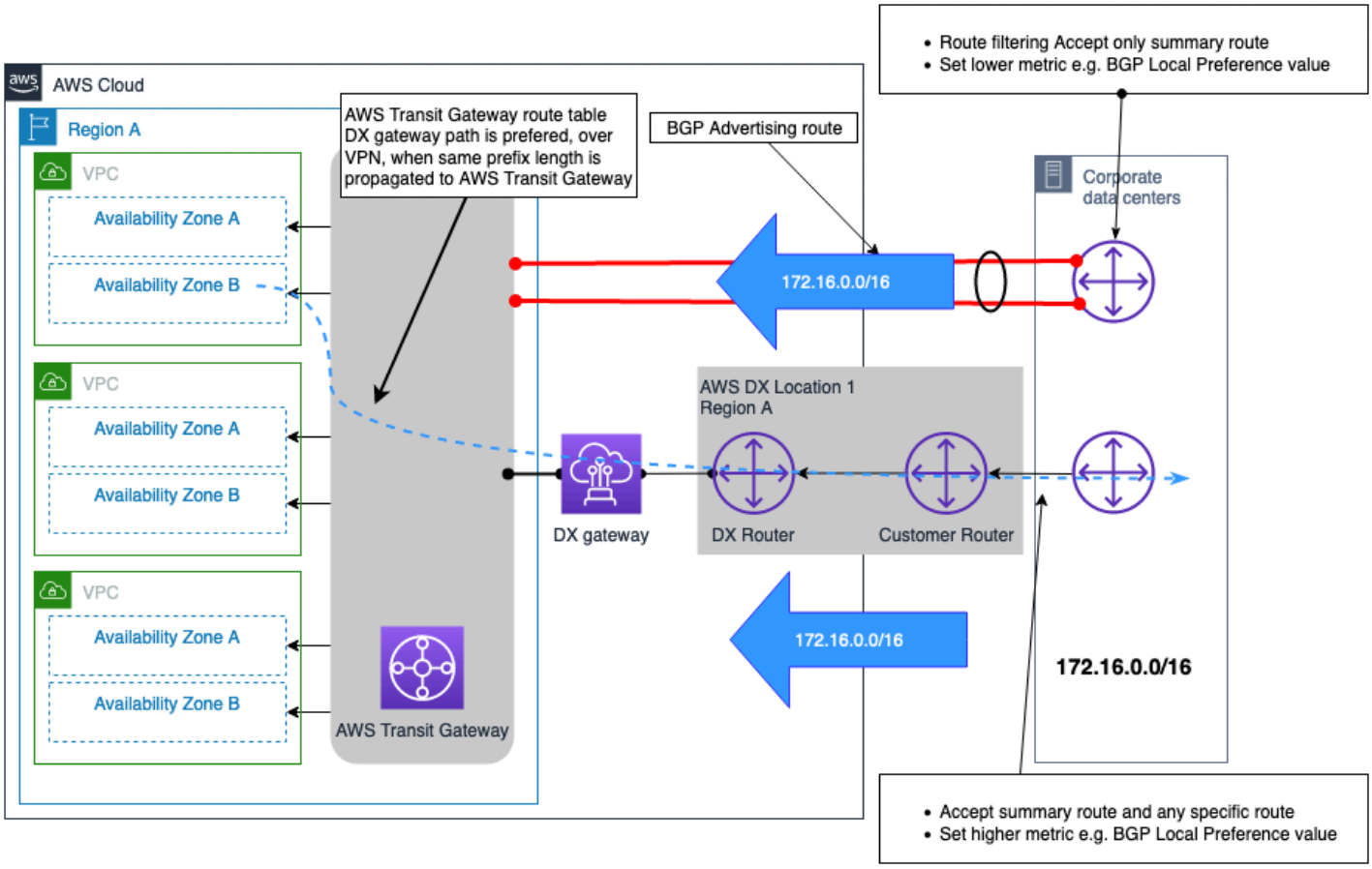

圖 12 – 作為 DX AWS VPN連線備份的連線範例

下列決策樹會引導您做出所需的決策，以達到彈性 （這將產生可靠的） 混合網路連線。如需詳細資訊，請參閱AWS Direct Connect 彈性工具組 。

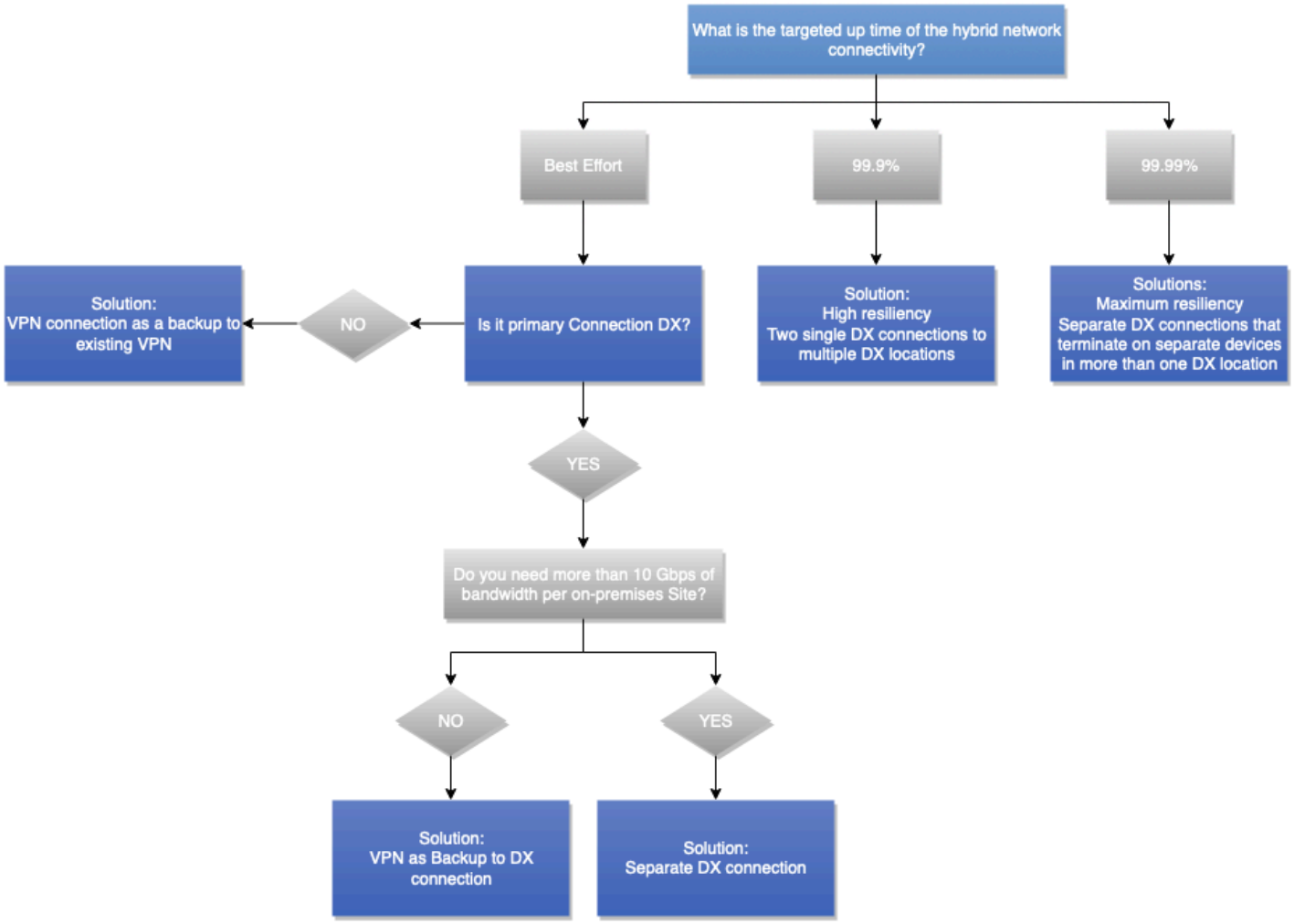

圖 13 – 可靠性決策樹

客戶受管VPN和 SD-WAN

定義

網際網路的連線能力是一種商品，可用的頻寬每年都會持續增加。有些客戶選擇在網際網路WAN上建置虛擬，而不是建置和操作私有 WAN。軟體定義的廣域網路 （SD-WAN） 可讓公司WAN透過聰明的軟體使用，快速佈建並集中管理此虛擬。其他客戶選擇將傳統自我管理網站套用至網站 VPNs。

對設計決策的影響

SDWAN 和客戶受管 VPNs 可以透過網際網路或 執行 AWS Direct Connect。SD-WAN （或任何軟體VPN覆蓋） 與基礎網路傳輸一樣可靠。因此，本白皮書前面討論的可靠性和SLA考量事項在此適用。例如，與透過 建置相比，透過網際網路建置 SD-WAN 覆蓋不會提供相同的可靠性 AWS Direct Connect。

需求定義

- 您是否在內部部署網路中使用 SD-WAN？
- 您需要哪些特定功能僅適用於用於VPN終止的特定虛擬設備？

技術解決方案

AWS 建議將 SD-WAN 與 整合 AWS Transit Gateway，並發佈支援 AWS Transit Gateway 整合的廠商清單。 AWS 可以充當 SD-WAN 站台的中樞或發言站台。骨幹可用於將部署在 AWS 中的不同 SD WAN中樞 AWS 與高度可靠且高效能的網路連接。SD-WAN 解決方案支援透過單一管理窗格中任何可用路徑的自動容錯移轉、額外監控和可觀測功能。與傳統 相比，廣泛使用自動組態和自動化可實現快速佈建和可見性WANs。但是，使用通道和加密額外負荷不會與私有連線中使用的專用、高速光纖連結進行比較。

在某些情況下，您可以選擇使用具有 VPN功能的虛擬設備。選擇自我管理虛擬設備的原因包括技術功能，以及與網路其餘部分的相容性。當您選擇使用在EC2執行個體中部署的虛擬設備自我管理VPN或 SD-WAN 解決方案時，您有責任管理此類設備。您也必須負責虛擬設備之間的高可用性和容錯移轉。這種設計會增加您的操作責任；但它可以為您提供更多的靈活性。解決方案的特徵和功能取決於您選擇的虛擬設備。

AWS Marketplace 包含許多VPN虛擬設備，客戶可以在 Amazon 上部署EC2。 AWS 建議從 AWS 受管 S2S 開始VPN，並在不符合您的需求時查看其他選項。虛擬設備的管理開銷是客戶的責任。

範例公司汽車使用案例

白皮書的這一部分示範如何使用考量、需求定義問題和決策樹來協助您決定最佳的混合式網路設計。識別和捕獲的要求是很重要的，因為它們被用作輸入到決策樹。預先擷取需求可避免進一步的設計迭代。如果必須重新審視設計並保留寶貴的資源，則可以將專案完全停止，並且在預先了解需求時最理想地避免這個專案。

實施例公司汽車將在整個部分作為說明客戶使用。他們希望最初部署他們的第一個分析項目AWS。該分析項目專注於分析公司生產的汽車以及公司數據中心已存在的其他數據集中的數據集的數據。最初，該公司的架構團隊認為他們需要一AWS 帳戶個 Amazon VPC 和少數子網來託管生產和開發環境。專案團隊渴望開始使用，而且他們要求儘快存取開發環境。他們的目標是從現在開始三個月後進行生產。

Example Corp. 汽車還計劃用AWS於其他幾個項目，例如將其 ERP 系統，虛擬桌面基礎架構（VDI）以及另外 20 個應用程序從內部部署遷AWS移到未來 6 個月。其他項目的一些要求仍在定義中，但很明顯，它們的AWS 雲端使用率將會增長。

架構團隊決定利用本白皮書中概述的方法。他們使用每個考量下概述的需求定義問題來捕獲輸入來做出他們的設計決策。

它們從與連接類型相關的需求開始，這些需求摘要如下表所示。

表 4-示例汽車公司可靠性輸入

連線類型選擇考量	需求定義問題	答案
部署時間	部署所需的時間表為何？ 小時，天，幾週或幾個月？	• 開發/測試：1 個月 • 生產：3 個月
安全性	您的安全要求和政策是否允許使用互聯網上的加密連接來連接AWS或強制使用私人網絡連接？	• 開發/測試：可接受 Site-to-Site VPN • 生產：需要私人網絡
	利用私人網路連線時，網路層是否必須在傳輸過程中提供加密？	否，將使用應用程式層加密。
SLA	是否需要含服務點數的混合式連線 SLA？	• 開發/測試：否

連線類型選擇考量	需求定義問題	答案
		• 生產：是
	什麼是正常運行時間目標？	• 開發/測試：N/A • 生產量:
	整個混合網絡是否遵守正常運行時間目標？	• 開發/測試：N/A • 生產：是
效能	什麼是所需的吞吐量？	• 開發/測試：100 兆比特 • 產量：500 兆比特增長至 2 千兆比特
	AWS與內部部署網路之間可接受的最大延遲是多少？	• 開發/測試：沒有硬性要求 • 製作：小於 30 毫秒
	最大可接受的網路抖動是多少？	• 開發/測試：沒有硬性要求 • 生產：所需的最小抖動
成本	您AWS每月會傳送多少資料？	• 開發/測試：2 TB • 產量：20 TB 成長至 50 TB
	您AWS每月會傳送多少資料？	• 開發/測試：1 TB • 產量：10 TB 成長至 25 TB
	此連線是永久性的嗎？	是

根據收到的需求，架構小組遵循連線類型決策樹狀結構圖 9。它允許架構團隊決定開發、測試和生產環境的連接類型。對於生產環境，他們考慮了立即以及即將到來的要求。對於開發和測試實例公司汽車將建立在互聯網上的 site-to-site VPN。對於生產，他們將與服務提供商合作以將其公司網絡連接起來 AWS Direct Connect。示例公司汽車最初考慮使用直接 Connect 託管 Connect，但由於AWS提供 SLA 的要求，他們選擇了直接連接專用連接。

決定連線類型之後，下一個步驟是擷取會影響連線設計選擇的需求。這與邏輯設計有關，例如連接的配置方式以及用於支持業AWS務和技術需求的服務。

為了掌握延展性和通訊模型需求，架構團隊使用本白皮書相關章節中的需求定義問題。下表摘要說明與這兩個考量相關的需求。

表 5 — 需求定義問題

連接性設計選擇考量	需求定義問題	答案
擴充性	需要連線至內部部署站台的目前或預期 VPC 數目為何？	2 最初，在 6 個月內增長到 30
	這些 VPC 是否部署在單一AWS 區域或多個區域？	單一區域
	需要連線到多少個內部部署網站AWS？	2 個數據中心
	您每個站台有多少個需要連線的客戶閘道裝置AWS？	每個資料中心 2 個路由器
	預計將向 AWS VPC 廣告多少條路由，以及從側面接收的預期路由AWS數量？	• 要廣告的路線 AWS：20 條路線 • 從接收的路線AWS：1 條/16路線
	是否有計劃在不久的 future 考慮連接AWS的帶寬增加？	• 開發/測試：100 兆比特 • 產量：500 兆每秒增長到 2 吉比特。
連接設計模型	是否需要啟用 VPC 間通訊 (在一個區域內和/或跨區域)？	是的，在 AWS 區域
	是否需要直接從內部部署存取AWS公用端點服務？	是
	是否需要從內部部AWS署使用 VPC 端點存取服務？	否

根據輸入，架構團隊會遵循「連線設計」區段中的決策樹狀結構。在預計未來 6 個月的 VPC 數量將從 2 增加到 30 之後，架構團隊決定將用AWS Transit Gateway作連線和 VPC 間路由的終止閘道。獨立AWS Transit Gateway的將終止用於開發和測試的 VPN 連接，以及與生產連接AWS Direct Connect。分離的 AWS Transit Gateway s 的使用使變更管理更簡單，並在開發/測試和生產環境之間提供了明確的分界。對於生產，因為需要AWS Direct Connect閘道AWS Transit Gateway。公用 VIF 將用於存取AWS公用端點服務。圖 14 說明了根據收集到的要求在決策樹上採取的路徑。

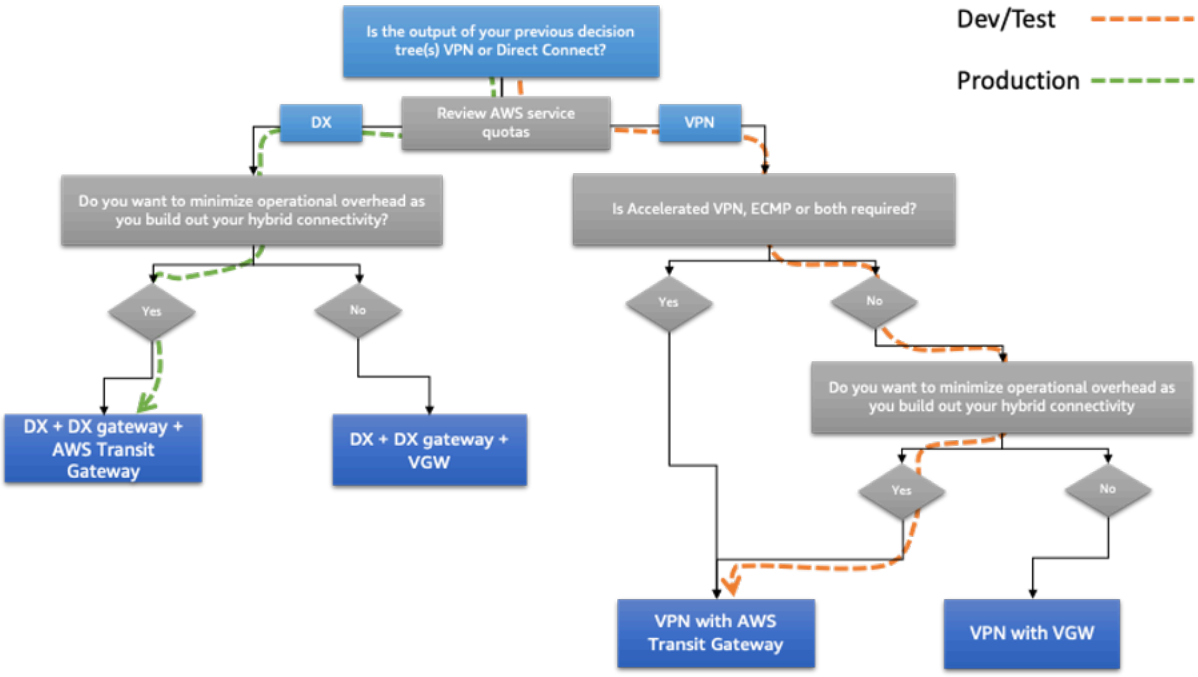

圖 14 — 範例公司汽車連接設計決策樹

在決定解決方案以滿足可擴展性和通信模型需求之後，下一步是捕獲與可靠性相關的要求。這與所需的可用性和恢復性等級有關。

為了掌握可靠性需求，架構團隊使用本白皮書相關章節中的需求定義問題。需求摘要如下表所示。

表 6 — 可靠性要求問題

連接性設計選擇考量	需求定義問題	答案
可靠性	在連線失敗的情況下，對企業的影響程度為何AWS？	• 開發/測試：低 • 生產：高

連接性設計選擇考量	需求定義問題	答案
	從業務角度來看，連接失敗後的成本是否會AWS超過部署高度可靠連接模型的成本？AWS	• 開發/測試：否 • 生產：是

根據收到的輸入，架構團隊會遵循本白皮書先前涵蓋的可靠性考量部分中的決策樹。在考慮到生產連線的正常執行時間目標為 99.99%，以及服務中斷時所產生的高企業影響之後，架構團隊決定使用 2 個 Direct Connect 位置，並從每個內部部署資料中心到每個 Direct Connect 位置有 2 個連結 (總共 4 個連結)。用於開發和測試的 VPN 連接也將使用兩個 VPN 連接來提供額外的冗餘。使用可靠性一節中討論的路由工程技術，連接性將配置如下：

- 對於開發和測試，流量將使用 ECMP 在通往主要資料中心的 2 個通道上進行負載平衡。這允許更高的吞吐量。通往輔助數據中心的隧道將在主隧道故障的情況下使用。
- 對於生產環境，內部部署和其中一AWS個直 Connect 位置之間的延遲非常相似。在此情況下，已決定透過前往主要資料中心內部部署系統之內部部署系統的兩個連線，負載平衡AWS與內部部署的流量。同樣地，對於在次要資料中心執行的內部部署系統，流量會在兩個連線到次要資料中心之間進行負載平衡。如果連接失敗，BGP 將促進自動故障轉移。

圖 15 說明了根據收集到的要求在決策樹上採取的路徑。

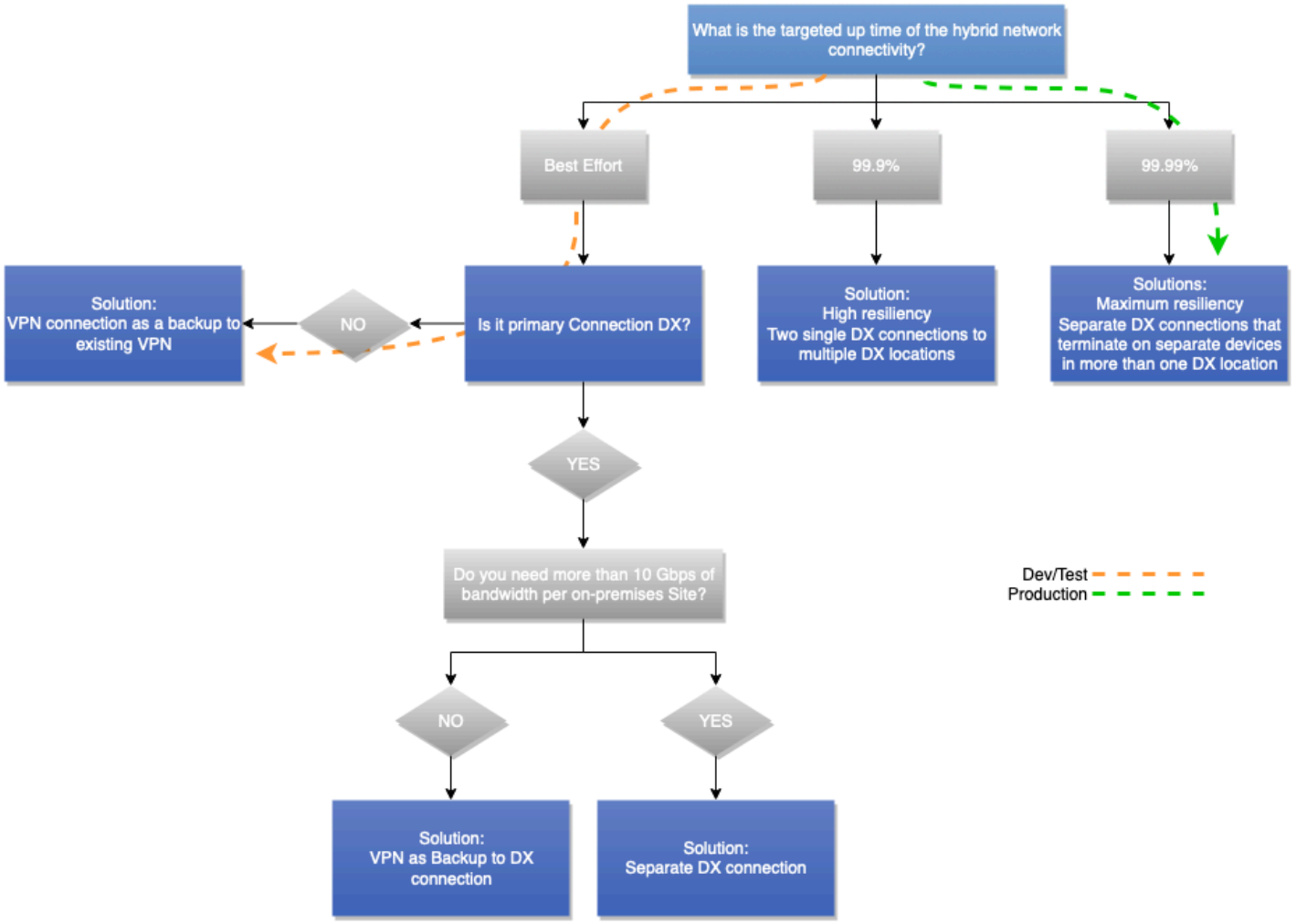

圖 15-實例公司汽車可靠性決策樹

由實施例公司選擇的架構汽車

下圖說明 Example Corp. Motorage 在收集需求並瀏覽本白皮書前面章節涵蓋的決策樹之後選取的架構。

它通過互聯網使用 AWS S2S VPN 終止開AWS Transit Gateway發和測試。然後，它AWS Direct Connect與直接 Connect 閘道和第二個用AWS Transit Gateway於生產流量。 AWS Transit Gateway用於 VPC 間路由。從資料路徑的角度來看，主要資料中心的 VPN 通道會用作開發和測試的主要路徑，而次要資料中心的通道則用作容錯移轉路徑。對於生產流量，所有連接都會同時使用。來自的流量會根據內部部署系統所在的資料中心，AWS偏好最選擇性的網路連線。Example Corp. Motorage 使用類似的路由工程技術，在傳送流量時偏好適當的路徑，以AWS確保使用對稱的流量路徑，以盡量減少內部部署主要和次要資料中心之間使用公司網路的情況。

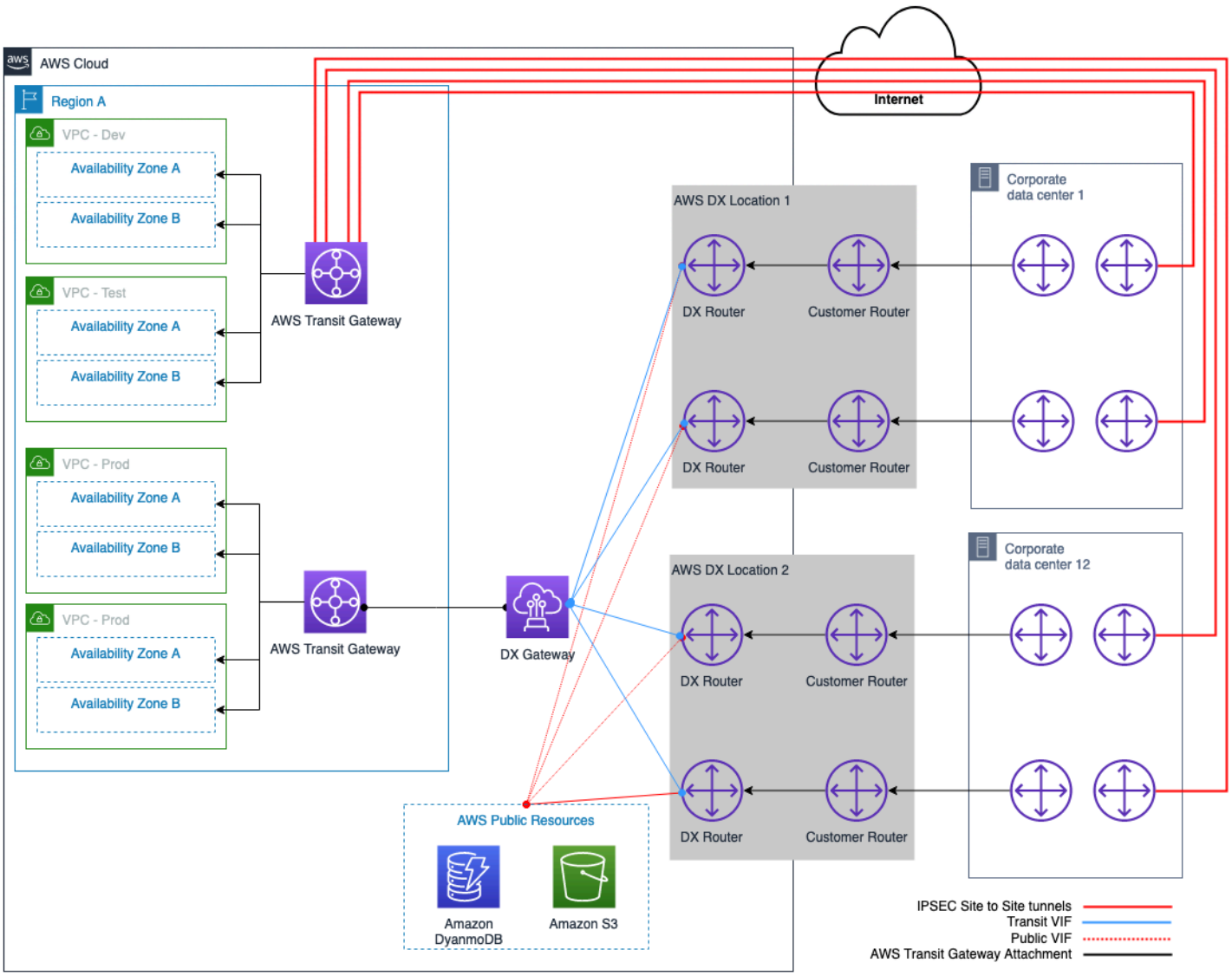

圖 16-實例公司汽車選擇的混合連接模型

結論

混合式連線模型是採用雲端運算的基本起點之一。您可以遵循本白皮書所述的連線模型選擇程序，使用最佳架構建立混合式網路。

該過程包括按邏輯順序安排的考慮因素。該訂單非常類似於心理模型，其次是經驗豐富的網絡和雲架構師。在每個考量組中，決策樹允許快速選擇連接模型，即使輸入需求有限。您可能會發現一些考量和相應的影響指向不同的解決方案。在這些情況下，作為決策者，您可能需要在某些需求上妥協，並選擇符合您業務和技術需求的最佳解決方案。

貢獻者

本文件的貢獻者包括：

- 詹姆斯·德文，首席解決方案架構師，Amazon Web Services
- 安德魯·格雷，首席解決方案架構師 — 聯網，Amazon Web Services
- 更多, 高級解決方案架構師, 亞馬遜 Web 服務
- 馬文·阿爾沙維，解決方案架構師，Amazon Web Services
- 聖地亞哥·弗雷塔斯，技術負責人，Amazon Web Services
- 葉夫根尼·瓦加諾夫，專業解決方案架構師 — 聯網，Amazon Web Services
- 湯姆·亞當斯基，專業解決方案架構師 — 網絡，Amazon Web Services
- 阿姆斯特朗 O奈wu，解決方案架構師，Amazon Web Services

深入閱讀

- 建立可擴展且安全的多個 VPC AWS 網路架構
- 亞馬遜 VPC 的混合雲 DNS 選項
- Amazon Virtual Private Cloud 連線選項
- Amazon Virtual Private Cloud 文件
- AWS Direct Connect 文件
- 託管虛擬界面（VIF）和託管連接有什麼區別？

文件修訂

如要接收此白皮書更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
次要更新	已更新以反映 DX 配額限制提高。	2023年7月10日
重大更新	已更新以納入最新的最佳做法、服務和功能。	2023 年 7 月 6 日
次要更新	更新了參考架構圖，以反映 DX 配額的變化。	2023 年 6 月 27 日
次要更新	修正了斷開的鏈接。	2022 年 3 月 22 日
初始出版	白皮書首次出版	2020 年 9 月 22 日

注意

客戶有責任對本文件中的資訊進行自行獨立評估。本文件：(a) 僅供參考，(b) 代表目前的AWS產品供應項目和做法，如有變更，恕不另行通知，且 (c) 不會向其關聯公司、供應商或授權人建立任何承諾或保證。AWS AWS產品或服務係依「原狀」提供，不含任何明示或暗示之擔保、陳述或條件。客戶的責任和責任由AWS協議控制，本文件不屬於與客戶之間AWS的任何協議的一部分，也不會修改。AWS

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

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。