



架構圖表

在 上實作 SD-WAN 解決方案的參考架構 AWS



在上實作 SD-WAN 解決方案的參考架構 AWS: 架構圖表

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

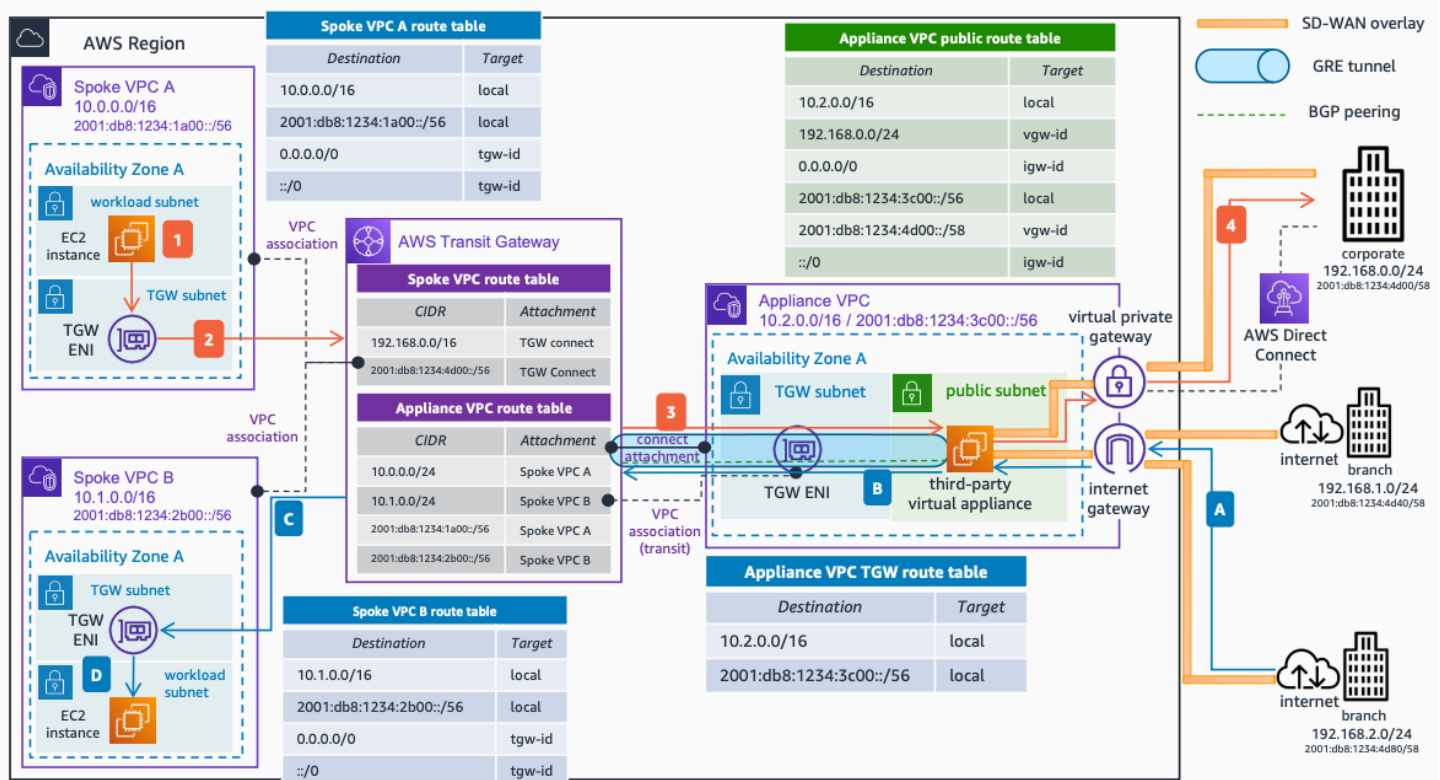
TGW Connect	1
與 AWS Transit Gateway Connect 架構的 SD-WAN 連線	1
深入閱讀	2
圖表歷史記錄	2
雲端 WAN Connect	4
使用 AWS Cloud WAN Connect 架構的 SD-WAN 連線	4
深入閱讀	5
圖表歷史記錄	5
Cloud WAN 無通道	7
使用 AWS Cloud WAN Tunnel-less Connect 架構的 SD-WAN 連線	7
深入閱讀	8
圖表歷史記錄	8
VPN 到 TGW	10
使用 AWS Site-to-Site VPN 連線至 AWS Transit Gateway 架構的 SD-WAN 連線	10
深入閱讀	11
圖表歷史記錄	11
VPN 到雲端 WAN	13
SD-WAN 連線至 AWS Site-to-Site VPN 到 AWS Cloud WAN 架構	13
深入閱讀	14
圖表歷史記錄	14
DX 搭配 TGW	16
SD-WAN 裝置與 AWS Transit Gateway 和 AWS Direct Connect 架構整合	16
深入閱讀	17
圖表歷史記錄	17
DX 搭配雲端 WAN	19
SD-WAN 裝置與 AWS Cloud WAN 和 AWS Direct Connect 架構整合	19
深入閱讀	20
圖表歷史記錄	20
.....	xxii

搭配 AWS Transit Gateway Connect Attachments 的 SD-WAN 連線

發佈日期：2024 年 12 月 28 日 ([圖表歷史記錄](#))

此架構說明如何使用 [AWS Transit Gateway](#) Connect 附件將軟體定義的廣域網路 (SD-WAN) 連線至 Transit Gateway，並簡化跨混合雲端環境的路由管理。SD-WAN 前端透過一般路由封裝 (GRE) 通道與 Transit Gateway 對等，允許此設計利用 Transit Gateway 的較高邊界閘道通訊協定 (BGP) 字首限制。此外，透過單一 Transit Gateway Connect 連接，您可以水平擴展連線的頻寬，最高可達 20 Gbps。

與 AWS Transit Gateway Connect 架構的 SD-WAN 連線



下列步驟說明 AWS 到內部部署流量流程：

1. 從 Spoke Amazon [VPC](#) A 中的 Amazon Elastic Compute Cloud 執行個體起始且目的地為公司資料中心的流量，會根據 Spoke VPC A 路由表路由至 Transit Gateway 彈性網路界面 (TGW ENI)。
2. 流量會轉送至 AWS Transit Gateway。根據呼叫 VPC 路由表，流量會透過 Transit Gateway Connect 附件路由至設備 VPC。

3. Transit Gateway Connect 連接使用 Amazon VPC 連接做為傳輸，並使用 GRE 通道和 BGP 將 Transit Gateway 連接到設備 VPC 中的第三方設備。
4. 第三方虛擬設備會封裝流量，使用 SD-WAN 浮水印（在 [AWS Direct Connect](#) 連結上方）來連接公司資料中心。

下列步驟說明內部部署到 AWS 流量流程：

來自 AWS 目的地為 Spoke Amazon VPC B 之外部分支的流量會透過網際網路上的 SD-WAN 浮水印到達設備 VPC 的網際網路閘道。

Connect VPC 中的第三方虛擬設備會透過 Connect 附件將流量轉送至 Transit Gateway。

根據 Transit Gateway Appliance Amazon VPC Route Table，流量會轉送至 Spoke VPC B 附件。

Spoke VPC B 的 Transit Gateway ENI 會將流量轉送至目的地。

如需 AWS Transit Gateway Connect 連接和 SD-WAN 連線的詳細資訊，請參閱[使用 AWS Transit Gateway Connect 簡化 SD-WAN 連線](#)。

深入閱讀

如需詳細資訊，請參閱下列資源：

- [AWS 架構圖示](#)
- [AWS Well-Architected](#)

圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

變更	描述	日期
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

 Note

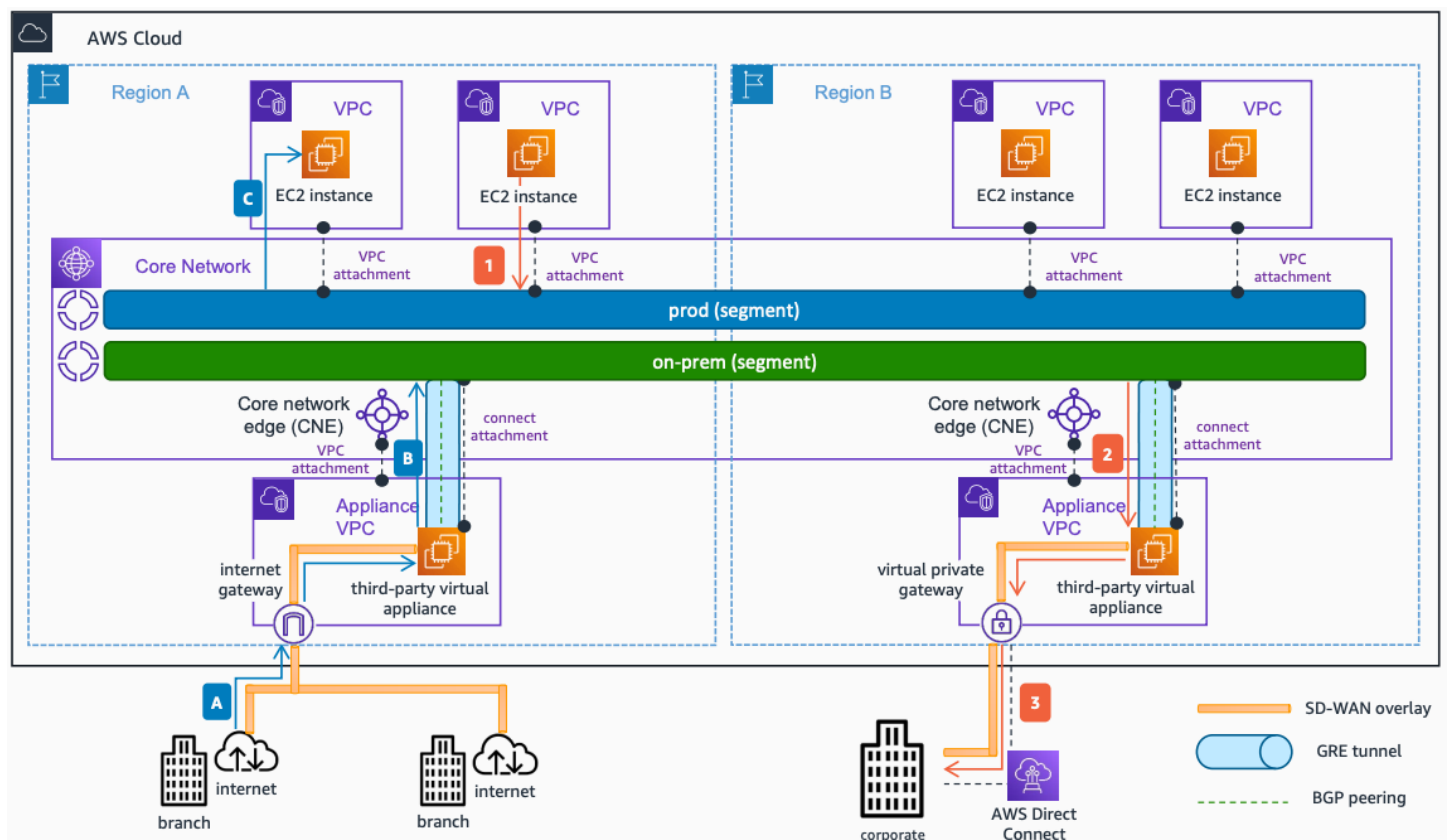
若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

使用 AWS Cloud WAN Connect Attachments 的 SD-WAN 連線能力

發佈日期：2024 年 12 月 28 日 ([圖表歷史記錄](#))

此架構說明如何使用 Connect 附件將 SD-WAN 連線至 AWS Cloud WAN，並簡化跨混合雲端環境的路由管理。SD-WAN 前端透過 GRE 通道與 Cloud WAN 的核心網路邊緣 (CNEs) 對等，允許此設計利用 [AWS Transit Gateway](#) 更高的 BGP 字首限制。此外，透過單一 Transit Gateway Connect 連接，您可以水平擴展連線的頻寬，最高可達 20 Gbps。

使用 AWS Cloud WAN Connect 架構的 SD-WAN 連線



下列步驟說明 AWS 到內部部署流量流程：

1. 從區域 A 中 Amazon [VPC](#) 中的 Amazon Elastic Compute Cloud 執行個體起始且目的地為公司資料中心的流量會轉送至 核心網路。Amazon VPC 連接與 prod 區段相關聯。

2. 根據核心網路政策，到達目的地為公司資料中心之生產客群的流量應轉送至區域 B 中的 Connect 連接。Connect 連接使用 Amazon VPC 連接做為傳輸，並使用 GRE 通道和 BGP 將核心網路連接到設備 Amazon VPC 中的第三方設備。
3. 第三方虛擬設備會封裝流量，使用 SD-WAN 浮水印（在 [AWS Direct Connect](#) 連結上方）來連接公司資料中心。

下列步驟說明內部部署到 AWS 流量流程：

- Na來自 AWS 目的地為區域 A 中 Amazon VPC 之外部分支的流量會透過網際網路上的 SD-WAN 浮水印到達設備 Amazon VPC 的網際網路閘道。
- NaConnect Amazon VPC 中的第三方虛擬設備會透過 Connect 附件將流量轉送至核心網路。Connect 附件與內部部署區段相關聯。
- Na根據 核心網路政策，流量會轉送至對應的 Amazon VPC，並將流量轉送至目的地。

深入閱讀

如需詳細資訊，請參閱下列資源：

- [AWS 架構圖示](#)
- [AWS Well-Architected](#)

圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

變更	描述	日期
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

Note

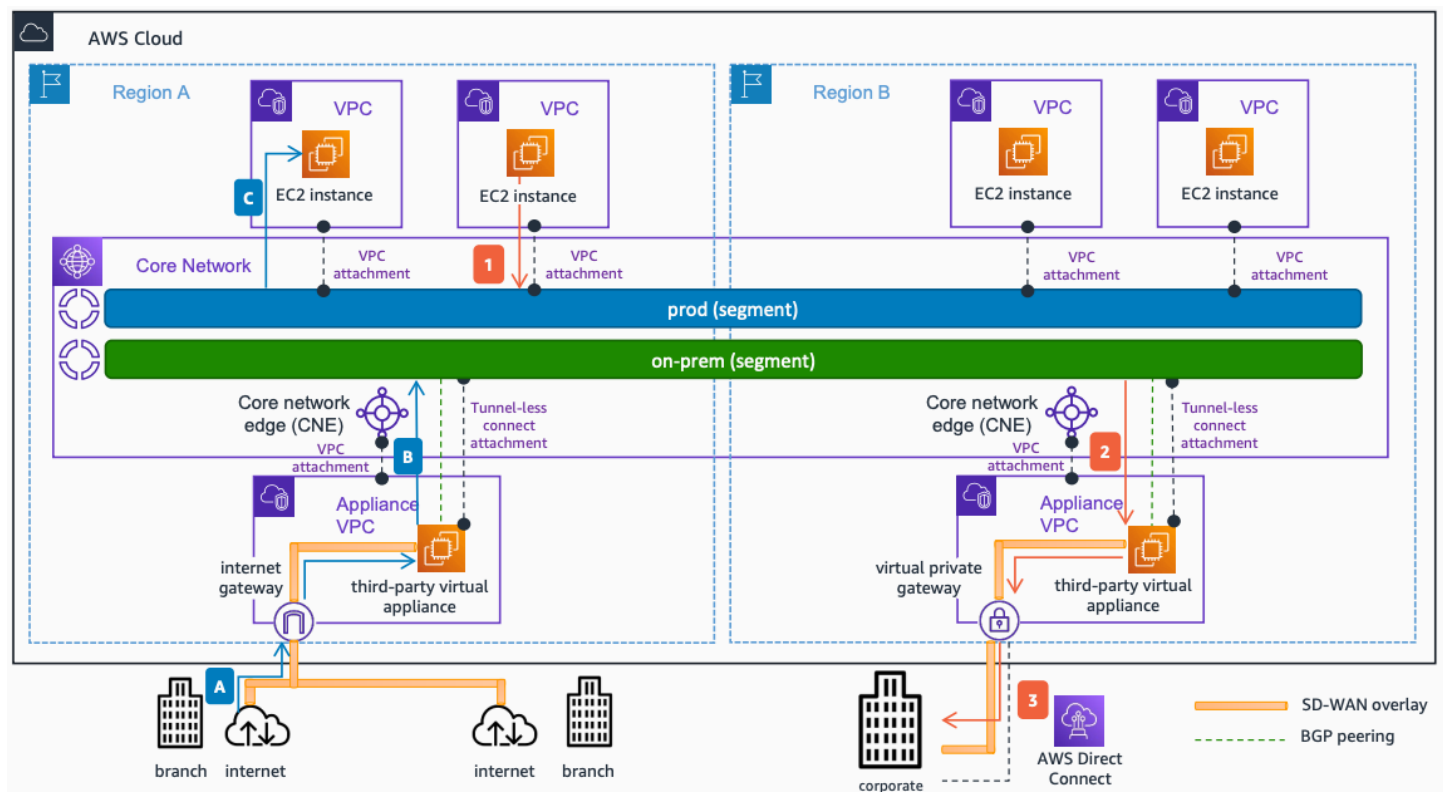
若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

使用 AWS Cloud WAN 無通道連線連接的 SD-WAN 連線

發佈日期：2024 年 12 月 28 日 ([圖表歷史記錄](#))

此架構說明如何使用無通道 Connect 連接，以更簡單且效能更高的方式，使用 AWS 全球網路做為中途傳輸網路，將 SD-WAN 連線至 AWS Cloud WAN。SD-WAN 前端透過 BGP 原生對等 Cloud WAN 的核心網路邊緣 (CNEs)，而不使用 GRE 等特殊通道通訊協定、消除通道額外負荷並改善輸送量效能，這會使用完整的 Amazon VPC 連接頻寬（每個可用區域最多 100 Gbps）。

使用 AWS Cloud WAN Tunnel-less Connect 架構的 SD-WAN 連線



下列步驟說明 AWS 到內部部署流量流程：

1. 從區域 A 中 Amazon [VPC](#) 中的 Amazon Elastic Compute Cloud 執行個體起始且目的地為公司資料中心的流量會轉送至 核心網路。Amazon VPC 連接與 prod 區段相關聯。
2. 根據核心網路政策，到達目的地為公司資料中心之生產客群的流量應轉送至區域 B 中的無通道連線附件。無通道連線附件使用 Amazon VPC 附件做為傳輸，並使用原生 BGP 將核心網路連接至設備 Amazon VPC 中的第三方設備。

3. 第三方虛擬設備會封裝流量，使用 SD-WAN 浮水印（在 [AWS Direct Connect](#) 連結上方）來連接公司資料中心。

下列步驟說明內部部署到 AWS 流量流程：

- 來自 AWS 目的地為區域 A 中 Amazon VPC 之外部分支的流量會透過網際網路上的 SD-WAN 浮水印到達設備 Amazon VPC 的網際網路閘道。
- Connect Amazon VPC 中的第三方虛擬設備會透過無通道 Connect 連接將流量轉送至核心網路。無通道 Connect 連接與內部部署區段相關聯。
- 根據核心網路政策，流量會轉送至對應的 Amazon VPC，並將流量轉送至目的地。

深入閱讀

如需詳細資訊，請參閱下列資源：

- [AWS 架構圖示](#)
- [AWS Well-Architected](#)

圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

變更	描述	日期
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

 Note

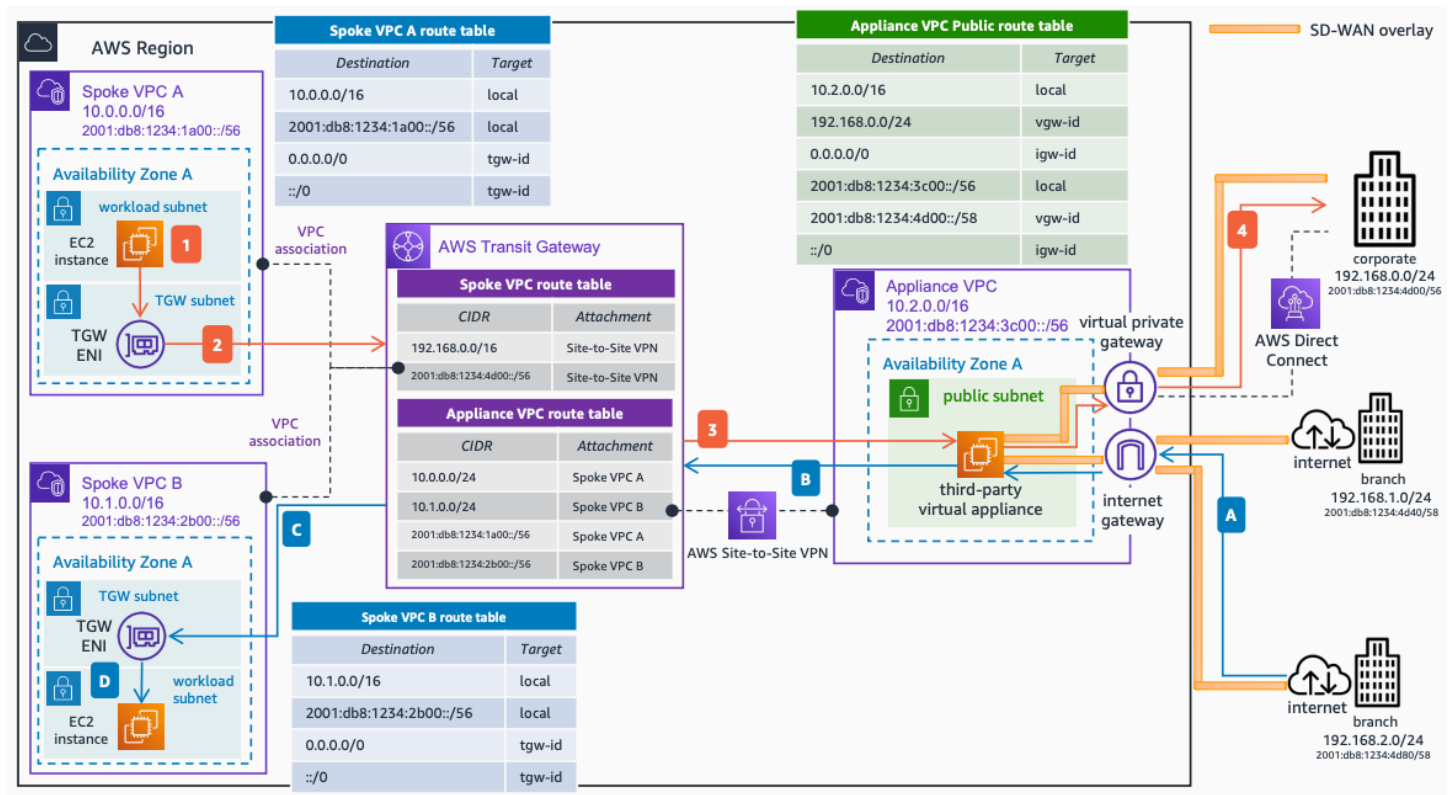
若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

使用 AWS Site-to-Site VPN 連線至 AWS Transit Gateway 的 SD-WAN 連線

發佈日期：2024 年 12 月 28 日 ([圖表歷史記錄](#))

如果您的第三方虛擬設備不支援 GRE，您仍然可以透過建立 AWS Transit Gateway Site-to-Site VPN 連接，使用 IPsec 通道將 SD-WAN 前端與 Transit Gateway 互連，將 SD-WAN 網路整合到 AWS Transit Gateway。SD-WAN 前端可以使用 BGP 與 Transit Gateway 對等來交換路由字首。如果您想要將頻寬增加到超過單一 Site-to-Site VPN 連線的 1.25 Gbps 限制，則額外的 IPsec VPN 連線可以與 Transit Gateway 對等成本多路徑 (ECMP) 的支援搭配使用。

使用 AWS Site-to-Site VPN 連線至 AWS Transit Gateway 架構的 SD-WAN 連線



下列步驟說明 AWS 到內部部署流量流程：

1. 從 Spoke [Amazon VPC](#) A 中的執行個體起始且目的地為公司資料中心的流量，會根據 Spoke VPC A 路由表路由至 TGW ENI。

2. 流量會轉送至 Transit Gateway。根據呼叫 VPC 路由表，流量會透過Site-to-Site VPN 連接路由至設備 VPC。
3. 流量會使用Site-to-Site VPN 連接，在 Transit Gateway 與第三方虛擬設備之間路由。
4. 第三方虛擬設備會封裝流量，使用 SD-WAN 浮水印（在 [AWS Direct Connect](#) 連結上方）來連接公司資料中心。

下列步驟說明內部部署到 AWS 流量流程：

- Na來自 AWS 目的地為 Spoke Amazon VPC B 之外部分支的流量會透過網際網路上的 SD-WAN 浮水印到達設備 VPC 的網際網路閘道。
- Na設備 VPC 中的第三方虛擬設備會透過Site-to-Site連接，將流量轉送至傳輸閘道。
- Na根據 Transit Gateway 設備 VPC 路由表，流量會轉送至 Spoke VPC B 連接。
- NaSpoke VPC B 的 TGW ENI 會將流量轉送至目的地。

深入閱讀

如需詳細資訊，請參閱下列資源：

- [AWS 架構圖示](#)
- [AWS Well-Architected](#)

圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

變更	描述	日期
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

Note

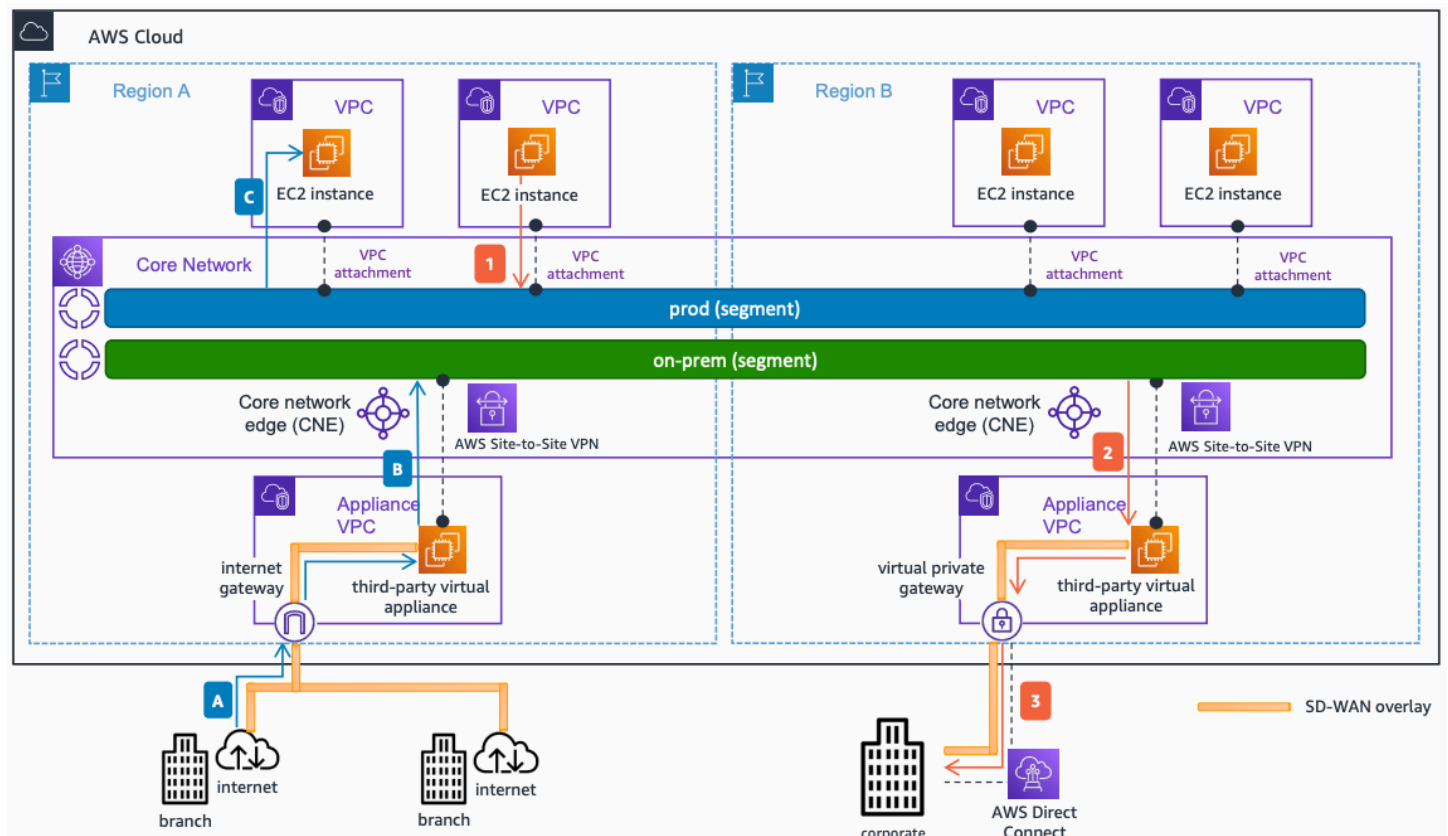
若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

使用 AWS Site-to-Site VPN 到 AWS Cloud WAN 的 SD-WAN 連線能力

發佈日期：2024 年 12 月 28 日 (圖表歷史記錄)

如果您的第三方虛擬設備不支援 GRE，您仍然可以透過建立 AWS Site-to-Site VPN 連接，使用 IPsec 通道將 SD-WAN 前端與 [Transit Gateway](#) 互連，將 SD-WAN 網路整合到 AWS Cloud WAN。SD-WAN 前端可以使用 BGP 與 Transit Gateway 對等來交換路由字首。如果您想要將頻寬增加到超過單一 Site-to-Site VPN 連接的 1.25 Gbps 限制，則額外的 IPsec VPN 連接可以與 Cloud WAN 對等成本多路徑 (ECMP) 的支援搭配使用。

SD-WAN 連線至 AWS Site-to-Site VPN 到 AWS Cloud WAN 架構



下列步驟說明 AWS 到內部部署流量流程：

1. 從區域 A 中 Amazon [VPC](#) 中的 Amazon Elastic Compute Cloud 執行個體起始且目的地為公司資料中心的流量會轉送至 核心網路。Amazon VPC 連接與 prod 區段相關聯。

2. 根據 核心網路政策，到達目的地為公司資料中心之生產區段的流量應轉送至區域 B Site-to-Site VPN 連接。流量會使用Site-to-Site VPN 連接，在核心網路與第三方虛擬設備之間路由。
3. 第三方虛擬設備會封裝流量，使用 SD-WAN 浮水印（在 [AWS Direct Connect](#) 連結上方）來連接公司資料中心。

下列步驟說明內部部署到 AWS 流量流程：

- Na來自 AWS 目的地為區域 A 中 Amazon VPC 之外部分支的流量會透過網際網路上的 SD-WAN 浮水印，到達該區域中設備 VPC 的網際網路閘道。
- Na設備 VPC 中的第三方虛擬設備會透過Site-to-Site連接將流量轉送至核心網路。
- Na根據 核心網路政策，流量會轉送至對應的 Amazon VPC，並將流量轉送至目的地。

深入閱讀

如需詳細資訊，請參閱下列資源：

- [AWS 架構圖示](#)
- [AWS Well-Architected](#)

圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

變更	描述	日期
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

[初次出版](#)

首先發佈參考架構圖。

2024 年 12 月 28 日

 Note

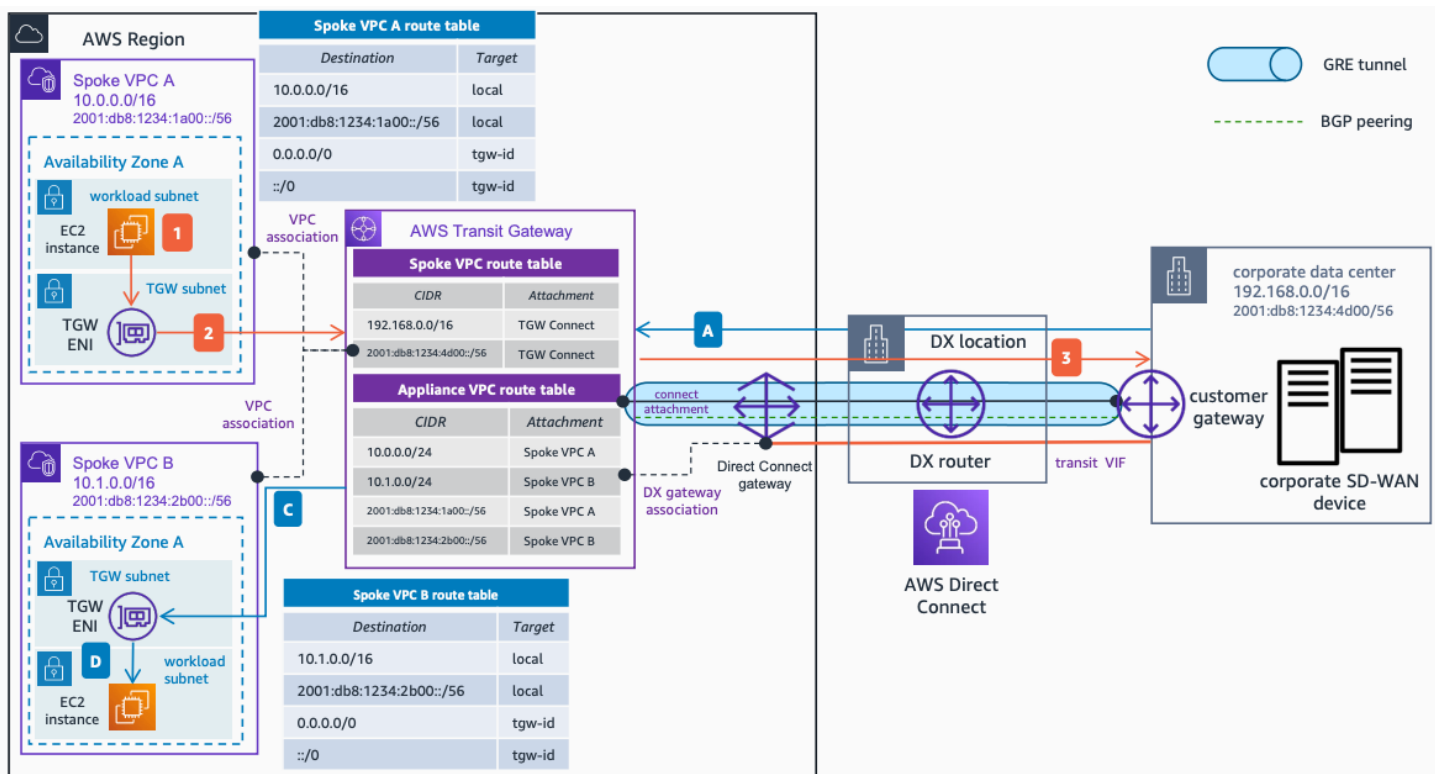
若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

SD-WAN 裝置與 AWS Transit Gateway 和 AWS Direct Connect 整合

發佈日期：2024 年 12 月 28 日 ([圖表歷史記錄](#))

此架構說明如何使用 [AWS Transit Gateway Connect](#) 連接和 [AWS Direct Connect](#) 將您的 SD-WAN 流量擴展和分段至 AWS 而無需新增額外的基礎設施。每個 Transit Gateway Connect 對等可以有自己的 Transit Gateway Route Table 和 BGP 對等，以在必要時擴展內部部署 VRF。

SD-WAN 裝置與 AWS Transit Gateway 和 AWS Direct Connect 架構整合



下列步驟說明 AWS 到內部部署流量流程：

1. 從 Spoke [Amazon VPC](#) A 中的執行個體起始且目的地為公司資料中心 SD-WAN 裝置的流量，會根據 Spoke Amazon VPC A Route Table 路由至 TGW ENI。
2. 流量會轉送至 Transit Gateway。根據呼叫 VPC 路由表，流量會透過 Transit Gateway Connect 連接路由至公司資料中心。

3. Transit Gateway Connect 連接使用 Direct Connect 連線做為傳輸，並使用 GRE 通道和 BGP 將 Transit Gateway 連接到公司資料中心 SD-WAN 裝置。

下列步驟說明內部部署到 AWS 流量流程：

- 來自目的地為 Spoke VPC B 之公司資料中心 SD-WAN 裝置的流量會透過 Transit Gateway 附件的 GRE 通道，透過 Direct Connect 連結轉送至 Transit Gateway。
- 根據 Transit Gateway Connect 路由表，流量會轉送至 Spoke VPC B 連接。
- Spoke VPC B 的 TGW ENI 會將流量轉送至目的地。

如需如何使用 AWS Transit Gateway 和 AWS Direct Connect 整合內部部署 SD-WAN 裝置的詳細資訊，請參閱[整合 SD-WAN 裝置與 AWS Transit Gateway 和 AWS Direct Connect](#)。

深入閱讀

如需詳細資訊，請參閱下列資源：

- [AWS 架構圖示](#)
- [AWS Well-Architected](#)

圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

變更	描述	日期
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

[初次出版](#)

首先發佈參考架構圖。

2024 年 12 月 28 日

 Note

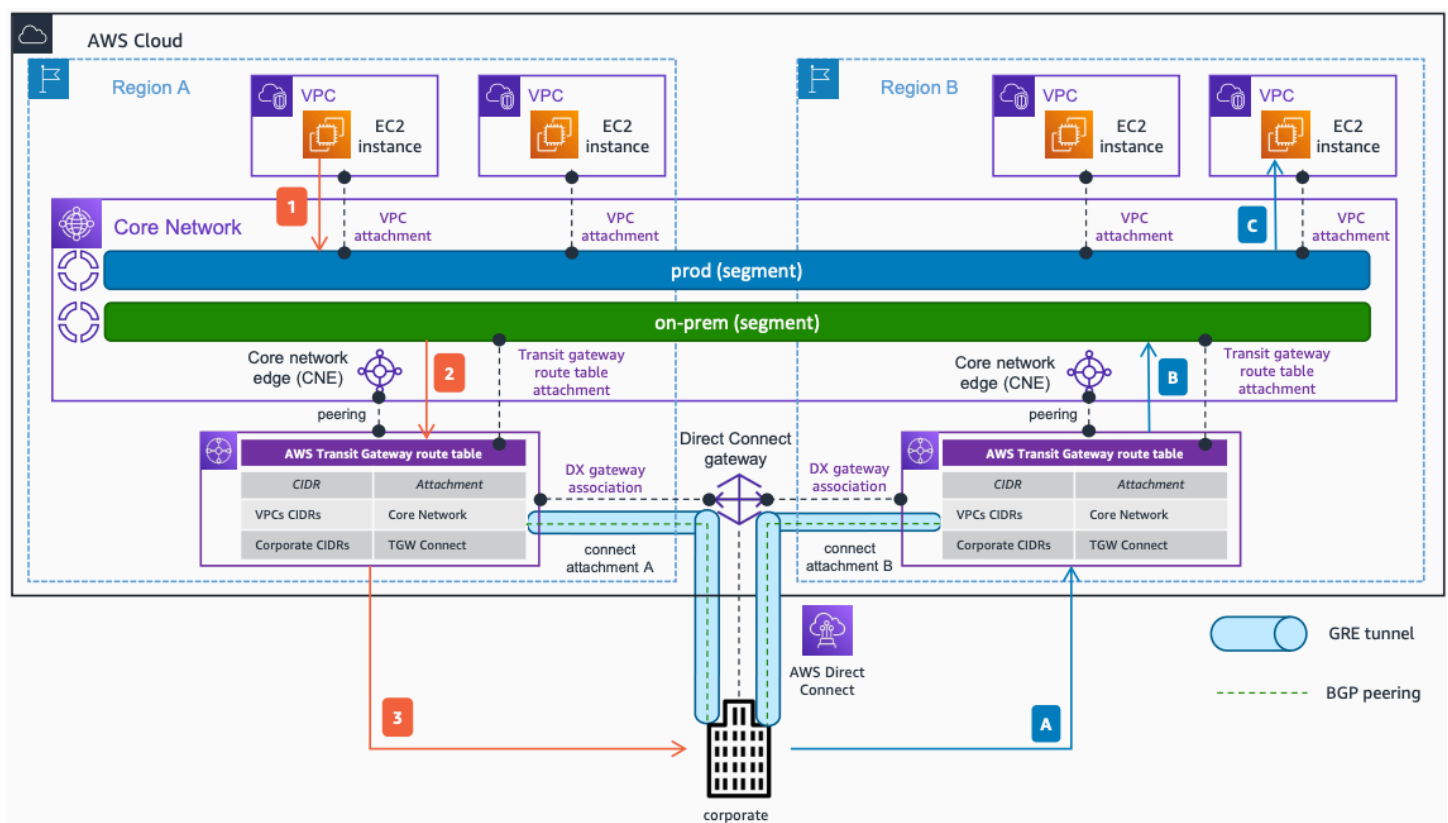
若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

SD-WAN 裝置透過 AWS Transit Gateway 與 AWS 雲端 WAN 和 AWS Direct Connect 整合 AWS Transit Gateway

發佈日期：2024 年 12 月 28 日 ([圖表歷史記錄](#))

透過 AWS [AWS Direct Connect](#) to AWS Cloud WAN 將 SD-WAN 流量擴展至時，您可以使用 [AWS Transit Gateway](#) Connect 連接和 Cloud WAN 和 Transit Gateway 之間的對等互連，以實現end-to-end 動態路由。您可以使用不同的 Transit Gateway Connect 對等和路由表，以及 Cloud WAN 路由表連接和區段，在內部部署環境中擴展每個 VRF。

SD-WAN 裝置與 AWS Cloud WAN 和 AWS Direct Connect 架構整合



下列步驟說明 AWS 到內部部署流量流程：

1. 從區域 A 中 [Amazon VPC](#) 中的執行個體起始且目的地為公司資料中心 SD-WAN 裝置的流量會轉送至核心網路。Amazon VPC 連接與 prod 區段相關聯。

2. 根據 核心網路政策，到達目的地為公司資料中心之生產客群的流量應轉送至 Transit Gateway 路由表附件。會偏好本機附件。流量會轉送至區域 A 中的 AWS Transit Gateway。
3. 根據 Transit Gateway 路由表，流量將透過 Transit Gateway Connect 連接 A 轉送。此連接使用 Direct Connect 連接作為傳輸，並使用 GRE 通道和 BGP 將 Transit Gateway 連接到公司資料中心 SD-WAN 裝置。

下列步驟說明內部部署到 AWS 流量流程：

- Na來自目的地為區域 B 中 Amazon VPC 的公司資料中心 SD-WAN 裝置的流量會透過 Transit Gateway Connect 附件 B，透過 Direct Connect 連結轉送至區域 B 中的 Transit Gateway。
- Na根據 Transit Gateway 路由表，流量會轉送至 核心網路。Transit Gateway 路由表附件與內部部署區段相關聯。
- Na核心網路會將流量轉送至對應的 Amazon VPC。

深入閱讀

如需詳細資訊，請參閱下列資源：

- [AWS 架構圖示](#)
- [AWS Well-Architected](#)

圖表歷史記錄

若要收到此參考架構圖的更新通知，請訂閱 RSS 摘要。

變更	描述	日期
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日
初次出版	首先發佈參考架構圖。	2024 年 12 月 28 日

Note

若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

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。