Cloud VPN（虛擬私有網路）

Cloud VPN 通過IPsec VPN連接，將您的對等網絡安全地連接到Virtual Private Cloud (VPC) 網絡。兩個網絡之間傳輸的流量由一個VPN 網關加密，再由另一個VPN 網關解密。此操作可以保護您的數據在互聯網上傳輸時的安全。您還可以將兩個Cloud VPN 實例相互連接。

- 高可用性VPN
- 傳統VPN

主要功能與特色

選擇合適的虛擬私有網路類型

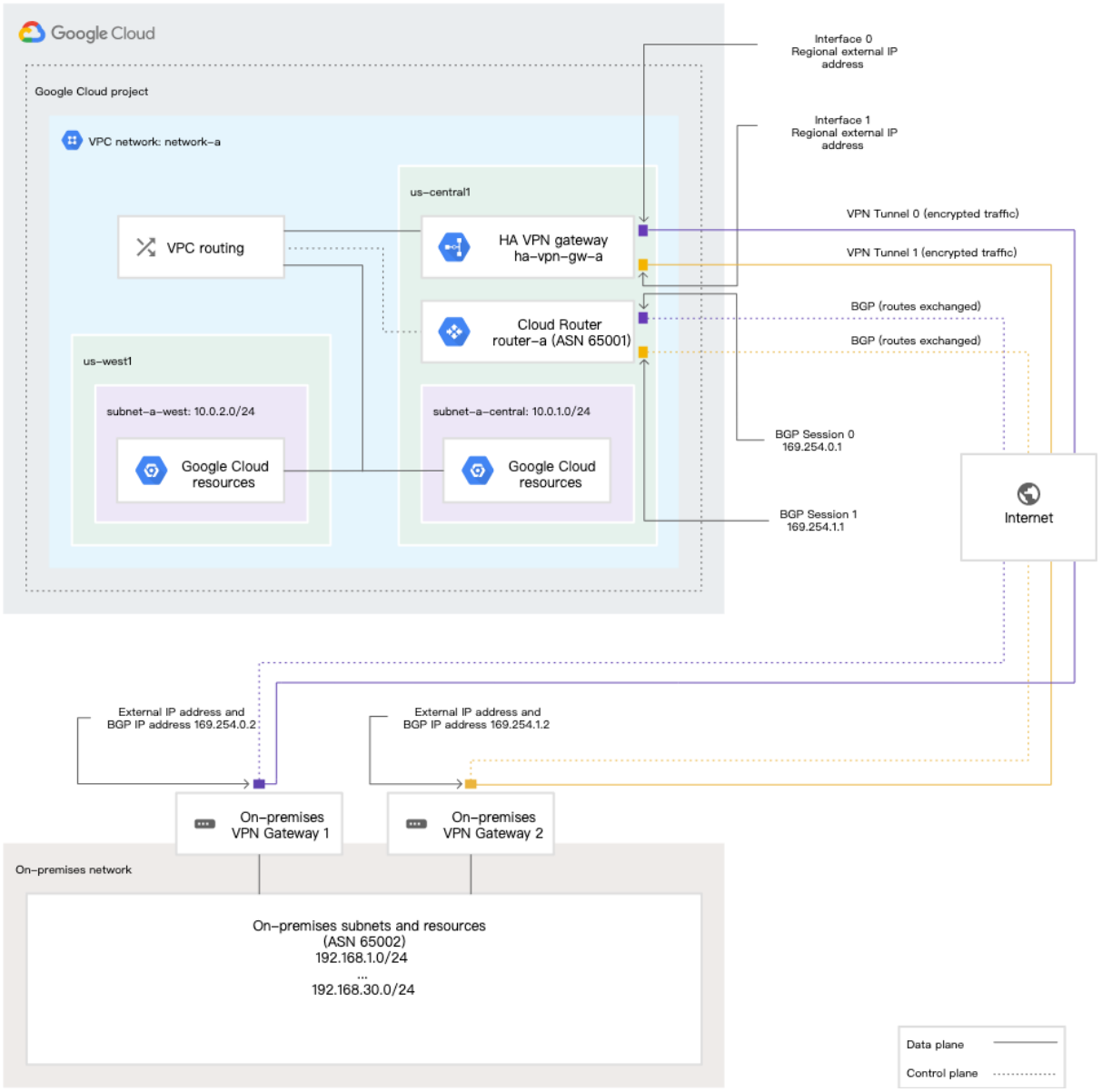
高可用性VPN

高可用性VPN 是一種高可用性(HA) Cloud VPN 解決方案，可讓您在單個地區中通過IPsec VPN 連接將您的本地網絡安全地連接到VPC 網絡。高可用性VPN 提供服務可用性達99.99% 的服務等級協議(SLA)。

創建高可用性VPN 網關時，Google Cloud 會自動選擇兩個外部IPv4 地址，兩個固定數量的接口各對應一個地址。每個IPv4 地址都是從唯一地址池中自動選取的，以支持高可用性。每個高可用性VPN 網關接口都支持多個隧道。您也可以創建多個高可用性VPN 網關。刪除高可用性VPN 網關時，Google Cloud 會釋放IP 地址以供重複使用。您可以將高可用性VPN 網關配置為只有一個活動接口和一個外部IP 地址；但是，此配置不會提供服務可用性達到99.99% 的SLA。

高可用性VPN 支持在預覽版中交換IPv6 流量。

高可用性VPN串接示意圖：

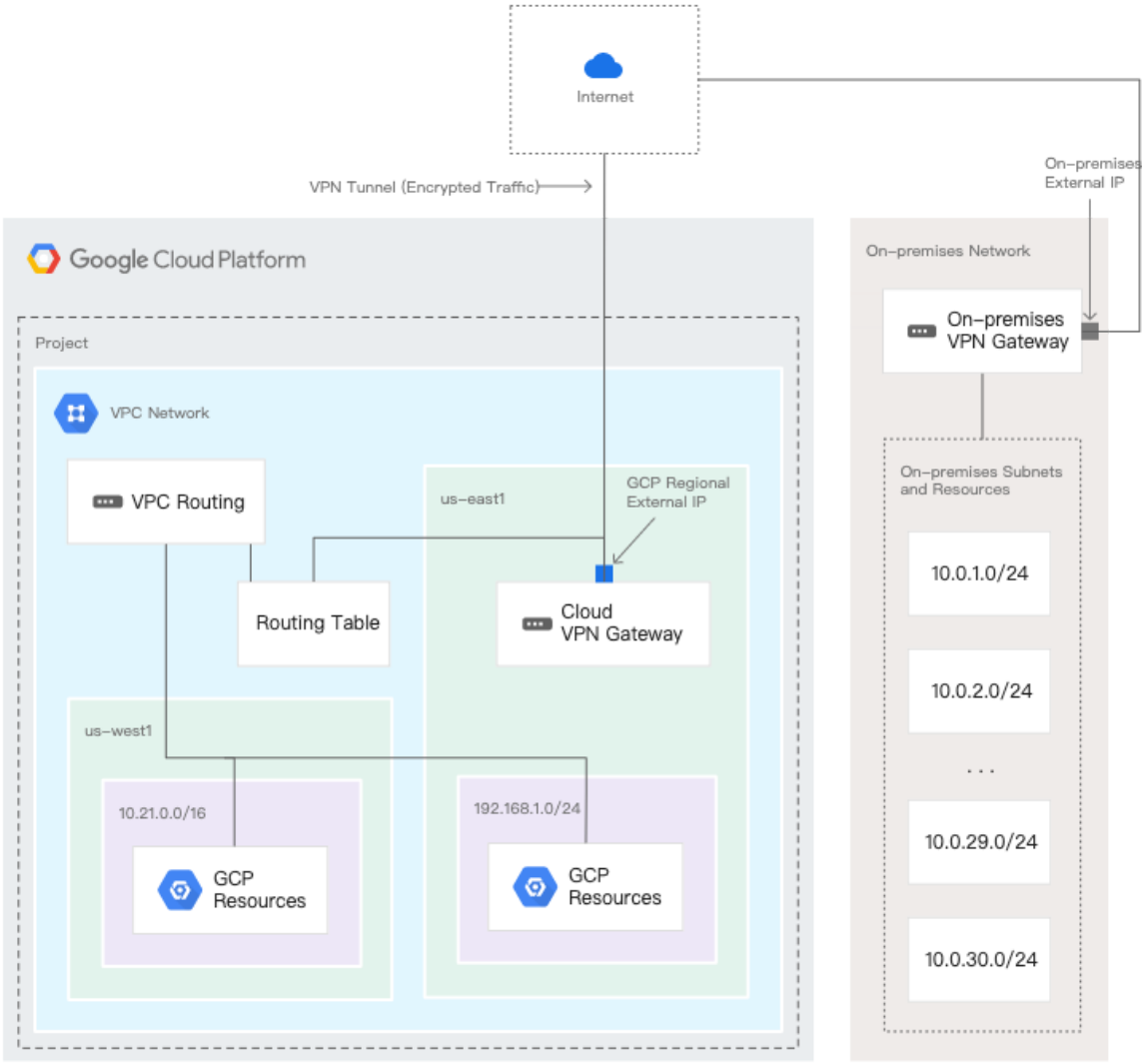


傳統VPN

相比高可用性VPN，傳統VPN 網關具有單個接口、單個外部IP 地址，並支持使用靜態路由（基於政策或基於路由）的隧道。您還可以為傳統VPN 配置動態路由(BGP)，但僅適用於連接到Google Cloud 虛擬機實例上運行的第三方VPN 網關軟件的隧道。

傳統VPN 網關提供服務可用性達99.9% 的服務等級協議(SLA)。

傳統VPN串接示意圖：



用途

選擇合適的虛擬私有網路類型

下表比較了高可用性VPN 功能與傳統VPN 功能，根據不同場景及需求，選擇適用的虛擬私有網路。

	高可用性**VPN**	傳統**VPN**

服務等級協議	在配置了兩個接口和兩個外部IP 地址時，可提供99.99% 的SLA。	提供了99.9% 的SLA。
創建外部IP 地址和轉發規則	從池創建的外部IP 地址；無需轉發規則。	必須創建外部IP 地址和轉發規則。
支持的路由選項	僅限動態路由(BGP)。	靜態路由（基於政策、基於路由）。只有連接到Google Cloud 虛擬機實例上運行的第三方VPN 網關軟件的隧道才支持動態路由。
從一個Cloud VPN 網關到相同對等網關的兩條隧道	支持	不支持
API 資源	稱為 vpn-gateway 資源。	稱為 target-vpn-gateway 資源。
IPv6 流量	在預覽版（雙棧IPv4 和IPv6 配置）中受支持	不支持

所有功能與特色

支援類型	Cloud VPN 僅支持站點到站點的IPsec VPN 連接，具體取決於本部分中列出的要求。它不支持客戶端到網關的方案。換句話說，Cloud VPN 不支持客戶端計算機需要使用客戶端VPN 軟件“撥號加入”VPN 的使用場景。
允許流量	傳統VPN 和高可用性VPN 網關使用外部（可通過互聯網路由）IPv4 地址。這些地址僅允500 和UDP 4500 流量。此規則既適用於為傳統VPN 手動配置的Cloud VPN 地址，也適性VPN 自動分配的IP 地址。
網路帶寬	每個Cloud VPN 隧道最多可支持3 Gbps 的入站流量和出站流量總和。 如果您已與Google 建立直接對等互連關係，則相較於通過公共互聯網發送VPN 流量，此吞吐量更高。 VPN 隧道利用率Recommender 會在利用率達到這些上限值的80% 時生成建議，以便您在達到上限之前添加新的VPN 隧道。

隧道MTU	Cloud VPN 使用的MTU 始終為1460 字節。如果隧道任一端的虛擬機和網絡具有更高的MTU，則Cloud VPN 會使用“MSS 固定”將TCP MTU 設置減少到1460。VPN 網關還可以使用ICMP 錯誤消息來啟用路徑MTU 發現(PMTUD)，從而將UDP 數據包的MTU 設置為較低。
支援IPv6	可以創建高可用性VPN 網關和隧道，用於將啟用IPv6 的VPC 網絡與其他啟用IPv6 的網絡連接起來。這些網絡可以是本地網絡、多云網絡或其他VPC 網絡。如需在高可用性VPN 隧道中傳輸IPv6 流量，啟用IPv6 的VPC 網絡必須包含雙棧子網。此外，您還必須為子網分配內部IPv6 範圍。
支援IPsec 和IKE	Cloud VPN 使用IKE 預共享密鑰（共享密鑰令牌）和IKE 加密支持IKEv1和IKEv2。Cloud VPN 僅支持用於身份驗證的預共享密鑰。創建Cloud VPN 隧道時，請指定預共享密鑰。在對等網關上創建隧道時，請指定相同的預共享密鑰。
高可用性 VPN 的主動/主動和主動/被動路由選項	連接到高可用性VPN 網關的VPN 隧道必須使用動態(BGP) 路由。您可以創建主動/主動或主動/被動路由配置，具體取決於您為高可用性VPN 隧道配置路由優先級的方式。對於這兩種路由配置，兩個VPN 隧道都會保持活躍狀態。
對等IP 地址	如果您是Organization Policy Administrator，則可以創建政策限制條件來限制用戶可以為對等VPN 網關指定的IP 地址。 該限制會應用於特定項目、文件夾或組織中的所有Cloud VPN 隧道，適用於傳統VPN 和高可用性VPN。
直觀呈現和監控虛擬私有網路	網絡拓撲是一種可視化工具，可顯示VPC 網絡的拓撲、與本地網絡的混合連接以及相關指標。您可以在網絡拓撲視圖中將Cloud VPN 網關和VPN 隧道視為實體。 基礎實體是特定層次結構的最低級層，表示可以通過網絡直接與其他資源進行通信的資源。網絡拓撲會將基礎實體聚合到可以展開或折疊的分層實體中。首次查看網絡拓撲圖時，它會將所有基礎實體聚合到其頂級層次結構中。
維護和可用性	Cloud VPN 會自動定期進行維護。維護期間，Cloud VPN 隧道將離線，會導致網絡流量短暫下降。維護完成後，Cloud VPN 隧道會自動重新建立。 Cloud VPN 維護是一項正常的操作任務，可能隨時發生，恕不事先通知。維護週期設計得足夠短，所以不會影響Cloud VPN 服務等級協議(SLA)。
日誌和指標	Cloud VPN 網關會將日誌信息發送給Cloud Logging，Cloud VPN 隧道會將監控指標發送給Cloud Monitoring。本頁面介紹日誌和指標及其查看方式。