IWAN和PfRv3簡介

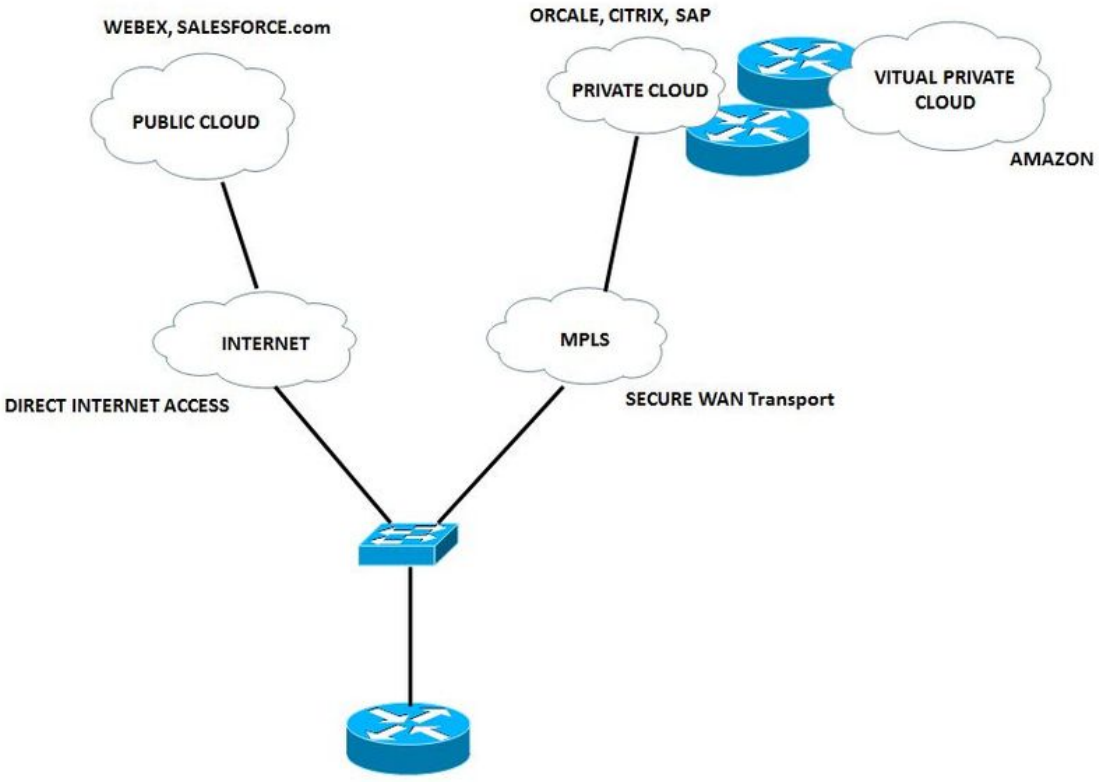
目錄

簡介

本檔案介紹思科智慧廣域網(IWAN)和思科效能路由(PfR)。

IWAN

思科IWAN是一個增強合作和雲應用效能的系統，同時也降低了廣域網的運營成本。IWAN解決方案為尋求部署獨立於傳輸的WAN的組織提供了設計和實施指南，IWAN具有智慧路徑控制、應用最佳化以及到Internet和分支機構位置的安全連線，同時還能降低WAN的運營成本。IWAN充分利用優質廣域網和經濟高效的網際網路服務來增加頻寬容量，而不會影響合作或基於雲的應用的效能、可靠性或安全性。組織可以使用IWAN將網際網路作為WAN傳輸方式，並直接訪問公共雲應用。



R1將優先使用語音和影片流量，以便在可用的兩條鏈路之間使用相對較少的延遲、抖動和/或丟失。其他流量進行負載均衡，以便最大化頻寬。

如果當前路徑降級(多協定標籤交換(Multiprotocol Label Switching，MPLS))，則會重新路由語音和影片，然後選擇直接網際網路接入(DIA)鏈路。

IWAN允許您：

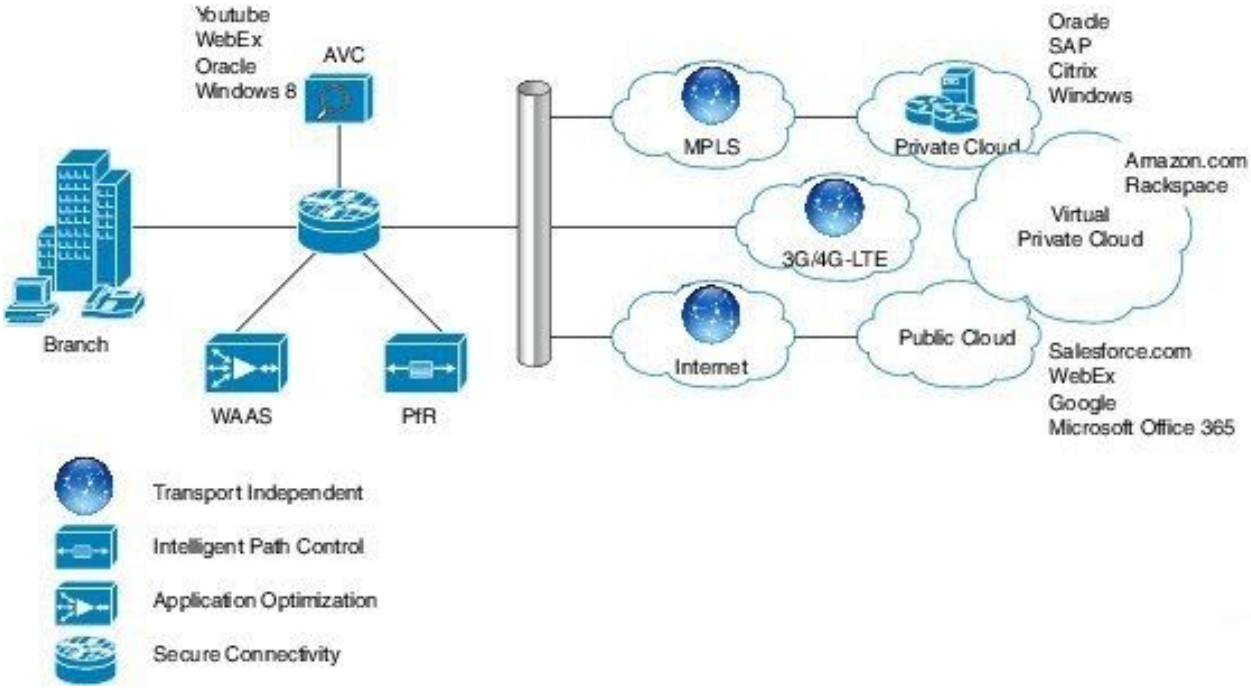
- 連線到成本較低的模式，如網際網路，獲取不太重要的資料。
- 允許廣域網使用應用最佳化、智慧快取和高度安全的DIA。

到目前為止，獲得具有可預測效能的可靠連線的唯一方法是利用MPLS或租用線路服務的專用WAN。但是，基於運營商的MPLS和租用線路服務可能非常昂貴，而且對於組織來說，用於廣域網傳輸以支援遠端站點連線不斷增長的頻寬要求並不總是經濟划算。組織尋求降低運營預算，同時為遠端站點提供充足的網路傳輸的方法。

IWAN使組織能夠通過任何連線提供不折不扣的體驗。藉助Cisco IWAN，IT組織可以使用更便宜的WAN傳輸選項為其分支機構連線提供更多頻寬，而不影響效能、安全性或可靠性。藉助IWAN解決方案，可以根據應用服務級別協定(SLA)、終端型別和網路條件動態路由流量，以提供最佳品質體驗。

藉助IWAN，您可以快速部署頻寬密集型應用，例如影片、虛擬案頭基礎設施(VDI)和訪客Wi-Fi服務。而且無論您選擇哪種傳輸模式，無論是MPLS、網際網路、蜂窩網路還是混合廣域網接入模式，都無關緊要。

本圖概述了IWAN解決方案的元件。績效路徑是此計畫的關鍵支柱：



IWAN的四個元件是：

- **安全且靈活的傳輸無關設計** — Dynamic Multipoint VPN(DMVPN)IWAN提供通過任何運營商服務產品（包括MPLS、寬頻和蜂窩3G/4G/LTE）輕鬆實現多歸屬的功能。 技術：DMVPN/IPsec重疊設計
- **智慧路徑控制** — 藉助Cisco PfR，此元件可提高應用交付和WAN效率。PfR通過檢視應用型別、效能、策略和路徑狀態來動態控制資料包轉發決策。PfR可保護業務應用免受廣域網效能波動的影響，同時根據應用策略在最佳效能路徑上智慧地負載均衡流量。PfR監控網路效能（抖動、丟包、延遲），並根據應用策略做出通過最佳效能路徑轉發關鍵應用的決策。Cisco PfR包括連

線到寬頻服務的邊界路由器，以及路由器上Cisco IOS®軟體支援的主要控制器應用。邊界路由器收集流量和路徑資訊並將其傳送到主控制器，主控制器檢測並實施服務策略以滿足應用要求。Cisco PfR可以根據電路成本選擇出口WAN路徑來智慧地負載均衡流量，從而降低公司的整體通訊費用。IWAN智慧路徑控制是通過Internet傳輸提供企業級廣域網的關鍵。 技術：PfR。PfR演變為一個稱為PfRv3的主要新版本。

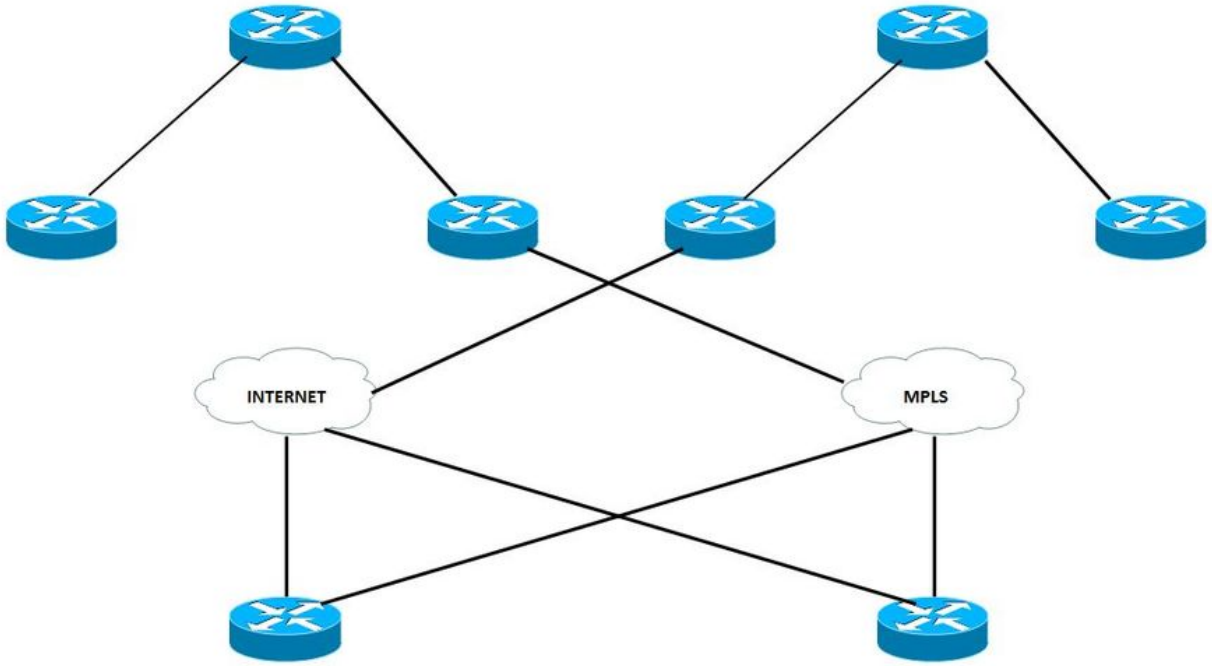
- **應用最佳化 —** 思科應用可視性與可控性(AVC)和思科廣域應用服務(WAAS)提供廣域網上的應用效能可視性和最佳化。隨著應用程式由於對公認埠(如HTTP（埠80）的重複使用而變得越來越不透明，應用程式的靜態埠分類已不再足夠。Cisco AVC通過深度資料包流量檢測提供應用感知，以識別和監控應用效能。通過AVC技術(如基於網路的應用識別2(NBAR2)、NetFlow、服務品質(QoS)、效能監控、Medianet等)提供應用級別（第7層）的可視性和控制能力。 技術:應用可視性與可控性(AVC)、WAAS、Akamai Connect

- **安全連線 —** 它可保護WAN，並將使用者流量直接解除安裝到Internet。使用強IPsec加密、基於區域的防火牆和嚴格的訪問清單來保護公共網際網路上的WAN。將分支機構使用者直接路由到網際網路可提高公共雲應用效能，同時減少廣域網流量。思科雲端網路安全(CWS)服務提供基於雲的Web代理，以集中管理和保護訪問網際網路的使用者流量。 技術:Cisco IOS防火牆/IPS、雲端網路安全(CWS)

為什麼使用DMVPN

IWAN採用規範化設計，並基於DMVPN採用獨立於混合傳輸的設計。DMVPN部署在MPLS和網際網路傳輸中。這通過使用包含兩個傳輸的單個路由域來大大簡化路由。DMVPN路由器使用支援IP單播以及IP組播和廣播流量的隧道介面，其中包括使用動態路由協定。初始分支到中心隧道處於活動狀態後，當站點到站點IP流量需要時，可以建立動態分支到分支隧道。

獨立傳輸設計基於每個提供商一個DMVPN雲。本指南使用兩個提供商，一個提供商被認為是主要(MPLS)，另一個提供商被認為是輔助（網際網路）。 分支站點連線到兩個DMVPN雲，並且兩個隧道均已啟用。



如圖所示，每個分支機構路由器都連線到兩個提供商，一個是MPLS（主要），另一個是INTERNET（輔助）。

根據流量的型別，每個提供程式都用於傳送流量。例如，高優先順序的資料可以通過MPLS傳送，低優先順序的資料可以通過INTERNET路由。這使它更具成本效益，並釋放可用資源，以用於更具創新性的業務目的。

獨立於傳輸的設計（雙DMVPN）

設計摘要

此設計提供主動 — 主動WAN路徑，可充分利用DMVPN實現一致的IPsec覆蓋。MPLS和網際網路連線可在單個路由器上終止，或在兩個獨立的路由器上終止，以實現額外的恢復能力。相同的設計可以通過MPLS、網際網路或3G/4G傳輸使用，這使得設計獨立於傳輸。

建議按照提供商使用DMVPN集線器(PfRv3 BR)並在集線器上進行傳輸。這使得路由配置更加簡單。

DMVPN要求使用網際網路金鑰管理協定第2版(IKEv2)保持連線間隔進行失效對等項檢測(DPD)，這對於加快重新收斂和使分支註冊在DMVPN中心重新載入的情況下能夠正常工作至關重要。此設計使分支可以檢測加密對等體已失敗以及與該對等體的IKEv2會話已過時，然後允許建立新的會話。如果沒有DPD，IPsec SA必須超時（預設值為60分鐘），並且當路由器無法重新協商新的SA時，將啟動新的IKEv2會話。最大等待時間大約為60分鐘。

DMVPN階段摘要

DMVPN有多個階段，概述如下：

DMVPN第1階段基於集中星型功能。

- 集線器上的配置簡化且更小
- 支援動態定址的CPE(NAT)
- 支援路由協定和組播
- 輻條不需要完整的路由表，可以在集線器上彙總

DMVPN第2階段在集線器上沒有彙總。

每個分支都有每個分支目標字首的下一跳（分支地址）。

PfR具有使用動態PBR實施路徑的所有資訊和正確的下一跳資訊。

DMVPN第3階段允許路由彙總：

- 當執行父路由查詢時，只有通往集線器的路由可用。
- NHRP動態安裝快捷隧道，因此填充RIB/CEF。
- PfR仍具有中心下一跳資訊，目前不知道下一跳更改。

PfRv3支援所有DMVPN階段。

有關DMVPN的詳細資訊，請參閱Cisco IOS DMVPN概述。