使用 VMware SD-WAN 實現企業廣域網路簡易性、效能和安全性

vmware SD-WAN™

VMware SD-WAN 可提高靈活性和成本效益，同時確保應用程式效能，以及企業站點在整體廣域網路中的網路安全性。

隨著企業尋求提高靈活性和經濟效益，以及配合應用程式移轉到雲端的趨勢，廣域網路正處於轉變時期。VMware SD-WAN™ 可在公用網際網路和私有網路上，提供企業級的效能、安全性、能見度和控制能力。VMware SD-WAN 備有零接觸部署、一鍵式業務原則、增強型防火牆服務、簡單的服務增強，以及雲端式網路即服務，能大幅簡化廣域網路。如此即能造就可靠度更高且效能更出色的廣域網路，不僅能降低成本，也能為分公司和遠端使用者提升安全性。

為了進行線上協同作業 (例如 Zoom、WebEx 和 Microsoft 365)、使用軟體即服務 (SaaS) 和雲端服務、存取大型豐富媒體檔案，以及使用其他需要大量頻寬的應用程式，現行分公司使用者的廣域網路 (WAN) 頻寬用量，正不斷向上攀升。 現有廣域網路的架構複雜性、缺乏安全性，以及成本考量，也為企業 IT 帶來了眾多嚴峻挑戰。

多數分公司的廣域網路流量，都會經由昂貴的租用線路 (例如私有 MPLS 線路)，或是難以預測且不安全的網際網路連線 (例如 DSL、纜線和 LTE) 傳輸，但這兩者其實都不甚理想。部署租用線路來滿足頻寬需求不僅成本驚人，也需耗費很多時間。使用公用網際網路，則可能因缺乏穩定性和網路攻擊防禦能力等緣故，導致使用者體驗不佳。雪上加霜的是，傳統廣域網路含有許多安全性隱憂。

VMware SD-WAN 可協助企業支援數量不斷增加的應用程式、簡化的分公司實作、網路和員工靈活性，以及強化的網路安全性。除了提供最佳化的存取方式，以透過各類型的傳輸機制同時存取雲端服務、私有資料中心和企業應用程式，VMware SD-WAN 也能藉由單一統一管理入口網站，運用增強型防火牆服務、入侵偵測系統和入侵防禦系統 (IDS/IPS)、代管防火牆日誌記錄，以及其他多項功能，著手降低網路攻擊風險。

分公司廣域網路所面臨的挑戰

當今大多數分公司使用的廣域網路技術，在最近幾十年可說幾乎沒有什麼變化。這些技術原先適用的對象，為位於私有、地端資料中心的應用程式。時至今日，傳統分公司廣域網路架構正面臨許多網路與安全性挑戰。常見的幾項挑戰包括：

- 一般來說，MPLS 可以提供很好的服務品質，但代價是受到容量限制，且成本較高，部署的前置時間也較長。僅透過私有線路連線的分公司，必須仰賴經由企業資料中心回傳所有雲端應用程式、軟體即服務與網際網路流量，這不僅造成延遲情況惡化、降低應用程式效能，還會讓網路頻寬成本不斷攀升。而傳統的軸輻式廣域網路架構，可能無法支援雲端移轉。
- 頻寬能提供快速部署與更多的容量，但可能缺乏可靠性、安全性和效能保證，因而造成使用者體驗不良。
- 傳統分公司網路缺乏集中的管理、控制、能見度和網路威脅防護措施。琳瑯滿目的管理工具，可能提高疑難排解或快速回應威脅的難度。
- 由於不同的安全性解決方案出自不同廠商之手，跨越多個分公司維護合規需求 (例如 PCI、HIPAA 和 GDPR 等) 往往窒礙難行。

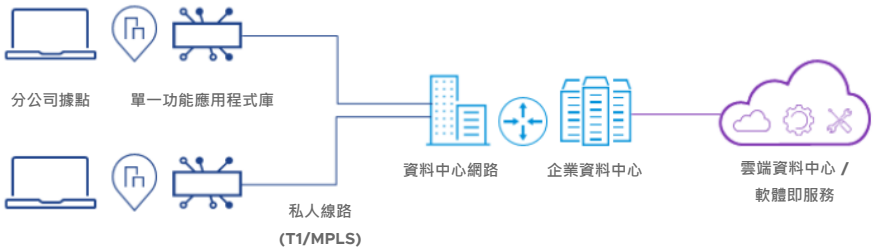

圖 1：傳統分公司廣域網路

VMware SD-WAN 概觀

VMware SD-WAN 以雲端式服務的部署速度和低維護需求，提升混合廣域網路的經濟效益和彈性。這包括原則式全網路應用程式效能、能見度和控制力，以及從雲端向分公司提供虛擬化服務，因此可大幅簡化廣域網路。

VMware SD-WAN Edge 應用裝置是一款精簡的邊緣裝置，從雲端進行零接觸佈建，提供安全且最佳化的應用程式與資料連線。VMware SD-WAN Edge 也可做為在客戶端設備 (CPE) 平台上具體化的虛擬網路功能 (VNF)，帶來更出色的部署彈性。

VMware SD-WAN Edge 使用 Dynamic Multipath Optimization™ (DMPO) 以及深度應用程式辨識功能，提升交付可靠性。 其彙總多種連結 (例如私有線路、纜線、DSL、4G-LTE 或 5G、衛星)，並將流量導引到最佳連結上，傳輸至分公司、私有資料中心、公司園區與總部的其他地端 VMware SD-WAN Edge。 VMware SD-WAN Edge 也可選擇連接到全域 VMware SD-WAN Gateway 系統，為雲端服務 (軟體即服務、基礎架構即服務、B2B 網際網路) 提供效能、安全性和能見度。

Edge 內建的增強型防火牆服務採用 VMware NSX 安全性技術，可進一步強化 SD-WAN 的分公司安全性。只要結合 NSX 安全性的強大威力，以及 VMware SD-WAN Edge 平台，客戶就能在不犧牲安全性的情況下，免除在分公司使用傳統防火牆的必要性、受惠於簡化的網路與安全性作業，同時善加利用 VMware 在威脅情報方面的投資成果。

為提供可延展的隨選雲端網路服務，本 VMware SD-WAN Gateway 系統會部署於全球的頂層雲端資料中心。VMware SD-WAN Gateway 會落實全域雲端服務 (軟體即服務、基礎架構即服務、網路服務) 與每個 VMware SD-WAN Edge 之間的 VMware DMPO、雲端 VPN 以及 VMware 多來源輸入服務品質 (QoS)，讓多條寬頻和私有租用線路能呈現為單一高效能廣域網路。使用雲端式 VMware Edge Cloud Orchestrator™ 佈建全網路業務原則、啟用服務增強功能、執行即時監控，以及分析應用程式效能。

數分鐘內部署完成

利用 VMware 的零接觸部署功能，就能快速安裝 VMware SD-WAN Edge。Edge 會運送到分公司，非技術人員只需要插入電源和網路纜線，啟用、設定和持續管理皆在雲端處理。

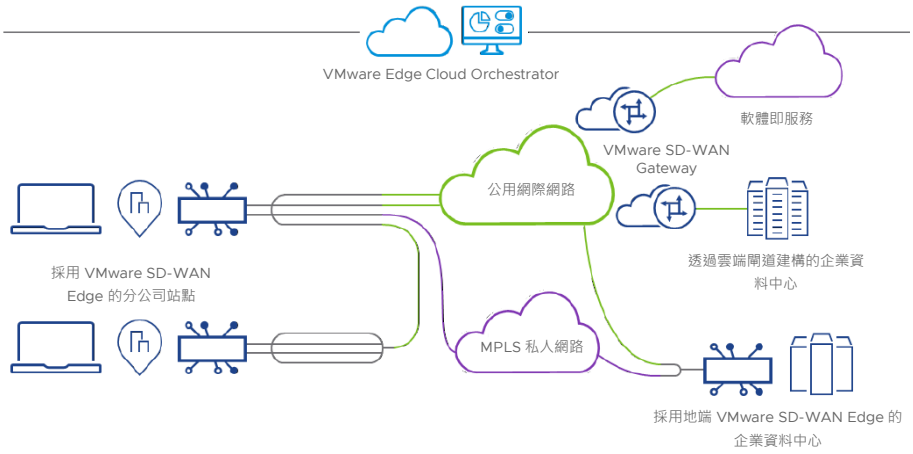

圖 2：VMware SD-WAN 服務

全企業通用業務原則

VMware SD-WAN 讓設定業務原則簡單到只需按一下即可。企業或其代管服務供應商能定義可在全企業許多 Edge 上套用的業務層級原則，而且完全透過集中化的雲端式 VMware Edge Cloud Orchestrator 來進行。連結導引、連結補救和服務品質，全都依據這些設定好的業務原則自動執行；不過，也可以利用特定設定進行覆寫。集中化的 VMware Edge Cloud Orchestrator 也會在層疊流量控制表內，提供全企業檢視以及路由可設定性，因此不再需要逐一進行複雜的節點路徑設定。

確保應用程式效能

VMware SD-WAN 會藉由實作其獨一無二的 DMPO，來提高混合式網路或標準寬頻網際網路連結的服務層級和容量。當中包含多項技術。

持續監控

會自動剖析廣域網路線路，以實現不需逐一手動調整站點設定參數的零接觸部署。持續監控連結與路徑品質以及可用容量，能提供即時意見，做為動態最佳化的依據。

動態應用程式導引

會依據業務的優先級別、內建的應用程式網路需求知識、即時連結效能和容量指標，自動辨識並將應用程式導引至最佳連結。每個封包導引的動態都可在串流中移動工作階段 (例如語音通話) 以避免連結效能降低，不需暫停通話，也不會感覺到語音品質不穩定。單一高頻寬流量可以利用彙總頻寬，讓回應時間更快。

隨選補救

只在僅有單一連結，或是同時連結效能降低無法導引時，才會隨選執行補救，包括錯誤修正、抖動緩衝和本機內重新傳輸。補救只能用在對網路敏感的優先應用程式，以及因節約用電導致連結效能降低時使用。

體驗品質

軟體定義廣域網路層疊搭配 DMPO，可實現應用程式特定的體驗品質。這能確保應用程式效能，透過涵蓋多個連結 (包括私有和網際網路寬頻) 的一個虛擬層疊，提供高品質和高容量的廣域網路。

統一且穩健的安全性

無論底層傳輸類型為何，VMware SD-WAN 都會提供統一且安全的通訊；且能針對分公司和資料中心之間的通訊，以及分公司之間的通訊，提供端對端標準 IPsec 加密。這款獨一無二的雲端交付架構，也提供從分公司到雲端閘道彙整點的自動化 VPN，帶來可互通存取的基礎架構即服務，而無需手動在雙邊設定從 1XN 個分公司到 1XN 個雲端資料中心的通道。 這款解決方案為公開金鑰基礎架構 (PKI) 提供延展性和穩健安全性，以及整合式憑證伺服器的整合管理、裝置安全上線和撤銷管理。透過將憑證與特定裝置綁定，並使用獨一無二的成對加密金鑰，可將風險降至最低。

VMware SD-WAN 解決方案將重要安全功能內建於 Edge 的資料轉發平台中。除了具連線狀態防火牆之外，當中還備有流量分段、入侵偵測和防禦 (IDS/IPS)，以及代管防火牆日誌記錄等功能。在 Edge 裝置上執行的增強型防火牆服務，可藉由偵測企業網路資產的未經授權存取、降低威脅風險，以及抵禦網路攻擊等方式，提高分公司的整體網路安全性。 今日的分散式企業可大幅受惠於增強型防火牆服務，進而保護使用者流量、整合硬體、簡單進行統一管理、減輕作業額外負荷，以及實現整體成本節約。內建於 VMware SD-WAN 中的增強型防火牆服務，為企業數位化轉型計畫的重要關鍵之一。

一鍵式服務交付

VMware SD-WAN 解決方案能簡化在分公司、整合性更高的企業服務集線器和雲端上的服務部署流程，讓分公司不再需要許多僅具備單一功能的裝置。一鍵式服務佈建功能會在分公司邊緣上啟動多項 VMware 原生服務，以及技術合作夥伴提供的協力廠商 VNF。一鍵式業務原則能以應用程式層級精細度，輕鬆規範從分公司傳輸到企業服務集線器和雲端服務的流量。

VMware SD-WAN 元件

VMware SD-WAN Edge 在分公司提供零接觸的軟體定義廣域網路部署，並在總部與資料中心位置提供可延展的地端集線器部署。

此外，可以直接透過 VMware 閘道，在雲端軟體即服務與基礎架構即服務位置上，獲得軟體定義廣域網路的所有優勢，包括確保效能、安全性與原則控制。雲端式 VMware Edge Cloud Orchestrator 提供全企業業務原則、設定、疑難排解與概觀式監控。

VMware SD-WAN Edge

若遠端分公司具備一定範圍的總流量、廣域網路與區域網路連線連接埠、整合式無線區域網路，以及安全性防火牆服務，就可使用 VMware SD-WAN Edge 輕鬆安裝應用裝置。動態路由可同時針對嵌入式與路徑外部署，啟用原則式層疊增強功能。高可用性 (HA) 設定可提供備援和容錯移轉。除了應用裝置選項外，還可使用 VMware SD-WAN Edge 做為 VNF 軟體，部署在 x86 伺服器 (包括虛擬 CPE 裝置) 上。增強型防火牆服務可協助企業軟體定義廣域網路分公司站點，防範內部網路資產遭到未經授權的存取。增強型防火牆服務內建多項進階安全功能 (例如應用程式感知和工作階段感知防火牆、IDS/IPS 和代管防火牆日誌記錄等)，能主動抵禦各種網路攻擊，並減少可能造成嚴重漏洞的潛在威脅。

VMware SD-WAN Gateway

VMware 與合作夥伴會將多租戶 VMware SD-WAN Gateway 部署在全球最頂層網路連接點 (PoP) 與雲端資料中心，以享受軟體定義廣域網路所帶來的完整優勢。VMware SD-WAN Gateway 提供可延展分散式基礎架構，具備代管網路即服務彈性的優點。VMware SD-WAN Gateway 提供理想的基礎架構，將雲端應用程式與資料中心的存取途徑，以及私有網路骨幹與舊版企業站點的存取途徑最佳化。

VMware Edge Cloud Orchestrator

VMware Edge Cloud Orchestrator 是一款雲端代管 (或位於地端) 的中央管理工具，適用於所有 VMware SASE 元件：VMware SD-WAN、VMware Secure Access、VMware Cloud Web Security 和 VMware Edge Network Intelligence。當中的網頁型使用者介面 (UI)，可提供簡化的設定、佈建、監控、故障管理、日誌記錄和報告功能。VMware Edge Cloud Orchestrator 能彈性實作業務型原則，以進行應用程式交付和流量管理。

VMware SD-Access™

VMware SD-Access 是一款雲端代管、安全且高效能的遠端存取解決方案，適用於今日分散各地的企業員工。VMware SD-Access 不僅以零信任網路存取 (ZTNA) 為基礎，也已針對速度進行最佳化，可確保應用程式品質，並讓遠端工作者受到保護且具有高度生產力。

這款雲端代管的可延展用戶端服務，可在數分鐘內完成設定，其能取代缺乏彈性的 VPN 基礎架構，並在伺服器、雲端，以及遠端工作者的桌面平台或行動裝置之間，交付高效能的私有網路架構，而且無需藉助於 SD-WAN Edge 應用裝置。使用者流量路徑已經過最佳化，進而避免「U 型往返」。VMware SD-Access 可大幅減少 IT 的資金和作業支出，同時將 SD-WAN 體驗延伸至出差或於遠端據點工作的使用者身上。

適用於廣域網路的安全 SDN

VMware SD-WAN 將軟體定義網路 (SDN) 概念帶進企業分公司廣域網路。VMware 的軟體式方法提供部署虛擬 SD-WAN Edge 的彈性和可移轉性，可部署到現成 x86 式硬體上，或做為 VNF 部署到虛擬 CPE 上。

在整個邏輯層疊上實作的業務原則，會將底層實體傳輸管道的應用程式流抽象化。藉由調整轉送實現靈活性，以符合原則和即時連結情況。SD-WAN 有一個分散式控制平台，可依照情境在本機內做出轉送決定，所以在整個廣域網路上都不會出現延遲問題或故障點。每個 SD-WAN 節點還是會收到集中化控制原則，以提供容易的可程式化功能和全企業能見度。安全性原則會透過 VMware Edge Cloud Orchestrator 使用者介面集中設定，並落實在分公司的 Edge 裝置上。管理可透過圖形化使用者介面或 REST API 執行。

VMware SD-WAN 與 VMware Secure Access Service Edge (SASE)

VMware SD-WAN 為整體 VMware SASE 解決方案的一環，而該解決方案則涵蓋多項雲端代管的軟體定義廣域網路和進階安全服務。VMware SASE 的架構旨在運用雲端威力的同時，將邊緣的複雜度降到最低；這款簡單好用的平台，可透過單一統一入口網站啟用統一邊緣與雲端服務模式，藉此管理業務原則、安全性、設定和監控。

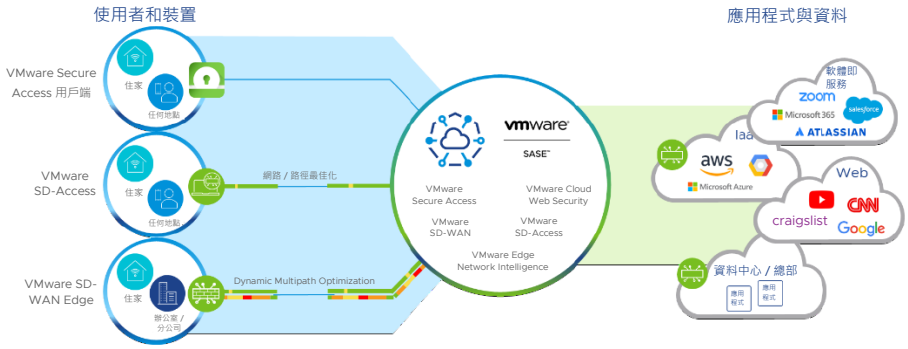

圖 3：VMware SASE

深入瞭解

- VMware SD-WAN：*sase.vmware.com/sd-wan*
- VMware SASE：*sase.vmware.com*

需要最佳且安全雲端應用程式存取功能的遠端與行動工作者，都可以利用 **VMware Secure Access™**。將外部部署的使用者帶入 VMware 光纖，讓遠端使用者能存取針對交付與效能最佳化的雲端式應用程式，並運用零信任網路存取 (ZTNA) 以及雲端代管解決方案的優勢。 VMware Secure Access 能簡化 IT 部署和維護昂貴虛擬私有網路 (VPN) 服務的程序。

使用者存取軟體即服務應用程式時，**VMware Cloud Web Security™** 可以為 IT 團隊提供能見度與控制力，並確保合規。此外也納入 URL 篩選功能，協助 IT 人員控制員工可以或不得存取的網站。IT 人員也能決定使用者可以或不得存取或上傳的內容類型，透過內容篩選功能減少攻擊範圍。他們可以使用最新的威脅情報來檢查內容，找出來自已知病毒的惡意軟體攻擊。這款解決方案支援在完備環境中檢查內容的沙箱，藉此抵禦惡意軟體的零時差攻擊。

VMware Edge Network Intelligence™ 是一款 AIOps 解決方案，讓 IT 人員能確實擁有物聯網與網路上終端使用者裝置的能見度與分析。針對不在控制範圍內的網路，IT 人員也能獲得能見度，例如遠端使用者的家用網路。這款經實證且不受限於廠商的解決方案，為分散各地的員工提供豐富的用戶端體驗，並有助於 IT 人員將探究根本原因的時間轉而投注在主動修復上。

文件編號：sdwan-564-Enterprise-WAN-Agility-so-0321