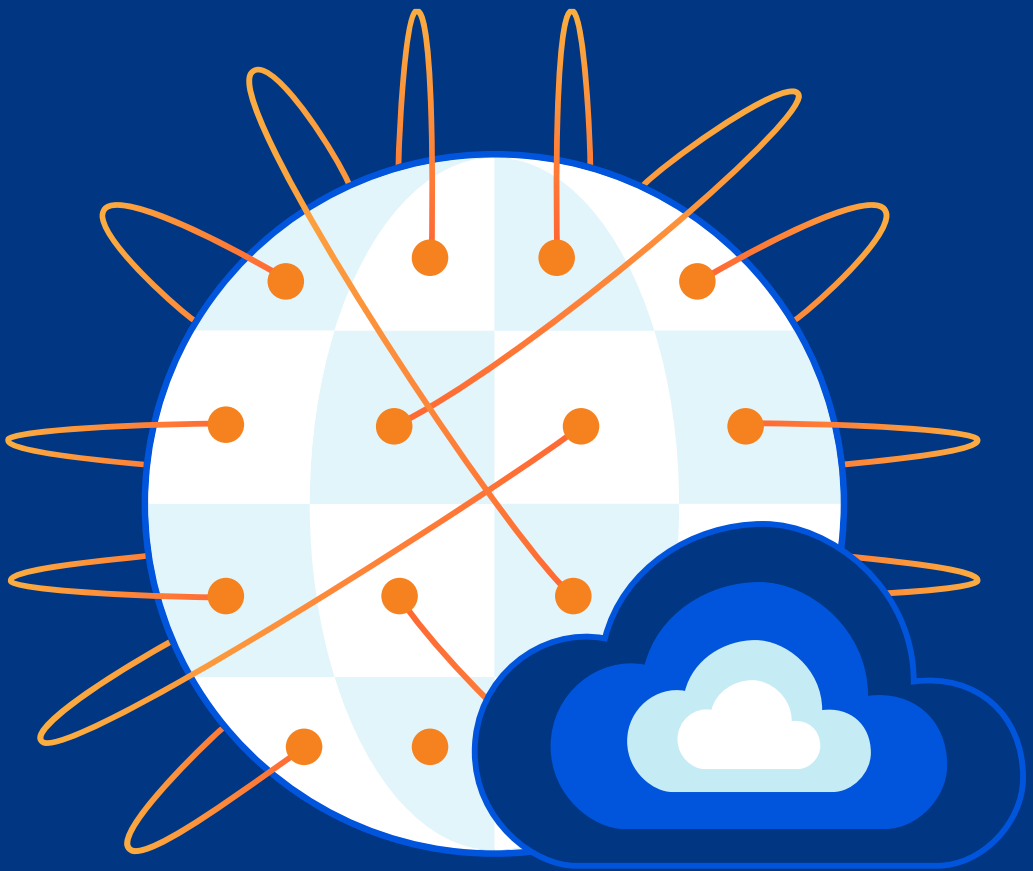
白皮書

CLOUDFLARE

WAN 即服務使網路能夠因應不斷變化的 IT 需求



+ 886 8 0185 7030 | e nterprise@cloudflare.com | www.cloudflare.com/zh-tw/

介紹

長期以來，企業一直依靠寬頻網際網路上的多協議標籤交換 (MPLS) 服務或 IPSec VPN 來建置廣域網路 (WAN)。這兩種方法一直都有其挑戰。MPLS 是一種橫跨私有資料中心、辦公室、零售店和其他位置建立虛擬專用網路 (VPN) 的可靠方法，但成本高昂。寬頻上的 IPSec VPN 更便宜，但本質上不可靠。

此外，這兩種 WAN 模式都是為應用程式位於私有資料中心且使用者主要位於辦公室的環境而設計。而今，隨著應用程式所涉的資料越來越多、在雲端執行的應用程式日益增加，並且所有員工都可以在家遠端工作，傳統的 WAN 很難跟上這一發展步伐。

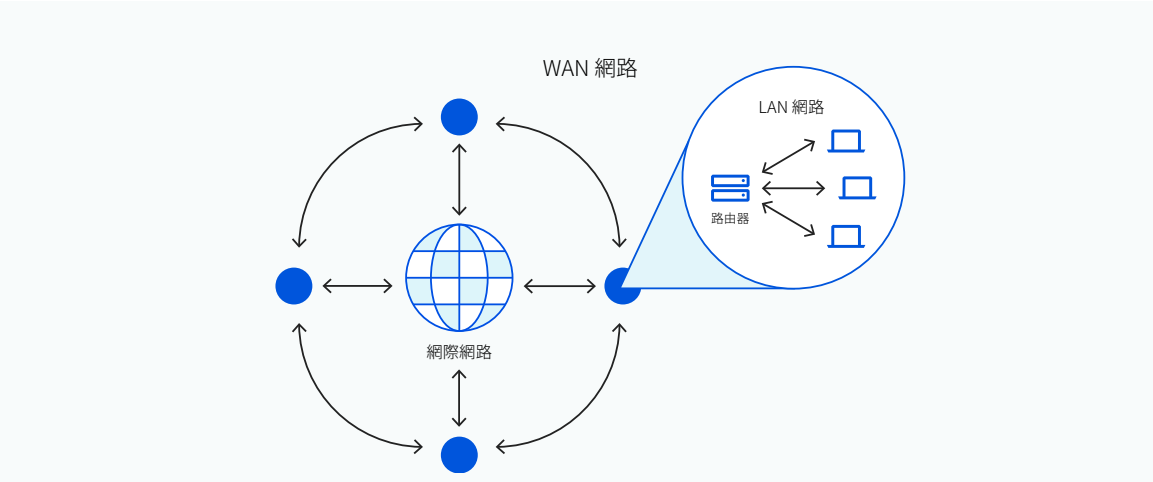
業界透過開發軟體定義廣域網路 (SD-WAN) 來因應這些挑戰。SD-WAN 可簡化網路原則設定和管理，同時協調多路徑和 WAN 架構 (例如寬頻和 MPLS) 上的流量。藉助這些優勢，企業得以發展他們的 WAN 並利用更便宜的連線選項。2020 年，全球 SD-WAN 市場規模為 19 億美元，預計到 2025 年將增長至 84 億美元。

儘管 SD-WAN 相對於傳統網路架構有所改進，但基本挑戰依然存在。雖然一些部署考慮到了當今不斷變化的流量模式，但雲端採用和遠端工作的爆炸性增長給許多 SD-WAN 架構帶來了壓力。安全性是另一個關鍵挑戰，因為去中心化的網路在保護網路安全方面的難度更大。

為了因應這些新挑戰，企業需要一種新的 WAN 架構：具有內建的網路安全、速度和可靠性，並且可以快速發展。WAN 即服務就屬於這種模式。這有望轉變企業網路架構並提供顯著的成本和效能優勢。

傳統 WAN 架構的挑戰

WAN 是一個大型網路，可遠距離連線各個位置 (如辦公室、資料中心、零售店等)。通常，每個位置都有自己的區域網路 (LAN)，透過乙太網路或 WiFi 等連線各個裝置。同時，WAN 連線使用 VPN、MPLS 或 IPSec 通道等方法。



WAN 使員工能夠安全地存取業務應用程式和工具。這還使機器能夠透過專用網路相互通訊。然而，傳統上用於提供這種互連的方法存在幾個挑戰：

MPLS VPN 挑戰

MPLS VPN 使企業能夠在廣泛的地理區域內連線多個資料中心和辦公地點。MPLS 不是讓每個核心路由器使用 IP 位址獨立計算路徑，而是沿著預定的網路路徑使用標籤，將資料從一個節點引導到下一個節點，藉此加速資料傳輸。

這種方法可簡化核心網路，為之提速，以便同時為多個企業 WAN 傳輸流量。這還對流量路徑進行更嚴格的控制，以確保服務的可靠性和品質。MPLS 通常包括多種服務類別，把等待時間敏感的應用程式 (如語音和視訊) 放在不太敏感的應用程式 (如資料庫備份) 之前。

雖然 MPLS 提供了速度和可靠性，但由於需要專門的路由器和預先設定，因此部署的建置成本較高且擴展速度慢。此外，必須在每個位置單獨設定資料隱私加密和其他外圍防火牆保護。組織還可能在將 MPLS 網路連線擴展到雲端伺服器時遇到困難，因此難以到達其資料和應用程式所在的位置。

MPLS 的優點：

- 提供 SLA 的高度可靠的服務
- 多種服務等級
- 不易受到 DDoS 等威脅的影響

MPLS 的缺點：

- 部署和擴展緩慢
- 無原生加密
- 未針對 SaaS 或公共雲端進行最佳化

寬頻網際網路 IPSec VPN 面臨的挑戰

企業還可以使用加密通道在公共網際網路上建置 VPN，進而在利用更便宜的寬頻網際網路連線的同時，確保資料隱私。許多 VPN 使用 IPsec 通訊協定套件來建立這些通道。IPSec VPN 通常由電訊廠商以服務的形式提供。

由於流量穿越公共網際網路，沒有服務品質保證，因此這種 WAN 架構在本質上不太可靠。公共網際網路擁塞、服務中斷、路由錯誤和其他障礙可能會損害 IPSec VPN 的效能和連線能力。此外，即使可以使用專用路由器在網路邊緣強制保證服務品質，所有流量一旦到達網際網路，也會得到同等對待。音訊和視訊通話不會在備份等不太敏感的流量之前得到處理。

此外，IPSec VPN 通常遵循中心輻射模型，其中來自遠端分支機構的流量被帶回中央資料「中心」。當大多數網路流量涉及託管在集中資料中心的業務應用程式時，中心輻射模型效果良好。然而，公共雲端、SaaS 和 IoT 的增長導致這種模型效率低下。例如，新加坡辦事處的使用者嘗試存取公司電子郵件，其流量可能會回傳到美國，即使電子郵件提供者在新加坡設有資料中心也不例外。這些長途往返傳送會損害應用程式效能。

IPsec VPN 的優點：	IPsec VPN 的缺點：
與 MPLS 相比成本低廉	可靠性不如 MPLS
操作彈性更高	中心輻射架構不足
原生加密	單一服務等級

混合 MPLS 和寬頻網際網路面臨的挑戰

一些公司同時在寬頻網際網路上使用 MPLS 和 IPSec 實施混合 WAN。這使他們能夠整合 MPLS 廠商可能無法提供服務或具有更簡單要求的其他站點，例如小型零售店。

這種混合 MPLS 寬頻方法雖然改進了頻寬分配，但並沒有緩解這兩種技術固有的缺點。企業仍然需要安裝和管理來自多個服務提供者的租用線路和寬頻網際網路，承擔越來越高的行政開支。此外，他們必須在每個辦公地點將一系列網路安全和效能裝置串在一起，才能克服每種連線模型的缺點。

此外，傳統 WAN 架構本身不包含網路安全服務，迫使企業在每個位置購買、安裝和管理裝置 (如網路防火牆、DDoS 緩解、WAN 最佳化和負載平衡)，以確保當今業務應用程式需要的網路安全、效能和可靠性。這種網路硬體會導致增加複雜性、成本、技術債務和複雜的依賴關係。

最後，傳統 WAN 對流量的可見性有限。由於來自 LAN、廠商 MPLS 網路和公共網際網路的效能資料十分零散，無法從中獲得洞見。例如，使用者在線上時在做什麼？網路安全原則的效果如何？哪些應用程式使用的頻寬最多？

混合 WAN 的優點：	混合 WAN 的缺點：
更好的頻寬分配	無原生網路安全
可靠性 (使用 MPLS 時)	硬體管理開支
成本效益 (使用 IPSec VPN 時)	可見度碎片化

SD-WAN 的優勢和挑戰

SD-WAN 在企業站點使用軟體和集中控制器來克服傳統 WAN 架構的一些限制。這使企業能夠從單個軟體平台管理多種連線類型 (包括寬頻網際網路、租用線路和 MPLS) 的流量。這還可以自動執行網路監測任務，做出即時流量控制決策，並使用直接連線和分裂通道最佳化對公共雲端和 SaaS 應用程式的存取。

SD-WAN 可以簡化管理，還能夠透過更便宜的寬頻網際網路連線提供類似 MPLS 的可靠性和效能，因此能夠降低組織的成本。但是，SD-WAN 也面臨著自己的挑戰。

網路安全性仍需加強

雖然 SD-WAN 允許從分支機構直接存取公共雲端和 SaaS 服務，但它們缺乏大多數企業所需的全套外圍網路安全控制。一些 SD-WAN 廠商包括基本的防火牆和 VPN 功能，但通常不足以提供強大的保護。

因此，大多數組織無法利用這些增強功能，仍然必須在啟用防火牆、入侵偵測、資料丟失防護和安全 Web 存取的情況下將流量回傳到資料中心所在的位置。

最終使用者等待時間

當流量必須回傳到集中位置時，視訊和電話等資料豐富的應用程式將受到影響。

端到端服務品質差

雖然 SD-WAN 可以簡化管理並降低成本，但它們仍然依賴不可預測的公共網際網路在站點之間傳輸流量。這表示視訊會議等對等待時間敏感且需要大量頻寬的應用程式可能會在網路擁塞期間執行不暢。雖然一些 SD-WAN 廠商營運自己的骨幹網路，但大多數是邊緣技術，無法保證端到端的良好應用程式體驗。

不擴展到遠端工作

許多行業的員工現在在家、在辦公室和在路上時都會工作。SD-WAN 無法擴展到遠端工作使用案例。雖然家庭辦公室 LAN 理論上可以整合到公司網路中，但出於多種原因，這樣做並不實際。大多數 SD-WAN 技術無法在連線到公司 WAN 的膝上型電腦上使用。員工希望無論身在何處都能獲得相同級別的存取權限，這需要分層添加額外的零信任網路存取解決方案。

SD-WAN 的優點：	SD-WAN 的缺點
簡化 WAN 管理	需要附加網路安全性
降低營運成本	端到端服務品質差
提高應用程式效能	更難滿足遠端工作者的需求

WAN 即服務滿足現代網路的需求

WAN 即服務是一種可解決上文所有挑戰的 WAN 模型。這使組織能夠利用 SD-WAN 的優勢，解決 SD-WAN 的不足，提高營運敏捷性並降低總持有成本。

WAN 即服務部署具有以下功能：

- **全球網路：**WAN 即服務使用由許多資料中心組成的大型全球網路作為 WAN 的連接橋樑。
- **互連性：**該網路與 ISP、雲端廠商和私有企業網路深度互連。
- **整合安全：**網路執行全套網路安全服務，包括防火牆、DDoS 緩解和零信任安全。
- **統一架構：**所有 WAN 功能和安全服務都在網路中每個資料中心的每台伺服器中執行。
- **單一儀表板：**所有這些服務都可以透過單一儀表板在瀏覽器中進行管理。

憑藉這些功能，WAN 即服務為常見的 WAN 和 SD-WAN 挑戰提供以下解決方案：

挑戰	WAN 即服務的優勢
取代昂貴的傳統服務和網路裝置	透過具有整合網路安全性的互連全球網路最佳化應用程式效能。
每個站點的專有硬體裝置	完全由軟體定義，雲端原生，無需自訂實體或虛擬裝置。
MPLS 擴展緩慢	擴展迅速，可容納新的辦公地點，透過全球分佈式互連網路處理成千上萬個遠端存取請求。
管理成本和資源流失	「即服務」表示網路管理現在成為涵蓋整個 WAN 的集中式營運費用項目。消除了昂貴的遠端現場維護成本。
可能受到公共網際網路擁塞的影響	WAN 即服務方法透過公共網際網路發送流量，但會使用其網路規模來尋找快速網路路徑並避免擁塞。
資料回傳導致的等待時間	WAN 即服務使用全球數百個網路位置，使工作負載更接近使用者，並消除了回傳資料的需要。這提高了效能，尤其是對於即時、資料傳輸量大的應用程式。
網路安全性附加解決方案	透過一個統一的控制平面，WAN 即服務從每個網路位置應用緊密整合的全網路安全性 (例如內建的、軟體定義的網路防火牆)。可以根據 IP、連接埠、封包長度和位元欄位比對來套用流量篩選器。規則可在瞬間部署到所有位置。額外的安全功能可以分層部署，用於 DNS 篩選、具有遠端瀏覽器隔離功能的 SWG 和 DDoS 保護。
網路分析和可見性碎片化	藉助 WAN 即服務，企業可以在統一的分析儀表板上查看其所有 WAN 流量，深入瞭解網路的使用方式和使用者。
不擴展到遠端工作	WAN 即服務可以容納遠端使用者和端點。所有遠端流量不再經由單一壅塞點 (例如企業網路「邊界」上的 VPN 集中器) 傳送，而是路由到最近的邊緣位置，透過最佳路徑引導。因此，客戶可以從任何位置實現卓越的應用程式效能和更好的最終使用者體驗。

Magic WAN

維護 MPLS 和網際網路電路以及 SD-WAN 控制器和內聯路由器的管理負擔會消耗資源並損害效能。Cloudflare 的 Magic WAN 提供「即服務」的便利性和功能。

Cloudflare 營運著全球最大的網路之一，其資料中心遍佈 100 個國家/地區的 200 多個城市。我們的網路與電訊廠商無關，與主要 ISP、雲端服務和企業建立了 9500 多組互連。我們網路中每個資料中心的每台伺服器都提供所有網路和效能服務。

Magic WAN 用 Cloudflare 的網路取代傳統的 WAN 架構，透過一個簡單的使用者介面提供全球連線、整合網路安全，以及高效能。

若要瞭解更多詳情，請造訪 cloudflare.com/magic-wan