



立即實現遠端存取安全 現代化的四個充分理由

Prisma Access 提供隨需可擴充性，
雲端中的完整防火牆功能等等

遠端是新常態

遠端工作（也稱為遠端辦公）並不是什麼新鮮事。1979 年，IBM 進行實驗，允許 5 名員工進行遠端工作，IBM 遠端工作者的人數在短短幾年內增加到 2,000 多名。¹ 從此之後，在家工作員工的比例持續穩定增加。Gallup 最近的一項調查顯示，每月至少有一天遠距離辦公的美國勞工比例從 2019 年的 42% 增加到 2020 年的 49%。²

COVID-19 疫情大流行加速這個趨勢。截至 2020 年 8 月，超過四分之一（26%）的美國員工完全在家工作，而近十分之四（38%）的員工在家工作的時間超過一半。³ 在通常有部份時間在家工作的勞工之中，在家工作日的平均天數增加一倍，從 2019 年的 5.8 天增加到 2020 年的 11.9 天。⁴ 隨著公司被迫將大部份工作者轉移到異地，許多人發現利大於弊。此外，勞工絕大多數贊成這種改變，全世界 76% 的辦公室工作人員表示希望繼續在家工作。⁵ 異地工作曾經是例外，現在已成為常態。

在家工作的平均天數/月數（美國）



舊型基礎結構無法充分因應

改採大多是遠端工作者的做法對於現有基礎結構帶來壓力，因此，許多企業對於三個關鍵領域（可擴充性、安全性和效能）試圖因應目前架構的侷限性。

無法擴充

COVID-19 封鎖實施時，企業發現本身的遠端工作者人數大幅增加，在某些情況下，幾乎是一夕之間增加數倍。舊型架構仰賴每個分公司位置部署的硬體型網路和安全設備，需要將實體運送到每個公司現場並並手動設定硬體。容納更多的遠端使用者會逼近北向網際網路連結的頻寬限制，因此需要新增其他硬體來擴充遠端使用者人數。不過，舊型架構過於欠缺彈性，需要難以負擔的高成本硬體和軟體升級。

安全複雜度

隨著企業將應用程式和資訊移轉到雲端，企業面臨安全架構的限制。安全架構師運用安全 Web 閘道（SWG）、網路應用程式防火牆（WAF）和雲端存取安全代理（CASB）等技術做為因應。這些技術能夠解決特定問題，不過同時也增加複雜度，因此難以維持一致的政策，並導致企業的整體安全狀況出現落差。

這個問題的另一個方面是，使用雲端式公有和私有軟體即服務（SaaS）取代內部部署應用程式的情況愈來愈多，例如企業資源規劃（ERP）、客戶關係管理（CRM）和人力資源管理（HRM）。由於大量使用未獲批准的個人雲端應用程式（所謂的「影子 IT」），導致企業難以在家保護受管理的公司裝置並實施可接受的使用政策。

¹ 「The History of Remote Work, 1560-Present」，TopTal，最後存取時間為 2020 年 12 月 15 日。

² Jeffrey M. Jones，「U.S. Remote Workdays Have Doubled During Pandemic」，Gallup，2020 年 8 月 31 日。

³ 同上。

⁴ 同上。

⁵ Mark Murphy，「The Surprising Truth About How Many Employees Want to Keep Working From Home」，富比士，2020 年 11 月 8 日。

效能降低

為地理位置集中的員工設計的架構無法充分支援現今分散各地的工作者。回傳是其中一例，這是透過總部的數據中心傳送所有遠端流量的做法（見圖 1）。雖然這種方法有助於實現安全標準化並且將網路監控簡化，不過也有缺點。一方面，無論目的地為何，所

有流量都必須流經集中的位置，這是導致網路效能降低並造成單點故障的瓶頸。另外，這種架構會增加延遲，因此可能不利於視訊會議和其他媒體應用程式。

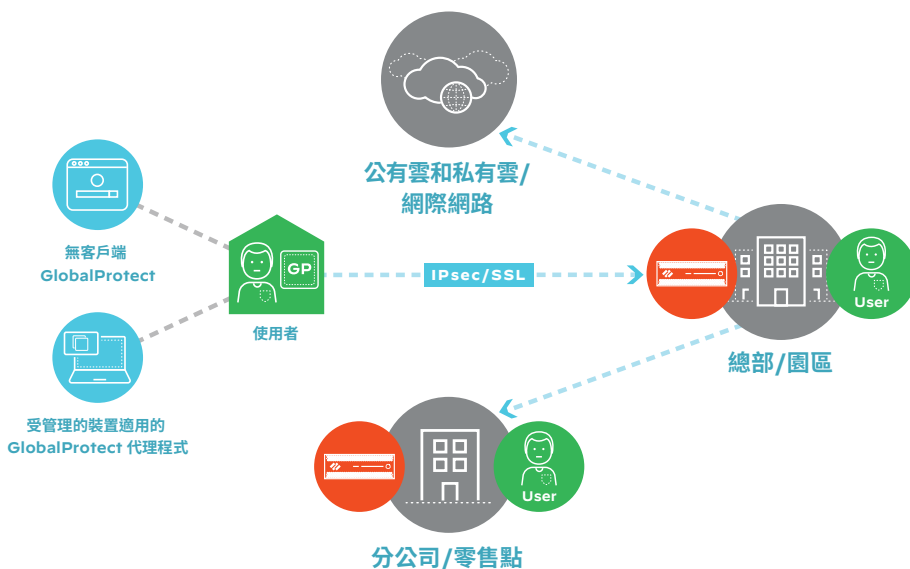


圖 1：傳統架構中的回傳

SASE 能夠解決這些問題並發揮其他功用

為了因應這些挑戰，企業逐漸改採安全存取服務邊緣 (SASE) 模型。SASE 將廣域網路 (WAN) 和網路安全服務 (例如 CASB、防火牆即服務 (FWaaS)、SWG 和零信任網路存取 (ZTNA)) 融合成單一雲端交付的服務模型。頂級 SASE 解決方案透過通用架構支援所有類型的雲端應用程式 (公有雲、私有雲和 SaaS) (見圖 2)。

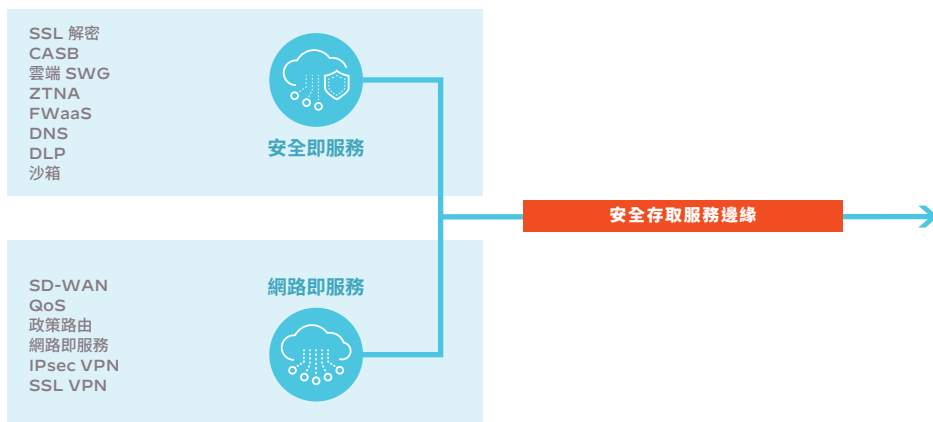


圖 2：典型 SASE 架構

Prisma Access：充分運用 SASE 的關鍵

Prisma® Access 是全面的 SASE 解決方案，讓企業能夠從雲端中提供保護，同時降低資本支出並減少通常與大規模部署安全性有關的開支。Prisma Access 使用雲端式通用基礎結構來提供網路連線和安全管理服務（見圖 3）。

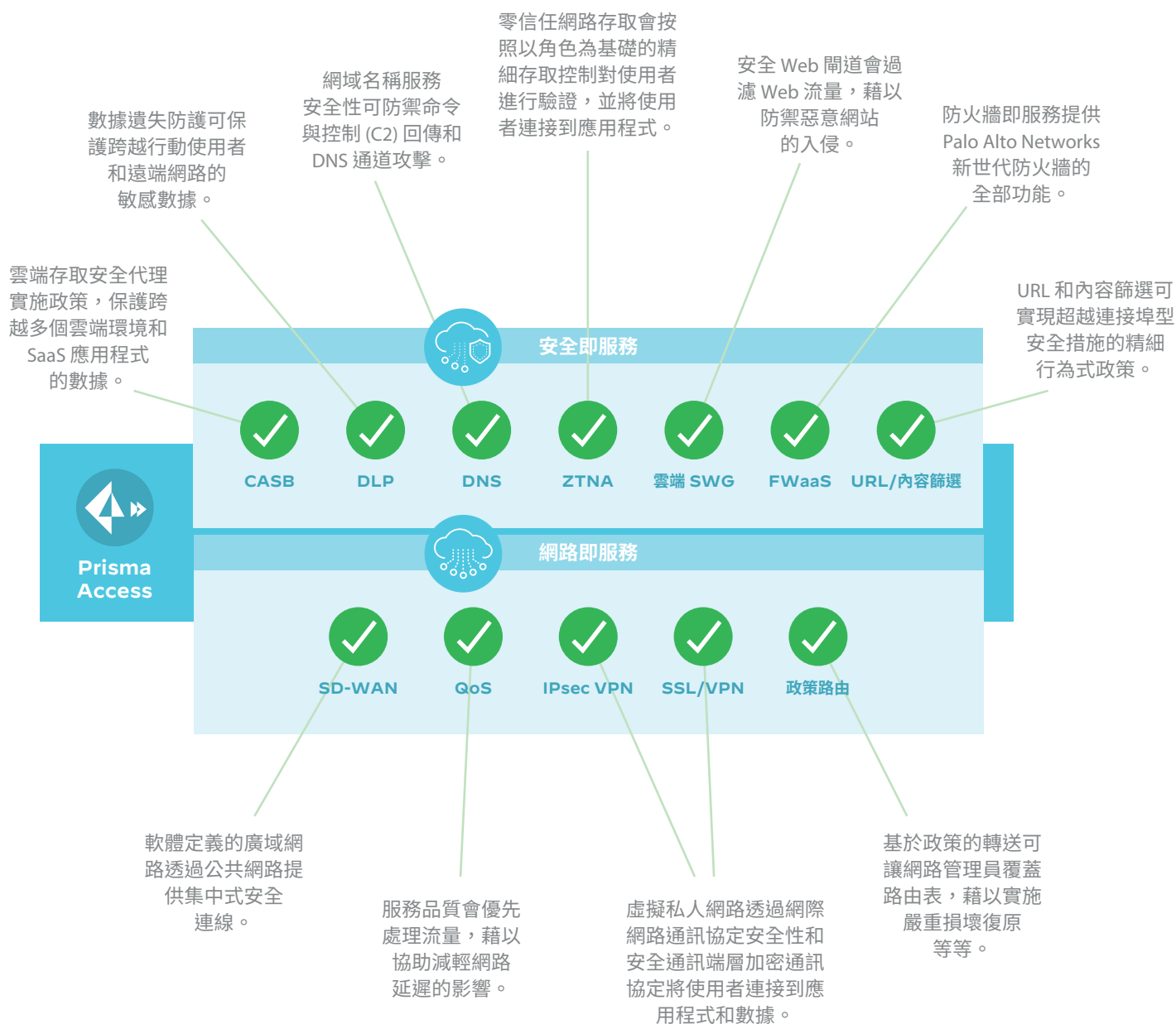


圖 3：Prisma Access 功能

Prisma Access 補強 GlobalProtect

如今，許多企業使用 GlobalProtect™ (與 Palo Alto Networks 新世代防火牆一起提供的 VPN 解決方案) 連接遠端工作者。藉由透過 GlobalProtect 擴展新世代防火牆功能，這些企業可以將公司安全政策 (見圖 4) 擴展到遠端使用者，就像在辦公室一樣。

Prisma Access 透過為遠端使用者提供隨需的彈性規模，為 Palo Alto Networks 新世代防火牆補強 GlobalProtect。遠端工作者不需要將流量回傳到總部，而是直接連接到全世界 Prisma Access 服務邊緣，這個服務邊緣提供整合式網路和安全服務，可用於存取公有雲和私有雲服務、數據中心應用程式和公開網際網路，展現順暢的使用者體驗。

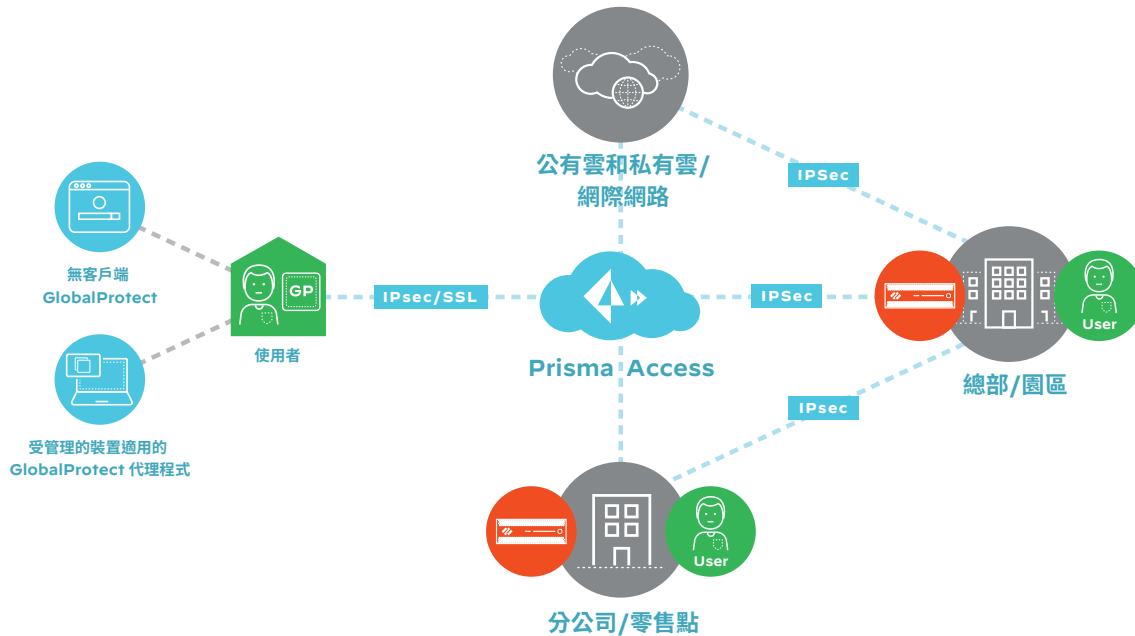


圖 4：Prisma Access 與 GlobalProtect 一起部署

⁶ Joe Delio, 「[Leveraging GlobalProtect and Prisma Access during the COVID-19 Pandemic](#)」, Palo Alto Networks, 2020 年 3 月 13 日。

為什麼應該考量 Prisma Access

使用 Prisma Access 的理由相當明顯，並且具有說服力。以下是在您的策略規劃中加入 Prisma Access 的四個充分理由。

理由 1：隨需可擴充性

Prisma Access 基於全球高效能網路建構，能夠確保無限的安全遠端存取可擴充性。Prisma Access 有 100 多個網路節點，能夠以低延遲 (SLA 保證少於 10 毫秒) 的執行時間達到五倍的可用性，藉以達到最佳的使用者體驗。

Schlumberger 在短短幾天內將遠端使用者人數增加三倍

COVID-19 危機對全世界能源巨擘 Schlumberger 構成嚴峻挑戰。幾乎一夕之間，需要從遠端位置安全地工作的遠端工作者人數急遽增加。Schlumberger 向 Palo Alto Networks 尋求協助。

Prisma Access 提供的新世代網路安全性促使該公司在幾天內將 25,000 名使用者擴展到 8 萬名，而且生產力完全不受影響。Schlumberger 也使用 GlobalProtect 將 Schlumberger 使用者體驗擴展到家中，並以 Cortex® XSOAR 做為公司在休斯敦新世代安全作業中心的樞紐。

理由 2：基礎結構現代化

部署 Prisma Access 有助於實現基礎結構現代化，藉以容納大量的遠端工作者。透過消除回傳，Prisma Access 將安全措施移到更接近最終使用者的位置 (見圖 5)。

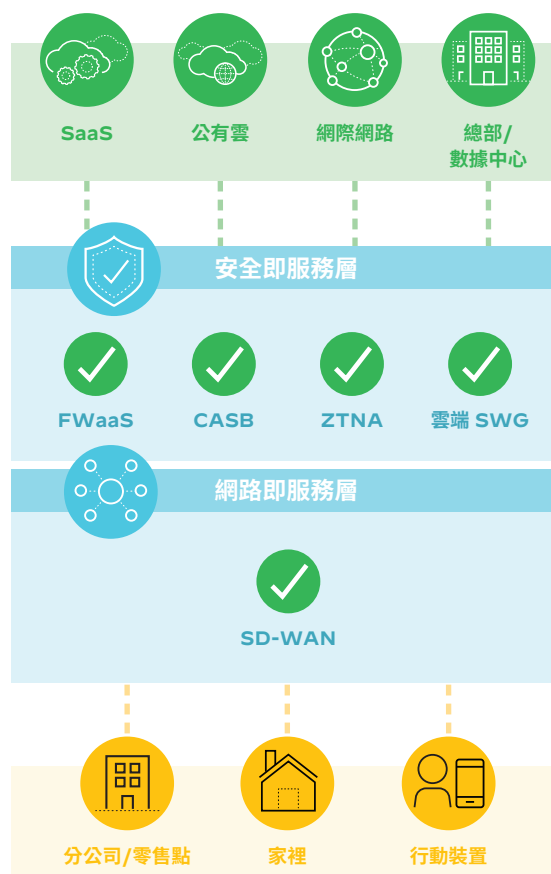


圖 5：藉由 Prisma Access 將基礎結構現代化

理由 3：簡化的 SaaS 移轉

移轉到雲端似乎是艱鉅的任務。每次將內部部署應用程式移轉到雲端 SaaS，都需要遵循所有應用程式、使用者和安全政策。Prisma Access 為您提供無縫移轉到雲端的捷徑。運用 Panorama 做為管理和政策介面，Prisma Access 能夠從防火牆部署中無縫移轉累積的使用者、安全性和應用程式特定政策。最重要的是，您可以運用現有的 GlobalProtect 部署，同時充分運用訓練安全分析師和工程師的所有現有投資（見圖 6）。



圖 6：移轉安全政策

理由 4：熟悉、可信賴的安全功能

Prisma Access 具有雲端式 Palo Alto Networks 新世代防火牆解決方案的所有功能，能夠保護遠端工作者。現在，完全不需要附加需要訓練並造成防護出現漏洞的其他安全元件。Prisma Access 可讓您以自己的步調輕鬆移轉到雲端，並確認自己獲得可信賴的知名安全解決方案所提供的保護，這套解決方案可以滿足並適應您的動態需求。

接下來的計劃

將應用程式和數據從內部部署基礎結構移轉到雲端並支援持續增加的遠端工作者可能相當有挑戰性。不過，部署遠端存取安全措施不一定如此。Prisma Access 為遠端工作的短期和中期急遽增加提供行動使用者可擴充性，並且能夠長期將基礎結構現代化。

隨著移轉到雲端的壓力持續增加，您已經無法等待。立即瞭解 Prisma Access，思考如何運用我們全面的 SASE 方法而獲益。立即聯絡 Palo Alto Networks 代表，或造訪

<https://www.paloaltonetworks.com/prisma/access>。