網路邊緣安全存取服務SASE發展趨勢

台灣亞太產業分析專業協進會 106 年認證資深產業分析師 徐富桂

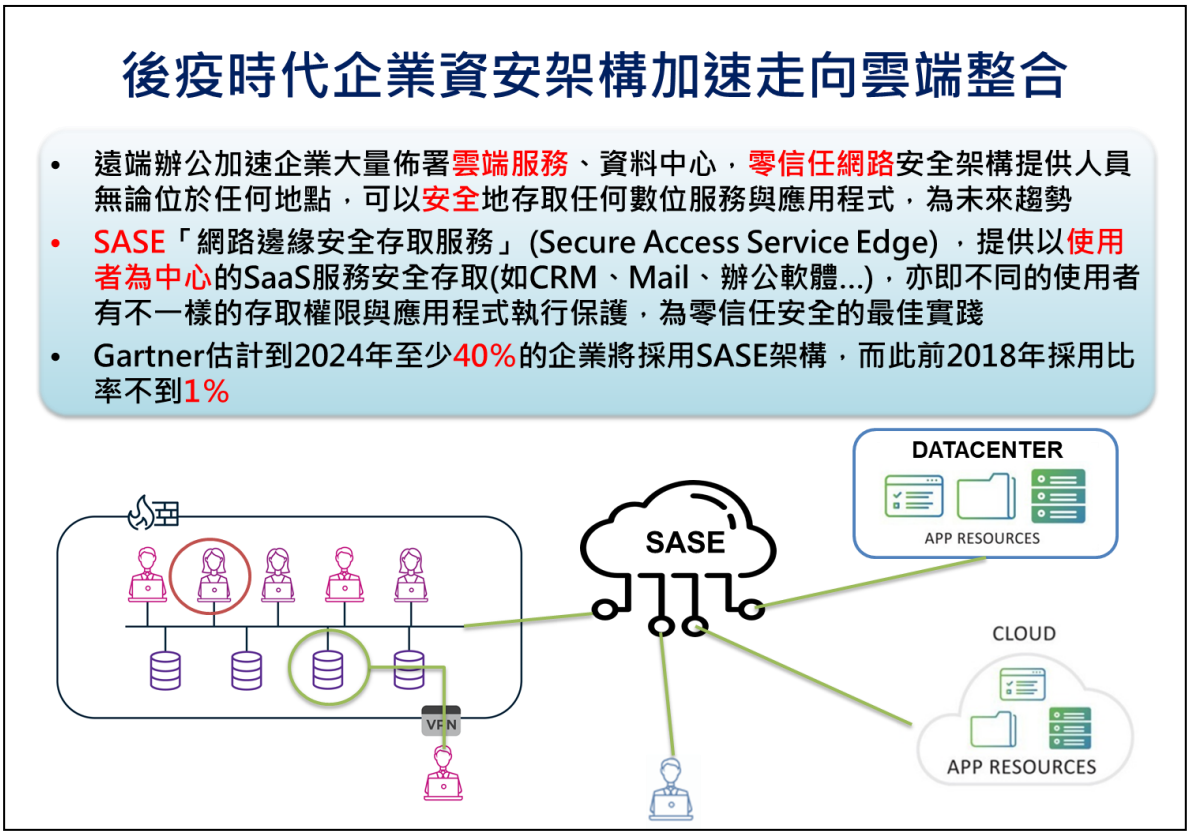
遠端存取與雲端運算存取已是疫情過後的全球商業新常態。企業面臨混合雲端配置、多樣化網路存取、關鍵資料安全保護、網路使用權限管理等諸多問題。網路邊緣安全存取服務架構SASE (Secure Access Service Edge)似乎是目前雲端安全的最佳解決方案，融合現今企業對於網路即服務與資安即服務的需求，將全面的廣域網路 WAN 功能(包括 SD-WAN、CDN 等)與網路及雲端安全功能(如 SWG、CASB、FWaaS 和 ZTNA)相互結合，依據使用者身份(可能是特定個人、分公司職員、第三方協力廠商、特定 IoT 設備…)在網路邊緣即進行網路存取權限分流，再直接對企業數據中心或是公有雲端應用或平台進行應用程式或是機敏資料的存取，而不用將網路流量導入總公司之後再轉往雲端增加資料傳輸風險以及被攻擊的面向。

一、SASE 網路邊緣安全存取服務架構簡介

2020 年疫情衝擊之下，VPN(企業虛擬私有網路)是企業最先搶進的遠端存取解決方案，但是隨著遠端辦公的新常態營運模式加速企業大量佈署雲端服務及應用與雲端資料中心、行動辦公室的蓬勃發展，打破以往所熟悉的網路邊界防護，VPN 面臨極大的挑戰。唯有建立起一個「可信任」的安全管理模型，才能夠讓使用者的認證及授權可信、資訊流及資安風險能夠可見可視及可控可管。零信任網路安全架構(Zero Trust)，認為應預設任何的網路存取要求均不可信任，唯有經過認證之後，才可以依管理政策權限存取。成為新常態經濟下最佳的網路安全示範。但零信任架構並不是指特定的技術，而是多種技術的應用整合概念，因此市調公司 Gartner 在其研究報告中歸納定義了「網路邊緣安全存取服務」SASE (Secure Access Service Edge) 市場，成為現今企業對於「零信任」安全的最佳實踐。

簡單來說，SASE 就是把身份管理落地到終端設備及網路邊緣，而網路流量則依照身份管理政策導流到應用雲端平台或企業內的資料中心，網路安全上的功能及設備則全部內建於雲端解決方案。尤其是在疫情之後的遠距工作模式以及 5G 時代的來臨，這種趨勢會越來越明顯。新常態下使用傳統網路存取模式在這種環境中會帶來非常複雜的網路管理配置問題，而 SASE 架構通過把廣域網路連接能力(如：SD-WAN)和網路安全防護能力(如：SWG、CASB、FWaaS、…)融合在一起，從而有效降低網路控制的複雜度。這樣既能提供一個具有彈性可擴充的網路，還

能提供基於使用者權限策略的“軟體定義”安全存取服務。這個彈性網路為數位化轉型企業的安全團隊提供前所未有的網路可視性(Visibility)與管理性(Manageability)，亦即可以根據使用者身份和封包內容上下文精確地指定每條網路連線的 QoS 性能、可靠性和安全性，從而使安全團隊能夠為分散在各地的行動使用者、分公司團隊和基於雲端應用的服務提供安全資料存取，從而安全地實現數位化轉型所需要的動態存取。



資料來源：工研院產科國際所(2021/04)

圖一 SASE 網路安全架構概念

Gartner 特別認為 SASE 網路邊緣安全存取服務架構需要具備以下幾個特點：

1. **以使用者身份為中心**：網路邊緣安全存取服務(SASE)是使用身份作為存取決策的新中心，而不是企業資料中心的存取權限。因此網路存取權限是綜整使用者身份、連線設備識別和應用程式存取權限等身份，而不是以往基於設備的 IP 位址或地理位置。正是這種邏輯層面定義策略的轉換，極大地簡化安全策略管理。

2. **以雲端應用為原生架構**：SASE 最大的假設是，企業逐漸將重要資料、服務雲端化、或是直接採用公有雲的 SaaS 服務(如 CRM、Mail、辦公軟體…)，因而在公司外部的行動使用者或駐外分公司的網路存取不會因使用 VPN 而將全部的網路流量導回總部，也不會放任自由連上廣域網路服務而失去網路安全的保護。SASE 在架構上充分利用雲端運算主要特性，例如：彈性、自我調整性、自動化、自恢復能力和自我維護等。

3. **網路安全設備及配置的簡化架構**：通過整合來自第三方安全產品提供商的安全存取服務，將有效減少供應商的總數量，減少駐外分公司中的實體或虛擬安全裝置的數量，並且減少使用者終端設備上所需代理程式的數量。同時，整合供應商設備，將有機會使用"單次通過(single pass)"架構進行網路內容的檢查。在這種架構下，所有網路會話層的封包會被一次性的解密，並使用多個安全策略引擎(FW、IDS…)並行地檢查一次，而不是多個安全檢查引擎進行串列式的檢查，徒增延遲時間。這將為用戶提供一致的網路存取體驗，無論用戶在哪裡、在訪問什麼、以及位於何處。

二、全球 SASE 架構主要廠商發展現況

自從 Gartner 依零信任架構為基礎，發表了 SASE 網路邊緣安全存取服務架構做為最佳實踐範例以來，迅速發展成為廣受網路產業以及資安產業的關注焦點。目前，已有不少主流 SD-WAN 和安全供應商開始採用 SASE 架構的相關產品及服務。當然這項技術也還在剛起步階段，在疫情爆發前普及率還不到 1%。不過經歷 2020 年的強烈需求，引起目前市場上既有的 SD-WAN 廠商包括 Cato Network、Juniper、Fortinet 和 Versa 等也積極搶進 SASE 市場。我們也可以透過 2020 年以來，相關業者透過收購相關新創技術的情形，一窺 SASE 存取服務平台的發展腳步。

(一) SASE 架構領導廠商 Cato Networks 發展

Cato Networks 由 Check Point 和 Imperva 的前聯合創始人 Shlomo Kramer 於 2015 年創立，為一家網路和安全服務的公司，其核心產品是一種雲端服務，融合了邊緣 SD-WAN、全球專用骨幹網路和雲端安全等。此雲端平台旨在提供覆蓋企業分支機構、移動用戶和企業雲端數據中心的安全連接服務。該公司的服務整合下世代防火牆（NGFW）、VPN、安全網路閘道(Secure Web Gateway)、進階威脅防護(ATP)及網路安全犯罪鑑識取證等。該公司在 2017 年即成為 Gartner 報告的中型企業「安全性酷廠商」、也入選 2018 年 RSAC 創新沙盒決賽，更自主宣稱 Cato Cloud 為世界上第一個 SASE 平台。而在 2020 年 Cato Network 因應疫情發展，針對居家

上班、遠端存取推出安全即服務(Security as a Service)的完整的企業級網路安全服務，可以檢查所有 WAN 和 Internet 流量，成為 SASE 架構發展的指標性廠商。

(二) 新進搶入網路邊緣安全存取服務 SASE 架構的廠商發展

1. Palo Alto Networks 以 4.2 億美元收購 CloudGenix

2020 年 3 月，Palo Alto Networks 宣佈將以 4.2 億美元收購 SD-WAN 廠商 CloudGenix，以增強其 SASE 的地位，這是迄今為止 SASE 網路邊緣安全存取服務架構下，規模最大的併購。早在 2019 年，Palo Alto Networks 將 SD-WAN 和資料遺失防護(DLP)技術集成到其 Prisma Access 平台時，即成為首批支持 SASE 架構的主要安全供應商之一。原本 Palo Alto Prisma Access 平台就具備基本的 SD-WAN 功能，但它是通過運行在最終使用者硬體上的代理程式實現的，並沒有直接向分支機構提供相對應服務。而對 CloudGenix 的收購正填補這一空白，使 Palo Alto Networks 能夠將 SASE 平台部署到遠端工作人員以及更多傳統的企業分支據點或零售地點。

表 1 2020 年 SASE 架構解決方案進展

合作廠商	解決方案	合作時間
paloalto NETWORKS CLOUDGENIX A PALO ALTO NETWORKS COMPANY	網路安全廠商併購 SD-WAN 解決方案	2020.03
FORTINET OPAQ	網路安全廠商併購 SD-WAN 雲端服務解決方案	2020.07
vmware nyansa	Vmware 今年積極從主控儀表板、AI 策略分析，CASB、RBI 技術等與同業合作	2020.01~ 2020.06
CLOUDFLARE S2 SYSTEMS	專注於解決遠端工作者面臨的問題以及分支機構的安全連接解決方案	2020.01
McAfee Light Point Security	將 RBI、CASB、SWG 和 DLP 等功能融合到一個雲端安全解決方案中。	2020.02
zscaler EDGEWISE NETWORKS	以 AI 和機器學習來自動識別及調整應用程式及使用者的合法存取權限規則	2020.05

資料來源：工研院產科國際所(2020/12)

2. Fortinet 通過收購 Opaq 獲得 SASE

Fortinet 也是最早採用 SASE 架構的安全和 SD-WAN 供應商之一。2020 年 7 月，該公司宣佈有意收購 SASE 初創公司 Opaq。Fortinet 除了取得基於雲端的網路存取平台外，還獲得 Opaq 的服務優勢。

在收購之前，Fortinet 主要是一家基於網路硬體安全和 SD-WAN 硬體平台的供應商，主要依靠強大自行研發的網路封包處理器 ASIC 進行網路安全防護。而 SASE 服務架構是一種主要基於雲端運算的架構，因此 Fortinet 收購 Opaq 將使該公司能夠更有效地在客戶需要的任何地方部署 SD-WAN 和網路安全功能，同時其 ASIC 能量也將繼續在 SASE 戰略中的邊緣接取(Access Gateway)發揮強大的作用。

3. VMware 通過 Nyansa 將 AI 注入 SASE 架構

VMware 也是早期採用 SASE 服務架構的 SD-WAN 供應商之一，主要致力於網路分支路由交換服務。2020 年 1 月，VMware 收購 AIOps 供應商 Nyansa，這為 VMware 的 SASE 平台注入人工智慧(AI）的應用。因為 Nyansa 的技術主要是在提供更好的網路可見性、以便進行監控和補救，VMware 表示 AIOps 的引進，將協助客戶更容易操作和解決駐外分公司、辦事處的網路安全部署問題。此次收購的核心是 Nyansa 的 AIOps 平台，該平台可以將來自各種硬體廠商的網路監控 Log 整合到一個統一的監控儀表板中，無需分別使用 Cisco Prime，Aruba Airwave 或 SolarWinds 等專有監控工具，從而避免了單一廠商不相容問題。也就是無論使用者操作哪種網路硬體設備或無線存取接入點，VMware 都能為用戶提供更佳的網路可見性。

4. McAfee 將 Light Point RBI 應用到 SASE 產品中

2020 年 2 月，McAfee 收購 Light Point Security，以加強其新推出的 SASE 服務產品線。McAfee 計畫將 Light Point 的 RBI 遠端瀏覽器隔離(RBI; Remote Browser Isolation)的技術集成到其安全的 Web 閘道器(SWG)中。另外 McAfee 還推出 Unified Cloud Edge，以此展示其進入 SASE 架構的雄心壯志，據稱該系統可以將 CASB、SWG 和資料丟失防護(DLP)等功能融合到一個雲端安全解決方案中。

McAfee 擁有 Skyhigh 和 Unified Cloud Edge 兩大產品線，可以保護進出雲端資料的安全，但在使用者瀏覽網際網路上，還存在一些安全隱患。因此併入 Light Point 提供可以在雲端沙箱中運行的瀏覽器，這樣設備就不會受到安全威脅影響。

三、結論：SASE 架構為網路服務與安全服務的融合

SASE 架構代表企業網路及安全體系結構性的融合趨勢，它適用於當今疫情之下遠端存取與企業服務上雲的趨勢，將安全性和網路存取融合在一起，可以適用於任何類型的終端存取方式，企業無需在設備上放置代理程式，也不需先連接到 VPN 再將所有流量重新路由導到 Internet，SASE 架構為每個單獨的存取服務帶來安全性。Gartner 預計，到 2024 年，至少有 40% 的企業將採用 SASE 架構的雲端服務。

構建一個完整的 SASE 存取服務平台並非易事，需要廣泛、多樣化技術，目前市場上能提供完整方案的廠商少之又少。這項技術也還在剛起步階段，雖然國內廠商雲端安全的佈局比較少，但是在網路安全設備以及 SD-WAN 相關設備方面，我國廠商都有不錯成績，在 2020 年產值即達 156.9 億台幣，年成長率達 12.4%。雖然大部份屬於替大廠代工或白牌高速網路安全平台、SD-WAN 設備生產。不過在雲端服務持續成長，SASE 存取服務平台帶動邊緣運算設備需求，未來成長仍然可期。

(本文作者為工研院產科國際所執行產業技術基磐研究與知識服務計畫產業分析師)

原文出處：ITIS 智網 http://www.itis.org.tw/