白皮書

最靈活部署的 Fortiet SASE 解決方案

摘要

數位創新、雲端應用以及最近越來越多轉向遠端辦公的趨勢，徹底改變了網路結構。隨著雲端資源，如：軟體即服務（SaaS）應用程式和資料從數據中心轉移到多雲環境的比重越來越高，需要一種新的方法來保護網路存取，特別是針對傳統網路架構中信任建構方式的挑戰。

如今的企業需要在任何時間、任何地點、任何設備上，立即、不間斷地存取網路和雲端資源和數據。這些挑戰在於，企業在數位創新下，同時也帶來了許多問題，例如動態更改網路配置和攻擊面的快速擴展，意味著許多傳統安全解決方案不再能符合企業和用戶所需的安全和存取控制能力。

安全存取服務前端（SASE）是一個新興的企業策略，它將廣域網路結合安全防護。SASE 的目標是支持當今企業的動態、安全的存取需求，這與 Fortinet 多年來一直積極開發和推廣的安全驅動網路策略保持一致。SASE 在確保將安全交付到任何地方扮演著關鍵角色，包括高度行動化的遠端辦公人員所使用的廣域網前端、雲端前端、資料中心（DC）前端、核心前端及終端設備。

客戶對簡單、具彈性、可擴展性、低延遲和安全性的需求，造就了一個 WAN 前端與網路安全結合的市場。[1]

從精確定義 SASE 開始

與任何新興技術一樣，SASE 解決方案的定義仍然在定義中。它該算是雲端產品嗎？還是硬體設備解決方案？ SASE 解決方案涵蓋了哪些技術？雖然 SASE 通常被歸類為雲端服務，但在一些常見情況下，可能需要同時結合設備和雲端服務，才能將 SASE 有效地整合到網路中。

這可能需包括將 SASE 連接性與遠端訪問者的網路存取控制和邊緣安全設備相結合，需要支援 SD-WAN 設備，甚至與各外點的無線網路的技術。因此，除了必要的雲端保護之外，一個強大的 SASE 解決方案還需要支持 IP 網段和合規性要求，如果不將流量導向雲端進行檢查，就無法提供雲端方面的安全保護。

因此，Fortinet 為 SASE 部署提供了最全面、最彈性的解決方案，涵蓋雲端與設備的整合和部署。

SASE 與安全存取有關

從概念上講，SASE 是一種新的嘗試，目的在解決 SD-WAN 供應商所帶來的安全挑戰，這些供應商可能提供了一種創新的網路解決方案，但未能提供全面的安全保護。Fortinet 已透過一個無縫整合安全 SD-WAN 的解決方案來面對這挑戰，我們的解決方案提供了其他供應商都無法實現的強大網路整合技術和安全防護。這些都是我們多年來一直為客戶提供的安全驅動網路和安全織網 Security Fabric 策略的一部分。

Fortinet 提供整合度最高的 SASE 解決方案，包括市場上最廣泛的設備和雲端的安全解決方案。

它從以下基本安全要素開始：

- **具備全功能 SD-WAN 解決方案**

  作為 SASE 解決方案的核心，SD-WAN 需要包括動態路徑選擇、自動的廣域網（WAN）功能以及為業務提供一致性的應用程式和用戶體驗。

- **次世代防火牆 NGFW（設備）或防火牆即服務 FWaaS（雲端）防火牆。**

  SASE 還需要包括涵蓋實體設備和雲端完整的安全性防護。例如，採用遠端辦公的企業需要結合前端安全和內部網段的細分來實

現，以防止來賓或物聯網（IoT）威脅轉移到受限制的公司網路資源，並結合雲端的安全來存取線上或雲端的資源。實體設備、強大處理器的硬體和可擴展的雲端原生安全可以自動分配提供同樣的高性能，為企業提供最大的彈性和安全性。

- **零信任網路存取（ZTNA）**
  ZTNA 是用來識別網路用戶和設備，並對應用程式進行身份驗證。因為 ZTNA 不僅是產品，而是更多的策略，它包含了多種技術協同工作，多因子驗證（MFA）識別所有用戶。在設備方面，ZTNA 包括安全網路存取控制（NAC）、存取政策實施以及與動態網路分段的整合，以限制對網路資源的存取。
  在雲端方面，ZTNA 支持微分割（microsegation）和流量檢查（traffic inspection），以確保用戶之間東西向的安全通信，以及始終保護網路內外設備的安全。透過結合設備和雲端的 ZTNA 服務，企業可以確保安全的存取和策略的執行，無論設備和用戶是在企業內部還是外部。
- **安全網頁閘道**
  安全網頁閘道用於透過執行上網安全和合規策略以及過濾惡意網路流量來保護用戶和設備免受安全威脅。它還可以為網頁存取執行上網使用規範，確保遵守法規，並防止數據洩漏。
- **雲端存取安全性代理程式 - CASB**
  使用 CASB 雲服務使企業能夠控制 SaaS 應用程式，包括保護應用程式存取和消除影子 IT 挑戰。這需要整合企業內部 DLP，以確保預防企業重要資料的丟失。

Figure 1: SASE diagram.

搭配其他技術強化 SASE

SASE 目的在增強和支持數位創新，但如果不整體考慮 SASE 作法，企業可能還會建立一個獨立且需從原有的安全架構分開管理的安全解決方案，這會嚴重限制整個網路的可見性和控制力。因此，除了提供強大的 SASE 解決方案所需的核心元素外，Fortinet 還提供了一些工具，目的在擴充和增強被 SASE 解決方案保護的用戶和設備的安全性。它們也確保整個解決方案可以無縫整合到更大的 Fortinet 安全織網中。

例如，端點安全，端點保護（EPP）和端點檢測和響應（EDR），確保被 SASE 保護的設備本身是安全的。高階虛擬私人網路（VPN）提供安全的資料傳輸和交易處理，同時也面臨當數百或數千個遠端辦公室和用戶需要互連時可能迅速出現的複雜性。此外，安全的 Wi-Fi 和 LAN 控制器可確保了進出網路的流量受到額外的檢查。

每個企業的需求都是不同的，但是，當更全面的網路和安全解決方案提供更豐富的業務價值時，企業如果僅應用那些被視為 SASE “核心” 的技術是不夠因應現今多變的網路挑戰。

有潛力的供應商太多，合格的供應商太少

雖然 SASE 目的在解決當今企業面臨的存取控制和網路安全的挑戰，但問題是很少有供應商有資格提供完整的 SASE 解決方案。例如，他們的工具，尤其是安全元件，幾乎沒有經過測試或認證。這表示消費者無法真正知道他們所購買的安全服務是否能夠在真實環境中保護他們。

即使在高度專業化的網路安全領域，這已經是一個嚴重的問題，在這個領域，當解決方案的效能無法達到業界預期時，供應商有時會選擇退出協力廠商測試和驗證。當供應商提供的 SASE 解決方案的安全保護有多處限制時，又急於利用 “SASE” 作為一個熱門的行銷術語，這個問題會更加嚴重。

Fortinet 優勢

在 Fortinet，我們經常被問到，“你的 SASE 策略是什麼？”

為了使 SASE 運作得更好，它的所有組件都需要整合成單一的系統彼此互相溝通，它的連接性與網路和安全等要素都是如此。對於我們 Fortinet 來說，聽起來如此熟悉的部分原因是，多年來我們一直在提供 SASE 的核心需求，甚至更多，並將它整合為安全平台和安全織網上的一部份。這創造了真正的網路和安全功能的融合，作為安全驅動網路的一部分，進一步加快數位創新的腳步也不犧牲安全保護。

我們有許多希望實現 SASE 的客戶發現，只要稍作調整，他們就已經有了 SASE 的解決方案，這要歸功於 Fortinet 安全織網的強大功能。SASE 努力解決了一個真正的問題。但這與 Fortinet 以前解決過的問題是一樣的。

- 我們是第一家將安全性完全整合到 SD-WAN 的主要安全供應商，我們能夠將多年的安全和網路經驗綜合到一個單一的統一解決方案中。
- Fortinet 開發了世界上第一個 SD-WAN 處理器，目的在加速網路和安全功能，以提供當今複雜的網路環境所需要的效能要求。
- 我們感到自豪的是，Fortinet 的安全工具是當今業界中測試、驗證和認證最多的解決方案。

這表示，為您的企業提供所需的 SASE 解決方案已經是我們網路和安全解決方法的一部分。我們可以使用一系列進階的連接性和安全功能來訂定解決方案，確保您的 SASE 解決方案能夠因應您的需求不斷改變、演進。

Fortinet 安全織網還可以整合和連動您其他部署的解決方案，無論是本地還是雲端。所有這些元素都包含在我們的單一的管理系統中，確保整個網路（包括 SASE 環境）擁有廣泛的可視性和精細控制。

Fortinet 的獨特定位是提供一個完整的 SASE 解決方案，不管是在 WAN 或雲端、資料中心、企業網路和端點等等，確保整個網路的任何位置都能隨地提供安全保護，以實現無縫連接、可視性管理和控制。我們對 SASE 最近的市場趨勢感到興奮，因為它進一步驗證了我們一直以來強力推廣的 Fortinet 安全織網解決方案。在雲端和數位創新的時代，網路和安全必須結合。再也不會回到過去孤立式的架構。Fortinet 就是專為 SASE 時代而設計的。

[1] Frank Marsala, “The Future of Network Security Is in the Cloud,” Gartner, September 13, 2019.

FORTINET

www.fortinet.com

November 30, 2020 11:17 AM

D:\00- (20200427)___Fortinet____Paid Search-DM \wp-FA-fortinet-delivers-the-most-flexible-sase-solution-7312020\wp-FA-fortinet-delivers-the-most-flexible-sase-solution-7312020

742476-0-0-EN