FORTINET

網路領導者安全 SD-WAN 指南

以安全來驅動網路的 Secure SD-WAN
實現敏捷高效又安全的網路邊緣。

目錄

FORTINET

概述

提到數位創新，軟體即服務 (SaaS) 或基礎設施即服務 (IaaS) 的跨雲平台等雲端解決方案，都在為有多據點的企業打造更高效率與營收。然而，這些不斷成長的網路流量因使用 MPLS (多通訊協定標籤交換) 技術，大大增加成本，且效能有限。所以，大多數網路營運廠商都在尋求軟體定義網路 (SD-WAN) 解決方案，取代過時的廣域網路。Fortinet 持續以 Secure SD-WAN 創新功能引領市場，是業界唯一一個提供原生 SD-WAN 解決方案以及整合式先進威脅防護的次世代防火牆 (NGFW) 服務供應商，不僅支援各種應用程式，可同時集中管理，效能更大幅提昇外，更保護來自各方的網路威脅，也因此有成千上萬的客戶選擇 Fortinet 安全 SD-WAN，讓組織擁有最佳的網路與安全體驗！

介紹

隨著數位創新為了要提供用戶最佳體驗，對於頻寬的要求越來越高，SD-WAN 技術雖日趨成熟，但許多解決方案仍尚未完善，像：擴充性限制、缺乏自動化與簡化操作、在跨雲平台以及與 SaaS 整合上乏善可陳等等問題，都導致不良的用戶體驗，也因此浪費了部署 SD-WAN 的價值。相反的，SD-WAN 解決方案需要一套強大的網路與連接工具，以便適應滿足數位創新的動態本質，特別是當組織更積極將網路環境佈局到雲端，或從區域網路佈局到全球範圍或擴大區域辦事處的情況下，這個問題更顯的重要。

Fortinet 提供業界唯一由 SD-WAN ASIC 驅動的安全 SD-WAN，能實現更好的應用體驗、更高的性能和更高的成本效益。

我們需要怎樣的 SD-WAN？

SD-WAN 讓原本的 WAN 服務得到更有效、更經濟地使用，讓跨分佈式組織的用戶能夠優化並創新業務流程，以更彈性地與客戶互動。同時，透過利用具備多重營運商線路的 WAN 創新能夠提供備援、負載平衡和應用程序流量的優化，使 WAN 的管理更具成本效益，這也是為什麼 SD-WAN 在可預見的未來將是一個強勁增長的市場。

為了滿足這一需求，在過去的幾年裏，市場已經出現了許多 SD-WAN 解決方案，但所使用的技術卻不盡相同。

SD-WAN 專家和業界分析人士表示，企業最佳的 SD-WAN 除了取決於組織的應用程式效能要求外，還要有更快的多雲存取到跨雲平台，同時集中管理，讓操作簡化以便降低複雜性，而且因為組織的分支佈局，經由 SD-WAN 頻寬的連接會讓組織資訊直接暴露在網路上，這仍需要次世代防火牆與 SD-WAN 的整合以解決資安問題。

所以為了滿足以上的種種需求，現代企業需要一個全面的 SD-WAN 解決方案，而 Fortinet 安全 SD-WAN，是目前業界唯一一個內建具有安全性和效能功能的 SD-WAN，可以靈活地在任何規模的企業中進行部署。

Fortinet 提供最佳的 SD-WAN 安全驅動型網路

Fortinet 安全 SD-WAN 採用了 Fortinet 次世代防火牆，取代各自獨立的 WAN 路由、WAN 優化和安全設備，例如：防火牆和安全 web 閘道 (SWGs) 的部份。這個方法還包括應用程式感知、智慧路徑選擇和對 VPN 的廣域網路覆蓋支援，不僅提供業界最佳的效能，而且 Fortinet 以安全來驅動網路的 Secure SD-WAN，透過快速應用程式識別和智能選路，可以實現卓越性能。

Fortinet 安全 SD-WAN 提供：

- **以精準檢測提供最佳應用體驗**
- **基於應用選路提昇高效業務策略**
- **來自 FortiGuard 研究室持續地應用數據庫更新**

提高服務級別的應用程式認知

Fortinet 安全 SD-WAN 是由新的 SOC4 專用晶片 (ASIC) 驅動，ASIC 可提供更快的應用程式控制和無可匹配的應用程式識別效能，這包括深度安全通訊端層 (SSL) 和傳輸層安全性 (TLS) 檢查。加密檢查方面還包括檢查封包的能力，好讓 SD-WAN 能够正確的路由通信流量。

從技術上來說，SD-WAN 的工作原理是在任何時間點通過最有效的 WAN 連接路由應用程序來工作，為了確保最佳的應用程序效能，SD-WAN 解決方案必須能夠識別廣泛的應用程式並在非常精細的級別上應用路由策略，如果沒有這些功能，當在使用 SaaS 服務、視訊和語音等等功能時，可能會減慢、降低或阻礙終端用戶的生產力。

為了解決這些問題，Fortinet 安全 SD-WAN 擁有一個應用程式控制資料庫，這之中包含了 5,000 多個應用程式識別 (再加上來自 FortiGuard 研究室威脅情報服務的定期更新)。

Fortinet 安全 SD-WAN 從第一個流量封包中即開始進行識別和分類應用，甚至是來自加密的雲端流量。

Fortinet 安全 SD-WAN 可準確辨識超過 5,000 個應用程式並優化其路由。

Fortinet 次世代防火牆可根據業務重要程度設定識別應用程式，比如：業務關鍵型的應用程式 (Office 365、Salesforce、SAP)、一般生產力的應用程式 (Dropbox) 或社交媒體 (Twitter、Instagram 等等)，這些應用程式均可被賦予不同的路由優先順序，也可以在更深層次為子應用程式 (例如 Office 365 中的 Word 或 OneNote) 給予單獨的策略與路由應用。

這種對流量模式與利用率的深入和廣泛的應用程式級別可見性，讓組織可根據業務的需求，為 WAN 的資源分配提供了更好的方式。

展現 WAN 效率毫不費力！

Fortinet 安全 SD-WAN 大大簡化了轉換舊有 WAN 邊緣基礎架構的過程，提供更強化的應用程式效能、更好的用戶體驗和更好的安全性。一旦設置了應用程式的關鍵性、效能要求、安全性原則和其他考慮因素，Fortinet 安全 SD-WAN 解決方案即可直接接管，更重要是，擁有 SOC4 ASIC 的 Fortinet 次世代防火牆，具有比競爭對手快 10 倍的安全性能。[1]

在 WAN 效率方面，Fortinet 安全 SD-WAN 的關鍵功能包括：

自動路徑優化

應用服務感知功能可以根據特定的應用程式和用戶在網路頻寬的使用上給予優先級選路。新的 SOC4 ASIC 為 Fortinet 安全 SD-WAN 提供業界最快的應用導引，可針對特定的業務環境動態選擇最佳的 WAN 連接，輕鬆定義 SD-WAN 服務級別協議 (SLAs)。對於中低優先級的應用程式，組織可以指定品質標準，由 FortiGate 選擇相應的鏈路。而對於高優先順序和業務關鍵型的應用程式，組織可以根據封包抖動數 (Jitter)、封包遺失和延遲指標的組合定義嚴格的服務級別協定。

自動故障轉移

當主要 WAN 路徑降級時，多路徑技術可以自動故障轉移到最佳可用網路。這種自動化內建於 Fortinet 次世代防火牆中，可以降低終端使用者的操作複雜性，提高網路體驗品質和生產力。

WAN 路徑修正

WAN 路徑修正是利用前向糾錯 (FEC) 來克服較差或嘈雜不良的網路連線。這樣做不僅提高資料傳輸的可靠性，並為語音、視訊等應用程式服務提供更好的用戶體驗。FEC 可將糾錯資料增加到出站的流量中，允許接收端可從傳輸過程中遺失的封包和其他錯誤中恢復數據，提高即時連線的品質。

優先應用設計

Fortinet 安全 SD-WAN 可針對特定的應用程式設定 QoS 優先級順序，同時對可能影響效能和終端使用者體驗的非關鍵應用程式進行速率限制，確保頻寬最佳利用率。

通道頻寬 (Tunnel bandwidth) 調配

對於需要更大頻寬的應用程式，Fortinet 安全 SD-WAN 透過組合兩個重疊通道來實現基於封包的負載平衡和傳輸，以最大限度地提高網路容量。

簡化管理並擁有業界最佳的總體擁有成本 (TCO)

在將 SD-WAN 邊緣設備佈局到眾多的遠端據點和分支機構時，技術人員通常有限，要架設到好還要兼顧資訊安全並不容易，且費用通常很昂貴，也讓網路工程和營運領導者常常陷入窘境。另外一個方面，運送提前設定好的設備也不安全。此外，一旦到了要部署邊緣設備時，資訊人員更必須同時兼顧網路的優化與資安兩個不同層面的問題，如此全面兼顧實在不容易！不過，Fortinet 安全 SD-WAN 可同時解決這兩個問題，這為企業與資訊人員帶來極大的方便，更降低了總體擁有成本 (TCO)，解決部署和管理的問題。

Fortinet 安全織網管理中心，為客戶提供有效的網路營運和靈活的網路管理。[2]

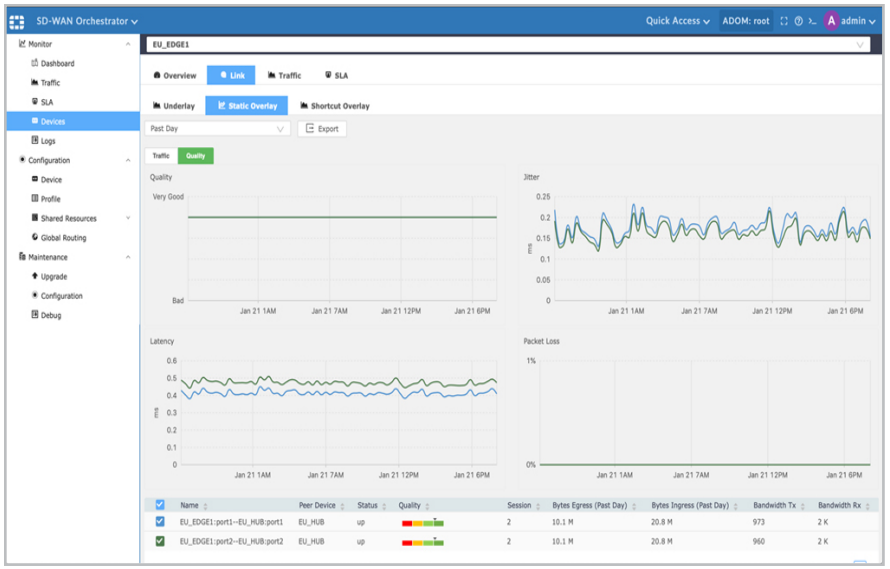
零接觸配置

Fortinet 安全 SD-WAN 的簡化部署功能使企業可將未設定的 Fortinet NGFW 設備傳送到每個遠端位置。電源接通後，FortiGate 將自動連接到 FortiCloud 中的 FortiDeploy 服務，並在幾秒鐘內對遠端設備進行身份驗證，並將其連接到中央 FortiManager 系統，非常方便！

集中式組態管理與監看

Fortinet 安全織網管理中心可整合集中查看組織中所有部署的 Fortinet 設備。Fortinet 安全 SD-WAN orchestrator 提供簡化的工作流程，只需簡單的點擊 / 步驟，即可完成部署和策略更新。

SD-WAN orchestrator 可自動建立與管理 Full Mesh VPN 覆蓋 ，確保各端點之間安全連接，借助流程引導、自動啟動相關步驟，這讓 IT 人員減少了在基礎架構上的部署時間，這可讓花費的時間從數月縮短到數分鐘。



SD-WAN 報告和分析

SD-WAN 報告針對 WAN 連結可用性、效能 SLA 和運行時應用程式流量以及歷史統計資料加強分析，這讓技術團隊能夠了解並快速解決網路問題。

Fortinet 安全織網管理中心為應用程式可見性和網路效能提供高階遙測，實現更快的分辨率並減少技術支援的負荷。按需要，SD-WAN 報告可提供對威脅態勢、信任級別和資產存取做更深入的了解，而這些行為是合規性的強制要求。

這些功能包括 SD-WAN 頻寬監測報告與資料集，可客制的 SLA 警報服務級別協定 (SLA) 日誌記錄和監控，以及應用程式使用情況報告和資訊總覽等等。它還可為 SD-WAN 的事件提供自我調整響應，以及跨應用程式和介面的 SLA 事件日誌記錄與歸檔。

分佈式雲端低延遲存取

提供低延遲的雲端資料存取來實現輕鬆協作功能，Fortinet 安全 SD-WAN 不僅提供即時多雲存取，還可快速採用共享應用程式如 Office365，它的內建安全為這些應用程式增加了另一層安全存取，同時透過公共網路來提供低延遲的連接，因此它們能夠成為受信任和可靠的 WAN 基礎設施的一部分。

這一特色尤其重要，因為針對在遠端工作的員工們，很多時候他們需要與家人或同事一起進行語音或視訊會議或使用功能豐富的雲端應用，雖然有些遠端應用程式提供了更強大的語音和視訊功能，但它們同時也會要求更高的可用頻寬，在大多數時候還需要對流量進行加密，而這為流量檢查帶來了更大的壓力。

Fortinet 安全 SD-WAN 具有子應用程式的智慧檢測功能，並以線速 (Line Rate) 為加密應用程式提供 SSL 檢查，不只確保這些應用程式能被引導到效能最佳的 WAN 鏈路，更提供最佳網路效能！

對於需要透過公用網路連結進行安全連結的用戶，只需按一下即可輕鬆設定 VPN。無論在本地或雲端，所有程序都節省了時間並簡化了 SD-WAN 管理，更減輕了技術團隊的壓力。Fortinet 提供了唯一可以從同一管理控制台來管理 SD-WAN 網路、安全和存取層控制的解決方案。

業界領先的總擁有成本 (TCO) 優勢

隨著雲端計算、行動應用、及全球化等轉向公共頻寬的發展趨勢，意味著昂貴的 MPLS 可被更具成本效益的選項取代。[3] Fortinet 安全 SD-WAN 提供每 Mbps 計算，業界領先的總擁有成本 (TCO) 優勢，可在六分鐘內零接觸下快速調配齊下網路資源的特色，且搭配 Fortinet transport-agnostic 解決方案，讓企業可以透過雙主 (Active/Active) 模式下來活用整個網路頻寬。

Fortinet 以安全的 SD-WAN 創新引領市場，從居家辦公到分支機構再到分散式雲端。[4]

由數位安全驅動的網路

Fortinet 實現了同類最佳的認證 SD-WAN，同時包含高性能與資安防護。Fortinet 次世代防火牆採用 SOC4 ASIC 晶片技術 ，提供業界最快的 SD-WAN 安全效能。在 2019 年 NSS 實驗室 “軟體定義的廣域網路測試報告” 中，Fortinet 連續獲得 “推薦” 評級。[5]

具體而言，Fortinet 安全 SD-WAN 具有強大的 SD-WAN 資安防護，包括其他業界 SD-WAN 外加防火牆的解決方案中不常見的第 3 層至第 7 層的安全控制：

- 完整的資安保護，從防火牆、防毒、入侵防禦系統 (IPS) 到應用程式控制。
- 高輸送量安全通訊端層 (SSL)/ 傳輸層安全 (TLS) 深度封包加密檢查，確保不會犧牲輸送量來實現完全的資安保護。
- Web 過濾功能可在不需要單獨的安全 Web 閘道 (SWG) 設備下提供網路安全。
- 雲端應用的高廣域網路效能，具有卓越的 VPN 覆蓋效能，可提供卓越的用戶體驗和低延遲效益。

支援安全 SD-WAN 的 Fortinet 次世代防火牆提供監視防火牆的規則和策略並注重最佳實踐，改善組織的整體安全。這有助於簡化對安全標準以及隱私法律和產業法規的遵守。自動化的稽核和報告工作流大符節省員工的時間，同時降低了遺漏和錯誤的風險。

啟用 SD-Branch

許多企業分支機構正決定同時更換廣域網路和區域網路的設備並且傾向深度整合與簡化分支營運管理。然而使用單獨的廣域網路和區域網路，不僅新增了分支機構網路的複雜性，更代表了有許多的設備需要部署和更新，及多個管理控制台需要管理，如此不僅降低了操作的可見性和增加管理複雜度，同時還增加了駭客利用的安全性漏洞的機會。為了解決這些挑戰，Fortinet 安全 SD-WAN 擁有包括對存取層的加速安全擴展，可大力幫助實現設備的安裝與轉換。

在動盪的 SD-WAN 市場中，Fortinet 是以安全為首的最佳選擇

隨著雲端應用和語音視訊等工具對分佈式企業越來越重要，Fortinet 安全 SD-WAN 可以幫助企業數位創新，而且不會限制應用程式效能、影響終端使用者的生產效率或將數據置於風險之中。

Fortinet 安全 SD-WAN 具有可擴展性，可幫助企業自信地支援更多遠端據點、支援對頻寬更敏感的業務關鍵型應用程式、更多雲端服務以及各據點所需的任何其他內容。

Fortinet 安全 SD-WAN 從金融、零售、製造到客戶服務，已在全球範圍內廣泛被應用。無論他們需要支援幾百個行動裝置還是數以萬計的據點，Fortinet 安全的 SD-WAN 都在實現最佳的安全防護與 SD-WAN 功能的最佳組合。

1 “Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report,” Fortinet, June 19, 2019.

2 “ Fortinet Leads the Market with Secure SD-WAN Innovation.” Fortinet, May 2020.

3 “SD-WAN Infrastructure Market Posied to Reach $5.25 Billion in 2023”, July 2019.

4 “Learn more about a Fortune 500 customer that achieved a 65% cost reduction,” Fortinet, April 24, 2020.

5 “ Ibid.

FORTINET

www.fortinet.com/tw

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

372656-0-0-EN

August 26, 2020 11:03 AM

eb-network-leaders-guide-to-secure-sd-wan_051520_1145