解決方案簡介

提供員工大規模的安全遠端連線

摘要

組織難免都會面臨許多不同的潛在緊急情況。如何讓組織能夠在危機中維持營運不間斷，對每一個組織而言都是非常重要的課題。

當一個組織在制定有關的業務推行不中斷的相關計畫時，都要考慮當遇到無法正常營運的狀況下，該如何利用遠端工作模式來確保業務的持續運作。

Fortinet 的 FortiGate 次世代防火牆遠端作業解決方案，內建 IPsec 虛擬專用網路 (VPN)，可讓在遠端工作的同仁們能夠安全連接回公司網路。透過由 FortiClient 的端點保護與 FortiAuthenticator 多因素身份驗證 (MFA)，讓組織在資安保護下遠端作業連線，讓業務不中斷。

由於停電、疾病或洪水來襲等類似不可預期的因素都可能造成員工發生危險，造成生命財產的損失，讓組織無法維持運作。遠端作業需要的網路安全與資安防護是任何組織中不可獲缺的組成部分，這也是組織裏業務持續推行計劃和災難恢復計畫裏非常重要的一部份。

在這些不可預期的場景中，組織必須能夠支援同時兼顧遠端網路的連線品質與安全，Fortinet 擁有超過 40 萬名客戶，在現有的技術已經包含了大多數企業想要的功能。FortiGate 次世代防火牆整合了對 IPsec VPN 的支援，為在備用工作地點工作的員工提供了網路安全連線的保障。

遠端工作可將員工的非生產性時間平均減少 27%。[1]

遠端工作員工平均每年比現場員工多工作 16.8 天。[2]

有 85% 的員工聲稱遠端工作可讓他們提高最高生產力。[3]

遠端工作為企業提高 95% 員工在職率。[4]

讓 FortiGate 次世代防火牆保護遠端作業的同仁

每個 FortiGate 次世代防火牆中的 IPsec 和 SSL VPN 中提供非常靈活的操作整合，在遠端工作的同仁可以用免安裝軟體的網頁模式 (Clientless) 體驗 SSL VPN 強大與安全的服務，也可以透過 FortiClient 端點安全解決方案，內建的胖客戶端 (Thick Client) 界面可以取得其它功能，而高階用戶和超級用戶們則可從 FortiAP 或 FortiGate 次世代防火牆中獲得更多有用的功能。

Fortinet 解決方案的設計從最初的購買到完成設定的操作都非常方便，FortiGate 次世代防火牆和 FortiAP 無線接入點的零接觸部署功能，讓在即將佈署遠端據點的設備可以在發貨前先進行預先設定，到現場作業直接自動完成對接，輕輕鬆鬆完成設備設定。而且 FortiGate 次世代防火牆可以作為實體和虛擬設備使用，亦可在公共和私有雲端中運行。

Fortinet 安全織網利用統一的 Fortinet 作業系統和開放的應用程式介面 (API) 環境來建立廣泛的、整合的、自動化的安全體系結構，使用 Fortinet 安全織網，可以從一個單一操作視窗進行監視、管理組織的所有設備，包括那些部署在遠端支援遠端工作的設備。透過部署在總部環境中的 FortiGate 次世代防火牆或 Fortimager 集中式管理平臺，安全團隊可以實現對所有連接設備的完全可見性，而無論其部署情況如何。

在自然災害或其他干擾正常營運的事件發生時 ,組織必須能夠迅速進入完全遠端的工作模式。表 1 顯示了每種型號的 FortiGate 次世代防火牆可以支援的同時連線的 VPN 用戶數。

除了透過 VPN 對傳輸中的數據進行加密之外，Fortinet 解決方案還提供了許多保護遠端員工的連線安全，這些功能包括：

- **多因素身份驗證**
  FortiToken 和 FortAuthenticator 支援遠端員工的雙因素身份驗證。
- **資料丟失預防 (DLP)**
  FortiGate 和 FortiWiFi 為遠端工作人員提供 DLP 功能，這對於經常存取公司機敏資料的遠端工作管理人員非常重要。
- **高階資安防護**
  FortiSandbox 可以在沙箱環境中將其到達目的地之前對惡意程式和其他可疑內容進行分析。

- **無線連線**
  FortiAPs 在遠端工作地點提供安全無虞的無線存取，在單一的視窗中進行全面整合配置管理。
- **網路電話**
  FortiFone 是一種安全的 IP 語音 (VoIP) 電話解決方案，其流量由 FortiGate 次世代防火牆進行安全、管理和監控，提供軟體用戶端和多種硬體選項功能。

型號	同時 SSL VPN 用戶數	同時 IPsec VPN 用戶數	納入管理的FortiAP數(Tunnel模式)
100E	500	10,000	32
100F	500	16,000	64
300E	5,000	50,000	256
500E	10,000	50,000	256
600E	10,000	50,000	512
1100E	10,000	100,000	2,048
2000E	30,000	100,000	2,048
較大型號 *	30,000	100,000	2,048

*3300E 支援 1024 個通道模式接入點

表格 1:FortiGate 次世代防火牆各種型號支援的同時 VPN 連接數。

支援遠端工作的 Fortinet 產品的範例

在遠端工作時，並非組織中的每個員工都需要相同級別的權限。Fortinet 為每個遠端工作的員工提供量身定制的遠端工作解決方案：

1. 基礎遠端工作員工

基本的遠端工作的員工只需要從遠端工作網站存取電子郵件、網路、進行電話會議、有限的文件共享和特定功能使用 (財務、人力資源等)。這包括存取雲端中的軟體即服務 (SaaS) 應用程式，如：Microsoft Office 365，以及與企業網路的安全連接。

基本在遠端工作的員工可以使用 ForticClient 整合 VPN 用戶端軟體來連接，並使用 FortiToken 身份驗證來進行多因素身份驗證。特別提醒：當高階用戶和超級用戶從遠端工作地點進行漫遊時，他們將恢復成基本的遠端工作的員工模式。

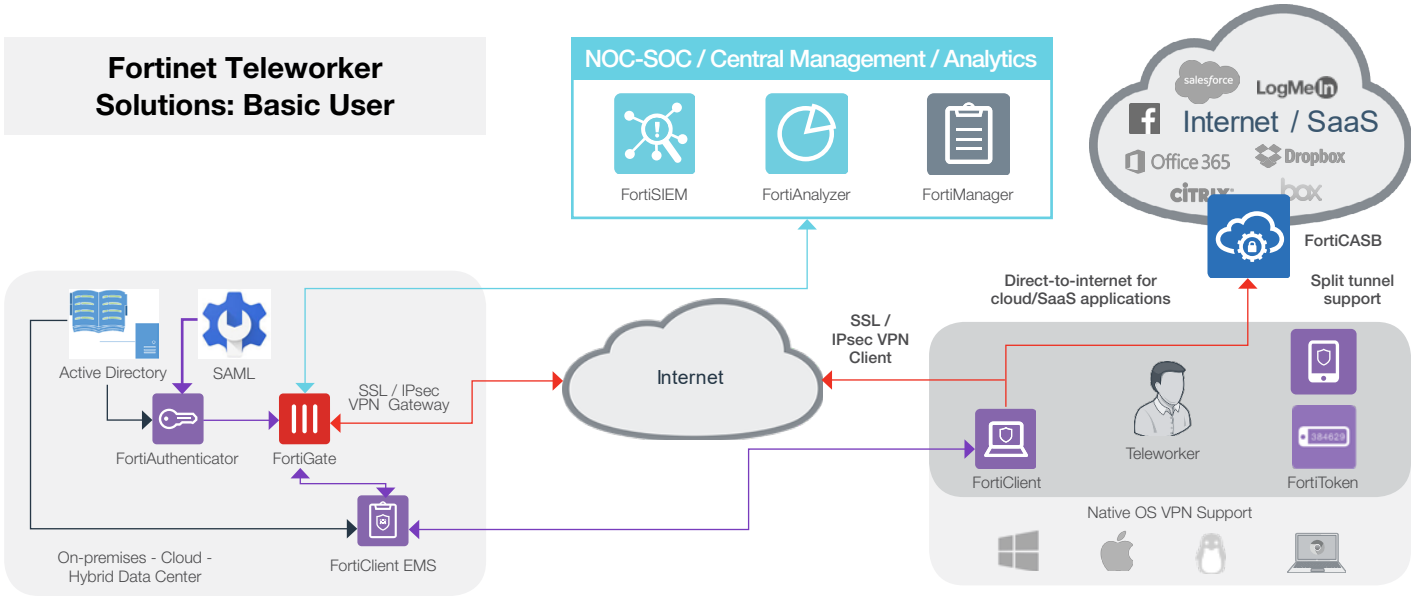

圖 1：Fortinet 基本遠端工作的概念性關係圖

2. 高階用戶

高階用戶是在遠端工作時需要更高階級別存取公司資源的同仁，包括系統管理員、IT 支援技術人員和應急人員等員工。

對於這些高階用戶，在他們的備用工作據點部署 FortiAP 可以提供所需的存取和安全級別，這使透過一個安全通道連至公司網路的安全無線連線成為可能。FortiAP 可使用零接觸配置 (ZTP) 進行部署，並由辦公室的 FortiGate 次世代防火牆統一管理。如果需要部署公司電話，只需將其插入 FortiAP 即可連接回總公司。

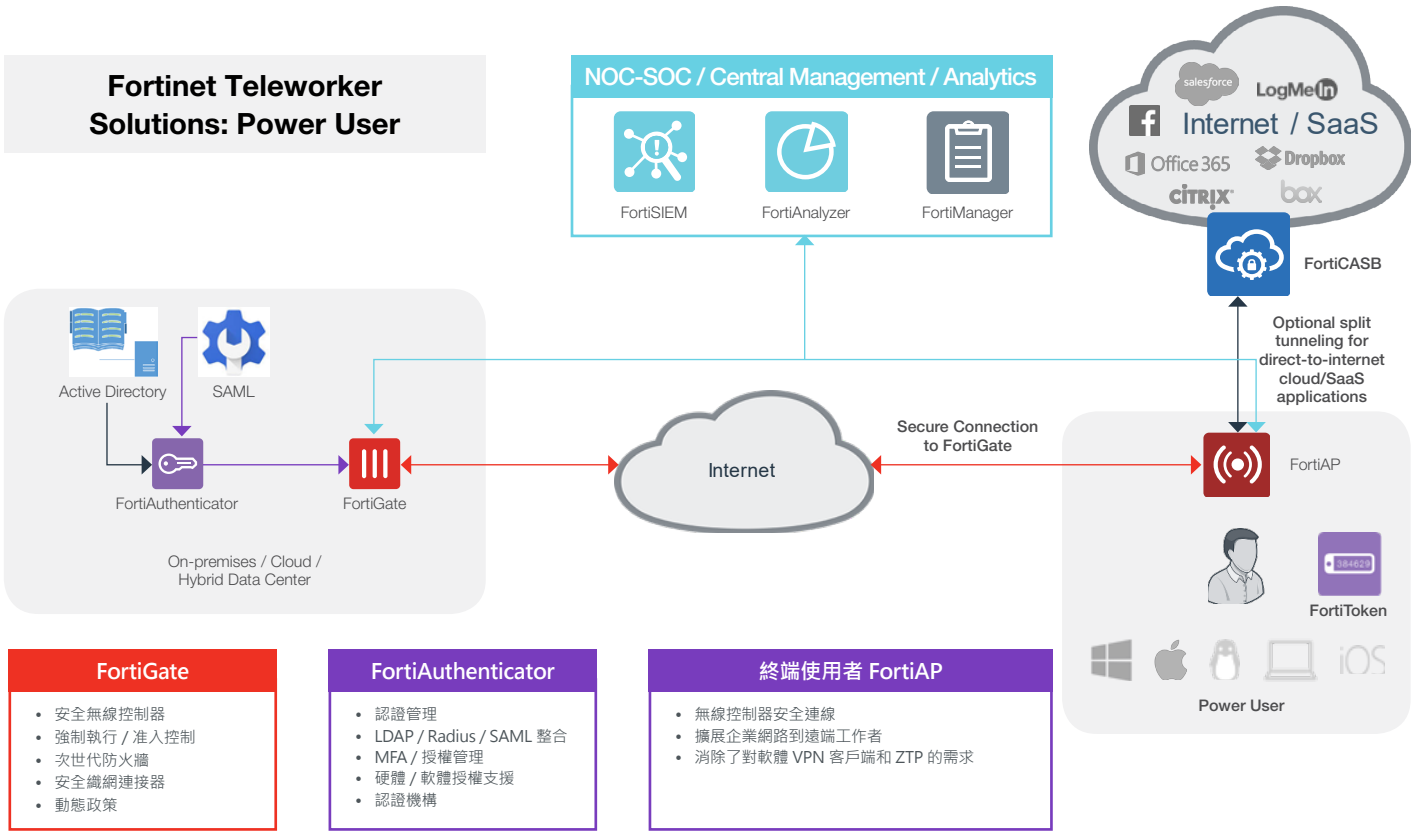

圖 2：Fortinet 高階用戶全國部署的解決方案。

3. 超級用戶

超級用戶是需要進階存取公司機密資源的員工，即使在異地辦公也是。他們經常需要處理極其機敏的公司資訊，這些員工身份包括擁有特權存取權限的管理員、技術支援人員、持續計劃中的關鍵合作夥伴、應急人員和公司管理階層等等。

對於這些超級用戶，應將其備用工作地點當成備用辦公室看待，他們需要與一般遠端工作者一樣的基本遠端辦公功能，同時也需要額外的解決方案。FortiAP 可與 FortiGate 次世代防火牆或 FortiWiFi 設備整合，實現內建的 DLP 安全無線連接。FortiFone 提供軟體或是硬體類 VoIP 網路電話，透過 FortiGate 次世代防火牆或部署在總部位置的 FortiManager 集中管理平臺進行管理和保護。

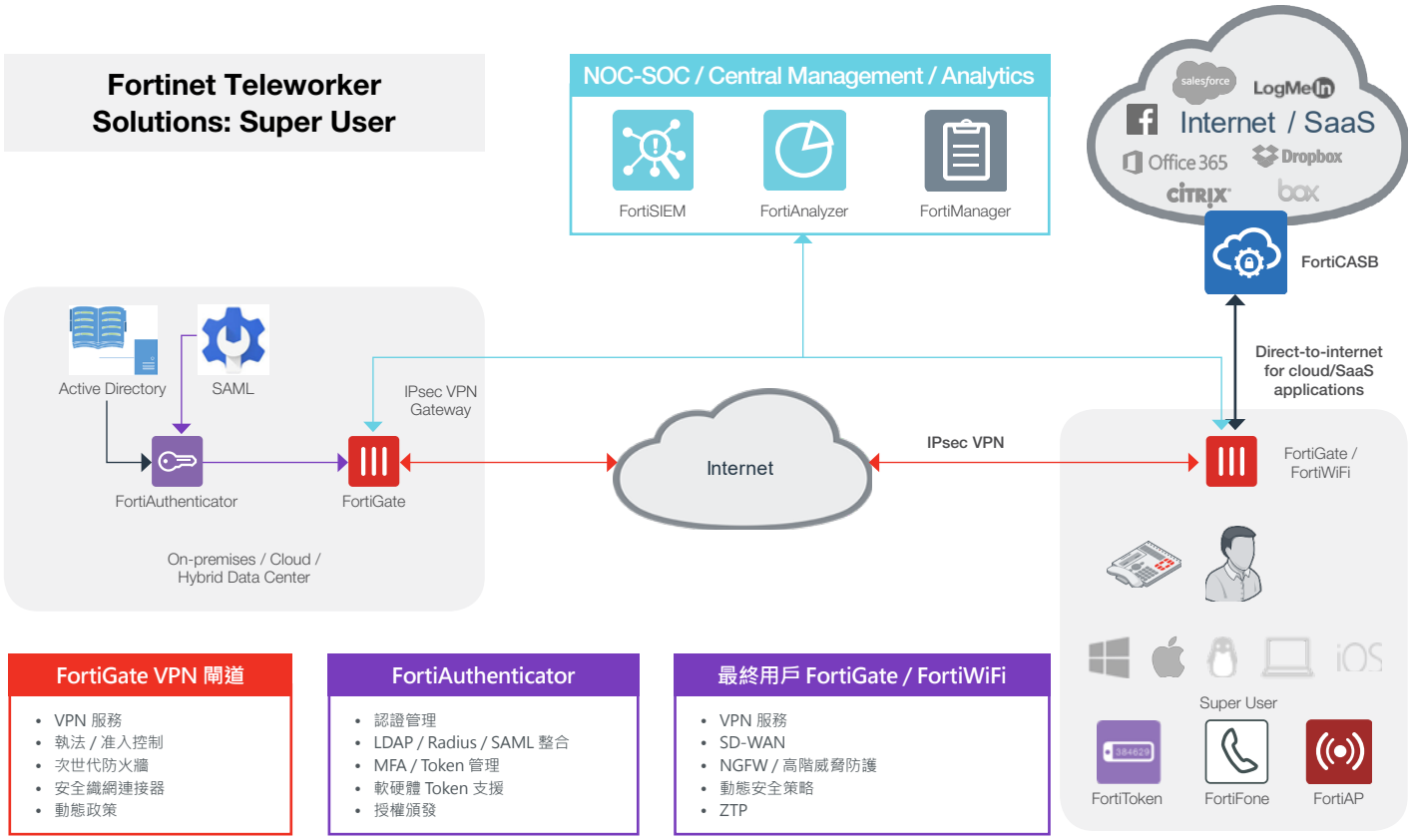

圖 3：Fortinet 超級用戶的全國解決方案相關部署。

支援遠端勞動力

Fortinet 解決方案可以很輕鬆的部署到遠端工作點。然而，組織也需要工作現場或雲端中的資源提供資安服務，來支援在遠端工作的員工。

雖然許多組織已經準備好了這些資源，因為它們是現有的安全體系架構的一部分。而 FortiGate 的次世代防火牆，它能夠在企業範圍內以最小的效能影響來檢查加密和通信的流量，這還包括一個 VPN 閘道的整合，做為在遠端工作的員工的加密連接的端點。

FortiGate 次世代防火牆也包含與 IT 通用基礎設施的整合，包括企業控制器服務，如 Microsoft Active Directory(AD)、MFA 和單點登錄 (SSO) 解決方案。FortiAuthenticator 為身份驗證解決方案提供了一個單一的集中整合點，並支援協力廠商解決方案以及 FortiToken，後者提供了硬、軟、電子郵件和行動授權選項。

因為 FortiGate-VM 能夠在 AWS 或其他大型雲端環境上以 20Gbps 的速度進行運作，不管是使用 ForticClient 還是其它不同的 VPN 用戶端，都可以充份支援數千個遠端連線，且許多據點都拿來連接公有雲安全服務中心來存取雲端中的應用程式。它還可以透過離自己最近的雲來存取最近的本地應用程式，並可在私人資料中心，提供從雲端到資料中心的高速資料傳輸的持續支援，反之亦然。

在管理遠端和分佈在各地的員工時，集中化的安全可見性和管理非常重要。所有的 Fortinet 解決方案都可以透過 Fortinet 安全織網整合，讓組織的資安團隊能夠使用 FortiManager 來實現單一視窗可視性與控制，使用 FortiAnalyzer 執行日誌聚合和安全分析，使用 FortiSIEM 來快速檢測和響應潛在安全問題。

運用 Fortinet 解決方案實現全面的資安整合

Fortinet 安全織網實現了組織遠端作業的無縫整合。所有的 Fortinet 解決方案都透過 Fortinet 安全織網進行連接，實現單一視窗的可視性、配置與監控，以及開放式的 API 環境、DevOps 社區支援，再加上大型的安全織網生態系統，整合支援 250 多個第三方解決方案，實現全面的資安整合。

而這當組織在準備業務持續計劃的時候相當重要。一個組織團隊很可能在沒有被告知的情況下被迫轉換成遠端工作模式。組織安全架構的單一視窗可視性和管理，可以確保在緊急過渡到遠端模式時不會影響組織的網路安全，而引發資安危機。

以下解決方案是 Fortinet 安全織網對於遠端工作安全支援的部分：

- **FortiClient**
  FortiClient 可透過可視性的整合、控制和主動防禦來加強端點安全，使組織能夠即時發現、監控並評估端點風險。
- **FortiGate**
  FortiGate 次世代防火牆擁有特製的網路安全處理器，提供組織頂級的保護、點對點的可視性和集中控制，並且可對明文和加密流量進行高性能的檢查。
- **FortiWiFi**
  FortiWiFi 無線閘道將 FortiGate 次世代防火牆的安全優勢與無線接入點相結合，為在遠端工作的員工們提供網路與安全整合解決方案。
- **FortiFone**
  FortiFone 透過由 FortiGate 次世代防火牆進行加密保護和管理的 VoIP 通訊協定提供統一的語音通訊。FortiFone 軟體用戶端介面允許用戶直接從行動設備撥打或接聽電話，並可存取語音郵件、檢查通話歷史記錄與查詢組織的目錄。並有多樣的硬體型號提供選擇。
- **FortiToken**
  FortiToken 透過硬體 Token，或是行動應用程式，提供第二道認證程序加強身份驗證。
- **FortiAuthenticator**
  FortiAuthenticator 提供集中的身份驗證服務，包括單點登入服務、憑證管理和訪客管理。
- **FortiAP**
  FortiAP 可透過 FortiGate 次世代防火牆或雲端來輕鬆管理，為分佈式企業和遠端工作人員提供安全無線存取。
- **FortiManager**
  FortiManager 提供整個企業單一視窗管理以及策略控制，辯識網路流量中的威脅。包含高階攻擊防護的功能以及多達 10,000 個 Fortinet 設備的擴充，讓資安人員完全深入了解組織網路的資安狀況。
- **FortiAnalyzer**
  FortiAnalyzer 提供網路安全和日誌管理的報告分析，幫助資安人員進行資安檢測和漏洞預防的改進。
- **FortiSandbox**
  FortiSandbox 沙箱解決方案，透過提供先進的檢測、封鎖目標、攻擊自動化防護、可操作的有用資訊以及彈性的部署方式的強大組合，阻止針對性的攻擊避免後續的資料丟失。以雲服務的方式提供並可以在大部份的 FortiGuard 訂閱服務中找到。

以安全為基礎， 確保業務的持續推行

讓業務持續推行和為災難恢復做好準備對任何企業來說都非常重要。其中一個重要的組成，就是能夠在幾乎沒有預知的情況下，就可以達成並支援大部分或完全的遠端作業。

在制定業務持續計畫時，必須確保組織有足夠的資源能保障遠端員工們的安全。Fortinet 解決方案非常容易部署和設置，讓組織能夠輕鬆達成完全的安全、可見和管理，而不管其身處的環境如何。

1 "The Benefits of Working From Home," Airtasker, September 9, 2019.

2 Ibid.

3 Abdullahi Muhammed, "Here's Why Remote Workers Are More Productive Than In-House Teams," Forbes, May 21, 2019.

4 Ibid.

FORTINET

www.fortinet.com/tw

September 28, 2020 5:52 PM

618770-0-0-TW