FORTINET

確定遠端勞動力的大規模支援與安全需求

設計安全的遠端工作

目錄

概述

做為企業營運持續性計劃的一部份，各組織應該為在遠端工作的同仁們提供安全與技術支援，因為工作環境與現場工作的情況截然不同，網路的安全與順暢將是組織一個新挑戰。

所以，保護遠端工作的員工和總部網路，都需要安全解決方案。對大多數員工而言，大部份或許只需要安全存取公司網路和雲端等相關應用，這方面只要用 VPN 存取和多因素身份驗證 (MFA) 即可達成。然而網路系統管理員和管理人員可能需要持續連接和安全通信等解決方案的額外需求，所以組織總部的網路必須能夠提供更多的支援，這就將需要更高階的外圍安全防護網等強大的解決方案。

介紹

當組織可以支援在遠端工作的員工時，這樣可以幫助改善組織的業務可持續計劃。它能使組織在自然災害或疾病大流行發生等許多不可預期的情況下時，讓員工無法到現場工作時有能力進行調配。

因事件來的突然，在這種情況下，每個組織單位可能被迫要快速轉換成大部份或是全部遠端工作模式。然而，在規劃或轉換到遠端工作時，不僅要考慮網路本身的問題，遠端工作所帶來的資安問題，更是要特別注意。

滿足基本遠端工作需求

每個組織下的員工可能對遠端工作環境有不同的要求。然而，所有在遠端工作的員工都有一個基本需求，就是確保與公司網路的連線是一個安全、經過驗證的連線。其中包括存取 VPN 和强大的身份驗證，這樣才有法保護帳戶的安全與保障。

VPN 虛擬專用網路

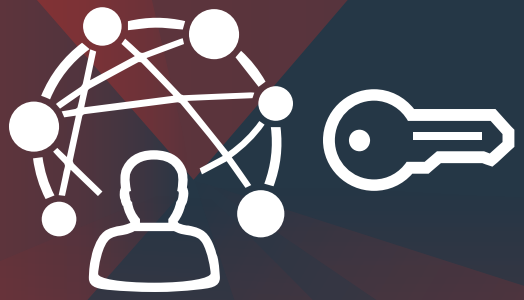
當員工在遠端工作時，員工將使用家裏的網路來處理公司的敏感資料。要做好資安防護，保護這些資料免遭駭客入侵，就需要有確保與公司網路連接的資訊防護能力。

在遠端工作的員工需要能夠存取 VPN，讓他們的機器和公司網路之間提供直接加密連接，這不只可大幅加強公司機敏資料的機密性和完整性，還確保員工與公共網路之間的所有通信都受到組織資安建設的監控和保護。

多因素身份驗證

隨著員工在家工作，被盜用的登錄憑證與對無人看守機器被使用的一起發生的情況下，發生未經授權的帳戶存取的可能性將增加。在這種情況下，許多檢測異常存取模式的功能可能不適用如認證的時間與地點等，因為員工的工作模式由於在家辦公而發生變化。

與傳統的使用者名和密碼相比，保護對公司網路、資源和資料的存取需要更強大的身份驗證解決方案。我們應該為所有遠端工作人員頒發安全的身份憑證 (authentication token)。 MFA 憑證的選項包括諸如密鑰之類的實體設備或行動應用程式之類的軟體解決方案，可用在使用者建立與公司網路的 VPN 連接或存取公司的敏感資源驗證身份。



PCI DSS 遠端工作指南：要求擁有存取持卡人資料的同仁必須透過 VPN 進行並使用多因素身份驗證。[1]

支援超級遠端工作使用者

雖然許多在遠端工作的員工可以透過 VPN 連線和 MFA 憑證進行工作，但還有其它層級的員工有額外的要求，比如：高階使用者 (包括網路系統管理員和管理人員)，他們需要更高階的遠端辦公室方案來執行他們的工作，如：企業網路的持久連接和安全電話解決方案。

持久連接

有一些使用者，如網路系統管理員和資安人員，需要更靈活和持久地存取公司網路。這些員工可能有多個設備必須連結，或者需要不受超時限制的長時間連接。

透過部署無線接入點，可以滿足在家工作者的高階使用者需求，為存取企業網路提供可靠的 VPN 連線。為了確保安全連接，該無線接入點應與次世代防火牆相結合，除了提供流量檢測，還可以擁有存取管理和進階資安防護。

安全電話解決方案

在遠端工作時，為了保護敏感的通訊和公司資料，工作人員，尤其是公司的管理階層應需要使用安全電話解決方案。否則，公司就有可能因遭遇竊聽風險，讓惡意行動應用程式入侵而暴露敏感數據。

為非現場的工作人員提供安全電話的有效方法是利用 IP 語音（VoIP）通話。如果使用者已經可以存取安全 持續和可靠的 internet，則透過此路由的語音通信量只需最少的額外支出。這也使組織能夠監視語音通信量，並在網路週邊掃描它，查找潛在的攻擊 VoIP 軟體漏洞的惡意內容。

為在遠端工作的員工提供的電話解決方案應該要為他們提供商務電話的所有功能。這樣可以最大限度降低員工使用個人設備進行商務通信的可能性。重要的選項包括電話的撥打和接聽、語音郵件存取、檢查通話歷史記錄及存取組織的電話簿等等功能。

有 72% 的 CEO 工作都花在會議上，所以遠端辦公的資安通信必不可少。[2]

源端的安全性和穩定性

遠端工作的安全方案其實不只在使用者端，越來越增加的遠端工作的員工也對組織總部帶來新的安全威脅與網路品質需求。

為了設計能讓業務持續推行的遠端工作系統，基本上總部的網路能對要存取的遠端使用者和設備進行身份驗證，並管理和保護更多的入站 VPN 連接。

使用者和設備驗證

當一個組織開始大規格或完全導入的遠端作業模式時，零信任安全模型非常重要！員工可能會使用已連線在不受信任網路上的未知或他們自己的個人設備連接到公司網路，這樣的行為如未加以管理，會加深網路資安的危害。

保護組織的網路及組織的敏感數據和資源，需要能對試圖連接到該網路的使用者和設備進行身份驗證，而這可以透過連接到組織活動的目錄，輕量級目錄存取協定（LDAP）和遠端使用者撥入驗證服務（RADIUS）的中央身份驗證伺服器來實現。

該伺服器應具有擴展能力，可以滿足大量的遠端工作人員的需求，而不會影響使用者的工作效率。對透過單一登錄（SSO）、證書管理和訪客管理的支援還可以確保使用者身份驗證，而不會給遠端員工造成重大負擔。

網路邊界保護

在現場工作的員工和遠端工作的員工之間的一個區別是組織必須能夠管理 VPN 連接的數量。工作現場的員工直接連接到公司的區域網路，但遠端工作的員工必須透過 VPN 的連接來傳送他們的資料。組織的防火牆必須有能力接受所有 VPN 連接並執行大量加密網路連接的檢查效能。由於加密流量檢測的成本很高，所以組織的防火牆需要能夠擴充以滿足需求。要這樣做就需要防火牆配備專用的高階安全處理器，以最大限度地減少延遲並最大限度地提高傳輸量，防止網路瓶頸而降低員工的工作效率。

前端的防火牆還必須對所有流量執行第 7 層檢查，這在任何企業環境中都非常重要，但是對於遠端工作人員，組織可能會認為更多的惡意內容集中在遠端工作人員的入站連接。這是因為連接到個人網路的員工電腦感染惡意軟體的可能性更高，惡意軟體可能會嘗試橫向移動到公司網路裏。第 7 層防火牆可以識別入站封包試圖到達的應用程式，並阻止來自具有已知漏洞的應用程式的封包。前端的防火牆還應該與沙箱功能做整合，來安全分析與已知威脅無關但可疑的內容。

檢查傳輸層安全性（TLS）/ 安全通訊端層（SSL）可讓防火牆處理效能 Throughput 平均降低 60%。[3]

結論

當快速和大規模轉換到遠端工作營運模式時，組織不僅必須維持運作，還要確保在遠端工作的同仁及他們所處理的敏感資料的安全。

這樣做組織需要在遠端工作的同仁與他們的工作地點和公司的主要網路上佈局安全解決方案，且必須選擇能夠解決與遠端工作相關獨特的設施需求與資安問題，且萬一在遇到災難的情況下，需要立即得到回應時，一個可以快速輕鬆部署的解決方案，將對企業或組織的營運貢獻不可磨滅。

[1] Emma Sutcliffe, "How the PCI DSS Can Help Remote Workers," PCI Security Standards Council, March 26, 2020.

[2] Michael E. Porter and Nitin Nohria, "How CEOs Manage Time," Harvard Business Review, July 2018.

[3] "NSS Labs Expands 2018 NGFW Group Test with SSL/TLS Security and Performance Test Reports," NSS Labs, July 24, 2018.

www.fortinet.com/tw

628535-0-0-TW

August 26, 2020 11:42 AM

ebook-teleworker-solutions