企業 VPN 保安指南

企業 VPN 是一個常用的技術，以在全球爆發疫情的情況下支援在家工作。然而，如果在使用企業 VPN 時缺乏充足的風險評估以及相應的風險管理措施，可能會導致網絡保安事故。針對企業 VPN 設備的網絡攻擊十分常見，其中的例子包括針對舊版本 VPN 設備的加密勒索軟件風潮，導致洩露敏感資料及損害商譽。隨著網絡安全風險不斷轉變，我們必須在設置企業 VPN 時做保安措施。

1. 題要

本指南旨在列出使用企業 VPN 時的常見安全問題，同時為資訊科技經理和技術人員提供保安指引，以應對相關的風險，並建議相應策略。

本指南採用檢查清單形式，方便讀者採用較佳的保安措施並自行評估。本指南主要分為三部份:

(一) 保安管理和規劃

本部份的內容是關於企業 VPN 的安全政策、容量規劃、效能調整及變更管理，以支援業務需求。本部份供資訊科技經理參考。

(二) 安全架構、強化和存取控制

本部分建議於企業 VPN 的結構設計中加入安全考慮，以及如何通過定期維護和安全管控來減少被攻擊面。本部份供技術人員參考。

(三) 保安監控和事故應變

本部分建議適當地管理保安記錄，以增加網絡可見性和支援事故應變。本部份供技術人員參考。

2. 保安管理和規劃

本部份供資訊科技經理參考。

常見保安問題	保安指引
1. 對使用企業 VPN 的規則缺乏認知。例如： • 設立企業 VPN 之目的 • 誰可使用企業 VPN • 如何設定及使用 • 使用規則 • 注意事項 • 哪些設備可得到支援 • 如有問題，誰人可提供協助 • 使用者責任	1) 為企業 VPN 制訂安全政策並將之執行，以支援業務需要，例如制訂業務連續性計劃。 ☐ 制訂高級別的企業 VPN 保安政策，當中包含員工/用戶明白及認同的資料。保安政策應清楚說明設立企業 VPN 的目的、其使用規則、使用者的責任，以符合管理層對管理網絡保安風險的期望，例如為避免將病毒帶入公司網絡，在連接到企業 VPN 之前，必須為電腦安裝最新的安全更新並安裝防毒軟件。 如有需要，請參考 SANS 的安全政策範本，以建立企業 VPN 保安政策： https://www.sans.org/information-security-policy/ (在上述連結選擇 "Virtual Private Network Policy" 或 "Remote Access Policy" 以取得安全政策範本)
2. 企業 VPN 的容量不足，例如： • VPN 無法同時支援公司所有用戶 • 部分用戶在繁忙時段無法連接到 VPN • VPN 速度緩慢	2) 定期進行容量規劃和效能調整 ☐ 預先規劃企業 VPN 的容量，估算 VPN 設備可同時支援的用戶數目，如有需要可增購額外資源。一般來說，企業應該事先預計將來的用戶增長。 ☐ 根據業務需求和過往數據進行估算。一般而言，這兩個因素被視為主要的因素。 ☐ 建議將估算容量額外增加百分之 20 至 30 作為緩衝，以應付突發的需求。 請參考「附錄 1」中的情景例子，以更詳細了解此安全建議。

常見保安問題	保安指引
3. 企業在沒有進行適當的變更管理程序下，緊急部署/擴展VPN，例如在進行前並未讓持份者檢視。這將為企業網絡安全帶來風險。	3) 變更管理是部署/擴展 VPN 時必須進行的重要工作。 ☐ 評估變更風險。 ☐ 制訂一個階段性的變更計劃並予以執行。 ☐ 預備一個還原計劃，以應付意料之外的情況。 ☐ 變更後進行測試和檢視。 請參考「附錄 2」中的情景例子，以更詳細了解此安全建議。

3. 安全架構、強化和存取控制

本部份供技術人員參考。

常見保安問題	保安指引
1. 企業 VPN 結構設計中未有考慮安全性問題。例如： • 沒有區分企業 VPN 的網絡區域和現有防火牆上的網絡區域及 IP 子網 • 企業 VPN 可被公開存取，而且沒有適當的管控措施。例如管理介面可被公開存取，這可能會遭受網絡攻擊 • 容許通道分割(Split tunneling)，這可能會繞過保安控制措施 • 企業 VPN 單點故障	1) 安全的設計和深度防禦 ☐ 在企業 VPN 的防火牆上使用專用的網絡區域和 IP 子網，以實現精密的存取控制。 ☐ 使用防火牆保護企業 VPN 的管理介面，並限制只能被內部網域存取。 ☐ 使用防火牆保護 VPN 設備及為 VPN 服務設定「靜態 NAT」(將公共 IP 配對至私人 IP)。由於防火牆可控制「靜態 NAT」配對，來自互聯網的 VPN 請求會先經防火牆檢查後才可到達 VPN 設備。 ☐ 採用全隧道(full tunneling)強制所有客戶端流量盡可能通過 VPN 設備，以確保企業安全控制措施到位。

常見保安問題	保安指引
	☐ 採用容錯/高可用性設計（如適用）。請參考。附錄 3」中的情景例子，以更詳細了解此安全建議。
2. 於企業 VPN 中使用預設設定並缺乏維護。例如： • 舊版安全協議 SSL3.0, DES, RC4 • 使用舊的企業 VPN 軟件/韌體，使 VPN 存在漏洞。 • 啓動不必要的服務或功能 • 於 SSL-VPN, 使用網頁模式 (Portal VPN) • 使用預設服務埠	2) 強化與維護 ☐ 使用安全協議和加密算法。 備註：一般而言，建議在「客戶端到站台」VPN 和「站台到站台」VPN 分別使用「SSL VPN」和「IPsec VPN」，以在兼容性和安全性之間取得平衡。 例子: • 「客戶端到站台」VPN：員工利用手提電腦連接到公司網絡以存取內部文件 • 「站台到站台」 VPN：分公司和總部連接以同步銷售數據 請參考「附錄 4」中的安全協議和加密算法列表。 ☐ 更新/升級企業 VPN 的軟件/韌體以修復已知漏洞並支援最新協議/功能。 ☐ 停用不必要的服務或功能。 ☐ 於 SSL-VPN 盡可能使用隧道模式 (Tunnel VPN) 配合 VPN 客戶端軟件，以減低來自網頁模式（Portal VPN）的網絡相關漏洞風險。 ☐ 在可行情況下，使用非預設服務埠，例如 443 是 SSL-VPN 的預設服務埠，可改用 10443。 備註: 於某些情況下，使用非預設服務埠並不可行。例如某些非預設服務埠在海外被禁止使用，因此可能會導致一些用戶在海外期間無法使用企業 VPN。

常見保安問題	保安指引
3. 不足夠/不恰當的存取控制。例如： • 所有 VPN 用戶都可以通過企業 VPN 存取企業網絡的所有系統和資源 • 企業 VPN 設有多個入口（IP 位址 / 網址），當中有些入口沒有保安控制措施 • 所有公共 IP 位址都可以存取企業 VPN • 載有過期防毒軟件定義檔的裝置都可以連接到企業 VPN • 容許使用保安度低的密碼 • 沒有多重認證，只靠密碼 • 沒有登入失敗的次數上限 • 容許使用本地用戶帳號，令用戶可以繞過中央化的身分認證與存取管理系統 • 沒有閒置中斷功能 • 容許用戶於任何時間連接到企業 VPN	3) 存取控制 ☐ 採用「需知道」(need-to-know) 存取原則，僅將存取權限授予必需要知道/使用的用戶，以執行其職責。例如只有人力資源部的用戶可透過企業 VPN 存取人力資源系統，但銷售部的用戶則不可存取。 ☐ 限制企業 VPN 入口數量(IP 位址/網址)，以確保能做到存取控制。 ☐ 只容許特定 IP 位址和/或設備連接到企業 VPN。 ☐ 裝置連接到企業 VPN 前，需進行合規檢查。例如必須安裝和更新防病毒軟件，並且已通過漏洞掃描。 備註：某些 VPN 客戶端軟件或網絡存取控制解決方案可能會提供更多裝置合規檢查功能。詳情請參閱製造商的產品說明書。 ☐ 實施嚴格的密碼政策（包括資訊科技部門）。 ☐ 實施雙重認證 (2FA)。 ☐ 設定登入失敗的次數上限。 ☐ 使用 LDAP 或 RADIUS 作用戶身份驗證以便帳戶管理和控制。 ☐ 不允許相同用戶同時建立多個企業 VPN 連線。 ☐ 設定閒置連線中斷，減少暴露內部網絡，並保留資源，例如閒置 20 分鐘後，用戶的 VPN 連線將自動中斷。 ☐ 訂立企業 VPN 服務時段，例如：一般員工只能在辦公時間內連線至企業 VPN。

4. 安全監控和事故回應

本部份供技術人員參考。

常見保安問題	保安指引
1. 遺失/不充足的企業 VPN 記錄，例如： • 沒有在指定時間嘗試登入企業 VPN 的日誌 • 缺少成功/失敗登入企業 VPN 的日誌 • 缺少用戶成功連線至企業 VPN 後的網絡存取記錄	1) 作出足夠的記錄以實施責任制並促進保安監控和事故應對。 ☐ 記錄誰人(IP 位址/使用者帳戶)曾嘗試於指定時間連線至企業 VPN ☐ 記錄成功/失敗的登入嘗試 ☐ 記錄用戶成功連線至企業 VPN 後，下一個嘗試連線的地方，例如：內部檔案伺服器。
2. 沒有定期檢查企業 VPN 的記錄，例如： • 某些用戶報告自己的帳戶被鎖定，從而揭發於兩星期前開始一些來自海外的 IP 位址嘗試利用其帳戶登入企業 VPN	2) 定期檢查記錄，以防止濫用、偵測憑證洩漏和潛在的網絡威脅。 ☐ 訂立檢查記錄的時間表，以定期檢查企業 VPN 記錄，例如：每星期檢查一次
3. 沒有中央處理及儲存記錄。例如： • 由於個別設備的硬碟容量太少，未能保留足夠日子的記錄 • 難以將記錄與其他設備上的記錄相關聯 • 缺乏趨勢及模式資料作分析	3) 中央處理及儲存記錄 ☐ 確保中央記錄伺服器的容量足夠支援保安政策上的要求，例如：應該最少保留過去 3 個月的記錄 ☐ 將各種設備的記錄相關聯，以提升網絡活動的可見度。如果攻擊者成功地透過企業 VPN 入侵企業網絡，關聯記錄可以識別他在企業網絡上所做過的任何事情，如嘗試存取應用程序服務器和數據庫等。

常見保安問題	保安指引
4. 若發現以下情況，可能已成為網絡攻擊的目標： <u>竊取憑證:</u> • 從釣魚電郵中找到了虛假企業 VPN 的帳戶驗證網站 <u>暴力破解攻擊/嘗試入侵:</u> • 從同一用戶帳戶/ IP 位址偵測到多次登入失敗記錄 • 從同一用戶帳戶偵測到多次因登入失敗引致鎖定的記錄 • 偵測到使用不同用戶名稱嘗試登入失敗的記錄，例如： peterchan , peter_chan, peter.chan, peterchan@companyname.hk, peter_chan@companyname.hk • 用戶嘗試在非辦公時間（例如午夜）登入 • 有海外 IP 位址嘗試登入 VPN，但所有員工都在香港 <u>惡意掃描/通訊埠掃描:</u> • 接收到的 IPsec 錯誤記錄（未知遠端 IP 位址） • 由相同 IP 位址不斷產生連線錯誤記錄 <u>發現被入侵後:</u> • 於企業 VPN 發現不明來曆的本地用戶帳號有 VPN 用戶嘗試連接到不應存取的系統	☐ 支援報告功能，可提供有關系統安全的統計資料和趨勢報告。 4) 準備事故應變 ☐ 企業應該為事故應變做好準備： • 指派人手作事故回應，例如：建立事故回應隊伍。 • 建立緊急聯絡人列表，作通知和提升事故級別，例如包括供應商和服務提供商、高級管理層、監管者、持份者和媒體等。 • 將必要的工具和資源，例如文檔和網絡圖、系統變更記錄、手提電腦，分析和備份恢復工具等放於容易存取的地方 ☐ 為了有效地進行事故應變，企業應準備常見事故類型的詳細事故應變程序，並定期演練。 該程序應包括： • 分析情況，評估影響並找出可能的原因 • 通知相關人士或提升事件級別 (如有需要) • 採取後續行動以遏制（避免情況變得更壞，例如隔離受影響的部分）、根除（消除威脅並加強控制措施以避免再次發生）和恢復（恢復業務、測試和監控） • 回顧事件，從錯誤中學習

5. 結論

只要能減低相應的風險，企業 VPN 可以安全地讓員工進行遙距工作。在全球疫情大流行期間，企業在將業務數碼化的同時，亦要加強關注網絡安全風險及提高員工的保安意識。

6. 參考資料

1. NCSC: Advisory: COVID-19 exploited by malicious cyber actors
   https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory
2. certnz: Active ransomware campaign leveraging remote access technologies
   https://www.cert.govt.nz/it-specialists/advisories/active-ransomware-campaign-leveraging-remote-access-technologies/
3. SenseCy: GLOBAL RANSOMWARE ATTACKS IN 2020: THE TOP 4 VULNERABILITIES
   https://blog.sensecy.com/2020/08/20/global-ransomware-attacks-in-2020-the-top-4-vulnerabilities/
4. SANS: Security Policy Templates
   https://www.sans.org/information-security-policy/
5. SANS: NewsBites Drilldown for the Week Ending 10 July 2020
   https://www.sans.org/blog/newsbites-drilldown-for-the-week-ending-10-july-2020/
6. SANS: VPN Access and Activity Monitoring
   https://isc.sans.edu/forums/diary/VPN+Access+and+Activity+Monitoring/25906/
7. SANS: What's in Your Change Control Form?
   https://isc.sans.edu/diary/What%27s+in+Your+Change+Control+Form%3F/14563
8. Mozilla : Security/Server Side TLS
   https://wiki.mozilla.org/Security/Server_Side_TLS
9. IPsec VPNs vs. SSL VPNs
   https://www.cloudflare.com/learning/network-layer/ipsec-vs-ssl-vpn/
10. Four Risks to Consider with Expanded VPN Deployments
    https://www.f5.com/labs/articles/cisotociso/four-risks-to-consider-with-expanded-vpn-deployments
11. Cisco: SSL VPN Security
    https://tools.cisco.com/security/center/resources/ssl_vpn_security
12. Enterprise VPN Security
    https://us-cert.cisa.gov/ncas/alerts/aa20-073a
13. Guide to IPsec VPNs NIST.SP.800-77r1

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf
14. Guide to SSL VPNs NIST SP 800-113
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf
15. Incident Response Steps and Frameworks for SANS and NIST
https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide
16. Computer Security Incident Handling Guide NIST.SP.800-61r2
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

7. 附錄

附錄 1: 定期進行容量規劃和效能調整

例子: 一家初創公司擁有 10 名員工，他們每年增加 2 個新員工，所有員工都必須使用企業 VPN。企業 VPN 的網絡服務為 100Mbps，高峰時段的頻寬使用率為百分之百。 企業 VPN 設備能夠同時支持 10 位用戶（軟件許可證）。

根據以上歷史數據， 預計未來 3 年的容量共增加百分之 60，再加上百分之 20 至 30 的緩衝區，預計容量大約增加百分之 80 至 90。

在這個例子，我們知道效能瓶頸是頻寬和 VPN 設備。 解決這些問題可能會直接增加企業 VPN 的可用性。

附錄 2 : 變更管理是部署/擴展企業 VPN 不可或缺的部份

例子: 一家初創公司正擴展企業 VPN 的容量. 已編寫了變更計劃以確保變更有秩序地進行。此計劃列出了重要資訊，包括變更程序、還原計劃、涉及人員、受影響的服務和相關信息。

變更可以在涉及人員（包括安全團隊和管理層）審核並批准變更計劃之後執行。 如果他們在執行計劃期間遇到意外，他們仍然可以有系統地還原。

附錄 3: 設計安全和深度防禦

下面的樣本設計說明了「深度防禦」：當使用者連線至企業 VPN， 該請求必須首先通過防火牆(首項控制措施， 步驟 **1**) 然後是 VPN 設備 (第二項控制措置， 步驟 **2**)。 當認證成功後，該請求亦必須首先通過兩層控制措施才可訪問內部網絡，VPN 設備(首項控制措施， 步驟 **3**)和防火牆(第二項控制措置， 步驟 **4**)。

[圖 1 企業 VPN 樣本設計}

附錄 4: 強化與維護

SSL VPN	
TLS 安全協議	**加密算法**
TLS 1.3	• TLS_AES_128_GCM_SHA256 • TLS_AES_128_CCM_8_SHA256 • TLS_AES_128_CCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256
TLS 1.2 和 TLS 1.3	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-CHACHA20-POLY1305 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384

IPSec VPN (NSA 最低建議設置)	
ISAKMP/IKE	**IPsec**
• Diffie-Hellman group: 16 • encryption: AES-256 • hash: SHA-384	• encryption: AES-256 • hash: SHA-384 • block cipher mode : CBC

- 本文完 -