# Trey Research 公司

虛擬專用網路：Fabrikam, Inc. 技術概覽

**2023 年 12 月 15 日**

**虛擬專用網路 (VPN)** 為一種主流的網路安全解決方案，用以協助加密網路流量。[可作為安全通道加密網際網路流量，能有效防止第三方追蹤活動及竊取資料](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[1](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons).

## 導入 VPN 的優點：

* VPN 透過加密網際網路流量，提供多一層的隱私與安全保護。此舉讓第三方難以追蹤活動及竊取資料。
* VPN 有助於避免在機場或圖書館使用公用 Wi-Fi 時遭到駭客攻擊。此乃因 VPN 可作為安全通道，對網際網路流量進行加密。
* [VPN 可防止您的網際網路服務供應商 (ISP) 得知您所造訪的網站，因為您電腦的所有傳輸流量，均會通過 VPN 自行管理或付費租用的伺服器](https://www.bing.com/aclk?ld=e83gkJ29qbmUu8cYkNgVfaCjVUCUx3vCyorXNIwmWui8A8rISGT4ATMfXuQu_8nGJifMsVNZrD0_vVyNtSvYRynbmDYfM2jUvwoREzv_CIrOKnWn2gIEyYOWegOAxJPNIFOUp5hBSGQU35pxcSs4Qxqzw59vf63cS8Oh_e_94A9QZD8MND&u=aHR0cHMlM2ElMmYlMmZ3d3cudnBubWVudG9yLmNvbSUyZmluLXVzYS1iZXN0LXZwbiUzZmtleXdvcmQlM2R2cG4lMjUyMHJhbmtpbmclMjZnZW8lM2QxMTA3MzUlMjZkZXZpY2UlM2QlMjZ1dG1fc291cmNlJTNkYmluZyUyNmFkaWQlM2Q3NjIxMDA1Nzk0MzY4MCUyNm1zY2xraWQlM2Q3NTEzMDFiNzM2MTQxZTY2ZTBiZDY0MTA0MzJlYjBkYw&rlid=751301b736141e66e0bd6410432eb0dc) [1](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/).
* [VPN 可藉由遮罩您的 IP 位址並加密網際網路連線， 2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)以繞過內容的地理區域限制。當您連線至 VPN 伺服器時，您的網際網路流量將經由該 VPN 伺服器路由傳送，同時獲派一個新的 IP 位址。[如此一來，您的網路活動看起來便如同從不同位置進行存取，從而讓您得以繞過內容的地理區域限制。](https://www.bing.com/aclk?ld=e8YiIMdr2QtA2Sk-u0-9k1uDVUCUwZqJo7k-TZ_u3VURZI-3jr14Tl4u2r6BKbbALVRPh16htACtOCb2UysS_OGSA02FnjNda5d_7Dsl3j4em0VxQmLB5dYQ9xV9_8fwf4GatF_vLHO4kWLTXLy2sWMccuzGxta13Ki3OpGEZizfm9Lnk7&u=aHR0cHMlM2ElMmYlMmZ3d3cuZXhwcmVzc3Zwbi5jb20lMmZ3aGF0LWlzLXZwbiUyZnVuYmxvY2std2Vic2l0ZXMlM2ZvZmZlciUzZDNtb250aHNmcmVlJTI2b2ZmZXJfY29kZSUzZDNjNmhqb29yNjklMjZyZWZJRCUzZEJJX2NhbXBhaWduaWQlM2Q0MDU1NDQ1ODUlMjZtc2Nsa2lkJTNkNjU2NzIxOTRkNjRkMWQ1Y2UwNjc0NDMzYTMxNGNjMTE&rlid=65672194d64d1d5ce0674433a314cc11)

## 導入 VPN 的缺點：

* 連線速度可能較您的 ISP (網際網路服務供應商) 緩慢。[此乃因 VPN 會對您的網際網路流量額外增加加密及路由程序所致2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/).
* 某些威權國家禁止 VPN 使用。[在某些國家/地區，VPN 被禁止或受到嚴格管制](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/) [2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/).
* 使用免費 VPN 有暴露於廣告、惡意軟體及資料外洩的風險。[免費 VPN 可能會將使用者資料販售給第三方廣告商，或在網頁中植入廣告](https://www.consumerreports.org/electronics-computers/vpn-services/should-you-use-a-vpn-a5562069524/)[2](https://privacysavvy.com/vpn/guides/pros-and-cons-of-vpn/)。

## 安裝詳情：

* [會在執行 VPN 用戶端的系統與 VPN 伺服器之間建立加密通道，再經此通道透過 Proxy 將流量轉送至企業網路的其他部分](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[4](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/) 步驟包括︰
  1. VPN 用戶端安裝於使用者裝置後，即會對該裝置與 VPN 伺服器間的所有流量進行加密。
  2. VPN 伺服器會將流量解密，並將其轉送至預定目的地。
  3. 目的地伺服器會藉由將流量傳回 VPN 伺服器來回應要求。
  4. VPN 伺服器會加密流量，並將其傳回 VPN 用戶端。
  5. [VPN 用戶端會將流量解密，然後傳送至使用者裝置](https://www.bing.com/aclk?ld=e8OcZUYHFbvxJgBgmEWpxgCzVUCUz-UOb13n9w7mOCOGgLkPnDhd3Uh-ipDjPE6Hpo4QBuX2o2EUlY6g5-dRpoq53O3haHMQ8RcFRpVU95xD1yO9RVjEOu3gsgBNFb6xmA-Gvbq-gT8RFWo2P6R0BeJBd5LyAIvbSKlU_DPbqAqdr2ubUB&u=aHR0cHMlM2ElMmYlMmZ3d3cub3BlcmEuY29tJTJmZmVhdHVyZXMlMmZmcmVlLXZwbiUzZnV0bV9zb3VyY2UlM2RiaW5nJTI2dXRtX21lZGl1bSUzZHBhJTI2dXRtX2NhbXBhaWduJTNkVVMlMjUyMC0lMjUyMFBlcmZvcm1hbmNlJTI1MjBNYXglMjUyMC0lMjUyMEVOJTI2dXRtX2NvbnRlbnQlM2QlN2Jhc3NldEdyb3VwSWQlN2QlMjZtc2Nsa2lkJTNkZDVhYzJiMDEzNDM2MWVkNDRmNGE0ZWE2NDA1MDk5MjIlMjZ1dG1fdGVybSUzZHd3dy5vcGVyYS5jb20&rlid=d5ac2b0134361ed44f4a4ea640509922) [1](https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html).
* 若要安裝並設定 VPN 伺服器，請遵循下列步驟：
  1. 在您的電腦上建立 VPN 設定檔。
  2. 按一下 [開始]，然後按一下 [設定] 以開啟 [設定] 功能表。
  3. 在 [設定] 功能表中，按一下 [網路和網際網路]，然後按一下 [VPN]。
  4. 選取 [新增 VPN 連線]。
  5. 在 [新增 VPN 連線] 視窗中，有數個工作項目需要執行。
  6. [儲存您所做的變更](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[5](https://www.techzone360.com/topics/techzone/articles/2020/09/16/446567-how-install-configure-virtual-private-network-server.htm).

## 風險與緩解措施：

* 攻擊者早已意識到遠端工作在一段時間以來，皆為一個潛在的威脅途徑。基於數項原因，遠端工作環境對攻擊者而言，具有顯著的吸引力。首先，家用網路環境普遍缺乏專業管理。最關鍵的是，這表示許多家用網路系統並未定期套用修補程式，且部分系統在弱點緩解措施方面早已過時。若要在企業網路中持續潛伏，已入侵系統的攻擊者必須能規避偵測並抵抗清除措施。對攻擊者而言，家用網路環境更為有利：不僅幾乎沒有威脅偵測機制，補救措施也往往只是偶發情況，例如個人電腦因執行緩慢而重新安裝或汰換。為確保遠端工作環境的安全，進一步擴展零信任原則至為重要。[不應僅僅假設網路本身具有敵意，更應將企業無法有效控管的一切事物及環境皆視為潛在威脅](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[4](https://insights.sei.cmu.edu/blog/remote-work-vulnerabilities-and-threats-to-the-enterprise/).
* [請採用最新的軟體修補程式及安全設定，更新 VPN、網路基礎設施裝置，以及用於遠端存取工作環境的各類裝置。](https://bing.com/search?q=Virtual+Private+Networks+pros+and+cons)[6](https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a).

## 導入最佳實務：

在企業網路中導入 VPN 的最佳實務包括：

* [選用基於標準的 VPN，該 VPN 應採用公認標準，例如網際網路金鑰交換/網際網路安全協定 (IKE/IPSec)。相較於採用自訂程式碼透過 TLS 傳送流量的安全通訊端層/傳輸層安全機制 (SSL/TLS) VPN，這類基於標準的 VPN 通常風險較低且更為安全](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad)[1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/)。
* 請使用具備強固加密技術的 VPN。請驗證 VPN 所採用的加密演算法、驗證演算法及通訊協定是否足夠強化，並已通過 FIP 驗證。[設定所有 VPN 皆須使用多重要素驗證 (MFA)，並於情況允許時，透過儲存於智慧卡上的數位憑證，以用戶端驗證取代密碼式驗證](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad)[1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/).
* 管理軟體弱點。利用 VPN 弱點進行的攻擊，是網路犯罪者常用的攻擊媒介之一。選擇具有良好漏洞修補記錄的 VPN 廠商，並請求軟體物料清單 (SBOM) 來驗證第三方代碼是否是最新的和安全的。此外，尋找可以在執行時執行代碼驗證的產品以偵測潛在的入侵。[部署 VPN 後，請定期檢查並及時應用軟體更新](https://www.bing.com/aclk?ld=e8IaDdghmbnebPF9t8NDtSPTVUCUzEN_M1950bORweSvjTxQ_j5Hx8cAExcEXM0D9tIxdCoCR_Jw7t7hWJ87VsGu1b1NcLpgYJAJvLbk73VuMpBtE5y4UGUvcr2PV-wLevlqXTg4Ng7Q5s3eKLWASODIm5vCFYV3bH2LqA92NtuM3IAecU&u=&rlid=488aa28de39614beea91c72a9258abad) [1](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/)[2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/)。
* 為使用中的激增做好準備。[IT 安全人員應測試 VPN 限制，為大規模使用做好準備](https://resources.infosecinstitute.com/topic/how-to-choose-and-harden-your-vpn-best-practices-from-nsa-cisa/) [2](https://www.sdxcentral.com/security/definitions/what-is-encryption-definition/what-is-virtual-private-network-vpn/what-are-vpn-best-practices/)。
* 避免使用免費的 VPN。[使用免費 VPN 存在廣告、惡意軟體和洩密的風險3](https://forti1.com/en/ssl-vpn-best-practices-7-security-tips/)。