# 虛擬私有網絡保安 (VPN Security)

## *什麼是 VPN?*

VPN 是利用公共網絡將遠程網站和用戶連接在一起的私有網絡。VPN 並非使用租用線路等專用連接途徑，而是在一個共用或公共網絡將各地的用戶和網絡"虛擬"連接，情況猶如互聯網，資料經過加密後就像在私有連接線路上傳送一樣。

數據包在傳送前將先被壓縮成附有標題的新數據包。新標題爲數據包提供了路由資料，使數據包能穿過共用或公共網絡抵達目的地。壓縮數據包穿過共用或公共網絡的邏輯路徑稱爲「隧道」。數據包抵達隧道終點時會被解除壓縮，然後再被傳送到最終的目的地。

VPN 就像是穿過網際網路的一條「隧道」，將不同地點的電腦連接起來。在這個隧道裡，資料會被加密，然後以標準的 TCP/IP 資料封包型態，將它包裝起來，以便能夠在網際網路上流通。因爲資料是加密的，第三者將無法看懂內裡的資訊。

## *VPN 的用途*

- 遠程接達 VPN
  供家庭用戶和流動資訊產品用戶從遠距離地點連接機構私有網絡的接駁功能。這類 VPN 讓機構私有網絡與遠程用戶之間建立穩妥的加密網絡聯繫。

- 內聯網 VPN
  將多個固定地點（例如分支辦事處）連接起來。這種局部區域網之間的連接系統將多個遠距離地點連接起來，成爲單一的私有網絡。

- 外聯網 VPN
  用來連接供應商與客戶等業務夥伴。外聯網 VPN 使有關各方能夠在一個共用的環境下工作。

- 替代寬廣區域網絡
  VPN 提供了另類寬廣區域網絡的選擇。VPN 比使用租用線路的傳統私有網絡有更強的延展性，所需的費用和管理也較少。

總括而言，使用 VPN 有以下好處：
- 擴大連接地理範圍
- 加強遠程用戶和網絡連接的保安
- 相對於傳統的寬廣區域網絡更節省經營成本
- 爲遠程用戶節省時間和傳輸費用
- 因爲遠程網絡和用戶能夠接達資源而提高了生產力

### *VPN 連接的組件*

| 組件 | 用途 |
|---|---|
| VPN 伺服器 | 容許 VPN 客戶進行 VPN 連接的電腦。VPN 伺服器可供遠程 VPN 連接，或通訊閘至通訊閘的 VPN 連接 |
| VPN 客戶 | 與 VPN 伺服器建立 VPN 連接的電腦。VPN 客戶可以是建立遠程 VPN 連接的遠程電腦，或建立通訊閘至通訊閘 VPN 連接的路由器 |
| VPN 隧道 | 資料被壓縮及加密的連接路段 |
| 隧道規約 | 設定管理隧道和壓縮資料的通訊準則 |
| 經隧道傳送的資料 | 經壓縮和加密，並通過私有鏈路傳送的資料 |
| 傳送網絡 | 壓縮資料所經過的共用或公共網絡 |

### *VPN 產品種類*

| 產品種類 | 摘要 |
|---|---|
| 基於防火牆的 VPN | 兼具防火牆和 VPN 功能。利用防火牆的保安機制限制接達至內部網絡。這類產品提供網址轉換、用戶身份鑑定、實時警報和記錄大量資料等功能 |
| 基於硬件的 VPN | 由於無須承受處理器的損耗，所以網絡通過量最高，性能較佳、較可靠 |
| 基於軟件的 VPN | 在 VPN 終點由另一方控制，而且使用不同的防火牆和路由器的情況下適用。這類 VPN 可與硬件加密加速器同時使用以提高性能 |

### *常見的 VPN 隧道技術*

隧道規約在開放系統互連（OSI）的第二層（數據鏈路層）或第三層（網絡層）運行。最常用的隧道規約包括：

- 互聯網規約保安（IPSec）
- 點對點隧道規約（PPTP）
- 第 2 層隧道規約（L2TP）

### *VPN 的保安重點*

- 使用防火牆，以加強 VPN 連接的保安
- 可使用入侵偵測系統（IDS）更有效地監察攻擊
- 相連網絡及遠程客戶應安裝防電腦病毒軟件，以便在其中一端受電腦病毒感染時，防止電腦病毒散播
- 認證功能簡單或沒有認證功能的不安全或無人管理的系統不得與內部網絡建立 VPN 連接

- 提供記錄和審計功能以記錄網絡連接，尤其是意圖未經授權接達的記錄，並定期審閱記錄
- 向網絡／保安管理員和支援人員，以及遠程用戶提供培訓，以確保他們在推行和使用 VPN 時，遵守最佳保安作業實務和保安政策
- 向有關各方派發有關恰當使用 VPN 和網絡支援的保安政策和指引，以規範他們對 VPN 的使用
- VPN 進入點宜放置在隔離區內，以保護內部網絡
- 在連接 VPN 時，不宜同時利用分隔隧道連接至互聯網或其他不安全的網絡。如使用分隔隧道，則應同時使用防火牆和入侵偵測系統，以偵測和防範來自其他不安全網絡的攻擊
- 應限制不必要的內部網絡連接

### *VPN 產品的常見保安功能*

- 強化認證支援，例如智能卡等
- 具有強化密碼匙支援功能，並以加密算法保護傳輸中的數據
- 防電腦病毒支援
- 爲終端用戶提供個人防火牆支援
- 強化維護埠的保安預設
- 使用數碼證書，例如使用證書進行網站至網站認證
- 入侵偵測功能
- 地址管理(在私有網絡設定客戶地址，並爲私有地址保密)