

# 虛擬私有網絡（VPN）保安

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

**免責聲明：**政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

## 目錄

|   |    |
|---|----|
| 摘要.....   | 2  |
| I. 虛擬私有網絡 (VPN) 是什麼? .....                              | 3  |
| VPN 的保安特性 .....   | 3  |
| II. 商業上的考慮 .....  | 4  |
| VPN 的用途 .....   | 4  |
| VPN 產品種類 .....  | 4  |
| III. 常用的 VPN 隧道技術 .....                                 | 6  |
| 互聯網規約保安 (Internet Protocol Security, IPsec) .....       | 6  |
| 點對點隧道規約 (Point-to-Point Tunneling Protocol, PPTP) ..... | 8  |
| 第二層隧道規約 (Layer 2 Tunneling Protocol L2TP) .....         | 9  |
| SSL / TLS .....   | 10 |
| IV. VPN 的風險和限制 .....                                    | 11 |
| 入侵者攻擊 .....   | 11 |
| 用戶身份認證 .....  | 11 |
| 客戶方風險 .....   | 11 |
| 電腦病毒／惡意軟件感染 .....                                       | 11 |
| 不恰當的網絡接達權 .....   | 12 |
| 互用性 .....   | 12 |
| V. 保安考慮事項 .....   | 13 |
| 一般 VPN 保安考慮事項 .....                                     | 13 |
| 外聯網 VPN 保安考慮事項 .....                                    | 13 |
| 客戶端 VPN 保安考慮事項 .....                                    | 13 |
| VPN 產品常見的保安功能 .....                                     | 14 |
| VI. 總結.....   | 15 |

## 摘要

現今，由遙距網絡接達到內聯網的需求日漸增加，員工經常需要從家裡、酒店、機場或其它外部網絡經互聯網（互聯網基本上是不安全的）接達到內部私有網絡。當員工或業務伙伴經常由不安全的外部網絡接連到內部網絡，保安便成為重要的考慮因素。

虛擬私有網絡（Virtual Private Network, VPN）技術是保護在互聯網傳送資訊的方法之一。用戶可利用該技術與內部網絡建立一條虛擬私有隧道，通過不安全的網絡如互聯網，卻能夠安全地進入內部網絡，接達內部的資源、數據及進行通訊。

本文將提供有關 VPN 的概述和 VPN 核心技術，並探討可能涉及的保安風險，以及建立 VPN 時應注意的保安事項。

## I. 虛擬私有網絡 (VPN) 是什麼？

虛擬私有網絡 (Virtual Private Network, VPN) 指在不安全或不被信任的網絡上建立一條加密隧道，利用一些技術的組合令連接變得安全，成為安全的通訊網絡<sup>1</sup>。VPN 並非使用指定連接方式例如專線等，而是讓不同地域的用戶，在共享或公共網絡如互聯網上建立「虛擬」連接，讓數據猶如通過私有連接來傳輸。

VPN 通過隧道傳送數據，即在傳送數據包前先加上新的標頭，然後把它壓縮 (包裹) 成為新的數據包。這個標頭提供路由資料，因此它能夠於到達其隧道終點前穿過共享或公共網絡。數據包所穿過的邏輯路徑稱為隧道。當數據包抵達隧道終點時，便會被「解壓」然後前向至其目的地。當然，雙方的隧道終點均須支援同一項隧道規約。隧道規約在開放系統互連 (Open System Interconnection, OSI) 第二層 (數據鏈路層 (data-link layer)) 或第三層 (網絡層 (network layer)) 運作，最常用的隧道規約有 IPsec、L2TP、PPTP 和 SSL。把一個數據包擁有私有而不能以路由發送的 IP 位址，附於另外一個數據包內，然後通過獨一無二的 IP 位址在互聯網上以私有網絡傳送。

### VPN 的保安特性

VPN 利用加密來提供數據機密性。接達網絡後，VPN 便可善用以上所述的隧道機制壓縮加密數據，既形成保安隧道，又可在公共網絡上有可被公開讀取的標頭。在這情況下如沒有適當的解密匙，數據包在公共網絡上是不能被讀取的，因此能夠確保數據在傳送過程中不會被披露或修改。

VPN 亦可提供數據完整性查核，方法是使用信息摘要 (message digest)，以確保數據在傳送過程中沒有被竄改。

基本上，VPN 沒有提供或實施強化的用戶認證，用戶可輸入簡單的用戶名稱及密碼，以獲授權由家裡或通過其它不安全的網絡接達內部私有網絡。然而，VPN 也支援其它認證機制，例如智能卡、權標及 RADIUS。

---

<sup>1</sup> [http://cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/vpn.htm](http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm)

## II. 商業上的考慮

### VPN 的用途

機構和企業使用 VPN 的主要用途如下：

1. 遠程接達 VPN：這是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。
2. 內聯網 VPN：這類 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，成為單一的私有網絡。
3. 外聯網 VPN：這類 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。
4. 替代寬廣區域網絡：VPN 提供了另類寬廣區域網絡（Wide Area Networks, WANs）的選擇，這類 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少於寬廣區域網絡。然而，VPN 網絡的可靠性和性能可能較弱，特別是在互聯網經隧道傳輸數據及連接的時候。

### VPN 產品種類

VPNs 大致可分為以下各種類<sup>2</sup>：

1. 基於防火牆的 VPN 是兼具防火牆和 VPN 功能，利用防火牆的保安機制限制接達內部網絡，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。
2. 基於硬件的 VPN 由於毋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。
3. 基於軟件的 VPN 提供最高彈性的網絡通訊管理，特別是當 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。
4. SSL VPN<sup>3</sup> 讓用戶使用互聯網瀏覽器便可以連接 VPN 裝置，互聯網瀏覽器與 SSL VPN 裝置之間會使用 SSL（保密插口層）規約或 TLS（傳輸層保安）規約來加密通訊。使用 SSL VPNs 的其中一個好處是方便易用，因為所有標準的

---

<sup>2</sup> <http://www.processor.com/editorial/article.asp?article=articles%2Fp2634%2F31p34%2F31p34.asp>

<sup>3</sup> <http://csrc.nist.gov/publications/drafts/SP800-113/Draft-SP800-113.pdf>

互聯網瀏覽器均支援 SSL 規約，所以用戶毋須安裝或配置任何軟件。

### III. 常用的 VPN 隧道技術

以下是常用的 VPN 隧道技術：

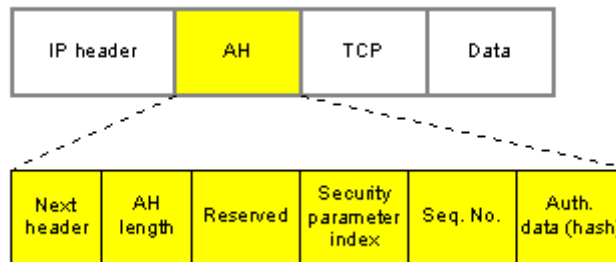
#### 互聯網規約保安 (Internet Protocol Security, IPsec)

IPsec 由互聯網工程專責組 (The Internet Engineering Task Force, IETF) 專為通過互聯網等公共互聯網規約網絡，在 OSI 第三層安全傳送資訊的目的而開發。IPsec 使系統能夠選擇和協商所需服務使用的保安規約、算法和密碼匙，並提供了基本的認證、數據完整性和加密服務。IPsec 運用了認證標頭 (Authentication header, AH) 和壓縮安全通訊協定 (Encapsulated Security Payload, ESP) 兩種保安規約，然而，IPsec 只限於寄送互聯網規約小包。

#### 通訊保安的保安規約

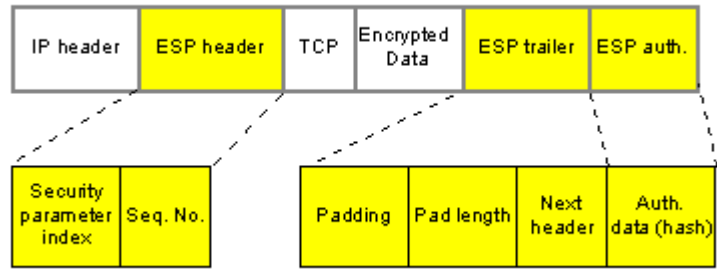
IPsec 使用 AH 及 ESP 規約以提供保安服務：

1. AH 規約能夠提供來源認證和確保 IP 數據包的完整性，但不提供加密功能。把 AH 標頭加進 IP 數據包，而這 IP 數據包含有雜湊函數、序數、以及可用作驗證寄件人、確保數據完整和防止中繼攻擊的資訊。



2. 除認證來源和確保完整性外，ESP規約還能夠保障數據的機密。ESP利用 3DES等對稱加密算法保障數據的機密，通訊雙方所用的加密算法必須相同。ESP亦支援純加密或純認證配置，然而，2007年一項調查顯示根據RFC而設定的IPsec使用純加密ESP時可被破解<sup>4</sup>。

<sup>4</sup> <http://eprint.iacr.org/2007/125>

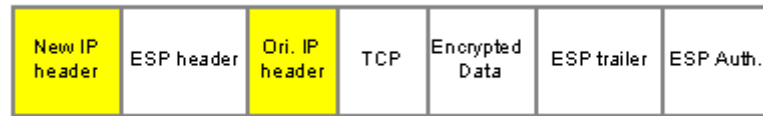


## 操作模式

每個保安規約支援兩種操作模式：隧道模式和傳輸模式。隧道模式將標頭和每一數據包的數據進行加密及／或認證，而傳輸模式只是將數據進行加密及／或認證。

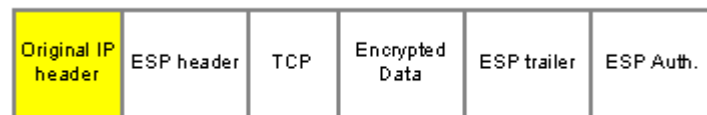
### 1. 隧道模式（端對端）

這模式保護整個數據包，原來的 IP 數據包和原來的目的地地址會插入新的 IP 數據包，AH 和 ESP 規約會應用在新的數據包。新的 IP 標頭會指向隧道的終點，在收到數據包時，隧道終點會將內容解密，原來的數據包便會在目標網絡中進一步傳送到原來的目的地。



### 2. 傳輸模式（主機對主機）

這模式將 AH 和 ESP 標頭加到原來的 IP 數據包，除了 IP 標頭，數據會被加密及／或認證，相對隧道模式的工作負荷較輕微。然而，最終目的地和發送人位址有機會被偷窺，攻擊者可根據這類標頭內的資料進行通訊分析。傳輸模式一般用來連接主機。



## 密碼匙交換和管理

IPsec 支援兩種互聯網密碼匙管理：自動和人手。

## 1. 自動密碼匙管理

互聯網密碼匙交換 (Internet Key Exchange, IKE) 是 IPsec 用來決定和協商規約、算法和密碼匙及認證通訊雙方的預設規約。自動密碼匙管理有助於大規模和廣泛部署推行 VPN。

IKEv2 規約於 2005 年發布，除了保留大部份 IKEv1 規約的功能，還支援網絡位址轉換 (Network Address Translation, NAT) 通過，功能上更富彈性。

IKE 同時支援數碼證書，用戶以數碼簽署密碼匙首次簽署數據作為認證，而另一端點則驗證簽署。IKE 在通訊雙方之間建立經過認證又安全的隧道，然後互相協商安全性關聯 (security association, SA) 並交換密碼匙。SA 是協商雙方為確保通訊安全而決定服務和機制所用的一系列參數，這些參數包括算法標識符、模式、密碼匙等。IKE 亦會追蹤密碼匙資料和更新通訊雙方之間所用的密碼匙，利用 ISAKMP (The Internet Security Association and Key Management Protocol) 和 Oakley 之類的規約以決定產生密碼匙、產生與管理 SA，以及認證的過程。

IPsec VPN 開口在遠程用戶認證中使用 IKE<sup>5</sup>，認證方法有幾種，包括併合認證 (hybrid)、擴展認證 (Xauth)、密碼匙質詢／回應認證 (CRACK) 及數碼證書，這樣便容許使用第三者認證服務以加強接達控制過程。

## 2. 人手密碼匙管理

密碼匙和 SA 在連接前由 VPN 通訊雙方人手配置，只有寄件人和收件人知悉保安服務的密碼匙。如果認證數據證實為有效，收件人便確知資訊由寄件人發出，而且資訊沒有被竄改。這種方法方便簡易，適合規模較小的靜態環境，卻不能大規模使用，因為事前必須把所有密碼匙安全地分發給通訊各方。如果密碼匙外洩，便有機會遭其它人冒充用戶連接 VPN。

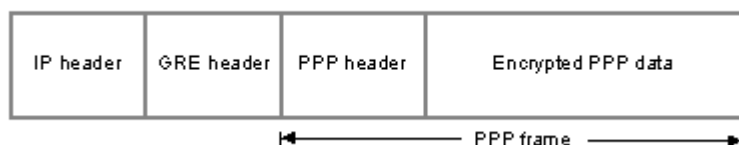
### 點對點隧道規約 (Point-to-Point Tunneling Protocol, PPTP)

PPTP 是建立在點對點規約 (Point-to-Point Protocol, PPP) 基礎上的 OSI 第二層規約。PPP 是一種用來連接互聯網的撥號多重規約，遠程用戶可撥號連接個人互聯網服務供應商，再通過 PPTP 接達私有網絡。PPTP 為各遠程客戶創造了一個虛擬網絡，以連接目標網絡。PPTP 在非 TCP/IP 規約 (例如互聯網規約、IPX 或 NetBEUI) 下，使 PPP 通訊得以穿過 IP 網絡進行。有關 PPTP 的資料已記錄於 RFC2637。

---

<sup>5</sup> <http://www.networkworld.com/community/node/23073>

基於 PPTP 的 VPN 連接，支援和 PPP 連接相同的認證機制，例如可擴展認證規約（Extensible Authentication Protocol, EAP）、MS-CHAP（Microsoft Challenge-Handshake Authentication Protocol）、CHAP、SPAP（Shiva Password Authentication Protocol）和 PAP（Password Authentication Protocol）。在加密方面，MPPE（Microsoft Point-to-Point Encryption）以 RSA RC4（40/56/128 位元）標準為基礎，用於加密連接，因此可選擇用 MPPE 為 PPP 數據進行加密。

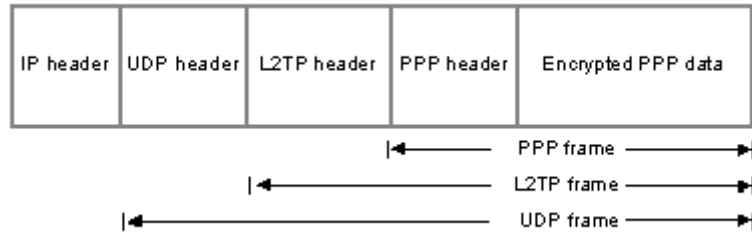


PPTP 數據隧道經過多重壓縮而形成，並利用經修改的通用路由壓縮（Generic Routing Encapsulation, GRE）版本將 PPP 格式壓縮成為在 IP 網絡（例如互聯網或私有內聯網）傳輸的數據。GRE 為傳遞 PPP 小包提供流向和阻塞受控的壓縮服務，經壓縮 PPP 格式的數據可以進行加密（及／或壓縮）。這樣產生的 GRE 和 PPP 壓縮數據將被加入 IP 標頭，該標頭包含適當的來源和目的地 IP 位址，為 PPTP 客戶和 PPTP 伺服器提供資料。在收取 PPTP 傳輸的數據時，PPTP 伺服器會處理並移除 IP、GRE 和 PPP 標頭，然後將 PPP 數據解密（及／或解除壓縮）。

## 第二層隧道規約（Layer 2 Tunneling Protocol L2TP）

L2TP 由 PPTP 和思科（Cisco）的 L2F（Layer Two Forwarding）規約結合而成。L2TP 能作為隧道規約使用，將 PPP 格式壓縮，以便在 IP、X.25、Frame Relay 或 ATM 網絡傳輸。多個連接可以經過一條隧道傳輸。如 PPTP 和 L2F 一樣，L2TP 在 OSI 第二層操作，第二層 VPN 規約將 PPP 格式的數據壓縮，並能夠在 IP 網絡傳輸非 IP 規約。有關 L2TP 的標準已被記錄於 RFC3931。

L2TP 使用的認證機制與 PPP 連接相同，例如 EAP、CHAP、MS-CHAP、PAP 及 SPAP。L2TP 隧道經過多重壓縮而形成，而 PPP 數據被壓縮在 PPP 標頭和 L2TP 標頭中。L2TP 的壓縮小包再被壓縮到 UDP 標頭中，來源及目的地埠則被設定為 1701。最後，小包再進一步被壓縮成為一個有 IP 標頭的封包，而該 IP 標頭包含了 VPN 客戶和 VPN 伺服器的來源和目的地 IP 位址。



由於 L2TP 缺乏機密性，使用時通常會配合 IPsec 成為 L2TP/IPsec。當 L2TP 在 IPsec 之上被使用，保安服務便會由 IPsec、AH 和 ESP 提供，而所有 L2TP 控制及數據對於 IPsec 系統來說則被視為是同類的 IP 數據包。

## SSL / TLS<sup>6</sup>

SSL / TLS 屬於傳輸層規約，使用 TCP 埠 443。SSL 規約由 IETF 訂立，最後版本為 3.1，其後再沒有其它新版本出現。TLS 1.0 和 TLS 1.1 是 TLS 兩個標準化的版本，而 TLS 1.0 等同 SSL 3.1。

SSL / TLS 提供了很多加密功能，包括機密性、完整性和數碼簽署。SSL / TLS 有別於 IPsec，後者須通訊雙方協意相同的加密功能，前者則使用密碼組合訂立加密功能，並且用於客戶和伺服器通訊傳輸。

只要由可信任的核證機關（Certification Authority, CA）簽署 SSL 伺服器證書，SSL VPN 閘口便能夠使用該核證向互聯網用戶作出認證，表示用戶可通過瀏覽器驗證自己正在與可信任的伺服器通訊。實際上，一些 SSL VPNs 或者會用自己簽署的數碼證書，而該證書並未獲大部份互聯網瀏覽器所信任。在這情況下，用戶須自行把 SSL VPN 的伺服器證書加入用戶的個人核證清單上，或選擇「接受」以表示信任該證書。

<sup>6</sup> <http://csrc.nist.gov/publications/drafts/SP800-113/Draft-SP800-113.pdf>

## IV. VPN 的風險和限制

### 入侵者攻擊

客戶電腦可能成為攻擊目標，或成為入侵者攻擊相連網絡的跳板。入侵者可能針對客戶電腦的保安漏洞或錯誤配置，甚至利用入侵工具發起攻擊。攻擊的種類包括 VPN 劫持或中間人攻擊：

1. VPN 劫持即未經授權從遠程客戶劫持已建立的 VPN 連接，並在相連的網絡中偽冒該客戶。
2. 中間人攻擊指影響通訊各方之間的信息往來，包括截取、介入、刪除、竄改信息、將信息寄返寄件人、重放舊信息及轉發信息。

### 用戶身份認證

雖然應該只有經認證的用戶才能夠連接 VPN，但基本上，VPN 沒有提供或實施強化預設的用戶認證。如果認證強度不足而未能遏止未經授權的接達，未經授權人士便有可能接達已連接的網絡和資源。部份 VPN 推行方案只提供有限度的認證方法，例如用於 PPTP 的 PAP 以純文字傳輸用戶名稱和密碼，讓第三者能夠竊取資料並用來接達網絡。

### 客戶方風險

家庭用戶的 VPN 客戶電腦可能使用分隔隧道，一邊用 VPN 連接私有網絡，同時以寬頻連接互聯網，這樣便會令已連接的私有網絡構成風險。

用戶可能同時與保安意識薄弱的使用者共用同一部電腦，另外，流動用戶可能使用手提電腦在酒店連接無線 LAN、在機場或經其它外國網絡連接互聯網。然而，上述大部份地點的保安保護並不足夠。VPN 客戶電腦不論在連接前，還是連接後被破解，都可能對相連接的網絡構成威脅。

### 電腦病毒／惡意軟件感染

當客戶端受到電腦病毒感染，相連接的網絡便有機會受影響。客戶電腦如果受到電腦病毒感染，則有可能向攻擊者發放連接 VPN 的密碼。就內聯網或外聯網 VPN 連接而言，

如果抗電腦病毒保護系統失效，而其中一個網絡受到電腦病毒感染，便有可能迅速地向其它網絡散播電腦病毒／蠕蟲。

### **不恰當的網絡接達權**

部份客戶及／或相連接網絡獲授予的接達權可能已超出所需。

### **互用性**

互用性是另一個值得注意的問題。舉例說，由兩個不同供應商提供的 IPsec 兼容軟件不一定可以一起使用。

## V. 保安考慮事項

### 一般 VPN 保安考慮事項

推行 VPN 時的一般保安建議如下：

1. 使用防火牆，以加強 VPN 連接的保安。
2. 可使用 IDS / IPS（入侵偵測／防禦系統）以便更有效地監察攻擊。
3. 須於遠程客戶端和網絡伺服器安裝抗電腦病毒軟件，當其中一端受電腦病毒感染時，便有助防止電腦病毒／蠕蟲散播。
4. 認證功能簡單或沒有認證功能的不安全系統或無人管理的系統不得與內部網絡建立 VPN 連接。
5. 必須提供記錄和審計功能，以記錄網絡連接，特別是意圖未經授權嘗試接達的情況，並定期審閱記錄。
6. 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。
7. 向有關方面派發恰當使用 VPN 和網絡支援的保安政策及指引，以規範他們對 VPN 的使用。
8. VPN 進入點應放置在隔離區（DMZ）內，以保護內部網絡。
9. 連接 VPN 時，不宜使用分隔隧道同時接達互聯網或其它不安全的網絡。如要使用分隔隧道，則應同時使用防火牆和 IDS，以偵測及防禦來自不安全網絡的攻擊。
10. 應規限及控制不必要的內部網絡接達。

### 外聯網 VPN 保安考慮事項

推行外聯網 VPN 時的額外保安考慮如下：

1. 必須實施強化用戶認證機制。
2. VPN 進入點應放置在 DMZ 內，以防止業務伙伴接達內部網絡。
3. 接達權必須因應需要而發放，對外部業務伙伴應只開放有必要接達的資源，而這些資源的擁有者須定期覆檢其接達權。

### 客戶端 VPN 保安考慮事項

給 VPN 用戶的一般保安考慮如下：

1. 用戶自廣泛而不信任的網絡接連 VPN 時須強化認證，例如：
  - 使用數碼證書及／或智能卡、或權標：  
智能卡用於儲存用戶配置檔、密碼匙和算法。智能卡通常使用 PIN 數字，權標卡則提供一個一次性的密碼。當用戶輸入正確的 PIN 數字並成功認證權標，咭上將顯示一個一次性的密碼，代表授權接達網絡。
  - 使用附加的認證系統，譬如 TACACS+或 RADIUS：  
這類中央認證系統包含所有 VPN 用戶的配置檔，以控制接達私有網絡的權利。
2. VPN 客戶電腦應妥善安裝及配置個人防火牆，以堵截未經授權接達，確保客戶電腦免受攻擊。近期不少遠程接達的 VPN 客戶已包括個人防火牆功能，其中一些還包括其它配置檢驗功能，例如當電腦病毒軟件未開啟或識別碼未更新，客戶電腦便不能夠連接網絡。
3. 客戶電腦應安裝抗電腦病毒軟件，還要不斷更新識別碼，以偵測及防禦電腦病毒。
4. 用戶應注意電腦的實體保安，特別是電腦內儲存了一些認證資料時。
5. 所有用戶應接受有關互聯網安全作業實務的培訓，從家中接達網絡，由於是經互聯網傳輸，所以應被列為不安全的渠道。

## VPN 產品常見的保安功能

選擇 VPN 產品時應注意以下的保安功能：

1. 支援強化認證，例如 TACACS+、RADIUS、智能卡／權標。
2. 業界證實有效的強化加密算法，具有長而強化的密碼匙支援能力，以保護傳輸中數據的機密性。
3. 支援抗電腦病毒軟件，並具有入侵偵測／防禦功能。
4. 強化所有管理／維護埠的保安預設。
5. 支援數碼證書，例如使用證書進行網站對網站認證。
6. 支援位址管理，譬如在私有網絡設定客戶位址，並且確保所有位址保持機密。

## VI. 總結

VPN 在不安全的公共網絡(例如互聯網)上為接達安全、私有的內部網絡提供連接方法，本文亦概述了多種 VPN 技術，其中 IPsec 和 SSL VPN 最為常用。雖然在不安全的網絡上使用 VPN 便能夠建立安全的傳輸渠道，然而，客戶端的保安考慮絕對不容忽視。