虛擬私人網路的工作原理

目錄

簡介

本檔案介紹VPN的基本原理，例如基本VPN元件、技術、通道和VPN安全性。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

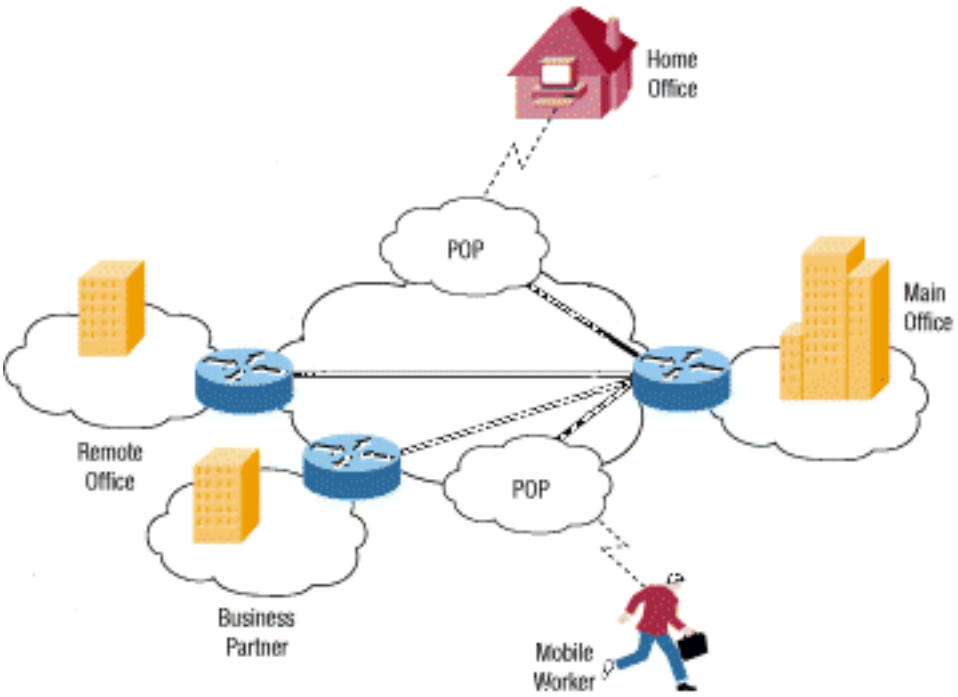
背景資訊

在過去的二十年裡，世界發生了很大變化。許多企業現在不得不考慮全球市場和物流，而不是只解決本地或地區問題。許多公司的設施遍佈全國甚至全世界。但有一件事所有公司都需要：一種無論其辦公室位於何處，都能保持快速、安全和可靠通訊的方式。

直到最近，可靠的通訊還意味著使用租用線路來維護廣域網(WAN)。 從整合多業務數位網路（ISDN，以144 Kbps的速度運行）到光載波–3（OC3，以155 Mbps的速度運行）光纖的租用線路

為公司提供了將私有網路擴展到其直接地理區域之外的途徑。就可靠性、效能和安全性而言，WAN比Internet這樣的公共網路有明顯的優勢；但是，維護WAN（尤其是使用租用線路時）成本可能非常高昂（隨著辦公室之間距離的增大，WAN的成本通常會增加）。 此外，對於部分員工具有高度移動性（市場行銷人員就是這樣），並且經常需要遠端連線到公司網路並訪問敏感資料的組織來說，租用線路並不是可行的解決方案。

隨著Internet的日益普及，企業紛紛將其用作擴展自身網路的手段。最先出現的是內部網，這是專為公司員工設計的網站。現在，許多公司都建立了自己的虛擬專用網路(VPN)來滿足遠端員工和遠端辦公室的需求。



典型的VPN可能在公司總部擁有主區域網(LAN)，在遠端辦公室或設施擁有其他LAN，以及在現場進行連線的個人使用者。

VPN是使用公共網路（通常是Internet）將遠端站點或使用者連線在一起的專用網路。VPN不使用專用的真實連線（如租用線路），而是使用通過Internet從公司專用網路路由到遠端站點或員工的「虛擬」連線。

什麼造就了VPN?

VPN有兩種常見型別。

- **遠端訪**問 — 也稱為虛擬專用撥號網路(VPDN)，這是公司使用的使用者到LAN連線，公司員工需要從各種遠端位置連線到專用網路。通常，希望設定大型遠端訪問VPN的公司會通過網際網路服務提供商(ISP)為其使用者提供某種形式的網際網路撥號帳戶。 然後，遠端工作者可以撥打1-800號碼以訪問網際網路，並使用其VPN客戶端軟體訪問公司網路。一家需要遠端訪問VPN的公司就是一個很好的例子，它是一家在現場有數百名銷售人員的大型公司。遠端訪問VPN允許公司專用網路和遠端使用者通過第三方服務提供商進行安全、加密的連線。
- **站點到站點** — 通過使用專用裝置和大規模加密，公司可以通過公共網路（如Internet）連線多個固定站點。每個站點只需要到同一公共網路的本地連線，因此節省了使用長專用租用線路的費用。站點到站點VPN可以進一步分為內部網或外部網。在同一公司的辦公室之間構建的站點到站點VPN稱為內部網VPN，而為連線公司與其合作夥伴或客戶而構建的VPN稱為外網VPN。

設計良好的VPN可為公司帶來巨大益處。例如，它可以：

- 擴展地理連通性
- 與傳統廣域網相比，降低運營成本
- 減少遠端使用者的傳輸時間和差旅成本
- 提高工作效率
- 簡化網路拓撲
- 提供全球聯網機會
- 提供遠端辦公支援
- 提供比傳統廣域網更快的投資回報(ROI)

設計良好的VPN需要哪些功能？它應包含以下內容：

- 安全
- 可靠性
- 可擴充性
- 網路管理
- 政策管理

類比：每個LAN都是IsLANd

想象一下你住在一個巨型海洋裡的島嶼上。在你周圍有成千上萬的其他島嶼，有些非常近，有些則更遠。通常的旅行方法是乘渡輪從你的島嶼前往你想要遊覽的任何島嶼。坐輪渡旅行意味著你幾乎沒有任何隱私。你所做的任何事都能被別人看到。

假設每個島嶼代表一個私有LAN，海洋代表網際網路。乘坐輪渡旅行時，類似於通過Internet連線到Web伺服器或另一台裝置。您對組成網際網路的電線和路由器沒有控制權，就像您對渡船上的其他人沒有控制權一樣。如果您嘗試使用公共資源連線兩個專用網路，則很容易出現安全問題。

你的島嶼決定建造一座通往另一個島嶼的橋樑，這樣人們就可以更方便、更安全、更直接地在兩個島嶼之間旅行。這座橋的修建和維護成本高昂，即使您連線的島嶼離這裡非常近。但是，對可靠、安全的路徑的需要是如此迫切，以至於您無論如何都要這樣做。你的島嶼想要連線到另一個距離遙遠的島嶼，但你卻認為成本太高。

這種情況與租用線路非常相似。橋樑（租用線路）與海洋（網際網路）是分開的，但它們能夠連線島嶼（區域網）。 許多公司之所以選擇這條路線，是因為它們需要連線遠端辦公室的安全性和可靠性。然而，如果辦公室之間距離很遠，那麼成本可能非常高 — 就像試圖修建一座跨越很大距離的橋樑一樣。

那麼VPN如何與這個類比相符呢？我們可以給我們島嶼的每一個居民他們自己的小型潛水艇帶這些特性。

- 速度很快。
- 無論你去哪裡都很容易隨身攜帶。
- 它可以完全將你隱藏起來，不讓任何其他船隻或潛艇進入。
- 它是可靠的。
- 一旦購買了第一艘潛艇，向您的艦隊增加額外潛艇的成本就非常低。

雖然他們和其他交通工具一起在海洋中旅行，但我們的兩個島嶼的居民可以隨時自由地往返旅行，而且有隱私和安全。這基本上就是VPN的工作方式。網路的每個遠端成員都可以使用Internet作為連線到專用LAN的介質，以安全可靠的方式進行通訊。VPN可以擴展以適應更多使用者和不同位置，比租用線路更簡單。事實上，可擴充性是VPN相對於典型租用線路的主要優勢。與成本隨距離增

加而成比例的租用線路不同，建立VPN時每個辦公室的地理位置無關緊要。

VPN技術

設計良好的VPN使用多種方法來確保連線和資料安全。

- **資料保**密性 — 這也許是任何VPN實施所提供的最重要服務。由於私有資料通過公共網路傳輸，因此資料保密性至關重要，可通過加密資料來實現。這個過程就是將一台電腦要傳送到另一台電腦的所有資料編碼成只有另一台電腦可以解碼的形式。大多數VPN使用其中一種協定來提供加密。**IPsec** -網際網路通訊協定安全通訊協定(IPsec)提供增強的安全功能，例如更強大的加密演算法和更全面的驗證。IPsec有兩種加密模式：隧道和運輸。通道模式會加密每個封包的標題和負載，而傳輸模式只會加密負載。只有符合IPsec規範的系統才能利用此協定。此外，所有裝置必須使用公共金鑰或證書，並且必須設定非常相似的安全策略。對於遠端訪問VPN使用者，某種形式的第三方軟體包可在使用者PC上提供連線和加密。IPsec支援56位（單DES）或168位（三重DES）加密。**PPTP/MPPE** — PPTP由PPTP論壇建立，該論壇是一個包括美國機器人、微軟、3COM、Ascend和ECI Telematics的聯盟。PPTP支援多協定VPN，使用稱為Microsoft點對點加密(MPPE)的協定進行40位和128位加密。 必須注意的是，PPTP本身不提供資料加密。**L2TP/IPsec** — 通常稱為L2TP over IPsec，這在第2層通道通訊協定(L2TP)的通道上提供IPsec通訊協定的安全性。L2TP是PPTP論壇、思科和Internet工程任務組(IETF)成員之間合作關係的產物。 主要用於Windows 2000作業系統的遠端訪問VPN，因為Windows 2000提供本地IPsec和L2TP客戶端。Internet服務提供商還可以為撥入使用者提供第2層TP連線，然後在接入點和遠端辦公室網路伺服器之間使用IPsec加密該流量。
- **資料完**整性 — 雖然資料必須通過公共網路進行加密，但驗證資料在傳輸過程中是否未更改也同樣重要。例如，IPsec有一種機制可以確保資料包的加密部分（或資料包的整個報頭和資料部分）沒有被篡改。如果檢測到篡改，資料包將被丟棄。資料完整性還包括對遠端對等體進行身份驗證。
- **資料來源**身份驗證 — 驗證傳送的資料的源身份非常重要。這是防範許多依賴於欺騙傳送者身份的攻擊所必需的。
- **Anti Replay** — 能夠檢測並拒絕重放的資料包，並幫助防止欺騙。
- **資料通道/流量保密性** — 通道是將整個封包封裝到另一個封包中並通過網路傳送封包的流程。在需要隱藏發起流量的裝置的身份的情況下，資料隧道非常有用。例如，使用IPsec的單個裝置會封裝屬於其後面大量主機的流量，並在現有資料包之上新增自己的報頭。透過加密原始封包和標頭（並根據在頂部新增的額外第3層標頭路由封包），通道裝置可有效隱藏封包的實際來源。只有受信任的對等方才能確定真正的源，在它去除附加報頭並解密原始報頭之後。如RFC 2401 中所述，「……在有些情況下，披露通訊的外在特徵也可能成為一項令人關注的問題。流量機密性是通過隱藏源和目標地址、消息長度或通訊頻率來解決後一個問題的服務。在IPsec環境中，在隧道模式下使用ESP（尤其是在安全網關上）可以提供某種級別的流量機密性。」此處列出的所有加密通訊協定也使用通道作為透過公用網路傳輸加密資料的方法。必須認識到，隧道本身並不提供資料安全性。原始封包僅封裝在另一個通訊協定中，如果沒有加密，封包擷取裝置可能仍會看到原始封包。但是此處提到它，因為它是VPN運作方式不可分割的一部分。通道需要三種不同的通訊協定。**乘客通**訊協定 — 傳送的原始資料(IPX、NetBeui、IP)。**封裝通**訊協定 — 封裝在原始資料周圍的通訊協定(GRE、IPsec、L2F、PPTP、L2TP)。**載體通**訊協定 — 資訊傳送所使用的網路通訊協定。原始封包（乘客通訊協定）會封裝在封裝通訊協定中，然後將該封包放在載波通訊協定的標頭（通常為IP）中，以便透過公用網路傳輸。請注意，封裝協定也經常執行資料加密。IPX和NetBeui等通常不會通過Internet傳輸的協定可以安全地進行傳輸。對於站點到站點VPN，封裝協定通常是IPsec或通用路由封裝(GRE)。GRE包括有關您要封裝的封包型別的資訊，以及有關使用者端和伺服器之間連線的資訊。對於遠端訪問

VPN，隧道通常使用點對點協定(PPP)進行。 作為TCP/IP協定棧的一部分，PPP是主機電腦與遠端系統之間通過網路通訊時其他IP協定的載體。PPP通道將使用PPTP、L2TP或思科的第2層轉送(L2F)之一。

- **AAA** — 身份驗證、授權和記賬用於在遠端訪問VPN環境中實現更安全的訪問。如果沒有使用者身份驗證，任何坐在具有預配置VPN客戶端軟體的筆記型電腦/PC上的人都可以建立到遠端網路的安全連線。但是，使用使用者身份驗證時，還必須輸入有效的使用者名稱和密碼才能完成連線。使用者名稱和密碼可以儲存在VPN終端裝置上，也可以儲存在外部AAA伺服器上，該伺服器可以為許多其他資料庫（如Windows NT、Novell、LDAP等）提供身份驗證。當建立隧道的請求從撥號客戶端傳入時，VPN裝置會提示輸入使用者名稱和密碼。接著可以本地驗證此檔案，或將其傳送到外部AAA伺服器，以檢查：您是誰（身份驗證）您有權執行的操作（授權）實際操作（會計）記帳資訊對於跟蹤出於安全稽核、計費或報告目的而使用的客戶端特別有用。
- **不可否**認性 — 在某些資料傳輸（尤其是與金融交易相關的資料傳輸）中，不可否認性是非常理想的特徵。這有助於防止出現一端拒絕參與交易的情況。與銀行要求您在兌現支票之前簽署一樣，不可否認性通過將數位簽章附加到已傳送的報文上而起作用，從而排除了傳送方拒絕參與交易的可能性。

存在許多可用於構建VPN解決方案的協定。所有這些協定都提供本文檔中列出的部分服務。協定的選擇取決於所需的服務集。例如，一個組織可能樂於接受以明文形式傳輸的資料，但極其關心保持其完整性，而另一個組織可能發現保持資料機密性絕對重要。因此，他們選擇的協定可能有所不同。有關可用協定及其相對優勢的詳細資訊，請參閱哪種VPN解決方案適合您？

VPN產品

根據VPN的型別（遠端訪問或站點到站點），您需要安裝某些元件來構建VPN。這些可能包括：

- 每個遠端使用者的案頭軟體客戶端
- 專用硬體，例如Cisco VPN集中器或Cisco Secure PIX防火牆
- 用於撥號服務的專用VPN伺服器
- 服務提供商用於遠端使用者VPN訪問的網路訪問伺服器(NAS)
- 專用網路和策略管理中心

由於沒有廣泛接受的實施VPN的標準，因此許多公司已經自行開發了返點解決方案。例如，思科提供多種VPN解決方案，其中包括：

- **VPN集中**器 — 結合最先進的加密和身份驗證技術，Cisco VPN集中器專門用於建立遠端訪問或站點到站點VPN，理想情況下是部署為單個裝置處理大量VPN隧道。VPN集中器是專門為滿足專門構建的遠端訪問VPN裝置的要求而開發的。集中器提供高可用性、高效能和可擴充性，並包括稱為可擴展加密處理(SEP)模組的元件，使使用者能夠輕鬆增加容量和吞吐量。集中器提供的型號適合具有100個或更少遠端訪問使用者的小型企業到具有10,000個併發遠端使用者的大型企業組織。

- **啟用VPN的路由器/VPN最佳化路由器** — 所有運行Cisco IOS®軟體的思科路由器都支援IPsec VPN。唯一的要求是路由器必須運行具有適當功能集的Cisco IOS映像。Cisco IOS VPN解決方案完全支援遠端訪問、內部網和外聯網VPN要求。這意味著Cisco路由器在連線到運行VPN客戶端軟體的遠端主機或連線到其他VPN裝置（如路由器、PIX防火牆或VPN集中器）時也能同樣正常工作。啟用VPN的路由器適用於具有中等加密和隧道要求的VPN，並完全通過Cisco IOS軟體功能提供VPN服務。支援VPN的路由器包括Cisco 1000、Cisco 1600、Cisco 2500、Cisco 4000、Cisco 4500和Cisco 4700系列。思科的VPN最佳化路由器提供可擴充性、路由、安全性和服務品質(QoS)。 這些路由器基於Cisco IOS軟體，而且有一種裝置適合各種情況，從小型辦公室/家庭辦公室(SOHO)訪問，到中央站點VPN聚合，再到大型企業需求。VPN最佳化路由器旨在滿足高加密和隧道要求，並且通常利用附加硬體（如加密卡）來實現高效能。VPN最佳化路由器的示例包括Cisco 800、Cisco 1700、Cisco 2600、Cisco 3600、Cisco 7200和Cisco

7500系列。
- **思科安全PIX防火牆** — 專用網際網路(PIX)防火牆將動態網路位址轉譯、代理伺服器、封包過濾、防火牆和VPN功能整合到單一硬體中。此裝置不是使用Cisco IOS軟體，而是具有高度簡化的作業系統，通過集中處理IP的能力來處理各種協定，從而獲得極強的穩定性和效能。與思科路由器一樣，所有PIX防火牆型號都支援IPsec VPN。只需要滿足啟用VPN功能的許可要求。

- **Cisco VPN Clients** — 思科同時提供硬體和軟體VPN客戶端。Cisco VPN客戶端（軟體）與Cisco VPN 3000系列集中器捆綁銷售，無需額外費用。此軟體客戶端可以安裝在主機上，用於安全地連線到中央站點集中器（或任何其他VPN裝置，如路由器或防火牆）。 VPN 3002硬體客戶端是在每台機器上部署VPN客戶端軟體的替代方案，它提供了到許多裝置的VPN連線。

選擇用於構建VPN解決方案的裝置最終是一個設計問題，取決於許多因素，包括所需的吞吐量和使用者數量。例如，在只有少數幾個使用者位於PIX 501之後的遠端站點上，您可以考慮將現有PIX配置為IPsec VPN端點，前提是您接受501的3DES吞吐量約為3 Mbps，且最大限製為5個VPN對等點。另一方面，在充當大量VPN隧道的VPN端點的中心站點上，進入VPN最佳化路由器或VPN集中器可能是一個好主意。現在根據型別（LAN到LAN或遠端訪問）和正在設定的VPN隧道數量進行選擇。支援VPN的眾多思科裝置為網路設計人員提供了大量的靈活性和穩健的解決方案，可滿足每一項設計需求。

相關資訊

- 瞭解VPDN

- 虛擬私人網路(VPN)
- Cisco VPN 3000系列集中器支援頁
- Cisco VPN 3000使用者端支援頁面
- IPsec協商/IKE通訊協定支援頁面
- PIX 500系列防火牆支援頁面
- RFC 1661:點對點通訊協定(PPP)
- RFC 2661:第二層通道通訊協定「L2TP」
- 工作方式：虛擬私人網路的工作原理
- VPN概述
- Tom Dunigan的VPN頁面
- 虛擬私人網路聯盟
- 要求建議 (RFC)
- 技術支援 - Cisco Systems