哪種VPN解決方案適合您？

目錄

簡介

虛擬私人網路(VPN)作為在廣域網路中部署網路的低成本且更靈活的方式，正變得越來越流行。隨著技術的進步，實施VPN解決方案的選項也越來越多。本技術說明將解釋其中的一些選項，並介紹這些選項的最佳使用位置。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

必要條件

本文件沒有特定先決條件。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

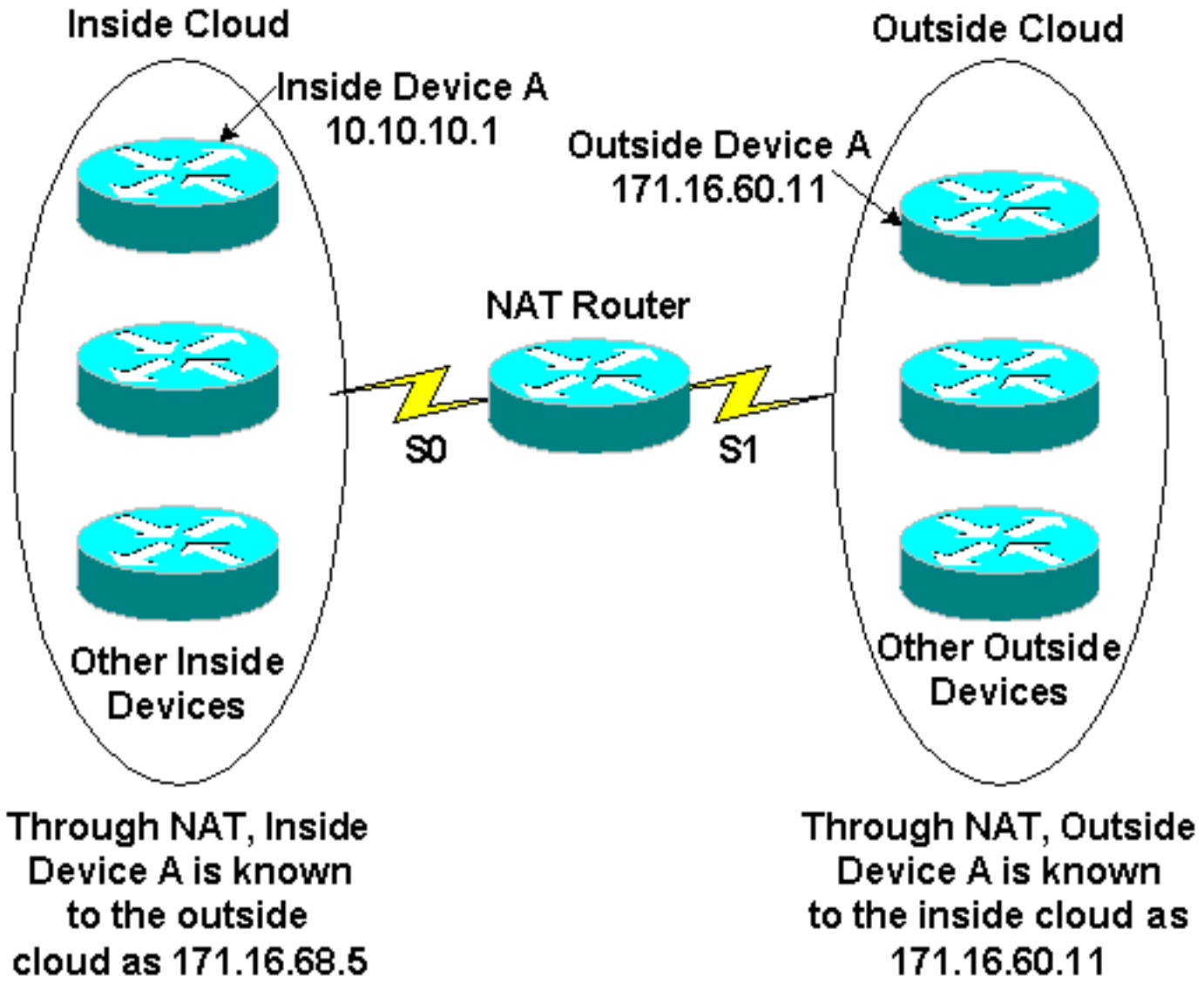
注意：思科還在非IOS平台（包括Cisco Secure PIX防火牆、Cisco VPN 3000集中器和Cisco VPN 5000集中器）中提供加密支援。

NAT

網際網路在短時間內經歷了爆炸式增長，遠遠超過了最初的設計者所能預見到的水準。IP版本4.0中可用地址的數量有限就是這種增長的證據，結果是地址空間變得越來越不可用。此問題的一個解決方案是網路地址轉換(NAT)。

使用NAT，路由器配置在內部/外部邊界上，以便外部（通常是Internet）看到一個或多個註冊地址，而內部可以使用私有編址方案擁有任意數量的主機。要維護地址轉換方案的完整性，必須在內部（專用）網路和外部（公共）網路之間的每個邊界路由器上配置NAT。從安全形度來看，NAT的優點之一是，除非將NAT網關專門配置為允許連線，否則私有網路上的系統無法從外部網路接收傳入IP連線。此外，NAT對源裝置和目的裝置完全透明。NAT的建議操作涉及RFC 1918 ，其中概述了正確的私有網路編址方案。RFC1631 中詳述NAT標準。

下圖顯示帶內部轉換網路地址池的NAT路由器邊界定義。

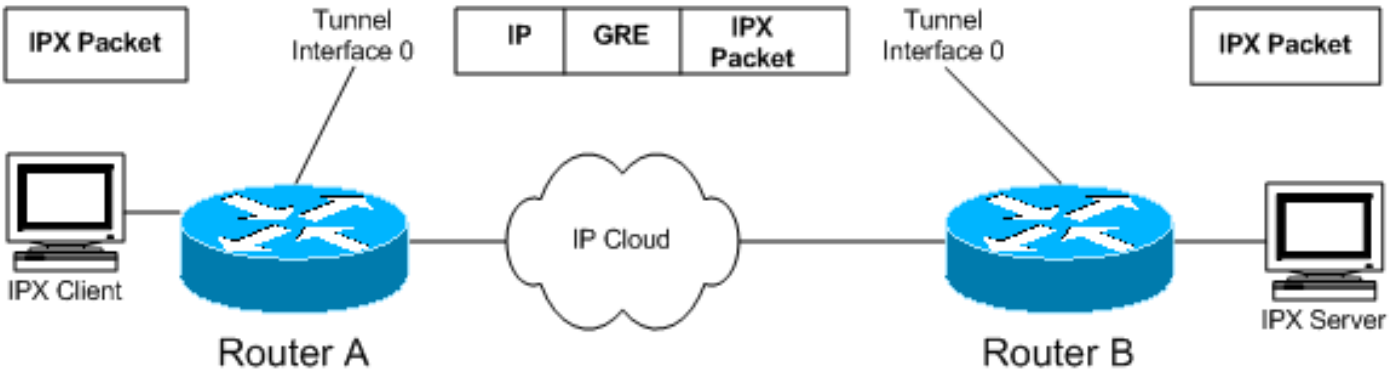


NAT通常用於保留Internet上可路由的IP地址，這些地址價格昂貴且數量有限。NAT還可以通過隱藏內部網路來防止Internet洩露，從而提供安全性。

有關NAT工作方式的資訊，請參閱NAT如何工作。

GRE封裝通道

通用路由封裝(GRE)通道提供跨共用WAN的特定路徑，並使用新封包標頭封裝流量，以確保傳送到特定目的地。網路是專用的，因為流量只能進入終端上的隧道，並且只能離開另一個終端。通道不提供真正的機密性（例如加密提供），但可以傳輸加密流量。通道是在傳輸流量的物理介面上配置的邏輯端點。



如圖所示，GRE隧道還可用於將非IP流量封裝到IP中，並通過Internet或IP網路傳送該流量。Internet資料包交換(IPX)和AppleTalk協定是非IP流量的示例。有關配置GRE的資訊，請參閱配置GRE中的「配置GRE通道介面」。

如果您擁有IPX或AppleTalk等多協定網路，並且必須通過Internet或IP網路傳送流量，則GRE是適合您的VPN解決方案。此外，GRE封裝通常與其他保護流量的方法（例如IPSec）結合使用。

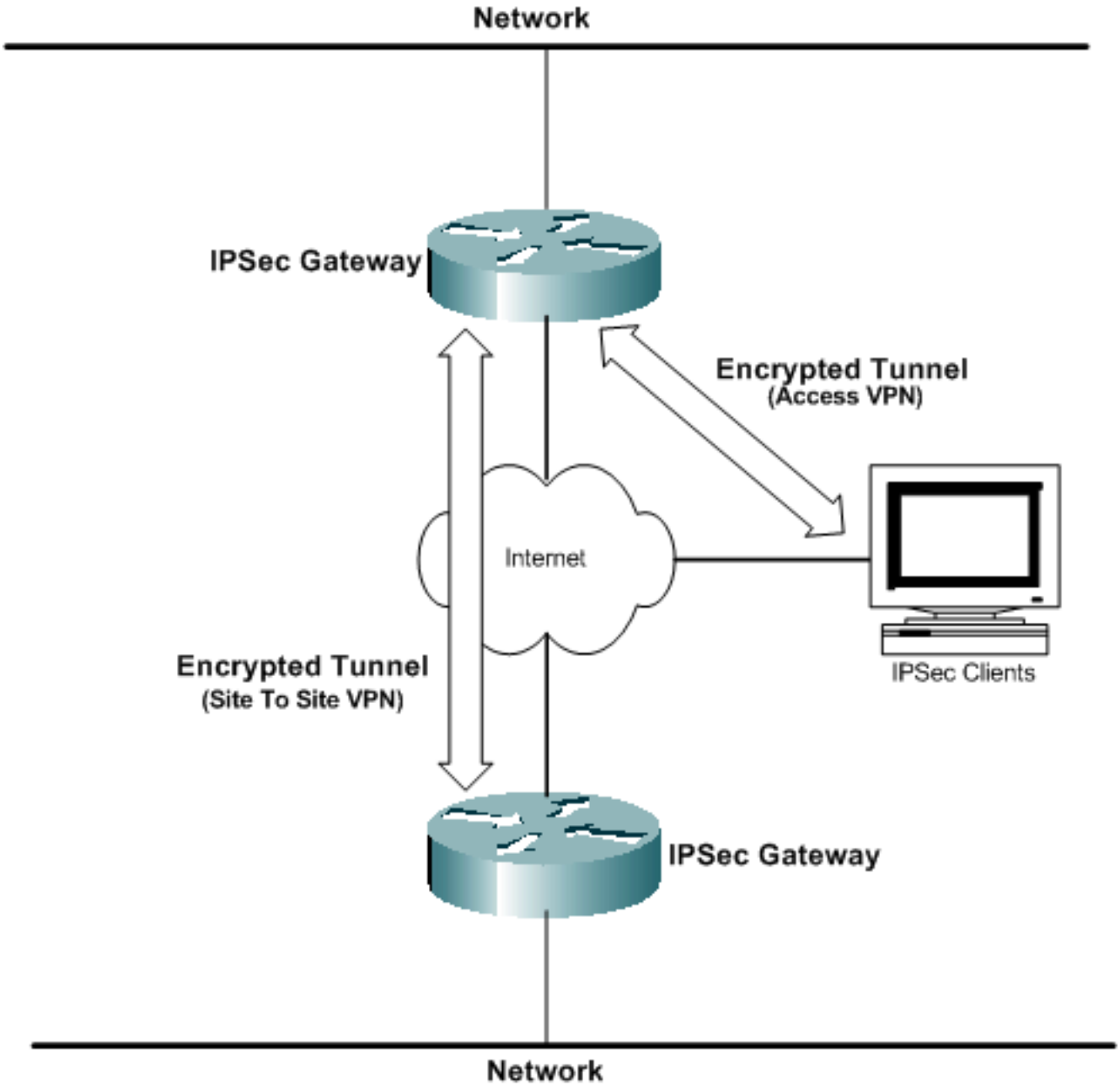
有關GRE的更多技術詳細資訊，請參閱RFC 1701 和RFC 2784 。

IPSec加密

通過共用網路傳送的資料加密是VPN最常與VPN相關聯的VPN技術。思科支援IP安全(IPSec)資料加密方法。IPSec是一個開放式標準框架，可在網路層的參與對等體之間提供資料機密性、資料完整性和資料身份驗證。

IPSec加密是Internet工程任務組(IETF)標準，在IPSec客戶端軟體中支援資料加密標準(DES)56位和三重DES(3DES)168位對稱金鑰加密演算法。IPSec的GRE配置是可選的。IPSec還支援證書頒發機構和網際網路金鑰交換(IKE)協商。IPSec加密可以在客戶端、路由器和防火牆之間的獨立環境中部署，也可以與接入VPN中的L2TP隧道結合使用。在各種作業系統平台上支援IPSec。

如果您希望網路具有真正的資料機密性，IPSec加密是適合您的VPN解決方案。IPSec也是一項開放標準，因此不同裝置之間的互操作性很容易實現。



PPTP和MPPE

點對點通道通訊協定(PPTP)是由Microsoft開發的；RFC2637 中對此進行了說明。PPTP廣泛部署在Windows 9x/ME、Windows NT和Windows 2000以及Windows XP客戶端軟體中，以啟用自願VPN。

Microsoft點對點加密(MPPE)是Microsoft提供的一種資訊性IETF草案，它使用基於RC4的40位或128位加密。MPPE是Microsoft PPTP客戶端軟體解決方案的一部分，在自願模式接入VPN架構中非常有用。大多數思科平台都支援PPTP/MPPE。

PPTP支援已新增到Cisco 7100和7200平台上的Cisco IOS軟體版本12.0.5.XE5。Cisco IOS 12.1.5.T新增了對更多平台的支援。Cisco Secure PIX Firewall和Cisco VPN 3000 Concentrator還支援PPTP客戶端連線。

由於PPTP支援非IP網路，因此，在遠端使用者必須撥入公司網路才能訪問異構公司網路時，它非常有用。

有關配置PPTP的資訊，請參閱配置PPTP。

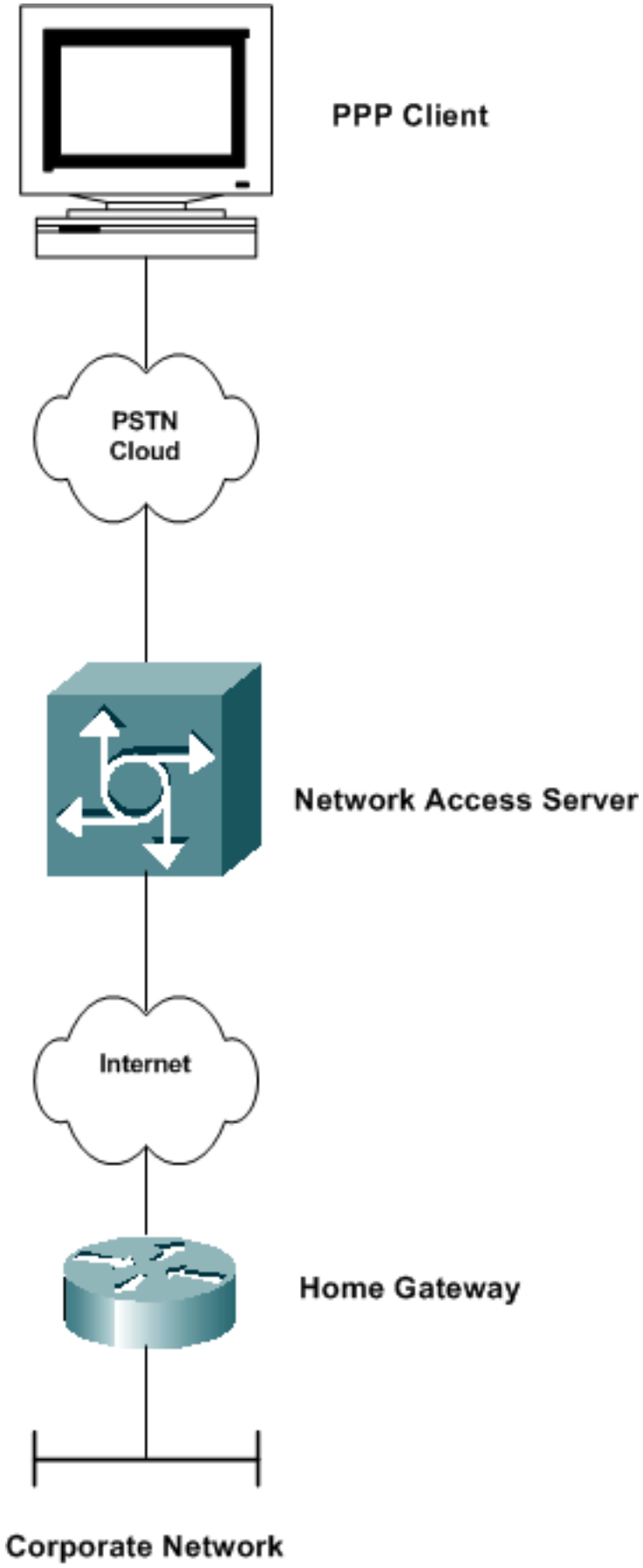
VPDN和L2TP

VPDN

虛擬專用撥接網路(VPDN)是思科的一項標準，允許私人網路撥入服務跨越到遠端存取伺服器。在VPDN的上下文中，撥入的存取伺服器（例如AS5300）通常稱為網路存取伺服器(NAS)。 撥入使用者的目的地稱為家庭網關(HGW)。

基本情景是點對點協定(PPP)客戶端撥入本地NAS。NAS確定PPP會話應轉發到該客戶端的家庭網關路由器。然後HGW對使用者進行身份驗證並啟動PPP協商。PPP設定完成後，所有幀都通過NAS傳送到客戶端和家庭網關。此方法整合了多個協定和概念。

有關配置VPDN的資訊，請參閱配置安全功能中的*配置虛擬專用撥號網路*。



L2TP

第2層通道通訊協定(L2TP)是一種IETF標準，它合併了PPTP和L2F的最佳屬性。L2TP隧道主要用於強制模式（即，將NAS撥號到HGW）訪問VPN，用於IP和非IP流量。Windows 2000和Windows XP已新增了對此協定的本機支援，作為VPN客戶端連線的方式。

L2TP用於使用IP在公共網路（例如Internet）上為PPP建立隧道。由於通道發生在第2層，因此上層通訊協定對通道一無所知。與GRE一樣，L2TP也可以封裝任何第3層協定。UDP埠1701用於通過隧道發起方傳送L2TP流量。

注意：在1996年，思科建立了一個第2層轉發(L2F)協定，允許VPDN連線發生。其他功能仍支援L2F，但已由L2TP取代。點對點通道通訊協定(PPTP)亦於1996年由IETF創立，為Internet草案。PPTP為PPP連線提供了類似於GRE的隧道協定的功能。

有關L2TP的詳細資訊，請參閱第2層隧道協定。

PPPoE

乙太網路PPP(PPPoE)是主要部署於數位使用者線路(DSL)環境中的一種資訊RFC。PPPoE利用現有的乙太網路基礎架構，讓使用者可以在同一個LAN中啟動多個PPP作業階段。此技術支援第3層服務選擇，這是一個新興應用程式，允許使用者通過單個遠端訪問連線同時連線到多個目標。帶有密碼驗證通訊協定(PAP)或挑戰握手驗證通訊協定(CHAP)的PPPoE通常用於通知中央站點哪些遠端路由器連線到它。

PPPoE主要用於服務提供商DSL部署和橋接乙太網拓撲。

有關配置PPPoE的詳細資訊，請參閱通過乙太網和IEEE 802.1Q VLAN配置PPPoE。

MPLS VPN

多協定標籤交換(MPLS)是基於思科標籤交換的新IETF標準，可實現自動調配、快速推廣和可擴充性功能，提供商需要經濟高效地提供接入、內部網和外聯網VPN服務。思科正在與服務提供商密切合作，以確保平穩過渡到支援MPLS的VPN服務。MPLS以基於標籤的模式工作，在資料包進入提供商網路時對其進行標籤，以通過無連線IP核心加快轉發。MPLS使用路由區分符來標識VPN成員身份並包含VPN社群內的流量。

MPLS還通過建立標籤交換路徑將面向連線的方法的優勢新增到IP路由模式，這些路徑是根據拓撲資訊而不是流量建立的。MPLS VPN廣泛部署於服務提供商環境中。

有關配置MPLS VPN的資訊，請參閱配置基本MPLS VPN。

相關資訊

- IPSec支援頁面
- 虛擬私人網路的工作原理
- NAT支援頁面
- GRE支援頁面
- VPDN支援頁面
- PPTP支援頁面
- PPPoE支援頁面
- 技術支援 - Cisco Systems