Quale soluzione VPN è giusta per te?

Sommario

Introduzione

Le VPN (Virtual Private Network) stanno diventando sempre più diffuse come metodo più flessibile e a basso costo per installare una rete in un'ampia area. Con i progressi tecnologici, aumenta la varietà di opzioni per l'implementazione di soluzioni VPN. In questa nota tecnica vengono illustrate alcune di queste opzioni e viene descritto il modo migliore per utilizzarle.

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

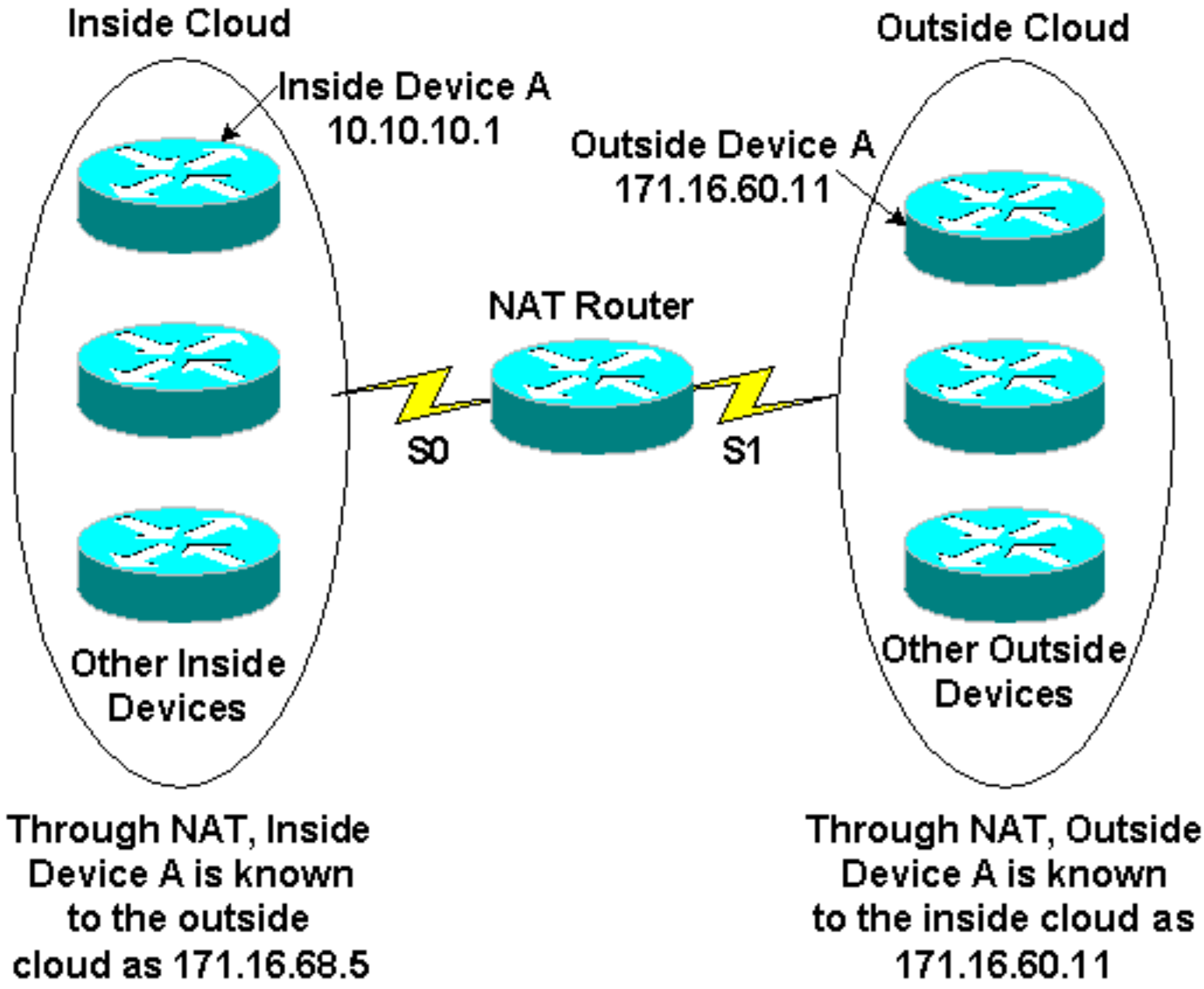
Nota: Cisco fornisce anche il supporto della crittografia nelle piattaforme non IOS, tra cui Cisco Secure PIX Firewall, Cisco VPN 3000 Concentrator e Cisco VPN 5000 Concentrator.

NAT

Internet ha conosciuto una crescita esplosiva in poco tempo, molto più di quanto i designer originali potessero prevedere. Il numero limitato di indirizzi disponibili nella versione IP 4.0 è la prova di questa crescita e il risultato è che lo spazio di indirizzi sta diventando sempre meno disponibile. Una soluzione a questo problema è NAT (Network Address Translation).

Utilizzando NAT, un router è configurato sui limiti interno/esterno in modo che l'esterno (generalmente Internet) veda uno o alcuni indirizzi registrati, mentre l'interno potrebbe avere un numero qualsiasi di host che utilizzano uno schema di indirizzamento privato. Per mantenere l'integrità dello schema di conversione degli indirizzi, NAT deve essere configurato su ogni router di confine tra la rete interna (privata) e la rete esterna (pubblica). Uno dei vantaggi di NAT dal punto di vista della sicurezza è che i sistemi della rete privata non possono ricevere una connessione IP in ingresso dalla rete esterna a meno che il gateway NAT non sia configurato in modo specifico per consentire la connessione. Inoltre, NAT è completamente trasparente nei confronti dei dispositivi di origine e destinazione. Il funzionamento consigliato da NAT prevede l'uso della RFC 1918 , che descrive schemi di indirizzamento della rete privata corretti. Lo standard NAT è descritto nella RFC1631 .

La figura seguente mostra la definizione dei limiti del router NAT con un pool di indirizzi della rete di conversione interna.

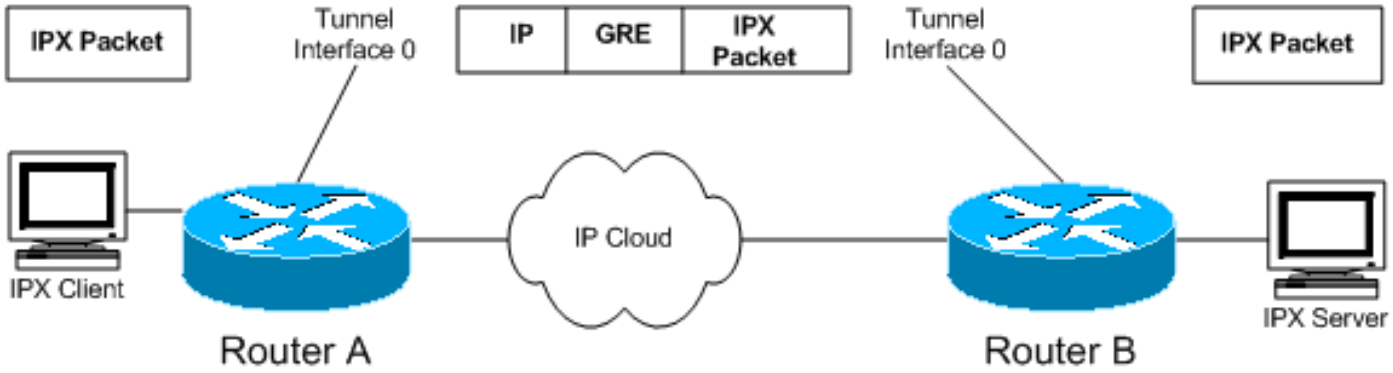


Il protocollo NAT viene generalmente utilizzato per conservare gli indirizzi IP instradabili su Internet, che sono costosi e di numero limitato. NAT garantisce inoltre la sicurezza nascondendo la rete interna da Internet.

Per informazioni sul funzionamento di NAT, vedere Funzionamento di NAT.

GRE Encapsulation Tunneling

I tunnel GRE (Generic Routing Encapsulation) forniscono un percorso specifico sulla WAN condivisa e incapsulano il traffico con nuove intestazioni di pacchetto per garantire la consegna a destinazioni specifiche. La rete è privata perché il traffico può entrare in un tunnel solo su un endpoint e può uscire solo sull'altro endpoint. I tunnel non garantiscono una reale riservatezza (come la crittografia), ma possono trasmettere il traffico crittografato. I tunnel sono endpoint logici configurati sulle interfacce fisiche attraverso cui viene trasportato il traffico.



Come mostrato nel diagramma, il tunneling GRE può essere usato anche per incapsulare il traffico non IP in IP e inviarlo su Internet o sulla rete IP. I protocolli Internet Packet Exchange (IPX) e AppleTalk sono esempi di traffico non IP. Per informazioni sulla configurazione del GRE, vedere "Configuring a GRE Tunnel Interface" in Configurazione del GRE.

GRE è la soluzione VPN giusta per te se hai una rete multiprotocollo come IPX o AppleTalk e devi inviare il traffico su Internet o una rete IP. Inoltre, l'incapsulamento GRE viene in genere utilizzato in combinazione con altri mezzi di sicurezza del traffico, ad esempio IPSec.

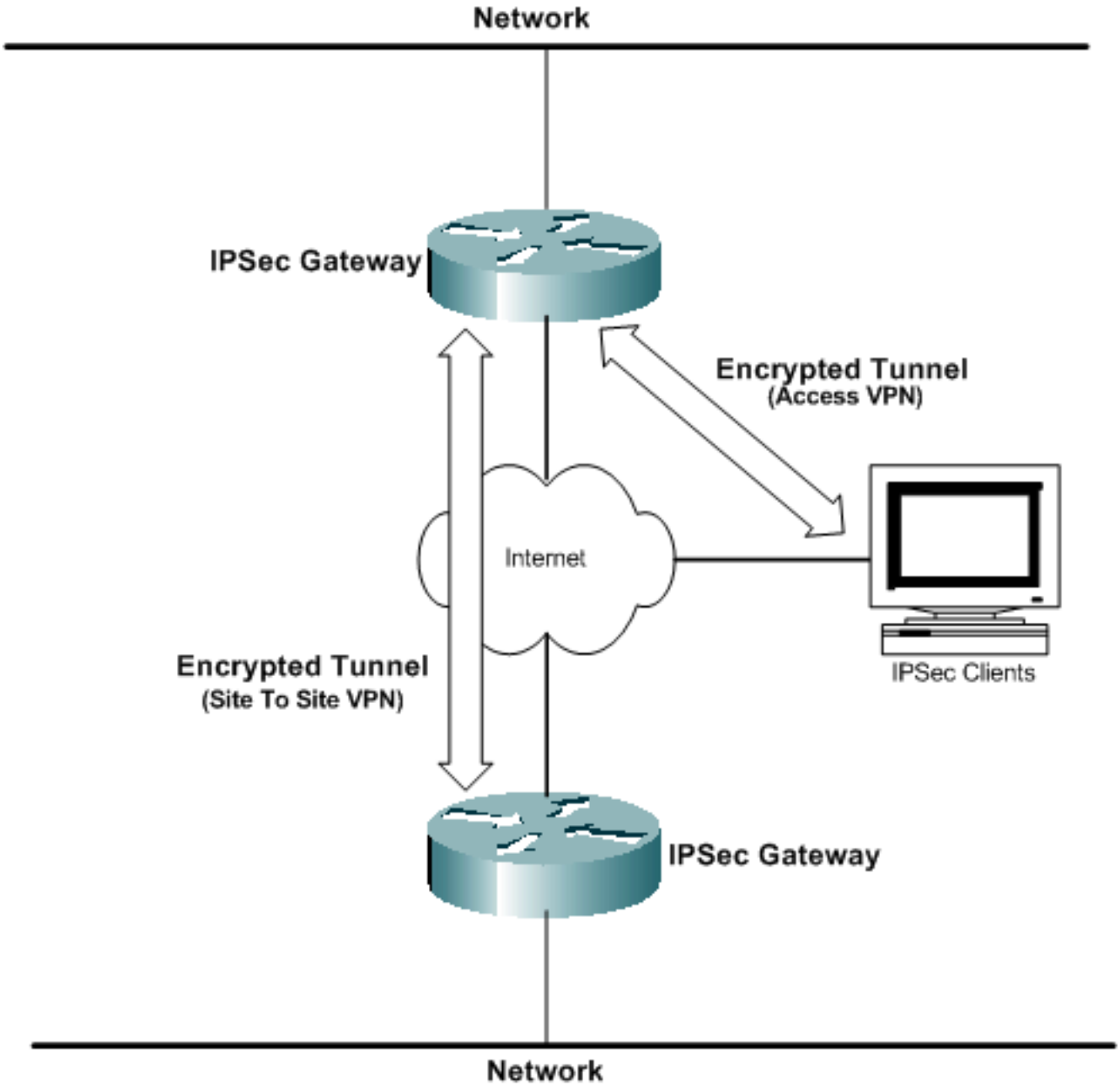
Per ulteriori dettagli tecnici sul GRE, consultare la RFC 1701 e la RFC 2784 .

Crittografia IPSec

La crittografia dei dati inviati tramite una rete condivisa è la tecnologia VPN più spesso associata alle VPN. Cisco supporta i metodi di crittografia dei dati IPSec (IP Security). IPSec è una struttura di standard aperti che fornisce la riservatezza, l'integrità e l'autenticazione dei dati tra i peer partecipanti a livello di rete.

La crittografia IPSec è uno standard IETF (Internet Engineering Task Force) che supporta gli algoritmi di crittografia a chiave simmetrica DES (Data Encryption Standard) a 56 bit e 3DES (Triple DES) a 168 bit nel software client IPSec. La configurazione GRE è facoltativa con IPSec. IPSec supporta inoltre le autorità di certificazione e la negoziazione IKE (Internet Key Exchange). La crittografia IPSec può essere implementata in ambienti standalone tra client, router e firewall oppure utilizzata in combinazione con il tunneling L2TP nelle VPN di accesso. IPSec è supportato in su diverse piattaforme di sistemi operativi.

La crittografia IPSec è la soluzione VPN ideale per le aziende che desiderano un'effettiva riservatezza dei dati per le reti. IPSec è anche uno standard aperto, pertanto l'interoperabilità tra dispositivi diversi è facile da implementare.



PPTP e MPPE

Il protocollo PPTP (Point-to-Point Tunneling Protocol) è stato sviluppato da Microsoft. è descritta nella RFC2637 . PPTP è ampiamente implementato nei software client Windows 9x/ME, Windows NT, Windows 2000 e Windows XP per abilitare le VPN volontarie.

MPPE (Microsoft Point-to-Point Encryption) è una bozza informativa IETF di Microsoft che utilizza la crittografia a 40 o 128 bit basata su RC4. MPPE fa parte della soluzione software client PPTP di Microsoft ed è utile nelle architetture VPN ad accesso volontario. PPTP/MPPE è supportato sulla maggior parte delle piattaforme Cisco.

Il supporto PPTP è stato aggiunto al software Cisco IOS versione 12.0.5.XE5 sulle piattaforme Cisco 7100 e 7200. Il supporto per più piattaforme è stato aggiunto in Cisco IOS 12.1.5.T. Cisco Secure PIX Firewall e Cisco VPN 3000 Concentrator includono anche il supporto per le connessioni client PPTP.

Poiché PPTP supporta le reti non IP, è utile quando gli utenti remoti devono connettersi alla rete

aziendale per accedere a reti aziendali eterogenee.

Per informazioni sulla configurazione di PPTP, vedere Configurazione di PPTP.

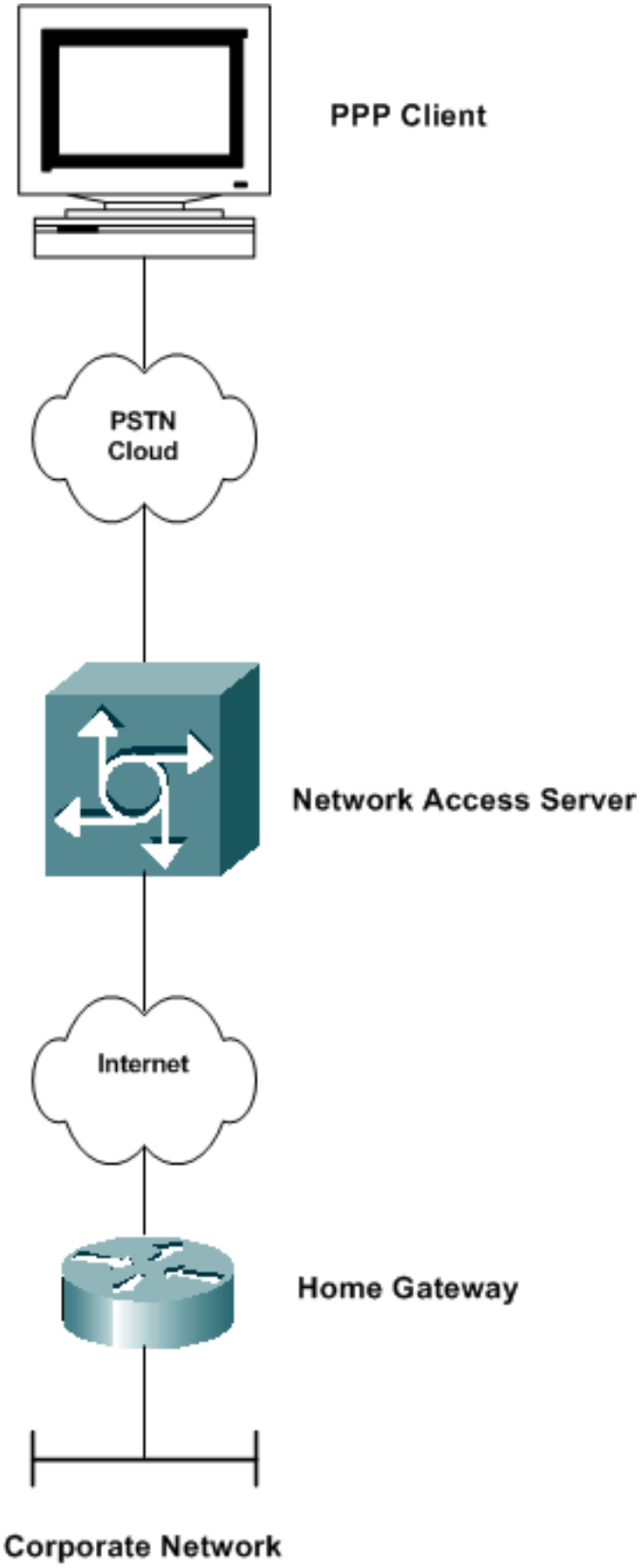
VPDN e L2TP

VPDN

VPDN (Virtual Private Dialup Network) è uno standard Cisco che consente a un servizio dial-in di rete privata di passare ai server di accesso remoto. Nel contesto della VPDN, il server di accesso (ad esempio, un AS5300) a cui si accede viene in genere denominato server di accesso alla rete (NAS). La destinazione dell'utente della chiamata in ingresso è detta gateway principale (HGW).

Lo scenario di base prevede la connessione di un client PPP (Point-to-Point Protocol) a un server NAS locale. Il server NAS determina che la sessione PPP deve essere inoltrata a un router gateway locale per quel client. HGW autentica quindi l'utente e avvia la negoziazione PPP. Al termine della configurazione del PPP, tutti i frame vengono inviati tramite NAS al client e ai gateway principali. Questo metodo integra diversi protocolli e concetti.

Per informazioni sulla configurazione della VPDN, vedere *Configurazione di una rete remota privata virtuale* in Configurazione delle funzionalità di sicurezza.



L2TP

Layer 2 Tunneling Protocol (L2TP) è uno standard IETF che incorpora i migliori attributi del PPTP e L2F. I tunnel L2TP sono utilizzati principalmente in modalità obbligatoria (vale a dire, connessione remota NAS a HGW) e VPN di accesso per il traffico IP e non IP. Windows 2000 e

Windows XP hanno aggiunto il supporto nativo per questo protocollo come mezzo di connessione client VPN.

L2TP viene utilizzato per eseguire il tunneling del protocollo PPP su una rete pubblica, ad esempio Internet, tramite IP. Poiché il tunnel si trova sul layer 2, i protocolli del layer superiore ignorano il tunnel. Come il GRE, l2TP può anche incapsulare qualsiasi protocollo di layer 3. La porta UDP 1701 viene utilizzata per inviare il traffico L2TP dall'iniziatore del tunnel.

Nota: nel 1996 Cisco ha creato un protocollo L2F (Layer 2 Forwarding) per consentire le connessioni VPDN. L2F è ancora supportato per altre funzioni, ma è stato sostituito da L2TP. Il protocollo PPTP (Point-to-Point Tunneling Protocol) è stato anch'esso creato nel 1996 dall'IETF con una bozza Internet. Il PPTP ha fornito una funzione simile al protocollo tunnel GRE per le connessioni PPP.

Per ulteriori informazioni su L2TP, vedere Layer 2 Tunnel Protocol.

PPPoE

PPP over Ethernet (PPPoE) è una RFC informativa implementata principalmente in ambienti DSL (Digital Subscriber Line). Il protocollo PPPoE sfrutta l'infrastruttura Ethernet esistente per consentire agli utenti di avviare più sessioni PPP sulla stessa LAN. Questa tecnologia consente di selezionare i servizi di layer 3, un'applicazione emergente che consente agli utenti di connettersi contemporaneamente a più destinazioni tramite un'unica connessione di accesso remoto. Il protocollo PPPoE con protocollo PAP (Password Authentication Protocol) o CHAP (Challenge Handshake Authentication Protocol) viene spesso utilizzato per informare il sito centrale a quali router remoti è connesso.

Il protocollo PPPoE viene utilizzato principalmente nelle distribuzioni DSL dei provider di servizi e nelle topologie Ethernet con bridging.

Per ulteriori informazioni sulla configurazione del protocollo PPPoE, vedere Configurazione di PPPoE over Ethernet e VLAN IEEE 802.1Q.

VPN MPLS

MPLS (Multiprotocol Label Switching) è un nuovo standard IETF basato su Cisco Tag Switching che consente il provisioning automatizzato, il rollout rapido e le funzionalità di scalabilità necessarie ai provider per fornire servizi VPN di accesso, Intranet ed Extranet a costi contenuti. Cisco sta collaborando con i provider di servizi per garantire una transizione graduale ai servizi VPN abilitati per MPLS. MPLS utilizza un paradigma basato su etichette e contrassegna i pacchetti quando entrano nella rete del provider per accelerare l'inoltro attraverso un core IP senza connessione. MPLS utilizza i differenziatori di route per identificare l'appartenenza alla VPN e contenere il traffico all'interno di una community VPN.

MPLS aggiunge anche i vantaggi di un approccio orientato alla connessione al paradigma del routing IP, attraverso la creazione di percorsi a commutazione di etichetta, creati in base alle informazioni sulla topologia piuttosto che al flusso del traffico. MPLS VPN è ampiamente implementata nell'ambiente dei provider di servizi.

Per informazioni sulla configurazione della VPN MPLS, vedere Configurazione di una VPN MPLS di base.

Informazioni correlate

- Pagina di supporto per IPSec
- Funzionamento delle reti private virtuali
- Pagina di supporto NAT
- Pagina di supporto GRE
- Pagina di supporto VPDN
- Pagina di supporto PPTP
- Pagina di supporto per PPPoE
- Supporto tecnico – Cisco Systems