Welke VPN-oplossing is geschikt voor u?

Inhoud

Inleiding

Virtual Private Networks (VPN's) worden steeds populairder als lagere kosten en flexibeler manier om een netwerk voor een groot gebied in te zetten. Dankzij de vooruitgang op het gebied van de technologie zijn er steeds meer opties voor het implementeren van VPN-oplossingen. In deze technische notitie worden een aantal van deze opties beschreven en beschreven waar ze het best kunnen worden gebruikt.

Voordat u begint

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Voorwaarden

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

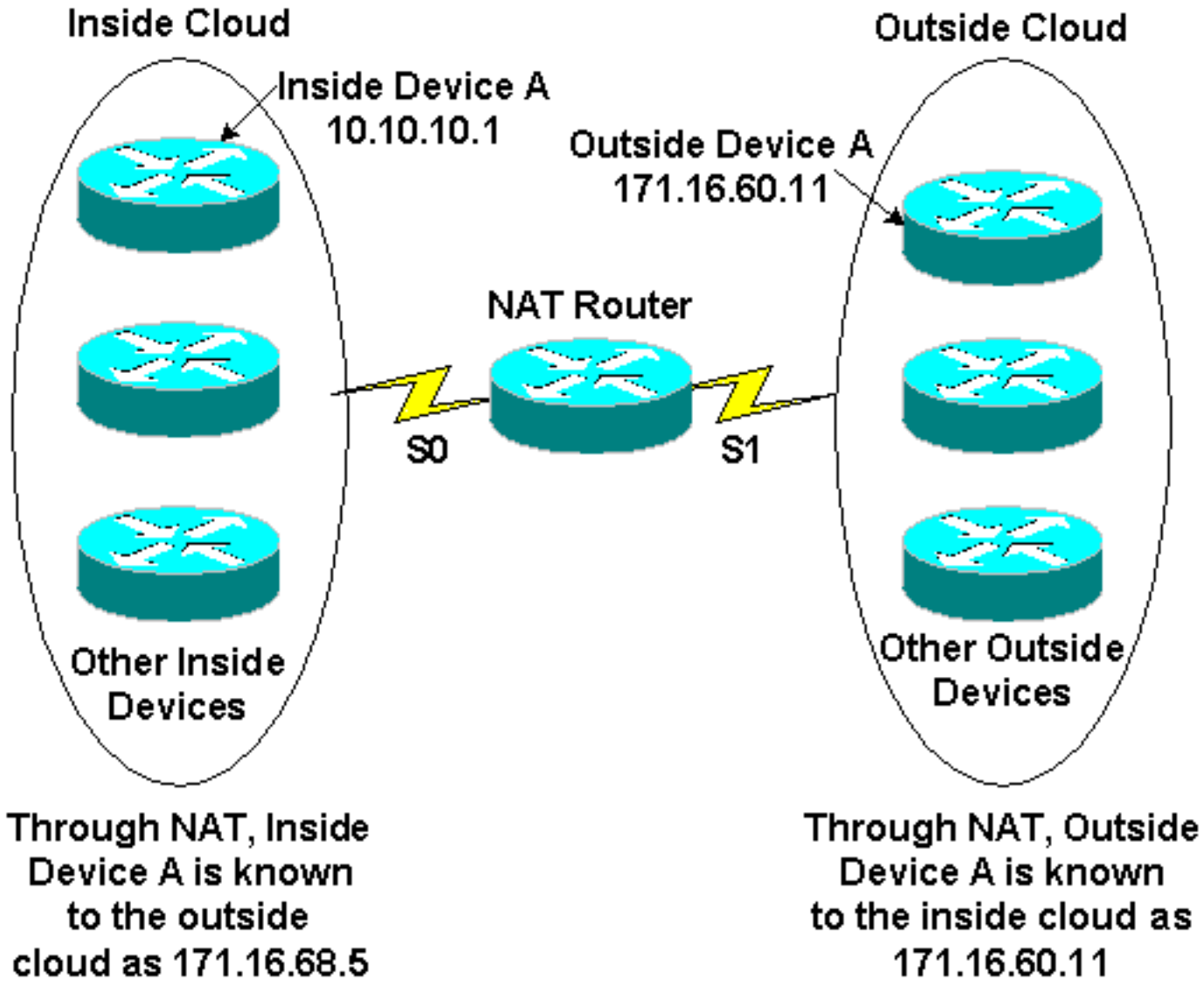
Opmerking: Cisco biedt ook coderingsondersteuning in niet-IOS platforms, inclusief de Cisco Secure PIX-firewall, Cisco VPN 3000 Concentrator en Cisco VPN 5000 Concentrator.

NAT

Het internet heeft in korte tijd een explosieve groei gekend, veel meer dan de oorspronkelijke ontwerpers hadden kunnen voorzien. Het beperkte aantal adressen dat in IP versie 4.0 beschikbaar is, is het bewijs van deze groei, en het resultaat is dat adresruimte minder beschikbaar wordt. Eén oplossing voor dit probleem is Netwerkadresomzetting (NAT).

Het gebruiken van NAT een router wordt gevormd op binnen/buiten grenzen zodat de buitenkant (gewoonlijk het Internet) één of een paar geregistreerde adressen ziet terwijl de binnenkant om het even welk aantal gastheren kon hebben die een privé adresseringsregeling gebruiken. Om de integriteit van het adresvertaalprogramma te behouden, moet NAT op elke grensrouter tussen het interne (private) netwerk en het externe (openbare) netwerk worden geconfigureerd. Een van de voordelen van NAT vanuit een veiligheidsstandpunt is dat de systemen op het particuliere netwerk geen inkomende IP-verbinding van het externe netwerk kunnen ontvangen tenzij de NAT-gateway specifiek is geconfigureerd om de verbinding mogelijk te maken. Bovendien is NAT volledig transparant voor de bron- en doelapparaten. De aanbevolen operatie van NAT betreft RFC 1918 , die de juiste privé-netwerkadresseringsschema's schetst. De standaard voor NAT wordt beschreven in RFC1631 .

Het volgende cijfer toont de definitie van de routergrens van NAT met een interne pool van vertaalnetwerken.

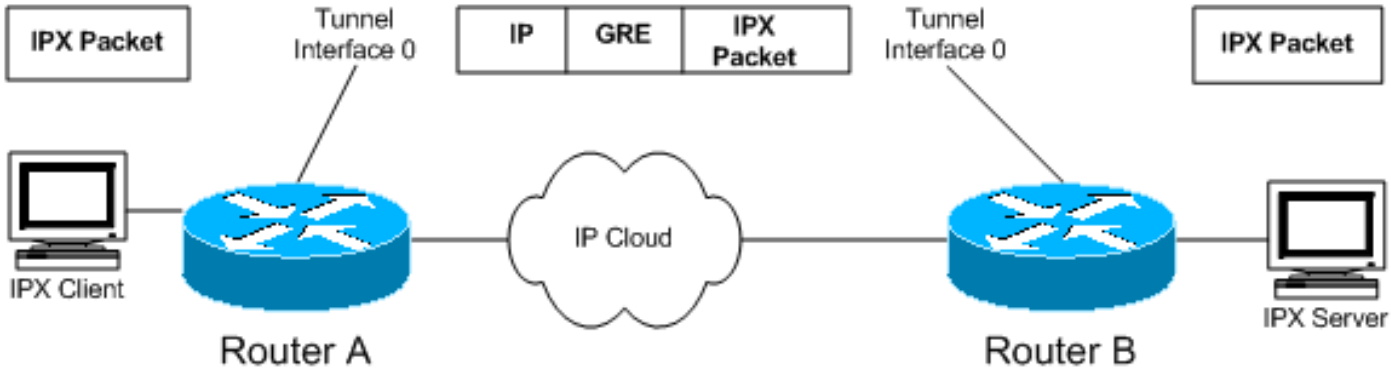


NAT wordt over het algemeen gebruikt om IP-adressen te besparen die op het internet te bedienen zijn, en die duur zijn en in aantal beperkt zijn. NAT biedt ook beveiliging door het binnennetwerk te verbergen voor het internet.

Zie Hoe NAT werkt voor informatie over het werken van NAT.

GRE-insluiting voor tunneling

Generic Routing Encapsulation (GRE)-tunnels bieden een specifieke route via het gedeelde WAN en omvatten verkeer met nieuwe pakketheaders om levering aan specifieke bestemmingen te garanderen. Het netwerk is privé omdat het verkeer een tunnel slechts op een eindpunt kan ingaan en slechts op het andere eindpunt kan verlaten. De tunnels bieden geen ware vertrouwelijkheid (zoals encryptie) maar kunnen gecodeerd verkeer dragen. tunnels zijn logische eindpunten die zijn ingesteld op de fysieke interfaces waardoor het verkeer wordt vervoerd.



Zoals in het diagram wordt geïllustreerd, kan de GRE-tunneling ook worden gebruikt om niet-IP-verkeer in IP in te sluiten en het via het internet of IP-netwerk te verzenden. De Internet Packet Exchange (IPX) en AppleTalk-protocollen zijn voorbeelden van niet-IP-verkeer. Zie "Een GRE-tunnelinterface configureren" in het configureren van GRE.

GRE is de juiste VPN-oplossing voor u als u een multiprotocol netwerk hebt zoals IPX of AppleTalk en u verkeer via het internet of een IP-netwerk moet verzenden. Tevens wordt de GRE-insluiting in het algemeen gebruikt in combinatie met andere middelen om verkeer te beveiligen, zoals IPSec.

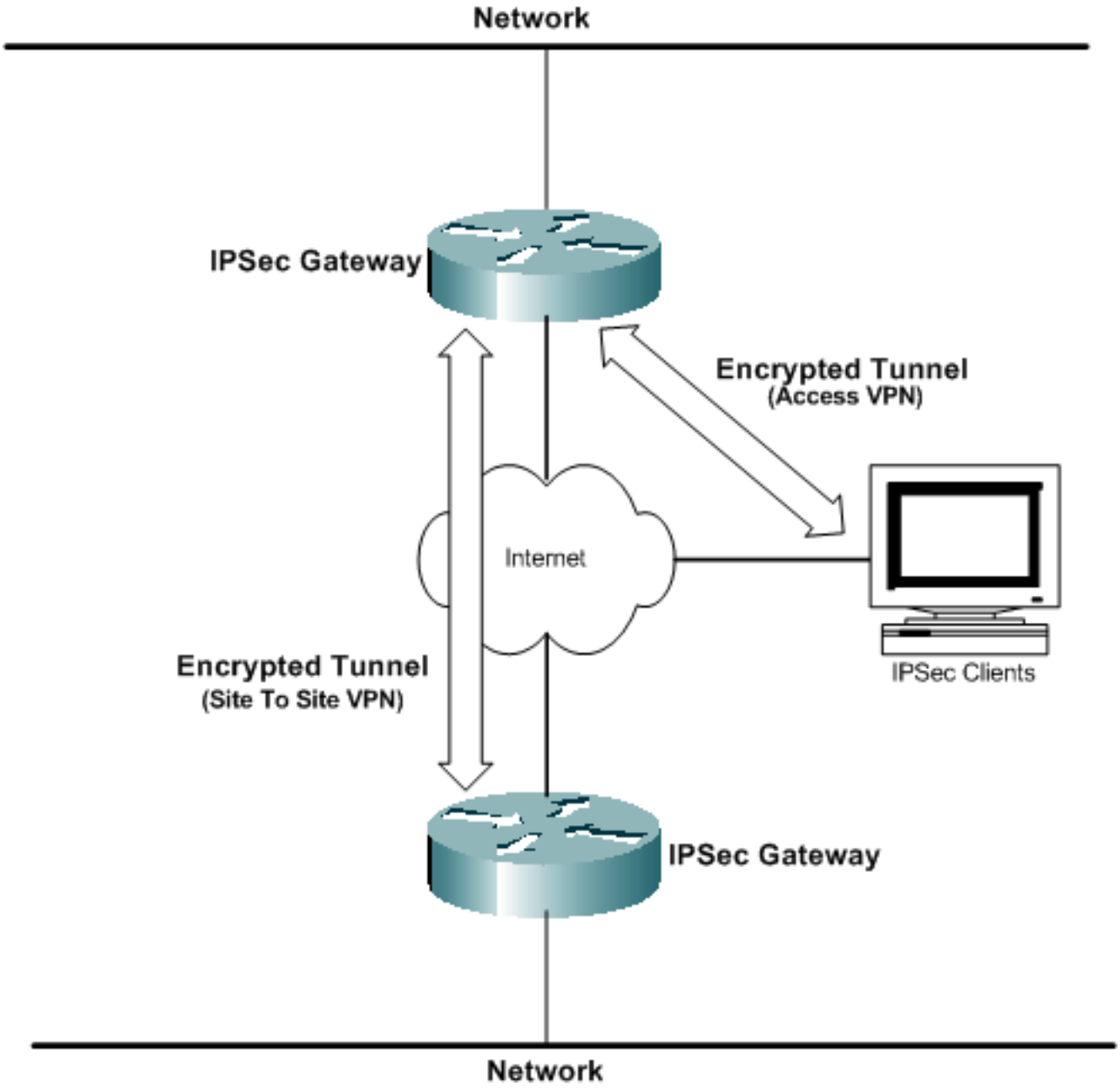
Voor meer technische details over GRE, zie RFC 1701 en RFC 2784 .

IPsec-encryptie

De encryptie van gegevens die over een gedeeld netwerk worden verzonden is de VPN technologie die het vaakst met VPN's verbonden is. Cisco ondersteunt de IP Security (IPSec) gegevenscoderingsmethoden. IPSec is een kader van open standaarden die gegevensvertrouwelijkheid, gegevensintegriteit en gegevensauthenticatie tussen deelnemende peers op de netwerklaag bieden.

IPSec encryptie is een standaard van Internet Engineering Task Force (IETF) die Data Encryption Standard (DES) 56-bits en Triple DES (3DES) 168-bits symmetrische sleutelencryptie-algoritmen in IPSec-clientsoftware ondersteunt. GRE-configuratie is optioneel met IPSec. IPSec ondersteunt ook certificeringsinstanties en onderhandeling over internet Key Exchange (IKE). IPSec-encryptie kan worden uitgevoerd in standalone omgevingen tussen klanten, routers en firewalls, of gebruikt in combinatie met L2TP-tunneling in access VPN's. IPSec wordt ondersteund op diverse besturingssysteemplatforms.

IPSec encryptie is de juiste VPN oplossing voor u als u ware gegevensvertrouwelijkheid voor uw netwerken wilt. IPSec is ook een open norm, zodat interoperabiliteit tussen verschillende apparaten makkelijk te implementeren is.



PPTP en MPPE

Point-to-Point Tunneling Protocol (PPTP) is ontwikkeld door Microsoft; het wordt beschreven in RFC2637 . PPTP wordt uitgebreid ingezet in Windows 9x/ME, Windows NT en Windows 2000 en Windows XP clientsoftware om vrijwillige VPN's mogelijk te maken.

Microsoft Point-to-Point Encryption (MPPE) is een informatief IETF-concept van Microsoft dat op RC4-gebaseerde 40-bits of 128-bits codering gebruikt. MPPE maakt deel uit van de PPTP client software oplossing van Microsoft en is handig in VPN-architecturen met vrijwillige toegang. PPTP/MPPE wordt ondersteund op de meeste Cisco-platforms.

PPTP-ondersteuning is toegevoegd aan Cisco IOS-softwarerelease 12.0.5.XE5 op de Cisco 7100- en 7200-platforms. Ondersteuning voor meer platforms is toegevoegd in Cisco IOS 12.1.5.T. Cisco Secure PIX-firewall en Cisco VPN 3000 Concentrator omvatten ook ondersteuning voor PPTP-clientverbindingen.

Aangezien PPTP niet-IP-netwerken ondersteunt, is het handig waar de externe gebruikers naar

het bedrijfsnetwerk moeten inbellen om toegang te krijgen tot heterogene bedrijfsnetwerken.

Zie PPTP configureren voor meer informatie over het configureren van PPTP.

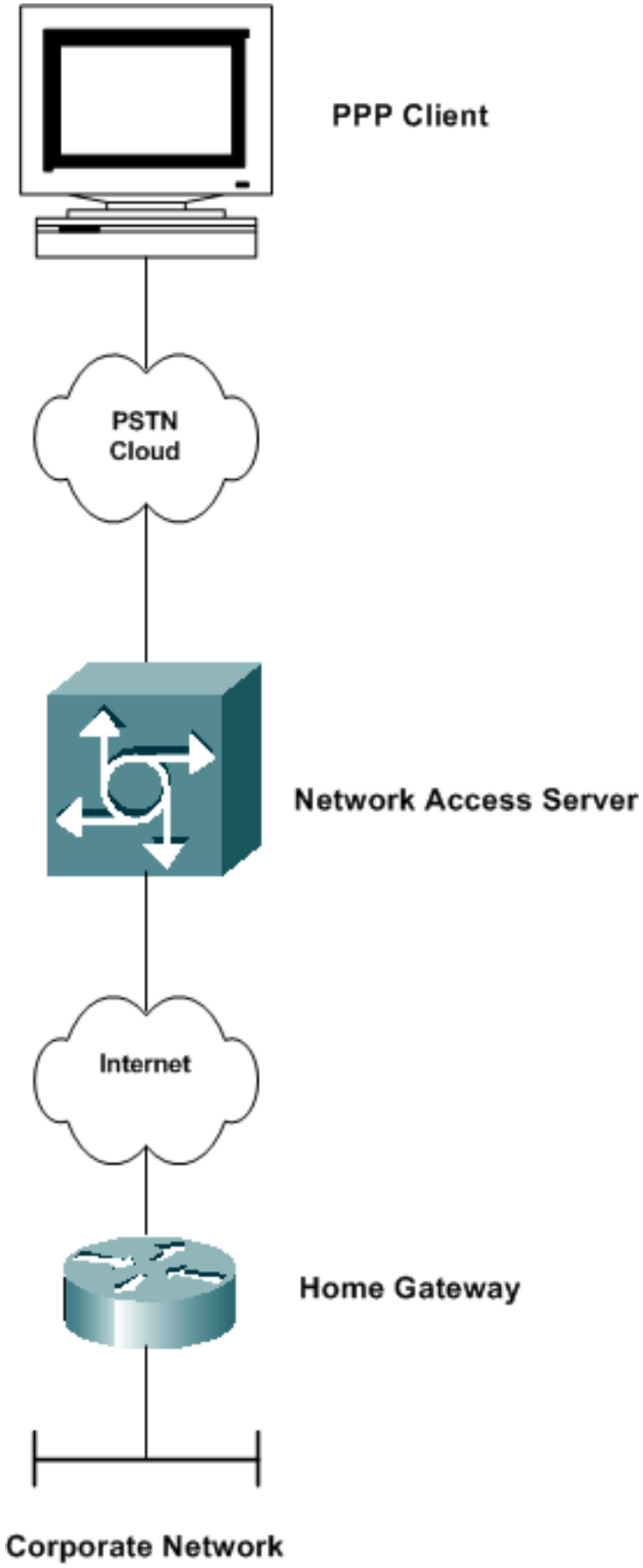
VPDN en L2TP

VPDN

Virtual Private Dialup Network (VPDN) is een Cisco-standaard waarmee een inbelservice voor een privaat netwerk kan worden uitgebreid naar externe toegangsservers. In de context van VPDN wordt de toegangsserver (bijvoorbeeld een AS5300) die wordt ingestuurd, gewoonlijk de Network Access Server (NAS) genoemd. De bestemming van de inbelgebruiker wordt aangeduid als de startgateway (HGW).

Het basisscenario is dat een Point-to-Point Protocol (PPP)-client naar een lokale NAS wijst. NAS bepaalt dat de PPP zitting aan een router van de huisgateway voor die client zou moeten worden doorgestuurd. HGW authenticeert de gebruiker en start de PPP onderhandeling. Nadat PPP de instelling is voltooid, worden alle frames via NAS naar de client en home gateways verzonden. Deze methode integreert verschillende protocollen en concepten.

Zie VPDN *configureren* voor meer informatie over het configureren *van een Virtual Private Dial-Up Network* in het configureren van beveiligingsfuncties.



L2TP

Layer 2 Tunneling Protocol (L2TP) is een IETF-standaard die de beste eigenschappen van PPTP en L2F omvat. L2TP-tunnels worden primair gebruikt in de verplichte modus (dat wil zeggen, dialup NAS to HGW) access VPN's voor zowel IP- als niet-IP-verkeer. Windows 2000 en Windows

XP hebben ondersteuning voor dit protocol toegevoegd als een middel voor VPN-clientverbinding.

L2TP wordt gebruikt om PPP over een openbaar netwerk, zoals het Internet, te tunnelen dat IP gebruikt. Aangezien de tunnel op Layer 2 plaatsvindt, zijn de bovenste laagprotocollen niet bekend van de tunnel. Net zoals GRE kan L2TP ook elk Layer 3-protocol insluiten. UDP-poort 1701 wordt gebruikt om L2TP-verkeer te verzenden door de initiatiefnemer van de tunnel.

Opmerking: In 1996 creëerde Cisco een Layer 2 Forwarding (L2F)-protocol om VPDN-verbindingen mogelijk te maken. L2F wordt nog steeds ondersteund voor andere functies, maar is vervangen door L2TP. Point-to-Point Tunneling Protocol (PPTP) werd in 1996 ook in het leven geroepen en door de IETF een internetontwerp. PPTP verstrekte een functie die vergelijkbaar is met GRE-achtige tunnelprotocol voor PPP-verbindingen.

Zie Layer 2 Tunnel Protocol voor meer informatie over L2TP.

PPPoE

PPP over Ethernet (PPPoE) is een informatieve RFC die primair wordt ingezet in DSL-omgevingen (Digital Subscriber Line). PPPoE benut bestaande Ethernet-infrastructuur om gebruikers toe te staan om meerdere PPP-sessies binnen hetzelfde LAN te initiëren. Deze technologie maakt Layer 3 service selectie mogelijk, een opkomende toepassing die gebruikers tegelijkertijd verbinding maakt met verschillende bestemmingen via één enkele externe toegangsverbinding. PPPoE met Password Authentication Protocol (PAP) of Challenge Handshake Authentication Protocol (CHAP) wordt vaak gebruikt om de centrale site te informeren over de externe routers die erop worden aangesloten.

PPPoE wordt over het algemeen gebruikt in DSL-implementaties van serviceproviders en gebride Ethernet-topologieën.

Voor meer informatie over het configureren van PPPoE, zie PPPoE over Ethernet en IEEE 802.1Q VLAN configureren.

MPLS VPN

Multiprotocol Label Switching (MPLS) is een nieuwe IETF-standaard die is gebaseerd op Cisco Label Switching die geautomatiseerde levering, snelle uitrol en schaalbaarheidsfuncties mogelijk maakt die providers op kosteneffectieve wijze toegang, intranet en extranet VPN-services moeten leveren. Cisco werkt nauw samen met serviceproviders om een soepele overgang naar MPLS-enabled VPN-services te waarborgen. MPLS werkt op een label gebaseerd paradigma, het taggen van pakketten zoals zij het providernetwerk binnendringen om het verzenden door een connectioneloze IP kern te versnellen. MPLS gebruikt routeonderscheidaars om VPN-leden te identificeren en verkeer binnen een VPN-gemeenschap te bevatten.

MPLS voegt ook de voordelen van een op connectie gerichte benadering van het IP-routingparadigma toe, door het instellen van label-switched paden, die gebaseerd worden op topologie-informatie in plaats van op verkeersstroom. MPLS VPN wordt uitgebreid ingezet in de service-provider-omgeving.

Zie Een basis-MPLS VPN configureren voor informatie over het configureren van MPLS VPN.

Gerelateerde informatie

- IPsec-ondersteuningspagina
- Hoe Virtual Private Networks werken
- NAT-ondersteuningspagina
- GRE-ondersteuningspagina
- VPDN-ondersteuningspagina
- PPTP-ondersteuningspagina
- Categoriepagina voor PPPoE-ondersteuning
- Technische ondersteuning - Cisco-systemen