Quelle solution VPN est la bonne pour vous ?

Contenu

Introduction

Les réseaux privés virtuels (VPN) sont de plus en plus répandus, car ils constituent un moyen flexible et peu coûteux de déployer un réseau sur une zone étendue. Les nouvelles percées technologiques amènent de nombreuses façons de mettre en place des solutions VPN. Cette note technique explique certaines de ces méthodes et les situations où leur utilisation est optimale.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

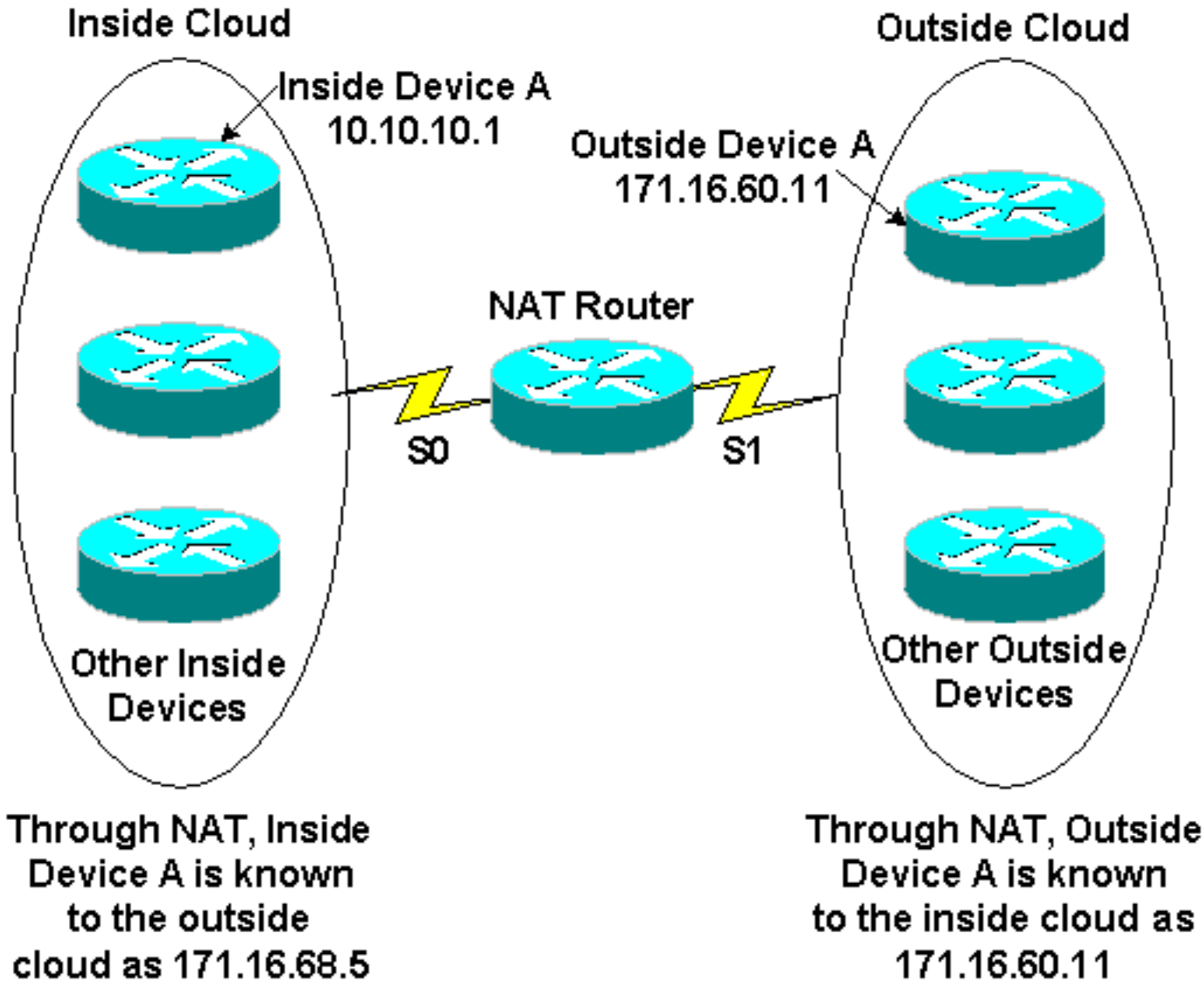
Remarque: Cisco fournit également la prise en charge du chiffrement dans des Plateformes non-IOS comprenant le pare-feu Cisco Secure PIX, le concentrateur de Cisco VPN 3000, et le concentrateur de Cisco VPN 5000.

NAT

L'Internet a connu la croissance explosive en peu de temps, bien plus que les créateurs d'origine pourraient avoir prévu. Le nombre limité d'adresses disponible dans la version d'IP 4.0 est des preuves de cette croissance, et le résultat est que l'espace d'adressage devient moins disponible. Une solution au problème est Traduction d'adresses de réseau (NAT).

Utilisant NAT un routeur est en fonction configurées des bornes d'intérieur/extérieur tels que l'extérieur (habituellement l'Internet) voit une ou quelque adresses enregistrées tandis que l'intérieur pourrait avoir un certain nombre d'hôtes utilisant un système d'adressage privé. Pour mettre à jour l'intégrité de la structure de traduction d'adresses, NAT doit être configurée sur chaque routeur de borne entre le réseau (privé) intérieur et le réseau (public) extérieur. Un des avantages de NAT d'un point de vue de la sécurité est que les systèmes sur le réseau privé ne peuvent pas recevoir une connexion IP en entrée du réseau extérieur à moins que la passerelle NAT soit spécifiquement configurée pour permettre la connexion. D'ailleurs, NAT est complètement transparent aux périphériques sources et de destination. L'exécution recommandée du NAT implique le RFC 1918 , qui trace les grandes lignes des systèmes d'adressage du réseau privés appropriés. La norme pour NAT est décrite dans RFC1631 .

La figure suivante affiche la définition des limites du routeur NAT avec un pool d'adresses réseau de traduction interne.

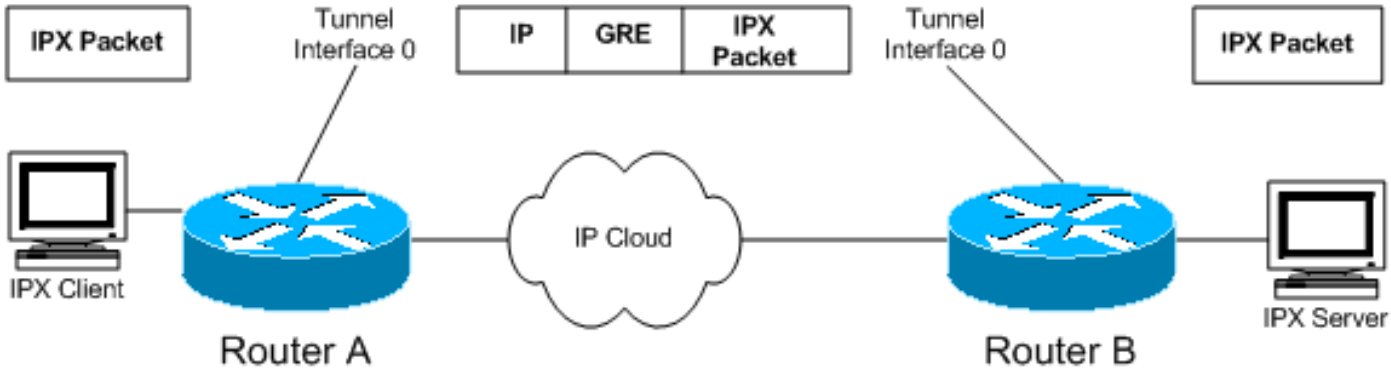


NAT est généralement utilisé pour économiser les adresses IP routable sur l'Internet, qui sont chères et limitées en nombre. NAT fournit également la Sécurité en masquant le réseau intérieur de l'Internet.

Pour les informations sur le fonctionnement de NAT, voyez comment les travaux NAT.

Tunnellisation d'encapsulation GRE

Les tunnels d'Encapsulation de routage générique (GRE) fournissent une voie spécifique à travers le WAN partagé et encapsulent le trafic avec de nouvelles en-têtes de paquet pour assurer la livraison aux destinations spécifiques. Le réseau est privé parce que le trafic peut entrer dans un tunnel seulement à un point final et peut partir seulement à l'autre point final. Les tunnels ne fournissent pas la confidentialité vraie (comme le cryptage fait) mais peuvent porter le trafic chiffré. Les tunnels sont des points finaux logiques configurés sur les interfaces physiques par lesquelles le trafic est porté.



Comme illustré dans le diagramme, le Tunnellisation GRE peut également être utilisé pour encapsuler le trafic non-IP dans l'IP et pour l'envoyer au-dessus de l'Internet ou du réseau IP. L'échange de paquet d'Internet (IPX) et les appletalks protocols sont des exemples du trafic non-IP. Pour les informations sur configurer GRE, voyez « configurer une interface de tunnel GRE » en configurant GRE.

GRE est la bonne solution VPN pour vous si vous avez un réseau multiprotocole comme l'IPX ou l'AppleTalk et devez envoyer le trafic au-dessus de l'Internet ou d'un réseau IP. En outre, l'encapsulation GRE est généralement utilisée en même temps que des autres moyens de sécuriser le trafic, tel qu'IPSec.

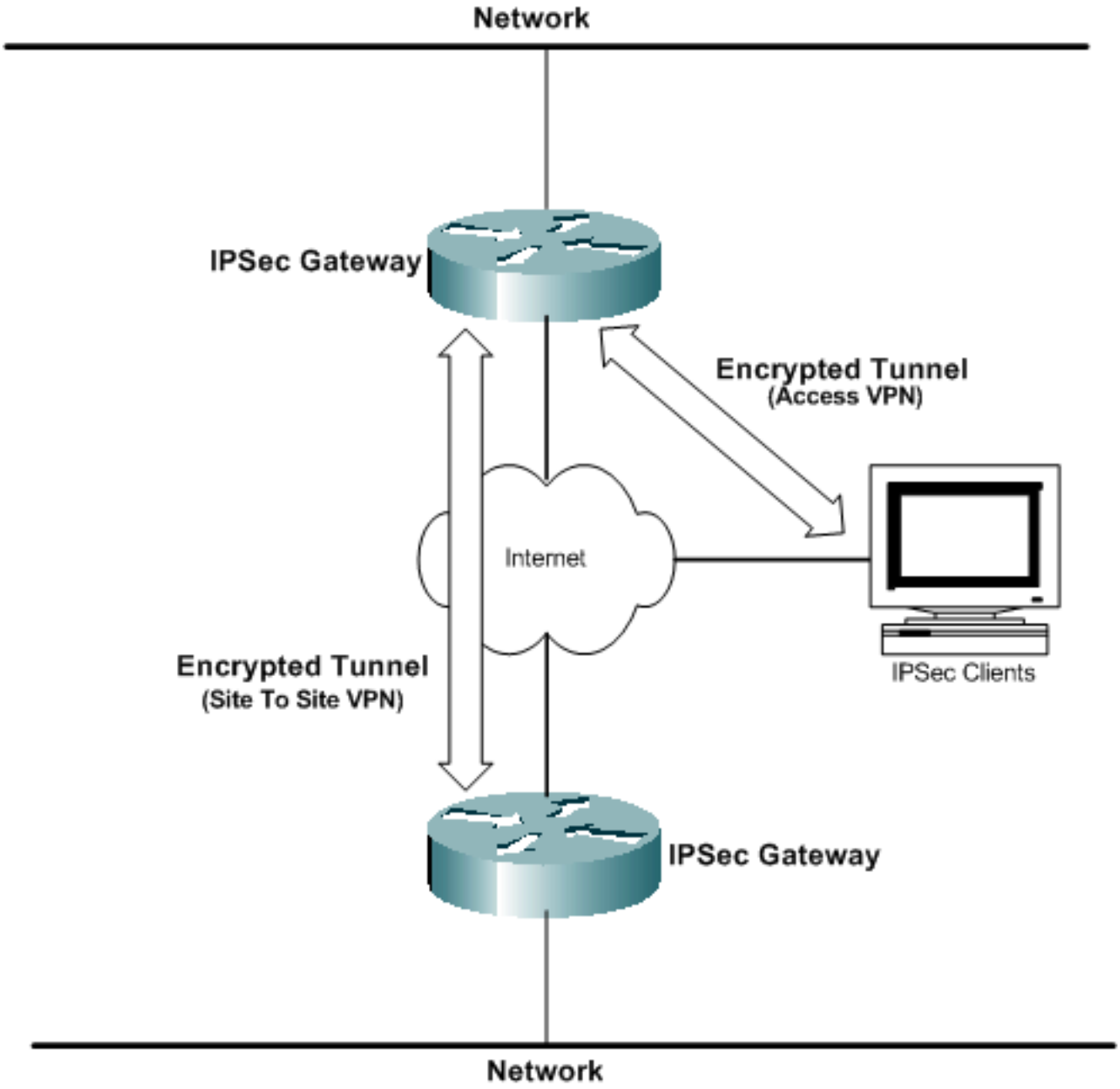
Pour un détail plus technique sur GRE, référez-vous à RFC 1701 et à RFC 2784 .

Chiffrement IPSec

Le cryptage des données transmises à travers un réseau partagé est la technologie VPN le plus souvent associée aux VPN. Cisco prend en charge les méthodes de chiffrement de données de sécurité IP (IPSec). IPSec est un cadre des standards ouverts qui fournit la confidentialité des données, l'intégrité des données, et l'authentification des données entre les pairs participants à la couche réseau.

Le chiffrement IPSec est une norme de l'Internet Engineering Task Force (IETF) qui les algorithmes prend en charge du Norme de chiffrement de données (DES) 56-bit et du triple DES (3DES) chiffrement à clé 168-bit symétriques en logiciel client d'IPSec. La configuration GRE est facultative avec IPSec. IPSec prend en charge également des autorités de certification et la négociation d'Échange de clés Internet (IKE). Le chiffrement IPSec peut être déployé dans les environnements autonomes entre les clients, les Routeurs, et les Pare-feu, ou être utilisé en même temps que le Tunnellisation L2TP dans l'accès VPN. IPSec est pris en charge dedans sur de diverses Plateformes du système d'exploitation.

Le chiffrement IPSec est la bonne solution VPN pour vous si vous voulez la confidentialité des données vraie pour vos réseaux. IPSec est également un standard ouvert, ainsi il est facile implémenter Interopérabilité entre les différents périphériques.



PPTP et MPPE

Le Protocole PPTP (Point-to-Point Tunneling Protocol) a été développé par Microsoft ; il est décrit dans RFC2637 . PPTP est largement déployé en logiciel client de Windows 9x/ME, de Windows NT, et de Windows 2000, et de Windows XP pour activer des VPN volontaires.

Le cryptage point par point de Microsoft (MPPE) est une ébauche informative de l'IETF de Microsoft qui utilise le cryptage 40-bit ou 128-bit RC4-based. Le MPPE fait partie de solution de logiciel client PPTP de Microsoft et est utile en architectures de VPN d'accès de volontaire-mode. PPTP/MPPE est pris en charge sur la plupart des Plateformes de Cisco.

Le support PPTP a été ajouté à la version du logiciel Cisco IOS 12.0.5.XE5 sur le Cisco 7100 et 7200 Plateformes. Le soutien de plus de Plateformes a été ajouté dans le Cisco IOS 12.1.5.T. Le concentrateur de pare-feu Cisco Secure PIX et de Cisco VPN 3000 incluent également le soutien des connexions client PPTP.

Puisque PPTP prend en charge les réseaux non-IP, il est utile où les utilisateurs distants doivent

se connecter au réseau d'entreprise pour accéder aux réseaux d'entreprise hétérogènes.

Pour les informations sur configurer PPTP, voyez configurer PPTP.

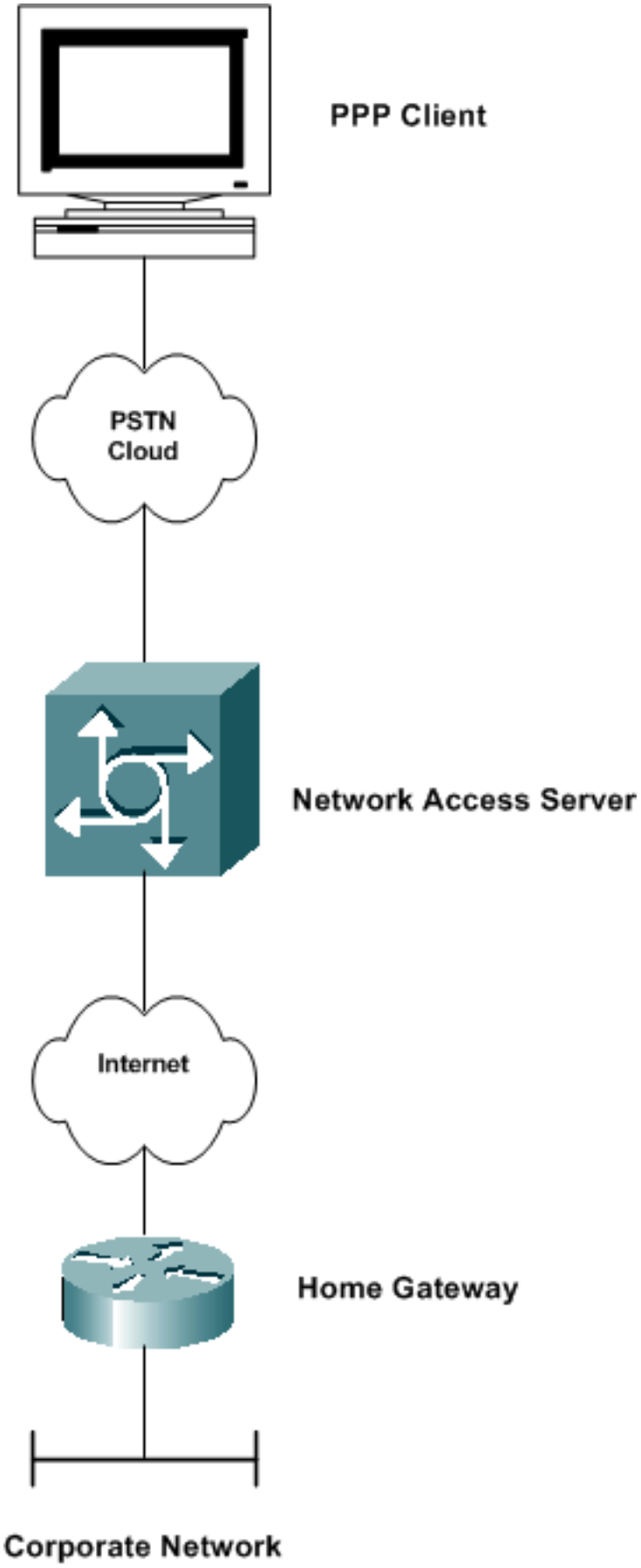
VPDN et L2TP

VPDN

Le Réseau privé virtuel à accès commuté (VPDN) est une norme de Cisco qui permet à un service d'accès distant privé pour la répartir à travers aux Remote Access Server. Dans le cadre de VPDN, le serveur d'accès (par exemple, un AS5300) dans lequel est introduit désigné habituellement sous le nom du serveur d'accès à distance (NAS). La destination de l'utilisateur en accès entrant désigné sous le nom de la passerelle domestique (HGW).

Le scénario de base est qu'un client de Protocole point à point (PPP) se connecte à l'le NAS local. Le NAS détermine que la session PPP devrait être expédiée à un routeur de passerelle domestique pour ce client. Le HGW alors authentifie l'utilisateur et commence la négociation PPP. Après que l'installation de PPP soit complète, toutes les trames sont envoyées par l'intermédiaire du NAS au client et aux passerelles domestiques. Cette méthode intègre plusieurs protocoles et concepts.

Pour les informations sur configurer VPDN, voyez *configurer un réseau commuté de connexion privée virtuelle* en configurant des fonctionnalités de sécurité.



L2TP

Le Layer 2 Tunneling Protocol (L2TP) est une norme IETF qui incorpore les meilleurs attributs de PPTP et de L2F. Des tunnels L2TP sont utilisés principalement dans l'accès VPN du l'obligatoire-mode (c'est-à-dire, NAS commuté à HGW) pour le trafic IP et non-IP. Le Windows 2000 et le

Windows XP ont ajouté la prise en charge native pour ce protocole afin de la connexion client VPN.

L2TP est utilisé pour percer un tunnel le PPP au-dessus d'un réseau public, tel que l'Internet, utilisant l'IP. Puisque le tunnel se produit sur la couche 2, les protocoles de couche supérieure sont ignorants du tunnel. Comme GRE, L2TP peut également encapsuler n'importe quel protocole de la couche 3. Le port UDP 1701 est utilisé pour envoyer le trafic L2TP par le demandeur du tunnel.

Remarque: En 1996 Cisco a créé un protocole de l'expédition de la couche 2 (L2F) pour permettre à des connexions VPDN pour se produire. L2F est encore pris en charge pour d'autres fonctions, mais a été remplacé par L2TP. Le Protocole PPTP (Point-to-Point Tunneling Protocol) était en 1996 également créé un projet Internet par l'IETF. PPTP a fourni une fonction semblable au protocole comme GRE de tunnel pour des connexions PPP.

Pour plus d'informations sur L2TP, voir le tunnel Protocol de la couche 2.

PPPoE

Le PPP au-dessus des Ethernets (PPPoE) est un RFC informationnel qui est principalement déployé dans la ligne d'abonné numérique (DSL) environnements. Le PPPoE accroît les infrastructures Ethernet existantes pour permettre à des utilisateurs pour initier de plusieurs sessions PPP dans le même RÉSEAU LOCAL. Cette technologie active la sélection de service de la couche 3, une application émergente qui permet des utilisateurs simultanément de se connecter à plusieurs destinations par une connexion simple d'Accès à distance. Le PPPoE avec le Password Authentication Protocol (PAP) ou le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol) est employé souvent pour informer le lieu d'exploitation principal quels Routeurs distants sont connectés à lui.

Le PPPoE est en grande partie utilisé dans des déploiements du fournisseur de services DSL et des topologies d'Ethernets pontés.

Pour plus d'informations sur configurer le PPPoE, voyez configurer le PPPoE au-dessus du 802.1Q VLAN d'Ethernets et d'IEEE.

MPLS VPN

Le Commutation multiprotocole par étiquette (MPLS) est une nouvelle norme IETF basée sur la commutation de balise de Cisco qui active la mise en service automatisée, la mise en service rapide, et les caractéristiques d'évolutivité dont les fournisseurs ont besoin pour fournir de manière rentable l'accès, l'intranet, et les services de l'extranet VPN. Cisco fonctionne étroitement avec des fournisseurs de services pour assurer un service MPLS-activé lisse de la transition VPN. Le MPLS travaille à un paradigme d'étiquettes, étiquetant des paquets pendant qu'ils entrent dans le réseau du fournisseur pour accélérer l'expédition par un noyau IP sans connexion. Moteurs de distinction de route d'utilisations MPLS pour identifier l'adhésion VPN et pour contenir le trafic au sein d'une communauté VPN.

Le MPLS ajoute également les avantages d'une approche connectée au paradigme de Routage IP, par l'établissement des chemins étiquette-commutés, qui sont créés ont basé sur la circulation des informations topologiques plutôt puis. MPLS VPN est largement déployé dans l'environnement de prestataire de service.

Pour les informations sur configurer MPLS VPN, voyez configurer un MPLS de base VPN.

Informations connexes

- Page d'assistance IPsec
- Fonctionnement des réseaux VPN
- Page de support NAT
- Page de support GRE
- Page de support VPDN
- Page de support PPTP
- Page de Soutien PPPoE
- Support technique - Cisco Systems