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.

Components Used

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

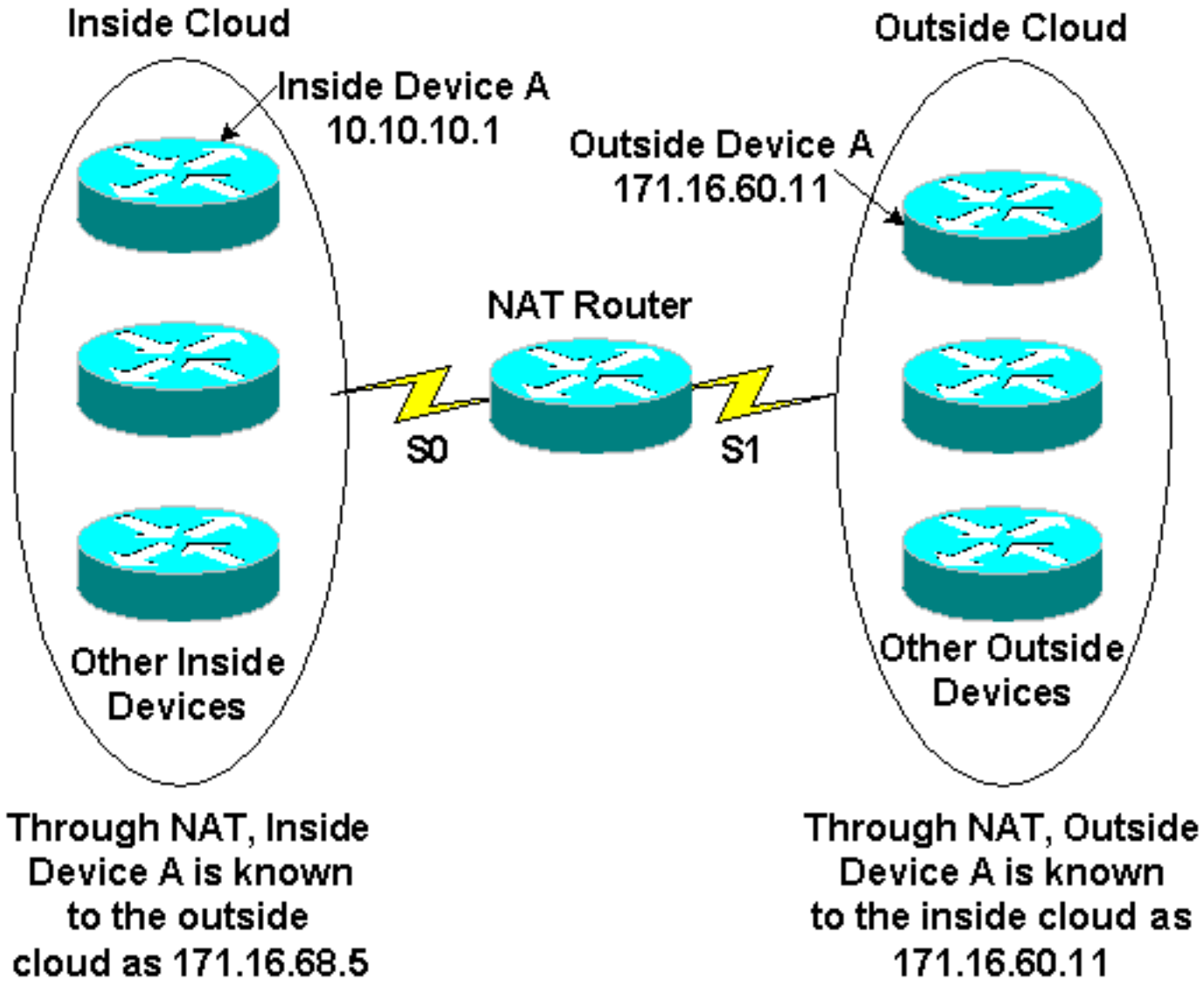
Remarque : Cisco assure également la prise en charge du chiffrement sur les plates-formes non IOS, notamment le pare-feu Cisco Secure PIX Firewall, le concentrateur Cisco VPN 3000 et le concentrateur Cisco VPN 5000.

NAT

Internet a connu une croissance explosive en peu de temps, bien plus que ce que les concepteurs d'origine auraient pu prévoir. Le nombre limité d'adresses disponibles dans la version 4.0 d'IP est la preuve de cette croissance et le résultat est que l'espace d'adressage devient de moins en moins disponible. Une solution à ce problème est la traduction d'adresses de réseau (NAT).

Àl'aide de la fonction NAT, un routeur est configuré sur des limites internes/externes de sorte que l'extérieur (généralement Internet) voit une ou quelques adresses enregistrées tandis que l'intérieur peut avoir n'importe quel nombre d'hôtes utilisant un schéma d'adressage privé. Pour maintenir l'intégrité du schéma de traduction d'adresses, la NAT doit être configurée sur chaque routeur de périphérie entre le réseau interne (privé) et le réseau externe (public). Un des avantages de la fonction NAT du point de vue de la sécurité est que les systèmes du réseau privé ne peuvent pas recevoir de connexion IP entrante du réseau externe, à moins que la passerelle NAT ne soit spécifiquement configurée pour autoriser la connexion. En outre, la NAT est totalement transparente pour les périphériques source et de destination. L'opération recommandée par NAT concerne RFC 1918 , qui décrit les schémas d'adressage de réseau privé appropriés. La norme NAT est décrite dans RFC1631 .

La figure suivante illustre la définition de la frontière du routeur NAT avec un pool d'adresses réseau de traduction interne.

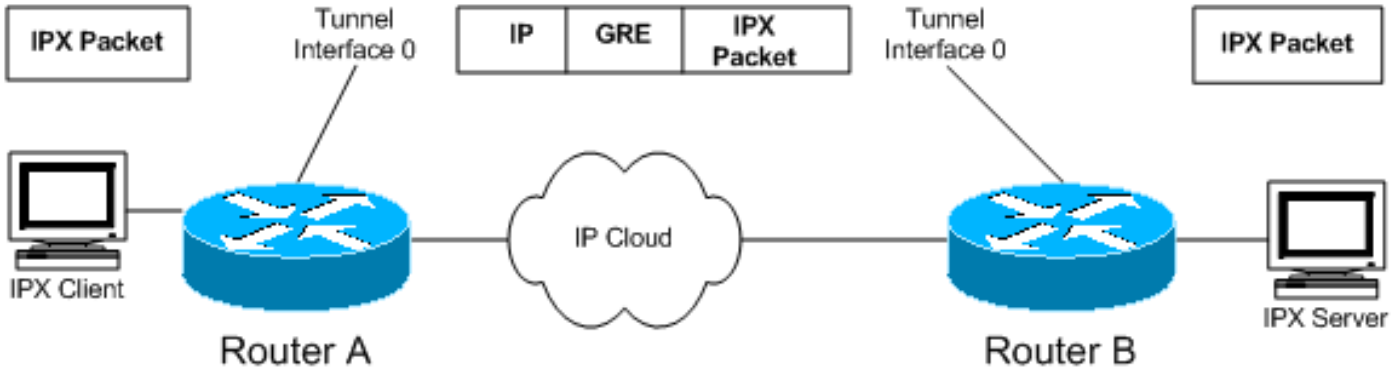


La fonction NAT est généralement utilisée pour conserver les adresses IP routables sur Internet, qui sont chères et limitées en nombre. La fonction NAT assure également la sécurité en masquant le réseau interne d'Internet.

Pour plus d'informations sur le fonctionnement de NAT, consultez Fonctionnement de NAT.

Tunnellisation d'encapsulation GRE

Les tunnels GRE (Generic Routing Encapsulation) fournissent un chemin spécifique à travers le WAN partagé et encapsulent le trafic avec de nouveaux en-têtes de paquets pour garantir la livraison vers des destinations spécifiques. Le réseau est privé, car le trafic ne peut entrer dans un tunnel qu'à un point d'extrémité et ne peut quitter qu'à l'autre point d'extrémité. Les tunnels ne fournissent pas une véritable confidentialité (comme le chiffrement), mais peuvent transporter du trafic chiffré. Les tunnels sont des points de terminaison logiques configurés sur les interfaces physiques via lesquelles le trafic est acheminé.



Comme l'illustre le schéma, la transmission tunnel GRE peut également être utilisée pour encapsuler le trafic non IP dans IP et l'envoyer sur Internet ou sur le réseau IP. Les protocoles IPX (Internet Packet Exchange) et AppleTalk sont des exemples de trafic non IP. Pour plus d'informations sur la configuration de GRE, reportez-vous à Configuration d'une interface de tunnel GRE dans Configuration de GRE.

GRE est la solution VPN qui vous convient si vous avez un réseau multiprotocole comme IPX ou AppleTalk et que vous devez envoyer du trafic sur Internet ou un réseau IP. En outre, l'encapsulation GRE est généralement utilisée conjointement avec d'autres moyens de sécurisation du trafic, tels qu'IPSec.

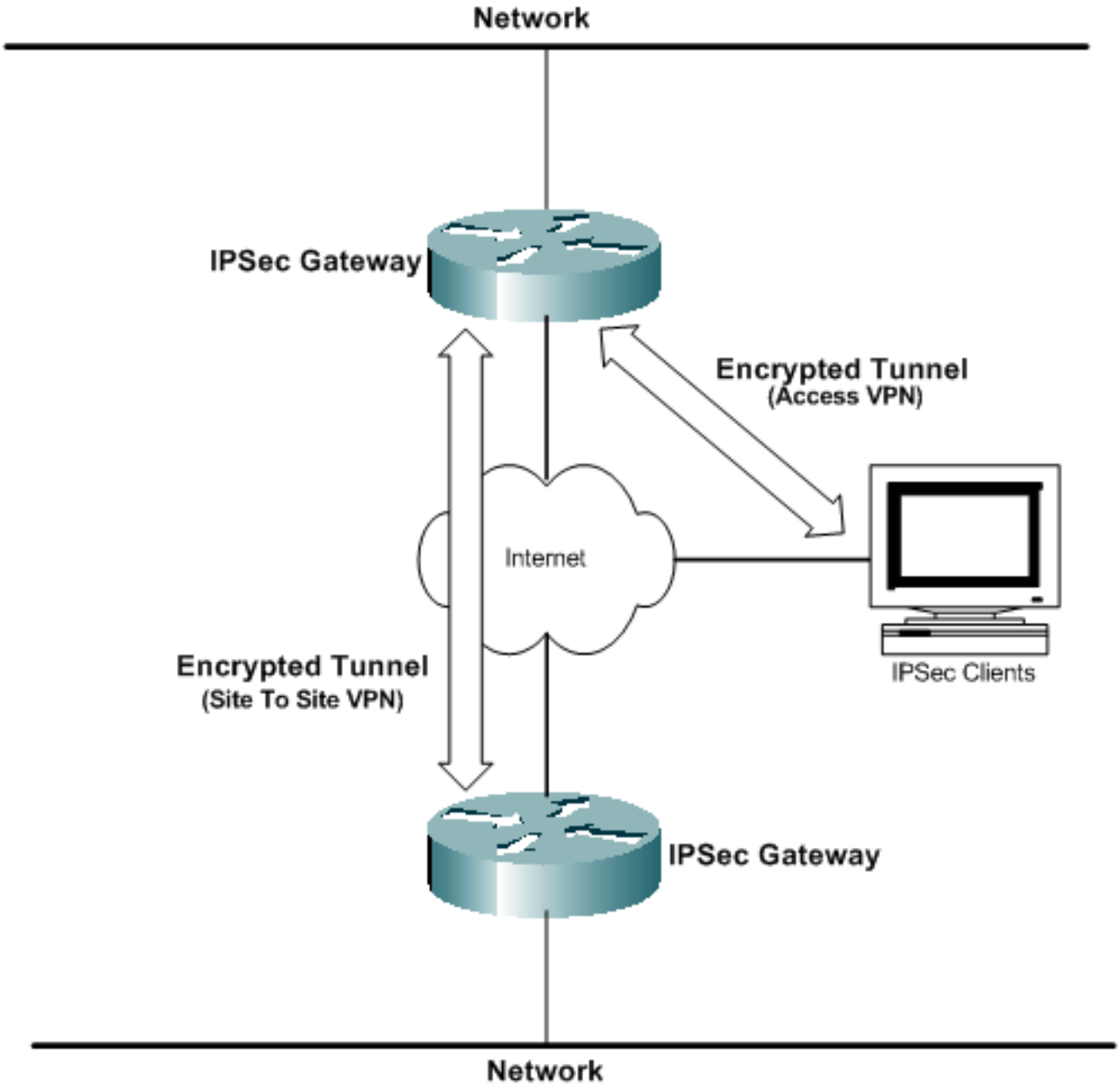
Pour plus de détails techniques sur GRE, reportez-vous aux documents RFC 1701 et RFC 2784 .

Cryptage IPSec

Le chiffrement des données envoyées sur un réseau partagé est la technologie VPN la plus souvent associée aux VPN. Cisco prend en charge les méthodes de cryptage des données IPSec (IP Security). IPSec est un cadre de normes ouvertes qui assure la confidentialité des données, l'intégrité des données et l'authentification des données entre homologues participants au niveau de la couche réseau.

Le cryptage IPSec est une norme IETF (Internet Engineering Task Force) qui prend en charge les algorithmes de cryptage symétrique DES (Data Encryption Standard) 56 bits et 3DES (Triple DES) 168 bits dans le logiciel client IPSec. La configuration GRE est facultative avec IPSec. IPSec prend également en charge les autorités de certification et la négociation IKE (Internet Key Exchange). Le cryptage IPSec peut être déployé dans des environnements autonomes entre des clients, des routeurs et des pare-feu, ou utilisé en association avec le tunneling L2TP dans les VPN d'accès. IPSec est pris en charge sur différentes plates-formes de système d'exploitation.

Le cryptage IPSec est la solution VPN idéale pour vous si vous souhaitez une véritable confidentialité des données pour vos réseaux. IPSec est également une norme ouverte. L'interopérabilité entre différents périphériques est donc facile à mettre en oeuvre.



PPTP et MPPE

Le protocole PPTP (Point-to-Point Tunneling Protocol) a été développé par Microsoft ; elle est décrite dans RFC2637 . PPTP est largement déployé dans les logiciels clients Windows 9x/ME, Windows NT et Windows 2000 et Windows XP pour activer les VPN volontaires.

Microsoft Point-to-Point Encryption (MPPE) est un brouillon IETF informatif de Microsoft qui utilise un cryptage 40 bits ou 128 bits basé sur RC4. MPPE fait partie de la solution logicielle client PPTP de Microsoft et est utile dans les architectures VPN d'accès en mode volontaire. PPTP/MPPE est pris en charge sur la plupart des plates-formes Cisco.

La prise en charge PPTP a été ajoutée au logiciel Cisco IOS Version 12.0.5.XE5 sur les plates-formes Cisco 7100 et 7200. La prise en charge d'autres plates-formes a été ajoutée dans Cisco IOS 12.1.5.T. Le pare-feu Cisco Secure PIX Firewall et le concentrateur Cisco VPN 3000 prennent également en charge les connexions de clients PPTP.

Puisque PPTP prend en charge les réseaux non IP, il est utile lorsque les utilisateurs distants

doivent se connecter au réseau d'entreprise pour accéder à des réseaux d'entreprise hétérogènes.

Pour plus d'informations sur la configuration de PPTP, consultez Configuration de PPTP.

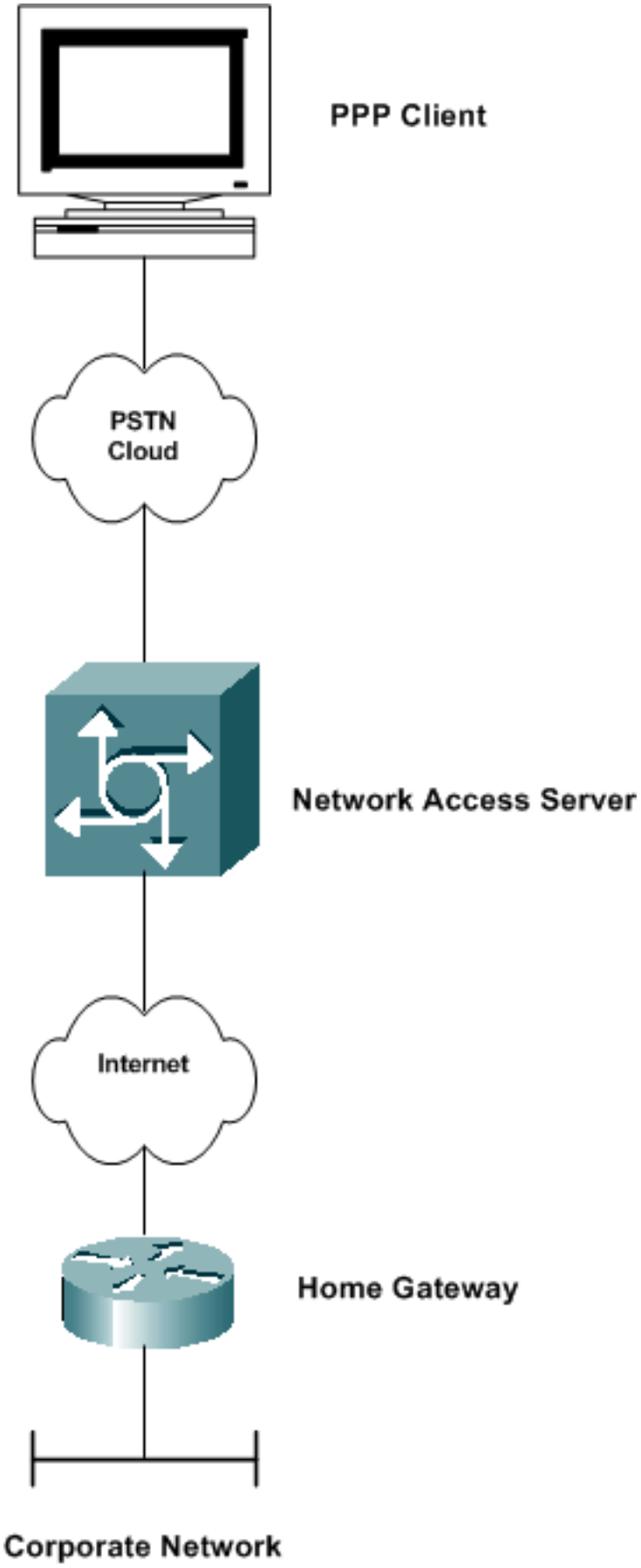
VPDN et L2TP

VPDN

Virtual Private Dialup Network (VPDN) est une norme Cisco qui permet à un service de connexion réseau privé de s'étendre aux serveurs d'accès à distance. Dans le contexte du VPDN, le serveur d'accès (par exemple, un AS5300) qui est composé est généralement appelé serveur d'accès réseau (NAS). La destination de l'utilisateur entrant est appelée passerelle principale (HGW).

Le scénario de base est qu'un client PPP (Point-to-Point Protocol) se connecte à un NAS local. Le NAS détermine que la session PPP doit être transférée à un routeur de passerelle domestique pour ce client. Le HGW authentifie ensuite l'utilisateur et lance la négociation PPP. Une fois la configuration PPP terminée, toutes les trames sont envoyées via le NAS aux passerelles client et maison. Cette méthode intègre plusieurs protocoles et concepts.

Pour plus d'informations sur la configuration du VPDN, consultez *Configuration d'un réseau privé virtuel à accès commuté* dans Configuration des fonctions de sécurité.



L2TP

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

et Windows XP ont ajouté la prise en charge native de ce protocole comme moyen de connexion client VPN.

L2TP est utilisé pour le tunnel PPP sur un réseau public, tel qu'Internet, à l'aide d'IP. Puisque le tunnel se produit sur la couche 2, les protocoles de couche supérieure ignorent le tunnel. Comme GRE, L2TP peut également encapsuler n'importe quel protocole de couche 3. Le port UDP 1701 est utilisé pour envoyer le trafic L2TP par l'initiateur du tunnel.

Remarque : En 1996, Cisco a créé un protocole L2F (Layer 2 Forwarding) pour autoriser les connexions VPDN. L2F est toujours pris en charge pour d'autres fonctions, mais a été remplacé par L2TP. Le protocole PPTP (Point-to-Point Tunneling Protocol) a également été créé en 1996 et un projet Internet a été élaboré par l'IETF. PPTP a fourni une fonction similaire au protocole de tunnel de type GRE pour les connexions PPP.

Pour plus d'informations sur L2TP, consultez Protocole de tunnel de couche 2.

PPPoE

PPP over Ethernet (PPPoE) est une RFC informative qui est principalement déployée dans des environnements DSL (Digital Subscriber Line). PPPoE exploite l'infrastructure Ethernet existante pour permettre aux utilisateurs d'initier plusieurs sessions PPP au sein d'un même réseau local. Cette technologie permet la sélection de services de couche 3, une application émergente qui permet aux utilisateurs de se connecter simultanément à plusieurs destinations via une seule connexion d'accès à distance. PPPoE avec le protocole PAP (Password Authentication Protocol) ou le protocole CHAP (Challenge Handshake Authentication Protocol) est souvent utilisé pour informer le site central des routeurs distants qui y sont connectés.

Le protocole PPPoE est principalement utilisé dans les déploiements DSL des fournisseurs de services et les topologies Ethernet pontées.

Pour plus d'informations sur la configuration de PPPoE, consultez Configuration de PPPoE sur Ethernet et VLAN IEEE 802.1Q.

VPN MPLS

La commutation multiprotocole par étiquette (MPLS) est une nouvelle norme IETF basée sur la commutation Cisco Tag Switching qui permet d'automatiser le provisionnement, le déploiement rapide et l'évolutivité dont les fournisseurs ont besoin pour fournir de manière rentable des services VPN d'accès, intranet et extranet. Cisco travaille en étroite collaboration avec les fournisseurs de services pour assurer une transition en douceur vers les services VPN MPLS. MPLS fonctionne selon un paradigme basé sur les étiquettes, en étiquetant les paquets lorsqu'ils pénètrent dans le réseau du fournisseur pour accélérer le transfert via un coeur IP non orienté connexion. MPLS utilise des identificateurs de route pour identifier l'appartenance au VPN et contenir le trafic au sein d'une communauté VPN.

MPLS ajoute également les avantages d'une approche orientée connexion au paradigme de routage IP, par l'établissement de chemins commutés par étiquette, créés en fonction des informations de topologie plutôt que du flux de trafic. Le VPN MPLS est largement déployé dans l'environnement du fournisseur de services.

Pour plus d'informations sur la configuration du VPN MPLS, consultez Configuration d'un VPN

MPLS de base.

Informations connexes

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