Que solução de VPN é perfeita para você?

Índice

Introdução

As VPNs (Redes privadas virtuais) estão se tornando amplamente populares como um modo mais flexível e de baixo custo de implementar uma rede em uma grande área. Com os avanços na tecnologia, surge uma maior variedade de opções para implantar soluções de VPN. Esta nota técnica explica algumas dessas opções e descreve onde elas podem ser melhor utilizadas.

Antes de Começar

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Pré-requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

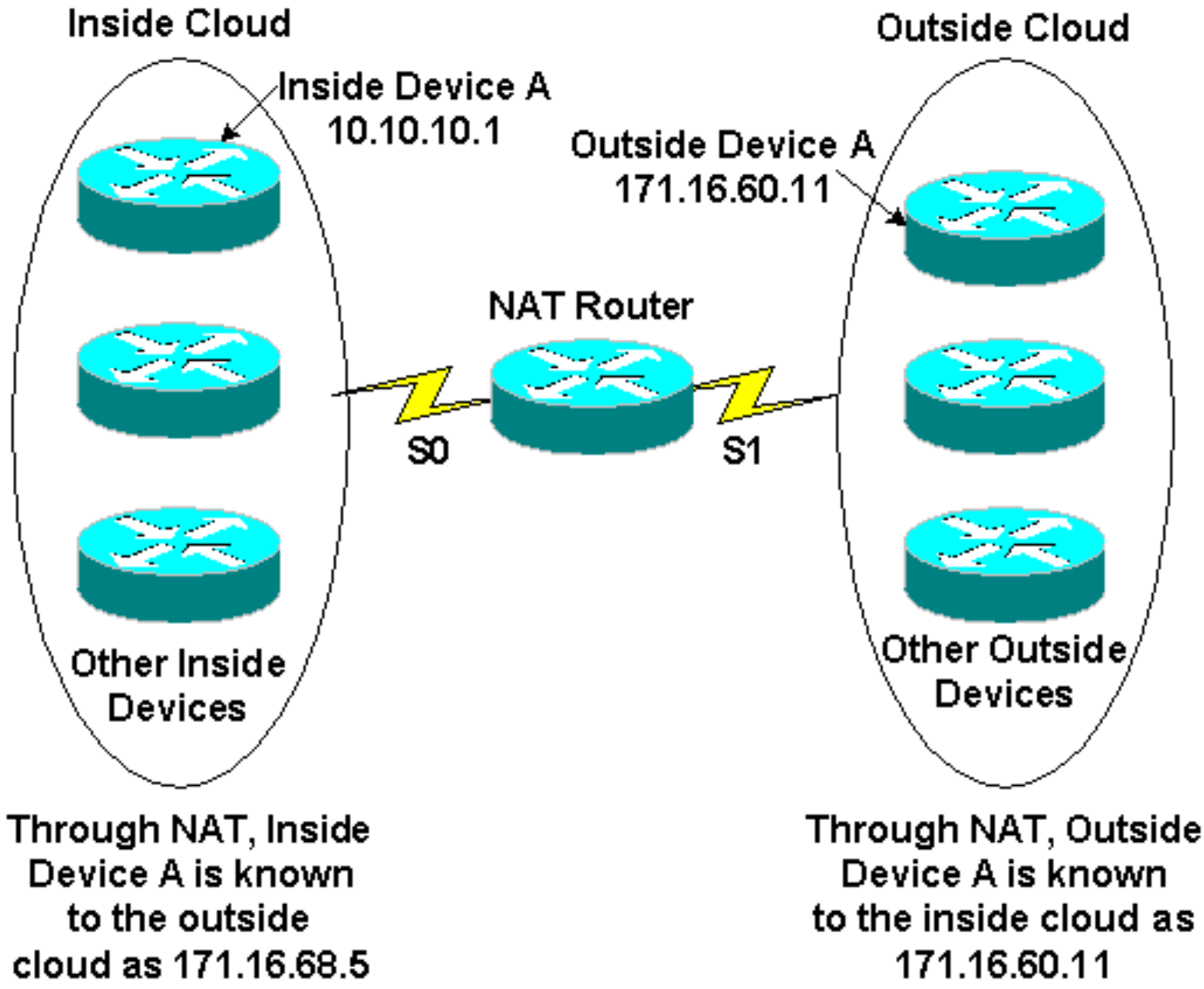
Nota: A Cisco também fornece suporte de criptografia em plataformas não-IOS, incluindo Cisco Secure PIX Firewall, Cisco VPN 3000 Concentrator e Cisco VPN 5000 Concentrator.

NAT

O Internet experimentou o crescimento explosivo em um curto período de tempo, distante mais do que os designer originais poderiam ter previsto. O número limitado de endereços disponíveis no IP versão 4.0 é evidência desse crescimento e o resultado é que o espaço de endereços está se tornando menos disponível. Uma solução para esse problema é a Tradução de Endereço de Rede (NAT).

Usando o NAT, um roteador é configurado nos limites internos/externos de forma que a parte externa (em geral a Internet) vê um ou alguns endereços registrados, enquanto a partir interna pode ter qualquer número de hosts usando um esquema de endereçamento particular. Para manter a integridade do esquema de tradução de endereço, NAT deve ser configurado em cada roteador de limite entre a rede (particular) interna e a rede (pública) externa. Uma das vantagens do NAT sob o ponto de vista da segurança é que os sistemas na rede privada não conseguem receber uma conexão IP`de entrada a partir da rede externa a não que o gateway NAT esteja especificamente configurado para permitir a conexão. Além disso, o NAT é completamente transparente aos dispositivos de origem e de destino. A operação recomendada do NAT envolve o RFC 1918 , que esboça esquemas apropriados de endereçamento de rede privada. O padrão para o NAT é descrito no RFC1631 .

A seguinte figura mostra a definição do limite de NAT Router com um conjunto de endereços de rede de tradução interna.

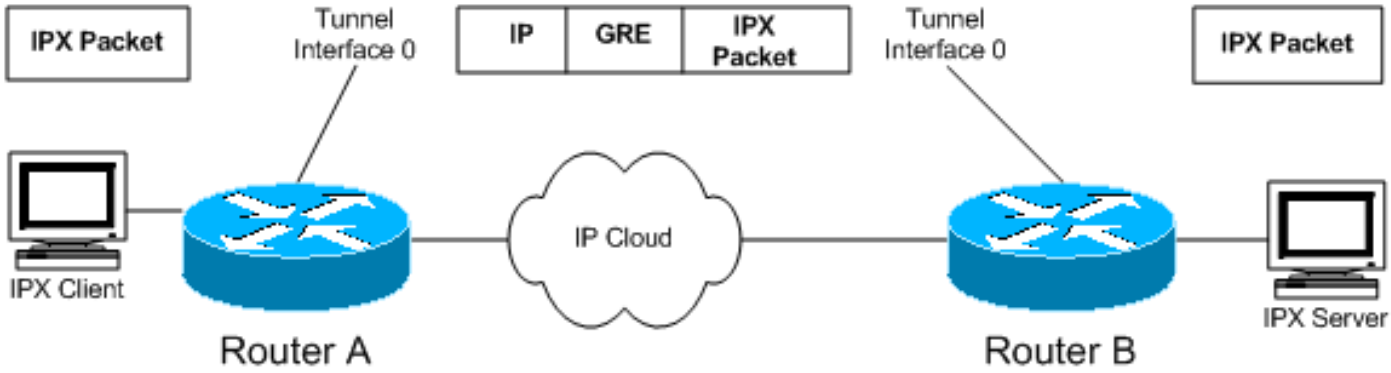


O NAT é usado geralmente para conservar o roteável dos endereços IP de Um ou Mais Servidores Cisco ICM NT no Internet, que são caros e limitados em número. O NAT igualmente fornece a Segurança escondendo a rede interna do Internet.

Para obter informações sobre do trabalho do NAT, veja como o NAT trabalha.

Tunelamento do encapsulamento de GRE

Os túneis de encapsulamento de roteamento genéricos (GRE) fornecem um caminho específico através de WAN compartilhado e encapsulam o tráfego com cabeçalhos de pacote de informação novos para assegurar a entrega aos destinos específicos. A rede é privada porque o tráfego pode incorporar um túnel somente em um valor-limite e pode sair somente no outro valor-limite. Os túneis não fornecem a confidencialidade verdadeira (como a criptografia faz) mas podem levar o tráfego criptografado. Os túneis são pontos finais lógicos configurados nas interfaces física através de que o tráfego é levado.



Como ilustrado no diagrama, o tunelamento GRE pode igualmente ser usado para encapsular o tráfego não-IP no IP e para enviá-lo sobre o Internet ou a rede IP. O Internet Packet Exchange (IPX) e os protocolos Appletalk são exemplos do tráfego não-IP. Para obter informações sobre de configurar o GRE, veja “configurar uma interface do túnel GRE” em configurar o GRE.

O GRE é a solução de VPN direita para você se você tem uma rede multiprotocolo como o IPX ou o APPLETALK e tem que enviar o tráfego sobre o Internet ou uma rede IP. Também, o encapsulamento de GRE é usado geralmente conjuntamente com outros meios de fixar o tráfego, tal como o IPsec.

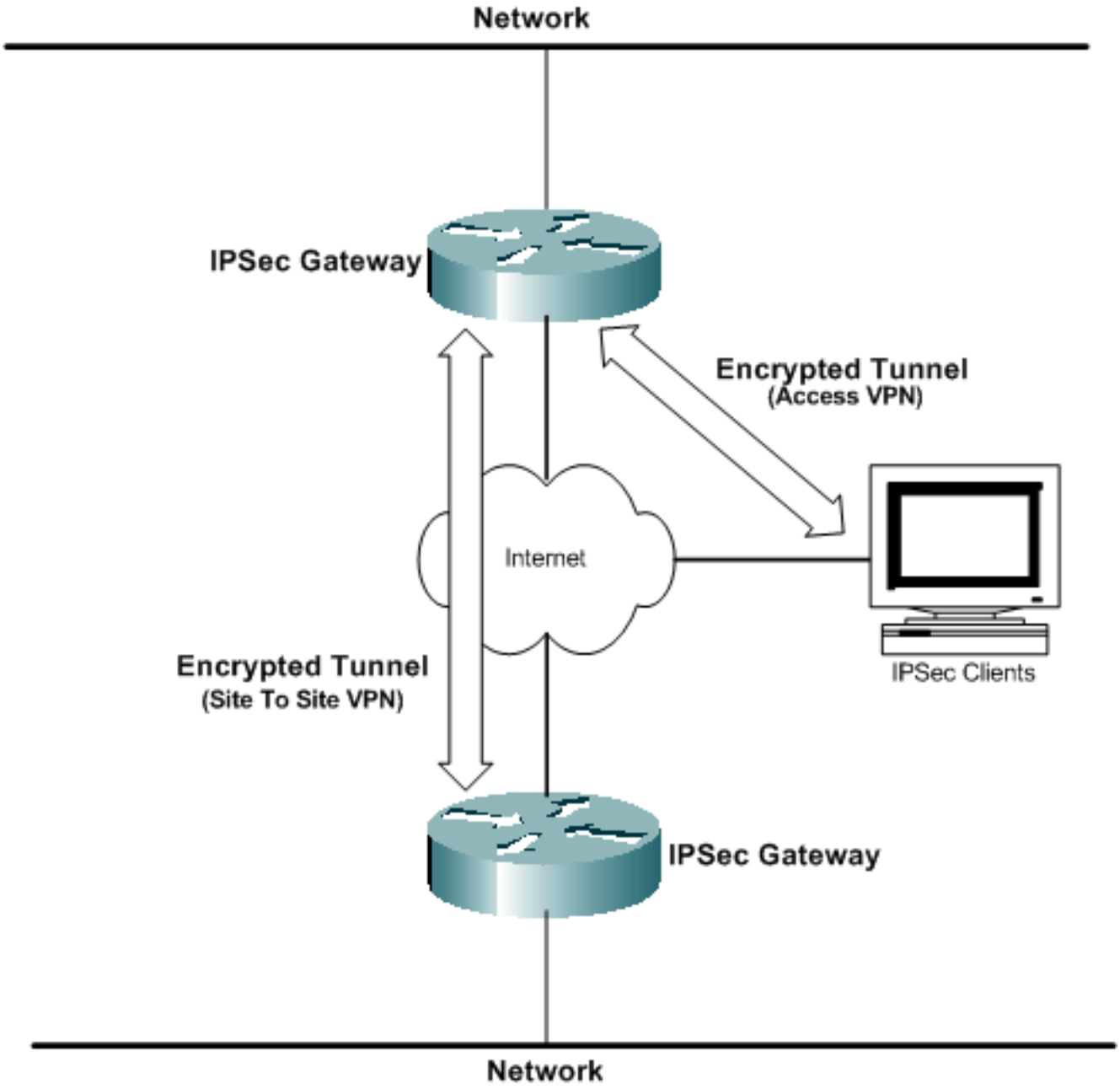
Para mais detalhe técnico no GRE, refira o RFC 1701 e o RFC 2784 .

Criptografia IPSec

A criptografia dos dados enviados através de uma rede compartilhada é a tecnologia de VPN o mais frequentemente associada com VPN. Cisco apoia os métodos de criptografia de dados da Segurança IP (IPsec). O IPsec é uma estrutura dos padrões abertos que forneça a confidencialidade de dados, a integridade de dados, e a autenticação de dados entre peer participantes na camada de rede.

A criptografia IPSec é um padrão do Internet Engineering Task Force (IETF) que apoie algoritmos de criptografia de chave simétrica do 168-bit do Data Encryption Standard (DES) 56-bit e do DES triplo (3DES) no software do cliente de IPSec. A configuração do GRE é opcional com IPsec. O IPSec suporta também autoridades certificadas e negociação do Internet Key Exchange (IKE). A criptografia IPSec pode ser distribuída em ambientes independentes entre clientes, roteadores e firewalls ou pode usada em conjunto com o tunelamento L2TP em VPNs de acesso. O IPsec é apoiado dentro em várias plataformas de sistema operacional.

A criptografia IPSec é a solução de VPN direita para você se você quer a confidencialidade de dados verdadeira para suas redes. O IPsec é igualmente um padrão aberto, assim que a Interoperabilidade entre dispositivos diferentes é fácil de executar.



PPTP e MPPE

O Point-to-Point Tunneling Protocol (PPTP) foi desenvolvido por Microsoft; é descrito no RFC2637 . O PPTP é distribuído extensamente no software do cliente de Windows 9x/ME, do Windows NT, e do Windows 2000, e do Windows XP para permitir VPN voluntários.

Microsoft Point-to-Point Encryption (MPPE) é um rascunho informativo IETF da Microsoft que usa criptografia de 40 bits ou 128 bits com base em RC4. O MPPE é parte de solução de software do cliente de PPTP de Microsoft e é útil nas arquiteturas de VPN de acesso voluntário-MODE. O PPTP/MPPE é apoiado na maioria de plataformas Cisco.

O suporte a PPTP foi adicionado ao software Cisco IOS versão 12.0.5.XE5 nas plataformas Cisco 7100 e 7200. Foi adicionado suporte para mais plataformas no Cisco IOS 12.1.5.T. O Cisco Secure PIX Firewall e o Cisco VPN 3000 Concentrator também incluem suporte para conexões de clientes PPTP.

Desde que o PPTP apoia redes não-IP, é útil onde os usuários remotos têm que discar dentro à

rede corporativa para alcançar redes corporativas heterogêneas.

Para obter informações sobre de configurar o PPTP, veja configurar o PPTP.

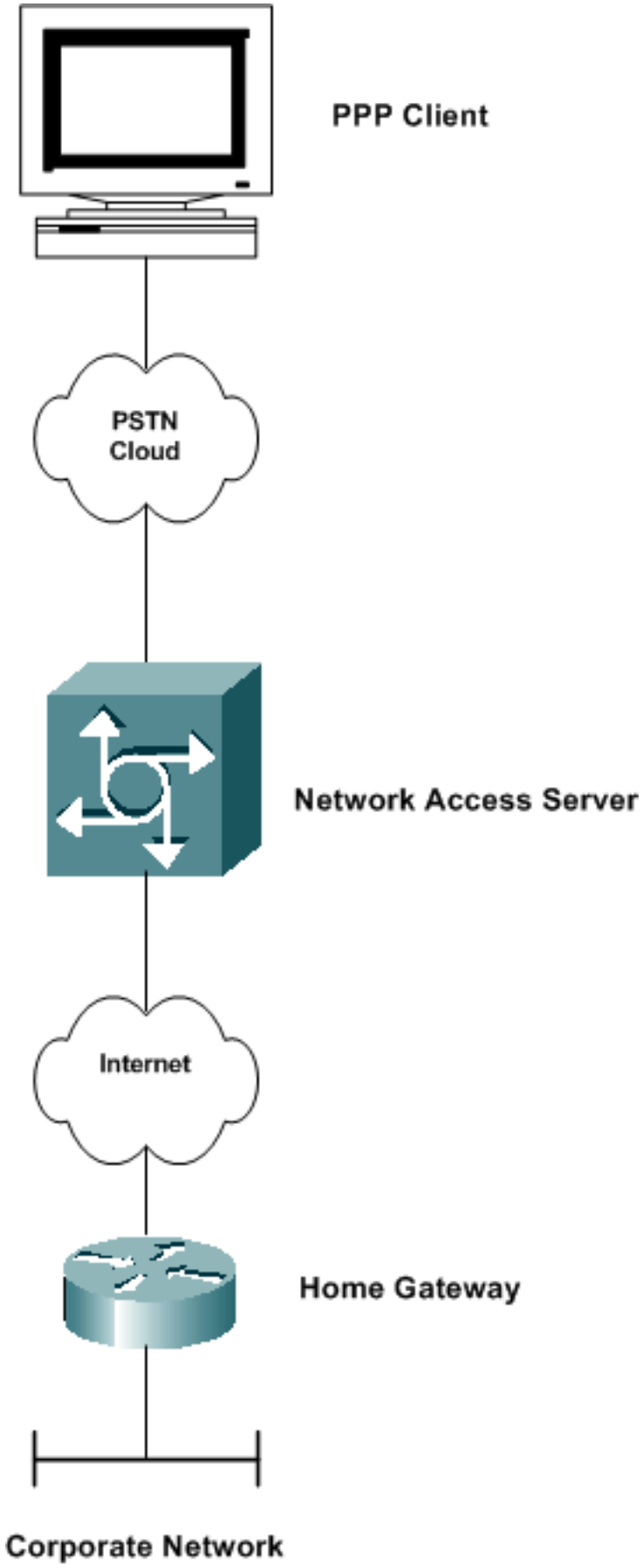
VPDN e L2TP

VPDN

O VPDN (Rede Privada Virtual) é um padrão da Cisco que permite que um serviço de discagem de entrada de rede privada se estenda para servidores de acesso remoto. No contexto da VPDN, o servidor de acesso (por exemplo, um AS5300) discado é, normalmente, chamado Servidor de Acesso de Rede (NAS). O destino do usuário de discagem de entrada é referido como o home gateway (HGW).

O cenário básico é que um cliente do tipo Point-to-Point Protocol (PPP) disca em um NAS local. O NAS determina que a sessão de PPP deve ser enviada a um roteador do Home Gateway para esse cliente. O HGW então autentica o usuário e inicia a negociação PPP. Depois de concluída a instalação do PPP, todos os quadros são enviados via NAS para o cliente e os home gateways. Este método integra diversos protocolos e conceitos

Para obter informações sobre de configurar o VPDN, veja *configurar uma rede dial-up privada virtual em* configurar recursos de segurança.



L2TP

O L2TP (Protocolo de túnel de camada 2) é um padrão IETF que incorpora os melhores atributos do PPTP e L2F. Túneis L2TP são usados principalmente em VPNs de no acesso de modo obrigatório (ou seja, discagem NAS para HGW) para tráfego de IP e não-IP. O Windows 2000 e o

Windows XP adicionaram suporte nativo a esse protocolo como um meio de conexão de cliente VPN.

O L2TP é usado para escavar um túnel o PPP sobre uma rede pública, tal como o Internet, usando o IP. Desde que o túnel ocorre na camada 2, os protocolos de camada superior são ignorantes do túnel. Como o GRE, o L2TP pode igualmente encapsular todo o protocolo da camada 3. A porta 1701 UDP é usada para enviar o tráfego L2TP pelo iniciador do túnel.

Nota: Em 1996 Cisco criou um protocolo da transmissão da camada 2 (L2F) para permitir que as conexões de VPDN ocorram. O L2F ainda é suportado para outras funções, mas foi substituído por L2TP. O protocolo PPTP (Protocolo de túnel ponto a ponto) também foi criado em 1996 como um rascunho da Internet pelo IETF. O PPTP forneceu uma função semelhante à do protocolo de túnel do tipo GRE para as conexões PPP.

Para obter mais informações sobre do L2TP, veja o protocolo de túnel da camada 2.

PPPoE

O PPP over Ethernet (PPPoE) é um RFC informativo que seja distribuído primeiramente em ambientes do digital subscriber line (DSL). O PPPoE tira proveito das infra-estruturas Ethernet existentes para permitir que os usuários iniciem várias sessões PPP com a mesma LAN. Esta tecnologia habilita a seleção do serviço de Camada 3, um aplicativo emergente que permite aos usuários estabelecer conexão simultânea com vários destinos por meio de uma conexão de acesso remoto única. O PPPoE com protocolo password authentication (PAP) ou protocolo de autenticação de cumprimento do desafio (RACHADURA) é usado frequentemente informar a instalação central que roteadores remotos lhe são conectados.

O PPPoE é usado na maior parte em distribuições de DSL do provedor de serviços e em topologias dos Ethernet bridged (transposto).

Para obter mais informações sobre de configurar o PPPoE, veja configurar o PPPoE sobre os Ethernet e o IEEE 802.1Q VLAN.

MPLS VPN

Multiprotocol Label Switching (MPLS) é um novo padrão de IETF baseado no Cisco Tag Switching que ativa os recursos de abastecimento automatizado, implementação rápida e escalabilidade que os provedores precisam para fornecer acesso econômico aos serviços de VPN intranet e extranet. Cisco está trabalhando proximamente com provedores de serviços para assegurar serviços MPLS-permitidos da transição fácil um VPN. O MPLS funciona em um paradigma baseado em rótulo, rotulando pacotes conforme estes entram na rede de provedor, para expedir o encaminhamento através de um centro de IP sem conexão. O MPLS usa distinguidores de rota para identificar a sociedade de VPN e conter o tráfego dentro de uma comunidade de VPN.

O MPLS igualmente adiciona os benefícios de uma aproximação conexão-orientada ao paradigma de Roteamento IP, através do estabelecimento dos caminhos comutados por rótulo, que são criados com base no fluxo de tráfego da informação de topologia um pouco então. O MPLS VPN é distribuído extensamente no ambiente de provedor de serviços.

Para obter informações sobre de configurar o MPLS VPN, veja configurar um MPLS VPN básico.

Informações Relacionadas

- Página de suporte do IPSec
- Como as redes privadas virtuais funcionam
- Página de suporte de NAT
- Página de suporte GRE
- Página de suporte VPDN
- Página de suporte do PPTP
- Página do Suporte PPPoE
- Suporte Técnico - Cisco Systems