Que solução de VPN é perfeita para você?

Contents

Introduction

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

Conventions

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

Prerequisites

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

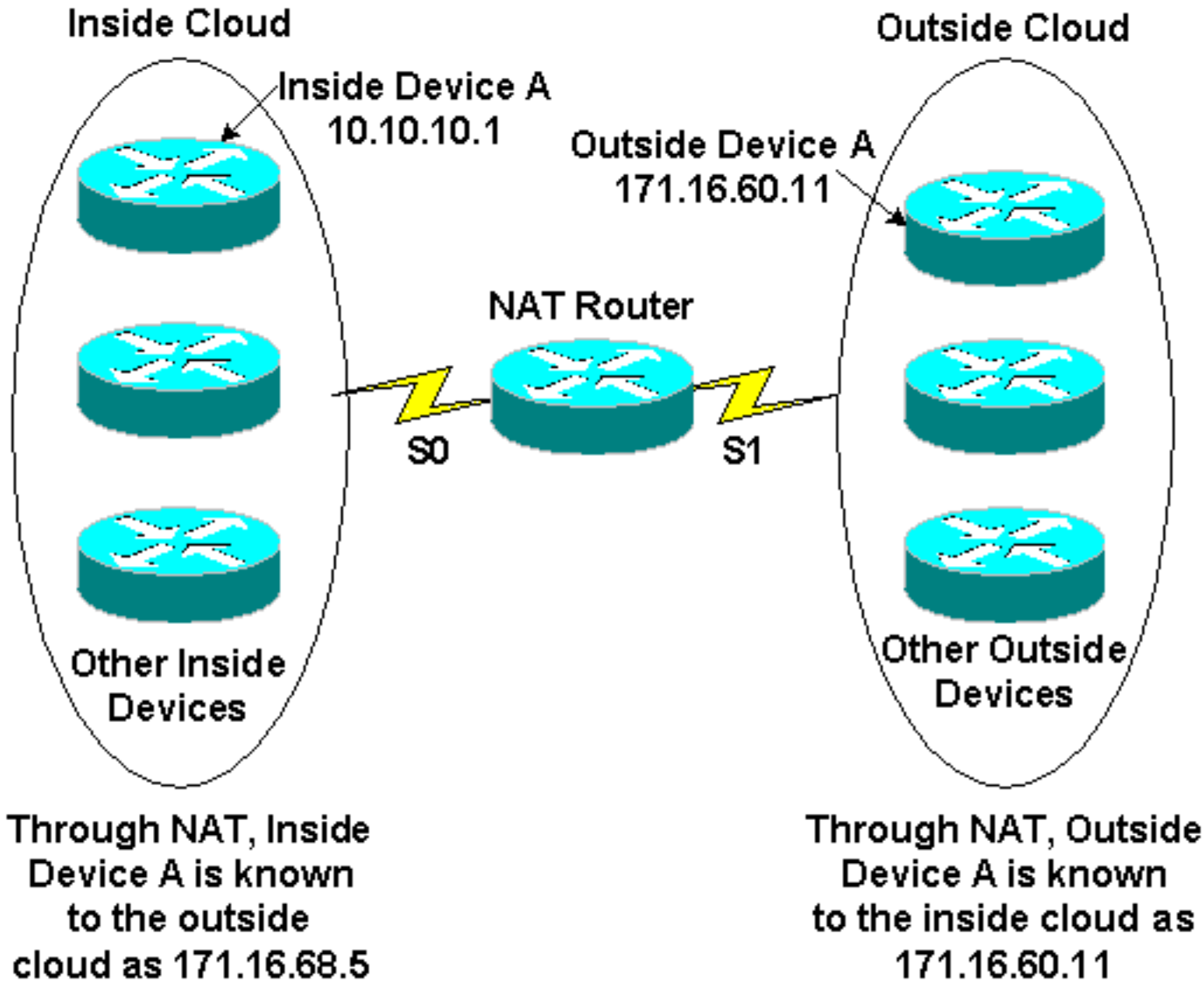
Observação: a Cisco também oferece suporte à criptografia em plataformas não IOS, incluindo o Cisco Secure PIX Firewall, o Cisco VPN 3000 Concentrator e o Cisco VPN 5000 Concentrator.

NAT

A Internet tem vivido um crescimento explosivo em pouco tempo, muito mais do que os criadores 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 para os dispositivos origem e destino. A operação recomendada da NAT envolve RFC 1918 , que descreve esquemas de endereçamento de rede privada adequados. O padrão para NAT é descrito em RFC1631 .

A figura a seguir mostra a definição do limite do roteador NAT com um pool de endereços de rede de tradução interna.

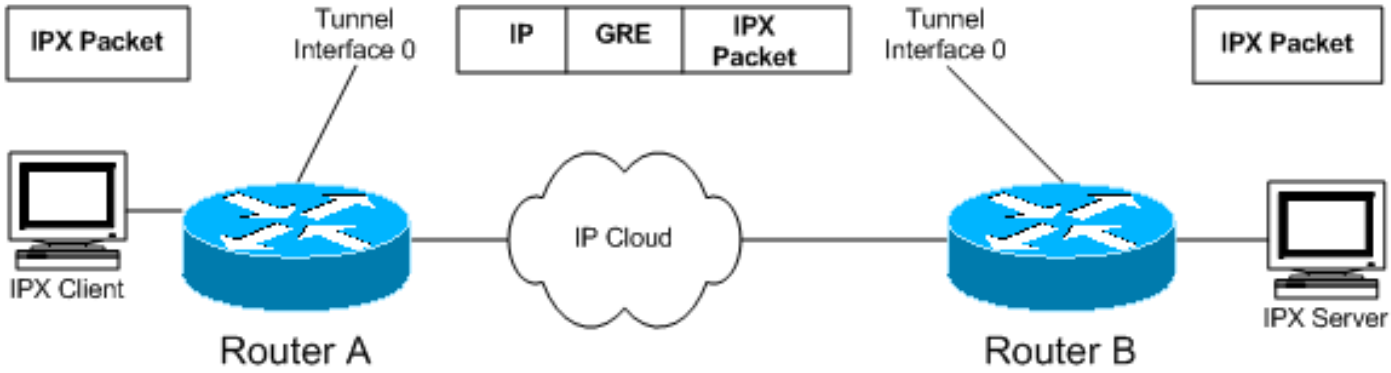


O NAT é geralmente usado para conservar endereços IP roteáveis na Internet, que são caros e em número limitado. O NAT também fornece segurança ocultando a rede interna da Internet.

Para obter informações sobre o funcionamento do NAT, consulte Como o NAT funciona.

Encapsulamento GRE

Os túneis GRE (Generic Routing Encapsulation) fornecem um caminho específico através da WAN compartilhada e encapsulam o tráfego com novos cabeçalhos de pacote para garantir a entrega a destinos específicos. A rede é privada porque o tráfego pode entrar em um túnel somente em um endpoint e pode sair somente no outro endpoint. Os túneis não fornecem verdadeira confidencialidade (como a criptografia faz), mas podem transportar tráfego criptografado. Os túneis são endpoints lógicos configurados nas interfaces físicas através das quais o tráfego é transportado.



Como ilustrado no diagrama, o tunelamento GRE também pode ser usado para encapsular o tráfego não IP no IP e enviá-lo pela Internet ou pela rede IP. Os protocolos Internet Packet Exchange (IPX) e AppleTalk são exemplos de tráfego não IP. Para obter informações sobre como configurar o GRE, consulte "Configurando uma Interface de Túnel GRE" em Configurando o GRE.

O GRE é a solução VPN certa para você se tiver uma rede multiprotocolo como IPX ou AppleTalk e tiver que enviar tráfego pela Internet ou por uma rede IP. Além disso, o encapsulamento GRE é geralmente usado em conjunto com outros meios de proteger o tráfego, como IPSec.

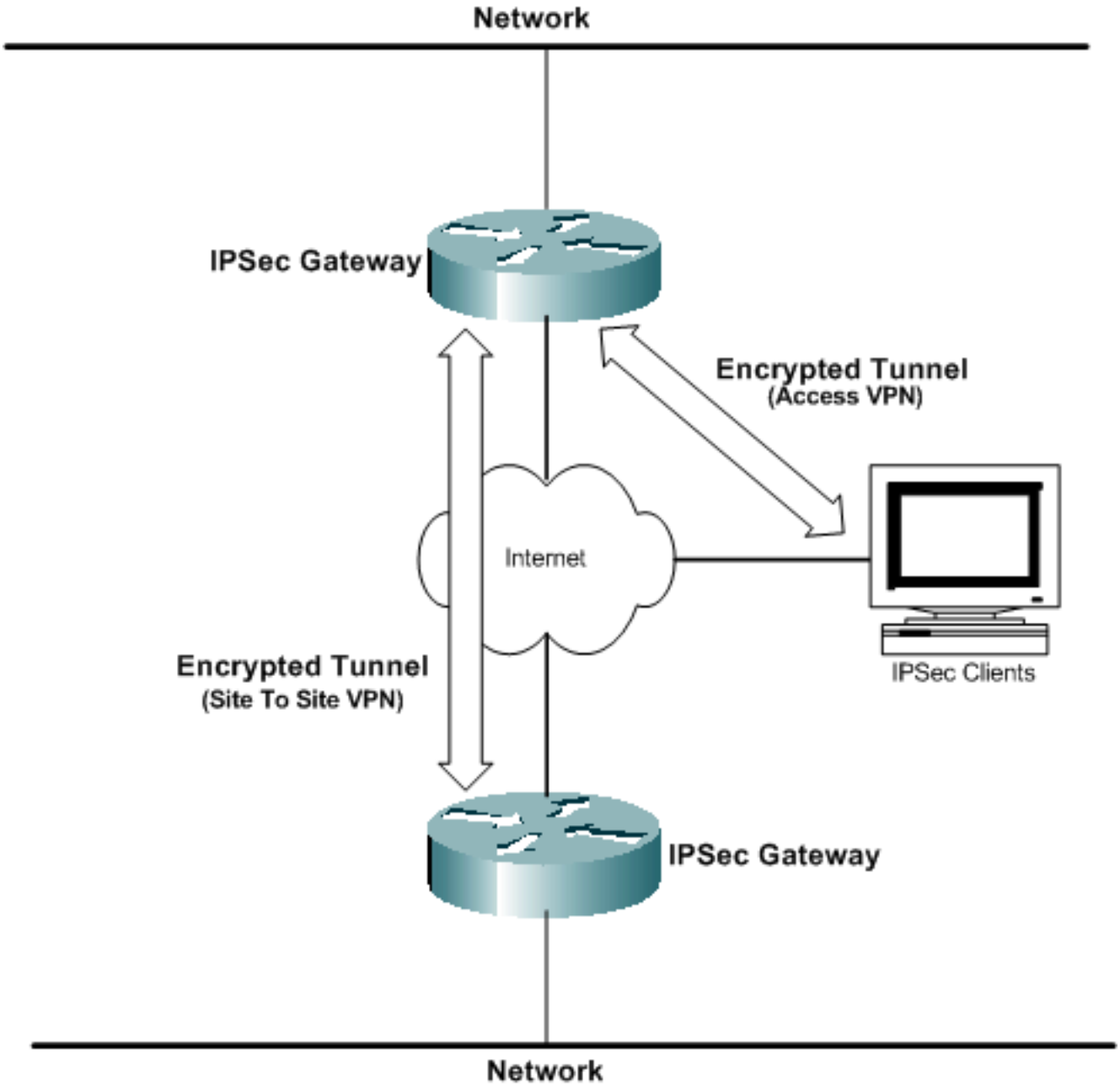
Para obter mais detalhes técnicos sobre GRE, consulte RFC 1701 e RFC 2784 .

Criptografia IPSec

A criptografia de dados enviados através de uma rede compartilhada é a tecnologia VPN mais frequentemente associada a VPNs. A Cisco oferece suporte aos métodos de criptografia de dados IPSec (IP Security). O IPSec é uma estrutura de padrões abertos que fornece confidencialidade de dados, integridade de dados e autenticação de dados entre os correspondentes participantes na camada de rede.

A criptografia IPSec é um padrão da Internet Engineering Task Force (IETF) que suporta algoritmos de criptografia de chave simétrica de 168 bits DES (Data Encryption Standard) de 56 bits e 3DES (3DES) no software cliente IPSec. A configuração de 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 suportado em várias plataformas de sistema operacional.

A criptografia IPSec é a solução VPN certa para você, se quiser a verdadeira confidencialidade dos dados em suas redes. O IPSec também é um padrão aberto, portanto, a interoperabilidade entre diferentes dispositivos é fácil de implementar.



PPTP e MPPE

O PPTP (Point-to-Point Tunneling Protocol) foi desenvolvido pela Microsoft; ele é descrito no RFC2637 . O PPTP é amplamente implantado no software cliente Windows 9x/ME, Windows NT e Windows 2000 e Windows XP para ativar VPNs voluntárias.

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 faz parte da solução de software cliente PPTP da Microsoft e é útil em arquiteturas VPN de acesso de modo voluntário. O PPTP/MPPE é suportado na maioria das 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.

Como o PPTP suporta redes não IP, é útil onde os usuários remotos têm que discar para a rede

corporativa para acessar redes corporativas heterogêneas.

Para obter informações sobre como configurar o PPTP, consulte Configurando o PPTP.

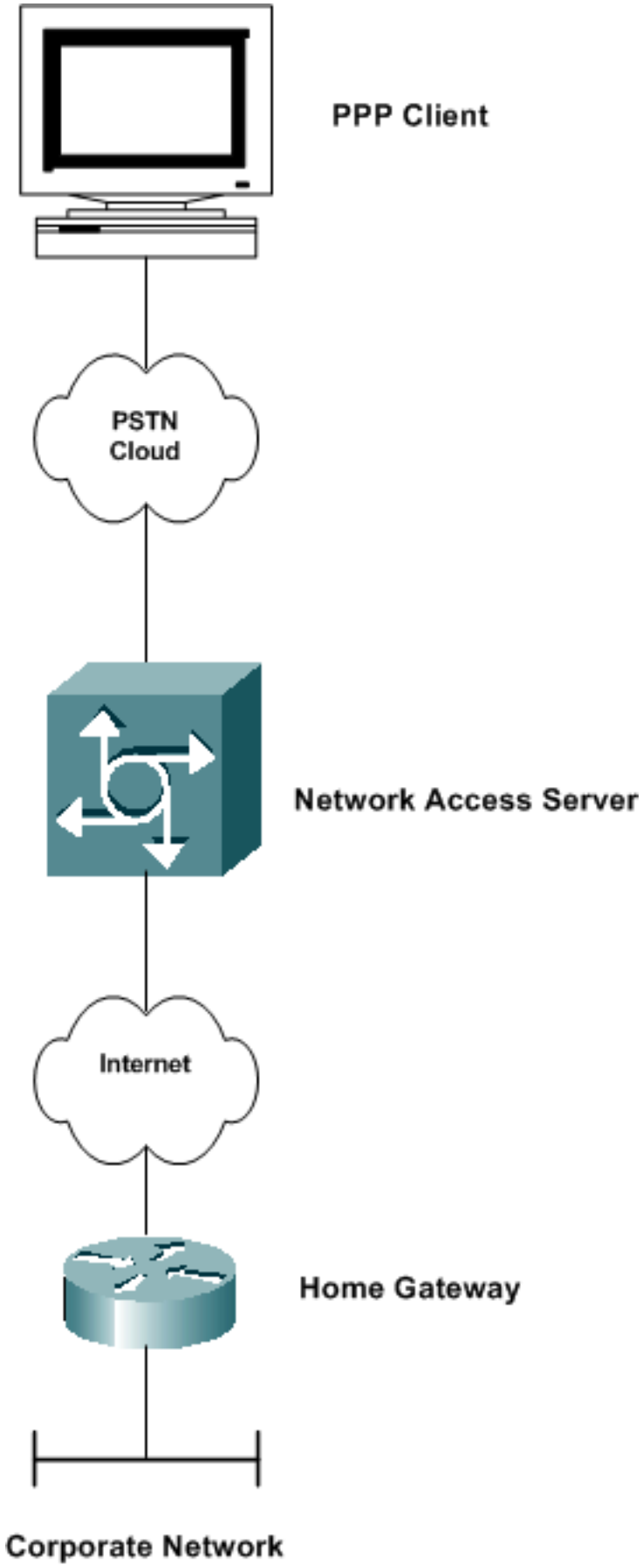
VPDN e L2TP

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 é conhecido como gateway residencial (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 PPP deve ser encaminhada a um roteador de gateway doméstico 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 como configurar a VPDN, consulte *Configuração de uma Rede Virtual Privada de Discagem* em Configuração de 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 fazer o túnel do PPP em uma rede pública, como a Internet, usando o IP. Como o túnel ocorre na camada 2, os protocolos da camada superior ignoram o túnel. Como o GRE, o L2TP também pode encapsular qualquer protocolo da camada 3. A porta UDP 1701 é usada para enviar tráfego L2TP pelo iniciador do túnel.

Observação: em 1996, a Cisco criou um protocolo L2F (Layer 2 Forwarding) para permitir a ocorrência de conexões VPDN. 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 L2TP, consulte Protocolo de Túnel da Camada 2.

PPPoE

PPP over Ethernet (PPPoE) é um RFC informativo que é implantado principalmente em ambientes de linha de assinante digital (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. PPPoE com PAP (Password Authentication Protocol Protocolo de Autenticação de Senha) ou CHAP (Challenge Handshake Authentication Protocol Protocolo de Autenticação de Handshake de Desafio) é frequentemente usado para informar ao site central quais roteadores remotos estão conectados a ele.

O PPPoE é usado principalmente em implantações DSL de provedor de serviços e topologias Ethernet com bridge.

Para obter mais informações sobre como configurar o PPPoE, consulte Configurando o PPPoE sobre Ethernet e a VLAN IEEE 802.1Q.

VPN MPLS

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. A Cisco está trabalhando em conjunto com provedores de serviços para garantir uma transição tranquila para serviços VPN habilitados para MPLS. 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 rotas para identificar a associação VPN e conter o tráfego em uma comunidade VPN.

O MPLS também adiciona os benefícios de uma abordagem orientada a conexão ao paradigma de roteamento IP, através do estabelecimento de caminhos comutados por rótulo, que são criados com base nas informações de topologia e não no fluxo de tráfego. A VPN MPLS é amplamente implantada no ambiente do provedor de serviços.

Para obter informações sobre como configurar a VPN MPLS, consulte Configurando uma VPN MPLS básica.

Informações Relacionadas

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