

Which VPN Solution is Right for You?

Document ID: 14147

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

NAT

GRE Encapsulation Tunneling

IPSec Encryption

PPTP and MPPE

VPDN and L2TP

VPDN

L2TP

PPPoE

MPLS VPN

Related Information

Introduction

Virtual Private Networks (VPNs) are becoming increasingly popular as a lower cost and more flexible way to deploy a network across a wide area. With advances in technology comes an increasing variety of options for implementing VPN solutions. This tech note explains some of these options and describes where they might best be used.

Before You Begin

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

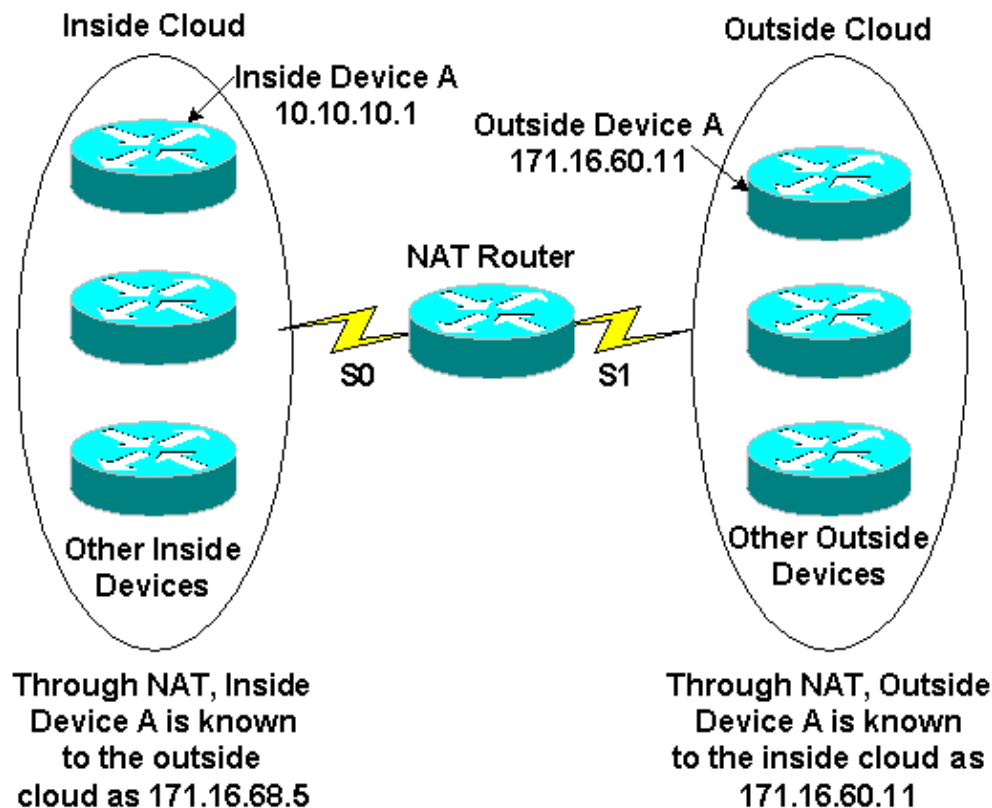
Note: Cisco also provides encryption support in non-IOS platforms including the Cisco Secure PIX Firewall, the Cisco VPN 3000 Concentrator, and the Cisco VPN 5000 Concentrator.

NAT

The Internet has experienced explosive growth in a short time, far more than the original designers could have foreseen. The limited number of addresses available in IP version 4.0 is evidence of this growth, and the result is that address space is becoming less available. One solution to this problem is Network Address Translation (NAT).

Using NAT a router is configured on inside/outside boundaries such that the outside (usually the Internet) sees one or a few registered addresses while the inside could have any number of hosts using a private addressing scheme. To maintain the integrity of the address translation scheme, NAT must be configured on every boundary router between the inside (private) network and the outside (public) network. One of the advantages of NAT from a security standpoint is that the systems on the private network cannot receive an incoming IP connection from the outside network unless the NAT gateway is specifically configured to allow the connection. Moreover, NAT is completely transparent to the source and destination devices. NAT's recommended operation involves RFC 1918 , which outlines proper private network addressing schemes. The standard for NAT is described in RFC1631 .

The following figure shows NAT router boundary definition with an internal translation network address pool.

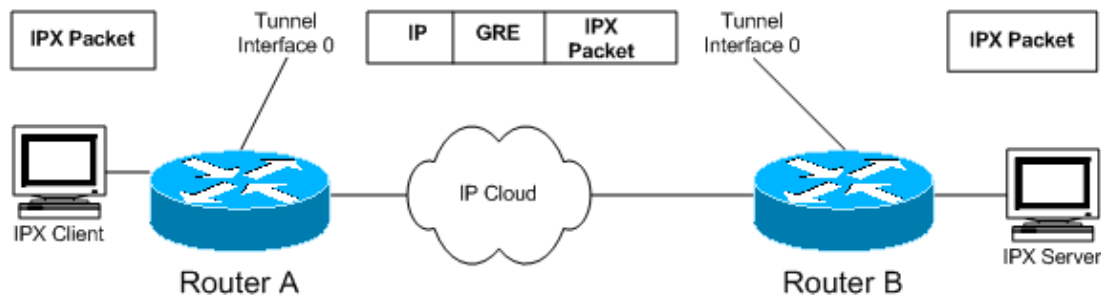


NAT is generally used to conserve IP addresses routable on the Internet, which are expensive and limited in number. NAT also provides security by hiding the inside network from the Internet.

For information on working of NAT, see [How NAT Works](#).

GRE Encapsulation Tunneling

Generic Routing Encapsulation (GRE) tunnels provide a specific pathway across the shared WAN and encapsulate traffic with new packet headers to ensure delivery to specific destinations. The network is private because traffic can enter a tunnel only at an endpoint and can leave only at the other endpoint. Tunnels do not provide true confidentiality (like encryption does) but can carry encrypted traffic. Tunnels are logical endpoints configured on the physical interfaces through which traffic is carried.



As illustrated in the diagram, GRE tunneling can also be used to encapsulate non-IP traffic into IP and send it over the Internet or IP network. The Internet Packet Exchange (IPX) and AppleTalk protocols are examples of non-IP traffic. For information on configuring GRE, see "Configuring a GRE Tunnel Interface" in *Configuring GRE*.

GRE is the right VPN solution for you if you have a multiprotocol network like IPX or AppleTalk and have to send traffic over the Internet or an IP network. Also, GRE encapsulation is generally used in conjunction with other means of securing traffic, such as IPsec.

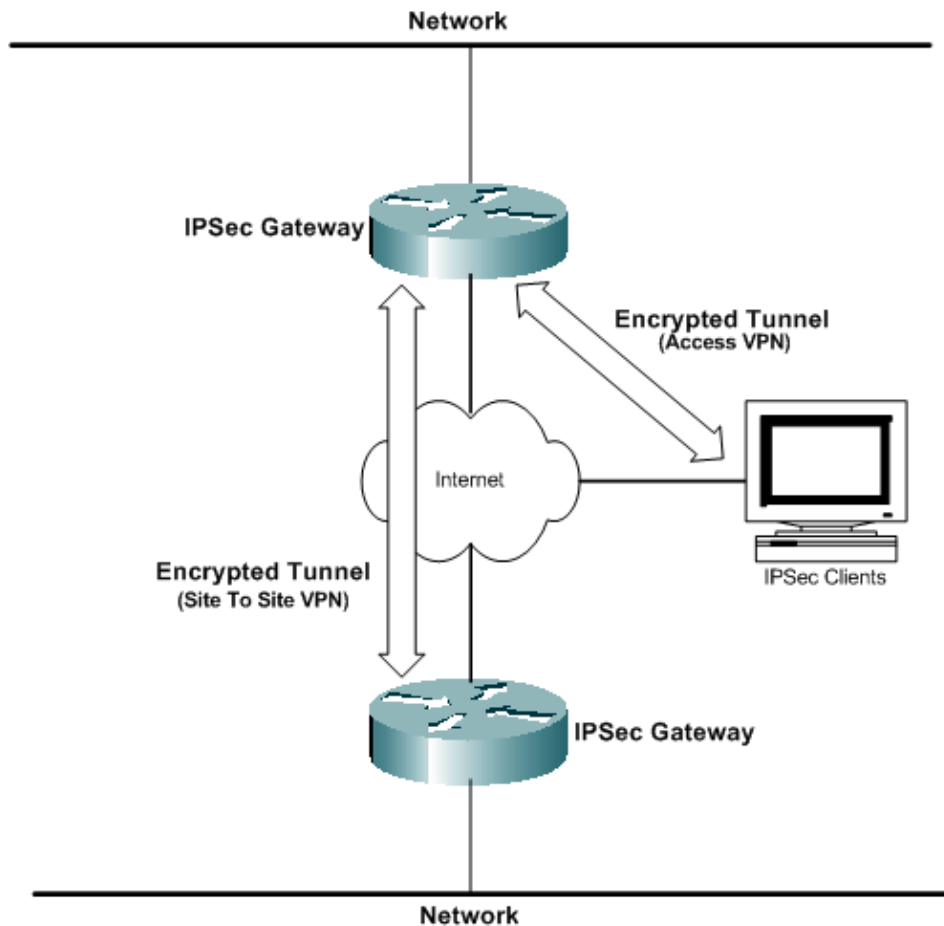
For more technical detail on GRE, refer to RFC 1701 and RFC 2784 .

IPSec Encryption

Encryption of data sent across a shared network is the VPN technology most often associated with VPNs. Cisco supports the IP Security (IPsec) data encryption methods. IPsec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers at the network layer.

IPsec encryption is an Internet Engineering Task Force (IETF) standard that supports Data Encryption Standard (DES) 56-bit and Triple DES (3DES) 168-bit symmetric key encryption algorithms in IPsec client software. GRE configuration is optional with IPsec. IPsec also supports certificate authorities and Internet Key Exchange (IKE) negotiation. IPsec encryption can be deployed in standalone environments between clients, routers, and firewalls, or used in conjunction with L2TP tunneling in access VPNs. IPsec is supported in on various operating system platforms.

IPsec encryption is the right VPN solution for you if you want true data confidentiality for your networks. IPsec is also an open standard, so interoperability between different devices is easy to implement.



PPTP and MPPE

Point-to-Point Tunneling Protocol (PPTP) was developed by Microsoft; it is described in RFC2637 . PPTP is widely deployed in Windows 9x/ME, Windows NT, and Windows 2000, and Windows XP client software to enable voluntary VPNs.

Microsoft Point-to-Point Encryption (MPPE) is an informational IETF draft from Microsoft that uses RC4-based 40-bit or 128-bit encryption. MPPE is part of Microsoft's PPTP client software solution and is useful in voluntary-mode access VPN architectures. PPTP/MPPE is supported on most Cisco platforms.

PPTP support was added to Cisco IOS Software Release 12.0.5.XE5 on the Cisco 7100 and 7200 platforms. Support for more platforms was added in Cisco IOS 12.1.5.T. The Cisco Secure PIX Firewall and Cisco VPN 3000 Concentrator also include support for PPTP client connections.

Since PPTP supports non-IP networks, it is useful where the remote users have to dial in to the corporate network to access heterogeneous corporate networks.

For information on configuring PPTP, see [Configuring PPTP](#).

VPDN and L2TP

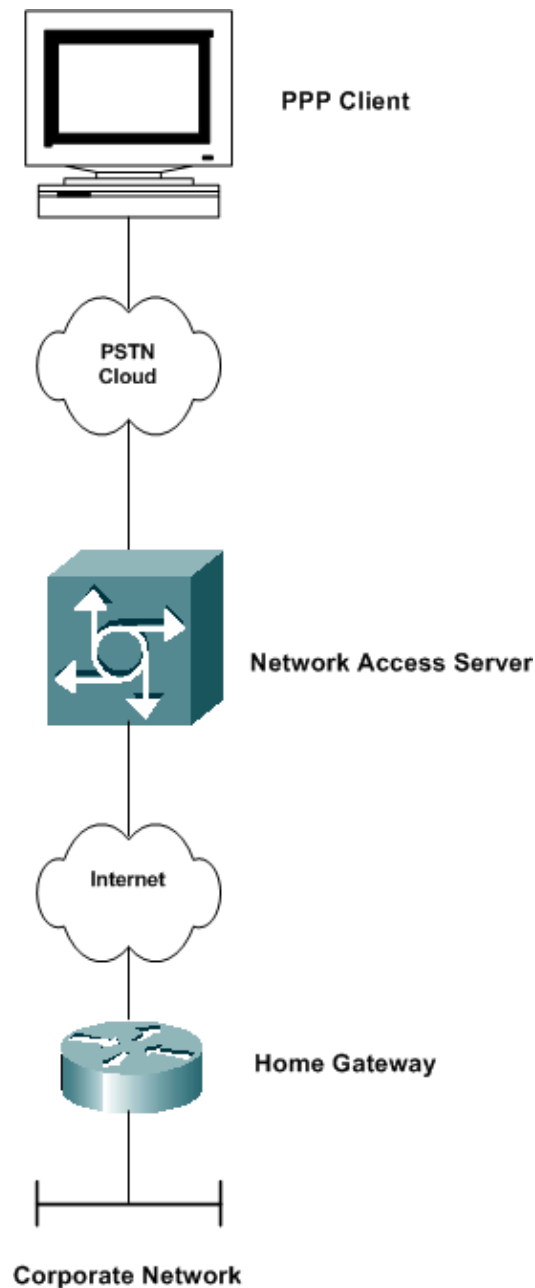
VPDN

Virtual Private Dialup Network (VPDN) is a Cisco standard that allows a private network dial-in service to span across to remote access servers. In the context of VPDN, the access server (for example, an AS5300) that

is dialed into is usually referred to as the Network Access Server (NAS). The dial-in user's destination is referred to as the home gateway (HGW).

The basic scenario is that a Point-to-Point Protocol (PPP) client dials in to a local NAS. The NAS determines that the PPP session should be forwarded to a home gateway router for that client. The HGW then authenticates the user and starts the PPP negotiation. After PPP setup is complete, all frames are sent via the NAS to the client and home gateways. This method integrates several protocols and concepts.

For information on configuring VPDN, see *Configuring a Virtual Private Dial-Up Network* in *Configuring Security Features*.



L2TP

Layer 2 Tunneling Protocol (L2TP) is an IETF standard that incorporates the best attributes of PPTP and L2F. L2TP tunnels are used primarily in compulsory-mode (that is, dialup NAS to HGW) access VPNs for both IP and non-IP traffic. Windows 2000 and Windows XP have added native support for this protocol as a means

of VPN client connection.

L2TP is used to tunnel PPP over a public network, such as the Internet, using IP. Since the tunnel occurs on Layer 2, the upper layer protocols are ignorant of the tunnel. Like GRE, L2TP can also encapsulate any Layer 3 protocol. UDP port 1701 is used to send L2TP traffic by the initiator of the tunnel.

Note: In 1996 Cisco created a Layer 2 Forwarding (L2F) protocol to allow VPDN connections to occur. L2F is still supported for other functions, but has been replaced by L2TP. Point-to-Point Tunneling Protocol (PPTP) was also created in 1996 as an Internet draft by the IETF. PPTP provided a function similar to GRE-like tunnel protocol for PPP connections.

For more information on L2TP, see Layer 2 Tunnel Protocol.

PPPoE

PPP over Ethernet (PPPoE) is an informational RFC that is primarily deployed in digital subscriber line (DSL) environments. PPPoE leverages existing Ethernet infrastructures to allow users to initiate multiple PPP sessions within the same LAN. This technology enables Layer 3 service selection, an emerging application that lets users simultaneously connect to several destinations through a single remote access connection. PPPoE with Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) is often used to inform the central site which remote routers are connected to it.

PPPoE is mostly used in service provider DSL deployments and bridged Ethernet topologies.

For more information on configuring PPPoE, see Configuring PPPoE over Ethernet and IEEE 802.1Q VLAN.

MPLS VPN

Multiprotocol Label Switching (MPLS) is a new IETF standard based on Cisco Tag Switching that enables automated provisioning, rapid rollout, and scalability features that providers need to cost-effectively provide access, intranet, and extranet VPN services. Cisco is working closely with service providers to ensure a smooth transition to MPLS-enabled VPN services. MPLS works on a label-based paradigm, tagging packets as they enter the provider network to expedite forwarding through a connectionless IP core. MPLS uses route distinguishers to identify VPN membership and contain traffic within a VPN community.

MPLS also adds the benefits of a connection-oriented approach to the IP routing paradigm, through the establishment of label-switched paths, which are created based on topology information rather than traffic flow. MPLS VPN is widely deployed in the service-provider environment.

For information on configuring MPLS VPN, see Configuring a Basic MPLS VPN.

Related Information

- [IPSec Support Page](#)
 - [How Virtual Private Networks Work](#)
 - [NAT Support Page](#)
 - [GRE Support Page](#)
 - [VPDN Support Page](#)
 - [PPTP Support Page](#)
 - [PPPoE Support Page](#)
 - [Technical Support – Cisco Systems](#)
-

