Virtual Private Networks – Solutions for Secure Remote Access

---

White Paper

Last revised: June 2006

Table of Contents

Table of Contents 3
Virtual Private Networks – Solutions for Secure Remote Access 4
Abstract 4
What is a VPN 4
Responsibilities of a VPN 5
VPN Categories 6
Elements of a VPN Connection 7
Tunneling Protocols 8
VPN Risks 10
Summary 12

Virtual Private Networks – Solutions for Secure Remote Access

Abstract

Virtual Private Networks, or VPNs, have become an essential part of company network infrastructures both large and small. The ability for users to access resources in an internal corporate network securely from remote locations has created a wealth of opportunities for companies both from a functional as well as convenience standpoint. The technology involved in creating secure network connections over the public Internet is complex, and can involve a number of communications protocols along with various hardware and software components. This paper will provide an overview of VPNs. Topics of discussion include the responsibilities of a VPN, essential elements, tunneling protocols, and risks associated with using VPNs.

What is a VPN

In today's information technology environments, a network whose only function is connecting fixed corporate sites is no longer a feasible solution of many companies. Remote users, such as telecommuters, sales representatives, consultants, and external business partners, now require access to internal corporate resources. The popularity of telecommuting alone has resulted in an ever increasing number of VPN implementations. Companies can also use VPN solutions to gain a competitive edge. For example, sales and marketing representatives can easily access the latest information from corporate

headquarters from anywhere in the world at a moments notice. All that is required is a connection to the public network.

A VPN is a private communications network usually used within a company, or by several different companies or organizations, to communicate over a public network. VPN message traffic is carried on public networking infrastructure, like the Internet, using standard protocols, or over a service provider's network providing VPN service. A VPN can utilize existing transport technologies, such as the public Internet, service provider IP backbones, as well as Frame Relay and ATM network infrastructures to allow remote users to access corporate intranets from virtually anywhere.

Responsibilities of a VPN

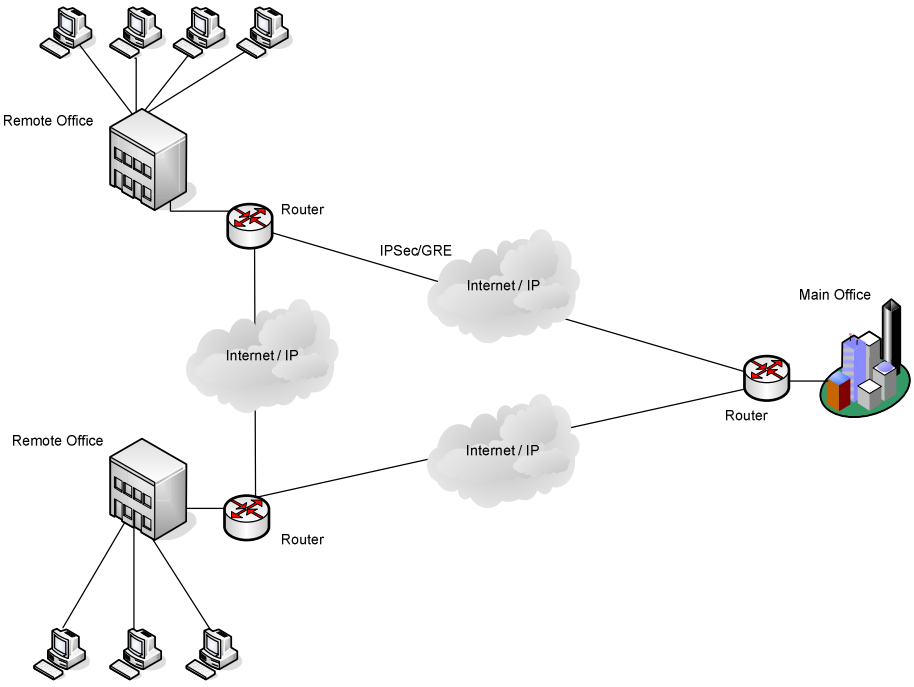
A VPN implementation should satisfy a number of basic requirements, the first of which is user authentication. Opening any kind of access to an internal corporate network, no matter how secure, poses a significant security risk. The remote access solution must ensure that only those clients that should access the internal resources should be allowed to do so. The next requirement is address management. The VPN server is responsible for assigning ip (internet protocol) addresses to incoming client connections and the secure tunnel through the public network needs to keep the private IP addresses used during the VPN session in private hands. Another essential responsibility of a VPN is data encryption. The secure connection provided by the VPN tunnel is only one layer of security. Encryption of the actual data being transferred is additional protection in the event the security of the tunnel is compromised. Finally, the VPN solution must support the different network protocols most commonly used on public

networks. This last requirement is no different than any other communication that takes place across public networks.

VPN Categories

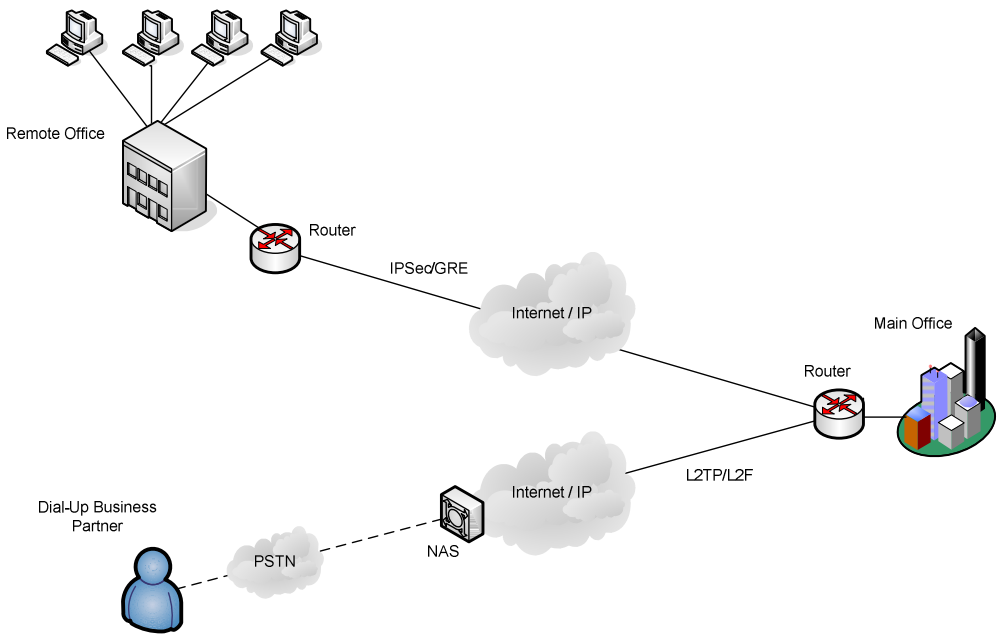
VPNs are divided into three categories: remote access, intranet, and extranet. Remote access VPNs connect remote users and smaller satellite offices with minimal traffic to a corporate wide area network (WAN) where internal company resources can be accessed. Intranet VPNs connect branch offices and home offices with higher network traffic to a company's intranet, as shown in Figure 1-1:

Figure 1-1



Extranet VPNs supply secure connectivity and provide shared information to business partners, such as suppliers or customers. Figure 1-2 shows this configuration:

Figure 1-2



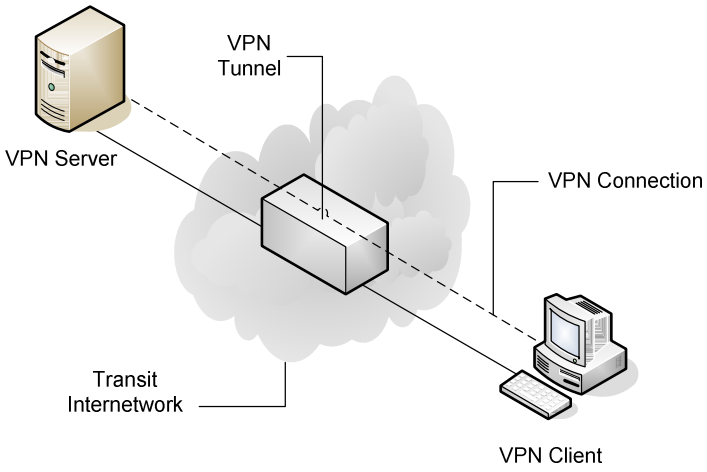
Each category contains different elements but has one essential characteristic in common; the security policies of these remote connections all match the standard policies implemented within that particular company's internal network.

Elements of a VPN Connection

There are four essential elements of a VPN connection. The first is the VPN server, which is a computer located on the corporate side of the connection that manages incoming connection requests from the outside world. The second is the VPN client. This is the computer that initiated the connection request to the VPN server. Once these two machines achieve a secure connection the third element of the VPN is created, which is the tunnel. This is the secure channel that is created across the public Internet and is where the data is encapsulated, that is, the data is embedded in another secure layer. The

final element is the VPN connection, which handles the actual encryption of the data. Figure 1-3 shows these elements and where they are in relation to each other:

Figure 1-3

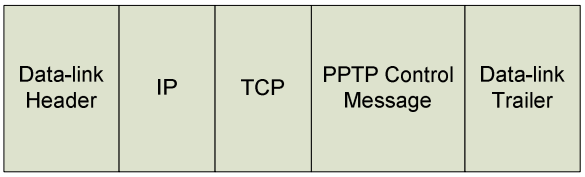


Tunneling Protocols

Up until recently, VPN connections utilized one of four protocols: Point-to-Point Tunneling Protocol (PPTP), Internet Security Protocol (IPSec), Layer 2 Tunneling Protocol (L2TP), or Layer 2 Forwarding (L2F). Each protocol functions in different ways with significantly different packet configurations.

PPTP was developed by Microsoft, U.S. Robotics, and a number of smaller vendors known as the PPTP Forum. PPTP works at Layer 2, which is the Datalink layer, of the OSI model. It encapsulates PPP frames into IP datagrams via Generic Routing Encapsulation (GRE) and transmits them over an IP network. PPTP utilizes a TCP connection to establish and maintain the secure tunnel. Figure 1-4 shows the components of a PPTP packet:

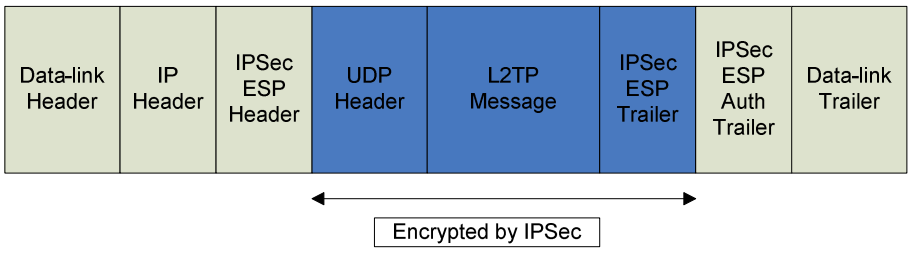
Figure 1-4



The IPSec protocol is similar to TCP/IP and uses IP for routing purposes. However, IPSec's strength is its encryption capabilities, which are used to ensure the data is unreadable by intruders, and that the two ends of a connection are authenticated, and make sure each packet arrives successfully at its destination. Both client and server must be IPSec compliant, and a public key is required for IPSec to work.

L2TP originated from Cisco Systems and combines features of PPTP and Layer 2 Forwarding. As the name suggests, L2TP is also an OSI Layer 2 protocol. Like PPTP, this protocol encapsulates PPP frames, which are then sent as User Datagram Protocol (UDP) messages. This UDP packet is then encapsulated into an IPSec packet, which contains the source and destination IP addresses of the VPN tunnel and ensures that the UDP packet is delivered securely. As can be seen in Figure 1-5, the structure of an L2TP packet is quite different from a PPTP packet:

Figure 1-5



L2TP is really a successor to PPTP as it is based on the PPTP specifications. L2TP combines the best of PPTP with the security of IPSec to form a hybrid product that is starting to gain wide support. L2TP is harder to install and configure, as well as manage, than either PPTP or IPSec, but it is starting to gain popularity because of its security and reliability. To date, only a few L2TP products are available, but the number is sure to grow as VPNs become more popular.

L2F has been kept proprietary by Cisco and is found only in their products, although some of the L2F features have been incorporated into L2TP.

The latest technology to emerge for VPNs is the Secure Sockets Layer (SSL) protocol. It is used to secure web-based communications over the Internet. This has allowed VPN solution providers to develop web-based VPN solutions, which greatly simplifies the overall VPN configuration, especially on the client side. For instance, all that is required for a SSL VPN connection is access to the Internet. No software needs to be installed on the client machine. This means that even hardware such as cell phones and handheld devices can now establish VPN connections. The fact that no client-based software is required for SSL VPN greatly reduces the workload of corporate IT departments, who do not have to worry about installations, support, and upgrades on the client side.

VPN Risks

Even though VPN technology is an extremely secure method of communications, there remain risks associated with its use. No communication across a public network should be considered 100% secure. Weak points that would-be hackers will try to exploit will always exist, no matter how diligently and securely the remote access solution is

designed. Microsoft's PPTP, for example, has suffered from a number of security-related flaws over the course of its development. Many patches released by Microsoft to resolve existing problems at times created new ones, which in turn had to be fixed. These problems are not always identified immediately, so months or years can pass before a security hole is closed. Although L2TP avoided the problems associated with many proprietary protocols, its specification reveals that it is easy to inject malicious packets into L2TP tunnels once communication has been authenticated. While IPSec theoretically offers a high level of security, its specifications are so complex that they have proven difficult to analyze and thus difficult to implement effectively. If a VPN's security foundation is not solid, then it is no more secure than a non-private virtual network routed over the Internet.

Finally, configuring an effective VPN solution is by its own nature complex. IT Professionals who are not familiar with VPN technology often attempt to implement a solution on their own, resulting in a misconfigured and unsecured VPN solution. The author of this paper was approached at a previous place of employment with the task of implementing a VPN solution for the company. The company was quite small, and budget constraints were such that the company's president insisted that we forgo outside assistance. Three people were employed in the IT department, none of whom had any experience with VPNs. After weeks of lobbying and pleading, the president decided that the VPN infrastructure was one area where the company should spend more money, rather than suffer the consequences of saving money on one of the most important pieces of the network infrastructure. An experienced consultant was ultimately used for installation, configuration, and comprehensive training.

Summary

Virtual Private Networks allow businesses an incredible amount of flexibility in where and how employees conduct business. The convenience of being able to access the information and resources from basically anywhere in the world should be considered one of the greatest achievements in the realm of data communications. The VPN industry is expanding at a rapid rate, and continues to introduce new VPN solutions, such as web-based VPNs, that allow for even easier access. One of the reasons for the rapid evolution of VPN technology is the need for VPN solution providers to remain one step ahead of any potential threats to their systems. Transmitting sensitive material across a public network, even in a secure and encrypted connection, can be somewhat of a leap of faith. However, VPN popularity, and the way the technology has influenced the business plans of a majority of the world's companies, is evidence that companies are willing accept the potential risks involved in exchange for the convenience and capabilities that VPNs provide.