GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

What's a VPN?

By Sam Clayton

➢ Introduction

As the title suggests the purpose of this paper is to provide an introduction to VPNs. This brief discussion will include information on some of the VPN protocols and provide brief examples of when these protocols should be used. However, before any of this can be discussed it is first necessary to define the acronym VPN, what a VPN is, and what it does. VPN stands for virtual private network. A VPN device can either be software or hardware and may need to be installed on both client (receiver) and server (sender) machines. These VPN devices are used to create secure private links between the client and server. Virtual private networks use a public network as a link to two or more other endpoints. For this paper the primary example of a public network will be the Internet, however this does not mean that a virtual private network could not be set up using some other backbone connection. An endpoint could be a local area network (LAN) device such as a router or an end-user workstation. In a situation where both end points are LAN devices the connection is described as LAN-to-LAN. If an end point is an end-user workstation then the connection is said to be a LAN-to-network-client connection. The link between these end points only exists when necessary, so when the transaction or session has been completed the link between the end points is destroyed. Connectivity between the end points of a VPN connection is established through tunneling. To establish a tunnel, both the tunnel client and the tunnel server must be using the same tunneling protocol. Tunnels are created using tunneling protocols that hide and encapsulate private network data in Internet Protocol (IP) packets. Tunnels also protect the packets against snooping by outsiders via methods of encryption.

Virtual private networks can be used in many situations. As mentioned earlier there are two general categories that can be used to describe VPN connections. These categories are LAN-to-LAN and LAN-to-network-client. An example of when to implement a LAN-to-LAN VPN connection is when different buildings/companies need to be connected. For instance, an office in Ohio needs to be linked to the office in New York. Another, instance of a LAN-to-LAN VPN would be connecting computers over an intranet. In this situation there may be information that only select people in the company require. Given the sensitive nature of the information this data must also be encrypted as it travels over the company's intranet so that curios workers are not able to intercept the data packets. A circumstance that may require a company to use a LAN-to-network-client VPN connection would be when employees are traveling around the country and may need to connect to the corporate network. VPN connections of this type most likely require a dial-up connection, where the employee on the remote computer dials-up a local Internet service provider (ISP) connection and the VPN software then creates the secure connection with the corporate network.

➢ Protocols

Prior to discussing the implementation of a VPN it is important to know a little about the different VPN protocols also referred to as tunneling protocols. These protocols include Point-to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding (L2F),

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Layer 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPSec) Protocol. Of these four protocols PPTP, L2F, and L2TP are very closely related to one another by Point-to-Point Protocol (PPP). PPP is a dial-up protocol used to connect to the Internet. The early use of PPP facilitated accessing the Internet by automating the login process and essentially handling all of the configuration details needed to communicate with the Internet. These automated features reduced the input required from the user. This meant that the user simply had to supply a login ID, password, and the telephone number of the dial-up Internet service provider (ISP) or network server. Once these three pieces of information were given the PPP software would complete the remaining configurations.

When it comes to dialing into a remote network using a modem PPP is the most popular option. PPP transmits data by encapsulating network specific packet in to IP packet for transmission over the Internet. In this way PPP has the capability to transport multi-protocols, which means that it can transport non-routable protocols like IPX (Internetwork Packet Exchange), NetBEUI, and AppleTalk, in addition to TCP/IP. A further advantage of PPP is its ability to transport multi-protocols over the same connection at the same time. It is important to recognize the capabilities of PPP because of the role it plays in the development of the more advanced VPN protocols of PPTP, L2F, and L2TP. All three of these protocols are primarily focused on usage in dial-up network VPNs, and inherit, if you will, their dial-in capabilities and ease of use from PPP technology.

One of the first and most popular of these dial-in protocols to be developed for VPNs is PPTP. PPTP encapsulates PPP frames in IP datagrams for transmission over an IP capable network, such as the Internet. The primary reason of the popularity of PPTP is due to its support by the Windows operating systems. PPTP receives many of it characteristics from PPP (Point-to-Point Protocol). Because of the relationship between the two protocols PPTP is considered to be very flexible because just like PPP it can be used in non-TCP/IP (Transmission Control Protocol/Internet Protocol) environments. This means that it can handle non-routable protocols such as IPX (Internetwork Packet Exchange) and NetBEUI. This relationship extends to PPTP security in that it uses the standard PPP authentication methods of PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol). Additionally, Microsoft has provided an enhanced version of the CHAP authentication method for PPTP called MS-CHAP. The enhancement that MS-CHAP provides is the ability to use the information within the NT domains for security. Also, instead of using PPP to encrypt data Microsoft employs a stronger encryption for use with PPTP, called MPPE (Microsoft Point-to-Point Encryption).

Layer 2 Forwarding (L2F) has many of the same capabilities as PPTP. L2F is designed to work with PPP and supports non-routable protocols like PPTP. In addition to those capabilities L2F can support more authentication standards such as TACACS+ (Terminal Access Controller Access Control System) and RADIUS (Remote Authentication Dial-in User Service). These types of authentication standards authenticate at the beginning of the transmission. L2F is also able to work on different networks such as Frame Relay, and ATM (Asynchronous Transfer Mode) networks. Another significant improvement over PPTP is that L2F allows for multiple connections through a single tunnel, whereas PPTP allows for only one connection.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Layer 2 Tunneling Protocol (L2TP) is another VPN protocol. L2TP has the same capabilities as L2F and PPTP. L2TP allows multiple connections through one tunnel, works with various network types just as L2F does, and also supports non-routable protocol and uses PPP to provide dial-up access like PPTP. One major difference is that L2TP has IPSec compliant, unlike the others. IPSec is another protocol designed for VPN use. IPSec provides strong security standards for encryption, authentication and key management. Using IPSec allows the sender of packets to either authenticate and/or encrypt each IP packet. The separation of these two options has led to two different modes in which IPSec can be used. One mode is the transport mode, wherein only the transport-layer segment of the IP packet is encrypted or authenticated. This is less secure than the other mode option of tunnel mode. In tunnel mode encryption authentication is applied to the entire packet not just one segment. Encrypting and authenticating the entire packet increases the security because it provides more protection against attacks and snooping. In an environment where TCP/IP is the only protocol used IPSec will provide the best in confidentiality, data integrity, encryption, and authentication.

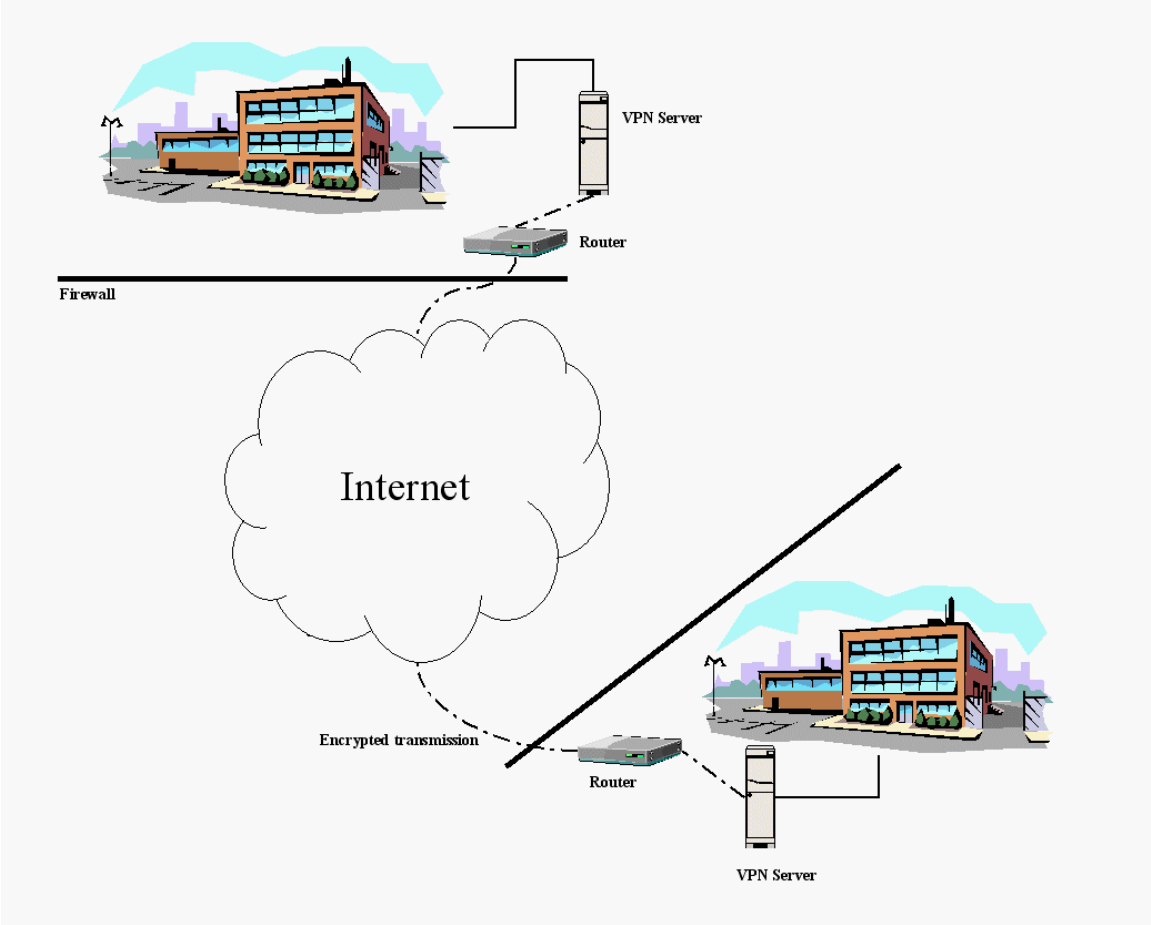
The primary difference between these VPN protocols is their use. Depending on the situation one protocol may be better or more practical than the other. This is evident by the fact that PPTP, L2F and L2TP are mainly suited for use with dial-up VPNs, while IPSec is built to play a greater role in network-to-network VPNs. One more thing to note about these protocols is that PPTP, L2F and L2TP operate on Layer 2 of the Open Systems Interconnection (OSI) model, where as IPSec operates at layer 3. Layer 2 is the Data-link layer and layer 3 is the Network layer. Data-link layer VPN protocols encapsulate their data in PPP frames to be sent across an internetwork, where as Network layer VPN protocols use packets. The advantage to operating at the Data-link layer is the capability to transmit protocols other than IP through the tunnels. Conversely, IPSec operating at the network layer is limited to using IP only protocols. In a LAN-to-network-client situation PPTP, L2F, or L2TP protocols would be useful and of those three L2TP would be the best choice. In this situation the all options are based on the assumption that the remote client has to dial-in. However, if you where trying to create a LAN-to-LAN situation you would still have the choice of all three tunneling protocols in addition to IPSec, and out of the four choices IPSec would be best option. In this scenario the best option assumes that each LAN is connected via a connection that does not require dial-up, but is always on such as a DSL (digital subscriber line) line or a T1 connection to the Internet.

- **Implementation**

Finally, using all the information provided in this report a general VPN construction or implementation can take shape. In implementing a VPN there are a few things that must be done before any work can begin. In any project such as this it is always wise to plan. Planning can be accomplished by simply analyzing your current network situation (if you have one) and based on that information developing an efficient order of operations by which to get your VPN on-line. Once a plan has been decided on the components for constructing your VPN can be acquired.

This philosophy of analyzing your needs, planning your strategy, and gathering materials for executing the plan can be utilized in the example on the next page. Looking

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

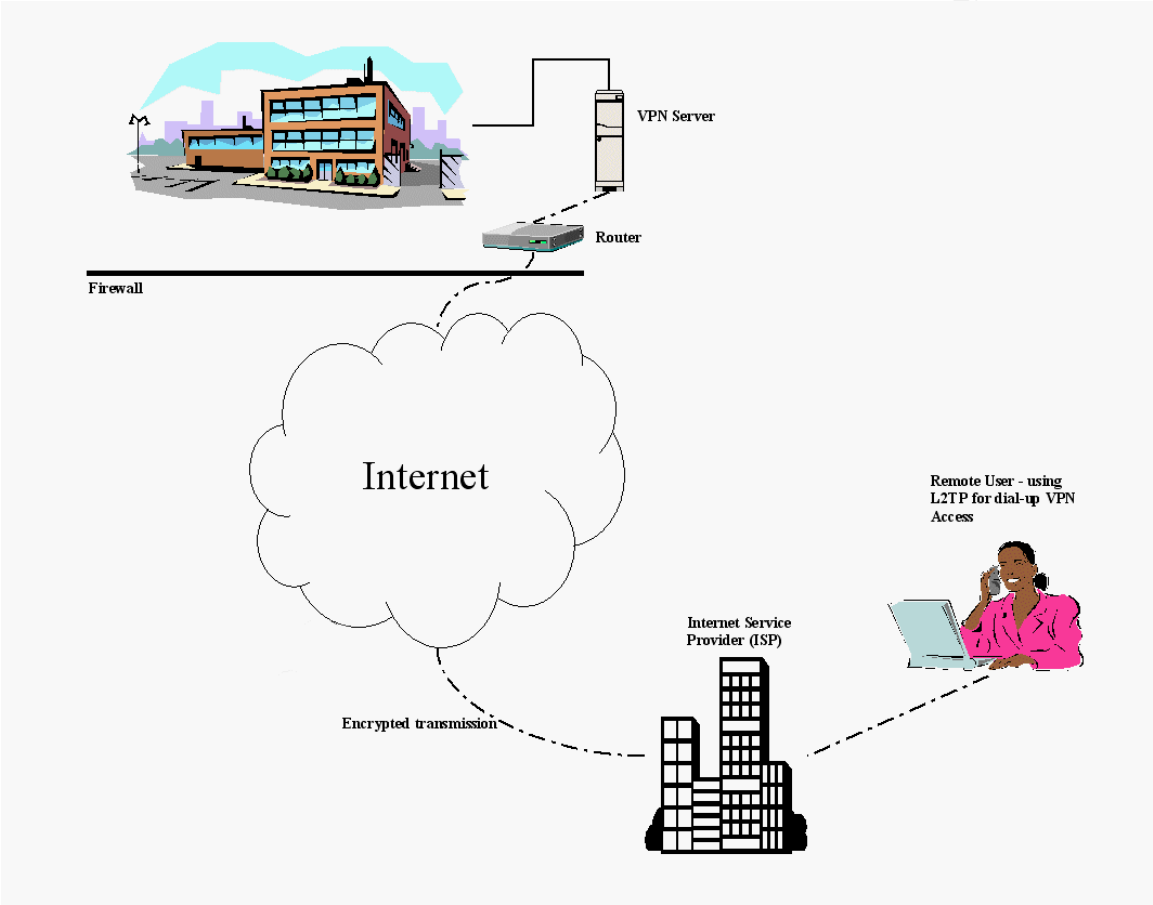


at this example, there are two remote sites (LANs) that need to be connected so that they can operate as one large network and share information securely. Both of these LANs are located behind a firewall and are directly connected to the Internet by high bandwidth DSL. After analyzing the situation and planning the operation the company buys two routers and a VPN protocol server (VPN server). This VPN server will be using IPSec as its VPN protocol. As mentioned earlier IPSec is the best option when working in a LAN-to-LAN environment where there is no need to dial-in to an ISP. In this example all the encryption and decryption is handled by the VPN servers, the client workstations do not actually perform any encrypting. When a workstation in Building A sends information to a workstation in Building B, the VPN server in Building A encrypts the data and sends it out through the router to Building B. Upon receiving the information Building B sends the information through its router which then sends it to be decrypted by the VPN server in Building B. Finally, the VPN server in Building B sends it to the destination workstation.

While this process answered the need to connect both sites securely it still does not help the members of the company that travel and need to access the network remotely using their laptop, for instance. In order to maintain the level of security provided by the LAN-to-LAN connection the company will have to provide an additional VPN service for dial-in remote users. For these types of remote transmissions and/or connections to occur you will most likely have to use a dial-in ISP to connect to the company's server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As seen below this process can be executed securely by using one of the dial-in VPN protocols. In the following example the company has decided to use L2TP as its dial-in VPN protocol. Using this protocol the remote user can create a secure connection with the company server. This example unlike the previous example required that the VPN protocol exist on the remote user's workstation. In this way the remote workstation is said to have a software VPN implentation, which is contrary to the previous LAN-to-LAN scenario where the VPNs could both be considered hardware VPNs.



This report has presented a very high-level explanation for the process by which VPNs are implemented. However, a significant amount of information has been provided in terms of the describing what a VPN is and the protocols behind making it a secure way to send information over the Internet or any internetwork. The union of these various VPN topic has provided a more than adequate introduction to the capabilities and benefits of a VPN, as well as what is required to wisely implement such a network.

➢ Definitions

Tunneling – a method of using an internetwork infrastructure to transfer data from one network to another.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Frames (packets) – a grouping of information transmitted as a unit across a network at the Data Link layer of the OSI model.

Datagram – groupings of information that are transmitted as a unit at the Network layer of the OSI model.

- Sources

Network World. "VPN Audio Roundtable Transcript." 12 April 1999
URL: http://www.nwfusion.com/netresources/vpnroundtable.html (01 March 2001).

Microsoft Corporation. "Virtual Private Networking: An Overview." 29 May 1998.
URL: http://msdn.microsoft.com/workshop/server/feature/vpnovw.asp (01 March 2001).

PC Magazine. "The Internet VPN Process." 1997.
URL: http://www.cyplex.com/vpnproc.html (01 March 2001).

Wilson, Matthew D. "VPN How To." December 1999.
URL: http://www.ibiblio.org/mdw/HOWTO/VPN-HOWTO.html#toc1 (01 March 2001).

Packet Magazine Archives. "Virtual Private Networks – Build or Buy? July 1998.
URL: http://www.lsiinc.com/warp/public/784/packet/july98/4.html (01 March 2001).

Melissa Craft, Mark A. Poplar, David V. Watts, and Will Willis, Exam Prep Network+ (Certification Insider Press, 1999), p. 368-384.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.