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

GIAC Security Essentials Certification (GSEC)

Assignment Version 1.4
Option 1

Understanding VPNs - Roles and Responsibilities

© SANS Institute 2000 - 2002, Author retains full rights.

Submitted by:
Thomas M. Santacroce
October 17, 2002

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

INTRODUCTION

Security in the home, at work and at play is a concern we all have. Today's environment has made this need a necessity not a luxury. As individuals we are responsible for our personal security. In a better world our employers are responsible for our physical security. At home paper shredders protect against identity theft. At work it is the responsibility of the Information Technology Staff to secure the Information Systems. Securing the network and remote PCs will support the integrity and confidentiality of the resident data, applications and multitasking operational systems. It will enable the operation system to protect itself from user programs and rogue processes.

This paper will focus primarily on one of many security options available to the IT Security Professional, specifically the Virtual Private Network (VPN). It will address what is a VPN, why is it needed and review some of the security components of a Virtual Private Network.

NETWORK SECURITY ISSUES

In this age of International Corporations with offices/branches, employees, customers and business partners geographically dispersed the corporate employee is no longer restricted to the physical office setting. Remote Access to the corporate information network is a necessity. It provides the user with access to the network resources, up to date information (i.e. financial, competitive, customer), enables those working at home and on the road network access, and can reduce corporate expenses such as networking costs by utilizing the Internet instead of expensive dedicated lines.

Remote access can streamline access to resources and information through Internet and intranet connections and provide a competitive advantage by letting partners, suppliers and customers have closely controlled links. The most common types of remote connectivity methods used are VPNs, dial-up connections, ISDN, cable modems, DSL connections and wireless technologies. 1(Harris,p.462)

The volume of users accessing the Internet via their 'work' PCs has exploded. Whether for professional or personal/recreational reasons this has made Network Owners extremely concerned with security. The telecommuters/road warrior user that access the network remotely is extremely vulnerable to Internet based hackers. The transmission of sensitive information over the Internet or other public line is a major concern of the Business Community. Additional major concerns are the unrestricted access of sensitive data (i.e. financial, competitive etc.), at what level and how it is disseminated. The network is exposed to theft of data, unauthorized access of resources, intrusion of viruses, data corruption, destruction of technology infrastructure and possible financial and legal ramifications.

In response to these and other concerns, IT management teams, vendors etc. developed protocols that would increase the security of information and Network access.

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

For the purpose of this document the term Protocol is defined as a set of rules and formats that enable the proper exchange of information between systems; a standard set of rules that determine how systems will communicate across networks. 2(Harris, pp. 936,344)

In order to secure network architecture the IT security administrator must understand the networking platforms and devices, how the data flows through the network, which protocols work, their purposes, their interactions with other protocols, and how to choose and implement the appropriate types of protocols in a given environment. Terminology such as authentication, encryption, firewalls, routers, servers, switches, tunneling etc. must be part of the Security Administrators vernacular.

THE VIRTUAL PRIVATE NETWORK - VPN

A way to provide and maintain fast secure and reliable communications throughout a company's global network facilities was needed. Intranets and extranets were introduced. The Intranet enables multiple company sites to be interconnected via the Internet. It primarily uses an IP address and provides a degree of safety because they can not be routed on the Internet. The Extranet enables an external party such as a company's partners, suppliers or customers to share common information and resources by extending the bounds of the Network. However, the confidentiality and security of information was still a concern. Now companies are establishing Virtual Private Networks.

A VPN provides its user with a secure method for communication throughout their organization and customer base while ensuring the integrity of the information and controlling the access to it. The introduction of the VPN and its increasing use has enabled fast, secure and reliable direct access to communication and information resources of a corporation. It is an economical alternative to expensive lease lines and can utilize existing IP infrastructures and equipment.

Depending on the article, book, author etc. the definition of the VPN varies. Everyone 'knows or understands' what a VPN is but establishing a definitive definition is difficult at best. A VPN has been defined as:

- A private network that utilizes a public accessible network (usually the Internet) to connect remote or multiple sites together.
- The private connection between two or more computers to transmit private data over a shared or public network.
- A point-to-point networking configuration that offers encryption, tunneling, authentication, and access control.
- Allows any valid remote user to become part of a company's private network utilizing the same network scheme and addressing as users on this network.
- Each Company's private network can also be responsible for validating their own users.

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

The continuing evolution of the VPN technologies, as well as the growing sophistication of the users demands greatly impact the roles and responsibilities of the Data Security Administration/Management.

The user analysis, functional design, development review, system acceptance and implementation of the appropriate technology and its upgrades are critical to the meeting and surpassing of the customers expectations.

The VPN IT/data security administrator must be concerned with

- the general design and functional characteristics of the VPN
- The system acceptability of the users existing framework, structure, hardware software etc.
- The feasibility of the customers existing network accepting the integration of the VPN technology.

Now, many companies are creating their own VPNs to accommodate the needs of remote employees and distant offices. The current technology enables a Company's private Network to securely share information with branch offices, telecommuters, mobile users, home users and business partners. Securing the company's IP structures will protect the integrity, confidentiality and availability/accessibility of the data and applications that are resident on it.

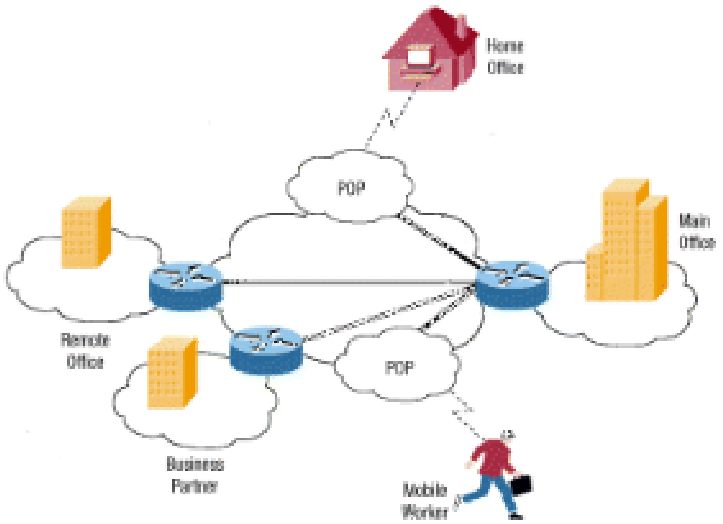


Image courtesy Cisco Systems, Inc.

A typical VPN might have a main LAN at the corporate headquarters of a company, other LANs at remote offices or facilities and individual users connecting from out in the field.

3(Tyson, p.2)

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

The VPN is a 'private' network connection that utilizes a public infrastructure such as the Internet to connect remote sites and users. It provides secure communication between systems across the Internet. It accommodates the needs of multiple and geographically distant offices and remote employees (telecommuters and road warriors).

Virtual Private Networks can be classified into two (2) categories.

- Site-to-Site Access VPNs
- Point-to-Site (Remote Access) VPNs

Site-to-Site Access pertains to both Intranet and Extranet VPNs
Through the use of dedicated equipment and large scale encryption a company can connect multiple fixed sites over a public network. Site-to-Site VPNs can be either Intranet or Extranet based.

Each site must have a complete network containing several nodes or sub-networks. The sites may have different network structures with different client and server applications or may have similar client and server applications.

Intranet VPN
An Intranet VPN is a network with a shared set of services that utilizes Internet- or Web-based user interface/technology. It is used to connect similar groups in geographically dispersed locations. It connects fixed locations such as branch offices and home offices.

If a company has one or more remote locations that they want to connect to a private network they can create the Intranet-based VPN which would connect LAN-to-LAN. For example, Branch offices are connected to their corporate headquarters through tunnels that transport traffic over the Internet.

Extranet VPN
An Extranet VPN is a network with a shared set of services that utilizes Internet- or Web-based user interface/technology. It is used to connect dissimilar groups in geographically dispersed locations. It extends outside the bounds of a company's network. It connects business partners such as suppliers and customers.

If a company has partners, suppliers or customers that they want to connect to their private network they can create the Extranet-based VPN which would connect LAN-to-LAN. The basic premise of the extranet-based VPN is to use the access control and authentication services with a VPN implementation to deny or grant customers/partners access to specific information.

© SANS Institute 2000 - 2002, Author retains full rights.

Point-to-Site (Remote-Access)
As a result of the rapid increase in telecommuting, establishing Point-to-Site VPNs enables the remote user access to data information while preventing unauthorized disclosure. The Point-to-Site (Remote Access) VPN connects the telecommuters, mobile users and small remote offices with minimal traffic to the company's WAN and corporate resources.

This is a user/network-client to LAN connection utilized by a company that has employees who need to connect to that company's private network from various locations. A user would dial into a service provider's point-of-presence (POP), which would establish a tunnel back to headquarters over the providers network or internet. The user would authenticate him/her-self to gain access to the corporate network. The POP is usually a bank of modems and access servers at an ISP location.

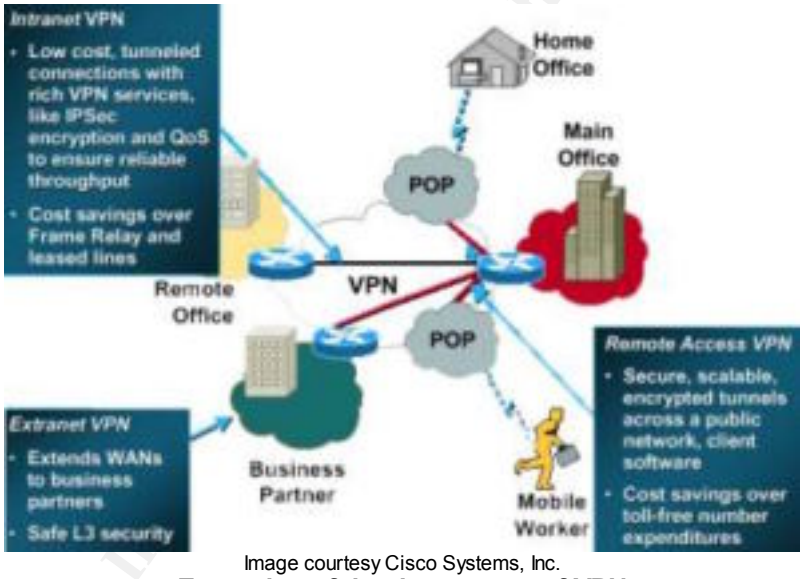


Image courtesy Cisco Systems, Inc.
Examples of the three types of VPN

4(Tyson, p.3)

All VPNs create tunnels (encrypted data communication session) directly between VPN devices across the Internet. This private tunnel establishes the endpoint-to-endpoint connection.

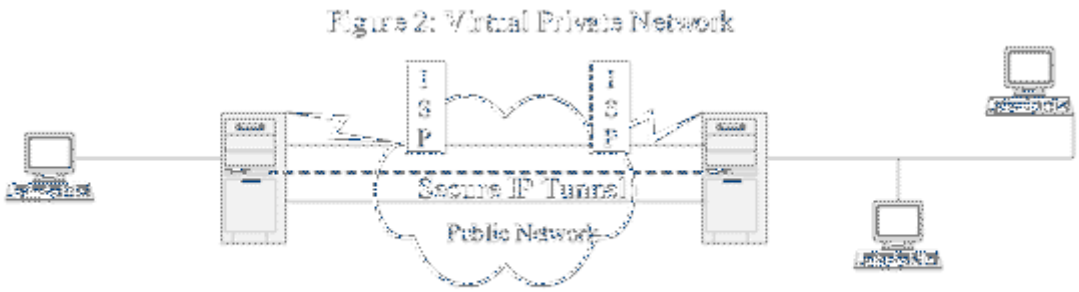
VPN devices can be either software or hardware and may need to be installed on both client (receiver) and server (sender) machines. These devices are used to create the secure/private links between the two machines. A public network, such as the Internet or

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

some other backbone connection, is used as a link to two or more other endpoints. The endpoint can be a LAN device such as a router or can be an end-user workstation. LAN-to-Network/client describes the connection between a LAN device and an end-user workstation. If both endpoints are LAN devices the connection is called LAN-to-LAN. The connectivity between the various endpoints of the VPN connection is established through tunneling.

Tunneling

Tunneling is the primary component to a VPN due to the simple fact that TUNNELING is how the private connection is created.



5(Fraser, p2)

A Tunnel is a virtual path across a public network that enables data packets that are encapsulated and possibly encrypted to be transmitted. Tunnels are designed by using tunneling protocols that hide and encapsulate private network data within the IP packets. It protects the packets against inquisitive eyes by automatically encrypting it before it is sent from one private network to another, encapsulating it into an IP packet and automatically decrypting it at the other end.

Encryption is the transformation of plaintext into unreadable cipher text. The CISSP Certification Exam Guide defines the two types or methods encryption and also encapsulation. These definitions are provided for your information.

> End-to-End Encryption: the technology that encrypts data at its origin is transmitted encrypted and then is decrypted at its destination, versus being decrypted at each and every hop during its travels. 6(Harris, p.931)

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

> Link Encryption: data is encrypted at it origin and decrypted and re-encrypted at each hop during its travel to it destination. Each network communication node or hop must decrypt it to read its address and routing information. 7(Harris, p.560)
>
> Encapsulation: a message is constructed at the application layer and then passed down through the protocol stack. Each layer adds its own information to the message; thus, the message grows in size as it goes down the protocol stack. The message is then sent to the destination computer and the encapsulation is reversed by taking the message apart through the same steps as the source computer that encapsulated it. 8(Harris, p.345)

The connection between the VPN endpoints is established through tunneling. In order to establish this tunnel the endpoints (client & server) must utilize the same tunneling protocol.

The Tunneling Protocols include:

- Point-to-Point Tunneling Protocol - PPTP
- Layer 2 Forwarding - L2F
- Layer 2 Tunneling Protocol - L2TP
- Internet Protocol Security Protocol - IPSec

PPTP, L2F, and L2TP are related to each other by Point-to-Point Protocol (PPP).

Point-to-Point Protocol - PPP
PPP is a dial-up protocol used to connect to the Internet. It is used to establish dial-up connections between routers, user-to-router and user-to-user. It establishes a single point-to-point connection between two computers. PPP transmits data by encapsulating network specific data packets in to the IP packet and transmitting through an IP network such as the Internet. PPP can transport multi-protocols thereby enabling it to transport non-routable protocols like IPX, NetBEUI as well as TCP/IP. PPP can transmit multi-protocols over the same connection at the same time.

Point-to-Point Tunneling Protocol - PPTP
PPTP is an encapsulating protocol based on Point-to-Point Protocol (PPP).
PPTP encapsulates PPP frames in IP datagrams for transmission over an IP capable network. It should be noted that PPTP is supported by the Windows operating systems. PPTP is very flexible in that it can be used in non TCP/IP environments. It uses the standard PPP authentication methods such as PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol) and Extensible Authentication Protocol (EAP).

© SANS Institute 2000 - 2002, Author retains full rights.

Microsoft offers an enhanced version, of the CHAP authentication method for PPTP called MS-CHAP, which provides the ability to use information within the NT domains for security. Microsoft also offers an improved encryption for use with PPTP. It is called Microsoft Point-to-Point Encryption (MPPE).

PPTP offers payload privacy but does not encrypt session control traffic.

Layer 2 Forwarding - L2F
As stated previously L2F and PPTP share certain characteristics. L2F is also designed to work with PPP as well as supporting the non-routable protocols (IPX, NetBEUI etc.).

L2F can support additional authentication standards such as (Terminal Access Controller Access Control System (TACACS+) and Remote Authentication Dial-in User Service (RADIUS). TACACS+ and RADIUS authenticate at the beginning of the transmission. L2F has the capability to work on different networks such as Frame Relay and ATM (Asynchronous Transfer Mode).

L2F does not provide data privacy. Customer traffic travels the network as clear text.

Layer 2 Tunneling Protocol - L2TP
L2F was combined with PPTP which resulted in the Layer 2Tunneling Protocol. L2TP has the same capabilities as L2F and PPTP. It allows multiple connections through one tunnel, works with various types of networks and supports non-routable protocol and uses PPP for dial-in access.

L2TP differs from PPTP/L2F in that it is IPSec compliant. In addition, PPTP is an encryption protocol while L2TP is not. If customers require data confidentiality L2TP would need to be run with IPSec. Combined with IPSec it would provide such security.

Internet Protocol Security Protocol – IPSec
IPSec is primarily used to establish VPNs although it can be used to establish communication between two computers. IPSec protocol provides enhanced security features such as improved encryption, algorithms and more comprehensive authentication that employ public key cryptography. IPSec uses two basic security protocols which are Authentication header (AH) and Encapsulating Security Payload (ESP).

The Authentication Header (AH) is the authenticating protocol which can authenticate the sender of the packet by user or by source IP address. Security is provided by adding authentication information to the IP datagram. It (AH) allows the recipient to confirm the identity of a packet sender and protects against modification.

The Encapsulating Security Payload (ESP) is the authentication and encrypting protocol that uses cryptographic mechanisms to provide authentication, integrity and

© SANS Institute 2000 - 2002, Author retains full rights.

confidentiality to the IP datagrams. It (ESP) encrypts packets by encapsulating a private IP packet inside an outer public IP packet. Another standard/protocol known as ISAKMP can be used for stronger authentication of tunnel endpoints and key management.

IPSec works in two encryption modes Transport Mode and Tunnel Mode.
In the Transport Mode only the payload of each packet is encrypted. It encrypts the actual message so that it can not be accessed/read by unauthorized users. In the Tunnel Mode the payload and the routing and header of each packet are encrypted. It encrypts the actual message as well as protects the header and trailer data so that it can not be accessed/read by unauthorized users.

IPSec is not a strict protocol. The IT Security Administrator has flexibility in terms what type of algorithms, keys and authentication methods to be chosen.

IPSec supports Site-to-Site VPNs by creating security associations between gateways at the edge of customer's networks. A security association (SA) is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely. Each device (that shares the 'secure' tunnel) will have one security association for each session that it uses. When a device receives a data packet, it is the SA that provides the instructions as to what to do with the packet. The SA is the record of configurations, such as the authentication and encryption keys, the previously agreed on algorithms, and source IP address that the device requires to support an IPSec connection. (FYI: The Security Parameter Index (SPI) maintains the SA organized to ensure that the appropriate SA is initiated for the appropriate connection.)

IPSec supports Remote Access VPNs by tunneling from individual host to a security gateway. IP packets sent by an IPSec host to a protected network are encrypted and delivered to the security gateway for that network.

VPNs are based on one or a combination of these tunneling protocols (PPTP, L2F, L2TP, and IPSec). IPSec appears to be considered the standard currently. Corporations requiring stronger encryption and authentication are willing to build an IPSec infrastructure. Some vendors recommend L2TP over IPSec, while others enhance IPSec.

The VPN tunnel protocols ensure the integrity and confidentiality of the data packets while in transit from endpoint to the network and also ensure the authentication of the user(s) logging in.

In order to protect the systems and applications that are connected to a corporate network via the VPN, additional security methods can and should be implemented. These include but are not limited to Firewalls, Intrusion Detection System (IDS) and Anti Virus Software.

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

Firewalls
A Firewall is a device that executes the company's security policy. It provides a strong barrier between the private network and the internet. Firewalls can be set up

- to restrict access to one network segment from another;
- to restrict access into the network from Internet users
- to restrict one internal network segment from accessing another internal segment
- to restrict or filter out packets that do not meet the security requirements

Firewalls are often established as a DMZ (demilitarized zone). A network segment that is located between the protected and unprotected networks. A firewall can be a router, server, authentication server, or hardware device. Firewall-proxy servers control the applications that have network access and hiding protected network information from external or un-trusted devices.

Personal Firewalls should be installed on all remote users' computers and securely configured. They provide packet filtering capabilities as well as blocking TCP and UDP ports.

Intrusion Detection System (IDS)
The installation and its continual upgrading of IDS are critical to the security of the VPN. IDS is a software package tool installed to constantly monitor and detect possible attacks and questionable behaviors that deviate from the norm. IDS can be network-based (monitoring network traffic) or host-based agents (monitoring activities of a specific system)

Anti-Virus Software
A quality anti-virus software package which is configures accurately will ensure that the known virus will be detected and eliminated as much as possible. The software must be automatically updated to ensure it is up to date.

CONCLUSION

The potential for the growth of Virtual Private Networks (VPNs) is apparent due to corporations benefiting from the cost and time saving technologies it provides as well as providing them with a secure method for communication throughout their organization and customer base.

Just as each customer's requirements and capabilities differ, so should those of their VPN. The user analysis, functional design, development review, system acceptance testing and implementation of the appropriate VPN technologies and their continuous upgrading need to be done. The Security Administrator needs to understand the various levels to VPN and Network security. There needs to be standardization as well as the ability to customize components to meet both the customer and Security needs. We need to know our customers' needs and requirement and understanding level.

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

There is a definite need for an increase of the training and education of users to ensure their understanding and acceptance of the VPN as well as the use of any and all upgrades. The user MUST understand their responsibilities for security of information.

© SANS Institute 2000 - 2002, Author retains full rights.

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

BIBLIOGRAPHY

Azzad. MD, Ghauth. MD. GSEC Practical Assignment, V1.2f. "VPN: Another Network Security Solution."
http://www.giac.org/practical/MdAzzad_MdGhauth_GSEC.doc

Covey, Jeremy. GSEC Practical Assignment, V1.2f "Securing Your VPN".
http://www.giac.org/practical/Jeremy_Covey_GSEC.doc

Fraser, Moye. "Understanding Virtual Private Networks VPN"
http://rr.sans.org/encryption/understanding_VPN.php

Gannon, Patrick. "Virtual Private Networks". Predictive Systems. August 2001
http://www.predictive.com/publications/netspectives/netspectives.cfm?article=288&issue=1&number=2

Harris, Shon. CISSP All-in-One Certification Exam Guide. Berkley: McGraw-Hill, 2002,

Moskowitz, Robert. "What is a Virtual Private Network?"
http://www.networkcomputing.com/905/905colmoskowitz.html

Phifer,Lisa, "Virtual Private Networks".
http://www.intranetjournal.com/articles/200009/pvpn.html

Tyson, Jeff. "How Virtual Private Networks Work". How Stuff Works
http://www.howstuffworks.com/vpn.htm

Verton, Dan. "What's a VPN", Computerword. July 15, 2002
http://www.computerworld.com/securitytopics/security/story/0,10801,72657,00.html

"Virtual Private Networks"
http://www.rad.net.id/homes/edward/intranet/intra7

"(VPN) Virtual Private Network FAQs"
http://findvpn.com/articles/faq.cfm

© SANS Institute 2000 - 2002 Author Retains full rights.

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