Table of Contents

CHAPTER 1

Virtual Private Network (VPN)

1.1 Introduction

In this chapter reader will be introduced with term VPN, what does private mean and which benefits can be achieved using this technology. Also this chapter will give answers on questions: why this technology is growing so fast and why is so popular today.

1.2 Why Do People Need a Virtual Private Network?

Since people start to use technology to communicate there has always been a clear division between public and private networks. A public network, like the public communicate system and the Internet, is a large collection of unrelated peers that exchange information more or less freely with each other. The people with access to the public network may or may not have anything in common, and any given person on that network may only communicate with a small fraction of his potential users.

A private network is made of computers owned by a private organization that share data specifically with each other. They're assured that they are going to be the only ones using the network, and that data sent between them will only be seen by others in the group. The typical corporate Local Area Network (LAN) or Wide Area Network (WAN) are some examples of a private network. The line between a private and public network has always been drawn at the gateway router, where a company will erect a firewall to keep intruders from the public network out of their private network, or to keep their own internal users from perusing the public network.

In the past, when companies could allow their LANs to operate as separate, isolated islands. Each branch office might have its own LAN, with its own naming scheme, email system, and even its own favorite network protocol—none of which might be compatible with

other offices setups. As more company resources moved to computers, however, there came a need for these offices to interconnect. This was traditionally done using leased phone lines of varying speeds. By using leased lines, a company can be assured that the connection is always available, and private. Leased phone lines, however, can be expensive. They're typically billed based upon a flat monthly fee, plus mileage expenses. If a company has offices across the country, this cost can be prohibitive.

Private networks also have trouble handling roving users, such as traveling salespeople. If the salesperson doesn't happen to be near one of the corporate computers, he or she has to dial into a corporation's modem long-distance, which is an extremely expensive proposition.**[1]**

1.3 What is VPN?

A VPN is a supplement of an enterprise's private Internet across a public network such as the Internet, creating a secure private connection, essentially through a private tunnel. VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network as shown on figure 1.

It will help the users to understand the concepts discussed in this thesis to summarize and return to the basic concepts that distinguish VPN from other components of a networking infrastructure as well as from mere application security solutions:

- **It is virtual:** This means that the physical infrastructure of the network has to be transparent to any VPN connection. In most cases it also means that the physical network is not owned by the user of a VPN but is a public network shared with many other users. To facilitate the necessary transparency to the upper layers, protocol tunneling techniques are used. To overcome the implications of not owning the physical network, service level agreements with network providers should be established to provide, in the best possible way, the performance and avilability requirements needed by the VPN.

- **It is private:** Private as a term in the VPN context refers to the privacy of the traffic that is to flow over the VPN. As mentioned before, VPN traffic often flows over public networks (hence the confusion with the world 'private') and therefore, precautions must be met to provide the necessary security that is required for any

particular traffic profile that is to flow over a VPN connection. Those security requirements include: data encryption, data origin authentication, secure generation and timely refresh of cryptographic keys needed for encryption and authentication, protection against replay of packets and address spoofing.

- **It is a network:** Even though not physically existent, a VPN must effectively be perceived and treated as an extension to company's network infrastructure. This means that it must be made available to the rest of the network, to all or a specified subset of its devices and applications, by regular means of topology such as routing and addressing.[2]

1.4 What Does a VPN Do?

A virtual private network is a way to simulate a private network over a public network, such as the Internet. It is called "virtual" because it depends on the use of virtual connections that is, temporary connections that have no real physical presence, but consist of packets routed over various machines on the Internet on an ad hoc basis. Secure virtual connections are created between two machines, a machine and a network, or two networks.

Using the Internet for remote access saves a lot of money. It should be done to dial in wherever user Internet service provider (ISP) has a point-of-presence (POP). If an ISP is choosen with nationwide POPs, there's a good chance LAN will be a local phone call away. Some ISPs have expanded internationally as well, or have alliances with ISPs overseas. Even many of the smaller ISPs have tollfree numbers for their roaming users. At the time of this writing, unlimited access dial-up PPP accounts, suitable for business use, are around $25 per month per user in America. At any rate, well-chosen ISP accounts should be cheaper than setting up a modem pool for remote users and paying the longdistance bill for roaming users. Even toll-free access from an ISP is typically cheaper than having your own toll-free number, because ISPs purchase hours in bulk from the long-distance companies.

In many cases, long-haul connections of networks are done with a leased line, a connection to a frame relay network, or ISDN. It has been mentioned the costs of leasing a "high cap" leased line such as a T1. Frame relay lines can also give to user high speeds without the mileage charges. A connection is bought to a frame cloud, which connects user through switches to destination. Unlike a leased line, the amount that is paid is based more on

the bandwidth that's committed to circuit than distance. Frame connections are still somewhat expensive, however. ISDN, like the plain old telephone system, incurs long-distance charges. In many locations, the local telephone company charges per minute even for local calls, which again runs expenses up. For situations where corporate office networks are in separate cities, having each office get a T1, frame relay, or ISDN line to an ISP's local POP would be much cheaper than connecting the two offices using these technologies. A VPN could then be instituted between the routers at the two offices, over the Internet. In addition, a VPN will allow user to consolidate Internet and WAN connections into a single router and single line, saving money on equipment and telecommunications infrastructure.**[1]**

1.5 VPN Benefits

With the explosive growth of the Internet, companies are beginning to wonder that How can they best exploit the Internet for our business? Initially, companies were using the Internet to promote their image, products, and services by providing World Wide Web (WWW) access to corporate Web sites. Today, however, the Internet potential is limitless, and the focus has shifted to e-business, using the global reach of the Internet for easy access to key business applications and data that reside in traditional I/T systems. Companies are looking for the best solution to securely and cost-effectively extend the reach of their applications and data across the world. While Web-enabled applications can be used to achieve this, a virtual private network offers more comprehensive and secure solutions.

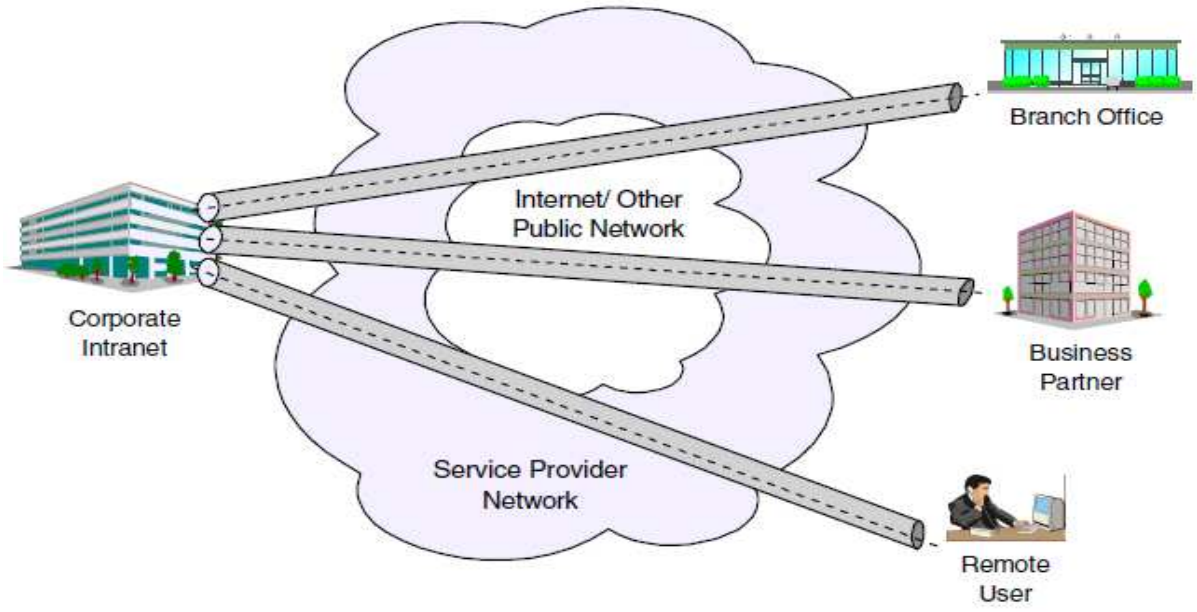

Figure 1: Virtual Private Network (VPN)

VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network, as shown in Figure 1. Internet service providers (ISPs) offer cost-effective access to the Internet (via direct lines or local telephone numbers), enabling companies to eliminate their current, expensive, leased lines, long-distance calls, and toll-free telephone numbers.

A 1997 VPN Research Report, by Infonetics Research, Inc., estimates savings from 20% to 47% of wide area network (WAN) costs by replacing leased lines to remote sites with VPNs. And, for remote access VPNs, savings can be 60% to 80% of corporate remote access dial-up costs. Additionally, Internet access is available worldwide where other connectivity alternatives may not be available.

Although the technology to implement these virtual private networks is just becoming standardized, not all the products in the market support all VPN methods. While some VPN methods can be used in conjunction with each other, some are alternative solutions to each other. A proper VPN solution should be determined according to your needs by taking the following issues into consideration: Business need, Security, Perfomance, Interoperability of the solution with your current systems.

The key to maximizing the value of a VPN is the ability for companies to evolve their VPNs as their business needs change and to easily upgrade to future technology. Vendors who support a broad range of hardware and software VPN products provide the flexibility to meet

these requirements. IPSec-based VPN solutions today run mainly in the IPv4 environment, but it is important that they have the capability of being upgraded to IPv6 to remain interoperable with your business partner's and/or supplier's VPN solutions. Perhaps equally critical is the ability to work with a vendor who understands the issues of deploying a VPN. The implementation of a successful VPN involves more than technology. The vendor's networking experience plays heavily into this equation.**[2]**

1.6 Why Do We Use VPN?

There are two common VPN types:

• **Remote-access** - Also called a virtual private dial-up network (VPDN), this is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations. Typically, a corporation that wishes to set up a large remote-access VPN will outsource to an enterprise service provider (ESP). The ESP sets up a network access server (NAS) and provides the remote users with desktop client software for their computers. The telecommuters can then dial a toll-free number to reach the NAS and use their VPN client software to access the corporate network. A good example of a company that needs a remote-access VPN would be a large firm with hundreds of sales people in the field. Remote-access VPNs permit secure, encrypted_connections between a company's private network and remote users through a third-party service provider.

• **Site-to-site** - Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network such as the Internet. Site-to-site VPNs can be either:

 Intranet-based - If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.

 Extranet-based - When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

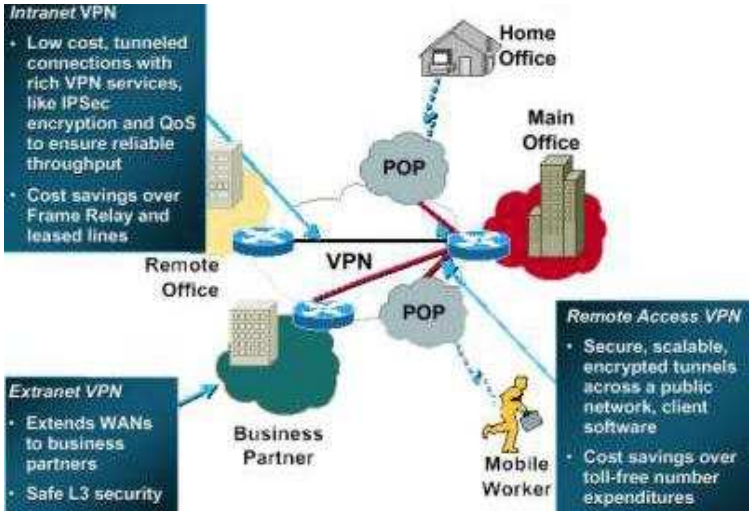

Figure 2: Examples of the three types of VPN

A well-designed VPN can greatly benefit a company. For example, it can: extend geographic connectivity, improve security, reduce operational costs versus traditional WAN, reduce transit time and transportation costs for remote users, improve productivity, simplify network topology, provide global networking opportunities, provide telecommuter support, provide broadband networking compatibility, provide faster ROI (return on investment) than traditional WAN. What features are needed in a well-designed VPN? It should incorporate: security, reliability, scalability, network management, policy management.**[3]**

1.7 Outline

In the first chapter of this thesis it is mentioned about what is VPN?, why and where do peopl use it?, and what is its benefits? In the second chapter, some information about VPN protocols (L2TP, PPTP, L2F, L3TP, IPSec, MPLS, and IP-in-IP), comparing their specialities could be seen. In chapter three there are mentioned about VPN technologies which are firewall, encryption and authentication. In the fourth chapter the security and risks are explained. Some informaiton about basic firewalls, network attacks, and cryptographic assaults which are some of the causes that VPN has to meet in order to provide a high-level security are given in this chapter. And last chapter is about implementing of some VPN designs: small VPN design, medium VPN design, and large VPN design. And also list of references is put at the end of the thesis.

CHAPTER 2

VPN Protocols

2.1 Introduction

In the first chapter, there is mentioned about what VPN is, why people start to use it, and what it does for benefit of people.

In the first part of this chapter there will be mentioned about protocols that allow a layer-2 connection, typically PPP, to be tunneled over another network, typically IP. This sounds like a complicated approach involving a lot of overhead, but several benefits can be derived from this approach which are useful or even invaluable for building VPNs. In fact, the number of Internet VPN scenarios or variations thereof would be quite limited without the use of layer-2 tunneling technique. And then IPSec, a VPN technology that operates on the network layer, and its supporting component, the Internet Key Exchange (IKE) protocol are explained. IPSec protocols require symmetric keys to secure traffic between peers, but IPSec itself does not provide a mechanism for generating and distributing those keys. This is the role that IKE is playing to support IPSec peers by enabling key management for security associations. IKE, as will be seen later, provides security for its own traffic in addition to providing IPSec protocols with the necessary cryptographic keys for authentication and encryption.

2.2 Layer 2 Tunneling Protocol (L2TP)

The Layer 2 Tunneling Protocol (L2TP) is one of the emerging techniques for providing a remote connection to the corporate intranet. The L2TP protocol has been developed merging two different protocols: the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F).

The remote dial-in user scenario is the most common situation for using L2TP. Remote users do not need to make a long-distance call or use a toll-free number to connect directly to the corporate servers but cost constraints suggest the use of ISPs' points of presence (POPs) as

a more cost-effective solution. In this case the dial-in user connects to the nearest POP provided by the ISP and then the session is routed through the ISPs and/or the Internet cloud to reach the corporate LAN access. This environment has more than one point of critical security and reliability issues.

L2TP provides a technique for building a Point-to-Point Protocol (PPP) tunnel connection that, instead of being terminated at the ISP's nearest POP, is extended to the final corporate intranet access gateway. The tunnel can be initiated either by the remote host or by the ISP's gateway access. L2TP provides a reliable way of connecting remote users in a virtual private network that can support multiprotocol traffic, that is, all the network layer protocols supported by the PPP protocol. Moreover, it provides support for any network layer private addressing scheme for the connection over the Internet.

2.2.1 Overview and Standards

L2TP can support remote LAN access using any network layer protocol supported by PPP over the tunnel session, and this is managed by terminating the PPP connection directly in the corporate intranet access gateway.

2.2.2 L2TP Flows

There are a number of steps that occur for L2TP: Establish control connection and tunnel, initiate call, establish L2TP session, and forward PPP packets

Between two devices there may be more than one tunnel and each tunnel must have its own control connection. The control connection can be initiated by either the LSN or LAC.

Within the tunnel there can be many L2TP sessions and each session represents a single PPP stream between the LNS and the LAC. Normally this session is established by the LAC.

2.2.3 Compulsory and Voluntary Tunnel Modes

L2TP supports two types of tunnels, the compulsory model and the voluntary model. They are explained below deeply.

2.2.3.1 L2TP compulsory tunnels

With this model, the L2TP tunnel is established between a LAC, an ISP and an LNS at the corporate network. This requires the cooperation of a service provider that has to support L2TP in the first place and has to determine based upon authentication information whether L2TP should be used for a particular session, and where a tunnel should be directed. However, this approach does not require any changes at the remote client, and it allows for, centralized IP address assignment to a remote client by the corporate network. Also, no Internet access is provided to the remote client other than via a gateway in the corporate network that allows for better security control and accounting.

An L2TP compulsory tunnel is established as follows:

1. The remote user initiates a PPP connection to an ISP.
2. The ISP accepts the connection and the PPP link is established.
3. The ISP now undertakes a partial authentication to learn the user name.
4. ISP-maintained databases map users to services and LNS tunnel endpoints.
5. LAC then initiates an L2TP tunnel to LNS.
6. If LNS accepts the connection, LAC then encapsulates PPP with L2TP and forwards the appropriate tunnel.
7. LNS accepts these frames, strips L2TP, and processes them as normal incoming PPP frames.
8. LNS then uses PPP authentication to validate the user and then assigns the IP address.

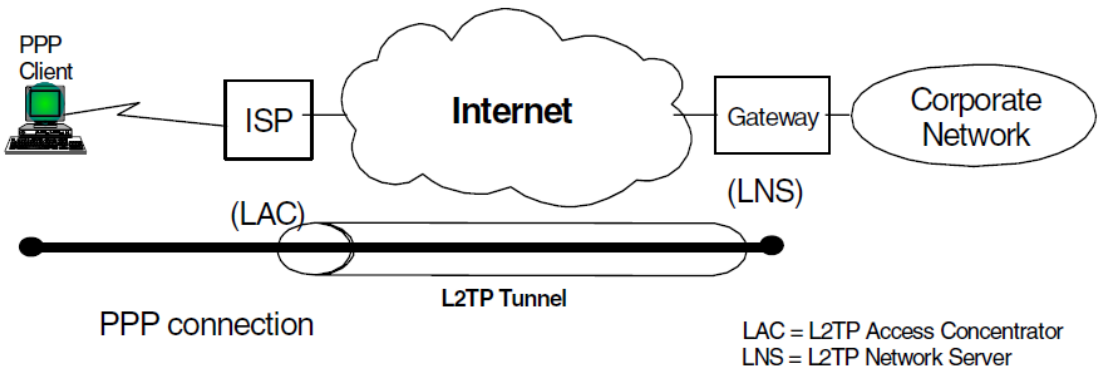

Figure 3: L2TP Compulsory Tunnel Model

2.2.3.2 L2TP voluntary tunnels

With this model, the L2TP tunnel is established between a remote client (which is effectively acting as a LAC) and an LNS at a corporate network. This method is similar to PPTP and is essentially transparent to an ISP but requires L2TP support at the client. This approach allows the remote client to have Internet access as well as one or multiple VPN connections at the same time. However, the client ultimately ends up being assigned multiple IP addresses; one from the ISP for the original PPP connection, and one per L2TP VPN tunnel assigned from a corporate network. This opens the client as well as the corporate networks to potential attacks from the outside, and it requires client applications to determine the correct destinations for their data traffic.

An L2TP voluntary tunnel is established as follows:

1. The remote user has a pre-established connection to an ISP.
2. The L2TP Client (LAC) initiates the L2TP tunnel to LNS.
3. If LNS accepts the connection, LAC then encapsulates PPP and L2TP, and forwards through a tunnel.
4. LNS accepts these frames, strips L2TP, and processes them as normal incoming frames.
5. LNS then uses PPP authentication to validate the user and then assign the IP address.

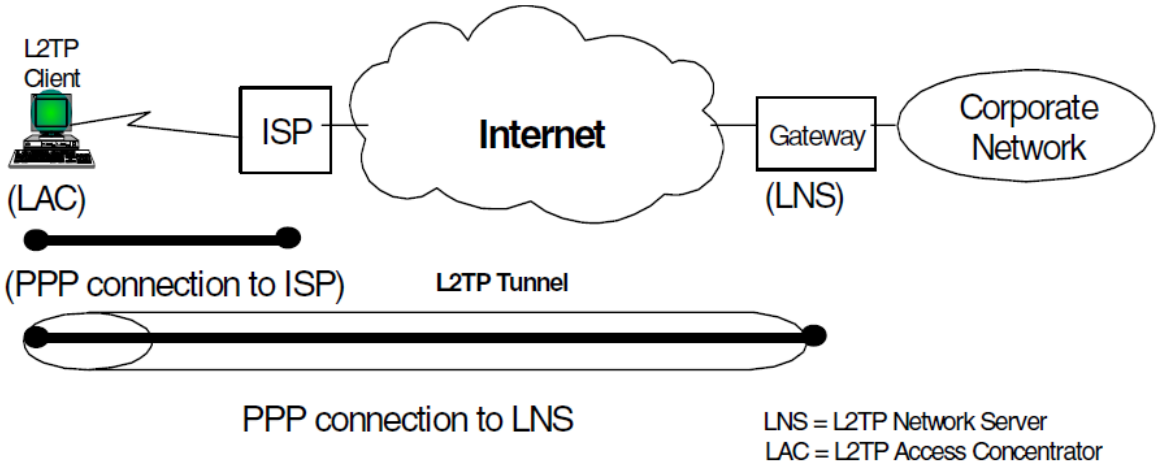

Figure 4: L2TP Voluntary Tunnel Model

2.2.4 Multiprotocol Support

Because L2TP tunnels PPP sessions, any protocol that is supported over PPP can be tunneled by L2TP. Protocols such as SNA, IPX and others are carried as a PPP payload and

therefore transparent to L2TP. This makes L2TP a good choice for connecting corporate networks that require multiprotocol support.

2.2.5 Layer-2 Tunneling Authentication and Encryption

In this section the options for authentication and encryption that are available with the aforementioned layer-2 tunneling protocols are explained.

2.2.5.1 Authentication Options

Authentication is one of the key requirements for VPNs. The following sections discuss some commonly used remote access authentication techniques and highlight their suitability for VPNs.

2.2.5.1.1 Password Authentication Protocol (PAP)

PAP was, and maybe still is, the most common authentication protocol for dial-up connection to ISPs. It authenticates the PPP user before a connection can be established, but it sends the user information and password in the clear which makes it entirely unsuitable to VPNs. PAP also authenticates the user only once, at connection establishment. Once connected, a cracker could potentially take over the connection and would not have to worry about further authentication requirements (even though thay would be easy to meet with PAP if the cracker already listened in on the original authentication exchange).

2.2.5.1.2 Challenge Handshake Protocol (CHAP)

CHAP fixes some of the problems with PAP in that, it requires the user and access server to have a shared secret between them. The server challenges the client for identification upon which the client responds with a hashed value (usually using MD5) of the secret. If that matches at the server where the same hash onthe presumed secret is performed, the client is authenticated. This effectively avoids having to send cleartext passwords over the line. CHAP also provides for multiple authentication challenges by the server during a connection which makes it harder for crackers to take over.

2.2.5.1.3 RADIUS and TACACS

RADIUS and TACACS provide centralized authentication for remote access users. Both technologies work in a similar way: A remote access server implements a RADIUS or

TACACS client that forwards authentication requests to a central server where the request is processed and access granted or denied. That provides great flexibility and scalability over large numbers of access servers which is typically required by ISPs and large corporations. RADIUS and TACACS also allow to pass on configuration information to the client from a central database which is convenient from a management standpoint. RADIUS can optionally be tied into other central authentication systems such as Kerberos, DCE or RACF.

2.2.5.2 Encryption options

Encryption and key exchange are two of the key requirements for VPNs. In the following sections some commonly used remote access encryption techniques and highlight their suitability for VPNs will be discussed.

2.2.5.2.1 Microsoft Point-to-Point Encryption (MPPE)

MPPE uses the MD4 hash created during MS-CHAP authentication "Microsoft CHAP (MS-CHAP)" to derive a secret session key for a PPP connection. This is typically used for PPTP with Microsoft clients. The encryption algorithm used by MPPE is RC4 with 40-bit keys, which is considered very weak by the standard of today's cracking techniques. Microsoft also offers a 128-bit key version for the U.S. market. Microsoft implementations of PPTP refresh a key every 256 packets, though the PPTP standards allow other intervals.

2.2.5.2.2 Encryption Control Protocol (ECP)

ECP can be used to negotiate encryption for a PPP link once the link is established and authenticated. ECP allows for using different encryption algorithms in each direction, but it does not provide key refresh. The standard encryption algorithm defined in the standard is DES, but vendors are free to implement any algorithm they wish.

2.6.2.3 IPSec

IPSec offers encryption with the Encapsulating Security Payload (ESP) protocols and uses the Internet Key Exchange (IKE) protocol for key generation and refresh. ESP provides encryption per packet as long as a session is active and offers a choice of low, medium, strong and very strong encryption algorithms, ranging from 40-bit DES to 192-bit triple DES. IKE authenticates the parties that need to exchange secret information based on strong authentication algorithms and also encrypts the key refresh messages. The keys generated by

IKE are then used by ESP (and also by AH). ESP optionally provides authentication per packetand replay protection. This makes IPSec encryption much more flexible and secure than traditional PPP authentication options, but it incurs a higher processing overhead at the performing devices. IPSec is the recommended security protocol for L2TP and can be used with L2F and theoretically with PPTP as well. For more information on IPSec AH and ESP.

2.3 Point-to-Point Tunneling Protocol (PPTP)

One of the more "established" techniques for remote connection is the Point-to-Point Tunneling Protocol (PPTP). PPTP is a vendor solution that meets the requirements for a VPN.

PPTP is an extension of the basic PPP protocol (see Figure 5). It is due to this fact that PPTP does not support multipoint connections, connections must be point-to-point.

PPTP does not change the PPP protocol. PPTP only defines a new way, a tunneled way, of transporting PPP traffic.

PPTP is currently being replaced by implementations of L2TP. However, some vendors are still developing solutions with PPTP.

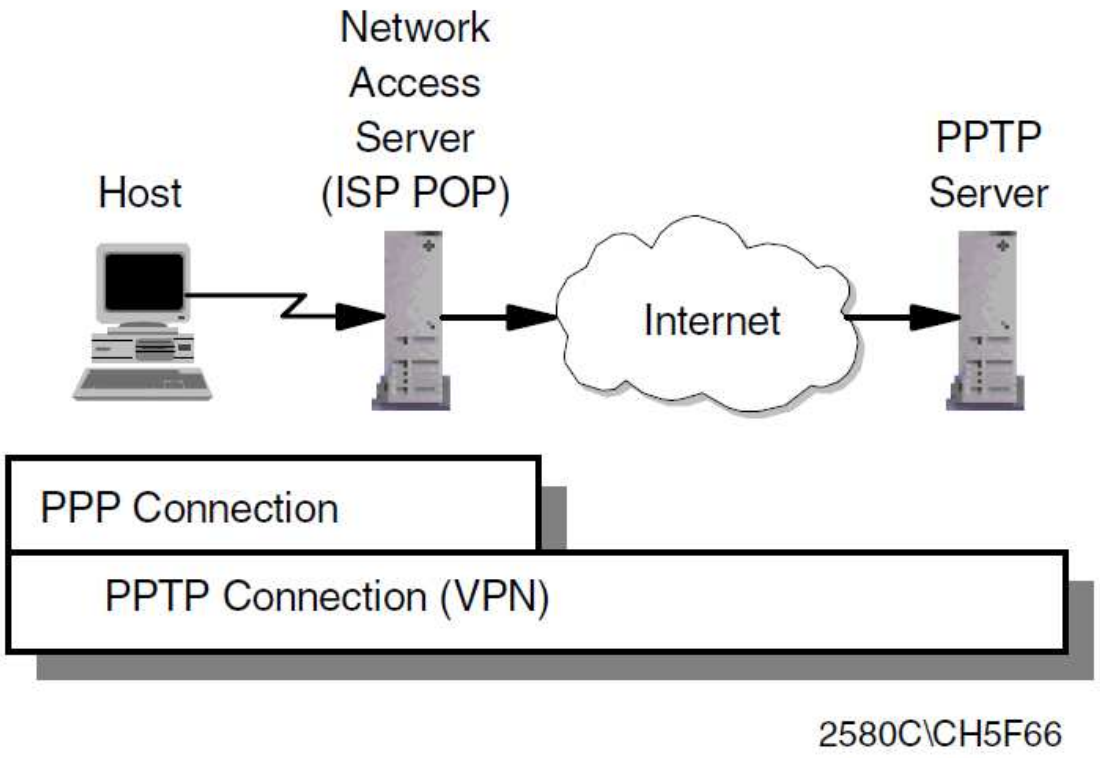

Figure 5: PPTP System Overview

2.4 Layer 2 Forwarding (L2F)

Layer 2 Forwarding (L2F) was developed by Cisco Systems at the same time that PPTP was being developed. It is another protocol that enables remote hosts to access an organization's intranet through public infrastructure, with security and manageability maintained.

As with PPTP, L2F enables secure private network access through public infrastructure by building a "tunnel" through the public network between the client and the host. The difference between PPTP and L2F is that L2F tunneling is not dependent on IP; it is able to work with other network protocols natively, such as frame relay, ATM or FDDI. The service requires only local dial-up capability, reducing user costs and providing the same level of security found in private networks.

An L2F tunnel supports more than one connection, a limitation of PPTP. L2F is able to do this as it defines connections within the tunnel. This is especially useful in situations where more than one user is located at a remote site, only one dial-up connection is required. Alternatively, if tunneling is used only between the POP and the gateway to the internal network, fewer connections are required from the ISP, reducing costs.

L2F uses PPP for client authentication, as does PPTP, however, L2F also supports TACACS+ and RADIUS for authentication. L2F authentication comprises two levels, first when the remote user connects to the ISP's POP, and then when the connection is made to the organization's intranet gateway.

L2F passes packets through the virtual tunnel between endpoints of a point-to-point connection. L2F does this at the protocol level. A frame from the remote host is received at the POP; the linked framing/transparency bytes are removed. The frame is then encapsulated in L2F and forwarded over the appropriate tunnel. The organization's gateway accepts the L2F frame, removes the L2F encapsulation, and processes the incoming frame. Because L2F is a layer-2 protocol, it can be used for protocols other than IP, such as IPX and NetBEUI.

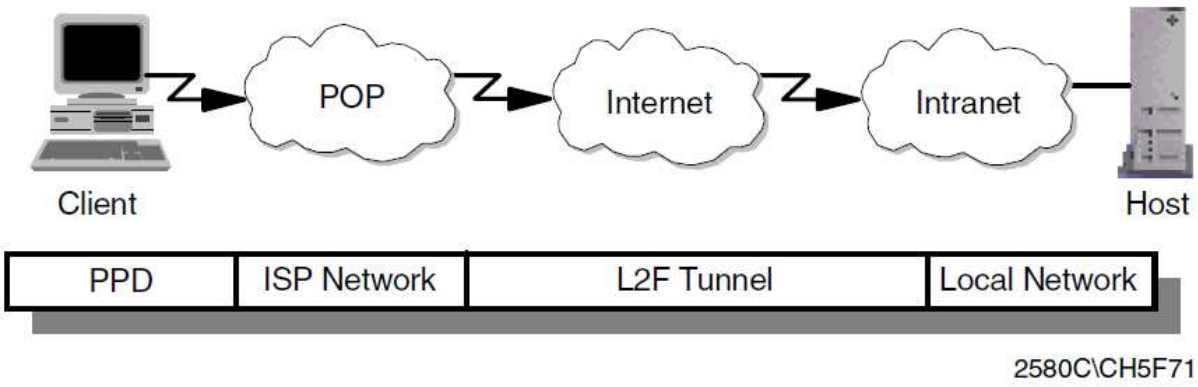

Figure 6: L2F Tunnel from POP to Intranet Gateway

With L2F, a complete end-to-end secure VPN can be created and used. It is a reliable and scalable solution. However, it has shortcomings that are addressed with L2TP.

2.4.1 Comparing Remote Access Tunneling Protocols

The following table provides a quick comparison of the three predominant remote access tunneling protocols, L2TP, PPTP and L2F:

Table 1. Comparing Remote Access Tunneling Protocols

Feature	PPTP	L2F	L2TP
Standard/Status	RFC 2637 (informational)	RFC 2341 (informational)	RFC 2661 (standards track)
Carrier	IP/GRE	IP/UDP, FR, ATM	IP/UDP, FR, ATM

Feature	PPTP	L2F	L2TP
Private address assignments	Yes	Yes	Yes
Multiprotocol support	Yes	Yes	Yes
Call types	Incoming and outgoing	Incoming	Incoming and outgoing
Control protocol	Control over TCP Port 1723	Control over UDP Port 1701	Control over UDP Port 1701
Encryption	Microsoft PPP encryption (MPPE)	PPP encryption (MPPE); IPSec optional	PPP encryption (MPPE/ECP); IPSec optional
Authentication	PPP authentication (user)	PPP authentication (user); IPSec optional (packet)	PPP authentication (user); IPSec optional (packet)
Tunnel modes	Typically voluntary tunneling model	Compulsory tunneling model	Compulsory and voluntary models
Multiple calls per tunnel	No	Yes	Yes
PPP multilink support	No	Yes	Yes

2.5 Layer-3 VPN Protocols

In this section IPSec, a VPN technology that operates on the network layer, and its supporting component, the Internet Key Exchange (IKE) protocol are discussed. Even though IPSec is the architecture that implements layer-3 security and IKE uses an application running at or above layer-5, there is an inherent relationship between the two. IPSec protocols require symmetric keys to secure traffic between peers, but IPSec itself does not provide a mechanism for generating and distributing those keys. This is the role that IKE is playing to support IPSec peers by enabling key management for security associations. IKE, as will be seen later, provides security for its own traffic in addition to providing IPSec protocols with the necessary cryptographic keys for authentication and encryption.

2.6 IP Security Architecture (IPSec)

In this section, a brief overview of the Security Architecture for the Internet Protocol (IPSec) is provided. This section presents a valuable addition to this redbook because it is based on the latest Internet standards.

2.6.1 Overview and Standards

The IP Security Architecture (IPSec) provides a framework for security at the IP layer for both IPv4 and IPv6. By providing security at this layer, higher layer transport protocols and applications can use IPSec protection without the need of being changed. This has turned out to be a major advantage in designing modern networks and has made IPSec one of the most, if not the most attractive technologies to provide IP network security.

IPSec is an open, standards-based security architecture that offers the following features:

• Provides authentication, encryption, data integrity and replay protection
• Provides secure creation and automatic refresh of cryptographic keys
• Uses strong cryptographic algorithms to provide security
• Provides certificate-based authentication
• Accommodation of future cryptographic algorithms and key exchange protocols
• Provides security for L2TP and PPTP remote access tunneling protocols

IPSec was designed for interoperability. When correctly implemented, it does not affect networks and hosts that do not support it. IPSec uses state-of-the-art cryptographic algorithms. The specific implementation of an algorithm for use by an IPSec protocol is often called a transform. For example, the DES algorithm used in ESP is called the ESP DES-CBC transform. The transforms, as the protocols, are published in RFCs and in Internet drafts.

2.6.2 IP Authentication Header (AH)

AH provides origin authentication for a whole IP datagram and is an effective measure against IP spoofing and session hijacking attacks. AH has the following features:

• Provides data integrity and replay protection
• Uses hashed message authentication codes (HMAC), based on shared secrets
• Cryptographically strong but economical on CPU load

• Datagram content is not encrypted

• Does not use changeable IP header fields to compute integrity check value (ICV), which are:

• TOS, Flags, Fragment Offset, TTL, Checksum

AH adds approximately 24 bytes per packet that can be a consideration for throughput calculation, fragmentation, and path MTU discovery. AH is illustrated in Figure 12 **[2]**

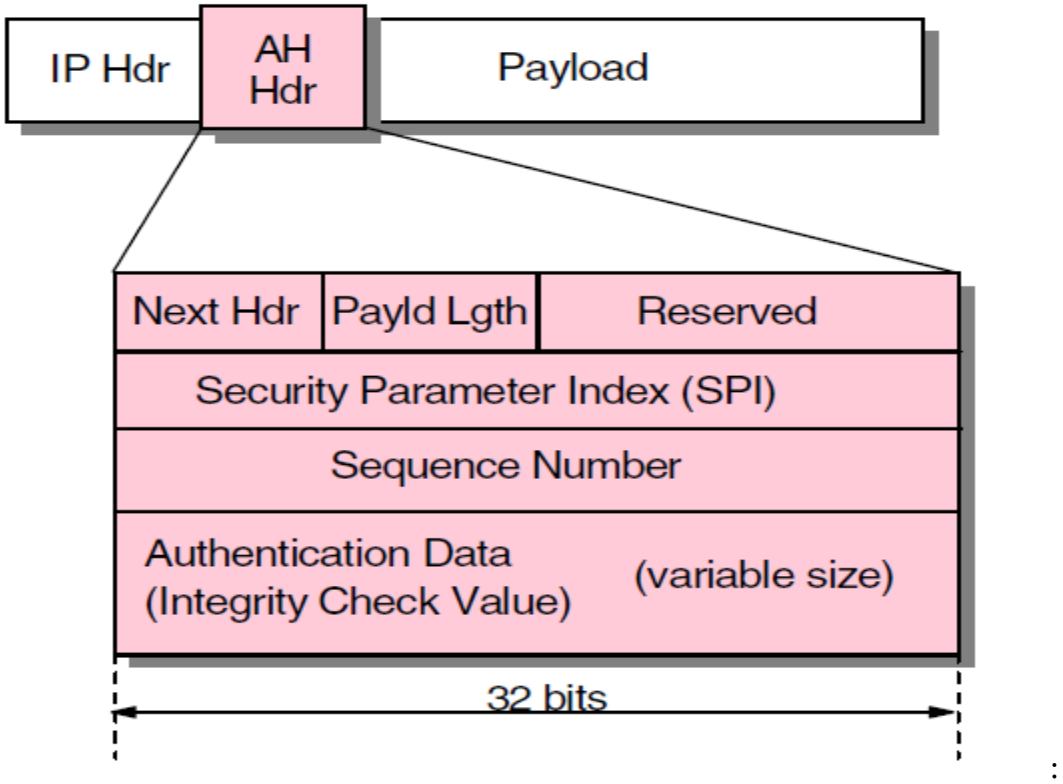

Figure 7: IPSec Authentication Header (AH)

2.7 MPLS

Multiprotocol Label Switching (MPLS) is a way of tunneling IP datagrams, usually within and among autonomous systems.

Actually, MPLS can be used to tunnel any type of network-layer packetthus, multiprotocol. Because tunnels in the Internet are concerned, and MPLS's use with IP.

The idea is that a small label is inserted between the interface- and network-layer protocol headers, as shown in figure, by the router at the entrance to the tunnel. Downstream routers use the label to make routing decisions, and do not need to consult the network-layer header at all. Thus, like all tunnels, MPLS treats the encapsulated IP datagram as opaque data and does not access it in any way while it's in the tunnel.

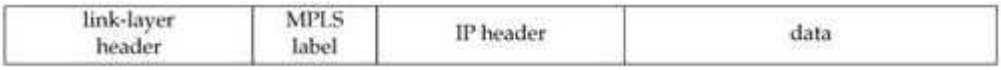

Figure 8: MPLS Label Encapsulation

MPLS was originally envisioned as a way to perform network-layer routing at the interface layerthat is, at ATM or frame relayspeeds. MPLS is now perceived as a means of providing traffic engineering, including quality of service; ATM-like virtual circuits at the network layer; interface-layer tunnels, such as Ethernet over IP/MPLS; a special type of VPN for enterprises that provides security comparable to that obtained with frame relay or ATM circuits; and a generally simplified network architecture where, for example, many ATM control plane functions are migrated to the network layer.

After looking briefly at how MPLS tunnels work, it then be seen how they can be used to provide a type of VPN. Because MPLS is usually implemented at the network service providerthat is, the autonomous systemlevel, most of us will not come into direct contact with it, but it does provide an interesting example of tunneling and is well worth our study.

2.8 IP-in-IP

In this tunnel, IP diagrams are encapsulated in IP datagrams, as shown in the figure.

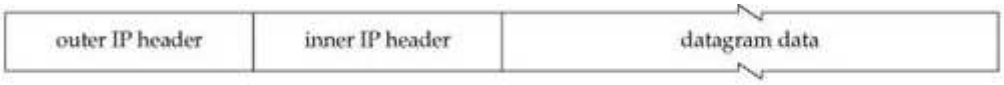

Figure 9: IP-in-IP Encapsulation

The outer IP header will have a kind of protocol field, indicating that its payload is another IP datagram. The inner IP header will have a protocol field indicating the protocol that it is carrying.

IP-in-IP tunnels may not be clear, so we consider a common example. Suppose that there are two geographically separated networks with RFC 1918 (private) addresses and it can be made the two networks appear as a single large network. For specificity, the hosts in the first network have addresses in the 10.0.1.110.0.1.126 range and that the hosts in the second network have addresses in the 10.0.1.12910.0.1.254 range. If the two networks should appear as a single large network, it means that the host at 10.0.1.1 should be able to send a datagram directly to 10.0.1.129. That is, the IP datagram will have a source address of 10.0.1.1 and a destination address of 10.0.1.129.

Note that this problem can not be solved with NAT, because the destination address is nonroutable. NAT can still adjust the source address, of course, but it can not compensate for the nonroutable destination address.

The solution to this problem is shown in figure, where the two networks are connected by an IP-in-IP tunnel. The two gateway routers in the figure (GW_1 and GW_2) are called the tunnel endpoints. As shown in the figure, the physical addresses of the tunnel are 96.29.5.1 and 96.29.5.2. The logical endpoints are 10.0.1.126 and 10.0.1.254. Hosts on the left network have an entry in their routing table that specifies GW_1 as the next hop for traffic addressed to the 10.0.1.128/25 network. Hosts on the right network have a similar entry in their routing table specifying GW_2 as the next hop for the 10.0.1.0/25 network.

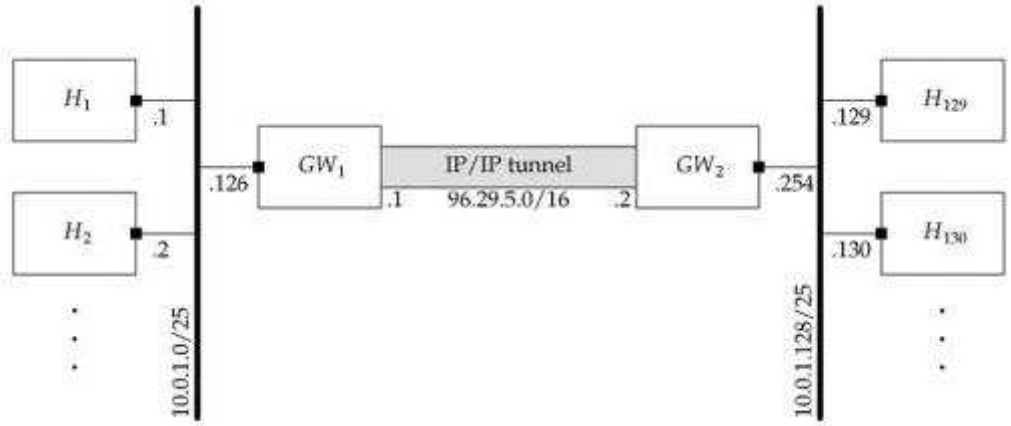

Figure 10: An IP-in-IP Tunnel

When host H_1 (10.0.1.1) wants to send a datagram to H_{129} (10.0.1.129), it first sends it to GW_1 because of the entry in the routing tablefrom which it is sent through the tunnel to GW_2. When the encapsulated datagram reaches GW_2, the outer IP header is stripped off, and the inner datagram is delivered to H_{129}. Figure shows this sequence of events for a ping packet sent from H_1 to H_{129}.**[4]**

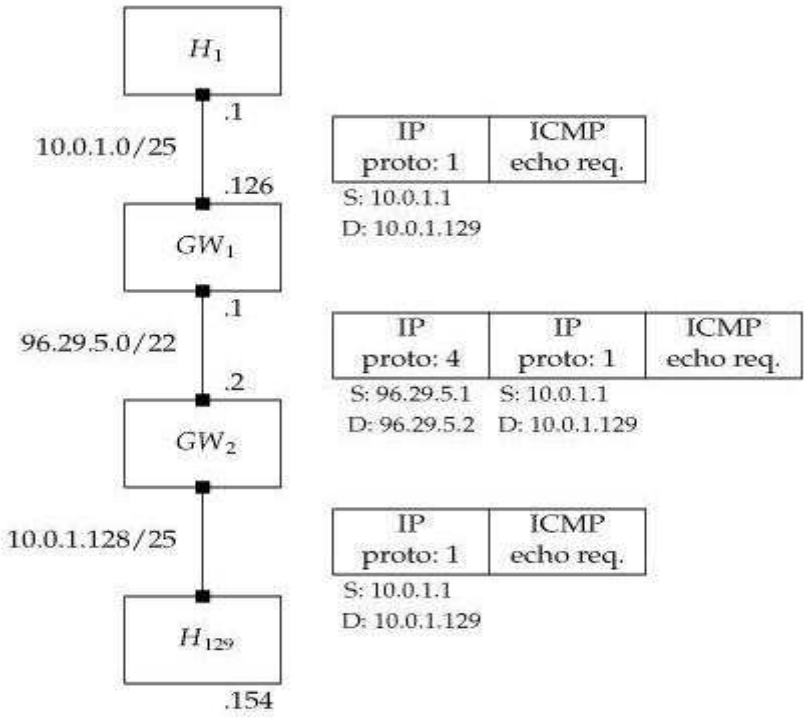

Figure 11: Packet flow from H_1 to H_{129}

2.9 Conclusion

One major difference between protocols of VPN is the service that is provided to the VPN user. Layer 2 solutions are in some ways more flexible particularly in terms of the higher layer protocols used in the VPN. Layer 3 VPNs can have advantages in terms of management. PPTP is an technique that for remote connections. L2F is a devoloping protocol of PPTP. L2F can make more than one connection, a limitation of PPTP. MPLS is usefull mainly within an autunomous system, however it can be used across autonomous system if their directors agree and coordinate labels. And IPSec enables a framework for security at the IP layer for both IPv4 and IPv6.

CHAPTER 3

VPN Technologies

3.1 Introduction

In the previous chapter, there are mentioned about VPN protocols and some security ways for these protocols such as encryption and authentication.

In this chapter there will be presented an overview and background of the technologies which be used to build a VPN and how they are incorporated into the products and services covered in this dissertation. Firstly, it is a discussion of how firewall techniques are used to protect an entire network at it gateways routers. Then, it is presented you a general information on encryption: how it is used in a traditional sense, and how it will be deployed using the VPN. After that, authentication techniques are explained and how they are used in conjuction with the encryption algorithms with VPNs.

3.2 What is a Firewall?

Probably the most powerfull country on data sensitivity (The U.S. Department of Defense) and security controls, used a system of confidences defined as security levels to restrict access to classified docements. The criteria for determining how a governmental computer should be protected were detailed in the fabled "Orange Book." It stated that to secure highly sensitive data, one must never connect the computer to an exterior network. This is of course the best firewall strategy that exists, but it is too restrictive to be practical. As known, the value of interconnection; people should be realized that the best firewall for extremely sensitive materials is to isolate them on a computer without a network connection at all.

Firewalls usually serve two main functions for a network administrator. The first is to control which machines an outsider can see and the services on those machines with which he or she can converse. The second controls what machines on the Internet an internal user can

see, as well as what services he or she can use. A firewall is much like a traffic cop, organizing which paths network traffic can take, and stopping some altogether. Internet firewalls usually do this by inspecting every packet that tranverses the gateway router, which is why they are usually referred to as "packet filtration" systems.

3.2.1 Firewall Deployment

The first of the security-related technologies that it is covered in this dissertation is the firewall. A firewall is a system which stands between your internal network and the world outside. Firewalls have been employed on large public networks for many years and are a great starting place in the development of a security strategy. The reason to start with firewalls is that they are generally placed at the point at which your network interconnects with a public network, like the Internet. Maybe it is not a perfect strategy, a firewall is easy to configure, that it requires only the modification of one gateway router. Of course, if you have a large, multiplyconnected WAN, with many paths to the Internet, then it should be noted that you will need to create a firewall for each interconnection point. The complexity of this process increases dramatically from the single point gateway to the multiple point gateway.

3.2.2 What Types of Firewalls Are There?

Since almost all firewalling techniques are designed around a similar model, a centralized point of control, there are only a few variations at the top level that need to be explored. Most people who are interested in VPN are probably already familiar with the packet filtration firewall, given the recent attention paid to it by the news media. In this section the operation and configuration of four architectures of firewall design will be explained. There are many variations of the four that you may have seen implemented, and several of the most complex and advanced architectures will be omitted. However, people who read this thesis can understand easily what a firewall is, how it works, how to set one up, and, most relevant to this book, how it fits into the world of the virtual private network.

3.2.2.1 Packet restriction or packet filtering routers

Routers and computers that conduct packet filtration choose to send traffic to a network based on a predefined table of rules. The router can not make decisions based on what is included in the packet's payload, but rather on where it is coming from and where it is

destined. It only considers that if the packet matches a set of parameters, it should take appropriate action to either allow or deny the transit. These allow and deny tables are set up to conform to theoverall network security policies put in place by the network administrator or security coordinator.

Packet filtering can take on two basic forms. First is an open network with selective filtering of traffic that is unwanted. For each type of network attack, an appropriate filter must be put in place on the router. Second is the closed network with selective filtering of desired traffic. Although affording greater security, even for those attacks that haven't been thought of yet, the drawback for the network administrator is having to update the firewall as new computers or services are added or changed.

Further, to be glad for performance reasons that the router does not actually open all the packets it gets. Routers these days are asked to perform miracles, especially with the race for more and more bandwidth. The job of the routers is to decide where to send the traffic, not really to catch and throw away packets that are security risks.

Probably, there will be a huge market change in what gateway networks will be look like in the future, and there will be a decoupling of routing equipment and packet filtration in the very near term. Actually, that may already be the case by some companies. New products are already coming out that support dynamic authentication through a packet filtering router directly to the user level, even across an encrypted link.

A last impediment is that frequent changes to the network may require wholesale reconfiguration of the gateway router and the packet filtration firewall that lives on it. This can be time-consuming and disaster-prone if either an uncaught mistake leaves most of the network wide open, or a subtle change leaves the router crippled and unable to perform its first duty as a network traffic director.

3.2.2.2 Proxy servers

Proxies act much like bastion hosts, and in some firewall texts, the two overlap almost completely. The term "bastion host" is used to refer to a computer that acts as a staging area for information that is in transit either to or from the Internet. The term "proxy server" is used to refer to a type of bastion host that is running specialized software that masquerades as an internal machine to an external one. In the following example, a typical bastion host and typical proxy server are contrasted.

A good illustration of an application for a bastion host is email. A bastion host is typically set up to act as the "delivery point" for email inbound from the Internet. Hence a DNS mailexchanger record (MX) is traditionally set up to point traffic to the bastion for delivery. From there, the bastion may re-deliver the mail to an interior mail host (which it can see due to its position in the firewall), or it could hold onto the mail, waiting for the client to read it with a POP mail client. A whole selection of different firewalls can be constructed in this manner.

By contrast, a proxy service is more of an "in-transit" checkpoint than an information staging area. The proxy pretends to be one end of a connection, but protects the true sender or recipient from traffic which is unwanted. The service that presents the biggest trouble to a security manager's life is the standard file transfer protocol (FTP). It's insecure because it uses random, high-numbered ports to establish a peer-to-peer session with the client.

3.2.3 Use of Firewalling in a VPN

The importance of firewalling to a virtual private network(VPN) is straightforward and to the point. Since a VPN is an interconnection of two or more disconnected networks utilizing public resources (such as the Internet) for transit, it follows that these networks individually must be protected in and of themselves. Imagine that each network need to be placed in a VPN as a separate bubble, with its own connections and users.

Viewed this way, each separate bubble needs a protective wall around it to make it safe from invasion. The concept behind using firewalls with a VPN is to secure the networks as if they were isolated; then the system administrator opens specific ports in the packet filtering router to allow the encrypted data to stream from one bubble to the next. Thus, a private and secure communication (based on the type and implementation of the cryptographic routines used) is set up in a channel between two sites. The VPN software provides the security and the application layer routing, so that

Firewall techniques are the first line of protection in the fabric of a VPN, so they must be developed and tested before the benefits of the VPN can be fully harvested. Even if the VPN software or hardware you deploy has built-in firewalling that seems to be everything you would ever need, chances are that you will need to follow some security guidelines on your network anyway, just to stay on the safe side.

3.3 Encryption and Authentication

The configuration and deployment of a VPN is more than a packet filtration router. The real concept of a VPN, is the secure communication between two distinct networks over a public medium, done in such a way that they seem to be sharing a LAN from either end. Firewalls either allow or deny traffic based on the source and destination, but once the traffic makes it into your network, the disciplines of authentication and encryption add further protection by securing the conversation.

Encryption can be regarded as a method for altering data into a form that is unusable by anyone other than the intended recipient, who has the means necessary to decrypt it. The input to an encryption algorithm is typically called clear text, while the output is referred to as ciphertext or crypt text. The encryption process protects the data by making the assailant work too hard or too long to get at what's being hidden. As we will discover, cryptographic routines use mathematics to alter the data in such a way that the process is difficult and expensive to reverse.

In this section cryptography that is the art and science of authentication will be mentioned. Where encryption and cryptography deal with the conversion of data into a protected form for transmission to a trusted party in a hostile environment, authentication is the identity checking and confirmation of that entity, which guarantees their claim with a great degree of certainty. The notion of authentication is very important to the concepts employed by creating a VPN. If certainty the identity of a participant is not known, there also can not be entrusted a data communication channel to them. It would be like inviting them over to client office and giving them the keys to the filing cabinet and access to a photocopier.

3.3.1 A Brief History of Cryptography

A major tenet of the art and science of cryptography is that the transformation process must be a fairly quick one for the owner of the data (the encryptor) yet computationally difficult (if intercepted) for a hostile third party to reverse. Hence, most algorithms that morph data for security purposes do so in a way that is programmatically complex. In this section, the world of ciphers from about five thousand feet up will be explored. There will be covered some of the nastier mathematics that make encryption work, but the purpose is to do so in a fashion that will not leave people wanting a degree in higher math.

There are three basic categories of algorithms:

The first category of algorithms uses a one-way transformation process to alter the clear text into ciphertext. These transformation programs are typically referred to as hash algorithms. The value of hashes and message digests is that they are easy to compute but hard to reverse, and rarely repeat. Hashes do not normally have keys associated with them, as do the next two types of encryption techniques.

The second and third types of encryption algorithms are the private key and public key cryptosystems. There are other common names for these encryption procedures, including asymmetric and symmetric algorithms, or one-key and two-key systems. All these terms refer to the same processes. The hash algorithms briefly discussed in the previous paragraph are sometimes referred to as no-key or zero-key encryption operations because, as the name would suggest, hash algorithms do not use a key.

To produce a "cryptographically strong key" on the fly, a computer must have access to a good pool of random numbers. Using something seemingly random, like transformations based on clock time, seconds past a certain fixed date, or other easily obtainable environmental conditions, proves to be an inadequate solution. If the attacker knows that the key generator uses the time of day for the key, it is highly likely that a constrained brute force approach could be used to help narrow the scope of the problem to one that is not computationally infeasible.

3.3.2 Cryptography in Network Communications

Protecting a network conversation is almost as fundamental as having one. The protection part comes from the need to send data over an unknown public network. This is commonly referred to as the "transmission over an insecure channel" problem, and is almost always solved by one of two methods.

The one of the solution that the easiest one is to make the channel secure by privatizing the medium. If you make sure that third parties do not have access to the physical line, snooping becomes extraordinarily difficult, so the connection is solid. As usual, this is not always the best approach, for several reasons. It is expensive to secure an entire media delivery system, which may be unfeasible as well as impractical to alter in a timely fashion, not to mention that sometimes it is impossible to secure a delivery system to a user's complete satisfaction.

This is exactly the reason why the VPN will be deployed on a large scale in the coming years. Since the solution is not to privatize an existing delivery system, it must be to secure the data itself on the insecure channel. That means that make it accessible for everyone, but transform it in a way (using cryptography) that only an affiliate can undo it.

3.3.3 Use of Cryptography and Authentication in a VPN

As with all secure communications, all protection systems have three important functions in common. Secure communications first protects the data in transit so that hostile or curious third parties in the middle are not able to intercept and read the transmission (this is the concept of encryption).

Second, both parties must know with confidence that they are speaking to one another. In other words, A girl is certain she is speaking with a boy, and vice versa, even though they can not see each other (this is the idea of authentication).

Lastly, both girl and boy need to be able to detect if any third party is trying to tamper with the messages, either with a destructive goal (like the insertion of many messages to prevent girl from reaching boy) or even a benign one (like infrequently inserting garbage to test a hypothesis). This is the concept of message integrity, and is sometimes referred to as a message digest.**[1]**

3.4 Conclusion

In this chapter are considered security questions in VPN, because it is imposible to create VPN without giving an important attention to security of data transmitted in VPN tunnels. With well configured firewall, which represents central point of security system, security issues can be avoided. In tunnels transmitted data are used by encryption and authentication to protect the private information from the attackers. Three basic of algorithms are explained in this chapter from the weakest one to the strongest one.

CHAPTER 4

Security and Risks in VPN

4.1 Introduction

In the previous chapter, there are mentioned about some VPN technologies. Firewall is described, and encryption and authantication are explained.

In this chapter security and risks in VPN will be explained by connecting to the previous chapter. VPN is a kind of technology that is based on an independent public network infrastructure like Internet. The public network is used on it to transmit data across to the other users, probably, safe in transit. However, the safety of data in transit over the Internet can not be guarranteed because of its clearly used public network infrastructure. Data over the Internet is uncontrollably defenceless and the technologies used to promote security issues are untrustworthy. So, someone can steal easily someone else's credit card number, curious into other private ducuments or gaining access to restricted machines over the Internet. These are just a few examples to verify the vulnerability of data in transit over the web. Also there are many other known and unknown loopholes in this technology that the user may not even be aware of.

Some of the causes that VPN has to meet in order to provide a high-level security are to protect against basic firewalls, network attacks and cryptographic assaults from the hackers. They are described in the following sentences.

4.1.1 Basic Firewalls

Firewalls are one of the key components to provide security in VPN. It scans restricted IP addresses or port requests and discards those who try to login with your password. When some of networks are connected over the public network, using of firewalls sounds more acceptable and safe. However, not all the services offered in a firewalled network can be trusted. There are methods to go into firewalled network and access information readily.

Especially in VPN, the sole use of firewalls do not do good to protect connections in a public area. Other mechanisms must be implemented for a higher level of security. With the use of basic firewalls, it only opens a hole in security of VPN technology. Firewall attacks are common among the attackers who want to access the services that a firewall blocks and the machines they are restricted into.

4.1.2 Network Attacks

The thieves do not prefer to use network attacks aggaints opponents or competitors to either destroy their critical data or steal their usefull information. These attacks usually happen in the Internet. Since VPN is a based on the Internet platform, these attacks must be taken care of in the security of VPN technology. Hackers wisely try many forms of such attacks for an aim. Some of them are deny of service attacks, address creeping, session hijacking, man-in-the-middle attack, replay attack, and detection and clean up.

4.1.3 Cryptographic Assaults

Cryptographic assaults are difficult to break into and require a greater depth of understanding of crypto systems. It is usually the code breakers or cryptanalysts who are the experts in breaking crypto systems. It consumes longer hours and requires an in-depth knowledge of advanced mathematics. Some of the common cryptographic attacks are ciphertext-only attack, known plaintext attack, chosen plaintext attack, chosen ciphertext attack, brute force attack, password guessers and dictionary attacks and social engineering.**[4]**

4.2 Common VPN Flaws

The VPN users can use some ways to protect their network:

4.2.1 Insecure Storage of Authentication Credentials by VPN Clients

Many VPN client programs offer to store some or all of the authentication credentials (e.g. username and password), and for some clients, this is the default setting. While this makes the VPN easier to use it also introduces security risks, especially if the credentials are not well protected.

The common client issues that have been seen are:

• Storing the username unencrypted in a file or the registry:

Anyone with access to the client computer can obtain the username. If the VPN is using IKE Aggressive Mode, then knowledge of the username allows an offline cracking attack against the password.

• Storing the password in a scrambled form:

This is often referred to as “encryption”, but it is really obfuscation rather than encryption because there is no unique key needed to decrypt it. If the obfuscation algorithm becomes known, then it is a simple matter to obtain the password if you have access to the client computer.

• Storing the plain-text password in memory:

If storing an obfuscated version of the password in a file or registry is not bad enough, many clients decrypt this when they start up, and store a plaintext version of the password in memory. In this case, anyone with access to the client computer can obtain the password by starting the VPN client and then dumping the process memory with a tool such as ‘pmdump’, or crashing the computer to get a dump of physical memory.

• Weak registry or file permissions for stored credentials:

It is a bad idea to cache credentials at all, but this is made worse if they are stored in a file or registry entry that is readable by everybody. This allows these details to be obtained from guest or anonymous network connections as well as via physical access to the client system.

4.2.2 Username Enumeration Vulnerabilities

Many remote access VPNs use IKE Aggressive Mode with pre-shared key (PSK) authentication as the default authenticationmethod. The PSK authenticationmethod is essentially the well-known username/password authentication scheme, although the terminology used can be different, for example the username is sometimes known as the id or groupname, and the password is sometimes referred to as the secret or pre-shared key.

One of the basic security requirements of a username/password authentication scheme such as this is that the response to an incorrect login attempt should not leak information about which of the credentials (username or password) was incorrect, because this would allow an attacker to deduce whether a given username is valid or not.

This requirement has been known for at least 30 years. The first known reference to this is in the November 1979 Morris Password Security paper which discusses the authentication

security of the Unix V7 operating system, which was released in January 1979. In this paper, it is stated:

"To login successfully on the UNIX system, it is necessary after dialing in to type a valid user name, and then the correct password for that user name. It is poor design to write the login command in such a way that it tells an interloper when he has typed in an invalid user name. The response to an invalid name should be identical to that for a valid name.

When the slow encryption algorithm was first implemented, the encryption was done only if the user name was valid, because otherwise there was no encrypted password to compare with the supplied password. The result was that the response was delayed by about one half second if the name was valid, but was immediate if invalid. The bad guy could find out whether a particular user name was valid. The routine was modified to do the encryption in either case."**[5]**

Although this security requirement has been known for decades, many implementations of PSK authentication do not abide by it and give a different response for an invalid username than for a valid one.

Figure 12 shows the initial packet exchange for aggressive mode PSK authentication. In this exchange, the client sends an IKE packet to the VPN server, and the VPN server responds with an IKE packet. Both packets contain several ISAKMP payloads, but the important ones for this discussion are the Identity payload sent by the client, which contains the username, and the Hash payload sent by the server, which is an HMAC hash of various things including the password (preshared key). In a real authentication, the client would then respond with a third packet containing an HMAC hash of various things including the password, but this discussion is only concerned with the first two packets.

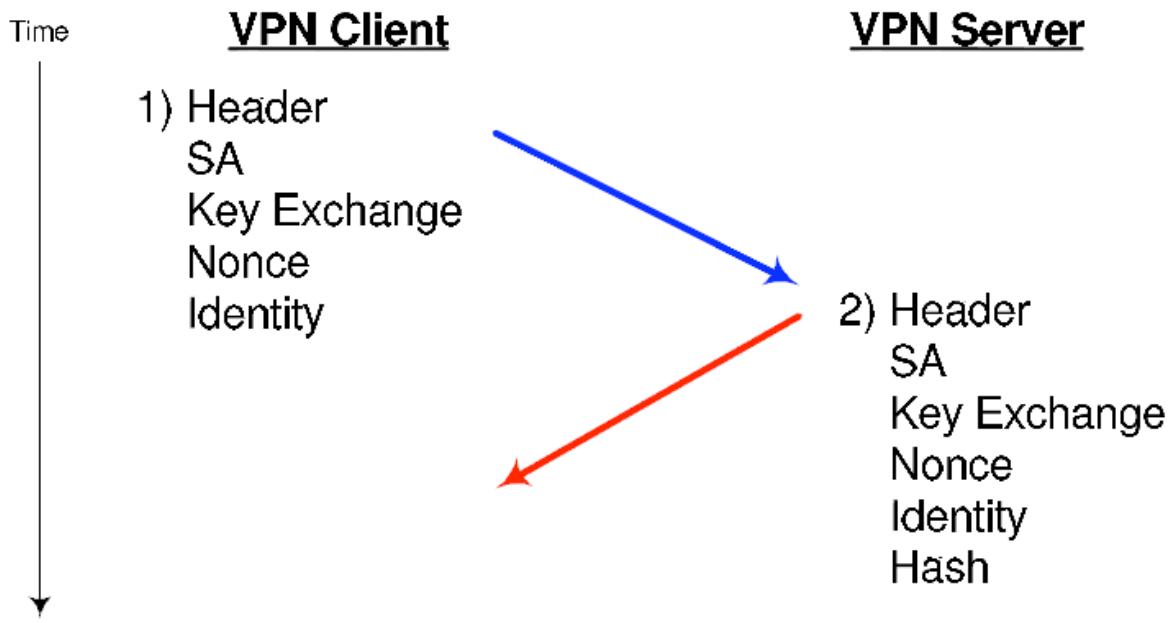

Figure 12: Packet Exchange for Aggressive Mode PSK Authentication

Three common faults were found in the way that VPN servers respond to the first packet from the client:

1. Some VPN servers only respond to the client if the username is valid, they do not respond at all to invalid usernames;

2. Some VPN servers will respond with a notificationmessage, e.g. no-proposalchosen, if the username is incorrect; and

3. Some VPN servers respond to both valid and invalid usernames, but the hash payload for invalid usernames is calculated using a null password, and it is simple for the client to determine this.

In all three cases, the response to an invalid username is different to that for a valid username, and this allows the client to determine if a given username is valid or not.

4.2.3 Offline Password Cracking

Once a valid username is obtained using IKE AggressiveMode, it is then possible to obtain a hash from the VPN server and use this hash to mount an offline attack to crack the associated password.

To perform the offline dictionary attack, a list of candidate passwords is taken, and each one is run through the hash function. The resulting hash is then compared with the hash that the server sent, and if they match then the correct password has been found. Because this is an offline attack, it does not cause any entries in the VPN server log, nor would it trigger account

lockout. This attack is very fast: typically several hundreds of thousands of guesses per second. Some speed figures for the pre-shared-key cracking tool psk-crack are shown in table 2. The PSK cracking speed achievable depends mainly on the underlying hash performance: each PSK calculation consists of two HMAC calculations, and each HMAC calculation consists of two hash calculations (either MD5 or SHA1 depending on the hash algorithm used), therefore the PSK cracking speed should be approximately one quarter of the hash speed.

Table 2. Psk-crack Cracking Speeds

CPU type and speed	MD5 attempts per second	SHA1 attempts per second
Intel P3, 1.13GHz	153,000	88,000
Intel P4, 2.8GHz	264,000	136,000
AMD Athlon XP 2800+	315,000	212,000

Table 3 shows the maximum time required for a brute-force attack against various password complexities using a single AMD Athlon XP 2800+ system.

Table 3. Psk-crack Cracking Speeds

Password Complexity	Number of Combinations	Brute Force Time
6 characters a-z	309 Million	16 minutes
6 characters a-z, A-Z, 0-9	57 Billion	2 days
8 characters a-z	209 Billion	8 days
8 characters a-z, A-Z, 0-9	218 Trillion	22 years

4.2.4 Man-in-the-Middle Attacks

If the VPN server is using IKE Aggressive Mode, and it is possible to determine a valid username and password, then an Internet Security Association and Key Management Protocol (ISAKMP) SA can be established to the VPN server. Even if the VPN server enforces a second level of authentication, this often relies on the security of this ISAKMP SA. In this case, if it is possible to establish an ISAKMP SA then the second level of authentication would not provide complete protection because it would be vulnerable to a man-in-the-middle attack. This risk is acknowledged in the XAUTH IETF draft:

“The protocol described in this memo strictly extends the authentication methods described in [IKE]. It does not in any way affect the authenticated nature of the phase 1

security association. In fact, this protocol heavily relies on the authenticated nature of the phase 1 SA. Without complete phase 1 authentication, this protocol does not provide any authentication at all, since it becomes easily vulnerable to Man-in-the-Middle (MitM) attacks."

An example scenario showing how this could be exploited against a VPN server using XAUTH is given below:

1. Install the MitM system in the path of the VPN Client/Server traffic. Installing the system on an Ethernet link that the traffic flows over, and using ARP spoofing to re-direct the traffic could achieve this.

In this position, the MitM system could sniff the usernames (which are passed in the clear) and crack the passwords using the information in the 1st and 2nd packets. Alternatively, it could be fed a list of usernames and passwords that had previously been obtained by group name enumeration and password cracking.

2. When the real client connects, allow them to establish an ISAKMP SA to the MitM system, and establish a second ISAKMP SA from the MitM system to the VPN server.

The client user thinks he is connected to the VPN server, but is really connected to the MitM system.

An ISAKMP SA can be established from the MitM system to the VPN server because the username and password are known.

3. The VPN server will issue an XAUTH challenge to the MitM system. The MitM system passes this on to the client.

4. The client sends the response (e.g. second username and SecurID PIN + passcode) to the MitM system, which passes it on to the VPN server.

5. Now the client is connected to the MitM system, and the MitM system is fully authenticated to the VPN server.

At this point, the VPN security is breached. The MitM system has three options:

(a) Intercept and log traffic between the client and VPN server;

(b) Alter traffic between the client and VPN server; or

(c) Drop the connection with the client and proceed to complete IKE Phase-2 with the VPN server and gain access to the internal resources.**[6]**

4.3 Conclusion

Basicly, there are three causes that VPN to be protect: basic firewalls, network attacks, and cryptographic assaults from the hackers. Firewalls are not preferred to protect connections in public area, since it only opens a hole in security of VPN technology. And, also there are some flaws in VPN such as insecure storage of authentication credentials, username enumeration vulnerabilities, offline password cracking, and man-in-the-middle attacks. To use one of these methods depends on client's issues. If the credentials are not well protected, they have to store some or all of the authentication credentials. If the password is not safety, and someone tries to crack password, the client can use IKE Aggressive Mode. And if someone tries to intercept between victims connection, they can use ISAKMP as best way to protect their conversation.

CHAPTER 5

Implementation of VPN Designs

5.1 Introduction

In the previous chapter there is mentioned about risks and security in VPN: what do the hackers do to attack, and how can the computer users protect their data from that attacks.

In this chapter there are explained VPN designs. Three types of VPN designs will be mentioned in this chapter. First one is “Small VPN Design”, second one is “Medium VPN design” and the last one is “Large VPN design”. They are seperated, since there are used different corporate Internet module.

5.2 Small VPN Design

This design supports both ‘site-to-site’ and ‘remote-access VPN’s’, with some caveats included in the configuration section. The main information in this design is based on the premise that this design will operate as the headend for a corporation. Specific design changes when used as a branch are also included. The small network design is contained within the small network corporate Internet module. The all small business design is shown here for reference.

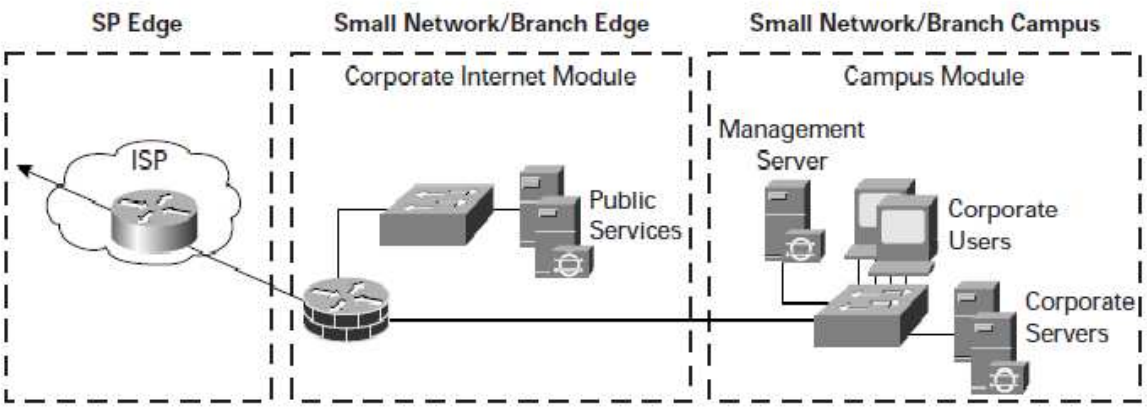

Figure 13.Detailed Model of Small Network

5.2.1 Corporate Internet Module

The corporate Internet module provides internal users with connectivity to Internet services and Internet users access to information on public servers. VPN access was also provided to remote locations and telecommuters.

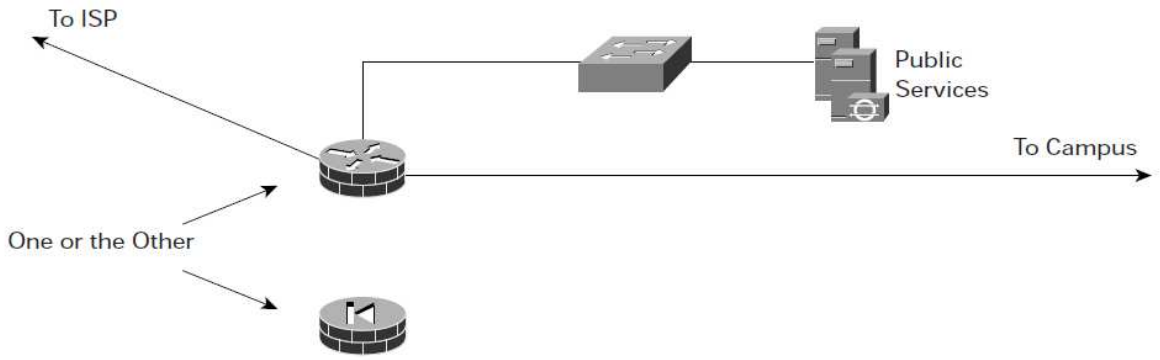

Figure 14: Detailed Model of Small Network Corporate Internet Module

5.2.2 Design Guidelines

This module represents the ultimate in scaled-down VPN network design, where the VPN functions are compressed into a single box that also performs routing. NAT (Network Adress Translation), IDS (Intrusion Detection System), and firewalling. Two principal alternatives come into play when deciding how to implement this functionality. The first is to use a router with firewall and VPN functionality. This scenario yields the greatest flexibility for the small network because the router will support all the advanced services that may be necessary in today's networks. As an alternative, a dedicated firewall with VPN may be used instead of the router. This setup places some restrictions on the deployment. First, firewalls are generally ethernet only, a setup that would require some conversion to the appropriate WAN protocol. In today’s environments, most cable and DSL routers/modems are provided by the service provider and can be used to connect to the firewall over ethernet. If WAN connectivity on the device is required, then a router must be used. Using a dedicated firewall has the advantage of being generally easier to configure security and VPN services and can provide improved performance when doing firewall functions. Whatever the selection of device, there are numerous VPN considerations. Remember that routers tend to start out permitting traffic, whereas firewalls tend to deny traffic by default.

The VPN functionality as implemented in this design is similar, regardless of the hardware platform chosen. Both router and firewall support stateful firewalling, basic NIDS, NAT, and IPSec. Because there is no headend resiliency unless the small design is used as a

branch of the large design (discussed later), basic tunnel-mode IPSec was chosen without any options. The following sections detail the specific design considerations for the small network.

5.2.3 Identity

For site-to-site VPN connections to remote locations, preshared keys and the IPSec peer IP addresses are used to validate the identity of the IPSec devices. Although this scenario does not have the security of a digital certificate, for a small VPN, preshared keys can be easily managed because the number of sites tends to be fewer than ten.

The remote-access VPN connections employ a two-part authentication scheme that uses a wildcard preshared key on the device coupled with a secondary user authentication through RADIUS. Because this authentication does not include OTP, a greater reliance is placed on a user's selection of a strong password. Passwords should also be aged quickly, and users should be locked out of the VPN after a certain number of failed login attempts. This scenario will aid in the prevention of brute-force attacks if someone is able to steal a user's laptop and it is not immediately informed. Remember that this fixed-password authentication scheme is in no way strong, and it leaves the organization with a very thin layer of defense if one of the two authentication schemes is compromised.

5.2.4 Security

From a security perspective, the inbound ACL allows only IKE and ESP traffic to terminate on the public interface of the VPN device. From there, traffic was decrypted and then filtered again through the firewall function on the device. This scenario allows the administrators of the small network VPN to define the types of protocols it wants to allow into the network. Remote access VPN users are not allowed to split tunnel but remote site-to site devices are allowed.

5.2.5 Scalability

This type of design is not particularly scalable. It is designed for fewer than 20 remote sites and fewer than 50 concurrent remote users. However, this design will meet the needs of most small networks.

5.2.6 Routing

With the exception of some simple static routes, routing was not needed in this configuration given the flat network. A default route could be attained dynamically from the ISP (Internet Service Provider). All the internal users by default route to the VPN device, which then default routes to the ISP. Static routes to remote sites are not needed because after the packet is routed to the outside interface it is encrypted and sent to the remote peer.

5.2.7 Performance

Typically the WAN connection is the limiting factor in small networks today. When VPN traffic is coupled with standard Internet traffic, care should be taken to avoid overflowing Internet link with VPN traffic. Allowing remote sites to use split tunneling can aid in this. Because most VPN devices do not yet offer the ability to limit VPN traffic or the number of users on a device, the mix of traffic at the headend will need to be carefully watched.

5.2.8 Alternatives

The most obvious need in the small VPN design is stronger authentication for remote users. This authentication can be achieved through the addition of OTP (On Time Paswoord) into the small environment. It was not included in this design because many small networks are unable to make the financial commitment to use OTP technology. Any other deviation from this design would be geared toward increasing the capacity of the network, or separating the various security functions onto distinct devices. If these changes are incorporated, the design will start to look more and more like the medium VPN design discussed later in this document. A first step rather than adopting the complete medium design might be the addition of a dedicated remote-access VPN concentrator to increase the manageability of the remote-user community.

5.3 Medium VPN Design

This design supports both site-to-site and remote-access VPNs. Most of the discussion in this design is based on the premise that this design will operate as the headend for a corporation. Specific design changes when used as a branch are also included. The medium VPN design is contained within the medium-network corporate Internet module. The entire medium-network design is shown here for reference:

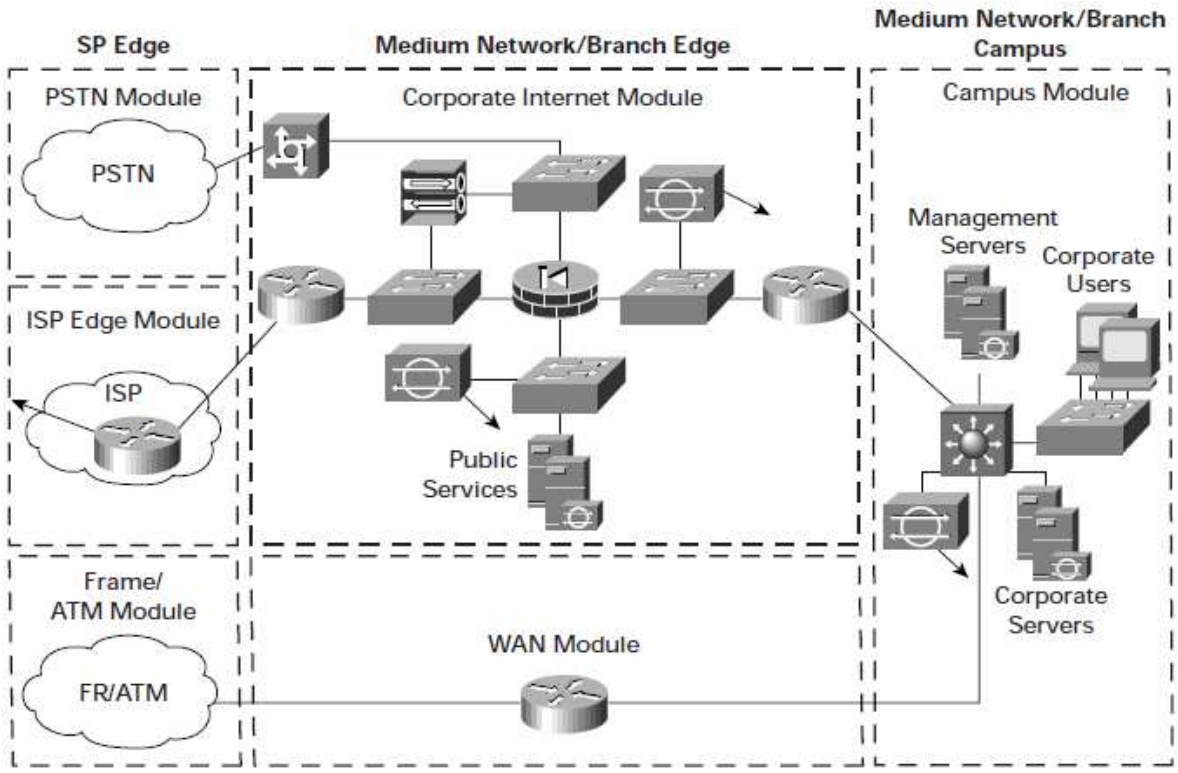

Figure 15: Detailed Model of Medium Network

5.3.1 Corporate Internet Module

The goal of the corporate Internet module is to provide internal users with connectivity to Internet services and Internet users access to information on the public servers (Hypertext Transfer Protocol [HTTP], FTP, Simple Mail Transfer Protocol [SMTP], and DNS). Additionally, this module terminates VPN traffic from remote users and remote sites as well as traffic from traditional dial-in users.

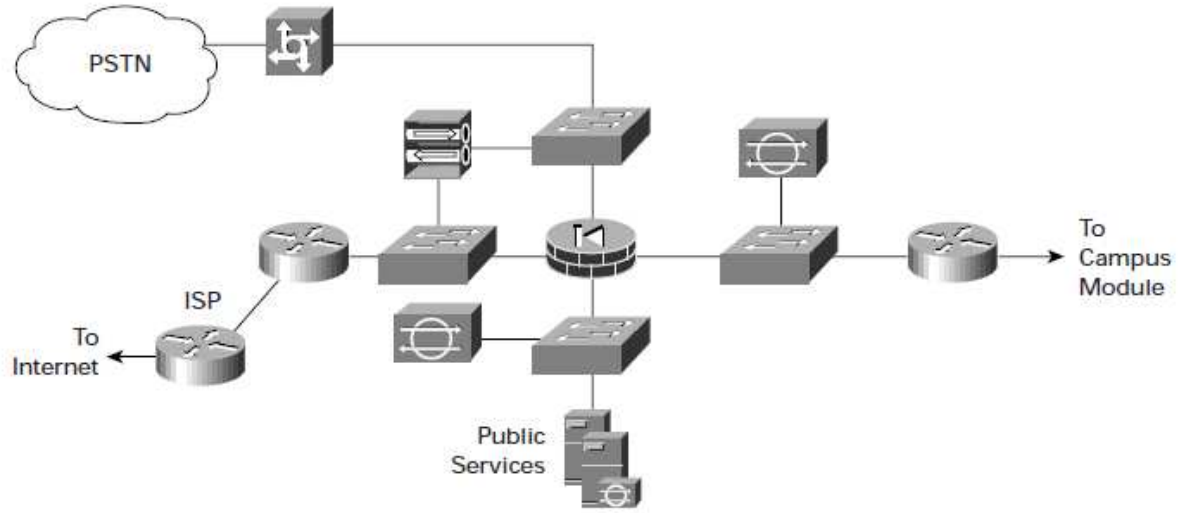

Figure 16: Detailed Model of Medium Network Corporate InternetMmodule

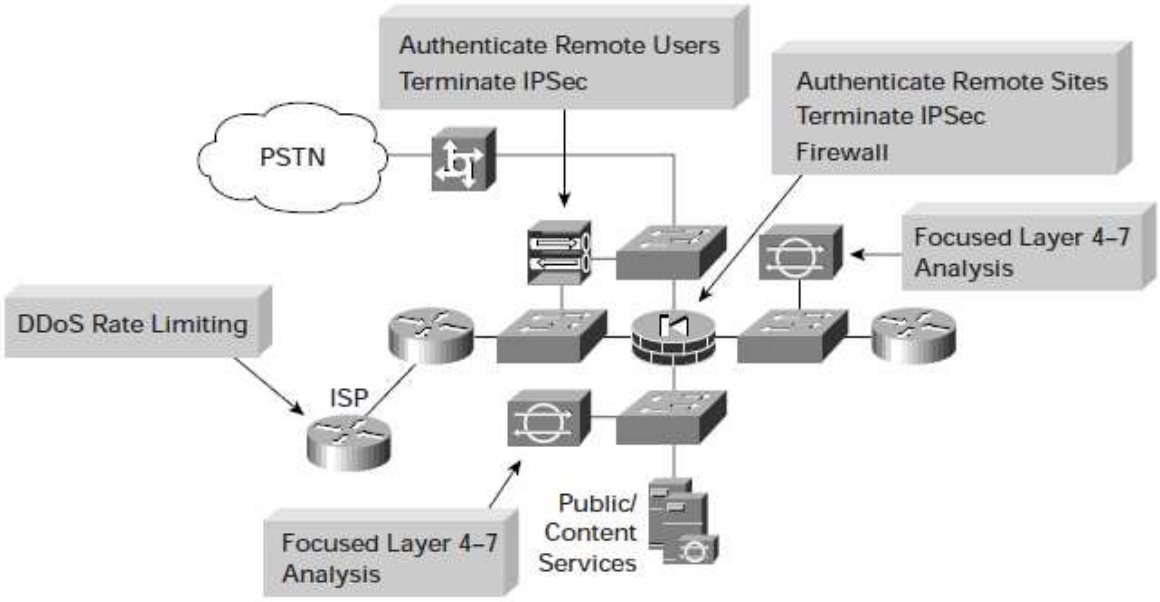

Figure 17: Detailed Model of Medium Network Corporate Internet Module: VPN

5.3.2 Design Guidelines

The medium VPN design separates site-to-site and remote-access VPN traffic onto two separate devices. This setup allows better performance because each device is concerned with only one type of VPN. By moving to a dedicated remote-access VPN device, manageability of the remote-user community also increases. The site-to-site VPNs are done on the dedicated firewall at the heart of the module. Because resilience was not a part of this design, as in the small design, standard tunnel mode IPSec was used.

5.3.3 Identity

For site-to-site VPN connections to remote locations, digital certificates and the IPSec peer IP addresses are used to validate the identity of the peer devices. This scenario provides better security and manageability over standard preshared keys. The remote-access VPN connections employ a two-part authentication that uses a wildcard preshared key on the device coupled with a secondary user authentication via OTPs.

5.3.4 Security

From a security perspective, the edge router allows only IKE and ESP traffic to terminate on the public interfaces of the VPN devices. From there, traffic is decrypted and then either passed to a firewall if it is remote-access VPN traffic or filtered locally using the firewall

function in the case of site-to-site VPNs. After filtering has occurred, the traffic passes a layer of NIDS as traffic is sent to either the public services segment or is routed into the campus. This NIDS is configured to shun on the firewall for certain alarms. Remote access VPN users are not allowed to split tunnel but remote site-to-site devices are allowed.

5.3.5 Scalability

This type of design is much more scalable than the small design. With hardware acceleration, this design can easily support over 500 concurrent remote users and up to 50 remote sites. Depending on the amount of bandwidth each remote site and user consumes, these numbers could be larger or smaller. If you think that you will be pushing the limits of this design but do not have the financial resources for the large design, consider the alternatives section for this design below.

5.3.6 Routing

All internal user traffic is routed to the VPN firewall. It then routes via a static-route, remote-access client-bound traffic to the VPN concentrator and routes all other traffic via a default route to the edge router. This scenario results in remote site-bound traffic to trigger the cryptographic ACLs (Access Control Lists).

5.3.7 Performance

Like the small network, the WAN connection will probably be the limiting factor in this design. The equipment in the design could easily saturate a DS3 link (45 Mbps) or more. Most networks of this size will have less bandwidth, however, and the network will need to be designed carefully to avoid overflowing it. Allowing remote sites to use split tunneling can aid in this overflow prevention. Because most VPN devices do not yet offer the ability to limit VPN traffic or the number of users on a device, the mix of traffic at the headend will need to be carefully watched.

5.3.8 Alternatives

The most common modification to this design would be to dedicate all remote access and site-to-site VPN functionality to the concentrator. Many customers choose this option because they prefer to specialize the functions of their VPN and firewalls with two separate devices. This scenario frees the firewall to perform firewalling only and allows the VPN device to

focus on IPSec. Another option would be to deploy a site-to-site VPN device on the same network, or a parallel network, with the concentrator thus providing remote access and site-to-site VPN separation. Both options yield greater scalability and manageability to the medium network and are similar to the large VPN design in the next section.

5.4 Large VPN Design

The large network VPN design is contained within the large enterprise VPN and remote-access module and supports both site-to-site and remote-access VPNs. This module was redesigned to provide high-speed, highly available VPN termination. The entire large business design is shown here for reference:

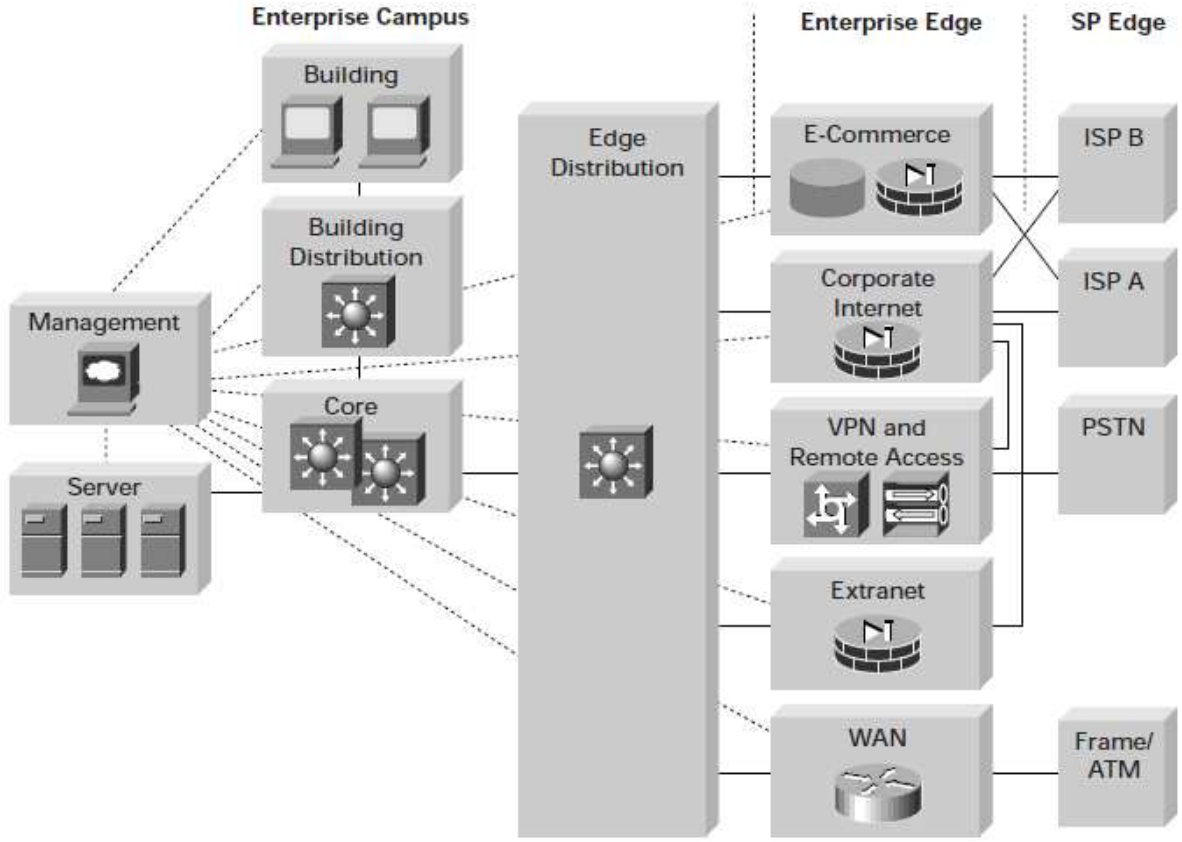

Figure 18: Detailed Model of Large Network

5.4.1 VPN Remote-Access Module

The VPN and remote-access module provides termination of VPN traffic from remote users, VPN traffic from remote sites, and termination of traditional dial-in users. The designer is given an option to choose a VPN router or VPN firewall for site-to-site VPN termination. This device is labeled “VPN” in the module layout shown below. Because of the high-speed

requirements for the VPN, purpose-defined devices are deployed throughout the module, providing disparate functions.

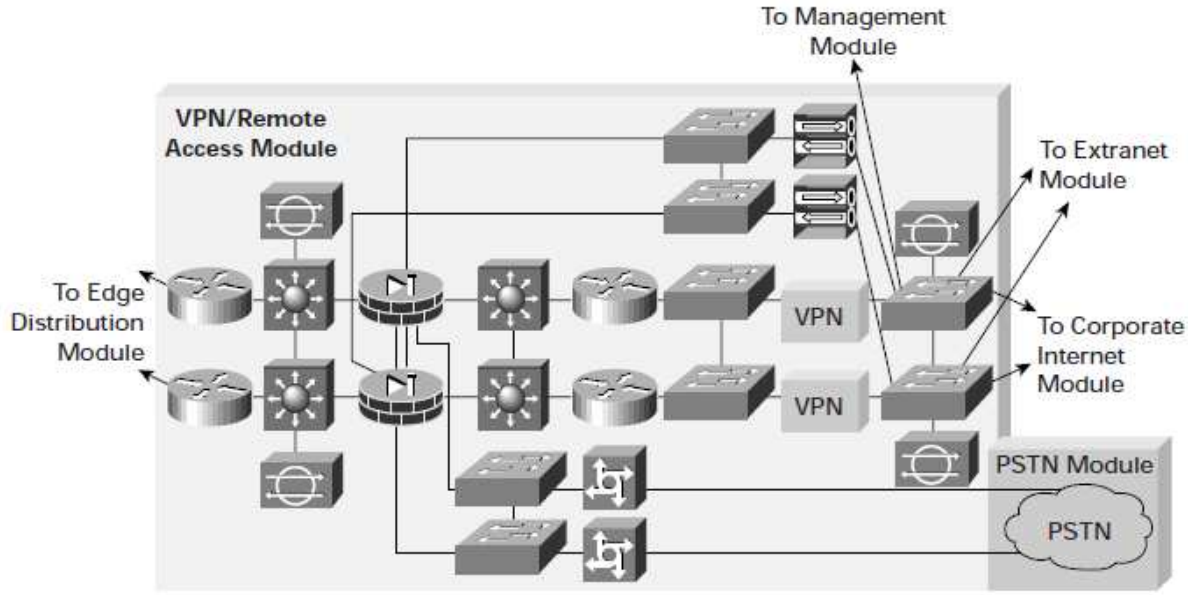

Figure 19: Detailed Model of VPN and Remote-Access Module

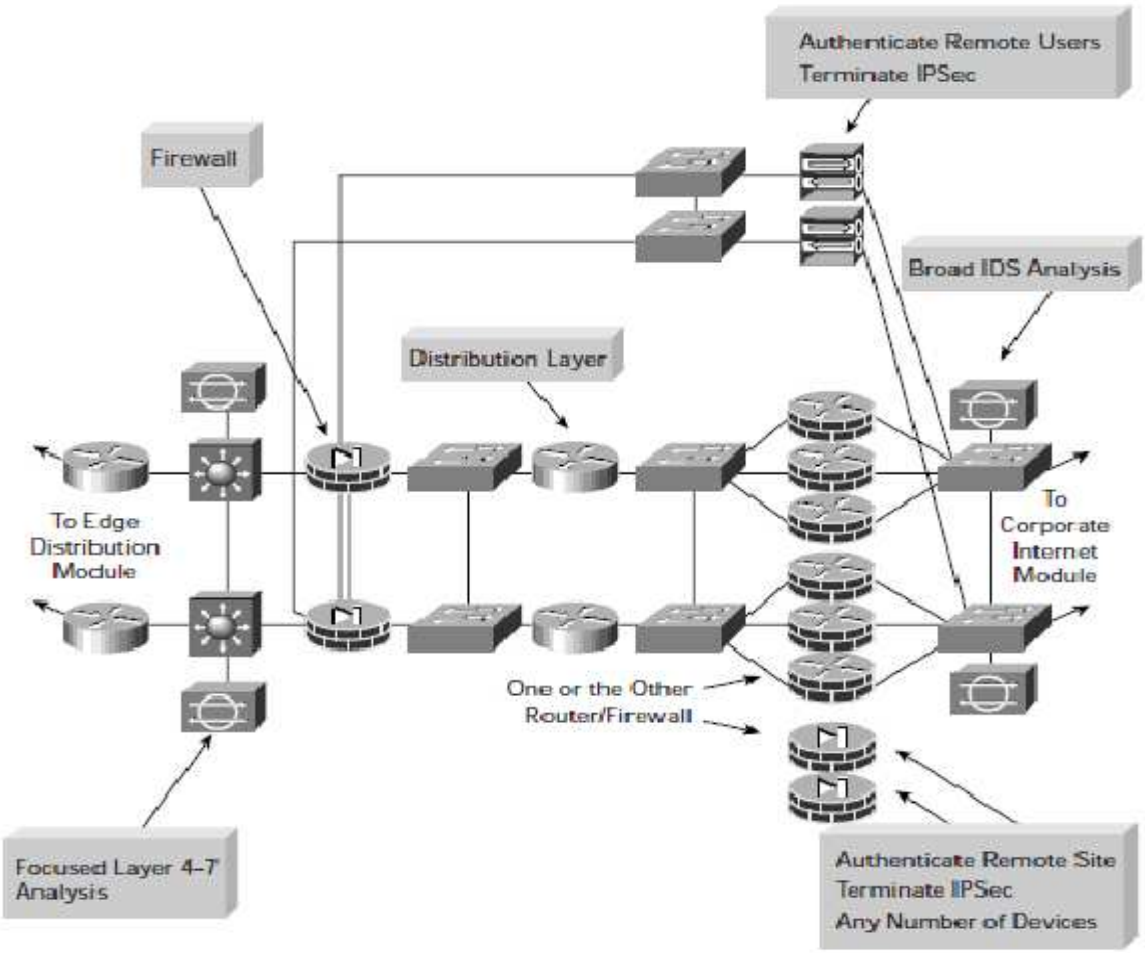

Figure 20: Detailed Model of VPN and Remote-Access Module: VPN

5.4.2 Design Guidelines

The core VPN requirement of this module is to authenticate remote devices and users and terminate IPSec. Multiple VPN termination devices generate gigabit traffic load, driving the need for high-speed Layer 3 switching in the module from the egress of the termination devices to the ingress to the edge distribution module. For this reason, and because of the need for packet classification for differentiated services, the interior routing and distribution layer functionality were carried out using high-speed Layer 3 switching. These factors also drove the requirement of a gigabit-line-rate-capable firewall for stateful inspection and filtering of all traffic in the module and high-speed IDS appliances for attack detection. Because the traffic comes from different sources outside the enterprise network, the decision was made to provide a separate interface on the firewall for each of these services. The design considerations for the VPN functions of each of these services are addressed below. Extranet VPNs are addressed in the extranet module in a later section of this thesis.

5.4.3 Identity

For site-to-site VPN connections to remote locations, digital certificates are used for strong and scalable device authentication. The remote-access VPN connections employ a two-part authentication scheme that uses a group preshared key on the device coupled with a secondary user authentication via OTPs.

5.4.4 Security

Given the high level of access to the corporate Intranet, this module exhibits a high level of security. The stateful firewall software on the VPN firewall allows only IKE and ESP traffic to terminate on the public interface of the VPN firewall. The VPN router option was configured with inbound ACLs to allow only IKE and ESP traffic to terminate on the public interfaces of the VPN routers. The VPN concentrator allows only ESP, IKE, and UDP port 10,000 on its public interface. Filtering that occurs before traffic is passed to the remote-access and VPN module allows only the following traffic flows:

• ESP, IKE, and UDP port 10,000 from any address to the public and virtual cluster IP addresses of the VPN concentrators

• ESP and IKE from known static IP-addressed remote sites to the public IP address of the VPN firewall

• ESP and IKE from known static IP-addressed remote sites to the public IP address of the VPN router

Any flows not listed above will trigger the IDS sensor to high-severity alarm. After decryption, all VPN-sourced traffic is immediately forwarded to the interior firewall, where it is filtered and statefully inspected. While the traffic is being forwarded to the interior router, IDS on that segment performs detailed Layer 4-7 traffic analysis. If IDS detects an attack in a flow, it will shun that flow on the interior firewall.

5.4.5 Scalability

This type of design is extremely scalable. Depending on the remote-site bandwidth requirements, this module can support between 100 and 250 remote-site tunnels per device, possibly even more with very-low-bandwidth remote sites. Because the infrastructure surrounding the VPN devices was designed for the high-speed requirements, this factor was not a limiting one. As with any large-scale VPN design, the primary limiting factor is the number of remote sites that can be terminated given the high-availability mechanism chosen. Remote-access user termination can scale up to 5000 or more of concurrent users.

5.4.6 Routing

The edge distribution layer is aware of which subnets are used by remote users and sites. The edge distribution routers use a default network to determine reachability to these subnets in the remote-access and VPN module. The default network used was the internal firewall and IDS segment. This way, the edge distribution routers can track the availability of the VPN module via advertisements by its two interior edge routers. The interior edge routers in turn track Intranet reachability via dynamic routing updates and statically route all remote-user and site-destined traffic to the firewall. The interior firewall statically routes remote-access traffic to the VPN concentrator segment and statically routes remote-site traffic to the HSRP virtual address on the distribution routers or VPN Firewalls (whichever is used). The distribution routers run the same routing protocol as the VPN routers terminating the site-to-site VPN traffic and receive updates regarding remote-site network availability. The distribution routers also inject a static route for the major enterprise network into the routing table for redistribution so that remote sites have reachability to the corporate Intranet. Otherwise, reachability to the major network by remote sites would not be possible because routing protocols do not pass through the firewall.

5.4.7 Performance

Large numbers of remote sites and users mandate the use of hardware acceleration at high speed with low latency. Given the bandwidth requirements of the network, high-speed WAN links such as OC-3 (155 Mbps) or greater will be required. Because the remote sites do split tunnel, this setup will alleviate some of the headend bandwidth requirements. However, disallowing the split-tunneling of high-speed DSL/cable users may use significant amounts of data. Care should be taken to not overrun the WAN with VPN traffic.

5.4.8 Alternatives

If the VPN router solution is chosen and the number of devices needed remains small, multiple HSRP groups on the VPN routers could substitute for the distribution layer of routing. However, this solution will not scale as the number of headends grow. If successful personal firewall software deployment occurs as outlined in the axioms, consider enabling remote-access client split tunneling to reduce the performance requirements at the headend. You may consider digital certificates for remote-access user device authentication; however, given the scalability requirements, deployment will be extremely difficult. In this design, the same WAN infrastructure is used for Internet access, e-commerce, and VPN. Finally, given the performance requirements for networks, this size of a dedicated VPNWAN infrastructure may be in order. This solution also requires less bandwidth management at the edge because only VPN traffic is routed.**[7]**

5.5 Conclusion

In this chapter there are mentioned about three types of VPN design: each three design are used in site-to-site and remote-access VPN's. In small VPN design there is some caveats included in the configuration section. Most of the discussion in medium VPN design is based on the premise that this design will operate as the headend for a corporation. Large medium design was redesigned to provide high-speed, highly available VPN termination.

CHAPTER 6

Conclusion

VPN allows users or companies to connect to remote servers, between departments, or to other factories over a public network, as providing secure communications. In these cases, the secure connection occurs to the user as a private network communication although the fact that this communication appears over a public network. VPN technology is designed to address issues surrounding the current business trend toward increased telecommuting and widely distributed global operations, where workers must be able to connect to central resources and communicate with each other.

This thesis contains some basic information about VPN, then it is mentioned about VPN technologies, such as firewalls, encryption and authentication. After that there is focused on security and risks in VPN deeply. IKE and ISAKMP are shown as the best ways to protect the data. Beside these there are discoursed about three types of VPN designs which are small, medium, and large VPN designs, also their design guidlines, identity, security, scalability, routing, performance, and alternatives are shown respectively.

Moreover, VPN protocols are approached as the main topic, since they cover all of other sections in this dissertation. These VPN protocols are explained in chapter 2 in detail: L2TP, PPTP, L2F, Layer3, IPSec, MPLS, and IP-in-IP. Layer 2 solutions are in some ways more flexible particularly in terms of the higher layer protocols used in the VPN. Layer 3 VPNs can have advantages in terms of management. PPTP is an technique that for remote connections. L2F is a devoloping protocol of PPTP. L2F can make more than one connection, a limitation of PPTP. MPLS is usefull mainly within an autunomous system, however it can be used across autonomous system if their directors agree and coordinate labels.

From these protocols, IPSec is indicated as the best one, since its advantages. The main and the most important benefit of IPSec is that it is a universal protocol. IPSec is an international standard because of the flexibility and power of IP. It can provide security and communicate with a variety of different networks from around the world. Through IP, IPSec

can be applied in networks of all sizes including LAN's to global networks. Because of these advantages IPSec is recommended as the future of VPN protocols in our opinion.

References

[1] Charlie Scott, Paul Wolfe and Mike Erwin," Virtual Private Networks", Second Edition January 1999.

[2] Martin W. Murhammer, Orcun Atakan, Zikrun Badri, Beomjun Cho Hyun Jeong Lee, Alexander Schmid, "A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management", November 1999.

[3] How Virtual Private Networks Work by Jeff Tyson
http://computer.howstuffworks.com/vpn.htm

[4] Virtual Private Networks by Shamod Lacoul
http://www.slidefinder.net/V/Virtual_Private_Networks_Shamod_Lacoul/32104518

[5] Robert Morris, Ken Thompson, "Password Security: A Case History", Bell Laboratories Murray Hill, New Jersey 07974

[6] Roy Hills, " Common VPN Security Flaws", January 2005.

[7] Jason Halpern, "SAFE VPN IPSec Virtual Private Networks in Depth White Paper"