GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

## Interested in learning more?

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

**Why Virtual Private Network (VPN)? And considerations when implementing VPN**
**Ramiah Marappan**
**Version 1.3**

## 1 Introduction

This paper presents some of the challenges faced by business and employees in communicating with their partners, suppliers and Headquarters. These challenges can be addressed by the Internet infrastructure, which today covers most of the cities and towns in the world. However, Internet, which is public network, has its concerns in relation to information security. To address the concerns of security covering confidentiality, integrity and authenticity, the information being sent through the internet has to encrypted and measures in place to ensure that the data is not modified in the internet. The technology used to achieve this is called Virtual Private Network (VPN).

VPN components are software/hardware based VPN clients at the employees' home/branch site, connection to the local Internet service provider (ISP), and Internet infrastructure, leased line connection from the local Internet Service provider, VPN concentrator and its connection to the firewall and the intranet. The 3 main VPN technologies are IPSEC (IP Security Protocol), PPTP (Point to Point Tunneling Protocol) and L2TP (layer 2 Tunneling Protocol). The technology being widely deployed is IPSEC. There are several modes of operation for IPSEC based VPN. The appropriate mode has to be selected based on the VPN architecture. The appropriate mode selection is one of the important activities in the setup and operation of the VPN.

## 2 Why VPN?

In the last 5 years, Internet infrastructure has grown tremendously and is available in all locations in developed countries, most of the locations in developing countries and major cities in under-developed countries. Internet is evolving to be data equivalent of the public telephone network and has opened up interesting opportunities which address the challenges, businesses are facing as listed below:

**The first challenge** is that employees who are away on business travel (hotel, convention centers, airports, cafes and customer sites) or want to work from home require access to the Corporate Intranet in a cost-effective manner. Employees are accessing the Intranet through telephone dialup lines. The dialup costs can be expensive (depending from where they are calling) and also the business has to maintain a number of telephone lines, modems and Remote access server facility at the corporate site.

**The second challenge** is the businesses are expanding their reach by going to new

© SANS Institute 2000 - 2005 Author retains full rights.

locations, cities and countries and require connectivity to these location from head quarters. Big Corporations can afford to operate a private network to link their branch offices and partners. The cost of operating a private network (based on leased lines or Frame relay) is expensive. It also takes time to link a new location to the private network. Therefore, most businesses were unable to have a private network.

These 2 challenges can be addressed by using the Internet infrastructure, as it is widely available. It can be accessed by employees/business dialing into the local ISP (at local instead of inter city rates)

However, as Internet is network of networks and no one entity owns and manages, there are security concerns. The information sent through it can be tapped and modified by intruders. Intruders can place sniffing software and collect information on user ID, passwords and other sensitive information. The information can also be modified, for example, financial information being sent through Internet can be altered. The information being sent through Internet is no longer confidential and also no guarantee on data integrity. Internet is also liable to Denial of Service attacks.

To address the issues of information confidentiality and data integrity in Internet, the information sent need to be **encrypted and hashed** and users/devices accessing the resources must be **authenticated.**

So the network which can provide encryption, data integrity checking and authentication is called **Virtual Private Network (VPN).**

There are 3 types of VPN. **Intranet VPN** is for branch offices to connect to Head quarters and other Branches. **Extranet VPN** is for extending the corporate resources to business partners and suppliers. **Remote Access VPN** is for employees to access the corporate resources from home and when away from home/office. Employees have to dial to the local Internet Services Provider (ISP) and only local call charges are incurred. (Reference – 1)

**VPN provides the following benefits:**

- Reduce the dialup and maintenance costs of accessing corporate resources. The modem banks, telephone lines and Remote Access server hardware are no longer required.
- Increase the productivity of employees as they can access resources from anywhere and anytime
- Partners and suppliers can access information efficiently and in a secure manner
- Increase revenue as businesses can provide their services in more locations and countries

© SANS Institute 2000 - 2005 Author retains full rights.

- New Employees and Businesses can have access setup in the shortest time through dialup, ADSL broadband or Cable as Internet service providers have points of presence readily in most locations.

Corporate resources include the IT hardware (servers, printers, scanners and storage devices), the applications and the information available at the Corporate IT facility.

## 3 What applications/environment suitable for VPN?

VPN suitable for accessing applications and data, which does not demand guaranteed bandwidth and tolerant to delay. As VPN is based on Public Internet and not managed by one service provider, there is no guarantee on the bandwidth allocated to each application, on the maximum delay in transmitting the data across the Internet and the network uptime. Based on these considerations, VPN can work with the following applications/environment

- Delay insensitive such as email and office automation applications. Employees can access their email (be it Lotus Notes or Microsoft Exchange) from anywhere through the Internet through a Lotus Notes/Outlook and VPN client running on their laptops/personnel computers.
- Batch applications such as file transfer. There are requirements for partners and suppliers to transfer files and documents to each other. By having the VPN setup between the two partners through internet and activating the file transfer program, partners can transfer files between each other
- Some companies in the past were not able to provide access to their interactive applications such as airline reservations in speedy manner to their travel agents as setting up private network took time or was not feasible to setup. Setting up private network in some countries in Asia Pacific takes a long time and also costly. But as Internet is available in these countries and using VPN, the travel agents can access the reservations applications to make bookings. This is a win- win situation as the travel agents can work productively as they need not make a telephone call to the airlines for making bookings as well reduce their telephone bills. For the airlines, they can deploy their staff for more productive tasks as well increase their revenue.

## 5 Security consideration at Employees/Businesses/Partners desktop/notebook when accessing Corporate resources using VPN

Enabling access through Internet from anywhere and anytime poses security threats to corporate network resources. Therefore it is vital that employees and business partner do the following when accessing the Intranet( reference 2):

- Employees access the Internet through a firewall. This is to prevent/minimize hackers probing the notebook/desktop, identify vulnerabilities and install virus,

© SANS Institute 2000 - 2005 Author retains full rights.

worms and Trojans.
- Partners and suppliers have necessary security infrastructure program covering firewalls in place to prevent/reduce attacks from Internet.
- Must use strong authentication such as one time passwords
- Do not access unfamiliar and strange websites.
- Do not run remote access software such as PCAnywhere and Remote access software
- Turn off print and file sharing. If possible do not bind Microsoft client to TCP/IP(Transmission Control Protocol / Internet Protocol ) stack
- Anti-virus software must be enabled in the desktop/notebook. This is to Scan for viruses, worms and Trojans.

So when providing VPN to employees and partners, access and flexibility to employees must not compromise corporate resources confidentiality, availability and integrity.

## 5 **Design goal**

The design goal of VPN is as follows (reference 3):
- Employees and business partners can access the Corporate resources in a secure (confidentiality, integrity and authentication) and reliable manner
- Implementation of VPN network infrastructure does not compromise existing corporate security or make it vulnerable to attacks
- VPN infrastructure must be scalable to cater for growth , provide good performance and reliability
- VPN infrastructure must include tools for monitoring the performance, logging of access into the network and alarms/event logging.

## 6 VPN Architecture

The planning and implementation to meet the design goal requires a sound VPN architecture (reference 4) . The VPN architecture to provide access to corporate headquarters from employees/branch locations includes the following:
- Software based VPN client residing on the employee or the business partner notebook/desktop. The remote client can use PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) or IPSEC (IP security protocol) to set up a session and communicate with the VPN concentrator. These protocols support encryption, data integrity and device authentication.
- Hardware based VPN device when you have several employees in a branch office accessing the corporate resources. The protocols supported are PPTP, L2TP and IPSEC. In this environment, VPN client software is not required on the employee's notebook/desktop.
- Broadband ADSL( asymmetric digital subscriber line) or cable router or modem is required at the employee's location or branch site

© SANS Institute 2000 - 2005, Author retains full rights.

- Access to the local ISP( Internet service Provider) through dialup, broadband or cable or leased line
- Local ISP is in turn connected to other ISP's .The corporate headquarters ISP can be the different from the employees ISP. The ISP's are interconnected directly to each other or can be through other ISP's.
- Leased line connection from the ISP to the corporate headquarters. The bandwidth of the leased line is dependent on the number of concurrent employees and partners accessing the applications and data at the corporate site.
- Router and modem is required at the corporate site to connect to the ISP.
- VPN concentrator receives the traffic from all the remote client/devices, authenticates, decrypts and forwards the traffic to the firewall. VPN concentrator also encrypts the traffic from the corporate site destined for the remote clients. VPN concentrator can use IPSEC, L2TP and PPTP technologies for encryption, integrity and authentication.
- Authentication server will authenticate the employee by requesting for user ID/password, token, smart card, and biometrics credentials. Upon successful verification, then the employees are permitted to access the applications and data. User ID/password is the most popular and lowest cost authentication mechanism followed by token, Employees with token will key in the random number displayed on the token as password to access the applications. The random number changes every one-minute and therefore the password is dynamic. Token authentication is also called (OTP) one time password. There are also more secure but expensive authentication methods such as biometrics are based on what you know what you have and what you are.
- Connection of the VPN concentrator to Firewall and internal LAN (local area Network). The location of the VPN is important as it impacts the security of the corporate network.

## 7 IPSEC/L2TP/PPTP protocol feature comparison

There are 3 main technologies for VPN clients/hardware devices to communicate with the VPN concentrator ( reference 5 ). These technologies provide encryption, authentication and data integrity they are:

- IPSEC( IP Security Protocol)
- L2TP ( Layer 2 Tunneling Protocol)
- PPTP ( Point to Point Tunneling Protocol)

IPSEC is a Layer 3 / network layer protocol and is being widely adopted in VPN. Next is PPTP and followed by L2TP. PPTP and L2TP are layer 2 protocols. PPTP lacked strong security features as it used only 40-bit encryption.

Features of the protocols are in table below

© SANS Institute 2000 - 2005 Author retains full rights.

| | | |
|---|---|---|
| PPTP | L2TP/IPSEC | IPSEC |

© SANS Institute 2000 - 2005, Author retains full rights.

| | | |
|---|---|---|
| • Layer 2 protocol and supports multiple layers 3 protocols (Netbeui IPX, IP). Netbeui (NETBIOS extended user interface) is a IBM protocol designed for one PC to talk to another PC. IPX is a Novell protocol for PC to talk to Novell file server. IP (internet protocol) is the protocol used from one device to another through the internet and the local area network. It supports by encapsulating layer 3 protocols.<br>• Developed by consortium formed by Microsoft,US Robotics,ECI,3COM and Ascend<br>• Microsoft point to point encryption (MPPE) is enhanced version based on RSA (Ronald Rivest, Adi Shamir and Len Adleman professors who developed the algorithm) encryption algorithm.<br>• Authenticates sessions and not individual packets<br>• Works in NAT (Network address translation) environment.<br>• Uses TCP(transmission control protocol) destination port number 1723 and source port number 1023 for communication between the 2 devices<br>• Uses GRE(Generic Routing Encapsulation) for encapsulation with IP protocol type 47<br>• No congestion control<br>• Implementation mostly based on Microsoft version<br>• Session key is a hash | • Layer 2 protocol and supports IP and non-IP layer 3 protocols such as (Netbeiu,IPX,IP)<br>• Merger of L2F(layer 2 forwarding and PPTP developed by Cisco and Microsoft respectively<br>• L2TP uses UDP(user datagram protocol) port 1701<br>• IPSEC/IKE(Internet Key Exchange) uses UDP port 500<br>• ESP (encapsulation security payload) uses IP protocol type 50<br>• AH (Authentication header protocol) uses IP protocol type 51<br>• Can be used with IPSEC<br>• Can tunnel PPP(point to point protocol) frames across Internet<br>• L2TP header and payload are encapsulated by UDP and IP headers<br>• No authentication for individual packets<br>• Supports DES( Data Encryption Standard) /CBC (Cipher Block Chaining) encryption with 56 bits<br>• Supports MD5 (Message Digest 5) for data integrity and works with DES<br>• Supports also 3DES/CBC encryption with 128bits<br>• Supports MAC(Message authentication code) SHA-1(Secure hash Algorithm) for data integrity. This integrity feature works in conjunction with 3DES | • Layer 3 protocol and supports IP only<br>• IPSEC/IKE(Internet Key exchange) uses UDP port 500<br>• ESP(encapsulation security payload) uses IP protocol type 50<br>• Device authentication through pre-shared keys (unique/group/wildcard) or digital certificates. Pre-shared keys suitable for small VPN setup. Pre-shared key is used to hash the password. The client sends user ID (clear text) and hashed password to VPN server. User ID/hashed password is validated against the server database .OK message sent to client upon successful authentication. Digital certificates based on public and private keys provide a higher level of security but also increases the admin effort of VPN deployment and support<br>• Pre-shared key device authentication can be made more secure by using one time password at user level authentication<br>• Default MTU (Message Transfer Unit) setting for IPSEC packet is reduced to 1372 bytes to take into account IPSEC overheads. This is to prevent fragmentation of packets<br>• Supports tunnel and transport modes. |

© SANS Institu ll rights.

8 **Pros and Cons of authentication protocols**

Authentication is one of the essential elements in a security set up including VPN. (Reference 6) Authentication is the process to verify the identity of a user/device who is attempting to access the corporate resources such as application and data Types of authentication are listed below with the pros/cons. In high security environment, a combination of authentication can provide extra protection. For eg can have user ID/password and finger print scanning.

| Credential input devices (physical) | Method/protocol | Pros | Cons |
|---|---|---|---|
| User ID/password (what you know) | • Password authentication protocol (PAP), Challenge Handshake authentication protocol (CHAP)<br>• Password is hashed using MD5 in CHAP and clear text in PAP and sent over for verification | • Low cost<br>• PAP is supported by many operating systems | • Easy to crack using brute force techniques<br>• Need to use strong passwords which normally comprises of a minimum of 8 characters comprising of upper case, lower case, special and numeric characters. Users find these type of passwords difficult to remember and tend to write their passwords in stick pad and stick under the keyboard or behind the monitor.<br>• Users can deny that they accessed the resources |

© SANS Institute 2000 - 2005 Author retains full rights.

| | | | |
|---|---|---|---|
| One time password (token, what you know and have)) | • Proprietary | • Password is dynamic and cannot be reused<br>• Users need not remember the password<br>• Users cannot deny that they accessed the resources (similar to ATM card) | • Higher cost<br>• Users need to remember to carry token. |
| Biometrics (what you know, what you are and what you have) | • Compares finger print, voice, retina or iris pattern with one stored in Database | • Each pattern is unique<br>• Users need not carry a device like token or smart card<br>• This method of proving one's identity is very difficult to falsify | • Not matured yet<br>• Need a scanner<br>• Very high costs |
| Smart card (storing the private and public keys) | • Use PKI (Public key infrastructure)protocol(combination of symmetric and asymmetric keys) | • Secure as you need a password and smart card<br>• More user friendly as this could be integrated into credit card | • Higher cost<br>• Needs a smart card reader<br>• Effort required in administration of the keys |

9 **Pros and Cons of VPN location**

VPN device will be located at the corporate network site. VPN can be located in several ways in relation to the firewall. Pros/Cons of the various options is listed below:

| | Pros | Cons |
|---|---|---|

© SANS Institute 2000 - 2005 Author retains full rights.

| | | |
|---|---|---|
| VPN (behind firewall) | • Traffic is encrypted in public zone | • IPSEC packets will not be processed by firewall in PAT(Port address Translation) environment<br>• Firewall does not know the content of the packet as it is encrypted and therefore cannot enforce rules based on TCP/UDP ports<br>• VPN and firewall policies need synchronization so not to compromise security |
| VPN (in front of firewall) | • No IPSEC issue in relation to translation | • Traffic is decrypted before entering the firewall and information exposed in the public zone<br>• Firewall is unable to differentiate normal traffic from encrypted traffic and may require additional level of authentication at firewall for encrypted traffic |
| VPN (by the side with one leg to public internet and one to firewall) | • No IPSEC issue in relation to translation<br>• Firewall can differentiate and have specific rules for VPN traffic | • Routing of packets to and from internal LAN(local area Network)<br>• Firewall and VPN rules has to be synchronized |
| Firewall based VPN | • No IPSEC issue in relation to translation<br>• Firewall can differentiate and have specific rules for VPN traffic | • Firewall has to do encryption/decryption, which is CPU intensive activity. May impact performance |

10 **Pros/Cons of hardware/software/router based VPN**

The VPN function at the corporate site can be implemented through the following:

- Hardware based VPN
- Router based VPN
- Software based VPN

© SANS Institute 2000 - 2005 Author retains full rights.

Each option has its pros and cons and are as follows ( reference 7):

| | Pros | Cons |
|---|---|---|
| Hardware based VPN (dedicated) | • Has the computing power for IPSEC encryption and authentication<br>• Dedicated operating system and lesser vulnerabilities<br>• Suitable where both endpoints of tunnel are not controlled by same organization<br>• Suitable for high reliability and performance requirements | • Higher costs<br>• Additional device to be managed |
| Router based VPN | • Lower cost<br>• Can support hardware based encrypting | • Has to IPSEC encryption and authentication and may impact performance<br>• Not scalable |
| Software based VPN(firewall) | • Lower cost<br>• Support hardware based encrypting to reduce the load on the firewall | • Has to IPSEC encryption and authentication and may impact performance<br>• Mean time between failure(MTBF) is lower than hardware based VPN as it contains components like hard disk<br>• Uses standard operating system which are prone to attacks<br>• Requires patching to resolve vulnerabilities identified in operating system |

## 11 IPSEC protocol overview

It is important to understand IPSEC protocol in relation to key exchange, session setup, encryption and, authentication. This understanding will help in deciding the parameters for configuring the IPSEC devices.

© SANS Institute 2000 - 2005 Author retains full rights.

IPSEC comprises of Authentication header (AH), Encapsulating Security Payload (ESP) and Key Management Protocols. AH and ESP can be used together and separately in Tunnel and Transport modes. (reference 8)

In Tunnel mode, the IP header, TCP (Transmission control Protocol) header and the data payload are taken into account in the AH and ESP processing. In Transport mode, TCP header and the data payload are taken into account in the AH or ESP processing. When using AH and ESP together, AH should be in transport mode and ESP in tunnel mode. ESP should be carried out on the original IP packet in tunnel mode and then followed by AH in transport mode

The algorithm used in AH is **(**HMAC-MD5, HMAC-SHA1**).** The algorithm used in ESP is **(**DES, 3DES)

IPSEC uses the concept of Security association (SA). It contains information about AH or ESP security services. SA is identified by Destination IP address, Security Parameter Index (SPI) and type of AH/ESP service

ISA/KMP (Internet Security Association and key Management Protocol) is the protocol used to negotiate and establish one or more security associations.. The negotiation is carried out in 2 phases. In phase 1, authentication and establishment of ISAKMP SA is carried out. The channel can be considered secure when the two parties agree on how to protect phase 2 traffic. In Phase 2., Negotiation and establishment of IPSEC SA is carried out

Phase 1 has Main and Aggressive mode. Aggressive mode uses fewer transactions. Phase 1 negotiation includes authentication method, encryption and hash algorithm.

12 **Relationship of AH and ESP to tunnel and transport mode**

There are 2 modes in IPSEC protocol ( reference 9)
In Tunnel mode: inserts IPSEC data between new IP header and encapsulate IP packet
In Transport mode: inserts additional IPSEC data between IP header and TCP/UDP header

| | **Tunnel** (keeps original IP packet including the addresses/port number and encapsulates in a new IP header. | **Transport** |
|---|---|---|

© SANS Institute 2000 - 2005 Author retains full rights.

| | | |
|---|---|---|
| **IPSEC authentication header -AH (HMAC-**MD5,HMAC-SHA1**)** **(** Message authentication code-Message Digest 5), Message authentication code-secure Hash Algorithm) | • Authenticate IP datagram (static fields**)**<br>• No confidentiality<br>• Increase in processing time as it requires insertion of AH at sending end and validation at receiving end<br>• AH sequence number to provide playback protection<br>• AH header comprises of Next header, Payload length, security parameter index(SPI),sequence number and authenticated data checksum<br>• AH header is inserted between new IP header and payload | • Authenticate IP datagram (static fields**)**<br>• No confidentiality<br>• Increase in processing time as it requires insertion of AH at sending end and validation at receiving end<br>• AH sequence number to provide playback protection<br>• Insert authentication header between IP header and payload<br>• Does not work in NAT(Network Address translation) environment |
| **IPSEC encapsulated security payload –ESP (**DES, 3DES**)** (Data Encryption Standard**)** | • High confidentiality as the entire IP packet is encrypted including the IP addresses<br>• ESP contains SPI, sequence number field, Payload data<br>• ESP header is inserted between IP header and encrypted entire IP packet | • TCP/UDP data is encrypted<br>• ESP header is inserted between original IP header and encrypted IP payload<br>• Does not work in NAT environment |

13 **IPSEC issues**

IPSEC is a network layer protocol and it should be transparent to applications. However IPSEC based client in tunnel mode with ESP has problems when working through software and hardware proxies.(reference 10)

The proxies are doing a network port address translation (NPAT) on the IPSEC packet, It modifies some of the fields in the ESP header and therefore the receiving end is unable to process the IPSEC packet. Proxy vendors like Wingate are working on a solution.

There is also a issue when remote IPSEC client (set to transport mode with

© SANS Institute 2000 - 2005 Author retains full rights.

authentication header) is routed through a network address translation (NAT) device be it firewall or router. The NAT device modifies the source address of IPSEC packet. Upon arriving at the receiving end, the authentication data in the packet is invalid because the NAT device modified the IP header information.

To deal with this issue, VPN product vendors are releasing IPSEC NAT traversal capabilities into their products. Different standards and vendor implementations are being used to resolve this issue. The solution is based on some kind of IPSEC encapsulation into UDP packets. Because the IPSEC packet is now encapsulated, NAT devices do not affect the packet's IP header information and therefore IPSEC authentication data is still valid.

Some NPAT devices do not support multiple simultaneous IPSEC sessions. The sessions are IKE and IPSEC/UDP. Some NPAT devices use UDP port 500 for all IKE sessions even if there are multiple sessions simultaneously. This will only allow 1 session to work at any one time. If there is a second IKE session being initiated from behind the NPAT device, the first session will be terminated. The solution is to use NPAT device that maps additional sessions to unique ports. Cisco has come out with a solution based on encapsulating the IPSEC packets in TCP packets which each session having a unique TCP source port.

## 14 **Implementation checklists for setting up VPN**

The following activities should be carried out for successful VPN implementation:

- Assess remote access requirements like number of users, locations, countries, applications accessed
- Prepare a feasibility report and Get Management approval
- Design the VPN setup ( includes bandwidth sizing, hardware configuration and location of VPN server)
- Select appropriate IPSEC authentication, encryption , tunnel , Transport and Data Integrity parameters and prepare configuration document
- Prepare IP address assignment , routing changes and firewall rules to support VPN
- Install and Configure the VPN as per configuration document
- Test access to VPN and applications
- Monitor and Manage the VPN

## 15 Proposed VPN design

I have also included a proposed VPN design based on the above discussion. The design is based on information from (reference 4):

The key elements are:

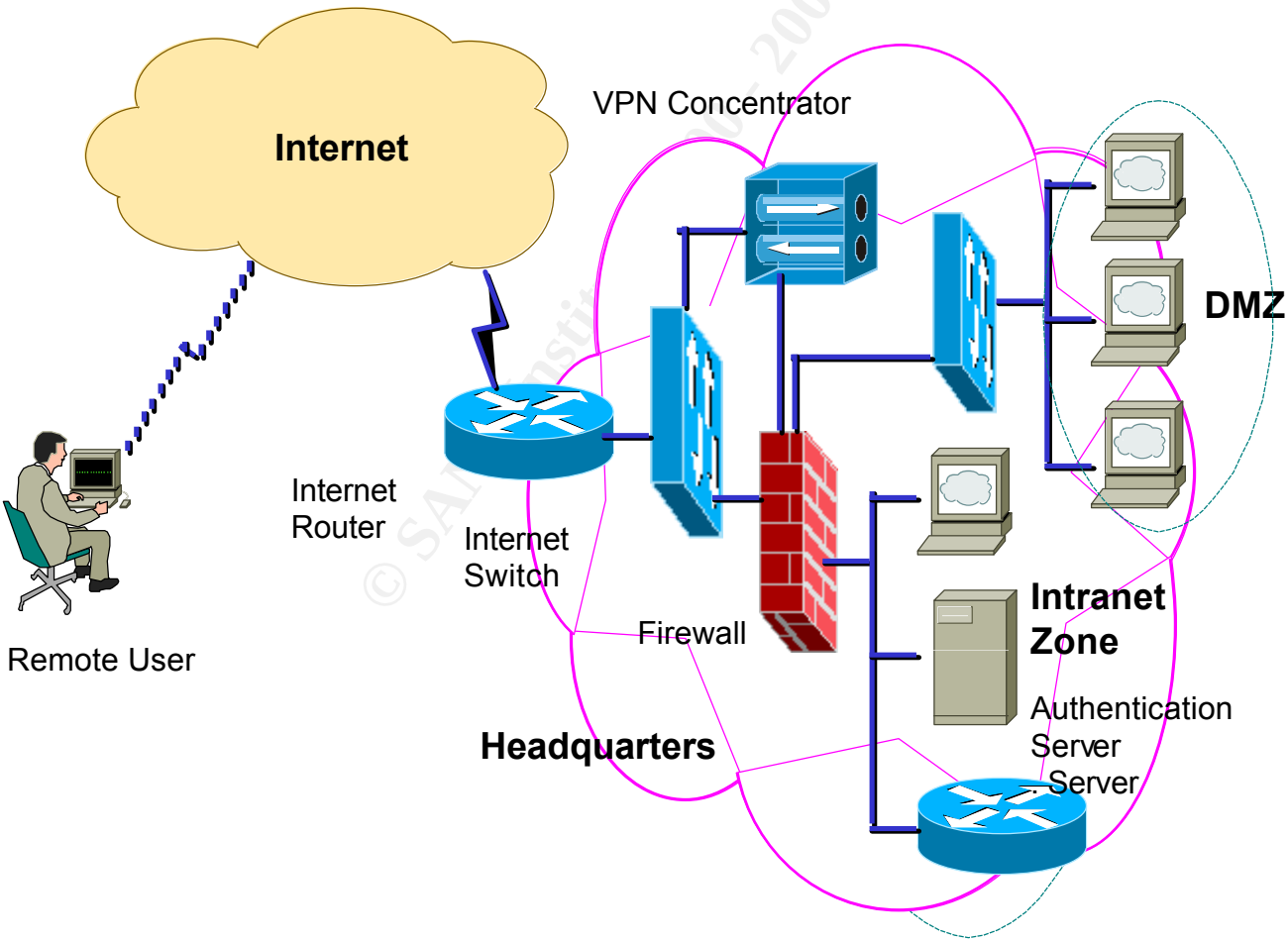
- Dedicated hardware based VPN server. I have selected Hardware based VPN

© SANS Institute 2000 - 2005, Author retains full rights.

as not to load the router or the firewall.

- VPN concentrator will be connected to the firewall and public Internet. All the packets from the VPN concentrator destined for the DMZ and Intranet will be inspected by the firewall as per the policies.
- IPSEC tunnel mode with ESP
- IPSEC software client for remote users
- Token based user authentication ( what you know and have)

The drawing is drawn on power point with the graphic symbols imported from Cisco template and (reference 4)




© SANS Institute 2000 - 2005, Author retains full rights.

## 16 Conclusion

Employees and business are increasingly using VPN. The VPN protocol is being widely used is IPSEC. IPSEC implementation is not compatible in PAT (port address translation) and NAT (Network address translation) environments. Meanwhile IPSEC Clients in tunnel mode with ESP works perfectly in NAT environment. IPSEC clients work perfectly in PAT environments in tunnel mode with UDP encapsulation.

## 17 References


1. Author unknown "White Paper IPSEC" Cisco July 1 2000
URL:
http://www.cisco.com/warp/public/cc/techno/protocol/ipsecur/ipsec/tech/ipsec_wp.htm (March 1 2002)

2. Mike Burgess "Computer Security (LV 142 A) " IWS Computer Security July 17 2001
URL: http://www.iwar.org.uk/comsec/resources/security-lecture/indes.html
(March 5 2002)

3. Sean Convery and Roland Saville "White Paper SAFE – Extending the Security Blueprint to Small, Midsize, and Remote-User Networks" Cisco January 11 2002
URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.htm (March 2, 2002)

4. Jason Halpern "White paper Safe VPN, IPSEC Virtual Private Networks in Depth" Cisco August 16 2001
URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm (March 1 2002)

5. Tina Bird "Virtual Private Networks Frequently Asked Questions" August 19, 2001
URL http://kubarb.phsx.ukans.edu/~tbird/vpn/FAQ.html ( March 2, 2002)

6. Deb Shinder "User access needs and data sensitivity drive authentication strategy" TechRepublic October 23, 2001


© SANS Institute 2000 - 2005, Author retains full rights.

URL:
http://www.techrepublic.com/printer/friendly.jhtml?id=r00220011023dls01.htm&rcode= ( March 5, 2002)

7. Tina Bird "Building VPNs: The 10-point plan" Counterpane Internet security No date
URL http://kubarb.phsx.ukans.edu/~tbird/tenpointplan.html (March 2, 2002)

8. Ghislaine Labouret " IPSEC: a technical overview " HSC June 16 2000
URL: http://www.hsc.fr/resources/articles/ipsec-tech/index.html.en (March 5 2002)

9. Egil Halvorsen & Rune Hansen "IPSEC based Virtual Private Networks (VPN)" Department of Computer and Information Science, Norwegian University of Science and Technology No date
URL:http://www.idi.ntnu.no/~runhan/project/report-html/ (March 2, 2002)

10. Edmund X Dejesus "VPNS: HANDLE WITH CARE" InfoSec World Conference & Expo 2002 March 18-20 2002
URL: http://www.infosecuritymag.com/articles/july00/features1.shtml (March 2, 2002)

11. Greg Marcott "Protocols serve up VPN Security" Network world May 31, 1999
URL: http://www.nwfusion.com/news/tech/0531tech.html (February 20, 2002 )

12. David Davis "Learn why NAT can cause VPN connection problems" TechRepublic Net Admin Nov 8, 2001
URL:http://www.techrepublic.com/article/.jhtml?id=r00220011026dad01.htm&src=bc
( February 26, 2002)

13. John McCormick "IPSEC and L2TP lead the Windows 2000 security lineup" TechRepublic NetAdmin Feb 2, 2000
URL:
http://www.techrepublic.com/article.jhtml?src=search&id=r00220000202eje02.ht
(March 5, 2002)

14. Jason Hiner "Configuring VPN connections with firewalls" TechRepublic NetAdmin Nov 8, 2000
URL: http://www.techrepublic.com/article.jhtml?id=r00220001108jim03.htm
(March 5, 2002)

© SANS Institute 2000 - 2005 Author retains full rights.

15. No author " PPTP and IPSEC dominate VPN protocols" TechRepublic NetAdmin Nov 20, 2001
URL: http://www.techrepublic.com/article.jhtml?id=r00220011120ern02.htm&src=bc (March 5, 2002)

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: September 21st, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| Rocky Mountain Fall 2017 | Denver, CO | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Copenhagen 2017 | Copenhagen, Denmark | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| SANS Baltimore Fall 2017 | Baltimore, MD | Sep 25, 2017 - Sep 30, 2017 | Live Event |
| Community SANS New York SEC401* | New York, NY | Sep 25, 2017 - Sep 30, 2017 | Community SANS |
| Community SANS Sacramento SEC401 | Sacramento, CA | Oct 02, 2017 - Oct 07, 2017 | Community SANS |
| SANS DFIR Prague 2017 | Prague, Czech Republic | Oct 02, 2017 - Oct 08, 2017 | Live Event |
| Mentor Session - SEC401 | Minneapolis, MN | Oct 03, 2017 - Nov 14, 2017 | Mentor |
| SANS Phoenix-Mesa 2017 | Mesa, AZ | Oct 09, 2017 - Oct 14, 2017 | Live Event |
| SANS October Singapore 2017 | Singapore, Singapore | Oct 09, 2017 - Oct 28, 2017 | Live Event |
| SANS Tysons Corner Fall 2017 | McLean, VA | Oct 14, 2017 - Oct 21, 2017 | Live Event |
| SANS Tokyo Autumn 2017 | Tokyo, Japan | Oct 16, 2017 - Oct 28, 2017 | Live Event |
| CCB Private SEC401 Oct 17 | Brussels, Belgium | Oct 16, 2017 - Oct 21, 2017 | |
| SANS vLive - SEC401: Security Essentials Bootcamp Style | SEC401 - 201710, | Oct 23, 2017 - Nov 29, 2017 | vLive |
| Community SANS Omaha SEC401 | Omaha, NE | Oct 23, 2017 - Oct 28, 2017 | Community SANS |
| San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style | San Diego, CA | Oct 30, 2017 - Nov 04, 2017 | vLive |
| SANS San Diego 2017 | San Diego, CA | Oct 30, 2017 - Nov 04, 2017 | Live Event |
| SANS Seattle 2017 | Seattle, WA | Oct 30, 2017 - Nov 04, 2017 | Live Event |
| SANS Gulf Region 2017 | Dubai, United Arab Emirates | Nov 04, 2017 - Nov 16, 2017 | Live Event |
| Community SANS Colorado Springs SEC401** | Colorado Springs, CO | Nov 06, 2017 - Nov 11, 2017 | Community SANS |
| SANS Miami 2017 | Miami, FL | Nov 06, 2017 - Nov 11, 2017 | Live Event |
| Community SANS Vancouver SEC401* | Vancouver, BC | Nov 06, 2017 - Nov 11, 2017 | Community SANS |
| SANS Paris November 2017 | Paris, France | Nov 13, 2017 - Nov 18, 2017 | Live Event |
| SANS Sydney 2017 | Sydney, Australia | Nov 13, 2017 - Nov 25, 2017 | Live Event |
| SANS San Francisco Winter 2017 | San Francisco, CA | Nov 27, 2017 - Dec 02, 2017 | Live Event |
| Community SANS St. Louis SEC401 | St Louis, MO | Nov 27, 2017 - Dec 02, 2017 | Community SANS |
| Community SANS Portland SEC401 | Portland, OR | Nov 27, 2017 - Dec 02, 2017 | Community SANS |
| SANS London November 2017 | London, United Kingdom | Nov 27, 2017 - Dec 02, 2017 | Live Event |
| SANS Khobar 2017 | Khobar, Saudi Arabia | Dec 02, 2017 - Dec 07, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Dec 04, 2017 - Dec 09, 2017 | Community SANS |
| SANS Munich December 2017 | Munich, Germany | Dec 04, 2017 - Dec 09, 2017 | Live Event |
| SANS Austin Winter 2017 | Austin, TX | Dec 04, 2017 - Dec 09, 2017 | Live Event |