BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Journal of Computer Science Research
https://ojs.bilpublishing.com/index.php/jcsr

ARTICLE

Secure Remote Access IPSEC Virtual Private Network to University Network System

Gajendra Sharma*

Department of Computer Science & Engineering, Kathmandu University, Dhulikhel, Kavre

ARTICLE INFO

Article history
Received: 28 December 2020
Accepted: 19 January 2021
Published Online: 31 January 2021

Keywords:
IPSEC
VPN
Network
Communication
Data
Encryption
Integrity authentication
Remote access
University
Security
Server
Client
Peer

ABSTRACT

With the popularity of the Internet and improvement of information technology, digital information sharing increasingly becomes the trend. More and More universities pay attention to the digital campus, and the construction of digital library has become the focus of digital campus. A set of manageable, authenticated and secure solutions are needed for remote access to make the campus network be a transit point for the outside users. Remote Access IPSEC Virtual Private Network gives the solution of remote access to e-library resources, networks resources and so on very safely through a public network. It establishes a safe and stable tunnel which encrypts the data passing through it with robust secured algorithms. It is to establish a virtual private network in Internet, so that the two long-distance network users can transmit data to each other in a dedicated network channel. Using this technology, multi-network campus can communicate securely in the unreliable public internet.

1. Introduction

With the wide availability of public connection like Internet, most universities are willing to provide their students and staff member access to centrally located servers and database remotely. In more specific cases, instructors are willing to perform and guide lab activities remotely. However, the use of internet increases network security threats and challenges. Due to these reasons, campus and departments under the universities implement a mechanism that uses encryption and tunneling protocols to make the communication between the central site (university) and remote clients (students or staff members) secure. This secure mechanism in general, is termed as Virtual Private Network or in short VPN. A VPN is an IP based model that makes use of encryption algorithms and tun-

**Corresponding Author:*
Gajendra Sharma,
Department of Computer Science & Engineering, Kathmandu University, Dhulikhel, Kavre;
Email: gajendra.sharma@ku.edu.np

DOI: https://doi.org/10.30564/jcsr.v3i1.2730

neling protocols and the entire connection can be a viewed as a secure pipe carrying encapsulated data over public network like internet [1].

The first and the easiest decision for every organization is to implement VPN for remote communication, however, there are several queries that needs to be addressed before its deployment. It needs to be understood on how many ways VPNs can be implemented and which one should be chosen depending on the requirements. An IPSEC provides permanent and always-on VPN access requirement [2]. It provides full access to all network devices, servers and other resources located on central site.

Internet Protocol Security provides secured communication between network-network, host-host, and network-host by authenticating and encrypting each IP packet of a communication session [3]. It uses the cryptographic keys to negotiate and protect communications over IP networks. It supports authentication, data integrity, data confidentiality [4]. People are still unaware of internet threats due to lack of sufficient knowledge in this technology of secured protocol IPSEC VPN.

Mainly, there are two types of IPSEC VPNs; Site-to-Site IPSEC VPN and Remote access IPSEC VPN. These two types of VPN can be utilized on the basis of requirements. The name of Site-to-Site VPN itself indicates the implementation of VPN between one site to another site. It is mostly used in those companies which have different branches situated in different location. An example of it can be a real life implementation of banking networks between head office to its branch offices. Similarly, Remote access IPSEC Virtual Private network is another VPN type which can be used when company resources need to be accessed anywhere and anytime.

1.1 Research Objective

The following are the main objectives of this study:

(1) Implementing RAIVPN by creating LAB environment in Packet Tracer or GNS3

(2) Provide remote access to only authorized personnel to various Networking devices located within the periphery of University

(3) Mitigating the overhead of sharing files and confidential data using the internet from both sides by providing remote access to remote users

1.2 Research Questions

Based on literature review and the present scenario of secured connection deployment in an organization to access the resources remotely and securely in Nepal and the current requirement to enhance the system.

(1) What will be the cost and benefits in the deployment of this technology in comparison to older system?

(2) Will this system deliver robust secured connectivity to remote users?

(3) What type of security algorithms will this system use for the encryption of entire IP Packets?

2. Literature Review

2.1 Evolution of Private Networks

Before the emergence and popularity, virtual private networks have gained as a secure and cheaper medium for sensitive information to be accessed and transmitted between two or more corporate network over a public network such as the internet, other network technologies have been innovated and used to connect within business sites and across to other sites that are miles away from each other [5]. The analog phone lines were permanently wired to the sites and were specially selected lines (called conditional lines) that were specifically built for full time use by companies; these lines are different from regular phone lines. This technology ensured full bandwidth and privacy but this came at a great cost, i.e. payment is expected for the full bandwidth even if the line was used or not. It is a Virtual Connection (VC) form of WAN packet switching which logically separates data streams. With this function, the service provider is able to send as many point-to-point VCs across a switch network infrastructure, depending each endpoints have a device that facilitates communication in the site. The components for setting up this kind of technologies involved the use of customer IP routers (customer premise equipment, or CPE) interconnected in a partial or full mesh of frame relay or ATM VCs to other CPE devices, in other words less equipment are needed for its set up.

With the advent of the internet and its wide use in everyday transaction, businesses have adopted the technology for transmitting and accessing data across various sites by implementing a VPN connection, which is relatively cheap, flexible and scalable, between both sites in order to secure the data that are sent across the insecure internet from being tampered by unauthorized persons.

The use of public telecommunication infrastructure to provide secure communication between members of certain groups (like company headquarters and its branches), maintaining privacy by the use of tunneling protocols and security procedures instead of dedicated physical connection, is known as Virtual Private Network or in short, VPN [1].

A VPN gateway which can be a router, VPN Concentrator or other Security Appliance is used to encapsulate and

 DOI: https://doi.org/10.30564/jcsr.v3i1.2730

encrypt all outbound traffic over the VPN tunnel through the internet to the VPN gateway at the remote target site. Once the remote VPN gateway receives the TCP/IP traffic, it strips the header, decrypts the packets and relays it to the destined hosts in its network [6]. Before the introduction of IPSEC, there were widespread problems with IP address spoofing and data integrity, authenticating and guaranteeing confidentiality of information. IPSEC is generally considered a "means by which to ensure the authenticity, integrity, and confidentiality of data at the network layer of the Open System Interconnection (OSI) model. In other words the IPSEC protocol was developed to ensure that users could communicate more securely over the internet [7].

2.2 Authentication, Authorization, and Accounting (AAA)

Limitations with passwords remain the simplest form of authentication. Cisco devices can be limited using a login name and password on console, vty and aux ports. However, these are considered as least secure means of security. Password only logins are considered even more vulnerable to brute-force attacks, an attack which involves the entry of all possible combination of password in order to find the correct one [6].

2.3 Internet Protocol Security (IPSEC)

IPSEC is the framework of open standards for a set of Internet Protocols (IP) responsible for secure communication. It relies on existing algorithms to implement the encryption, authentication and key exchange [8]. Cisco has been the leader in proposing and implementing IPSEC as a standard (or set of standards and technologies) for Remote Access VPNs [9].

Authentication Header (AH)

AH is also known as IP protocol 51 and is implemented when confidentiality is not required or permitted. It provides authentication for as much of the IP header as possible, as well as for upper level protocol data. But some IP header fields may change in the transit and the value of these fields may not be predictable by the sender. Such values of the fields cannot be protected by AH. Thus, the protection provided by AH is only partial in many cases. AH can be implemented alone or in combination with Encapsulating Security Payload (ESP) [9].

2.4 The IPSEC Framework

IPSEC works at the Network layer, and is responsible for protecting and authenticating the IP packets between participating IPSEC devices (peers). Earlier, security measures were implemented on Layer 7 of the communication model. IPSEC can protect virtually all application traffic because protection can be implemented from Layer 4 through Layer 7. IPSEC is especially used to implement Virtual Private Networks and for remote user access. One of the big advantages of IPSEC is that, security arrangement can be handled without the requirements of much hardware and software in remote user PCs.

(1) Confidentiality

Confidentiality is achieved using different encryption algorithms. The degree of security depends upon the length of the key of the encryption algorithm used. The following are some encryption algorithms and key lengths that VPNs use [10].

(2) Asymmetric Encryption

It is used when private keys are used to decrypt data, while public keys are used to encrypt data. First public keys, which are mathematically similar to the private keys, are exchanged. These public keys are used to encrypt data which is sent to the individual. The individual may then use their private key to decrypt the data. This form of encryption is considered more secure [7].

(3) Security Key Exchange

Any method in cryptography, by which cryptographic keys are exchanged between users allowing the use of cryptographic algorithm, is known as Secure Key Exchange method. The Diffie-Hellman (DH) algorithms is one of the cryptographic algorithms used to provide public key exchange method for two peers to establish a shared secret key that only they know even if they are communicating over an insecure channel (Microsoft TechNet, n.d.). To put simply, DH is typically not used to encrypt data, but in VPN implementations, they are used to share keying information securely, such as DES, 3DES, AES, SHA, MD5 and other symmetric keys as described above in this section, across an insecure public network, like the internet. Figure 2.5-1 describes how DH algorithm works. It uses six distinct steps to share symmetric keys across an insecure network [11].

2.5 Internet Security Association and Key Management Protocol (ISAKMP)

Internet Security Association and Key Management Protocol (ISAKMP), protocol defines the procedures for authenticating a communicating peer, creation and management of Security Associations (SAs), key generation

DOI: https://doi.org/10.30564/jcsr.v3i1.2730

techniques, and threats mitigations [12]. It defines procedures and packet formats to establish, negotiate, modify and delete security association. It also defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism. ISAKMP typically utilizes Internet Key exchange (IKE) for key exchange [13]. Security Association and Internet Key exchange are briefly described in the following sub-section.

2.6 Transform Sets

A combination of individual IPSEC transforms designed to enact a specific policy for traffic is known as transform set. The peers of VPN use particular transform set for protecting a particular data flow during the ISAKMP IPSEC SA negotiation that occur in IKE process.

Transform set consists of combination of AH transform, an ESP transform and the IPSEC mode (either transport or tunnel). The IPSEC SA negotiation uses the transform set that is defined in the crypto map entry to protect the data flows that are specified by Access lists of that crypto map entry. The command that invokes crypto-transform configuration mode is [6]:

Standard Access Lists

Standard Access Lists range from 1 to 99. They allow or deny traffic from specific IP addresses (i.e. based on source). These are used to filter traffic based solely on layer 3 source of information [6].

2.7 Firewall

A system or a group of systems that enforces an access control policy between networks is known as a Firewall. A Firewall can be implemented in different ways but all firewalls have some common properties. For example:

(1) A firewall must provide resistance to attacks

(2) It must be the only transit point between the networks i.e. all traffic must flow through the firewall

(3) A firewall should enforce the access control policy

Split tunneling also has a major disadvantage if implemented, the VPN will be vulnerable to attacks as it be accessible over public network i.e. (Internet) through the same endpoint device [14].

Dhall et al. [15] have proposed a working principle implementation of IPSEC in various network devices (hosts and routers). Their research was focused on AH implemented and ESP implemented data packets. When comparing the time difference with AH implemented and without AH implemented data packet for variable number of nodes, compared to a lower number of total nodes (3-11) versus higher number of nodes (11-15), time difference when delivering the packets differs considerably; but for the extra time, all users in the network can get authentication service for all data packets in ad-hoc network. When comparing the time difference with ESP implemented and without ESP implemented data packets, the time difference varies slightly. Their findings showed compared to AH, ESP has more timing overhead and the time difference between ESP implemented packets is higher than AH implemented packets. However, the service provided with ESP implemented packets is more than AH implemented packets.

Qu et al. [16] have presented the results of the sub-project within the Secure Active VPN Environment (SAVE) project conducted at Dalhousie University. The principal objective of the paper is to avail the design and implementation of a secure wireless LAN based on the IPSEC VPN tunneling protocol and explore its performance to render inherently vulnerable wireless communication more secure, VPN technology was used in this project. An IPSEC-compliant VPN was constructed and the traffic between the wireless node and the IPSEC gateway was protected in the IPSEC tunnel. PGP certification, an instance of the PKI referral method, was used to provide a strong binding between the public key and its attributes so the receiver could verify that the sender was as claimed to be without asking the sender. For the completeness of this solution, the relationship of a packet filter firewall and an IPSEC gateway was deployed on the basis of FreeSiWAN and IPCHAINS on the Linux operating system with kernel 2.2.x. The whole system made the wireless communication effectively secure.

Sun [17] deliberated the comparison analysis between IPSEC & SSL VPN from the aspects of benefits, working layers, security, access control and deployment. Analysis has indicated some pros of SSL VPN in security, flexibility, and cost reduction which have become the reasons of selection of it as the remote access way in HengShui University. On the other hand, the differences between access-control, working layers and encryption from client's web browser to the web server behind the VPN server, no need of VPN client software, and deployment of IPSEC and SSL VPN has been shown the best approach with respect to SSL VPN.

Apart from positive aspects of IPSEC VPN, this paper has concluded in the favor of easy working process by SSL VPN for remote access. It has been shown that SSL VPN has become better option for remote access while IPSEC VPN has become well suited for site-to- site VPN.

 DOI: https://doi.org/10.30564/jcsr.v3i1.2730

Lee et al. [18] have stated the secured connectivity to corporate networks for IPV6 mobile users remotely and securely through the means of IPSEC VPN under the consideration of near future. They have proposed the efficient communication procedure by considering two cases for mobile user's VPN access. One case is for the internal home agent that exists in VPN domain and the other is the case for external home agent which is away from VPN domain.

The paper approached that the communication packets within the private network doesn't need to be protected as VPN tunnel cares for it and the communication packets which is not in the private network needs to be protected by establishing IPSEC tunnel. Finally, it has made the conclusion on efficient communication with mobile nodes and VPN gateway by the use of IKEv2 initial exchange and IKEv2 informational exchange.

Kim et al. [19] have addressed the problem of disruptions to applications due to IPSEC tunnel re-establishment during the mobility of MobileIP and so made some general modifications in an IPsec implementation without compromising its security parameters.

They have experimentally shown by removing the dependence of identifying a Security Association on the outerheader destination address so that the same security parameters can be used even in the new network. Two new private messages are added to ISAKMP to enable the required signaling to update new tunnel endpoint addresses. Routing Table of new mobile host has been updated for existing IPsec tunnels which need to be sent through a new network.

Removing the dependency of tunnel destination address for locating SA without affecting the normal IPsec operations, and adding two messages to ISAKMP to communicate the address changes of mobile hosts, prompting proper updates to Security Associations Database (SAD) have been presented to mitigate the issues of interruptions in network applications for MobileIP.

Lakbabi et al. [20] presented the differences between protocols strengths and weaknesses from a security and management perspective of IPSEC and SSL VPN technologies. They have briefed the general overview of all the layer 2 VPN technologies which have got no encryption mechanism, and so, IPSEC and SSL VPN has been the topic of discussion in this paper. Some weakness and issues of IPSEC that has been mentioned are dynamic addressing,

NAT/PAT, opened ports of 50(ESP), 51(AH), and 500(ISAKMP) for IPSEC needed to be allowed in comparison to only 443(HTTPS) for SSL, tunnel establishment of N(N-1)/2 tunnels with N sites, flexible and granular access control to network resources.

SSL VPN is strong security protocol from the aspects of security, mobility, and management in comparison to IPSEC VPN presented in this paper has made the decision to go ahead for SSL VPN in future.

It has been revealed that IPSEC VPN even though the greater solution for security has become resource intensive and cost prohibitive such as requirement of client-side software, public key infrastructure deployment, technical complexity, and more infrastructure overhead when deployed across large enterprise.

It has been indicated that even though IPSEC has got several issues in comparison to SSL VPN, it is a solution to large problems as it can be deployed incrementally, ability of dictating the requirement of current antivirus and firewall software and to ensure the operating systems are patched virtually eliminating the risk of malicious intent, and the requirements of VPN client software reducing the risk of security breach.

3. Methodology

3.1 System Overview

Since there is a lack of system in place which is capable of providing access to the resources for students, pro-

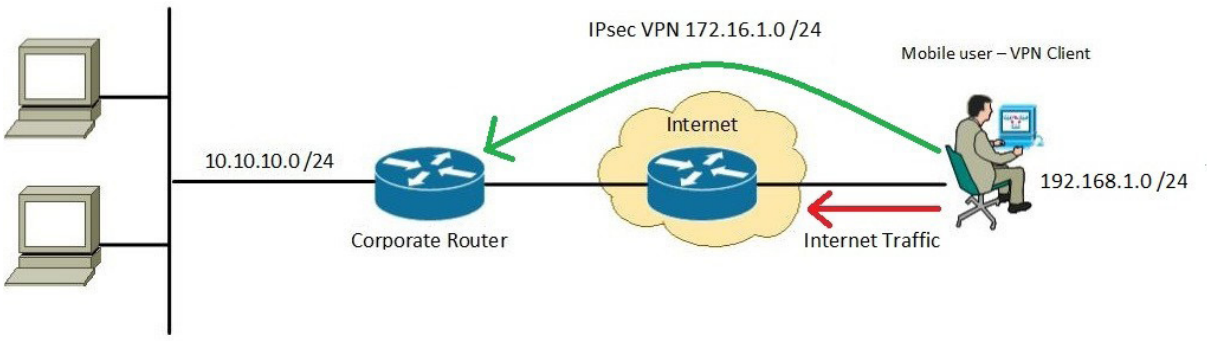

Figure 1. Remote Access IPSEC VPN

DOI: https://doi.org/10.30564/jcsr.v3i1.2730

fessors, and staffs from universities to its affiliated colleges of Nepal, a system design has been proposed regarding the design and implementation of remote access IPSEC VPN through the public network to access the resources securely and remotely.

This section is about the lab implementation of Remote Access IPSEC VPN Server performed in Graphical Network Simulator (GNS3) emulator emulated along with the internet for the universities/colleges. This system has been designed and built in GNS3 software connected with Internet. The main scope of this research is to demonstrate the access to the enterprise resources remotely and securely. Since it is needless to have physical lab setup for the implementation of this system, it has utilized the GNS3 tool and Virtual Box.

This study mainly describes about providing network access to Universities' resources from outside network i.e. internet securely. All the traffic before entering to inside network is encrypted and encapsulated first at client side. There after it is sent to VPN Server over the internet and upon receipt, it decrypts the content and relays the packet toward the target host inside its private network only when the security parameters matches between VPN Server and VPN Client. The main purpose of this demonstration is to provide the access to universities stuff located inside the server to only rightful personnel remotely and securely.

This Network System has been designed based on Local Area Network (LAN) and Wide Area Network (WAN) which means inside and outside network of a campus respectively. In this system, Figure demonstrates Router R1 is playing a role of VPN Server which performs its job of securing the access to inside network from undesirable network traffic coming from outside network. It is also acting as a DHCP Server which provide IP addresses to VLAN_B dynamically.

R1 consists of 3 Fast Ethernet interfaces fa0/0, fa1/0, fa2/0 in which one of its interface fa2/0 is further divided into two sub interfaces fa2/0.5 and fa2/0.10 which are connected as two local area networks VLAN_A for the campus servers and VLAN_B for other representatives of a campus respectively whereas other two remaining interface fa0/0 and fa1/0 are connected to internet and one remote user respectively. In order to access the inside network of a campus for users, they need to cooperate with VPN Server first with correct security parameters. If it corresponds to the configured parameters at R1 then only authorized users and devices will get access to the private networks.

3.2 System Specification

Deployment of this system needs the hardware and software on the basis of minimum requirement of enterprise networks. VPN Routers and Switches can be taken from other vendors too which is capable of supporting RAIVPN. In order to make user friendly and ease of this system installation and deployment, following network devices and applications have been used for the configuration of RAIVPN.

(1) VPN Server is a 7200 router (VXR) that runs Cisco IOS Software Release 7200 Software (C7200-ADVIP-SERVICESK9-M), Version 15.2(4)S5, RELEASE SOFT-

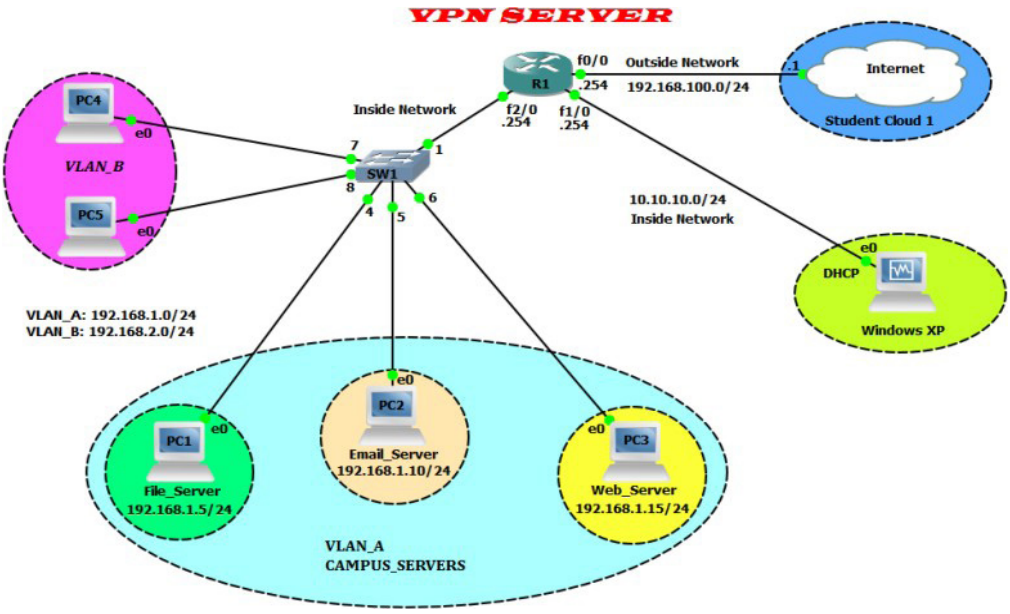

Figure 2. Remote Access IPSEC VPN System

 DOI: https://doi.org/10.30564/jcsr.v3i1.2730

Table 1. Prerequisite Commands to Configure VPN

Feature	Requirement	Configuration Example
Secure access	SSH and HTTPS	Router(config)# **ip http secure-server** Router(config)# **ip http authentication local** Router(config)# **line vty 0 15** Router(config)# **login local** Router(config-line)# **transport input ssh** Router(config-line)# **transport output ssh**
Non- Secure access	Telnet and HTTP	Router(config)# **ip http server** Router(config)# **ip http authentication local** Router(config)# **line vty 0 15** Router(config)# **login local** Router(config-line)# **transport input telnet** Router(config-line)# **transport output telnet**
User privilege level	15	Router(config)# **username admin privilege 15 secret 0 admin**

WARE (fc1). Cisco Routers 800, 1700, 1800, 2800, 3600, etc. are also supported by VPN Server with IOS release of 12.2 (9) T or later.

(2) Cisco Layer 2/3 Switch for configuring LAN networks

(3) Cisco Configuration Professional (CCP) v 2.6

It is Graphical User interface based application to login and configure the routers. Command Line Interface (CLI) can also be used to access the routers through:

(1) Putty (for both console and telnet)

(2) Secure CRT (for both console and telnet)

(3) Hyperterminal (for console)

To run Cisco CP, a router configuration must meet the requirements shown in Table 1.

(1) Cisco VPN Client Software

(2) Web Browser, Java Runtime Environment (JRE), and Flash Player

(3) Several Web browsers are supported by CCP

Internet Explorer 6.0 and later versions

(4) The following JRE is supported by CCP

Java version "1.6.0_11"

JRE Settings for Cisco CP

It is a network emulation software which is used to design and build the networks without the requirement of hardware. It runs the operating system (OS) of networking hardware from multiple vendors which supports in emulating the real behavior of real network and is free as well. It can be connected with real network too which means the networking devices configured on the GNS3 can connect with Internet. The version of this tool is 1.3.11. Following

are some minimum requirements to install this software in PC.

Table 2. PC Requirements to Install GNS3

OS	Windows 7 (32/64 bit) and later, Mavericks (10.9) and later, Any Linux Distro - Debian/Ubuntu
Processor	Core 2 Duo and later release
Memory	2 GB RAM
Storage	1 GB available space for installation and store networking hardware's OS

(5) PC System Requirements

Table lists the system requirements for a PC running

DOI: https://doi.org/10.30564/jcsr.v3i1.2730

Table 3. PC requirements for Cisco CP

System Component	Requirement
Processor	2 GHz processor or faster
Random Access Memory	1 GB DRAM minimum; 2 GB recommended
Hard disk available memory	400 MB
Operating System	Any of the following: (1) Microsoft Windows 7-32 and 64 bit (2) Microsoft Windows Vista Business Edition (3) Microsoft Windows Vista Ultimate Edition (4) Microsoft Windows XP with Service Pack 3-32 bit (5) Mac OSX 10.5.6 running Windows XP using VMWare 2.0
Screen Resolution	1024 X 768

Cisco CP

3.3 IP Addressing

In this network topology, Internet Protocol (IP) Addressing has been distributed statically and dynamically to LAN and WAN networks. Table shows the IP Addresses assigned to router, host PCs, and Internet Cloud.

Table 4. IP Address assignment to Router R1

IP DISTRIBUTION_R1			
LAN Interface (Inside)		**WAN Interface (Outside)**	
Fa 2/0.5	Fa 2/0.10	Fa 0/0	Fa 1/0
192.168.1.254 /24	192.168.2.254 /24	192.168.100.254 /24	10.10.10.254 /24

Table 5. IP Address assignment to host PCs

IP DISTRIBUTION_ LANs	**LAN_A (SW 1)**	PC 1	192.168.1.5/24
		PC 2	192.168.1.10/24
		PC 3	192.168.1.15/24
	LAN_B (SW 2)	PC 4	DHCP
		PC 5	DHCP

Table 6. IP Address assignment to LAN and VBOX PC

IP DISTRIBUTION_WANs	**WAN_A (LAN Adapter)**	192.168.100.11/24 (DHCP) GW: 192.168.100.1
	WAN_B (VirtualBox_ 192.168.56.1)	10.10.10.1/24 (DHCP) GW: 10.0.2.1

Dynamic NAT with overload for single public IP address has been implemented on the VPN router in order to minimize the cost by utilizing only single public IP address Internet connection to the LAN hosts. The following table shows the NAT configuration done in VPN Server R1.

The following table illustrates the IP address translations after a host 192.168.2.1 reaches www.google.com.

If we observe the Internet Control Message Protocol (ICMP) from the table above, the inside global address of the host that just issue a ping command, is 192.168.100.254. This is the IP address to which the outside network is addressing the particular inside host, even though its exact IP address is the inside local 192.168.2.1.

 DOI: https://doi.org/10.30564/jcsr.v3i1.2730

Table 7. Output of NAT Translations

SERVER#show ip nat translations				
Pro	**Inside global**	**Inside local**	**Outside local**	**Outside global**
udp	192.168.100.254:4501	192.168.2.1:14503	192.168.100.1:53	192.168.100.1:53
icmp	192.168.100.254:1024	192.168.2.1:17169	202.166.193.159:17169	202.166.193.159:1024
icmp	192.168.100.254:1025	192.168.2.1:17425	202.166.193.159:17425	202.166.193.159:1025
icmp	192.168.100.254:1026	192.168.2.1:17937	202.166.193.159:17937	202.166.193.159:1026
icmp	192.168.100.254:1027	192.168.2.1:18193	202.166.193.159:18193	202.166.193.159:1027
icmp	192.168.100.254:1028	192.168.2.1:18449	202.166.193.159:18449	202.166.193.159:1028

All the hosts are in this way provided access to the internet using one public IP address 192.168.100.254.

3.4 System Verification

This section presents the verification of different properties of IPSEC VPN Server for the proposed system. It has been further divided into two sub categories to verify the secured network connectivity established from the clients to the VPN server through VPN tunnel. The verification of this system has been done from two sides of this system which are server and client side. The demonstration of this system verification has been presented after one of the client has been able to connect to the VPN Server and sending and receiving the network packets through VPN Tunnel successfully.

3.5 VPN Server

In the above figure, the responsibility of VPN server is playing by Cisco router named asVPN server. It is connected to one switch which has been distributed to two LANs. One is at the network of 192.168.1.0/24 whereas other is at 192.168.2.0/24. Since the servers of enterprises have to be secured, they have been separated from other networks. It is connected to the Internet through Fa0/0 interface. All the PCs in inside networks has access to the Internet even servers too. The main scope of this section is to show the secured connection established by remote users through VPN tunnel.

Following figure represents the VPN connection between VPN server and Remote client.

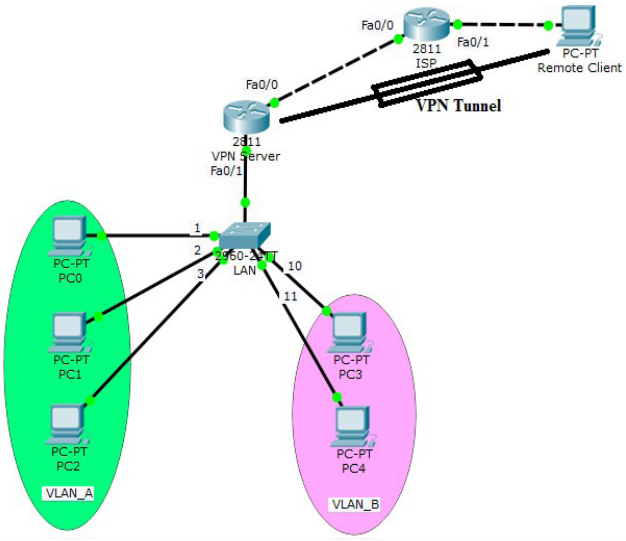

Figure 4. VPN Tunnel Connectivity between VPN Server and Remote Client

3.5.1 IPSEC User Authentication, Accounting, and Authorization (AAA)

Before going to look after IPSEC VPN establishment, it needs to define authentication credentials for the remote users who are associated with the company. It has defined two users who are Ram as a student and John as a professor who has been associated with two group student and professor respectively. Below table depicts the authentication credentials configured for remote user Ram and John on VPN server.

DOI: https://doi.org/10.30564/jcsr.v3i1.2730

Table 8. Username and Password Configuration in CLI mode

```
EZVPN_SERVER#sh run | s username
username ram@student privilege 15 secret
5 $1$aHpU$lcOW3C6ITBIYDEmhsaJhg/
username john@professor privilege 15 secret 5
$1$pfMe$nOk54rtQq35iGDk5j4rJt1
```

To hide the password, the password set for users has been encrypted.

3.5.2 Peer Establishment Verification

It is to show that remote user has established VPN connectivity by negotiating the security associations with VPN server. The two figures mentioned below illustrates that the remote peer 10.10.10.1 has successfully connected to VPN server through VPN tunnel and the two commands verify the currently established VPN tunnel from a remote peer.

Show crypto isakmp sa

It shows the current Internet Security Association Key Management Protocol (ISAKMP) Security Associations (SAs) built between peers. In this figure, the output simply tells that an IPSEC tunnel has been successfully created between 192.168.100.254 as the source tunnel point and destination 10.10.10.1 as tunnel end point. The state QM_IDLE states that the tunnel is up and the IKE SA key exchange is successful and is now actively ready to transfer the data through the tunnel.

4. Discussion

In this section, the discussions has been carried out in the analysis of secure remote access IPSEC VPN during the implementation of it in GNS3 emulator. It also argues on the problems and limitations in the designed system.

This network system has been designed in one laptop machine where an emulator GNS3, CCP has been installed. This system has been designed based on the real time network in enterprises analogy. Here, the enterprise networks has been designed in GNS3 which works with LAN adapter connected to the Internet through the laptop machine. Two remote users have been assigned to connect to the VPN server one from virtual PC where it has its operating system in Virtual Box and other is from another laptop which is connected to the same Internet.

4.1 Summary of Results/Findings

A secured system has been developed on the basis of deploying secured network system to the existing network infrastructure of the Universities/Colleges and Enterprises. This system has been realized in GNS3 emulator for the instance with three servers in one private network and others in another private network for professors, students, and IT admins. It is built with additional security to the existing trends of network system in Institutional Organization. The developed system is analogous to the current network system of Universities. Considering GNS3 system as the network system of Universities, the edge router is the VPN server which is directly connected to the Internet and two remote users, professor and student are connected to the same Internet. It means that, with no VPN connection, any user whether the users from within the University or outside only has access to visit the website of University. Access to the file server and email server is restricted to anyone, except the IT admin for the purpose of security. For remote users to access the file server through the Internet, they must have VPN user credentials which should be matched with VPN server to establish VPN tunnel. Following results have been carried out after the establishment of IPSEC tunnel successfully:

(1) Remote User "Professor" has access to the file server only and at the same time they have been provided access to the Internet as well. All the traffic except the Internet that is destined for file server will be traversed through the VPN tunnel.

(2) Remote User "Student" doesn't have access to the Internet and other servers except to the file server during the data traffic flow via VPN tunnel because of various security risks in order to secure the system from Trojans and other viruses.

(3) The Network throughput is slightly lower for tunneled traffic in comparison to non-tunneled traffic due to the overheads of encryption but not much variations was faced in the speed of data flow.

(4) Three virtual PCs have been deliberated as real servers for the system and access verification has been realized through ICMP reachability, which performed successfully after the VPN connection.

(5) Finally, it has been concluded that user professor who has access to the Internet, and student that doesn't have Internet connection during the VPN connection are able to connect to the VPN server and File server remotely and securely successfully which is the main goal of this research work.

4.2 Contributions

The main scope of this system development is to contribute the secured remote access operations to enterprise network system from anywhere/anytime for only the

 DOI: https://doi.org/10.30564/jcsr.v3i1.2730

associated members of that organizations. Following contributions have been deliberated on the deployment of this secured system:

(1) Everyone can access the organizational network devices and server remotely and securely from anywhere/anytime depending on whom the authority has been provided in comparison to the current unsecured network system of Universities and Colleges

(2) It is extremely strong in security for which no one has to hesitate in deploying this system

(3) System Administrators can manage the internal system from anywhere/anytime

(4) Professors can assign the class activities, upload the assignments, evaluate the performance of students from home Internet

(5) Students who will be unable to show their presence in the class due to the personal problems can study, remotely access to the assignments and lab activities of that day from anywhere/anytime securely

(6) It offers no such vulnerabilities and risk factors from the outside attacks like man-in-the-middle attack, DoS attack if configured properly with correct security attributes

4.3 Limitations

(1) It is required to have Cisco IOS software release 12.3 (11) T or later

(2) It needs VPN client software at remote users PC to authenticate and pass the security attributes to them

(3) Cisco Easy VPN IPSEC server works only for Cisco IOS Router, ASA, and PIX. It doesn't work for the devices from other vendors

(4) The issues with IPSEC VPN are implementation issues, packet overhead, and processing overhead

(5) The encryption and decryption services on the hundreds of megabytes of data flowing through the equipment requires quite a bit of processing power and which leads to higher processing loads

(6) It is time consuming for the system administrators to configure individual and group access rules

(7) If it is lightly configured, meaning if no valid certificates are used, then it poses a huge security risk

5. Conclusion and Future Work

Remote Access IPSEC VPN allows remote users in different locations to establish secure connections with universities network. These users can access the secure resources on that network as if they were directly plugged into the network's servers. In the University, students can easily access the e-library resources, class notes, assignments and so on very securely from their home. It mitigates the risk factors of sharing confidential information between professors and students publically. It solves the technical problem of knowledge sharing and resource sharing, and really plays the library role in the sharing and popularity of knowledge and resources in the whole society.

Cisco Systems have provided customers with easy to use software tools that assist system administrators. Firewalls and VPN server configuration using Cisco CCP tool is smooth and simple. Most essentially, remote client configurations and setup is not much technical, so it can be easily configured by general user once the required authentication information is provided.

References

[1] Kajal, R., Saini, D., Grewal, K. Virtual Private Network. International Journal of Advanced Research in Computer Science and Software Engineering. 2012, 2(10), Retrieved from: http://www.ijarcsse.com/docs/papers/10_October2012/Volume_2_issue_10_October2012/V2I900209.pdf

[2] Sastry, A. IPSec VPN vs. SSL VPN: Comparing respective VPN security risks. 2011. Retrieved from TechTarget: http://searchsecurity.techtarget.com/tip/IPSec-VPN-vs-SSL-VPN-Comparing-respective-VPN-security-risks

[3] Clayton, N., Pandya, H. M. VPN Over IPSEC. In FreeBSD Handbook, 2016: 742. Retrieved from: https://www.freebsd.org/doc/handbook/ipsec.html

[4] Kang, B., Balitanas, M. O. Vulnerabilities of VPN using IPSec and Defensive Measures. International Journal of Advanced Science and Technology, 2009, 8: 9-18.

[5] Ssycxz. Overview of VPN - Evolution of Private Networks, 2016. Retrieved from: http://ssycxz.kinja.com/overview-of-vpn-evolution-of-private-networks-1763248734

[6] Cisco Systems. CCNA Security Course Booklet Version 1.0. Indianapolis: Cisco Press, 2009.

[7] Powell, J. M. The Impact of Virtual Private Network (VPN) on Acompany's Network, 2010. Retrieved from: http://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1056&context=honors

[8] Singh, Y., Chaba, Y., Rani, P. Integrating - VPN and IDS - An approach to Networks Security. International Journal of Computer Science and Security, 2007, 1(3): 1-13. Retrieved from:

DOI: https://doi.org/10.30564/jcsr.v3i1.2730

http://www.cscjournals.org/

[9] Rouse, M. IPsec (Internet Protocol Security), 2010. Retrieved from TechTarget: http://searchmidmarketsecurity.techtarget.com/definition/IPsec

[10] Rehman, M. H. Design and Implementation of Mobility for Virtual Private Network Users. Global Journal of Computer Science and Technology Network, Web & Security, 2013, 13(9): 34-39. Retrieved from: https://globaljournals.org

[11] Deal, R. Key Exchange. Retrieved from The Complete Cisco VPN Configuration Guide, 2005: http://www.fengnet.com/book/vpnconf/ch02lev1sec4.html

[12] VelMurugan. What is ISAKMP, 2008. Retrieved from: http://discuss.itacumens.com/index.php?topic=32692.0

[13] Maughan, D. Internet Security Association and Key Management Protocol (ISAKMP), 1998. Retrieved from: https://tools.ietf.org/html/rfc2408

[14] Oliver, P. G. Making Sense of Split Tunneling. Retrieved from Infosec ISLAND, 2013: http://www.infosecisland.com/blogview/22859-Making-Sense-of-Split- Tunneling-.html

[15] Dhall, Batra, Rani, a. Implementation of ipsec protocol. 2012 Second International Conference on Advanced Computing & Communication Technologies, 2012: 176-181.
Rohtak: IEEE. DOI: 10.1109/ACCT.2012.64

[16] Qu, W., Srinivas, S. IPSec-based secure wireless virtual private network. MILCOM 2002. Proceedings, 2002, 2, 1107-1112.
DOI: 10.1109/MILCOM.2002.1179632

[17] Sun, S. H. The Advantages and the Implementation of SSL VPN. 2011 IEEE 2nd International Conference on Software Engineering and Service Science. Beijing: IEEE, 2011: 548- 551.
DOI: 10.1109/ICSESS.2011.5982375

[18] Lee, H., Nah, J., Jung, K. The Remote Access to IPsec-VPN Gateway over. The 7th International Conference on Advanced Communication Technology, 2005: 567- 569. Taejeon: IEEE.
DOI: 10.1109/ICACT.2005.245934

[19] Kim, B.-J., Srinivasan, S. Simple Mobility Support for IPsec Tunnel Mode. 2003, 3: 1999-2003.
DOI: 10.1109/VETECF.2003.1285375

[20] Lakbabi, A., Orhanou, G., Hajji, S. E. VPN IPSEC & SSL Technology. 2012 Next Generation Networks and Services NGNS. Agdal: IEEE, 2012: 202-208 .
DOI: 10.1109/NGNS.2012.6656108