DESIGN AND IMPLEMENTATION OF A SECURE NETWORK CONNECTION OF THE UNIVERSITY

Thin Naing[1], Aung Nway Oo[2]

[1] *University of Information Technology, Myanmar*

ABSTRACT

A network security is the most vital component of a campus network design. Campus network faces the security challenges which are influenced by network infrastructure. Secured network will guard valuable data and information of an organization from security attacks associated with network. A university network has a various type of usages, such as teaching, learning, research, management, e-library, result publishing and connection with the external users. The university network needs to have security network design to protect from different types of threats and attacks. Most of organizations use physical firewalls and encryption mechanisms to adapt the security features of campus network. This paper provides a framework for implementing secure VPN connection with IPCop opensource firewall in campus network. According to the evaluation of the users' interview, the usage of this technique has become possible to provide cost effective, reliability and data integrity in secure data transmission.

Keyword - *VPN, Network Security, Firewalls, IPcop, Opensource. Reliability, Integrity*

1. INTRODUCTION

The evolution of networking and the Internet, the threats to information and networks have risen dramatically. Many of these threats have become cleverly exercised attacks causing damage or committing theft. Government and business critical applications become more prevalent on the Internet, there are many immediate benefits. However, these network-based applications and services can pose security risks to individuals as well as to the information resources of companies and government [1].

Network security is the most vital component in information security because it is responsible for securing all information passed through networked computers. To be successful in preventing information loss, must follow three fundamental precepts. First, a secure network must have integrity such that all the information stored therein is always correct and protected against fortuitous data corruption as well as willful alterations. Next, to secure a network there must be confidentiality, or the ability to share information on the network with only those people for whom the viewing is intended. Finally, network security requires availability of information to its necessary recipients at the predetermined times without exception. To fulfil the three perspective, the secure virtual private network (VPN) tunnel is one of the techniques in data communication. VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private "tunnel" to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet. Three types of devices router (with VPN features), Hardware firewall and software firewall are used to deploy the secure tunnel for remote user access [2].

Additionally, firewalls and encryption should be incorporated into a network to heighten its security. Firewalls are yet another measure used in increasing the level of security in a network. A firewall is an essence path through which information enters and exits. Without adequate protection or network security, many individuals, businesses, universities and governments are at risk of losing that asset [2].

Typically, these threats are persistent due to vulnerabilities, which can arise from mis-configured hardware or software, without using secure private tunnel, poor network design, inherent technology weaknesses, or end-user carelessness.

The system is proposed to design a secure VPN and a solution of implementing a Virtual Private Network over the university between its Head Office, ministry's office, staffs and students to access to various resources from remote places. The IPSec features of IPcop open source software firewall is used to configure a proposed design.

2. VPN – Virtual Private Network

A Virtual Private Network (VPN) extends a private network across a public network, such as the Internet. It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the public network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. Major implementations of VPN include Open VPN and IPsec [3].

VPNs need to provide the following four critical functions to ensure security for data:

- Authentication – validates that the data was sent from the sender.
- Access control – limiting unauthorized users from accessing the network.
- Confidentiality – preventing the data to be read or copied as the data is being transported.
- Data Integrity – ensuring that the data has not been altered.

There are two major types of VPNs: (i) remote access VPN and (ii) site-to-site VPN.

(i) Remote-access VPNs:

Some users might need to build a VPN connection from their individual computer to the corporate head office of organization (or to the destination, they want to connect to). This is referred to as a remote-access VPN connection. Remote-access VPNs can use IPsec or SSL technologies for their VPN [2] as shown in Fig - 1.

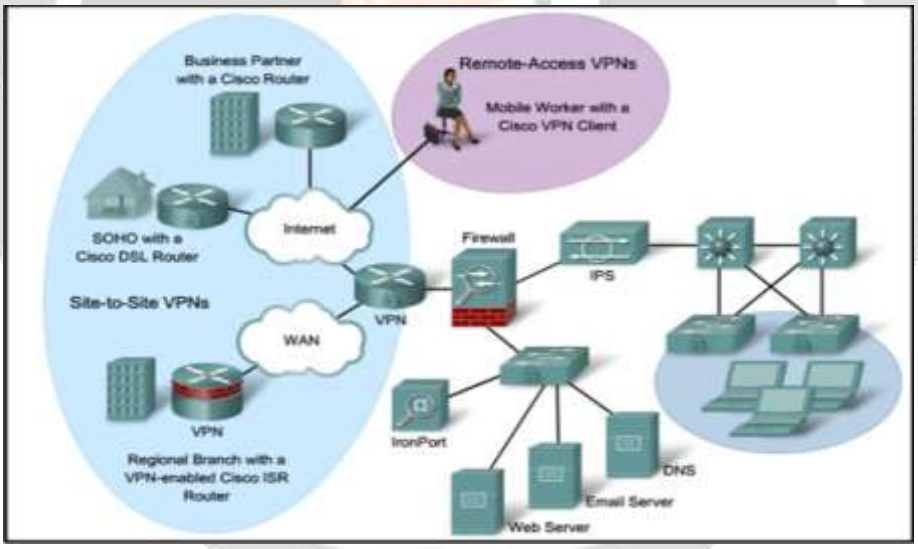

Fig - 1: Remote-access VPNs

(ii). Site-to-site VPNs:

The other main VPN implementation is by companies that may have two or more sites that they want to connect securely together (likely using the Internet) so that each site can communicate with the other site or sites. This implementation is called a site-to-site VPN. Site-to-site VPNs traditionally use a collection of VPN technologies called IPsec [2] illustrated in Fig – 2.

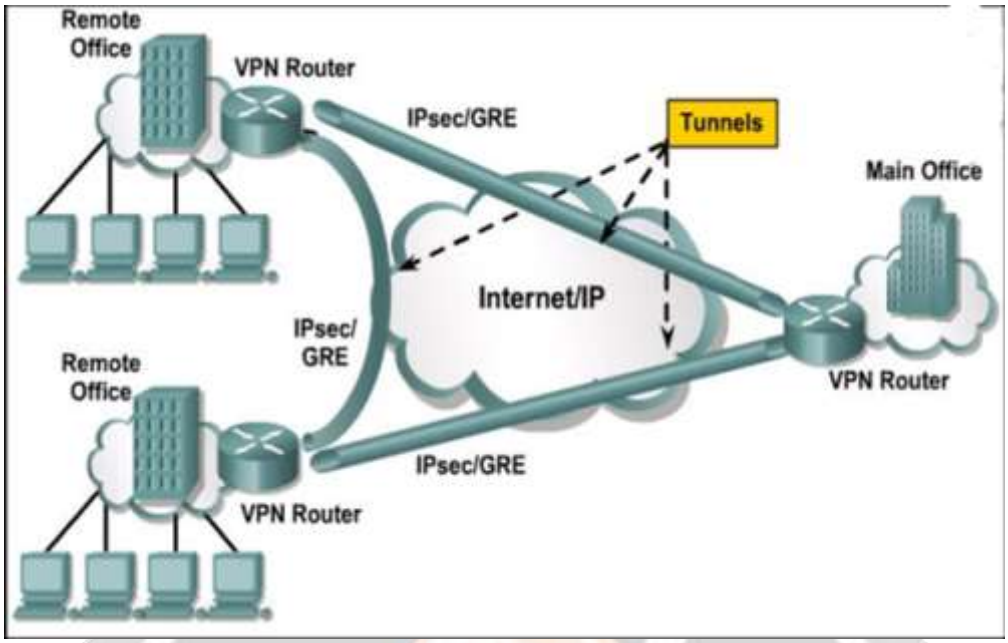

Fig – 2: Site-to-Site VPN

3. DEPLOYING IPCop AND DESIGNING SECURE CONNECTION

3.1 IPCop

IPCop is a firewall software based on a Linux distribution that aims to provide a simple and configurable hardware firewall using a standard PC. IPCop is licensed under the GPL and is developed with the traditional style of Open Source: the project is developed through the collaboration of several developers scattered around the globe. The graphical interface is available in 17 different languages. The distribution also includes an elegant and simple system upgrade [9].

IPCop offers a wide range of technical features, ranging from standard Linux netfilter capabilities of NAT support for DNAT DMZ away from supporting DHCP (client and server) to support and serve NTP to synchronize the date and time, the ability to activate a proxy to enable an IDS. It also supports four network cards and an unlimited number of VPN connections, as well as offering the possibility to backup and restore of the configuration. It is also easily extensible with many modules available on the Internet. IPCorp also has the ability to partition the network into a green, safe network protected from Internet, a blue network for the wireless LAN and a DMZ or orange network containing publicity accessible servers, partially protected from the Internet (RED) as shown in Fig-3.

The detail meanings of these colors are:

RED - the interface is connected to the Internet. (ISP - PPPoE - PPPoA, xDSL Router)

GREEN - is the interface for the internal network. (Private LAN)

BLUE - is the interface for a second internal network or a wireless network. (WiFi)

ORANGE - is the interface for any DMZ where there are servers that offer services outside. (Demilitarized Network).

The four types of network interface - Green, Red, Blue, and Orange supported by IPCop have differing levels of trust associated with them. Table 1 describes the relationship of interfaces such as which type of traffic is allowed to go to and from which interfaces.

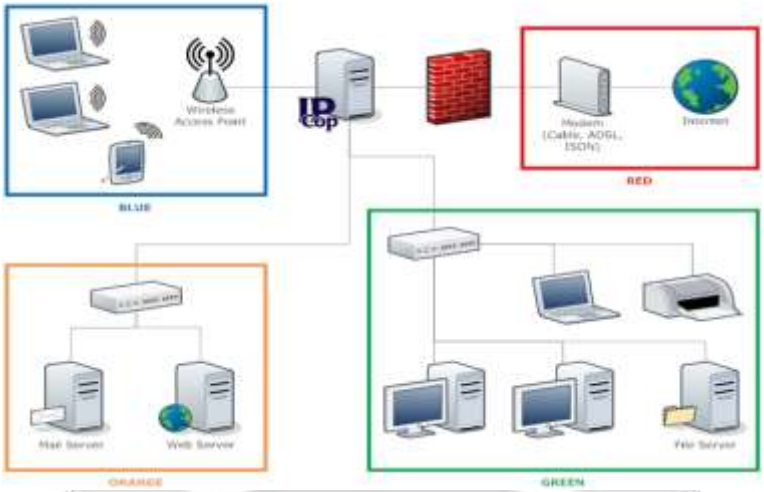

Fig -3: Four Types of Network Interfaces in IPCop

Table 1: Relationships of Interfaces

	IPCop	RED	GREEN	BLUE	ORANGE
RED	Closed EA		Closed PF, VPN	closed PF, VPN	closed PF
GREEN	open	open		open	open
BLUE	closed BA	closed BA	closed DP, VPN		closed BA
ORANGE	closed	open	closed DP	closed DP	

EA: External Access PF: Port Forwarding VPN: Virtual Private Network
DP: DMZ Pinholes BA: Blue Access

4. IMPLEMENTING SECURE CONNECTION OF THE UNIVERSITY

The system developed two types of secure VPN connection (remote-access and site-to-site) with IPCop firewall software, using all four network interfaces to protect a with an internal (Green) network, an Internet or WAN connection (Red), a DMZ containing more than one Server (Orange), and a wireless segment (Blue) with an IPSec VPN system as shown in Fig – 4.

On the Green interface, the system permits connectivity to all interfaces, as workstations and Servers within the Green segment are managed service workstations on which users do not have the necessary level of access to cause damage to the resources to which they have access.

The Port Forwarding feature of firewall policy is invoked on external (RED) interface to access mail and secure web services to the mail server on port 25 in the DMZ, and also to port 443 (HTTPS) on the mail server in order to allow connections to the business webmail system. At this part, host-to-Net VPN connection is configured with IPSec feature of the IPCop firewall in order to grant remote access to staff, lecturers and professors who work remotely and to provide remote connectivity for support purposes for the university resources and third-party software and hardware vendors as illustrated in Fig-4.

The university is providing connectivity via an IPSec VPN for clients in order that they can access services run from Servers internally on the Green segment and DMZ segment at the BLUE interface. Vendors and visitors are

allowed access to the Green segment through use of WPA in pre-shared key mode configured on the wireless access point.

The university always communicates and transfers data to the office of Ministry which places in remote via the Internet. The traffic between these two offices travels over an "open" channel, risking confidentiality (unauthorized snooping of data) and integrity (unauthorized tampering of data). To overcome these risks, the site-to-site or net-to-net VPN feature proposed to encrypt traffic over the Internet.

The two private networks, main office of university and the office of ministry are connected using inexpensive Internet bandwidth. For data security, the tunnel is implemented between IPCOP1 of university and IPCop2 for office of ministry. All traffic flowing through it is encrypted, to ensure confidentiality and integrity.

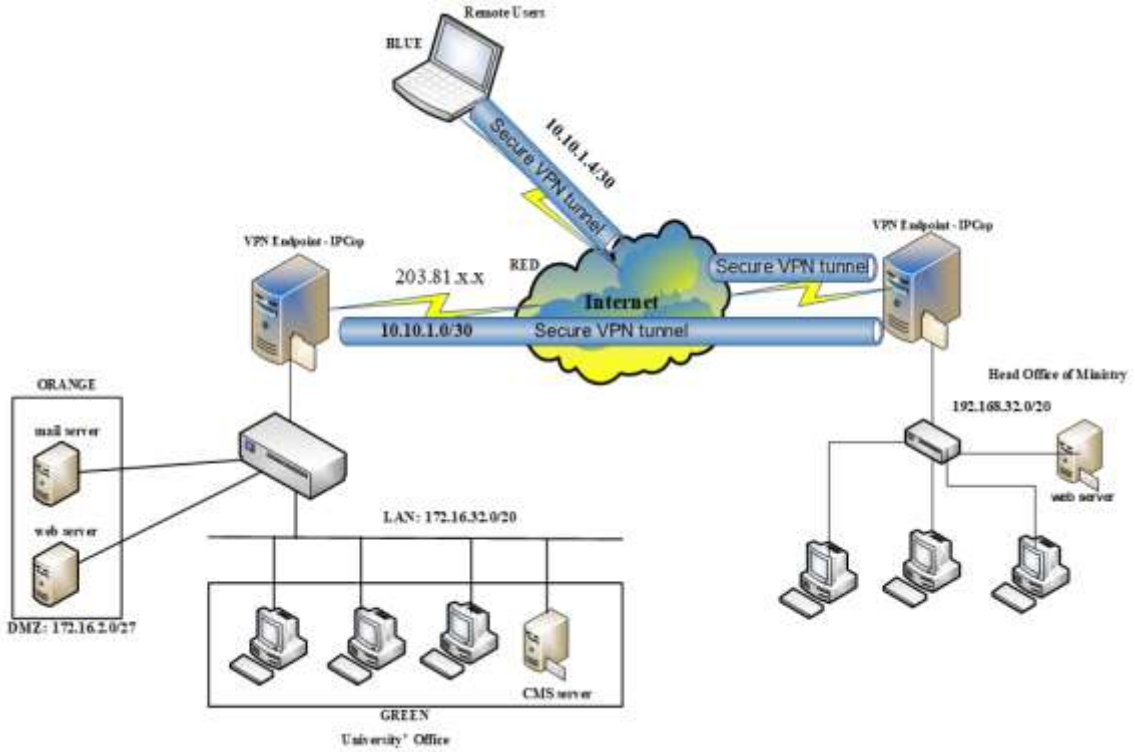

Fig - 4: Secure Connection of the University

5. EVALUATION OF SECURE NETWORK DESIGN

A VPN relies on a VPN server and a VPN client to establish a secure connection for the university. When the connection is established, an encrypted tunnel is created between the client and the server. The external users or users of remote office request any connection through the client to the web or mail servers are encrypted and sent to the server.

Afterwards, the server decrypts the requests and forwards them to respective server services or resources. Once the requested data is received, it is encrypted by the server, and then sent back to the client.

When the university uses secure VPN connection in data processing with external users and staffs of remote office, a VPN hides the original IP address of LAN and encrypts the data transmitting traffic, it essentially makes sure that nobody can't be tracked digital footprints of data processing on the Internet. Online hackers won't be able to use the real IP address of LAN and to find out any information of university, and government surveillance agencies and ISPs won't get to monitor what do online by snooping on university traffic.

6. CONCLUSION

In this paper, the system is developed to configure secure VPN connection for university network using IPCop software firewall. VPN became important to secure data transfer since current Internet protocols do not protect data

sufficiently enough. Firstly, the system implemented host-to-net VPN for remote users for secure data processing and then Net-to-Net VPN is proposed to communicate securely between main office and office of ministry of education. If leased lines are used, it is very expensive, especially at long distances between enterprise networks. Therefore, it became necessary to use the technique that provide the security and in the same time not expensive. In this approach, the VPN technique have been used and a set of standard security Internet Protocols knows as IP Security (IPSec) have been developed. According the recommendation of the staffs the usage of this technique has become possible to provide cost effective, reliability and data integrity in secure data transmitting.

7. REFERENCES

[1]. Salah Alabady, "Design and Implementation of a Network Security Model for Cooperative Network", International Arab Journal of e-Technology, Vol. 1, No. 2, June 2009.
[2]. R Keith Barker, Scott Morris, "CCNA Security 640-554 ", Official Cert Guide, pulished by Cisco Press, 800 East 96th Street,Indianapolis, IN 46240, 2013.
[3]. W.S Hayale, E.A Jebur, " Implementing Virtual Private Network using Ipsec Framework", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181. Vol. 3 Issue 8, August-2014.
[4]. D. Sampaio, J. Bernardino, "Evaluation of Firewall Open Source Software", In Proceedings of the 13th International Conference on Web Information Systems and Technologies (WEBIST 2017), pages 356-362 ISBN: 978-989-758-246-2.
[5]. Krupa C. Patel, Dr.Priyanka Sharma, "A Review paper on pfsense – an Open source firewall introducing with different capabilities & customization", IJARIIE-ISSN(O)-2395-4396, Vol-3 Issue-2 2017.
[7]. Mohammed N",adir Bin Ali, Mohamed Emran Hossain, Md. Masud Parvez, "Design and Implementation of a Secure Campus Network", International Journal of Emerging Technology and Advanced Engineering.
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 7, July 2015)
[8]. Pradip Nath, Abdullah Al Noman, "Design and Implementation of Secured VPN of a Bank using Cisco Devices", Department of Electronics and Communications Engineering. East West University.
[9]. http://ipcop.sourceforge.net.