Virtual Private Network Implementation on PC as a Router for Privacy of Data Transfer

Prof. Leena Patil[1], Antoinette Fernandes[2], Arundhati Kahate[3], Devika Salunkhe[4]

[1]Professor, Dept. of Electronics and Telecommunication, Xavier Institute of Engineering, Mumbai, Maharashtra, India
[2,3,4]Student, Department of Electronics and Telecommunication, Xavier Institute of Engineering, Mumbai, Maharashtra, India

---***---

Abstract – *Sensors is a way of providing real time authentic data for various applications. They are applied in fields such as military, home automation and health care. Monitoring of these sensors could be done remotely with the help of communication networks. To do this, Internet is needed for such applications. However, there is a huge concern regarding privacy and security. Virtual Private Networks provides various protocols for securing networks and communications. The VPN tunnel suggested in this paper is IPsec VPN because IPsec uses a tunnel between two end connections; the transferring data is safer and reliable. The suggested work is done with security protocols consisting of Cryptography, site-to-site IPsec and using RIP. To convert a physical CPU into router, Vyos is used which is a network operating system and supports various routing protocols.*

Key Words: **Site-to Site IPsec, VPN, Cryptography, Security and Privacy, Tunnelling, IKE.**

1. INTRODUCTION

Over the past years, technology experts ranked data breaches as the most dangerous information security risks. As mentioned in Data Breach Investigation Report by Verizon, 32% of confirmed data breaches happen due to phishing attacks. Such attacks aim to obtain sensitive information such as bank details and security numbers. The Internet of Things is made up by connecting multiple devices to a network, i.e. home appliances and services sensors. Once the data leaves the device and travels through routers or internet, it is prone to hackers if the path traveled by packets is not secured and private. This could result in leaked private information. A well know solution is IPsec VPN which provides a secured tunnel to allow the packets to travel, to and back, from two different remote locations [1]. Figure 1 shows a VPN tunneling structure for two different remote locations. To protect our data, we use VPN because it provides secure and encrypted virtual connections over IP network by encrypting and encapsulates each packet before passing it through a tunnel. VPN provides authentication to ensure data integrity and confidentiality. VPN tunneling adds an overhead to IP packets size, that effect bandwidth utilization in a network more specifically if the packet is short in size. This effect will also be on the destination router to decapsulate the packet and performs decryption for the packet. Also, there are a variety of formats: authentication, confidentiality (data encryption), and access control (firewall) possible while using VPN [2]. A research described how remote monitoring of gas sensors using VPN connections using LabVIEW software has made it easy for controlling and monitoring at various areas [3].

Cryptography is used to ensure that the contents of a message are very confidentiality transmitted and would not be altered [4].

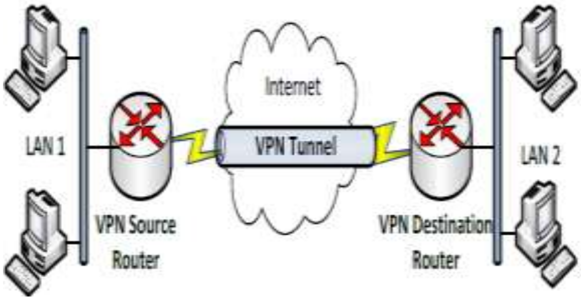

Fig.1. VPN tunneling structure

Past research show how IPsec VPN tunnel was established and calls were initiated from one site to another using SIP softphones that were connected to Asterisk server and performances were measured in terms of delay, bandwidth, and jitter in the network to demonstrate the effectiveness of security in prohibiting attackers [1].

To implement VPN over a vast network, for example, college campuses, Multi-VLAN can be implemented. Benefits of Multi-VLAN include its increase in protection and security, and it can also reduce the network administrators' management of maintaining and managing the network as a whole, even if the two campuses are far away and maintain data transmission efficiency [2].

2. PROPOSED TOPOLOGY

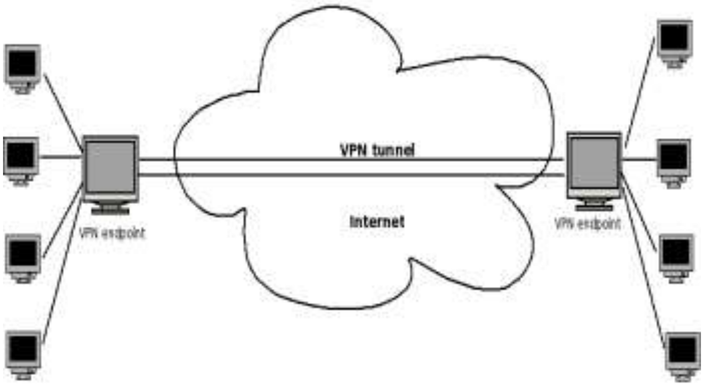

Fig.2. Proposed topology

The above diagram shows the proposed topology to implement VPN between two different networks using Vyos routers. The path between R1 and R3 is what must be secured through IPsec VPN tunneling.

3. PROPOSED MODEL

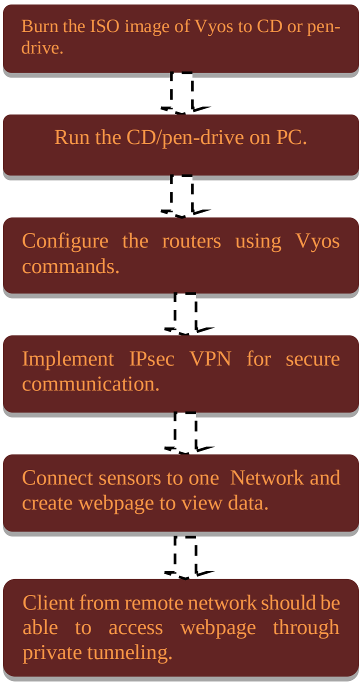
Burn the ISO image of Vyos to CD or pen-drive.
Run the CD/pen-drive on PC.
Configure the routers using Vyos commands.
Implement IPsec VPN for secure communication.
Connect sensors to one Network and create webpage to view data.
Client from remote network should be able to access webpage through private tunneling.

Fig.3. Proposed model

3.1 Virtual Private Network

VPN offers number of services like low cost, flexible functionality, secure and private connections on public network structure. The most popular protocols linked with VPN development are point to point tunneling protocol (PPTP), layer 2 tunneling protocol (L2TP), Internet protocol security (IPsec) and Secure socket layer (SSL). These protocols provide authentication and encryption mechanisms for VPN.

1. Point to Point Tunneling Protocol (PPTP)

PPTP operates at data link layer. It uses the same authentication mechanisms as point-to-point protocol PPP.

2. Layer 2 Tunneling Protocol (L2TP)

L2TP establishes a tunnel between the routers or the router and clients and it is capable of establishing multiple tunnels simultaneously between two tunnel endpoints.

3. Internet Protocol Security (IPsec)

IPsec offer data integrity, data confidentiality, and authentication of data at the network layer in OSI model. It uses different protocols such as: IPsec Key Exchange and Management Protocol (ISAKMP) for key management which is used for specifying the negotiation, establishment, alteration, and omission of security association. Internet Key Exchange (IKE) for key exchange which create secure channel to protect the negotiation for setting up the IPsec tunnel for traffic protection. Authentication Header (AH) offers authentication and connectionless integrity. Encapsulated Security Payload (ESP) offers authentication originality, connectionless integrity and data confidentiality. IPsec employs two encryption modes: transport mode which encrypts data only and tunnel mode that encrypts header and data.

4. Secure Socket Layer (SSL)

SSL offers encryption and authentication for web traffic over an encrypted tunnel and supports specific applications such web and email services since SSL tunnel traffic at session layer

3.2 VPN Packet Transmission

In VPN, before transmission, packets are first encrypted before it is sent out over the internet. The encrypted packet is first placed inside an unencrypted packet, then the unencrypted outer packet is read by the routing protocol so that it may be properly routed to its destination and once the packet reaches its destination, the outer packet is removed and the inner packet is decrypted [5].

3.3 Cryptography

Cryptography is used because of its purposes such as:-

i. *Authentication*:
Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified [4].

ii. *Confidentiality*:
The principle of confidentiality specifies that only the sender and the intended recipient should be able to process the contents of a message [4].

iii. *Availability*:
The principle of availability states that resources should be available to authorized parties all the times [4].

iv. *Integrity*:
The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender [4].

v. *Access Control*:
Access Control specifies and controls who can access the process [4].

Types of Cryptography

I. *Secret-Key Cryptography*:

Defined as when the same key is used for both encryption and decryption. DES, Triple DES, AES, RC5 and etc., are examples of such encryption. This mechanism is known as secret-key cryptography.

II. *Public-Key Cryptography*:

Defined as when two different keys are used, that is one key for encryption and another key for decryption. RSA, Elliptic Curve and etc., are examples of such encryption. This mechanism is known as public-key cryptography.

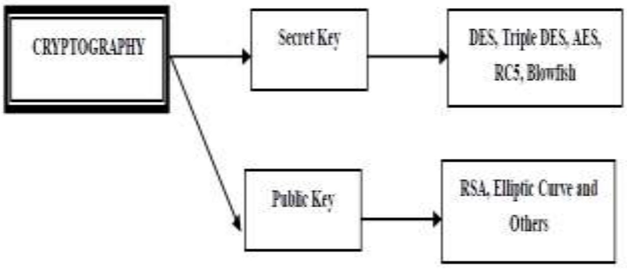
CRYPTOGRAPHY
Secret Key
DES, Triple DES, AES, RC5, Blowfish
Public Key
RSA, Elliptic Curve and Others

Fig.4. Classification of Cryptography

3.4 Vyos

Vyos is a "router first" network operating system. It supports static routing, policy routing, and dynamic routing like RIP, OSPF, and BGP. It supports protocols like IPsec, VTI, VXLAN, L2TPv3, L2TP/IPsec and PPTP servers, tunnel interfaces (GRE, IPIP, SIT), OpenVPN in client, server, or site-to-site mode.

For initial testing of Vyos as a virtual machine, Oracle VirtualBox or VMware can be used with the available IOS image file. Commands used for Vyos are different as compared to Cisco routers.

4. CONCLUSIONS

In this paper, we propose a method on how to convert a physical PC as a router, by using Vyos which is an open-source operating system. Virtual Private Network (VPN) is a technology that will create private networks through public networks. For security purposes, VPN needs to be used to create secure connections that will protect the traffic which flows between controlled and trusted endpoints. It is important to implement Site-to-Site IPsec for privacy, authentication and integrity of data. This case study is a good practice for cost-effective training of networking protocols on a physical machine.

5. ACKNOWLEDGEMENT

We would like to thank our project guide Professor. Leena Patil who has been our source of inspiration for this project. We are also grateful to the authorities, faculties of Xavier Institute of Engineering who have helped us to be better acquainted with recent trends in the technology.

6. REFERENCES

[1] Amirisetti Sushma and Teerapat Sanguankotchakom, “Implementation of IPsec VPN with SIP Softphones using GNS3,” ICNCC 2018, December 14-16, 2018, Taipei City, Taiwan.

[2] Sasalak Tongkaw and Aumnat Tongkaw, “Multi-VLAN Design over IPSec VPN for Campus Network”,2018 IEEE Conference on Wireless Sensors (ICWiSe).

[3] Dr. Mohammed Basheer Al-Somaidai and Omar Mowaffak Ahmad Alsaydia, “Remote Monitoring and Controlling of Gas Sensors Using VPN Connections”, 2012 International Conference on Future Communication Networks.

[4] A. Joseph Amalraj and Dr. J. John Raybin Jose, “A Survey Paper on Cryptography Techniques” International Journal of Computer Science and Mobile Computing, Vol.5 Issue.8, August- 2016.

[5] M.Krithikaa, M.Priyadharsini and C.Subha, “Virtual Private Network- A Survey” International Journal of Trend in Research and Development, Volume 3(1), Jan - Feb 2016