International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

VPN Simulation using IPSec Framework with Cisco Packet Tracer

Sachin Raina[1], Jasmeet Kaur[2], Nancy Sharma[3], Krishna Nand Patel[4]

U.G. Student, Department of Computer Science and Engineering, Chandigarh University, Punjab, India[1]

U.G. Student, Department of Computer Science and Engineering, Chandigarh University, Punjab, India[2]

U.G. Student, Department of Computer Science and Engineering, Chandigarh University, Punjab, India[3]

U.G. Student, Department of Computer Science and Engineering, Chandigarh University, Punjab, India[4]

ABSTRACT: We are living in the era of digital world where we are surrounded by machines, networks and computers where we share our data from one computer to another via internet, but this way of sharing information is insecure by nature and has the tendency to expose our personal details to various intruders which are present in between sender and receiver end. VPN (Virtual Private Network) provides a tunnel from source to destination to send the data so it can't be accessed by any third party present in between the network. There are various VPN technologies available like PPTP, L2TP, MPLS, GRE and SSL. This research paper explains what virtual private network is and how to implement it using Packet Tracer. Packet tracer is virtual network simulator software which is used to troubleshoot, design and configure the computer networks.

KEYWORDS: VPN, Computer networks, IPSec, Packet Tracer, Remote access, IP.

I. INTRODUCTION

Virtual private network gives an encrypted and secure path called tunnel from source end to destination end through the internet. The ease of using internet has increased the use of data transfer through the networks and this leads to the increase in the VPN construction by lots of companies. The term VPN refers to a logical connection between two devices i.e. sender and receiver to transfer the data.

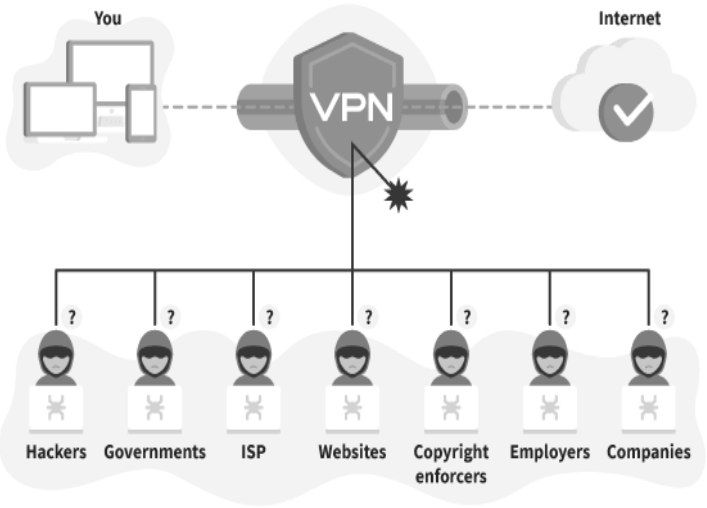


Fig.1 VPN tunnel

Confidentiality and data integrity is maintained in VPN so that when anyone tries to get the sense of shared data gets nothing in return because the original data is encrypted and they do not have the key to decrypt the data to know what

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

the actual data is. VPN has the implementation of secure network using switching or routing capabilities. It also uses integrity checking to make sure that VPN is monitoring correctly the packets that they are not modified maliciously along its route. VPN is basically the combination of tunneling and encryption. VPN is also used for remote access, file sharing and conferencing.

Virtual private network = Tunneling + Encryption

II. TYPES OF VPN

There are basically two types of VPN remote access and site-to-site which are explained below.

Remote-access VPN

Remote access VPN allows the users to connect to different computer and access its information remotely from different location. Home user or private user uses this VPN to access the blocked websites. IPSec or SSL technologies are used by this type of VPN.

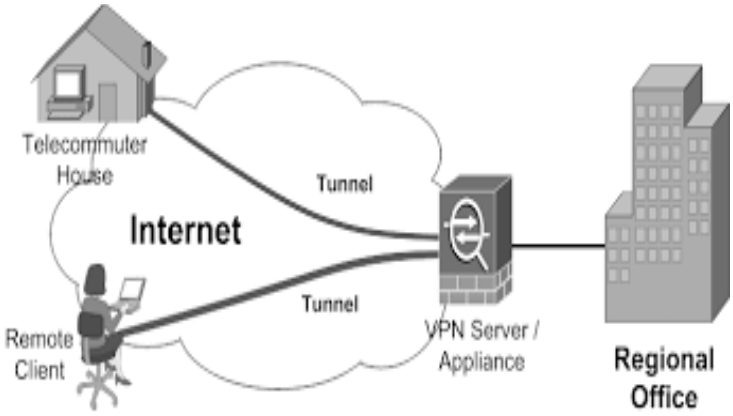


Fig.2 Remote access VPN

Site-to-Site VPN

It is also known as Router-to-Router VPN and is used by large companies which has various offices or branches located at different geographical locations. A site-to-site vpn is used to establish a secure and private connection between different offices or branches of the company. In this VPN one router acts as VPN server and other acts as VPN client. Communication between server and client starts after the authentication is validated from both ends.

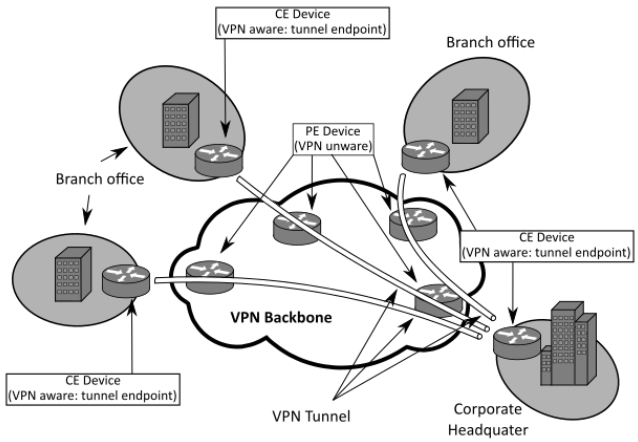


Fig.3 Site-to- Site VPN

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

III. THE PROBLEM

As we all know that sharing files through internet is very fast and easy but it is not safe because any third party present in the same network can access the data. The situation is depicted in fig.5.

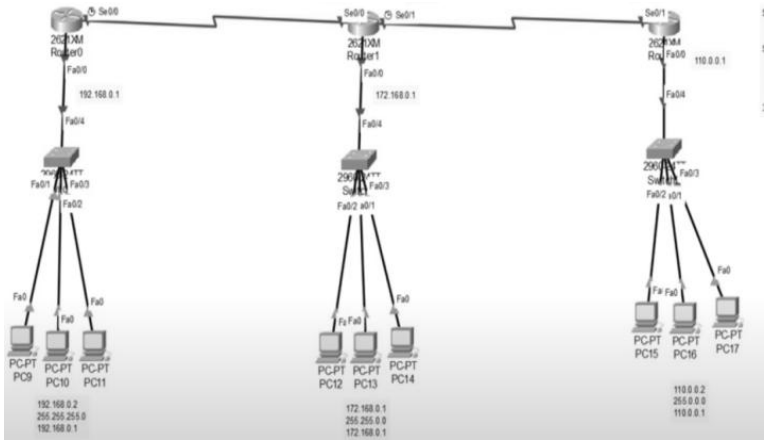


Fig.4 Design of network

Considering the above diagram if we want to send data from router R2 to router R0 then R1 in their between can access their information. It can be proved by tracing the route from R2 to R0 which is shown in fig.6 where 110.0.0.1 is the IP address of R2 and 10.0.0.1 is the IP of R0 but in their between IP address of R1 which is 11.0.0.1 is present and so it can access the shared messages between R0 and R2.

```
C:\>tracert 10.0.0.1

Tracing route to 10.0.0.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      110.0.0.1
  2    1 ms      0 ms      1 ms      11.0.0.1
  3    1 ms      1 ms      2 ms      10.0.0.1

Trace complete.
```

Fig.5 Route tracing

IV.THE SOLUTION

This problem of data security can be solved by creating a secure and private connection (an IPSec tunnel) from sender to receiver so that third party can't access the data.

V. IMPLEMENTATION

Implementation of VPN is divided into three steps which are explained below in details.

Configure Interface IP

In IP address the IP stands for Internet Protocol and address refers to a unique identification number that linked to all the networking devices. There is no use of Cisco routers without an IP address. So IP configuration is one of the most important steps which can be done for all the interfaces by using CLI (Command Line Interface).

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

||Volume 9, Issue 4, April 2020||

```
Router(config)#host r2
r2(config)#
r2(config)#int f0/0
r2(config-if)#
r2(config-if)#ip add 172.168.0.1 255.255.0.0
r2(config-if)#no shut

r2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
```

Fig.6 IP configuration of Interfaces

Apply Protocols

In this implementation we have used RIP protocol which stands for "Routing Information Protocol" for all the interfaces as shown below.

```
R1(config-if)#
R1(config-if)#
R1(config-if)#router rip
R1(config-router)#
R1(config-router)#
R1(config-router)#
R1(config-router)#net 10.0.0.0
R1(config-router)#net 192.168.0.0
R1(config-router)#
```

(a)

```
%LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/1, changed state to up
router rip
r2(config-router)#
r2(config-router)#
r2(config-router)#
r2(config-router)#net 10.0.0.0
r2(config-router)#net 11.0.0.0
r2(config-router)#net 172.168.0.0
```

(b)

```
r3(config-if)#
r3(config-if)#
r3(config-if)#
r3(config-if)#router rip
r3(config-router)#net 11.0.0.0
r3(config-router)#net 110.0.0.0
r3(config-router)#
```

(c)

Fig. 7 (a) Router 1 protocols (b) Router 2 protocols (c) Router 3 protocols

Apply VPN using Tunnel

Tunneling is the technique of secure movement of data from one to another network. It is also known as port forwarding and transfers the data through a secure connection. Data is monitored as it travels through the tunnel so that there is not any malicious modification in data through its route. Data is divided into packets and are encrypted as they go through tunnel it again decrypted as they reach the destination.

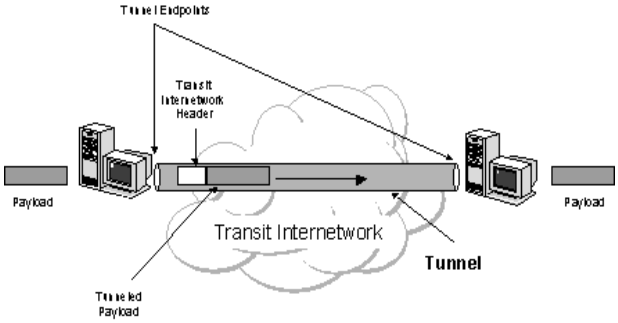


Fig.8 Tunneling

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.089|

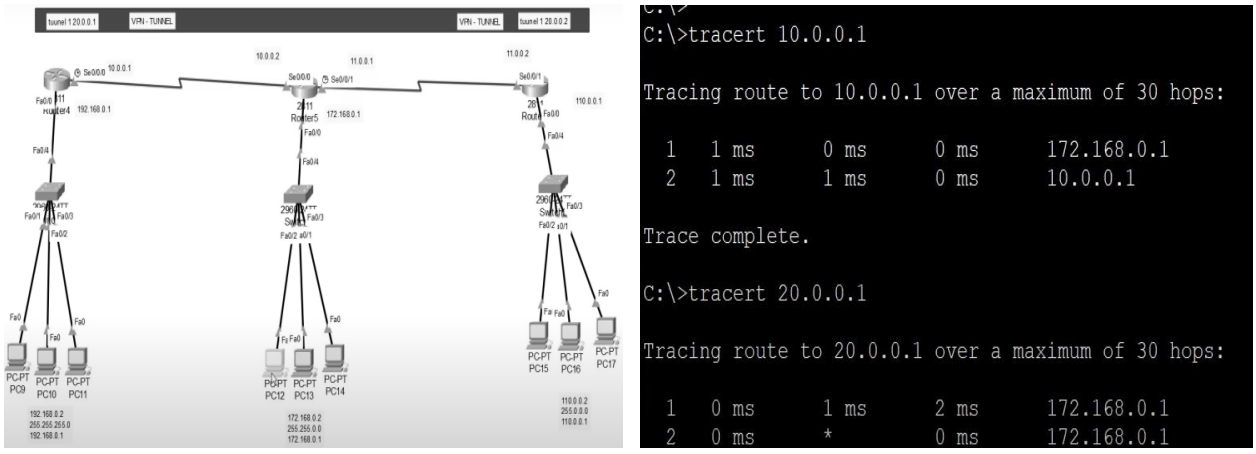
||Volume 9, Issue 4, April 2020||

There are various protocols that provide tunneling some of them are explained below.

- Point to Point Tunneling Protocol (PPTP): It was developed by Microsoft and is released with Windows 95, It enrypts the data and divides it in packets and then send it through tunnel.
- Layer Two Tunneling Protocol (L2TP): It is used with IPSec (Internet Protocol Security) to create more secure tunnel than PPTP. It creates two layer of encryption by wrapping the encrypted data again with IPSec.
- Secure Socket Tunneling Protocol (SSTP): It is available only for windows operating systems, it transfers the data through secure sockets layer which is also known as SSL. It is also used with Transport Layer Security (TLS)

VI. RESULTS AND DISCUSSION

After applying all the steps including configuration of interface IP, configuration of protocols and creating VPN tunnel.VPN is now created and the data transferred between end devices is confidential and can't be accessed by the device present in their between. Remote access VPN is used by the employees to access the data from their office by creating VPN tunnel.
Complete VPN is shown by fig.10.



(a) (b)

Fig. 9 (a) Complete VPN tunnel (b) Route tracing

Fig 9(b) shows that only two devices are present and they are sender and receiver no third device is present in their between.

VII. CONCLUSION

So to access our data remotely from some different geographic locations or to send our data privately to other users it is necessary to maintain the privacy and data confidentiality so it is better to use VPN tunnels so that data is protected

REFERENCES

[1] B. Gleeson at al, IP Based Virtual Private Networks, RFC 2764, February2000.

[2] Ministry of Justice, Republic of Macedonia, Ministry of Justice, Strategy for Justice Information Communication Technology 2007-2010, Skopje, July 2007, Version 4.0.

[3] R.D.Doverspike, K.K. Ramakrishnan, C.Chase, Chapter 2. Structural Overview of ISP Networks, C.R. Kalmanek et al. (eds.), Guide to Reliable Internet Services and Applications,Computer Communications and Networks, DOI 10.1007/978-1-84882-828-5 2, Springer-Verlag London Limited 2010.

[4] L.Todd, Chapter 16: Cisco Certified Network Associate Deluxe Study Guide, Sixth Edition, Sybex © 2011 Books 24X7.