International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 143-146
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

CURING MAN IN THE MIDDLE ATTACK

Rajneesh Tanwar,
Department Of Information Technology
Amity University,Nodia

***Abstract*— Now a day, securing confidential information while sending on network is important. Confidential information is safe when sending via private network but cost of private network communication is not affordable by everyone. Public network is used and many third party software are present in the market but all can be hacked easily which led to access of information. Firewall is one technique which is good but due to only one authentication it also fails. For secure communication on public network like internet can be achieved by using VPN technology. This technology forms a tunnel between sender and receiver due to which no other person is able to access the communication i.e. get fully protected from MAN IN THE MIDDLE attack.**

Keywords— **MAN IN THE MIDDLE attack, Firewall, Private Network, Public Network, VPN Technology**

I. INTRODUCTION

A VPN (Virtual Private Network) is a private network that uses a public infrastructure (usually the Internet) to connect remote sites or users. The VPN as the name suggest uses "virtual "connections routed through the Internet from the business's private network to the remote site or remote employee. It is a new technology which can be applied to LAN as well as to WLAN. A VPN maintains privacy of data through security procedures and tunneling protocols. In effect, data is encrypted at sender side and forwarded via "tunnel" which is then decrypted at receiver side. An additional layer of security can be added by encrypting not only the data, but also the originating and receiving network addresses.[2]

There are two types of Virtual Private Networks.

1. Site-to-Site Virtual Private Networks
2. Remote-access Virtual Private Networks

Site-to-Site VPNs encrypted VPNs provide the same benefits as a private WAN, ensuring private communication from one trusted site to another, providing multiprotocol support, high reliability, and extensive scalability. In addition Site-to-Site encrypted VPNs are cost-effective, secure, and allow for greater administrative flexibility than legacy private WANs. Remote-access VPNs connect telecommuters, mobile users, or even smaller remote offices with minimal traffic to the enterprise WAN and corporate computing resources.[1]

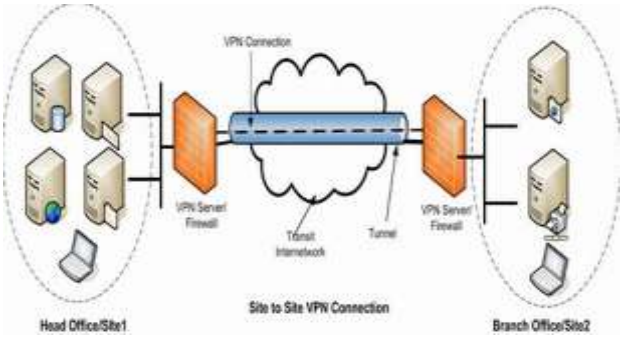

Figure 1: Site to Site VPN [4]

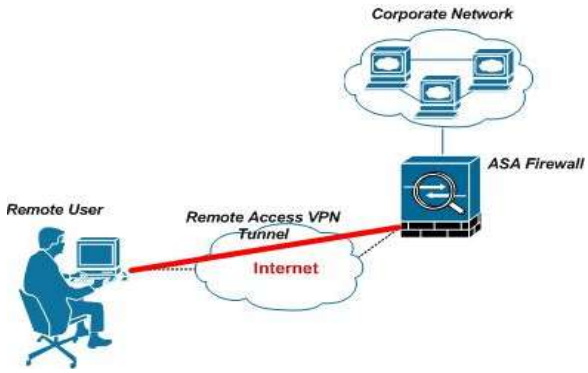

Figure 2: Remote Access VPN [5]

Different protocols used in VPN are -:

- ISAKMP (Internet Security Association and Key Management Protocol)
- IKE (Internet Key Exchange)
- IPSec (Internet Protocol Security)
- PPTP (Point-to-Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- Encryption

1. 3des and des (Data Encryption Standard)
2. aes, aes-192 and aes-256 (Advanced Encryption Standard)

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 143-146
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

Man-in-the-middle attacks have been described on several occasions especially when describing the security in cryptographic protocols. When concerning the Internet, this has been described in different steps where IP-spoofing was considered as the first step toward a working man-in-the-middle attack. IP-spoofing, is a technique where the source address of the IP-packet is forged. The problem when using this technique is to be able to get the answers, since they are sent to the forged address.[3]

II. PROBLEM CONCEPTUALIZATION

Now a day, confidential data sending or important communication over internet is not safe until unless private network communication is not done. Private network formation and communication over that is good for communication but communication over such network is very risky as public network is easily accessible to all and anyone can access the shared information and can make changes.
To get rid of such type of attack called MAN IN THE MIDDLE attack can be achieved by making communication over public network using VPN (Virtual Private Network). Firewall can also be used but in firewall only one authentication is done which can easily be attacked and cracked by hacker. VPN has more advantage over firewall, as VPN firstly forms the tunnel between sender and receiver and secondly it does double authentication to move further in the communication.

III. PROPOSED ALGORITHM

In this system, VPN is implemented and make the secure communication over public network. This will include following steps:

1. Connection of sender and receiver over the public network
2. Formation of ISAKMP tunnel
3. Key Sharing between communicators
4. Formation of IPsec tunnel
5. Access List formation

Following work is done over the GNS3 (Graphical Network Simulator 3) tool which provides the real environment of network devices.

A. Connection of Sender and Receiver over Public Network

The connection between the sender and receiver will be done. Sender and receiver both get connected to public network like internet so that both can identify that are connected.

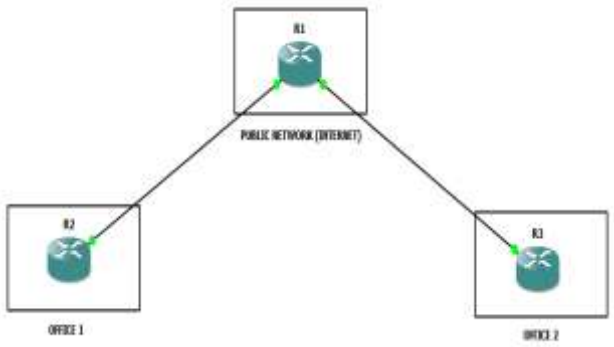

Figure 3: Site with three Routers: Sender, Receiver and acting as Public Network

Above figure 3 is describing a site in which one is sender and another is receiver. One router to which other two are connected is acting like a public network in which anyone can get connected. Sender i.e. office 1 and receiver i.e. office 2, both are now connected and is ready to make communication.
But before starting communication, VPN tunnel should be formed between them so that no other user is able to see the communication and information remain confidential.

B. Formation of ISAKMP Tunnel

ISAKMP (Internet Security Association and Key Management Protocol) is one which is used for forming the inner layer of the tunnel in VPN. Implementation of ISAKMP comes in phase I in which policies of ISAKMP are defined.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 2, Issue 1, ISSN No. 2455-2143, Pages 143-146
Published Online November-December 2016 in IJEAST (http://www.ijeast.com)

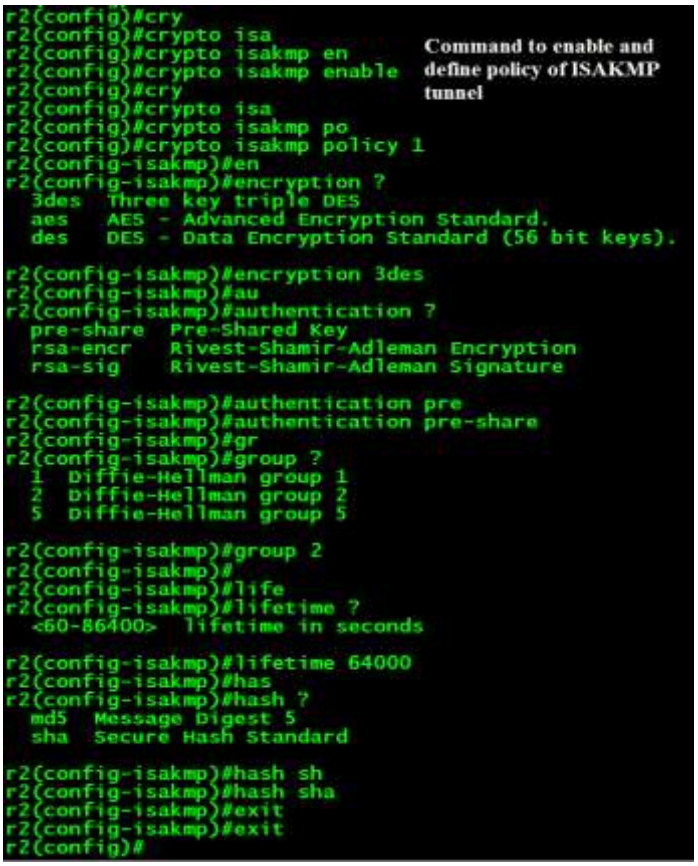

Figure 4: Commands for Phase I in VPN

C. Key Sharing between Communicators

Key sharing process is done after defining the policies of ISAKMP. In this, key should be same at both the site while configuring otherwise it may led to no communication between the two sites.

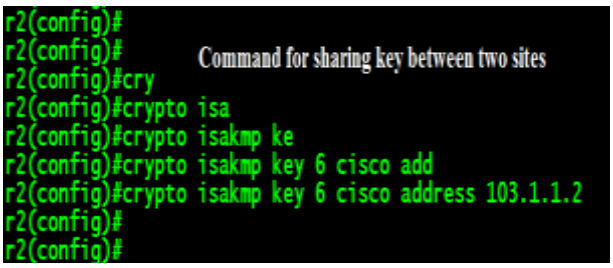

Figure 5: Command for sharing Keys

D. Formation of IPsec Tunnel

IPsec (Internet Protocol Security) is used to form the second layer of the VPN tunnel. This is used for double authentication purpose and also concatenate with ISAKMP. Formation of IPsec tunnel is the Phase II of VPN. Without IPsec, VPn cannot be formed and will not work. IT act as ending phase of formation of VPN Tunnel.

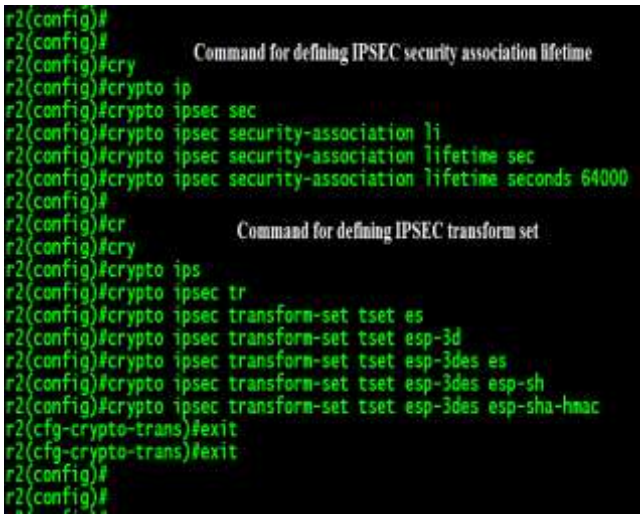

Figure 6: Command for Implementing IPsec

E. Access List Formation

Access list is used to be defined after completion of IPsec tunnel process as this will act as a gate which will allow only defined IP's to enter and get authenticated further. This is used for cancelling the request from strangers IP to directly contact with VPN tunnel.

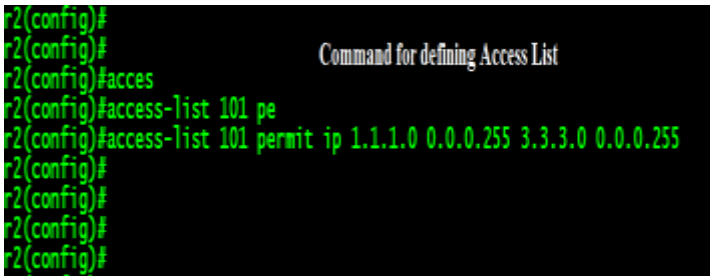

Figure 7: Command for Implementing Access List

IV. CONCLUSION

This proposed system is able to make the communication between two users secure over the public network. This system is able to defend MAN IN THE MIDDLE attack very easily as it will not allow the user to enter in the VPN area and in case it enter then VPN protocols will unauthenticated that machine and disallow it to enter into the communication. By this secure communication over public network like Internet is achieved. This is also cost efficient as no need of private network for secure communication and also easy to implement. In future, it can be implemented on network or machine which wants to send confidential data or do transaction over public network. This will also reduce the cases of leaking of credit card information over internet during transaction.

V. REFERENCE

[1] "Managing Cisco networking security", Michael J.Wenstrom, Cisco Press, Indianapolis, IN 46290 USA

[2] "IP Based Virtual Private Network Implementation on Financial Institution and Banking System", Dr. Amir Hassan Pathan and Munizan Irshad,SZABIST, Pakistan, National Conference of Emerging Technology, 2004.

[3] "An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions", Mattias Eriksson, Simovits Consulting, Wenner - Gren Center, 113 46 Stockholm, Sweden,2011.

[4] Date of Access: 21st October 2016 https://www.google.co.in/search?q=site+to+site+vpn&biw=1366&bih=677&source=lnms&tbm=isch&sa=X&sqi=2&ved=0ahUKEwiFs_2j38nKAhXKC44KHRTVC44Q_AUIBigB#imgrc=Xn5UXAtiTX5NPM%3A

[5] Date Of Access: 21st October 2016 https://www.google.co.in/search?q=site+to+site+vpn&biw=1366&bih=677&source=lnms&tbm=isch&sa=X&sqi=2&ved=0ahUKEwiFs_2j38nKAhXKC44KHRTVC44Q_AUIBigB#tbm=isch&q=remote+access+vpn&imgrc=f5ECZAii0IWk0M%3A