International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-3, February 2013

Providing Security in VPN by using Tunneling and Firewall

Sonam Wadhwa, Kunwar Pal

Abstract *-- The use of security increased consistently day by day. Huge amount of network requires large amount of security. For maintain things consistent and proper functioning, people require secure way to share information over the network. To accomplish this goal Virtual Private Network is one of the popular techniques. It constructs logical link by using existing public infrastructure. Internet is one of the public networks and VPN utilize the internet to connect the users. IPSec Protocol is a protocol suite based on VPN to protect the communication. For uninterrupted VPN services, it is necessary to provide some mechanism by the combination of tunneling and firewall. This paper proposes a new kind of configuration for security to the public network.*

Keywords*: Tunneling, Firewall, IPSec, Virtual Private Network, Algorithm.*

I.INTRODUCTION

Security and Privacy are the two major requirements for communication over the internet. They require some kind of security services like confidentiality, Integrity and authentication. Before providing security to the network, their mechanism should know about the possible attacks which are connected to it. Virtual Private Network is one of the strongest key for communication over IP network. Virtual Private Network that virtualizes the private network. VPN supports communication services like voice, video, traffic and images. It ensures privacy at network layer [7].

Internet Protocol Security (IPSec) is a protocol suite to protect communication by using tunnel over the internet. IPSec was developed by Internet Engineering Task Force. IPSec has network layer security control and each IP packet has data stream. It is easy to handle small packets of data. IPSec is the compilation of techniques and protocols and collection of RFC [9] defines the architecture and specific protocol used in IPSec. To ensure the data integrity, a standard were developed i.e. IP security. It provides some security services are authentication, integrity and confidentiality and these services provided by Authentication Header and Encapsulating Security Payload [3]. The technical way to encapsulate the IP packet keen on other IP packet, tunneling is used.

Manuscript published on 28 February 2013.
***** Correspondence Author (s)
Sonam Wadhwa She achieved her B.Tech degree in computer Science and Engineering from G.B.K.I.E.T, Malout, Punjab, India in 2009, now She is pursuing M.Tech (CSE) from Lovely Professional University, Phagwara, Punjab, India.
Kunwar Pal , He achieved her B.Tech degree in computer Science and Engineering from KNIT, Sultanpur, India in 2009 and M.Tech (CSE) from Punjab Engineering College, Chd, India in 2011. Now He is an Assistant Professor in Lovely Professional University, Phagwara, India

Tunneling is one of the powerful methods to protect the traffic from the external source. Set up tunnel to treat the internet as one hop between two parties [6]. Tunnel which are used between two parties encapsulate the source packets. This tunnel will establish a secure VPN. To create a tunnel, there are several protocols are: IPSec, PPTP, SSL that carry traffic [1].

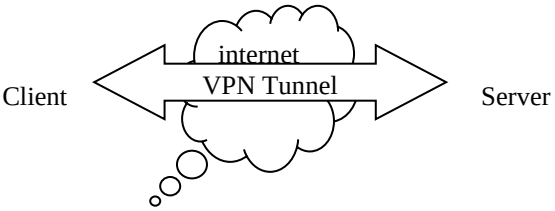

Fig 1: Tunneling in VPN

Firewall is a network mechanism and to establish the firewall, some methods are used. These methods filter the traffic at the network layer. The predecessors to firewall for network security were the routers used in late 1980s to break up networks from one another. All data among the two networks must pass through the firewall. The data which are filtered present in the form of packets. The organization which setup the firewall should need backup plan in case of firewall fails. Some features of firewall are filter on network layer, filtering on protocol, filtering for IP, easy to use, high performance. Firewall can be of hardware based or software based. Hardware gives better performance with high expenses on the other hand software based firewall is easy to implement and its expenses is too low [10]. Firewalls that defend networks from attacks originate in the outside Internet by filtering and managing Internet traffic. A Firewall Vulnerability can occur during designing, implementation of firewall so that can be exploited to attack the trusted network that the firewall is made-up to protect. This vulnerability includes: Validation error, Authorization error, Domain error, Incorrect design error that effects Execution of code, Denial of services.

Application Layer
Presentation Layer
Transport Layer
Session Layer
Network Layer
Link Layer
Physical Layer

Fig 2: Layers for Firewall Filtering

Some algorithms are used for authentication, confidentiality and data integrity over the internet to providing security i.e. AES, DES, 3DES, HMAC-SHA, MD5. The MD5 digest used for data integrity in software systems. MD5 used for storing secure information and transmitting data from source to destination, i.e. password and user name. Every user wants to gain access for some resources with entering the password. If the system constructed properly or authenticated that save the password then verification process is done by comparing MD5 digest of stored password to an entered password [4].

It is necessary to know about attacks in any network whether it is a private network or a public network.

1. Man-in-the-middle attacks affect data when sent between two communicating nodes. It can include modification message, deletion of message and insertion of message, reflect that message at the sender side, replay old message.
2. VPN hijacking is an unauthorized technique that established VPN connection, and assumes that client on the connecting network.
3. Password can be leaked if client side infects with virus, to an attacker [11].

II. RELATED WORK

It is necessary to include security considerations to secure the network from the attacks. Strong security considerations should be in use to protect against hijacking, Denial- of-services [1]. VPN have large and complex structure needs strong security support. Early VPN establishment are chained together with different device strategies routers, gateways and firewalls. [2]. IPSec is a framework that will provide security services at network layer. To establish the secure IP connection, we require gateways, routers, firewall then it will support strong encryption and data integrity mechanism. Two traffic protocols used in IPSec is Authentication Header (AH) and Encapsulating Security Payload (ESP). Due to including AH and ESP, it increases the overhead and also increases traffic load. When traffic load increases, congestion will also increase so it is feasible to execute IPSec VPNs for small size network [3]. To secure the data transmission various technologies are used tunneling and firewall. IPSec can be combined with several technologies that will provide confidentiality, integrity and authenticity. It can use encryption algorithm, digital certificates and hashing algorithm. Hashing algorithm with HMAC, it is recommended to use MD5 [4]. To establish a good command of network, its basic requirement should be accomplish i.e. scalability, performance, reliability, usability, ease of management, protocol support [5]. Attacks can increase the delay, jitter, packet loss. Some attacks can be preventing by software fixes or by some hardware fixes. To prevent attacks at higher level, we need to utilize faster hardware or filters. As filters, we can use firewall. Filters are more effective to differentiate attack packet from authorized packet [6]. Packet Delay variation and Packet End to End Delay for network increases because extra time needed for encapsulation [7] . Packet filtering is one of the techniques of firewall. Packet filtering can be filtered the traffic based on some criteria: source address, destination address, protocol type used, source port, destination port so it can reduce the problem of load of traffic in the network and can reduce congestion [10].

III. PROPOSED WORK

This paper proposes a scenario for providing security to the public network by establish the Private network. Secure VPN provide security to the packets by establish tunnel with IPSec. As a tunnel, we can use Hash Algorithm i.e. MD5. MD5 algorithm is much secure; it will provide data integrity and if once the message is made than it can't be change, come back to the original message will be tough in that case. Firewall is used before establish the VPN. Firewall will filter the packets and this packet filtering can be much faster. Packet filter will use various kind of information to generate their decision on whether or not to forward the packets i.e. source, destination address, and transport level protocol. It can reduce the congestion in the network due to traffic load decreases and it can block attacks due to its speed and flexibility.

IV. CONCLUSION

This paper focuses on providing security over the insecure network. The main reason behind this paper is to reduce the congestion over the network by using the packet filter firewall. It will protect the information in order to make the traffic message secure and will also protect the data from the attacks.

REFERENCES

[1] Samuel Patton, Bryan Smith, David Doss, William Yurcik, "A Layered Framework of Deploying High Assurance VPNs", Department of Applied Computer Science Illinois State University, USA, November 2000.

[2] Beyong-Ho Kang and Maricel O. Balitanas, "Vulnerabilities of VPN using IPSec and Defensive Measures", Department of Multimedia Engineering, University of Tasmania and Hannam University, Australia, July 2009.

[3] Ritu Malik and Rupali Syal, "Performance Analysis of IP Security VPN", International Journal of Computer Application, Volume 8-N0.4, October 2010.

[4] Vishal Sharma and Manish Kalra, "Performance Analysis and Enhancement in IPSec VPN to Reduce Connection Establishment Overhead and Transmission Delay: Part 1", International Journal of Advanced Science and Technology, Volume 8, July, 2009.

[5] M.Sreedevi and Dr.R.Seshadri, "An Innovative Kind of Security Protocol Using Fusion Encryption In Vitual Private Networking", International Journal of Distributed and Parallel System, Vol.3, No.1,January 2012.

[6] S.Saraswathi and P.Yogesh, "Mitigating Strategy to Shield the VPN Service from DoS Attack, International Journal on Cryptography and Information Security,Vol.2,No.2,June 2012.

[7] Aruna Malik and Harsh K.Verma, " Performance Analysis of Virtual Private Network for Securing Voice and Video Traffic", International Journal of Computer Application ,Volume 46-N0.16,May 2012.

[8] William Stallings (2007); "Network Security Essentials: Applications and Standards", Prentice Hall, Publications.

[9] Kent S, Atkinson R. Security architecture for the internet protocol, RFC2401, 1998.

[10] Kenneth Ingham and Stephanie Forrest, "A History and Servey of Network Firewalls",

[11] ACM Journal, Vol V, NO. N, 2000.

[12] http://www.nta-monitor.com/

She achieved her B.Tech degree in computer Science and Engineering from G.B.K.I.E.T, Malout, Punjab, India in 2009, now She is pursuing M.Tech (CSE) from Lovely Professional University, Phagwara, Punjab, India. Her research interests include network security and grid computing.

He achieved her B.Tech degree in computer Science and Engineering from KNIT, Sultanpur, India in 2009 and M.Tech (CSE) from Punjab Engineering College, Chd, India in 2011. Now He is an Assistant Professor in Lovely Professional University, Phagwara, India. His research interests include network security.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)