INGRESS FILTERING AT EDGE NETWORK TO PROTECT VPN SERVICE FROM DOS ATTACK

S.Saraswathi[1] and P.Yogesh[2]

Department of IST, College of Engineering, Gunidy,
Anna University, Chennai
[1]sarasuthan@yahoo.co.in, [2]yogesh@annauniv.edu

ABSTRACT

Internet Protocol (IP) examines only the packet header to forward the packet but it does not examine the data in it. As internet is open to public, the seeking for sensitive data by the attacker has increased. It has become a necessity to protect data through the Internet. Virtual Private Network (VPN) is a popular service to logically construct private network using the existing public infrastructure. It helps in constructing a geographically dispersed LAN that can securely communicate data using the Internet as the backbone communication network.

IP Security (IPSec) VPN provides confidentiality, integrity and availability through tunnelling and encryption. IPSec protocol provides various security features but it does not provide any protection against Denial of Service (DoS) attack. DoS attacks to VPN represent a serious threat to enterprises operating over the Internet. It also hinders the services provided by the service providers. Malicious traffic enters into the Internet only through the edge network. To provide an uninterrupted VPN service, a protection mechanism is to be added at the edge network. This paper discusses such protection mechanisms based on filtering and cryptographic technique.

KEYWORDS

VPN, DoS

1. INTRODUCTION

The exponential growth of internet and drastic enhancement in telecommunication has made the Internet a part of every aspect in the world. Internet packet forwarding is based on the IP. It is used for communicating between systems with varying capabilities. IP is the only protocol, always active at the network layer. Here, only the packet header is examined for forwarding but not the data. It is more flexible but vulnerable to various security attacks. As internet is open to public, the seeking for sensitive data by the attacker has increased. It has become a necessity to protect data through The Internet.

A technical solution to protect data through Internet is VPN [1]. VPN is a virtualization concept that virtualizes the private network. It uses strong security solution for providing private communications over the public physical network. VPN is an alternative to Private Network or Private leased line connection. Private network is very much secured compared to the Internet provided VPN. But it is very expensive, requires much time and space to install and not feasible for every enterprise. A single private network will constitute only a single VPN. Large geographically dispersed network is difficult to administrate and maintain. Restoration and communication become worse during link failure.

David C. Wyld, et al. (Eds): CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 35–44, 2012.
DOI : 10.5121/csit.2012.2205

VPN is a popular service to logically construct a geographically dispersed LAN. This logical private network can securely communicate data using Internet [2]. A single physical network infrastructure is shared among multiple VPN and possibly also by non-VPN. This is the advantage of Internet provided VPN over a private network. In such VPN, physical network infrastructure is shared among various logical networks. The term VPN here refers to a set of communicating sites that logically form a private network. Here the communication between sites outside the logical private network and sites inside the logical private network is restricted, even though the communication of the sites of various VPN takes place over the same network infrastructure.

VPN provides remote access service for the mobile user which is impossible using leased line or private network. If the logical link fails then an alternate logical path can be chosen to provide a reliable VPN service. VPN is a combination of tunnelling, authentication, integrity, encryption and access control [3]. VPN that uses internet as the backbone communication network provides cost effective, highly scalable and reliable service with less administrative overhead. However security is still a major concern.

Our work is towards the protection of the IPSec based VPN service against DoS attack. The various sections below deal with the types of VPN, IPSec based VPN, our proposed model, its security issues and the mitigation strategies.

2. VPN OVERVIEW

VPN can be constructed at different layers under different categories. The following subsection deals with it.

2.1. VPN Technologies in TCP/IP Networking Model

VPN is capable of providing virtualization on Layer 1 - Physical Layer, Layer 2 - Data Link Layer, Layer 3 - Network Layer and upper layers - Transport Layer/Session Layer. Each layer provides virtualization respectively on the level of links, switches, routers and end systems [2].

Layer 1 VPN implementation adopts the traditional TDM (Time Division Multiplexing) solution - SONET/SDH (Synchronous Optical Network / Synchronous Digital Hierarchy) or the Optical implementation - GMPLS (Generalized Multi-Protocol Label Switching). Layer 2 VPN implementation adopts the traditional switched solution - VC (Virtual Circuits) based on X.25, Frame Relay or tunnelling - L2TP (Layer 2 Tunnelling Protocol), PPTP (Point to point Tunnelling Protocol). Layer3 VPN implementation adopts IP tunnelling – GRE (Generic Routing Encapsulation), IPSec (Internet Protocol Security) or Label Switching - MPLS (Multi Protocol Label Switching) network. VPN implementation at Upper layer is based on SSL/TLS - (Secure Sockets Layer/Transport Layer Security). Irrespective of the layer of implementation, the VPN is exposed to DoS attack. This paper deals with IPSec VPN at layer 3 and its DoS attack.

2.2. VPN Categories

VPN can be categorized as Secure or Trusted VPN and Site–to–Site VPN or Remote Access VPN [4]. These categories of VPN often overlap each other. Trusted VPN is a purchased service from the Internet Service Provider (ISP). Here the customer trusts the ISP for the secure data transfer. The data packets move over a set of paths that satisfy the customer requirement and are controlled by the ISP. These types of VPN technology are infrastructure based. Technologies used to implement this VPN are Frame Relay, ATM, and MPLS at layer2 or MPLS/BGP and PPVPN at layer3. Secure VPN uses cryptographic tunnelling protocols that protect data through encryption and authentication. If the customer does not trust the ISP, then customer should go for the secure VPN. It helps in transmitting sensitive information securely over the Internet. Here security of the data transfer is the responsibility of the customer. Secure VPN provides security to the packet. However it does not guarantee the delivery of packets. Trusted VPN provides guarantee on the delivery of packets (QoS), but no security. The focus of this paper is on VPN service that uses the IPSec protocol. It is a hybrid VPN model that combines the Secure and Trusted VPN.

In general, the Secured or Trusted VPN can be categorized into Site-to-Site VPN and Remote access VPN. Site-to-Site VPN allows communication between offices dispersed geographically. The location of the site is fixed. It is again categorized into Intranet that connects organizations' branch offices and Extranet that provides restricted connections to the organizations with their partners. Site-to-Site VPN can be implemented using IPSec, MPLS or combination of both. Remote access VPN connects mobile or home users to their organization. It connects a user to LAN. It can be implemented using IPSec or SSL. The focus of this paper is on security of Site-to-Site VPN.

3. IPSec Based VPN

VPN uses two components for carrying private traffic - the Security Services and Tunnelling. IPSec provides the necessary security service along with the tunnelling capability. Traditional implementation of VPN relies on IPSec. IPSec creates a virtual tunnel between two endpoints. The traffic within the VPN tunnel is encrypted to prevent the interception and analysis of datagram's while they are in the public network. IPSec VPN carries traffic through different types of shared networks, like the Internet in a secured manner.

IPSec is an Internet Engineering Task Force (IETF) standard technology that forms a framework to build security features in IP. IPSec can be deployed across any available network where IP is used for packet forwarding. There is no need to build a new network or make changes in the individual user computer. It reduces the deployment cost of VPN. IPSec works on the Network Layer of the TCP/IP Model [5]. It secures everything that is put on top of the IP layer through encapsulation without considering the type of the application. It supports a variety of encryption algorithms and checks the integrity of the transmitted data. IPSec provides secured key exchange and strong data protection - confidentiality, integrity, and authentication. IPSec VPN client computer becomes a member of the corporate LAN virtually. However IPSec does not protect the VPN service from DoS attack and traffic analysis. Also IPSec VPN solutions are implemented through non standard third-party hardware or software.

IPSec architecture provides a security association (SA) between the end points; SA is a one-way relationship between the end points. It specifies the security parameter index (SPI), destination IP address and security protocol. IPSec is implemented in two phases. In the first phase, it uses Internet Key Exchange (IKE) protocol for handshaking and distributing session keys. In the second phase, it uses Authentication Header (AH) and Encapsulating Security Payload (ESP) for securing the data. These two protocols are the building blocks of the security feature provided by IPSec to build a secure VPN over the IP protocol.

3.1. IPSec Modes

IPSec provides security under two modes of operation - transport mode and tunnel mode. These two modes provide security through any of the ESP or AH protocols [6], [7]. These protocols are meant to provide protection to upper layer. IPSec transport mode is used for a direct communication between the end points. It encapsulates or authenticates only the IP payload. The AH or ESP protocol header is inserted between the IP header and the IP payload. IPSec Tunnel mode is an encapsulation of an IP packet within an IP packet to form an IPSec packet. The payload of this IPSec packet is the original IP packet including both the original IP header and IP payload. The outer IP header is inserted to the IPSec packet to show the tunnel endpoint. This tunnel mode is used to construct a secured VPN. Tunnelling helps in constructing a VPN without the intervention of ISP.

3.2. IPSec Protocols

AH and ESP are the two protocols that provide security service to IPSec. They can operate in tunnel mode or transport mode. AH provides data authentication and integrity service for the IP packet, but it does not provide confidentiality. Internet Assigned Numbers Authority (IANA) has assigned a protocol number 51 to this protocol. The outer IP header's protocol field is set to 51, which shows that the packet is authenticated. The AH header contains Next Header, Length of AH, SPI, Sequence Number and Authentication Data fields. The authentication data is generated using HMAC algorithm – MD5 or SHA on the IP packet.

The ESP protocol provides authentication, integrity as well as confidentiality. IANA has assigned a protocol number 50 to this protocol. The protocol field of the outer IP header is set to 50 to indicate that the packet is encapsulated. ESP packet contains outer IP header, ESP header, IP payload, ESP trailer and the ESP authentication data. The ESP header contains SPI and Sequence Number fields. The ESP trailer contains Padding, Padding Length, Next Header fields and the ESP authentication contains Authentication Data field. The encryption algorithms like DES, 3DES are used.

4. VPN REQUIREMENTS

Customers are expecting ISP to deliver data and telecom connectivity over one or more shared networks with Service Level Agreement (SLA). Customer satisfaction depends on the following factors - Scalability, Stability, Security, and QoS [8], [9]. It is difficult to achieve all at once due to vendor specific service and lack of standards. It is also by its nature that if one factor is improved then the other factor will get affected.

Scalability can be considered at various perspectives like number of VPN, number of sites VPN can support and Number of VPN per PE. Technologies like IPSec, MPLS support different levels of scalability. Stability refers to the availability of the VPN service even though the parts of the network resources are unavailable due to attack or resources depletion or resource failure. The availability of the VPN depends on several components like VPN routing, tunnel stability.

Security is a major problem as the service relies on the shared ISP network to establish its connectivity. To ensure that every VPN on the shared network remains private, a variety of security mechanisms to be addressed include - tunneling, encryption, encapsulation, constrained routing, separation of traffic between different VPN, routing-table separation between VPN, packet authentication, user authentication and access control. The IPSec protocol helps to achieve this. QoS is also a major requirement. Due to Internet connectivity, it is difficult to aggregate traffic flows. Technologies like Integrated Service and Differentiated Service provide prioritized levels of service for voice, video and data applications.

5. THREATS TO IPSEC BASED VPN

The various types of attacks on VPN are Intrusion and DoS attacks [10]. Protection against these attacks is a critical requirement. Intrusions are from outside the VPN in to the VPN, providing unauthorized access into a VPN. DoS attack may be from outside or inside a VPN, preventing access to all authorized users. These attacks may be from any point in the network – the core, other VPN, the trusted site etc. They can attack any point of the network – the edge routers at customer side or provider side, the core router, the VPN site, the end host etc.

Intrusion is an act to bypass the security. Intrusion affects the confidentiality, integrity, availability of resource. A hacker has to send packets, in order to intrude into the trusted zone of the VPN. Here the outsider gets control over some part of VPN. Effective protection of the edge network is required to secure VPN. Effective Intrusion detection system has to be installed to assure that the intrusion points are controllable; that is, there are no hidden intrusion points.

The DoS attack is considered to be a serious attack. DoS attack sends a huge amount of data to the victim. This data can be sent either in many small messages or as one non-ending stream. This useless traffic hinders the normal communication between the organization sites. Frequency of attack is increasing in number and size. The growth rate is very critical. The motives can be personal reasons, prestige issues, material gain or political reasons.

Methods of DoS attack are Protocol based attack and Infrastructure based attack. Protocol based attacks are TCP SYN flood, Teardrop, Black Holes, Ping of death. The attacker makes use of the imperfection in the protocol and services to attack the traffic. This attack can be overcome by checking the vulnerabilities in the protocol and by adding the corresponding patches. Infrastructure based attacks are attacks on any point of the network like edge router, core router. This attack increases the delay, jitter, packet loss and affects the packet delivery ratio. The current Internet infrastructure is in such a way that the attack is possible and the attackers are invisible. Internet allows sending packets to any destination regardless of whether the destination needs it or not. The packet switching technique used by the Internet allows the packet to travel in multiple paths and also there is no technique available to check the path traveled by the packet. The Internet has no centralized management. The DoS attacks directed at network infrastructure can have a serious impact on the overall operation of the Internet and hence the VPN.

Infrastructure based attack is again categorized into two types. They are bandwidth attack and resource depletion attack [11], [12]. By invoking these attacks, the malicious user blocks legitimate user's communication, attempts to consume the resources of a host or application and prevent it from functioning. Bandwidth depletion is also known as flooding attack. Massive consumption of the bandwidth leads to network congestion which causes network breakdown. These types of attacks cannot be prevented by software fixes. To prevent these, we need to use faster hardware or filters. Faster hardware can be effective against hackers with limited resources. Filters are effective in differentiating attack packet from legitimate packet. Because the attack packets have some distinguishing features like same IP address, same contents or recognizable pattern in port number choices. These features can be identified and routers can be configured to drop the malicious packets. Filtering techniques such as History-based IP Filter, Ingress egress filtering and Hop count based filtering are available. Resource depletion (also Flaw-based) depletes the key resources such as CPU, memory, buffer in the router, end system, firewalls etc. It can lead to loss of availability or unintended behavior due to processing delays. It makes use of bugs in software to deplete resources. Installing respective software patches or using latest software can prevent these types of DoS attacks.

Direction to handle DoS is - Prevent before the attack occurs and respond at once as the attack occurs. The growth in DoS attack is so high that the prevention, detection, protection have to be done near the source of the attack than at the victim's end. Earlier detection is necessary for better protection. It also helps to prevent the attack from saturating the high speed link inside the core. Attacks are difficult or impossible to block completely. It forces organizations to monitor traffic continuously and react quickly to any suspicious activity. If it is possible to find the origin of the attack then the IP address can be recognized and packet can be dropped. The attack router can be identified and shield. There is no general solution; all solutions are specific to the attack type. Preventing DoS attack is a tedious task. The IPSec protocol protects VPN from various types of attacks against integrity, confidentiality, authentication and replay attack but does not stop DoS. Our focus is to protect IPSec based VPN service from DoS attack.

6. RELATED WORKS

In [13] the author deals with mitigation strategies against access link flooding attack in VPN. The strategies proposed are assigning multiple IP addresses to the endpoints of the VPN and implementing tunnel splitting. The problem faced by these methods is described below. Assigning multiple IP addresses results in inefficient usage of scarcely available IP address space. Tunnel splitting uses trusted third party tunnel concatenation device (TCD) [14] and employs multiple IPSec encryption and decryption. This impairs the performance of the overall VPN. In addition to this, the TCD is a trusted third party.

In [15], the author discusses protection of signaling and routing mechanism in MPLS VPN from DoS attack. Authors suggest mechanism to harden the network perimeter. This concentrates on the routing mechanism. They propose the protection through firewall and anomaly detection techniques.

7. ATTACK MODEL AND ASSUMPTIONS

We consider the following network model to construct the VPN in our research work. The VPN is considered as an overlay network over the traditional IP network service offered by one or more providers. The overlay service is a SLA between the customer and the ISP. The keys used are pre shared and considered to be protected adequately. Hose model or pipe model can be used for bandwidth allocation. The control plane in this model is assumed to be secure. Our focus is on the data plane. Type of VPN considered in this work is a Layer-3 IPSec based site-to-site VPN. Each host in a customer network is connected to the Customer Edge (CE) router. The CE is connected through an access link to the Provider Edge (PE) router. The PE router connects the site to the Internet ISP network. The provider core can be an ordinary IP network or it can be an MPLS network.

The IPSec protocol in its tunnel mode is used to construct the VPN. The VPN sites need not have to use globally unique addresses rather they can use their local LAN addresses. The packets from a customer network cannot be transmitted over the ISP network with their local IP addresses. This problem is solved by the IPSec tunneling mechanism. The IPSec tunnel is set between the CE peers which form the VPN gateway. The CE peers act as the VPN end points and tunnel termination points [16], [17]. The different sites of the VPN are securely inter-connected through tunnels. Tunneling helps in encapsulating the packet in such a way that the packet gets a globally unique IP address and at the same time it retains its local IP address. The packet forwarding principle of this VPN model is similar to ordinary IP packet forwarding except that the packet is forwarded through an IPSec tunnel. Packet originating from a host on one site of the VPN is encapsulated using IPSec protocol (ESP/AH) in the CE connected to that site and then routed to its peer site. The peer CE decapsulates it and forwards to the intended host. The described model is shown in Figure 1.

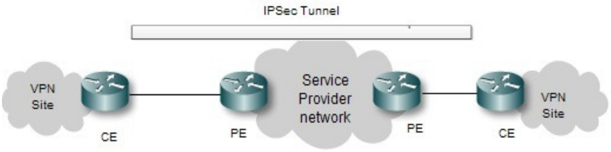

Figure 1. IPSec VPN with CE to CE tunneling.

8. SECURITY ANALYSIS OF THE MODEL

The proposed VPN is based on IPSec protocol. AH and ESP protocols of IPSec as described in Section III, provide various security features like confidentiality, authenticity, protection against reply attack and integrity but it does not provide any protection against DoS attack. Our proposal is to protect this VPN network model from DoS attack so that the VPN service is stable.

8.1. Spoofing

The DoS attack against a VPN may affect the network infrastructure of the VPN site or the network infrastructure of the ISP. The network is protected against the randomly generated DoS attack that is launched against the ISP infrastructure by using a simple filtering technique at the edge routers. The edge routers are protected with packet filters to allow only the IP VPN traffic through the overlay network. The filtering technique filters all packets with random and unroutable IP address. It allows only the VPN with the registered flow label - the source destination pair. This makes the VPN protected from the randomly generated packets [18]. Hence DoS attack against this VPN model can be mounted only by attempting to insert spoofed packet. Filtering technique will not filter spoofed packet. Flooding spoofed packet in small quantity is very much enough to affect the QoS. These packets are non-authentic packets from outside of a VPN into a VPN. These non authentic packets might exhaust the bandwidth available to the overlay VPN and as the result the VPN service gets affected. The defense mechanism is a complicated one as the original source cannot be identified from the spoofed packets.

8.2. Point of Protection

The attack to the VPN service is possible only through the edge router namely PE which is part of the ISP network. In the edge network if the PE is shared by several CEs, then a CE router can spoof packets and attack a VPN. The malicious traffic does originate from any of the CE that is connected to the PE. The packet flooding directed at the PE router with arbitrary source addresses will not be able to attack the VPN service as they can be filtered at the PE router. Hence the VPN service will only be affected by attack traffic directed at the PE router with a spoofed source address of the VPN flow. Better implementation of the DoS defense is towards the source of the attack. This shows that it is better to implement the DoS defense at the PE router. This would stop attack packet from entering into the network, also avoids congestion and resource exhaust. If the PE router is protected then the provider network infrastructure, VPN services and VPN user sites can be protected.

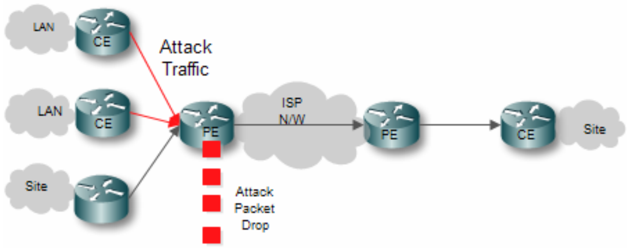

Figure 2. Attack packet dropped at PE router

9. PROPOSED STRATEGY

The Protection mechanisms focus on flooding attack at the data plane of the VPN. We describe two categories of protection. The first type of protection mechanisms is based on filtering technique and the other is based on cryptographic technique. The VPN service can be effectively protected if its edge network is effectively protected. Our techniques focus on protecting the edge network. All the protection mechanisms are to be implemented at edge router namely the PE. This has the advantage that only the PE router has to implement these mechanisms and the core router can forward without any need to add extra features to it. Figure 2 represents the proposed strategy.

9.1. Filtering Mechanism

We now describe our proposal for protecting the VPN service against the spoofed packet flooding attack. The protection is through a simple filtering technique. We assume that the traffic from the edge router CE attached to the VPN site is of valid packets and malicious traffic can only be generated by outsiders of VPN. The outsider has no knowledge of the shared secrets between the edge CE routers. The spoofed packet which arrives at PE will have IP address spoofed but it will not be encapsulated in an IPSec protocol. This provides a way for another filtering rule to be added to the filter at the PE router. The rule is to filter all packets even with a valid source destination address, if the protocol number present in the IP headers' protocol field is not ESP–50 or AH-51 number of IPSec protocol. The above technique will filter all spoofed packets towards the VPN which are not encapsulated in IPSec. If the spoofed packet is encapsulated in IPSec then the following method can be used to filter the flooding packet. In addition to checking protocol number of the incoming packet, the PE router can also check the SPI and the sequence number order.

9.2. Cryptographic Mechanism

We propose another mechanism to protect VPN service from DoS attack. It works in between the CE and PE at the source side. This is based on random number and cryptographic encryption and decryption techniques. The random numbers generated and the key used for encryption decryption are assumed to be secured. Nonce - the random number is shared by PE router to CE router of the VPN. The nonce is encrypted by the CE router at the source side using the pre shared secret key. This nonce is attached in between the IP header and ESP header. This forms the extended ESP header (Figure 3). The PE router at the edge network will decrypt the extended part of ESP header. The PE now checks if the nonce it got through decryption is the one which it has already shared. If the verification is concluded to be true then the packet is forwarded otherwise the packet is not a valid one and it is dropped.

IP header	Extended ESP header	ESP payload	ESP Auth

Figure 3. IPSec packet with extended ESP header

10. CONCLUSIONS

We proposed two techniques to protect site-to-site VPN service from DoS attack. One is based on filtering technique and the other is on extended ESP header based cryptographic technique. The paper considers the best point to enhance the security is PE router at the edge network. PE router should be strengthened to identify the illegitimate packets and to prevent them from entering the service provider network. This helps to protect the service provider network and makes it fool proof. This also helps in hardening the perimeter of service provider. Once the service provider network is secured, the customer networks are also secured. Our current work is towards the outside attack through IP Spoofing. We are also to extend our work to inside attack.

REFERENCES

[1] Olalekan Adeyinka, (2008) “Analysis of problems associated with IPSec VPN Technology”, *Electrical and Computer Engineering, CCECE*, pp 1903-1908.

[2] Wafaa Bou Diab, Samir Tohme & Carole Bassil, (2007) “Critical VPN Security Analysis and New Approach for Securing VoIP Communications over VPN Networks”, *WMuNeP”07*, pp 92-96.

[3] Roger Younglove, (2000) “Virtual Private Networks - how they work”, *Computing and Control Engineering journal,* pp 260-262.

[4] Jaha A.A., Ben Shatwan.F. & Ashibani M., (2008) “Proper Virtual Private Network(VPN) Solution”, *Second International Conference on Next Generation Mobile Application Services and Technologies*, pp 309-314.

[5] S. Kent & R. Atkinson, (1998) “Security Architecture for the Internet Protocol”, *RFC 2401*, IETF Network Working Group.

[6] S. Kent & R. Atkinson, (1998) “IP encapsulating security payload (ESP)”, *RFC 2406*, IETF, Network Working Group.

[7] S. Kent & R. Atkinson, (1998) “IP Authentication Header (AH)”, *RFC 2402*, IETF, Network Working Group.

[8] Perry B. Gentryl & Pricewaterhouse Coopers, (2001) “What is a VPN?”, *Information Security Technical Report*, Elsevier Science Ltd, Vol. 6, pp 15-22.

[9] Matthew Finlayson, Jon Harrison & Richard Sugarman, (2003) “VPN Technologies - A Comparison”, *Data Connection Limited, http://www.dataconnection.com.*

[10] Michael H. Behringer & Monique J. Morrow, (2005) “MPLS VPN Security”, *Cisco Press*, 312 pages.

[11] Peng.T., Leckie.C. & Ramamohanarao. K., (2007) “Survey of network-based defense mechanisms countering the DoS and DDoS problems”, *ACM Comput.* pp 39-42.

[12] Michael Glenn, (2003) “A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment”, *SANS Institute*, GSEC Practical Version 1.4b.

[13] R. Ramanujan, M. Kaddoura, J. Wu, C. Sanders & K. Millikin, (2003) “VPNshield: protecting VPN services from denial-of-service (DoS) attacks”, *DARPA Information Survivability Conference and Exposition*, Proceedings, vol. 2, 2003, pp138-139.

[14] Ranga S. Ramanujan, Maher Kaddoura, John Wu, Kevin Millikin, Doug Harper & David Baca, (2002) “Oragnic Techniques for Protecting Virtual Private Network (VPN) Services from Access Link Flooding Attacks”, *ICN.*

[15] Denise Grayson, Daniel Guernsey, Jonathan Butts, Michael Spainhower & Sujeet Shenoi, (2009) “Analysis of security threats to MPLS virtual private networks”, *International Journal of Critical Infrastructure Protection*, pp146-153.

[16] Syed Noor-ul-Hassan Shirazi, Muhammad Asim, Muhammad Irfan, & Nassar Ikram, (2010) “MPLS Unleashed: Remedy Using IPSEC over MPLS VPN “, *Springer-Verlag Berlin Heidelberg, ISA, CCIS 76*, pp241-48.

[17] Satish Raghunath, K. K. Ramakrishnan, & Shivkumar Kalyanaraman, (2007) “Measurement-Based Characterization of IP VPNs”, IEEE*/ACM Transactions on Networking*, Vol. 15, No. 6, pp1428-1441.

[18] www.firstnetsecurity.com/library/ibm/ipsecvpn.pdf, (1998) “Using IPSec to Construct Secure Virtual Private Network”, *IBM Corp*.