International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

Firewall and VPN Technology

Amruta Jagtap

Abstract: ***Corporations and organizations world-wide hinge on Firewall and VPN technologies for safeguarding their crucial resources and information while sharing their services on the Internet. This review paper briefly describes the types of firewall technologies and the VPN technologies along with the detailed working of the firewall and VPN technology. Firewall technology is used mainly to block or allow connections to applications hosted by corporations or organizations while VPN technology is used for secure communications between organizations located at several destinations across the world.***

Keywords: packet filtering, encapsulation, firewall

1. Introduction

With the advancement of technologies and the exponential growth of crucial data led to the need of information and systems defense mechanisms. Most salient factor of developing a technology includes security from the outside untrusted network. Firewalls and VPNs are the two most crucial defense mechanisms implemented by corporations, organizations and agencies to safeguard resources and information. Firewall technology is used to provide security and prevent malicious attacks on data and systems. The literal meaning of firewall is a wall of brick that prevents fire from spreading out. In the digital world, firewalls preclude the proliferation of detrimental malicious codes that make the system vulnerable through filtering. Firewall can be a hardware device or software installed on a hardware device. There are two main types of implementations of firewall technology: host firewall and network firewall. Firewalls implemented to protect only the host device from external networks are host firewalls and firewall protecting an entire network from outside network is a network firewall.

Firewalls provide the mechanisms to allow or block internet traffic incoming or outgoing to network applications. This is done by maintaining predetermined firewall rules that allow or block the communications traffic. Firewalls maintain a database of rules known as ACL – Access Control List, which contains set of firewall rules. ACLs are used during verification of the incoming and outgoing packets. If the firewall rules are not matched, then the incoming or outgoing data packets are dropped. For example, iptables, firewall in-built in Linux distributions and does not need any service to be installed. There are three main default policies of iptables which are: Accept, drop and reject. Following are the commands to implement default policies or the ACL rules in Linux firewall:

1. To allow incoming and outgoing packets:
   iptables –P INPUT ACCEPT
   iptables –P OUTPUT ACCEPT

   To allow data forwarding from one interface to another:
   iptables –P FORWARD ACCEPT

2. To allow or drop/reject packets of specific protocols:
   iptables –A INPUT –p icmp –j ACCEPT
   iptables –A INPUT –p icmp –j DROP

where –A indicates append this rule on incoming packets and –j indicates jump to accept the packet or drop/reject the packet. Reject policy is used instead of Drop policy.

Firewall technology mainly alerts the monitoring systems of unauthorized connections intending to break in through techniques such as IP spoofing, malicious codes hidden in the data sections or header of the packets etc. These alerts are then processed by antivirus tools that analyze the packet for any malicious codes and avert it from making a system vulnerable.

2. Theory

Packet filtering

In packet filtering, each packet arriving at the firewall is inspected according to the rules predetermined by the firewall administrators. Based on the firewall filtering rules the packet is dropped, allowed to pass through the firewall or rejected. Packet filtering technology is the first generation firewall technology developed in 1988 by engineers at DEC. Implementation of packet filter firewall is less complex as it requires less hardware components, for example the basic implementation does not need a hard drive and can boot from a CD or floppy. At the network layer, two fields in the IP header of a packet are inspected: Source and destination IP address and protocol field. At the Transport layer, source and destination port number is inspected in the TCP header. The packet matching the rules of the firewall is allowed to pass through to access the application behind the firewall. In stateless filtering firewall or packet filtering, the firewall does not store the state of each packet.The data section of the packet is not inspected hence it does not know the state of the packet i.e. if thepacket belongs to any established connection or is establishing a connection. [1] Advantage of packet filtering firewall is – easy installation and faster performance, but it is easier to trick a stateless filtering firewall by IP spoofing as it does not store the state of packet. Packet filtering firewall is not favorable for FTP as FTP server communicates with the client from port 21 and needs access to port between 1024 and 65535. This port number is allocated dynamically by the application and is used temporarily only for that session. Packet filtering firewall does not store the state of packet hence it is likely that the FTP packet will be dropped. [1] Stateless packet filtering firewall operates at layer 3 (network layer) of the OSI model.

Application Proxies

Application layer firewall is a second generation firewall that operates at seventh layer of the OSI model. Packet filtering firewalls can prevent cyber-attacks at higher layers but only after the inculcation of additional software. Application layer firewall, an extension of packet filtering firewalls, overcomes this short come. This type of firewall is not based on port number evaluation but on the evaluation of the data section of packet. Application layer firewall inspects the data section of the packet along with packet headers. If the information in the data section and the packet headers matches the firewall rules specified in the firewall database, then the firewall allows a connection to be initiated with the server hosting the application. Application firewall acts as a proxy between the server and the outside network. It inspects the incoming traffic and initiates connection between the server and the approved hosts on behalf of the server.

The incoming traffic is first inspected according to the rules specified in ACL and then the state session is monitored. After the basic stateful packet filtering, connection between server and the host is initiated. The application firewall monitors the data section of the packets i.e. the digital signature or the pattern of the data. The application firewall provides proxy for applications like FTP, HTTP, telnet and SOCKS. The firewall is complex and requires high end hardware configuration. Firewall maintains a cache to temporarily store the data packets while it is being processed. Application firewalls also support secure authentication methods. This firewall establishes additional connection which might cause firewall to become bottleneck, which might make the system vulnerable.

Stateful packet inspection [SPI]:

Stateful inspection, also known as dynamic filtering was developed in 1994 by Check Point Software in the FireWall 1 product. Stateful firewall inspects the state of the data packet. Also known as circuit level gateway firewall, it acts as a gateway between server and outside network. This firewall monitors the TCP Handshaking between an untrusted host and the server to decide if the TCP session is valid. [3] Circuit level gateway firewall monitors the data in the packet headers when a session is being created, thus operating at session layer of the OSI model. The circuit level gateway first allows a connection to be initiated after the basic packet filtering and then initiates a TCP handshake session.

Stateful firewalls maintain a dynamic state table that stores the state of the data packet. The state of a packet represents information such as SYN request, SYN-ACK, SYN-ACK-SYN and additional information such as SYN flag, sequence number of the packet etc. that indicates the session it belongs to. During the TCP handshake, to determine if the TCP session is valid, firewall monitors the data in the packet headers and inspects if the SYN flag, ACK number and sequence number is logical. If the TCP Handshake is valid, the client to server session is initiated.When establishing a new connection, extensive inspection is done of the packet. It is also cross checked with the ACL and if satisfies the packet is passed through. Packets belonging to already established connections are passed through by checking the packet information with a table of current connections maintained by the firewall. When a session is terminated, the connection entry is removed from the firewall. Circuit level gateway firewall acts as a proxy between the server and the untrusted hosts. This firewall helps prevents attacks such as SYN flood on the server.

For example, Iptables in Linux is a type of stateful packet inspection firewall. Iptables can be configured to allow packets of specific state belonging to already established connections. Commands to configure iptables to allow state monitoring of packets:

iptables –A INPUT –m state --state RELATED,ESTABLISHED –j ACCEPT

where –m indicates the module and state indicates the state of the data packet.

Virtual Private Network (VPN)

Virtual Private Network is a private point-to-point network created over an already existing network such as Internet Protocol (IP) Network, with the inculcation of additional features such as encryption, user confidentiality and protection of data. In VPN a private point-to-point link is established between two peers by encapsulating the communications payload with VPN protocol headers. VPN also provides encryption to the payload by using cryptographic algorithms. Authentication is provided by VPN by using public keys and digital signatures. Data integrity check is done by using a message digest to check if the data has been tampered with during transmission. VPN includes two types of architectures: Gateway to gateway architecture and Dial up VPN architecture. Secure communication channel established between organization's gateways is gateway to gateway VPN. While a dial up VPN is a secure connection established between an organization's gateway and an official at remote location, to access organization's resources is a Dial up VPN.VPN incorporates following tunneling protocols:

- Point to Point Tunneling Protocol
- Internet Protocol security
- Layer 2Tunneling Protocol
- Secure Socket Tunneling Protocol

IP Security [IPSec]

IPsec, open standard, is a network layer tunneling protocol used in VPN technology. IPsec provides authentication, data integrity, encryption and confidentiality and precludes data replays. In Linux, NETKEY is Linux kernel implementation of IPsec. IPsec VPN works in two modes – transport mode and tunnel mode.

1) Transport mode

Transport mode is less secure as there is no additional header. As there is less overhead, transport mode is faster than the tunnel mode. ESP or AH header is inserted after the IP header. Transport mode works well with NAT devices.

2) Tunnel Mode

Tunnel mode operation is slower than the transport mode as additional IP header is added to the IPsec encapsulated packet. In this mode, there is a need for NAT traversal in case of NAT devices, AH with tunnel mode does not work on NAT device as a new IP header is added in the tunnel

mode and the hash value generated is different in a NAT device. Hence NAT traversal is used in this case. In NAT traversal, IKE negotiations use UDP 4500 port in phase 1. UDP port 4500, IKE port 500 and protocol port 50 or 51 should be open during NAT traversal. [2] IPsec VPN includes four important protocols that establish the VPN connection:

a) Internet Key Exchange
b) Authentication Header
c) Encrypted Security Protocol
d) Security Associations

a) Internet Key Exchange [IKE]

IKE provides the mechanism to exchange security services and session authentication and encryption keys. In Linux libreswan, openswan and stronswan implementation provides IKE daemon 'pluto'. IKE has two phases of operation:

Phase 1: In phase 1 of IKE, the tunnel ends are authenticated. IKE authentication methods include digital signature, public key and pre-shared key. In pre-shared key method, hash key is generated and used by VPN entities to authenticate each other. IKE SA are negotiated and established for secure key exchange. Secret keys are then generated using the Diffie-Hellman algorithm. [2] Diffie-Hellman generates cipher keys using the pair of private and public keys of the tunnel entities. Diffie-Hellman includes three groups: group 1 of 768 bits, group 2 of 1024 bits and group 3 of 2048 bits.

Phase 2: In phase 2 of IKE, pair of IPsec SAs is established for secure data transfer. [2]

b) AH Authentication Header [AH]:

The authentication header is an IPsec protocol that provides source authentication, integrity of packets and anti-replay service. In this protocol, an authentication header is added in the IPsec data packet after the IP header. The IP address does not change in this protocol hence this protocol does not facilitate payload encryption. The authentication header consists of hashed value of packet information such as Security Parameter Index (SPI), sequence number which is allotted to every packet, header length and hashed authentication data. Security Parameter Index is a 32 bit number that indicates the protocol number used i.e. AH (51). [2] AH protocol uses the sliding window method, where every packet is sequenced and the packet is permitted in the window if the sequence number is within the window, to prevent replay of packets.

c) Encrypted Security Protocol [ESP]:

Encrypted Security Protocol is another IPsec protocol that provides data integrity, source authentication along with data encryption. In this protocol the payload is encapsulated by the ESP header and the ESP trailer. The ESP header is appended after the IP header and the ESP trailer is appended at the end after the payload. [8] Encrypted Security Protocol also provides source authentication for the encapsulated payload. ESP configuration for authentication-only or encryption-only is possible in IPsec VPN. ESP header consists of Security Parameter Index (SPI) that indicates the protocol number as ESP(50) and the sequence number of the packet. ESP provides an additional feature which is not provided in AH i.e. payload encryption. Encryption of payload is done by using symmetric encryption algorithms such as AES, DES, 3DES and Blowfish. [2]

Point to Point Transport Protocol [PPTP]:

Point to Point Transport Protocol is an older VPN tunneling protocol, still supported by windows and Linux systems. The working of PPTP is a communications protocol used widely for point to point access, mainly based on communications protocol PPP (Point to Point Protocol) and TCP/IP. PPP facilitates communication between two directly connected entities in which IP packet is encapsulated in PPP packet. [7] Generic Routing Encapsulation protocol allows encapsulation of network protocols over a different set of network protocols. PPTP uses Generic Routing Encapsulation (GRE) protocol for encapsulation of PPP data.PPP packet is encapsulated in GRE protocol packet with a GRE header which contains the routing information. [2] This GRE packet is encapsulated in a normal IP packet, where in the protocol number is 47 which indicate GRE protocol. The payload encapsulated by PPP header is encrypted using the cryptographic algorithms supported by PPP. This payload is the PPTP control connection message that maintains the PPTP tunnel. In Point-to-Point Tunneling Protocol, source authentication is done by the protocols supported by PPP such as Extensible Authentication Protocol (EAP), Challenge Handshake Protocol (CHAP), Shiva Password Authentication Protocol (SPAP) and Password Authentication Protocol (PAP). [2] PPTP network server (PNS) establishes a tunnel through TCP connection known as the control connection with the PPTP access concentrator (PAC). This control connection is responsible for creating, maintaining and terminating the GRE tunnel through which encrypted data is communicated between two entities using PPTP VPN.

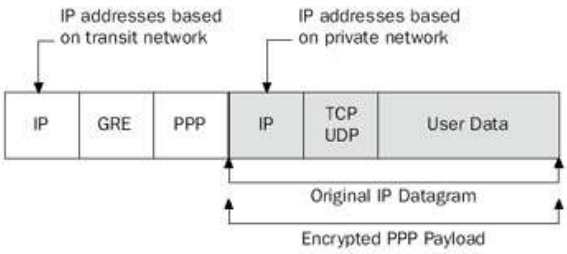

Figure 4: Packet formation PPTP

Layer 2Tunneling Protocol [L2TP]:

L2TP, layer 2 tunneling protocol, is a product of partnership between Cisco and Microsoft. It is a combination of PPTP and Layer two Forwarding. In L2TP VPN the PPP payload is encapsulated in L2TP frames while sending over IP, x.25, frame relay or ATM networks. These L2TP frames are encapsulated in UDP packets. The working of L2TP is similar to that of PPTP with additional features and strong encryption algorithms. Similar to PPTP, a control connection is created between a Network Access Server (NAS) or ISP which acts as a L2TP Access Concentrator (LAC) and L2TP Network server (LNS) using UDP control messages for maintaining the tunnel. PPP packet is encapsulated with a L2TP header that contains the control message for maintaining the connection. [7]L2TP Network Server and L2TP Access Concentrator use UDP port 1701. LAC and LNS are two endpoints of L2TP connection. The

L2TP tunnel endpoints authenticate each other using the authentication methods supported by PPP such as CHAP.

L2TP can also be configured using IPsec. In L2TP with IPsec, the L2TP encapsulated payload is encrypted using IPsec encryption algorithms. This encrypted payload in encapsulated with IPsec header and IPsec trailer. IPsec provides the confidentiality, source authentication and data integrity. L2TP with IPSEC uses 56 bit DES or 168 bit 3DES.[2]

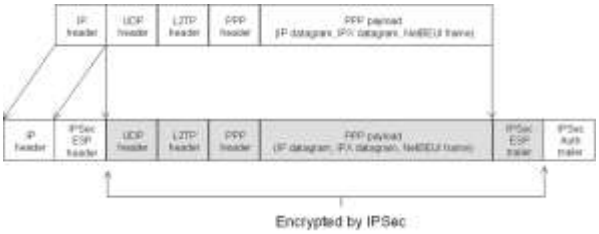

Figure: Format of packet encapsulated by L2TP with IPsec

3. Secure Socket Tunneling Protocol SSTP

SSTP is a new Microsoft proprietary VPN tunneling protocol that provides transport level security. SSTP facilitates a mechanism to transfer PPP traffic through SSL/TLS protocol. SSTP VPN is a built-in service in windows 7, 8 and 10. The SSTP client connects with the SSTP server on port 443 through TCP. The SSTP client sends the SSTP server an SSL Hello message that mentions the protocol version it is using for this session and the cryptographic algorithms it supports. SSTP server then selects the cryptographic algorithm and sends back a hello message to the client that consists of certificates. SSTP client generates a session key and uses these certificates to encrypt the session key, which is sent to the SSTP server. [4] SSTP server decrypts this key using its private key and the further communications are encrypted with the session key and the encryption algorithm thus providing confidentiality. The SSTP client and server negotiate and establish PPP tunnel that includes authentication using the authentication protocols supported by PPP. The SSTP client then begins sending IPv4 or IPv6 traffic over the PPP tunnel. SSTP has strong encryption algorithms such as AES that uses keys of size 128, 192 or 256 bits. [9]

4. Conclusion

With the Firewall technology and VPN technology, implementation of the CIA model in the network communications became easier. Firewalls not only provide security to resources but also allow monitoring of the network traffic. Firewall incorporated with Antivirus tools makes real time network defense possible. But for complete security requires additional components or tools. Advancement of VPN technology provides confidentiality and security, the most significant requirements of organizations. Although VPN technology provides security, its complexity does not always work with proprieties of different organizations.

References

[1] Rohit Goel1, Durgesh Kumar2, Abhishek Raja, "A Packet Filtering Firewall", February 2014
[2] Poonam Arora, Prem R. Vemuganti, Praveen Allani, “Comparison of VPN Protocols – IPSec, PPTP, and L2TP”
[3] Robert Zalenski. Firewall technologies. In the IEEE Conference 2002.
[4] [MS-SSTP] - v20160714, Secure Socket Tunneling Protocol (SSTP), Microsoft Corporation, July 14, 2016
[5] Packet Filtering http://www.informit.com/articles/article.aspx?p=376125&seqNum=10
[6] Firewalls https://technet.microsoft.com/en-us/library/cc700820.aspx
[7] What is VPN?
[8] https://technet.microsoft.com/en-us/library/cc731954(v=ws.10).aspx
[9] What is IPsec?
[10] https://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx
[11] SSTP Remote Access Step-by-Step Guide: Deployment
[12] https://technet.microsoft.com/en-us/library/cc731352(v=ws.10).aspx