International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Firewall: A Security Point of a Network

Manoj Parmar[1]

[1]IT Department, Government Polytechnic, Himatnagar

Abstract: ***A firewall is a software program or hardware with software program that creates a security perimeter whose main function is control unauthorized access of incoming and outgoing data or information over a network. Firewalls protect you from offensive software that may come to reside on your systems or from prying hackers. When connected to the internet, even a standalone PC or a network of interconnected computers make easy targets for malicious software & unscrupulous hackers. A firewall can offer the security that makes you less vulnerable and also protect your data from being compromised or your computers being taken hostage. A firewall protects the flow of traffic over internet and is less restrictive of outward and inward information and also provides internal user the illusion of anonymous FTP and www connectivity to internet.***

Keywords: Firewall, attacks, gateways, packet filter, intruder, application gateways.

1. Introduction

Any computer network is designed to connect two or more computers located at same or different places. They are free to exchange information with any other computer connected in a network [1]. This type of sharing is having very good advantage for both individuals as well as for corporate world but as we know in today's era, most important and confidential information is also exchanged on internet so an intruder or an attacker can do easily attack and can find out the important information and can harm the company in any manner.

2. Types of Attacks in a Network

Main types of attacks in a network by external entity are:

2.1 Passive Attack

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user [2].

2.2 Active Attack

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data [2].

2.3 Distributed Attack

A distributed attack requires that the adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date [2].

To secure network from these types of attacks, it is desirable to introduce firewall in a network.

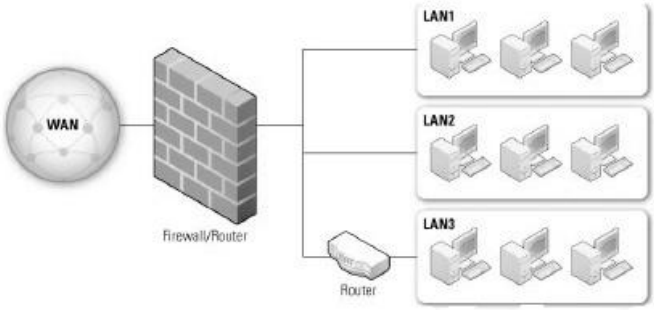

Figure 1: Sample use of firewall in a network [3]

3. Characteristics of Good Firewall :[4]-[5]

3.1 Transfer of information either from inside to outside or from outside to inside must pass through the firewall.
3.2 The authorized traffic should be allowed to pass.
3.3 The firewall must be strong enough to prevent from attacks.

4. Firewall Logic

Firewalls use 3 types of filtering mechanisms:

4.1 Packet filtering or packet purity

Data flow consists of packets of information and firewalls analyze these packets to sniff out offensive or unwanted

packets depending on what you have defined as unwanted packets [3].

4.2 Proxy

Firewalls in this case assume the role of a recipient & in turn send it to the node that has requested the information & vice versa [3].

4.3 Inspection

In this case Firewalls instead of sifting through all of the information in the packets, mark key features in all outgoing requests & check for the same matching characteristics in the inflow to decide if it relevant information that is coming through [3].

5. Firewall Actions and Policies

To protect private networks and individual machines from the dangers of the greater Internet, a firewall can be employed to filter incoming or outgoing traffic based on a predefined set of rules called firewall policies.

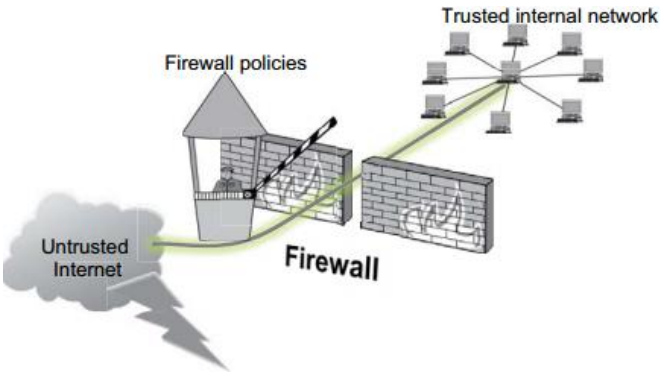

Figure 2: Schematic connection of firewall [5].

Packets flowing through a firewall can have one of three outcomes: –

- Accepted: permitted through the firewall
- Dropped: not allowed through with no indication of failure
- Rejected: not allowed through, accompanied by an attempt to inform the source that the packet was rejected

Policies used by the firewall to handle packets are based on several properties of the packets being inspected, including the protocol used, such as:

- TCP or UDP
- The source and destination IP addresses
- The source and destination ports
- The application-level payload of the packet.

6. Types of Firewalls

There are different kinds of technique which may be implemented by a firewall. Some of them are as follows:

6.1 Packet Filtering Firewall

A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet (Figure 3). The firewall is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

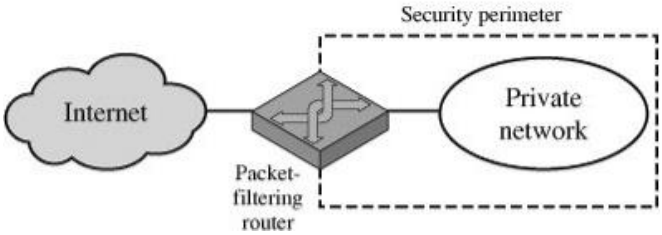

Figure 3: Packet Filter firewall [5]-[6]

6.2 Application-Level Gateway

An application-level gateway, also called an application proxy, acts as a relay of application-level traffic (Figure 4). The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. If the gateway does not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features.

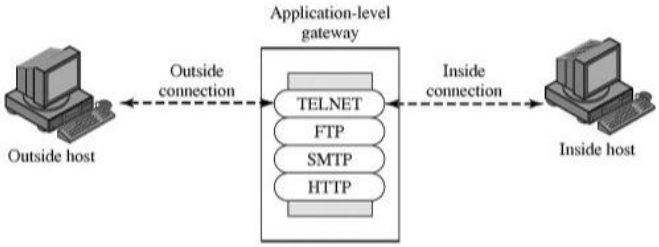

Figure 4: Packet Filter firewall [5]-[6]

6.3 Circuit-Level Gateway

A fourth type of firewall is the circuit-level gateway or circuit-level proxy (Figure 5). This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed. A typical use of circuit-level gateways is a situation

in which the system administrator trusts the internal users. The gateway can be configured to support application- level or proxy service on inbound connections and circuit-level functions for outbound connections. In this configuration, the gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.

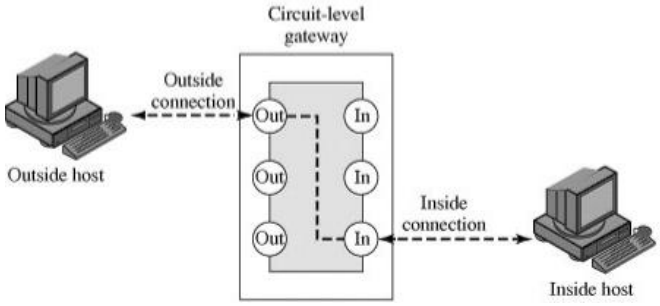

Figure 5: Packet Filter firewall [5]-[6]

7. Comparision

Table 1: comparison of various types of firewall [7].

Firewall type	Performance	Modify client Application	Defends against attacks
Packet filter	Best	No	Worst
Circuit Level Gateway	Medium	No	Medium
Application Level Gateway	Worst	Yes	Best

8. Conclusion

The requirement of firewalls has led to their ubiquity. Almost every organization connected to the Internet has installed some types of firewall. The result of this is that most organizations have some level of protection against threats from the outside. Attackers still probe for vulnerabilities that are likely to only apply to machines inside of the firewall. They also target servers, especially web servers. However, these attackers are also now targeting home users who are less likely to be well protected. The beginnings of a simple form of distributed firewalls are already here, with personal firewalls being installed on individual machines. However, many organizations will require that these individual firewalls respond to configuration directives from a central policy server. This architecture will simply serve as the next level in an arms race, as the central server and the protocol(s) it uses become special targets for attackers. Firewalls and the restrictions they commonly impose have affected how application-level protocols have evolved. Because traffic initiated by an internal machine is often not as tightly controlled, newer protocols typically begin with the client contacting the server; not the reverse as active FTP did. The restrictions imposed by firewalls have also affected the attacks that are developed. The rise of email-based attacks is one example of this change.

References

[1] https://www.microsoft.com/security/pcsecurity/firewalls-whatis.aspx
[2] http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-ttack.html
[3] http://www.firewallinformation.com/
[4] Cryptography and Network Security, 2nd Edition, Forouzan Mukhopadhyay, McGraw Hill Publication.
[5] Network Security Essentials, 4th Edition, William Stallings, Pearson Publication.
[6] http://cs.brown.edu/cgc/net.secbook/se01/handouts/Ch06-Firewalls.pdf
[7] http://www.deic.uab.es/material/26118-stallings_firewalls.pdf

Author Profile

Manoj Parmar received the B.E. degree in Electronics & Communication engineering from Nirma Institute of Technology, Ahmedabad and M.E. degree in Electronics & Communication Engineering from Charotar Institute of Technology, Changa, Gujarat in 2010. He is now working as a Senior Lecturer, IT Department Government Polytechnic, and Himatnagar.