Firewall

Presented By –

Kornel Das
Dept.:- CSE
Roll:- 16800117046

CONTENT

- Introduction
- What is firewall
- Application of Firewall
- Types of Firewall
- Software Firewall Vs. Hardware Firewall
- Role of Firewall

CONTENT

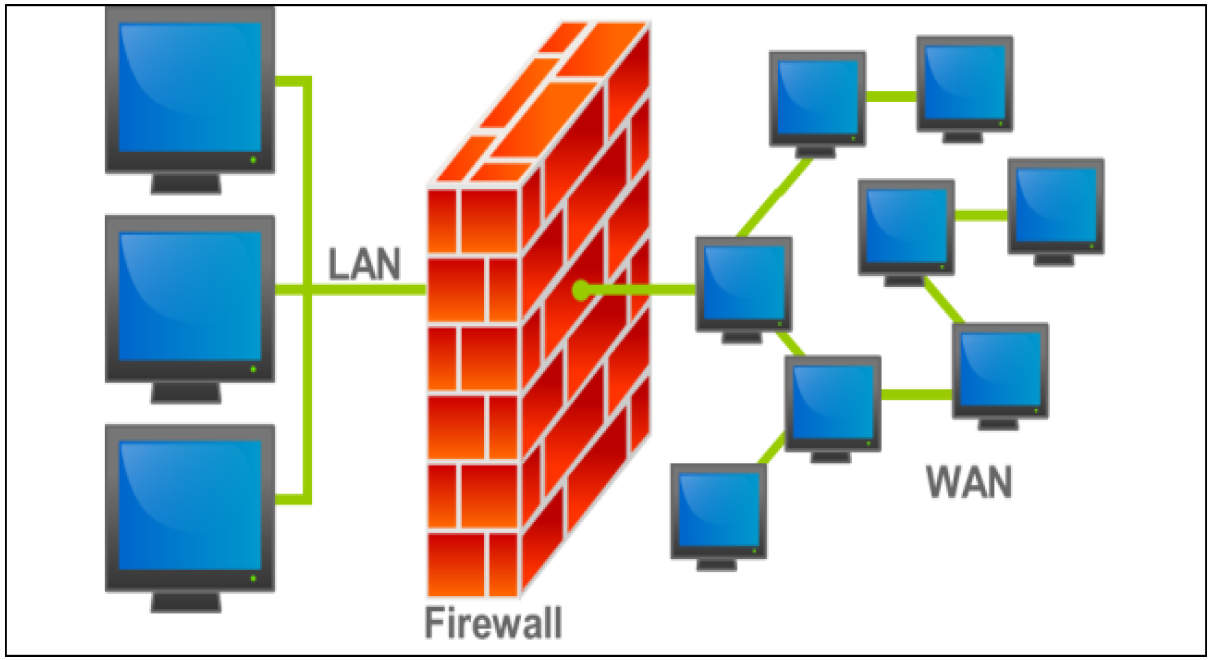
- Advantages of Firewall
- Disadvantages of Firewall
- Conclusion

INTRODUCTION

- The Internet has made large amount of information available to the average computer user at home, in Business and Education.
- For many people, having access to this information is no longer just an advantage, it is essential.
- Therefore, security of network the main criteria here and Firewalls provide this security .

What is Firewall?

- A Firewall is simply a program or hardware device that filters the information coming through the internet connection info your private network or computer system.



What is an application of Firewall?

- An application firewall is a special firewall that is specially coded for the type of traffic it is inspecting.
- The most widely developed application firewall is the web application firewall.

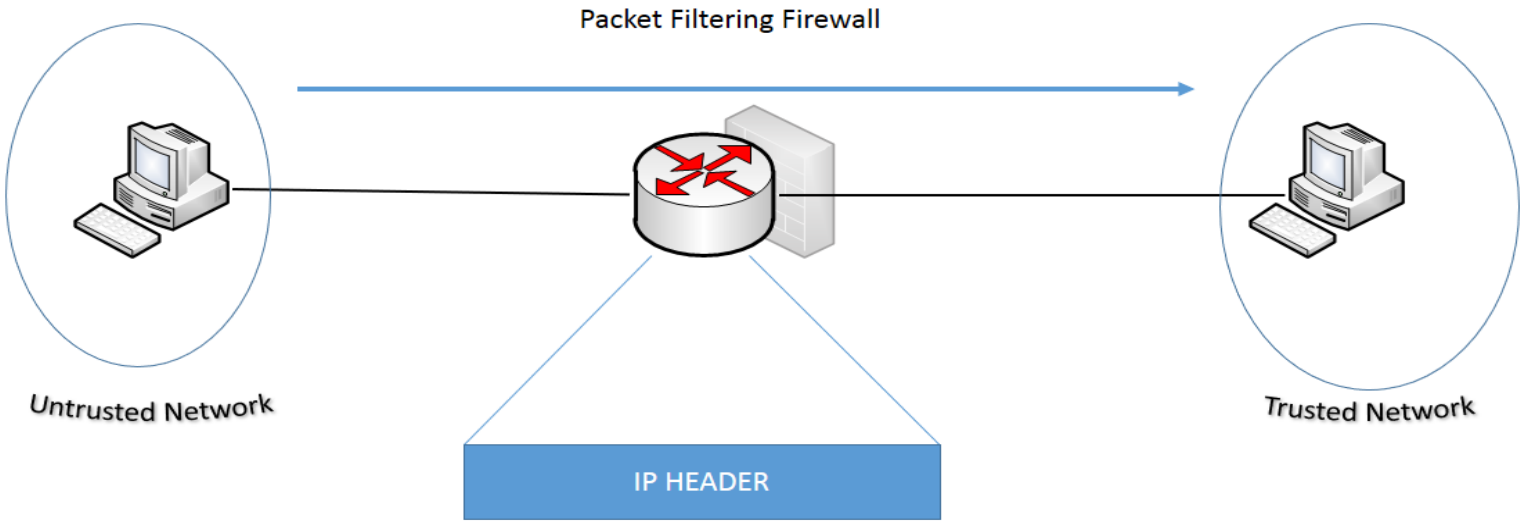
Types of Firewall

There are mainly five types Firewall-

A. Packet-Filtering Router
B. Circuit-Level Gateway
C. Stateful Inspection firewall
D. Application-Level gateway
E. Next-Generation firewall

Packet-Filtering Router

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet.
- Filter packets going in both direction.

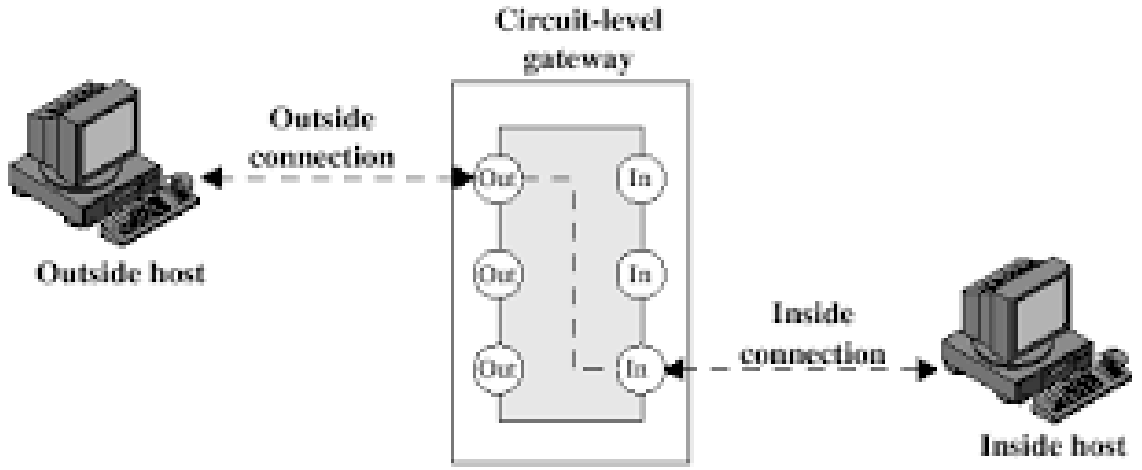


Packet-Filtering Router

- The packet-Filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
- Two default policies (Discard or Forward).

Circuit-Level Gateway

- Stand alone system.
- Specialized function perform by an Application-Level Gateway.

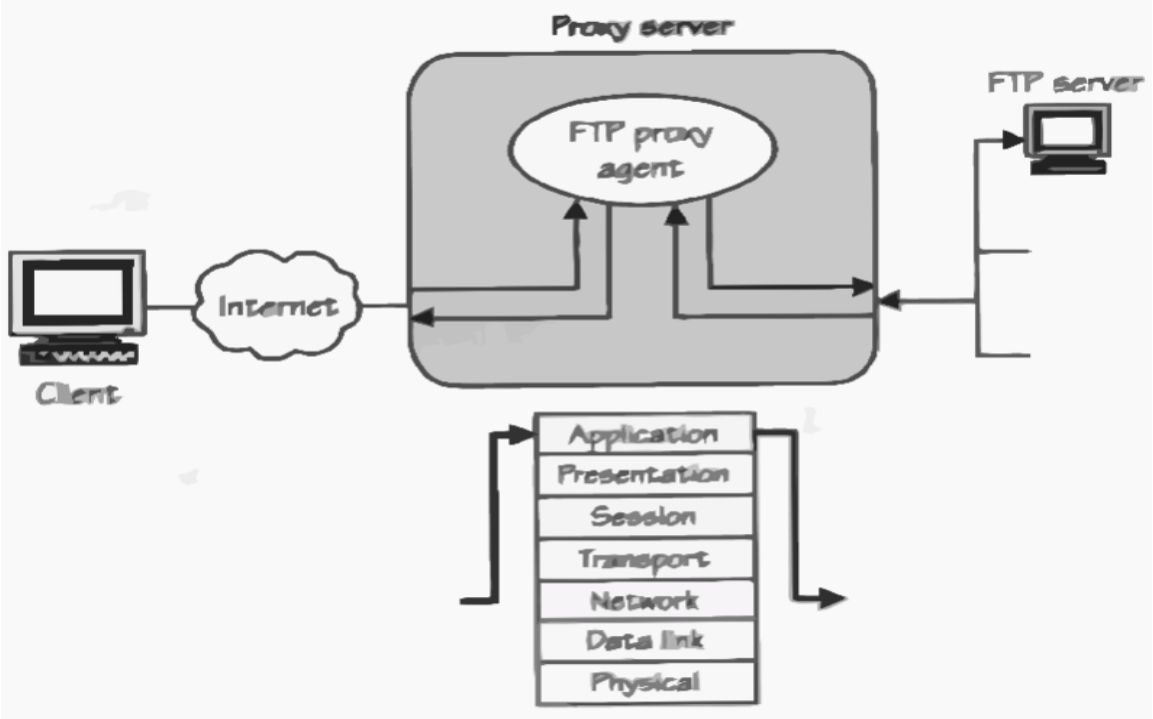


Circuit-Level Gateway

- Sets up two TCP connections.
- The gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connection will be allowed.

Stateful Inspection Firewall

- State-aware devices, on the other hand, not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session.

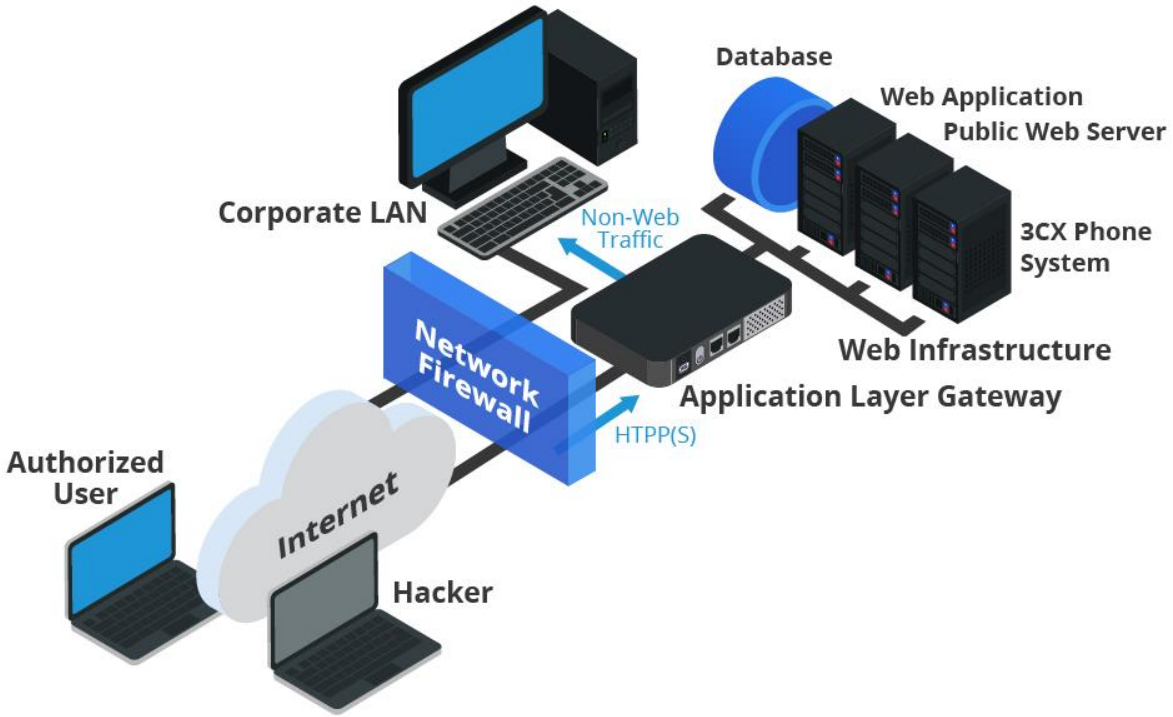


Stateful Inspection Firewall

- This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.
- A further variant of stateful inspection is the multilayer inspection firewall, which considers the flow of transactions in process across multiple protocol layers of the seven-layer open systems interconnection model.

Application-Level Gateway

- This kind of device technically a proxy and sometimes referred to as a proxy Firewall.

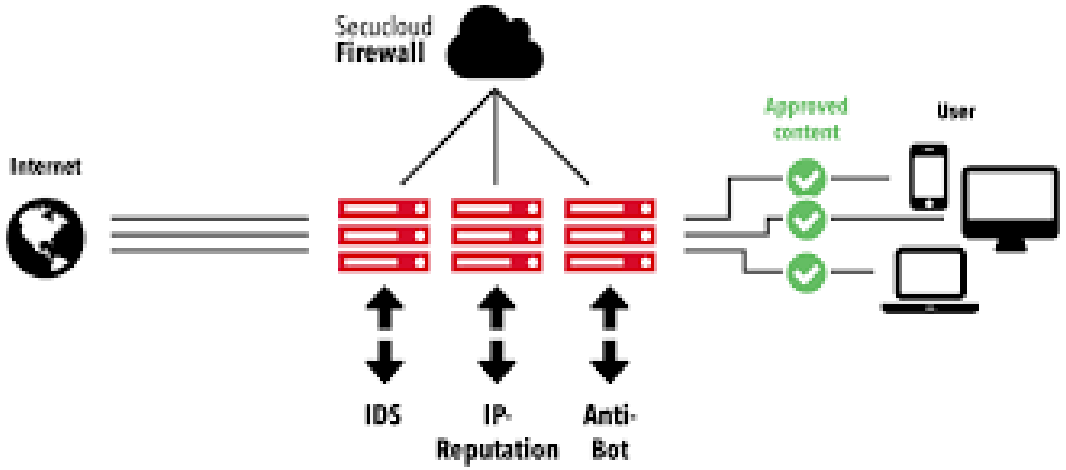


Application-Level Gateway

- It combines some of the attributes of packet filtering firewalls with those of circuit-level gateways. They filter packets not only according to the service for which they are intended as specified by the destination port but also by certain other characteristics, such as the HTTP request string.
- While gateways that filter at the application layer provide considerable data security, they can dramatically affect network performance.

Next-Generation Firewall

- A typical NGFW combines packet inspection with stateful inspection and also includes some variety of deep packet inspection, as well as other network security systems, such as intrusion detection/prevention, malware filtering and antivirus.



Next-Generation Firewall

- While packet inspection in traditional firewalls looks exclusively at the protocol header of the packet, deep packet inspection looks at the actual data the packet is carrying. A deep packet inspection firewall tracks the progress of a web browsing session and is capable of noticing whether a packet payload, when assembled with other packets in an HTTP server reply, constitutes a legitimate HTML formatted response.

Hardware Firewall vs. Software Firewall

- Hardware Firewall are integrated into the router that sits between a computer and the internet.

- Software Firewalls are installed on individual servers. They intercept each connection request and then determine whether the request is valid or not.

Role of Firewall

- A firewall is a term used for a ‘barrier’ between a network of machines and users that operate under a common security policy and generally trust each other, and the outside world.
- There are two basic reasons for using a firewall at present: to save money in concentrating your security on a small number of components, and to simplify the architecture of a system by restricting access only to machines that trust each other.

Advantages of Firewall

- Concentration of security all modified software and logging is located on the firewall system as oppose to being distributed on many hosts.
- Protocol filtering, where the firewall filters protocols and services that are either not necessary or that cannot be adequately secured from exploitation.

Advantages of Firewall

- Information hiding, in which a firewall can hide names of internal systems or electronic mail address, thereby revealing less information to outside hosts.
- Application gateways, where the firewall requires inside or outside users to connect first to the firewall before connecting further, thereby filtering the protocol.

Disadvantages of Firewall

- The most obvious being that certain types of network access may be hampered or even blocked telnet, ftp, X, Windows, NFS, NIS, etc.
- A second disadvantage with a firewall system is that it concentrates security in one spot as oppose to distributing it among systems, thus a compromise of the firewall could be disastrous to other less-protected systems on the subnet.

CONCLUSION

- One of the best thing about a firewall from a security standpoint is that it stops anyone on the outside from logging into a computer in your private network.
- While this is a big deal for business, most home networks will probably not be threatened in this manner. Still, putting a firewall in place provides some peace of mind.