Firewalls - Computer Networks

Published on Sunday, December 20, 2015

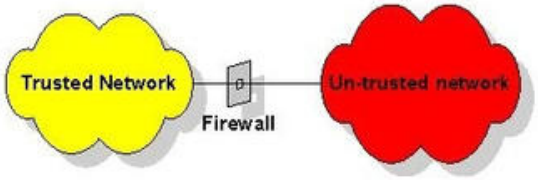
Aspirants,

Hope your preparations are going well for exams ahead. Today, we'll be learning Firewalls and all about them as a part of networks. Feel free to share your views/doubts/clarifications in comments section.

This article is a part of PK Series (IT)

What is a Firewall?

A firewall is a device designed to **control the flow of traffic** into and out-of a network. In general, firewalls are installed to prevent attacks. It disrupts free communication between a trusted and un-
trusted network in order to mange the information flow and restrict unwarranted dangerous access.
Hardware firewall is a physical device between internet and your computer while Software firewall is installed as a program on computer.

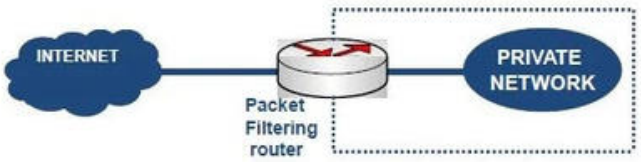


Types of Firewalls

Packet Filtering Firewall

It applies a set of rules to each incoming packet and then **forwards/discards** (two default policies) the packet. It filters packets going in **both directions**. The packet filter is typically set up as a list of rules based on matches to fields in IP or TCP header. Some of the attacks that can be made on packet filtering routers are: **IP address spoofing, Source Routing attacks, Tiny Fragment attacks.**

Advantages: Simplicity, transparency to users and high speed.
Disadvantages: Difficult to set up, lack of authentication.



Application Level Gateway Firewall

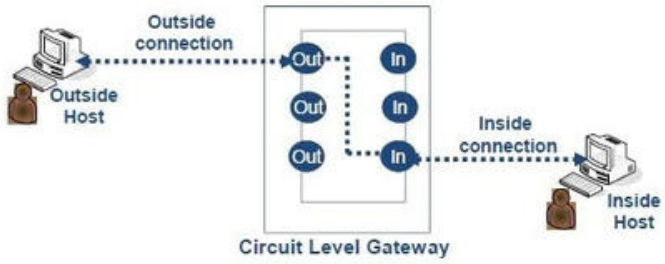
In this, when a client establishes connection with the destination service, it connects to an application gateway. It is also called a **proxy server**. The proxy then establishes the connection with destination behind the firewall and acts on behalf of client, making all packet forwarding decisions. It acts as a **relay of application level traffic**. Also, it needs **separate proxies for each service**- SMTP, DNS and other custom services.

Advantages: Higher security than packet filters, Easy to log and audit all incoming traffic.
Disadvantages: Requires great memory and processor resources.

Circuit Level Gateway Firewall

This firewall works at **session layer** of OSI model. Traffic is allowed only if a session request is legitimate. It sets up **two TCP connections.** The gateway typically relays TCP segments from one connection to other without examining the contents and security function determines whether to allow it further or not. A proxy server as explained above is a security barrier between internal and external computers while a circuit level gateway is a **virtual circuit between proxy server and internal hosts**.

Advantages: Hides private network data, doesn't need a separate proxy server for each application, simple to implement.
Disadvantages: Doesn't filter individual packets, attacker may take advantage after establishing a connection.



What is a Bastion Host?

It is a system identified by firewall administrator as a crucial point in network's security. It executes a **secure version** of OS and is trusted. It requires **additional authentication** before access is allowed. It is designed specifically to **withstand attacks** as it is on public side of the network. Firewalls and Routers can be considered as Bastion Hosts.