Firewall Technologies

Firewalls are used to protect computer networks from hostile intrusions. A hardware firewall separates trusted internal networks (e.g Internal corporate LAN) from external non-trusted networks (e.g Internet or untrusted WAN). The primary objective of the firewall is to examine all inbound and outbound traffic to see if it meets specific criteria (firewall policy rules). If the traffic complies with the firewall policy it is permitted, otherwise it is dropped.

Firewall operations are based on the following general firewall technologies:

- Packet Filtering
- Proxy Server Firewall

Stateful packet Firewall

Packet Filtering
A firewall can use packet filtering to limit information that enters a network and information moving from one segment of a network to another. Packet filtering uses access control lists (ACLs), which allow a firewall to accept or deny access based on packet types and other variables.

This method is effective when a protected netwoyrk receives a packet from an unprotected network. Any packet that is sent to the protected network and does not fit the criteria defined by the ACLs is dropped.

Problems with packet filtering are as follows:

- Arbitrary packets can be sent that fir the ACL criteria and therefore pass through the filter.
- Packets can pass through the filter by being fragmented.
- Complex ACLs are difficult to implement and maintain correctly.
- Some services can not be filtered.

Packet Filtering is usually used on **Cisco Routers** using Access Control Lists. This filtering technology is good as a first line of defence on border gateway routers.
Proxy Server Firewall
A proxy server is a firewall device that examines packets at higher layers of the OSI model. This device hides valuable data by requiring users to communicate with a secure system by means of a proxy. Users gain access to the network by going through a process that establishes session state, user authentication, and authorization policy. This means that users connect to outside services via application programs (proxies) that are running on the gateway that is connected to the outside unprotected zone.

Problems with the proxy server are as follows:

- The proxy server creates a single point of failure, which means that if the entrance to the network is compromised, then the entire network is compromised.
- Adding new services to the firewall is difficult.
- The proxy server performs more slowly under stress.

Stateful Packet Firewall
Stateful packet filtering firewall is the method that is used by the Cisco security appliances. This technlology maintains complete session state of the traffic passing through the firewall. Each time a TCP or UDP connection is established for inbound or outbound connections, the information is logged in a stateful session flow table.

The stateful session flow table, also known as the state table, contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP or UDP connection that is associated with the particular session. This information creates a connection object, and consequently, all inbound and outbound packets are compared against session flows in the stateful session flow table. Data is permitted through the firewall only if an appropriate connection exists to validate its passage.

This method is effective for three reasons.

- It works both on packets and on connections.
- It operates at a higher performance level than packet filtering or using a proxy server.
- It records data in a table for every connection and connectionless transaction. This table serves as a reference point for determining if packets belong to an existing connection or are from an unauthorized source.

Some examples of stateful firewalls are the Cisco PIX and ASA models.

Source from: http://www.cisco-tips.com/firewall-technologies/