FIREWALLS IN NETWORK SECURITY

- A firewall in an information security program is similar to a building‘s firewall in that it prevents specific types of information from moving between the outside world, known as the untrusted network(eg., the Internet), and the inside world, known as the trusted network.
- The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices.

Firewall Categorization Methods:

- Firewalls can be categorized by processing mode, development era, or structure.
- There are FIVE major processing –mode categories of firewalls: Packet filtering Firewalls, Application gateways, Circuit gateways, MAC layer firewalls and Hybrids.(Hybrid firewalls use a combination of other three methods, and in practice, most firewalls fall into this category)
- Firewalls categorized by which level of technology they employ are identified by generation, with the later generations being more complex and more recently developed.

- Firewalls categorized by intended structure are typically divided into categories

including residential-or commercial-grade, hardware-based, software-based, or appliance-based devices.

Firewalls categorized by processing mode:

The FIVE processing modes are:

1. Packet Filtering
2. Application Gateways
3. Circuit Gateways
4. MAC layer firewalls
5. Hybrids

I. Packet Filtering

Packet filtering firewall or simply filtering firewall examine the header information of data packets that come into a network. A packet filtering firewall installed on a TCP/IP based network typically functions at the Ip level and determines whether to drop a packet (Deny) or forward it to the next network connection (Allow) based on the rules programmed into the firewall. Packet filtering firewalls examine evry incoming packet header and can selectively filter packets based on header information such as destination address, source address, packet types, and other key information.

Fig.6-1 shows the structure of an IP packet.

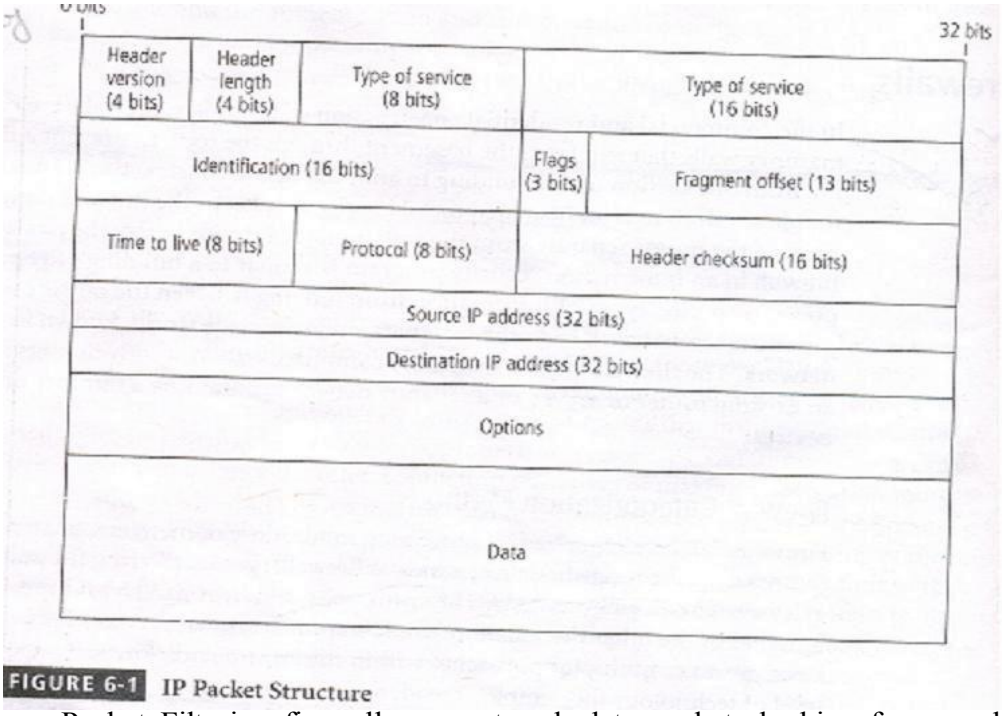

FIGURE 6-1 IP Packet Structure

Packet Filtering firewalls san network data packets looking for compliance with or vilation of the rules of the firewalls database.Filtering firewalls inspect packets at the network layer, or Layer 3 of the OSI model. If the device finds a packet that matches a restriction, it stops the packet from travelling from one network to another.

The restrictions most commonly implemented in packet filtering firewalls are based on a combination of the following:

1. IP source and destination address.
2. Direction (in bound or outbound)
3. Transmission Control Protocol (TCP) or User Datagram protocol(UDP) source and destination port requests.

A packets content will vary instructure , depending on the nature of the packet. The two primary service types are TCP and UDP .Fig 6-2 and 6-3 show the structure of these two major elements of the combined protocol known as TCP/IP Simple firewall models examine TWO aspects of the packet header: the

destination and source address. They enforce address restrictions, rules

designed to prohibit packets with certain address or partial addresses from passing through the device.They accomplish this through access control lists(ACLs), which are created and modified by the firewall administrators. Fig6-4 shows how a packet filtering router can be used as a simple firewall to filter data packets from inbound connections and allow outbound connections unrestricted access the public network.

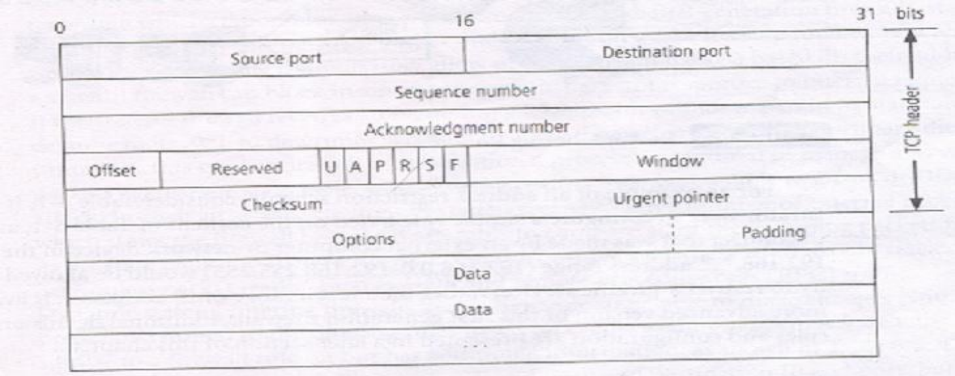

FIGURE 6-2 TCP Packet Structure

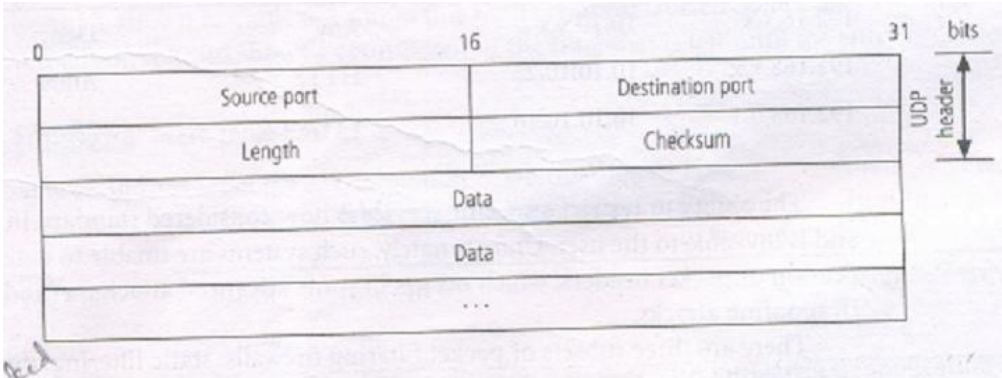

FIGURE 6-3 UDP Datagram Structure

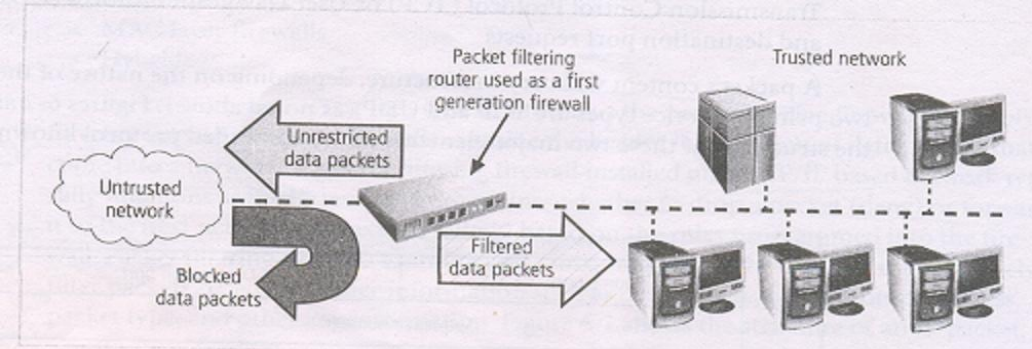

FIGURE 6-4 Packet Filtering Router

For an example of an address restriction scheme, consider Table 6-1.If an administrator were to configure a simple rule based on the content of the table, any attempt to connect that was made by an external computer or network device in the 192.168.*.* address range (192.168.0.0-192.168.255.255) would be aloowed. The ability to restrict a specific service , rather than just a range of IP address, is available in a more advanced version of this first generation firewall.

TABLE 6-1 Sample Firewall Rule and Format

Source Address	Destination Address	Service (HTTP, SMTP, FTP, Telnet)	Action (Allow or Deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

The ability to restrict a specific service is now considered standard in most routers and is invisible to the user. Unfortunately, such systems are unable to detect the modification of packet headers, which occurs in some advanced attack methods, including IP spoofing attacks.

There are THREE subsets of packet filtering firewalls: Static filtering, Dynamic Filtering, and stateful inspection

Static Filtering: Static filtering requires that the filtering rules governing how the firewall decides which packets are allowed and which are denied are developed and installed. This type of filtering is common in network routers and gateways.

Dynamic Filtering: Dynamic Filtering allows to react to an emergent event and update or create rules to deal with the event. This reaction could be positive , as in allowing an internal user to engage in a specific activity upon request, or negative as in dropping all packets from a particular address when an increase in the presence of a particular type of malformed packet is detected.

While static filtering firewalls allow entire sets of one type of packet to enter in response to authorized requests, the dynamic packet filtering firewall allows only a particular packet with a particular source, destination, and port address to enter through the firewall. It does this by opening and closing doors in the firewall based on the information contained in the packet header, which makes dynamic packet filters an intermediate form, between traditional static packet filters and application proxies.

Stateful Inspection: Stateful Inspection firewalls , also called stateful firewalls, keep track of each network connection between internal and external systems using a state table.
A state table tracks the state and context of each packet in the conversation by recording which station sent what packet and when.Staeful inspection firewalls perform packet filtering like they can block incoming packets that are not responses to internal requests.
If the stateful firewall receives an incoming packet that it cannot match in its state table ,it defaults to its ACL to determine whether to allow the packet to pass.

The primary disadvantage of this type of firewall is the additional processing required to manage and verify packets against the state table , which can leave the system vulnerable to a Dos or DDoS attack.In such an attack , the firewall system receives a large number

of external packets, which slows the firewall because it attempts to compare all of the incoming packets first to the state table and then to the ACL.

On the positive side, these firewalls can track connectionless packet traffic, such as UDP and remote procedure calls (RPC) traffic.

Dynamic stateful filtering firewalls keep a dynamic state table to make changes within predefined limits tot eh filtering rules based on events as they happen.A state table looks similar to a firewall rule set but has additional information, as shown in table 6-2.
The state table contains the familiar source IP and port , and destination IP and port , but ads information on the protocol used (UDP or TCP), total time in seconds, and time remaining in seconds.Many state table implementations allow a connection to remain in place for up to 60 minutes without any activity before the state is deleted.

The example shown in Table 6-2 shows this in column labeled Total Time.The time remaining column shows a countdown of the time that is left until the entry is deleted.

TABLE 6-2 State Table Entries

Source Address	Source Port	Destination Address	Destination Port	Time Remaining in Seconds	Total Time in Seconds	Protocol
192.168.2.5	1028	10.10.10.7	80	2725	3600	TCP

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf