Unit 1: Firewall And Packet Filters

1

Unit Structure

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Understand various types of firewalls
- Understand packet filtering
- Understand intrusion detection system

1.2 FIREWALL

Every small and big enterprise comprises the network of machines. They tend to communicate, sharing information, sharing resources, data in and out of the network. They are also connected to the internet. But once the machines are connected to the internet it opens all the ways for the outsiders or better to say hackers which has the malicious intent and start attacking the machines.

This is the point where the concept of a firewall comes into the picture. In simple terms, a firewall can be explained as a wall built to protect from the fire and slow down its spread. In networks also it has a similar concept and understanding. A firewall intended to stop unauthorized users from accessing the network. The most common place to deploy the firewall is between the trusted and untrusted network of organization which typically is the internet.

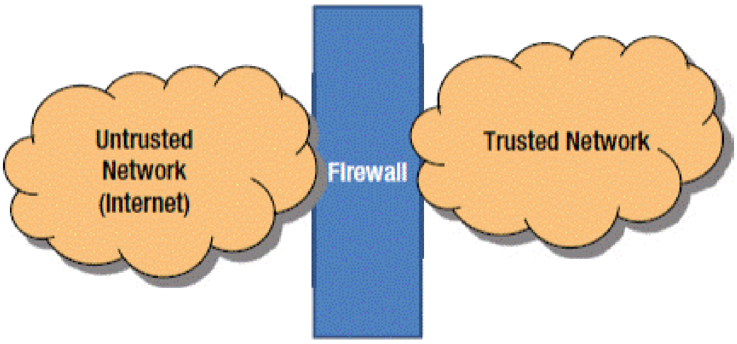


Figure 1.1 Firewall Deployments

The term firewall has different meanings which are based on the implementation and purpose. That will be the place where the security policies are implemented. The firewall's external network interface card is the gateway to the internet. The purpose is simple; to protect what is there on your side of the gateway.

According to RFC 2647l, a firewall is a device, operating system, or application program that enforces an access control policy between networks.

A firewall acts as a gatekeeper between your local area network and the internet. All traffic from in and out of the LAN must pass through the firewall. There needs to be some type of firewall installed in your network even if you are a home user having a broadband connection or high-speed connection.

Firewall setup can be done in different ways based on implementation and usage. You can purchase a hardware firewall which is basically a router with inbuilt firewall features. Also, most of the hardware appliances come with the web-based interface which will provide an easy interface to connect with firewall and setting can be easily configured. The purpose here to configure the firewall will enforce the policy which is defined during the configuration which will allow or deny the internet traffic based on that rules and policies configured. Security policies are all about the access control and authenticated use of private or protected use of the application, file services and programs.

Another way is to install a server computer and use it as the firewall. In large networks, it is sometimes hard to figure out where to place the firewall or perimeter. Perimeter is used to describe the location of the firewall inside the large networks(WAN). Let us discuss different types of firewall techniques.

1.2.1 TYPES OF FIREWALL

Packet Filtering: Packet filter firewall examines each packet that crosses the firewall and checks the packet according to the set of rules which are defined. If all rules are satisfied with the packet that it is allowed and if not then the packet is rejected.

It is the very least expensive type of firewall. Packet filters work by inspecting the source IP address, destination IP address, a port number assigned to each service.

The decision can be based on factors other than IP header fields such as ICMP message type, TCP SYN, and ACK bits, etc.

Packet filtering rule has two parts:

- **Selection criteria** − It is used as a condition and pattern matching for decision making.

- **Action field** − this part specifies an action to be taken if an IP packet meets the selection criteria. The action could be either block (deny) or permit (allow) the packet across the firewall.

Packet filtering is generally accomplished by configuring Access Control Lists (ACL) on routers or switches. ACL is a table of packet filter rules. As traffic enters or exits an interface, firewall applies ACLs from top to bottom to each incoming packet, finds matching criteria and either permit or denies the individual packets. As it is the most common firewall technique it has its own weakness.

One of the biggest weaknesses of packet filtering is that it trusts that the packets themselves are telling the truth when they say who they're from and who they're going to. Hackers exploit this weakness by using a hacking technique called IP spoofing, in which they insert fake IP addresses in packets and they send to your network.

Another weakness of packet filtering is that it examines each without considering what packets have gone through the firewall before and what packets may follow. In other words, packet filtering is stateless. In spite of these weaknesses, packet filter firewalls have several advantages also.

Packet filters are very efficient. They hold up each inbound and outbound packet for only a few milliseconds while they look inside the packet to determine the destination and source ports and addresses. After these addresses and ports have been determined, the packet filter quickly applies its rules and either sends the packet along or rejects it.

Packet filters are inexpensive. Most routers include built-in packet filtering.

Stateful Packet Inspection: Stateful firewalls can watch traffic streams from end to end. They are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption. In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, synchronization acknowledges or established). It can tell if the MTU has changed and whether packets have fragmented. etc. Stateful firewalls are better at identifying unauthorized and forged communications.

Circuit Level Gateway: A circuit-level gateway manages connections between clients and servers based on TCP/IP addresses and port numbers. After the connection is established, the gateway doesn’t interfere with packets flowing between the systems.

SOCKS(RFC 1928) refers to a circuit-level gateway. It is a networking proxy mechanism that enables hosts on one side of a SOCKS server to gain full access to hosts on the other side without requiring direct IP reachability. The client connects to the SOCKS server at the firewall. Then the client enters a negotiation for the authentication method to be used and authenticates with the chosen method.

The client sends a connection relay request to the SOCKS server, containing the desired destination IP address and transport port. The server accepts the request after checking that the client meets the basic filtering criteria. Then, on behalf of the client, the gateway opens a connection to the requested untrusted host and then closely monitors the TCP handshaking that follows.

The SOCKS server informs the client, and in case of success, starts relaying the data between the two connections. Circuit level gateways are used when the organization trusts the internal users and does not want to inspect the contents or application data sent on the Internet.

Application Level Gateway:

Application level gateway firewall systems are more advanced in terms of its features and working in compare to packet filtering or stateful packet inspection or circuit level gateway. It treats all the packets as equal level or equal priority. Application gateway firewall system knows the details that which application has generated these packets.

In addition to that application level gateway is also worked as proxy servers. A proxy server is a server that sits between the client machine and server machine. The proxy server will intercept the packet and will identify that the packets that are intended for the server machine or not and then it process them.

For eg: web proxies are often stores the copies of the commonly used web pages in their local cache memory. When a user requests to access such pages which are present in the local cache memory that proxies itself reply to the user request, which in turns is very effective for the faster response. If it does not have the copy of the webpage it passes the request to the server machine.

Application level gateway is aware of the details, how a server machine handles TCP/IP requests and sequence of packets. So they can easily identify if the incoming packet is legitimate or fake or is part of an attack.

Application level gateway is more costly in terms of the price and cost of configuration and maintaining them. Application level gateway can slow down the network as it checks every packet in the deep which takes more time to process the packet before allowing them in or out of the network.

Firewall with Demilitarized Zone(DMZ): The term DMZ originally arrives from the military where an area between two territories, military operations are prohibited.Similar way, many organizations are facing is how to enable or allow to access to legitimate services of their organization to public services. While considering that not to compromise any other services of the organization. To achieve this the typical approach is to use a firewall to achieve the DMZ.

It will help to maintain and improve the security of the organization, by segregating the devices and machines on the opposite sides of the firewall. DMZ will act as a small and isolated network established between that internet and private network.

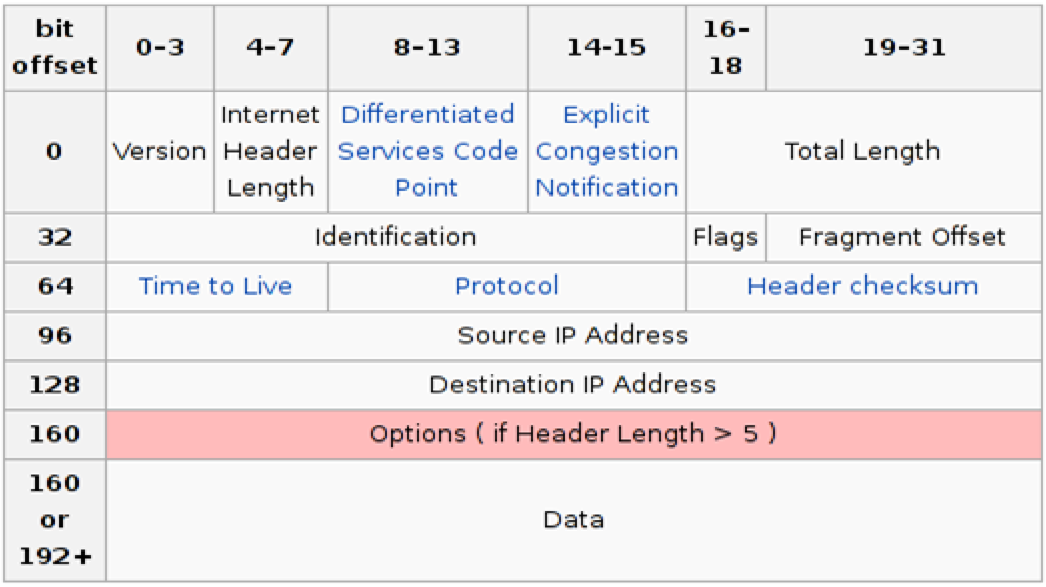
Some of the important functions of the DMZ are:

- All the traffic that goes in and out is inspected.
- Resources inside the DMZ are under continuous security monitoring to save them from being compromised from external cyber attack.
- It acts as a protective boundary for the private network.

1.3 PACKET FILTERING

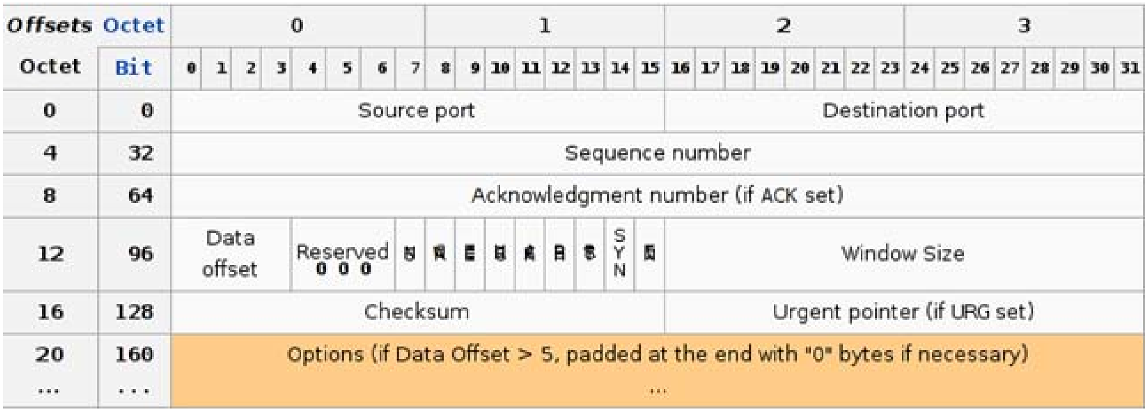
Packet filtering is a process of allowing or blocking packets at one of the OSI layers which are usually a network layer, which also contains an IP header. IP header is used for routing packets through the internet as it contains all the important information of all protocols, IP address such as Source IP address and port, destination IP address and port as IP V4 is of 32 bit we have the similar IP V6 which is of 128 bit and contains similar information.

There is another protocol apart from the IP which is TCP protocol.



bit offset	0-3	4-7	8-13	14-15	16-18	19-31
0	Version	Internet Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total Length	
32	Identification				Flags	Fragment Offset
64	Time to Live		Protocol		Header checksum	
96	Source IP Address					
128	Destination IP Address					
160	Options (if Header Length > 5)					
160 or 192+	Data					

Figure 1.2 IP Header Source: Wikipedia



Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0			[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	S Y N	[illegible]	Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20 ...	160 ...	Options (if Data Offset > 5, padded at the end with "0" bytes if necessary) ...																															

Figure 1.3 TCP Header Source: Wikipedia

Important pieces of the TCP protocol header are the following fields:

- Source port: from which port the packet was sent.
- Destination port: to which port the packet is going.
- Flags: URG, ACK, PSH, RST, SYN, FIN

Packet filtering looks at the source IP address, destination IP address, source port number, destination port number, flags and other information to decide whether some packet should be accepted or rejected.

Usually, packet filtering is also smart enough to remember previous packets that are all analyzed together to decide if a packet is considered malicious and is rejected/dropped, or if it should be passed through.

Check Your Progress 1

1. Which type of firewall technique stores the local copy of the data accessed by user?

2. Which is an expensive and time consuming firewall technique?

3. Which are 3 important piece of information which is useful in packet filtering?

Capabilities of Packet Filter: A packet filter has to have the following capabilities:

- Examination of each packet data and headers.

  Each packet is examined when it comes to the packet filter. This is done with the help of filtering rules defined in the next point.

- Set of rules which define what to do with the packet.

  These rules define what a packet filter should look for when it receives a packet. It usually looks for the information we’ve already talked about, like source IP address, destination IP address, source port number, destination port number, etc.

- What actions are taken based on the result of the examination.

  There are numerous actions which can be used when a packet filter receives a packet and has filtering rules defined. Based on defined filtering rules, a packet filter can do the following:

- Accept only packets that are certainly safe based on a set of rules. Drop all other packets.

- Drop only packets that are certainly unsafe based on a set of rules. Accept all other packets.

- If a packet is received for which there is no filtering rule defined, ask a user what to do with it.

- Block a user coming from a defined source IP address because too many packets were received in too short of a time window.

- Almost any action can be applied against a packet or a set of packets. If we want to send an HTTP response, which includes “Hello, How Are You?” to every HTTP request coming from IP xxx.xxx.xxx.xxx, we could define a rule that could do that.
- Packet filter also identifies whether the packets are broken or not received properly.

Limitations:

Packet filter does not read the content of the packet or it cannot check the payload of the network packet; which implies that it cannot stop the application layer attack.

Packet Filtering Categories: An overview of packet filtering categories are shown in the below image.

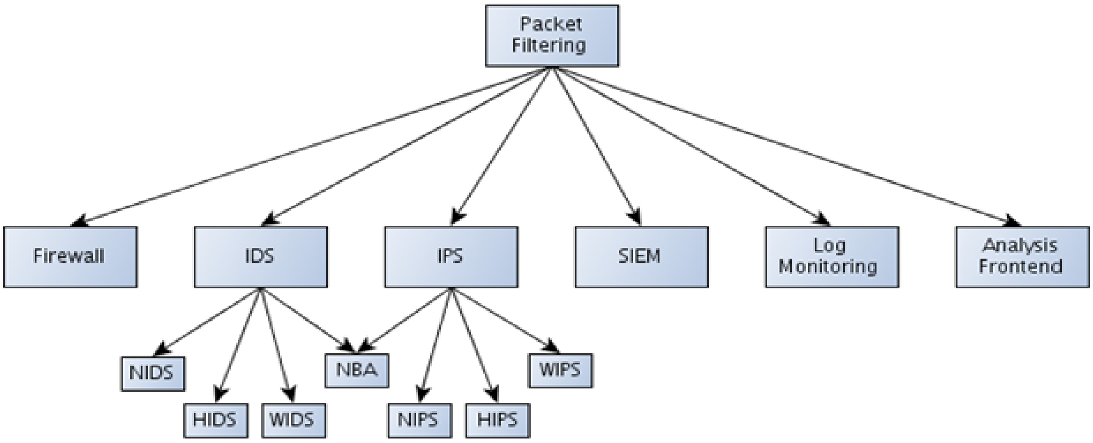


Figure 1.4 Categories of Packet Filters Source: resources.infosecinstitute.com

As we have already seen the detail introduction of Firewall we will see details regarding other components. But before that, it is better to understand that other components are not a replacement of the firewall but can be used along with the firewall for better security measures.

1.4 INTRUSION DETECTION SYSTEM (IDS)

An intrusion detection system can be software-based or hardware-based and is used to monitor network packets or system for malicious activity and perform a specific action if such activity is detected. Usually, if malicious activity is detected on the network, the source IP of the malicious traffic is blocked for a certain period of time, and all of the packets from that IP address will be rejected.

There are several types of intrusion detection systems:

- **Network intrusion detection system (NIDS)**

  NIDS detects malicious activity by monitoring and examining network traffic. This type of IDS usually runs when packets enter a specific network on a special hardware component whose only job is to monitor and accept/reject packets from the Internet and let them into the local network. Example: Snort.

- **A host-based intrusion detection system (HIDS)**

  HIDS detects malicious activity by monitoring and examining system calls, application logs, access control lists, etc. HIDS usually contains a software agent that needs to be installed on the operating system. Examples: Tripwire, OSSEC. A wireless intrusion detection system (WIDS)

  WIDS monitors the wireless network for malicious behavior, which can be the number of packets sent in a time window, too many deauthentication packets, too many broadcast requests, etc. WIDS usually run on an AP (Access Point) and doesn't allow certain users to connect to it if malicious activity is detected.

- Network behavior analysis (NDA)

  NDA monitors network traffic passively to detect unknown and unusual patterns that might be a threat. It should be used together with the firewall as well as other types of IDS systems.

Check Your Progress 2

1. Mention the limitation of packet filtering.

2. Where the firewall is placed inside the network?

3. Where do we generally use the ACL(Access Control List) ?

1.5 INTRUSION PREVENTION SYSTEM (IPS)

The intrusion prevention system is basically an upgrade of the intrusion detection system. Where the IDS is used to detect and log the attack, the IPS is used to detect, block and log the attack. The IPS systems are able to prevent certain attacks while they are happening.

There are multiple versions of the IPS systems, but we won't describe them in detail, since they are the same as with IDS systems, with the exception that all of the types of IPS system also prevent the attack from continuing. The types of IPS systems are NIPS, HIPS, WIPS.

1.6 SECURITY INFORMATION AND EVENT MANAGEMENT

With SIEM we can monitor security alerts generated by various software or hardware solutions that are used for detecting malicious activity. SIEM consists of:

- SIM (Security Information Management): provides the analysis and reporting of the logged data.
- SEM (Security Event Management): provides monitoring and correlation of events.

A SIEM gathers information or data at a single point and provides a human-readable security report about the malicious behavior that is happening in our network. A SIEM solution must work in real time, so we can secure our network in a timely fashion.

What would happen if we received a report about a security breach that is a month old, it wouldn't help us a lot since the attacker is probably long gone with all the data that he needed.

SIEM capabilities are as following:

- Data Aggregation: provides means to join data together from many sources: network, servers, databases, applications.
- Correlation: correlates data into meaningful sets to learn something new from it.
- Alerting: analysis of correlated events and alerting the recipients of detected security issues.
- Dashboards: provides means to present data in meaningful charts.
- Compliance: automatically gather all the needed data and produce reports.
- Retention: provides long-term storage of historical data for later analysis.

SIEM also implements log monitoring and analysis frontend, but we've nevertheless pointed them out as independent points in the above picture because other tools can be available just for that. We can also write our own script that would take the logs and report some malicious activity.

Log Monitoring and Analysis Frontend: It is an important part of the overall picture since this is the tool we use to look at the malicious activity that happened on our network. There are quite a few frontends available such as OSSIM, Sguil.

1.7 LET US SUM UP

In this chapter we have seen concepts of the firewall and packet filters. Also What all different types of firewall technique is there and how it is used in the organization.

1.8 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check your progress 1

1. Web Proxy

2. Application Level Gateway

3. Source & Destination IP and Flags

Check your progress 2

1. Limitation of packet filtering are itcannot read the content of the packet and make a decision, complex configuration.

2. Between trusted and untrusted network

3. ACL is generally used in routers