Chapter 4 – Firewalls and Proxy servers

The word 'firewall' has come from a kind of arrangement in automobiles, to prevent the passengers from engine components. The firewalls in computers also work with similar concept. It is defined as *'the collection of components that are placed between the local (unprotected) private network / workstation and the Internet (unprotected) which is the external public network'*.

Firewalls come in various categories, configurations, set of devices and products which run on the hosts in the network. They work like logical security guards which keep an eye on the outgoing and incoming traffic. The various types of firewalls are as discussed under.

4.1 Kinds of Firewalls:

In general, the firewalls have been classified as per the work carried out by them. They have two basic types (1) *Packet Filtering* and (2) *Application Level*. Two more types have also resulted based on these two primary types. They are (3) *Circuit level gateways* and (4) *Stateful Multi-layer inspection* (*Dynamic*). Each type is discussed below in detail.

4.2 Packet Filters:

This is the basic level of the firewalls. As the name suggests, this firewall checks for each and every IP packet individually, either coming in or going out of private network. According to the selected policies (called Rulesets or Access Control Lists or ACLs) it determines whether to accept a packet or reject it. This is the first line of defense against the intruders, and is not totally foolproof. It has to be combined with other techniques as well, to strengthen the security.

Packet filtering can also be incorporated in Routers. Many routers have this capability in which the Rulesets can be hardcoaded into them. Thus, apart from normal routing decisions, a router can also be made capable of performing packet filtering. Another implementation of packet filters is kernel based in which the kernel is configured to carry out packet filtering. In case of Linux operating system, command line tools such as ipchains (now replaced with iptables) can also be used to define, modify or apply the specific Rulesets for packet filters.

Packet filtering is simple and straightforward mechanism. This works at the *Internet Layer* in the TCP/IP model. Usually, a packet is checked for the following information for filtering: 1. Source IP address, 2. Destination IP address, 3.Source TCP/UDP port, 4. Destination TCP/UDP port. Hence using these, a security decision may suggest blocking certain address or a website, which are not trustworthy.

<u>Advantages of packet filters:</u>

1. Simple and straightforward mechanism.
2. Operation is totally transparent to the users.
3. Faster in operation.

Disadvantages of packet filters:

1. Rule-sets to be defined for a packet filter may be very complex to specify as well as to test.
2. In order to allow certain access, some exceptions to the rules need to be added. This may add further to the complexity.
3. Some packet filters do not filter on the source TCP/UDP ports at all, which may increase the flaws in the filtering system.
4. These do not possess any auditing capabilities and auditing is considered to be of major importance in security.
5. All the applications on Internet may not be fully supported by packet filtering firewalls.
6. These type of firewalls do not attempt to *hide* the private network topology to the outside network and hence it gets exposed.
7. Using packet filters may be complex as graphical interface is not available in most of the cases.

4.3 Application level filtering:

The Application level firewalls work at the *topmost* layer in the network i.e. the Application Layer. Hence, they can monitor the flow of information in great details. They do not need to check each and every packet but rather check an application as a whole and determine whether it should be allowed the access of a network both in-bound as well as out-bound. Hence, they are more secure than the packet filters. These are also called Application level gateways as they are between the local network and the Internet. They require the policies to be set up by using specific softwares and hence *are NOT transparent to the end users.*

Another variation in them is called a *Proxy server*. These are the hosts which make/receive the requests to/from the Internet to the local network which they do *on behalf of* the local clients. These provide a single point of entry for Internet traffic into the local network. The Proxy servers work with two *faces* - one towards the local network (with an internal IP address) and another towards the Internet (using an external IP address), which is similar to the coin with two sides. Local network clients refer to it using its local IP address whereas anyone from the Internet uses its external IP address for communication. The services which are *proxied* include FTP, DNS, TELNET, HTTP, SMTP and so on. Thus, the application gateway allows the clients to *think* or believe that they are getting the direct connection to the Internet, in fact it is routed always through the proxy server.

Examples of Application level firewalls include Zone Lab's Zone Alarm, and Zone Alarm-Pro, IBM firewall, McaFee Firewall, Norton Firewall, Linux based Mitel Networks SME server, Squid proxy server, Wingate, Winproxy and many more with various facilities and configurations.

Advantages of Application level firewalls

1. Checks traffic in greater details than the packet filters.
2. No need to check each and every packet, but checks application as a whole.
3. Provides more security than the packet filters.
4. These are available as softwares with Graphical interface, hence specifying, changing the Rulesets is easier in this case.
5. Ability to hide the structure, topology and other sensitive information of the private

network from the external parties.

6. Has capability of complete auditing/logging of events which is an important aspect of security.
7. Easier to install, setup and operate from the point of users (also called as personal firewalls sometimes)

Disadvantages of Application level firewalls

1. Operation may be slower since it has to check the traffic in more detail.
2. The software products used may be costly to procure.
3. In some cases, setup may be difficult and require administrative help.
4. They are not transparent to the end users, and may have to be set up specifically on the client nodes.

4.4 Circuit level Gateways:

Another variation of firewalls are called the Circuit Level Gateways. These are set to run on the Transport level of TCP/IP model (or Session layer in case of the OSI model). These check for the specific sessions or services for filtering. They neither check individual packets nor the entire applications for filtering purpose. They are sometimes called as the *Relays* which relay the sessions / services (also called circuits) for the users. Normally they relay the services such as Telnet or FTP for the users. But in the process, they tend to break the standard client-server model.

Thus, for every request/response, there will be two connections to be set-up: one from the client machine to the firewall, and the second between the firewall to the external server, and similarly in reverse way. But they provide the facility to control these services. It is hence possible to enable/disable these services through the circuit gateways. A good example of this type of firewalls is the SOCKS server.

Advantages of Circuit level gateways:

1. More secure than packet filters since work on higher level.
2. Do not check individual packets inbound or outbound.
3. Can hide internal network structure to the external entities.
4. Flexibility to enable or disable sessions or services is available.
5. Less expensive compared to the Application level products.
6. Operation is transparent to the end-users

Disadvantages of Circuit level gateways:

1. Less secure compared to application level gateways.
2. Breaks the client-server model.
3. Requires two dedicated connections to be set up for each service / response.

4.5 Dynamic (Stateful Multi-layer Inspection) Firewalls:

The last category of firewalls is the Dynamic also known as the Stateful, multi-layer inspection type. As the name suggests it checks the traffic in multiple layers viz. Application, Transport as well as Internet layer. Hence, it combines all the advantages of the first three categories of firewalls. These are the recent type of firewalls being used. They check the individual packets at the Internet layer, checks for valid sessions at the Transport layer and evaluates the application at the topmost layer.

Another difference between this type and earlier ones is the awareness of a *State* and the *Dynamic* nature of them. This means, the firewall can *modify itself* or can *adopt to changes in situations* and can change the rules dynamically. This facility is not available in any of the earlier types which makes this a more efficient type of firewall and hence they are known to be *Stateless*. For this purpose the firewall needs to maintain some historical information about all the transactions in a form called *state tables.* These state tables are updated as and when new events are generated. These are used by the firewall to *modify* or *update* the Rulesets in different situations.

Examples of this type of firewall include Checkpoint's Firewall-1, Sun's SunScreen etc.

Advantages of Dynamic Firewalls

1. Scans the traffic in three different layers in great details
2. Provides much more security than in first three types of firewalls
3. Facility to adopt to the changes in the stage of network.
4. More flexible in its operation due to its dynamic nature.
5. Combines most of the advantages of first three types of firewalls.

Disadvantages of Dynamic Firewalls:

1. Operation much slower, may reduce the overall performance.
2. Applications need to be procured, specially and can be expensive.
3. Setup or implementation may be more difficult.

4.4 Distributed Firewalls

The Distributed firewalls are the host-resident security solutions which protect the enterprise network's critical end points against the intrusion. As the name suggests, the firewall implementation is distributed over multiple points rather than providing a single-point-entry into your network in case of traditional firewalls. With distributed firewalls, one can provide separate *level* of security to the Web, Mail servers, Application servers or individual nodes in the setup.

These are meant to provide higher security to the corporate networks. These can also prevent the malicious *inside attacks* also within the network, as they treat all traffic as *unfriendly* whether it is originating from the Internet or your Local network. This is more important advantage, since most of the attacks are initiated from inside the network. These firewalls also guard the individual machines the same way as the perimeter firewall guards the entire network.

These are like the personal firewalls but the additional features include the centralized management, logging and a fine access-control granularity. These are the prime features considered for implementation of firewalls in larger enterprises. These protect remote employees, precious servers of the enterprise, internal network as well as the individual terminals. Presently, organizations of various types that are security conscious are deploying the Distributed type of firewalls and has a scope of unlimited scalability even keeping the same performance. In some cases, even the perimeter firewalls need not be installed at all when distributed firewalls are deployed.

Some key differences between the Traditional Firewall implementations and the Distributed Firewall Implementations are as stated below.

Traditional Firewalls	Distributed Firewalls
Provide single entry point into the network	Provide multiple check points
More prone to attacks	Less prone (is in multiple forms).
Cannot prevent inside attacks	Possible to prevent inside attacks
Less secure implementation	More secure implementation
Servers have to be inside perimeter	Servers can be outside perimeter
Has less flexibility of operation	More flexibility in operation
Provides same level of security	Different security levels possible

4.4 What Firewalls cannot do ?

As seen normally, firewalls provide good amount of security to the private network. But there are certain aspects not covered or protected by any general form of a firewall. These are named as the things the firewalls cannot do. They include following:

1. Firewalls in general, cannot prevent from Internal attacks at all.
2. Does not prevent viruses from entering into the local network.
3. Do not differentiate between users on a single side i.e. either the Internet side or the Local side. This means one Internet user can spoof another or one local user can spoof other. They only try to differentiate between local and the External members.
4. Do not protect any connection that is not going through them or in some way *bypassing* them.
5. Can be bypassed by users in order to avail of the services normally blocked in which case they fail to provide any security to these connections. e.g. using modems or RAS to connect to Internet directly.
6. Cannot prevent from any new kind of threats or attacks for which the firewalls may not have been configured.
7. Fail to provide enough security, if not properly configured or not updated continuously.

4.5 Filtering Services:

Various services are provided through the Internet to the users. It is possible to present various kinds of attacks through these services and hence filtering of the services is essential. This is possible using the firewalls or proxy server products. On one side, they should provide the services to the users, but on the other they should also prevent intruders to take undue advantage of available or open services. Thus the internal users should be secured by filtering various services.

Reasonable services to filter:

1. Filtering Telnet: This services gives the feel of a 'virtual terminal' to the users so that they can use the remote terminal as if it is their own. This is very dangerous services

to be left open to 'public' as it is vulnerable. In order to filter Telnet, it can either be turned off totally (refraining anyone to remotely log in to your host), or can be turned on only for administrators choosing very good, secure password. In most of the products, it is not advised to leave Telnet open to public and should be turned off. This may prevent malicious intruders away to some extent.

2. Filtering Mail services: The E-mail is probably the most widely used service of the Internet. The protocols used for this viz. POP(Version 3), SMTP or IMAP can be filtered or specific rules can be added through the firewall software for filtering them. Examples of Email filtering include 1. Not allowing any mail if it has no. of recipients more than some fixed number (may be a spam), 2. Not allowing some specific extensions as attachment, 3. Not accepting mail if sender's ID is not included in the list and so forth. Using these kind of filtering, the E-mail services can be protected.
3. Filtering World Wide Web services: When users want to browse the world wide web, many malicious intrusions can occur without their knowledge. Users may not be aware about these situations. While filtering www services (the HTTP protocol especially), ruleset conditions can be added such that, the traffic from untrusted or undesired web sites can be blocked. Using packet filters or even application level filters, the conditions can be added to prevent particular sites, addresses or hosts which are not trustworthy.
4. Filtering FTP services: Yet another service offered is in the form of File transfers. Users can directly upload or download contents from the specific location reserved for it, using the File Transfer Protocol. While certain organizations prevent these services to public at all, some allow it only with some privileges. In rare cases, anonymous users can be entertained for the FTP services. While filtering FTP, the secure passwords will have to be chosen in order to prevent possible intrusions due to various types of attempts to the FTP servers. Also, the FTP servers can be placed in DMZ (De Meliterized Zones) to make isolated or can be kept separately available which are not providing any other services.

Default Allow / Default Deny on proxies:

As far as allowing or disallowing the services, there are mainly two approaches or methods. First is the *Allow All* approach and the second one is the *Deny All* approach. The first one is more open while later one is more conservative. In Default Allow approach, first by default everything is 'open'. Later on, the rules can be added for whatever you wish to block to the users. In the second approach, by default or in beginning everything is 'blocked' and as and when required rules can be added to open up the services/information that is required or is thought as trustworthy.

On the application level gateways orproxy servers, especially linux based, there exists the configuration files called hosts.allow and hosts.deny using which specific configurations can be made. The addresses added in hosts.allow file will be necessarily allowed and similarly the addresses in the hosts.deny file will be prevented.