3.2 Firewall Types

Packet filtering firewalls are the simplest and often the least expensive type of firewalls. Several other types of firewalls offer their own distinct advantages and disadvantages. The basic types of firewalls are:

- Packet filtering
- Application gateway
- Circuit level gateway
- Stateful packet inspection

3.2.1 Packet Filtering Firewall

The packet filtering firewall is the most basic type of firewall. In a packet filtering firewall, each incoming packet is examined. Only those packets that match the criteria you set are allowed through. Many operating systems, such as Windows clients (such as Windows 8 and 10) and many Linux distributions, include basic packet filtering software with the operating system.

Packet filtering firewalls are also referred to as screening firewalls. They can filter packets based on packet size, protocol used, source IP address, and many other parameters. Some routers offer this type of firewall protection in addition to their normal routing functions.

Packet filtering firewalls work by examining a packet’s source address, destination address, source port, destination port, and protocol type. Based on these factors and the rules that the firewall has been configured to use, they either allow or deny passage to the packet. These firewalls are very easy to configure and are also quite inexpensive. Some operating systems, such as Windows 10 and Linux, include built-in packet filtering capabilities.

There are a few disadvantages of packet filtering firewalls. One disadvantage is that they do not actually examine the packet or compare it to previous packets; therefore, they are quite susceptible to either a ping flood or SYN flood. They also do not offer any user authentication. As this type of firewall looks only at the packet header for information, it has no information about the packet contents.

It also does not track packets, so it contains no information about the preceding packets. Therefore, if thousands of packets come from the

same IP address in a short period of time, a host will not notice that this pattern is unusual. Such a pattern often indicates that the IP address in question attempts to perform a DoS attack on the network.

To configure a packet filtering firewall, simply establish appropriate filtering rules. A set of rules for a given firewall would need to cover the following:

- What types of protocols to allow (FTP, SMTP, POP3, etc.)
- What source ports to allow
- What destination ports to allow
- What source IP addresses to allow (you can block certain IP addresses if you wish)

These rules will allow the firewall to determine what traffic to allow in and what traffic to block. Due to this type of firewall using very limited system resources, it is relatively easy to configure and can be obtained inexpensively or even for free. Although it is not the most secure type of firewall, you are most likely to encounter it frequently.

3.2.2 Stateful Packet Inspection

The stateful packet inspection (SPI) firewall is an improvement of basic packet filtering. This type of firewall will examine each packet. It will then deny or permit access based not only on the examination of the current packet, but also on data derived from previous packets in the conversation.

This means that the firewall is aware of the context in which a specific packet was sent. This makes these firewalls far less susceptible to ping floods and SYN floods, as well as being less susceptible to spoofing. SPI firewalls are less susceptible to these attacks for the following reasons:

- They can tell whether the packet is part of an abnormally large stream of packets from a particular IP address, thus indicating a possible DoS attack in progress.
- They can tell whether the packet has a source IP address that appears to come from inside the firewall, thus indicating IP spoofing is in progress.
- They can also look at the actual contents of the packet, allowing some highly advanced filtering capabilities.

Nowadays, most quality firewalls use the stateful packet inspection method; when possible, this is the recommended type of firewall for most systems. In fact, most home routers have the option of using stateful packet inspection.

The name stateful packet inspection derives from the fact that in addition to examining the packet, the firewall examines the packet's state in relationship to the entire IP conversation. This means the firewall can refer to the preceding packets, as well as those packets' contents, source, and destination. As you might suspect, SPI firewalls are becoming quite common.

3.2.3 Application Gateway

An application gateway (also known as application proxy or application-level proxy) is a program that runs on a firewall. This type of firewall derives its name from the fact that it works by negotiating with various types of applications to allow their traffic to pass through the firewall. In networking terminology, negotiation is a term used to refer to the process of authentication and verification. In other words, rather than looking at the protocol and port the packet is using, an application gateway will examine the client application and the server-side application to which it is trying to connect to.

It will then determine if that particular client application's traffic is permitted through the firewall. This is significantly different from a packet filtering firewall, which examines the packets and has no knowledge of what sort of application sends them. Application gateways enable the administrator to allow access only to certain specified types of applications, such as web browsers or FTP clients.

When a client program, such as a web browser, establishes a connection to a destination service, such as a web server, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to gain access to the destination service.

In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall. This process actually creates two connections. There is one connection between the client and the proxy server and another connection between the proxy server and the destination.

Once a connection is established, the application gateway makes all decisions about which packets to forward. Since all communication is conducted through the proxy server, computers behind the firewall are protected.

With an application gateway, each supported client program requires a unique program to accept client application data. This sort of firewall allows for individual user authentication, which makes them quite effective at blocking unwanted traffic. However, the disadvantage is that these firewalls use a lot of system resources. The process of authenticating client applications uses more memory and CPU time than simple packet filtering.

Application gateways are also susceptible to various flooding attacks (SYN flood, ping flood, etc.) for two reasons. The first potential cause of a flooding attack may be the additional time it takes for an application to negotiate authenticating a request. Remember that both the client application and the user may need to be authenticated. This takes more time than simply filtering packets based on certain parameters.

For this reason, a flood of connection requests can overwhelm the firewall, preventing it from responding to legitimate requests. Application gateways may also be more susceptible to flooding attacks because once a connection is made, packets are not checked. If a connection is established, then that connection can be used to send a flooding attack to the server it has connected to, such as a web server or e-mail server.

This vulnerability is mitigated somewhat by authenticating users. Provided the user logon method is secure (appropriate passwords, encrypted transmission, etc.), the likelihood that someone can use a legitimate connection through an application gateway for a flooding attack is significantly reduced.

3.2.4 Circuit Level Gateway

Circuit level gateway firewalls are similar to application gateways but are more secure and generally implemented on high-end equipment. These types of firewalls also employ user authentication, but they do so earlier in the process.

With an application gateway, first the client application is checked to see if access should be granted, and then the user is authenticated.

With circuit level gateways, authenticating the user is the first step. The user’s logon ID and password are checked, and the user is granted access before the connection to the router is established. This means that each individual, either by username or IP address, must be verified before any further communication can take place.

Once this verification takes place and the connection between the source and destination is established, the firewall simply passes bytes between the systems. A virtual “circuit” exists between the internal client and the proxy server. Internet requests go through this circuit to the proxy server, and the proxy server delivers those requests to the Internet after changing the IP address. External users only see the IP address of the proxy server.

Responses are then received by the proxy server and sent back through the circuit to the client. It is this virtual circuit that makes the circuit level gateway secure. The private secure connection between the client application and the firewall is a more secure solution than some other options, such as the simple packet filtering firewall and the application gateway.

While traffic is allowed through, external systems never see the internal systems.