5.2.5.1. Firewalls

When the Internet was only a research network interconnecting research labs, security was not a concern, and most hosts agreed to exchange packets over TCP connections with most other hosts. However, as more and more users and companies became connected to the Internet, allowing unlimited access to hosts that they managed started to concern companies. Furthermore, at the end of the 1980s, several security issues affected the Internet, such as the first Internet worm [RE1989] and some widely publicised security breaches [Stoll1988] [CB2003] [Cheswick1990].

These security problems convinced the industry that IP networks are a key part of a company’s infrastructure, that should be protected by special devices like security guards and fences are used to protect buildings. These special devices were quickly called firewalls. A typical firewall has two interfaces:

- an external interface connected to the global Internet
- an internal interface connected to a trusted network

The first firewalls included configurable packet filters. A packet filter is a set of rules defining the security policy of a network. In practice, these rules are based on the values of fields in the IP or transport layer headers. Any field of the IP or transport header can be used in a firewall rule, but the most common ones are:

- filter on the source address. For example, a company may decide to discard all packets received from one of its competitors. In this case, all packets whose source address belong to the competitor’s address block would be rejected
- filter on destination address. For example, the hosts of the research lab of a company may receive packets from the global Internet, but not the hosts of the financial department
- filter on the Protocol number found in the IP header. For example, a company may only allow its hosts to use TCP or UDP, but not other, more experimental, transport protocols
- filter on the TCP or UDP port numbers. For example, only the DNS server of a company should received UDP segments whose destination port is set to 53 or only the official SMTP servers of the company can send TCP segments whose source ports are set to 25
filter on the TCP flags. For example, a simple solution to prohibit external hosts from opening TCP connections with hosts inside the company is to discard all TCP segments received from the external interface with only the SYN flag set.

Such firewalls are often called *stateless* firewalls because they do not maintain any state about the TCP connections that pass through them.

Another type of firewalls are *stateful* firewalls. A stateful firewall tracks the state of each TCP connection passing through it and maintains a TCB for each of these TCP connection. This TCB allows it to reassemble the received segments in order to extract their payload and perform verifications in the application layer. Some firewalls are able to inspect the URLs accessed using HTTP and log all URLs visited or block TCP connections where a dangerous URL is exchanged. Some firewalls can verify that SMTP commands are used when a TCP connection is established on port 25 or that a TCP connection on port 80 carries HTTP commands and responses.

**Note**

Beyond firewalls

Apart from firewalls, different types of “security” devices have been installed at the periphery of corporate networks. Intrusion Detection Systems (IDS), such as the popular *snort*, are stateful devices that are capable of matching reassembled segments against regular expressions corresponding to signatures of viruses, worms or other types of attacks. Deep Packet Inspection (DPI) is another type of middlebox that analyses the packet’s payload and is able to reassemble TCP segments in order to detect inappropriate usages. While IDS are mainly used in corporate networks, DPI is mainly used in Internet Service Providers. Some ISPs use DPI to detect and limit the bandwidth consumed by peer-to-peer applications. Some countries such as China or Iran use DPI to detect inappropriate Internet usage.