Firewalls

CISC 3325 — CUNY Brooklyn College
Lecture Notes

Firewalls

In this chapter, we will:

1. Explain why firewalls are used for and properly define this term.
2. Present the basic functions of a firewall. That is, what activities do we expect a firewall to perform?
3. Discuss the activity of Packet Filtering and show several examples of filtering rules.

Firewalls: Motivation

In the early days of computing, there was no outside connectivity and no World Wide Web. Networks belonging to businesses would usually implemented a **closed network**, which typically allowed secure access only to known parties and employees. Since no 'outsider' device was connected to such a network, there was no danger of hacking this network remotely.

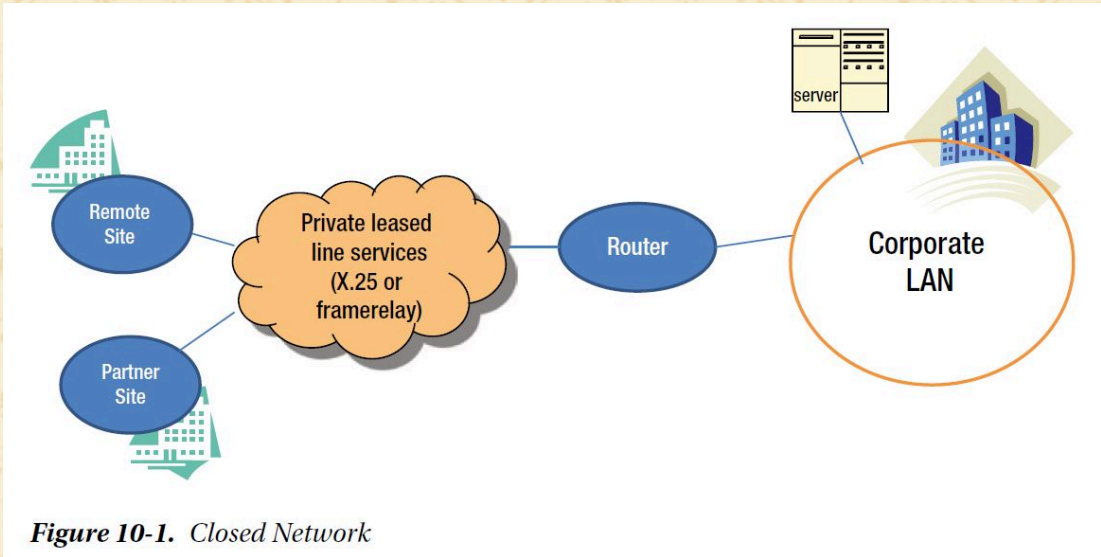

Figure 10-1. *Closed Network*

"Figure 10-1: Closed Network" (page 206), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

Firewalls: Motivation

This concept worked well until the advent of World Wide Web and e-business.

As e-business, World Wide Web, and related applications continue to grow, a closed network was no longer closed and private networks started getting connected to the outside public Internet as well. **Extranet** connected internal and external business processes. Enterprises realized the benefit of e-commerce applications to business partners and consumers, and connecting sales-force automation systems to mobile sales force.

Today, an enterprise network demands an **Open Network** (see illustration on the next slide) with the flexibility to connect to the Internet and web apps, and to support telecommuters accessing through mobile devices, and much more. According to the latest statistics, more than 15 billion devices have been connected to the Internet in 2023, and experts predict that the number will be 17 billion in 2024.

Though these applications have an immediate benefit to the end user, they can pose security risks to the individual user and the information resources of a company and government. ***How can a network protect itself from malicious connections?***

Firewalls: Motivation

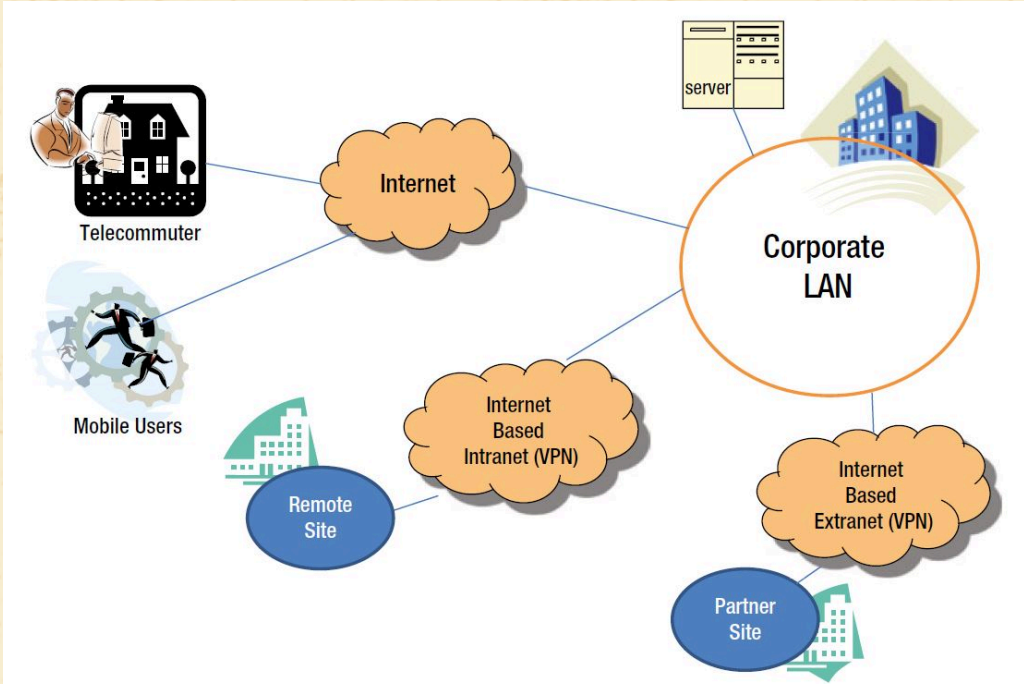

Figure 10-2. *Open Network*

"Figure 10-2: Open Network" (page 207), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

Firewalls: Definition

This motivation brings us to the discussion of firewalls.

The term **firewall**, in the real world, means a wall that was built to protect from fire and intended to slow the spread of fire through a structure.

The same concept is used in networks too: a **network firewall** is intended to stop unauthorized users from accessing the network and its services from other external networks. Specifically, a firewall is a combination of software and hardware that decides what kinds of connection requests and what specific data packets can pass to and from a computer or a local network.

The most common deployment of firewalls is between a trusted network of an organization to an untrusted network (typically the Internet) as shown on the next slide. Typically, the Internet Service Provider (ISP) connection terminates at a border router and then connects to a firewall.

Firewalls: Definition

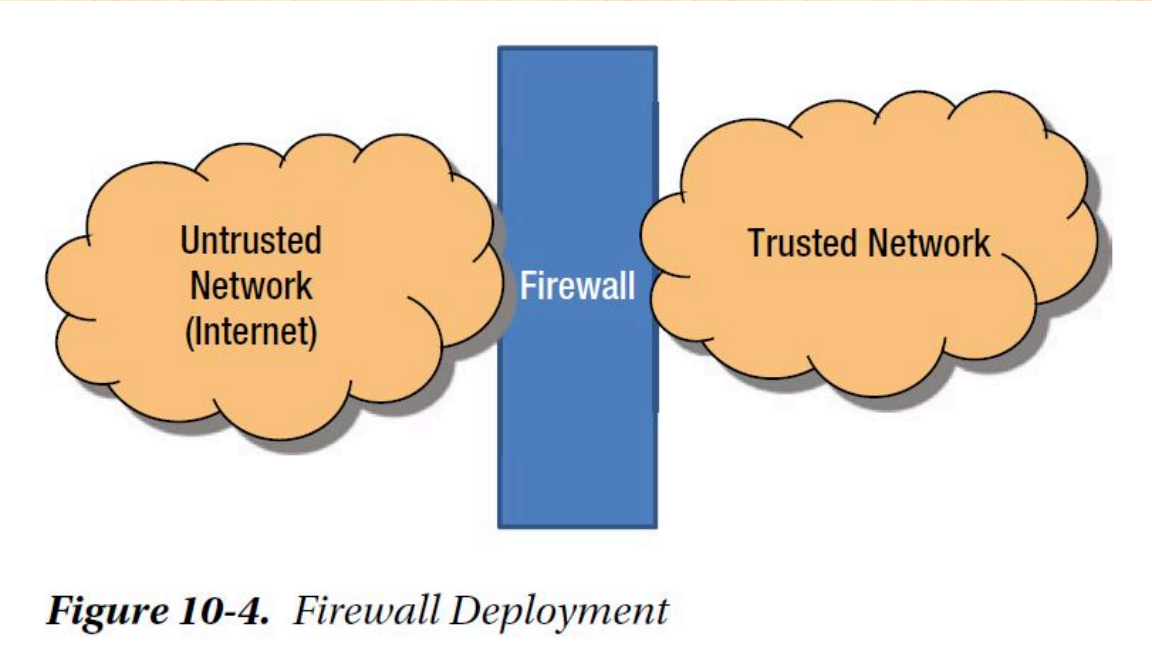

Figure 10-4. *Firewall Deployment*

"Figure 10-4: Firewall Deployment" (page 209), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

Firewalls: Definition

Any questions?

Basic Functions of Firewalls

A firewall in the networking world should examine the traffic that is entering into the network and pass the "wall" based on some rules defined by the network and its resources. It acts as a security guard, who normally sits at the main gate, and checks your identity and access privileges and lets you in.

The main responsibilities of a firewall include:

1. **(Stateless) Packet filtering**: A firewall filters IP packets. The IP headers of all the packets that enter or exit the network firewall are inspected (to check their source, destination address, etc.) Firewall makes an explicit decision on each packet that enters as to whether to allow the packet or deny the packet.
2. **Stateful Packet Filtering**: Here the packet filtering goes beyond basic packet filtering. This keeps track of state of connection flows for all the packets, in both directions. It also keeps track of all the IP addresses currently connected at any point of time.
3. **Application Level Gateways (Proxy)**: A firewall is also capable of inspecting application level protocols. This requires the firewall to understand certain specific application protocols.

Basic Functions of Firewalls

4. **Logging**: A firewall should generate and save a log of all its activities, especially on data packets it has blocked. This log will be used in the future when the user/administrator of the network would like to audit the firewall activity.
5. **Speed and transparency**: A firewall should perform the aforementioned activities a fast way, transparent to the user.

In the scope of this course, we will elaborate on the packet filtering responsibility of a firewall.

As the name suggests, a **packet-filtering firewall** filters the packets that are entering and leaving the network. The firewall inspects each IP packet and a decision is made. Each packet is compared with a set of **filter rules** and based on any match, the packet is either allowed, denied, or the connection is dropped. Packet filtering works on the network layer and transport layer of the OSI model or TCP and IP layer of the TCP/IP model (see Slide 14 of Topic 8: Networks & Network Security.) It does not remember the state of a network (when the connection started, the previous states of the connection, etc.) and hence it is called a **stateless firewall**.

Packet Filtering

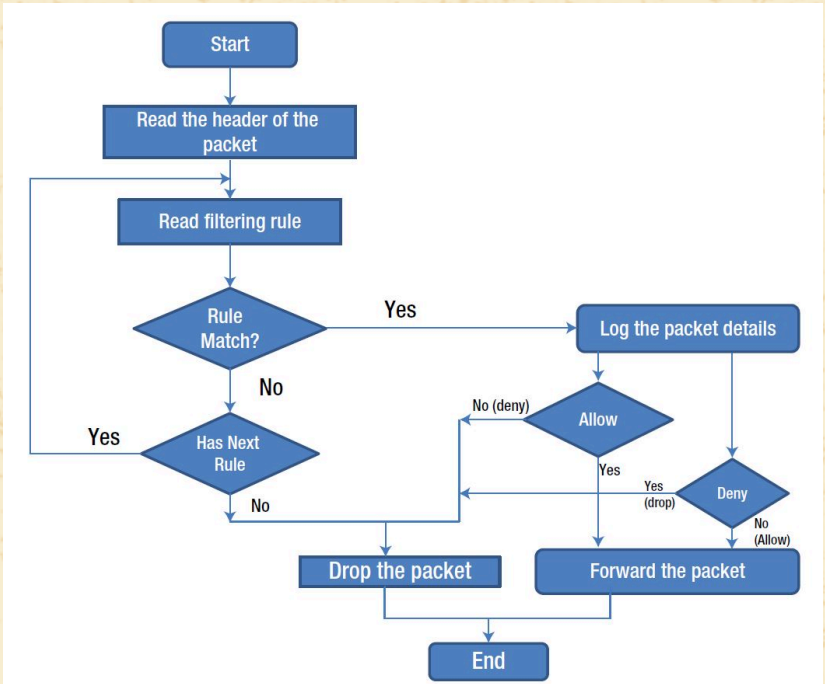

Figure 10-6. *Packet filtering flow diagram*

"Figure 10-6: Packet Filtering Flow Diagram" (page 211), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

Packet Filtering Rules

A packet filter firewall is configured with a set of rules that define when to accept a packet or deny. When the firewall receives a packet, the filter checks the rules defined against IP address, port number, protocol, and so on. In particular, if a rule says 'accept,' then the packet is accepted in the network, otherwise it is dropped (= the packet isn't sent to the destination.)

The following table contains an example set of rules that tell a firewall what do to with packets:

Table 10-2. *Packet filtering rules*

Rule	Direction	Source Address	Destination Address	Application (TCP port)	Filter Set	Action
1	Inbound	Trusted external host (162.22.34.56)	Internal (10*.*)	Http	Any	Permit
2	Outbound	Internal	Trusted External host (162*.*)	SMTP	Any	Permit
3	Inbound or Outbound	Any	Any	TFTP	Any	Deny

"Table 10-2: Packet filtering rules" (page 213), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

Packet Filtering Rules

In the example above, a packet sent from IP `162.22.34.56` into the current network is accepted according to Rule 1 of the table, and, therefore, is sent to the destination. On the other hand, a packet sent from another IP address, e.g., `175.236.120.12` will match Rule 3 (since none of Rules 1 and 2 match,) which means that the packet will be dropped.

Besides using the source and destination IP addresses, a firewall might also make its decisions based on the protocols used for the transmission of this packet, the source or destination port numbers, and even the contents of the packet itself. The latter method of filtering based on the content of the packet is called **content filtering**.

A few more examples of packet filtering:

- Allow e-mail and HTTP (web) services, but block services such as TFTP and Telnet.
- Block all incoming connections from the outside except for SMTP (so that you can keep receiving emails).
- Allow port `443` (= the default port for secure HTTPS traffic) for all service destination addresses.
- Allow port `80` (= the default port for secure HTTP traffic) for all service destination addresses.

Advantages and Disadvantages of Packet Filtering

The main advantages of the packet filter firewall:

- A strategically placed packet filtering firewall can protect the entire network. Most of the routers support packet filtering. If you have a border router placed just after Internet ISP, with the packet filtering enabled, you can protect an entire network regardless of the network size.
- Packet filtering is widely available in routers. Leading networking vendors like Cisco, Juniper, and HP provide packet filtering on their routers known as Access Control Lists (ACL), which is configured in all the border routers.

There are a few disadvantages:

- The packet filtering rules tend to be hard to configure. A network/system administrator needs a lot of expertise and proper strategy to configure it right.
- Once it is configured, it is difficult to comprehensively test and verify whether it is working correctly or not.
- It is a stateless machine. It does not remember the state of the previous packet. Stateless packet filters are vulnerable to attacks. Hence, some of the attacks, such as spoofing attacks, can easily bypass firewall rules of this kind of a firewall.

Advantages and Disadvantages of Packet Filtering

Any questions?

Firewalls: Sources

Rao, Umesh Hodeghatta, and Umesha Nayak. "Chapter 10: Firewalls." *The InfoSec handbook: An introduction to information security.* Springer Nature, 2014, pp. 205-223. URL: https://link.springer.com/content/pdf/10.1007/978-1-4302-6383-8.pdf#chapter+10:+firewalls

Salomon, David. "Chapter 7, Section 6: Firewall Basics." *Elements of computer security.* Springer Science & Business Media, 2010, pp. 202-205. URL: https://link-springer-com.brooklyn.ezproxy.cuny.edu/content/pdf/10.1007/978-0-85729-006-9.pdf#7.6+firewall+basics