Middleboxes: Firewalls

In this lesson, we'll study middleboxes!

We'll cover the following

Introduction

When the TCP/IP architecture and the IP protocol were defined, two types of devices were considered in the network layer:

1. **End hosts** which are the sources and destinations of IP packets
2. **Routers** that forward packets. When a router forwards an IP packet, it consults its forwarding table, updates the packet's TTL, recomputes its checksum and forwards it to the next hop. A router **does not need to read or change** the contents of the **packet's payload**.

However, in today's Internet, there exist devices called **middleboxes** that are **not strictly routers** but which **process, sometimes modify, and forward IP packets** (RFC 3234). Some middleboxes only operate in the network layer, but most middleboxes are able to analyze the payload of the received packets and extract the transport header, and in some cases the application layer headers.

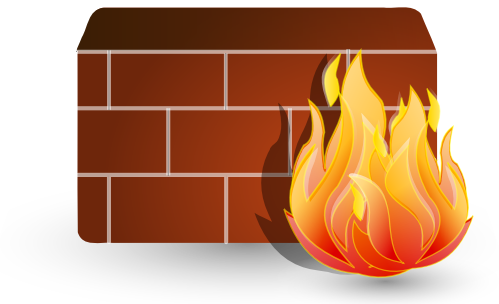
Over the next couple of lessons, we'll briefly describe **two types of middleboxes: firewalls and network address translation (NAT) devices**.

Firewalls

Firewalls

Why Firewalls?

When the Internet was only a research network interconnecting research labs, security was not a concern. However, as the Internet grew in popularity, security concerns grew.



This was exacerbated by several security issues at the end of the 1980s such as the first Internet worm and some other widely publicized security breaches.

> 🔎 **Did You Know?** The term **firewall** originates from a special wall used to confine the spread of fire in a building. It was also used to refer to a metallic wall between the engine compartment and the passenger area in a car. The purpose of this metallic wall is to prevent the spread of a fire in the engine compartment into the passenger area.

Firewall Interfaces

These security problems convinced the industry that their networks should be protected by special devices the way security guards and fences are used to protect buildings. These special devices came to be called **firewalls**. A typical firewall has **two interfaces**:

1. An external interface connected to the global Internet.
2. An internal interface connected to a trusted network.

Firewall Filters

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 certain portions of the network while maintaining access to public resources.

Another example of source based filtering is **black lists**. Any packets from an IP on the black list will be discarded. IPs known for their use by spammers, for instance, are blacklisted by many networks.

- Filter on the **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 receive 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.

Stateless Vs. Stateful Firewalls

A firewall that does not maintain the state of flows passing through it is known as a **stateless firewall**.

However, a **stateful firewall**, on the other hand, sees the first packet in a flow that is allowed by the configured security rules it creates a **session state** for it.

All subsequent packets belonging to that flow are allowed to go through. This filtering is more efficient compared to stateless firewalls that have to apply their rules to each and every packet. The flip side is the maintenance of state, which needs to be controlled.

Host-based Vs. Network-based Firewalls

Network-based firewalls are hardware based and generally deployed on the edge of a network. They are easy to scale and simple to maintain.

A host based firewalls, however, are software based and are deployed on end-systems. They are generally not easy to scale and require maintenance.

Quick Quiz!

1 What is the purpose of firewalls?

- A) They speed up the traffic that passes through them
- B) They only allow certain types of traffic to pass through them
- C) They ensure that only packets with a valid checksum pass through them

COMPLETED 0%

1 of 2

In the next lesson, we'll have a look at another middlebox, NAT!