Chapter 1

Firewalls and Tunnels

1.1 Networking

Definition 1.1.1 ▶ Datagram, Packet

Networked data is delivered as a series of ***datagrams*** (or ***packets***) which are each composed of:

- a ***header*** that provides information to help route the datagram, and
- a ***payload*** that contains the actual data transmitted.

If a datagram is too large, it can be broken into fragments.

Layer 1: The Physical Layer

This is the physical connection between computers that actually sends data between computers. This is nearly always a CAT cable that uses copper wire to transmit electrical signals representing bits. Different cat cables provide different levels of speed.

Layer 2: Data Link

The data link defines how data is transferred over a physical medium. This converts layer 2 datagrams into electrical signals. Most devices use the ethernet protocol where devices are identified using a MAC address.

Layer 3: Network Layer

Definition 1.1.2 ▸ Packet-Switched Networking, Hop

Packet-switched networking refers to a networking protocol where packets are sent via a series of connected devices. Each stop on the pathway between sender and receiver is called a ***hop***.

This means routes are not negotiated beforehand! Every packet has to "find" its route to its destination.

The `traceroute` program can be used to see the hops between your device and the specified server.

Definition 1.1.3 ▸ Internet Control Message Protocol (ICMP)

ICMP is a protocol used to communicate among devices on the same network about problems with data transmission

Layer 4: Transport Layer

Definition 1.1.4 ▸ TCP

TCP simulates a connection over a packet-switched network for bidirectional communication. It provides reliable and in-order packet delivery at the cost of some performance.

TCP sockets are bound ot individual connections defined by the tuple (local IP, local port, remote IP, remote port). Servers have a well-defined server-side port, but clients usually use a temporary/random port for their side of the connection. Servers accept connections using a server socket which results in the creation of a normal TCP socket for each client connection.

To establish a connection, a three-way handshake is used:

1. `SYN` packet sent by the client
2. `SYN-ACK` packet sent by the server acknowladging the first packet
3. `ACK` packet sent by client acknowledging the second packet

To confirm that data is received by the other side, all packets will set the "acknowledged" flag,

denoted `ACK`. Any "holes" in the information are filled by the TCP protocol.

Definition 1.1.5 ▶ UDP

UDP is a connectionless, one-directional network protocol that does not guarantee reliability or in-order packets.

Layer 5: Application

This is where the application handles the data. Many have multiple sublayers (e.g. TLS is layered below HTTP to create HTTPS).

IPSec

Initially, IP was created without security in mind. It did not guarantee confidentiality, integrity, nor authentication. ***IPSEC*** was initially designed to secure IPv6 and was later backported to IPv4.

1.2 Firewall

Definition 1.2.1 ▶ Firewall

A ***firewall*** is some mechanism that inspects traffic entering of leaving a device in the network. It can filter ***inbound packets*** to protect against external adversaries, and it can filter ***outbound packets*** to protect against malicious insiders.

Packet Filters

The most common type of firewall is a ***packet filter***, which filters traffic at a packet-level based on a list of rules. The most common actions are `ALLOW`, `DROP`, or `REJECT`.

Some limitations include:

- Requires a true perimiter (can be fixed by zero-trust networking)
- Does not protect against lateral movement within the network
- Does not protect against malicious content from a benign connection (e.g. cross-site scripting attack)

- Can be circumvented by tunneling malicious traffic through a benign connection

Proxy Firewall

A ***proxy firewall*** is a proxy that is an intermediary connection between two hosts. It can then pass all traffic to an app-level filter for inspection. It can view all traffic, including encrypted traffic. In addition to allowing or denying traffic, it can even modify traffic to possibly add or remove functionality. To any user, the proxy can be entirely transparent.