**Firewalls**

**What is a Firewall?**

Software application that helps prevent access from one side to another

* Can be host based or networked based

**Host-Based**

Windows

* Windows Defender

Linux

* Iptables
* Firewalld

Web apps will use Web App Firewall (WAF)

**Network-based**

Cisco, Pfsense

Normally between networks and the internet

* Normally handles the access for a DMZ

2 types of firewall settings

* Packet filtering
* Stateful inspection

**ACL -** Access Control List

A list that holds the access rules for the firewall

First do deny all rule, then allow what you want

* Can allow, block, drop etc. based on any number of parameters

**Packet Filtering Firewall**

Also known as Stateless Inspection Firewall

Allows or denies packets based on the following:

* Source IP
* Dst IP
* Src port
* Dst port

**Doesn’t look at the packet (data itself), just looks at the IP header info^**

Not commonly used any more

* Provides weak protection due to the limitations of the access rules
* Doesn’t inspect full packet so cant differentiate misbehaving data/packets from genuine ones
  + Traffic could be disguised and it wouldn’t know
* Can be bypassed with tunnelling

**Stateful Inspecting Firewall**

Keeps track of active connections and **inspect packet itself**

* Will identify malicious/dodgy traffic
  + E.g., HTTPS running through SSH port
* Commonly used with network-based firewalls
* Built on top of a stateless backbone

Can be a bottleneck for the network traffic

* Trying to inspect every single packet can:
  + Slow the traffic
  + Block the traffic

Test before massive scans are done

* Scans can be blocked
* Scans can take down the firewall

**Web Application Firewall**

Used between browser and web app

* Similar concept to standard firewall but only for web apps

Rule set is based on attacks like SQLi, XSS etc.