2. Firewalls & Filtering Techniques

A firewall is either a hardware device or a utility program that monitors incoming and outgoing network traffic and blocks any traffic that it deems suspicious. It's like the high wall around a castle, blocking out the invading hordes, whilst still allowing friendly citizens in and out through its drawbridge.

The difference between the hardware firewall and the software firewall is that the hardware firewall is an actual physical device that will sit between your local area network and the internet. Whereas the software firewall will be installed on each individual device.

This means the hardware firewall can stop bad data from ever entering the network, while software firewalls can offer closer controls over specific devices and how they interact with the network and internet.

There are a few different techniques that firewalls use to filter data.

Packet Filtering & Inspection

With packet filtering, the firewall inspects each packet of data and compares it to pre-defined security rules (known as the firewall policy, or ruleset). If the packet is flagged by the rules, then it is prevented from passing through the firewall.

Application Level Awareness

An application firewall is a form of firewall that controls the input and output of packets to an application. This is important as hackers may attack a network directly at the application layer, exploiting flaws in the security of specific applications. So, if an attacker gets past the network firewall, there is an added layer of protection.

Inbound and Outbound Rules

Inbound and outbound rules are used as part of the filtering performed in packet filtering and application filtering. We mentioned the security rules when explaining packet filtering, these are the inbound and outbound rules.

Inbound rules will define what data should be accepted, rejected or dropped from entering the network or computer. While outbound rules will do the same for data leaving the network or computer.

We mention the terms accepted, rejected and dropped. These are the responses that can be performed by these firewall rules. These can be summarised as:

- **Accepted** – allow the traffic through.
- **Rejected** – do not allow the traffic through and send an “unreachable” reply.
- **Dropped** – do not allow the traffic through and send no response.

Network Address

All devices on a network are assigned an IP address to uniquely identify them. We often use these addresses in firewalls as part of our rules as we may want to block or allow data from or to a specific address or range of addresses.

We can use Network Address Translation to assign private IP addresses to our devices within our private network. The NAT will translate our private addresses to our public internet gateway address when sending or receiving data over the public internet.

Part of the reason for this is due to the limited number of IP addresses that were available using IPv4. Considering, without NAT, every computer in every network would need a completely unique IP.

However, NAT also adds security to the network by hiding our devices addresses from the outside world.

Further Thoughts

Will an organisation use a hardware firewall, software firewall, or both? Research the answer to this online.

Lesson Summary

- Anti-virus software is a utility program that is used to prevent malicious software from infecting your computer or detect and remove malicious software that has already infected your computer.
- Signature detection identifies malware using a pattern (the signature) for the malware code that is compared to programs on your hard disk to identify the viruses.
- Heuristic detection monitors the behaviour of programs to identify any suspicious behaviour and flags it as a possible virus.

- Once detected, users have the option to clean, quarantine or delete the viruses detected.
- Firewalls are either a hardware device or a utility program that monitors incoming and outgoing network traffic and blocks any traffic that it deems suspicious.
- Packet filtering is where the firewall inspects each packet of data and compares it to pre-defined security rules. If the packet is flagged by the rules, then it is prevented from passing through the firewall.
- An application layer firewall controls the input and output of packets to an application.
- Inbound and outbound rules define what packets should be allowed by the firewall. We can set accept, reject or drop rules.

Network address translation is used to hide the addresses of our device from the outside world.