1.3.3 Internet Security

Firewall

A **firewall** is a piece of hardware or software that controls access to and from a network.

Firewall rules determine which network traffic is allowed through or blocked.

Packet filtering

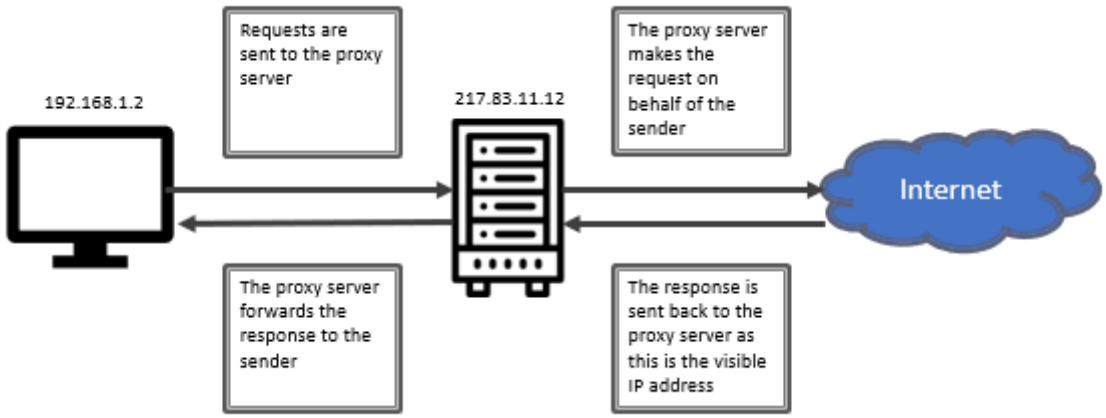
- Packets of data are inspected by the firewall as they arrive to check which port they are trying to access.
- If the traffic is to be allowed through, the firewall will open the port for the duration of the connection.

Proxy Server

A **proxy server** makes a web request on behalf of your own computer.

This hides the IP address of the device that made the real request behind that of the proxy server.

The web server sees the proxy server's IP address rather than the client's IP address.



Malware

Malware is a piece of software with malicious intent.

Virus

- A virus infects by attaching itself to a legitimate host program.
- When the program executable is run, the virus activates and begins to replicate, corrupt files or damage systems.

Worm

- Worms are self-replicating and do not need interaction to run.
- They spread automatically over networks using vulnerabilities or open ports.
- Can carry payloads such as ransomware

Trojans

- Trojans disguise themselves as a legitimate program.
- The user is tricked into installing or running the program.
- Once inside it performs malicious actions such as spying or opening backdoors.

Vulnerabilities Exploited by Malware

Malware can exploit weaknesses in software, operating systems or user behaviour.

- Unpatched software — known security vulnerabilities may be exploited.
- Open ports/network vulnerabilities — worms can spread between vulnerable devices.
- Weak security practices — users may be tricked into installing a Trojan.
- Poor input validation — vulnerabilities such as buffer overflows can be exploited.

Protections Against Malware

Improved code quality, monitoring and security measures can reduce the risk and impact of malware.

Measures include:

- **Keep software and operating systems patched** to remove known vulnerabilities.
- **Use input validation and bounds checking** to reduce vulnerabilities such as buffer overflows.
- **Use strong passwords and two-factor authentication** to reduce unauthorised access.
- **Use access rights/permissions** to limit what compromised programs or users can access.
- **Monitor systems and network activity** to detect unusual behaviour.
- **Use anti-malware software** to detect and remove malicious software.