INTERNET SECURITY

Firewall

Hardware or software for protecting against unauthorised access to a network

Combination of techniques used to protect an organisations network (LAN) from unauthorised access by users outside the network (Internet / WAN)

Packet Filtering

Technique for examining the contents of packets entering a network and rejecting them if they do not confirm to certain rules.
Check Packet Header to determine if it has come from a recognised source (IP address)

Stateful Inspection

Technique for examining the contents of packets entering a network and rejecting them if they do not form part of a recognised communication
Connection request, reply, subsequent requests & replies

Application Level

Extends Stateful Inspection by understanding certain Applications & Protocols (DNS, HTTP, FTP etc). Can detect if a protocol is being abused in some way by an unwanted application

Proxy server

Server that acts on behalf of other nodes on the LAN. By routing through a proxy server there is no direct connection between the computer on the LAN and the Internet.

Rules can be set up for outbound & inbound packets to control what is allowed to happen

- Content filtering to meet Acceptable Use Policies
- User Authentication for external Log In
- Caching proxies can save replies from previous requests (DNS replies, Web pages etc) which speed up the response time for multiple users of the same external server

Proxy server can be considered to perform a similar role to NAT but they operate at different levels in the Protocol Stack

- NAT works at the Network level (On each packet via IP Address & Port No)
- Proxy works at the Application level (On requests based on the program & protocol being used)

Private – public key encryption

Symmetric encryption: where the sender and the receiver both use the same key to encrypt and decrypt data

Asymmetric encryption: where a public and a private key are used to encrypt and decrypt data

Digital certificate (aka SSL Secure Socket Layer) and signature: method of ensuring that encrypted message is from a trusted source as they have a certificate from a Certification Authority.

Private key is a code used to encrypt/decrypt data that is only known by one user but is mathematically linked to a corresponding Public key.

Public key is a code used to encrypt / decrypt data that can be made public and is mathematically linked to a corresponding Private key

Asymmetric encryption:

Encryption with receiver's public key

↓

Decryption with receiver's private key

Digital signature:

Broadcast containing encryption with sender's private key

↓

Verification by decrypting with receiver's private key

Malwares

- Trojans: malware program that is hidden within another file on your computer
  - Does not replicate itself
  - Can be activated by user by double clicking on it
  - Can be activated by a hacker remotely

- Virus: malware program that attaches itself to another file in order to infect a computer. It replicates via a host file and so spread quickly in the computer and network.

- Worm: malware or a type of virus that replicates itself and spreads around a computer system. It does not need to be attached to another file in order to infect a computer.

Protecting against attacks

- Users
  - observe warnings about expired Digital Certificates & missing Digital Signatures
  - Use passwords on programs & files
  - Encrypt data files
- Programmers
  - Use encryption on sensitive data
  - Use programming languages with in-built security features
  - Keep code up to date with respect to new security threats
  - Use access rights appropriate to the user role
  - Write secure code
- Administrators
  - Use firewall with packet filtering & stateful inspection
  - Use anti-virus and ensure it is up to date
  - Use up to date Network Operating Systems