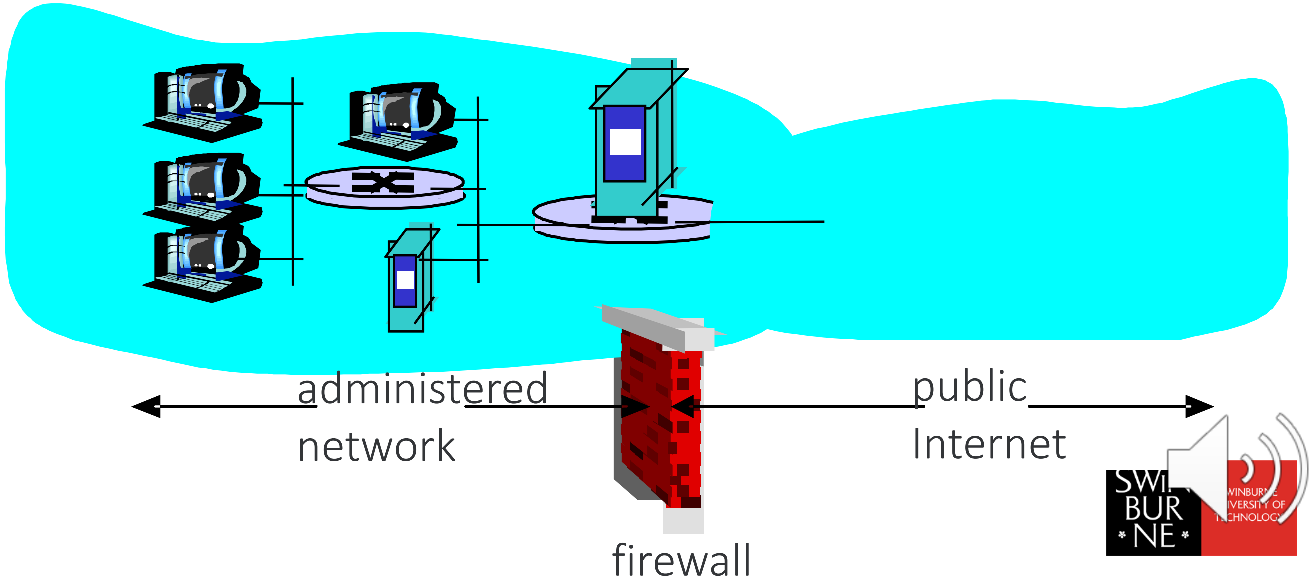
Firewalls

Firewalls: Why

- **prevent denial of service attacks:**
  - SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections
- **prevent illegal modification/access of internal data.**
  - e.g., attacker replaces CIA’s homepage with something else
- **allow only authorized access to inside network** (set of authenticated users/hosts)
- **three types of firewalls:**
  - stateless packet filters
  - stateful packet filters
  - application gateways



Firewalls and port blocking

- A firewall filters incoming traffic according to a set of rules depending on things like:
  - the destination IP address or host +domain name
  - the source IP address or domain name
  - the protocol being used (bound to specific ports)
  - the port number of the destination
  - the process (program name) listening at the destination
  - the contents of a packet (high end firewalls and IDS)
- The primary defence offered by a firewall is to block particular destination ports or source IP addresses.
  - Some firewalls use NAT traversal to 'hide' the inside of the network.

Firewalls…

- The old approach to managing a firewall was "default allow":
  - ➢ leave all ports open to all IP addresses
  - ➢ create a rule to close a port / block an IP if under attack.
  - ➢ This policy allows zero-day exploits free access to a server.

Firewalls…

- The modern approach is "default deny":
  - ➢ All ports are blocked to all IP addresses except those which are needed for particular services (e.g. HTTP, FTP, SSH).
  - ➢ If another service is needed, a rule is created to allow traffic to it through a specific port, often from a restricted range of IPs or subnet. Zero-day exploits are much easier to resist if almost every port is locked down.

Proxy servers and IP addresses

- Proxy servers perform three functions:
  - Filter packets based on content, source IP address or domain name.
  - Cache downloads to speed up repeated downloading of web pages, media files and archived material.
  - Perform NAT traversal to facilitate the sharing of one external IP address by an internal network of hosts.

Proxy Servers

- A side effect of NAT traversal is that the proxy server re-addresses the source IP of each out-bound packet to that of it's external interface, effectively making the originator of the packet anonymous.
- Returning packets are re-addressed so that they go to the internal network host which requested them.
- Proxy servers can be used for intercepting and logging internet traffic.
- Proxy servers are capable of port mapping – directing traffic to a particular IP address depending on which port it arrived on.

Firewalls..

- Stateless firewalls
  - fast, efficient
  - don’t prevent SYN floods, port scanning
- Stateful firewalls
  - can detect patterns of behaviour, scans, floods
  - richer set of firewall rules
- Application layer firewalls
  - do deep packet inspection
  - detect malware in payload
  - classify traffic according to payload