



Data Communications and Networking

Lecturer: Toby Daniel

IP Ports

- The TCP layer requires a **port*** number to be assigned to each message. This way it can determine the type of service being provided.
 - These ports are reference numbers used to define a service.
 - Each IP address has port numbers that range from 1 – 65,535
 - Ports are used by TCP to name the ends of logical connections between two computers.
- *Note that these are not serial and parallel ports that you find on the back of your computer

Ports

- The following example shows the standard notation for writing the IP address and Port number:

192.168.0.46:80

- This example indicates that a message will be sent to port 80 of the IP address 192.168.0.46

Port Numbers

The port numbers are divided into three ranges:

- **Well Known Ports** are those from 0 - 1023.
- **Registered Ports** are those from 1024 - 49151.
- **Dynamic and/or Private Ports** are those from 49152 - 65535.

Well Known Ports

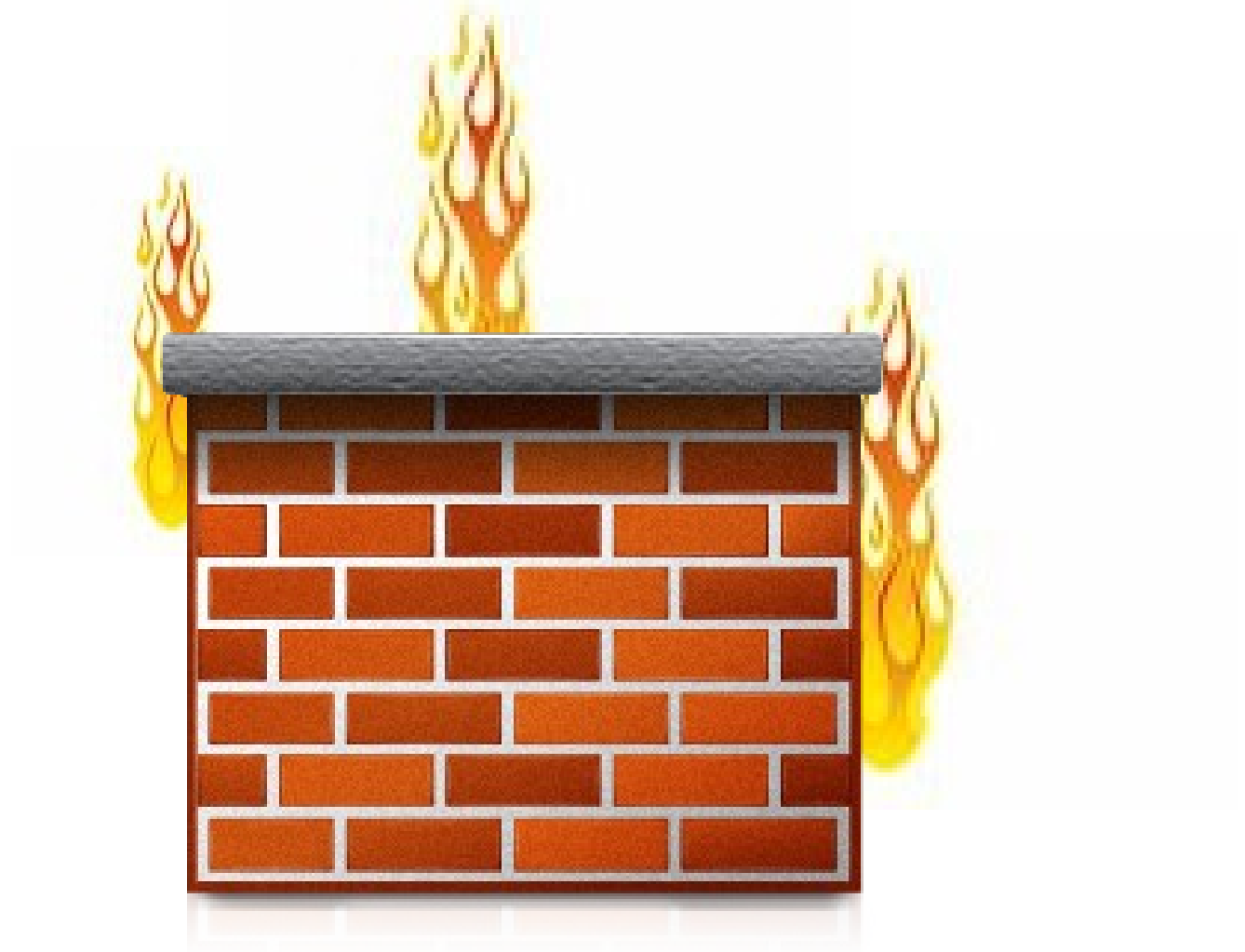
- The Well Known Ports are assigned by the IANA (Internet Assigned Numbers Authority)
- On most systems they can only be used by system processes or by programs executed by privileged users.
- Common Internet services have specific Well Known Port numbers assigned to them.

Common Internet Service Ports

- 21 FTP - File Transfer Protocol
- 23 Telnet - terminal emulation over TCP/IP
- 25 SMTP - Simple Mail Transfer Protocol
- 53 DNS - Domain Name System
- 80 HTTP - HyperText Transfer Protocol
- 110 POP3 - Post Office Protocol
- 161 SNMP - Simple Network Management Protocol
- 194 IRC - Internet Relay Chat
- 443 HTTPS - secure HTTP (SSL)
- 569 MSN- Microsoft Network instant messaging

Plus many more!

Firewalls



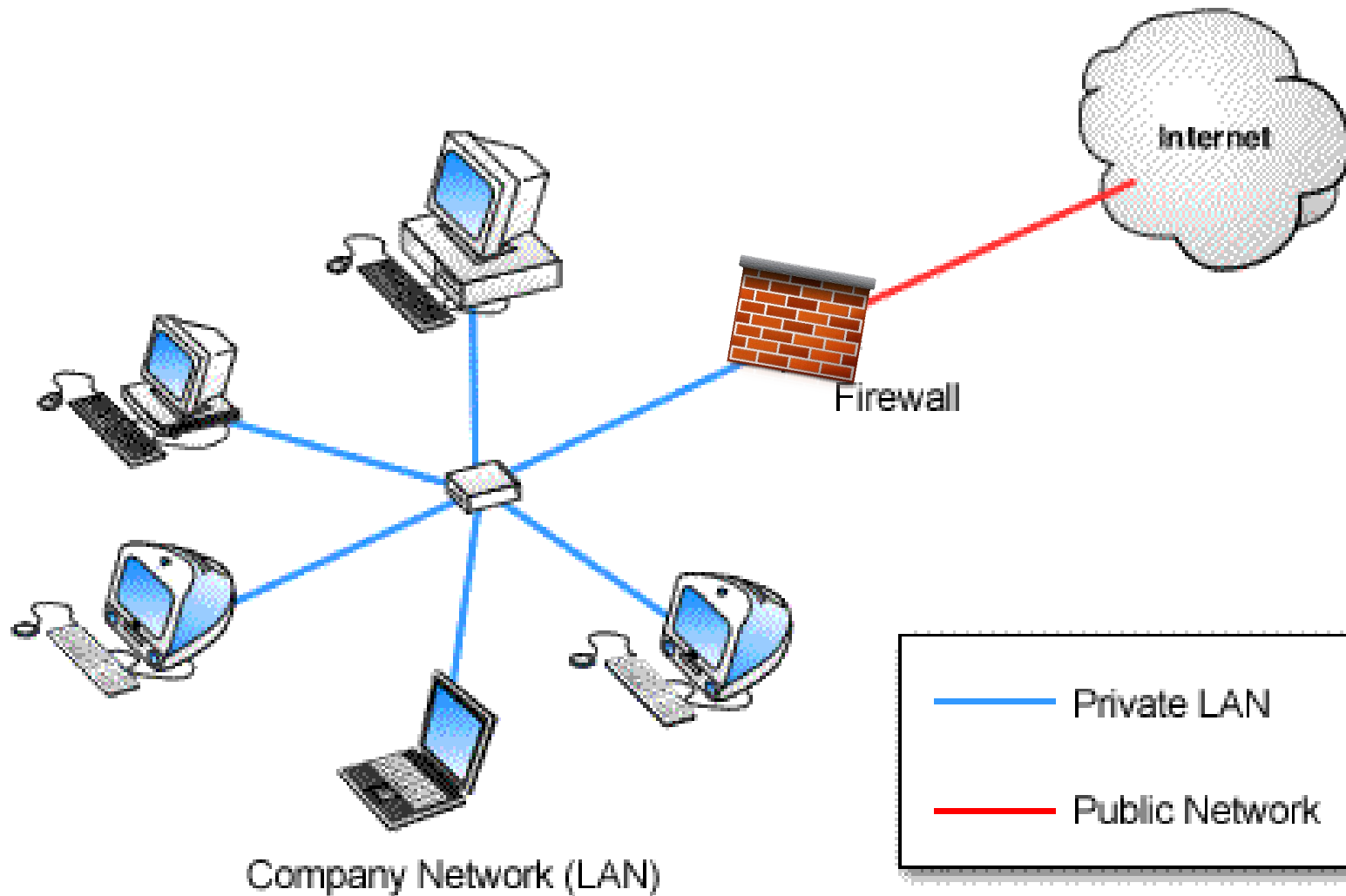
What is a firewall?

- In the building industry, a firewall is a specially designed wall that controls the spreading of a fire.
- In networking, a firewall is a specially designed device that controls the spreading of a network threat.
- The most commonly talked about source of network threats is the Internet.

Firewall

- A firewall is a system that secures a network, shielding it from access by unauthorized users.
- Firewalls can be implemented in software, hardware or a combination of both.
- In addition to preventing unrestricted access into a network, a firewall can also restrict data from flowing out of a network.

Simple LAN Firewall Placement



What firewalls do:

- Packet-filtering
- Circuit-level security
- Application-level security

Most firewalls provide one or more of the above protective measures.

Packet Filtering

- Packet filtering screens incoming and outgoing packets.
- The firewall accepts or denies packets based on information contained in the packets' TCP and IP headers.
 - Source address 192.168.0.14
 - Destination address 172.17.30.45
 - Application or protocol HTTP
 - Source port number 80
 - Destination port number 80
- The firewall compares the packet information to **rules** that have been configured on the firewall.

Example of Packet Filtering Rules

- Deny access from a specified IP address
- Allow access only from a specified range of IP addresses
- Block all ports except specified ones from entering and leaving the LAN
 - Ports are left open for required services
http, ftp, email etc.
- Hackers and spyware software can use high number ports to access computers on a network and compromise them.

Packet Filtering

- Packet filtering operates at the Network layer of the OSI model.
- The packet filter only looks at the header information not at the contents of the packet. This is quick and easy.
- Hackers can get their packets through this type of firewall by changing the packet headers to satisfy the firewall rules.

Circuit-level Security

- Circuit-level security monitors the connection of sessions between two computers as they communicate over the internet.
- Circuit-level security relies on data contained in the packet headers from the session-layer of the OSI.
- As a general rule:
 - the higher up the OSI layers a firewall is working, the stronger the security.

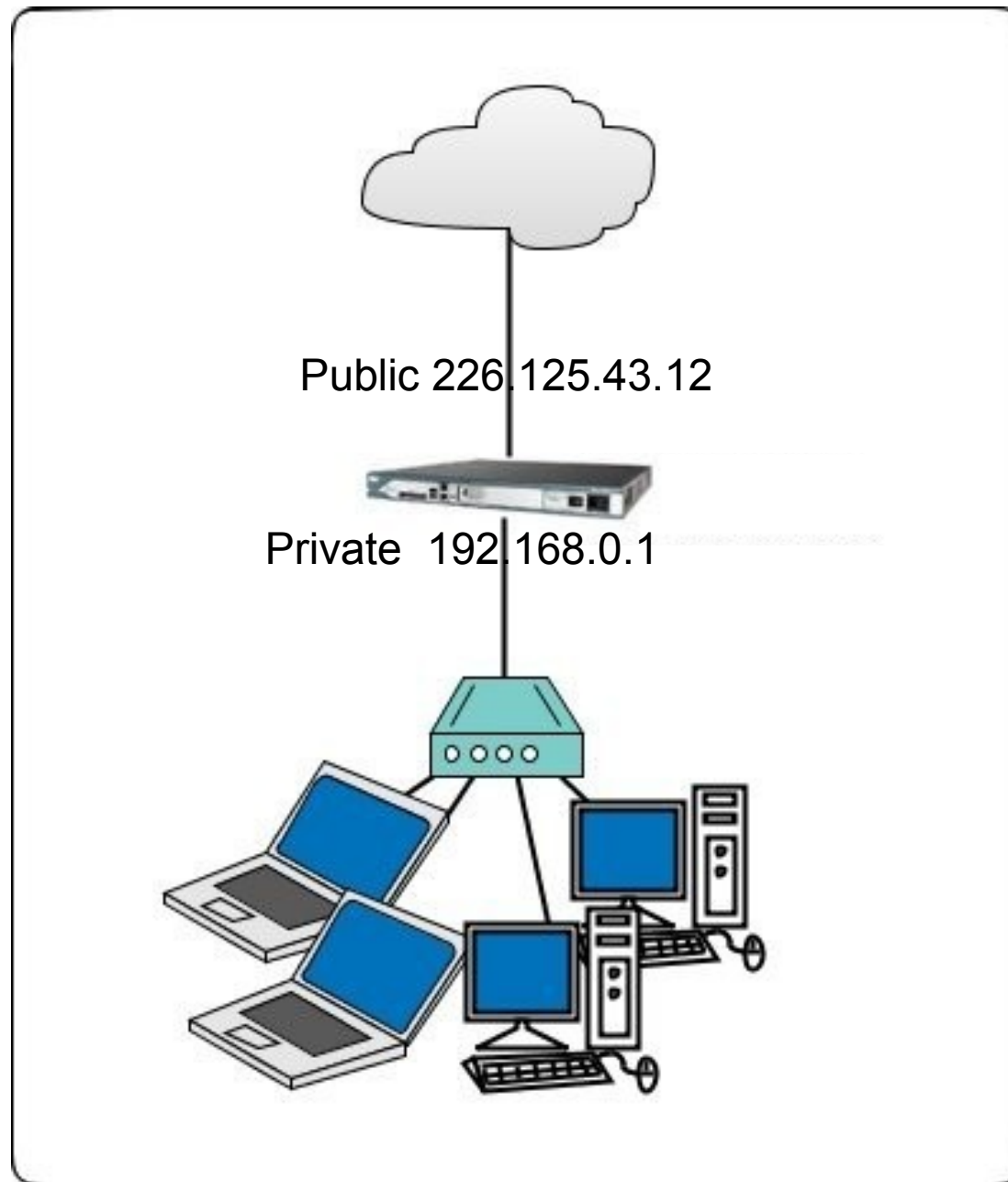
Circuit-level Security

- A computer requests a service, and the firewall accepts this request.
- Acting on behalf of the local computer, the gateway opens a connection to the destination computer and then closely monitors the session.
- It monitors SYN (synchronize) and ACK (acknowledge) messages to and from the destination to make sure they aren't fake.
- It then passes the packets back to the local computer.

Circuit-level Security - NAT

- On a network with a circuit-level security, all outgoing packets appear to have originated from the firewall, preventing direct contact between the trusted network and the untrusted network.
- The IP address of the firewall is the only active IP address and the only IP address that the untrusted network is aware of.
- This is sometimes called Network Address Translation (NAT)
 - * remember about the private IP address range?

NAT – Network Address Translation



Circuit-level Security Vulnerabilities

- Once a session has been checked and is allowed to continue it is possible to pass malicious data to the destination computer.
- Hackers can exploit this vulnerability.
- This is possible because circuit-level security does not inspect the contents of the packets – it just checks that the session is real.

Application-level security

The concept of application-level security is similar to circuit-level security. It is different in the following ways:

- The forwarding of data is application specific.
- It works at the application layer of the OSI (the highest layer!)

Application-level security

- Application-level firewalls check each packet that passes through the gateway, verifying the contents of the packet.
- They can filter particular kinds of commands or information in the application protocols.
- They can restrict specific actions from being performed. (ie. writing to a server using FTP)

Application-level security

- Because application-level security takes the network traffic all the way up the OSI layer it suffers from performance problems.
- Many application-level firewalls require users to log-in to the firewall before they connect to the internet. This means that they are not as user friendly or as transparent (invisible) as other types of firewalls.

Public and Private Parts!

- Many LANs that are connected to other networks contain **private areas** (the internal computers) and **public areas** (web servers, mail servers etc.)
- It is important to secure the private areas but allow appropriate access to the public areas.
- Networks can be designed and configured with appropriately placed firewalls to separate public from private.

Perimeter Networks and DMZs

- A **perimeter network** is a network section that is added between a protected (**private**) network and an external network (ie. Internet).
- The perimeter network provides an additional layer of security.
- Both the private network and the perimeter network are protected by firewalls.
- This is like locking the doors of your house AND putting a fence around the garden with a lock on the gate.

DMZs in History

DMZ = Demilitarized Zone

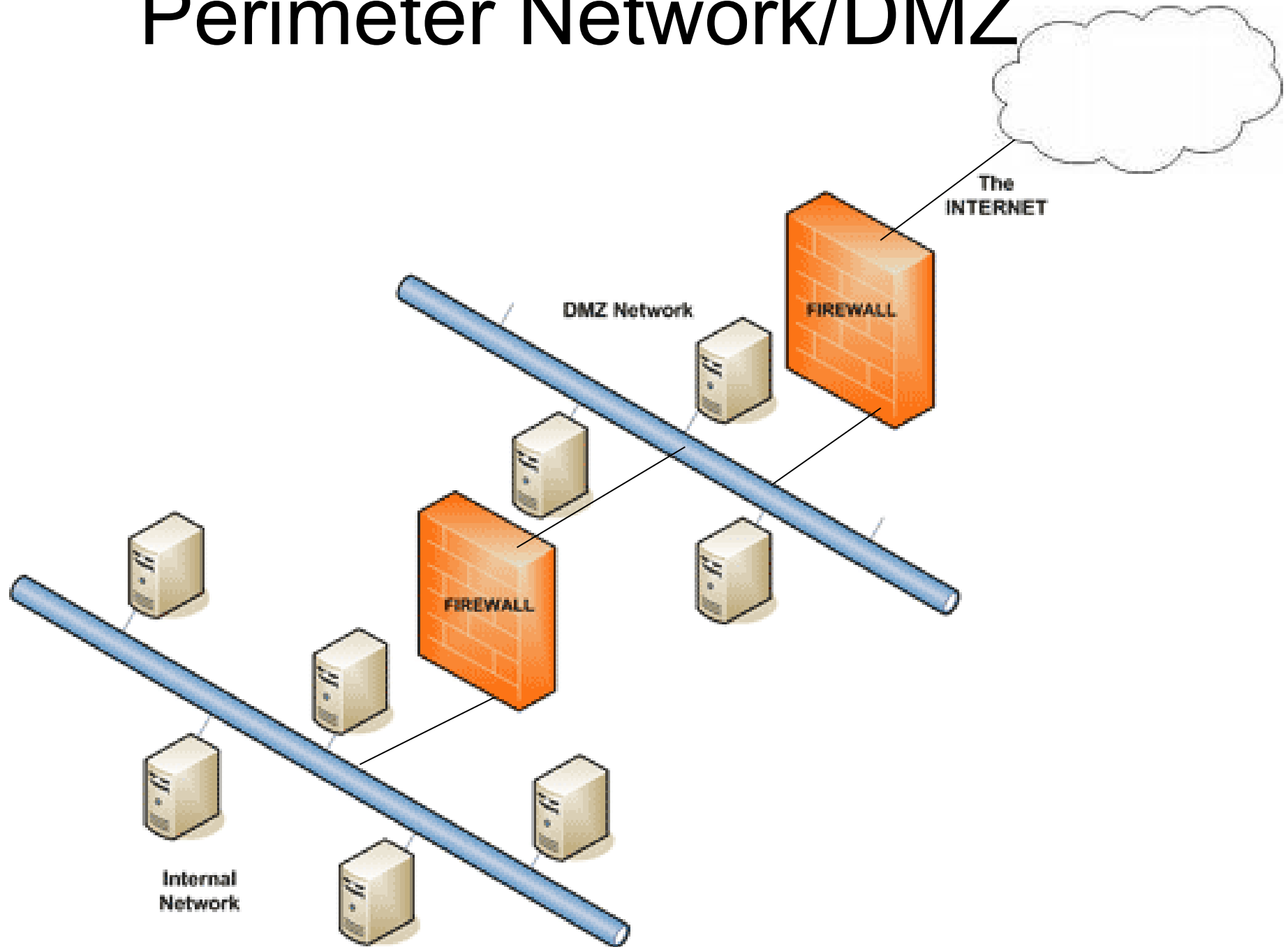
- In 1954 a temporary boundary between North and South Vietnam was set up where no military activity could take place.
- This was a “buffer” zone between two conflicting sides.
- Other DMZs include that between North and South Korea



DMZs in Networking

- A Demilitarized Zone is part of the network that is neither part of the internal network nor directly part of the Internet.
- Basically a DMZ is similar to that which you see in the history books, a zone sitting between two opposing territories.
- The DMZ has public services that belong to the internal network.
- It provides additional levels of security whilst enabling external access to information.

Perimeter Network/DMZ



DMZ with multi-homed firewall

