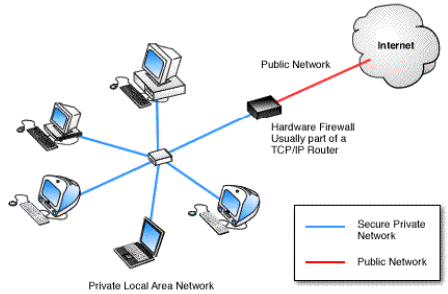
Firewalls

COMP620

Purpose

- A **firewall** is designed to block unauthorized access while permitting authorized communications



Hardware or Software

- Computers may have firewall software which filters network traffic to and from that computer.
- Firewalls can be built into network routers. These are often placed between the local network and the Internet.
- Separate firewall boxes are available to filter the traffic.

Types of Firewall Techniques

- Packet filter – Network layer
- Circuit-level gateway – Transport layer
- Application gateway – Application layer
- NAT or Proxy server

Packet Filtering

- A simple firewall is a packet filter. It only allows packets to pass through the firewall if they meet a specified criteria.
- Firewalls need to be configured to define what network traffic is desired and what should be prohibited.

Filter Criteria

Firewalls can filter network traffic based on several criteria.

- **Source address** – The IP address of the computer sending the packet. *This can be forged.*
- **Destination address** – The IP address of the computer to receive the packet.
- **Port number** – The UDP or TCP port of the destination.
- **Protocol** – The network protocol used.

Application Filtering

- Applies security mechanisms to specific applications, such as FTP and Telnet
- Can be very effective, but can impose a performance degradation
- Modern application firewalls may also offload encryption from servers

Circuit-Level Firewalls

- Applies security mechanisms when a TCP connection is established
- Once the connection has been made, packets can flow between the hosts without further checking
- More efficient since checks are only made during connections
- Not applicable to UDP

Stateless Filtering

- Firewall filtering can be stateless or state full.
- Stateless filtering analyzes each packet based only on the information in the packet.
- More sophisticated firewalls analyze traffic streams. Packets replying to locally originating connections are allowed.

Configuration

- Typically a firewall needs to be configured to define what you want to prevent or allow
- A new application may require access to the Internet in a manner that was previously denied
- There is a wide range of firewall configuration interfaces

Perimeter Protection

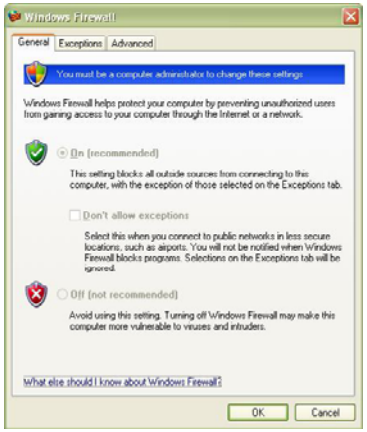
- Firewalls typically block traffic as it enters or leaves the network.
- Attacks from within the local network are not filtered by a router firewall.

DMZ

- An intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a “perimeter network” or demilitarized zone (DMZ)
- A public web server might be located in the DMZ. You have to allow public access although you may want to restrict the type of access

Microsoft Windows Firewall

- The firewall can be accessed from the control panel.
- You must be an administrator.
- You can allow or prohibit specific network traffic.



How do you know a bad packet when you see one?

- It is often difficult to characterize an evil packet.
- Many firewall systems block everything unless there is a known need for a specific traffic type.
- Denial of service flooding attacks typically send a large number of “valid” packets.

Email Filtering

- Email filters attempt to remove malicious email and spam
- More than 97% of all emails sent over the net are unwanted
- As of June 2007 there were 100 billion spam emails sent per day