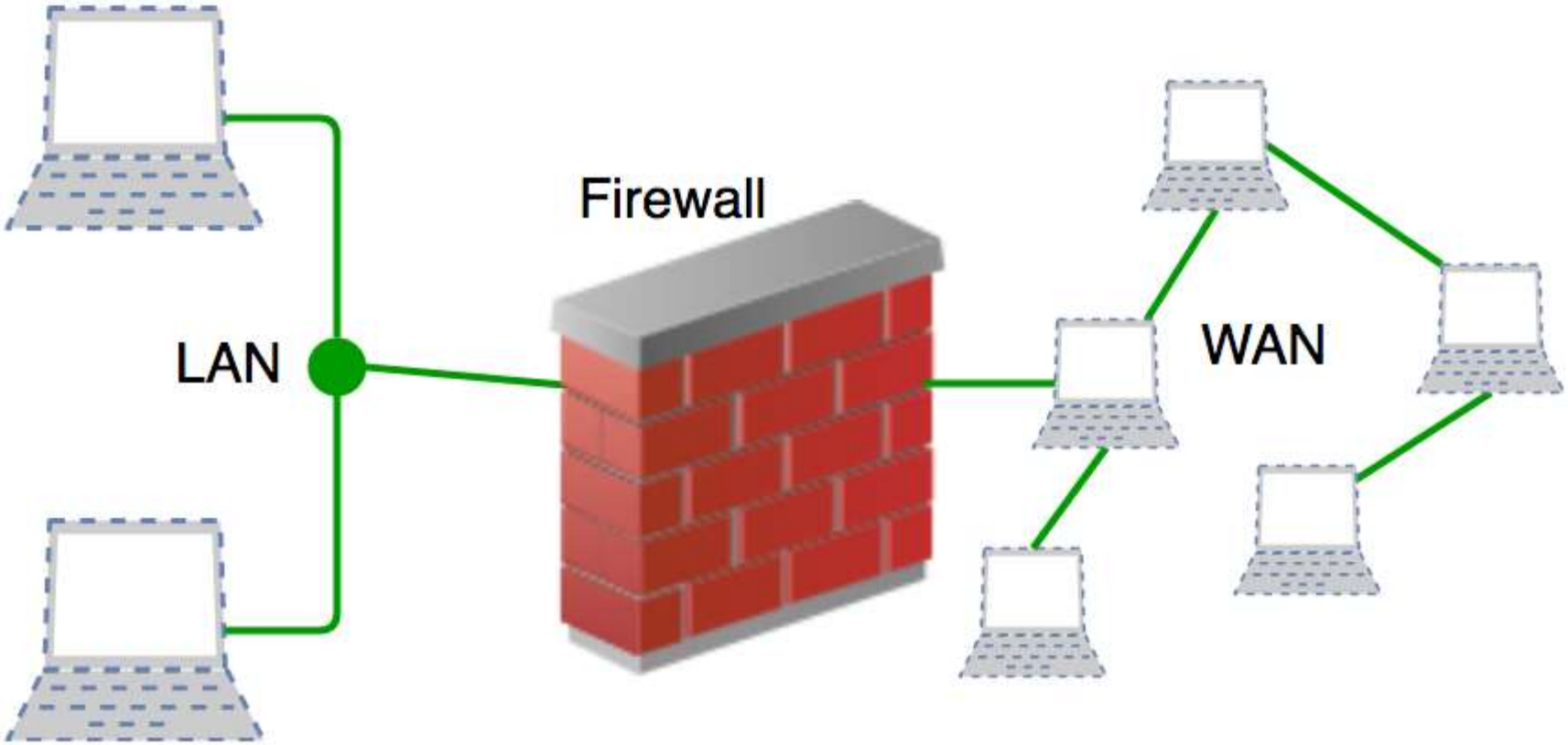
Overview of Firewalls

- As the name implies, a firewall acts to provide secured access between two networks
- A firewall may be implemented as a standalone hardware device or in the form of a software on a client computer or a proxy server
  - The two types of firewall are generally known as the hardware firewall and the software firewall

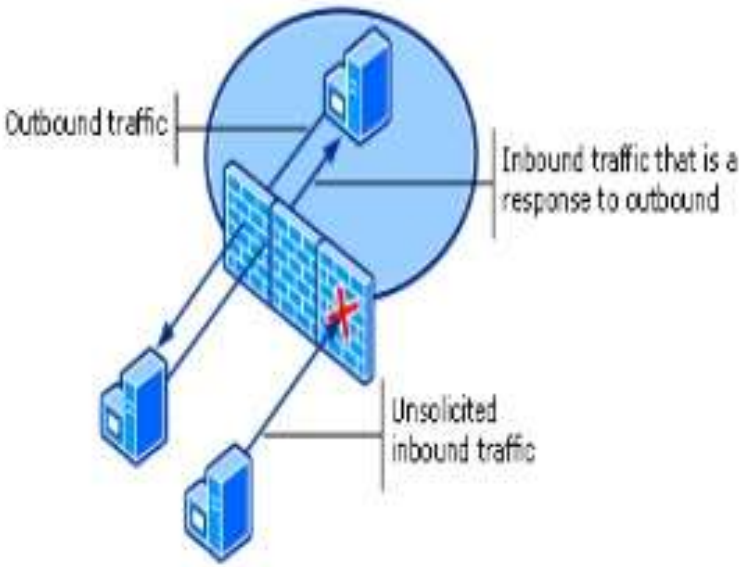

Firewall
LAN
WAN

Firewalls in Practice

A computer may be protected by both a hardware and a software firewall.

Mode of Operation

A firewall that stands in between two networks will inspect a packet that is ready to pass between the networks and allow or block the packet based on the rules set for the firewall to operate.



General Firewall Features

- Port Control
- Network Address Translation
- Application Monitoring (Program Control)
- Packet Filtering

Additional Firewall Features

- Data encryption
- Hiding presence
- Reporting/logging
- e-mail virus protection
- Pop-up ad blocking
- Cookie digestion
- Spy ware protection etc.

Viruses and Firewalls

- In general, firewalls cannot protect against viruses
  - An anti-virus software is needed for that purpose
- However, many security suites such as those offered by MacAfee and Norton offer the complete protection.
- Some software firewalls such as Zone Alarm Pro may contain limited virus protection features.

Firewall Layer of Operation

- Network Layer
- Application Layer

Network Layer

- Makes decision based on the source, destination addresses, and ports in individual IP packets.
- Based on routers
- Has the ability to perform static and dynamic packet filtering and stateful inspection.

Static & Dynamic Filtering

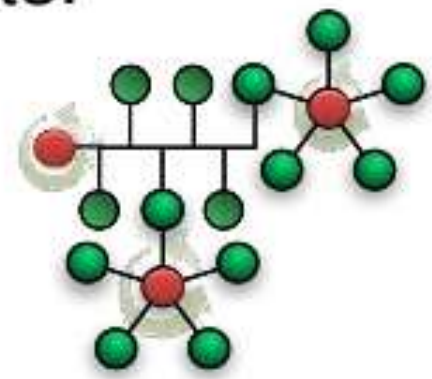
- Static Packet Filtering looks at minimal information in the packets to allow or block traffic between specific service ports
  - Offers little protection.
- Dynamic Packet Filtering maintains a connection table in order to monitor requests and replies.

Stateful Inspection

- Compares certain key parts of the packet to a database of trusted information. Incoming information is compared to outgoing information characteristics. Information is allowed through only If comparison yields a reasonable match.

Application Layer

- They are generally, hosts running proxy servers which perform logging and auditing of traffic through the network.
- Logging and access control are done through software components.



Proxy Services

- Application that mediates traffic between a protected network and the internet.
- Able to understand the application protocol being utilized and implement protocol specific security.
- Application protocols include: FTP, HTTP, Telnet etc.

Port Scans

- When hackers remotely spy on your computers to see what software and services they have.
- Port scans are common but with a properly configured and maintained firewall you can restrict access.

DMZ

- Demilitarized zone
- Neither part of the internal network nor part of the Internet
- Never offer attackers more to work with than is absolutely necessary

Hardware Firewall (Cont.)

What is it?

- It is just a software firewall running on a dedicated piece of hardware or specialized device.
- Basically, it is a barrier to keep destructive forces away from your property.
- You can use a firewall to protect your home network and family from offensive Web sites and potential hackers.

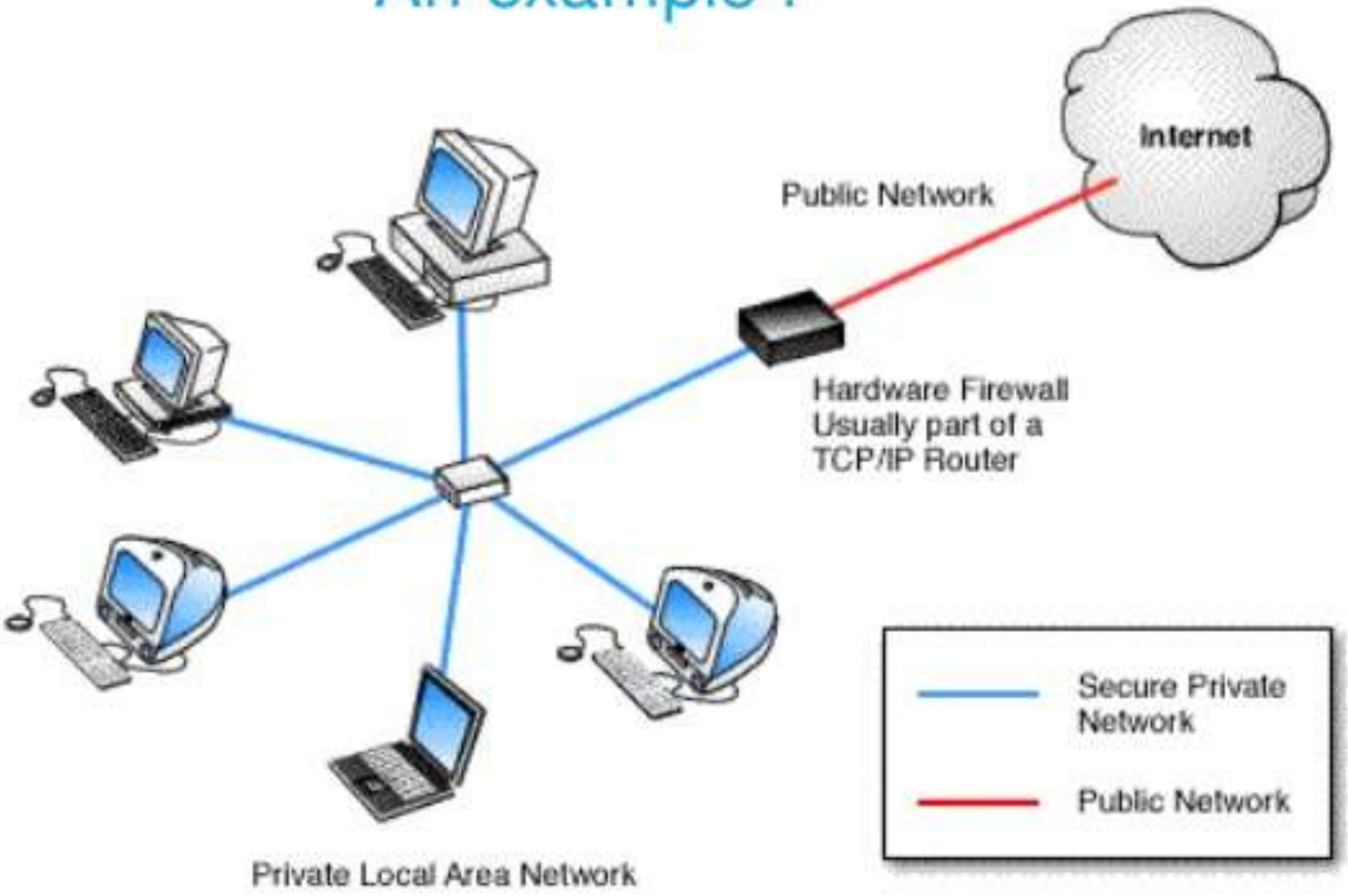
Hardware Firewall (Cont.)

What it does !

- It is a hardware device that filters the information coming through the Internet connection into your private network or computer system.
- An incoming packet of information is flagged by the filters, it is not allowed through.

Hardware Firewall (Cont.)

An example !



Hardware Firewall (Cont.)

Firewalls Use

- Firewalls use one or more of three methods to control traffic flowing in and out of the network:
  - Packet filtering
  - Proxy service
  - State-full inspection

Hardware Firewall (Cont.)

- Packet filtering - Packets are analyzed against a set of filters.
- Proxy service - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.
- State-full inspection – It compares certain key parts of the packet to a database of trusted information. Information traveling from inside to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics.

Hardware Firewall (Cont.)

- What it protects you from:
  - Remote logins
  - Application backdoors
  - SMTP session hijacking
  - E-mail Addresses
  - Spam
  - Denial of service
  - E-mail bombs
    - E-mail sent 1000's of times till mailbox is full
    - Macros
    - Viruses

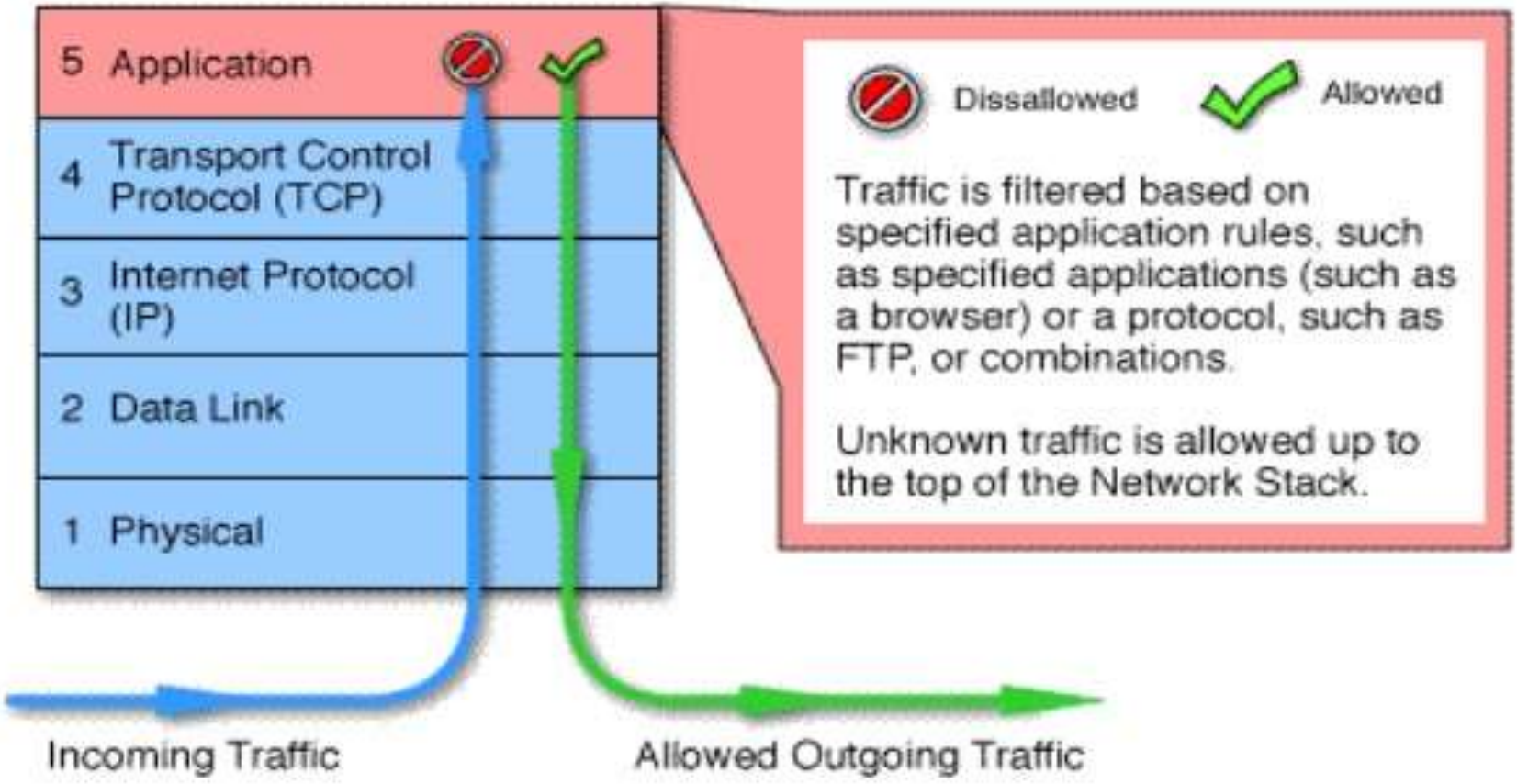
Software Firewall

What it is?

- Also called Application Level Firewalls
- It is firewall that operate at the Application Layer of the OSI
- They filter packets at the network layer
- It Operating between the Datalink Layer and the Network Layer
- It monitor the communication type (TCP, UDP, ICMP, etc.) as well as the origination of the packet, destination port of the packet, and application (program) the packet is coming from or headed to.

Software Firewall (Cont.)

How does software firewall works ?



Software Firewall (Cont.)

Benefit of using application firewalls

- allow direct connection between client and host
- ability to report to intrusion detection software
- equipped with a certain level of logic
- Make intelligent decisions
- configured to check for a known Vulnerability
- large amount of logging

Software Firewall (Cont.)

Benefit of application firewalls (Cont.)

- easier to track when a potential vulnerability happens
- protect against new vulnerabilities before they are found and exploited
- ability to "understand" applications specific information structure
- Incoming or outgoing packets cannot access services for which there is no proxy

Software Firewall (Cont.)

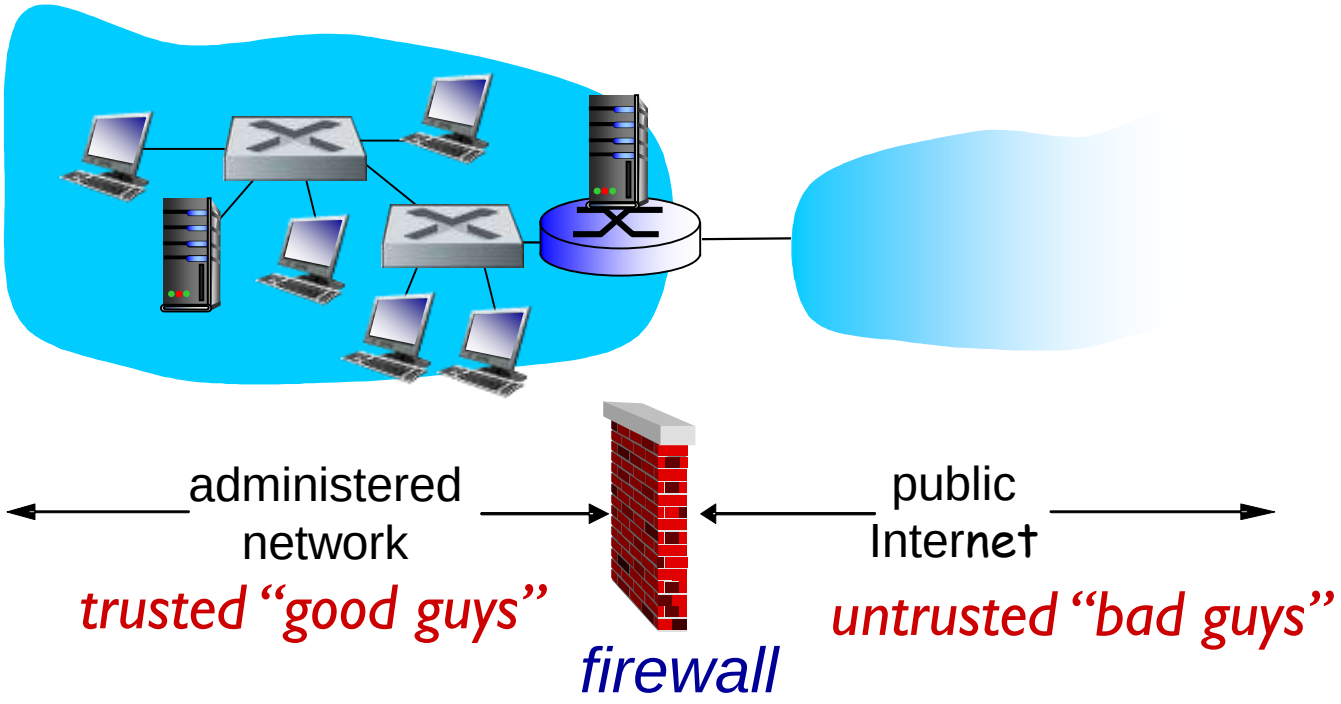
Disadvantage of Firewall:

- slow down network access dramatically
- more susceptible to distributed denial of service (DDOS) attacks.
- not transparent to end users
- require manual configuration of each client computer

Firewalls

firewall

Isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others



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

allow only authorized access to inside network

- set of authenticated users/hosts

three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

Generation of Firewall

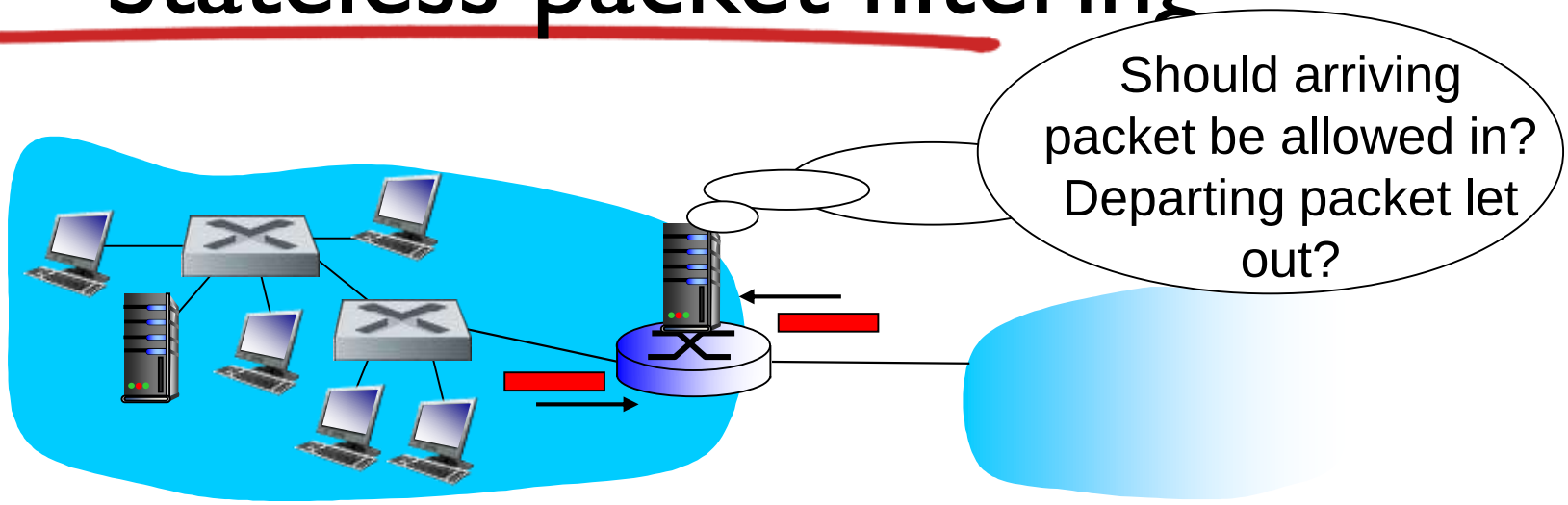
- **First Generation- Packet Filtering Firewall :** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers).
  Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.

- **Second Generation- Stateful Inspection Firewall :** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

- **Third Generation- Application Layer Firewall : ** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.
  In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.

- **Next Generation Firewalls (NGFW) :** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

Stateless packet filtering



- internal network connected to Internet via *router firewall*
- router *filters packet-by-packet,* decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

Stateless packet filtering: example

- *example 1:* block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23
  - *result:* all incoming, outgoing UDP flows and telnet connections are blocked
- *example 2:* block inbound TCP segments with ACK=0.
  - *result:* prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Stateless packet filtering: more examples

Policy	*Firewall Setting*
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80

Stateful Packet Filters

- In a traditional packet filter, filtering decisions are made on each packet in isolation.

- Stateful filters actually track TCP connections, and use this knowledge to make filtering decisions.

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

Application gateways

- The packet-level filtering allows an organization to perform coarse-grain filtering on the basis of the contents of IP and TCP/UDP headers, including IP addresses, port numbers, and acknowledgment bits.

- But what if an organization wants to provide a Telnet service to a restricted set of internal users (as opposed to IP addresses)?

Application gateways

- Application gateways look beyond the IP/TCP/UDP headers and make policy decisions based on application data.

- An **application gateway is an** application-specific server through which all application data (inbound and outbound) must pass.

- Multiple application gateways can run on the same host, but each gateway is a separate server with its own processes.

Application gateways

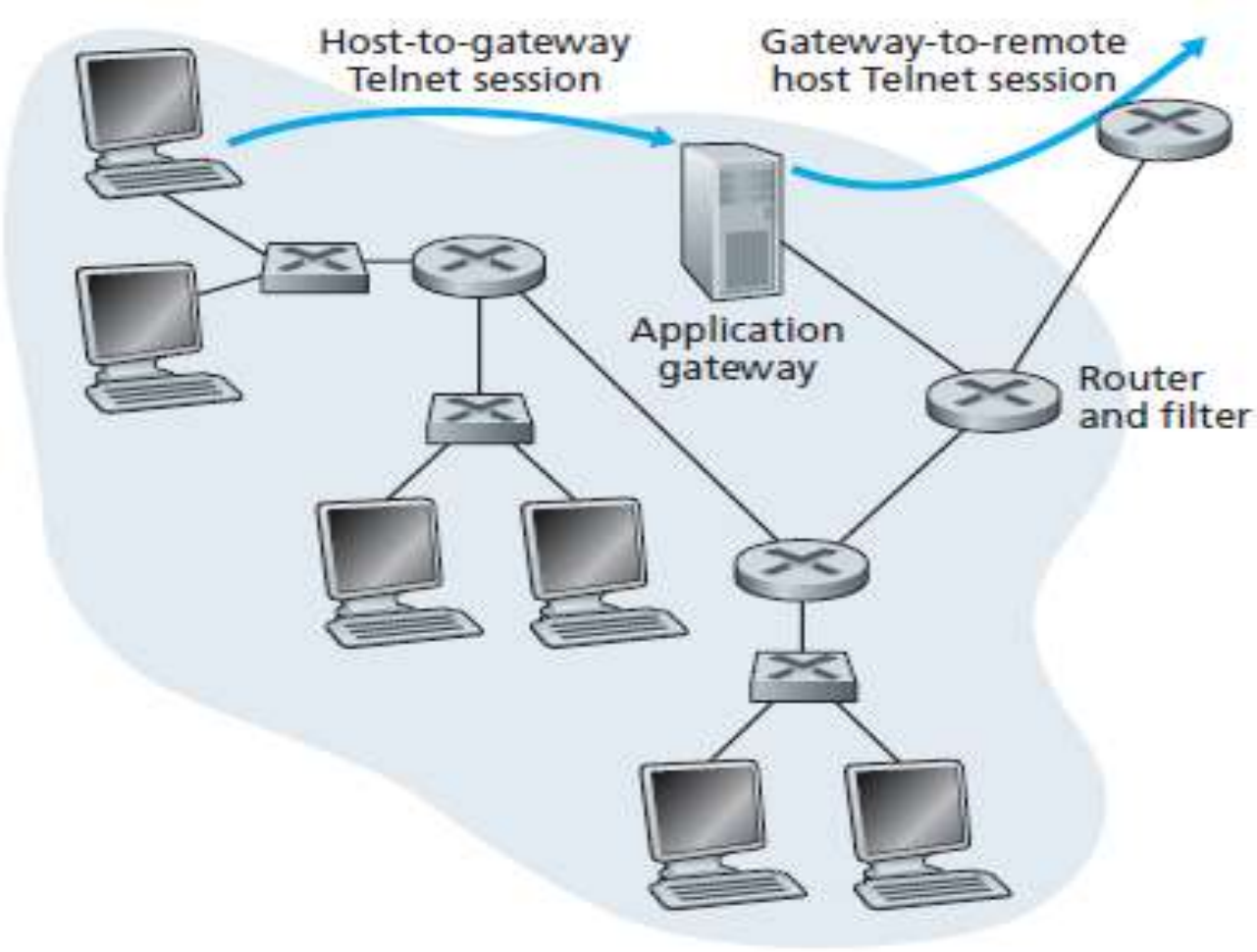


Figure 8.34 ♦ Firewall consisting of an application gateway and a filter

Application gateways

- Filters packets on application data as well as on IP/TCP/UDP fields.
- *Example:* allow selected internal users to telnet outside.
- implementing a combination of a packet filter (in a router) and a Telnet application gateway,

1. Require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.

Limitations of firewalls, gateways

- *IP spoofing:* router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser

Types of Firewall

- Firewalls are generally of two types: *Host-based* and *Network-based.*
- **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

- **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.