CS 126:

INTRODUCTION TO IT SECURITY

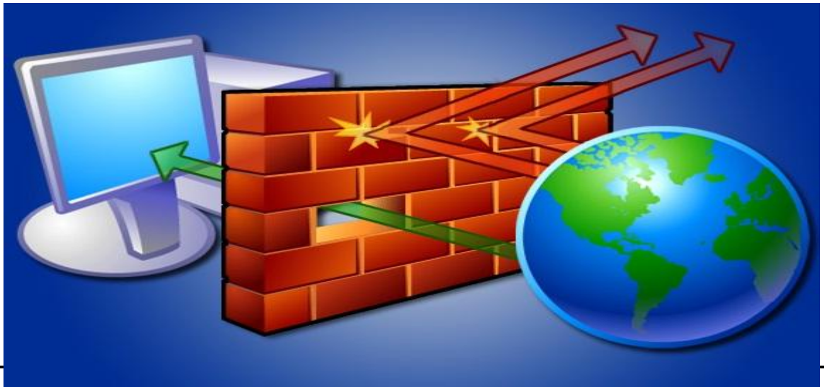
FIREWALLS

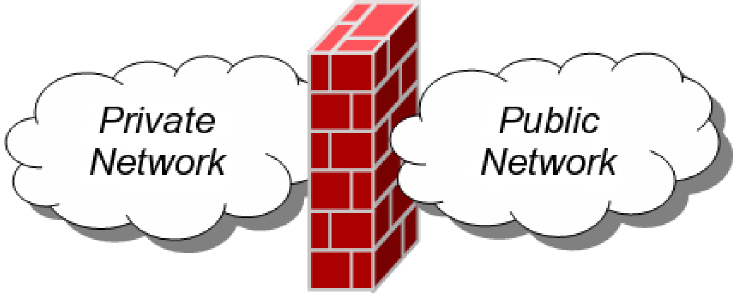
Lecture: 08

Useful **“First Line”** of defense - commonly deployed on routers

WHAT IS A FIREWALLS

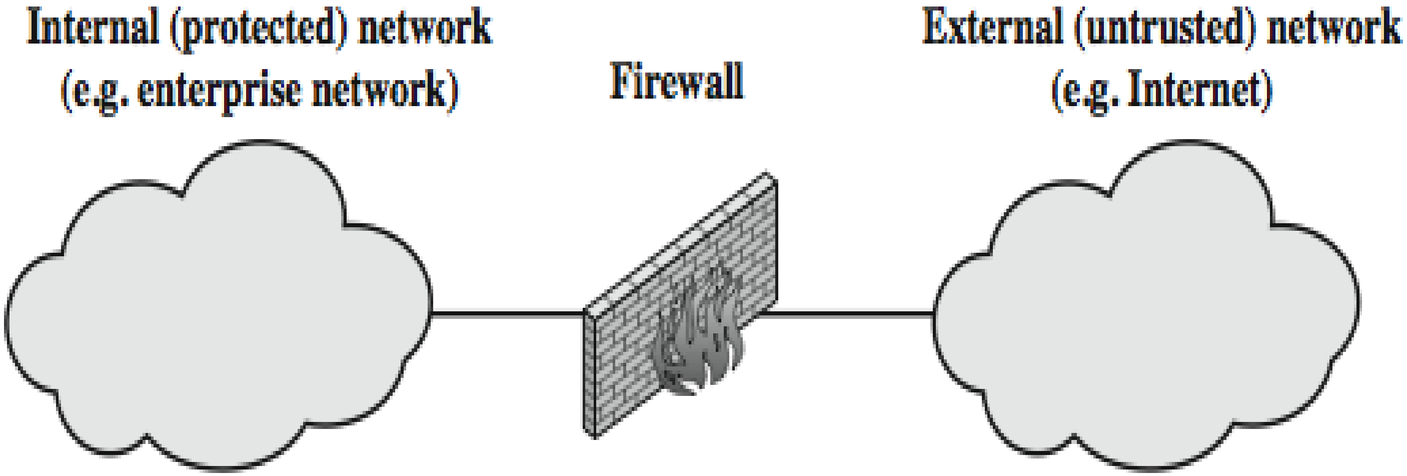
- A firewall is software or hardware that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to your computer, depending on your firewall settings.
- Is defines a single **choke point** of control and monitoring that keeps unauthorized users out of the protected network.
- Isolates organization's internal network from larger Internet, allowing some packets to pass, blocking others.





WHAT IS A FIREWALLS

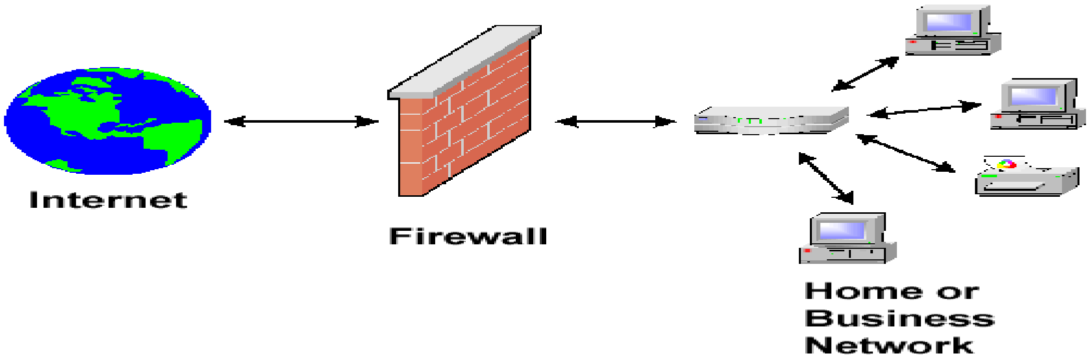
- **A Network Firewall** is a system or group of systems used to control access between two networks; a trusted network and an untrusted network using pre-configured rules or filters.


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)

The firewall can permit, deny, or redirect the flow of data.

FIREWALLS

- **For a firewall to function effectively:**
  - ✓ All traffic between the internal and external networks must flow through the firewall- this gives us a single point of control
  - ✓ It must be properly configured, managed, and audited.
- Used to implement and enforce a security policy for communication between networks
- The earliest firewalls were simply routers.



FIREWALL DESIGN PRINCIPLES

- The firewall is inserted between the premises network and the Internet
- **Aims:**
  - ✓Establish a controlled link
  - ✓Protect the premises network from Internet-based attacks
  - ✓Provide a single check point that simplifies security management (keeps unauthorized users out of protected network).

FIREWALL IMPLEMENTATIONS

- It may be a **hardware device** or a **software program** running on a secure host computer.
- In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to.

Hardware (network devices)

- ✓ Protect an entire network
- ✓ Implemented on the router level
- ✓ Usually more expensive, harder to configure
- ✓ **Examples**: Cisco PIX, Sonicwall, Watchguard Firebox

Software (applications)

- Protect a single computer
- Usually less expensive, easier to configure

Examples: Windows: ZoneAlarm, Norton Personal Firewall, BlackICE; **Unix and variants:** ipfw, ipchains, iptables, ipf

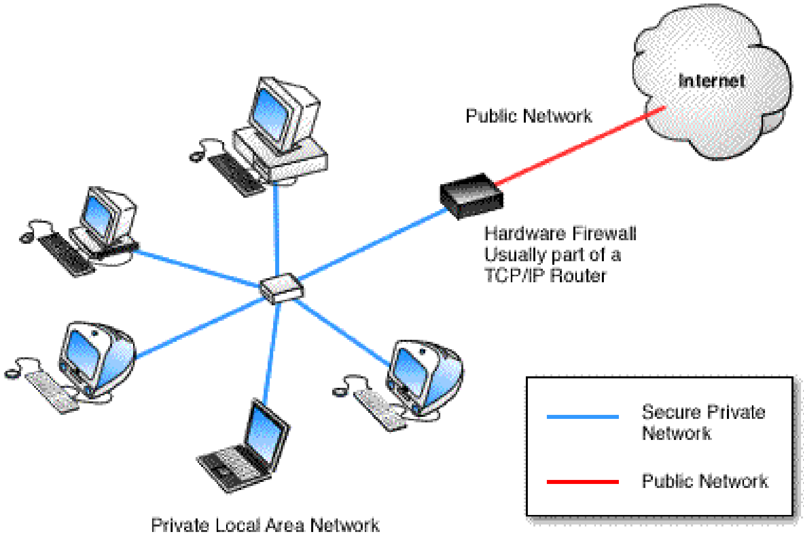
FIREWALL IMPLEMENTATIONS

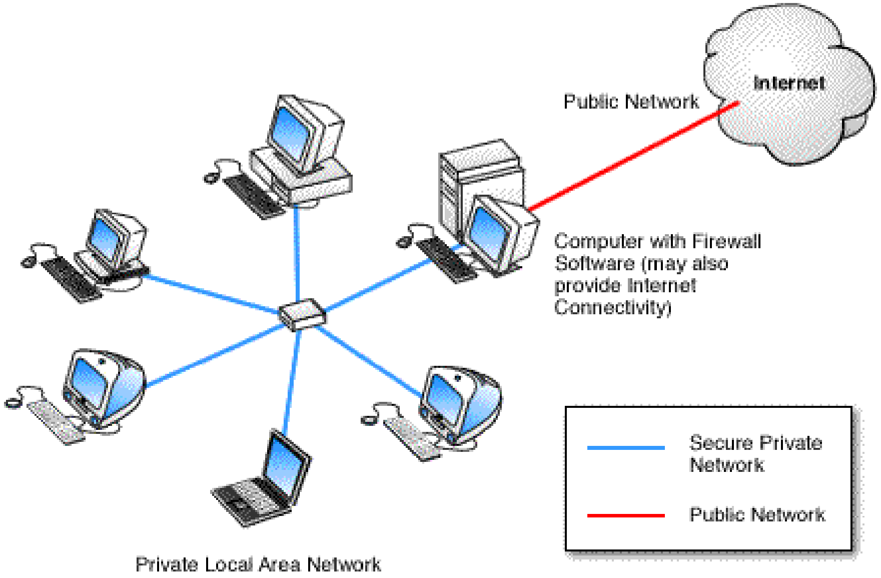
Hardware Firewall.

- Hardware firewall providing protection to a Local Network.

Computer with Software Firewall.

- Computer running firewall software to provide protection





WHY FIREWALLS?

- **Internet connectivity** is no longer an option for most corporations

The Internet allows you access to worldwide resources, but……the Internet also allows the *WORLD* to try and access your resources

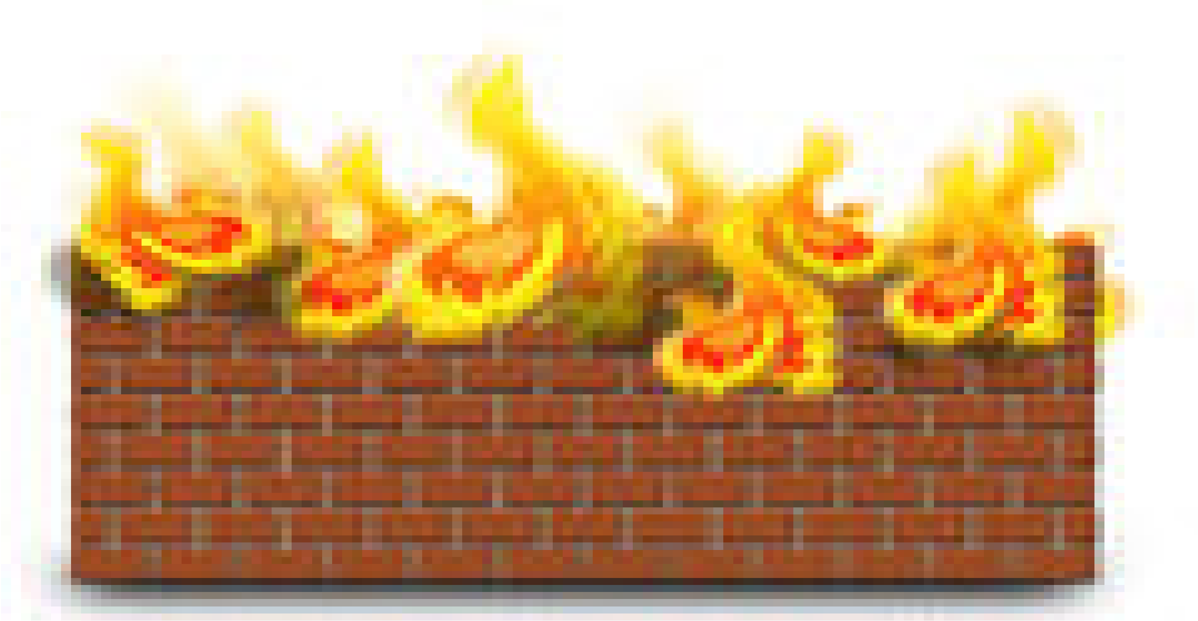
- ✓ This is a **grave risk** to most organizations

- **Firewall:** Establishes a **perimeter** and provides a **choke point** where security and audits can be imposed

Therefore

- ✓ Prevent attacks from untrusted networks
- ✓ Protect data integrity of critical information
- ✓ Preserve customer and partner confidence

WHO NEEDS A FIREWALL?



WHO NEEDS A FIREWALL?

- Anyone who is responsible for a **private network** that is connected to a **public network** needs firewall protection.
- Furthermore, anyone who connects so much as a **single computer** to the **Internet** via modem should have personal firewall software.

SCOPE OF FIREWALLS

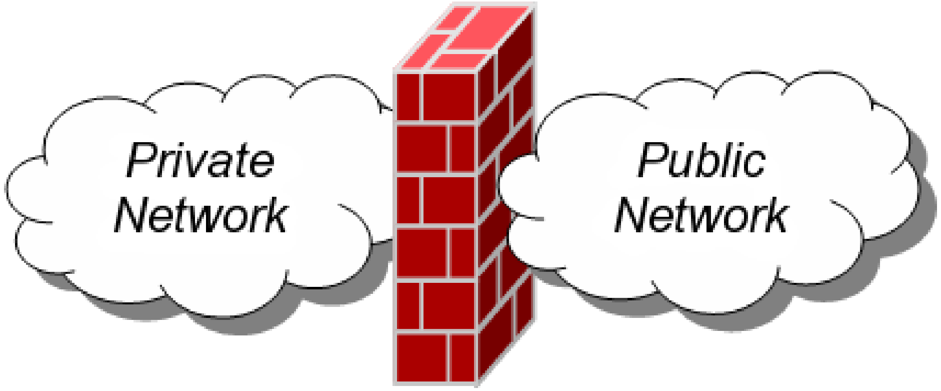
- **Single choke point:** To protect vulnerable services from various kinds of attack (spoofing, DOS)
- **Singular monitoring point:** Location for monitoring, auditing and event triggering
- **Platform for non-security functions** – can be used for network address translation and network management
- **Platform for IPSec** – implements VPN via tunnel mode

FIREWALL LIMITATIONS

- **The firewall cannot protect against attacks that bypass the firewall - bypass attack**
  - ✓Individual users with modems dialling into or out of the network, bypassing the firewall altogether.
- **The firewall does not protect against internal threats**
  - ✓Employee misconduct or carelessness cannot be controlled by firewalls.
  - ✓Policies involving the use and misuse of passwords and user accounts must be strictly enforced.
- **The firewall cannot protect against the transfer of virus - infected programs or files**

FIREWALL DESIGN PRINCIPLES

1. Firewall **characteristics**
2. **Types** of firewall
3. Firewall **configuration**



1. FIREWALL CHARACTERISTICS

Design goals:

- **All traffic** from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
- Only **authorized traffic** (defined by the local security police) will be allowed to pass
- The firewall itself is **immune to penetration** (use of trusted system with a secure operating system)

Access Control Techniques: Four general techniques:

- **Service control:** Determines the types of Internet services that can be accessed, inbound or outbound
- **Direction control:** Determines the direction in which particular service requests are allowed to flow
- **User control:** Controls access to a service according to which user is attempting to access it
- **Behavior control:** Controls how particular services are used (e.g. filter e-mail)

2. TYPES OF FIREWALLS

Three common types of Firewalls

1. **Packet Filtering** Router
2. **Circuit Level** Gateway
3. **Application Level** Gateway
4. **Stateful multilayer** inspection firewalls.

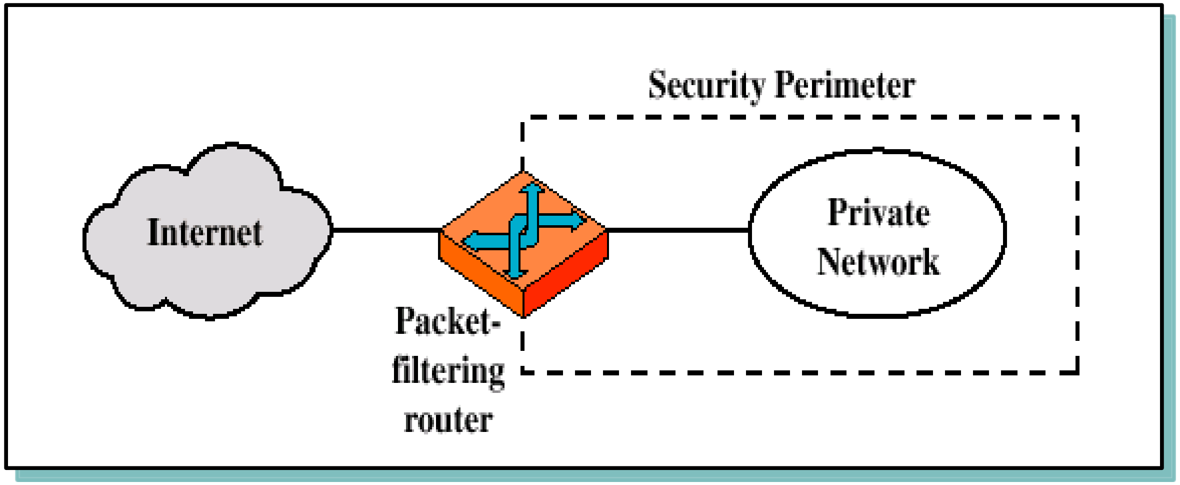
2. TYPES OF FIREWALLS

Packet-filtering Router

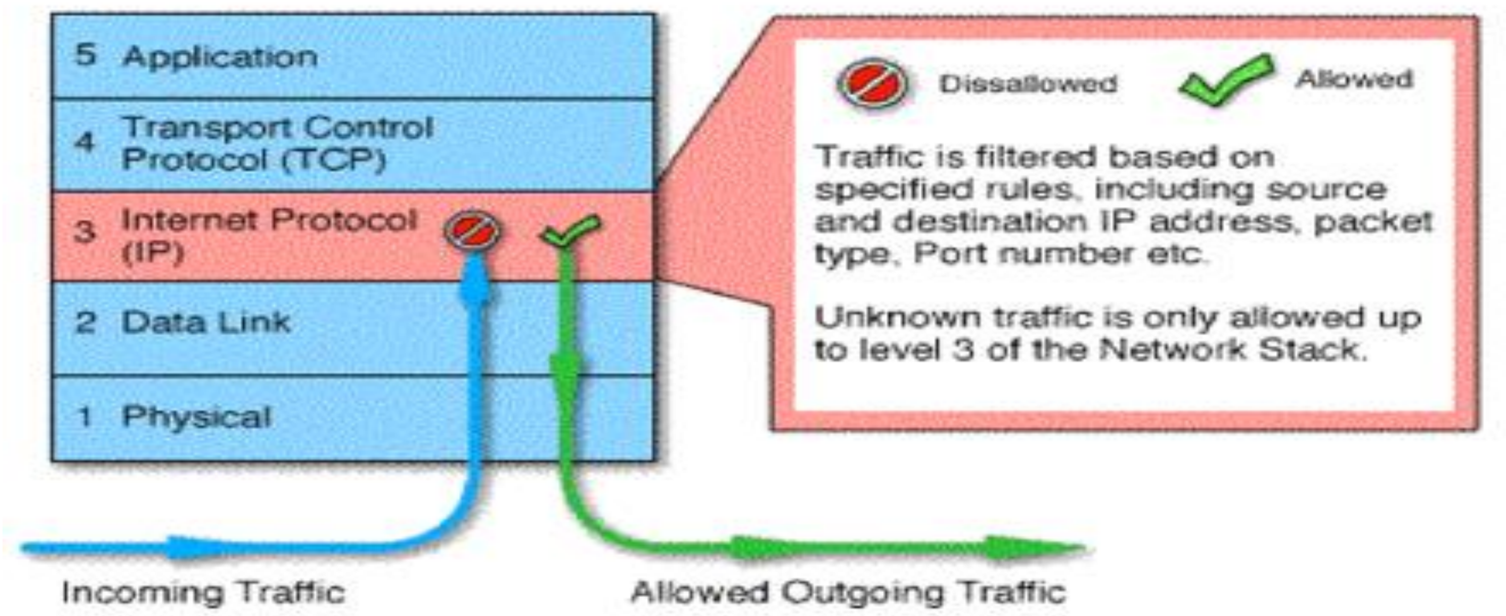
- Simple accept or reject decision model
- **Applies a set** of rules to each incoming IP packet and then **forwards** or **discards** the packet
- Filter packets going in **both directions**
- The packet filter is typically set up as a list of **rules**
- Rules based on **source** and **destination** address and **port** number (fields in the IP or TCP header)
- **List of rules** looking for a match
- If no match, ***default*** action is taken
  - ✓ Two default access denial policies (**discard** or **forward**)
    - ❑ **Default = Discard:** *That which is not expressly permitted is **prohibited***
    - ❑ **Default = Forward:** *That which is not expressly prohibited is **permitted***

PACKET FILTERING ROUTER

- Packets examined at the network layer of the OSI model, or the IP layer of TCP/IP
- **Address Filtering:** Firewalls can filter packets based on their source and destination addresses and port numbers.
- **Protocol Filtering:** Firewalls can filter specific types of network traffic. The decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, FTP or telnet.

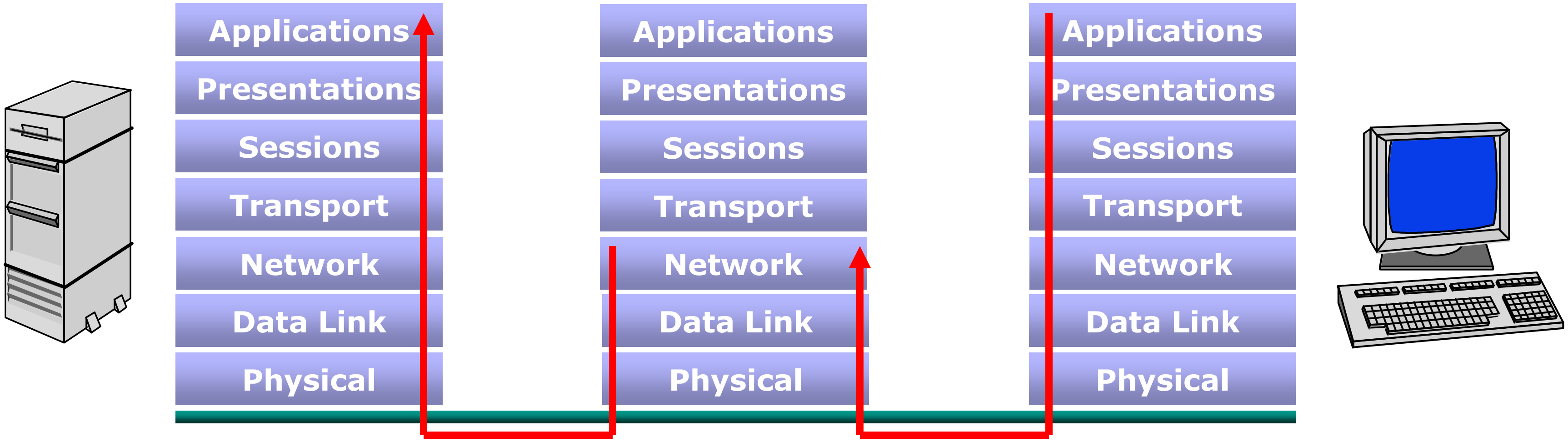


2. TYPES OF FIREWALLS



Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.

Unknown traffic is only allowed up to level 3 of the Network Stack.



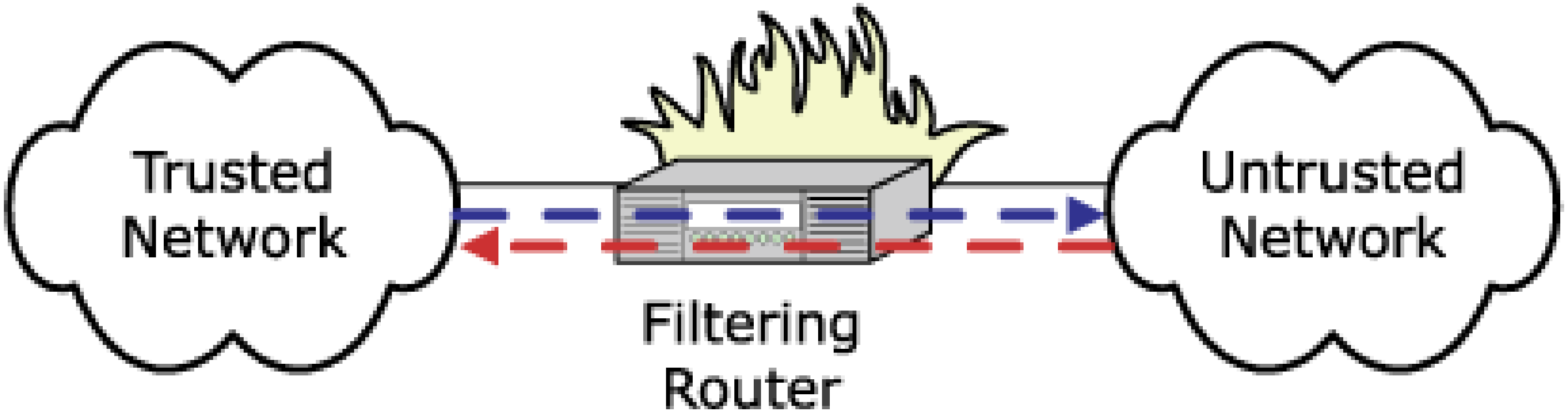
PACKET-FILTERING ROUTER

Advantages:

- Simplicity
- Transparency to users
- High speed

Disadvantages:

- Difficulty of setting up packet filter rules
- Lack of Authentication



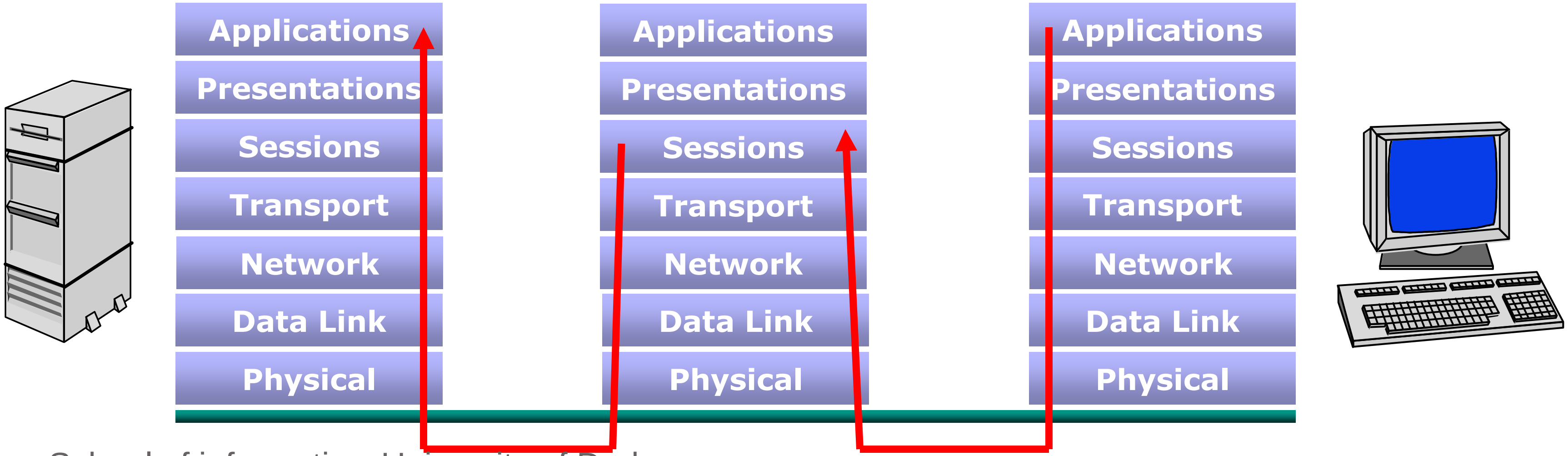
POSSIBLE ATTACKS AND APPROPRIATE COUNTERMEASURES

- **IP address spoofing:** Fake source address **-** *authenticate*
  - Packets from the outside have internal addresses in their source IP address field**:** *discard packet with an inside source address if the packets arrives on an external interface*
- **Source routing attacks:** Attacker sets a route other than default - *block source routed packets*
  - Route of packet is specified to bypass security measures**:** *discard all packets*
- **Tiny fragment attacks:** Split header info over several tiny packets **-** *either discard or reassemble before check*
  - Designed to circumvent filtering rules that depend on TCP header information**:** *discard all subsequent fragments*

2. TYPES OF FIREWALLS

Circuit-Level Gateway

- Stand-alone system or Specialized function performed by an Application-level Gateway
- Circuit level gateways work at the **session layer of the OSI model**, or the **Transport/TCP layer of TCP/IP**
- Monitor TCP handshaking between packets to determine whether a requested session is legitimate.



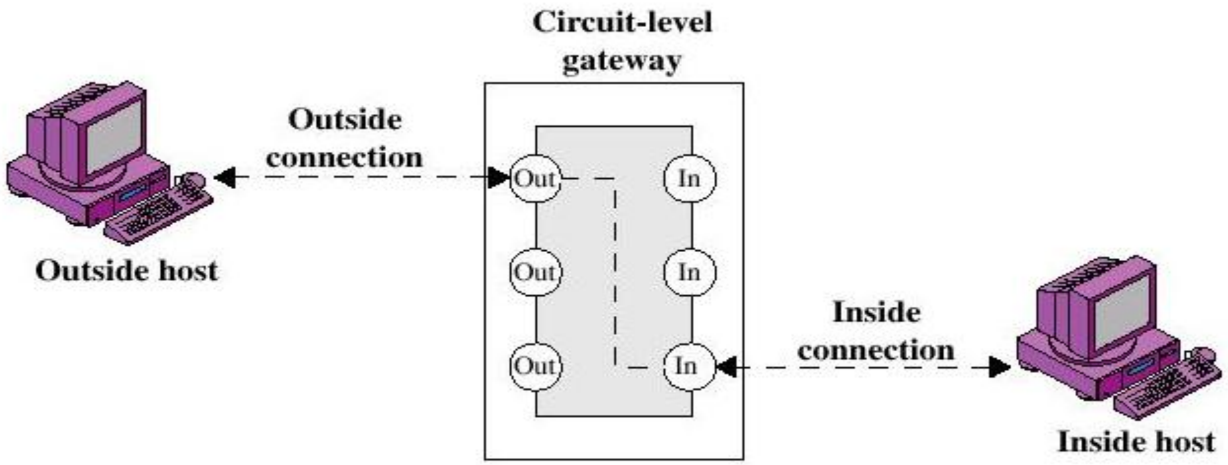
Applications
Presentations
Sessions
Transport
Network
Data Link
Physical

Applications
Presentations
Sessions
Transport
Network
Data Link
Physical

Applications
Presentations
Sessions
Transport
Network
Data Link
Physical

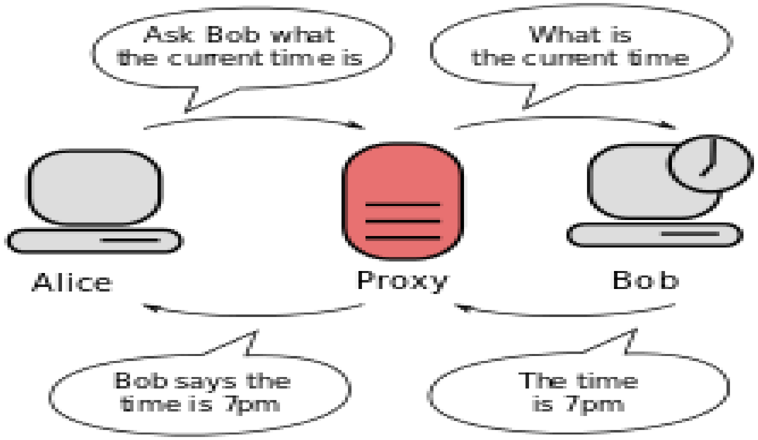
CIRCUIT LEVEL GATEWAY

- Unlike a packet filtering firewall, a circuit-level gateway does not examine individual packets. Instead, circuit-level gateways monitor TCP or UDP sessions.
- Once a session has been established, it leaves the port open to allow all other packets belonging to that session to pass. The port is closed when the session is terminated.
- ***Security function*** (implements policy) determines which connections will be allowed
- Typically use is a situation in which the system administrator **trusts the internal users** for all outbound services



CIRCUIT LEVEL GATEWAY

- Often *combined with a proxy* for inbound services
  - ✓ **proxy server** is a **server** (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other **servers**.

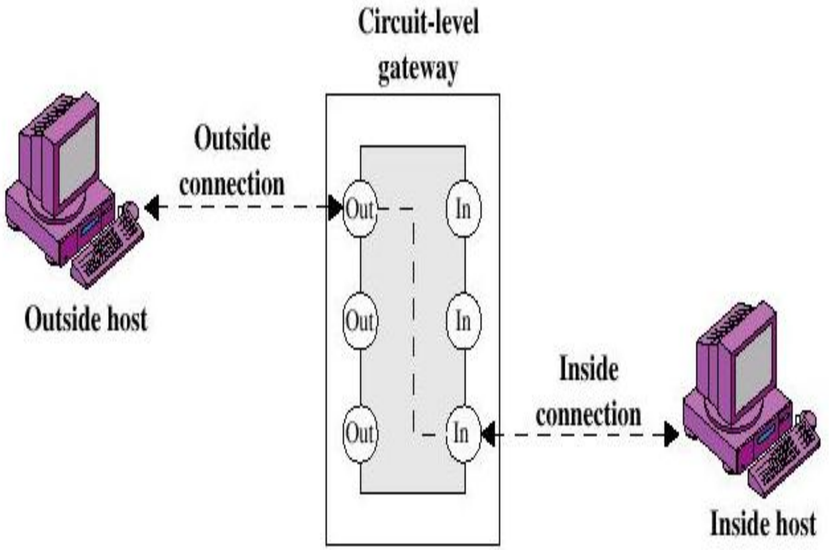


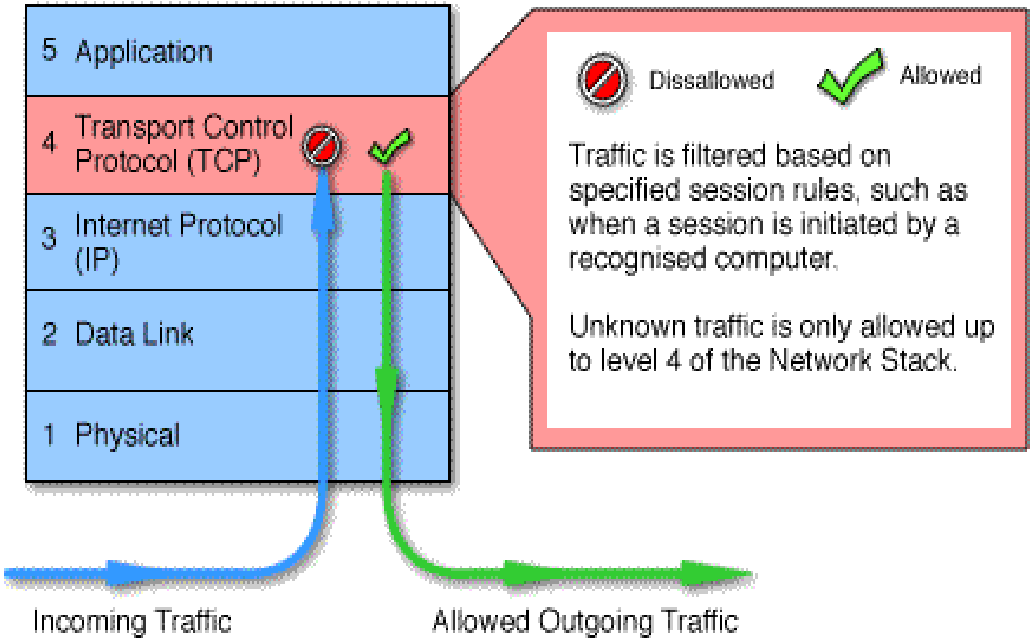
✓ An example is the SOCKS package: **Socket Secure** (**SOCKS**) is an Internet protocol that exchanges network packets between a **client** and **server** through a **proxy server**.

- Information passed through a circuit level gateway, to the internet, appears to have come from the circuit level gateway. So, there is no way for a remote computer or a host to determine the internal private IP addresses of an organization

CIRCUIT LEVEL GATEWAY

- Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect.
- On the other hand, they do not filter individual packets.





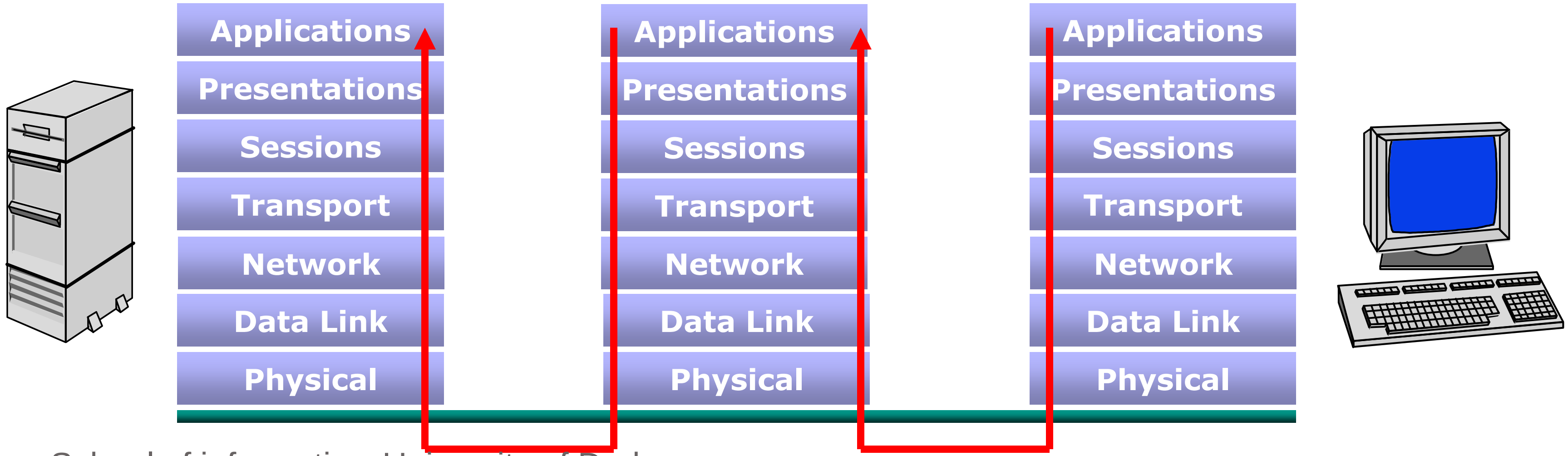
Traffic is filtered based on specified session rules, such as when a session is initiated by a recognised computer.

Unknown traffic is only allowed up to level 4 of the Network Stack.

2. TYPES OF FIREWALLS

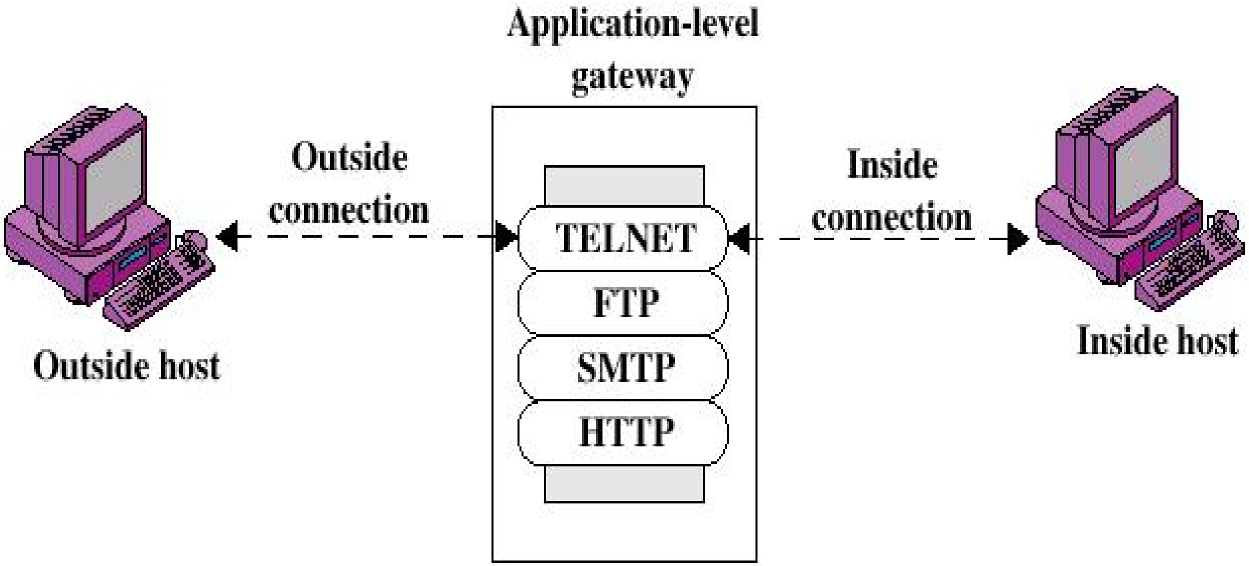
Application-level Gateway

- Also called **proxy server**
- Packets examined at the application layer
- Asks for valid user ID and authentication information for remote host to be accessed
- Acts as a **relay** of application-level traffic

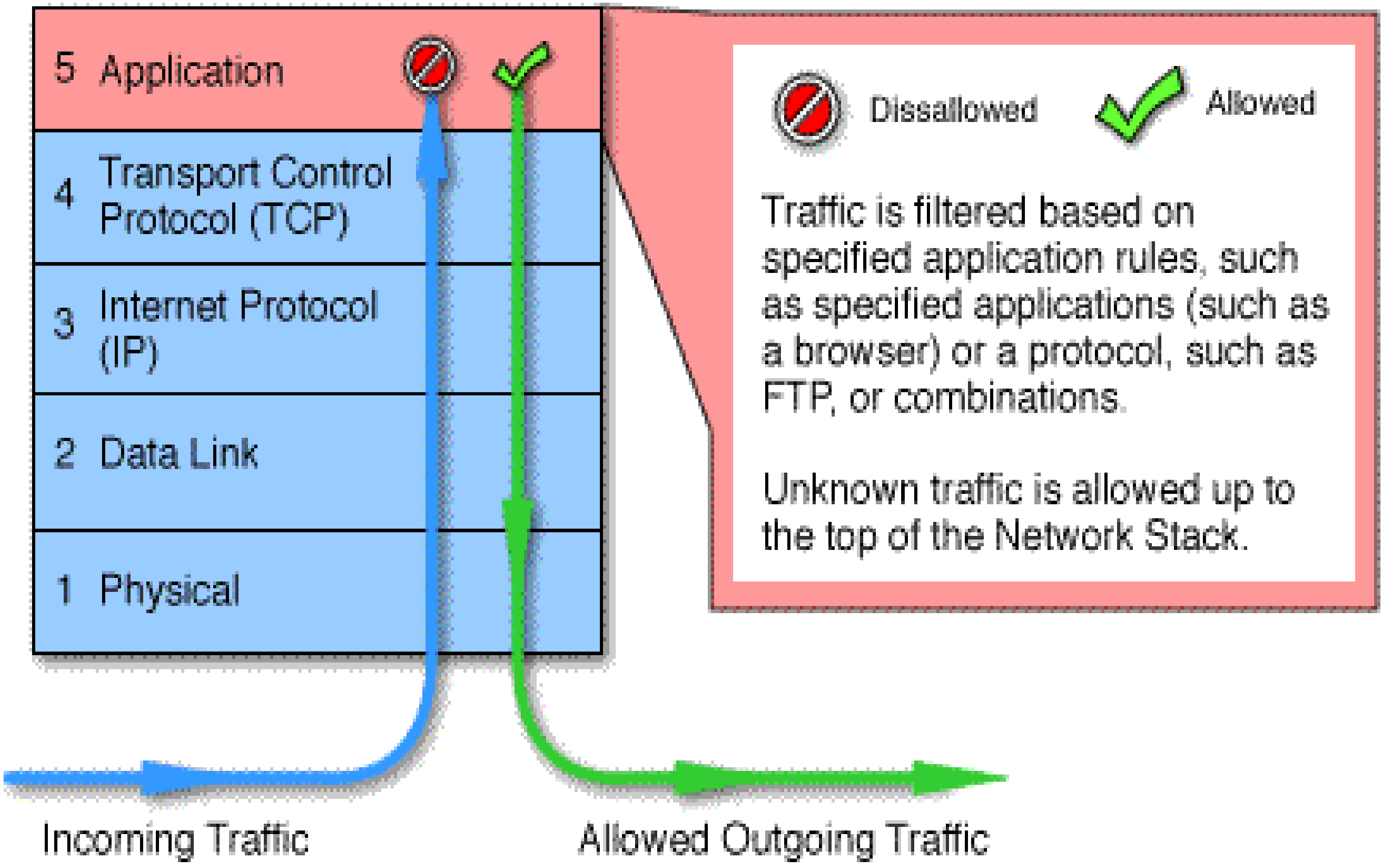


APPLICATION LEVEL GATEWAY

- User contacts gateway for TELNET to remote host, user is authenticated, then gateway contacts remote host and **relays** info between two end points
- Can examine the packets to ensure the security of the application – full packet awareness



APPLICATION LEVEL GATEWAY



Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.

Unknown traffic is allowed up to the top of the Network Stack.

APPLICATION LEVEL GATEWAY

Advantages:

- Higher security than packet filters
- Only need to scrutinize a few allowable applications
- Easy to log and audit all incoming traffic

Disadvantages:

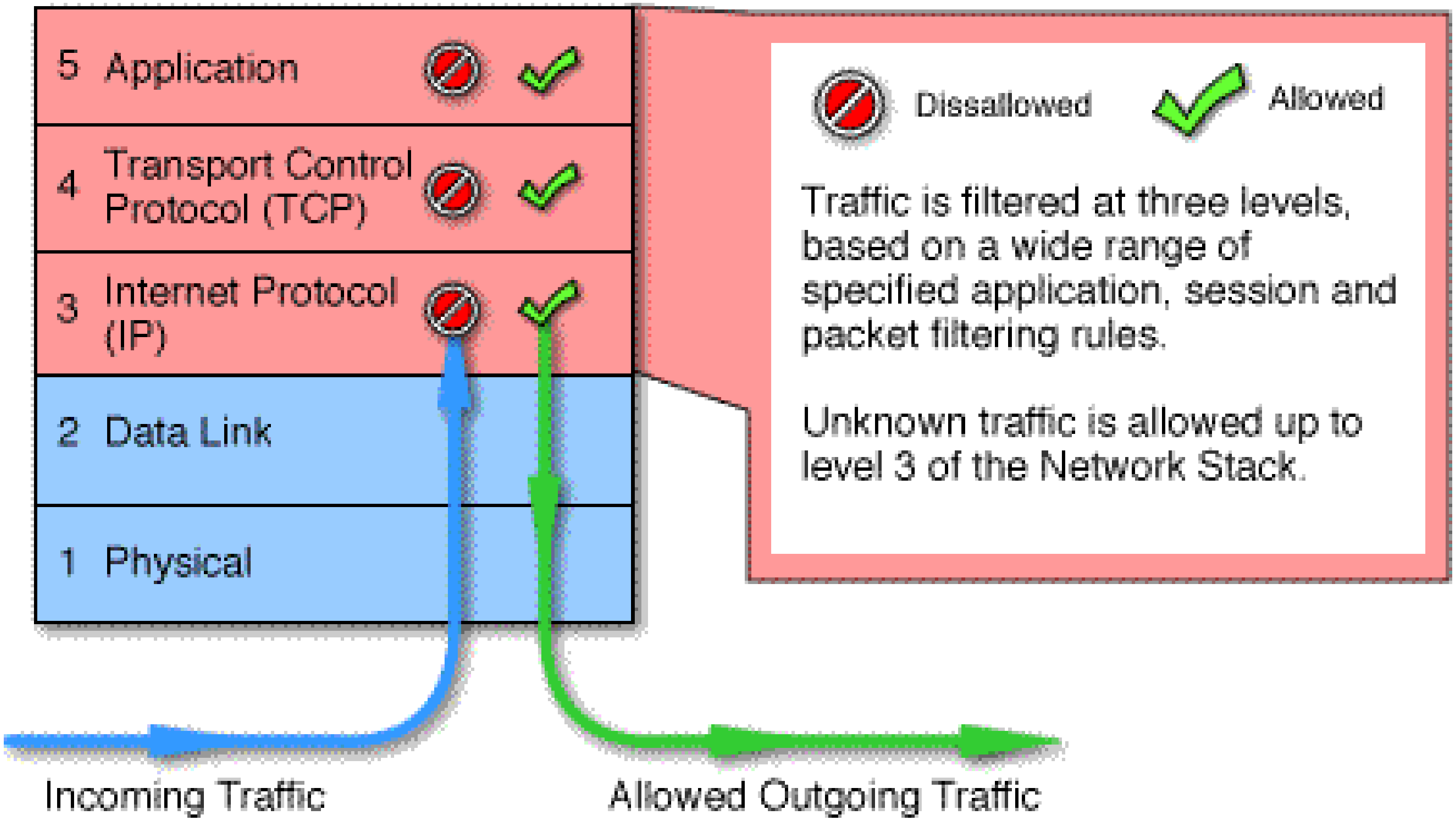
- Additional processing overhead on each connection (gateway as splice point)

TYPES OF FIREWALLS

Stateful multilayer inspection firewalls:

- Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls.
- They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer. And allow the packets to pass though if they pass all of them, individually.
- Stateful multilayer inspection firewalls offer a high level of security, good performance and transparency to end users.
- They are expensive however, and due to their complexity are potentially less secure than simpler types of firewalls if not administered by highly competent personnel.

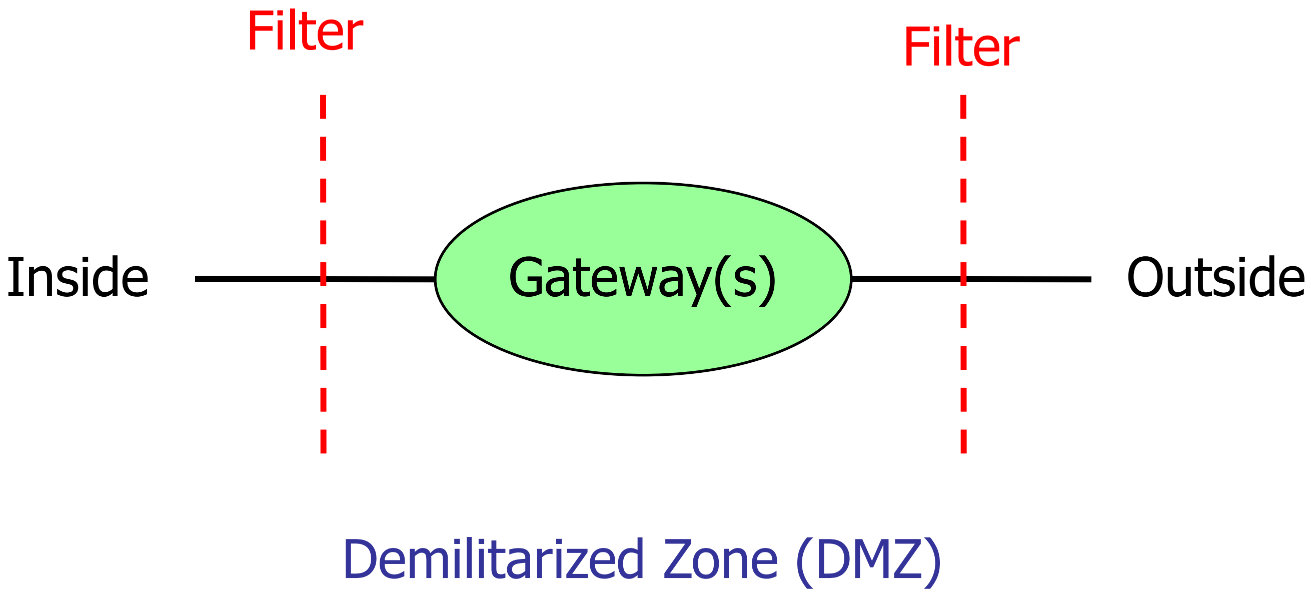
STATEFUL MULTILAYER INSPECTION FIREWALLS



Traffic is filtered at three levels, based on a wide range of specified application, session and packet filtering rules.

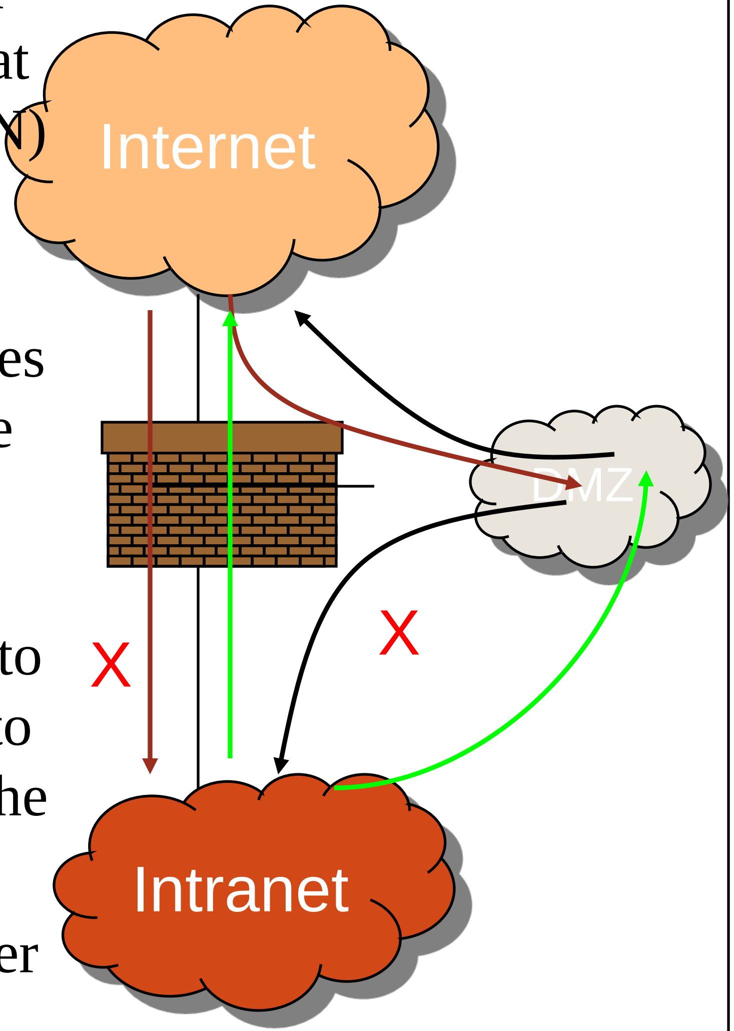
Unknown traffic is allowed up to level 3 of the Network Stack.

SCHEMATIC OF A FIREWALL

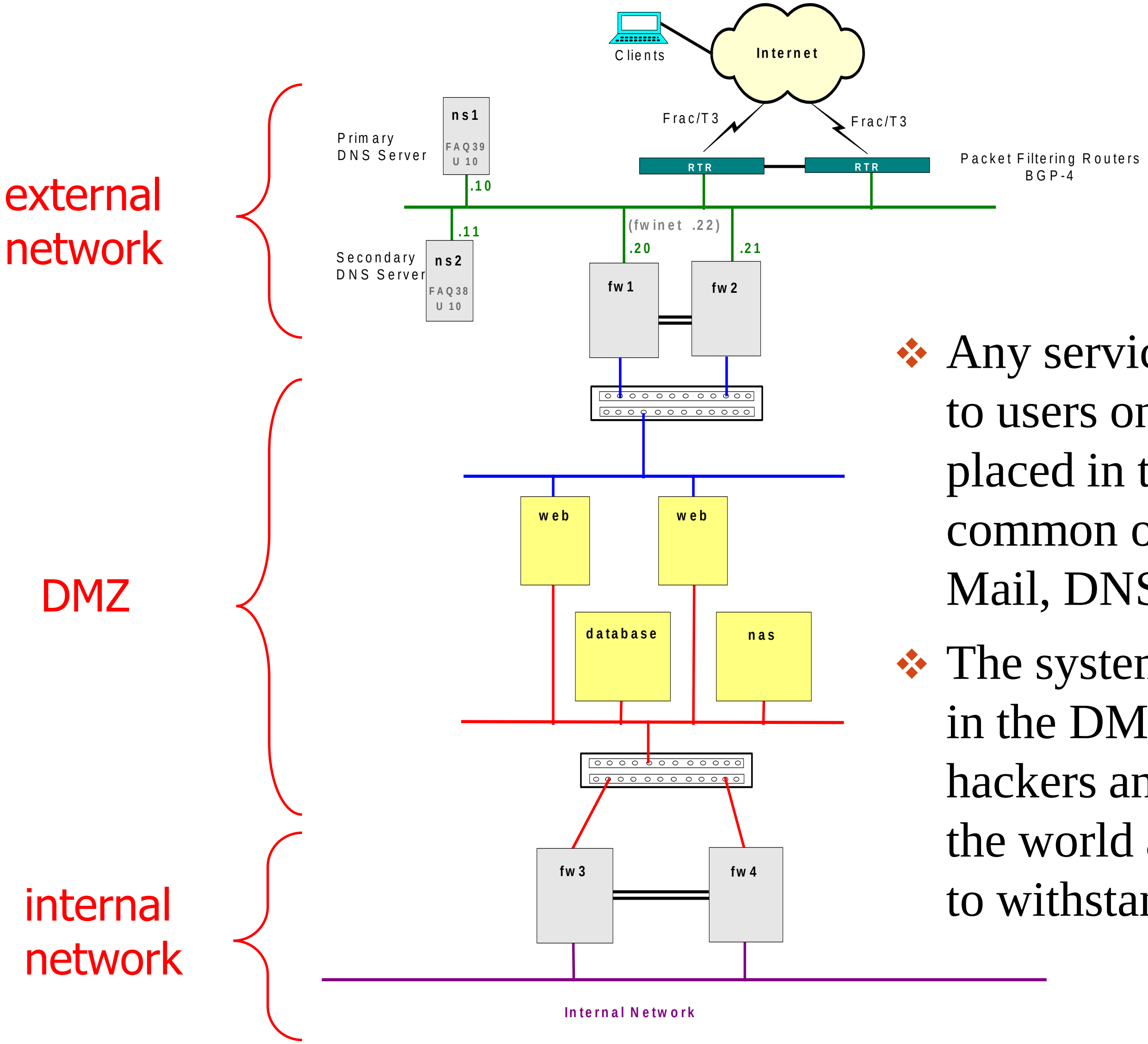


TYPICAL FIREWALL CONFIGURATION

- In computer networks, a DMZ (demilitarized zone) is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet.
- External-facing servers, resources and services are located in the DMZ so they are accessible from the Internet but the rest of the internal LAN remains unreachable.
- This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data via the Internet.
- A DMZ is now often referred to as a perimeter network.



TYPICAL DMZ



- Any service that is being provided to users on the Internet should be placed in the DMZ. The most common of these services are: Web, Mail, DNS, FTP, and VoIP.
- The systems running these services in the DMZ are reachable by hackers and cybercriminals around the world and need to be hardened to withstand constant attack.

SCHEMATIC OF A FIREWALL

Bastion Host

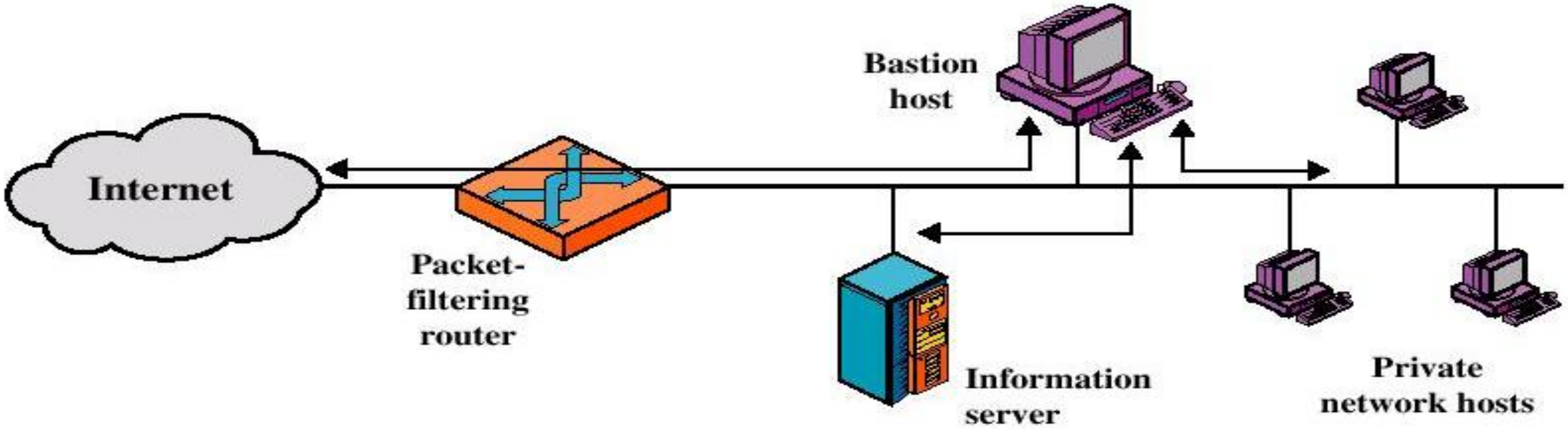
- A **Bastion host** is a special purpose computer on a network specifically designed and configured to withstand attacks.
- The system is on the public side of the DMZ, unprotected by a firewall or filtering router. Frequently the roles of these systems are critical to the network security system.
- The computer generally **hosts** a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.
  - ✓ The bastion host serves as a platform for an application-level or circuit-level gateway
  - ✓ *Choke point* for discovering and terminating intruder attacks
- Indeed, the firewalls and routers can also be considered **bastion hosts**.

3. FIREWALL CONFIGURATIONS

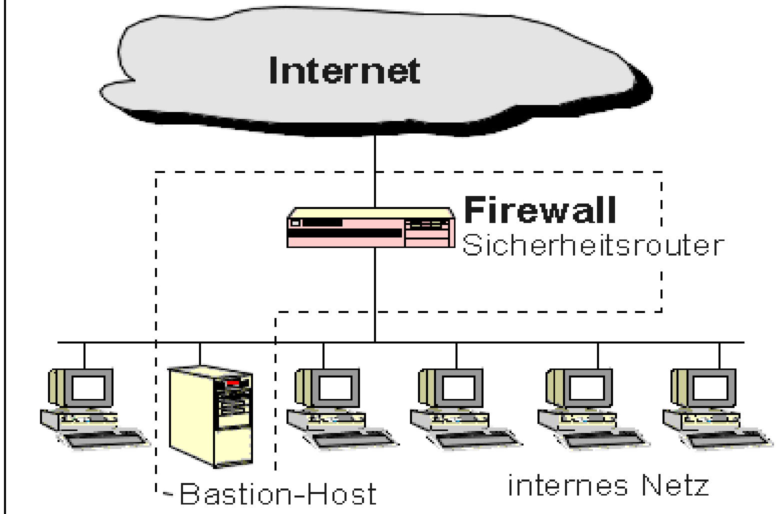
- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), more complex configurations are possible
- **Three common configurations**
  - Screened host firewall system **(single-homed bastion host)**
  - Screened host firewall system **(dual-homed bastion host)**
  - Screened-subnet firewall system

3. FIREWALL CONFIGURATIONS

Screened host firewall system (single-homed bastion host)



- Firewall consists of two systems:
  1. A packet-filtering router
  2. A bastion host

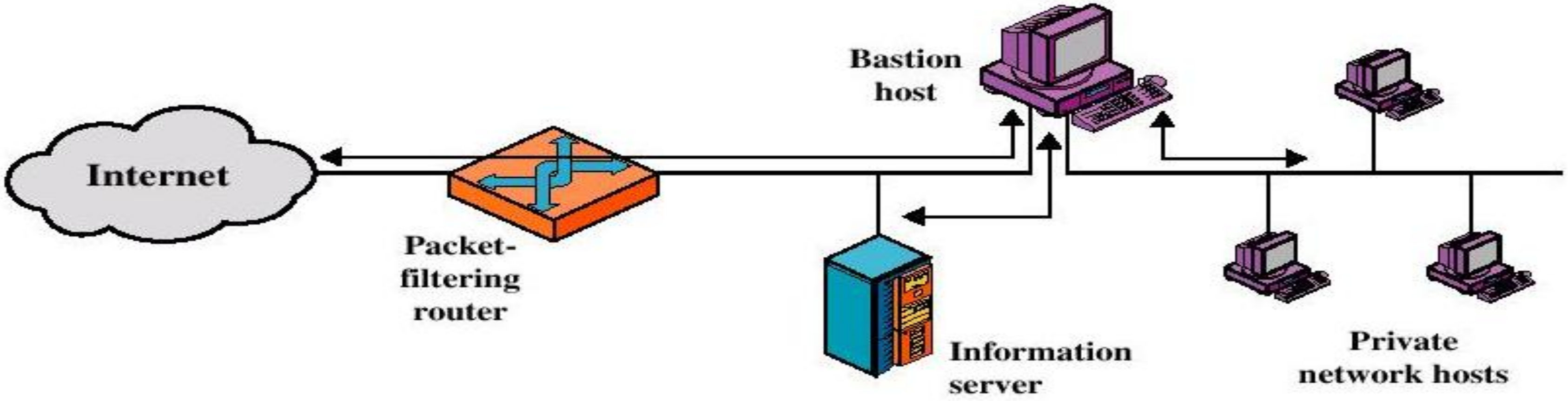


SINGLE-HOMED BASTION HOST

- **Configuration for the packet-filtering router:**
  - ✓Only packets from and to the bastion host are allowed to pass through the router
    - ❑For traffic from the *Internet*, only IP packets *destined* for the *bastion* host are allowed
    - ❑For traffic from the *internal network*, only relayed packets *from* the *bastion* host are allowed out
- **The bastion host performs authentication and proxy functions**
  - ✓Implements *both* packet level and application level filtering
- Intruder *penetrates two separate systems* before internal network is compromiseds

3. FIREWALL CONFIGURATIONS

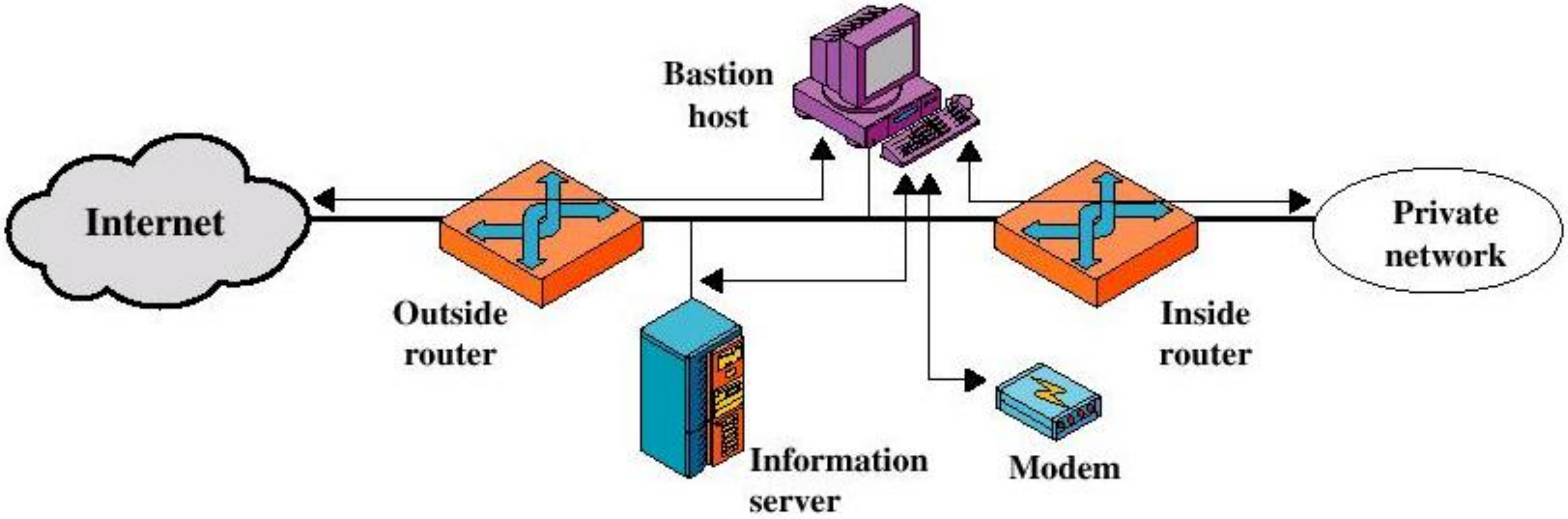
Screened host firewall system (dual-homed bastion host)



- Internal network is completely isolated
  - ✓ The packet-filtering router is not completely compromised
- Bastion host *second defense layer*
  - ✓ Traffic between the Internet and other hosts on the private network has to flow through the bastion host
- Packet forwarding is turned off
- More secure

3. FIREWALL CONFIGURATIONS

Screened-subnet firewall system



SCREENED-SUBNET FIREWALL SYSTEM

- Screened subnet firewall configuration
  - **Most secure** configuration of the three
  - **Two packet-filtering** routers are used
  - Creation of an **isolated sub-network** with bastion host between two packet filtering routers
- **Advantages:**
  - Three levels of defense to thwart intruders
  - The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet)
  - The inside router advertises only the existence of the screened subnet to the internal network (the systems on the inside network cannot construct direct routes to the Internet)

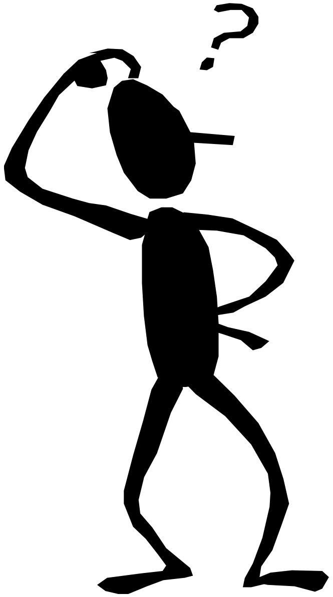
HOW DO I IMPLEMENT A FIREWALL?

- We suggest you approach the task of implementing a firewall by going through the following steps:
  - ✓Determine the access denial methodology to use.
  - ✓Determine inbound access policy.
  - ✓Determine outbound access policy
  - ✓Determine if dial-in or dial-out access is required.
  - ✓Decide whether to buy a complete firewall product, have one implemented by a systems integrator or implement one yourself.

FIREWALL RELATED PROBLEMS

- Firewalls can constitute a traffic bottleneck.
- They concentrate security in one spot, aggravating the single point of failure phenomenon.
- The alternatives however are either no Internet access, or no security, neither of which are acceptable in most organizations.

THANK YOU



END

CS 126: LECTURE 08