Why Firewalls?

- Firewalls are effective to:
  - Protect local systems.
  - Protect network-based security threats.
  - Provide secured and controlled access to Internet.
  - Provide restricted and controlled access from the Internet to local servers.

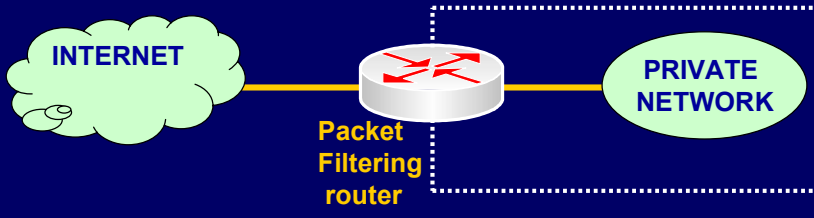
Firewall Characteristics

- Design goals:
  - All traffic from inside to outside must pass through the firewall.
  - Only authorized traffic will be allowed to pass.
    - Defined by local security policy.
  - The firewall itself is immune to penetration.
    - Use of trusted system with a secure operating system.

Types of Firewalls

1. Packet filters.
2. Application-level gateways.
3. Circuit-level gateways.

Packet Filtering Firewall



Some of the attacks that can be made on packet filtering routers:

- IP address spoofing
- Source Routing attacks
- Tiny fragment attacks

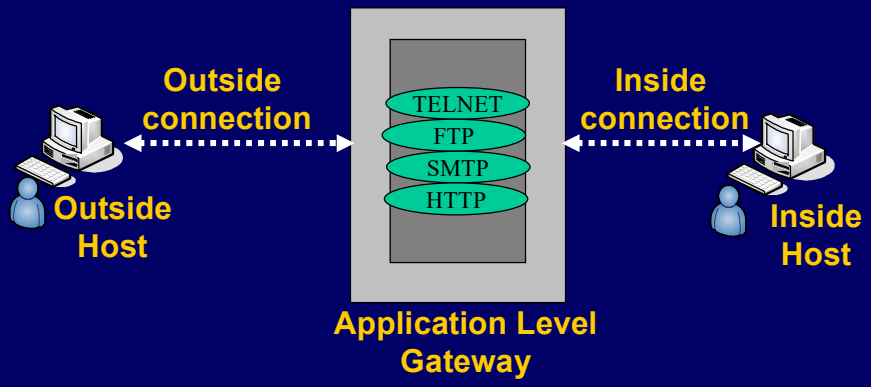
Packet Filtering Firewall (contd.)

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet.
  - Typically based on IP addresses and port numbers.
- Filter packets going in both directions.
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
- Two default policies (discard or forward).

Packet Filtering Firewall (contd.)

- **Advantages:**
  - Simplicity
  - Transparency to users
  - High speed
- **Disadvantages:**
  - Difficulty of setting up packet filter rules
  - Lack of authentication

Application-level Gateway

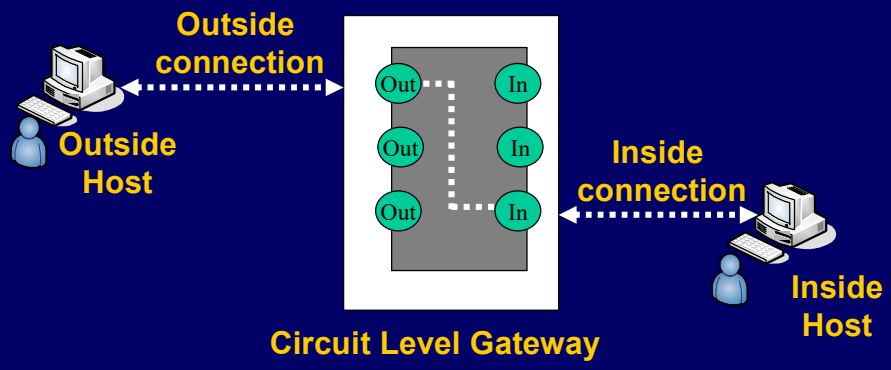


- Also called a Proxy Server; acts as relay of application level traffic.
- It is service specific.

Application-level Gateway

- Application-level Gateway
  - Also called proxy server
  - Acts as a relay of application-level traffic
- 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)

Circuit-Level gateway



Circuit-level Gateway (contd.)

- Stand-alone system, or specialized function performed by an Application-level Gateway.
- Does not permit end-to-end TCP connection; rather the gateway sets up two TCP connections:
  - The gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.

- Typically use is a situation in which the system administrator trusts the internal users.
  - An example is the SOCKS package.

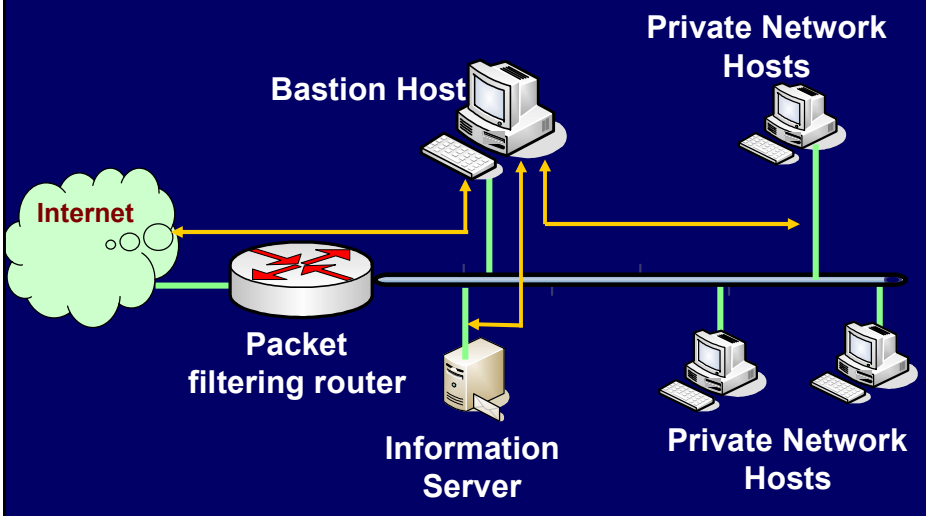
Bastion Host

- It is a system identified by the firewall administrator as a critical point in the network's security.
  - It executes a secure version of its OS and is trusted.
  - It consists of services which are essential.
  - Requires additional authentication before access is allowed.

Firewall Configurations

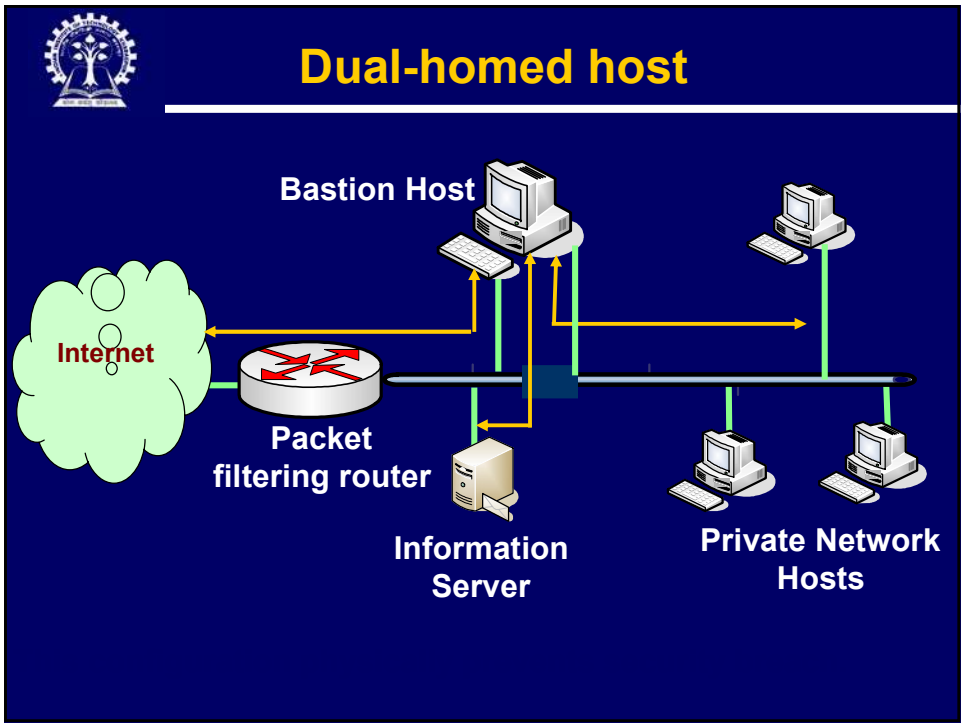
- In addition to the use of simple configuration of a single system, more complex configurations are possible.
- Three common configurations are in popular use.
  - Single-homed host.
  - Dual-homed host.
  - Screened subnet.

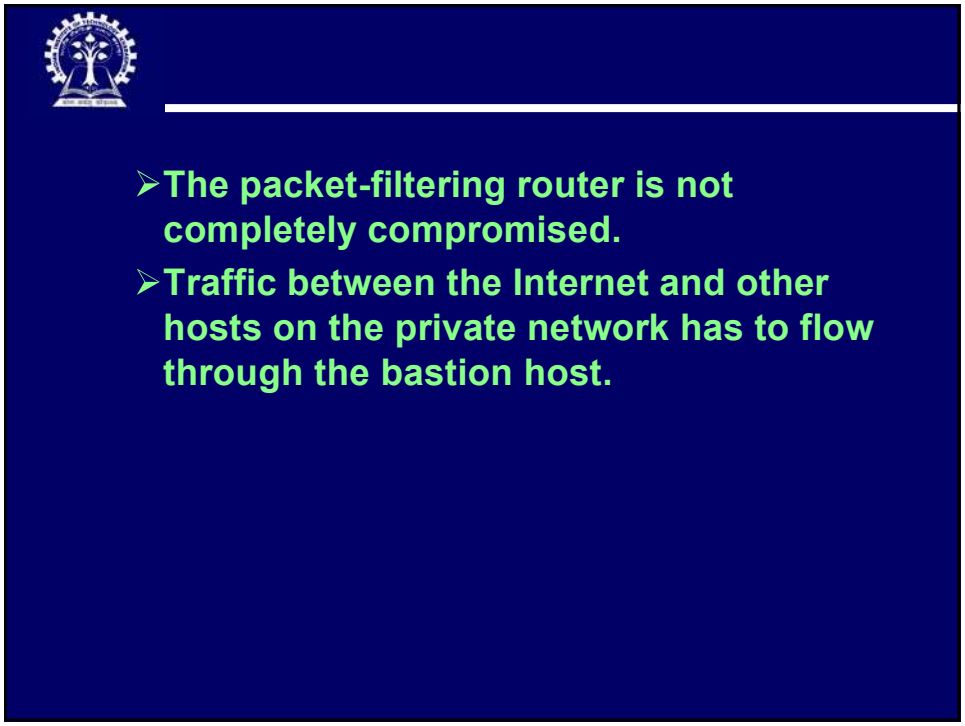
Single-homed Host



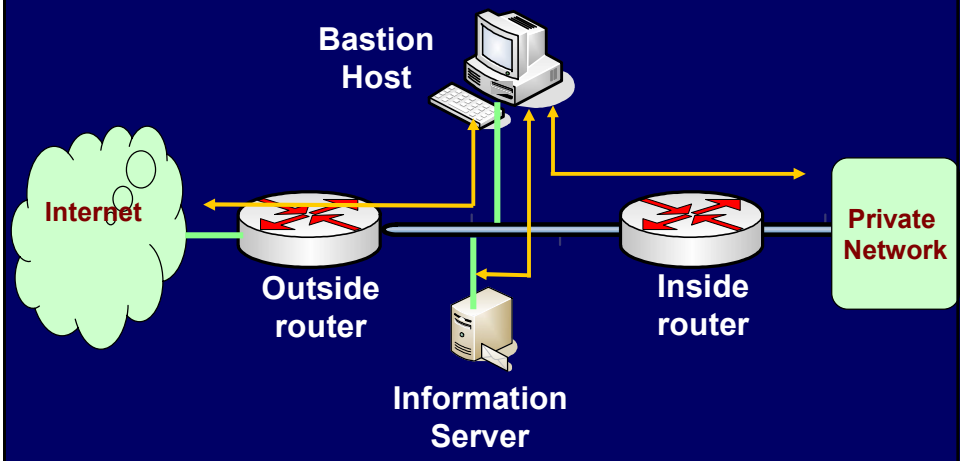
- Firewall consists of two systems:
  - A packet-filtering router
  - A bastion host
- Configuration for the packet-filtering router:
  - Only packets from and to the bastion host are allowed to pass through the router.
- The bastion host performs authentication and proxy functions.

- Greater security than single configurations because of two reasons:
  - Implements both packet-level and application-level filtering (allowing for flexibility in defining security policy).
  - An intruder must generally penetrate two separate systems.


Dual-homed host
Bastion Host
Internet
Packet
filtering router
Information
Server
Private Network
Hosts


The packet-filtering router is not completely compromised.
Traffic between the Internet and other hosts on the private network has to flow through the bastion host.

Screened Subnet



- Most secure configuration of the three.
- Two packet-filtering routers are used.
- Creation of an isolated sub-network.