Indian Institute of Technology Kharagpur

Intranet, Extranet, Firewall

Prof. Indranil Sen Gupta
Dept. of Computer Science & Engg.
I.I.T. Kharagpur, INDIA

Lecture 31: Intranet, Extranet, Firewall

On completion, the student will be able to:

- Define the terms Intranet and Extranet.
- Define the functionalities of Internet firewall.
- Describe various design alternatives for implementing a firewall.
- Illustrate a typical design of Intranet / Extranet.

Intranet and Extranet

What is Intranet?

- **Definition:**
  - **An Intranet is a private computer network that uses Internet protocols, network connectivity, and possibly the public telecommunication system to securely share part of an organization’s information or operations with its employees.**

- Basically ….
  - It uses the same concepts and technologies of the Internet (clients and servers) running on the TCP/IP protocol suite.
  - HTTP, FTP and SMTP are very commonly used.
  - Access to information is typically through browsers.
    - Platform independent.
    - No need to install special software on clients.

- Advantages:
  - Intranets help employees to quickly locate information and applications relevant to their roles and responsibilities.
  - Standard interface, allowing “access from anywhere”.
  - Can serve as a powerful tool for communication within an organization.
    - Both vertically and horizontally.
  - Permits information to be published.

What is Extranet?

- Definition:
  - ➢An Extranet is a private network that uses Internet protocols, network connectivity, and possibly the public communication system to securely share part of an organization's information or operations with suppliers, partners, customers, or other businesses.
  - ➢Can be viewed as part of a company's Intranet that is extended to users outside the company.

- Basically ….
  - ➢It is "a private internet over the Internet".
  - ➢Used to designate "private parts" of a website.
    - Only registered users can navigate.
  - ➢It requires security and privacy.
    - Firewall server management.
    - Issuance and use of digital certificates or similar means of authentication.
    - Encryption of messages.
    - Use of Virtual Private Networks (VPN) that tunnel through the public network.

- Advantages:
  - Can improve organization productivity.
  - Allows information to be viewed at times convenient for external users.
    - Cuts down on meeting times.
  - Information can be updated instantly.
    - Authorized users have immediate access to latest information.
  - Can improve relationships with customers.

Firewall

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.

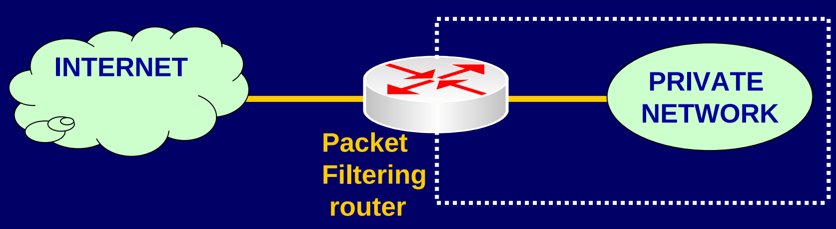
Firewall Characteristics

- 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

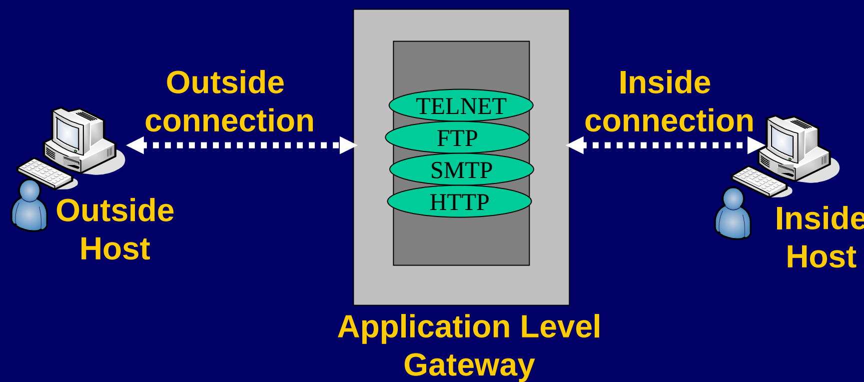
Packet Filtering Firewall (contd.)

- 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

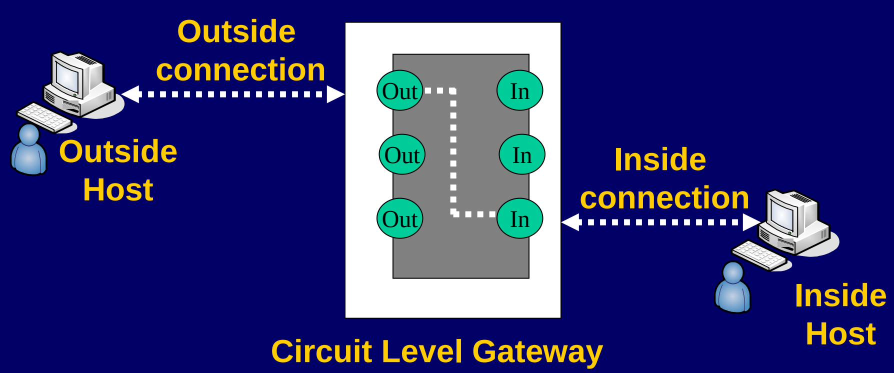


- Also called a Proxy Server; acts as relay of application level traffic.
- It is service specific.

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.

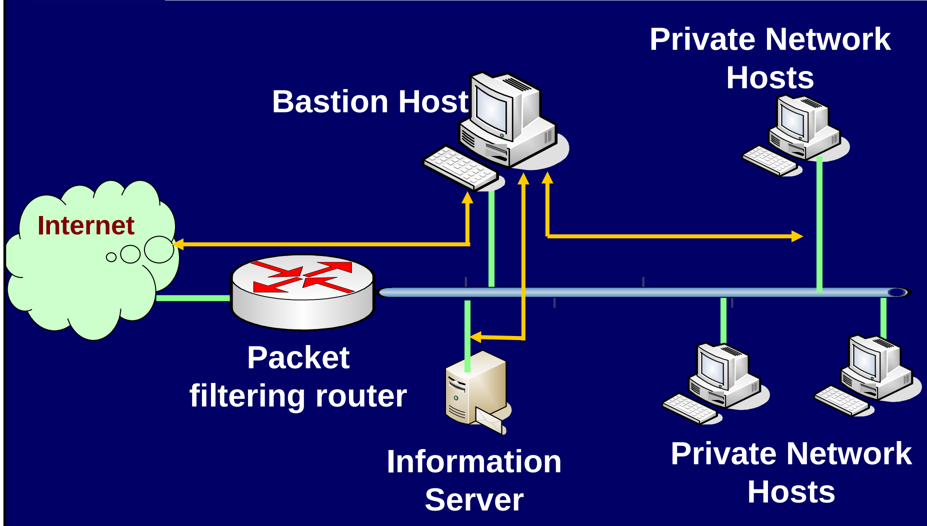
Bastion Host

- 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.

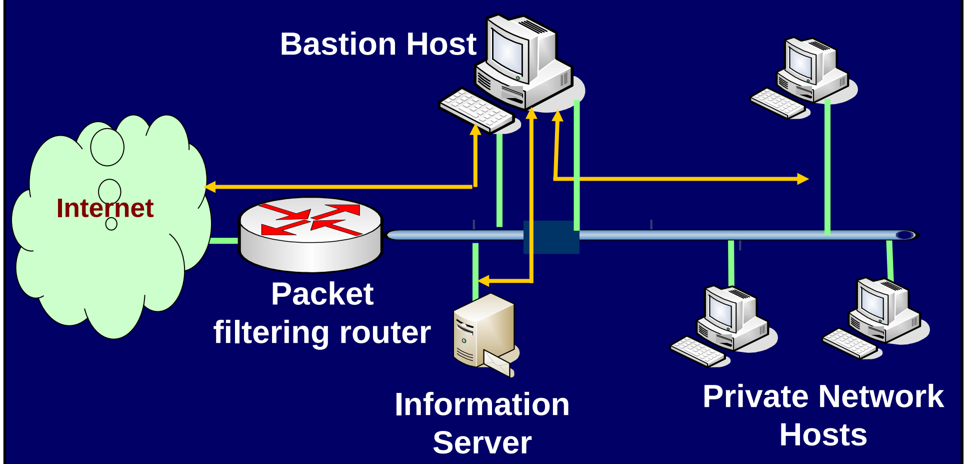
Single-homed Host



- 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.

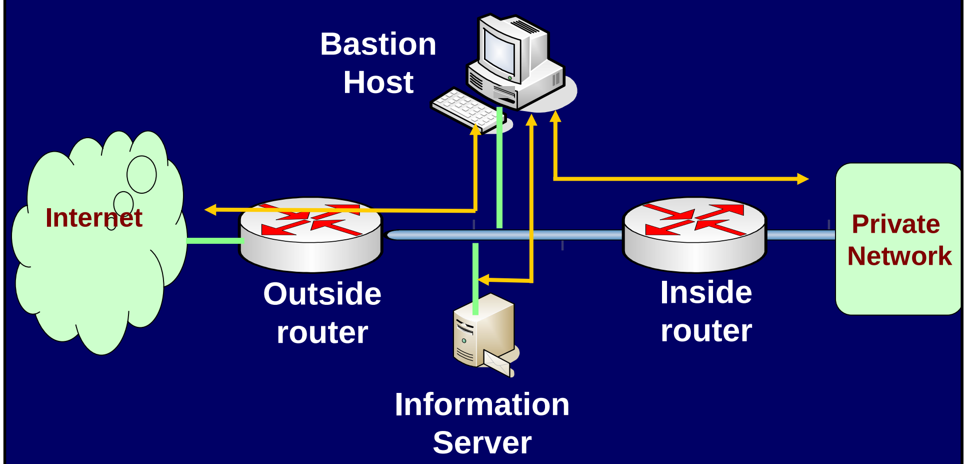
- Greater security than single configurations because of two reasons:
  - Implements both packet-level and application-level filtering (allowing for flexibility in defining security policy).
  - An intruder must generally penetrate two separate systems.

Dual-homed host



- 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.

- **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.**

Intranet / Extranet Design Issues

- For Intranet:
  - Analysis of the organization flow.
  - Identify various cross-sections of employees, and their access privileges.
  - Enforce authentication mechanism.
- For Extranet:
  - Security is the major concern.
  - Combination of firewalls, authentication, VPN, etc. must be used.

End of Lecture 31

SOLUTIONS TO QUIZ QUESTIONS ON LECTURE 30

Quiz Solutions on Lecture 30

1. What is the basic concept behind InputStream and OutputStream in Java?

   They are abstract classes supported by Java.

   - Concept of InputStream can be used to abstract any kind of input.
   - Concept of OutputStream can be used to abstract any kind of output.

Quiz Solutions on Lecture 30

2. How can you read one line of text at a time from a file called "data.in"?

   DataInputStream inp = new DataInputStream
   (new FileInputStream ("data.in"));
   String line = inp.readLine();

3. What are the functions of the ServerSocket() and the accept() methods?

   The ServerSocket() method is used to initialize a server socket, and the accept() method is used to make the server wait for client connection.

Quiz Solutions on Lecture 30

4. When would you prefer to have a concurrent server?

   Concurrent servers are preferred in cases where multiple simultaneous client requests are likely, and also the service time is considerably long.

Quiz Solutions on Lecture 30

5. **What are the functions of the DatagramPacket and the DatagramSocket classes?**

   The DatagramPacket class acts as the data container; the packet data are contained in it.

   The DatagramSocket class defines the socket for sending and receiving datagrams.

QUIZ QUESTIONS ON LECTURE 31

Quiz Questions on Lecture 31

1. What is the main difference between an Intranet and an Extranet?
2. How does a packet filtering router typically filters packets?
3. How does an application level gateway carry out the filtering process?
4. Which would be more suitable for email filtering: packet-level filter or application-level gateway?
5. What is a bastion host?

Quiz Questions on Lecture 31

6. In the dual-homed host firewall, how many security points must be broken by an intruder before he can get into the internal network?
7. Repeat the above for screened subnet firewall.