CHAPTER 20

Firewalls

Firewall Design Principles

- The firewall is inserted between the premises network and the Internet to establish a controlled link and to establish an outer security wall or perimeter.

- The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and audit can be imposed.

- The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

Firewall Characteristics

The design goals for a firewall are as follows: **(2014)**

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.

2. Only authorized traffic (defined by the local security policy) will be allowed to pass.

3. The firewall itself is immune to penetration. This implies that use of a trusted system with secure operating system.

Firewall Characteristics Continue…

Four general techniques to control access and enforce the site's security policy:

1. Service control:

   Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address and TCP port number.

2. Direction control:

   Determines the direction in which particular service requests may be initiated and allowed to flow.

3. User control:

   Controls access to a service according to which user is attempting to access it.

4. Behavior control:

   Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam or it may enable external access to only a portion of the information on a local web server.

Firewall Characteristics Continue…

What one can expect from a firewall? **(2012)**

1. A firewall defines a single choke point that
   - keeps unauthorized users out of the protected network.
   - Prohibits vulnerable services from entering or leaving the network.
   - Provides protection from various kinds of IP spoofing and routing attacks.

2. A firewall provides a location for monitoring security-related events.

3. A firewall acts as a network address translator and perform a network management function that audits or logs Internet usage.

4. A firewall can serve as the platform for IPSec.

Firewall Characteristics Continue…

Firewalls have their limitations, including the following: (2015)

1. The firewall cannot protect against attacks that bypass the firewall.

2. The firewall does not protect against internal threats such as an employee who wittingly cooperates with an external attacker.

3. The firewall cannot protect against the transfer of virus-infected programs or files (it is impossible for the firewall to scan all incoming files, email, and messages for viruses).

Types of Firewalls

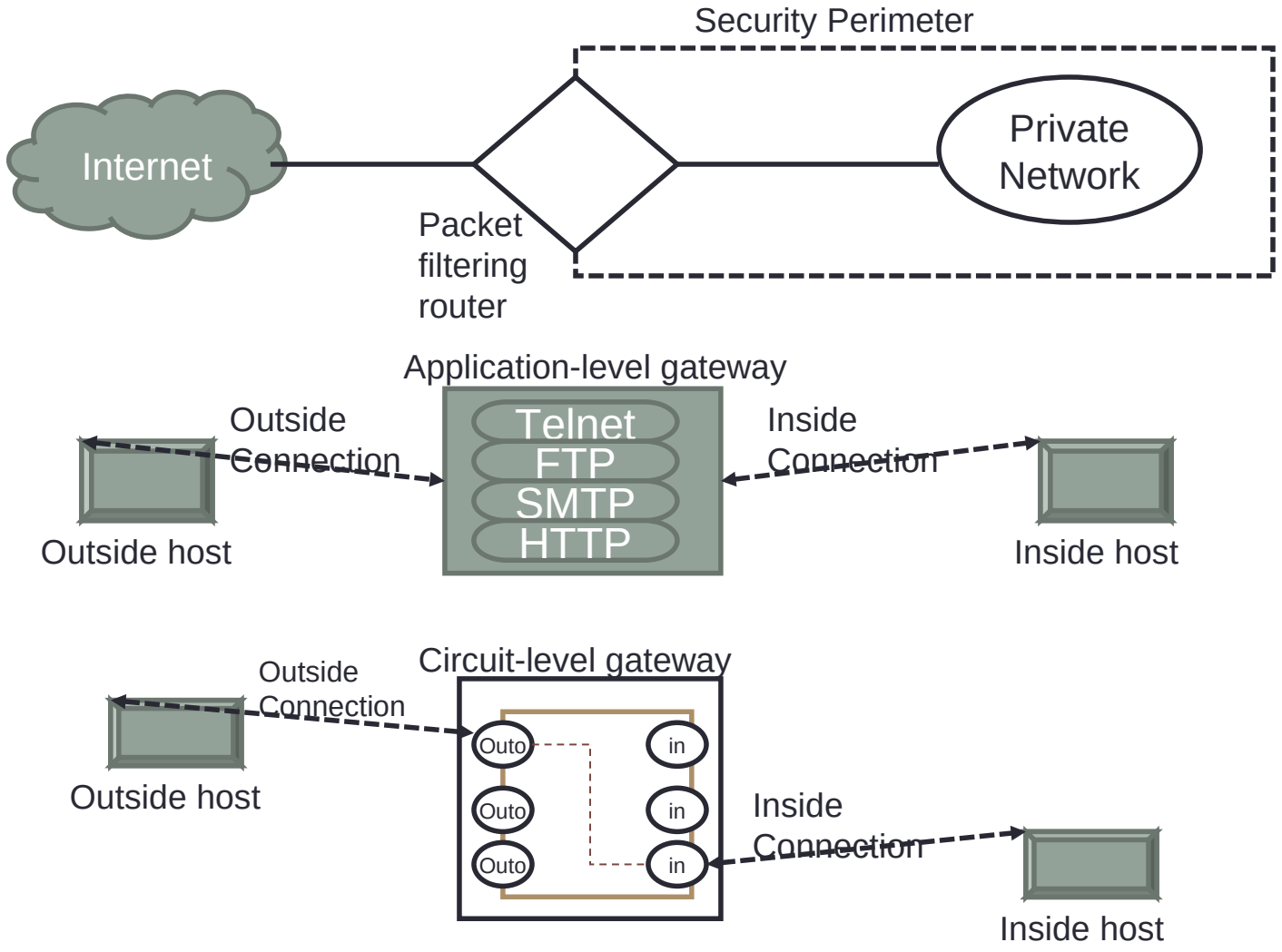
- Figure on the next slide illustrates the three common types of firewalls:
  1. **Packet filters.**
  2. **Application-level gateways. And**
  3. **Circuit-level gateways.**

1. Packet-Filtering Router: (2010)

A packet filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet. Filtering rules are based on information contained in a network packet:

- Source IP address: IP (ex 192.168.1.1) of the originated system.
- Destination IP address: IP (ex 192.168.1.2) of the system the IP packet is trying to reach.
- Source and destination transport-level address:
- IP protocol field: Defines the transport protocol.
- Interface: for a router with 3 or more ports, which interface of the router the packet came from or which interface of the router the packet is destined for.

Figure: Firewall Types



Application-Level Gateway (2006,2007)

- Also called a proxy server, acts as a relay of application-level traffic.
- The user contacts the gateway using a TCP/IP application such as Telnet or FTP, and the gateway asks the user for the names of the remote host to be accessed.
- When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
- If the gateway does implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall.
- Application-level gateway tend to be more secure than packet filters.
- The application-level gateway need only scan a few allowable applications.
- It is easy to log and audit all incoming traffic at the application level.
- A prime disadvantage is the additional processing overhead on each connection.

Circuit-Level Gateway

- A circuit-level gateway does not support end-to-end TCP connection.

- Rather the gateway sets up two TCP connections,
  1. one between itself and a TCP user on an inner host and
  2. One between itself and a TCP user on an outside host.

- A typical use of a circuit-level gateways is a situation in which the system administrator trusts the internal users.