THEME 2

Firewalls

Telecommunication systems department

Lecturer: assistant professor Persikov Anatoliy Valentinovich

NEED FOR INTERNET CONNECTIVITY

Information systems in corporations, government agencies, and other organizations have undergone a steady evolution:

- **Centralized data processing system**, with a central mainframe supporting a number of directly connected terminals;
- **Local area networks** (LANs) interconnecting PCs and terminals to each other and the mainframe;
- **Premises network**, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two;
- **Enterprise-wide network**, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN);
- **Internet connectivity**, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN.

Internet connectivity is no longer optional for organizations. The information and services available are essential to the organization. Moreover, individual users within the organization want and need Internet access, and if this is not provided via their LAN, they will use connection capability from their PC to an Internet service provider (ISP).

NEED FOR FIREWALLS

However, while Internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates a threat to the organization.

While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this is not a practical approach.

Consider a network with hundreds or even thousands of systems, running a mix of various versions of UNIX, plus Windows. When a security flaw is discovered, each potentially affected system must be upgraded to fix that flaw.

The alternative, increasingly accepted, is the **firewall**. The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect 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

Design goals for a firewall:

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. Various configurations are possible.

2. **Only authorized traffic**, as defined by the local security policy, **will be allowed to pass**. Various types of firewalls are used, which implement various types of security policies.

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

FIREWALL CHARACTERISTICS

Four general techniques that firewalls use 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; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.

2) **Direction control:** Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

3) **User control:** Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology, such as is provided in IPSec.

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 CAPABILITIES

The following capabilities are within the scope of a firewall:

1) A firewall defines a **single choke point** that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.

2) A firewall provides **a location for monitoring security-related events**. Audits and alarms can be implemented on the firewall system.

3) A firewall is a **convenient platform for several Internet functions that are not security related**. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.

4) A firewall can serve as **the platform for virtual private network**.

FIREWALL LIMITATIONS

Firewalls have their limitations, including the following:

1) **The firewall cannot protect against attacks that bypass the firewall**. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.

2) **The firewall does not protect against internal threats**, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.

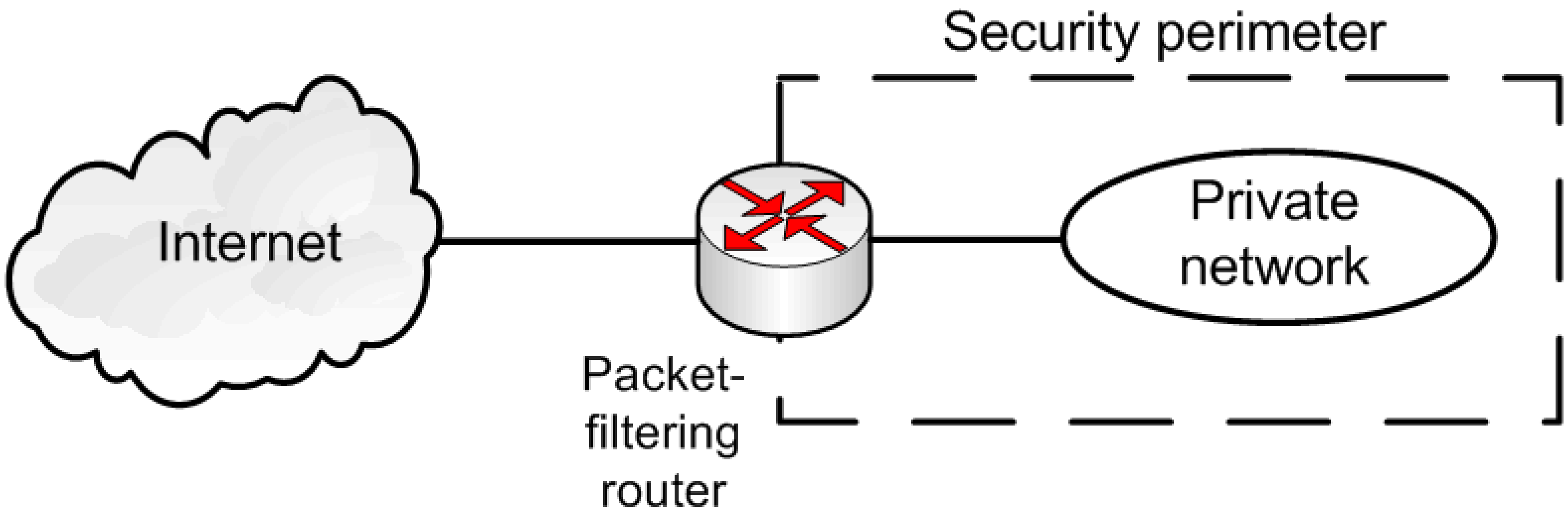
3) **The firewall cannot protect against the transfer of virus-infected programs or files**. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

PACKET-FILTERING ROUTER

A **packet-filtering router** applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The router is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet:

- **Source IP address:** The IP address of the system that originated the IP packet (e.g., 192.178.1.1)
- **Destination IP address:** The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)
- Source and destination transport-level address: The transport level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET
- **IP protocol field:** Defines the transport protocol.
- **Interface:** For a router with three or more ports, which interface of the router the packet came from or which interface of the router the packet is destined for.

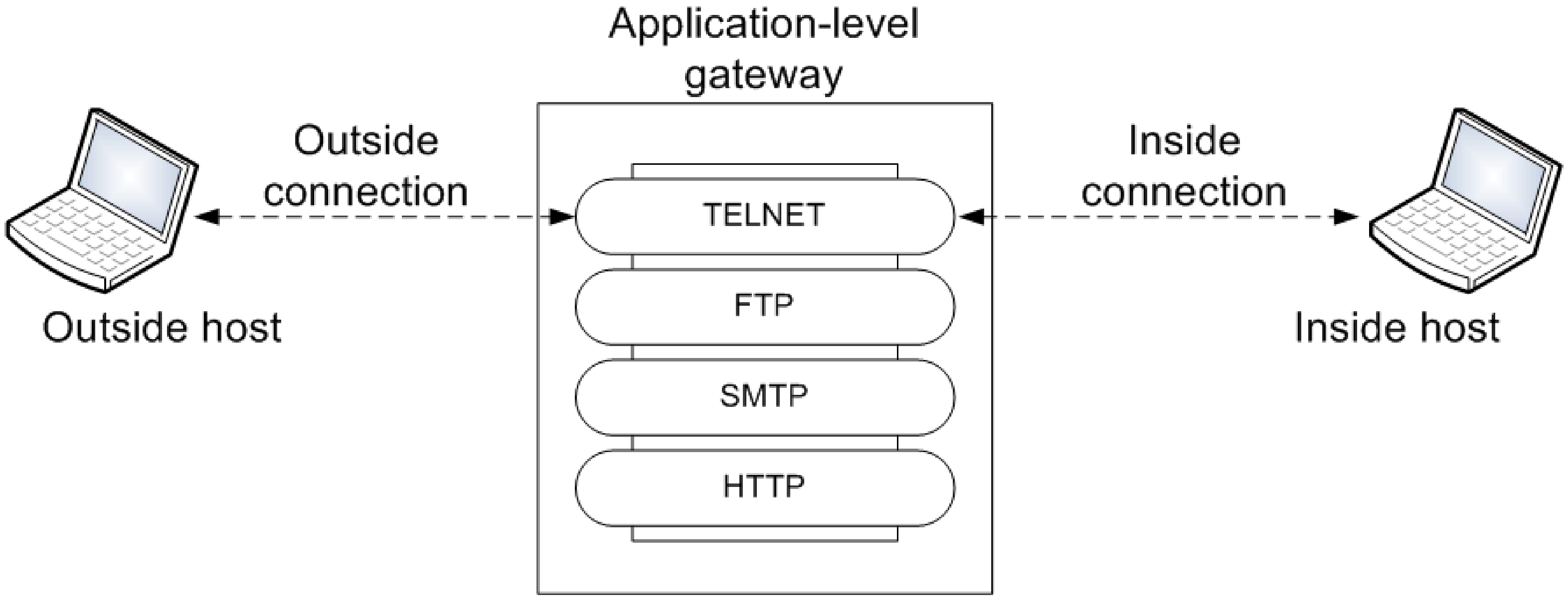
PACKET-FILTERING ROUTER



The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken. Two default policies are possible:

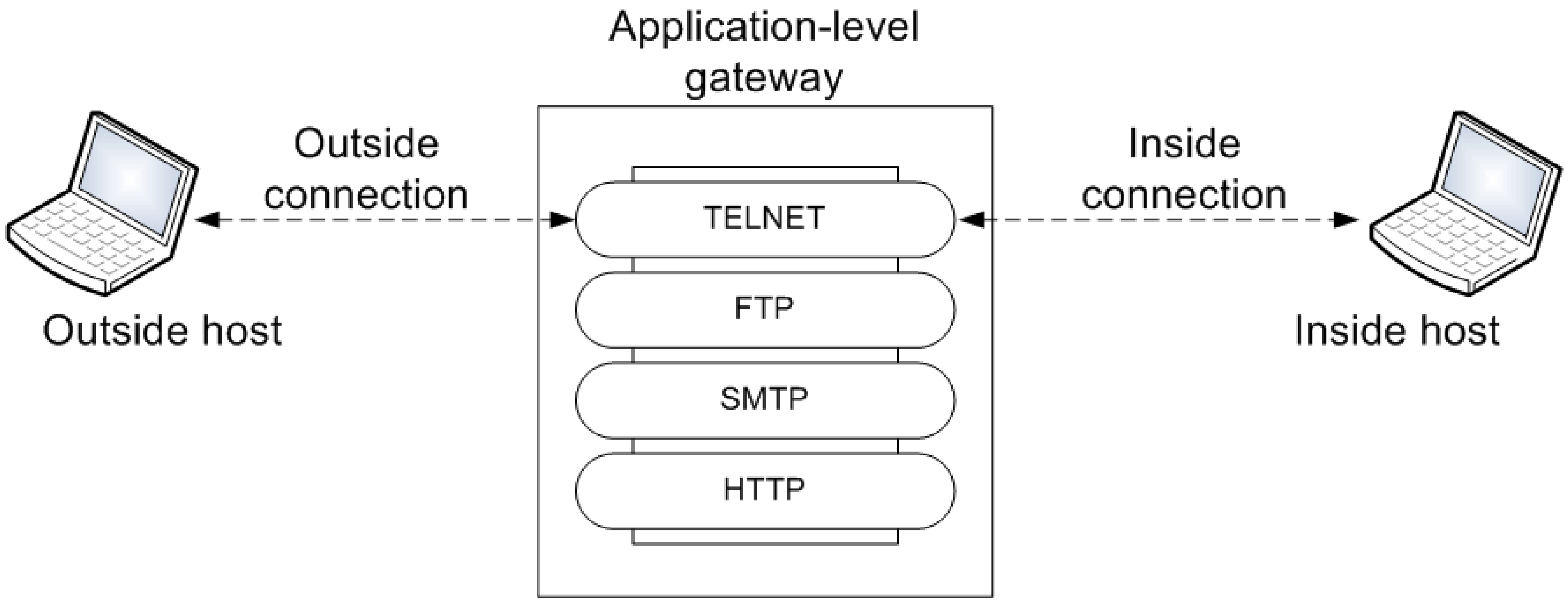
– Default = discard: That which is not expressly permitted is prohibited.
– Default = forward: That which is not expressly prohibited is permitted.

APPLICATION-LEVEL GATEWAY



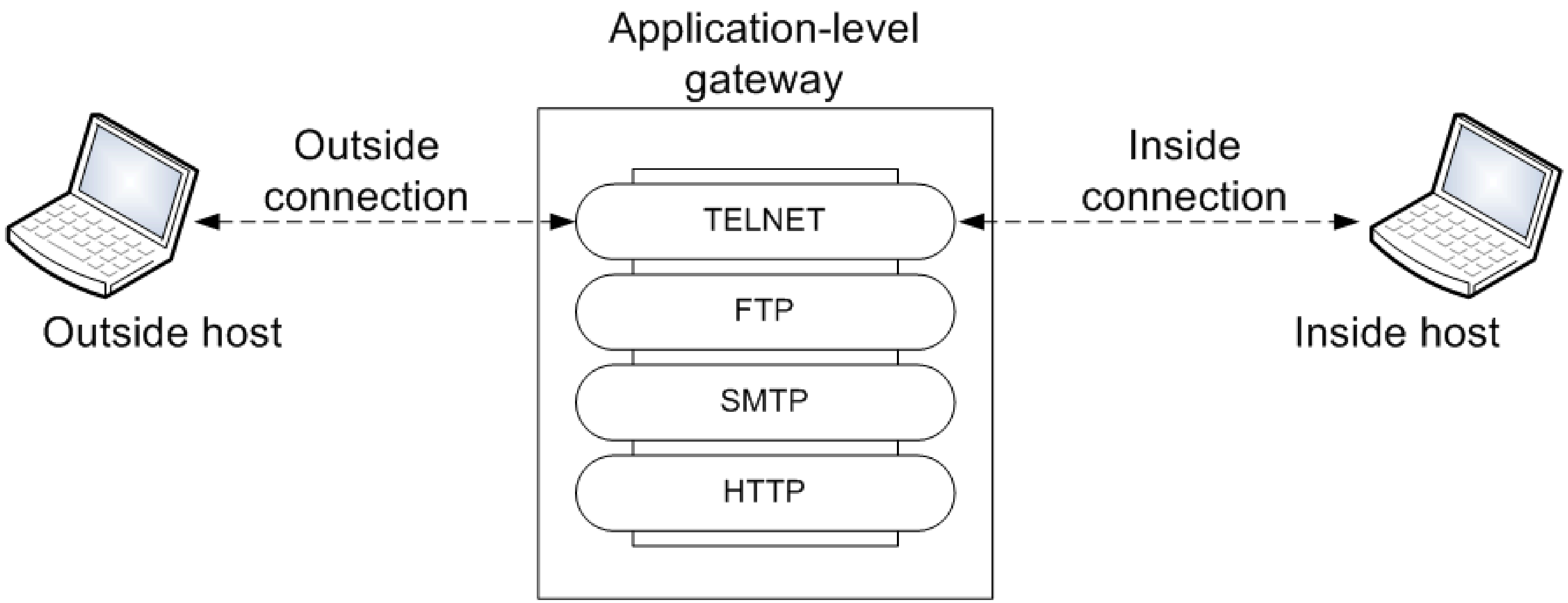
An application-level gateway, also called a **proxy server**, acts as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.

APPLICATION-LEVEL GATEWAY



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 not implement the proxy code for a specific application, the service is not supported and cannot be forwarded across the firewall. Further, the gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features.

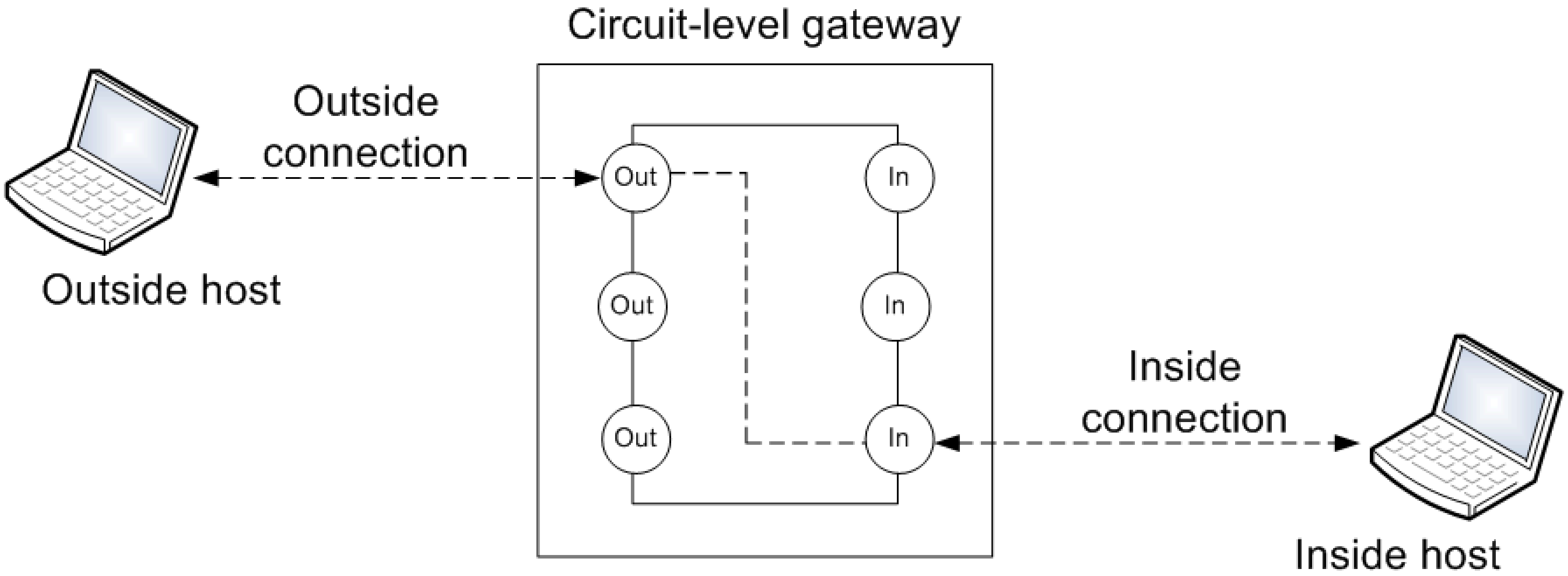
APPLICATION-LEVEL GATEWAY



Application-level gateways tend to be more secure than packet filters. Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only scrutinize a few allowable applications. In addition, it is easy to log and audit all incoming traffic at the application level.

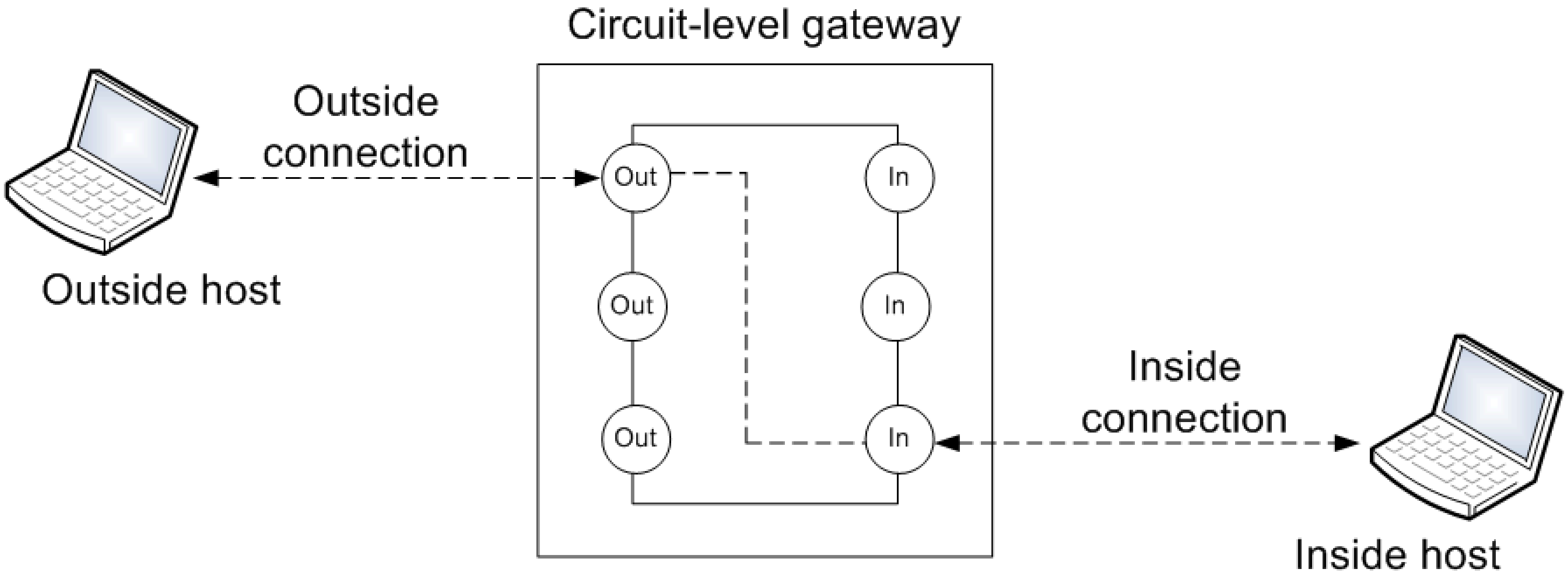
A **prime disadvantage** of this type of gateway is the additional processing overhead on each connection. In effect, there are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examine and forward all traffic in both directions.

CIRCUIT-LEVEL GATEWAY



This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications. A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, 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.

CIRCUIT-LEVEL GATEWAY



A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections. In this configuration, the gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.

BASTION HOST

A **bastion host** is a system identified by the firewall administrator as a critical strong point in the network's security. Typically, the bastion host serves as a platform for an application-level or circuit-level gateway. **Common characteristics of a bastion host** include the following:

- The bastion host hardware platform executes a secure version of its operating system, making it a trusted system.
- Only the services that the network administrator considers essential are installed on the bastion host. These include proxy applications such as Telnet, DNS, FTP, SMTP, and user authentication.
- The bastion host may require additional authentication before a user is allowed access to the proxy services. Each proxy service may require its own authentication before granting user access.
- Each proxy is configured to support only a subset of the standard application's command set.
- Each proxy is configured to allow access only to specific host systems. This means that the limited command/feature set may be applied only to a subset of systems on the protected network.

BASTION HOST

- Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection. The audit log is an tool for discovering and terminating intruder attacks.

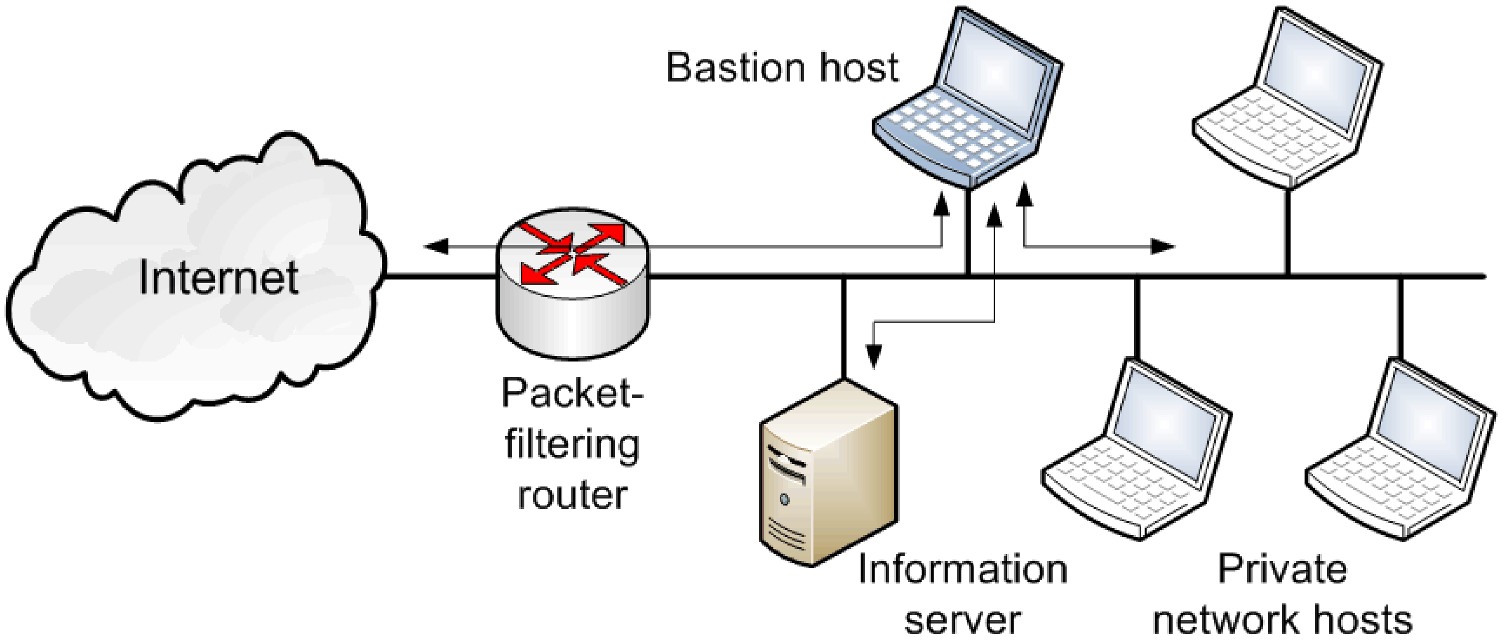
- Each proxy module is a very small software package specifically designed for network security. Because of its relative simplicity, it is easier to check such modules for security flaws.

- Each proxy is independent of other proxies on the bastion host. If there is a problem with the operation of any proxy, or if a future vulnerability is discovered, it can be uninstalled without affecting the operation of the other proxy applications. Also, if the user population requires support for a new service, the network administrator can easily install the required proxy on the bastion host.

- A proxy generally performs no disk access other than to read its initial configuration file. This makes it difficult for an intruder to install Trojan horse sniffers or other dangerous files on the bastion host.

- Each proxy runs as a nonprivileged user in a private and secured directory on the bastion host.

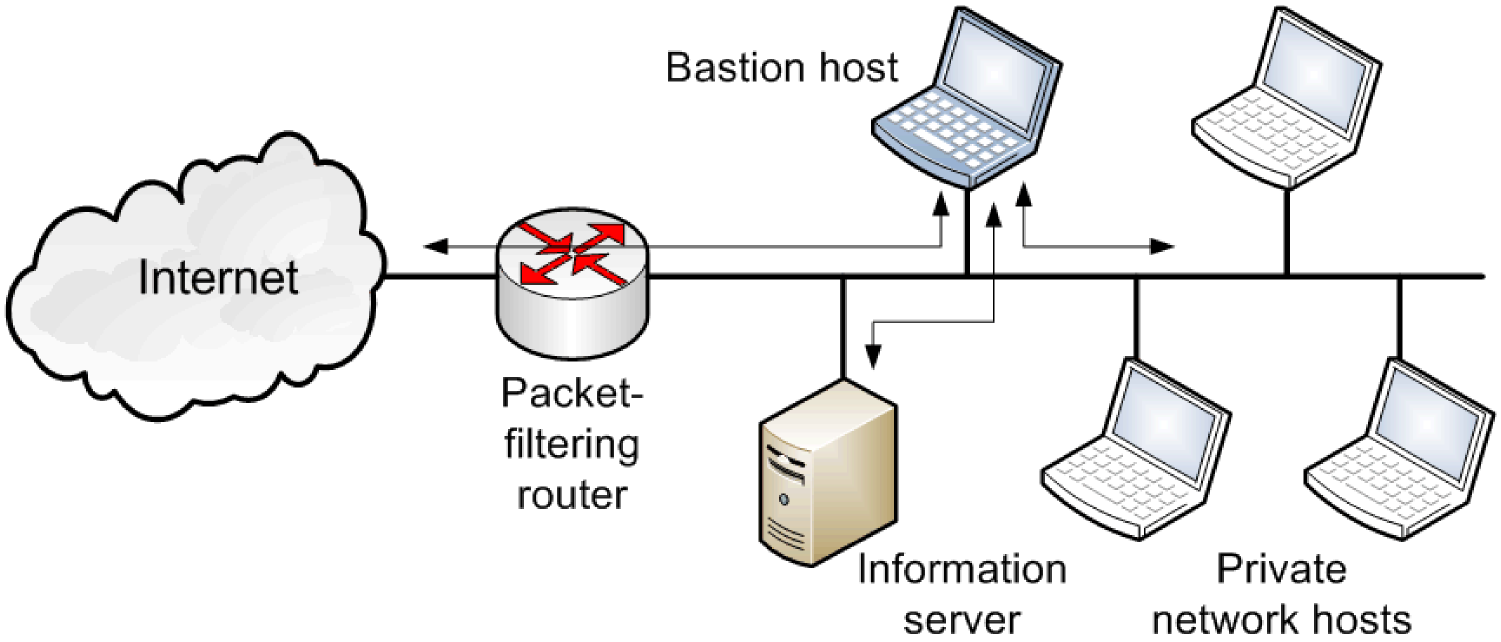
FIREWALL CONFIGURATIONS



In **single-homed bastion configuration** the firewall consists of two systems: a packet-filtering router and a bastion host. Typically, the router is configured so that

1) For traffic from the Internet, only IP packets destined for the bastion host are allowed in.
2) For traffic from the internal network, only IP packets from the bastion host are allowed out.

FIREWALL CONFIGURATIONS

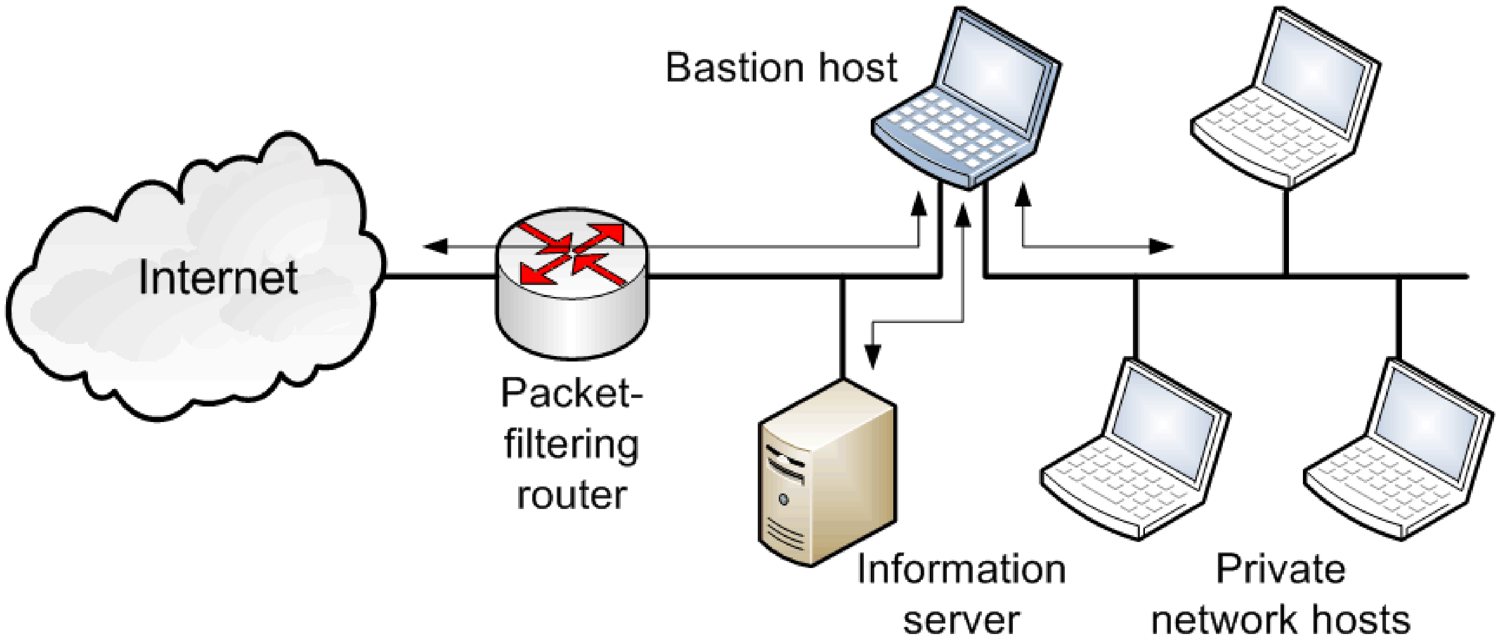


The bastion host performs authentication and proxy functions. This configuration has greater security than simply a packet-filtering router or an application-level gateway alone, for two reasons.

First, this configuration implements both packet-level and application-level filtering, allowing for considerable flexibility in defining security policy.

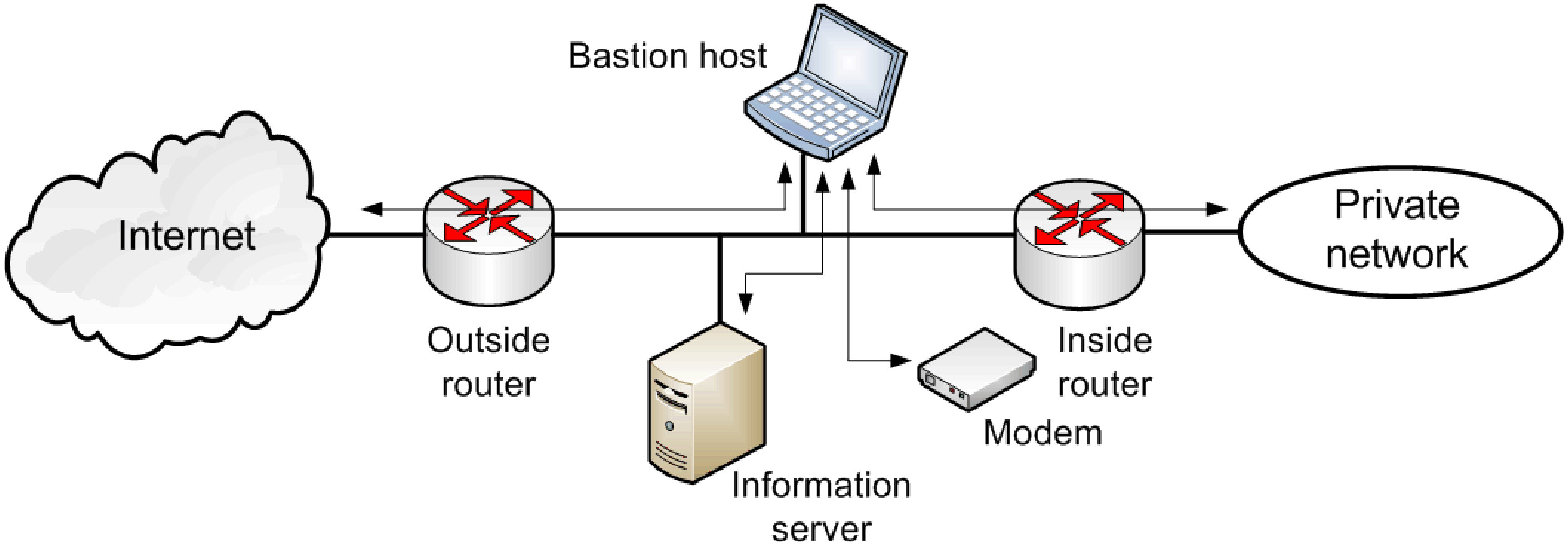
Second, an intruder must generally penetrate two separate systems before the security of the internal network is compromised.

FIREWALL CONFIGURATIONS



In the single-homed configuration just described, if the packet-filtering router is completely compromised, traffic could flow directly through the router between the Internet and other hosts on the private network. The screened host firewall, **dual-homed bastion configuration** physically prevents such a security breach. The advantages of dual layers of security that were present in the previous configuration are present here as well. Again, an information server or other hosts can be allowed direct communication with the router if this is in accord with the security policy.

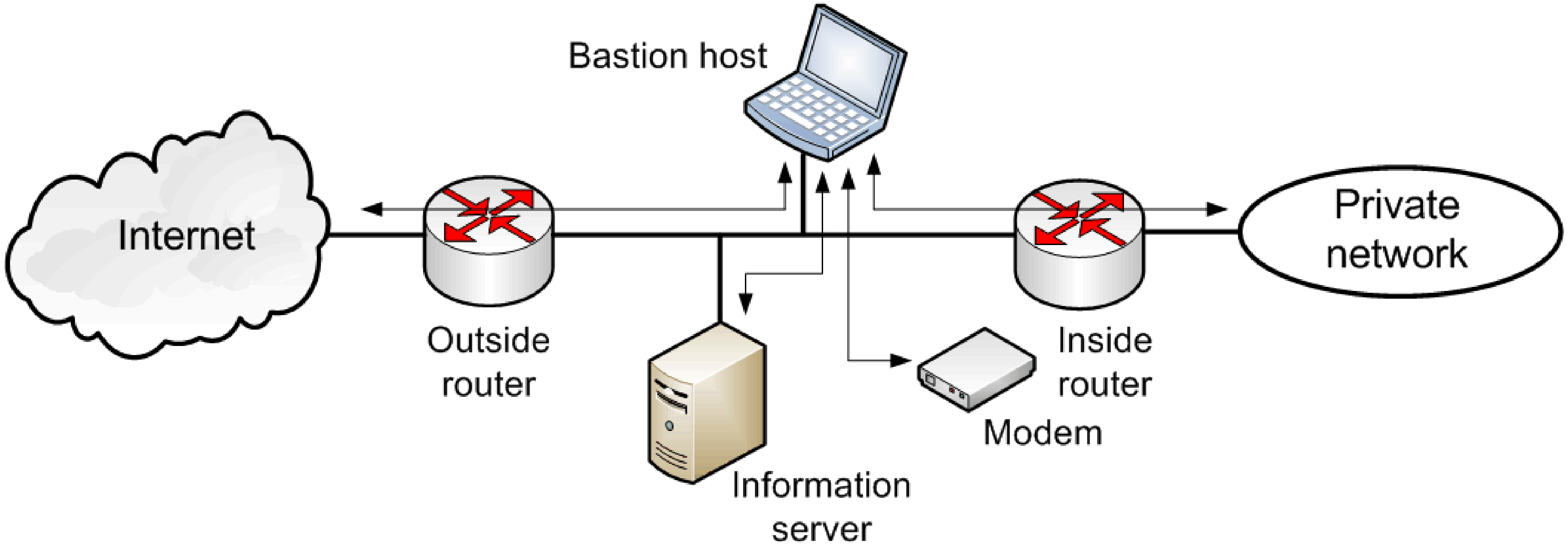
FIREWALL CONFIGURATIONS



The **screened subnet firewall configuration** is the most secure of those we have considered. In this configuration, two packet-filtering routers are used, one between the bastion host and the Internet and one between the bastion host and the internal network. This configuration creates an isolated subnetwork, which may consist of simply the bastion host but may also include one or more information servers and modems for dial-in capability.

Typically, both the Internet and the internal network have access to hosts on the screened subnet, but traffic across the screened subnet is blocked.

FIREWALL CONFIGURATIONS



This configuration offers several advantages:

- There are now three levels of defense to thwart intruders.
- The outside router advertises only the existence of the screened subnet to the Internet; therefore, the internal network is invisible to the Internet.
- Similarly, the inside router advertises only the existence of the screened subnet to the internal network; therefore, the systems on the inside network cannot construct direct routes to the Internet.