CHAPTER - 11

FIREWALLS

- Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.
- The firewall provides an additional layer of defense, insulating the internal systems from external networks following the classic military doctrine of “**defense in depth**”.

Key Points

- A firewall forms a barrier through which the traffic going in each direction must pass.
- A firewall security policy dictates which traffic is authorized to pass in each direction.
- A firewall may be designed to operate as a filter at the level of IP packets, or may operate at a higher protocol layer.

11.1 The Need For Firewalls

- Notable developments in corporations, government agencies, and other organizations have undergone a steady evolution. E.g.
  - Centralized data processing system, with a central mainframe supporting a number of directly connected terminals
  - Local area networks (LANs)
  - Premises network, consisting of a number of LANs
  - Enterprise-wide network
  - Internet connectivity
- Internet connectivity is no longer optional for organizations.
- If this is not provided via their LAN, they will use dial-up capability from their PC to an Internet service provider (ISP).

The Need For Firewalls

- But this also enables the outside world to reach and interact with local network assets.
- Each workstation and server on the premises network can be equipped with intrusion protection system, but this may not be sufficient and in some cases is not cost-effective.
- A widely accepted alternative or at least complement to host-based security services 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.

11.2 Firewall Characteristics

- **Goals for a firewall**
  - 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.
  - Only authorized traffic, as defined by the local security policy, will be allowed to pass.
  - There are number of types of firewalls with various types of security polices.
  - The firewall itself is immune to penetration.

Firewall Techniques

- General techniques that firewalls use to control access and enforce the site's security policy are:
- **Service control:** Types of Internet services that can be accessed, inbound or outbound.
- It may filter traffic on the basis of IP address, protocol,
- or 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.
- **Direction control:** the direction in which particular service requests may be initiated and allowed to flow through the firewall.

Firewall Techniques

- **User control:** Controls access to a service according to which user is attempting to access it, typically applied to users inside the firewall perimeter (local users).
- With secure authentication technology, it may be applied to incoming traffic from external users.
- **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.

Scope of Firewall

- A firewall defines a single choke point, protects against vulnerable services, IP spoofing and routing attacks.
- A firewall provides a location for monitoring security-related events. E.g. Audits and alarms.
- A firewall is a convenient platform for several Internet functions that are not security related. E.g. a n/w address translator, a network management function.
- A firewall can serve as the platform for Ipsec with tunnel mode to implement virtual private networks.

Firewalls Limitations

- The firewall cannot protect against attacks that bypass the firewall
- The firewall may not protect fully against internal threats
- An improperly secured wireless LAN
- A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally

11.3 Types of Firewalls

- A firewall may act as a packet filter.
- It can operate as a positive or negative filter according to certain criteria.
- Depending on the type of firewall, it may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets.

Packet Filtering Firewalls

- A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet
- Filtering rules are based on information contained in a network packet
  - Source IP address
  - Destination IP address
  - 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 firewall with 3 or more ports, which interface the packet came from or which interface the packet is destined for.

Packet Filtering Firewall

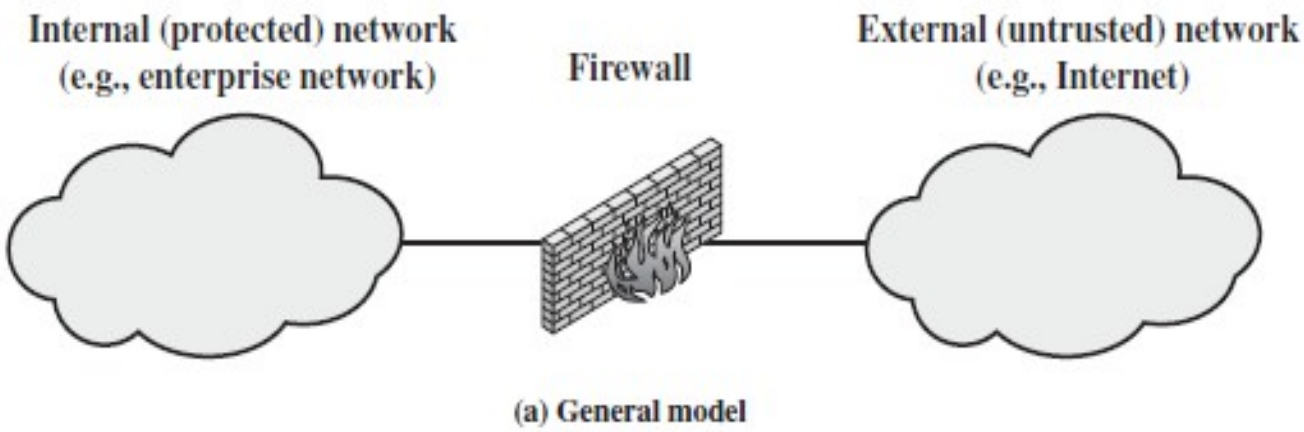
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
- **Two default policies are possible**
  - **Default = discard**: That which is not expressly permitted is prohibited.
  - **Default = forward**: That which is not expressly prohibited is permitted.
  - The default discard policy is more conservative, blocks everything and services must be added on a case-by-case basis.

Packet Filtering Firewall

- Normal users may see firewall as a hindrance. However, this is the policy likely to be preferred by businesses and government organizations.
- The default forward policy increases ease of use for end users but provides reduced security; the security administrator must, in essence, react to each new security threat as it becomes known.
- This policy may be used by generally more open organizations, such as universities.

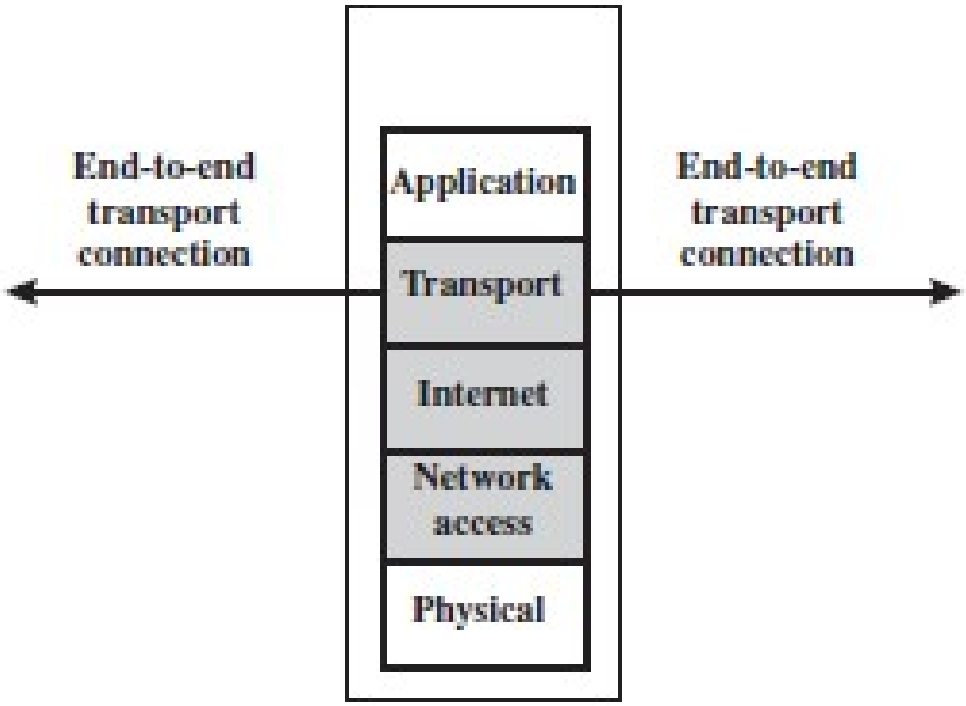
Packet Filtering Firewall

- Table 11.1 gives some examples of packet filtering rulesets.
- In each set, the rules are applied top to bottom. The “*” in a field is a wildcard designator that matches everything.
- We assume that the default = discard policy is in force.



(a) General model

Packet Filtering Firewall



(b) Packet filtering firewall

Table 11.1 Packet-Filtering Examples

Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Packet Filtering Firewall

- One advantage of a packet filtering firewall is its simplicity.
- Also, packet filters typically are transparent to users and are very fast.
- **Weaknesses of packet filter firewalls**
  - They cannot prevent attacks that employ application-specific vulnerabilities or functions.
  - Limited information available to the firewall
  - Most packet filter firewalls do not support advanced user authentication schemes
  - Network layer address spoofing
  - Packet filter firewalls are susceptible to security breaches caused by improper configurations

Packet Filtering Firewall

- Some of the attacks that can be made on packet filtering firewalls and the appropriate countermeasures are the following
  - IP address spoofing
  - Source routing attacks
  - Tiny fragment attacks

Stateful Inspection Firewalls

- A traditional packet filter makes filtering decisions on an individual packet basis rather than any higher layer context.
- A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, as shown in Table 11.2.
- There is an entry for each currently established connection.
- The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.

Stateful Inspection Firewalls

Table 11.2 Example Stateful Firewall Connection State Table [WACK02]

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

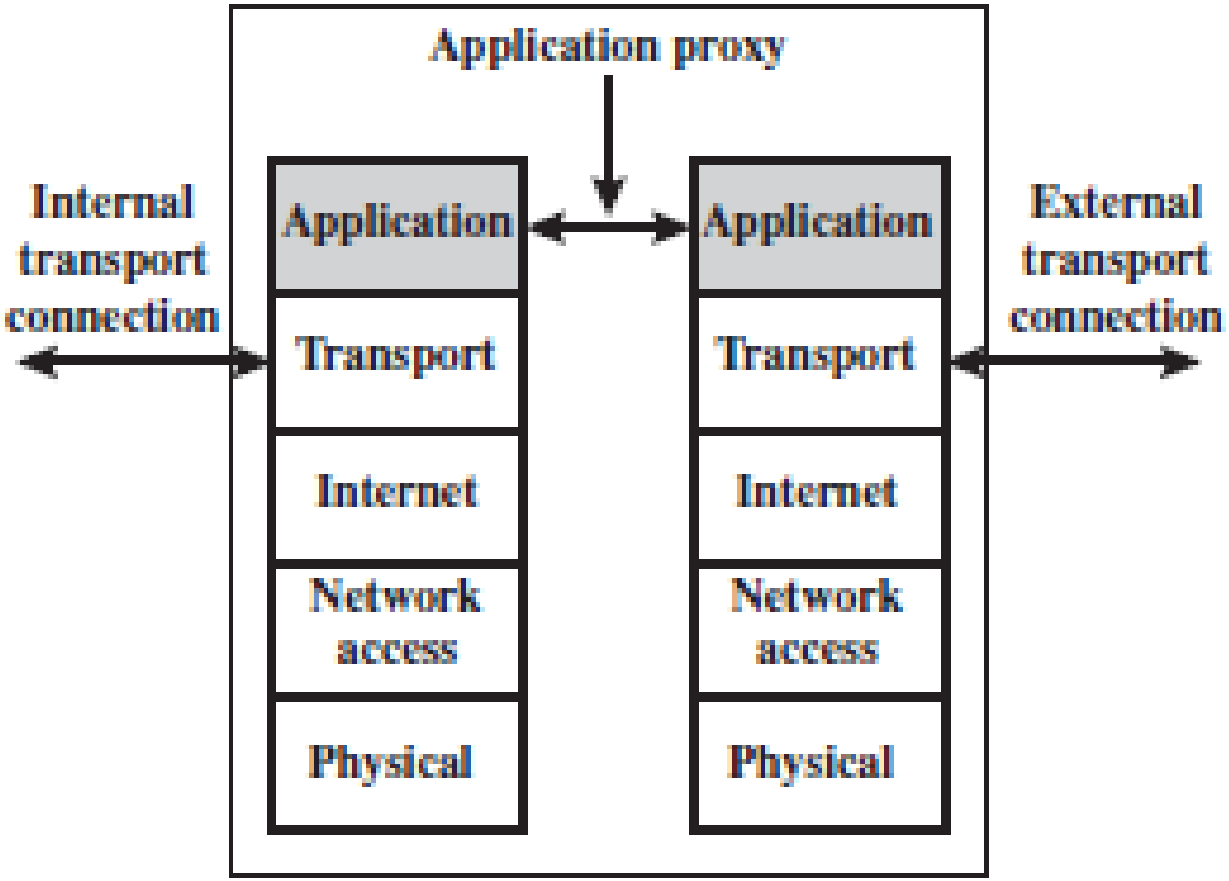
Application-Level Gateway

- An application-level gateway, also called an application proxy, 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.
- When the user 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.

Application-Level Gateway

- The gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features.
- The service which is not supported, cannot be forwarded across the firewall.
- Application-level gateways tend to be more secure than packet filters.
- A prime disadvantage of this type of gateway is the additional processing overhead on each connection.

Application-Level Gateway



(d) Application proxy firewall

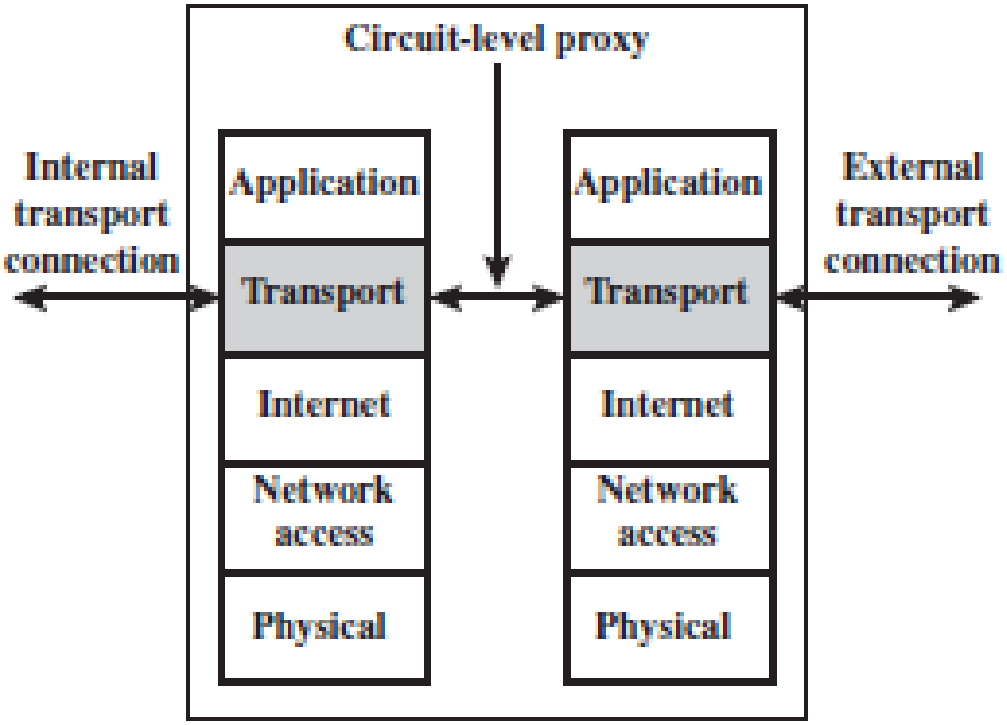
Circuit-Level Gateway

- This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications.
- As with an application gateway, 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 where 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.
- The gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.

Circuit-Level Gateway



(e) Circuit-level proxy firewall

11.4 Firewall Basing

- It is common to base a firewall on a stand-alone machine running a common operating system, such as UNIX or Linux.
- Firewall functionality can also be implemented as a software module in a router or LAN switch.
- The bastion host serves as a platform for an application-level or circuit-level gateway. Common characteristics of a bastion host are as follows:

Bastion Host

- The bastion host hardware platform executes a secure version of its operating system, making it a hardened system.
- Only the services that the network administrator considers essential are installed on the bastion host. E.g. proxy applications for DNS, FTP, HTTP, and SMTP.
- The bastion host may require additional authentication to get 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 for discovering and terminating intruder attacks.
- Each proxy module is a very small and simple software and so easy to check security flaws.
- For example, a typical UNIX mail application may contain over 20,000 lines of code, while a mail proxy may contain fewer than 1000.
- Each proxy is independent of others. In case of problem in any proxy operation or vulnerability, it can be uninstalled without any side effects to other proxy applications.
- If a new service support is required, the network administrator can easily install the required proxy on the bastion host.

Bastion Host

- A proxy generally performs no disk access other than to read its initial configuration file.
- Hence, the portions of the file system containing executable code can be made read only making 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.

Host-Based Firewalls

- A host-based firewall is a software module used to secure an individual host.
- Such modules are available in many operating systems or can be provided as an add-on package.
- Like conventional stand-alone firewalls, host-resident firewalls filter and restrict the flow of packets. A common location for such firewalls is a server.

Host-Based Firewalls

- **Advantages**
- Filtering rules can be tailored to the host environment with specific corporate security policies and with different filters for servers used for different application.
- Protection is provided independent of topology. Thus both internal and external attacks must pass through the firewall.
- Used in conjunction with stand-alone firewalls, the host-based firewall provides an additional layer of protection.
- A new type of server can be added to the network, with its own firewall, without the necessity of altering the network firewall configuration.

A Personal Firewall

- A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side, used in the home environment and on corporate intranets.
- Firewall functionality can also be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface.
- Personal firewall is much less complex than either server-based firewalls or stand-alone firewalls

A Personal Firewall

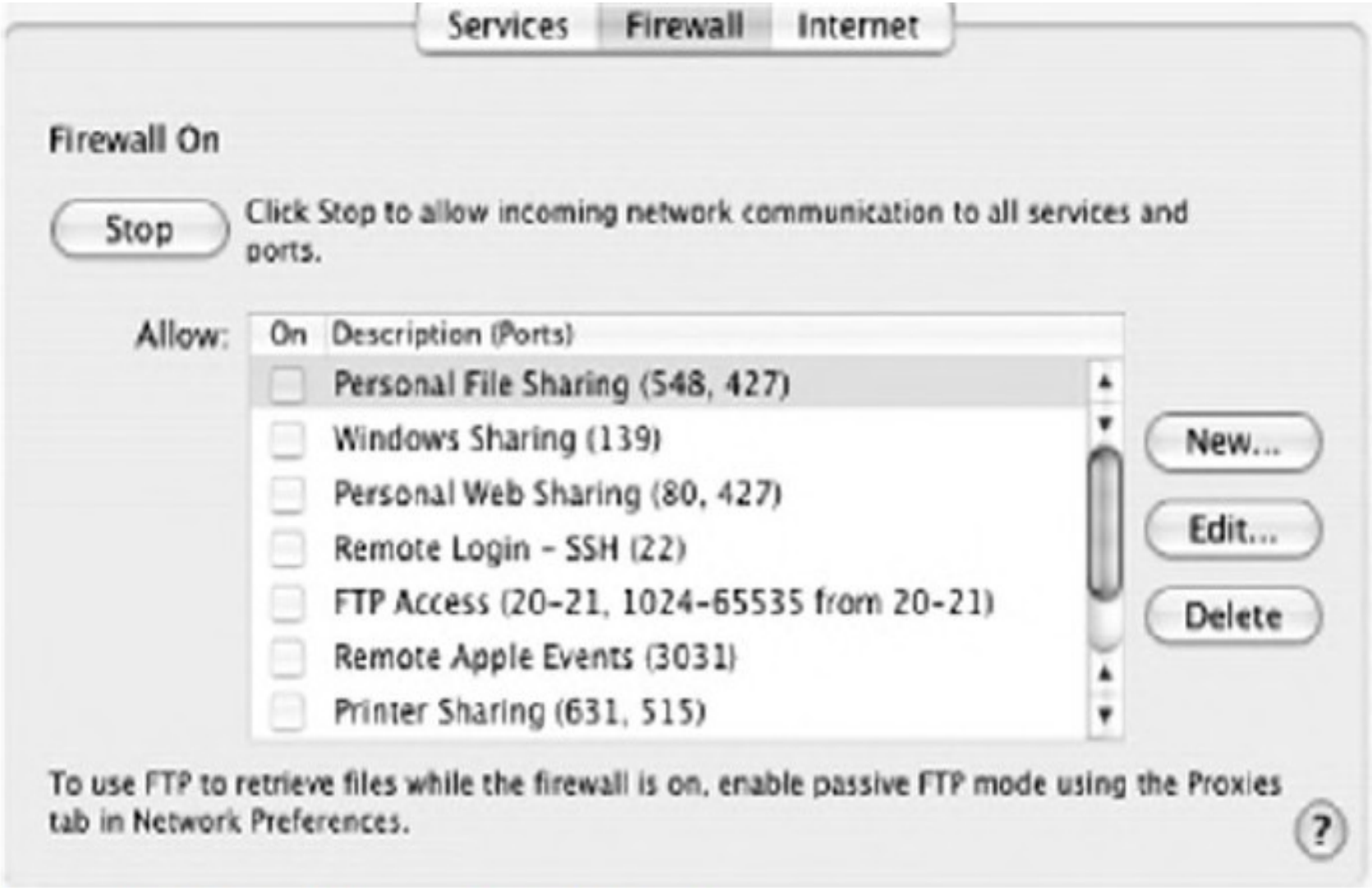


Figure 11.2 Example Personal Firewall Interface

11.5 Firewall Location and Configurations

- **DMZ Networks (demilitarized zone)**
  - External firewall
  - Internal firewall
  - DMZ (demilitarized zone) network

Firewall Location and Configurations

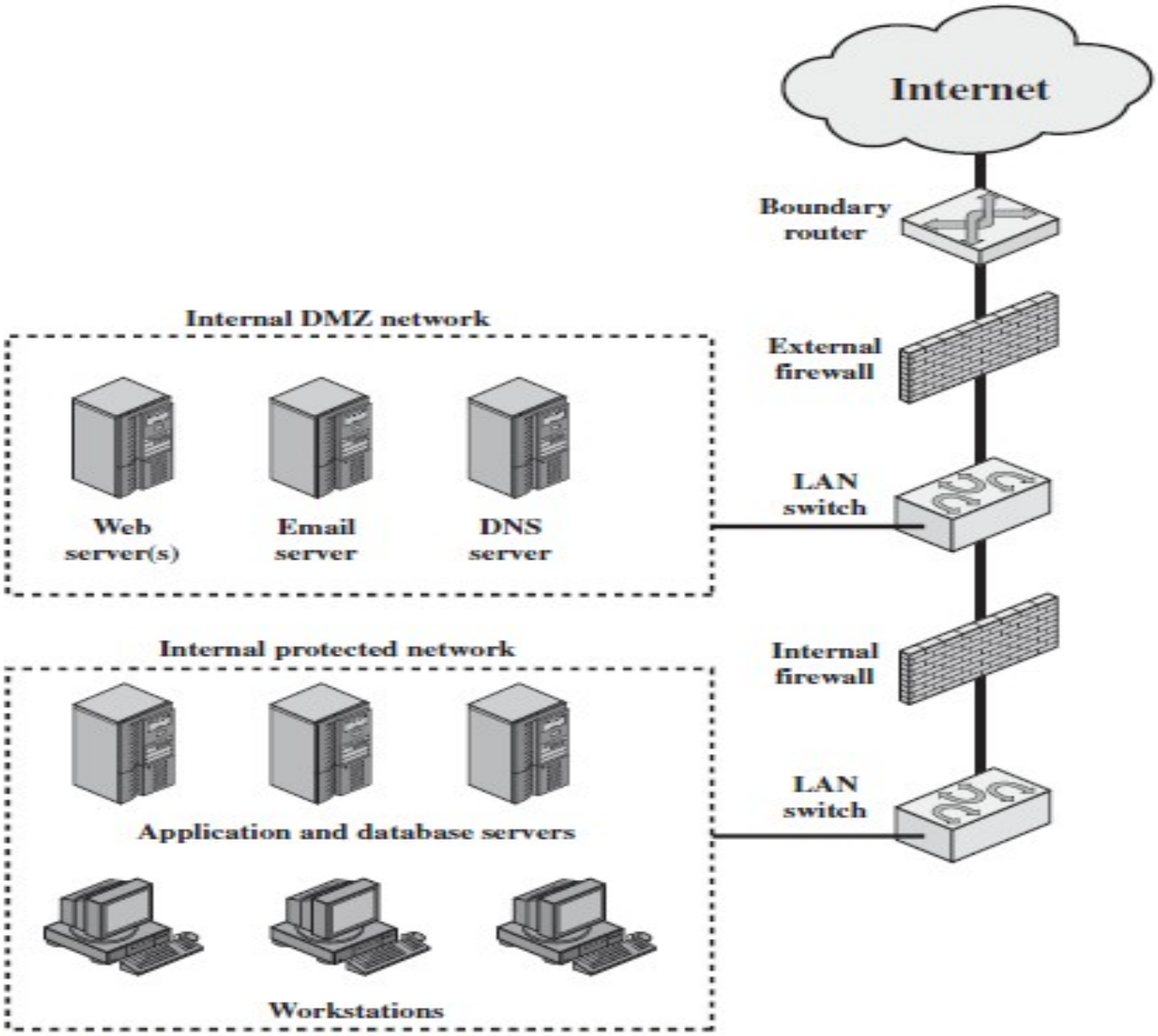


Figure 11.3 Example Firewall Configuration

Virtual Private Networks

- VPN consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security.
- At each corporate site, workstations, servers, and databases are linked by one or more local area networks (LANs).

Virtual Private Networks

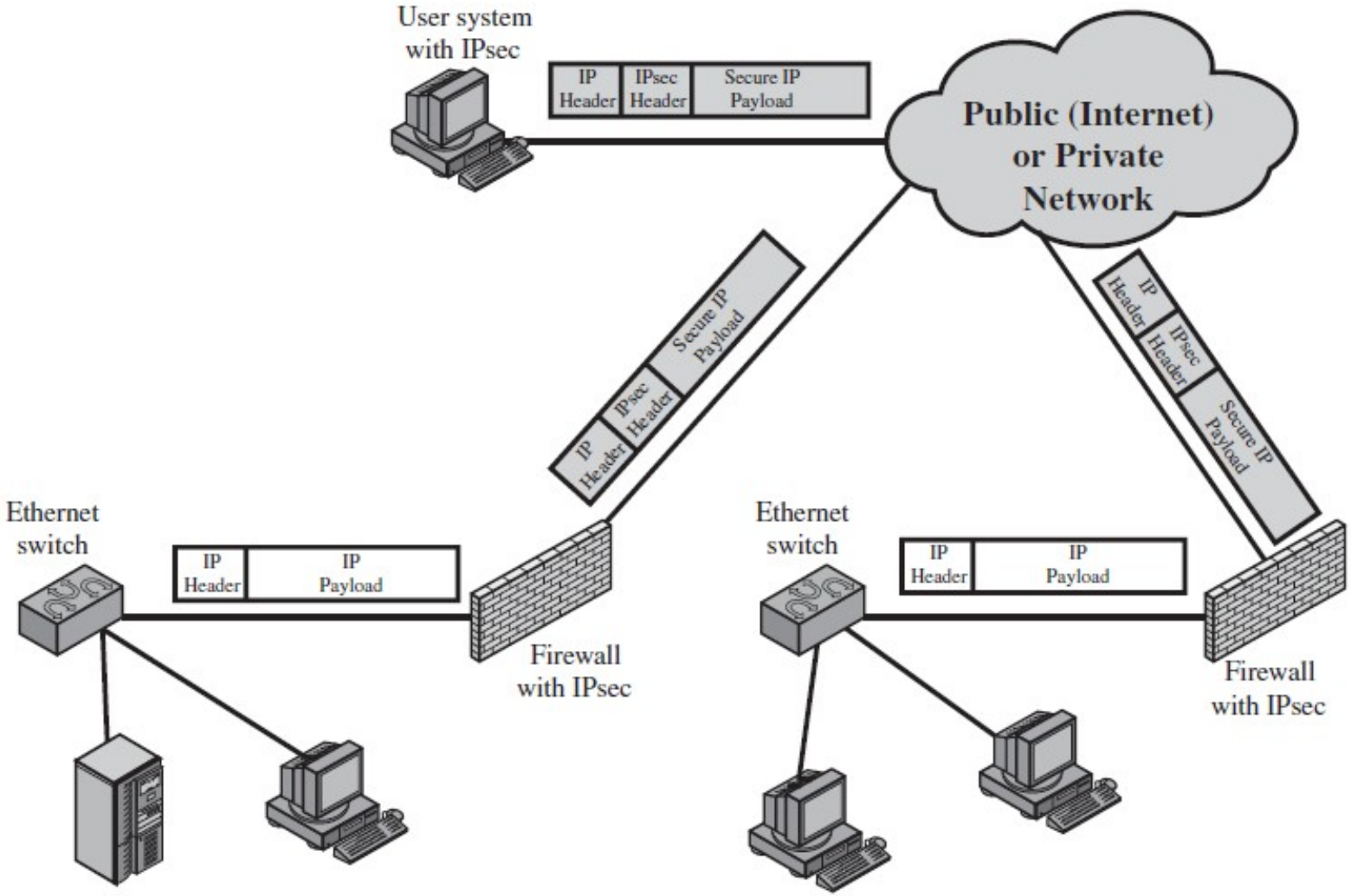


Figure 11.4 A VPN Security Scenario

Distributed Firewalls

- A distributed firewall configuration involves stand-alone firewall devices plus host-based firewalls working together under a central administrative control.
- Administrators can configure host-resident firewalls on hundreds of servers and workstations as well as configure personal firewalls on local and remote user systems.
- Distributed firewall monitoring of log aggregation and analysis, firewall statistics, and fine-grained remote monitoring of individual hosts if needed.

Distributed Firewalls

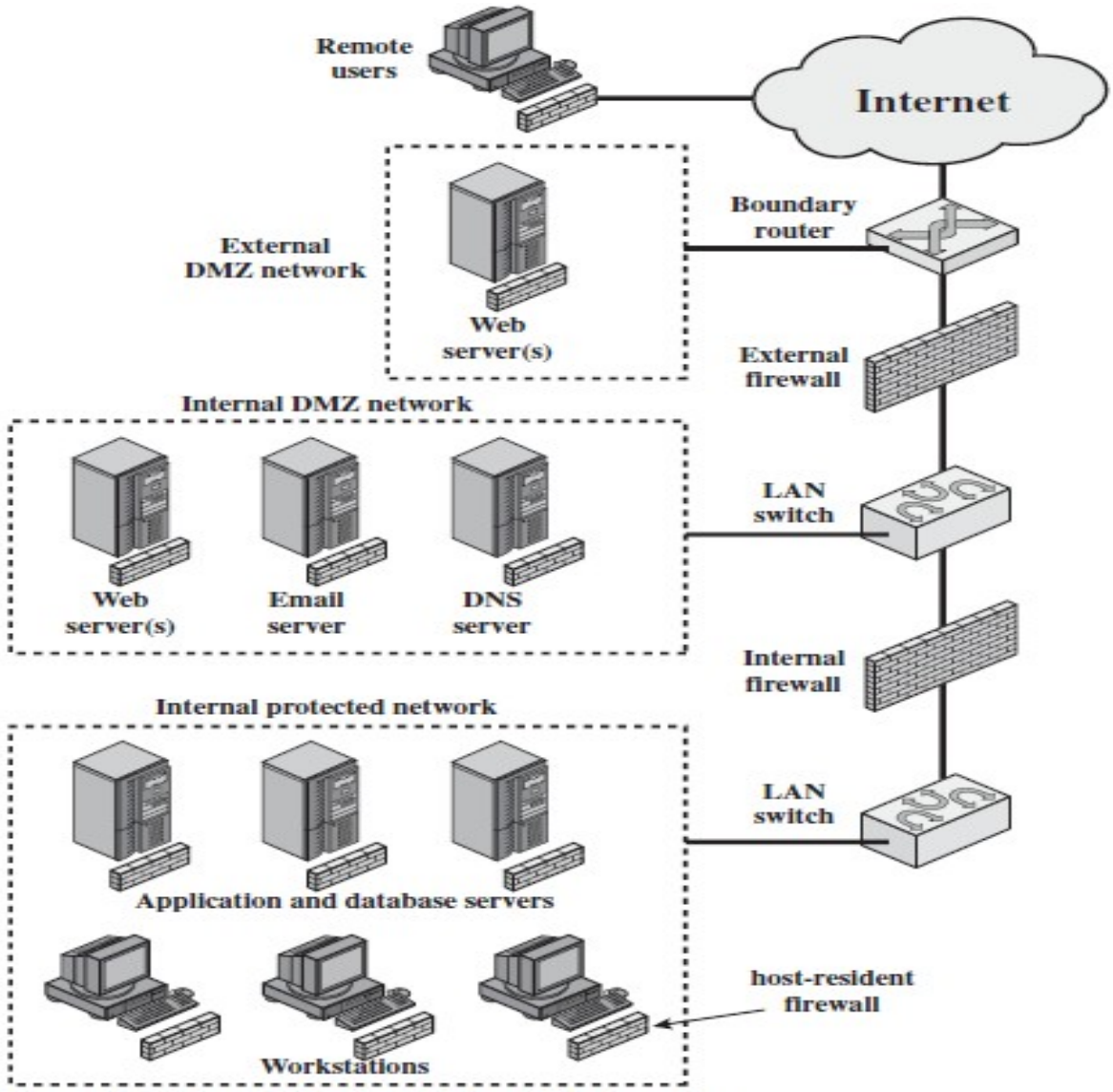


Figure 11.5 Example Distributed Firewall Configuration