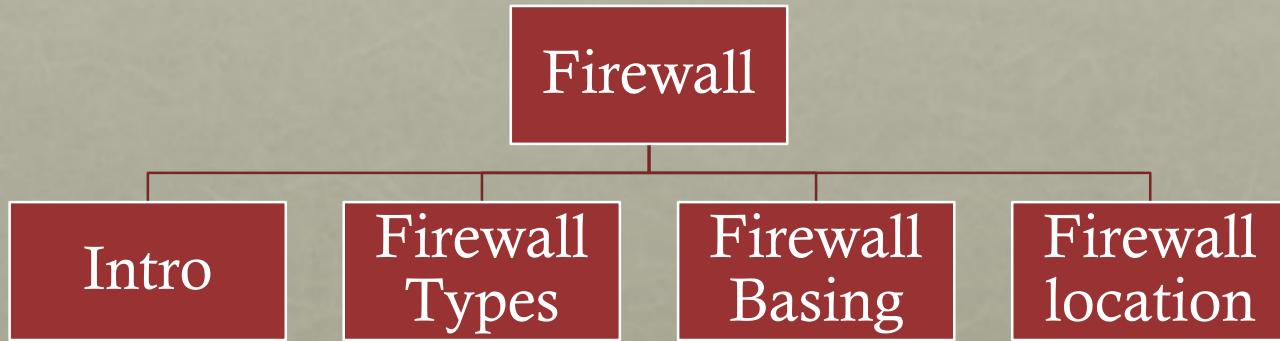


CHAPTER 12

Firewalls

OUTLINE



THE NEED FOR FIREWALLS

- Internet connectivity is no longer optional for organizations
- 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, this may not be sufficient and in some cases is not cost-effective
- Firewall
 - An alternative, or at least complement, to host-based security services
 - 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 auditing can be imposed
 - 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:
 - All traffic from inside to outside, and vice versa, must pass through the firewall
 - Only authorized traffic, as defined by the local security policy, will be allowed to pass
 - The firewall itself is immune to penetration
- Characteristics that a firewall access policy could use to filter traffic:

IP Address and Protocol Values

- Controls access based on the source or destination addresses and port numbers, direction of flow being inbound or outbound, and other network and transport layer characteristics

Application Protocol

- Controls access on the basis of authorized application protocol data

User Identity

- Controls access based on the user's identity, typically for inside users who identify themselves using some form of secure authentication technology, such as IPSec

Network Activity

- Controls access based on considerations such as the time or request

FIREWALL EXPECTATIONS

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

Provides a location for monitoring security-related events

A firewall

Is a convenient platform for several Internet functions that are not security related

Can serve as the platform for IPsec

FIREWALL LIMITATIONS

Cannot protect against attacks that bypass the firewall

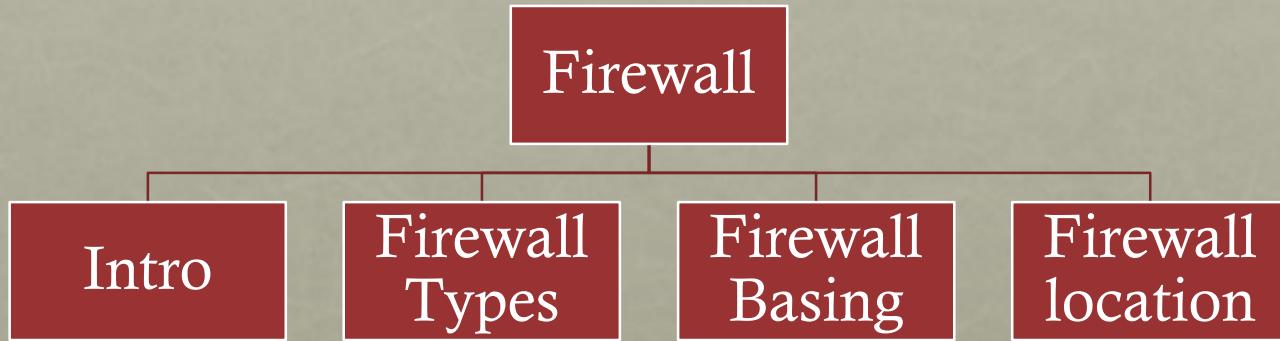
A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally

May not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker

A Firewall

Cannot guard against wireless communications between local systems on different sides of the internal firewall

OUTLINE



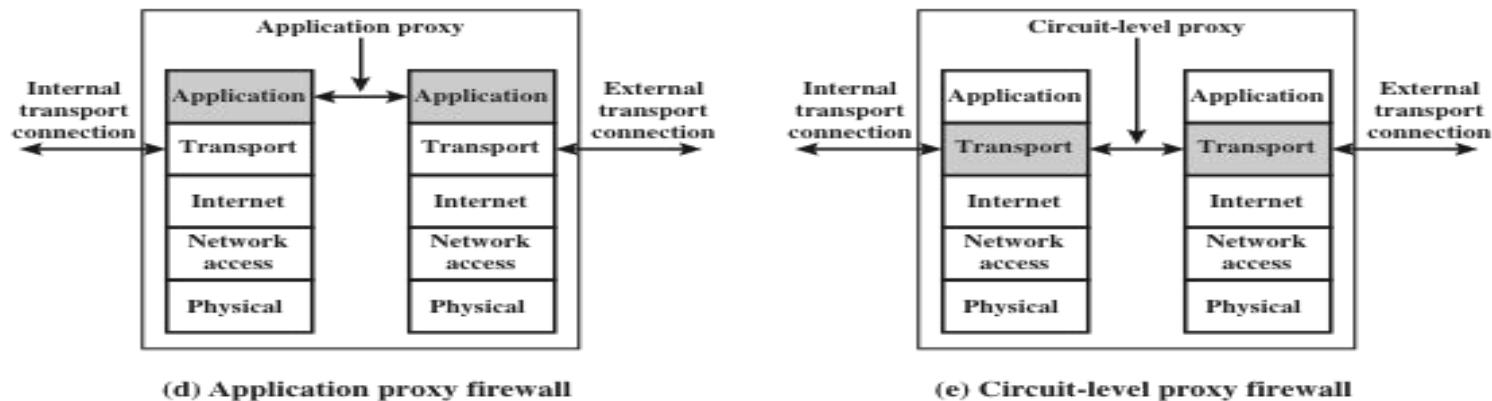
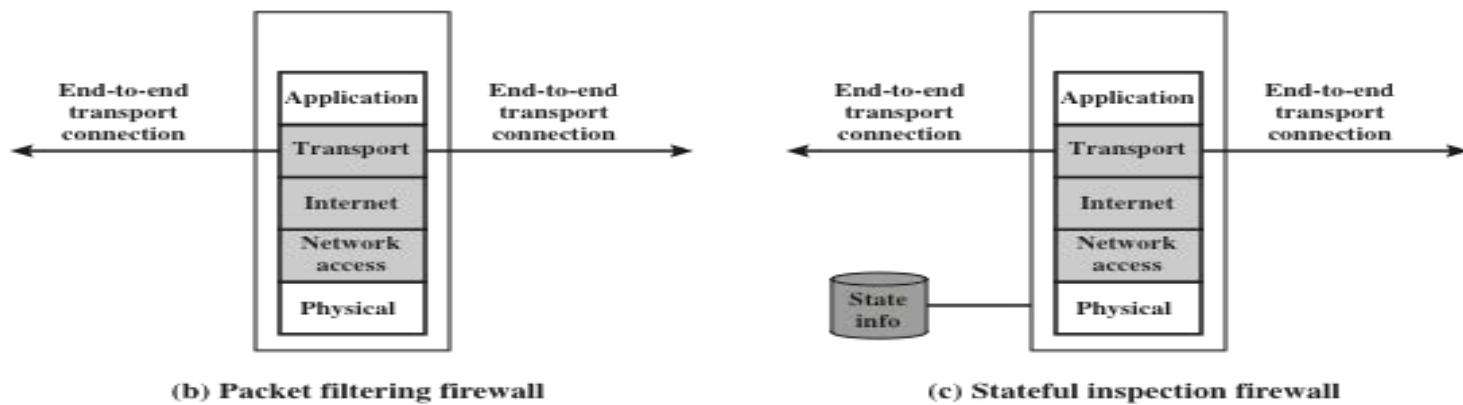
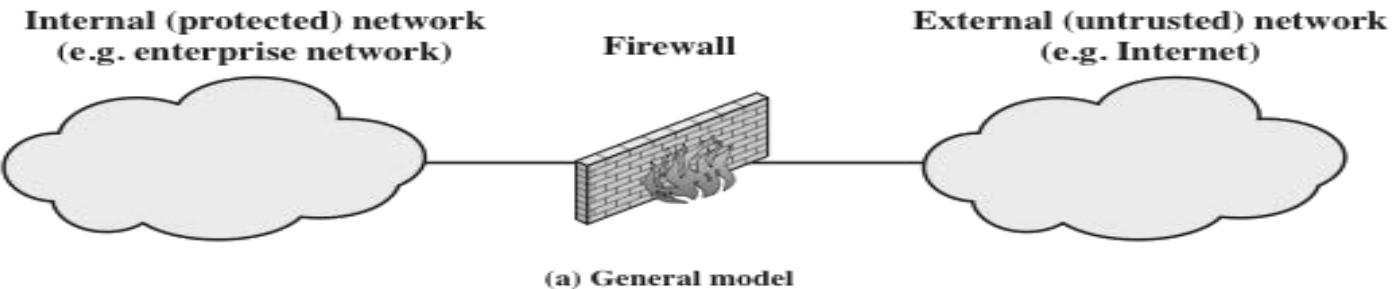


Figure 12.1 Types of Firewalls

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Table 12.1
Packet-Filtering Example

PACKET FILTERING FIREWALLS

Weaknesses

- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions
- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited
- Most packet filter firewalls do not support advanced user authentication schemes
- Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack
- Due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations

Strengths

- Its simplicity
- Transparent to users and are very fast

ATTACKS AND COUNTERMEASURES

IP address spoofing

The intruder transmits packets from the outside with a source IP address field containing an address of an internal host

Countermeasure is to discard packets with an inside source address if the packet arrives on an external interface

Source routing attacks

The source station specifies the route that a packet should take as it crosses the internet, in the hopes that this will bypass security measures that do not analyze the source routing information

Countermeasure is to discard all packets that use this option

Tiny fragment attacks

The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment

Countermeasure is to enforce a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header

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

Table 12.2
Example Stateful Firewall Connection State Table [SCAR09b]

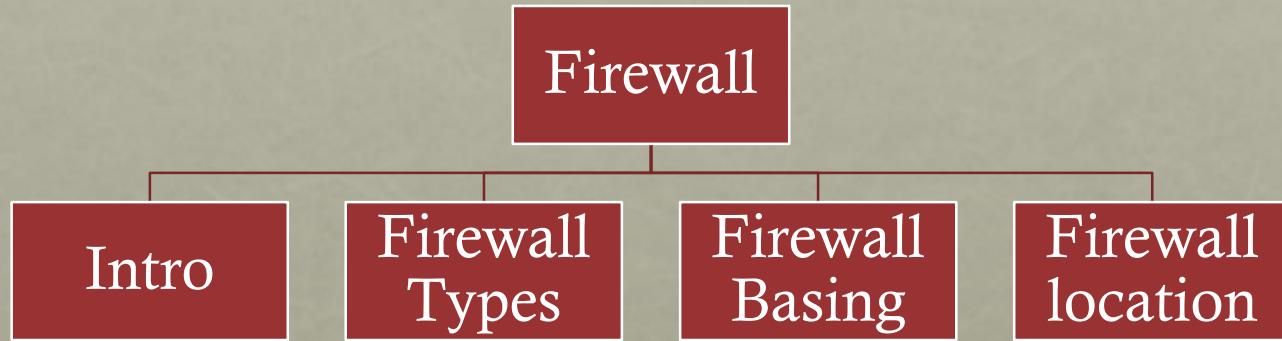
APPLICATION LEVEL GATEWAY

- Also called an *application proxy*
- Acts as a relay of application-level traffic
- 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
- The gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features
- Creates two connections and could require authentication.
- Tend to be more secure than packet filters
- Disadvantage:
 - The additional processing overhead on each connection

CIRCUIT-LEVEL GATEWAY

- Also called *circuit-level proxy*
- *Runs on the session layer*
- Can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications
- Does not permit an end-to-end TCP connection
- The security function consists of determining which connections will be allowed
- Typical use 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

OUTLINE



BASTION HOST

- A system identified by the firewall administrator as a critical strong point in the network's security
- Typically serves as a platform for an application-level or circuit-level gateway
- Common characteristics:
 - Executes a secure version of its operating system, making it a hardened system
 - Only the services that the network administrator considers essential are installed
 - May require additional authentication before a user is allowed access to the proxy services
 - 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
 - Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection
 - Each proxy module is a very small software package specifically designed for network security
 - Each proxy is independent of other proxies on the bastion host
 - A proxy generally performs no disk access other than to read its initial configuration file
 - Each proxy runs as a nonprivileged user in a private and secured directory on the bastion host

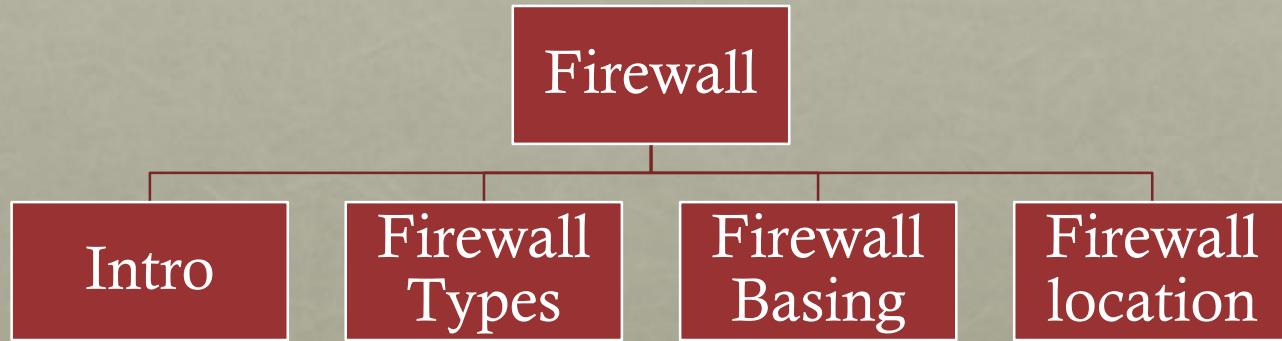
HOST-BASED FIREWALL

- A software module used to secure an individual host
- Is available in many operating systems or can be provided as an add-on package
- Filters and restricts the flow of packets
- Common location is a server
- Advantages:
 - Filtering rules can be tailored to the host environment
 - Protection is provided independent of topology
 - Used in conjunction with stand-alone firewalls, provides an additional layer of protection

PERSONAL FIREWALL

- Controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side
- Can be used in the home environment and on corporate intranets
- Typically is a software module on the personal computer
- Can also be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Primary role is to deny unauthorized remote access to the computer
- Can also monitor outgoing activity in an attempt to detect and block worms and other malware

OUTLINE



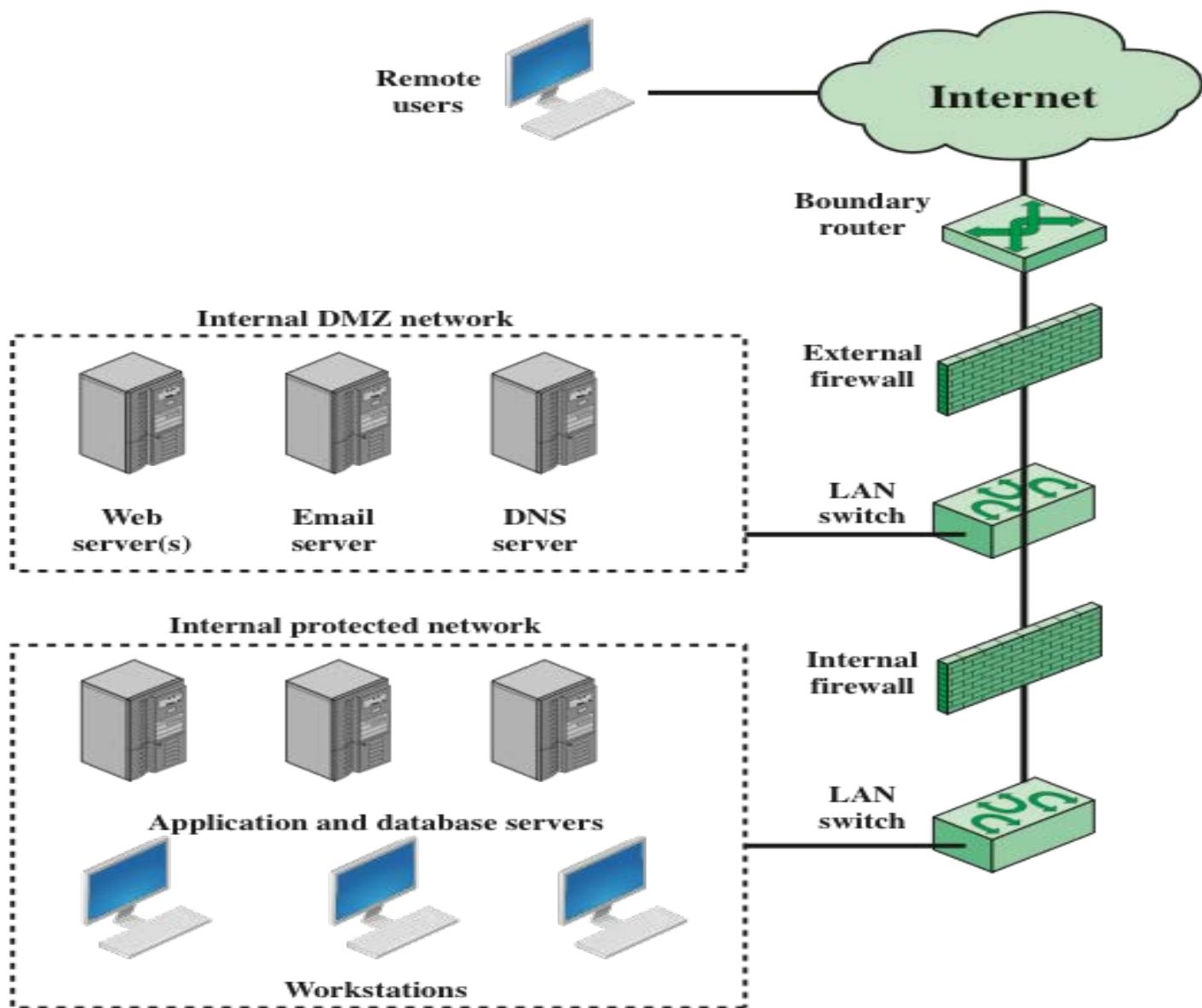


Figure 12.2 Example Firewall Configuration

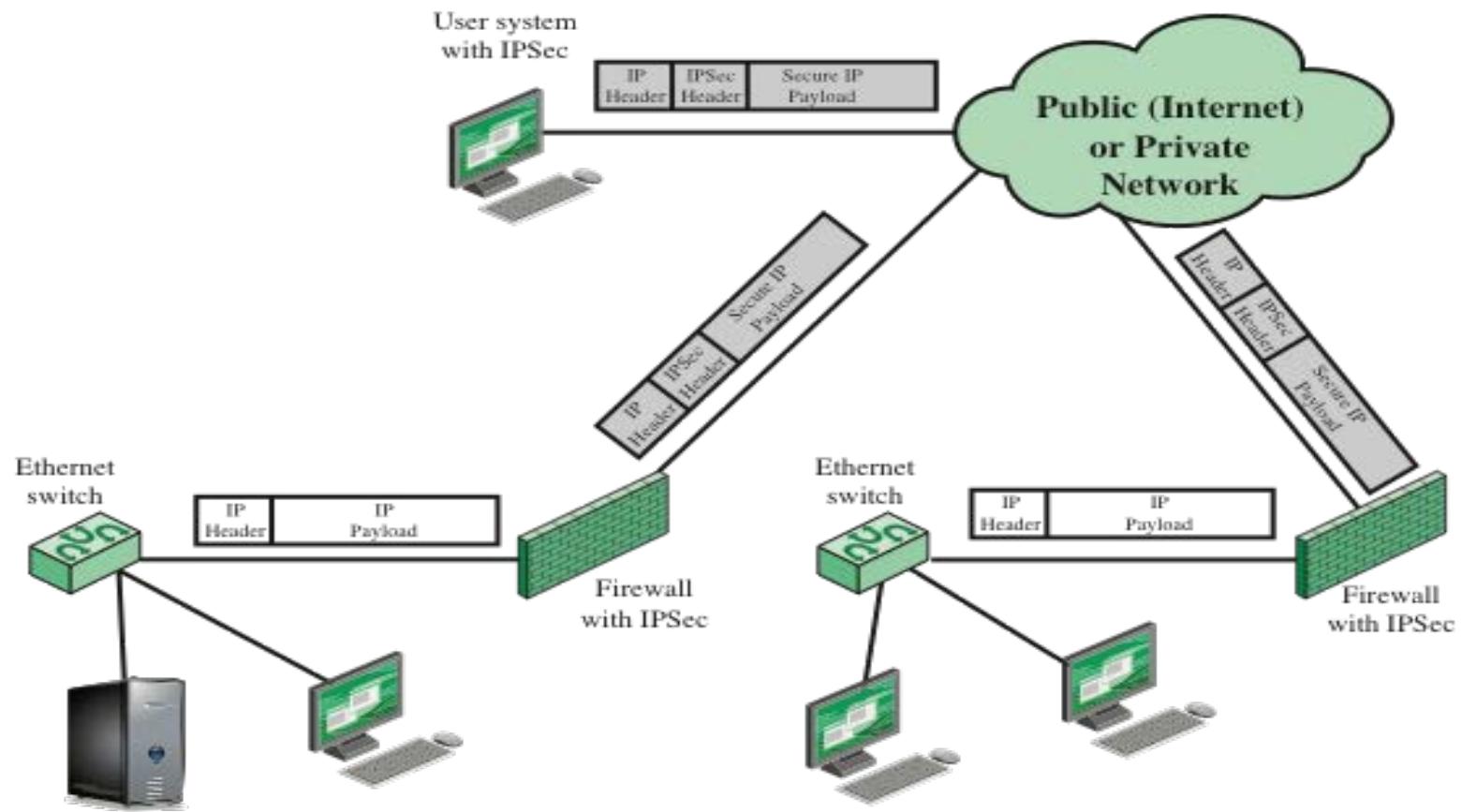


Figure 12.3 A VPN Security Scenario

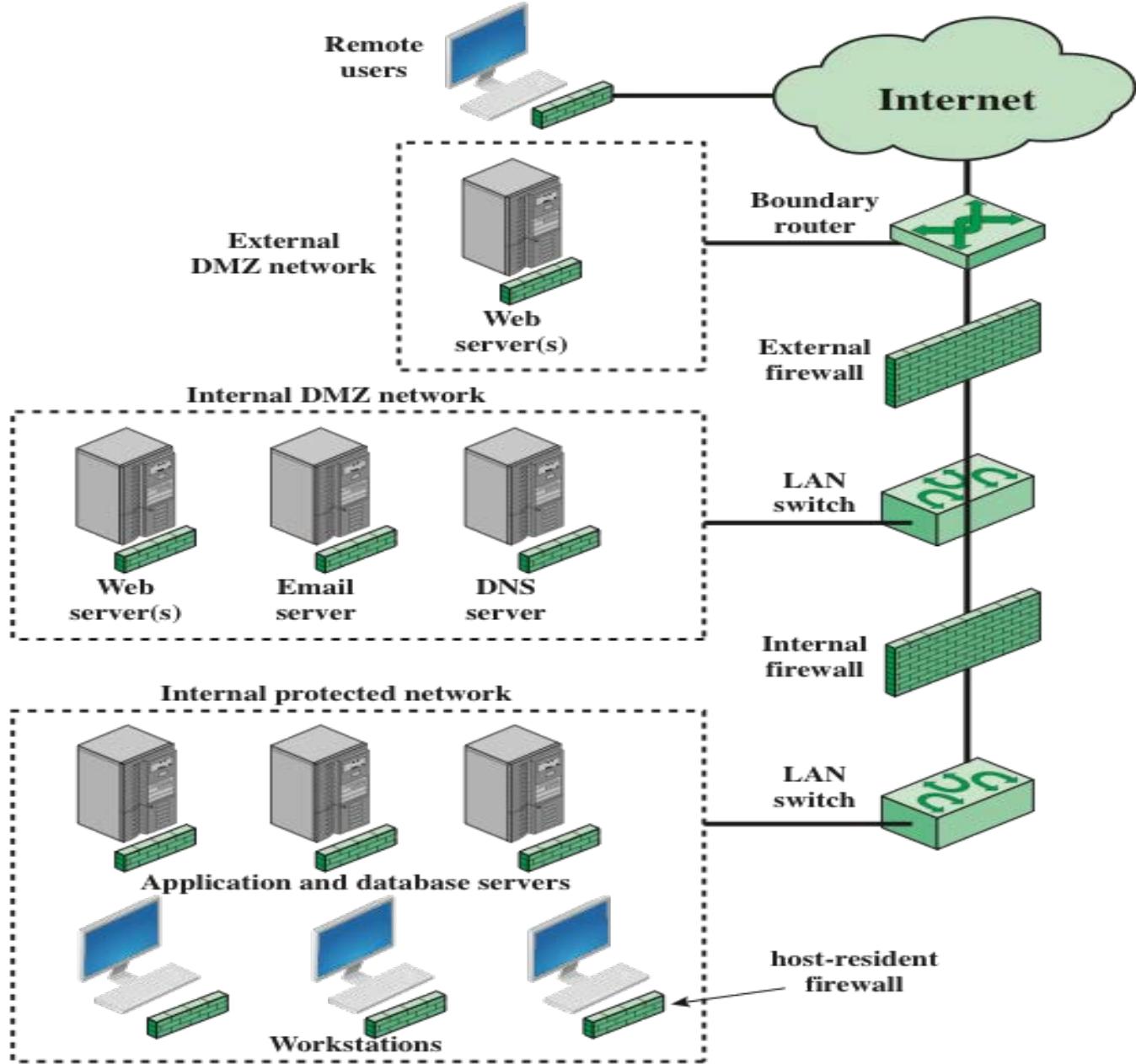


Figure 12.4 Example Distributed Firewall Configuration

SUMMARY OF FIREWALL LOCATIONS AND TOPOLOGIES

- **Host-resident firewall**
 - This category includes personal firewall software and firewall software on servers
 - Can be used alone or as part of an in-depth firewall deployment
- **Screening router**
 - A single router between internal and external networks with stateless or full packet filtering
 - This arrangement is typical for small office/home office (SOHO) applications
- **Single bastion inline**
 - A single firewall device between an internal and external router
 - This is the typical firewall appliance configuration for small-to-medium sized organizations
- **Single bastion T**
 - Similar to single bastion inline but has a third network interface on bastion to a DMZ where externally visible servers are placed
- **Double bastion inline**
 - DMZ is sandwiched between bastion firewalls
- **Double bastion T**
 - DMZ is on a separate network interface on the bastion firewall
- **Distributed firewall configuration**
 - Used by some large businesses and government organizations

SUMMARY

- The need for firewalls
- Firewall characteristics and access policy
- Types of firewalls
 - Packet filtering firewall
 - Stateful inspection firewalls
 - Application level gateway
 - Circuit level gateway
- Firewall basing
 - Bastion host
 - Host based firewalls
 - Personal firewall
- Firewall locations and configurations
 - DMZ networks
 - Virtual private networks
 - Distributed firewalls
 - Firewall location and topologies summary