System and Network Security

Firewalls

Group 4

NAME	REG No	STUDENT No
FAHAD Guma	2021/HD05/2350U	2100702350
MUSA Rahim	2021/HD05/2354U	2100702354
FLORENCE Nanteza	2021/HD05/4137U	2100704137
MUGOYA Dihfahsih	2021/HD05/2353U	2100702353

Overview of the presentation

The Need for Firewalls
Firewall Characteristics
Types of Firewalls

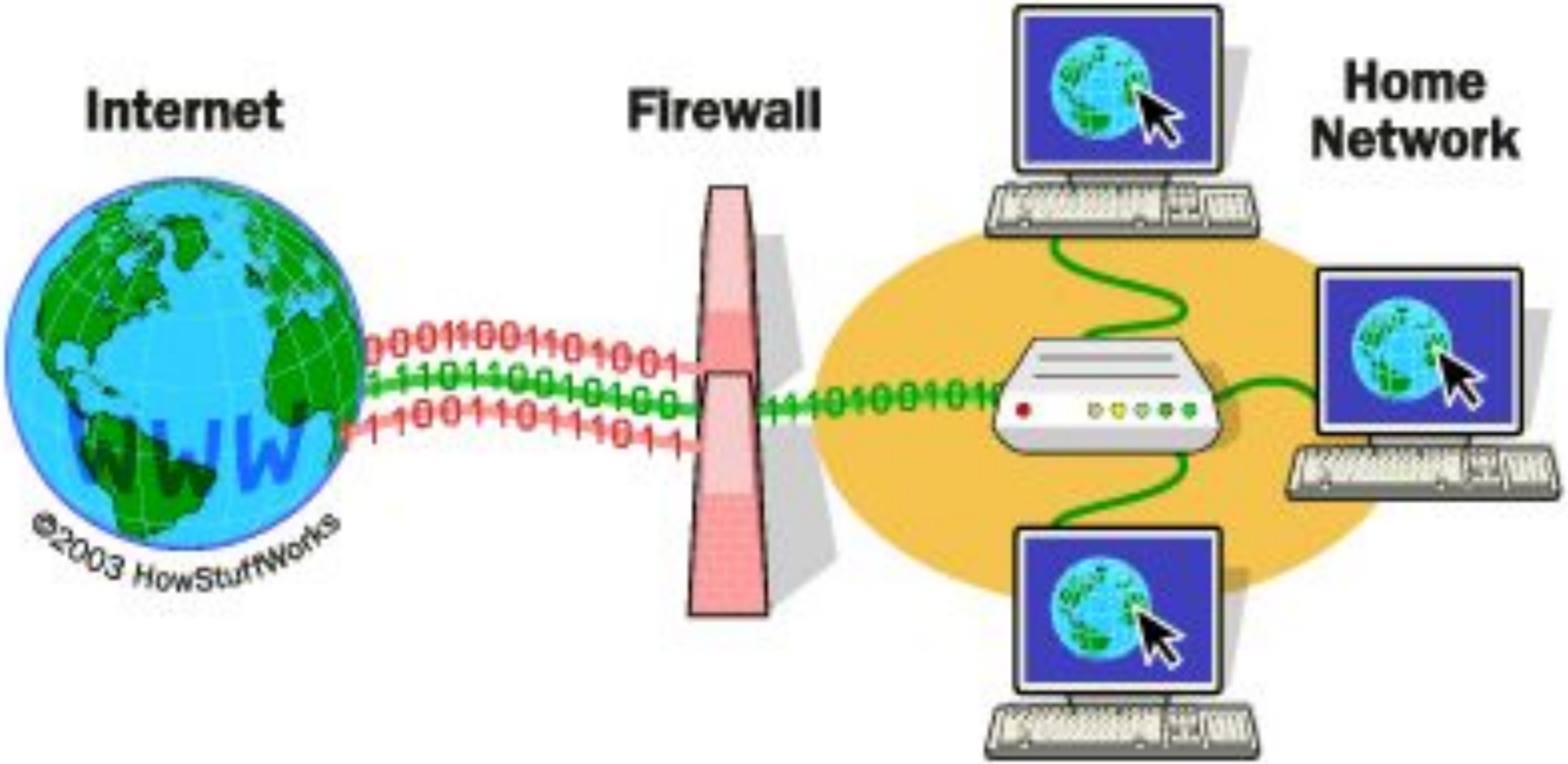
- ❖ Packet Filtering Firewall
- ❖ Stateful Inspection Firewalls
- ❖ Application-Level Gateway

Firewall Basing

- ❖ Bastion Host
- ❖ Host-Based Firewalls
- ❖ Personal Firewall

Firewall Location and Configurations

- ❖ DMZ Networks
- ❖ Virtual Private Networks
- ❖ Distributed Firewalls
- ❖ Summary of Firewall Locations and Topologies


Internet
Firewall
Home
Network
WWW
00011001101001
110110010100
1100110111011
1110100101
©2003 HowStuffWorks

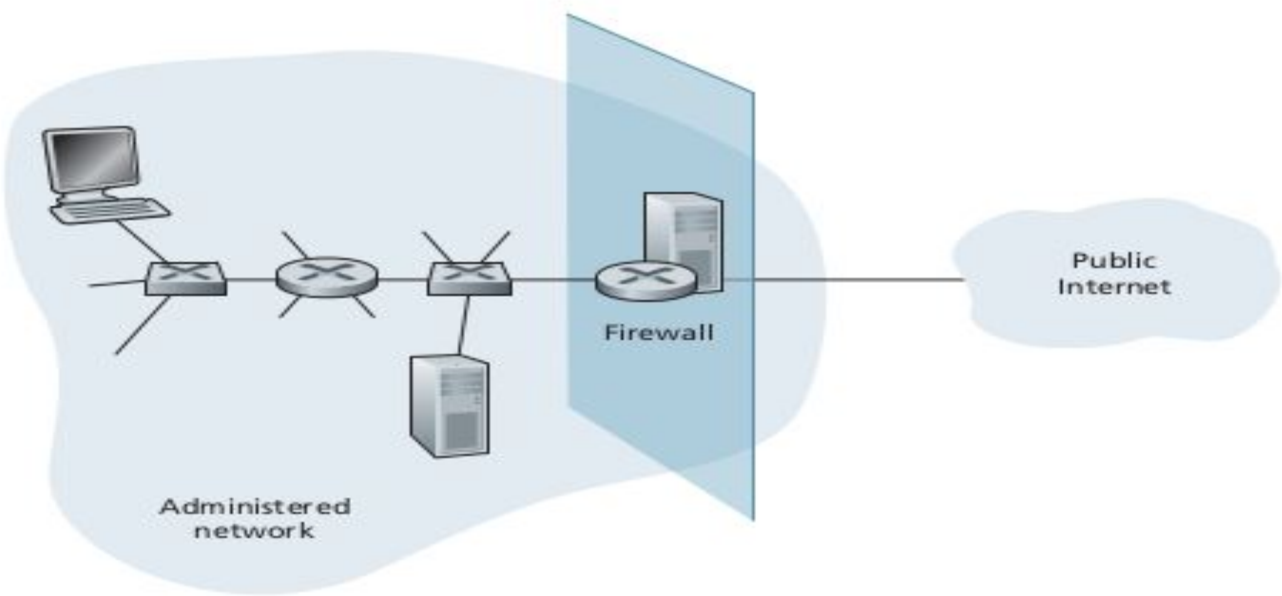
Firewalls

- 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.
- 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 Need For Firewalls

- Information systems in corporations, government agencies, and other organizations have undergone a steady evolution. The following are notable developments:
  - Centralized data processing system, with a central mainframe supporting several directly connected terminals
  - Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe.
  - Premises network, consisting of several 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

Characteristics of firewalls



- All traffic from outside to inside, and vice versa, passes through the firewall. As show in the figure, sitting squarely at the boundary between the administered network and the rest of the internet.
- Large organizations may use multiple levels of firewalls or distributed firewalls.
- Locating a firewall at a single access point to the network, makes it easy to manage and enforce a security-access policy.

- Only authorized traffic as defined by the local security policy , will be allowed to pass.
- The firewall can restrict access to unauthorized traffic.
- Firewall is immune to penetration, it can be compromised if not properly installed and configured hence providing a false sense of security.

A firewall is a security gateway, the Demilitarized Zone (DMZ) is protected from both the outside world and the rest of the cooperate LAN by firewalls.

Firewall functionality can be implemented as a software module in a router or LAN switch

Local configurations include a secure LAN known as a DMZ identified at 1.2.4.0/24.

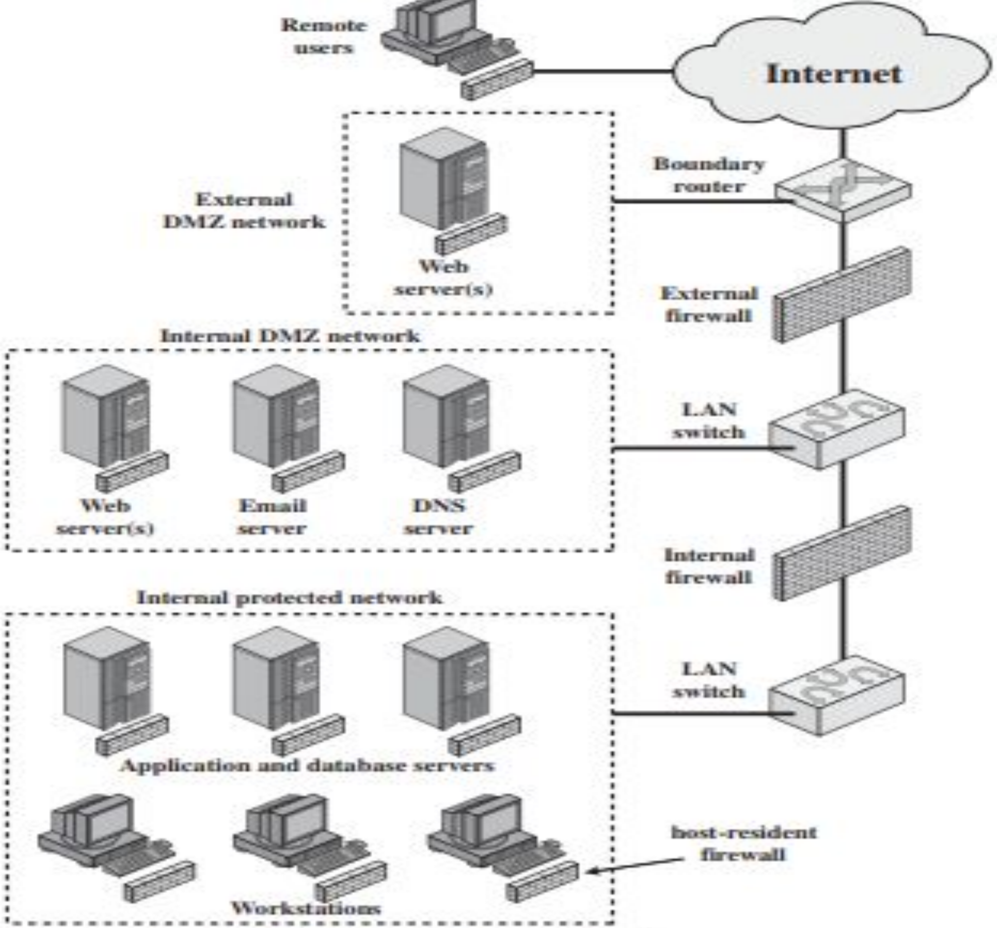


Figure 11.5 Example Distributed Firewall Configuration

Types of Firewalls

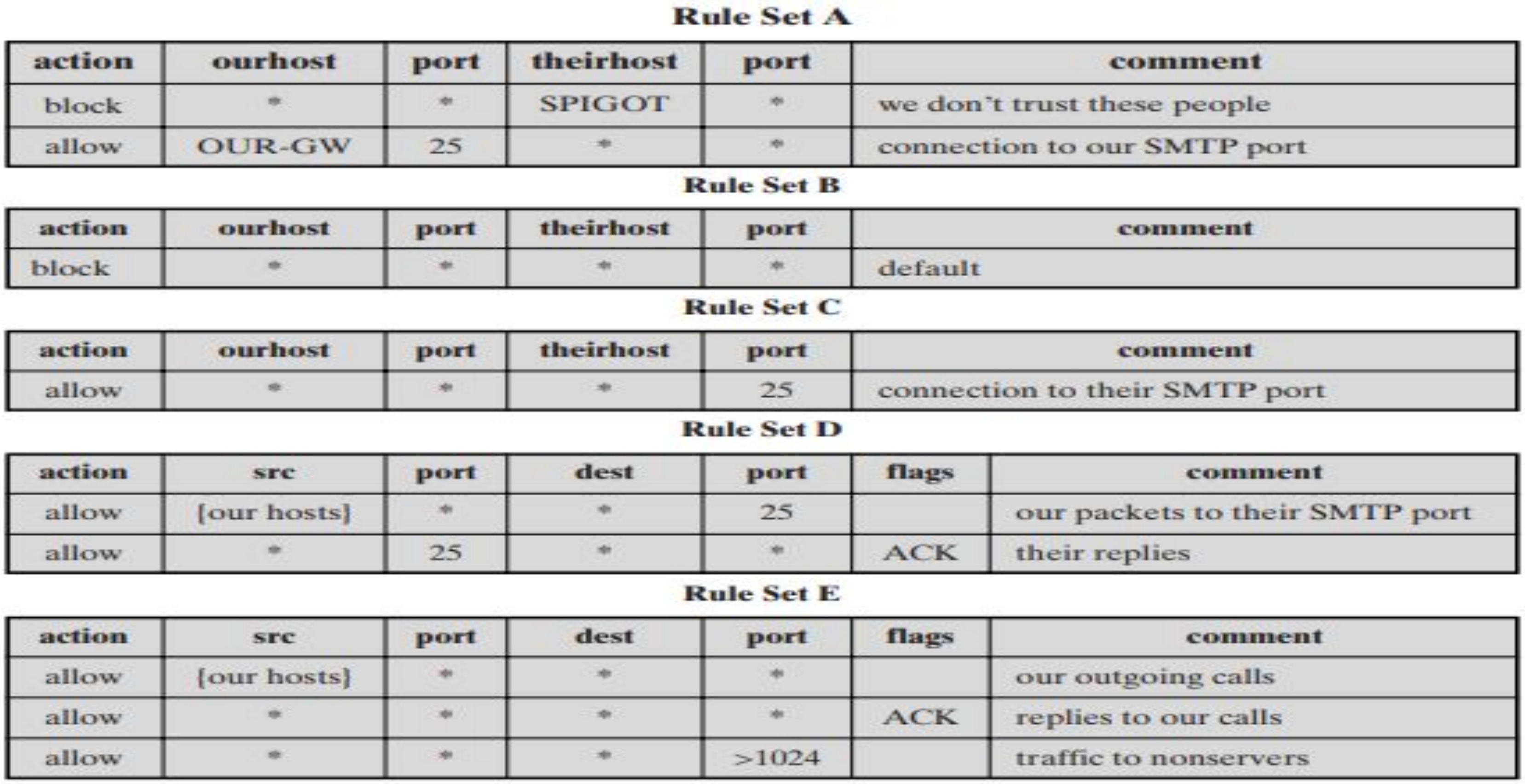
A Packet Filtering Firewall

- A firewall can operate as a positive filter allowing to pass only packets that meet a specific criteria or a negative filter rejecting a packet that meets a certain criteria.
- The firewall is configured to filter packets going from and to the internal network.
- The packet filter is based on the list of rules based on matches in the IP and TCP header if there is a match the rule is invoked to determine whether to forward or discard 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
- IP protocol field – defines the Transport protocol
- Interface for a firewall of three or more ports.

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

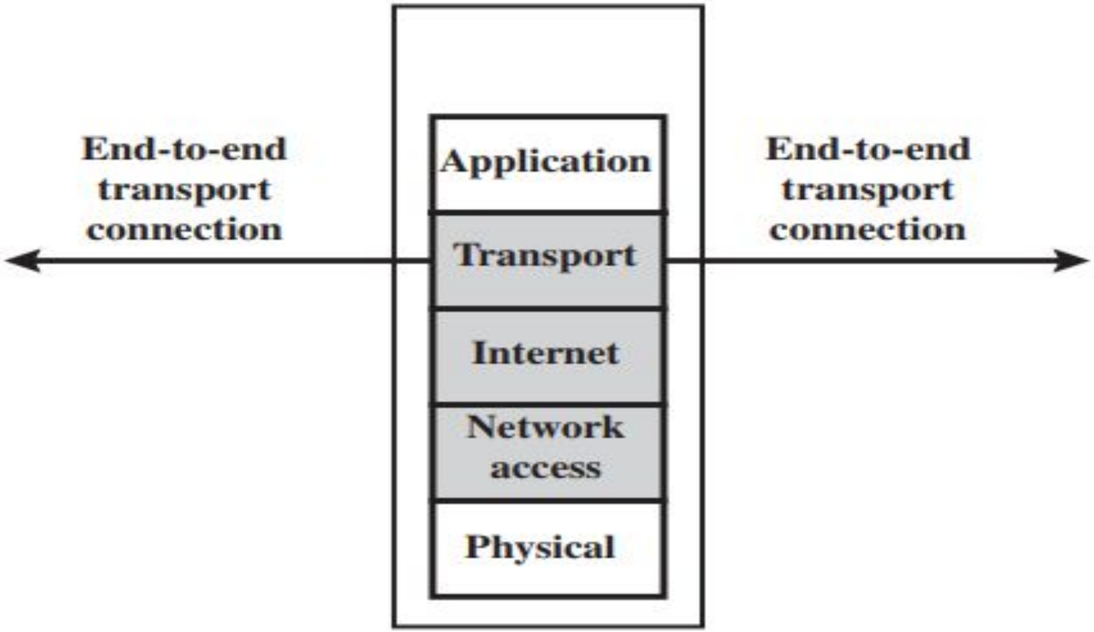
action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

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


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection

(b) Packet filtering firewall

Stateful Inspection firewalls

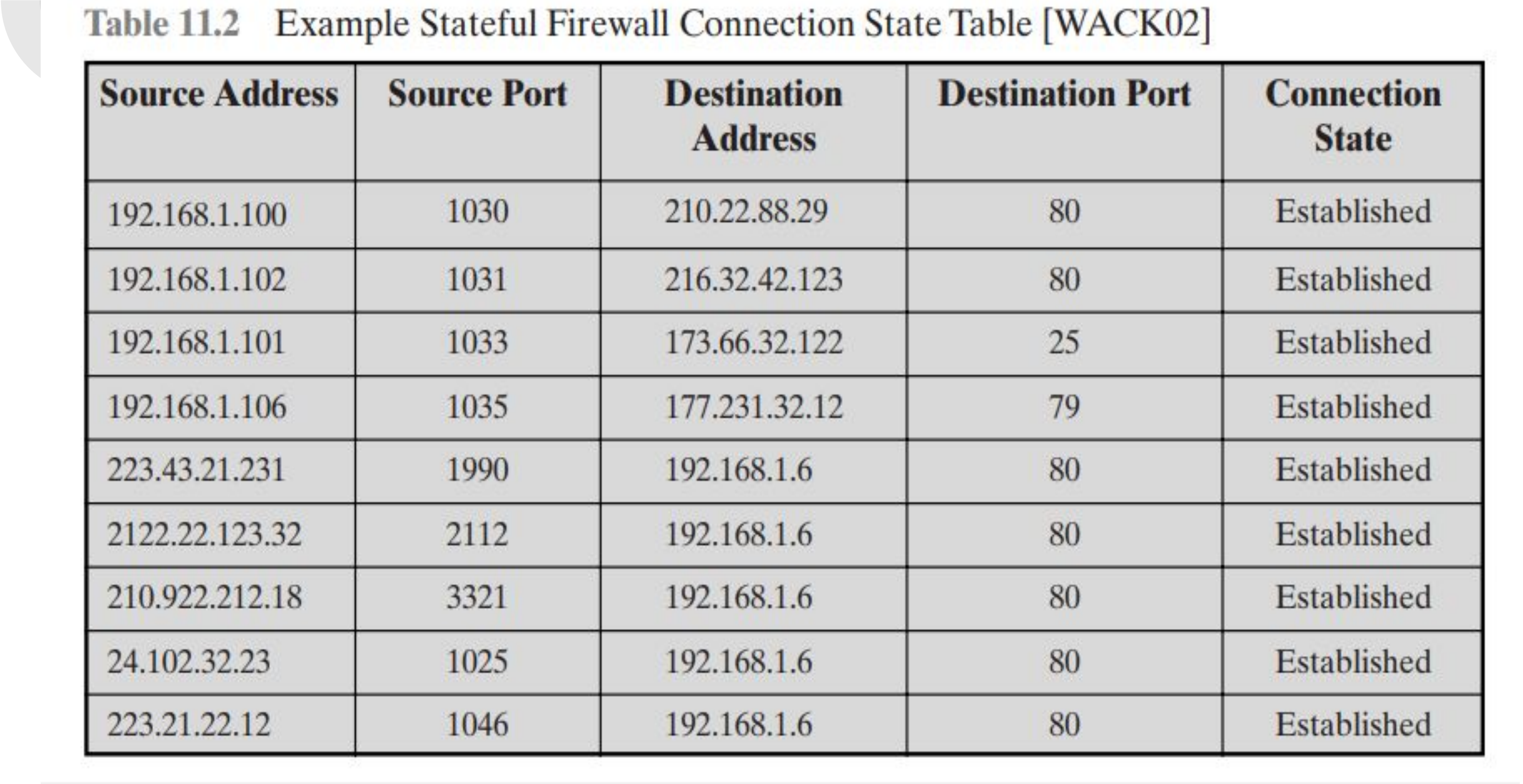
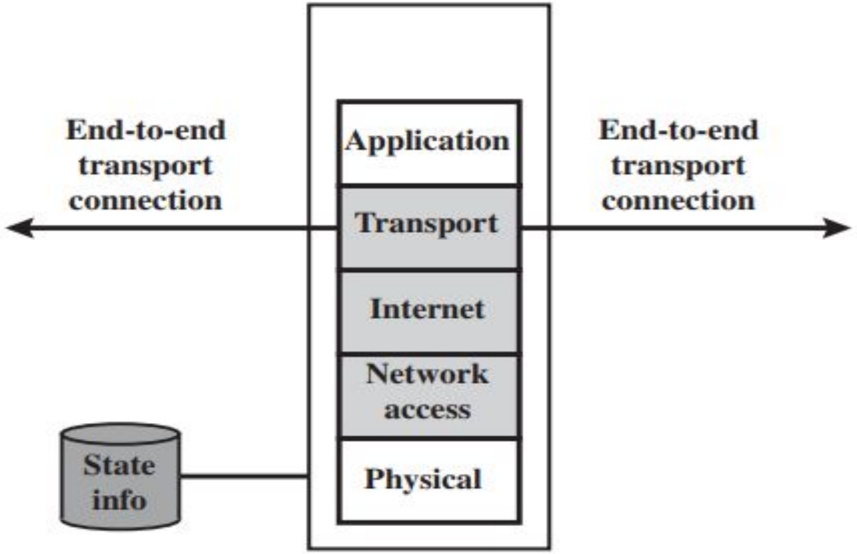


Table 11.2 Example Stateful Firewall Connection State Table [WACK02]

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

Stateful inspection firewall A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections

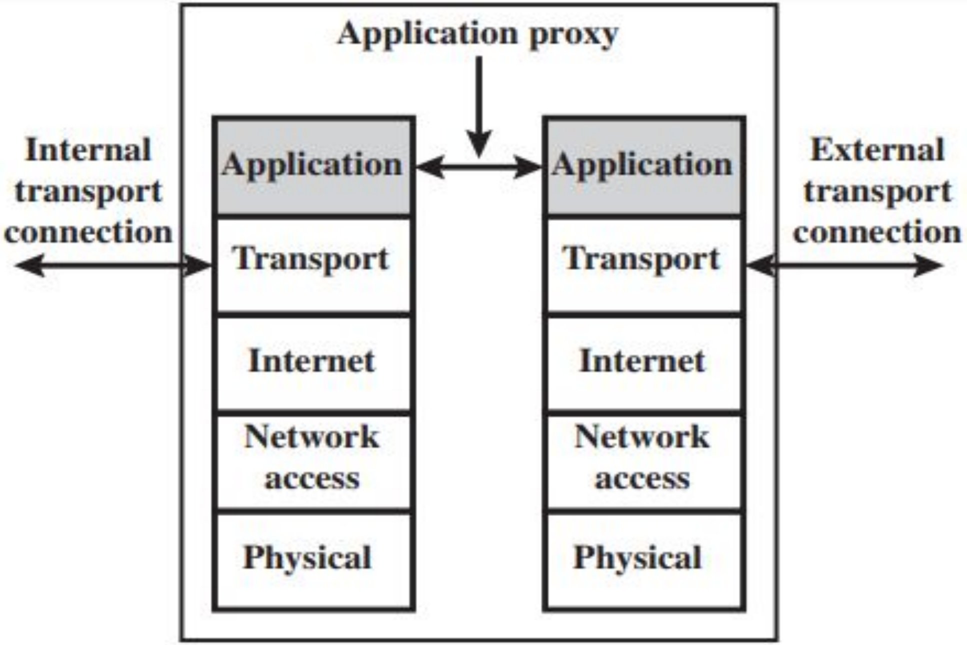

End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info

(c) Stateful inspection firewall

Application level gateway

Application level gateway known as an application proxy.

An application proxy acts as a relay of application level traffic where a user contacts the gateway using a TCP/IP application such as telnet or FTP.



(d) Application proxy firewall

Circuit level gateway

It can be a stand-alone system or a specialised function performed by an application level gateway for certain applications.

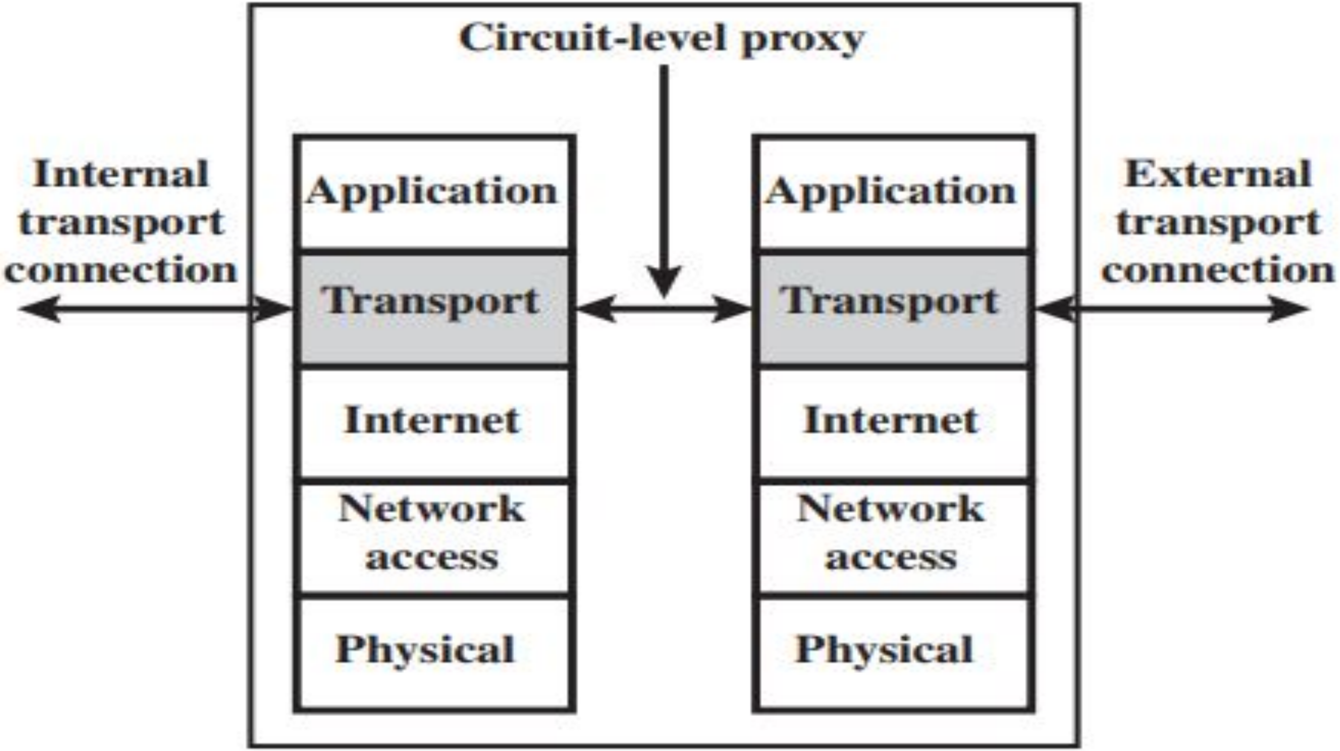
A circuit-level gateway does not permit an end-to-end TCP connection but the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host.

An example of a circuit-level gateway implementation is the SOCKS package.

SOCKS components include the SOCKS server which often runs on a UNIX-based firewall.

SOCKS is also implemented on Windows systems.

The SOCKS client library which runs on internal hosts protected by the firewall.


Circuit-level proxy
Internal transport connection
Application
Transport
Internet
Network access
Physical
Application
Transport
Internet
Network access
Physical
External transport connection

FIREWALL

Basing

Configurations and Location

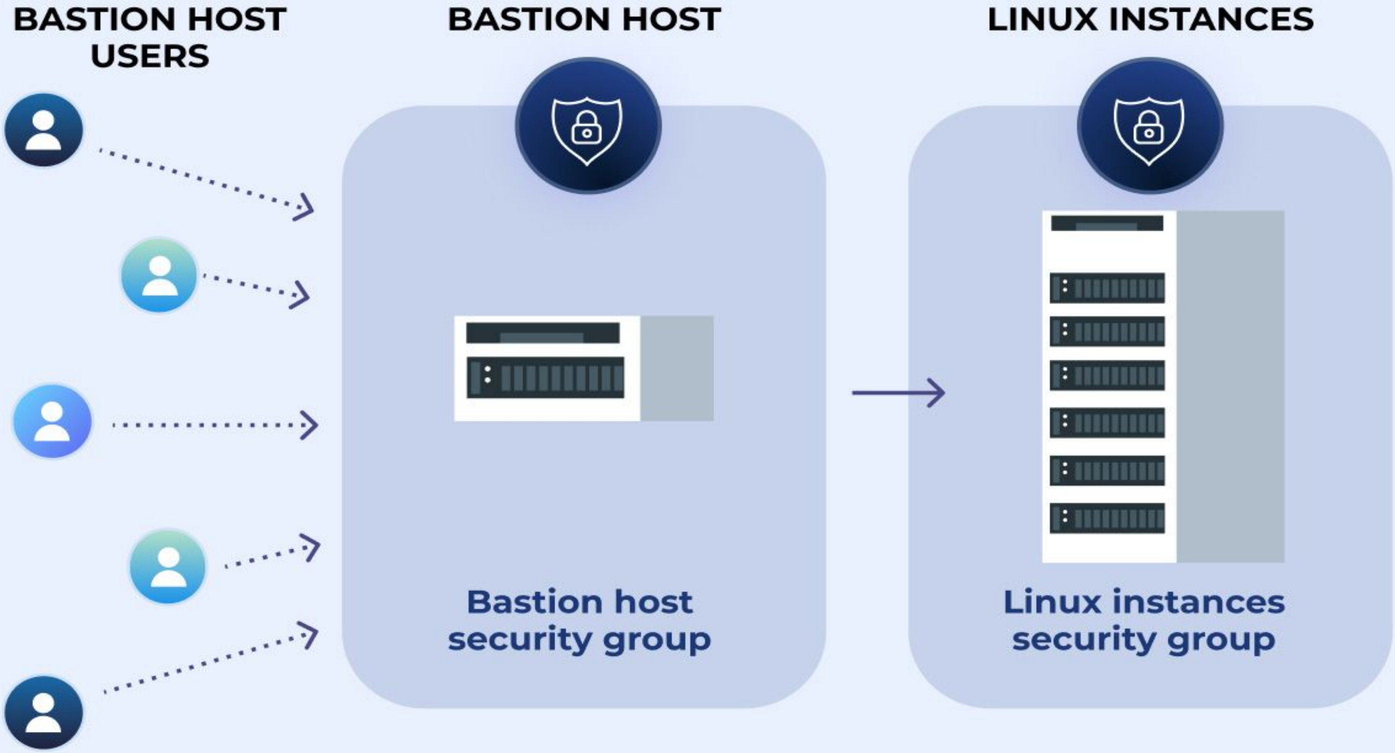
Firewall Basing

There are several options for locating firewall

Firewall basing considerations

- Bastion Host
- Host-Based firewall
- Personal Firewall

BASTION HOST



A **bastion** host is a special-purpose computer on a network specifically designed and configured to withstand attacks.

The computer generally hosts a single application or process, for example a proxy server or load balancer and all other services are removed or limited to reduce the threat to the computer.

The bastion host serves as a platform for an application-level or circuit-level gateway

How do bastion hosts work?

To understand how a bastion host works, we will look at a simple scenario in which a company’s administrators need access to Linux instances connected on a subnet within a virtual private cloud.

Exposing a port in each instance to the public internet would give administrators the access they need. But the security implications make that approach too risky.

Instead, a bastion host is used as a bridge between the public internet and the private subnet. The bastion runs as a locked-down, single-purpose system — in this case, an SSH proxy server.

The bastion host resides on its own subnet with an IP address that is accessible from the public internet.

The bastion only accepts SSH connections from a limited range of IP addresses in the IT department. ACLs, allowlists, and other network-level access controls limit access from the bastion to its protected subnets.

When authorized users need to access a resource on the private subnet, they must first use their SSH keys to establish a connection with the bastion host.

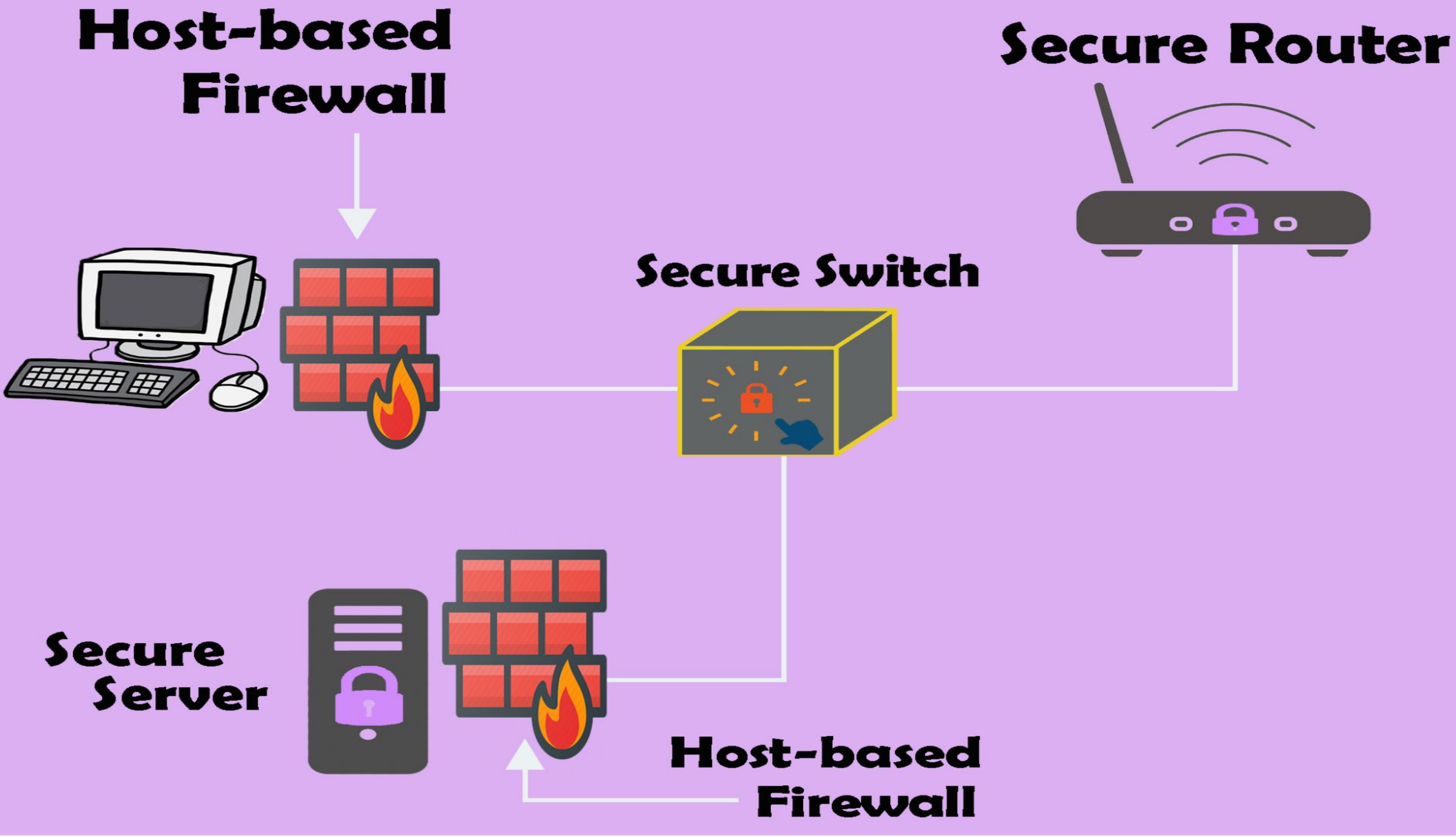
Once authenticated, they can then use another set of SSH keys to connect with the private network.

Characteristics of a bastion

- 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. such as SMTP, FTP
- The bastion host 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

Characteristics of bastion .... ctd

- 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. If there is a problem with the operation of any proxy, or if a future vulnerability is discovered,
- A proxy generally performs no disk access other than to read its initial configuration file.
- Each proxy runs as a non-privileged user in a private and secured directory on the bastion host.



Host-based Firewall

Secure Router

Secure Switch

Secure Server

Host-based Firewall

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.

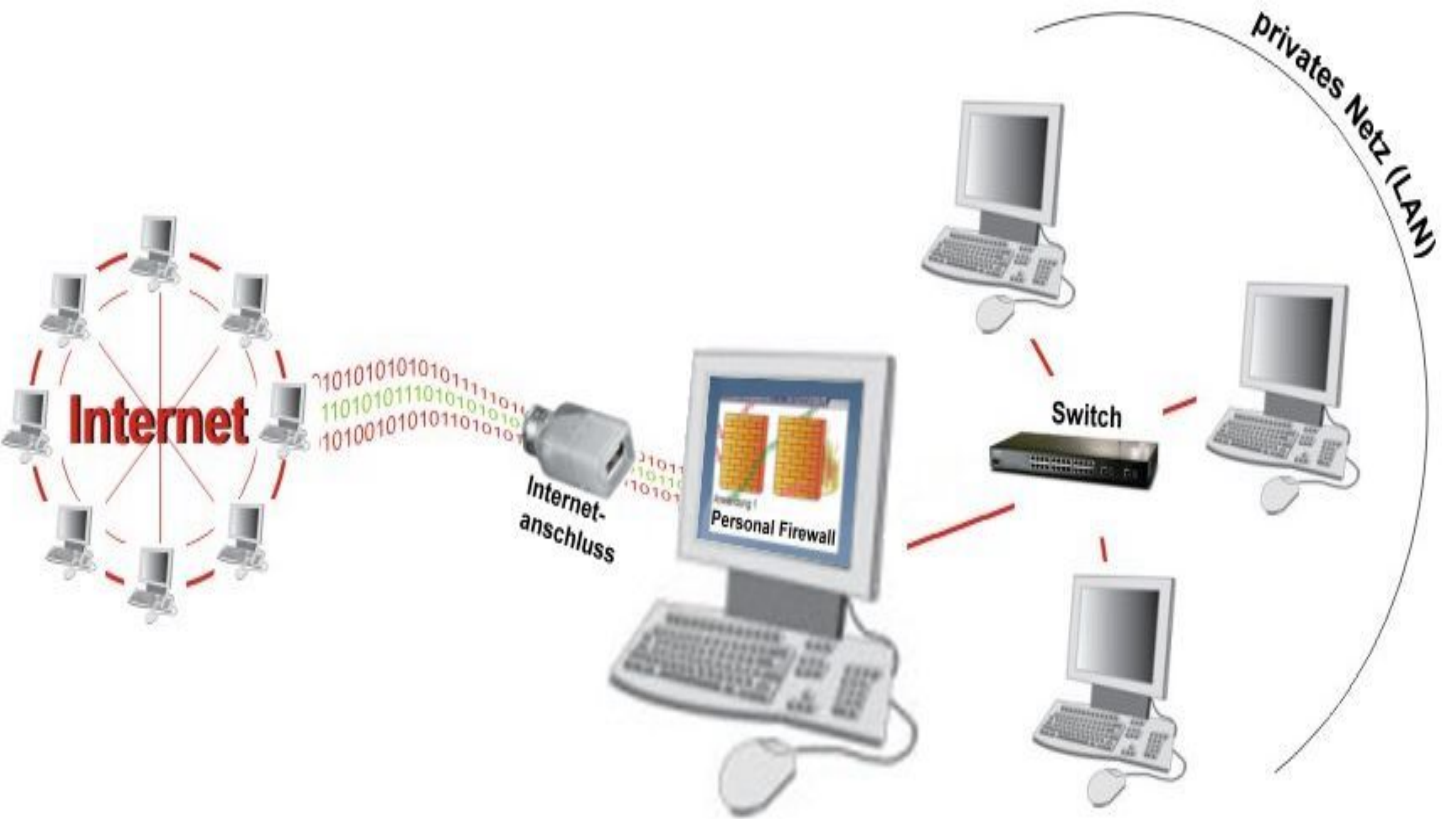
A common location for such firewalls is a **server**

Advantages of a server-based

- Filtering rules can be tailored to the host environment.

  Specific corporate security policies for servers can be implemented, 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.


Internet
Internet-
anschluss
Personal Firewall
Switch
privates Netz (LAN)

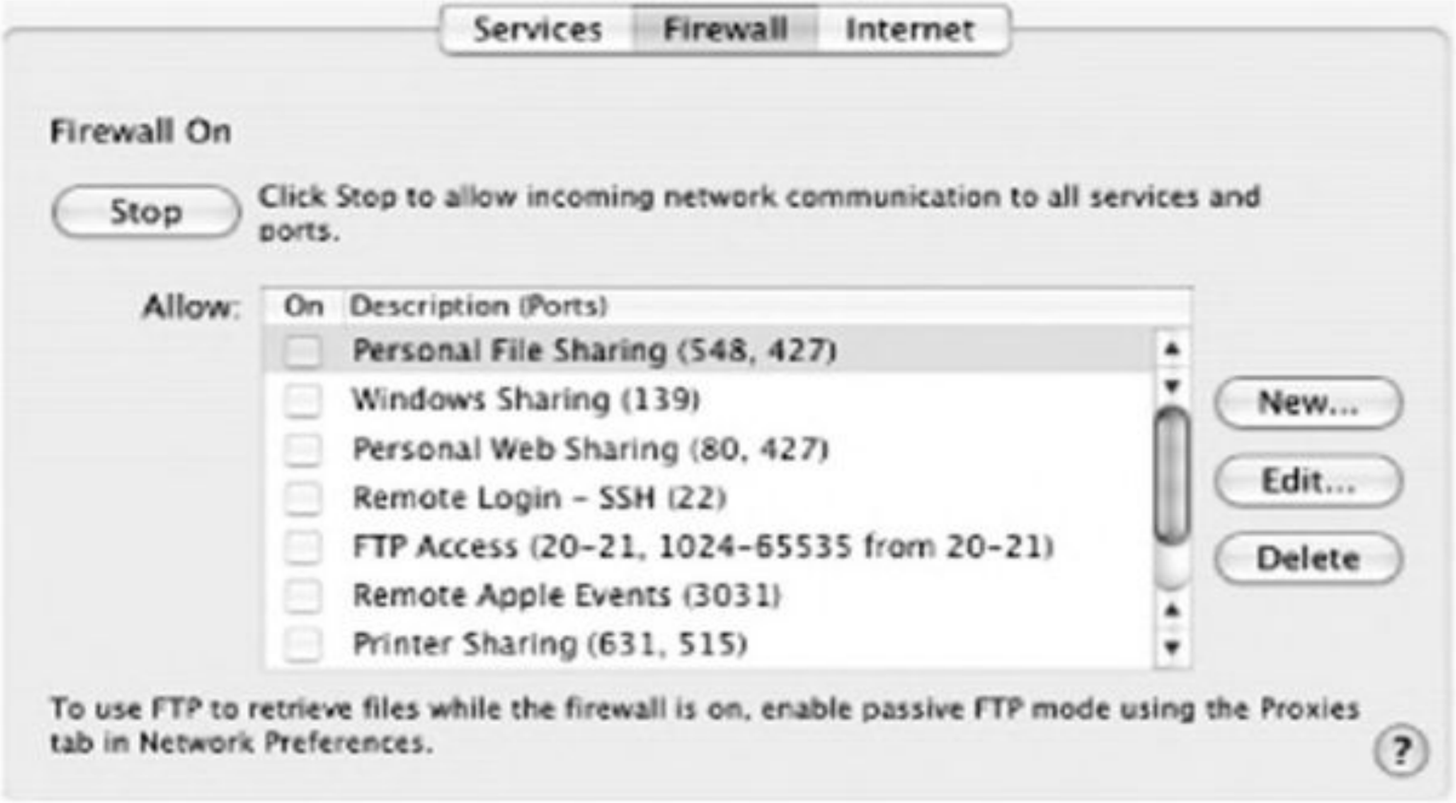
Personal Firewall

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. This firewall is basically a software on a person computer.

In a home environment with multiple computers connected to the Internet, 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.

The primary role of the personal firewall is to deny unauthorized remote access to the computer.

The firewall can also monitor outgoing activity in an attempt to detect and block worms and other malware.



Firewall On

Click Stop to allow incoming network communication to all services and ports.

Allow:

On	Description (Ports)
☐	Personal File Sharing (548, 427)
☐	Windows Sharing (139)
☐	Personal Web Sharing (80, 427)
☐	Remote Login - SSH (22)
☐	FTP Access (20-21, 1024-65535 from 20-21)
☐	Remote Apple Events (3031)
☐	Printer Sharing (631, 515)

To use FTP to retrieve files while the firewall is on, enable passive FTP mode using the Proxies tab in Network Preferences.

Figure 11.2 Example Personal Firewall Interface

In bound services that can be permitted

-Personal file sharing (548, 427)

- Windows sharing (139)

- Personal Web sharing (80, 427)

- Remote login - SSH (22)

- FTP access (20-21, 1024-64535 from 20-21)

- Remote Apple events (3031)

- Printer sharing (631, 515)

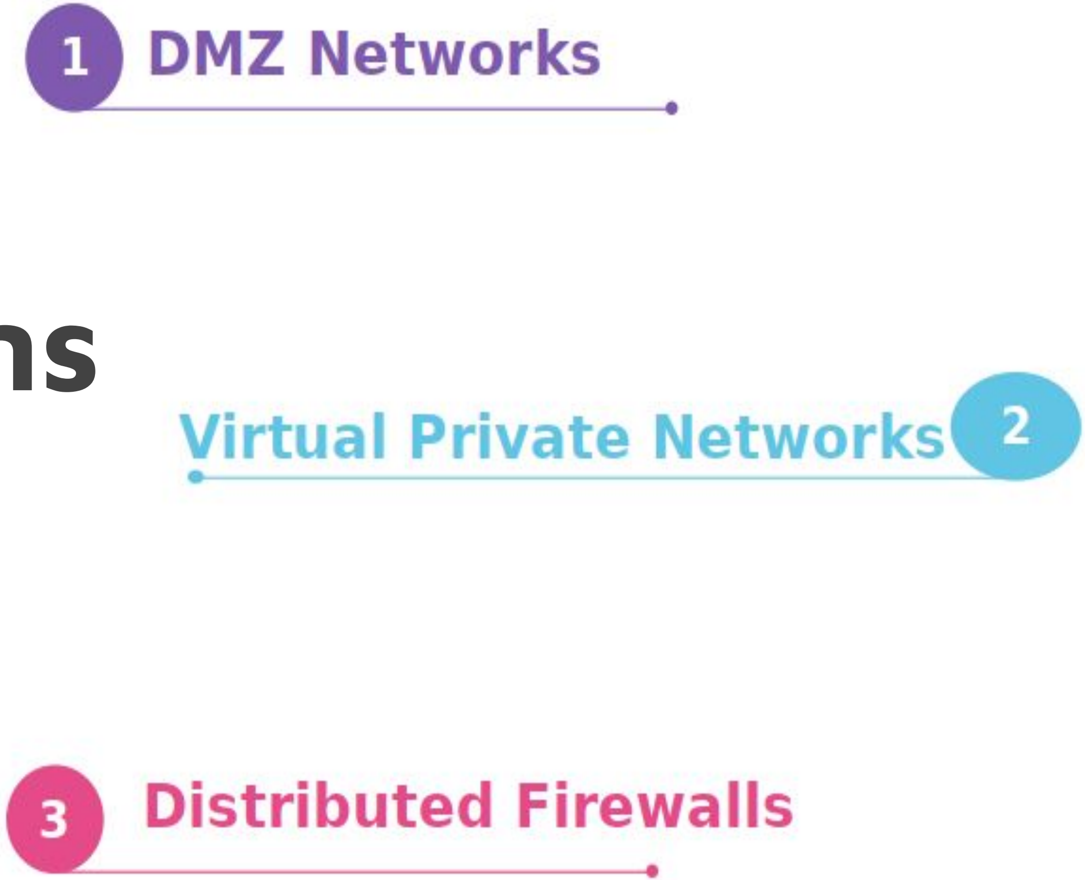
- IChat Rendezvous (5297, 5298)

- ITunes Music Sharing (3869)

- CVS (2401)

- For increased protection, advanced firewall features are available through easy-to-configure checkboxes.
- UDP packets can be blocked, restricting network traffic to TCP packets only for open ports.
- The firewall also supports logging, an important tool for checking on unwanted activity.

Firewall Configurations and Location



1 DMZ Networks

2 Virtual Private Networks

3 Distributed Firewalls

A firewall is positioned to provide a protective barrier between an external, potentially untrusted source of traffic and an internal network.

With that general principle in mind, a security administrator must decide on the location and on the number of firewalls needed. In this section, we look at some common options.

1

DMZ Networks

Demilitarized zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical sub network that contains and exposes an organization's external-facing services to an un trusted, usually larger, network such as the Internet.

An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN).

In a typical enterprise network, one or more internal firewalls are set up to protect it against possible attacks.

Systems that are externally accessible but need some protection are located in DMZ network.

The systems in the DMZ require connectivity such as a corporate Web site, an e-mail server, or a DNS (domain name system) server.

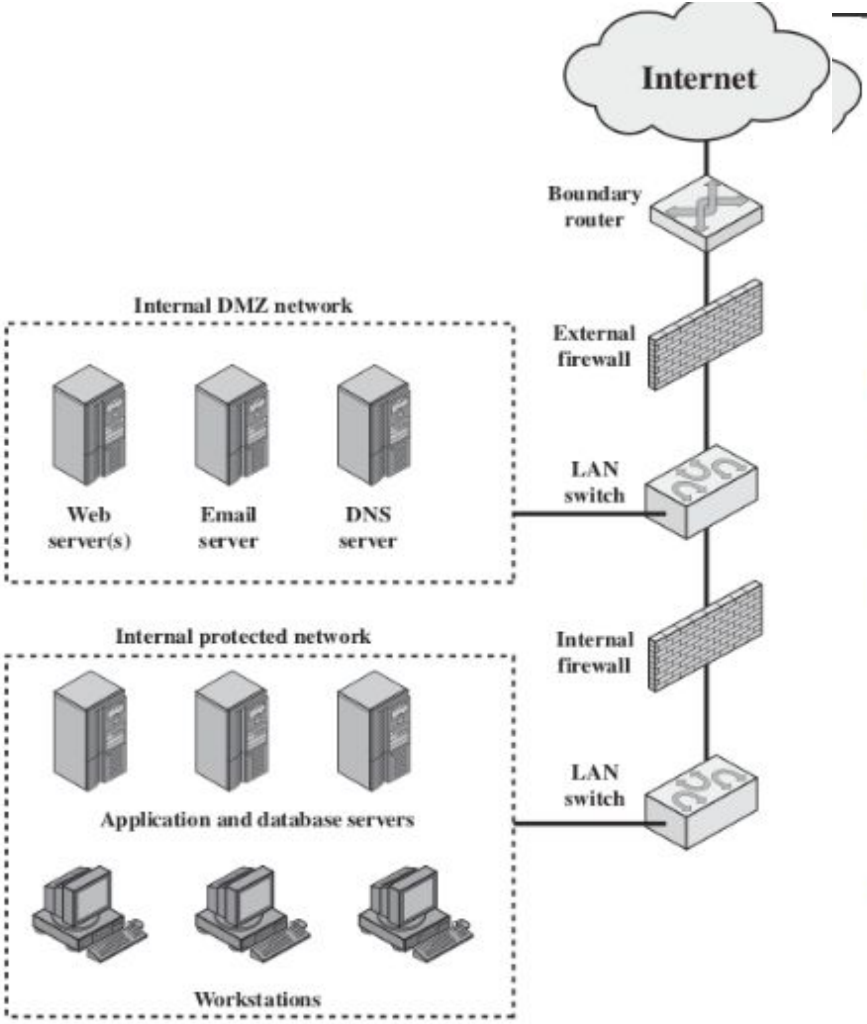


Figure 11.3 Example Firewall Configuration

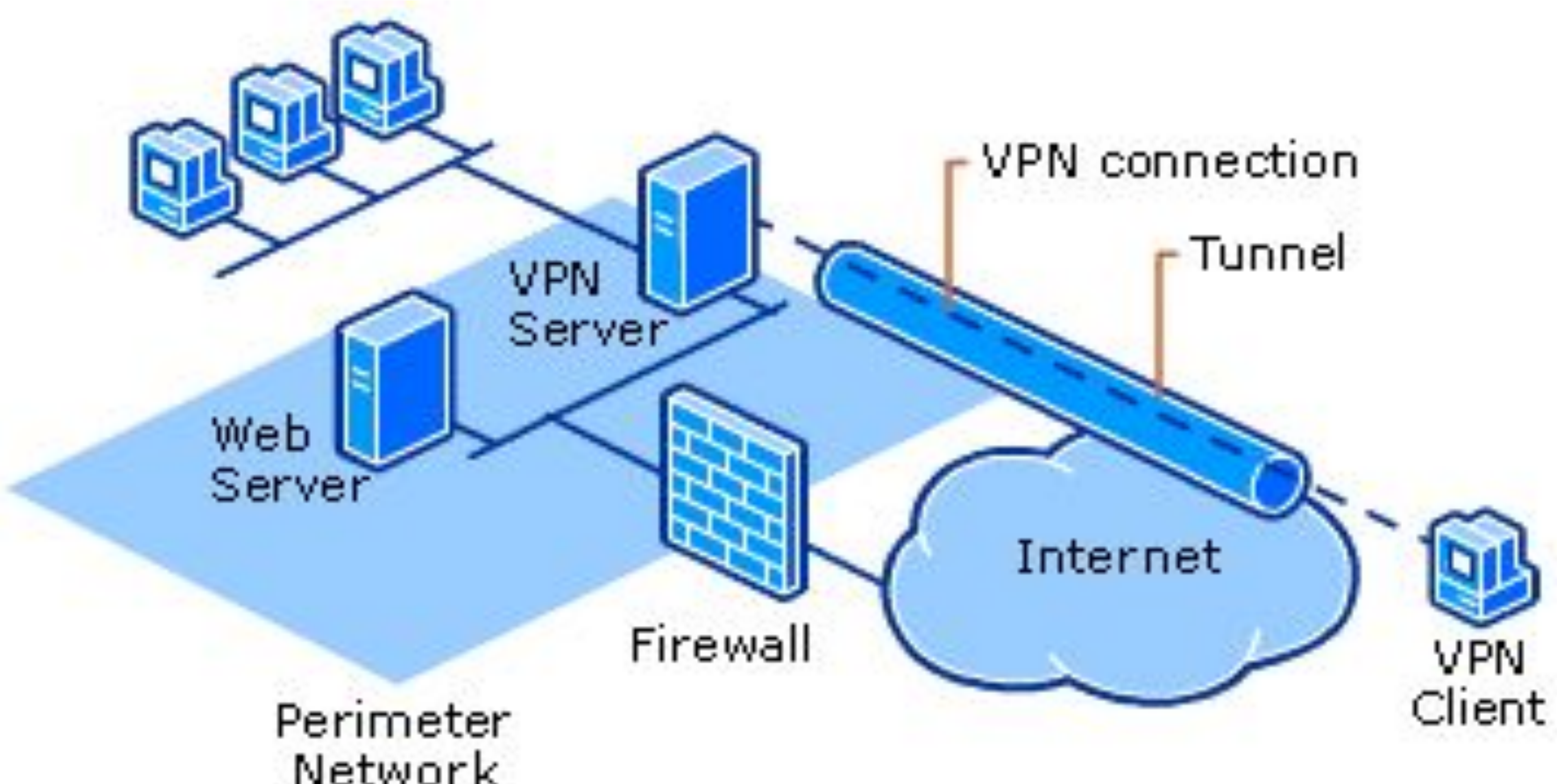
The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity.

Purposes of Internal Firewall

1) Adds more stringent filtering capabilities.
2) The internal firewall provides two-way protection with respect to the DMZ.
   - attacks launched from DMZ systems.
   - attack from the internal protected network.
3) Multiple internal firewalls can be used to protect portions of the internal network from each other.

2 Virtual Private Networks

The **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.


VPN connection
Tunnel
VPN Server
Web Server
Firewall
Internet
VPN Client
Perimeter Network

- Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users.
- A VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet
- VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends.
- The VPN encryption maybe performed by the firewall software. IPsec is the protocol mechanism used to ensure VPN encryption

  If IPsec is implemented behind to the firewall, then the firewall will be unable to perform filtering, access control, logging or viruses scanning. Implementing Ipsec in boundary router, outside firewall will make device less secure

Public Network

Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users.

Encryption

A VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet

Cost

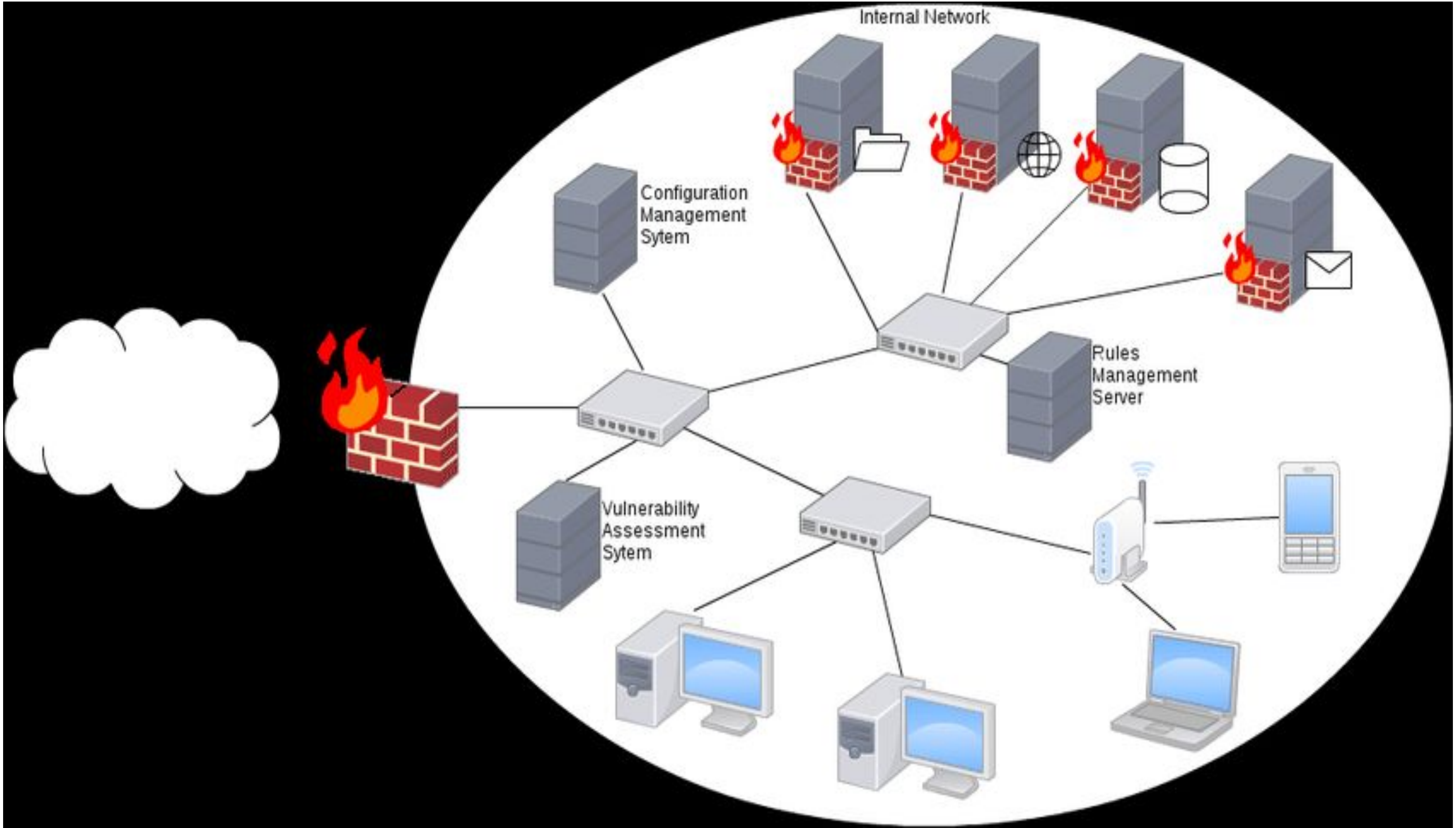
VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends

IPsec

The VPN encryption maybe performed by the firewall software. IPsec is the protocol mechanism used to ensure VPN encryption

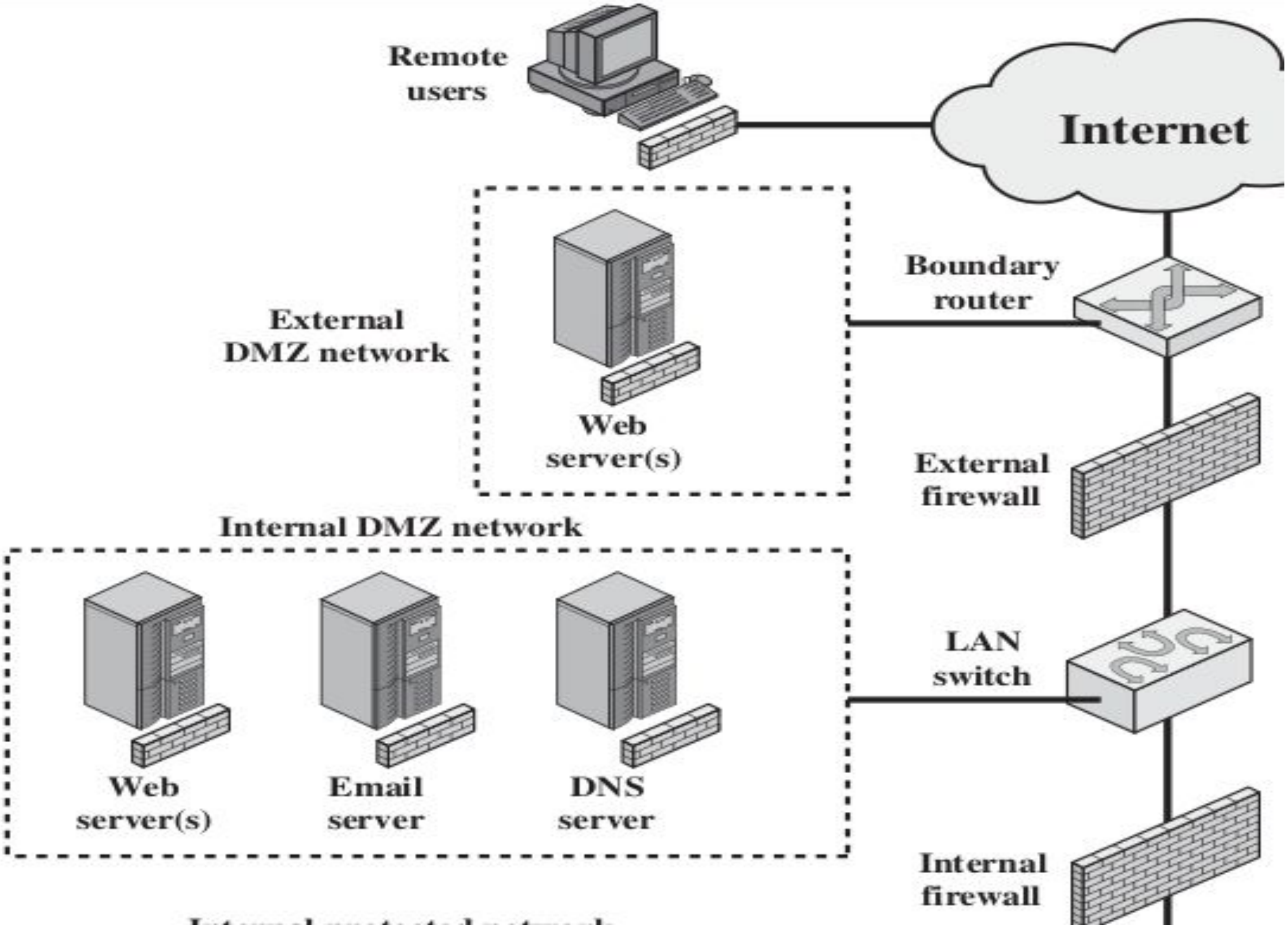
3 Distributed Firewalls

A distributed firewall configuration involves stand-alone firewall devices plus host-based firewalls working together under a central administrative control.


Internal Network
Configuration Management Sytem
Rules Management Server
Vulnerability Assessment Sytem

- Administrators can configure host resident firewalls on hundreds of servers and workstations as well as configure personal firewalls on local and remote user systems.
- Tools let the network administrator set policies and monitor security across the entire network.
- These firewalls protect against internal attacks and provide protection tailored to specific machines and applications.
- Stand-alone firewalls provide global protection, including internal firewalls and an external firewall.

- An establishment of both an internal and an external DMZ.
- Web servers that need less protection because they have less critical information on them could be placed in an external DMZ, outside the external firewall.
- What protection is needed is provided by host-based firewalls on these Servers.
- A distributed firewall is tasked with monitoring Security.


Remote users
Internet
External DMZ network
Web server(s)
Boundary router
External firewall
Internal DMZ network
Web server(s)
Email server
DNS server
LAN switch
Internal firewall
Internal protected network

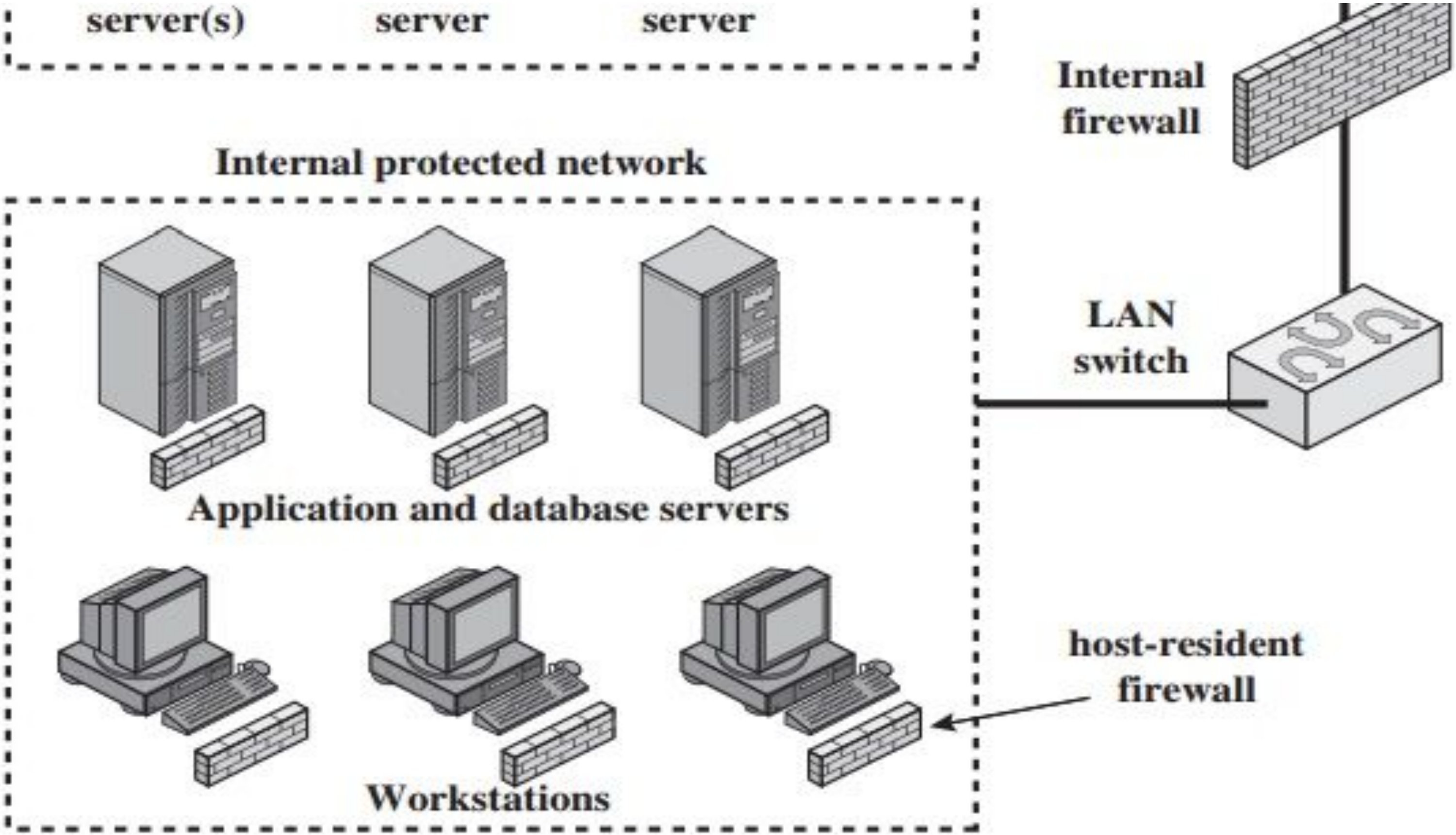


Figure 22.5 Example Distributed Firewall Configuration

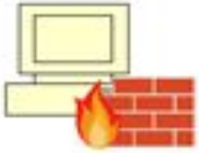
Summary of Firewall Locations and Topologies

To define a spectrum of firewall locations and topologies. The following alternatives can be identified:

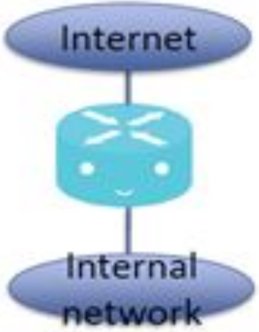
- Host-resident firewall
- Screening router
- Single bastion inline

- Single bastion T
- Double bastion inline
- Double bastion T
- Distributed firewall configuration

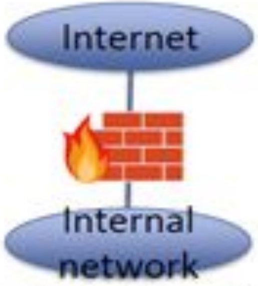
Firewall Topologies



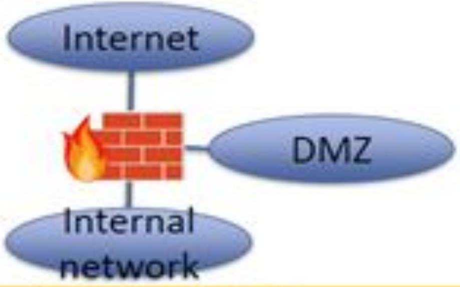
Host-resident firewall



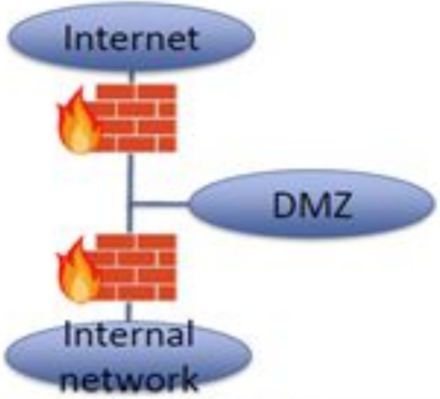
Screening router



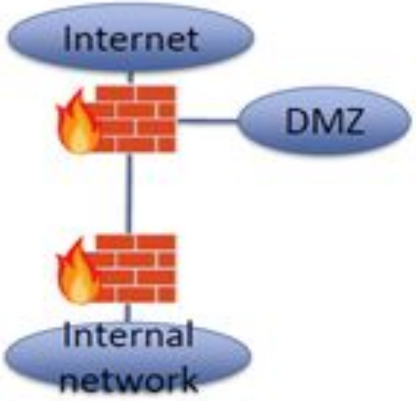
Single bastion inline



Single bastion T



Double bastion inline



Double bastion T

Host-resident firewall: personal firewall and firewall on servers (used alone or part of a defense in-depth)

Screening router: a single router between internal and external networks, e.g., SOHO apps)

Single bastion inline: single firewall device between an internal and external router (stateful or app proxies)

Single bastion T: similar to above but has a 3rd NIC on bastion to a DMZ (for medium to large organizations)

Double bastion inline: DMZ is between (for large organizations)

Double bastion T: The DMZ is on a separate network interface on the bastion firewall. This configuration is also common for large businesses and government organizations and may be required

Distributed firewall configuration:This configuration is used by some large businesses and government organizations