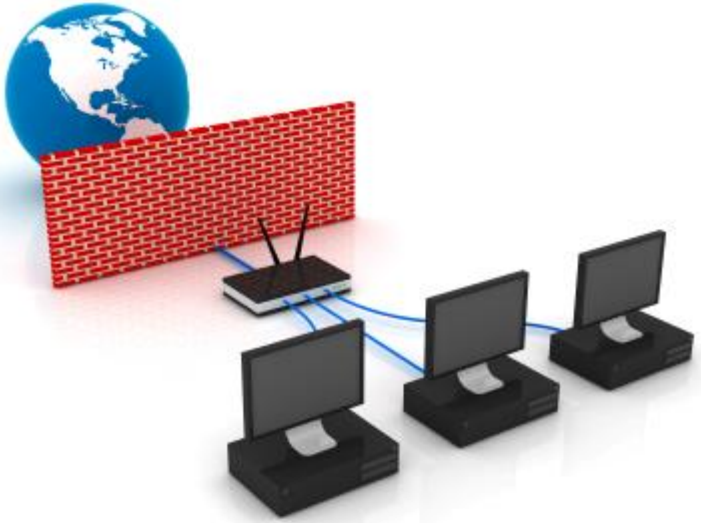
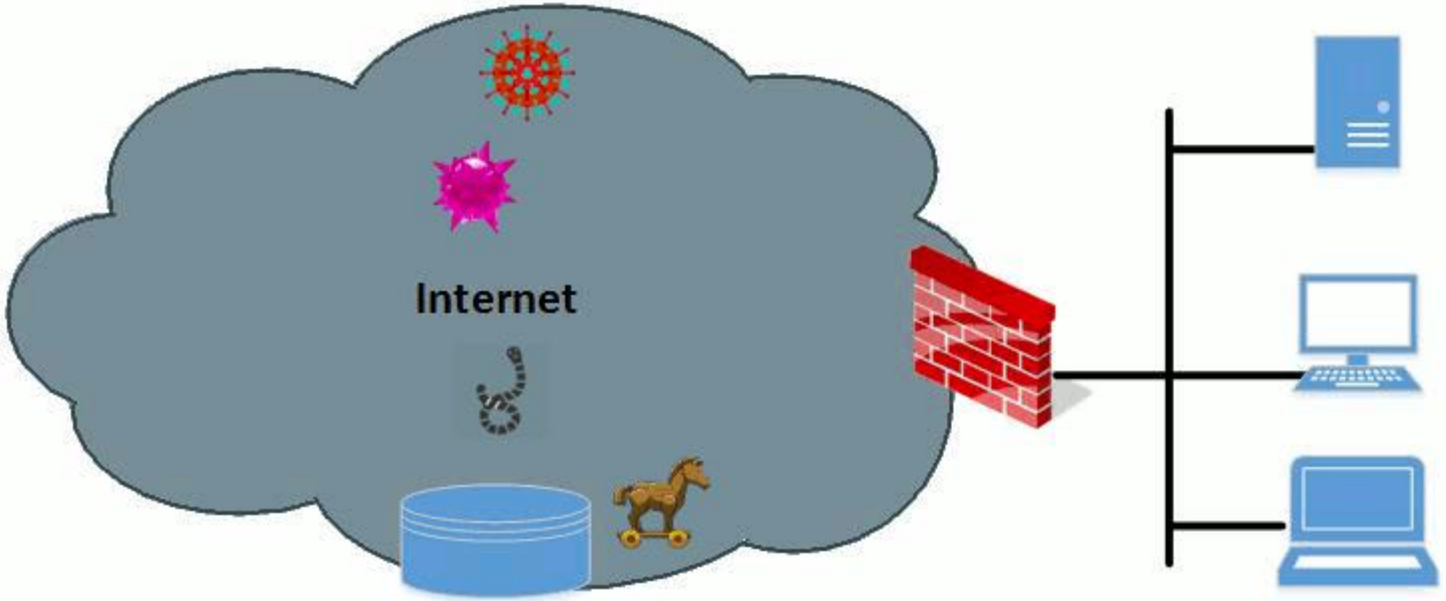




FIREWALLS

Mukesh Chinta
Asst Prof, CSE, VRSEC

NEED FOR FIREWALLS

- Information systems in corporations, government agencies, and other organizations have undergone a steady evolution from mainframes to LANs.
- Internet connectivity is no longer optional, with information and services essential to the organization.
- However, while Internet access provides benefits, it enables the outside world to reach and interact with local network assets, creating a threat to the organization.
- While it is possible to equip each workstation and server on the premises network with strong security features, this is not a practical approach in general.
- *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*.

FIREWALL CHARACTERISTICS

- Design goals:
  - All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall).
  - Only authorized traffic (defined by the local security policy) will be allowed to pass.
  - The firewall itself is immune to penetration (use of trusted system with a secure operating system).

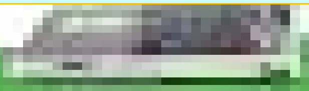
- Four general techniques used by firewalls to control access and enforce the site's security policy:

❖ Service control: - Determines the types of Internet services that can be accessed, inbound or outbound

❖ Direction control: - Determines the direction in which particular service requests are allowed to flow

❖ User control: - Controls access to a service according to which user is attempting to access it

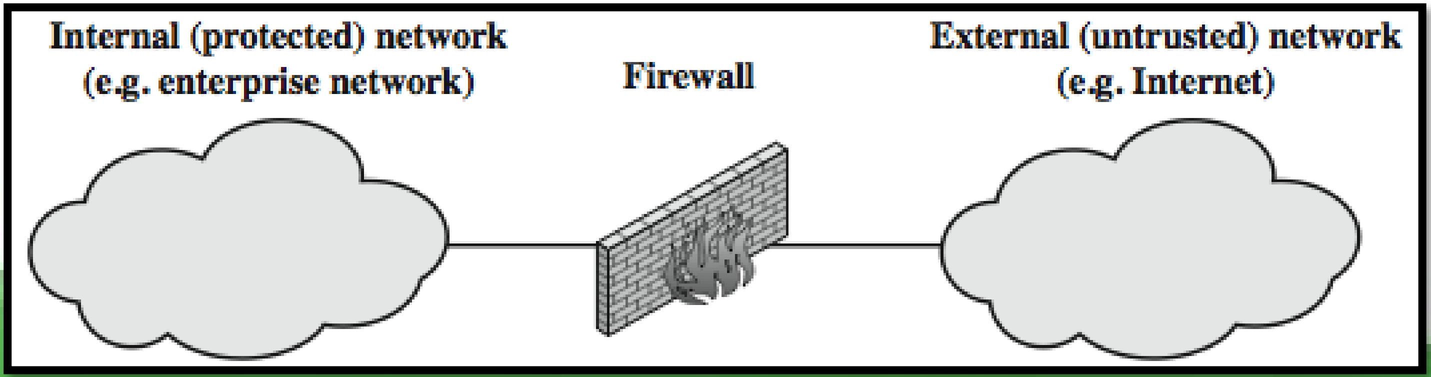
❖ Behavior control: - Controls how particular services are used (e.g. filter e-mail)



FIREWALL CAPABILITIES

The following capabilities are within the scope of a firewall:

1. *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.*
2. *Provides a location for monitoring security-related events*
3. *Firewall is a convenient platform for several Internet functions that are not security related, such as NAT and Internet usage audits or logs*
4. *A firewall can serve as the platform for IPSec to implement virtual private networks.*


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)

LIMITATIONS OF A FIREWALL

- cannot protect from attacks bypassing it
  - *eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)*

- cannot protect against internal threats
  - *eg disgruntled or colluding employees*
- cannot protect against access via WLAN
  - *if improperly secured against external use*
- cannot protect against malware imported via laptop, PDA, storage infected outside

TYPES OF FIREWALLS

Have three common types of firewalls:

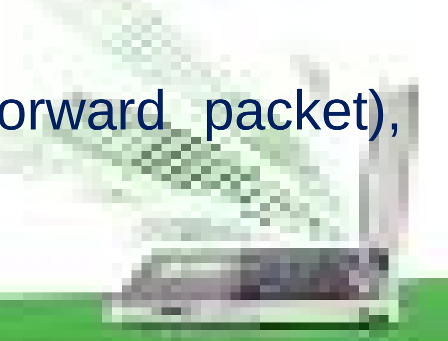
- Packet filters, Application-level gateways, & Circuit-level gateways.

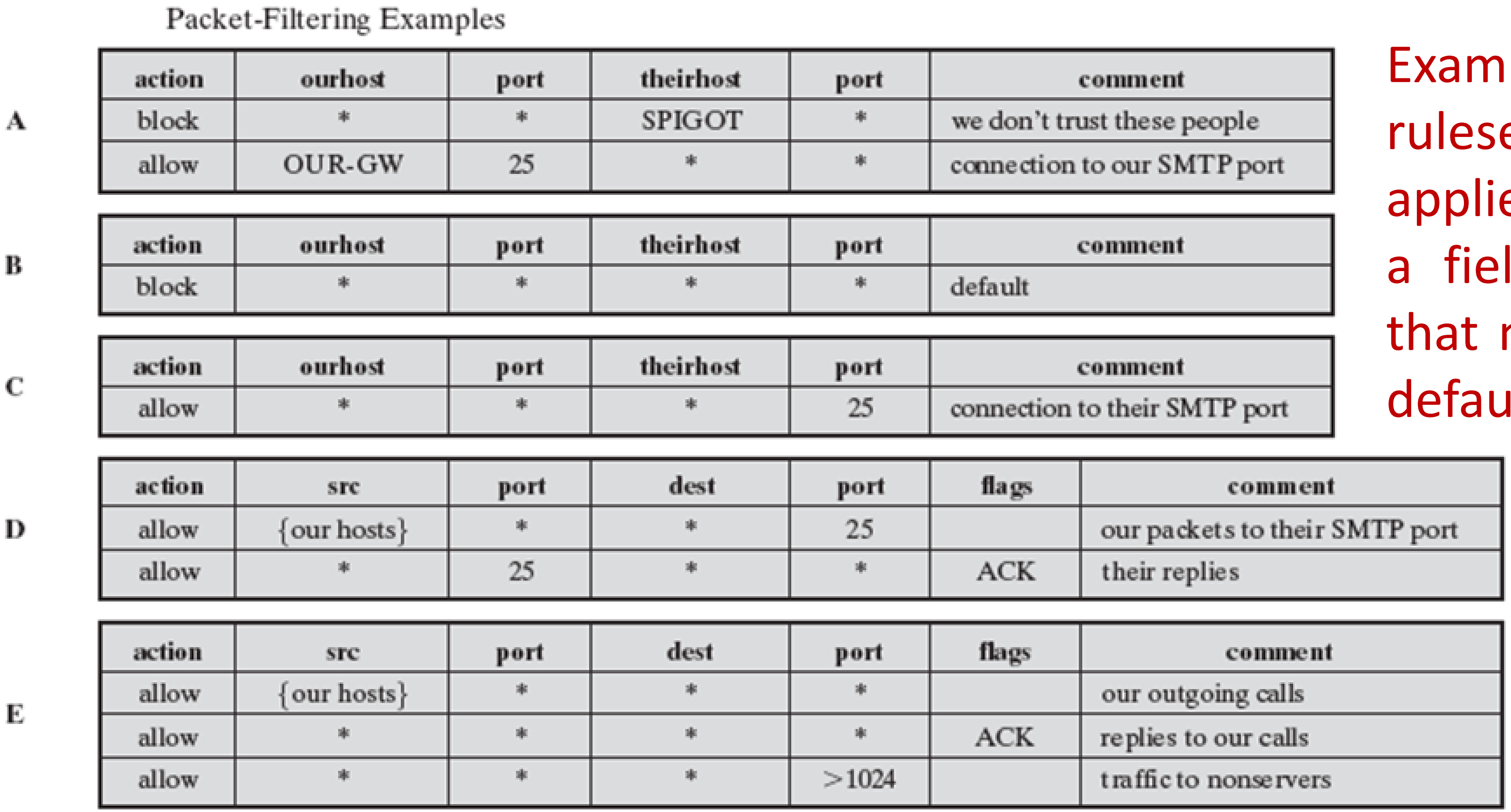
Packet Filtering Firewall

- A packet-filtering router applies a set of rules to each incoming and outgoing IP packet to forward or discard the packet.
- Filtering rules are based on information contained in a network packet such as source & destination IP addresses, ports, transport protocol & interface.
- Some advantages are simplicity, transparency & speed.

If there is no match to any rule, then one of two default policies are applied:

- that which is not expressly permitted is prohibited (default action is discard packet), **conservative policy**
- that which is not expressly prohibited is permitted (default action is forward packet), **permissive policy**





Packet-Filtering Examples

A

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

B

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

C

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

D

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

E

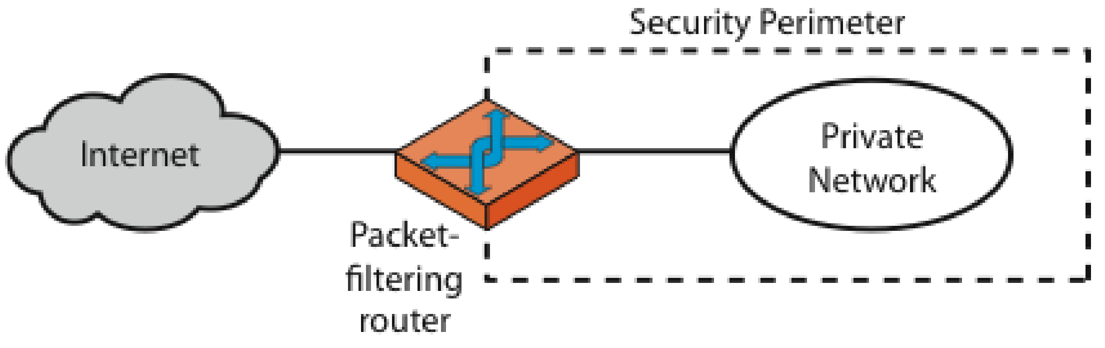
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

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. Assume default = discard policy is in force.

A. Inbound mail is allowed to a gateway host only (port 25) is for SMTP incoming
B. Explicit statement of the default policy
C. Tries to specify that any inside host can send mail to the outside, but has problem that an outside machine could be configured to have some other application linked to port 25
D. Properly implements mail sending rule, by checking ACK flag of a TCP segment is set
E. This rule set is one approach for handling FTP connections

Some of the attacks that can be made on packet-filtering routers & countermeasures are:

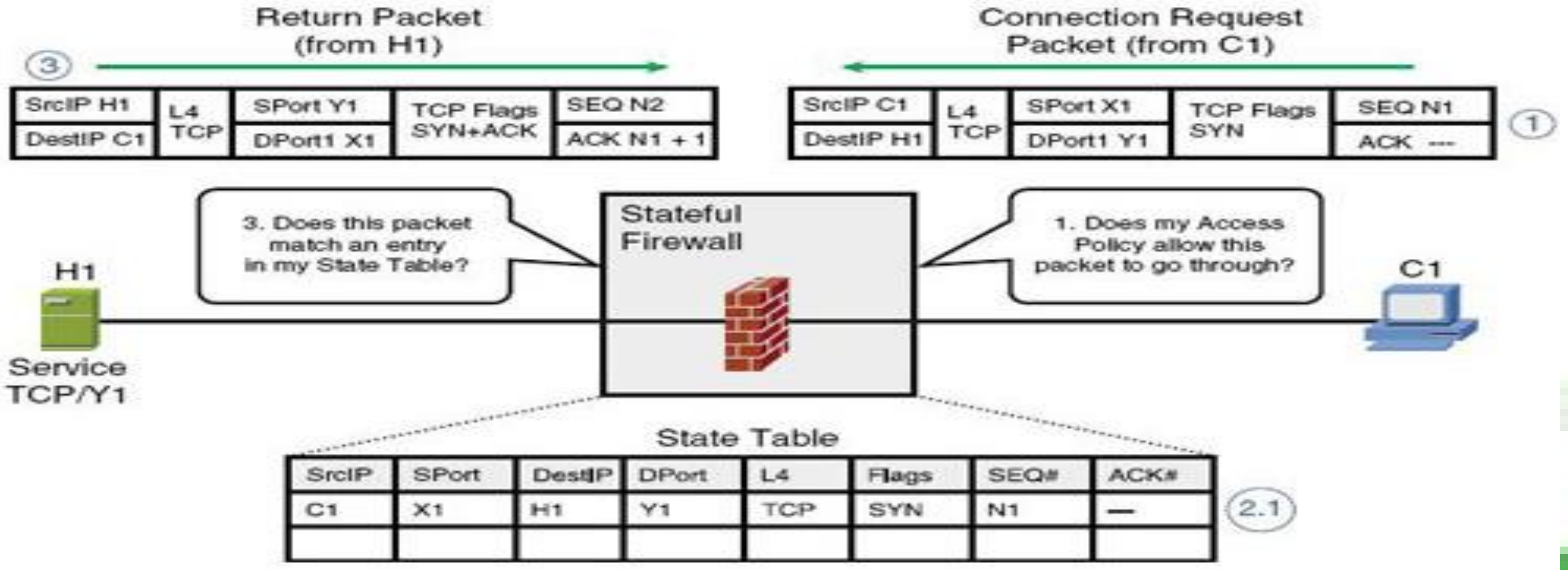
- **IP address spoofing:** where intruder transmits packets from the outside with internal host source IP address - need to filter & discard such packets
- **Source routing attacks:** where source specifies the route that a packet should take to bypass security measures - should discard all source routed packets
- **Tiny fragment attacks:** intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate fragment to circumvent filtering rules needing full header info - can enforce minimum fragment size to include full header.



(a) Packet-filtering router

Firewalls – Stateful Packet Filters

- A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context.
- A stateful inspection packet filter (also referred to as dynamic packet filtering) tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, and will allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.
- Hence they are better able to detect bogus packets sent out of context.
- A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections.

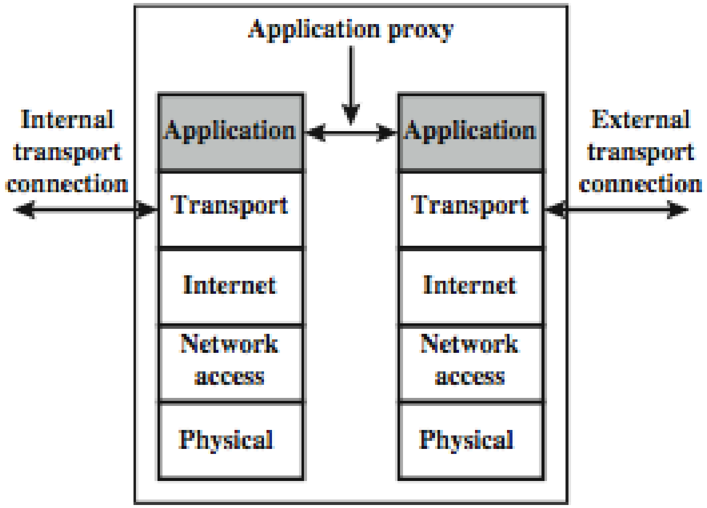


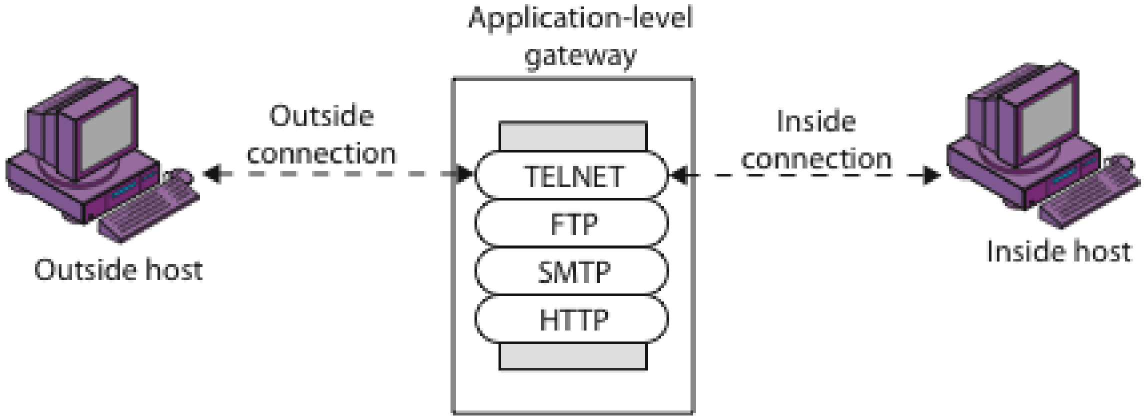
SrcIP	SPort	DestIP	DPort	L4	Flags	SEQ#	ACK#
C1	X1	H1	Y1	TCP	SYN	N1	—

Overview of Stateful Firewalls

Application Level Gateway (or Proxy)

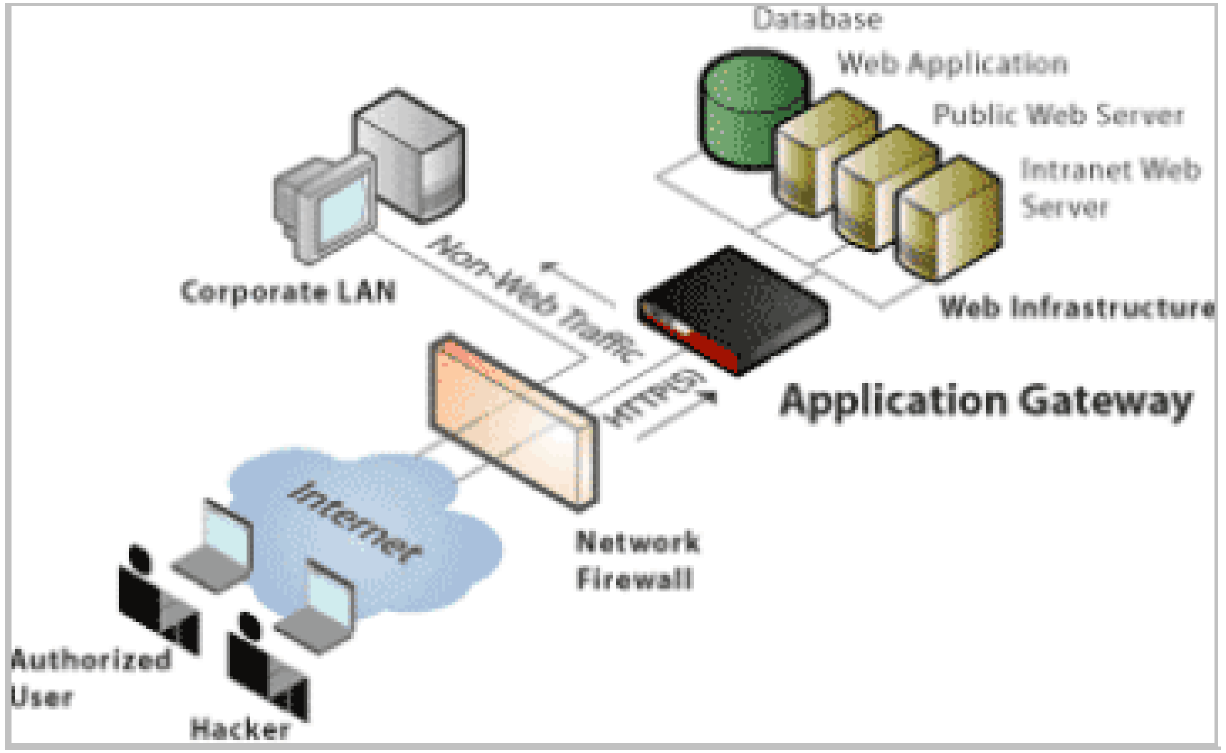
- An application-level gateway (or proxy server), acts as a relay of application-level traffic.





(b) Application-level gateway

- ➢ Application level Gateway, as the name suggests, operates in the Application layer of the OSI model and actively inspects the contents of packets that are passed through to the gateway.
- ➢ An application-level gateway acts as a intermediate system between the Internet and the application server that understands the relevant application protocol.
- ➢ An application-level gateway intercepts the incoming and outgoing packets, runs a proxy to copy and forward information across the gateway, and functions as a proxy server, thereby preventing any direct connection between a trusted server or client and an untrusted host.

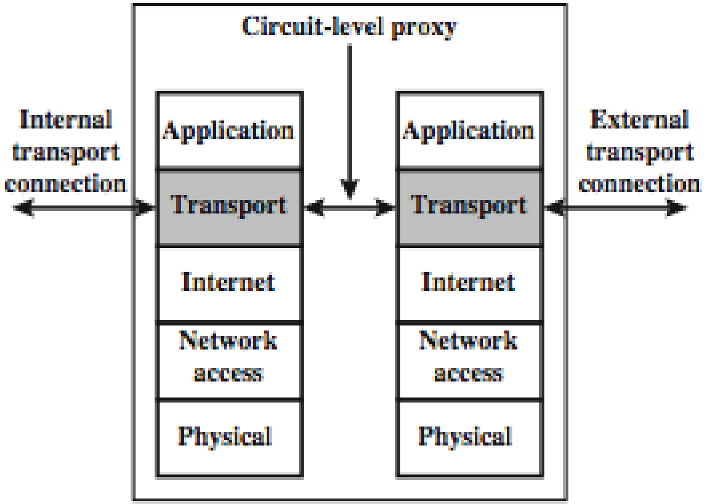


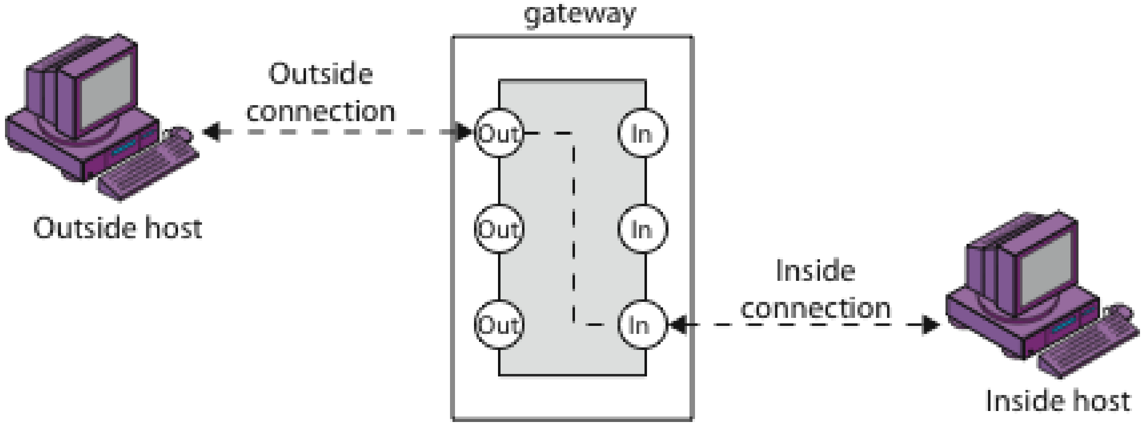
In addition, the ALG can be configured to support only specified features of an application that the network administrator considers acceptable while denying all other features.

- Application-level gateways tend to be more secure than packet filters, & can log and audit traffic at application level.
- A prime disadvantage of this type of gateway is the additional processing overhead on each connection.

Circuit Level Gateway

- A fourth type of firewall is the circuit-level gateway or **circuit-level proxy.** This can be a stand-alone system or can be a specialized function performed by an application-level gateway for certain applications.



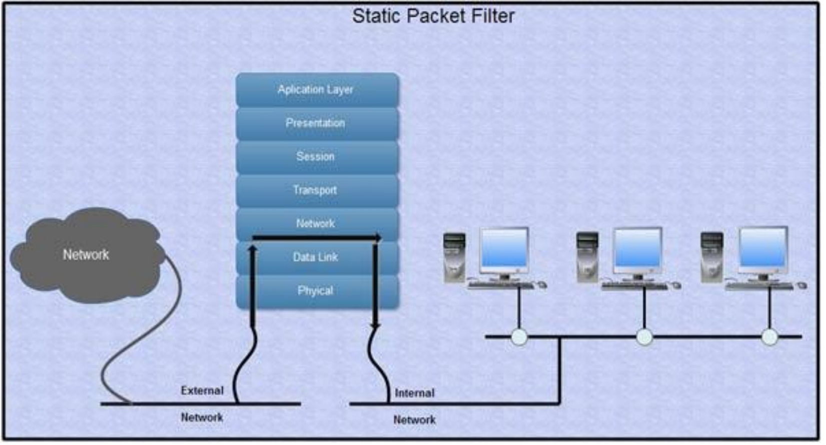


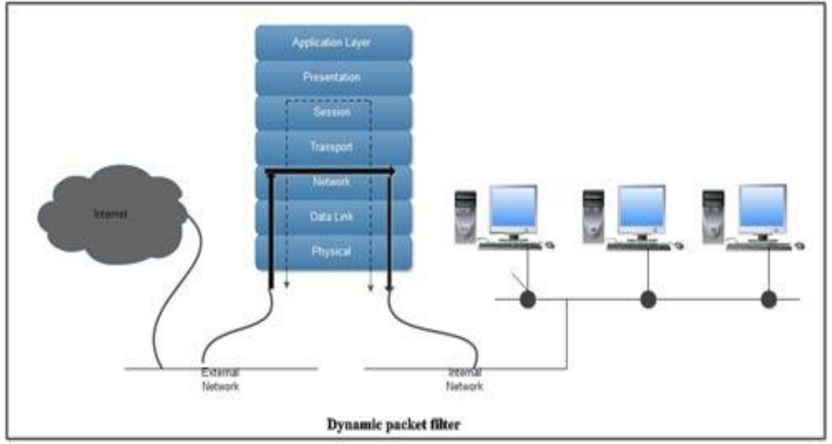
(c) Circuit-level gateway

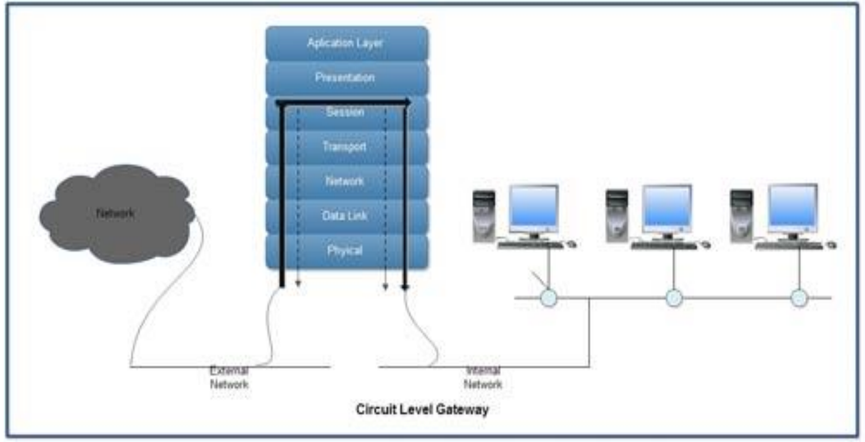
- A circuit level gateway is simply an extension of a packet filter in that it typically performs basic packet filter operations and then adds verification of proper handshaking of TCP and the legitimacy of the session information used in establishing the connection. Hence, the circuit level gateway has more data to act upon than a standard static or dynamic packet filter.
- A circuit-level gateway relays two TCP connections, one between itself and an inside TCP user, and the other between itself and a TCP user on an outside host. Once the two connections are established, it relays TCP data from one connection to the other without examining its contents. The security function consists of determining which connections will be allowed. It is typically used when internal users are trusted to decide what external services to access

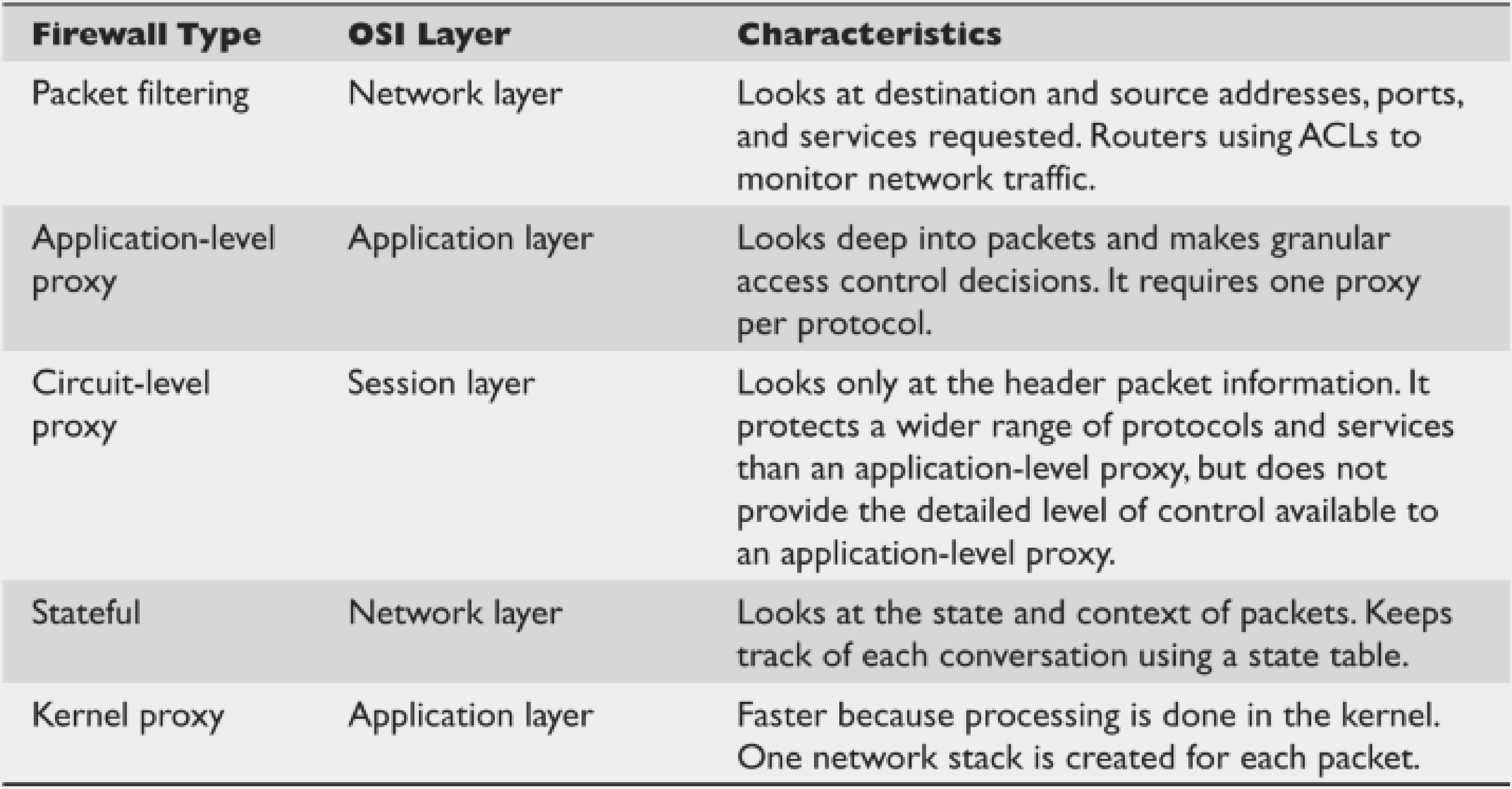
SOCKS

- One of the most common circuit-level gateways is SOCKS, defined in RFC 1928.
- It consists of a SOCKS server on the firewall, and a SOCKS library & SOCKS-aware applications on internal clients.
- When a TCP-based client wishes to establish a connection to an object that is reachable only via a firewall (such determination is left up to the implementation), it must open a TCP connection to the appropriate SOCKS port on the SOCKS server system.
- If the connection request succeeds, the client enters a negotiation for the authentication method to be used, authenticates with the chosen method, and then sends a relay request. The SOCKS server evaluates the request and either establishes the appropriate connection or denies it. UDP exchanges are handled in a similar fashion.









Firewall Type	OSI Layer	Characteristics
Packet filtering	Network layer	Looks at destination and source addresses, ports, and services requested. Routers using ACLs to monitor network traffic.
Application-level proxy	Application layer	Looks deep into packets and makes granular access control decisions. It requires one proxy per protocol.
Circuit-level proxy	Session layer	Looks only at the header packet information. It protects a wider range of protocols and services than an application-level proxy, but does not provide the detailed level of control available to an application-level proxy.
Stateful	Network layer	Looks at the state and context of packets. Keeps track of each conversation using a state table.
Kernel proxy	Application layer	Faster because processing is done in the kernel. One network stack is created for each packet.

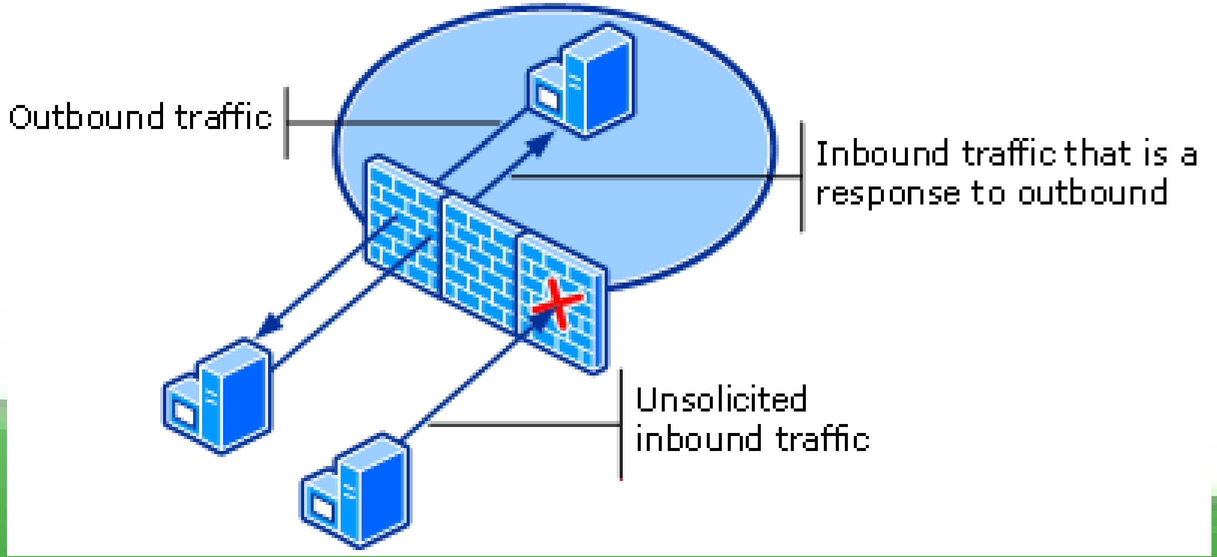
Firewall Basing

Bastion Host

- A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security.
- A bastion host is a critical strong point in the network's security, serving as a platform for an application-level or circuit-level gateway, or for external services. It is thus potentially exposed to "hostile" elements and must be secured to withstand this. Common characteristics of a bastion host include that it:
  - **executes a secure version of its OS, making it a trusted system**
  - **has only essential services installed on the bastion host**
  - **may require additional authentication before a user may access to proxy services**
  - **configured to use only subset of standard commands, access only specific hosts**
  - **maintains detailed audit information by logging all traffic**
  - **each proxy module a very small software package designed for network security**
  - **has each proxy independent of other proxies on the bastion host- in case of problems, can be uninstalled without affecting others.**
  - **have a proxy performs no disk access other than read its initial configuration file to safeguard against Trojan horses.**
  - **have each proxy run as a non-privileged user in a private and secured directory**
- A bastion host may have two or more network interfaces (or ports), and must be trusted to enforce trusted separation between these network connections, relaying traffic only according to policy.

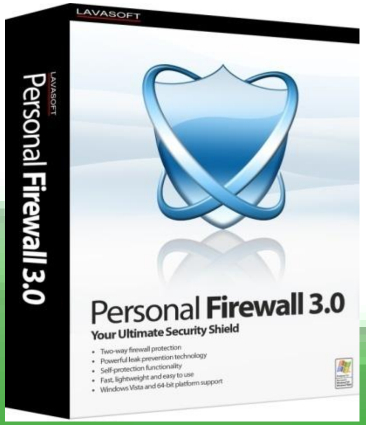
Host-Based Firewalls

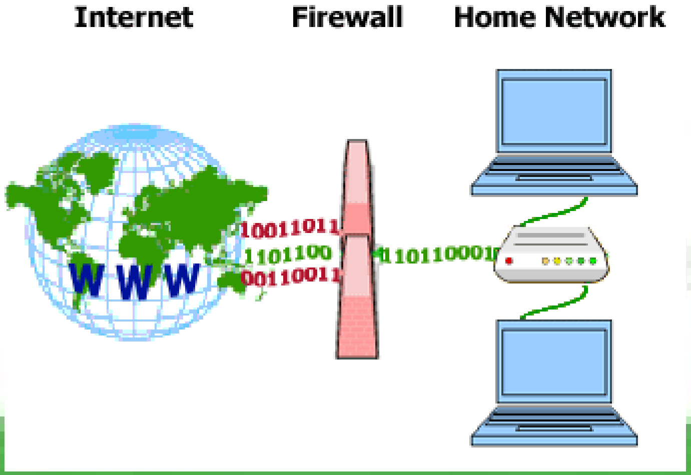
- A host-based firewall is a software module used to secure an individual host. Such modules are available in many operating systems or can be provided as an add-on package. Like conventional stand-alone firewalls, host-resident firewalls filter and restrict the flow of packets.
- A common location for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

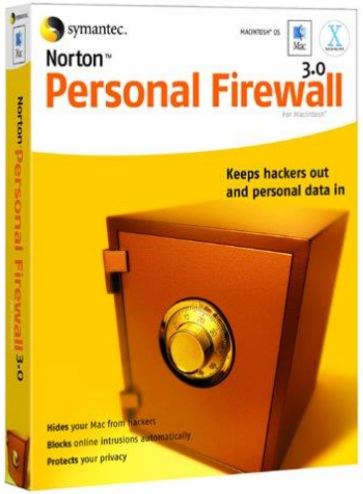

Outbound traffic
Inbound traffic that is a response to outbound
Unsolicited inbound traffic

Personal Firewalls

- 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. Personal firewall functionality can be used in the home environment and on corporate intranets. Typically, the personal firewall is a software module on the personal 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.
- Personal firewalls are typically much less complex than either server-based firewalls or stand-alone firewalls. 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.


LAVASOFT
LAVASOFT
Personal Firewall 3.0
Personal Firewall 3.0
Your Ultimate Security Shield
Two-way firewall protection
Powerful leak prevention technology
Self-protection functionality
Fast, lightweight and easy to use
Windows Vista and 64-bit platform support

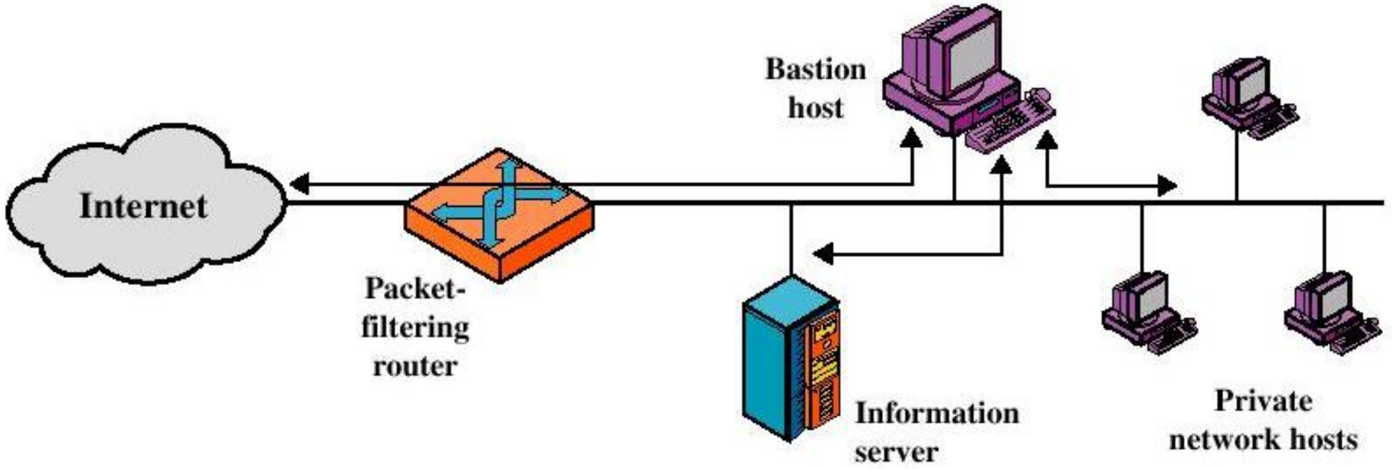




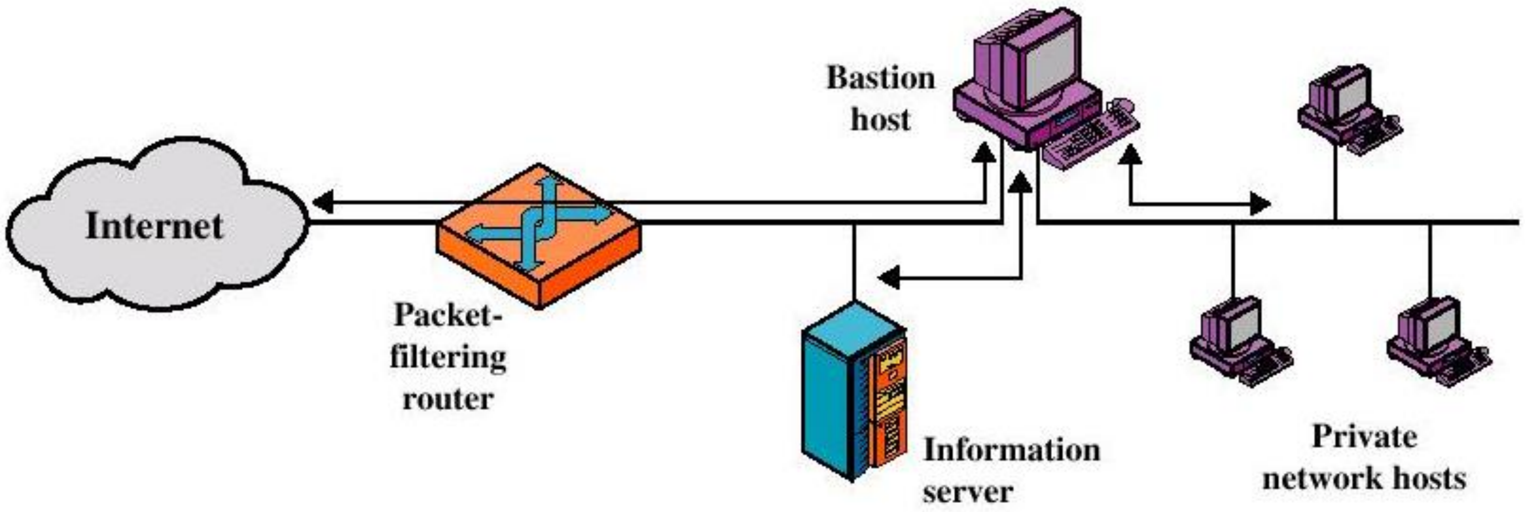
Firewall Configurations

- 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 addition to the use of a simple configuration consisting of a single system, more complex configurations are possible and indeed more common. Three common configurations exist:
  - ❖ screened host firewall, single-homed bastion configuration
  - ❖ screened host firewall, dual-homed bastion configuration
  - ❖ screened subnet firewall configuration

- In **Screened host firewall, single-homed bastion configuration**, the firewall consists of two systems:
  - a packet-filtering router - allows Internet packets to/from bastion only
  - a bastion host - performs authentication and proxy functions

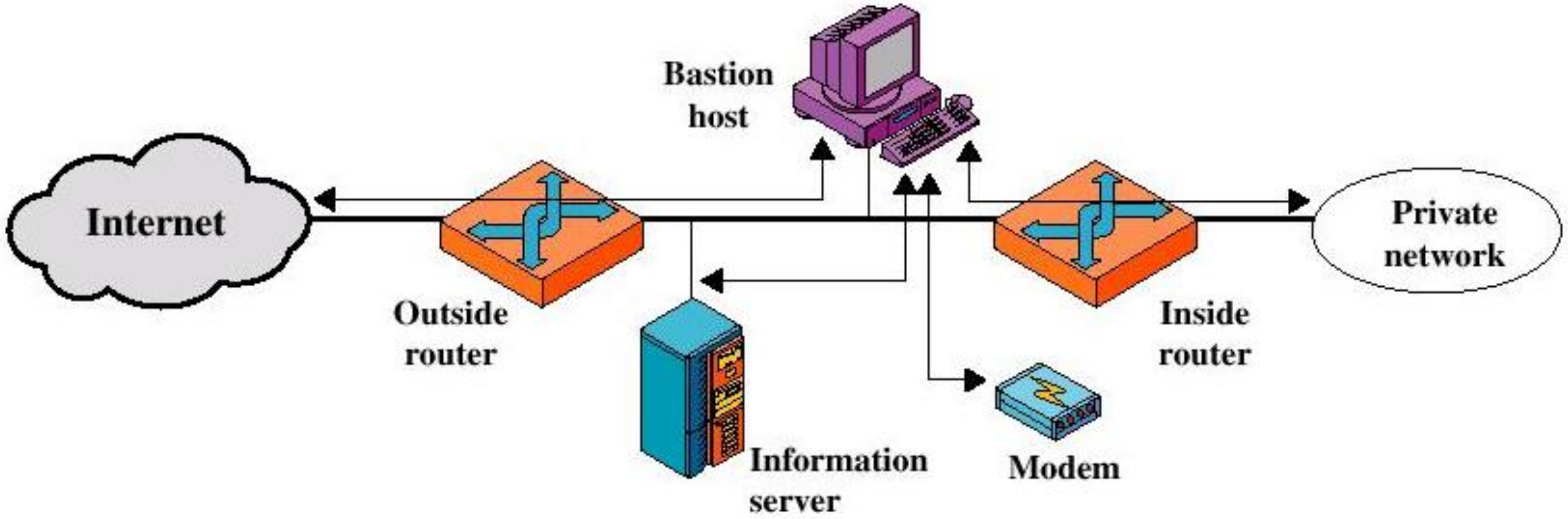


- This configuration has greater security, as it implements both packet-level & application-level filtering, forces an intruder to generally penetrate two separate systems to compromise internal security, & also affords flexibility in providing direct Internet access to specific internal servers (eg web) if desired.



- In the “**screened host firewall, dual-homed bastion configuration**” which physically separates the external and internal networks, ensuring two systems must be compromised to breach security. The advantages of dual layers of security are also present here.
- Again, an information server or other hosts can be allowed direct communication with the router if this is in accord with the security policy, but are now separated from the internal network.

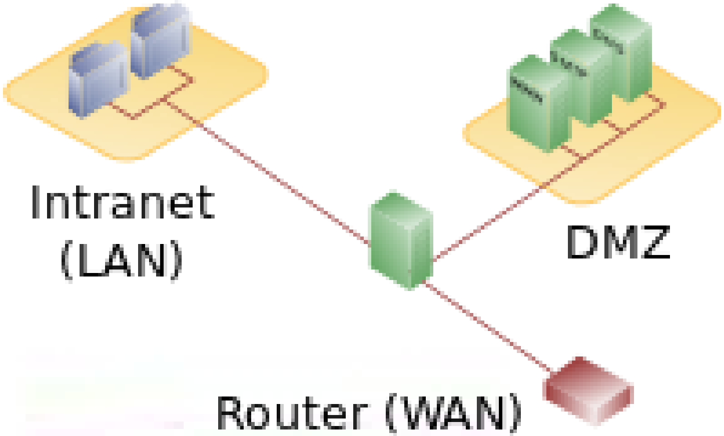
The **screened subnet firewall** configuration is most secure. It has two packet-filtering routers, one between the bastion host and the Internet and the other between the bastion host and the internal network, creating an isolated subnetwork. This may consist of simply the bastion host but may also 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.

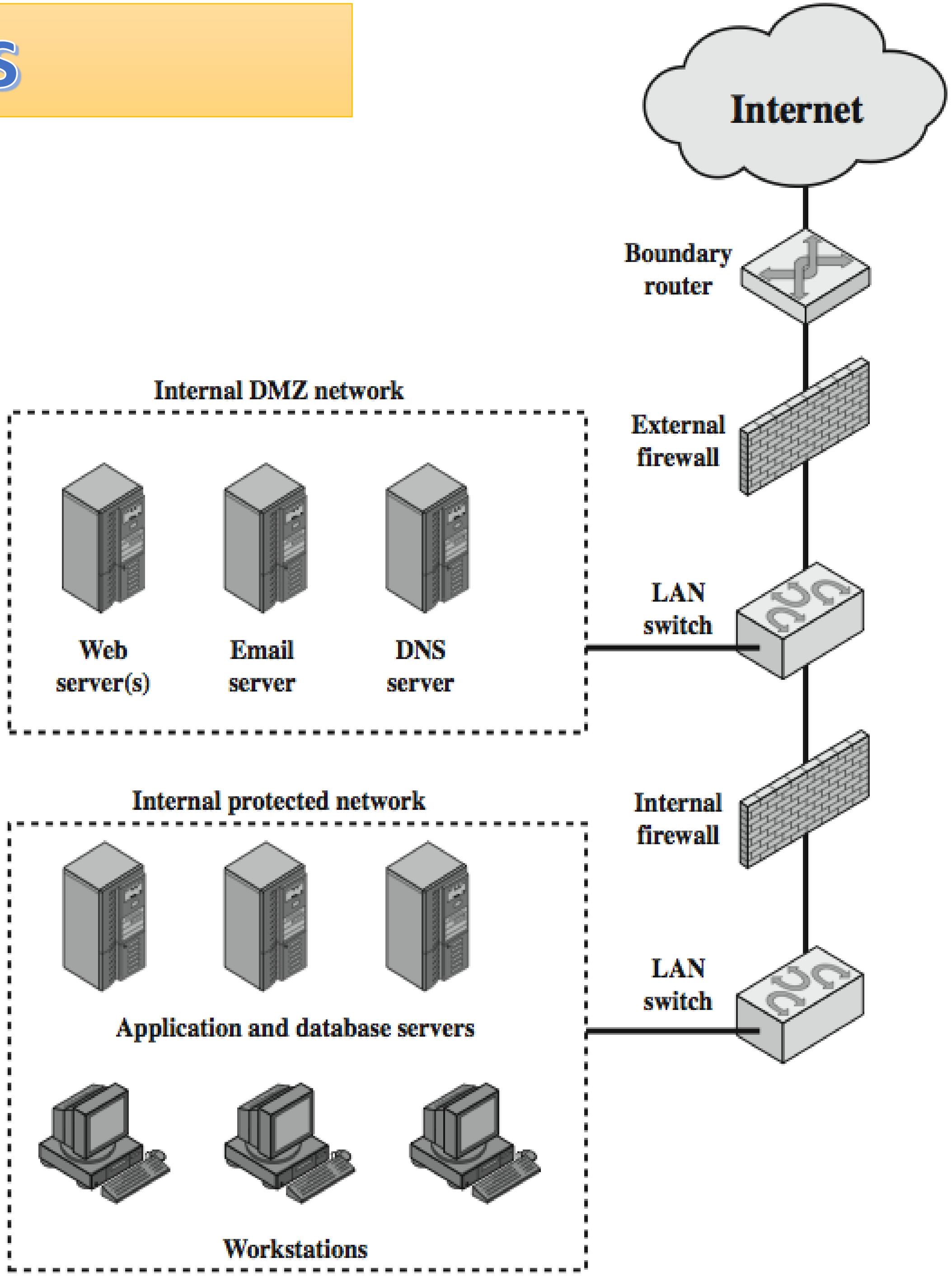


- This configuration offers several advantages:
  - There are now three levels of defense to thwart intruders
  - The outside router advertises only the existence of the screened subnet to the Internet; therefore the internal network is invisible to the Internet

DMZ Networks

- In computer security, a **DMZ** or **demilitarized zone** (sometimes referred to as a **perimeter network**) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a usually larger and untrusted network, usually the Internet.
- The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.



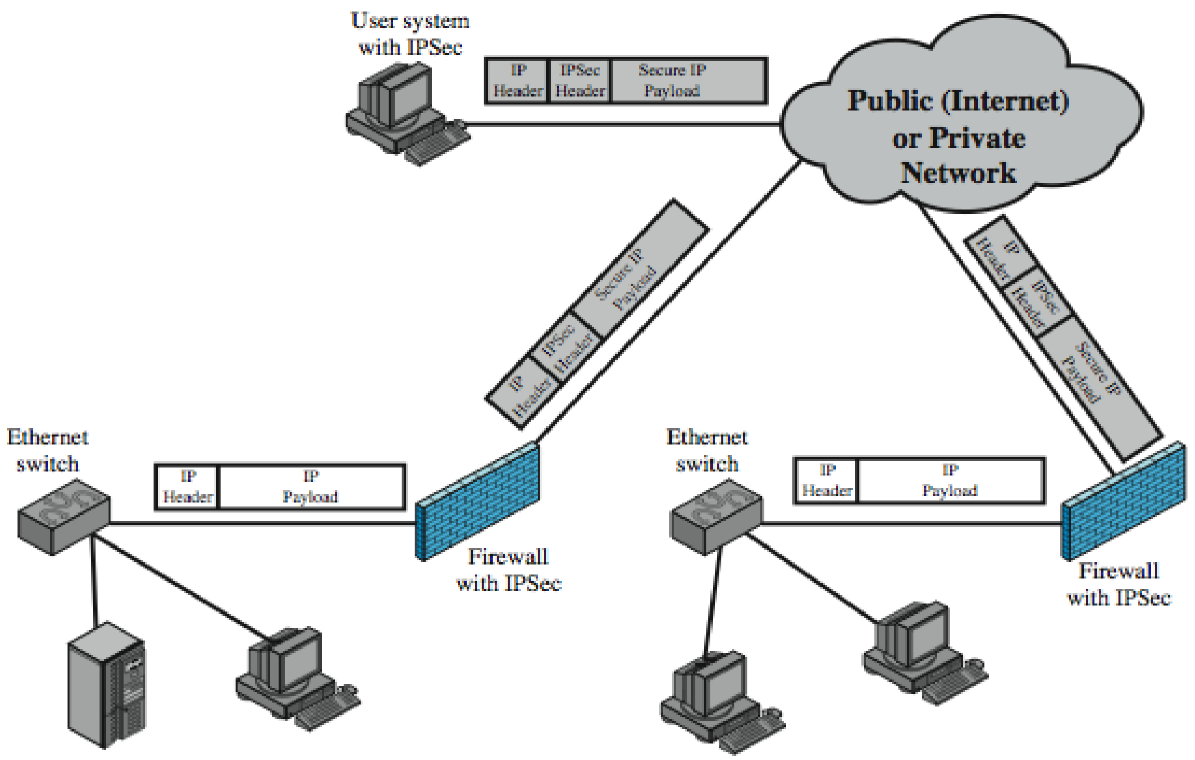


- An external firewall is placed at the edge of a local or enterprise network, just inside the boundary router that connects to the Internet or some wide area network (WAN). One or more internal firewalls protect the bulk of the enterprise network. Systems that are externally accessible but need some protections are usually located on DMZ networks.
- Typically, the systems in the DMZ require or foster external connectivity, such as a corporate Web site, an e-mail server, or a DNS (domain name system) server. The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. The external firewall also provides a basic level of protection for the remainder of the enterprise network.
- In this type of configuration, internal firewalls serve three purposes:
  1. The internal firewall adds more stringent filtering capability, vs the external firewall, to protect enterprise servers and workstations from external attack.
  2. The internal firewall provides two-way protection with respect to the DMZ, as it protects the remainder of the network from attacks launched from DMZ systems, and protects DMZ systems from attack by internal hosts.
  3. Multiple internal firewalls can be used to protect portions of the internal network from each other.
- A common practice is to place the DMZ on a different network interface on the external firewall from that used to access the internal networks.

Virtual Private Networks

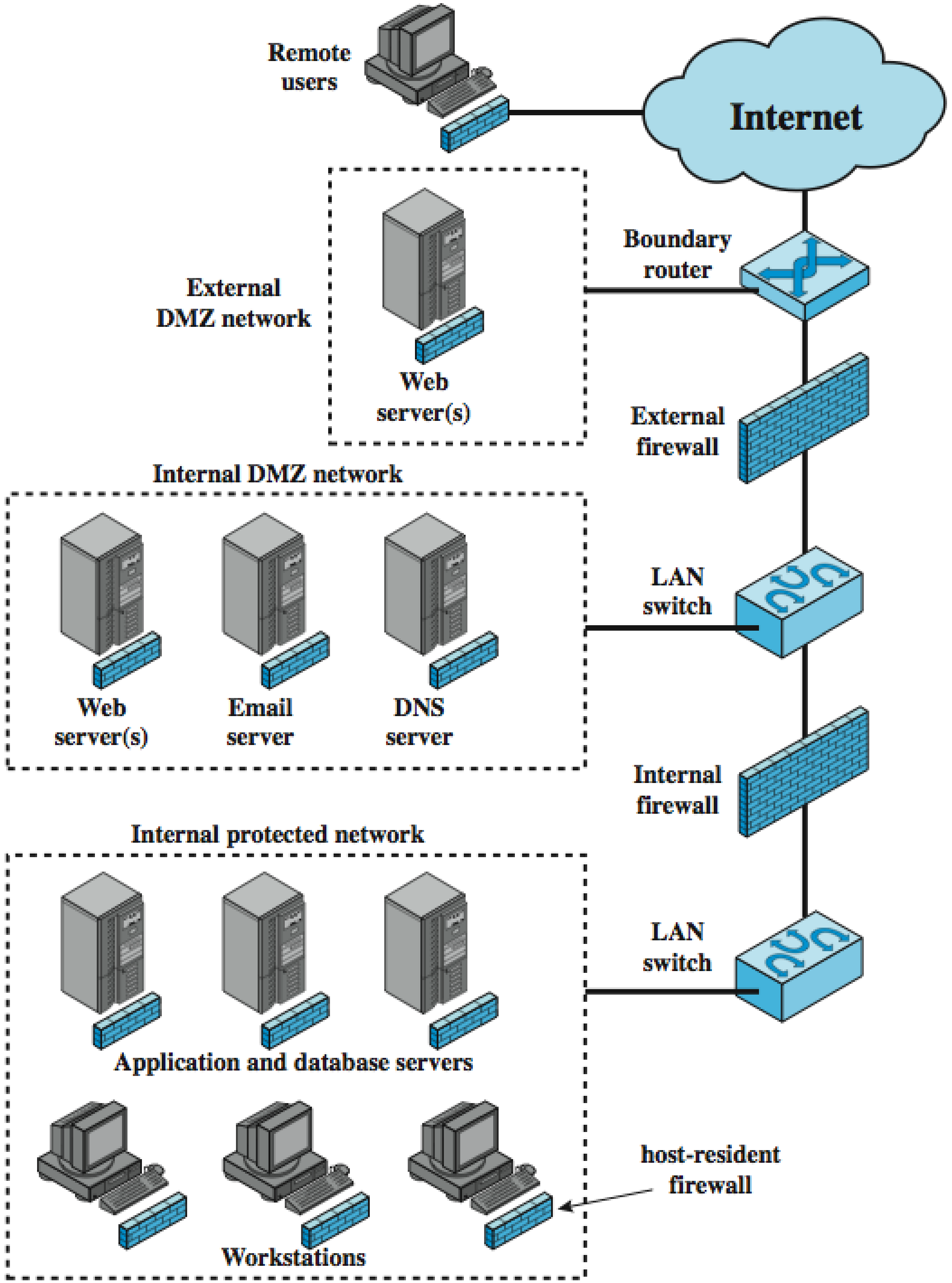
- In today's distributed computing environment, the **virtual private network (VPN)** offers an attractive solution to network managers. The VPN consists of a set of computers that interconnect by means of a relatively unsecure network and that make use of encryption and special protocols to provide security. At each corporate site, workstations, servers, and databases are linked by one or more local area networks (LANs).
- The Internet or some other public network can be used to interconnect sites, providing a cost savings over the use of a private network and offloading the wide area network management task to the public network provider. That same public network provides an access path for telecommuters and other mobile employees to log on to corporate systems from remote sites.

- A logical means of implementing an IPSec is in a firewall. If IPSec is implemented in a separate box behind (internal to) the firewall, then VPN traffic passing through the firewall in both directions is encrypted.
- In this case, the firewall is unable to perform its filtering function or other security functions, such as access control, logging, or scanning for viruses.
- IPSec could be implemented in the boundary router, outside the firewall. However, this device is likely to be less secure than the firewall and thus less desirable as an IPSec platform.



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 workstation 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.
- An important aspect of a distributed firewall configuration is security monitoring. Such monitoring typically includes log aggregation and analysis, firewall statistics, and fine-grained remote monitoring of individual hosts if needed



Summary of Firewall Locations and Topologies

- **Host-resident firewall**: includes personal firewall software and firewall software on servers, 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. Typical for small office/home office (SOHO) use.
- **Single bastion inline:** A single firewall device between an internal and external router. The firewall may implement stateful filters and/or application proxies. 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. Again, this is a common appliance configuration for medium to large organizations.
- **Double bastion inline:** The DMZ is sandwiched between bastion firewalls. This configuration is common for large businesses and government 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. For example, this configuration is required for Australian government use.
- **Distributed firewall configuration**: This configuration is used by some large businesses and government organizations.