Cryptography and Network Security

Chapter 10

Firewalls

Lectured by
Nguyễn Đức Thái

Outline

- The Need for Firewalls
- Firewall Characteristics
- Types of Firewalls
- Firewall Basing
- Firewall Location and Configurations

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***.

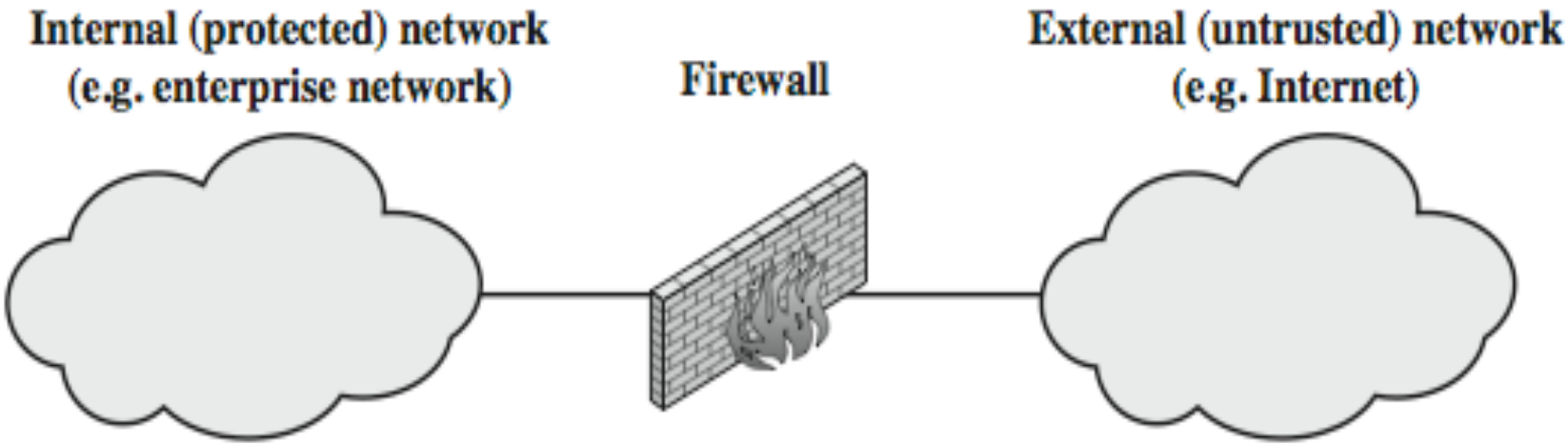
Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet

The Needs for Firewalls

Where we need firewalls?

- 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

What is a Firewall?



What is 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.

What is a Firewall?

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 IPsec***. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

Firewall Characteristics

Design 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. Various configurations are possible.
- 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***.
- The firewall ***itself*** is ***immune*** to penetration. This implies the use of a hardened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall and often required in government applications.

Firewall Characteristics

Firewalls have been evolved, provide services:

- **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, 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**: Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
- **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 (Chapter 19).
- **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 Characteristics

Firewalls capability:

- 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.
- A firewall provides a ***location for monitoring*** security-related events. Audits and alarms can be implemented on the firewall system.
- 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.
- A firewall can serve as the ***platform for IPsec***. Using the tunnel mode capability, the firewall can be used to implement virtual private networks.

Firewall Limitations

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 ***may not protect*** fully against ***internal threats***, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
3. An improperly secured wireless LAN may be accessed from outside the organization. An ***internal firewall*** that separates portions of an enterprise network ***cannot guard*** against wireless communications between local systems on different sides of the internal firewall.
4. A laptop, PDA, or portable storage device ***may be used*** and infected outside the corporate network, and then attached and used internally.

Types of Firewalls

- A firewall may act as a ***packet filter***.
- It can operate
  - as a ***positive filter***, allowing to pass only packets that meet specific criteria,

  or
  - as a ***negative filter***, rejecting any packet that meets 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 Firewall

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

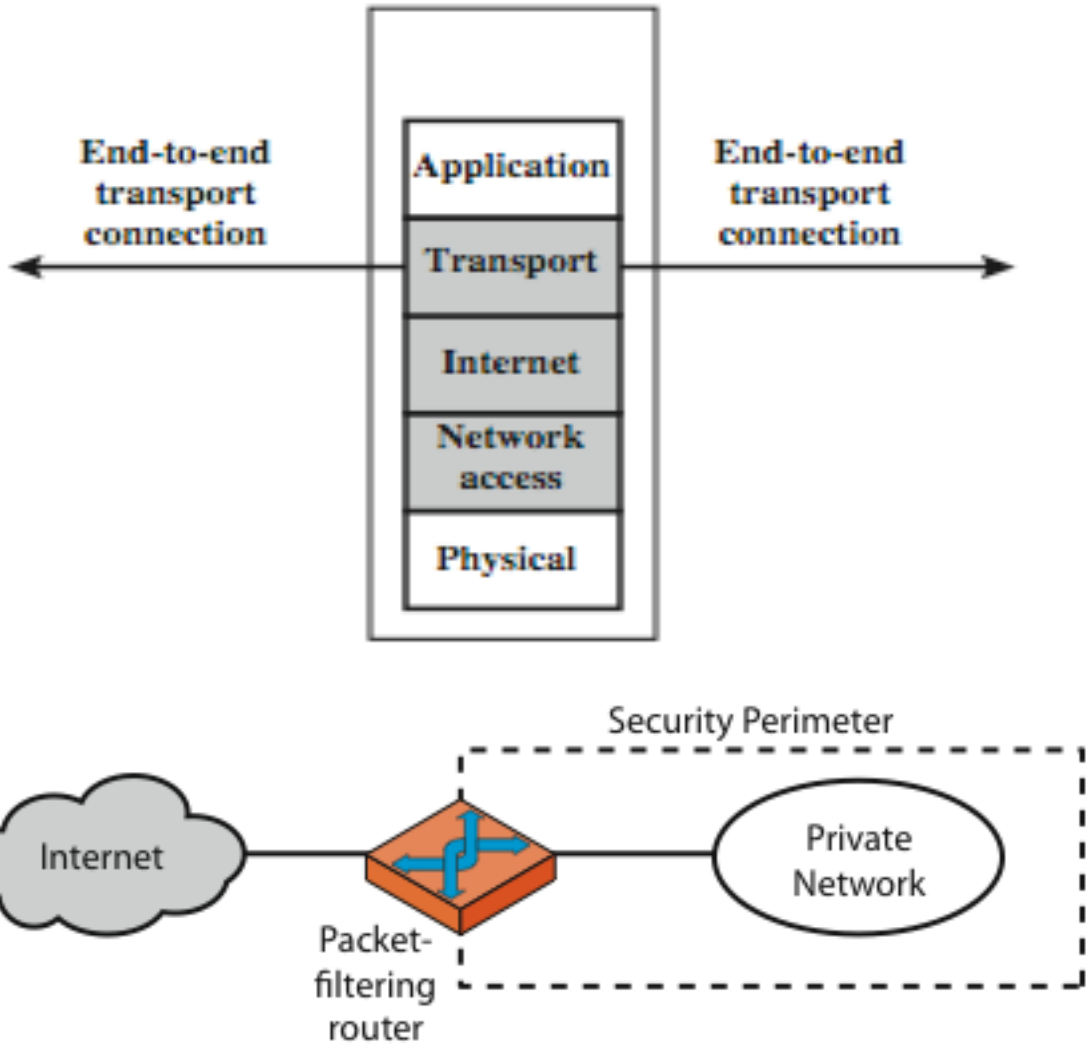
Packet Filtering Firewall

- **Filtering rules are based on information contained in a network packet:**
  - Source IP address
  - Destination IP address
  - Source and destination transport-level address: ***port***
  - IP protocol field: *(Defines the transport protocol)*
  - Interface: *(For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall 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.
- 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.

Packet Filtering Firewall



(a) Packet-filtering router

Firewalls – Packet Filters

Table 20.1 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

Attacks on Packet Filters

- **IP Address Spoofing**
  - **fake** source address to be trusted
  - add filters on router to block
- **Source Routing Attacks**
  - attacker sets a route other than default
  - block source routed packets
- **Tiny Fragment Attacks**
  - split header info over several tiny packets
  - either discard or reassemble before check

IP Address Spoofing

- The intruder ***transmits packets*** from the outside with a source IP address field containing an address of an internal host.
- The attacker hopes that the use of a spoofed address will ***allow penetration of systems*** that employ simple source address security, in which packets from specific trusted internal hosts are accepted.
- The countermeasure is to ***discard packets*** with an inside source address if the packet arrives on an external interface.
- In fact, this countermeasure is often implemented at the router ***external to*** the firewall

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.
- Typically, a packet filter will make a filtering decision on the ***first fragment of a packet***.
- All subsequent fragments of that packet are ***filtered*** out solely on the basis that they are part of the packet whose first fragment was rejected.
- The attacker hopes that the filtering firewall examines only the first fragment and that the remaining fragments are passed through.
- A tiny fragment attack can be defeated by enforcing a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header.
- If the first fragment is rejected, the filter can remember the packet and discard all subsequent fragments.

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.
- The countermeasure is to ***discard all packets*** that use this option

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.

Firewall Basing

- Bastion Host
- Host-Based Firewalls
- Personal Firewall

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.

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***.

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.
- 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 Firewall

- 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

Firewall Location and Configurations

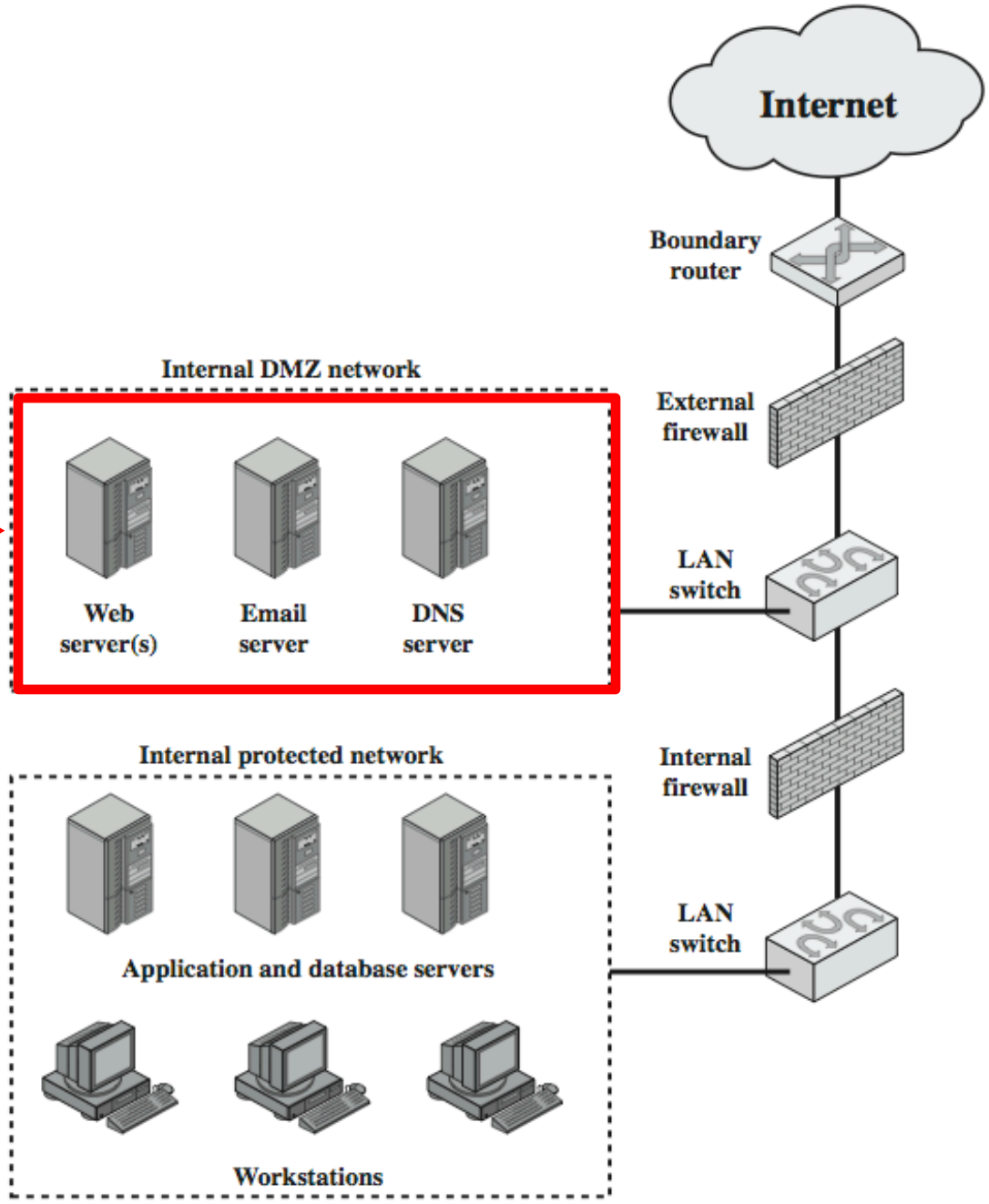
- A firewall is positioned to provide a protective barrier between an external, potentially untrusted source of traffic and an internal network.
- With that general principle in mind, a security administrator must ***decide*** on the ***location*** and on the ***number*** of firewalls needed.

DMZ Networks

Demilitarized Zone

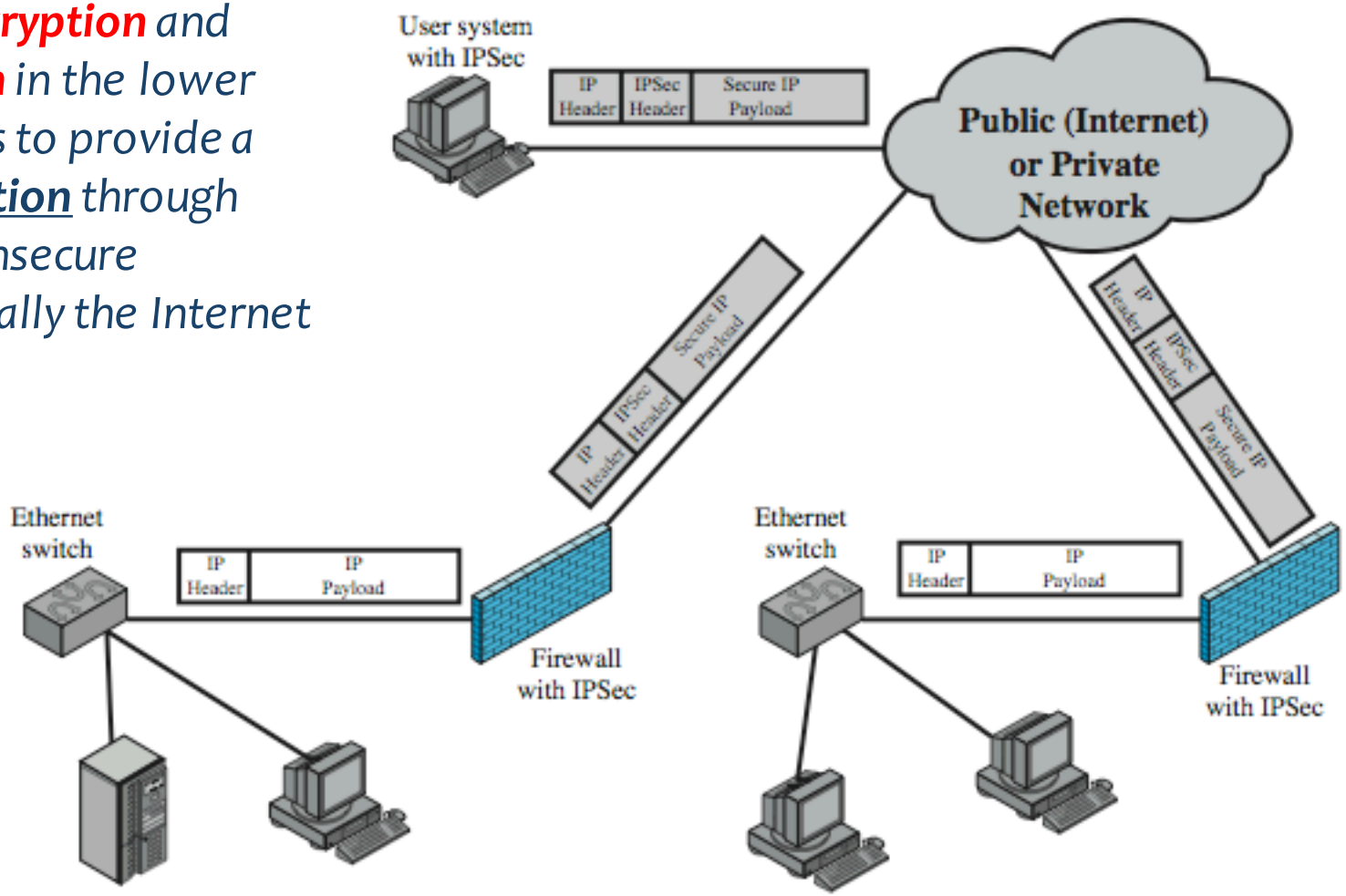
*Network **between** **external** and **internal** firewalls*

DMZ



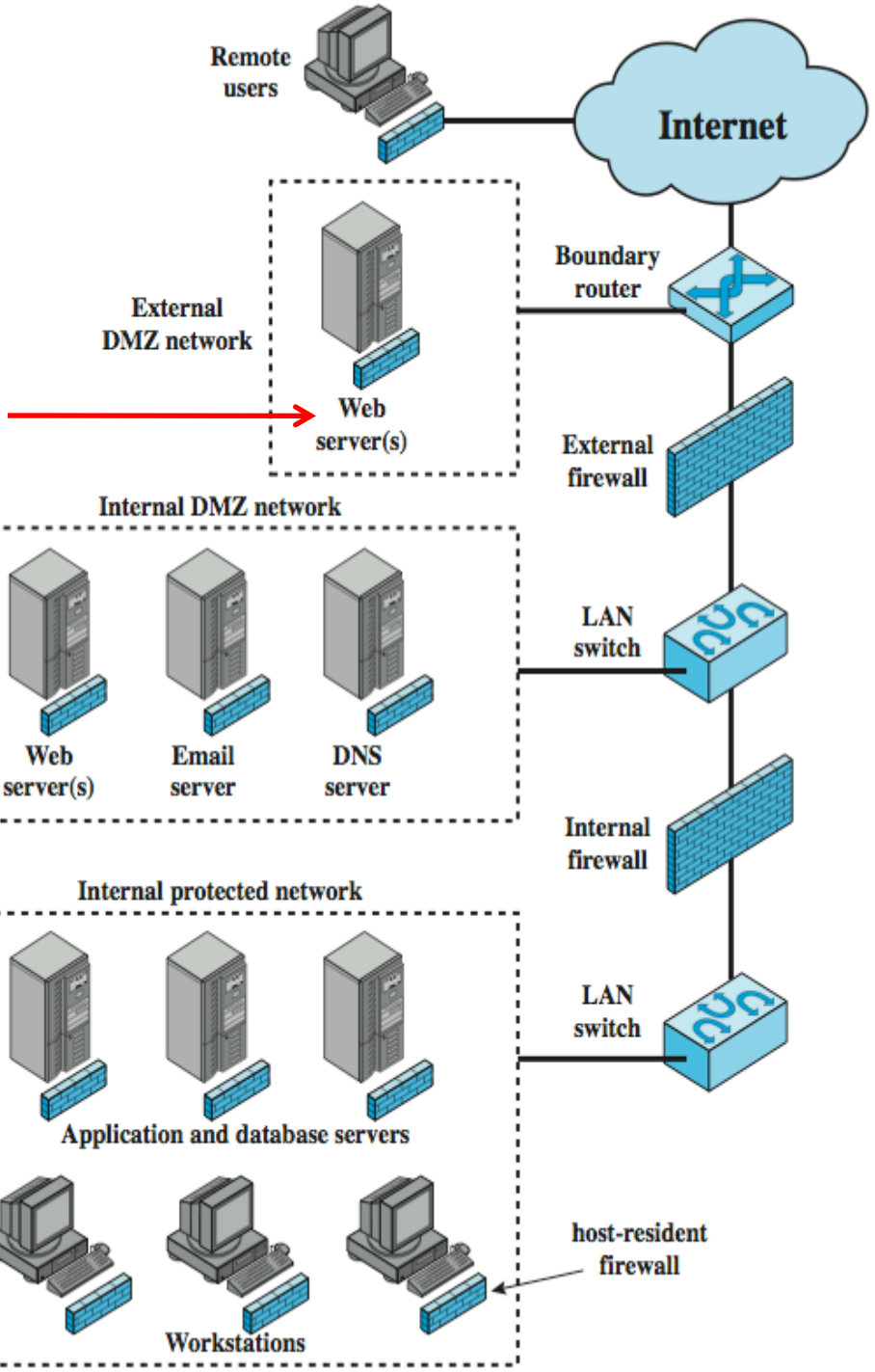
Virtual Private Networks (VPN)

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



Distributed Firewalls

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.*



Distributed Firewalls

- Administrators can configure host-resident firewalls on *hundreds* of servers and workstations as well as configure personal firewalls on *local* and *remote* user systems
- With distributed firewalls, it may make sense to establish both an internal and an external DMZ.
- An important aspect of a distributed firewall configuration is ***security monitoring***.

Summary of Firewall Locations & Topols

- ***Host-resident firewall***: This category includes *personal* firewall software and firewall software on servers.
- ***Screening router***: A *single router* between internal and external networks with stateless or full packet filtering.
- ***Single bastion inline***: A *single firewall device* between an internal and external router.
- ***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***: configuration, where the DMZ is sandwiched between bastion firewalls.
- ***Double bastion T***: The DMZ is on a separate network interface on the bastion firewall.
- ***Distributed firewall configuration***

Summary

- The Need for Firewalls
- Firewall Characteristics
- Types of Firewalls
- Firewall Basing
- Firewall Location and Configurations

References

1. Cryptography and Network Security, Principles and Practice, William Stallings, Prentice Hall, Sixth Edition, 2013