



MONASH University
Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

COMMONWEALTH OF AUSTRALIA

Copyright Regulations 1969

WARNING

This material has been reproduced and communicated to you by or on behalf of Monash University pursuant to Part VB of the *Copyright Act 1968* (the Act).

The material in this communication may be subject to copyright under the Act. Any further reproduction or communication of this material by you may be the subject of copyright protection under the Act.

Do not remove this notice.

Lecture 11:

Firewall

Unit Objectives

- ✓ OSI security architecture
 - **common security standards and protocols for network security applications**
 - **common information risks and requirements**
- ✓ operation of private key encryption techniques
- ✓ operation of public encryption techniques
- ✓ concepts and techniques for digital signatures, authentication and non-repudiation
- ✓ security threats of web servers, and their possible countermeasures
- ✓ Wireless Network Security Issues
- ✓ security threats of email systems and their possible countermeasures
- ✓ IP security
- ✓ intrusion detection techniques for security purpose
- ✓ risk of malicious software, virus and worm threats, and countermeasures
- ✓ **firewall deployment and configuration to enhance protection of information assets**

Review of previous Lecture

Key points from the last lecture:

- Perhaps the biggest threat to computer system comes from malicious software
- Strong countermeasures are necessary to protect computer systems and information assets
- Malicious programs can be host dependent or self contained; similarly replicating or non-replicating
- **Malicious programs can be divided into five types**
 - Trap door
 - Logic bomb
 - Trojan horse
 - Virus
 - Worm
- Virus and worm attacks are the two most widely known attacks that sometimes spread world-wide very quickly infecting millions of computers
- Antivirus software is deployed to scan for virus infection
- **Generic Decryption & Digital Immune System** are two advanced antivirus techniques
- Distributed Denial of Service attacks

Lecture 11: Learning Objective

On completion of this session you should:

- Understand why firewalls are necessary
- Discuss the design goals of firewalls
- Discuss what firewalls can do and cannot do
- Be familiar with different types of firewalls
- Describe the advantages and disadvantages of different types of firewalls
- Be familiar with various firewall configurations
- Discuss what level of security each configuration offers

Lecture 11: Outline

- **What is a firewall?**
- **Firewall design goals**
- **What firewalls can do**
- **What firewalls can't do**
- **Types of firewalls**
- **Firewall configurations**

Firewalls: Introduction

- **Information systems have evolved**
 - from centralized data processing system to → Inter-networked distributed data access and Internet connection
- **This growth has introduced persistent security concerns, because**
 - it is **not practical to equip** each workstation and server with intrusion protection
 - flawless OS and software **can't be guaranteed**
 - networks usually consists of hundreds and thousands of systems running **mixed version of software**
- **A firewall can add to the security scheme**
 - erects an outer security wall
 - provides a single point where security and audit can be imposed
 - acts as the first line of defense

Firewall: Design Goals

- **Firewalls are based on the following design goals:**
 - all traffic in **both** direction must pass through the firewall
 - > implemented by physically blocking all accesses to the local network except via the firewall
 - only **authorized** traffic, defined by local security policies, will be allowed to pass
 - firewall itself must be **immune** to penetration
 - > underpins the use of trusted system with a secure operating system

Firewall: Services

Techniques used by firewalls to control access and enforce site's security policy:

- **Service control:**
 - determines the types of Internet services that can be accessed, inbound and outbound
 - e.g., may filter traffic on the basis of IP address and TCP port number
- **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 by authorized users
 - applied to internal and external users
- **Behavior control:**
 - controls how particular services are used
 - e.g., filters e-mail to eliminate spam, allows access to only a portion of information on web server

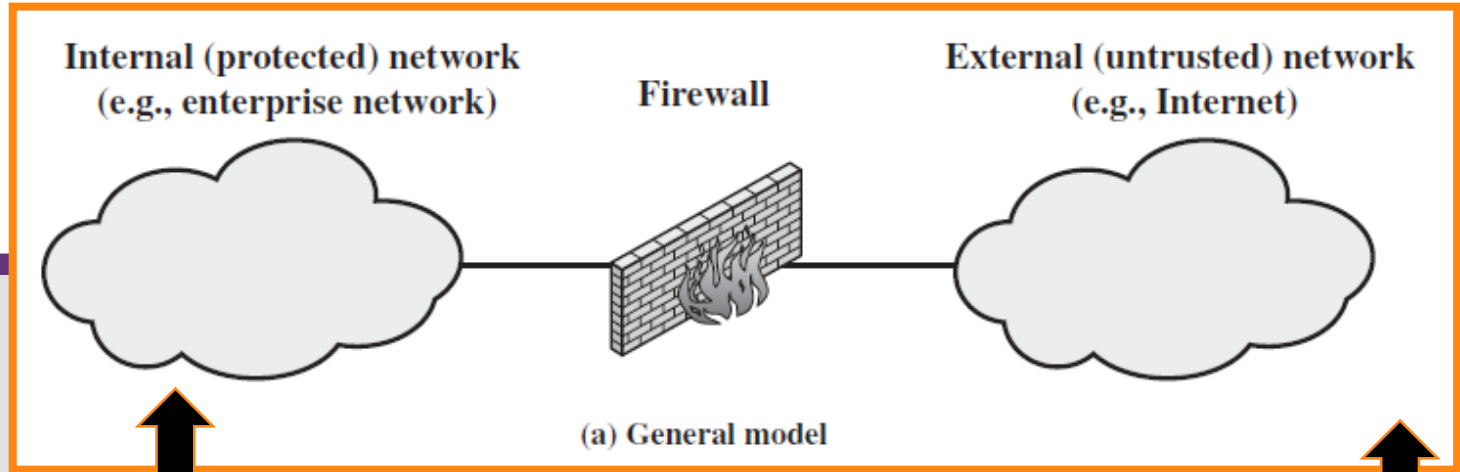
What Firewalls can do? ---(1)

- Manage **access between the organization's network (trusted) ↔ Internet (untrusted)**
 - without a firewall, security depends on the "hardness" of **each host's security features**
 - overall security is only as good as the **weakest link**
- Allow the network administrator to define a centralized "**choke point**"
 - *offer access control, protection from vulnerable services and routing attacks*
 - *simplify security management*
- Offer a convenient network point where security-related events can be **monitored and alarms** can be generated
- **NAT** (Network Address Translator) can be deployed at the firewall
- Firewall is a convenient point to **audit or log** Internet usage
- implement **VPNs** using IPsec
- must be **immune** to any **penetration** attack

What Firewalls can do? --- (2)

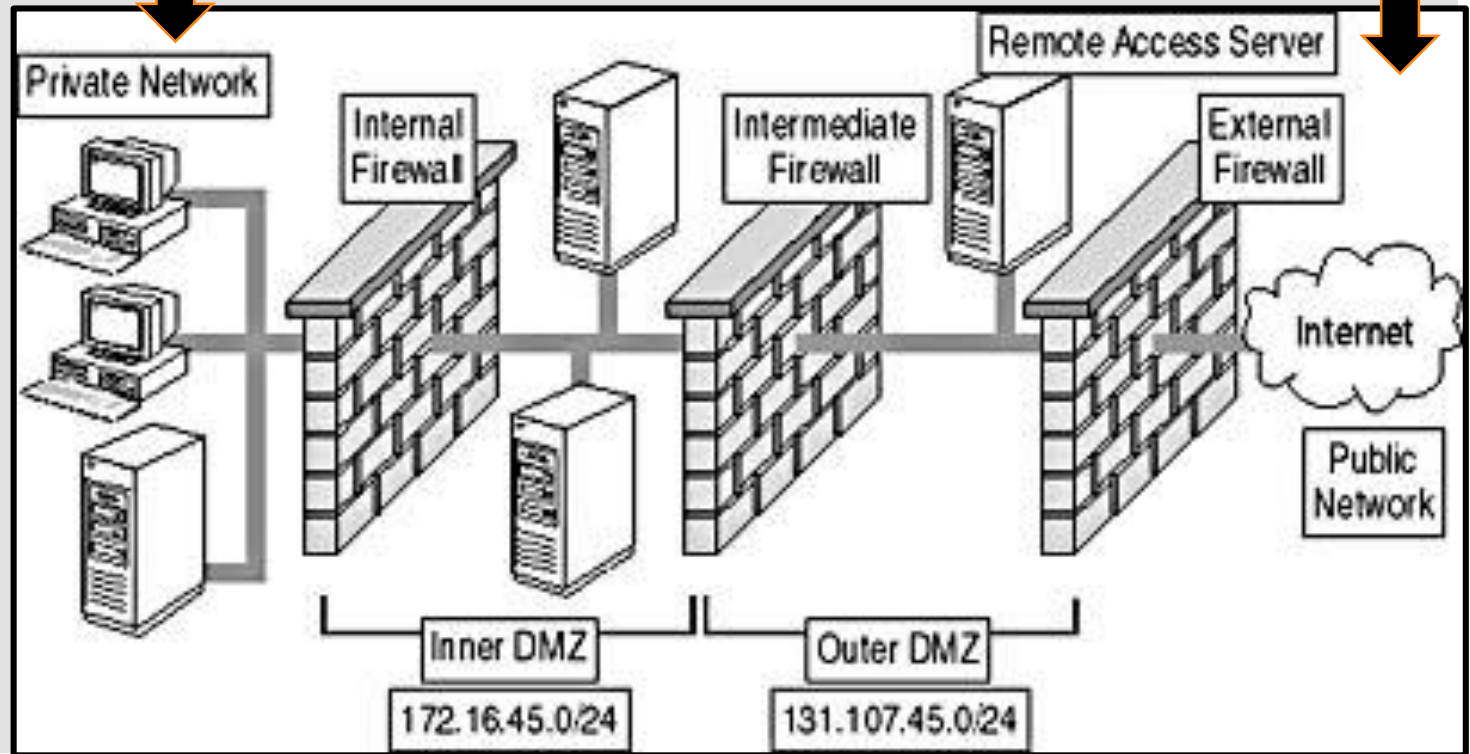
- There are **arguments** that the deployment of firewalls creates a **single point of failure**
- It should be emphasized that, just because we have **deployed firewalls**, security of individual host systems **cannot be neglected**
- Appropriate **security policies** must also be implemented in individual hosts to ensure security of **organization's network**

Simple firewall setup



What is a Firewall?


Complex firewall setup



What Firewalls can't do? ---Firewall Limitations

- cannot **protect from attacks bypassing it**
 - e.g. sneaker net, utility modems, trusted organisations, trusted services (e.g. SSL/SSH)
- cannot **protect against internal threats**
 - e.g. 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

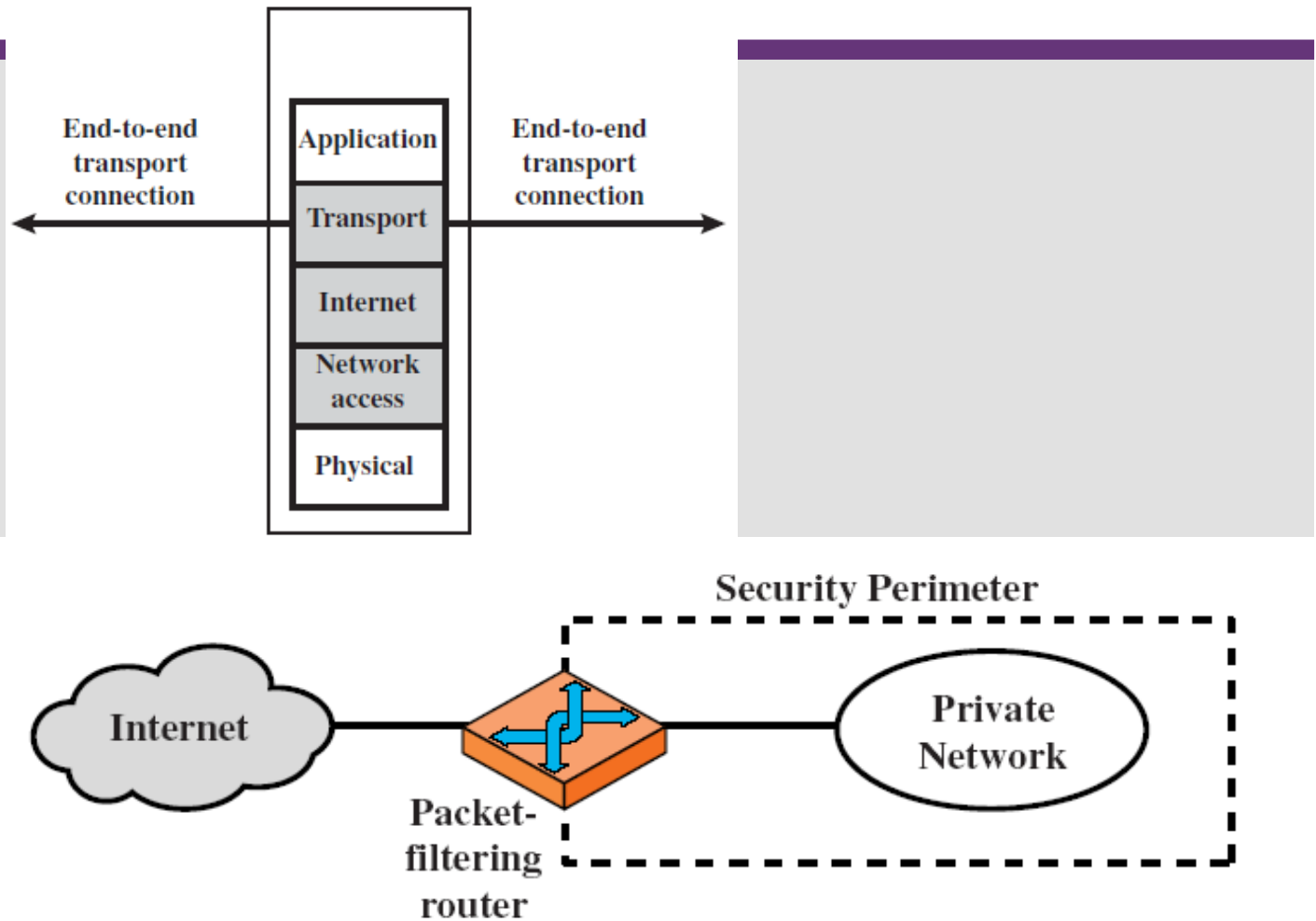
- **Packet filtering firewalls**
 - IP layer
 - Stateful packet filters
 - **Application gateway firewalls**
 - Application layer
 - **Circuit relay firewalls (Circuit Level Gateway)**
 - TCP layer
 - **Combinations of these**
- 

Packet filtering firewalls (1)

- Apply a **SET OF RULES** to each incoming IP packet and then either forwards or discards the packet
- Filter packets going in **BOTH DIRECTIONS**
- The packet filter is typically set up as a list of rules based on matches to fields in the **IP or TCP** header
 - source IP address
 - destination IP address
 - source and destination TCP or UDP port number
 - type of the protocol (IP, TCP, UDP or ICMP)
 - Message type (SYN, ACK, FIN, RST)

Firewalls – Packet Filters

Figure illustrates the packet filter firewall role as utilizing information from the transport, network & data link layers to make decisions on allowable traffic flows.



Packet filtering firewalls (4)

TABLE – packet-filtering rule sets:

- for each set
 - the rules are applied **top to bottom**
- ▶ Rule Set A
- Allow: Inbound mail to gateway host only except host - SPIGOT are blocked (Spammer)
- ▶ Rule Set B
- explicit **default policy (last rule)**
- ▶ Rule Set C
- Inside host can send mail to the outside **AND Outside machine could linked to inside port 25**
- ▶ Rule Set D
- Correct mail outbound rule with ACK flag of a TCP segment is set
- ▶ Rule Set E
- One approach to handling FTP connections

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 firewalls (3)

- **Two default policies (discard or forward)**
 - **Discard**: traffic expressly not permitted is prohibited
→ **more conservative**
 - **Forward**: traffic expressly not prohibited is permitted
→ **hence reduced security**
- **Allow all packets going to specific TCP ports while rest of the packets are dropped**
 - e.g., Web (port 80), DNS (port 53), and SMTP (port 25) be allowed
- **Do not allow any packets from external network with a source IP address of the internal network**
 - provides **anti-spoofing** protection

Packet filtering firewalls (4)

Advantages:

- Typically **faster** than other types of firewalls
 - because packet filtering is done at the **lower levels** of the OSI model, the time it takes to process a packet is **much quicker**
- Can be **implemented transparently**, typically require no additional configuration for clients
- Quite **inexpensive** to build routers with packet-filtering abilities
 - routers are already in the network providing routing functionality, with packet-filtering capabilities
 - thus avoids additional cost of deploying a packet-filter firewall
- Packet filtering firewalls typically **scale better** than other types of firewalls
- Packet filtering firewalls are **application independent**

Packet filtering firewalls (5)

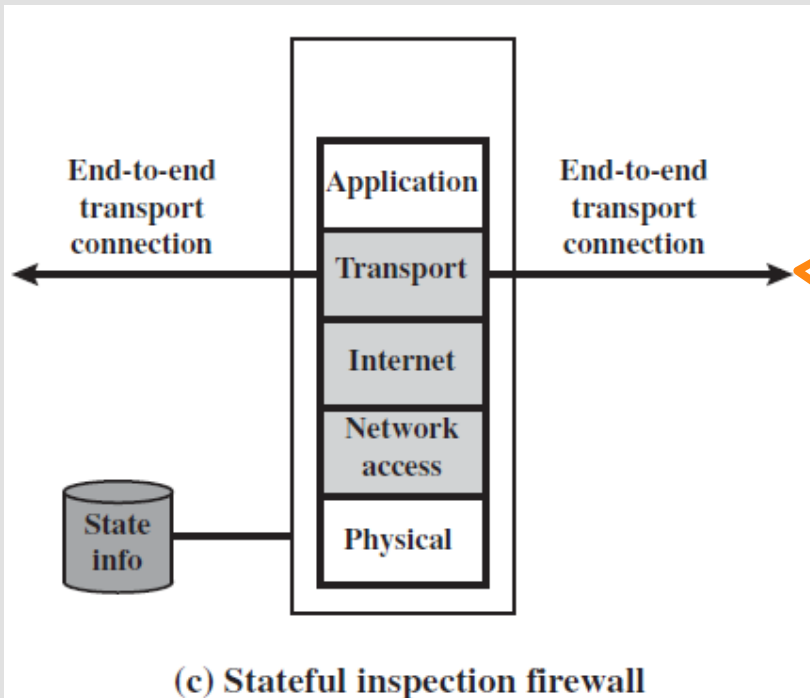
Disadvantages:

- **can't prevent** attacks that employ **application-specific** vulnerabilities
- **lack** advanced **user authentication**
- defining **rules and filters** on a packet filtering firewall can be a **complex task**
- **accuracy of rules** or filters on packet filtering firewalls can be very **difficult to test**
- packet filtering firewalls **are prone** to certain types of attacks,
 - e.g., DoS attack.
- packet filtering firewalls **do not work well** in an environment that needs **dynamic rules**

Attacks on Packet Filter

- **IP address spoofing**
 - fakes source address so that it appears to be coming from a trusted source
 - > countermeasure: **discards packets** with an inside source address if the packets arrive on an external interface
- **Source routing attacks**
 - attacker sets a route other than default
 - > countermeasure: **block source routed** packets
- **Tiny fragment attacks**
 - intruder uses the IP fragmentation option
 - split header info over several tiny packets
 - **countermeasure: either discard or check before reassemble**

Firewalls – Stateful Packet Filters



A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections. A stateful packet inspection firewall reviews information as a packet filtering firewall, but also records information about TCP connections. Some stateful firewalls also keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking.

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

Firewalls – Stateful Packet Filters

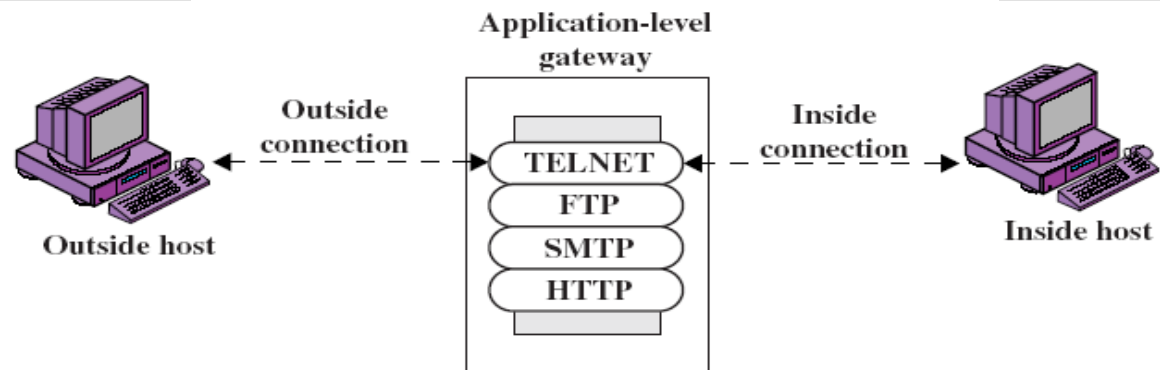
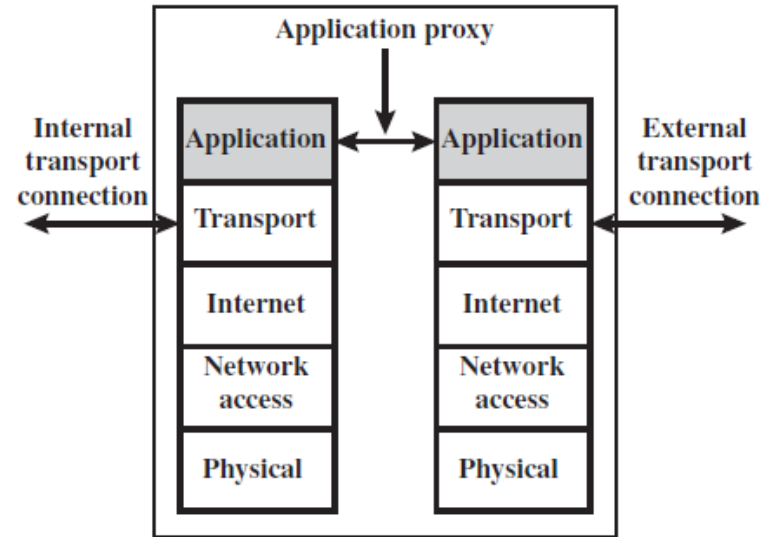
- **traditional packet filters do not examine higher layer context**
 - i.e. matching return packets with outgoing flow
- **stateful packet filters address this need**
- **they examine each IP packet in context**
 - keep track of client-server sessions
 - check each packet validity of its session
- **hence are able to detect bogus packets out of context**
- **may also even inspect limited application data**

Firewalls – Application Level Gateway(1)

- **Use an application specific gateway/proxy**
 - act as a relay of application level traffic
 - operates at layer 7 of the OSI model
- **Has full access to protocol**
 - user requests service from proxy
 - proxy validates request as legal
 - then actions request and returns result to user
- **Need separate proxies for each application**
 - some services naturally support proxying
 - others are more problematic
 - can be configured to support only **specific features of an application**

Firewalls – Application Level Gateway (2)

an application-level gateway (or proxy server), emphasizes that it only supports a specific list of application services. It acts as a relay of application-level traffic. A user contacts the gateway to access some service, provides details of the service, remote host & authentication details, contacts the application on the remote host and relays all data between the two endpoints. Application-level gateways tend to be more secure than packet filters, stateful packet filter, & can log and audit traffic at application level.



Firewalls – Application Level Gateway: Operation

- A client on the **internal network** requests access to an application (e.g. web access) on the **external network**
- The **request is forwarded to the proxy sever** (e.g., HTTP proxy server)
- The proxy determines whether the request **is valid**
 - checks against the security policies of the organization
- Then **sends a new request on behalf of the client to the destination**
 - **no direct connection from internal to external network**
 - the request appears to have originated from the application gateway/proxy
- Any response from the external network is sent back to the application gateway/proxy
 - proxy determines **if it is valid** and then sends it on to the client

Firewalls – Application Level Gateway (3)

Advantages:

- more secure than packet filters
- Only needs to scrutinize a few allowable applications
 - do not need to deal with numerous combination of filtering rules
- it is **easy to log** and **audit** all incoming traffic at the application level
- allows the network administrator to have more control over traffic passing through the firewall
- application gateways/proxies **offer robust user authentication**

Firewalls – Application Level Gateway (4)

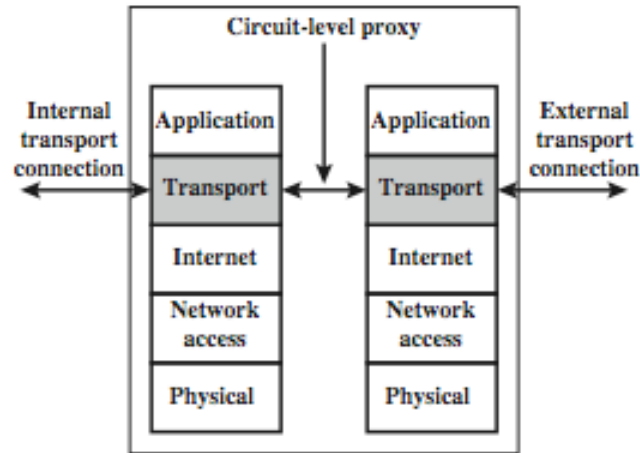
Disadvantages:

- The prime disadvantage is the **additional processing overload** on each connection
 - **slower** than packet-filtering firewall
- Each protocol (HTTP, SMTP, etc.) requires its own gateway/proxy application
 - if one does not exist, then the corresponding protocol will not be allowed through the firewall
- Typically requires **additional client configuration**
- **Proxy can be a single point of failure**
 - since all requests are channeled through the proxy server
- **Implementation costs** can be **high**
 - may require the purchase of additional hardware, software, expertise, or support

Circuit Level Gateway or Circuit-level-Proxy (1)

- Stand-alone system or specialized function performed by an Application-level Gateway
- Sets up two TCP connections
 - one between itself and a TCP user on internal host and another between itself and a TCP user on the outside host
- 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
- Typically used in situations where system administrators trust the internal users
- An example of circuit level gateway implementation is the SOCKS package specified in RFC1928.

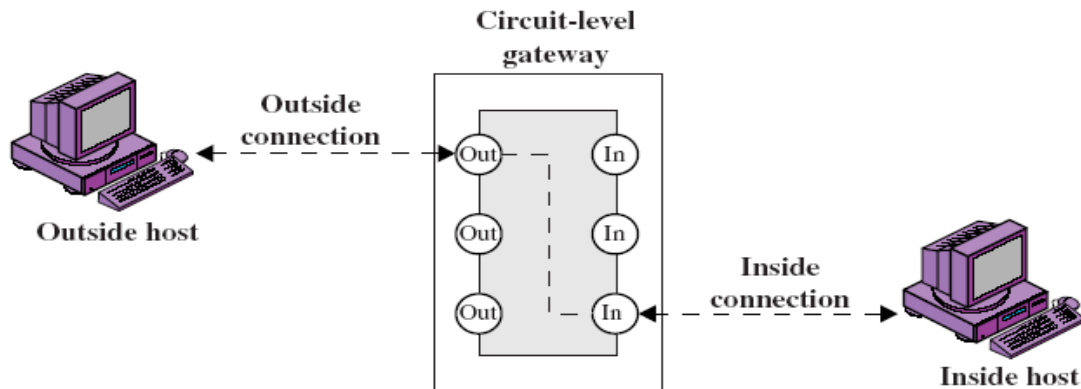
Circuit Level Gateway or Circuit-level-Proxy (2)



(e) Circuit-level proxy firewall

A circuit-level gateway, showing how it relays between 2 TCP connections.

- ✓ Note that it can be implemented in a stand-alone system or can be a specialized function in an application-level gateway for certain applications.
- ✓ Note also that relaying UDP packets is more problematical, because of the lack of connection context, and require a parallel TCP connection to provide these details.



(c) Circuit-level gateway

Bastion Host

- **highly secure host system**
- **runs circuit / application level gateways**
- **or provides externally accessible services**
- **potentially exposed to "hostile" elements**
- **hence is secured to withstand this**
 - hardened O/S, essential services, extra authentication
 - proxies small, secure, independent, non-privileged
- **may support 2 or more network connections**
- **may be trusted to enforce policy of trusted separation between these net connections**

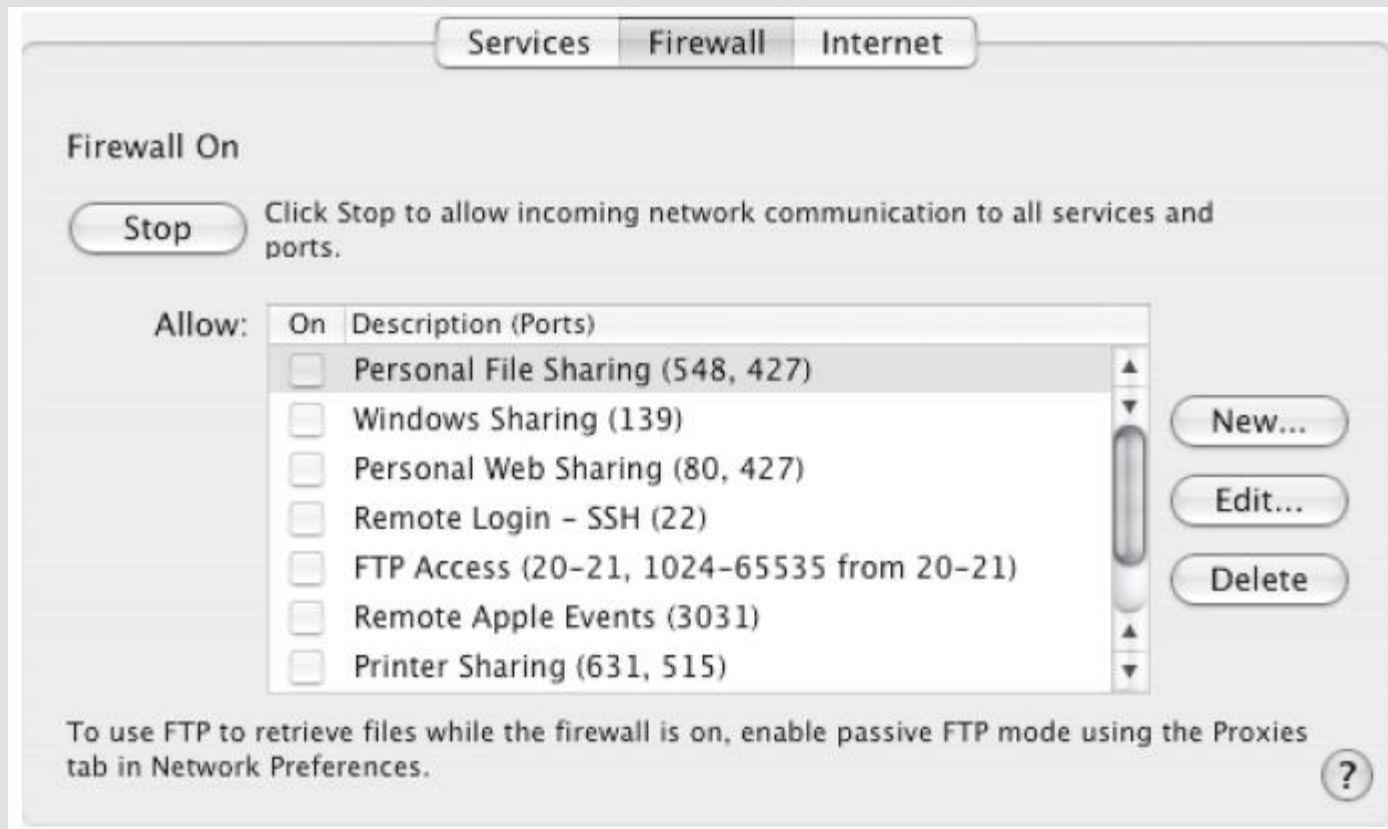
Host-Based Firewalls

- **s/w module used to secure individual host**
 - available in many O.S
 - or can be installed as an add-on package
- **often used on servers**
- **advantages:**
 - can tailor filtering rules to host environment
 - protection is provided independent of topology
 - provides an additional layer of protection

Personal Firewalls

- **controls traffic between**
 - PC and Internet or PC and enterprise network
- **a software module on personal computer**
- **or in home/office DSL/cable/ISP router**
- **typically much less complex than other firewall types**
- **primary role is to deny unauthorized remote access to the computer**
- **and monitor outgoing activity for malware**

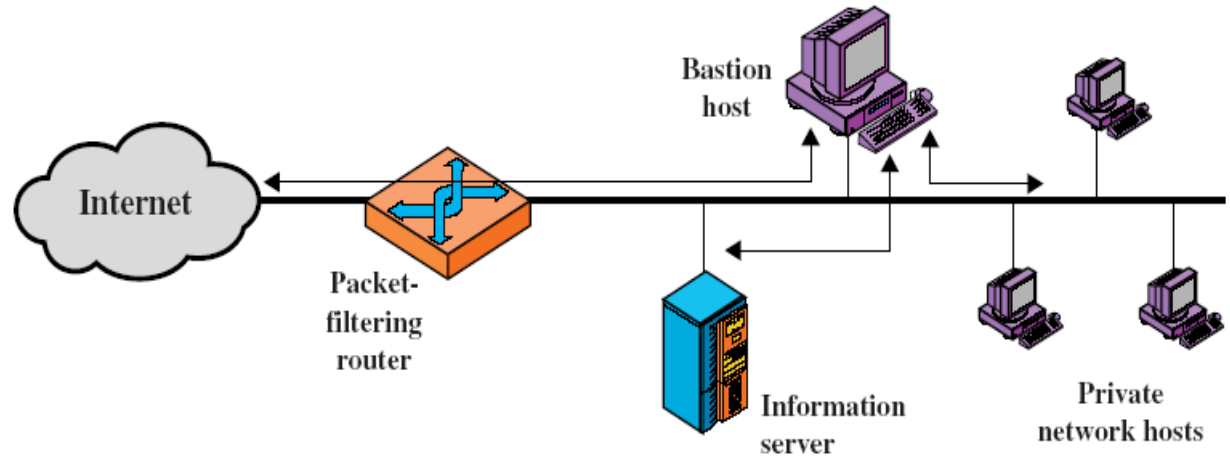
Personal Firewalls



Firewall Configurations

- In addition to the use of simple configuration of a single system (single packet filtering router or single gateway), **more complex configurations are possible**
- Three common configurations
 - **Screened host firewall system**
(single-homed bastion host)
 - **Screened host firewall system**
(dual-homed bastion host)
 - **Screened-subnet firewall system**
(Demilitarized Zone-DMZ)

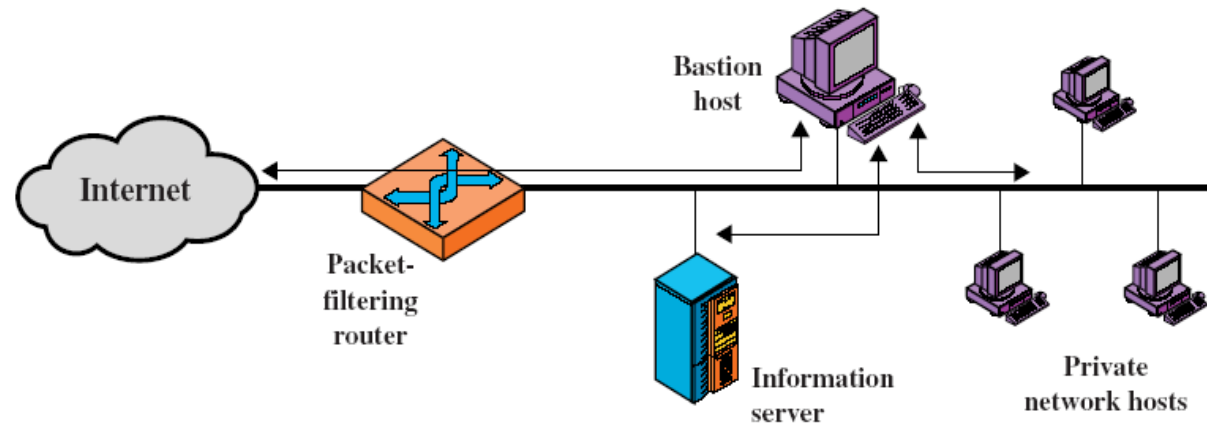
Screened host firewall system (Single-homed bastion host)(1)



(a) Screened host firewall system (single-homed bastion host)

- **Firewall consists of two systems:**
 - a packet-filtering router
 - a bastion host
- **Configuration for the router:**
 - traffic from Internet: only IP packets destined for the bastion host are allowed in
 - traffic from internal network: only IP packet from the bastion host are allowed out
- The bastion host performs authentication and proxy functions

Screened host firewall system (Single-homed bastion host)(2)

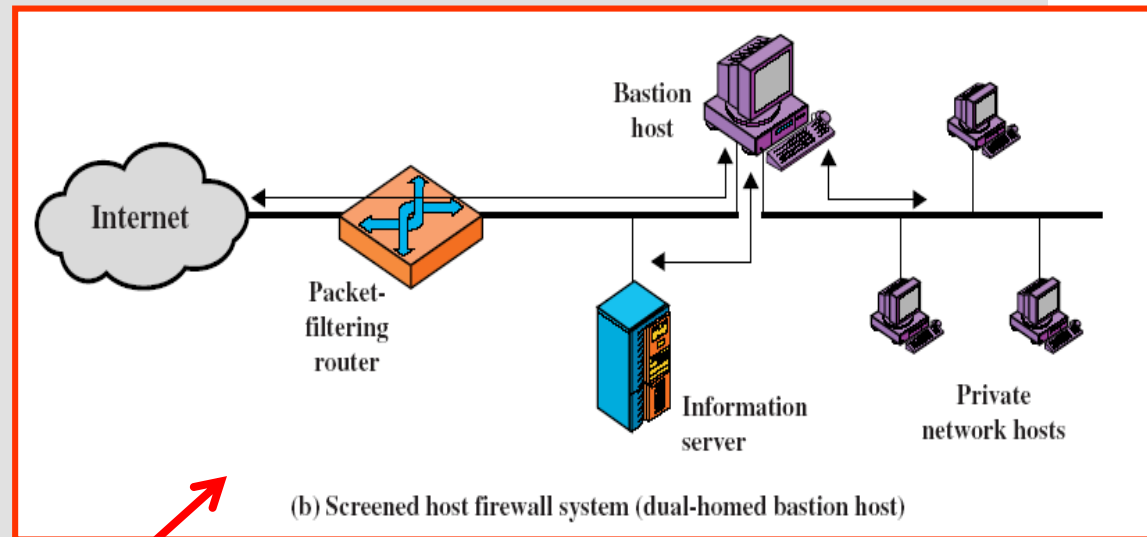


(a) Screened host firewall system (single-homed bastion host)

- **Greater security than single configurations**
 - implements both packet-level and application-level filtering
 - > allows for flexibility in defining security policy
 - intruder must generally penetrate two separate systems
- **Configuration can be made flexible**
 - may include a public information server (e.g., web server) accessible directly from the Internet through router

Screened host firewall system (dual-homed)

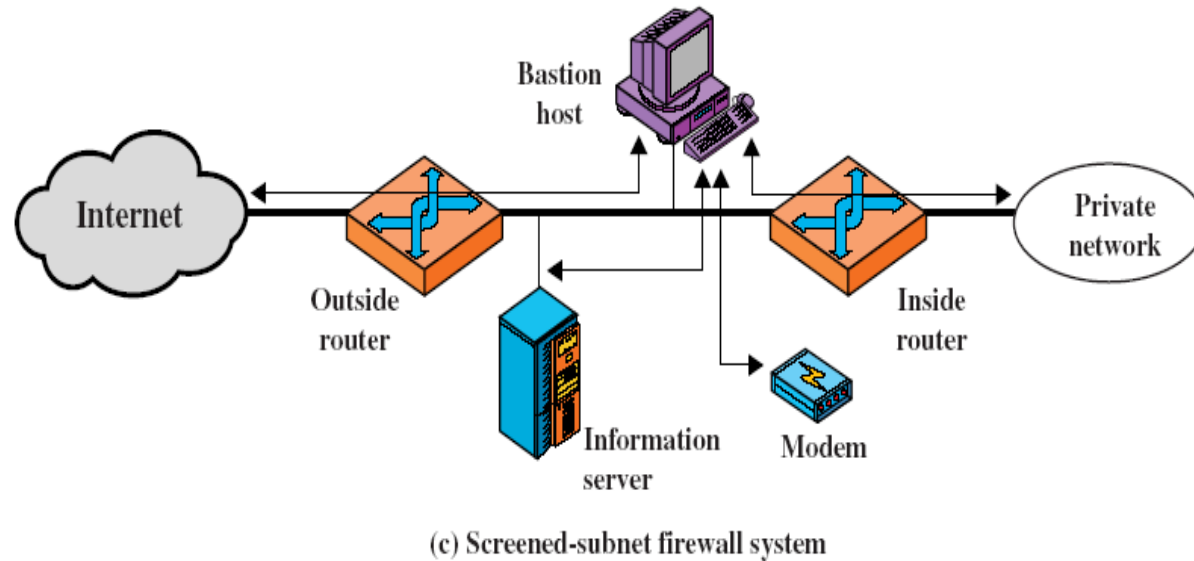
- In **single-homed firewall**, internal network may become vulnerable if security of the router is compromised
 - traffic may flow directly between the Internet and other hosts bypassing bastion host



- **Dual-homed bastion configuration physically prevents such security breaches**
 - forces all traffic to go through the bastion host
- **Configuration can be made flexible**
 - may allow direct communication between information server and the Internet through router

Screened subnet firewall (1)

- **Most secure configuration of the three**
- **Two packet-filtering routers are used**
 - between the **bastion host** and the **Internet**
 - between the **bastion host** and **private network**

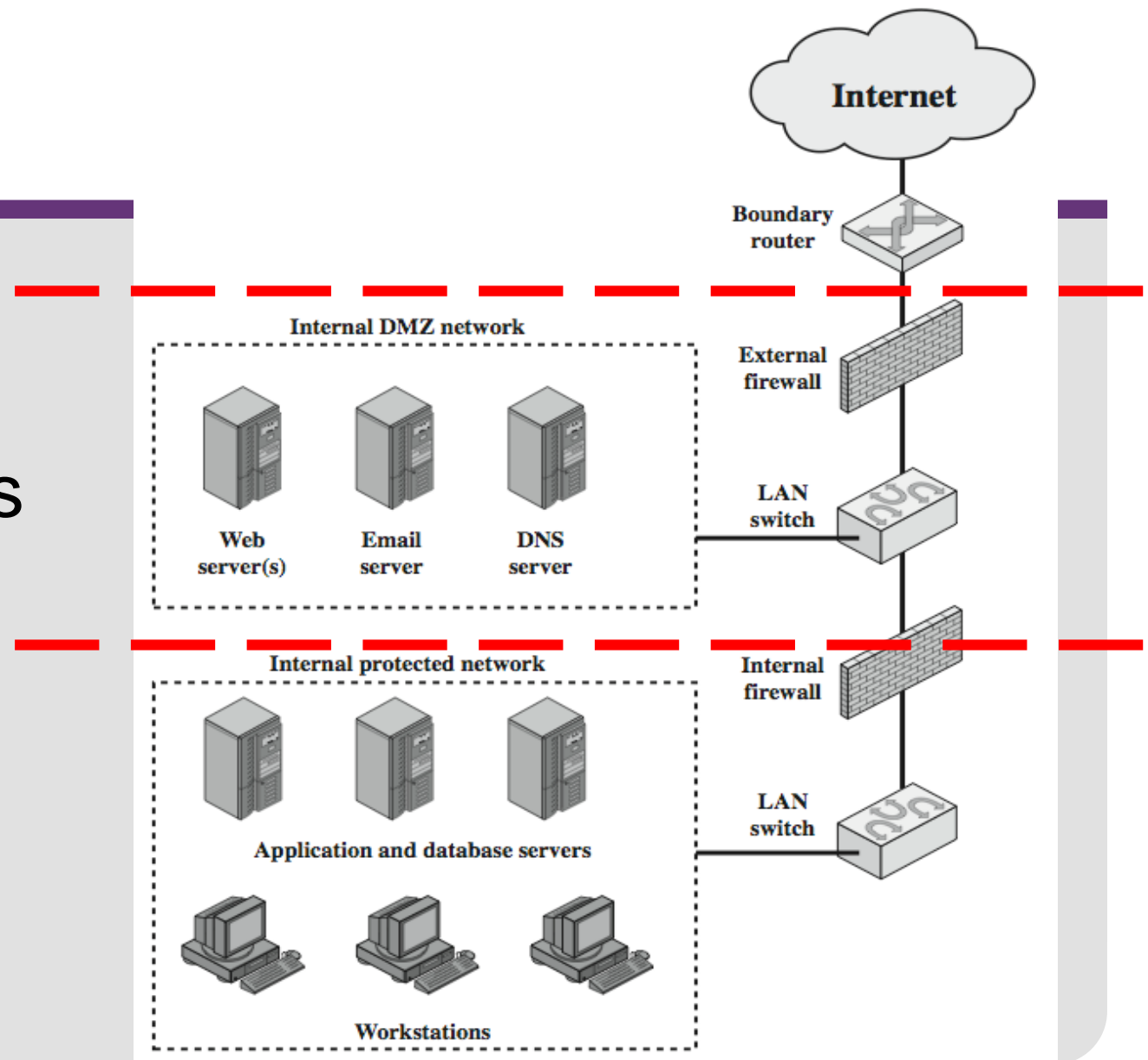


- **Creation of an isolated sub-network**
 - consisting of bastion host, information server and modems
 - also known as demilitarized zone (DMZ)
- **Both Internet and internal network have access to DMZ but traffic across DMZ is blocked**

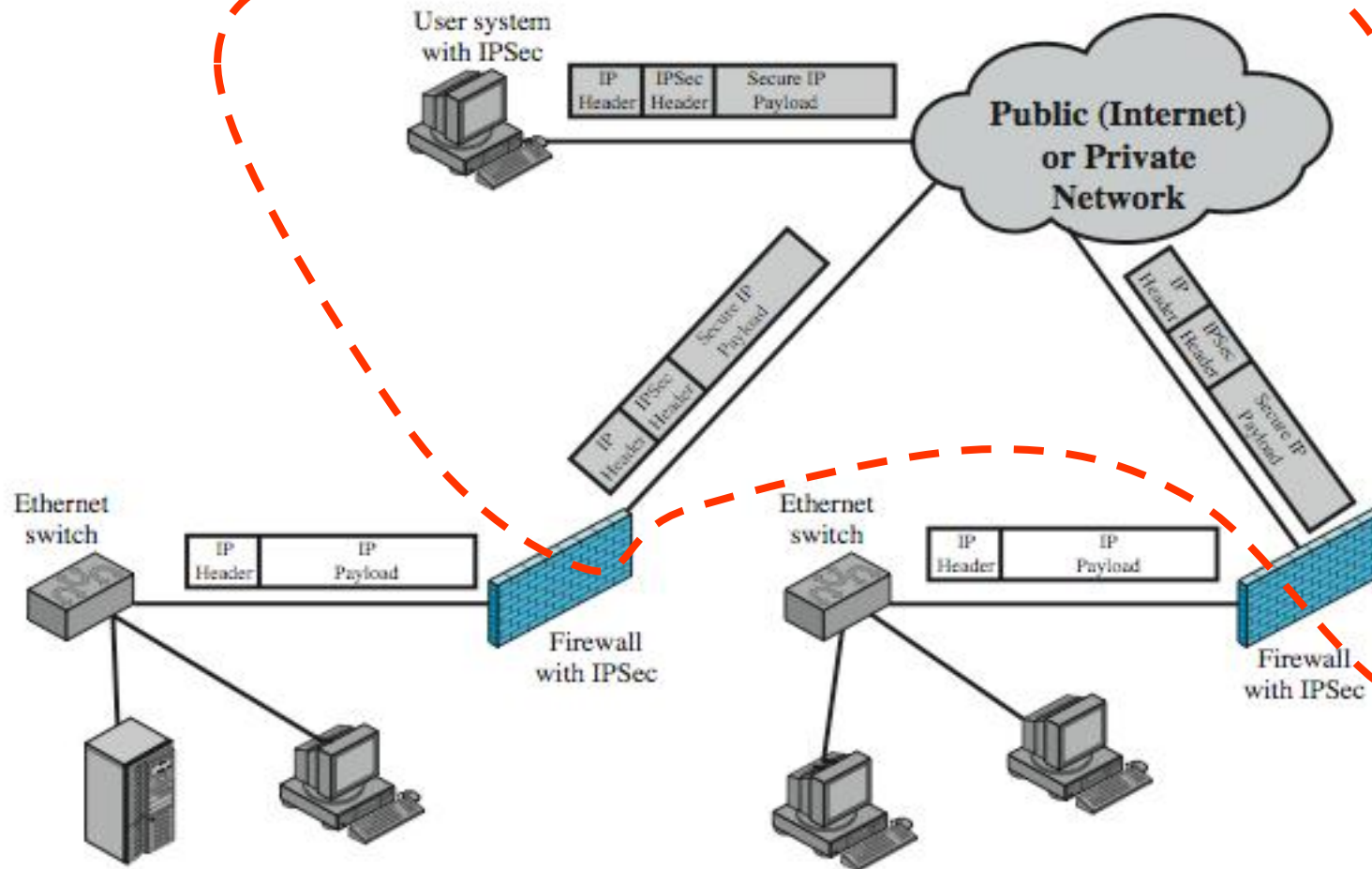
Screened subnet firewall (2)

- **Advantages:**
 - **Three levels of defense**
 - The outside router advertises only the existence of the screened subnet to the Internet
 - > internal network is **invisible** to the Internet
 - The inside router advertises only the existence of the screened subnet to the internal network
 - > the systems on the inside network **cannot construct direct routes to the Internet**

DMZ Networks



Virtual Private Networks



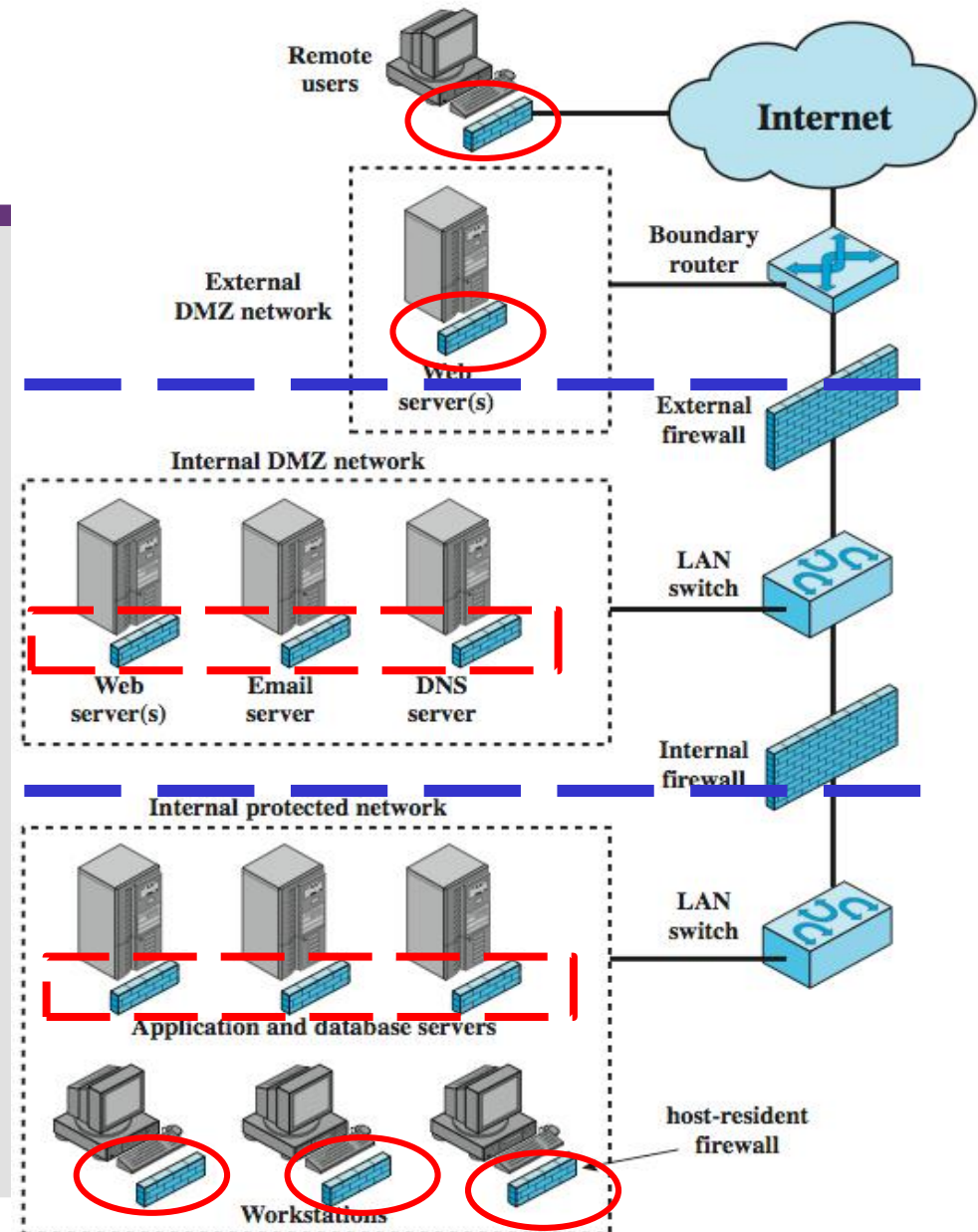
Distributed Firewalls

Distributed firewall configuration requires:

- **Host-based firewalls**

+

- **Stand-alone firewalls working together**
Under a central administrative control
Important aspect of a distributed firewall configuration is **security monitoring**



Summary of Firewall Locations and Topologies

- **Host-resident firewall** - PC firewall software for standalone_PC
- **Screening router** - single router between INT-EXT networks with stateless or full packet filtering → small office
- **Single bastion inline** - single FW between INT-EXT networks with stateful filtering and/or application proxies → mid-range
- **Single bastion T** - Similar to single bastion inline; but has a **third network interface** on bastion to a DMZ for externally servers → medium/large
- **Double bastion inline** - DMZ is sandwiched between two bastion firewalls → large-Govt Orgs
- **Double bastion T** - Similar to double bastion inline; but has a **third network interface** for both FW for DMZ to be sandwiched between two bastion firewalls → Australian Govt uses this configuration
- **Distributed firewall configuration** - Host-based firewalls + Stand-alone firewalls (Double bastion T) working together → large-Govt/Businesses Orgs

Summary

- **We have considered:**
 - firewalls
 - types of firewalls
 - > packet-filter, stateful inspection, application proxy, circuit-level
 - basing
 - > bastion, host, personal
 - location and configurations
 - > DMZ, VPN, distributed, topologies

[illegible]

FIT3031 Exam Discussion



FIT3031 Final Exam Format – Summer-B 2017

- Total exam mark is 100 and it contributes 60% of the assessment. Even though you have good marks in the assignments, you should get at least **40 marks** in the exam to **pass** this unit.
- The exam duration is of **3** hours. Check exam date at my Monash portal.
- apart from textbook and SG, please go meticulously through lecture notes.
- All tutorial solutions have been released. Go through all tutorial questions.
- The exam format will be the same as the sample exam paper already posted. A sample solution of exam paper will be released. Going through this paper will give you a good idea about the exam.
- Exam questions will more or less cover all the study sessions. If you want to get good marks you must go through all of them.

FIT3031 Final Exam Format – Summer-B 2017

The FIT3031 exam consists of 2 parts.

- **Part 1**
 - consists of SEVEN questions; please answer ALL questions in the exam question paper
 - Write all answers within the box below the question.
- **Part 2**
 - consists of T/F, MCQs and Short Answers.
- **Total marks - 100.**
 - Part 1 + Part 2
 - This exam contributes 60% to your result for this unit.

FIT3031 Final Exam Format – Summer-B 2017

- There are two parts (A & B) to the Exam. Total of 100 Marks
- The FIT3031 exam consists of 2 parts.
- **Part A** consists of SEVEN questions; (Lecture-1 to Lecture-11) i.e. up to Firewall.
- Please write the answer in the space provided below the question in the box
- Total marks - **100**. This exam contributes **60%** to your result for this unit.
- For **Part B**, please select only one choice that is correct for the following:
 - (Lecture-1 to Lecture-11) i.e. up to Firewall.
 - Review all the online weekly quizzes
 - 10 each T/F questions, MCQ's, & Short Answer Questions.

Sample Exam & SWOT-VAC week Consultations

FIT3031

**Practice Sample Exam
released at the start of the SWOT-VAC
week**

Solution at the end of SWOT-VAC week
SWOT-VAC week Consultations
TBA in Moodle!