Firewall

Dr. Asem Kitana

What is a Firewall?

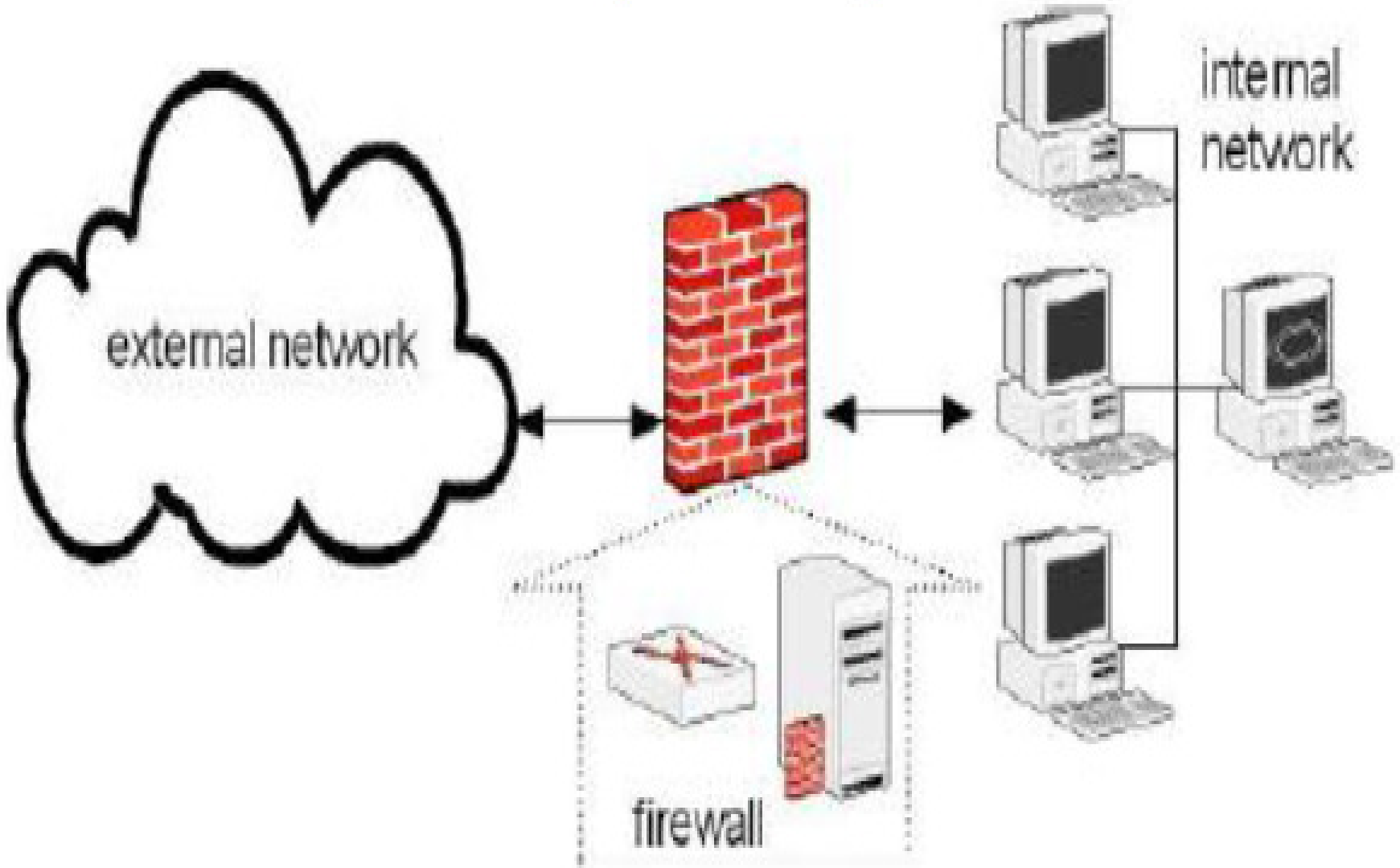
- A firewall is a system that enforces access policy between two (or more) networks.
- A firewall makes the decision on what to do with connection packets based on rules/policies.
- The actions a firewall can take are:
  - Forward/accept the packet (Allows authorized traffic).
  - Drop the packet silently (Blocks prohibited traffic).
  - Drop the packet and send back ICMP messages to the source to notify why it was dropped (Blocks prohibited traffic with notification). but is this action wise?

Firewall Mechanism

- Two main approaches to setup a firewall:
  - Block all that is not explicitly authorized.
  - Allow all that is not specifically blocked.

- Firewall Mechanism:
  - Firewall examines all traffic packets between the networks.
  - Packets are evaluated against a list of “rules/policies” and conditions.
  - When the packet matches a rule: the action is triggered (reject or allow). The rest of the rules are not evaluated.
  - Rules are checked from top to bottom and the first rule found is applied. If no rules match, the packet is blocked by default.

Firewall Architecture



Firewall Architecture

- The previous example shows a firewall architecture made of two blocks. The external network (left side) and the internal network composed of four computers (right side) are two entities separated physically by a firewall, whose goal is filter the inbound traffic and outbound traffic.

- Inbound traffic: the traffic that comes from the external network and destined to the internal network.

- Outbound traffic: the traffic that goes from the internal network towards the external network.

Default Firewall Policies

- Default to block all
  - If we don't explicitly enable it, then it is blocked
  - May block unintended items
  - Most secure implementation
  - Often implemented by a refinement process…
- Default to allow all
  - If we aren't explicitly blocking it, then it is allowed
  - May miss things you want to block
  - Least secure implementation
  - Hard to refine, hard to audit. Can you really trust it???

Types of Firewalls

- Stateless Packet Filtering – Network Layer
- Stateful Packet Filtering – Network Layer
- Circuit Proxy – Transport Layer
- Application Proxy – Application Layer

Stateless Packet Filtering Firewalls

- Stateless packet filtering firewall acts at layer 3 (Network Layer)
- Control the forwarding or dropping of the data based on the IP header information, not the payloads.
- The information and fields that may be taken into consideration are:
  - IP destination address, IP source address, Protocol type (e.g. TCP, UDP, ICMP), Source protocol port number (e.g. TCP/80, UDP/53), Destination protocol port number, Flags (e.g. SYN, ACK, FIN)
- It does not keep track of the connection or session state.

Stateless Packet Filtering Example

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

Stateful Packet Filtering

- Stateful packet filtering firewall acts at layer 3 (Network Layer)
- Perform all the functions of a stateless packet filtering firewall but also keep track of the state of the connection and past packets in the communication.
- Stateful packet filtering firewall allows inspecting both complex combinations of payload (message content) and context established by prior packets to influence filtering decisions.

Stateful Packet Filtering

- The firewall will attempt to track all the information in the communication. For instance:
  - If it evaluate a TCP packet from B to A that has a SYN-ACK flag, it will verify that it has seen a corresponding SYN packet from A to B before (is the TCP connection behaving correctly?).
- In other words: the stateful packet filter will keep track of all conversations and ensure that all packets transiting comply with proper protocol rules and operations.

Stateful Packet Filtering Example

-The connection tracking states used in building rules include the following:

State	Meaning
NEW	This packet belongs to a session that is not an already known connection. Thus, it is considered to be a NEW connection.
ESTABLISHED	Packets belong to a session that has seen traffic flowing in both directions.
RELATED	This connection is related to another connection (in NEW or ESTABLISHED state).
INVALID	A state that denotes an error.

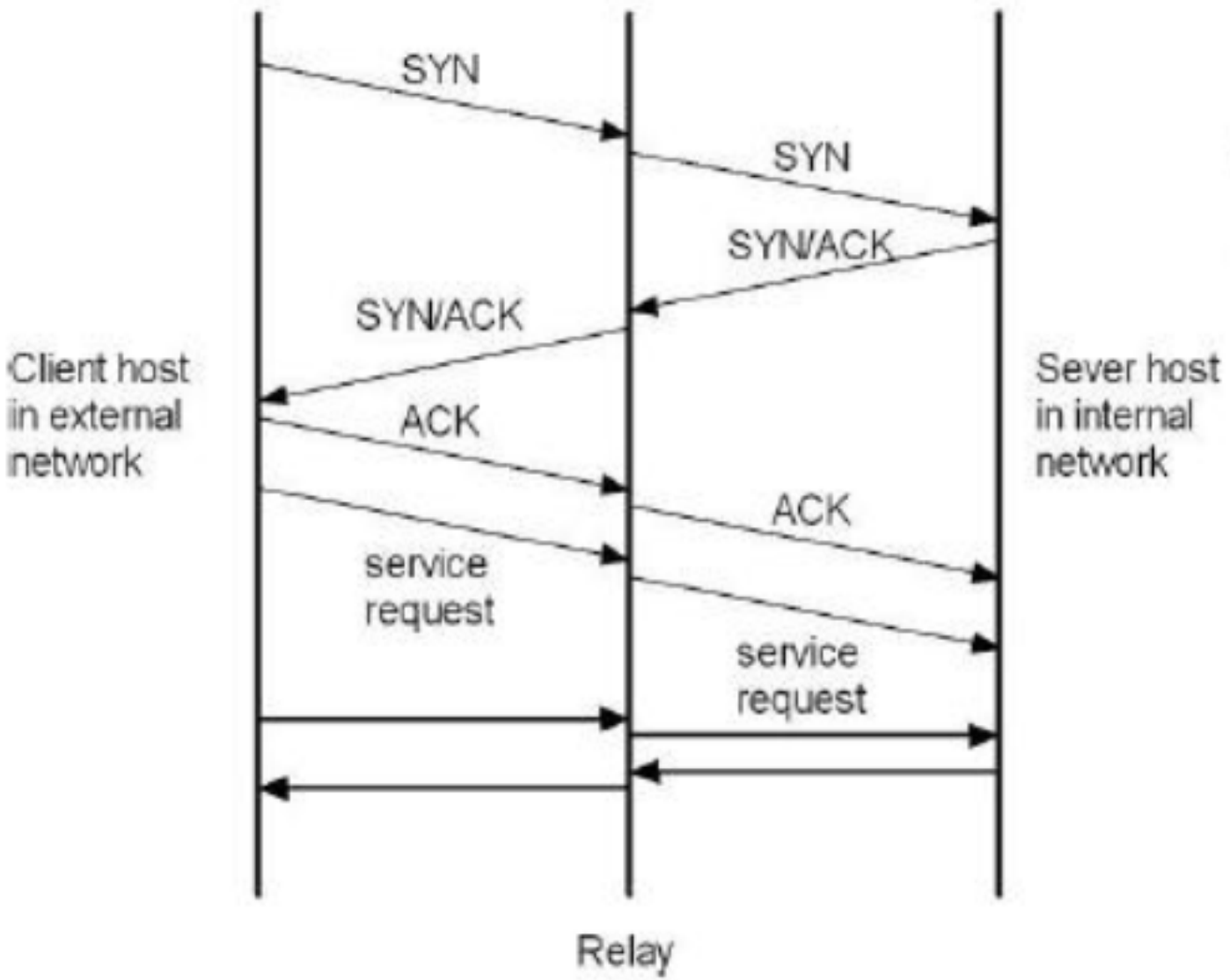
Connection state table example

client addr	client port	server addr	server port	connection state	protocol
219.22.101.32	1030	129.63.24.84	25	established	TCP
219.22.101.54	1034	129.63.24.84	161	established	UDP
210.99.201.14	2001	129.63.24.87	80	established	TCP
24.102.129.21	3389	129.63.24.87	110	established	TCP

Circuit Proxy

- Circuit proxy firewall acts at layer 4 (Transport Layer).
- Their purpose is to examine information of IP addresses and port numbers in TCP/UDP headers to determine if a connection is allowed.
- They act as intermediate that relay a TCP connection between an internal and external host.
- They disallow the direct connection between the external and the internal networks.

Circuit Proxy



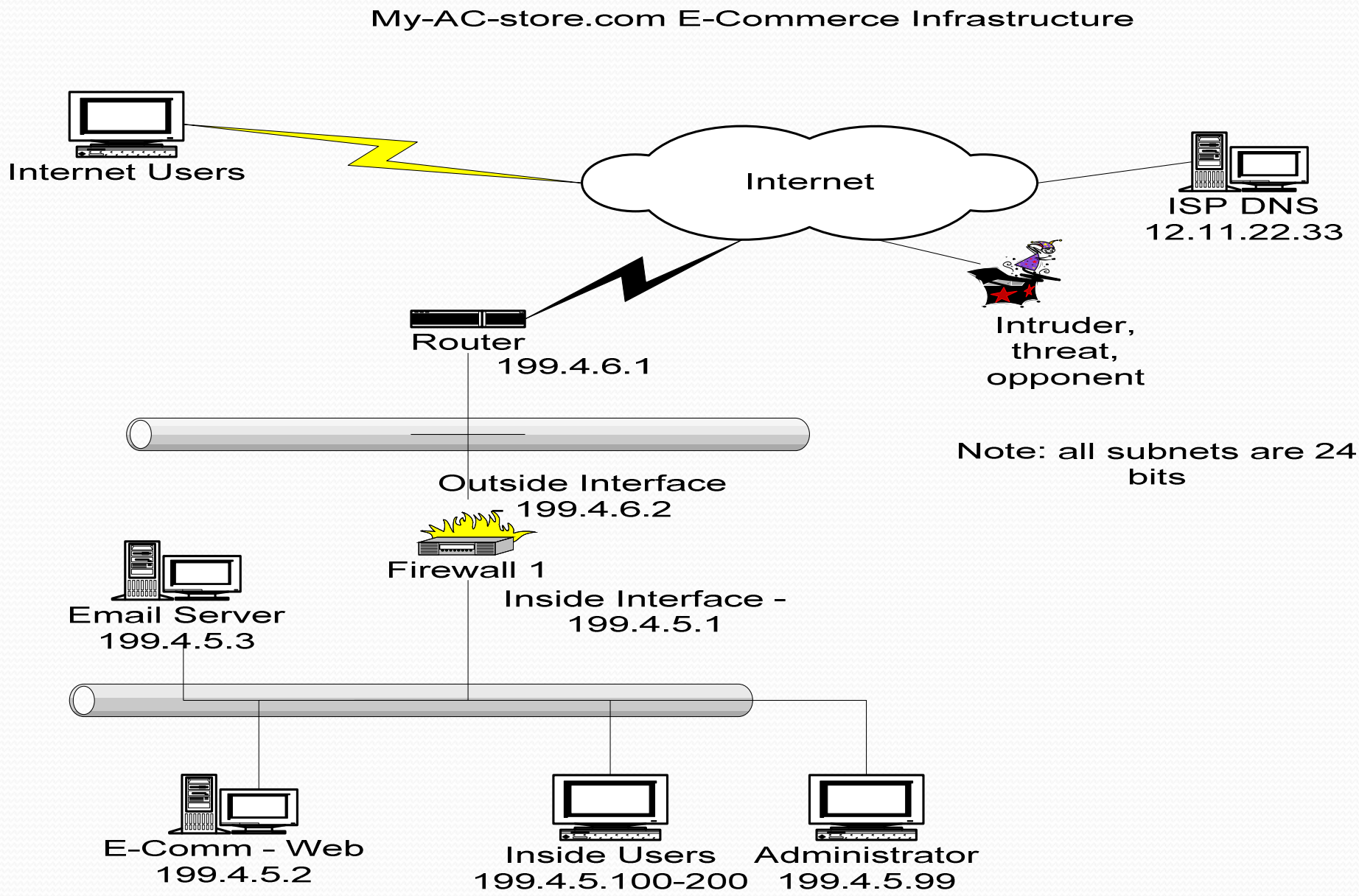
Application Proxy

- Application proxy firewall acts as an intermediate communication point between 2 parties:
  - Each party “think” they directly communicate to the other.
  - Actually they communicate to the Application Proxy Firewall.
  - A – Proxy – B: A communicates to the proxy, the proxy then “acts” as A when communicating to B and vice-versa.
- These application proxy firewalls act at layer 7 (Application Layer).

Application Proxy

- Basic functionalities of application proxy include:
- Accepting the client sessions and appearing to them as a server.
- Receiving from the client software the name of the actual server.
- Contacting the actual server and appearing to it as a client.
- Relaying all the data from the client to a server.
- Performing access control and enforcement functions by checking, and accepting or rejecting the incoming and outgoing connections.

Firewall Policy



Firewall Policy

Set Name	Rule #	Protocol	A/R	Source IP	Src Port	Dest IP	Dest Port	Flag	Comments
set1	1	tcp	R	any	any	any	any	SYN+FIN	
set1	2	tcp	A	any	any	199.4.5.2	80/443		
set1	3	tcp	A	any	any	199.4.5.3	smtp + pop3		
set1	4	tcp	A	any	80/443	199.4.5.99	any	ack	
set1	5	udp	A	any	53	199.4.5.0	any		
set1	6	IP	R	any	any	any	any	any	
set2	1	tcp	A	199.4.5.99	any	any	80/443		
set2	2	udp	A	199.4.5.0	any	any	53		
set2	3	tcp	A	199.4.5.99	any	199.4.5.1	23		
set2	4	tcp	A	199.4.5.2	80/443	any	any	ack	
set2	5	tcp	A	199.4.5.3	smtp + pop3	any	any	ack	
set2	6	IP	R	any	any	any	any	any	

Set1 applied to outside interface of firewall
Set2 applied to inside interface of firewall

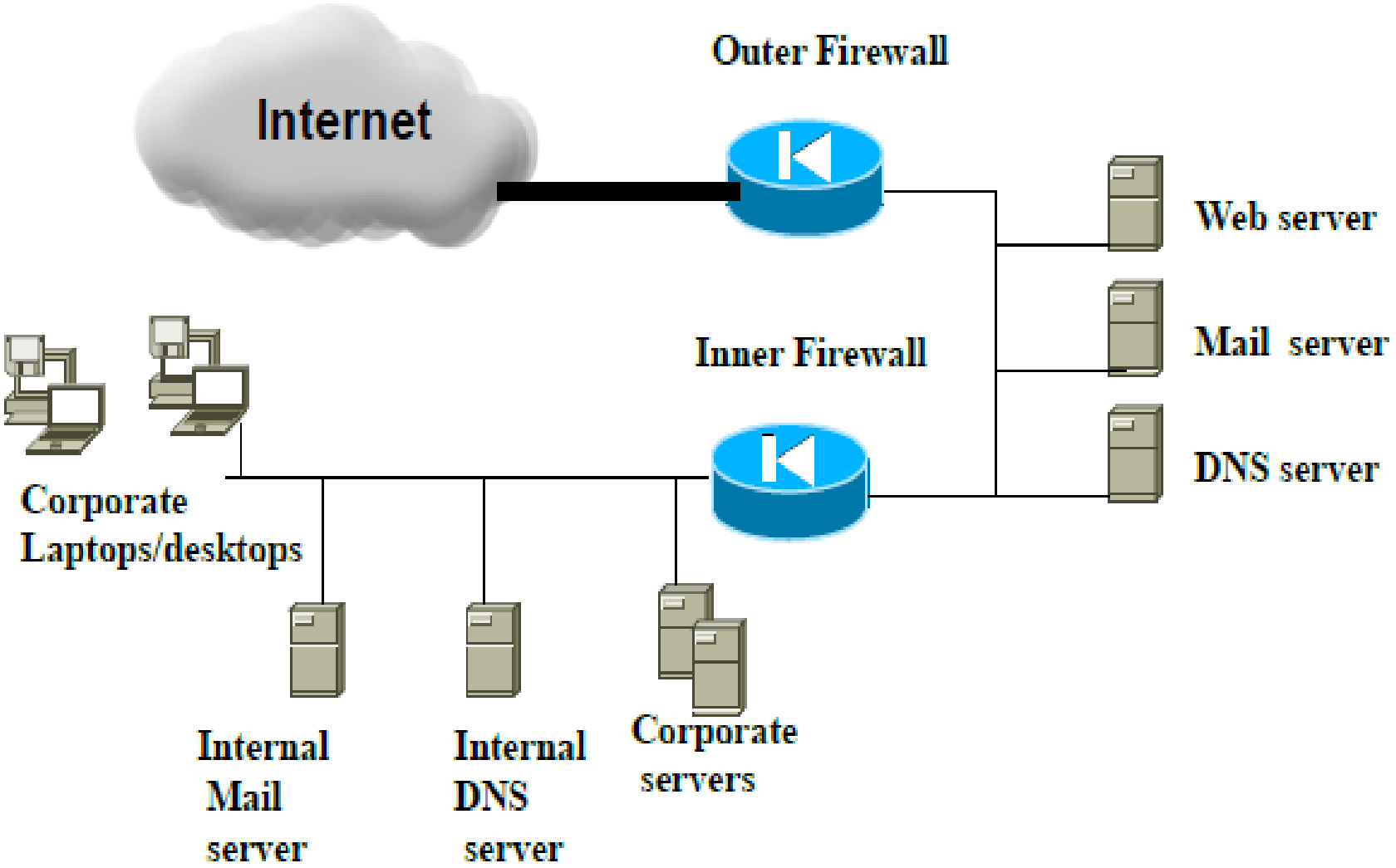
Demilitarized Zones (DMZ)

DMZ is a subnet between two firewalls in an internal network

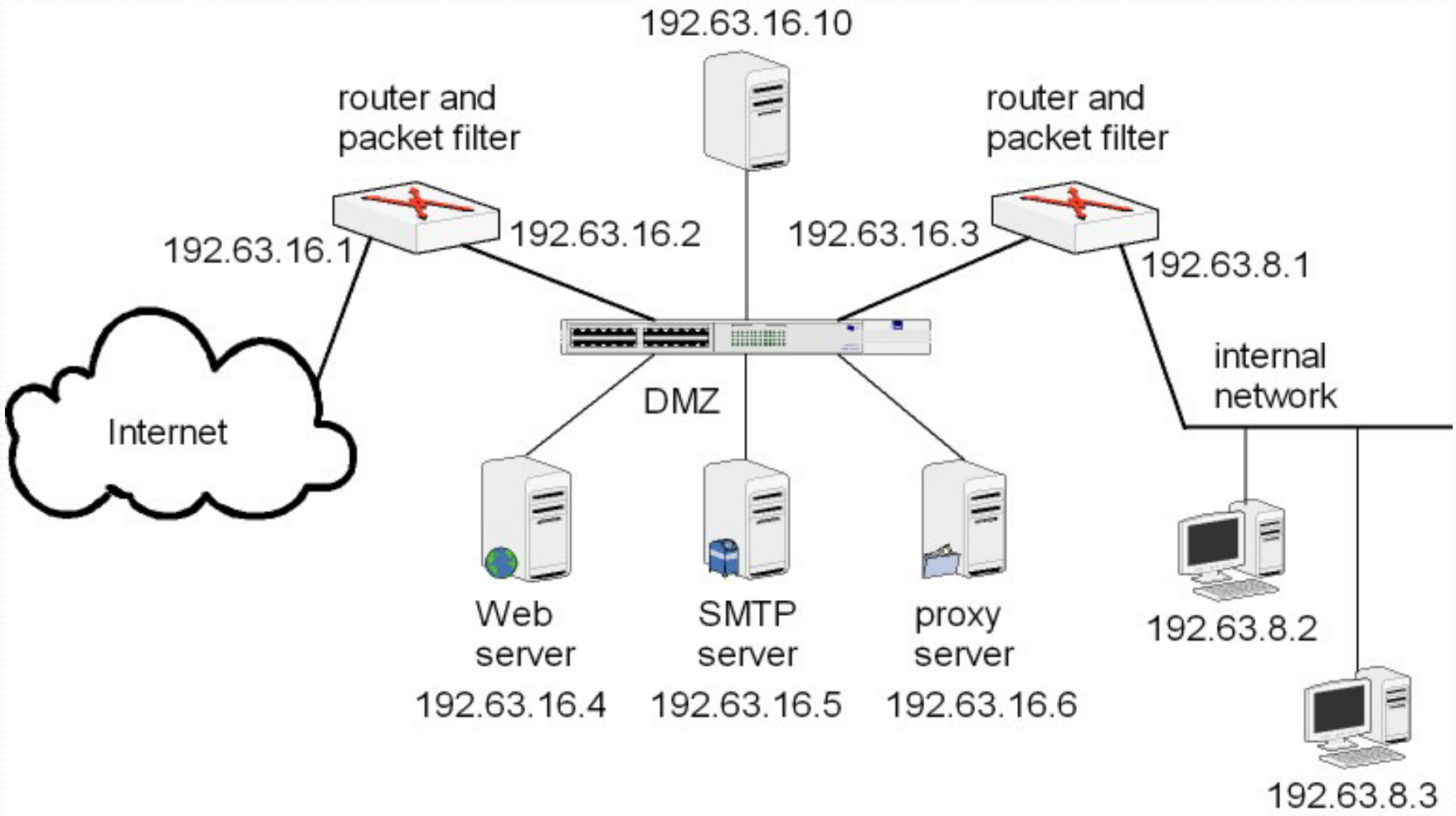
- External firewall protects DMZ from external threats
- Internal firewall protects internal network from DMZ

- The role of the DMZ is to provide strong separation between the external and internal networks.

DMZ Example1



DMZ Example2



Benefits of Firewall

- Control access based on sender or receiver addresses.
- Control access based on the service requested.
- Hiding the internal network (e.g., topology, addresses, traffic, etc.)
- Authentication based on the source of traffic.
- Choke point for security audit (Logging activities).
- Reduce attacks by hackers.