CO325 – Lab 01: Follow-up Questions

1) Section: Check Default Functionality of the Firewall

a) What is the default behavior (in terms of Packet Filtering strategy) of Cisco ASA 5510 firewall?

The inside and the outside networks can only ping, make SSH and HTTP connections for only themselves. We can not ping from inside network to outside network.
And we can't communicate from outside to inside by using ping, SSH and HTTP.

	In-out	Out-in
ping	unsuccessful	unsuccessful
SSH	successful	unsuccessful
HTTP	successful	unsuccessful

b) Identify the advantages and disadvantages of this default functionality.

Advantages

- Even if there is no any ACE the inside network is secure from unauthorized access.
- It is easier to configure default functionality.

Disadvantages

- Packet filters do not handle the FTP protocol well because data transfer occur over high-numbered TCP ports.
- Packet filters does not offer any value-added features, such as HTTP object caching, URL filtering, and authentication because they do not understand the protocols being used.
- Difficulty of setting up packet filtering rules in a firewalls.

2) Section: Modify Packet Filtering Rules on ASA – Configure Access Control Entries (ACEs)

a. **Scenario# 1: Permit Any**

i) What are the specific purposes of "access-list" and "access-group" commands?

access-list

An access list is a sequential list that consists of at least one **permit** statement and possibly one or more **deny** statements. In the case of IP access lists, these statements can apply to IP addresses, upper-layer IP protocols, or other fields in IP packets.

access-group

After configuring an access list, for the access list to take effect, must either apply the access list to an interface. By using access-group command this can be done and a vty (by using the **access-class** command), or reference the access list by any command that accepts an access list.

ii) What has been excluded from the filtering (i.e., permitted) by the ACEs in this scenario? Be precise!

It permits any ip in the outside to communicate with inside network and permit any ip in the inside to communicate with outside network.

	In-out	**Out-in**
ping	successful	successful
SSH	successful	successful
HTTP	successful	successful

iii) Identify the pros and cons of this approach in permitting traffic from outside to reach the internal network.

Anyone in the outside can access any service in the inside network and then there is no any protection to inside network. It will cause to confidentiality and integrity of inside network. There is a lot of traffic through the network. Denial of services may happen due to this reason.

b. **Scenario# 2a: Permit Outside Host to Inside Any**

i) What has been permitted by the ACE in this scenario? Be precise!

It permits outside ip 172.16.100.10 to communicate (ping, SSH, HTTP any service) with any inside network. And any inside ip can communicate with inside ip 172.16.100.10 using ping, SSH and HTTP.

	In-out	**Out-in**
ping	successful	successful
SSH	successful	successful
HTTP	successful	successful

ii) Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.

In this case it only allows a particular host in the inside network. When a person has a static ip this will be useful. Then he can do anything he like in the network, because he has permission to use any service.

c. **Scenario# 2b: Permit Outside Any to Inside Host**

i) What has been permitted by the ACE in this scenario? Be precise!

This will permit any ip in the outside network to access inside host with ip 192.168.100.10. That means any outside can communicate by ping, SSH and HTTP.

Also the inside host can communicate the outside network through ping, SSH and HTTP.

	In-out	**Out-in**
ping	successful	successful
SSH	successful	successful
HTTP	successful	successful

ii) Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.

In this case it allows outside any type of traffic to only a particular inside host. This can be used on a webserver communication. And this case outside can do anything because there is no any restriction. This ACE not good for communication.

d. **Scenario# 3a: Permit Outside Any to Inside Any – TCP**

i) What has been permitted by the ACE in this scenario? Be precise!

This will allow to access outside any host to inside any host only through TCP. That means they can only connect through SSH and HTTP. Nobody can ping from outside to inside and form inside to outside.

	In-out	**Out-in**
ping	unsuccessful	unsuccessful
SSH	successful	successful
HTTP	successful	successful

ii) How does this compare with Scenario# 1? What effect does this have in terms of the "cons" you identified in question 2.a.iii. above.

In the scenario# 1 it permits any outside to access inside any through any service but in this scenario it permits to access outside any to inside any only through TCP. Outside network cannot ping to inside because it use ICMP. In this case confidentiality of data in inside network will be secured.

e. **Scenario# 3b: Permit Outside Any to Inside Any – ICMP**
i) What has been permitted by the ACE in this scenario? Be precise!

This will allow to access outside any host to inside any host only through ICMP. That means they can only connect through ping.
Also inside network can communicate with outside through ping, SSH and HTTP.

	In-out	**Out-in**
ping	successful	successful
SSH	successful	unsuccessful
HTTP	successful	unsuccessful

ii) Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.

In this scenario only allow ping because it uses ICMP. When setting up networks it will be useful because we can check local internal and external connectivity. But we cannot check HTTP and SSH connectivity.

f. **Scenario# 4a: Permit Outside host to Inside Subnet – TCP/SSH**
i) What has been permitted by the ACE in this scenario? Be precise!

This will allow to access outside host 172.16.100.10 to inside subnet 192.168.100.0 /24 only through TCP connection which is equal to SSH. And pinging and connecting through HTTP cannot be done from outside to inside.

Also from the inside subnet can communicate to outside network through SSH and HTTP but pinging cannot be done.

	In-out	**Out-in**
ping	unsuccessful	unsuccessful
SSH	successful	successful
HTTP	successful	unsuccessful

ii) Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.

In this situation it allows only one outside host which has a particular static ip to access inside. So this is a drawback. This only allows the SSH connectivity from outside to inside. This will be useful when an administrator wants an SSH connection to any hosts in a particular subnet in this example 192.168.100.0/24 subnet.

g. **Scenario# 4b: Permit Outside Any to Inside Host – TCP/HTTP**
i) What has been permitted by the ACE in this scenario? Be precise!

This will allow to access outside any to inside host 192.168.100.10 only through TCP connection which is equal to HTTP. And pinging and connecting through HTTP cannot be done from outside to inside.

Also from the inside network can communicate to outside network through SSH and HTTP but pinging cannot be done.

	In-out	**Out-in**
ping	unsuccessful	unsuccessful
SSH	successful	unsuccessful
HTTP	successful	successful

ii) Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.

This will useful in a web server connection. In a webserver outside network can be accessed inside. In general servers have static ip addresses like in this case.

h. **Scenario# 5a: Deny Outside Any to Inside Host – TCP/HTTP + Permit Any**
i) What has been permitted by the ACE in this scenario? Be precise!

All the services ping, SSH and HTTP can be happened from outside to inside. Also inside network can access outside through ping, SSH and HTTP.

	In-out	**Out-in**
ping	successful	successful
SSH	successful	successful
HTTP	successful	successful

ii) Compare this approach of traffic filtering with the approach used in scenarios 2 – 4.
From 2 - 4 scenarios the ACEs allow the outside network to access the inside network through specific services like ping, SSH, HTTP. But in this scenario the ACE deny specific service (HTTP) but before that permit ip any any rule is applied. So it allow any services to use as in scenario#1.

iii) Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.

As per the test results shown in the above table this policy does not restrict anything. It not really needed to have this policy if it allows traffic as shown in the table above. Ip any any rule is better to use if this thing want to happen.

i. **Scenario# 5b: Permit Any + Deny Outside Any to Inside Host – TCP/SSH**
i) What has been permitted by the ACE in this scenario? Be precise!

This will deny outside any host accessing inside host 192.168.100.10 through TCP connection which is equal to SSH. And all other services are allowed from outside to inside.
Also inside network can access outside through ping, SSH and HTTP.

	In-out	**Out-in**
ping	successful	successful
SSH	successful	unsuccessful
HTTP	successful	successful

ii) Compare this with the scenario above (5a).

In scenario# 5a it allows all the connection ping, SSH and HTTP. But in this scenario the rule denies SSH and other ones (ping, HTTP) are allowed from outside to inside.