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?

Configures an interface for management so you can connect to it using ASDM, with which you can then complete your configuration.
By default, the Management 0/0 interface is configured for management-only traffic (the **management-only** command). For supported models in routed mode, you can remove the limitation and pass through traffic. The Management interfaces might not be optimized for through-traffic, however. The Management 0/0 interface is configured for ASDM access as part of the default factory configuration.

	In -> Out	Out -> In
Ping	X	X
SSH	√	X
HTTP	√	X

With the default permit strategy, you give the firewall the set of conditions that will result in data being blocked. Any host or protocol that is not covered by your policy will be passed by default.
By default we can can't ping either from inside network to outside network or outside network to inside network. We can use ssh or http connection to connect from inside to outside network while it doesn't work with outside to inside network.

b) Identify the advantages and disadvantages of this default functionality

Advantages

The primary advantage of default functionality is that it is easier to configure: you simply block out the protocols that are "too dangerous," and rely on your awareness to block new dangerous protocols as they are developed (or discovered).

Disadvantages

Default permit is not a panacea. With this policy, you can create a firewall that is either secure or unsecure, by permitting (or failing to deny) "dangerous" protocols.

Filter rule sets can be very complex. Due to the complexity, you might not know if they are correct or not.

There is no easy way to test filters except through direct experimentation, which may prove problematical in many situations.

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

a. Scenario# 1: Permit Any

	In -> Out	Out -> In
Ping	√	√
SSH	√	√
HTTP	√	√

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

An **access** control **list** (ACL) consists of one or more **access** control entries (ACEs) that collectively define the network traffic profile. This profile can then be referenced to software features such as traffic filtering, priority or custom queueing, and dynamic **access** control.

To apply an access list to a physical interface, the "access-group" command is used.To apply an IPv4 access control list (ACL) to a Layer 3 interface as a router ACL, use the **ip access-group** command. To remove an IPv4 ACL from an interface, use the **no** form of this command.

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

Nothing is excluded from the filtering. As mentioned in the table, any ip address (IPV4 or IPV6) from outside network will be allowed to access the inside network.
And also inside network can connect to outside network using ping, ssh or http.

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

Cons: Permitting traffic from outside to reach the internal network will reduce the security of the internal network. And also it will increase the traffic since all the external networks can communicate.
Pros: There is no need to ask for permission from inside network by any of the outside network.

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

	In -> Out	Out -> In
Ping	√	√
SSH	√	√
HTTP	√	√

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

Outside host(172.16.100.10) has been permitted by any of the inside network. So the outside host can communicate with any inside network via pinging, ssh or http.
And also inside network can access the host 172.16.100.10 through ping, ssh and http.

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

Here, this allows only a particular host (172.16.100.10) only. So this can be useful when the person always has the static ip and that person is allowed to do anything (like an administrator) . But no one else is allowed other than that person. So this can be a disadvantage. Moreover the authorized person should always bear the same ip address**.**

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

	In -> Out	Out -> In
Ping	√	√
SSH	√	√
HTTP	√	√

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

Here, any outside host can access to the inside host of 192.168.100.10 via pinging, ssh or http.
Also the inside host 192.168.100.10 also can connect with any of the outside hosts via pinging, ssh or http.

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

Here, this allows connection only to a particular host (192.168.100.10). So this can be useful when the host always has the static ip. And not only HTTP, even SSH service also could be accessed by outside. Basically outside host can do anything to this internal host 192.168.100.10 ,because there is no restriction.so this ACL is also not recommended to use.

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

	In -> Out	Out -> In
Ping	X	X
SSH	√	√
HTTP	√	√

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

Any TCP request (ssh,http) from outside hosts or inside hosts will be allowed to access any inside hosts or outside hosts respectively.
But pinging is not allowed by either side of the networks to the other side of the network

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.

This scenario will help to secure the confidentiality of data since only the tcp requests are allowed to connect to the inside network.

e. Scenario# 3b: Permit Outside Any to Inside Any – ICMP

	In -> Out	Out -> In
Ping	√	√
SSH	√	X
HTTP	√	X

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

Inside hosts can connect to any outside hosts via pinging, ssh or http.
But Outside hosts are allowed only to connect to inside network by pinging, not through ssh or http.

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

Here, this ACL can only be used to to check the connectivity between internal and external host, and nothing else can be done by this ACL. So web services like a webserver or ssh can not be accessed.

f. <u>Scenario# 4a: Permit Outside host to Inside Subnet – TCP/SSH</u>

	In -> Out	Out -> In
Ping	X	X
SSH	√	√
HTTP	√	X

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

Inside subnet is allowed only to connect to outside host only by ssh or http, Pinging is not allowed.
Outside host(172.16.100.10) can connect inside subnet only by ssh, not by pinging or http.

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

It permits only a specific outside host only. SO only the outside host with ip address 172.16.100.10 will be allowed. But this reduce the traffic since only one host is allowed.

g. <u>Scenario# 4b: Permit Outside Any to Inside Host – TCP/HTTP</u>

	In -> Out	Out -> In
Ping	X	X
SSH	√	X
HTTP	√	√

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

Only the http-tcp requests, from the outside hosts are allowed to access the inside host 192.168.100.10. From outside hosts we cannot access inside host 192.168.100.10 by pinging, ssh.

From inside network we cannot ping to the outside network. But from inside to outside ssh and http is connecting.

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

Any host from outside is allowed to access the inside host. But this will increase the traffic since any host from outside is allowed to access the inside host.

h. <u>Scenario# 5a: Deny Outside Any to Inside Host – TCP/HTTP + Permit Any</u>

	In -> Out	Out -> In
Ping	√	√
SSH	√	√
HTTP	√	√

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

Inside network allow access to outside network by ping, ssh and http. And also inside network can access the outside network by ping, ssh and http.

ii. Compare this approach of traffic filtering with the approach used in scenarios 2 – 4.

According to the above table it actually allows any traffic from inside to outside and vice versa, because the policy include permit any. So it's more like Scenario# 2. But when comparing with Scenario# 4 it can be said this policy is weaker than Scenario# 4 because Scenario# 4 restricted some traffic.

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

This policy does not deny connection. So it will be useless to have such a policy if it allows every one to access.

i. <u>Scenario# 5b: Permit Any + Deny Outside Any to Inside Host – TCP/SSH</u>

	In -> Out	Out -> In
Ping	√	√
SSH	√	X
HTTP	√	√

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

Any tcp request other than the ssh request from the outside network to inside 192.168.100.10 host is allowed to access.

Any tcp request through ping, ssh or http from the inside 192.168.100.10 host to outside is allowed to access.

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

Both policies give alike results except one**.** So it will also be useless to have such a policy if it allows every one to access.