CO325 – Lab 01: Follow-up Questions

1. Section: Check Default Functionality of the Firewall

	In -> out	Out -> in
ping	×	×
ssh	√	×
http	√	×

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

In the default behavior we cannot ping from the inside network to outside network. But we can connect using ssh and http from inside network to outside network.

And also outside network cannot connect to inside network using ping, ssh or http.

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

Default functionality is according to the packet filtering.

Advantages

The primary advantage of default permit 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).

This is flexible. For example, if you discover that a person on a particular subnet, say 204.17.191.0, is trying to break into your computer, you can simply block all access to your network from that subnet.

Disadvantages

Filters typically do not have very sophisticated systems for logging the amount of traffic that has crossed the firewall, logging break-in attempts, or giving different kinds of access to different users.

Filter rule sets can be very complex - so complex that 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.

Packet filters do not handle the FTP protocol well because data transfers occur over high-numbered TCP ports; however, this problem can be alleviated by FTP clients that support the FTP passive mode.

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 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.

After you configure an access list, for the access list to take effect, you must either apply the access list to an interface (by using the **ip access-**

group command), 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!

Any ip address (IPV4 or IPV6) from outside network will be allowed to access the inside network. Nothing is excluded from the filtering.

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.

There will be no protection to inside network. So it will affect the confidentiality and integrity of the data in the inside network. And also it will make a high traffic of network and it will cause the denial of services.

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

	In -> out	Out -> int
ping	√	√
ssh	√	√
http	√	√

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

Permits outside host 172.16.100.10 to connect to any of the inside hosts. That means 172.16.100.10 can access the inside network through ping, 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.

This allows only one host (172.16.100.10) from outside network to access the inside network. So this could be useful to a person who has a static ip and only he/she is allowed to access the inside network. The disadvantage is this person should always use the same ip. If that person change the ip address then he/she will not be allowed to access the inside network.

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

	In -> out	Out -> int
ping	√	√
ssh	√	√
http	√	√

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

Permits any outside hosts to access the inside host 192.168.100.10 through ping, ssh and http.

And also inside host can access the outside through ping, ssh and http.

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

In here any outside host have access only to a particular host (192.168.100.10) in the inside network. So when all the outside hosts try to access the inside host, this will create a large traffic and may stop the exchange of data.

This can be useful when the inside host always has a static ip which is like a web server.

But any outside host access the inside host, therefore the security of the network is very low.

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

	In -> out	Out -> in
ping	×	×
ssh	√	√
http	√	√

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

Any tcp request (ssh,http) from outside hosts will be allowed to access the any inside hosts.

Any tcp request (ssh,http) from inside hosts will be allowed to access the outside hosts.

But pinging from inside to outside as well as from outside to inside did not happen.

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.

Since only the tcp connections are allowed to connect to the inside network from the outside it will secure the confidentiality of the data. And it will guarantee that data will be send to that specified one.

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

	In -> out	Out -> int
ping	√	√
ssh	√	×
http	√	×

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

Outside hosts are allowed to ping to the inside hosts. But it cannot connect to inside hosts through ssh or http.

The inside hosts can connect to the outside hosts through ping, ssh and http.

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

Outside host will be allowed to able to connect to the inside network by pinging. This can used when we want only to check the internal external connection.

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

	In -> out	Out -> int
ping	×	×
ssh	√	√
http	√	×

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

Only the tcp request which is equal to ssh, from the host 172.16.100.10(outside) is allow to access the inside 192.168.100.10. From outside host we cannot access inside host by pinging. And also http connection cannot be done from outside to inside.

From inside host we cannot ping to the outside host. 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.

In this scenario also only one host from the outside is allowed to access the inside host. So it will be drawback of this network because the outside host's ip address cannot be changed.

And it allows access only to ssh tcp requests. So this can be used when the client only wants a ssh connection between inside and outside.

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

	In -> out	Out -> int
ping	×	×
ssh	√	×
http	√	√

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

Only the tcp request which is equal to http, 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. And also ssh connection cannot be done from outside to inside.

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.

Many hosts can connect to inside host which is 192.168.100.10. And only the http requests from outside is allowed to access the inside network. So this policy can be used when the clients want only to connect to a web server. Inside host 192.168.100.10 will be having a static ip.

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

	In -> out	Out -> int
ping	√	√
ssh	√	√
http	√	√

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

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

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

This rule is same as in scenarios of 2. Scenario 4 is very different from this traffic filtering because they allow access only to ssh or http requests.

This policy also include a deny of TCP/HTTP. But it will not be run because of the order of policies. First policy allow any outside host to inside host. So there will be no room for the second rule to apply.

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

There will be no protection to inside network. So it will affect the confidentiality and integrity of the data in the inside network. And also it will make a high traffic of network and it will cause the denial of services.

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

	In -> out	Out -> int
ping	√	√
ssh	√	×
http	√	√

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

Any tcp request of ssh from the outside network to inside 192.168.100.10 host is not allowed to access. Any other request ping and http from outside to inside will be allowed to access.

Any request ping, ssh and http from inside to outside will be allowed to access.

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

Here the deny policy is first applied. So before the permit any it will deny any http requests from outside to inside. But it will allow any other request other than that.