E/15/220
Malihtha k.h.h.

CO325- Computer & Network Security

Lab 01 - Introduction to ASA and Basic network security handling

Follow-up Questions

1. **Section: Check Default Functionality of the Firewall**

	In → Out	Out → In
ping	**x**	**x**
ssh	↓	**x**
http	↓	**x**

(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.

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 → In
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.

In this situation 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 on the other hand no one else is allowed.so this can be a disadvantage.moreover the authorized person should always bear the same ip address.

This is what happens if the ip address of the outside host is changed to 172.16.100.11

	In → Out	Out → In
ping	**x**	**x**
ssh	**x**	**x**
http	**x**	**x**

Since the ip now is not 172.16.100.10 ,we cannot communicate from both sides,this can be a drawback of this policy.

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!

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 this situation this allows only the traffic to a particular host (192.168.100.10) only.so this can be useful when the host always has the static ip (like a webserver).

But on the other hand there is no restriction for the people who access something from 192.168.100.10 ,in other words 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 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.

This policy is more precise than the **Scenario# 1** .because in this scenario only TCP packets are allowed, so PING will not be allowed since it uses ICMP.so this policy kind of adds a restriction to the policy used in **Scenario# 1**.it has kind of overcome the cons of allowing any to any.so now even UDP packets will not be allowed,so this can be a side effect of this ACL.

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!

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.

To permit only the ICMP requests to communicate(only ping).
As in the above table Outside only allows the PING traffic which uses ICMP.

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

	In → Out	Out → In
ping	**x**	**x**
ssh	↵	↵
http	↵	**x**

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.

Before everything else, it allows only a particular host only.so this can be a drawback as discussed in the **Scenario# 2a**. So the outside host should always have the 172.16.100.10 ip address. But this actually restricts the other traffic.only SSH traffic is allowed from IN to OUT.so this is 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

	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 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.

To permit only the http requests to communicate with a given inside host from outside.

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

	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 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.

As per 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.

As per the test results shown in the above table this policy does not restrict anything. In my point of view,it's not really needed to have this policy if it allows traffic as shown in the table above.

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

	In → Out	Out → In
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).

In 5a all are woking fine. But in this ssh is not working from outside to inside.
This is happen because of the order of rules are applied.
Rules are check from start to end, if one rule is match then other rules are not considered.
That's why these two results are different.