E/15/280

Premathilaka M.P.U

CO325 - Assignment 1

1. Section: Check Default Functionality of the Firewall

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

   In default configuration after setting the security level between inside interface (100) and outside interface (0), since the security level of the inside interface is high, inside devices can communicate with outside devices using any protocol. But outside devices cannot communicate with inside devices even from Pinging, SSH session or HTTP request.

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

   Advantages:

   1. Since outside devices cannot access to the inside network, in this scenario inside network has the highest security.
   2. Traffic is low in the inside network
   3. Firewall has a less work load in the outside interface

   Disadvantages:

   1. Outside network cannot grant services provided by the inside network such as DNS server, Web server or DHCP server

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

   a. Scenario# 1: Permit Any

   1. What are the specific purposes of “access-list” and “access-group” commands?

      access-list

      An access control list (ACL) consists of one or more access control entries (ACEs). These access control lists are defined by access-list command and the user can add name to the list that define by him. Name of a particular IPv4 access list cannot contain a spaces or quotation marks, but can include numbers. Generally, these access lists define permitting and denying communications between inside and outside interfaces. If the user denies particular host from entering to a network the ASA firewall will filter the host at the relevant interface. User can decide which protocols should filter by the ASA. And most importantly, the use enters multiple access lists, ACL give priority to the access list entered first by the user.

      access-group

      access-group command is used to apply defined access-list (ACL) to specified interface (inbound or outbound)

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

	Internal to External	External to Internal
Ping	✓	✓
SSH	✓	✓
HTTP	✓	✓

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

Pros:

1. ACL does not need to filter outside traffic. Therefore, the work load to the outside interface of ACL firewall will be decreased
2. Since there is no restrictions, outsiders can communicate with the inside network without any issue

Cons:

1. Since there is no packet filtering, anyone can access to the inside network. There will be a huge security issue in this method.
2. Inside network traffic will be increased.

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

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

	Internal to External	External to Internal
Ping	✓	✓
SSH	✓	✓
HTTP	✓	✓

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

- When we get a network-based service from an outside company, we will have to allow them to access our network in order to fix failures and to do troubleshooting. We can allow specified host(technician) from their network to access our inside network.
- Due to security reasons, some government hosts are not allowed to permit by firewalls.

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

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

	Internal to External	External to Internal
Ping	✓	✓
SSH	✓	✓
HTTP	✓	✓

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

   - If the inside host is a server which should be public. Ex: DNS server, DHCP server or Web server

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

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

	Internal to External	External to Internal
Ping	×	×
SSH	✓	✓
HTTP	✓	✓

2. 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.

   "access-list any2anytcp extended permit tcp any any"

   In the Scenario #1 access-list is defined as permit any. Therefor, all 3 connections could be established. But in this case access list specified such that protocols which use tcp could communicate with the inside network. Since Ping works at layer 3 in the TCP/IP suite it does not use tcp connections at the transport layer. SSH and HTTP are application layer protocols and they use tcp connections.

   Ping does not work from internal computer to the external computer. Since the outside interface deny protocols other than tcp, the reply message of pinging will not come back to the internal computer from the external computer.

   By adding this to firewall, attacks are which running below the transport layer will not affect to the inside network and also the network traffic by protocols such as ICMP will be restricted.

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

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

	Internal to External	External to Internal
Ping	✓	✓
SSH	✓	×
HTTP	✓	×

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

- When the internal network wants to restrict accessing their web server by the outside network.
- When internal network wants to restrict creating ssh tunneling to their devices by the outside network
- When internal network wants to use all the application level protocols to access outside network by restricting outside network to access inside network using application level protocols.

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

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

	Internal to External	External to Internal
Ping	×	×
SSH	✓	✓
HTTP	✓	×

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

Since only SSH is allowed to the internal network, there can be security issues by providing remotely control internal hosts to the outside. Therefore, this situation will not use in practice.

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

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

	Internal to External	External to Internal
Ping	×	×
SSH	✓	×
HTTP	✓	✓

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

- If the webserver located in inside network, we would have to use this configuration.
- When we want SSH tunneling to be restricted by the outside network

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

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

	Internal to External	External to Internal
Ping	✓	✓
SSH	✓	✓
HTTP	✓	✓

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

```
ciscoasa(config)# access-list out2in extended permit ip any any
ciscoasa(config)#access-list out2in extended deny tcp any host 192.168.100.10 eq http
ciscoasa(config)# access-group out2inin interface outside
```

Since as the first access-list is not replaced by the second access-list, any outside host/protocol can communicate with the inside network.

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

Since anyone from the outside network could communicate with the inside network there is a huge security issue. Thus, this type of ACE is not used.

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

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

	Internal to External	External to Internal
Ping	✓	✓
SSH	✓	×
HTTP	✓	✓

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

```
ciscoasa(config)# access-list out2inextended deny tcp any host 192.168.100.10 eq ssh
ciscoasa(config)# access-list out2in extended permit ip any any
ciscoasa(config)# access-groupout2inin interfaceoutside
```

Unlike in scenario 5a, here the permit any is entered as the second command. Since it does not replace the first access-list, ACL accept the first access-list.