K A D NADEESHAN

E/13/234

SEMESTER 5

**LAB 01 – COMPUTER NETWORK SECURITY**

CO325 – Computer Network Security

Lab 01 - Introduction to ASA and Basic network security handling

**Section 01: Check Default Functionality of the Firewall**

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

In Cisco ASA 5510 firewall, it has method to compare every packet to a set of criteria prior to forwarding it. It can either drop or forward the packets to destination according to the criteria and packet.

This packet filtering mechanism work on Network layer of OSI model (IP layer of TCP/IP).

This packet filtering strategy, using ACL, it permits or denies the packet traffic on,

* Source IP address
* Destination IP address
* TCP/UDP port numbers

It can also track the TCP/UDP sessions in a flow table.

1. *Identify the advantages and disadvantages of this default functionality.*

Low cost and Low impact on network performance are the advantages. But it is not easy to upgrade, configure, maintain the system and need physical space including cabling are the disadvantages.

**Section 02: Modify Packet Filtering Rules on ASA – Configure Access Control Entries (ACEs)**

1. ***Scenario# 1: Permit Any***
2. What are the specific purposes of “access-list” and “access-group” commands?

Every IP traffic from a higher-security interface to a lower-security interface is allowed by default, but not vice versa. But we can configure whether it is allowed or not from lower secure interface to higher secure interface using the access list. When the packet arrived, the interface access list will be applied and permit or deny the traffic (if there is no per-user access list). access-group is used to apply an ACL to an "physical - interface". The **access-group** command cannot reference empty access lists or access lists that contain only a remark.

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

In this, it is allowed to both direction (server->client & client->server) both HTTP requests and ping requests.

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

Pros: Quick access and service

Cons: It is very risky in security side because it can be attacked by any device easily

1. ***Scenario# 2a: Permit Outside Host to Inside Any***
2. What has been permitted by the ACE in this scenario? Be precise!

As above scenario, it is allowed to both direction (server->client & client->server) both HTTP requests and ping requests. And also, this allows from a specific outside host to any device inside of the network.

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

Let’s think, if a company has network and they want to give access to new client for short time they can use this type of access

1. ***Scenario# 2b: Permit Outside Any to Inside Host***
2. What has been permitted by the ACE in this scenario? Be precise!

In this, it is allowed to both direction (server->client & client->server) both HTTP requests and ping requests. This allows from a specific outside device to any inside host of the network.

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

Let’s assume some company has a network and they want only their web server to be visible to Internet and other internal devices should not be visible. Giving access to only the web server and hiding other internal devices in the network can be done by above access type.

1. ***Scenario# 3a: Permit Outside Any to Inside Any –TCP***
2. What has been permitted by the ACE in this scenario? Be precise!

In here, ping requests are not allowed and HTTP requests are allow to client🡨🡪server.

1. How does this compare with Scenario# 1? What effect does this have in terms of the “cons” you identified in question 2.a.3. above.

This allows only the TCP packets from any outside device to any inside device. That’s

The reason to success HTTP request. But ping uses ICMP, it was not permitted.

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

This is the opposite of above scenario. That mean this allows only the ICMP packets from

any outside device to any inside device. That’s the reason to success ping request to

client🡨🡪server. But HTTP uses TCP, it was not permitted.

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

When we want to communicate only in command line and not using web browser we can use this type of access.

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

This is not allowed to neither HTTP request nor ping request from client-server and vice versa. This allows only TCP/SSH packets on specified subnet like 192.168.10.0/24.

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

If we want to transfer packets in specified subnet and want to reduce the unnecessary traffic, we can use this kind of access type.

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

This is only allowed HTTP request and ping request is not possible.

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

When some organization wants to permit only http request on web server, they can use this scenario.

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

This is possible to make the all three requests HTTP and ping.

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

When the router evaluates traffic against the list, it starts at the beginning of the list and

moves down, either permitting or denying traffic as it goes. When it has worked its way

through the list, the processing stops.

That means whichever rule comes first takes precedence. If the first part of the ACL

denies traffic, but a lower part of the ACL allows it, the router will still deny the traffic.

So even it denies a part in the second line, this does not count since whatever comes

first takes more precedence. So the denying part will not be in function at it is same as

the Scenario #1.

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

As same as in scenario 1 this is used in most commonly. But this is riskier because any device can access and attack.

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

This is not permit the TCP requests but http request as above scenario without ping requests.

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

When some organization has the web server and it is under maintaining. Then we can use this scenario. This is deny the TCP/SSH from outside device to inside server/host.

**Summery table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Scenario** | **Ping**  **Client -> server** | **Ping**  **Server -> client** | **HTTP** |
| **1** | **OK** | **OK** | **OK** |
| **2a** | **OK** | **OK** | **OK** |
| **2b** | **OK** | **OK** | **OK** |
| **3a** | **-** | **-** | **OK** |
| **3b** | **OK** | **OK** | **-** |
| **4a** | **-** | **-** | **-** |
| **4b** | **-** | **-** | **OK** |
| **5a** | **OK** | **OK** | **OK** |
| **5b** | **OK** | **OK** | **OK** |