# CO 325- lab1

# 1)

i). Default behavior would be if it's in routed mode:

High security level (100) in inside host..low security level in outside.

Traffic from low security level to high security level will allowed if there is static NAT configuration and ACL applied on the low security level interface to allow inbound traffic.

ii). There are security rules which can block traffic based on IP protocol.

An advantage of a default behavior is the server(inside ) is safe. Outside hosts cannot access and send malware to the server.

A disadvantage of the default configuration is even in a necessary situation outside hosts cannot access the server/inside.

# 2)

## a)scenario #1:

i). access-list used to apply an ACL to a line

Access-group used to apply an ACL to an interface

ii). This access list allows all outside hosts (on the interface to which applied the access list) to access the any inside host.

Ping and http connections were established between inside and outside computers.

iii). Any outside machine can access any inside computer. Therefore people can attack the internal network. As a pros the outside people can browse the network.

## b). scenario #2 a:

i). This access list allows considered outside host (192.168.200.10) to access inside any host.

Ping and http connections were established between inside computers and considered outside computer.

ii).Setting up a new staff account in pdn site to a new lecturer.

## c). Scenario #2b:

i). This access list allows considered outside any host to access inside considered host(192.168.200.10)

Ping and HTTP connections were established between inside considered computer and outside computers.

ii).Popular servers allow access to any users.

## d). Scenario #3a:

i). This access list allows only TCP for all outside hosts (on the interface to which applied the access list) to access the any inside host.

HTTP connections were established but pinging was not supported.

ii).In this situation pinging requests were timed out. Because in here allows only TCP routings. ICMP is the protocol that is used in pinging. Above configuration blocks the ICMP in scenario #3a.

In scenario#1 there is no blocking for any protocol .Therefore ping and http works.

## e). Scenario #3b:

i). This access list allows only ICMP for all outside hosts (on the interface to which applied the access list) to access the any inside host.

Ping command worked , but http request timed out.

Here allows only ICMP. Therefore TCP requests not supported.

ii).Allows same type of data to access

## f). Scenario #4a:

i)This access list allows only TCP/SSH for outside host to inside subnet.

Ping command not worked, but TCP/SSH worked.

ii).To connect outside host to inside subnet

## g) Scenario #4b:

i)Only permit http connections from outside any host to inside considered host(192.168.200.10).

http connections were established but pinging was not supported.

ii)To send same type of data to a server

## h).Scenario #5a:

i).In this scenario allows to access outside any. Blocks TCP/HTTP traffic to inside host (192.168.200.10).

ii).In Scenario #2a- It allows **any traffic** from **outside specified host** to **inside any host** .

In Scenario #2b -It allows **any traffic** from **outside any host** to **inside specified host.**

In Scenario #4a - allows **only TCP/HTTP traffic** from **outside any host** to **inside specified host.**

In Scenario #5a- Here specialty is **blocking** a inside host.

iii).In a company if one of its servers has to be modified. Therefore Company wants to block the server until done the modification.

## i). Scenario #5b:

i). In here TCP/SSH traffic blocked from outside any host to inside host(192.168.200.10).

Ping command worked .TCP traffic allowed except above any host to 192.168.200.10 TCP/SSH traffic.

ii). #5a blocked A inside host to the outside.#5b blocked TCP/SSH protocol

| | **Outside ping** | **Inside(server) ping** | **HTTP** | **SSH** |
|---|---|---|---|---|
| **Scenario #1** | YES | YES | YES | YES |
| **Scenario #2a** | YES | YES | YES | YES |
| **Scenario #2b** | YES | YES | YES | YES |
| **Scenario #3a** | NO | NO | YES | NO |
| **Scenario #3b** | YES | YES | NO | NO |
| **Scenario #4a** | NO | NO | NO | YES |
| **Scenario #4b** | NO | NO | YES | NO |
| **Scenario #5a** | YES | YES | NO | YES |
| **Scenario #5b** | YES | YES | YES | NO |

References:

https://supportforums.cisco.com/document/69281/asa-using-packet-capture-troubleshoot-asa-firewall-configuration-and-scenarios