CO325 – Computer & Network Security

Lab 01 – Introduction to ASA and Basic network security handling

Objective: Learn the basic functionality and configuration of a Firewall

Goals:

1. Get familiarized with a Firewall Device (a Cisco ASA to be precise) using the CLI
2. Learn & perform the basic configuration of the device
3. Learn & identify the default functionality of a firewall
4. Configure a firewall to allow particular type of traffic
5. Learn different ways to configure a firewall to achieve the intended purpose and compare.

1. Setting up the Firewall Device (Cisco ASA 5510)

Login/Connect to Firewall device

- **Console Port** – You will get the prompt/mode at the previous exit
- **SSH/Telnet –** You will get the *user EXEC* mode

```
ciscoasa>
```

Enter *privileged EXEC* mode

```
ciscoasa> enable
password: ******* (provide password – changeme)
ciscoasa#
```

Enable configuration mode

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Check current (running) configuration

```
ciscoasa# show running-config
```

Change hostname/devicename (optional)

```
ciscoasa(config)# hostname CE-LAB-ASA5510
CE-LAB-ASA5510(config)#
```

Configure interfaces

(Group 1 use the Interfaces 0/0 and 0/1 – Use 100 as the third octet in IP addresses)
(Group 2 use the interfaces 0/2 and 0/3 – Use 200 as the third octet in IP addresses)

Configure "inside" interface (Ethernet 0/0 for Group 1, Ethernet 0/2 for Group 2)

```
ciscoasa(config)# interface ethernet 0/0
```

Give Label

```
ciscoasa(config-if)# nameif inside
```

Specify Security Level (this is automatically set based on the label – can change)

```
ciscoasa(config-if)# security-level 100
```

Assign IP

```
ciscoasa(config-if)# ip address 192.168.100.1 255.255.255.0
```

Bring up the Interface

```
ciscoasa(config-if)# no shutdown
```

Configure “outside” interface (Ethernet 0/1 for Group 1, Ethernet 0/3 for Group 2)

```
ciscoasa(config)# interface ethernet 0/1
```

Give Label

```
ciscoasa(config-if)# nameif outside
```

Specify Security Level (this is automatically set based on the label – can change)

```
ciscoasa(config-if)# security-level 0
```

Assign IP

```
ciscoasa(config-if)# ip address 172.16.100.1 255.255.255.0
```

Bring up the Interface

```
ciscoasa(config-if)# no shutdown
```

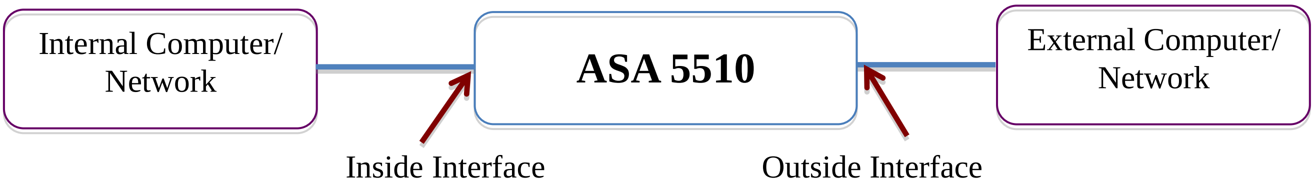
Check Particular Interface information

```
ciscoasa# sh interface ethernet 0/0
```

HINT: by typing ? after each command/option you can see the item/option expected next, and the format it has to be given.

2. Setup Network – Connecting “inside” and “outside” terminals

Network Diagram



Setting up the Network

- Connect your internal & external computers to your groups “inside” and “outside” interfaces in the ASA, respectively
- Configure the respective interfaces in the internal/external computers to be in the corresponding subnets. E.g.,
  a. **Internal Computer**
     IP Address: 192.168.100.10
     Mask: 255.255.255.0
     Gateway: 192.168.100.1
  b. **External Computer**
     IP Address: 172.16.100.10
     Mask: 255.255.255.0
     Gateway: 172.16.100.1
- Verify the basic network setup by checking the connectivity (ping) between the interfaces in the same subnet (e.g., between “inside” interface & internal computer) – from both sides.

3. Check Default Functionality of the Firewall

SSH Connections Between Internal & External Computers

- Make sure SSHD (OpenSSH Server) is running on the Internal & External Computers
- Check the connectivity (ping) between Internal and External Computers
- Try to create the following SSH Sessions
  - From Internal Computer to External Computer
  - From External Computer to Internal Computer

HTTP Connections between Internal & External Computers

- Make sure HTTP Server is running on the Internal & External Computers
- Check the connectivity (ping) between Internal and External Computers
- Try to create the following Browser Sessions
    - Check the main page on External Computer from the Internal Computer
    - Check the main page on Internal Computer from the External Computer

4. Modify Packet Filtering Rules on ASA – Configure Access Control Entries (ACEs)

Scenario# 1: Permit Any

Add Access Control List (ACL)

```
ciscoasa(config)#access-list out2inall extended permit ip any any
```

Apply an ACL to an Interface

```
ciscoasa(config)#access-group out2inall in interface outside
```

Check Ping, SSH and HTTP connections between Internal & External computers

Remove the ACEs

To remove any configuration use the same command with “no” keyword. E.g.,

ciscoasa(config)# **no** access-group out2inall in interface outside
ciscoasa(config)# **no** access-list out2inall extended permit ip any any

NOTE: For all the scenarios given below, make sure to remove the existing ACEs before configuring the new ACEs. Also, please append your group# to the ACL name (e.g., out2in_2).

Scenario# 2a: Permit Outside Host to Inside Any

```
ciscoasa(config)# access-list host2any extended permit ip host 172.16.100.10 any
ciscoasa(config)# access-group host2any in interface outside
```

Check Ping, SSH and HTTP connections between Internal & External computers

Scenario# 2b: Permit Outside Any to Inside Host

```
ciscoasa(config)# access-list any2host extended permit ip any host 192.168.100.10
ciscoasa(config)# access-group any2host in interface outside
```

Check Ping, SSH and HTTP connections between Internal & External computers

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

```
ciscoasa(config)# access-list any2anytcp extended permit tcp any any
ciscoasa(config)# access-group any2anytcp in interface outside
```

Check Ping, SSH and HTTP connections between Internal & External computers

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

```
ciscoasa(config)# access-list any2anyicmp extended permit icmp any any
ciscoasa(config)# access-group any2anyicmp in interface outside
```

Check Ping, SSH and HTTP connections between Internal & External computers

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

```
ciscoasa(config)#access-list host2subnettcpssh extended permit tcp host 172.16.100.10
                        192.168.100.0 255.255.255.0 eq ssh
ciscoasa(config)# access-group host2subnettcpssh in interface outside
```

Check Ping, SSH and HTTP connections between Internal & External computers

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

```
ciscoasa(config)# access-list any2hosttcphttp extended permit tcp any host 192.168.100.10
                  eq http
ciscoasa(config)# access-group any2hosttcphttp in interface outside
```

Check Ping, SSH and HTTP connections between Internal & External computers

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

```
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 out2in in interface outside
```

Check Ping, SSH and HTTP connections between Internal & External computers

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

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

Check Ping, SSH and HTTP connections between Internal & External computers

******************** Additional tasks and Commands ********************

Setup SSH Access to the ASA

Configure the Management interface (i.e., interface Management 0/0)

IP Address = 10.0.0.1/255.255.255.0
Nameif = MGMT

Check SSL encryption

```
ciscoasa# show running-config ssl
```

Set SSL encryption (if “show run ssl” is empty or contains basic SSL. E.g., only des-sha1)

```
ciscoasa(config)# ssl encryption aes256-sha1 aes128-sha1 3des-sha1 des-sha1
```

Generate RSA key

```
ciscoasa(config)# crypto key generate rsa modulus 1024
```

Enable SSH Access on the Management Interface (from any host)

```
ciscoasa(config)# ssh 0.0.0.0 0.0.0.0 MGMT
```

Setup Authentication With local database

```
ciscoasa(config)#username celab password celab123
ciscoasa(config)# aaa authentication ssh console LOCAL
```

Login to management console via SSH – From a computer that has an interface in the same subnet as the ASA Management interface & connected to the same LAN.

Saving & Restoring Configuration Settings

Save current (running) configuration

```
ciscoasa(config)# write memory
```

This is equivalent to:

```
ciscoasa(config)# copy running-config startup-config
```

Backup current (running) configuration

ciscoasa(config)# copy running-config disk0:/*file_name*

Restoring Configurations – Multiple options

Merge "running-config" with "Startup-config"

```
ciscoasa(config)# copy startup-config running-config
```

Reload the device with "startup-config"; discard running-config (unless saved!)

```
ciscoasa(config)# reload
```

Discard "running-config" and load "startup-config" (or saved config) without reload

```
ciscoasa(config)# clear configure all
ciscoasa(config)# copy startup-config running-config OR
ciscoasa(config)# copy disk0:/saved_config_file running-config
```

Other Useful Commands:

How to verify Version

```
ciscoasa(config)# sh version
```

How to Set Time & Date

```
ciscoasa# clock set 03:40:50 26 march 2015
```

How to Set Desired Banners

```
ciscoasa(config)# banner exec "you are off"
```

How to check state table

```
ciscoasa(config)# sh conn
```

How to check memory status

```
ciscoasa# sh memory
```

How to restrict access on Privilege mode

```
ciscoasa(config)# enable password new_password
```

How to check History of CLI

```
ciscoasa# sh history
```

How to check the applied IP Addresses on the Device

```
ciscoasa# sh ip addresses
```

How to check interface Labels

```
ciscoasa# sh nameif
```

How to check Interfaces summary

```
ciscoasa(config)# sh interface ip brief
```

Basic commands and use of "?" and tab (How to get a help)

clear	Reset functions
enable	Turn on privileged commands
exit	Exit from the EXEC
help	Interactive help for commands
login	Log in as a particular user
logout	Exit from the EXEC
ping	Send echo messages
quit	Exit from the EXEC
show	Show running system information
traceroute	Trace route to destination

ASA Configuration Guides: http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

- Find the correct ASA software version by using the command "show version".
- Get the corresponding ASA documentation for most accurate information

CO325 – Lab 01: Follow-up Questions

1. **Section: Check Default Functionality of the Firewall**
   a. What is the default behavior (in terms of Packet Filtering strategy) of Cisco ASA 5510 firewall?
   b. Identify the advantages and disadvantages of this default functionality.
2. **Section: Modify Packet Filtering Rules on ASA – Configure Access Control Entries (ACEs)**
   a. **Scenario# 1: Permit Any**
      i. What are the specific purposes of “access-list” and “access-group” commands?
      ii. What has been excluded from the filtering (i.e., permitted) by the ACEs in this scenario? Be precise!
      iii. Identify the pros and cons of this approach in permitting traffic from outside to reach the internal network.
   b. **Scenario# 2a: Permit Outside Host to Inside Any**
      i. What has been permitted by the ACE in this scenario? Be precise!
      ii. Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.
   c. **Scenario# 2b: Permit Outside Any to Inside Host**
      i. What has been permitted by the ACE in this scenario? Be precise!
      ii. Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.
   d. **Scenario# 3a: Permit Outside Any to Inside Any – TCP**
      i. What has been permitted by the ACE in this scenario? Be precise!
      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.
   e. **Scenario# 3b: Permit Outside Any to Inside Any – ICMP**
      i. What has been permitted by the ACE in this scenario? Be precise!
      ii. Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.
   f. **Scenario# 4a: Permit Outside host to Inside Subnet – TCP/SSH**
      i. What has been permitted by the ACE in this scenario? Be precise!
      ii. Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.
   g. **Scenario# 4b: Permit Outside Any to Inside Host – TCP/HTTP**
      i. What has been permitted by the ACE in this scenario? Be precise!
      ii. Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.
   h. **Scenario# 5a: Deny Outside Any to Inside Host – TCP/HTTP + Permit Any**
      i. What has been permitted by the ACE in this scenario? Be precise!
      ii. Compare this approach of traffic filtering with the approach used in scenarios 2 – 4.
      iii. Identify the situation(s) that are best suited for such an ACE, if any. If not, explain why.
   i. **Scenario# 5b: Permit Any + Deny Outside Any to Inside Host – TCP/SSH**
      i. What has been permitted by the ACE in this scenario? Be precise!
      ii. Compare this with the scenario above (5a).

DEADLINE will be announced on FEeLS!