ICT2203/ICT2203X Network Security

2021-2022 Trimester 3

Laboratory 6:
Attacks and Defense of IP Networks with Firewalls

LEARNING OUTCOMES

Upon completion of this laboratory exercise, you should be able to:

- Configure ASA firewall with security level, ACL and MPF
- Conduct and defend against TCP SYN attack using ASA firewall
- Conduct and defend against Slowloris attack using ASA firewall

REQUIRED HARDWARE

- 1 x Rack of Cisco network devices
- 1 x Box of Ethernet and console cables
- 3 x Laptops

REQUIRED SOFTWARE

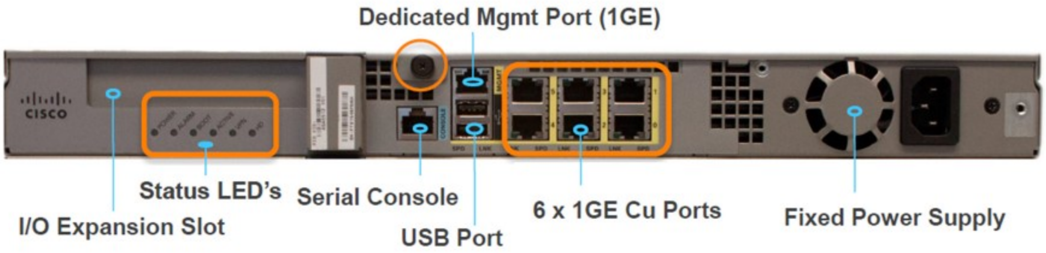
- Tera Term 4.106 http://ttssh2.osdn.jp/index.html.en
- Kali Linux Live Boot USB drive or equivalent

EXERCISE 1: GETTING TO KNOW CISCO ASA FIREWALL

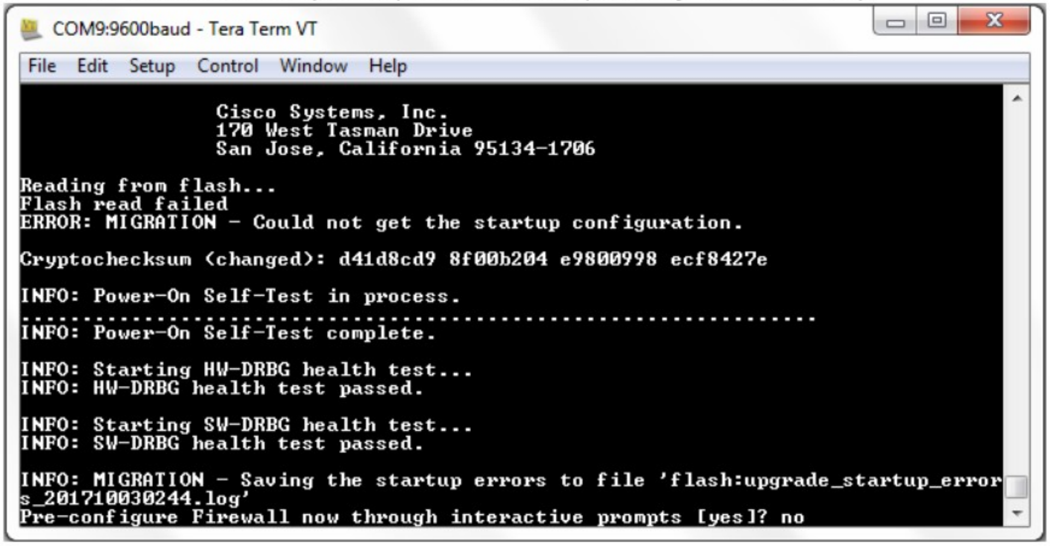
1.0: Establish Console Session with Cisco ASA Firewall and Optionally Initialize It

1.0.1 Similar to Cisco routers, Cisco ASA can be configured using CLI commands. (However, note that some commands are slightly different.)

1.0.2 To begin, power up ASA and connect a console cable to your PC and the ASA serial console port as shown in below diagram:



1.0.3 Start Tera Term, regardless whether you see the prompt as shown below asking for 'Pre-configure Firewall now through interactive prompts [yes]? or you may see a blank screen, just key in '**no**' before pressing the 'Enter' key.


COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
                 Cisco Systems, Inc.
                 170 West Tasman Drive
                 San Jose, California 95134-1706

Reading from flash...
Flash read failed
ERROR: MIGRATION - Could not get the startup configuration.

Cryptochecksum (changed): d41d8cd9 8f00b204 e9800998 ecf8427e

INFO: Power-On Self-Test in process.
.......................................................................
INFO: Power-On Self-Test complete.

INFO: Starting HW-DRBG health test...
INFO: HW-DRBG health test passed.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.

INFO: MIGRATION - Saving the startup errors to file 'flash:upgrade_startup_error
s_201710030244.log'
Pre-configure Firewall now through interactive prompts [yes]? no
```

1.0.4 If you simply press 'Enter' key which will default to '**yes**', the ASA will bring you through a long tedious process of interactive configurations.

Note: If you are stuck in the interactive configurations, press and hold on to the power button on the ASA to power it off. Wait for a while and then power it on again.

Remember patience is virtue! If you keep pressing the ‘Enter’ key during powering up, you may be brought into the interactive configurations again, and you will have to repeat the whole process again and again.

1.0.5 Once you are out of the interactive configurations trap, you will be in the user EXEC mode similar as Cisco switches and routers. Congrats! You have successfully establish a console session with ASA.

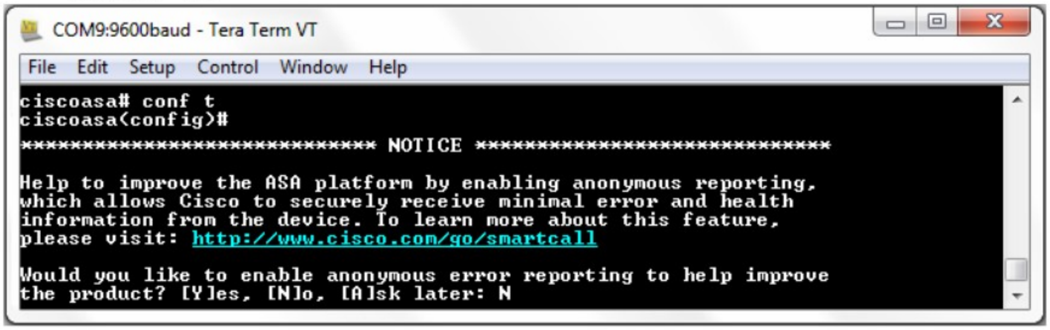
ciscoasa>

1.0.6 To go to the privileged EXEC mode, enter the **enable** command and password which is none by default.

ciscoasa> **enable**
Password: (simply press 'Enter' key because none was set by default)
ciscoasa#

Warning: Be considerate. Do NOT set your password on any network device without being told to do so which will prevent others from using them. Violators will have marks deducted.

1.0.7 To go to the global configuration mode, enter the same **config t** command. You may be asked if you wish to enable anonymous reporting as shown below. Answer '**N**'.


COM9:9600baud - Tera Term VT
File Edit Setup Control Window Help

```
ciscoasa# conf t
ciscoasa(config)#
***************************** NOTICE *****************************

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: N
```

1.0.8 Now you may optionally restore ASA to its factory default settings by using the command:

```
ciscoasa# configure t
ciscoasa(config)# configure factory-default

WARNING: The boot system configuration will be cleared. The
first image found in disk0:/ will be used to boot the system
on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
...
<output omitted>
```

1.0.9 Alternatively, you may remove the the startup-config from the flash memory:

```
ciscoasa# write erase

Erase configuration in flash memory? [confirm]
[OK]
ciscoasa#
```

1.0.10 And then restart the ASA by entering the **reload** command. Remember to respond with **N** if prompted that the config has been modified and needs to be saved.

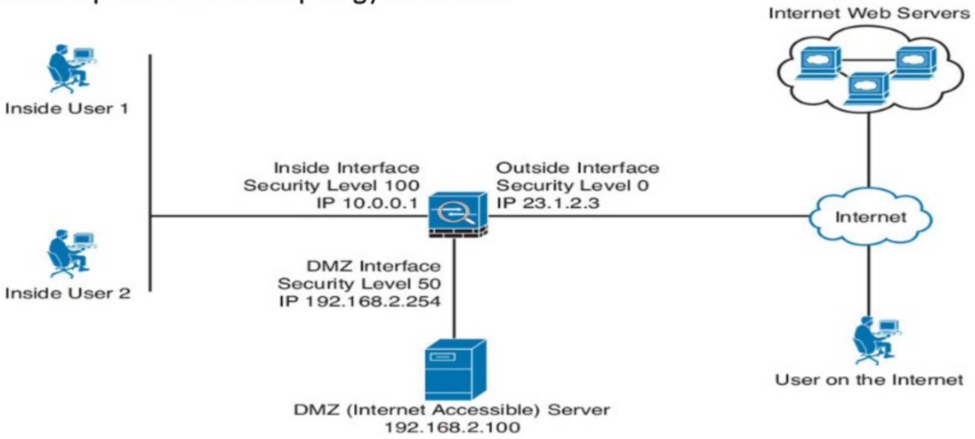
```
ciscoasa# reload

System config has been modified. Save? [Y]es / [N]o: N
Proceed with reload? [confirm]
```

```
ciscoasa#
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down File system
***
*** --- SHUTDOWN NOW ---
Process shutdown finished Rebooting.....
CISCO SYSTEMS
...
<output omitted>
```

1.1: Configure ASA Interface Security Level

1.1.1 Setup the network topology as shown:



1.1.2 Connect 1 PC to the inside interface of the ASA to act as Inside User, 1 PC to the DMZ interface to act as a web server, and 1 PC to the outside interface to act as Internet User which may also be an external attacker.

1.1.3 Configure the interfaces of the ASA with appropriate names, IP addresses and security levels.

1.1.4 When done, your ASA should be operational.

1.1.5 Boot up the Outside PC in Kali Linux, and the others in Windows.

1.1.6 Configure appropriate IP addresses, subnet masks and default gateways to the PCs.

1.1.7 Launch XAMPP and run Apache web server in the DMZ PC.

1.1.8 Startup a web browser at the Outside PC. Can it browse the website hosted at the DMZ PC? Why or why not?

1.1.9 Similarly, startup a web browser at the Inside PC. Can it browse the website hosted at the DMZ PC? Why or why not?

1.1.10 At the ASA, show the state tables as shown in Lab 6 Notes pg 21. What do you observe?

1.2: Override ASA Interface Security Level Access Control with ACL

1.2.1 As discussed, the design of DMZ (DeMilitarized Zone) is to allow organizations to host services, e.g. web servers, email servers, DNS, etc., for users from the Internet to access.

1.2.2 However by default, ASA will block Internet users with lower security level from initiating a connection to the DMZ and inside networks with higher security levels.

1.2.3 Nevertheless, you are able to override the security level access control in the ASA using ACLs.

1.2.4 Use the example in Lab 6 Notes pg 26-27 as a guide, configure an ACL to allow Outside PC to access the website hosted at the DMZ PC.

1.2.5 Next, startup a web browser at the Outside PC. Can it browse the website hosted at the DMZ PC now?

1.2.6 Again at the ASA, show the state tables. What do you observe?

1.3: Configure ASA Service Policy using MPF

1.3.1 For security reason, ASA will block ICMP ping packets by default, which explains why till now you've not been asked to use ping to verify your connection setup is correct.

1.3.2 In this exercise, you are going to practice using MPF to modify the default ASA access control policy to allow ping packets to pass through.

1.3.3 Read through Lab 6 Notes pg 30 - 39 on MPF.

1.3.4 Now, try using MPF to configure ASA to allow ICMP ping packets, e.g. as shown in Lab 6 Notes pg 34.

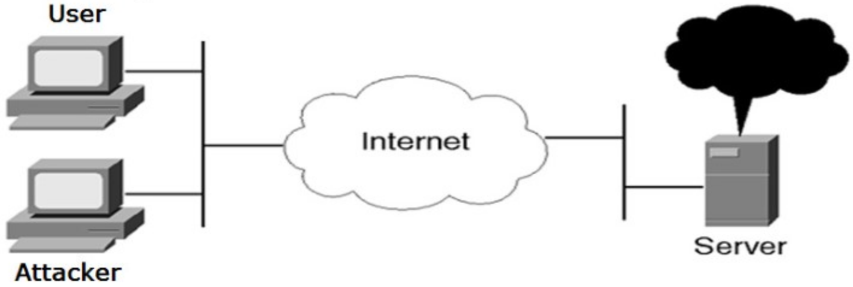
1.3.5 When done, verify that the Inside PC can indeed ping DMZ PC and Outside PC.

1.3.6 Similarly, show the state tables at the ASA. What do you observe?

EXERCISE 2: CONDUCT AND DEFEND AGAINST TCP SYN ATTACK

2.1: Conduct TCP SYN attack using hping3

2.1.1 Setup the network topology as shown, using a Cisco ASA firewall to act as the Internet with one interface connecting to the Server, and another interface connecting via a switch to the User PC and Attacker PC:



2.1.2 Bootup the Attacker PC in Kali Linux and the User PC may be in Windows or Kali Linux.

2.1.3 Bootup the Server in Windows and start XAMPP to run Apache Web server that you've learned in ICT1004.

2.1.4 Configure suitable IP address on the PCs and Server.

2.1.5 In addition, configure suitable IP addresses, names, security levels and ACL on ASA.

2.1.6 When done, verify that the User and Attacker's PCs are able to browse the Web Server to ensure that your setup is correct.

2.1.7 Next, conduct TCP SYN flooding attack from the Attacker's PC to the Web Server.

2.1.8 Start a terminal on the Web Server. Are you able to see many TCP SYN_RECEIVED states similar as Lab 6 Notes pg 42?

2.1.9 Does the response, e.g. mouse movements, at the Web Server become sluggish during attack?

2.1.10 Is the User PC able to visit the Web Server during the attack?

2.2: Defend against TCP SYN attack using ASA MPF service policy

2.2.1 Configure embryonic connection limits using MPF as discussed in Lab 6 Notes pg 43.

2.2.2 In addition, enable threat detection statistics as shown in Lab 6 Notes pg 47.

2.2.3 Restart XAMPP running Apache at the Web Server.

2.2.4 When done, conduct TCP SYN flooding attack from the Attacker's PC to the Web Server again.

2.2.5 At the terminal on the Web Server, do you see less TCP SYN_RECEIVED states as compared to that shown in Step 2.1.8?

2.2.6 Does the response, e.g. mouse movements, at the Web Server become sluggish during attack now?

2.2.7 Is the User able to visit the Web Server during the attack now?

2.2.8 What do you observe about the TCP intercept statistics?

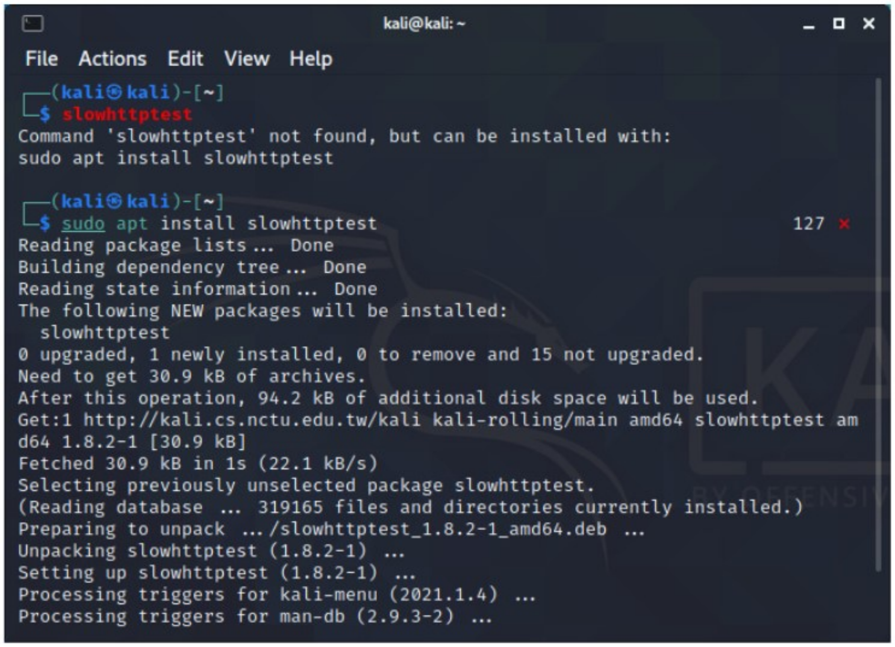
2.2.9 Do you think that ASA MPF service policy is useful against TCP SYN attack?

EXERCISE 3: CONDUCT AND DEFEND AGAINST SLOWLORIS ATTACK

3.1: Conduct Slowloris attack using slowhttptest

3.1.1 Reuse the same network topology as in Exercise 2.

3.1.2 Ensure your Kali Linux host has access to the Internet and install slowhttptest as shown:



```
┌──(kali㉿kali)-[~]
└─$ slowhttptest
Command 'slowhttptest' not found, but can be installed with:
sudo apt install slowhttptest

┌──(kali㉿kali)-[~]
└─$ sudo apt install slowhttptest                                    127 ×
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  slowhttptest
0 upgraded, 1 newly installed, 0 to remove and 15 not upgraded.
Need to get 30.9 kB of archives.
After this operation, 94.2 kB of additional disk space will be used.
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 slowhttptest am
d64 1.8.2-1 [30.9 kB]
Fetched 30.9 kB in 1s (22.1 kB/s)
Selecting previously unselected package slowhttptest.
(Reading database ... 319165 files and directories currently installed.)
Preparing to unpack .../slowhttptest_1.8.2-1_amd64.deb ...
Unpacking slowhttptest (1.8.2-1) ...
Setting up slowhttptest (1.8.2-1) ...
Processing triggers for kali-menu (2021.1.4) ...
Processing triggers for man-db (2.9.3-2) ...
```

3.1.3 When done, launch Slowloris attack as shown in Lab 6 Notes pg 50 at the Web Server.

3.1.4 How soon does the web server become unavailable during the attack?

3.1.5 Is the User PC able to visit the Web Server PC during the attack?

3.2: Defend against Slowloris attack using ASA MPF service policy

3.2.1 Using similar format as the MPF example to defend against TCP SYN attack in Lab 6 notes pg 43 as a guide, try configuring suitable MPF service policy to defend against Slowloris attack.

Hint: In the configuration of policy-map, use '?' to explore suitable commands to use to defend against the characteristics of Slowloris attack.

3.2.2 When done, launch Slowloris attack at the Web Server from the Attacker's PC again.

3.2.3 Is the User PC able to visit the Web Server during the attack now? If not, repeat Step 3.2.1 with different commands and try again.

3.2.4 Did slowhttptest wrongly indicate that the service was not available even when Slowloris attack was defended by your MPF service policy? Why?

3.2.5 Do you think that ASA MPF service policy is useful to minimise the success of Slowloris attack?