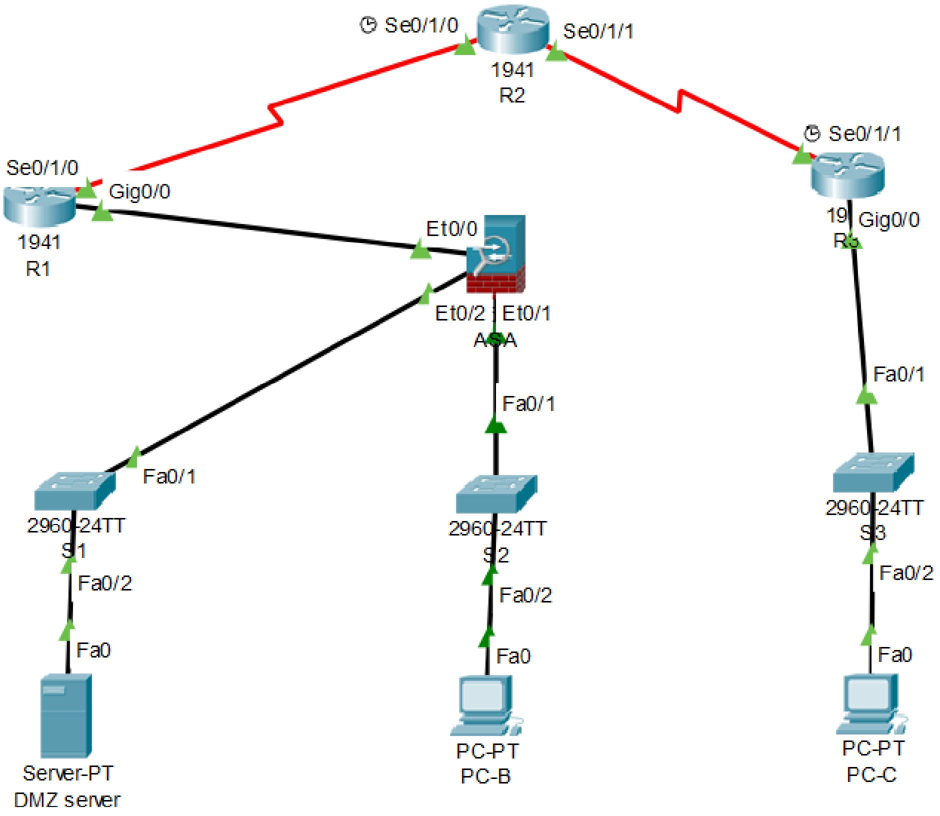
Security In Computing Practical’s

Practical 10: Configuring ASA Basic Settings and Firewall Using CLI

Topology:



Addressing Table:

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	gig0/0	209.165.200.225	255.255.255.248	N/A
	Se0/1/0	10.1.1.1	255.255.255.252	N/A
R2	Se0/1/0	10.1.1.2	255.255.255.252	N/A
	Se0/1/1	10.2.2.2	255.255.255.252	N/A
R3	gig0/0	172.16.3.1	255.255.255.0	N/A
	Se0/1/0	10.2.2.1	255.255.255.252	N/A
ASA	VLAN 1 (Et0/1)	192.168.1.1	255.255.255.0	N/A
ASA	VLAN 2 (Et0/0)	209.165.200.226	255.255.255.248	N/A
ASA	VLAN 3 (Et0/2)	192.168.2.1	255.255.255.0	N/A
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

Security In Computing Practical’s

Objectives:

- Verify connectivity and explore the ASA
- Configure basic ASA settings and interface security levels using CLI
- Configure routing, address translation, and inspection policy using CLI
- Configure DHCP, AAA, and SSH
- Configure a DMZ, Static NAT, and ACLs

Part 1: Configure Router

Step 1: Configure secret on router

Execute command on all routers

```
R(config)# enable secret enpa55
```

Step 2: Configure console password on router

Execute command on all routers

```
R(config)# line console 0
R(config-line)# password conpa55
R(config-line)# login
```

Step 3: Configure SSH login on router

Execute command on all routers

```
R(config)# ip domain-name ccnasecurity.com
R(config)# username admin secret pa55
R(config)# line vty 0 4
R(config-line)# login local
R(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
```

Step 4: Configure OSPF on routers

Execute command on all routers

```
R1(config)#router ospf 1
R1(config-router)# network 209.165.200.0 0.0.0.7 area 0
R1(config-router)# network 10.1.1.0 0.0.0.3 area 0

R2(config)#router ospf 1
R2(config-router)# network 10.1.1.0 0.0.0.3 area 0
R2(config-router)# network 10.2.2.0 0.0.0.3 area 0

R3(config)#router ospf 1
R3(config-router)# network 172.16.3.0 0.0.0.255 area 0
R3(config-router)# network 10.2.2.0 0.0.0.3 area 0
```

Part 2: Verify Connectivity and Explore the ASA

Step 1: Verify connectivity.

Send packets from:

PCC -> R1, R2, R3

(Successful)

Send packets from:

PCC -> ASA, PC-B, DMZ server.

(Unsuccessful)

Step 2: Determine the ASA version, interfaces, and license.

Enter privileged EXEC mode. A password has not been set. Press Enter when prompted for a password.

```
ASA# show version
```

Step 3: Determine the file system and contents of flash memory.

```
ASA# show file system
ASA# show flash:
```

Part 3: Configure ASA Settings and Interface Security Using the CLI

Step 1: Configure the hostname and domain name.

```
ASA (config)#hostname CCNAS-ASA
CCNAS-ASA (config)# domain-name ccnasecurity.com
```

Step 2: Configure the enable mode password.

```
CCNAS-ASA (config)# enable password enpa55
```

Step 3: Set the date and time. *(your current time)*

```
CCNAS-ASA (config)#clock set 21:24:00 31 March 2022
```

Step 4: Configure the inside and outside interfaces.

```
CCNAS-ASA(config)# int vlan 1
CCNAS-ASA(config-if)# nameif inside
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# security-level 100
CCNAS-ASA(config-if)# int vlan 2
```

```
CCNAS-ASA(config-if)# nameif outside
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# security-level 0
```

Step 5: Check the configurations

```
CCNAS-ASA# show int ip brief
CCNAS-ASA# show ip address
CCNAS-ASA# show switch vlan
```

Step 6: Test connectivity to the ASA. (*Send packets*)

PCB -> ASA

(Successful)

PCB -> R1

(Unsuccessful)

Part 4: Configure Routing, Address Translation, and Inspection Policy Using the CLI

Step 1: Configure a static default route for the ASA.

```
CCNAS-ASA# show route
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
CCNAS-ASA# show route
```

Step 2: Test connectivity. (*Send packets*)

ASA -> R1

(Successful)

Step 3: Configure address translation using PAT and network objects.

```
CCNAS-ASA(config)# object network inside-net
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
```

Step 4: Test connectivity.

```
CCNAS-ASA# show run
```

PCB -> R1 (***Send packets***)

(Unsuccessful)

```
CCNAS-ASA# show nat
```

Step 5: Modify the default MPF application inspection global service policy.

```
CCNAS-ASA(config)# class-map inspection_default
CCNAS-ASA(config-cmap)# match default-inspection-traffic
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# inspect icmp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config)# service-policy global_policy global
```

Step 6: Test connectivity. (*Send packets*)

PCB -> R1

(Successful)

Part 5: Configure DHCP, AAA, and SSH

Step 1: Configure the ASA as a DHCP server.

```
CCNAS-ASA(config)# dhcpd address 192.168.1.5-192.168.1.36 inside
CCNAS-ASA(config)# dhcpd dns 209.165.201.2 int inside
CCNAS-ASA(config)# dhcpd enable inside
```

Change PC-B from a static IP address to a DHCP client, and verify that it receives IP addressing information.

Step 2: Configure AAA to use the local database for authentication.

```
CCNAS-ASA(config)# username admin password adminpa55
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
```

Step 3: Configure remote access to the ASA.

```
CCNAS-ASA(config)# crypto key generate rsa modulus 1024
Do you really want to replace them? [yes/no]: no
CCNAS-ASA(config)# ssh 192.168.1.0 255.255.255.0 inside
CCNAS-ASA(config)# ssh 172.16.3.3 255.255.255.255 outside
CCNAS-ASA(config)# ssh timeout 10
```

Step 4: Verify SSH session

```
PCB>ssh –l admin 192.168.1.1
Password:adminpa55
CCNAS-ASA>exit
```

Part 6: Configure a DMZ, Static NAT, and ACLs

Step 1: Configure the DMZ interface VLAN 3 on the ASA.

```
CCNAS-ASA(config)# int vlan 3
```

```
CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)# no forward int vlan 1
CCNAS-ASA(config-if)# nameif dmz
CCNAS-ASA(config-if)# security-level 70
CCNAS-ASA(config-if)# int et0/2
CCNAS-ASA(config-if)# switchport access vlan 3
```

Step 2: Check the configurations

```
CCNAS-ASA# show int ip brief
CCNAS-ASA# show ip address
CCNAS-ASA# show switch vlan
```

Step 3: Configure static NAT to the DMZ server using a network object.

```
CCNAS-ASA(config)# object network dmz-server
CCNAS-ASA(config-network-object)# host 192.168.2.3
CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227
CCNAS-ASA(config-network-object)# exit
```

Step 4: Configure an ACL to allow access to the DMZ server from the Internet.

```
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
CCNAS-ASA(config)# access-group OUTSIDE-DMZ in int outside
```

Step 5: Test access to the DMZ server.

The ability to successfully test outside access to the DMZ web server was not in place; therefore, successful testing is not required. Practical ends here

Security In Computing Practical’s