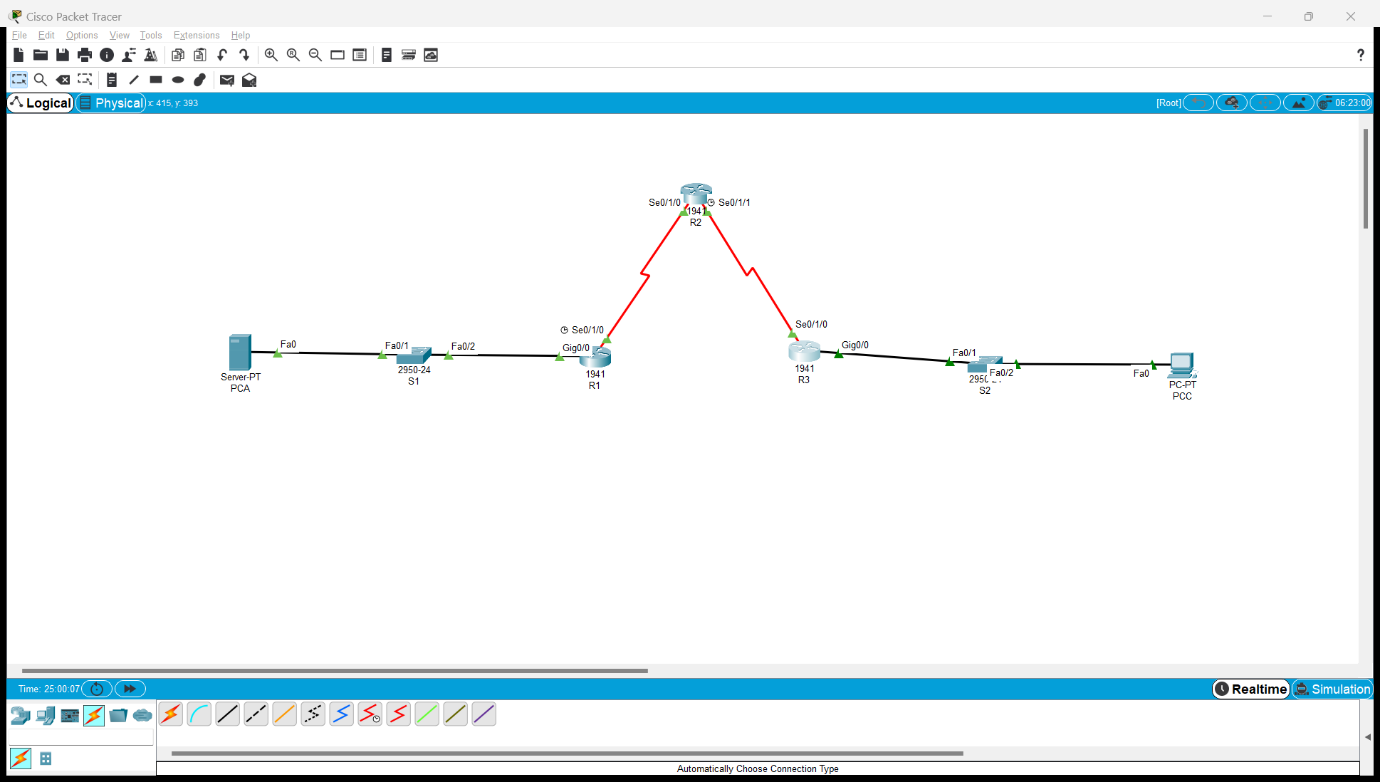
**Security In Computing Practical**

**Practical 5: Configuring a Zone-Based Policy Firewall (ZPF)**

**Topology:**



**Addressing Table:**

**Setting Display Name and Hostname**

Device - > Config - > Settings

Router -> R1/R2/R3

Switch S1/S2

Server->PCA

PC->PCC

**IP Addressing through CLI**

R1>en

R1#config t

R1(config)#interface GigabitEthernet0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#no shut

R1(config-if)#exit

R1(config)#interface Serial0/1/0

R1(config-if)#ip address 10.1.1.1 255.255.255.252

R1(config-if)#no shut

R1(config-if)#exit

R2>en

R2#config t

R2(config)#int se0/1/0

R2(config-if)#ip address 10.1.1.2 255.255.255.252

R2(config-if)#no shut

R2(config-if)#exit

R2(config)#int se0/1/1

R2(config-if)#ip address 10.2.2.2 255.255.255.252

R2(config-if)#no shut

R2(config-if)#exit

R3>en

R3#config t

R3(config)#interface GigabitEthernet0/0

R3(config-if)#ip address 192.168.3.1 255.255.255.0

R3(config-if)#no shut

R3(config-if)#exit

R3(config)#interface Serial0/1/0

R3(config-if)#ip address 10.1.2.1 255.255.255.252

R3(config-if)#no shut

R3(config-if)#exit

**Configure Router:**

**Step 1: 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 2: Configure password for vty lines**

***Execute command on all routers***

R(config)# line vty 0 4

R(config-line)# password vtypa55

R(config-line)# login

**Step 3: Configure secret on router**

***Execute command on all routers***

R(config) # enable secret enpa55

**Step 4: Configure SSH login on router**

***Execute command on all routers***

R(config)# ip domain-name ccnasecurity.com

R(config)# username admin secret adminpa55

R(config)# line vty 0 4

R(config-line)# login local

R(config-line)# crypto key generate rsa

How many bits in the modulus [512]: 1024

**Step 5: Configure OSPF routing on routers**

R1(config)#router ospf 1

R1(config-R1)#network 192.168.1.0 0.0.0.255 area 0

R1(config-R1)#network 10.1.1.0 0.255.255.255 area 0

R1(config-R1)#exit

R1(config)#exit

R1#show ip ospf interface gig0/0

R1#show ip ospf interface se0/1/0

R2(config)#router ospf 1

R2(config-R2)#network 10.1.1.0 0.255.255.255 area 0

R2(config-R2)#network 10.2.2.0 0.255.255.255 area 0

R2(config-R2)#exit

R2(config)#exit

R2#show ip ospf interface se0/1/0

R2#show ip ospf interface se0/1/1

R3(config)#router ospf 1

R3(config-R3)#network 192.168.3.0 0.0.0.255 area 0

R3(config-R3)#network 10.2.2.0 0.255.255.255 area 0

R3(config-R3)#exit

R3(config)#exit

R3#show ip ospf interface gig0/0

R3#show ip ospf interface se0/1/0

**Part 2: Verify Basic Network Connectivity**

**Step 1: Check connectivity from PCA to PCC**

PCA>ping 192.168.3.3

(Successful)

**Step 2: Access R2 using SSH.**

PCC>ssh –l admin 10.2.2.2

Password:adminpa55

R2>exit

**Step 3: From PC-C, open a web browser to the PC-A server.**

Desktop -> Web Browser

URL: http://192.168.1.3

(Successful)

**Part 3: Create the Firewall Zones on R3**

**Step 1: Verify that the Security Technology package**

R3# show version

**Step 2: Enable the Security Technology package**

R3(config)# license boot module c1900 technology-package securityk9

**Step 3: Save the running-config and reload the router**

R3#copy run start

R3# reload

**Step 4: Verify that the Security Technology package**

R3# show version

**Step 5: Create an internal zone.**

R3(config)# zone security IN-ZONE

R3(config-sec-zone)# exit

**Step 6: Create an external zone.**

R3(config)# zone security OUT-ZONE

R3(config-sec-zone)# exit

**Part 4: Identify Traffic Using a Class-Map**

**Step 1: Create an ACL that defines internal traffic.**

R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any

**Step 2: Create a class map referencing the internal traffic ACL**

R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP

R3(config-cmap)# match access-group 101

R3(config-cmap)# exit

**Part 5: Specify Firewall Policies**

**Step 1: Create a policy map to determine what to do with matched traffic.**

R3(config)# policy-map type inspect IN-2-OUT-PMAP

**Step 2: Specify a class type of inspect and reference class map IN-NET CLASS-MAP.**

R3(config-pmap)# class type inspect IN-NET-CLASS-MAP

**Step 3: Specify the action of inspect for this policy map.**

R3(config-pmap-c)# inspect

R3(config-pmap-c)# exit

R3(config-pmap)# exit

Part 6: Apply Firewall Policies

**Step 1: Create a pair of zones.**

R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE

**Step 2: Specify the policy map for handling the traffic between the two zones.**

R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP

R3(config-sec-zone-pair)# exit

R3(config)#

**Step 3: Assign interfaces to the appropriate security zones.**

R3(config)# int g0/0

R3(config-if)# zone-member security IN-ZONE

R3(config-if)# exit

R3(config)# int s0/1/0

R3(config-if)# zone-member security OUT-ZONE

R3(config-if)# exit

**Step 4: Copy the running configuration to the startup configuration.**

R3# copy run start

R3# reload

**Part 7: Test Firewall Functionality from IN-ZONE to OUT-ZONE**

**Step 1: From internal PC-C, ping the external PC-A server.**

PCC>ping 192.168.1.3

(Successful)

**Step 2: Access R2 using SSH.**

PCC>ssh –l admin 10.2.2.2

Password:

R2>

**Step 3: View established sessions**

R3# show policy-map type inspect zone-pair sessions

**Step 4: From PC-C, exit the SSH session on R2 and close the command prompt window.**

R2>exit

**Step 5: From internal PC-C, open a web browser to the PC-A server web page.**

Desktop -> Web Browser

URL: http://192.168.1.3

(Successful)

**Step 6: View established sessions**

R3# show policy-map type inspect zone-pair sessions

**Part 8: Test Firewall Functionality from OUT-ZONE to INZONE**

**Step 1: From internal PC-A, ping the external PC-C server.**

PCA>ping 192.168.3.3

(Unsuccessful – Request timed out)

**Step 2: From R2, ping PC-C.**

R2# ping 192.168.3.3

(Unsuccessful – Request timed out