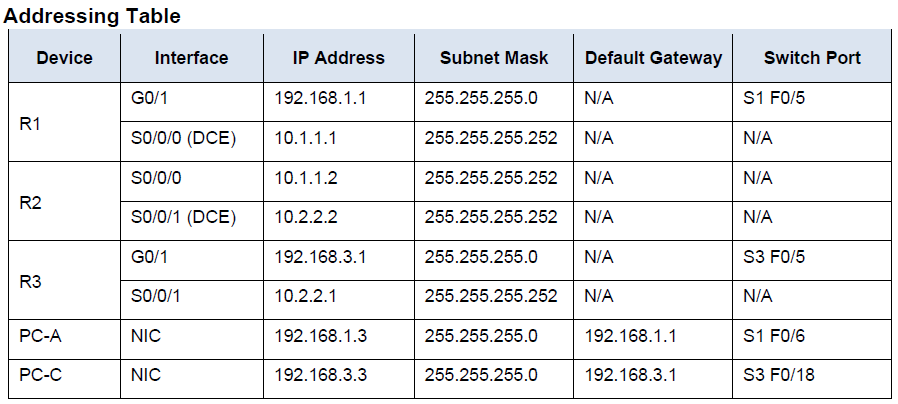
**Practical 6: Configuring a Zone-Based Policy Firewall (ZPF)**





Apply Static routing

Check connectivity from PCA

ping 192.168.1.1

ping 192.168.3.1

ping 192.168.3.3

ping 10.1.1.1

ping 10.1.1.2

ping 10.2.2.2

ping 10.2.2.1

for all routers

enable secret tyit1819

hostname R1

username Admin1 secret adminit2019

exit

end

password:tyit1819

config t

AAA new-model

AAA authentication login default local

Line console 0

Login authentication default

End

Exit

User access verification

Admin1

Adminit2019

En

Tyit1819

Config t

Ip domain-name tyit.com

Crypto key generate rsa

AAA authentication login SSH-LOGIN local

Line vty 0 4

Login authentication SSH-LOGIN

End

On command prompt of PC-C

ssh –l Admin1 10.2.2.2

On web browser of PC-C

<http://192.168.1.3>

**Create the Firewall Zones on R3**

Router 3

**Step 1: Enable the Security Technology package.**

a. On **R3**, issue the **show version** command to view the Technology Package license information.

b. If the Security Technology package has not been enabled, use the following command to enable the package.

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

c. Accept the end-user license agreement.

d. Save the running-config and reload the router to enable the security license.

e. Verify that the Security Technology package has been enabled by using the **show version** command.

**Step 2: Create an internal zone.** Use the **zone security** command to create a zone named **IN-ZONE**. R3(config)# **zone security IN-ZONE**

R3(config-sec-zone) exit

**Step 3: Create an external zone.** Use the **zone security** command to create a zone named **OUT-ZONE**.

R3(config-sec-zone)# **zone security OUT-ZONE** R3(config-sec-zone)# **exit**

**Part 3: Identify Traffic Using a Class-Map**

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

create extended ACL **101** to permit all IP protocols from the **192.168.3.0/24** source network to any destination.

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 4: Specify Firewall Policies**

**Step 1: Create a policy map to determine what to do with matched traffic.** Use the **policy-map type inspect** command and create a policy map named **IN-2-OUT-PMAP**.

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.**

The use of the **inspect** command invokes context-based access control (other options include pass and drop).

R3(config-pmap-c)# inspect

%No specific protocol configured in class IN-NET-CLASS-MAP for inspection. All protocols will be inspected. Issue the **exit** command twice to leave **config-pmap-c** mode and return to **config** mode.

R3(config-pmap-c)# exit

R3(config-pmap)# exit

**Part 5: Apply Firewall Policies**

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

Create a zone pair named **IN-2-OUT-ZPAIR**. Specify the source and destination zones that were created.

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

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

Attach a policy-map and its associated actions to the zone pair using the **service-policy type inspect** command and reference the policy map previously created, **IN-2-OUT-PMAP**.

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)# **interface g0/1**

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

R3(config-if)# exit

R3(config)# **interface s0/0/1**

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

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

**Part 6: Test Firewall Functionality from IN-ZONE to OUT-ZONE**

1. From the **PC-C** command prompt, ping **PC-A** at 192.168.1.3.
2. **From internal PC-C, SSH to the R2 S0/0/1 interface.**

**a.**  From the **PC-C** command prompt, SSH to **R2** at 10.2.2.2. Use the username **Admin** and the password **Adminpa55** to access R2. The SSH session should succeed.

1. b. While the SSH session is active, issue the command **show policy-map type inspect zone-pair sessions** on **R3** to view established sessions.

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

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

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

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

**5: Close the browser on PC-C.**

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

**Step 1: From the PC-A server command prompt, ping PC-C.**

From the **PC-A** command prompt, ping **PC-C** at 192.168.3.3. The ping should fail.

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

From **R2**, ping **PC-C** at 192.168.3.3. The ping should fail.