**Configuring a Zone-Based Policy Firewall**  **(ZPF)**

**Configure Router: (** Execute command on all routers  **)** R(config) #

**Step 1: Configure console password on router**

line console 0

password conpa55

login

exit

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

line vty 0 4

password vtypa55

login

exit

**Step 3: Configure secret on router**

enable secret enpa55

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

ip domain-name ccnasecurity.com

username admin secret adminpa55

line vty 0 4

login local

crypto key generate rsa

How many bits in the modulus [512]: 1024

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

ip route destination-network-address subnetmask next-hopdestination-address

**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)

**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

**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

**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

**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

zone-member security IN-ZONE

exit

int s0/1/0

zone-member security OUT-ZONE

exit

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

R3# copy run start

R3# reload

**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

**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)