Practical 6

1. Configuring a zone Based Policy Firewall (ZPF).

Part 1 - Verify Basic Network connectivity

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

PC-A > ping 192.168.3.3

Step 2 - Access R2 using SSH

PC-C > ssh -l Admin 10.2.2.2

Password:

R2 # exit

Step 3 - From PC-C, open a web-browser to PC-A

Click the Desktop tab and then click the web browser application, Enter the PC-A IP address 192.168.1.3.

Part 2 - Create the firewall zones on R3

Step 1 - Enable the security technology package on R3.

R3# show version
R3# conf t
R3(config)# license boot module c1900 technology-package security k9
R3(config)# exit
R3# copy run start
Destination filename [start-up-config]? [ENTER]
Building Configurations...
[OK]
R3# reload
R3# en
Password:
R3# show version

Step 2 - Create an internal zone

R3# conf t
R3(config)# zone security IN-ZONE
R3(config-sec-zone)# exit

Step 3 - Create an external zone

R3(config)# 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

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 Rules & 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 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 5- Apply Firewall Policies

Step 1- Create a pair of zones.

R3(config)# zone-pair security IN-Z-OUT-PAIR source IN-ZONE destination OUT-ZONE

Step 2- Specify the policy map for handling the traffic between the 2 zones.

R3(config-sec-zone-pair)# service-policy type inspect IN2-OUT-PM AP

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

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)# interface S0/0/1
R3(config-if)# zone-member security OUT-ZONE

Step 4- Copy the running configuration to the startup configuration.

R3# copy run start

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

Step1 - From Internal PC-C, ping PC-A server

PC-C > ping 192.168.1.3 # ping should succeed

Step2 - From Internal PC-C, connect SSH in R2

a) PC-C > ssh -l Admin 10.2.2.2
the ssh should succeed.

b) Using show -policy-map type inspect zone-pair sessions on R3 to view the established sessions

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

Step 3 - From PC-C exit the SSH session and open web browser and type 192.168.1.3; It should succeed.

Step 4 - Use the same show policy-map command to view the sessions.

R3 # show policy map type inspect zone pair sessions.

Step 5 - Close the web browser

Part 7 - Test the firewall functionality from OUT-ZONE to IN-ZONE

Step 1- From internal PC-A, ping internal PC-C i.e. this should fail.

PC-A > ping 192.168.3.3

Step 2- From internal router R2, ping the internal PC-C

R2#ping 192.168.3.3