Q. 6) configure IOS Intrusion Prevention System (IPS) using the CLI.

Step 1: Setting Up the Network Topology

* Drag and place the following devices on the workspace:

1. 1 Router (Place it in the center)
2. 2 Switches (Position them on either side of the router)
3. 1 PC (Connect it to one of the switches)
4. 1 Server (Connect it to the other switch)

* Click on the first wire with the lightning symbol (Automatically Choose Connection Type).

Connect the devices as follows:

Configuring IOS Intrusion Prevention System (IPS) Using CLI

Step 1: Securing Router Access

R1(config)# enable secret enpa55 (Sets a privileged mode password )

R1(config)# line console 0

R1(config-line)# password conpa55 (Sets console access password)

R1(config-line)# login ( Enables login for console )

R1(config)# exit

R1(config)# ip domain-name ccnasecurity.com (Defines domain name)

R1(config)# username admin secret adminpa5 (Creates an admin user)

R1(config)# line vty 0 4

R1(config-line)# login local (Enables remote login )

R1(config-line)# exit

R1(config)# crypto key generate rsa (Generates encryption keys)

[1024] (Key length)

Step 2: Enabling Security License & Reloading Router

R1(config)# exit

R1# conf terminal

R1# show version (Displays router details)

R1# conf terminal

R1(config)# license boot module c1900 technology-package securityk9

[yes] ( Enables security package)

R1(config)# exit

R1# reload (Reloads the router)

[yes]

Step 3: Configuring IPS Directory & Initial Setup

password: conpa55

R1> enable (Enters privileged mode)

Password: enpa55 (Enter enable password)

R1# mkdir iosips (Creates IPS directory)

Step 4: Managing Step 4: Configuring IPS (Intrusion Prevention System)

R1# conf t

R1(config)# ip ips config location flash:iosips (Sets IPS storage location)

R1(config)# ip ips name iosips (Creates IPS rule set)

R1(config)# ip ips signature-category

R1(config-ips-category)# category all

R1(config-ips-category-action)# retired true (Disables all signatures)

R1(config-ips-category-action)# exit

R1(config-ips-category)# category ios\_ips basic

R1(config-ips-category-action)# retired false (Enables selected signatures)

R1(config-ips-category-action)# exit

R1(config-ips-category)# exit

Do you want to accept these changes? [confirm]

Applying Category configuration to signatures...

Step 5: Applying IPS to an Interface and Setting System Time & Logging Configuration

R1(config)# interface gi0/0

R1(config-if)# ip ips iosips out (Applies IPS outbound)

R1(config-if)# exit

R1(config)#

R1(config)# ip ips notify log (Enables IPS logging )

R1(config)# exit

R1#

R1# clock set 11:58:00 07 March 2025 # Sets the system clock

R1# conf t

R1(config)# service timestamps log datetime msec (Enables log timestamps )

R1(config)# logging host 10.10.10.2 (Sends logs to a remote server)

Step 6: Configuring a Custom IPS Signature

R1(config)# ip ips signature-definition

R1(config-sigdef)# signature 2004 0 (Defines a new signature)

R1(config-sigdef-sig)# status

R1(config-sigdef-sig-status)# retired true (Disables default signature)

R1(config-sigdef-sig-status)# enabled true (Enables custom signature)

R1(config-sigdef-sig-status)# retired false (Re-enables it)

R1(config-sigdef-sig-status)# exit

R1(config-sigdef-sig)# event-action produce-alert (Generates alert when matched)

R1(config-sigdef-sig)# event-action deny-packet-inline (Blocks malicious packets)

R1(config-sigdef-sig)# exit

R1(config-sigdef)# exit

Do you want to accept these changes? [confirm]

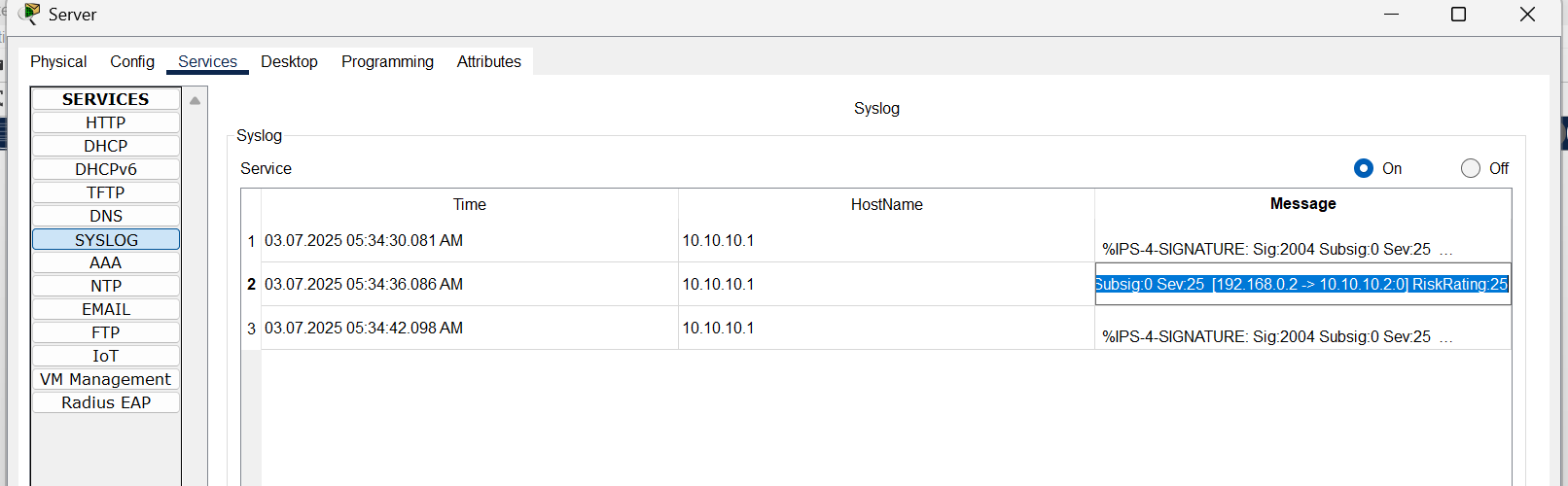
Step 7: Verify IPS Functionality by Pinging the Server

* Go to the Command Prompt (cmd) of the PC1.
* Run the command: ping 10.10.10.2

The ping should show "Request timed out," indicating that the Intrusion Prevention System (IPS) is actively blocking the traffic.

Step 9: Check Logs in the Syslog Server

* + Go to the Server → Syslog.
  + The logs should display entries indicating that the Intrusion Prevention System (IPS) has blocked the ping request from the PC.



Step 10: Add Another PC and Verify IPS Functionality

* + Drag and place another PC in the workspace.
  + Connect it to the switch using the appropriate cable.
  + Configure the new PC with:
* IP Address: 192.168.0.3
* Subnet Mask: 255.255.255.0
* Default Gateway: 192.168.0.1
* Open Command Prompt PC2 and run: ping 10.10.10.2

The ping should also show "Request timed out," confirming that IPS is actively blocking traffic from both PCs.