Exp no: 05 Configure IDPS/IPS in Cisco Packet
Date: 08/09/25 Tracer

Aim:

To configure Intrusion Detection and Prevention System (IDPS/IPS) on Cisco packet router, apply signatures, enable security features and verify intrusion alerts and packet blocking.

Procedure:

Device Required:

a. 1 Router
b. 2 PCs
c. 1 system Server

connections:

a. PC0 <→ R1 (Gigabit Ethernet 0/0)
b. PC1 <→ R1 (Gigabit Ethernet 0/1)
c. Syslog Server <→ R1 (connected to LAN)

Step 1: Enable user authentication

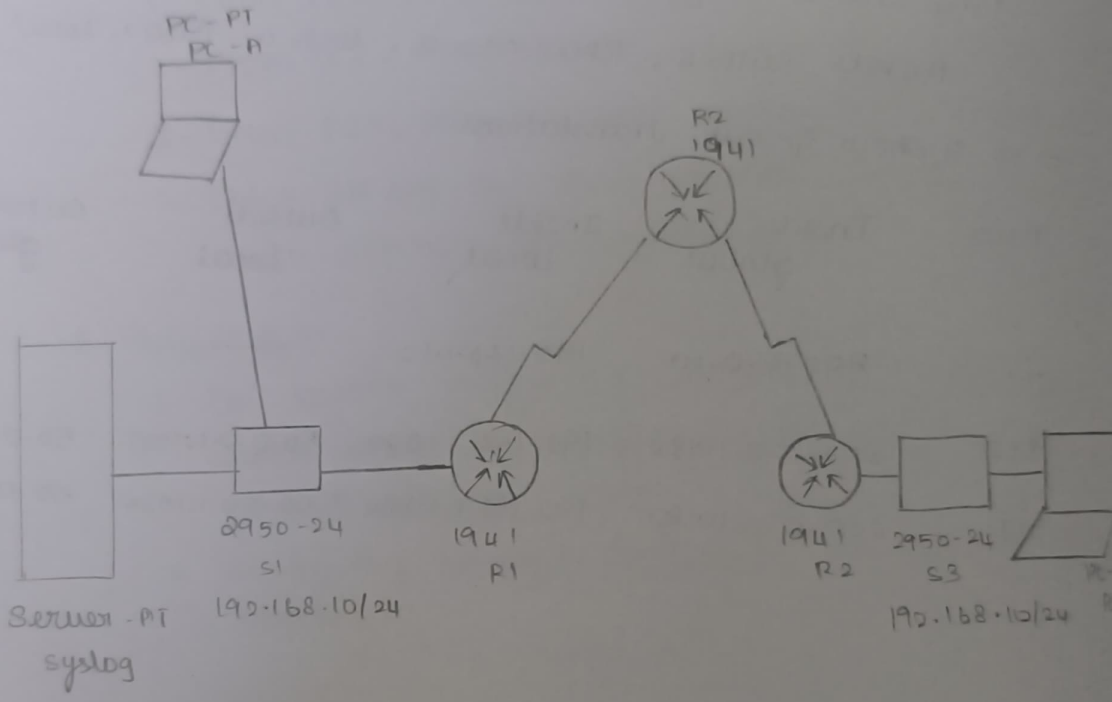
1. Create a local user account with a secret password
2. Enable AAA authentication
3. Configure console line login using AAA.

Step 2: Enable security package

1. Verify available licenses using show version
2. Activate security k9 technology package
3. Save configuration and reload the router
4. After reload, re-check with show version

Step 3: Basic connectivity check

1. From PC0 → Ping PC1 → should succeed
2. From PC1 → Ping PC0 → should succeed


PC-PT
PC-A
R2
1941
2950-24
S1
1941
R1
1941
R2
2950-24
S3
Server-PT
syslog
192.168.10/24
192.168.10/24

Step 4: Configure IPS on Router

1. Create a directory in flash memory for files
2. Specify IPS configuration location in flash
3. Create an IPS policy
4. Enable IPS notification to logs

Step 5: Configure time & logging

1. Set the correct clock on the router
2. Enable timestamp logging

Configure syslog server

Step 6: IPS signature configuration

1. Retire all default IPS signatures
2. Activate basic IOS IPS signatures only

Step 7: Apply IPS to interface.

1. On interface Gigabit Ethernet 0/1, apply IPS policy ios ips in the outbound direction.

Step 8: Modify ICMP signature

1. Edit ICMP signature
2. Ensure signature is enabled and active
3. Define event actions:
   a. Produce alert
   b. Deny packet Inline

Step 9: Verification

Use show ip ips all to verify IPS status, signatures and applied interfaces.

Step 10: Testing

a. From PC0 → Ping PC1 → should fail
b. From PC1 → Ping PC0 → should succeed
c. On syslog server → check logs for IPS alerts generated during ping attempt

Result:

Thus the cisco packet tracer is succesfully configured and verified.