Experiment - 5

Date: 10/09/2025

Configure IDS/IPS in Cisco Packet Tracer Network Topology

Aim:

To configure Intrusion Detection System/ Intrusion Prevention System in Cisco Packet Tracer.

Procedure:

Step-1: Configure User Authentication on Router1
#enable
#configure terminal
#username xxxx secret yyyy
#aaa new-model
#aaa authentication login default local
#line console 0
#login authentication default
#exit

Step-2: Enable Security License on Router1
#show version
#configure terminal
#license boot module c1900 technology-package securityk9
#yes
#end
#copy running-config startup-config
#reload
#show version

Step-3: Test basic connectivity
- On PC0, ping PC1 IP address
- On PC1, ping PC0 IP address

Step-4: Configure IPS directory and IPS policy
#mkdir ipsdir
#configure terminal
#ip ips config location flash:ipsdir
#ip ips name iosips
#ip ips notify log

#exit

Step-5: Configure clock, logging, and IPS signature
#clock set 19:25:59 9 July 2023
#configure terminal
#service timestamps log datetime msec
#logging host 192.168.1.50
#ip ips signature-category
#category all
#retired true
#exit
#category ios_ips basic
#retired false
#exit
Do you want to accept these changes? [Confirm]

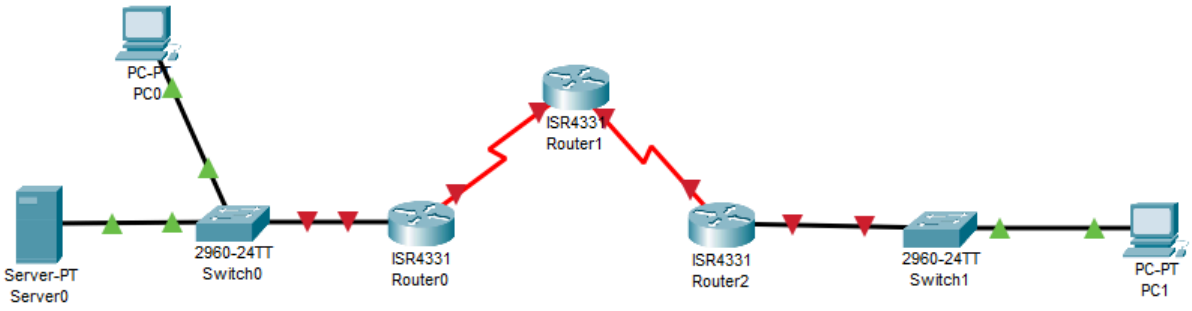
Step-6: Apply IPS policy to interface
#interface g0/1
#ip ips iosips out

Step-7: Modify IPS signature to deny ICMP echo replies
#ip ips signature-definition
#signature 2004 0
#status
#retired false
#enabled true
#engine
#event-action produce-alert
#event-action deny-packet-inline
#exit
#exit [Confirm]
#end
#show ip ips all

Step-8: Verify functionality
- From PC1, ping PC0 (should be denied and timeout)
- From PC0, ping PC1 (should be successful)

Step-9: Check Syslog Server
- Open Syslog server to view IPS logs.

Output:



1. IPS is enabled on Router1 and applied to the interface.
2. ICMP echo reply packets are denied as per IPS rule.
3. Syslog server successfully logs IPS alerts.
4. Ping from PC1 to PC0 fails, while ping from PC0 to PC1 succeeds.

Result:

The IDS/IPS was successfully configured on Router1 in Cisco Packet Tracer. The IPS detected and blocked ICMP echo reply packets as per the defined signature. Logging was enabled and syslog server captured the alerts, thus meeting all objectives of the experiment.