# Lab 08

# Configuring IOS Intrusion Prevention System (IPS)

|  |  |
| --- | --- |
| **Name:** | **Student ID:** |

## 7.1 Objective

The Objectives of this lab are:

* Enable IOS IPS.
* Configure logging.
* Modify an IPS signature.
* Verify IPS.

**7.2 Background**

Your task is to enable IPS on R1 to scan traffic entering the 192.168.1.0 network.

The server labeled Syslog is used to log IPS messages. You must configure the router to identify the syslog server to receive logging messages. Displaying the correct time and date in syslog messages is vital when using syslog to monitor the network. Set the clock and configure the timestamp service for logging on the routers. Finally, enable IPS to produce an alert and drop ICMP echo reply packets inline.

The server and PCs have been preconfigured. The routers have also been preconfigured with the following:

* Enable password: **ciscoenpa55**
* Console password: **ciscoconpa55**
* SSH username and password: **SSHadmin / ciscosshpa55**
* OSPF 101

**Topology**

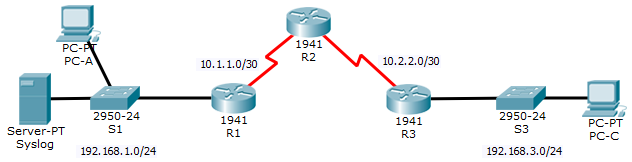


Figure 1: Topology

**Addressing Table**

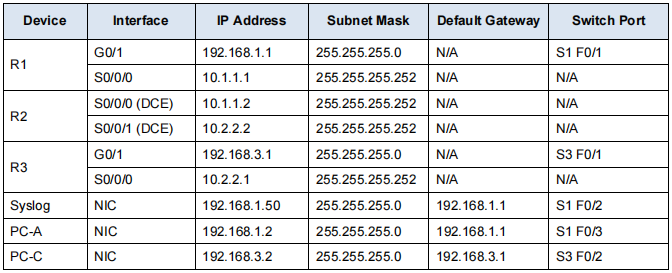


Table 1: Addressing Table

### Task 1: Enable IOS IPS

**Note:** Within Packet Tracer, the routers already have the signature files imported and in place. They are the default xml files in flash. For this reason, it is not necessary to configure the public crypto key and complete a manual import of the signature files.

1. Enable the Security Technology package on **R1**.
2. Verify network connectivity
3. Ping from **PC-C** to **PC-A**. The ping should be successful
4. Ping from **PC-A** to **PC-C**. The ping should be successful.
5. Create an IOS IPS configuration directory in flash.

On **R1**, create a directory in flash using **mkdir** command. Name the directory **ipsdir.**

1. Configure the IPS signature storage location.

On **R1**, configure the IPS signature storage location to the directory you just created.

R1(config)#**ip ips config location flash:ipsdir**

1. Create an IPS rule.

On **R1**, create an IPS rule name using **ip ips name** *name* command in global configuration mode. Name the IPS rule **iosips**.

1. Enable logging. IOS IPS supports the use of syslog to send event notification. Syslog notification is enabled by default. If logging console is enabled, IPS syslog messages display.
2. Enable syslog if it is not enabled.

R1(config)# **ip ips notify log**

1. If necessary, use the **clock set** command from privileged EXEC mode to reset the clock.
2. Verify that the timestamp service for logging is enabled on the router using the **show run** command.
3. Send log messages to the syslog server at IP address 192.168.1.50
4. Configure IOS IPS to use signature categories.

Retire the **all** signature category with the **retired true** command (all signatures within the signature release). Unretire the **IOS\_IPS Basic** category with the **retired false** command.

1. Apply the IPS rule to an interface.

Apply the IPS rule to an interface with the **ip ips name** *direction* command in interface configuration mode. Apply the rule outbound on the G0/1 interface of **R1**. After you enable IPS, some log messages will be sent to the console line indicating that the IPS engines are being initialized.

**Note:** The direction **in** means that IPS inspects only traffic going into the interface. Similarly, **out** means that IPS inspects only traffic going out of the interface.

**Task 2: Modify the Signature**

**Note:** For all configuration tasks, be sure to use the exact names as specified.

1. Change the event-action of a signature.

Un-retire the echo request signature (signature 2004, subsig ID 0), enable it, and change the signature action to alert and drop.

1. Use show commands to verify IPS.

Use the **show ip ips all** command to view the IPS configuration status summary. To which interfaces and in which direction is the **iosips** rule applied?

1. Verify that IPS is working properly.
2. From **PC-C**, attempt to ping **PC-A**. Were the pings successful? Explain.
3. From **PC-A**, attempt to ping **PC-C**. Were the pings successful? Explain.
4. View the syslog messages.
5. Click the **Syslog** server.
6. Select the **Services** tab.
7. In the navigation menu, select **SYSLOG** to view the log file.
8. Check results.

Your completion percentage should be 100%. Click **Check Results** to see feedback and verification of which required components have been completed.

## **Assessment Rubric**

**Lab 08**

**Configuring IOS Intrusion Prevention System (IPS)**

|  |  |
| --- | --- |
| **Name:** | **Student ID:** |

**Points Distribution**

|  |  |  |  |
| --- | --- | --- | --- |
| **Task No.** | **LR 2**  **Simulation** | **LR5**  **Results/Plots** | **LR9**  **Report** |
| Task 1 | 30 | 15 |  |
| Task 2 | 30 | 15 |  |
| Total | /60 | /30 | /10 |
| **CLO Mapped** | CLO 3 | CLO 3 | CLO3 |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Affective Domain Rubric** | | **Points** | **CLO Mapped** |
| AR 7 | Report Submission | /10 | CLO 3 |

|  |  |  |
| --- | --- | --- |
| **CLO** | **Total Points** | **Points Obtained** |
| 3 | 100 |  |
| **Total** | **100** |  |

*For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.*

**Lab Evaluation Assessment Rubric**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Assessment Elements** | **Level 1: Unsatisfactory**  **Points 0-1** | **Level 2: Developing**  **Points 2** | **Level 3:Good**  **Points 3** | **Level 4:Exemplary**  **Points 4** |
| **LR2** | **Program/Code/ Simulation Model/ Network Model** | Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software. | Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software. | Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine. | Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software. |
| **LR5** | **Results & Plots** | Figures/ graphs / tables are not developed or are poorly constructed with erroneous results. Titles, captions, units are not mentioned. Data is presented in an obscure manner. | Figures, graphs and tables are drawn but contain errors. Titles, captions, units are not accurate. Data presentation is not too clear. | All figures, graphs, tables are correctly drawn but contain minor errors or some of the details are missing. | Figures / graphs / tables are correctly drawn and appropriate titles/captions and proper units are mentioned. Data presentation is systematic. |
| **LR9** | **Report** | All the in-lab tasks are not included in report and / or the report is submitted too late. | Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date. | Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely. | Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables. |