Lab 08

Configuring IOS Intrusion Prevention System (IPS)

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

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

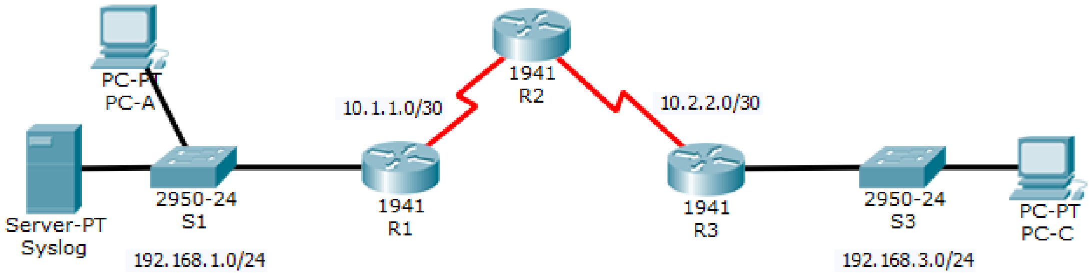
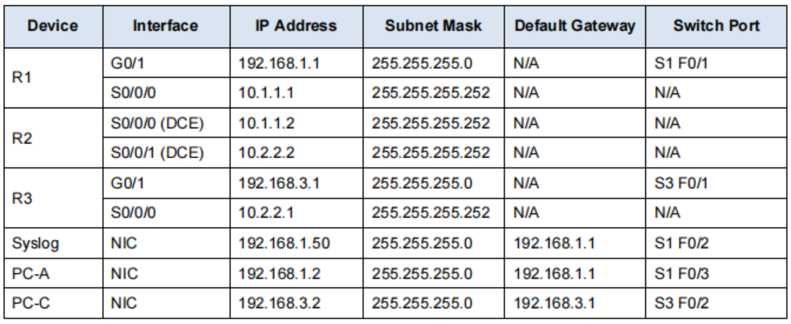


Figure 1: Topology

Addressing Table



Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/1
	S0/0/0	10.2.2.1	255.255.255.252	N/A	N/A
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1	S1 F0/2
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/2

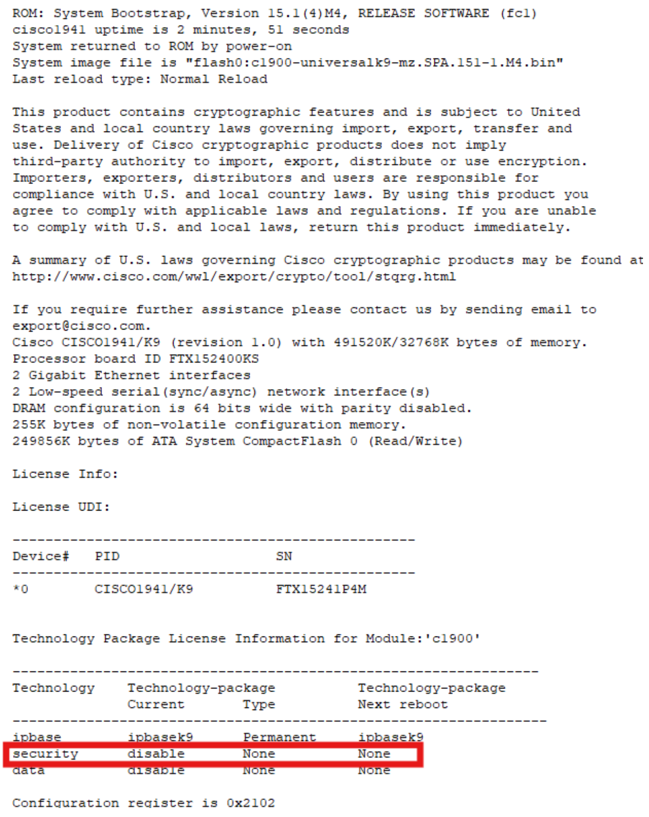
Table 1: Addressing Table

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**.

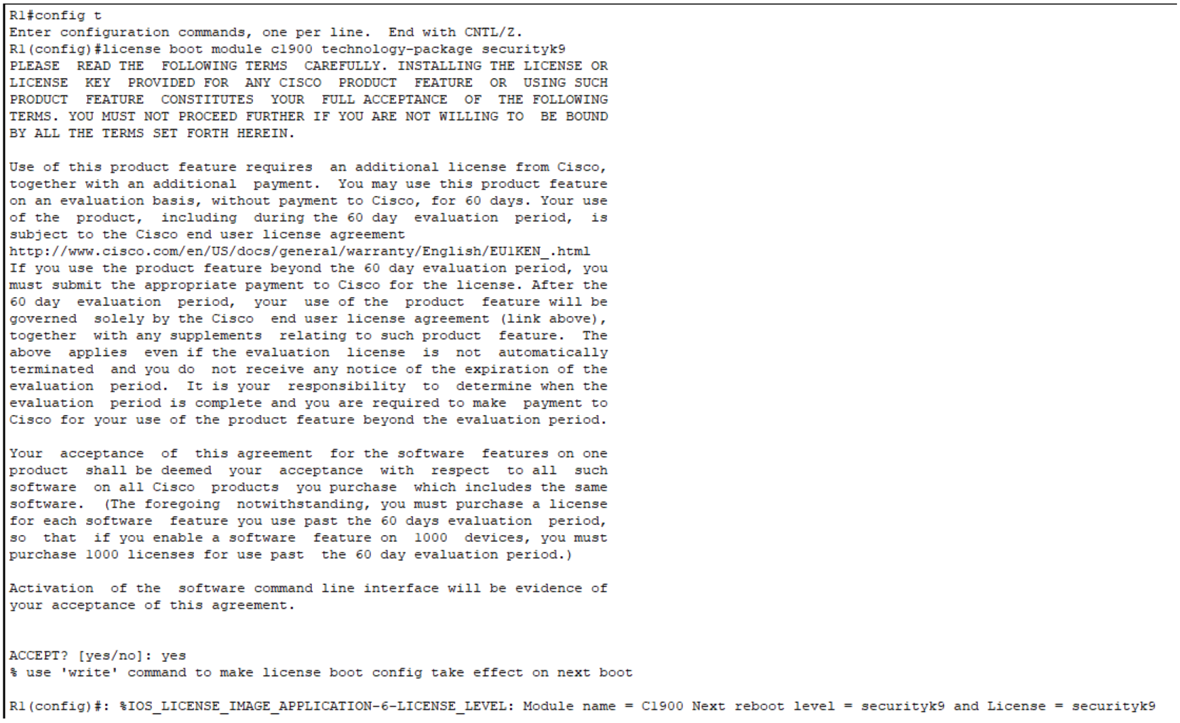
We ran the "show version" on Privilege 1 on Zero Level, and we got the following information https://www.oreilly.com/library/view/hardening-cisco-routers/0596001665/ch04.html



```
ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 2 minutes, 51 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX15241P4M


Technology Package License Information for Module:'c1900'

----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      disable       None          None
data          disable       None          None

Configuration register is 0x2102
```

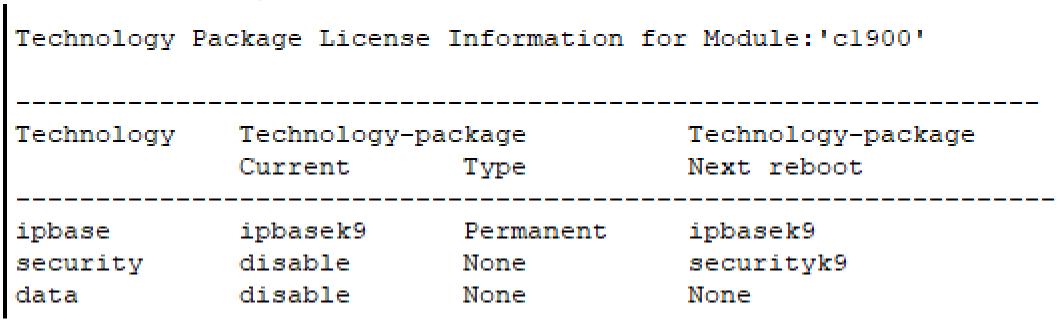
As we can observe, it tells us that the "current **security** package" is disabled. The type is **none** indicating that no valid license for the security package is currently installed. The "Next Reboot" field also having **None** tells us that unless the technology package is installed, security package will remain disabled.

Thus, I will now try enabling the Security Package.
Going in Configuration Mode (Level 15 Privilege)



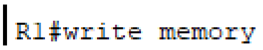
```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

R1(config)#: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = C1900 Next reboot level = securityk9 and License = securityk9
```

As we can see it will get enabled in next reboot



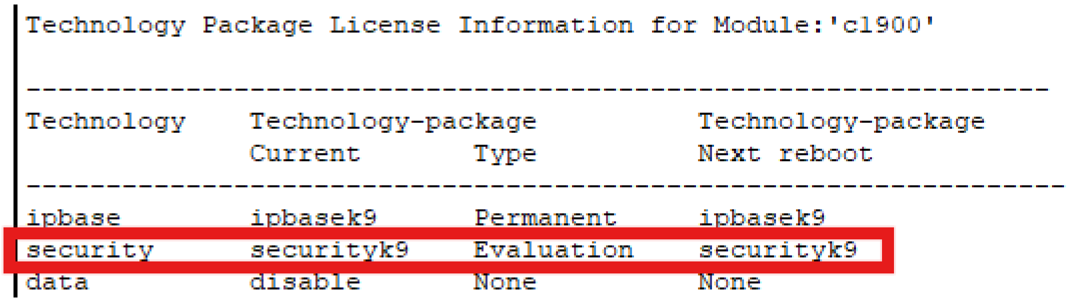
```
Technology Package License Information for Module:'c1900'

-------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
--------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      disable       None           securityk9
data          disable       None           None
```

Before we reboot, we must make sure that Router actually remembers the said security packet.



```
R1#write memory
```

After rebooting with “ R1# Reload”



```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      securityk9    Evaluation     securityk9
data          disable       None           None
```

The **securityk9 license** on Cisco routers enables a range of advanced security features designed to protect network communications and infrastructure. It provides **VPN capabilities**, including IPSec and SSL VPN, allowing for secure data transmission over public networks. The license also includes **stateful firewall services**, which offer in-depth traffic inspection to guard against unauthorized access. Additionally, it supports **encryption features like AES and 3DES**, ensuring data privacy with secure communications. Other key capabilities include Intrusion Prevention System (IPS) on some models, which detects and mitigates malicious threats, as well as secure connectivity protocols such as IKEv2 and SSL/TLS encryption for enhanced security. These features are essential for building robust, secure networks in enterprise environments.

Typical Syntax:
license boot module <module-name> technology-package securityk9

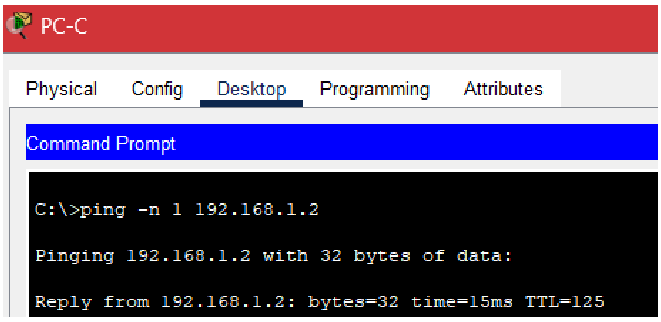
license boot: This part of the command tells the router to boot with a specific license or technology package enabled.
module c1900: Specifies the hardware module (in this case, a Cisco 1900 series router) on which the license is being applied.
technology-package securityk9: Specifies the technology package you want to enable. In this case, it's the securityk9 package, which includes advanced security features like VPN, firewall, and encryption.

Thus, that's we ran:
license boot module c1900 technology-package securityk9

modulename is just given above the table for the security package information when we run "show version"

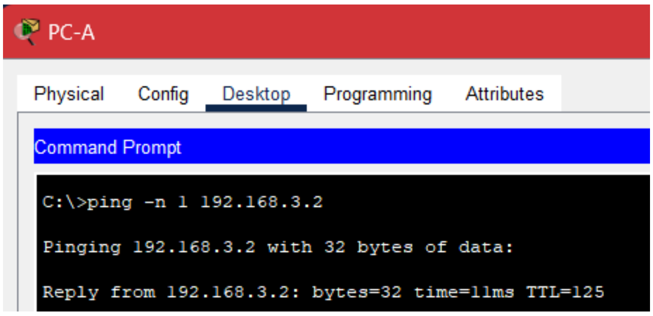
2. Verify network connectivity
   a. Ping from **PC-C** to **PC-A**. The ping should be successful

PC-C: 192.168.3.2
PC-A: 192.168.1.2



```
C:\>ping -n 1 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=15ms TTL=125
```

b. Ping from **PC-A** to **PC-C**. The ping should be successful.



```
C:\>ping -n 1 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=11ms TTL=125
```

3. Create an IOS IPS configuration directory in flash.

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

Creating a directory in flash TO store IPS signatures.

```
R1#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir
```

Confirming whether it actually exists or not:

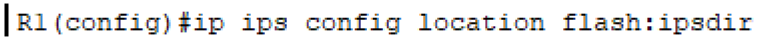
```
R1#
%SYS-5-CONFIG_I: Configured from console by console
dir flash:
Directory of flash0:/

    3  -rw-    33591768          <no date>  c1900-universalk9-mz.SPA.151-4.M4.bin
    4  drw-         192          <no date>  ipsdir
    2  -rw-       28282          <no date>  sigdef-category.xml
    1  -rw-      227537          <no date>  sigdef-default.xml

255744000 bytes total (221441339 bytes free)
```

4. Configure the IPS signature storage location.

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

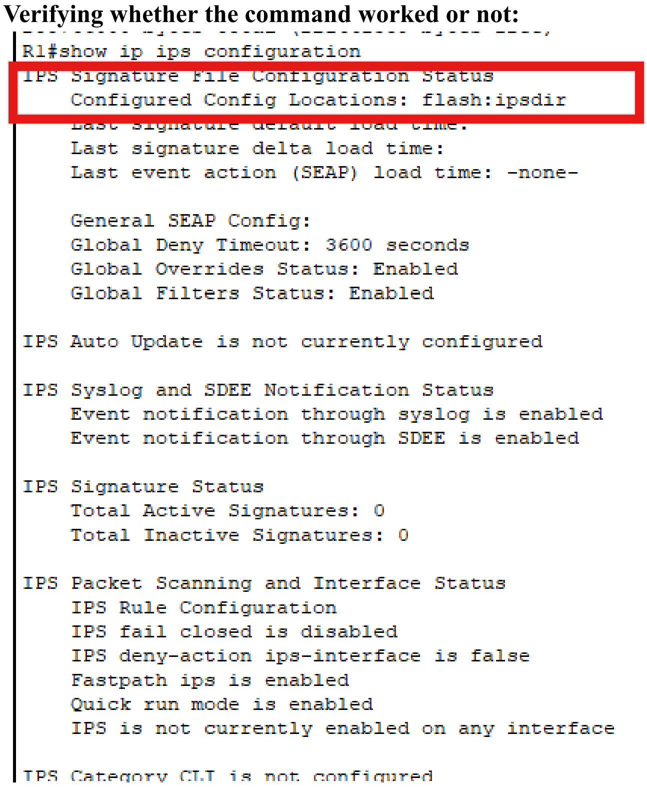
   ```
   R1(config)#ip ips config location flash:ipsdir
   ```

Configuring to store IPS Signatures in "ipsdir"



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

Verifying whether the command worked or not:

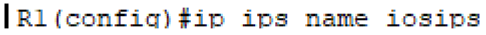


```
R1#show ip ips configuration
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 0
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    IPS is not currently enabled on any interface

IPS Category CLI is not configured
```

5. 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**.

Running:

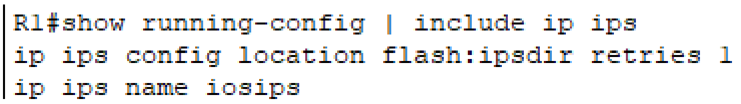


```
R1(config)#ip ips name iosips
```

Command Breakdown

- ip ips: This is the base command that indicates you are configuring the IPS feature.
- name: This keyword specifies that you are assigning a name to the IPS policy.
- iosips: This is the name you are assigning to the IPS policy. It can be any valid identifier as per Cisco's naming conventions.

Verifying:

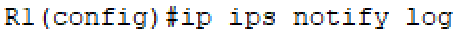


```
R1#show running-config | include ip ips
ip ips config location flash:ipsdir retries 1
ip ips name iosips
```

6. 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.

   a. Enable syslog if it is not enabled.

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



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

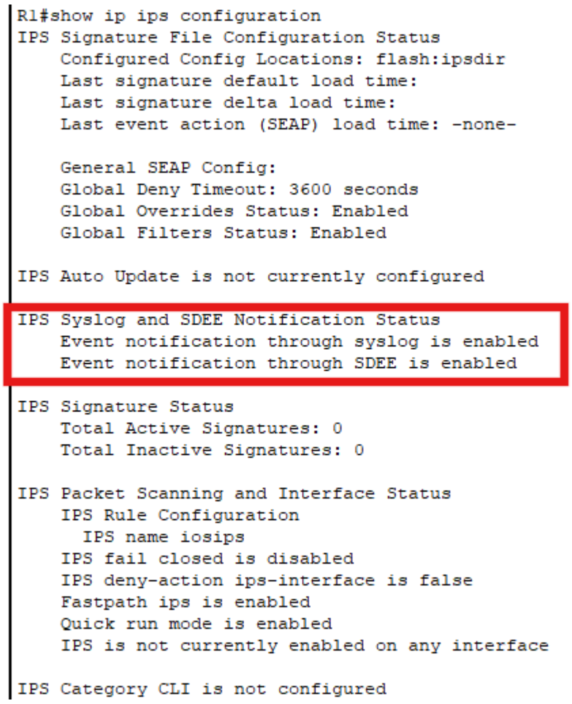
Command Explanation:
This command configures the Intrusion Prevention System (IPS) to log notifications whenever an event occurs that matches the IPS rules. This helps in monitoring and auditing security events.

Verification Methods:

- show ip ips configuration
  show ip ips name iosips
- show log (after purposely having the traffic that can trigger go through)
- show ip ips events (to see ips related events)

It was apparently configured and enabled from before but we still ran the command.

Verification:



```
R1#show ip ips configuration
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 0
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    IPS is not currently enabled on any interface

IPS Category CLI is not configured
```

   b. If necessary, use the **clock set** command from privileged EXEC mode to reset the clock.

Checking the Clock:

```
R1#show clock
*0:32:34.796 UTC Mon Mar 1 1993
```

Resetting the Clock:

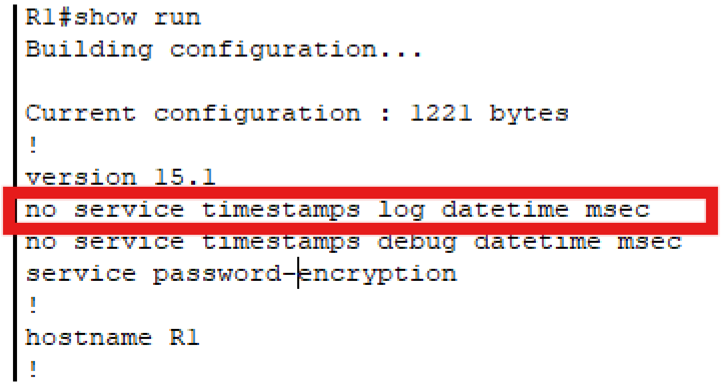
```
R1#clock set 10:30:00 Oct 10 2024
```

Checking the new Clock:

```
R1#show clock
10:30:2.406 UTC Thu Oct 10 2024
```

c. Verify that the timestamp service for logging is enabled on the router using the **show run** command.

Verifying that the timestamp service for logging is enabled on the router using the show run command.



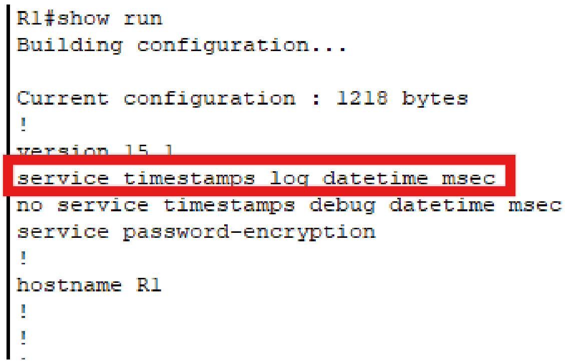
```
R1#show run
Building configuration...

Current configuration : 1221 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
```

As we can observe, it is disabled.

Enabling:

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

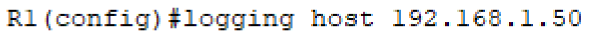
Verification:



```
R1#show run
Building configuration...

Current configuration : 1218 bytes
!
version 15.1
service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1
!
!
```

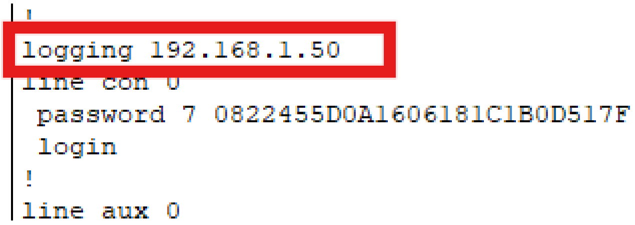
Before we were getting "no service timestamps log datetime msec" and now we are getting "service timestamps log datetime msec". This tells us that timestamp service for logging has now successfully been enabled.

d. Send log messages to the syslog server at IP address 192.168.1.50



```
R1(config)#logging host 192.168.1.50
```

when doing "running-config" you should see an output which says this

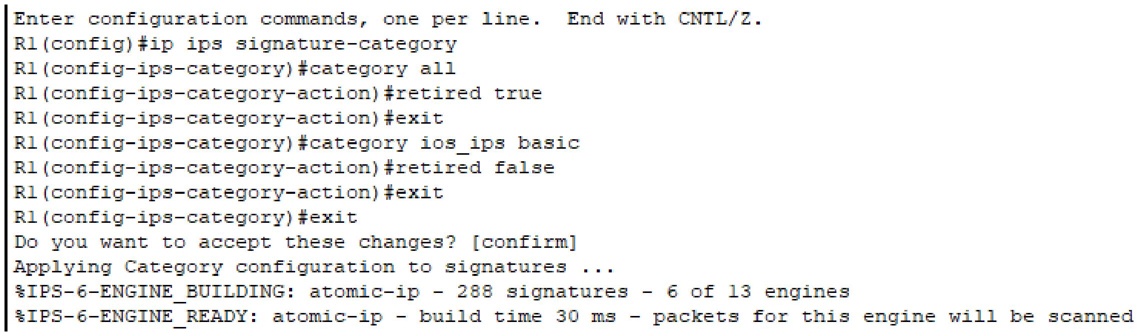


```
!
logging 192.168.1.50
line con 0
 password 7 0822455D0A1606181C1B0D517F
 login
!
line aux 0
```

This verifies that it did that successfully.

7. 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.



```
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned
```

Explaining Commands:
ip ips signature-catogory
This command enters the IPS signature category configuration mode, where you can specify actions related to specific signature categories.

category all
This command selects all signature categories for configuration. By targeting all categories, you can apply a uniform action (retirement) to every signature.

retired true
This command marks all signatures in the selected category (all signatures) as retired. Retiring signatures means they will no longer be used to analyze traffic, which reduces the load on the IPS and minimizes false positives.

We then exit the current configuration

category ios_ips basic
This command selects the "ios_ips basic" category for configuration. This category typically contains fundamental signatures that protect against common threats.

retired false
This command unretired the basic category, enabling the signatures within it to be active again. This ensures that the IPS continues to provide protection against essential threats.

We then exit the current configuration and save it

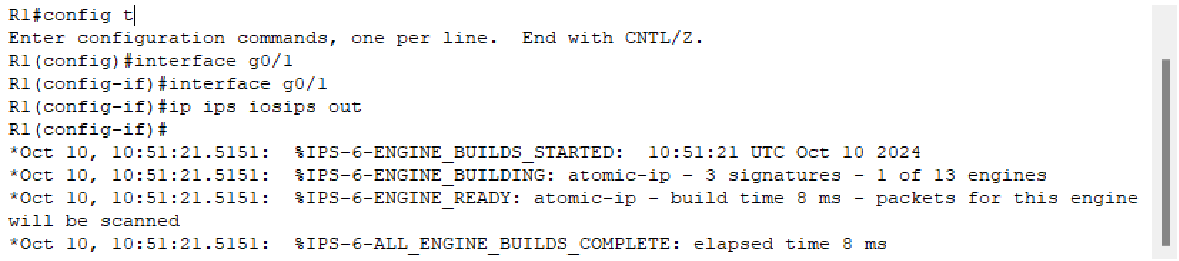
So basically, we optimized our IOS IPS for current threats, focusing on only relevant essential signatures **while reducing unnecessary overhead**.
This configuration process is vital for maintaining an effective and efficient intrusion prevention system that can adapt to the evolving security landscape.

Summary:
The purpose of configuring IOS IPS to use signature categories includes improving the security posture by focusing on relevant threats and reducing noise from less critical alerts. This helps enhance network security without overwhelming monitoring systems. Additionally, managing signature updates is important, as retiring outdated or irrelevant signatures keeps the IPS efficient by processing only active and necessary ones. Unretiring the "ios_ips basic" category ensures that essential signatures remain active, providing protection against common vulnerabilities and exploits.

8. 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.



```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/1
R1(config-if)#interface g0/1
R1(config-if)#ip ips iosips out
R1(config-if)#
*Oct 10, 10:51:21.5151:  %IPS-6-ENGINE_BUILDS_STARTED:  10:51:21 UTC Oct 10 2024
*Oct 10, 10:51:21.5151:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Oct 10, 10:51:21.5151:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine
will be scanned
*Oct 10, 10:51:21.5151:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
```

Explaining:
ip ips iosips out
This command enables the IOS IPS (Intrusion Prevention System) feature on the interface we selected beforehand. It specifies that the IPS should inspect traffic going *out* of the GigabitEthernet 0/1 interface using the iosips signature set.

Summary of Log Output Explanation
The log messages indicate the activity of the IPS engine following the command to enable it on the interface.
The process starts with the message **%IPS-6-ENGINE_BUILDS_STARTED**, signaling that the IPS engine is building signatures for inspection.
The message **%IPS-6-ENGINE_BUILDING** reveals that the atomic-ip engine is constructing three signatures as part of the total thirteen engines available.
Once the build is complete, the **%IPS-6-ENGINE_READY** message confirms that the engine is prepared to scan packets, taking just 8 milliseconds for the process.
Finally, **%IPS-6-ALL_ENGINE_BUILDS_COMPLETE** indicates that all engines are ready, confirming that the IPS is fully operational.

What it achieves successfully:

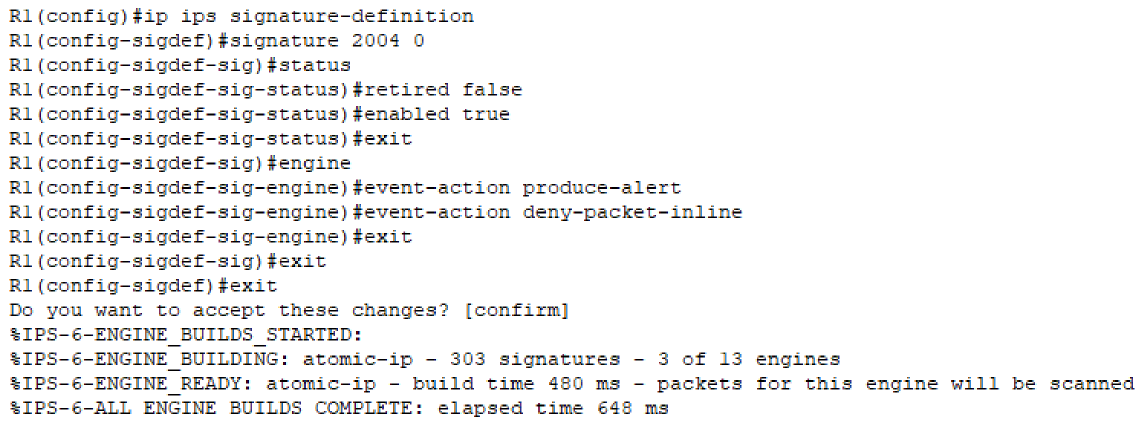
1. **Traffic Inspection:** By enabling the IPS on the specified interface, all outbound traffic from that interface will be analyzed for potential security threats based on the defined signature set.
2. **Real-Time Protection:** The IPS can actively block or alert on detected threats, providing real-time protection against attacks such as network intrusions, denial-of-service attacks, and exploitation of vulnerabilities.
3. **Efficient Signature Management:** The log confirms that the IPS is using its signature engines effectively, optimizing the scanning process to protect the network without significant delays.

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.



```
R1(config)#ip ips signature-definition
R1(config-sigdef)#signature 2004 0
R1(config-sigdef-sig)#status
R1(config-sigdef-sig-status)#retired false
R1(config-sigdef-sig-status)#enabled true
R1(config-sigdef-sig-status)#exit
R1(config-sigdef-sig)#engine
R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#event-action deny-packet-inline
R1(config-sigdef-sig-engine)#exit
R1(config-sigdef-sig)#exit
R1(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be scanned
%IPS-6-ALL ENGINE BUILDS COMPLETE: elapsed time 648 ms
```

Explanation:
ip ips signature-defination
we are defining a new signature here, “ip” tells us we are working with ip-related configurations.

signature 2004 0
This command specifies the signature you want to configure.
The first number (2004) refers to the specific signature ID you are working with, and the second number (0) is typically used to indicate the signature revision or sub-type.

status
This command allows you to enter the status configuration mode for the specified signature, where you can view and set its operational status.

retired false
We are telling the signature should become part of the configuration, but sadly it’s still not being actively used in monitoring traffic, thus we do this

enabled true
The signature becomes fully operational. The IPS can now actively analyze incoming traffic for matches against the signature, and it can respond to any detected threats.

We then exit out of the current configuration
engine
This command enters the engine configuration mode for the specified signature, **allowing you to define how the IPS should respond to detected threats.**

event-action produce-alert
This command configures the signature to generate an alert when the signature is matched, allowing network administrators to be notified of potential threats.

event-action deny-packet-inline
This command configures the IPS to block packets that match the signature in real-time, providing immediate protection against threats.

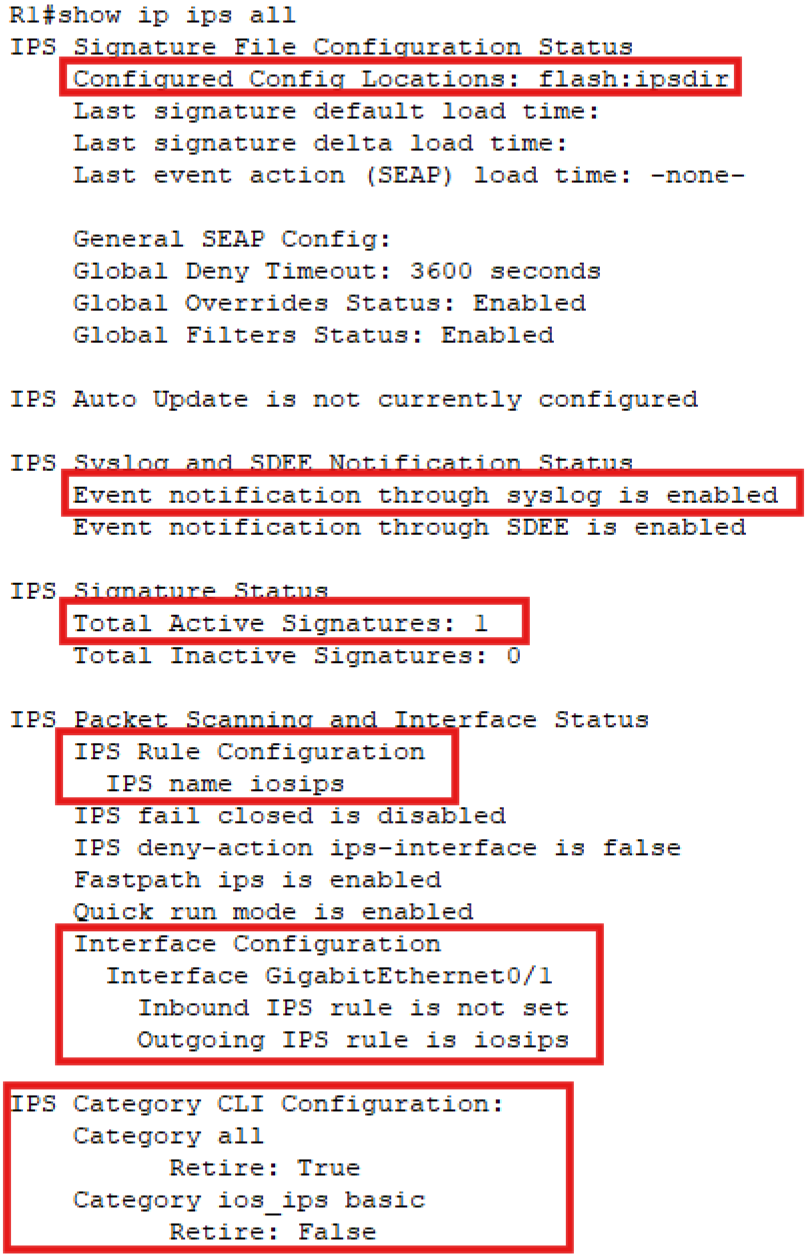
Exiting Engine Configuration:
This command exits the engine configuration mode.

we then exit and confirm to save the configuration.

2. 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?

All the configuration thus far!



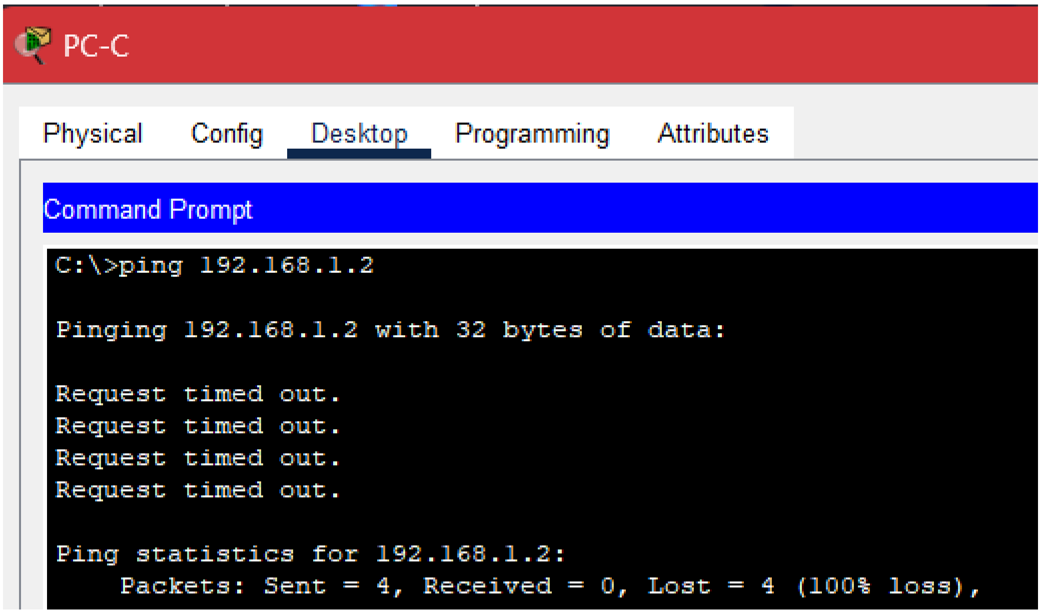
```
R1#show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface GigabitEthernet0/1
        Inbound IPS rule is not set
        Outgoing IPS rule is iosips

IPS Category CLI Configuration:
    Category all
          Retire: True
    Category ios_ips basic
          Retire: False
```

,

G0/1 outbound.

3. Verify that IPS is working properly.
   a. From **PC-C**, attempt to ping **PC-A**. Were the pings successful? Explain.

Results: FAILED

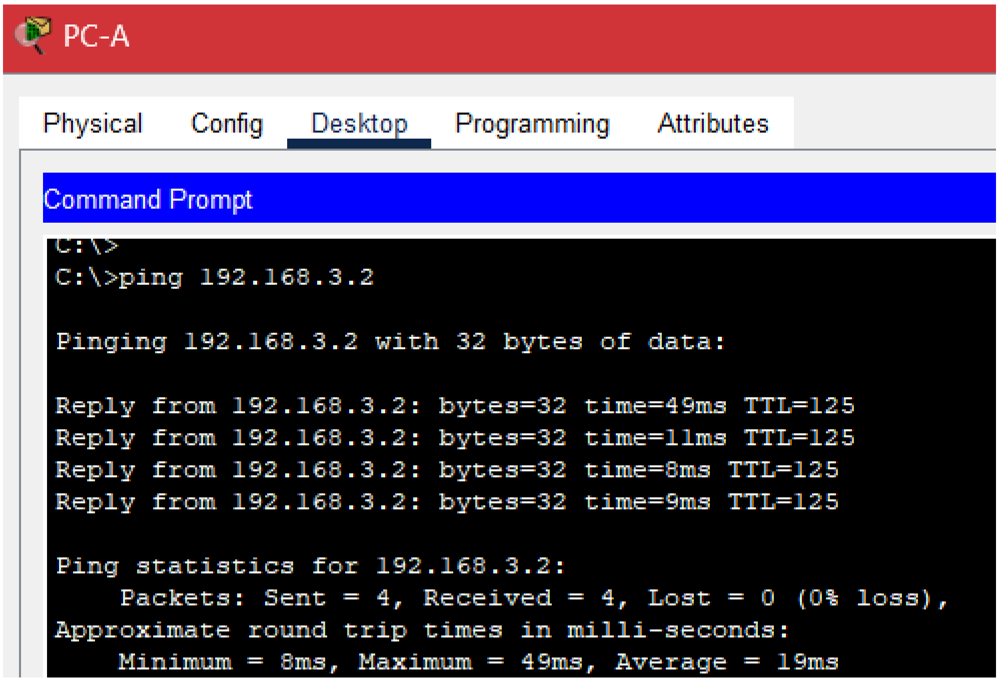


```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Explanation:
This result makes sense cause we specifically set the IPS (Intrusion Prevention System) rule for the event-action of an echo request to specifically set to **fail** by doing the command "denypacket-inline"

   b. From **PC-A**, attempt to ping **PC-C**. Were the pings successful? Explain.

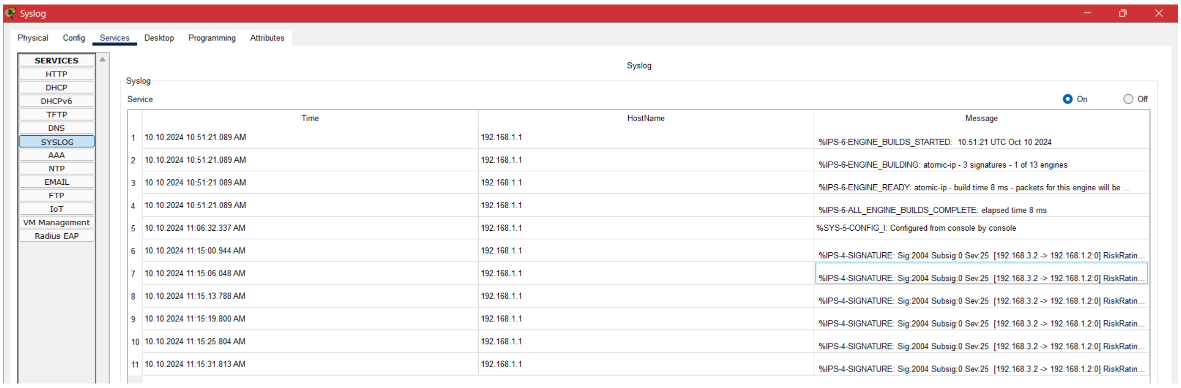
Results: SUCCESS



```
C:\>
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=49ms TTL=125
Reply from 192.168.3.2: bytes=32 time=11ms TTL=125
Reply from 192.168.3.2: bytes=32 time=8ms TTL=125
Reply from 192.168.3.2: bytes=32 time=9ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 49ms, Average = 19ms
```

Explanation:
The result makes sense cause our IPS-rule doesn't cover "echo-reply" (different from echo-request!).
When PC-A pings PC-C, PC-C should and does respond with an echo reply.

4. View the syslog messages.
   a. Click the **Syslog** server.
   b. Select the **Services** tab.
   c. In the navigation menu, select **SYSLOG** to view the log file.



Syslog

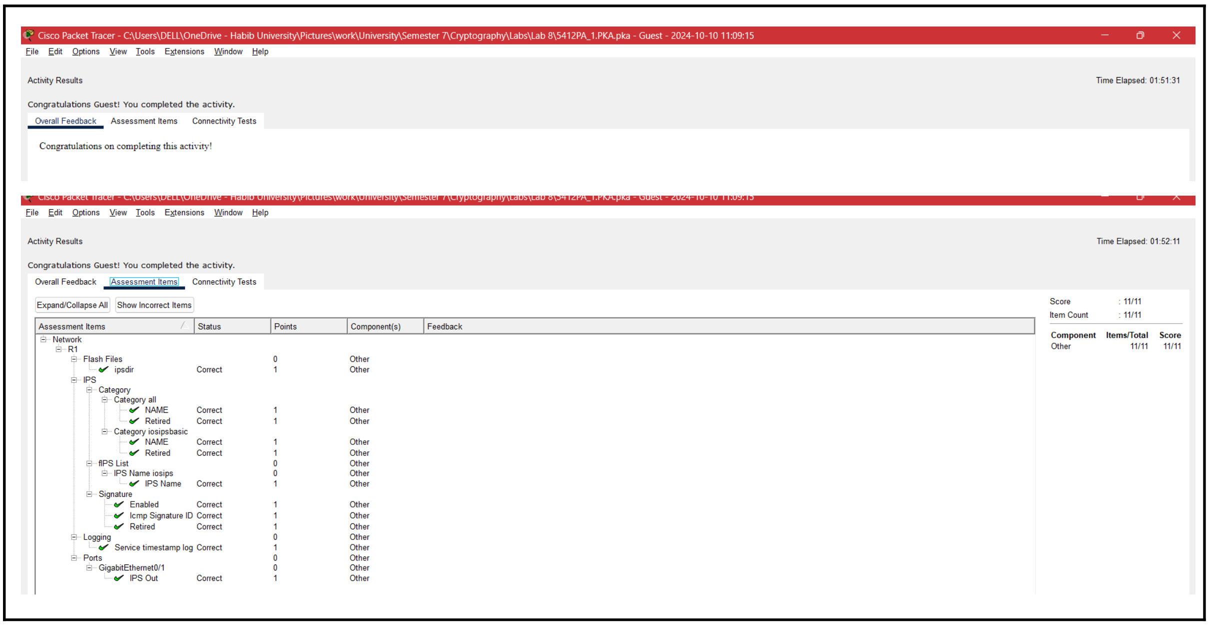
Service ● On ○ Off

	Time	HostName	Message
1	10.10.2024 10:51:21.089 AM	192.168.1.1	%IPS-6-ENGINE_BUILDS_STARTED: 10:51:21 UTC Oct 10 2024
2	10.10.2024 10:51:21.089 AM	192.168.1.1	%IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
3	10.10.2024 10:51:21.089 AM	192.168.1.1	%IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be ...
4	10.10.2024 10:51:21.089 AM	192.168.1.1	%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
5	10.10.2024 11:06:32.337 AM	192.168.1.1	%SYS-5-CONFIG_I: Configured from console by console
6	10.10.2024 11:15:00.944 AM	192.168.1.1	%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.3.2 -> 192.168.1.2:0] RiskRatin...
7	10.10.2024 11:15:06.048 AM	192.168.1.1	%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.3.2 -> 192.168.1.2:0] RiskRatin...
8	10.10.2024 11:15:13.788 AM	192.168.1.1	%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.3.2 -> 192.168.1.2:0] RiskRatin...
9	10.10.2024 11:15:19.800 AM	192.168.1.1	%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.3.2 -> 192.168.1.2:0] RiskRatin...
10	10.10.2024 11:15:25.804 AM	192.168.1.1	%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.3.2 -> 192.168.1.2:0] RiskRatin...
11	10.10.2024 11:15:31.813 AM	192.168.1.1	%IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 [192.168.3.2 -> 192.168.1.2:0] RiskRatin...

5. Check results.

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

PROOF OF COMPLETION



Cisco Packet Tracer - C:\Users\DELL\OneDrive - Habib University\Pictures\work\University\Semester 7\Cryptography\Labs\Lab 8\5412PA_1.PKA.pka - Guest - 2024-10-10 11:09:15

Activity Results

Time Elapsed: 01:51:31

Congratulations Guest! You completed the activity.

Congratulations on completing this activity!

Cisco Packet Tracer - C:\Users\DELL\OneDrive - Habib University\Pictures\work\University\Semester 7\Cryptography\Labs\Lab 8\5412PA_1.PKA.pka - Guest - 2024-10-10 11:09:15

Activity Results

Time Elapsed: 01:52:11

Congratulations Guest! You completed the activity.

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R1				
Flash Files		0	Other	
✓ ipsdir	Correct	1	Other	
IPS				
Category				
Category all				
✓ NAME	Correct	1	Other	
✓ Retired	Correct	1	Other	
Category iosipsbasic				
✓ NAME	Correct	1	Other	
✓ Retired	Correct	1	Other	
fIPS List		0	Other	
IPS Name iosips		0	Other	
✓ IPS Name	Correct	1	Other	
Signature				
✓ Enabled	Correct	1	Other	
✓ Icmp Signature ID	Correct	1	Other	
✓ Retired	Correct	1	Other	
Logging		0	Other	
✓ Service timestamp log	Correct	1	Other	
Ports		0	Other	
GigabitEthernet0/1		0	Other	
✓ IPS Out	Correct	1	Other	

Score : 11/11
Item Count : 11/11

Component	Items/Total	Score
Other	11/11	11/11

Assessment Rubric

Lab 08

Configuring IOS Intrusion Prevention System (IPS)

Name: Syed Asghar Abbas Zaidi	**Student ID: 07201**

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.