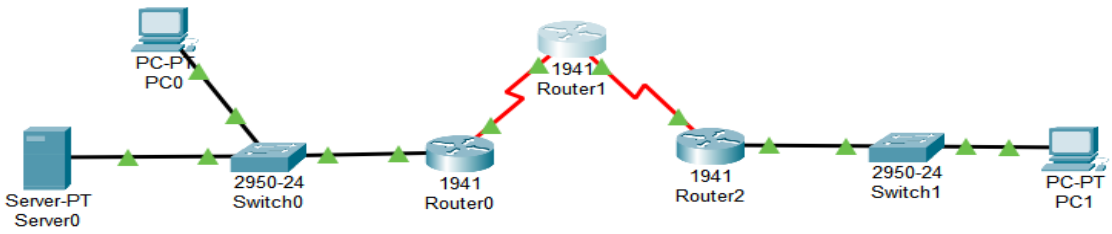
Experiment -5 **Date:25/08/2025**

Configure IDS/IPS in Cisco Packet Tracer

NetworkTopology



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

Objectives:

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

User Access Authentication

Step-1

```
Router#en
Router#conf t
Enter configuration commands, one per line.  End with
Router(config)#username xxxx secret yyyy
Router(config)#aaa new
Router(config)#aaa new-model
Router(config)#aaa authentication?
authentication
Router(config)#aaa authentication login?
login
Router(config)#aaa authentication login default?
default  WORD
Router(config)#aaa authentication login default local
Router(config)#line console 0
Router(config-line)#login authentication?
authentication
Router(config-line)#login authentication default
Router(config-line)#exit
Router(config)#
```

Step-2 Click on Router1

#enable

#show version

#conf t

#license boot module c1900 technology-package securityk9

#yes

#end

```
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#router
Translating "router"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################ [OK]
Smart Init is enabled
smart init is sizing iomem
                  TYPE       MEMORY_REQ
            HWIC Slot 0      0x00200000      Onboard devices &
           buffer pools      0x01E8F000
------------------------------------------------
                 TOTAL:      0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/512Mb]
```

```
             Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

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)

Press RETURN to get started!
```

```
User Access Verification

Username: xxxx
Password:
Router>show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
ciscol941 uptime is 58 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

Router>en
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
ciscol941 uptime is 1 minutes, 27 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
```

Step-3

In R0

```
Router(config)#int g0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#int s0/0/0
Router(config-if)#ip addr 10.1.1.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#end
```

```
Router(config)#ip route 192.168.3.0 255.255.255.0 10.1.1.2
```

In R1

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip address 10.1.1.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#clock rate 64000
This command applies only to DCE interfaces
Router(config-if)#int s0/0/1
Router(config-if)#ip addr 10.2.2.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#clock rate 64000
This command applies only to DCE interfaces
Router(config-if)#end
```

```
Router(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
Router(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.1
```

In R2

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g0/0
Router(config-if)#ip addr 192.168.3.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int s0/0/0
Router(config-if)#ip addr 10.2.2.1 255.255.255.252
Router(config-if)#no shut
Router(config-if)#end
```

```
Router(config)#ip route 192.168.1.0 255.255.255.0 10.2.2.2
```

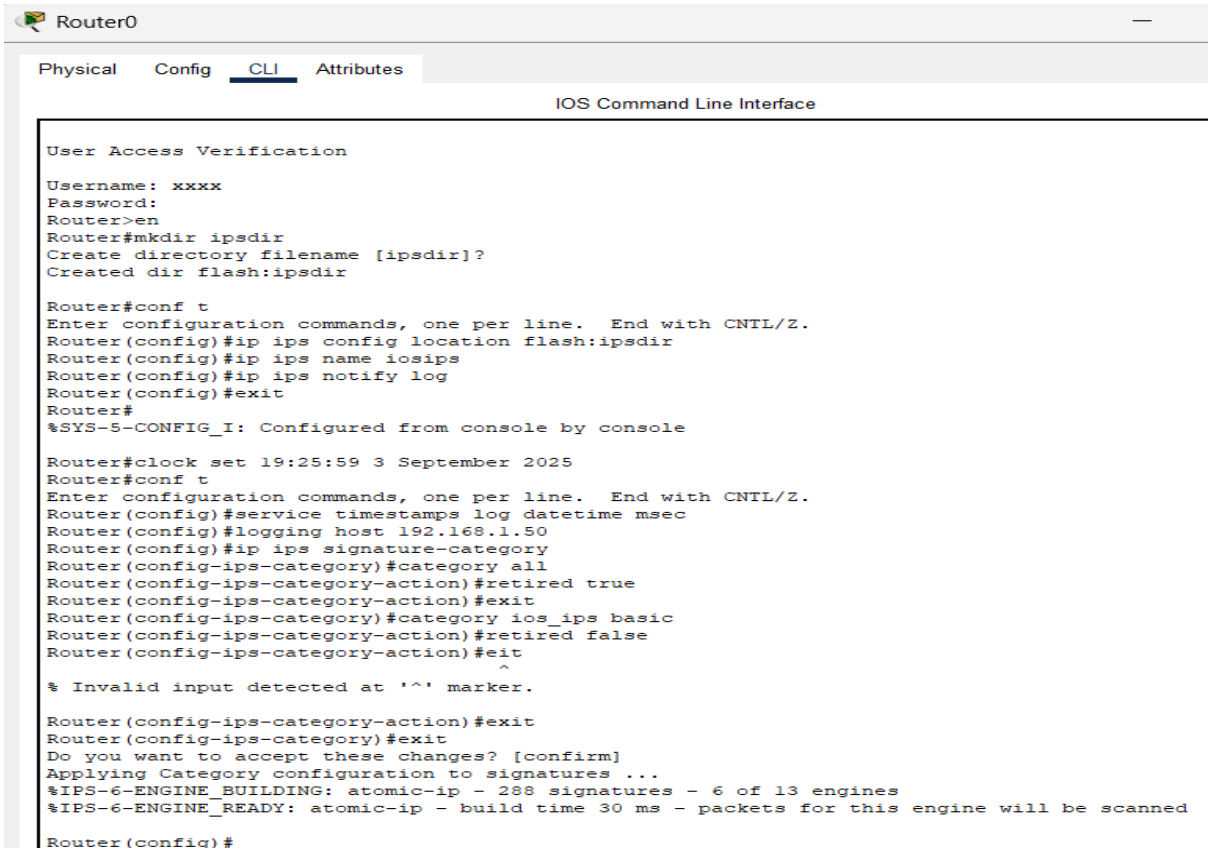
Click on PC0 Ping PC1 IP address

```
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=18ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms 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 = 2ms, Maximum = 18ms, Average = 10ms

C:\>tracert 192.168.3.2

Tracing route to 192.168.3.2 over a maximum of 30 hops:

  1    0 ms       0 ms       0 ms       192.168.1.1
  2    4 ms       0 ms       0 ms       10.1.1.2
  3    7 ms       0 ms       0 ms       10.2.2.1
  4    1 ms       0 ms       4 ms       192.168.3.2

Trace complete.
```

Step-4 Click on PC1 ping PC0 IP address

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=17ms TTL=125
Reply from 192.168.1.2: bytes=32 time=6ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=10ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 17ms, Average = 8ms
```

Step-5 Click on R1




```
User Access Verification

Username: xxxx
Password:
Router>en
Router#mkdir ipsdir
Create directory filename [ipsdir]?
Created dir flash:ipsdir

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip ips config location flash:ipsdir
Router(config)#ip ips name iosips
Router(config)#ip ips notify log
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#clock set 19:25:59 3 September 2025
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service timestamps log datetime msec
Router(config)#logging host 192.168.1.50
Router(config)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#eit
                                   ^
% Invalid input detected at '^' marker.

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

Router(config)#
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned

Router(config)#int g0/0
Router(config-if)#ip ips iosips out
Router(config-if)#
*Sep 03, 19:29:22.2929:  %IPS-6-ENGINE_BUILDS_STARTED:  19:29:22 UTC Sep 03 2025
*Sep 03, 19:29:22.2929:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Sep 03, 19:29:22.2929:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine
will be scanned
*Sep 03, 19:29:22.2929:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
Router(config-if)#signature 2004 0
                  ^
% Invalid input detected at '^' marker.

Router(config-if)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#exit
Router(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

Router(config)#end
Router#
*Sep 03, 19:32:37.3232: SYS-5-CONFIG_I: Configured from console by console
*Sep 03, 19:32:37.3232:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.50 port 514
started - CLI initiatedshow 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
 --More-- |
```

Step-6 Ping PC1

(Now, the request connection should be timeout the packets between the devices should deny the packets from the given IP address. This ping should fail. This PC2 the IPS rule for event-action of an echo request was set to deny-packet- inline.)

From pc1,

```
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),
```

Step-7 Ping PC0

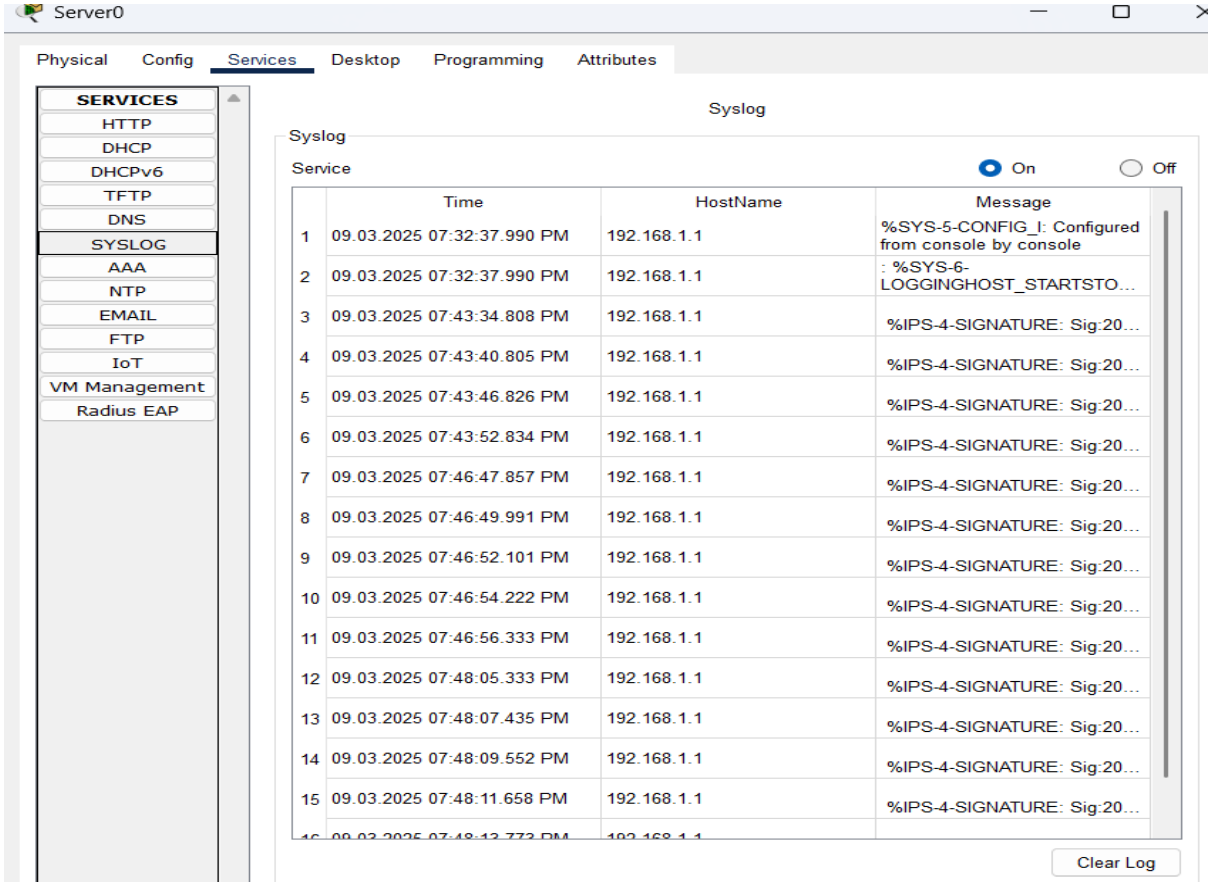
(Now, the request should be successful….)

From pc0

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=11ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
Reply from 192.168.1.2: bytes=32 time=5ms TTL=128
Reply from 192.168.1.2: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 11ms, Average = 6ms

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=24ms TTL=125
Reply from 192.168.3.2: bytes=32 time=16ms TTL=125
Reply from 192.168.3.2: bytes=32 time=11ms TTL=125
Reply from 192.168.3.2: bytes=32 time=11ms 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 = 11ms, Maximum = 24ms, Average = 15ms
```

```
Router>en
Router#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Router#ping 192.168.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/9/11 ms

Router#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Step-8 Check syslog (in server)



RESULT:

The IDS/IPS is configured successfully in cisco packet tracer.