Université Abdelmalek Essaâdi

Faculté des Sciences et Techniques-Tanger

Département Génie Informatique

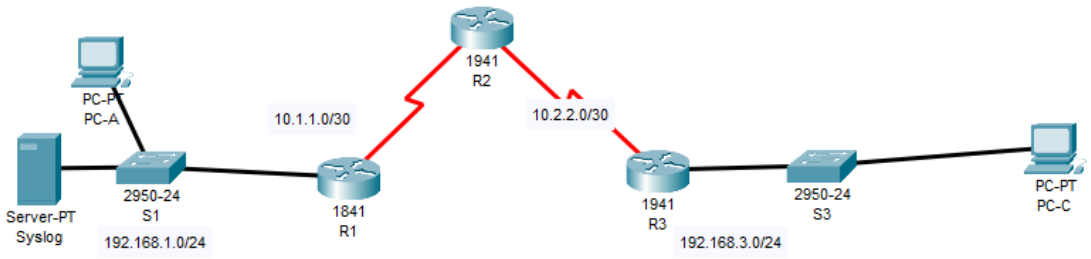
Cryptographie-Sécurité Services

LAB-IPS

Réalisé Par :

Yossra safi chetouan

LAB: Configure IOS Intrusion Prevention System (IPS) Using CLI



Part 1: Enable IOS IPS

Step 1: Verify network connectivity

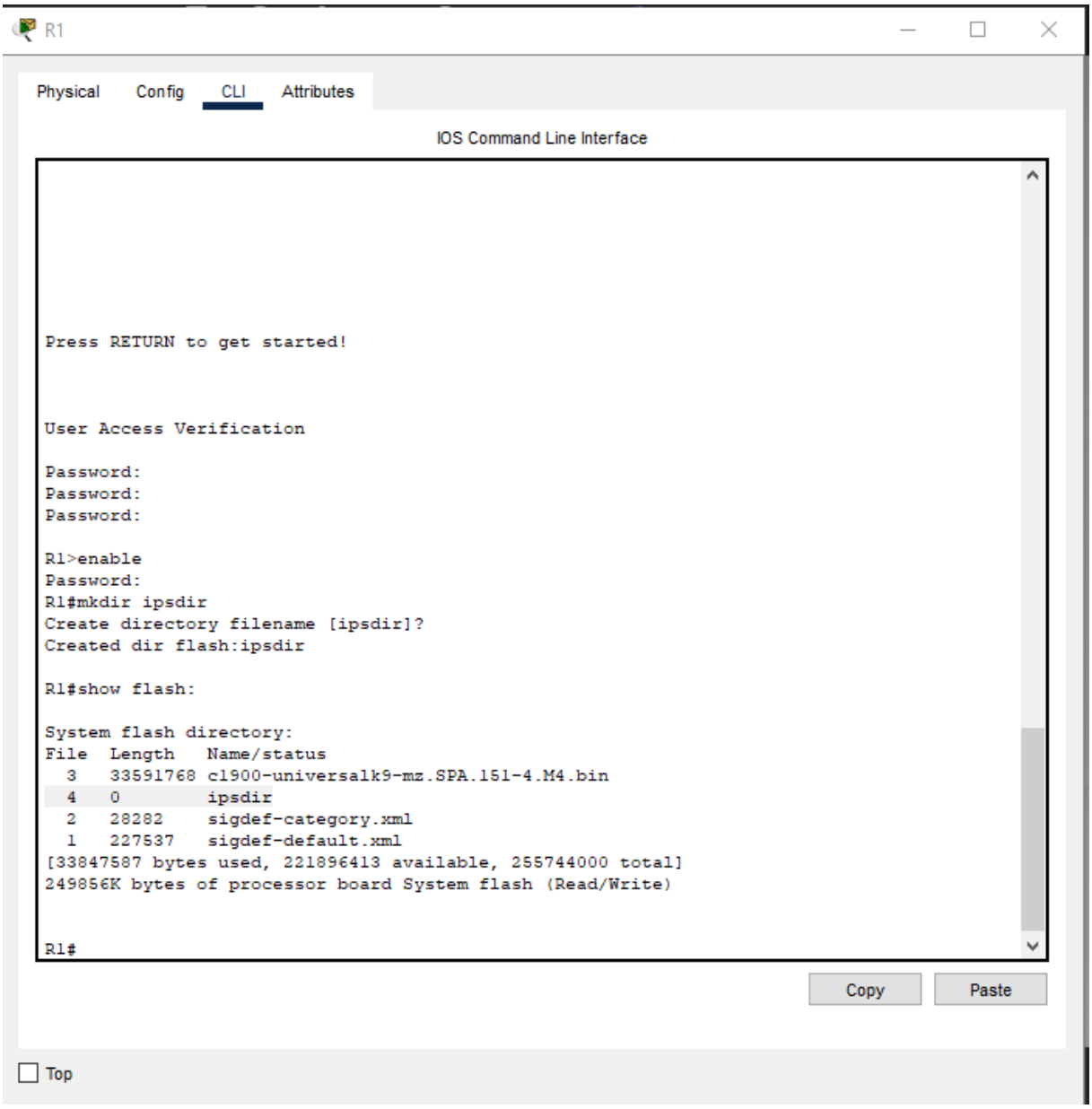
a. Ping from PC-C to PC-A. The ping should be successful:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC-C	PC-A	ICMP		0.000	N	0	(edit)

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

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC-A	PC-C	ICMP		0.000	N	0	(edit)

Step 2: Create an IOS IPS configuration directory in flash.



Step 3: Configure the IPS signature storage location.

```
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#
Router(config)#ip ips config location flash:ipsdir
Router(config)#
```

Step 4: Create an IPS rule.

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

Step 5: Enable logging.

a. Enable syslog if it is not enabled.

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

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

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

Router#
Router#clock set 10:20:00 15 april 2021
Router#
Router#
```

c.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#service timestamps log datetime msec
Router(config)#
Router(config)#
```

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

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

Step 6: Configure IOS IPS to use the signature categories.

```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
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)#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)#
```

Step 7: Apply the IPS rule to an interface.

```
Router(config)#
Router(config)#
Router(config)#interface fa0/0
Router(config-if)#ip ips iosips out
Router(config-if)#
```

Part 2: Modify the Signature

Step 1: Change the event-action of a signature.

```
Router(config)#
Router(config)#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)#
```

Step 2: Use show commands to verify IPS.

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#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 FastEthernet0/0
        Inbound IPS rule is not set
        Outgoing IPS rule is iosips

IPS Category CLI Configuration:
    Category all
```

Copy Paste

Top

Step 3: Verify that IPS is working properly.

Ping PC-C vers PC-A

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Failed	PC-C	PC-A	ICMP		0.000	N	0	(edit)

Les pings devraient échouer. Cela est dû au fait que la règle IPS pour l'action-événement d'une demande d'écho a été définie sur "deny-packet-inline".

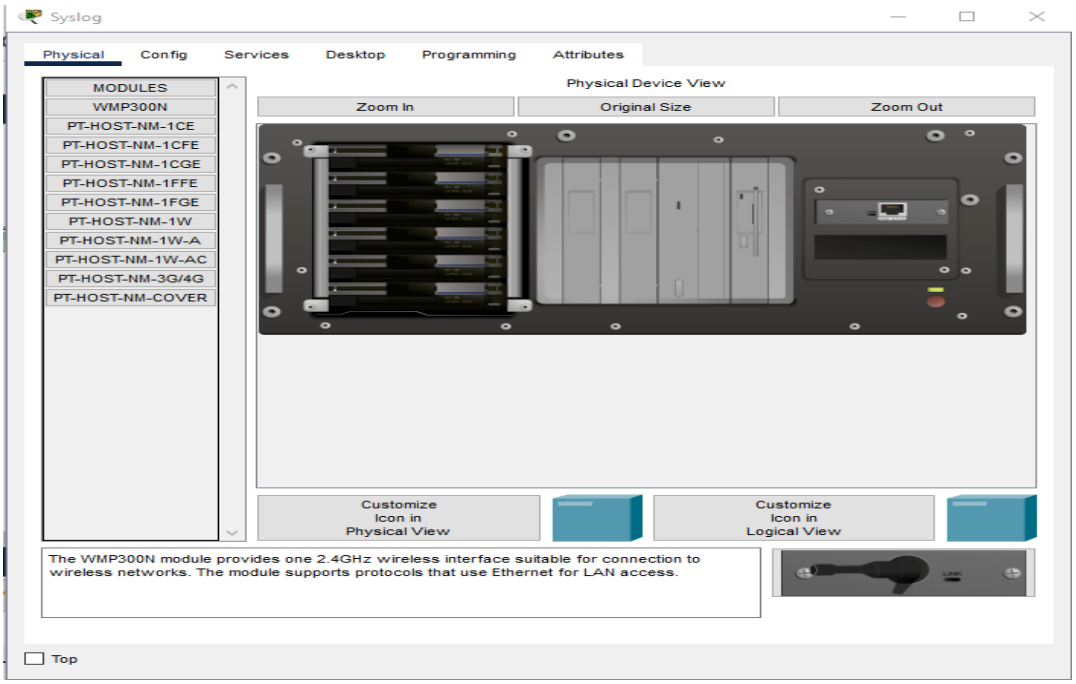
Ping PC-A vers PC-C

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC-A	PC-C	ICMP		0.000	N	0	(edit)

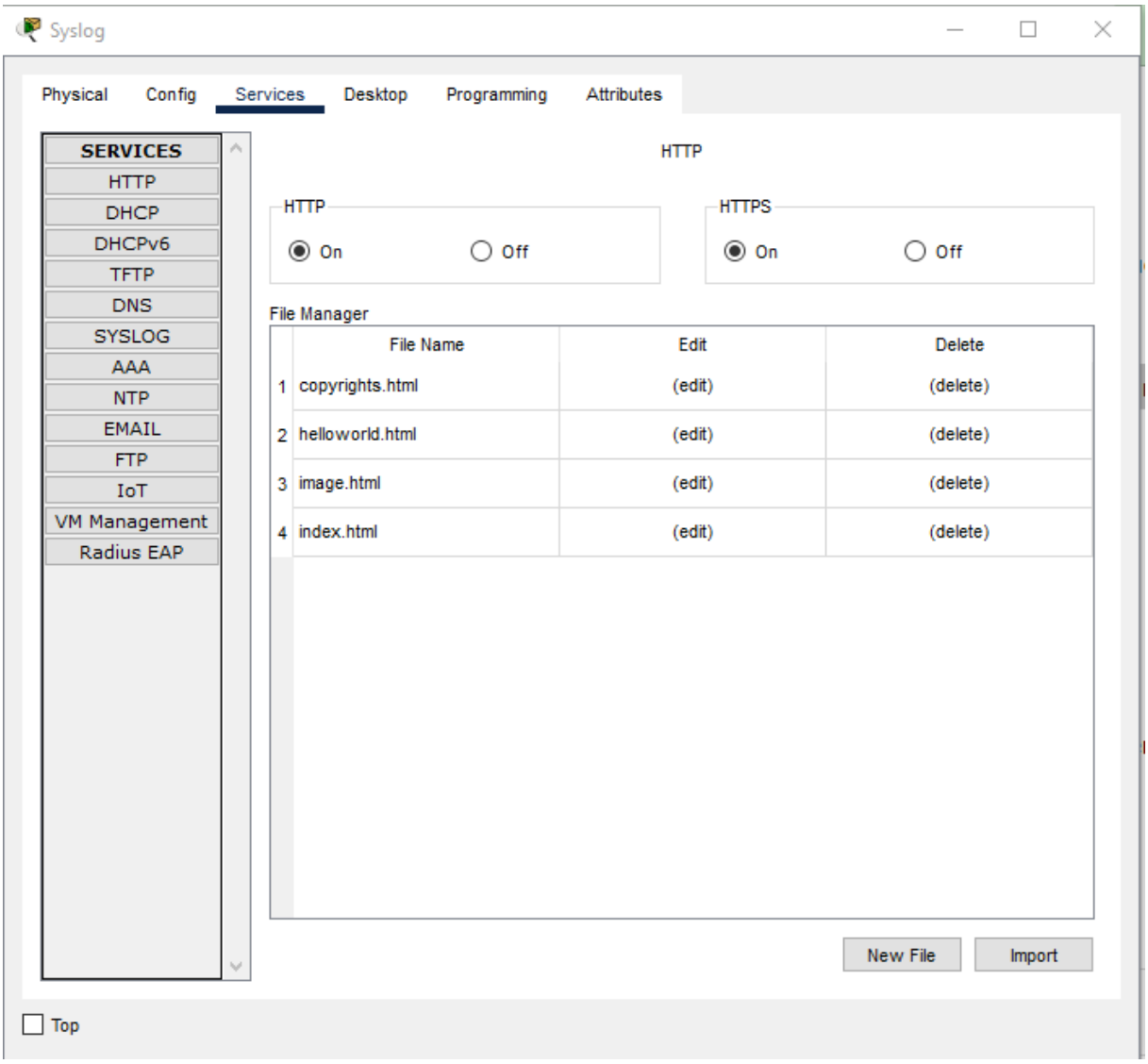
Le ping devrait être réussi. En effet, la règle IPS ne couvre pas la réponse en écho. Lorsque PC-A envoie une requête ping à PC-C, PC-C répond par une réponse d'écho.

Step 4: View the syslog messages.

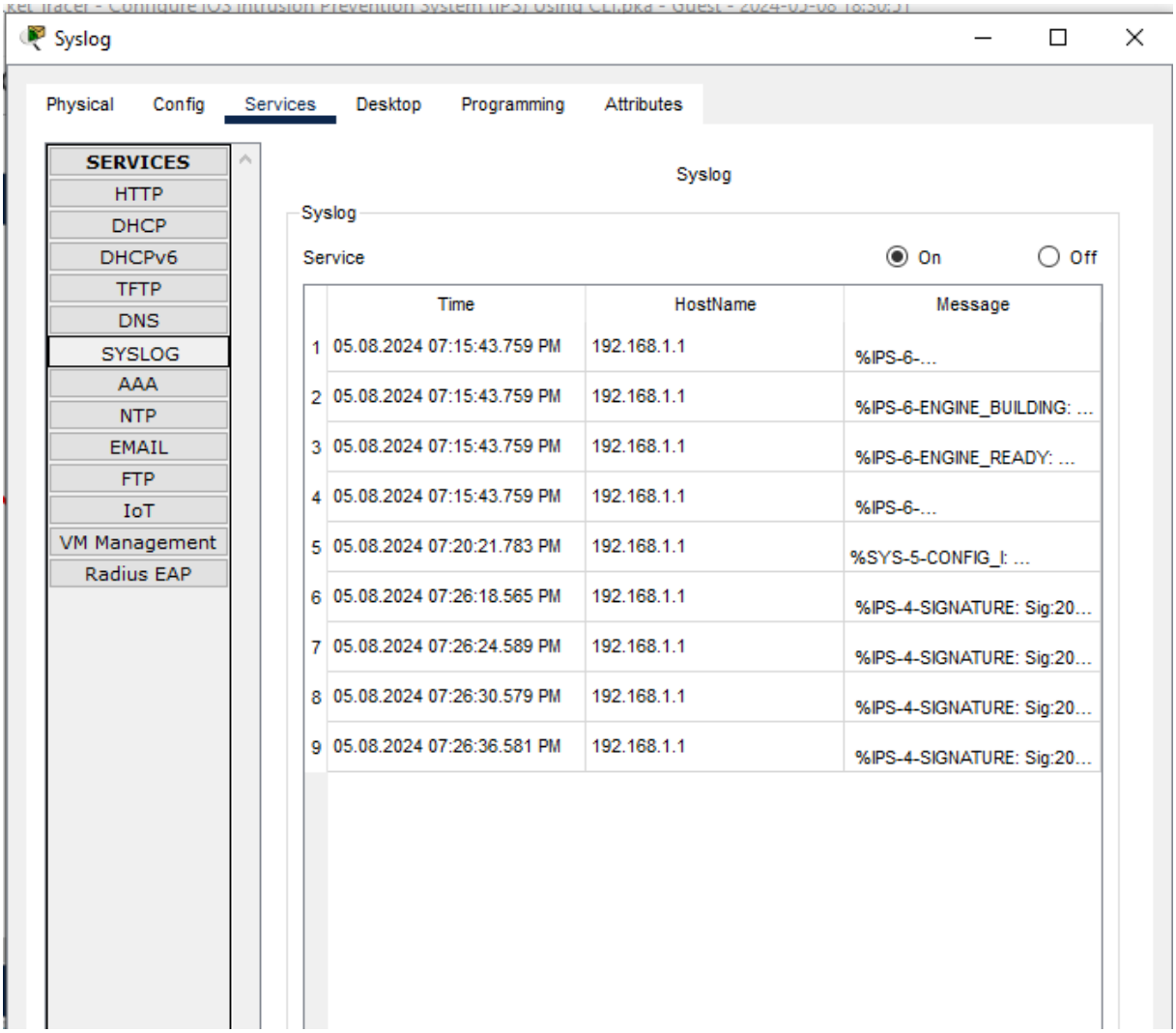
a. Click the Syslog server.



b. Select the Services tab.



In the left navigation menu, select SYSLOG to view the log file.


Syslog
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
Syslog
Syslog
Service
On
Off
Time
HostName
Message
1 05.08.2024 07:15:43.759 PM 192.168.1.1 %IPS-6-...
2 05.08.2024 07:15:43.759 PM 192.168.1.1 %IPS-6-ENGINE_BUILDING: ...
3 05.08.2024 07:15:43.759 PM 192.168.1.1 %IPS-6-ENGINE_READY: ...
4 05.08.2024 07:15:43.759 PM 192.168.1.1 %IPS-6-...
5 05.08.2024 07:20:21.783 PM 192.168.1.1 %SYS-5-CONFIG_I: ...
6 05.08.2024 07:26:18.565 PM 192.168.1.1 %IPS-4-SIGNATURE: Sig:20...
7 05.08.2024 07:26:24.589 PM 192.168.1.1 %IPS-4-SIGNATURE: Sig:20...
8 05.08.2024 07:26:30.579 PM 192.168.1.1 %IPS-4-SIGNATURE: Sig:20...
9 05.08.2024 07:26:36.581 PM 192.168.1.1 %IPS-4-SIGNATURE: Sig:20...