**Université Abdelmalek Essaâdi**

**Faculté des Sciences et Techniques-Tanger**

**Département Génie Informatique**

[**Cryptographie-Sécurité Services**](https://classroom.google.com/c/NjY1MDU4MTM5NTAy)

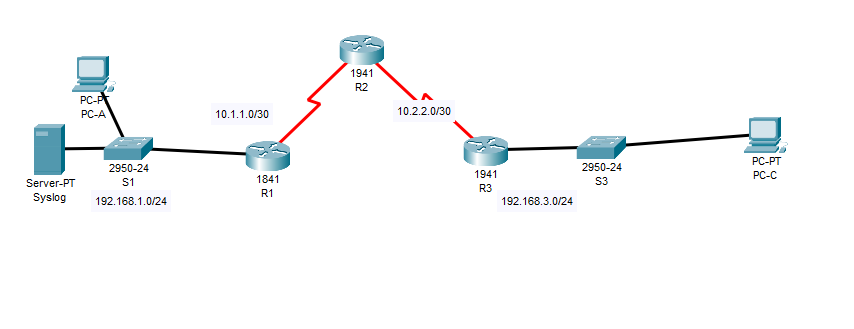
LAB-IPS



Réalisé Par :

Yossra safi chetouan

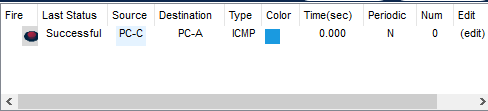
LAB: Configure IOS Intrusion Prevention System (IPS) Using CLI



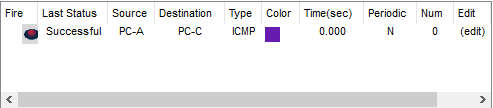
Part 1: Enable IOS IPS

Step 1: Verify network connectivity

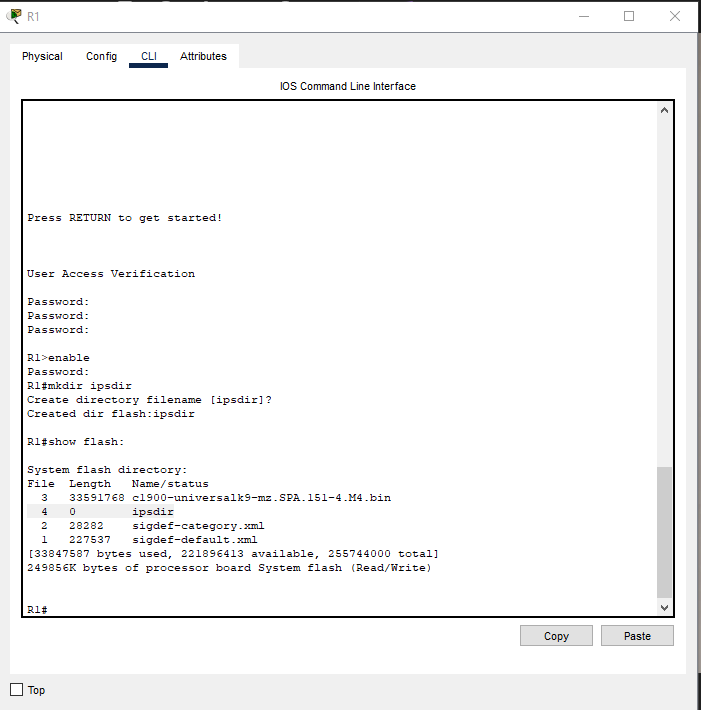
1. Ping from PC-C to PC-A. The ping should be successful:



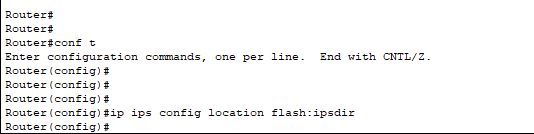
1. Ping from PC-A to PC-C. The ping should be successful:



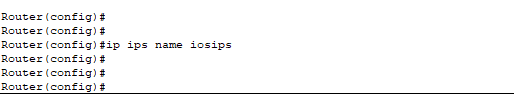
Step 2: Create an IOS IPS configuration directory in flash.



Step 3: Configure the IPS signature storage location.



Step 4: Create an IPS rule.

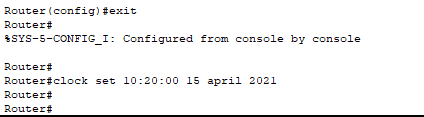


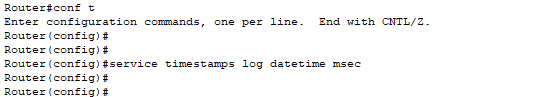
Step 5: Enable logging.

1. Enable syslog if it is not enabled.



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

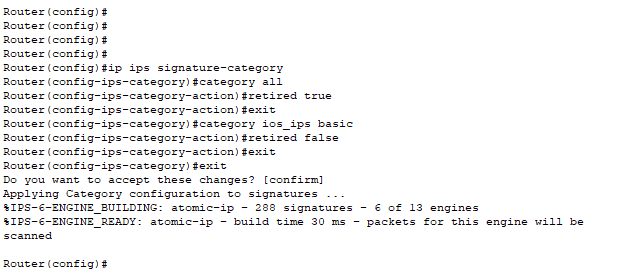




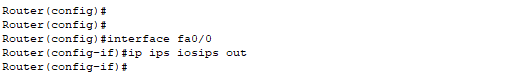
1. Send log messages to the syslog server at IP address 192.168.1.50.



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

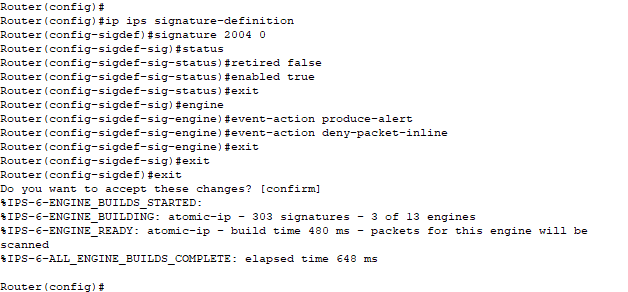


Step 7: Apply the IPS rule to an interface.

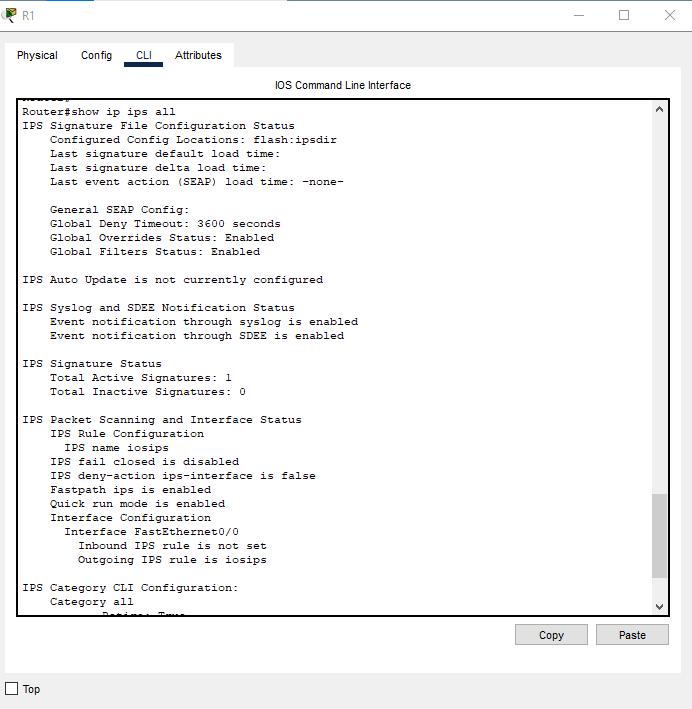


Part 2: Modify the Signature

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

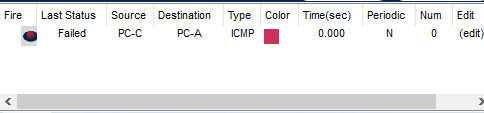


Step 2: Use show commands to verify IPS.



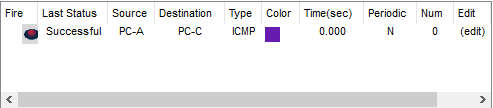
Step 3: Verify that IPS is working properly.

Ping PC-C vers PC-A



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".

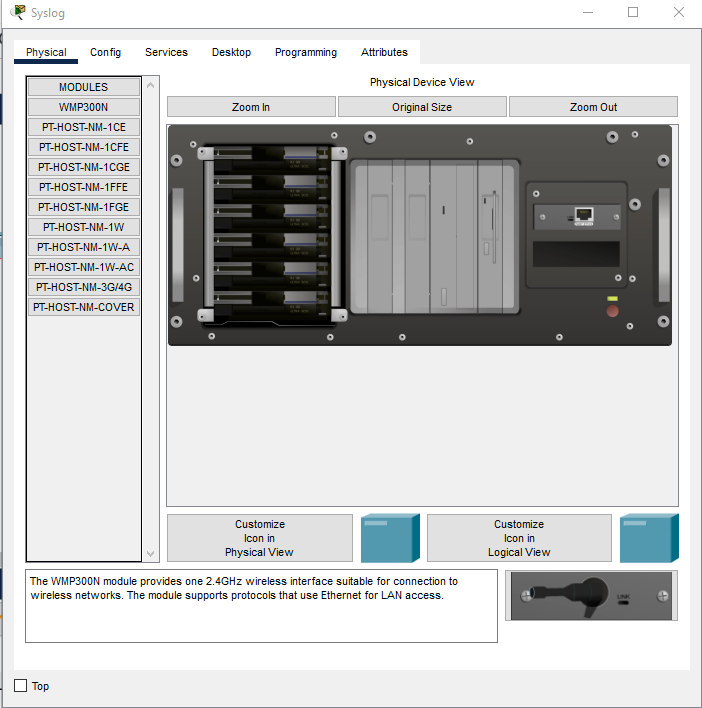
Ping PC-A vers PC-C



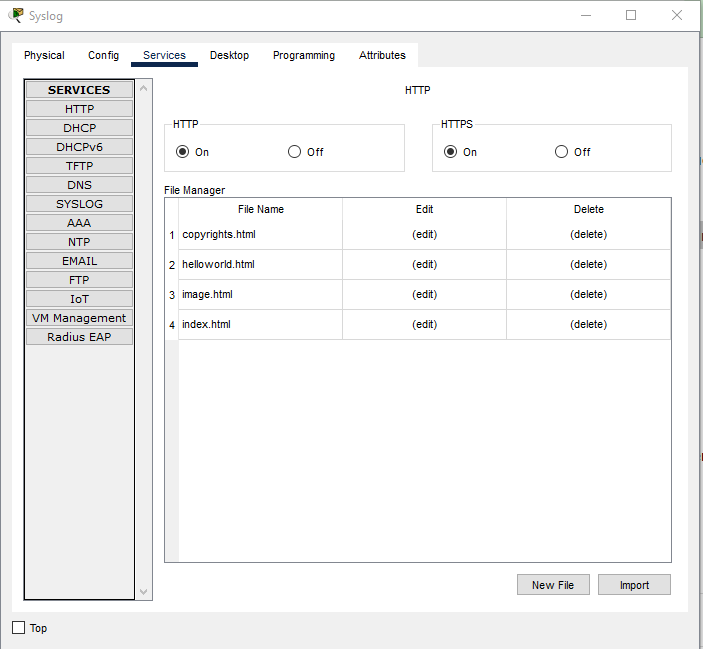
Le ping devrait être réussi. En effet, la règle IPS ne couvre pas la réponse en écho. Lorsque PC-A envoie une requête ping à PC-C, PC-C répond par une réponse d'écho.

Step 4: View the syslog messages.

1. Click the Syslog server.



1. Select the Services tab.



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

