

Ulrich Noéjules OGO NDAYEGUIA

Etudiant en Réseaux et Systèmes / Virtualisation et Cloud Computing

ogo.ulrich@gmail.com / jules.ndayeguia@gmail.com

LinkedIn: <https://www.linkedin.com/in/jules-ndayeguia-2b0098306>

18/10/2024



Projet : Mise en place d'un système de  
détection d'intrusion avec Snort (IDS/IPS)

Fait par :

Ulrich Noéjules OGO NDAYEGUIA

## Méthodologie

1. Installation de Snort sur un serveur (UBUNTU).
2. Configuration des interfaces réseau pour capturer le trafic.
3. Mise en place des règles Snort (détection d'attaques, etc).
4. Test du fonctionnement de l'IDS/IPS
5. Analyse des alertes générées et ajustement des règles pour une meilleure protection

## Environnement Technique

- **Système d'exploitation** : UBUNTU 22.04
- **Outil principal** : Snort (version 2.9.15.1)
- **Outils complémentaires** : Wireshark (pour l'analyse des logs)
- **Matériel requis** : Une machine virtuelle installée sous VMware Workstation, GNS3, un hyperviseur du type 2 VMware Workstation ou autre.



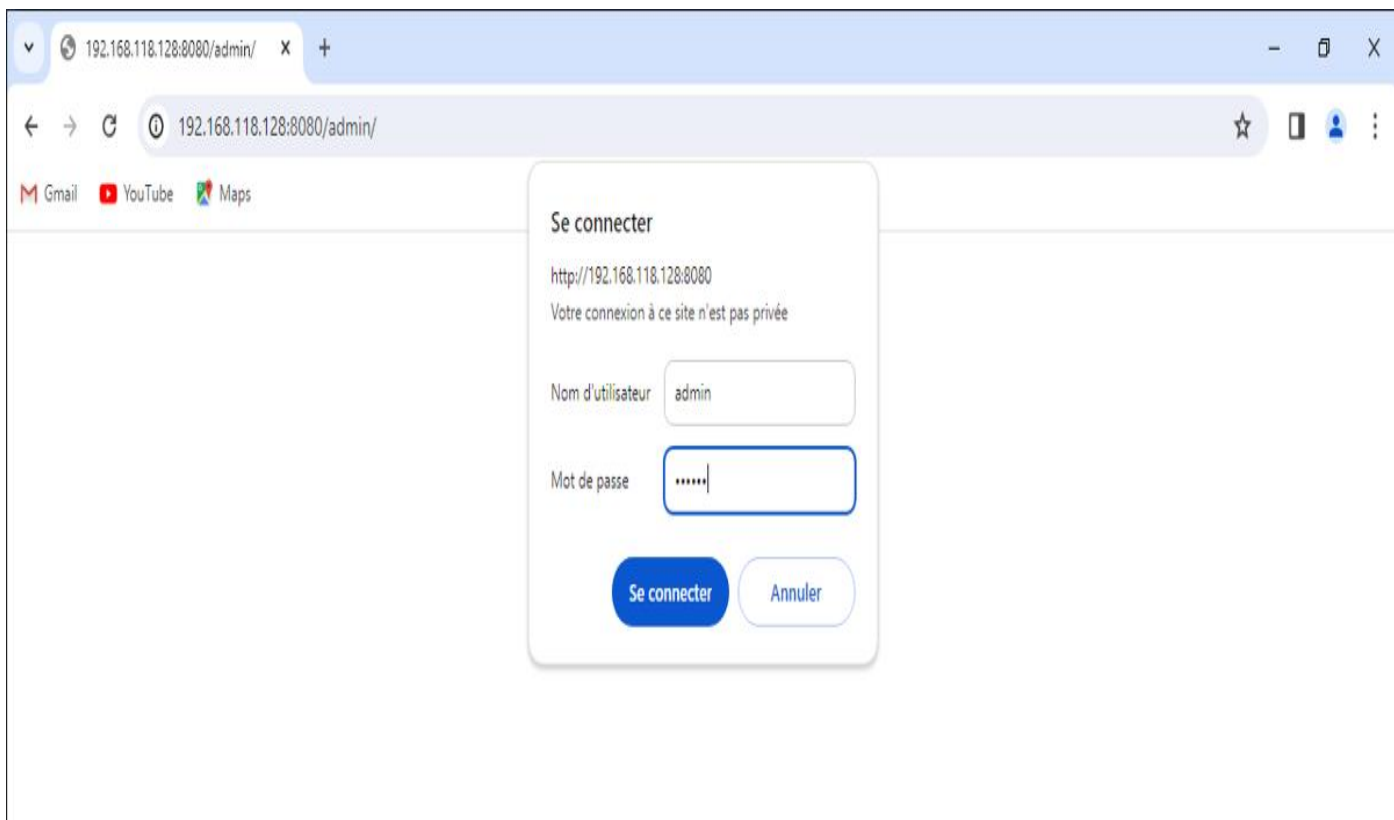
# INTRODUCTION

Snort est un système de détection d'intrusion réseau (IDS) open-source, écrit en langage C. Développé en 1998 par Martin Roesch, il est aujourd'hui maintenu par Cisco. Cet outil permet aux administrateurs réseau d'analyser le trafic en temps réel afin d'identifier et de bloquer les paquets potentiellement malveillants.

Dans ce projet, nous nous focaliserons sur la configuration pratique de Snort pour la détection d'intrusions et son intégration dans un environnement réseau. Nous détaillerons les différentes étapes de son installation, la personnalisation de ses règles et son déploiement dans un contexte réel. Enfin, nous réaliserons une simulation sous GNS3 afin de tester et d'évaluer son efficacité face à des scénarios d'attaques réels.

Pour le moment, l'accent sera mis sur l'installation et la détection d'intrusions. Pour aller plus loin, nous pourrions également implémenter Barnyard2 pour traiter les alertes de Snort et les stocker dans une base de données telle que MySQL ou PostgreSQL. Une interface web telle que BASE pourrait ensuite être utilisée pour analyser et visualiser les alertes générées par Snort et stockées dans la base de données via Barnyard2.

## Test et fonctionnement du Site



## INSTALLATION, CONFIGURATION ET INTEGRATION DE SNORT DANS NOTRE RESEAU

```
khady@mame: ~  
khady@mame:~$ sudo apt install snort  
[sudo] Mot de passe de khady :  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
Les paquets supplémentaires suivants seront installés :  
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1  
  oinkmaster snort-common snort-common-libraries snort-rules-default  
Paquets suggérés :  
  snort-doc  
Les NOUVEAUX paquets suivants seront installés :  
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1  
  oinkmaster snort snort-common snort-common-libraries snort-rules-default  
0 mis à jour, 10 nouvellement installés, 0 à enlever et 2 non mis à jour.  
Il est nécessaire de prendre 2349 ko dans les archives.  
Après cette opération, 10,6 Mo d'espace disque supplémentaires seront utilisés.  
Souhaitez-vous continuer ? [0/n] o
```

**sudo apt install snort** : La commande apt = aptitude qui est une commande qui permet d'installer un paquet dans un environnement Linux (Ubuntu, Debian).

```
khady@mame: ~
khady@mame:~$ snort --version

  ,,-
 o" )~
  ' '

-*> Snort! <*-
Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.

Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.1 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

Rhythmbox
khady@mame:~$
```

**Snort - -version** : Pour vérifier la version de notre snort installé

```
khady@mame: /etc/snort
#####
# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.118.0/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
-- INSERTION --
72,31 7%
```

Ajoutons l'adresse réseau au niveau de : **ipvar HOME\_NET : 192.168.118.0/24**



```
khady@mame: /etc/snort
# rules files that are available in your system (in the /etc/snort/rules
# directory)

# site specific rules
include $RULE_PATH/local.rules

# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:
#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
-- INSERTION --                               597.37      84%
```

On supprime toutes les règles qui s'y trouvent dans `/etc/snort/local.rules`

```
khady@mame: /etc/snort/rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert icmp any any -> $HOME_NET any (msg: "ICMP Detected"; sid: 100000; rev:1)
alert tcp any any -> any 22 (msg: "SSH Detected"; sid: 1000002; rev:1)
~
~
~
~
~
~
~
~
~
~
-- INSERTION --                               10,70      Tout
```

On personnalise nous-même nos règles pour mieux contrôler le fonctionnement de Snort.

## 1ère Partie : Test IDS/IPS de l'interface physique vers l'interface virtuelle de Ubuntu avec Snort

```
Invite de commandes
Microsoft Windows [version 10.0.18362.30]
(c) 2019 Microsoft Corporation. Tous droits réservés.

C:\Users\Dell>ping 192.168.118.128

Envoi d'une requête 'Ping' 192.168.118.128 avec 32 octets de données :
Réponse de 192.168.118.128 : octets=32 temps<1ms TTL=64
Réponse de 192.168.118.128 : octets=32 temps<1ms TTL=64
Réponse de 192.168.118.128 : octets=32 temps<1ms TTL=64
Réponse de 192.168.118.128 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.118.128:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Dell>
C:\Users\Dell>
```

L'envoi des pings à l'adresse de notre serveur **192.168.118.128** à laquelle snort est configuré alors 192.168.118.1 est l'adresse physique de UBUNTU-SERVER puisque les deux adresses IP sont dans le même réseau.

```
khady@mame: /etc/snort/rules
khady@mame:/etc/snort/rules$ sudo snort -A console -q -i ens37 -c /etc/snort/snort.conf -k none
02/04-19:28:55.374440  [**] [1:100000:1] ICMP Detected [**] [Priority: 0] {ICMP}
192.168.118.1 -> 192.168.118.128
02/04-19:28:55.374583  [**] [1:100000:1] ICMP Detected [**] [Priority: 0] {ICMP}
192.168.118.128 -> 192.168.118.1
02/04-19:28:56.387952  [**] [1:100000:1] ICMP Detected [**] [Priority: 0] {ICMP}
192.168.118.1 -> 192.168.118.128
02/04-19:28:56.388010  [**] [1:100000:1] ICMP Detected [**] [Priority: 0] {ICMP}
192.168.118.128 -> 192.168.118.1
02/04-19:28:57.398437  [**] [1:100000:1] ICMP Detected [**] [Priority: 0] {ICMP}
192.168.118.1 -> 192.168.118.128
02/04-19:28:57.398489  [**] [1:100000:1] ICMP Detected [**] [Priority: 0] {ICMP}
192.168.118.128 -> 192.168.118.1
02/04-19:28:58.410337  [**] [1:100000:1] ICMP Detected [**] [Priority: 0] {ICMP}
192.168.118.1 -> 192.168.118.128
02/04-19:28:58.410422  [**] [1:100000:1] ICMP Detected [**] [Priority: 0] {ICMP}
192.168.118.128 -> 192.168.118.1
^C*** Caught Int-Signal
khady@mame:/etc/snort/rules$
khady@mame:/etc/snort/rules$
khady@mame:/etc/snort/rules$
khady@mame:/etc/snort/rules$
khady@mame:/etc/snort/rules$
```

Détection d'intrusion à l'adresse **192.168.118.1** de l'interface physique vers le serveur Ubuntu à l'adresse **192.168.118.128**. 192.168.118.1 pings provenant de l'interface physique.

```
Sélection OpenSSH SSH client
Microsoft Windows [version 10.0.18362.30]
(c) 2019 Microsoft Corporation. Tous droits réservés.

C:\Users\Dell>ssh -l ndiaye 192.168.118.128
ndiaye@192.168.118.128's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-17-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

La maintenance de sécurité étendue pour Applications n'est pas activée.

0 mise à jour peut être appliquée immédiatement.

11 mises à jour de sécurité supplémentaires peuvent être appliquées avec ESM Apps.
En savoir plus sur l'activation du service ESM Apps at https://ubuntu.com/esm

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

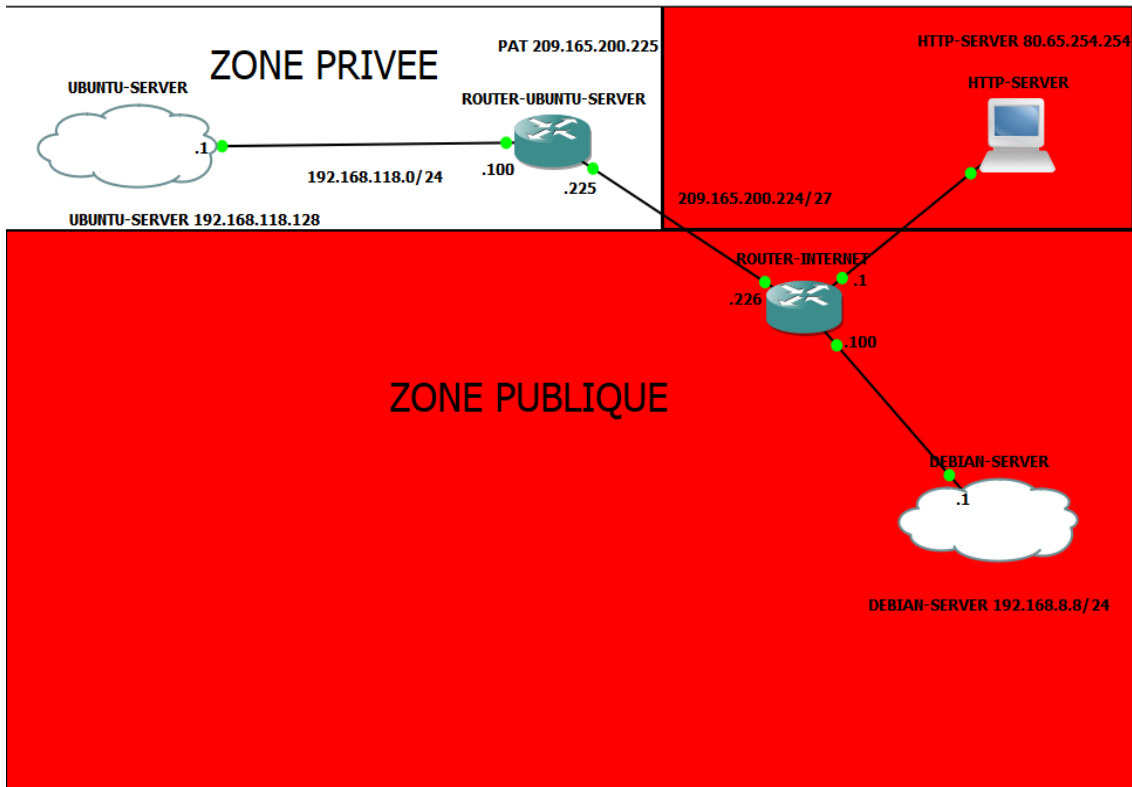
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Fri Feb 16 00:08:45 2024 from 192.168.118.1
Could not chdir to home directory /home/ndiaye: Permission denied
-bash: /home/ndiaye/.bash_profile: Permission non accordée
ndiaye@mame:/$
```

Connexion ssh : du PC physique **192.168.118.1** vers le serveur Ubuntu **192.168.118.128**  
vers le shell de l'utilisateur ndiaye (serveur Ubuntu)

```
khady@mame: /etc/snort/rules
khady@mame: /etc/snort/rules$ sudo snort -A console -q -i ens37 -c /etc/snort/snort.conf -k none
02/04-19:48:42.787434  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52198 -> 192.168.118.128:22
02/04-19:48:42.833157  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52198 -> 192.168.118.128:22
02/04-19:48:44.232850  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52198 -> 192.168.118.128:22
02/04-19:48:44.245196  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52198 -> 192.168.118.128:22
02/04-19:48:44.247705  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52198 -> 192.168.118.128:22
02/04-19:48:44.247707  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52198 -> 192.168.118.128:22
02/04-19:48:44.248542  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52198 -> 192.168.118.128:22
02/04-19:48:46.273269  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52205 -> 192.168.118.128:22
02/04-19:48:46.273701  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52205 -> 192.168.118.128:22
02/04-19:48:46.277249  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52205 -> 192.168.118.128:22
02/04-19:48:46.315849  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.118.1:52205 -> 192.168.118.128:22
```

## 2ème PARTIE : TEST SNORT avec le simulateur réseau GNS3



ROUTER-INTERNET : Configuration et adressage IP sur les interfaces : f0/0, f0/1, f3/0

```
ROUTER-INTERNET
inistratively down
*Feb 14 16:10:00.015: %LINK-5-CHANGED: Interface Serial2/3, changed state to adm
inistratively down
ROUTER-INTERNET#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-INTERNET(config)#int f0/0
ROUTER-INTERNET(config-if)#no sh
ROUTER-INTERNET(config-if)#ip add
*Feb 14 16:13:03.747: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Feb 14 16:13:04.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
ROUTER-INTERNET(config-if)#ip add 192.168.8.100 255.255.255.0
ROUTER-INTERNET(config-if)#ex
ROUTER-INTERNET(config)#int f0/0
ROUTER-INTERNET(config-if)#int f0/1
ROUTER-INTERNET(config-if)#no sh
ROUTER-INTERNET(config-if)#ip add
*Feb 14 16:13:36.059: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Feb 14 16:13:37.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
ROUTER-INTERNET(config-if)#ip add 80.65.254.1 255.255.255.0
ROUTER-INTERNET(config-if)#ex
```

→ IP route 0.0.0.0 0.0.0.0 209.165.200.225 -> route statique par défaut vers ROUTER-UBUNTU SERVER.

```
ROUTER-INTERNET
ROUTER-INTERNET(config)#int f3/0
ROUTER-INTERNET(config-if)#no sh
ROUTER-INTERNET(config-if)#ip add 209.
*Feb 14 16:13:55.059: %LINK-3-UPDOWN: Interface FastEthernet3/0, changed state to up
*Feb 14 16:13:56.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/0, changed state to up
ROUTER-INTERNET(config-if)#ip add 209.165.200.226 255.255.255.0
ROUTER-INTERNET(config-if)#ip add 209.165.200.226 255.255.255.224
ROUTER-INTERNET(config-if)#
ROUTER-INTERNET(config-if)#ex
ROUTER-INTERNET(config)#
ROUTER-INTERNET(config)#
*Feb 14 16:15:41.859: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/0, changed state to down
ROUTER-INTERNET(config)#
*Feb 14 16:16:20.859: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/0, changed state to up
ROUTER-INTERNET(config)#
ROUTER-INTERNET(config)#
ROUTER-INTERNET(config)#
ROUTER-INTERNET(config)#
ROUTER-INTERNET(config)#
ROUTER-INTERNET(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

→ IP route 0.0.0.0 0.0.0.0 209.165.200.226 -> route statique par défaut vers ROUTER-INTERNET

```
ROUTER-UBUNTU-SERVER
ministratively down
ROUTER-UBUNTU-SERVER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-UBUNTU-SERVER(config)#int f0/0
ROUTER-UBUNTU-SERVER(config-if)#no sh
ROUTER-UBUNTU-SERVER(config-if)#ip add 192.
*Feb 14 16:23:26.987: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
ROUTER-UBUNTU-SERVER(config-if)#ip add 192.168.
*Feb 14 16:23:27.987: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
ROUTER-UBUNTU-SERVER(config-if)#ip add 192.168.118.100 255.255.255.0
ROUTER-UBUNTU-SERVER(config-if)#ex
ROUTER-UBUNTU-SERVER(config)#int f3/0
ROUTER-UBUNTU-SERVER(config-if)#ip add 209.165.200.225 255.255.255.224
ROUTER-UBUNTU-SERVER(config-if)#no sh
ROUTER-UBUNTU-SERVER(config-if)#exit
ROUTER-UBUNTU-SERVER(config)#
*Feb 14 16:24:10.927: %LINK-3-UPDOWN: Interface FastEthernet3/0, changed state to up
*Feb 14 16:24:11.927: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/0, changed state to up
ROUTER-UBUNTU-SERVER(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
ROUTER-UBUNTU-SERVER(config)#
```

## 🚦 Sauvegarde de la configuration sur le ROUTER-INTERNET et ROUTER-UBUNTU-SERVER

```
ROUTER-INTERNET
ROUTER-INTERNET(config)#end
ROUTER-INTERNET#co
*Feb 14 16:29:04.711: %SYS-5-CONFIG_I: Configured from console by console
ROUTER-INTERNET#copy run st
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
ROUTER-INTERNET#
```

```
ROUTER-UBUNTU-SERVER
ROUTER-UBUNTU-SERVER(config)#end
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
*Feb 14 16:27:49.831: %SYS-5-CONFIG_I: Configured from console by console
ROUTER-UBUNTU-SERVER#copy run st
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
```

## TEST PING VERS LE SERVEUR DEBIAN

```
khady@mame: ~  
khady@mame:~$ ping 192.168.8.8  
PING 192.168.8.8 (192.168.8.8) 56(84) bytes of data.  
64 bytes from 192.168.8.8: icmp_seq=1 ttl=62 time=27.0 ms  
64 bytes from 192.168.8.8: icmp_seq=2 ttl=62 time=33.9 ms  
64 bytes from 192.168.8.8: icmp_seq=3 ttl=62 time=30.4 ms  
64 bytes from 192.168.8.8: icmp_seq=4 ttl=62 time=24.9 ms  
64 bytes from 192.168.8.8: icmp_seq=5 ttl=62 time=37.4 ms  
64 bytes from 192.168.8.8: icmp_seq=6 ttl=62 time=31.3 ms  
64 bytes from 192.168.8.8: icmp_seq=7 ttl=62 time=22.6 ms  
64 bytes from 192.168.8.8: icmp_seq=8 ttl=62 time=29.7 ms  
64 bytes from 192.168.8.8: icmp_seq=9 ttl=62 time=28.9 ms  
64 bytes from 192.168.8.8: icmp_seq=10 ttl=62 time=28.5 ms  
^C  
--- 192.168.8.8 ping statistics ---  
10 packets transmitted, 10 received, 0% packet loss, time 9015ms  
rtt min/avg/max/mdev = 22.623/29.458/37.449/4.035 ms  
khady@mame:~$ ping 80.65.254.1  
PING 80.65.254.1 (80.65.254.1) 56(84) bytes of data.  
64 bytes from 80.65.254.1: icmp_seq=1 ttl=254 time=12.1 ms  
64 bytes from 80.65.254.1: icmp_seq=2 ttl=254 time=17.7 ms  
^C  
--- 80.65.254.1 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1002ms  
rtt min/avg/max/mdev = 12.116/14.928/17.740/2.812 ms
```

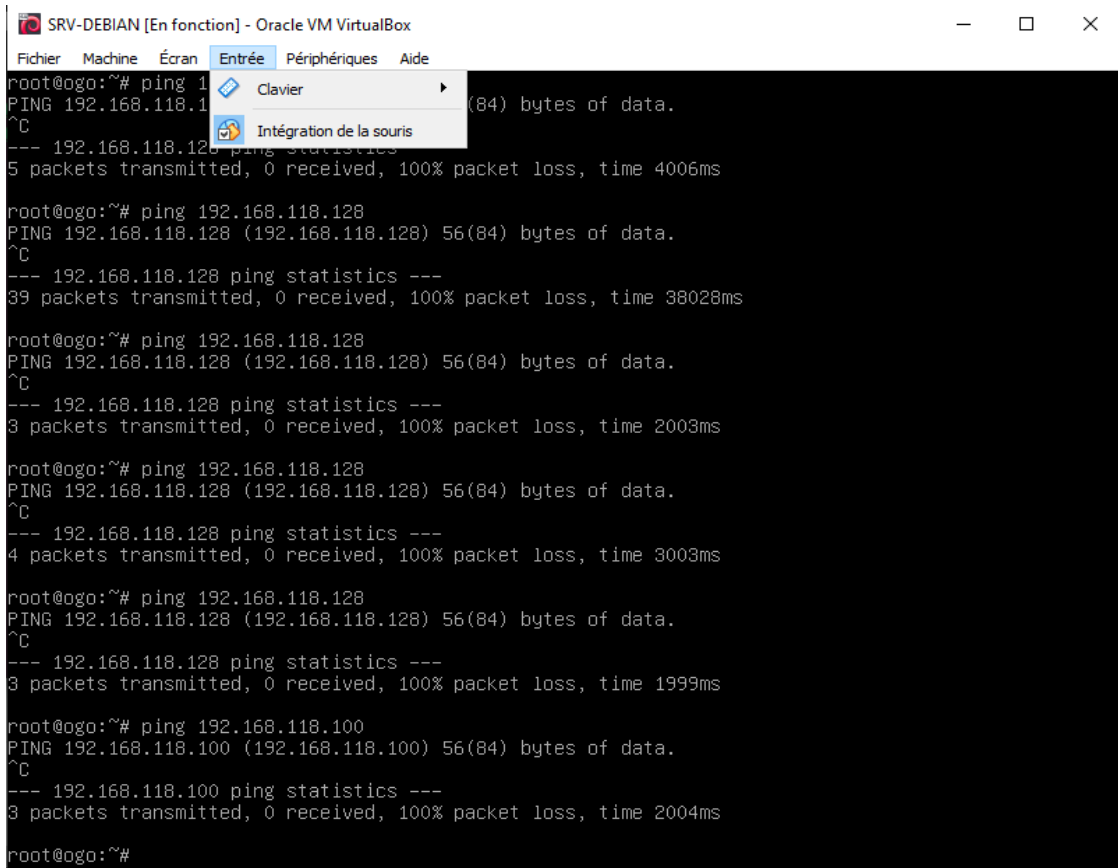
## TEST PING VERS LE SERVEUR HTTP

```
khady@mame: ~  
khady@mame:~$ ping 80.65.254.254  
PING 80.65.254.254 (80.65.254.254) 56(84) bytes of data.  
64 bytes from 80.65.254.254: icmp_seq=1 ttl=62 time=273 ms  
64 bytes from 80.65.254.254: icmp_seq=2 ttl=62 time=33.8 ms  
64 bytes from 80.65.254.254: icmp_seq=3 ttl=62 time=69.8 ms  
64 bytes from 80.65.254.254: icmp_seq=4 ttl=62 time=29.6 ms  
64 bytes from 80.65.254.254: icmp_seq=5 ttl=62 time=24.3 ms  
64 bytes from 80.65.254.254: icmp_seq=6 ttl=62 time=37.8 ms  
64 bytes from 80.65.254.254: icmp_seq=7 ttl=62 time=23.3 ms  
64 bytes from 80.65.254.254: icmp_seq=8 ttl=62 time=28.8 ms  
64 bytes from 80.65.254.254: icmp_seq=9 ttl=62 time=25.0 ms  
^C  
--- 80.65.254.254 ping statistics ---  
9 packets transmitted, 9 received, 0% packet loss, time 8013ms  
rtt min/avg/max/mdev = 23.283/60.542/272.572/76.164 ms  
khady@mame:~$ ping 80.65.254.1  
PING 80.65.254.1 (80.65.254.1) 56(84) bytes of data.  
64 bytes from 80.65.254.1: icmp_seq=1 ttl=254 time=21.1 ms  
^C  
--- 80.65.254.1 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 21.065/21.065/21.065/0.000 ms  
khady@mame:~$
```

## CONFIGURATION DU PAT (Port Address Translation) SUR LE ROUTER-UBUNTU-SERVER

```
ROUTER-UBUNTU-SERVER
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#
ROUTER-UBUNTU-SERVER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER-UBUNTU-SERVER(config)#int f3/0
ROUTER-UBUNTU-SERVER(config-if)#ip nat outside
ROUTER-UBUNTU-SERVER(config-if)#int f0/0
ROUTER-UBUNTU-SERVER(config-if)#ip nat inside
ROUTER-UBUNTU-SERVER(config-if)#
ROUTER-UBUNTU-SERVER(config-if)#ip nat inside source list 1 inter f3/0 overload
ROUTER-UBUNTU-SERVER(config)#
ROUTER-UBUNTU-SERVER(config)#access-list 1 permit any any
Translating "any"
^
% Invalid input detected at '^' marker.
ROUTER-UBUNTU-SERVER(config)#access-list 1 permit any
ROUTER-UBUNTU-SERVER(config)#
```

## PING DE DEBIAN-SERVER VERS UBUNTU-SERVER



```
SRV-DEBIAN [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
root@ogo:~# ping 192.168.118.128
PING 192.168.118.128 (192.168.118.128) 56(84) bytes of data.
^C
--- 192.168.118.128 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4006ms

root@ogo:~# ping 192.168.118.128
PING 192.168.118.128 (192.168.118.128) 56(84) bytes of data.
^C
--- 192.168.118.128 ping statistics ---
39 packets transmitted, 0 received, 100% packet loss, time 38028ms

root@ogo:~# ping 192.168.118.128
PING 192.168.118.128 (192.168.118.128) 56(84) bytes of data.
^C
--- 192.168.118.128 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2003ms

root@ogo:~# ping 192.168.118.128
PING 192.168.118.128 (192.168.118.128) 56(84) bytes of data.
^C
--- 192.168.118.128 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3003ms

root@ogo:~# ping 192.168.118.128
PING 192.168.118.128 (192.168.118.128) 56(84) bytes of data.
^C
--- 192.168.118.128 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms

root@ogo:~# ping 192.168.118.100
PING 192.168.118.100 (192.168.118.100) 56(84) bytes of data.
^C
--- 192.168.118.100 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2004ms

root@ogo:~#
```

Si on voit bien les pings vers UBUNTU-SERVER ne passent pas, pourquoi parce que PAT Bloque déjà l'accès à notre adresse IP privée alors le PAT fait la translation des adresses IP provenant de la ZONE PUBLIQUE vers la ZONE PRIVEE avec l'IP 209.165.200.225.

```
khady@mame: ~
khady@mame:~$ sudo snort -A console -q -i ens37 -c /etc/snort/snort.conf
[sudo] Mot de passe de khady :
02/14-16:54:35.052102  [**] [1:1000001:1] ICMP Detected [**] [Priority: 0] {ICMP
} 192.168.8.8 -> 192.168.118.128
02/14-16:54:36.053199  [**] [1:1000001:1] ICMP Detected [**] [Priority: 0] {ICMP
} 192.168.8.8 -> 192.168.118.128
02/14-16:54:37.051224  [**] [1:1000001:1] ICMP Detected [**] [Priority: 0] {ICMP
} 192.168.8.8 -> 192.168.118.128
02/14-16:54:38.049148  [**] [1:1000001:1] ICMP Detected [**] [Priority: 0] {ICMP
} 192.168.8.8 -> 192.168.118.128
02/14-16:54:39.054785  [**] [1:1000001:1] ICMP Detected [**] [Priority: 0] {ICMP
} 192.168.8.8 -> 192.168.118.128
02/14-16:54:40.054405  [**] [1:1000001:1] ICMP Detected [**] [Priority: 0] {ICMP
} 192.168.8.8 -> 192.168.118.128
02/14-16:54:41.054057  [**] [1:1000001:1] ICMP Detected [**] [Priority: 0] {ICMP
} 192.168.8.8 -> 192.168.118.128
02/14-16:54:42.056637  [**] [1:1000001:1] ICMP Detected [**] [Priority: 0] {ICMP
} 192.168.8.8 -> 192.168.118.128
02/14-16:54:43.061112  [**] [1:1000001:1] ICMP Detected [**] [Priority: 0] {ICMP
} 192.168.8.8 -> 192.168.118.128
02/14-16:54:43.195929  [**] [1:1000001:1] ICMP Detected [**] [Priority: 0] {ICMP
} 209.165.200.226 -> 192.168.118.128
^C*** Caught Int-Signal
```

Détection des paquets ICMP provenant du DEBIAN-SERVER vers notre UBUNTU-SERVER malgré que les pings ne passent mais cela ne montre pas que UBUNTU-SERVER n'a pas reçu les pings provenant du DEBIAN-SERVER, juste que les ICMP sont bloqués au niveau du PAT et n'autorise pas les pings vers la ZONE PRIVEE.

```
SRV-DEBIAN [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
root@ogo:~# ssh -l ndiaye 192.168.118.128
^C
root@ogo:~# ssh -l ndiaye 192.168.118.128^C
root@ogo:~#
root@ogo:~# ssh -l ndiaye 192.168.118.128
^C
root@ogo:~# _
```

Ci-dessus est la tentative de connexion SSH vers notre ZONE PRIVEE qui ne se passe pas comme prévu, toujours le PAT bloque l'accès à DEBIAN-SERVER d'y avoir accès au service SSH via UBUNTU-SERVER, pour que DEBIAN-SERVER n'accède pas au shell de l'utilisateur ndiaye.

```
khady@mame: ~
^C*** Caught Int-Signal
khady@mame:~$ sudo snort -A console -q -i ens37 -c /etc/snort/snort.conf
02/14-18:29:10.809488  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.8.8:59846 -> 192.168.118.128:22
02/14-18:29:10.841401  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.8.8:59846 -> 192.168.118.128:22
02/14-18:29:11.842863  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.8.8:59846 -> 192.168.118.128:22
02/14-18:29:11.876082  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.8.8:59846 -> 192.168.118.128:22
02/14-18:29:13.852449  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.8.8:59846 -> 192.168.118.128:22
02/14-18:29:13.883416  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.8.8:59846 -> 192.168.118.128:22
02/14-18:29:18.042847  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.8.8:59846 -> 192.168.118.128:22
02/14-18:29:18.074291  [**] [1:1000002:1] SSH Detected [**] [Priority: 0] {TCP}
192.168.8.8:59846 -> 192.168.118.128:22
^C*** Caught Int-Signal
khady@mame:~$
khady@mame:~$
khady@mame:~$
khady@mame:~$
khady@mame:~$
```

Détection de connexion SSH provenant du DEBIAN-SERVER malgré qu'il n'ait pas pu se connecter au shell de l'utilisateur ndiaye de UBUNTU-SERVER.

## **CONCLUSION**

Ce projet nous a permis de configurer Snort et d'évaluer son efficacité à travers des tests en environnement simulé. Son bon fonctionnement repose sur une configuration rigoureuse et une mise à jour continue des règles de détection. Les simulations sous GNS3 ont souligné l'importance d'un paramétrage précis pour une détection optimale des menaces. Ainsi, Snort constitue un outil puissant pour la sécurisation des réseaux, à condition d'être intégré dans une stratégie de cybersécurité proactive.

FIN