Suricata

IDS / IPS — Detection et Prevention d'Intrusion

Infrastructure mvgroup.local — Proxmox VE

Auteur	Samuel
Version	1.0
Date	Mai 2026
VM dedie	SURICATA-SAM — Ubuntu 24.04 — 10.0.0.40
Version Suricata	8.0.5 RELEASE

1. Introduction et objectifs

Ce document decrit la mise en place d'un systeme de detection et de prevention d'intrusion (IDS/IPS) base sur Suricata au sein du lab mvgroup.local. Suricata est un moteur open source de reference capable d'analyser le trafic reseau en temps reel, de generer des alertes de securite et, en mode IPS, de bloquer activement les menaces.

1.1 Difference IDS et IPS

Mode	IDS — Intrusion Detection System	IPS — Intrusion Prevention System
Fonction	Detection et alertes uniquement	Detection + blocage actif
Action sur trafic	Aucune (ecoute passive)	Drop / Reject des paquets
Mecanisme	af-packet (copie du trafic)	nfqueue (trafic inline)
Risque	Faible (pas d'impact reseau)	Peut bloquer du trafic legitime

1.2 Objectifs du projet

- Installer Suricata 8.0.5 sur une VM Ubuntu 24.04 dediee
- Configurer le mode IDS avec les regles Emerging Threats
- Integrer Suricata avec Wazuh pour centraliser les alertes
- Passer en mode IPS avec blocage actif via nfqueue
- Valider le blocage avec une regle personnalisee

2. Architecture

2.1 VM dedie — SURICATA-SAM

Parametre	Valeur
Hostname	SURICATA-SAM
Adresse IP	10.0.0.40
OS	Ubuntu Server 24.04 LTS
Reseau	10.0.0.0/16 — passerelle 10.0.0.1
DNS	10.0.200.2 (AD mvgroup.local)
Agent Wazuh	ID 003 — version 4.11.2

2.2 Interactions avec le lab

Composant	IP	Role
SECURITY-SAM	10.0.100.6	Source des tests (Nmap, ping)
WAZUH-MANAGER-SAM	10.0.0.11	Reception des alertes Suricata
WAZUH-DASHBOARD-SAM	10.0.0.12	Visualisation des alertes

3. Installation de Suricata

3.1 Ajout du depot officiel OISF

Suricata est installe depuis le depot officiel OISF (Open Information Security Foundation) pour obtenir la derniere version stable :

```
add-apt-repository ppa:oisf/suricata-stable -y
apt-get update
apt-get install -y suricata
suricata --version   # Suricata version 8.0.5
```

3.2 Configuration de base

Fichier /etc/suricata/suricata.yaml — parametres principaux :

Definition du reseau surveille (HOME_NET) :

```
vars:
  address-groups:
    HOME_NET: "[10.0.0.0/16]"
    EXTERNAL_NET: "!$HOME_NET"
```

Interface d'ecoute (af-packet pour le mode IDS) :

```
af-packet:
  - interface: ens18
    cluster-id: 99
    cluster-type: cluster_flow
    defrag: yes
```

Activation des logs EVE JSON (format compatible Wazuh) :

```
outputs:
  - eve-log:
      enabled: yes
      filename: /var/log/suricata/eve.json
      types:
        - alert
        - dns
        - http
        - tls
```

3.3 Telechargement des regles

Les regles de detection sont telechargees via suricata-update, qui integre les regles Emerging Threats (ET Open) — base de donnees de signatures de menaces connues :

```
pip3 install --upgrade suricata-update --break-system-packages
suricata-update
# Resultat : 50298 regles chargees
```

3.4 Demarrage du service IDS

```
suricata -T -c /etc/suricata/suricata.yaml -v   # Validation config
systemctl enable suricata
systemctl start suricata
```

4. Mode IDS — Detection et alertes

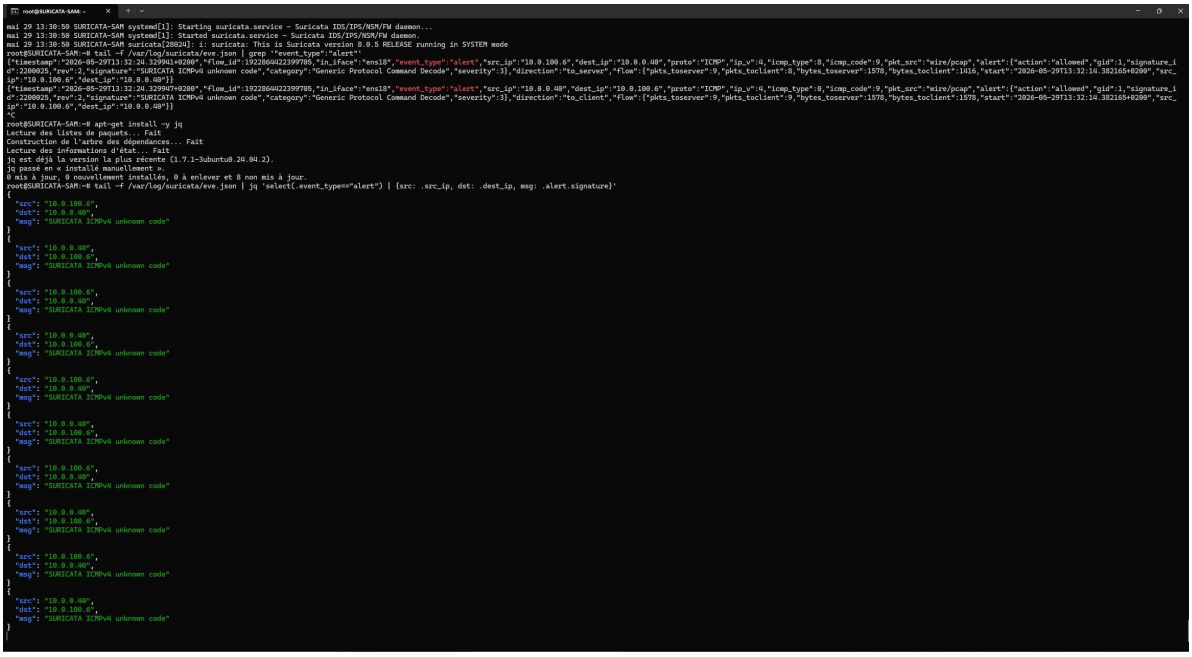
4.1 Test de detection — scan Nmap

Un scan Nmap agressif est lance depuis SECURITY-SAM (10.0.100.6) vers SURICATA-SAM pour declencher des alertes :

```
nmap -sS -A 10.0.0.40    # Depuis SECURITY-SAM
```

Les alertes sont consultees en temps reel sur SURICATA-SAM avec jq :

```
tail -f /var/log/suricata/eve.json | jq 'select(.event_type=="alert") |
{src: .src_ip, dst: .dest_ip, msg: .alert.signature}'
```



SURICATA-SAM — alertes IDS en temps reel : detection du scan ICMP depuis SECURITY-SAM (10.0.100.6) avec signature SURICATA ICMPv4 unknown code

4.2 Analyse des alertes

Champ	Valeur	Description
event_type	alert	Type d'evenement Suricata
src_ip	10.0.100.6	Source : SECURITY-SAM
dest_ip	10.0.0.40	Destination : SURICATA-SAM
signature	SURICATA ICMPv4 unknown code	Regle Suricata declenchee
action	allowed	Mode IDS : detection sans blocage
severity	3	Niveau de severite

5. Integration Suricata — Wazuh

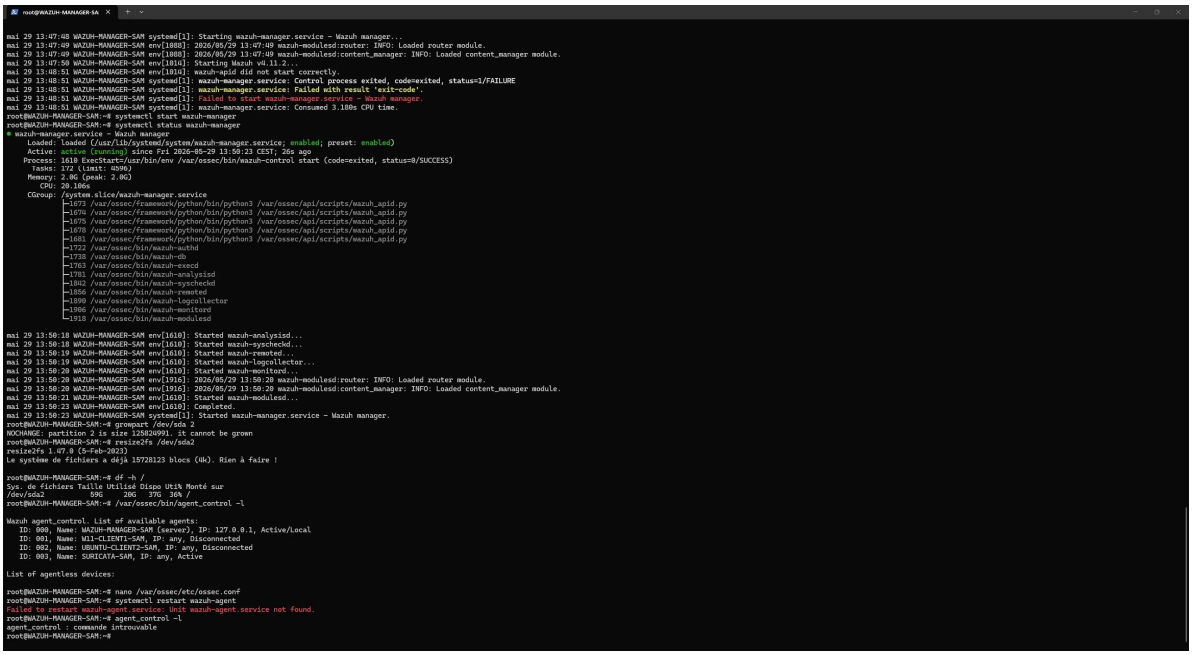
5.1 Installation de l'agent Wazuh

L'agent Wazuh 4.11.2 est installe sur SURICATA-SAM pour remonter les alertes vers le Manager (10.0.0.11). La version doit etre identique ou inferieure a celle du Manager.

```
# Ajout du depot Wazuh
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring \
  --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import
chmod 644 /usr/share/keyrings/wazuh.gpg
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" \
  | tee /etc/apt/sources.list.d/wazuh.list
apt-get update
apt-get install -y wazuh-agent=4.11.2-1
```

Enregistrement aupres du Manager :

```
sed -i 's|<address>MANAGER_IP</address>|<address>10.0.0.11</address>|' /var/ossec/etc/ossec.conf
/var/ossec/bin/agent-auth -m 10.0.0.11 -A SURICATA-SAM
systemctl enable wazuh-agent && systemctl start wazuh-agent
```



WAZUH-MANAGER-SAM — agent_control -l : SURICATA-SAM enregistre avec ID 003, statut Active

5.2 Configuration de la lecture des logs Suricata

L'agent Wazuh est configure pour lire le fichier eve.json de Suricata en format JSON :

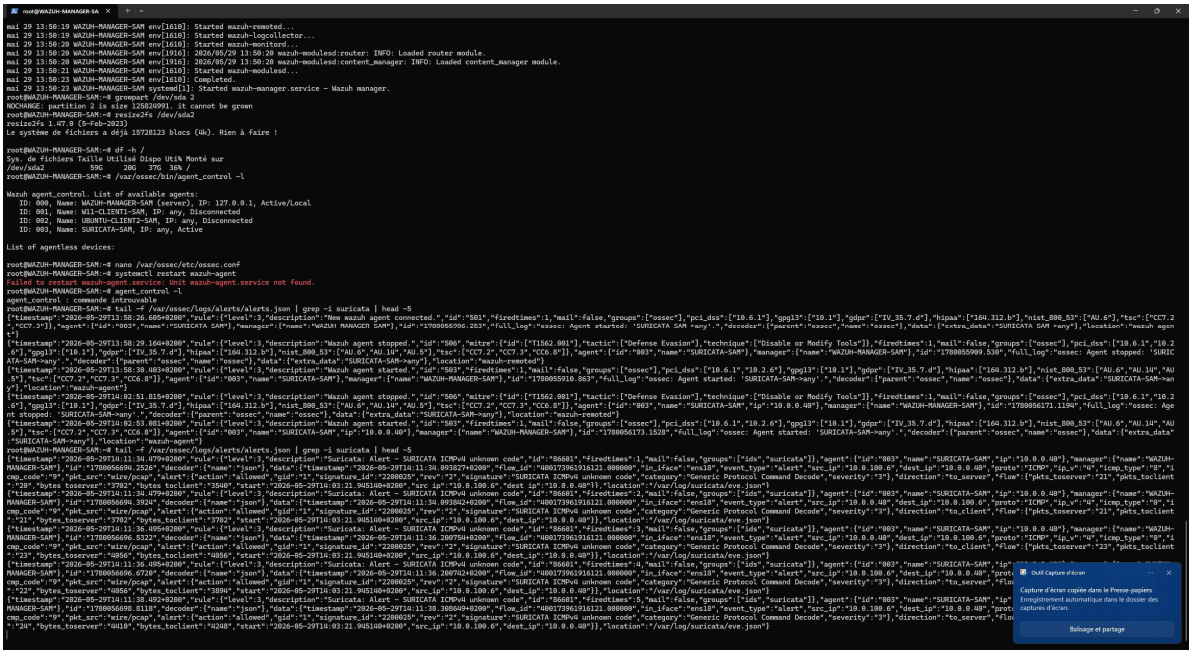
```
# Dans /var/ossec/etc/ossec.conf, ajouter avant </ossec_config> :
<localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>
```

```
systemctl restart wazuh-agent
```

5.3 Verification des alertes dans Wazuh

Les alertes Suricata remontent dans Wazuh avec le groupe 'ids' et la regle 86601. Verification sur le Manager :

```
tail -f /var/ossec/logs/alerts/alerts.json | grep -i suricata | head -5
```



WAZUH-MANAGER-SAM — alerts.json : alertes Suricata remontees avec groups:[ids,suricata], agent SURICATA-SAM (ID 003), signature SURICATA ICMPv4 unknown code

6. Mode IPS — Prevention et blocage actif

6.1 Principe du mode IPS avec nfqueue

En mode IPS, Suricata s'intercale dans la pile reseau Linux via nfqueue (Netfilter Queue). Contrairement au mode IDS ou Suricata recoit une copie du trafic, en mode IPS le trafic passe obligatoirement par Suricata avant d'etre transmis ou bloque.

Etape	Mode IDS	Mode IPS
1 — Trafic	Copie via af-packet	Trafic redirige via iptables → nfqueue
2 — Analyse	Suricata analyse la copie	Suricata analyse le paquet reel
3 — Decision	Alerte uniquement	Accept ou Drop du paquet
4 — Impact	Aucun sur le trafic	Paquet bloque si regle match

6.2 Creation du service suricata-ips

Un service systemd dedie est cree pour gerer le mode IPS avec la protection SSH incluse :

```
# /etc/systemd/system/suricata-ips.service
[Unit]
Description=Suricata IPS mode
After=network.target

[Service]
ExecStartPre=/sbin/iptables -I INPUT 1 -p tcp --dport 22 -j ACCEPT
ExecStartPre=/sbin/iptables -I OUTPUT 1 -p tcp --sport 22 -j ACCEPT
ExecStartPre=/sbin/iptables -A INPUT -j NFQUEUE --queue-num 0
ExecStartPre=/sbin/iptables -A OUTPUT -j NFQUEUE --queue-num 0
ExecStartPre=/sbin/iptables -A FORWARD -j NFQUEUE --queue-num 0
ExecStart=/usr/bin/suricata -c /etc/suricata/suricata.yaml -q 0
ExecStopPost=/sbin/iptables -D INPUT -p tcp --dport 22 -j ACCEPT
ExecStopPost=/sbin/iptables -D OUTPUT -p tcp --sport 22 -j ACCEPT
ExecStopPost=/sbin/iptables -D INPUT -j NFQUEUE --queue-num 0
ExecStopPost=/sbin/iptables -D OUTPUT -j NFQUEUE --queue-num 0
ExecStopPost=/sbin/iptables -D FORWARD -j NFQUEUE --queue-num 0
Restart=on-failure
```

Note : Le port SSH (22) est exclu du nfqueue pour eviter la perte de la connexion d'administration lors du demarrage du mode IPS.

6.3 Regle de blocage personnalisee

Une regle de test est creee dans /var/lib/suricata/rules/test-ips.rules pour valider le blocage actif des pings en provenance de SECURITY-SAM :

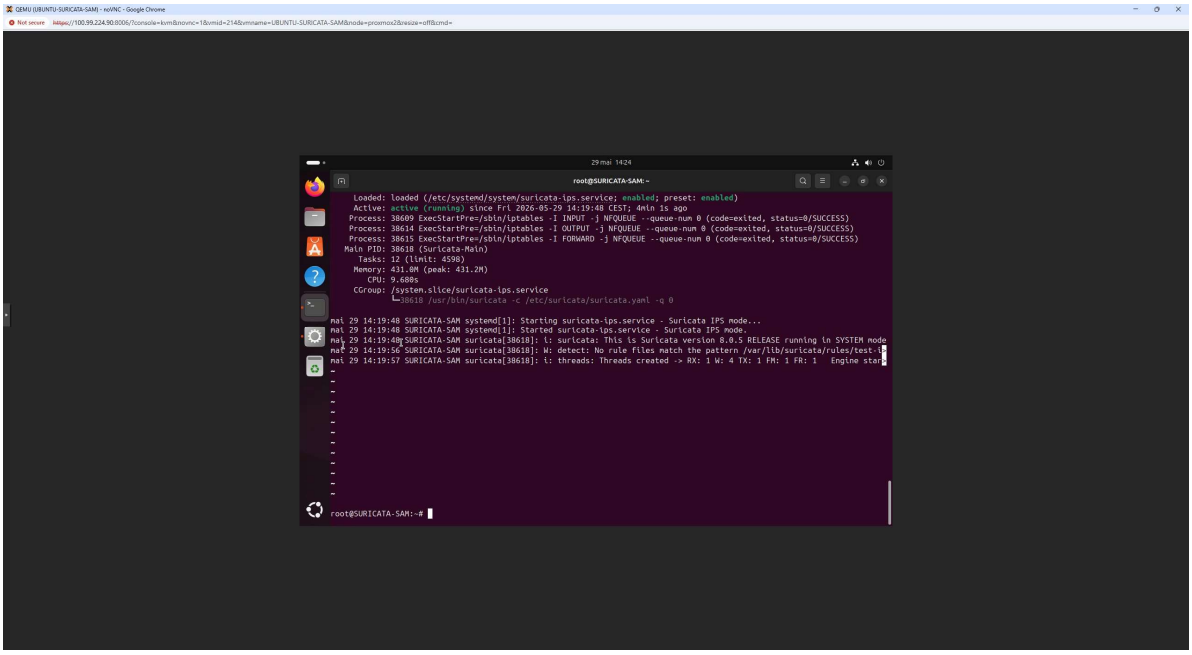
```
drop icmp 10.0.100.6 any -> 10.0.0.40 any (msg:"IPS - Bloc ping SECURITY-
SAM"; sid:9000001; rev:1;)
```

La regle est ajoutee dans suricata.yaml :

```
rule-files:
  - suricata.rules
  - test-ips.rules
```

6.4 Demarrage du service IPS

```
systemctl daemon-reload
systemctl enable suricata-ips
systemctl start suricata-ips
```



SURICATA-SAM — suricata-ips.service active (running), nfqueue configure, regles iptables appliquees

```
root@SURICATA-SAM: ~
samuel@SURICATA-SAM:~$ sudo -i
[sudo] Mot de passe de samuel :
root@SURICATA-SAM:~# tail -20 /var/log/suricata/suricata.log
[38624 - RX-NFQ#0] 2026-05-29 14:27:52 Notice: nfq: (RX-NFQ#0) Treated: Pkts 2535, Bytes 2228983, Errors 0
[38624 - RX-NFQ#0] 2026-05-29 14:27:52 Notice: nfq: (RX-NFQ#0) Verdict: Accepted 2516, Dropped 18, Replaced 0
[38618 - Suricata-Main] 2026-05-29 14:27:52 Info: counters: Alerts: 0
[38860 - Suricata-Main] 2026-05-29 14:27:53 Notice: suricata: This is Suricata version 8.0.5 RELEASE running in SYSTEM m
ode
[38860 - Suricata-Main] 2026-05-29 14:27:53 Info: cpu: CPUs/cores online: 4
[38860 - Suricata-Main] 2026-05-29 14:27:53 Info: exception-policy: master exception-policy set to: auto
[38860 - Suricata-Main] 2026-05-29 14:27:53 Info: nfq: NFQ running in standard ACCEPT/DROP mode
[38860 - Suricata-Main] 2026-05-29 14:27:53 Info: suricata: Preparing unexpected signal handling
[38860 - Suricata-Main] 2026-05-29 14:27:53 Info: conf: Running in live mode, activating unix socket
[38860 - Suricata-Main] 2026-05-29 14:27:53 Info: logopenfile: fast output device (regular) initialized: fast.log
[38860 - Suricata-Main] 2026-05-29 14:27:53 Info: logopenfile: eve-log output device (regular) initialized: /var/log/sur
icata/eve.json
[38860 - Suricata-Main] 2026-05-29 14:27:53 Info: logopenfile: stats output device (regular) initialized: stats.log
[38860 - Suricata-Main] 2026-05-29 14:28:01 Info: detect: 2 rule files processed. 50298 rules successfully loaded, 0 rul
es failed, 0 rules skipped
[38860 - Suricata-Main] 2026-05-29 14:28:01 Info: threshold-config: Threshold config parsed: 0 rule(s) found
[38860 - Suricata-Main] 2026-05-29 14:28:01 Info: detect: 50303 signatures processed. 1288 are IP-only rules, 4490 are i
nspecting packet payload, 44289 inspect application layer, 110 are decoder event only
[38860 - Suricata-Main] 2026-05-29 14:28:02 Info: unix-manager: unix socket '/var/run/suricata/suricata-command.socket'
[38864 - RX-NFQ#0] 2026-05-29 14:28:02 Info: nfq: binding this thread 0 to queue '0'
[38864 - RX-NFQ#0] 2026-05-29 14:28:02 Info: nfq: setting queue length to 4096
[38864 - RX-NFQ#0] 2026-05-29 14:28:02 Info: nfq: setting nfnl bufsize to 6144000
[38860 - Suricata-Main] 2026-05-29 14:28:02 Notice: threads: Threads created -> RX: 1 W: 4 TX: 1 FM: 1 FR: 1   Engine st
arted.
root@SURICATA-SAM:~# grep "Starting" /var/log/suricata/suricata.log | tail -3
root@SURICATA-SAM:~#
```

SURICATA-SAM — log de demarrage : NFQ running in standard ACCEPT/DROP mode, 2 rule files processed, 50298 rules loaded, Engine started

7. Tests et validation

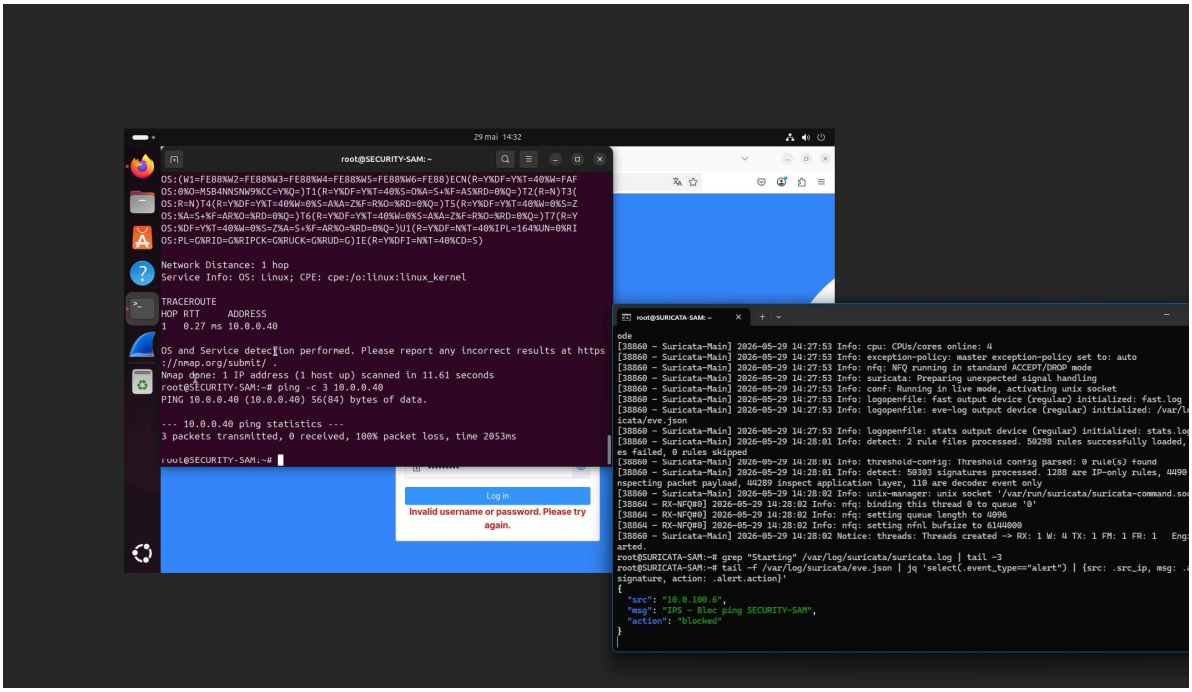
7.1 Test de blocage IPS — ping depuis SECURITY-SAM

Depuis SECURITY-SAM, un ping est envoye vers SURICATA-SAM pour declencher la regle de blocage :

```
ping -c 3 10.0.0.40    # Depuis SECURITY-SAM (10.0.100.6)
```

Simultanement, les alertes sont surveillees sur SURICATA-SAM :

```
tail -f /var/log/suricata/eve.json | jq 'select(.event_type=="alert") |
{src: .src_ip, msg: .alert.signature, action: .alert.action}'
```



Resultat IPS : SECURITY-SAM (gauche) — 3 packets transmitted, 0 received, 100% packet loss. SURICATA-SAM (droite) — action: blocked, msg: IPS - Bloc ping SECURITY-SAM

7.2 Analyse du resultat

Test	Resultat	Observation
Detection IDS (scan Nmap)	Reussi	Alertes generees dans eve.json
Integration Wazuh	Reussi	Agent ID 003 Active, alertes dans alerts.json
Blocage IPS (ping)	Reussi	100% packet loss, action: blocked
Regle personnalisee	Reussi	drop icmp sid:9000001 active
Protection SSH	Reussi	Connexion SSH maintenue en mode IPS

8. Conclusion

Ce projet a permis de mettre en oeuvre un systeme complet de detection et prevention d'intrusion base sur Suricata 8.0.5, integre dans l'ecosysteme de securite du lab mvgroup.local.

- Mode IDS : Suricata analyse passivement le trafic et genere des alertes dans eve.json via les regles Emerging Threats (50298 signatures chargees)
- Integration Wazuh : les alertes Suricata remontent automatiquement dans le SIEM Wazuh (Manager 10.0.0.11, Dashboard 10.0.0.12) via l'agent ID 003
- Mode IPS : en mode nfqueue, Suricata s'intercale dans la pile reseau et bloque activement les paquets correspondant aux regles drop
- Regle personnalisee : validation du blocage avec une signature drop ICMP ciblant SECURITY-SAM — 100% packet loss confirme

Cette implementation demontre la progression naturelle IDS → IPS : d'abord la detection passive pour comprendre le trafic, puis le passage au blocage actif une fois les regles validees. Cette approche est conforme aux bonnes pratiques de securite en production.

Fin du document — Suricata IDS/IPS