Mode Opératoire

Consulter et traiter les alertes Suricata IDS

Code :	MO-SEC-002
Version :	1.1
Date :	16 avril 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	07/04/2026	Création initiale
1.1	16/04/2026	Correction de l'origine du trafic STUN (WebRTC navigateur, non AnyDesk) ; mise à jour catalogue rulesets (68 disponibles) ; ajout section *Origines courantes du STUN* ; renvois croisés vers MO-SEC-004 et MO-NET-001

1 Objet

Ce mode opératoire décrit la procédure de consultation et d'interprétation des alertes générées par **Suricata IDS**, le système de détection d'intrusion déployé sur le pare-feu OPNsense de l'infrastructure BTS SIO du Lycée Jean Lurçat.

Suricata fonctionne en mode **IDS** (*Intrusion Detection System*) : il analyse le trafic réseau en temps réel et génère des alertes lorsqu'il détecte un comportement suspect ou malveillant, sans toutefois bloquer les flux. Ce choix a été retenu pour la phase initiale de déploiement, le temps de calibrer les règles et d'éliminer les faux positifs.

Le document couvre l'accès à l'interface OPNsense, la navigation dans le module Suricata, la lecture des alertes, leur filtrage, l'interprétation des signatures courantes et les actions à entreprendre face aux différents types d'alertes.

2 Champ d'application

Public concerné	Enseignants de l'équipe BTS SIO, administrateurs de l'infrastructure pédagogique
Système	Pare-feu OPNsense (`10.0.112.1`), moteur Suricata en mode IDS
Interfaces surveillées	WAN et LAN
Durée estimée	5–10 minutes (consultation), 15–20 minutes (analyse approfondie)

3 Prérequis

Prérequis

— Compte administrateur OPNsense (identifiants dans le gestionnaire de mots de passe de l'équipe)
— Accès réseau au pare-feu : `10.0.112.1` (câble RJ45 ou tunnel VPN WireGuard)
— Navigateur web récent (Firefox, Chrome ou Edge)

Contexte technique

Suricata a été activé le 6 avril 2026 avec **32 rulesets sur 68 disponibles** (catalogue vérifié le 16/04/2026 via l'API `GET /api/ids/settings/listRulesets`), soit environ 240 000 règles de détection chargées. Les interfaces WAN et LAN sont toutes deux surveillées. Le mode IDS (détection seule, sans blocage) est volontairement conservé pendant la phase de rodage pour éviter de perturber le trafic légitime.

4 Procédure

4.1 Se connecter à l'interface OPNsense

Étape 1 — Accéder à la page de connexion

Ouvrir un navigateur et accéder à :

`https://10.0.112.1`

Le navigateur affiche un avertissement de certificat auto-signé : accepter l'exception pour continuer. La page de connexion OPNsense apparaît.

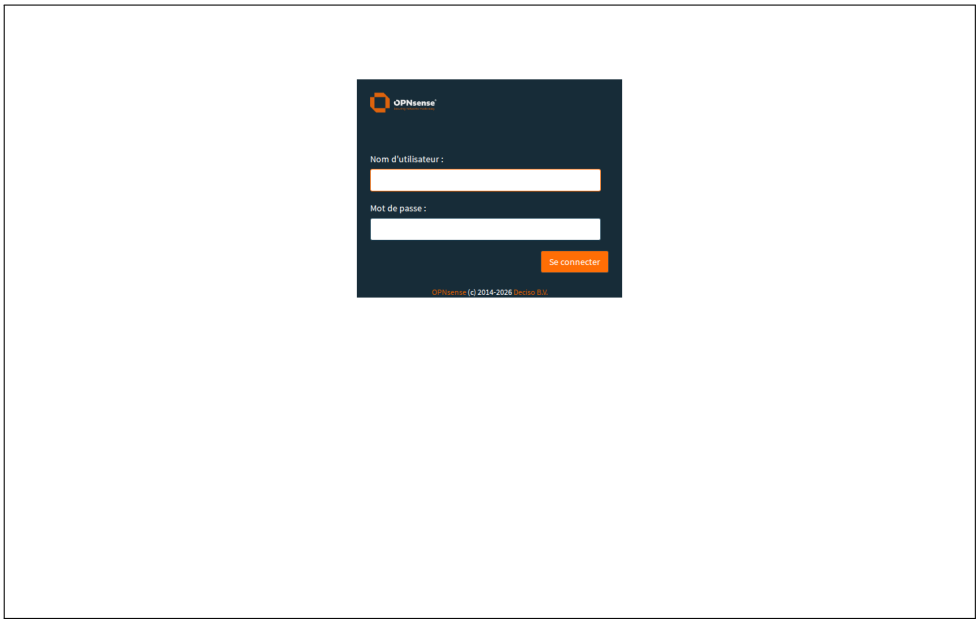

Figure 1 – Page de connexion de l'interface OPNsense

Étape 2 — S'authentifier

Saisir les identifiants :

— *Username* : `admin`

— *Password* : le mot de passe communiqué par l'administrateur

Cliquer sur **Login**. Le tableau de bord OPNsense s'affiche.

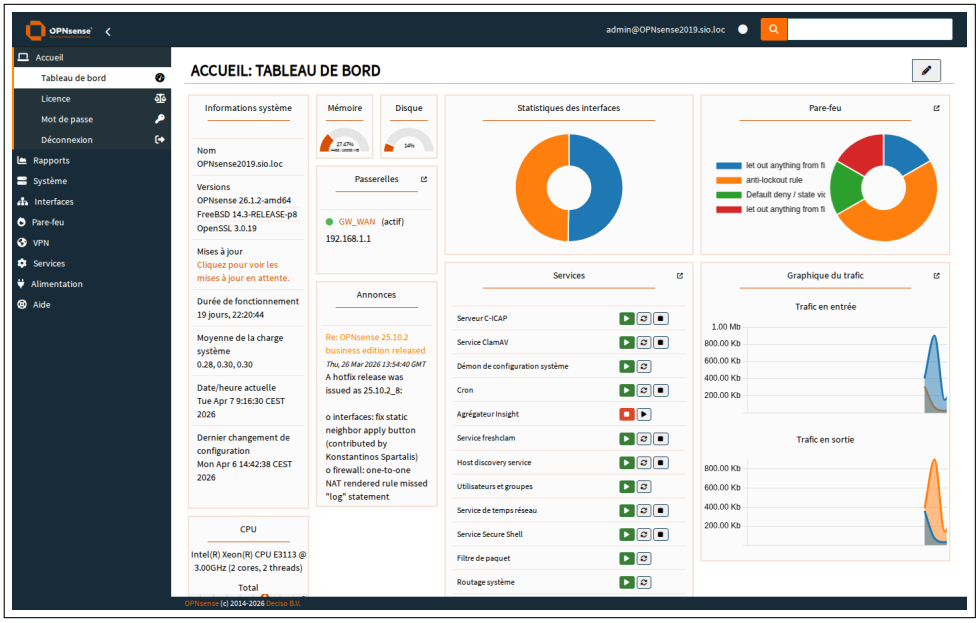

Figure 2 – Tableau de bord OPNsense après authentification

4.2 Accéder au module Suricata IDS

Étape 3 — Ouvrir le module de détection d'intrusion

Dans le menu latéral gauche, naviguer vers :

Services → Intrusion Detection

La page d'administration du module Suricata s'ouvre. Elle comporte plusieurs onglets : **Administration**, **Rules**, **Alerts**, **Policy**, **Schedule**.

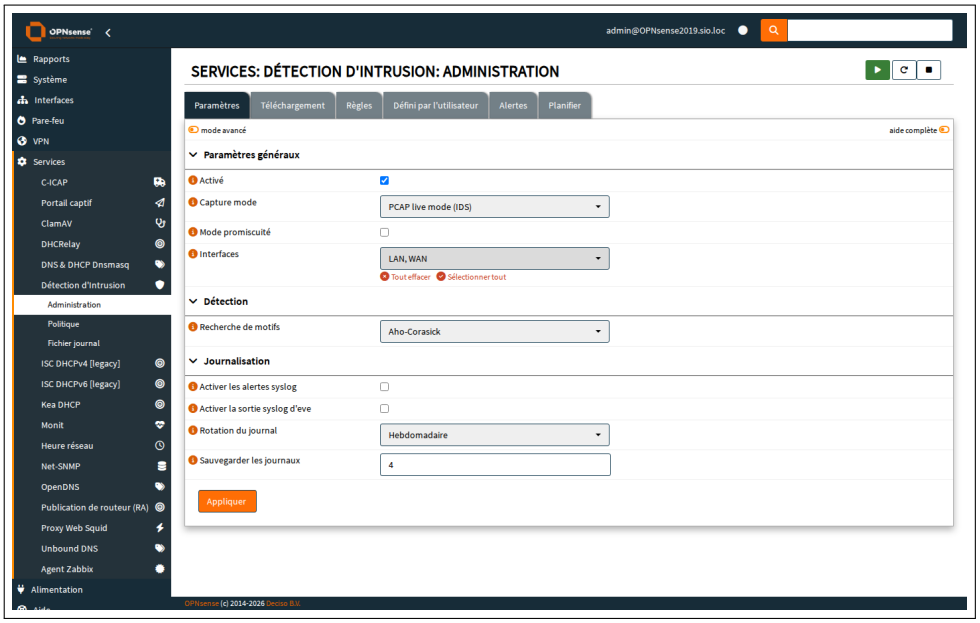

Figure 3 – Page d'administration du module Suricata IDS

Étape 4 — Vérifier l'état du service

Sur l'onglet **Administration**, vérifier que :

— Le champ *Enabled* est coché

— Le champ *IDS mode* indique bien **IDS** (et non IPS)

— Les interfaces `WAN` et `LAN` apparaissent dans *Interfaces*

Si le service n'est pas démarré, cliquer sur le bouton Play (▶) en bas de la page pour le lancer.

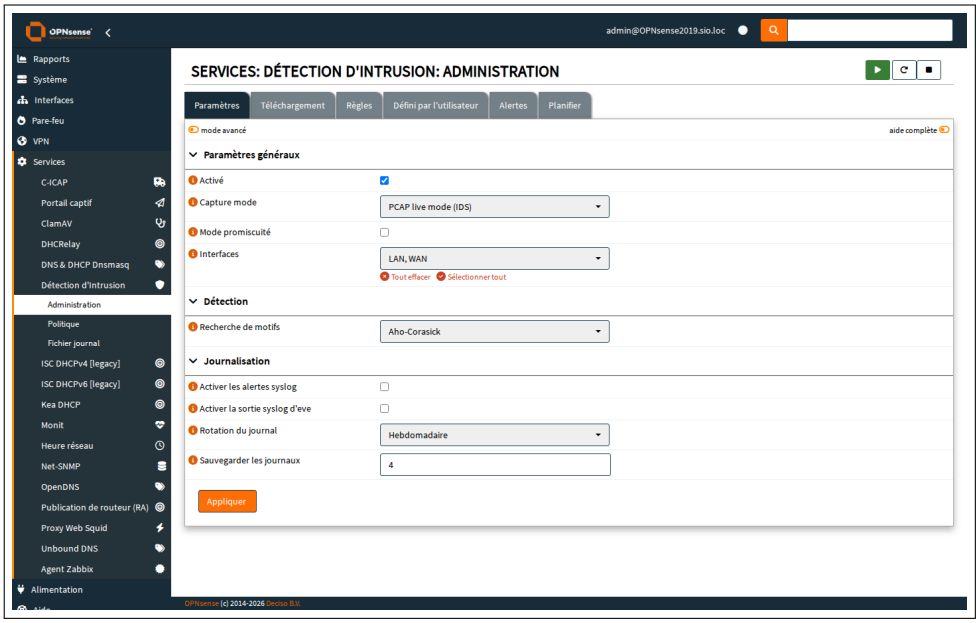

Figure 4 – Paramètres de configuration Suricata

4.3 Consulter les alertes

Étape 5 — Ouvrir l'onglet Alertes

Cliquer sur l'onglet **Alerts** en haut de la page du module de détection d'intrusion. La liste des alertes s'affiche par ordre chronologique inverse (les plus récentes en premier). Chaque ligne correspond à un événement détecté par Suricata.

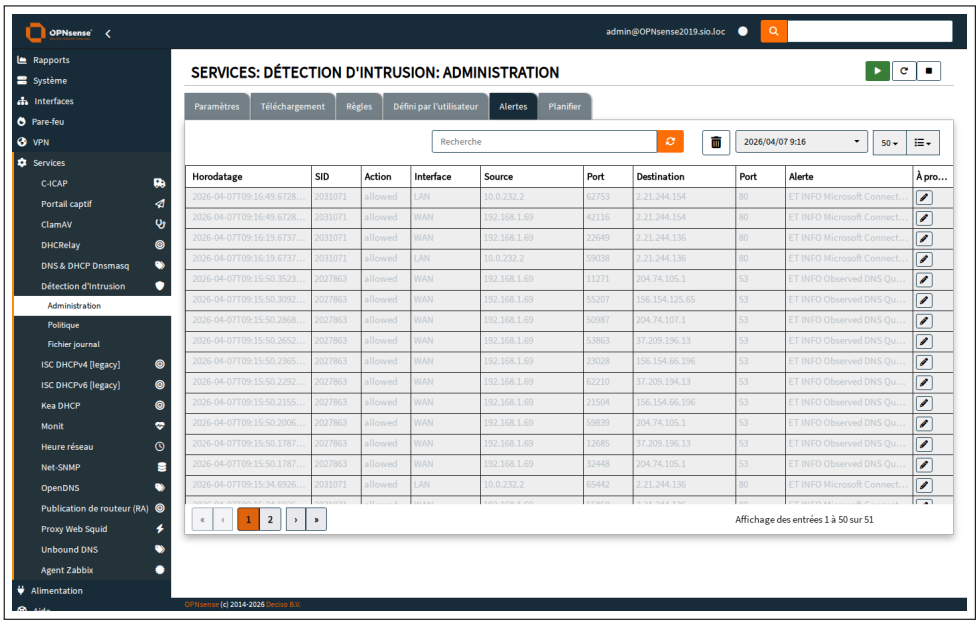

Figure 5 – Liste des alertes Suricata

Étape 6 — Comprendre les colonnes d'une alerte

Chaque alerte affiche les informations suivantes :

Colonne	Description
Date	Horodatage précis de l'événement
SID	Identifiant unique de la règle déclenchée (*Signature ID*)
Signature	Nom de la règle qui a généré l'alerte
Source	Adresse IP et port de l'émetteur du trafic suspect
Destination	Adresse IP et port du destinataire
Severity	Niveau de sévérité (1 = informationnel, 3 = élevé)

Il est normal d'observer un volume important d'alertes, notamment au démarrage. Lors de la mise en service (7 avril 2026), près de 1 500 alertes ont été générées en 8 minutes — dont 98 % correspondaient à du trafic STUN (protocole de traversal NAT) émis par le navigateur **Brave** (candidats ICE WebRTC) sur le poste `10.0.232.29`, comme l'a confirmé l'investigation directe du 16 avril 2026 (cf. § 4.5).

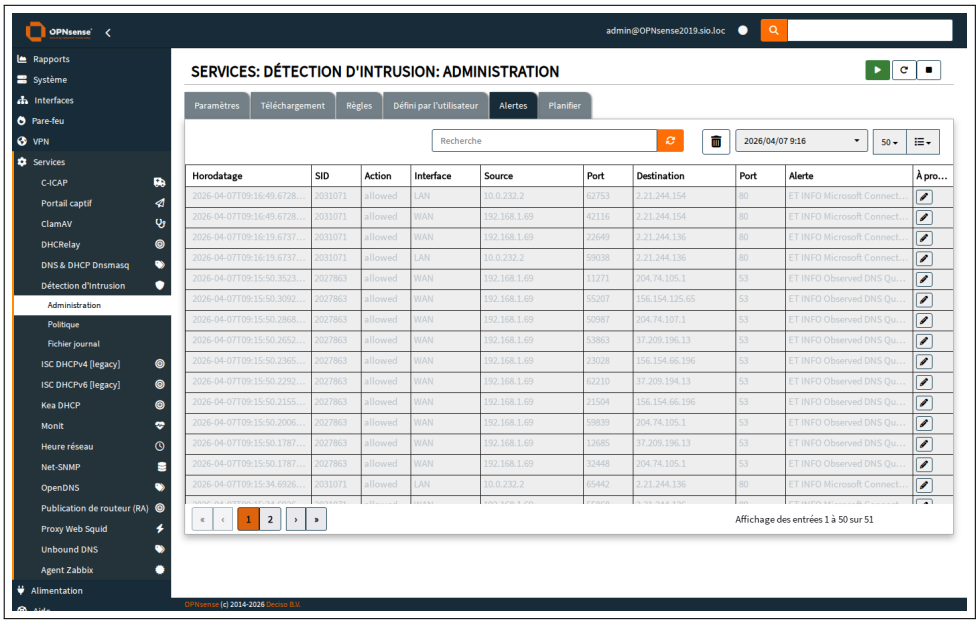

Figure 6 – Détail des alertes avec informations source et destination

⚠ Volume d'alertes initial

Au premier démarrage de Suricata, le nombre d'alertes peut paraître élevé. C'est attendu : le moteur analyse l'intégralité du trafic sur les interfaces WAN et LAN, et de nombreuses règles se déclenchent sur du trafic légitime (mises à jour, outils d'administration distante, etc.). L'objectif est précisément d'identifier ces faux positifs pour affiner la configuration.

4.4 Filtrer les alertes

Étape 7 — Utiliser les filtres de l'interface

L'interface OPNsense propose plusieurs mécanismes de filtrage :

- **Par sévérité** : utiliser le sélecteur en haut de la liste pour n'afficher que les alertes d'un niveau donné (1, 2 ou 3)
- **Par adresse IP** : saisir une adresse dans le champ de recherche pour isoler les alertes provenant d'une machine particulière
- **Par signature (SID)** : rechercher un identifiant de règle spécifique pour voir toutes les occurrences d'un même type d'alerte

💡 Stratégie de tri recommandée

Pour une consultation quotidienne efficace :

1. Commencer par filtrer les alertes de **sévérité 3** (haute) : ce sont les plus critiques
2. Passer ensuite aux alertes de **sévérité 2** (moyenne) : elles méritent un examen
3. Ignorer les alertes de **sévérité 1** (basse) en routine, sauf investigation ciblée

En période normale, l'examen des alertes de sévérité 2 et 3 devrait prendre moins de cinq minutes.

4.5 Interpréter les signatures courantes

Voici les signatures les plus fréquemment rencontrées sur l'infrastructure BTS SIO, avec l'action recommandée pour chacune :

SID	Signature	Sév.	Action recommandée
2033078	ET INFO STUN Binding Request	1	Identifier le poste source. Vérifier la présence d'un *navigateur web ouvrant une page WebRTC* (Meet, Jitsi, Element, Discord web) ou d'un logiciel de visioconférence (Teams, Zoom). Trafic généralement légitime dans un contexte pédagogique. Voir § 4.5.
2013504	ET POLICY GNU/Linux APT User-Agent	1	Normal : mises à jour automatiques des systèmes Debian/Ubuntu. Aucune action requise.
2100498	GPL ATTACK_RESPONSE id check	2	Investiguer la source : un hôte exécute la commande `id` de manière visible sur le réseau. Peut indiquer une activité de reconnaissance post-compromission.
2024364	ET SCAN Nmap	3	Identifier l'utilisateur immédiatement. S'assurer qu'il s'agit d'un exercice pédagogique autorisé. En dehors d'un TP, considérer comme suspect.

Origines courantes du trafic STUN

Le protocole STUN (*Session Traversal Utilities for NAT*, RFC 5389) sert à découvrir l'adresse publique d'un hôte derrière NAT pour établir des sessions UDP *peer-to-peer*. Plusieurs catégories de logiciels en font usage :

Source	Fréquence	Justification
Navigateurs web (Brave, Chrome, Firefox, Edge)	**Très courante**	WebRTC ICE candidates émis automatiquement dès qu'une page contient l'API `RTCPeerConnection` (Meet, Jitsi, Element, Discord web, certains sites de support en ligne)
Logiciels de visioconférence dektop	Courante	Microsoft Teams, Zoom, Slack Calls, Signal Desktop
Outils de collaboration P2P	Occasionnelle	WebTorrent, Syncthing avec relais STUN
Outils d'administration distante	Rare sur cette infra	AnyDesk, TeamViewer (l'usage d'AnyDesk fait l'objet d'une discussion d'équipe en avril 2026, cf. T6)
Trafic suspect	À investiguer	Tunneling P2P détourné, exfiltration via UDP, malware

Démarche d'investigation rapide

Pour distinguer un trafic STUN légitime d'un trafic suspect :

1. Sur le poste source : `ss -unap | grep -E ':(3478|5349|19302)'` — aucun listener dédié sur ces ports = WebRTC opportuniste (bénin)
2. `pgrep -a 'firefox|chrome|brave|teams|slack|discord|jitsi'` — un navigateur ou client RTC en cours = explication immédiate
3. Vérifier l'horaire (heure de cours, pause déjeuner, nuit) — du STUN nocturne sur un poste personnel *sans* navigateur ouvert mérite enquête
4. Comparer la destination IP à la liste des fournisseurs RTC connus (Google `74.125.0.0/16`, Cloudflare `104.16.0.0/12`, Fastly `151.101.0.0/16`) — une destination hors de ces plages à volume élevé est anormale

Cas pratique résolu — 16/04/2026

L'alerte historique « 1 500 STUN en 8 minutes depuis `10.0.232.29` » a été formellement attribuée au navigateur **Brave** après investigation directe sur le poste : aucun listener UDP sur les ports STUN dédiés, aucun socket vers des serveurs STUN tiers, mais 32 processus Brave actifs. Conclusion : candidats ICE émis lors de la visite de pages WebRTC, comportement normal d'un navigateur moderne. La règle SID 2033078 sur cette IP peut être supprimée via une règle `suppress by_src` (cf. MO-SEC-004 § 4.3).

4.6 Consulter les rulesets actifs

Étape 8 — Vérifier les rulesets chargés

Cliquer sur l'onglet **Rules** dans le module de détection d'intrusion.
Cette page affiche l'ensemble des rulesets (jeux de règles) disponibles et leur état : activé ou désactivé. Le nombre de règles contenues dans chaque ruleset est indiqué.

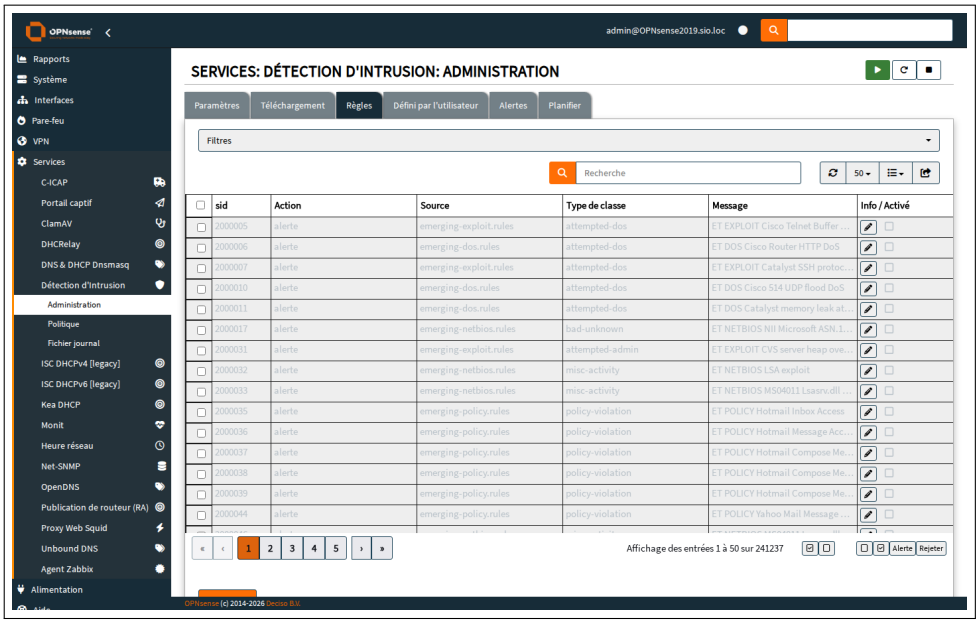

Figure 7 – Rulesets Suricata activés sur OPNsense

Actuellement, **32 rulesets sur 68** sont activés, couvrant les catégories suivantes :

- **ET emerging-*** : règles Emerging Threats (menaces récentes, malwares, exploits)
- **ET policy-*** : politiques de sécurité (logiciels non autorisés, protocoles à risque)
- **ET scan-*** : détection de scans réseau (Nmap, port sweeps)
- **ET info-*** : trafic informatif (DNS, HTTP, mises à jour)

⚠ Ne pas modifier les rulesets sans concertation

L'activation ou la désactivation de rulesets modifie directement le périmètre de détection. Toute modification doit être validée par l'administrateur responsable et documentée. En cas de doute, ne rien changer : il est préférable d'avoir trop d'alertes que d'en rater une.

4.7 Actions possibles face à une alerte

Selon la nature et la sévérité de l'alerte, trois niveaux de réaction s'appliquent :

Action	Sév. typique	Démarche
Ignorer / classer	1	L'alerte correspond à un comportement connu et légitime (mises à jour APT, trafic STUN émis par un navigateur WebRTC ou un client de visio-conférence). La noter comme identifiée. À terme, la règle pourra être désactivée si elle génère trop de bruit.
Investiguer	2	Identifier le poste source (IP → nom machine). Vérifier si l'activité est attendue (TP en cours, maintenance planifiée). Consulter l'enseignant concerné si besoin.
Bloquer / escalader	3	Événement potentiellement malveillant. Identifier l'utilisateur. Si aucune justification pédagogique, isoler le poste du réseau et prévenir le référent infrastructure. Envisager le passage en mode IPS pour cette règle.

Passage en mode IPS

Le mode IPS (*Intrusion Prevention System*) permet à Suricata de **bloquer** le trafic détecté comme malveillant, et non plus seulement de le signaler. Ce passage nécessite une validation préalable de l'administrateur et ne doit être activé qu'après une période suffisante de fonctionnement en mode IDS pour éviter le blocage de trafic légitime.

5 Vérification

Vérification

Après avoir effectué les opérations de ce mode opératoire, vérifier les points suivants :

- ☐ L'interface OPNsense est accessible via `https://10.0.112.1`
- ☐ Le service Suricata est actif (icône verte sur la page d'administration)
- ☐ Les interfaces WAN et LAN sont bien sélectionnées dans la configuration
- ☐ Les alertes sont visibles dans l'onglet **Alerts**
- ☐ Le filtrage par sévérité fonctionne correctement
- ☐ Au moins 32 rulesets sont activés dans l'onglet **Rules**
- ☐ Aucune alerte de sévérité 3 n'est restée sans investigation

Voir aussi

— **MO-SEC-004** — *Gérer Suricata pendant les TP de cybersécurité* (procédure complémentaire pour les séances TP qui génèrent du trafic intrusif légitime)
— **MO-NET-001** — *Vérification post-hardening OPNsense* (cadre général de validation du pare-feu, dont l'IDS est un module)
— **MO-SEC-001** — *Exploitation Wazuh* (corrélation des alertes Suricata vers le SIEM, hors périmètre IDS strict)

6 Dépannage

Problème	Solution
Aucune alerte visible dans l'onglet	Vérifier que le service Suricata est bien démarré (bouton ▶ en bas de la page **Administration**). Contrôler que les interfaces WAN et/ou LAN sont configurées. Après un redémarrage du service, patienter quelques minutes avant l'apparition des premières alertes.
Trop d'alertes de sévérité 1 (bruit)	Filtrer par sévérité ≥ 2 pour la consultation quotidienne. Identifier les signatures récurrentes et évaluer si le ruleset concerné est pertinent pour l'environnement pédagogique. Ne désactiver une règle qu'après validation par l'administrateur.
Le service Suricata ne démarre pas	Vérifier le champ *Enabled* dans **Services** → **Intrusion Detection** → **Administration**. Contrôler les journaux système via **System** → **Log Files** → **General**. Un nombre trop élevé de rulesets activés peut entraîner un dépassement de mémoire.
Service arrêté après un redémarrage d'OPNsense	Vérifier que le paramètre *Enabled* est bien coché dans les paramètres IDS. Si le problème persiste, consulter les journaux du firewall au redémarrage pour identifier un éventuel conflit de ressources.
Interface OPNsense inaccessible	Vérifier la connectivité réseau vers `10.0.112.1`. S'assurer d'être connecté au bon réseau (câble ou VPN WireGuard). Tester avec `ping 10.0.112.1` puis `curl -k https://10.0.112.1`.