Mode Opératoire

Gérer Suricata pendant les TP de cybersécurité

Code :	MO-SEC-004
Version :	1.0
Date :	16 avril 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	16/04/2026	Création initiale

1 Objet

Ce mode opératoire décrit la conduite à tenir vis-à-vis du moteur **Suricata IDS** de l'infrastructure BTS SIO lorsqu'une séance de travaux pratiques de cybersécurité génère du trafic légitimement intrusif (scan de ports, fuzzing, brute-force, exploitation de vulnérabilités sur cibles de laboratoire).

Sans préparation, ces TP saturent l'onglet **Alerts** de plusieurs centaines d'événements de sévérité 2 et 3, ce qui produit deux effets indésirables :

— le bruit pédagogique masque les éventuelles alertes *réelles* concomitantes (compromission, scan extérieur) ;

— l'historique d'alertes devient inexploitable pour la consultation quotidienne décrite dans **MO-SEC-002**.

Le présent document propose un cadre opérationnel en trois temps — avant, pendant, après la séance — pour isoler le trafic TP du trafic légitime, sans altérer durablement la posture de détection.

Mode actuel = IDS, pas IPS

Suricata est déployé en mode **IDS** (`PCAP live mode`, configuration vérifiée le 16 avril 2026) : il *détecte* mais ne *bloque pas*. Conséquence directe : aucun TP n'est techniquement entravé par la présence du moteur. La préparation décrite ici vise uniquement la lisibilité des alertes. Si le moteur passe un jour en mode IPS, ce mode opératoire devra être complété d'une section sur la désactivation *stricte* des règles bloquantes pendant les TP.

2 Champ d'application

Public concerné	Enseignants intervenant dans les TP de cybersécurité BTS SIO option SISR (modules *Sécurité des réseaux* et *Détection d'intrusion*)
Système	Pare-feu OPNsense (`10.0.112.1`), moteur Suricata en mode IDS, 32 rulesets actifs sur 68 disponibles
Salle TP	Plage IP des postes étudiants (typiquement `10.0.232.0/24`)
Cibles autorisées	VMs de laboratoire dédiées (Metasploitable, DVWA, machines isolées du réseau de production)
Durée estimée	10 min de préparation, 5 min de restauration

3 Prérequis

Prérequis

- Compte administrateur OPNsense (identifiants dans le coffre Vaultwarden de l'équipe)
- Accès réseau au pare-feu `10.0.112.1` (câble RJ45 ou tunnel VPN WireGuard)
- Connaissance de **MO-SEC-002** (consultation des alertes Suricata)
- Liste des postes participants (IP ou plage) communiquée en amont par l'enseignant responsable du TP
- Périmètre d'exercice validé (cibles autorisées, durée, types d'attaques pratiquées)

Aucune attaque hors périmètre

Les alertes ignorées ou supprimées pendant un TP doivent l'être *uniquement* pour les IPs et SID pédagogiques prévus. Toute alerte d'origine externe au TP, même concomitante, doit rester visible et traitée selon **MO-SEC-002**.

4 Procédure

4.1 Avant le TP — préparation

Étape 1 — Recenser les postes participants

Demander à l'enseignant responsable la liste des postes étudiants utilisés pour le TP. Convertir en plage CIDR si possible (ex. `10.0.232.0/24` pour la salle complète, `10.0.232.10-25` pour un sous-ensemble).

Noter également :

— l'horaire prévu (début / fin) ;

— les types d'attaques (scan, brute-force, exploitation, sniffing) ;

— les machines cibles (IPs des VMs de laboratoire).

Cette information sert de référentiel pour la suite du MO et pour l'entrée du journal de bord en § 4.6.

Étape 2 — Se connecter à l'interface OPNsense

Ouvrir `http://10.0.112.1` et s'authentifier avec le compte administrateur (cf. MO-SEC-002 § 4.1). Naviguer vers :

Services → Intrusion Detection → Administration

Vérifier que le service est en état *Running* (point vert) avant toute modification.

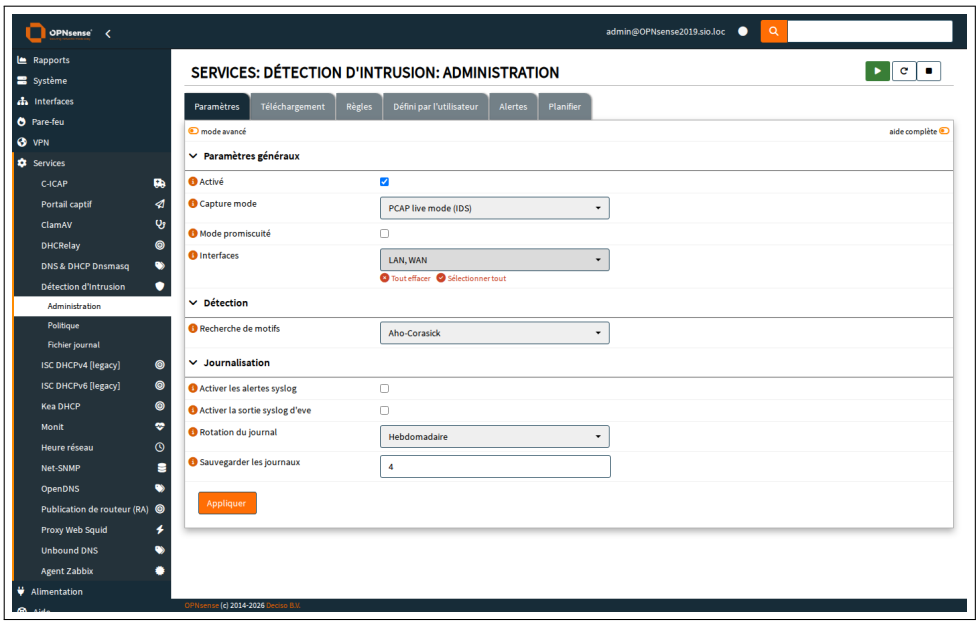

Figure 1 – État du module Suricata avant intervention — service actif, mode PCAP IDS

Étape 3 — Snapshot de l'état des rulesets

Avant toute désactivation, exporter la liste des rulesets actifs pour pouvoir restaurer fidèlement à l'issue du TP. Depuis un poste connecté au LAN, exécuter :

```
curl -s -b cookies.txt \
    'http://10.0.112.1/api/ids/settings/listRulesets' \
    | jq '.rows[] | select(.enabled=="1") | .filename' \
    > /tmp/suricata_rulesets_avant.txt
wc -l /tmp/suricata_rulesets_avant.txt
```

Ce fichier servira de référence pour la restauration en § 4.5. Une méthode équivalente via l'UI consiste à prendre une capture d'écran de l'onglet **Rules** avec les rulesets activés.

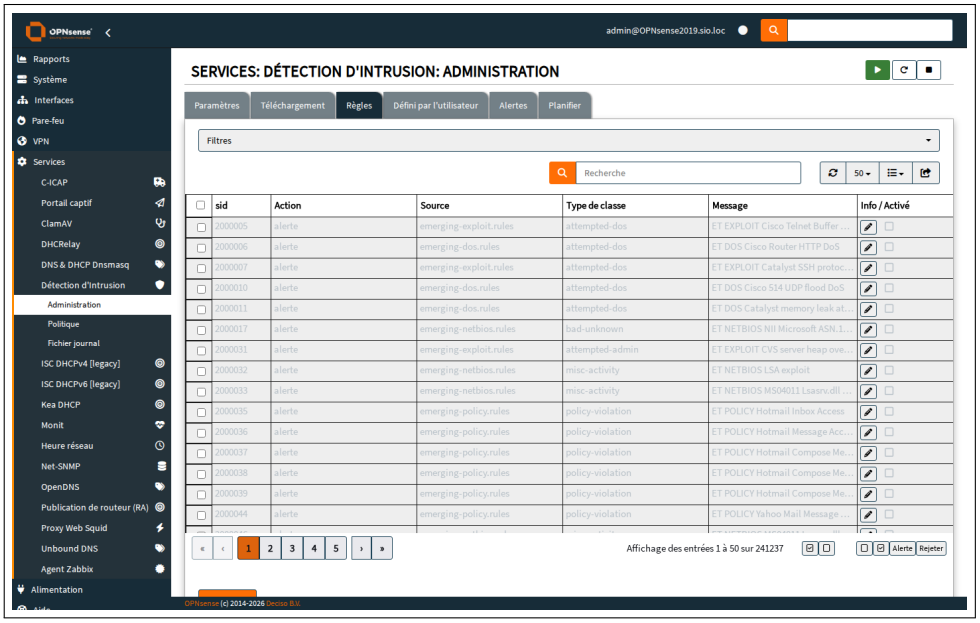

Figure 2 – Onglet *Rules* avant le TP — 32 rulesets actifs sur 68 disponibles

4.2 Désactiver les rulesets bruyants pour le TP

Étape 4 — Identifier les rulesets concernés par le type de TP

Selon la nature du TP, certains rulesets génèrent un volume disproportionné d'alertes attendues. Le tableau ci-dessous indique les rulesets à désactiver *temporairement* :

Type de TP	**Rulesets à désactiver temporairement**
Scan Nmap, recon réseau	`ET scan.rules`, `ET policy.rules` (partiellement)
Brute-force SSH/HTTP (Hydra)	`ET attack_response.rules`, `ET hunting.rules`
Exploitation Metasploit	`ET exploit.rules`, `ET shellcode.rules`
Sniffing / ARP poisoning	Aucun (écoute passive non détectée par Suricata)
Web app testing (DVWA, OWASP Juice Shop)	`ET web_specific_apps.rules`, `ET web_server.rules`

Étape 5 — Désactiver un ruleset depuis l'UI

Dans l'onglet **Rules**, localiser le ruleset cible (utiliser le filtre de recherche). Décocher la case *Enabled* sur la ligne correspondante, puis cliquer sur Save.

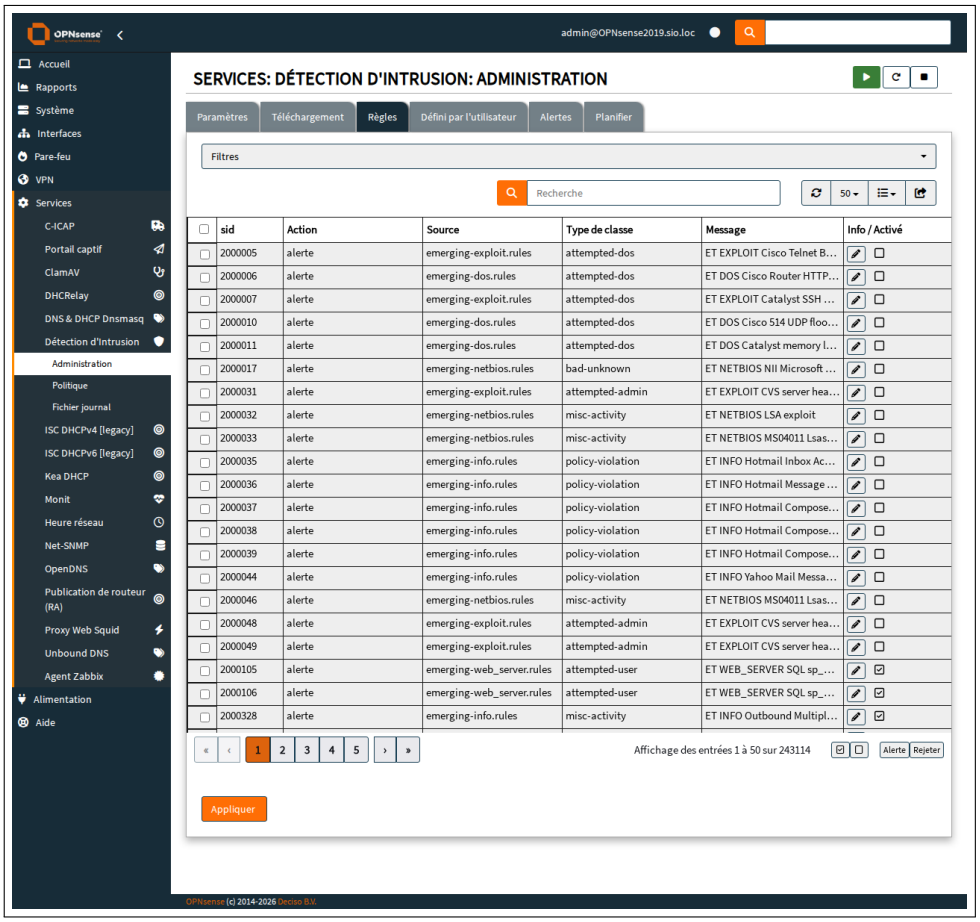

Figure 3 – Désactivation du ruleset `ET scan.rules` pour un TP Nmap

Étape 6 — Recharger la configuration

Après avoir modifié l'ensemble des rulesets pertinents, retourner sur l'onglet **Administration** et cliquer sur Apply en haut à droite (icône 🔄).

L'opération prend environ 30 secondes à 1 minute selon le nombre de règles. Pendant ce temps, le service est redémarré : aucune alerte n'est capturée durant cette fenêtre courte.

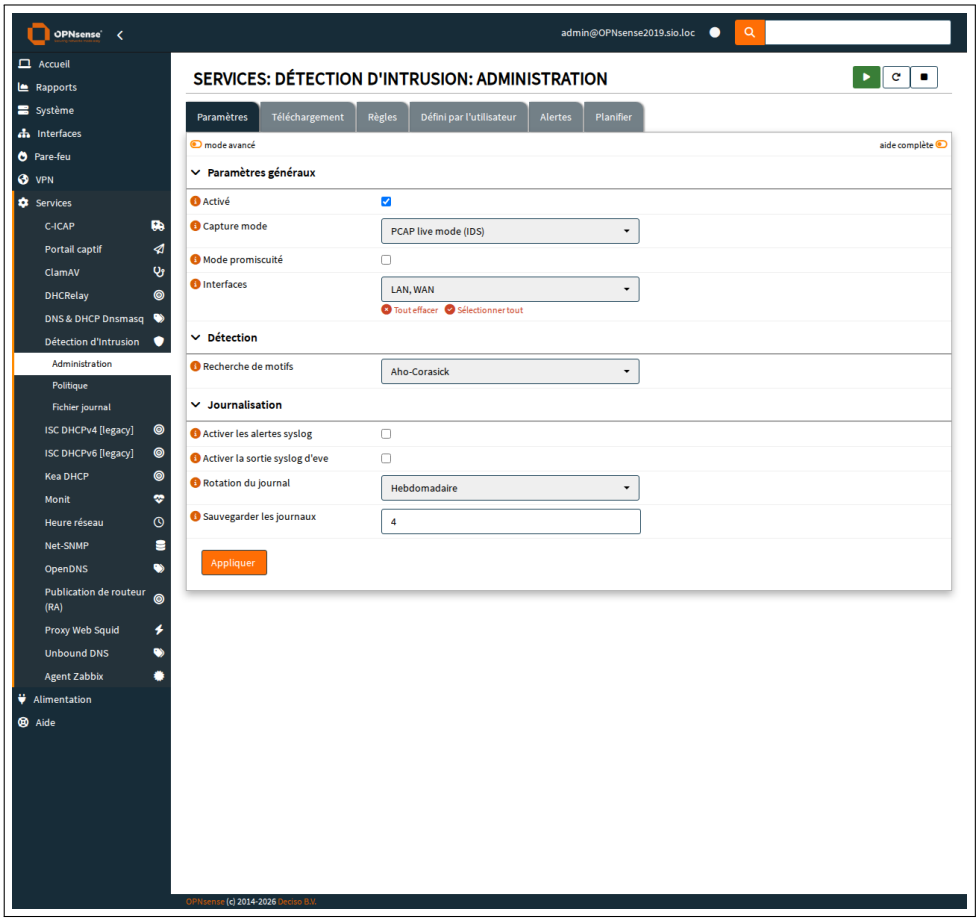

Figure 4 – Application des modifications de rulesets

Alternative ciblée — suppress par SID

Plutôt que de désactiver un ruleset entier, il est possible de **supprimer** l'alerte uniquement pour certaines IP source via une règle `suppress`. Plus chirurgical, mais plus long à configurer pour un TP ponctuel. Voir § 4.3 ci-dessous.

4.3 Ajouter des règles d'exception (alternative chirurgicale)

Étape 7 — Accéder à la page des exceptions

Dans le module IDS, naviguer vers :

Services → Intrusion Detection → User defined

Cette page permet de définir des actions personnalisées par SID, source ou destination, sans toucher aux rulesets globaux.

Étape 8 — Créer une suppression d'alerte par SID et IP source

Cliquer sur **+ Add** et remplir :

— *Action* : `suppress`

— *SID* : identifiant de la règle (ex. `2024364` pour ET SCAN Nmap)

— *Track* : `by_src` (par adresse source)

— *IP* : plage TP (ex. `10.0.232.0/24`)

— *Description* : `TP Nmap salle 232 - 16/04/2026`

Sauvegarder, puis appliquer la configuration depuis l'onglet **Administration**.

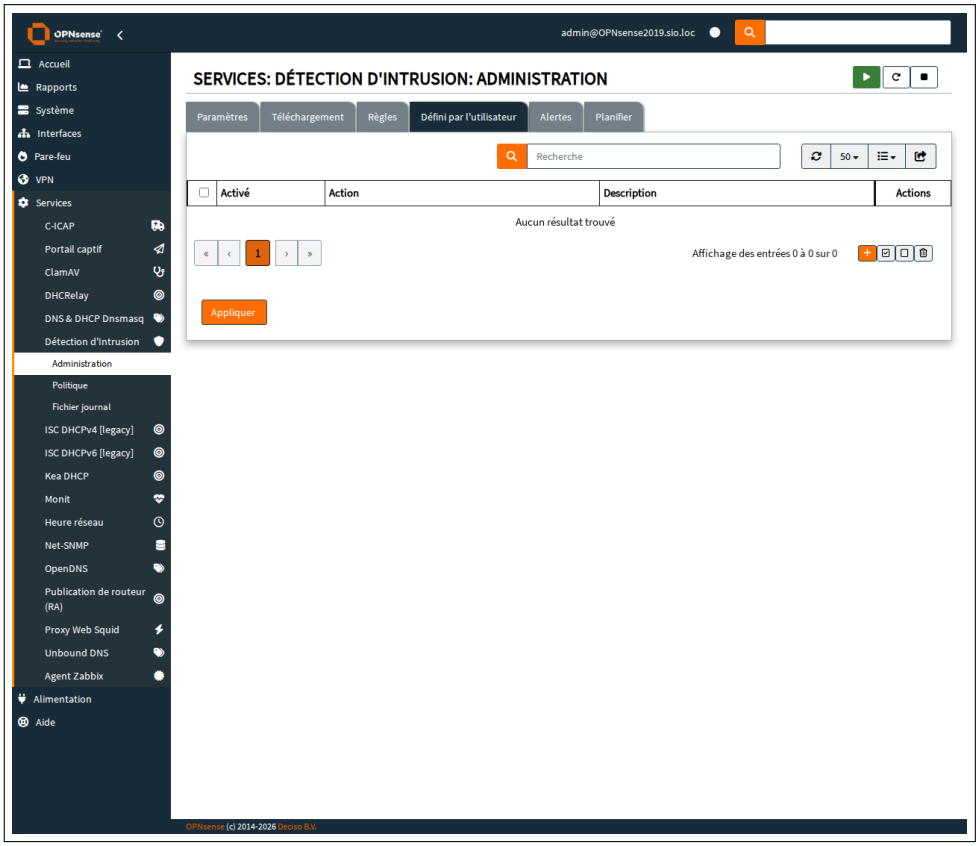

Figure 5 – Création d'une règle de suppression ciblée

Quand préférer suppress à la désactivation de ruleset

Utiliser `suppress` si :

— le TP ne concerne qu'un sous-ensemble de SID dans un ruleset ;

— d'autres règles du même ruleset doivent rester actives sur d'autres IP ;

— l'enseignant souhaite garder une trace même partielle (ex. SID logué, alerte non remontée dans l'UI).

Préférer la désactivation complète du ruleset si :

— le TP est court ($< 1\,\text{h}$) et concerne un nombre élevé de SID ;

— la classe couvre l'ensemble de la salle (gain de temps).

4.4 Pendant le TP — surveillance parallèle

Étape 9 — Filtrer les alertes hors TP

Garder ouvert l'onglet **Alerts** dans une fenêtre séparée. Appliquer le filtre suivant pour exclure le trafic de la plage TP :

```
!10.0.232.0/24
```

Toute alerte qui apparaît *malgré* ce filtre provient d'une autre source et doit être traitée selon **MO-SEC-002**.

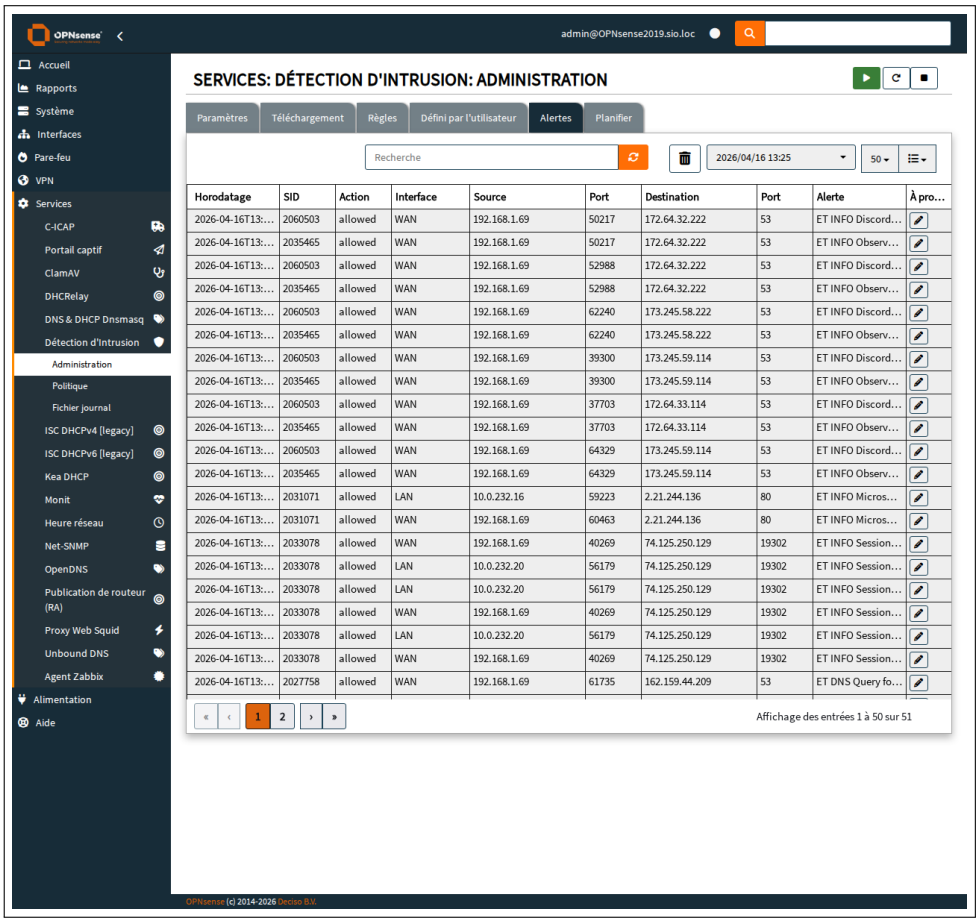

Figure 6 – Alertes hors périmètre TP pendant la séance

Étape 10 — Surveiller la sévérité 3

Appliquer un second filtre par sévérité : *Severity = 3*. Toute alerte de sévérité 3 hors périmètre TP justifie une interruption immédiate du TP et une investigation (cf. MO-SEC-002 § 4.7).

⚠ Ne pas se fier à la quantité

Un volume *nul* d'alertes hors plage TP n'est pas une garantie d'absence d'incident. Suricata peut être saturé par le trafic TP même après désactivation des rulesets concernés. Vérifier la charge CPU du moteur dans **Lobby** → **Dashboard**.

4.5 Après le TP — restauration de l'état nominal

Étape 11 — Réactiver les rulesets désactivés

Retourner dans **Rules** et réactiver chaque ruleset listé dans le snapshot pris en § 4.1. La case *Enabled* doit être à nouveau cochée pour chaque ruleset concerné.

Vérifier en comparant avec le fichier `/tmp/suricata_rulesets_avant.txt` ou avec la capture d'écran de référence.

Étape 12 — Supprimer les règles d'exception créées

Retourner dans **User defined**. Cocher chaque règle créée pour le TP (repérables à la description `TP ...-- date`) et cliquer sur Delete.

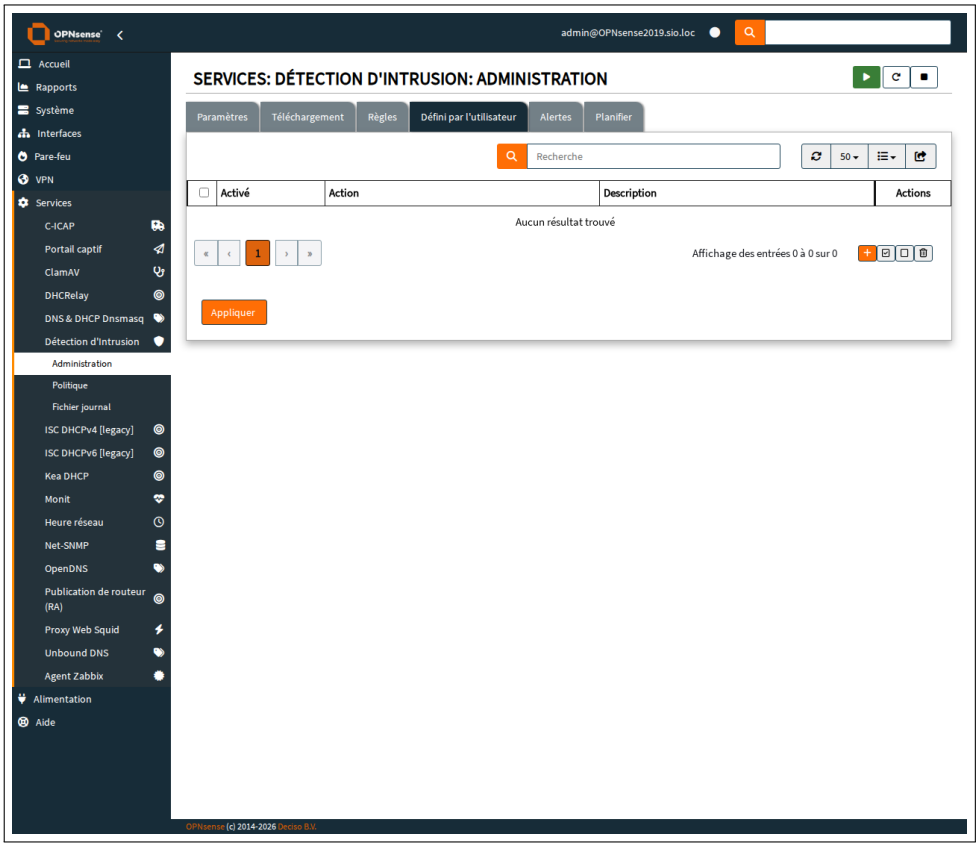

Figure 7 – Suppression des exceptions créées pour le TP

Étape 13 — Recharger la configuration

Onglet **Administration**, cliquer sur Apply. Attendre la fin du redémarrage du moteur (point vert).
Vérifier le compteur de rulesets actifs : il doit être identique à celui noté avant le TP (32 sur 68 dans la configuration de référence d'avril 2026).

4.6 Documenter la séance

Étape 14 — Créer une entrée dans le journal de bord

Sur le wiki interne (https://wiki.legrand-tech.fr/fr/journal-de-bord), ajouter une entrée datée contenant :

— Date, horaire, salle TP
— Nom de l'enseignant et intitulé du TP
— Plage IP impactée
— Liste des rulesets et SID neutralisés
— Heure de restauration de l'état nominal
— Éventuelles alertes hors périmètre observées pendant la séance

Cette traçabilité permet de corréler a posteriori des incidents potentiels avec des fenêtres TP, et d'identifier les rulesets récurrement neutralisés (candidats à un ajustement permanent).

Modèle d'entrée journal

```
### TP Nmap -- Salle 232 -- 16/04/2026 14:00-16:00

- Enseignant : <NOM>
- Module : SISR-S2 -- Detection d'intrusion
- Plage IP TP : 10.0.232.0/24 (16 postes)
- Cible : VM Metasploitable 10.0.232.250
- Rulesets desactives : ET scan.rules
- SID supprimes : aucun (ruleset entier)
- Restauration : 16/04 16:05
- Alertes hors perimetre : 0
```

5 Cas types

5.1 TP Nmap (scan de ports)

— Désactiver `ET scan.rules` (couvre la plupart des techniques de scan TCP/UDP/SYN)
— Optionnellement, suppress sur SID 2024364 (*ET SCAN Nmap*) si seuls quelques postes scannent
— Après TP : vérifier qu'aucune alerte `ET SCAN` n'est restée dans la file post-réactivation

5.2 TP Hydra (brute-force SSH ou HTTP)

— Désactiver `ET attack_response.rules` (alertes sur tentatives de connexion répétées)
— Si Hydra cible une cible HTTPS interne, désactiver aussi `ET hunting.rules`
— Garantir que la cible est bien une VM de laboratoire isolée

5.3 TP Metasploit (exploitation de vulnérabilités)

— Désactiver `ET exploit.rules` et `ET shellcode.rules`
— Valider en amont la liste des exploits utilisés avec l'enseignant (certains modules déclenchent encore d'autres rulesets)
— Après TP, prendre 5 minutes pour relire les alertes capturées *avant* la désactivation : elles documentent les signatures que les étudiants ont déclenchées

5.4 TP Wireshark (sniffing passif)

— Aucune action requise sur Suricata : l'écoute passive n'émet aucun trafic détectable
— Profiter de la séance pour faire découvrir aux étudiants l'onglet **Alerts** comme outil complémentaire de Wireshark

5.5 TP Web (DVWA, OWASP Juice Shop)

— Désactiver `ET web_specific_apps.rules`
— Selon les modules pratiqués (XSS, SQLi), `ET web_server.rules` peut aussi générer du bruit
— Confirmer que la cible (DVWA) est sur une VM ou un conteneur isolé, jamais sur l'infrastructure de production

6 Vérification

Vérification

Après la séance, contrôler les points suivants :

- ☐ Le service Suricata est *Running* (point vert dans **Administration**)
- ☐ Le nombre de rulesets actifs correspond à l'état avant TP (32 sur 68 par défaut)
- ☐ Aucune règle dans **User defined** n'a un libellé `TP ...` restant
- ☐ Les alertes après restauration concernent du trafic légitime de l'infrastructure (pas de SID pédagogique récent provenant de la plage TP)
- ☐ Une entrée a été créée dans le journal de bord du wiki
- ☐ L'enseignant responsable du TP a confirmé la fin de la séance

7 Dépannage

Problème	Solution
Après **Apply**, le service ne redémarre pas	Consulter **System** → **Log Files** → **General** pour identifier l'erreur. Cause fréquente : une règle `suppress` mal formée (SID inexistant ou IP invalide). Supprimer la règle fâcheuse et réappliquer.
Le compteur de rulesets ne revient pas à 32 après restauration	Comparer ligne à ligne le contenu de l'onglet **Rules** avec la capture prise en § 4.1. Un ruleset peut avoir été oublié. Réactiver manuellement et appliquer.
Volume d'alertes anormalement élevé après la séance	Vérifier que la plage TP ne génère plus de trafic intrusif (poste oublié, scan en arrière-plan). Filtrer les alertes par IP et investiguer les sources résiduelles.
Aucune alerte capture pendant la séance, même hors plage TP	Vérifier que les interfaces WAN et LAN sont toujours cochées dans **Administration**. Un **Apply** sur une configuration incomplète peut désélectionner les interfaces dans certaines versions d'OPNsense.
Conflit avec une autre séance en parallèle	Coordonner avec les autres enseignants : un seul TP cybersécu actif à la fois sur l'infrastructure pour éviter d'enchevêtrer les exceptions. Sinon, isoler chaque TP par un sous-réseau distinct et utiliser exclusivement `suppress by_src`.

Voir aussi

— **MO-SEC-002** : Consulter et traiter les alertes Suricata IDS (procédure quotidienne)
— **MO-NET-001** : Vérification post-hardening OPNsense (cadre de validation générale)
— **MO-SEC-001** : Exploitation Wazuh (corrélation alertes Suricata → SIEM, hors périmètre IDS strict)