LYCÉE LOUIS PERGAUD
BTS SIO 2

JANVIER
2026

COMPTE RENDU

Mise en place d'un IDS sur OPNSense

RÉALISÉ PAR
GENSSE Mathéo

LYCÉELOUISPERGAUD

LYCÉE LOUIS PERGAUD
BTS SIO 2

SOMMAIRE

C’EST QUOI UN IDS ? DANS QUEL CONTEXTE L’UTILISE T’ON ACTUELLEMENT ?

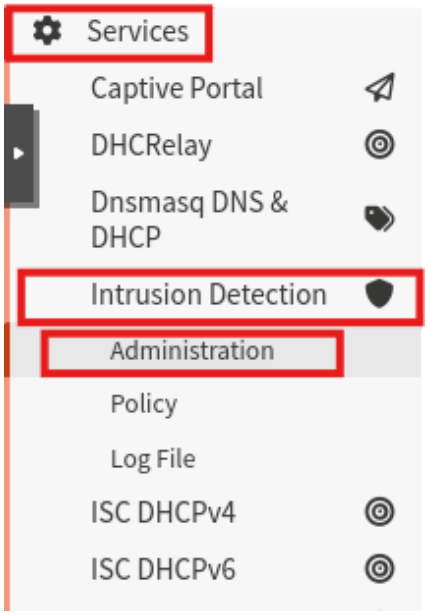
Un IDS (Système de Détection d'Intrusion) est un dispositif de sécurité qui surveille, analyse et alerte sur les activités suspectes ou malveillantes au sein d'un réseau ou sur un système, sans les bloquer activement.

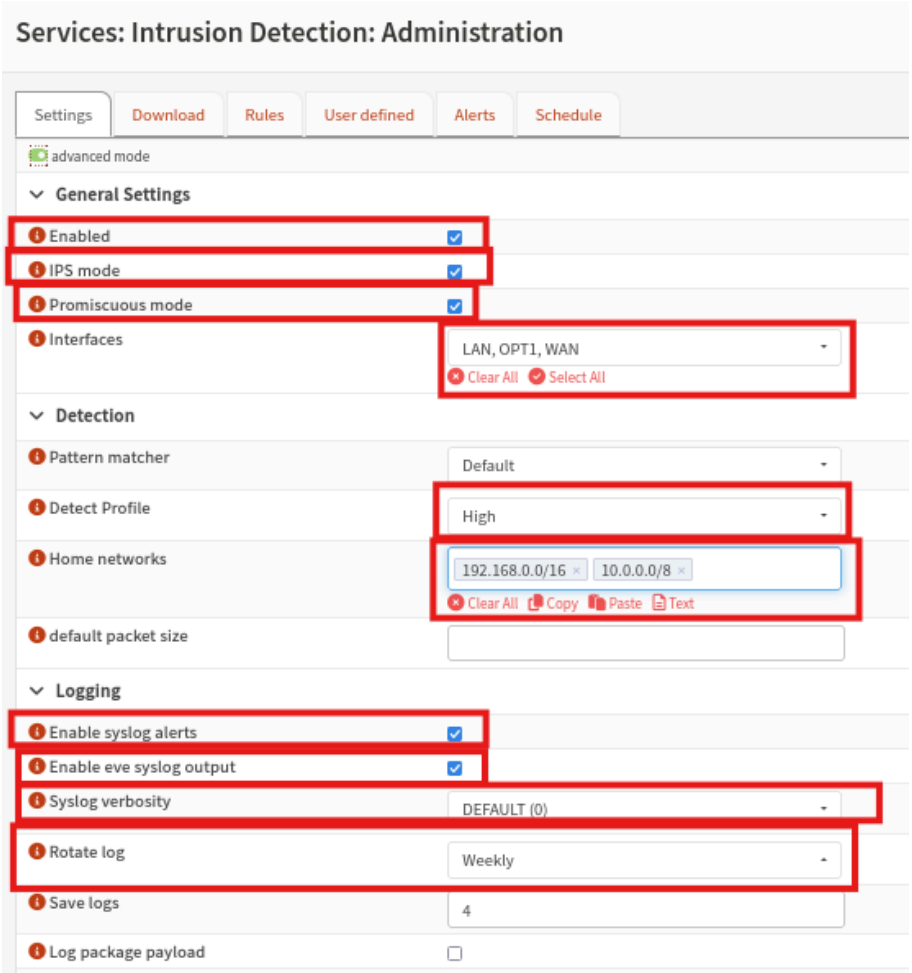
Actuellement dans notre cas, on souhaite être en mesure de détecter rapidement les tentatives d’intrusion dans le Système d’Information de l’entreprise GSB. L’objectif étant d’être en mesure d’intervenir rapidement et de détecter les failles potentiels l'entrée du SI de l’entreprise sur l’interface WAN (172.31.13.1) la plus exposé à internet.
C’est pourquoi nous allons mettre en place un IDS sur le pare feu externe du réseau de l’entreprise GSB afin grâce à l’IDS de loguer les activités jugées suspectes.

MISE EN PLACE D'UN IDS SUR OPNSENSE

COMMENT ON ACTIVE UN IDS SUR UN PARE FEU OPNSENSE ?

Afin d'activer l'IDS dans le pare-feu, se rendre dans l'onglet Service > Intrusion Detection > Administration





Dans la section IDS activez le mode avancé puis renseignez les champs comme ci-contre :

- Activation de IDS
- Activation mode IPS
- Activation du mode promiscuité pour capturer tout paquet passant par les interfaces définies par la suite.

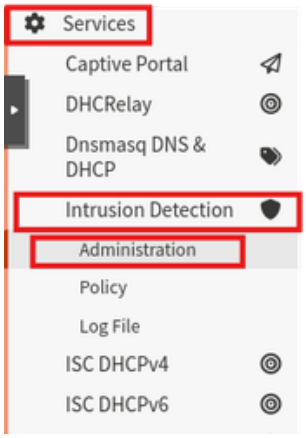
COMMENT ON ACTIVE UN IDS SUR UN PARE FEU OPNSENSE ?

- Ajout des 3 interfaces d’écoutes
- Mise du profil de détection en Elevée
- Activation de la journalisation des alertes / événements détectés comme suspect
- Ajout des réseaux dit internes
- Configuration de l’intervalle de rotation de régénération des logs

MISE EN PLACE D'UN IDS SUR OPNSENSE

MISE EN PLACE DES RÈGLES DE DÉTECTION DES INTRUSIONS

Place maintenant à la mise en place des règles de détection des intrusions. Pour se faire, toujours dans :

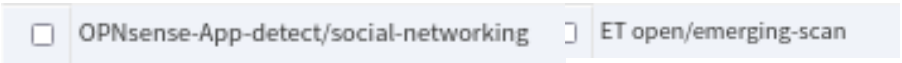


On se rend maintenant dans la section de téléchargement des modules de règles :

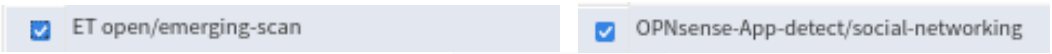
Parmi la liste, recherchez les modules souhaitez. Dans notre cas, on voudra :

- Avertir et considérer une connexion à Facebook comme étant suspect
- Avertir et considérer un test de port NMAP comme étant une tentative d'intrusion

Ainsi, on va télécharger 2 modules :



Afin de télécharger ces modules, les sélectionner de la sorte :



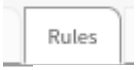
Puis activer la sélection avec :

Enfin Télécharger :

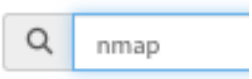
Une fois le module téléchargé, on doit activer les règles associées souhaitées.

Dans notre cas on activera toutes les règles contenus dans le modules open/emerging-scan dont le message contient NMAP. Puis pour Facebook on activera le module qui renvoie une alerte lors du passage d'un package DNS (port 53) demandant résolution de facebook.com.

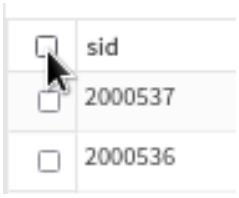
Donc, se rendre dans l'onglet Rules cette fois ci :



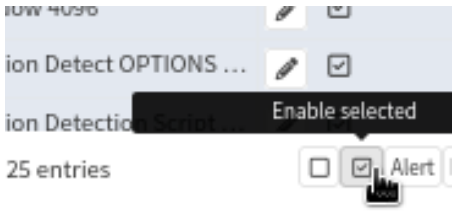
Puis recherchez NMAP dans la barre de recherche :



Une fois que vous avez fait Entrer cliquez ici pour tout sélectionner :



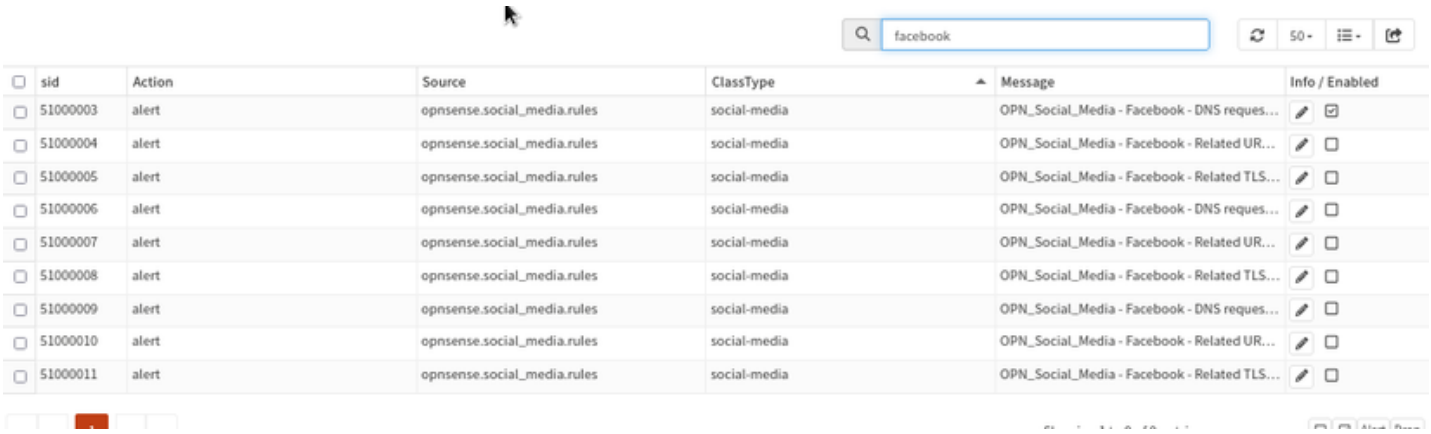
Puis en bas à droite, cliquez comme ci contre pour activer toutes les règles sélectionnés :



MISE EN PLACE DES RÈGLES DE DÉTECTION DES INTRUSIONS

Enfin n'oubliez pas d'appliquer les modifications : 

Faire de même pour la recherche et l'activation de la règle relative aux résolutions DNS de facebook.com. On recherche Facebook, on prend UNIQUEMENT ici, la règle de résolutions DNS de Facebook puis on l'active.



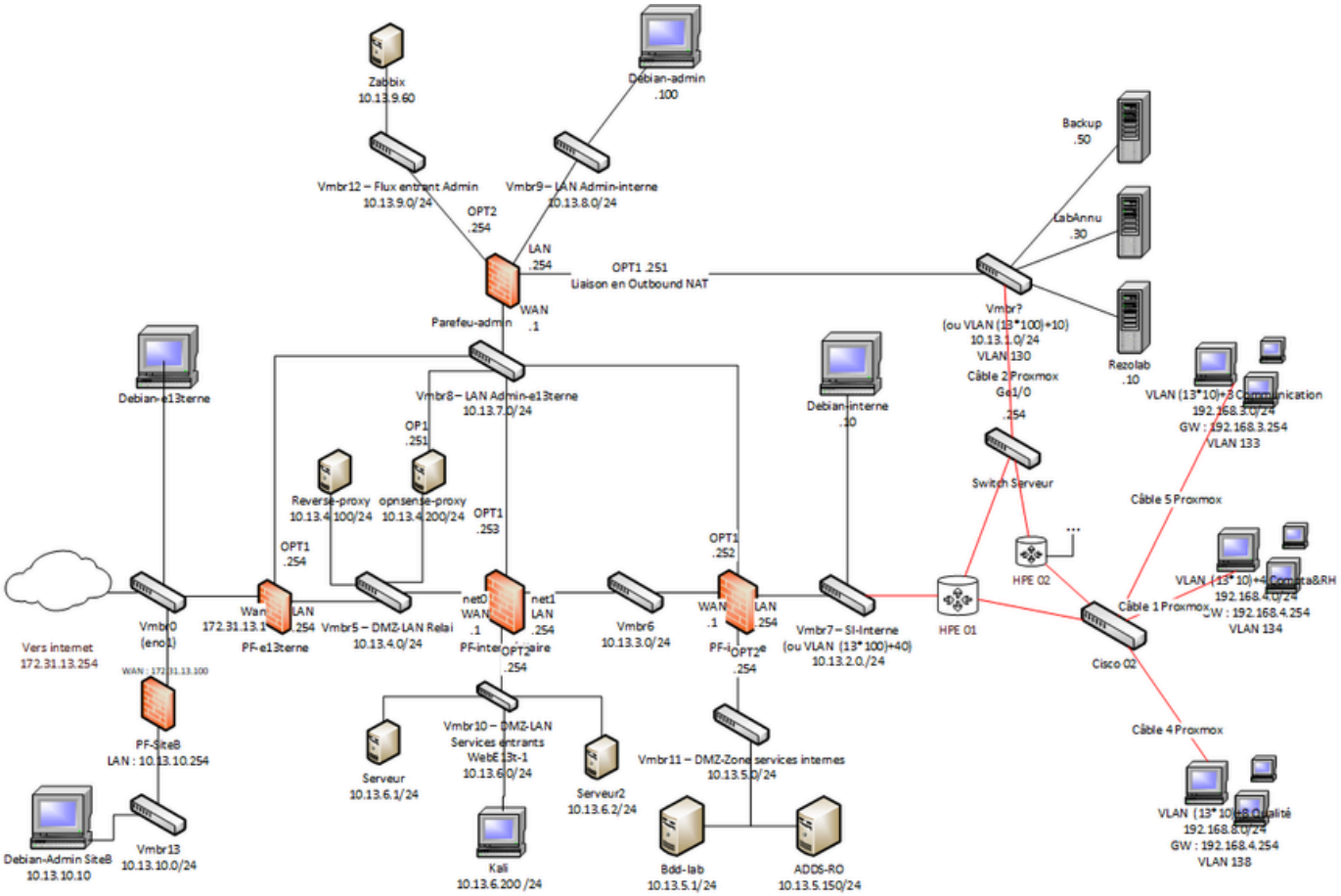
Chaque règle possède une fonction particulière pour détecter et alerter dans les logs.

MISE EN PLACE D'UN IDS SUR OPNSENSE

VÉRIFICATION DU BON FONCTIONNEMENT VIA UNE CAPTURE DE TRAMES

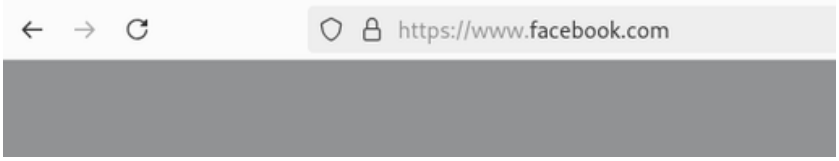
Maintenant que la mise en place des règles d'IDS est effective, place à la vérification du bon fonctionnement de celle-ci. On écoute donc sur toutes les interfaces donc les test sont libres.

Commençons par le test de détection lorsqu'un utilisateur (de l'entreprise GSB par exemple) se rend sur le site de Facebook. Pour l'exemple on a choisi (de façon temporaire évidemment) de procéder à l'ouverture de fluxs en "Open Bar" sur l'interface OPT1 de notre pare-feu externe ainsi que sur la LAN du pare-feu admin afin de laisser passer les flux WEB vers l'extérieur (initialement Bloquer).
On rappelle que le réseau de GSB se présente de la façon suivante :

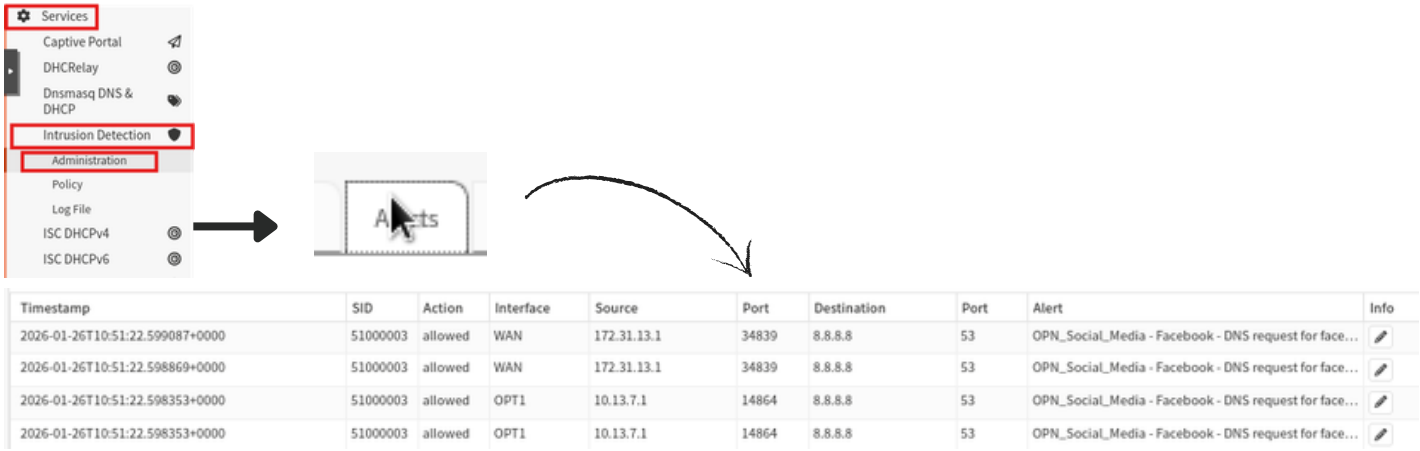


VÉRIFICATION DU BON FONCTIONNEMENT VIA UNE CAPTURE DE TRAMES

Sur la Debian d'administration, ouvrir dans un navigateur le site facebook.com :



Puis, sur votre Debian d'administration toujours, retournez sur l'interface Web du pare-feu externe pour vérifier que la requête à bien été loguer détecter en intrusion dans l'IDS. Pour se faire



La requête à bien été loguer, cela fonctionne bien.

Place à la vérification pour les analyse de port NMAP. Connectez-vous sur une machine externe (ici Debian externe) puis ouvrir le CMD puis taper :

```
utilisateur@Debian12-1-XP:~$ su root
Mot de passe :
```

Une fois en administrateur, lancer l'analyse :

```
root@Debian12-1-XP:/home/utilisateur# nmap -sS -T4 172.31.13.1 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2026-01-26 12:49 CET
Nmap scan report for 172.31.13.1
Host is up (0.00037s latency).
All 1000 scanned ports on 172.31.13.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: BC:24:11:4C:83:8F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.20 seconds
root@Debian12-1-XP:/home/utilisateur#
```

VÉRIFICATION DU BON FONCTIONNEMENT VIA UNE CAPTURE DE TRAMES

Une fois lancé et terminé, de retour dans :

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2026-01-26T11:49:13.266980+0000	2009582	allowed	LAN	172.31.13.100	63606	10.13.6.1	443	ET SCAN NMAP -sS window 1024	

Et on remarque bien que le scan à été logué