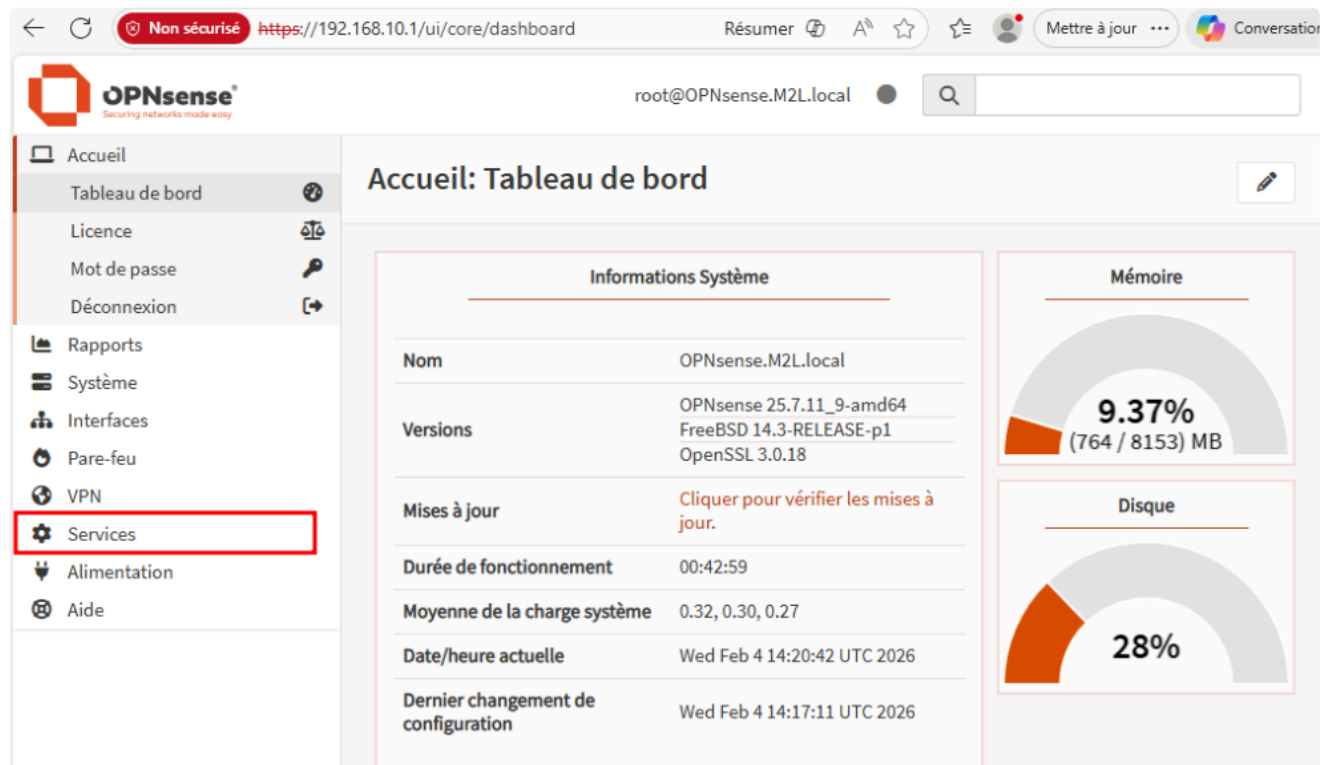


0 - Prérequis

- Un serveur avec OPNSense d'installé.
- une connection internet.
- Un accès a l'interface web de OPNSense.

1 - Activation du Service de OPNSense

On navigue dans le menu de la détection d'intrusion :



The screenshot shows the OPNSense web interface. The browser address bar indicates the URL <https://192.168.10.1/ui/core/dashboard>. The user is logged in as `root@OPNsense.M2L.local`. The left sidebar menu is visible, with the 'Services' option highlighted by a red box. The main content area displays the 'Accueil: Tableau de bord' (Dashboard) with several widgets:

- Informations Système**: A table listing system details.

Nom	OPNsense.M2L.local
Versions	OPNsense 25.7.11_9-amd64 FreeBSD 14.3-RELEASE-p1 OpenSSL 3.0.18
Mises à jour	Cliquer pour vérifier les mises à jour.
Durée de fonctionnement	00:42:59
Moyenne de la charge système	0.32, 0.30, 0.27
Date/heure actuelle	Wed Feb 4 14:20:42 UTC 2026
Dernier changement de configuration	Wed Feb 4 14:17:11 UTC 2026
- Mémoire**: A gauge showing 9.37% usage (764 / 8153 MB).
- Disque**: A gauge showing 28% usage.

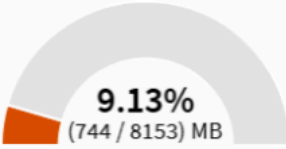
- Accueil
- Rapports
- Système
- Interfaces
- Pare-feu
- VPN
- Services
 - Portail Captif
 - DHCRelay
 - Dnsmasq DNS & DHCP
 - Détection d'Intrusion**
 - Administration
 - Politique
 - Fichier journal
 - ISC DHCPv4
 - ISC DHCPv6
 - Kea DHCP

Accueil: Tableau de bord

Informations Système

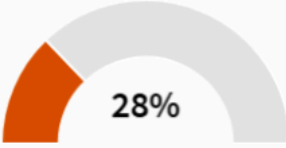
Nom	OPNsense.M2L.local
Versions	OPNsense 25.7.11_9-amd64 FreeBSD 14.3-RELEASE-p1 OpenSSL 3.0.18
Mises à jour	Cliquer pour vérifier les mises à jour.
Durée de fonctionnement	00:43:49
Moyenne de la charge système	0.37, 0.32, 0.27
Date/heure actuelle	Wed Feb 4 14:21:32 UTC 2026
Dernier changement de configuration	Wed Feb 4 14:17:11 UTC 2026

Mémoire




9.13%
(744 / 8153) MB

Disque



28%

On coche la case activé et on sélectionne les interface a surveiller :


root@OPNsense.M2L.local

- Interfaces
- Pare-feu
- VPN
- Services
 - Portail Captif
 - DHCRelay
 - Dnsmasq DNS & DHCP
 - Détection d'Intrusion
 - Administration**
 - Politique
 - Fichier journal
 - ISC DHCPv4

Services: Détection d'Intrusion: Administration

Paramètres
Téléchargement
Règles
Défini par l'utilisateur
Alertes
Planifier

mode avancé
aide complète

▼ Réglages généraux

- Activé**
- Mode IPS
- Mode promiscuité
- Interfaces** DMZ, GUEST, HYPV, INFO, MZ, VPN, WAN

✖ Tout effacer ✔ Sélectionner tout

On laisse la configuration par défaut du reste et on clique sur appliquer en bas de la page :

✖ Tout effacer
✔ Sélectionner tout

▼ Détection

i Recherche de motifs

▼ Journalisation

i Activer les alertes syslog

 Envoyer les alertes au journal du système au format de journal rapide. Cela ne modifiera pas la journalisation des alertes utilisée par le produit lui-même.

i Activer la sortie syslog d'eve

i Rotation du journal

i Sauvegarder les journaux

Appliquer

Ensuite dans l'onglet téléchargement on peut installer des règles générales pré-faites. Dans notre cas, je vais toutes les sélectionner et cliquer sur Activer la sélection:

Paramètres
Téléchargement
Règles
Défini par l'utilisateur
Alertes
Planifier

i Ensemble de règles

Activer la sélection
Désactiver la sélection

<input checked="" type="checkbox"/>	Description	Dernière mis...	Activé	Éditer
<input checked="" type="checkbox"/>	abuse.ch/Feodo Tracker	non-installé	✖	
<input checked="" type="checkbox"/>	abuse.ch/SSL Fingerprint Blacklist	non-installé	✖	
<input checked="" type="checkbox"/>	abuse.ch/SSL IP Blacklist	non-installé	✖	
<input checked="" type="checkbox"/>	abuse.ch/ThreatFox	non-installé	✖	
<input checked="" type="checkbox"/>	abuse.ch/URLhaus	non-installé	✖	
<input checked="" type="checkbox"/>	ET open/3coresec	non-installé	✖	
<input checked="" type="checkbox"/>	ET open/botcc	non-installé	✖	








Dans l'onglet règles, on peut bien voir que nos packs de règles sont bien installés. On peut toutes les sélectionner et les activer:

Paramètres Téléchargement Règles Défini par l'utilisateur Alertes Planifier

Filtres

Recherche

50

<input type="checkbox"/>	sid	Action	Source	Type de classe	Message	Info / Activé
<input type="checkbox"/>	2000016	alerte	emerging-de...	attempted-dos	ET DELETED ...	 <input type="checkbox"/>
<input type="checkbox"/>	2000017	alerte	emerging-ne...	bad-unknown	ET NETBIOS ...	 <input type="checkbox"/>
<input type="checkbox"/>	2000024	alerte	emerging-de...	trojan-activity	ET DELETED ...	 <input type="checkbox"/>
<input type="checkbox"/>	2000025	alerte	emerging-ad...	pup-activity	ET ADWARE_...	 <input type="checkbox"/>
<input type="checkbox"/>	2000026	alerte	emerging-ad...	pup-activity	ET ADWARE_...	 <input type="checkbox"/>
<input type="checkbox"/>	2000031	alerte	emerging-ex...	attempted-a...	ET EXPLOIT ...	 <input type="checkbox"/>
<input type="checkbox"/>	2000032	alerte	emerging-ne...	misc-activity	ET NETBIOS ...	 <input type="checkbox"/>