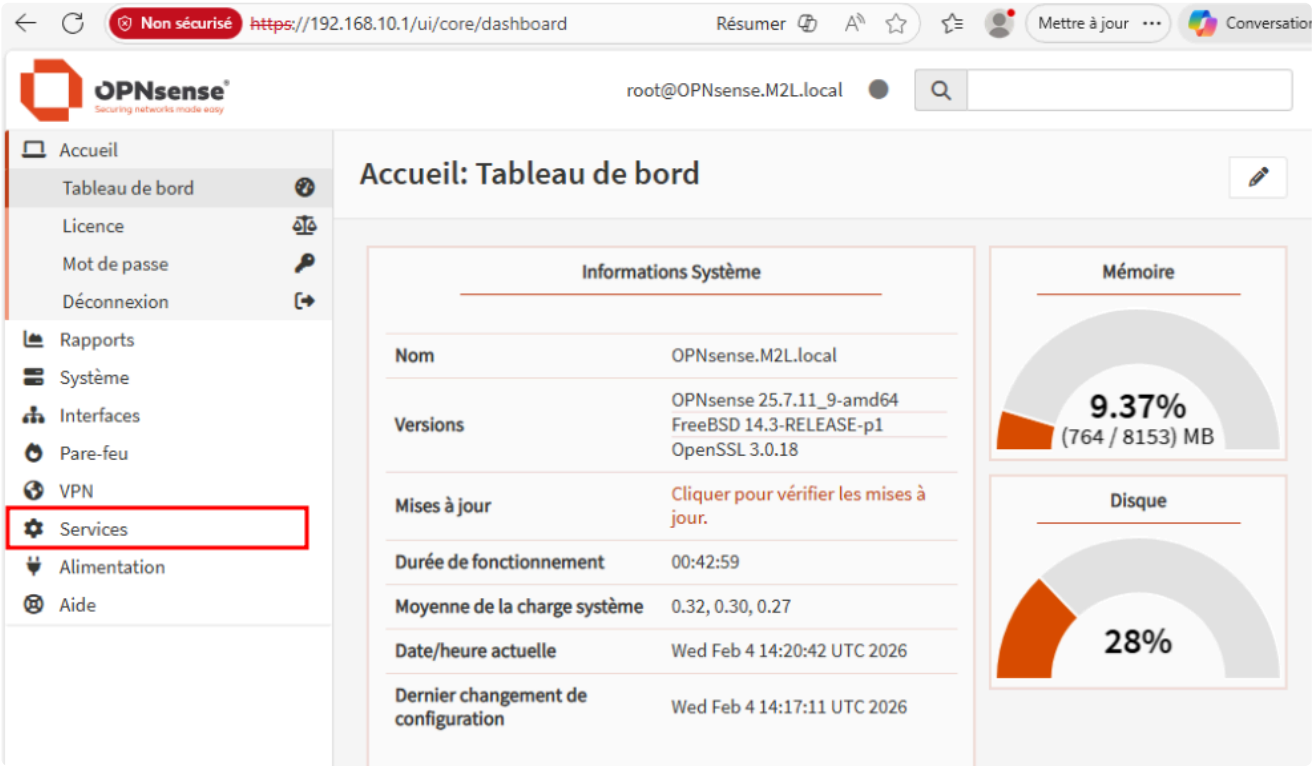
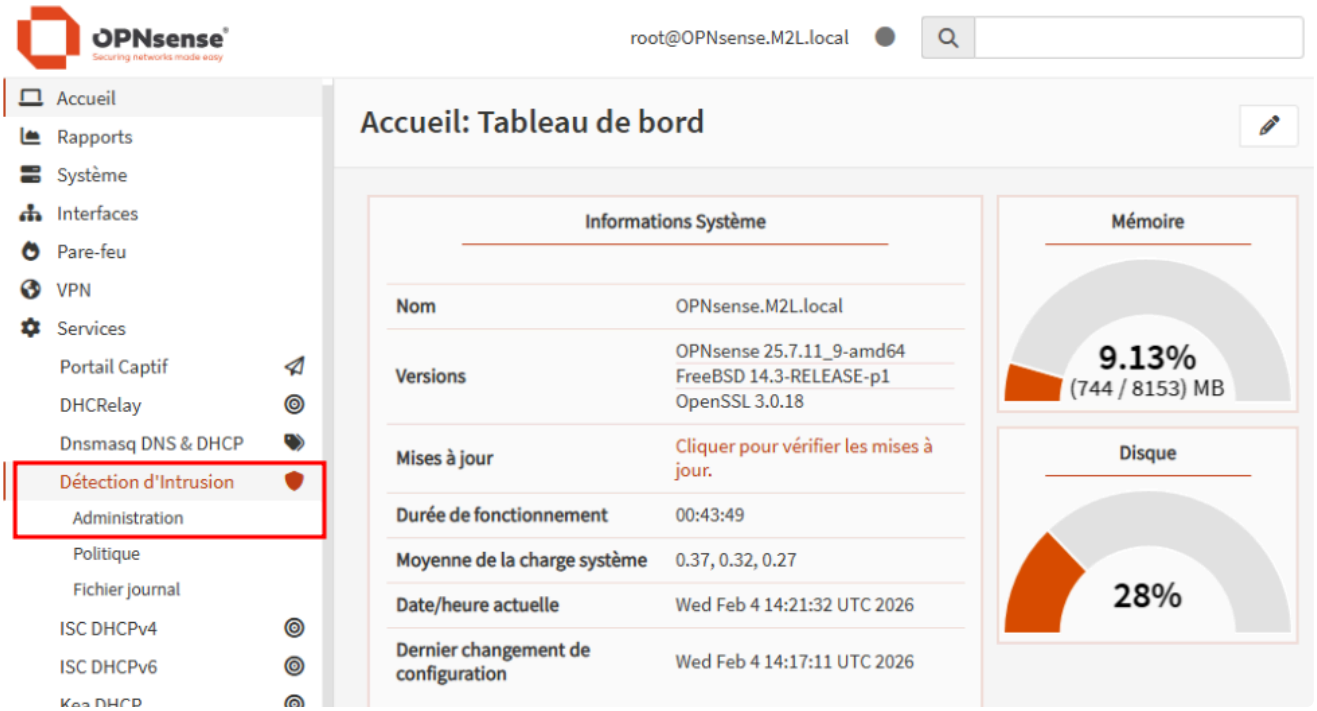
0 - Prérequis

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

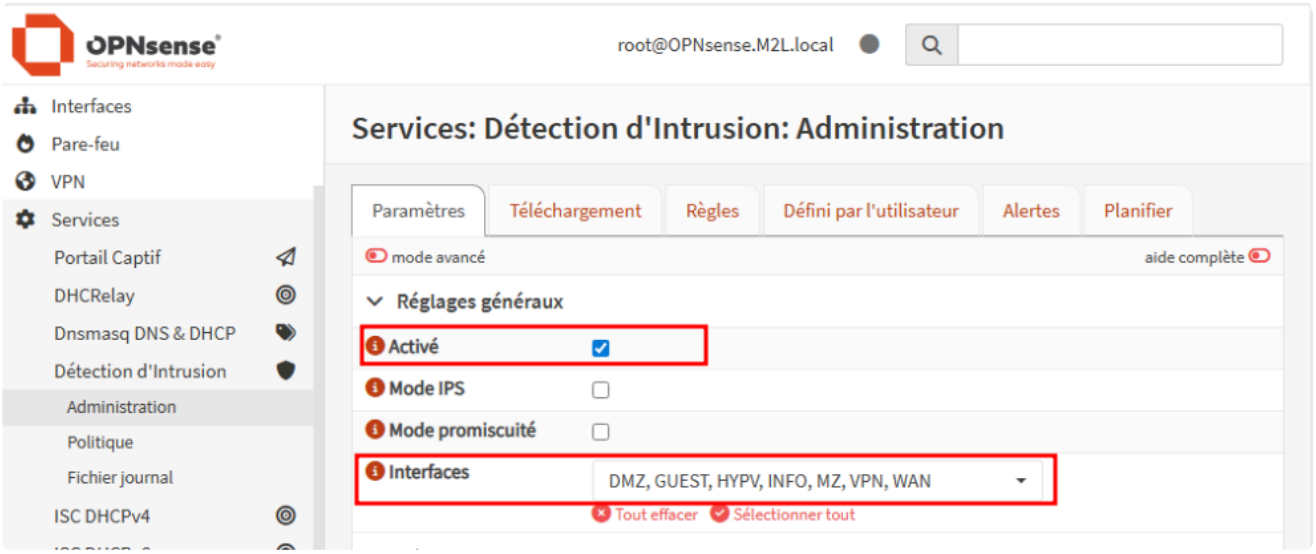
1 - Activation du Service de OPNSense

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

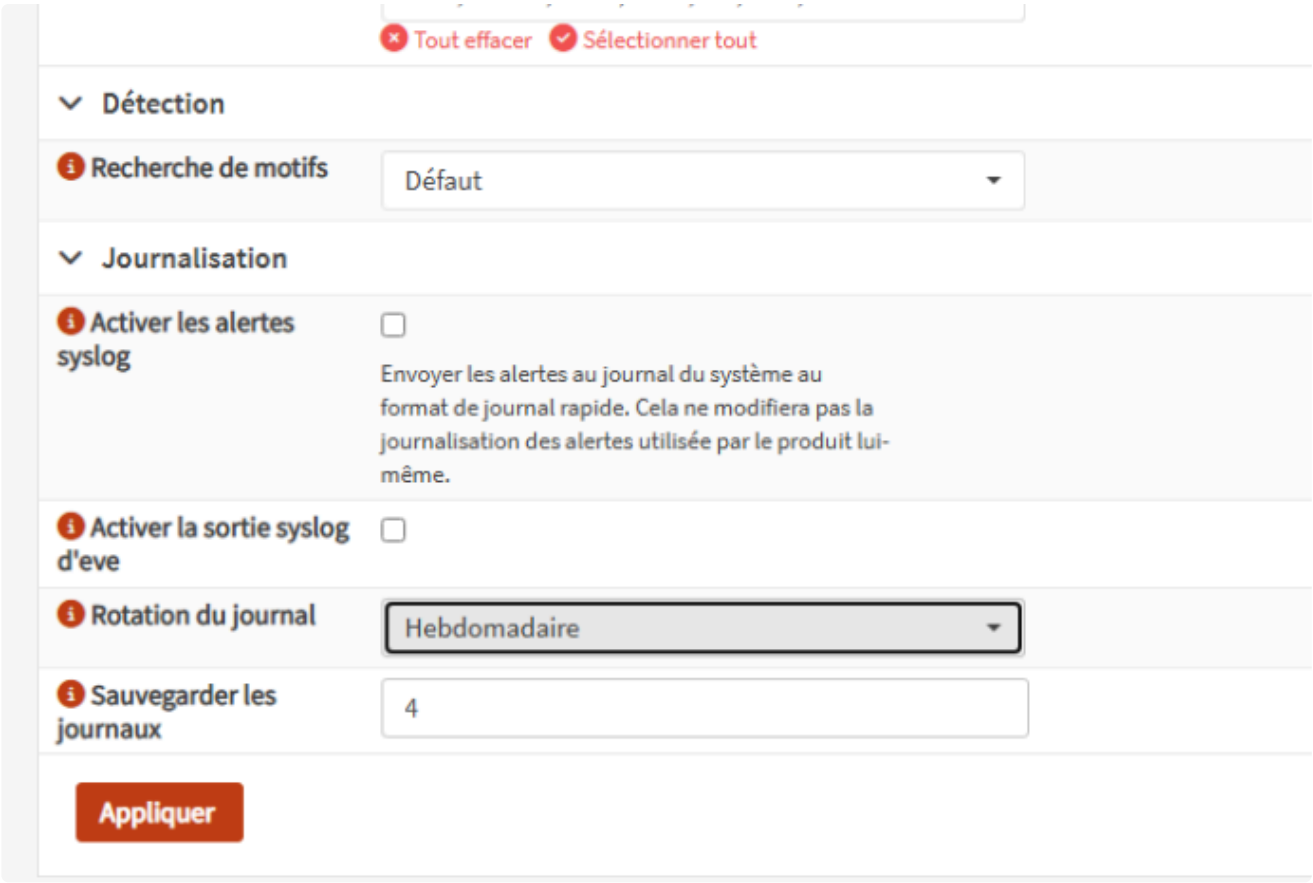




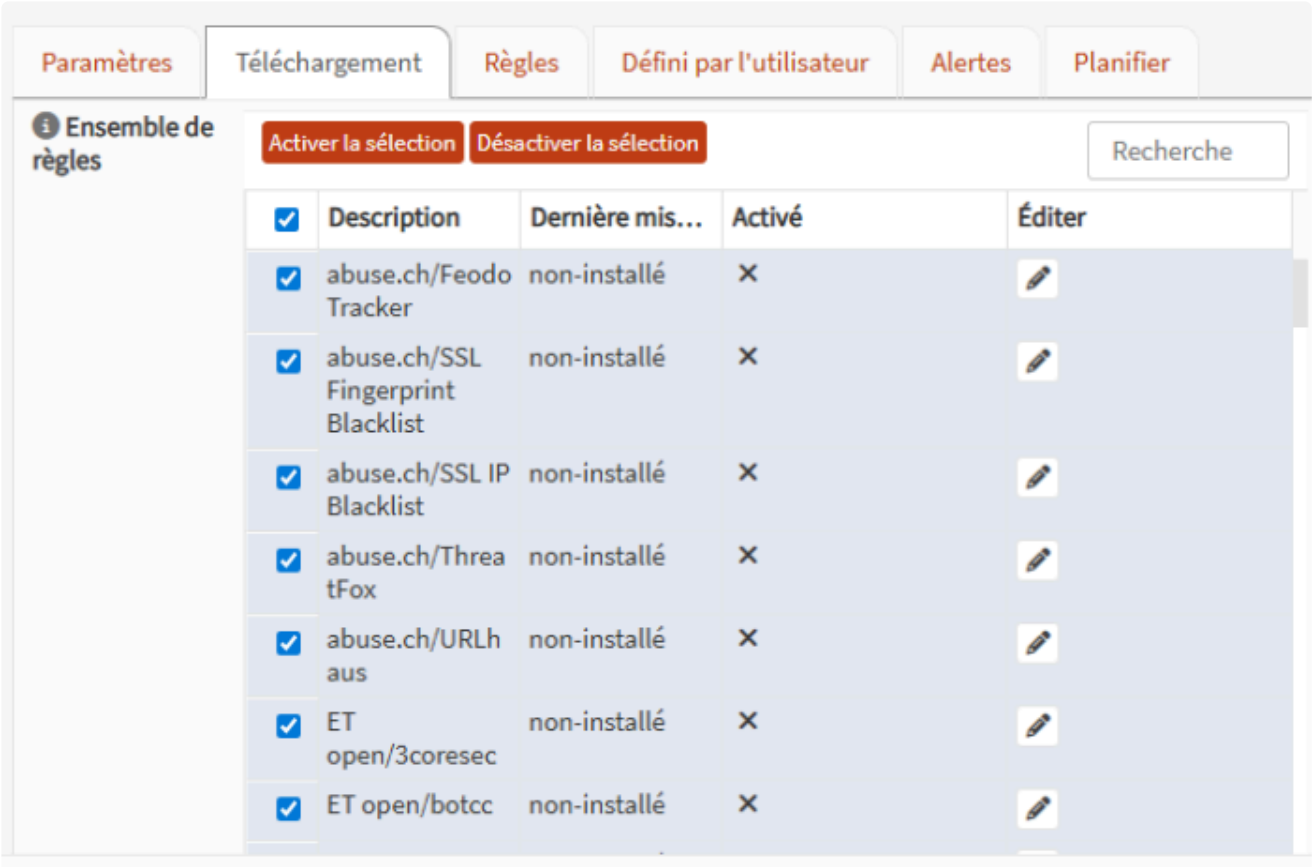
On coche la case activé et on sélectionne les interface a surveiller :



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

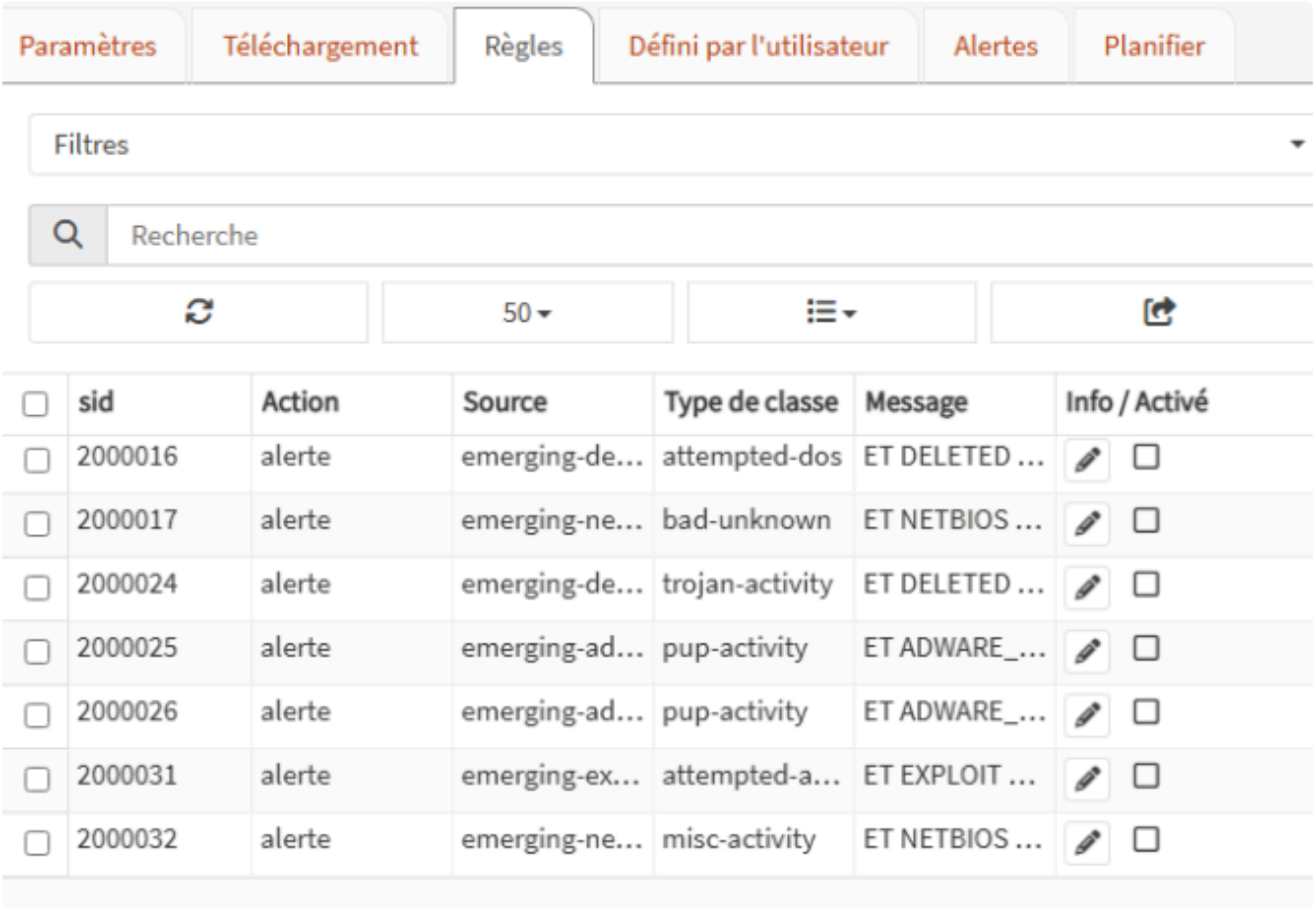


Ensuite dans l'onglet téléchargement on peut installer des règles générales pré-faite. Dans notre cas, je vais toutes les sélectionner et cliquer sur Activer la sélection:



Pierre Frichet

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



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