Brette Morgane BTS SIO 2 **2024/2025**

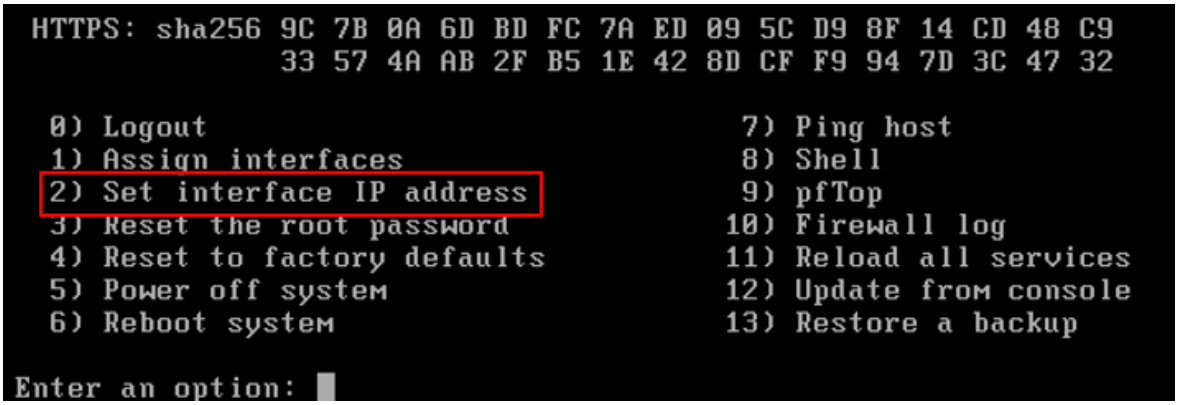
Guide de configuration et d'administration du pare-feu OPNsense

Table des matières

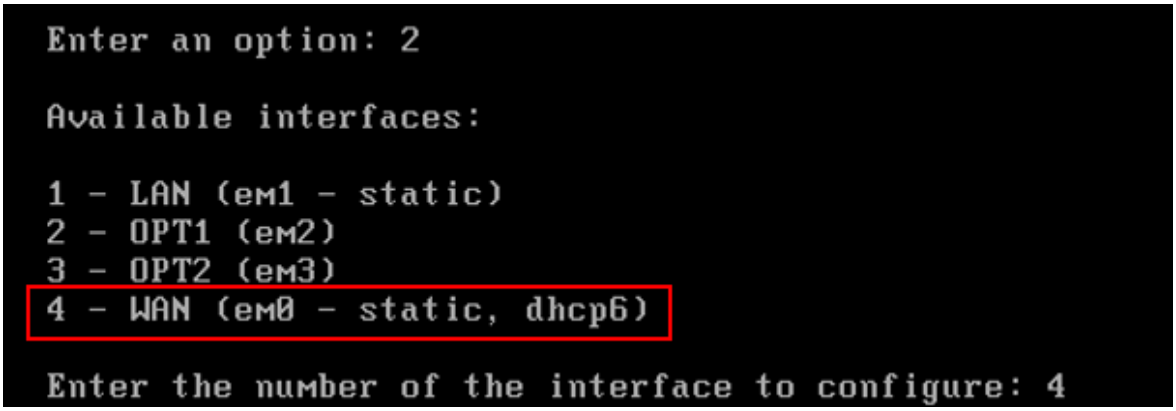
1) Définir les interfaces

Etape 1 : Définir l'adresse IP de l'interface WAN

1. Aller : Rentrer l'option « 2) Set interface IP address »

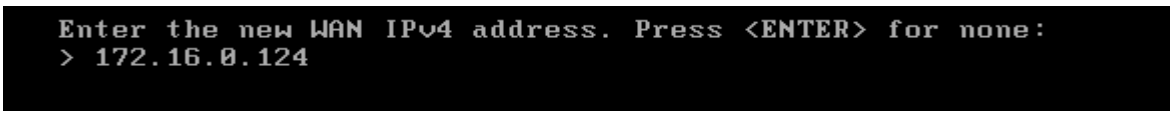


2. Aller : Choisir l'interface « WAN (em0) » > Entrer le nombre « 4 »

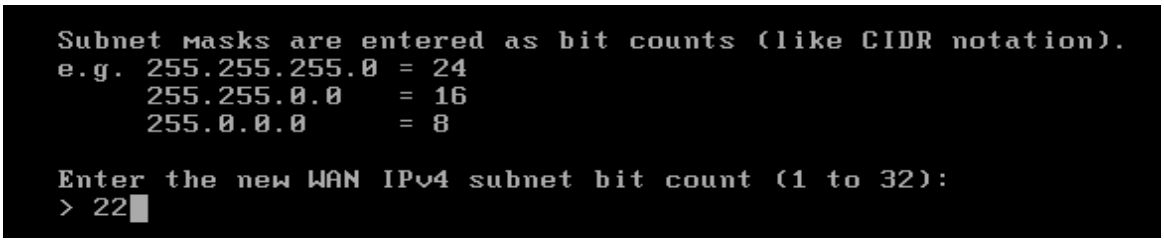


3.Ne pas configurer l'adresse IPv4 de l'interface du WAN par le DHCP> **Mettre « N » pour No**

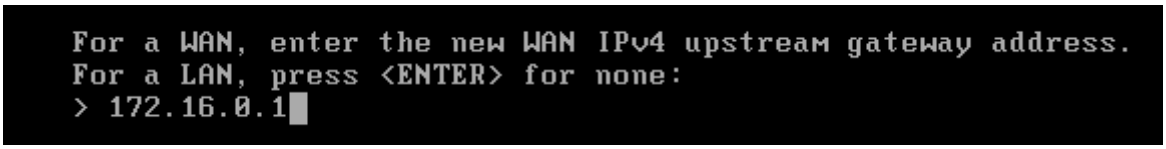
4. Rentrer adresse IP du WAN



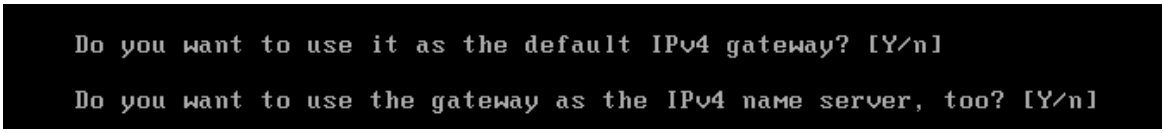
5. Rentrer le masque sous forme décimale



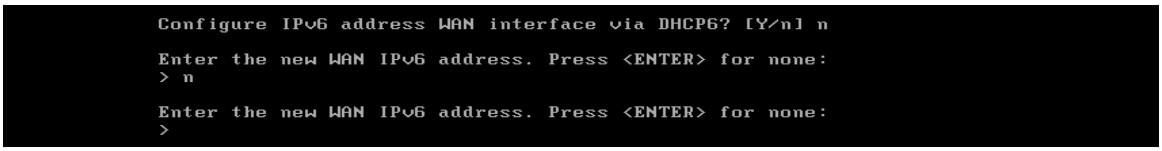
6. Rentrer la passerelle « 172.16.0.1 » : ici correspondant à l'adresse du routeur du réseau de la FDME, dont est rattachée la patte WAN du firewall du réseau de la M2L



7. → « N » : pas utiliser cette adresse comme passerelle par défault
→ « N » : ni l'utiliser comme Domaine Name Server

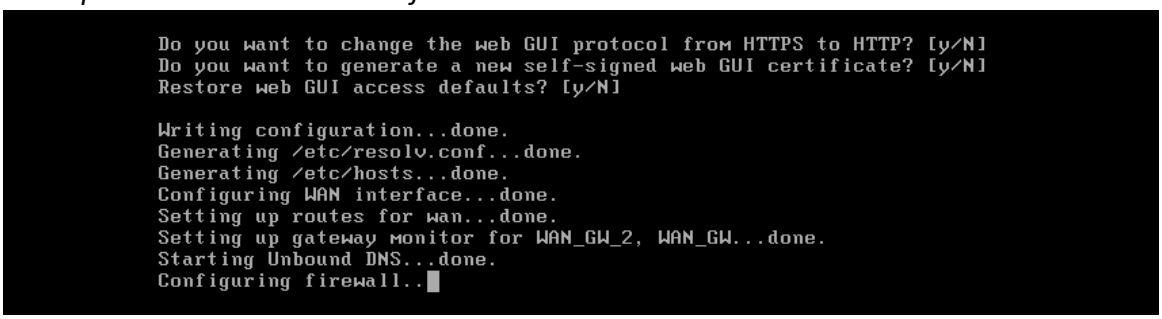


8. « N » : pas configurer d'adresse IPv6 interface WAN via le DHCP
Appuyer sur « ENTREE » pour ne pas rentrer d'adresse IPv6 au WAN



9. → « N » : pas changer le protocole de **l'interface web** (**web GUI**) de **HTTPS**[1] à HTTP
→ « N » : pas générer nouveau certificat **auto-signé**[2] pour **l'interface web**
→ « N » : ne pas restorer les accès par défaut à **l'interface web**

Choix permettre conserver interface web sécurisé



[1] Protocole de communication sécurisé permettant de chiffrer les échanges de données entre un client (navigateur) et un serveur web.
[2] Certificat auto-signé servir sécuriser connexion comme HTTPS, mais pas vérifié par une autorité de confiance.

Etape 2 : Définir l'adresse IP de l'interface LAN

1. Aller : Voir «Etape 1 : définir l'adresse IP de l'interface WAN »

```
Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.1.4


Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 26
```

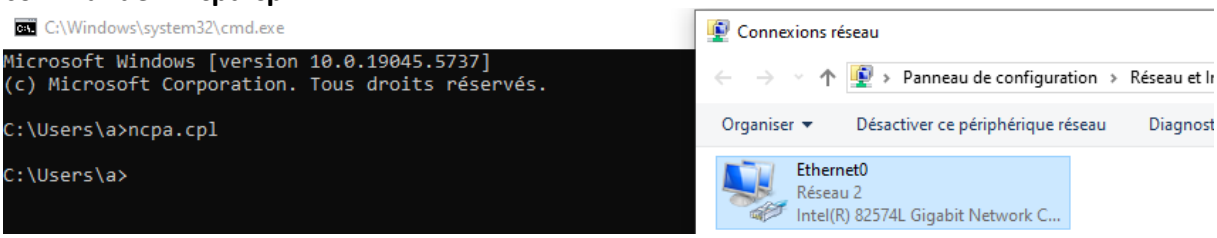
2. Presser « ENTREE » : pas besoin d'une passerelle configurée pour l'interface LAN

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

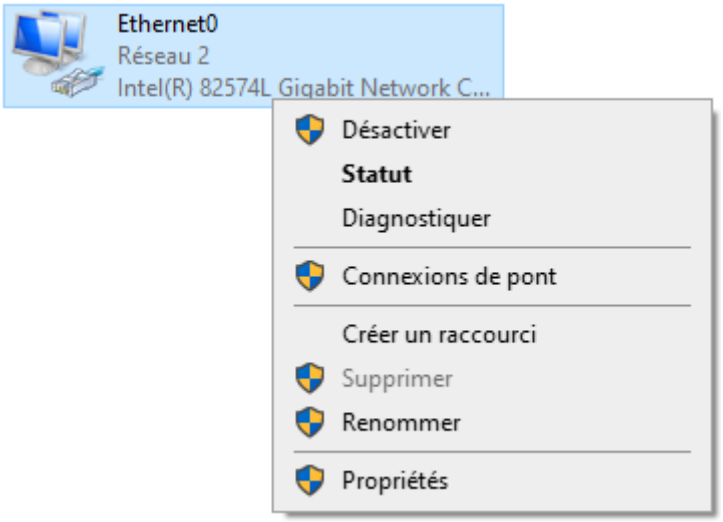
2) Configuration adressage pc administrateur

Etape : Configurer manuellement adressage du pc administrateur par lequel accéder à l'interface web de web GUI

1. Appuyer simultanément w+r > Ecrire « cmd » puis appuyer sur « ENTREE » > Rentrer la commande « **ncpa.cpl** [3]»

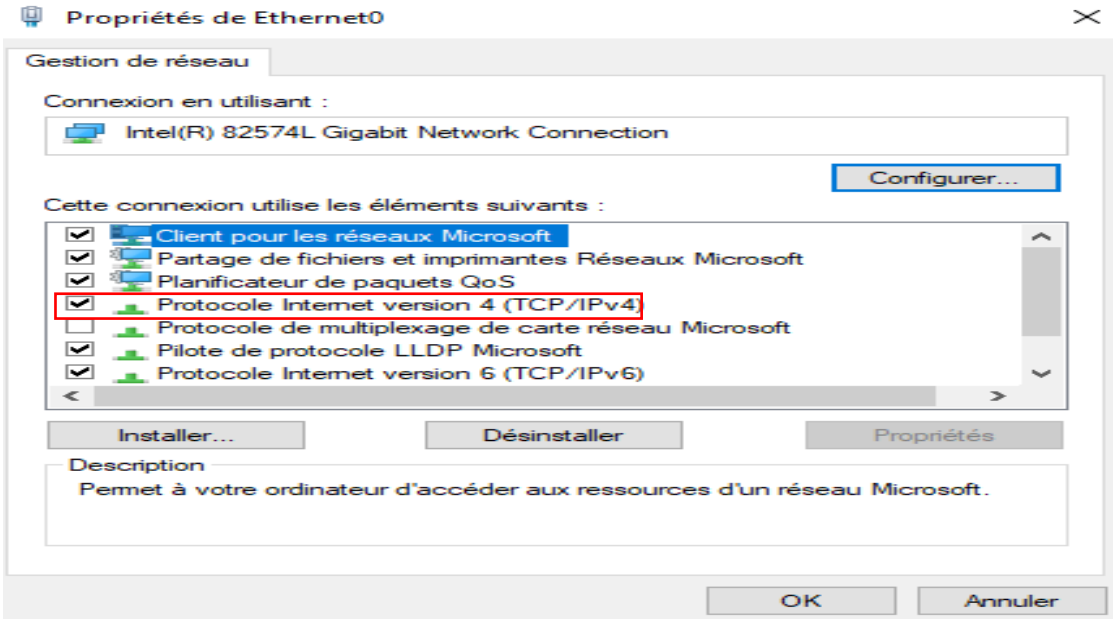


2. Clic droit l'interface réseau « Ethernet 0 » > Cliquer sur « Propriétés »



[3] Commande permettant accéder directement aux connexions réseaux afin de les configurer, et autres.

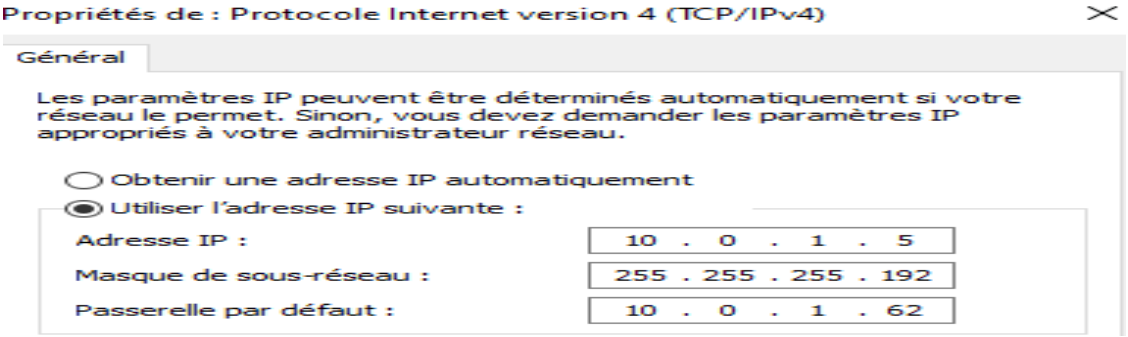
3. Doubles clics sur « Protocole Internet version 4 (TCP/IPv4) »



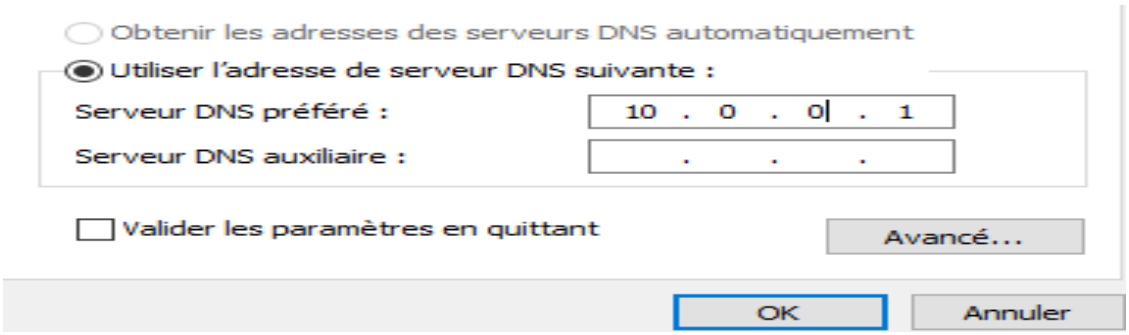
4. → Rentrer dans « Adresse IP » : une adresse IPv4 disponible dans la plage d'adressage du VLAN dans lequel être le pc administrateur

→ Rentrer masque correspondant à la plage d'adressage du VLAN

→ Rentrer passerelle du VLAN



5. Rentrer adresse IP du serveur DNS du réseau > Cliquer sur « Ok »



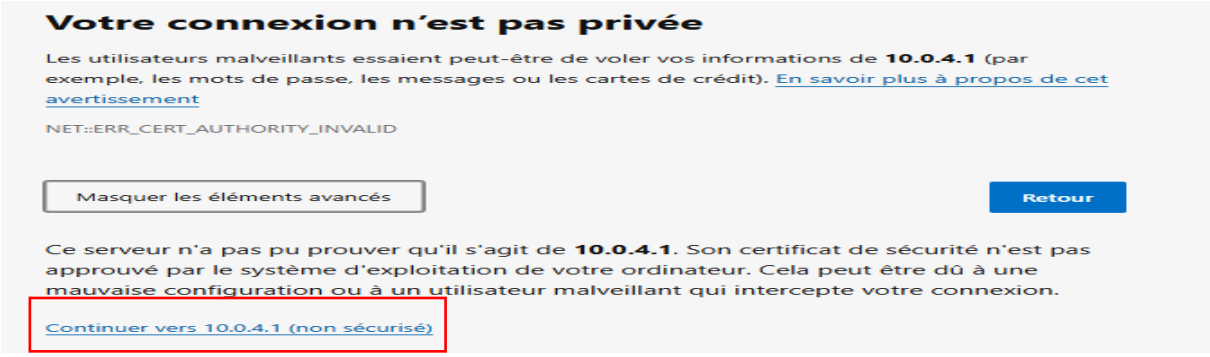
3) Accès et configuration initiale du pare-feu

Etape 1 : Accès interface web GUI

1. Ouvrir navigateur (Chrome, Firefox, …)
2.Entrer dans barre de recherche adresse IP accès interface web GUI (adresse IP du LAN)

3. Cliquer sur « Avancé »
Accès en https pour chiffrer les échanges, et le certificat SSL auto-signé d'où le warning du navigateur.

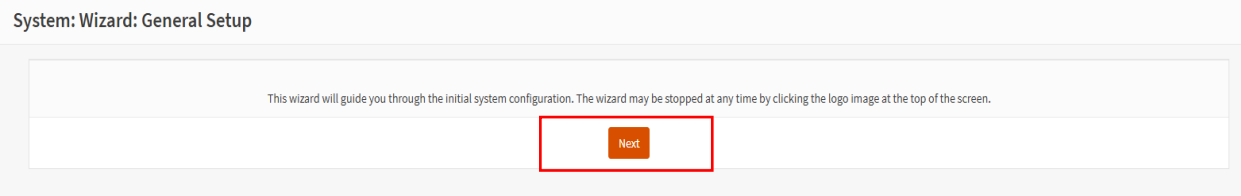
4. Cliquer sur « Continuer vers 10.0.1.4 « non sécurisé » »



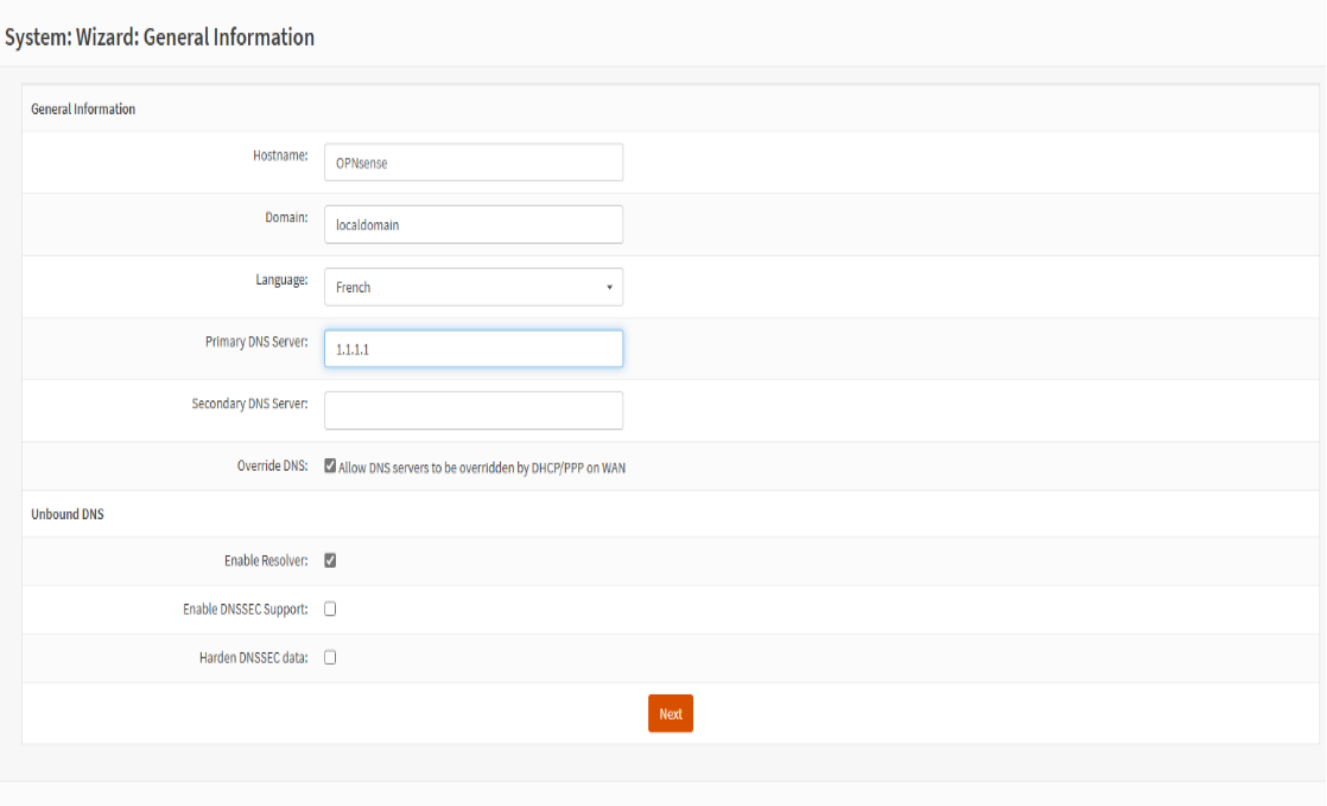
5. Arriver sur page d'authentification afin accéder interface web GUI d'OPNsense
→ Rentrer : identifiant et mot de passe (voir guide d'installation d'OPNsense)

Etape 2 : Configuration initiale d'OPNsense

1. Cliquer sur « Next »



2. Informations importantes :
→ Language : Sélectionner « French »
→ Primary DNS server : serveur utilisé, ne pas modifier déjà configuré
→ Laisser cocher « Enable Resolver » : permettre utiliser le serveur comme **résolveur DNS**[4]



[4] Pare-feu recevoir les requêtes DNS des machines du réseau et les transmettra à Internet

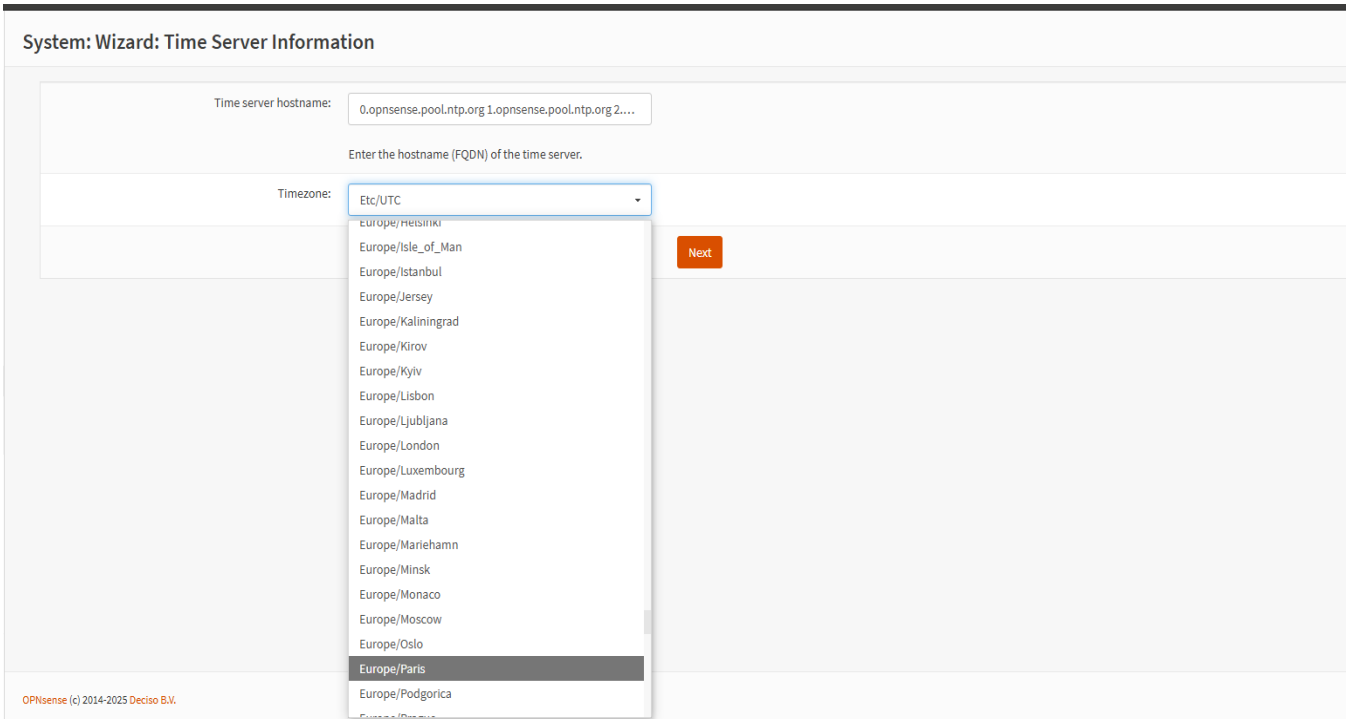
3. « Timezone » : choix du fuséau horaire selon emplacement géographique

ESSENTIEL :

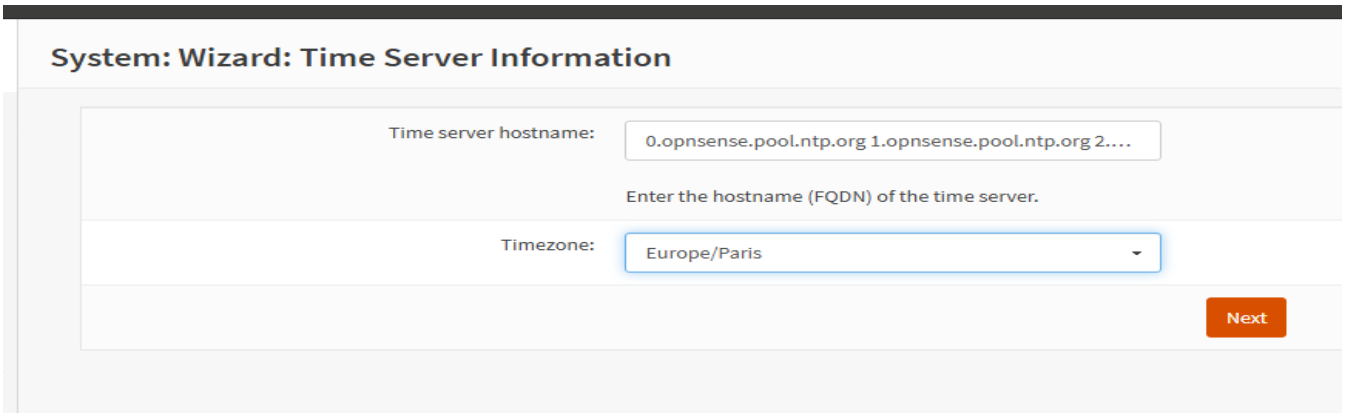
*garantir une synchronisation correcte de l'horloge système du firewall

*une cohérence des journaux et des **horodatages** [5](logs, Netflow, SSH, etc.)

*une compatibilité avec l'Active Directory



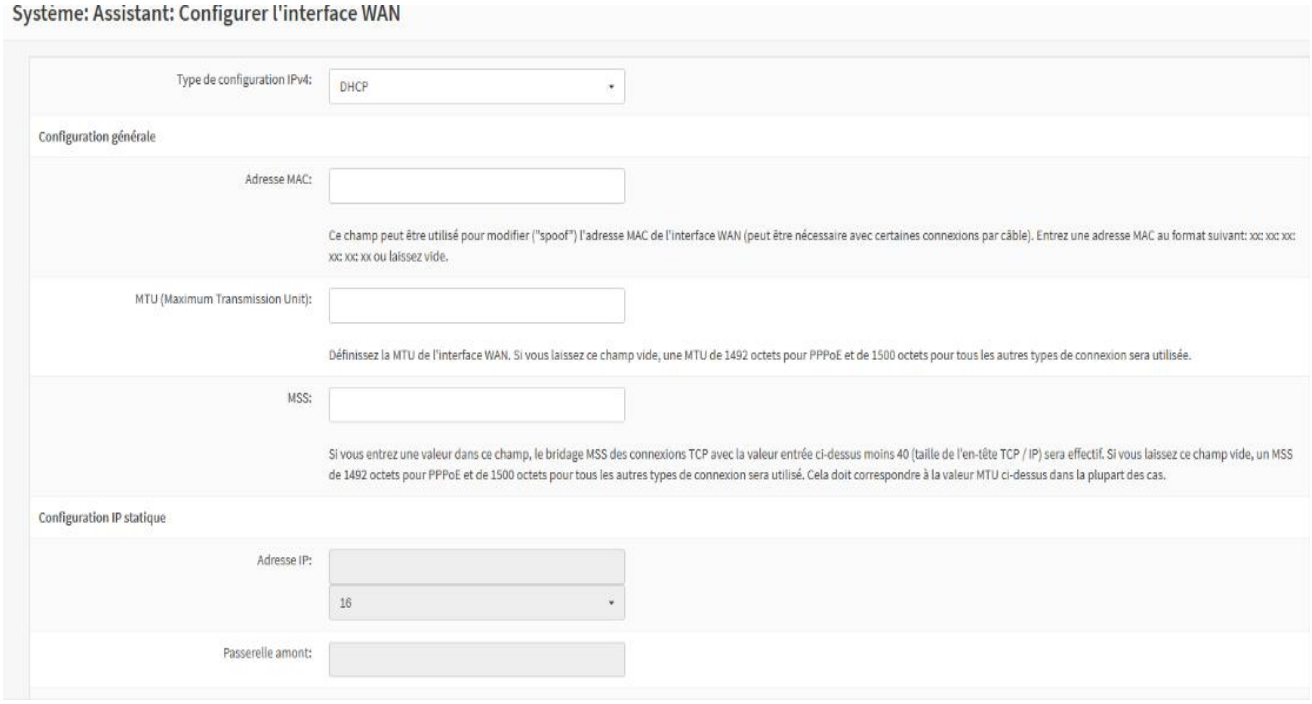
4. Choix serveur **NTP**[6]



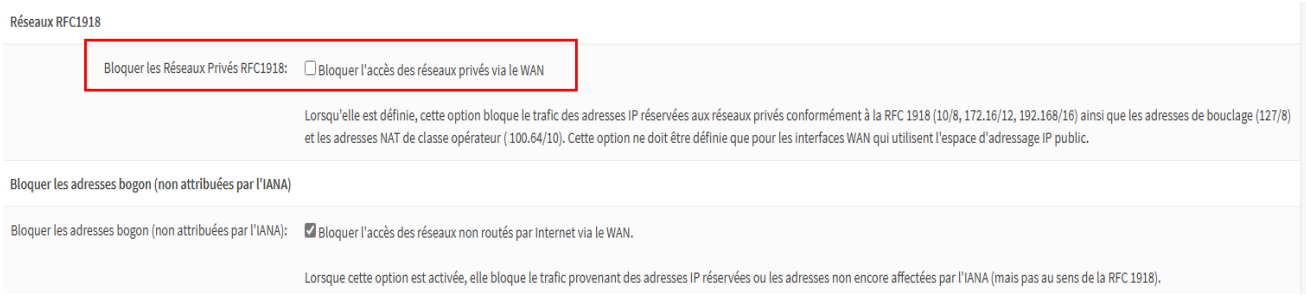
[5] *Timestamp* en anglais, fait rajouter une heure et une date précise à un évènement et une donnée (ex : identifier chronologie d'un évènement, synchroniser équipements, …).

[6] *Network Time Protocol*, serveur de temps en français (ou protocole de synchronisation réseau), servir à synchroniserde manière fiable via un réseau informatique, l'heure locale sur le pare-feu, les ordinateurs, (…).

7. Options inchangées dans notre contexte, Aller directement à « Réseaux RFC1918 »



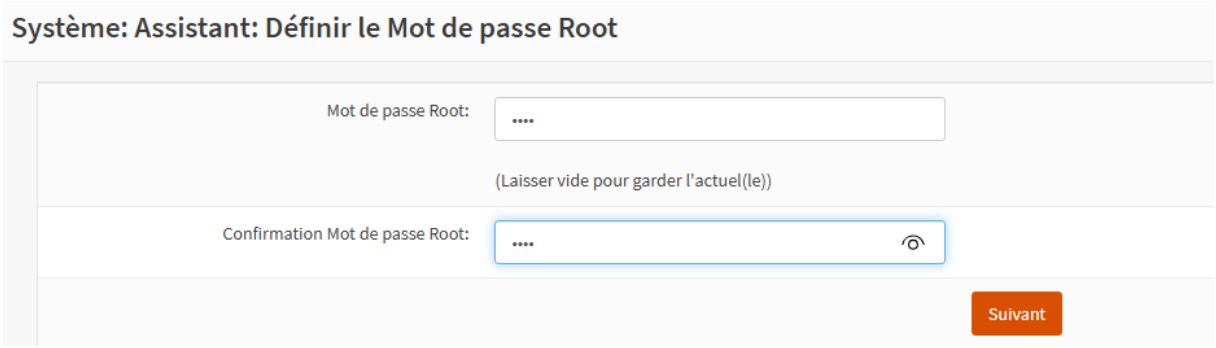
8. Décocher « Bloquer les Réseaux Privés **RFC1918**[7] » : ici interface WAN connectée à un réseau privé (fourni par le routeur de la FDME).
Si option reste cochée :
*OPNsense bloquer tout trafic provenant de ce réseau sur l'interface WAN
*Nécessaire de la décocher pour permettre les communications entrantes depuis le réseau de l'école vers notre infrastructure, y compris tentatives de connexions légitimes (exemple si professeur nécessité de se connecter pour intervenir).



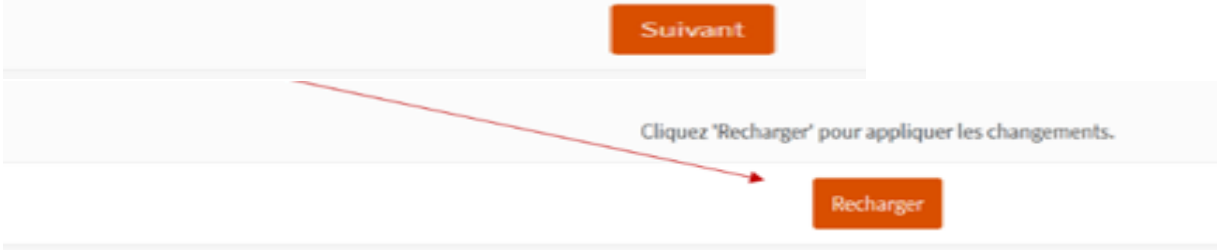
9. Adpresse IP du LAN + masque sous-réseau

[7] *Request for Comments 1918*, norme définie par l'IETF (*Internet Engineering Task Force*, organisme de normalisation) réservant des plages d'adresses IP pour un usage privé, c'est-à-dire non routables sur Internet (pas circuler directement sur le réseau public Internet).

10. Possibilité redéfinir mot de passe « root »



11. Finir la configuration : Cliquer sur « Suivant » > Cliquer sur « Recharger »



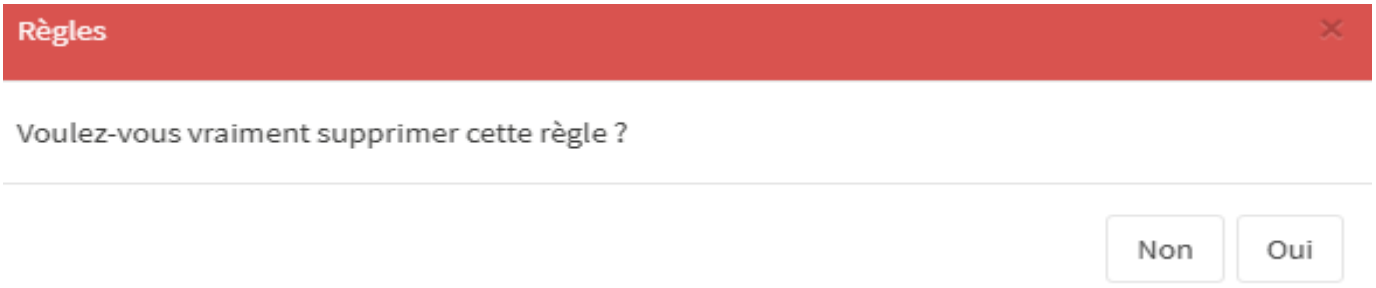
4) Configuration des règles (cas du LAN)

Etape 1 : Supprimer les règles existantes

1. Aller : « Pare-feu » > « Règles » > « LAN »

2. Supprimer les règles existantes : Cliquer sur icône « Poubelle »

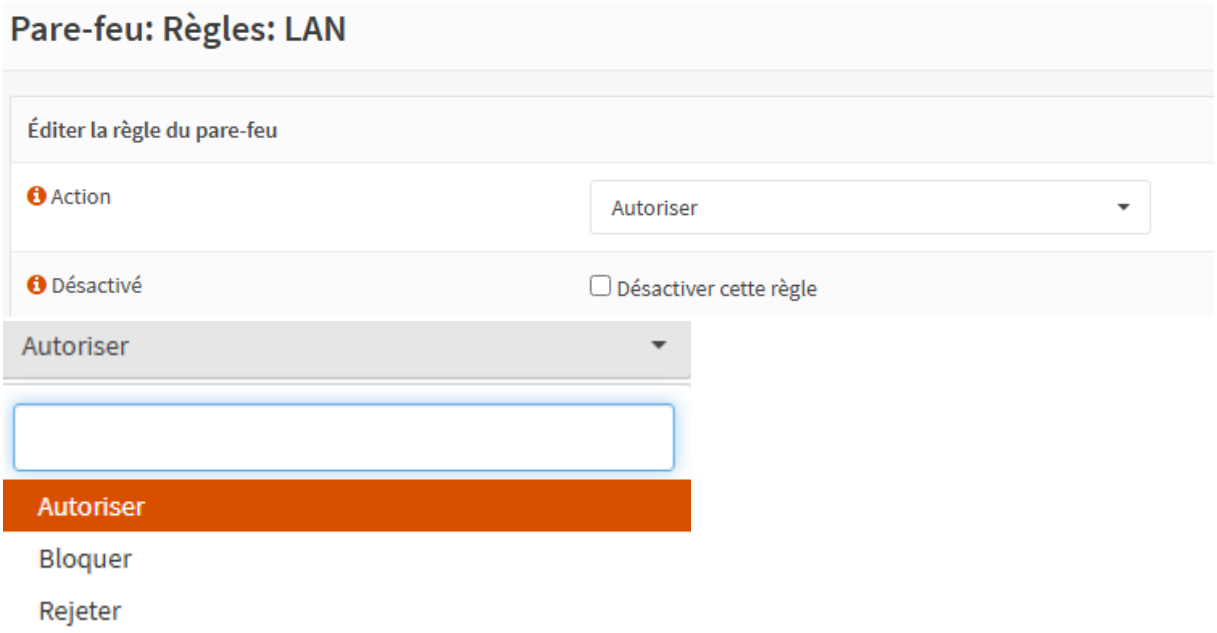
3. Confirmer « Oui » > « Appliquer les changements »



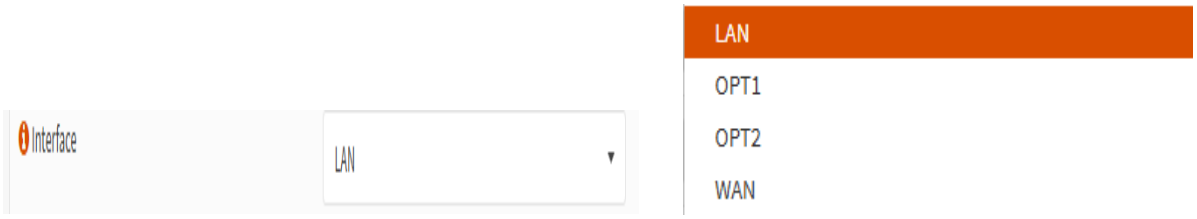
Etape 2 : Créer une règle LAN vers WAN : ici règle DNS[8]

1. Ajouter une règle : appuyer sur le « + »

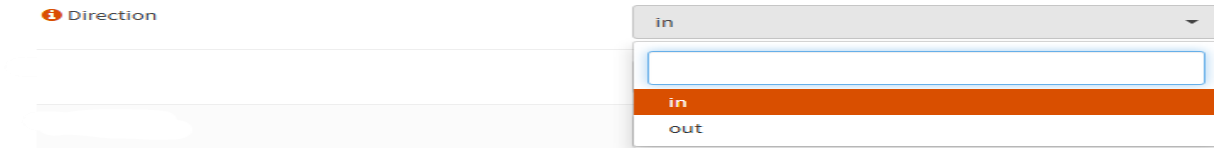
2. Choix « Action » de la règle :
*autoriser (laisser passer les flux autorisés)
*bloquer
*rejeter (servir interdire certains types de trafic)
→ (« Autoriser » ici, car on veut laisser passer les flux)
→ Possibilité de désactiver la règle (tester l'effet d'une règle sans la supprimer)



3. Choix interface concernée : LAN/WAN/(…)



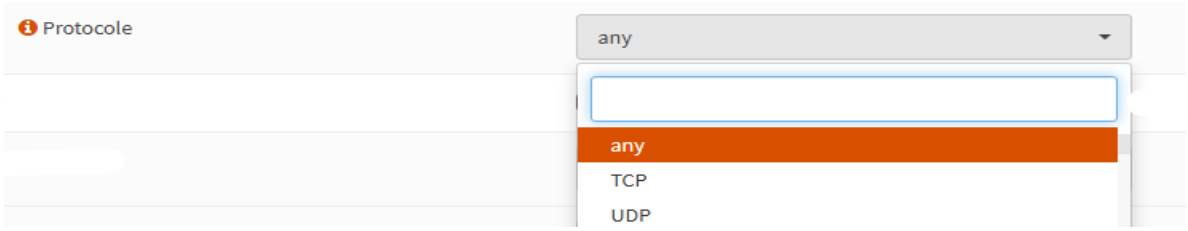
4. Choix direction : IN (rentrant) / OUT (sortant) : ici IN



[8] *Domain Name Server*, service permettant de traduire les noms de domaine en adresse IP.

5. Choix du protocole réseau utilisé (IPv4/IPv6/IPv4+IPv6)

6. Choix du protocole pour transporter les paquets : ici UDP pour DNS

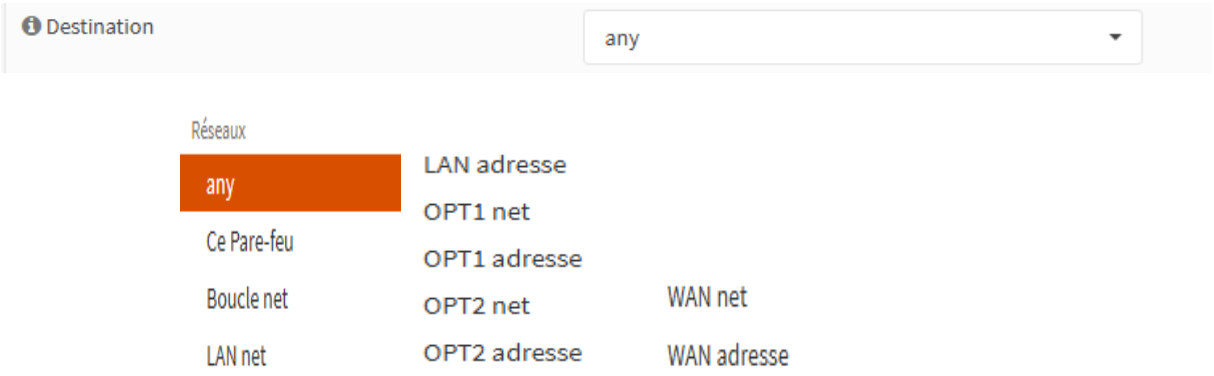


7. Choix de la source

Option	Signification	Utilisation typique
Any	N'importe quelle adresse IP ou réseau, sans restriction	Pour autoriser vers Internet ou tout réseau
Ce Pare-feu	Adresse IP locale de l'interface sur OPNsense (celle que la règle traite)	autoriser l'accès à OPNsense (ex: DNS local)
Boucle net	Adresse de loopback (127.0.0.1/8) — pour le trafic vers/depuis lui-même	Rarement utile ici
LAN net	Réseau défini sur l'interface LAN	Pour filtrer ce qui sort du LAN
LAN adresse	Adresse IP de l'interface LAN d'OPNsens	Utiliser pour règles très ciblées
WAN net	Réseau auquel est connecté l'interface WAN	Restreindre les règles vers WAN seulement
WAN adresse	Adresse IP de l'interface WAN	Bloquer/autoriser trafic vers cette IP
OPT1 net / adresse	Réseau ou IP de l'interface OPT1 (DMZ)	Segmenter plusieurs zones réseau
OPT2 net / adresse	Réseau ou IP de l'interface OPT2 (Wifi)	Segmenter plusieurs zones réseau

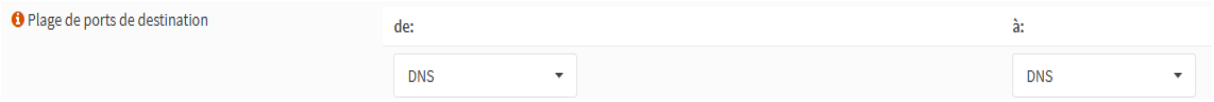
Ici source « LAN net » : à l'origine du trafic

8. Choix de la destination : l'endroit où va aller le trafic

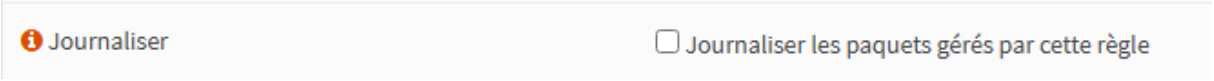


Ici : « Any »

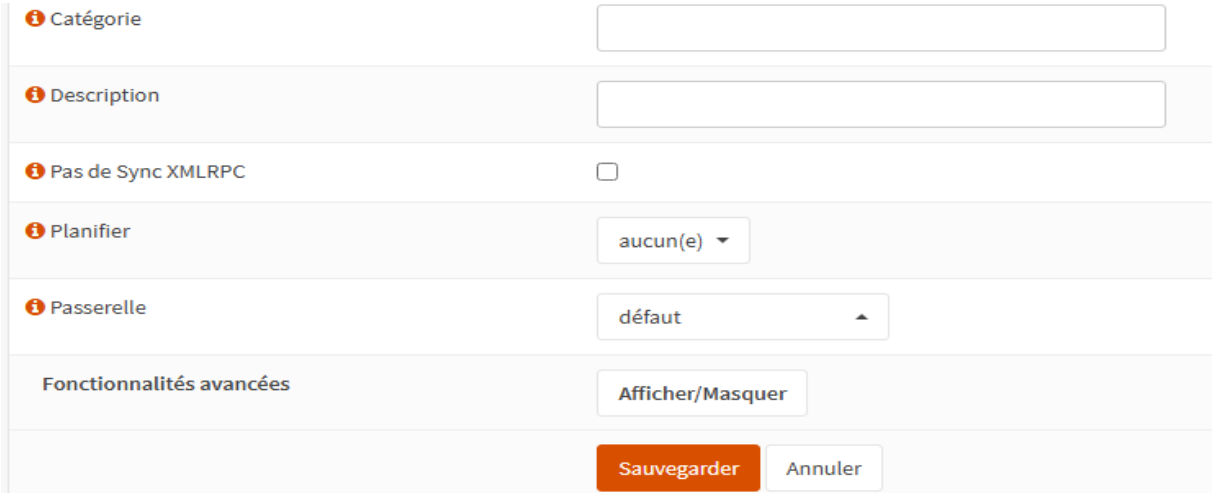
9. Choix du port de destination : port de service ciblé, ici DNS (port 53)



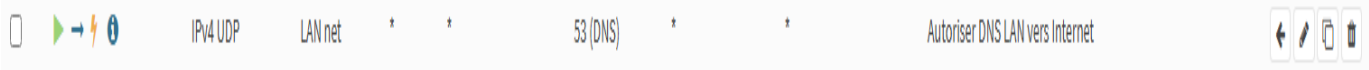
10. A cocher : pour voir dans les logs les paquets utilisant cette règle (pratique pour débug)



11. Saisir « Description » : afin de savoir utilité de cette règle

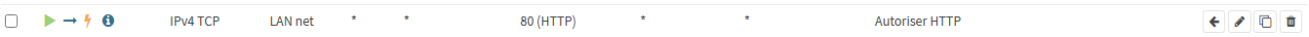


12. « Sauvegarder » > « Appliquer les changements »



Etape 3 : Créer les autres règles

1. Règle autorisant le trafic HTTP

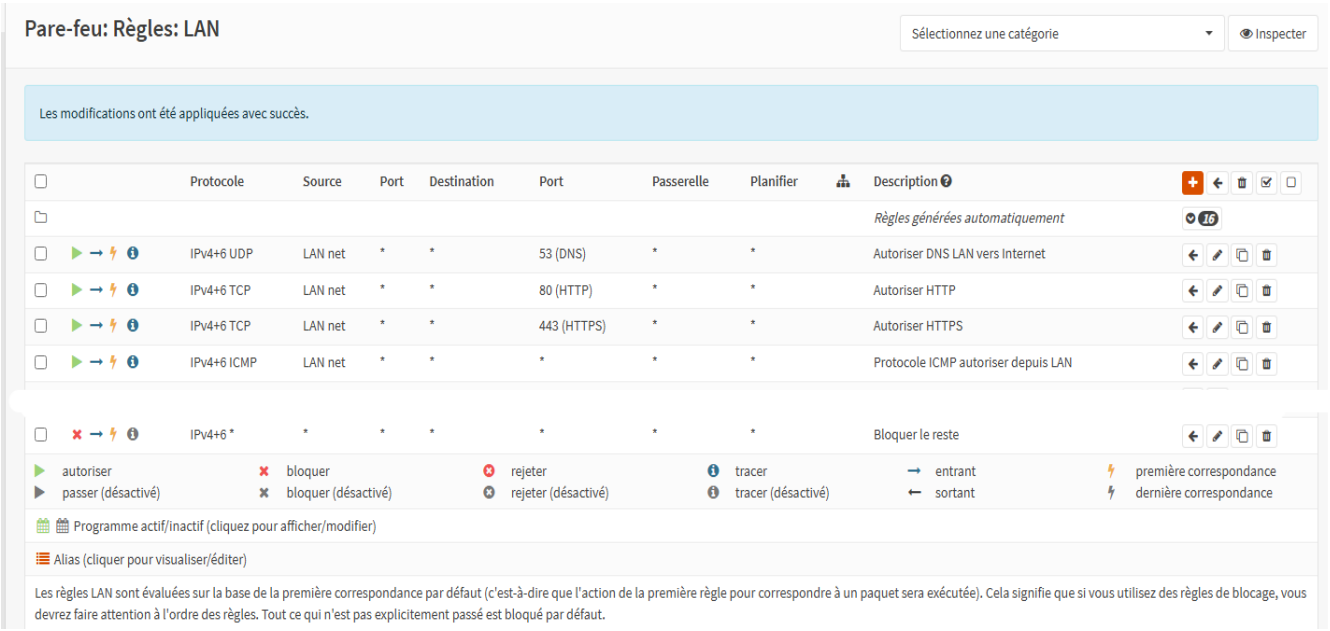


2. Règle autorisant le trafic HTTPS

3. Règle autorisant le protocole ICMP[9]

4. Règle empêchant tout trafic non autorisé

5. Résumé des règles créées



[9] *Internet Control Message Protocol* un protocole réseau utilisé pour envoyer des messages de diagnostic et d'erreur entre les équipements (ping AdresseIP)

Etape 4 : Vérifier cela fonctionne depuis poste client situé dans même réseau que le LAN

1. Tester si DNS fonctionner : CMD > « **nslookup**[10] nomdomaine » (ex : airfrance.fr)

```
C:\Users\a>nslookup airfrance.fr
Serveur :   one.one.one.one
Address:  1.1.1.1

Réponse ne faisant pas autorité :
Nom :    airfrance.fr
Addresses:  2a02:26f0:82::17c8:5731
          2a02:26f0:82::17c8:5732
          96.16.248.136
          96.16.248.177
```

2. Tester si HTTP fonctionner : CDM > « **curl**[11] http//example.com »
*Si réponse en html : HTTP fonctionner

```
C:\Users\a>curl http://example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You may use this
    domain in literature without prior coordination or asking for permission.</p>
    <p><a href="https://www.iana.org/domains/example">More information...</a></p>
</div>
</body>
</html>
```

3. Tester HTTPS : CDM > « curl https://example.com »
*Idem à HTTP

[10]Programme interrogeant les serveurs DNS pour obtenir les informations définies pour un domaine déterminé.
[11] Outil en ligne de commande permettant de tester directement les connexions HTTP ou HTTPS.

4. Tester ICMP : CMD > « ping 8.8.8.8 »

```
C:\Users\a>ping 1.1.1.1

Envoi d'une requête 'Ping'  1.1.1.1 avec 32 octets de données :
Réponse de 1.1.1.1 : octets=32 temps=4 ms TTL=127
Réponse de 1.1.1.1 : octets=32 temps=4 ms TTL=127

Statistiques Ping pour 1.1.1.1:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 4ms, Moyenne = 4ms
```

5. Vérifier blocage du reste : CMD > « **telnet**[12] google.com 21 »

```
C:\Users\a>telnet google.com 21
Connexion à google.com...Impossible d'ouvrir une connexion à l'hôte, sur le port 21: Échec lors de la connexion
```

Ici échec, car port 21 non autorisé donc resté bloqué = « échec lors de la connexion »

[12] *TELecommunication NETwork* protocole réseau utilisé pour établir une connexion distante à un autre ordinateur via une interface en ligne de commande.

5) Configuration Suricata

Etape 1 : Activer et configurer Suricata[13]

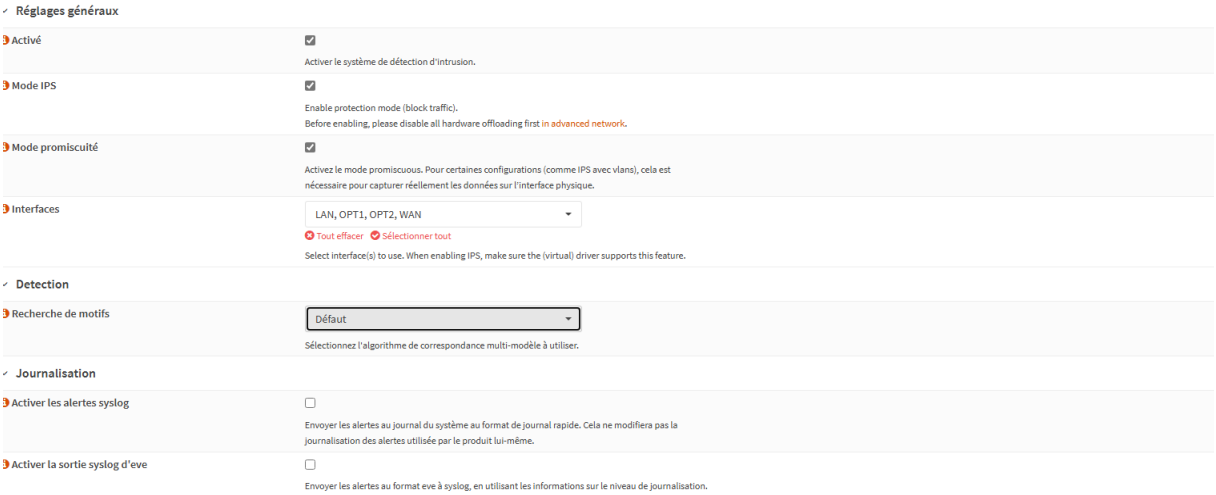
1. Aller : « Services » > « Détection d'Intrusion » > « Administration »

2. → Cocher « Activé » + « Mode **IPS** [14]» + « Mode **promiscuité** [15]» : Permettre analyser et bloquer efficacement tout le trafic réseau, doit voir tous les paquets (mode promiscuité)+ autorisé à intervenir dessus (mode IPS).

→ Choisir les interfaces « LAN + WAN + DMZ + WIFI »

→ Cocher « Activer les alertes syslog » : envoyer alertes dans les journaux système d'OPNsense

→ Pas besoin de cocher « Activer la sortie syslog d'eve » : pas exploiter ou centraliser ici en détail les logs sur serveur externe

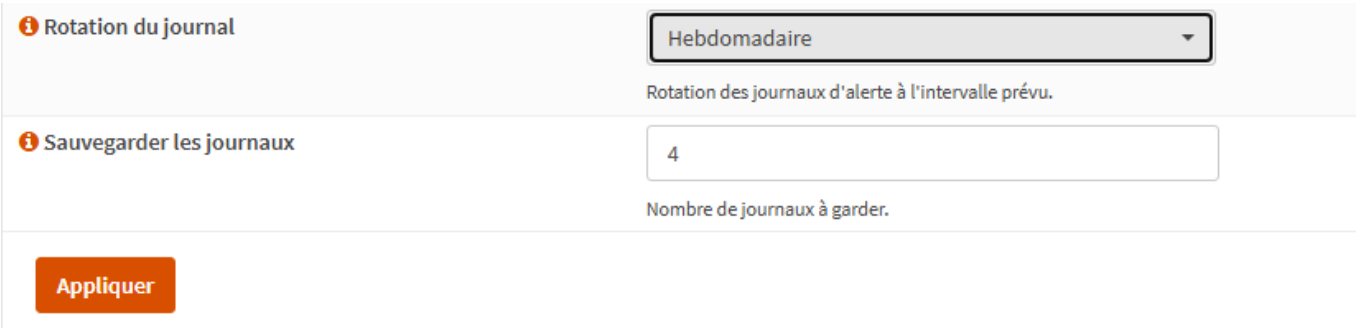


[13] Système de détection et de prévention d'intrusion (IDS/IPS) analysant en temps réel le trafic réseau pour identifier et bloquer les menaces.

[14] IPS (*Intrusion Prevention System*) :Activer la prévention, donc bloquer activement les paquets malveillants détectés, en plus de les détecter.

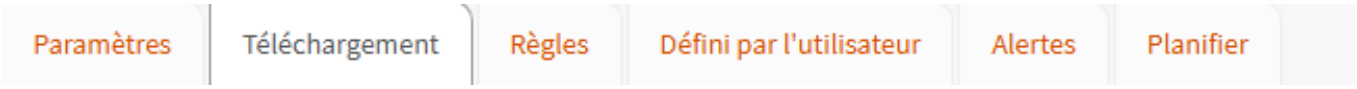
[15] Permettre à l'interface réseau de voir tout le trafic, même celui pas destiné directement à elle (utile pour inspection complète du réseau).

3. → Choisir « Rotation du journal » si archivages des logs tous les jours/toutes les semaines
→ « Sauvegarder les journaux » : ici Suricata garder les 4 derniers fichiers de journaux d'alertes
→Puis Cliquer sur « Sauvegarder »

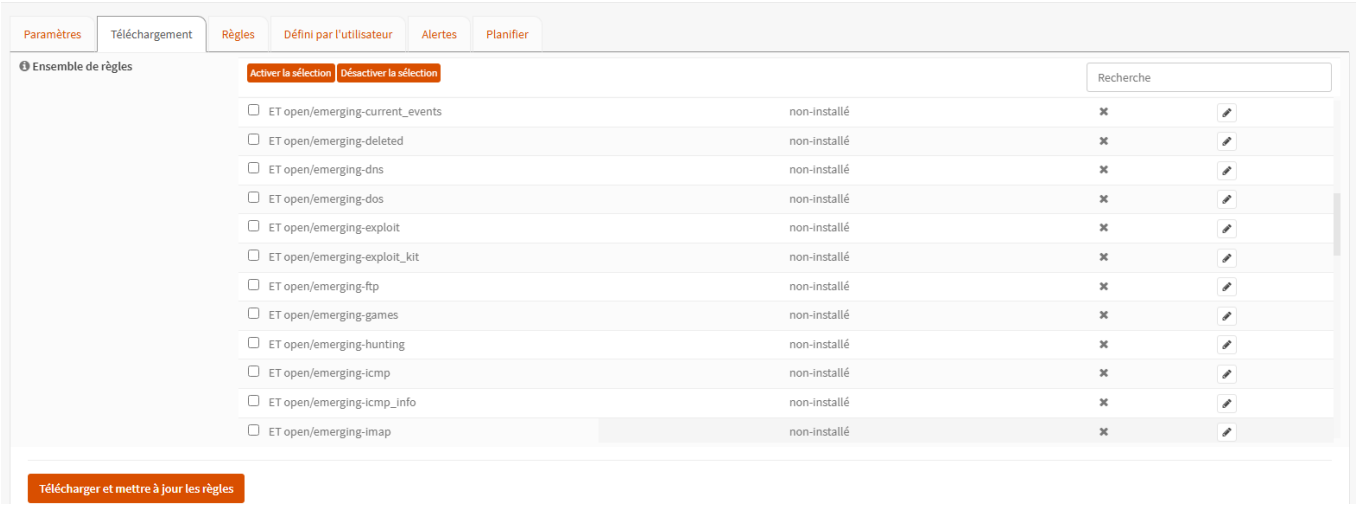


Etape 2 : Télécharger les règles

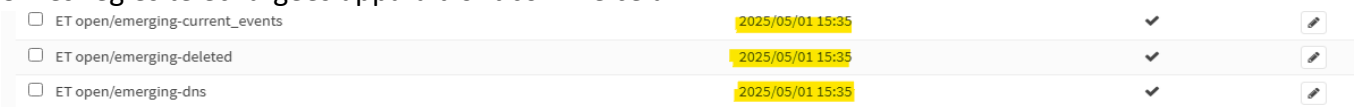
1. Se rendre dans « Téléchargements »



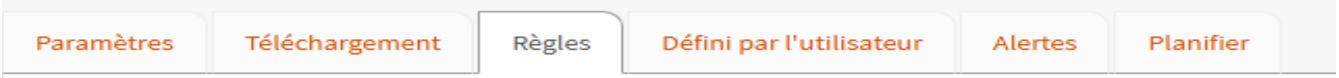
2. → Cocher les règles qu'on veut télécharger
→ Cliquer sur « Activer la sélection »
→ Cliquer sur « Télécharger et mettre à jour les règles »



3. Les règles téléchargées apparaitront comme cela



4. Se rendre dans « Règles »



5. Sélectionner celles qui nous intéressent

→ Cocher à gauche / si sélectionner tous cliquer sur « sid »

→ Les activer en cliquant sur « Alerter »

6. Règles activées apparaître en étant cochées à « Activé » > Cliquer sur « Valider »

Etape 3 : Exemple règle ET open/compromised[16]

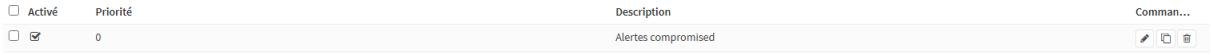
1. Chercher et cocher la règle suivante dans la liste : « ET open/emerging »

2. Télécharger et mettre à jour la règle

3. Aller : Onglet « Politique »

[16] Règle permettant de détecter des connexions vers des IP ou domaines compromis.

4. Ajouter une règle



5. Configurer la règle

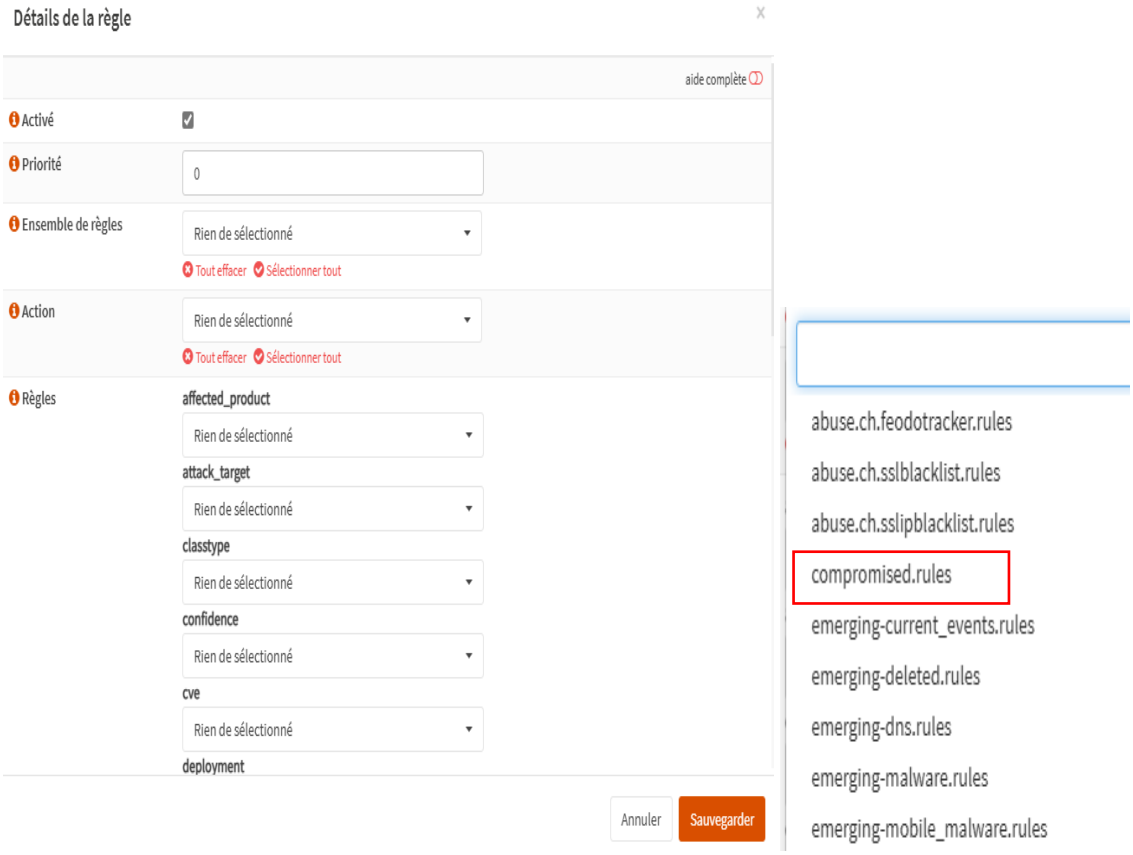
→ Choisir niveau de priorité (ex : 3 faible priorité)

→ Choisir les ensembles de règles (ex :Compromised.rules)

→ Choisir action : désactiver/alerter/rejeter

→ Sauvegarder

→ Appliquer

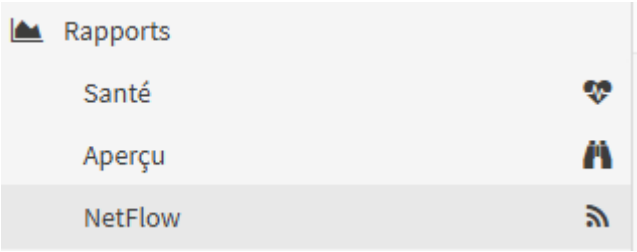


6. Consulter résultats dans « Services » > « Détection d'Intrusion » > « Fichier journal »

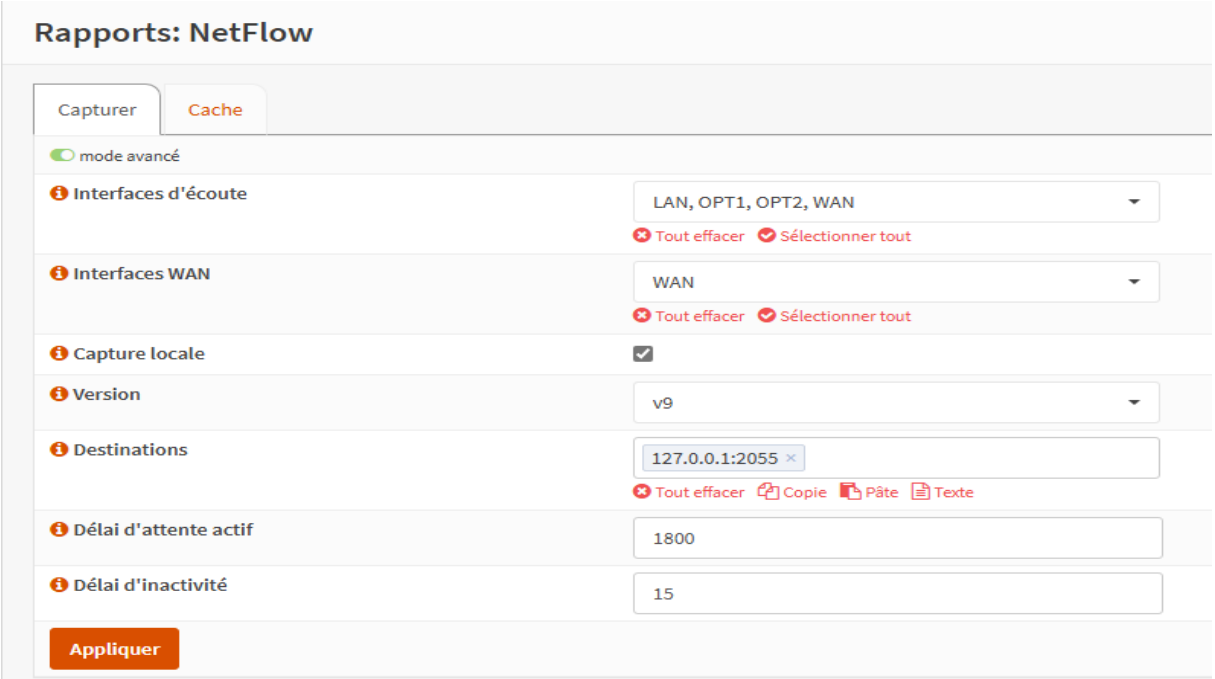
6) Configuration Netflow[17]

Etape 1 : Configurer Netflow

1. Se rendre dans « Rapports » > « Netflow »



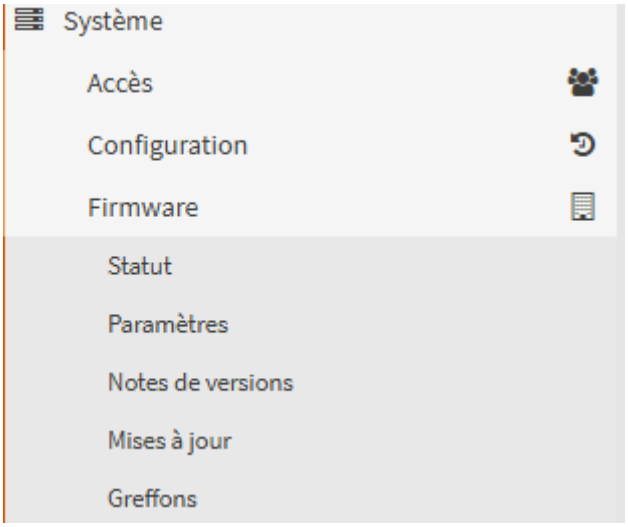
2. Configurer Netflow
→Sélectionner les interfaces d'écoute
→Laisser l'interface en WAN : afin de bien classifier le trafic Internet
→Cocher « Capture locale »
→Rentrer l'IP de destination vers laquell envoyée les données Netflow
*127.0.0.1 = localhost
*2055 port standart de réception Netflow v9
→Appliquer



[17] Protocole de collecte de données de trafic réseau **MAIS NE STOCKE PAS NI NE VISUALISE CES DONNEES PAR DEFAUT**.

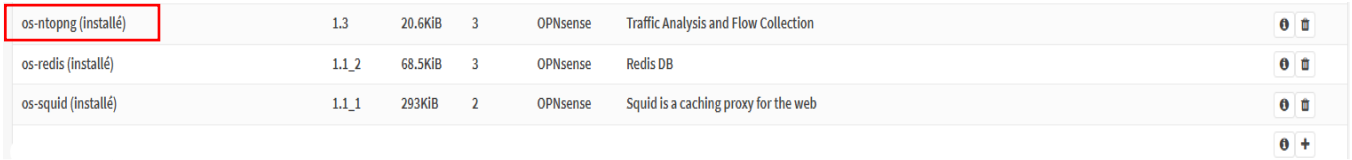
Etape 2 : Télécharger le greffon « os-ntopng[18] »

1. Se rendre dans « Système » > « Firmware » > « Greffons »



2. Rechercher « os-ntopng » > Cliquer sur « + » pour l'installer

3. Apparaitre comme « installé »



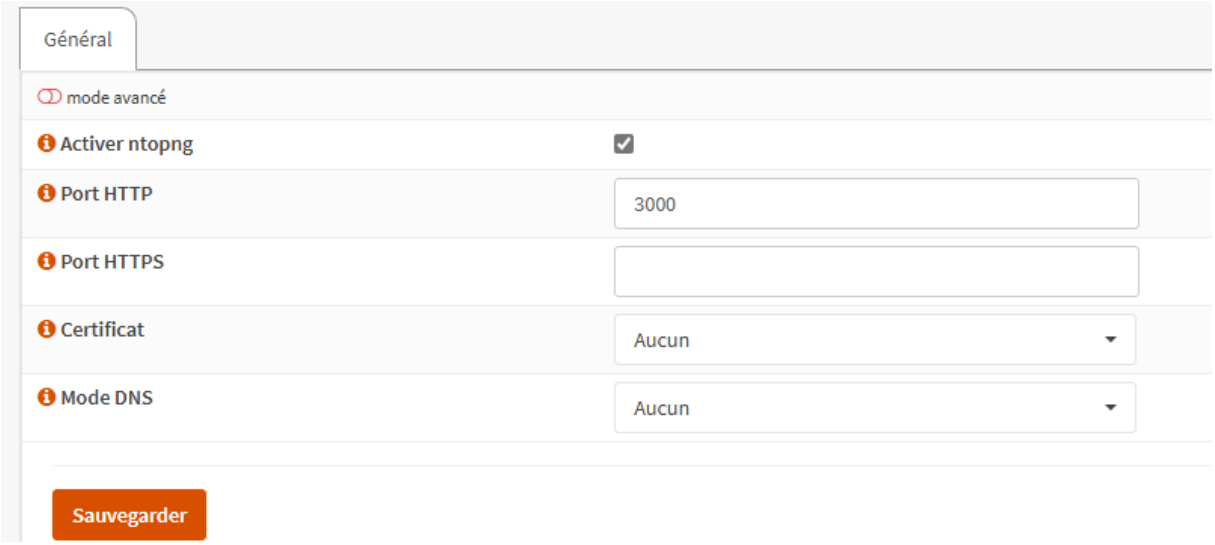
Etape 3 : Même démarcher pour installer « os-redis[19] »

[18] Visualiseur/analyste de trafic réseau : reçoit les données NetFlow et les présente dans une interface graphique.

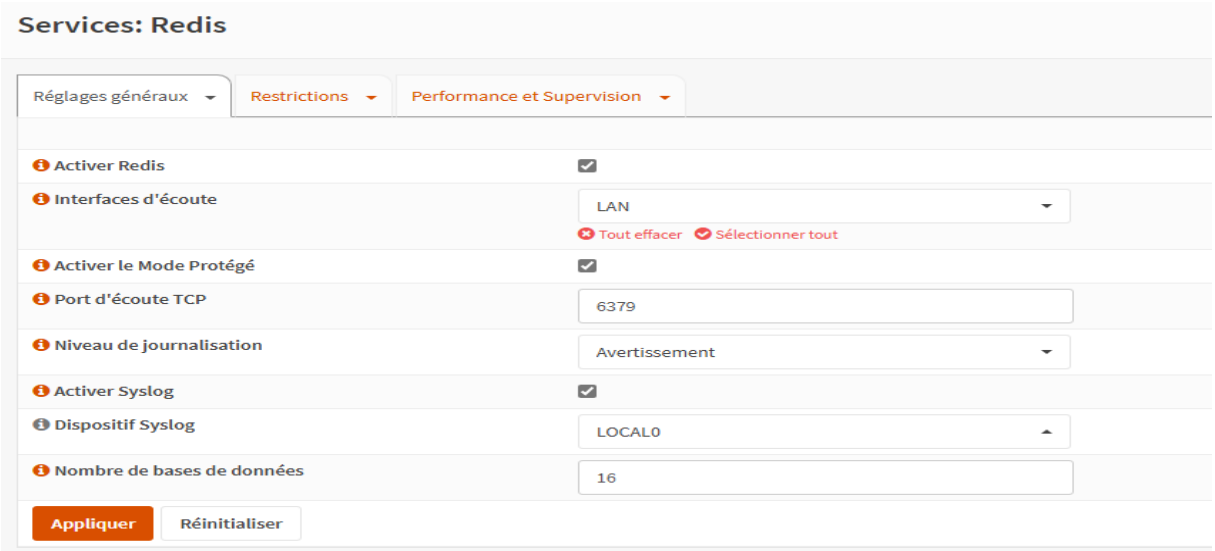
[19] Base de données en mémoire rapide, utilisée par ntopng pour stocker temporairement les données réseau, dans OPNsense ntopng pas fonctionner sans Redis.

Etape 4 : Configurer Ntopng et Redis

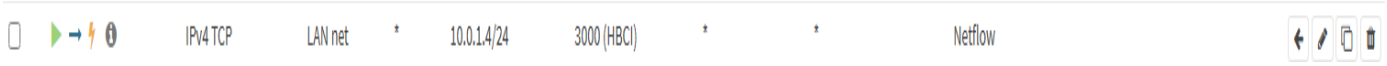
1. Configurer Ntopng
→Cocher « Activer »
→Laisser le port HTTP « 3000 »
→Sauvegarder



2. Configurer Redis
→Cocher « Activer »
→Choisir l'interface d'écoute
→ « Activer le mode protégé »
→ »Activer Syslog »

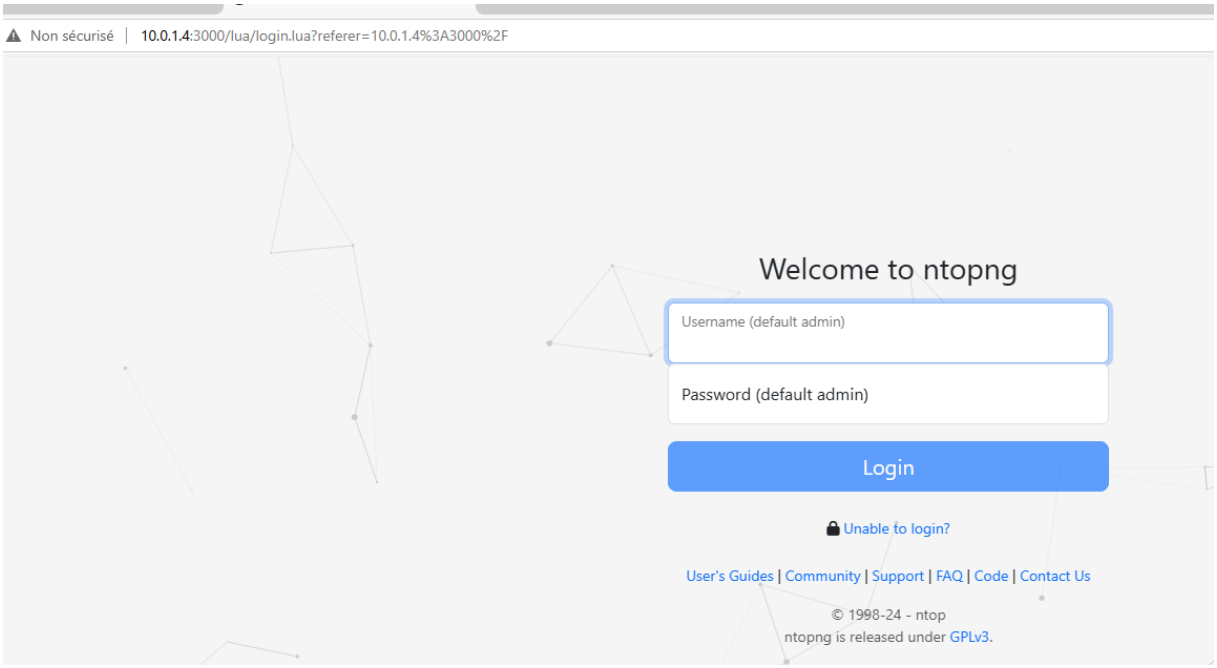


Etape 5 : Créer une règle LAN permettant accès à l'interface web Ntopng



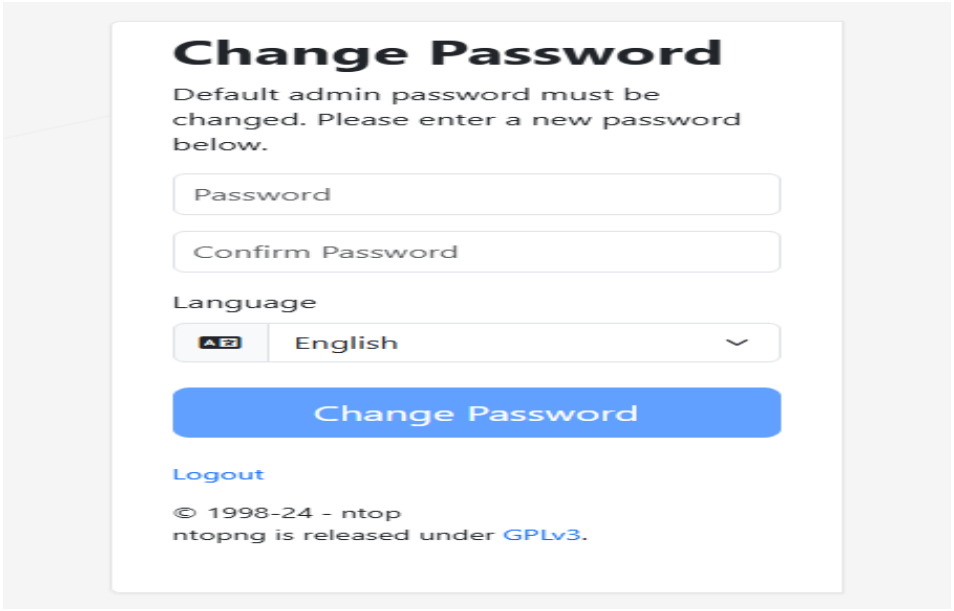
Etape 6 : Se rendre sur l'interface web de Ntopng

1. Rendrer dans barre recherche navigateur adresse ip : http://10.0.1.4:3000

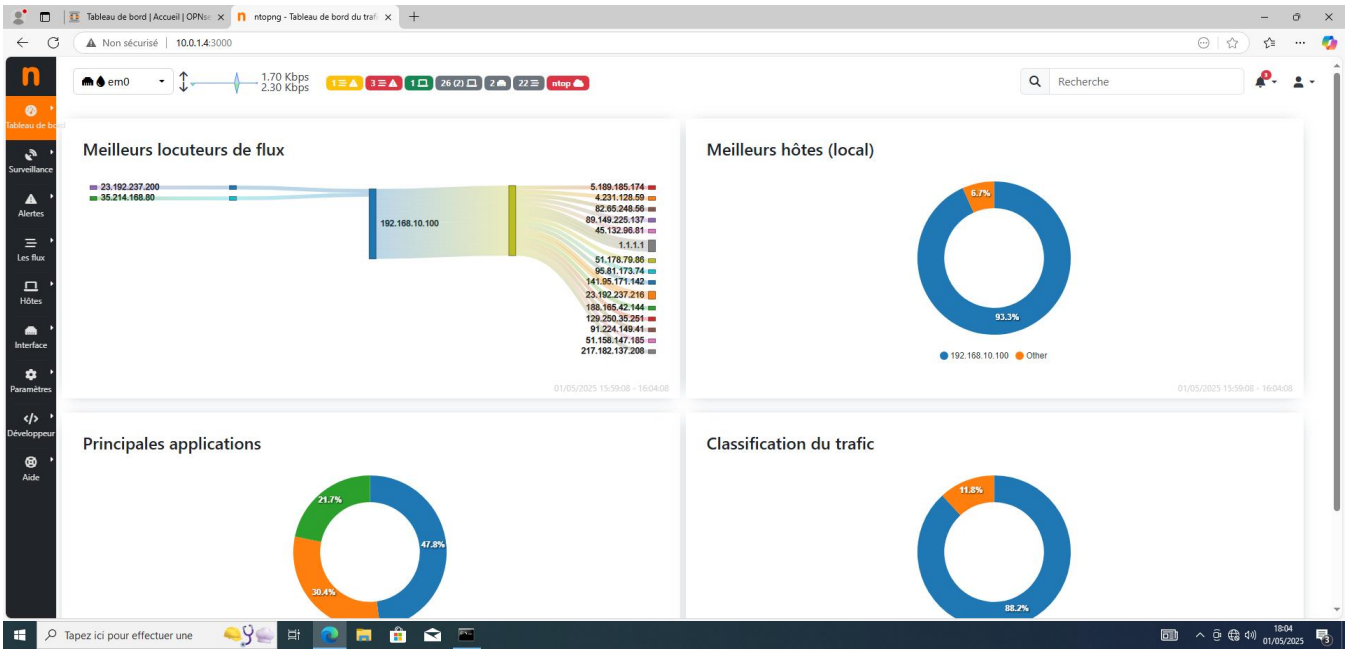


2. Accès rentrer comme username et password par défaut : admin

3.Changer mot de passe + sélectionner langue « French »



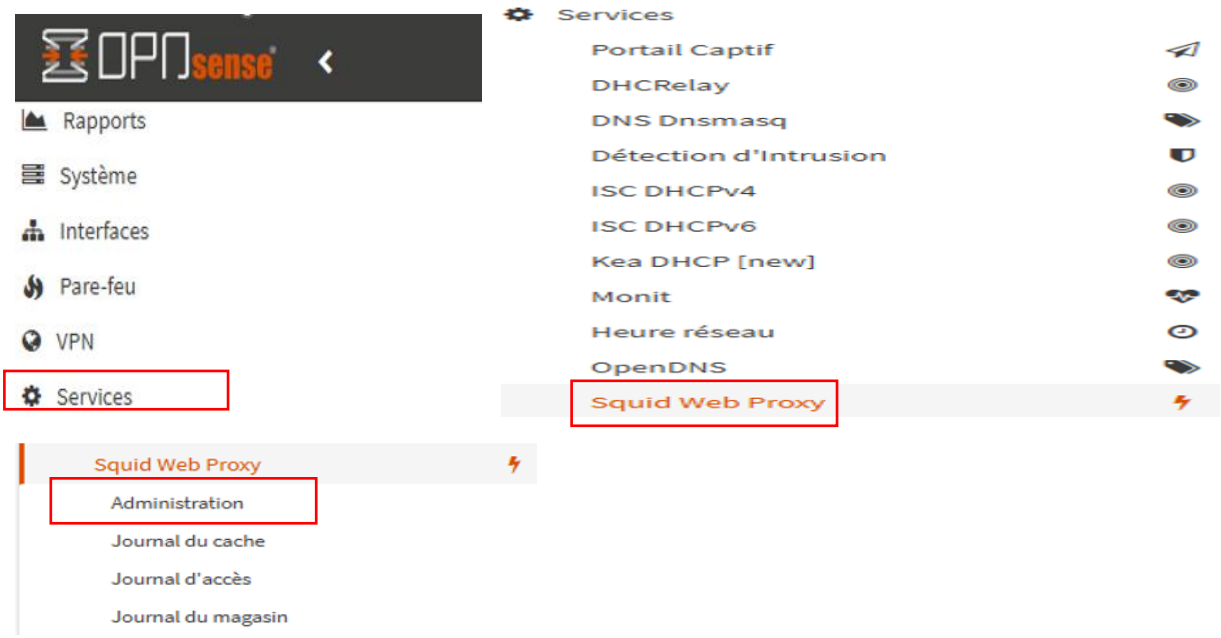
4. Bienvenue sur l’interface web Ntopng



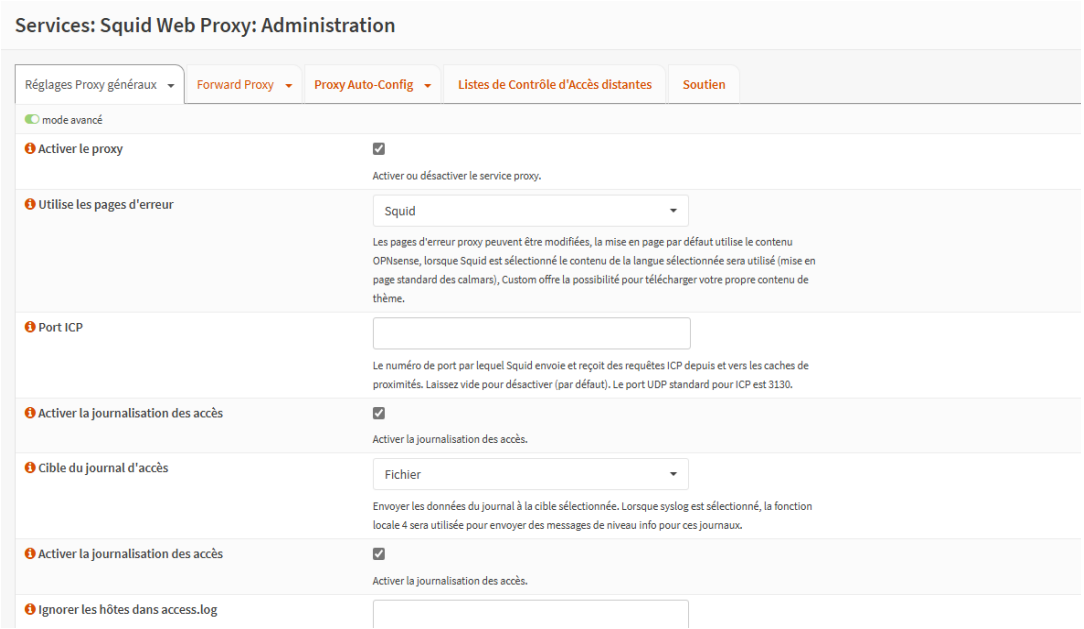
7) Configuration du proxy Squid (ici exemple sur interface LAN)

Etape 1 : Activer le proxy Squid

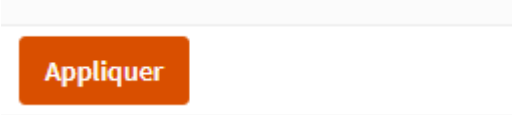
1. Aller : Cliquer sur « Services » > Cliquer sur « Squid Web Proxy » > Cliquer sur « Administration »



2. Cocher « Mode Avancée » > Cocher sur « Activer le proxy » > Cocher sur « Activer la journalisation des accès »

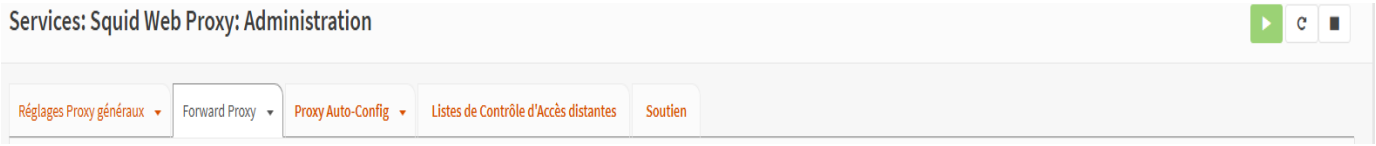


3. Cliquer sur «Appliquer »

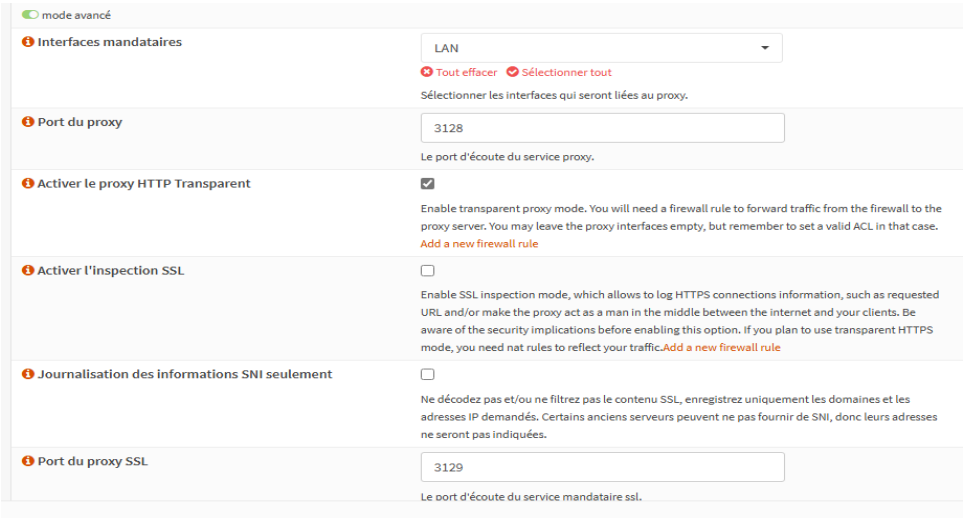


Etape 2 : Activer le mode transparent

1. Cliquer sur « Forward proxy »



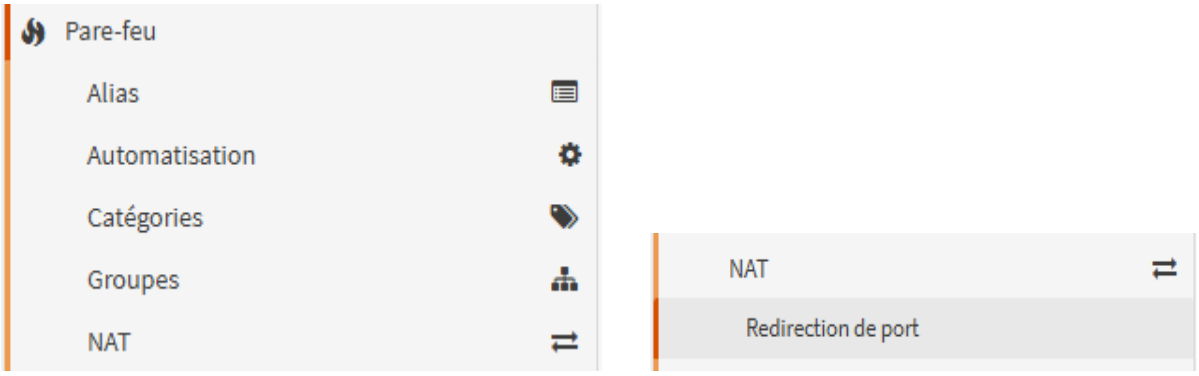
2. Cocher « Activer le **mode transparent**[20] » > Sélectionner « Interfaces mandataires » > Choisir « Lan » > Cliquer sur « Appliquer »



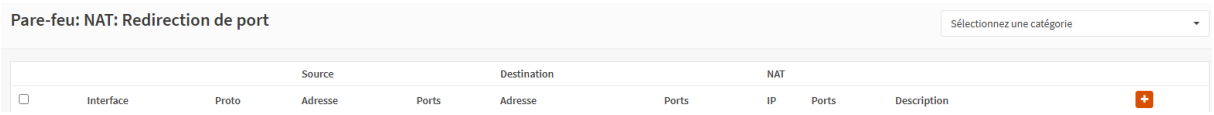
[20] Avec le mode transparent : firewall rediriger automatiquement trafic web (port 80) vers le proxy + utilisateur rien à configurer + tout passer par le proxy, de force. Différent mode clair : tout configurer manuellement chaque poste (navigateur, OS) pour utiliser proxy + si utilisateur pas le faire pas, le trafic sortir direct vers Internet, bypassant le proxy.

Etape 3 : Créer une règle NAT de redirection vers le proxy (ici cas trafic HTTP, pas HTTPS car nécessiter interception SSL, configuration possible plus tard)

1. Cliquer sur « Pare-feu » > Cliquer sur « Nat » > Cliquer sur « Redirection de port »

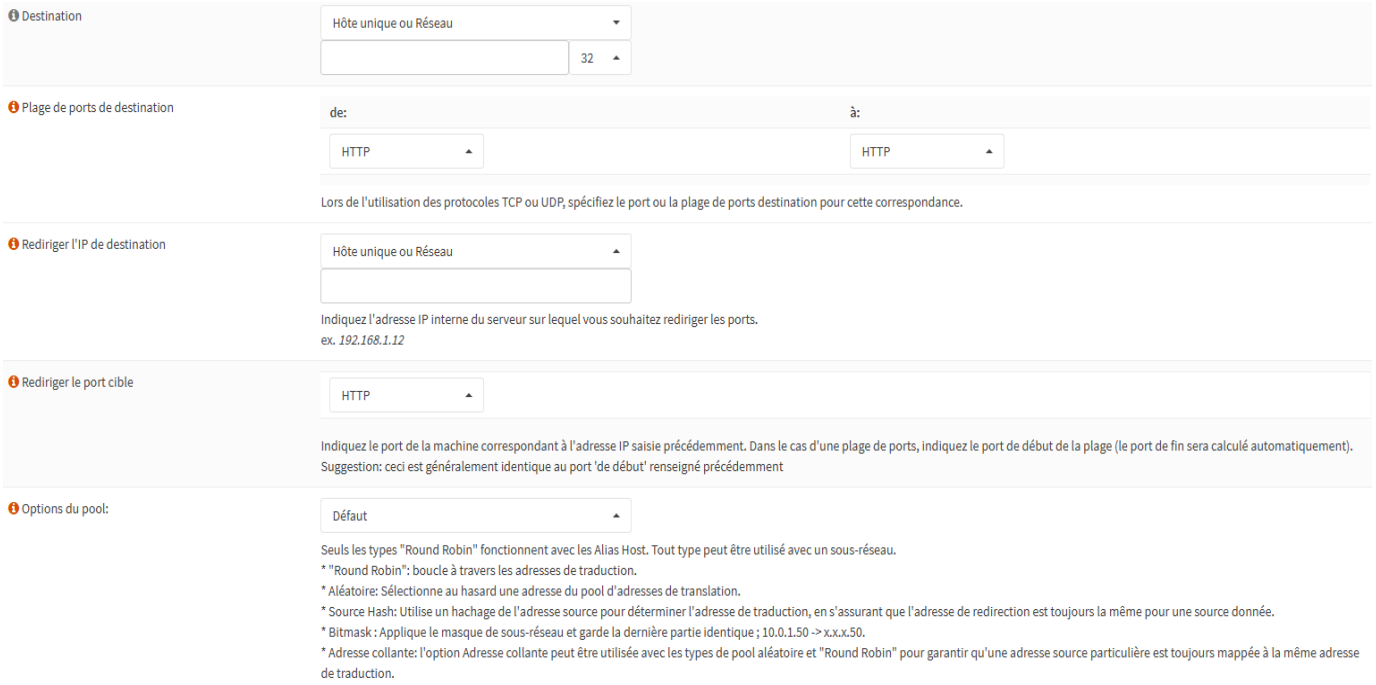


2. Cliquer sur « + »



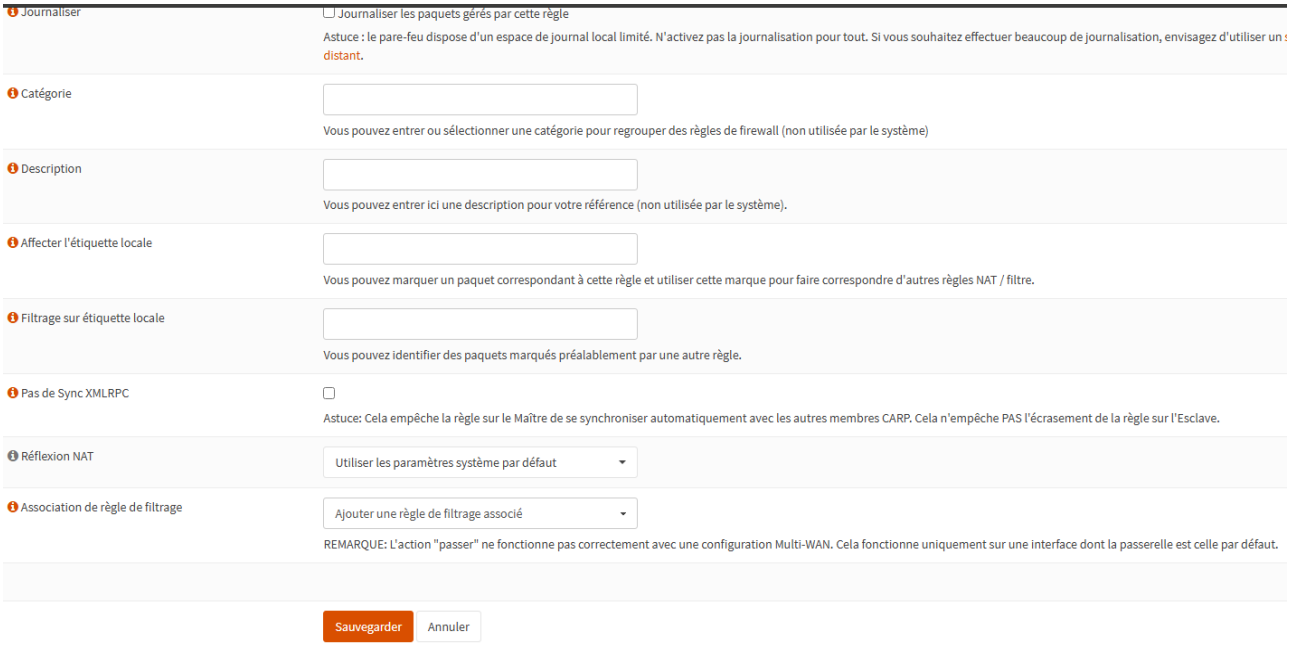
3. → Cliquer « Interface » > Choisir « LAN »
   → « Version TCP/IP » laisser « IPv4 »
   → « Protocole » laisser « TCP »
   → « Source » laisser vide ou choisir « Any »

4. → « Destination » laisser vide signife « tout trafic vers n'importe quelle destination »
   → « Plages de ports destination » laisser http
   → « Rediriger l'IP de destination » : 127.0.0.1 (proxy fonctionner localement sur OPNsense)
   → « Rediriger le port cible »



5. « Rediriger le port cible » écrire 3128, car port par défaut du proxy Squid

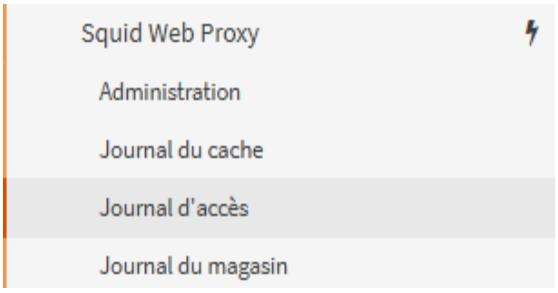
6. « Description » : « rediriger http vers proxy Squid »



7. « Sauvegarder » > « Appliquer les changements »

Etape 4 : Tester redirection du NAT vers le proxy

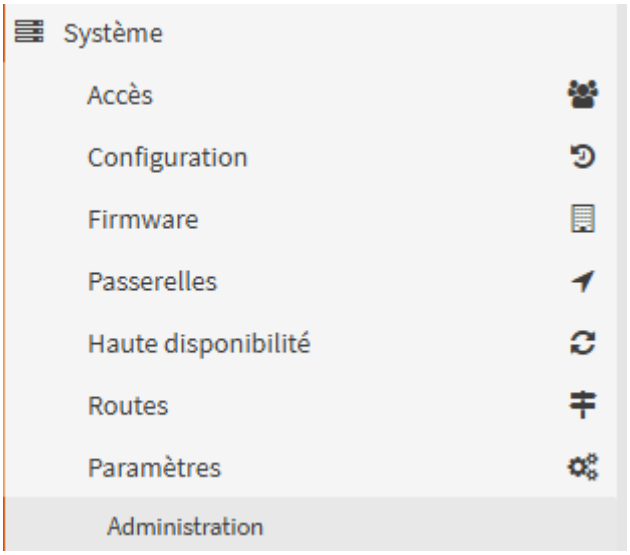
1. Aller : Cliquer sur « Services » > « Squid Web Proxy » > « Journal d'accès » (vérifier les logs du proxy)



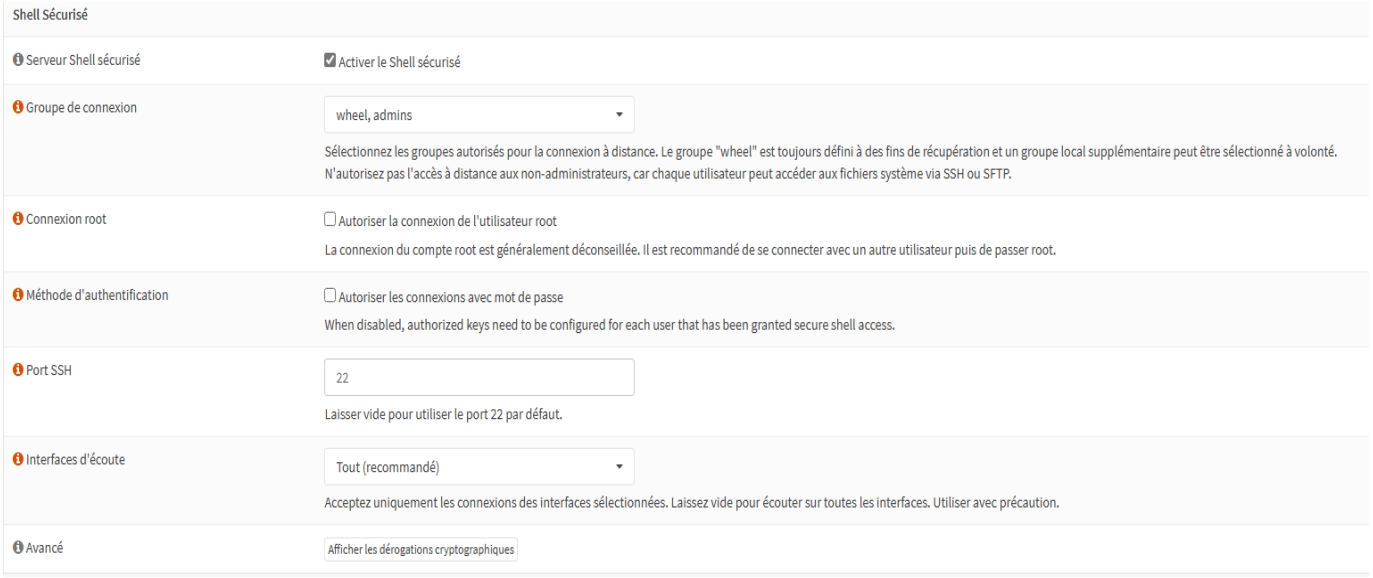
8) Configuration SSH

Etape 1 : Activer le serveur SSH

1. Cliquer sur « Système » > « Paramètres » > « Administration

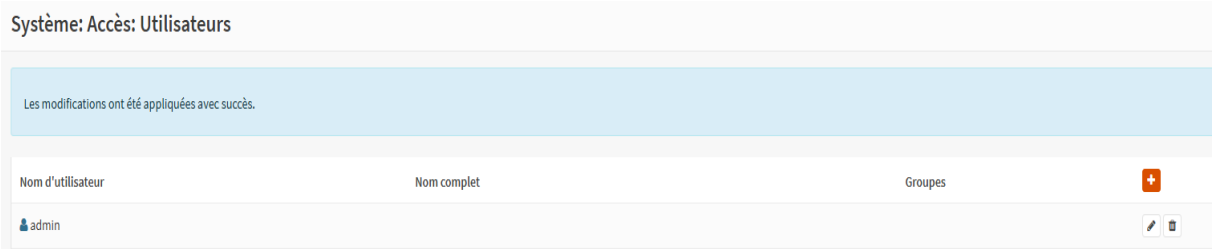


2. → Cocher « Activer le Shell sécurisé »
   → « Connexion root » désactivée pour raisons de sécurité
   → « Méthode d'authenfication » laisser désactiver : connexion par clé uniquement
   →Cliquer sur « Sauvegarder »



Etape 2 : Création clé publique SSH associée à un compte OPNsense

1. Vérifier autre compte que Root auquel associé clé SSH
Ici présente compte « admin » auquel être associé clé SSH créée



2. Création de la clé publique SSH :
→ouvrir Windows PowerShell
→Rentrer commande suivante « ssh-keygen -t rsa -b 2048 -f C:\Users\NomUtilisateur\.ssh\id_rsa »

```
PS C:\Users\a> ssh-keygen -t rsa -b 2048 -f C:\Users\a\.ssh\id_rsa
```

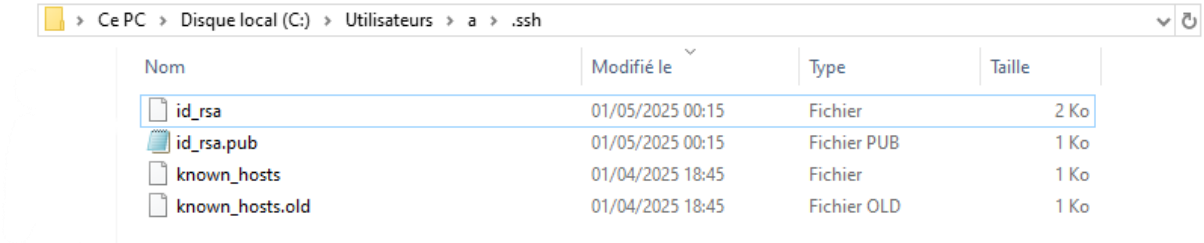
3.Inviter à rentrer une phrase : facultatif > Presser « ENTREE » pour continuer

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

4. Indiquer le chemin où clé générée et enregistrée : Disque C > Dossier « Users » > « Dossier « a » > «Dossier « .ssh »

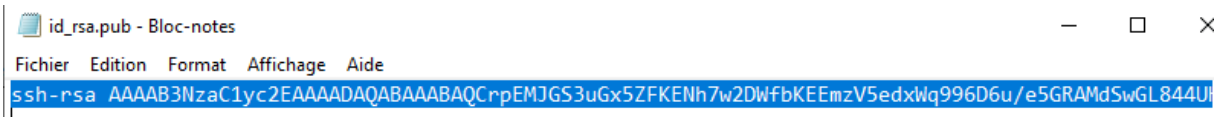
```
Your identification has been saved in C:\Users\a\.ssh\id_rsa
Your public key has been saved in C:\Users\a\.ssh\id_rsa.pub
The key fingerprint is:
SHA256:XEp+N84tkPUrgylNzpE8BxwhC2C6bxX/1HBh1cMmtjw a@DESKTOP-T7Q49E0
The key's randomart image is:
+---[RSA 2048]----+
|      o.. . o.o.o. |
|     o    . + o + +.|
|  .     . o = = + .|
|   .     * + O E   |
|    .   . S @ = o  |
|     . .   O @ o . |
|      o     . B * o|
|       .      .   +|
|                   |
+----[SHA256]-----+
```

5. Choisir clé dans « id_**rsa**.pub[21] » : attention « id_rsa » = Clé privée donc restée confidentielle !



[21] RSA : Clé être de type RSA 2048 bits : RSA algorithme de chiffrement asymétrique (Rivest Shamir Adelman) + longueur clé utilisée dans algorithme être taille clé 2048 bits

6. Copier la totalité de la clé publique



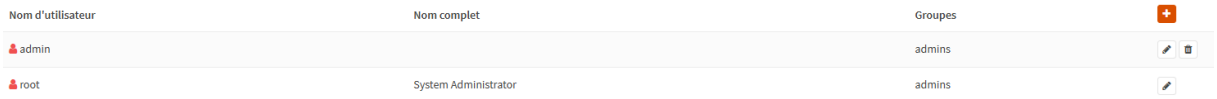
7. →Modifier dans compte « admin » « Shell de connexion » > Choisir « /bin/csh » permettre de se connecter via SSH + utiliser un shell classic

→ Ajouter la clé publique à OPNsense au compte « admin »

8. Rendre membre le compte « admin » dans groupe « admins »

9. Coller la clé publique SSH dans « Clés autorisées » > « Sauvegarder et sortir »

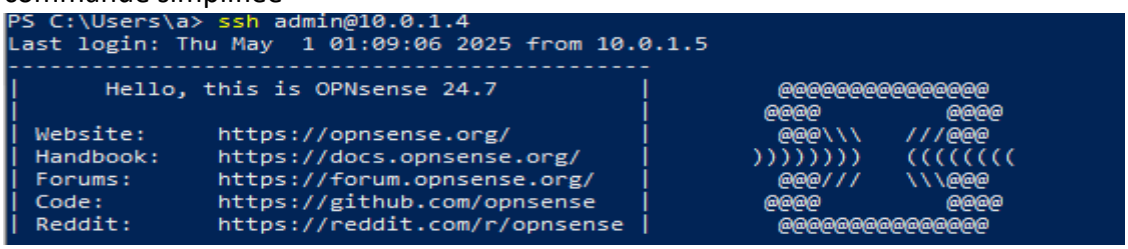
10. Compte « admin » bien dans groupe « admins » : couleur « Nom d'utilisateur » passée à orange = tres important si pas dans ce groupe pas accès via ssh.



Etape 3 : Vérifier que cela fonctionne

1. Ouvrir PowerShell

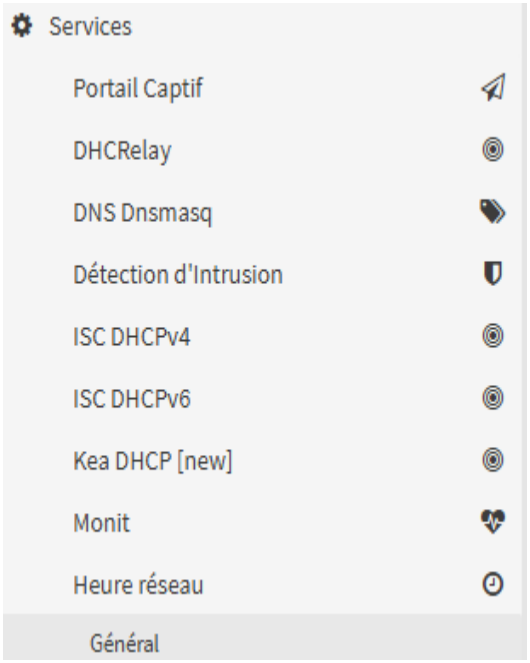
2. Rentrer commande « ssh NomUtilisateur@adresseIPinterfaceOPNsense » exemple « ssh admin@10.0.1.4 » («admin » = nom compte utilisateur créé dans OPNsense)
Ci-dessous menu texte (TUI) de l'interface console d'OPNsense : interface en ligne de commande simplifiée



9) Configuration NTP

Etape 1 : Vérifier le service NTP

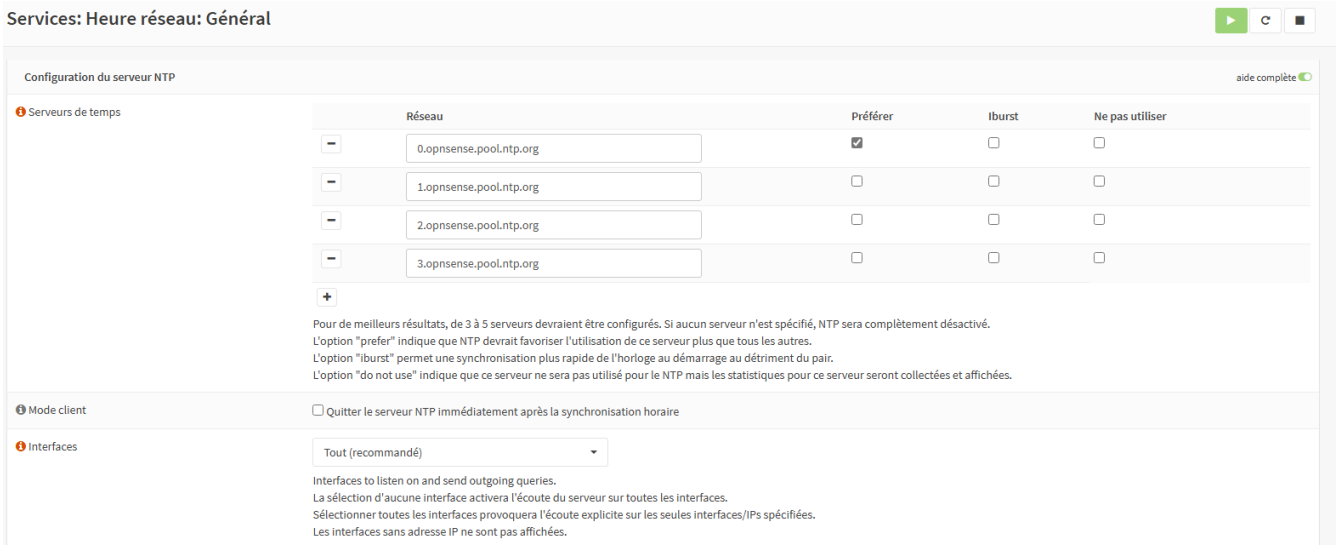
1. Accéder au service : « Services » > « Heure réseau » > « Général »



2. →Serveurs de temps : ici 4 serveurs NTP

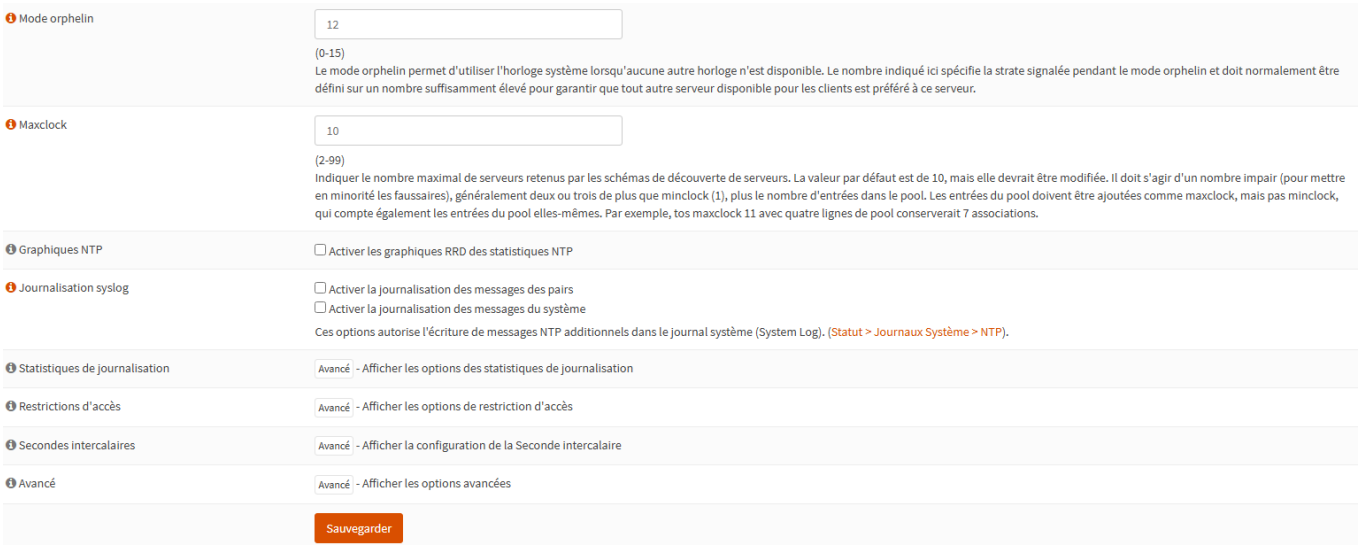
→Serveur « 0.opnsense.pool.ntp.org » : serveur NTP principal qu'OPNsense doit prioriser pour synchronisation = ne pas modifier

→Laisser interface d'écoute sur « Tout » : recevoir et répondre via toutes les interfaces disponibles

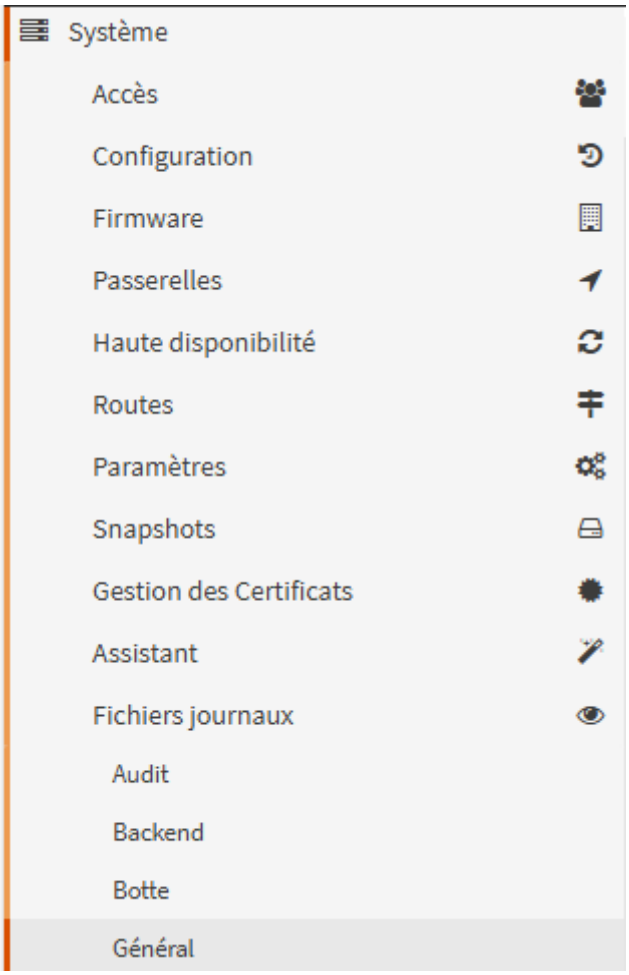


3. → Cocher « Activer les graphiques RRD des statistiques NTP » : surveiller visuellement la synchronisation avec les serveurs NTP

→ Cliquer sur « Sauvegarder »

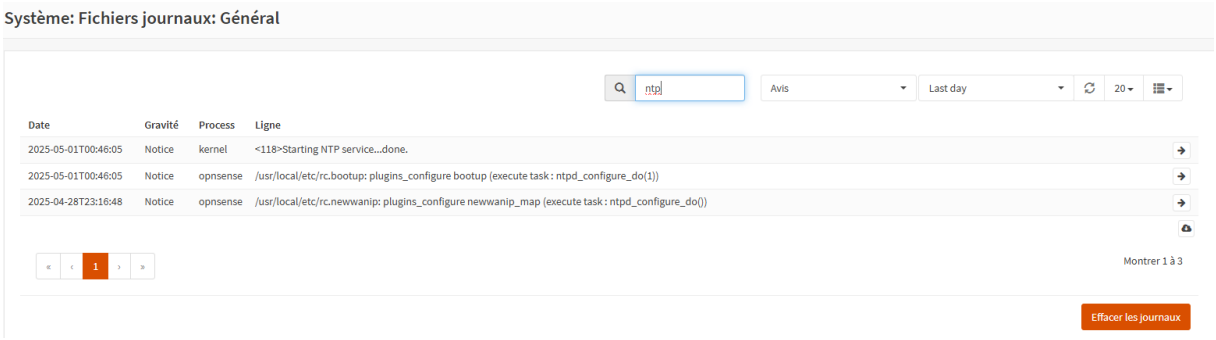


4. Vérifier NTP fonctionnel : « Système » > « Fichiers journaux » > « Général »



5. Filtrer par « NTP »

Ici service NTP bien démarré : « <118> Starting NTP service... done. »



Etape 2 : Test côté client

1. Vérification côté client : ouvrir PowerShell > Rentrer commande « w32tm /stripchart /computer:10.0.1.4 /samples:5 /dataonly »

*Client bien communiqué avec le serveur NTP situé à 10.0.1.4

*reçu 5 échantillons valides

*décalage stable à environ -1,64 seconde, signifiant que l'horloge locale être en avance d'un peu plus d'une seconde, mais synchronisée donc serveur NTP fonctionner correctement

```
PS C:\Users\a> w32tm /stripchart /computer:10.0.1.4 /samples:5 /dataonly
Suivi de 10.0.1.4 [10.0.1.4:123].
Collecte de 5 échantillons.
L'heure actuelle est 01/05/2025 01:36:24.
01:36:24, -01.6415393s
01:36:26, -01.6415022s
01:36:28, -01.6416287s
01:36:30, -01.6415064s
```