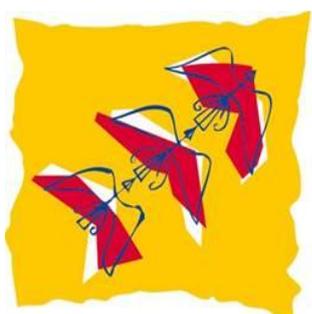


**Guide de configuration et d'administration du pare-feu
OPNsense**



La Région

Lorraine

Table des matières

1) Définir les interfaces	3
Etape 1 : Définir l'adresse IP de l'interface WAN	3
Etape 2 : Définir l'adresse IP de l'interface LAN	5
2) Configuration adressage pc administrateur.....	6
3) Accès et configuration initiale du pare-feu	8
Etape 1 : Accès interface web GUI	8
Etape 2 : Configuration initiale d'OPNsense	9
4) Configuration des règles (cas du LAN).....	13
Etape 1 : Supprimer les règles existantes	13
Etape 2 : Créer une règle LAN vers WAN : ici règle DNS	14
Etape 3 : Créer les autres règles.....	17
Etape 4 : Vérifier cela fonctionne depuis poste client situé dans même réseau que le LAN....	18
5) Configuration Suricata	20
Etape 1 : Activer et configurer Suricata.....	20
Etape 2 : Télécharger les règles	21
Etape 3 : Exemple règle ET open/compromised	22
6) Configuration Netflow	24
Etape 1 : Configurer Netflow.....	24
Etape 2 : Télécharger le greffon « os-ntopng »	25
Etape 3 : Même démarcher pour installer « os-redis.....	25
Etape 4 : Configurer Ntopng et Redis.....	26
Etape 5 : Créer règle LAN permettant accès interface web Ntopng.....	27
Etape 6 : Se rendre sur l'interface web de Ntopng.....	27
7) Configuration du proxy Squid (ici exemple sur interface LAN).....	29
Etape 1 : Activer le proxy Squid	29
Etape 2 : Activer le mode transparent.....	30
Etape 3 : Créer règle NAT de redirection vers proxy	31
Etape 4 : Tester redirection du NAT vers le proxy	33
8) Configuration SSH	34
Etape 1 : Activer le serveur SSH	34
Etape 2 : Création clé publique SSH associée à un compte OPNsense.....	35
Etape 3 : Vérifier que cela fonctionne	36
9) Configuration NTP.....	37
Etape 1 : Vérifier le service NTP.....	37
Etape 2 : Test côté client.....	39

1) Définir les interfaces

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

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

```
HTTPS: sha256 9C 7B 0A 6D BD FC 7A ED 09 5C D9 8F 14 CD 48 C9
          33 57 4A AB 2F B5 1E 42 8D CF F9 94 7D 3C 47 32

0) Logout                                7) Ping host
1) Assign interfaces                      8) Shell
2) Set interface IP address              9) pfTop
3) Reset the root password               10) Firewall log
4) Reset to factory defaults            11) Reload all services
5) Power off system                     12) Update from console
6) Reboot system                        13) Restore a backup

Enter an option: █
```

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

```
Enter an option: 2

Available interfaces:

1 - LAN (em1 - static)
2 - OPT1 (em2)
3 - OPT2 (em3)
4 - WAN (em0 - static, dhcp6)

Enter the number of the interface to configure: 4
```

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

```
Configure IPv4 address WAN interface via DHCP? [Y/n] n
```

4. Rentrer adresse IP du WAN

```
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 172.16.0.124
```

5. Rentrer le masque sous forme décimale

```
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 WAN IPv4 subnet bit count (1 to 32):
> 22
```

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

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.16.0.1
```

7. → « N » : pas utiliser cette adresse comme passerelle par défaut

→ « N » : ni l'utiliser comme Domain Name Server

```
Do you want to use it as the default IPv4 gateway? [Y/n]
Do you want to use the gateway as the IPv4 name server, too? [Y/n]
```

8. « N » : pas configurer d'adresse IPv6 interface WAN via le DHCP

Appuyer sur « ENTREE » pour ne pas rentrer d'adresse IPv6 au WAN

```
Configure IPv6 address WAN interface via DHCP? [Y/n] n
Enter the new WAN IPv6 address. Press <ENTER> for none:
> n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
```

9. → « N » : pas changer le protocole de l'interface web (web GUI) de HTTPS¹ à HTTP

→ « N » : pas générer nouveau certificat auto-signé² pour l'interface web

→ « N » : ne pas restorer les accès par défaut à l'interface web

Choix permettre conserver interface web sécurisé

```
Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N]
Do you want to generate a new self-signed web GUI certificate? [y/N]
Restore web GUI access defaults? [y/N]

Writing configuration...done.
Generating /etc/resolv.conf...done.
Generating /etc/hosts...done.
Configuring WAN interface...done.
Setting up routes for wan...done.
Setting up gateway monitor for WAN_GW_2, WAN_GW...done.
Starting Unbound DNS...done.
Configuring firewall..
```

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
```

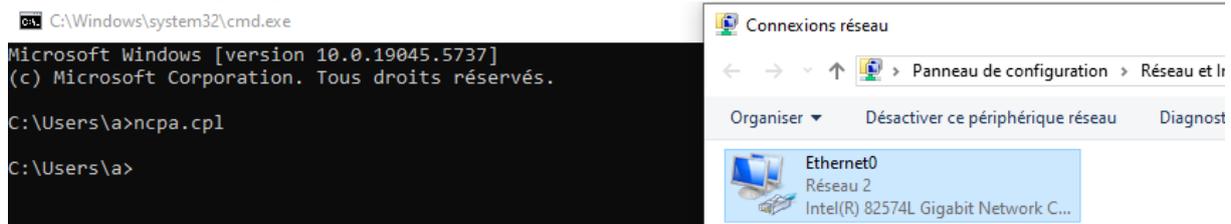
2. Presser « ENTREE » : pas besoin d'une passerelle configurée pour l'interface LAN

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

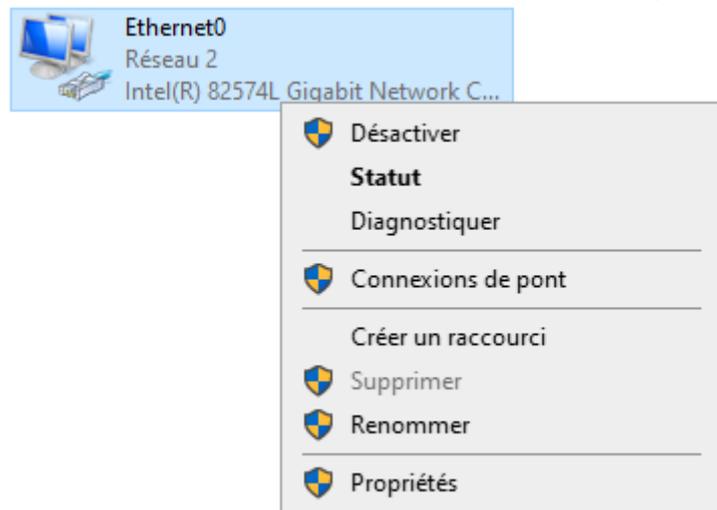
2) Configuration adressage pc administrateur

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»

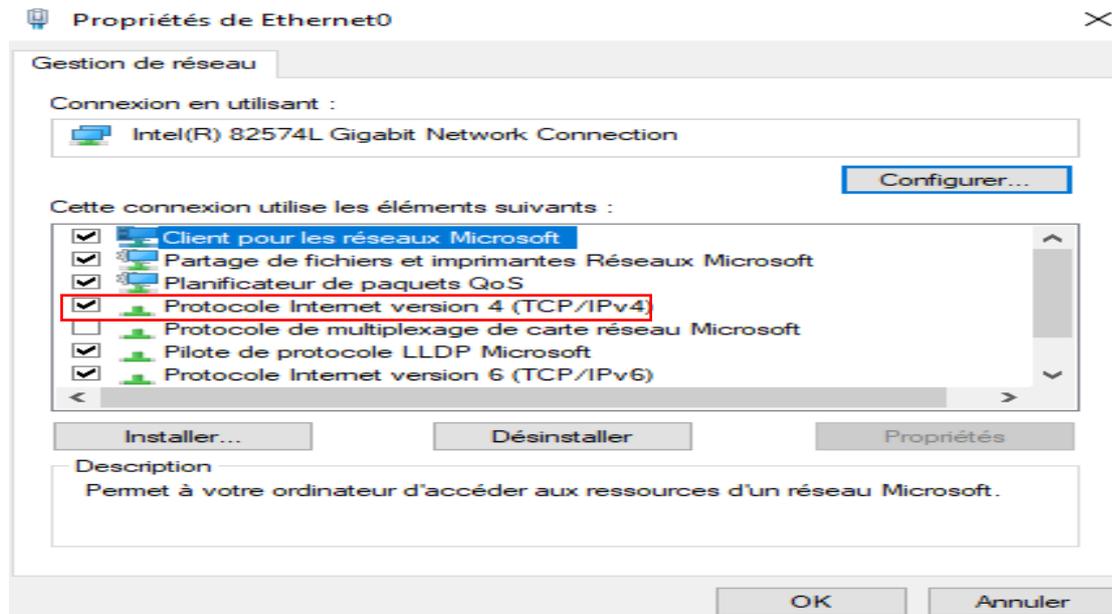


2. Clic droit l'interface réseau « Ethernet 0 » > Cliquer sur « Propriétés »



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

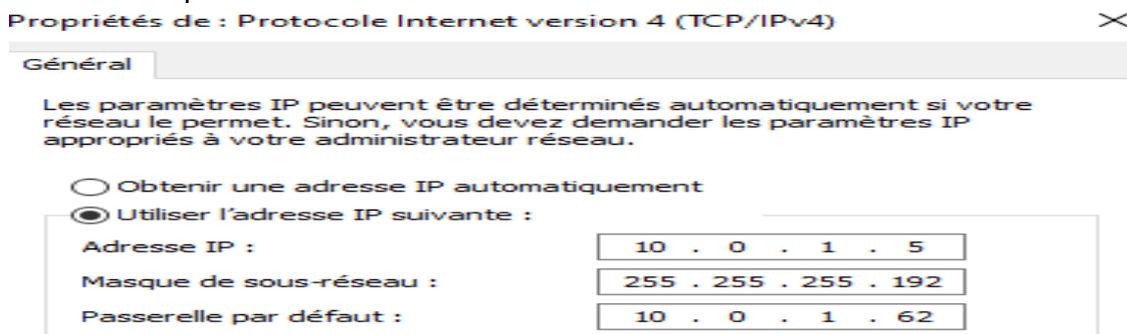
3. Doubles clics sur « Protocole Internet version 4 (TCP/IPv4) »



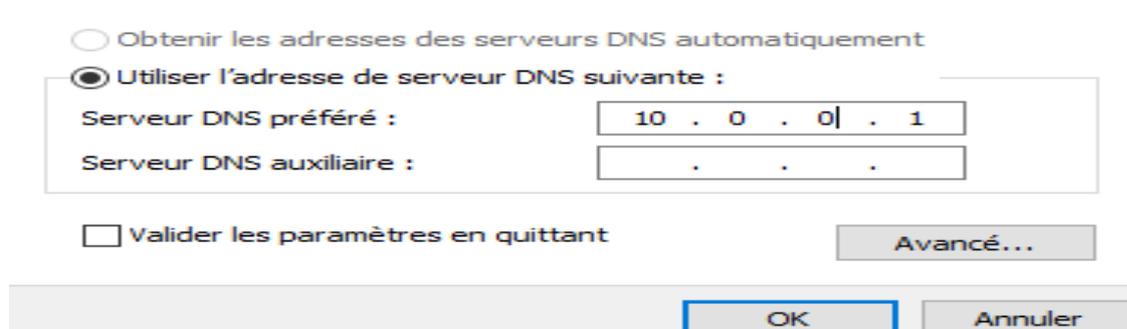
4. → Rentrer dans « Adresse IP » : une adresse IPv4 disponible dans la plage d'adressage du VLAN dans lequel être le pc administrateur

→ 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)

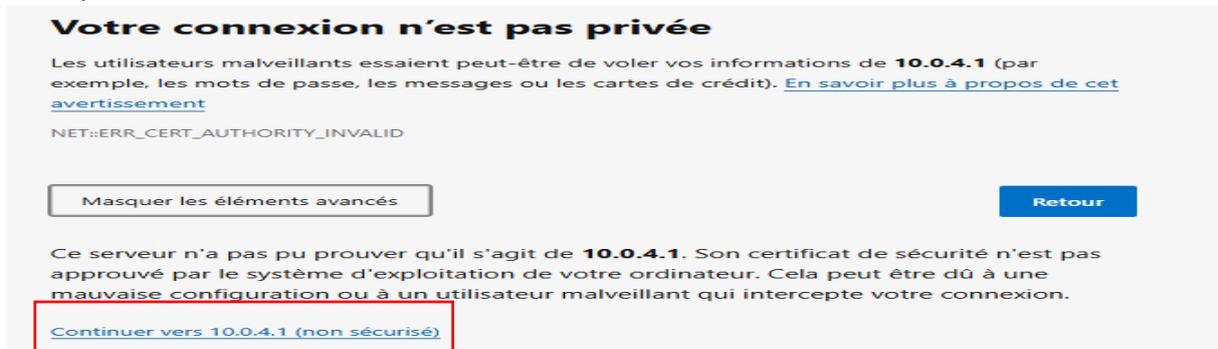


3. Cliquer sur « Avancé »

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 »

System: Wizard: General Setup

This wizard will guide you through the initial system configuration. The wizard may be stopped at any time by clicking the logo image at the top of the screen.

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

System: Wizard: General Information

General Information

Hostname: OPNsense

Domain: localdomain

Language: French

Primary DNS Server: 1.1.1.1

Secondary DNS Server:

Override DNS: Allow DNS servers to be overridden by DHCP/PPP on WAN

Unbound DNS

Enable Resolver:

Enable DNSSEC Support:

Harden DNSSEC data:

Next

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

3. « Timezone » : choix du fuseau 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

System: Wizard: Time Server Information

Time server hostname:

Enter the hostname (FQDN) of the time server.

Timezone:

- Europe/Helsinki
- Europe/Isle_of_Man
- Europe/Istanbul
- Europe/Jersey
- Europe/Kaliningrad
- Europe/Kirov
- Europe/Kyiv
- Europe/Lisbon
- Europe/Ljubljana
- Europe/London
- Europe/Luxembourg
- Europe/Madrid
- Europe/Malta
- Europe/Mariehamn
- Europe/Minsk
- Europe/Monaco
- Europe/Moscow
- Europe/Oslo
- Europe/Paris**
- Europe/Podgorica

Next

OPNsense (c) 2014-2025 Deciso B.V.

4. Choix serveur NTP⁶

System: Wizard: Time Server Information

Time server hostname:

Enter the hostname (FQDN) of the time server.

Timezone:

Next

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 synchroniser de 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 »

Système: Assistant: Configurer l'interface WAN

Type de configuration IPv4: DHCP

Configuration générale

Adresse MAC:

Ce champ peut être utilisé pour modifier ("spoof") l'adresse MAC de l'interface WAN (peut être nécessaire avec certaines connexions par câble). Entrez une adresse MAC au format suivant: xx:xx:xx:xx:xx:xx ou laissez vide.

MTU (Maximum Transmission Unit):

Définissez la MTU de l'interface WAN. Si vous laissez ce champ vide, une MTU de 1492 octets pour PPPoE et de 1500 octets pour tous les autres types de connexion sera utilisée.

MSS:

Si vous entrez une valeur dans ce champ, le bridage MSS des connexions TCP avec la valeur entrée ci-dessus moins 40 (taille de l'en-tête TCP / IP) sera effectif. Si vous laissez ce champ vide, un MSS de 1492 octets pour PPPoE et de 1500 octets pour tous les autres types de connexion sera utilisé. Cela doit correspondre à la valeur MTU ci-dessus dans la plupart des cas.

Configuration IP statique

Adresse IP:

Passerelle amont:

8. Décocher « Bloquer les Réseaux Privés RFC1918⁷ » : 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).

Réseaux RFC1918

Bloquer les Réseaux Privés RFC1918: Bloquer l'accès des réseaux privés via le WAN

Lorsqu'elle est définie, cette option bloque le trafic des adresses IP réservées aux réseaux privés conformément à la RFC 1918 (10/8, 172.16/12, 192.168/16) ainsi que les adresses de bouclage (127/8) et les adresses NAT de classe opérateur (100.64/10). Cette option ne doit être définie que pour les interfaces WAN qui utilisent l'espace d'adressage IP public.

Bloquer les adresses bogon (non attribuées par l'IANA)

Bloquer les adresses bogon (non attribuées par l'IANA): Bloquer l'accès des réseaux non routés par Internet via le WAN.

Lorsque cette option est activée, elle bloque le trafic provenant des adresses IP réservées ou les adresses non encore affectées par l'IANA (mais pas au sens de la RFC 1918).

9. Adresse IP du LAN + masque sous-réseau

Système: Assistant: Configurer l'interface LAN

Adresse IP LAN:

(Laisser vide pour aucun)

Masque de 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 »

Système: Assistant: Définir le Mot de passe Root

Mot de passe Root:

(Laisser vide pour garder l'actuel(le))

Confirmation Mot de passe Root:

[Suivant](#)

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

[Suivant](#)

Cliquez 'Recharger' pour appliquer les changements.

[Recharger](#)

Configuration initiale terminée!



Félicitations! OPNsense est maintenant configuré.

Veuillez envisager de faire un don au projet pour nous aider à payer nos frais généraux. Consultez [notre site internet](#) pour faire un don ou acheter des services d'assistance OPNsense disponibles.

Cliquez pour continuer vers [le tableau de bord](#). Ou cliquez sur [check for updates](#).

4) Configuration des règles (cas du LAN)

Etape 1 : Supprimer les règles existantes

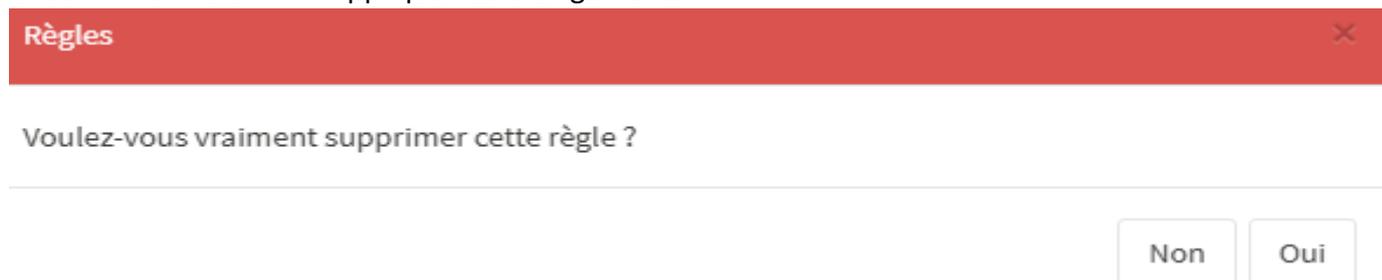
1. Aller : « Pare-feu » > « Règles » > « LAN »



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

<input type="checkbox"/>		IPv4 *	LAN net	*	*	*	*	*	Default allow LAN to any rule		
<input type="checkbox"/>		IPv6 *	LAN net	*	*	*	*	*	Default allow LAN IPv6 to any rule		

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



Etape 2 : Créer une règle LAN vers WAN : ici règle DNS⁸

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)

Pare-feu: Règles: LAN

Éditer la règle du pare-feu

Action Autoriser

Désactivé Désactiver cette règle

Autoriser

Autoriser

Bloquer

Rejeter

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

Interface LAN

LAN

LAN

OPT1

OPT2

WAN

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

Direction in

in

in

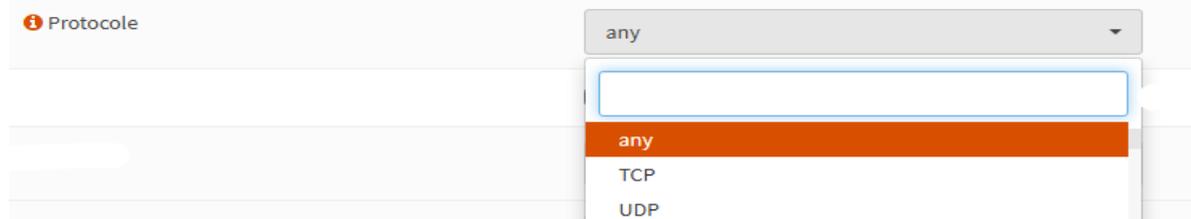
out

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

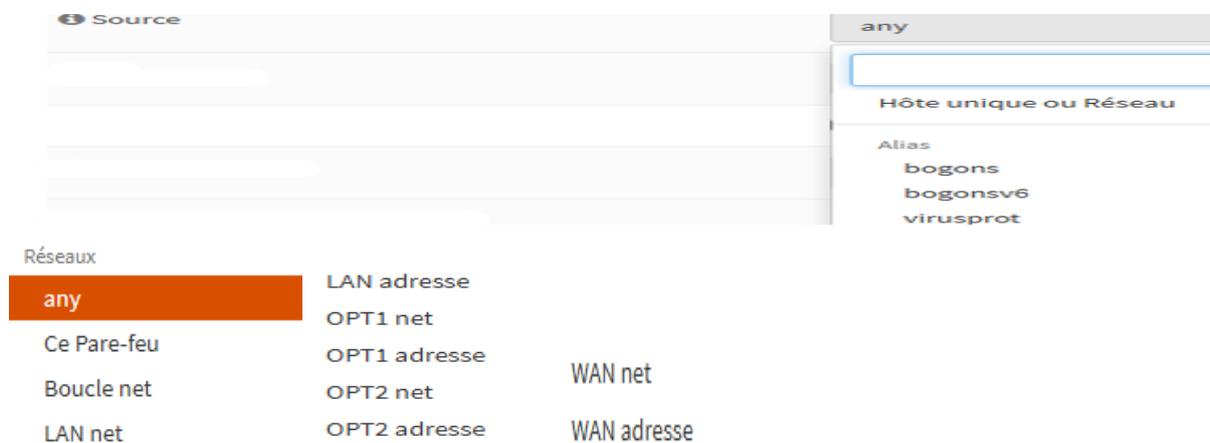
5. Choix du protocole réseau utilisé (IPv4/IPv6/IPv4+IPv6)



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

Destination any

Réseaux

any	LAN adresse	
Ce Pare-feu	OPT1 net	
Boucle net	OPT1 adresse	
LAN net	OPT2 net	WAN net
	OPT2 adresse	WAN adresse

Ici : « Any »

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

Plage de ports de destination de: à:

DNS DNS

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

Journaliser Journaliser les paquets gérés par cette règle

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

Catégorie

Description

Pas de Sync XMLRPC

Planifier aucun(e) ▼

Passerelle défaut ▲

Fonctionnalités avancées **Afficher/Masquer**

Sauvegarder **Annuler**

12. « Sauvegarder » > « Appliquer les changements »

IPv4 UDP LAN net * * 53 (DNS) * * Autoriser DNS LAN vers Internet

Etape 3 : Créer les autres règles

1. Règle autorisant le trafic HTTP



2. Règle autorisant le trafic HTTPS



3. Règle autorisant le protocole ICMP⁹



4. Règle empêchant tout trafic non autorisé



5. Résumé des règles créées

Pare-feu: Règles: LAN

Sélectionnez une catégorie

Inspecter

Les modifications ont été appliquées avec succès.

Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description
							Règles générées automatiquement
IPv4+6 UDP	LAN net	*	*	53 (DNS)	*	*	Autoriser DNS LAN vers Internet
IPv4+6 TCP	LAN net	*	*	80 (HTTP)	*	*	Autoriser HTTP
IPv4+6 TCP	LAN net	*	*	443 (HTTPS)	*	*	Autoriser HTTPS
IPv4+6 ICMP	LAN net	*	*	*	*	*	Protocole ICMP autoriser depuis LAN
IPv4+6 *	*	*	*	*	*	*	Bloquer le reste

autoriser bloquer rejeter tracer entrant première correspondance
passer (désactivé) bloquer (désactivé) rejeter (désactivé) tracer (désactivé) sortant dernière correspondance

Programme actif/inactif (cliquez pour afficher/modifier)

Alias (cliquez pour visualiser/éditer)

Les règles LAN sont évaluées sur la base de la première correspondance par défaut (c'est-à-dire que l'action de la première règle pour correspondre à un paquet sera exécutée). Cela signifie que si vous utilisez des règles de blocage, vous devrez faire attention à l'ordre des règles. Tout ce qui n'est pas explicitement passé est bloqué par défaut.

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

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

¹⁰Programme 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 Suricata¹³

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

~/ Réglages généraux

Activé	<input checked="" type="checkbox"/>	Activer le système de détection d'intrusion.
Mode IPS	<input checked="" type="checkbox"/>	Enable protection mode (block traffic). Before enabling, please disable all hardware offloading first in advanced network .
Mode promiscuité	<input checked="" type="checkbox"/>	Activez le mode promiscuous. Pour certaines configurations (comme IPS avec vlans), cela est nécessaire pour capturer réellement les données sur l'interface physique.
Interfaces	<input type="text" value="LAN, OPT1, OPT2, WAN"/>	<input type="button" value="Tout effacer"/> <input type="button" value="Sélectionner tout"/> Select interface(s) to use. When enabling IPS, make sure the (virtual) driver supports this feature.
~/ Detection		
Recherche de motifs	<input type="text" value="Défaut"/>	Sélectionnez l'algorithme de correspondance multi-modèle à utiliser.
~/ Journalisation		
Activer les alertes syslog	<input type="checkbox"/>	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.
Activer la sortie syslog d'eve	<input type="checkbox"/>	Envoyer les alertes au format eve à syslog, en utilisant les informations sur le niveau de journalisation.

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).

- 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 »

Rotation du journal

Hebdomadaire

Rotation des journaux d'alerte à l'intervalle prévu.

Sauvegarder les journaux

4

Nombre de journaux à garder.

Appliquer

Etape 2 : Télécharger les règles

- Se rendre dans « Téléchargements »



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

Paramètres
Téléchargement
Règles
Défini par l'utilisateur
Alertes
Planifier

Ensemble de règles

Activer la sélection
Désactiver la sélection

<input type="checkbox"/>	ET open/emerging-current_events	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-deleted	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-dns	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-dos	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-exploit	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-exploit_kit	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-ftp	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-games	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-hunting	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-icmp	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-icmp_info	non-installé	x	✎
<input type="checkbox"/>	ET open/emerging-imap	non-installé	x	✎

Recherche

Télécharger et mettre à jour les règles

- Les règles téléchargées apparaitront comme cela

<input type="checkbox"/>	ET open/emerging-current_events	2025/05/01 15:35	✓	✎
<input type="checkbox"/>	ET open/emerging-deleted	2025/05/01 15:35	✓	✎
<input type="checkbox"/>	ET open/emerging-dns	2025/05/01 15:35	✓	✎

- 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 »

<input type="checkbox"/> sid	Action	Source	Type de classe	Message	Info / Activé
<input type="checkbox"/> 2000009	alerte	emerging-deleted.rules	attempted-dos	ET DELETED Cisco IOS HTTP DoS	<input type="checkbox"/>
<input type="checkbox"/> 2000012	alerte	emerging-deleted.rules	attempted-dos	ET DELETED Cisco %u IDS evasion	<input type="checkbox"/>
<input checked="" type="checkbox"/> 2000013	alerte	emerging-deleted.rules	attempted-dos	ET DELETED Cisco IDS HTTP server DoS	<input type="checkbox"/>
<input type="checkbox"/> 2000016	alerte	emerging-deleted.rules	attempted-dos	ET DELETED SSL Bomb DoS Attempt	<input type="checkbox"/>
<input type="checkbox"/> 2000024	alerte	emerging-deleted.rules	trojan-activity	ET DELETED eprograms	<input type="checkbox"/>
<input type="checkbox"/> 2000040	alerte	emerging-deleted.rules	misc-activity	ET DELETED Sasser FTP Traffic	<input type="checkbox"/>
<input type="checkbox"/> 2000041	alerte	emerging-deleted.rules	policy-violation	ET DELETED Yahoo Mail Inbox View	<input type="checkbox"/>
<input type="checkbox"/> 2000042	alerte	emerging-deleted.rules	policy-violation	ET DELETED Yahoo Mail Message View	<input type="checkbox"/>
<input type="checkbox"/> 2000043	alerte	emerging-deleted.rules	policy-violation	ET DELETED Yahoo Mail Message Compose Open	<input type="checkbox"/>
<input type="checkbox"/> 2000045	alerte	emerging-deleted.rules	policy-violation	ET DELETED Yahoo Mail Message Send Info Capture	<input type="checkbox"/>

Alerter

Affichage des entrées 1 à 10 sur 10720

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

<input type="checkbox"/> sid	Action	Source	Type de classe	Message	Info / Activé
<input type="checkbox"/> 2000009	alerte	emerging-deleted.rules	attempted-dos	ET DELETED Cisco IOS HTTP DoS	<input checked="" type="checkbox"/>
<input type="checkbox"/> 2000012	alerte	emerging-deleted.rules	attempted-dos	ET DELETED Cisco %u IDS evasion	<input checked="" type="checkbox"/>
<input type="checkbox"/> 2000013	alerte	emerging-deleted.rules	attempted-dos	ET DELETED Cisco IDS HTTP server DoS	<input checked="" type="checkbox"/>

Etape 3 : Exemple règle ET open/compromised¹⁶

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

Paramètres	Téléchargement	Règles	Défini par l'utilisateur	Alertes	Planifier
Ensemble de règles					
Activer la sélection Déactiver la sélection					
ET Open					
<input type="checkbox"/>		ET open/botcc.portgrouped	non-installé	x	
<input type="checkbox"/>		ET open/clarmy	non-installé	x	
<input checked="" type="checkbox"/>		ET open/compromised	non-installé	x	

2. Télécharger et mettre à jour la règle

<input type="checkbox"/> ET open/compromised	2025/05/01 16:11	✓	
--	------------------	---	--

3. Aller : Onglet « Politique »



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

4. Ajouter une règle

Activé	Priorité	Description	Comman...
<input type="checkbox"/>	0	Alertes compromised	  

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

Détails de la règle X

aide complète 

Activé

Priorité

Ensemble de règles Rien de sélectionné 
 Tout effacer  Sélectionner tout

Action Rien de sélectionné 
 Tout effacer  Sélectionner tout

Règles

affected_product Rien de sélectionné 

attack_target Rien de sélectionné 

classtype Rien de sélectionné 

confidence Rien de sélectionné 

cve Rien de sélectionné 

deployment

- abuse.ch.feodotracker.rules
- abuse.ch.sslblacklist.rules
- abuse.ch.sslipblacklist.rules
- compromised.rules**
- emerging-current_events.rules
- emerging-deleted.rules
- emerging-dns.rules
- emerging-malware.rules
- emerging-mobile_malware.rules

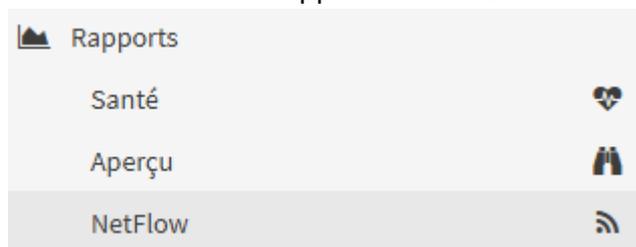
6. Consulter résultats dans « Services » > « Détection d’Intrusion » > « Fichier journal »



6) Configuration Netflow¹⁷

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 classer le trafic Internet

→ Cocher « Capture locale »

→ Rentrer l'IP de destination vers laquelle envoyée les données Netflow

*127.0.0.1 = localhost

*2055 port standard de réception Netflow v9

→ Appliquer

Rapports: NetFlow

Capturer Cache

mode avancé

Interfaces d'écoute LAN, OPT1, OPT2, WAN
✖ Tout effacer ✔ Sélectionner tout

Interfaces WAN WAN
✖ Tout effacer ✔ Sélectionner tout

Capture locale

Version v9

Destinations 127.0.0.1:2055
✖ Tout effacer Copie Pâte Texte

Délai d'attente actif 1800

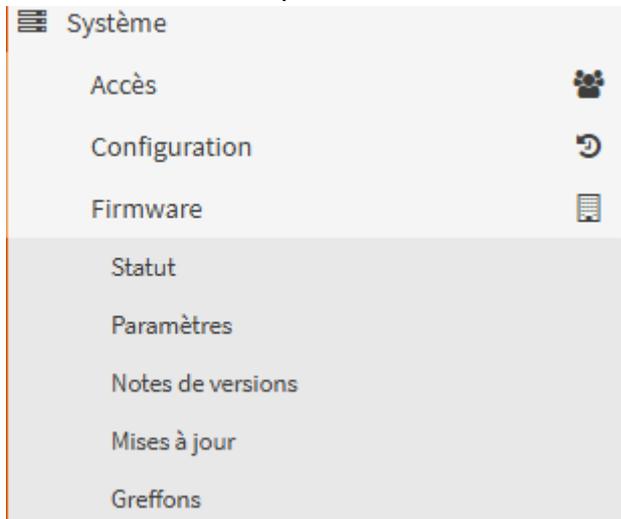
Délai d'inactivité 15

Appliquer

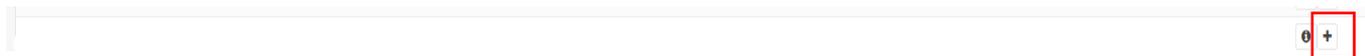
¹⁷ Protocole de collecte de données de trafic réseau **MAIS NE STOCKE PAS NI NE VISUALISE CES DONNEES PAR DEFAUT.**

Etape 2 : Télécharger le greffon « os-ntopng¹⁸ »

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



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



3. Apparaître comme « installé »

os-ntopng (installé)	1.3	20.6KIB	3	OPNsense	Traffic Analysis and Flow Collection	 
os-redis (installé)	1.1_2	68.5KIB	3	OPNsense	Redis DB	 
os-squid (installé)	1.1_1	293KIB	2	OPNsense	Squid is a caching proxy for the web	 
						 

Etape 3 : Même démarcher pour installer « os-redis¹⁹ »

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

The screenshot shows the 'Général' (General) configuration tab for Ntopng. At the top, there is a 'mode avancé' (advanced mode) toggle. Below it, several configuration options are listed:

- Activer ntopng**: Checked with a checkbox.
- Port HTTP**: Text input field containing '3000'.
- Port HTTPS**: Empty text input field.
- Certificat**: Dropdown menu with 'Aucun' (None) selected.
- Mode DNS**: Dropdown menu with 'Aucun' (None) selected.

At the bottom of the configuration area, there is an orange 'Sauvegarder' (Save) button.

2. Configurer Redis

→ Cocher « Activer »

→ Choisir l'interface d'écoute

→ « Activer le mode protégé »

→ »Activer Syslog »

The screenshot shows the 'Services: Redis' configuration section. At the top, there are three tabs: 'Réglages généraux' (General Settings), 'Restrictions', and 'Performance et Supervision'. The 'Réglages généraux' tab is active. Below it, several configuration options are listed:

- Activer Redis**: Checked with a checkbox.
- Interfaces d'écoute**: Dropdown menu with 'LAN' selected. Below the dropdown are two links: 'Tout effacer' (Clear all) and 'Sélectionner tout' (Select all).
- Activer le Mode Protégé**: Checked with a checkbox.
- Port d'écoute TCP**: Text input field containing '6379'.
- Niveau de journalisation**: Dropdown menu with 'Avertissement' (Warning) selected.
- Activer Syslog**: Checked with a checkbox.
- Dispositif Syslog**: Dropdown menu with 'LOCAL0' selected.
- Nombre de bases de données**: Text input field containing '16'.

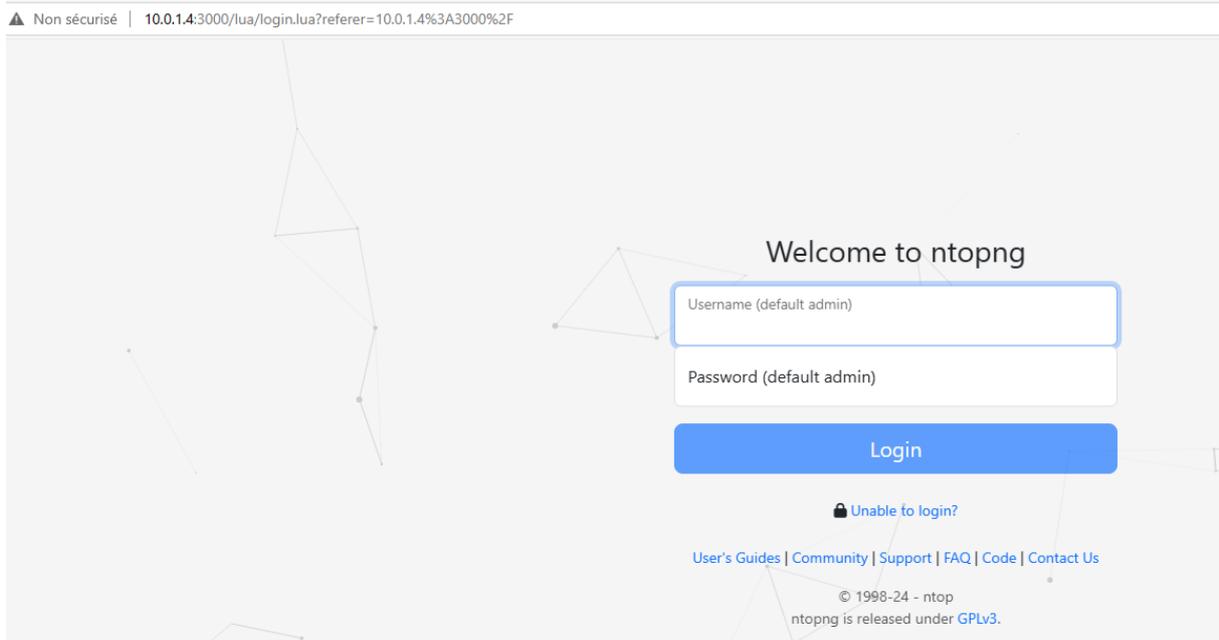
At the bottom of the configuration area, there are two buttons: 'Appliquer' (Apply) and 'Réinitialiser' (Reset).

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



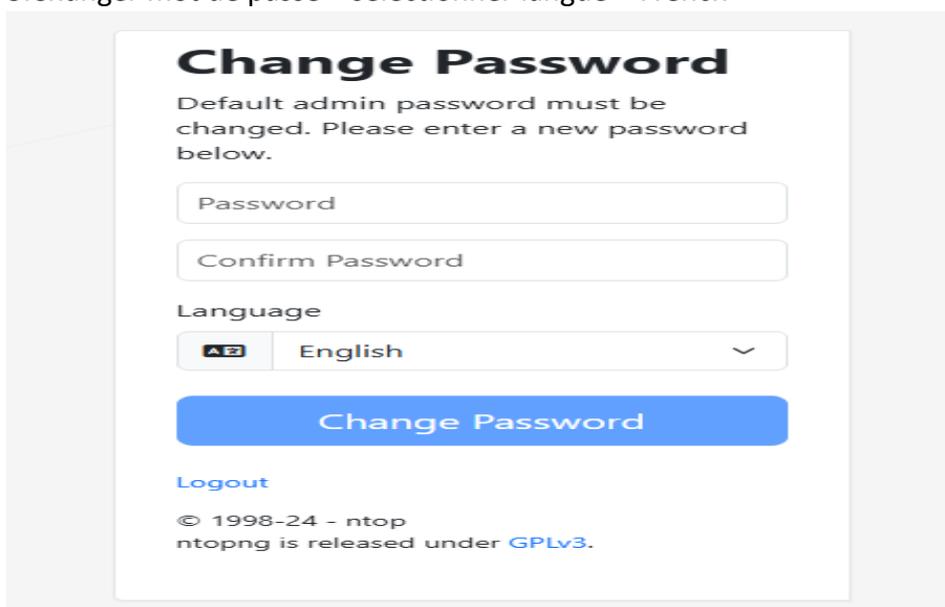
Etape 6 : Se rendre sur l'interface web de Ntopng

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

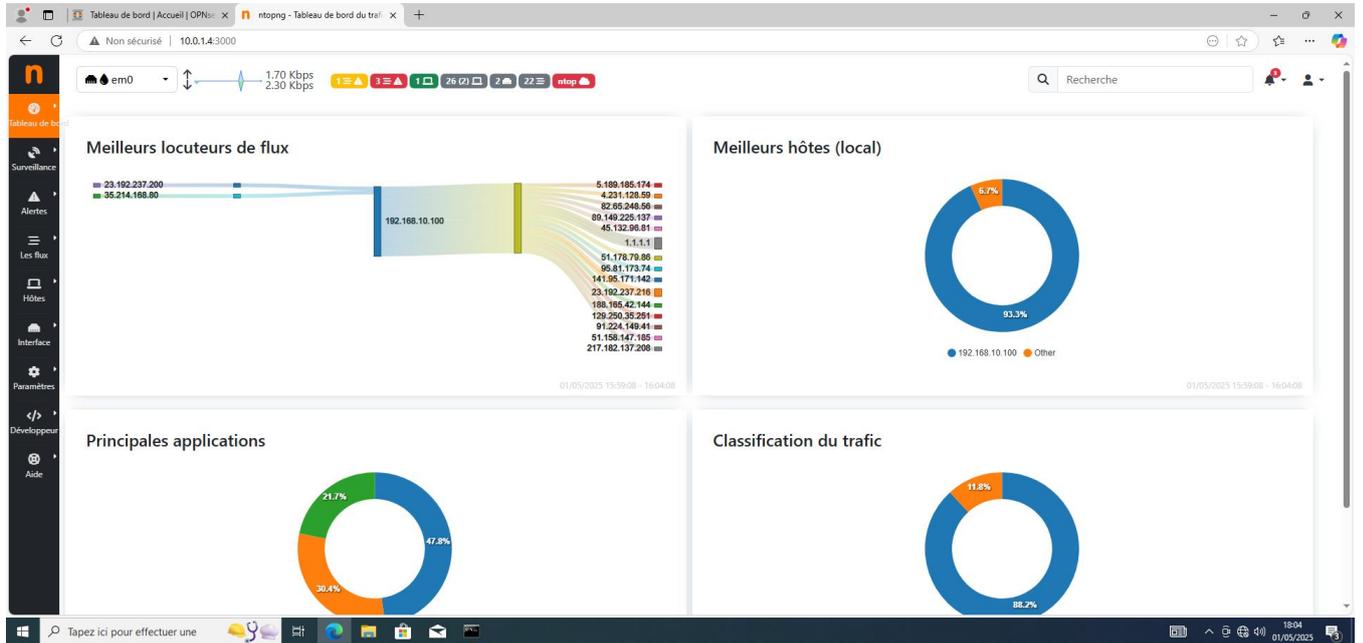


2. Accès rentrer comme username et password par défaut : admin

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



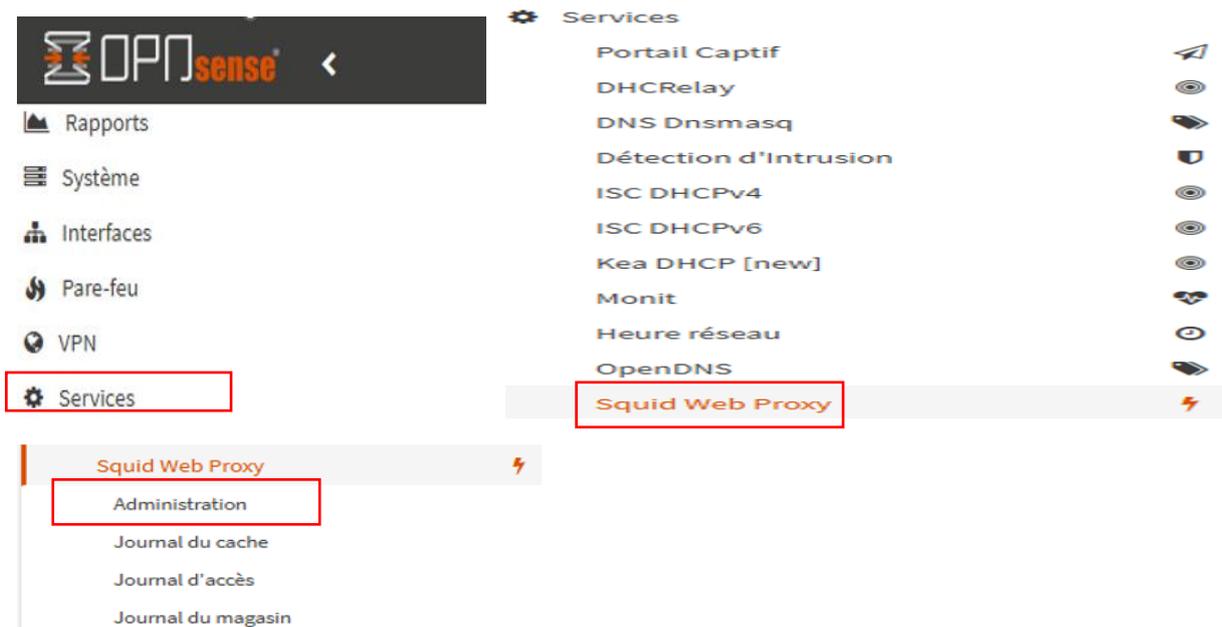
4. Bienvenue sur l'interface web Ntopng



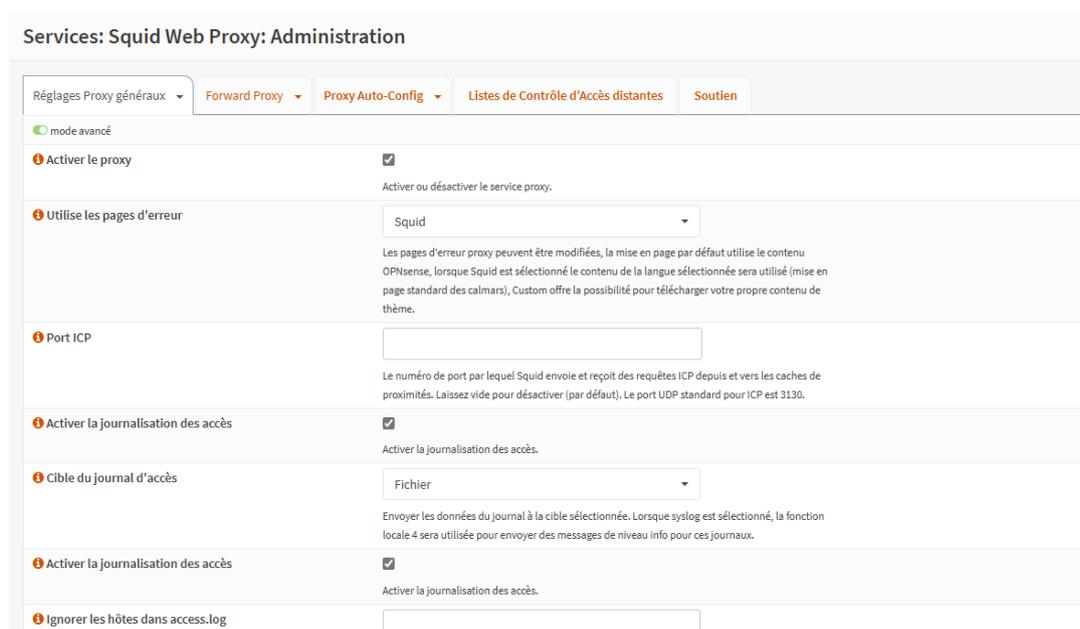
7) Configuration du proxy Squid (ici exemple sur interface LAN)

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 »

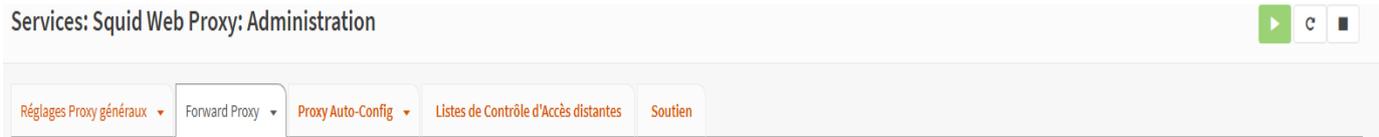


3. Cliquer sur «Appliquer »

Appliquer

Etape 2 : Activer le mode transparent

1. Cliquer sur « Forward proxy »



2. Cocher « Activer le mode transparent²⁰ » > Sélectionner « Interfaces mandataires » > Choisir « Lan » > Cliquer sur « Appliquer »

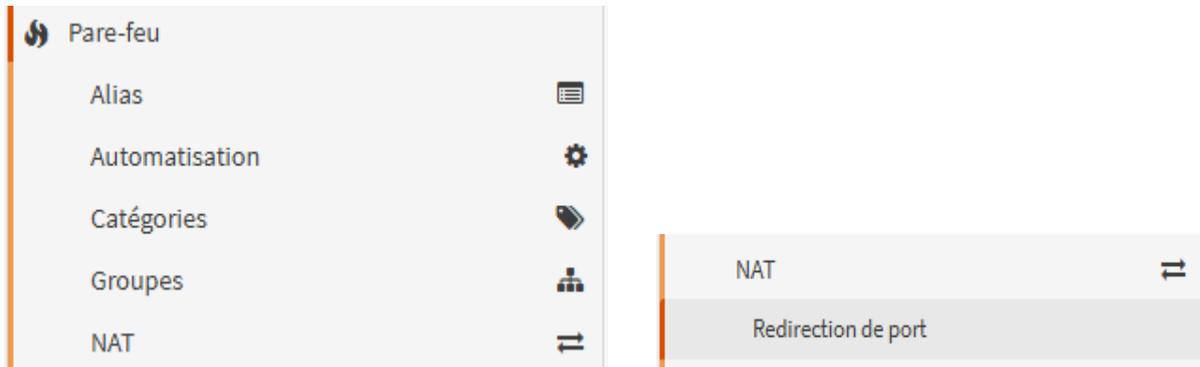
mode avancé

Interfaces mandataires	LAN Tout effacer Sélectionner tout Sélectionner les interfaces qui seront liées au proxy.
Port du proxy	3128 Le port d'écoute du service proxy.
Activer le proxy HTTP Transparent	<input checked="" type="checkbox"/> Enable transparent proxy mode. You will need a firewall rule to forward traffic from the firewall to the proxy server. You may leave the proxy interfaces empty, but remember to set a valid ACL in that case. Add a new firewall rule
Activer l'inspection SSL	<input type="checkbox"/> Enable SSL inspection mode, which allows to log HTTPS connections information, such as requested URL and/or make the proxy act as a man in the middle between the internet and your clients. Be aware of the security implications before enabling this option. If you plan to use transparent HTTPS mode, you need nat rules to reflect your traffic. Add a new firewall rule
Journalisation des informations SNI seulement	<input type="checkbox"/> Ne décryptez pas et/ou ne filtrez pas le contenu SSL, enregistrez uniquement les domaines et les adresses IP demandés. Certains anciens serveurs peuvent ne pas fournir de SNI, donc leurs adresses ne seront pas indiquées.
Port du proxy SSL	3129 Le port d'écoute du service mandataire ssl.

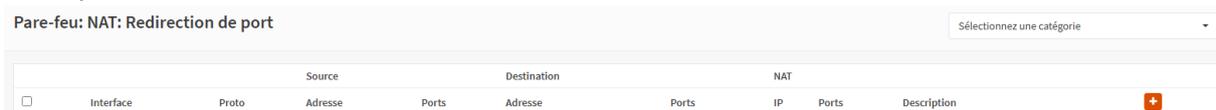
²⁰ Avec le mode transparent : firewall rediriger automatiquement trafic web (port 80) vers le proxy + utilisateur rien à configurer + tout passer par le proxy, de force. Différent mode clair : tout configurer manuellement chaque poste (navigateur, OS) pour utiliser proxy + si utilisateur pas le faire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

Pare-feu: NAT: Redirection de port

Modifier entrée de Redirection

<input type="checkbox"/> Désactivé	<input type="checkbox"/> Désactiver cette règle Sélectionnez cette option pour désactiver cette règle sans la retirer de la liste.
<input type="checkbox"/> Pas de RDR (SANS)	<input type="checkbox"/> Activer cette option permet de désactiver la redirection du trafic correspondant à cette règle Suggestion: cette option est rarement nécessaire, ne l'utilisez pas sauf si vous savez ce que vous faites.
<input type="checkbox"/> Interface	WAN Choisissez sur quelle interface cette règle sera appliquée. Suggestion: dans la plupart des cas, vous devriez utiliser WAN ici.
<input type="checkbox"/> Version TCP/IP	IPv4 Sélectionnez la version d'IP qui s'applique à cette règle
<input type="checkbox"/> Protocole	TCP Choisissez à quel protocole IP cette règle doit correspondre. Suggestion: dans la plupart des cas, vous devriez spécifier TCP ici.
Source	Avancé Afficher l'adresse source et la plage de ports
<input type="checkbox"/> Destination / Inverser	<input type="checkbox"/> Utilisez cette option pour inverser le sens de la correspondance.

4. → « Destination » laisser vide signifie « 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 »

Destination
 Hôte unique ou Réseau
 32

Plage de ports de destination
 de: HTTP à: HTTP
 Lors de l'utilisation des protocoles TCP ou UDP, spécifiez le port ou la plage de ports destination pour cette correspondance.

Rediriger l'IP de destination
 Hôte unique ou Réseau
 Indiquez l'adresse IP interne du serveur sur lequel vous souhaitez rediriger les ports.
 ex. 192.168.1.12

Rediriger le port cible
 HTTP
 Indiquez le port de la machine correspondant à l'adresse IP saisie précédemment. Dans le cas d'une plage de ports, indiquez le port de début de la plage (le port de fin sera calculé automatiquement).
 Suggestion: ceci est généralement identique au port 'de début' renseigné précédemment

Options du pool:
 Défaut
 Seuls les types "Round Robin" fonctionnent avec les Alias Host. Tout type peut être utilisé avec un sous-réseau.
 * "Round Robin": boucle à travers les adresses de traduction.
 * Aléatoire: Sélectionne au hasard une adresse du pool d'adresses de traduction.
 * Source Hash: Utilise un hachage de l'adresse source pour déterminer l'adresse de traduction, en s'assurant que l'adresse de redirection est toujours la même pour une source donnée.
 * Bitmask: Applique le masque de sous-réseau et garde la dernière partie identique; 10.0.1.50 -> x.x.x.50.
 * Adresse collante: l'option Adresse collante peut être utilisée avec les types de pool aléatoire et "Round Robin" pour garantir qu'une adresse source particulière est toujours mappée à la même adresse de traduction.

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

HTTP (autres)
 (autres) 3128

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

Journaliser Journaliser les paquets gérés par cette règle
Astuce : le pare-feu dispose d'un espace de journal local limité. N'activez pas la journalisation pour tout. Si vous souhaitez effectuer beaucoup de journalisation, envisagez d'utiliser un : **distant**.

Catégorie
Vous pouvez entrer ou sélectionner une catégorie pour regrouper des règles de firewall (non utilisée par le système)

Description
Vous pouvez entrer ici une description pour votre référence (non utilisée par le système).

Affecter l'étiquette locale
Vous pouvez marquer un paquet correspondant à cette règle et utiliser cette marque pour faire correspondre d'autres règles NAT / filtre.

Filtrage sur étiquette locale
Vous pouvez identifier des paquets marqués préalablement par une autre règle.

Pas de Sync XMLRPC
Astuce: Cela empêche la règle sur le Maître de se synchroniser automatiquement avec les autres membres CARP. Cela n'empêche PAS l'écrasement de la règle sur l'Esclave.

Réflexion NAT

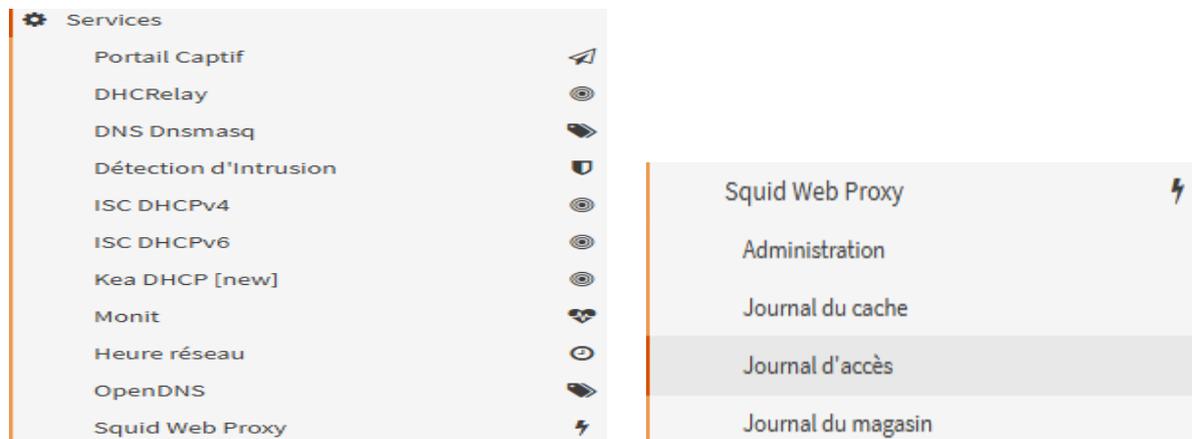
Association de règle de filtrage
REMARQUE: L'action "passer" ne fonctionne pas correctement avec une configuration Multi-WAN. Cela fonctionne uniquement sur une interface dont la passerelle est celle par défaut.

Sauvegarder **Annuler**

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'authentification » laisser désactiver : connexion par clé uniquement

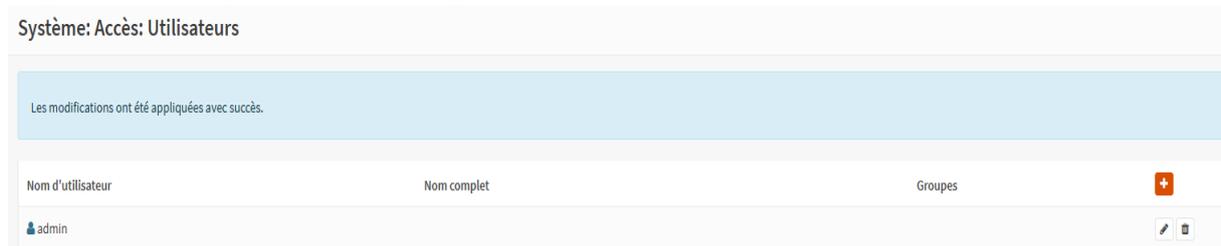
→ Cliquer sur « Sauvegarder »

Shell Sécurisé	
📘 Serveur Shell sécurisé	<input checked="" type="checkbox"/> Activer le Shell sécurisé
📘 Groupe de connexion	<input type="text" value="wheel, admins"/> <small>Sélectionnez les groupes autorisés pour la connexion à distance. Le groupe "wheel" est toujours défini à des fins de récupération et un groupe local supplémentaire peut être sélectionné à volonté. N'autorisez pas l'accès à distance aux non-administrateurs, car chaque utilisateur peut accéder aux fichiers système via SSH ou SFTP.</small>
📘 Connexion root	<input type="checkbox"/> Autoriser la connexion de l'utilisateur root <small>La connexion du compte root est généralement déconseillée. Il est recommandé de se connecter avec un autre utilisateur puis de passer root.</small>
📘 Méthode d'authentification	<input type="checkbox"/> Autoriser les connexions avec mot de passe <small>When disabled, authorized keys need to be configured for each user that has been granted secure shell access.</small>
📘 Port SSH	<input type="text" value="22"/> <small>Laisser vide pour utiliser le port 22 par défaut.</small>
📘 Interfaces d'écoute	<input type="text" value="Tout (recommandé)"/> <small>Acceptez uniquement les connexions des interfaces sélectionnées. Laissez vide pour écouter sur toutes les interfaces. Utiliser avec précaution.</small>
📘 Avancé	<input type="text" value="Afficher les dérogations cryptographiques"/>

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
```

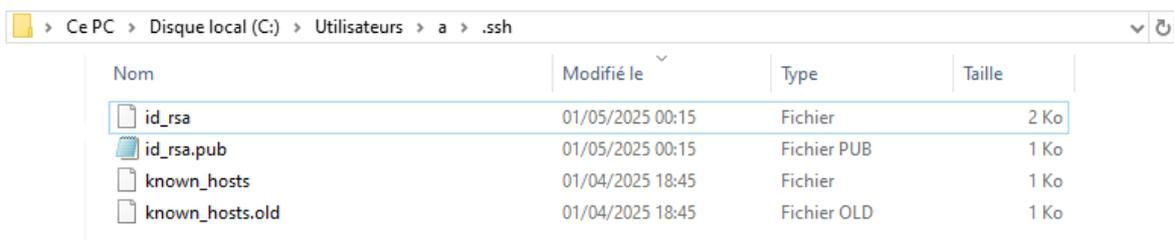
3. Inviter à rentrer une phrase : facultatif > Presser « ENTREE » pour continuer

```
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+N84tkPurgylNzpeE8BxwhC2C6bxX/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.  
-B*o  
+  
+---[SHA256]-----+
```

5. Choisir clé dans « id_rsa.pub²¹ » : attention « id_rsa » = Clé privée donc restée confidentielle !

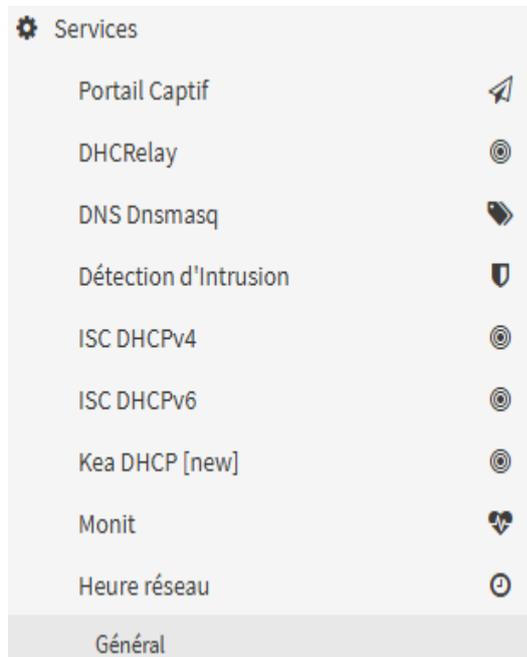


²¹ RSA : Clé être de type RSA 2048 bits : RSA algorithme de chiffrement asymétrique (Rivest Shamir Adelman) + longueur clé utilisée dans algorithme être taille clé 2048 bits

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

Services: Heure réseau: Général

Configuration du serveur NTP

Réseau	Préférer	Iburst	Ne pas utiliser
0.opnsense.pool.ntp.org	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.opnsense.pool.ntp.org	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.opnsense.pool.ntp.org	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.opnsense.pool.ntp.org	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

+

Pour de meilleurs résultats, de 3 à 5 serveurs devraient être configurés. Si aucun serveur n'est spécifié, NTP sera complètement désactivé.
L'option "prefer" indique que NTP devrait favoriser l'utilisation de ce serveur plus que tous les autres.
L'option "iburst" permet une synchronisation plus rapide de l'horloge au démarrage au détriment du pair.
L'option "do not use" indique que ce serveur ne sera pas utilisé pour le NTP mais les statistiques pour ce serveur seront collectées et affichées.

Mode client Quitter le serveur NTP immédiatement après la synchronisation horaire

Interfaces

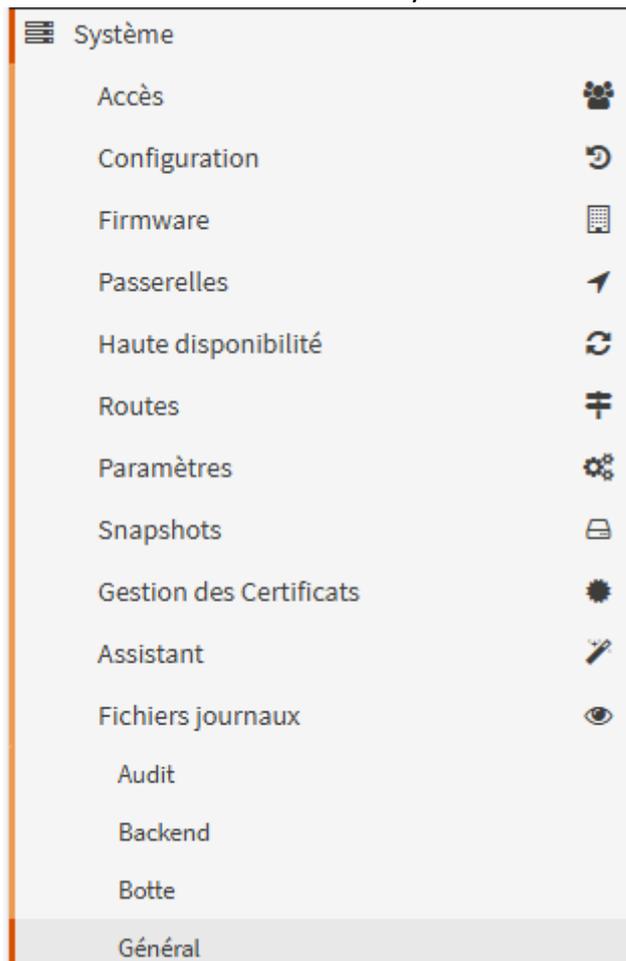
Interfaces to listen on and send outgoing queries.
La sélection d'aucune interface activera l'écoute du serveur sur toutes les interfaces.
Sélectionner toutes les interfaces provoquera l'écoute explicite sur les seules interfaces/IPs spécifiées.
Les interfaces sans adresse IP ne sont pas affichées.

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

→ Cliquer sur « Sauvegarder »

Mode orphelin	<input type="text" value="12"/>	(0-15) Le mode orphelin permet d'utiliser l'horloge système lorsqu'aucune autre horloge n'est disponible. Le nombre indiqué ici spécifie la strate signalée pendant le mode orphelin et doit normalement être défini sur un nombre suffisamment élevé pour garantir que tout autre serveur disponible pour les clients est préféré à ce serveur.
Maxclock	<input type="text" value="10"/>	(2-99) Indiquer le nombre maximal de serveurs retenus par les schémas de découverte de serveurs. La valeur par défaut est de 10, mais elle devrait être modifiée. Il doit s'agir d'un nombre impair (pour mettre en minorité les faussaires), généralement deux ou trois de plus que minclock (1), plus le nombre d'entrées dans le pool. Les entrées du pool doivent être ajoutées comme maxclock, mais pas minclock, qui compte également les entrées du pool elles-mêmes. Par exemple, tos maxclock 11 avec quatre lignes de pool conserverait 7 associations.
Graphiques NTP	<input type="checkbox"/>	Activer les graphiques RRD des statistiques NTP
Journalisation syslog	<input type="checkbox"/>	Activer la journalisation des messages des pairs
	<input type="checkbox"/>	Activer la journalisation des messages du système
		Ces options autorise l'écriture de messages NTP additionnels dans le journal système (System Log). (Statut > Journaux Système > NTP).
Statistiques de journalisation	<input type="text" value="Avancé"/>	Afficher les options des statistiques de journalisation
Restrictions d'accès	<input type="text" value="Avancé"/>	Afficher les options de restriction d'accès
Secondes intercalaires	<input type="text" value="Avancé"/>	Afficher la configuration de la Seconde intercalaire
Avancé	<input type="text" value="Avancé"/>	Afficher les options avancées
<input type="button" value="Sauvegarder"/>		

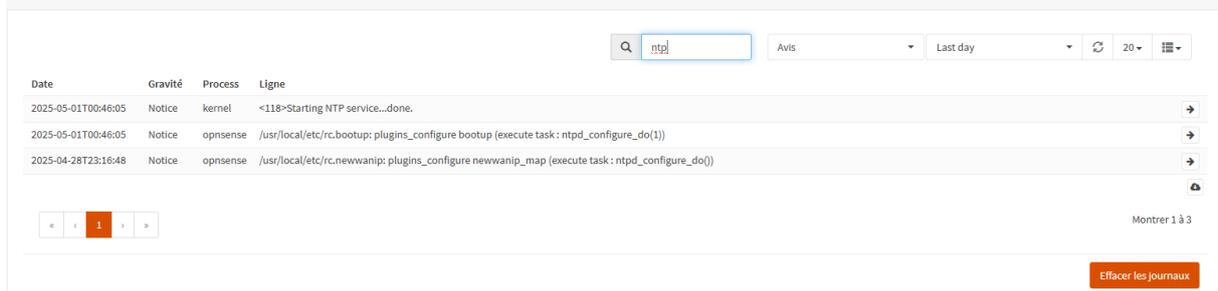
4. Vérifier NTP fonctionnel : « Système » > « Fichiers journaux » > « Général »



5. Filtrer par « NTP »

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

Système: Fichiers journaux: Général



The screenshot shows a log viewer interface with a search bar containing 'ntp'. The log entries are as follows:

Date	Gravité	Process	Ligne
2025-05-01T00:46:05	Notice	kernel	<118>Starting NTP service...done.
2025-05-01T00:46:05	Notice	opnsense	/usr/local/etc/rc.bootup: plugins_configure bootup (execute task: ntpd_configure_do(1))
2025-04-28T23:16:48	Notice	opnsense	/usr/local/etc/rc.newwanip: plugins_configure newwanip_map (execute task: ntpd_configure_do(0))

At the bottom right of the log viewer, there is a button labeled 'Effacer les journaux'.

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
```