29
Novembre
2024

NATHAN GABRIELE

AP_PFSENSE_PARE-FEU_MISE_EN_PLACE_RÉSEAU

SIO2 option SISR

Sommaire

Introduction

PfSense est une solution open-source basée sur FreeBSD, conçue pour fournir un pare-feu et un routeur réseau hautement performant. En s'appuyant sur le filtre de paquets à états Packet Filter, elle propose des fonctionnalités avancées telles que le routage, la gestion de la bande passante, la traduction d'adresses réseau (NAT), et le support des réseaux privés virtuels (VPN), faisant d'elle un outil polyvalent et robuste pour la gestion et la sécurisation des réseaux.

Cet atelier est conçu pour lui permettre de se familiariser avec les bases et les fonctionnalités avancées de PfSense. Il explore des aspects techniques tels que la création de règles de pare-feu précises, la configuration de redirections de ports, la gestion des certificats SSL/TLS pour sécuriser les communications, et l'utilisation d'outils de sécurité intégrés comme Snort pour la détection d'intrusions et ClamAV pour la protection antivirus.

Avec ces compétences, il pourra mettre en œuvre des solutions de sécurité efficaces, contrôler avec précision les flux réseau entrants et sortants, et garantir une protection avancée contre les menaces potentielles, tout en optimisant les performances des infrastructures qu'il gère.

Schéma Réseau

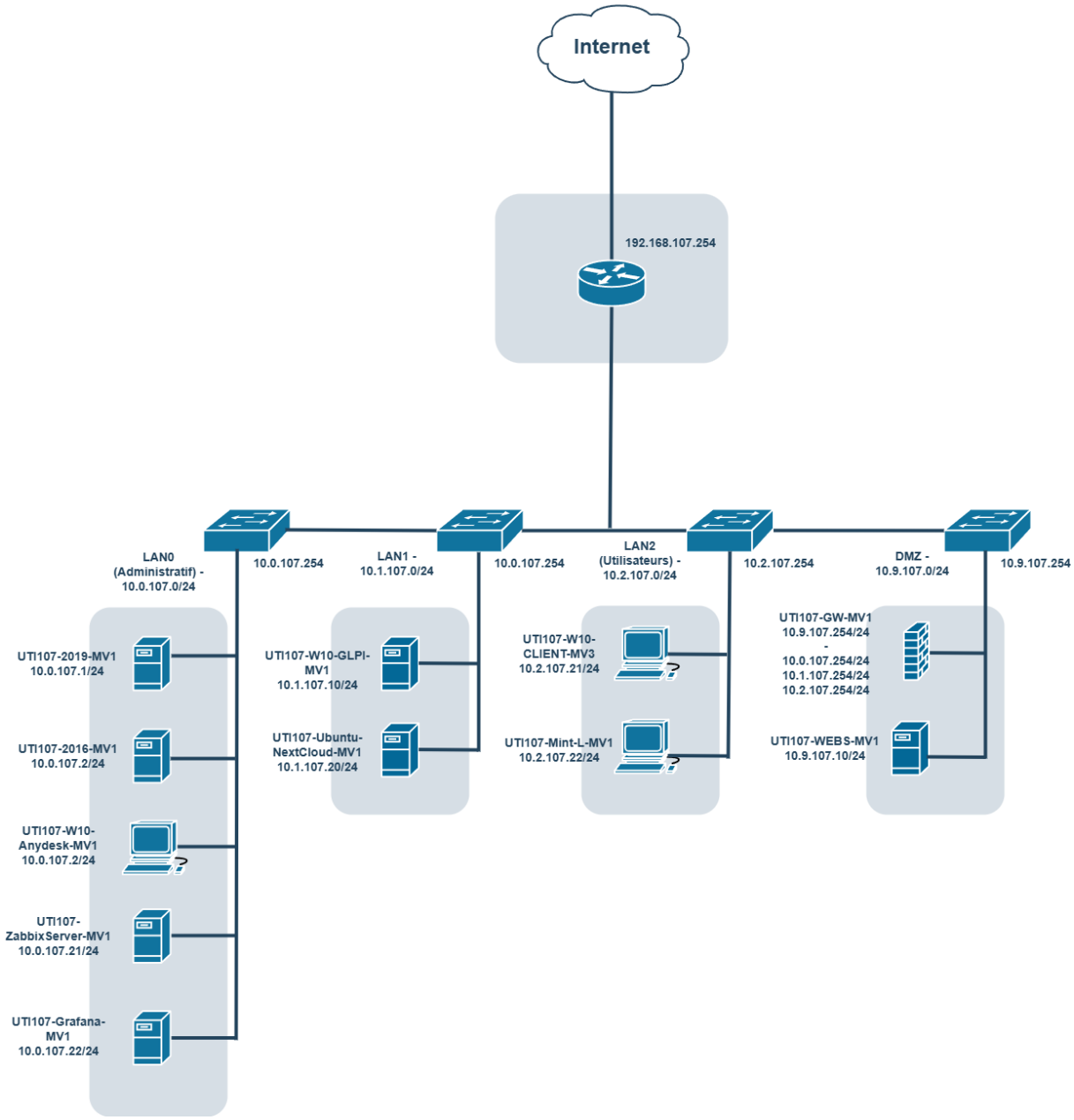
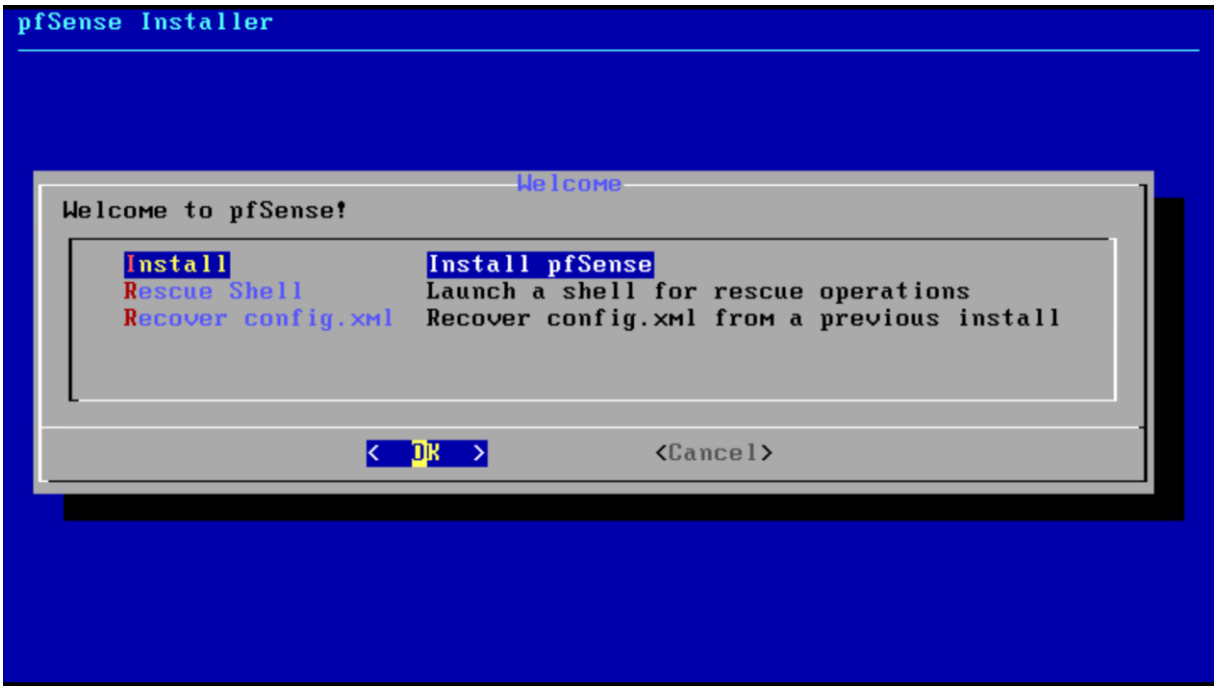


Schéma Réseau

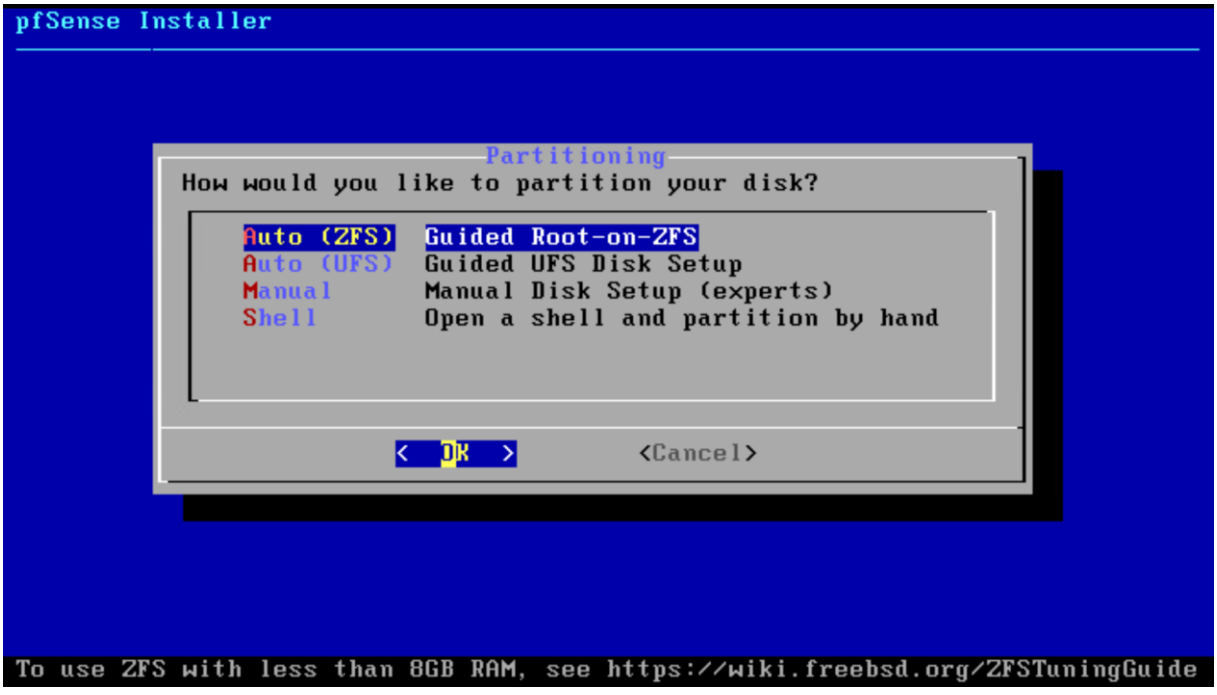
	Adresse IP	Masque de sous-réseau	Passerelle par défaut	DNS
UTI107-GW-MV1	192.168.107.254 10.0.107.254	255.255.255.0	Lui-même	10.0.107. 1 172.31.1.4 172.31.1.6
UTI107-WEBS-MV1	10.9.107.10	255.255.255.0	10.9.107. 254	10.0.107. 1 1.1.1.1
UTI107-2019-MV1	10.0.107.1	255.255.255.0	10.0.107. 254	Lui-même
UTI107-2016-MV1	10.0.107.2	255.255.255.0	10.0.107. 254	10.0.107. 1 1.1.1.1
UTI107-W10-Anydesk-MV1	10.0.107.30	255.255.255.0	10.0.107. 254	10.0.107.1 1.1.1.1
UTI107-Ubuntu-NextCloud-MV1	10.1.107.20	255.255.255.0	10.1.107. 254	10.0.107. 1 1.1.1.1
UTI107-W10-GLPI-MV1	10.1.107.10	255.255.255.0	10.0.107. 254	10.0.107. 1 1.1.1.1
UTI107-WIN10-Client-MV3	10.2.107.21	255.255.255.0	10.2.107. 254	10.0.107. 1 1.1.1.1
UTI107-Mint-L-MV1	10.2.107.22	255.255.255.0	10.2.107. 254	10.0.107.1

Mise en place et Installation du Pfsense (Pare-Feu)

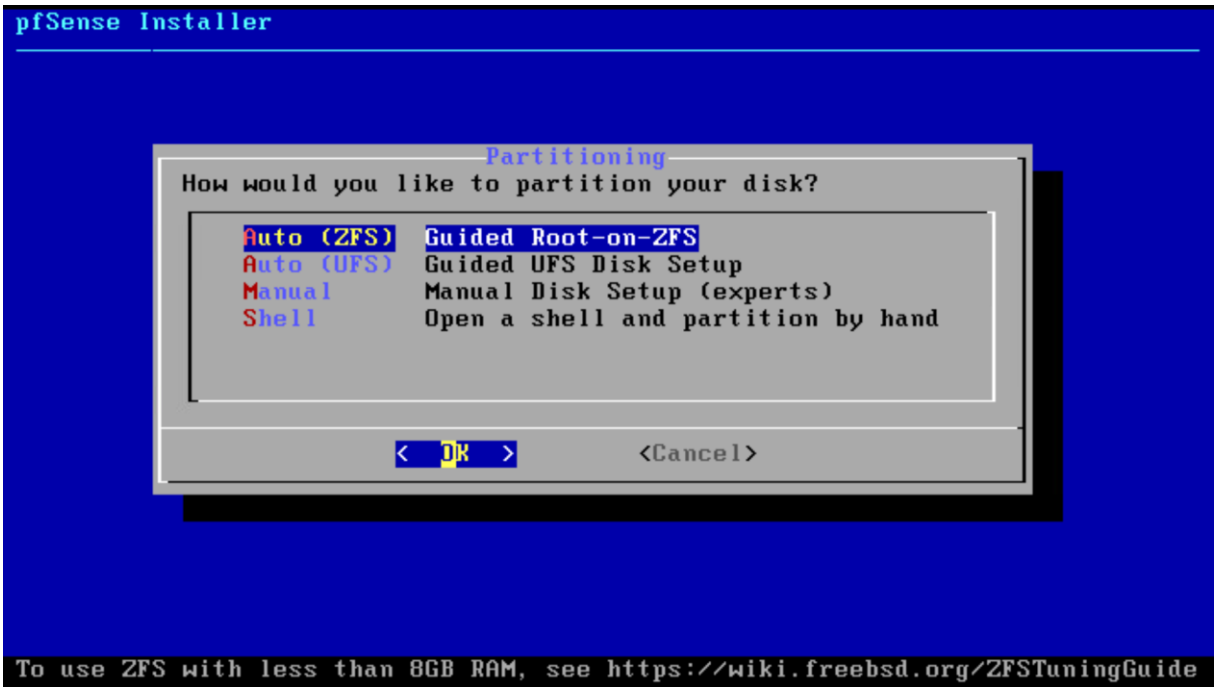
L'utilisateur a choisi l'option "Install pfSense". Ce choix démarre le processus d'installation standard. Cette méthode est préférée pour configurer un pare-feu complet et fonctionnel sans options avancées immédiates. Les autres options, comme le "Rescue Shell", sont destinées à la maintenance ou au dépannage.



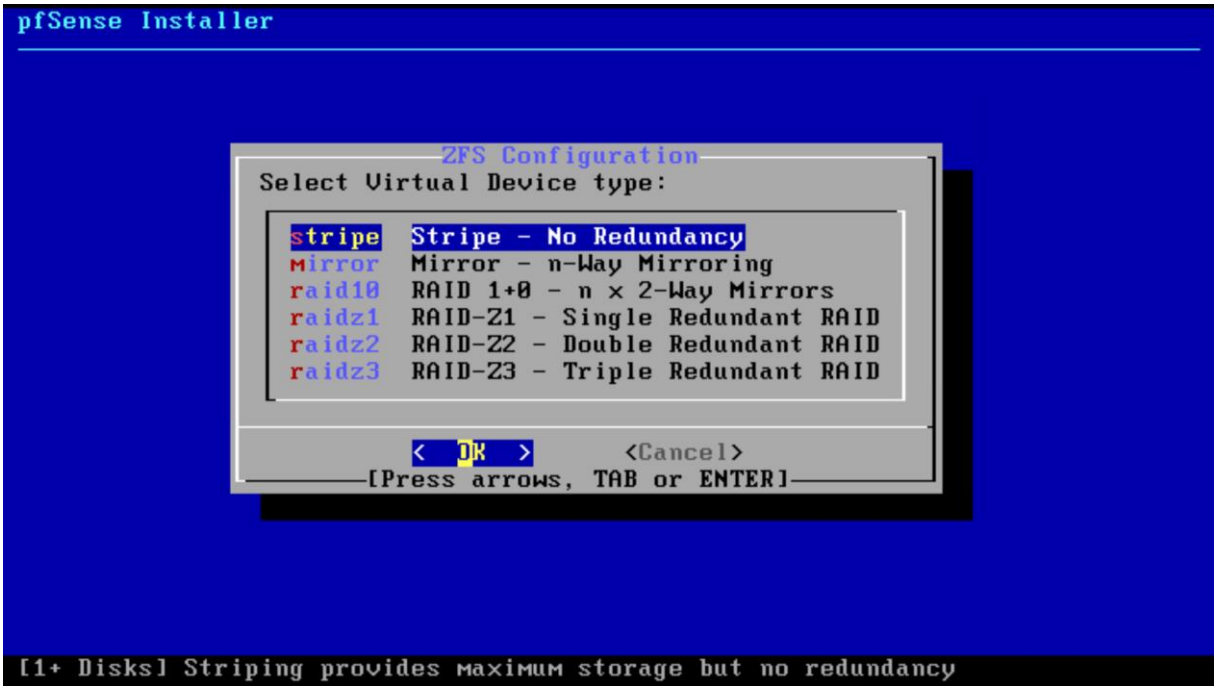
Le partitionnement automatique avec "Auto (ZFS)" a été sélectionné. ZFS est idéal pour sa fiabilité et sa capacité à gérer les volumes de stockage avancés, comme les snapshots. Ce choix est pertinent pour une utilisation moderne avec des besoins de sauvegarde ou de récupération. Si la machine dispose de moins de 8 Go de RAM, il serait préférable d'utiliser UFS.



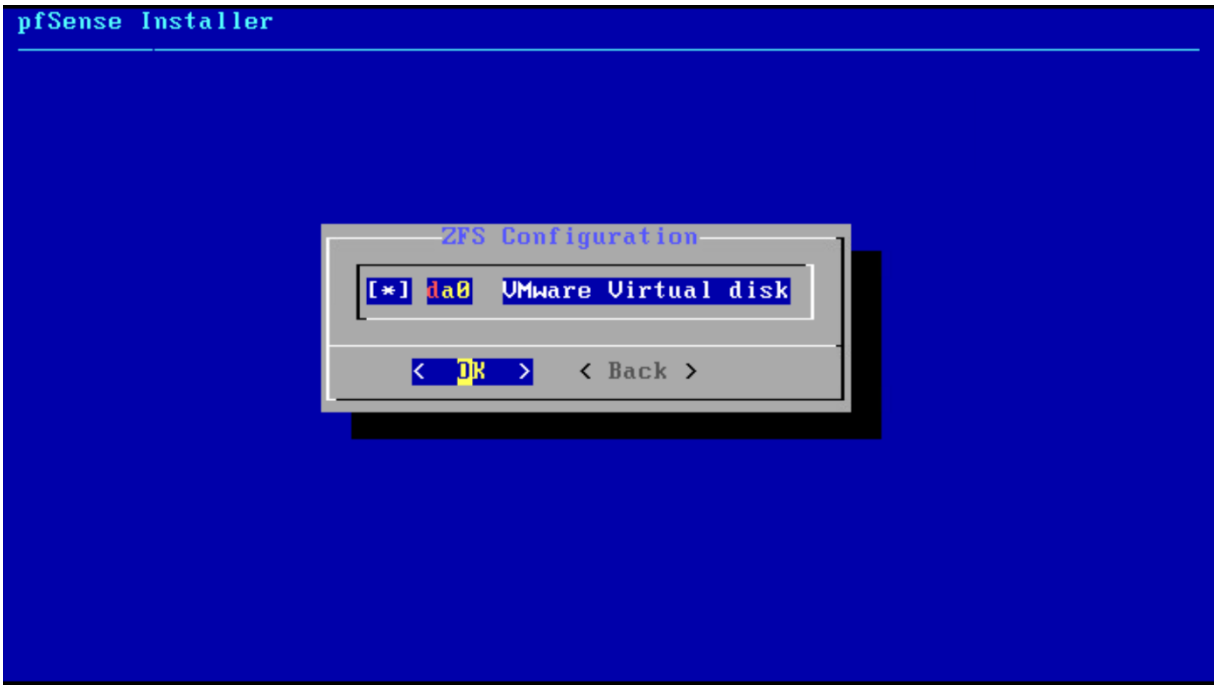
L'option "Stripe - No Redundancy" a été choisie. Cette configuration maximise l'espace disque disponible, mais n'offre pas de redondance. Cela peut convenir dans un environnement où les performances ou l'utilisation maximale de l'espace sont prioritaires, plutôt que la tolérance aux pannes.



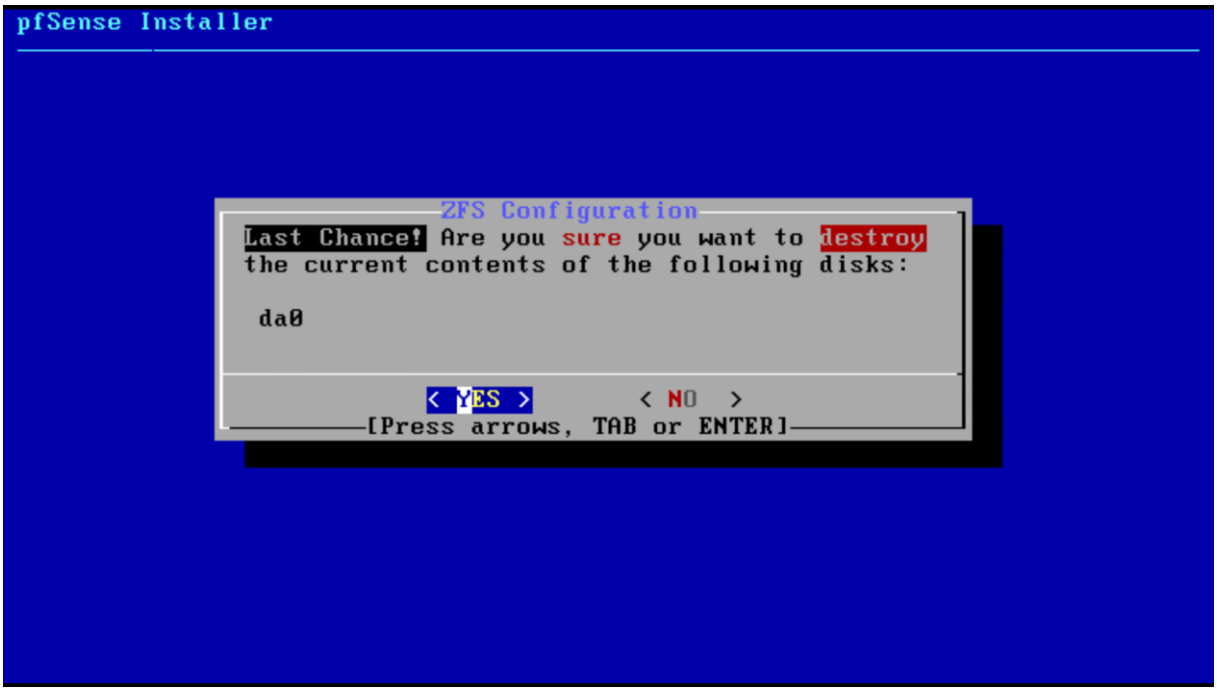
Le disque détecté, "da0" (VMware Virtual Disk), a été sélectionné. Cette action prépare le disque principal de la machine virtuelle à être configuré pour l'installation de pfSense. Ce choix est cohérent avec un déploiement sur VMware.



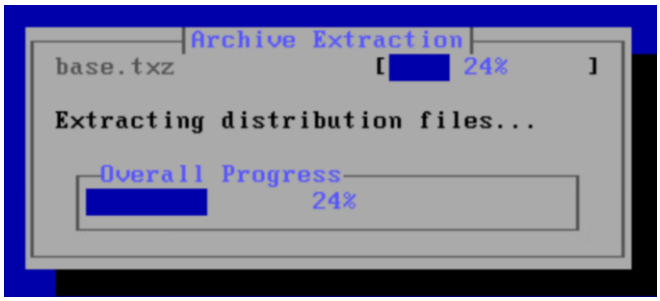
Un avertissement invite l'utilisateur à confirmer la suppression des données existantes sur "da0". Cette étape est critique pour éviter une perte accidentelle. En confirmant "Yes", le disque est préparé pour une nouvelle installation.



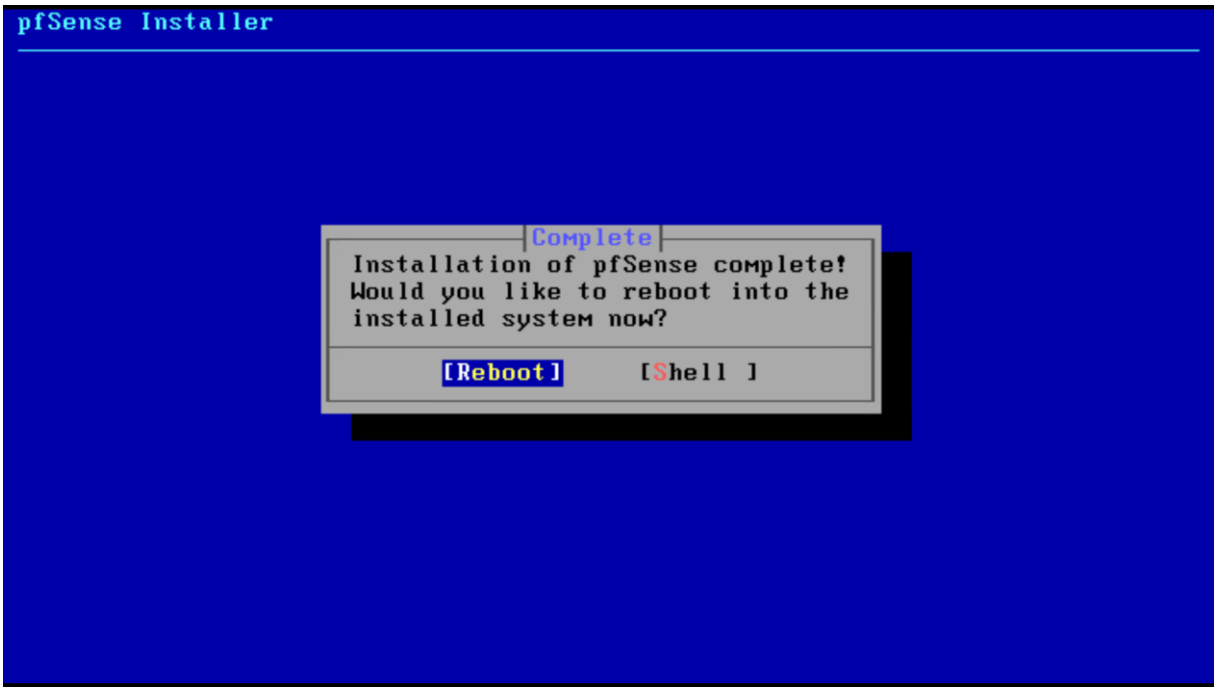
Le système extrait les fichiers nécessaires au déploiement de pfSense. Cette phase automatise l'installation et configure le système d'exploitation sur le disque sélectionné. La progression est affichée pour indiquer l'état en temps réel.



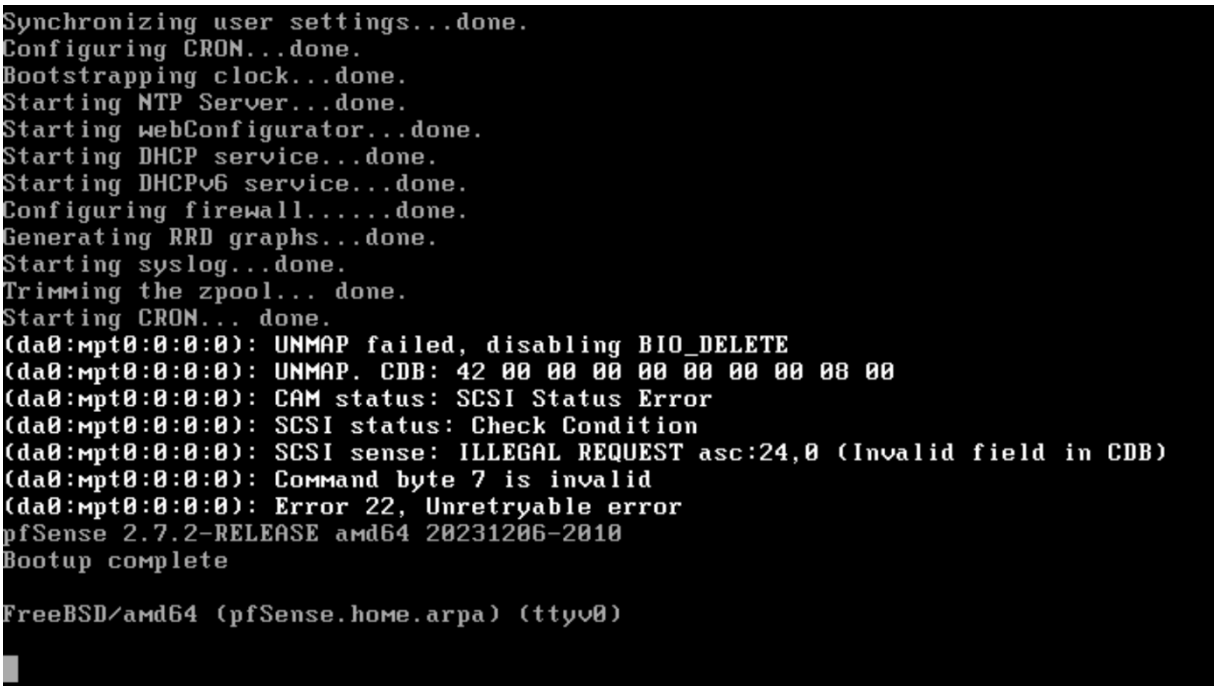
À ce stade, il suffit de patienter pendant l’extraction des fichiers nécessaires à l’installation de pfSense. Cette opération transfère et prépare les composants essentiels du système, garantissant une installation complète et fonctionnelle. La progression est affichée pour informer l'utilisateur de l'avancement.



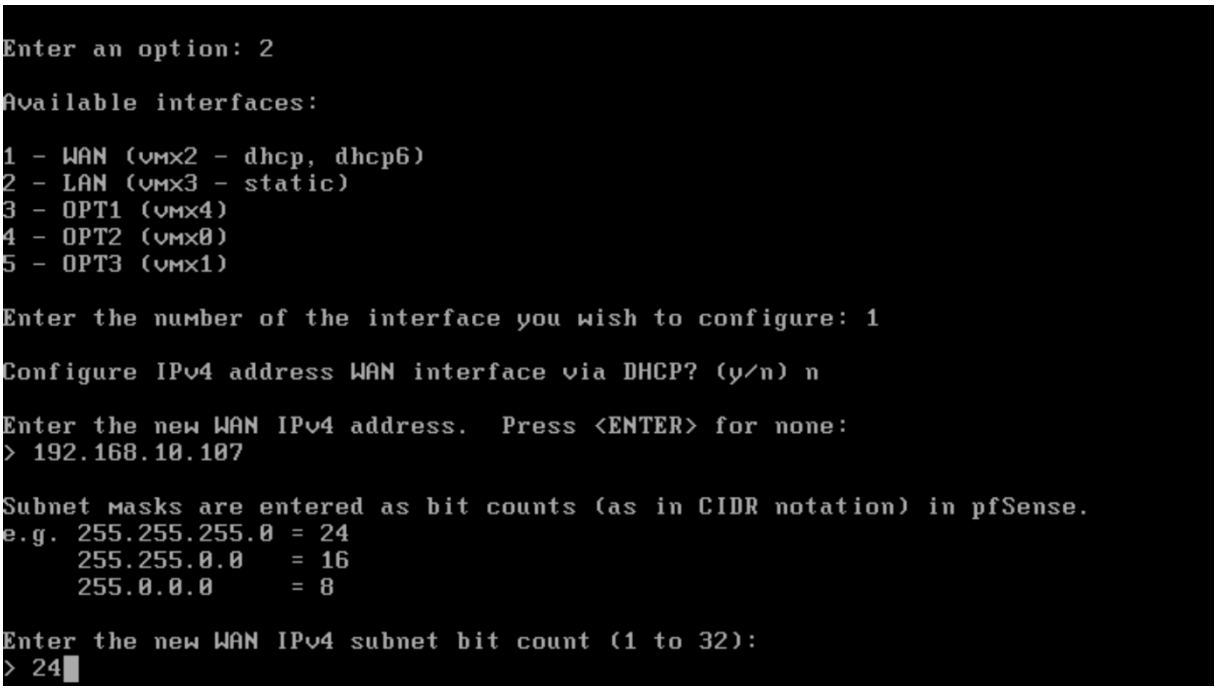
Une fois l'installation terminée, l'utilisateur est invité à redémarrer le système. En choisissant "Reboot", le système démarre avec pfSense installé, prêt à être configuré pour un environnement réseau.



Une fois le système démarré, des messages relatifs à des erreurs SCSI sont affichés. Ces erreurs, souvent liées à l’utilisation de disques virtuels dans des environnements virtualisés, n’affectent pas le fonctionnement général de pfSense et peuvent être ignorées dans ce contexte. Le système atteint l'état "Bootup complete", signalant que pfSense est prêt pour les configurations réseau.



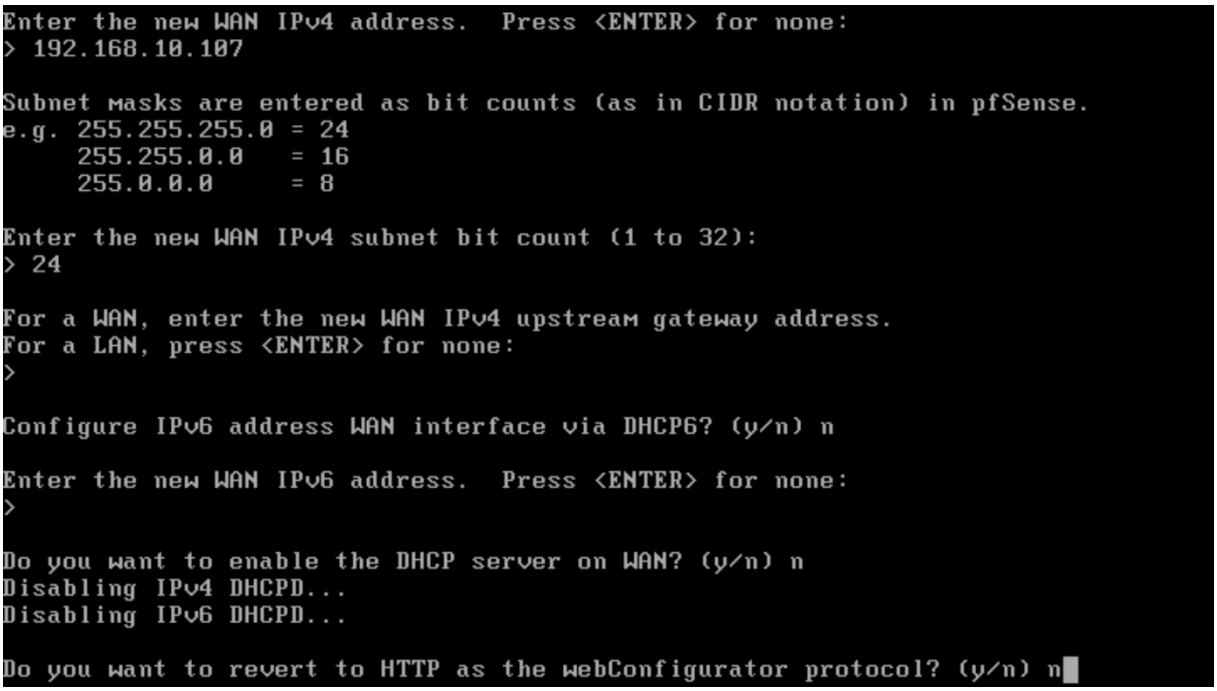
La première configuration concerne l'interface WAN, où une adresse IP statique est définie sans utiliser le DHCP. Le choix de l'adresse IP 192.168.10.107/24 permet d'assurer une gestion fixe et prévisible des connexions externes, essentielle dans des environnements nécessitant une stabilité des adresses. L'utilisation d'IPv6 est désactivée, simplifiant la configuration lorsqu'aucun besoin spécifique de ce protocole n'existe.



L'interface LAN est configurée avec l'adresse statique 10.0.107.254/24, qui servira de passerelle par défaut pour les clients internes. Le DHCP est également désactivé sur cette interface, ce qui est adapté lorsque le réseau local dispose d'une gestion

d’adresses centralisée ou si une configuration manuelle est privilégiée pour plus de contrôle.

L’interface LAN est configurée avec l’adresse statique 10.0.107.254/24, qui servira de passerelle par défaut pour les clients internes. Le DHCP est également désactivé sur cette interface, ce qui est adapté lorsque le réseau local dispose d’une gestion d’adresses centralisée ou si une configuration manuelle est privilégiée pour plus de contrôle.



L’interface WAN est configurée avec une adresse IPv4 statique **192.168.10.107/24**, permettant une passerelle par défaut stable et contrôlée, essentielle pour un réseau fiable. L’IPv6 et le serveur DHCP sont désactivés pour simplifier la configuration et éviter des services non nécessaires sur l’interface externe, renforçant la sécurité. Le choix de HTTPS pour le WebConfigurator garantit une gestion sécurisée de pfSense via l’adresse **https://10.0.107.254,** assurant la confidentialité des données administratives échangées.

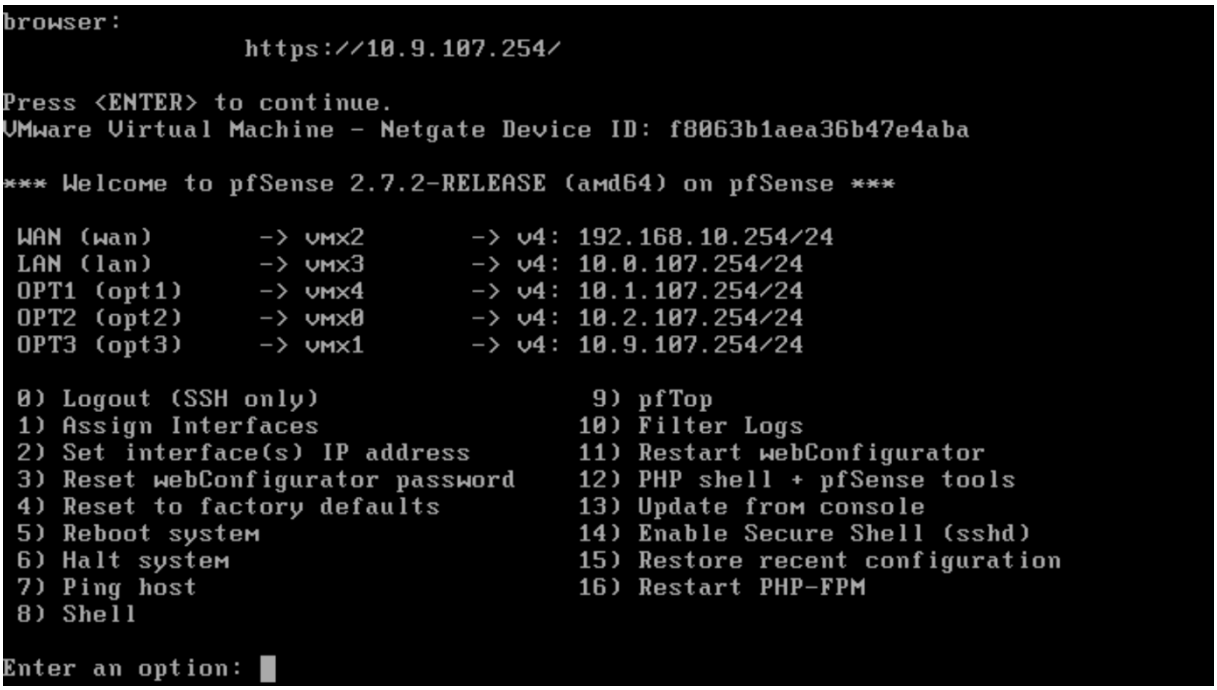
```
For a LAN, press <ENTER> for none:
>

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on WAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 WAN address has been set to 192.168.10.107/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.10.107/

Press <ENTER> to continue.
```

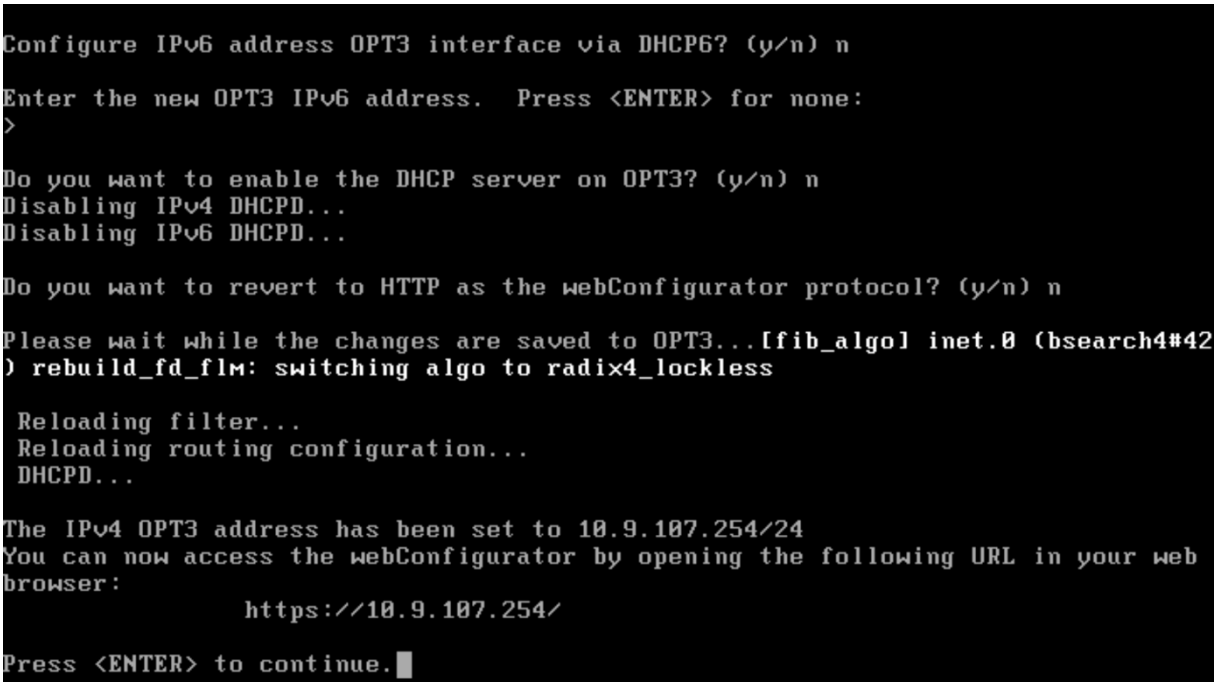
Des interfaces supplémentaires, telles qu'OPT1, OPT2, et OPT3, sont ensuite paramétrées avec des plages d'adresses distinctes, notamment 10.1.107.254/24, 10.2.107.254/24 et 10.9.107.254/24. Ces configurations segmentent le réseau en sous-réseaux isolés, permettant de gérer des zones dédiées à des usages spécifiques, tels que des serveurs, des invités ou des environnements test. Ce découpage assure une meilleure gestion des flux réseau et renforce la sécurité en isolant les différentes parties du réseau.

```
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 10.0.107.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://10.0.107.254/

Press <ENTER> to continue.
```

Pour vérifier les informations, un résumé des interfaces et de leurs configurations est présenté. Il regroupe les adresses IP assignées à chaque interface et confirme que le

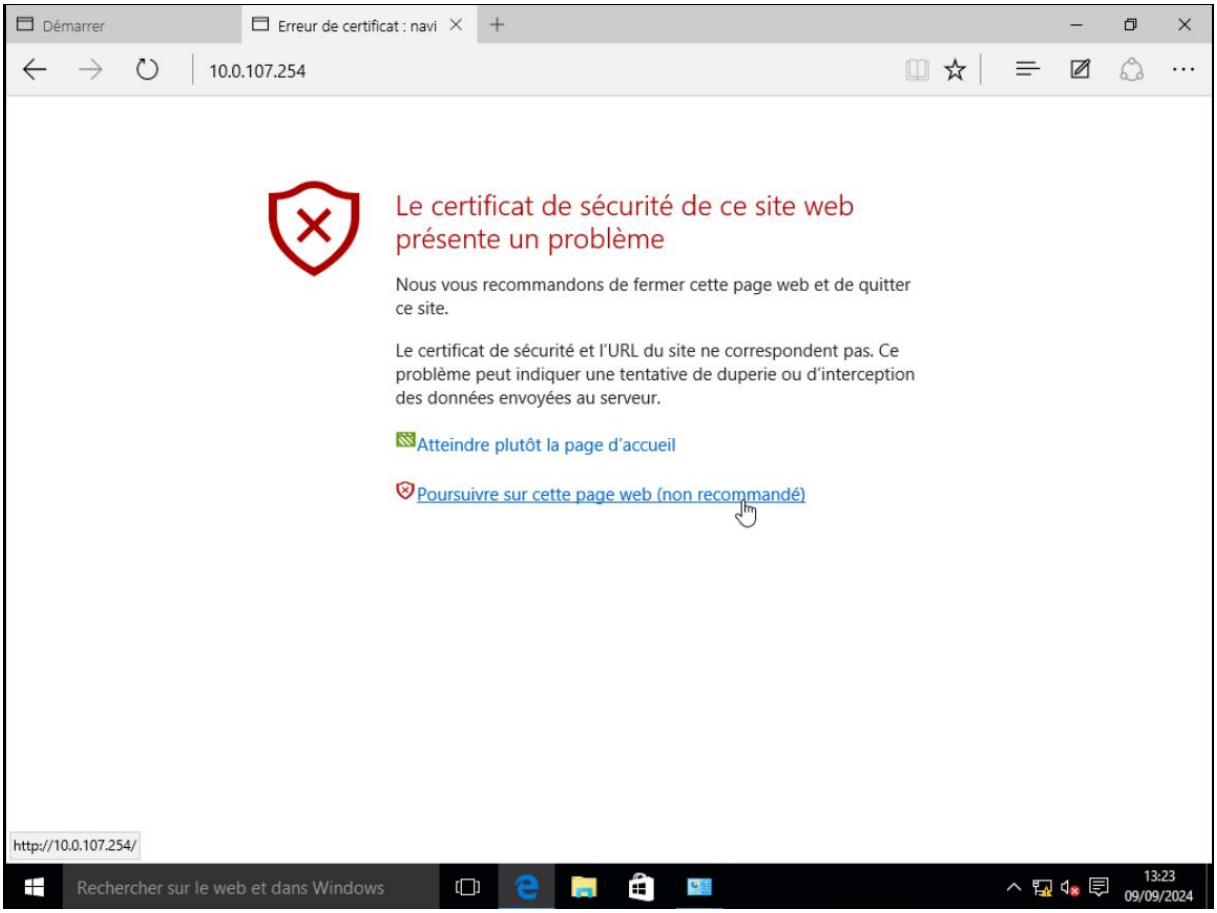
pare-feu est prêt à être administré via l'interface web. L'ensemble des configurations reflète une approche méthodique, adaptée aux besoins d'un réseau structuré et sécurisé, tout en exploitant au mieux les fonctionnalités de pfSense.





Paramètres et Configuration

Lors de l'accès à l'interface web de pfSense, un message indique une erreur de certificat. Cela se produit parce que pfSense utilise un certificat auto-signé par défaut, ce qui est normal pour les déploiements internes. En choisissant "Poursuivre sur cette page web", l'utilisateur peut accéder à l'interface tout en maintenant une connexion sécurisée via HTTPS.

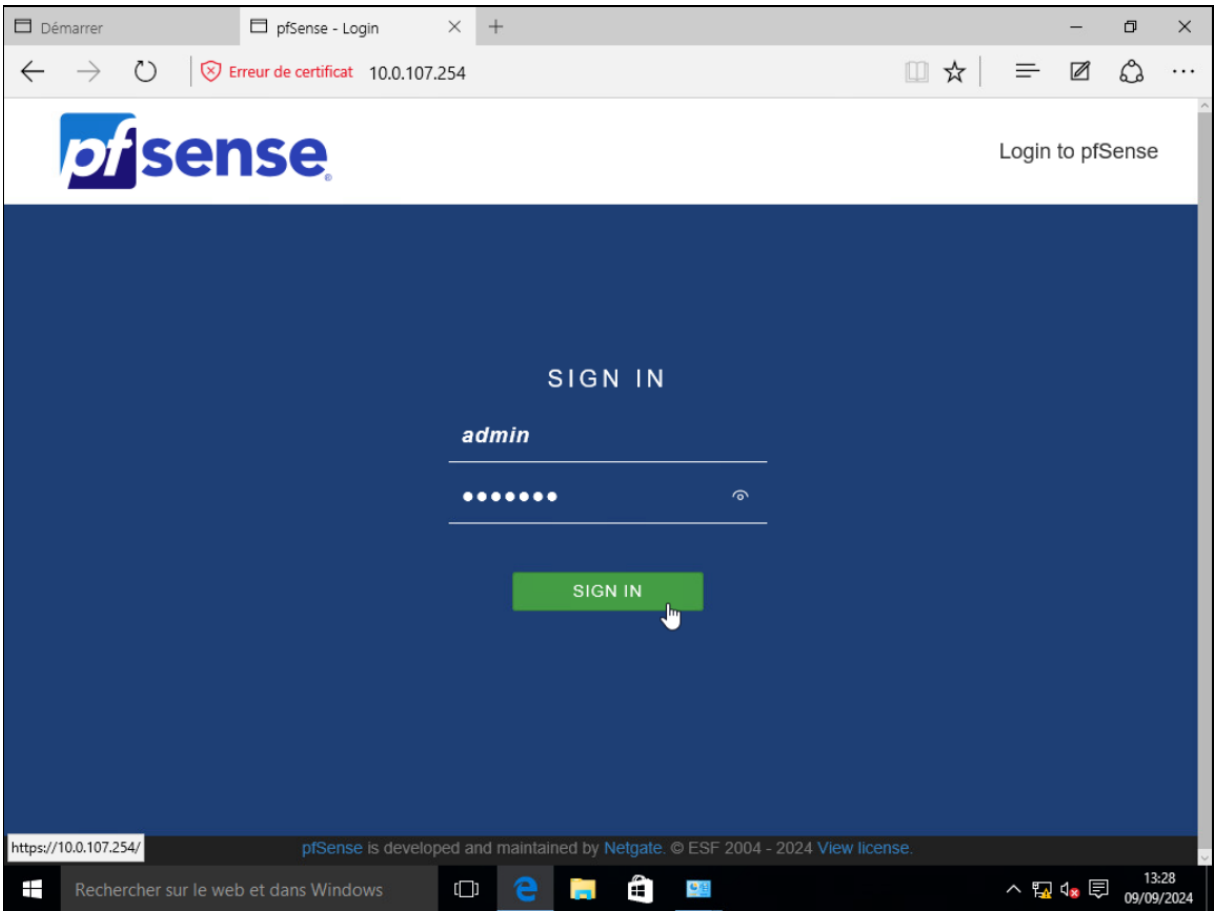


La connexion à l'interface web se fait via l'identifiant "admin" et le mot de passe par défaut. Il est fortement recommandé de modifier ce mot de passe dès que possible pour renforcer la sécurité et éviter tout accès non autorisé.

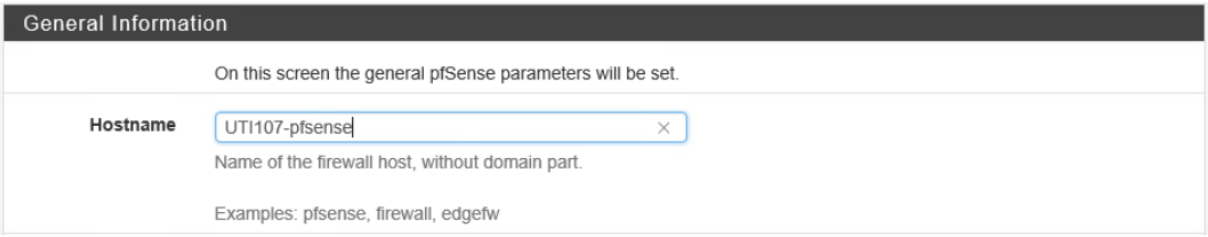
Identifiant : Admin

Mot de passe : pfsense

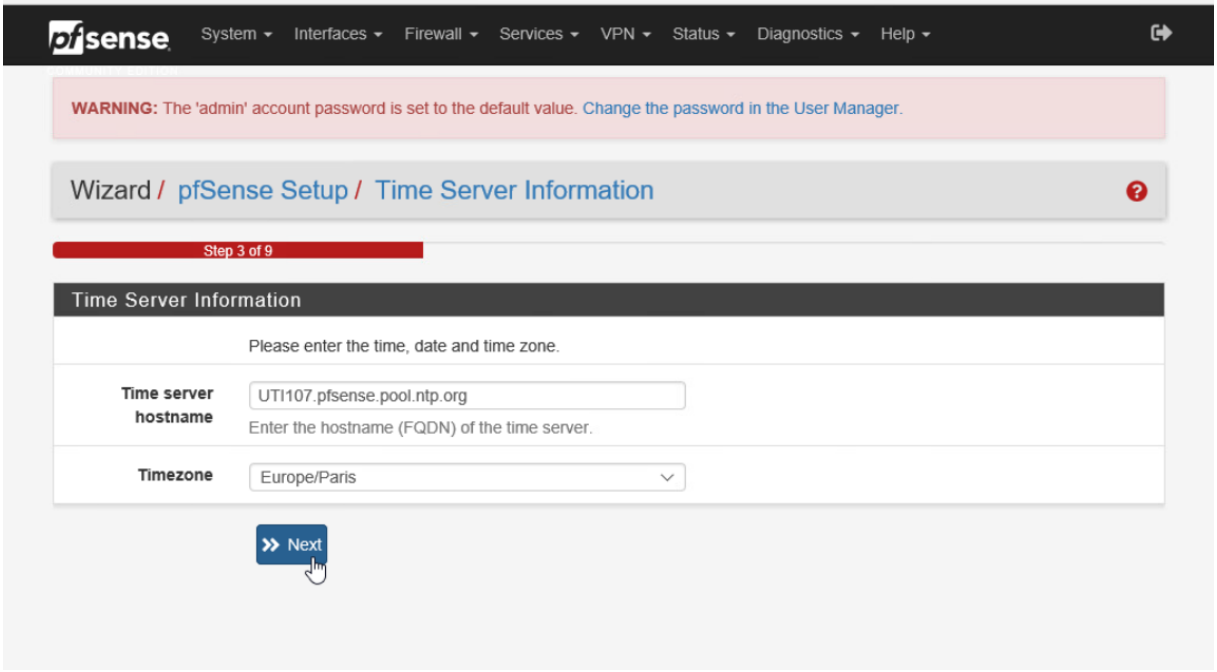
Ensuite cliquer sur « Sign in »



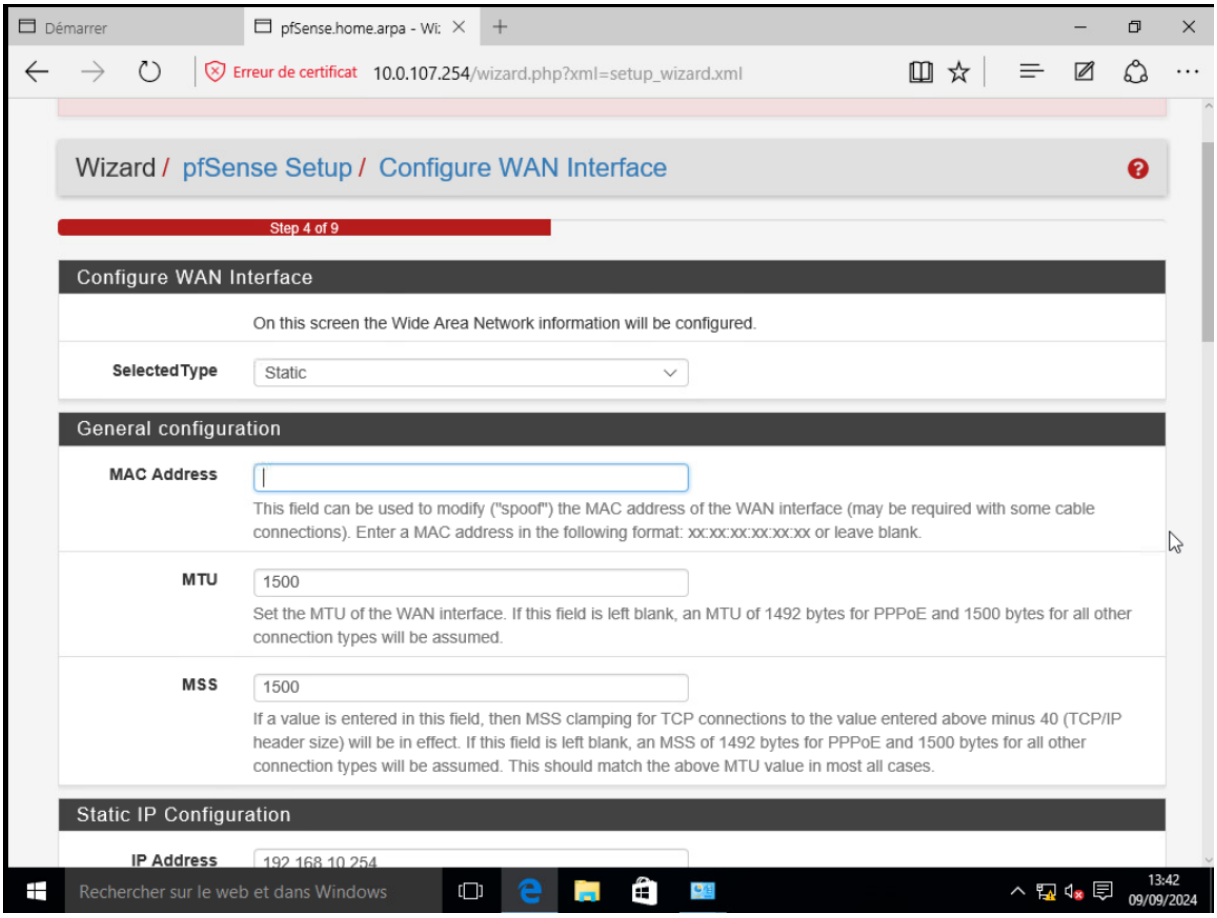
Le nom d'hôte, ici "UTI107-pfsense", est défini pour identifier clairement le pare-feu sur le réseau. Cela facilite la gestion, le suivi des logs et la communication avec d'autres équipements.



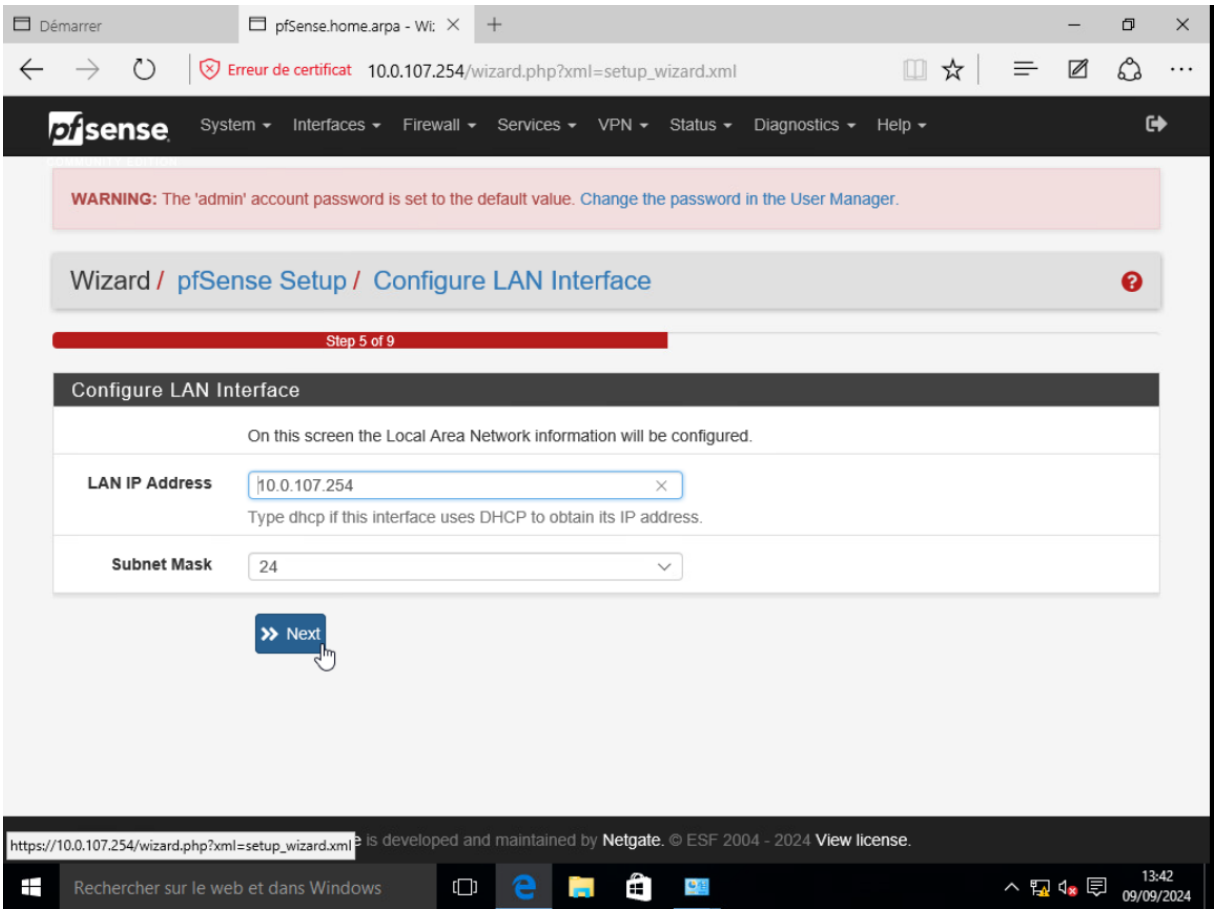
Le serveur de temps (NTP) est configuré pour garantir une synchronisation correcte des horloges réseau. Le fuseau horaire est ajusté sur "Europe/Paris" pour correspondre à la localisation, ce qui est crucial pour une gestion précise des logs et des événements.
Dans un premier temps nous allons configuré notre propre « UTI107.pfsense.pool.ntp.org » en attendant de trouver un plus fiable.



L'interface WAN est configurée avec une adresse IP statique (192.168.10.254). Ce choix garantit une connectivité stable et prévisible. Les autres paramètres, comme l'adresse MAC ou la MTU, sont laissés par défaut sauf en cas de configuration spécifique.



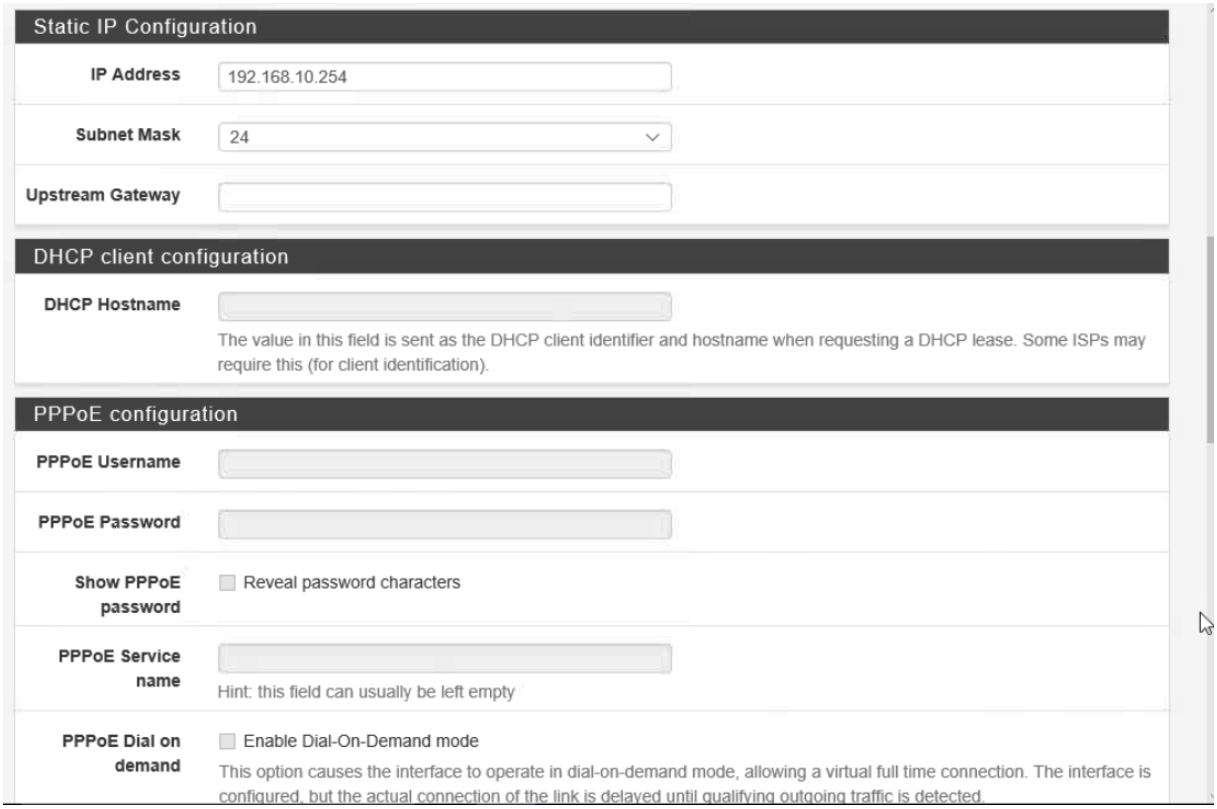
L'adresse LAN est définie sur 10.0.107.254 avec un masque de sous-réseau /24. Cette configuration offre un accès fiable aux équipements internes et prépare le réseau pour une gestion centralisée.



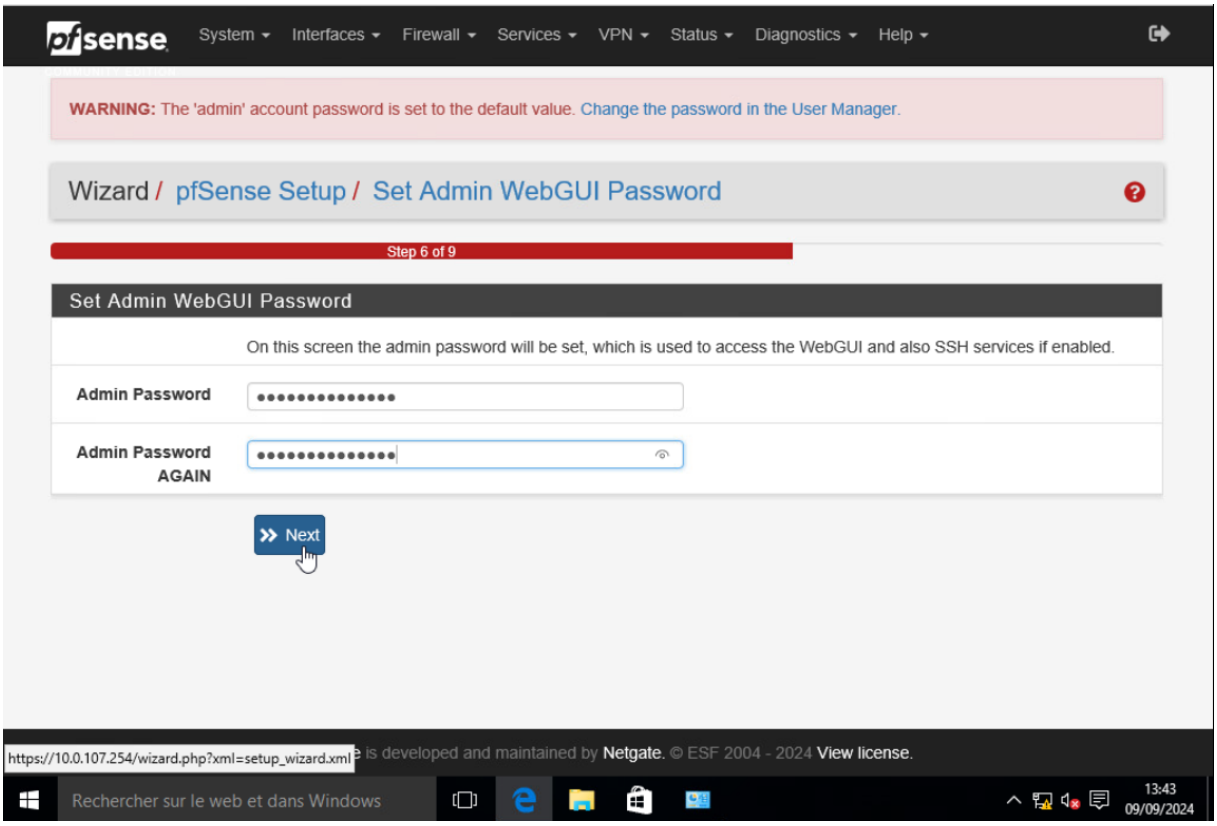
Dans la configuration de l'interface réseau, une adresse IP statique, ici **192.168.10.254**, est spécifiée avec un masque de sous-réseau /24. Cela garantit une connectivité stable et une segmentation claire du réseau. Cette approche est idéale pour éviter les conflits d'adresses et fournir une passerelle fiable pour le trafic réseau.

Le champ "Upstream Gateway" reste vide, car il n'est requis que si une route spécifique doit être définie manuellement. Cela est généralement utilisé dans des configurations plus avancées pour définir des chemins précis vers d'autres réseaux.

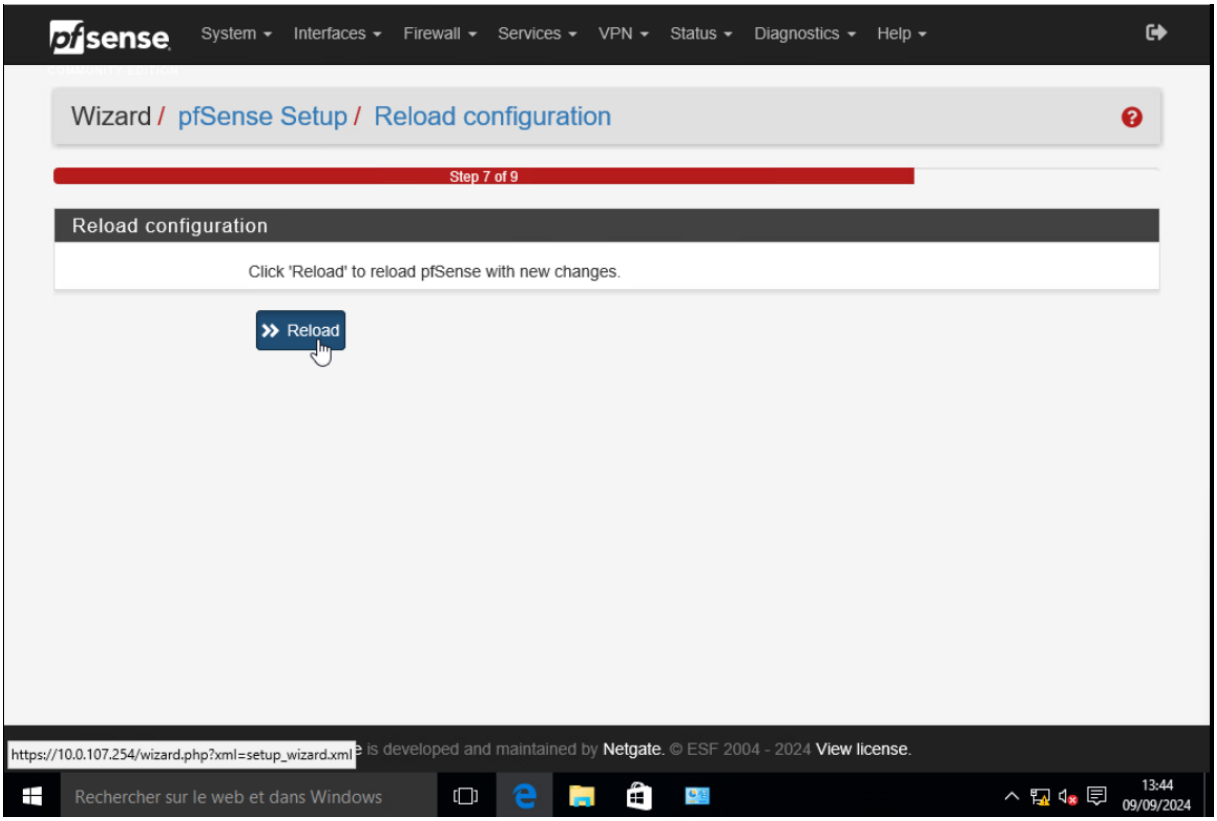
Les sections relatives au DHCP et au PPPoE ne sont pas remplies, car elles ne s'appliquent pas dans ce cas particulier. Le DHCP n'est pas configuré, car une adresse IP statique est préférée pour un meilleur contrôle, tandis que le PPPoE est inutile si l'environnement réseau n'utilise pas cette méthode d'authentification. Cette configuration optimise les performances tout en simplifiant l'administration.



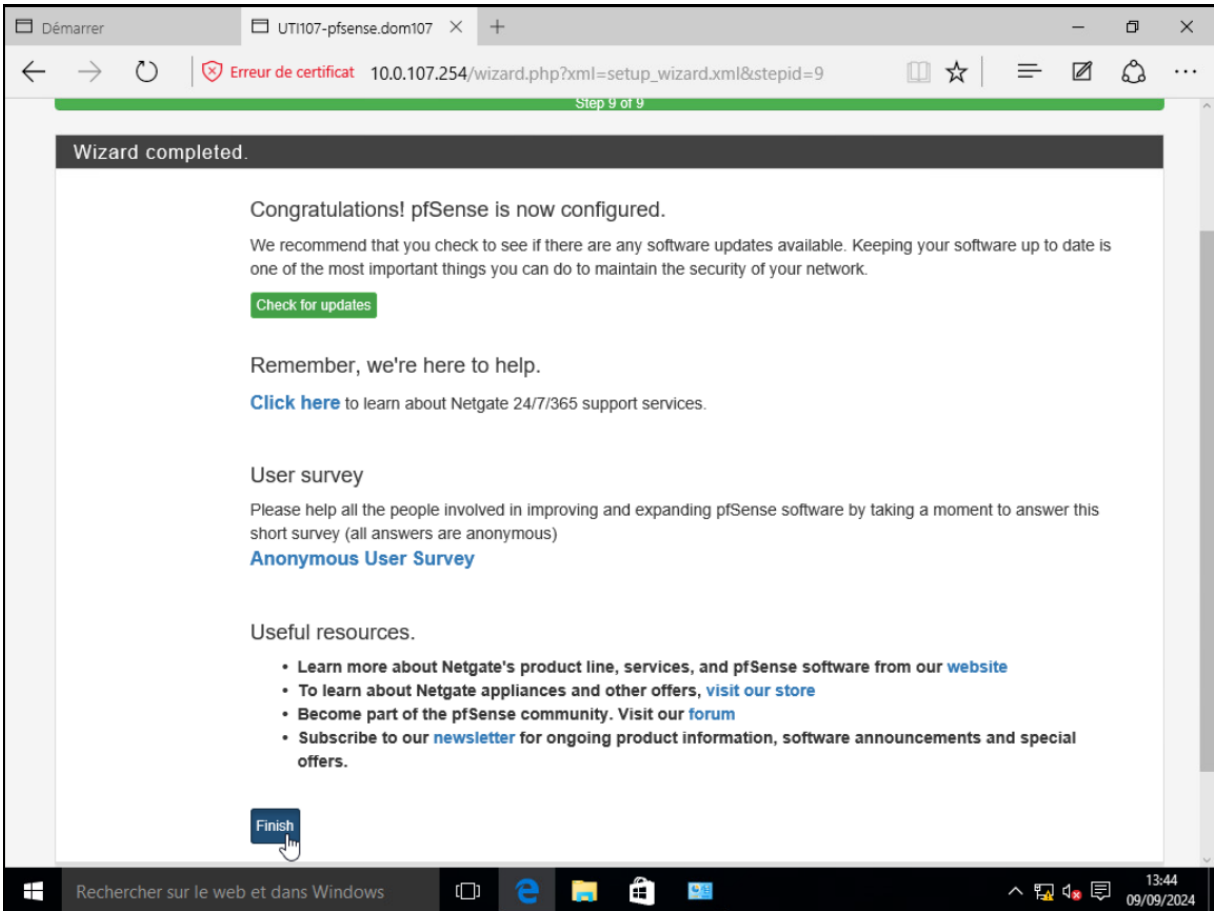
Le mot de passe administrateur est modifié pour sécuriser l'accès à l'interface Web et éviter toute utilisation des informations par défaut. Cette mesure est essentielle pour protéger l'administration du pare-feu.



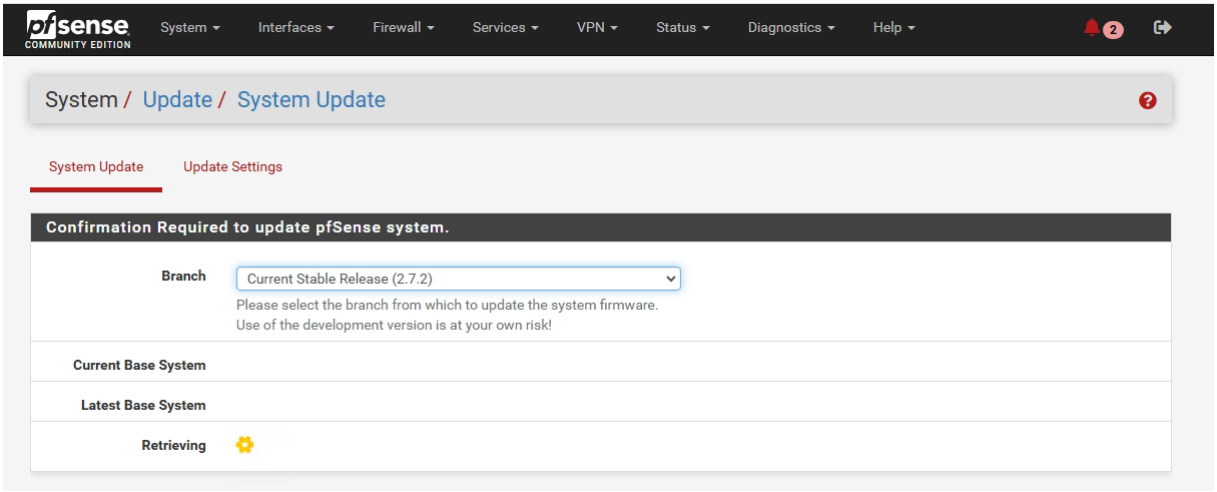
Les nouveaux paramètres sont appliqués en rechargeant la configuration. Cette étape permet de s'assurer que toutes les modifications, comme les adresses IP et les mots de passe, sont prises en compte par pfSense.

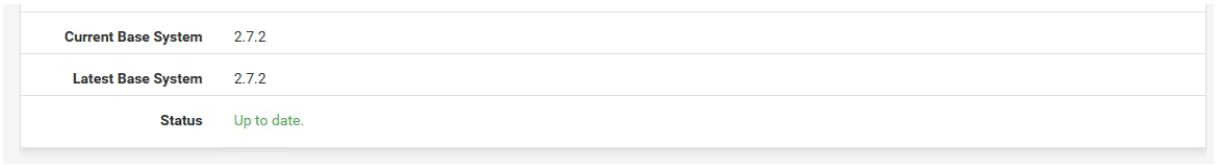


Le message final confirme que pfSense est entièrement configuré et fonctionnel. L'utilisateur est invité à vérifier les mises à jour pour s'assurer que le système est à jour et sécurisé. L'installation est maintenant prête pour une utilisation dans un environnement réseau.

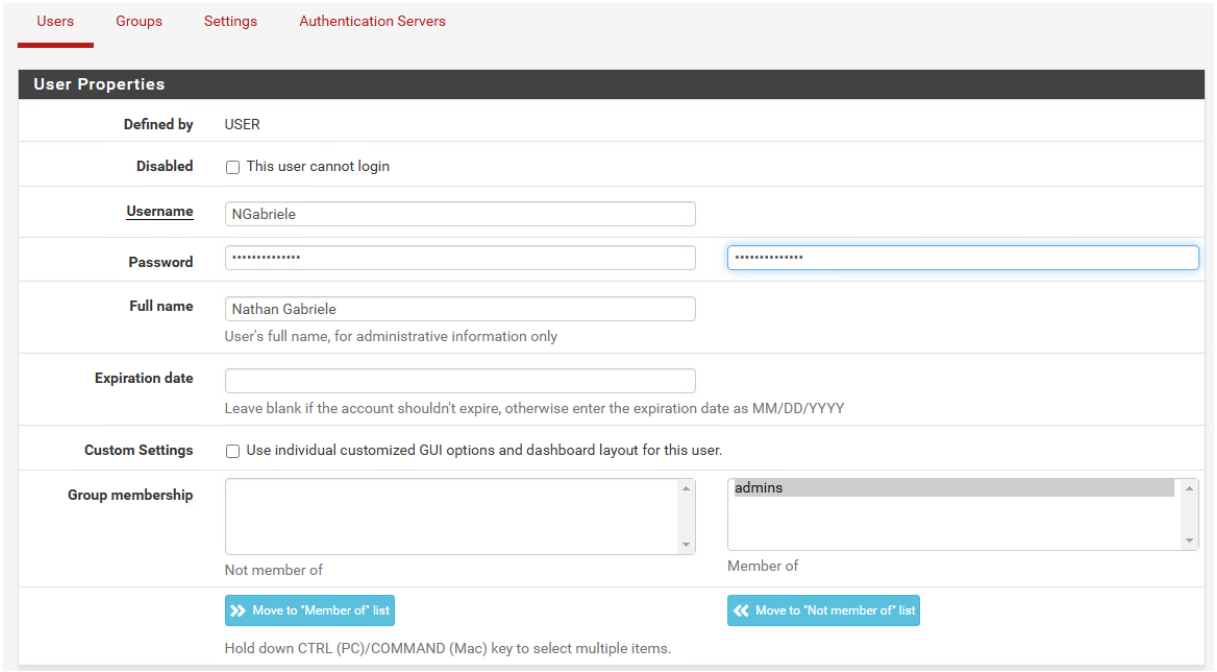


La page de mise à jour affiche que la version actuelle du système est **2.7.2** et qu'elle correspond à la dernière version stable disponible. Cette vérification garantit que le système bénéficie des correctifs de sécurité et des améliorations récentes. Le choix de rester sur la branche stable renforce la fiabilité, évitant les risques liés à des versions de développement.

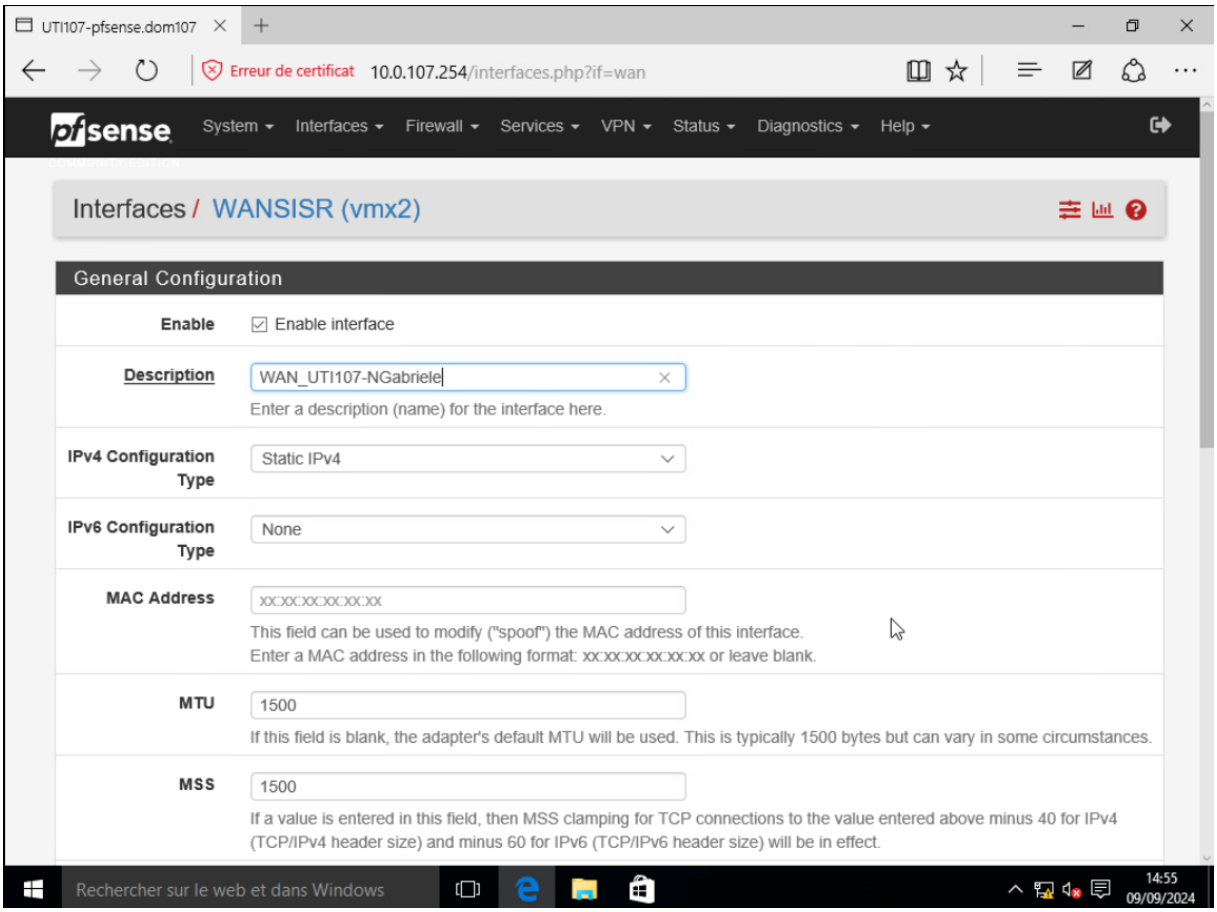




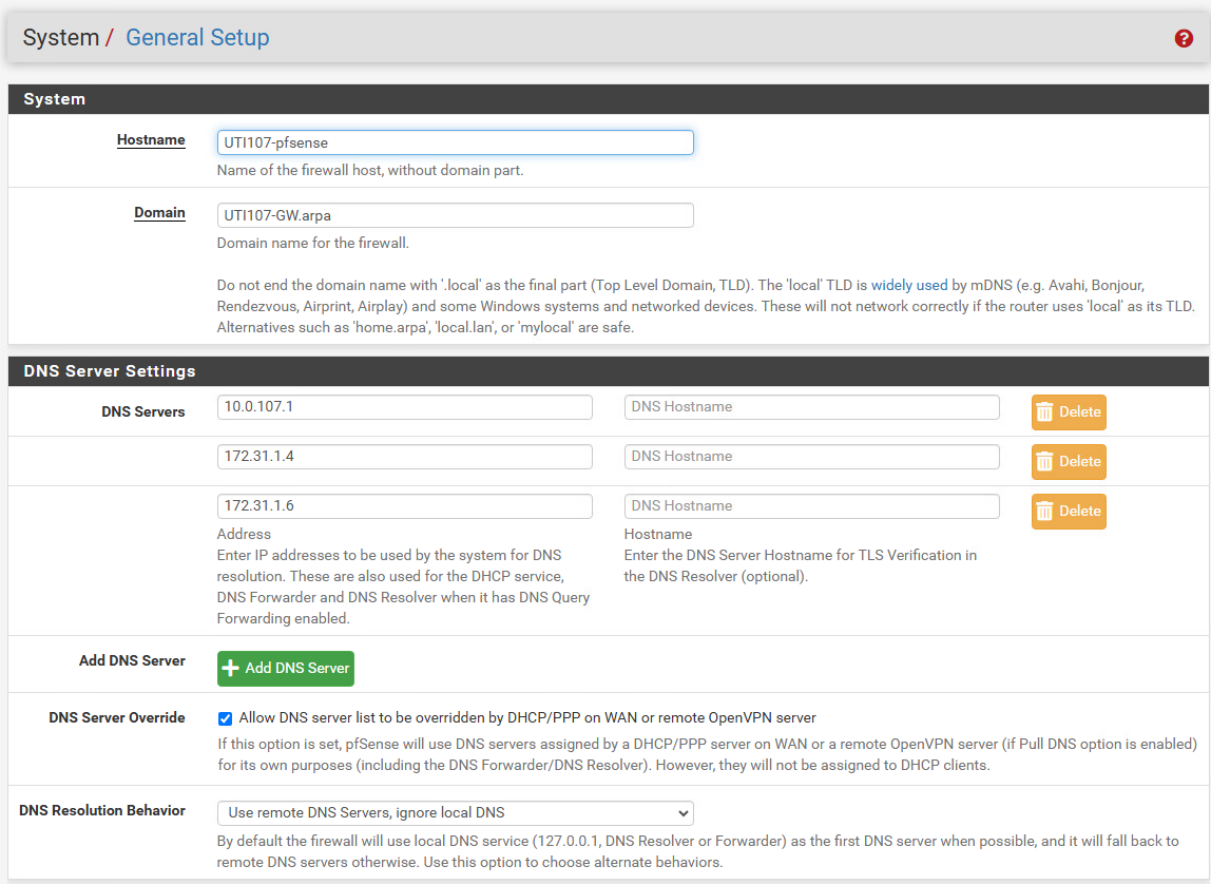
Un utilisateur "NGabriele" est créé avec un mot de passe sécurisé et assigné au groupe "admins". Cette configuration permet de déléguer les privilèges administratifs tout en maintenant une gestion centralisée. L'inclusion d'un nom complet améliore la traçabilité des actions dans les journaux système, ce qui est essentiel pour le suivi et la sécurité.



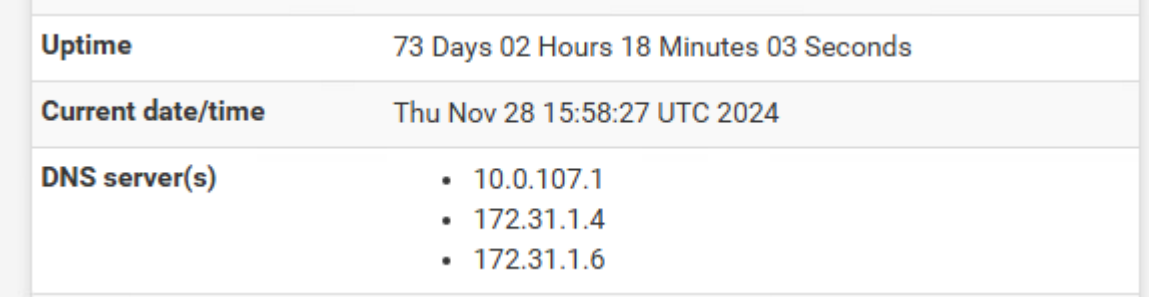
L'interface WAN est activée avec une configuration IPv4 statique, tandis qu'IPv6 est désactivé pour simplifier l'administration dans un environnement où IPv6 n'est pas requis. Une description précise "WAN_UTI107-NGabriele" permet d'identifier cette interface rapidement dans des réseaux complexes, et les paramètres par défaut, comme la MTU, assurent une compatibilité optimale.



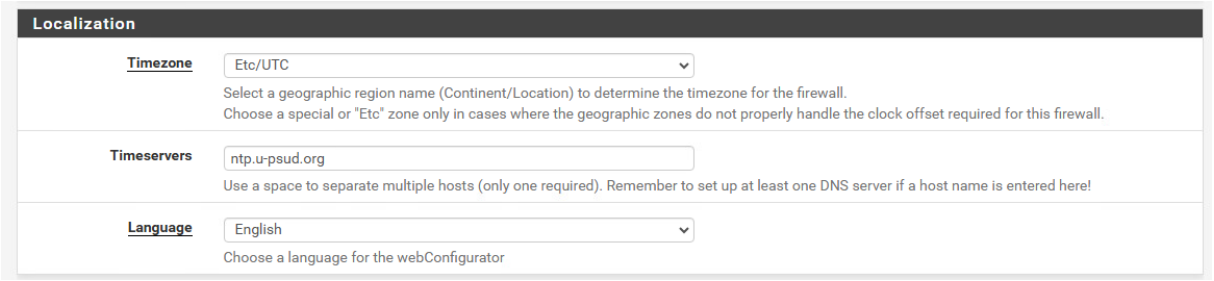
Le nom d'hôte "UTI107-pfsense" et le domaine "UTI107-GW.arpa" sont définis pour identifier le pare-feu dans le réseau. Des serveurs DNS internes (10.0.107.1, 172.31.1.4, 172.31.1.6) sont configurés pour accélérer la résolution des noms et garantir un contrôle total. L'option "DNS Server Override" est activée pour permettre une flexibilité dans la gestion DNS si nécessaire.



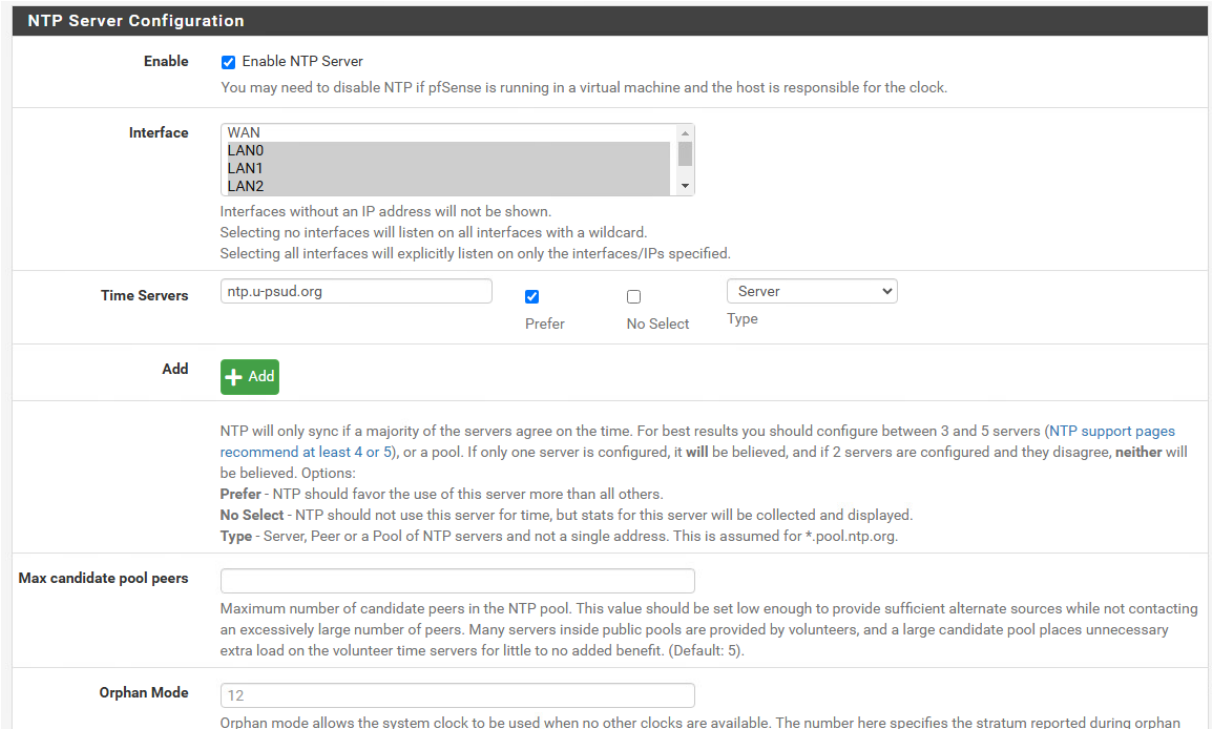
Le tableau indique que le système est opérationnel depuis plus de 73 jours, témoignant de sa stabilité. Les adresses DNS utilisées (10.0.107.1, 172.31.1.4, 172.31.1.6) correspondent aux serveurs configurés précédemment, confirmant leur bon fonctionnement et leur intégration dans l'environnement réseau.



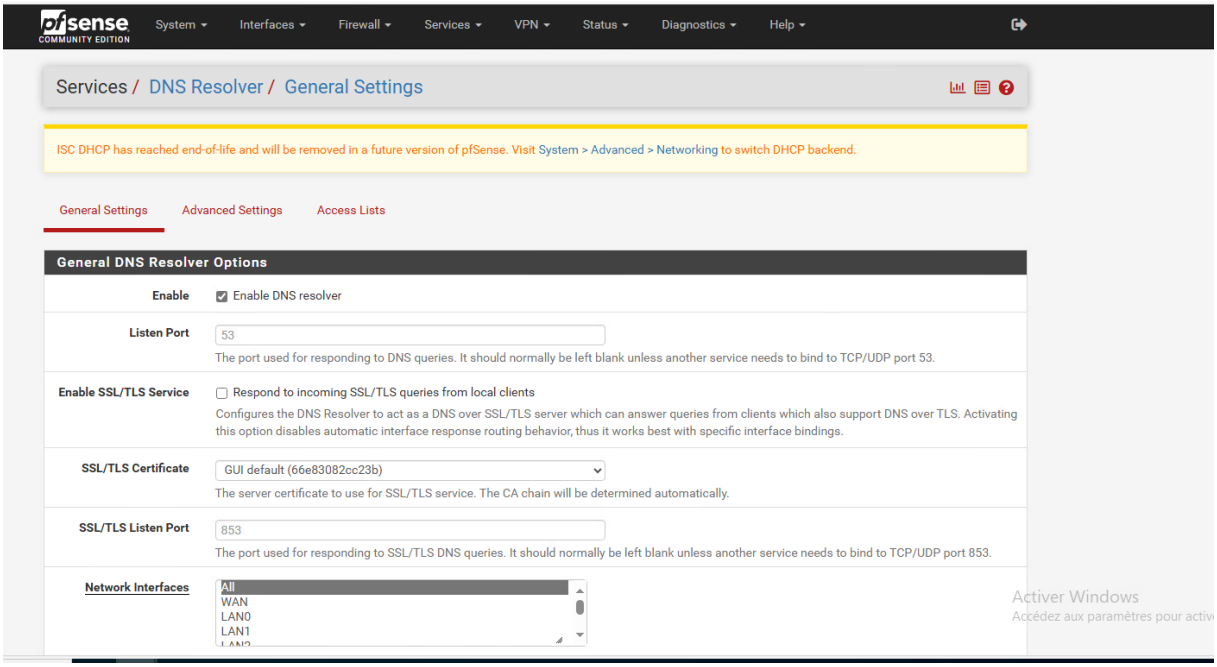
Le serveur NTP est activé et configuré pour écouter sur les interfaces WAN, LAN0, LAN1 et LAN2. Le serveur "ntp.u-psud.org" est utilisé comme source de synchronisation, garantissant des horloges réseau cohérentes. Des paramètres avancés, comme le "Max candidate pool peers", permettent d'ajuster les performances en fonction de l'environnement.



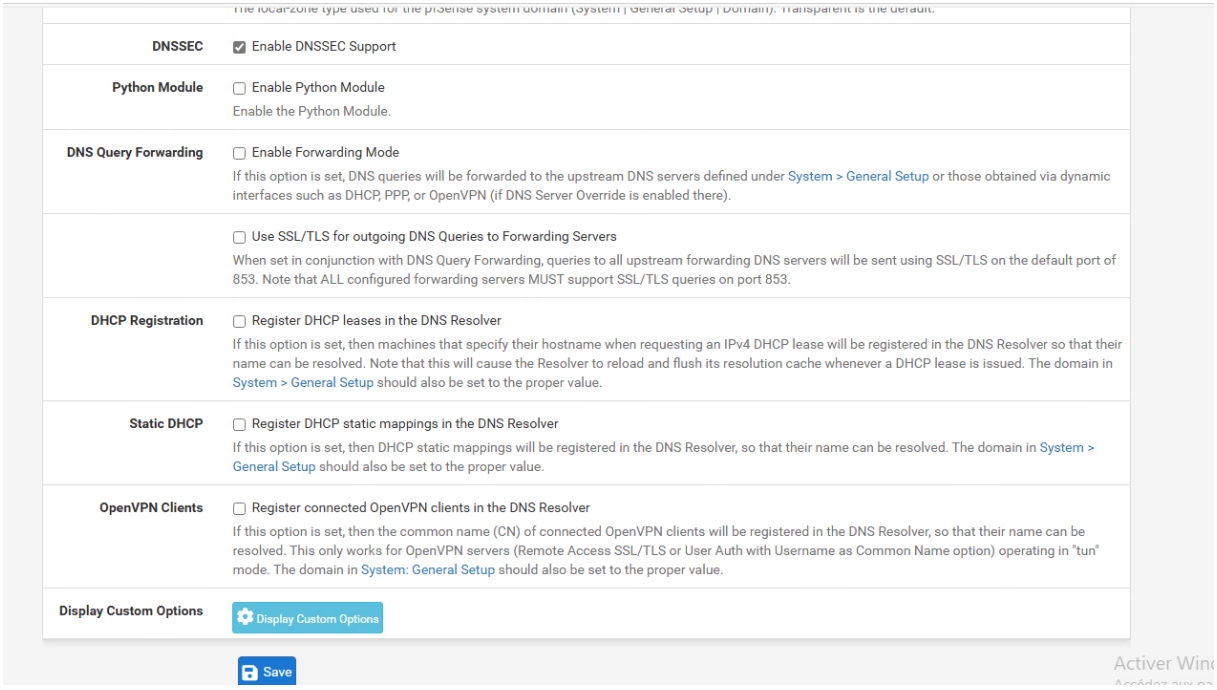
La configuration NTP permet d'activer le service pour synchroniser l'heure sur plusieurs interfaces réseau (WAN, LAN0, LAN1, LAN2). Le serveur "ntp.u-psud.org" est spécifié pour une précision horaire fiable. L'option "Max candidate pool peers" offre un contrôle sur le nombre de serveurs candidats, garantissant une redondance tout en évitant une surcharge. Le mode orphelin est défini à 12 pour assurer une continuité même sans serveur principal.



Des fonctionnalités comme DNSSEC pour valider l'intégrité des réponses DNS et l'enregistrement des baux DHCP dans le résolveur sont activées. Cela améliore la sécurité et facilite la résolution locale des noms. L'utilisation de la redirection DNS n'est pas activée, maintenant ainsi le contrôle direct sur les requêtes locales.



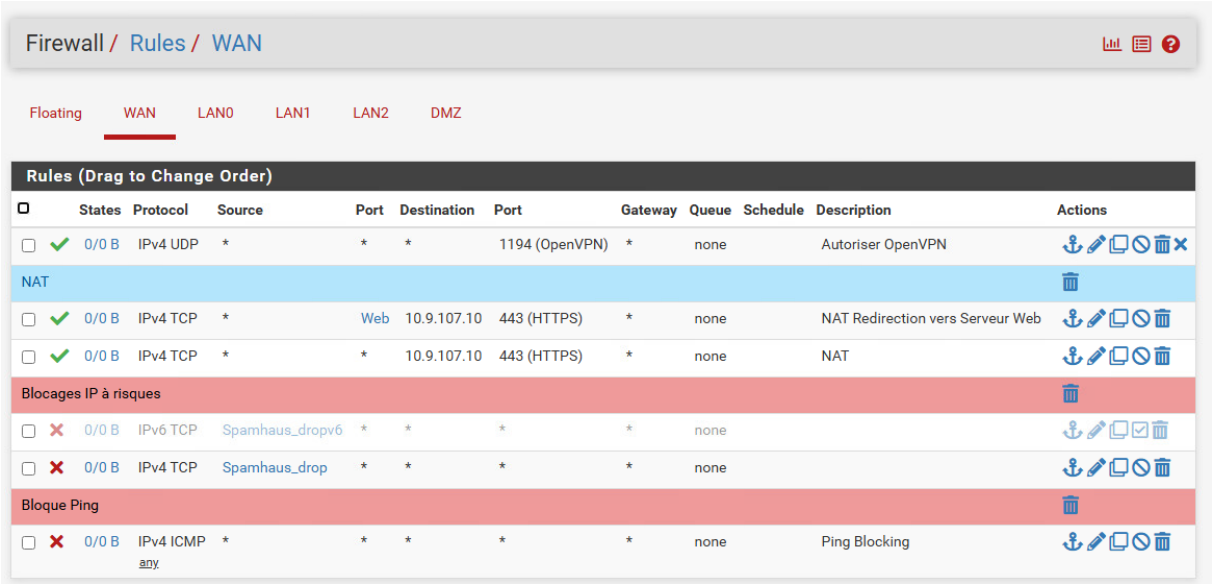
Après avoir ajusté les paramètres du résolveur DNS, une notification invite à appliquer les changements pour les rendre effectifs. Cette étape assure la mise à jour immédiate de la configuration réseau. Une mise en garde est affichée concernant la fin de vie de ISC DHCP, incitant à envisager des alternatives futures.



Configuration des règles de pare-feu

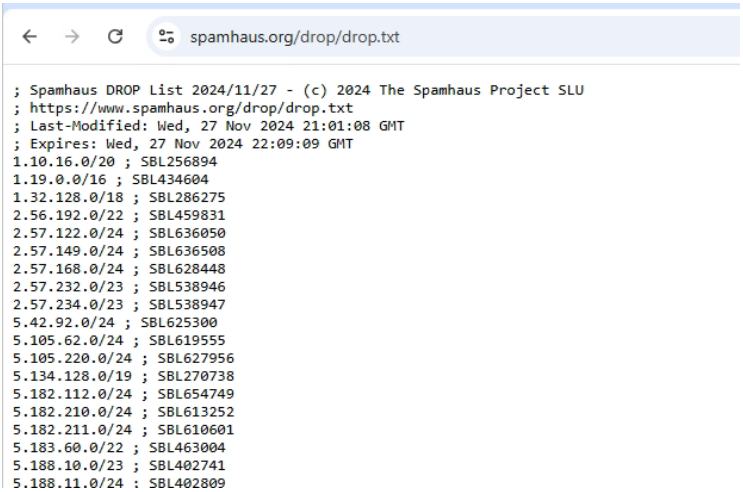
La configuration des règles sur un pare-feu est indispensable pour contrôler et sécuriser les échanges entre les différentes zones du réseau et l'extérieur. En définissant des politiques adaptées, il est possible d’autoriser uniquement les services essentiels, tout

en bloquant les flux indésirables ou malveillants. Cette démarche permet de protéger les systèmes contre les intrusions, les abus et les cyberattaques tout en assurant une gestion optimale du trafic réseau. Dans cette partie, nous appliquerons ces principes à notre pare-feu pfSense, en configurant les interfaces WAN, LAN0, LAN1, LAN2 et DMZ, afin d'implémenter des politiques spécifiques pour chaque segment réseau et garantir une sécurité renforcée.

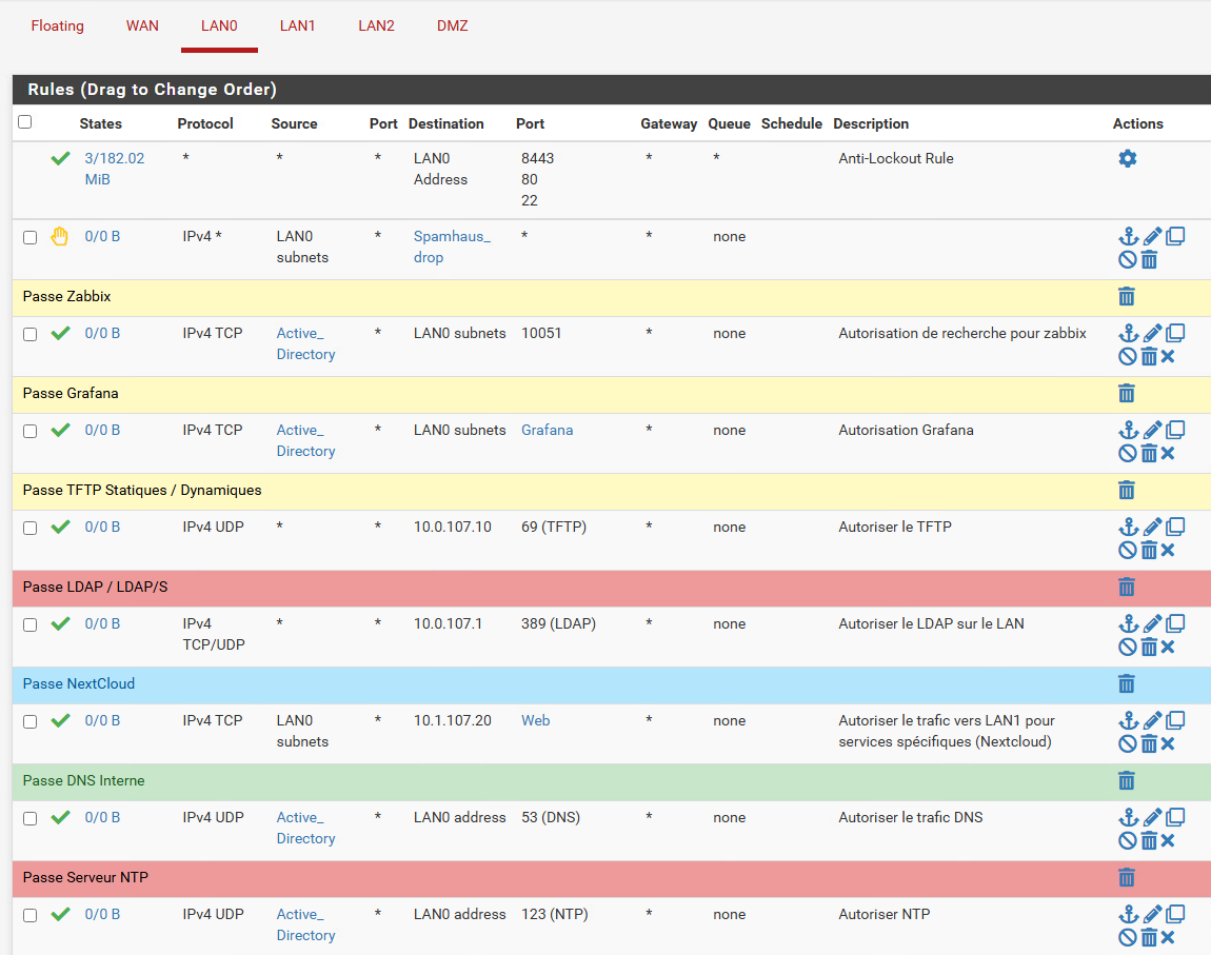


Interface WAN

1. **OpenVPN (Port 1194)** :
    - **Protocole** : IPv4 UDP.
    - **Action** : Autoriser.
    - **Justification** : Permettre les connexions VPN sécurisées via OpenVPN pour accéder au réseau interne depuis l'extérieur.
2. **NAT vers Serveur Web (Ports 80, 443)** :
    - **Protocole** : IPv4 TCP.
    - **Action** : Autoriser avec redirection.
    - **Justification** : Diriger le trafic entrant HTTP/HTTPS vers le serveur web interne, essentiel pour l'accès aux applications web.



3. **Blocage IP Spamhaus** :
    - **Protocole** : IPv4 TCP et IPv6 TCP.
    - **Action** : Bloquer.
    - **Justification** : Rejet des adresses identifiées comme malveillantes via la liste Spamhaus, renforçant la sécurité du réseau.
4. **Blocage Ping** :
    - **Protocole** : IPv4 ICMP.
    - **Action** : Bloquer.
    - **Justification** : Désactiver les réponses aux requêtes ICMP pour limiter la reconnaissance réseau externe.



Floating | WAN | LAN0 | LAN1 | LAN2 | DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	3/182.02 MiB	*	*	*	LAN0 Address	8443 80 22	*	*		Anti-Lockout Rule	⚙
☐	0/0 B	IPv4 *	LAN0 subnets	*	Spamhaus_ drop	*	*	none			⚓ ✎ ⧉ ⊘ 🗑
Passe Zabbix											🗑
☐	0/0 B	IPv4 TCP	Active_ Directory	*	LAN0 subnets	10051	*	none		Autorisation de recherche pour zabbix	⚓ ✎ ⧉ ⊘ 🗑 ✕
Passe Grafana											🗑
☐	0/0 B	IPv4 TCP	Active_ Directory	*	LAN0 subnets	Grafana	*	none		Autorisation Grafana	⚓ ✎ ⧉ ⊘ 🗑 ✕
Passe TFTP Statiques / Dynamiques											🗑
☐	0/0 B	IPv4 UDP	*	*	10.0.107.10	69 (TFTP)	*	none		Autoriser le TFTP	⚓ ✎ ⧉ ⊘ 🗑 ✕
Passe LDAP / LDAP/S											🗑
☐	0/0 B	IPv4 TCP/UDP	*	*	10.0.107.1	389 (LDAP)	*	none		Autoriser le LDAP sur le LAN	⚓ ✎ ⧉ ⊘ 🗑 ✕
Passe NextCloud											🗑
☐	0/0 B	IPv4 TCP	LAN0 subnets	*	10.1.107.20	Web	*	none		Autoriser le trafic vers LAN1 pour services spécifiques (Nextcloud)	⚓ ✎ ⧉ ⊘ 🗑 ✕
Passe DNS Interne											🗑
☐	0/0 B	IPv4 UDP	Active_ Directory	*	LAN0 address	53 (DNS)	*	none		Autoriser le trafic DNS	⚓ ✎ ⧉ ⊘ 🗑 ✕
Passe Serveur NTP											🗑
☐	0/0 B	IPv4 UDP	Active_ Directory	*	LAN0 address	123 (NTP)	*	none		Autoriser NTP	⚓ ✎ ⧉ ⊘ 🗑 ✕

Interface LAN0

1. **Règle Anti-Lockout** :
    - **Protocole** : Tous.
    - **Action** : Autoriser.
    - **Justification** : Prévention de l'impossibilité de se connecter en cas de configuration incorrecte.
2. **Zabbix Monitoring (Port 10051)** :
    - **Protocole** : IPv4 TCP.
    - **Action** : Autoriser.
    - **Justification** : Permettre la communication entre le serveur Zabbix et les hôtes surveillés.
3. **Accès Grafana (Port 3000)** :
    - **Protocole** : IPv4 TCP.
    - **Action** : Autoriser.

- **Justification** : Autoriser l'accès à l'interface graphique de supervision Grafana.

4. **TFTP (Port 69)** :
   - **Protocole** : IPv4 UDP.
   - **Action** : Autoriser.
   - **Justification** : Activer le transfert de fichiers via TFTP pour les périphériques réseau.
5. **LDAP (Port 389)** :
   - **Protocole** : IPv4 TCP/UDP.
   - **Action** : Autoriser.
   - **Justification** : Assurer la connectivité au serveur LDAP pour l'authentification et la gestion des utilisateurs.
6. **DNS et NTP** :
   - **Protocole** : IPv4 UDP.
   - **Action** : Autoriser.
   - **Justification** : Nécessaire pour les résolutions DNS et la synchronisation temporelle.

Passe Applications Spécifiques									
0/0 B	IPv4 TCP/UDP	*	*	*	Trafic_App_Specifique	*	none	Règle pour applications spécifiques	
Passe AnyDesk									
0/0 B	IPv4 TCP/UDP	LAN2 subnets	*	WAN address	ANYDESK_Port	*	none	Autorisation Anydesk	
Accès Internet									
0/0 B	IPv4 TCP/UDP	*	*	*	Web	*	none		
0/0 B	IPv4 TCP	LAN0 subnets	*	10.1.107.10	Web	*	none		
Accès SSH									
0/0 B	IPv4 TCP	LAN0 subnets	*	LAN0 subnets	2222	*	none		
Passe tout									
26/787.02 MiB	IPv4 *	*	*	*	*	*	none		
Bloque tout									
0/560 B	IPv4 *	*	*	*	*	*	none		
0/0 B	IPv4 *	LAN0 subnets	*	Spamhaus_drop	*	*	none		

Applications Spécifiques :

- **Protocole :** IPv4 TCP/UDP.
- **Action :** Autoriser.
- **Justification :** Permettre le trafic pour des applications spécifiques nécessitant des ports définis pour leur fonctionnement.

AnyDesk :

- **Protocole :** IPv4 TCP/UDP.
- **Action :** Autoriser.
- **Justification :** Autoriser l'accès à distance via AnyDesk depuis le réseau LAN2 vers l'adresse WAN.

Accès Internet :

- **Protocole :** IPv4 TCP/UDP.
- **Action :** Autoriser.
- **Justification :** Garantir l'accès général à Internet pour les hôtes du LAN0. Une règle spécifique est également définie pour le trafic web vers l'adresse interne 10.1.107.10.

Accès SSH :

- **Protocole :** IPv4 TCP.
- **Action :** Autoriser.
- **Justification :** Faciliter la gestion sécurisée des machines au sein du LAN0 en autorisant les connexions SSH sur le port 2222.

Passe Tout :

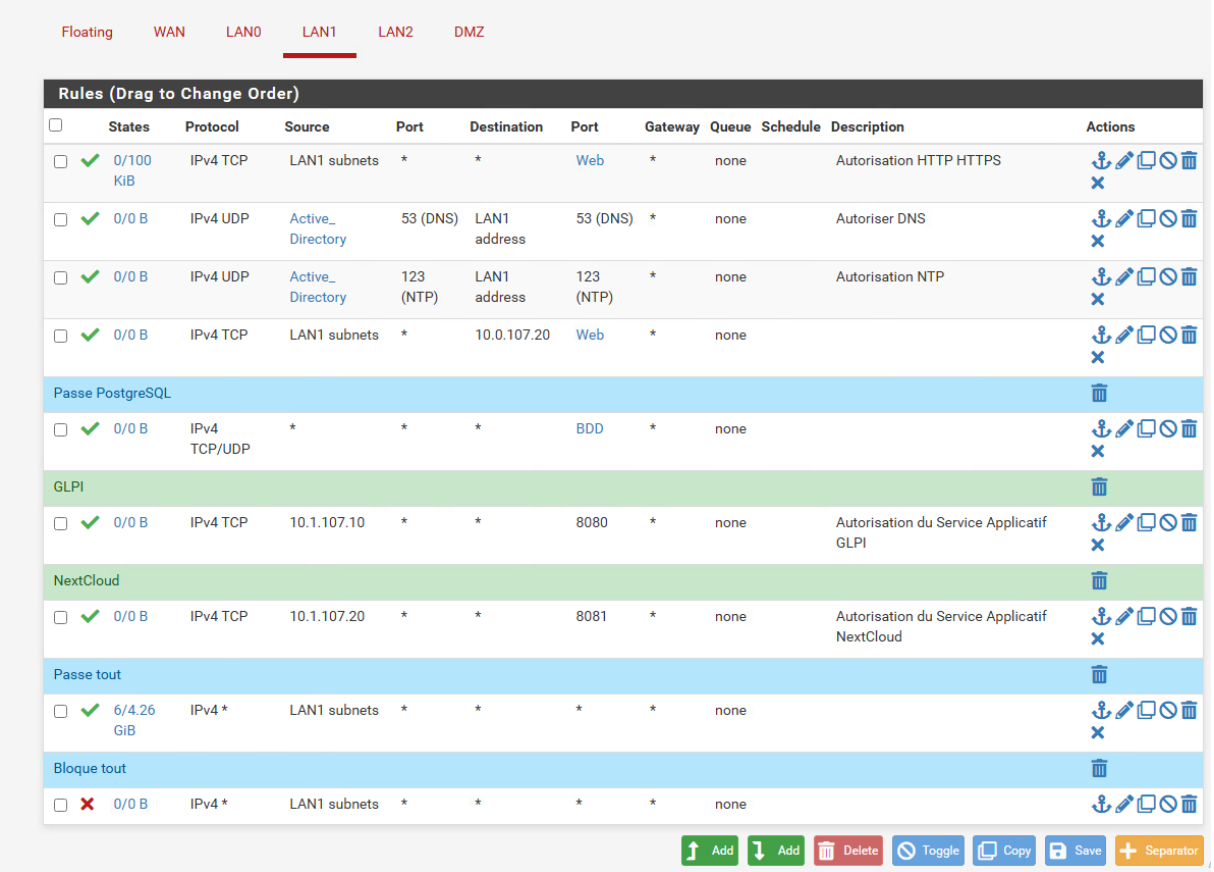
- **Protocole :** IPv4 Tous.
- **Action :** Autoriser.
- **Justification :** Utilisée pour tester la connectivité et valider les configurations, en permettant temporairement tout le trafic IPv4.

Bloque Tout :

- **Protocole :** IPv4 Tous.
- **Action :** Bloquer.
- **Justification :** Bloquer tout le trafic non autorisé par les règles précédentes pour renforcer la sécurité du réseau.

Blocage Spamhaus :

- **Protocole :** IPv4 Tous.
- **Action :** Bloquer.
- **Justification :** Empêcher toute communication avec les adresses IP répertoriées comme malveillantes par Spamhaus pour réduire les risques d'intrusion et de cyberattaques.

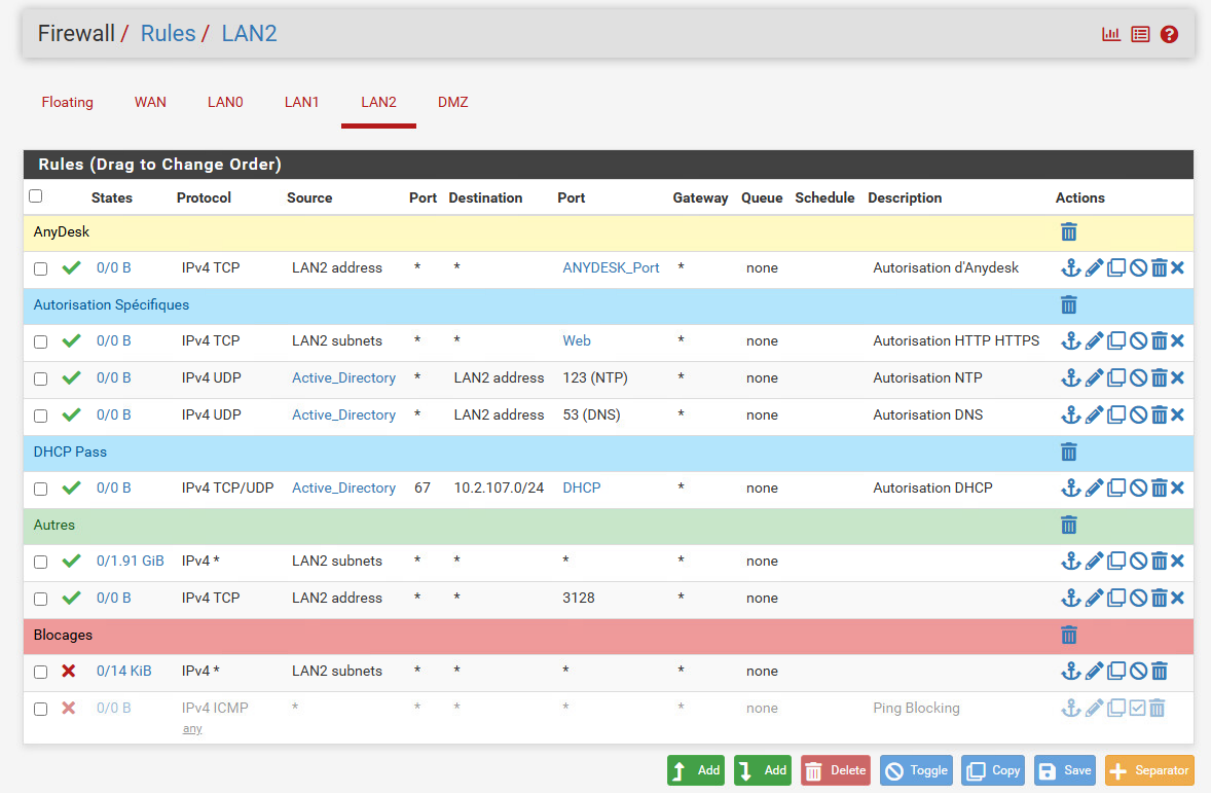


Interface LAN1

1. **DNS et NTP** :
    - **Protocole** : IPv4 UDP.
    - **Action** : Autoriser.
    - **Justification** : Faciliter la résolution de noms et le maintien d'une heure système correcte.
2. **Accès GLPI (Port 8080)** :
    - **Protocole** : IPv4 TCP.
    - **Action** : Autoriser.

- **Justification** : Garantir l'accès à l'outil de gestion des services informatiques.

3. **NextCloud (Port 8081)** :
   - **Protocole** : IPv4 TCP.
   - **Action** : Autoriser.
   - **Justification** : Permettre l'accès au service de stockage et partage de fichiers.
4. **Blocage Global** :
   - **Protocole** : IPv4 Tous.
   - **Action** : Bloquer.
   - **Justification** : Bloquer tout trafic non explicitement autorisé.

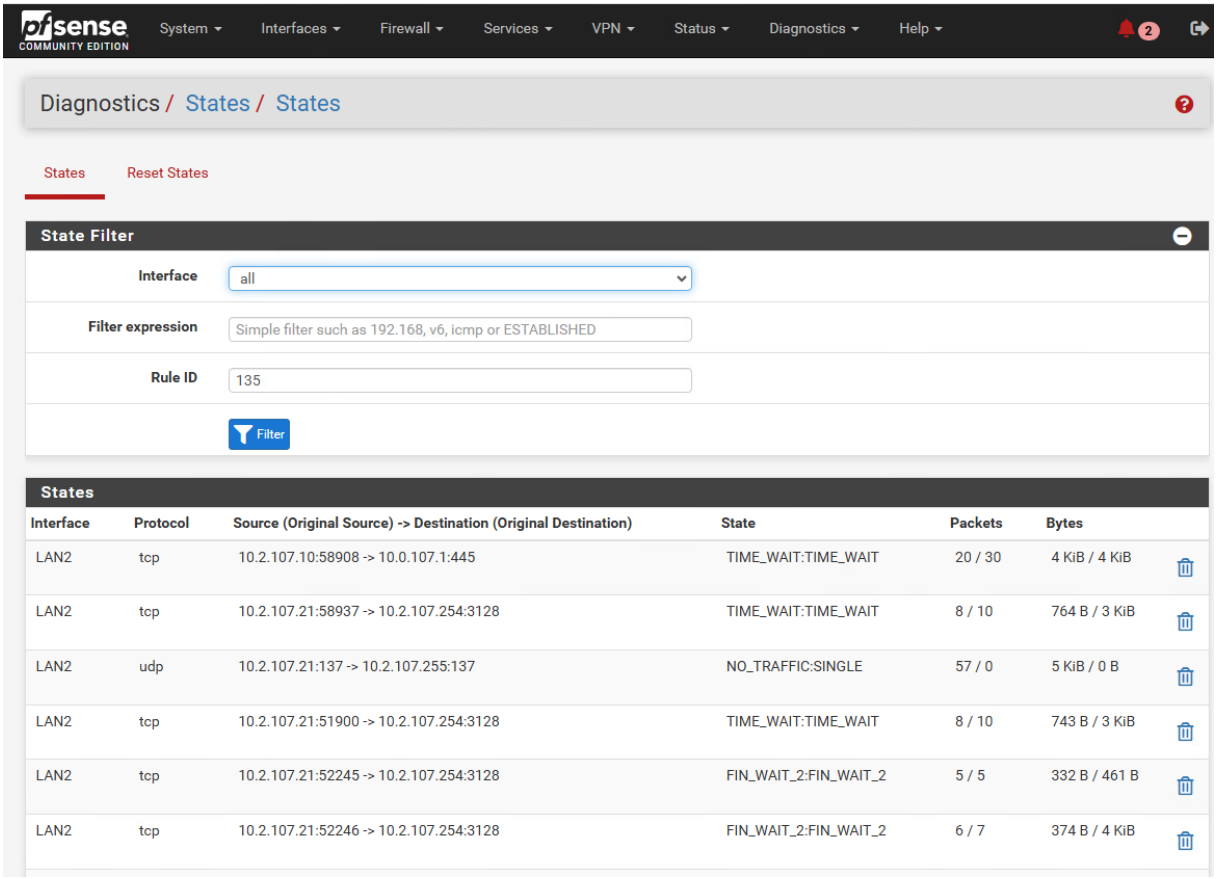


L'interface de diagnostic des états réseau permet d'observer les connexions actives sur chaque interface du pare-feu. Elle détaille les protocoles utilisés, les adresses source et destination, l'état des connexions (comme "TIME_WAIT" pour les connexions TCP en fin de session), ainsi que le nombre de paquets et d'octets échangés.

Cette fonctionnalité est cruciale pour surveiller en temps réel les flux traversant le réseau, confirmant l'application correcte des règles de pare-feu. Par exemple, les

connexions "NO_TRAFFIC:SINGLE" indiquent des tentatives sans échanges effectifs, suggérant un blocage ou une mauvaise configuration côté client ou serveur.

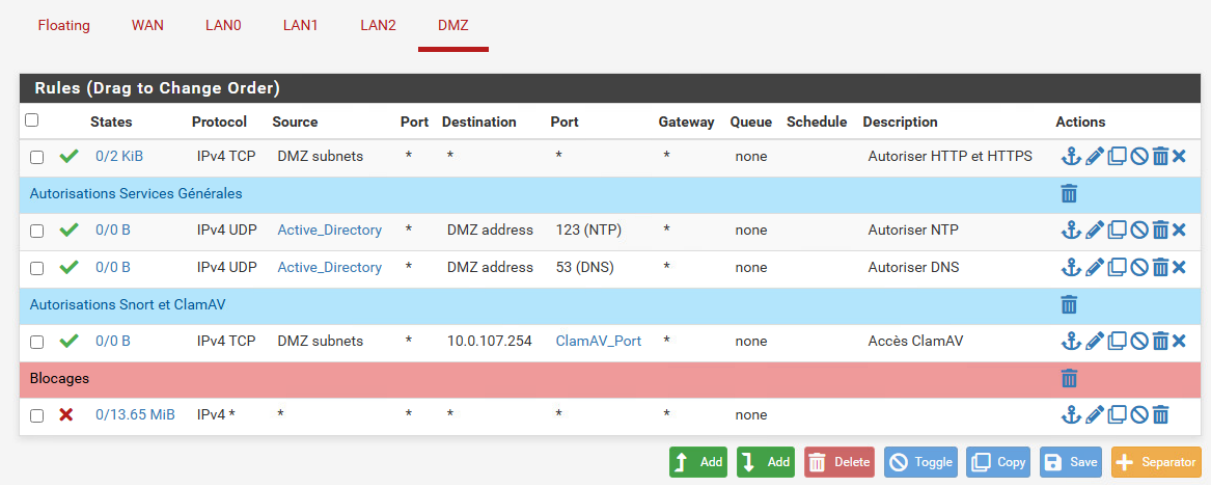
Elle offre également la possibilité de repérer rapidement des activités inhabituelles ou suspectes, comme des flux non autorisés ou des communications excessives, permettant une intervention immédiate pour ajuster les règles ou enquêter sur des comportements anormaux.



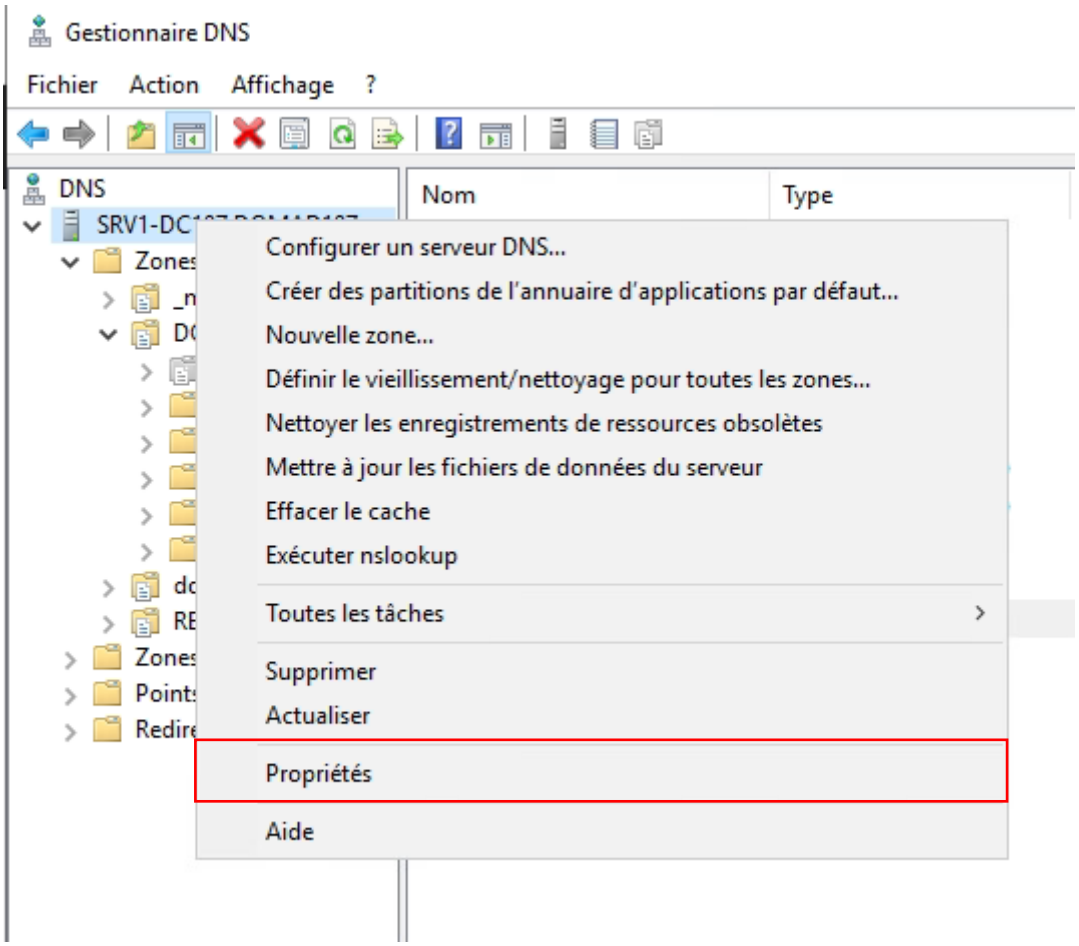
Interface DMZ

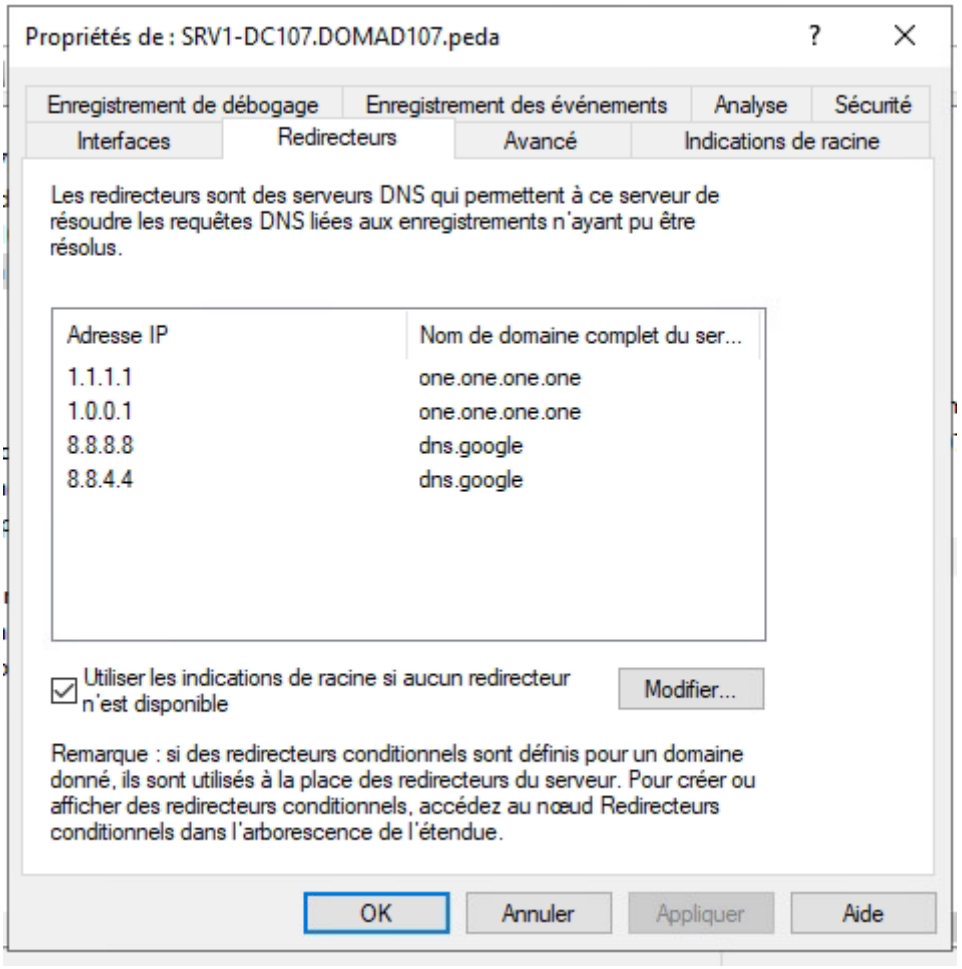
1. **HTTP/HTTPS** :
    - **Protocole** : IPv4 TCP.
    - **Action** : Autoriser.
    - **Justification** : Activer l'accès aux services web publics.
2. **NTP/DNS** :
    - **Protocole** : IPv4 UDP.
    - **Action** : Autoriser.
    - **Justification** : Maintenir les services de résolution DNS et de synchronisation NTP fonctionnels.

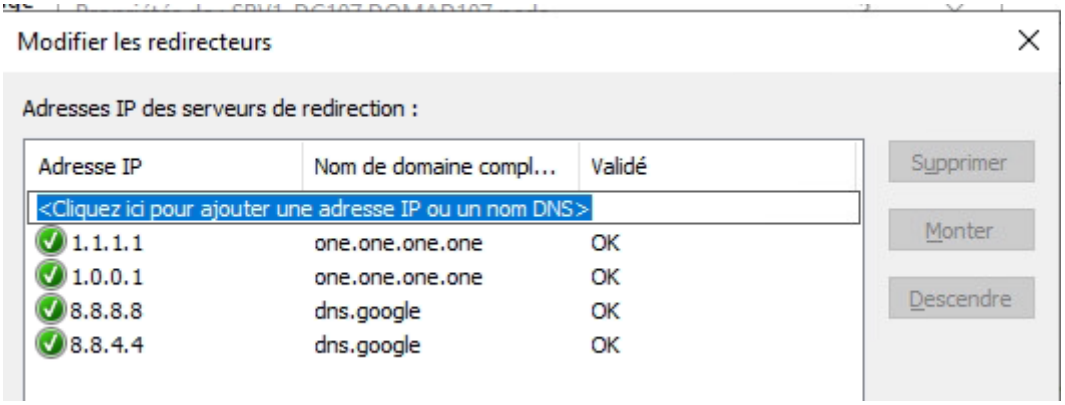
3. **Accès ClamAV** :
    - **Protocole** : IPv4 TCP.
    - **Action** : Autoriser.
    - **Justification** : Permettre aux hôtes de la DMZ d'accéder au service antivirus pour la protection des fichiers.
4. **Blocage Global** :
    - **Protocole** : IPv4 Tous.
    - **Action** : Bloquer.
    - **Justification** : Empêcher tout trafic non autorisé entre la DMZ et les autres réseaux.



Redirecteurs DNS


Gestionnaire DNS
Fichier
Action
Affichage
?
DNS
Nom
Type
Configurer un serveur DNS...
Créer des partitions de l'annuaire d'applications par défaut...
Nouvelle zone...
Définir le vieillissement/nettoyage pour toutes les zones...
Nettoyer les enregistrements de ressources obsolètes
Mettre à jour les fichiers de données du serveur
Effacer le cache
Exécuter nslookup
Toutes les tâches
Supprimer
Actualiser
Propriétés
Aide

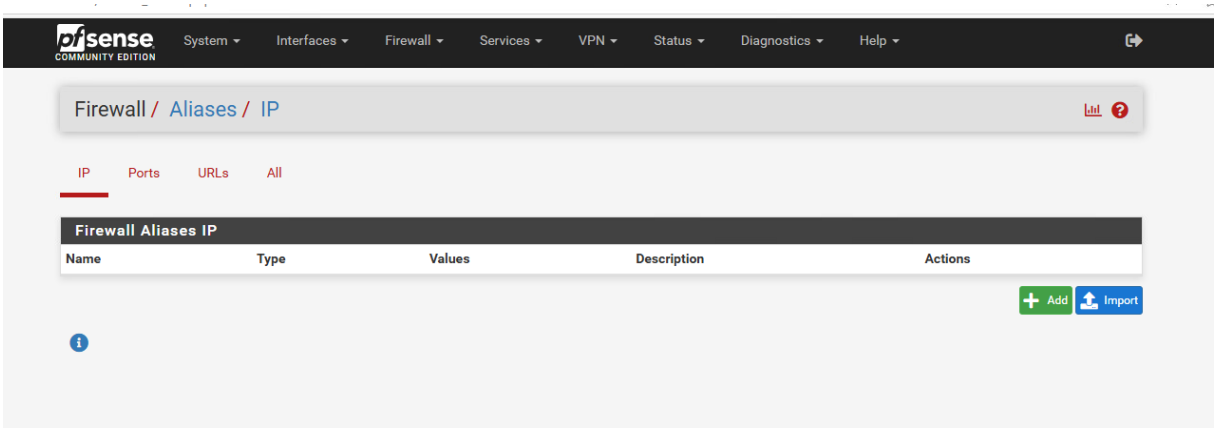


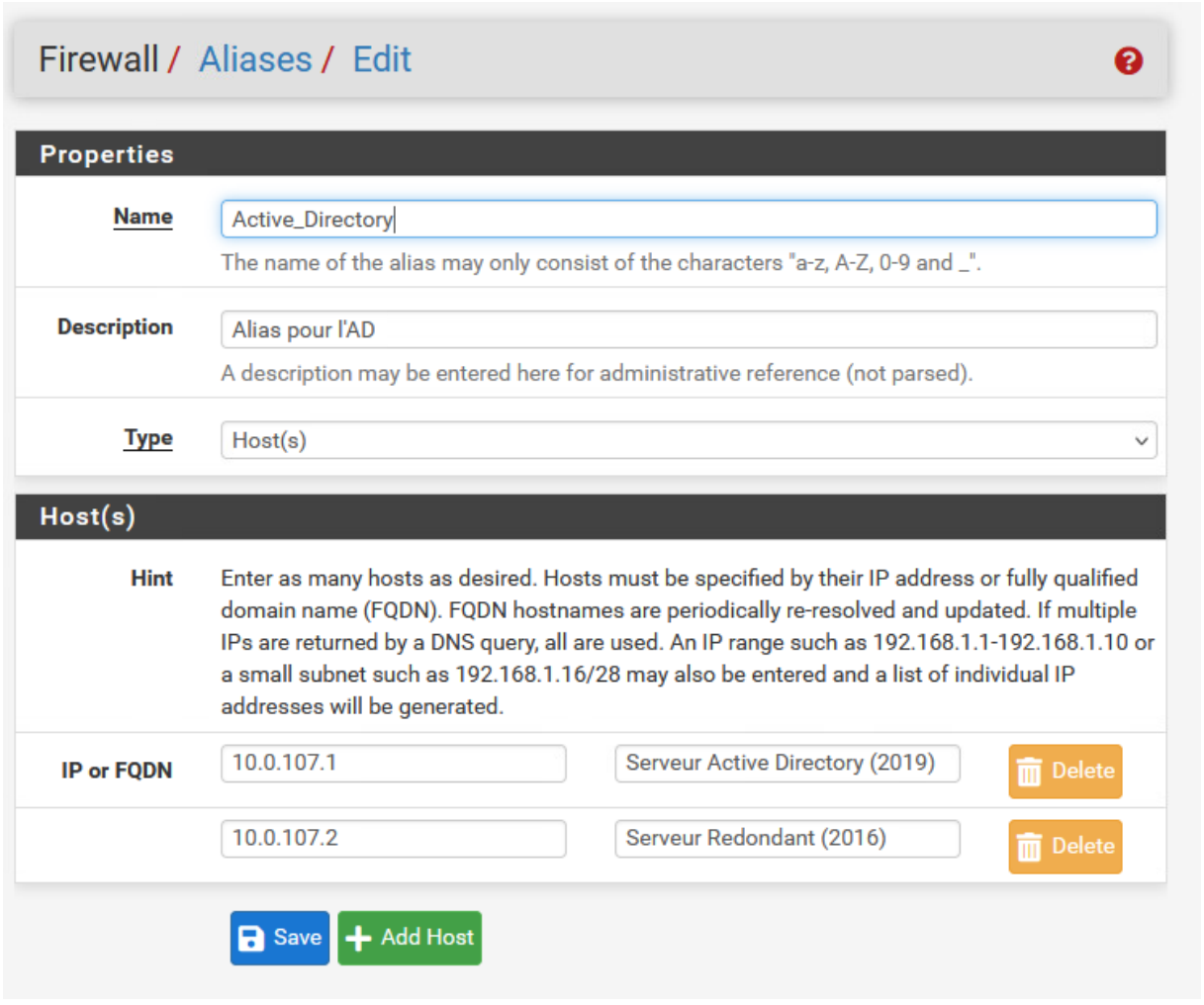


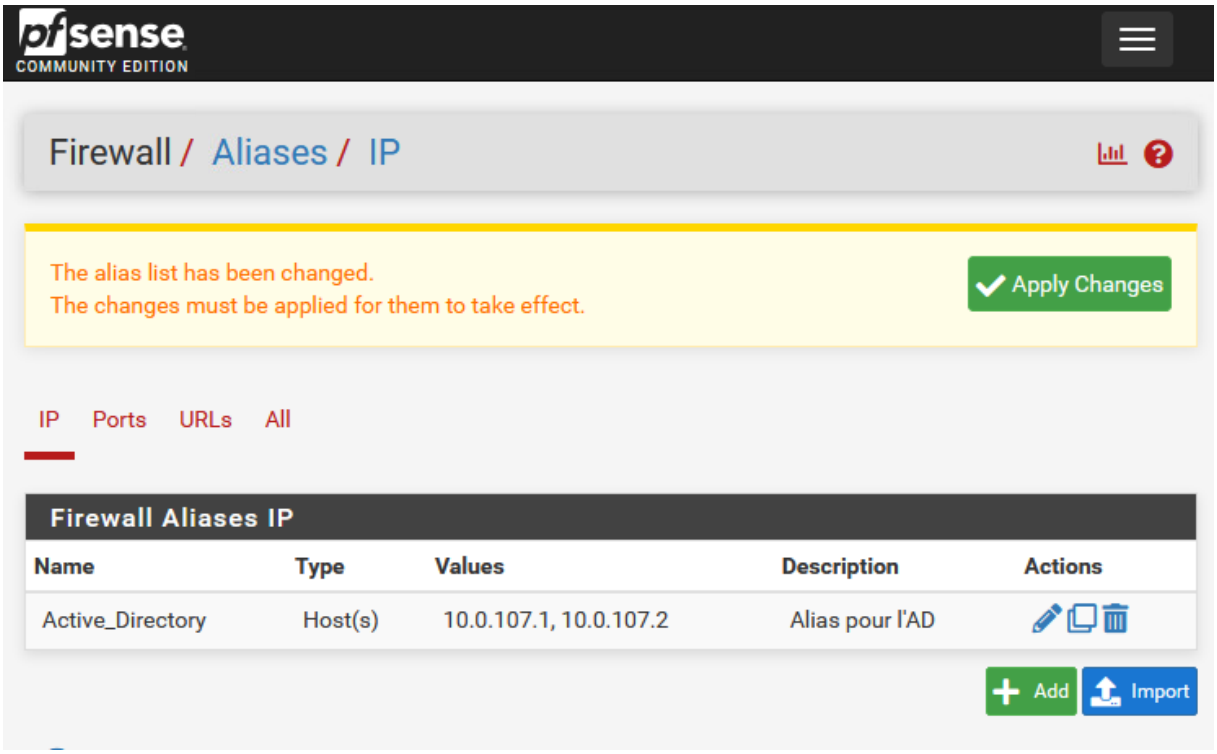
Création d'Alias

Par port

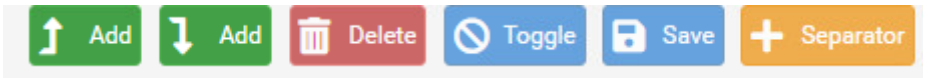
Par IP

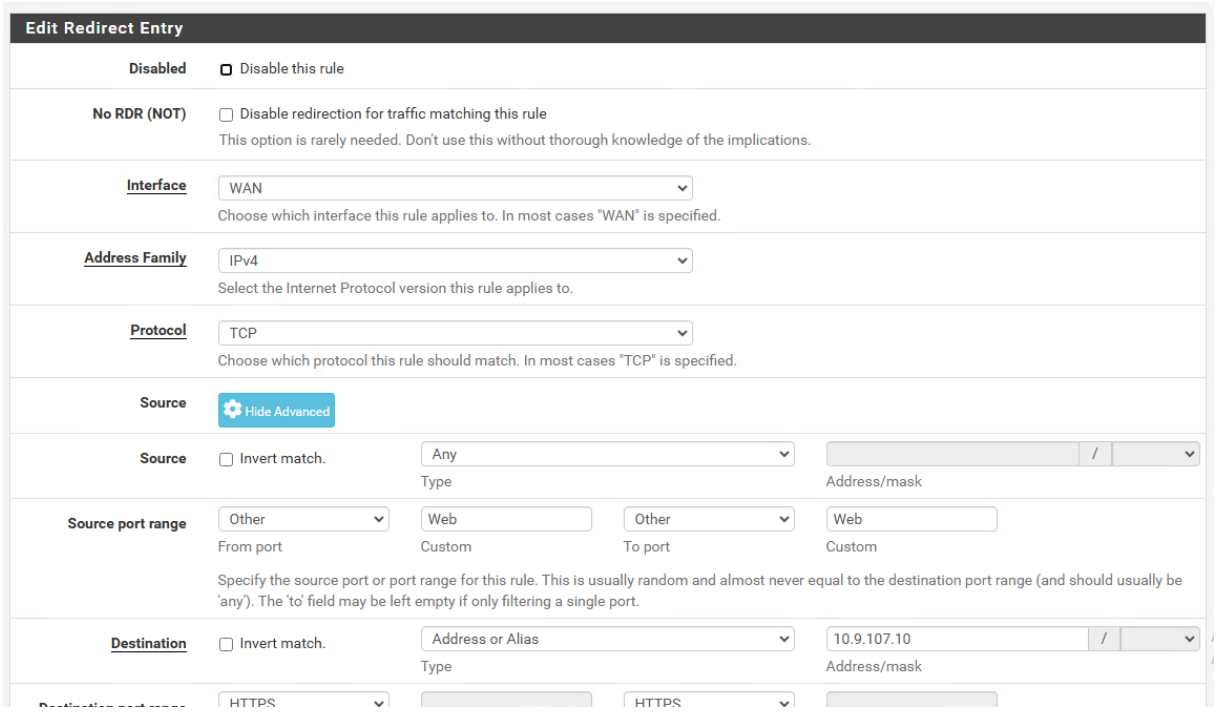

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Aliases / IP
IP
Ports
URLs
All
Firewall Aliases IP
Name
Type
Values
Description
Actions
Add
Import

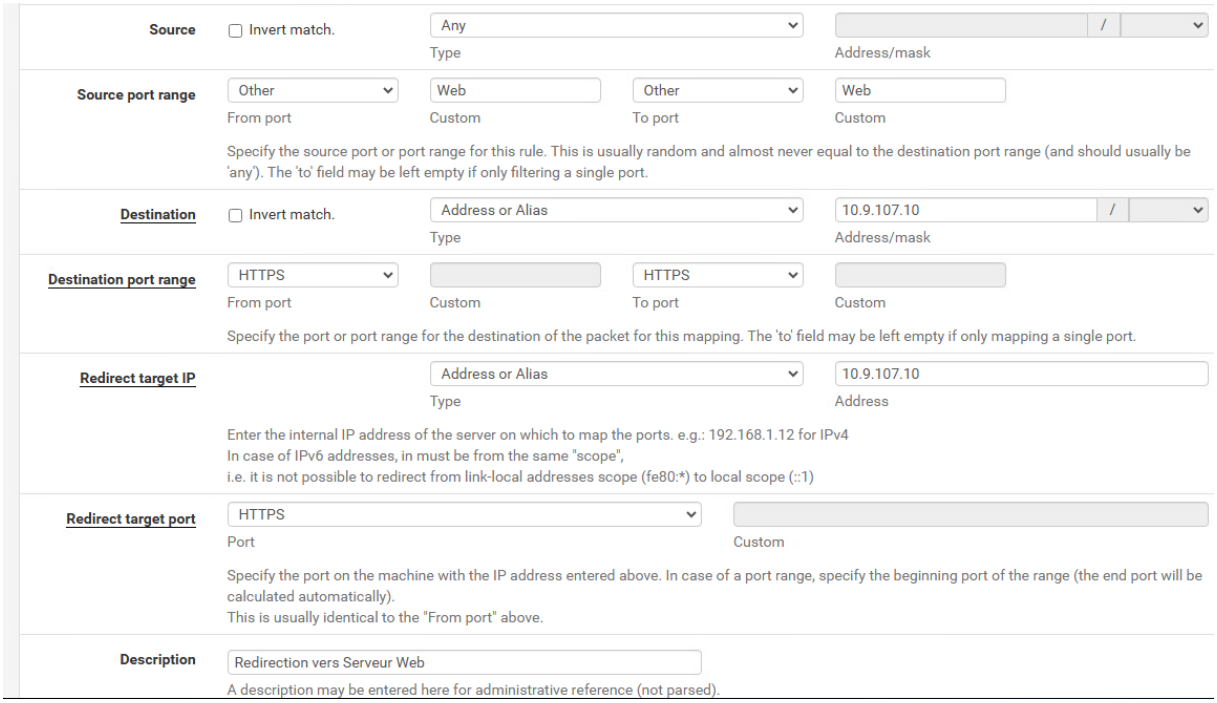

Firewall / Aliases / Edit
Properties
Name
Active_Directory
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description
Alias pour l'AD
A description may be entered here for administrative reference (not parsed).
Type
Host(s)
Host(s)
Hint
Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.
IP or FQDN
10.0.107.1
Serveur Active Directory (2019)
Delete
10.0.107.2
Serveur Redondant (2016)
Delete
Save
Add Host

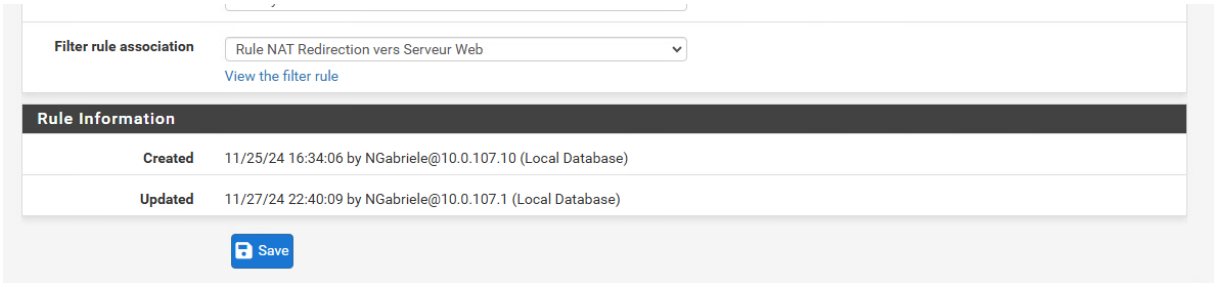


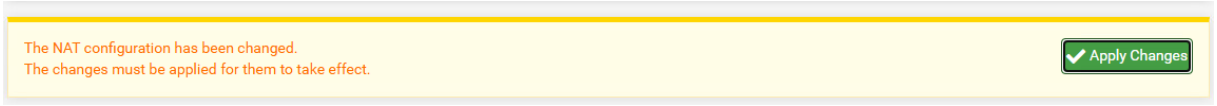
Configuration des transmission de ports

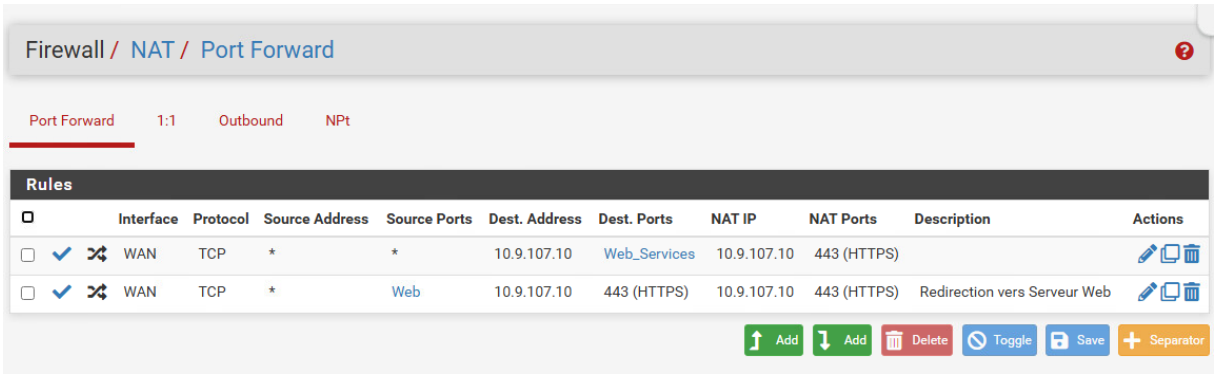






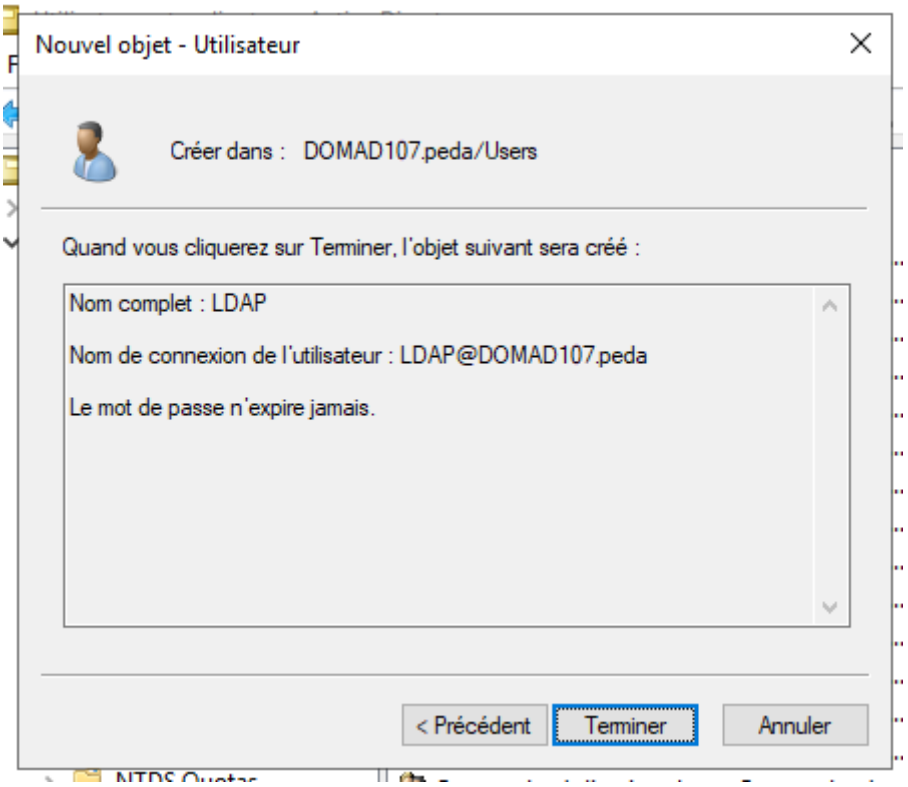


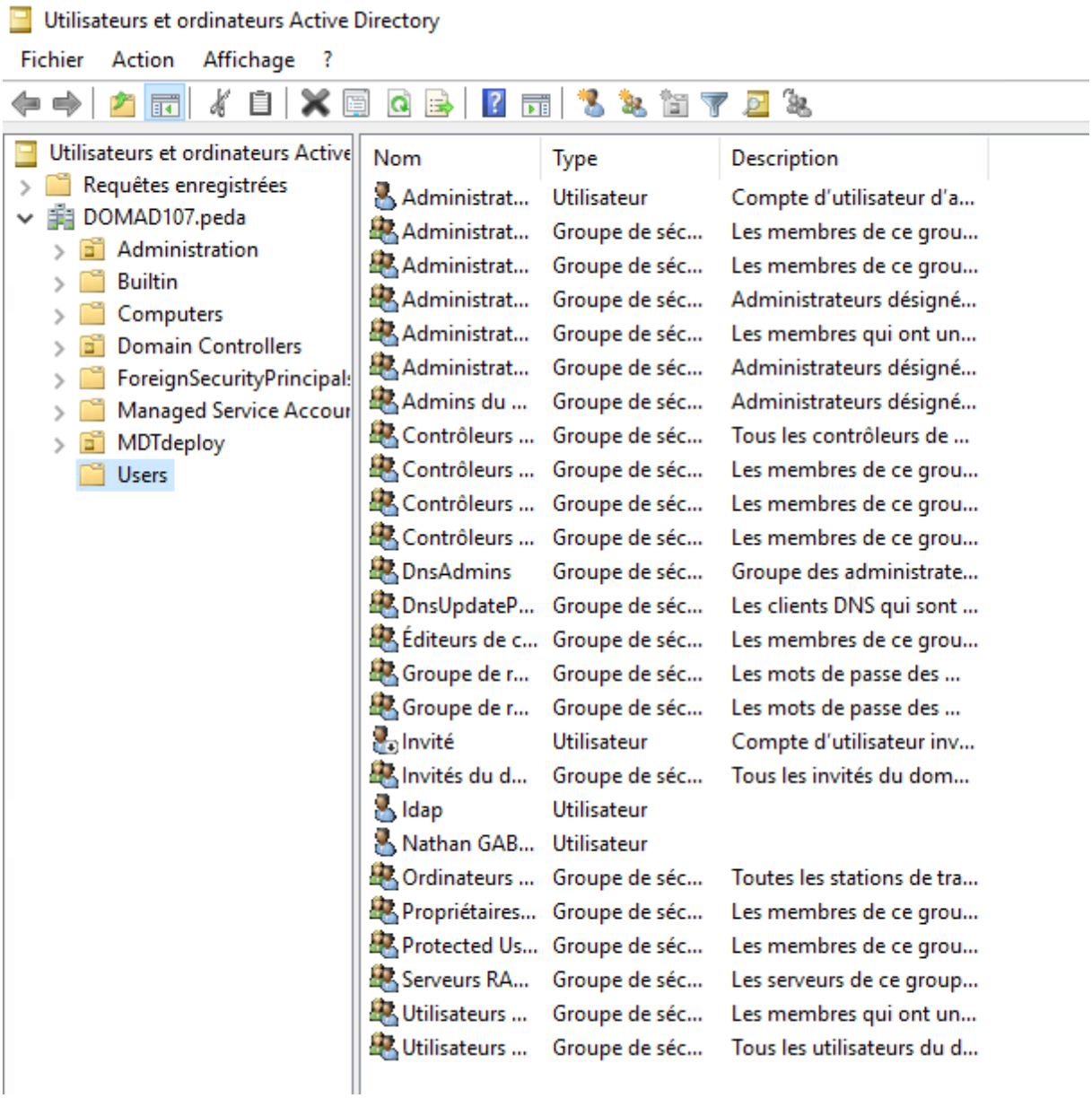


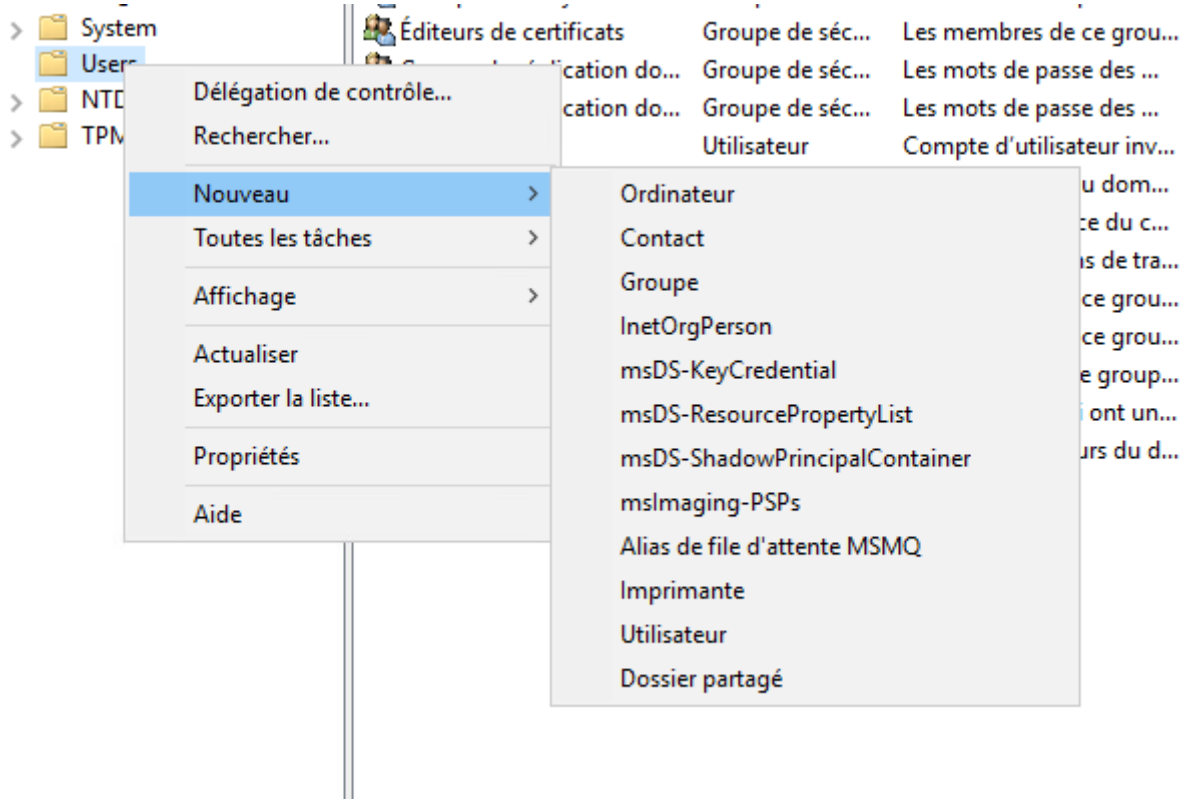


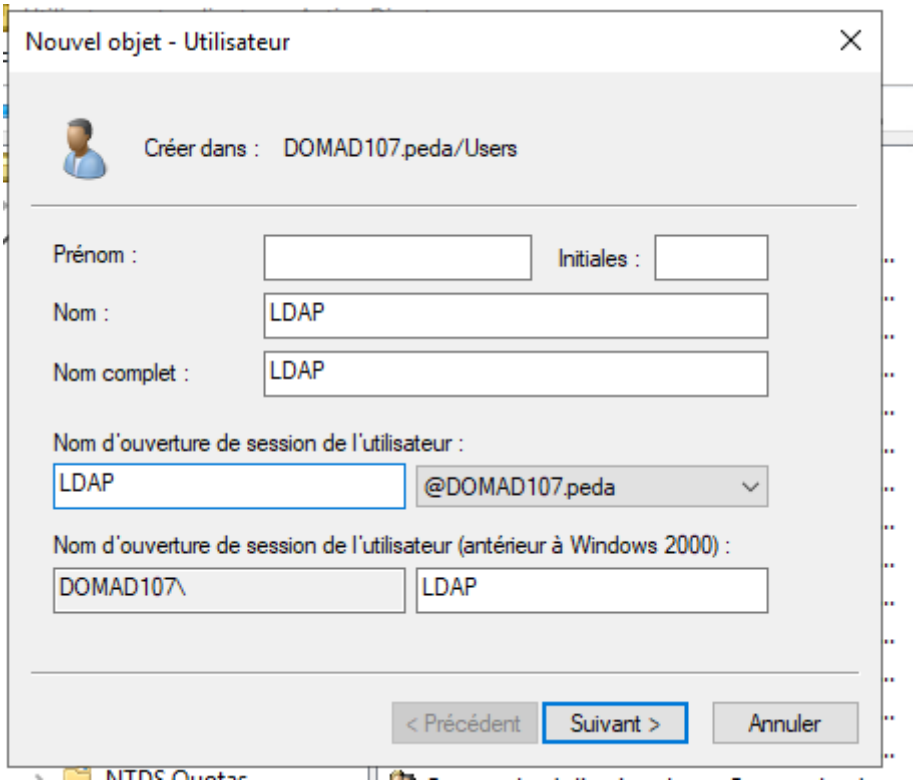
Configuration des services et applications tiers

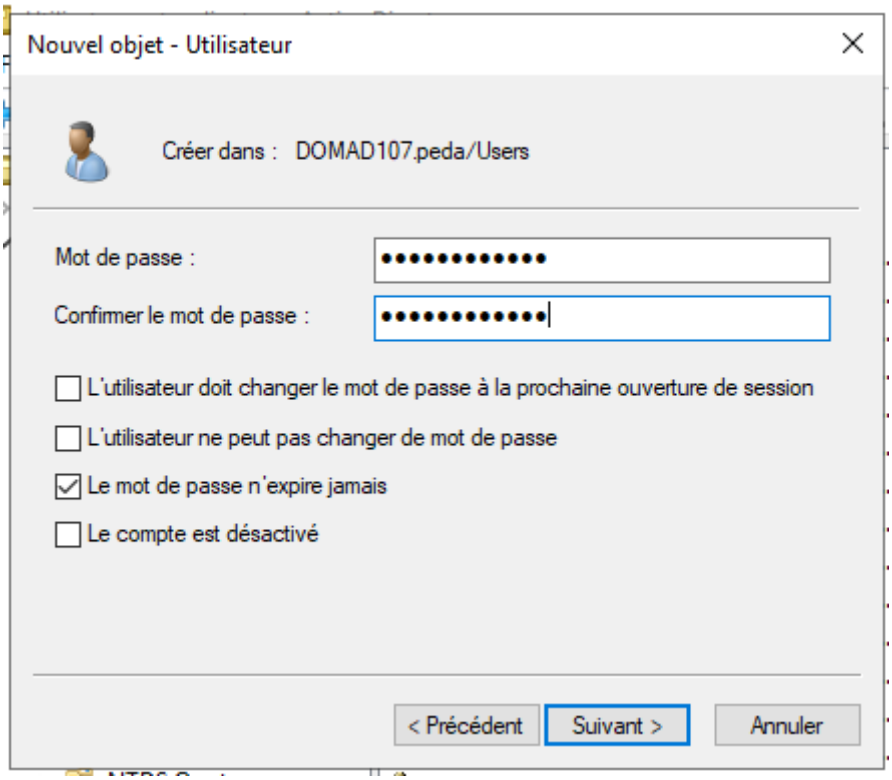
LDAP

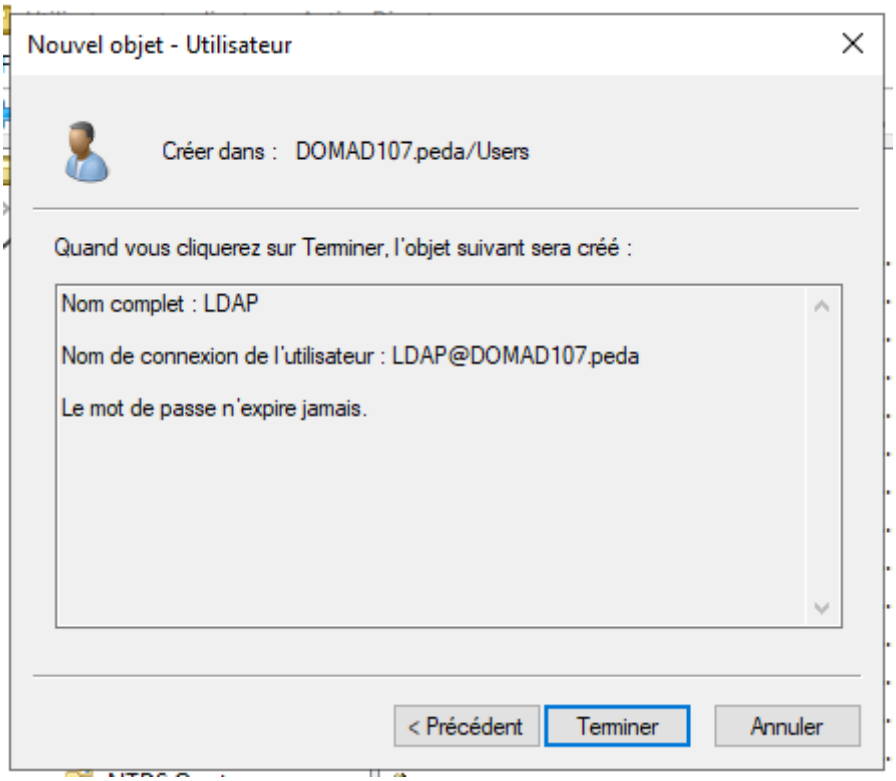

Nouvel objet - Utilisateur
Créer dans : DOMAD107.peda/Users
Quand vous cliquerez sur Terminer, l'objet suivant sera créé :
Nom complet : LDAP
Nom de connexion de l'utilisateur : LDAP@DOMAD107.peda
Le mot de passe n'expire jamais.
< Précédent
Terminer
Annuler

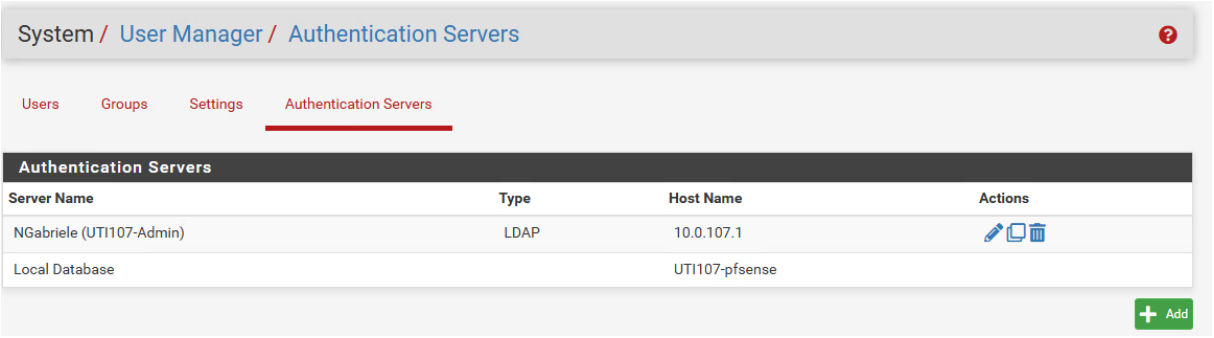

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
DOMAD107.peda
Administration
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
MDTdeploy
Users
Nom Type Description
Administrat... Utilisateur Compte d'utilisateur d'a...
Administrat... Groupe de séc... Les membres de ce grou...
Administrat... Groupe de séc... Les membres de ce grou...
Administrat... Groupe de séc... Administrateurs désigné...
Administrat... Groupe de séc... Les membres qui ont un...
Administrat... Groupe de séc... Administrateurs désigné...
Admins du ... Groupe de séc... Administrateurs désigné...
Contrôleurs ... Groupe de séc... Tous les contrôleurs de ...
Contrôleurs ... Groupe de séc... Les membres de ce grou...
Contrôleurs ... Groupe de séc... Les membres de ce grou...
Contrôleurs ... Groupe de séc... Les membres de ce grou...
DnsAdmins Groupe de séc... Groupe des administrate...
DnsUpdateP... Groupe de séc... Les clients DNS qui sont ...
Éditeurs de c... Groupe de séc... Les membres de ce grou...
Groupe de r... Groupe de séc... Les mots de passe des ...
Groupe de r... Groupe de séc... Les mots de passe des ...
Invité Utilisateur Compte d'utilisateur inv...
Invités du d... Groupe de séc... Tous les invités du dom...
ldap Utilisateur
Nathan GAB... Utilisateur
Ordinateurs ... Groupe de séc... Toutes les stations de tra...
Propriétaires... Groupe de séc... Les membres de ce grou...
Protected Us... Groupe de séc... Les membres de ce grou...
Serveurs RA... Groupe de séc... Les serveurs de ce group...
Utilisateurs ... Groupe de séc... Les membres qui ont un...
Utilisateurs ... Groupe de séc... Tous les utilisateurs du d...


System
Users
NTDS Quotas
TPM
Éditeurs de certificats
Groupe de séc...
Les membres de ce grou...
Groupe de séc...
Les mots de passe des ...
Groupe de séc...
Les mots de passe des ...
Utilisateur
Compte d'utilisateur inv...
Délégation de contrôle...
Rechercher...
Nouveau
Toutes les tâches
Affichage
Actualiser
Exporter la liste...
Propriétés
Aide
Ordinateur
Contact
Groupe
InetOrgPerson
msDS-KeyCredential
msDS-ResourcePropertyList
msDS-ShadowPrincipalContainer
msImaging-PSPs
Alias de file d'attente MSMQ
Imprimante
Utilisateur
Dossier partagé


Nouvel objet - Utilisateur
Créer dans : DOMAD107.peda/Users
Prénom :
Initiales :
Nom :
LDAP
Nom complet :
LDAP
Nom d'ouverture de session de l'utilisateur :
LDAP
@DOMAD107.peda
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
DOMAD107\
LDAP
< Précédent
Suivant >
Annuler


Nouvel objet - Utilisateur
Créer dans : DOMAD107.peda/Users
Mot de passe :
Confirmer le mot de passe :
L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
L'utilisateur ne peut pas changer de mot de passe
Le mot de passe n'expire jamais
Le compte est désactivé
< Précédent
Suivant >
Annuler

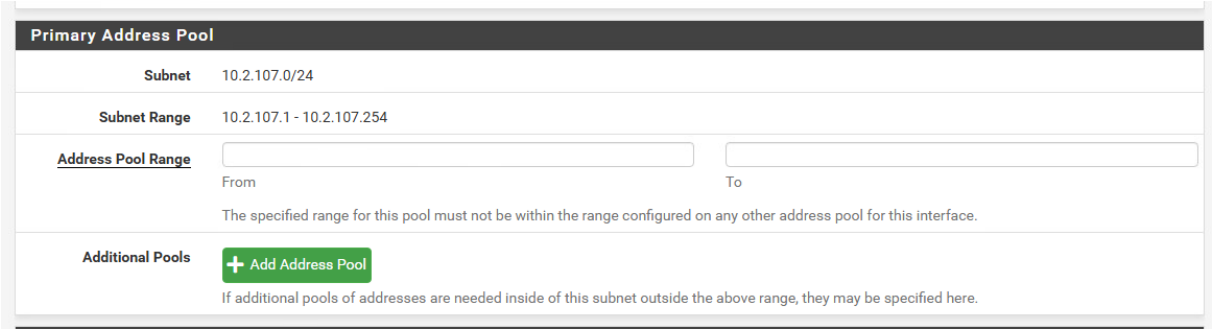

Nouvel objet - Utilisateur
Créer dans : DOMAD107.peda/Users
Quand vous cliquerez sur Terminer, l'objet suivant sera créé :
Nom complet : LDAP
Nom de connexion de l'utilisateur : LDAP@DOMAD107.peda
Le mot de passe n'expire jamais.
< Précédent
Terminer
Annuler



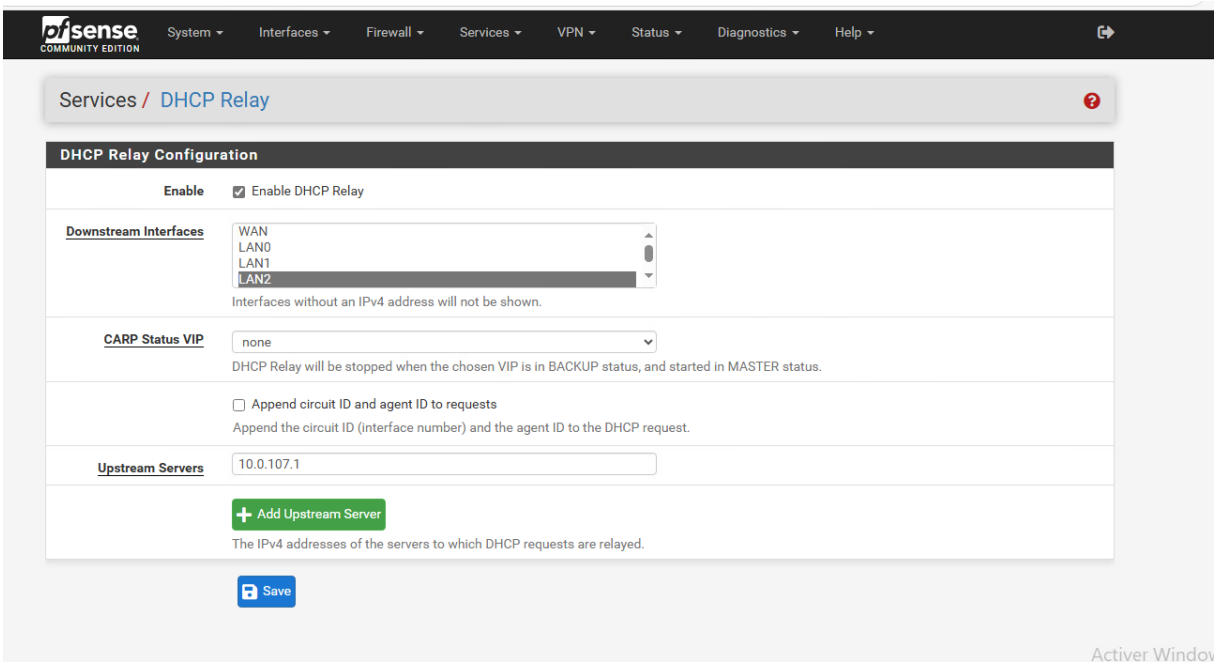
Création et configuration de la machine cliente

SNMP

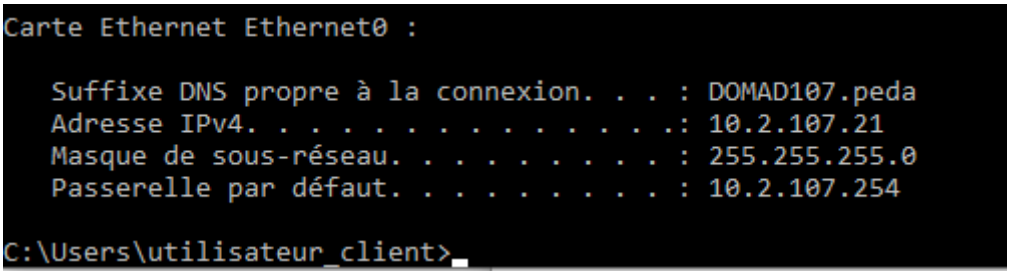
DHCP



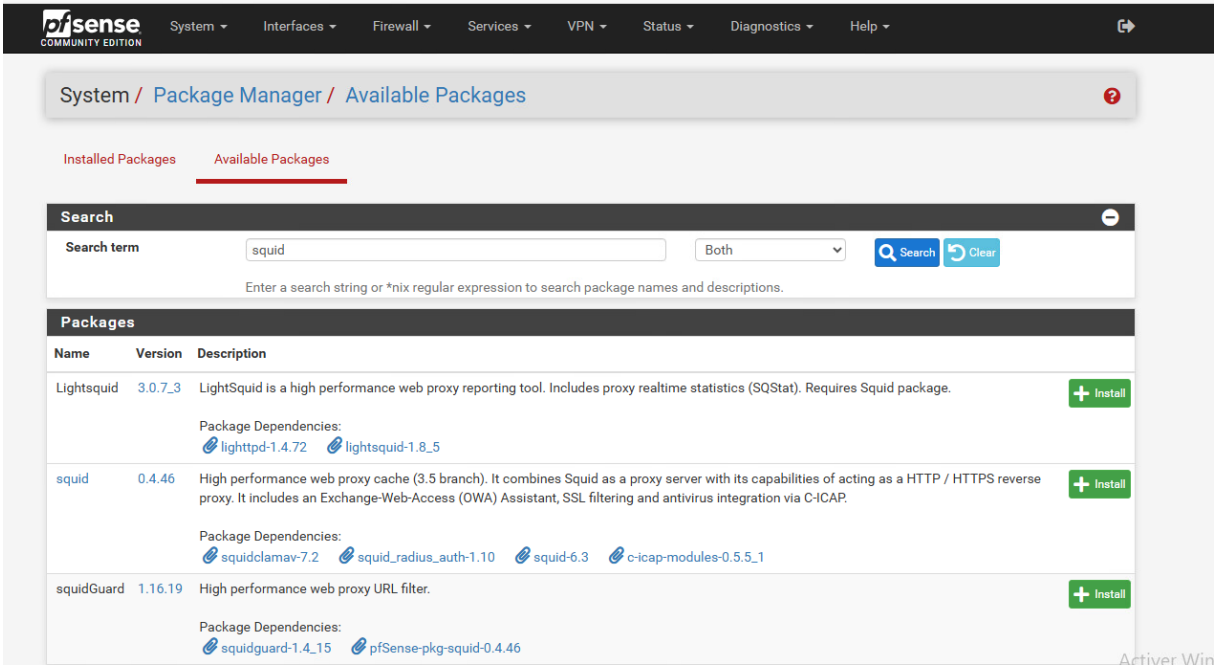
DHCP Relay

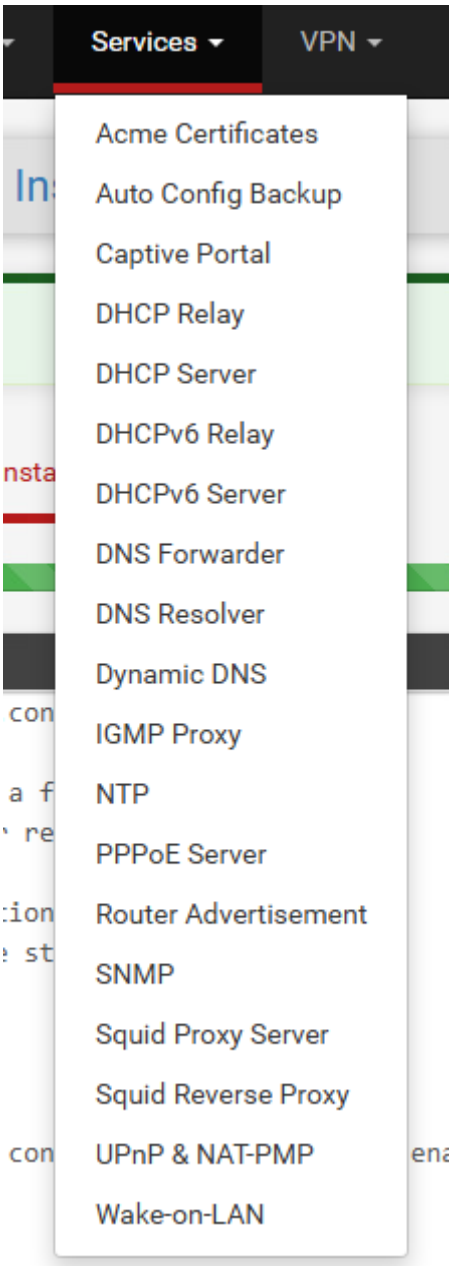


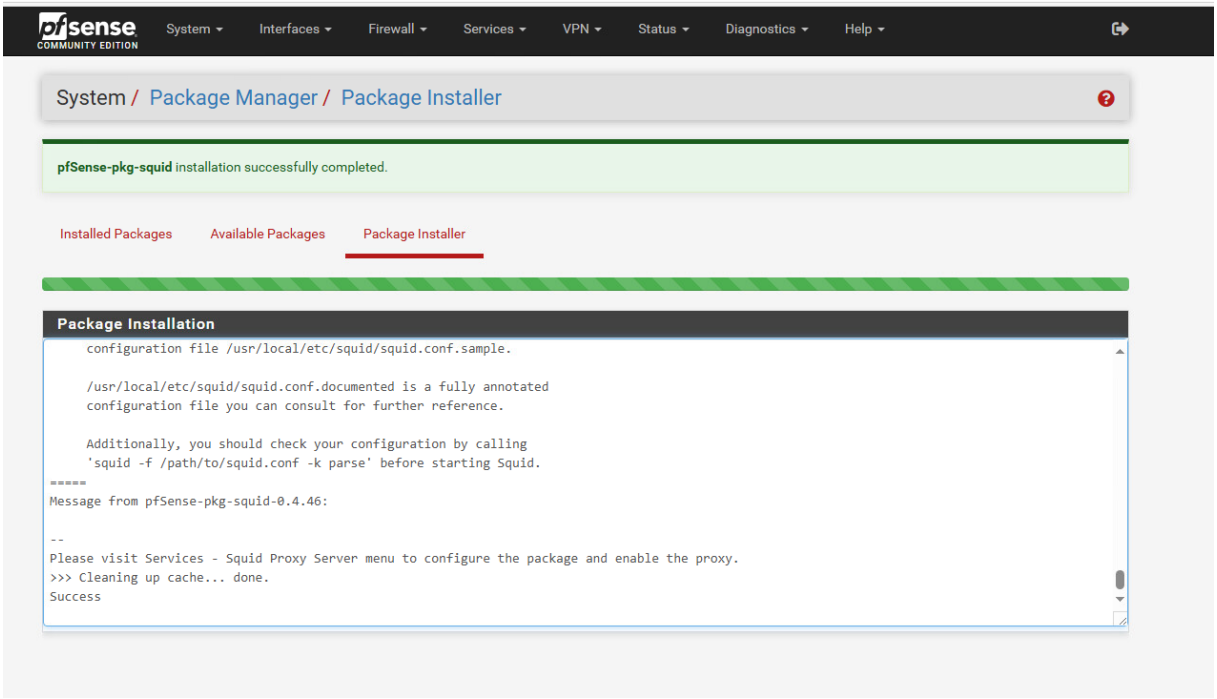
Configuration du poste client sous windows 10 en DHCP

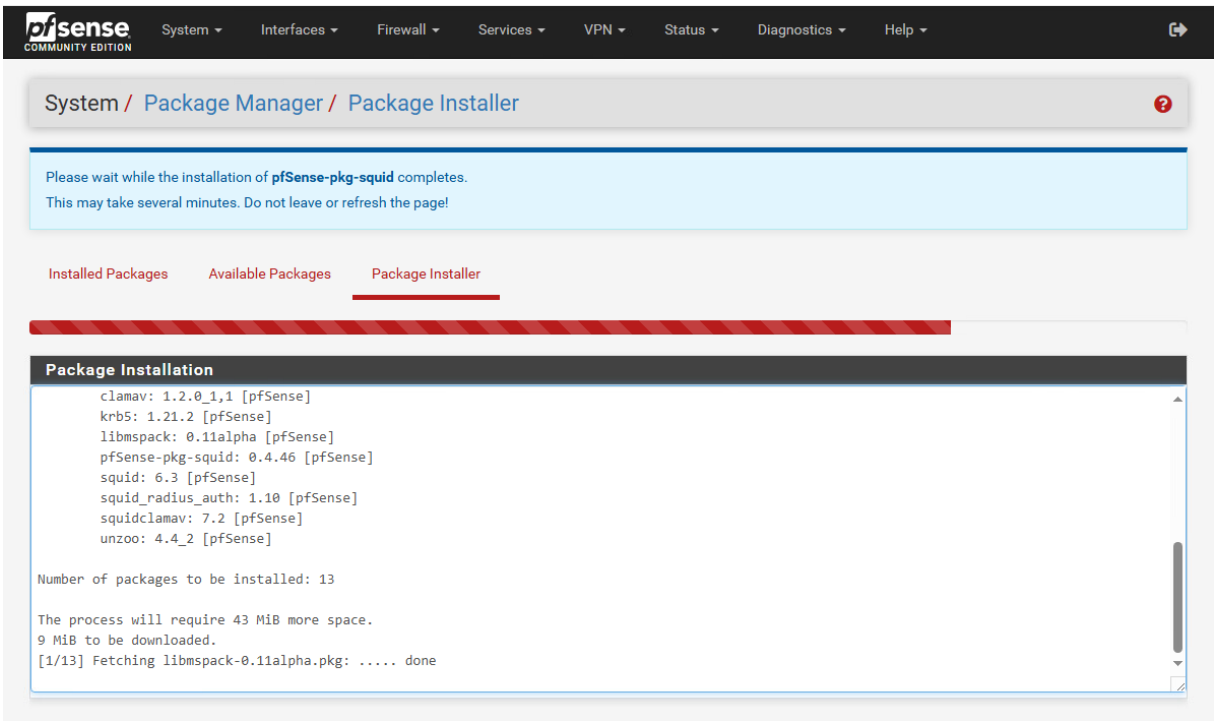


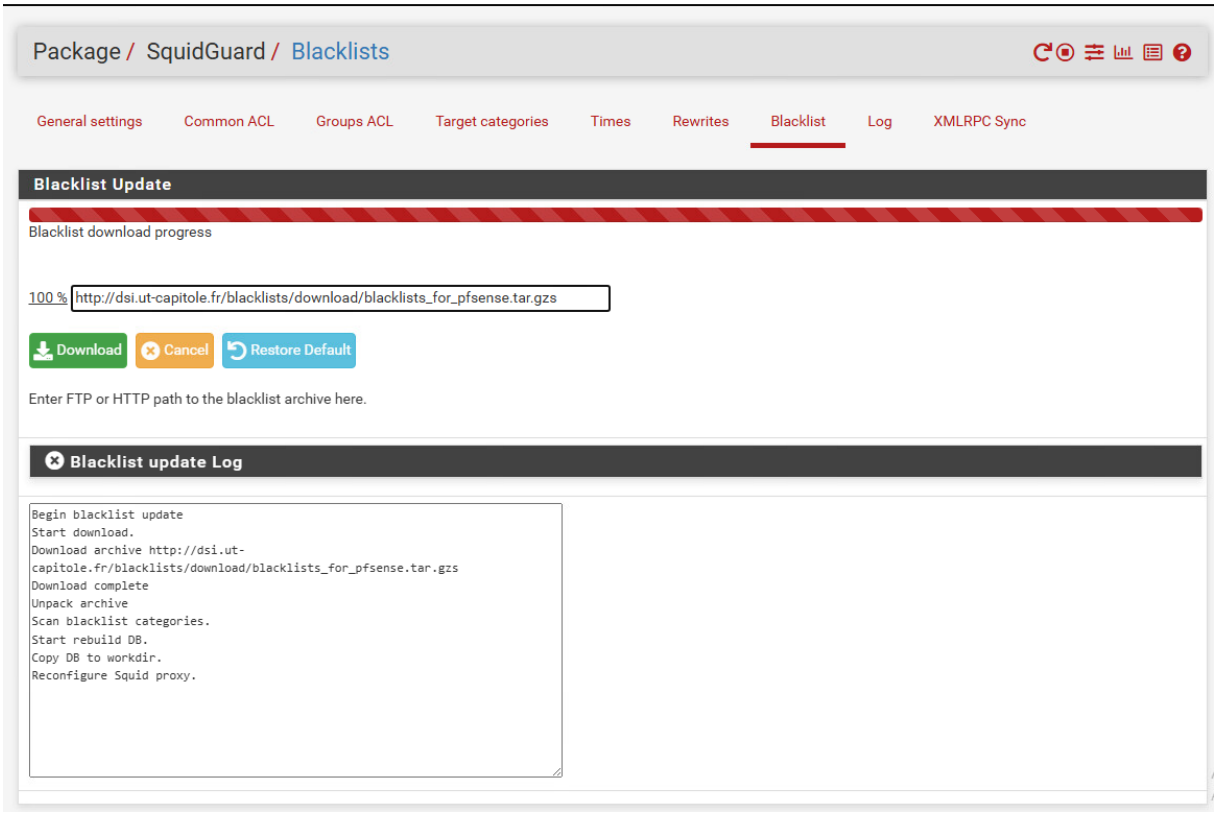
Mise en place du proxy SquidGuard sur le LAN2

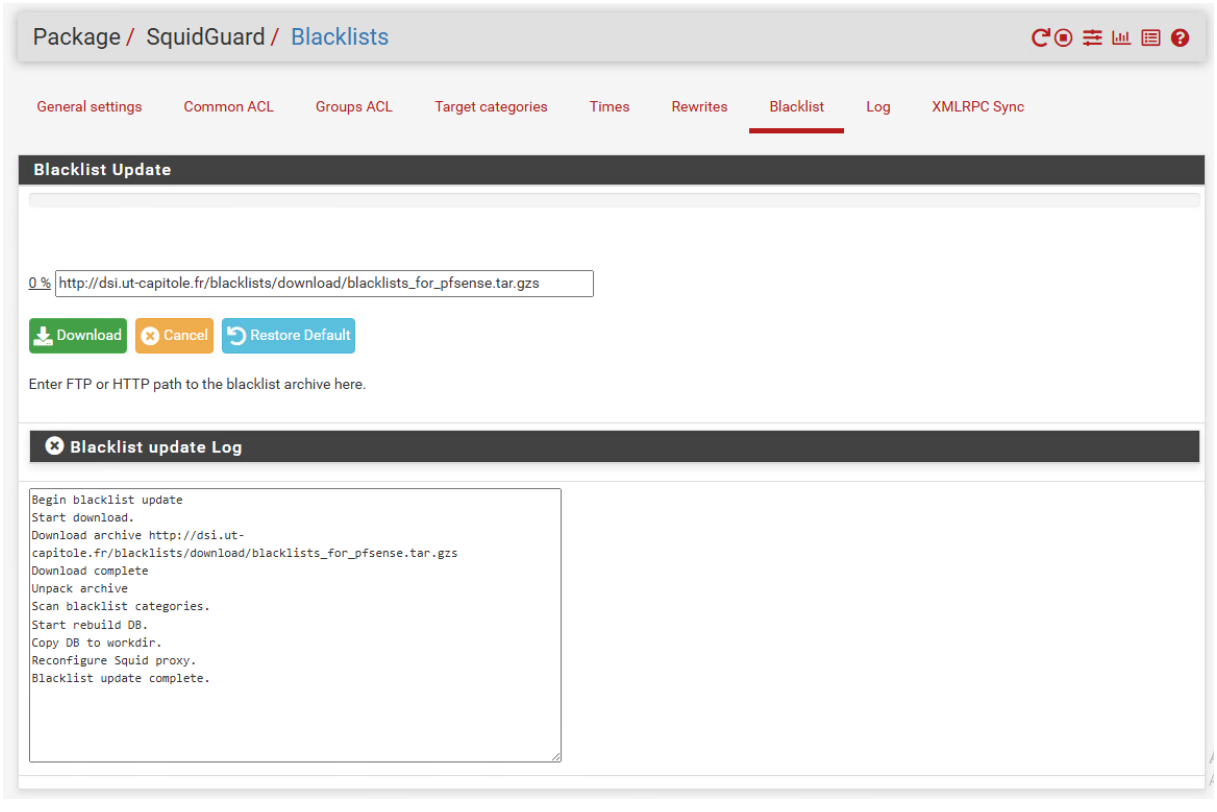


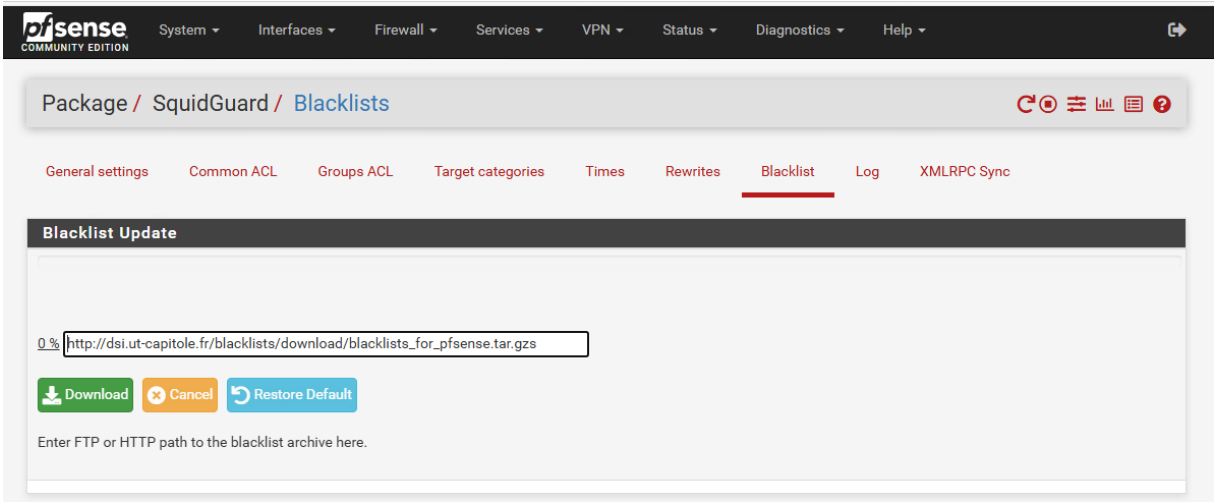

Services
VPN
Acme Certificates
Auto Config Backup
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server
DNS Forwarder
DNS Resolver
Dynamic DNS
IGMP Proxy
NTP
PPPoE Server
Router Advertisement
SNMP
Squid Proxy Server
Squid Reverse Proxy
UPnP & NAT-PMP
Wake-on-LAN

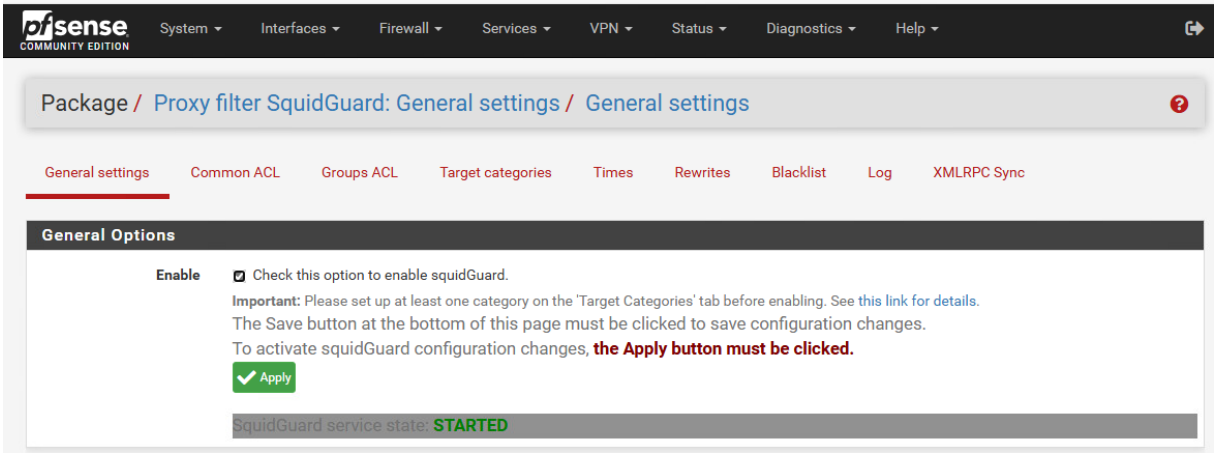

pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
System / Package Manager / Package Installer
pfSense-pkg-squid installation successfully completed.
Installed Packages
Available Packages
Package Installer
Package Installation
configuration file /usr/local/etc/squid/squid.conf.sample.
/usr/local/etc/squid/squid.conf.documented is a fully annotated
configuration file you can consult for further reference.
Additionally, you should check your configuration by calling
'squid -f /path/to/squid.conf -k parse' before starting Squid.
=====
Message from pfSense-pkg-squid-0.4.46:
--
Please visit Services - Squid Proxy Server menu to configure the package and enable the proxy.
>>> Cleaning up cache... done.
Success

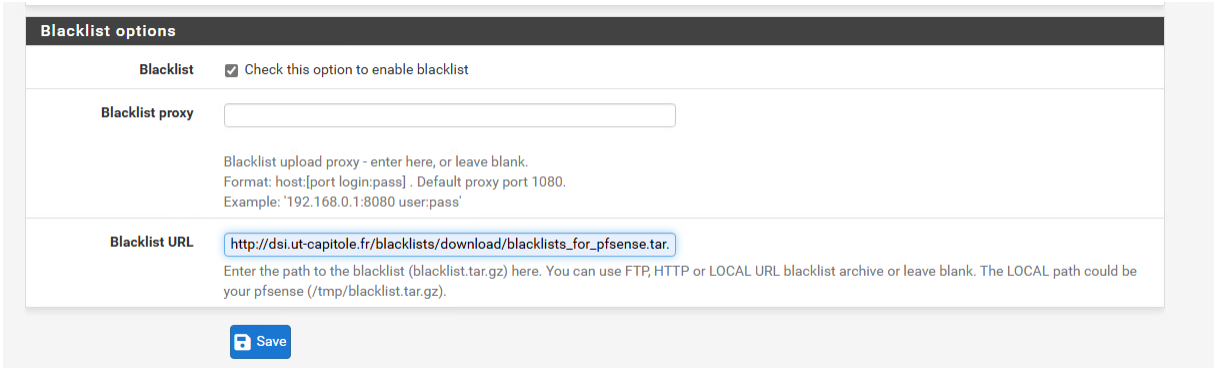

pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
System / Package Manager / Package Installer
Please wait while the installation of pfSense-pkg-squid completes.
This may take several minutes. Do not leave or refresh the page!
Installed Packages
Available Packages
Package Installer
Package Installation
clamav: 1.2.0_1,1 [pfSense]
krb5: 1.21.2 [pfSense]
libmspack: 0.11alpha [pfSense]
pfSense-pkg-squid: 0.4.46 [pfSense]
squid: 6.3 [pfSense]
squid_radius_auth: 1.10 [pfSense]
squidclamav: 7.2 [pfSense]
unzoo: 4.4_2 [pfSense]
Number of packages to be installed: 13
The process will require 43 MiB more space.
9 MiB to be downloaded.
[1/13] Fetching libmspack-0.11alpha.pkg: ..... done

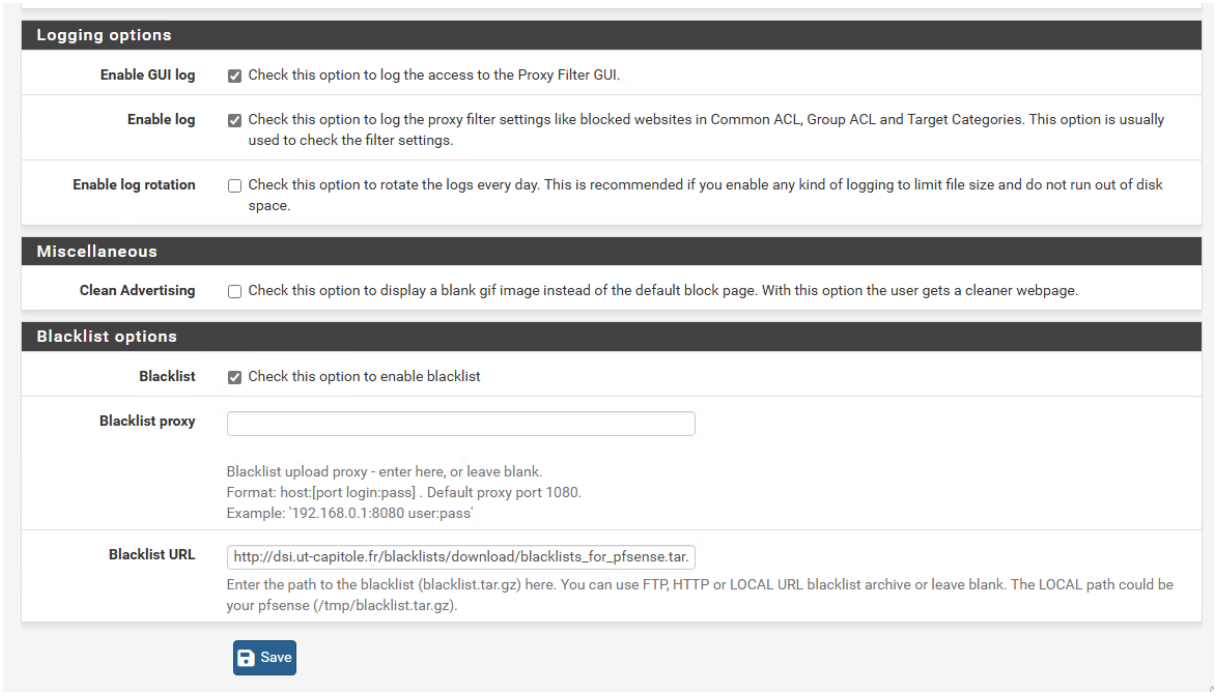

Package / SquidGuard / Blacklists
General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync
Blacklist Update
Blacklist download progress
100 %
http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gzs
Download
Cancel
Restore Default
Enter FTP or HTTP path to the blacklist archive here.
Blacklist update Log
Begin blacklist update
Start download.
Download archive http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gzs
Download complete
Unpack archive
Scan blacklist categories.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.

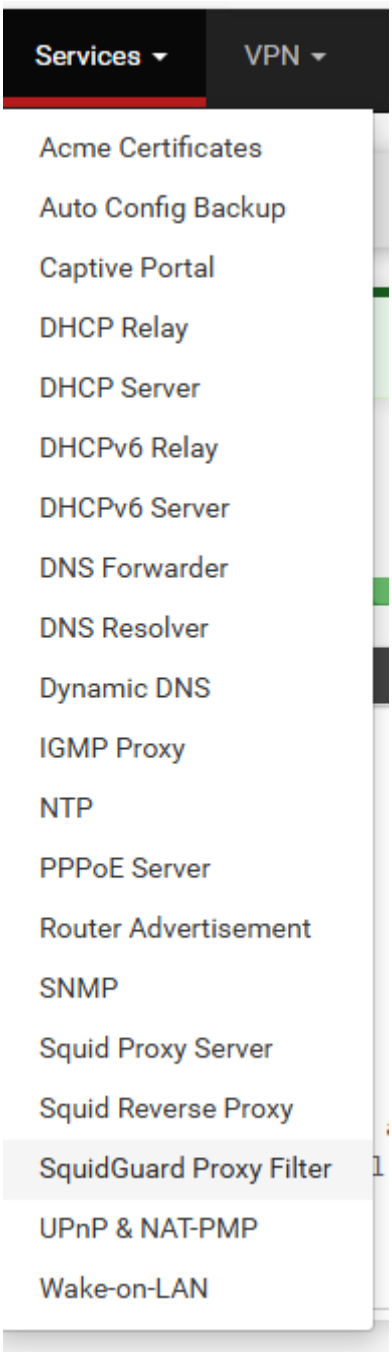

Package / SquidGuard / Blacklists
General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync
Blacklist Update
0 %
http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gzs
Download
Cancel
Restore Default
Enter FTP or HTTP path to the blacklist archive here.
Blacklist update Log
Begin blacklist update
Start download.
Download archive http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gzs
Download complete
Unpack archive
Scan blacklist categories.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Package / SquidGuard / Blacklists
General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync
Blacklist Update
0 %
http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gzs
Download
Cancel
Restore Default
Enter FTP or HTTP path to the blacklist archive here.

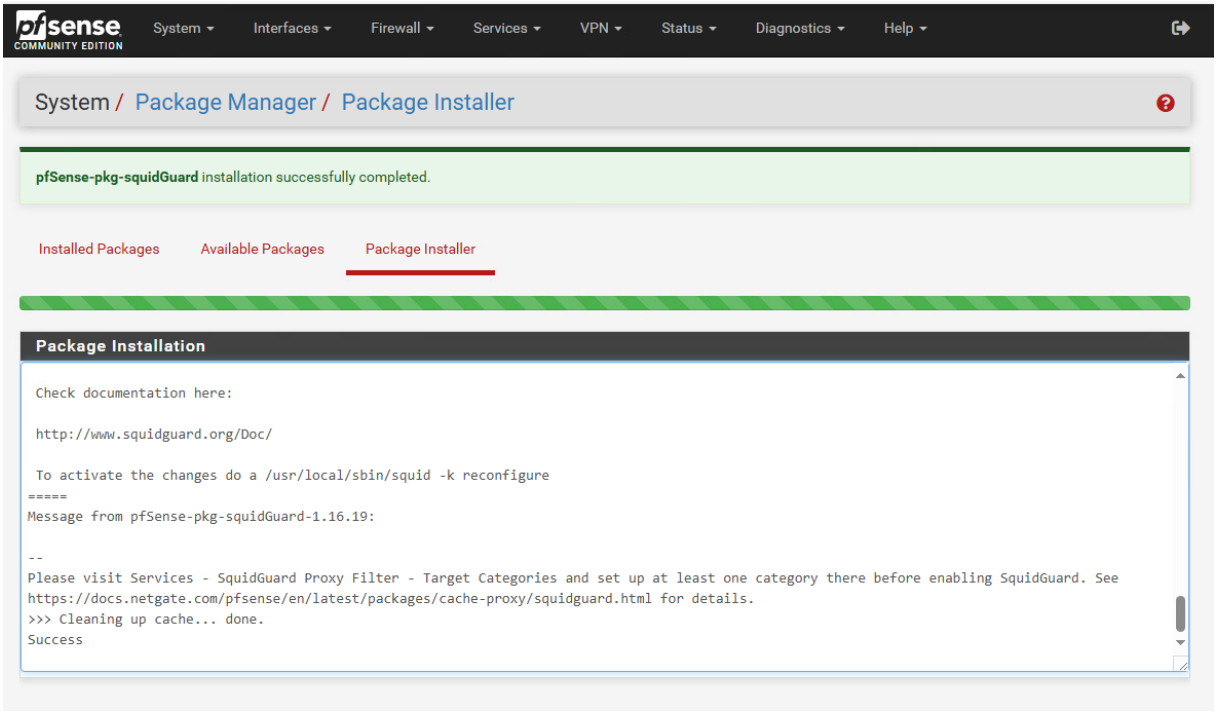

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Package / Proxy filter SquidGuard: General settings / General settings
General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync
General Options
Enable
Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details.
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, the Apply button must be clicked.
Apply
SquidGuard service state: STARTED

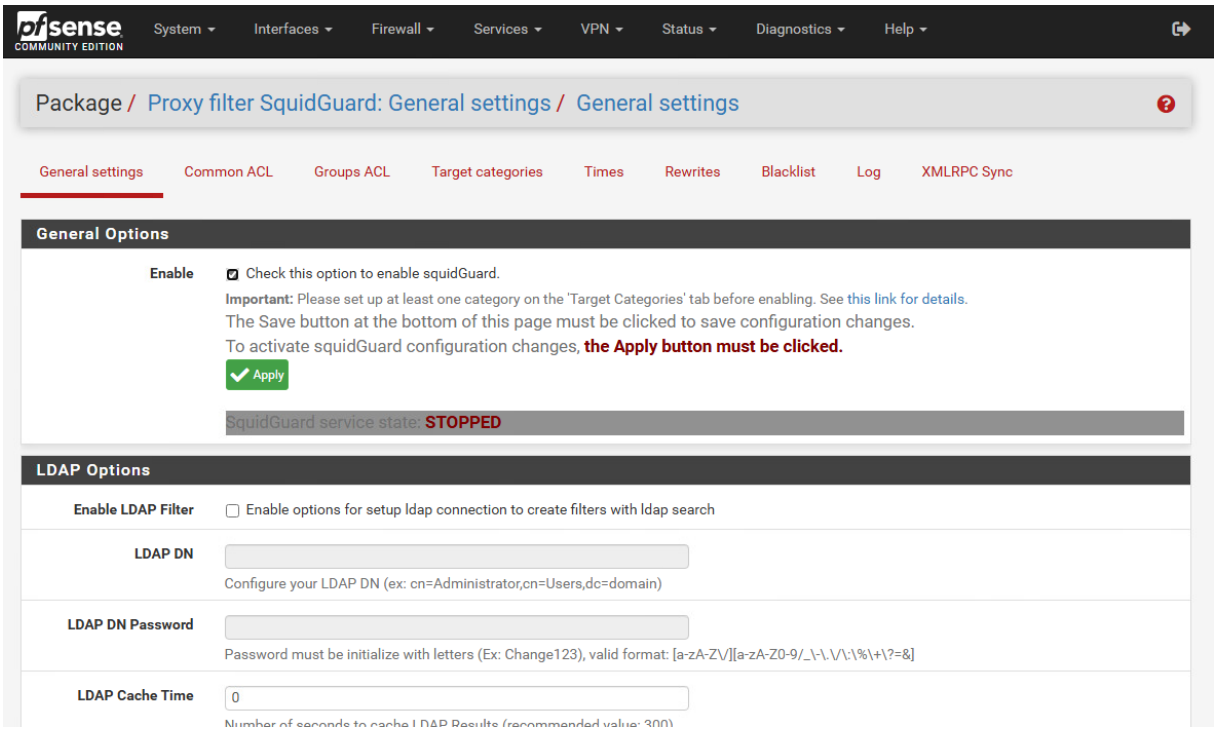

Blacklist options
Blacklist
Check this option to enable blacklist
Blacklist proxy
Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'
Blacklist URL
http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.
Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).
Save


Logging options
Enable GUI log
Check this option to log the access to the Proxy Filter GUI.
Enable log
Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.
Enable log rotation
Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.
Miscellaneous
Clean Advertising
Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.
Blacklist options
Blacklist
Check this option to enable blacklist
Blacklist proxy
Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'
Blacklist URL
http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.
Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).
Save


Services
VPN
Acme Certificates
Auto Config Backup
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server
DNS Forwarder
DNS Resolver
Dynamic DNS
IGMP Proxy
NTP
PPPoE Server
Router Advertisement
SNMP
Squid Proxy Server
Squid Reverse Proxy
SquidGuard Proxy Filter
UPnP & NAT-PMP
Wake-on-LAN

SquidGuard


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
System / Package Manager / Package Installer
pfSense-pkg-squidGuard installation successfully completed.
Installed Packages
Available Packages
Package Installer
Package Installation
Check documentation here:
http://www.squidguard.org/Doc/
To activate the changes do a /usr/local/sbin/squid -k reconfigure
=====
Message from pfSense-pkg-squidGuard-1.16.19:
--
Please visit Services - SquidGuard Proxy Filter - Target Categories and set up at least one category there before enabling SquidGuard. See
https://docs.netgate.com/pfsense/en/latest/packages/cache-proxy/squidguard.html for details.
>>> Cleaning up cache... done.
Success


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Package / Proxy filter SquidGuard: General settings / General settings
General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync
General Options
Enable
Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details.
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, the Apply button must be clicked.
Apply
SquidGuard service state: STOPPED
LDAP Options
Enable LDAP Filter
Enable options for setup ldap connection to create filters with ldap search
LDAP DN
Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)
LDAP DN Password
Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z\/][a-zA-Z0-9/_\-\.\/\:\%\+\?=&]
LDAP Cache Time
0

Put each entry on a separate line.

Whitelist

Destination domains that will be accessible to the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.

Blacklist

impots.gouv.fr

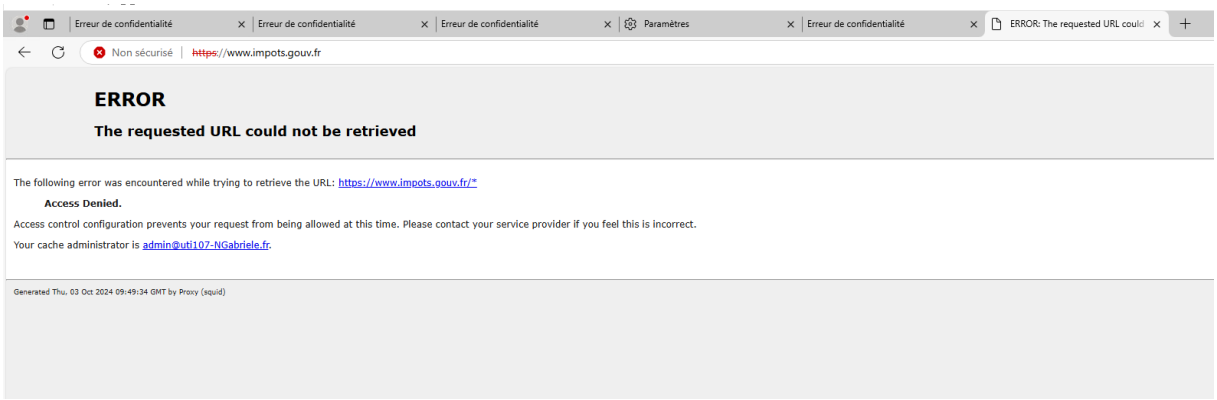
Destination domains that will be blocked for the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.

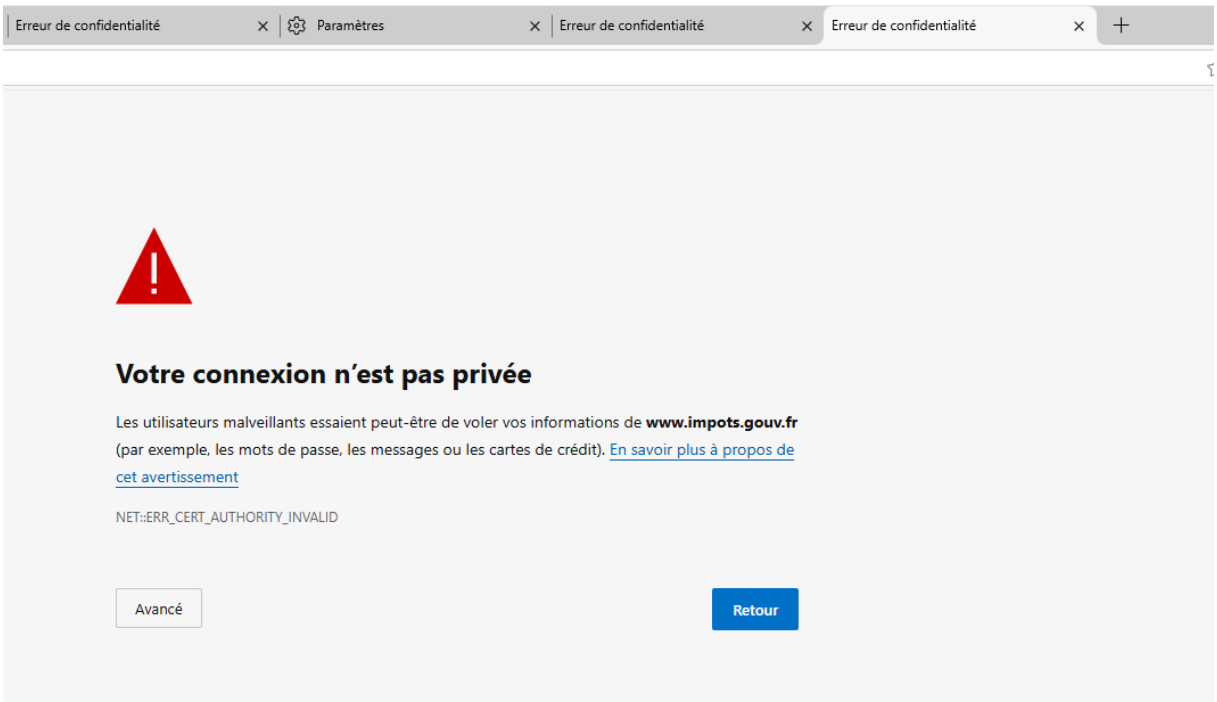
Block User Agents

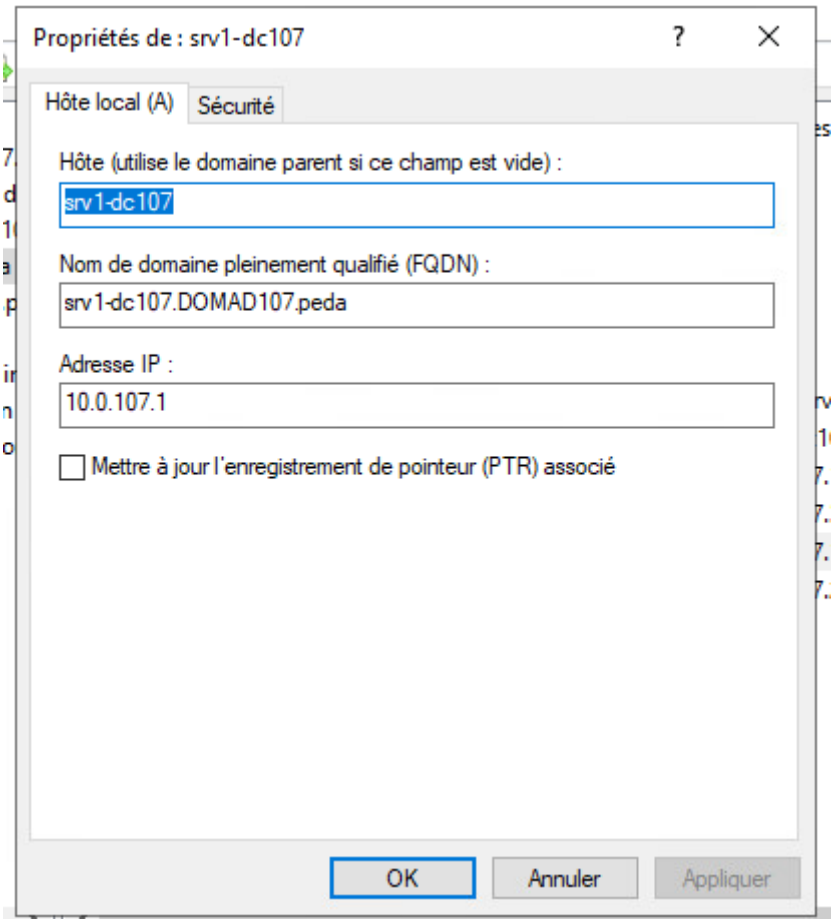
Enter user agents that will be blocked for the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.

Block MIME Types (Reply Only)

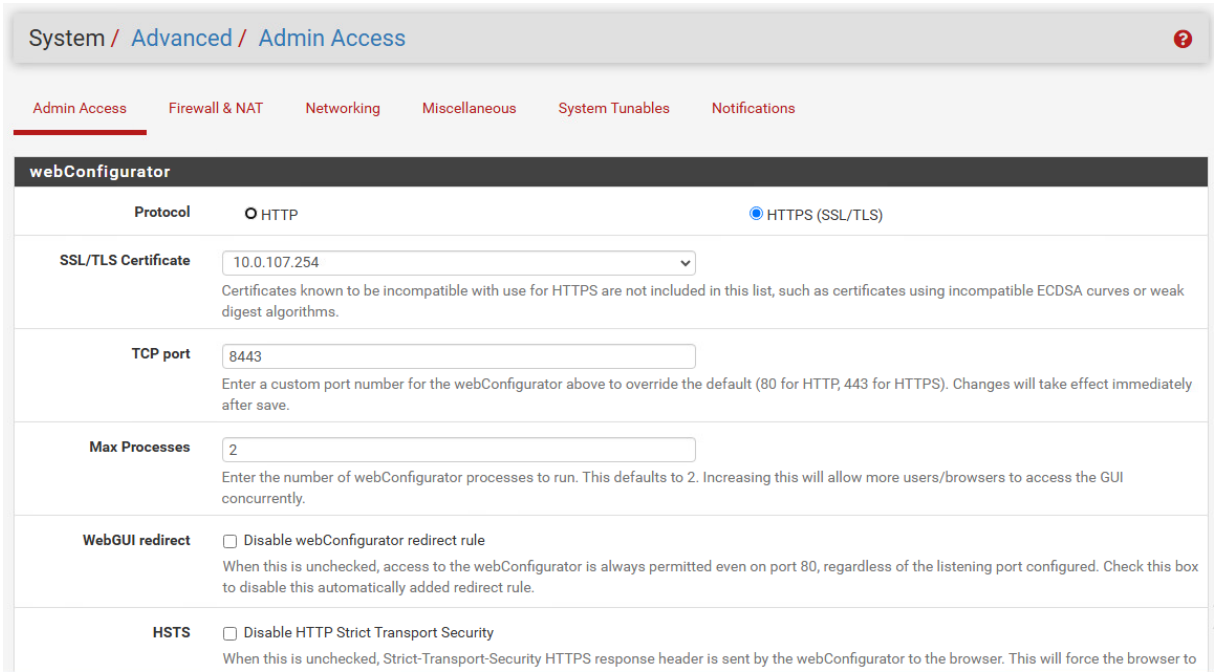
Enter MIME types that will be blocked for the users that are allowed to use the proxy. Useful to block javascript (application/javascript).
Put each entry on a separate line. You can also use regular expressions.

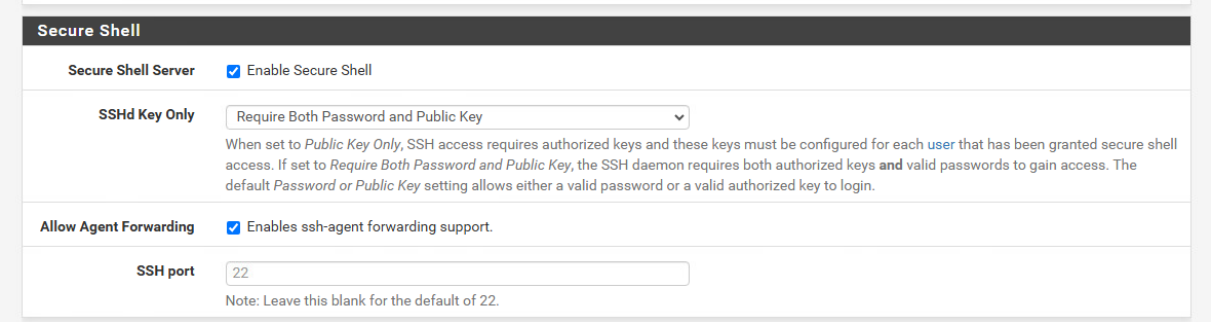


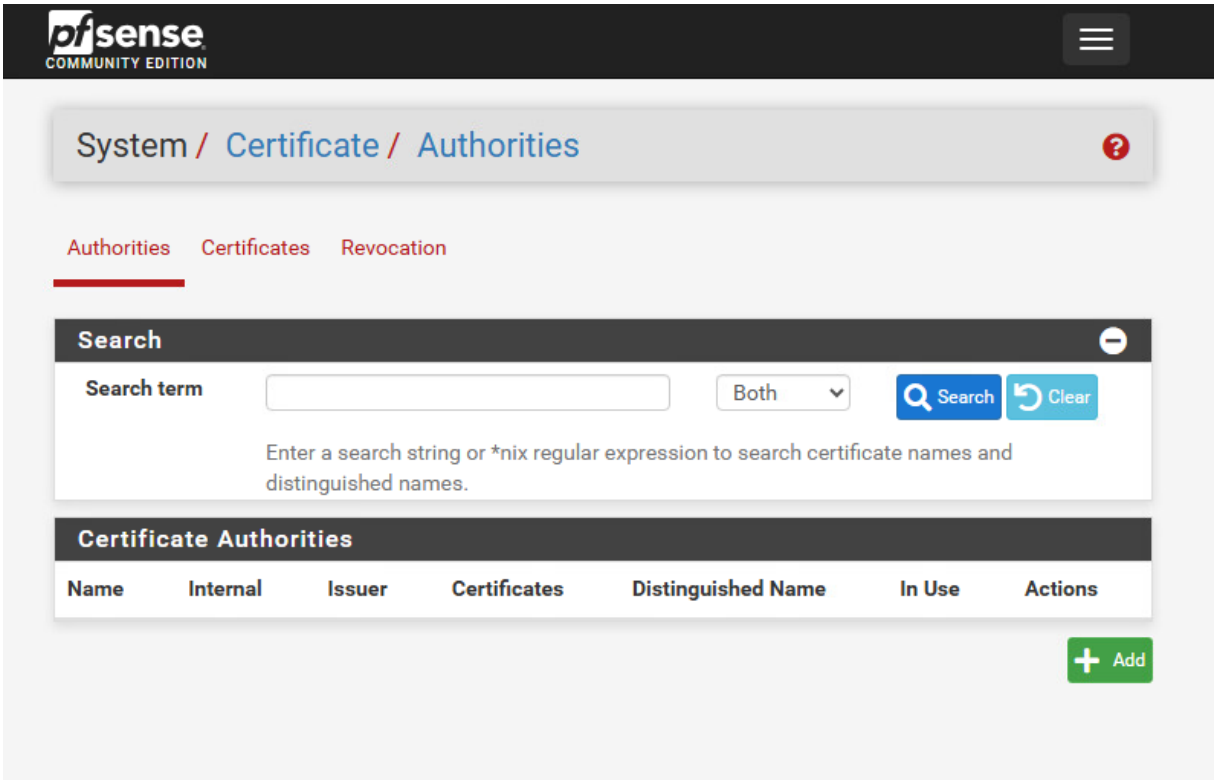


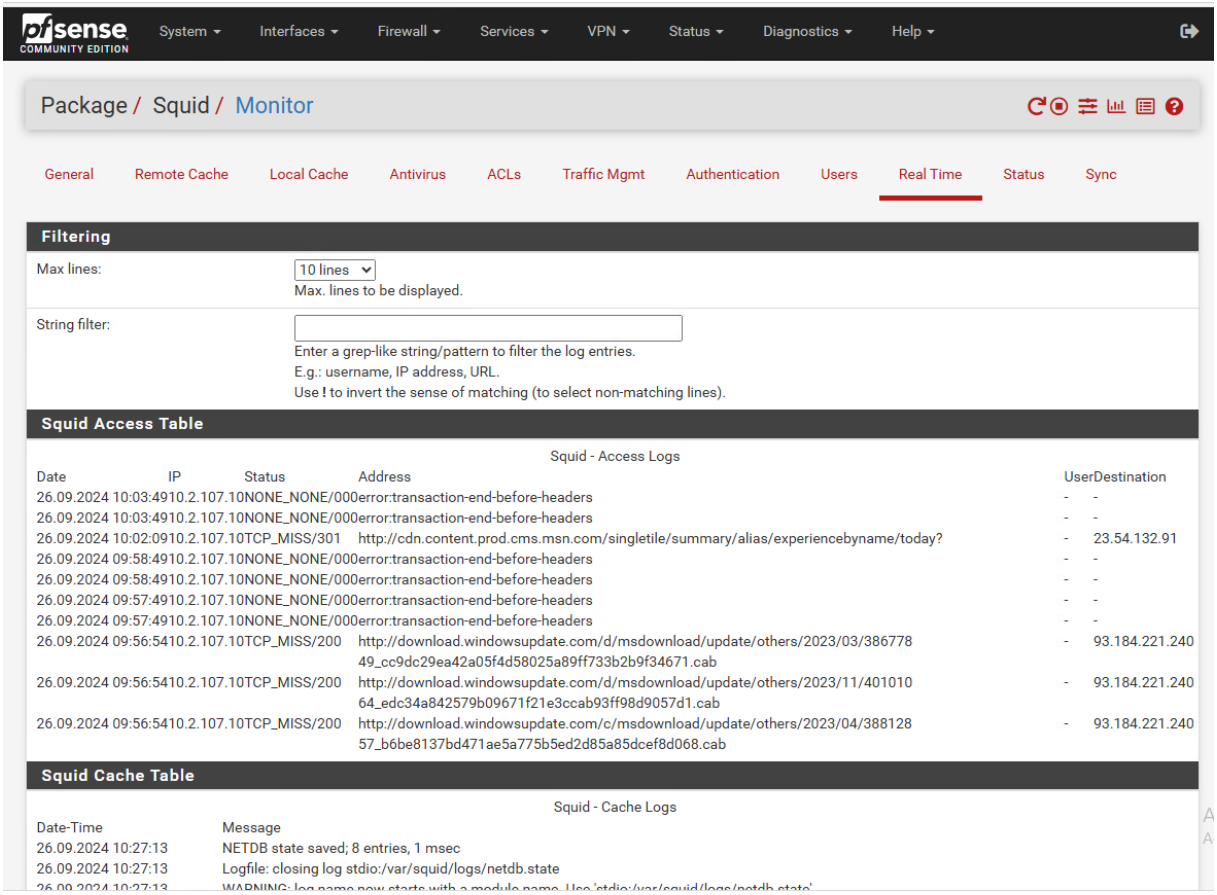


Certificats

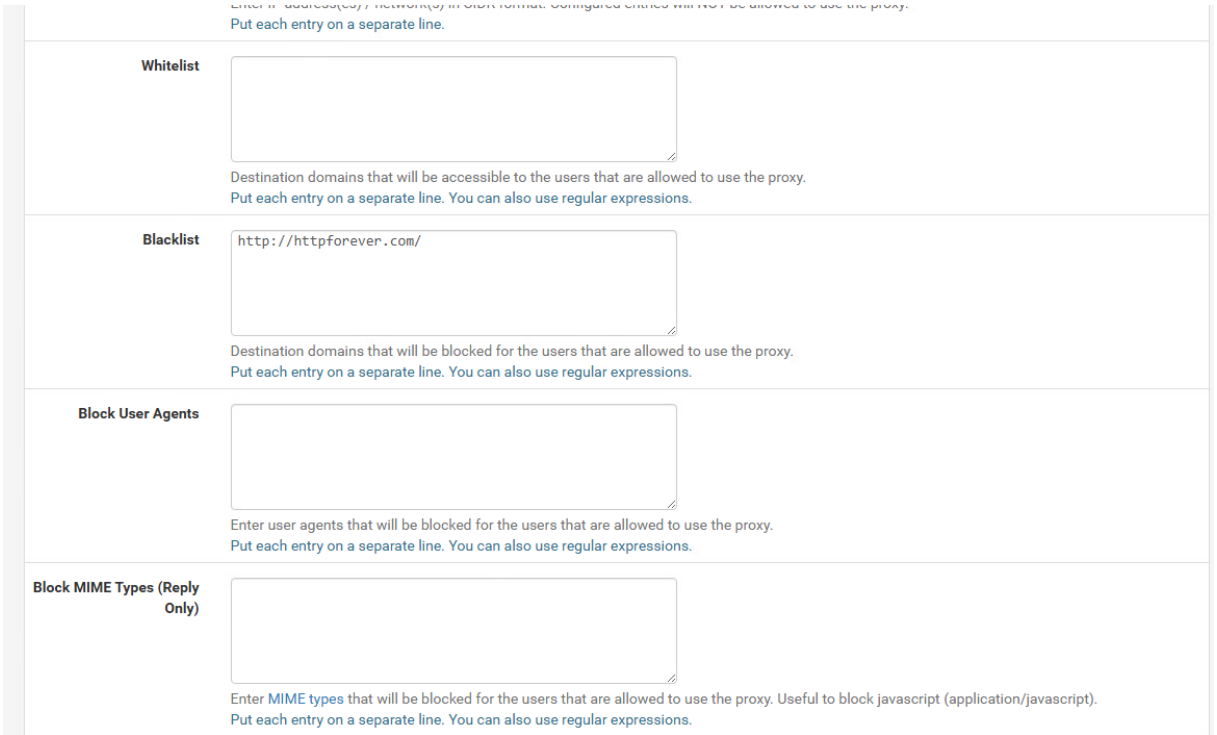


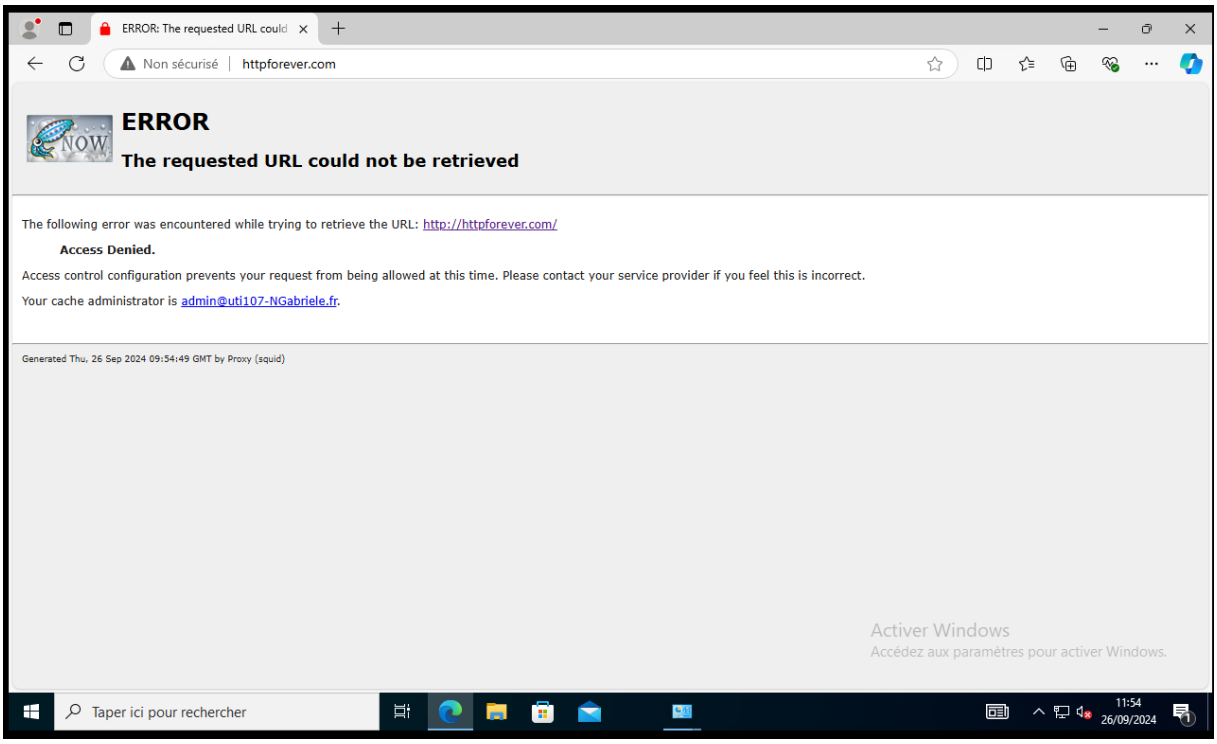

Secure Shell
Secure Shell Server
Enable Secure Shell
SSHd Key Only
Require Both Password and Public Key
When set to Public Key Only, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to Require Both Password and Public Key, the SSH daemon requires both authorized keys and valid passwords to gain access. The default Password or Public Key setting allows either a valid password or a valid authorized key to login.
Allow Agent Forwarding
Enables ssh-agent forwarding support.
SSH port
22
Note: Leave this blank for the default of 22.


pfsense
COMMUNITY EDITION
System / Certificate / Authorities
Authorities
Certificates
Revocation
Search
Search term
Both
Search
Clear
Enter a search string or *nix regular expression to search certificate names and distinguished names.
Certificate Authorities
Name
Internal
Issuer
Certificates
Distinguished Name
In Use
Actions
Add

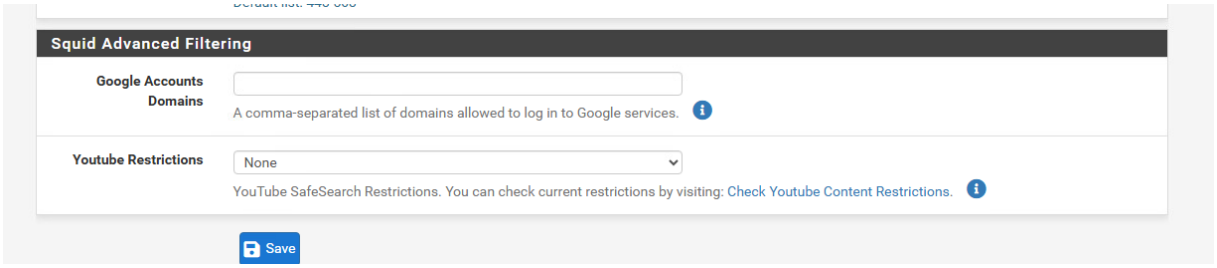

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Package / Squid / Monitor
General
Remote Cache
Local Cache
Antivirus
ACLs
Traffic Mgmt
Authentication
Users
Real Time
Status
Sync
Filtering
Max lines:
10 lines
Max. lines to be displayed.
String filter:
Enter a grep-like string/pattern to filter the log entries.
E.g.: username, IP address, URL.
Use ! to invert the sense of matching (to select non-matching lines).
Squid Access Table
Squid - Access Logs
Date IP Status Address User Destination
26.09.2024 10:03:49 10.2.107.10 NONE_NONE/000 error:transaction-end-before-headers - -
26.09.2024 10:03:49 10.2.107.10 NONE_NONE/000 error:transaction-end-before-headers - -
26.09.2024 10:02:09 10.2.107.10 TCP_MISS/301 http://cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today? - 23.54.132.91
26.09.2024 09:58:49 10.2.107.10 NONE_NONE/000 error:transaction-end-before-headers - -
26.09.2024 09:58:49 10.2.107.10 NONE_NONE/000 error:transaction-end-before-headers - -
26.09.2024 09:57:49 10.2.107.10 NONE_NONE/000 error:transaction-end-before-headers - -
26.09.2024 09:57:49 10.2.107.10 NONE_NONE/000 error:transaction-end-before-headers - -
26.09.2024 09:56:54 10.2.107.10 TCP_MISS/200 http://download.windowsupdate.com/d/msdownload/update/others/2023/03/38677849_cc9dc29ea42a05f4d58025a89ff733b2b9f34671.cab - 93.184.221.240
26.09.2024 09:56:54 10.2.107.10 TCP_MISS/200 http://download.windowsupdate.com/d/msdownload/update/others/2023/11/40101064_edc34a842579b09671f21e3ccab93ff98d9057d1.cab - 93.184.221.240
26.09.2024 09:56:54 10.2.107.10 TCP_MISS/200 http://download.windowsupdate.com/c/msdownload/update/others/2023/04/38812857_b6be8137bd471ae5a775b5ed2d85a85dcef8d068.cab - 93.184.221.240
Squid Cache Table
Squid - Cache Logs
Date-Time Message
26.09.2024 10:27:13 NETDB state saved; 8 entries, 1 msec
26.09.2024 10:27:13 Logfile: closing log stdio:/var/squid/logs/netdb.state

Blacklists :


Put each entry on a separate line.
Whitelist
Destination domains that will be accessible to the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.
Blacklist
http://httpforever.com/
Destination domains that will be blocked for the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.
Block User Agents
Enter user agents that will be blocked for the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.
Block MIME Types (Reply Only)
Enter MIME types that will be blocked for the users that are allowed to use the proxy. Useful to block javascript (application/javascript).
Put each entry on a separate line. You can also use regular expressions.



Il propose également des options avancées de blacklistages :



Headers Handling, Language and Other Customizations

Visible Hostname
Proxy UTI107-NGabriele
This is the hostname to be displayed in proxy server error messages.

Administrator's Email
admin@uti107-NGabriele.fr
This is the email address displayed in error messages to the users.

Error Language
fr
Select the language in which the proxy server will display error messages to users.

X-Forwarded Header Mode
(on)
Choose how to handle X-Forwarded-For headers. Default: on

Disable VIA Header
☐ If not set, Squid will include a Via header in requests and replies as required by RFC2616.

URI Whitespace Characters Handling
strip
Choose how to handle whitespace characters in URL. Default: strip

Suppress Squid Version
☑ Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

Save | Show Advanced Options

Enable Access Logging
☑ This will enable the access log.
Warning: Do NOT enable if available disk space is low.

Log Store Directory
/var/squid/logs
The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs
Important: Do NOT include the trailing / when setting a custom location.

Rotate Logs
365
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Log Pages Denied by SquidGuard
☐ Makes it possible for SquidGuard denied log to be included on Squid logs.
Click Info for detailed instructions.

Headers Handling, Language and Other Customizations

Visible Hostname
localhost
This is the hostname to be displayed in proxy server error messages.

Administrator's Email
admin@localhost
This is the email address displayed in error messages to the users.

Error Language
en
Select the language in which the proxy server will display error messages to users.

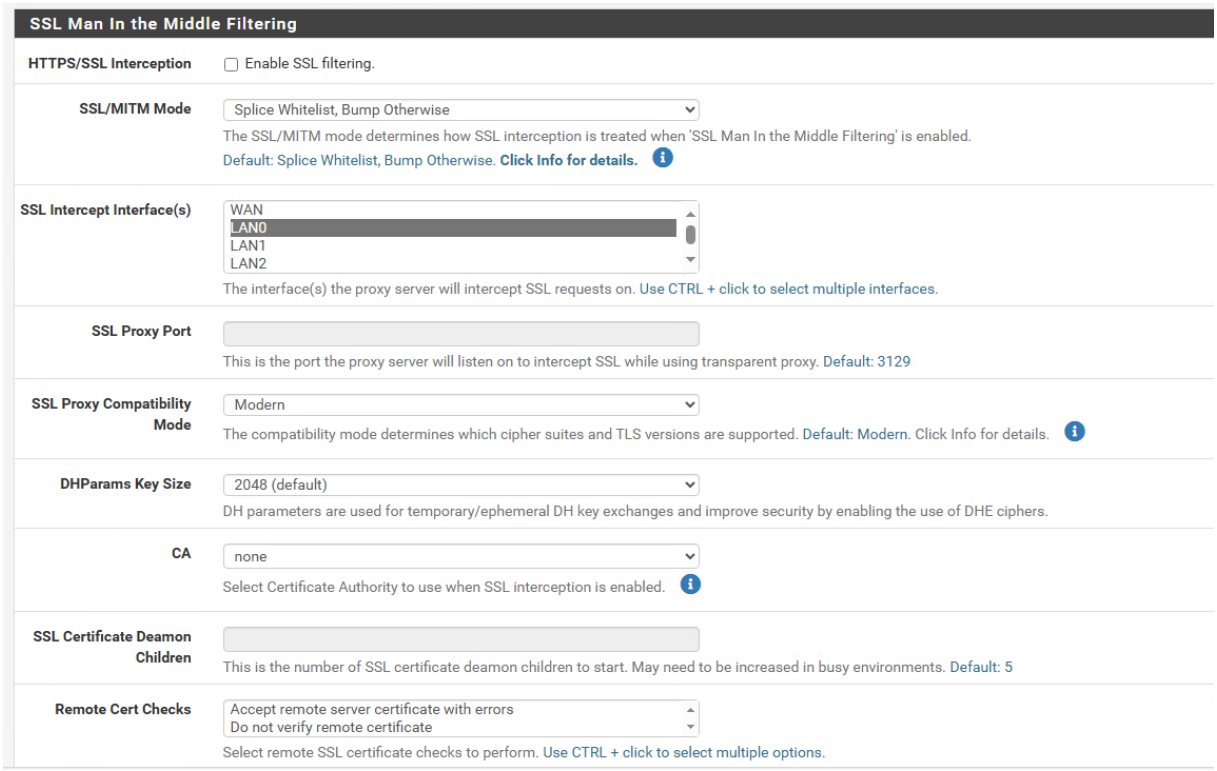
X-Forwarded Header Mode
(on)
Choose how to handle X-Forwarded-For headers. Default: on

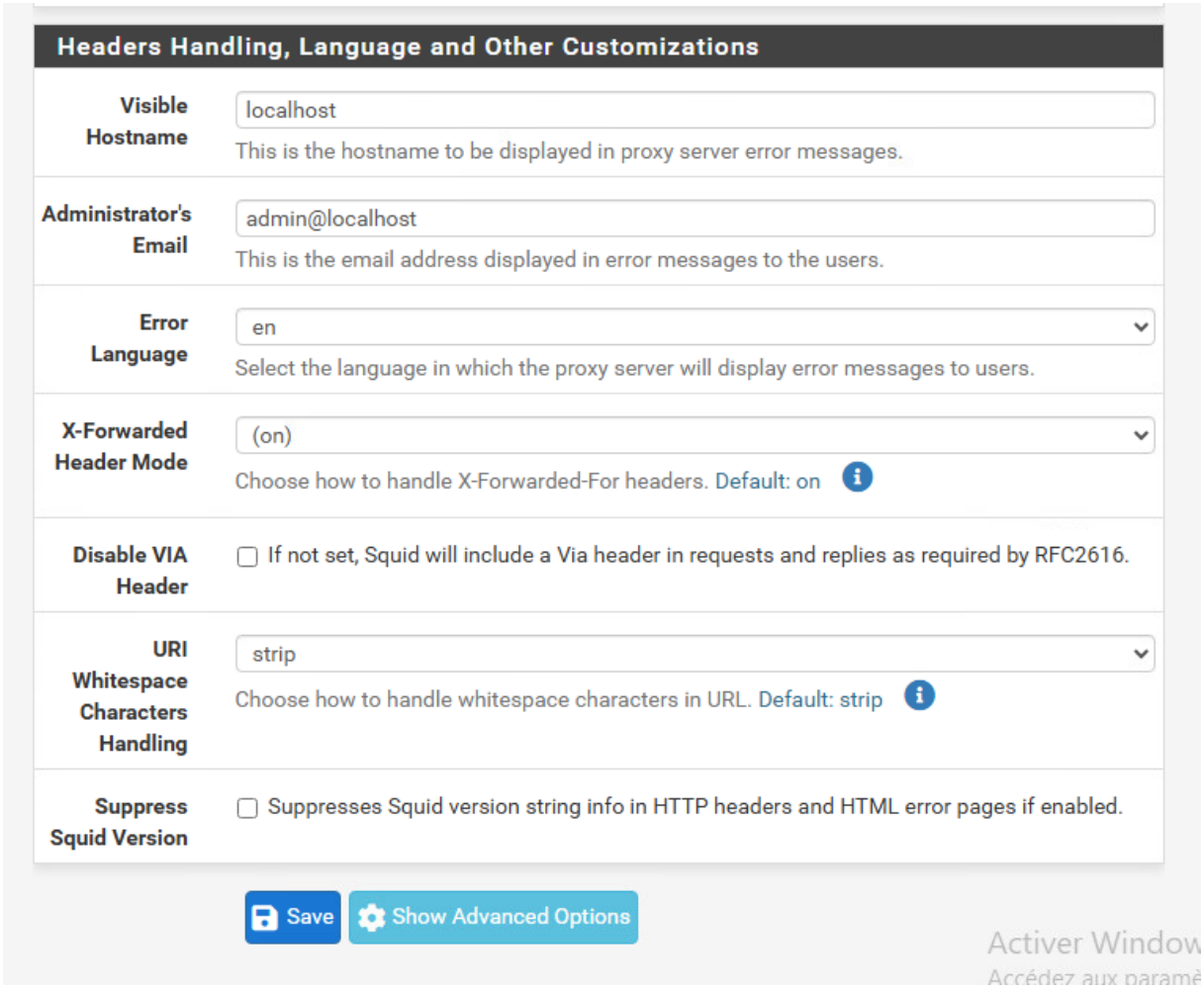
Disable VIA Header
☐ If not set, Squid will include a Via header in requests and replies as required by RFC2616.

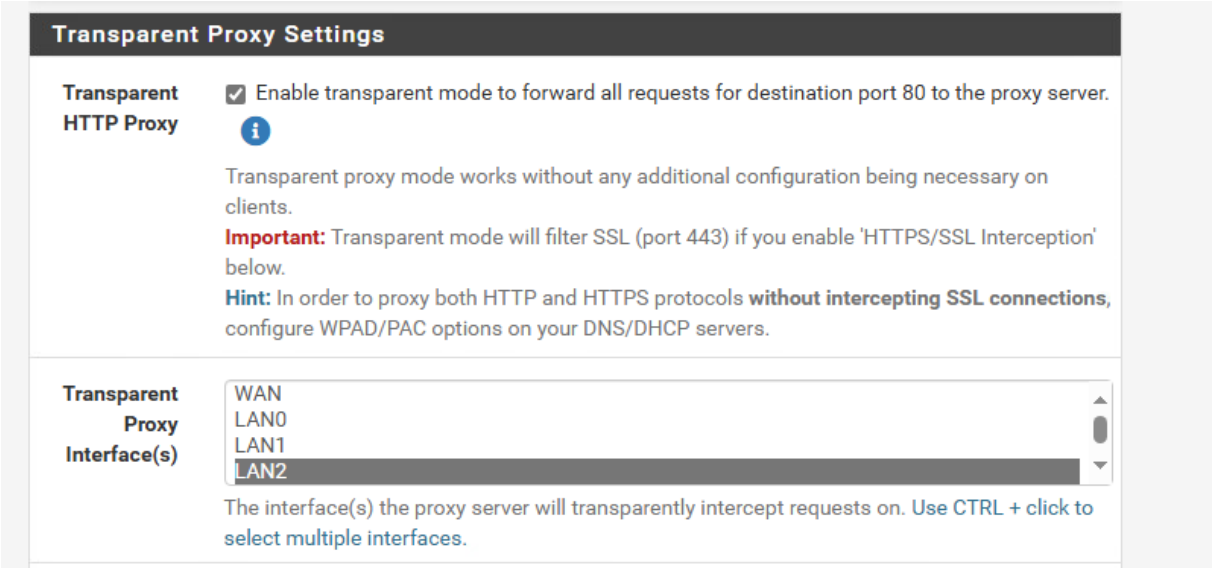
URI Whitespace Characters Handling
strip
Choose how to handle whitespace characters in URL. Default: strip

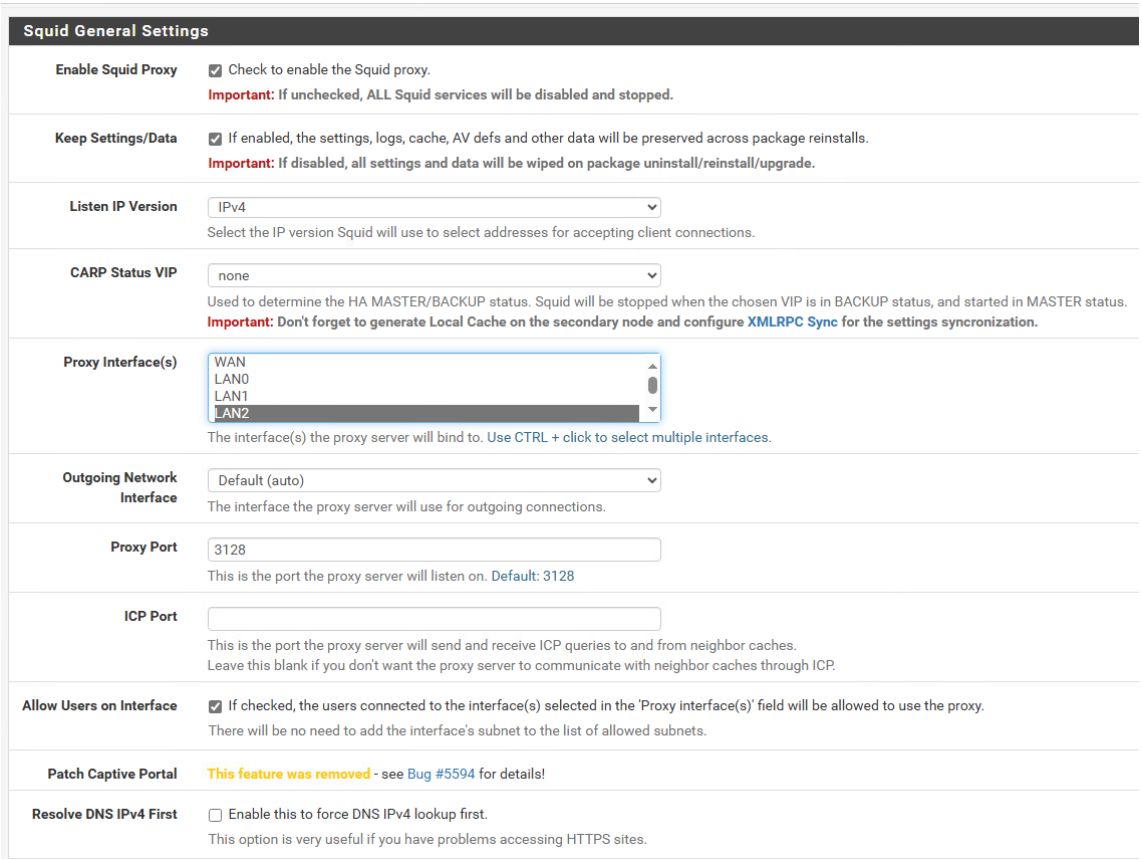
Suppress Squid Version
☐ Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

Save | Show Advanced Options


SSL Man In the Middle Filtering
HTTPS/SSL Interception
Enable SSL filtering.
SSL/MITM Mode
Splice Whitelist, Bump Otherwise
The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled.
Default: Splice Whitelist, Bump Otherwise. Click Info for details.
SSL Intercept Interface(s)
WAN
LAN0
LAN1
LAN2
The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.
SSL Proxy Port
This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129
SSL Proxy Compatibility Mode
Modern
The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details.
DHParams Key Size
2048 (default)
DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.
CA
none
Select Certificate Authority to use when SSL interception is enabled.
SSL Certificate Deamon Children
This is the number of SSL certificate deamon children to start. May need to be increased in busy environments. Default: 5
Remote Cert Checks
Accept remote server certificate with errors
Do not verify remote certificate
Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.


Headers Handling, Language and Other Customizations
Visible Hostname
localhost
This is the hostname to be displayed in proxy server error messages.
Administrator's Email
admin@localhost
This is the email address displayed in error messages to the users.
Error Language
en
Select the language in which the proxy server will display error messages to users.
X-Forwarded Header Mode
(on)
Choose how to handle X-Forwarded-For headers. Default: on
Disable VIA Header
If not set, Squid will include a Via header in requests and replies as required by RFC2616.
URI Whitespace Characters Handling
strip
Choose how to handle whitespace characters in URL. Default: strip
Suppress Squid Version
Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.
Save
Show Advanced Options
Activer Window
Accédez aux paramè


Transparent Proxy Settings
Transparent HTTP Proxy
Enable transparent mode to forward all requests for destination port 80 to the proxy server.
Transparent proxy mode works without any additional configuration being necessary on clients.
Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.
Hint: In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections, configure WPAD/PAC options on your DNS/DHCP servers.
Transparent Proxy Interface(s)
WAN
LAN0
LAN1
LAN2
The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.


Squid General Settings
Enable Squid Proxy
Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data
If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Listen IP Version
IPv4
Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP
none
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.
Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings syncronization.
Proxy Interface(s)
WAN
LAN0
LAN1
LAN2
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface
Default (auto)
The interface the proxy server will use for outgoing connections.
Proxy Port
3128
This is the port the proxy server will listen on. Default: 3128
ICP Port
This is the port the proxy server will send and receive ICP queries to and from neighbor caches.
Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
Allow Users on Interface
If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.
There will be no need to add the interface's subnet to the list of allowed subnets.
Patch Captive Portal
This feature was removed - see Bug #5594 for details!
Resolve DNS IPv4 First
Enable this to force DNS IPv4 lookup first.
This option is very useful if you have problems accessing HTTPS sites.

Cache Size

Specifies the ideal amount of physical RAM (in megabytes) to be used for In-Transit objects, Hot Objects and Negative-Cached objects.
Minimum value: 1 (MB). Default: 64 (MB)

Maximum Object Size in RAM

256

Objects greater than this size (in kilobytes) will not be attempted to kept in the memory cache.
Default: 256 (KB)

Memory Replacement Policy

Heap GDSF

The memory replacement policy determines which objects are purged from memory when space is needed. Default: heap GDSF

Dynamic and Update Content

Cache Dynamic Content

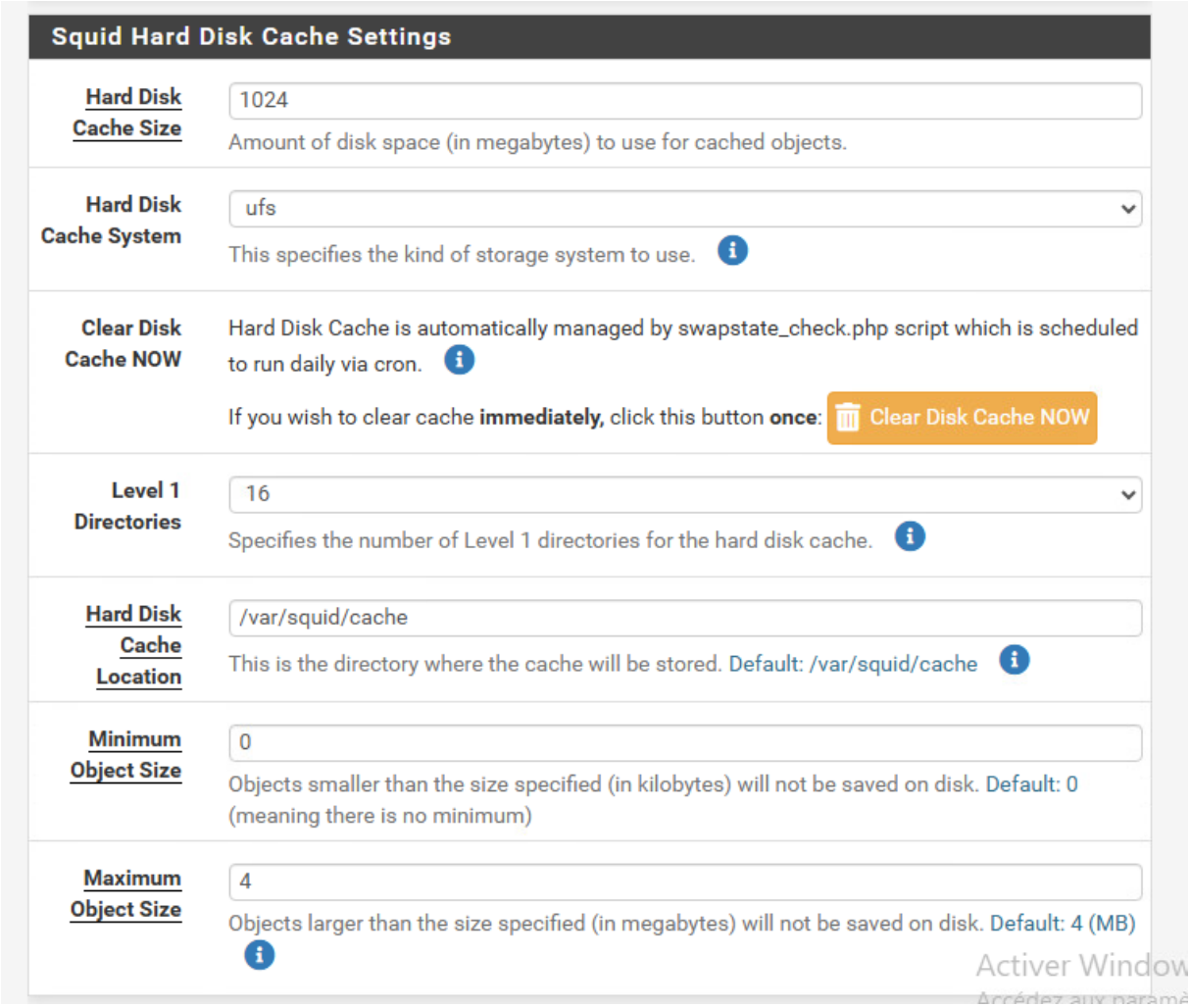
☐ Select to enable caching of dynamic content.

With dynamic cache enabled, you can also apply refresh_patterns to sites like Windows Updates.

Custom refresh_patterns

Enter custom refresh_patterns for better dynamic cache usage.
Note: These refresh_patterns will only be included if 'Cache Dynamic Content' is enabled.

Save


Squid Hard Disk Cache Settings
Hard Disk Cache Size
1024
Amount of disk space (in megabytes) to use for cached objects.
Hard Disk Cache System
ufs
This specifies the kind of storage system to use.
Clear Disk Cache NOW
Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron.
If you wish to clear cache immediately, click this button once:
Clear Disk Cache NOW
Level 1 Directories
16
Specifies the number of Level 1 directories for the hard disk cache.
Hard Disk Cache Location
/var/squid/cache
This is the directory where the cache will be stored. Default: /var/squid/cache
Minimum Object Size
0
Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)
Maximum Object Size
4
Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB)
Activer Window

Squid Hard Disk Cache Settings

Hard Disk Cache Size
100
Amount of disk space (in megabytes) to use for cached objects.

Hard Disk Cache System
ufs
This specifies the kind of storage system to use.

Clear Disk Cache NOW
Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron.

If you wish to clear cache **immediately**, click this button **once**: Clear Disk Cache NOW

Level 1 Directories
16
Specifies the number of Level 1 directories for the hard disk cache.

Hard Disk Cache Location
/var/squid/cache
This is the directory where the cache will be stored. Default: /var/squid/cache

Minimum Object Size
0
Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)

Maximum Object Size
4
Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB)

Squid Memory Cache Settings

Squid Hard Disk Cache Settings

Hard Disk Cache Size
100
Amount of disk space (in megabytes) to use for cached objects.

Hard Disk Cache System
ufs
This specifies the kind of storage system to use.

Clear Disk Cache NOW
Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron.

If you wish to clear cache **immediately**, click this button **once**: Clear Disk Cache NOW

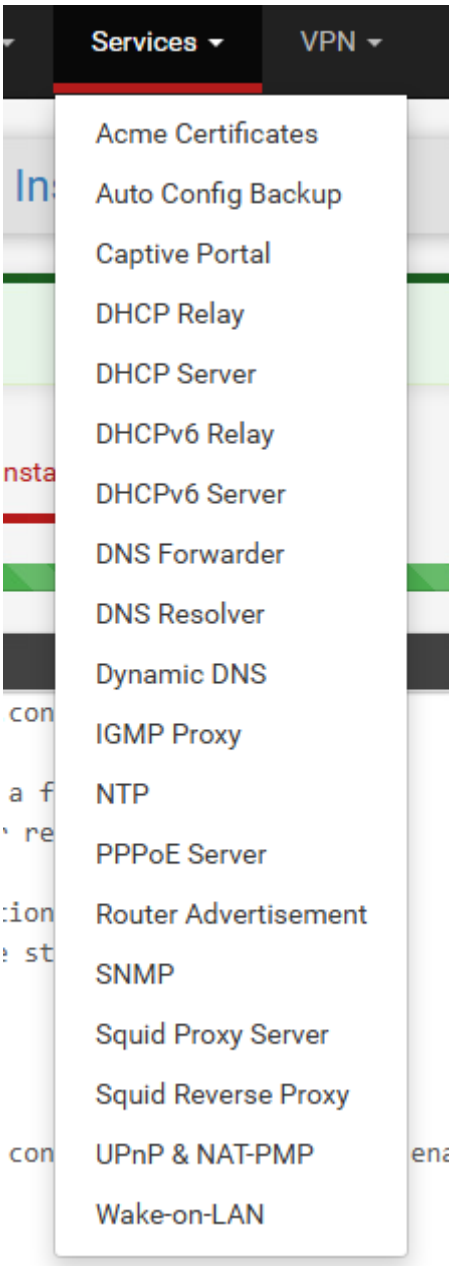
Level 1 Directories
16
Specifies the number of Level 1 directories for the hard disk cache.

Hard Disk Cache Location
/var/squid/cache
This is the directory where the cache will be stored. Default: /var/squid/cache

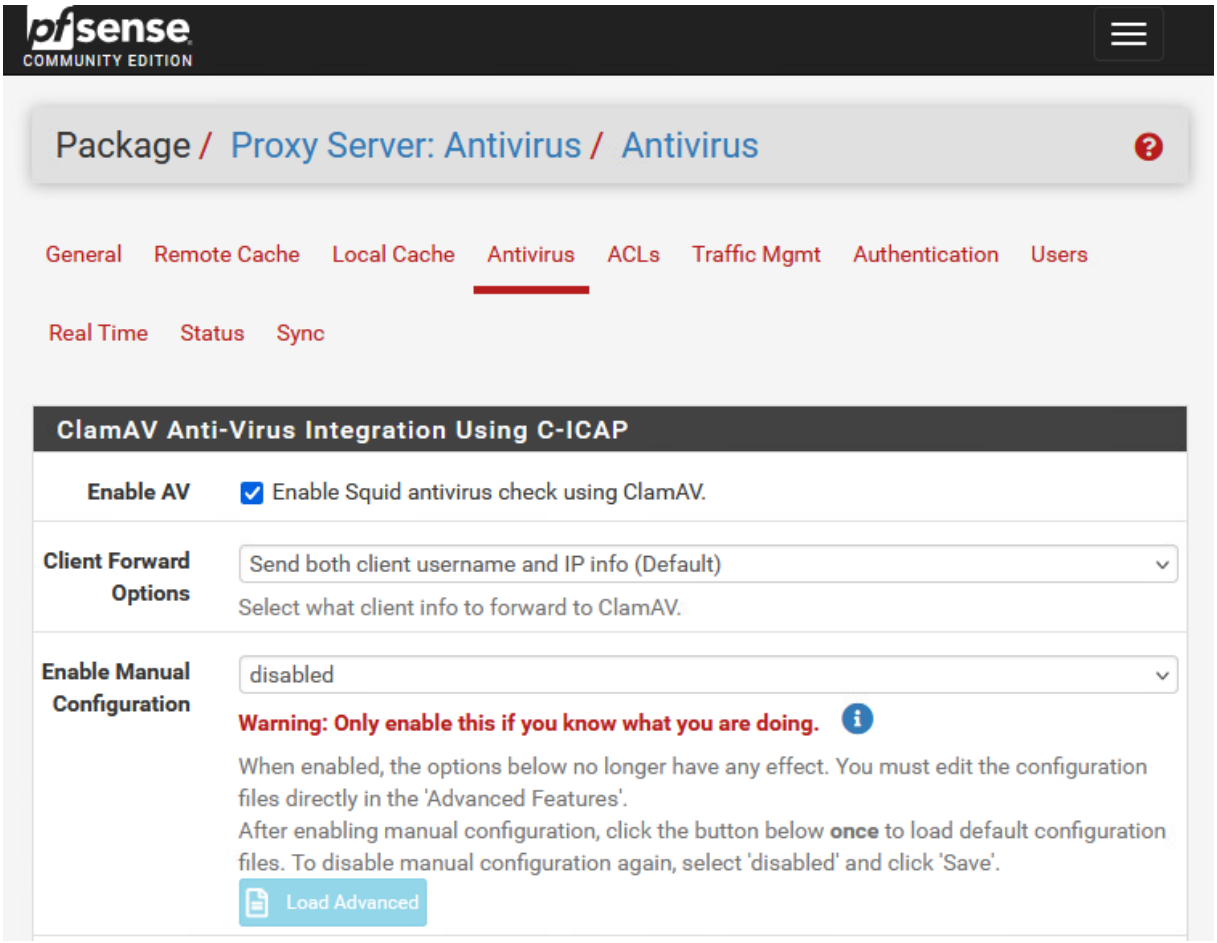
Minimum Object Size
0
Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)

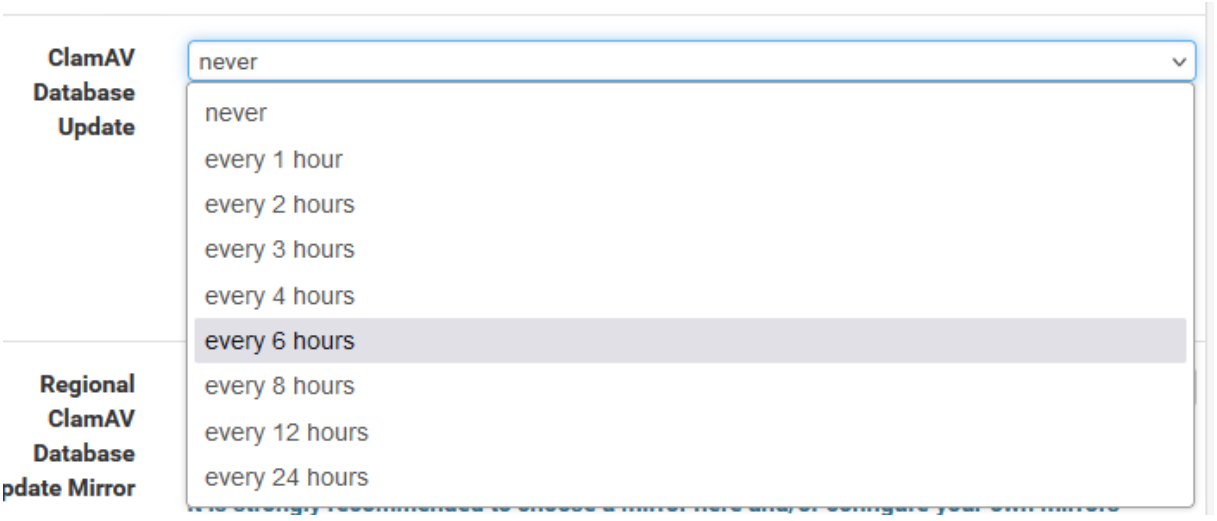
Maximum Object Size
4
Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB)

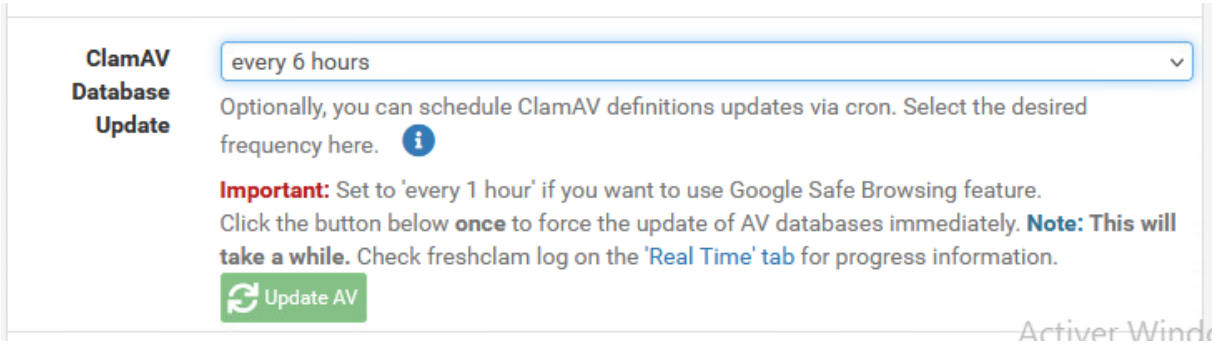
Squid Memory Cache Settings


Services
VPN
Acme Certificates
Auto Config Backup
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server
DNS Forwarder
DNS Resolver
Dynamic DNS
IGMP Proxy
NTP
PPPoE Server
Router Advertisement
SNMP
Squid Proxy Server
Squid Reverse Proxy
UPnP & NAT-PMP
Wake-on-LAN

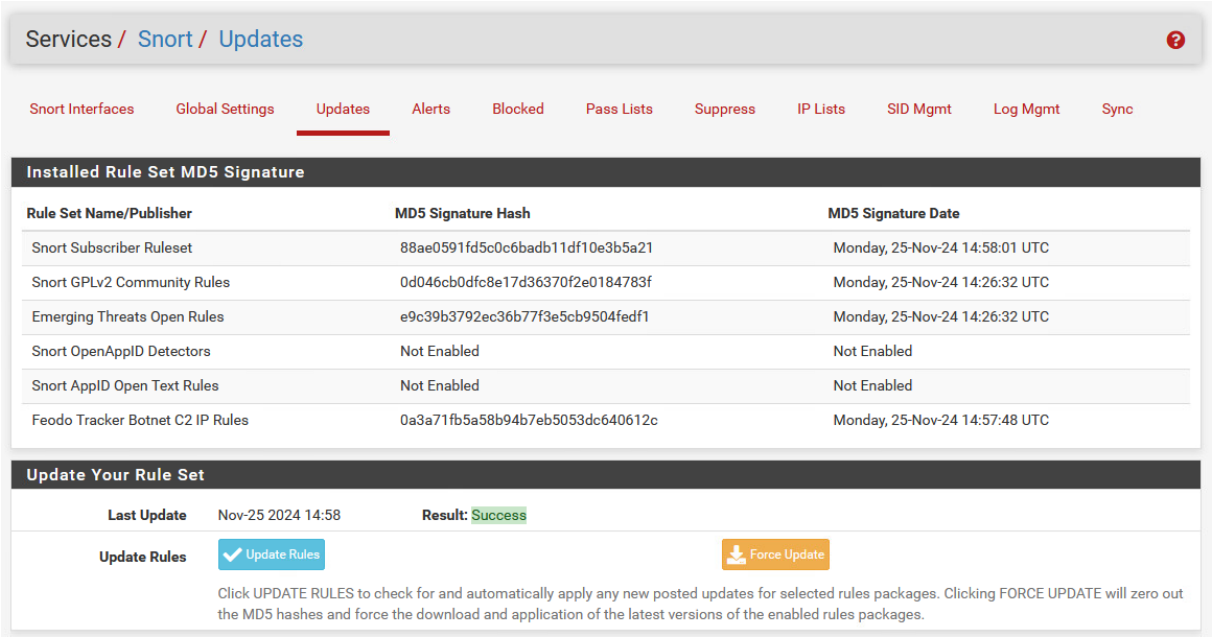
ClamAV

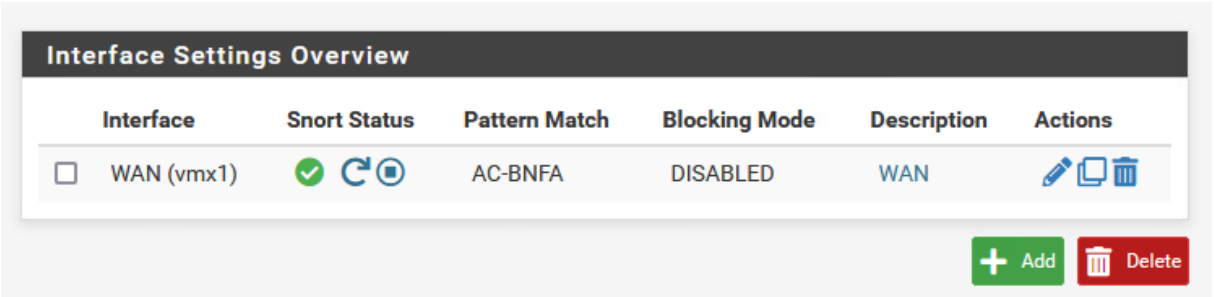

pfsense
COMMUNITY EDITION
Package / Proxy Server: Antivirus / Antivirus
General
Remote Cache
Local Cache
Antivirus
ACLs
Traffic Mgmt
Authentication
Users
Real Time
Status
Sync
ClamAV Anti-Virus Integration Using C-ICAP
Enable AV
Enable Squid antivirus check using ClamAV.
Client Forward Options
Send both client username and IP info (Default)
Select what client info to forward to ClamAV.
Enable Manual Configuration
disabled
Warning: Only enable this if you know what you are doing.
When enabled, the options below no longer have any effect. You must edit the configuration files directly in the 'Advanced Features'.
After enabling manual configuration, click the button below once to load default configuration files. To disable manual configuration again, select 'disabled' and click 'Save'.
Load Advanced

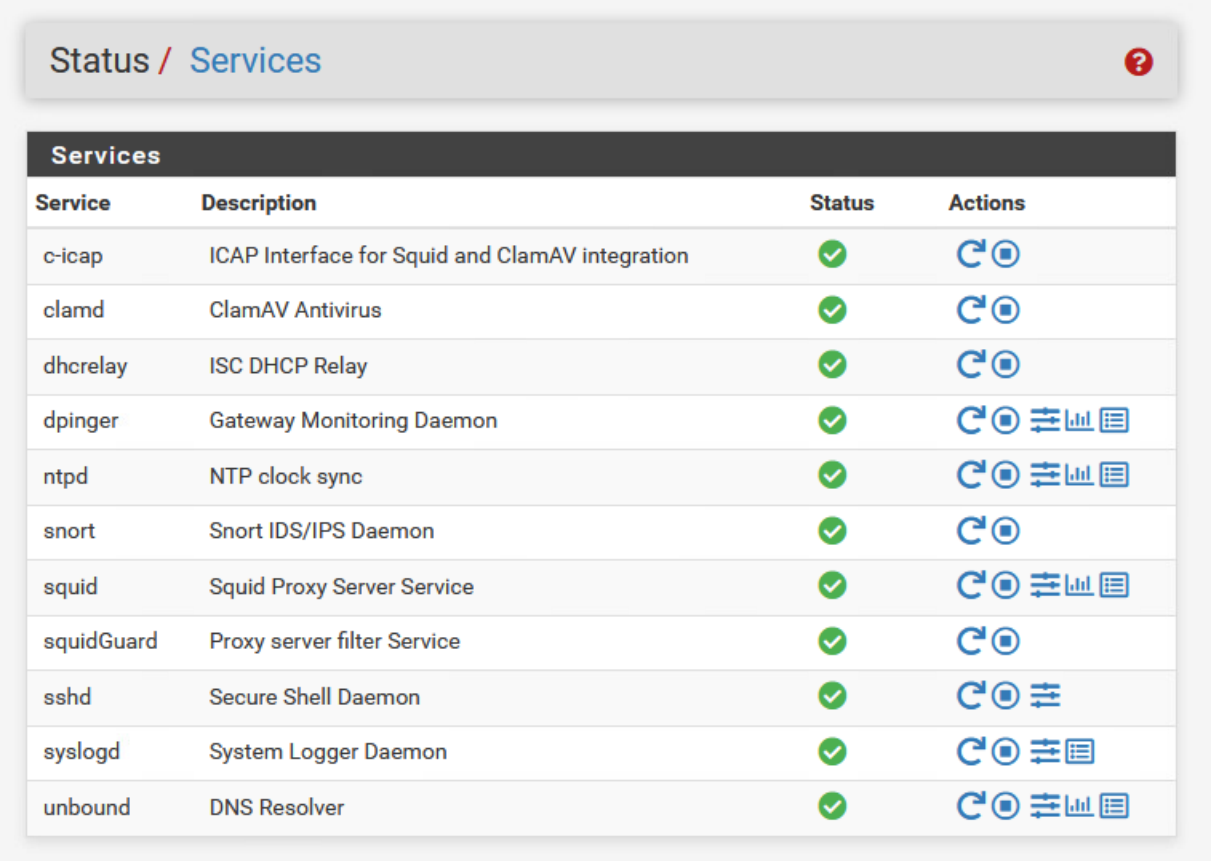

ClamAV Database Update
never
never
every 1 hour
every 2 hours
every 3 hours
every 4 hours
every 6 hours
every 8 hours
every 12 hours
every 24 hours
Regional ClamAV Database pdate Mirror


ClamAV Database Update
every 6 hours
Optionally, you can schedule ClamAV definitions updates via cron. Select the desired frequency here.
Important: Set to 'every 1 hour' if you want to use Google Safe Browsing feature.
Click the button below once to force the update of AV databases immediately. Note: This will take a while. Check freshclam log on the 'Real Time' tab for progress information.
Update AV

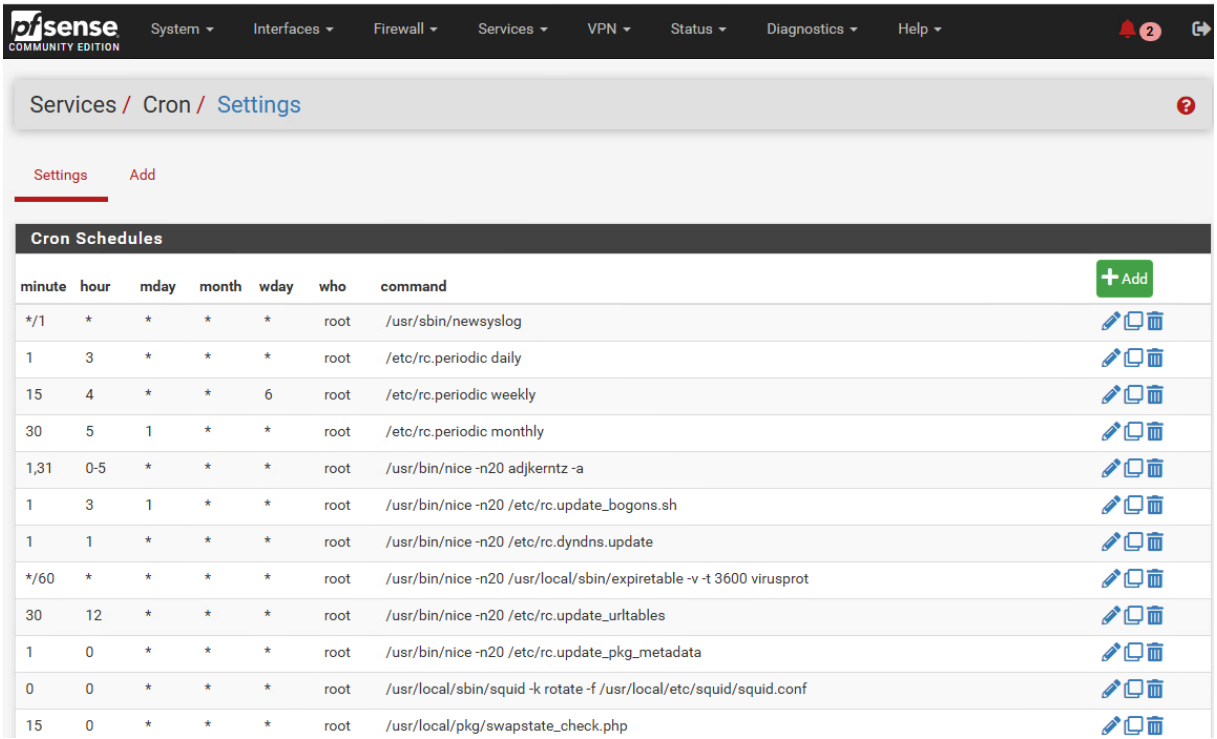
Snort


Services / Snort / Updates
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Installed Rule Set MD5 Signature
Rule Set Name/Publisher
MD5 Signature Hash
MD5 Signature Date
Snort Subscriber Ruleset
88ae0591fd5c0c6badb11df10e3b5a21
Monday, 25-Nov-24 14:58:01 UTC
Snort GPLv2 Community Rules
0d046cb0dfc8e17d36370f2e0184783f
Monday, 25-Nov-24 14:26:32 UTC
Emerging Threats Open Rules
e9c39b3792ec36b77f3e5cb9504fedf1
Monday, 25-Nov-24 14:26:32 UTC
Snort OpenAppID Detectors
Not Enabled
Not Enabled
Snort AppID Open Text Rules
Not Enabled
Not Enabled
Feodo Tracker Botnet C2 IP Rules
0a3a71fb5a58b94b7eb5053dc640612c
Monday, 25-Nov-24 14:57:48 UTC
Update Your Rule Set
Last Update
Nov-25 2024 14:58
Result: Success
Update Rules
Update Rules
Force Update
Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

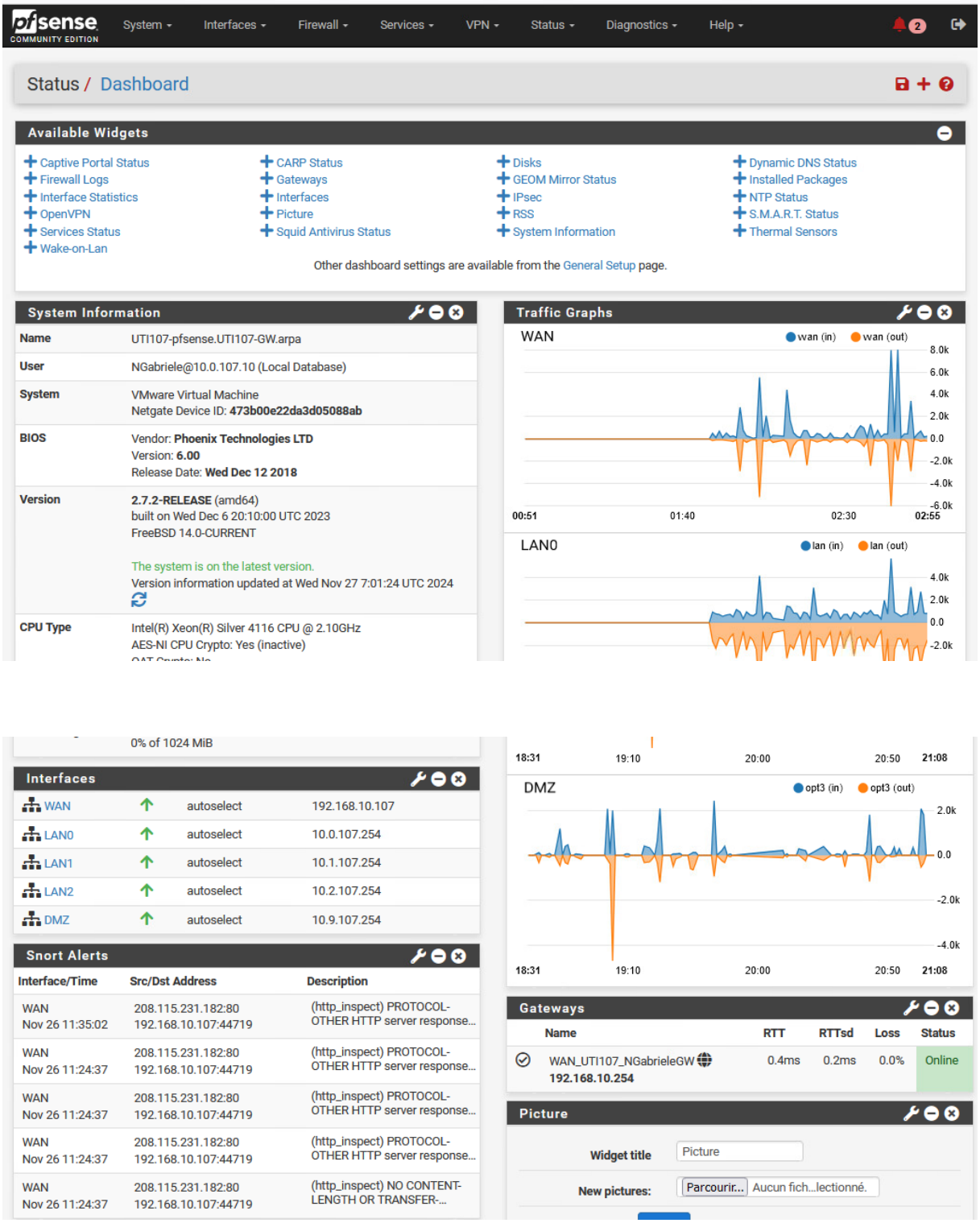

Interface Settings Overview
Interface
Snort Status
Pattern Match
Blocking Mode
Description
Actions
WAN (vmx1)
AC-BNFA
DISABLED
WAN
Add
Delete

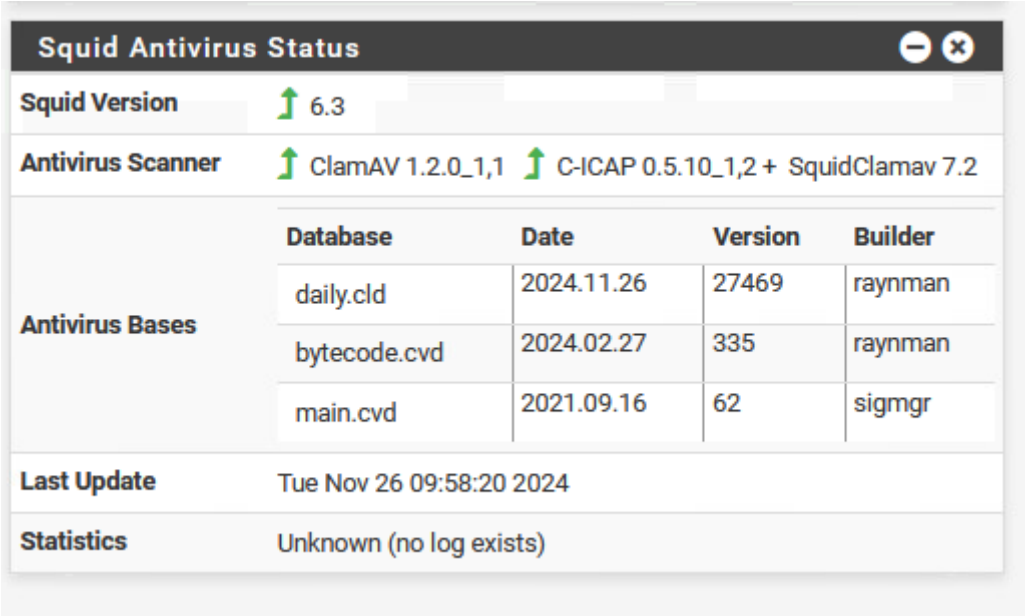

Status / Services
Services
Service
Description
Status
Actions
c-icap
ICAP Interface for Squid and ClamAV integration
clamd
ClamAV Antivirus
dhcrelay
ISC DHCP Relay
dpinger
Gateway Monitoring Daemon
ntpd
NTP clock sync
snort
Snort IDS/IPS Daemon
squid
Squid Proxy Server Service
squidGuard
Proxy server filter Service
sshd
Secure Shell Daemon
syslogd
System Logger Daemon
unbound
DNS Resolver

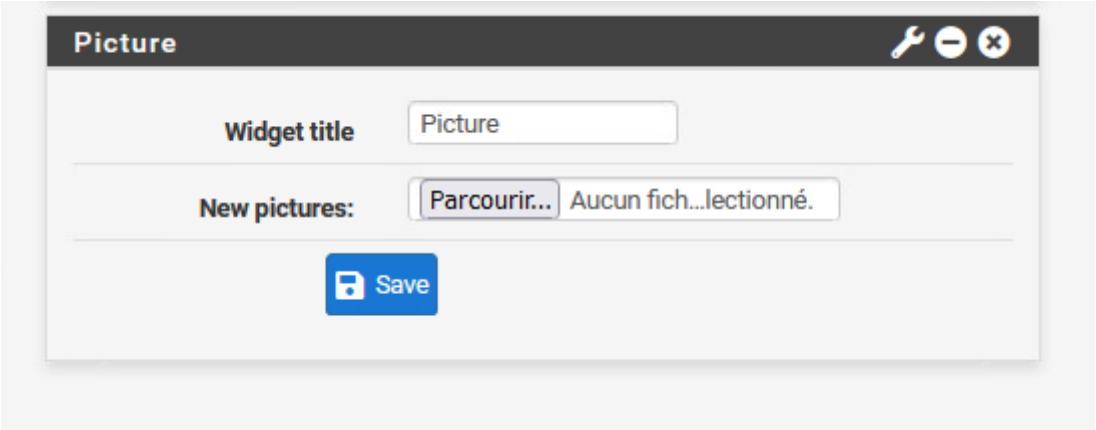
Cron

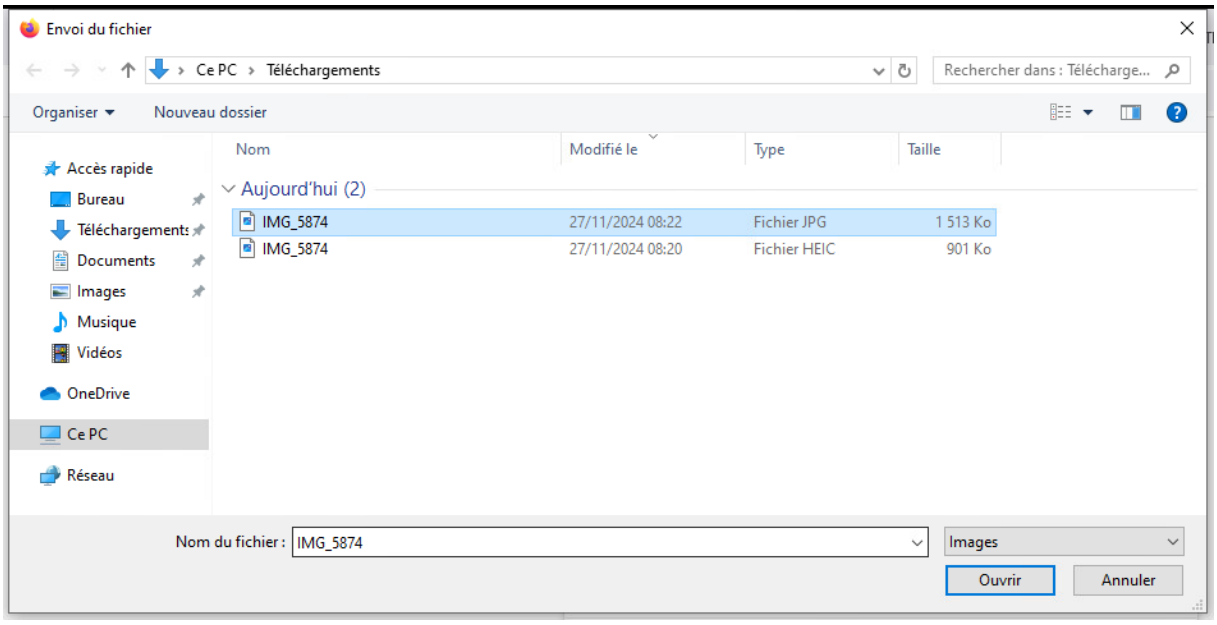

pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Services / Cron / Settings
Settings
Add
Cron Schedules
minute
hour
mday
month
wday
who
command
Add
*/1 * * * * root /usr/sbin/newsyslog
1 3 * * * root /etc/rc.periodic daily
15 4 * * 6 root /etc/rc.periodic weekly
30 5 1 * * root /etc/rc.periodic monthly
1,31 0-5 * * * root /usr/bin/nice -n20 adjkerntz -a
1 3 1 * * root /usr/bin/nice -n20 /etc/rc.update_bogons.sh
1 1 * * * root /usr/bin/nice -n20 /etc/rc.dyndns.update
*/60 * * * * root /usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600 virusprot
30 12 * * * root /usr/bin/nice -n20 /etc/rc.update_urltables
1 0 * * * root /usr/bin/nice -n20 /etc/rc.update_pkg_metadata
0 0 * * * root /usr/local/sbin/squid -k rotate -f /usr/local/etc/squid/squid.conf
15 0 * * * root /usr/local/pkg/swapstate_check.php

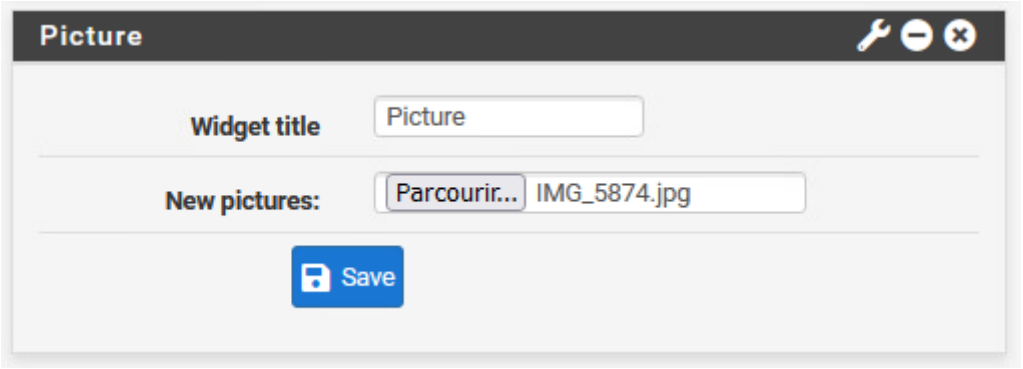
Optimisation du dashboard




Squid Antivirus Status
Squid Version
6.3
Antivirus Scanner
ClamAV 1.2.0_1,1
C-ICAP 0.5.10_1,2 + SquidClamav 7.2
Antivirus Bases
Database
Date
Version
Builder
daily.cld
2024.11.26
27469
raynman
bytecode.cvd
2024.02.27
335
raynman
main.cvd
2021.09.16
62
sigmgr
Last Update
Tue Nov 26 09:58:20 2024
Statistics
Unknown (no log exists)

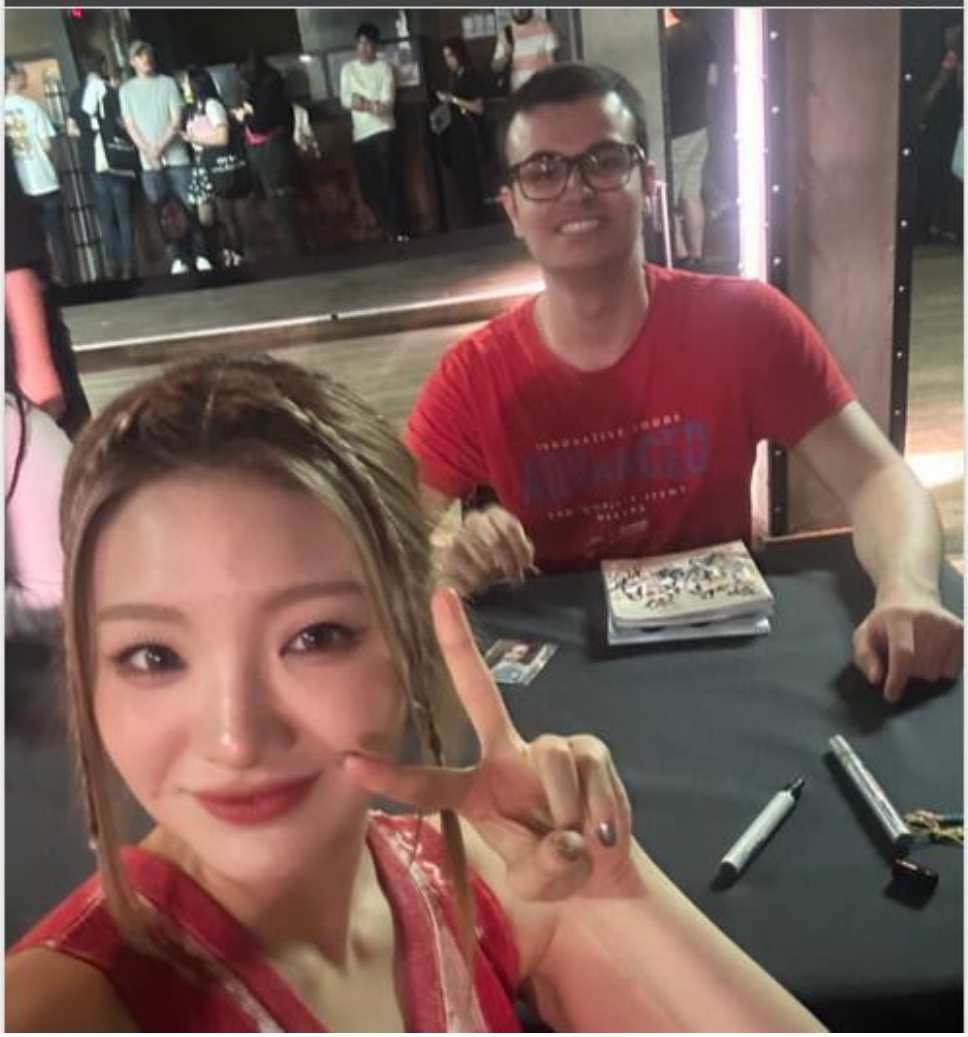

Picture
Widget title
Picture
New pictures:
Parcourir...
Aucun fich...lectionné.
Save


Envoi du fichier
Ce PC › Téléchargements
Rechercher dans : Télécharge...
Organiser
Nouveau dossier
Accès rapide
Bureau
Téléchargements
Documents
Images
Musique
Vidéos
OneDrive
Ce PC
Réseau
Nom
Modifié le
Type
Taille
Aujourd'hui (2)
IMG_5874 27/11/2024 08:22 Fichier JPG 1 513 Ko
IMG_5874 27/11/2024 08:20 Fichier HEIC 901 Ko
Nom du fichier : IMG_5874
Images
Ouvrir
Annuler

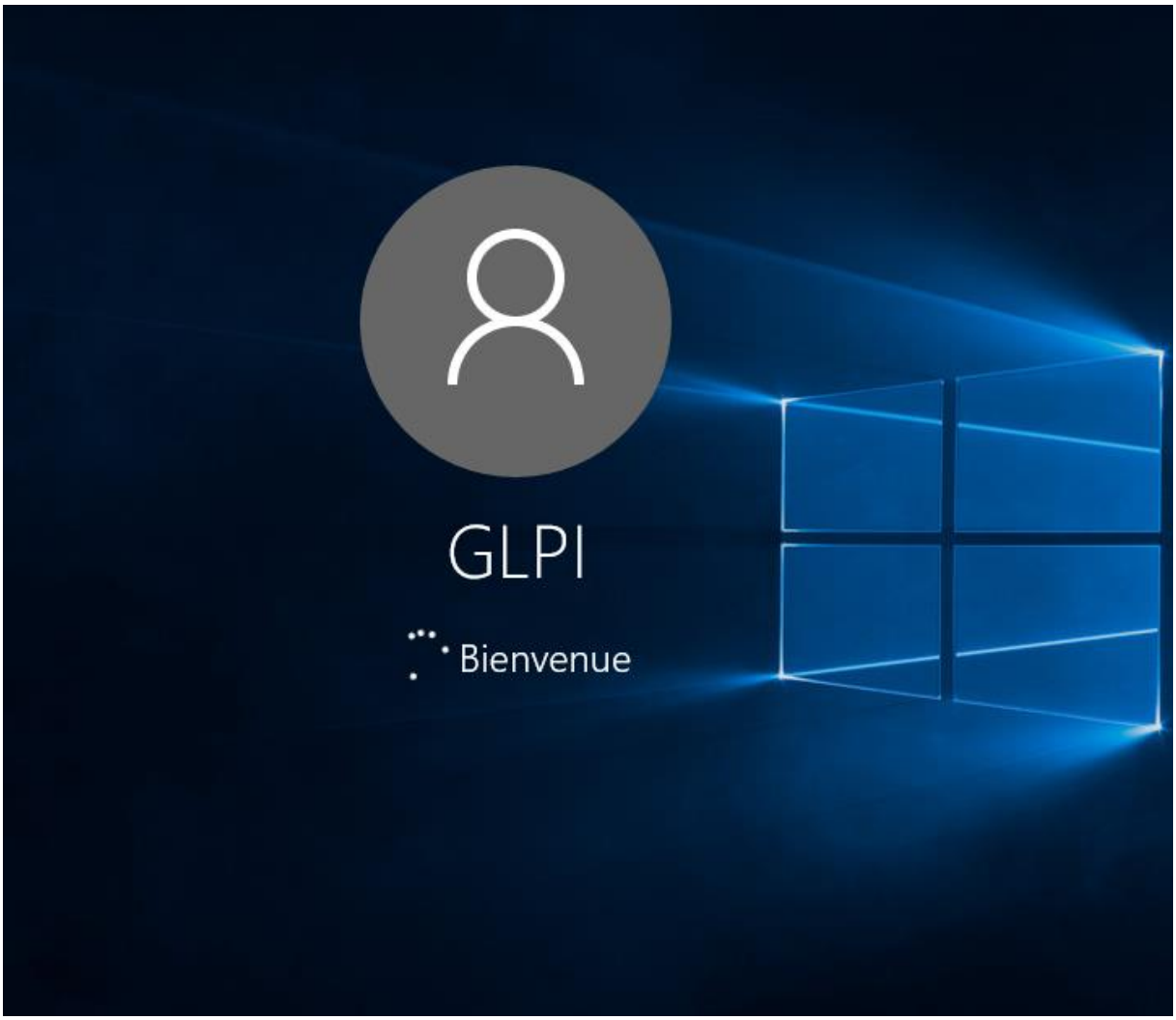

Picture
Widget title
Picture
New pictures:
Parcourir...
IMG_5874.jpg
Save

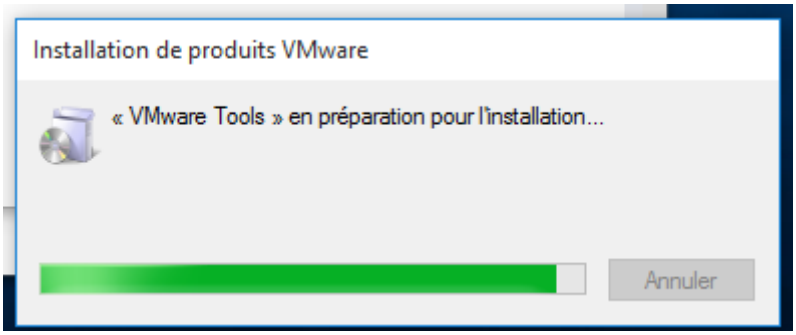
L-
onse...
L-
onse...
ENT-
...

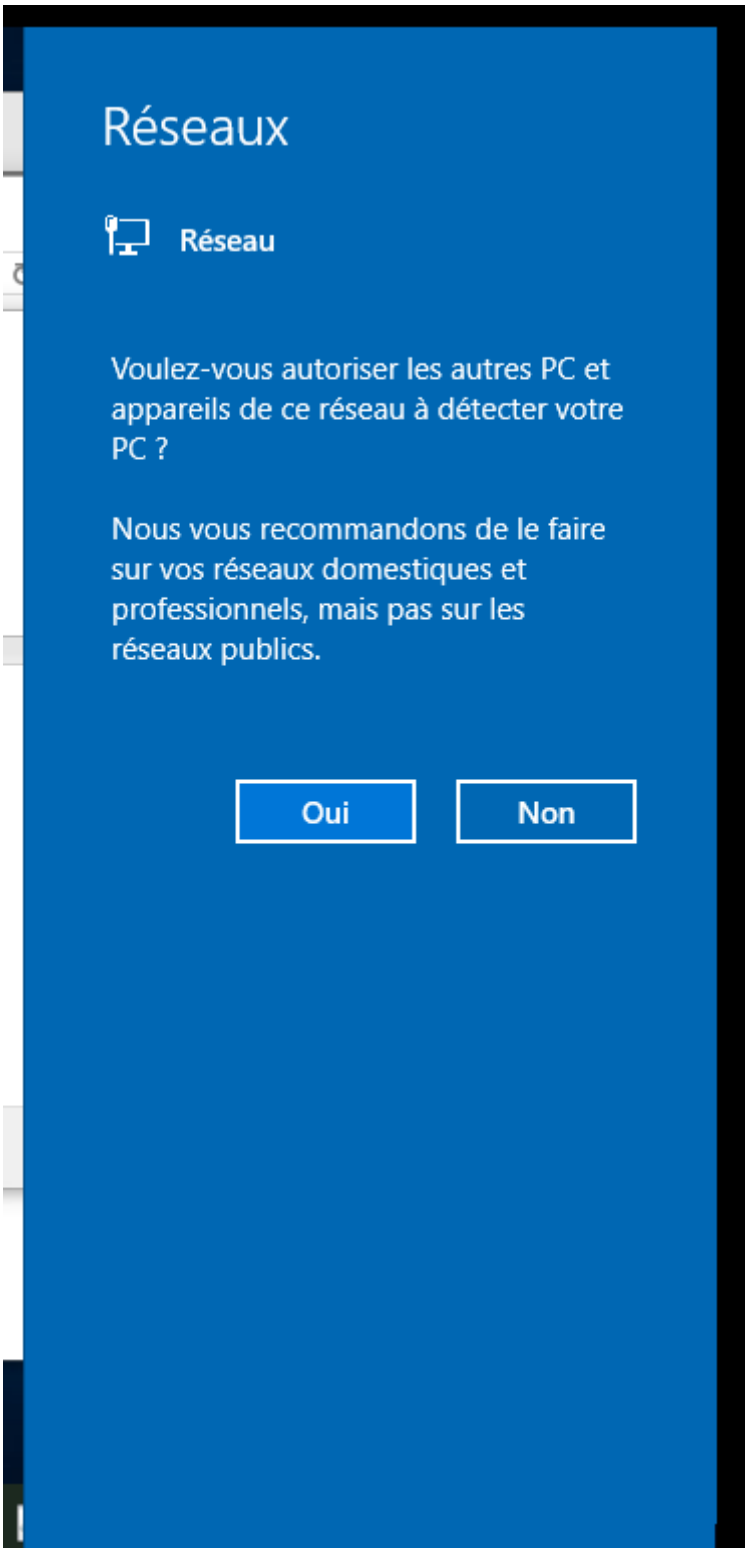
Picture

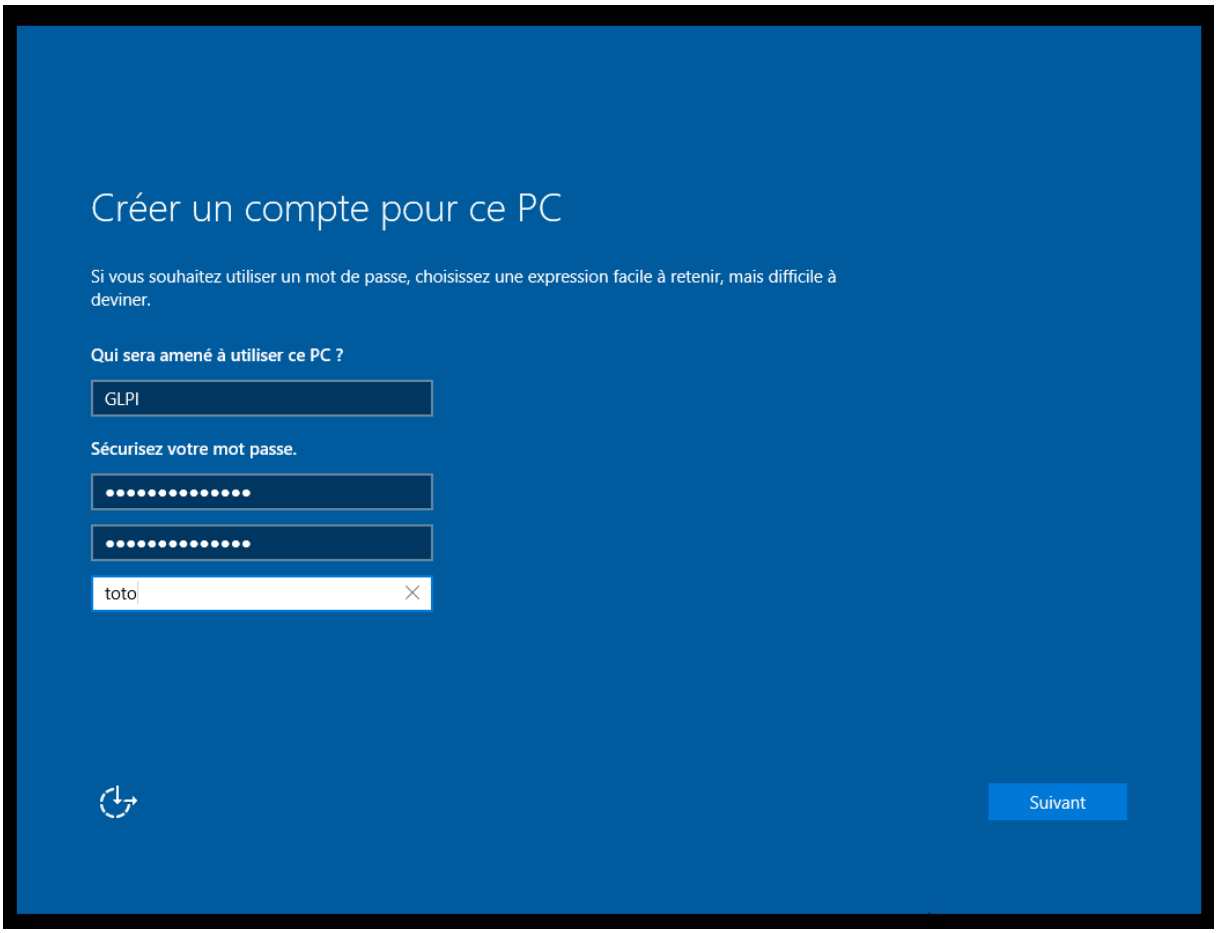


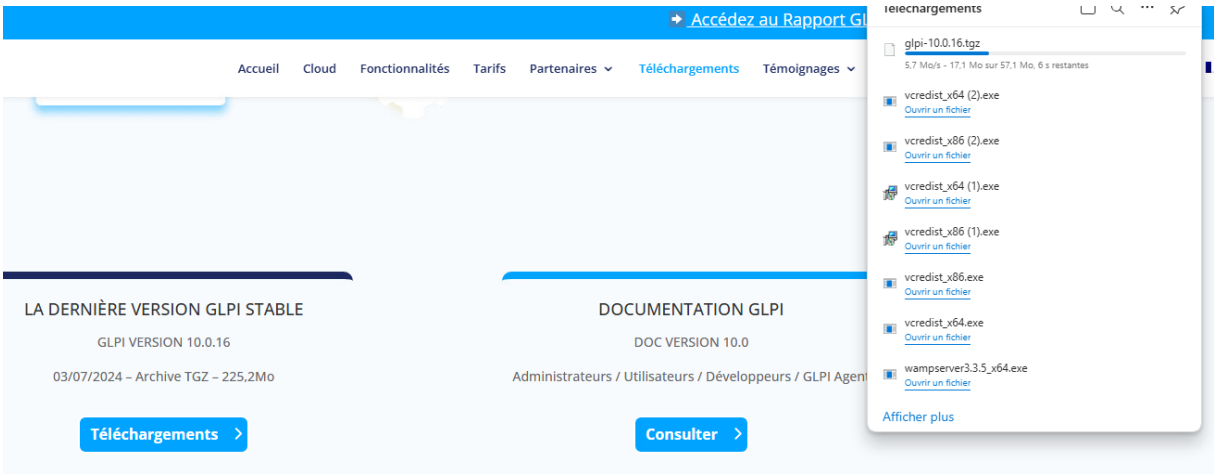
Installation de GLPI

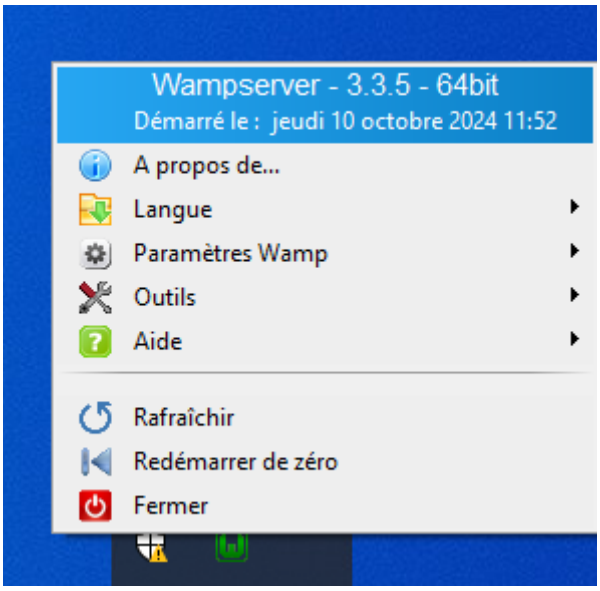




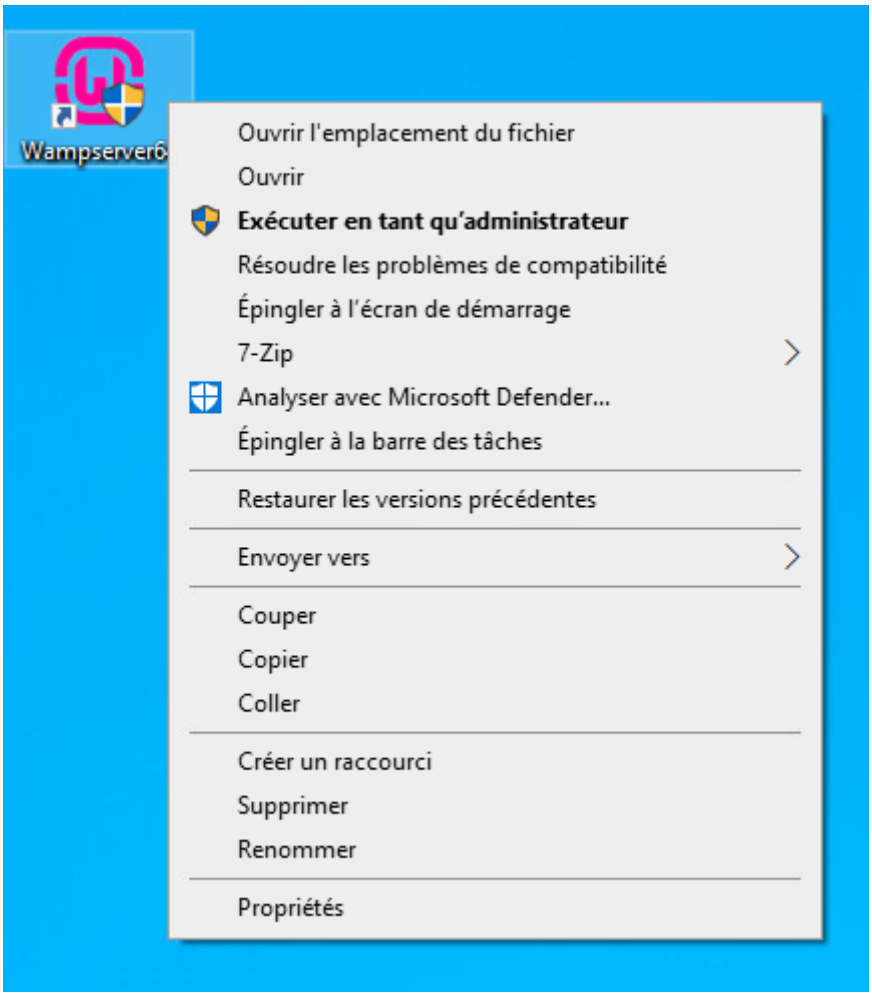

Réseaux
Réseau
Voulez-vous autoriser les autres PC et appareils de ce réseau à détecter votre PC ?
Nous vous recommandons de le faire sur vos réseaux domestiques et professionnels, mais pas sur les réseaux publics.
Oui
Non

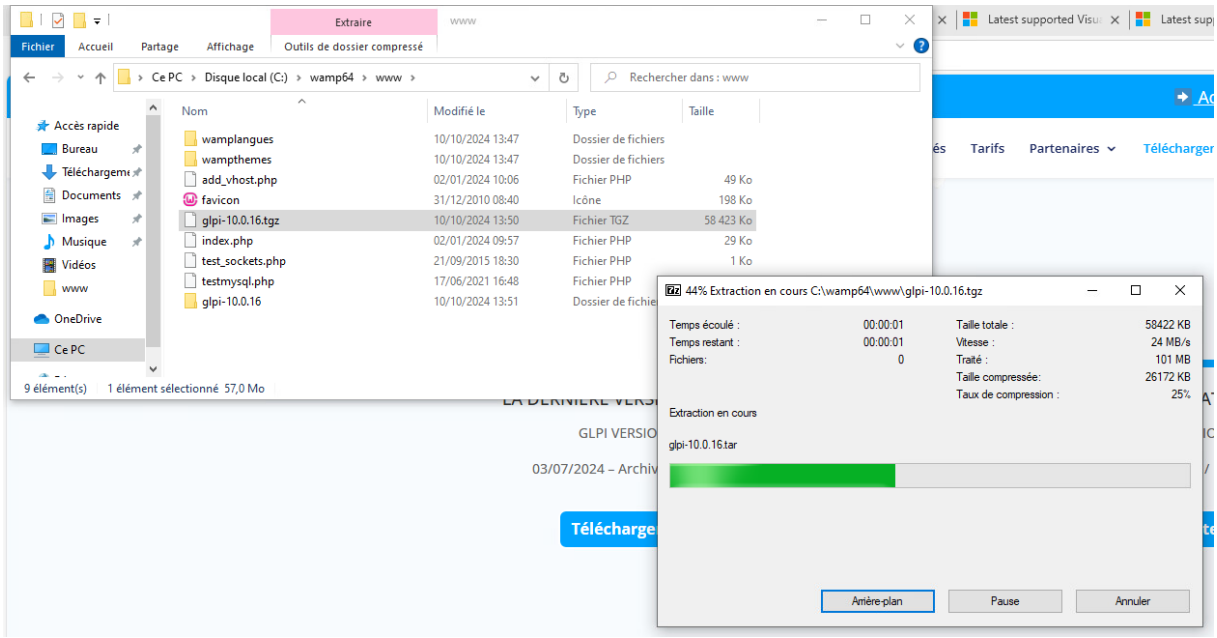

Créer un compte pour ce PC
Si vous souhaitez utiliser un mot de passe, choisissez une expression facile à retenir, mais difficile à deviner.
Qui sera amené à utiliser ce PC ?
GLPI
Sécurisez votre mot passe.
toto
Suivant


Accédez au Rapport Gl
Accueil
Cloud
Fonctionnalités
Tarifs
Partenaires
Téléchargements
Témoignages
LA DERNIÈRE VERSION GLPI STABLE
GLPI VERSION 10.0.16
03/07/2024 – Archive TGZ – 225,2Mo
Téléchargements
DOCUMENTATION GLPI
DOC VERSION 10.0
Consulter
glpi-10.0.16.tgz
vcredist_x64 (2).exe
vcredist_x86 (2).exe
vcredist_x64 (1).exe
vcredist_x86 (1).exe
vcredist_x86.exe
vcredist_x64.exe
wampserver3.3.5_x64.exe
Ouvrir un fichier
Afficher plus


Wampserver - 3.3.5 - 64bit
Démarré le : jeudi 10 octobre 2024 11:52
A propos de...
Langue
Paramètres Wamp
Outils
Aide
Rafraîchir
Redémarrer de zéro
Fermer

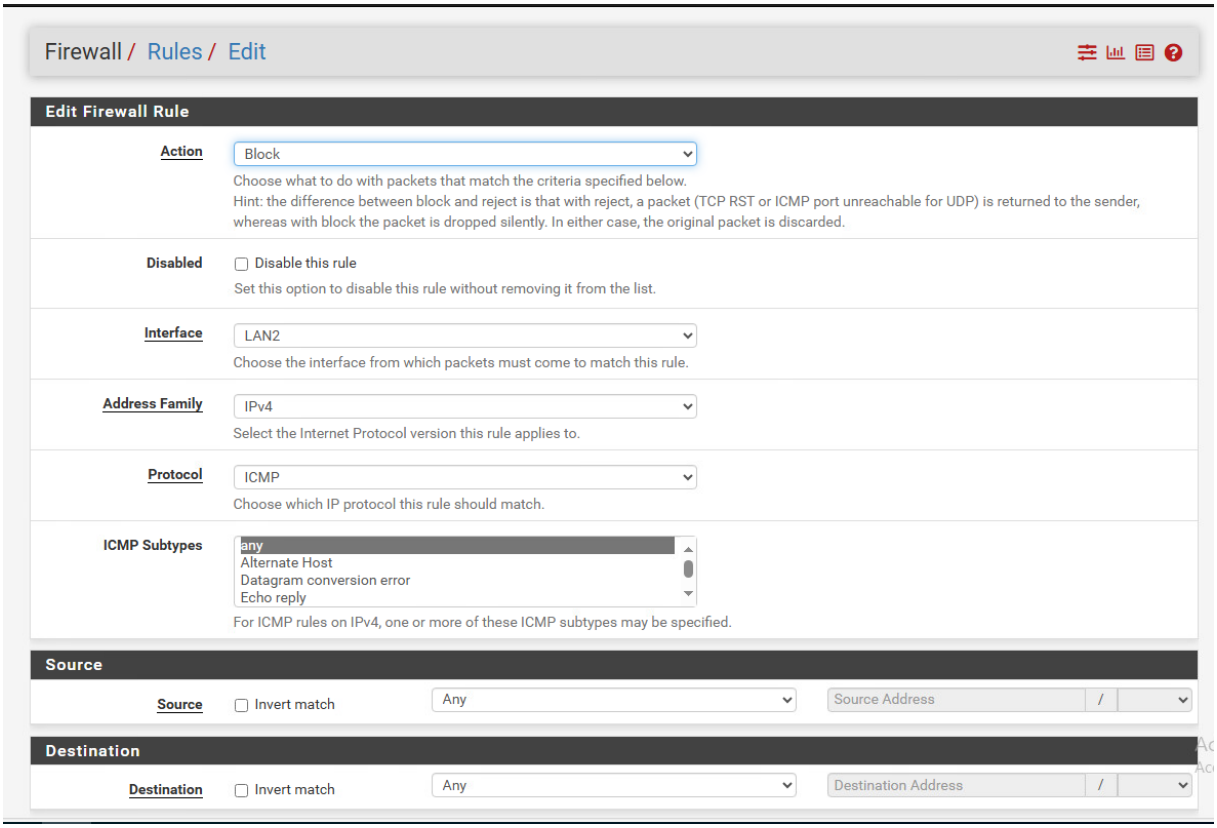

Wampserver
Start of services
Be patient!


Wampserver6
Ouvrir l'emplacement du fichier
Ouvrir
Exécuter en tant qu'administrateur
Résoudre les problèmes de compatibilité
Épingler à l'écran de démarrage
7-Zip
Analyser avec Microsoft Defender...
Épingler à la barre des tâches
Restaurer les versions précédentes
Envoyer vers
Couper
Copier
Coller
Créer un raccourci
Supprimer
Renommer
Propriétés


Extraire
www
Fichier
Accueil
Partage
Affichage
Outils de dossier compressé
Ce PC › Disque local (C:) › wamp64 › www ›
Rechercher dans : www
Accès rapide
Bureau
Documents
Images
Musique
Vidéos
www
OneDrive
Ce PC
Nom
Modifié le
Type
Taille
wamplangues 10/10/2024 13:47 Dossier de fichiers
wampthemes 10/10/2024 13:47 Dossier de fichiers
add_vhost.php 02/01/2024 10:06 Fichier PHP 49 Ko
favicon 31/12/2010 08:40 Icône 198 Ko
glpi-10.0.16.tgz 10/10/2024 13:50 Fichier TGZ 58 423 Ko
index.php 02/01/2024 09:57 Fichier PHP 29 Ko
test_sockets.php 21/09/2015 18:30 Fichier PHP 1 Ko
testmysql.php 17/06/2021 16:48 Fichier PHP
glpi-10.0.16 10/10/2024 13:51 Dossier de fichie
9 élément(s)
1 élément sélectionné 57,0 Mo
44% Extraction en cours C:\wamp64\www\glpi-10.0.16.tgz
Temps écoulé : 00:00:01
Temps restant : 00:00:01
Fichiers: 0
Taille totale : 58422 KB
Vitesse : 24 MB/s
Traité : 101 MB
Taille compressée: 26172 KB
Taux de compression : 25%
Extraction en cours
glpi-10.0.16.tar
Arrière-plan
Pause
Annuler
Tarifs
Partenaires
Télécharger
GLPI VERSIO
03/07/2024 – Archiv
Télécharge

Aujourd'hui (11)

vcredist_x64 (2)	10/10/2024 13:45	Application	7 032 Ko
vcredist_x86 (2)	10/10/2024 13:45	Application	6 358 Ko
vcredist_x64 (1)	10/10/2024 13:45	Application	7 019 Ko
vcredist_x86 (1)	10/10/2024 13:45	Application	6 401 Ko
vcredist_x86	10/10/2024 13:45	Application	8 783 Ko
vcredist_x64	10/10/2024 13:45	Application	10 037 Ko
wampserver3.3.5_x64	10/10/2024 13:43	Application	335 471 Ko
7z2408-x64	10/10/2024 13:26	Application	1 587 Ko
VC_redist.x64	10/10/2024 13:00	Application	24 905 Ko
VC_redist.x86	10/10/2024 13:00	Application	13 624 Ko
glpi-10.0.16.tgz	10/10/2024 13:50	Fichier TGZ	58 423 Ko



Installation des VMWare Tools sur Ubuntu (Linux) :

```
nextcloud@nextcloud-virtual-machine:~$ /usr/bin/vmware-toolbox-cmd -v
12.3.5.46049 (build-22544099)
```

```
nextcloud@nextcloud-virtual-machine:~$ sudo apt-get install open-vm-tools open-vm-tools-desktop
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
open-vm-tools est déjà la version la plus récente (2:12.3.5-3~ubuntu0.22.04.1).
Les NOUVEAUX paquets suivants seront installés :
  open-vm-tools-desktop
0 mis à jour, 1 nouvellement installés, 0 à enlever et 544 non mis à jour.
Il est nécessaire de prendre 139 ko dans les archives.
Après cette opération, 518 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
Réception de :1 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 open-vm-tools-desktop amd64 2:12.3.5-3~ubuntu0.22.04.1 [139 kB]
139 ko réceptionnés en 0s (1 273 ko/s)
Sélection du paquet open-vm-tools-desktop précédemment désélectionné.
(Lecture de la base de données... 165009 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../open-vm-tools-desktop_2%3a12.3.5-3~ubuntu0.22.04.1_amd64.deb ...
Dépaquetage de open-vm-tools-desktop (2:12.3.5-3~ubuntu0.22.04.1) ...
Paramétrage de open-vm-tools-desktop (2:12.3.5-3~ubuntu0.22.04.1) ...
```

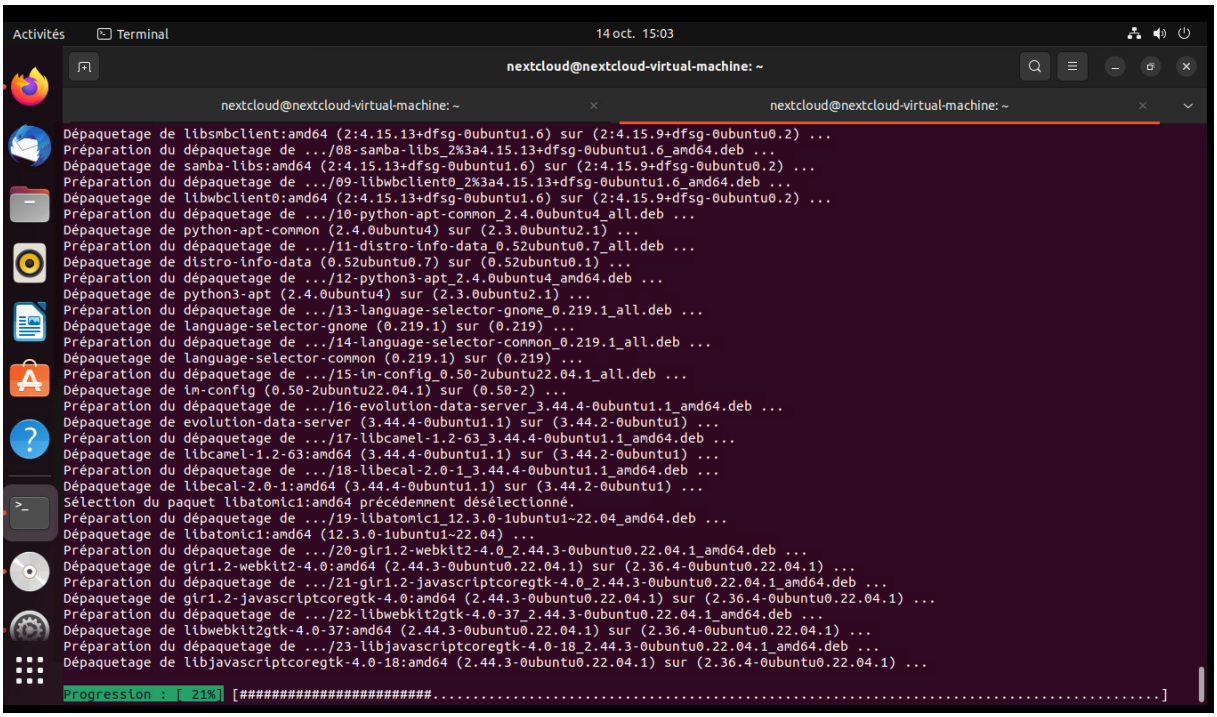
```
nextcloud@nextcloud-virtual-machine:~$ sudo apt-get install open-vm-tools
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  ethtool libmspack0 libxmlsec1-openssl zerofree
Paquets suggérés :
  open-vm-tools-desktop cloud-init open-vm-tools-containerinfo
  open-vm-tools-salt-minion
Les NOUVEAUX paquets suivants seront installés :
  ethtool libmspack0 libxmlsec1-openssl open-vm-tools zerofree
0 mis à jour, 5 nouvellement installés, 0 à enlever et 544 non mis à jour.
Il est nécessaire de prendre 1 087 ko dans les archives.
Après cette opération, 4 321 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
```

```
nextcloud@nextcloud-virtual-machine:~$ sudo apt-get update
[sudo] Mot de passe de nextcloud :
Réception de :1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Réception de :2 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Réception de :3 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Réception de :4 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Réception de :5 http://fr.archive.ubuntu.com/ubuntu jammy/main amd64 Packages [1 395 kB]
Réception de :6 http://fr.archive.ubuntu.com/ubuntu jammy/main i386 Packages [1 040 kB]
Réception de :7 http://fr.archive.ubuntu.com/ubuntu jammy/main Translation-fr [486 kB]
```

Installation NextCloud

sudo apt install php-ldap

```
nextcloud@nextcloud-virtual-machine:~$ cd /tmp
nextcloud@nextcloud-virtual-machine:/tmp$ wget https://download.nextcloud.com/server/releases/nextcloud-22.2.0.zip
--2024-10-14 15:12:19--  https://download.nextcloud.com/server/releases/nextcloud-22.2.0.zip
Résolution de download.nextcloud.com (download.nextcloud.com)… 5.9.202.145, 2a01:4f8:210:21c8::145
Connexion à download.nextcloud.com (download.nextcloud.com)|5.9.202.145|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 159315304 (152M) [application/zip]
Enregistre : ‘nextcloud-22.2.0.zip’

nextcloud-22.2.0.zip               39%[=======================>                                ]  60,71M  10,0MB/s    tps 9s
```




```
nextcloud@nextcloud-virtual-machine:~$    sudo apt update && sudo apt upgrade -y
[sudo] Mot de passe de nextcloud :
Atteint :1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
Atteint :2 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease
Atteint :3 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease
Atteint :4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Lecture des listes de paquets… 79%
```

```
nextcloud@nextcloud-virtual-machine:~$ sudo apt-get install wget unzip
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
unzip est déjà la version la plus récente (6.0-26ubuntu3.2).
unzip passé en « installé manuellement ».
wget est déjà la version la plus récente (1.21.2-2ubuntu1.1).
wget passé en « installé manuellement ».
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libflashrom1 libftdi1-2
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 28 non mis à jour.
nextcloud@nextcloud-virtual-machine:~$
```

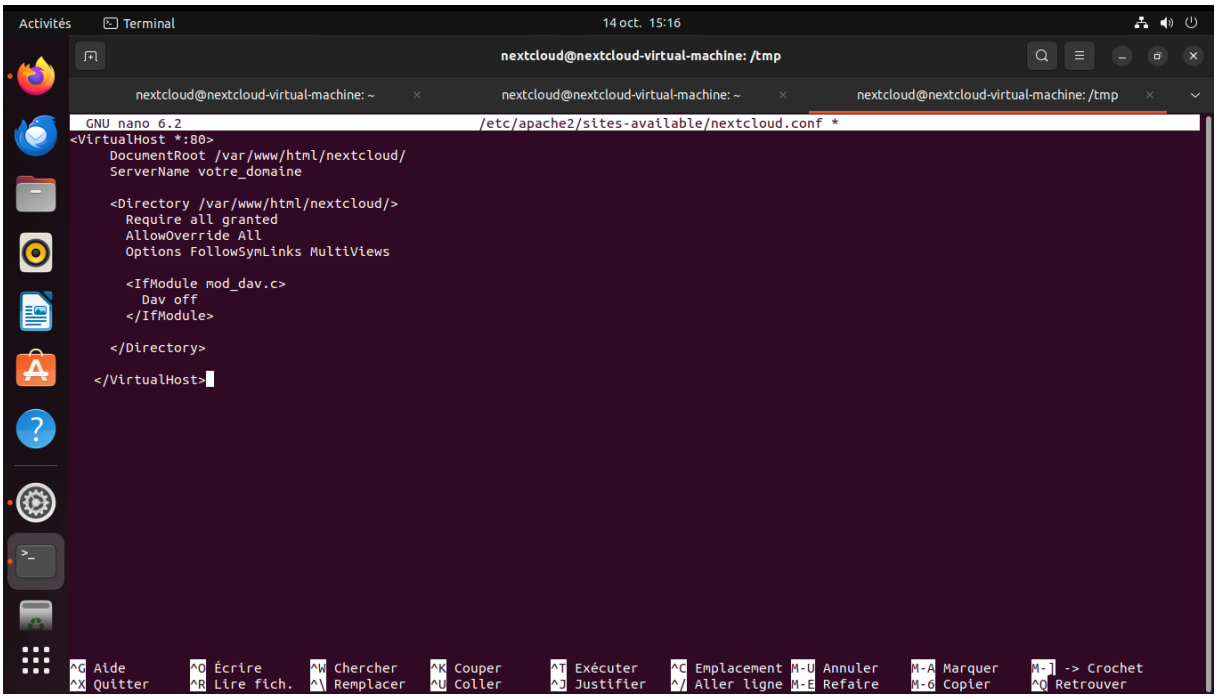
```
nextcloud@nextcloud-virtual-machine:/tmp$ sudo wget https://download.nextcloud.com/server/releases/latest.zip
--2024-10-14 17:14:55--  https://download.nextcloud.com/server/releases/latest.zip
Résolution de download.nextcloud.com (download.nextcloud.com)… 5.9.202.145, 2a01:4f8:210:21c8::145
Connexion à download.nextcloud.com (download.nextcloud.com)|5.9.202.145|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 218308106 (208M) [application/zip]
Enregistre : ‘latest.zip’

latest.zip                    29%[==================>                                  ]  62,05M  7,28MB/s    tps 22s
```

```
nextcloud@nextcloud-virtual-machine:~$ sudo apt-get install apache2 mariadb-server php8.1 php8.1-common php8.1-curl php8.1-gd php8.1-intl php
8.1-mbstring php8.1-xmlrpc php8.1-mysql php8.1-xml php8.1-cli php8.1-zip
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libflashrom1 libftdi1-2
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  apache2-bin apache2-data apache2-utils galera-4 gawk libapache2-mod-php8.1 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
  libcgi-fast-perl libcgi-pm-perl libconfig-inifiles-perl libdbd-mysql-perl libdbi-perl libfcgi-bin libfcgi-perl libfcgi0ldbl
  libhtml-template-perl libmariadb3 libmysqlclient21 libonig5 libsigsegv2 libsnappy1v5 libterm-readkey-perl liburing2 libxmlrpc-epi0
  libzip4 mariadb-client-10.6 mariadb-client-core-10.6 mariadb-common mariadb-server-10.6 mariadb-server-core-10.6 mysql-common php-common
  php8.1-opcache php8.1-readline socat
Paquets suggérés :
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser gawk-doc php-pear libmldbm-perl libnet-daemon-perl
  libsql-statement-perl libipc-sharedcache-perl mailx mariadb-test
Les NOUVEAUX paquets suivants seront installés :
  apache2 apache2-bin apache2-data apache2-utils galera-4 gawk libapache2-mod-php8.1 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libcgi-fast-perl libcgi-pm-perl libconfig-inifiles-perl libdbd-mysql-perl libdbi-perl libfcgi-bin libfcgi-perl
  libfcgi0ldbl libhtml-template-perl libmariadb3 libmysqlclient21 libonig5 libsigsegv2 libsnappy1v5 libterm-readkey-perl liburing2
  libxmlrpc-epi0 libzip4 mariadb-client-10.6 mariadb-client-core-10.6 mariadb-common mariadb-server mariadb-server-10.6
  mariadb-server-core-10.6 mysql-common php-common php8.1 php8.1-cli php8.1-common php8.1-curl php8.1-gd php8.1-intl php8.1-mbstring
  php8.1-mysql php8.1-opcache php8.1-readline php8.1-xml php8.1-xmlrpc php8.1-zip socat
0 mis à jour, 51 nouvellement installés, 0 à enlever et 28 non mis à jour.
Il est nécessaire de prendre 27,0 Mo dans les archives.
Après cette opération, 198 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
```

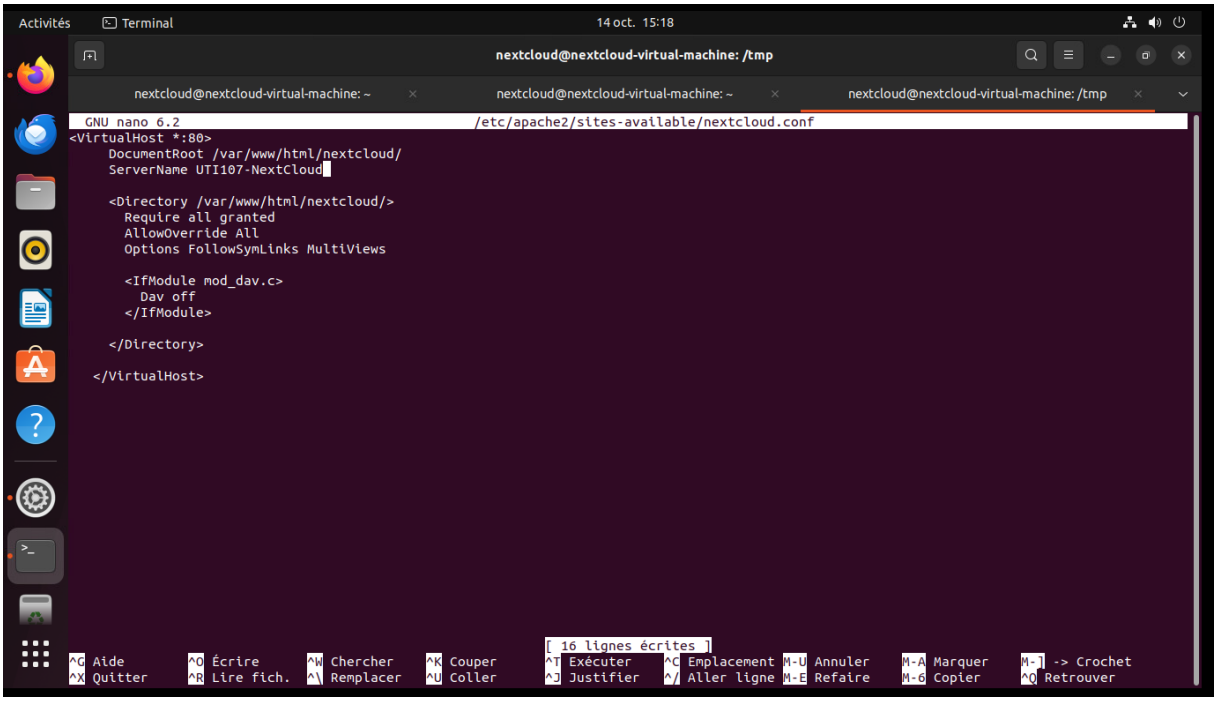
```
  Il est nécessaire de prendre 798 Mo dans les archives.
  Après cette opération, 291 Mo d'espace disque supplémentaires seront utilisés.
  Souhaitez-vous continuer ? [O/n] O
  Réception de :1 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libc6-dbg amd64 2.35-0ubuntu3.8 [13,8 MB]
  1% [1 libc6-dbg 10,7 MB/13,8 MB 78%]
```

```
su: Échec de l'authentification
nextcloud@nextcloud-virtual-machine:~$ sudo apt-get update
[sudo] Mot de passe de nextcloud :
Réception de :1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease [270 kB]
Réception de :2 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Réception de :3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Réception de :4 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Réception de :5 http://fr.archive.ubuntu.com/ubuntu jammy/main i386 Packages [1 040 kB]
Réception de :6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1 854 kB]
Réception de :7 http://fr.archive.ubuntu.com/ubuntu jammy/main amd64 Packages [1 395 kB]
Réception de :8 http://fr.archive.ubuntu.com/ubuntu jammy/main Translation-fr [486 kB]
Réception de :9 http://fr.archive.ubuntu.com/ubuntu jammy/main Translation-en [510 kB]
Réception de :10 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [547 kB]
Réception de :11 http://fr.archive.ubuntu.com/ubuntu jammy/main amd64 DEP-11 Metadata [423 kB]
Réception de :12 http://fr.archive.ubuntu.com/ubuntu jammy/main DEP-11 48x48 Icons [100,0 kB]
Réception de :13 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [300 kB]
Réception de :14 http://fr.archive.ubuntu.com/ubuntu jammy/main DEP-11 64x64 Icons [148 kB]
Réception de :15 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [43,2 kB]
Réception de :16 http://security.ubuntu.com/ubuntu jammy-security/main DEP-11 48x48 Icons [16,9 kB]
Réception de :17 http://security.ubuntu.com/ubuntu jammy-security/main DEP-11 64x64 Icons [26,5 kB]
Réception de :18 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [13,3 kB]
Réception de :19 http://security.ubuntu.com/ubuntu jammy-security/restricted i386 Packages [37,7 kB]
Réception de :20 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [2 451 kB]
Réception de :21 http://fr.archive.ubuntu.com/ubuntu jammy/main DEP-11 64x64@2 Icons [15,8 kB]
Réception de :22 http://fr.archive.ubuntu.com/ubuntu jammy/main amd64 c-n-f Metadata [30,3 kB]
Réception de :23 http://fr.archive.ubuntu.com/ubuntu jammy/restricted i386 Packages [30,4 kB]
```

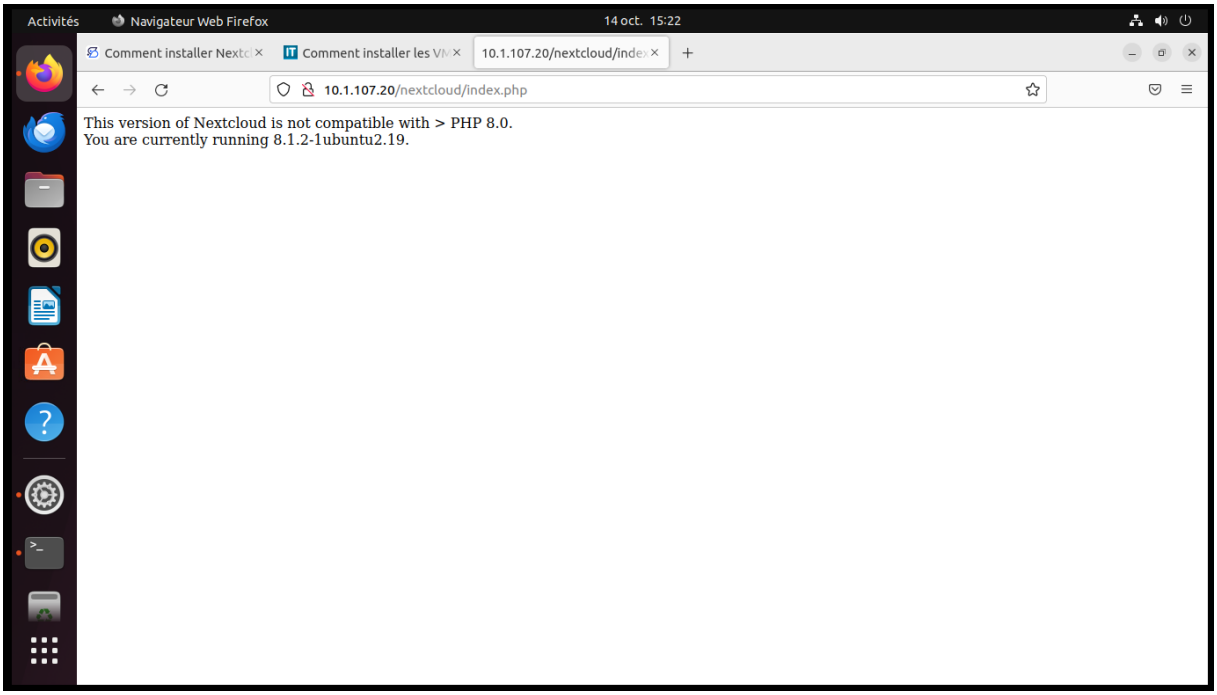
```
nextcloud@nextcloud-virtual-machine:/tmp$  sudo mv nextcloud /var/www/html/nextcloud
[sudo] Mot de passe de nextcloud :
nextcloud@nextcloud-virtual-machine:/tmp$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.18-MariaDB-0ubuntu0.22.04.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE nextclouddb;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]>    GRANT ALL ON nextclouddb.* TO 'nextclouduser'@'localhost' IDENTIFIED BY 'votre_mot_de_passe';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]>    FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]>    EXIT;
Bye
nextcloud@nextcloud-virtual-machine:/tmp$
nextcloud@nextcloud-virtual-machine:/tmp$ sudo nano /etc/apache2/sites-available/nextcloud.conf
nextcloud@nextcloud-virtual-machine:/tmp$
```

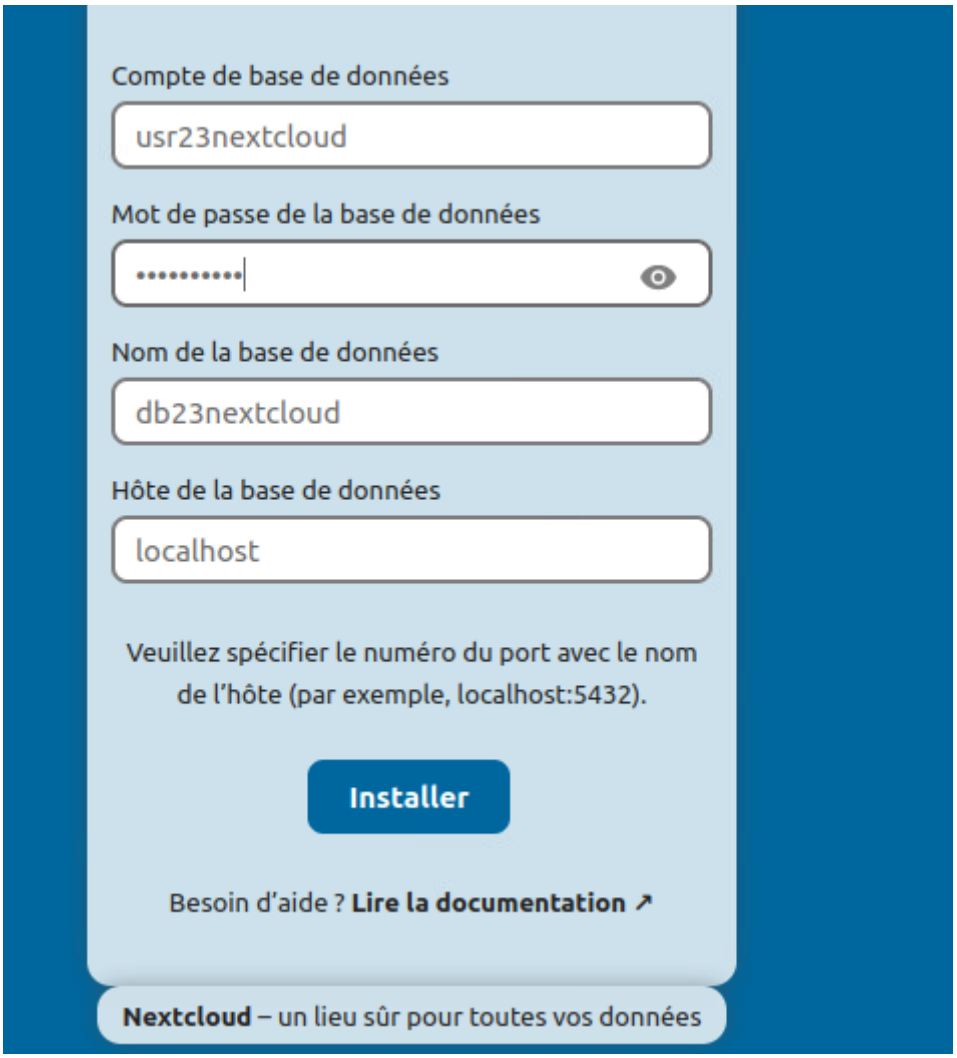


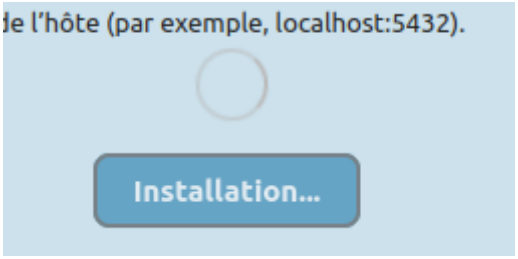

```
nextcloud@nextcloud-virtual-machine:/tmp$
nextcloud@nextcloud-virtual-machine:/tmp$ sudo nano /etc/apache2/sites-available/nextcloud.conf
nextcloud@nextcloud-virtual-machine:/tmp$
nextcloud@nextcloud-virtual-machine:/tmp$ sudo nano /etc/apache2/sites-available/nextcloud.conf
nextcloud@nextcloud-virtual-machine:/tmp$
nextcloud@nextcloud-virtual-machine:/tmp$ sudo a2ensite nextcloud
Enabling site nextcloud.
To activate the new configuration, you need to run:
  systemctl reload apache2
nextcloud@nextcloud-virtual-machine:/tmp$ sudo a2enmod rewrite headers env dir mime
Enabling module rewrite.
Enabling module headers.
Module env already enabled
Module dir already enabled
Module mime already enabled
To activate the new configuration, you need to run:
  systemctl restart apache2
nextcloud@nextcloud-virtual-machine:/tmp$ sudo systemctl restart apache2
nextcloud@nextcloud-virtual-machine:/tmp$
```



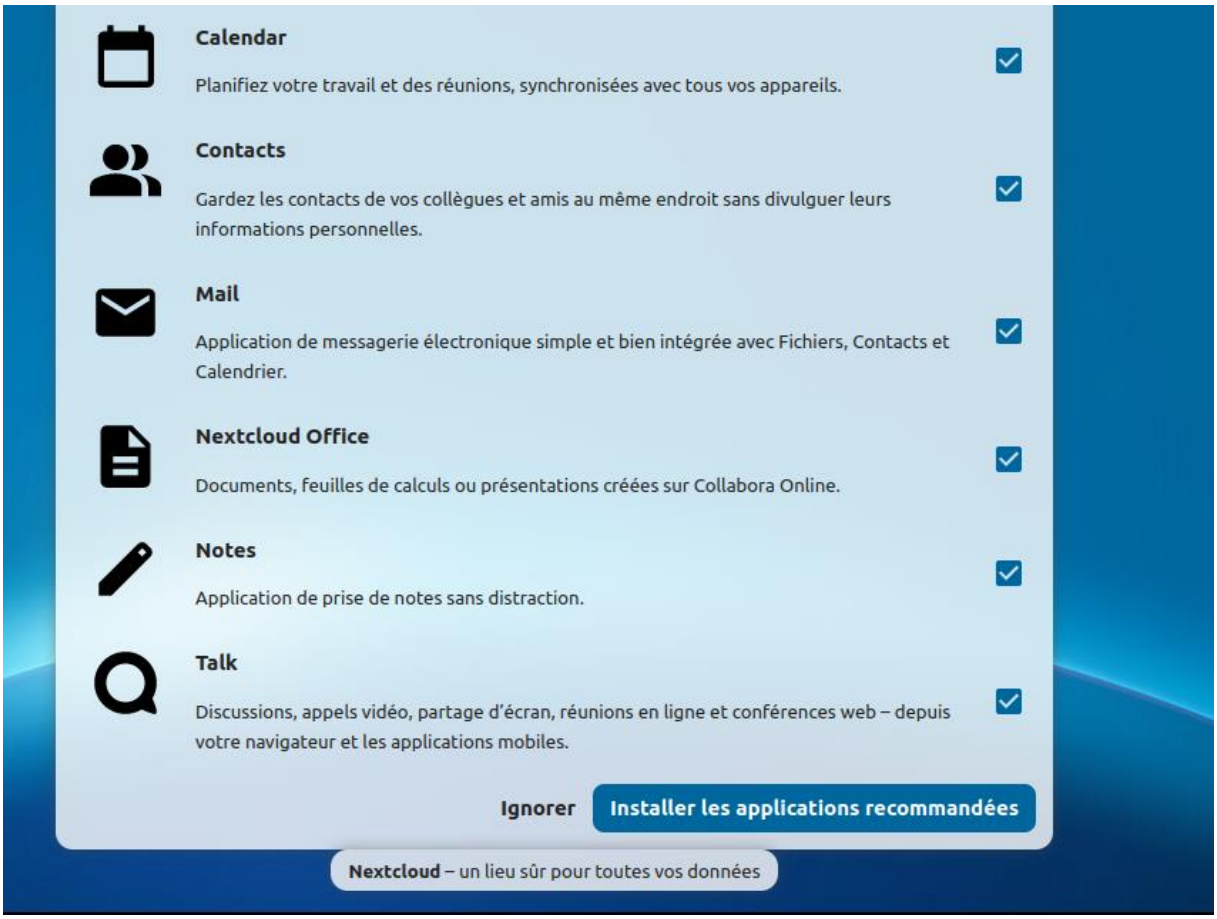
```
nextcloud@nextcloud-virtual-machine:/tmp$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-10-14 15:16:54 CEST; 17s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 52752 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 52757 (apache2)
      Tasks: 6 (limit: 4629)
     Memory: 14.6M
        CPU: 89ms
     CGroup: /system.slice/apache2.service
             ├─52757 /usr/sbin/apache2 -k start
             ├─52758 /usr/sbin/apache2 -k start
             ├─52759 /usr/sbin/apache2 -k start
             ├─52760 /usr/sbin/apache2 -k start
             ├─52761 /usr/sbin/apache2 -k start
             └─52762 /usr/sbin/apache2 -k start

oct. 14 15:16:54 nextcloud-virtual-machine systemd[1]: apache2.service: Found left-over process 52616 (apache2) in control group while start>
oct. 14 15:16:54 nextcloud-virtual-machine systemd[1]: This usually indicates unclean termination of a previous run, or service implementati>
oct. 14 15:16:54 nextcloud-virtual-machine systemd[1]: Starting The Apache HTTP Server...
oct. 14 15:16:54 nextcloud-virtual-machine apachectl[52755]: AH00558: apache2: Could not reliably determine the server's fully qualified dom>
oct. 14 15:16:54 nextcloud-virtual-machine systemd[1]: Started The Apache HTTP Server.
lines 1-22/22 (END)
```



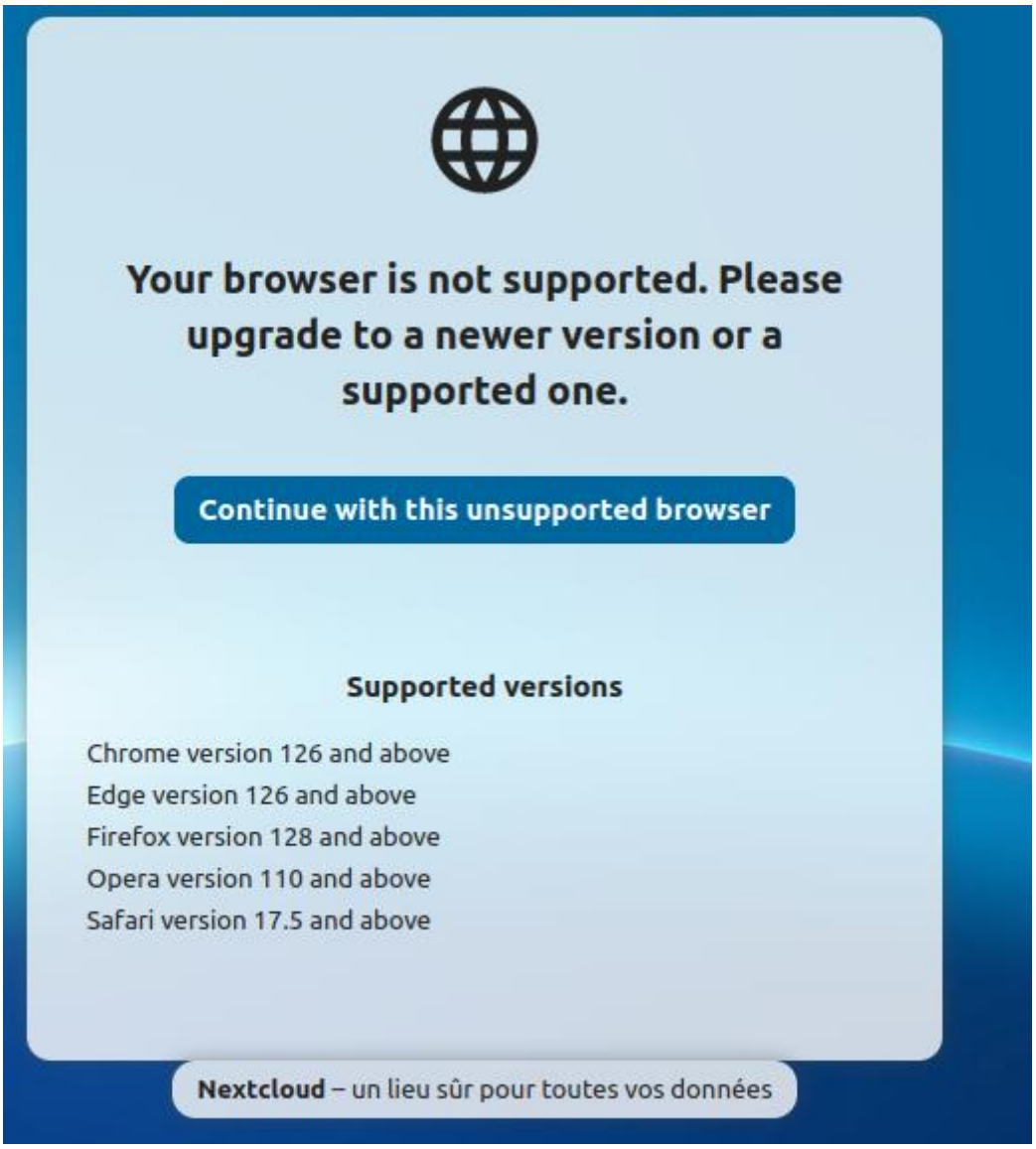

Compte de base de données
usr23nextcloud
Mot de passe de la base de données
Nom de la base de données
db23nextcloud
Hôte de la base de données
localhost
Veuillez spécifier le numéro du port avec le nom de l'hôte (par exemple, localhost:5432).
Installer
Besoin d'aide ? Lire la documentation ↗
Nextcloud – un lieu sûr pour toutes vos données

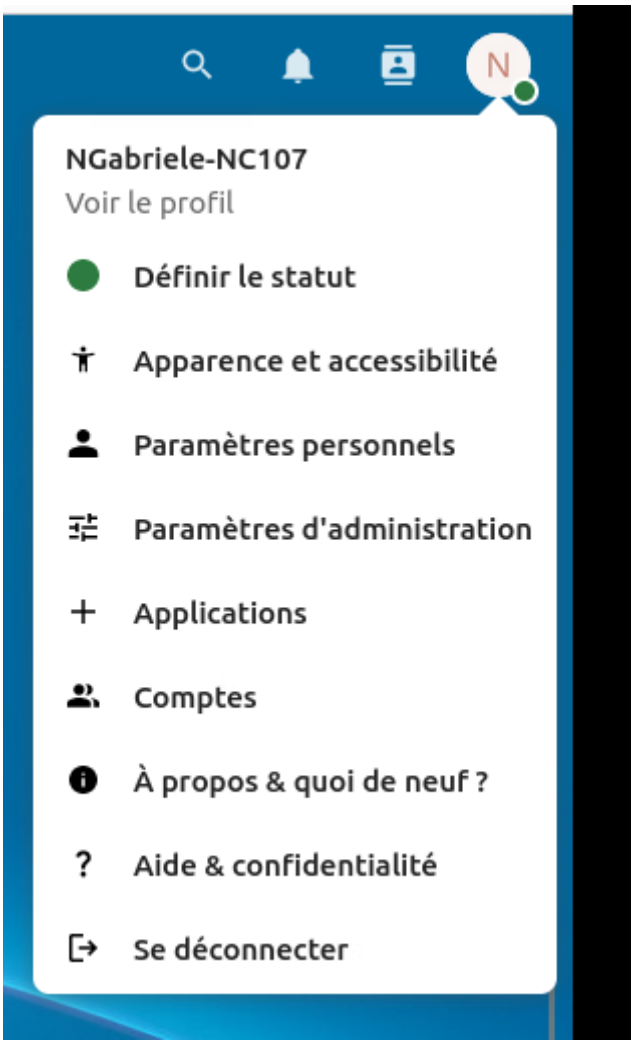

de l'hôte (par exemple, localhost:5432).
Installation...

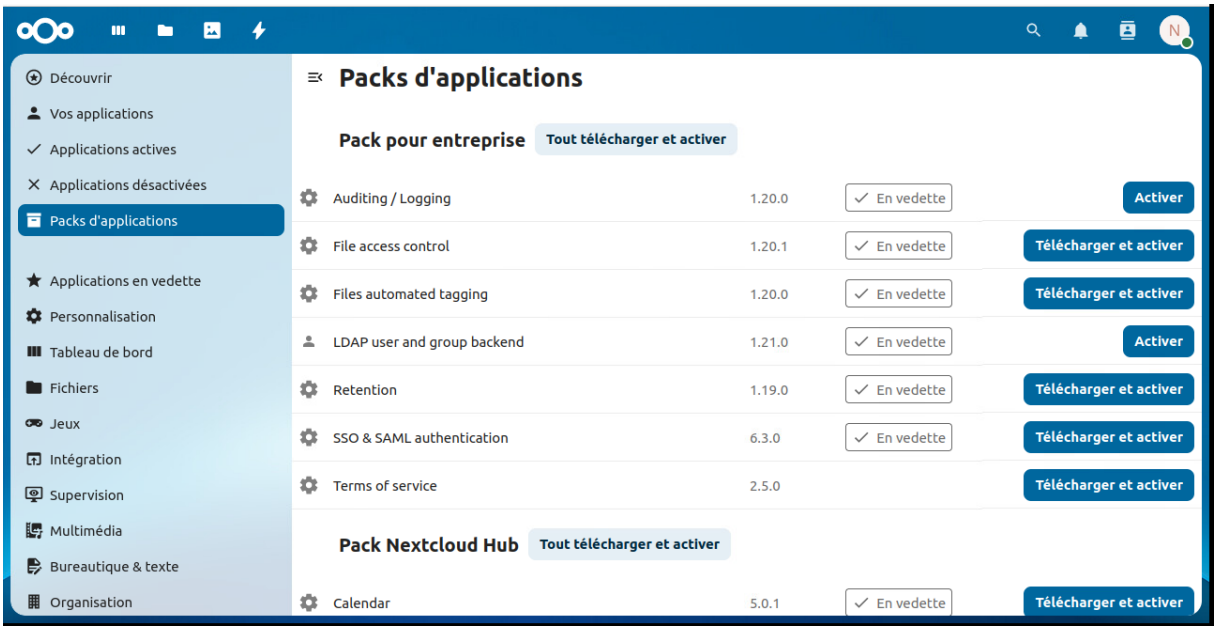

Créer un **compte administrateur**
S'identifier
NGabriele-NC107
Mot de passe
••••••••••••••
Stockage & base de données
Répertoire des données
/var/www/html/nextcloud/data
Configurer la base de données
Seul(e) MySQL/MariaDB est disponible. Installez et activez les modules PHP additionnels adéquats pour choisir d'autres types de base de données.
Consultez la documentation pour plus de détails. ↗
Compte de base de données

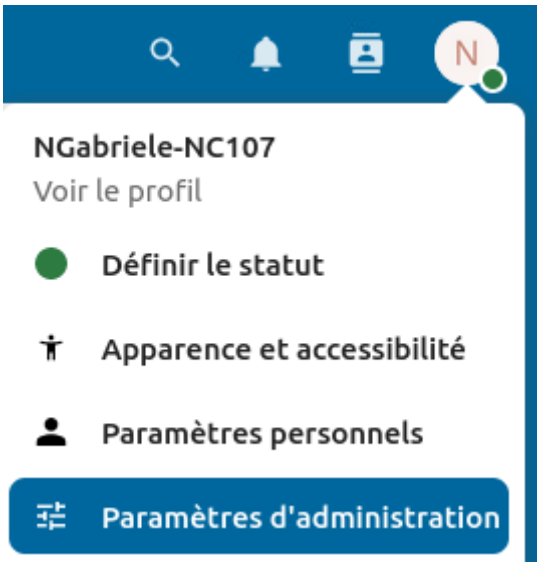

Calendar
Planifiez votre travail et des réunions, synchronisées avec tous vos appareils.
Contacts
Gardez les contacts de vos collègues et amis au même endroit sans divulguer leurs informations personnelles.
Mail
Application de messagerie électronique simple et bien intégrée avec Fichiers, Contacts et Calendrier.
Nextcloud Office
Documents, feuilles de calculs ou présentations créées sur Collabora Online.
Notes
Application de prise de notes sans distraction.
Talk
Discussions, appels vidéo, partage d'écran, réunions en ligne et conférences web – depuis votre navigateur et les applications mobiles.
Ignorer
Installer les applications recommandées
Nextcloud – un lieu sûr pour toutes vos données

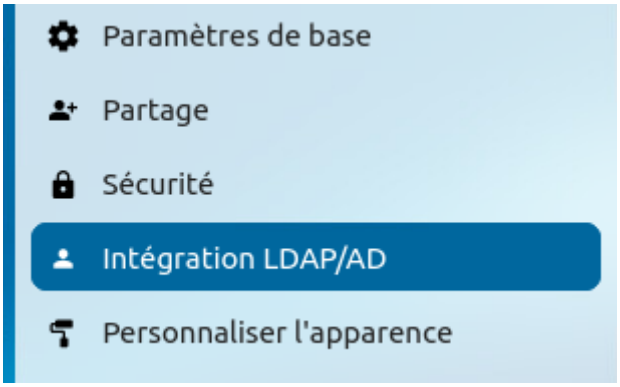

Nextcloud
Une plateforme de collaboration qui vous donne le contrôle
Confidentialité
Hébergez vos données et vos fichiers où vous voulez.
Productivité
Collaborez et communiquez sur n'importe quelle plateforme.
Interopérabilité
Importez et exportez ce que vous voulez avec des standards ouverts.
Communauté
Profitez des améliorations continues d'une communauté open-source dynamique.
Ce Nextcloud est à la version 30.0.0
Quoi de neuf ? →
Nextcloud sur tous vos appareils →


Your browser is not supported. Please upgrade to a newer version or a supported one.
Continue with this unsupported browser
Supported versions
Chrome version 126 and above
Edge version 126 and above
Firefox version 128 and above
Opera version 110 and above
Safari version 17.5 and above
Nextcloud – un lieu sûr pour toutes vos données

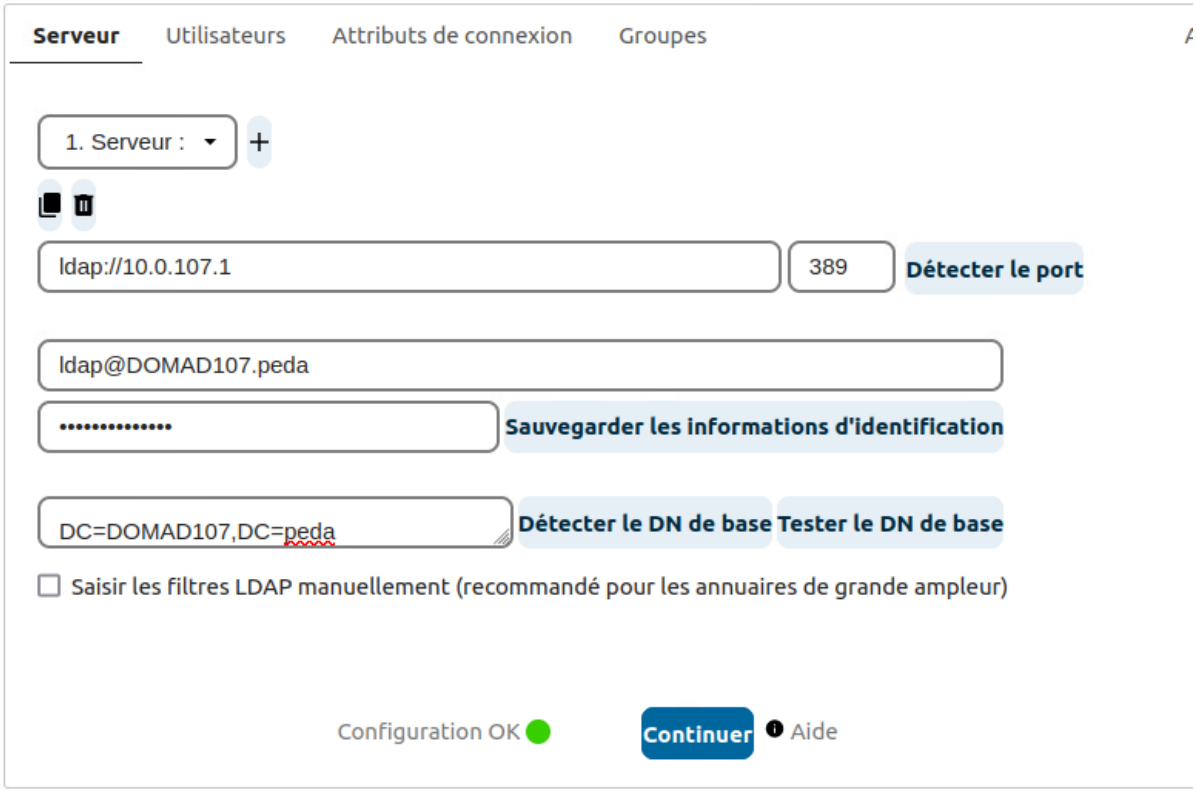

N
NGabriele-NC107
Voir le profil
Définir le statut
Apparence et accessibilité
Paramètres personnels
Paramètres d'administration
Applications
Comptes
À propos & quoi de neuf ?
Aide & confidentialité
Se déconnecter

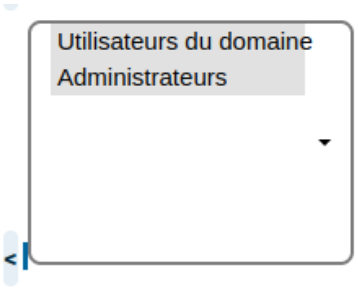

Découvrir
Vos applications
Applications actives
Applications désactivées
Packs d'applications
Applications en vedette
Personnalisation
Tableau de bord
Fichiers
Jeux
Intégration
Supervision
Multimédia
Bureautique & texte
Organisation
Packs d'applications
Pack pour entreprise
Tout télécharger et activer
Auditing / Logging 1.20.0 En vedette Activer
File access control 1.20.1 En vedette Télécharger et activer
Files automated tagging 1.20.0 En vedette Télécharger et activer
LDAP user and group backend 1.21.0 En vedette Activer
Retention 1.19.0 En vedette Télécharger et activer
SSO & SAML authentication 6.3.0 En vedette Télécharger et activer
Terms of service 2.5.0 Télécharger et activer
Pack Nextcloud Hub
Tout télécharger et activer
Calendar 5.0.1 En vedette Télécharger et activer


N
NGabriele-NC107
Voir le profil
Définir le statut
Apparence et accessibilité
Paramètres personnels
Paramètres d'administration


Paramètres de base
Partage
Sécurité
Intégration LDAP/AD
Personnaliser l'apparence

Intégration LDAP/AD





↓ Modifier la requête LDAP

Filtre LDAP : (&(|(objectclass=person))
(|(|(memberof=CN=Administrateurs,CN=Builtin,DC=DOMAD107,DC=peda)
(primaryGroupID=544))
(|(memberof=CN=Utilisateurs du
domaine,CN=Users,DC=DOMAD107,DC=peda)
(primaryGroupID=513))))

À la connexion, Nextcloud cherchera l'utilisateur sur la base des attributs suivant :

Nom d'utilisateur LDAP/AD : ☑

Adresse e-mail LDAP/AD : ☑

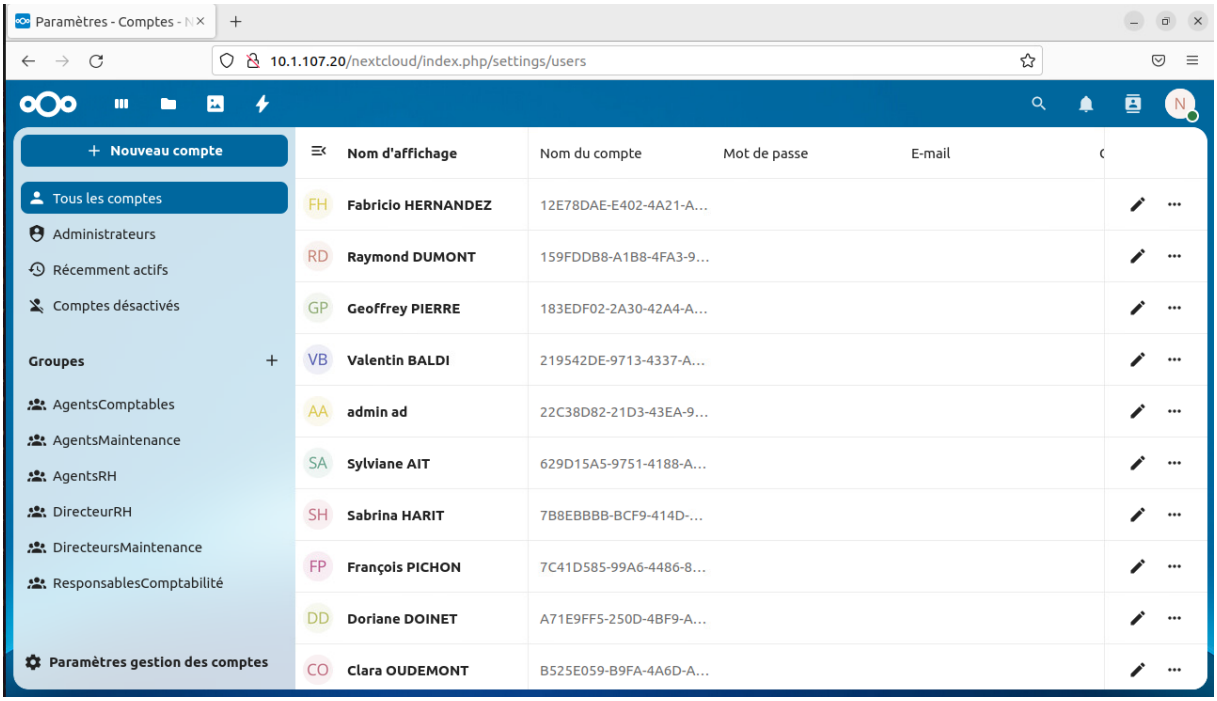
ResponsablesComptabilité
AgentsRH
AgentsMaintenance
AgentsComptables
DirecteursMaintenance
DirecteursRH

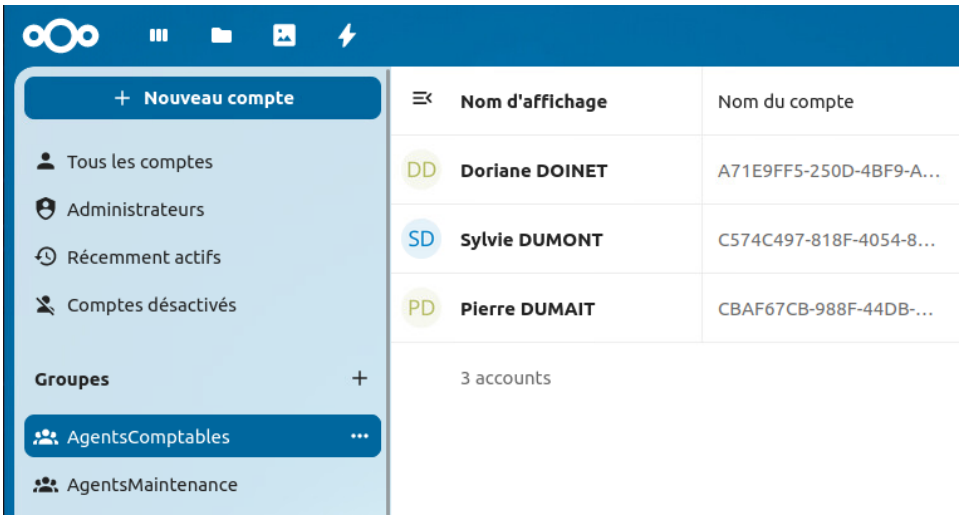
↓ Modifier la requête LDAP

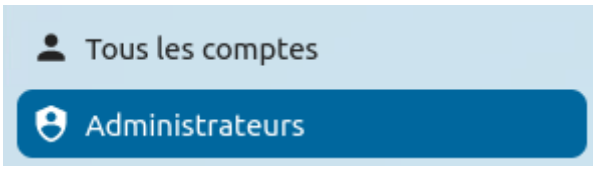
Filtre LDAP : (|(cn=AgentsRH)(cn=AgentsMaintenance)
(cn=AgentsComptables)
(cn=DirecteursMaintenance)
(cn=DirecteursRH)
(cn=ResponsablesComptabilité))

Vérifier les paramètres et compter les groupes 6 groupes trouvés

Configuration OK **Retour**

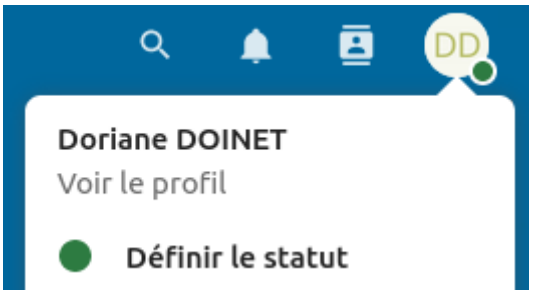


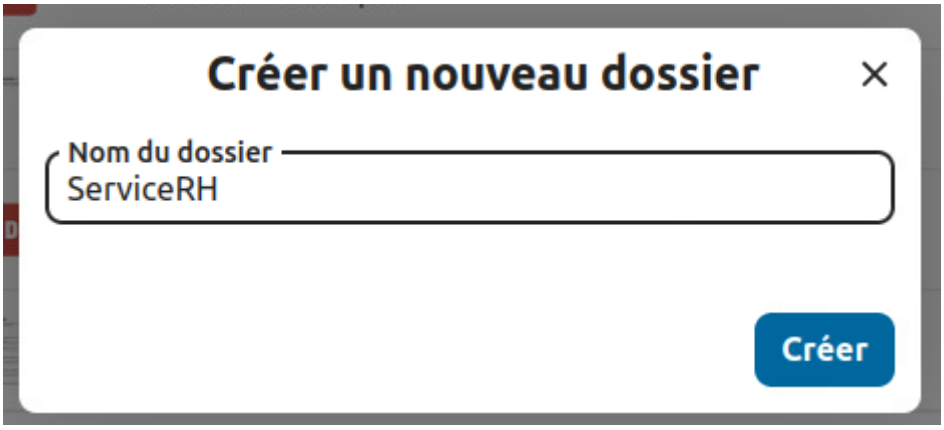

Nouveau compte
Tous les comptes
Administrateurs
Récemment actifs
Comptes désactivés
Groupes
AgentsComptables
AgentsMaintenance
Nom d'affichage
Nom du compte
DD
Doriane DOINET
A71E9FF5-250D-4BF9-A...
SD
Sylvie DUMONT
C574C497-818F-4054-8...
PD
Pierre DUMAIT
CBAF67CB-988F-44DB-...
3 accounts

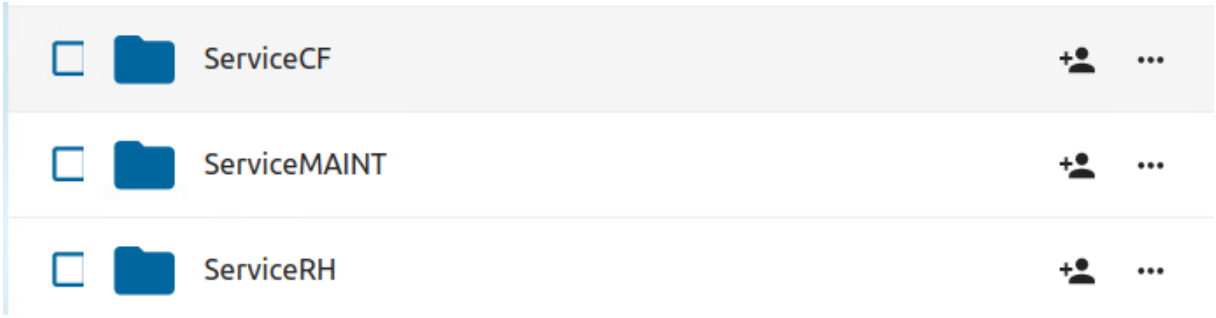

Tous les comptes
Administrateurs

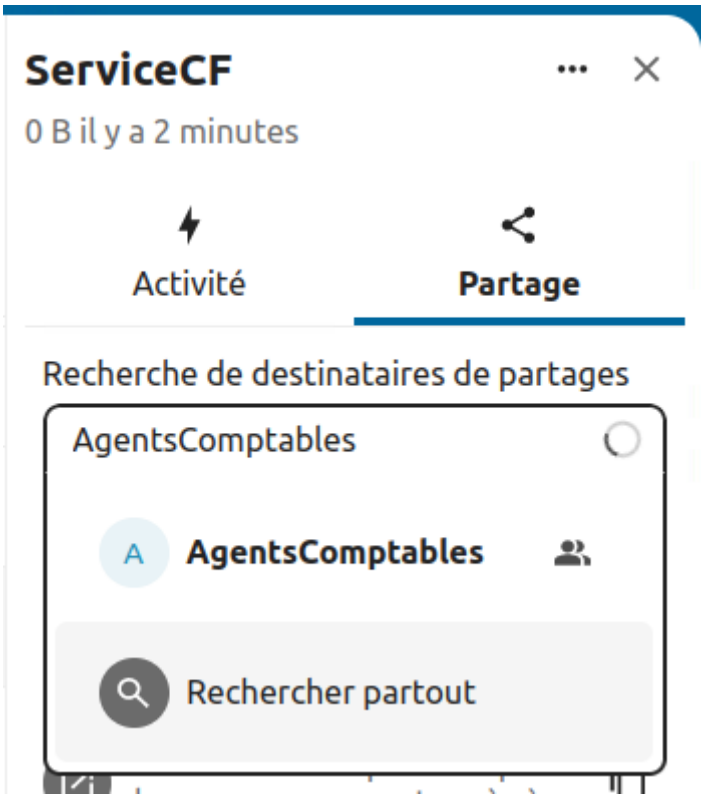

Nom d'affichage
Nom du compte
Mot de passe
E-mail
NGabriele-NC107
NGabriele-NC107

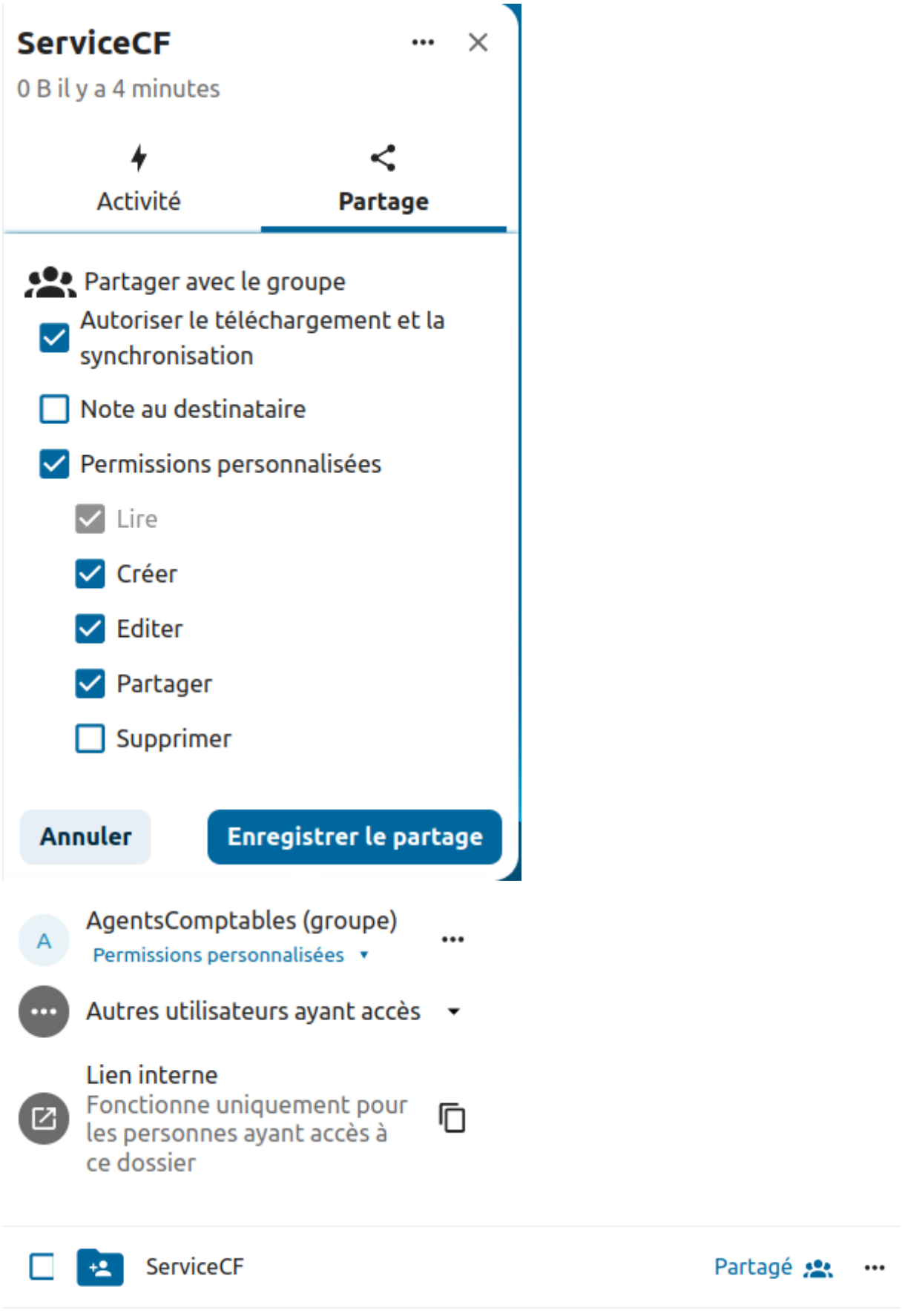

Se connecter à Nextcloud
Nom d'utilisateur ou adresse e-mail
ddoinet
Mot de passe
Se connecter
Mot de passe oublié ?


DD
Doriane DOINET
Voir le profil
Définir le statut


Créer un nouveau dossier
Nom du dossier
ServiceRH
Créer


ServiceCF
ServiceMAINT
ServiceRH


ServiceCF
0 B il y a 2 minutes
Activité
Partage
Recherche de destinataires de partages
AgentsComptables
A
AgentsComptables
Rechercher partout


ServiceCF
0 B il y a 4 minutes
Activité
Partage
Partager avec le groupe
Autoriser le téléchargement et la synchronisation
Note au destinataire
Permissions personnalisées
Lire
Créer
Editer
Partager
Supprimer
Annuler
Enregistrer le partage
A
AgentsComptables (groupe)
Permissions personnalisées
Autres utilisateurs ayant accès
Lien interne
Fonctionne uniquement pour les personnes ayant accès à ce dossier
ServiceCF
Partagé

Pour vérifier la communication en cas de base erronée, j'ai installé ldap-utils en utilisant la commande :

Sudo apt install ldap-utils

```
nextcloud@nextcloud-virtual-machine:~$ sudo apt install ldap-utils
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libflashrom1 libftdi1-2
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les NOUVEAUX paquets suivants seront installés :
  ldap-utils
0 mis à jour, 1 nouvellement installés, 0 à enlever et 34 non mis à jour.
Il est nécessaire de prendre 147 ko dans les archives.
Après cette opération, 711 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ldap-utils amd64 2.5.18+dfsg-0ubuntu0.22.04.2 [147 kB]
 [.....................................................................]
Sélection du paquet ldap-utils précédemment désélectionné.
(Lecture de la base de données... 205473 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../ldap-utils_2.5.18+dfsg-0ubuntu0.22.04.2_amd64.
deb ...
Dépaquetage de ldap-utils (2.5.18+dfsg-0ubuntu0.22.04.2) ...
Paramétrage de ldap-utils (2.5.18+dfsg-0ubuntu0.22.04.2) ...
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
```

ldapsearch -x -H ldap://10.0.107.1 -D "ldap@DOMAD107.peda" -w "GABAdmin-3892" -s base b ""

```
nextcloud@nextcloud-virtual-machine:~$ ldapsearch -x -H ldap://10.0.107.1 -D "ldap@DOMAD107.peda" -w "GABAdmin-3892" -s base b ""
ldap_bind: Invalid credentials (49)
        additional info: 80090308: LdapErr: DSID-0C09050F, comment: AcceptSecurityContext error, data 52e, v4563
```

```
PS C:\Users\Administrateur> Get-ADDomain


AllowedDNSSuffixes                : {}
ChildDomains                      : {}
ComputersContainer                : CN=Computers,DC=DOMAD107,DC=peda
DeletedObjectsContainer           : CN=Deleted Objects,DC=DOMAD107,DC=peda
DistinguishedName                 : DC=DOMAD107,DC=peda
DNSRoot                           : DOMAD107.peda
DomainControllersContainer        : OU=Domain Controllers,DC=DOMAD107,DC=peda
DomainMode                        : Windows2016Domain
DomainSID                         : S-1-5-21-3718978507-2797367783-1451696534
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=DOMAD107,DC=peda
Forest                            : DOMAD107.peda
InfrastructureMaster              : SRV1-DC107.DOMAD107.peda
LastLogonReplicationInterval      :
LinkedGroupPolicyObjects          : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=DOMAD107,DC=peda}
LostAndFoundContainer             : CN=LostAndFound,DC=DOMAD107,DC=peda
ManagedBy                         :
Name                              : DOMAD107
NetBIOSName                       : DOMAD107
ObjectClass                       : domainDNS
ObjectGUID                        : ba2591db-cab3-4468-b2c6-0bbf43ddec2f
ParentDomain                      :
PDCEmulator                       : SRV1-DC107.DOMAD107.peda
PublicKeyRequiredPasswordRolling  : True
QuotasContainer                   : CN=NTDS Quotas,DC=DOMAD107,DC=peda
ReadOnlyReplicaDirectoryServers   : {}
ReplicaDirectoryServers           : {SRV1-DC107.DOMAD107.peda}
RIDMaster                         : SRV1-DC107.DOMAD107.peda
SubordinateReferences             : {DC=ForestDnsZones,DC=DOMAD107,DC=peda, DC=DomainDnsZones,DC=DOMAD107,DC=peda, CN=Configuration,DC=DOMAD107,DC=peda}
SystemsContainer                  : CN=System,DC=DOMAD107,DC=peda
UsersContainer                    : CN=Users,DC=DOMAD107,DC=peda
```

Installation de GLPI

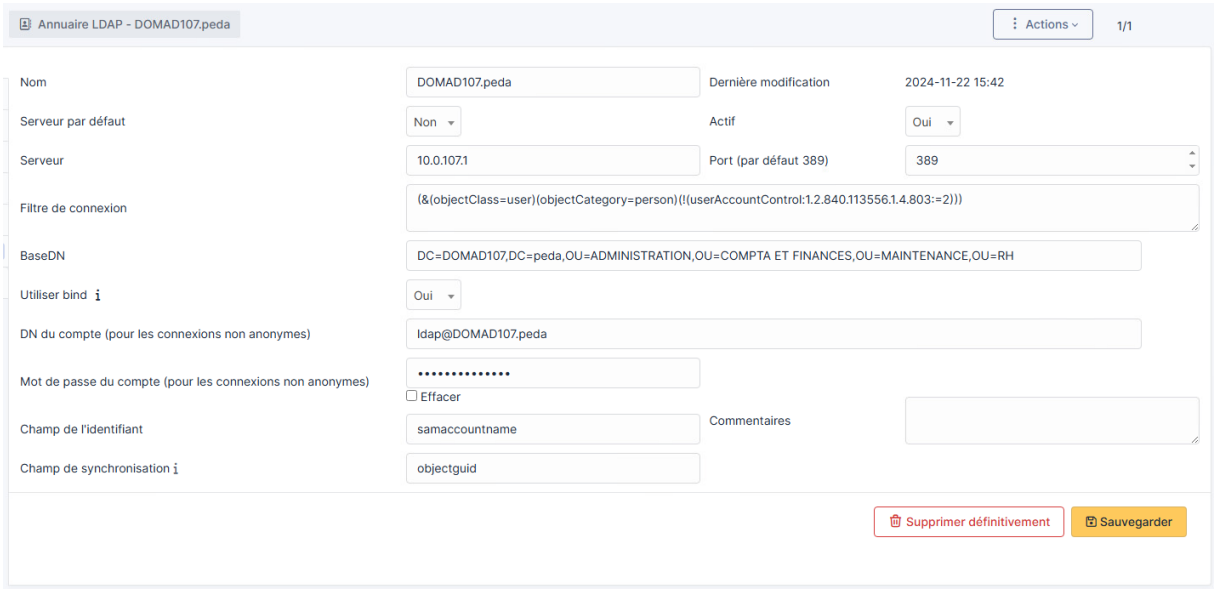
sudo apt-get update && sudo apt-get upgrade

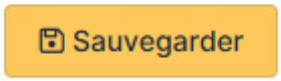
sudo apt-get install apache2 php mariadb-server

sudo apt-get install php-xml php-common php-json php-mysql php-mbstring php-curl php-gd php-intl php-zip php-bz2 php-imap php-apcu

sudo apt-get install php-ldap

sudo mysql_secure_installation


Annuaire LDAP - DOMAD107.peda
Actions
1/1
Nom
DOMAD107.peda
Dernière modification
2024-11-22 15:42
Serveur par défaut
Non
Actif
Oui
Serveur
10.0.107.1
Port (par défaut 389)
389
Filtre de connexion
(&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
BaseDN
DC=DOMAD107,DC=peda,OU=ADMINISTRATION,OU=COMPTA ET FINANCES,OU=MAINTENANCE,OU=RH
Utiliser bind
Oui
DN du compte (pour les connexions non anonymes)
ldap@DOMAD107.peda
Mot de passe du compte (pour les connexions non anonymes)
Effacer
Champ de l'identifiant
samaccountname
Commentaires
Champ de synchronisation
objectguid
Supprimer définitivement
Sauvegarder


Sauvegarder

Conclusion

Cet atelier m'a permis de développer des compétences cruciales en administration réseau et en sécurité informatique, notamment dans la gestion et la configuration d'un pare-feu virtuel avec PfSense. Cette solution open-source, à la fois puissante et flexible, m'a offert l'opportunité de mieux appréhender les mécanismes nécessaires pour protéger et optimiser une infrastructure réseau. J'ai également appris à concevoir des règles de pare-feu optimisées grâce à l'utilisation d'alias, ce qui simplifie la gestion des configurations complexes tout en renforçant leur efficacité.

L'approfondissement des configurations m'a permis de mieux comprendre les enjeux liés à la sécurité des communications internes et externes. J'ai découvert l'utilité d'outils comme Snort pour la détection d'intrusions, Squid pour le proxy, et ClamAV pour la protection antivirus, des solutions qui se complètent pour offrir une défense robuste des infrastructures réseau. En maîtrisant ces technologies, j'ai pu identifier et mettre en œuvre des mesures pour sécuriser les services critiques, limiter les accès indésirables et prévenir des attaques comme les attaques de type Man-in-the-Middle (MITM).

Cependant, certaines difficultés ont marqué ce travail, notamment la gestion et l'optimisation des règles de pare-feu. Il a fallu trouver un équilibre entre sécurité et performance, tout en évitant les conflits qui pourraient compromettre le fonctionnement du réseau. La création d'alias s'est avérée être un outil clé pour simplifier ces configurations. Une autre difficulté a été la migration des services HTTP vers HTTPS, un processus délicat qui exige de maintenir la compatibilité tout en assurant une sécurité accrue.

Malgré ces défis, cet atelier m'a permis d'acquérir une compréhension approfondie de la configuration des pare-feu open-source, ainsi que des compétences avancées en gestion des règles réseau. J'ai également intégré des outils tiers pour surveiller et protéger efficacement les infrastructures. Ces connaissances pratiques et techniques constituent un bagage solide que je pourrai appliquer dans des contextes professionnels variés pour sécuriser et optimiser des systèmes informatiques.

Webographie