

NATHAN GABRIELE

# **AP\_PFSENSE\_PARE- FEU\_MISE\_EN\_PLACE\_RÉSEAU**

---

# Sommaire

Introduction .....	1
Schéma Réseau .....	2
Schéma Réseau .....	3
Mise en place et Installation du Pfsense (Pare-Feu).....	3
Paramètres et Configuration.....	12
Configuration des règles de pare-feu .....	23
Redirecteurs DNS .....	32
Création d'Alias .....	34
Par port.....	34
Par IP .....	35
Configuration des transmission de ports .....	36
Configuration des services et applications tiers.....	37
LDAP.....	37
Création et configuration de la machine cliente .....	42
SNMP .....	42
DHCP .....	42
DHCP Relay.....	43
Configuration du poste client sous windows 10 en DHCP .....	43
Mise en place du proxy SquidGuard sur le LAN2 .....	44
SquidGuard .....	51
Certificats .....	53
ClamAV.....	64
Snort.....	66
Cron .....	67
Optimisation du dashboard.....	68
Installation de GLPI .....	72
Installation NextCloud .....	78
Conclusion .....	98
Webographie .....	99



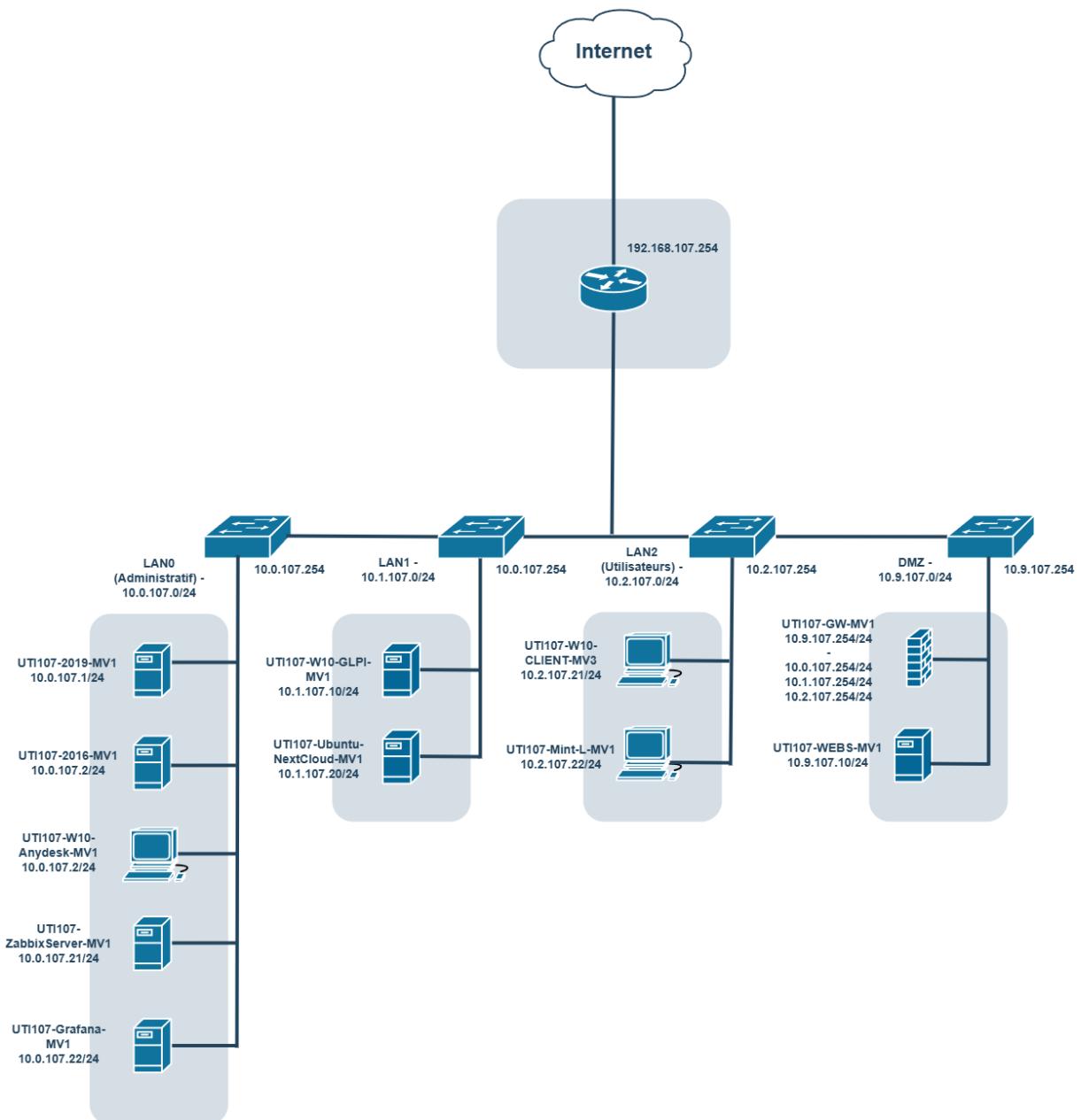
## **Introduction**

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

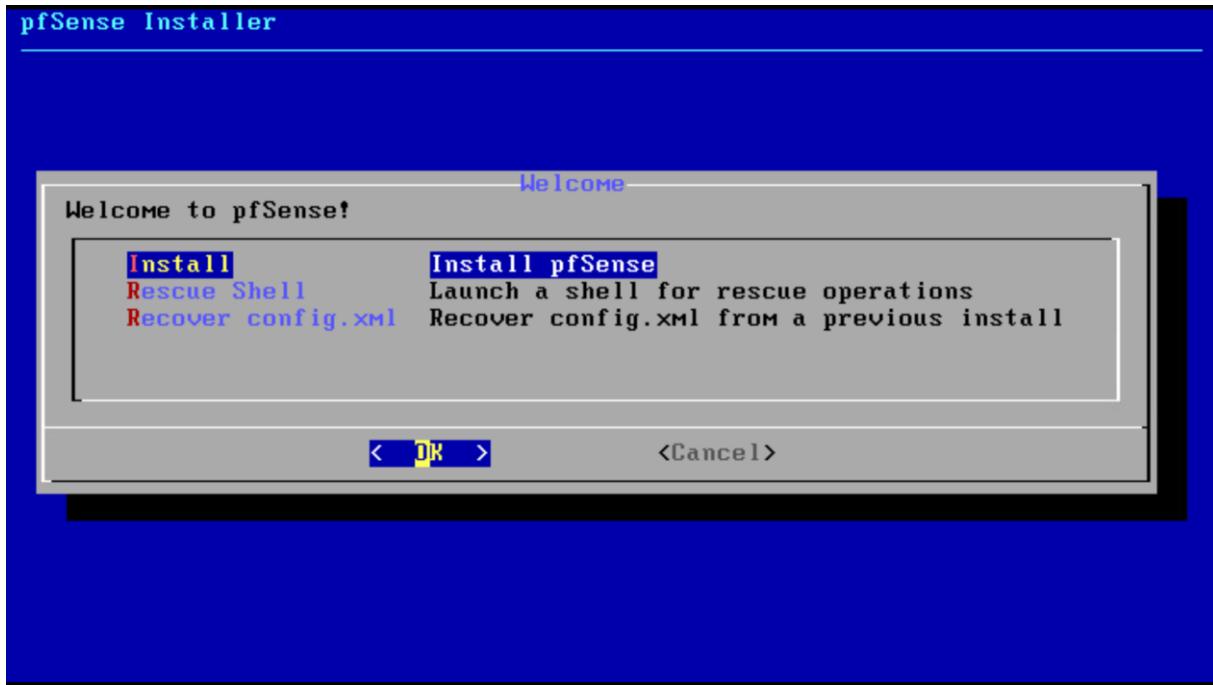


## Schéma Réseau

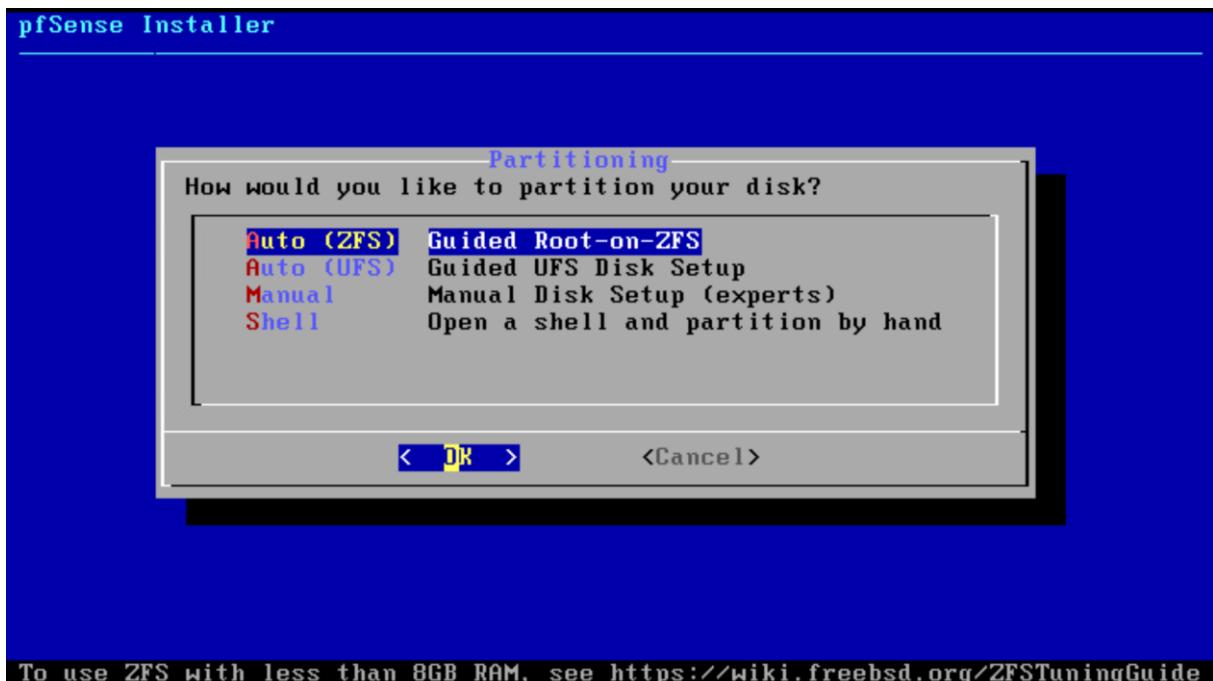
	Adresse IP	Masque de sous-réseau	Passerelle par défaut	DNS
UTI107-GW-MV1	192.168.107.254 10.0.107.254	255.255.255.0	Lui-même	10.0.107. 1 172.31.1.4 172.31.1.6
UTI107-WEBS-MV1	10.9.107.10	255.255.255.0	10.9.107. 254	10.0.107. 1 1.1.1.1
UTI107-2019-MV1	10.0.107.1	255.255.255.0	10.0.107. 254	Lui-même
UTI107-2016-MV1	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.

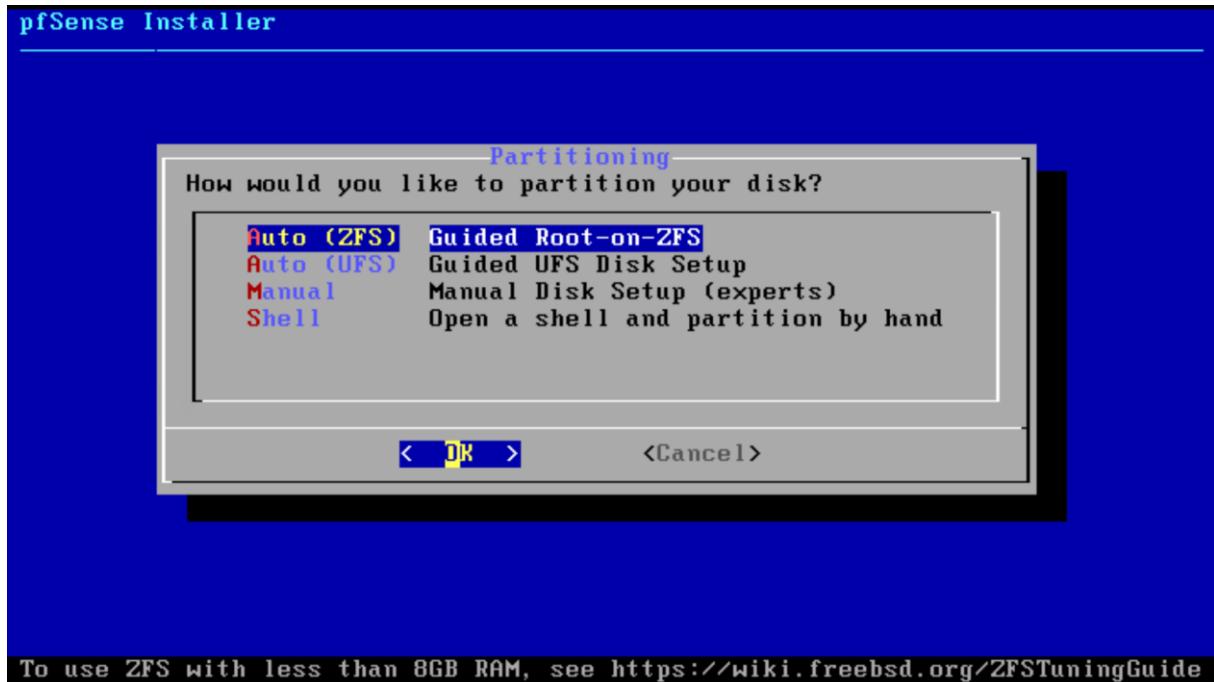


Le partitionnement automatique avec "Auto (ZFS)" a été sélectionné. ZFS est idéal pour sa fiabilité et sa capacité à gérer les volumes de stockage avancés, comme les snapshots. Ce choix est pertinent pour une utilisation moderne avec des besoins de sauvegarde ou de récupération. Si la machine dispose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



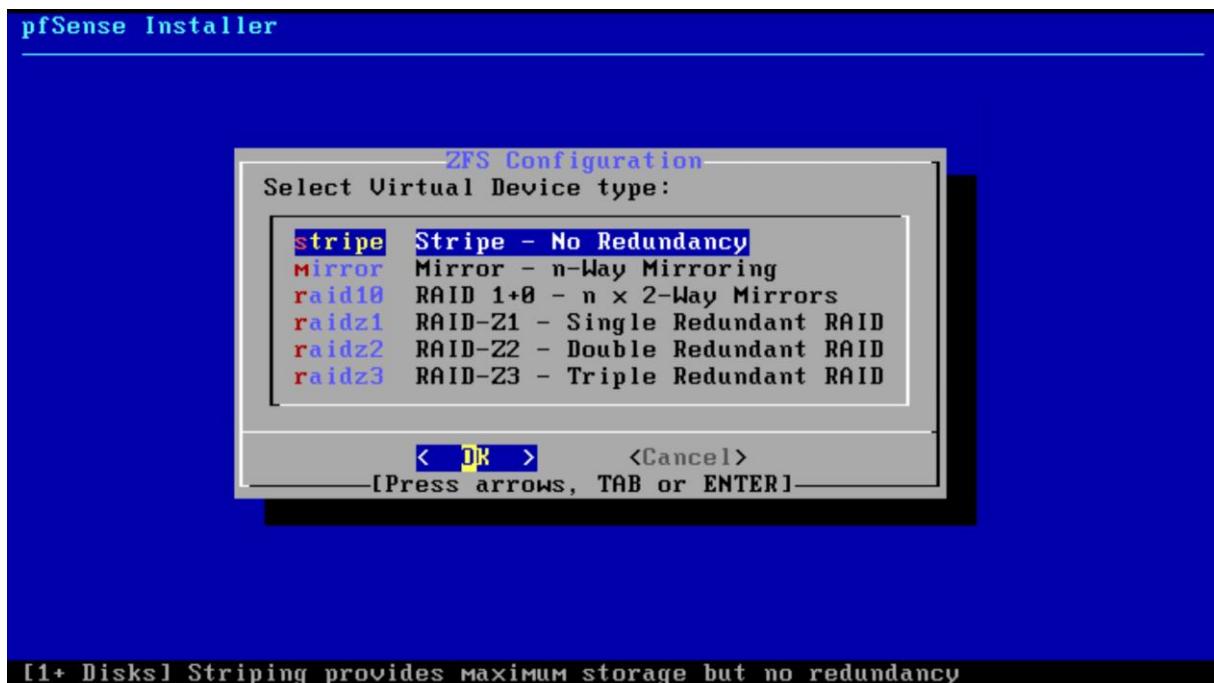
To use ZFS with less than 8GB RAM, see <https://wiki.freebsd.org/ZFSTuningGuide>

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.

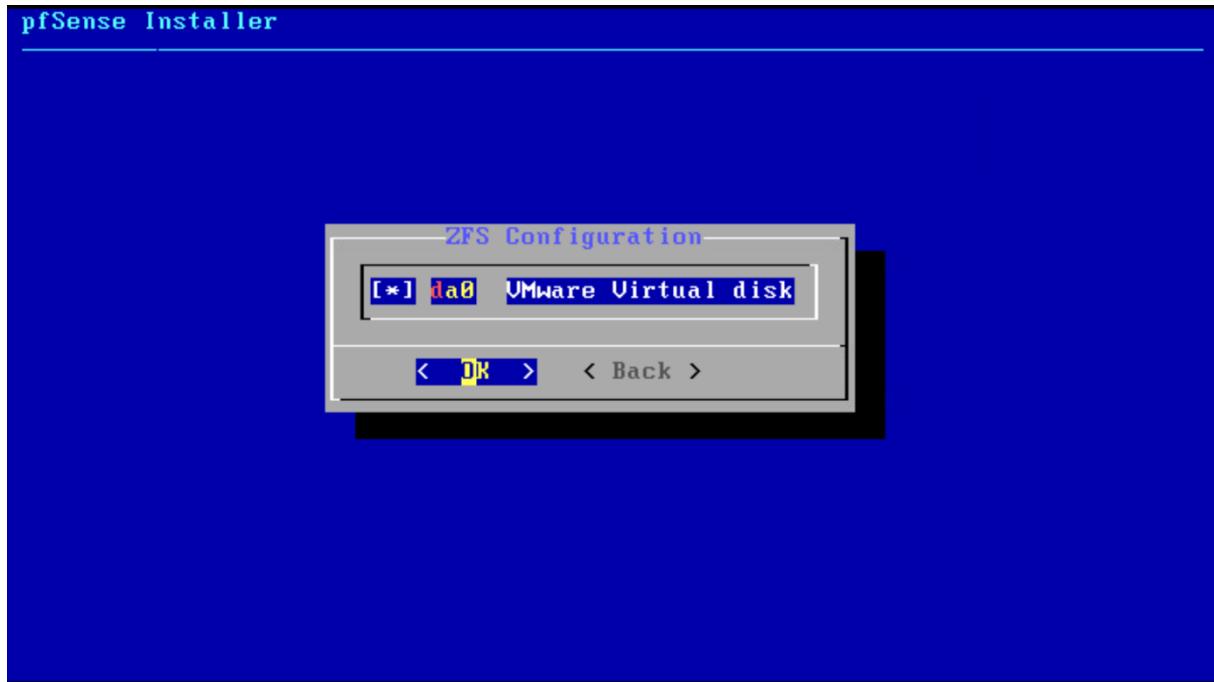


To use ZFS with less than 8GB RAM, see <https://wiki.freebsd.org/ZFSTuningGuide>

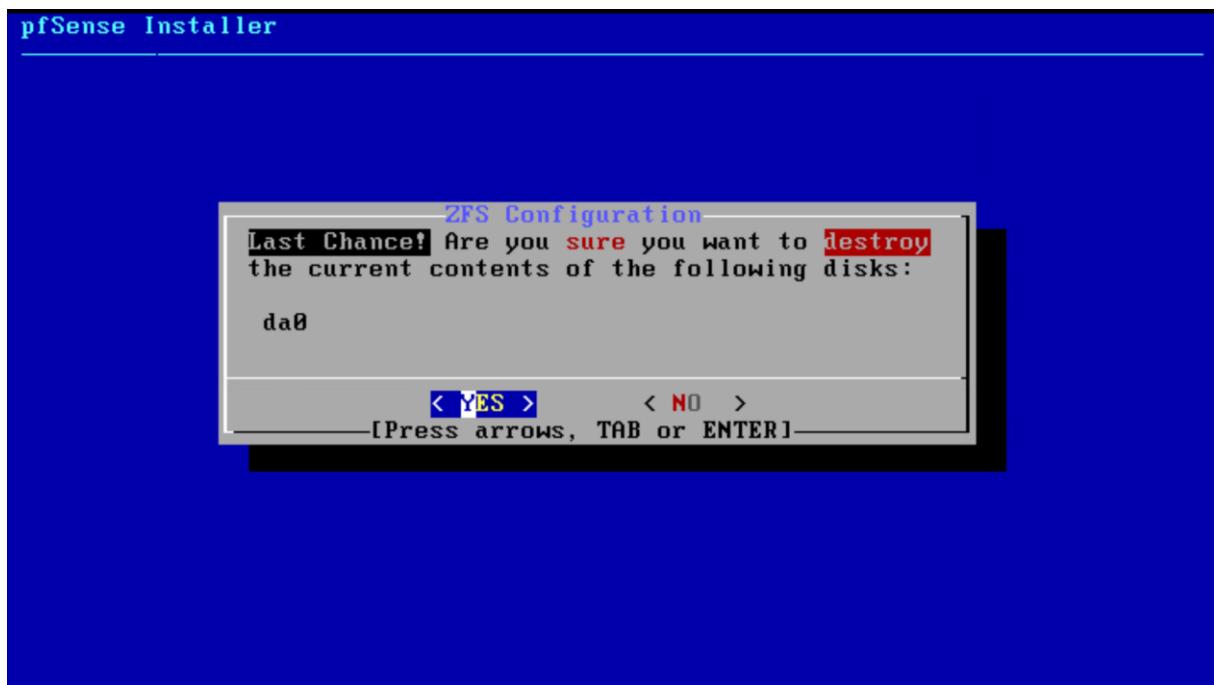
Le disque détecté, "da0" (VMware Virtual Disk), a été sélectionné. Cette action prépare le disque principal de la machine virtuelle à être configuré pour l'installation de pfSense. Ce choix est cohérent avec un déploiement sur VMware.



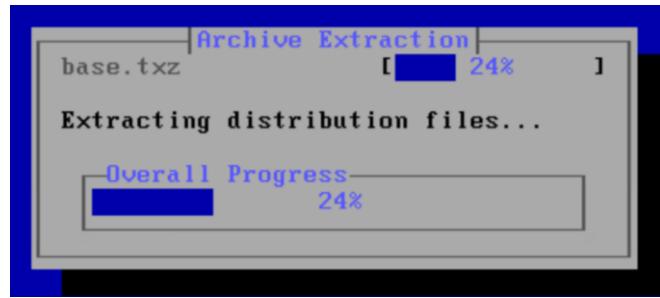
Un avertissement invite l'utilisateur à confirmer la suppression des données existantes sur "da0". Cette étape est critique pour éviter une perte accidentelle. En confirmant "Yes", le disque est préparé pour une nouvelle installation.



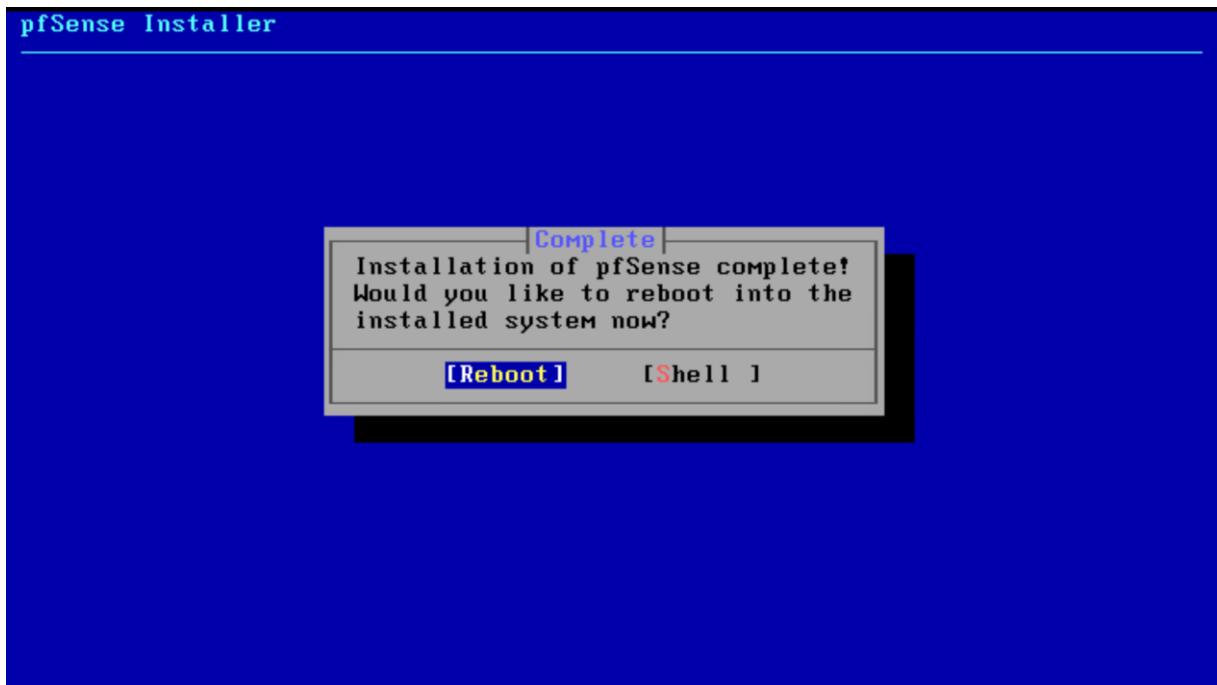
Le système extrait les fichiers nécessaires au déploiement de pfSense. Cette phase automatise l'installation et configure le système d'exploitation sur le disque sélectionné. La progression est affichée pour indiquer l'état en temps réel.



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.

```

Synchronizing user settings...done.
Configuring CRON...done.
Bootstrapping clock...done.
Starting NTP Server...done.
Starting webConfigurator...done.
Starting DHCP service...done.
Starting DHCPv6 service...done.
Configuring firewall.....done.
Generating RRD graphs...done.
Starting syslog...done.
Trimming the zpool... done.
Starting CRON... done.
(da0:mpt0:0:0:0): UNMAP failed, disabling BIO_DELETE
(da0:mpt0:0:0:0): UNMAP. CDB: 42 00 00 00 00 00 00 00 08 00
(da0:mpt0:0:0:0): CAM status: SCSI Status Error
(da0:mpt0:0:0:0): SCSI status: Check Condition
(da0:mpt0:0:0:0): SCSI sense: ILLEGAL REQUEST asc:24,0 (Invalid field in CDB)
(da0:mpt0:0:0:0): Command byte 7 is invalid
(da0:mpt0:0:0:0): Error 22, Unretryable error
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

```

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.

```

Enter an option: 2

Available interfaces:

1 - WAN (vmx2 - dhcp, dhcp6)
2 - LAN (vmx3 - static)
3 - OPT1 (vmx4)
4 - OPT2 (vmx0)
5 - OPT3 (vmx1)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.10.107

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

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

```

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.

```
Enter the new WAN IPv4 address.  Press <ENTER> for none:  
> 192.168.10.107  
  
Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense.  
e.g. 255.255.255.0 = 24  
     255.255.0.0 = 16  
     255.0.0.0 = 8  
  
Enter the new WAN IPv4 subnet bit count (1 to 32):  
> 24  
  
For a WAN, enter the new WAN IPv4 upstream gateway address.  
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
```

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.

```
browser: https://10.9.107.254/
Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: f8063b1aea36b47e4aba

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vmx2      -> v4: 192.168.10.254/24
LAN (lan)      -> vmx3      -> v4: 10.0.107.254/24
OPT1 (opt1)    -> vmx4      -> v4: 10.1.107.254/24
OPT2 (opt2)    -> vmx0      -> v4: 10.2.107.254/24
OPT3 (opt3)    -> vmx1      -> v4: 10.9.107.254/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: ■
```

```
Configure IPv6 address OPT3 interface via DHCP6? (y/n) n
Enter the new OPT3 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT3? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

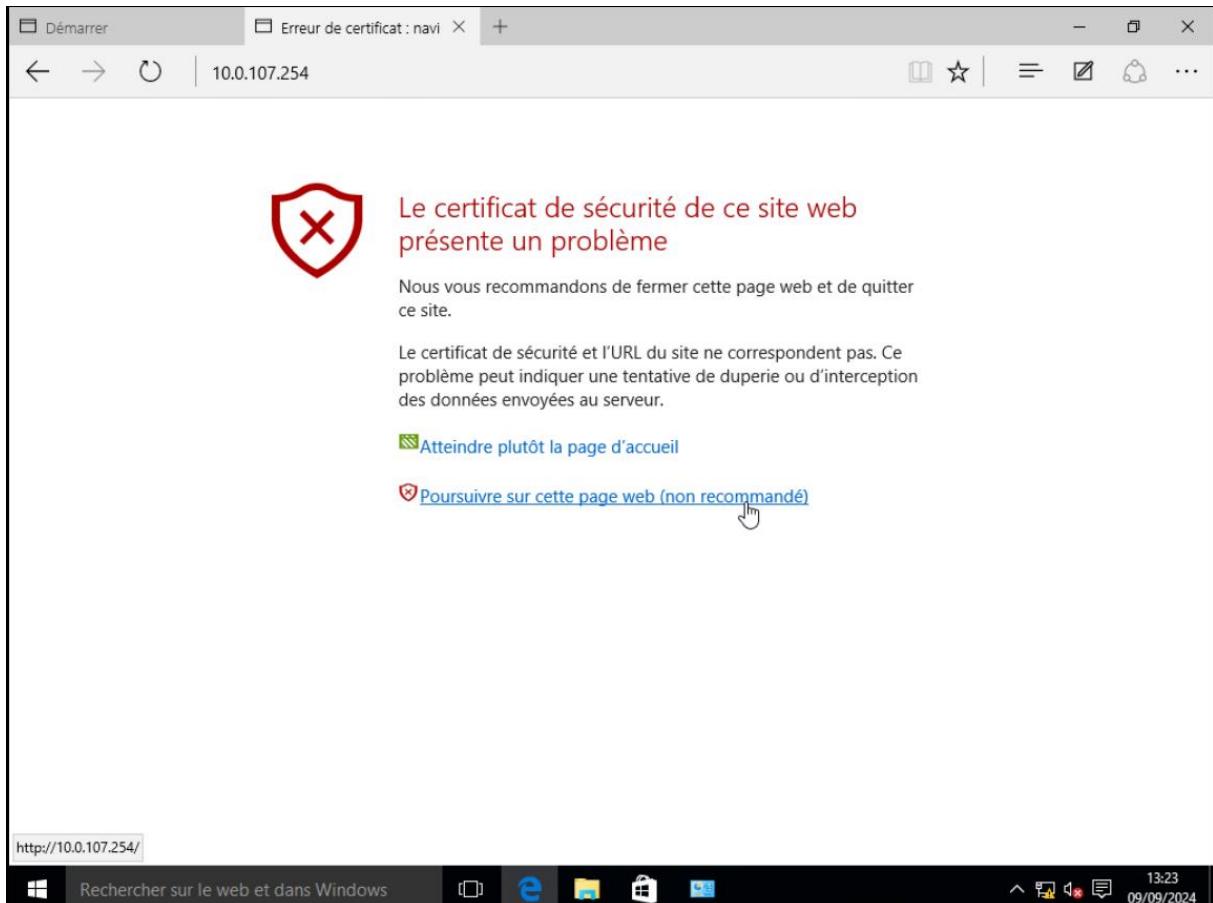
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Please wait while the changes are saved to OPT3...[fib_algo] inet.0 (bsearch4#42)
rebuild_fd_flm: switching algo to radix4_lockless

Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 OPT3 address has been set to 10.9.107.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://10.9.107.254/
Press <ENTER> to continue. ■
```

## 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.

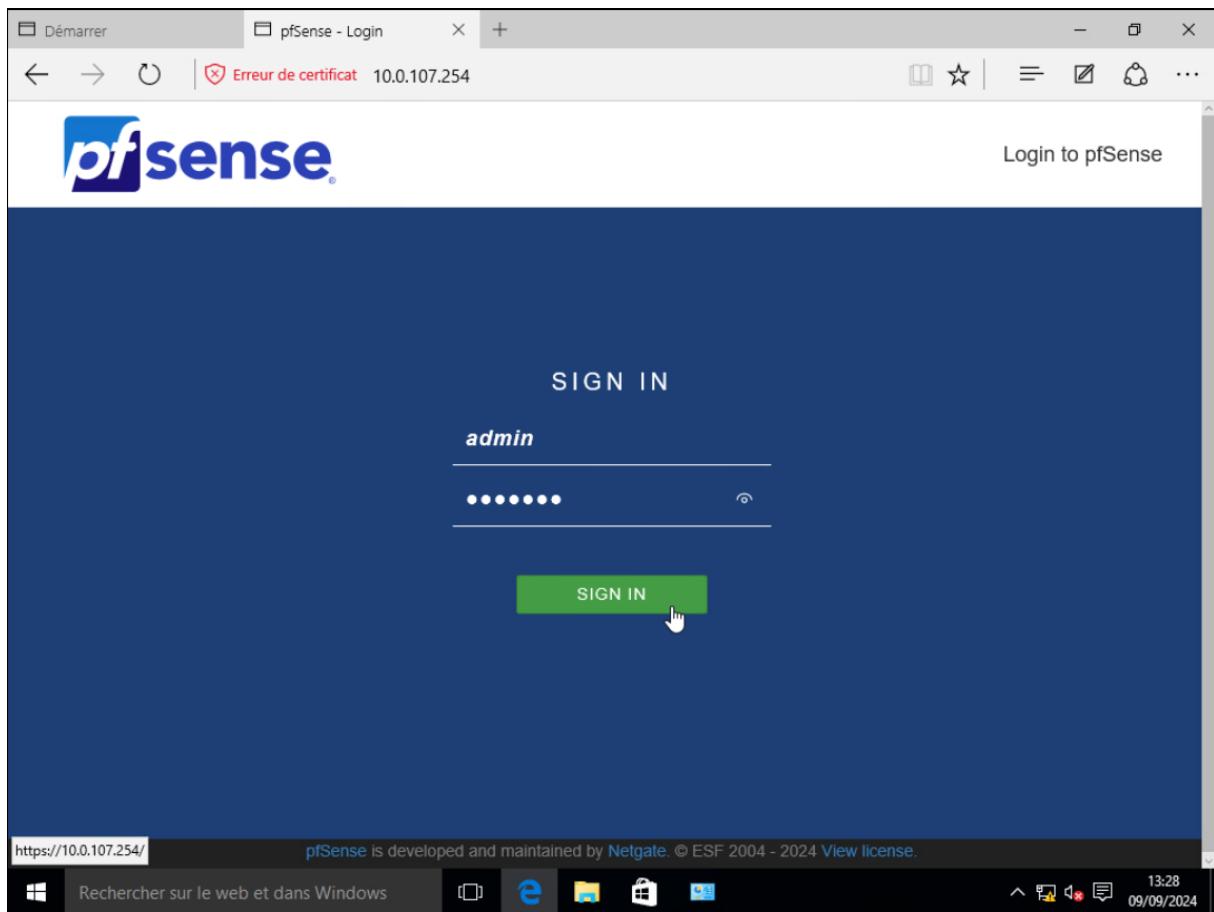


La connexion à l'interface web se fait via l'identifiant "admin" et le mot de passe par défaut. Il est fortement recommandé de modifier ce mot de passe dès que possible pour renforcer la sécurité et éviter tout accès non autorisé.

Identifiant : Admin

Mot de passe : pfsense

Ensuite cliquer sur « Sign in »



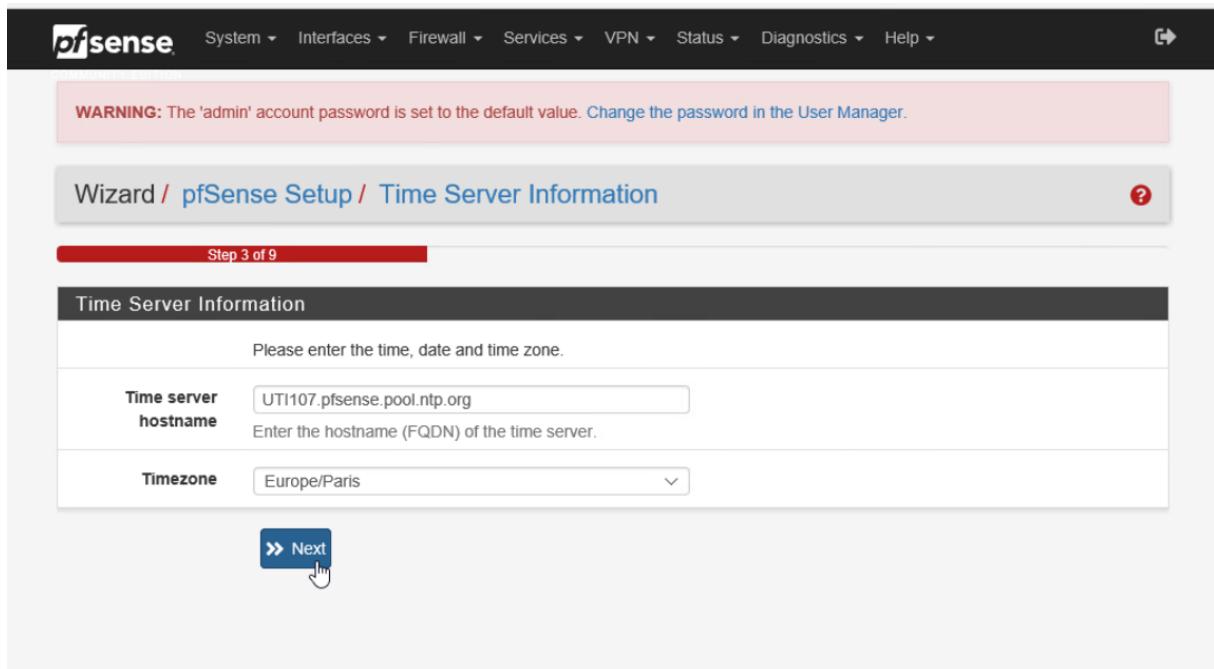
Le nom d'hôte, ici "UTI107-pfsense", est défini pour identifier clairement le pare-feu sur le réseau. Cela facilite la gestion, le suivi des logs et la communication avec d'autres équipements.

General Information

On this screen the general pfSense parameters will be set.

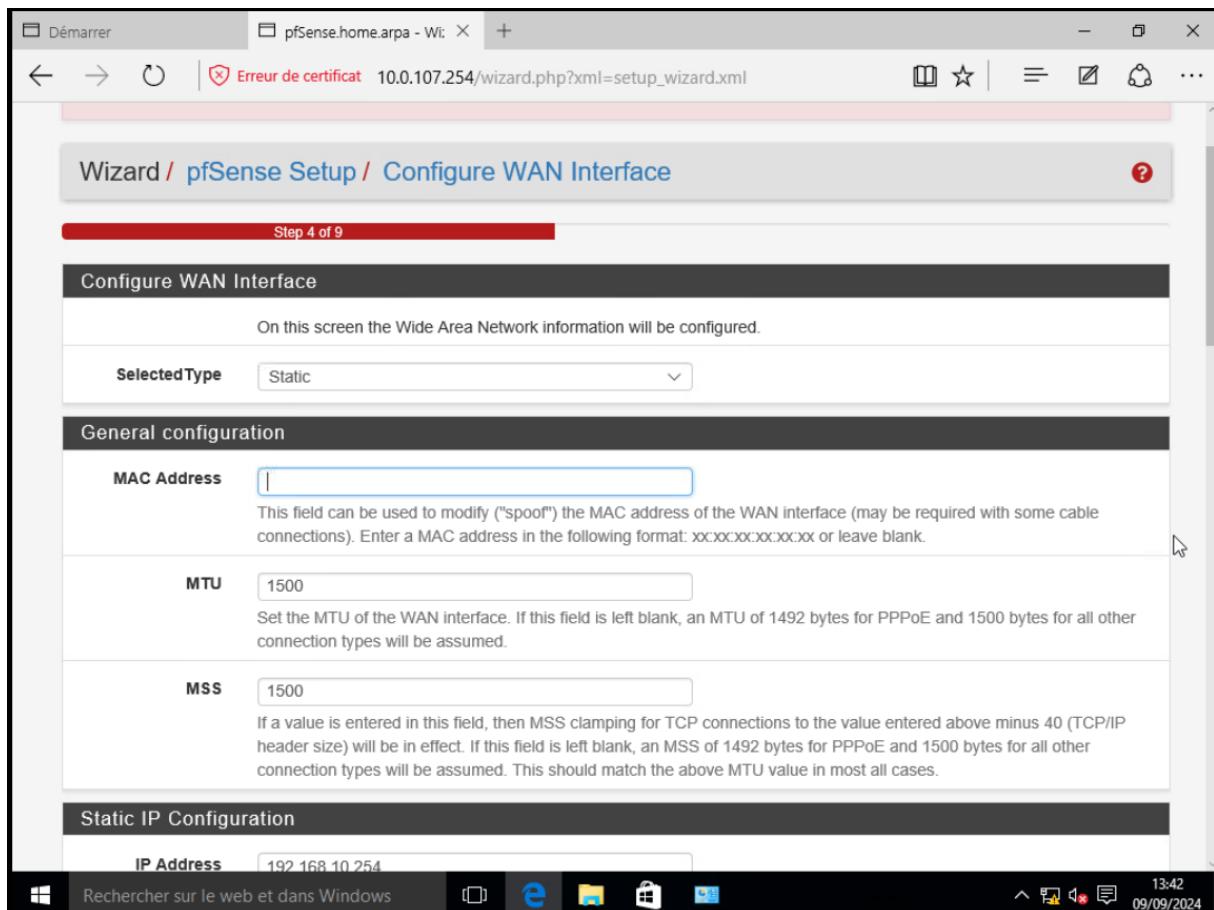
Hostname	UTI107-pfsense	X
Name of the firewall host, without domain part.		
Examples: pfsense, firewall, edgefw		

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 configurer notre propre « UTI107.pfsense.pool.ntp.org » en attendant de trouver un plus fiable.



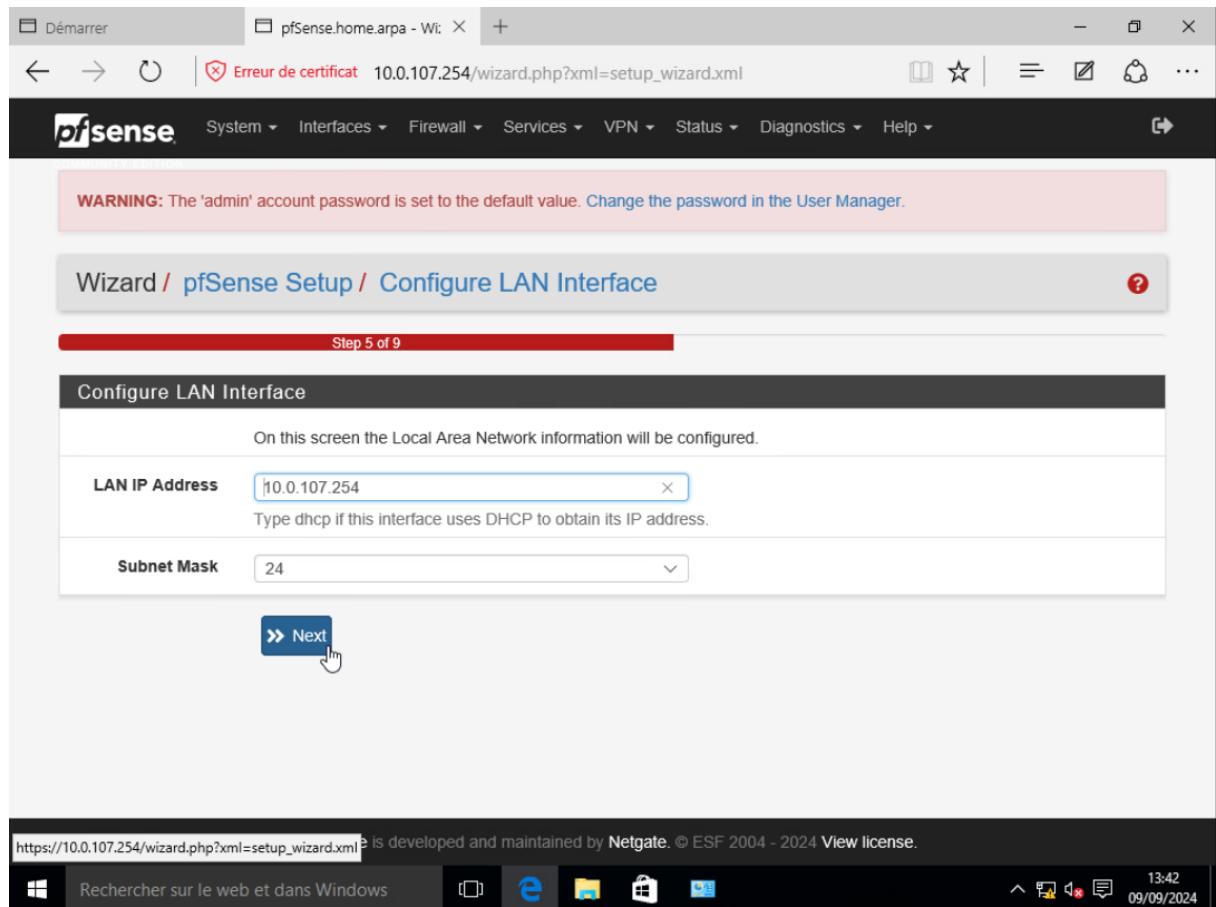
The screenshot shows the 'Time Server Information' step of the pfSense setup wizard. The 'Time server hostname' field is populated with 'UT107.pfsense.pool.ntp.org'. The 'Timezone' dropdown is set to 'Europe/Paris'. A 'Next' button is visible at the bottom of the form.

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.



The screenshot shows the 'Configure WAN Interface' step of the pfSense setup wizard. The 'SelectedType' dropdown is set to 'Static'. Under 'General configuration', the 'MAC Address' field is empty, 'MTU' is set to 1500, and 'MSS' is set to 1500. A 'Static IP Configuration' section is visible at the bottom.

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.



The screenshot shows a browser window for pfSense setup. The address bar shows 'pfSense.home.arpa - Wi: 10.0.107.254/wizard.php?xml=setup\_wizard.xml'. A warning message at the top of the page reads: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The main content is 'Wizard / pfSense Setup / Configure LAN Interface' (Step 5 of 9). It shows fields for 'LAN IP Address' (10.0.107.254) and 'Subnet Mask' (24). A 'Next' button is at the bottom. The pfSense navigation bar is visible at the top.

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.

**Static IP Configuration**

<b>IP Address</b>	192.168.10.254
<b>Subnet Mask</b>	24
<b>Upstream Gateway</b>	

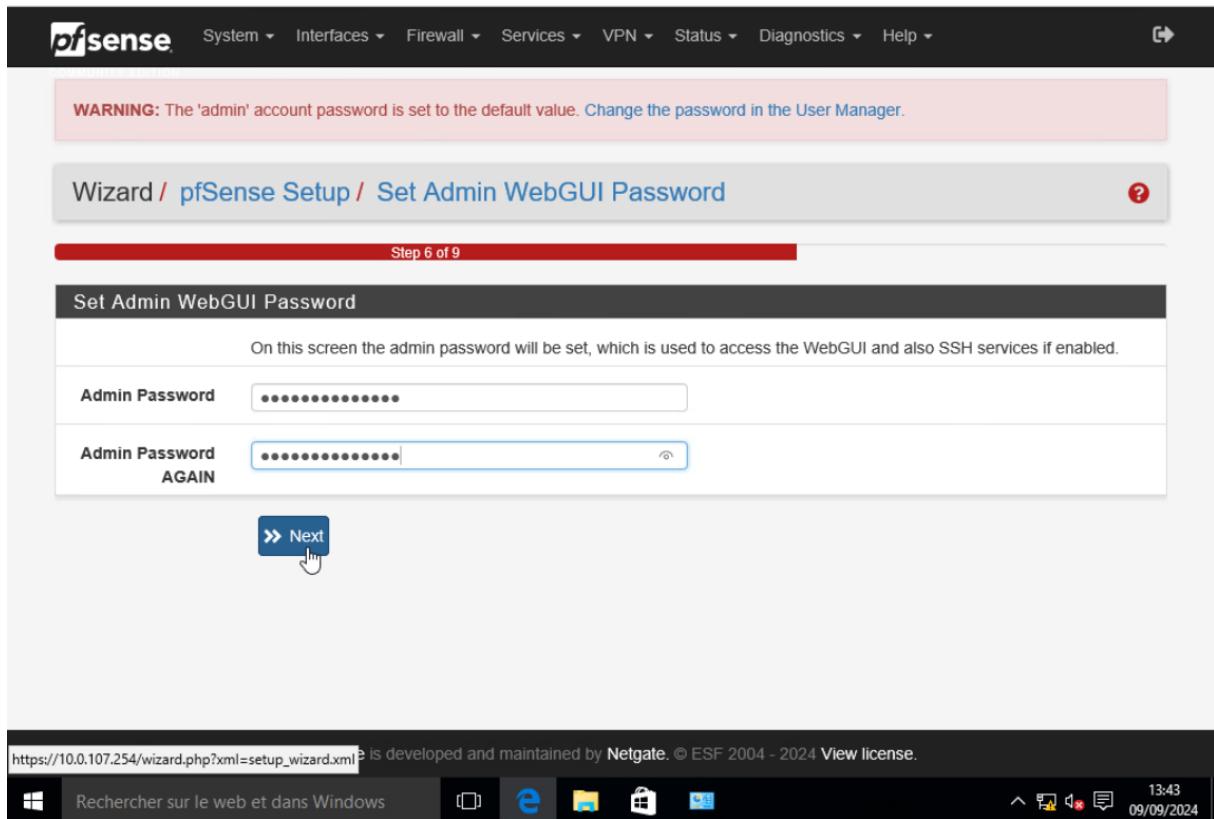
**DHCP client configuration**

<b>DHCP Hostname</b>	
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).	

**PPPoE configuration**

<b>PPPoE Username</b>	
<b>PPPoE Password</b>	
<b>Show PPPoE password</b>	<input type="checkbox"/> Reveal password characters
<b>PPPoE Service name</b>	Hint: this field can usually be left empty
<b>PPPoE Dial on demand</b>	<input type="checkbox"/> Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

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.



pfSense System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

**Wizard / pfSense Setup / Set Admin WebGUI Password**

Step 6 of 9

**Set Admin WebGUI Password**

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password:

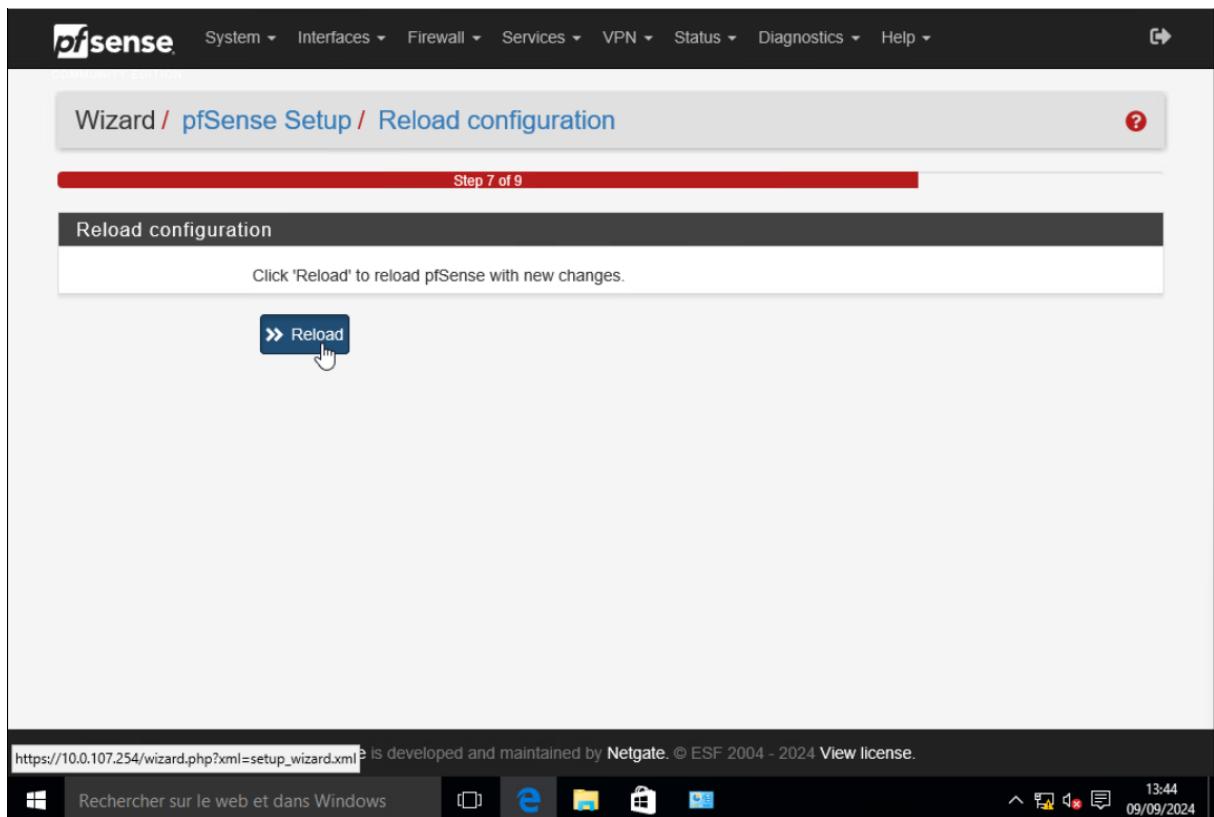
Admin Password AGAIN:

**>> Next**

https://10.0.107.254/wizard.php?xml=setup\_wizard.xml is developed and maintained by Netgate. © ESF 2004 - 2024 [View license](#).

13:43 09/09/2024

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.



pfSense System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**Wizard / pfSense Setup / Reload configuration**

Step 7 of 9

**Reload configuration**

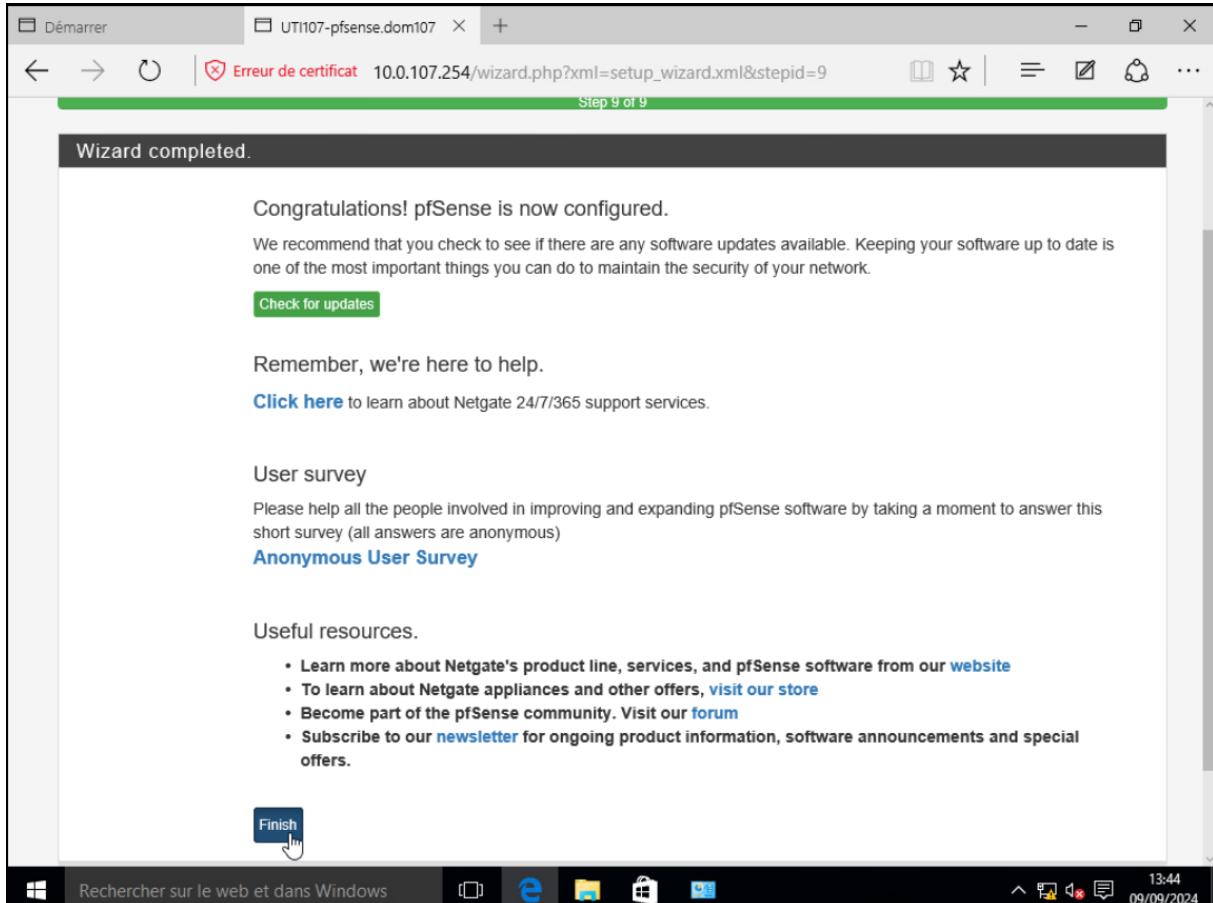
Click 'Reload' to reload pfSense with new changes.

**>> Reload**

https://10.0.107.254/wizard.php?xml=setup\_wizard.xml is developed and maintained by Netgate. © ESF 2004 - 2024 [View license](#).

13:44 09/09/2024

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.

The screenshot shows the pfSense System Update interface. At the top, a confirmation dialog box is displayed with the title "Confirmation Required to update pfSense system." It contains a dropdown menu for "Branch" set to "Current Stable Release (2.7.2)" with the note "Please select the branch from which to update the system firmware. Use of the development version is at your own risk!". Below this, a table provides system status: "Current Base System" is 2.7.2, "Latest Base System" is 2.7.2, and the "Status" is "Up to date.".

Un utilisateur "NGabriele" est créé avec un mot de passe sécurisé et assigné au groupe "admins". Cette configuration permet de déléguer les priviléges 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.

The screenshot shows the pfSense User Properties configuration page for the user "NGabriele". The "User Properties" section includes fields for "Defined by" (USER), "Disabled" (unchecked), "Username" (NGabriele), "Password" (redacted), "Full name" (Nathan Gabriele), "Expiration date" (unchecked), "Custom Settings" (unchecked), and "Group membership". The "Group membership" section shows "Not member of" and "Member of" dropdowns, with "admins" selected in the "Member of" dropdown. Buttons at the bottom include "Move to 'Member of' list" and "Move to 'Not member of' list". A note at the bottom states: "Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items."

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.

The screenshot shows the pfSense web interface for managing network interfaces. The current page is 'Interfaces / WANISIR (vmx2)'. The 'General Configuration' section is displayed, containing the following settings:

- Enable:** Checked, with the sub-option 'Enable interface'.
- Description:** WAN\_UTI107-NGabriele
- IPv4 Configuration Type:** Static IPv4
- IPv6 Configuration Type:** None
- MAC Address:** xx:xx:xx:xx:xx:xx
- MTU:** 1500
- MSS:** 1500

Below the configuration table, the Windows taskbar is visible, showing the date and time (09/09/2024, 14:55).

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.

System / General Setup

**System**

<b>Hostname</b>	UTI107-pfsense	Name of the firewall host, without domain part.
<b>Domain</b>	UTI107-GW.arpa	Domain name for the firewall.
<p>Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is <b>widely used</b> by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.</p>		

**DNS Server Settings**

<b>DNS Servers</b>	10.0.107.1	DNS Hostname	
	172.31.1.4	DNS Hostname	
	172.31.1.6	DNS Hostname	
<p>Address Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.</p>			
<b>Add DNS Server</b>			
<b>DNS Server Override</b>	<input checked="" type="checkbox"/> Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server <p>If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.</p>		
<b>DNS Resolution Behavior</b>	<input type="button" value="Use remote DNS Servers, ignore local DNS"/> <p>By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.</p>		

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.

<b>Uptime</b>	73 Days 02 Hours 18 Minutes 03 Seconds
<b>Current date/time</b>	Thu Nov 28 15:58:27 UTC 2024
<b>DNS server(s)</b>	<ul style="list-style-type: none"> <li>10.0.107.1</li> <li>172.31.1.4</li> <li>172.31.1.6</li> </ul>

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.

**Localization**

<u>Timezone</u>	Etc/UTC	Select a geographic region name (Continent/Location) to determine the timezone for the firewall. Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.
<u>Timeservers</u>	ntp.u-psud.org	Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!
<u>Language</u>	English	Choose a language for the webConfigurator

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.

**NTP Server Configuration**

<b>Enable</b>	<input checked="" type="checkbox"/> Enable NTP Server	You may need to disable NTP if pfSense is running in a virtual machine and the host is responsible for the clock.
<b>Interface</b>	WAN LAN0 LAN1 LAN2	Interfaces without an IP address will not be shown. Selecting no interfaces will listen on all interfaces with a wildcard. Selecting all interfaces will explicitly listen on only the interfaces/ IPs specified.
<b>Time Servers</b>	ntp.u-psud.org	<input checked="" type="checkbox"/> Prefer <input type="checkbox"/> No Select <input type="checkbox"/> Server <input type="checkbox"/> Type
<b>Add</b>	<b>+ Add</b>	NTP will only sync if a majority of the servers agree on the time. For best results you should configure between 3 and 5 servers ( <a href="#">NTP support pages recommend at least 4 or 5</a> ), or a pool. If only one server is configured, it <b>will</b> be believed, and if 2 servers are configured and they disagree, <b>neither</b> will be believed. Options: <b>Prefer</b> - NTP should favor the use of this server more than all others. <b>No Select</b> - NTP should not use this server for time, but stats for this server will be collected and displayed. <b>Type</b> - Server, Peer or a Pool of NTP servers and not a single address. This is assumed for *.pool.ntp.org.
<b>Max candidate pool peers</b>	Maximum number of candidate peers in the NTP pool. This value should be set low enough to provide sufficient alternate sources while not contacting an excessively large number of peers. Many servers inside public pools are provided by volunteers, and a large candidate pool places unnecessary extra load on the volunteer time servers for little to no added benefit. (Default: 5).	
<b>Orphan Mode</b>	12 Orphan mode allows the system clock to be used when no other clocks are available. The number here specifies the stratum reported during orphan	

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.

Rules (Drag to Change Order)											
Action	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 UDP	*	*	1194 (OpenVPN)	*	none		Autoriser OpenVPN	
NAT											
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	Web	10.9.107.10	443 (HTTPS)	*	none	NAT Redirection vers Serveur Web	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	10.9.107.10	443 (HTTPS)	*	none	NAT	
Blocages IP à risques											
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv6 TCP	Spamhaus_dropv6	*	*	*	*	none		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	Spamhaus_drop	*	*	*	*	none		
Bloque Ping											
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP	*	*	*	*	*	none	Ping Blocking	
any											

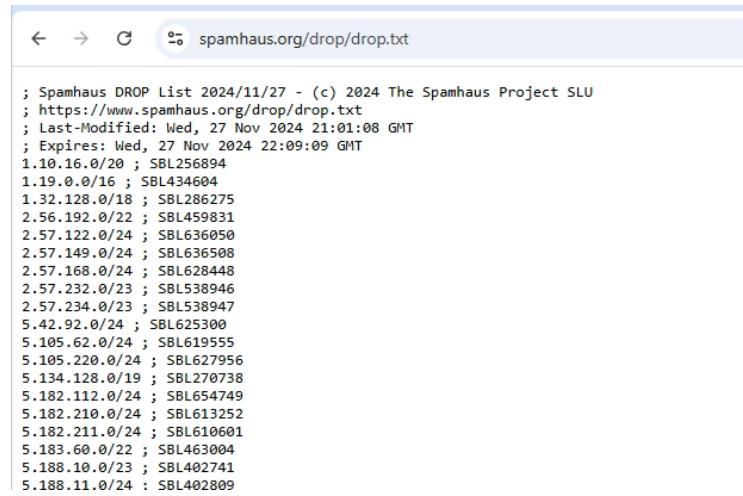
## Interface WAN

### 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.



spamhaus.org/drop/drop.txt

```
; Spamhaus DROP List 2024/11/27 - (c) 2024 The Spamhaus Project SLU
; https://www.spamhaus.org/drop/drop.txt
; Last-Modified: Wed, 27 Nov 2024 21:01:08 GMT
; Expires: Wed, 27 Nov 2024 22:09:09 GMT
1.10.16.0/20 ; SBL256894
1.19.0.0/16 ; SBL434604
1.32.128.0/18 ; SBL286275
2.56.192.0/22 ; SBL459831
2.57.122.0/24 ; SBL636050
2.57.149.0/24 ; SBL636508
2.57.168.0/24 ; SBL628448
2.57.232.0/23 ; SBL538946
2.57.234.0/23 ; SBL538947
5.42.92.0/24 ; SBL625300
5.105.62.0/24 ; SBL619555
5.105.220.0/24 ; SBL627956
5.134.128.0/19 ; SBL270738
5.182.112.0/24 ; SBL654749
5.182.210.0/24 ; SBL613252
5.182.211.0/24 ; SBL610601
5.183.60.0/22 ; SBL463004
5.188.18.0/23 ; SBL402741
5.188.11.0/24 ; SBL402809
```

### 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	
<input checked="" type="checkbox"/>	3/182.02 MiB	*	*	*	LAN0 Address	8443 80 22	*	*		Anti-Lockout Rule		
<input type="checkbox"/>	 0/0 B	IPv4 *	LAN0 subnets	*	Spamhaus_drop	*	*		none		  	
Passe Zabbix												
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	Active_Directory	*	LAN0 subnets	10051	*		none	Autorisation de recherche pour zabbix	  	
Passe Grafana												
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	Active_Directory	*	LAN0 subnets	Grafana	*		none	Autorisation Grafana	  	
Passe TFTP Statiques / Dynamiques												
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	*	*	10.0.107.10	69 (TFTP)	*		none	Autoriser le TFTP	  	
Passe LDAP / LDAPS												
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP/UDP	*	*	10.0.107.1	389 (LDAP)	*		none	Autoriser le LDAP sur le LAN	  	
Passe NextCloud												
<input type="checkbox"/>	<input checked="" type="checkbox"/> 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												
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	Active_Directory	*	LAN0 address	53 (DNS)	*		none	Autoriser le trafic DNS	  	
Passe Serveur NTP												
<input type="checkbox"/>	<input checked="" type="checkbox"/> 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										
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP	*	*	*	Trafic_App_Specifique	*	none	Règle pour applications spécifiques 
Passe AnyDesk										
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP	LAN2 subnets	*	WAN address	ANYDESK_Port	*	none	Autorisation Anydesk 
Accès Internet										
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP	*	*	*	Web	*	none	
<input type="checkbox"/>		0/0 B	IPv4 TCP	LAN0 subnets	*	10.1.107.10	Web	*	none	
Accès SSH										
<input type="checkbox"/>		0/0 B	IPv4 TCP	LAN0 subnets	*	LAN0 subnets	2222	*	none	
Passe tout										
<input type="checkbox"/>		26/787.02 MiB	IPv4 *	*	*	*	*	*	none	
Bloque tout										
<input type="checkbox"/>		0/560 B	IPv4 *	*	*	*	*	*	none	
<input type="checkbox"/>		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.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/100 KiB	IPv4 TCP	LAN1 subnets	*	*	Web	*	none		Autorisation HTTP HTTPS	    
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	Active_Directory	53 (DNS)	LAN1 address	53 (DNS)	*	none		Autoriser DNS	    
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	Active_Directory	123 (NTP)	LAN1 address	123 (NTP)	*	none		Autorisation NTP	    
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	LAN1 subnets	*	10.0.107.20	Web	*	none			    
Passe PostgreSQL											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP/UDP	*	*	*	BDD	*	none			    
GLPI											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	10.1.107.10	*	*	8080	*	none		Autorisation du Service Applicatif GLPI	    
NextCloud											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	10.1.107.20	*	*	8081	*	none		Autorisation du Service Applicatif NextCloud	    
Passe tout											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 6/4.26 GiB	IPv4 *	LAN1 subnets	*	*	*	*	*	none		    
Bloque tout											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 *	LAN1 subnets	*	*	*	*	*	none		    

## 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.

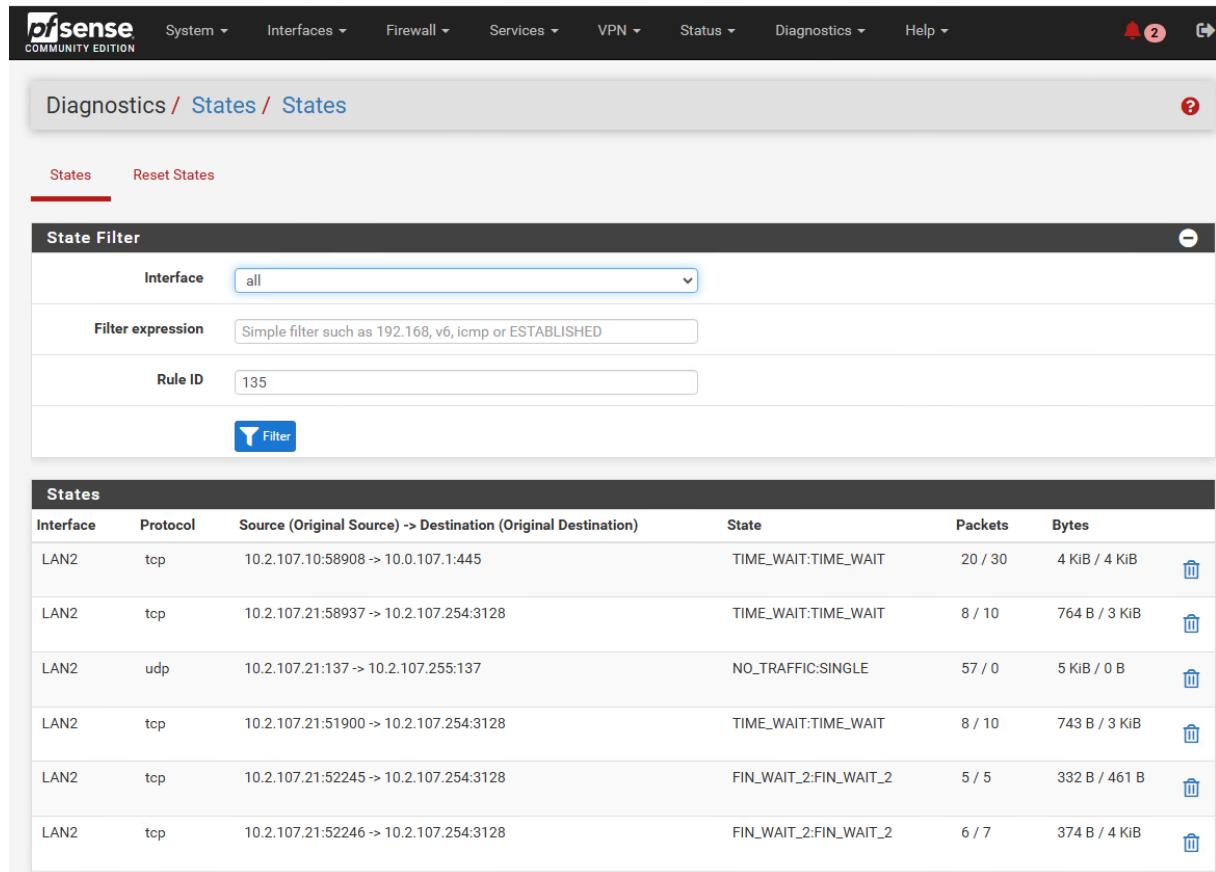
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
											<span>trash</span>
	AnyDesk										<span>trash</span>
<input type="checkbox"/>	<span>✓</span> 0/0 B	IPv4 TCP	LAN2 address	*	*		ANYDESK_Port	*	none	Autorisation d'Anydesk	<span>anchor</span> <span>edit</span> <span>copy</span> <span>trash</span>
											<span>trash</span>
	Autorisation Spécifiques										
<input type="checkbox"/>	<span>✓</span> 0/0 B	IPv4 TCP	LAN2 subnets	*	*	Web	*	none		Autorisation HTTP HTTPS	<span>anchor</span> <span>edit</span> <span>copy</span> <span>trash</span>
<input type="checkbox"/>	<span>✓</span> 0/0 B	IPv4 UDP	Active_Directory	*	LAN2 address	123 (NTP)	*	none		Autorisation NTP	<span>anchor</span> <span>edit</span> <span>copy</span> <span>trash</span>
<input type="checkbox"/>	<span>✓</span> 0/0 B	IPv4 UDP	Active_Directory	*	LAN2 address	53 (DNS)	*	none		Autorisation DNS	<span>anchor</span> <span>edit</span> <span>copy</span> <span>trash</span>
											<span>trash</span>
	DHCP Pass										
<input type="checkbox"/>	<span>✓</span> 0/0 B	IPv4 TCP/UDP	Active_Directory	67	10.2.107.0/24	DHCP	*	none		Autorisation DHCP	<span>anchor</span> <span>edit</span> <span>copy</span> <span>trash</span>
											<span>trash</span>
	Autres										
<input type="checkbox"/>	<span>✓</span> 0/1.91 GiB	IPv4 *	LAN2 subnets	*	*	*	*	none			<span>anchor</span> <span>edit</span> <span>copy</span> <span>trash</span>
<input type="checkbox"/>	<span>✓</span> 0/0 B	IPv4 TCP	LAN2 address	*	*	3128	*	none			<span>anchor</span> <span>edit</span> <span>copy</span> <span>trash</span>
											<span>trash</span>
	Blocages										
<input type="checkbox"/>	<span>✗</span> 0/14 KIB	IPv4 *	LAN2 subnets	*	*	*	*	none			<span>anchor</span> <span>edit</span> <span>copy</span> <span>trash</span>
<input type="checkbox"/>	<span>✗</span> 0/0 B	IPv4 ICMP any		*	*	*	*	none		Ping Blocking	<span>anchor</span> <span>edit</span> <span>copy</span> <span>trash</span>

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.



The screenshot shows the pfSense Diagnostic States page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A notification bell icon shows 2 pending notifications. The main title is "Diagnostics / States / States". Below the title, there are two buttons: "States" (which is selected and highlighted in red) and "Reset States". A "State Filter" section contains fields for "Interface" (set to "all"), "Filter expression" (empty), and "Rule ID" (set to 135). A "Filter" button is located below these fields. The main table displays the following data:

States						
Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	packets	bytes	
LAN2	tcp	10.2.107.10:58908 -> 10.0.107.1:445	TIME_WAIT:TIME_WAIT	20 / 30	4 KiB / 4 KiB	
LAN2	tcp	10.2.107.21:58937 -> 10.2.107.254:3128	TIME_WAIT:TIME_WAIT	8 / 10	764 B / 3 KiB	
LAN2	udp	10.2.107.21:137 -> 10.2.107.255:137	NO_TRAFFIC:SINGLE	57 / 0	5 KiB / 0 B	
LAN2	tcp	10.2.107.21:51900 -> 10.2.107.254:3128	TIME_WAIT:TIME_WAIT	8 / 10	743 B / 3 KiB	
LAN2	tcp	10.2.107.21:52245 -> 10.2.107.254:3128	FIN_WAIT_2:FIN_WAIT_2	5 / 5	332 B / 461 B	
LAN2	tcp	10.2.107.21:52246 -> 10.2.107.254:3128	FIN_WAIT_2:FIN_WAIT_2	6 / 7	374 B / 4 KiB	

## 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 :

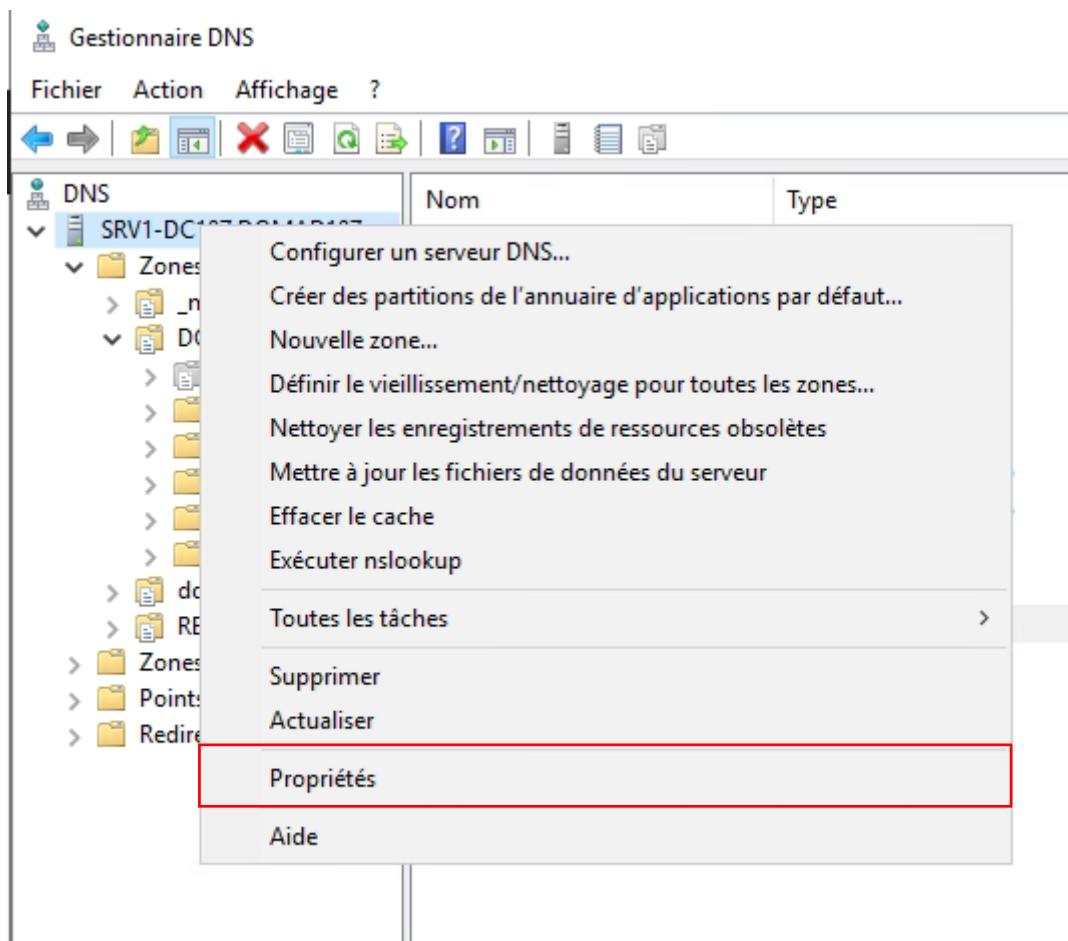
- **Protocole :** IPv4 TCP.
- **Action :** Autoriser.
- **Justification :** Permettre aux hôtes de la DMZ d'accéder au service antivirus pour la protection des fichiers.

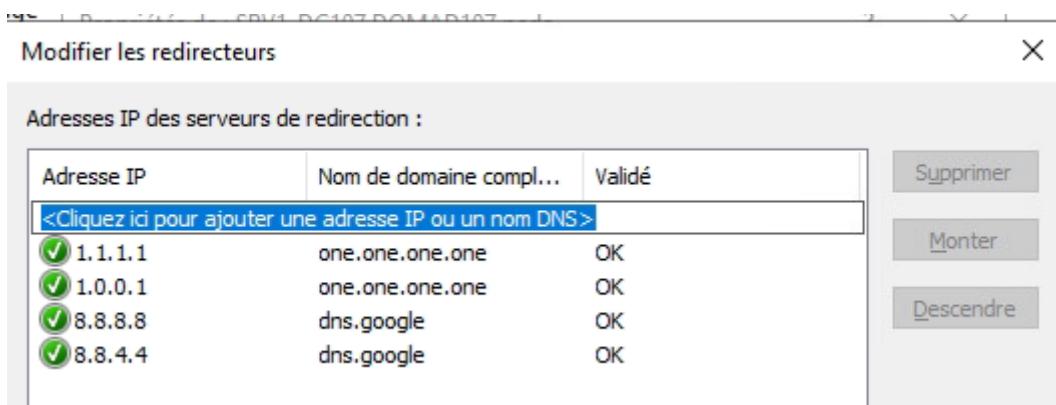
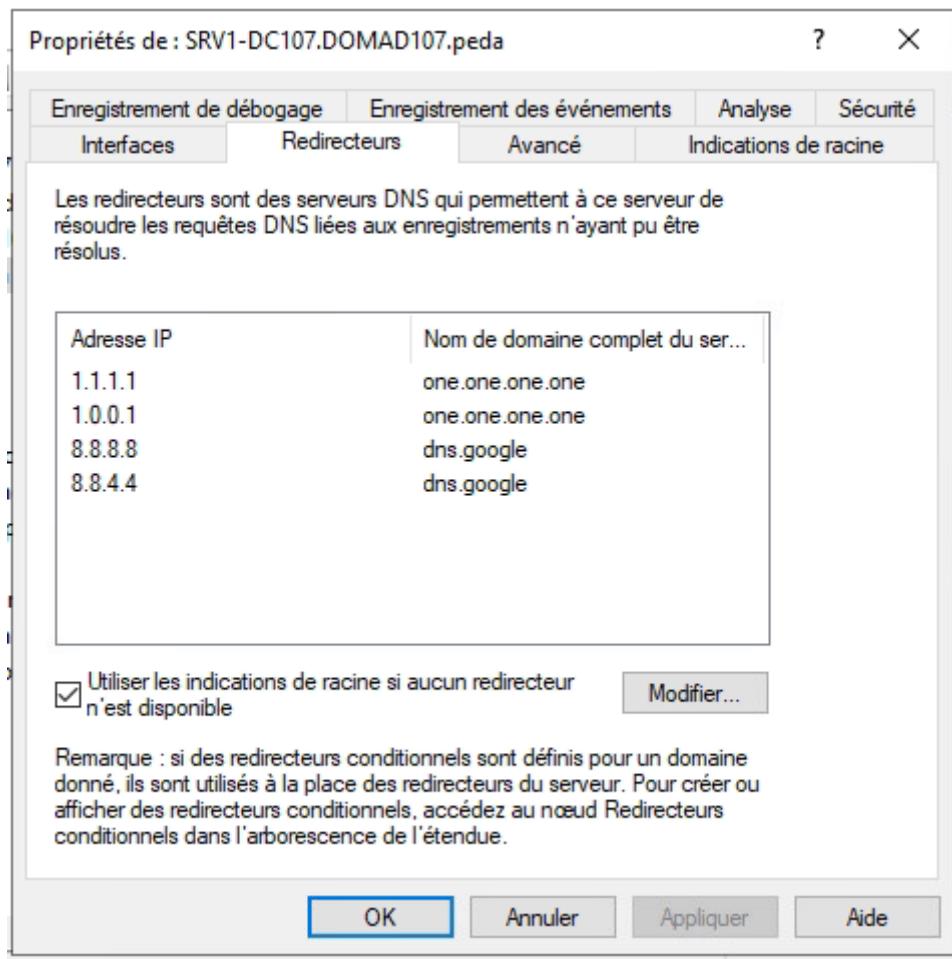
### 4. Blocage Global :

- **Protocole :** IPv4 Tous.
- **Action :** Bloquer.
- **Justification :** Empêcher tout trafic non autorisé entre la DMZ et les autres réseaux.

Rules (Drag to Change Order)											Actions
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/2 KIB	IPv4 TCP	DMZ subnets	*	*	*	*	none		Autoriser HTTP et HTTPS	
Autorisations Services Générales											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	Active_Directory	*	DMZ address	123 (NTP)	*	none		Autoriser NTP	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	Active_Directory	*	DMZ address	53 (DNS)	*	none		Autoriser DNS	
Autorisations Snort et ClamAV											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	DMZ subnets	*	10.0.107.254	ClamAV_Port	*	none		Accès ClamAV	
Blocages											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/13.65 MIB	IPv4 *	*	*	*	*	*	none			

## Redirecteurs DNS





## Création d'Alias

Par port

## Par IP

The image shows two screenshots of the pfSense web interface. The top screenshot is the 'Firewall / Aliases / IP' page, showing a table of aliases. The bottom screenshot is the 'Firewall / Aliases / Edit' page, showing the configuration for a specific alias named 'Active\_Directory'.

**Firewall / Aliases / IP**

Name	Type	Values	Description	Actions
				<a href="#">+ Add</a> <a href="#">Import</a>

**Firewall / Aliases / Edit**

**Properties**

<b>Name</b>	Active_Directory
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".	
<b>Description</b>	Alias pour l'AD
A description may be entered here for administrative reference (not parsed).	
<b>Type</b>	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.

<b>IP or FQDN</b>	10.0.107.1	Serveur Active Directory (2019)	<a href="#">Delete</a>
	10.0.107.2	Serveur Redondant (2016)	<a href="#">Delete</a>

[Save](#) [+ Add Host](#)

**pfSense®**  
COMMUNITY EDITION

Firewall / Aliases / IP

The alias list has been changed.  
The changes must be applied for them to take effect.

IP Ports URLs All

**Firewall Aliases IP**

Name	Type	Values	Description	Actions
Active_Directory	Host(s)	10.0.107.1, 10.0.107.2	Alias pour l'AD	

**Add** **Import**

## Configuration des transmission de ports

**Add** **Delete** **Toggle** **Save** **Separator**

**Edit Redirect Entry**

**Disabled**  Disable this rule

**No RDR (NOT)**  Disable redirection for traffic matching this rule  
This option is rarely needed. Don't use this without thorough knowledge of the implications.

**Interface**  Choose which interface this rule applies to. In most cases "WAN" is specified.

**Address Family**  Select the Internet Protocol version this rule applies to.

**Protocol**  Choose which protocol this rule should match. In most cases "TCP" is specified.

**Source**

**Source**  Invert match.  Type

**Source port range**  From port  To port  Custom  
Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.

**Destination**  Invert match.  Type  Address/mask

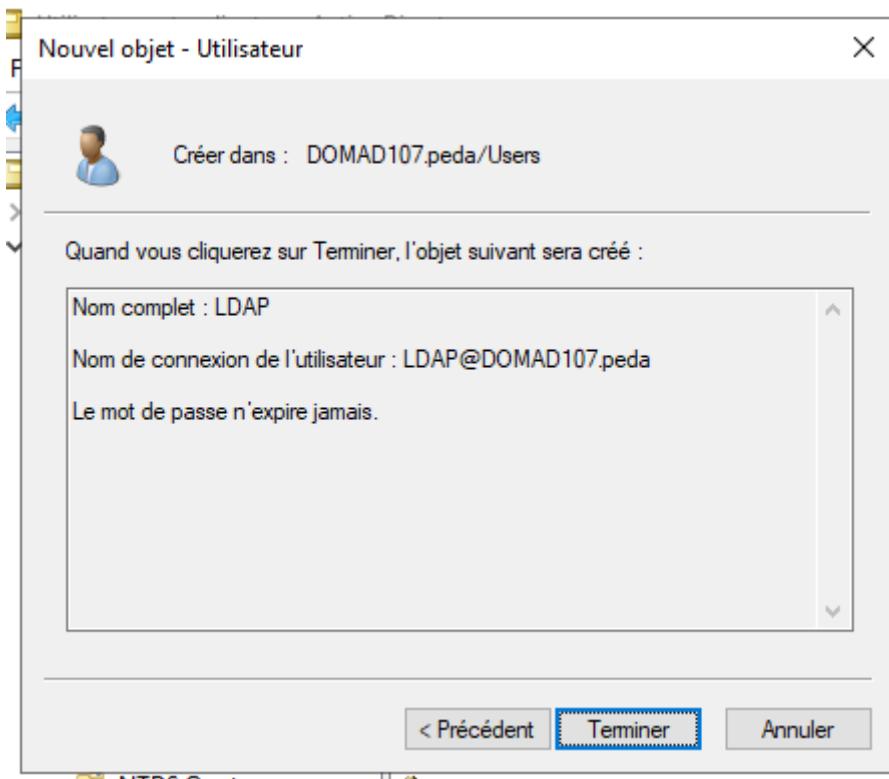
<b>Source</b>	<input type="checkbox"/> Invert match.	Any	/	Address/mask				
<b>Source port range</b>	Other	Web	Other	Web				
	From port	Custom	To port	Custom				
Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.								
<b>Destination</b>	<input type="checkbox"/> Invert match.	Address or Alias	10.9.107.10	/				
<b>Destination port range</b>	HTTPS		HTTPS					
	From port	Custom	To port	Custom				
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.								
<b>Redirect target IP</b>	Address or Alias							
	Type	10.9.107.10						
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::*) to local scope (::1)								
<b>Redirect target port</b>	HTTPS	Custom						
	Port	Custom						
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.								
<b>Description</b>	Redirection vers Serveur Web							
A description may be entered here for administrative reference (not parsed).								
<b>Filter rule association</b> Rule NAT Redirection vers Serveur Web <a href="#">View the filter rule</a>								
<b>Rule Information</b> <table border="1"> <tr> <td><b>Created</b></td> <td>11/25/24 16:34:06 by NGabriele@10.0.107.10 (Local Database)</td> </tr> <tr> <td><b>Updated</b></td> <td>11/27/24 22:40:09 by NGabriele@10.0.107.1 (Local Database)</td> </tr> </table>					<b>Created</b>	11/25/24 16:34:06 by NGabriele@10.0.107.10 (Local Database)	<b>Updated</b>	11/27/24 22:40:09 by NGabriele@10.0.107.1 (Local Database)
<b>Created</b>	11/25/24 16:34:06 by NGabriele@10.0.107.10 (Local Database)							
<b>Updated</b>	11/27/24 22:40:09 by NGabriele@10.0.107.1 (Local Database)							
<input type="button" value="Save"/>								

The NAT configuration has been changed.  
The changes must be applied for them to take effect.

Firewall / NAT / Port Forward		?																																			
Port Forward	1:1	Outbound	NPt																																		
<b>Rules</b> <table border="1"> <thead> <tr> <th></th> <th>Interface</th> <th>Protocol</th> <th>Source Address</th> <th>Source Ports</th> <th>Dest. Address</th> <th>Dest. Ports</th> <th>NAT IP</th> <th>NAT Ports</th> <th>Description</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>WAN</td> <td>TCP</td> <td>*</td> <td>*</td> <td>10.9.107.10</td> <td>Web_Services</td> <td>10.9.107.10</td> <td>443 (HTTPS)</td> <td></td> <td><input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Separator"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>WAN</td> <td>TCP</td> <td>*</td> <td>Web</td> <td>10.9.107.10</td> <td>443 (HTTPS)</td> <td>10.9.107.10</td> <td>443 (HTTPS)</td> <td>Redirection vers Serveur Web</td> <td><input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Separator"/></td> </tr> </tbody> </table>						Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions	<input type="checkbox"/>	WAN	TCP	*	*	10.9.107.10	Web_Services	10.9.107.10	443 (HTTPS)		<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Separator"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	Web	10.9.107.10	443 (HTTPS)	10.9.107.10	443 (HTTPS)	Redirection vers Serveur Web	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Separator"/>
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions																											
<input type="checkbox"/>	WAN	TCP	*	*	10.9.107.10	Web_Services	10.9.107.10	443 (HTTPS)		<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Separator"/>																											
<input checked="" type="checkbox"/>	WAN	TCP	*	Web	10.9.107.10	443 (HTTPS)	10.9.107.10	443 (HTTPS)	Redirection vers Serveur Web	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Separator"/>																											
<input type="button" value="Add"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Toggle"/> <input type="button" value="Save"/> <input type="button" value="Separator"/>																																					

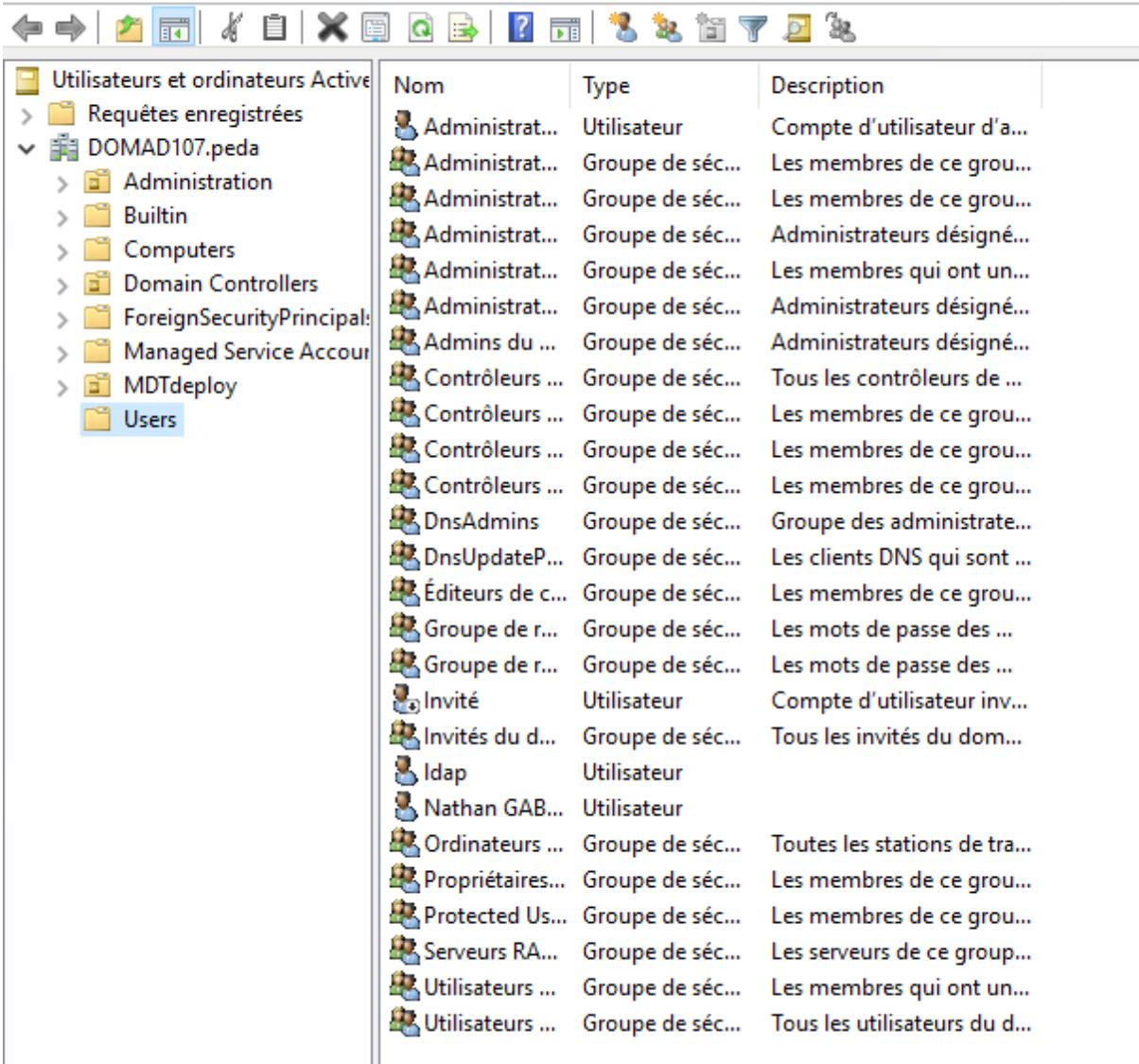
## Configuration des services et applications tiers

### LDAP

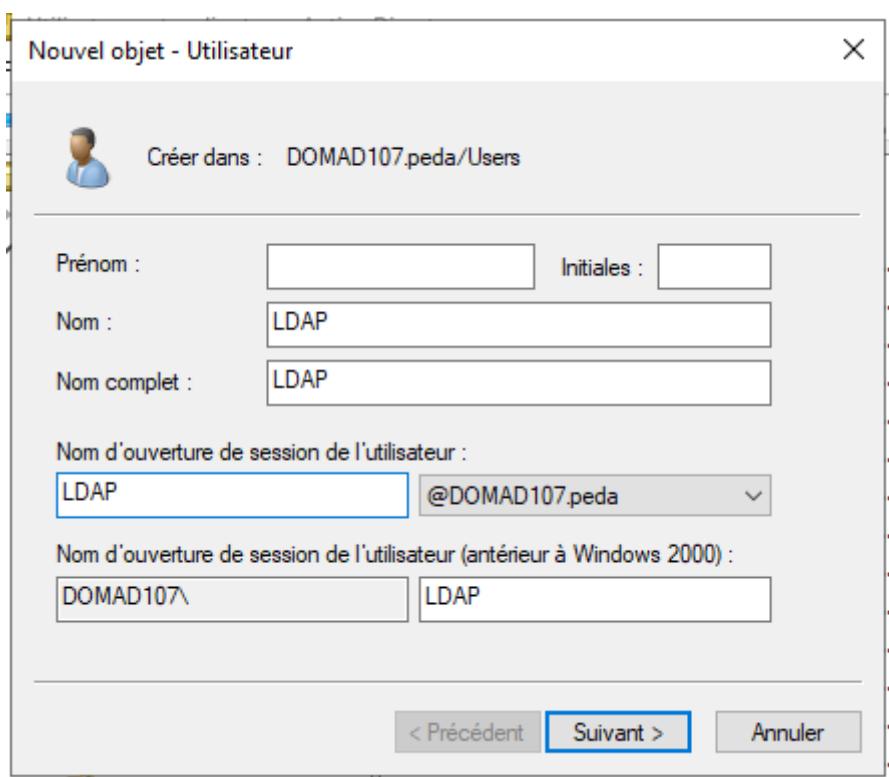
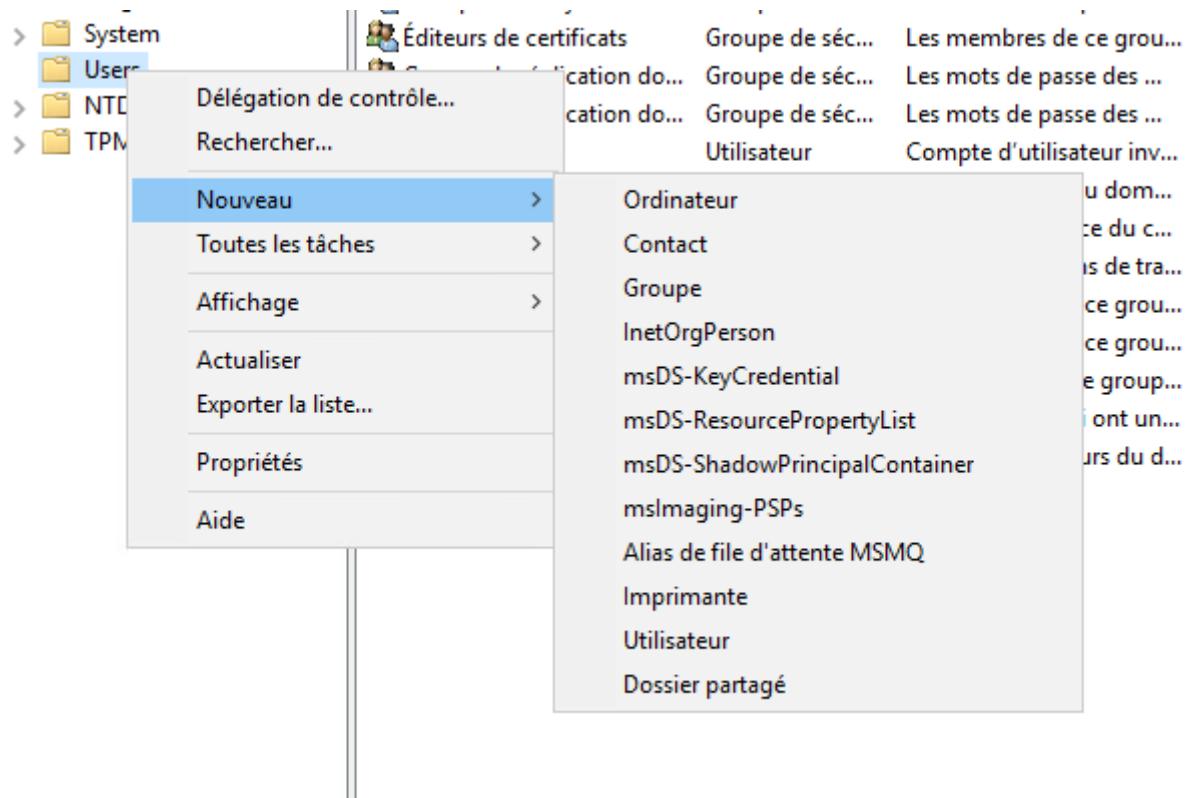


## Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?



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...
DnsAdmins	Groupe de séc...	Groupe des administrat...
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...
Idap	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...



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

System / User Manager / Authentication Servers

?

Users Groups Settings Authentication Servers

Authentication Servers			
Server Name	Type	Host Name	Actions
NGabriele (UT1107-Admin)	LDAP	10.0.107.1	
Local Database		UT1107-pfsense	

Add

## Création et configuration de la machine cliente

### SNMP

### DHCP

Primary Address Pool

Subnet	10.2.107.0/24
Subnet Range	10.2.107.1 - 10.2.107.254
Address Pool Range	<input type="text"/> From <input type="text"/> To
The specified range for this pool must not be within the range configured on any other address pool for this interface.	
Additional Pools	Add Address Pool
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.	

## DHCP Relay

piSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ 

## Services / DHCP Relay

### DHCP Relay Configuration

**Enable**  **Enable DHCP Relay**

**Downstream Interfaces**

WAN
LAN0
LAN1
LAN2

Interfaces without an IPv4 address will not be shown.

**CARP Status VIP**  DHCP Relay will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.

Append circuit ID and agent ID to requests  
Append the circuit ID (interface number) and the agent ID to the DHCP request.

**Upstream Servers**

 The IPv4 addresses of the servers to which DHCP requests are relayed.



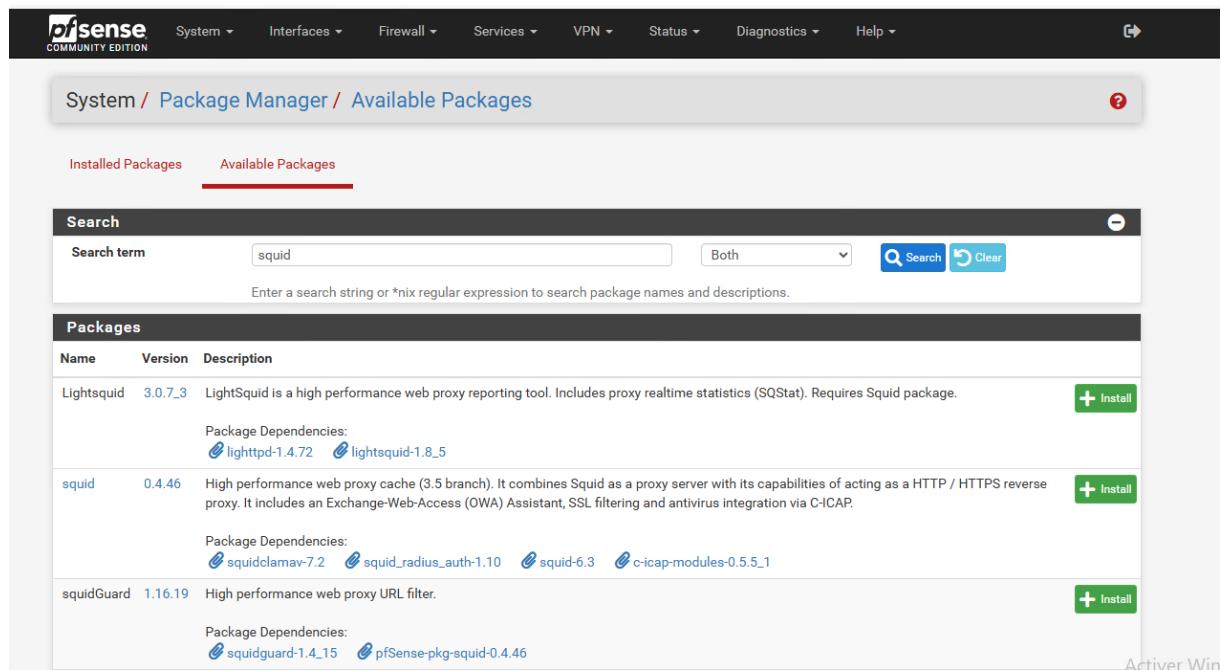
## Activer Window

## Configuration du poste client sous windows 10 en DHCP

### Carte Ethernet Ethernet0 :

C:\Users\utilisateur\_client>

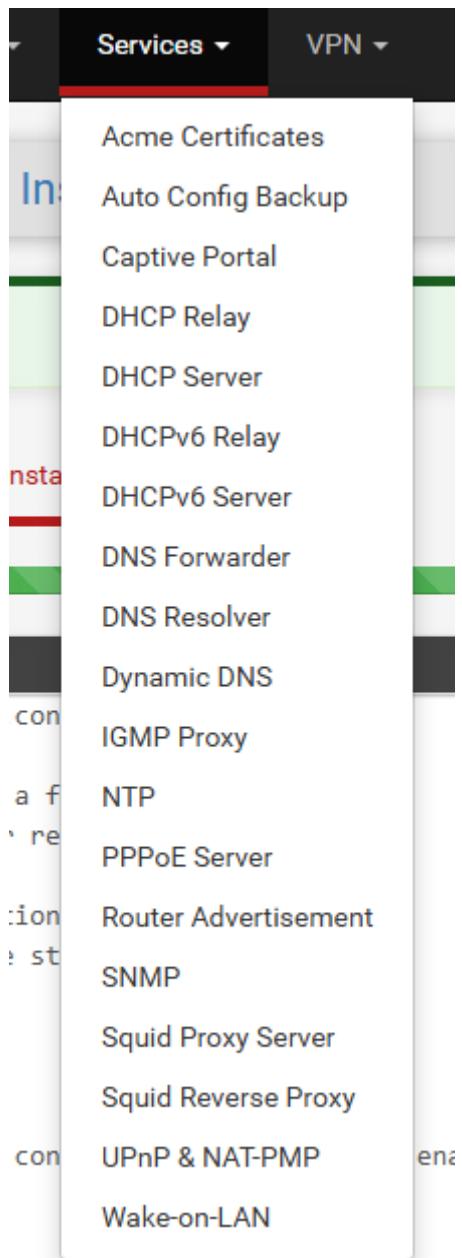
## Mise en place du proxy SquidGuard sur le LAN2

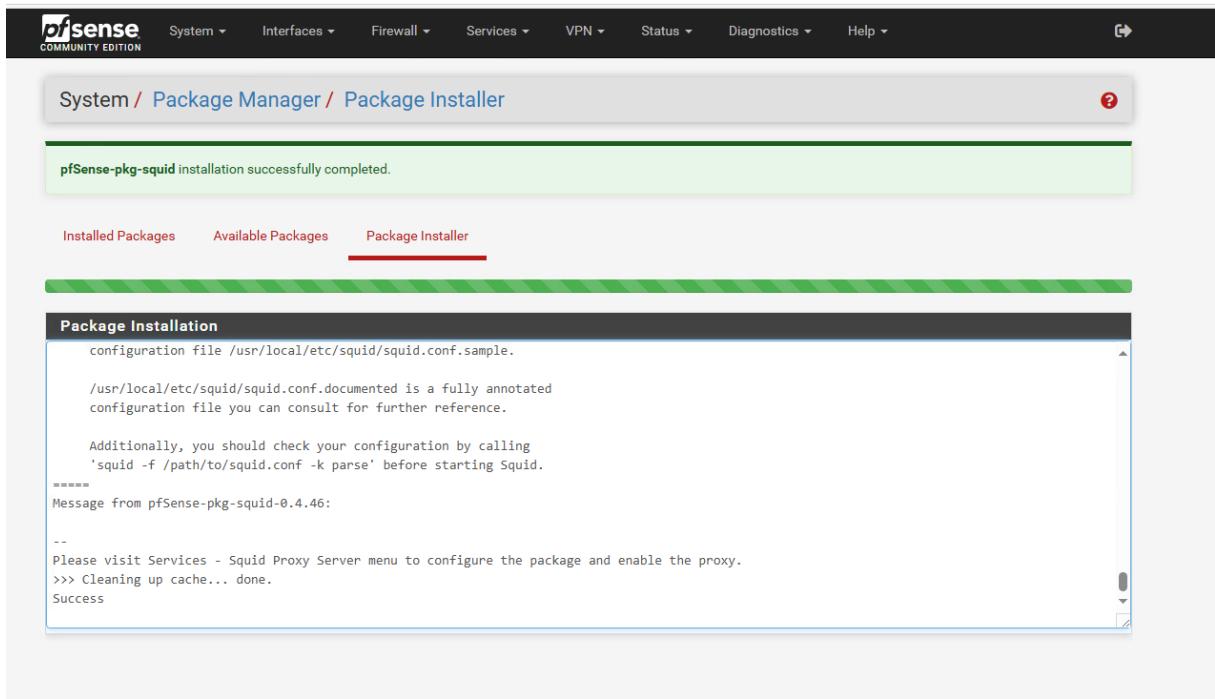


The screenshot shows the pfSense Package Manager interface. The search term 'squid' is entered, and the results list three packages:

Name	Version	Description	Action
Lightsquid	3.0.7_3	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	<a href="#">+ Install</a>
squid	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	<a href="#">+ Install</a>
squidGuard	1.16.19	High performance web proxy URL filter.	<a href="#">+ Install</a>

Package Dependencies are listed for each package, and a note at the bottom right says 'Activer Win'.





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

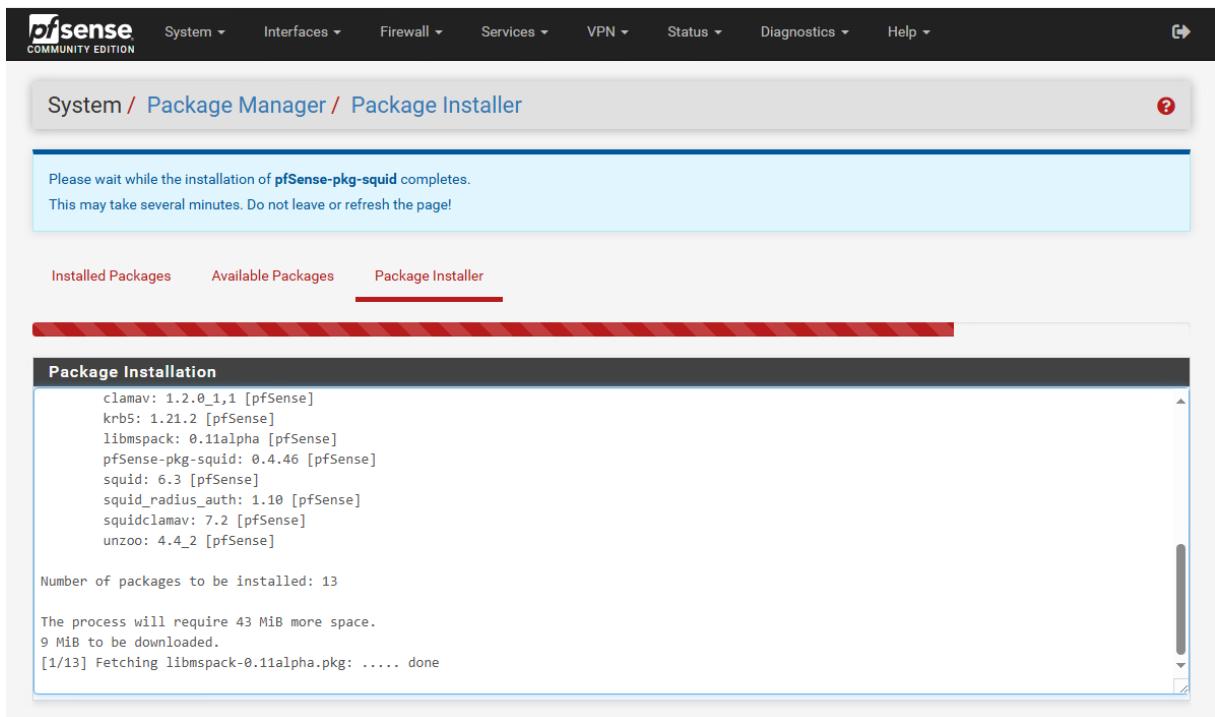
**Package Installation**

```
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
```

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.gz](http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfSense.tar.gz)

 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.gz
Download complete
Unpack archive
Scan blacklist categories.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
```

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.gz](http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfSense.tar.gz)

 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.gz
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**

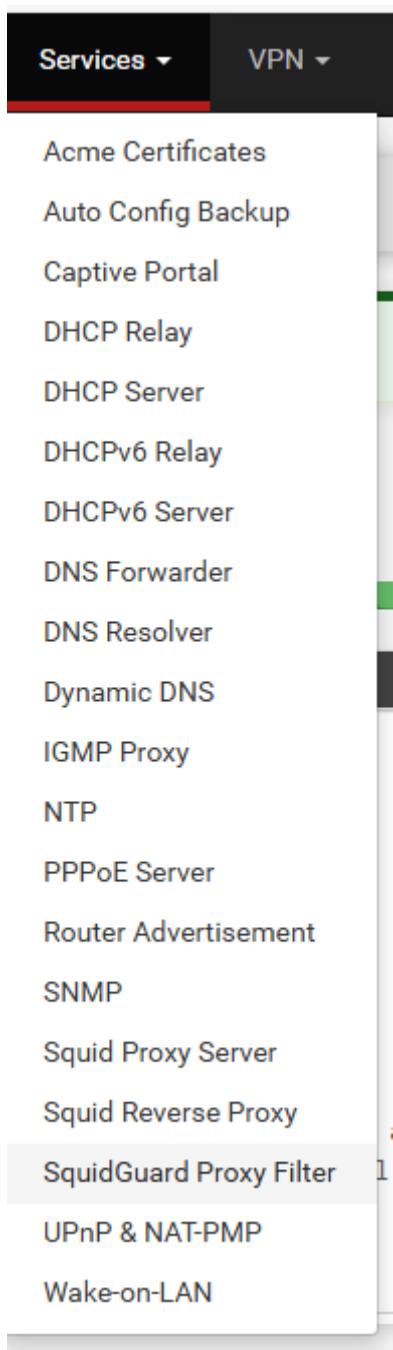
Blacklist upload proxy - enter here, or leave blank.  
Format: host:[port login:pass]. Default proxy port 1080.  
Example: '192.168.0.1:8080 user:pass'

**Blacklist URL**

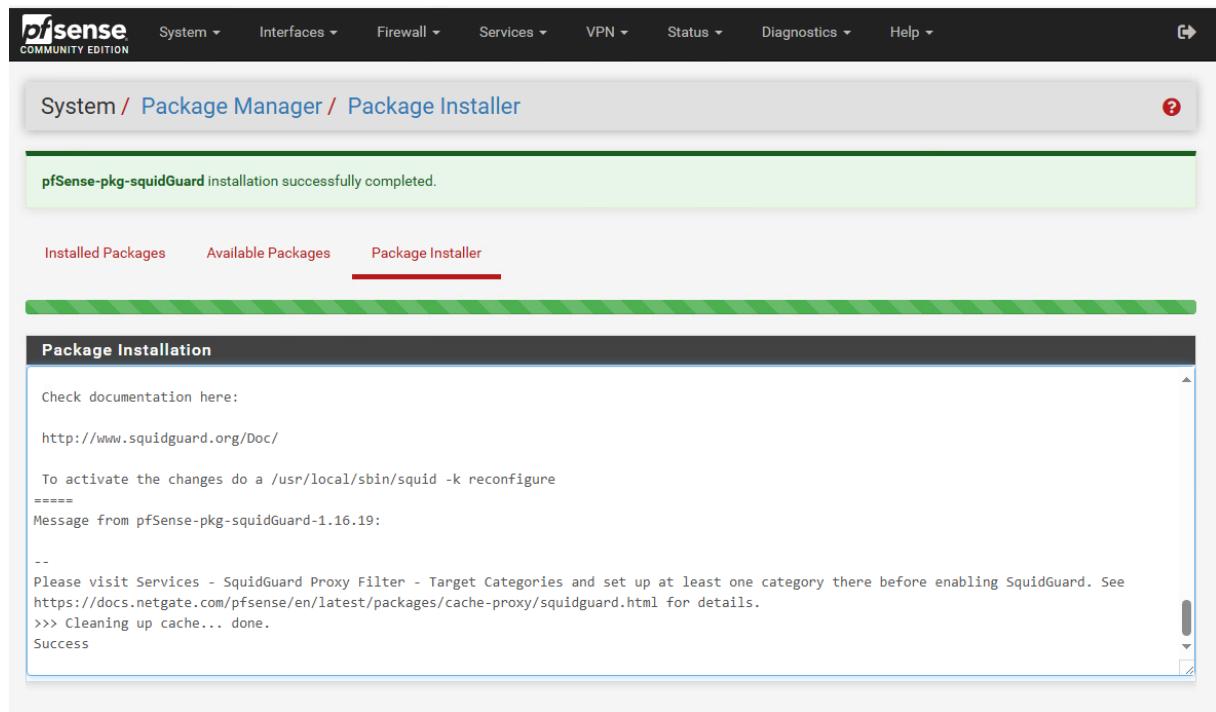
Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).

**Save**

<b>Logging options</b>	
<b>Enable GUI log</b>	<input checked="" type="checkbox"/> Check this option to log the access to the Proxy Filter GUI.
<b>Enable log</b>	<input checked="" type="checkbox"/> 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.
<b>Enable log rotation</b>	<input type="checkbox"/> 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.
<b>Miscellaneous</b>	
<b>Clean Advertising</b>	<input type="checkbox"/> Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.
<b>Blacklist options</b>	
<b>Blacklist</b>	<input checked="" type="checkbox"/> Check this option to enable blacklist
<b>Blacklist proxy</b>	<input type="text"/>
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'	
<b>Blacklist URL</b>	<input type="text" value="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).
<b>Save</b>	



# SquidGuard



pfSense-pkg-squidGuard installation successfully completed.

Installed Packages Available Packages **Package Installer**

**Package Installation**

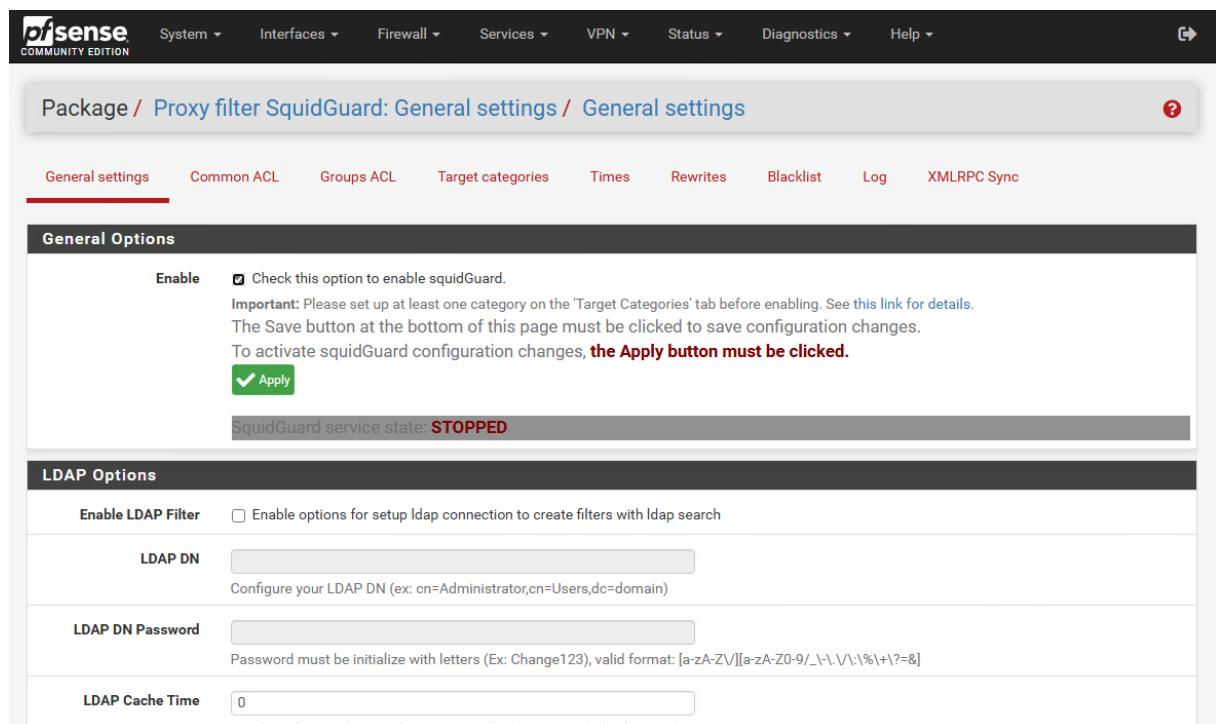
Check documentation here:  
<http://www.squidguard.org/Doc/>

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



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**  Number of seconds to cache LDAP Results (recommended value: 300)

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**

imposts.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.

Erreurs de confidentialité

Non sécurisé | <https://www.impots.gouv.fr>

**ERROR**

**The requested URL could not be retrieved**

The following error was encountered while trying to retrieve the URL: [https://www.impots.gouv.fr/\\*](https://www.impots.gouv.fr/*)

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is [admin@ut107-NGabriele.fr](mailto:admin@ut107-NGabriele.fr).

Generated Thu, 03 Oct 2024 09:49:34 GMT by Proxy (squid)

Erreurs de confidentialité

Paramètres

Erreurs de confidentialité

Erreurs de confidentialité

**!**

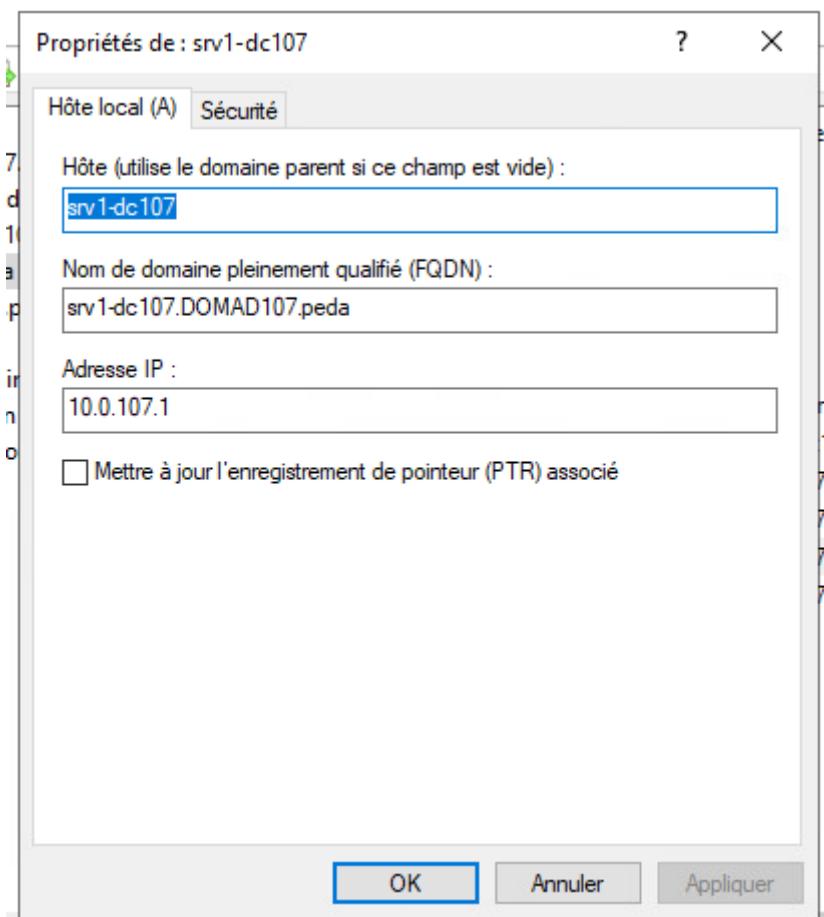
**Votre connexion n'est pas privée**

Les utilisateurs malveillants essaient peut-être de voler vos informations de **www.impots.gouv.fr** (par exemple, les mots de passe, les messages ou les cartes de crédit). [En savoir plus à propos de cet avertissement](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Avancé

Retour



## Certificats

System / Advanced / Admin Access

Admin Access    Firewall & NAT    Networking    Miscellaneous    System Tunables    Notifications

**webConfigurator**

Protocol	<input type="radio"/> HTTP	<input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate	10.0.107.254	
Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.		
TCP port	8443	
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.		
Max Processes	2	
Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.		
WebGUI redirect	<input type="checkbox"/> Disable webConfigurator redirect rule	
When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.		
HSTS	<input type="checkbox"/> Disable HTTP Strict Transport Security	
When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to		

Secure Shell

Secure Shell Server	<input checked="" type="checkbox"/> Enable Secure Shell
SSHD Key Only	<input type="button" value="Require Both Password and Public Key"/> <small>When set to <i>Public Key Only</i>, SSH access requires authorized keys and these keys must be configured for each <a href="#">user</a> that has been granted secure shell access. If set to <i>Require Both Password and Public Key</i>, the SSH daemon requires both authorized keys <b>and</b> valid passwords to gain access. The default <i>Password or Public Key</i> setting allows either a valid password or a valid authorized key to login.</small>
Allow Agent Forwarding	<input checked="" type="checkbox"/> Enables ssh-agent forwarding support.
SSH port	22
<small>Note: Leave this blank for the default of 22.</small>	


≡

## 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:  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	UserDestination
26.09.2024 10:03:49	10.2.107.10	NONE_NONE/000error	:transaction-end-before-headers	- -
26.09.2024 10:03:49	10.2.107.10	NONE_NONE/000error	: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/000error	:transaction-end-before-headers	- -
26.09.2024 09:58:49	10.2.107.10	NONE_NONE/000error	:transaction-end-before-headers	- -
26.09.2024 09:57:49	10.2.107.10	NONE_NONE/000error	:transaction-end-before-headers	- -
26.09.2024 09:57:49	10.2.107.10	NONE_NONE/000error	: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/2023/03/386778	93.184.221.240
			49_cc9dc29ea42a05f4d58025a89f733b2b9f34671.cab	
26.09.2024 09:56:54	10.2.107.10	TCP_MISS/200	http://download.windowsupdate.com/d/msdownload/update/others/2023/11/401010	93.184.221.240
			64_ecd34a842579b09671f21e3ccab93ff98d9057d1.cab	
26.09.2024 09:56:54	10.2.107.10	TCP_MISS/200	http://download.windowsupdate.com/c/msdownload/update/others/2023/04/388128	93.184.221.240
			57_b6be8137bd471ae5a775b5ed2d85a85dcf8d068.cab	

**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
26.09.2024 10:27:13	WARNING: log name now starts with a module name. Use 'stdio:/var/squid/logs/netdb.state'.

## Blacklists :

Enter addresses/URLs in plain format. Comma separated entries must not be enclosed to use the proxy.  
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/

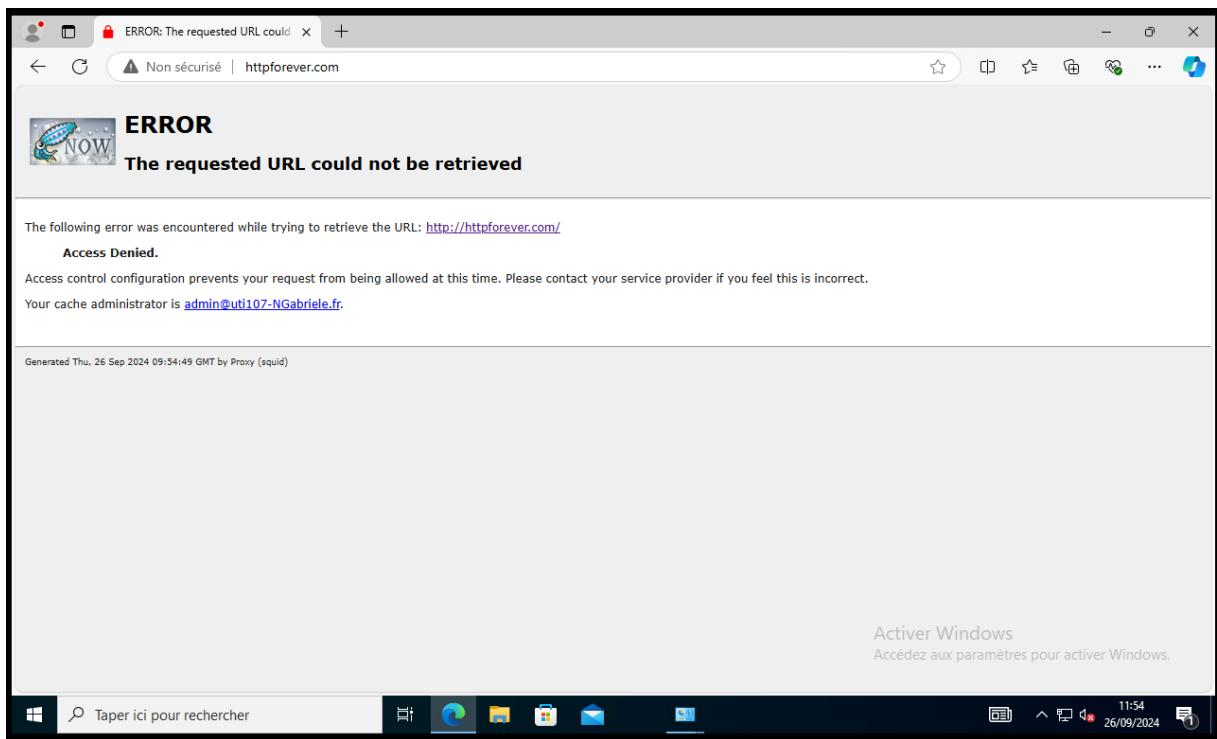
Destination domains that will be blocked for the users that are allowed to use the proxy.  
Put each entry on a separate line. You can also use regular expressions.

**Block User Agents**

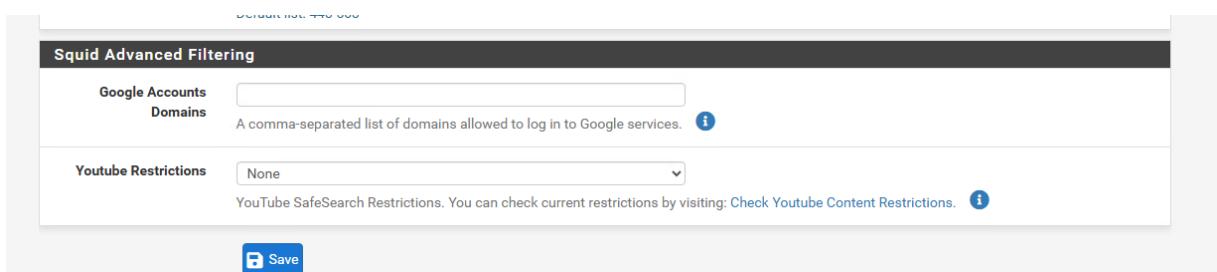
Enter user agents that will be blocked for the users that are allowed to use the proxy.  
Put each entry on a separate line. You can also use regular expressions.

**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

<b>Visible Hostname</b>	Proxy UTI107-NGabriele
	This is the hostname to be displayed in proxy server error messages.
<b>Administrator's Email</b>	admin@uti107-NGabriele.fr
	This is the email address displayed in error messages to the users.
<b>Error Language</b>	fr
	Select the language in which the proxy server will display error messages to users.
<b>X-Forwarded Header Mode</b>	(on)
	Choose how to handle X-Forwarded-For headers. Default: on <a href="#">i</a>
<b>Disable VIA Header</b>	<input type="checkbox"/> If not set, Squid will include a Via header in requests and replies as required by RFC2616.
<b>URI Whitespace Characters Handling</b>	strip
	Choose how to handle whitespace characters in URL. Default: strip <a href="#">i</a>
<b>Suppress Squid Version</b>	<input checked="" type="checkbox"/> Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

[Save](#) [Show Advanced Options](#)

Activer Windows

<b>Enable Access Logging</b>	<input checked="" type="checkbox"/> This will enable the access log. <b>Warning:</b> Do NOT enable if available disk space is low.
<b>Log Store Directory</b>	/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 <b>Important:</b> DO NOT include the trailing / when setting a custom location.
<b>Rotate Logs</b>	365
	Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
<b>Log Pages Denied by SquidGuard</b>	<input type="checkbox"/> Makes it possible for SquidGuard denied log to be included on Squid logs. Click Info for detailed instructions. <a href="#">i</a>

### Headers Handling, Language and Other Customizations

<b>Visible Hostname</b>	localhost
	This is the hostname to be displayed in proxy server error messages.
<b>Administrator's Email</b>	admin@localhost
	This is the email address displayed in error messages to the users.
<b>Error Language</b>	en
	Select the language in which the proxy server will display error messages to users.
<b>X-Forwarded Header Mode</b>	(on)
	Choose how to handle X-Forwarded-For headers. Default: on <a href="#">i</a>
<b>Disable VIA Header</b>	<input type="checkbox"/> If not set, Squid will include a Via header in requests and replies as required by RFC2616.
<b>URI Whitespace Characters Handling</b>	strip
	Choose how to handle whitespace characters in URL. Default: strip <a href="#">i</a>
<b>Suppress Squid Version</b>	<input type="checkbox"/> Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

[Save](#) [Show Advanced Options](#)

Activer Windows  
Accédez aux

### 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)**   
  
  
 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 paramètres

## 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.

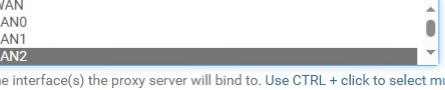
**Keep Settings/Data**  If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.

**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 synchronization.

**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**   
 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.

<b>Cache Size</b>	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) 
<b>Maximum Object Size in RAM</b>	256 Objects greater than this size (in kilobytes) will not be attempted to kept in the memory cache. Default: 256 (KB)
<b>Memory Replacement Policy</b>	Heap GDSF The memory replacement policy determines which objects are purged from memory when space is needed. Default: heap GDSF 
<b>Dynamic and Update Content</b>	
<b>Cache Dynamic Content</b>	<input type="checkbox"/> Select to enable caching of dynamic content. With <a href="#">dynamic cache</a> enabled, you can also apply <a href="#">refresh_patterns</a> to sites like <a href="#">Windows Updates</a> . 
<b>Custom refresh_patterns</b>	<div style="border: 1px solid #ccc; padding: 5px; height: 150px; width: 100%;"></div> <p>Enter custom refresh_patterns for better dynamic cache usage. <b>Note:</b> These refresh_patterns will only be included if 'Cache Dynamic Content' is enabled.</p>
     	

## Squid Hard Disk Cache Settings

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

Activar Windows  
Acceder a mi perfil

### Squid Hard Disk Cache Settings

<b>Hard Disk Cache Size</b>	<input type="text" value="100"/> 100	Amount of disk space (in megabytes) to use for cached objects.
<b>Hard Disk Cache System</b>	<input type="text" value="ufs"/> ufs	
This specifies the kind of storage system to use. <a href="#">i</a>		
<b>Clear Disk Cache NOW</b>	Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron. <a href="#">i</a>	
If you wish to clear cache <b>immediately</b> , click this button <b>once</b> : <a href="#">Clear Disk Cache NOW</a>		
<b>Level 1 Directories</b>	<input type="text" value="16"/> 16	Specifies the number of Level 1 directories for the hard disk cache. <a href="#">i</a>
<b>Hard Disk Cache Location</b>	<input type="text" value="/var/squid/cache"/> /var/squid/cache	
This is the directory where the cache will be stored. Default: /var/squid/cache <a href="#">i</a>		
<b>Minimum Object Size</b>	<input type="text" value="0"/> 0	Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)
<b>Maximum Object Size</b>	<input type="text" value="4"/> 4	Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB) <a href="#">i</a>

### Squid Memory Cache Settings

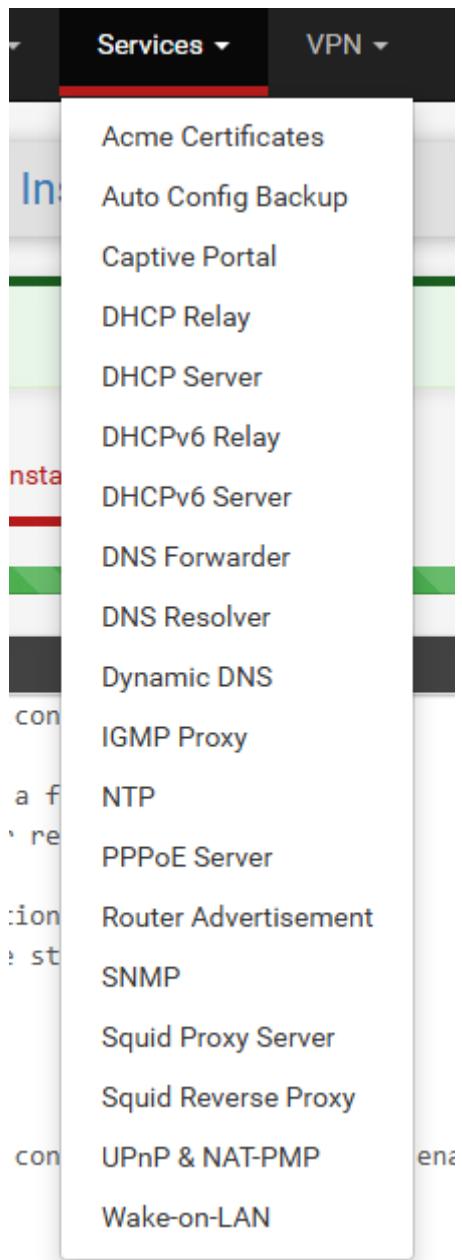
Activer Windows  
Accédez aux paramètres pour

### Squid Hard Disk Cache Settings

<b>Hard Disk Cache Size</b>	<input type="text" value="100"/>	Amount of disk space (in megabytes) to use for cached objects.
<b>Hard Disk Cache System</b>	<input type="text" value="ufs"/>	This specifies the kind of storage system to use. <a href="#">i</a>
<b>Clear Disk Cache NOW</b>	Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron. <a href="#">i</a>	
<p>If you wish to clear cache <b>immediately</b>, click this button <b>once</b>:  <b>Clear Disk Cache NOW</b></p>		
<b>Level 1 Directories</b>	<input type="text" value="16"/>	Specifies the number of Level 1 directories for the hard disk cache. <a href="#">i</a>
<b>Hard Disk Cache Location</b>	<input type="text" value="/var/squid/cache"/>	
<b>Minimum Object Size</b>	<input type="text" value="0"/>	Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)
<b>Maximum Object Size</b>	<input type="text" value="4"/>	Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB) <a href="#">i</a>

### Squid Memory Cache Settings

Activer Windows  
Accédez aux paramètres po



ClamAV

## 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](#)

<b>ClamAV Database Update</b>	never
	never
	every 1 hour
	every 2 hours
	every 3 hours
	every 4 hours
	<b>every 6 hours</b>
	every 8 hours
	every 12 hours
	every 24 hours

---

<b>Regional ClamAV Database Mirror</b>	never
	never
	every 1 hour
	every 2 hours
	every 3 hours
	every 4 hours
	<b>every 6 hours</b>
	every 8 hours
	every 12 hours
	every 24 hours

**ClamAV Database Update**

every 6 hours

Optional, you can schedule ClamAV definitions updates via cron. Select the desired frequency here. [i](#)

**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](#)

Active Windows

## 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](#)  

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
<input type="checkbox"/> WAN (vmx1)	 	AC-BNFA	DISABLED	WAN	  

 [Add](#)  [Delete](#)

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

Cron Schedules						
minute	hour	mday	month	wday	who	command
*/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_uritables
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

pfSense COMMUNITY EDITION

Status / Dashboard

**Available Widgets**

- + Captive Portal Status
- + Firewall Logs
- + Interface Statistics
- + OpenVPN
- + Services Status
- + Wake-on-Lan
- + CARP Status
- + Gateways
- + Interfaces
- + Picture
- + Squid Antivirus Status
- + Disks
- + GEOM Mirror Status
- + IPsec
- + RSS
- + System Information
- + Dynamic DNS Status
- + Installed Packages
- + NTP Status
- + S.M.A.R.T. Status
- + Thermal Sensors

Other dashboard settings are available from the [General Setup](#) page.

**System Information**

Name	UT1107-pfsense.UT1107-GW.arpa
User	NGabriele@10.0.107.10 (Local Database)
System	VMware Virtual Machine Netgate Device ID: 473b00e22da3d05088ab
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Wed Dec 12 2018
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT
The system is on the latest version. Version information updated at Wed Nov 27 7:01:24 UTC 2024	
CPU Type	Intel(R) Xeon(R) Silver 4116 CPU @ 2.10GHz AES-NI CPU Crypto: Yes (inactive)

**Traffic Graphs**

**WAN**

**LAN0**

**Interfaces**

WAN	autoselect	192.168.10.107
LAN0	autoselect	10.0.107.254
LAN1	autoselect	10.1.107.254
LAN2	autoselect	10.2.107.254
DMZ	autoselect	10.9.107.254

**Snort Alerts**

Interface/Time	Src/Dst Address	Description
WAN Nov 26 11:35:02	208.115.231.182:80 192.168.10.107:44719	(http_inspect) PROTOCOL- OTHER HTTP server response...
WAN Nov 26 11:24:37	208.115.231.182:80 192.168.10.107:44719	(http_inspect) PROTOCOL- OTHER HTTP server response...
WAN Nov 26 11:24:37	208.115.231.182:80 192.168.10.107:44719	(http_inspect) PROTOCOL- OTHER HTTP server response...
WAN Nov 26 11:24:37	208.115.231.182:80 192.168.10.107:44719	(http_inspect) PROTOCOL- OTHER HTTP server response...
WAN Nov 26 11:24:37	208.115.231.182:80 192.168.10.107:44719	(http_inspect) NO CONTENT- LENGTH OR TRANSFER-...

**DMZ**

**Gateways**

Name	RTT	RTTsd	Loss	Status
WAN_UT1107_NGabrieleGW 192.168.10.254	0.4ms	0.2ms	0.0%	Online

**Picture**

Widget title: Picture

New pictures: Parcourir... Aucun fichier sélectionné.

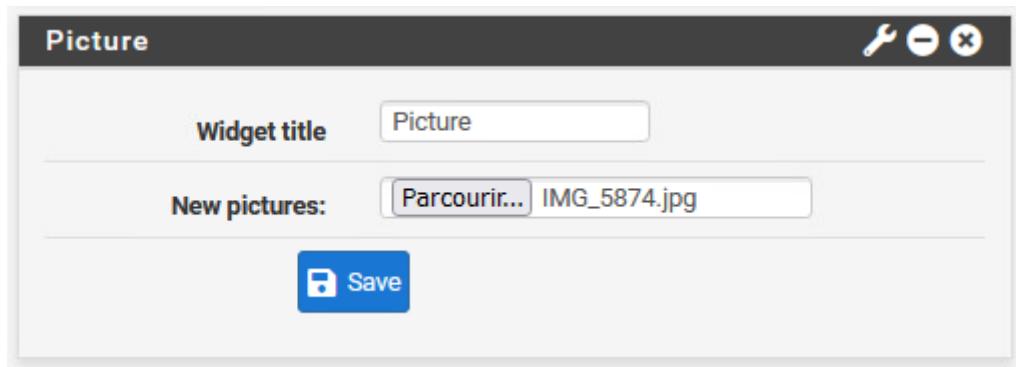
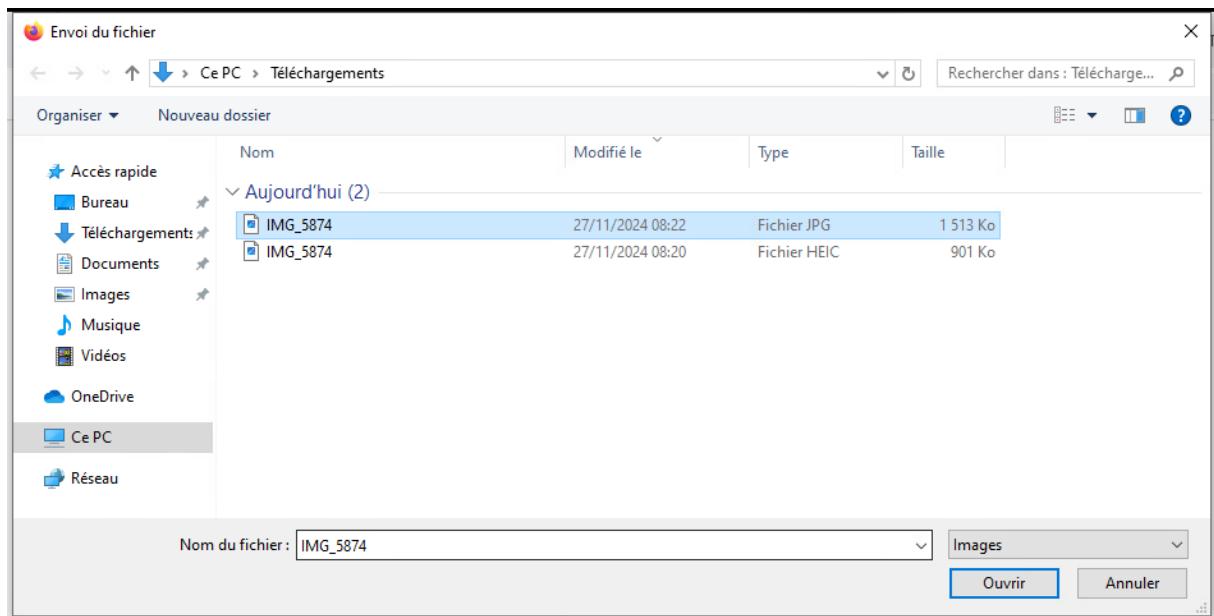
Squid Antivirus Status				
Squid Version	6.3			
Antivirus Scanner	ClamAV 1.2.0_1,1 C-ICAP 0.5.10_1,2 + SquidClamav 7.2			
Antivirus Bases	Database	Date	Version	Builder
	daily.cld	2024.11.26	27469	raynman
	bytecode.cvd	2024.02.27	335	raynman
	main.cvd	2021.09.16	62	sigmgr
Last Update	Tue Nov 26 09:58:20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

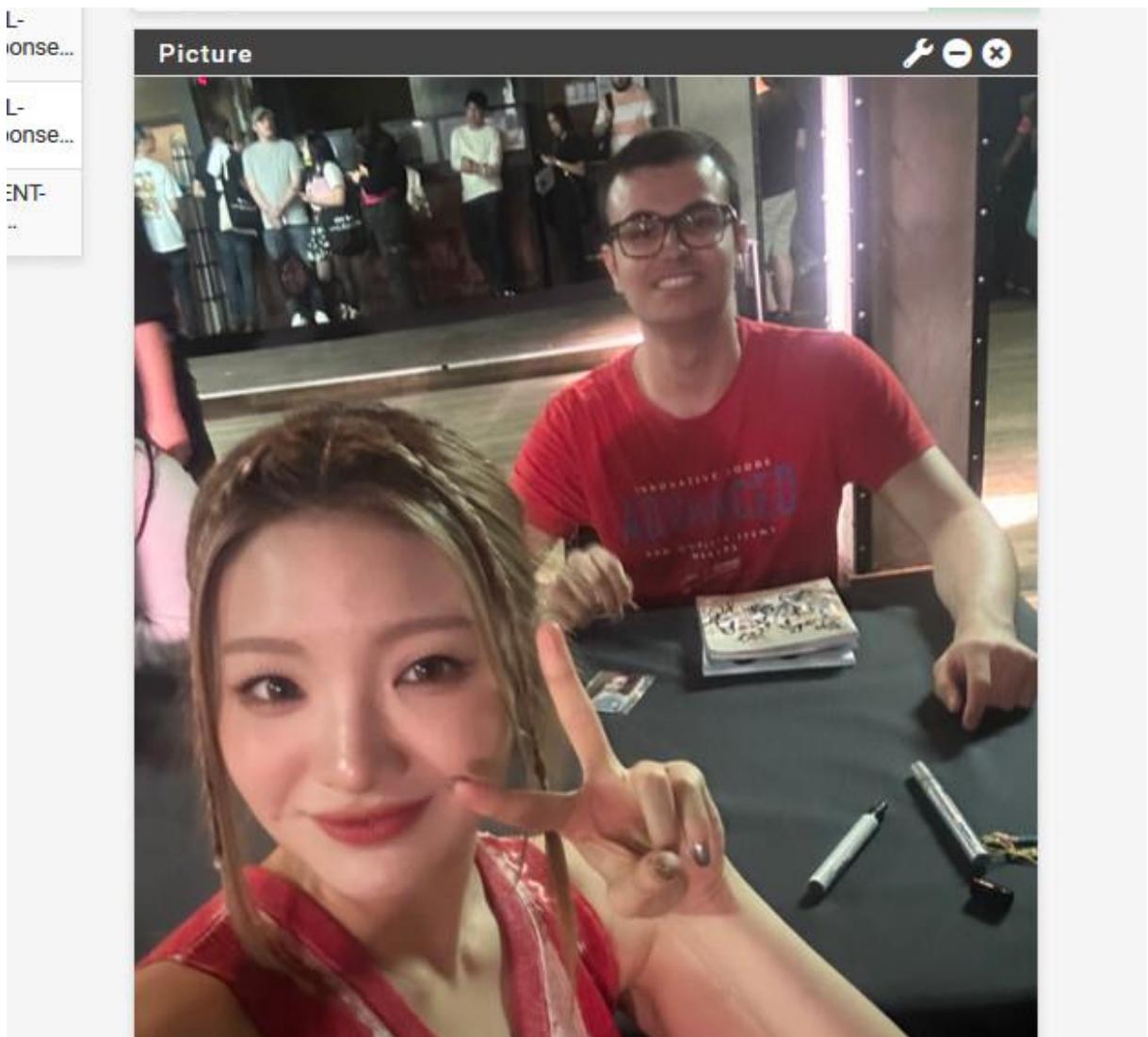
**Picture**

Widget title: Picture

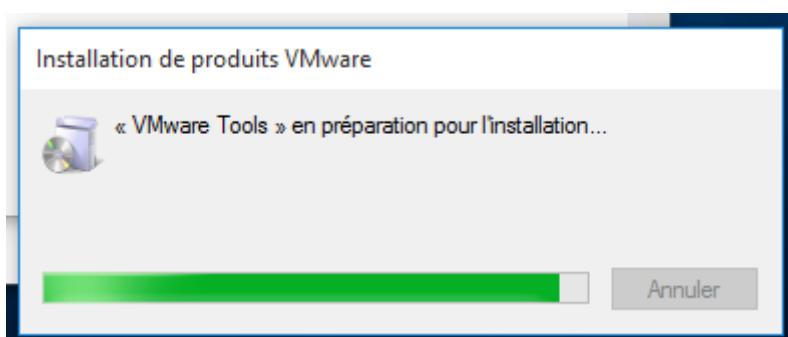
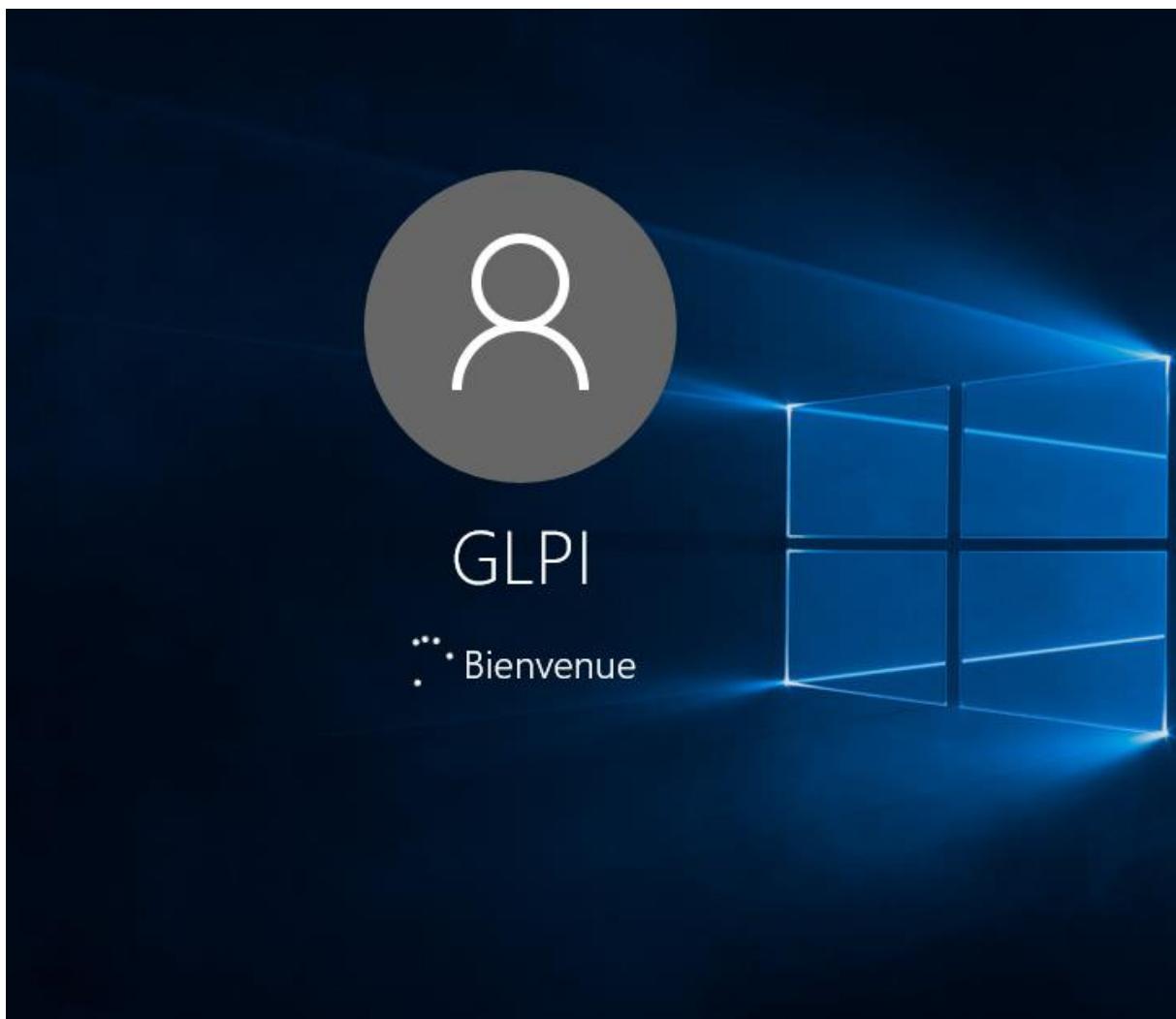
New pictures: Parcourir... Aucun fichier sélectionné.

**Save**





## Installation de GLPI



# Réseaux



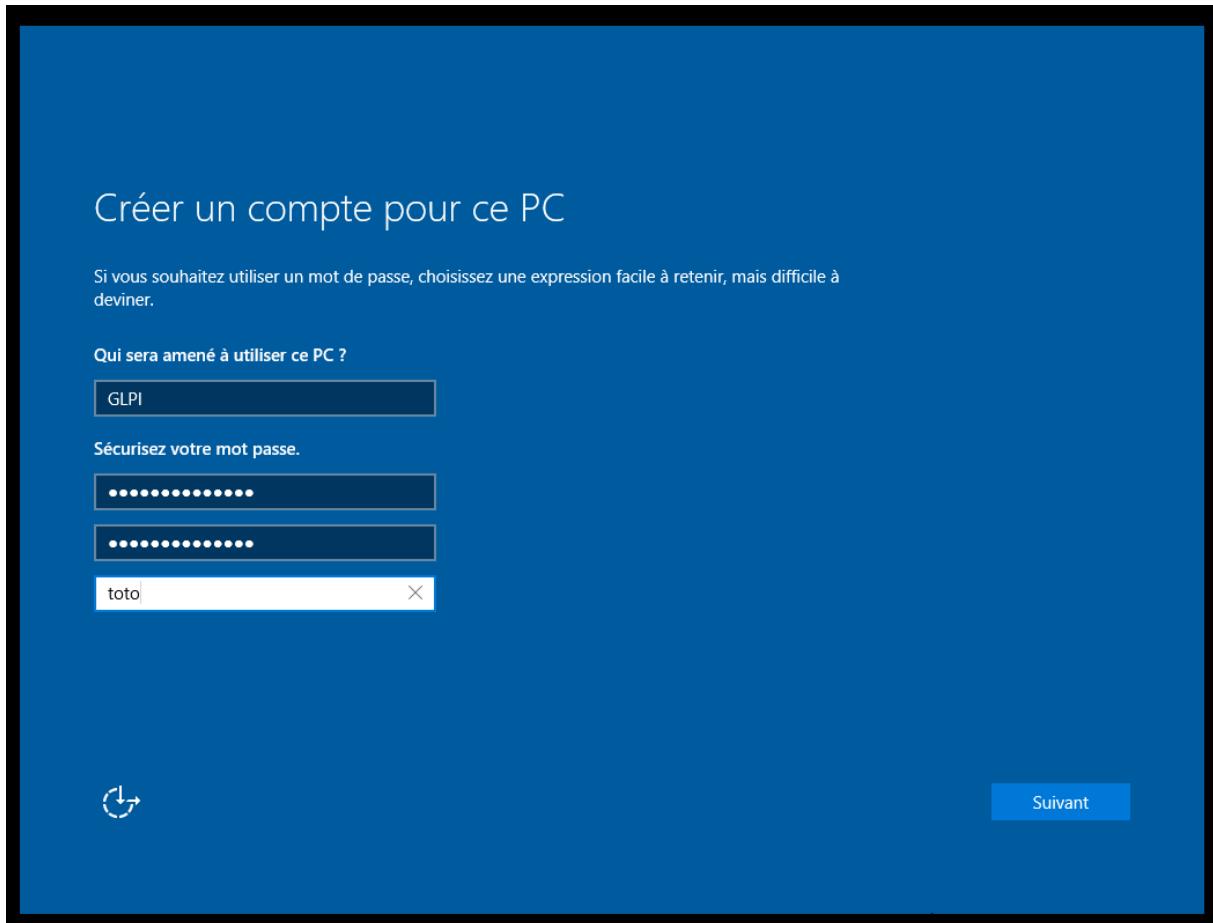
## Réseau

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



Accédez au Rapport GLPI

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

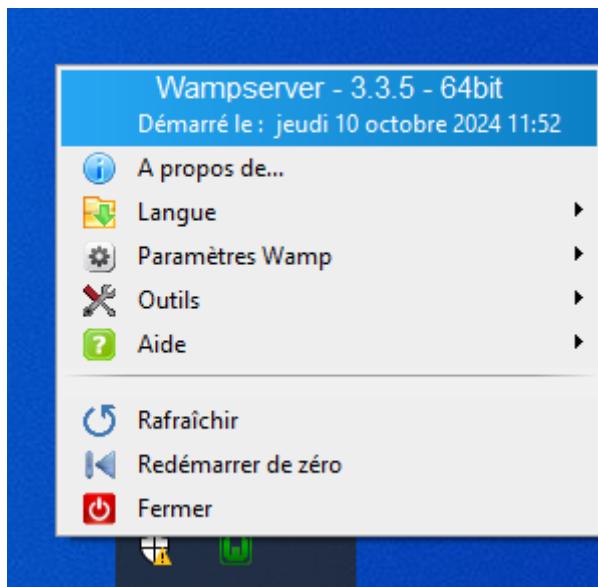
Administrateurs / Utilisateurs / Développeurs / GLPI Agent

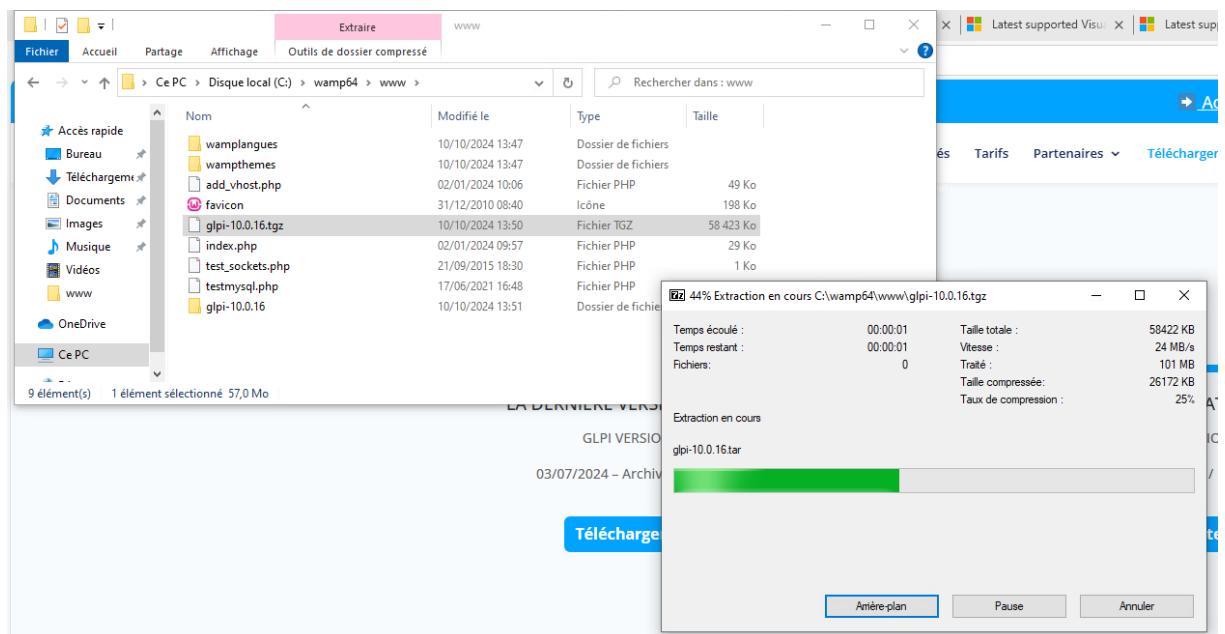
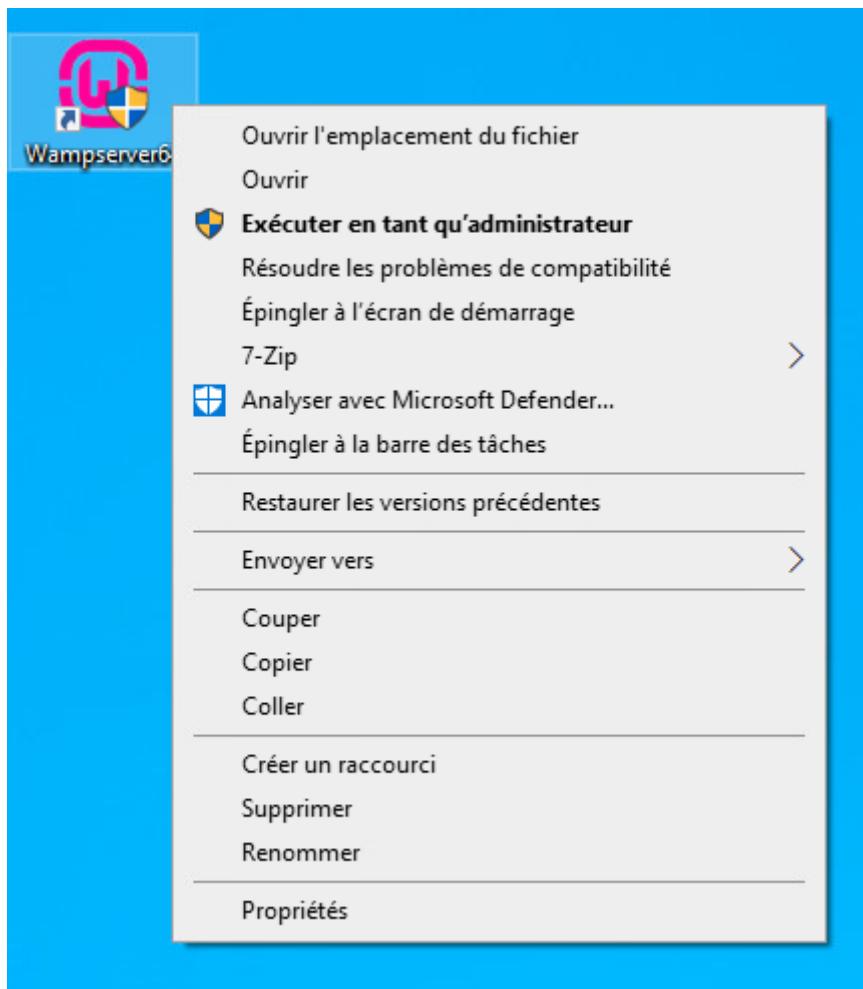
Consulter >

Téléchargements

- glpi-10.0.16.tgz
- vccredit\_x64 (2).exe
- vccredit\_x86 (2).exe
- vccredit\_x64 (1).exe
- vccredit\_x86 (1).exe
- vccredit\_x86.exe
- vccredit\_x64.exe
- wampserver3.3.5\_x64.exe

Afficher plus





## ✓ 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

Firewall / Rules / Edit

**Edit Firewall Rule**

**Action**  Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule Set this option to disable this rule without removing it from the list.

**Interface**  Choose the interface from which packets must come to match this rule.

**Address Family**  Select the Internet Protocol version this rule applies to.

**Protocol**  Choose which IP protocol this rule should match.

**ICMP Subtypes**     For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

**Source**

**Source**  Invert match   /

**Destination**

**Destination**  Invert match   /

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 ? [0/n] 0
Récception 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 kB 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_2k3a12.3.5-3~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 zeroconf
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 zeroconf
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 ? [0/n] 0
```

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

Activités Terminal 14 oct. 15:03

nextcloud@nextcloud-virtual-machine: ~

```

Dépaquetage de libsmclient:amd64 (2:4.15.13+dfsg-0ubuntu1.6) sur (2:4.15.9+dfsg-0ubuntu0.2) ...
Préparation du dépaquetage de .../08-samba-libs_2%3a4.15.13+dfsg-0ubuntu1.6_amd64.deb ...
Dépaquetage de samba-libs:amd64 (2:4.15.13+dfsg-0ubuntu1.6) sur (2:4.15.9+dfsg-0ubuntu0.2) ...
Préparation du dépaquetage de .../09-libwbclient0_2%3a4.15.13+dfsg-0ubuntu1.6_amd64.deb ...
Dépaquetage de libwbclient0:amd64 (2:4.15.13+dfsg-0ubuntu1.6) sur (2:4.15.9+dfsg-0ubuntu0.2) ...
Préparation du dépaquetage de .../10-python-apt-common_2.4.0ubuntu4_all.deb ...
Dépaquetage de python-apt-common (2.4.0ubuntu4) sur (2.3.0ubuntu2.1) ...
Préparation du dépaquetage de .../11-distro-info-data_0.52ubuntu0.7_all.deb ...
Dépaquetage de distro-info-data (0.52ubuntu0.7) sur (0.52ubuntu0.1) ...
Préparation du dépaquetage de .../12-python3-apt_2.4.0ubuntu4_amd64.deb ...
Dépaquetage de python3-apt (2.4.0ubuntu4) sur (2.3.0ubuntu2.1) ...
Préparation du dépaquetage de .../13-language-selector-gnome_0.219.1_all.deb ...
Dépaquetage de language-selector-gnome (0.219.1) sur (0.219) ...
Préparation du dépaquetage de .../14-language-selector-common_0.219.1_all.deb ...
Dépaquetage de language-selector-common (0.219.1) ...
Préparation du dépaquetage de .../15-im-config_0.50-2ubuntu22.04.1_all.deb ...
Dépaquetage de im-config (0.50-2ubuntu22.04.1) sur (0.50-2) ...
Préparation du dépaquetage de .../16-evolution-data-server_3.44.4-0ubuntu1.1_amd64.deb ...
Dépaquetage de evolution-data-server (3.44.4-0ubuntu1.1) sur (3.44.2-0ubuntu1) ...
Préparation du dépaquetage de .../17-libcamel1.2-63.3_3.44.4-0ubuntu1.1_amd64.deb ...
Dépaquetage de libcamel1.2-63.3_3.44.4-0ubuntu1.1 (3.44.4-0ubuntu1) ...
Préparation du dépaquetage de .../18-libecal2.0-1_3.44.4-0ubuntu1.1_amd64.deb ...
Dépaquetage de libecal2.0-1:amd64 (3.44.4-0ubuntu1.1) sur (3.44.2-0ubuntu1) ...
Sélection du paquet libatomic1:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../19-libatomic1_12.3.0-1ubuntu1-22.04_amd64.deb ...
Dépaquetage de libatomic1:amd64 (12.3.0-1ubuntu1-22.04) ...
Préparation du dépaquetage de .../20-gir1.2-webkit2-4.0_2.44.3-0ubuntu0.22.04.1_amd64.deb ...
Dépaquetage de gir1.2-webkit2-4.0:amd64 (2.44.3-0ubuntu0.22.04.1) sur (2.36.4-0ubuntu0.22.04.1) ...
Préparation du dépaquetage de .../21-gir1.2-javascriptcoregtk-4.0_2.44.3-0ubuntu0.22.04.1_amd64.deb ...
Dépaquetage de gir1.2-javascriptcoregtk-4.0:amd64 (2.44.3-0ubuntu0.22.04.1) sur (2.36.4-0ubuntu0.22.04.1) ...
Préparation du dépaquetage de .../22-libwebkit2gtk-4.0-37_2.44.3-0ubuntu0.22.04.1_amd64.deb ...
Dépaquetage de libwebkit2gtk-4.0-37:amd64 (2.44.3-0ubuntu0.22.04.1) sur (2.36.4-0ubuntu0.22.04.1) ...
Préparation du dépaquetage de .../23-libjavascriptcoregtk-4.0-18_2.44.3-0ubuntu0.22.04.1_amd64.deb ...
Dépaquetage de libjavascriptcoregtk-4.0-18:amd64 (2.44.3-0ubuntu0.22.04.1) sur (2.36.4-0ubuntu0.22.04.1) ...

Progression : [ 21% [#####

```

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%

Prétraitement des actions différentes (« triggers ») pour empêchez nos phpMyAdmin (0.1.2-1ubuntu2.1) ...

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 (6.0-2ubuntu3.2).

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 php8.1-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 liblftd1-2
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-perl libdbi-perl libfcgi-bin libfcgi-perl libfcgi0ldbl
  libhtml-template-perl libmariadb3 libmysqlclient21 libbonig5 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-peach 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 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 libbonig5 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-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 ? [0/n] 0
```

```
Il est nécessaire de prendre 798 Mo dans les archives.
Après cette opération, 291 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n] 0
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. Echec 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://fr.archive.ubuntu.com/ubuntu jammy/main DEP-11 64x64@2 Icons [15,8 kB]
Réception de :21 http://fr.archive.ubuntu.com/ubuntu jammy/main amd64 c-n-f Metadata [30,3 kB]
Réception de :22 http://fr.archive.ubuntu.com/ubuntu jammy/restricted i386 Packages [30,4 kB]
```

```
rm -rf /var/www/html/nextcloud
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.

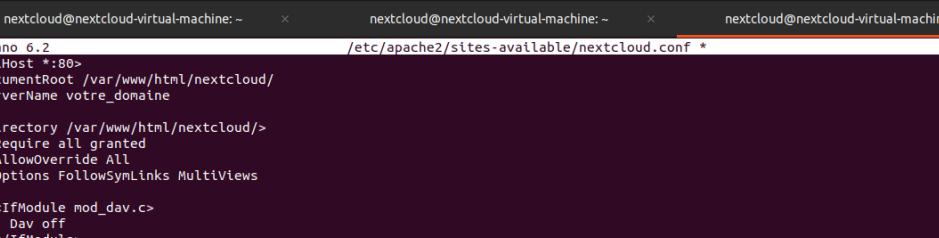
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

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

MariaDB [(none)]> GRANT ALL ON nextcloud.* 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$
```



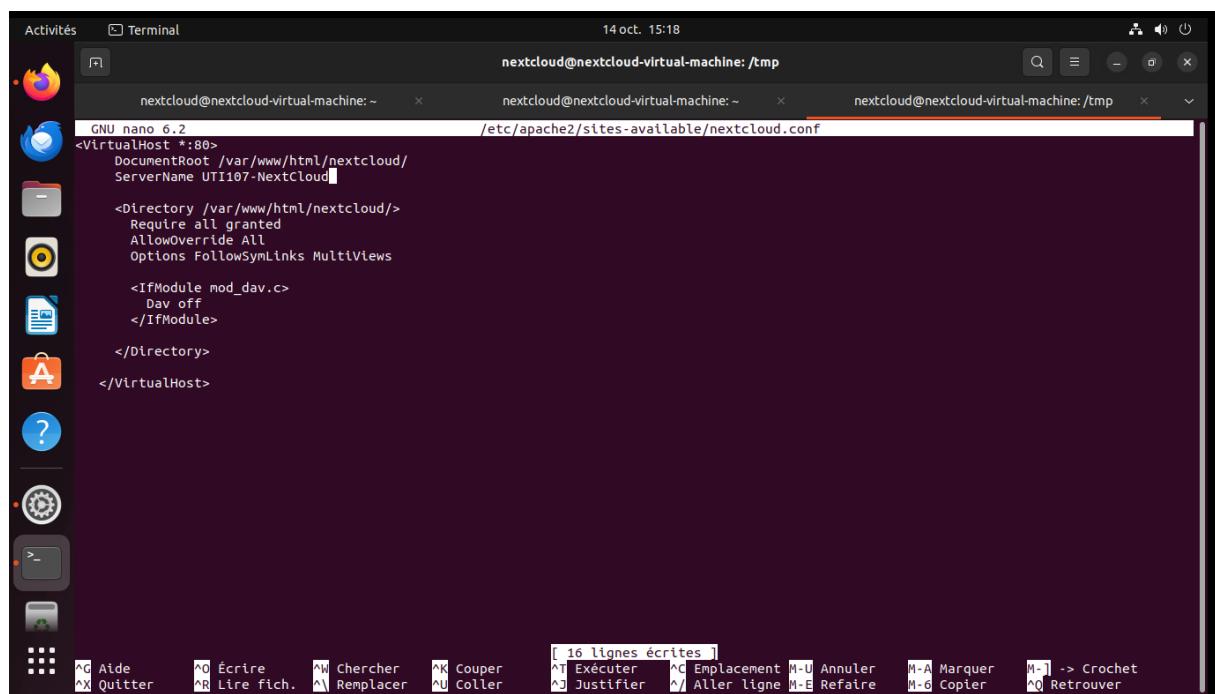
```
nextcloud@nextcloud-virtual-machine: ~          nextcloud@nextcloud-virtual-machine: ~          nextcloud@nextcloud-virtual-machine: /tmp
GNU nano 6.2                                     /etc/apache2/sites-available/nextcloud.conf *
<VirtualHost *:80>
    DocumentRoot /var/www/html/nextcloud/
    ServerName votre_domaine

    <Directory /var/www/html/nextcloud/>
        Require all granted
        AllowOverride All
        Options FollowSymLinks MultiViews

        <IfModule mod_dav.c>
            Dav off
        </IfModule>

    </Directory>
</VirtualHost>
```

```
nextcloud@nextcloud-virtual-machine:/tmp$ sudo nano /etc/apache2/sites-available/nextcloud.conf
nextcloud@nextcloud-virtual-machine:/tmp$ sudo nano /etc/apache2/sites-available/nextcloud.conf
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$ █
```



Activités Terminal 14 oct. 15:18 nextcloud@nextcloud-virtual-machine: /tmp

```
nextcloud@nextcloud-virtual-machine: ~ x nextcloud@nextcloud-virtual-machine: ~ x nextcloud@nextcloud-virtual-machine: /tmp x
GNU nano 6.2 /etc/apache2/sites-available/nextcloud.conf
<VirtualHost *:80>
    DocumentRoot /var/www/html/nextcloud/
    ServerName UTI107-NextCloud

    <directory /var/www/html/nextcloud/>
        Require all granted
        AllowOverride All
        Options FollowSymLinks MultiViews

        <IfModule mod_dav.c>
            Dav off
        </IfModule>

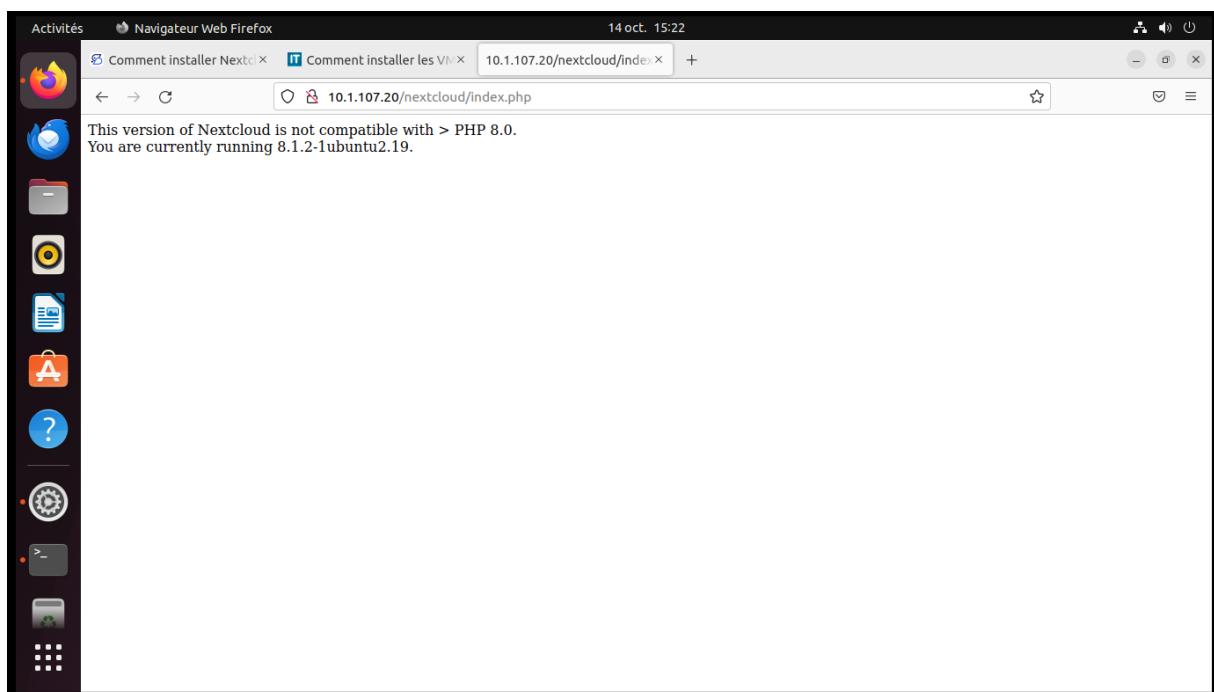
    </directory>
</VirtualHost>
```

[ 16 lignes écrites ]

Àide Écrire Chercher Couper Exécuter Emplacement Annuler Marquer → Crochet quitter Lire fich. Remplacer Coller Justifier Aller ligne Refaire Copier Retrouver

```
nextcloud@nextcloud-virtual-machine:~$ 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 starting.
oct. 14 15:16:54 nextcloud-virtual-machine systemd[1]: This usually indicates unclean termination of a previous run, or service implementation error.
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 domain name, using 10.1.107.20.
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

Mot de passe

#### Stockage & base de données ▾

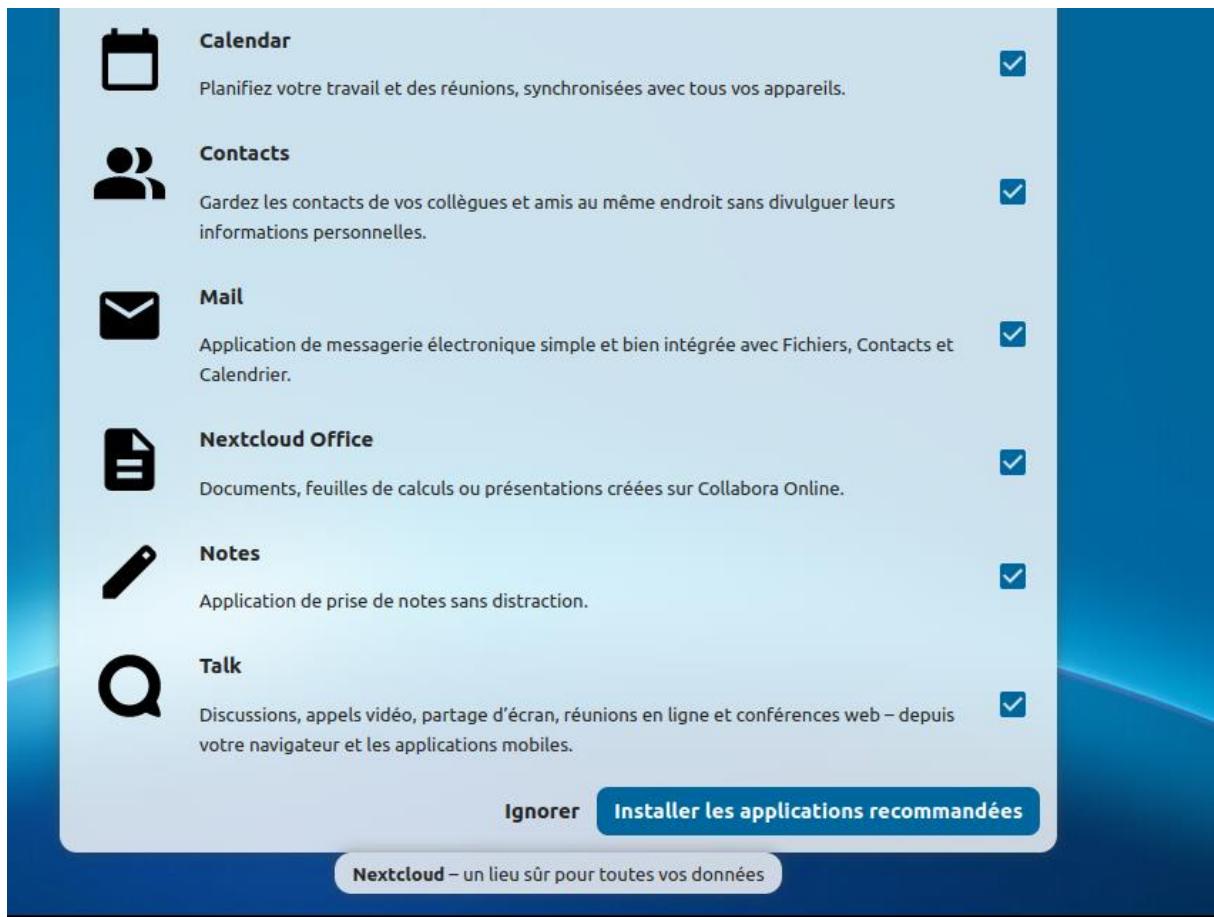
Répertoire des données

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



X

## 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 →](#)



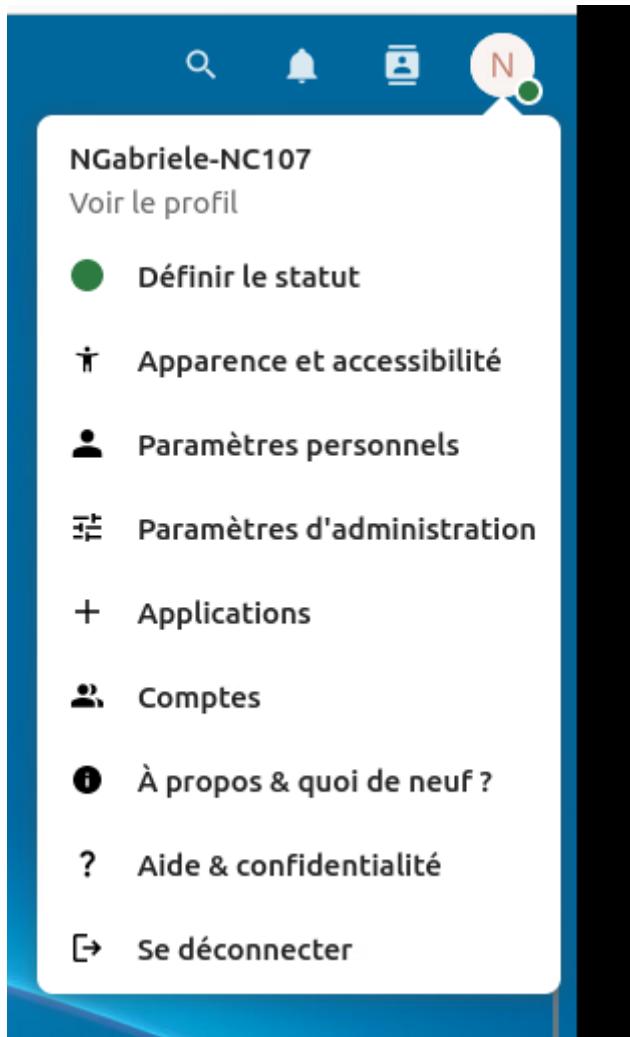
**Your browser is not supported. Please  
upgrade to a newer version or a  
supported one.**

[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



The screenshot shows the Nextcloud web interface. On the left, a sidebar menu includes: Découvrir, Vos applications, Applications actives, Applications désactivées, **Packs d'applications** (highlighted in blue), Applications en vedette, Personnalisation, Tableau de bord, Fichiers, Jeux, Intégration, Supervision, Multimédia, Bureautique & texte, and Organisation. The main content area is titled 'Packs d'applications'.

**Pack pour entreprise** [Tout télécharger et activer](#)

Application	Version	Status	Action
Auditing / Logging	1.20.0	<input checked="" type="checkbox"/> En vedette	<a href="#">Activer</a>
File access control	1.20.1	<input checked="" type="checkbox"/> En vedette	<a href="#">Télécharger et activer</a>
Files automated tagging	1.20.0	<input checked="" type="checkbox"/> En vedette	<a href="#">Télécharger et activer</a>
LDAP user and group backend	1.21.0	<input checked="" type="checkbox"/> En vedette	<a href="#">Activer</a>
Retention	1.19.0	<input checked="" type="checkbox"/> En vedette	<a href="#">Télécharger et activer</a>
SSO & SAML authentication	6.3.0	<input checked="" type="checkbox"/> En vedette	<a href="#">Télécharger et activer</a>
Terms of service	2.5.0		<a href="#">Télécharger et activer</a>

**Pack Nextcloud Hub** [Tout télécharger et activer](#)

Application	Version	Status	Action
Calendar	5.0.1	<input checked="" type="checkbox"/> En vedette	<a href="#">Télécharger et activer</a>



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

Serveur Utilisateurs Attributs de connexion Groupes A

1. Serveur :

ldap://10.0.107.1

ldap@DOMAD107.peda

.....

DC=DOMAD107,DC=peda

Saisir les filtres LDAP manuellement (recommandé pour les annuaires de grande ampleur)

Configuration OK ●  ● Aide

Utilisateurs du domaine  
Administrateurs

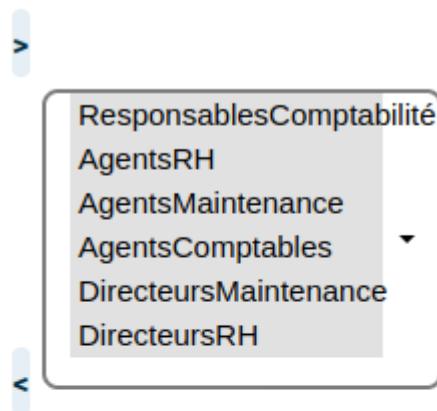
↓ Modifier la requête

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   
:



[↓ 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](#)

Paramètres - Comptes - N X					
10.1.107.20/nextcloud/index.php/settings/users					
Tous les comptes		Nom d'affichage	Nom du compte	Mot de passe	E-mail
	FH	<b>Fabricio HERNANDEZ</b>	12E78DAE-E402-4A21-A...		
	RD	<b>Raymond DUMONT</b>	159FDBB8-A1B8-4FA3-9...		
	GP	<b>Geoffrey PIERRE</b>	183EDF02-2A30-42A4-A...		
	VB	<b>Valentin BALDI</b>	219542DE-9713-4337-A...		
	AA	<b>admin ad</b>	22C38D82-21D3-43EA-9...		
	SA	<b>Sylviane AIT</b>	629D15A5-9751-4188-A...		
	SH	<b>Sabrina HARIT</b>	7B8EBBBB-BCF9-414D-...		
	FP	<b>François PICHON</b>	7C41D585-99A6-4486-8...		
	DD	<b>Dorlène DOINET</b>	A71E9FF5-250D-4BF9-A...		
	CO	<b>Clara OUDEMONT</b>	B525E059-B9FA-4A6D-A...		

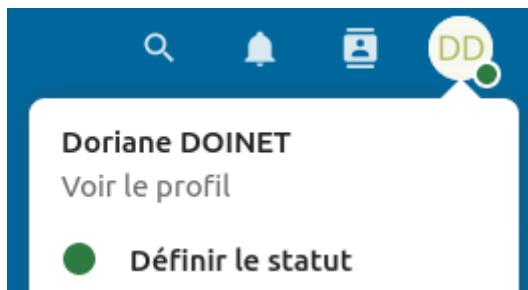
The screenshot shows the Nextcloud web interface. On the left, a sidebar lists account categories: 'Tous les comptes', 'Administrateurs', 'Récemment actifs', and 'Comptes désactivés'. Below this is a 'Groupes' section with 'AgentsComptables' selected and 'AgentsMaintenance' listed. The main area displays a table of users with columns: 'Nom d'affichage', 'Nom du compte', 'Mot de passe', and 'E-mail'. The users listed are Doriane DOINET, Sylvie DUMONT, and Pierre DUMAIT. A note indicates '3 accounts'.

Nom d'affichage	Nom du compte	Mot de passe	E-mail
DD Doriane DOINET	A71E9FF5-250D-4BF9-A...		
SD Sylvie DUMONT	C574C497-818F-4054-8...		
PD Pierre DUMAIT	CBAF67CB-988F-44DB...		

The screenshot shows the Nextcloud web interface with the 'Administrateurs' group selected in the sidebar. The main area displays a table of users with columns: 'Nom d'affichage', 'Nom du compte', 'Mot de passe', and 'E-mail'. The user listed is NGabriele-NC107.

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

The screenshot shows the Nextcloud login page. It features a large 'Se connecter à Nextcloud' button. Below it are two input fields: 'Nom d'utilisateur ou adresse e-mail' containing 'ddoinet' and 'Mot de passe' containing '\*\*\*\*\*'. A 'Se connecter' button with a right-pointing arrow is at the bottom. A link 'Mot de passe oublié ?' is at the bottom right.



Doriane DOINET

Voir le profil

● Définir le statut

### Créer un nouveau dossier

Nom du dossier

**Créer**

<input type="checkbox"/>	 ServiceCF	 ...
<input type="checkbox"/>	 ServiceMAINT	 ...
<input type="checkbox"/>	 ServiceRH	 ...

## ServiceCF

... X

0 B il y a 2 minutes



Activité



Partage

Recherche de destinataires de partages

AgentsComptables



AgentsComptables



Rechercher partout

## ServiceCF

...

X

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

Éditer

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 liblftdii-2
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les NOUVEAUX paquets suivants seront installés :
  ldap-utils
0 mis à jour, 1 nouvellement installé, 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=Groups,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	10.0.1071	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 <small>i</small>	Oui		
DN du compte (pour les connexions non anonymes)	ldap@DOMAD107.peda		
Mot de passe du compte (pour les connexions non anonymes)	*****	<input type="checkbox"/> Effacer	
Champ de l'identifiant	samaccountname	Commentaires	
Champ de synchronisation <small>i</small>	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