PROJET PERSONNEL ENCADRÉE

7 avril 2024

NESUX

05 / 04 / 2024

CRAMPON Nicolas

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2024**

Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :**
Nom, prénom : CRAMPON Nicolas	**N° candidat :**
Épreuve ponctuelle non **Contrôle en cours de formation** oui	**Date :** 05 / 04 / 2024
Organisation support de la réalisation professionnelle	
Intitulé de la réalisation professionnelle	
Période de réalisation : mars → 5 Avril 2024 **Lieu :** Senlis **Modalité :** oui **Seul(e)** non **En équipe**	
Compétences travaillées **oui** Concevoir une solution d'infrastructure réseau **oui** Installer, tester et déployer une solution d'infrastructure réseau **non** Exploiter, dépanner et superviser une solution d'infrastructure réseau	
Conditions de réalisation[1] (ressources fournies, résultats attendus) - 1 Windows Server 2022 → Active Directory - 2 Windows 10 → Clients - 1 Linux Server → GLPI - PfSense → CrowdSec et Squid - 1 Kali Linux - 1 téléphone : client VPN	
Description des ressources documentaires, matérielles et logicielles utilisées[2] **Ressources Documentaires :** Divers sites Internet comme IT-CONNECT **Ressources Matérielles :** Ordinateur portable avec 32 Go de ram, Core I7, RTX 4070 **Ressources Logiciels :** Tout mon environnement est virtualisé sur VMware Workstation 17 Pro	
Modalités d'accès aux productions[3] et à leur documentation[4] Page 8 pour tous les mots de passes de mon environnement	

Introduction

NESUX considère la sécurisation de son infrastructure réseau comme une priorité essentielle pour assurer le bon fonctionnement de ses activités. Dans cet objectif, des mesures stratégiques sont prévues pour garantir une connectivité stable et sécurisée, répondant ainsi aux besoins fondamentaux de l'entreprise.

1) CANEVAS

1.1 - Mise en situation

Dans le monde numérique en constante évolution, NESUX, une entreprise de développement logiciel en pleine croissance, se trouve à un tournant crucial dans son parcours. Consciente de l'importance capitale d'une infrastructure réseau fiable et sécurisée pour soutenir ses opérations, NESUX se lance dans un projet ambitieux visant à renforcer sa structure informatique.

Au cœur de cette initiative se trouve la création de deux zones distinctes : **la zone réseau local** et **la zone DMZ**. Dans la première, NESUX prévoit l'installation d'un **Active Directory central** pour gérer efficacement les identités et les accès des utilisateurs, ainsi que **deux clients Windows 10** pour faciliter l'accès aux ressources partagées. La zone DMZ va permettre de séparer les services critiques du réseau interne et de renforcer la sécurité contre les menaces externes. Un **serveur GLPI** sera déployé.

Pour protéger cette infrastructure contre les menaces en ligne croissantes, NESUX compte sur des solutions de sécurité avancées. **Un pare-feu pfSense** sera mis en place pour contrôler et surveiller le trafic réseau, tandis que **CrowdSec** sera utilisé pour détecter et bloquer les attaques par bruteforce provenant d'un **Kali Linux**, une machine dédiée aux tests de sécurité. De plus, l'intégration de **Squid** permettra de filtrer et de bloquer sélectivement l'accès à certains sites Web et communications c to c, renforçant ainsi la sécurité et la productivité des employés.

Afin de permettre un accès sécurisé aux ressources internes, même à distance, NESUX configurera **un client VPN**, permettant ainsi aux employés externes de se connecter en toute sécurité au réseau local de l'entreprise.

Ce projet représente un engagement fort de NESUX envers la sécurité et la fiabilité de son infrastructure réseau, assurant ainsi une connectivité stable et sécurisée pour ses employés, quel que soit leur emplacement. *(Le réseau sera réalisé avec VMWARE)*

1.2 - Cahier des charges

- ★ Ce que l'entreprise souhaite mettre en place réellement :
  - Zone locale : 1 Active Directory et 2 clients windows 10
  - Zone DMZ : Serveur GLPI
  - Un pare-feu pfSense : CrowdSec et Squid
  - Un kali linux afin de tester les attaques
  - Un client Vpn pour se connecter à la zone locale

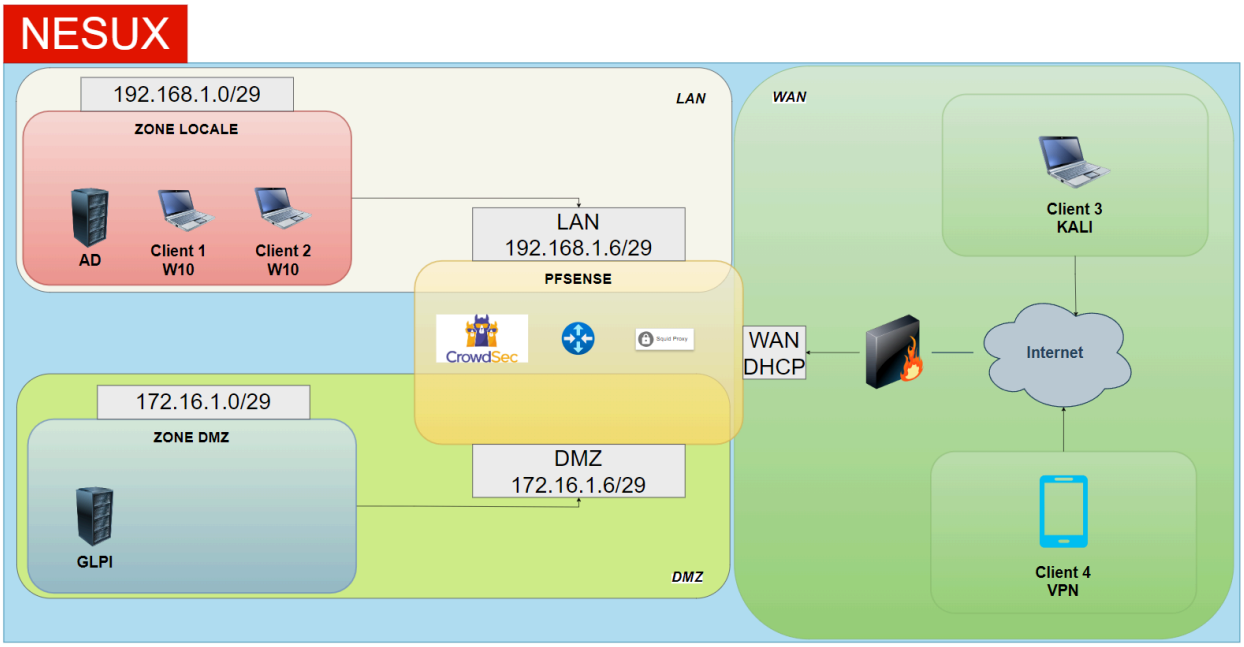
1.3 - Solution

- ★ Zone locale, Installation et configuration
- ★ PFSENSE, Installation et configuration
- ★ PFSENSE, Création de l'interface DMZ
- ★ PFSENSE, Création des règles
- ★ Installation et configuration de la machine Kali
- ★ Installation de Hydra
- ★ Installation du dictionnaire
- ★ Cracker le mot de passe SSH
- ★ Crowdsec Installation et blocage
- ★ Enregistrement DNS
- ★ Création du certificat HTTPS
- ★ Installation de Squid
- ★ Blocage des C&C
- ★ Installation et configuration d'OpenVpn sur PFSENSE
- ★ Test OpenVPN
- ★ LDAP pour les utilisateurs de la zone locale (en cours)
- ★ Synthèse des règles (en cours)

1.4 - Équipements et Logiciels nécéssaires

- ★ 1 Windows Server 2022 → Active Directory
- ★ 2 Windows 10 → Clients
- ★ 1 Linux Server → GLPI
- ★ PfSense → CrowdSec et Squid
- ★ 1 Kali Linux
- ★ 1 téléphone : client VPN

1.5 - Schéma réseau



- **LAN** : 192.168.1.0/24
    - Zone locale : 192.168.1.0/29
- **DMZ** : 172.16.1.0/24
    - Zone DMZ : 172.16.1.0/29
- **WAN** : DHCP

1.6 - Tableau d’adressage

LAN

	IP	MASQUE	BROADCAST	DNS	DNS2
AD	192.168.1.1	/29	192.168.1.6	X	X
CLIENT 1	192.168.1.2	/29	192.168.1.6	192.168.1.1	X
CLIENT 2	192.168.1.3	/29	192.168.1.6	192.168.1.1	X

DMZ

GLPI	172.16.1.1	/29	172.16.2.6	192.168.2.1	X

WAN

CLIENT 3	DHCP	DHCP	DHCP	DHCP	DHCP
CLIENT 4	DHCP	DHCP	DHCP	DHCP	DHCP

PFSENSE

LAN	192.168.1.6	/29	X	192.168.2.1	X
DMZ	172.16.1.6	/29	X	X	X
WAN	DHCP	DHCP	DHCP	DHCP	DHCP

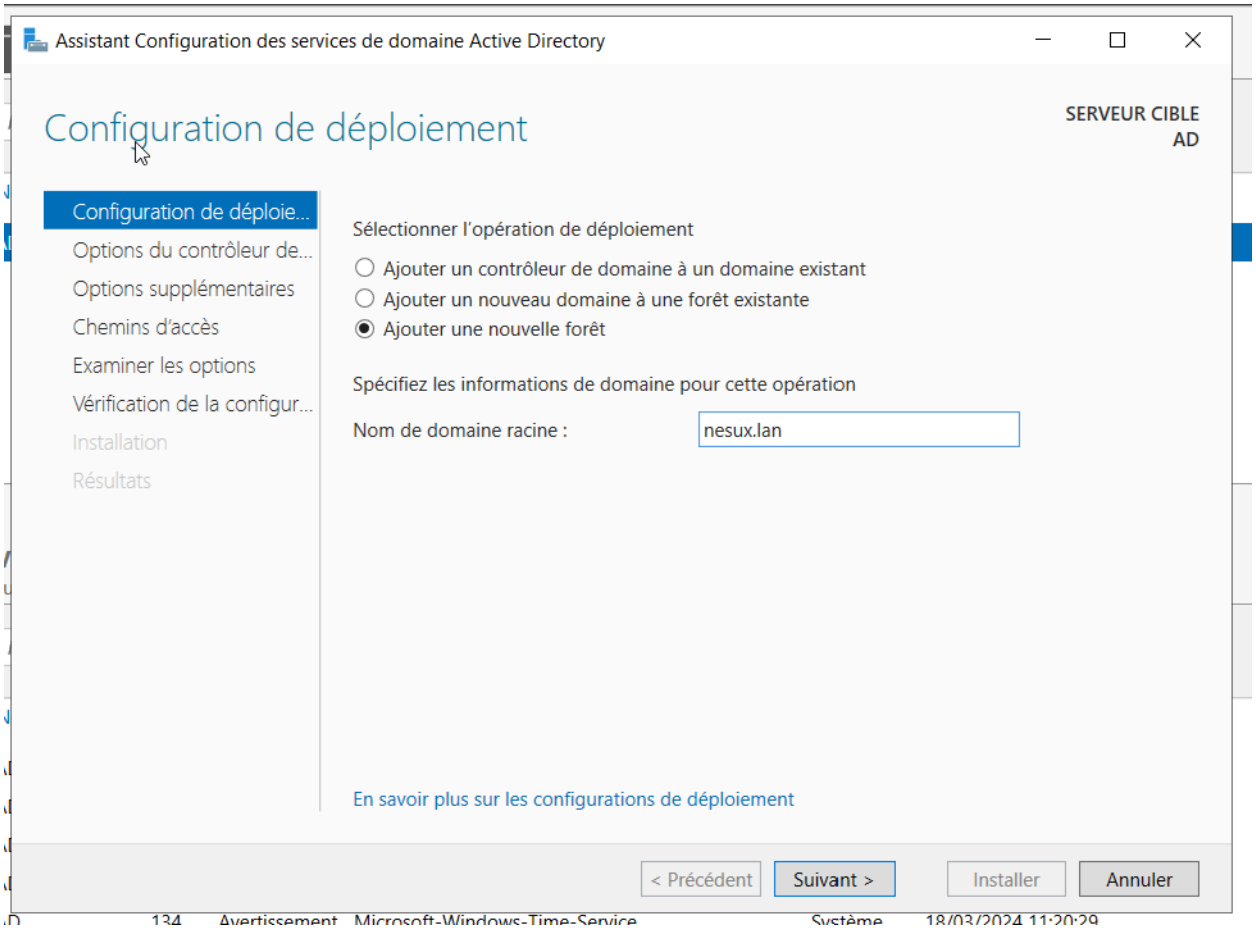
1.7 - Tableau Mots de passe

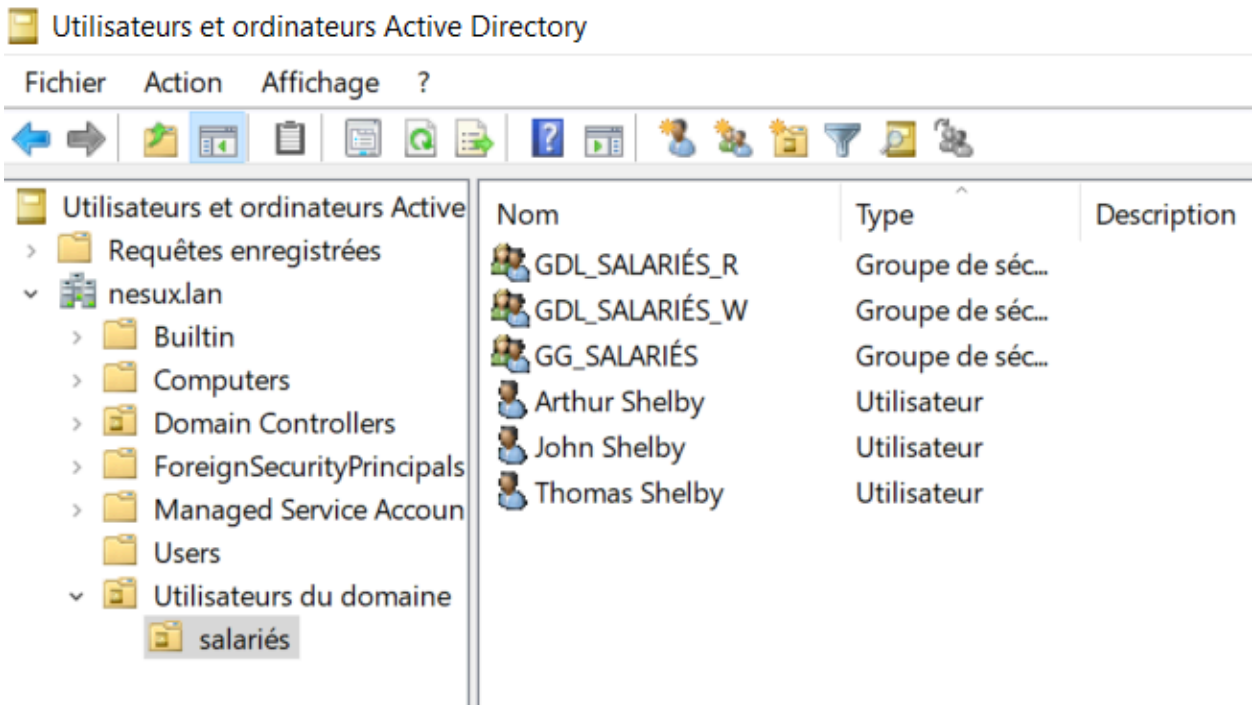
	Utilisateur	Mots de passe
AD	Administrateur	Admin00
GLPI	debian	root
PFSENSE	admin	Admin00
Client 1 (Thomas Shelby)	t.shelby	Admin00
Client 2 (Arthur Shelby)	a.shelby	Admin00
Client 3 (John Shelby)	j.shelby	Admin00
Client 4 (VPN)	vpn.pfsense.nesux	Admin00

2) SOLUTION

2.1 - Zone locale, Installation et configuration

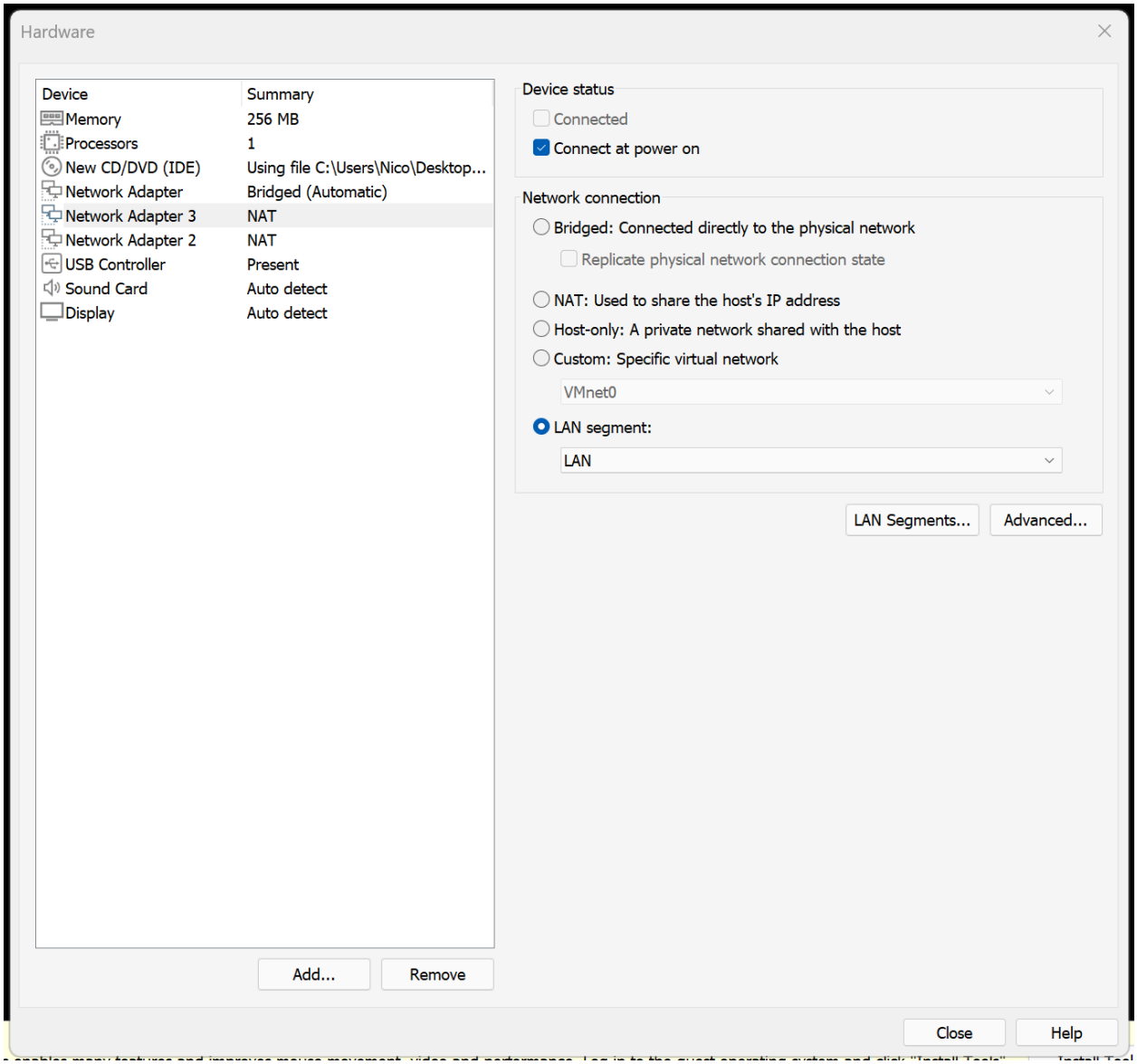
Je commence par installer et configurer Windows Server, et créer mon domaine. En suivant la méthode AGDLP, j'ajoute des groupes, et je crée les utilisateurs nécessaires. Une fois cette étape terminée, j'intègre ces utilisateurs dans le domaine nouvellement créé. Client1 et Client2 avec leur adresse IP respective.




Utilisateurs et ordinateurs Active Directory
Fichier
Action
Affichage
?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
nesux.lan
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accoun
Users
Utilisateurs du domaine
salariés
Nom
Type
Description
GDL_SALARIÉS_R
Groupe de séc...
GDL_SALARIÉS_W
Groupe de séc...
GG_SALARIÉS
Groupe de séc...
Arthur Shelby
Utilisateur
John Shelby
Utilisateur
Thomas Shelby
Utilisateur

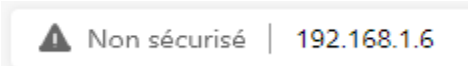
2.2 - PFSENSE, Installation et configuration

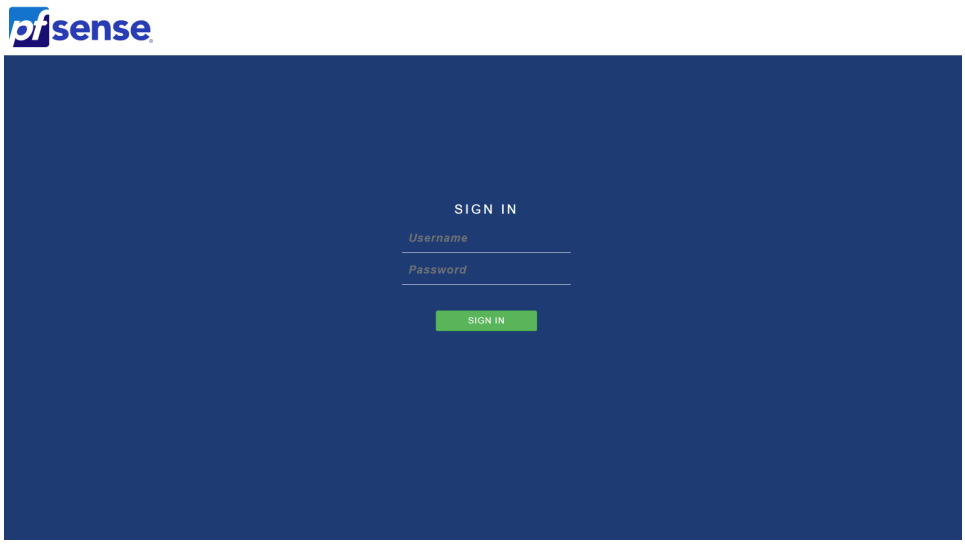
J’ajoute une carte réseau avec un segment LAN destiné à mon réseau local.



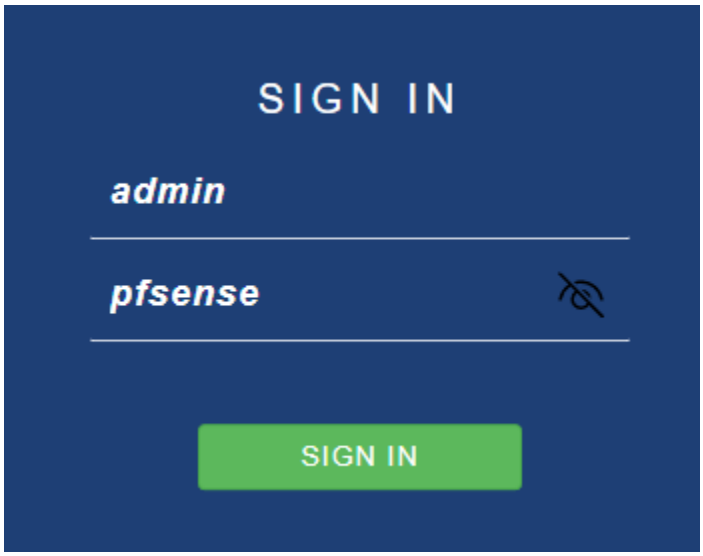
Je fais la même chose pour tous les appareils de mon réseau LAN.

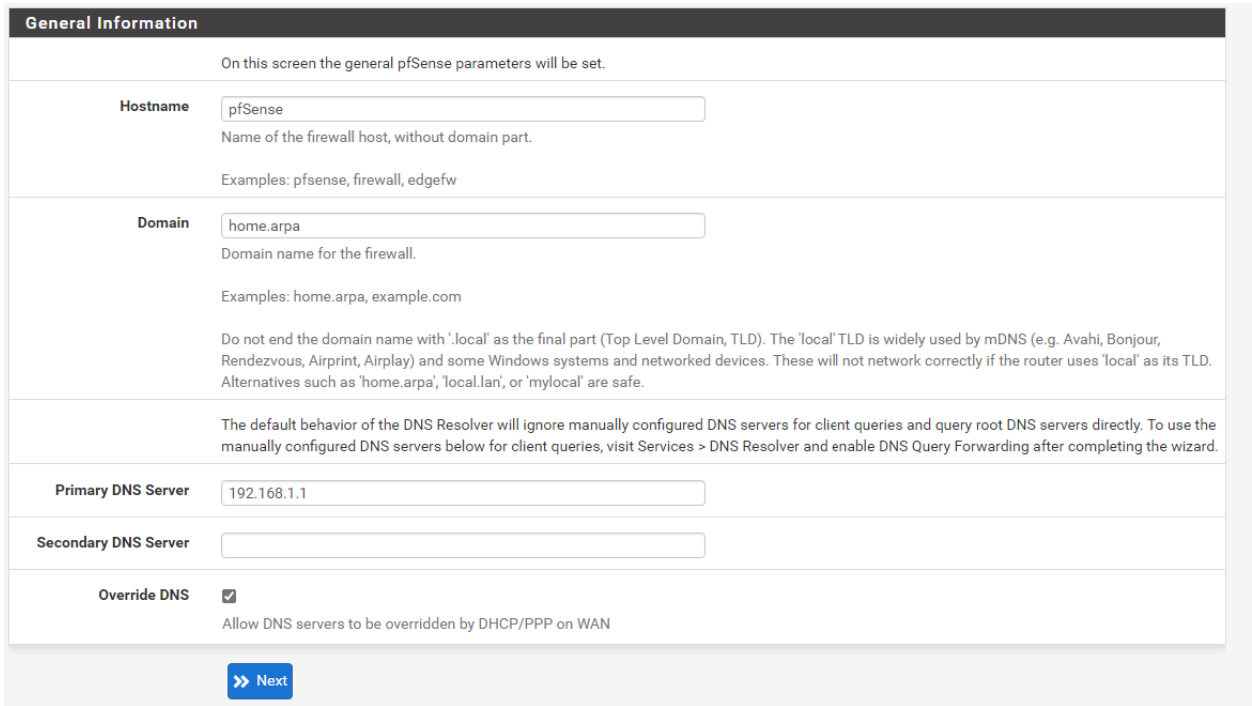
```
The IPv4 LAN address has been set to 192.168.1.6/29
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.1.6/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 19253ebec0d106ea42ec

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

 WAN (wan)       -> em0        -> v4/DHCP4: 10.101.32.99/16
 LAN (lan)       -> em1        -> v4: 192.168.1.6/29

 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:
```



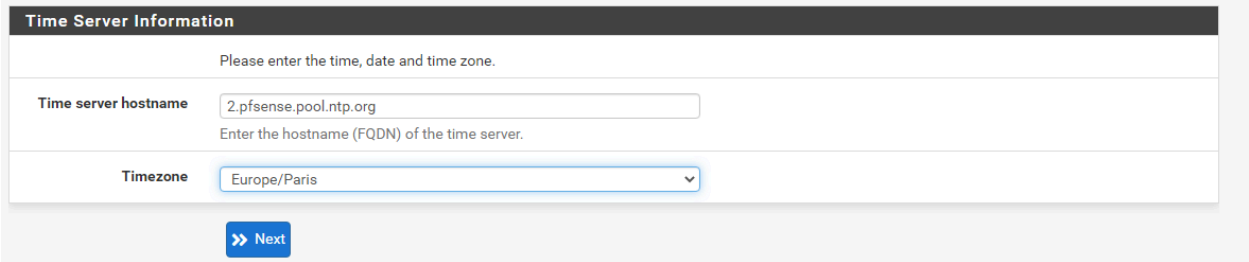


Je me connecte avec admin:pfsense

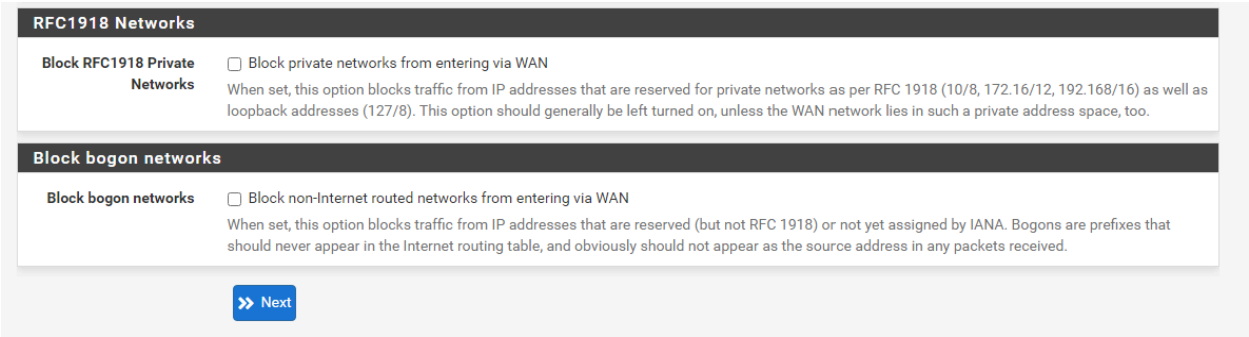




Je modifie le DNS.

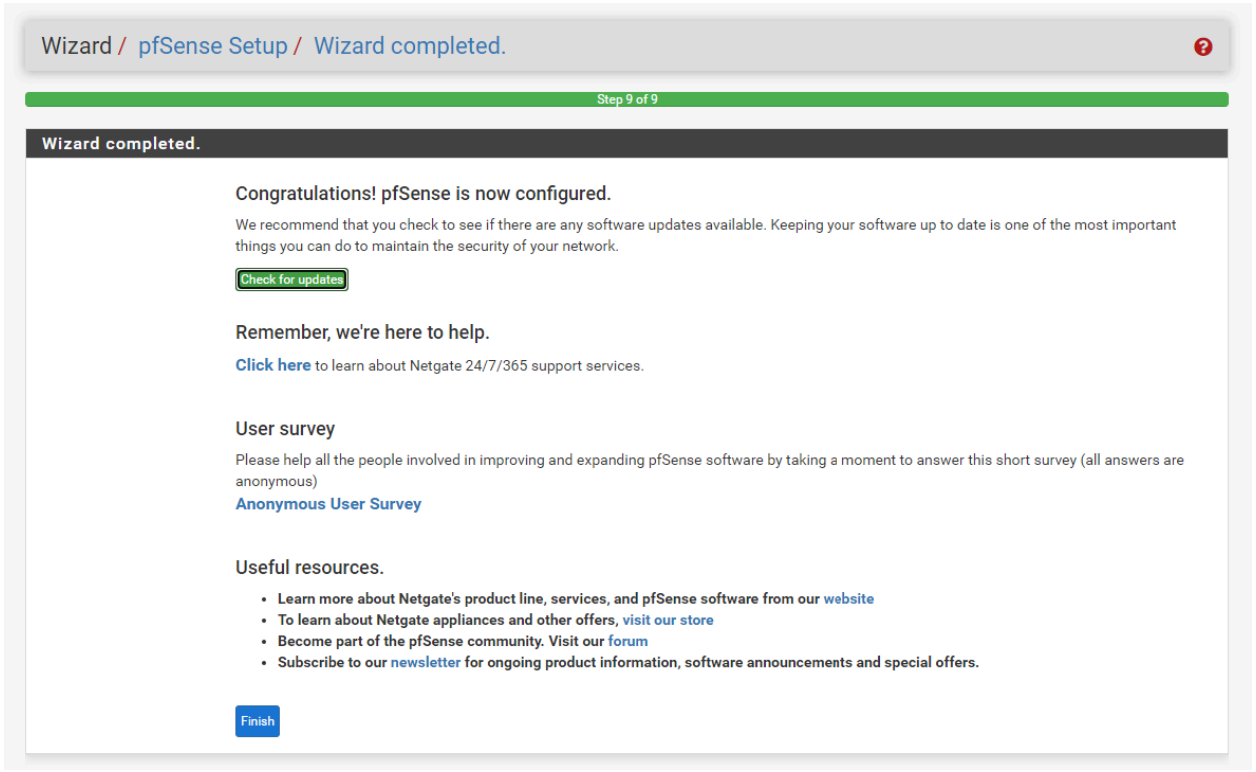


Je sélectionne Europe/Paris.

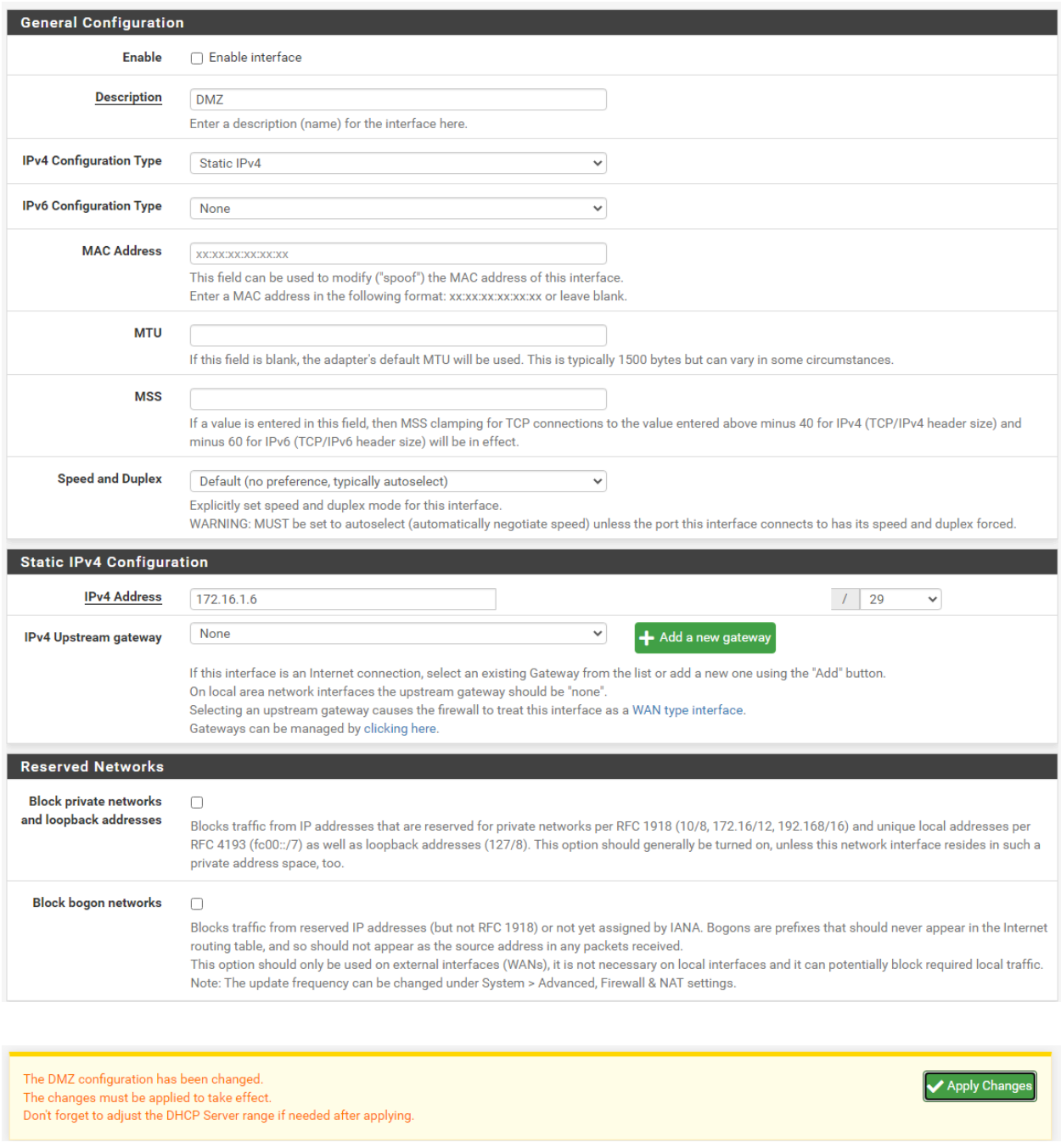


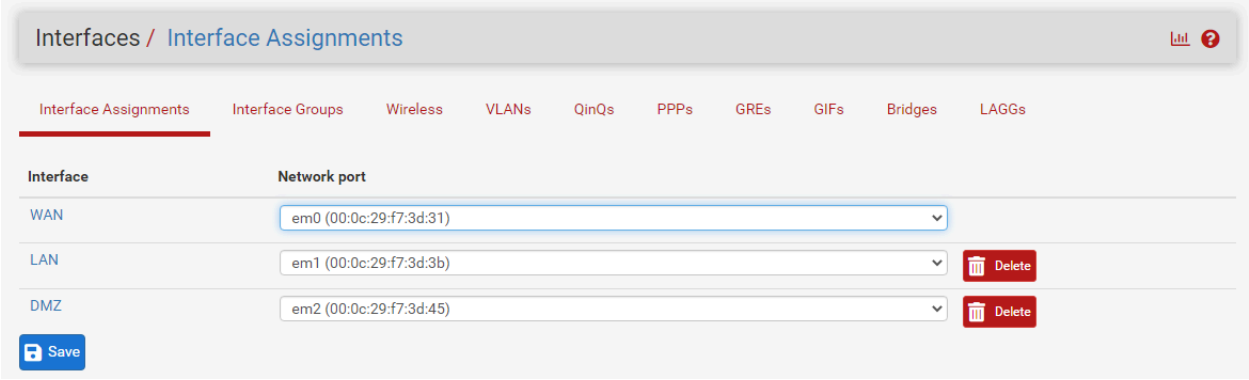
Je décoche ces deux cases pour ne pas bloquer le trafic entre le WAN et pfSense.

Je modifie le mot de passe avec Admin00.


Wizard / pfSense Setup / Wizard completed.
Step 9 of 9
Wizard completed.
Congratulations! pfSense is now configured.
We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.
Check for updates
Remember, we're here to help.
Click here to learn about Netgate 24/7/365 support services.
User survey
Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)
Anonymous User Survey
Useful resources.
Learn more about Netgate's product line, services, and pfSense software from our website
To learn about Netgate appliances and other offers, visit our store
Become part of the pfSense community. Visit our forum
Subscribe to our newsletter for ongoing product information, software announcements and special offers.
Finish

2.3 - PFSENSE, Création de l'interface DMZ

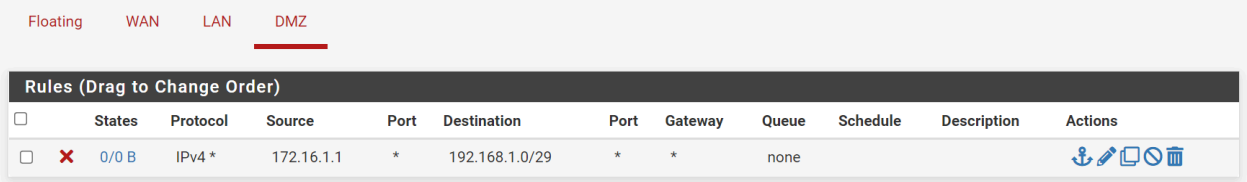



Interfaces / Interface Assignments
Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs
Interface
Network port
WAN
em0 (00:0c:29:f7:3d:31)
LAN
em1 (00:0c:29:f7:3d:3b)
Delete
DMZ
em2 (00:0c:29:f7:3d:45)
Delete
Save

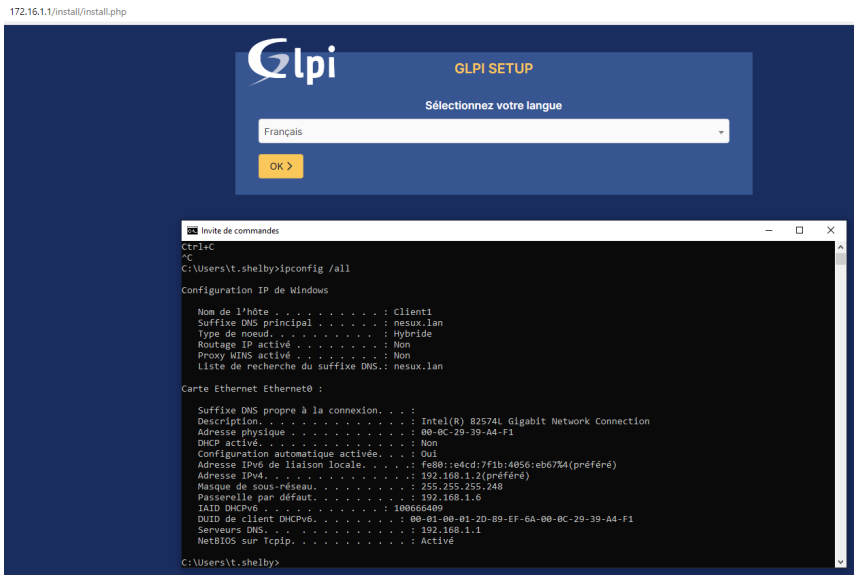
2.4 - PFSENSE, Création des règles

Le but principal d'avoir une zone DMZ est de séparer le réseau local des serveurs comme glpi afin d'ajouter une couche de sécurité à mon réseau. Les utilisateurs du réseau local pourront se connecter aux différents services mis en place mais à l'inverse les appareils de la zone DMZ ne pourront pas communiquer avec les postes de mon réseau local.

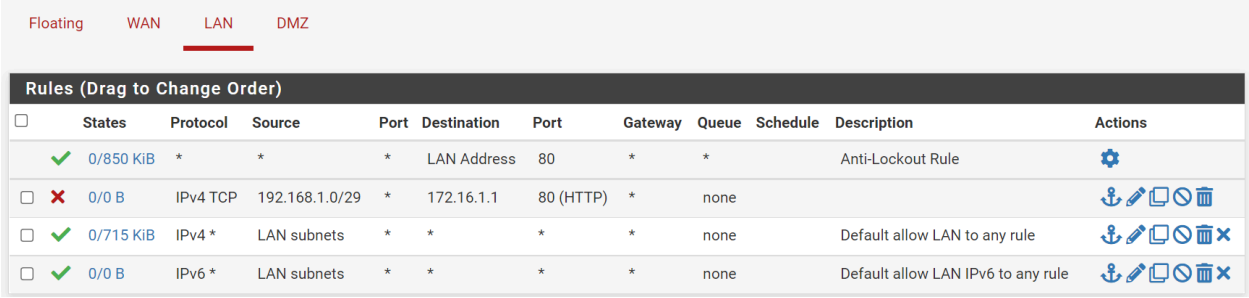
Donc pour le moment j'ai créé qu'une seule règle qui va permettre que ma machine glpi puisse ping mon réseau local.

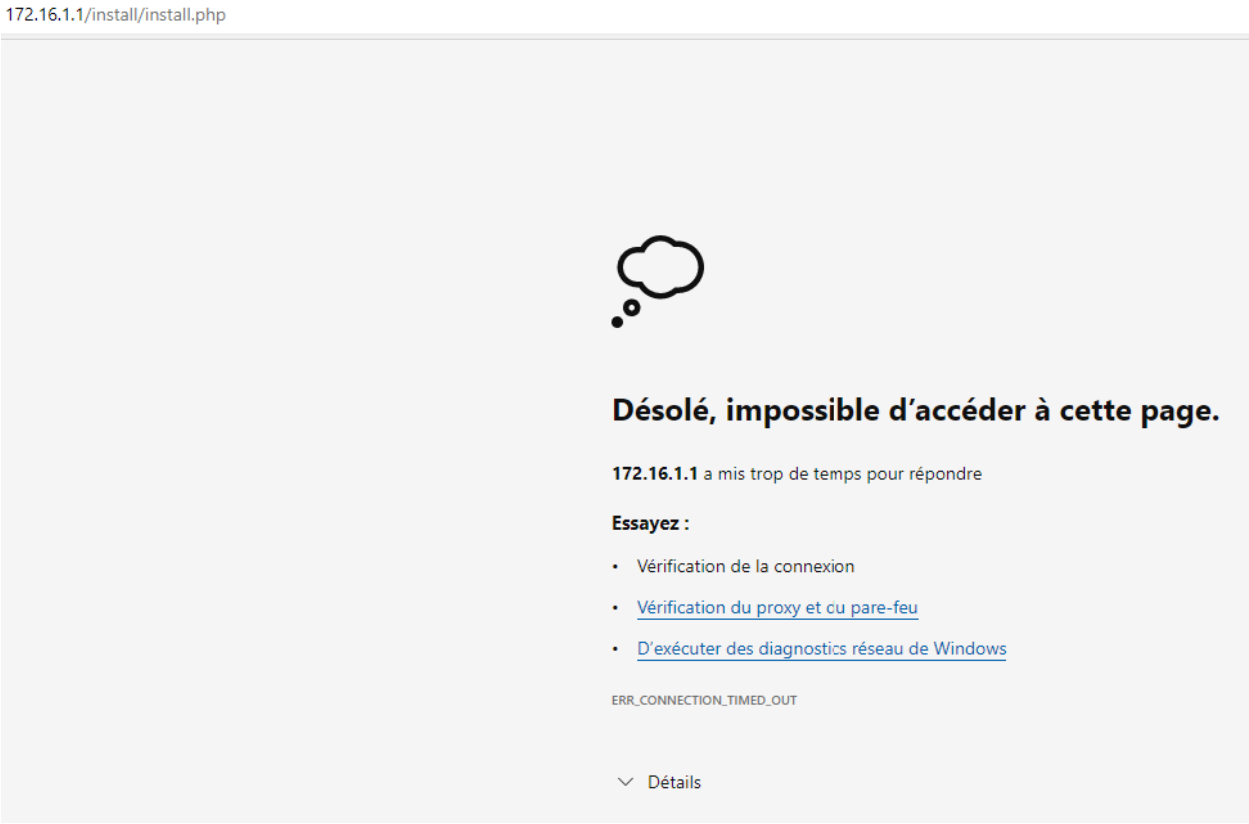


Je n'ai pas besoin de créer de règle pour autoriser l'accès à glpi depuis un client du réseau local car après test ça fonctionne de base.



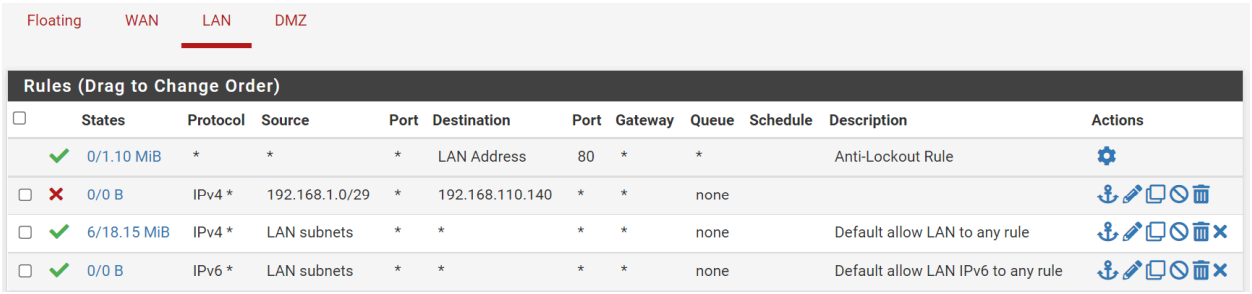
Mais si je mets en place cette règle je n'y ai plus accès.





Je l'enlève car ce n'est pas le but recherché.

Si jamais je veut bloquer mon réseau lan au wan je créer cette règle :



Mais ce n'est pas le but recherché non plus.

Maintenant il faut que mon réseau local ait accès à mon réseau wan donc je supprime cette règle. A noter que dans la configuration ip de ma machine client sur mon réseau local il faut mettre l'ip qui permet de se connecter à internet en dns, dans mon cas quand je suis a Promeo, je vais mettre 192.168.110.140. Sur ma machine physique où est installé vmware j'ouvre mon terminal et je tape ipconfig /all et j'observe bien que l'ip est dans le même réseau.

```
Carte Ethernet VMware Network Adapter VMnet8 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet8
   Adresse physique . . . . . . . . . . . : 00-50-56-C0-00-08
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::fd3d:117e:974d:25a8%16(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.110.1(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
   IAID DHCPv6 . . . . . . . . . . . : 704663638
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2D-50-E9-F2-74-5D-22-CF-33-1F
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

L'ip est aussi l'em0 sur mon pare-feu pour le réseau WAN.

Je veille à bien désactiver les pare-feux windows pour pouvoir autoriser la communication entre le wan et mon réseau local. Si jamais je veux que ma machine physique se connecte à mon lan je vais devoir créer 2 règles et désactiver la carte wifi par défaut pour laisser vmnet8 en priorité.

Rules (Drag to Change Order)

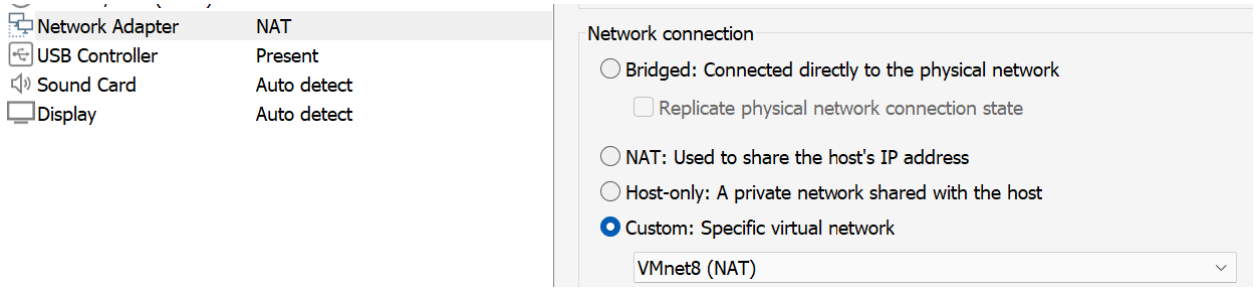
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 *	192.168.110.0/24	*	192.168.1.0/29	*	*	none		
☐	✓	0/240 B	IPv4 *	192.168.110.0/24	*	192.168.110.0/24	*	*	none		

Rules (Drag to Change Order)

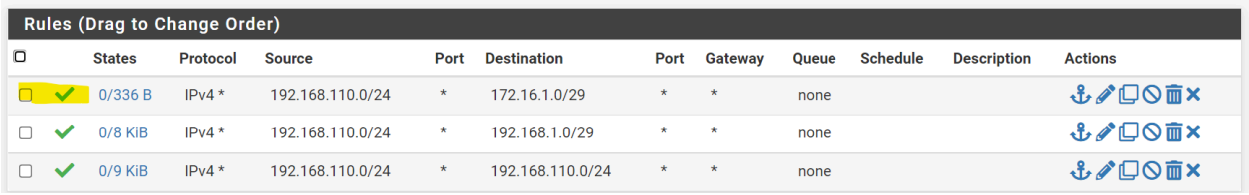
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	2/1.44 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
☐	✓	1/37 KiB	IPv4 *	192.168.1.0/29	*	192.168.110.0/24	*	*	none		
☐	✓	0/190.03 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule
☐	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule

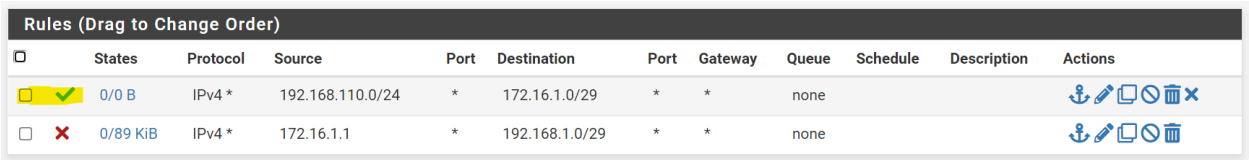
2.5 - Installation et configuration de la machine Kali

Je sélectionne bien la bonne carte réseau lors de son installation.



Ensuite j'ai ajouté 2 règles pour donner l'accès à la zone DMZ depuis le wan.





Et je modifie la configuration ip pour qu'elle soit sur le même réseau que mon wan.

2.6 - Installation de Hydra

Et j'ai installé hydra avec cette commande

```
┌──(admin㉿kali)-[/home/kali]
└─$ sudo apt-get install hydra
```

2.7 - Installation du dictionnaire

https://github.com/LandGrey/pydictor/tree/master

J'accède à ce site pour téléchargerl la wordlist pydictor.

Sur kali je vais utiliser cette commande pour créer un répertoire nommé pydictor et y télécharger le contenu.

git clone https://github.com/LandGrey/pydictor.git

Ensuite je peux accéder au répertoire avec la commande cd

et je cherche le .txt qui m'intéresse

```
┌──(root㉿kali)-[/home/kali/pydictor/wordlist/Web]
└─# ls
CommonWebAdminPass.txt
```

Le chemin est /home/kali/pydictor/wordlist/Web/CommonWebAdminPass.txt

2.8 - Cracker le mot de passe SSH

J'utilise la commande : hydra -t 50 -l debian -P /home/kali/pydictor/wordlist/Web/CommonWebAdminPass.txt -s 22 -f 172.16.1.1 ssh -I

hydra : parce que j'utilise Hydra

-t 50 : 50 mdp seront testé simultanément

-l root : j'hack le mot de passe avec l'utilisateur root

-P /home/kali/pydictor/wordlist/Web/CommonWebAdminPass.txt : le chemin du dictionnaire

-s 22 : pour spécifier le port 22 ssh

-f : pour stopper le processus lorsque le mot de passe sera trouvé

172.16.1.1 : l'adresse ip de mon serveur ssh

ssh : le protocole utilisé

-I : pour hydra lorsque le mot de passe sera trouvé

Et j'attends une bonne trentaine de minutes.

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -t 50 -l debian -P /home/kali/pydictor/wordlist/Web/CommonWebAdminPass.txt -s 22 -f 172.16.1.1 ssh -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-21 13:12:44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 50 tasks per 1 server, overall 50 tasks, 1021 login tries (l:1/p:1021), ~21 tries per task
[DATA] attacking ssh://172.16.1.1:22/
[STATUS] 324.00 tries/min, 324 tries in 00:01h, 712 to do in 00:03h, 35 active
[STATUS] 287.50 tries/min, 575 tries in 00:02h, 463 to do in 00:02h, 33 active
[STATUS] 243.33 tries/min, 730 tries in 00:03h, 310 to do in 00:02h, 31 active
[STATUS] 228.75 tries/min, 915 tries in 00:04h, 129 to do in 00:01h, 27 active
[22][ssh] host: 172.16.1.1   login: debian   password: root
[STATUS] attack finished for 172.16.1.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-21 13:17:26
```

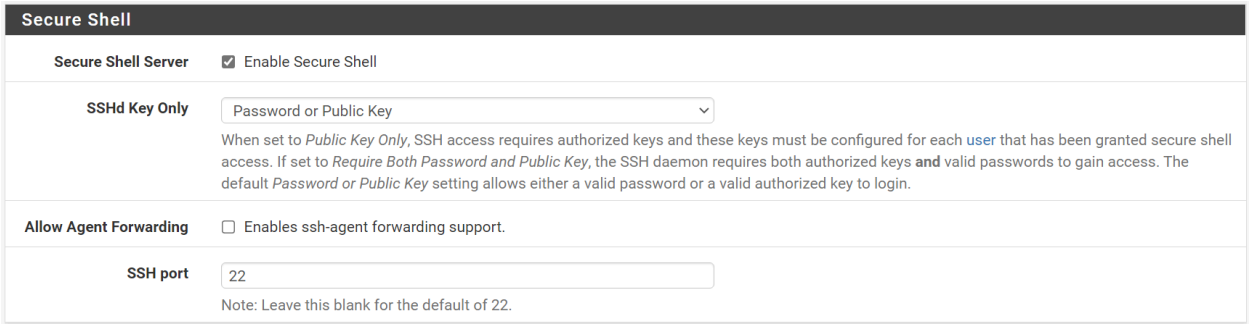
Et voilà le mot de passe à été trouvé.

2.9 - Crowdsec Installation et blocage

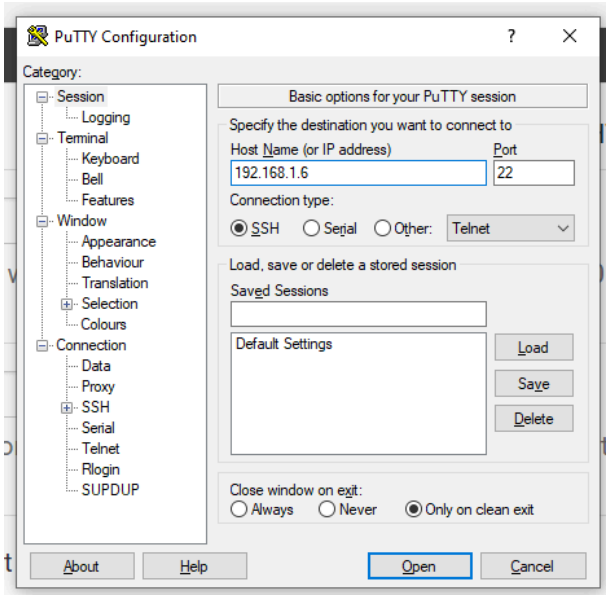
Maintenant je vais installer Crowdsec pour pouvoir détecter l'attaque et la bloquer.

Je commence par me connecter en ssh à mon pare-feu pfsense.

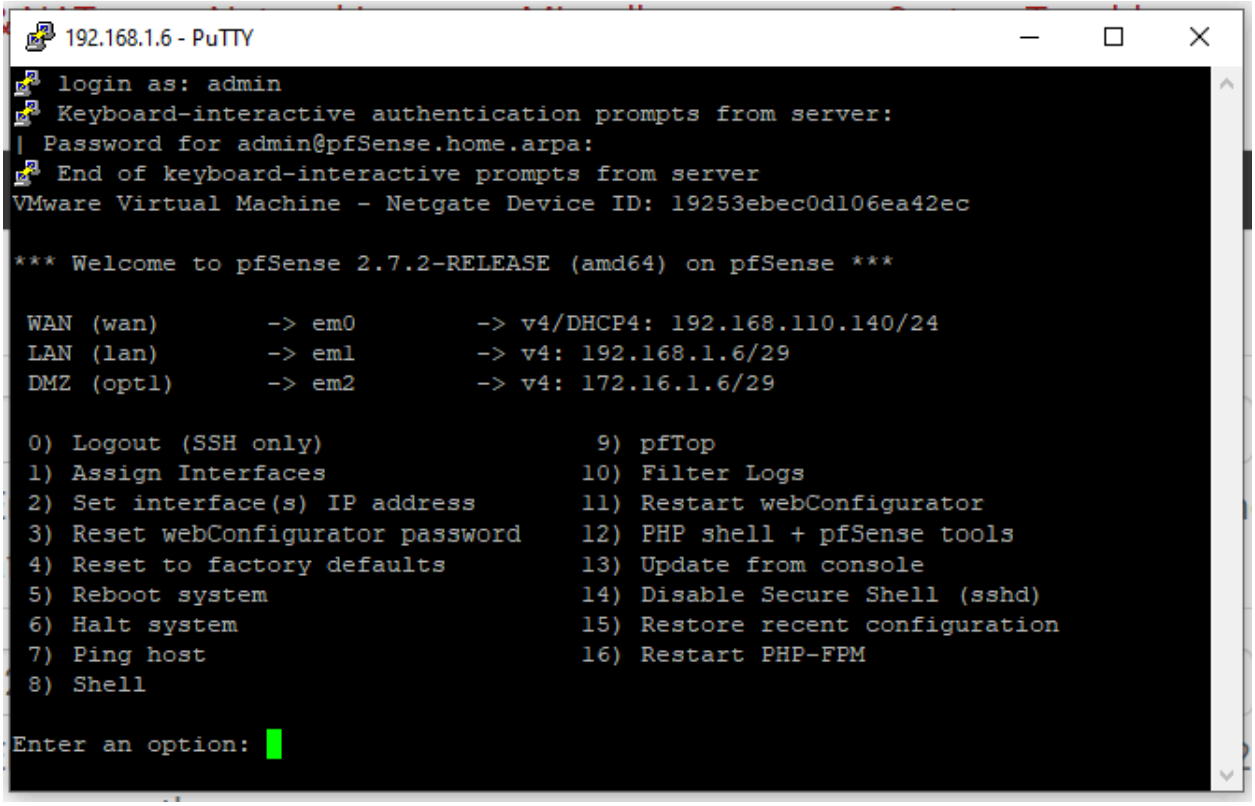
Pour ça j'active le ssh de pfsense.



et j'utilise putty pour y accéder.



Et je me connecte avec admin:Admin00



Et je saisis 8 pour ouvrir le Shell.

Et je tape les commande de l'installation :

setenv IGNORE_OSVERSION yes

pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/abseil-20230125.3.pkg

pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/re2-20231101.pkg

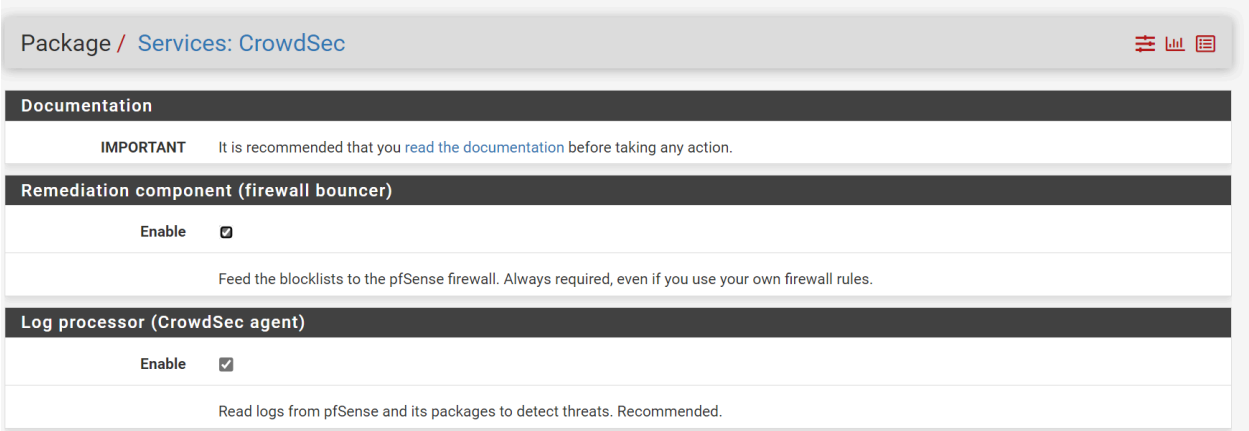
pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/crowdsec-1.6.0.pkg

pkg add -f
https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/crowdsec-firewall-bouncer-0.0.28_3.pkg

pkg add -f https://github.com/crowdsecurity/pfSense-pkg-crowdsec/releases/download/v0.1.3/pfSense-pkg-crowdsec-0.1.3.pkg

Et puis je redémarre pfsense afin que Crowdsec démarre.

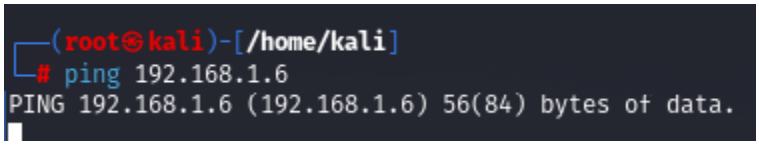
Maintenant je vais sur l'interface web et je vérifie que crowdsec est activé.



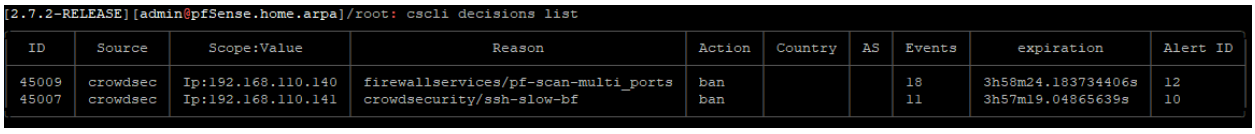
Si je lance une attaque bruteforce depuis ma machine kali

9	Ip:192.168.110.141	crowdsecurity/ssh-bf	ban:1	a few seconds ago
10	Ip:192.168.110.141	crowdsecurity/ssh-slow-bf	ban:1	a few seconds ago
11	Ip:192.168.110.140	firewallservices/pf-scan-multi_ports	ban:1	a few seconds ago

Je vois bien que l'attaque à été bloquée parce que maintenant, si j'essaie de ping mon pare-feu ça ne fonctionne plus.



Et dans le SLI du pare-feu on peut voir que l'ip de ma machine kali à été ban mais aussi celle de mon wan.



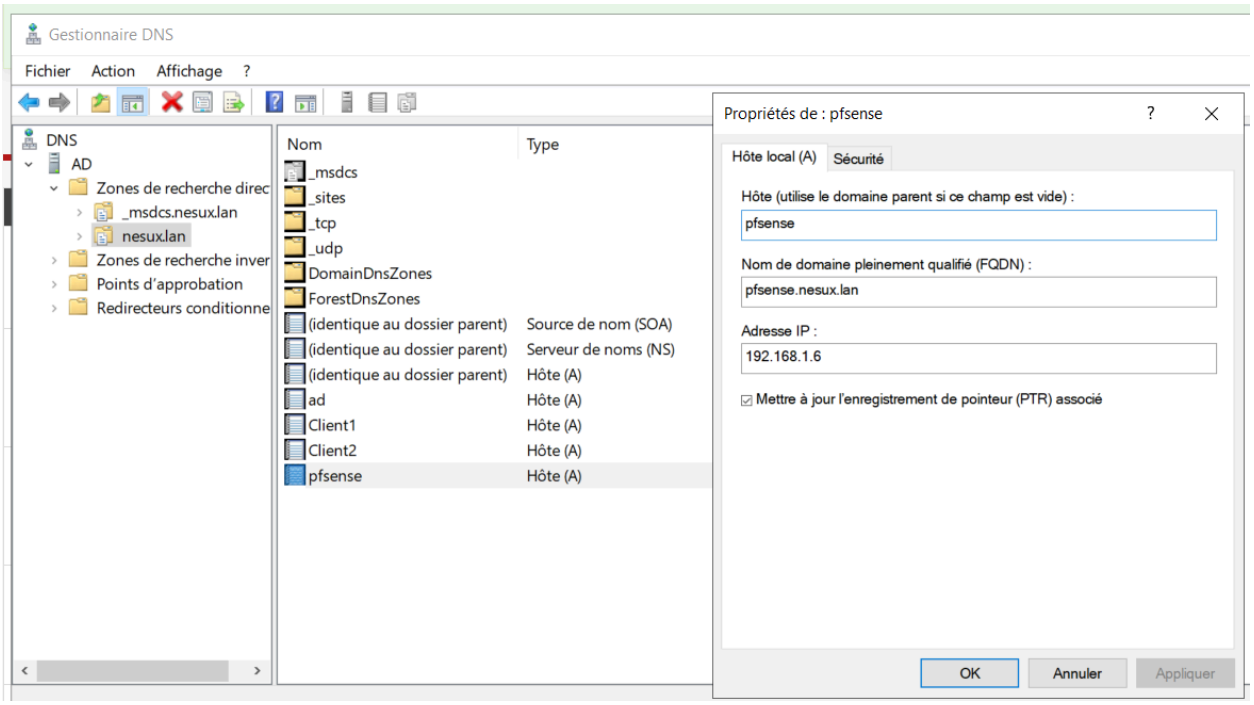
Pour les débloquer je peux faire : cscli decisions delete –ip x.x.x.x

```
2.7.2-RELEASE][admin@pfSense.home.arpa]/root: cscli decisions delete --ip 192.168.110.141
INFO[2024-03-22T09:47:11+01:00] 2 decision(s) deleted
2.7.2-RELEASE][admin@pfSense.home.arpa]/root: cscli decisions list
```

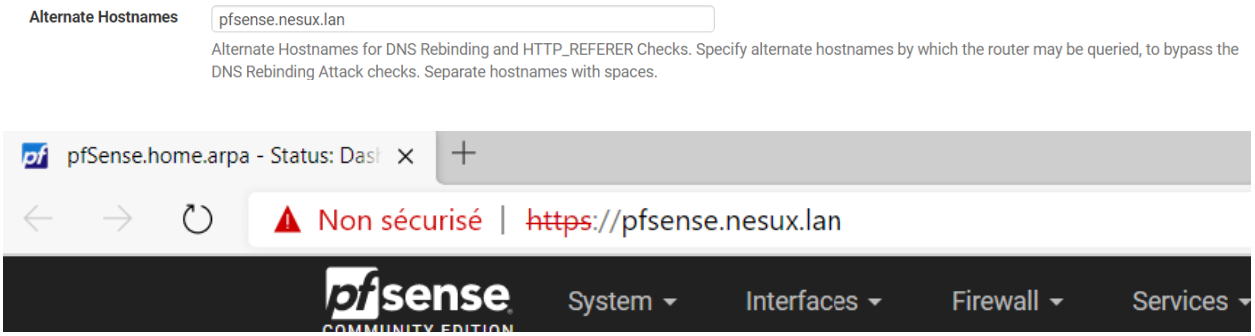
ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
45009	crowdsec	Ip:192.168.110.140	firewallservices/pf-scan-multi_ports	ban			18	3h56m4.168231551s	12

```
 duplicated entries skipped
2.7.2-RELEASE][admin@pfSense.home.arpa]/root: cscli decisions delete --ip 192.168.110.140
INFO[2024-03-22T09:47:25+01:00] 2 decision(s) deleted
2.7.2-RELEASE][admin@pfSense.home.arpa]/root: cscli decisions list
No active decisions
```

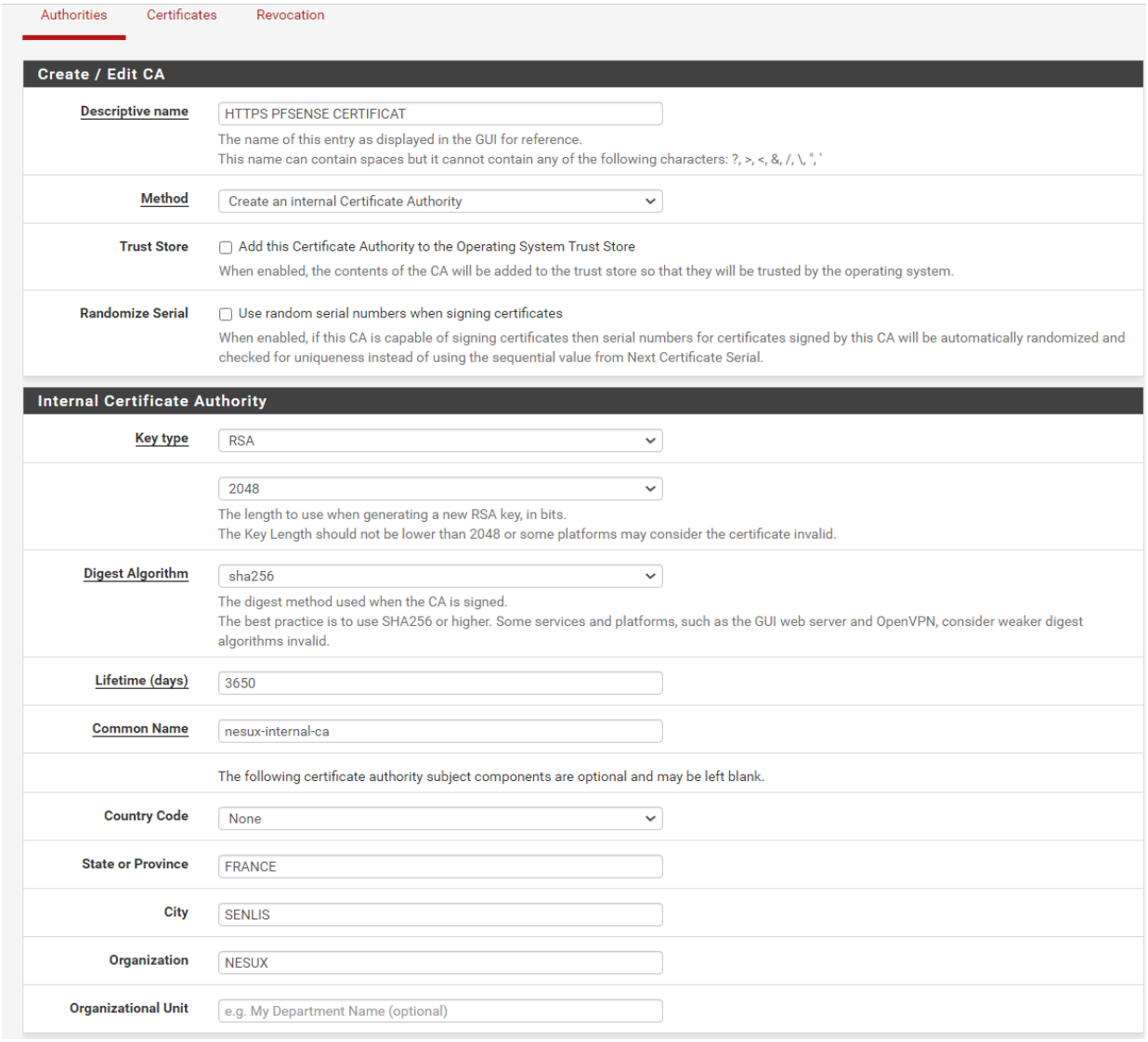
2.10 - Enregistrement DNS



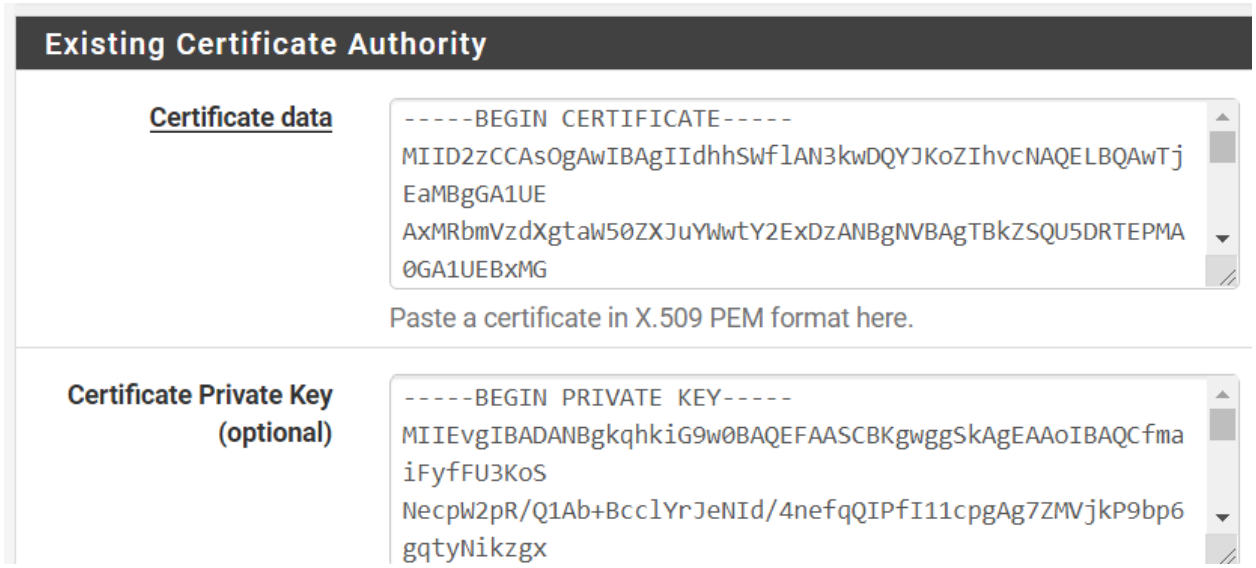
Et été dans SYSTEM → ADVANCED → ADMIN ACCESS sur mon pare-feu et j'ai entré le fqdn.



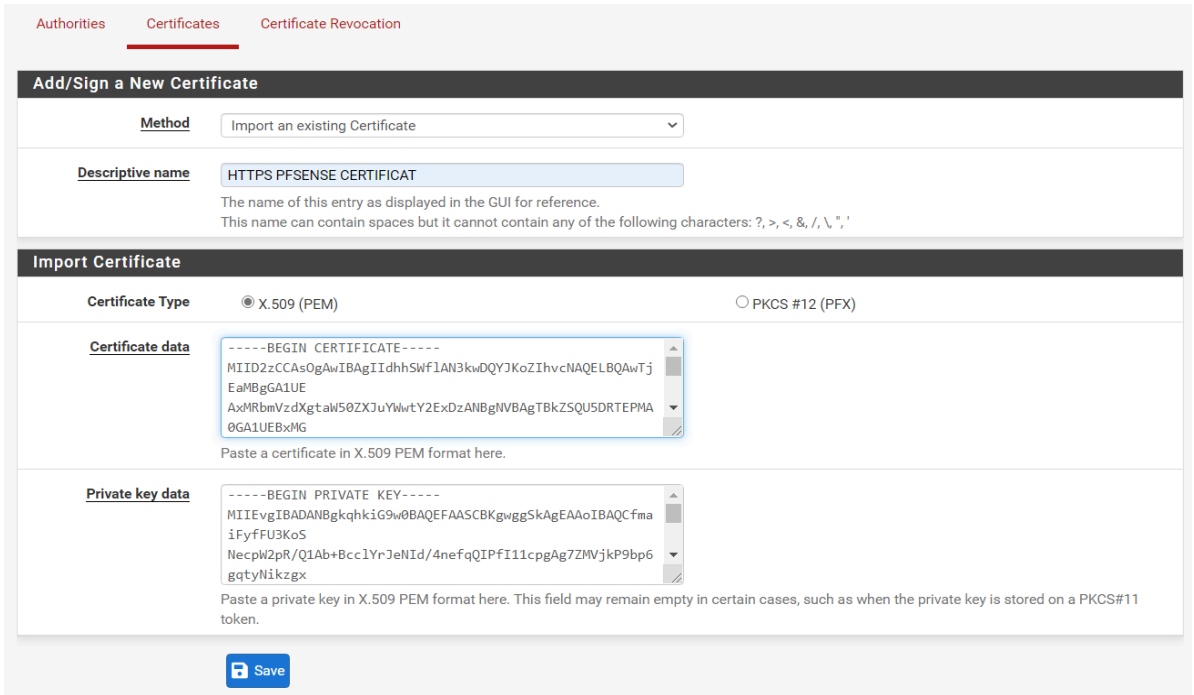
2.11 - Création du certificat HTTPS



Ensuite je copie certificate data et private key



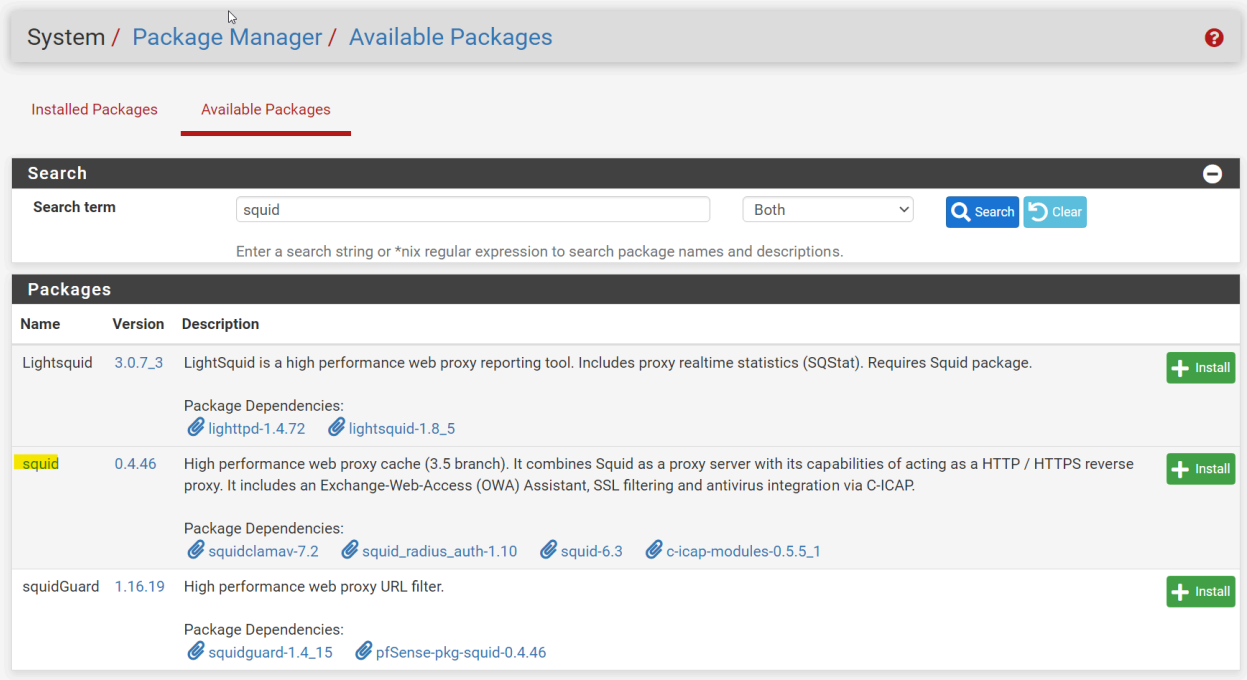
Et j'importe le certificat



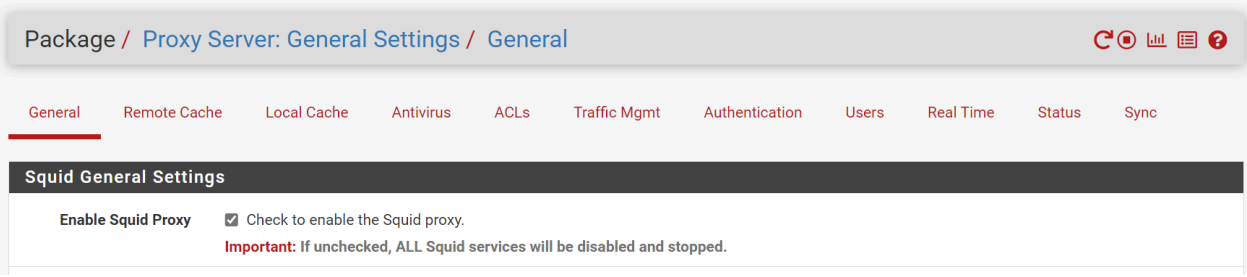
2.12 - Installation de Squid

Squid est un proxy qui va me permettre de bloquer des sites internet et des c to c.

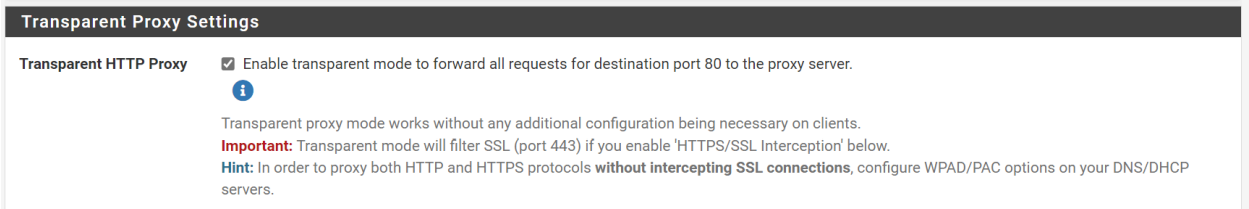
Je commence par l'installer sur mon pare-feu.



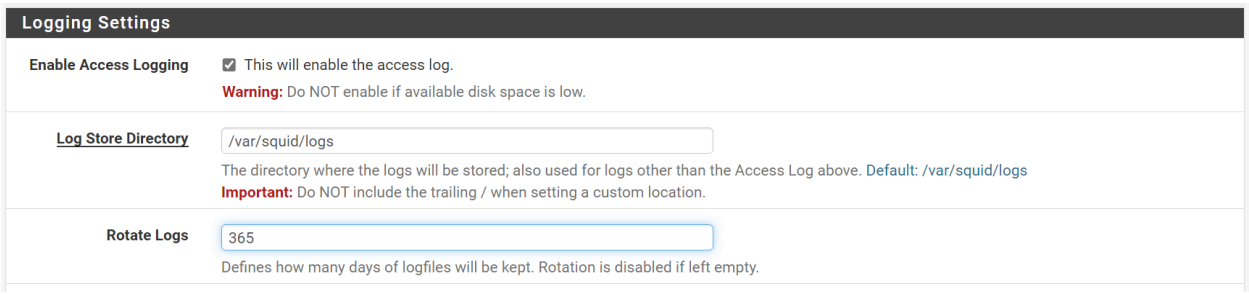
Et dans Service → Squid Proxy Server je save local cache et general en activant le proxy.



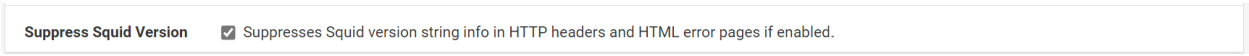
J’active le proxy transparent http.



Et j’active Access Logging pour permettre de savoir qui fait quoi sur Internet

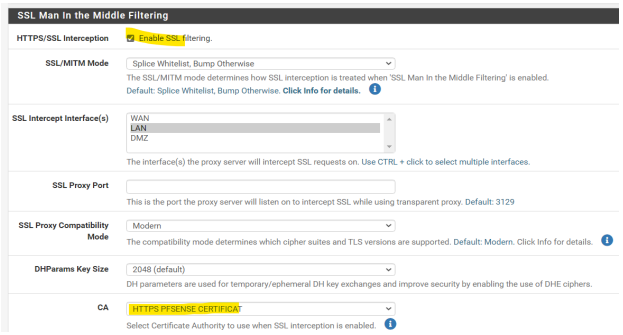


Et je décoche ça afin de masquer les informations sur Squid, comme la version.

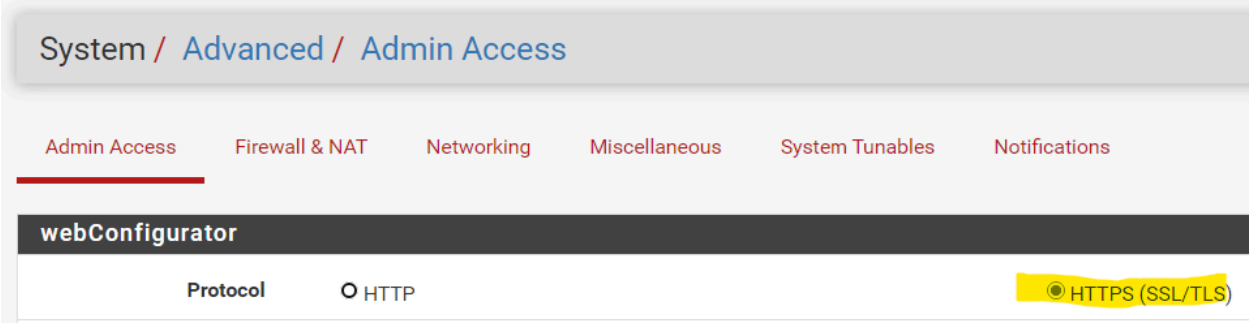


Maintenant le certificat HTTPS que j’ai créé juste avant va me servir à bloquer des sites web, il faut que je fasse 2 choses pour que cela fonctionne.

Dans PROXY SERVER → GENERAL

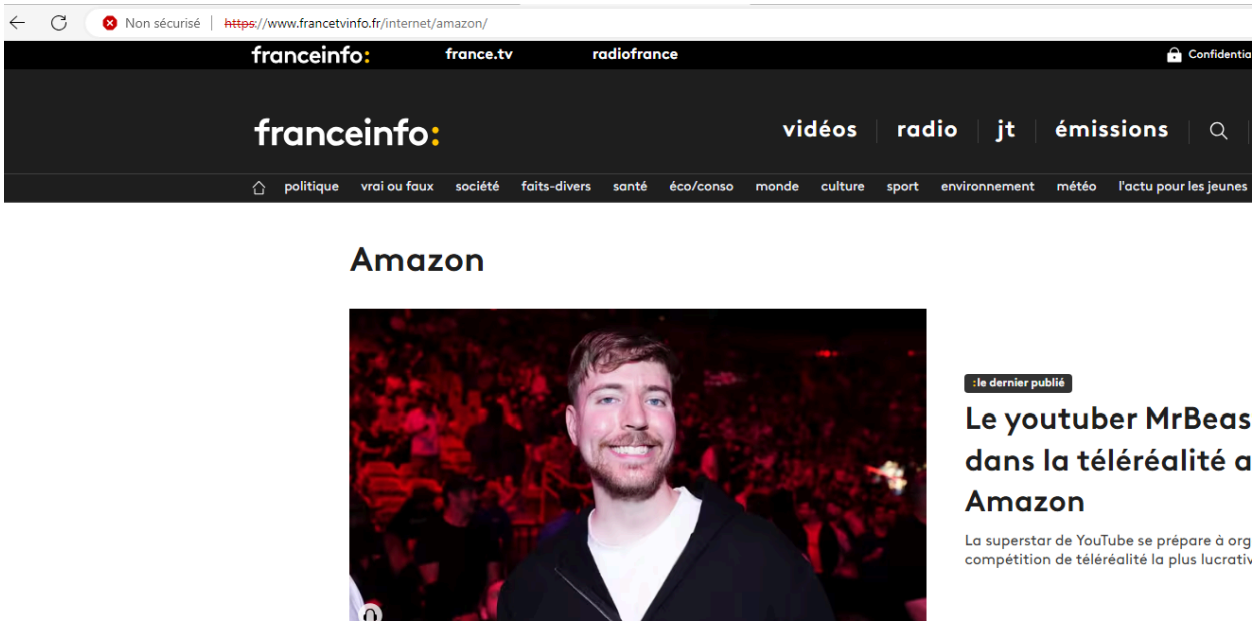


Et ensuite dans SYSTEM → ADVANCED j'active HTTPS(SSL/TLS)

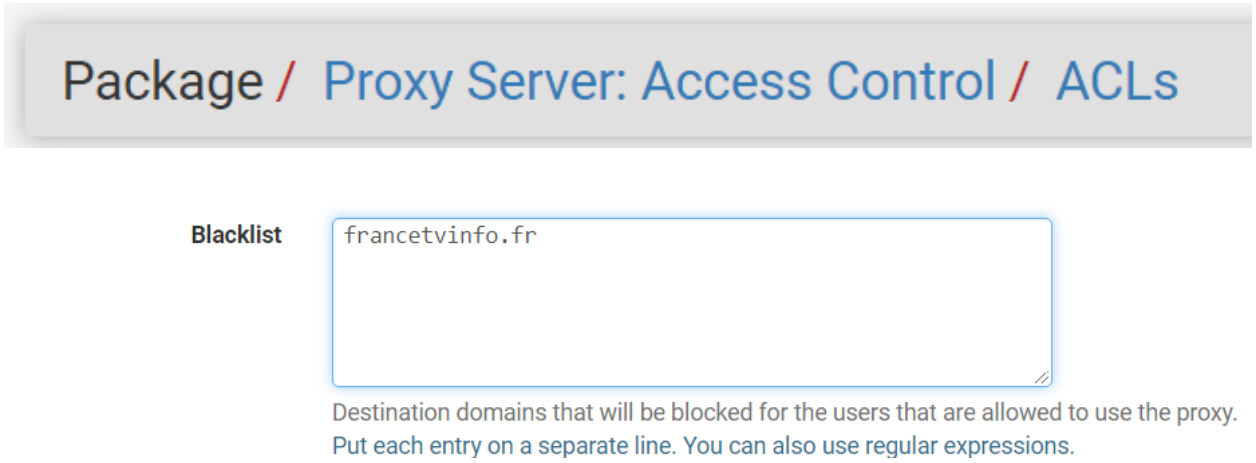


je vais faire le test avec francetvinfo.fr :

Avant blacklist :



Après blacklist :

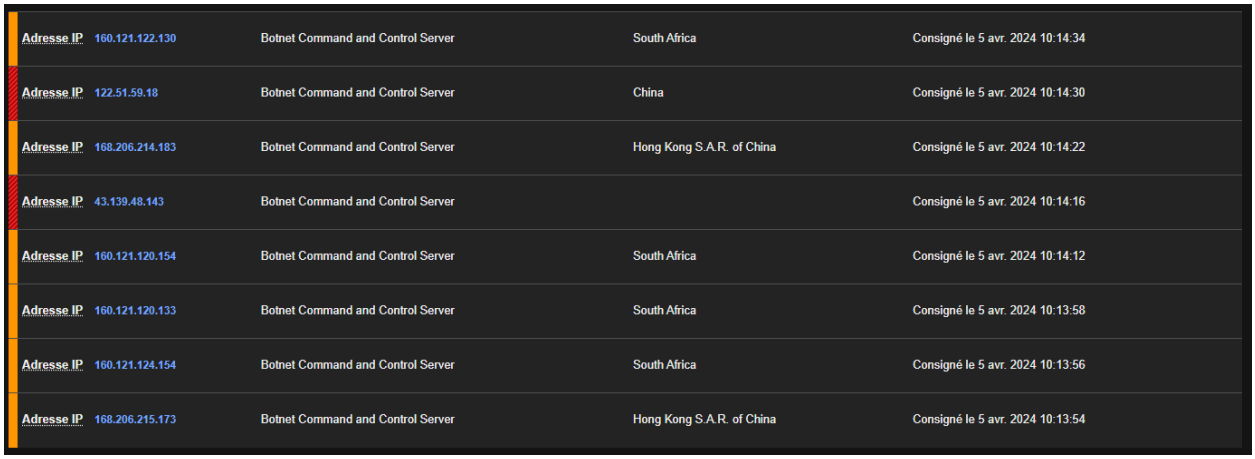


Voilà comment bloquer des sites avec Squid !

2.13 - Blocage des C&C

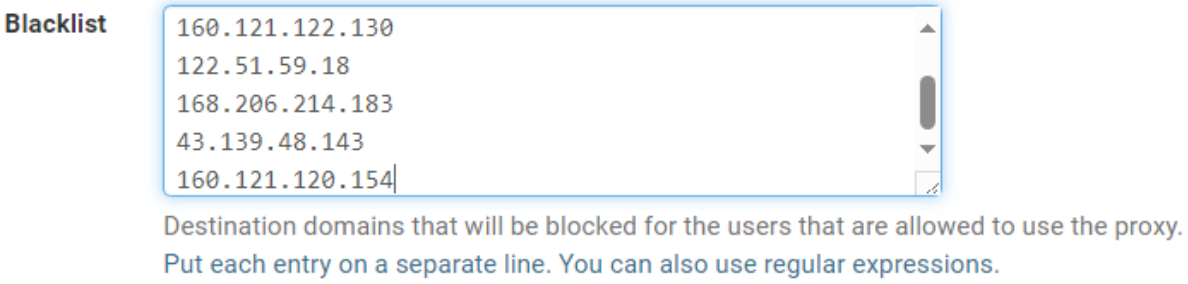
Je me rends sur ce site pour voir quelques adresses IP C&C :

https://exchange.xforce.ibmcloud.com/statshistory/botnetcommandandcontrolserver



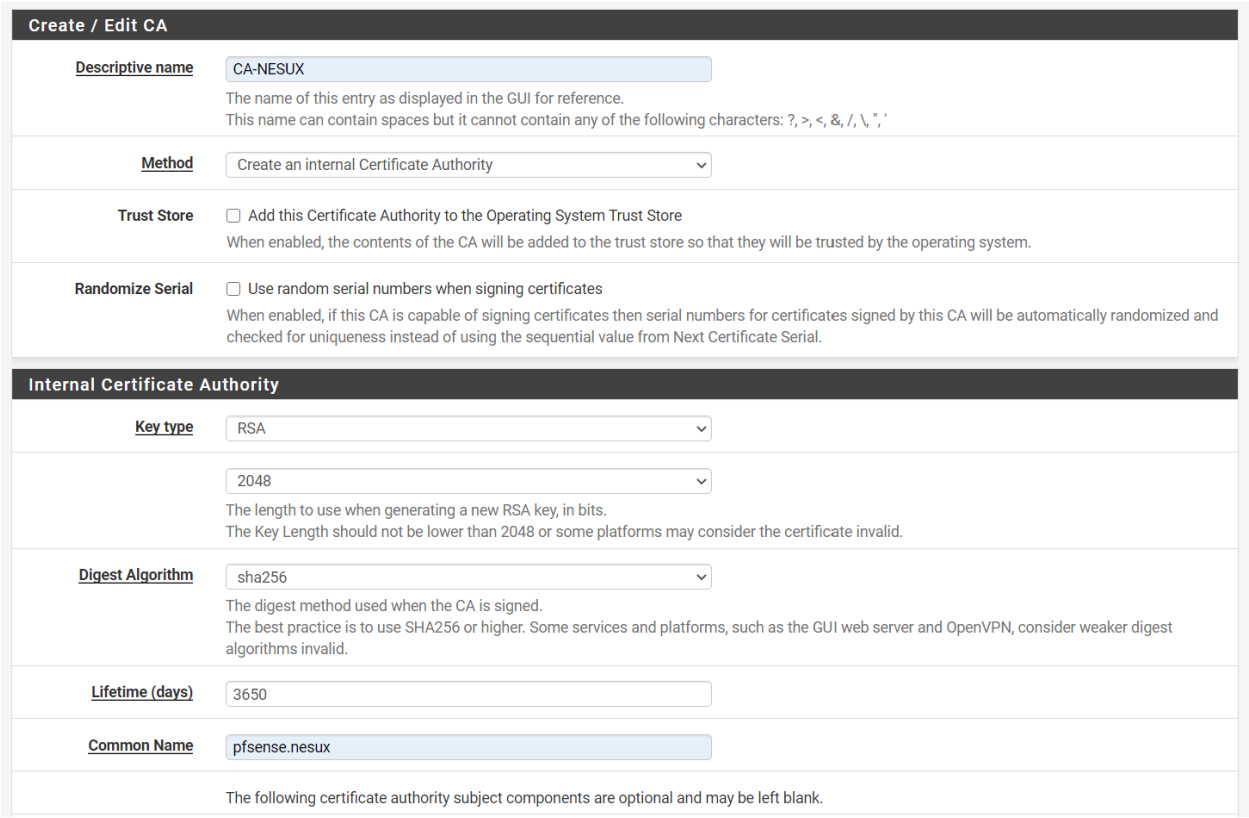
Adresse IP 160.121.122.130	Botnet Command and Control Server	South Africa	Consigné le 5 avr. 2024 10:14:34
Adresse IP 122.51.59.18	Botnet Command and Control Server	China	Consigné le 5 avr. 2024 10:14:30
Adresse IP 168.206.214.183	Botnet Command and Control Server	Hong Kong S.A.R. of China	Consigné le 5 avr. 2024 10:14:22
Adresse IP 43.139.48.143	Botnet Command and Control Server		Consigné le 5 avr. 2024 10:14:16
Adresse IP 160.121.120.154	Botnet Command and Control Server	South Africa	Consigné le 5 avr. 2024 10:14:12
Adresse IP 160.121.120.133	Botnet Command and Control Server	South Africa	Consigné le 5 avr. 2024 10:13:58
Adresse IP 160.121.124.154	Botnet Command and Control Server	South Africa	Consigné le 5 avr. 2024 10:13:56
Adresse IP 168.206.215.173	Botnet Command and Control Server	Hong Kong S.A.R. of China	Consigné le 5 avr. 2024 10:13:54

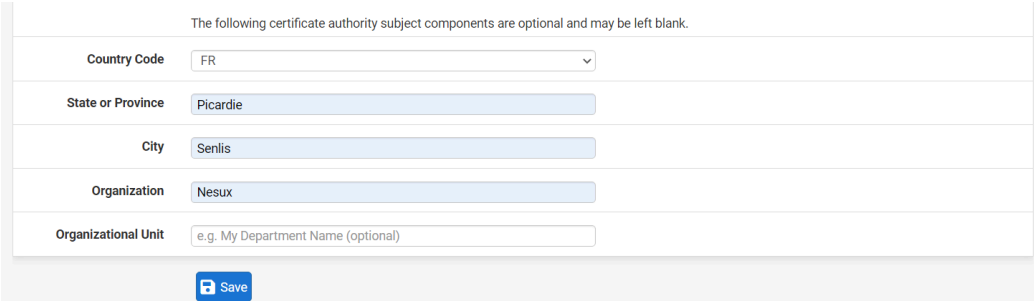
Et ensuite je les mets dans la blacklist.



2.14 - Installation et Configuration d'OpenVPN sur Pfsense

je commence par créer mon autorité de certification.





CA-NESUX	✔	*self-signed*	2	ST=Picardie, O=Nesux, L=Senlis, CN=pfsense.nesux, C=FR Valid From: **Wed, 03 Apr 2024 10:31:08 +0200** Valid Until: **Sat, 01 Apr 2034 10:31:08 +0200**	

Et je créer mon certificat en sélectionnant l'autorité créée juste avant.

Add/Sign a New Certificate

Method : Create an internal Certificate

Descriptive name : Certificat-OpenVPN

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '

Internal Certificate

Certificate authority : CA-NESUX

Key type : RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm : sha256

The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days) : 3650

The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name : pfsense-nesux-firewall

The following certificate subject components are optional and may be left blank.

Country Code : FR

State or Province : Picardie

City : Senlis

Organization : Nesux

Organizational Unit : e.g. My Department Name (optional)

Certificate Attributes

Attribute Notes : The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type : Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names : FQDN or Hostname

Type | Value

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add SAN Row : + Add SAN Row

Save

Certificat-OpenVPN *Server Certificate* CA: **No** Server: **Yes**	CA-NESUX	ST=Picardie, O=Nesux, L=Senlis, CN=pfsense-nesux-firewall, C=FR Valid From: **Wed, 03 Apr 2024 10:33:31 +0200** Valid Until: **Sat, 01 Apr 2034 10:33:31 +0200**	OpenVPN Server

Maintenant je crée l'utilisateur PFSENSE.

User Properties

Defined by	USER
Disabled	☐ This user cannot login
Username	vpn.pfsense.nesux
Password	••••••• •••••••
Full name	User's full name, for administrative information only
Expiration date	Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	☐ Use individual customized GUI options and dashboard layout for this user.
Group membership	admins (Not member of) — (Member of) » Move to "Member of" list — « Move to "Not member of" list Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.
Certificate	☑ Click to create a user certificate

Create Certificate for User

Descriptive name	Certificat-VPN-pfsense.nesux
Certificate authority	CA-NESUX
Key type	RSA
	2048

☐	vpn.pfsense.nesux	✔	

Ensuite je configure le serveur.

Ici j'ai modifié plusieurs choses :

- **DESCRIPTION :** description au choix
- **SERVER MODE :** Remote access (SSL/TLS + User Auth)
- **PEER CERTIFICAT AUTHORITY :** (Authorité de certification créé précédemment)
- **SERVER CERTIFICATE :** (Certificat créé précédemment)
- **IPV4 TUNNEL NETWORK :** (le tunnel va permettre plus de sécurité grâce à des protocoles de chiffrement et d'authentification afin de protéger la communication. Je lui ai mis le réseau 10.10.10.0/24)
- **IPV4 LOCAL NETWORK :** (Ici je déclare les réseaux qui seront accessible depuis le VPN)
- **CONCURRENT CONNECTION :** (J'ai mis 10 connection maximum)
- **DYNAMIC IP et TOPOLOGY :** (Je l'ai activé pour le maintien des connexions et j'ai sélectionner la topologie en /30)
- **DNS DEFAULT DOMAIN :** (j'ai mis le nom de mon domaine)
- **DNS SERVER :** (J'ai mis l'ip de mon Serveur)
- **CUSTOM OPTION :** (protection supplémentaire contre le vol des identifiants en refusant la mise en cache)

General Information

Description
Accès distant OpenVPN
A description of this VPN for administrative reference.

Disabled
☐ Disable this server
Set this option to disable this server without removing it from the list.

Unique VPN ID
Server 1 (ovpns1)

Mode Configuration

Server mode
Remote Access (SSL/TLS + User Auth)

Backend for authentication
Local Database

Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol
UDP on IPv4 only

Interface
WAN
The interface or Virtual IP address where OpenVPN will receive client connections.

Local port
1194
The port used by OpenVPN to receive client connections.

Cryptographic Settings

TLS Configuration
☑ Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.

TLS Key
```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
3f68674d68a44a1d7f3e3c64b2c62c55
```
Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.

TLS Key Usage Mode
TLS Authentication
In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

TLS keydir direction
Use default direction
The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Peer Certificate Authority
CA-NESUX

Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager

OCSP Check
☐ Check client certificates with OCSP

Server certificate
Certificat-OpenVPN (Server: Yes, CA: CA-NESUX, In Use)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.

ECDH Curve

Use Default

The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Algorithms

Available Data Encryption Algorithms:
AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

Allowed Data Encryption Algorithms:
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.

Fallback Data Encryption Algorithm

AES-256-CBC (256 bit key, 128 bit block)

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

Auth digest algorithm

SHA256 (256-bit)

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto

No Hardware Crypto Acceleration

Certificate Depth

One (Client+Server)

When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Strict User-CN Matching

☐ Enforce match

When authenticating users, enforce a match between the common name of the client certificate and the username given at login.

Client Certificate Key Usage Validation

☑ Enforce key usage

Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

General Information

Description

Accès distant OpenVPN

A description of this VPN for administrative reference.

Disabled

☐ Disable this server

Set this option to disable this server without removing it from the list.

Unique VPN ID

Server 1 (ovpns1)

Mode Configuration

Server mode

Remote Access (SSL/TLS + User Auth)

Backend for authentication

Local Database

Device mode

tun - Layer 3 Tunnel Mode

"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol

UDP on IPv4 only

Interface

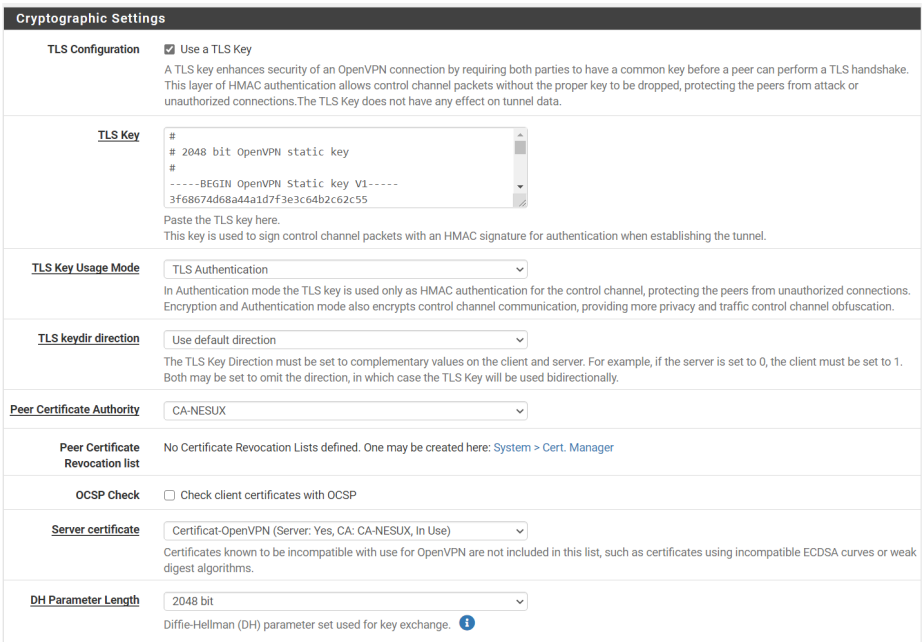
WAN

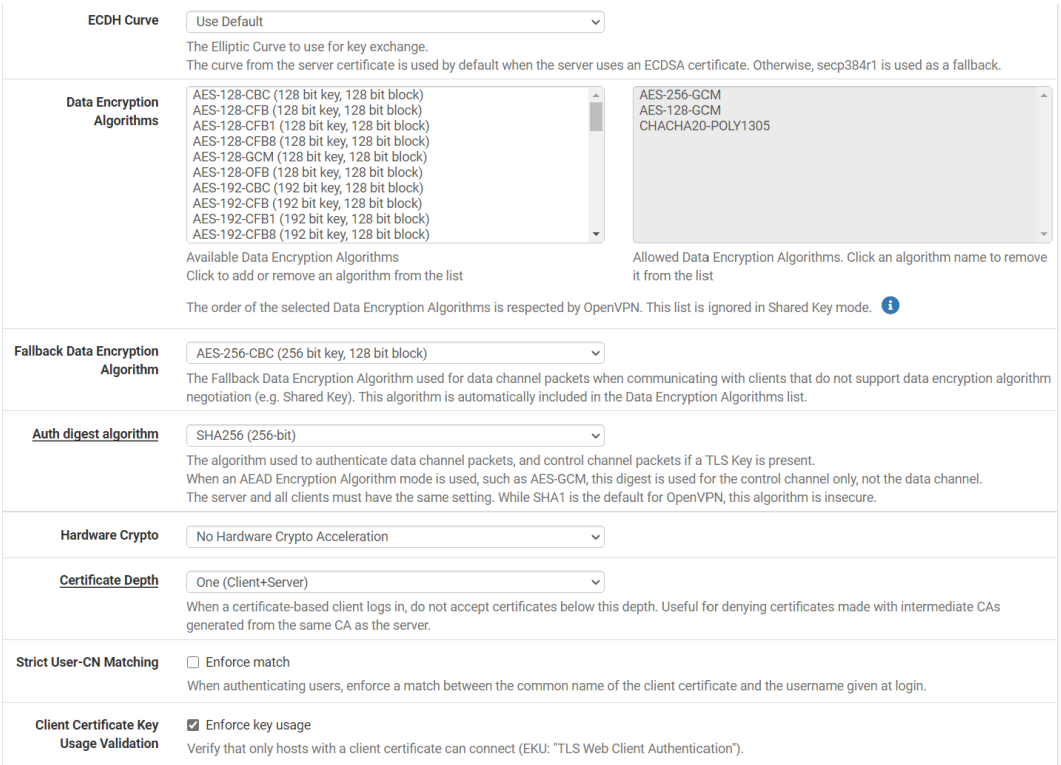
The interface or Virtual IP address where OpenVPN will receive client connections.

Local port

1194

The port used by OpenVPN to receive client connections.


Cryptographic Settings
TLS Configuration
Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.
TLS Key
#
2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
3f68674d68a44a1d7f3e3c64b2c62c55
Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.
TLS Key Usage Mode
TLS Authentication
In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.
TLS keydir direction
Use default direction
The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.
Peer Certificate Authority
CA-NESUX
Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check
Check client certificates with OCSP
Server certificate
Certificat-OpenVPN (Server: Yes, CA: CA-NESUX, In Use)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.
DH Parameter Length
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.


ECDH Curve
Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Algorithms
AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)
Available Data Encryption Algorithms
Click to add or remove an algorithm from the list
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305
Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list
The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.
Fallback Data Encryption Algorithm
AES-256-CBC (256 bit key, 128 bit block)
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.
Auth digest algorithm
SHA256 (256-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.
Hardware Crypto
No Hardware Crypto Acceleration
Certificate Depth
One (Client+Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.
Strict User-CN Matching
Enforce match
When authenticating users, enforce a match between the common name of the client certificate and the username given at login.
Client Certificate Key Usage Validation
Enforce key usage
Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

Tunnel Settings

IPv4 Tunnel Network

10.10.10.0/24

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway

☐ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway

☐ Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)

192.168.1.0/29

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent connections

10

Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression

Refuse any non-stub compression (Most secure)

Allow compression to be used with this VPN instance.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

Asymmetric compression allows an easier transition when connecting with older peers.

Type-of-Service

☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client communication

☐ Allow communication between clients connected to this server

Duplicate Connection

☐ Allow multiple concurrent connections from the same user

When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

Client Settings

Dynamic IP

☑ Allow connected clients to retain their connections if their IP address changes.

Topology

net30 – Isolated /30 network per client

Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4.
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Ping settings

Inactive

300

Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device.
Activity is based on the last incoming or outgoing tunnel packet.
A value of 0 disables this feature.
This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

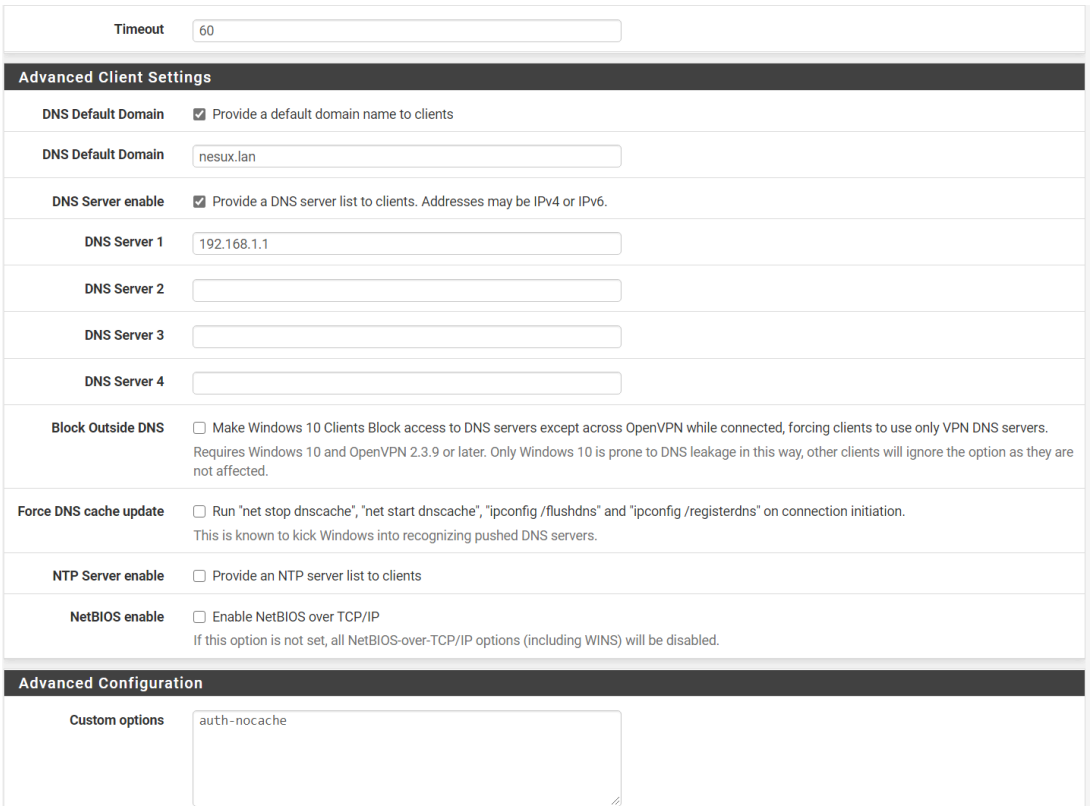
Ping method

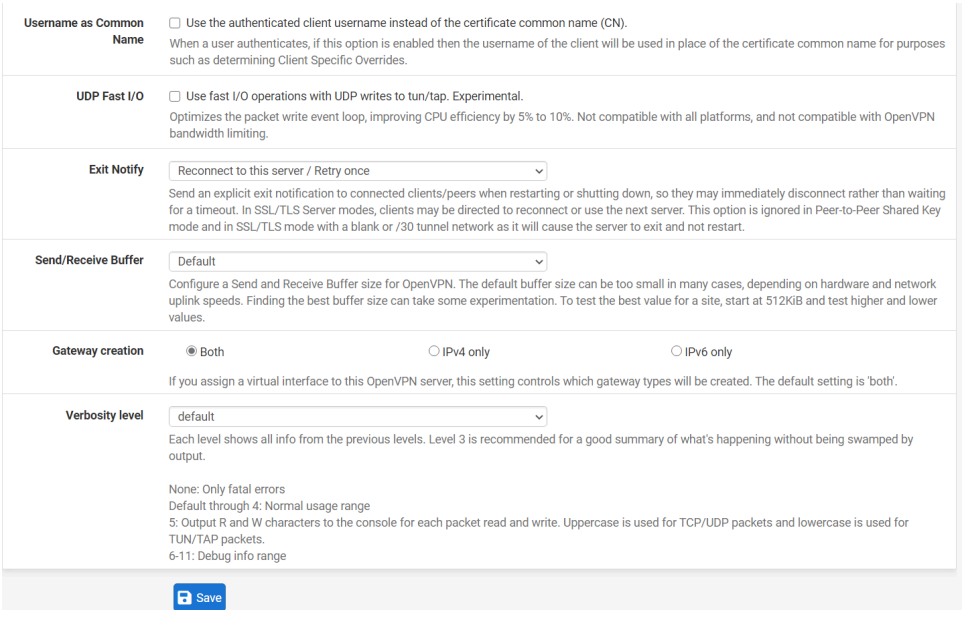
keepalive – Use keepalive helper to define ping configuration

keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:
ping = interval
ping-restart = timeout*2
push ping = interval
push ping-restart = timeout

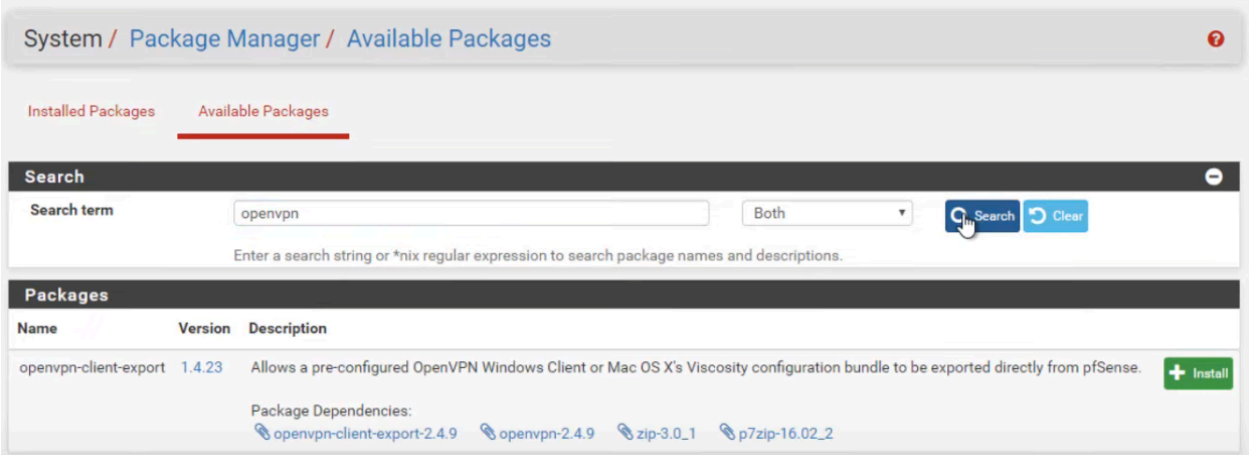
Interval

10


Timeout
60
Advanced Client Settings
DNS Default Domain
Provide a default domain name to clients
DNS Default Domain
nesux.lan
DNS Server enable
Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1
192.168.1.1
DNS Server 2
DNS Server 3
DNS Server 4
Block Outside DNS
Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Force DNS cache update
Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation.
This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable
Provide an NTP server list to clients
NetBIOS enable
Enable NetBIOS over TCP/IP
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
Advanced Configuration
Custom options
auth-nocache


Username as Common Name
Use the authenticated client username instead of the certificate common name (CN).
When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.
UDP Fast I/O
Use fast I/O operations with UDP writes to tun/tap. Experimental.
Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.
Exit Notify
Reconnect to this server / Retry once
Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.
Send/Receive Buffer
Default
Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.
Gateway creation
Both
IPv4 only
IPv6 only
If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.
Verbosity level
default
Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.
None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range
Save

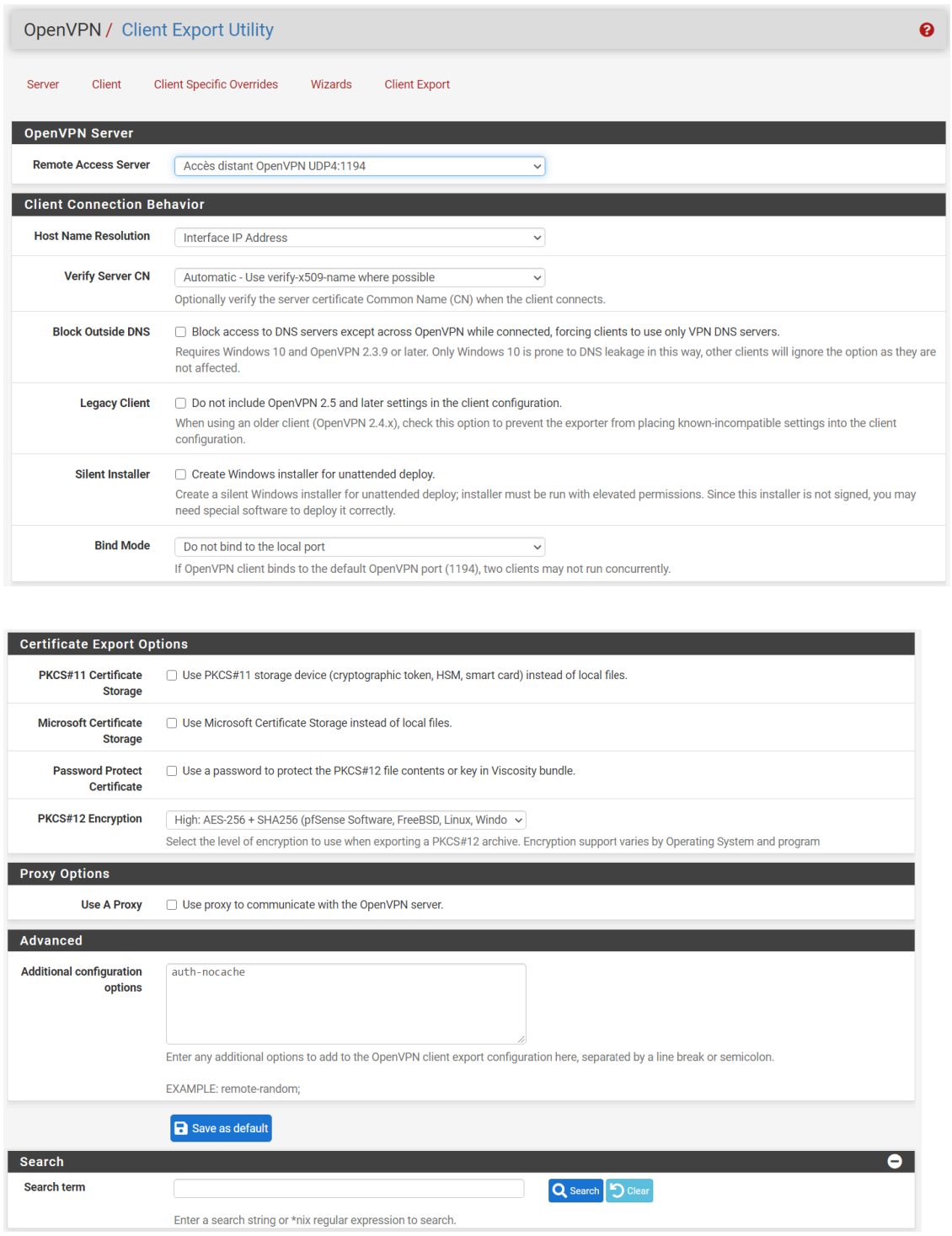
Maintenant j'exporte la configuration de mon utilisateur. Avant il faut installer "openvpn-client-export" dans System -> Package Manager -> Available Packages



Et je vais dans OpenVPN → Client Export

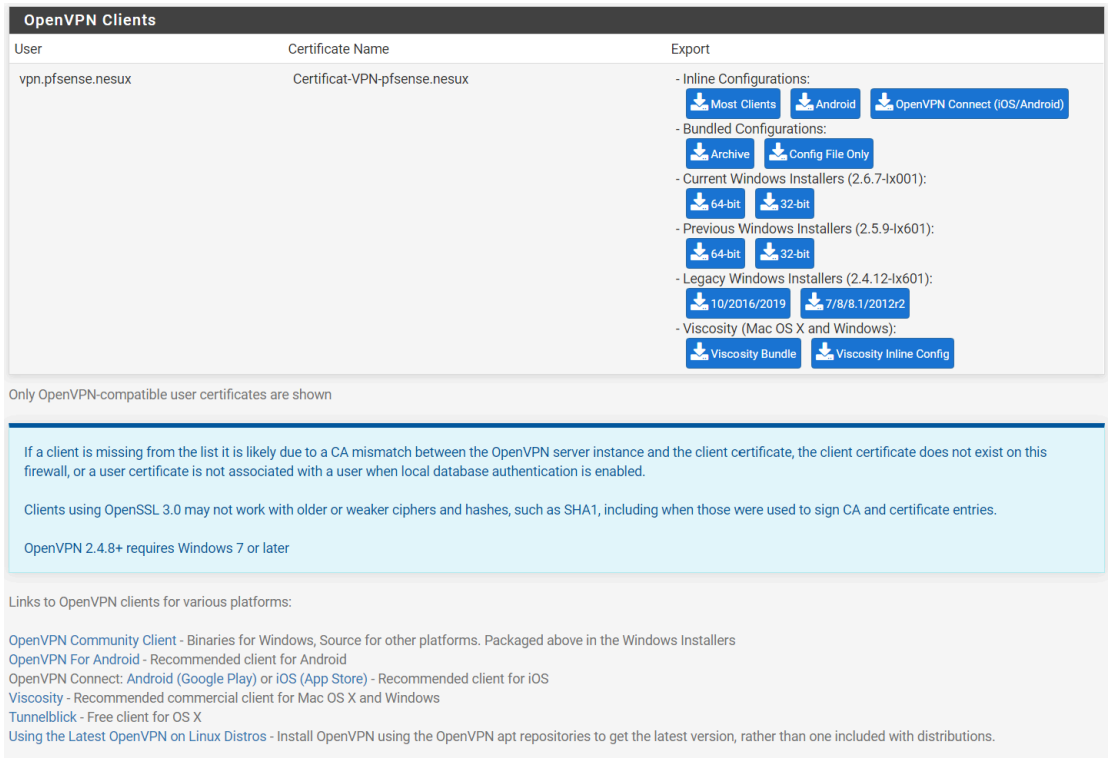
Voici les choses que j'ai modifié ici :

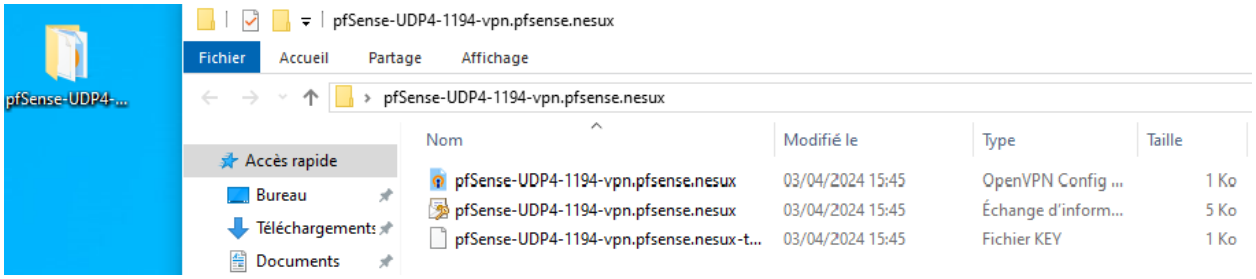
- **REMOTE ACCESS SERVER :** J'ai bien sélectionner le bon Serveur VPN créé juste avant
- **ADDITIONAL CONFIGURATION OPTIONS :** Je remets auth-nocache


OpenVPN / Client Export Utility
Server
Client
Client Specific Overrides
Wizards
Client Export
OpenVPN Server
Remote Access Server
Accès distant OpenVPN UDP4:1194
Client Connection Behavior
Host Name Resolution
Interface IP Address
Verify Server CN
Automatic - Use verify-x509-name where possible
Optionally verify the server certificate Common Name (CN) when the client connects.
Block Outside DNS
Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Legacy Client
Do not include OpenVPN 2.5 and later settings in the client configuration.
When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.
Silent Installer
Create Windows installer for unattended deploy.
Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.
Bind Mode
Do not bind to the local port
If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.
Certificate Export Options
PKCS#11 Certificate Storage
Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.
Microsoft Certificate Storage
Use Microsoft Certificate Storage instead of local files.
Password Protect Certificate
Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.
PKCS#12 Encryption
High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Windo
Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program
Proxy Options
Use A Proxy
Use proxy to communicate with the OpenVPN server.
Advanced
Additional configuration options
auth-nocache
Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.
EXAMPLE: remote-random;
Save as default
Search
Search term
Search
Clear
Enter a search string or *nix regular expression to search.

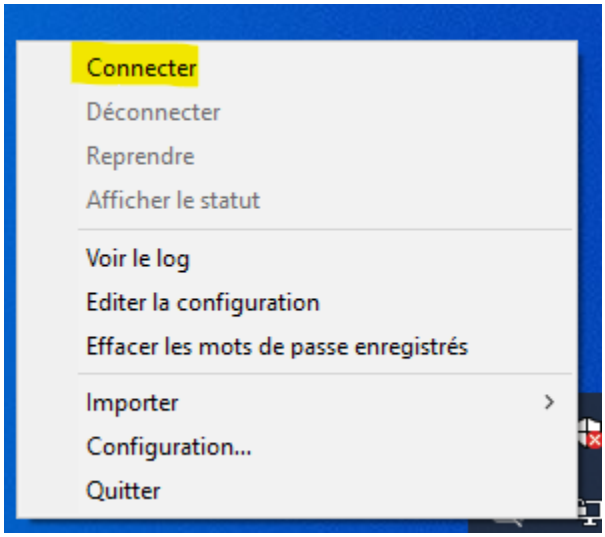
Et dans Bundled Configuration je télécharge l'archive.

Et dans Current Windows Installers (2.6.7-Ix001) je télécharge OpenVPN.

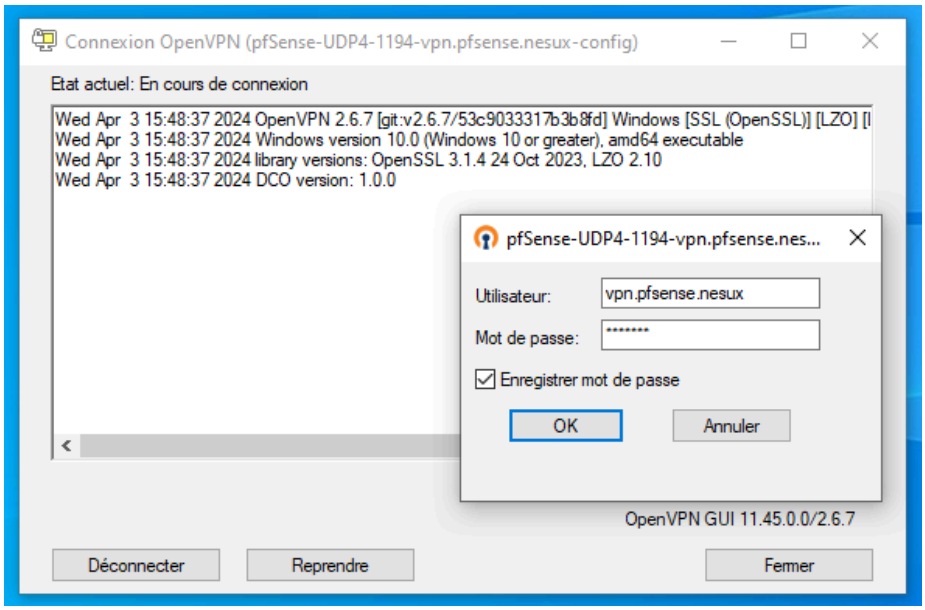




2.15 - Test OpenVPN



Je me connecte avec l'utilisateur créer sur pfsense.



ET VOILÀ !!!!

2.16 - LDAP pour les utilisateurs de la zone locale (en cours)

2.17 - Synthèse des règles (en cours)

3) CONCLUSION

L'entreprise de développement logiciels NESUX possède désormais un réseau fonctionnel avec une zone locale, une zone DMZ, un VPN et un pare-feu PFSENSE qui comporte les fonctionnalités CROWDSEC et SQUID.