05/04/2024

PFSENSE

Alexis PENET
TECHVISTA

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 : Alexis PENET	**N° candidat :**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 05/04/2023

Organisation support de la réalisation professionnelle

Intitulé de la réalisation professionnelle

Mise en d'un pare-feu sous PFSENSE.

Période de réalisation : 15/11/2023 – 15/12/2023 **Lieu :** Senlis

Modalité : ☒ **Seul(e)** ☐ **En équipe**

Compétences travaillées

- ☒ Concevoir une solution d'infrastructure réseau
- ☒ Installer, tester et déployer une solution d'infrastructure réseau
- ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[1] (ressources fournies, résultats attendus)

Serveur LINUX
Serveur AD
Client W10
Serveur AD
Serveur PFSENSE
Kali linux

Les résultats attendus du PPE sont :

SQUID
Crownsec
VPN
LDAP
DMZ (un serveur linux avec service web)
Lan (active directory et 2 clients windows)

Description des ressources documentaires, matérielles et logicielles utilisées[2]

https://www.it-connect.fr/tuto-installation-crowdsec-pare-feu-pfsense/?utm_content=cmp-true
https://www.it-connect.fr/mise-en-place-et-configuration-dun-proxy-avec-squid/

VMware Workstation 17
Pfsense
Windows 11 22h2
Debian 11
Windows server 2022
Word, bloc note

Modalités d'accès aux productions[3] et à leur documentation[4]

Windows 11 → 1er mdp Azerty1* 2ème Azerty1, Azerty12, alexis → Azerty12

Sommaire

Introduction

Cette mission consiste à installer 6 VM sous PFSENSE,LINUX,Windows,Windows Server, Kali linux afin de créer un réseau avec un pare-feu.

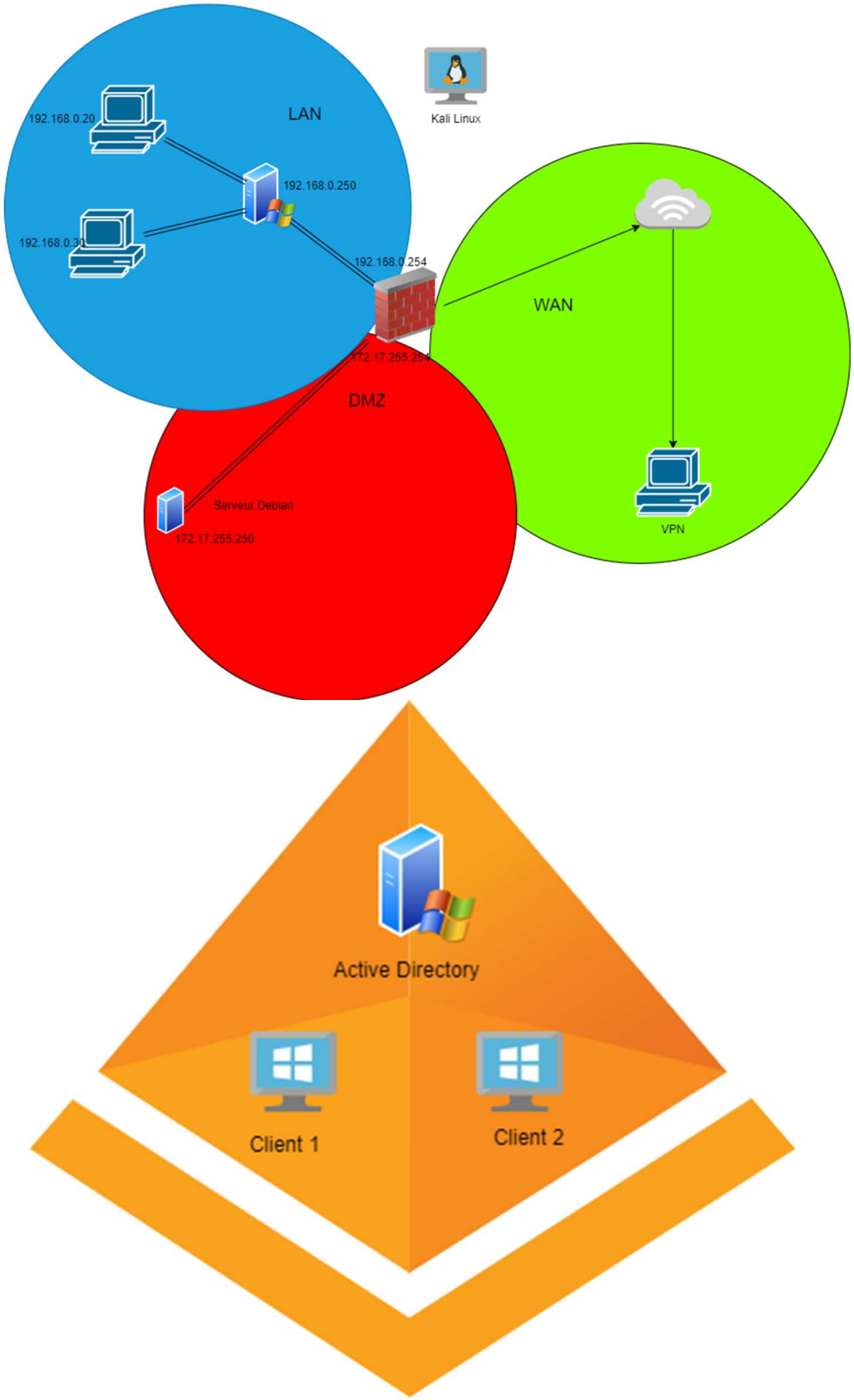
Le but est de construire un réseau avec 3 sites (WAN ,LAN,DMZ) pour mettre en place

- SQUID
- Crownsec
- VPN
- LDAP
- DMZ (un serveur linux avec service web)
- Lan (active directory et 2 clients windows)

Contexte

Dans le cadre d'un déploiement réseau pour une entreprise, l'équipe informatique utilise pfSense pour mettre en place une infrastructure sécurisée.
Trois zones principales sont définies : le WAN pour l'accès à Internet, le LAN pour les ressources internes, et la DMZ pour les serveurs accessibles depuis Internet.
Avec pfSense, des règles de pare-feu précises sont configurées pour contrôler le flux de trafic entre ces zones, assurant ainsi une sécurité renforcée et des performances optimales.

Architecture réseau



WAN = DHCP

LAN = 192.168.0.254 /24

DMZ = 172.17.255.254 /16

Serveur Debian (DMZ) = 172.17.255.250 /16

AD (LAN) = 192.168.0.250 /24

Client 1 (LAN) = 192.168.0.20 /24

Client 2 (LAN) = 192.168.0.30 /24

Kali linux = ?

Configuration PFSENSE

PFsense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.

1. Configuration des cartes WAN,LAN, DMZ.

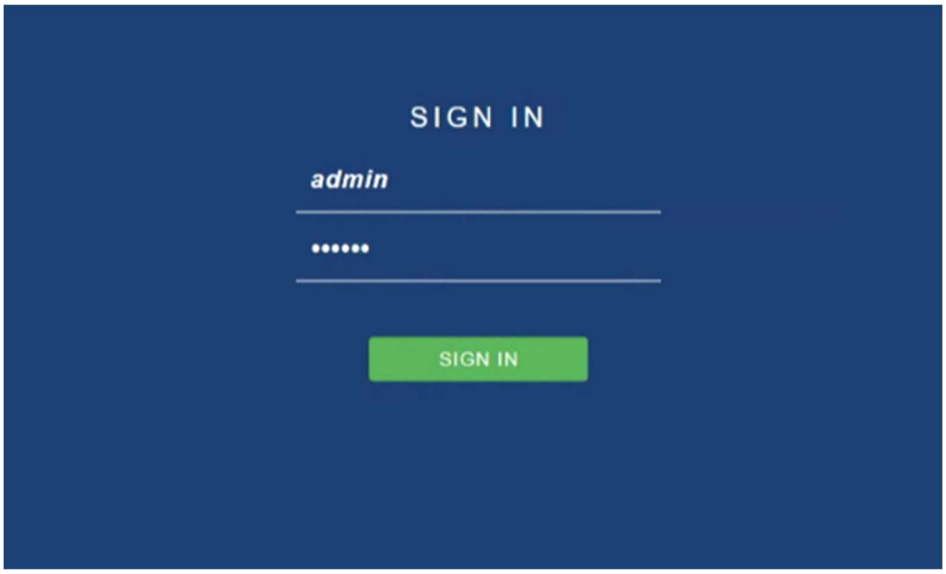
Un WAN (Wide Area Network, ou réseau étendu) est un réseau couvrant une zone géographique de grande envergure. Votre modem envoie et reçoit des informations depuis et vers Internet via son port WAN.

Le LAN (Local Area Network, ou réseau local) désigne les appareils connectés, par Wi-Fi ou connexion filaire, dans votre domicile ou bureau. Il s'agit d'un réseau personnel.

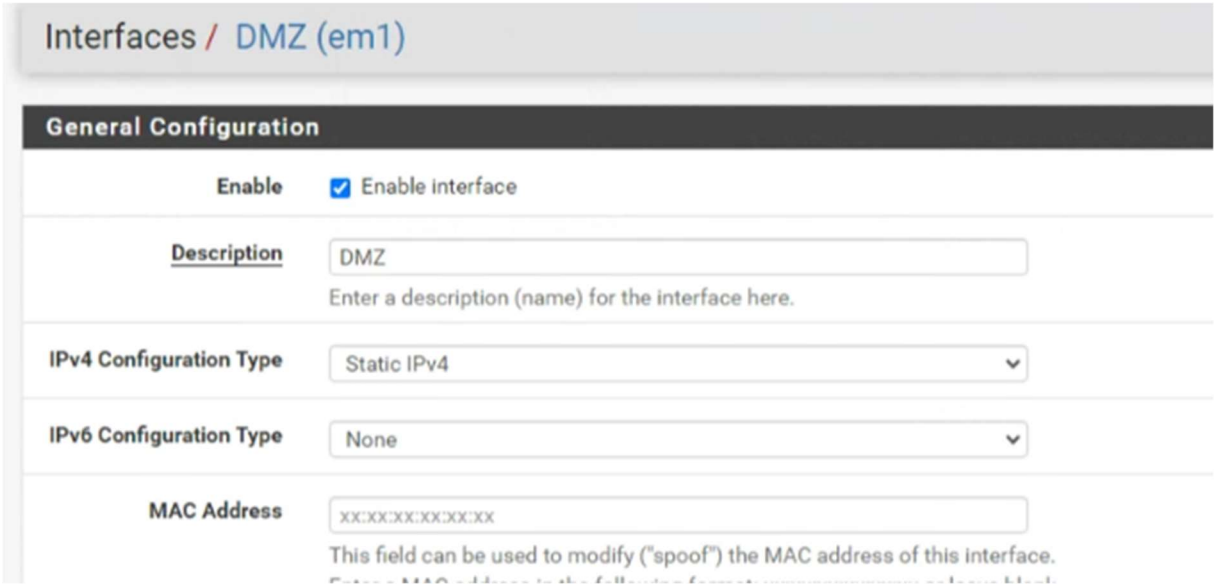
Une zone démilitarisée (DMZ, Demilitarized Zone) est un sous-réseau physique ou logique qui sépare un réseau local interne (LAN, Local Area Network) d'autres réseaux non sécurisés tels qu'Internet.

Pour configurer les cartes il faut ajouter des cartes virtuelles dans la vm PFSENSE, clic droit → settings → on ajoute 2 LAN SEGMENT qu'on appellera LAN et DMZ puis on ajoute une vmet en bridge pour le WAN.

Ensuite on appuie sur '' Assign Interfaces '' puis on suit les étapes pour ajouter les cartes virtuelles en faisant attention aux configurations précédentes.
On tape 2 pour ajouter des adresses au WAN,LAN et DMZ.
Une fois fait on prends un pc connecté au lan puis on se rend sur l'interfaces WEB du pfsense. '' http://192.168.0.254 ou https://192.168.0.254 ''



User=admin
Password=pfsense

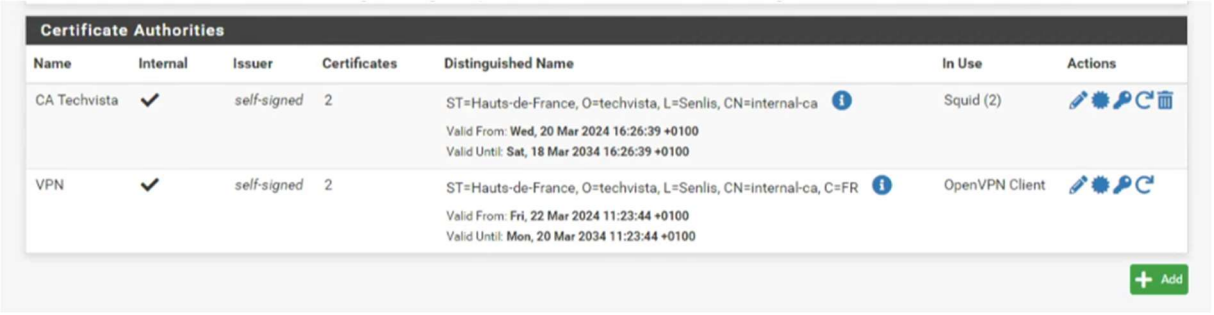


Une fois dans l'interface WEB on renomme la carte par DMZ puis on l'active.
Pour ce qui est des cartes tout est fait.

HTTPS

Le protocole HTTPS (hyper text tranfert protocol secure) c'est une extension du protocole http mais grâce à l'https les données entre le navigateur et l'internaute sont chiffrés, ils ne peuvent pas être espionnés. Une attaque MitmHTTP permet d'intercepter des communications pour pouvoir le lire le https offrent une option de cryptage ce qui nous permettra de ne pas être lu.

Nous allons voir comment le mettre en place.



On appuie sur ADD puis on remplit les cases correspondantes pour créer l'autorité de certification.

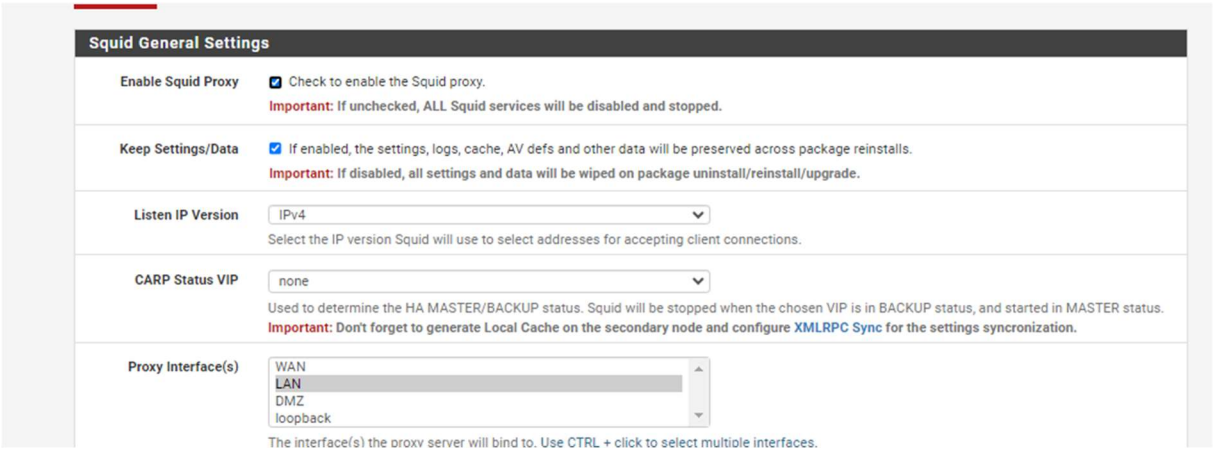
On appuie sur ADD puis on remplit toutes les cases. (exemple si dessous)
Pour le deuxième certificat on change le ''Certificate type'' par server certificate.

Ensuite on va dans système → Advanced → Admin Access puis on active le protocol HTTPS.

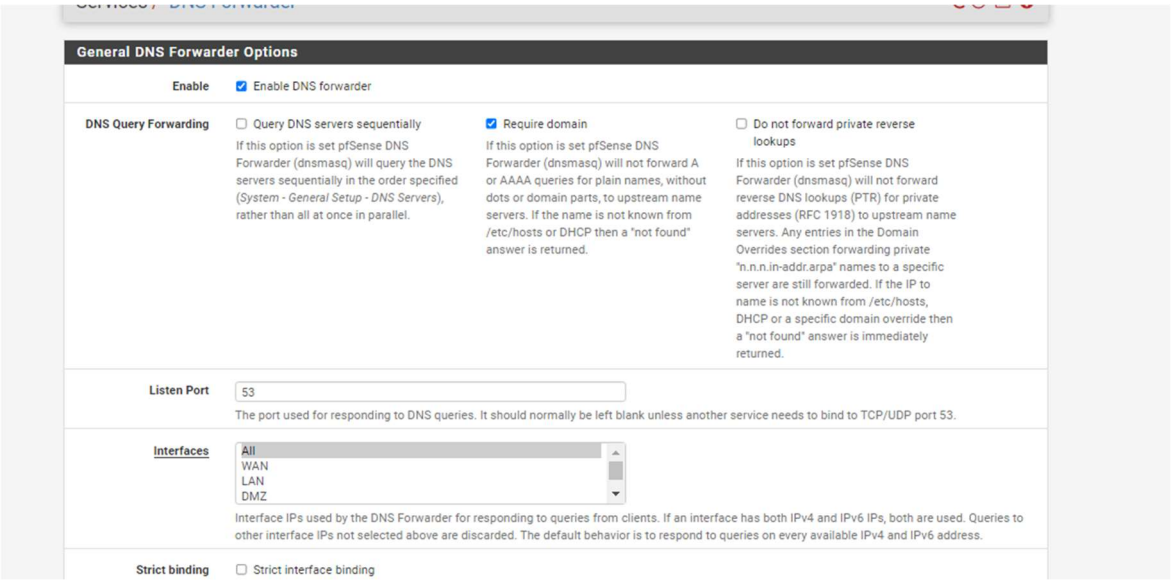
SQUID

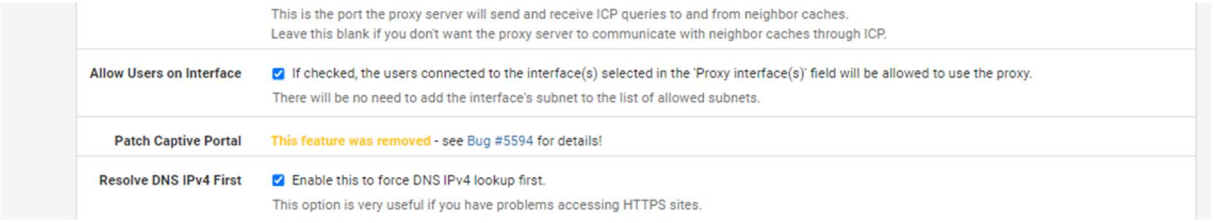
Squid est un serveur proxy spécialisé, basé sur Unix, qui agit comme un proxy de mise en cache pour les objets web accessibles par HTTP, HTTPS, FTP, etc. Il est couramment utilisé à plusieurs fins, notamment pour la mise en cache, l'équilibrage de la charge, le filtrage du trafic des sites web et la sécurité.

Pour commencer nous allons dans services → Squid Proxy Server → General.



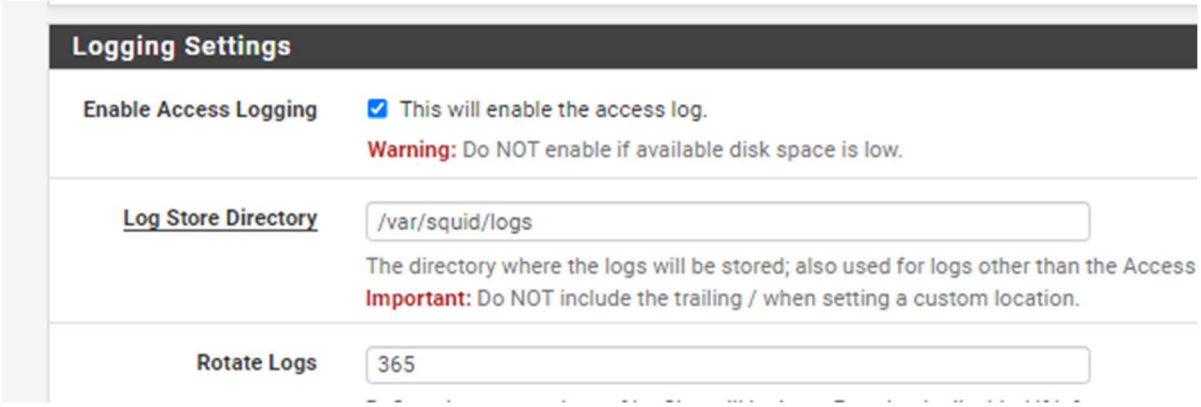
On coche les cases au-dessus.

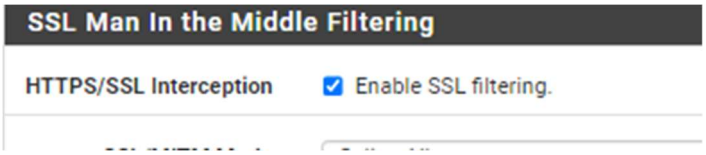


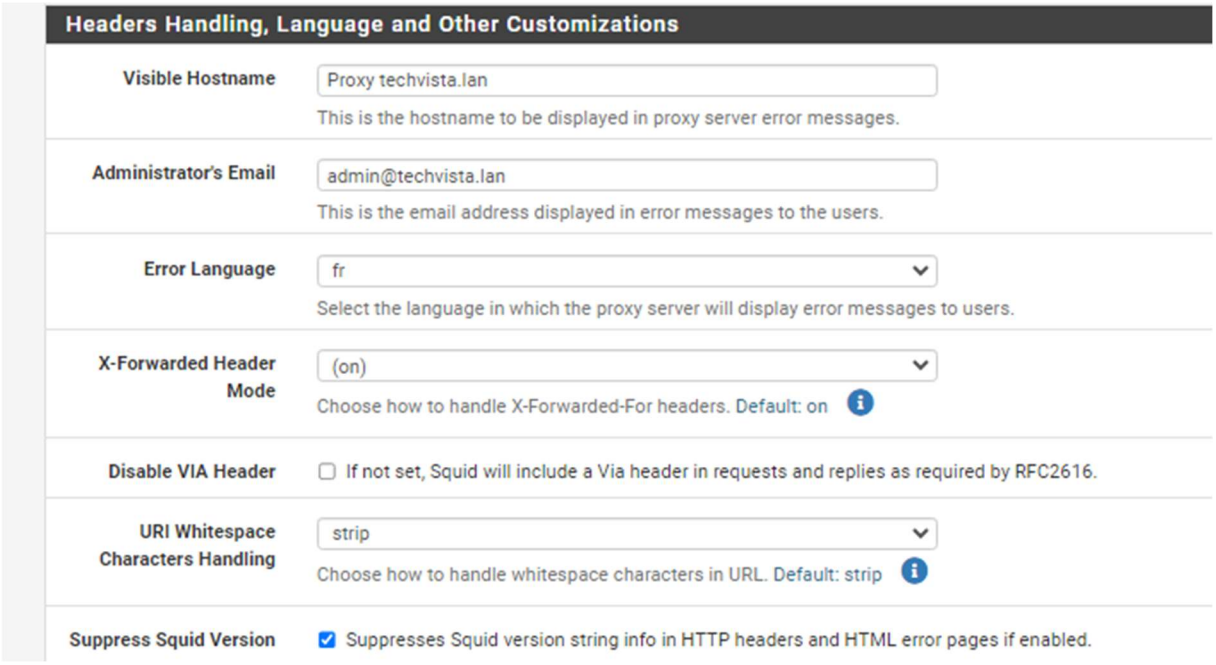


Dans service → DNS Forwarder on coche les cases suivantes pour pouvoir bloquer les sites en HTTPS.

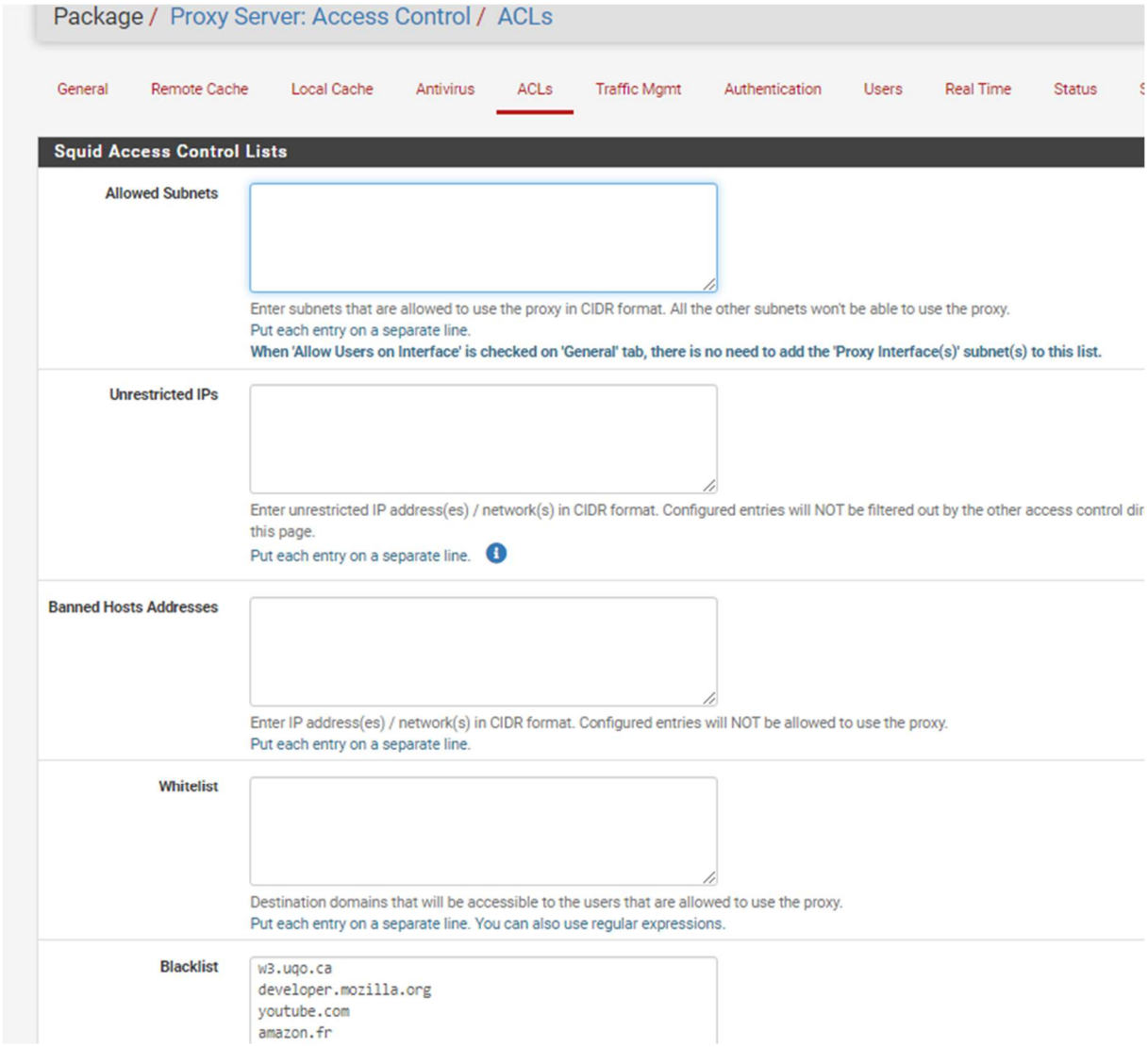
Puis dans services → Squid Proxy Server → General on remplis/coche toutes les cases ci-dessous.

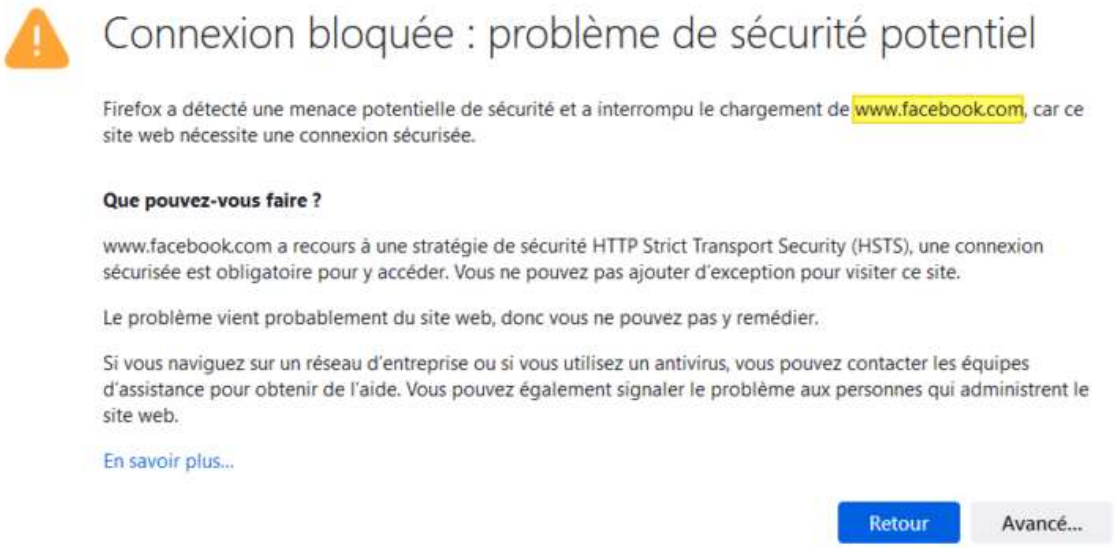






Une fois faits-nous pouvons faire un essai dans blacklist pour voir si le site bloque le HTTPS.



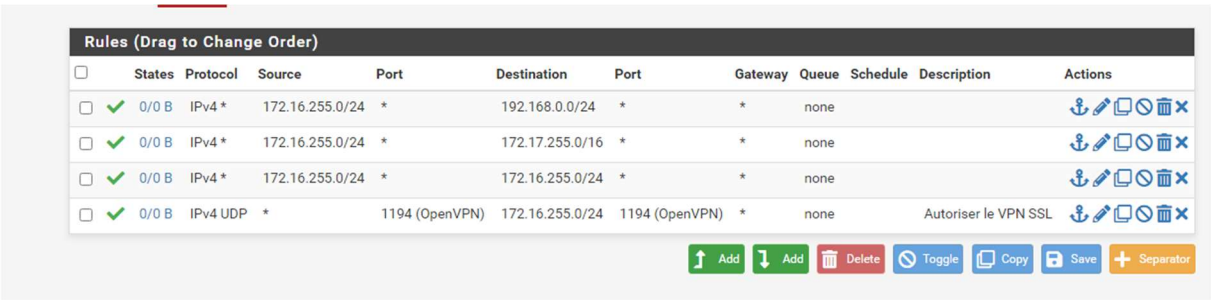


Nous pouvons voir que ça a fonctionner.

Règles pare-feu

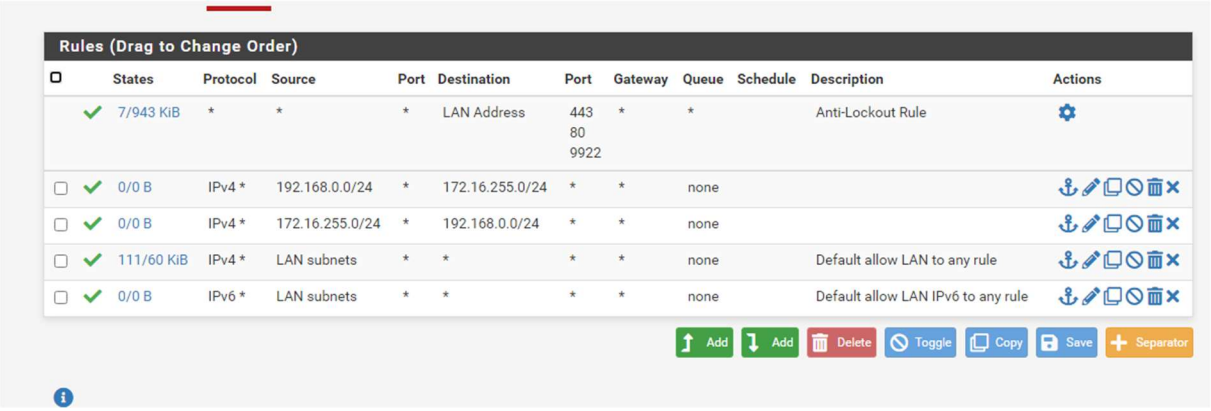
Nous allons ajouter des règles pour pouvoir autoriser des communications et interdire des communications en réseau.
Nous allons en appliquer sur le WAN, LAN et DMZ.

WAN :



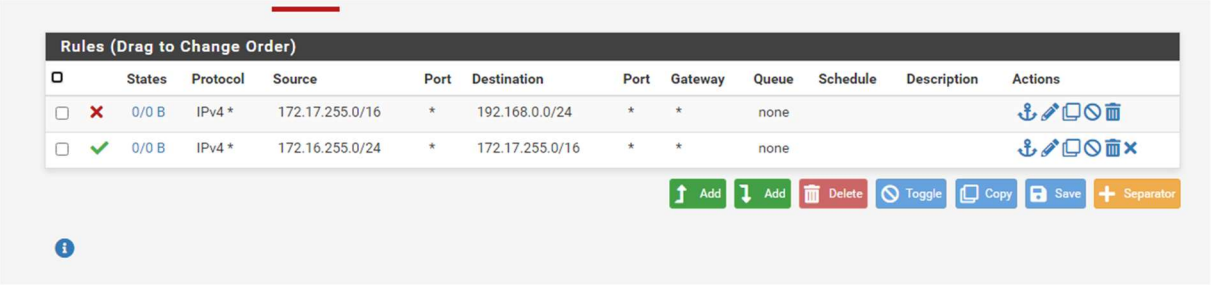
La première règle sert à autoriser le WAN à communiquer avec la LAN.
La deuxième sert à autoriser la communication entre la Wan et la DMZ.
La troisième sert à autoriser les communications du entre WAN.
La dernière sert à autoriser le flux VPN.

LAN :



La deuxième réglé sert à autoriser la connexion entre le Lan et le WAN.
La troisième sert à autoriser la communication en sens inverse du Wan au LAN.

DMZ :



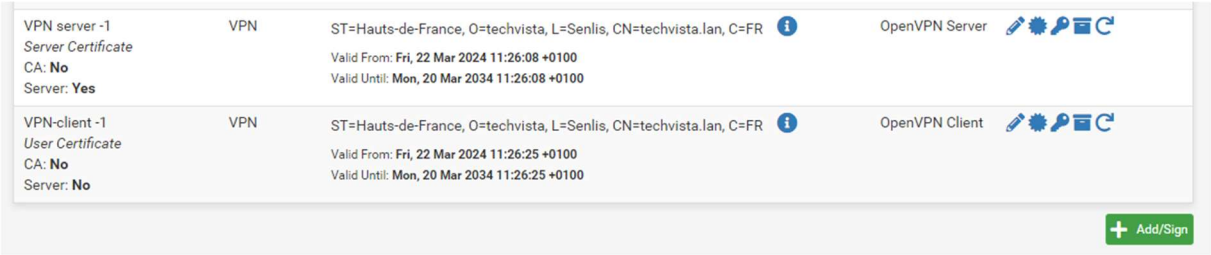
La première règle permet d'interdire la communication entre la DMZ et la LAN.
La deuxième règle permet d'autoriser la communication entre le WAN et la DMZ.

Toutes c'est règles sont utiles à notre réseau.

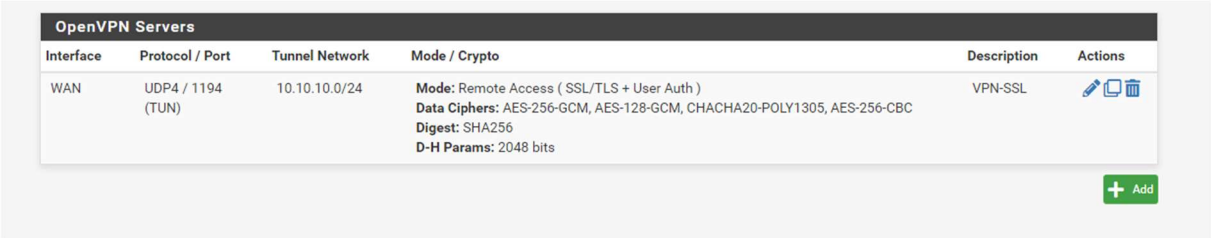
Mise en place du VPN

Les VPN servent à transmettre des données de manière sûre et anonyme sur des réseaux publics.
Le VPN créer un tunnel sécurisé d'un point A à un Point B.

Pour l'installation du VPN nous devons créer 2 certificats 1 pour le serveur et 1 pour le user.

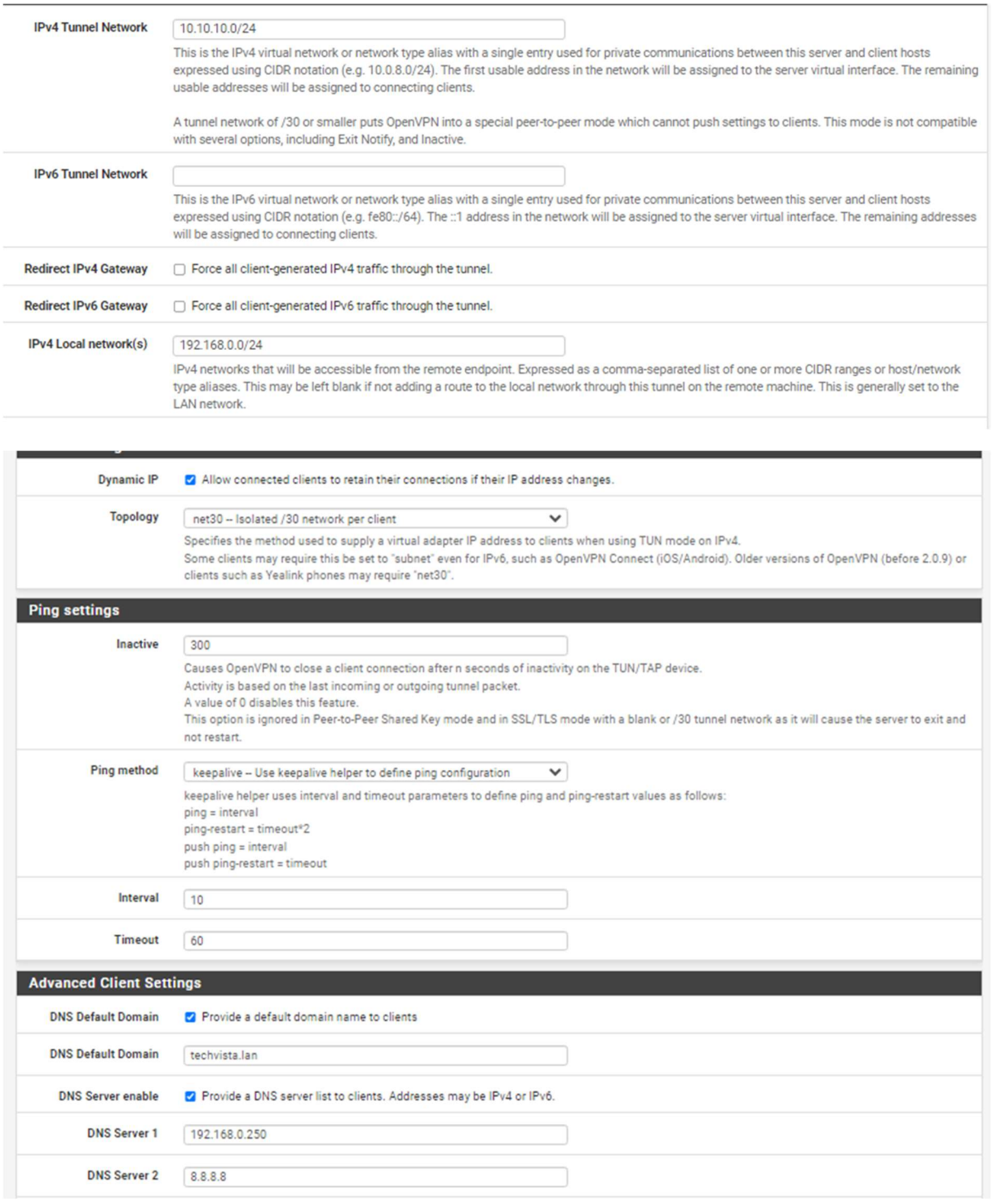


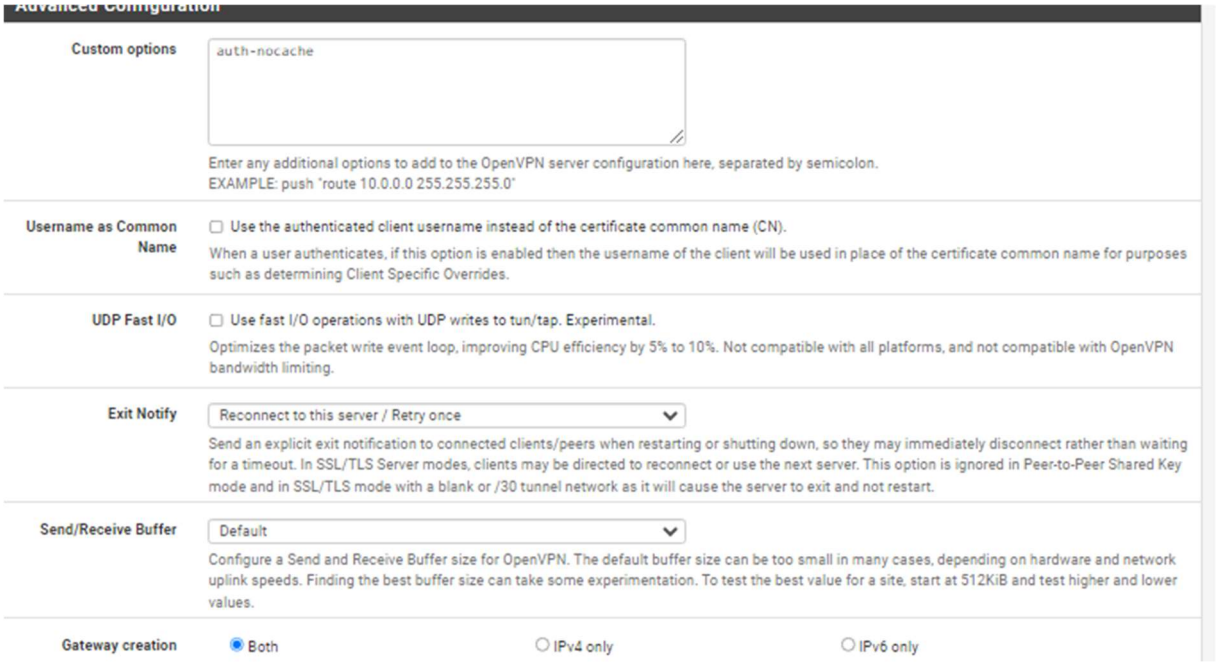
Une fois faits-nous allons dans VPN → OPENVPN –> Servers pour configurer l'accès VPN.



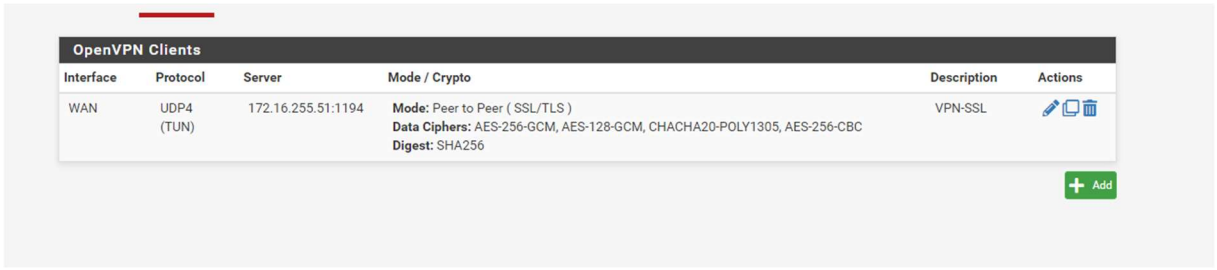
Ensuite il faudra remplir les cases comme en-dessous, attention il ne faut pas se tromper entre le certificat serveur et utilisateurs.

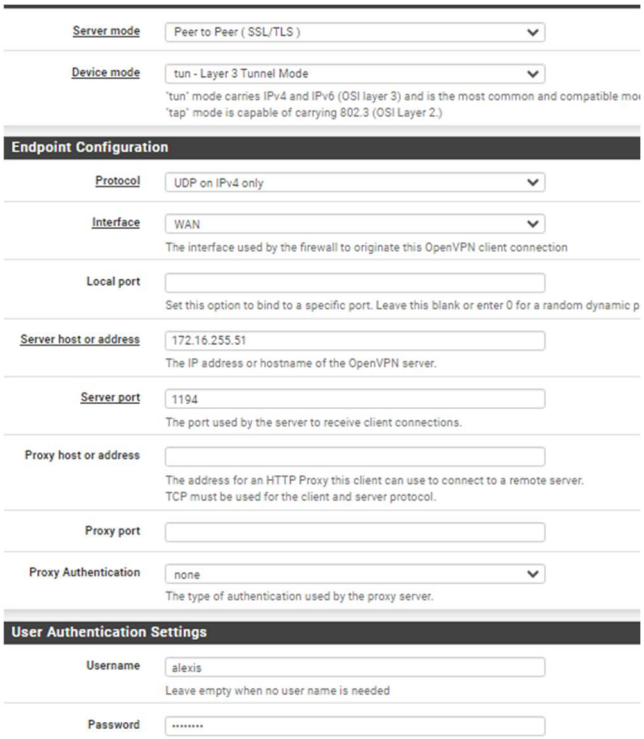

Mode Configuration
Server mode
Remote Access (SSL/TLS + User Auth)
Backend for authentication
LDAP Active Directory
Local Database
Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable 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-----
772799e4321c46bfe72f851dcd82ba3f
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
VPN
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
VPN server -1 (Server: Yes, CA: VPN, 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.

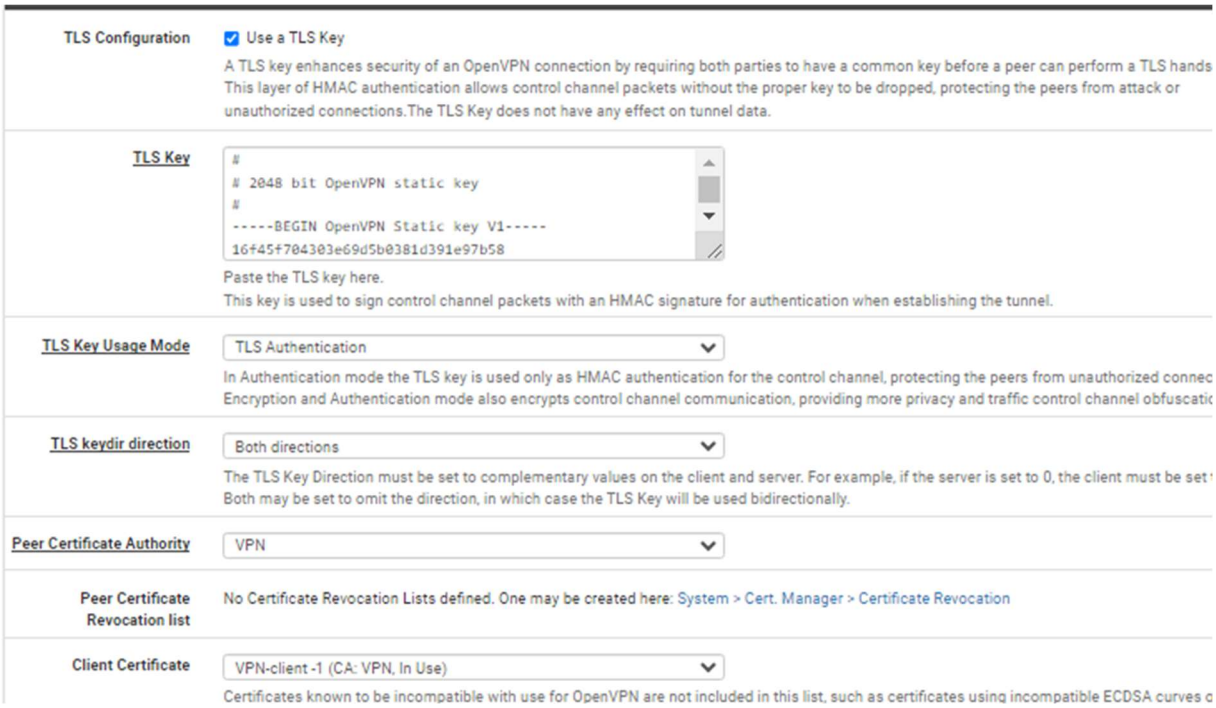

IPv4 Tunnel Network
10.10.10.0/24
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual 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)
192.168.0.0/24
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.
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
techvista.lan
DNS Server enable
Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1
192.168.0.250
DNS Server 2
8.8.8.8

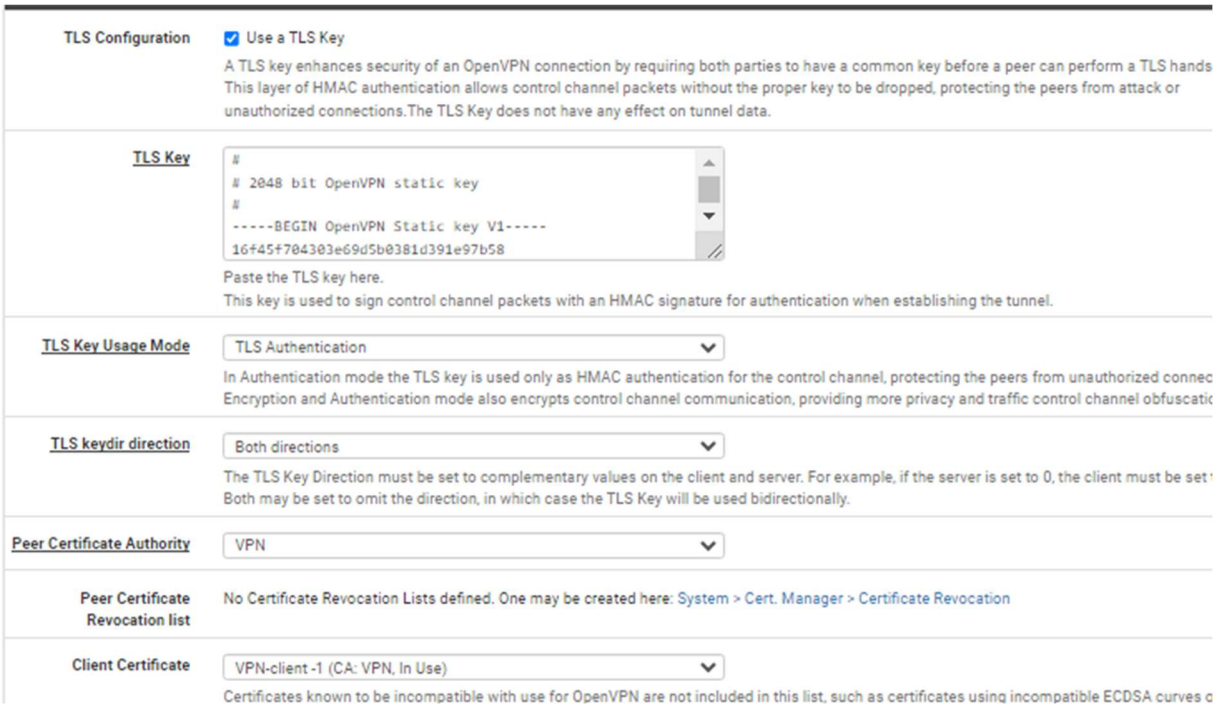

Advanced Configuration
Custom options
auth-nocache
Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"
Username as Common Name
Use the authenticated client username instead of the certificate common name (CN).
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

User :


OpenVPN Clients
Interface
Protocol
Server
Mode / Crypto
Description
Actions
WAN
UDP4 (TUN)
172.16.255.51:1194
Mode: Peer to Peer (SSL/TLS)
Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC
Digest: SHA256
VPN-SSL
Add

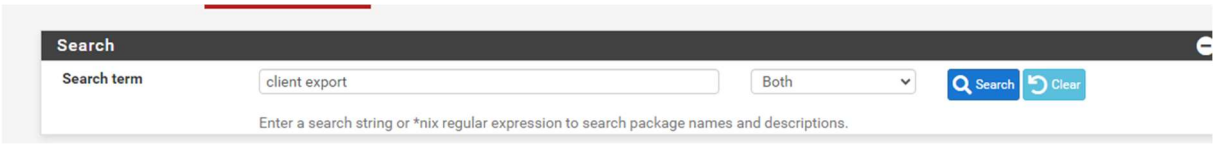

Server mode
Peer to Peer (SSL/TLS)
Device mode
tun - Layer 3 Tunnel Mode
'tun' mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mo
'tap' mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration
Protocol
UDP on IPv4 only
Interface
WAN
The interface used by the firewall to originate this OpenVPN client connection
Local port
Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic p
Server host or address
172.16.255.51
The IP address or hostname of the OpenVPN server.
Server port
1194
The port used by the server to receive client connections.
Proxy host or address
The address for an HTTP Proxy this client can use to connect to a remote server.
TCP must be used for the client and server protocol.
Proxy port
Proxy Authentication
none
The type of authentication used by the proxy server.
User Authentication Settings
Username
alexis
Leave empty when no user name is needed
Password



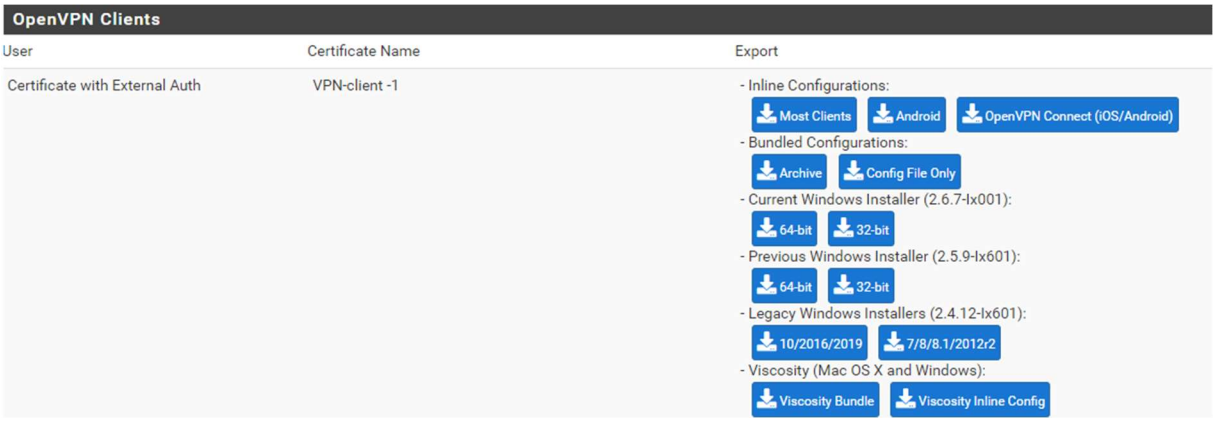


Ensuite nous allons dans Firewall → Rules →Wan puis on rentre cette règle.
Elle permet d'autoriser le flux VPN

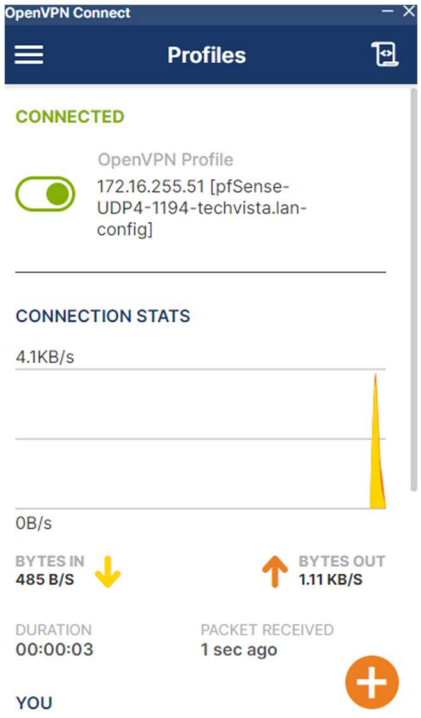
On installe client export pour exporter la configuration VPN.



On clique sur **Archive et Config File Only.**



On importe les fichiers OpenVPN puis on se connecte avec l'utilisateurs LDAP.



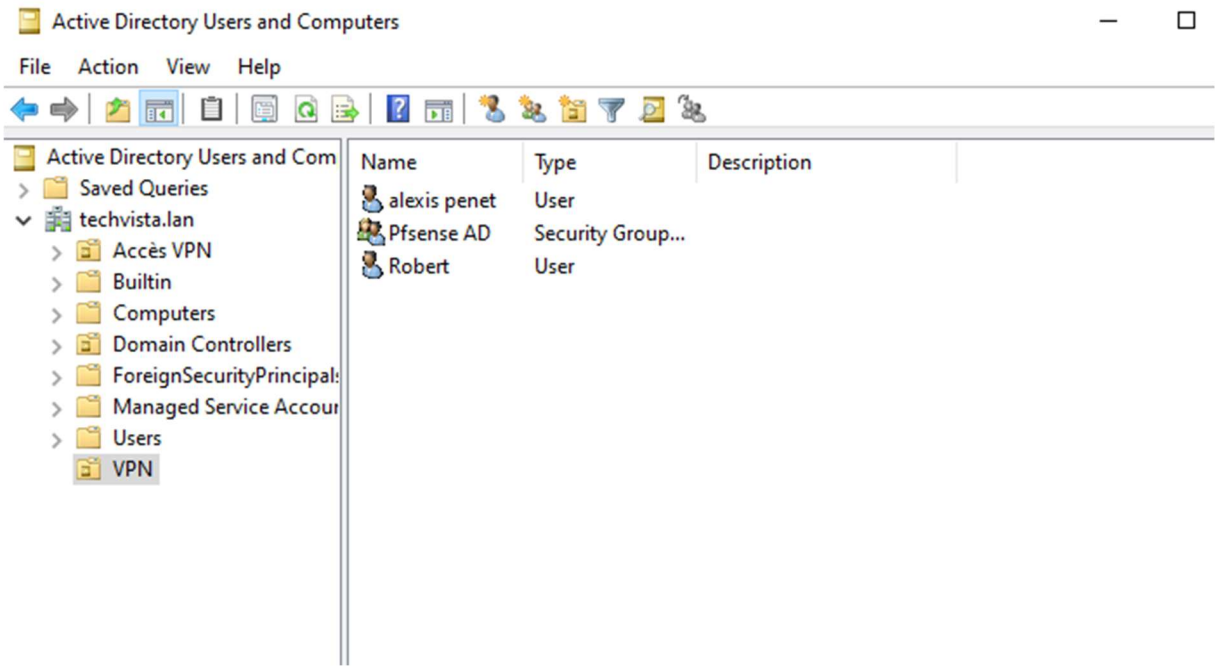
Connexion LDAP

Le LDAP est un protocole d'authentification pour les services d'annuaire. Ils stockent des informations telles que :

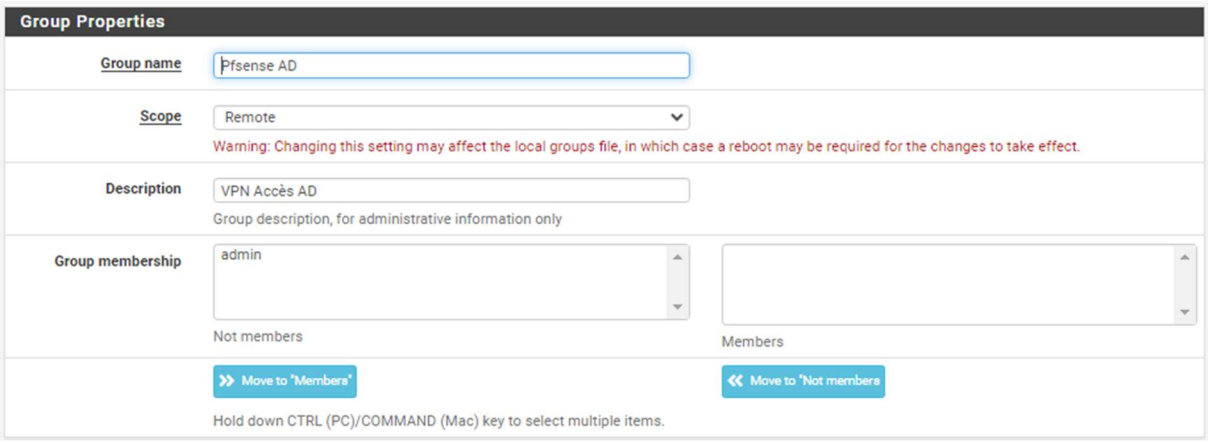
- Les utilisateurs
- Les caractéristiques de ces utilisateurs
- Le privilège d'appartenance à un groupe
- Et plus encore ...

Nous allons voir comment le mettre en place sur PFSense.

Pour commencer nous allons a créer un OU et un groupe d'utilisateurs. On mets les droits administrateurs à l'utilisateurs Alexis PENET.



Ensuite nous allons dans le PFSense dans système → User Manager puis on clique sur ADD pour créer un groupe. (Il faut qu'il soit écrit de la même manière)



Une fois fait on ajoute tous les droits captive portal et on ajoute All Pages.

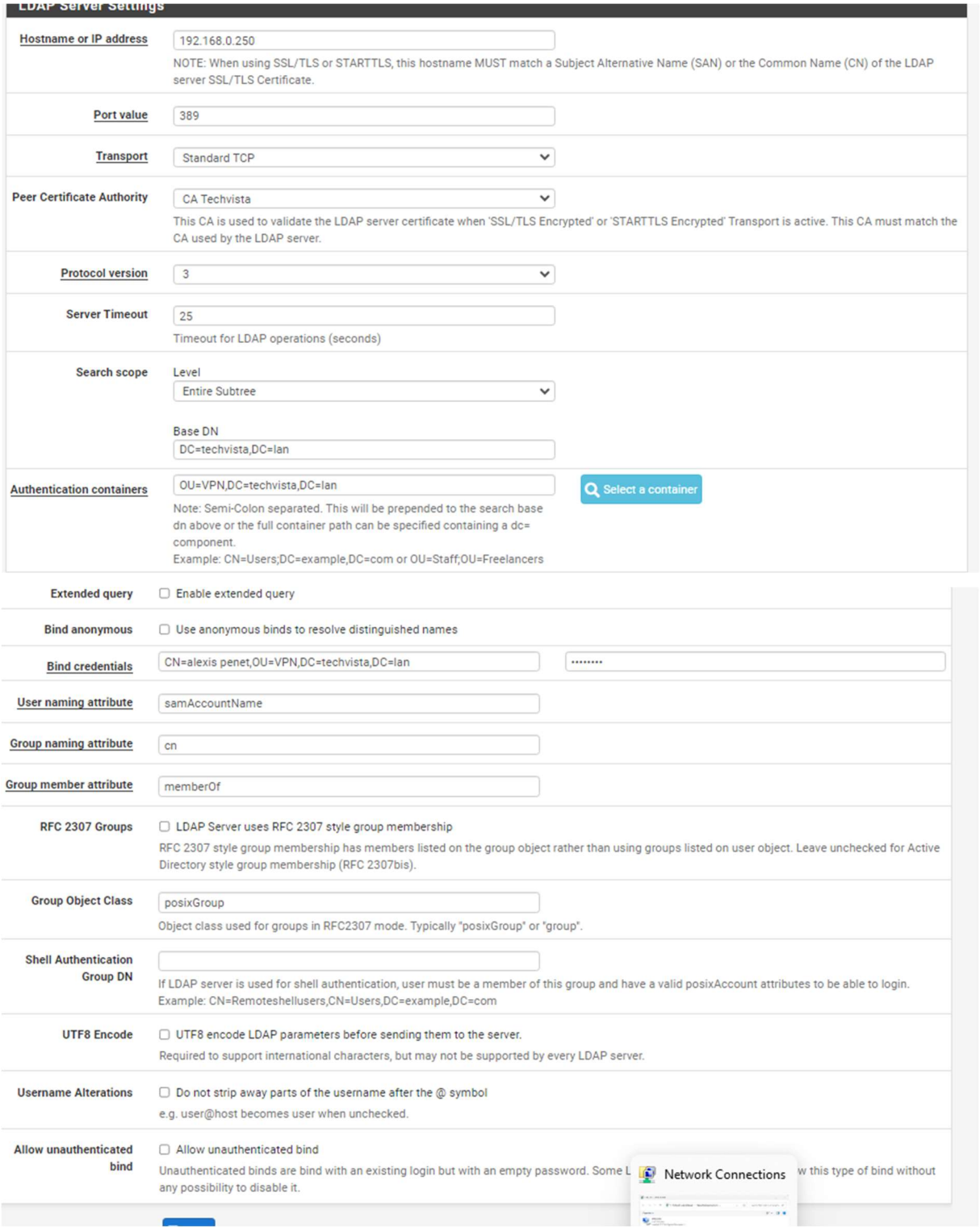
WebCfg - Services: Captive Portal: Allowed IPs	Allow access to the 'Services: Captive Portal: Allowed IPs' page.
WebCfg - Services: Captive Portal: Edit Allowed Hostnames	Allow access to the 'Services: Captive Portal: Edit Allowed Hostnames' page.
WebCfg - Services: Captive Portal: Edit Allowed IPs	Allow access to the 'Services: Captive Portal: Edit Allowed IPs' page.
WebCfg - Services: Captive Portal: Edit MAC Addresses	Allow access to the 'Services: Captive Portal: Edit MAC Addresses' page.
WebCfg - Services: Captive Portal: Edit Zones	Allow access to the 'Services: Captive Portal: Edit Zones' page.
WebCfg - Services: Captive Portal: File Manager	Allow access to the 'Services: Captive Portal: File Manager' page.
WebCfg - Services: Captive Portal: Mac Addresses	Allow access to the 'Services: Captive Portal: Mac Addresses' page.
WebCfg - Status: Captive Portal	Allow access to the 'Status: Captive Portal' page.
WebCfg - Status: Captive Portal Voucher Rolls	Allow access to the 'Status: Captive Portal Voucher Rolls' page.
WebCfg - Status: Captive Portal Vouchers	Allow access to the 'Status: Captive Portal Vouchers' page.
WebCfg - Status: Captive Portal: Expire Vouchers	Allow access to the 'Status: Captive Portal: Expire Vouchers' page.
WebCfg - Status: Captive Portal: Test Vouchers	Allow access to the 'Status: Captive Portal: Test Vouchers' page.
WebCfg - System: User Manager: Add Privileges	Allow access to the 'System: User Manager: Add Privileges' page. (admin privilege)
WebCfg - All pages	Allow access to all pages (admin privilege)
Security notice: Users in this group effectively have administrator-level access	

+ Add

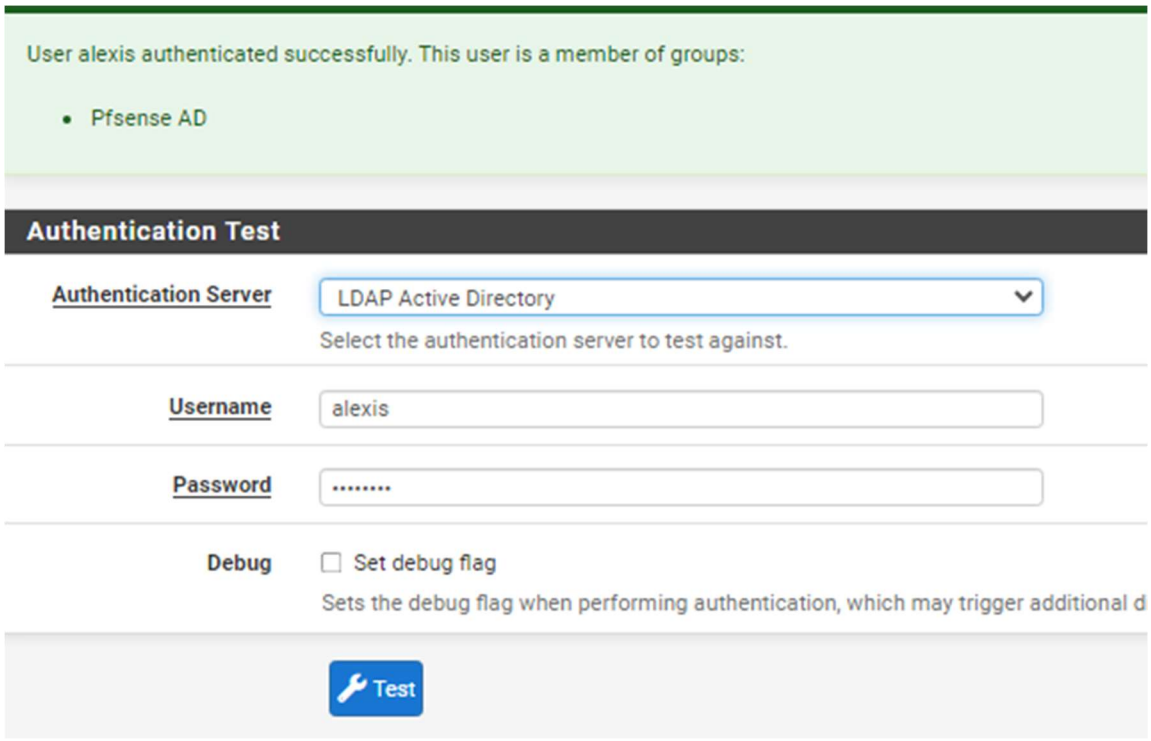
Après on vas dans authentification servers puis on configure le LDAP sur PFSsense.

Pour récupérer le distingued name pour la base DN, l'ou et l'utilisateurs il

suffit d’afficher les details puis on regarde les paramètres dans éditeurs d’attributs.



Ensuite on tente une connexion on va dans diagnostics → Authentification puis on fais le test.



On voit que c’est fonctionnel on peut donc se connecter avec un utilisateur de l’AD sur Pfsense.

Installation Crowdsec

Crowdsec sert à bloquer les adresses IP malveillantes, notamment à l'origine d'attaques brute force, de scans de port et de recherche de vulnérabilités web (HTTP).

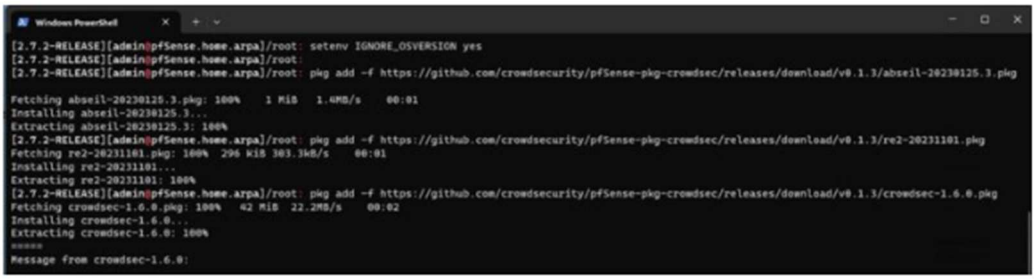
Nous allons voir comment le mettre en place.

Dans la console, saisissez cette commande :

```
setenv IGNORE_OSVERSION yes
```

Puis exécutez les commandes suivantes pour télécharger et installer les paquets :

```
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
```



L'installation de CrowdSec est effectuée à l'emplacement suivant :

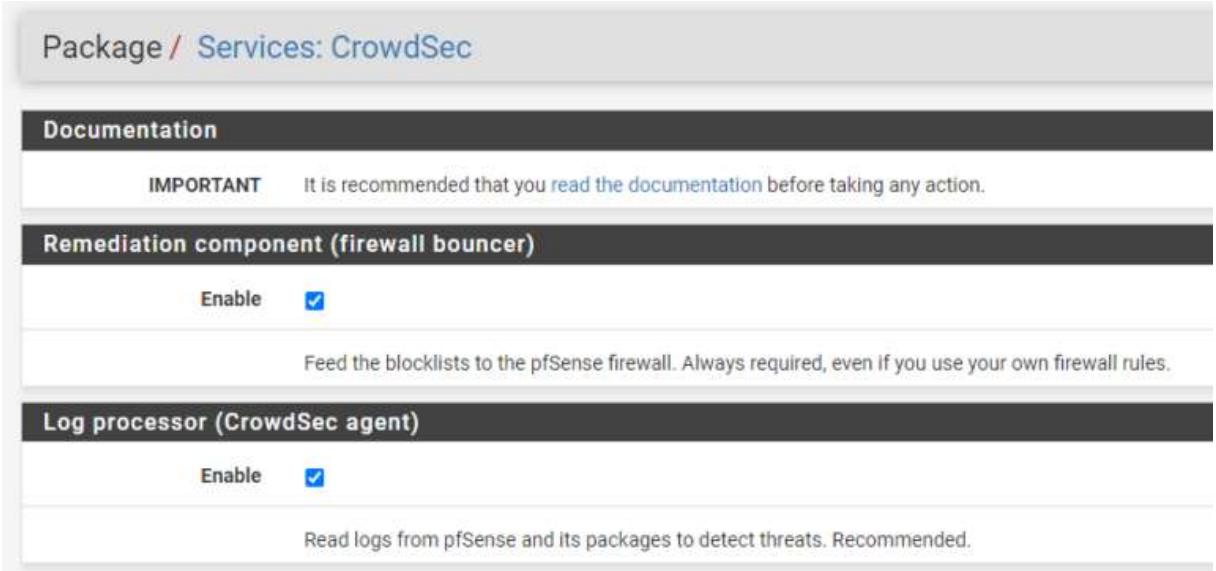
```
/usr/local/etc/crowdsec/
```

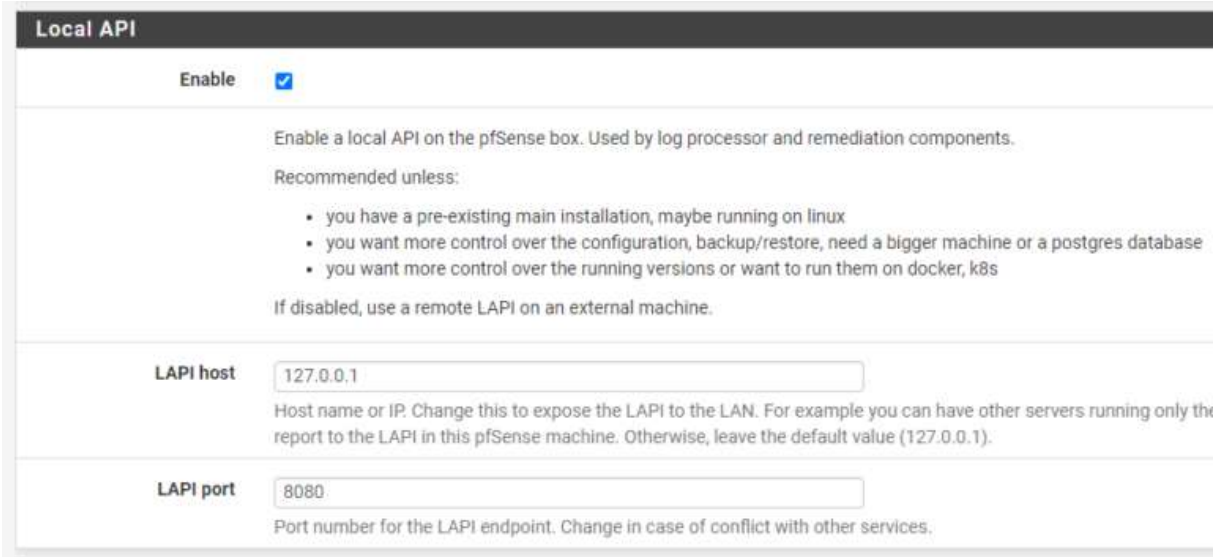
Par la suite, si vous avez besoin de redémarrer CrowdSec, utilisez cette commande (adaptez également pour l'arrêter / le démarrer) :

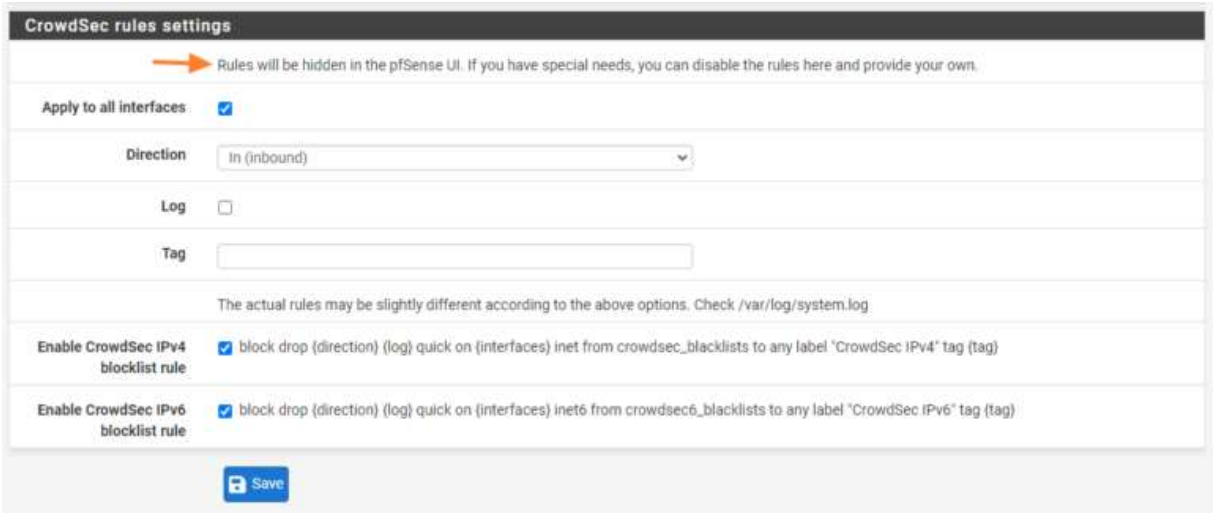
```
service crowdsec.sh restart
```

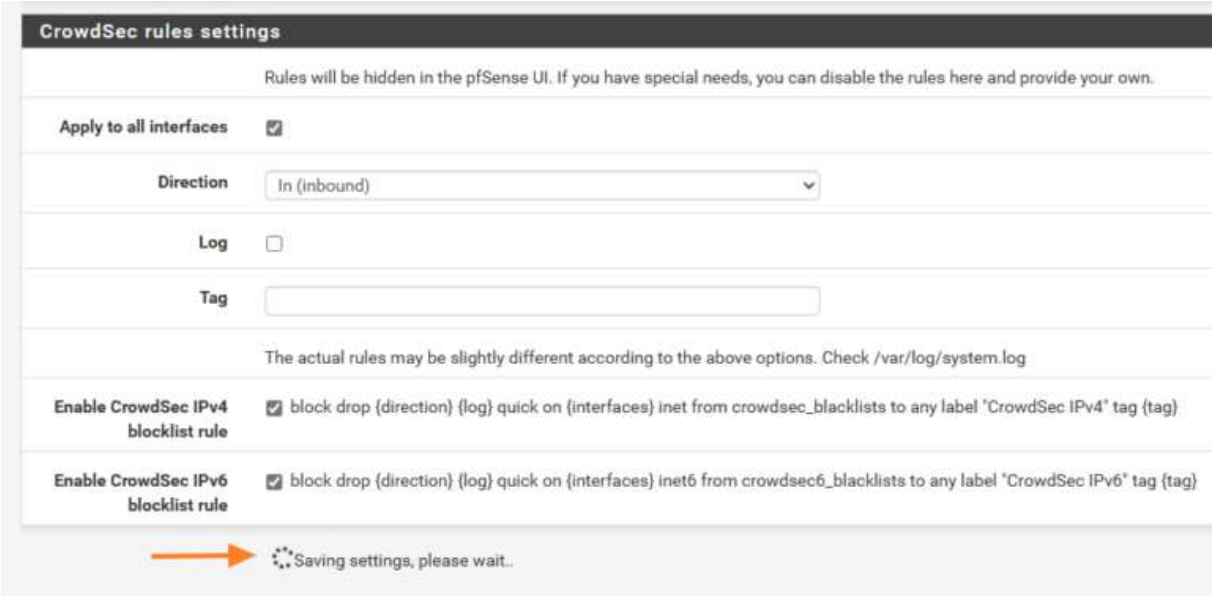
Une fois faits-nous allons dans service → Crowdsec.

On coche toutes les cases ci-dessous pour que crowdsec soit actif est opérationnel.


Package / Services: CrowdSec
Documentation
IMPORTANT
It is recommended that you read the documentation before taking any action.
Remediation component (firewall bouncer)
Enable
Feed the blocklists to the pfSense firewall. Always required, even if you use your own firewall rules.
Log processor (CrowdSec agent)
Enable
Read logs from pfSense and its packages to detect threats. Recommended.


Local API
Enable
Enable a local API on the pfSense box. Used by log processor and remediation components.
Recommended unless:
you have a pre-existing main installation, maybe running on linux
you want more control over the configuration, backup/restore, need a bigger machine or a postgres database
you want more control over the running versions or want to run them on docker, k8s
If disabled, use a remote LAPI on an external machine.
LAPI host
127.0.0.1
Host name or IP. Change this to expose the LAPI to the LAN. For example you can have other servers running only the
report to the LAPI in this pfSense machine. Otherwise, leave the default value (127.0.0.1).
LAPI port
8080
Port number for the LAPI endpoint. Change in case of conflict with other services.


CrowdSec rules settings
Rules will be hidden in the pfSense UI. If you have special needs, you can disable the rules here and provide your own.
Apply to all interfaces
Direction
In (inbound)
Log
Tag
The actual rules may be slightly different according to the above options. Check /var/log/system.log
Enable CrowdSec IPv4 blocklist rule
block drop (direction) (log) quick on (interfaces) inet from crowdsec_blacklists to any label "CrowdSec IPv4" tag (tag)
Enable CrowdSec IPv6 blocklist rule
block drop (direction) (log) quick on (interfaces) inet6 from crowdsec6_blacklists to any label "CrowdSec IPv6" tag (tag)
Save



Cette fois le crowdsec est opérationnel est fonctionnel.

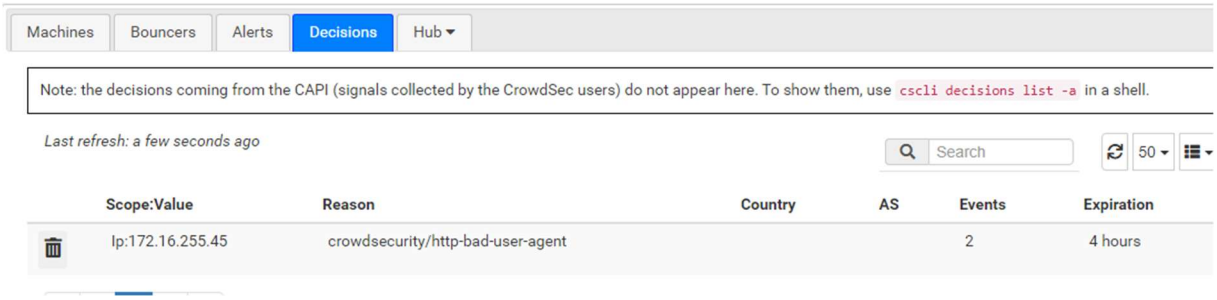
Attaque NMAP

NMAP (Network Mapper), il s'agit d'un des outils de découverte qui permet de fournir des informations sur les services et les systèmes d'exploitation qu'ils exécutent.

Nous allons voir comment le mettre en place.

On prend un Kali linux est on se mets sur le réseau WAN du PFSENSE.
On tape la commande ‘’sudo nmap 172.16.255.51 -Sv -v -Pn’’, ça permet de récupérer les ports.

Nous voyons que la commande est bien passé, maintenant nous devons voir si crowdsec à ban l’ip du Kali.
Pour ça nous allons dans → Status → Crowdsec Status.



Nous pouvons voir qu'à la suite de la commande le firewall a ban l'adresse ip du Kali linux.
Crowdsec est donc fonctionnel pour cette attaque.

Conclusion

Pour conclure, j'ai réalisé cette mission sous Vmare contenant Un pfsense avec WAN,LAN,DMZ, 1 Windows server (AD), 2 Windows 11, un Serveur Linux.
Ce réseau répondra au mieux aux besoins de l'entreprise TechVista.

L'entreprise d'un nouveau Pare-Feu sécurisé en HTTPS.
Des règles ont été fait pour sécuriser un maximum les différents réseaux, Squid est Crowdsec ont été installé , Une connexion LDAP a été configurés ainsi qu'un tunnel OPENVPN avec accès LAN et DMZ.

Ce nouveau site répondra aux mieux au besoin du réseau et à sa disponibilité.