VPN OPEN SSL

BTS – SIO 1 / SISR

Clément Paccard

29/01/2024

TABLE DES MATIERES

FIREWALL PFSENSE 1

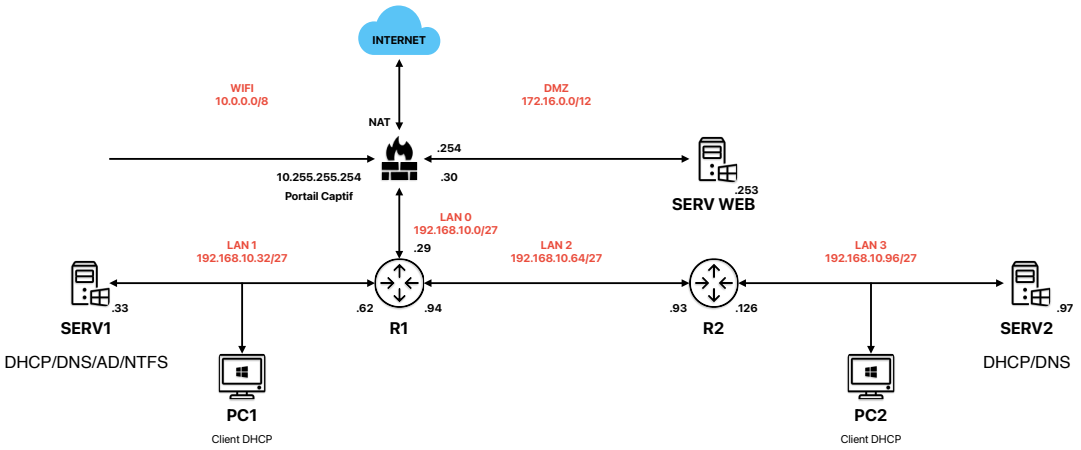
Introduction 1
1- Créer l'autorité de certification 2
2- Créer le certificat serveur 4
3- Configurer le serveur Open VPN 5
Conclusion 11

FIREWALL
PFSENSE

INTRODUCTION

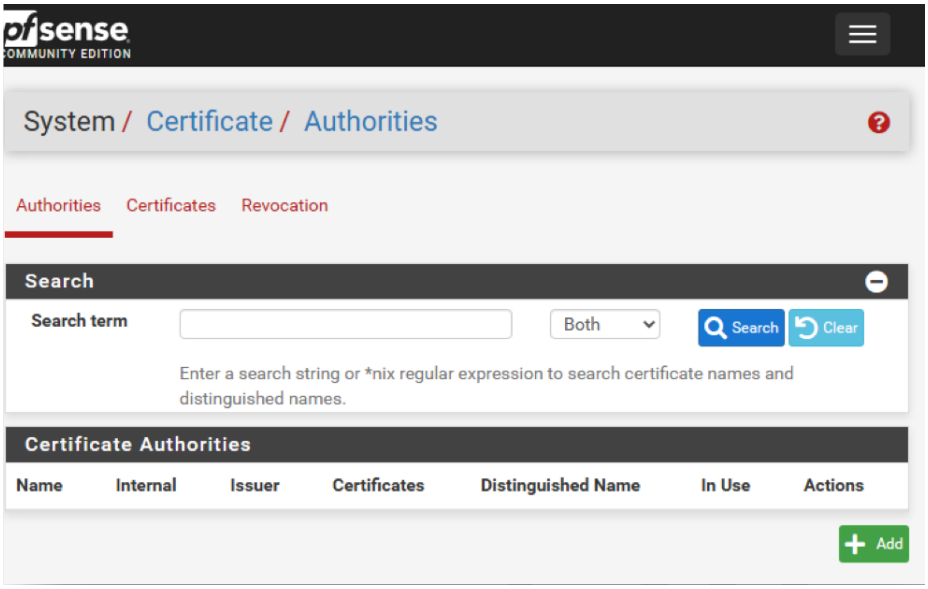
Cette procédure montre comment installer et paramétrer un VPN OPEN SSL sur un Pare-feu PFsense.

Un VPN SSL est un réseau privé virtuel créé à l'aide du protocole SSL (Secure Sockets Layer) pour établir une connexion sécurisée et chiffrée entre deux réseaux.

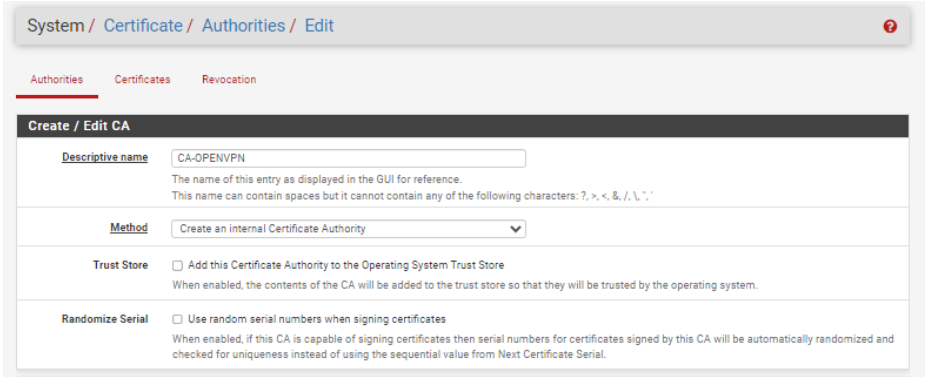


1-CRÉER L'AUTORITÉ DE CERTIFICATION

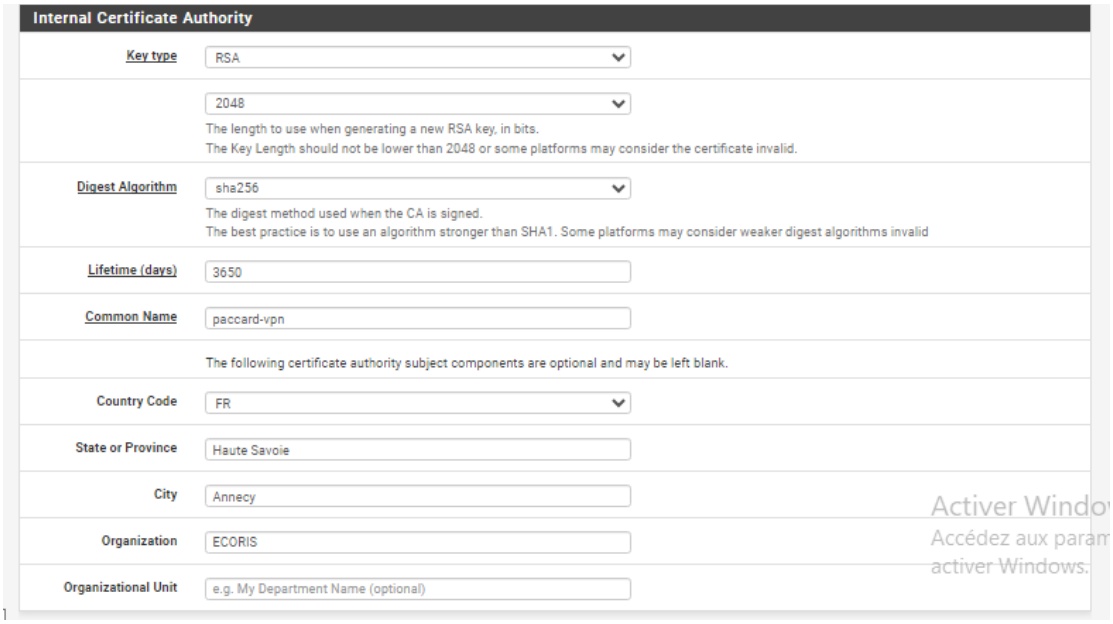
Pour ce faire allez dans System -> Certificate -> Authorities puis cliquez sur Add.



Ensuite on va nommer l'autorité (CA-OPENVPN)



Ensuite remplissez les informations pour votre entreprise :



2-CREER LE CERTIFICAT SERVEUR

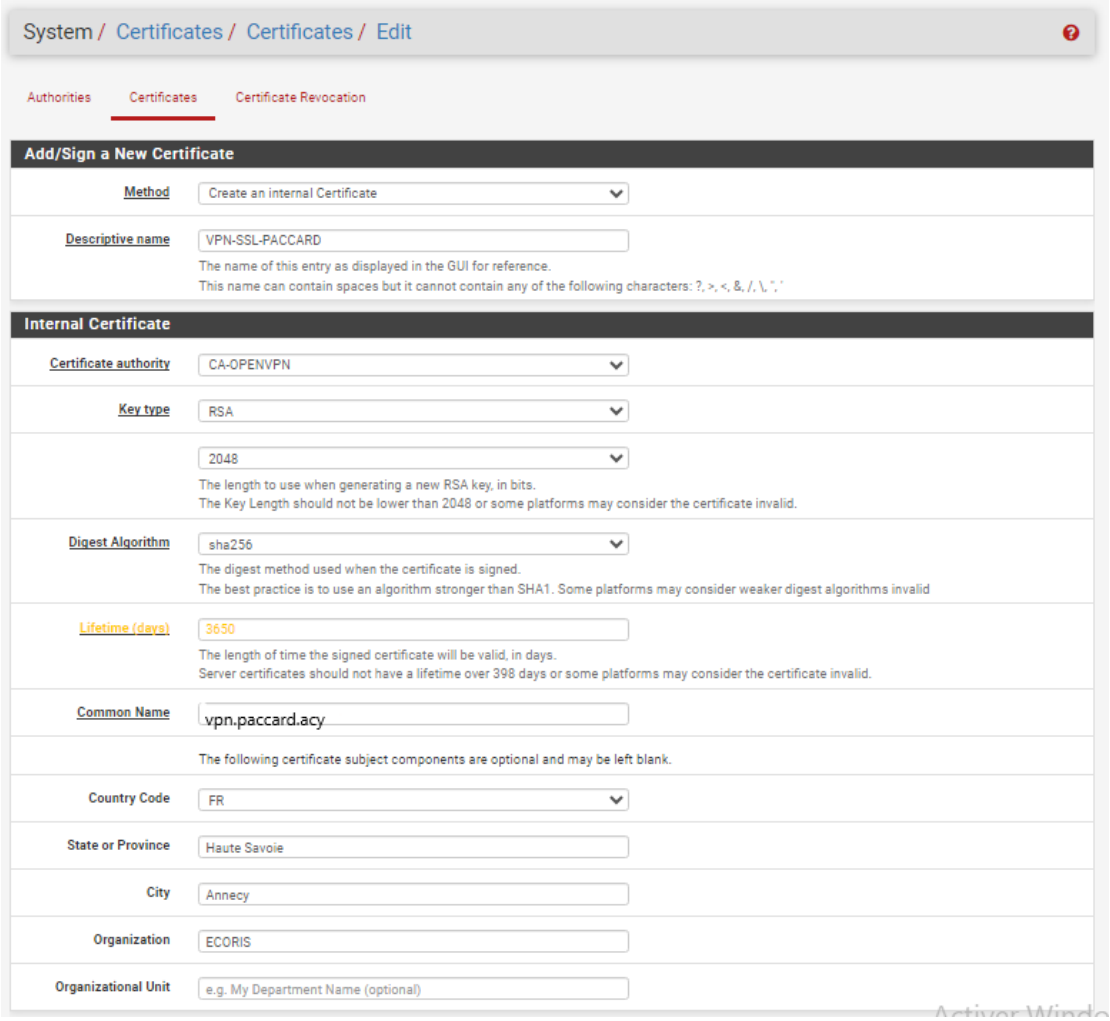
Maintenant nous allons créer le certificat du serveur.

System -> Certificate -> Certificates et cliquez sur le bouton Add/Sign

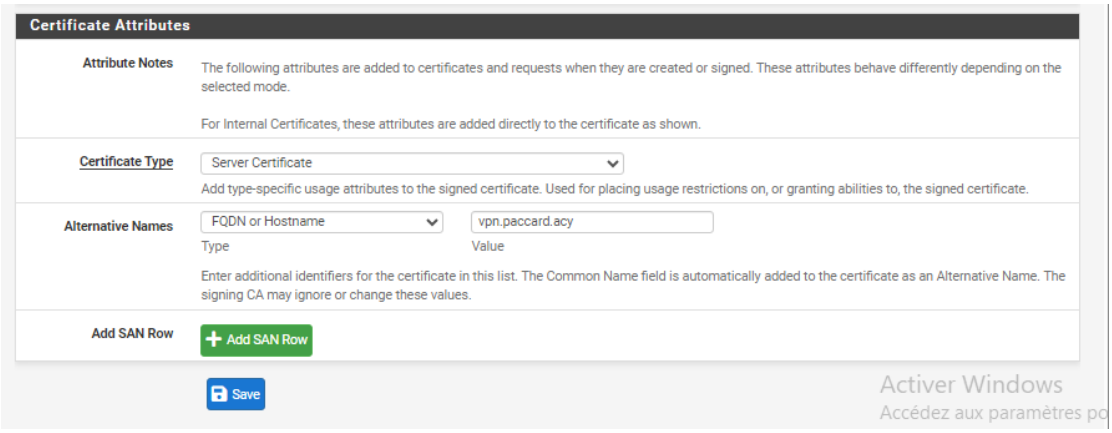
Choisissez ensuite Create an internal Certificate, on peut lui ajouter une description.

Ensuite choisissez l'autorité de certification (on choisit celle créé précédemment)

Ajoutez un nom puis remplissez les informations pour votre entreprise.



Enfin, sélectionnez Server Certificate pour le type de certificat.

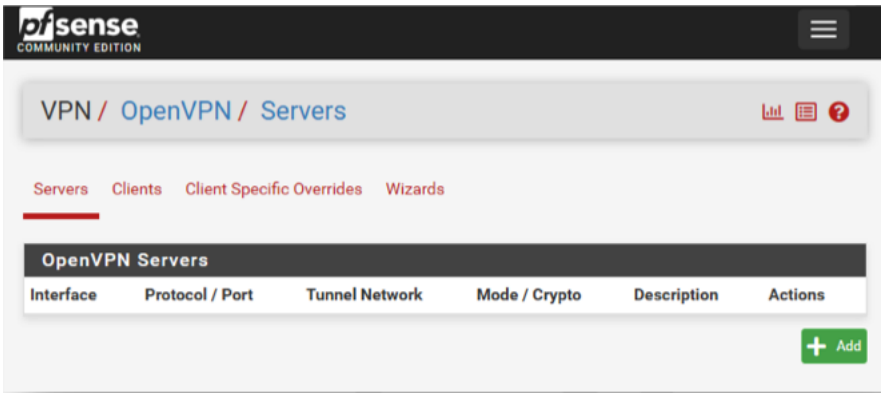


Validez avec Save, voilà le certificat apparaît maintenant dans la liste des certificats du Pare-Feu.

3-CONFIGURER LE SERVEUR OPEN VPN

On va maintenant configurer le VPN en lui-même. Pour ce faire allez dans le menu VPN -> OpenVPN

Dans l'onglet Server cliquez sur Add.



Ensuite il faut sélectionner le "Server Mode" suivant : Remote Access (SSL/TLS + User Auth).

On laisse bien l'interface WAN sélectionné et les paramètres suivants :


VPN / OpenVPN / Servers / Edit
Servers
Clients
Client Specific Overrides
Wizards
General Information
Description
VPN-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.
Mode Configuration
Server mode
Remote Access (SSL/TLS + User Auth)
Backend for authentication
Liaison LDAP
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.
Automatically generate a TLS Key.
Peer Certificate Authority
CA-OPENVPN
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-SSL-PACCARD (Server: Yes, CA: CA-OPENVPN)
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.
Activer Wind
Accédez aux par
activer Windows.

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

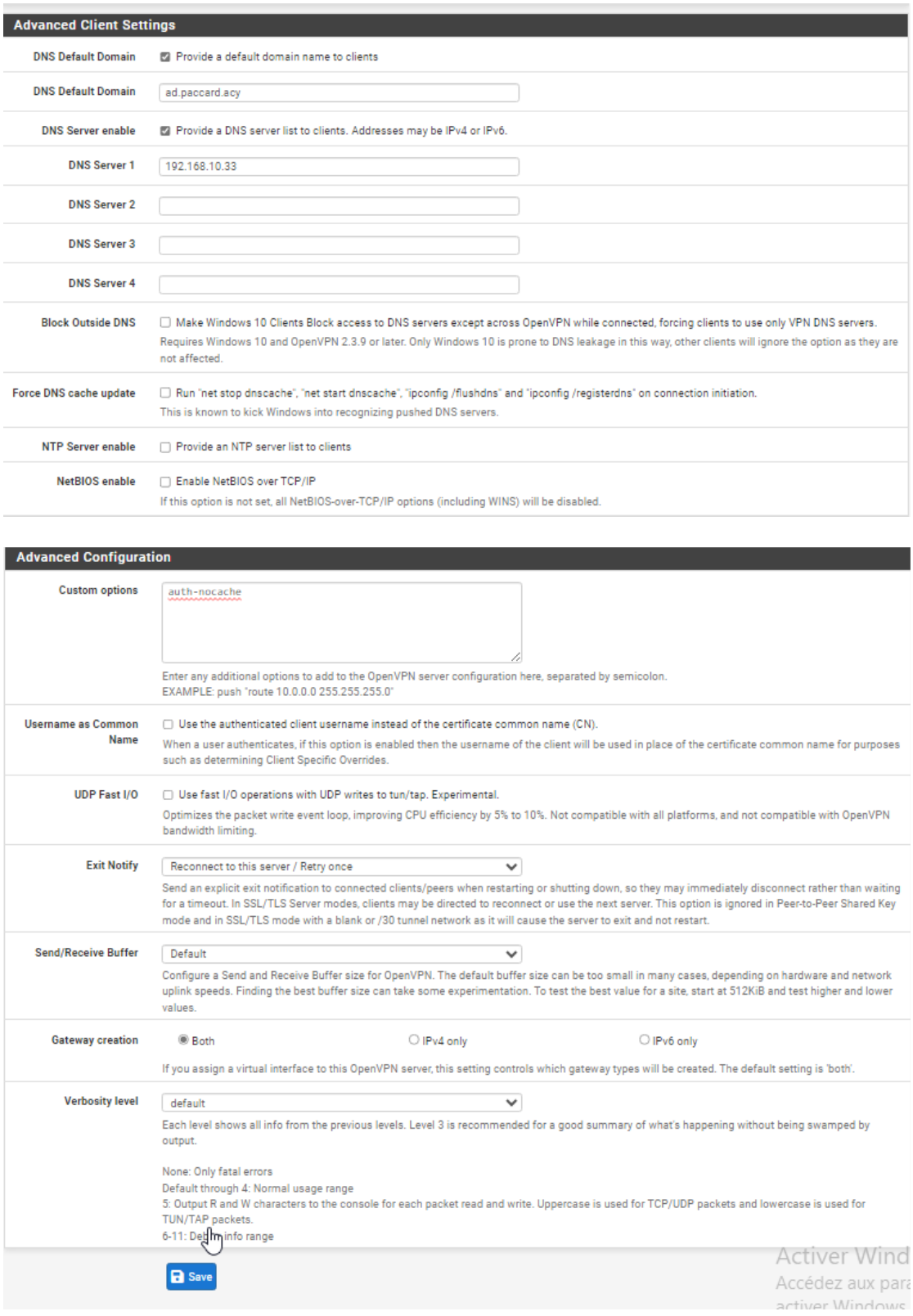
IPv4 Tunnel Network	10.10.10.0/29 This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual 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)	192.168.10.0/24 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.
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	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.

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



Il ne reste qu’à valider avec Save et voilà.

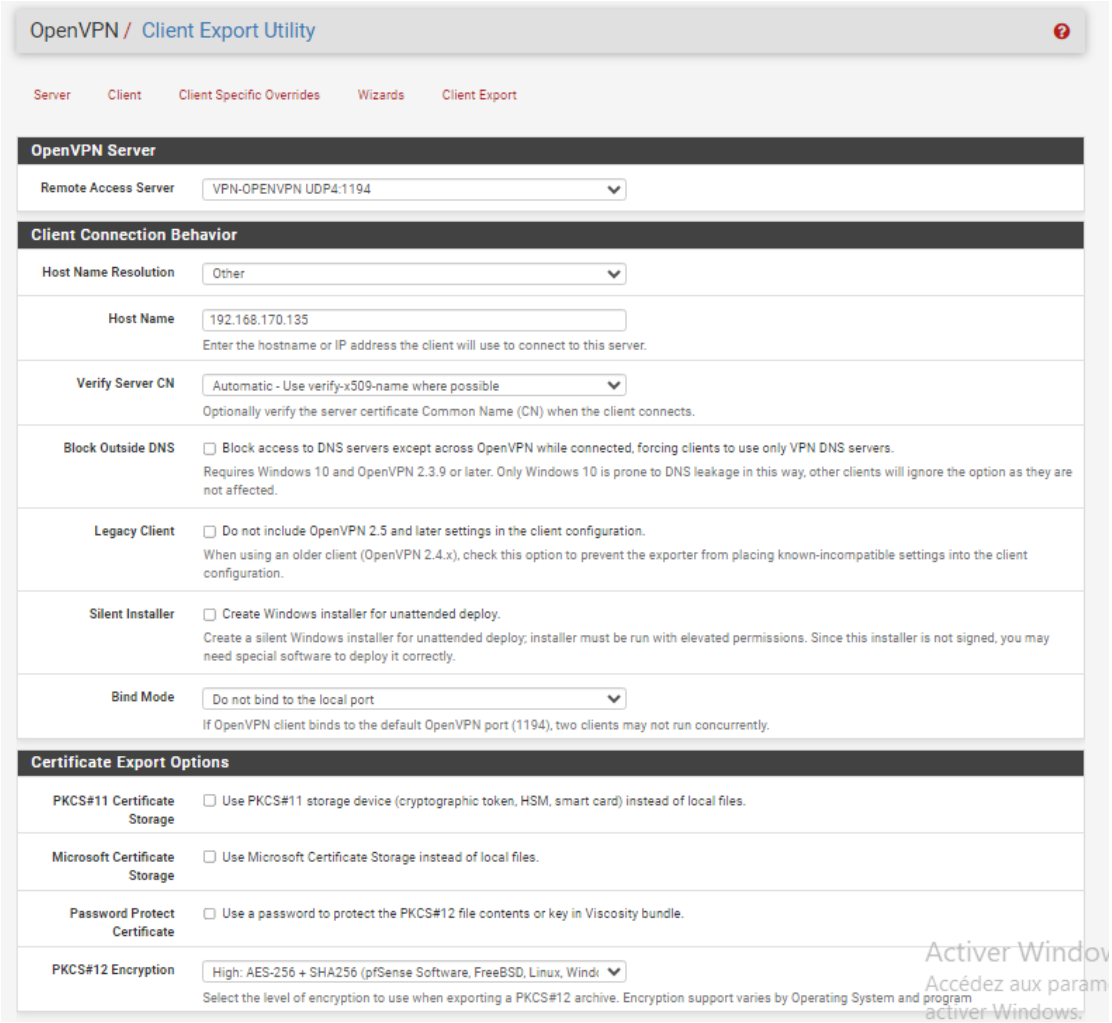
Pour télécharger la configuration au format .ovpn, il est nécessaire d'installer un paquet supplémentaire sur le pare-feu.

Rendez-vous dans le menu suivant :

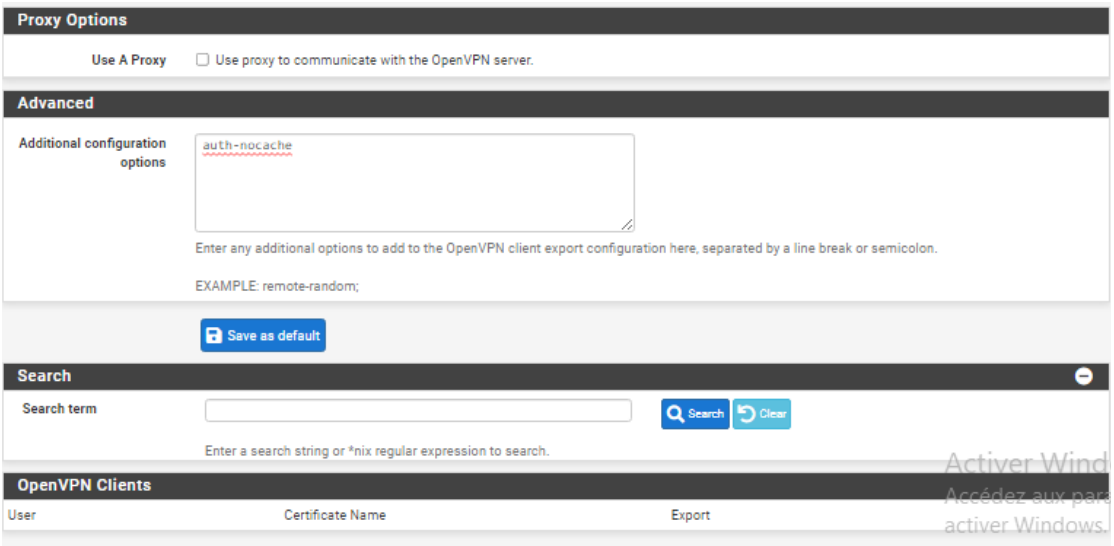
System -> Package Manager -> Available Packages.

Recherchez "openvpn" et installez le paquet : openvpn-client-export. Lorsque c'est fait, retournez dans le menu OpenVPN puis dans l'onglet "Client Export".

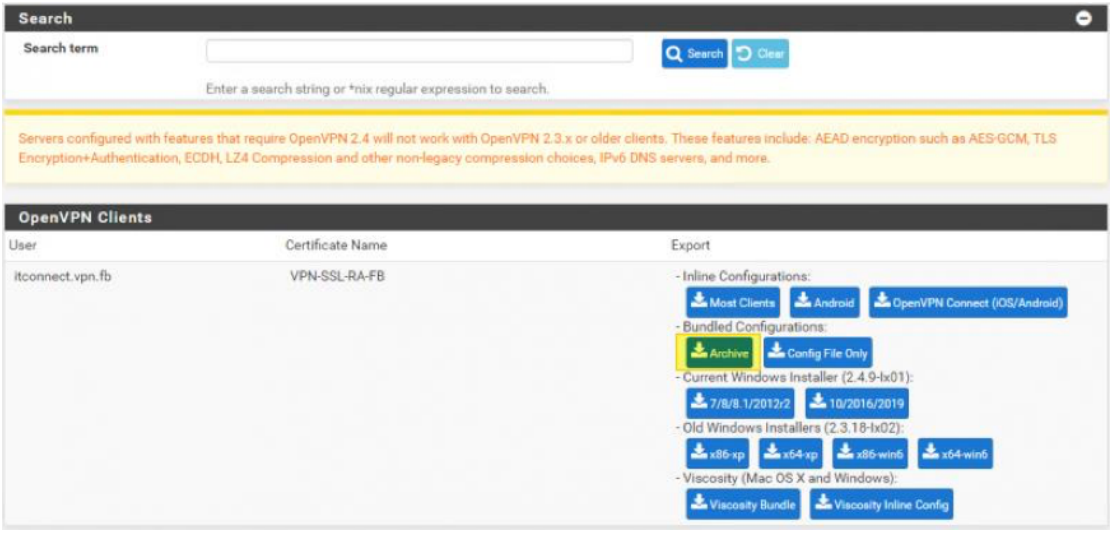
Si vous souhaitez utiliser l'adresse IP publique pour vous connecter, utilisez l'option "Interface IP Address" pour l'option "Host Name Resolution". Il y a d'autres options possibles, notamment par nom de domaine.



Les autres options peuvent être laissées par défaut... Il y a seulement notre option "auth-nocache" à reporter dans la section des options additionnelles.



Enfin dans les packages ont peu du coup télécharger le client pour les postes distants.



CONCLUSION

Voilà les utilisateurs peuvent maintenant se connecter avec leur compte Active Directory au VPN via une connexion internet et ainsi accéder aux ressources de l'entreprise.

Voici donc maintenant le schéma de l'infrastructure :