OPNsense - Configuration OpenVPN

> ***DISCLAIMER : Cette page est en cours de rédaction et son contenu peut être faux ou inexact. Merci de lire cette page avec toutes les précautions nécessaires.***

Difficulté : Intermédiaire

Notions : pare-feu, OPNsense, VPN, OpenVPN

I. Introduction

Dans le contexte du télétravail ou du travail des utilisateurs nomades, il est nécessaire de pouvoir assurer la confidentialité des échanges entre les utilisateurs et l'entreprise.

Pour cela, il faut mettre en place un VPN point-à-point.

C'est l'une des fonctionnalité d'OpenVPN. Celui-ci est présent par défaut dans les OPNsense.

OpenVPN peut être configuré de deux façons :

- Point à point (pour les clients)

- Site à site (pour relier les différents sites de l'entreprise entre eux)

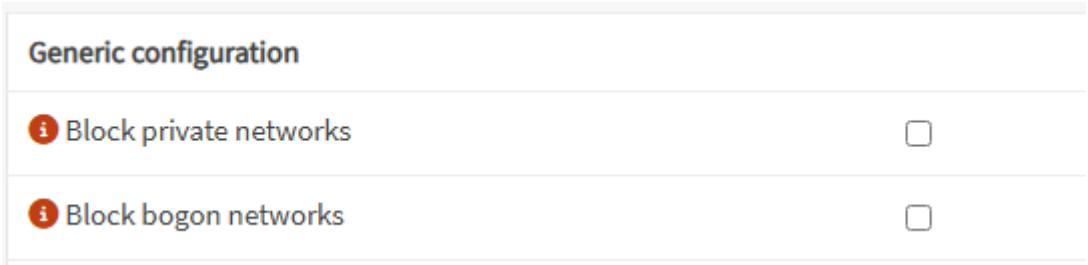
Cette procédure traitera de la mise en oeuvre d'OpenVPN pour le poit-à-point.

II. Prérequis

Dans le cadre d'une démonstration sur le réseau local.

Si il s'agit d'une installation de démonstration de principe, l'interface WAN est dans un réseau Local et le client sur ce même réseau.

Il faut donc désactiver les deux options suivantes dans les paramètres de l'interface WAN :

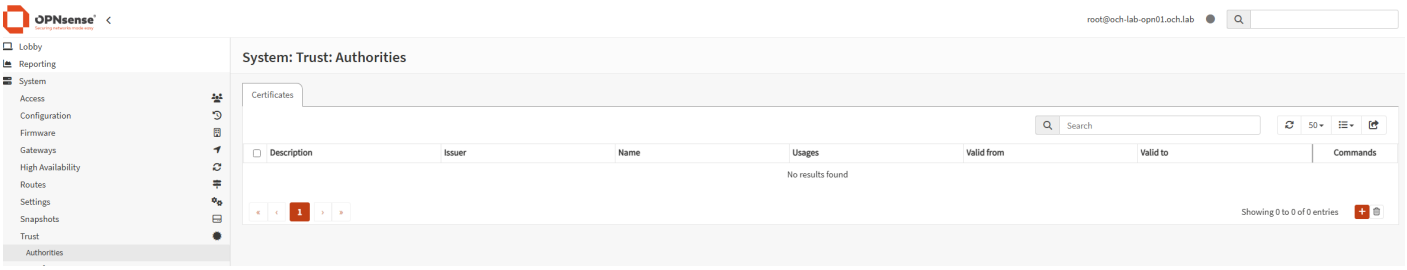


2.1 Initialisation de la CA

Pour plus de sécurité, il est préférable que le serveur et les clients puissent s'authentifier entre eux afin de garantir l'identité du pair.

Il faut pour cela initialiser une autorité de certification.

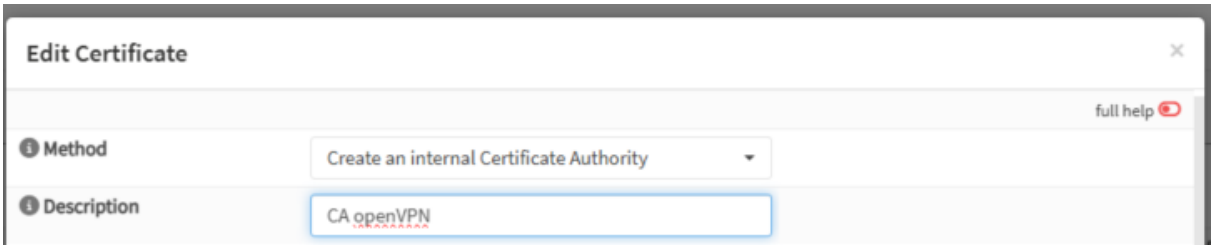
Aller dans '***System --> Trust --> Authorities***'



Cliquer sur le '**+**' pour créer une nouvelle CA.

Laisser la méthode par défaut '***Create an internal Certificate Authority***'.

Fournir une description parlante.



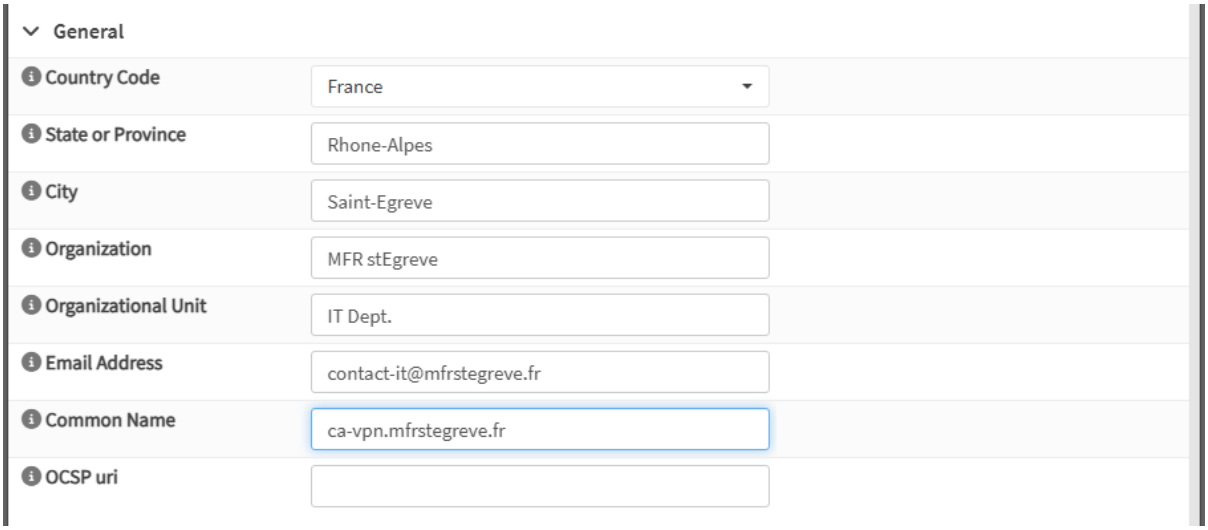
Passer le '***Key type***' à '***RSA-4096***'

Passer le '***Digest Algorithm***' à '***SHA512***'.

Laisser l'issuer à '***Self Signed***' si pas d'autorité au dessus pour signer la CA.

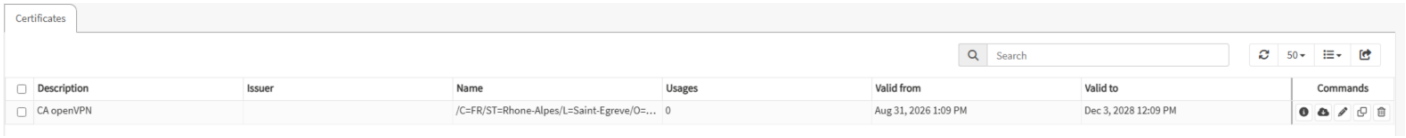
Choisir la durée de vie du certificat. Par défaut, elle est de 825 jours (soit 2 ans et 3 mois)

Remplir les détails du certificat.



Laisser le reste vide, puis faire '***Save***'.

La CA est désormais créée.

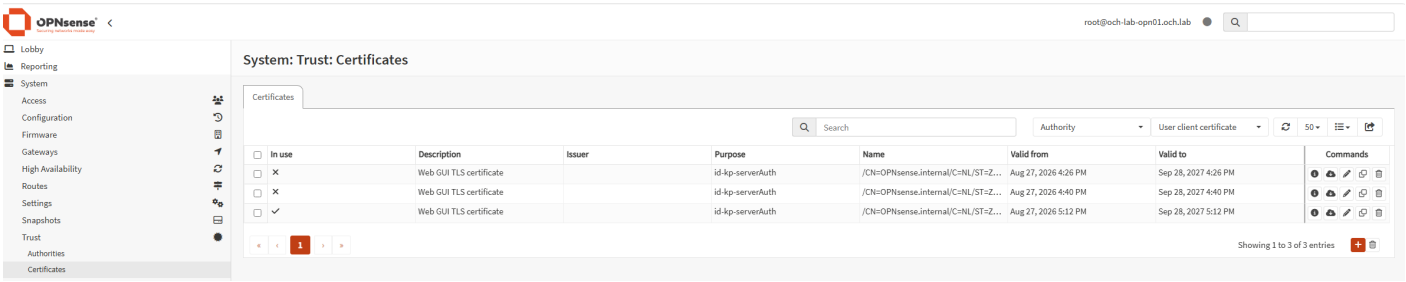


> **Info** : La CRL (Certificate Revocation List) a été créée en même temps que la CA. Pas besoin de la créer manuellement.

2.2 Générer le certificat du serveur

Afin que les clients puissent authentifier le serveur, il faut lui générer son certificat.

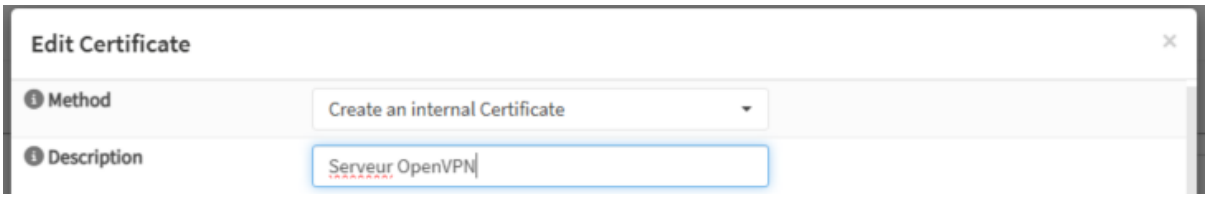
Pour cela, aller dans '***Trust --> Certificates***'.



Puis faire '**+**' pour créer un certificat.

Laisser la méthode '***Create an internal certificate***'.

Entrer la description.



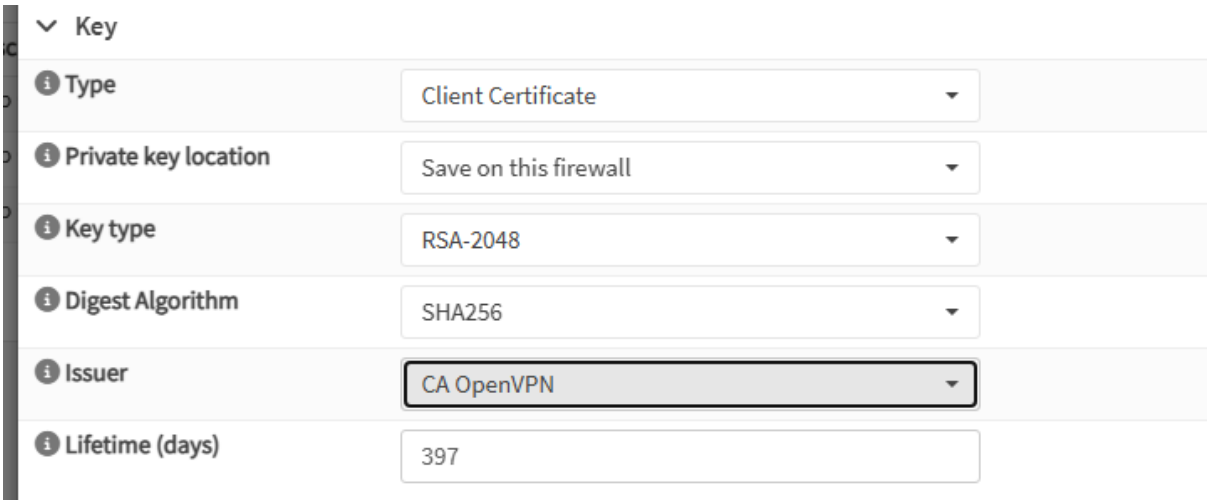
Choisir le type '***Server Certificate***'.

Laisser par défaut pour la '***Private Key Location***' : '***Save on this firewall***'.

Laisser ou modifier le '***Key type***' et le '***Digest Algorithm***' selon la convenance.

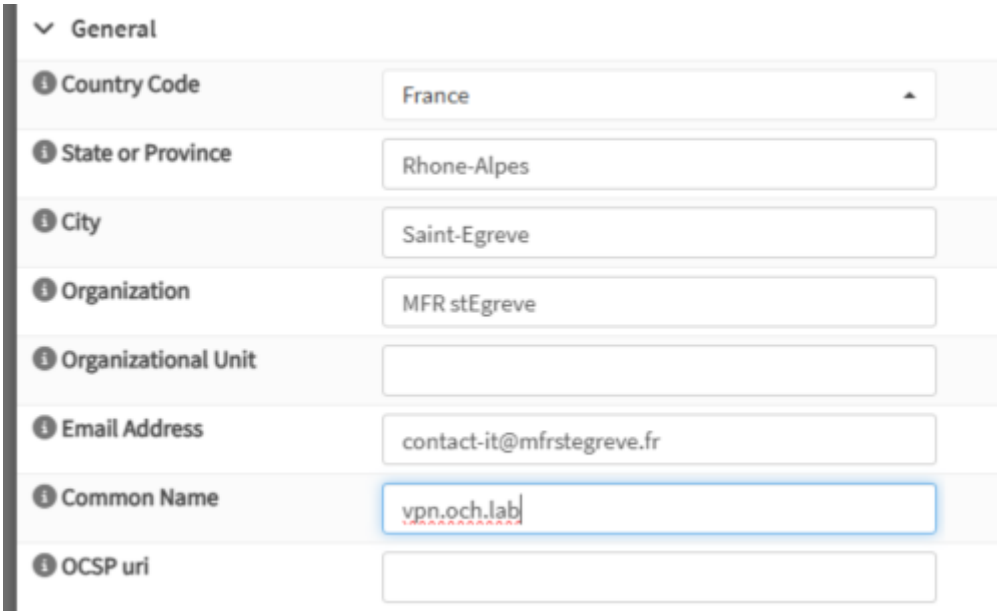
Changer '***Issuer***' pour le faire correspondre à la CA créée plus tôt.

Ajuster la '***Lifetime***' à la convenance (par défaut 397 jours soit 1an et 3 mois).



Les données du certificat sont pré-remplies avec celles de la CA. Il suffit d'ajouter le FQDN du serveur VPN.

> **Attention** : Il s'agit ici de l'adresse externe du VPN tel que les clients qui se situeront en dehors du parc la résoudront. Ce qui signifie qu'il faudra que cette adresse soiteffectivement résolvable.



Il est également possible de renseigner des noms alternatifs ou des IP si besoin.

Laisser le reste vide et faire '***Save***'.

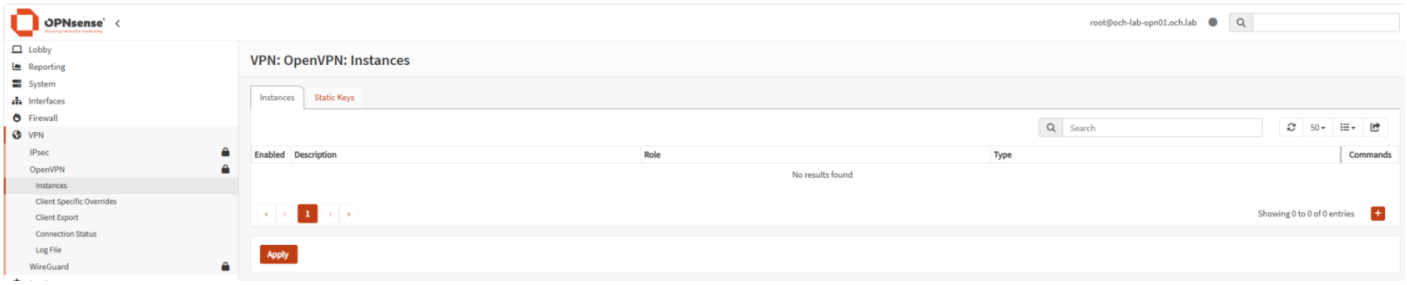
III. Configurer l'instance OpenVPN

3.1 Création de l'instance

Sur les versions récentes d'OPNsense, OpenVPN n'est plus installé en tant que '***serveur***'. Il est désormais initialisé en tant que '***Socket***' ou instance.

Ce qui rends possible l'hébergement de plusieurs instances pour un même serveur physique. Permettant ainsi de pouvoir cloisonner les instances selon les niveaux de privilèges / réseaux accessibles.

Pour créer l'instance, aller dans '***VPN --> OpenVPN --> Instances***'

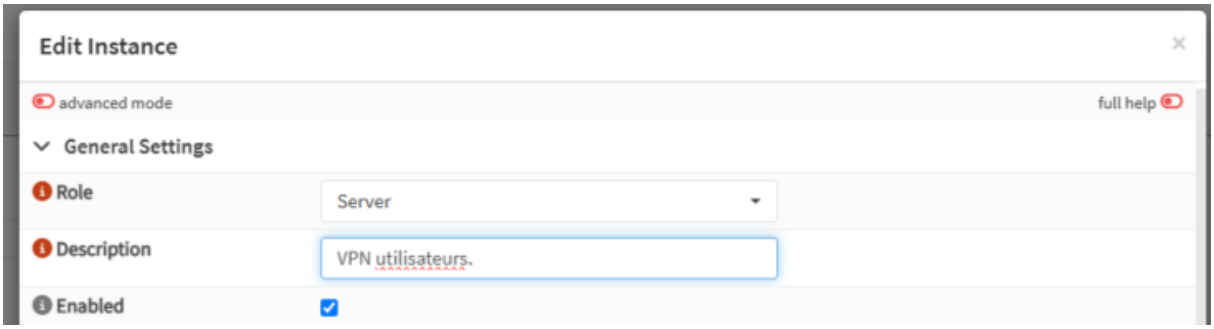


Puis utiliser '+' pour créer une instance.

Choisir le rôle '***Server***'.

Entrer une description parlante.

Laisser la case '***Enabled***' cochée.



Choisir le protocole à utiliser (ici '***UDP***').

- '***UDP***' --> Plus rapide, mais pas de contrôle d'intégrité donc perte de paquet si connexion pas stable.
- '***TCP***' --> Plus lent mais plus stable.

Choisir le port. Par convention, le port historique est : ***1194***

Définir la '***Bind address***'. C'est l'adresse sur laquelle l'instance sera en écoute. En l'occurence, '***l'IP publiq***ue'.

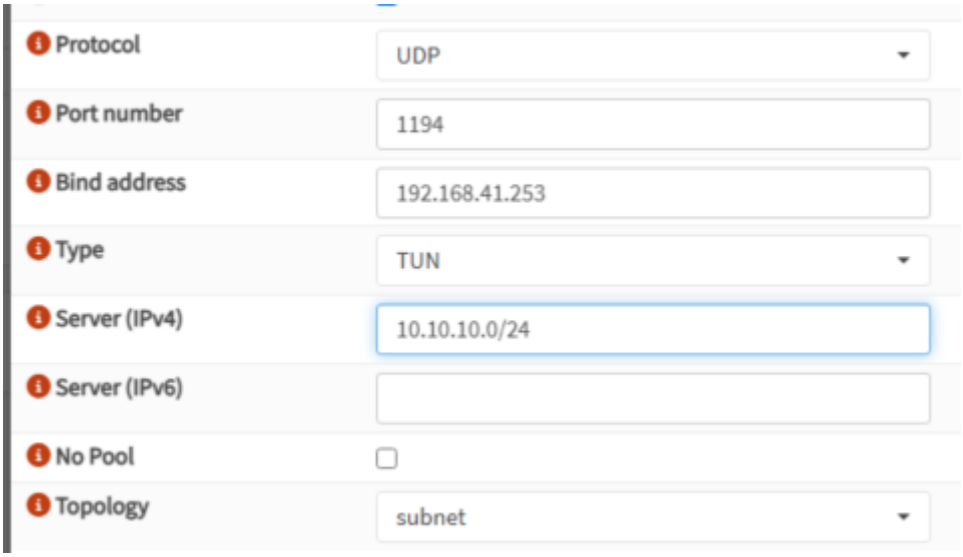
Choisir le type de montage (ici '***TUN***').

- '***TUN***' --> L3. Le tunnel est monté en tant que réseau d'interconnexion avec son adressage IP et son routage.
- '***TAP***' --> L2 over L3. Le tunnel est monté en tant qu'adaptateur réseau et un NAT est mis en place.

Entrer le réseau interne du VPN (ici 10.10.10.0/24).

Le serveur prendra automatiquement la première IP disponible sur la plage et affectera les suivantes séquentiellement aux clients.

Ne pas toucher aux autres options de cette catégorie.

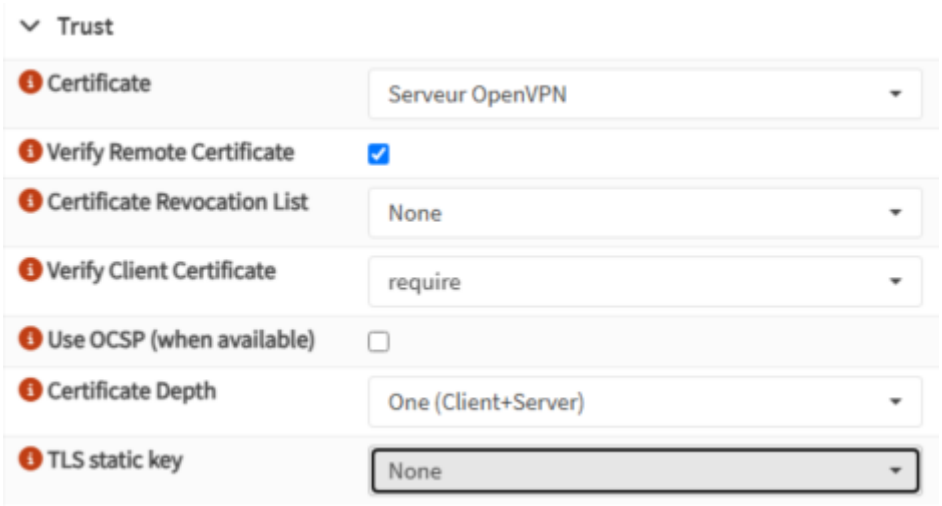


Pour les '***Trusts***', choisir le certificat de serveur généré plus tôt.

Cocher la case '***Verify Remote Certificate***'.

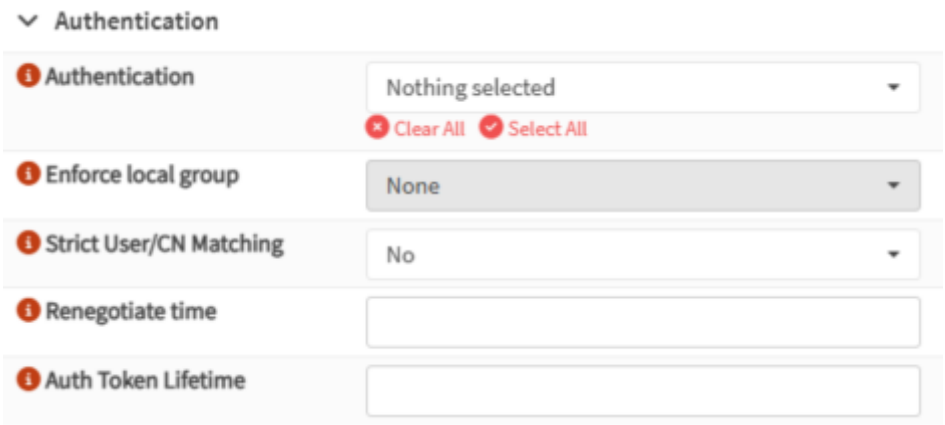
Laisser la CRL à '***none***' et la vérification du certificat client à '***Require***'.

Passer la '***Certificate Depth***' à '***One (Client+Server)***'.



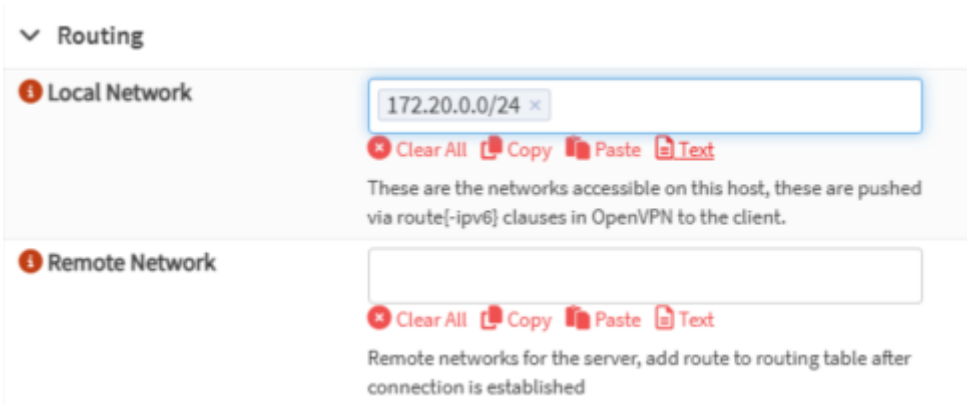
Par défaut, pas d'authentification. Celle-ci sera vue ci-après.

Laisser les autres options par défaut ou vides et passer directement à la partie '***Routing***'.



Pour le routage, ajouter les réseaux locaux qui seront accessibles aux client à travers le VPN dans '***Local Networks***'.

Laisser '***Remote network***' vide car il s'agit d'un VPN point à point et non site-to-site.

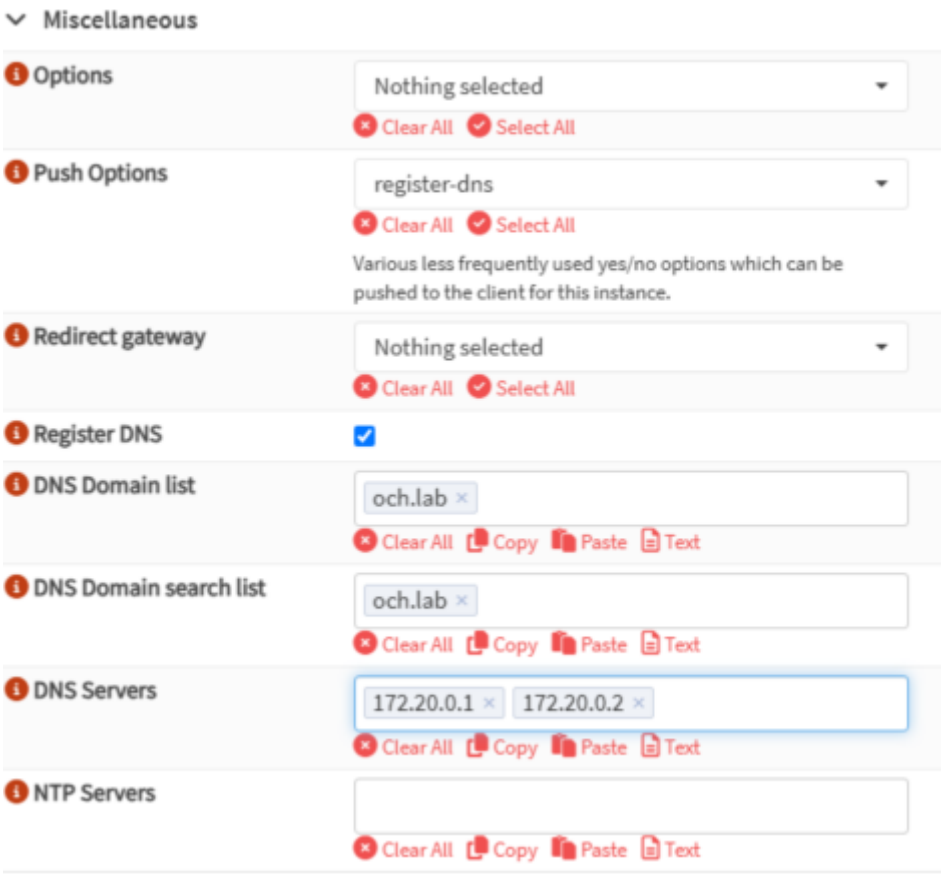


Afin que le client puisse résoudre les noms d'hôtes des services internes à l'entreprise, il faudra pousser les DNS internes et les domaines de recherche sur les clients.

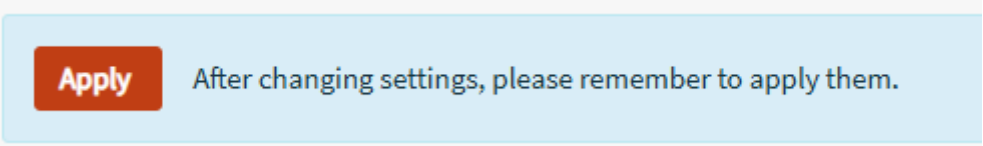
Utiliser '***Push Options***' et cocher dans la liste '***register-dns***'.

Cocher la case '***Register DNS***'.

Ajouter les domaines et l'adresse des serveurs DNS dans les champs correspondants.



Sauvegarder et appliquer.



Le serveur VPN est désormais créé et à l'écoute.

2.3 Ajouter les règles de firewall

Par défaut, OPNsense bloque tout le trafic entrant. Il faut donc ajouter la règle suivante

---

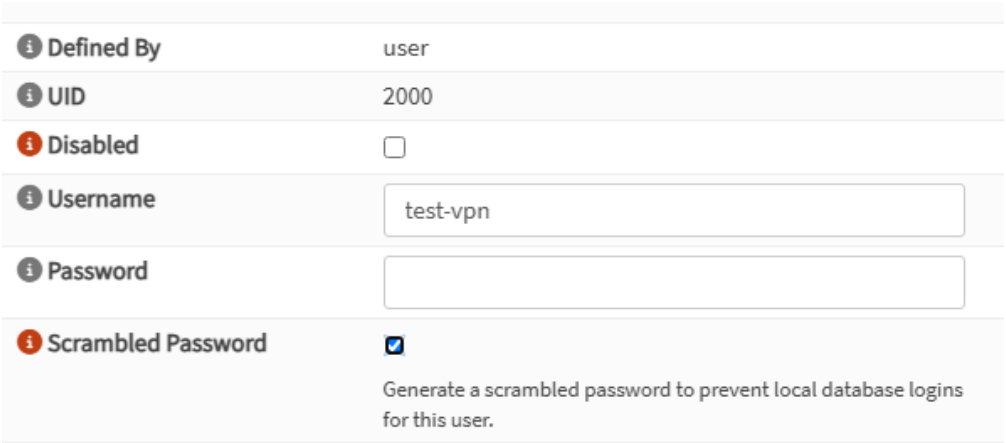
IV. Création des clients

3.1 Générer le certificat du client

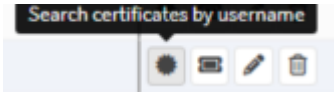
Pour ajouter un client, il faut tout d'abord créer son compte utilisateur. Aller dans '***System --> Users***' et créer le nouvel utilisateur pour le VPN avec '+'.

Entrer simplement un '***username***' et cocher la case '***Scrambled password***'.

Cela permettra de créer un utilisateur sans droits d'accès à l'OPNsense.



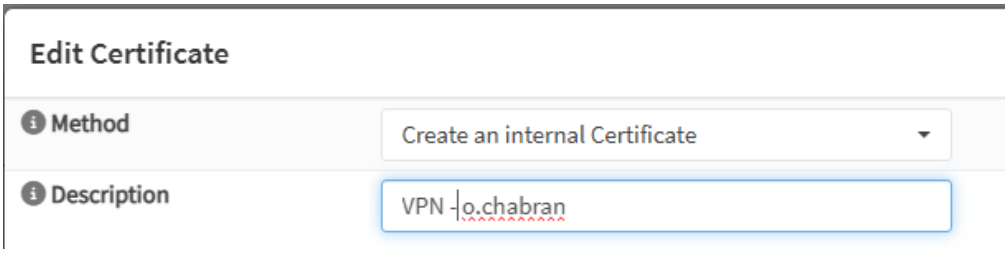
Puis, lui générer un certificat. Pour cela :

cliquer sur l'icône 

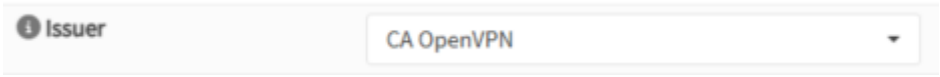
Ou

Aller dans '***System --> Trust --> Certificates***' puis faire '+'

Choisir '***Create an internal certificate***' et entrer en description le nom du client.



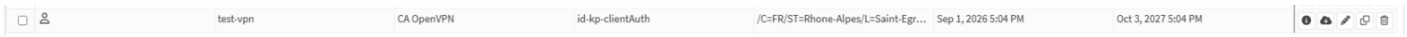
Choisir en '***Issuer***' la CA openVPN.



En CNAME, entrer le nom ***exact*** de l'utilisateur.

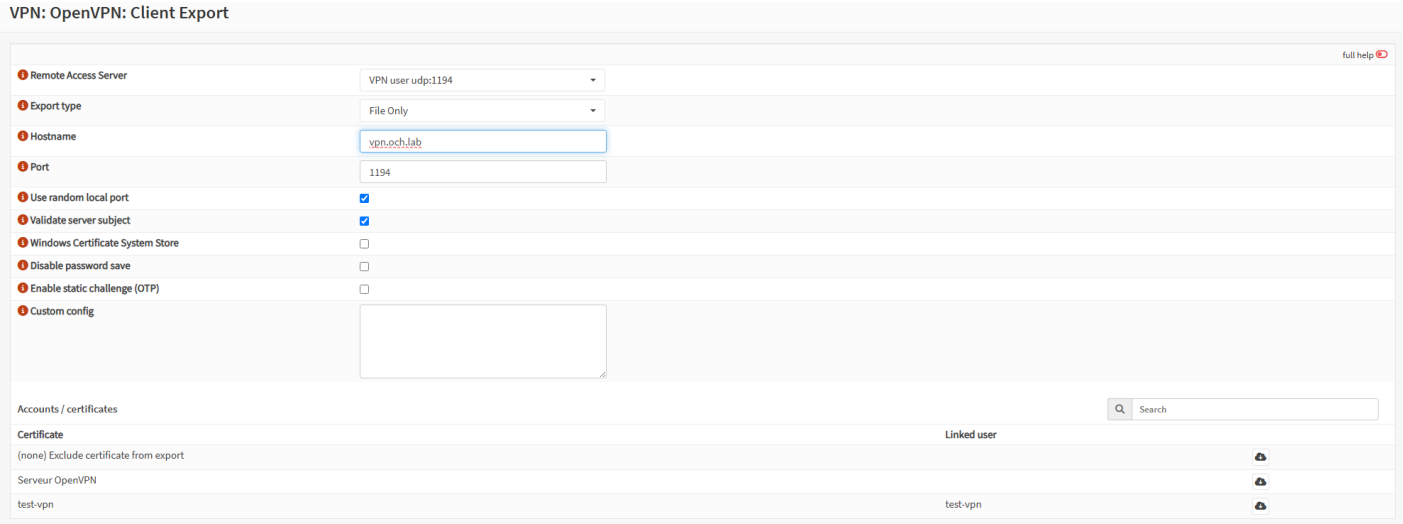
Si pas d'authentification en plus, pas de champs supplémentaires requis.

Sauvegarder.



3.2 Exporter la configuration

Pour exporter la configuration afin de la passer au client, il faut aller dans '***VPN --> OpenVPN --> Client Export***'



Choisir l'export en mode '***File Only***'.

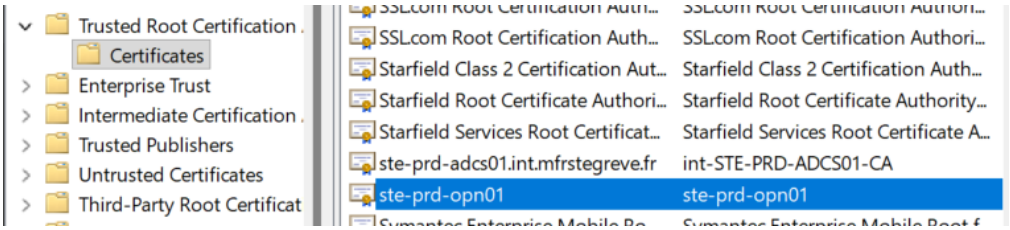
Entrer en '***Hostname***' le FQDN du serveur (externe).

Cocher la case '***Validate server subject***' afin de forcer le client a vérifier l'identité du serveur.

Cliquer sur le symbole  à côté du nom du client, pour télécharger son fichier de configuration.

3.3 Côté client

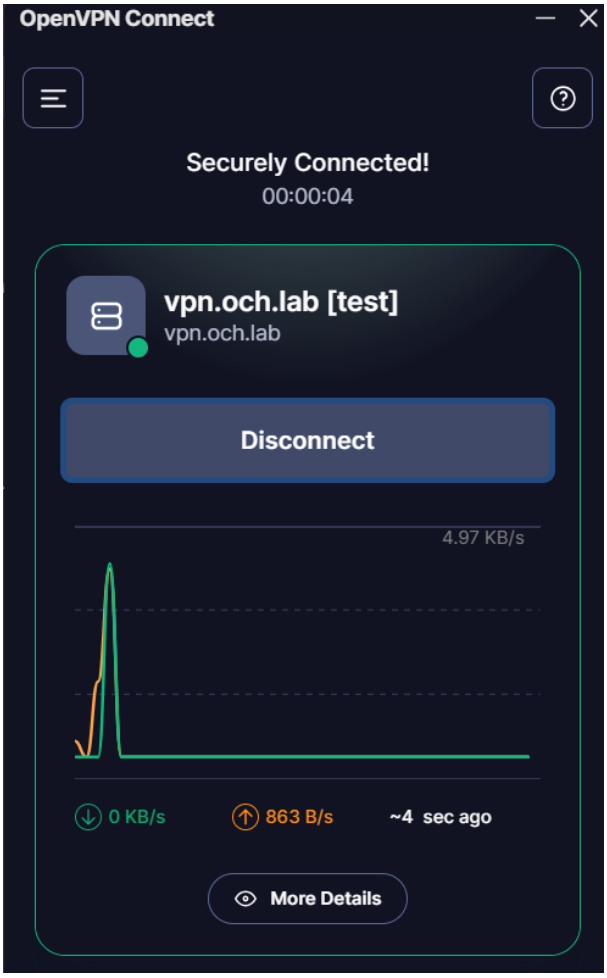
> **Prérequis** : Afin que les clients puissent authentifier le certificat du serveur, ils devront avoir le certificat de la CA dans leurs magasin '***Trusted root certification authorities***'.



Le client devra télécharger et installer le client VPN : [OpenVPN Connect for Windows]

Puis importer son profil depuis le fichier avec : **[OpenVPN Connect - Importer un profil]**

Le client peut désormais se connecter.



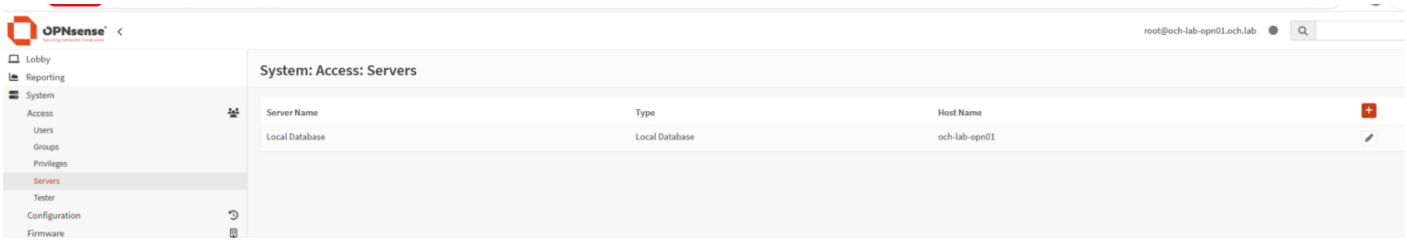
> **Conseil** : Afin de diagnostiquer d'éventuels problèmes de connexion, il est possibles de consulter les logs dans %APPDATA%\OpenVPN Client\Logs.

V. Authentification avec Active directory

5.1 Mise en place du lien LDAP(s)

> **Prérequis** : Un compte LDAP doit avoir préalablement été créé pour le bind.

Aller dans '***System --> Access --> Servers***'.



Utiliser '+' Pour ajouter un nouveau serveur d'authentification.

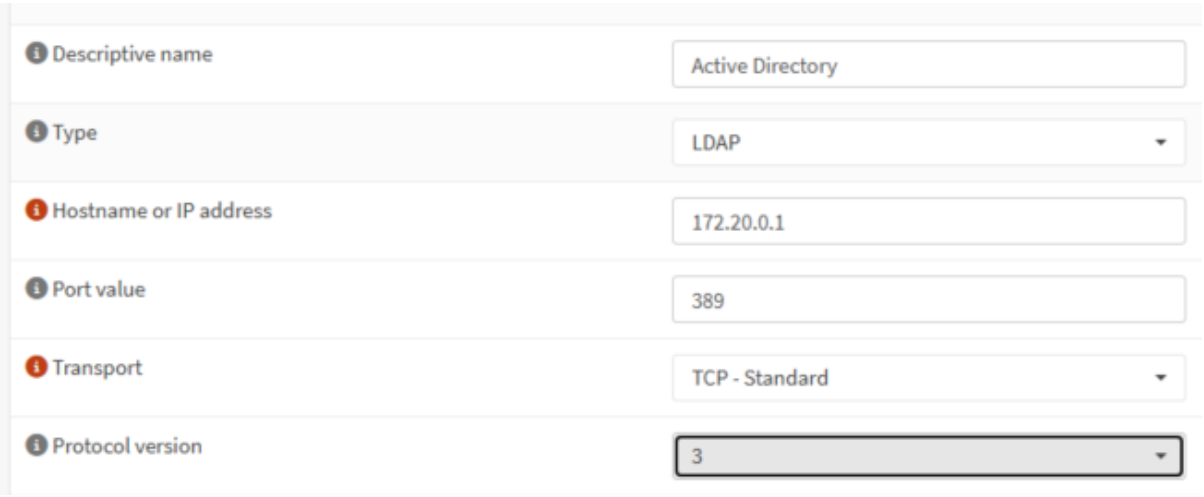
Entrer une Description parlante.

Choisir le type de connexion ('***LDAP***' ou '***LDAPS***').

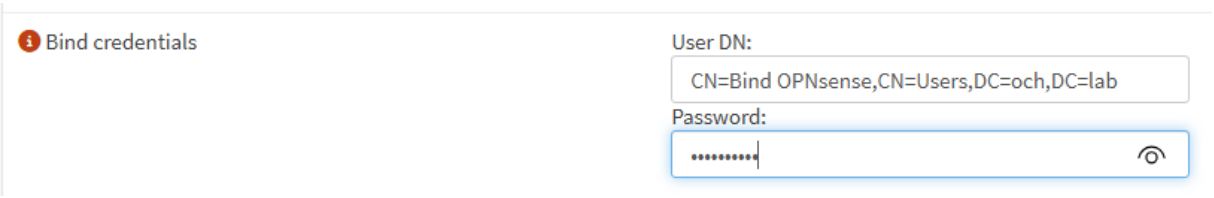
Entrer le port.

Laisser le protocole en '***TCP***'.

Laisser la version en '***3***'.

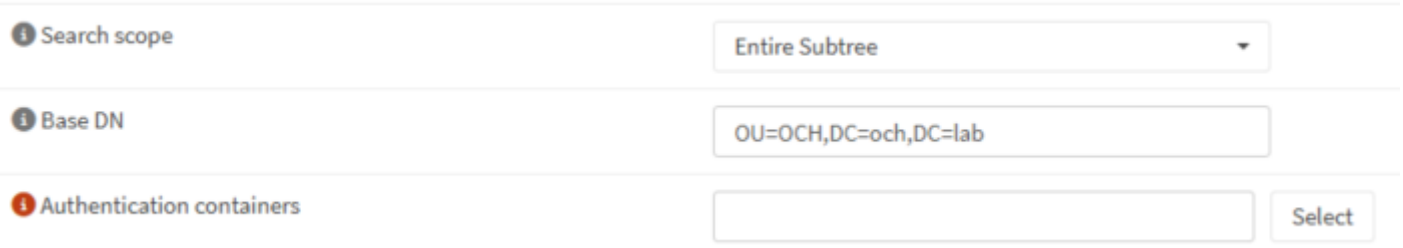


Entrer le '***User DN***' et son mot de passe.



Choisir en '***Search scope***' : '***Entire Subtree***'

Puis entrer le '***Base DN***'. Il s'agit de la racine à partir de laquelle l'OPNsense ira chercher les utilisateurs et groupes.



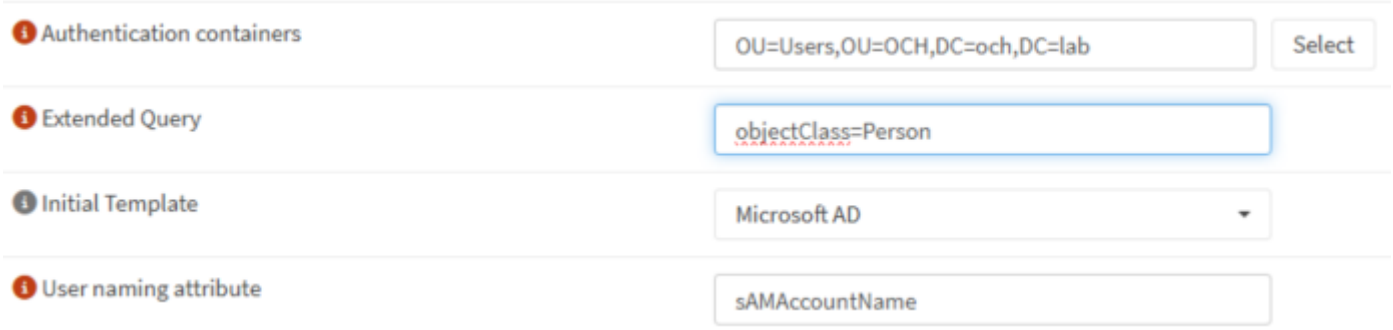
Cliquer ensuite sur '***Select***' pour sélectionner ensuite les OU à ajouter (celles ou se trouvent les utilisateurs).

> **Attention** : Si un message d'erreur s'affiche à la place de la fenêtre ci-dessus, consulter : KB-OPNsense - Bind LDAP Active directory 2025

Ajouter dans le champ '***Extended Query***' : '***objectClass=Person***' afin de ne remonter que les utilisateurs et ignorer les autres types d'objets.

Choisir le Template '***Microsoft AD***' et le '***User naming attribute***' qui sera utilisé comme login.

Par défaut, il s'agit du sAMAccountName, mais cela peut également être 'mail' ou autre.



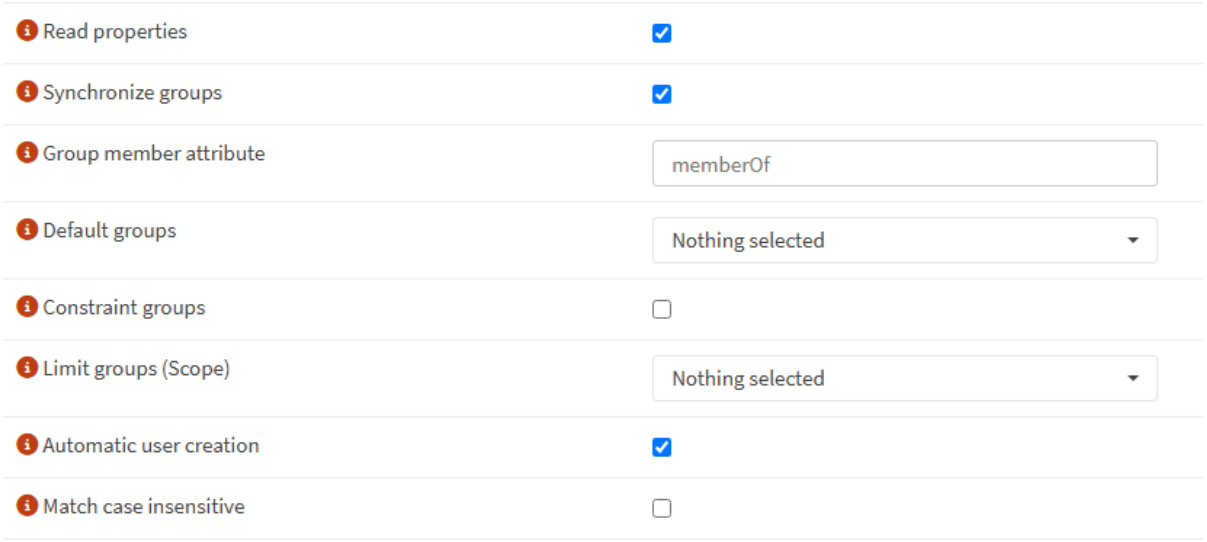
Cocher la case '***Read properties***' afin de pouvoir utiliser les autres champs et également pouvoir lire le 'memberOf' qui permet de faire le lien entre l'utilisateur et les groupes duquel il est membre.

Puis cocher la case '***Synchronize groups***'.

Utiliser l'attribut par défaut '***memberOf***''.

Afin de préserver l'appartenance aux groupes d'origine sur AD, laisser '***Default groups***', '***constraint groups***' et '***Limit groups***' vide.

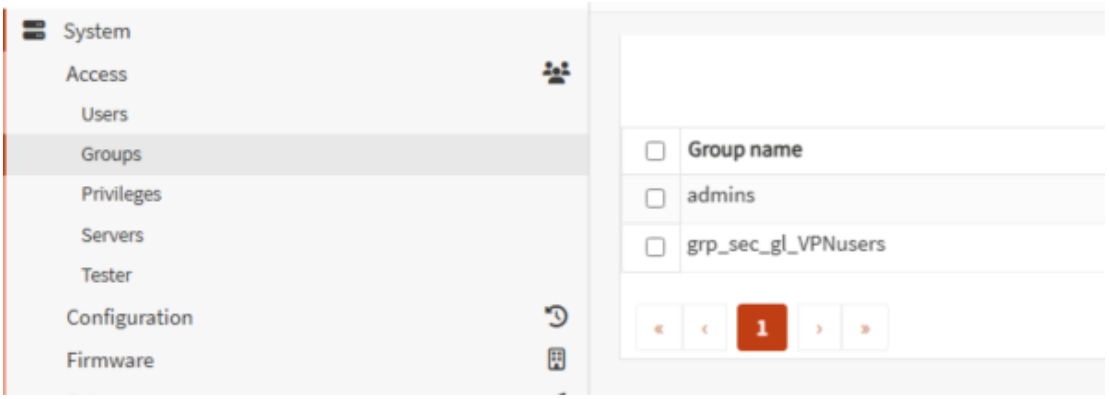
Cocher '***Automatic user creation***' afin de permettre la création des utilisateurs automatiquement lors de la connexion.



Une fois cette configuration terminée, Sauvegarder et quitter. Le serveur a été ajouté.

Il faudra ensuite créer le miroir des groupes présents dans Active directory, afin que l'affectation automatique au groupes fonctionne.

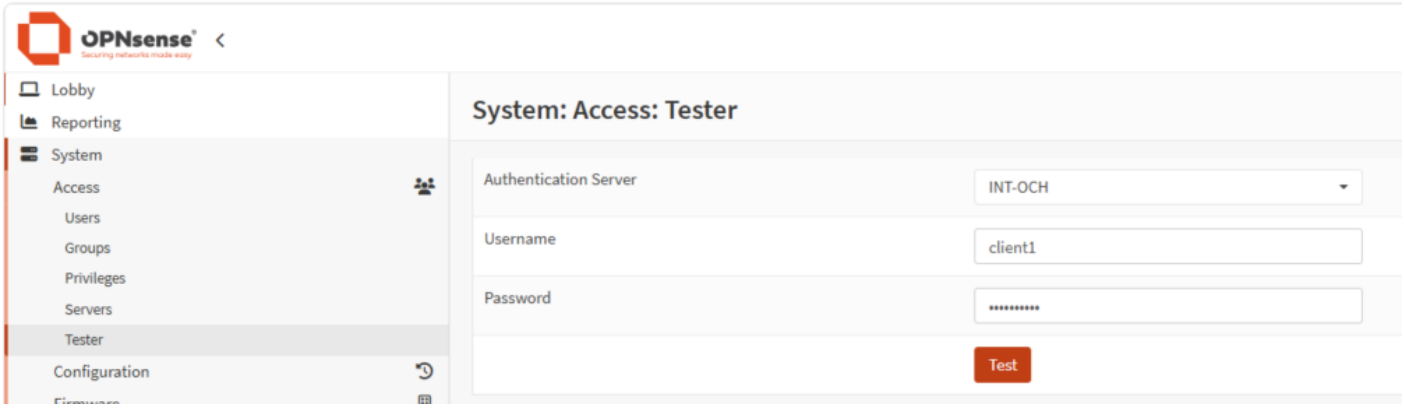
Créer le(s) groupe(s) nécessaires en allant dans '***System --> Access --> Groups***'.



> **Attention** : Il faut que les groupes aient le même nom que dans Active Directory, sinon la synchronisation des groupes ne se fera pas.

Les utilisateurs peuvent maintenant être ajoutés.

Pour les ajouter, le plus rapide est d'utiliser l'outil '***System --> Access --> Tester***'



Si tout est bien configuré, le client se connecte :

et son compte est automatiquement créé.

> **Info :** Il faudra ensuite créer son certificat selon la méthode évoquée plus haut.

> **Conseil** : L'OPN sense dispose d'une api, aussi ces opérations de création / modification pourront être automatisées lors de la création de l'utilisateur.

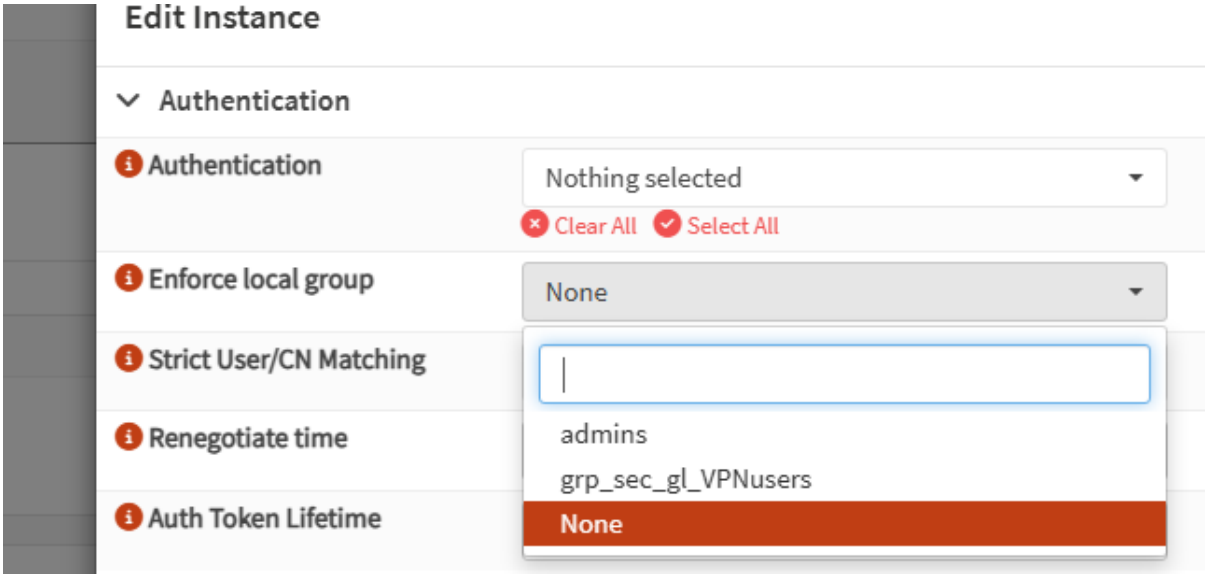
5.2 Affectation des instances aux groupes

OpenVPN permet la création de plusieurs instances. Chacune liée sur un port spécifique, et chacune représentant un réseau à part entière.

Ces instances peuvent forcer l'appartenance à un groupe. Appliquant de facto les règles de pare-feu associées à ce groupe.

Cela permet de fournir des accès séparés par exemple pour les utilisateurs et les administrateurs.

Cette appartenance se définit dans les propriétés de l'instance, sur l'attribut '***Enforce Local Group***'.

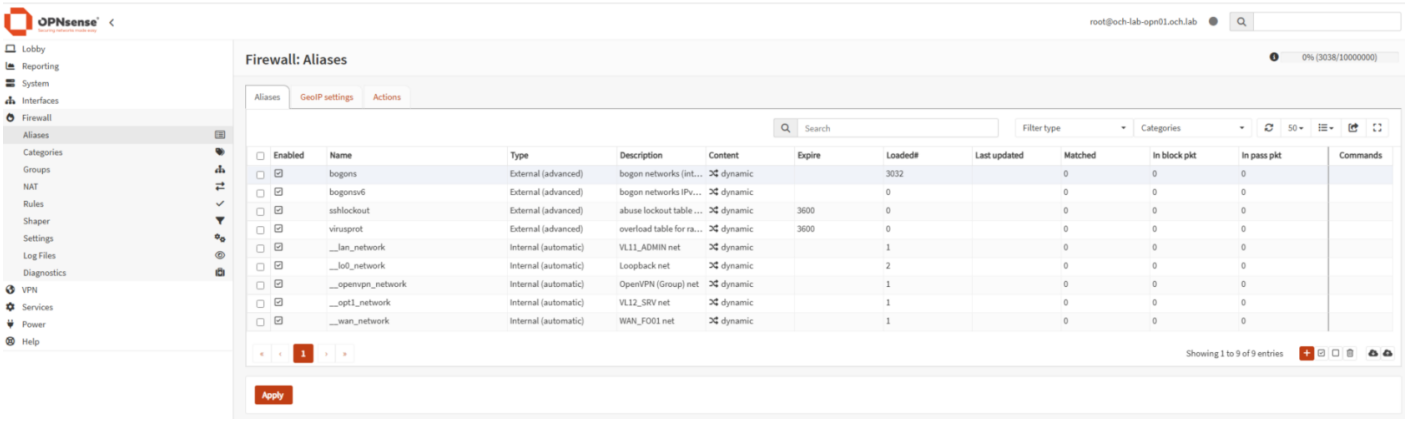


5.3 Création des règles de pare-feu par groupe

5.3.1 Création de l'alias

Pour créer des règles de pare-feu pour le VPN basés sur l'appartenance au groupe, il faut tout d'abord créer un alias à ce groupe.

Pour cela, aller dans '***Firewall --> Aliases***' et créer un alias avec '+'.



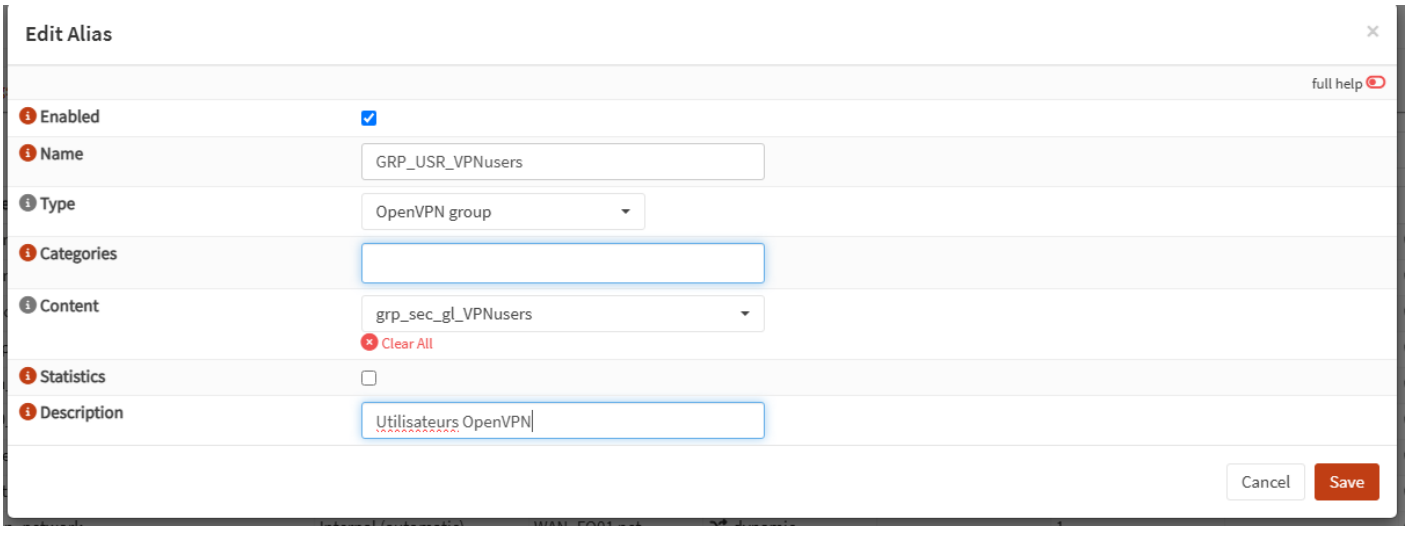
Cocher la case '***Enabled***'. Choisir un nom parlant.

Choisir le type '***OpenVPN Group***'.

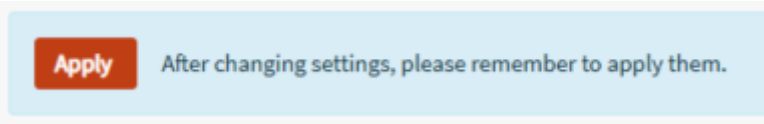
Définir des catégories si nécessaire.

En '***Content***', sélectionner le(s) groupe(s) à ajouter dans l'alias.

Le reste est à la convenance.

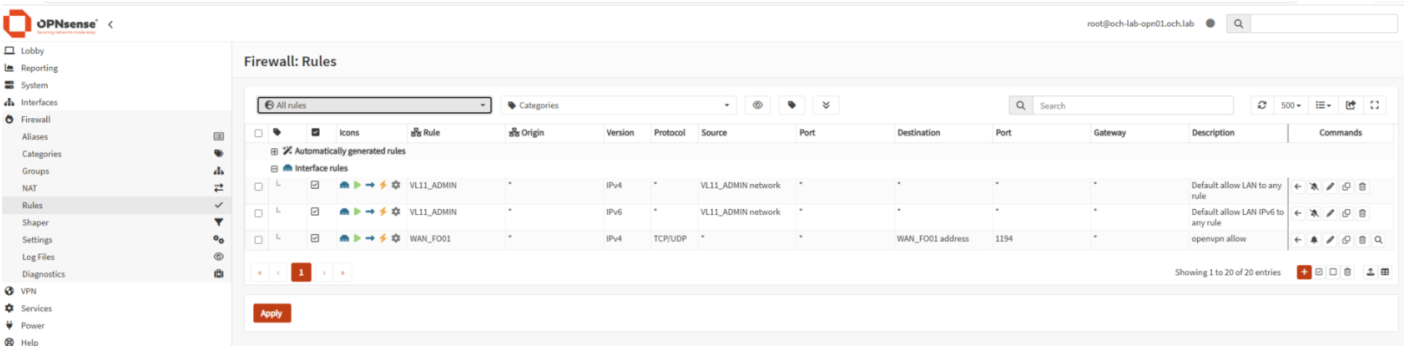


Après validation de l'ajout, ne pas oublier d'appliquer les changements.

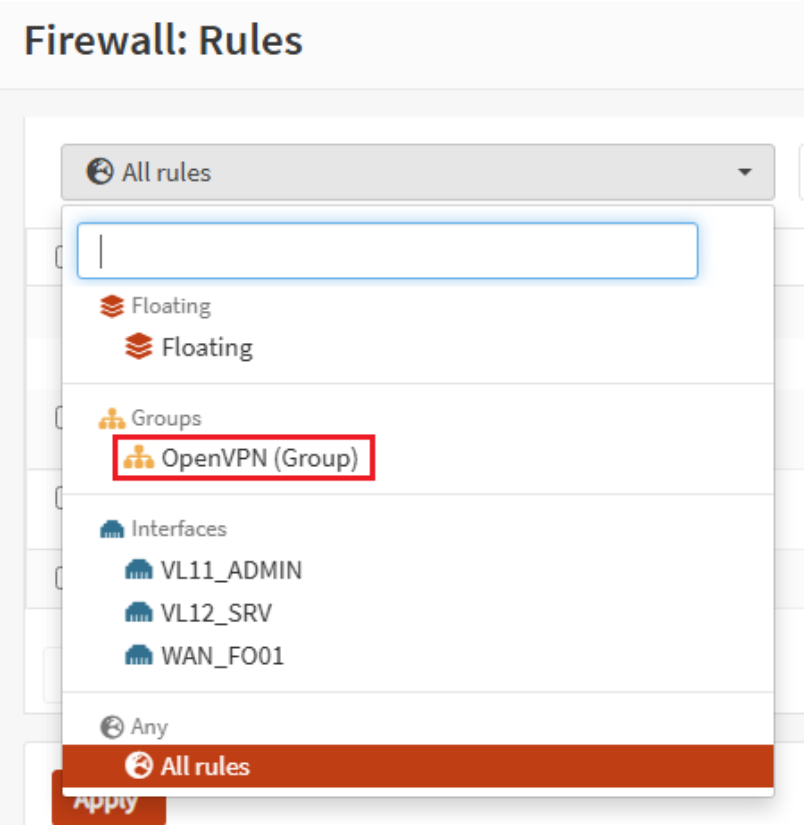


5.3.2 Création des règles

Les règles peuvent être créées à partir de '***Firewall --> Rules***'

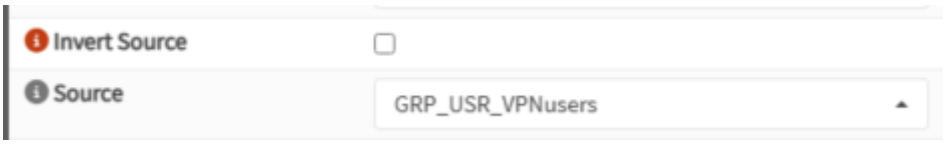


Ouvrir la liste déroulante et sélectionner :



Puis utiliser '+' pour créer la règle.

La création de la règle suit le processus classique. Pour l'appliquer au groupe OpenVN, il faudra choisir en source :



> **Info** : Chaque règle ainsi

Revision #8
Created 2026-08-28 10:12:15 UTC by Olivier
Updated 2026-09-02 10:29:12 UTC by Olivier