

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 fonctionnalités 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 :

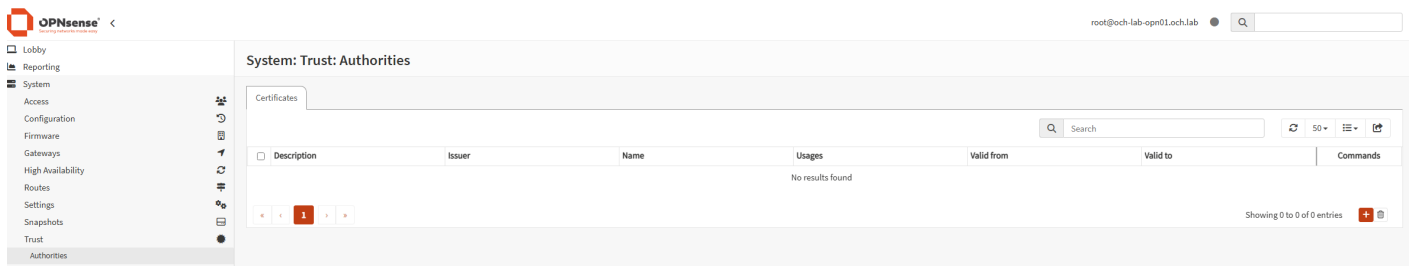
Generic configuration	
 Block private networks	☐
 Block bogon networks	☐

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.

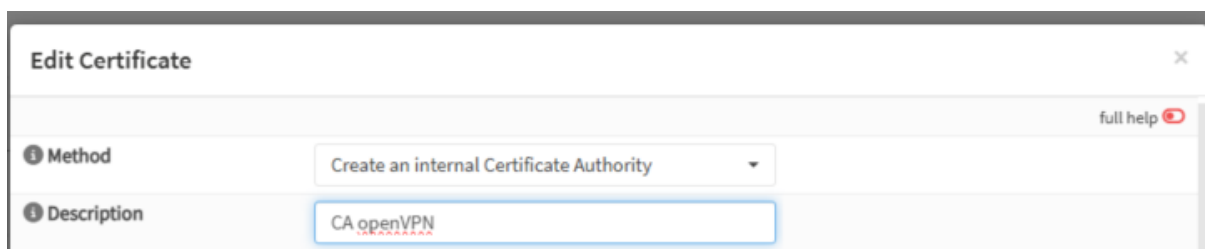
Aller dans '**System --> Trust --> Authorities**'



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.

General

Country Code	France
State or Province	Rhone-Alpes
City	Saint-Egreve
Organization	MFR stEgreve
Organizational Unit	IT Dept.
Email Address	contact-it@mfrstegreve.fr
Common Name	ca-vpn.mfrstegreve.fr
OCSP uri	

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

La CA est désormais créée.

Certificates						
Search						
☐ Description	Issuer	Name	Usages	Valid from	Valid to	Commands
☐ CA openVPN		/C=FR/ST=Rhone-Alpes/L=Saint-Egreve/O=...	0	Aug 31, 2026 1:09 PM	Dec 3, 2028 12:09 PM	Info Edit Delete

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.

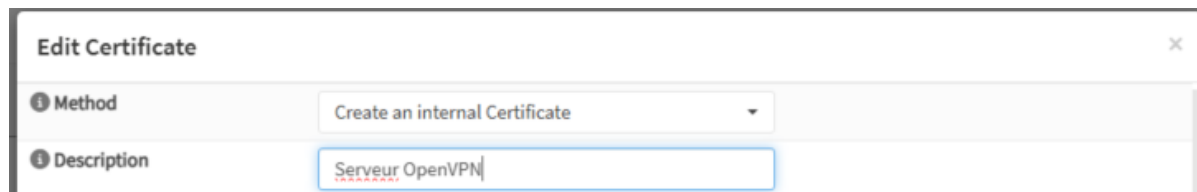
Pour cela, aller dans '**Trust --> Certificates**'.

OPNsense		root@och-lab-opn01.och.lab	
- Lobby - Reporting - System - Access - Configuration - Firmware - Gateways - High Availability - Routes - Settings - Snapshots - Trust - Authorities - Certificates		System: Trust: Certificates	
Certificates		Search	
☐ In use	Description	Issuer	Purpose
☐ x	Web GUI TLS certificate		id-kp-serverAuth
☐ x	Web GUI TLS certificate		id-kp-serverAuth
☐ ✓	Web GUI TLS certificate		id-kp-serverAuth
		Name	Valid from
		/CN=OPNsense.internal/C=NL/ST=Z...	Aug 27, 2026 4:26 PM
		/CN=OPNsense.internal/C=NL/ST=Z...	Aug 27, 2026 4:40 PM
		/CN=OPNsense.internal/C=NL/ST=Z...	Aug 27, 2026 5:12 PM
		Valid to	Commands
		Sep 28, 2027 4:26 PM	Info Edit Delete
		Sep 28, 2027 4:40 PM	Info Edit Delete
		Sep 28, 2027 5:12 PM	Info Edit Delete
Showing 1 to 3 of 3 entries			

Puis faire '+' pour créer un certificat.

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

Entrer la description.



The screenshot shows a dialog box titled 'Edit Certificate'. It has two main sections: 'Method' and 'Description'. The 'Method' dropdown menu is set to 'Create an internal Certificate'. The 'Description' text input field contains the text 'Serveur OpenVPN'.

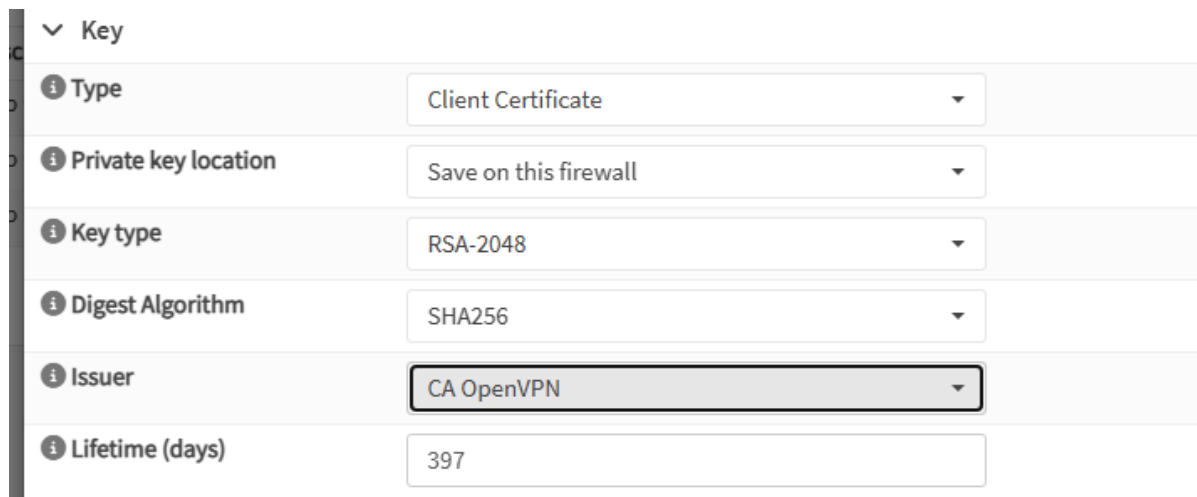
Choisir le type '**Server Certificate**'.

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).



The screenshot shows a configuration section titled 'Key'. It contains several settings, each with an information icon (i) on the left and a dropdown or text field on the right:

- Type: Client Certificate
- Private key location: Save on this firewall
- Key type: RSA-2048
- Digest Algorithm: SHA256
- Issuer: CA OpenVPN
- Lifetime (days): 397

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 soit effectivement résolvable.

▼ General

Country Code

France

State or Province

Rhone-Alpes

City

Saint-Egreve

Organization

MFR stEgreve

Organizational Unit

Email Address

contact-it@mfrstegreve.fr

Common Name

vpn.och.lab

OCSP uri

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

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

☐	✓	Web GUI TLS certificate		id-kp-serverAuth	/CN=OPNsense.internal/C=NL/ST=Z...	Aug 27, 2026 5:12 PM	Sep 28, 2027 5:12 PM	  
☐	✗	Serveur OpenVPN	CA OpenVPN	id-kp-clientAuth	/C=FR/ST=Rhone-Alpes/L=Saint-Egr...	Aug 31, 2026 1:26 PM	Oct 2, 2027 1:26 PM	  

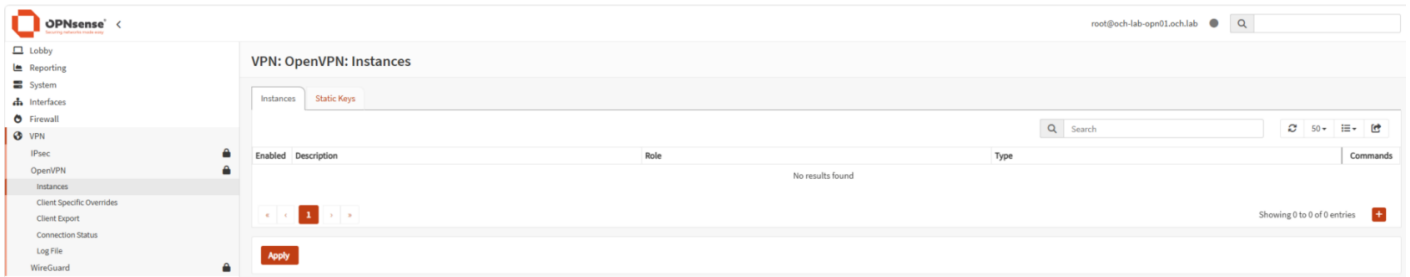
III. Configurer l'instance OpenVPN

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**'

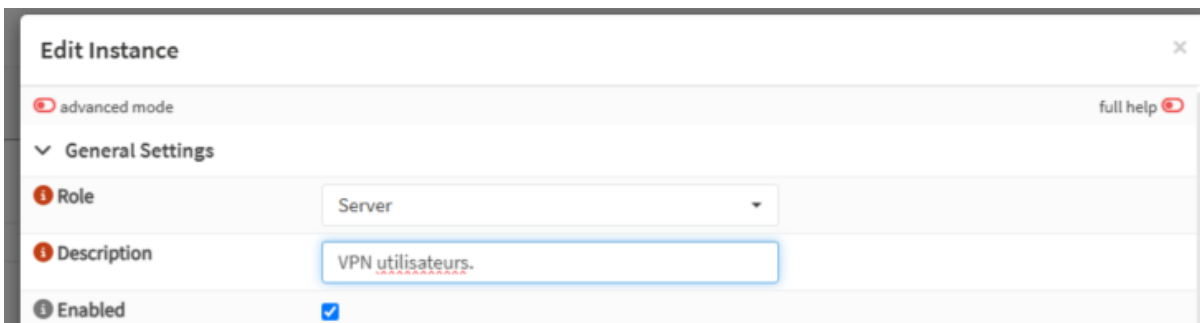


Puis utiliser '+' pour créer une instance.

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'occurrence, '**l'IP publique**'.

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.

Protocol	UDP
Port number	1194
Bind address	192.168.41.253
Type	TUN
Server (IPv4)	10.10.10.0/24
Server (IPv6)	
No Pool	☐
Topology	subnet

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)**'.

▼ Trust

Certificate	Serveur OpenVPN
Verify Remote Certificate	☒
Certificate Revocation List	None
Verify Client Certificate	require
Use OCSP (when available)	☐
Certificate Depth	One (Client+Server)
TLS static key	None

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**'.

▼ Authentication

Authentication	Nothing selected
	☒ Clear All ☒ Select All
Enforce local group	None
Strict User/CN Matching	No
Renegotiate time	
Auth Token Lifetime	

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.

▼ Routing

Local Network	172.20.0.0/24
	☒ Clear All ☐ Copy ☐ Paste ☐ Text
	These are the networks accessible on this host, these are pushed via route[-ipv6] clauses in OpenVPN to the client.
Remote Network	
	☒ Clear All ☐ Copy ☐ Paste ☐ Text
	Remote networks for the server, add route to routing table after connection is established

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.

▼ Miscellaneous

Options	Nothing selected	✖ Clear All ✔ Select All
Push Options	register-dns	✖ Clear All ✔ Select All
Various less frequently used yes/no options which can be pushed to the client for this instance.		
Redirect gateway	Nothing selected	✖ Clear All ✔ Select All
Register DNS	☒	
DNS Domain list	och.lab	✖ Clear All 📄 Copy 📄 Paste 📄 Text
DNS Domain search list	och.lab	✖ Clear All 📄 Copy 📄 Paste 📄 Text
DNS Servers	172.20.0.1 172.20.0.2	✖ Clear All 📄 Copy 📄 Paste 📄 Text
NTP Servers		✖ Clear All 📄 Copy 📄 Paste 📄 Text

Sauvegarder et appliquer.

Apply After changing settings, please remember to apply them.

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

L		    	WAN_FO01	IPv4	TCP/UDP	*	*	WAN_FO01.address	1194	*	openvpn allow
---	---	---	----------	------	---------	---	---	------------------	------	---	---------------

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 '+'.

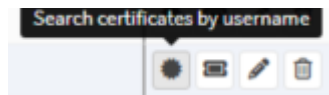
Entrer simplement un '**username**' et cocher la case '**Scrambled password**'.

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

 Defined By	user
 UID	2000
 Disabled	☐
 Username	test-vpn
 Password	
 Scrambled Password	☒ Generate a scrambled password to prevent local database logins for this user.

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.

Edit Certificate

Method

Create an internal Certificate

Description

VPN-o.chabran

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

Issuer

CA OpenVPN

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

Common Name

test-vpn

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

Sauvegarder.

☐		test-vpn	CA OpenVPN	id-kp-clientAuth	/C=FR/ST=Rhone-Alpes/L=Saint-Egr...	Sep 1, 2026 5:04 PM	Oct 3, 2027 5:04 PM	
--------------------------	--	----------	------------	------------------	-------------------------------------	---------------------	---------------------	--

3.2 Exporter la configuration

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

VPN: OpenVPN: Client Export full help

Remote Access Server	VPN user udp:1194
Export type	File Only
Hostname	vpn.ochlab
Port	1194
Use random local port	☒
Validate server subject	☒
Windows Certificate System Store	☐
Disable password save	☐
Enable static challenge (OTP)	☐
Custom config	

Accounts / certificates Search

Certificate	Linked user	
(none) Exclude certificate from export		
Serveur OpenVPN		
test-vpn	test-vpn	

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

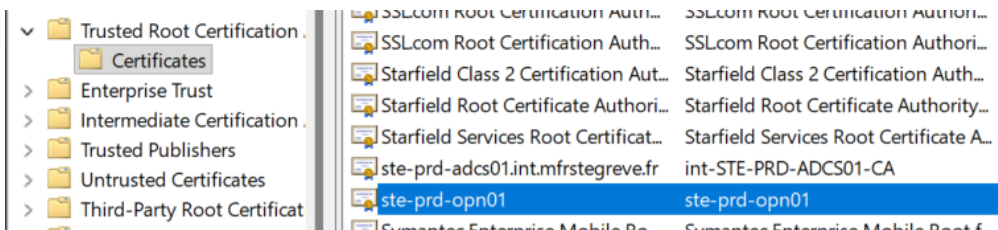
Entrer en '**Hostname**' le FQDN du serveur (externe).

Cocher la case '**Validate server subject**' afin de forcer le client à 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

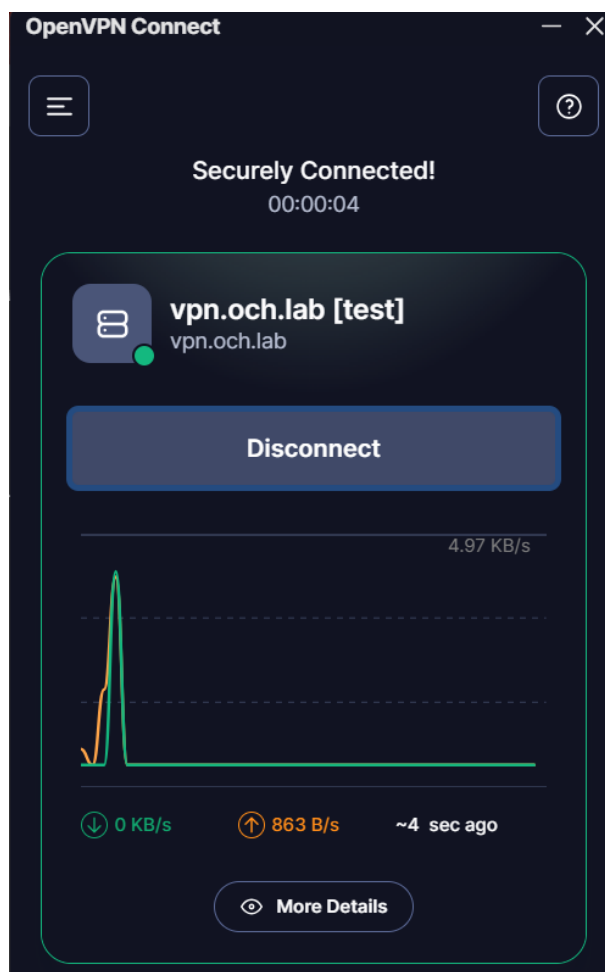
Prérequis : Afin que les clients puissent authentifier le certificat du serveur, ils devront avoir le certificat de la CA dans leurs magasin '**Trusted root certification authorities**'.



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.



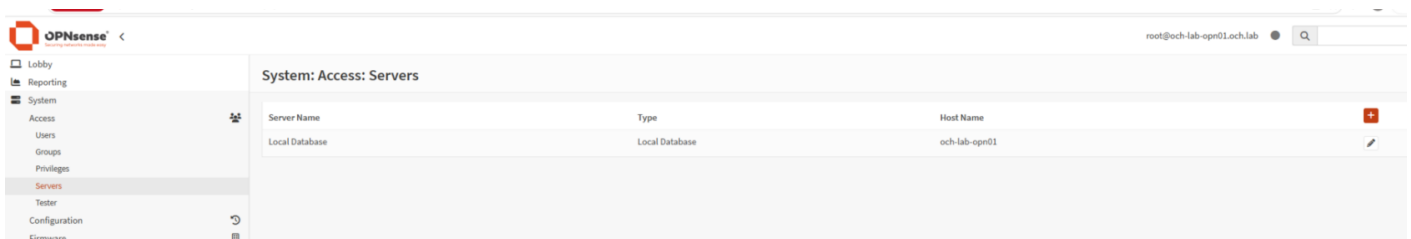
Conseil : Afin de diagnostiquer d'éventuels problèmes de connexion, il est possibles de consulter les logs dans %APPDATA%\OpenVPN Client\Logs.

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**'.

Descriptive name	Active Directory
Type	LDAP
Hostname or IP address	172.20.0.1
Port value	389
Transport	TCP - Standard
Protocol version	3

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

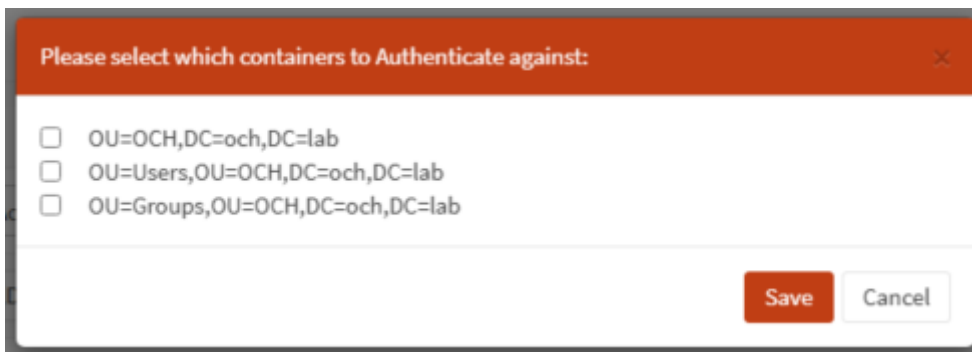
Bind credentials	User DN: CN=Bind OPNsense,CN=Users,DC=och,DC=lab Password:
------------------	---

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.

Search scope	Entire Subtree
Base DN	OU=OCH,DC=och,DC=lab
Authentication containers	Select

Cliquer ensuite sur '**Select**' pour sélectionner ensuite les OU à ajouter (celles où 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.

Authentication containers	OU=Users,OU=OCH,DC=och,DC=lab	Select
Extended Query	objectClass=Person	
Initial Template	Microsoft AD	
User naming attribute	sAMAccountName	

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.

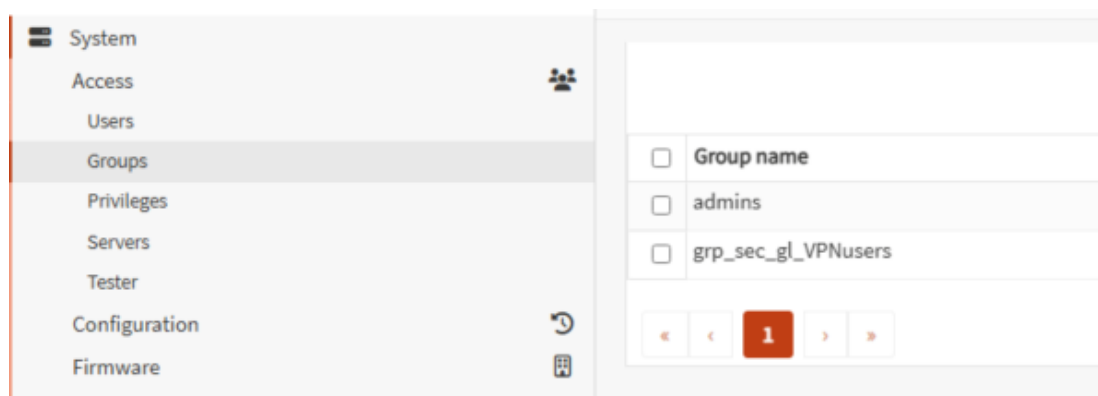
Cocher '**Automatic user creation**' afin de permettre la création des utilisateurs automatiquement lors de la connexion.

 Read properties	☒
 Synchronize groups	☒
 Group member attribute	memberOf
 Default groups	Nothing selected
 Constraint groups	☐
 Limit groups (Scope)	Nothing selected
 Automatic user creation	☒
 Match case insensitive	☐

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.

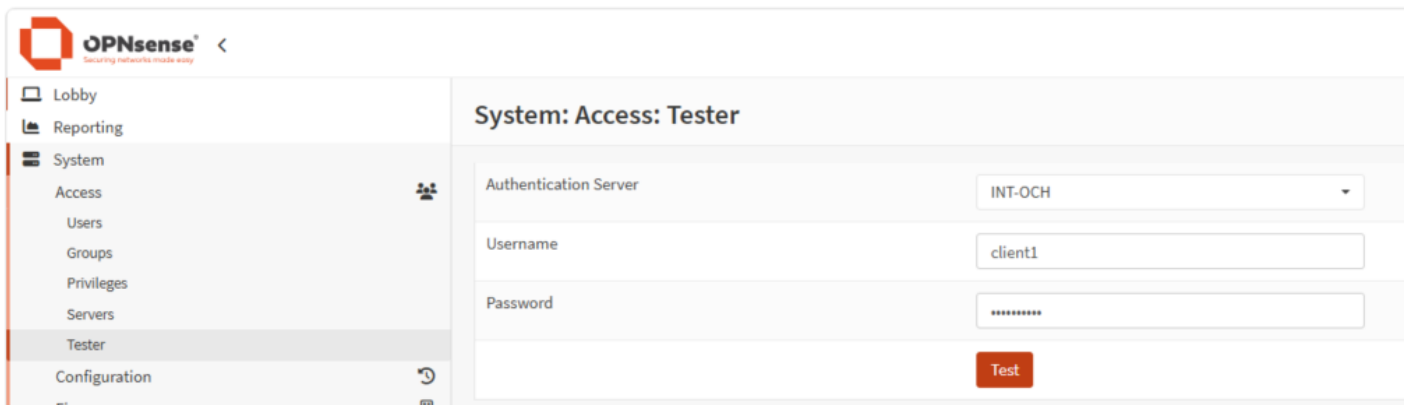
Créer le(s) groupe(s) nécessaires en allant dans '**System --> Access --> Groups**'.



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**'



The screenshot shows the OPNsense web interface. On the left is a sidebar menu with the following items: Lobby, Reporting, System (expanded), Access, Users, Groups, Privileges, Servers, Tester (highlighted), Configuration, and Firmware. The main content area is titled 'System: Access: Tester'. It contains three input fields: 'Authentication Server' with a dropdown menu showing 'INT-OCH', 'Username' with the text 'client1', and 'Password' with masked characters. Below these fields is a red 'Test' button.

Si tout est bien configuré, le client se connecte :

System: Access: Tester

User: client1 authenticated successfully.

This user is a member of these groups:

grp_sec_gl_VPNusers

May access the following locations, depending on source address:

Uri Networks

Attributes received from server:

dn => CN=Client1 VPN,OU=Users,OU=OCH,DC=och,DC=lab
objectclass => top
person
organizationalPerson
user
cn => Client1 VPN
sn => VPN
givenname => Client1
distinguishedname => CN=Client1 VPN,OU=Users,OU=OCH,DC=och,DC=lab
instancetype => 4
whencreated => 20260831154336.0Z
whenchanged => 20260902102345.0Z
displayname => Client1 VPN
usncreated => 20849
memberof => CN=grp_sec_gl_VPNusers,OU=Groups,OU=OCH,DC=och,DC=lab
usnchanged => 24791
name => Client1 VPN
objectguid => /0mPDKg2T
useraccountcontrol => 512
badpwdcount => 0
codepage => 0
countrycode => 0
badpasswordtime => 0
lastlogoff => 0
lastlogon => 0
pwdlastset => 134328182180266772
primarygroupid => 513
objectsid => r | 1sTEe QJ
accountexpires => 9223372036854775807
logoncount => 0
samaccountname => client1
samaccounttype => 805306368
userprincipalname => client1@och.lab
objectcategory => CN=Person,CN=Schema,CN=Configuration,DC=och,DC=lab
dscorepropagationdata => 16010101000000.0Z
lastlogontimestamp => 134328182258183417

et son compte est automatiquement créé.

☐	Username	Group membership
☐	 root	admins
☐	 client1	grp_sec_gl_VPNusers

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**'.

Edit Instance

▼ Authentication

- Authentication**: Nothing selected (Clear All, Select All)
- Enforce local group**: None
- Strict User/CN Matching**: [Search bar]
- Renegotiate time**: [Search bar]
- Auth Token Lifetime**: [Search bar]

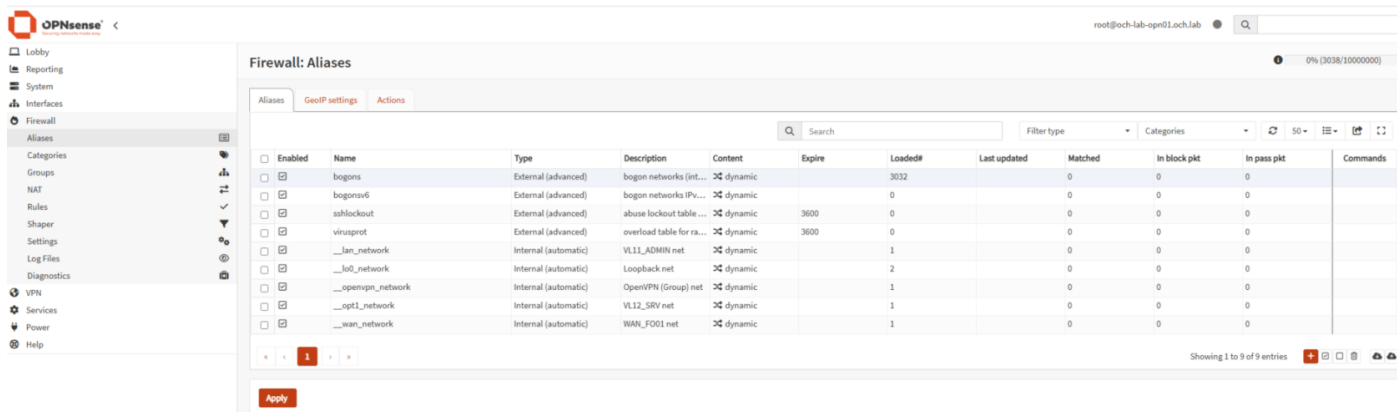
admins
grp_sec_gl_VPNusers
None

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.

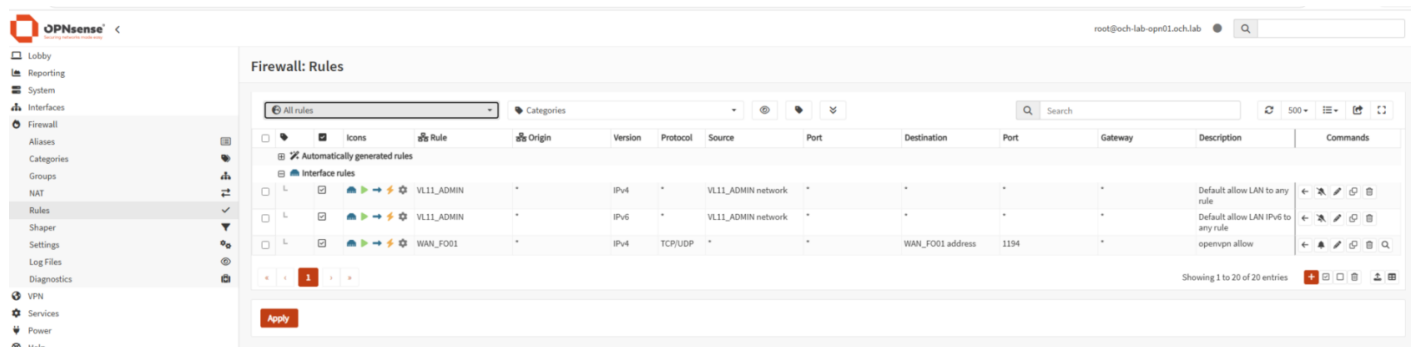
Après validation de l'ajout, ne pas oublier d'appliquer les changements.

Apply

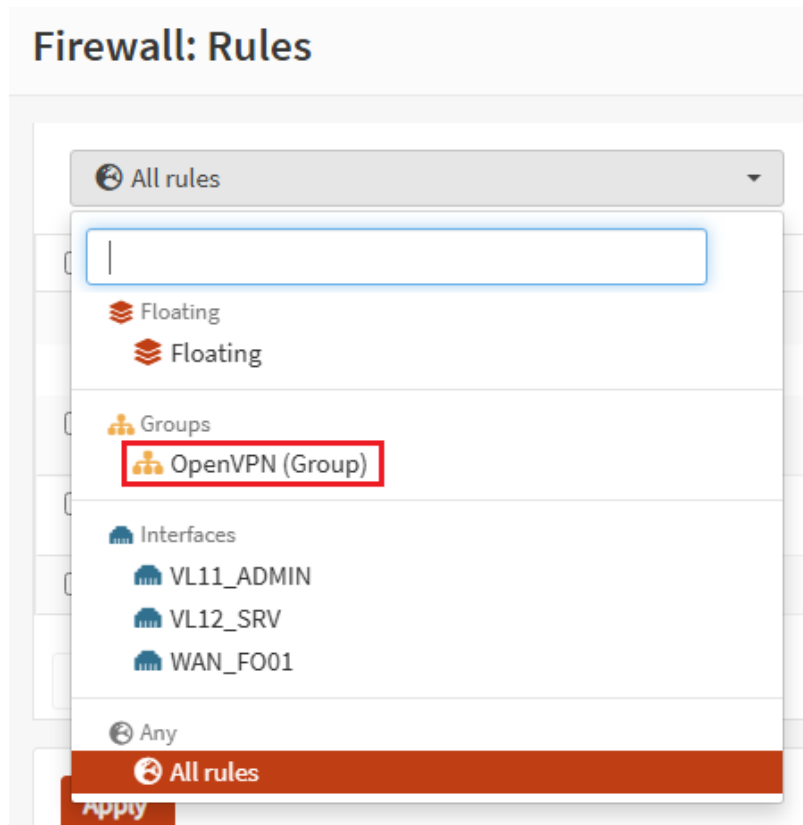
After changing settings, please remember to apply them.

5.3.2 Création des règles

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

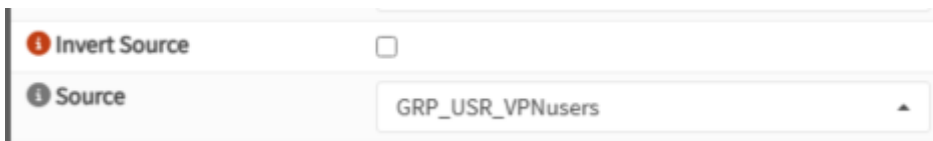


Ouvrir la liste déroulante et sélectionner :



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 :



The screenshot shows a configuration interface with two rows. The first row is labeled 'Invert Source' with an information icon on the left and an unchecked checkbox on the right. The second row is labeled 'Source' with an information icon on the left and a dropdown menu on the right. The dropdown menu is open, showing the selected option 'GRP_USR_VPNusers' and a small upward-pointing triangle at the end of the list.

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