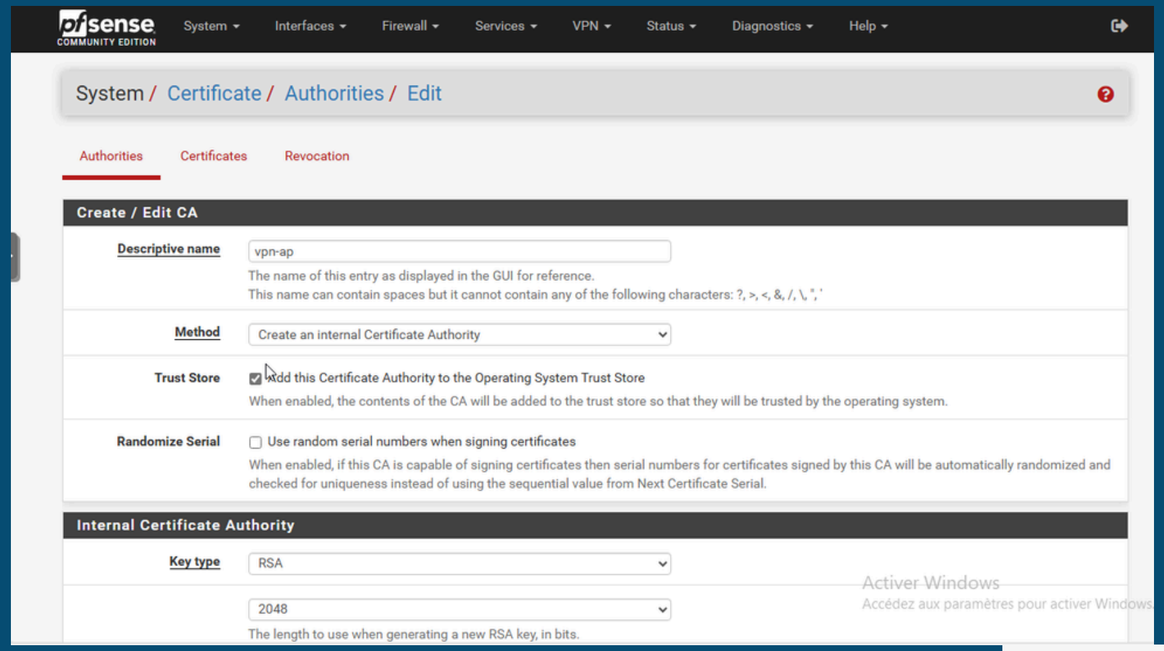
2024

BTS SIO2

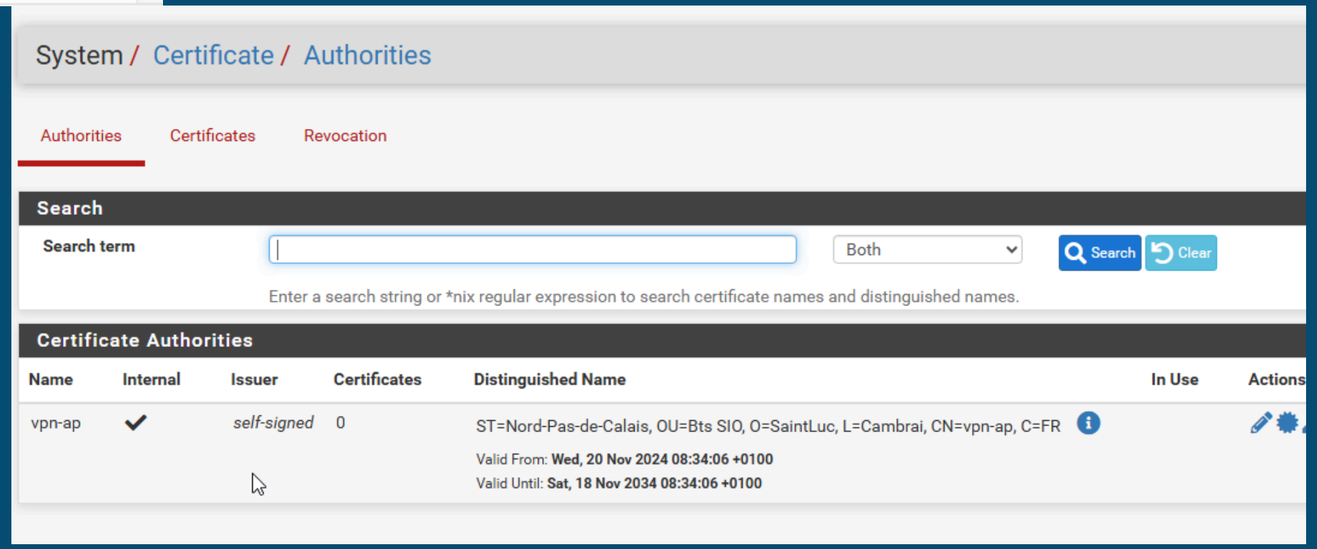
TP-OPENVPN

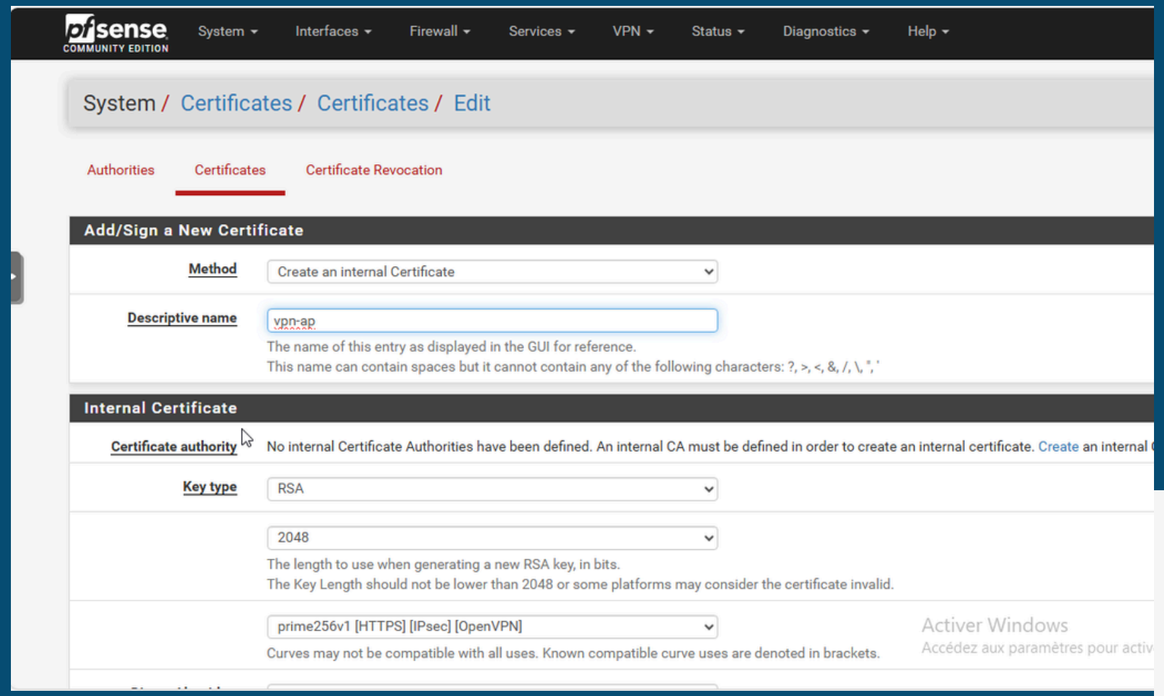
Nicolas Debut

OPENVPN OFFRE UN MOYEN SÉCURISÉ DE CONNECTER DES ORDINATEURS OU DES RÉSEAUX DISTANTS VIA INTERNET, EN UTILISANT DES PROTOCOLES DE CHIFFREMENT POUR PROTÉGER LES DONNÉES ÉCHANGÉES. OPENVPN EST TRÈS UTILISÉ EN ENTREPRISE POUR PERMETTRE AUX EMPLOYÉS D'ACCÉDER AU RÉSEAU INTERNE À DISTANCE, TOUT EN GARANTISSANT LA CONFIDENTIALITÉ ET L'INTÉGRITÉ DES INFORMATIONS. SON FONCTIONNEMENT REPOSE PRINCIPALEMENT SUR LE PROTOCOLE SSL/TLS, CE QUI LE REND FLEXIBLE, SÉCURISÉ ET COMPATIBLE AVEC DE NOMBREUX SYSTÈMES D'EXPLOITATION.

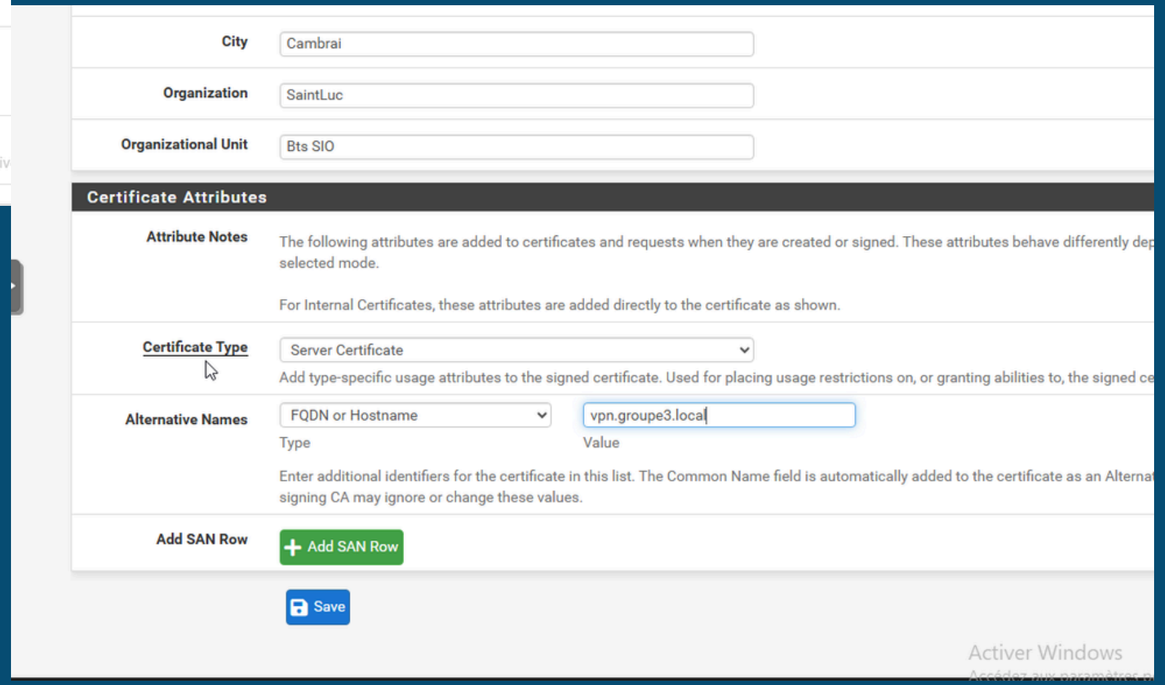


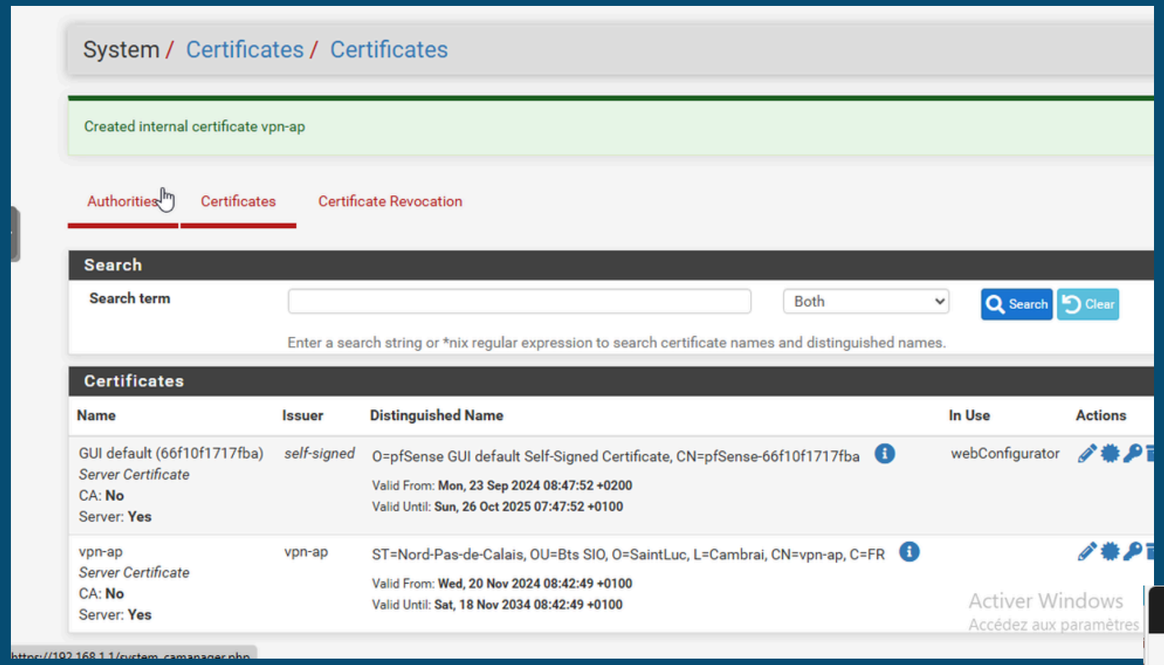
Dans un premier temps, nous allons créer une autorité de certification, que nous utiliserons ensuite lors de la création de notre certificat.
Pour ce faire, accédez à l'onglet Certificat dans la section Système, puis ajoutez une nouvelle autorité.



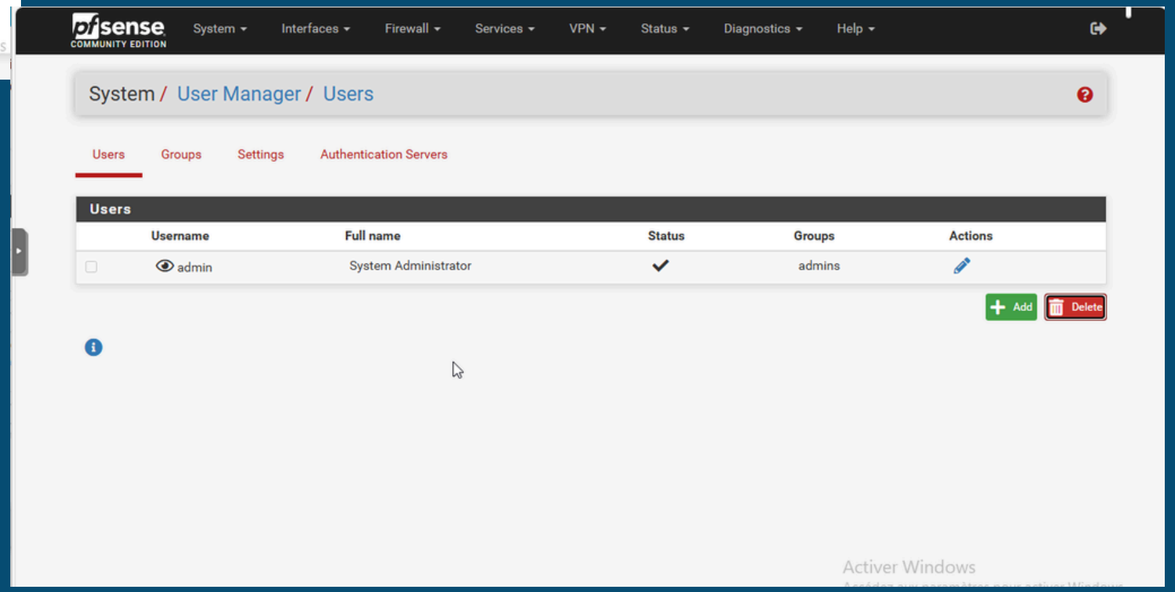


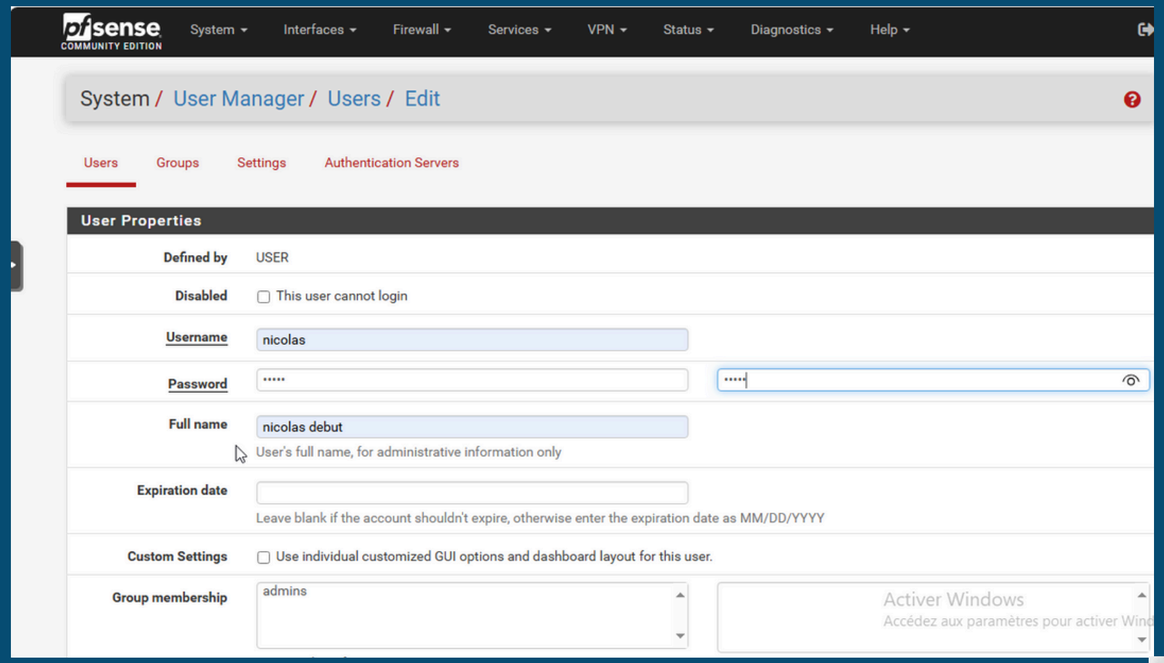
Une fois l'autorité créée, rendez-vous dans l'onglet Certificates et créez le certificat en sélectionnant votre autorité.



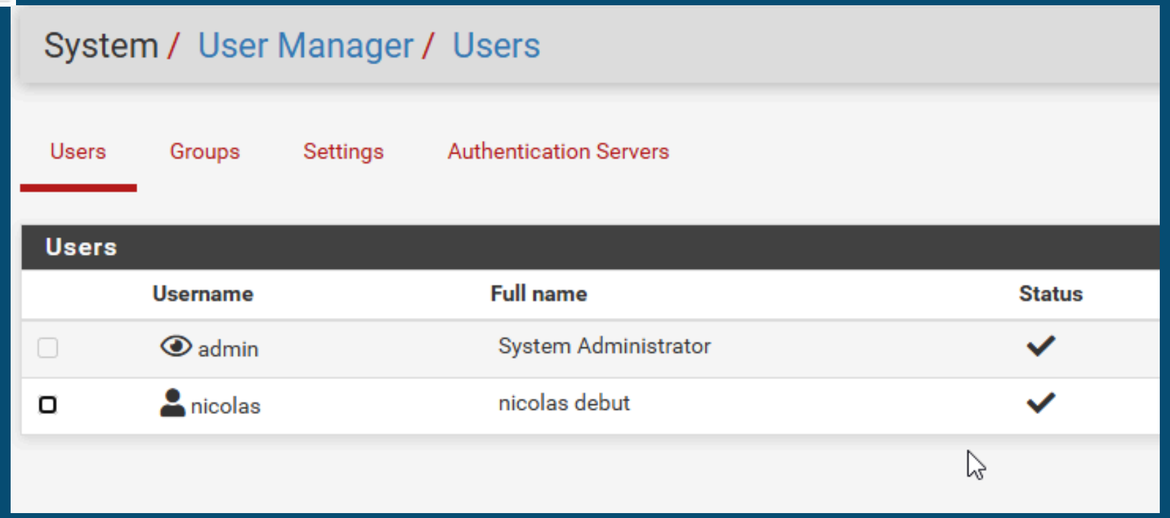


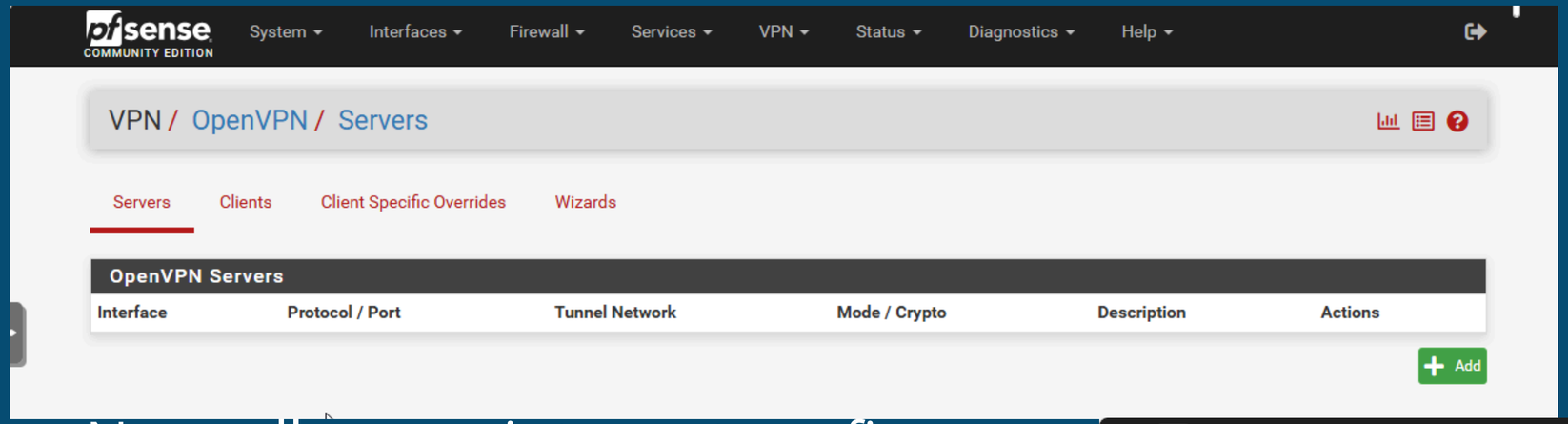
Une fois votre certificat serveur créé, nous allons créer nos utilisateurs. PfSense utilisera sa base d'utilisateurs pour autoriser les connexions VPN.





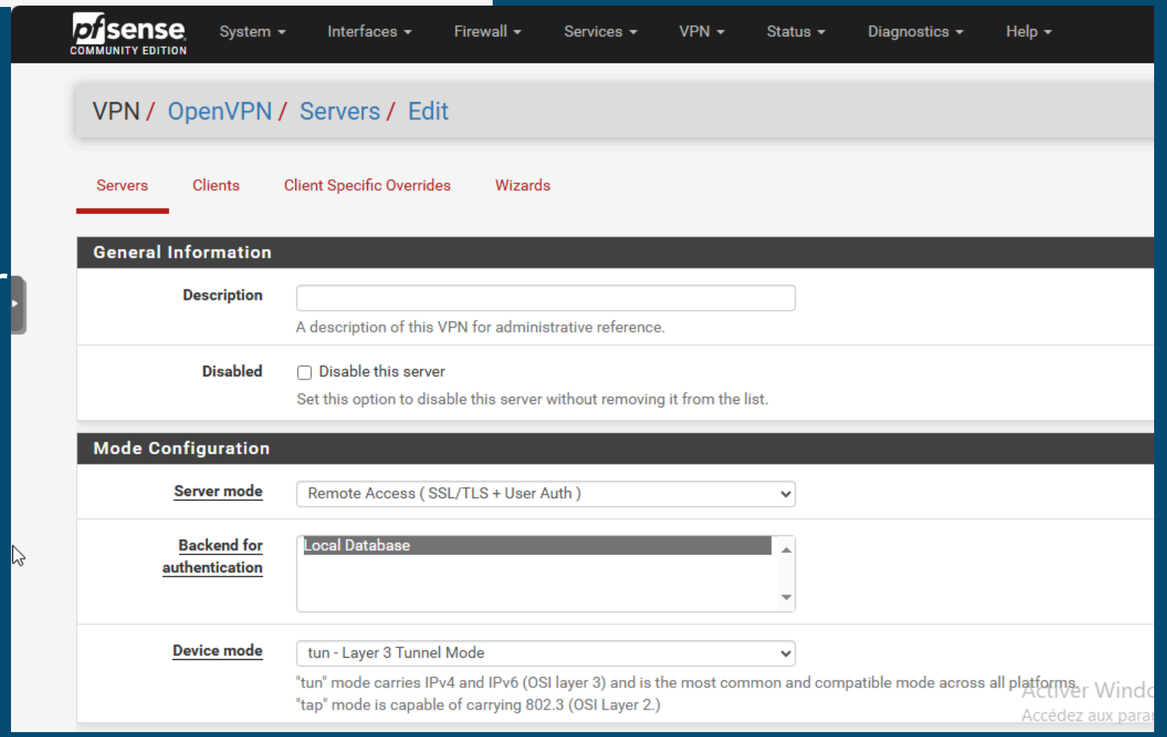
Attention, n'oubliez pas, lors de la création de l'utilisateur, de cocher l'option permettant la génération automatique du certificat associé.



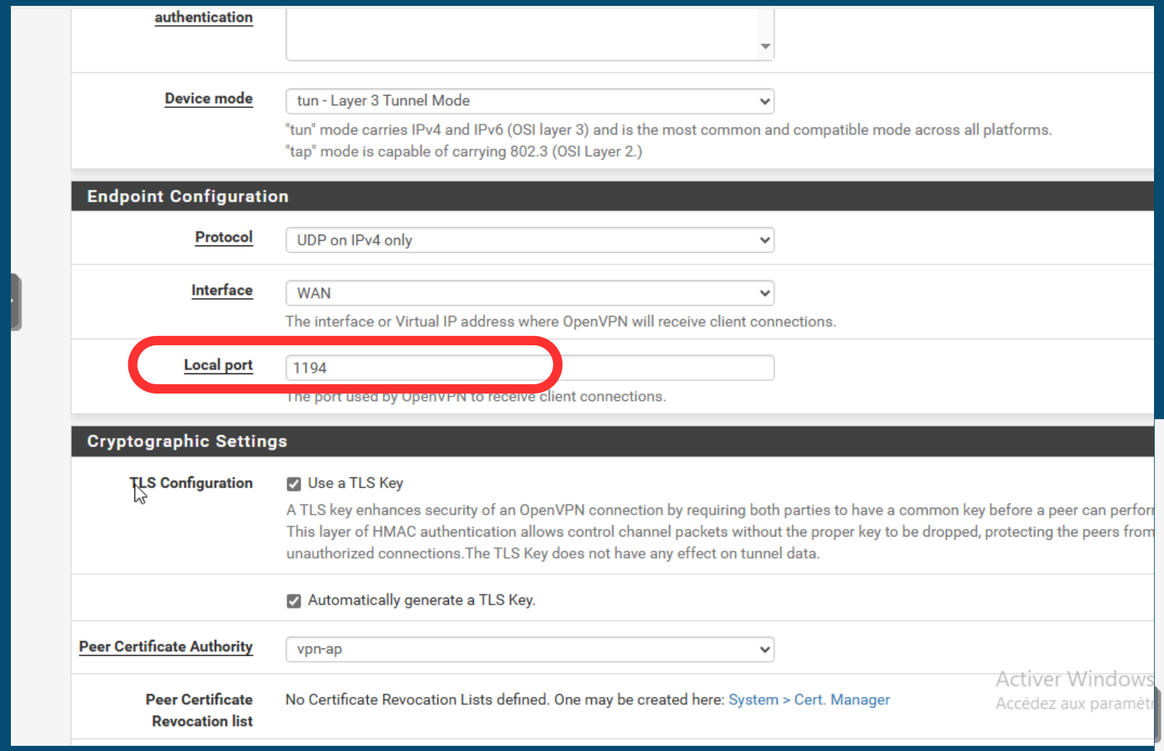


Nous allons maintenant configurer OpenVPN. Pour ce faire, rendez-vous dans la section VPN, puis dans la partie OpenVPN et l'onglet Servers. Cliquez sur Ajouter et configurez les différentes options.

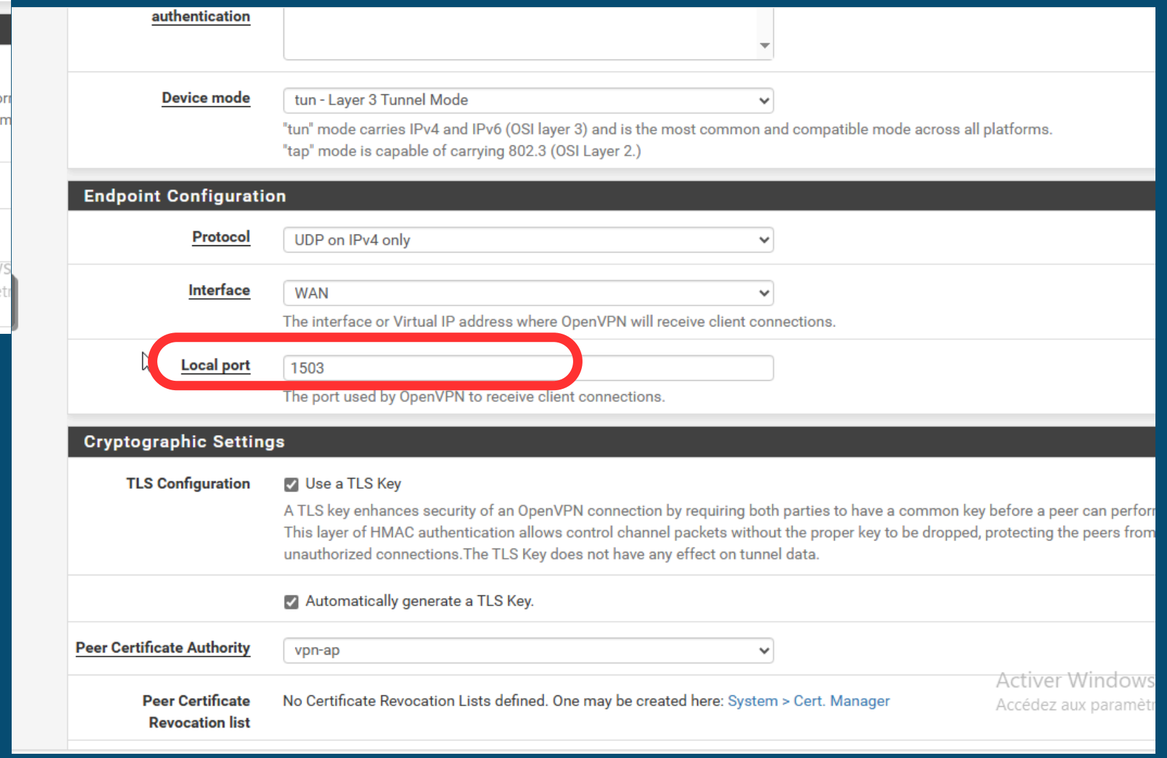
Nous vous conseillons de choisir un mode de serveur avec authentification pour plus de sécurité.

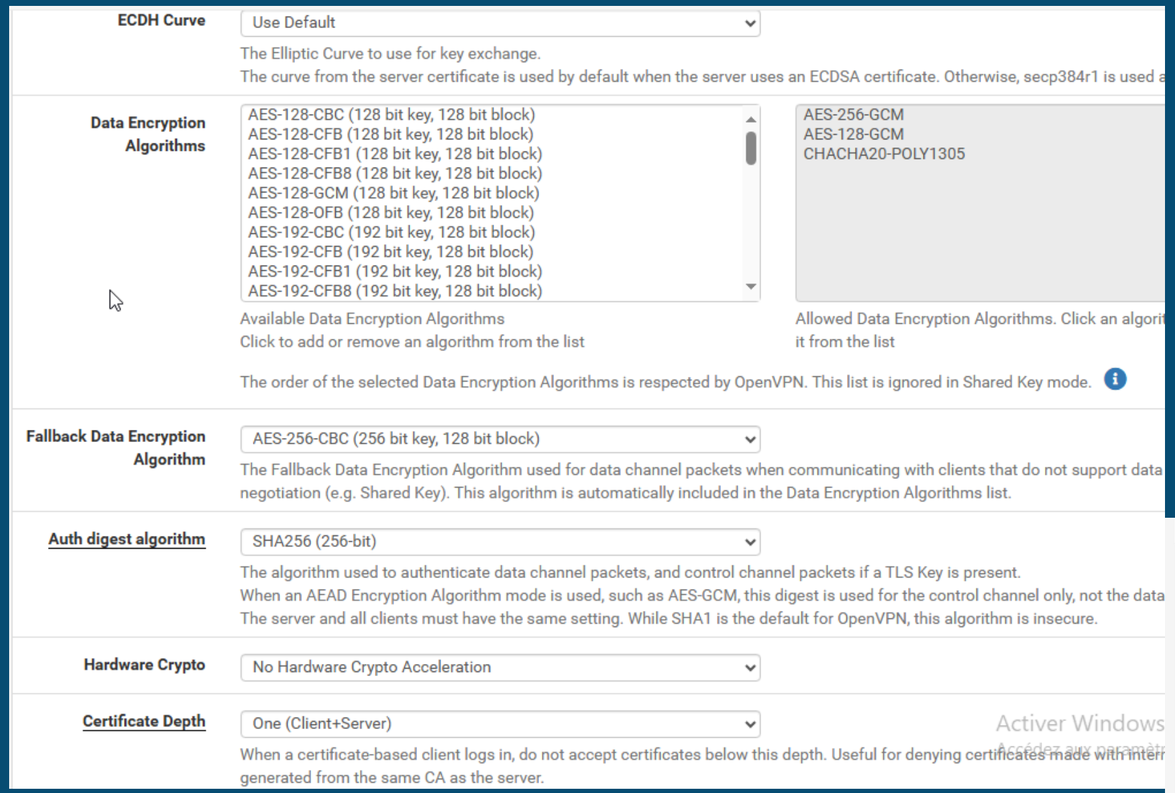


Le port par défaut utilisé par OpenVPN est le port 1194. Pour des raisons de sécurité, nous vous conseillons de le modifier afin de réduire les risques d'attaques potentielles.



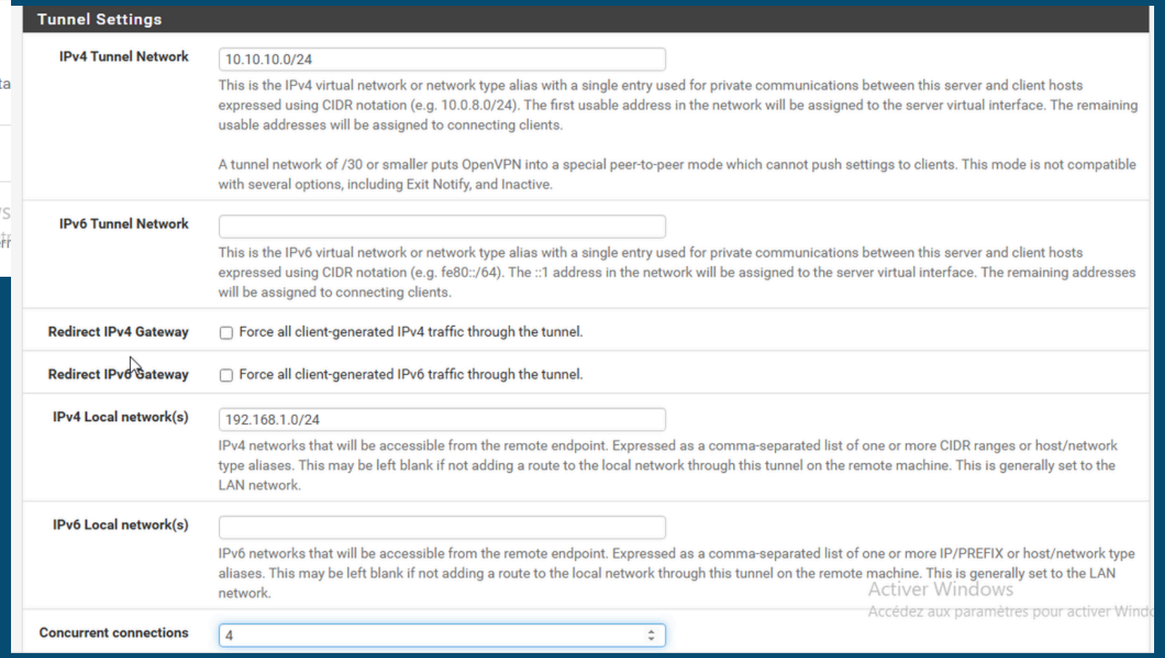
Vous devrez également indiquer l'autorité de certification que vous avez créée, ainsi que le certificat correspondant.

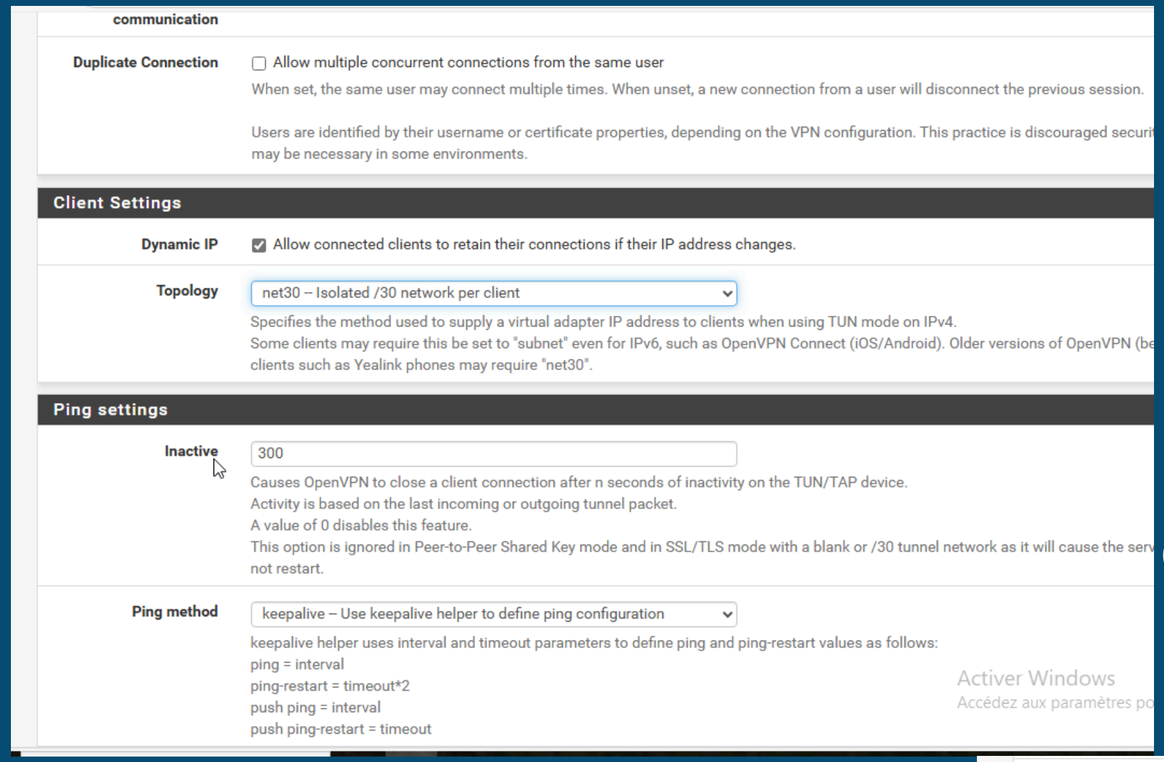




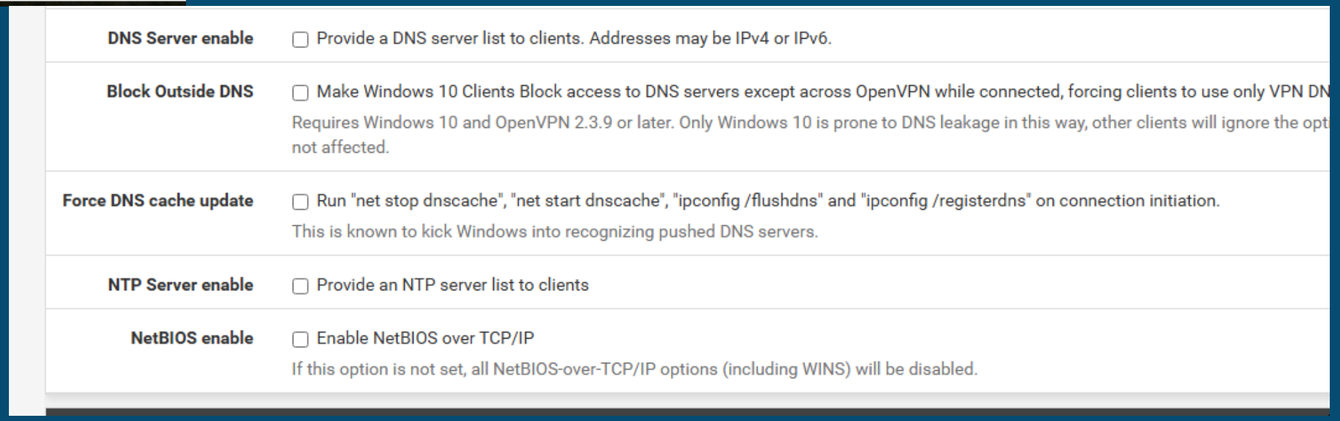
Vous devrez également indiquer le réseau de destination (dans notre cas, le réseau LAN) ainsi que le nombre maximum de connexions VPN autorisées simultanément.

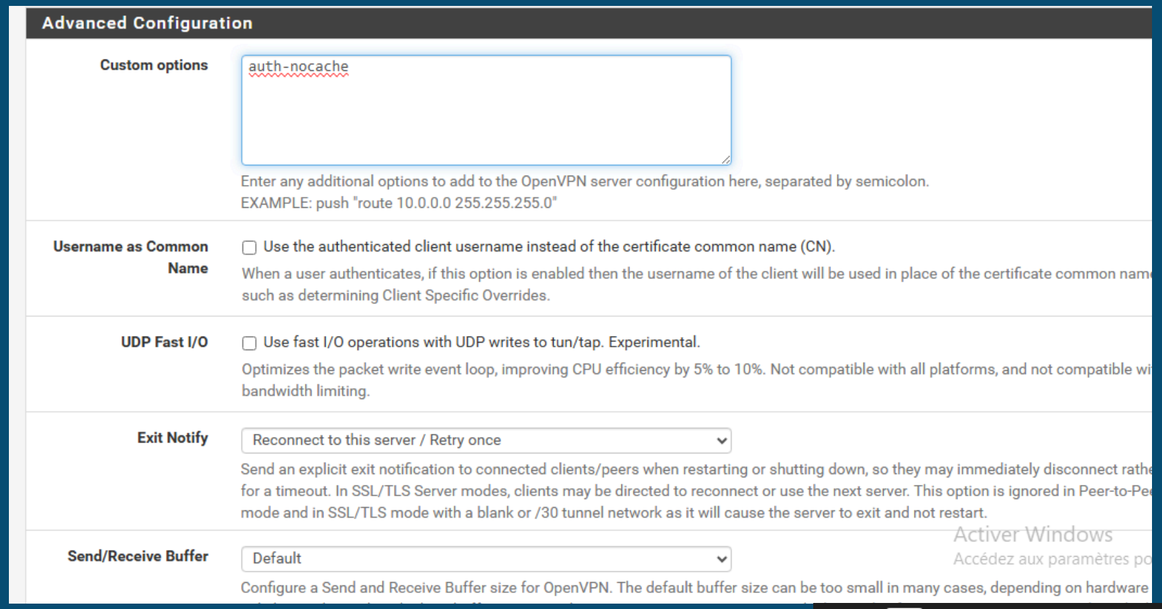
Vous devrez ensuite spécifier l'adresse réseau de votre tunnel. Il s'agit du réseau utilisé pour communiquer avec le poste client. Dans notre exemple, ce sera le réseau 10.10.10.0/24.





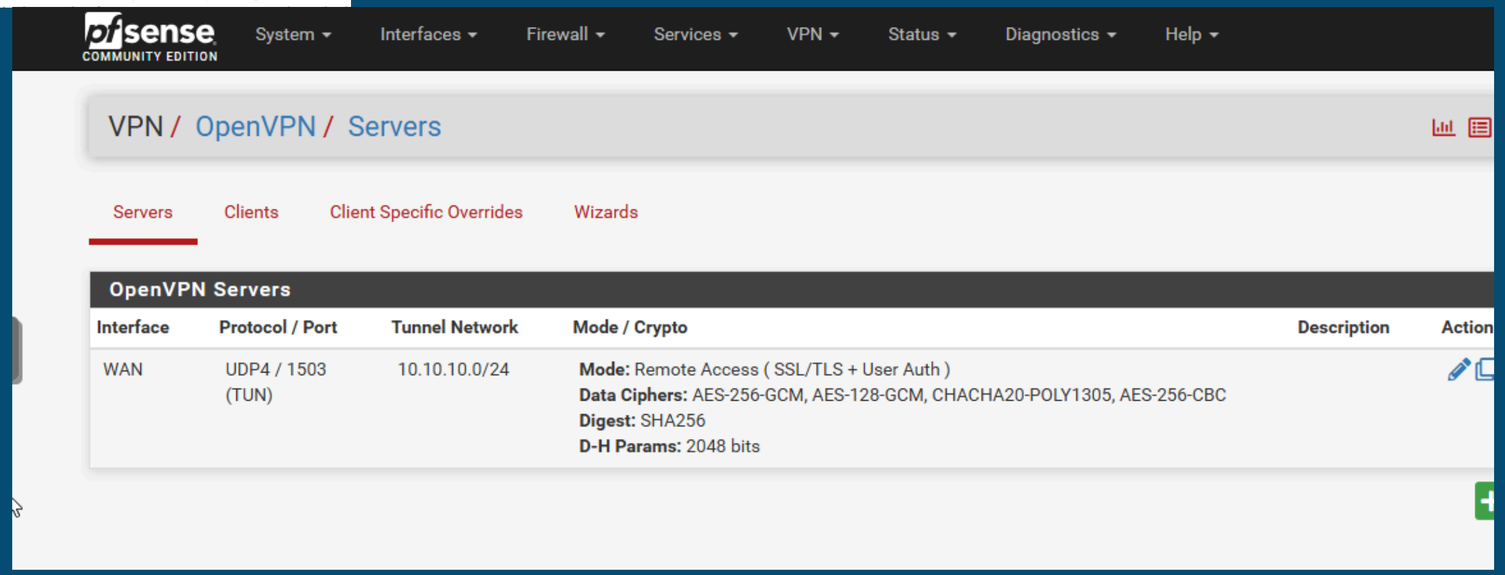
Nous vous conseillons également, au niveau de l'option topology, de choisir l'option que nous avons sélectionnée. Cela empêchera vos clients VPN de communiquer directement avec le reste du réseau.

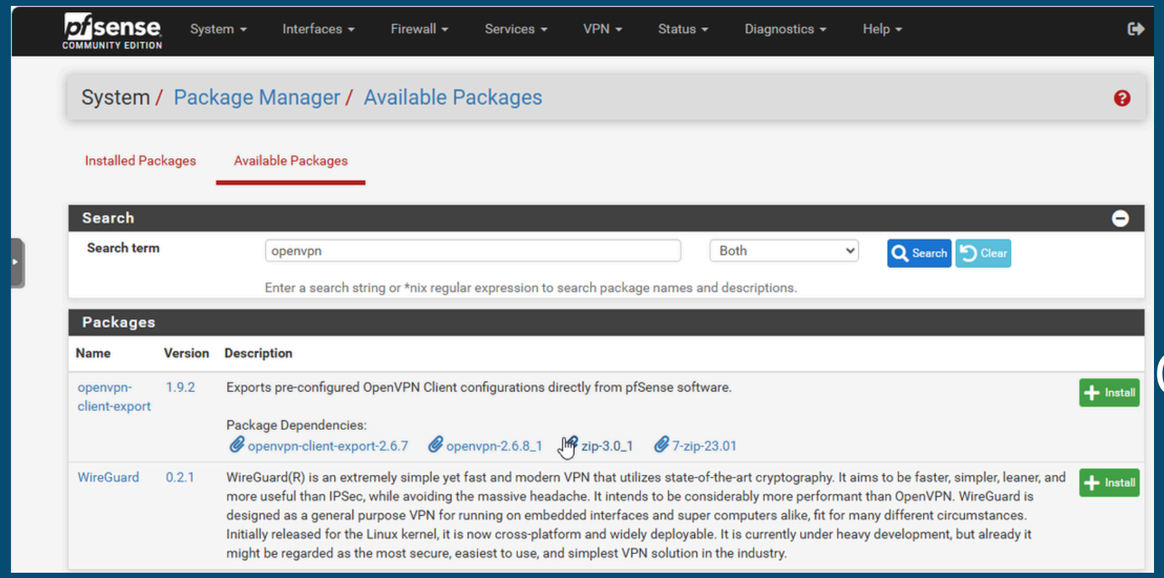




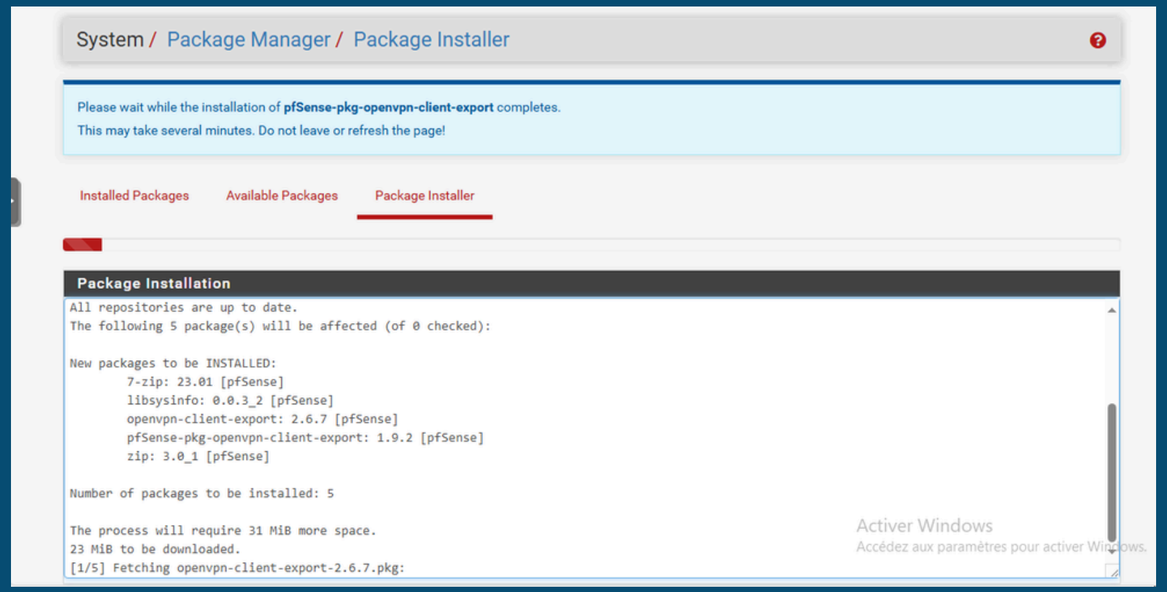
Dans la zone "Custom options", indiquez auth-nocache. Cette option offre une protection supplémentaire contre le vol des identifiants en empêchant leur mise en cache.

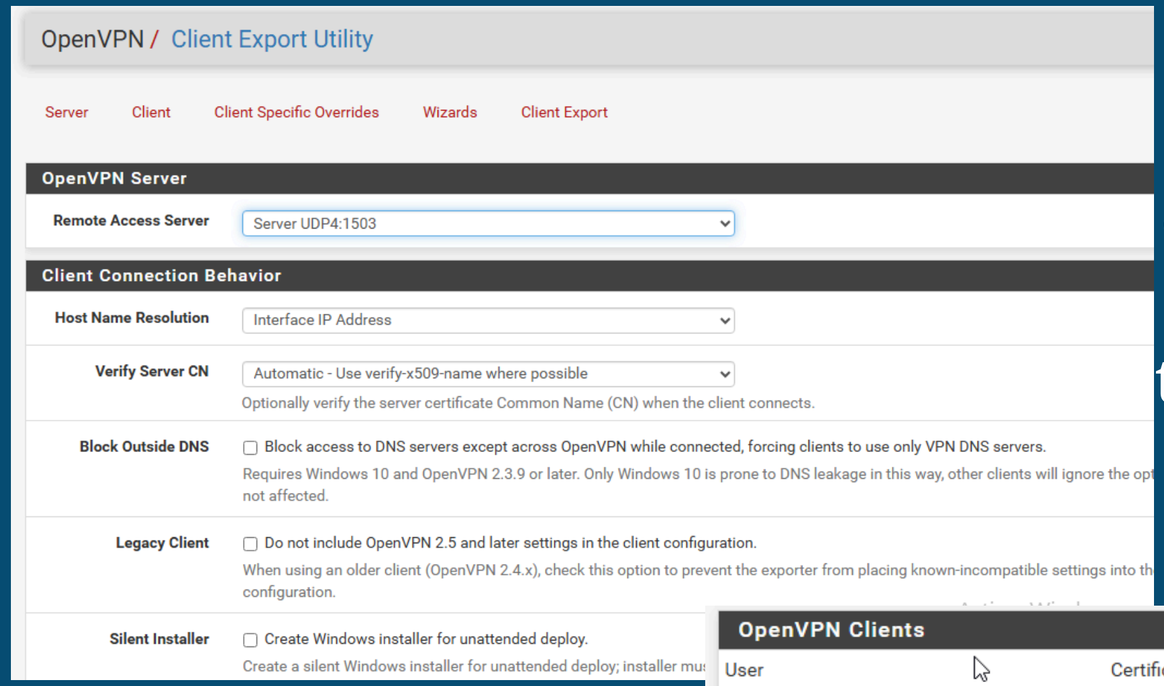
Et voici à quoi cela devrait ressembler une fois la configuration terminée.



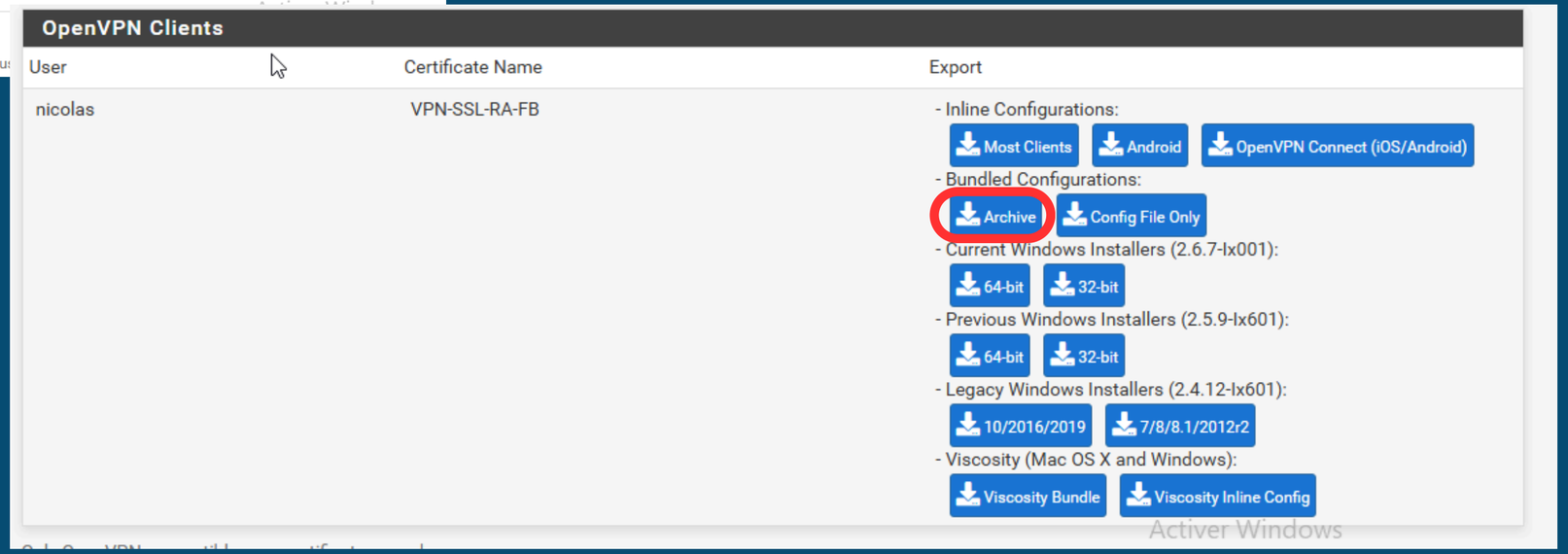


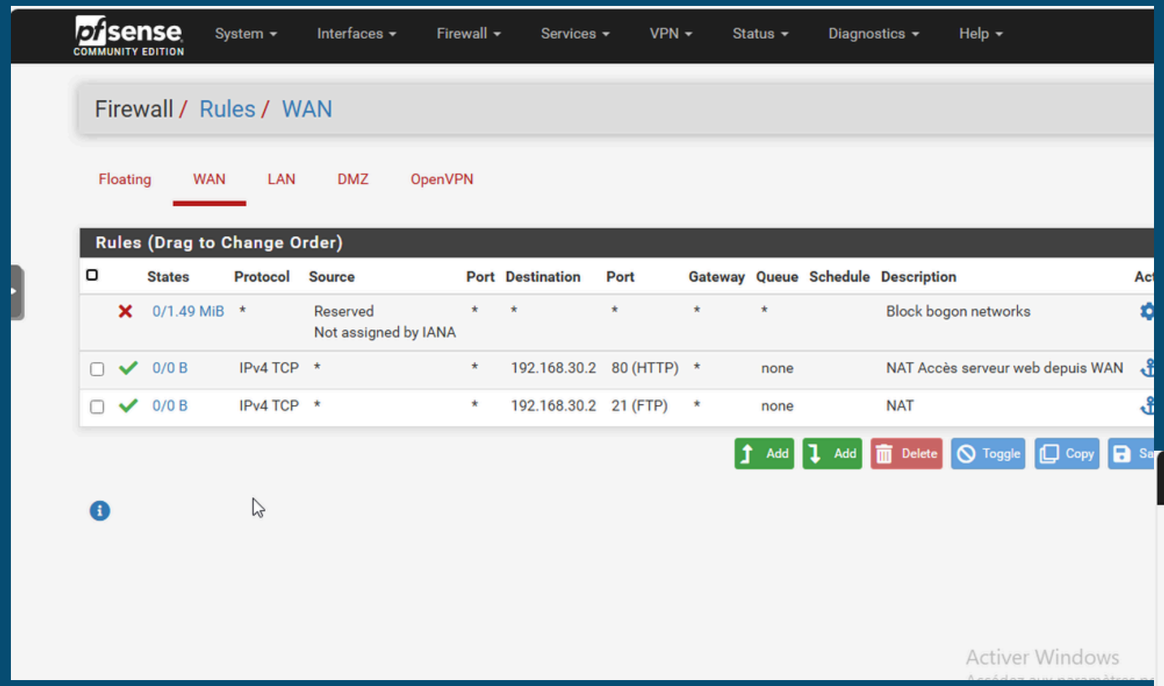
Pour exporter ensuite votre configuration VPN vers votre client, il faudra installer un paquet lié à OpenVPN, appelé openvpn-client-export.



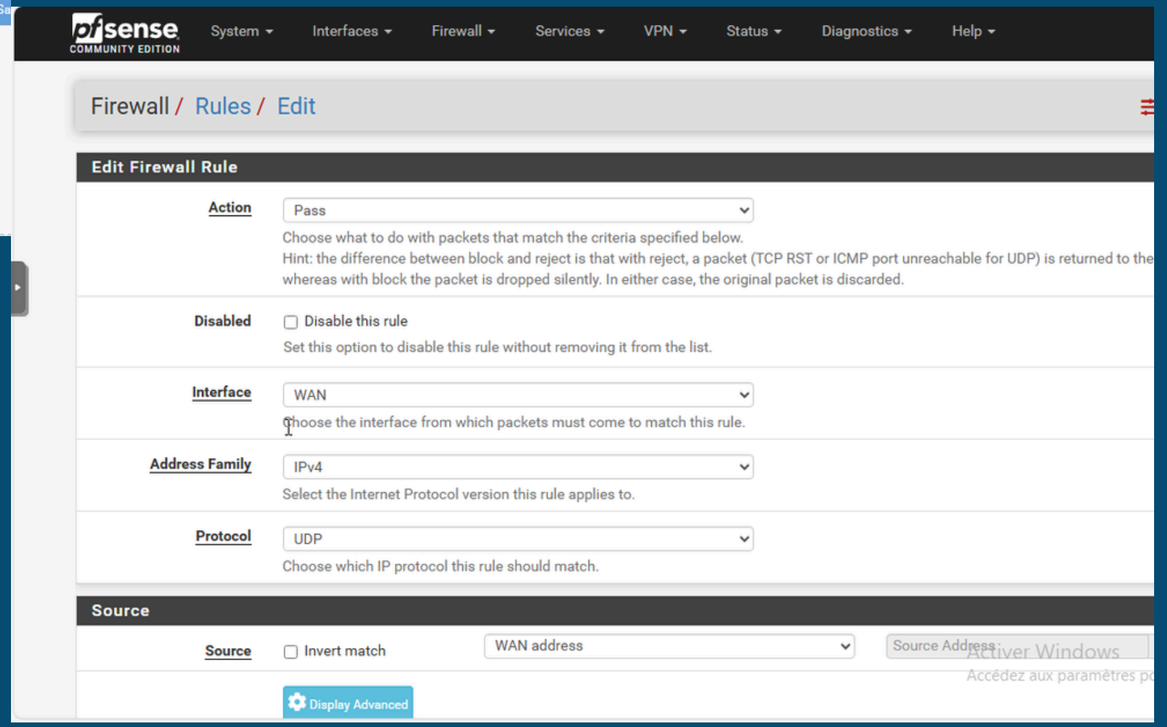


Une fois le paquet installé, retournez dans la section OpenVPN, puis accédez à Client Export Utility. C'est ici que vous trouverez le dossier de configuration à transférer à votre client, dans le dossier Archive de la partie Bundle Configurations.





Nous allons ensuite créer une règle afin d'autoriser les flux OpenVPN venant du WAN. Pour cela, suivez les paramètres indiqués sur nos captures d'écran.



Destination

Destination — Invert match — Any — Destination Address

Destination Port Range — OpenVPN (1194) — From — Custom — OpenVPN (1194) — To — Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log — Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslo
the Status: System Logs: Settings page).

Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in
log.

Advanced Options — Display Advanced

Save

pfSense COMMUNITY EDITION — System — Interfaces — Firewall — Services — VPN — Status — Diagnostics — Help

Firewall / Rules / WAN

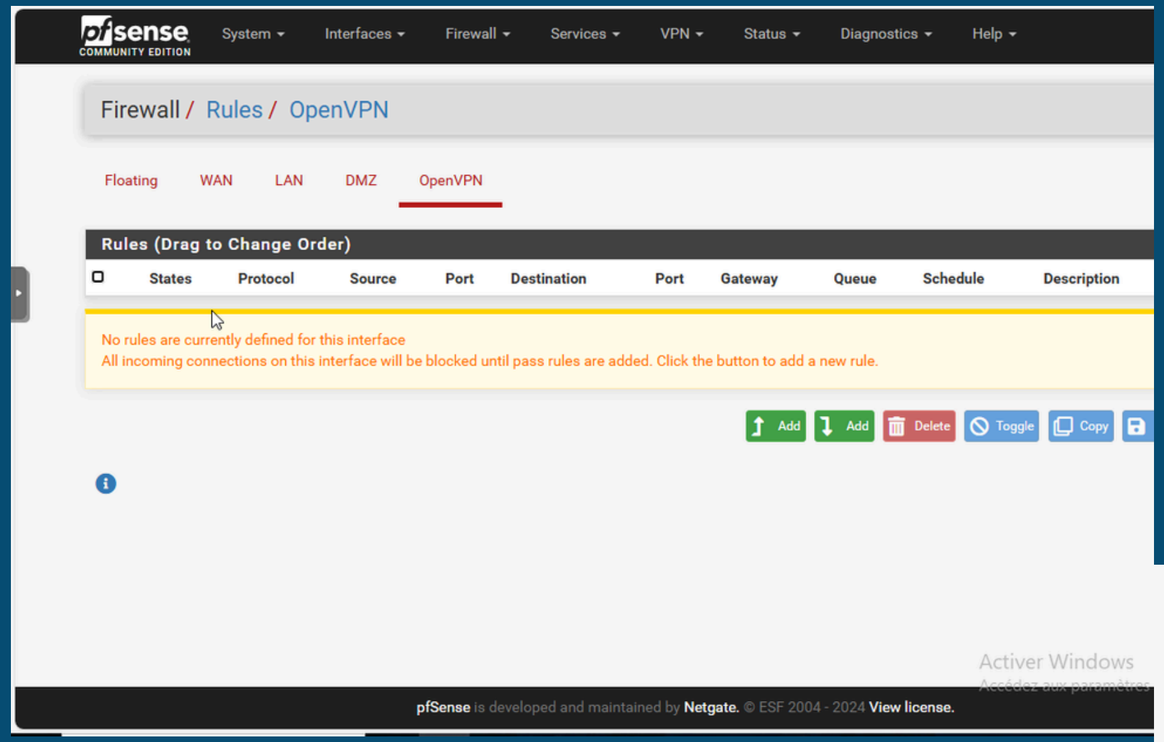
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

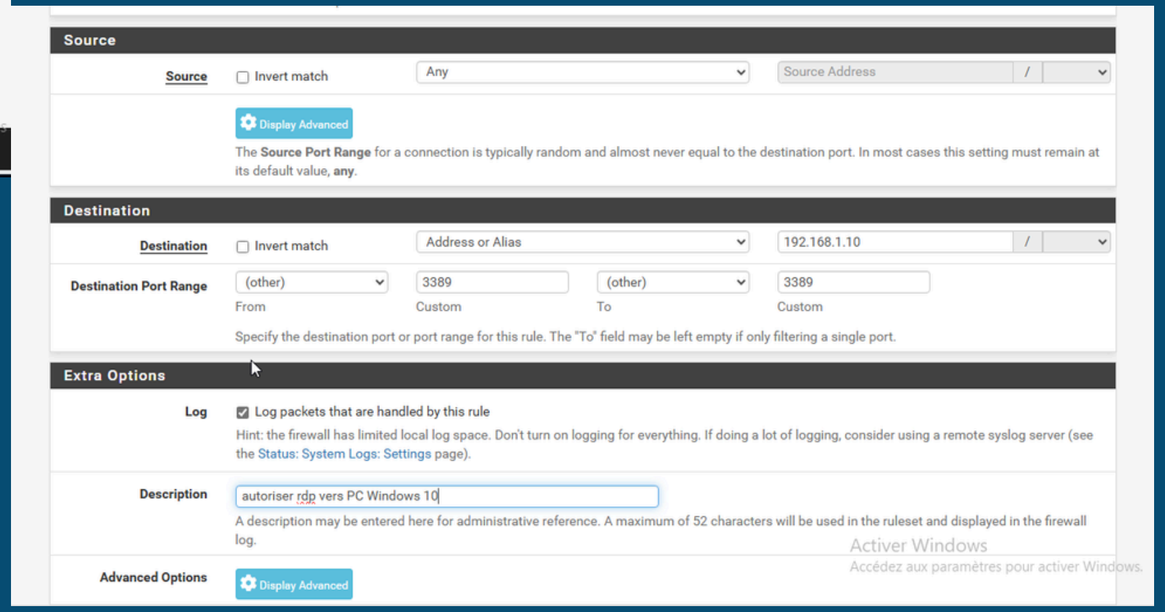
Floating | WAN | LAN | DMZ | OpenVPN

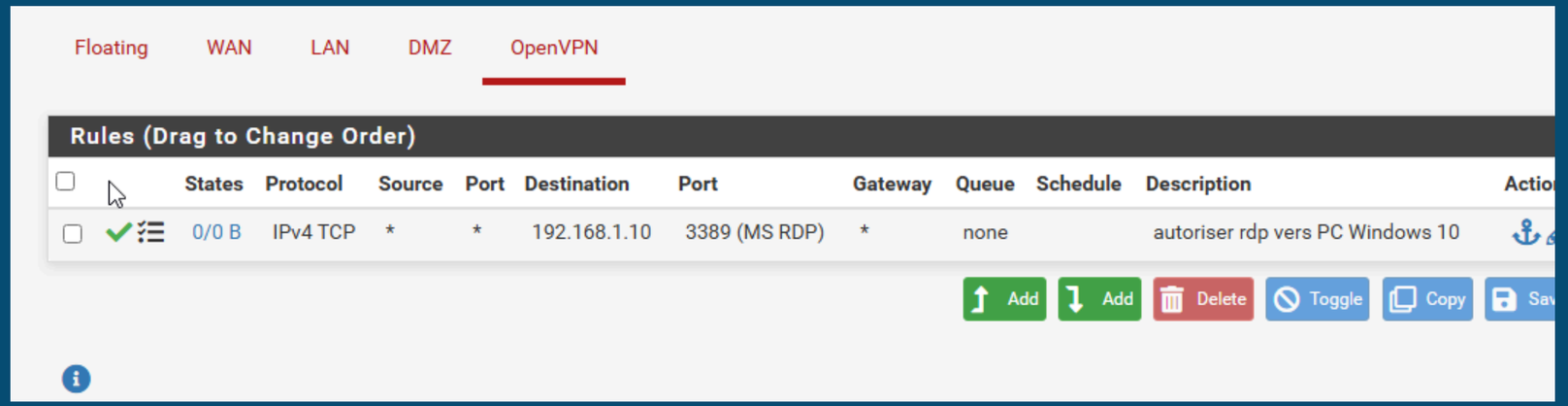
Rules (Drag to Change Order)

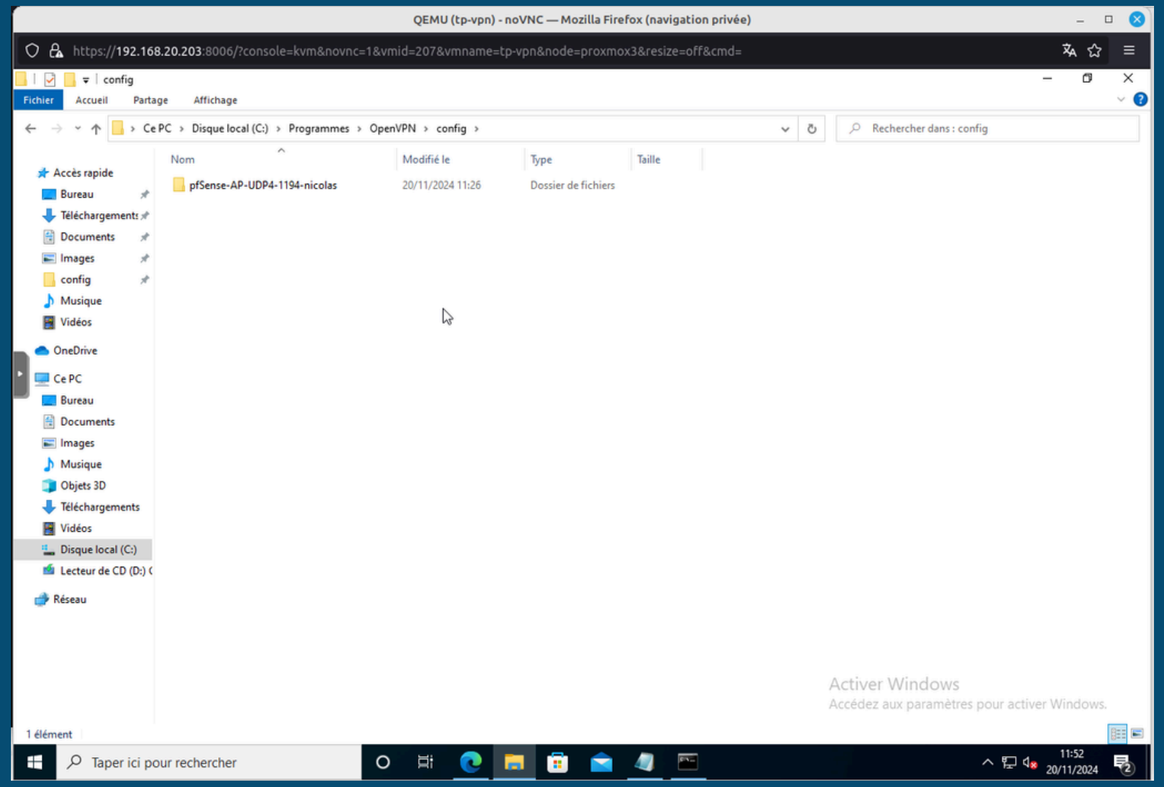
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/1.54 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
0/0 B	IPv4 TCP	*	*	192.168.30.2	80 (HTTP)	*	none		NAT Accès serveur web depuis WAN	
0/0 B	IPv4 TCP	*	*	192.168.30.2	21 (FTP)	*	none		NAT	
0/0 B	IPv4 UDP	WAN address	*	*	1194 (OpenVPN)	*	none			

Add | Add | Delete | Toggle | Copy | Save | Separator

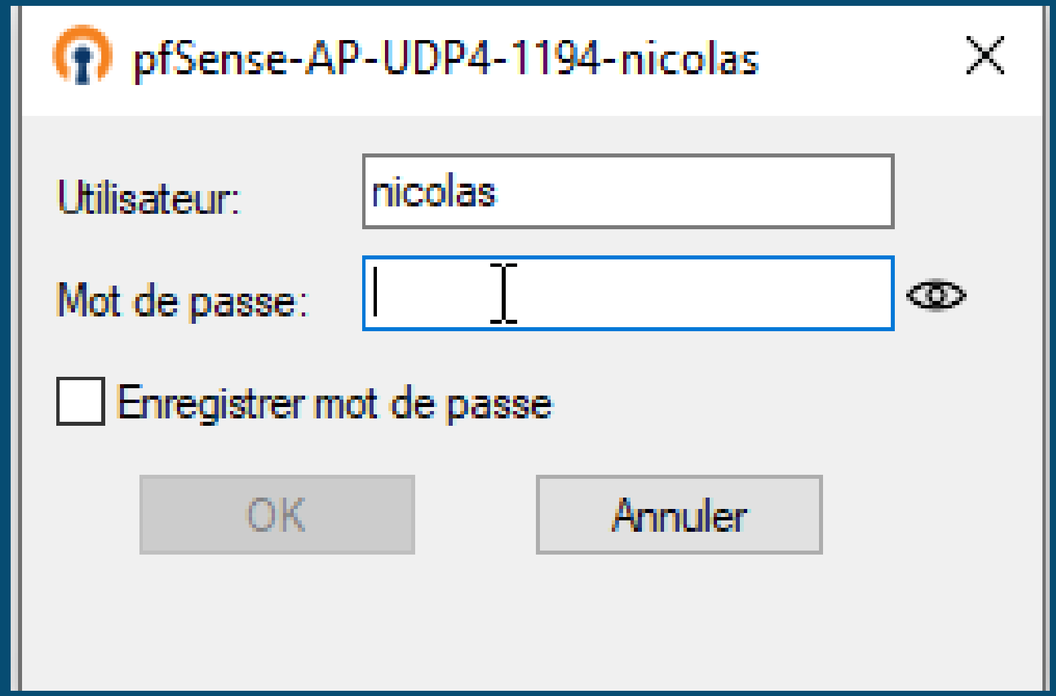

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / OpenVPN
Floating
WAN
LAN
DMZ
OpenVPN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.
Add
Add
Delete
Toggle
Copy
Activer Windows
Accédez aux paramètres
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

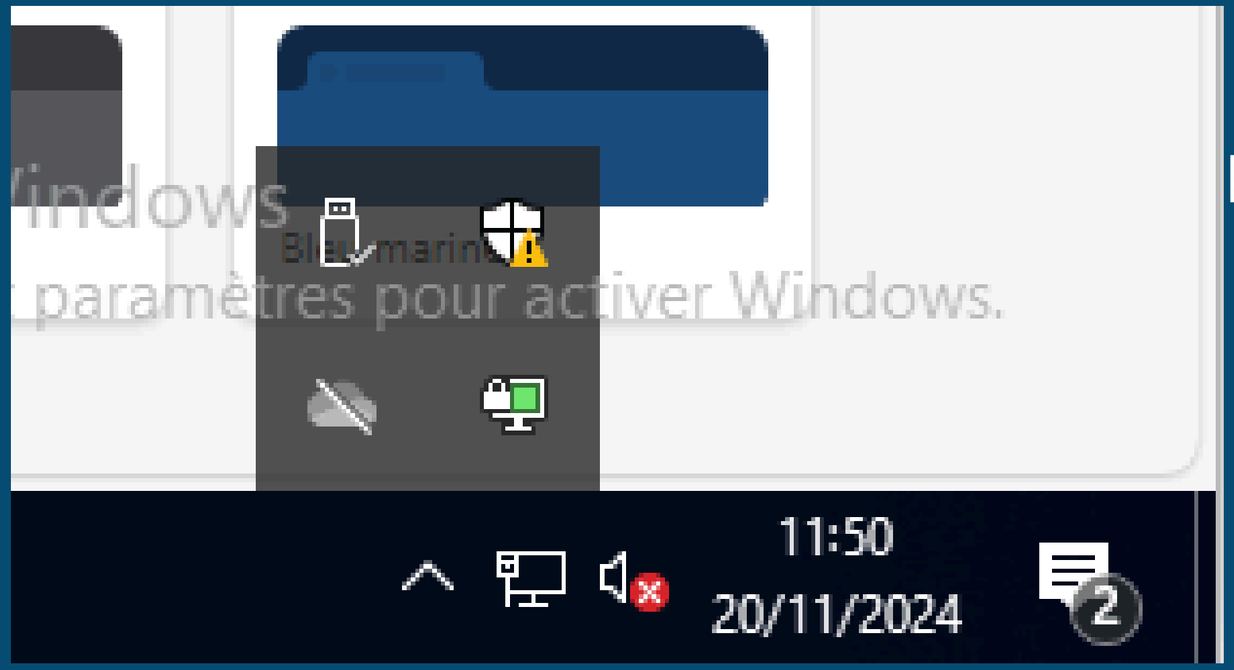

Source
Source
Invert match
Any
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
Address or Alias
192.168.1.10
Destination Port Range
(other)
3389
From
Custom
(other)
3389
To
Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
autoriser rdp vers PC Windows 10
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options
Display Advanced
Activer Windows
Accédez aux paramètres pour activer Windows.


Floating
WAN
LAN
DMZ
OpenVPN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actio
0/0 B
IPv4 TCP
*
*
192.168.1.10
3389 (MS RDP)
*
none
autoriser rdp vers PC Windows 10
Add
Add
Delete
Toggle
Copy
Sav



Une fois toutes vos configurations effectuées, intégrez votre dossier de configuration sur votre client (après avoir installé le client OpenVPN). Placez-le dans le dossier config d'OpenVPN, puis testez la connexion.





Si votre connexion est réussie, une petite icône en forme d'écran passera au vert. De plus, si vous effectuez un ipconfig, vous verrez une adresse IP correspondant au réseau de votre tunnel, celle que vous avez configurée précédemment.

```
Carte inconnue OpenVPN TAP-Windows6 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::2907:84ec:36a6:e13d%11
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.10.6
   Masque de sous-réseau. . . . . . . . . : 255.255.255.252
   Passerelle par défaut. . . . . . . . . :

Carte inconnue OpenVPN Data Channel Offload :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

C:\Users\Client>
```