



Configuration d'un VPN d'accès entre un client Windows et PFsense (OpenVPN)

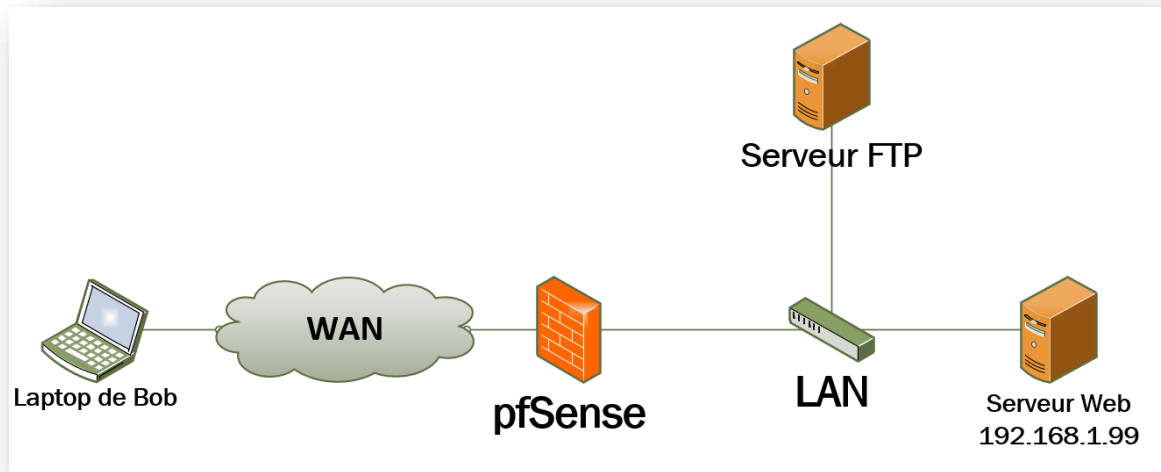
23 septembre 2021

Table des matières

1	Topologie	3
2	Installation du serveur OpenVPN	4
3	Configuration du serveur OpenVPN	7
4	Installation le client OpenVPN.....	20
5	Configuration du client OpenVPN	24

1 Topologie

Voici la topologie qui va nous permettre de réaliser un tunnel VPN en utilisant OpenVPN.

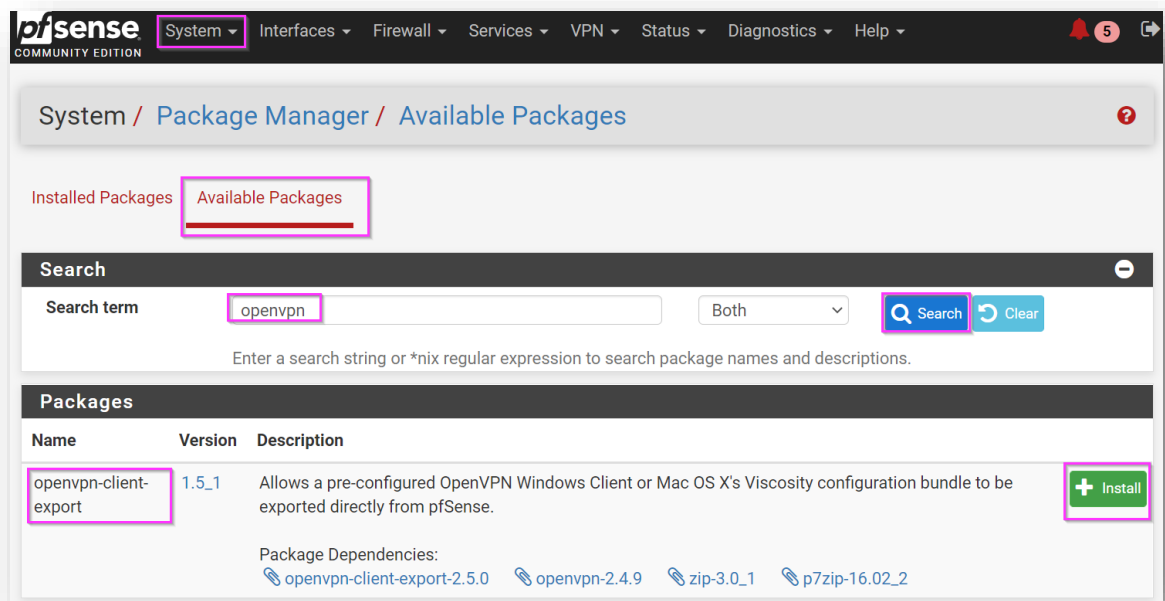


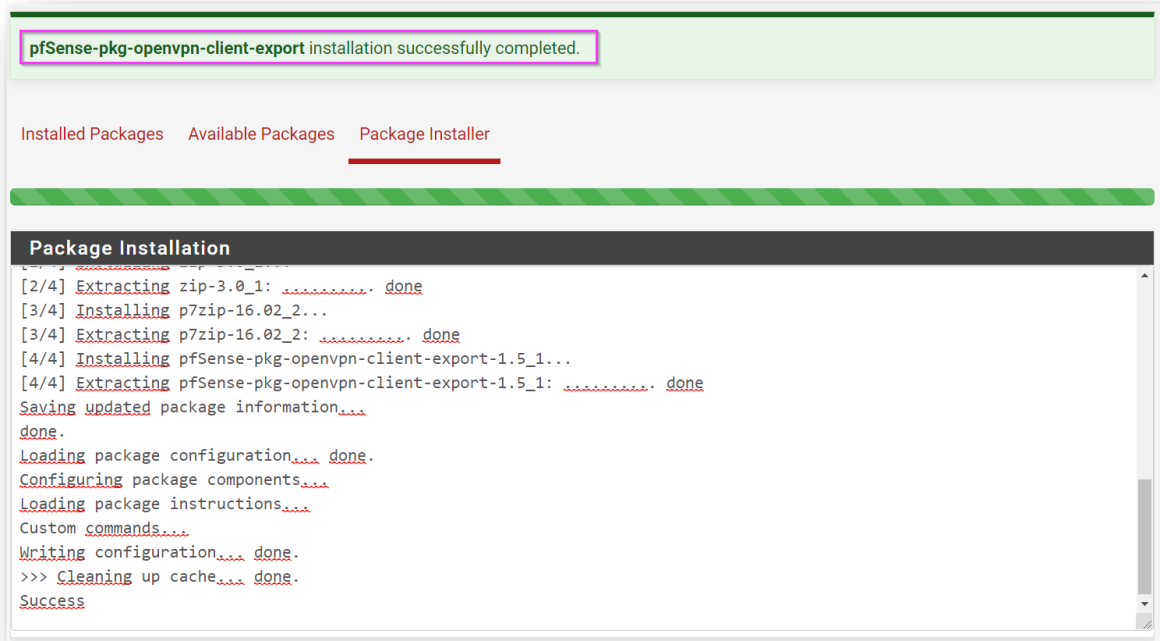
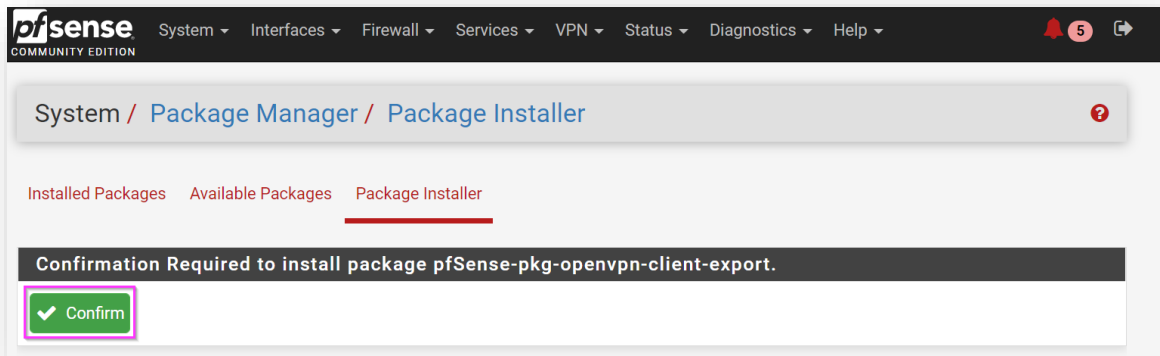
2 Installation du serveur OpenVPN

Nous allons d'abord installer le paquet **openvpn-client-export**.

Ce plugin de PfSense permet d'exporter les clients VPN sous forme de fichier exécutable pouvant être installé sur une machine client. Ce plugin est très pratique, car le VPN s'installera avec toutes les configurations nécessaires.

Pour ce faire, allez dans le menu **System** puis ouvrez **Package Manager**.













Installed Packages

Available Packages

Installed Packages

Name	Category	Version	Description	Actions
✓ openvpn-client-export	security	1.5_1	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	 

Package Dependencies:

 openvpn-client-export-2.5.0  openvpn-2.4.9  zip-3.0_1  p7zip-16.02_2 = Update ✓ = Current = Remove  = Information  = Reinstall

Newer version available

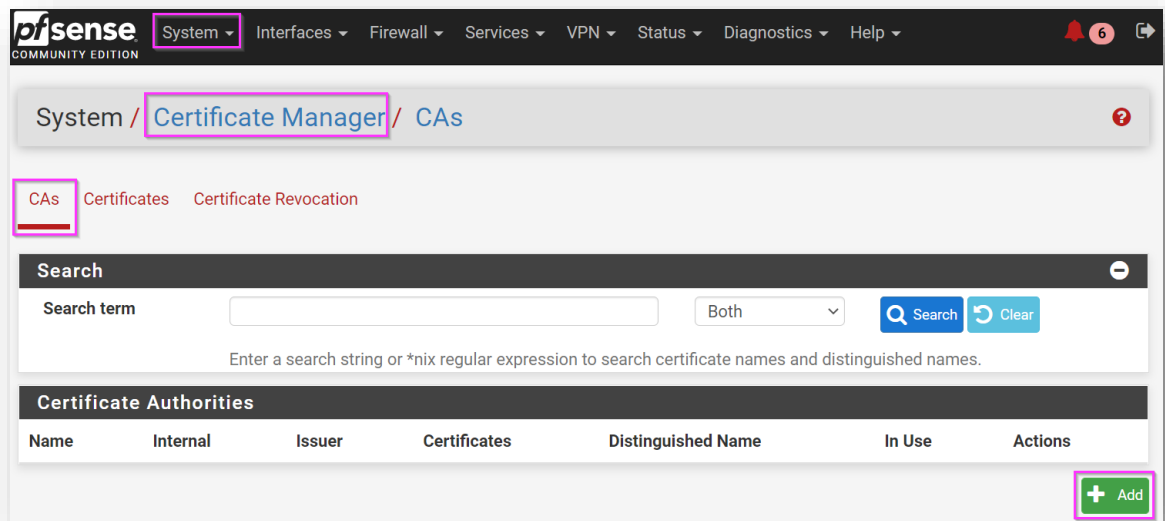
Package is configured but not (fully) installed or deprecated

3 Configuration du serveur OpenVPN

Comme OpenVPN fonctionne avec des certificats SSL pour chiffrer les échanges, il est nécessaire de configurer une autorité de certification (CA) qui nous permettra de générer tous les certificats de nos clients VPN.

Allez dans le menu **System** puis ouvrez **Certificate Manager**.

Cliquez sur **Add**.



Créez une nouvelle autorité de certification comme suit.

System / [Certificate Manager](#) / [CAs](#) / [Edit](#) ?

[CAs](#) [Certificates](#) [Certificate Revocation](#)

Create / Edit CA

Descriptive name

Method

Internal Certificate Authority

Key length (bits)

Digest Algorithm
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days)

Common Name

The following certificate authority subject components are optional and may be left blank.

Country Code

State or Province

City

Organization

Organizational Unit

Search

Search term

Both



Search



Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
orabec_ca	<input checked="" type="checkbox"/>	self-signed	0	ST=Québec, OU=TI, O=Orabec, L=Montréal, CN=internal-ca, C=CA Valid From: Fri, 13 Nov 2020 01:45:16 +0000 Valid Until: Mon, 11 Nov 2030 01:45:16 +0000		

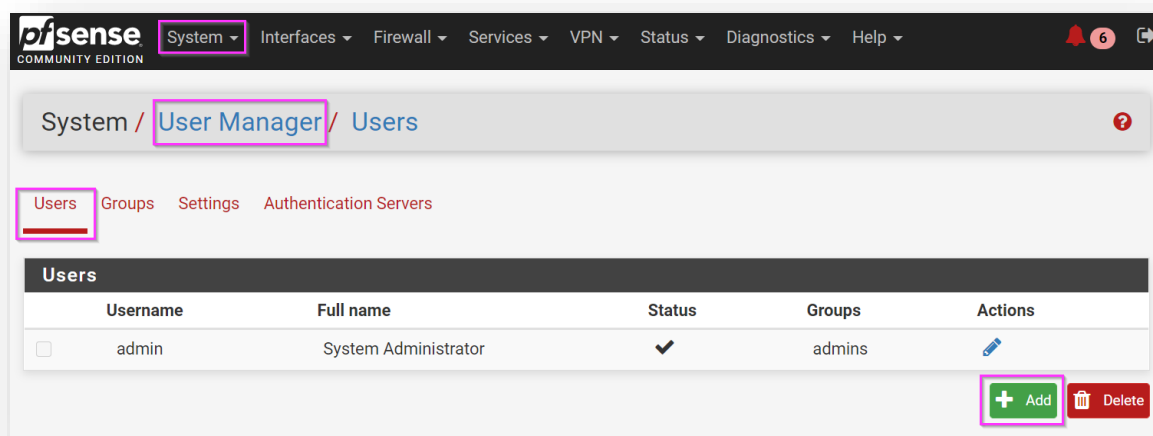


Add

L'authentification des utilisateurs du VPN peut se faire de plusieurs façons. Dans notre exemple, nous allons créer des comptes utilisateurs directement sur la passerelle PFSense.

Nous allons maintenant créer notre premier utilisateur VPN.

Allez dans le menu **System** puis ouvrez **User Manager**.



Cliquez sur **Add**.

Créez l'utilisateur Bob comme suit.

User Properties

Defined by: USER

Disabled: ☐ This user cannot login

Username: bob

Password: [masked]

Full name: Bob l'éponge
User's full name, for administrative information only

Expiration date: [blank]
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings: ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership: admins (Not member of) | [blank] (Member of)

Buttons: >> Move to "Member of" list, << Move to "Not member of" list
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate: ☒ Click to create a user certificate

Create Certificate for User

Descriptive name: Certificat Bob

Certificate authority: orabec_ca

Key length: 2048 bits
The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com.

Lifetime: 3650

Keys

Authorized SSH Keys

Enter authorized SSH keys for this user

IPsec Pre-Shared Key

Save

System / User Manager / Users

Users

Groups

Settings

Authentication Servers

Users

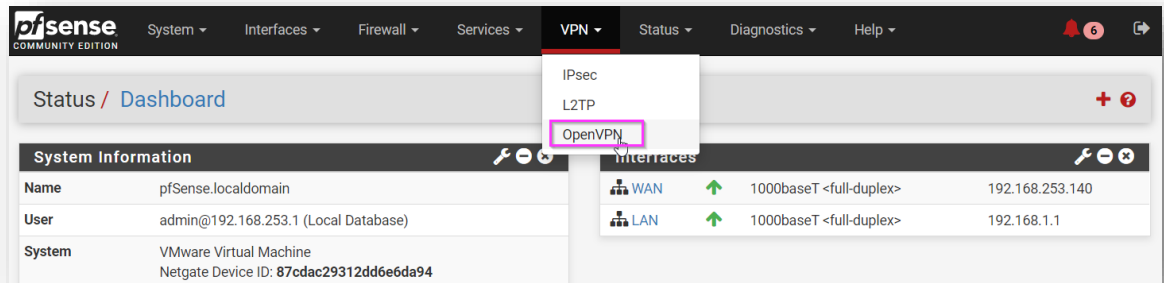
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	bob	Bob l'éponge	✓		

+ Add

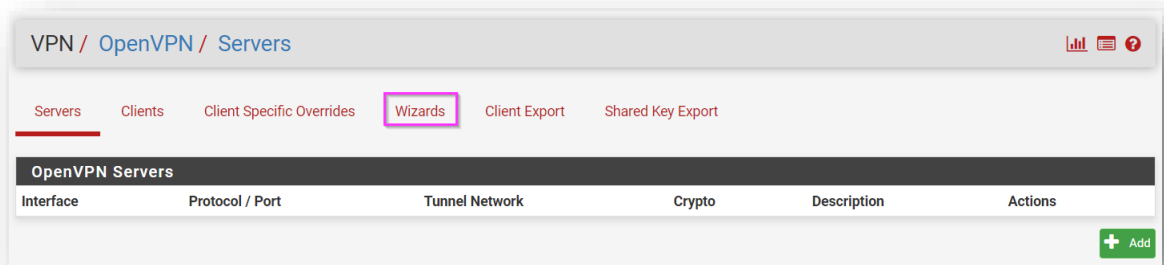
Delete

Nous allons maintenant activer le serveur OpenVPN pour qu'il accepte les connexions.

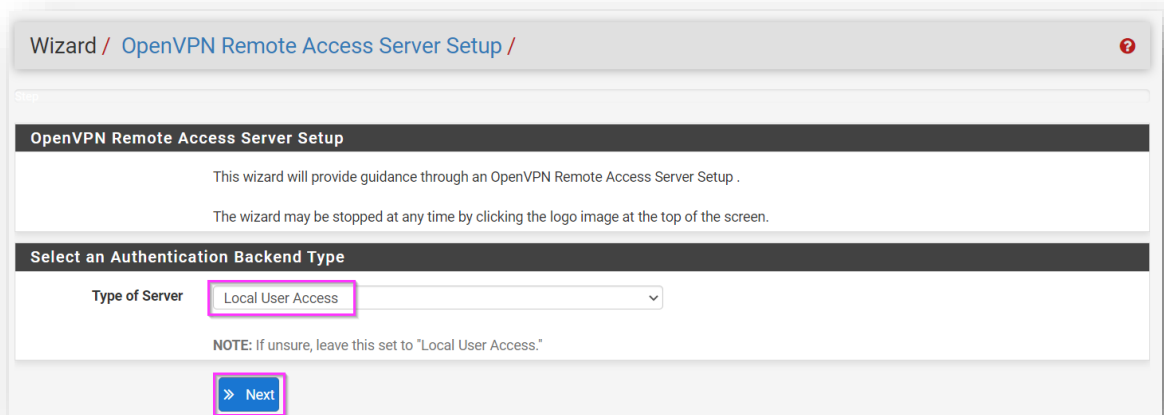
Allez dans le menu **VPN**, puis ouvrez **OpenVPN**.



Cliquez sur **Wizards**



Créez le VPN comme suit :



Sélectionnez l'autorité de certification :

The screenshot shows the 'Certificate Authority Selection' step (Step 5 of 11) of the 'OpenVPN Remote Access Server Setup Wizard'. The breadcrumb trail at the top reads 'Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection'. Below the title bar, a red progress bar indicates 'Step 5 of 11'. The main heading is 'Certificate Authority Selection', followed by the subtitle 'OpenVPN Remote Access Server Setup Wizard'. The section 'Choose a Certificate Authority (CA)' contains a dropdown menu labeled 'Certificate Authority' with 'orabec_ca' selected. At the bottom, there are two buttons: '» Add new CA' and '» Next'. The 'Next' button is highlighted with a pink rectangle.

Créer le certificat du serveur d'accès OpenVPN (pfsense)

The screenshot shows the 'Server Certificate Selection' step (Step 7 of 11) of the 'OpenVPN Remote Access Server Setup Wizard'. The breadcrumb trail at the top reads 'Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection'. Below the title bar, a red progress bar indicates 'Step 7 of 11'. The main heading is 'Server Certificate Selection', followed by the subtitle 'OpenVPN Remote Access Server Setup Wizard'. The section 'Choose a Server Certificate' contains a dropdown menu labeled 'Certificate' with 'Certificat Bob' selected. At the bottom, there are two buttons: '» Add new Certificate' and '» Next'. The 'Add new Certificate' button is highlighted with a pink rectangle.

Add a Server Certificate

OpenVPN Remote Access Server Setup Wizard

Create a New Server Certificate

Descriptive name

pfsense OpenVPN

A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."

Key length

2048 bit

Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime

398

Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Country Code

CA

Two-letter ISO country code (e.g. US, AU, CA)

State or Province

Québec

Full State of Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City

Montréal

City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organization

Orabec

Organization name, often the Company or Group name.

» Create new Certificate

Configuration du serveur d'accès OpenVPN

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Interface	WAN
The interface where OpenVPN will listen for incoming connections (typically WAN.)	
Protocol	UDP on IPv4 only
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.	
Local Port	1194
Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.	
Description	
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.	

Cryptographic Settings

TLS Authentication	<input checked="" type="checkbox"/>
Enable authentication of TLS packets.	
Generate TLS Key	<input checked="" type="checkbox"/>
Automatically generate a shared TLS authentication key.	
TLS Shared Key	<div></div>
Paste in a shared TLS key if one has already been generated.	
DH Parameters Length	2048 bit
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.	
Encryption Algorithm	AES-128-CBC (128 bit key, 128 bit block)
The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.	
Auth Digest Algorithm	SHA256 (256-bit)
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.	
Hardware Crypto	No Hardware Crypto Acceleration
The hardware cryptographic accelerator to use for this VPN connection, if any.	

Tunnel Settings

Tunnel Network 10.10.10.0/24

This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

Redirect Gateway

☐

Force all client generated traffic through the tunnel.

Local Network 192.168.1.0/24

This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. 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.

Compression

Omit Preference (Use OpenVPN Default) ▼

Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.

Type-of-Service

☐

Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.

**Inter-Client
Communication**

☐

Allow communication between clients connected to this server.

Duplicate Connections

☐

Allow multiple concurrent connections from clients using the same Common Name.
NOTE: This is not generally recommended, but may be needed for some scenarios.

Client Settings

Dynamic IP

☒

Allow connected clients to retain their connections if their IP address changes.

Topology

Subnet -- One IP address per client in a common subnet ▼

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".

DNS Default Domain

orabec.com

Provide a default domain name to clients.

DNS Server 1

8.8.8.8

DNS server IP to provide to connecting clients.

» Next

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule ☒

Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule ☒

Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

» Next

Step 11 of 11

Finished!





OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

The configuration is now complete.

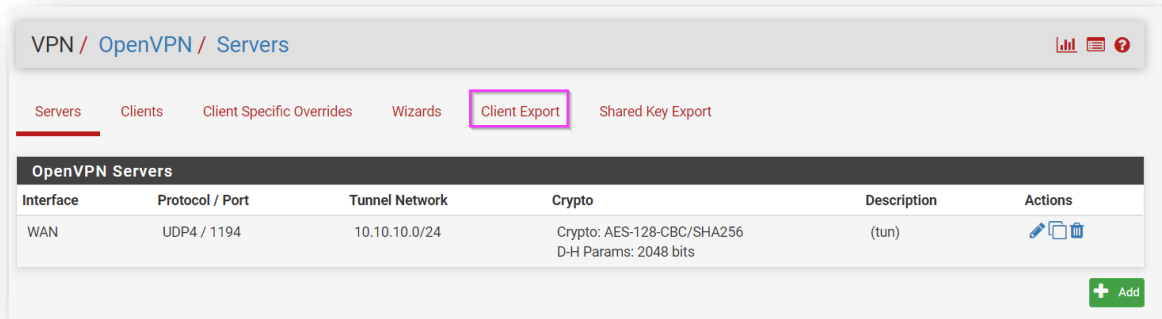
To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

» Finish

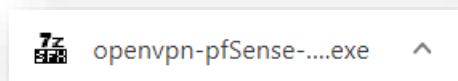
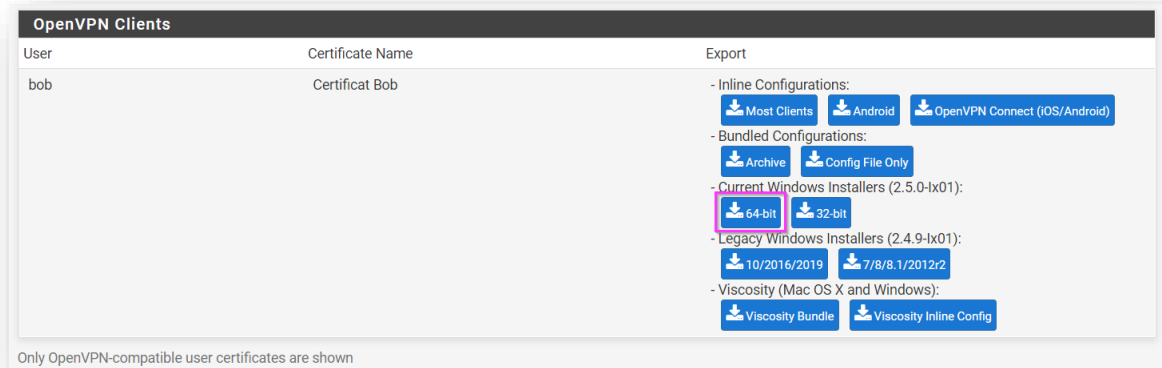
Servers	Clients	Client Specific Overrides	Wizards	Client Export	Shared Key Export
OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	10.10.10.0/24	Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits	(tun)	  
					 Add

Nous pouvons maintenant installer les clients OpenVPN.

Pour ce faire, rendez-vous dans Client Export.

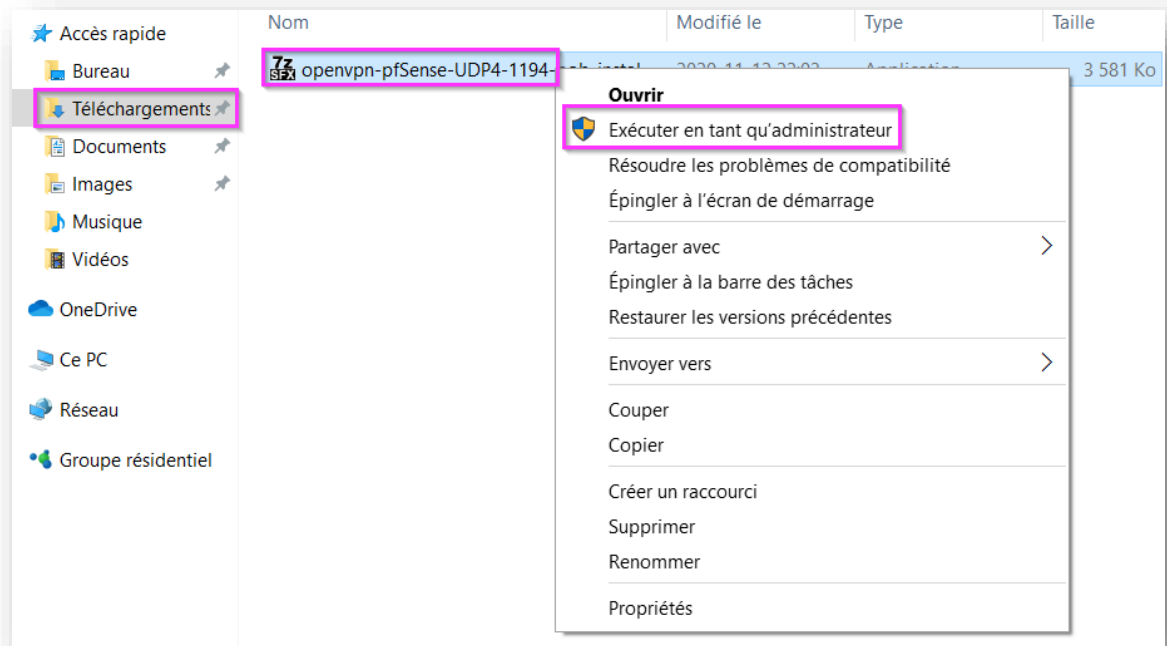


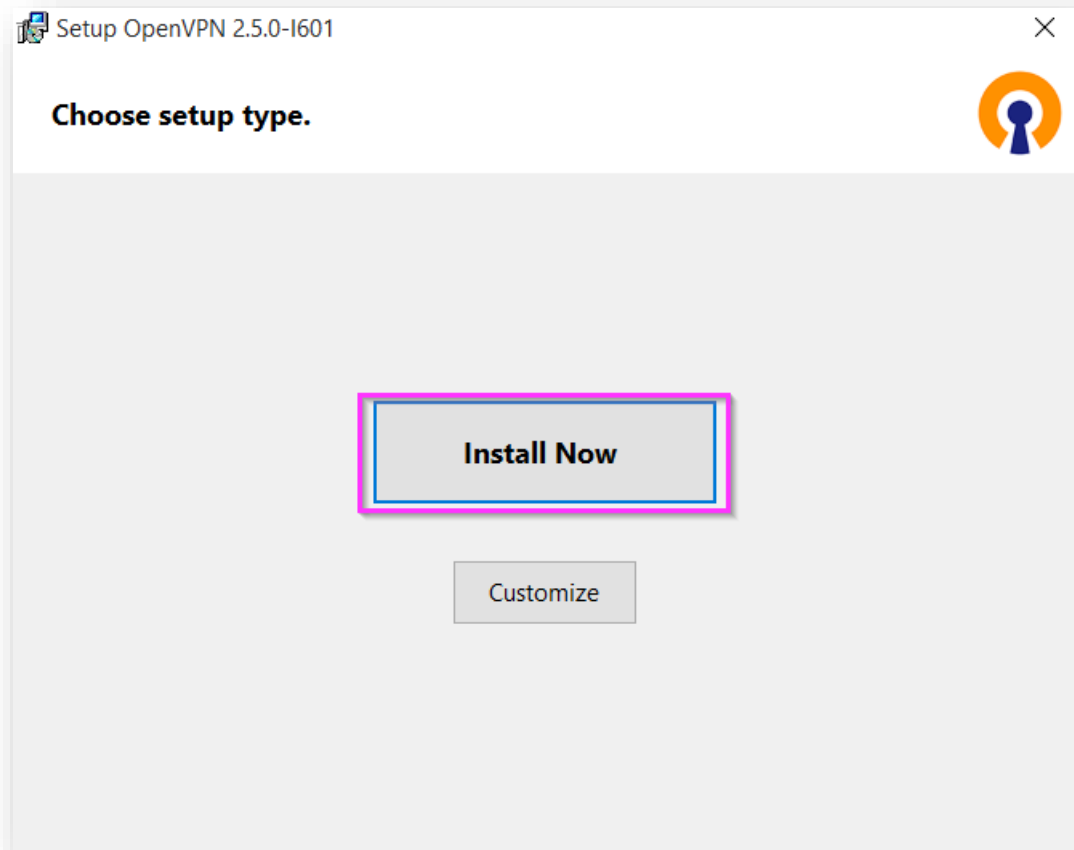
Dans le bas de la fenêtre, téléchargez le client VPN préconfiguré pour l'utilisateur **Bob** puis copiez-le sur une machine Windows 10 distante (Réseau NAT).

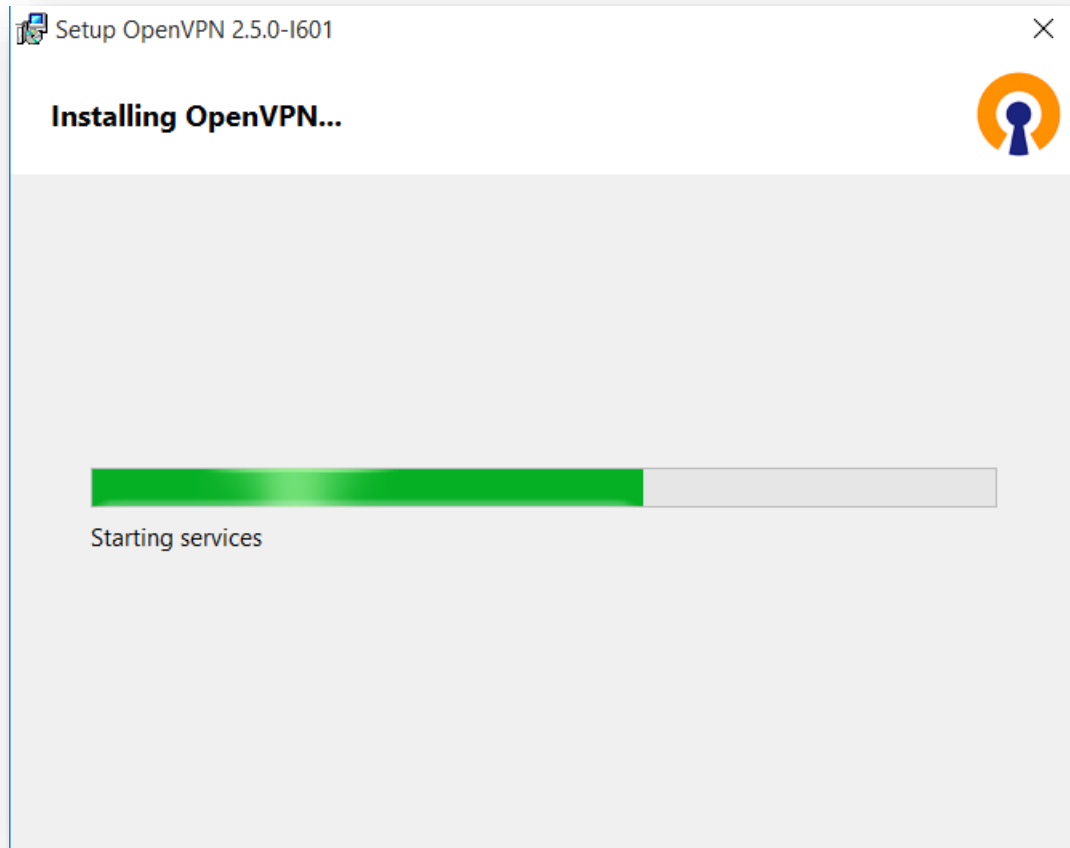


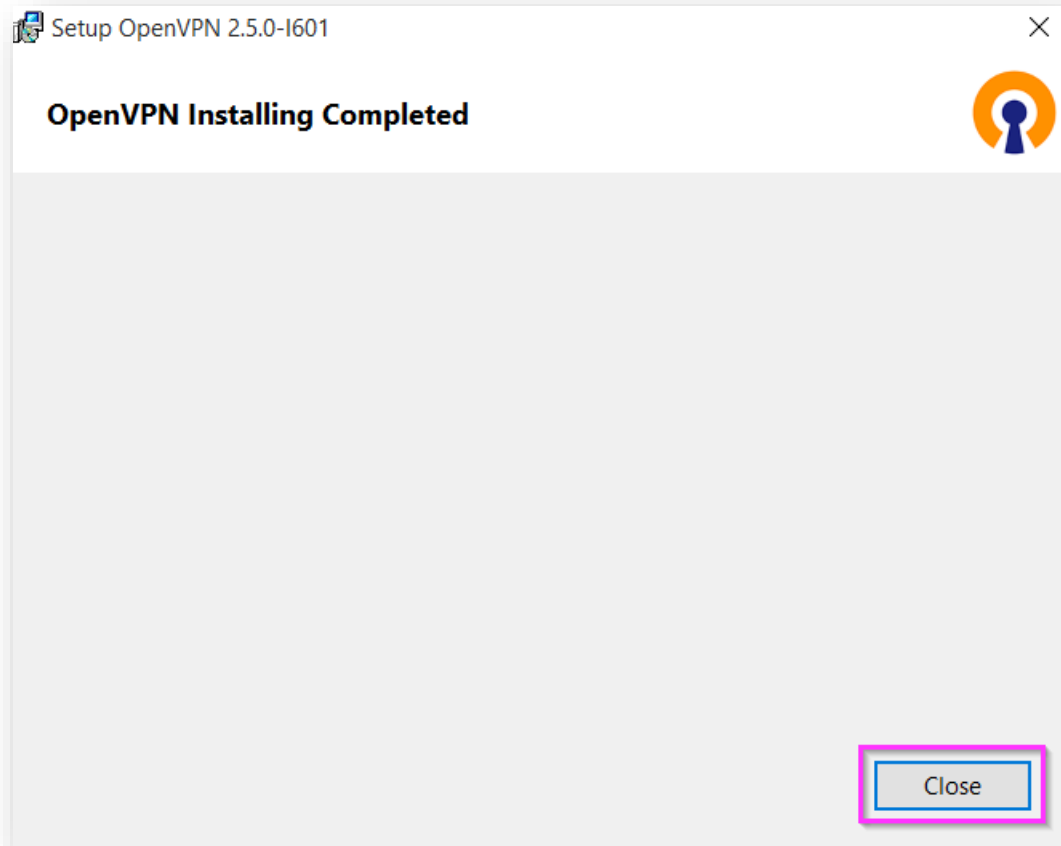
4 Installation du client OpenVPN

Lancez l'installation en tant qu'administrateur à partir de la machine Windows 10.

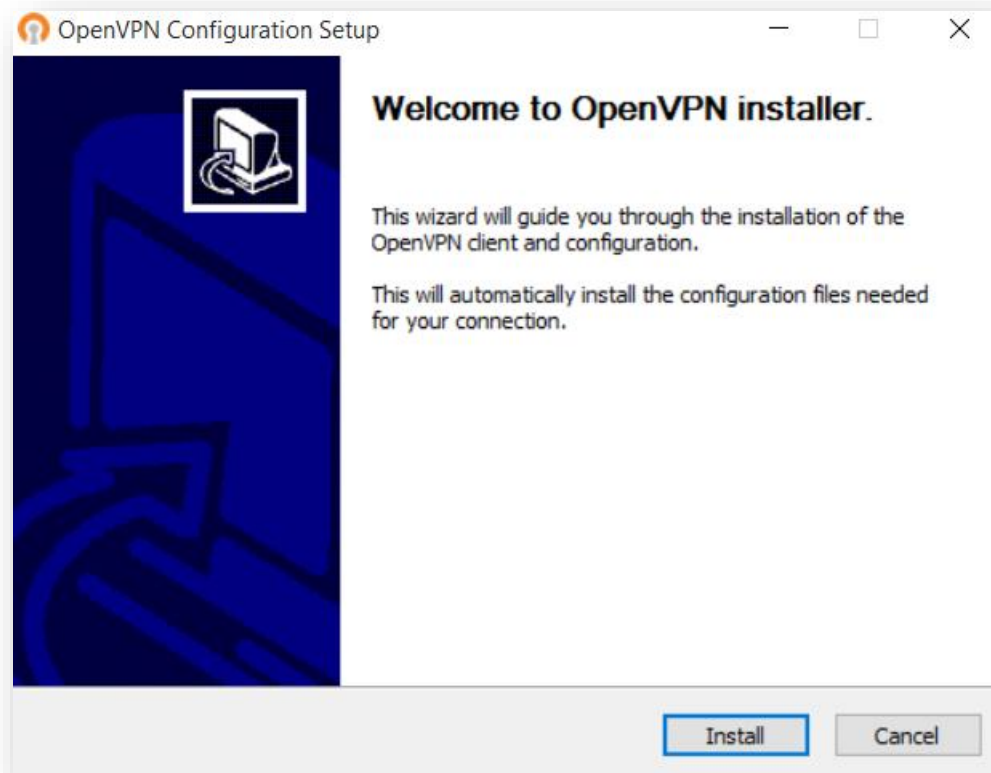


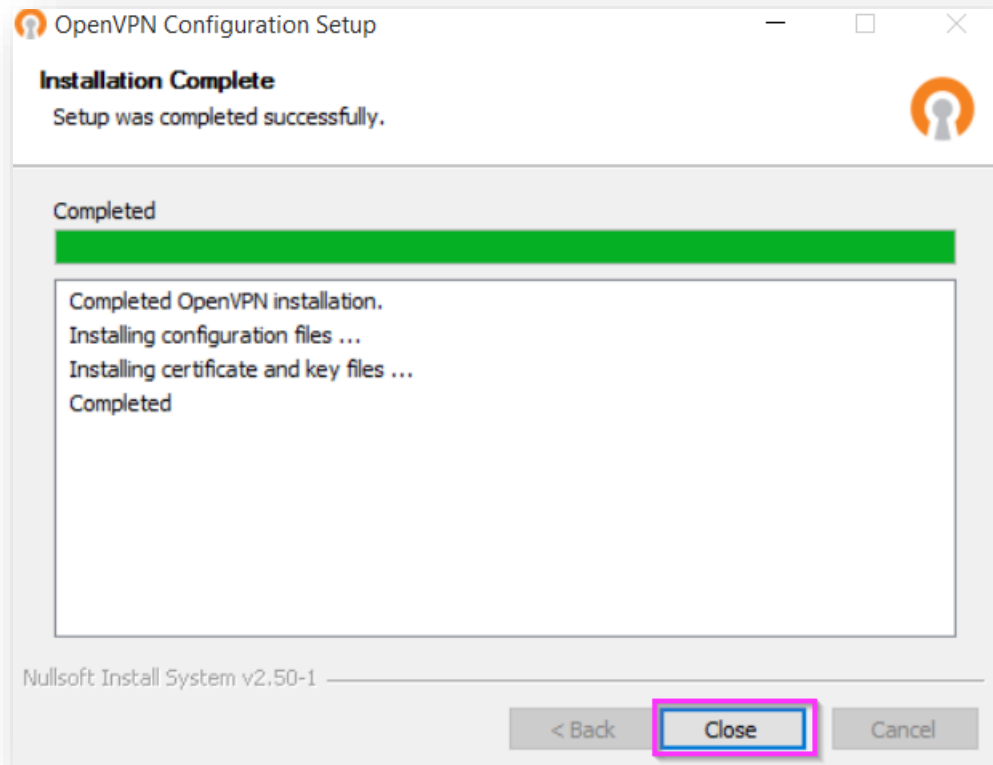




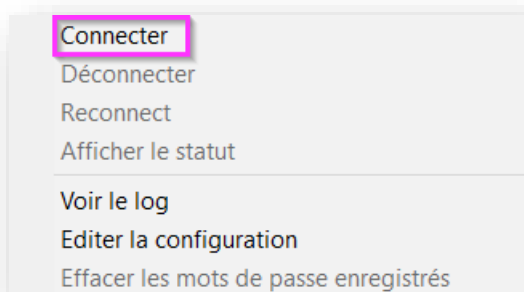
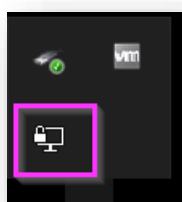
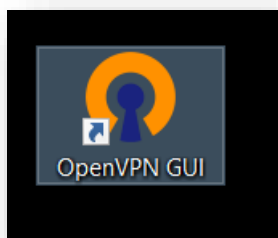


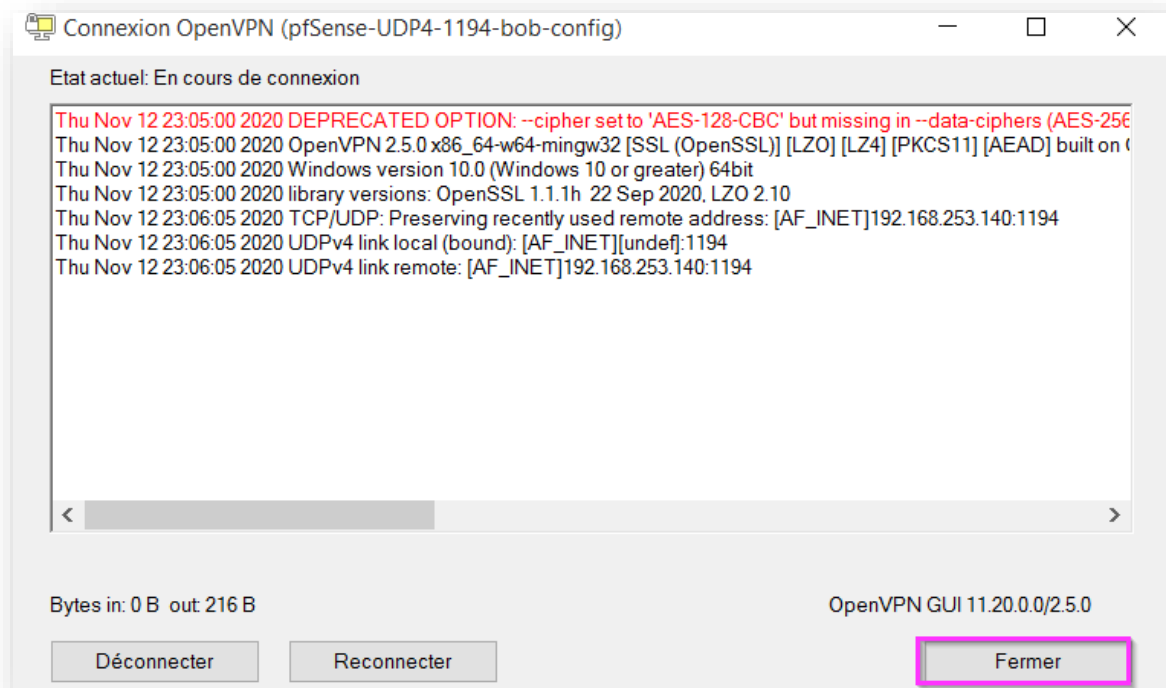
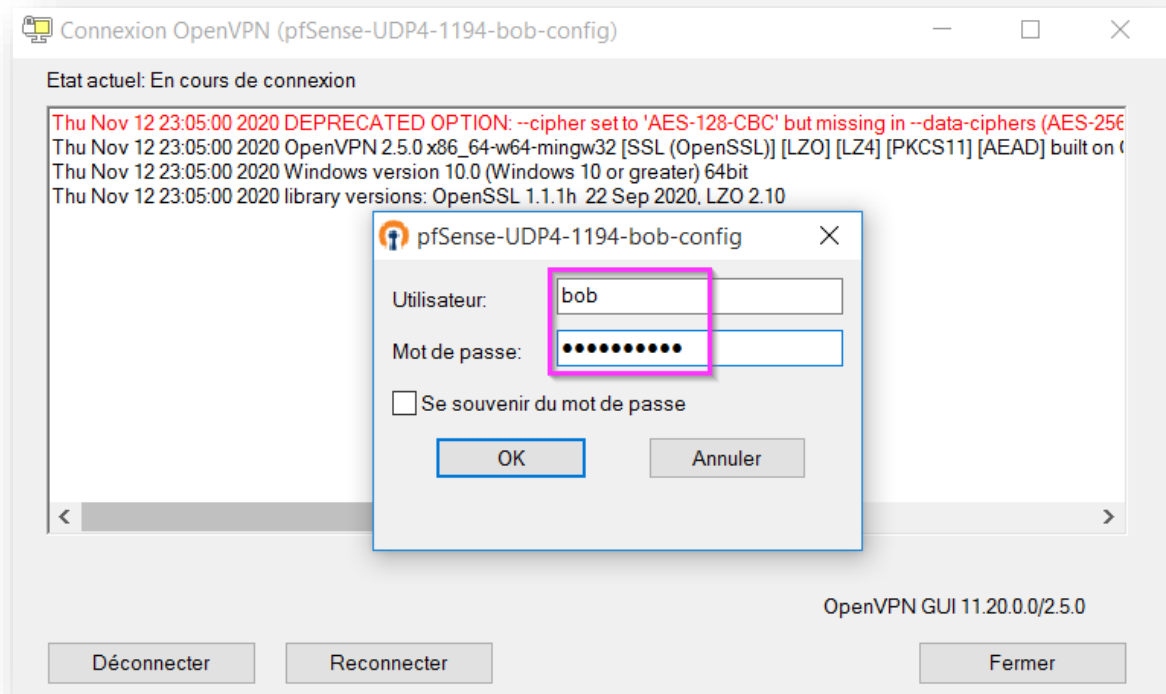
5 Configuration du client OpenVPN





Une fois installé, connectez-vous au VPN à l'aide de l'utilisateur et du mot de passe de Bob :





Vous devriez obtenir ce message.



pfSense-UDP4-1194-bob-config est désormais connecté.

Adresse IP assignée: 10.10.10.2

Invite de commandes

Carte Ethernet Ethernet0 :

```
Suffixe DNS propre à la connexion. . . : localdomain
Adresse IPv6 de liaison locale. . . . : fe80::a8cc:2739:1512:6fac%4
Adresse IPv4. . . . . : 192.168.253.143
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 192.168.253.2
```

Carte inconnue OpenVPN TAP-Windows6 :

```
Suffixe DNS propre à la connexion. . . : orabec.com
Adresse IPv6 de liaison locale. . . . : fe80::68bf:d3e5:9b21:fb1%11
Adresse IPv4. . . . . : 10.10.10.2
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :
```

Testez votre configuration en exécutant un ping les hôtes du réseau distant.

```
C:\>ping 192.168.1.99
```

```
Envoi d'une requête 'Ping' 192.168.1.99 avec 32 octets de données :
```

```
Réponse de 192.168.1.99 : octets=32 temps<1ms TTL=64
```

```
Réponse de 192.168.1.99 : octets=32 temps<1ms TTL=64
```

```
Réponse de 192.168.1.99 : octets=32 temps=1 ms TTL=64
```

```
Réponse de 192.168.1.99 : octets=32 temps=1 ms TTL=64
```

```
Statistiques Ping pour 192.168.1.99:
```

```
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

```
Durée approximative des boucles en millisecondes :
```

```
Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

Vérifier le statut à partir de pfsense :

The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The 'Status' menu is expanded, and 'OpenVPN' is selected. The main content area displays 'Server UDP4:1194 Client Connections' and 'Server UDP4:1194 Routing Table'. The client connections table has columns for Common Name, Real Address, Virtual Address, Connected Since, Bytes Sent, and Bytes Received. The routing table has columns for Common Name, Real Address, Target Network, and Last Used. A status bar at the bottom indicates the OpenVPN service is running with a green checkmark.

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received
bob	192.168.253.143:1194	10.10.10.2	Fri Nov 13 04:09:25 2020	10 KiB	25 KiB

Common Name	Real Address	Target Network	Last Used
bob	192.168.253.143:1194	10.10.10.2	Fri Nov 13 04:14:38 2020

An IP address followed by C indicates a host currently connected through the VPN.