

**MODULE 9**

CONFIGURER OPEN VPN DANS PFSENSE

SOMMAIRE

1. CREATION DE L'AUTORITE DE CERTIFICATION
2. CREATION DU CERTIFICAT SERVEUR
3. CREATION DES UTILISATEURS DU VPN
4. INSTALLATION DU PACKAGE « OpenVPN-Client-Export »
5. CONFIGURATION OPEN VPN
6. EXPORT DE LA CONFIGURATION OPEN VPN
7. INSTALLATION DU CLIENT OPEN VPN
8. CONFIGURATION DES REGLES DE PARE-FEU
9. TESTS DE CONNEXION VPN
10. CONFIGURATION D'UN ACCES RDP AU SERVEUR
11. TESTS DE CONNEXION RDP

© tutos-info.fr - 02/2025

DIFFICULTE

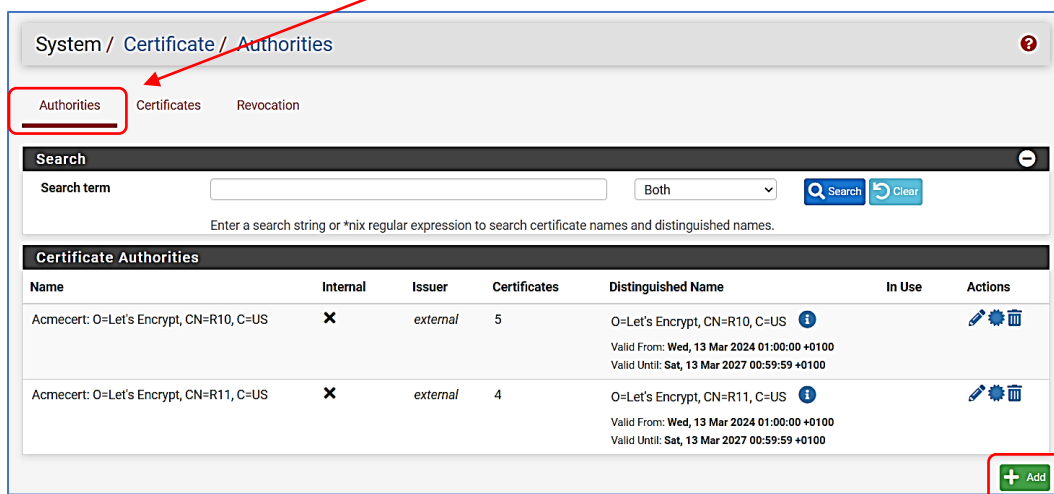


UTILISATION COMMERCIALE INTERDITE

1 – CREATION DE L'AUTORITE DE CERTIFICATION

Ce tutoriel a été réalisé avec la version pfSense 2.7.2 (février 2025).

- Depuis l'interface de gestion de pfSense, cliquez « **System** » - « **Certificates** »
- Cliquez le lien rouge « **Authorities** » et le **bouton vert** « **+ Add** » (dans le bas de la fenêtre) :



- Complétez les paramètres et cliquez le bouton « **Save** » :

Descriptive name CA-LABOPROF-OPENVPN

Method Create an internal Certificate Authority

Trust Store ☐ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial ☐ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Key type RSA

Key length 2048

Digest Algorithm sha256

Lifetime (days) 3650

Common Name laboprof-ca

Country Code FR

State or Province Manche

City AVRANCHES

Organization LABOPROF

Organizational Unit laboprof.sjo

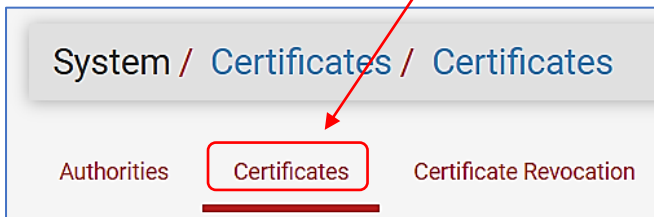
Save

L'autorité interne de certification apparaît ainsi dans l'interface de pfSense :

CA-LABOPROF-OPENVPN	✓	self-signed	0	ST=Manche, OU=laboprof.sio, O=LABOPROF, L=AVRANCHES, CN=laboprof-ca, C=FR	   
Valid From: Sun, 23 Feb 2025 14:45:46 +0100					
Valid Until: Wed, 21 Feb 2035 14:45:46 +0100					

2 – CREATION DU CERTIFICAT SERVEUR

- Depuis l'interface de gestion de pfSense, cliquez « **System** » - « **Certificates** »
- Cliquez le lien rouge « **Certificates** » et le bouton vert « **+ Add/Sign** » (dans le bas de la fenêtre) :



- Complétez la fenêtre avec les paramètres suivants :

Add/Sign a New Certificate	
Method	Create an internal Certificate
Descriptive name	VPN-LABOPROF
The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.	

On créé, ici, un certificat serveur interne avec un nom.

Internal Certificate	
Certificate authority	CA-LABOPROF-OPENVPN
On sélectionne, ici, l'autorité précédemment créée.	
Key type	RSA
	2048
The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	
Digest Algorithm	sha256
The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.	
Lifetime (days)	3650
Nous avons indiqué une durée de 10 ans pour le certificat. The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.	
Common Name	vpn-laboprof.sio
On nomme, ici, le certificat serveur. The following certificate subject components are optional and may be left blank.	
Country Code	FR
State or Province	Manche
City	AVRANCHES
Organization	LABOPROF
Organizational Unit	laboprof.sio
Vous pouvez renseigner cette partie (facultatif).	

- Dans la partie « **Certificate Type** », sélectionnez « **Server Certificate** » ; vous obtenez ceci :

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names FQDN or Hostname

Type Value

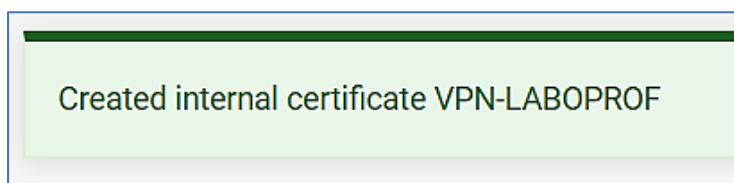
vpn-laboprof.sio

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add SAN Row + Add SAN Row

Save

- Cliquez le bouton bleu « **Save** » ; vous obtenez ceci :



VPN-LABOPROF Server Certificate CA: No Server: Yes	CA-LABOPROF-OPENVPN	ST=Manche, OU=laboprof.sio, O=LABOPROF, L=AVRANCHES, CN=vpn-laboprof.sio, C=FR ⓘ Valid From: Sun, 23 Feb 2025 14:54:58 +0100 Valid Until: Wed, 21 Feb 2035 14:54:58 +0100
---	---------------------	---

3 – CREATION DES UTILISATEURS DU VPN

Ici, nous allons créer un utilisateur local du VPN mais on pourrait également utiliser les utilisateurs d'un domaine via le protocole LDAP (nous étudierons cette fonctionnalité dans un autre module).

- Depuis l'interface de gestion de pfSense, cliquez « **System** » - « **User Manager** »
- Cliquez le lien rouge « **Users** » et le bouton vert « **+ Add** » :

System / User Manager / Users ⓘ

Users Groups Settings Authentication Servers

	Username	Full name	Status	Groups	Actions
☐	admin	System Administrator	✓	admins	

+ Add **Delete**

- Complétez les informations du client qui sera utilisateur du VPN :

User Properties

Defined by

USER

Disabled

☐ This user cannot login

Username

prof

Créer un utilisateur VPN avec un mot de passe fort.

Password

.....

.....

Full name

User's full name, for administrative information only

Expiration date

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

Member of

>> 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

Cliquez cette case pour créer le certificat utilisateur.

Create Certificate for User

Descriptive name

certif-prof-vpn

Certificate authority

CA-LABOPROF-OPENVPN

Donnez un nom au certificat et choisissez un type de clé et un algorithme suffisamment performant (minimum « sha256 ». Vous pouvez, également, définir une durée de vie pour le certificat.

Key type

RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm

sha256

The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime

3650

- Cliquez le bouton bleu « Save » ; l'utilisateur est créé et apparaît dans la liste des utilisateurs autorisés :

Users

Groups

Settings

Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
☐	admin	System Administrator	✓	admins	
☐	prof		✓		

+ Add

Delete

4 – INSTALLATION DU PACKAGE « OpenVPN-Client-Export »

- Depuis l'interface de gestion de pfSense, cliquez « **System** » - « **Package Manager** »
- Cliquez **le lien rouge** « **Available Packages** »
- Recherchez « **openvpn-client-export** » et cliquez **le bouton vert** « **+ Install** » :

openvpn-client-export 1.9.2 Exports pre-configured OpenVPN Client configurations directly from pfSense software.

Package Dependencies:
openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01

- Cliquez **le bouton vert** « **Confirm** » pour installer le package :

Installed Packages Available Packages **Package Installer**

Confirmation Required to install package pfSense-pkg-openvpn-client-export

Confirm

Une fois le package installé, vous obtenez ceci :

System / Package Manager / Package Installer

pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages **Package Installer**

Package Installation

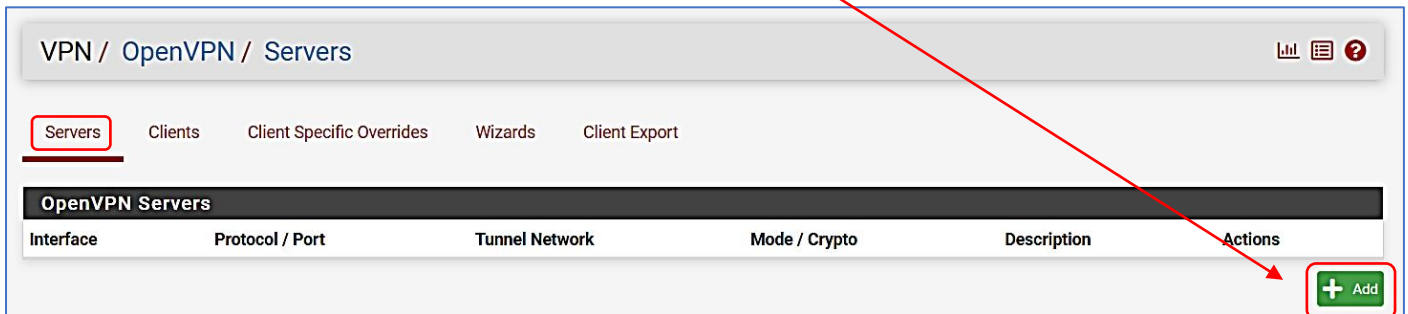
```
[4/5] Installing 7-zip-23.01...
[4/5] Extracting 7-zip-23.01: ..... done
[5/5] Installing pfSense-pkg-openvpn-client-export-1.9.2...
[5/5] Extracting pfSense-pkg-openvpn-client-export-1.9.2: ..... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Writing configuration... done.
>>> Cleaning up cache... done.
```

Success

Patiencez pendant l'installation du package. Un message s'affichera pour vous indiquer que ce dernier a été correctement installé sur votre routeur.

5 – CONFIGURATION OPEN VPN

- Depuis l'interface de gestion de pfSense, cliquez « **VPN** » - « **OpenVPN** »
- Cliquez **le lien rouge** « **Servers** » et **le bouton vert** « **+ Add** » :



- Complétez les paramètres OpenVPN ainsi :

General Information	
Description	VPN LABOPROF 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.

Informations sur le choix du « Server mode » :

- **Remote Access (SSL/TLS)** : pour monter un accès distant pour clients nomades en utilisant une authentification par certificat.
- **Remote Access (User Auth)** : pour monter un accès distant pour clients nomades en utilisant une authentification par login/password.
- **Remote Access (SSL/TLS + User Auth)** : pour monter un accès distant pour clients nomades en utilisant une authentification par certificat **et** par login/password.

Mode Configuration	
Server mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	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.

Par défaut, c'est le port 1194 qui sera utilisé mais vous pouvez le modifier.

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-LABOPROF-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-LABOPROF (Server: Yes, CA: CA-LABOPROF-OPENVPN)

Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length

2048 bit

Diffie-Hellman (DH) parameter set used for key exchange. [i](#)

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. [i](#)

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.

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").

Configuration du tunnel VPN :

- **IPv4 Tunnel Network** : adresse du réseau VPN, c'est-à-dire que lorsqu'un client va se connecter en VPN il obtiendra une adresse IP dans ce réseau au niveau de la carte réseau locale du PC.
- **Redirect IPv4 Gateway** : si vous cochez cette option, vous passez sur un full tunnel c'est-à-dire que tous les flux réseau du PC distant vont passer dans le VPN, sinon nous sommes en « split-tunnel ».
- **IPv4 Local network** : les adresses réseau des LAN que vous souhaitez rendre accessibles via ce tunnel VPN. Dans notre exemple, je souhaite rendre accessible le réseau 192.168.110.0/24 via le VPN. Si vous avez plusieurs valeurs à indiquer, il faut les séparer par une virgule.
- **Concurrent connections** : le nombre de connexions VPN simultanées que vous autorisez.

Tunnel Settings	
IPv4 Tunnel Network	10.0.110.0/24 Saisissez, ici, une adresse virtuelle pour le tunnel VPN. 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.
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	5 Saisissez, ici, le nombre maximum de clients autorisés à se connecter au VPN. 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. Asymmetric compression allows an easier transition when connecting with older peers.
Type-of-Service	☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication	☐ Allow communication between clients connected to this server
Duplicate Connection	☐ Allow multiple concurrent connections from the same user When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session. Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

Pour les paramètres des clients, il est conseillé **de cocher l'option « Dynamic IP »** : si l'adresse IP publique d'un client change, il pourra maintenir sa connexion VPN. C'est surtout utile si vous avez des personnes qui se connectent via une connexion 4G et en mobilité.

Au niveau de la « **Topology** », pour des raisons de sécurité, **il vaut mieux utiliser la topologie « net30 - isolated /30 network per client »** pour que **chaque client soit isolé dans un sous-réseau (de la plage réseau VPN) afin que les clients ne puissent pas communiquer entre eux !**

Cela n'est pas sans conséquence : plutôt qu'une connexion VPN consomme une adresse IP sur la plage réseau dédiée au VPN, **elle va consommer 4 adresses IP** : une adresse IP pour le PC, une adresse IP pour le pare-feu et les adresses de réseau et broadcast du sous-réseau en /30.

Si vous avez besoin de plus de 60 connexions VPN en simultanés, vous ne devez pas utiliser un réseau VPN en /24, mais vous devez prendre plus large. Dans ce cas, modifiez la valeur "IPv4 Tunnel Network" définie précédemment.

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

Advanced Client Settings

DNS Default Domain

☒ Provide a default domain name to clients

DNS Default Domain

laboprof.sio

DNS Server enable

☒ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

DNS Server 1

192.168.110.25

DNS Server 2

192.168.110.254

DNS Server 3

9.9.9.9

DNS Server 4

Block Outside DNS

☐ Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Force DNS cache update

☐ Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.

NTP Server enable

☐ Provide an NTP server list to clients

NetBIOS enable

☐ Enable NetBIOS over TCP/IP
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

Ces valeurs sont à adapter en fonction de votre architecture réseau.

- Indiquez « **auth-nocache** » dans la partie « **Custom options** » pour empêcher la mise en cache des identifiants de connexion au tunnel VPN :

Advanced Configuration

Custom options

auth-nocache

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Username as Common Name

☐ Use the authenticated client username instead of the certificate common name (CN).
When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.

UDP Fast I/O

☐ Use fast I/O operations with UDP writes to tun/tap. Experimental.
Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.

Exit Notify

Reconnect to this server / Retry once

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. 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.

Send/Receive Buffer

Default

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.

Gateway creation

☒ Both
☐ IPv4 only
☐ IPv6 only

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level

default

Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

Save

- Cliquez le bouton bleu « **Save** » pour valider la création du tunnel VPN

VPN / OpenVPN / Servers

Servers

Clients

Client Specific Overrides

Wizards

Client Export

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.110.110.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VPN LABOPROF	

6 – EXPORT DE LA CONFIGURATION OPEN VPN

Il faut maintenant télécharger la configuration OpenVPN au format « *.ovpn ». Pour cela, effectuez les manipulations suivantes :

- Depuis l'interface de gestion de pfSense, cliquez « **VPN** » - « **OpenVPN** »
- Cliquez **le lien rouge « Client Export »** ; une fenêtre s'affiche, complétez-la :

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards **Client Export**

OpenVPN Server

Remote Access Server: VPN LABOPROF UDP4:1194

Client Connection Behavior

Host Name Resolution: Other

Host Name: . **Saisissez, ici, le nom de domaine de votre serveur ou l'IP publique.**

Enter the hostname or IP address the client will use to connect to this server.

Verify Server CN: Automatic - Use verify-x509-name where possible

Optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS: ☐ Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Legacy Client: ☐ Do not include OpenVPN 2.5 and later settings in the client configuration. When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

Silent Installer: ☐ Create Windows installer for unattended deploy. Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.

Bind Mode: Do not bind to the local port

If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.

Certificate Export Options

PKCS#11 Certificate Storage: ☐ Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.

Microsoft Certificate Storage: ☐ Use Microsoft Certificate Storage instead of local files.

Password Protect Certificate: ☐ Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.

PKCS#12 Encryption: High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Windo)

Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program

Proxy Options

Use A Proxy: ☐ Use proxy to communicate with the OpenVPN server.

Advanced

Additional configuration options: **auth-nocache** **Saisissez, ici, « auth-nocache ».**

Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.

EXAMPLE: remote-random;

Save as default

- Cliquez **le bouton bleu « Save as default »** pour valider la configuration.

Dans le bas de la fenêtre, une rubrique « **OpenVPN Clients** » s'est affichée avec l'utilisateur du VPN :

OpenVPN Clients

User	Certificate Name	Export
prof	certif-prof-vpn	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installers (2.6.7-lx001): 64-bit 32-bit - Previous Windows Installers (2.5.9-lx601): 64-bit 32-bit - Legacy Windows Installers (2.4.12-lx601): 10/2016/2019 7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

Pour vous connecter au VPN depuis un mobile, choisissez la rubrique « Inline Configurations ».

Pour télécharger le « zip » contenant les fichiers de configuration du tunnel VPN (pour une machine Windows), cliquez sur « Archive ».

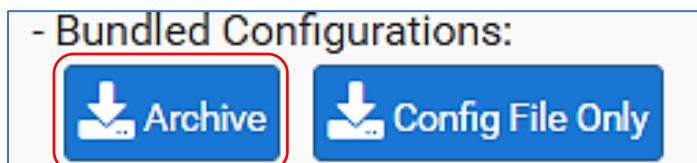
Remarque :

Si vous souhaitez vous connecter en VPN depuis une machine locale Windows, il faudra choisir le lien « **Bundled Configuration** » qui permet de récupérer tous les fichiers nécessaires à la configuration du tunnel (format « zip »).

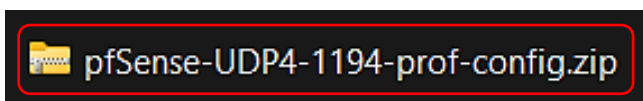
Pour l'utilisation du VPN depuis un mobile (avec l'application OpenVPN Connect), prenez la configuration « **Inline Configuration** ».

1^{ère} étape : téléchargement du fichier contenant les paramètres du tunnel VPN

- Cliquez le bouton bleu « **Archive** » dans la partie « **Bundled Configuration** » afin de télécharger le fichier « zip » comprenant les paramètres du tunnel VPN précédemment configuré :



Après avoir cliqué sur « **Archive** », le fichier « zip » est téléchargé sur votre machine locale Windows :



Décompressez-le, vous obtenez 3 fichiers à l'intérieur du dossier décompressé :

	pfSense-UDP4-1194-prof.ovpn	23/02/2025 16:17	OpenVPN Config F...	1 Ko
	pfSense-UDP4-1194-prof.p12	23/02/2025 16:17	Échange d'informa...	5 Ko
	pfSense-UDP4-1194-prof-tls.key	23/02/2025 16:17	Fichier KEY	1 Ko

L'archive a été téléchargée et décompressée. Elle contient maintenant 3 fichiers importants et nécessaires au fonctionnement de votre tunnel VPN.

2^{ème} étape : téléchargement du logiciel OpenVPN client

Il faut, ensuite, télécharger et installer le **logiciel client OpenVPN** sur votre machine locale Windows.

Pour récupérer le logiciel client pour Windows, vous pouvez cliquer le 1^{er} lien « **OpenVPN Community Client** » :

[OpenVPN Community Client](#) - Binaries for Windows, Source for other platforms. Packaged above in the Windows Installers
OpenVPN For Android - Recommended client for Android
OpenVPN Connect: Android (Google Play) or iOS (App Store) - Recommended client for iOS
Viscosity - Recommended commercial client for Mac OS X and Windows
Tunnelblick - Free client for OS X
Using the Latest OpenVPN on Linux Distros - Install OpenVPN using the OpenVPN apt repositories to get the latest version, rather than one included with distributions.

Lien à cliquer pour accéder à la page de téléchargement du logiciel :

Links to OpenVPN clients for various platforms:

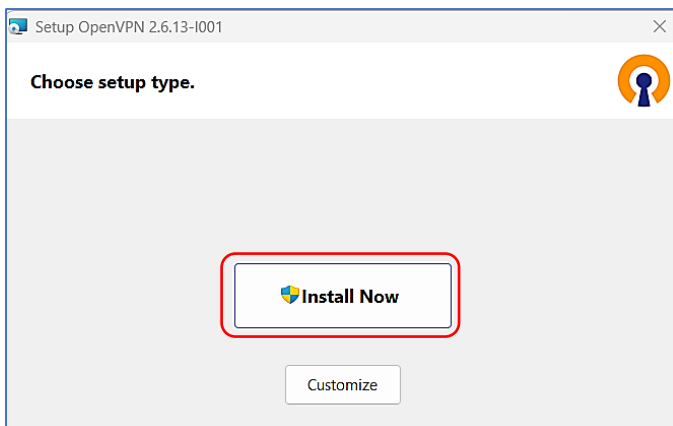
[OpenVPN Community Client - Binaries for Windows, Source for other platforms. Packaged above in the Windows Installers](#)

- Une fois sur la page de téléchargement du logiciel client OpenVPN, cliquez le lien de téléchargement (pour le client « **Windows 64-bit MSI installer** ») :

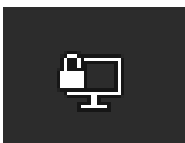
[Windows 64-bit MSI installer](#)[GnuPG Signature](#)[OpenVPN-2.6.13-I001-amd64.msi](#)

7 – INSTALLATION DU CLIENT OPENVPN SUR LE CLIENT WINDOWS

Après avoir téléchargé le logiciel client, double-cliquez le fichier « msi » téléchargé et lancez l'installation ç partir de l'assistant suivant (cliquez le bouton « **Install Now** ») :



Une fois le logiciel installé, vous constaterez qu'une petite icône est apparue dans la zone de notification de votre machine (en bas à droite, près de l'horloge) :



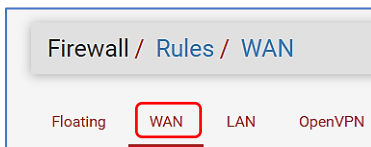
Une fois le logiciel OpenVPN client installé, vous trouverez cette petite icône dans la zone de notification de votre machine Windows (en bas à droite près de l'horloge). Elle servira à la connexion VPN.

8 – CONFIGURATION DES REGLES DANS LE PARE-FEU DE pfSENSE

Dans cette partie importante et nécessaire, nous devons **créer une règle pour autoriser les clients à monter la connexion VPN** et, d'autre part, nous devons **créer une ou plusieurs règles pour autoriser l'accès aux ressources** : serveur en RDP, serveur de fichiers, application web, etc.

Pour cela, effectuez les manipulations suivantes :

- Depuis l'interface de gestion de pfSENSE, cliquez « **Firewal** » - « **Rules** » - « **WAN** »



- Cliquez le bouton vert « **+ Add** » (en bas de la fenêtre) ; une fenêtre s'ouvre :

La destination sera l'adresse IP publique, c'est pour cela que nous choisissons « **WAN address** ».

Pour le port de destination, sélectionnez « **OpenVPN** » dans la liste (ou indiquez un port personnalisé si vous avez modifié le port 1194 par un autre) :

Si vous le souhaitez, vous pouvez ajouter une description à cette règle et activer les logs.

- Cliquez **le bouton bleu « Save »** pour valider :

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
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

- Cliquez **le bouton vert « Apply changes »** :

Firewall / Rules / WAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

☒	☒	0/0 B	IPv4	*	*	WAN address	1194 (OpenVPN)	*	none	Accès OPENVPN - SRV 2025	Edit Delete
-------------------------------------	-------------------------------------	-------	------	---	---	-------------	----------------	---	------	--------------------------	---

À partir de ce moment, **il est possible de monter le tunnel VPN depuis une machine cliente** mais les ressources de votre entreprise seront inaccessibles car **il est nécessaire d'ajouter des règles supplémentaires qui permettront l'accès aux ressources internes.**

Il faut donc créer une règle autorisant l'accès aux ressources tant du côté « WAN » que du côté « LAN ». Pour cela, effectuez les manipulations suivantes :

- Cliquez « **Firewall** » - « **Rules** » et « **OpenVPN** »
- Cliquez **le bouton vert « Add »** ; une fenêtre s'ouvre ; complétez-la et cliquez **le bouton bleu « Save »** :

Edit Firewall Rule

Action
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface
Choose the interface from which packets must come to match this rule.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Destination

Destination ☐ Invert match **Address or Alias** 192.168.168.111 /

Destination Port Range **From** MS RDP (3389) **Custom** **To** MS RDP (3389)

Specify the destination port or port range for this rule. The "To" field may be left empty if only one port is specified.

Indiquez, ici, l'adresse de votre serveur sur lequel vous voulez vous connecter en VPN.

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 Accès RDP - SRV 2025 (via OpenVPN)

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](#)

[Save](#)

- Cliquez le bouton vert « **Apply Changes** » pour valider la règle :

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

[✓ Apply Changes](#)

La règle doit ressembler à ceci :

Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	✓	0/0 B	IPv4 UDP	*	*	192.168.168.111	3389 (MS RDP)	*	none	Accès RDP - SRV 2025 (via OpenVPN)	↓ ↑ ✎ 🔗 🗑️ ✖

9 – TEST DE CONNEXION VPN

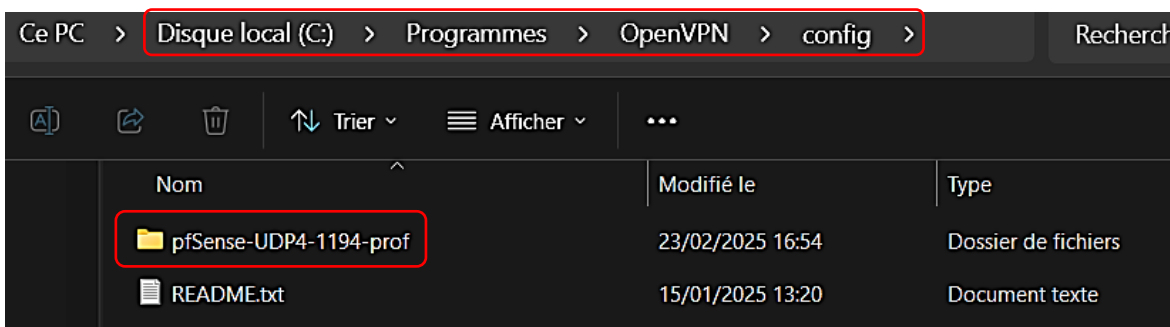
Il faut maintenant préparer le logiciel client OpenVPN téléchargé et installé sur votre machine locale. Pour cela, **vous devez copier les fichiers de l'archive décompressée dans « c:\Programmes\OpenVPN\config »** :

Chemin exact de l'emplacement des fichiers de configuration OpenVPN :

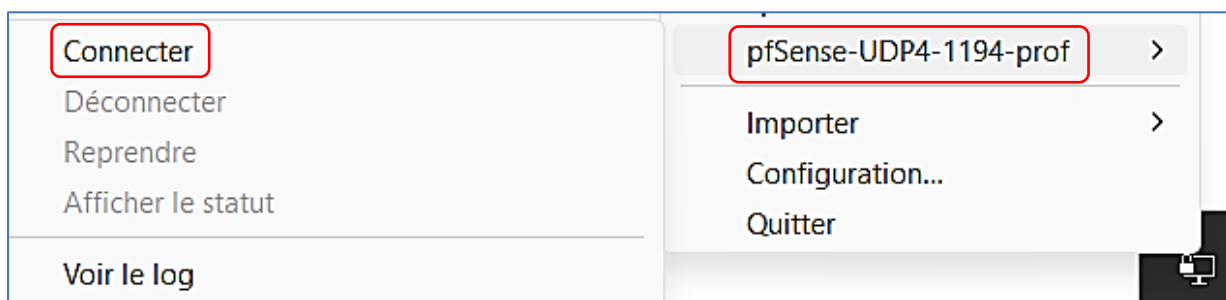
C:\Program Files\OpenVPN\config

Les fichiers de l'archive décompressée doivent être placés dans le dossier « config » d'OpenVPN.

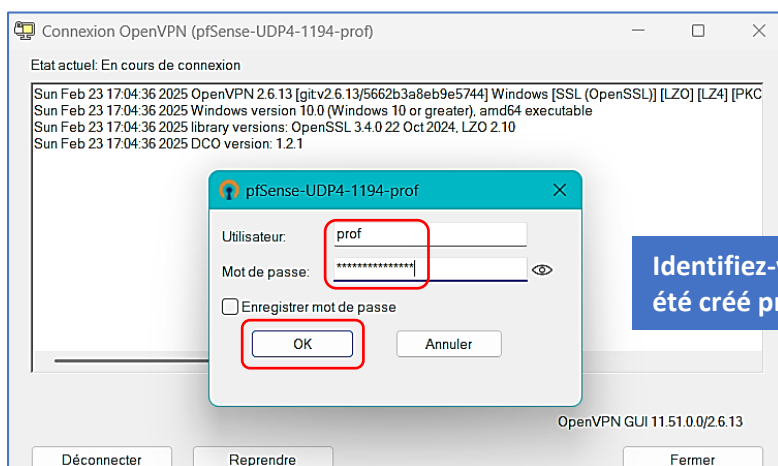
Vous devez obtenir ceci (sur votre machine cliente Windows) :



- Faites un clic droit sur l'icône OpenVPN client de votre machine locale (dans la zone de notification près de l'horloge) et cliquez « **Connecter** ». Logiquement vous devriez voir le nom de votre tunnel (ici nous avons « pfSense-UDP4-1194-prof ») :

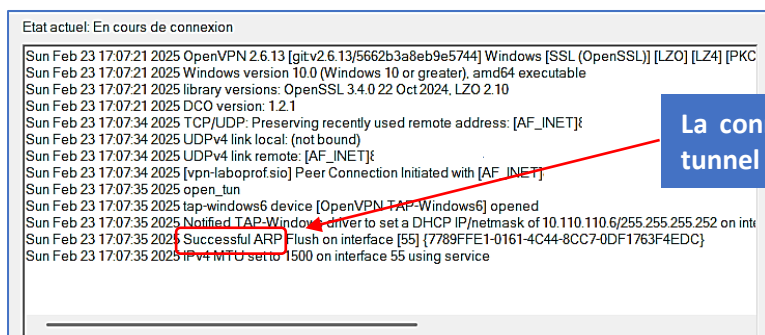


Si vos paramètres sont corrects et que vos règles de pare-feu sont fonctionnelles, la connexion au tunnel est demandée et une authentification est demandée ; saisissez l'utilisateur défini lors de la configuration initiale de votre VPN ainsi que son mot de passe et cliquez « **OK** » :



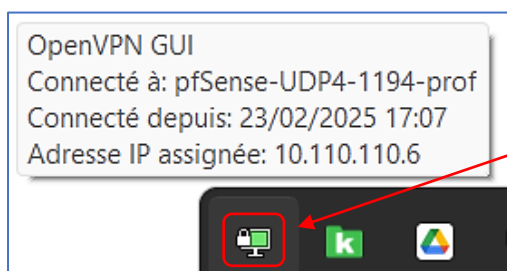
Identifiez-vous avec l'utilisateur VPN qui avait été créé préalablement (voir dans ce tutoriel).

La connexion s'établit ; patientez quelques instants et, si la connexion est validée, la fenêtre sera réduite automatiquement :



La connexion est établie : le tunnel VPN a été « monté ».

L'icône du client OpenVPN s'affiche en vert pour indiquer que le tunnel est connecté :



L'icône du logiciel client OpenVPN s'affiche en vert dans la zone de notification de votre machine.

Sur votre machine Windows cliente, ouvrez une console et saisissez la commande « **ipconfig /all** » ; vous constaterez que votre machine est connectée au tunnel avec une adresse IP telle que vous l'avez définie lors de la création du VPN (ici nous avons 10.110.110.6) :

```
Carte inconnue OpenVPN TAP-Windows6 :
Suffixe DNS propre à la connexion. . . : laboprof.sio
Description. . . . . : TAP-Windows Adapter V9
Adresse physique . . . . . : 00-FF-77-89-FF-E1
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::bb2:b900:4c96:ff24%55(préfééré)
Adresse IPv4. . . . . : 10.110.110.6(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.252
Bail obtenu. . . . . : dimanche 23 février 2025 17:07:36
Bail expirant. . . . . : lundi 23 février 2026 17:07:36
Passerelle par défaut. . . . . :
Serveur DHCP . . . . . : 10.110.110.5
IAID DHCPv6 . . . . . : 922812279
DUID de client DHCPv6. . . . . : 00-01-00-01-29-3C-DE-4A-18-C0-4D-93-3C-A3
Serveurs DNS. . . . . : 192.168.110.25
                        192.168.110.254
                        9.9.9.9
NetBIOS sur Tcpip. . . . . : Activé
```

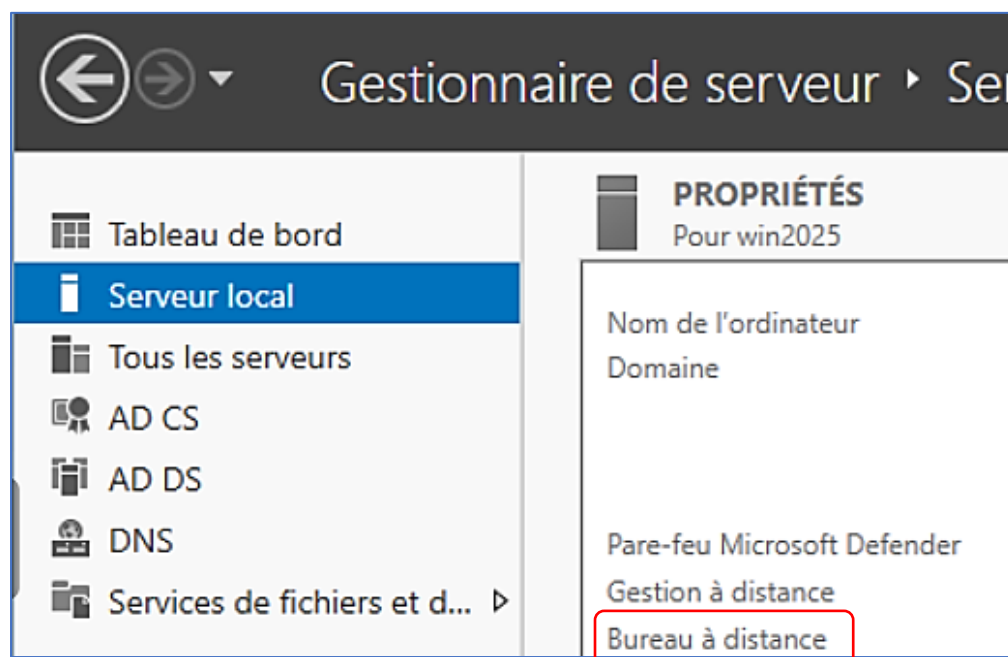
Votre tunnel est fonctionnel. Nous allons maintenant tester l'accès à notre serveur Windows via le protocole RDP (Bureau à distance de Microsoft).

10 – CONFIGURATION D'UN ACCES RDP AU SERVEUR VIA OPENVPN

1^{ère} étape : autorisation du bureau à distance sur le serveur

Le tunnel étant fonctionnel, nous allons maintenant présenter la méthodologie permettant d'accéder à notre serveur 2025 en utilisant le protocole RDP (bureau à distance de Microsoft). Par défaut, ce protocole utilise le **port 3389**.

- Ouvrez une session administrateur sur votre serveur
- Depuis le gestionnaire de serveur, cliquez « **Serveur local** » et cliquez le lien « **Désactivé** » qui se trouve en face de « **Bureau à distance** » :



- Cliquez « **Autoriser les connexions à distance à cet ordinateur** » et validez en cliquant « **OK** » :

Bureau à distance

Choisissez une option, puis spécifiez qui peut se connecter.

☐ Ne pas autoriser les connexions à distance à cet ordinateur

☒ **Autoriser les connexions à distance à cet ordinateur**

- Vérifiez que le **lien bleu** affiche « **Activé** » :

Bureau à distance **Activé**

2^{ème} étape : création des règles de pare-feu nécessaires pour autoriser l'accès RDP

- Depuis l'interface de gestion de pfSENSE, cliquez « **Firewal** » et « **NAT** »
- Une fenêtre s'affiche ; complétez-la ainsi :

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

☐ Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination ☐ Invert match. WAN address
Type

Destination port range MS RDP
From port Custom To port MS RDP
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Address or Alias
Type 192.168.168.111
Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4. In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1).

Redirect target port MS RDP
Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.

Description Accès RDP - SRV 2025 (via OpenVPN)
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync ☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Rule NAT Accès RDP - SRV 2025 (via OpenVPN)

Le port 3389 est le port du Bureau à distance Microsoft (nommé ici MS RDP).

Indiquez, ici, l'adresse IP du serveur que vous voulez atteindre via RDP.

No XMLRPC Sync ☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Rule NAT Accès RDP - SRV 2025 (via OpenVPN)
[View the filter rule](#)

Rule Information

Created	2/23/25 19:49:59 by admin@37.171.112.23 (Local Database)
Updated	2/23/25 20:17:11 by admin@37.165.115.105 (Local Database)

 Save

- Cliquez **le bouton bleu « Save »** et **le bouton vert « Apply Changes »** pour valider vos paramètres.
- Depuis l'interface de gestion de pfSENSE, cliquez « **Firewal** » et « **Rules** »
- Vérifiez que cette règle est présente :

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Associated filter rule This is associated with a NAT rule.
Editing the interface, protocol, source, or destination of associated filter rules is not permitted.
[View the NAT rule](#)

Interface WAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Destination

Destination ☐ Invert match Address or Alias 192.168.168.111 /

Destination Port Range MS RDP (3389) MS RDP (3389)
From Custom 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 NAT Accès RDP - SRV 2025 (via OpenVPN)
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 

Rule Information

Tracking ID	1740336599
Created	2/23/25 19:49:59 by NAT Port Forward

 Save

- Cliquez **le bouton bleu « Save »** ; vous obtenez ceci :

☒	☒	10/181 KiB	IPv4 TCP	*	*	192.168.168.111	3389 (MS RDP)	*	none	NAT Accès RDP - SRV 2025 (via OpenVPN)
-------------------------------------	-------------------------------------	---------------	-------------	---	---	-----------------	------------------	---	------	---

- Cliquez **le bouton vert « Apply changes »** pour valider vos paramètres.

Assurez-vous d'avoir les règles suivantes présentes dans votre pare-feu :

1 – Dans « Firewall » - « Rules » - « WAN » :

☐	☒	9/302 KiB	IPv4 TCP	*	*	192.168.168.111	3389 (MS RDP)	*	none	NAT Accès RDP - SRV 2025 (via OpenVPN)
--------------------------	-------------------------------------	--------------	-------------	---	---	-----------------	------------------	---	------	---

2 – Dans « Firewall » - « WAN » - « Open VPN » :

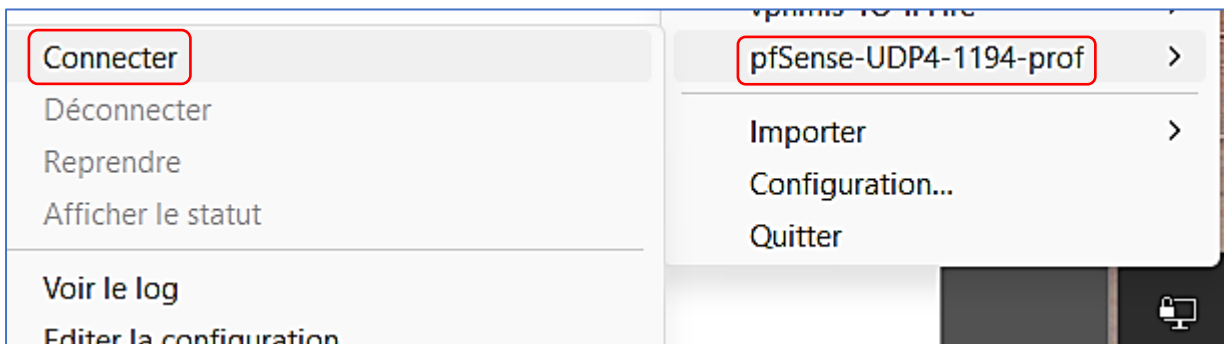
☐	☒	0/0 B	IPv4 UDP	*	*	192.168.168.111	3389 (MS RDP)	*	none	Accès RDP - SRV 2025 (via OpenVPN)
--------------------------	-------------------------------------	-------	----------	---	---	-----------------	---------------	---	------	------------------------------------

3 – Dans « Firewall » - « NAT » :

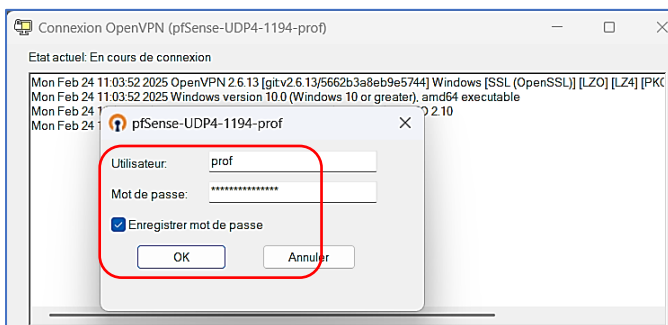
☐	☒	☒	WAN	TCP	*	*	WAN address	3389 (MS RDP)	192.168.168.111	3389 (MS RDP)	Accès RDP - SRV 2025 (via OpenVPN)
--------------------------	-------------------------------------	-------------------------------------	-----	-----	---	---	----------------	------------------	-----------------	------------------	------------------------------------

11 – TEST DE CONNEXION RDP AU SERVEUR VIA OPENVPN

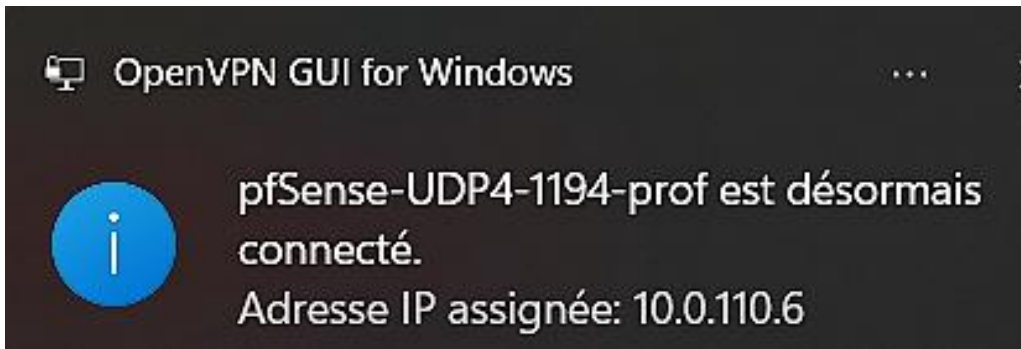
- Faites un clic droit sur l'icône OpenVPN de votre machine locale
- Cliquez « **Connecter** » (en choisissant la configuration VPN adéquate si vous en avez plusieurs) :



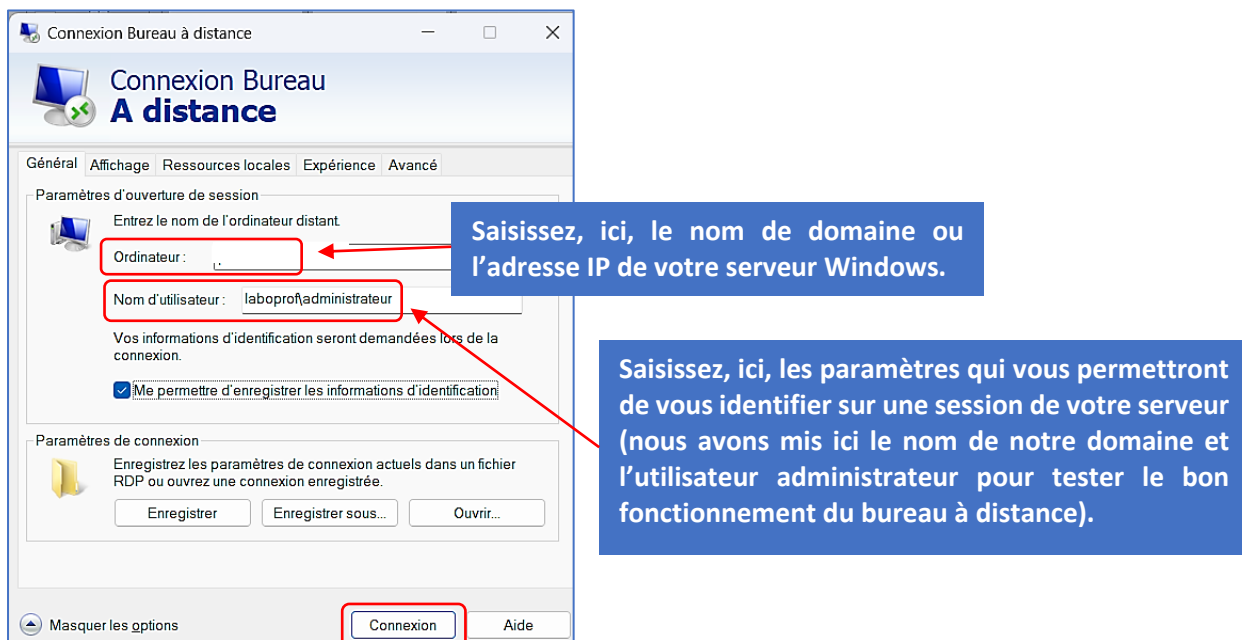
- Complétez la fenêtre d'identification avec l'utilisateur VPN créé dans les pages précédentes et validez en cliquant le bouton « **OK** » :



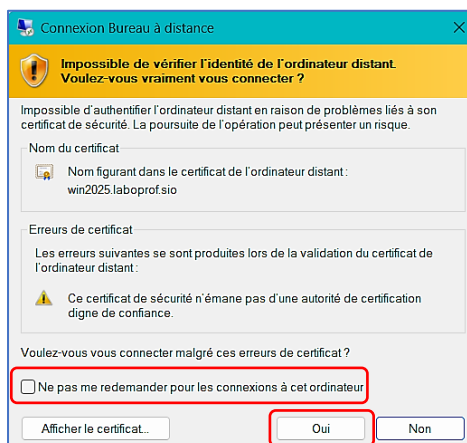
Le tunnel est monté ; la connexion VPN est établie :



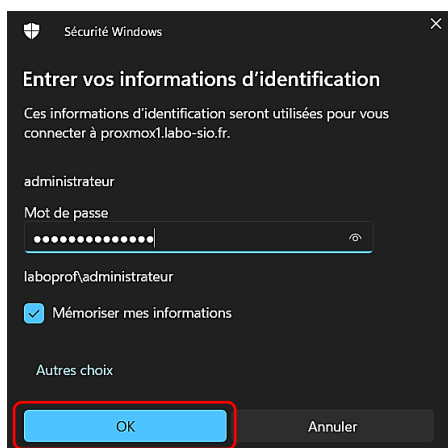
- Dans la barre de recherche de votre machine Windows locale, saisissez « **mstsc** » afin d’ouvrir la fenêtre de connexion du bureau à distance.
- Saisissez, dans la fenêtre, les identifiants qui vous permettront de vous logger à votre serveur (à adapter selon votre configuration) et cliquez le bouton « **Connexion** » :



- Cliquez le bouton « **Oui** » pour valider la connexion avec le certificat auto signé qui émane de notre autorité de certification créée sur pfSENSE (vous pouvez aussi cliquer la case « **Ne pas me redemander pour les connexions à cet ordinateur** ») :



- Identifiez-vous avec les identifiants et le mot de passe du compte avec lequel vous souhaitez ouvrir la session sur votre serveur et cliquez le bouton « **OK** » :



Saisissez, ici, les paramètres qui vous permettront de vous identifier sur une session de votre serveur (nous avons mis ici le nom de notre domaine et l'utilisateur administrateur pour tester le bon fonctionnement du bureau à distance).

Vous êtes maintenant connecté à votre serveur en RDP via votre tunnel VPN :



Remarque :

Ce tutoriel présente la démarche complète permettant de mettre en œuvre Open VPN sur pfSENSE. Nous n'avons pas abordé, ici, les notions de sécurité notamment concernant la connexion au serveur (conditions de tests ici).

Il est intéressant de préciser qu'il est possible, dans la partie VPN de pfSENSE, de créer un lien LDAP avec les utilisateurs du domaine. Ainsi, les utilisateurs du domaine pourront se connecter via Open VPN à leur machine du domaine en utilisant leurs identifiants habituels.

Cette partie sera étudiée dans un autre tutoriel.