

2024

BTS S102

---

# 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.

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

Create / Edit CA

**Descriptive name** vpn-ap  
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: ?, >, <, &, /, \, ", '.

**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.

**Internal Certificate Authority**

**Key type** RSA

2048  
The length to use when generating a new RSA key, in bits.

Activer Windows  
Accédez aux paramètres pour activer Windows.

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.

System / Certificate / Authorities

Authorities Certificates Revocation

**Search**

Search term  Both

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
vpn-ap	✓	self-signed	0	ST=Nord-Pas-de-Calais, OU=Bts SIO, O=SaintLuc, L=Cambrai, CN=vpn-ap, C=FR Valid From: Wed, 20 Nov 2024 08:34:06 +0100 Valid Until: Sat, 18 Nov 2034 08:34:06 +0100	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

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

**pfSense** COMMUNITY EDITION

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

### Add/Sign a New Certificate

**Method** Create an internal Certificate

**Descriptive name** vpn-ap  
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: ?, >, <, &, /, \, ' , "

### Internal Certificate

**Certificate authority** No internal Certificate Authorities have been defined. An internal CA must be defined in order to create an internal certificate. [Create an internal](#)

**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.

prime256v1 [HTTPS] [IPsec] [OpenVPN]  
Curves may not be compatible with all uses. Known compatible curve uses are denoted in brackets.

Activer Windows  
Accédez aux paramètres pour activ

City Cambrai

Organization SaintLuc

Organizational Unit Bts SIO

### 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 | vpn.groupe3.local|  
Type Value  
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. A signing CA may ignore or change these values.

Add SAN Row + Add SAN Row

Save

Activer Windows  
Accédez aux paramètres pour activ

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

System / Certificates / Certificates

Created internal certificate vpn-ap

Authorities Certificates Certificate Revocation

Search

Search term  Both

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

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (66f10f1717fba) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-66f10f1717fba Valid From: Mon, 23 Sep 2024 08:47:52 +0200 Valid Until: Sun, 26 Oct 2025 07:47:52 +0100	webConfigurator	
vpn-ap Server Certificate CA: No Server: Yes	vpn-ap	ST=Nord-Pas-de-Calais, OU=Bts SIO, O=SaintLuc, L=Cambrai, CN=vpn-ap, C=FR Valid From: Wed, 20 Nov 2024 08:42:49 +0100 Valid Until: Sat, 18 Nov 2034 08:42:49 +0100		

Activer Windows  
Accédez aux paramètres

System / User Manager / Users

Users Groups Settings Authentication Servers

Users

Username	Full name	Status	Groups	Actions
<input type="checkbox"/> admin	System Administrator	✓	admins	

Activer Windows  
Accédez aux paramètres

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

**User Properties**

Defined by: USER

Disabled:  This user cannot login

Username: nicolas

Password: [masked]

Full name: nicolas debut  
User's full name, for administrative information only

Expiration date: [empty]  
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

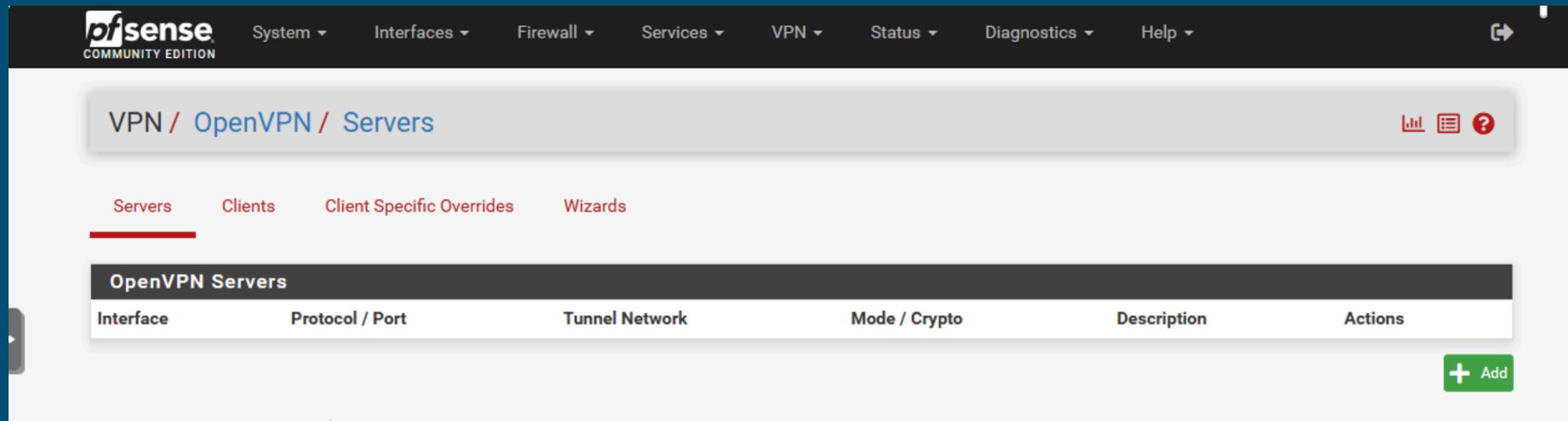
Attention, n'oubliez pas, lors de la création de l'utilisateur, de cocher l'option permettant la génération automatique du certificat associé.

System / User Manager / Users

Users Groups Settings Authentication Servers

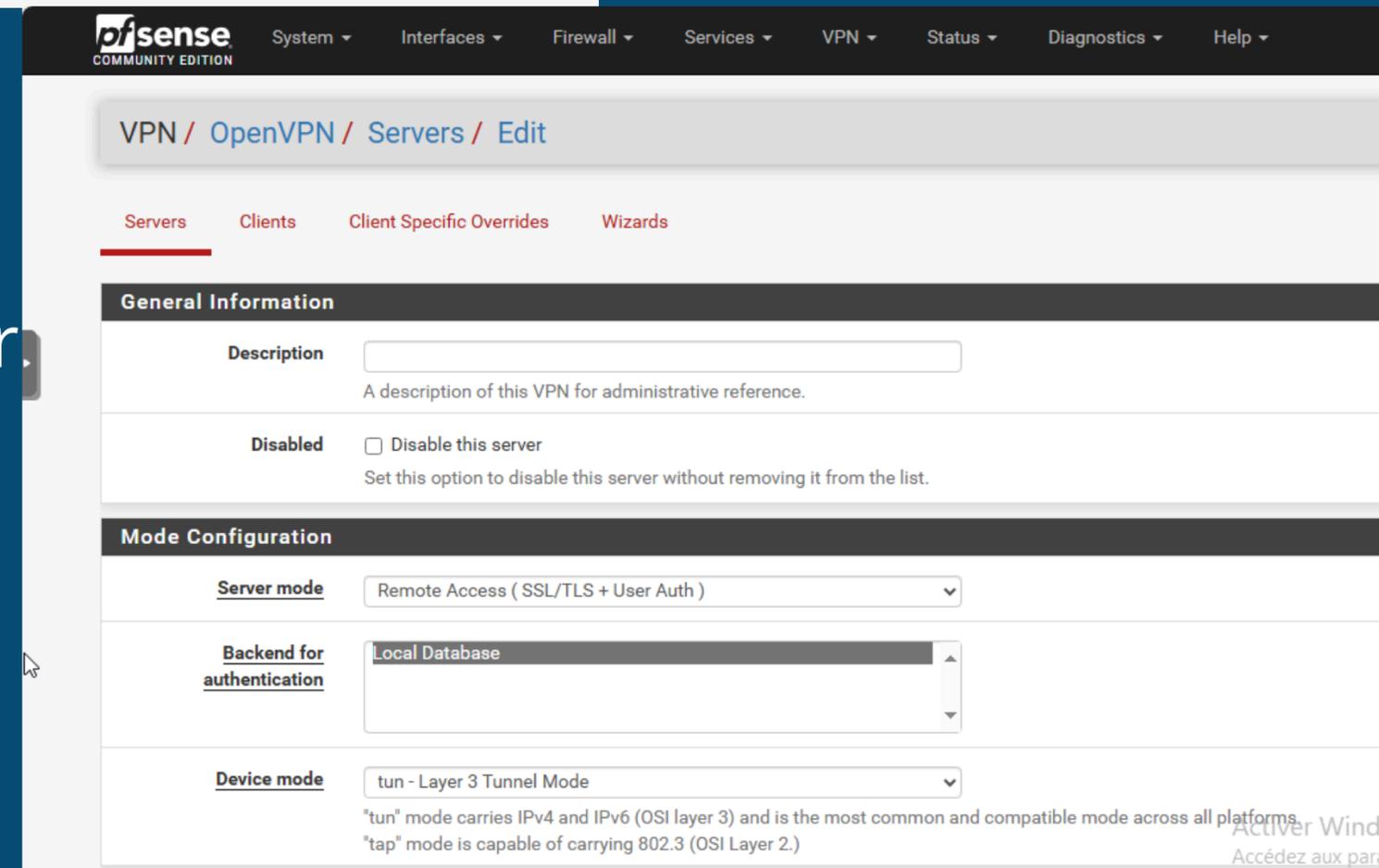
**Users**

	Username	Full name	Status
<input type="checkbox"/>	admin	System Administrator	✓
<input checked="" type="checkbox"/>	nicolas	nicolas debut	✓



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.

The screenshot shows the OpenVPN configuration interface. The 'Local port' field is highlighted with a red circle and contains the value '1194'. Below it, the text reads: 'The port used by OpenVPN to receive client connections.' Other visible settings include 'Device mode' set to 'tun - Layer 3 Tunnel Mode', 'Protocol' set to 'UDP on IPv4 only', and 'Interface' set to 'WAN'. The 'Cryptographic Settings' section is also visible, with 'Use a TLS Key' and 'Automatically generate a TLS Key' checked.

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

This screenshot is identical to the one on the left, but the 'Local port' field is highlighted with a red circle and contains the value '1503'. The rest of the configuration, including 'Device mode', 'Protocol', 'Interface', and 'Cryptographic Settings', remains the same.

**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 default.

**Data Encryption Algorithms**

Available Data Encryption Algorithms  
 Click to add or remove an algorithm from the list

Allowed Data Encryption Algorithms. Click an algorithm from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. ⓘ

**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 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.

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.

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

**Tunnel Settings**

**IPv4 Tunnel Network** 10.10.10.0/24  
 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.

**IPv4 Local network(s)** 192.168.1.0/24  
 IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges 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.

**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** 4

**communication**

**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 may be necessary in some environments.

---

**Client Settings**

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

**Topology**    
 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 2.3.9) and clients such as Yealink phones may require "net30".

---

**Ping settings**

**Inactive**    
 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 not restart.

**Ping method**    
 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

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.

**DNS Server enable**  Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

**Block Outside DNS**  Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS. 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 and not be 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.

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.

**Advanced Configuration**

**Custom options**

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 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 bandwidth limiting.

**Exit Notify**

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than 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 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**

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware.

**pfSense** COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

**OpenVPN Servers**

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Action
WAN	UDP4 / 1503 (TUN)	10.10.10.0/24	<b>Mode:</b> Remote Access ( SSL/TLS + User Auth ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256 <b>D-H Params:</b> 2048 bits		 

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term:  Both Search Clear

Enter a search string or \*nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.  Package Dependencies: <a href="#">openvpn-client-export-2.6.7</a> <a href="#">openvpn-2.6.8_1</a> <a href="#">zip-3.0_1</a> <a href="#">7-zip-23.01</a>	<a href="#">+ Install</a>
WireGuard	0.2.1	WireGuard(R) is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPsec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry.	<a href="#">+ Install</a>

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

System / Package Manager / Package Installer

Please wait while the installation of pfSense-pkg-openvpn-client-export completes.  
This may take several minutes. Do not leave or refresh the page!

Installed Packages Available Packages Package Installer

Package Installation

All repositories are up to date.  
The following 5 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:

- 7-zip: 23.01 [pfSense]
- libsysinfo: 0.0.3\_2 [pfSense]
- openvpn-client-export: 2.6.7 [pfSense]
- pfSense-pkg-openvpn-client-export: 1.9.2 [pfSense]
- zip: 3.0\_1 [pfSense]

Number of packages to be installed: 5

The process will require 31 MiB more space.  
23 MiB to be downloaded.

[1/5] Fetching openvpn-client-export-2.6.7.pkg:

Activer Windows  
Accédez aux paramètres pour activer Windows.

OpenVPN / Client Export Utility

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

**OpenVPN Server**

Remote Access Server Server UDP4:1503

**Client Connection Behavior**

Host Name Resolution Interface IP Address

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 and not be 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 configuration.

Silent Installer  Create Windows installer for unattended deploy.  
Create a silent Windows installer for unattended deploy; installer must be run as administrator.

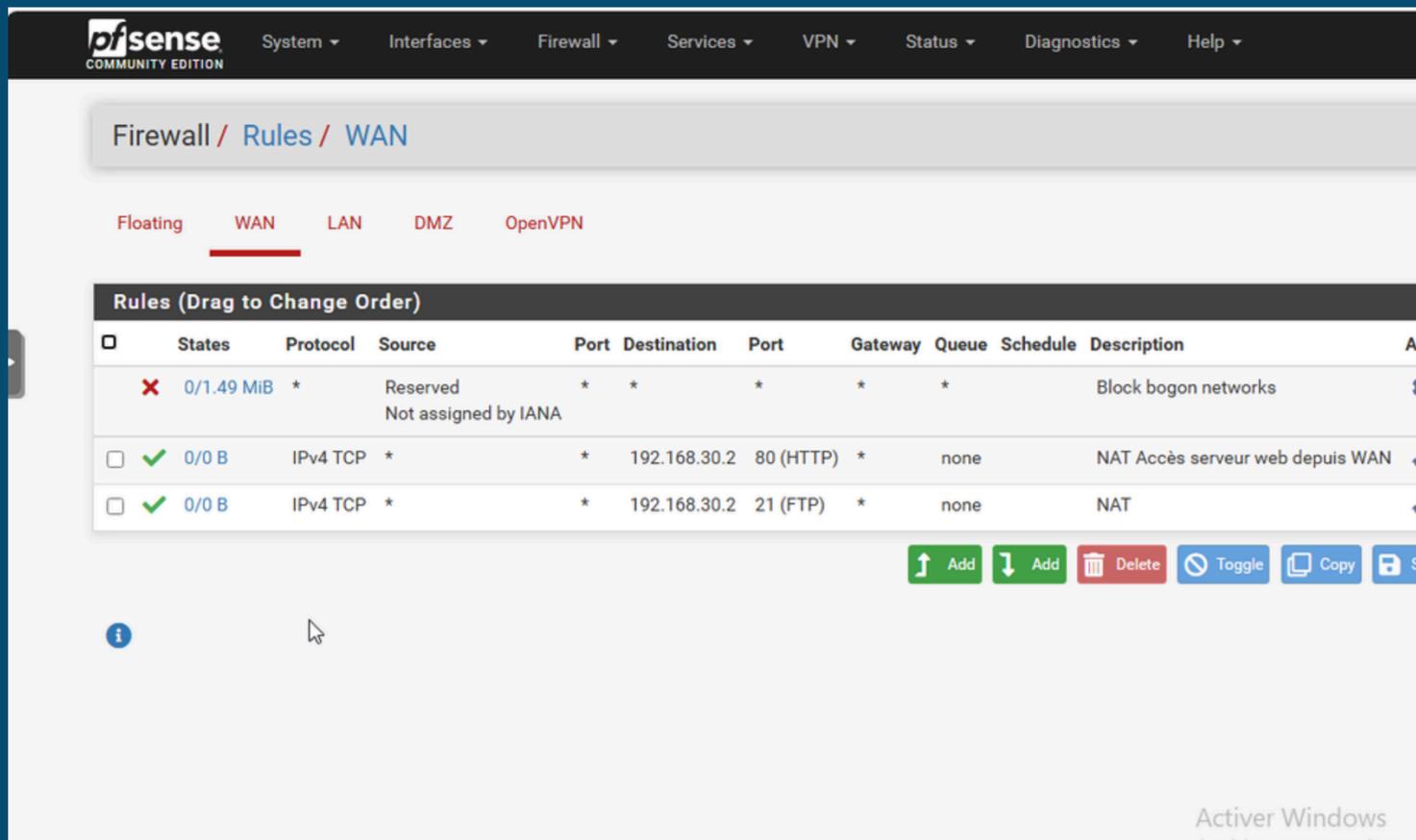
Une fois le paquet installé, retournez dans la section OpenVPN, puis accédez à Client Export Utility. C'est ici que vous trouverez le dossier de configuration à transférer à votre client, dans le dossier Archive de la partie Bundle Configurations.

**OpenVPN Clients**

User	Certificate Name	Export
nicolas	VPN-SSL-RA-FB	<p>- Inline Configurations: <a href="#">Most Clients</a> <a href="#">Android</a> <a href="#">OpenVPN Connect (iOS/Android)</a></p> <p>- Bundled Configurations: <a href="#">Archive</a> <a href="#">Config File Only</a></p> <p>- Current Windows Installers (2.6.7-1x001): <a href="#">64-bit</a> <a href="#">32-bit</a></p> <p>- Previous Windows Installers (2.5.9-1x601): <a href="#">64-bit</a> <a href="#">32-bit</a></p> <p>- Legacy Windows Installers (2.4.12-1x601): <a href="#">10/2016/2019</a> <a href="#">7/8/8.1/2012r2</a></p> <p>- Viscosity (Mac OS X and Windows): <a href="#">Viscosity Bundle</a> <a href="#">Viscosity Inline Config</a></p>

Activer Windows

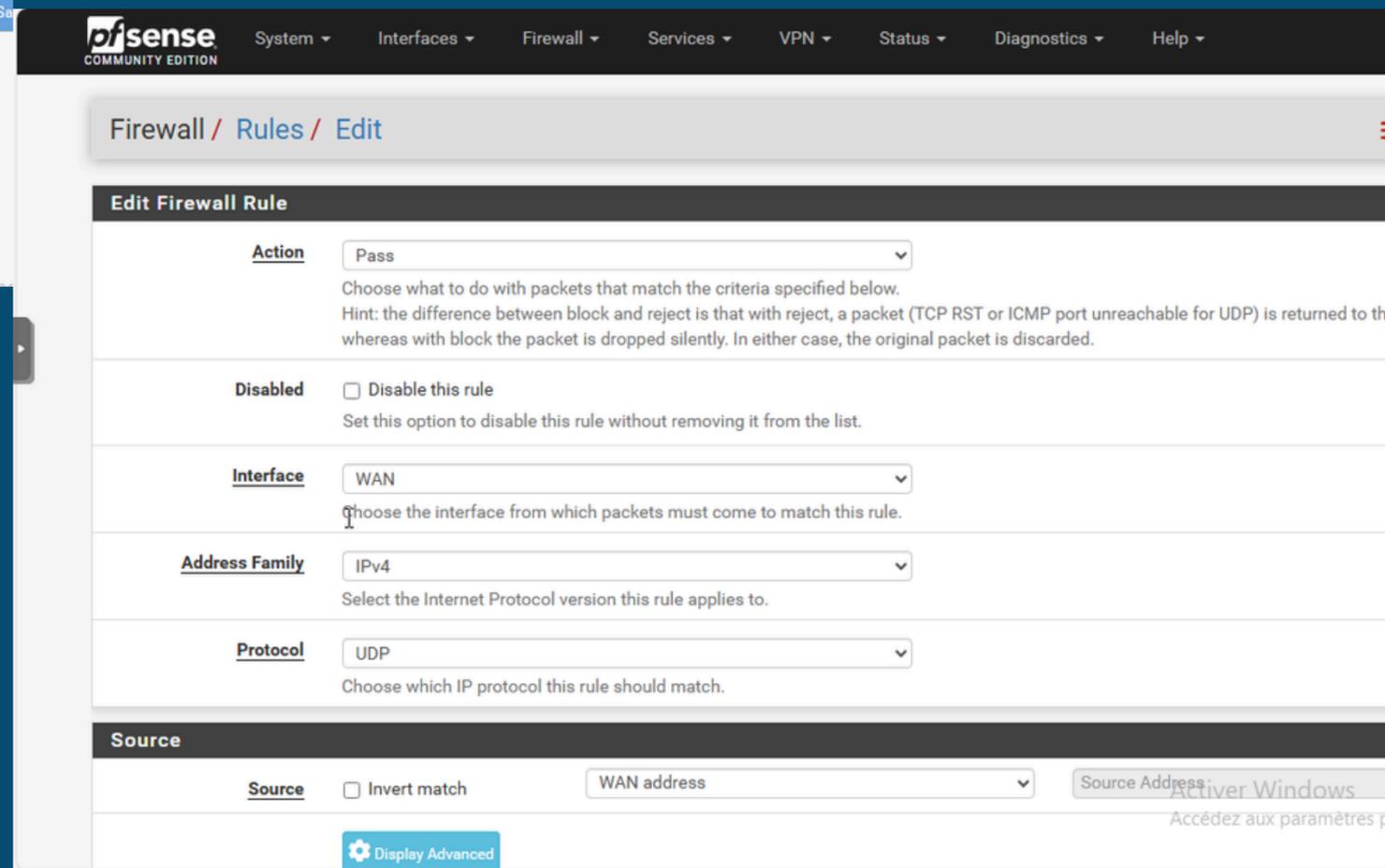
Nous allons ensuite créer une règle afin d'autoriser les flux OpenVPN venant du WAN. Pour cela, suivez les paramètres indiqués sur nos captures d'écran.



The screenshot shows the Mikrotik WinBox interface for the Firewall Rules configuration. The breadcrumb navigation is "Firewall / Rules / WAN". The "WAN" tab is selected. A table titled "Rules (Drag to Change Order)" lists existing rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
0/1.49 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

Below the table are buttons for "Add", "Delete", "Toggle", "Copy", and "Save".



The screenshot shows the "Edit Firewall Rule" configuration page in Mikrotik WinBox. The breadcrumb navigation is "Firewall / Rules / Edit". The configuration parameters are as follows:

- Action:** Pass
- Disabled:**  Disable this rule
- Interface:** WAN
- Address Family:** IPv4
- Protocol:** UDP
- Source:**  Invert match, WAN address

There is a "Display Advanced" button at the bottom.

**Destination**

**Destination**  Invert match Any

**Destination Port Range** OpenVPN (1194)  OpenVPN (1194)

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 system (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 log.

**Advanced Options**

Activer Windows

**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)**

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/1.54 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙️
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	192.168.30.2	80 (HTTP)	*	none		NAT Accès serveur web depuis WAN	📌 📄 🗑️ ✖️
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	192.168.30.2	21 (FTP)	*	none		NAT	📌 📄 🗑️ ✖️
<input type="checkbox"/>	0/0 B	IPv4 UDP	WAN address	*	*	1194 (OpenVPN)	*	none			📌 📄 🗑️ ✖️

Accédez aux paramètres pour activer Windows.

[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](#) [Save](#)

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 / (other) / 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**

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](#)

Floating WAN LAN DMZ OpenVPN

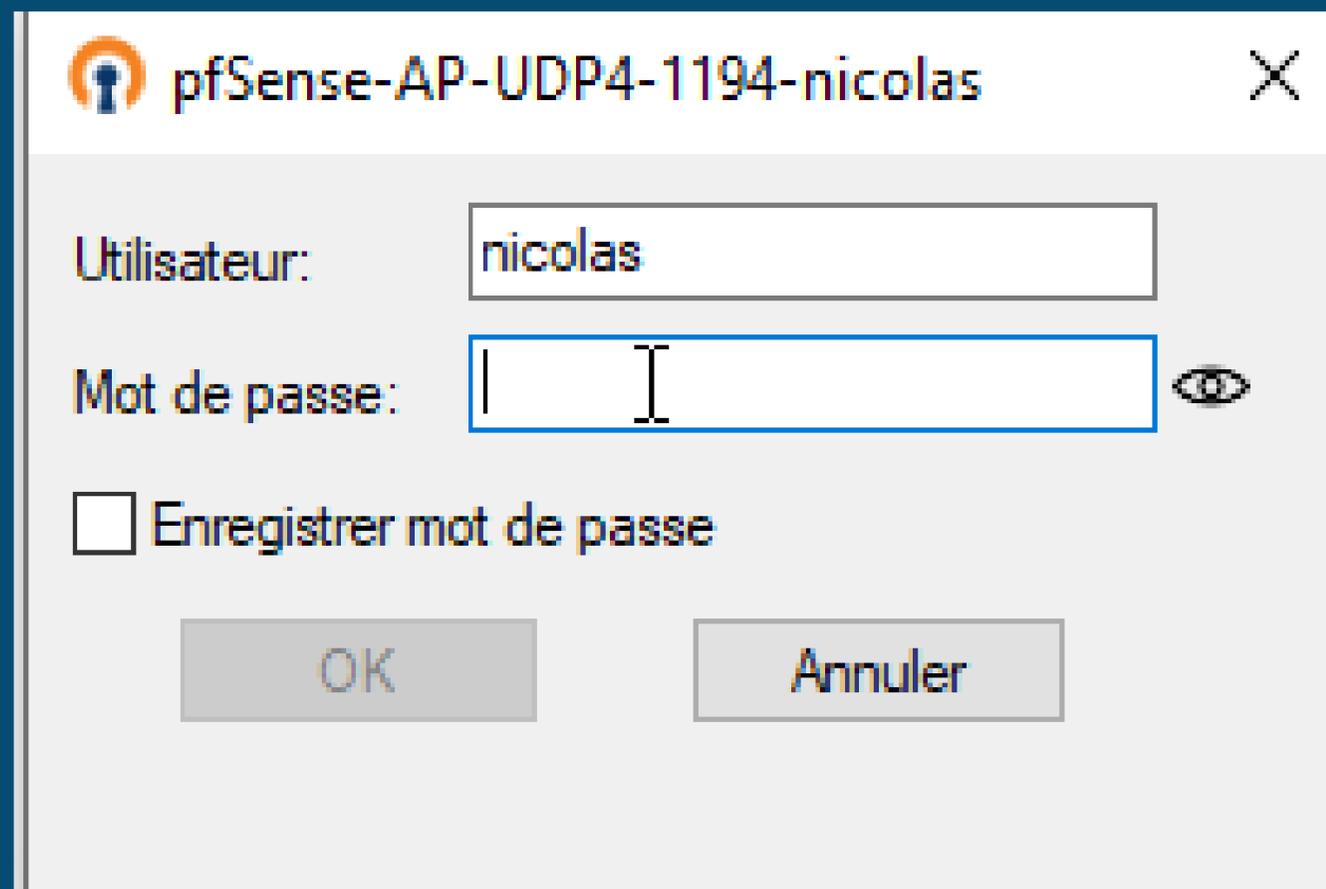
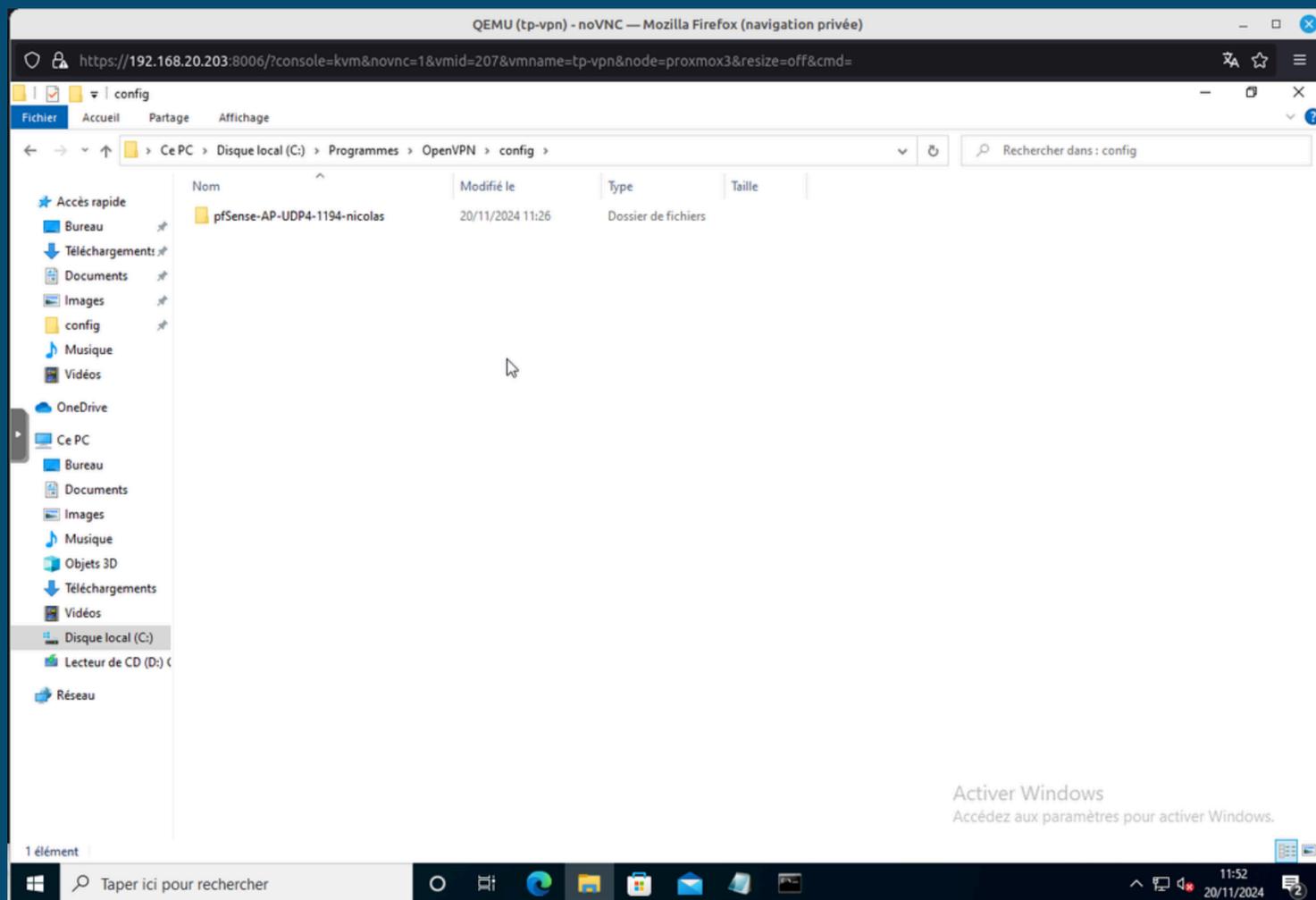
### Rules (Drag to Change Order)

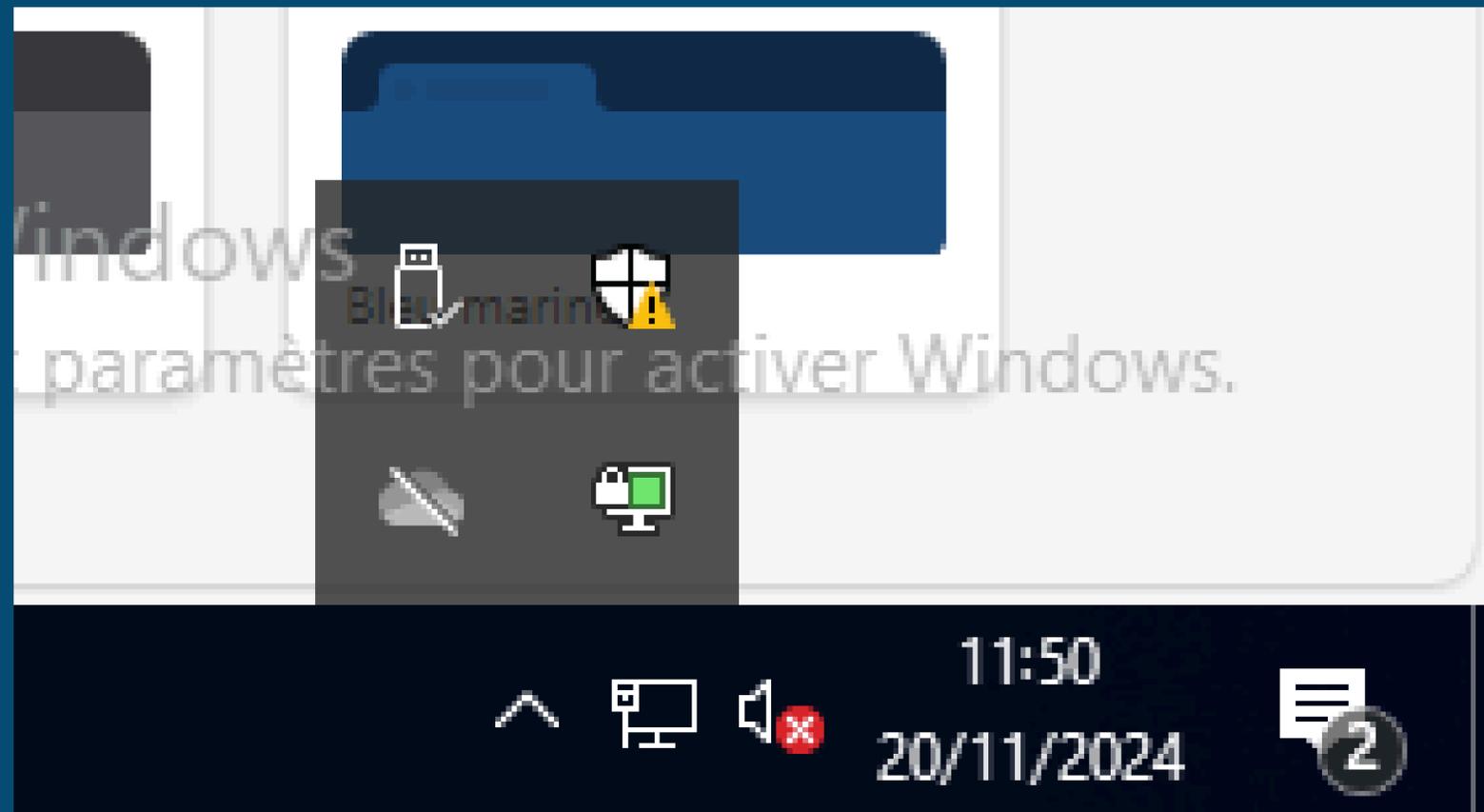
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Action
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.1.10	3389 (MS RDP)	*	none	autoriser rdp vers PC Windows 10	

Add Add Delete Toggle Copy Save



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:86a6: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>
```