

Documentation VPN Bgtw

Table des matières

Configuration VPN pour réseau ADM	2
Configuration du serveur VPN ADM4 :.....	4
Configuration pour réseau DEV4.....	9
Déclaration des utilisateurs :.....	14
Utilisateur ADM4 :.....	14
Utilisateur DEV4 :.....	16
Règle de pare-feu du VPN :	18
Tests VPN.....	19
Tests VPN Réseaux ADM :	19
Tests VPN Réseau DEV :	21

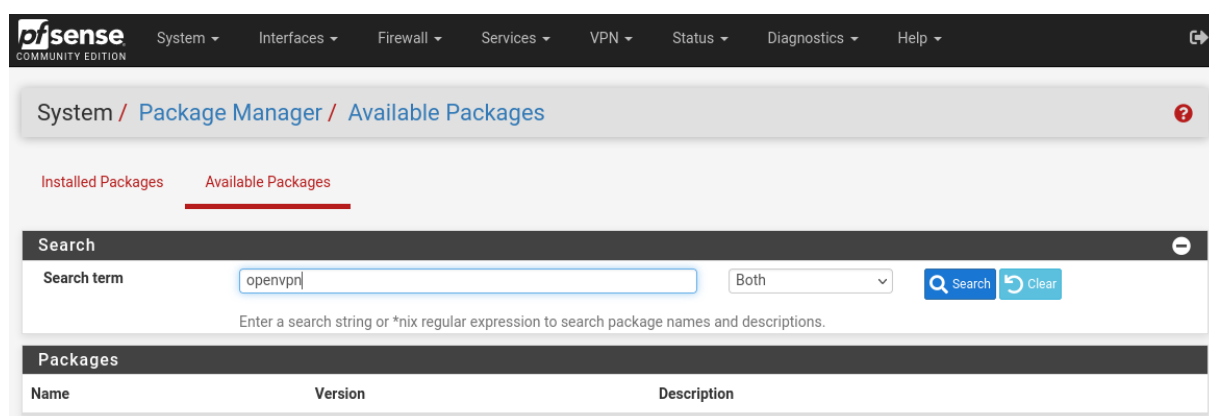
Configuration VPN pour réseau ADM

Nous devons fournir un accès aux utilisateurs du réseau ADM4 pour qu'ils puissent se connecter depuis internet au réseau interne de l'entreprise afin de pouvoir continuer à l'administrer depuis n'importe où.

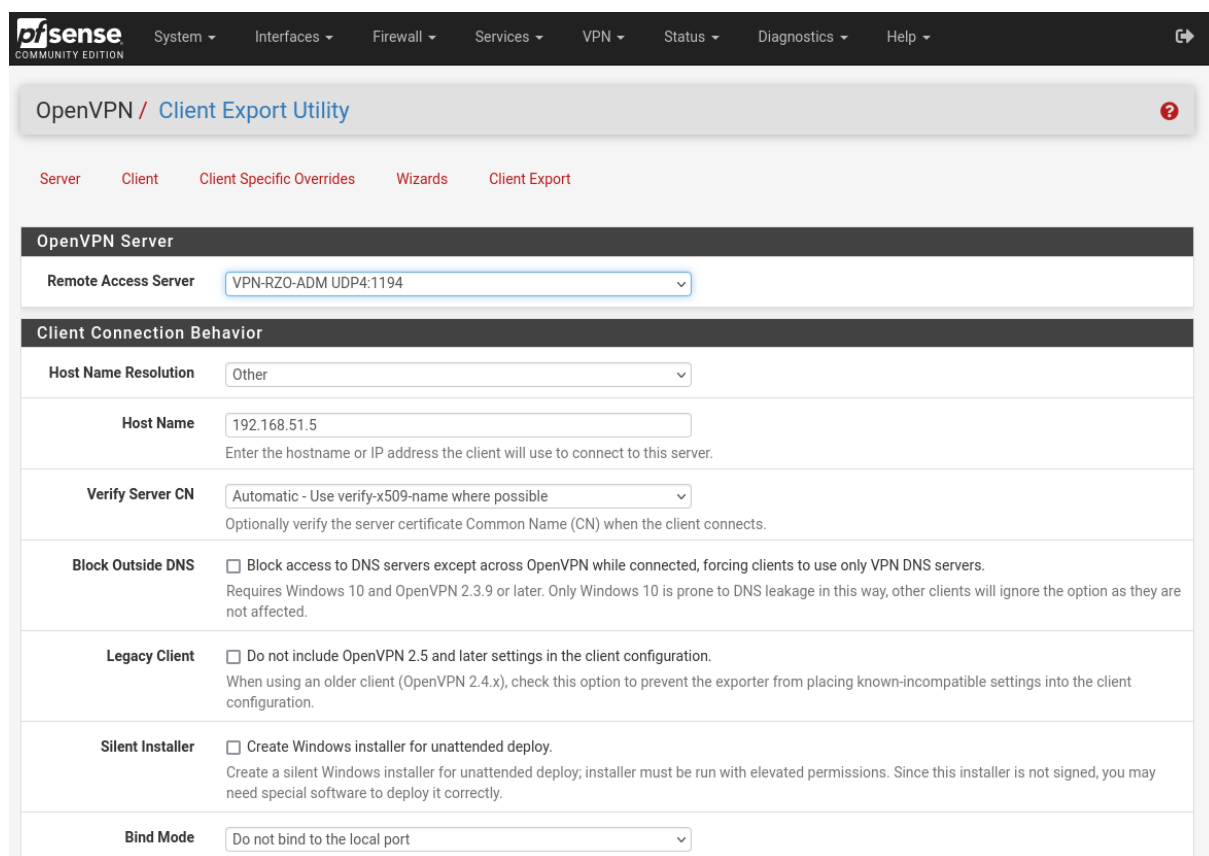
Il y avait aussi le réseau DEV4 qui devait pouvoir y accéder pour pouvoir notamment continuer d'administrer le site web de l'entreprise à distance.

Pour répondre à cela, nous avons mis en place un VPN avec OpenVPN.

Avant de configurer le serveur VPN, pour se faciliter le travail, nous allons installer le package qui permet d'exporter plus facilement les clients et donc avoir une connexion directe entre le client et le serveur sans avoir à modifier quoi que ce soit sur le poste du client.



The screenshot shows the pfSense Community Edition interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main breadcrumb trail is System / Package Manager / Available Packages. Below this, there are tabs for Installed Packages and Available Packages. A search bar is present with the text 'openvpn' entered. The search results table is empty, with columns for Name, Version, and Description.



The screenshot shows the pfSense OpenVPN Client Export Utility configuration page. The top navigation bar is the same as the previous screenshot. The main breadcrumb trail is OpenVPN / Client Export Utility. Below this, there are tabs for Server, Client, Client Specific Overrides, Wizards, and Client Export. The configuration section is titled 'OpenVPN Server' and includes a dropdown for 'Remote Access Server' set to 'VPN-RZO-ADM UDP4:1194'. Below this is the 'Client Connection Behavior' section, which includes several options: 'Host Name Resolution' set to 'Other', 'Host Name' set to '192.168.51.5', 'Verify Server CN' set to 'Automatic - Use verify-x509-name where possible', 'Block Outside DNS' (unchecked), 'Legacy Client' (unchecked), 'Silent Installer' (unchecked), and 'Bind Mode' set to 'Do not bind to the local port'.

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
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

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

Configuration du serveur VPN ADM4 :

Nous allons d'abord configurer le tunnel pour les utilisateurs du réseau ADM4 :

pfSense
COMMUNITY EDITION

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

VPN / OpenVPN / Servers / Edit

Refresh Save Cancel Help

Servers Clients Client Specific Overrides Wizards Client Export

General Information

Description

VPN-RZO-ADM

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.

Unique VPN ID

Server 1 (ovpns1)

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.)

Il faut bien choisir sur quelle interface on veut que le service tourne, en l'occurrence la patte PUB4 étant celle qui est reliée au routeur Fgtw. Il faut aussi choisir le bon port.

Endpoint Configuration	
Protocol	UDP on IPv4 only
Interface	PUB4 The interface or Virtual IP address where OpenVPN will receive client connections.
Local port	1194 The port used by OpenVPN to receive client connections.
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.
TLS Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 473becf5b94200578c2f61fc88c99438</pre> Paste the TLS key here. This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.
TLS Key Usage Mode	TLS Authentication In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.
TLS keydir direction	Use default direction The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.
Peer Certificate Authority	m2l.fr
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager

Il faut aussi choisir quel est le certificat d'autorité, nous c'est le certificat de l'entreprise du contexte. Nous devons choisir quels paramètres de chiffrement nous allons utiliser, la longueur du Diffie-Hellman etc....

Peer Certificate Authority	m2l.fr
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-Serv-Cert (Server: Yes, CA: m2l.fr, In Use) 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.

Nous allons déclarer quel sera le sous réseau utilisé par ce tunnel VPN, ici nous avons opté pour 10.7.4.0/29

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").
Tunnel Settings	
IPv4 Tunnel Network	10.7.4.0/29
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.

Nous allons autoriser les réseaux auxquels les utilisateurs de ADM4 peuvent accéder, étant donné que ce sont les administrateurs, ils ont le droit à tous les réseaux.

IPv4 Local network(s)	10.54.4.0/24, 172.20.0.0/16, 172.31.4.224/27, 192.168.104.0/24, 192.1
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	10 
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.

On va donner dynamiquement aux utilisateurs une configuration IP, un peu comme un DHCP.

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".
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

Voici la suite de la configuration IP :

Advanced Client Settings	
DNS Default Domain	☒ Provide a default domain name to clients
DNS Default Domain	m2l.fr
DNS Server enable	☒ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	10.54.4.253
DNS Server 2	
DNS Server 3	
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
NTP Server 1	10.54.4.253
NTP Server 2	
NetBIOS enable	☐ Enable NetBIOS over TCP/IP If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

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 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

C'est la fin de la configuration du Serveur VPN ADM, il est prêt à etre utilisé.

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
PUB4	UDP4 / 1194 (TUN)	10.7.4.0/29	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-RZO-ADM	  

Configuration pour réseau DEV4

Dans cette partie je vais montrer la configuration du VPN pour DEV4 :

Ici on va changer le nom, et surtout on va changer le port sur lequel le serveur écoute parce que sur une même interface, on ne peut pas avoir deux fois le même port en écoute.

The screenshot shows the Pfsense web interface for configuring an OpenVPN server. The breadcrumb trail is 'VPN / OpenVPN / Servers / Edit'. The 'Servers' tab is selected. The configuration is divided into three main sections: General Information, Mode Configuration, and Endpoint Configuration.

General Information	
Description	VPN-RZO-DEV 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.
Unique VPN ID	Server 2 (ovpns2)

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	PUB4 The interface or Virtual IP address where OpenVPN will receive client connections.
Local port	1195 The port used by OpenVPN to receive client connections.

Ici on prend toujours le certificat du serveur VPN et on choisit le certificat d'autorité de l'organisme.

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.
TLS Key	# # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 6a5ee833db29d3094a2d7579f050c0df Paste the TLS key here. This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.
TLS Key Usage Mode	TLS Authentication In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.
TLS keydir direction	Use default direction The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.
Peer Certificate Authority	m2l.fr
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-Serv-Cert (Server: Yes, CA: m2l.fr, In Use) 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 The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. i	AES-256-GCM AES-128-GCM CHACHA20-POLY1305 Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list
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").	

Ici, pour différencier les utilisateurs du serveur VPN ADM4 et ceux du VPN DEV4 on va mettre le réseau du tunnel en 10.6.4.0/28 et surtout on va autoriser uniquement les réseaux 10.54.4.0/24, 192.168.4.0/24 et 172.31.4.224/27 parce qu'ils ont besoin d'accéder uniquement à ces réseaux en tant que développeur.

Tunnel Settings	
IPv4 Tunnel Network	10.6.4.0/28 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)	10.54.4.0/24, 192.168.4.0/24, 172.31.4.224/27 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	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.

Ici on va choisir la configuration IP des utilisateurs qui utilisent le VPN.

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".
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

On rajoute les serveurs de temps et de noms et on peut continuer la configuration.

Advanced Client Settings	
DNS Default Domain	☒ Provide a default domain name to clients
DNS Default Domain	m2l.fr
DNS Server enable	☒ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	10.54.4.253
DNS Server 2	
DNS Server 3	
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
NTP Server 1	10.54.4.253
NTP Server 2	
NetBIOS enable	☐ Enable NetBIOS over TCP/IP If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

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 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	

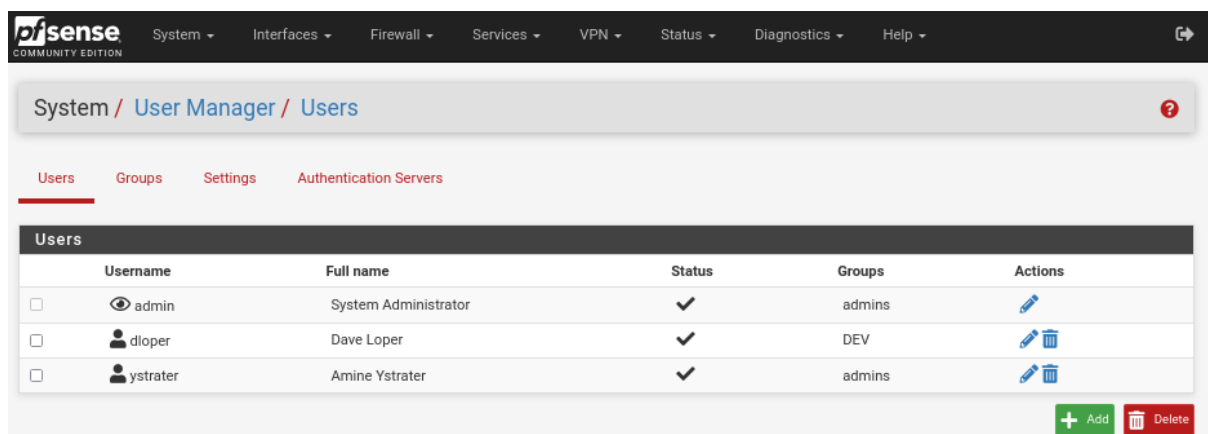
On peut voir ici que le serveur VPN DEV est créé et prêt à l'emploi.

PUB4	UDP4 / 1195 (TUN)	10.6.4.0/28	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-RZO-DEV   
------	----------------------	-------------	--	---

Déclaration des utilisateurs :

Utilisateur ADM4 :

On veut fournir la configuration pour le client afin qu'il puisse se connecter simplement en VPN, pour cela on va donc créer des utilisateurs dans le PfSense :

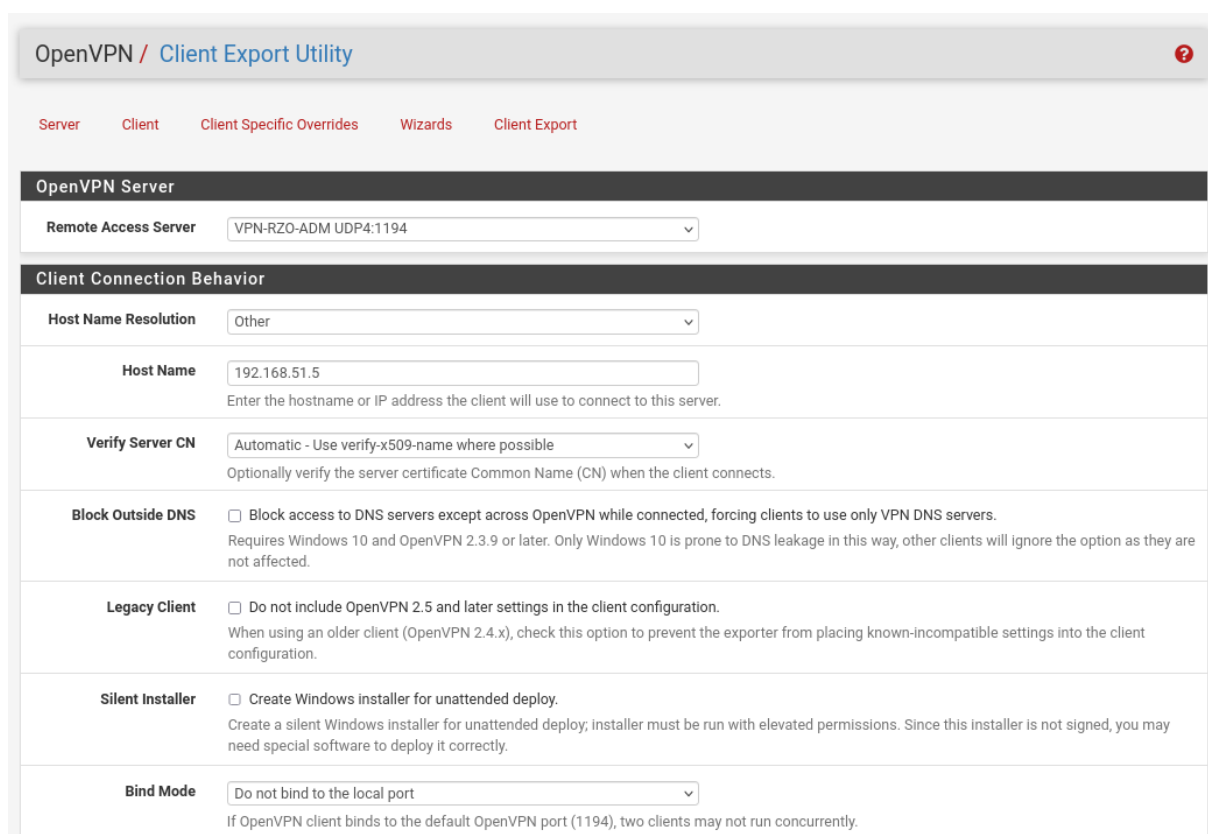


The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main breadcrumb trail is System / User Manager / Users. Below this, there are tabs for Users, Groups, Settings, and Authentication Servers. The 'Users' tab is active, displaying a table of users. The table has columns for Username, Full name, Status, Groups, and Actions. Three users are listed: 'admin' (System Administrator), 'dloper' (Dave Loper), and 'ystrater' (Amine Ystrater). Each user has a checkbox, an eye icon, and a status checkmark. The 'Actions' column contains edit and delete icons. At the bottom right, there are buttons for '+ Add' and 'Delete'.

	Username	Full name	Status	Groups	Actions
☐	admin	System Administrator	✓	admins	
☐	dloper	Dave Loper	✓	DEV	
☐	ystrater	Amine Ystrater	✓	admins	

Ici on va fournir au client «ystrater » un accès au VPN pour le réseau ADM :

L'interface de connexion au serveur VPN est donc la patte Internet du routeur Frontal Fgtw qui possède un Nat pour rediriger le flux vers notre patte PUB4 sur lequel le serveur VPN écoute.



The screenshot shows the pfSense web interface for the OpenVPN Client Export Utility. The top navigation bar includes links for Server, Client, Client Specific Overrides, Wizards, and Client Export. The 'Client Export' tab is active, displaying the 'OpenVPN Server' section. The 'Remote Access Server' dropdown is set to 'VPN-RZO-ADM UDP4:1194'. Below this, the 'Client Connection Behavior' section contains several settings: 'Host Name Resolution' is set to 'Other'; 'Host Name' is set to '192.168.51.5'; 'Verify Server CN' is set to 'Automatic - Use verify-x509-name where possible'; 'Block Outside DNS' is unchecked; 'Legacy Client' is unchecked; 'Silent Installer' is unchecked; and 'Bind Mode' is set to 'Do not bind to the local port'.

OpenVPN Server

Remote Access Server: VPN-RZO-ADM UDP4:1194

Client Connection Behavior

Host Name Resolution: Other

Host Name: 192.168.51.5
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.

Nous avons besoin de toucher à rien.

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, Window ▾) 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	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	

Notre utilisateur est prêt à être exporté et qu'il pourra désormais se connecter !

ystrater

ystrater_Cert

- Inline Configurations:

Most Clients

Android

OpenVPN Connect (iOS/Android)

- Bundled Configurations:

Archive

Config File Only

- Current Windows Installers (2.6.7-1x001):

64-bit

32-bit

- Previous Windows Installers (2.5.9-1x601):

64-bit

32-bit

- Legacy Windows Installers (2.4.12-1x601):

10/2016/2019

7/8/8.1/2012r2

- Viscosity (Mac OS X and Windows):

Viscosity Bundle

Viscosity Inline Config

Utilisateur DEV4 :

Pour donner un accès aux utilisateurs du réseau DEV4 il faut faire attention au serveur que l'on choisit, ici on doit choisir celui qui est sur le port 1195 pour qu'il ait les caractéristiques du réseau DEV4 :

OpenVPN / Client Export Utility

Server

Client

Client Specific Overrides

Wizards

Client Export

OpenVPN Server

Remote Access Server

VPN-RZO-DEV UDP4:1195

Client Connection Behavior

Host Name Resolution

Other

Host Name

192.168.51.5

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, Window

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

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

Search

Search term

Search

Clear

Enter a search string or *nix regular expression to search.

Notre utilisateur est créé et on peut l'utiliser :

OpenVPN Clients		
User	Certificate Name	Export
dloper	dloper_Cert	- 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

Règle de pare-feu du VPN :

pfSense

COMMUNITY EDITION

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

🔍 📄 ?

Firewall / Rules / OpenVPN

Floating PUB4 PRIV4 ADM4 DEV4 USR4 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 ICMP any	vpn_and_adm_subnet	*	*	*	none		Autoriser les requêtes ping	
☐	✓	0/0 B	IPv4 TCP	vpn_and_adm_subnet	*	priv4_auth	636 (LDAP/S)	*	none	LDAPS (Authentication Sécurisée)	
☐	✓	0/0 B	IPv4 UDP	vpn_and_adm_subnet	*	Fgtw_Pub	53 (DNS)	*	none	allow dns -> network	
☐	✓	0/0 B	IPv4 TCP	vpn_and_adm_subnet	*	ADM4 address	443 (HTTPS)	*	none	Autorise HTTPS VPN & ADM	
☐	✓	0/0 B	IPv4 TCP	vpn_and_adm_subnet	*	*	22 (SSH)	*	none	Administrer SSH	
☐	✓	0/0 B	IPv4 TCP	vpn_dev_and_dev_subnet	*	pub4_WebR	22 (SSH)	*	none	Déposer Code DEV - Pub4.WebR	
☐	✓	0/0 B	IPv4 TCP	vpn_dev_and_dev_subnet	*	priv4_auth	636 (LDAP/S)	*	none	LDAPS - authentication secure	
☐	✓	0/0 B	IPv4 TCP	vpn_dev_and_dev_subnet	*	pub4_WebR	443 (HTTPS)	*	none	Autorise vers HTTPS	
☐	✓	0/0 B	IPv4 *	*	*	! not INTERNET	*	*	none	Autorise Sortie Internet	
☐	✗	0/0 B	IPv4 *	*	*	*	*	none		TOUT BLOQUE	

↑ Add

↓ Add

🗑 Delete

🔄 Toggle

📄 Copy

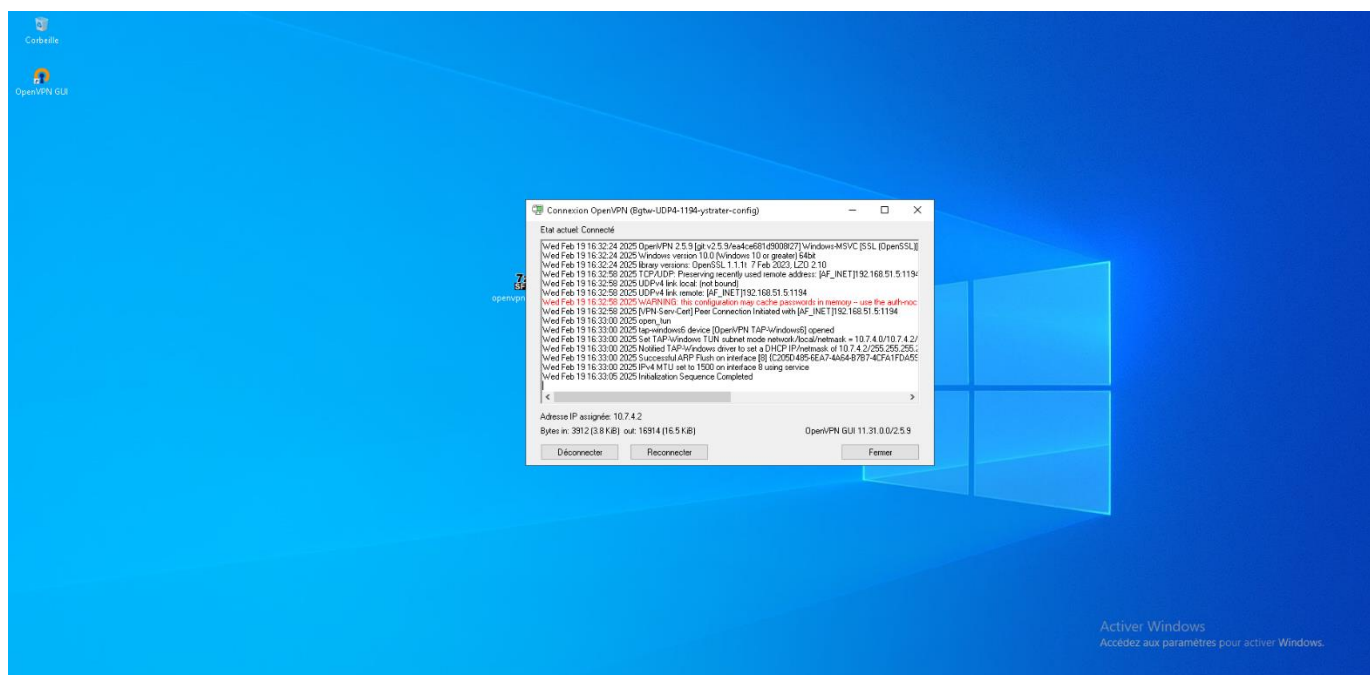
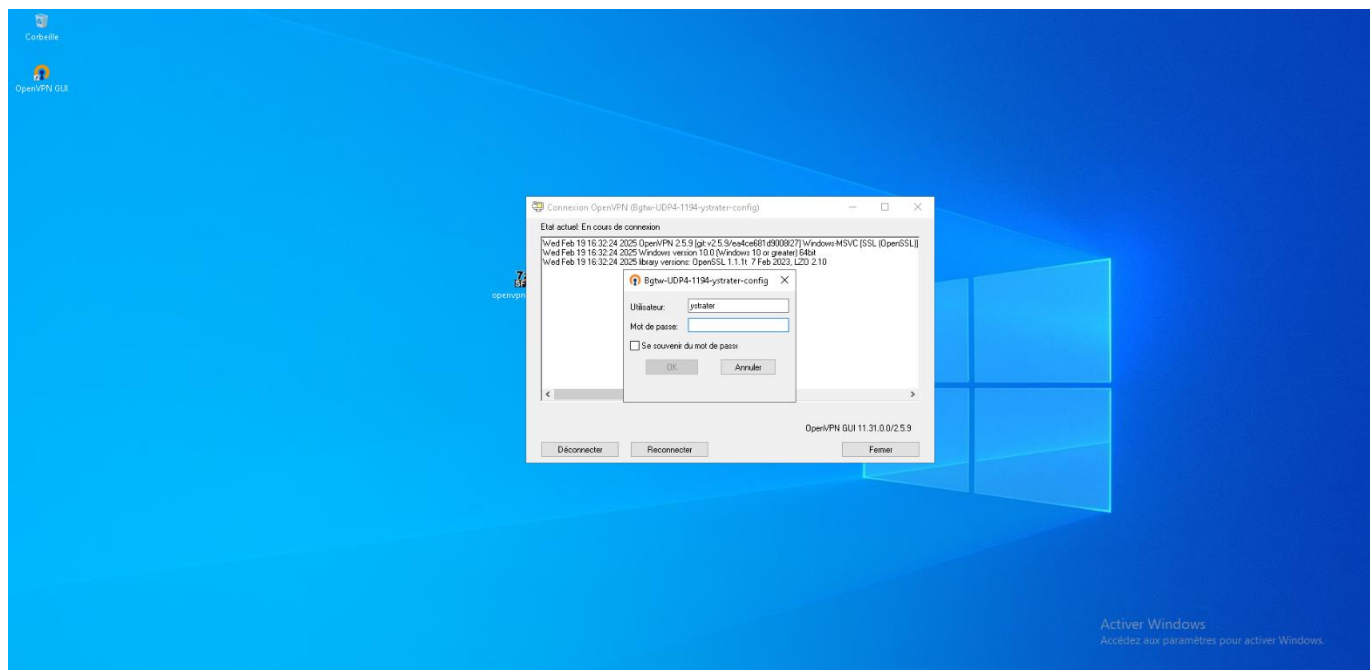
💾 Save

⚡ Separator

Tests VPN

Tests VPN Réseaux ADM :

On peut voir qu'on peut l'exporter et qu'il peut se connecter sur le réseau ADM :



Le client à bien récupéré l'adresse IP du tunnel et donc connecté dans le réseau de l'organisme :

```
C:\Users\sio>ipconfig

Configuration IP de Windows

Carte inconnue OpenVPN Wintun :

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

Carte Ethernet LAN :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv4. . . . . : 192.168.1.55
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.1

Carte inconnue OpenVPN TAP-Windows6 :

    Suffixe DNS propre à la connexion. . . : m2l.fr
    Adresse IPv6 de liaison locale. . . . : fe80::295b:8a7e:623d:253%13
    Adresse IPv4. . . . . : 10.7.4.2
    Masque de sous-réseau. . . . . : 255.255.255.248
    Passerelle par défaut. . . . . :
```

Nous sommes connecté et nous pouvons accéder à l'interface d'administration, chose qu'on ne peut pas faire en tant qu'utilisateur d'un autre réseau.

The screenshot displays the pfSense Status Dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into several sections:

- System Information:** Displays details about the system, including Name (Bgtw.m2l.fr), User (admin@10.7.4.2), Version (2.7.2-RELEASE), Uptime (05 Hours 20 Minutes 16 Seconds), Current date/time (Wed Feb 19 15:35:04 UTC 2025), DNS server(s) (10.54.4.253), Last config change (Wed Feb 19 15:05:17 UTC 2025), State table size (0% (31/198000)), MBUF Usage (1% (5842/1000000)), CPU usage (8%), Memory usage (20% of 1986 MB), and SWAP usage (0% of 1024 MB).
- Interfaces:** Lists network interfaces and their status. The table shows:

Interface	Speed	Link	IP Address
PUB4	1000baseT <full-duplex>	Up	10.54.4.254
PRIV4	1000baseT <full-duplex>	Up	172.31.4.254
ADM4	1000baseT <full-duplex>	Up	192.168.104.254
DEV4	1000baseT <full-duplex>	Up	192.168.4.254
USR4	1000baseT <full-duplex>	Up	172.20.255.254

- Gateways:** Lists configured gateways and their status. The table shows:

Name	RTT	RTTsd	Loss	Status
FgtwPub 10.54.4.253	1.7ms	1.4ms	0.0%	Online
GTW_PRIV 172.31.4.254	0.1ms	0.1ms	0.0%	Online
GTW_ADM 192.168.104.254	0.1ms	0.1ms	0.0%	Online
GTW_DEV 192.168.4.254	0.1ms	0.1ms	0.0%	Online
GTW_USR 172.20.255.254	0.1ms	0.1ms	0.0%	Online

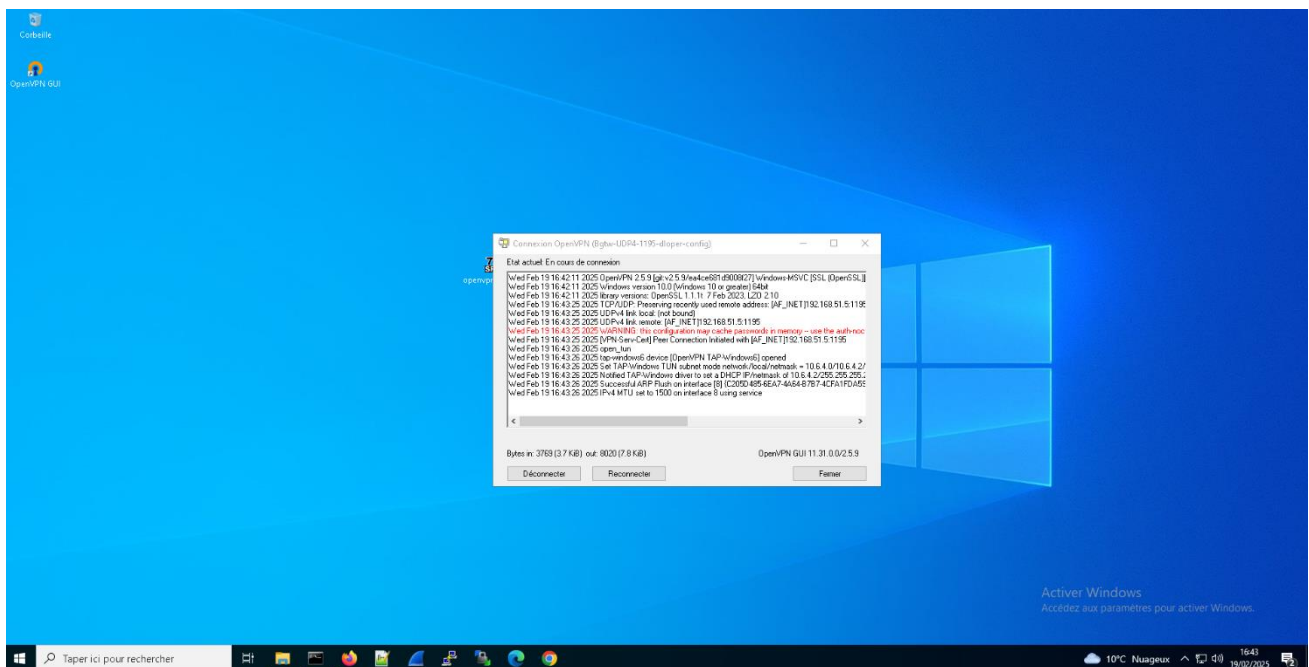
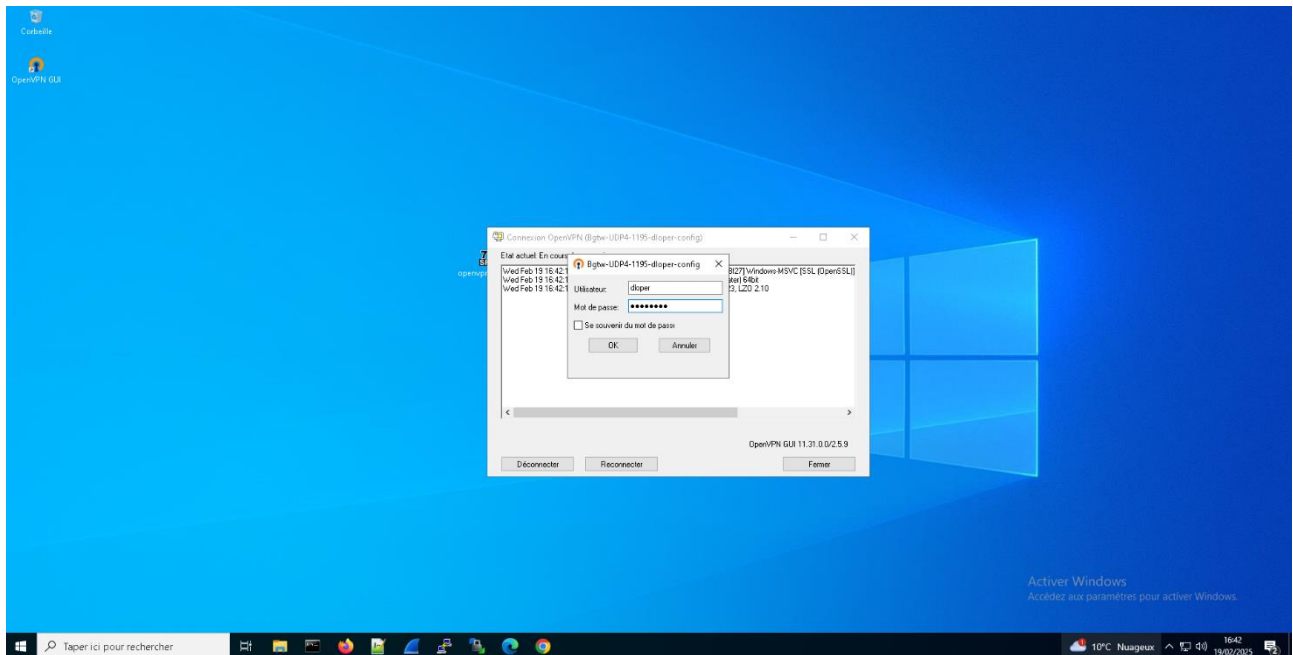
- Services Status:** Lists installed services and their status. The table shows:

Service	Description	Action
dpinger	Gateway Monitoring Daemon	Start/Stop/Restart
kea-dhcp4	Kee DHCP Server	Start/Stop/Restart
openvpn	OpenVPN server: VPN-RZD-ADM	Start/Stop/Restart
openvpn	OpenVPN server: VPN-RZD-DEV	Start/Stop/Restart

The bottom of the screen shows the Windows taskbar with the search bar and system tray.

Tests VPN Réseau DEV :

On peut s'y connecter :



On voit bien qu'on récupère le réseau VPN du tunnel DEV4

```
Corbeille
Invite de commandes

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

C:\Users\sio>ipconfig

Configuration IP de Windows

Carte inconnue OpenVPN Wintun :

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

Carte Ethernet LAN :

    Suffixe DNS propre à la connexion. . . : GEIFFEL.FR
    Adresse IPv4. . . . . : 192.168.51.6
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.51.254

Carte inconnue OpenVPN TAP-Windows6 :

    Suffixe DNS propre à la connexion. . . : m2l.fr
    Adresse IPv6 de liaison locale. . . . : fe80::f9d9:c61:1003:32e6%8
    Adresse IPv4. . . . . : 10.6.4.2
    Masque de sous-réseau. . . . . : 255.255.255.240
    Passerelle par défaut. . . . . :

C:\Users\sio>
```

Et qu'on ne peut pas ping l'interface d'administration :

```
Corbeille
Invite de commandes - ping 192.168.104.254

C:\Users\sio>ipconfig

Configuration IP de Windows

Carte inconnue OpenVPN Wintun :

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

Carte Ethernet LAN :

    Suffixe DNS propre à la connexion. . . : GEIFFEL.FR
    Adresse IPv4. . . . . : 192.168.51.6
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.51.254

Carte inconnue OpenVPN TAP-Windows6 :

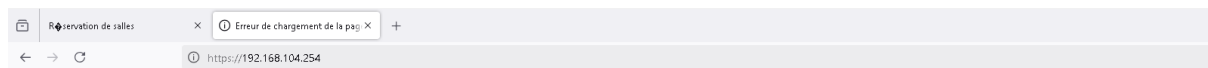
    Suffixe DNS propre à la connexion. . . : m2l.fr
    Adresse IPv6 de liaison locale. . . . : fe80::f9d9:c61:1003:32e6%8
    Adresse IPv4. . . . . : 10.6.4.2
    Masque de sous-réseau. . . . . : 255.255.255.240
    Passerelle par défaut. . . . . :

C:\Users\sio>ping 192.168.104.254

Envoi d'une requête 'Ping' 192.168.104.254 avec 32 octets de données :
Délai d'attente de la demande dépassé.

C:\Users\sio>
```

Ni s'y connecter, preuve que nous sommes bien dans le tunnel VPN pour développeur :



Le délai d'attente est dépassé

Le serveur à l'adresse 192.168.104.254 met trop de temps à répondre.

- Le site est peut-être temporairement indisponible ou surchargé. Réessayez plus tard ;
- Si vous n'arrivez à naviguer sur aucun site, vérifiez la connexion au réseau de votre ordinateur ;
- Si votre ordinateur ou votre réseau est protégé par un pare-feu ou un proxy, assurez-vous que Firefox est autorisé à accéder au Web.

Réessayer

Activer V