# DOCUMENTATION AP (Partie B)

# LEPINE Mattéo

# BTS SIO 2

# Table des matières :

1 - Création de l'interface DMZ sur Proxmox	2
2 - Ajout de l'interface au PfSense :	3
2.1 - Configuration de l'interface de la DMZ via l'interface Web du PfSense :	3
3 - Règles de pare-feu	5
3.1 - Règles du LAN :	5
3.2 - Règles sur le WAN :	5
3.3 - Règles sur le VPN :	5
3.4 - Redirection de port DMZ pour la page web :	5
3.5 - Communication vers internet de chacun des sous réseaux :	6
4 - Mise en place du VPN	6
4.1 - Création des certificats :	6
4.2 - Exportation de la configuration du VPN :	14
4.3 - Tests du VPN :	15

## 1 - Création de l'interface DMZ sur Proxmox

Sur ProxMox, on crée l'interface pour la DMZ :



On nomme l'interface et on y ajoute un commentaire si besoin :

Créer: Linux Brid	lge		$\otimes$
Nom: IPv4/CIDR: Passerelle (IPv4): IPv6/CIDR: Passerelle (IPv6):	vmbr5	Démarrage automatique: Gère les VLAN: Ports du pont (bridge): Commentaire:	☑ □ Interface DMZ
😧 Aide			Avancé 🗌 🛛 Créer

On applique la configuration pour démarrer l'interface sur le ProxMox :



# 2 - Ajout de l'interface au PfSense :

✓	┛ Résumé	Ajo	uter 🗸 Supprimer
💭 100 (Debian12) 🛑	>_ Console		Disque dur
🖵 101 (PfSense) 🔴	🖵 Matériel	0	Lecteur CD/DVD
🖵 102 (WindowsServer) 🔴	Cloud-Init	11	Carte réseau
			Diamus CCI

## 2.1 - Configuration de l'interface de la DMZ via l'interface Web du PfSense :

	System <del>-</del>	Interfaces 👻	Firew
		Assignments	]
Status / Da	shboard	WAN	
System Inform	ation	LAN	

## Ajouter l'interface :

Interfaces / Interface Assignments											
Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGG		
Interface			Network por	rt -							
WAN			vtnet0 (bc	24:11:f5:c8:	69)				~		
LAN			vtnet1 (bc	:24:11:e8:99	6c)				*	前 Delete	
Available network ports:	vtnet2 (bc:24:11:67:d6:03)						*	+ Add			

Aller sur le menu de l'interface et la configurer :

General Configuratio	n
Enable	Enable interface
Description	DMZ
	Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx or leave blank.
МТО	
	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	
	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect)
	Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configura	ition
IPv4 Address	193.253.40.194 / 30 ~
IPv4 Upstream gateway	None   Add a new gateway
	If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.

Ensuite sauvegarder la configuration et l'appliquer, la configuration est terminée.

## 3 - Règles de pare-feu

## 3.1 - Règles du LAN :

F	Firewall / Rules / LAN											
FI	oatin	g WAN	LAN	DMZ Open	/PN							
R	ules	(Drag to Cha	ange Orde	er)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	~	0/232 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	\$
	~	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	ϑ聋⊡⊘ <u>`</u> a×
	~	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	҄҈ℋ <b>ⅅ</b> Ѻ҆҄ <b>ӓ</b> ×
	~	0/794.49 MiB	IPv4*	193.253.40.0/24	*	*	*	*	none			ϑ聋⊡⊘亩×
	×	0/0 B	IPv4+6 *	LAN subnets	*	DMZ subnets	*	*	none		Bloquer les flux LAN vers la DMZ	ৼৢ৾৾৾৾৾৾৾৾৾৾৾৾৾৾৾

#### 3.2 - Règles sur le WAN :

Floating	WAN	LAN	DMZ Ope	enVPN							
Rules (D	rag to Char	ige Order	)								
٥	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□ ✓	6/21.97 MiB	IPv4*	WAN subnets	s *	*	*	*	none		Accès page WEB depuis le WAN	ᢤ᠕᠐ᢆ⊘
□ ✔≅	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		Règle OPENVPN	ℋⅆℚѺൎຓ×

## 3.3 - Règles sur le VPN :

Fl	pating	WAN I	.AN DM	Z 0	penVPN	_						
Ru	Rules (Drag to Change Order)											
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	<b>√</b> ?≣	1/13.34 MiB	IPv4 TCP	*	*	193.253.40.177	3389 (MS RDP)	*	none		Accès RDP WS	ϑ৶ৢঢ়৶
	~	7/3.77 MiB	IPv4 TCP	*	*	This Firewall (self)	80 (HTTP)	*	none		Accès page web	₰₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽

# 3.4 - Redirection de port DMZ pour la page web :

Port Forwa	ard 1:1	Outb	oound NPt							
Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□ ✓ ▶	► WAN	TCP	*	*	WAN address	80 - 443	193.253.40.195	80 - 443	Redirection de port pour page web	e 🖉 🖉

3.5 - Communication vers internet de chacun des sous réseaux :

Port Fo	rward	1:1	Outbound	NPt							
Outbo	und NAT	Mode									
	N	Node	0		۲		0		0		
	Automatic outbound NAT rule generation. (IPsec passthrough included)		Hybrid Outb rule generat (Automatic NAT + rules	Hybrid Outbound NAT F rule generation. r (Automatic Outbound ( NAT + rules below) (		Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)		nd NAT NAT rules)			
			Save								
Mappi	ngs										
	Interface	Sourc	e	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
□ ✓	WAN	193.2	253.40.0/24	*	*	*	WAN address	*	~	Accès internet Partout	Ø 🗆 💼

Pour des raisons de facilités, prendre la globalité du réseau est plus simple que faire chacun des sous réseaux à l'unité, à adapter suivant les besoins.

## 4 - Mise en place du VPN

#### 4.1 - Création des certificats :

Se rendre sur la page liée aux certificats :

	System -	Interf
_	Advanced	
Status / D	Certificates	

Dans l'onglet 'Autorité', créer le certificat auto-signé de l'autorité de certification :

Authorities	Certificates	Revocation						
Search								•
Search term				Both	~	Q Search	Clear	
		Enter a search string or *	nix regular expression to see	urch certificate names and distinguish	ed names.			
Certificate /	Authorities							
Name	Internal	Issuer	Certificates	Distinguished Name		In Use	Actions	
								+ Add

Entrer les informations dont on a besoin pour créer le certificat :

Create / Edit CA	
Descriptive name	CA-VPN
	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 cha
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
Randomize Serial	<ul> <li>Use random serial numbers when signing certificates</li> </ul>
	When enabled, if this CA is capable of signing certificates then serial numbe checked for uniqueness instead of using the sequential value from Next Cer

Internal Certificate A	uthority
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 con
Digest Algorithm	sha256
	The digest method used when the CA is signed. The best practice is to use SHA256 or higher. Some services and platforms algorithms invalid.
Lifetime (days)	3650
Common Name	vpn.dmh.btp
	The following certificate authority subject components are optional and ma
Country Code	FR 🗸
State or Province	Nouvelle Aquitaine
City	Barbezieux
Organization	BTSSIO
Organizational Unit	e.g. My Department Name (optional)

Ensuite on appuie sur "Sauvegarder", notre certificat est donc créé.

## Création du certificat du serveur VPN :

Authorities Certificates	Certificate	Revocation					
Search							•
Search term	1			Both	۷	Q Search	D Clear
	Enter a search	string or *nix regular expression to search certificate nar	mes a	and distinguished	names.		_
Certificates							
Name	Issuer	Distinguished Name				In Use	Actions
GUI default (6761544e569fb)	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfS	lense	-6761544e569fb	0		
Server Certificate CA: No Server: Yes		Valid From: Tae, 17 Dec 2024 10:37:02 +0000 Valid Untit: Mon, 19 Jan 2026 10:37:02 +0000					
							+ Add/Sig

## On appuie sur add pour créer le certificat du serveur :

Method       Create an internal Certificate         Descriptive name       Cert-ServVPN         The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the         Internal Certificate         Certificate authority       CA-VPN         Key type       RSA         2048       ~         Z048       ~         Inte length to use when generating a new RSA key, in bits. The key Length should not be lower than 2048 or some platforms may consi         Digest Algorithm       sha256         The digest method used when the certificate is signed. The digest method used when the certificate is signed. The digest practice is to use SHA256 or higher. Some services and platforms, a algorithms invalid.         Lifetime (days)       3650         The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platform         Common Name       von.dmh.btp.         The following certificate subject components are optional and may be left bits         Country Code       FR         State or Province       Nouvelle Aquitaine         Dispectation       Barbezieux         Organization       BTSSIO	
Descriptive name       Cert-ServVPN         The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the         nternal Certificate         Certificate authority         CA-VPN         Key type         RSA         2048         Calda         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 consil         Digest Algorithm         sha256         The digest method used when the certificate is signed. The length of time the signed certificate is signed.         Lifetime (daya)         5650         The following certificate subject components are optional and may be left bl         Country Code       FR         Key Depundent, btp.         State or Province       Nouvelle Aquitaine         City       Barbezieux         Organization       BTSSIO	~
Internal Certificate         Certificate authority         CA-VPN         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 consi         Digest Algorithm         sha256         The digest method used when the certificate is signed. The beat practice is to use SHA256 or higher. Some services and platforms, algorithms invalid.         Lifetime (days)       3650         The following certificate subject components are optional and may be left bl         Country Code       FR         Van drnh btp.       The following certificate subject components are optional and may be left bl         City       Barbezieux         Organization       BTSSIO	
Certificate authority       CA-VPN         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 consi          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, is algorithms invalid.          Lifetime (days)       3650         The length of time the signed certificate will be valid, in days.       Server certificates should not have a lifetime over 398 days or some platform         Common Name           Vpn.dmh.btp.           The following certificate subject components are optional and may be left bl          Country Code       FR          State or Province       Nouvelle Aquitaine          City       Barbezieux           Organization       BTSSIO	ie following ch
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 consi         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, : algorithms invalid.         Lifetime (days)       3650 The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platform         Common Name       vpn.dmh.btp.         The following certificate subject components are optional and may be left bl         Country Code       FR         Kite or Province       Nouvelle Aquitaine         City       Barbezieux         Organization       BTSSIO	
2048       Image: Comparison of the second of	
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, algorithms invalid.         Lifetime (days)       3650         The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platform         Common Name       vpn.dmh.btp         The following certificate subject components are optional and may be left bl         Country Code       FR         State or Province       Nouvelle Aquitaine         City       Barbezieux         Brtstl0	
Lifetime (days)       3650         The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platform         Common Name       vpn.dmh.btp         The following certificate subject components are optional and may be left bl         Country Code       FR         State or Province       Nouvelle Aquitaine         City       Barbezieux         Organization       BTSSI0	
Common Name     vpn.dmh.btp       The following certificate subject components are optional and may be left bl       Country Code     FR       State or Province     Nouvelle Aquitaine       City     Barbezieux       Organization     BTSSIO	
The following certificate subject components are optional and may be left bl         Country Code       FR         State or Province       Nouvelle Aquitaine         City       Barbezieux         Organization       BTSSIO	
Country Code     FR       State or Province     Nouvelle Aquitaine       City     Barbezieux       Organization     BTSSIO	
State or Province     Nouvelle Aquitaine       City     Barbezieux       Organization     BTSSIO	
City Barbezieux Organization BTSSIO	
Organization BTSSIO	
Organizational Unit e.g. My Department Name (optional)	

Certificate Attributes			
Attribute Notes	The following attributes are added to certificates and requests when they are created or sign selected mode.		
	For Internal Certificates, these attributes are added directly to the certificate as shown.		
Certificate Type	Server Certificate		
Alternative Names	FQDN or Hostname     V		
	Type Value		
	Enter additional identifiers for the certificate in this list. The Common Name field is automat signing CA may ignore or change these values.		
Add SAN Row	+ Add SAN Row		
	B Save		

Et on sauvegarde le certificat du serveur.

### 4.2 - Configuration du serveur VPN :

	System +	Interfaces 🗸	Firewall 🗸	Services +	VPN +	Status +
System / Certificates / Certificates						-
					OpenVPN	

Pour une configuration plus simple et rapide on utilise l'onglet "Wizards" :

VPN/ Op	enVPN / Servers				🔟 🗏 😧
Servers	Clients Client Specific Overrid	es Wizards			
OpenVPN S	ervers				
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
					+ Add

et ensuite on suit les étapes de la configuration :

J'ai au préalable configuré un serveur d'Authentification pour pouvoir utiliser les utilisateurs de mon AD lors de la connexion au VPN via le protocole LDAP.

0	pen\	VPN	Rem	ote /	Acces	s S	erver	Set	un
-					10003				

This wizard will provide guidance through an OpenVPN Remote Access Se

The wizard may be stopped at any time by clicking the logo image at the te

Select an Authentie	cation Backend Type
Type of Server	r LDAP 💙
	NOTE: If unsure leave this set to "Local User Access"
On choisit le certifi	icat de son autorité :
Certificate Authori	ty Selection
	OpenVPN Remote Access Server Setup Wizard
Choose a Certificat	te Authority (CA)
Certificate Authority	CA-VPN 🗸
On choisit le certifi	cat de son serveur VPN :
Server Certificate	Selection
	OpenVPN Remote Access Server Setup Wizard
Choose a Server C	ertificate
Certificate	e Cert-ServVPN 🗸
On configure le serv	veur : (à adapter suivant les besoins)
Server Setup	
	OpenVPN Remote Access Server Setup Wizard
General OpenVPN Ser	ver Information
Description	ServVPN
	A name for this OpenVPN instance, for administrative reference. It can be set howeve service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to id
Endpoint Configuration	on
Protocol	UDP on IPv4 only
	Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Interface	WAN 🗸
	The interface where OpenVPN will listen for incoming connections (typically WAN.)
Local Port	1194
	Local port upon which OpenVPN will listen for connections. The default port is 1194. used.

Cryptographic Setting	gs		
TLS Authentication	Enable authentication of TLS packets.	Tunnel Settings	
Generate TLS Key	Automatically generate a shared TLS authentication key.	IPv4 Tunnel Network	10.10.10.0/24 Adresse réseau du tunnel
TLS Shared Key			This is the virtual network used for private communications between this serv first network address will be assigned to the server virtual interface. The remain
		Redirect IPv4 Gateway	□ Force all client generated traffic through the tunnel.
	6	IPv4 Local Network	192.168.50.0/24 Réseau dont on veut avoir accès
	Paste in a shared TLS key if one has already been generated.		This is the network that will be accessible from the remote endpoint, expresse local network through this tunnel on the remote machine. This is generally set
DH Parameters Length	2048 bit 🗸	Concurrent Connections	10 Nombre connexions max en simultanées
	Length of Diffie-Hellman (DH) key exchange parameters, used for establishing		Specify the maximum number of clients allowed to concurrently connect to th
	from key sizes, but as with other such settings, the larger the key, the more set As of 2016, 2048 bit is a common and typical selection.	Allow Compression	Refuse any non-stub compression (Most secure)
Data Encryption	AES-256-GCM		Allow compression to be used with this VPN instance, which is potentially instance,
Algorithms	AES-128-GCM CHACHA20-POLY1305	Compression	Disable Compression [Omit Preference]
	List of algorithms clients can negotiate to encrypt traffic between endpoints. 1 Certain algorithms will perform better on different hardware, depending on the finishing the wizard for additional choices.		Compress tunnel packets using the chosen option. Can save bandwidth, but is compression is not allowed. Adaptive compression will dynamically disable of packets is not being compressed efficiently.
Fallback Data Encryption	AES-256-CBC (256 bit key, 128 bit block)	Type-of-Service	$\hfill\square$ Set the TOS IP header value of tunnel packets to match the encapsulated $\mu$
Algorithm	The algorithm used to encrypt traffic between endpoints when data encryptior	Inter-Client Communication	Allow communication between clients connected to this server.
Auth Digest Algorithm	SHA256 (256-bit)	Duplicate Connections	Allow multiple concurrent connections from clients using the same Comm
	The second s		NOTE This is not generally recommended, but may be needed for some scen-
	i ne metrioù usea to autrienticate tramic between endpoints. This setting must desired.	Duplicate Connection	10 connecter au von et combien de fois max
		Limit	Limit the number of concurrent connections from the same user
Hardware Crypto	No Hardware Crypto Acceleration		state and number of concurrent connections from the same user.

The hardware cryptographic accelerator to use for this VPN connection, if any.

Advanced Client Setti	ings		
DNS Default Domain	192.168.50.182		
	Provide a default domain name to clients.		
DNS Server 1			
	DNS server IP to provide to connecting clients.		
DNS Server 2			
	DNS server IP to provide to connecting clients.		
DNS Server 3			
	DNS server IP to provide to connecting clients.		
DNS Server 4			
	DNS server IP to provide to connecting clients.		
NTP Server		Settings	
	Network Time Protocol server to provide to connecting clients.	Dynamic IP	Allow connected clients to retain their connections if their IP address changes.
NTP Server 2			
	Network Time Protocol server to provide to connecting clients.	Topology	Subnet – One IP address per client in a common subnet 🔹 🗸
NetBIOS Options	Enable NetBIOS over TCP/IP.		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 "subpet" even for IPv6, such as OpenVPN Connect (iOS/Android)
	If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will		Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".
NetBIOS Node Type	none		
	Possible options: b-node (broadcasts), p-node (point-to-point name queries to (query name server, then broadcast).		
NotPIOS Soons ID			
Netbios Scope ID	A NetBIOS Scope ID provides an extended naming service for NetBIOS over T	(	
	to only those nodes with the same NetBIOS scope ID.		
WINS Server 1	192.168.50.182		
	A Windows Internet Name Service (WINS) server IP to provide to connecting of		
WINS Server 2			
	A Mindows Internet Name Cervice (MINIC) server ID to provide to connecting a		

Et enfin pour finir la configuration, on ajoute si on le souhaite, les règles (créées automatiquement) :

 Firewall Rule Configuration

 OpenVPN Remote Access Server Firewall Rules

 Rules control passing or blocking network traffic

 Rules must be added which allow traffic to reach

 OpenVPN tunnel.

 The options on this step can add automatic rules

 Traffic from clients to server

 Firewall Rule
 Add a rule to permit connections to this Oper

 Traffic from clients through VPN

 OpenVPN rule
 Add a rule to allow all traffic from connected

On clique sur "Next", et notre configuration est enfin terminée!

Finished!	
	OpenVPN Remote Access Server Setup Wizard
Configuration Comple	ete!
	The configuration is now complete.
	Adding users for the VPN depends on the chose For remote authentication servers, add certificat
	To easily export client configurations, browse to
	➢ Finish

### 4.3 - Exportation de la configuration du VPN :

Pour exporter la configuration du VPN, on doit installer un paquet nommé "openvpn-client-export"



Pour l'installer on se rend sur la page faites pour :

Et on installe le paquet.

Après l'installation on retourne sur la page précédente du service VPN et on va sur l'onglet "Client Export" :

OpenVPN / Client Export Utility					
Server	Client	Client Specific Overrides	Wizards	Client Export	
OpenVP	N Server				
Remote	Access Serv	ServVPN UDP4:1194			~

On descend tout en bas, et on récupère la configuration pour un client, et si on veut, même récupérer l'installateur de l'application pour le client :



#### 4.4 - Tests du VPN :

Sur mon hôte, après installation du client OpenVPN, il faut mettre les fichiers téléchargés juste avant, pour ainsi mettre la configuration :

<mark> </mark> → C	e PC > Disque local (C:)	> Programmes > Op	enVPN → config			
	Nom	^	Modifié le	Туре	Taille	
le	🏂 pfSense-UDP4-11	94-uservpn	07/01/2025 10:19	Échange d'inform		5 Ko
R	o pfSense-UDP4-11	94-uservpn-config	07/01/2025 10:19	OpenVPN Config		1 Ko
ements 🖈	pfSense-UDP4-11	94-uservpn-tls	07/01/2025 10:19	Apple Keynote		1 Ko
ts ≉	README		08/11/2023 22:07	Document texte		1 Ko
On ess	aie ensuite la conr	nexion au VPN : Sense-UDP4-1194-use	rvpn-config)	- 🗆	$\times$	
Etat	actuel: En cours de conne	exion				
Fri J	an 10 13:45:48 2025 libra an 10 13:45:48 2025 libra an 10 13:45:48 2025 DCC Util Mo	oversions: OpenSSL 3. D version: 1.0.0 pfSense-UDP4-1194- isateur: Idap t de passe: Enregistrer mot de passe OK	auservpn-config ×		>	
,						
			0	 penVPN GUI 11.45.0.0/2	.6.7	
	Déconnecter	Reprendre		Fermer		

On utilisateur un des utilisateurs adapté pour la connexion :

🖳 Connexion OpenVPN (pfSense-UDP4-1194-uservpn-config)	-		×
Etat actuel: En cours de connexion			
Fri Jan 10 13:46:34 2025 OpenVPN 2.6.7 [git:v2.6.7/53c9033317b3b8fd] Windows [S3 Fri Jan 10 13:46:34 2025 Windows version 10.0 (Windows 10 or greater), amd64 execut Fri Jan 10 13:46:34 2025 library versions: OpenSSL 3.1.4 24 Oct 2023, LZO 2.10 Fri Jan 10 13:46:34 2025 DCO version: 1.0.0 Fri Jan 10 13:46:36 2025 TCP/UDP: Preserving recently used remote address: [AF_INE Fri Jan 10 13:46:36 2025 UDPv4 link local: (not bound) Fri Jan 10 13:46:36 2025 UDPv4 link remote: [AF_INET]172.22.215.31:1194 Fri Jan 10 13:46:36 2025 [vpn.dmh.btp] Peer Connection Initiated with [AF_INET]172.2 Fri Jan 10 13:46:37 2025 open_tun Fri Jan 10 13:46:37 2025 open_tun Fri Jan 10 13:46:37 2025 Set TAP-Windows TUN subnet mode network/local/netmask Fri Jan 10 13:46:37 2025 Notified TAP-Windows driver to set a DHCP IP/netmask of 10 Fri Jan 10 13:46:37 2025 Successful ARP Flush on interface [6] {48EF9E36-B196-49B0 Fri Jan 10 13:46:37 2025 IPv4 MTU set to 1500 on interface 6 using service	SL (OpenS itable ET]172.22 2.215.31: 3 = 10.10. 0.10.10.2/ 6-B308-3E	SSL)] [LZO .215.31:1 1194 10.0/10.1( 255.255.2 7BC33484	)] [L2 194 0.10. 255.0 4F1} ≫
,			
OpenVP	N GUI 11.	45.0.0/2.6	6.7
Déconnecter Reprendre		Fermer	
OpenVPN GUI for Windows			
est désormais connecté. Adresse IP assignée: 10.10.10.4			
On est bien implanté dans le sous-réseau créé exprès.			
OpenVPN GUI Connecté à: pfSense-UDP4-1194-uservpn-config Connecté depuis: 10/01/2025 13:47 Adresse IP assignée: 10.10.10.4			

Nous sommes bien connectés.