# Installation de RADIUS

# Etape 1 : NPS

#### Installation du service NPS :

### Sélectionner des rôles de serveurs



Création d'un groupe de sécurité pfsense-adm :

<b>@</b>	
om du groupe :	
fsense-adm	
om de groupe (antérieur à Wi	ndows 2000) :
ifsense-adm	
Étendue du groupe	Type de groupe
O Domaine local	Sécurité
🖲 Globale	ODistribution
🔾 Universelle	

Ajout du compte Administrateur au groupe :



Propriétés de : pfsense-adm

? X

Nom Administrateur	Dossier Services de d leam.local/Users	omaine Active Dire	ctory	
-1010				

Faire clic droit sur NPS (Local) puis Inscrire un serveur dans Active Directory pour ajouter le serveur NPS à l'AD :

NPS (Locan		NOC /I
V 🛄 Client	Importer la configuration	
E CI	Exporter la configuration	
GI Straté	Démarrer le service NPS	
Struct	Arrêter le service NPS	
📑 St	Inscrire un serveur dans Active Director	у
➡ Gestic	Propriétés	
Se Se	Affichage	>
E Se	Aide	
	10	11

Faire clic droit sur Clients RADIUS puis Nouveau : Ajout de FW1 en tant que client RADIUS :

arametres	Avancé				
Activer	e client RAD				
	Se client NAD	105			
Sélectio	onner un mode	èle existant :			
					~
Nom et ac	dresse				
Nom conv	vivial :				
FW1					
Adresse (	P ou DNS) :				
10118					Várifier
Secret pa	rtagé				
011		1 같이 있었다. 11			
Selection	nez un modèl	e de secrets par	tagés existant :		
Aucun	nez un modèl	e de secrets par	agés existant :		~
Aucun Pour tape automatiq client RAI respecten	r manuelleme uement un se DIUS avec le ti la casse.	e de secrets par nt un secret par cret partagé, cli même secret pa	agés existant : agé, cliquez sur quez sur Génére rtagé entré ici. L	Manuel. Pour r. Vous devez es secrets par	générer configurer le tagés
Aucun Pour tape automatig client RAI respecten	r manuelleme uement un se DIUS avec le ti la casse. el	e de secrets par nt un secret par cret partagé, cli même secret pa O Générer	agés existant : agé, cliquez sur quez sur Génére rtagé entré ici. L	Manuel. Pour r. Vous devez es secrets par	générer configurer le tagés
Aucun Pour tape automatiq client RAI respecter	r manuelleme uement un se DIUS avec le it la casse. el	e de secrets par nt un secret part cret partagé, cli même secret pa O Générer	agés existant : agé, cliquez sur quez sur Génére rtagé entré ici. L	Manuel. Pour r. Vous devez es secrets par	générer configurer le tagés
Aucun Pour tape automatiq client RAI respecter (a) Manue Secret pa	nez un modèle r manuelleme juement un se DIUS avec le it la casse. el irtagé :	e de secrets par nt un secret part cret partagé, cli même secret pa O Générer	tagés existant : agé, cliquez sur quez sur Génére rtagé entré ici. L	Manuel. Pour r. Vous devez es secrets par	générer configurer le tagés
Aucun Aucun Pour tape automatig client RAI respecter © Manue Secret pa Confirmez	rez un modèle re manuelleme uement un se DIUS avec le it la casse. el irtagé : • • • •	e de secrets par cret partagé, cli même secret pa O Générer ragé :	tagés existant : agé, cliquez sur quez sur Génére rtagé entré ici. L	Manuel. Pour r. Vous devez es secrets par	générer configurer le tagés
Aucun Pour tape automatig client RAI respecter Manue Secret pa Confirmez	rr manuelleme uement un se DIUS avec le tt la casse. el rtagé : el se secret part	e de secrets par nt un secret part cret partagé, cli même secret pa Générer agé :	agé, cliquez sur agé, cliquez sur quez sur Génére rtagé entré ici. L	Manuel. Pour r. Vous devez es secrets par	générer configurer le tagés

Faire clic droit sur Stratégies réseau puis Nouveau :



Donner un nom à la stratégie réseau puis faire Suivant :

Nouvelle stratégie réseau

	Spécifier le nom de la stratégie réseau et le type de connexion
A	Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.
Nom de la :	stratégie :
pfsense-adm	
Méthode de c	xonnexion réseau
Sélectionnez valeur dans 1 serveur d'acc	le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une ype de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre sès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

#### Cliquer sur Ajouter :

onditions :				
Condition	Valeur			
Description de la conditio	on :			
		Ajo <u>u</u> ter	Modifi <u>e</u> r	Supprimer
électionner Grou	pe d'utilisateurs :			

×

Group	es	1
1	Groupes Windows La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.	
	Groupes d'ordinateurs La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.	
<b>.</b>	Groupes d'utilisateurs La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.	
Restri	ctions relatives aux jours et aux heures	
P	Restrictions relatives aux jours et aux heures Les restrictions relatives aux jours et aux heures indiquent les jours et les heures auxquels les tentatives de connexion sont autorisées ou non. Ces restrictions sont basées sur le fuseau horaire du serveur NPS (Network Policy Server)	

#### Ajouter le groupe pfsense-adm :

Con	ditions :	
	Condition	Valeur
2	Groupes d'utilisateurs	LEARN\pfsense-adm

Faire Suivant jusqu'à pouvoir cocher PAP, cocher la case et faire Suivant :

Authentification non chiffrée (PAP, SPAP)

Faire Suivant puis sur ce menu cliquer sur Ajouter :



Configurer les paramètres

Le serveur NPS applique des paramètres à la demande de connexion si toutes les conditions relatives à la stratégie de demande de connexion sont remplies.

Configurez les paramètres de cette stratégie réseau. Si la demande de connexion répond aux conditions et contraintes, et si la stratégie accorde l'accès, les paramètres sont appliqués.

Attributs RADIUS	Pour envoyer des att	ributs supplémentaires aux clients RADIUS, sélectionnez un attribut
🚯 Standard	RADIUS standard, p	uis cliquez sur Modifier. Si vous ne configurez pas d'attribut, celui-ci
Spécifiques au fournisseur Routage et accès à	RADIUS pour conna	x clients HADIUS. Consultez la documentation de votre client fitre les attributs nécessaires.
distance	Attributs :	
Jaisons multiples et	Nom	Valeur
(Bandwidth Allocation	Framed-Protocol	PPP
Protocol)	Service-Type	Framed
👕 Filtres IP		
Chiffrement		
💑 Paramètres IP		
	Ajouter	Modifier_ Supprimer

Sélectionner Class :

Pour ajouter un attribut personnalisé ou prédéfini spér sélectionnez Spécifique au fournisseur, puis cliquez s	écifique au fournisseur, fermez cette boîte de dialogue et sur Ajouter.
Tous	~
Attributs :	
Nom Acct-Interim-Interval Callback-Number Class	
Filter-Id Framed-Apple Talk-Link Framed-Apple Talk-Network	
	>
Spécifie la classification des enregistrements de com	nptabilité.
	Ajouter Fermer
Écrire pfsense-adm puis faire OK	۲, Suivant et Terminé :
Informations d'attribut	×
Nom de l'attribut : Class	

Numéro de l'attribut : 25

Format de l'attribut : OctetString

Chaîne
 Hexadécimal

Entrez la valeur d'attribut dans :

Sur l'interface web de pfSense, aller dans la section System puis dans le menu User Manager :

Annuler

OK

System 👻	Interf
Advanced	
Certificates	
General Setu	p
High Availab	ility
Package Ma	nager
Register	
Routing	
Setup Wizard	ł
Update	
User Manage	er

#### Dans Authentification Servers, cliquer sur Add :

Users Groups	Settings	Authentication Servers			
Authentication Se	ervers				
Server Name		Туре	Host Name	Actions	
Local Database			FW1		
					+ Ad

#### Entrer les informations suivantes puis faire Save :

Server Settings	
Descriptive name	DC1
Туре	RADIUS
RADIUS Server Settin	gs
Protocol	PAP ~
Hostname or IP address	10.1.1.1
Shared Secret	
Services offered	Authentication and Accounting
Authentication port	1812
Accounting port	1813
Authentication Timeout	
	This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.
RADIUS NAS IP Attribute	WAN - 10.10.0.255 🔹
	Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.
	P Save

Pour tester le bon fonctionnement de notre manipulation, se rendre dans la section Diagnostics puis dans le menu Authentification :



Sélectionner le bon serveur et inscrire les informations de connexion de l'utilisateur ajouté précédemment dans le groupe pfsense-adm :

uthentication Server	DC1 V
	Select the authentication server to test against.
Username	Administrateur
Password	[
Debug	□ Set debug flag
	Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

Un message positif devrait apparaître :

User Administrateur authenticated successfully. This user is a member of groups:

## **Etape 2 : VPN SSL**

Sur FW1, Se rendre dans la section System puis dans le menu Certificates :



System /	Certificate /	Authorities					6
Authorities	Certificates	Revocation					
Search							e
Search term				Both	~	Q Search 5	Clear
Certificate	Ente Authorities	er a search string or *i	nix regular expression to sea	irch certificate names and distinguished	names.		
Name	Internal	Issuer	Certificates	Distinguished Name		In Use	Actions
							+ /

#### Renseigner les informations principales puis faire Save :

eate / Edit CA				
Descriptive name	CA-VPN	I-SSL		
	The nam This nam	e of this entry as displayed in the GUI for	r reference. ain any of the following characters: $2 > < 8 / $	
		le can contain spaces but it cannot conta	an any of the following characters: () <) <) d <sub>1</sub> / () ()	
Method	Create	an internal Certificate Authority	~	
Trust Store	🗌 Add t	his Certificate Authority to the Operating \$	System Trust Store	
	When en	abled, the contents of the CA will be adde	led to the trust store so that they will be trusted by the operating system.	
Randomize Serial	🗌 Use r	andom serial numbers when signing certi	tificates	
	When en checked	abled, if this CA is capable of signing cert for uniqueness instead of using the segu	rtificates then serial numbers for certificates signed by this CA will be automatically randor uential value from Next Certificate Serial.	mized a
		3		_
ernal Certificate A	Authority			
Key type	RSA		~	
	2048		~	
	The leng	th to use when generating a new RSA key,	y, in bits.	
	The Key	Length should not be lower than 2048 or s	some platforms may consider the certificate invalid.	
Digest Algorithm	sha256	to set that i is an each something on	~	
	The dige The best	st method used when the CA is signed. practice is to use SHA256 or higher. Som	me services and platforms, such as the GUI web server and OpenVPN, consider weaker dig	est
	algorithn	ns invalid.		
Lifetime (days)	3650			
Common Name	[			
	vpirca			
		The following certificate au	uthority subject components are optional and may be left blank.	
Country	Code	FP		
State or Pro	vince	Lorraine		
		Londine		
	City	Metz		
	City	Metz		
Organiz	City	Metz		
Organiz	City zation	Metz		
Organiz	City zation	Metz Mewo	e (ontional)	

L'autorité de certification a été créée :

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-VPN-SSL	~	self-signed	0	ST=Lorraine, O=Mewo, L=Metz, CN=vpn-ca, C=FR 🚺		<i>∅</i> <b>* *</b> C in
				Valid From: Tue, 18 Jun 2024 17:41:36 +0000		
				Valid Until: Fri, 16 Jun 2034 17:41:36 +0000		

#### Cliquer sur l'onglet Certificates puis faire Add/Sign :

System/ Certificate	es / Cert	ificates		
Authorities Certificates	Certifica	te Revocation		
Search				
			-	
Search term		Both	✓ Q Search	Clear
Search term	Enter a searc	h string or *nix regular expression to search certificate names and distinguished nam	es.	Clear
Search term Certificates Name	Enter a searc	b string or *nix regular expression to search certificate names and distinguished nam Distinguished Name	es.	Actions
Search term Certificates Name GUI default (667199d01d587)	Enter a searc Issuer self-signed	Both h string or *nix regular expression to search certificate names and distinguished nam Distinguished Name O=pfSense GUI default Self-Signed Certificate, CN=pfSense-667199d01d587	C Search	Actions
Search term Certificates Name GUI default (667199d01d587) Server Certificate CA Na	Enter a searc Issuer self-signed	Both h string or *nix regular expression to search certificate names and distinguished nam Distinguished Name O=pfSense GUI default Self-Signed Certificate, CN=pfSense-667199d01d587 Valid From: Tue, 18 Jun 2024 14:29:36 +0000	In Use	Actions

#### Remplir les informations comme ci-dessous puis faire Save :

ld/Sign a New Cert	rtificate	
Method	Create an internal Certificate	
Descriptive name	VPN-SSL-REMOTE-ACCESS	
	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: ?, >, <, &, /,  ", "	
ernal Certificate		
Certificate authority	CA-VPN-SSL 🗸	
Key type	RSA	
	2048 🗸	
	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.	
Digest Algorithm	sha256 🗸	
	The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, con algorithms invalid.	sider weaker digest
Lifetime (days)		
	The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.	
Common Name	VPN-SSL	
	The following certificate subject components are optional and may be left blank.	
Country Code	FR	
State or Province	Lorraine	
City	Metz	
Organization	Mewo	
Organizational Unit	e.g. My Department Name (optional)	
rtificate Attributes	15	
Attribute Notes	The following attributes are added to certificates and requests when they are created or signed. These attributes behave differences selected mode.	rently depending on t
	For Internal Certificates, these attributes are added directly to the certificate as shown.	
Certificate Type	Server Certificate	
	Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the	signed certificate.
Alternative Names	FQDN or Hostname	
	Type value Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as a signing CA may ignore or change these values.	an Alternative Name. 1
Add SAN Row	+ Add SAN Row	

Le certificat à bien été créé :

Search				
Search term		Both	Y Q Search	Clear
	Enter a search	string or *nix regular expression to search certificate names and distinguished name	es.	
Certificates				
Name	lssuer	Distinguished Name	In Use	Actions
GUI default (667199d01d587) Server Certificate CA: <b>No</b> Server: <b>Yes</b>	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-667199d01d587 Valid From: Tue, 18 Jun 2024 14:29:36 +0000 Valid Until: Mon, 21 Jul 2025 14:29:36 +0000	webConfigurator	<b>/*₽</b> ■C
/PN-SSL-REMOTE-ACCESS Server Certificate CA: No	CA-VPN-SSL	ST=Lorraine, O=Mewo, L=Metz, CN=VPN-SSL, C=FR Valid From: Tue, 18 Jun 2024 17:48:07 +0000 Valid Until: Fri, 16 Jun 2034 17:48:07 +0000		<b>∥*₽</b> ∎C®

#### Dans la section VPN, aller dans le menu OpenVPN :

	VPN -	Status 🗸
	IPsec	
pa	L2TP	9
	OpenVPN	L I

#### Cliquer sur Add :

Servers Clients Client Specific Overrides Wizards	
OpenVPN Servers	Actions

Indiquer les informations suivantes et faire Save :

General Information		
Description		
	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.	
Mode Configuration	n in the second s	
Server mode	Remote Access ( SSL/TLS + User Auth )	
Backend for	DC1	
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 Configurat	tion	
Protocol	UDP on IPv4 only	
Interface	WAN	
Interface	The interface or Virtual IP address where OpenVPN will receive client connections.	
1		
Local port	1194 The part used by OpenVPN to receive client connections.	
Local port ryptographic Setting TLS Configuration	1194         The port used by OpenVPN to receive client connections.         Igs         Igs         Iss 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 this laws of MACC authorities in allows control observed products without the proper key to be drapped protecting the apper from a third laws of MACC authorities to allow a control observed products without the proper key to be drapped protecting the apper from a third laws of MACC authorities to a second products without the proper key to be drapped protecting the apper from a third laws of the proper key to be drapped protecting the apper from a the proper key to be drapped protecting the apper from a the proper key to be drapped protecting the apper from a the proper key to be drapped protecting the apper from a the proper key to be drapped protecting the apper from a the proper key to be drapped protecting the apper from a the proper key to be drapped protecting the apper from a the proper key to be drapped protecting the apper from a the proper key to be drapped protecting the apper from a the proper key to be drapped protecting the appen from a the proper key to be drapped protecting the appen from a the proper key to be drapped protecting the appen for the proper key to be drapped protecting the protecting the protecting the protecting the protecting the protecting the	a TLS handshake.
Local port	1194         The port used by OpenVPN to receive client connections.         Igs         Igs         In TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from at unauthorized connections. The TLS Key does not have any effect on tunnel data.	a TLS handshake. ttack or
Local port	1194         The port used by OpenVPN to receive client connections.         gs         Image: 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 at unauthorized connections. The TLS Key does not have any effect on tunnel data.         Image: Automatically generate a TLS Key.	a TLS handshake. ttack or
Local port	1194         The port used by OpenVPN to receive client connections.         Igs         I 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 This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from at unauthorized connections. The TLS Key does not have any effect on tunnel data.         Image: Automatically generate a TLS Key.         Image: CA-VPN-SSL	a TLS handshake. ttack or
Local port	1194         The port used by OpenVPN to receive client connections.         gs         Image: 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 at unauthorized connections. The TLS Key does not have any effect on tunnel data.         Image: Automatically generate a TLS Key.         CA-VPN-SSL         No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager	a TLS handshake. ttack or
Local port	Ing4         The port used by OpenVPN to receive client connections.         gs         Image: 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 at unauthorized connections. The TLS Key does not have any effect on tunnel data.         Image: Automatically generate a TLS Key.         Image: CA-VPN-SSL         Image: No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager	a TLS handshake. ttack or
Local port	1194         The port used by OpenVPN to receive client connections.         gs         Image: 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 at unauthorized connections. The TLS Key does not have any effect on tunnel data.         Image: Automatically generate a TLS Key.         CA-VPN-SSL         No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager         Image: Check client certificates with OCSP         VPN-SSL-REMOTE-ACCESS (Server; Yes, CA: CA-VPN-SSL)	a TLS handshake. ttack or
Local port TLS Configuration TLS Configuration er Certificate Authority Peer Certificate Revocation list OCSP Check Server certificate	1194         The port used by OpenVPN to receive client connections.         gs         Image: State of the point used by OpenVPN to receive client connection by requiring both parties to have a common key before a peer can perform at unauthorized connections. The TLS Key does not have any effect on tunnel data.         Image: Automatically generate a TLS Key.         Image: CA-VPN-SSL         Image: CA-VPN-SSL         Image: Check client certificates with OCSP         Image: VPN-SSL-REMOTE-ACCESS (Server: Yes, CA: CA-VPN-SSL)         Image: Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECD	a TLS handshake. ttack or DSA curves or wea
Local port Cryptographic Setting TLS Configuration TLS Configuration Peer Certificate Authority Peer Certificate Revocation list OCSP Check Server certificate	1194         The port used by OpenVPN to receive client connections.         gs         Image: State of the port used by OpenVPN connection by requiring both parties to have a common key before a peer can perform at unauthorized connections. The TLS Key does not have any effect on tunnel data.         Image: Automatically generate a TLS Key.         Image: CA-VPN-SSL         Image: CA-VPN-SSL         Image: Check client certificates with OCSP         Image: VPN-SSL-REMOTE-ACCESS (Server: Yes, CA: CA-VPN-SSL)         Image: Cartificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECCD digest algorithms.	a TLS handshake. ttack or SA curves or wea
Local port Cryptographic Setting TLS Configuration TLS Configuration Peer Certificate Authority Peer Certificate Revocation list OCSP Check Server certificate DH Parameter Length	I194         The port used by OpenVPN to receive client connections.         Igs         Image:	a TLS handshake. ttack or DSA curves or wea
Local port Cryptographic Setting TLS Configuration TLS Configuration eer Certificate Authority Peer Certificate Revocation list OCSP Check Server certificate DH Parameter Length	1194         The port used by OpenVPN to receive client connections.         gs         Image: I	a TLS handshake. ttack or DSA curves or wea
Local port Cryptographic Setting TLS Configuration TLS Configuration eer Certificate Authority Peer Certificate Revocation list OCSP Check Server certificate DH Parameter Length ECDH Curve	1194         The port used by OpenVPN to receive client connections.         gs         I 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 This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from at unauthorized connections. The TLS Key does not have any effect on tunnel data.         I Automatically generate a TLS Key.         CA-VPN-SSL         No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager         O Check client certificates with OCSP         VPN-SSL-REMOTE-ACCESS (Server: Yes, CA: CA-VPN-SSL)         Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECD digest algorithms.         2048 bit          Diffie-Hellman (DH) parameter set used for key exchange.       I         Use Default	a TLS handshake. ttack or DSA curves or wea
Local port Cryptographic Setting TLS Configuration TLS Configuration CPeer Certificate Peer Certificate Peer Certificate COCSP Check Server certificate DH Parameter Length ECDH Curve	1194         The port used by OpenVPN to receive client connections.         gs         I 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 This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from at unauthorized connections. The TLS Key does not have any effect on tunnel data.         I Automatically generate a TLS Key.         CA-VPN-SSL         No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager         O Check client certificates with OCSP         VPN-SSL-REMOTE-ACCESS (Server: Yes, CA: CA-VPN-SSL)         Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECD digest algorithms.         2048 bit       v         Diffie-Hellman (DH) parameter set used for key exchange.       Image: Correct on the set of	a TLS handshake. ttack or
Local port Cryptographic Setting TLS Configuration Beer Certificate Authority Peer Certificate Revocation list OCSP Check Server certificate DH Parameter Length ECDH Curve	1194         The port used by OpenVPN to receive client connections.         gs         Image: Start Skey         A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform at unauthorized connections. The TLS Key does not have any effect on tunnel data.         Image: Automatically generate a TLS Key.         CA-VPN-SSL         CA-VPN-SSL         Image: Open Control Content Contret Control Control Control Conterve Conthet S	a TLS handshake. ttack or DSA curves or wea

Failback Data Eliciyption	AES-256-CBC (256 bit key, 128 bit block)
Algorithm	The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption al 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	🕼 Enforce key usage
Usage Validation	Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").
Tunnel Settings	
IPv4 Tunnel Network	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 rer 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 com 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 addr 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)	10.1.1.0/24
	IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/networ 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 t 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/networ 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 L/ 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 VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to deci- the use case for this specific VPN is vulnerable to attack.
	Asymmetric compression allows an easier transition when connecting with older peers.
Push Compression	Push the selected Compression setting to connecting clients.

Inter-client communication	Allow communication between clients connected to this server					
Duplicate Connection	uplicate 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.					
Client Settings						
Dynamic IP	Allow connected clients to retain their connections if their IP address changes.					
Topology	net30 – Isolated /30 network per client 🗸					
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN ( 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					
DNS Default Domain	Ings					
DNS Default Domain						
DNS Default Domain	learn.local					
DNS Server enable	Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.					
DNS Server 1	10.1.1.1					
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					
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 Configurat	tion					
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     O IPv4 only     O 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     constraint      constraint					
	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					

Se rendre à cet emplacement et installer le package openvpn-client-export :

System / Package Manager / Available Packages				
Installed I	Packages	Available Packages		
Search			Θ	
Search te	Search term Openvpn Both V Q Search D Ck			
		Enter a search string or *nix regular expression to search package names and descriptions.		
Package	es			
Package Name	es Version	Description		
Package Name openvpn- client-	es Version 1.9.2	Description Exports pre-configured OpenVPN Client configurations directly from pfSense software.	+ Install	

Retourner dans le menu OpenVPN puis aller dans Client Export :

OpenVPN / Client Export Utility						0		
Server	Client	Client Specific Overrides	Wizards	Client Export				

Remplir ces informations puis cliquer sur Save as default :

OpenVPN Server							
Remote Access Server	Server UDP4:1194						
Client Connection B	lehavior						
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 as they are not affected.						
Legacy Client	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.						
Cartificata Export O							
Certificate Export C	prons						
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	Hinh: AES-256 + SHA256 (nfSense Software FreeBSD Linux Windo Y						
21	Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program						
Baser Oakland							
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						