Lebeau TP installation VPN SITE/client openvpn sur pfsense BTS SIO2

Mathéo

Intro :

Dans ce tp nous allons utiliser la solution openvpn qui va nous permettre de sécuriser nos échanges en créant un réseau vpn sur notre pare-feu et utiliser des connexions à distance sur un réseau distant vers notre serveur.

Pour commencer nous allons nous rendre sur le pare-feu pfsense et modifier les certificats et en créer un nouveau.



Puis quelques modifications suffisent avec le nom du certificat son nom commun et la langue FR ici

Create / Edit CA	
Descriptive name	CA-JAPON
	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: ?, >, <, &, /, ", '
Common Name	japon
	The following certificate authority subject components are optional and may be left blank.
Country Code	FR v

Enfin dans organisation également et on peut faire save

Organization	japon
Organizational Unit	e.g. My Departme
	Save

Puis dans l'onglet certificates on va aussi ajouter un autre certificat pour OpenVPN

Authorities Certificates Certificate Revocation Search Both Q Search Clear Search term Both Q Search Clear Enter a search string or *nix regular expression to search certificate names and distinguished names. In Use Actions Name Issuer Distinguished Name In Use Actions webConfigurator default (674436e0d93f7) Server Certificate, CN=pfSense- Server Certificate WebConfigurator Image Configurator Image Configurator Valid From: Mon, 25 Nov 2024 07:35:44-0100 Server: Yes Valid From: Mon, 25 Nov 2024 07:35:44-0100 Valid Until: Sun, 28 Dec 2025 07:35:44-0100 Valid Until: Sun, 28 Dec 2025 07:35:44-0100	System / Certificate	es / Certifica	ates		6
Search Both Q Search I Clear Both Q Search I Clear Enter a search string or *nix regular expression to search certificate names and distinguished names. In Use Certificates In Use Actions webConfigurator default (674436e0d93f7) self- signed 0=pfSense webConfigurator Self-Signed Certificate, CN=pfSense- valid Until: Sun, 28 Dec 2025 07:35:44 -0100 Valid Until: Sun, 28 Dec 2025 07:35:44 -0100 webConfigurator	Authorities Certificates	Certificate Rev	recation		
Search term Both Q Search Clear Enter a search string or *nix regular expression to search certificate names and distinguished names. In Use Actions Certificates In Use Actions webConfigurator default (674436e0d93f7) 0=pfSense webConfigurator Self-Signed Certificate, CN=pfSense- 674436e0d93f7 webConfigurator Im Use Actions Server Certificate CA: No Server: Yes Valid From: Mon, 25 Nov 2024 07:35:44-0100 Valid Until: Sun, 28 Dec 2025 07:35:44-0100 Valid From: Mon, 25 Nov 2024 07:35:44-0100 Valid From: Mon, 28 Dec 2025 07:35:44-0100	Search				e
Name Issuer Distinguished Name In Use Actions webConfigurator default (674436e0d9377) self- signed 0=pfSense webConfigurator Self-Signed Certificate, CN=pfSense- 674436e0d93f7 webConfigurator ************************************	Search term Certificates	Enter a search strir	Both	Q Search ames.	
webConfigurator default self- O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense- webConfigurator & (674436e0d93f7) signed 674436e0d93f7 i Server Certificate Valid From: Mon, 25 Nov 2024 07:35:44 -0100 Valid From: Sun, 28 Dec 2025 07:35:44 -0100 Server: Yes Valid Until: Sun, 28 Dec 2025 07:35:44 -0100 Valid Until: Sun, 28 Dec 2025 07:35:44 -0100	Name	lssuer	Distinguished Name	In Use	Actions
	webConfigurator default (674436e0d93f7) <i>Server Certificate</i> CA: No Server: Yes	self- signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense- 674436e0d93f7 () Valid From: Mon, 25 Nov 2024 07:35:44 -0100 Valid Until: Sun, 28 Dec 2025 07:35:44 -0100	webConfigurator	∅₩₽ ∎Ċ

Le paramétrage de nom est quasi identique.

Add/Sign a New Cert	ificate
Method	Create an internal Certificate
Descriptive name	Certificat-OpenVPN
	The name of this entry as displayed in the GUI for reference.
	This name can contain spaces but it cannot contain any of the following characters: ?, >, <,
Internal Certificate	
Certificate authority	CA-JAPON 🗸
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 certific
Digest Algorithm	sha256
	The digest method used when the certificate is signed.
	The best practice is to use an algorithm stronger than SHAT. Some platforms may conside
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 platforms may consid
Common Name	japon-firewall
	The following certificate subject components are optional and may be left blank.
Country Code	FR v
State or Province	e.g. Texas
City	e.g. Austin
Organization	Japon
Organizational Unit	e.g. My Department Name (optional)

Puis la partie en dessous est à modifier pour un certificat serveur et on save.

Attribute Notes	The following attributes are adde selected mode.	d to certificates and requests v
	For Internal Certificates, these att	ributes are added directly to th
Certificate Type	User Certificate	
Alternative Names	Server Certificate User Certificate	•
	Туре	Value
	Enter additional identifiers for the signing CA may ignore or change	ecertificate in this list. The Con these values.
Add SAN Row	+ Add SAN Row	
	B Save	

On va maintenant créer un utilisateur pfsense.

	SC System -	Interfaces -	Firewall 👻	Services -	VPN 🗸	Status 👻	Diagnostics 👻	Help 👻		¢ 2	•
Syster	m / User Mana	ager / Users									0
Users	Groups Settin	ngs Authentic	ation Servers								
Users	1										_
	Username	Full n	ame			Status	Grou	ps	Actions		
	 admin 	Syst	em Administrato	or		~	adm	iins	A		
									+ ^	dd 📊	Delete

Pour la première partie on va simplement créer un identifiant mot de passe et cocher la case en dessous créer un certificat utilisateur pour la suite

Defined by	USER
Disabled	This user cannot login
Username	vpn-japon
Password	

Puis on renseignera juste un nom et on peut enregistrer

	Hold down o'r RE (F 0)/ Colviniwardd (wad) key to select multiple items.
Certificate	Click to create a user certificate
Create Certificate for	r User
Descriptive name	Certificat-VPN-JAPON
Certificate authority	CA-JAPON 🗸
Key type	RSA
	2048 The length to use when generating a new RSA key in hits
	The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256 🗸
	The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime	3650

Maintenant que cette préparation est faite on va passer à la configuration open vpn



Et on fait ajouter comme les fois précédentes.

Pour les paramètres on sélectionnera remote acces avec le TLS et l'authentification utilisateur.

General Information		
Description	accès distant OpenVPN 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		
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 commo "tap" mode is capable of carrying 802.3 (OSI Layer 2.)	▼ n and compatible mode across all platform

Ensuite on modifiera le certificat serveur.

Server certificate Certificat-OpenVPN (Server: Yes, CA: CA-JAPON)

Et on va passer aux paramètres de tunnel et ip

En premier on spécifiera l'adresse qui sera donné pour le tunnel VPN

IPv4 Tunnel Network	10.10.10.0/24
	This is the IPv4 virtual network or network type alias with a single entry
io potro récocu pour indi	nuar la zana d'affat

Puis notre réseau pour indiquer la zone d'effet

IPv4 Local network(s)	192.168.30.0/24	
	IPv4 networks that will be accessible from the remote endpoint. Expresse	d as a

On peut également limiter le nombre d'accès simultané au VPN

10

Concurrent connections

Puis en dessous on va cocher une case et sélectionner la topologie net30 la case permet de maintenir une stabilité pour les postes nomades et la topologie elle met chaque utilisateur dans un sous réseau en /30 pour plus de sécurité

\$

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 o

On va ensuite ajouter un domaine par défaut aux clients qui est notre domaine de contexte

	Advanced Client Set	tings	
	DNS Default Domain	Provide a default domain name to clients	
	DNS Default Domain	japon.local)
Ain	si que nos dns		
	DNS Server enable	✓ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.	
	DNS Server 1	192.168.30.10	
	DNS Server 2	192.168.30.9	

Juste avant de sauvegarder

Custom options	auth-nocache

Cette option offre une protection supplémentaire contre le vol des identifiants en refusant la mise en cache.

Prochaine étape installer un package lié à openVPN

	Syst	em 👻	Interfaces 👻	Firewall 👻	Services -	VPN -	Status 👻	Diagnostics ·	- Η∉	elp -	G
System	/ Pack	age N	Manager / A	Available P	ackages						0
Installed Pa	ickages	Availa	able Packages								
Search											Ð
Search terr	n		openvpn					Both	~	Q Search 🕤 Clear	
			Enter a search stri	ing or *nix regula	r expression to s	earch package	e names and	descriptions.			
Packages	3										
Name	Version	Descrip	otion								
openvpn-	1.9.2	Export	s pre-configured C	penVPN Client c	onfigurations dir	ectly from pfS	ense softwar	e.			+ Install



Nous allons maintenant passer à l'export de la configuration openVPN serveur.

Pour la partie haute on sauvegarde sans rien changer.

Advanced	
Additional configuration options	auth-nocache
	Enter any additional options to add to the OpenVPN client export co
	EXAMPLE: remote-random;

Puis en dessous du bouton sauvegarder on va télécharger l'archive bundled configuration

User	Certificate Name	Export
vpn-japon	Certificat-VPN-JAPON	 Inline Configurations: ▲ Most Clients ▲ Android ▲ OpenVPN Connect (iOS/Android Bundled Configurations: ▲ Archive ▲ Config File Only Current Windows Installers (2.6.7-Ix001): ▲ 64-bit ▲ 32-bit Previous Windows Installers (2.5.9-Ix601): ▲ 64-bit ▲ 32-bit Legacy Windows Installers (2.4.12-Ix601): ▲ 10/2016/2019 ▲ 7/8/8.1/2012r2 Viscosity (Mac OS X and Windows): ▲ Viscosity Bundle ▲ Viscosity Inline Config

On va ajouter une règle dans le WAN sur le firewall pour autoriser les connections open vpn avec quelques changements

Firew	vall / Ru	es/WA	N								
Floatin	g WAN	LAN	CARP1	OpenVPN							
Rules	(Drag to C	hange Ord	ler)								
I	States	Protocol	Source		Port	Destination	Port	Gatewa	у		
×	0/56 KiB	*	RFC 1918 ne	tworks	*	*	*	*			
×	0/0 B	*	Reserved Not assigned	by IANA	*	*	*	*			
lo rule: All inco	s are currentl <u>y</u> ming connect	y defined for t tions on this i	his interface nterface will be	blocked until	pass rules	are added. Cli	ck the butt	ion to add	1.		
		Protoco	UDP Choos	e which IP	protoco	ol this rule s	should m	natch.		~	
-	estillatio	Destination	🗍 Invert r	match		WAN addre	SS			~	Destinat
		D	(other)		~	1194			(other)	~	1194
1	Destination	Port Range	From			Custom			То		Custom
			Specify the	e destinatior	port or p	port range for	this rule.	The "To	field may be left em	npty if only	y filtering a
E	xtra Optio	ons									
		Log	Log pa Hint: the fi the Status	ckets that an irewall has li a: System Log	e handle mited loc gs: Settin	d by this rule al log space. gs page).	Don't turr	n on logg	jing for everything. If	f doing a l	ot of loggin
	I	Description	Accès di	stant openVI	PN						
		al a									
nsi	qu'une	aeuxier	ne dans	ia partie	e oper	IVPN					
Оре	enVPN										



	Interface	Open\	VPN			~
estination						
Destination	 Invert match 		Address or Alias		~	192.168.30.15
Destination Port Range	MS RDP (3389)	~		MS RDP (3389) ~	
	From		Custom	То		Custom

On va maintenant se connecter via le post client avec tout d'abord l'installation du client vpn

	ELE D	
🛃 OpenVPN Connect Setup	-	□ X
Installing OpenVPN Connect		Ð
Please wait while the Setup Wizard installs OpenVPN Connect.		
Status: Deleting services		
Back Ne	xt	Cancel
Duk ne		Cantoon

Puis en bas à droite on va sur la petite icône qui est apparue et on fait connecter sur le profil crée récemment.



Puis on rentre les identifiants.

🔁 Connexion Op	penVPN (srv-pf1-	jp-UDP4-119	4-JAPONVPN-	config)		-		\times
Etat actuel: En co	ours de connexion							
Mon Apr 14 11:4 Mon Apr 14 11:4 Mon Apr 14 11:4 Mon Apr 14 11:4	0:40 2025 OpenVF 0:40 2025 Window 0:40 2025 library vo 0:40 2025 DCO ve	PN 2.6.7 [git:v. vs version 10.0 ersions: Open rsion: 1.0.0	2.6.7/53c90333) (Windows 10 or SSL 3.1.4 24 Oc	17b3b8fdj greater), t 2023, Li	Windows [amd64 exec ZO 2.10	SSL (Oper cutable	iSSL)] [LZ	<u>][</u>
	Utilisateur: Mot de passe:	JAPONVPN Azerty.2]]æ				
<	ОК		Annuler					>

OpenVPN GUI 11.45.0.0/2.6.7 On peut ensuite tenter la connexion à notre

session

serveur RDS

n Connexi	on Bureau à distance	_		×
-	Connexion Burea A distance	au		
Ordinateur : Nom	192.168.30.15 JAPON\informatique	~		
Vos informatio connexion.	ons d'identification seront dema	ndées lors de la	A: 1	
Afficher	les options	Connexion	Aide	ľ
and the second the second the second the second the second the second term is a second term in the second term in the second term is a second term in the second term is a second term in the second term in the second term in the second term is a second term in the second term in				
				On

vierge du serveur RDS le VPN fonctionne bel et bien.

Voilà qui conclue notre tp ou nous avons désormais un vpn pour notre infrastructure accessible sur les postes clients pour qu'ils puissent avoir accès à une session à distance prévu pour le travail via VPN. Avec des utilisateurs pour la gestion d'accès on va dans le prochain tp lié les utilisateurs active directory avec les utilisateurs pfsense.