

2022

TP_INTERCONNEXION_VPN

U4_CONCEVOIR_SOLUTION_INFRA
FEVRE & HUBER & YILMAZ

Table des matières

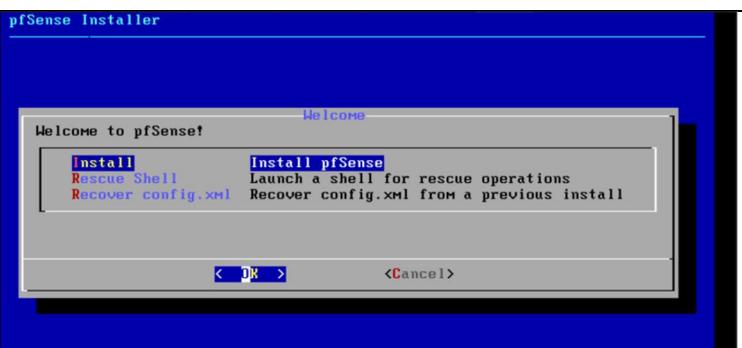
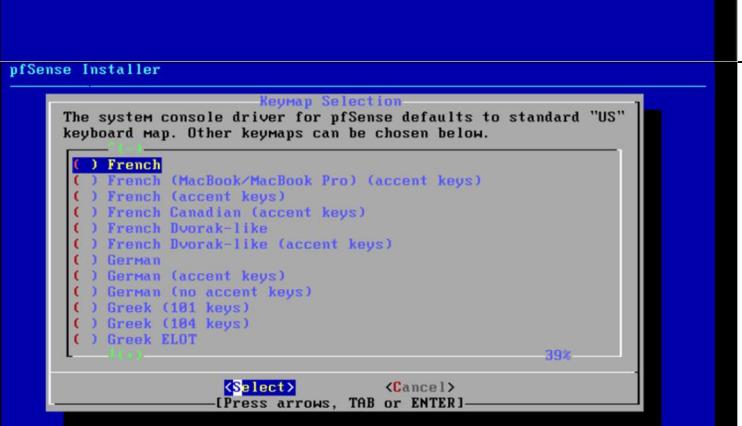
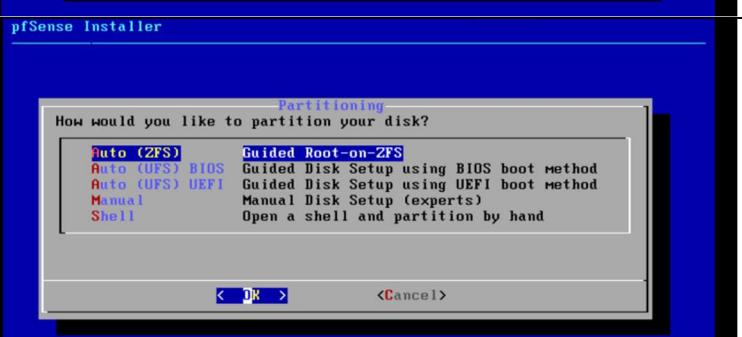
1. Savoir installer et configurer un serveur PfSense.....	2
1.1 Installation de pfsense freeBSD.....	2
1.2 Configuration de PFSense.....	4
1.3 Configuration depuis client Windows 10 Pro.....	4
2. Installer et configurer un VPN site à site (IPsec).....	5
2.1 Prérequis	5
2.2 IPSEC.....	5
2.3 Phase 2	8
2.4 RULES.....	9
2.5 Test de connexion	10
3. Installer et configurer un VPN distant (OpenVPN).....	11
3.1 Création de l'Autorité de Certification – CA.....	11
3.2 Création Certificat Serveur	13
3.3 Création utilisateur VPN	14
3.4 Installation du package « OpenVPN-Client-Export ».....	15
3.5 Configurer OpenVPN	17
3.6 Exporter la configuration VPN pour un Client.....	18
3.7 Configurer les règles du Pare-Feu pfSense.....	20
3.8 Test openvpn.....	21
3.9 Test OpenVPN sur mobile	23
4. Problèmes / Résolutions	24
4.1 Connexion.....	24
4.2 Connexion des serveurs en site-à-site.....	24
4.3 Problème rencontrés.....	25

1. Savoir installer et configurer un serveur PfSense.

Prérequis

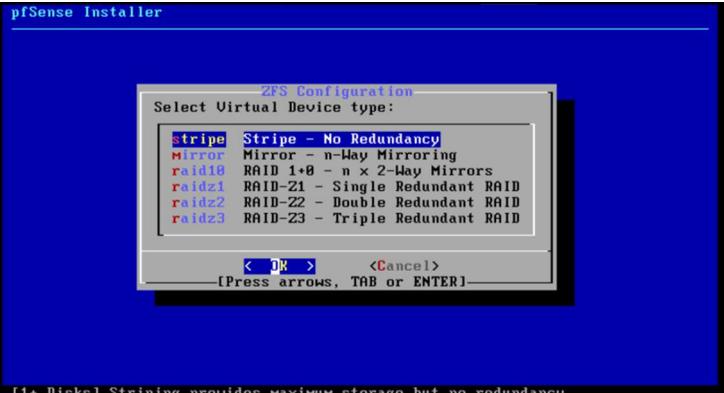
- Une vm PfSense FreeBSD sur VMware avec 2 cartes réseaux, une pour le WAN et une pour le LAN.
- Un client Windows 10 (ici c'est un PRO)

1.1 Installation de pfSense freeBSD

L'installation peut maintenant débuter en validant l'option : Install pfSense	
On choisit ensuite la langue du clavier : () French Puis Entrée.	
Une interface qui demande de partitionner le disque se propose. Restez sur le choix : Auto (2FS) et appuyez sur Entrée.	
La configuration du partitionnement du disque va être demandé, voici le paramétrage :	

Choisir :

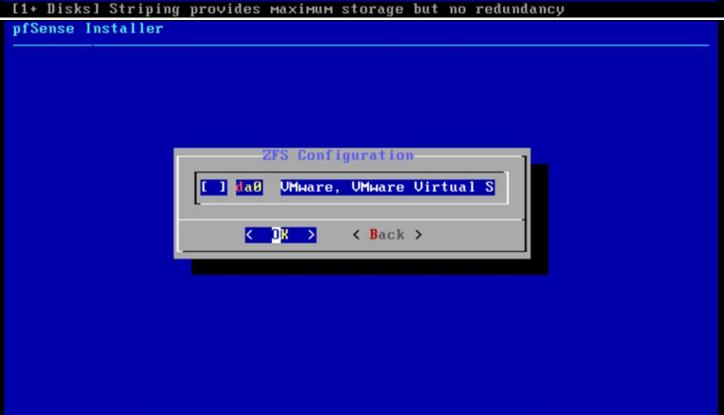
Stripe - No Redundancy



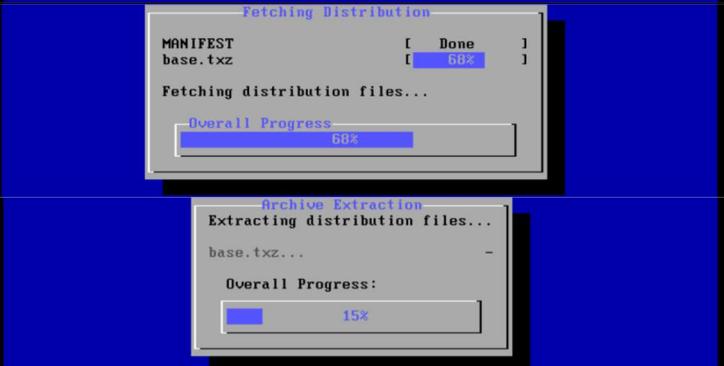
Il faut bien s'assurer à valider le choix :

[] **da0 VMware, VMware Virtual S**

avec **Espace**, puis appuyez sur Entrée.



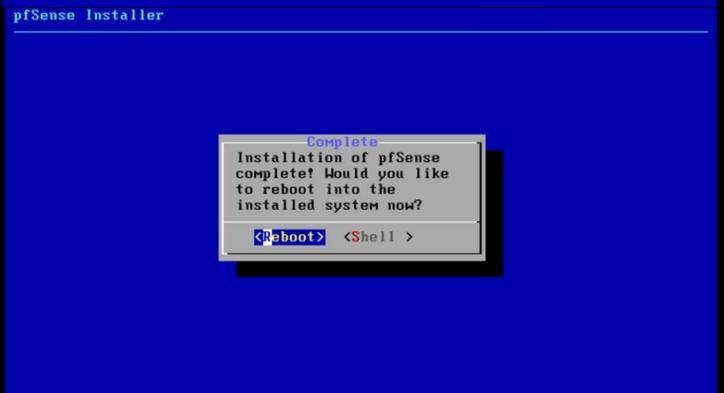
Le partitionnement du disque, puis l'installation de PFSense va alors se lancer.



Une interface qui demande d'ouvrir un shell (terminal) se propose. Restez sur le choix « No » et appuyez sur Entrée.



L'installation est à présent terminée.
Pour finir, appuyez sur Entrée pour reboot la machine et lancer PfSense.



1.2 Configuration de PFsense

<p>L'interface suivant sera proposée une fois la machine démarrée.</p> <p>A partir de ce menu, nous pouvons taper un numéro de 0 à 16 selon le besoin pour configurer la machine.</p>	<pre>Starting syslog...done. Starting CRON... done. pfSense 2.6.8-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022 Bootup complete FreeBSD/amd64 (pfSense.home.arpa) (ttyv0) VMware Virtual Machine - Netgate Device ID: 26f14b542340e3b6427e *** Welcome to pfSense 2.6.8-RELEASE (amd64) on pfSense *** WAN (wan) -> em0 -> v4/DHCP4: 192.168.6.146/24 LAN (lan) -> em1 -> v4: 192.168.1.1/24 0) Logout (SSH only) 9) pfTop 1) Assign Interfaces 10) Filter Logs 2) Set interface(s) IP address 11) Restart webConfigurator 3) Reset webConfigurator password 12) PHP shell + pfSense tools 4) Reset to factory defaults 13) Update from console 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 15) Restore recent configuration 7) Ping host 16) Restart PHP-FPM 8) Shell Enter an option: ■</pre>
<p>Avant de se lancer sur PFsense, il faut d'abord assigner une adresse IP à l'interface LAN.</p> <p>Tapez "2" puis Entrée.</p> <p>Il va alors proposer de choisir entre WAN ou LAN</p> <p>Tapez "2" puis configurer l'IP.</p>	<pre>WAN (wan) -> em0 -> v4/DHCP4: 192.168.6.146/24 LAN (lan) -> em1 -> v4: 192.168.1.1/24 0) Logout (SSH only) 9) pfTop 1) Assign Interfaces 10) Filter Logs 2) Set interface(s) IP address 11) Restart webConfigurator 3) Reset webConfigurator password 12) PHP shell + pfSense tools 4) Reset to factory defaults 13) Update from console 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 15) Restore recent configuration 7) Ping host 16) Restart PHP-FPM 8) Shell Enter an option: 2 Available interfaces: 1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static) Enter the number of the interface you wish to configure: 2 Enter the new LAN IPv4 address. Press <ENTER> for none: > 192.168.6.254■</pre>
<p>Définissez le masque de sous-réseau du réseau local, tapez 24</p>	<pre>4) Reset to factory defaults 13) Update from console 5) Reboot system 14) Enable Secure Shell (sshd) 6) Halt system 15) Restore recent configuration 7) Ping host 16) Restart PHP-FPM 8) Shell Enter an option: 2 Available interfaces: 1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static) Enter the number of the interface you wish to configure: 2 Enter the new LAN IPv4 address. Press <ENTER> for none: > 192.168.6.254 Subnet masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24 255.255.0.0 = 16 255.0.0.0 = 8 Enter the new LAN IPv4 subnet bit count (1 to 32): > 24■</pre>

1.3 Configuration depuis client Windows 10 Pro

Configuration de base = carte réseau avec l'IP sur le même réseau que pfsense et mettre l'IP de pfsense en passerelle (8.8.8.8 en dns pour internet).

Par défaut le login est : admin et le MDP est : pfsense

2. Installer et configurer un VPN site à site (IPsec)

2.1 Prérequis

Deux machines virtuelles PFSENSE sur la même connexion (Exemple : partage de connexion) avec l'adressage IP suivant :

Serveur 1: WAN : 192.168.125.113/24
LAN : 192.168.30.5

Serveur 2: WAN : 192.168.125.14/24
LAN : 192.168.20.5

2.2 IPSEC

Aller dans l'onglet VPN/IPSEC

The screenshot shows the pfSense web interface with the following details:

- Header:** pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, **VPN** (highlighted), Status.
- VPN Submenu:** IPsec (selected), L2TP, OpenVPN.
- Section Header:** VPN / IPsec / Tunnels.
- Text:** Click on the "add P1" button to add Phase 1.
- Table:** IPsec Tunnels (Tunnels tab selected).

ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
1	V2	WAN 192.168.125.14		AES (128 bits)	SHA256	14 (2048 bit)	vpn	Edit Delete Details
2	V2	WAN 192.168.125.128		AES (128 bits)	SHA256	14 (2048 bit)	vpn 2	Edit Delete Details
- Buttons:** Add P1, Delete P1s.
- Text at bottom:** Fill in according to the photo above.
In "Remote Gateway" enter the WAN IP of the second pfSense server.
In "preshared key", enter a word (e.g.: test vpn) or generate a key (it must be the same on both pfSense servers).

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Description
 A description may be entered here for administrative reference (not parsed).

Disabled Set this option to disable this phase1 without removing it from the list.

IKE Endpoint Configuration

Key Exchange version
 Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol
 Select the Internet Protocol family.

Interface
 Select the interface for the local endpoint of this phase1 entry.

Remote Gateway
 Enter the public IP address or host name of the remote gateway.

Renseignez l'adresse IP à laquelle
vous souhaitez vous connecter

Phase 1 Proposal (Authentication)

Authentication Method
 Must match the setting chosen on the remote side.

My Identifier
 Peer Identifier

Pre-Shared Key
 Enter the Pre-Shared Key string. This key must match on both peers.
 This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm	<input type="text" value="AES"/>	Algorithm	<input type="text" value="128 bits"/>	Key length	<input type="text" value="SHA256"/>	Hash	<input type="text" value="14 (2048 bit)"/>	DH Group	
----------------------	----------------------------------	-----------	---------------------------------------	------------	-------------------------------------	------	--	----------	--

Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm

Expiration and Replacement

Life Time
 Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

Rekey Time
 Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.

Reauth Time
 Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.

Rand Time
 A random value up to this amount will be subtracted from Rekey Time/Reauth Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Advanced Options

Child SA Start Action
 Set this option to force specific initiation/responder behavior for child SA (P2) entries

Child SA Close Action
 Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)

NAT Traversal
 Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.

MOBIKE
 Set this option to control the use of MOBIKE

Gateway duplicates	<input type="checkbox"/> Enable this to allow multiple phase 1 configurations with the same endpoint. When enabled, pfSense does not manage routing to the remote gateway and traffic will follow the default route without regard for the chosen interface. Static routes can override this behavior.
Split connections	<input type="checkbox"/> Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support only a single traffic selector per child SA.
PRF Selection	<input type="checkbox"/> Enable manual Pseudo-Random Function (PRF) selection Manual PRF selection is typically not required, but can be useful in combination with AEAD Encryption Algorithms such as AES-GCM
Custom IKE/NAT-T Ports	<input type="text" value="Remote IKE Port"/> <input type="text" value="Remote NAT-T Port"/> UDP port for IKE on the remote gateway. Leave empty for default UDP port for NAT-T on the remote gateway.
Dead Peer Detection	<input checked="" type="checkbox"/> Enable DPD Check the liveness of a peer by using IKEv2 INFORMATIONAL exchanges or IKEv1 R_U_THERE messages. Active DPD checking is only enforced if no IKE or ESP/AH packet has been received for the configured DPD delay.
Delay	<input type="text" value="10"/>
	Delay between sending peer acknowledgement messages. In IKEv2, a value of 0 sends no additional messages and only standard messages (such as those to rekey) are used to detect dead peers.
Max failures	<input type="text" value="5"/>
	Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the retransmission timeout is used instead.

Save

2.3 Phase 2

Cliquez sur « add P2 » pour renseigner la phase 2

Add P2

Remplir selon la photo ci-dessus. Dans le remote Network, bien renseignez l'adresse réseau de la LAN du second serveur PfSense

VPN / IPsec / Tunnels / Edit Phase 2

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Description: site 1 vers site 2
A description may be entered here for administrative reference (not parsed).

Disabled: Disable this phase 2 entry without removing it from the list.

Mode: Tunnel IPv4

Phase 1: vpn (IKE ID 1)

P2 reqid: 1

Networks

Local Network: LAN subnet / 0
Type: Address
Local network component of this IPsec security association.

NAT/BINAT translation: None / 0
Type: Address
If NAT/BINAT is required on this network specify the address to be translated

Remote Network: Network / 24
Type: Address
Address: 192.168.20.0 / 24
Remote network component of this IPsec security association.

Phase 2 Proposal (SA/Key Exchange)

Protocol: ESP
Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.

Encryption Algorithms: AES 128 bits
AES128-GCM 128 bits

<input type="checkbox"/> AES256-GCM	Auto	▼
<input type="checkbox"/> Blowfish	Auto	▼
<input type="checkbox"/> 3DES		
<input type="checkbox"/> CAST128		
Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.		
Hash Algorithms	<input type="checkbox"/> MD5 <input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC	
Note: Hash is ignored with GCM algorithms. MD5 and SHA1 provide weak security and should be avoided.		
PFS key group	14 (2048 bit)	▼
Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.		
Expiration and Replacement		
Life Time	3600	
Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.		
Rekey Time	3240	
Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.		
Rand Time	360	
A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.		
Keep Alive		
Automatically ping host	192.168.125.14	
Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation of a tunnel mode P2, but does not trigger initiation of a VTI mode P2.		
Keep Alive	<input type="checkbox"/> Enable periodic keep alive check	
Periodically checks to see if the P2 is disconnected and initiates when it is down. Does not send traffic inside the tunnel. Works for VTI and tunnel mode P2 entries. For IKEv2 without split connections, this only needs enabled on one P2.		
Save		

2.4 RULES

Allez dans « Interfaces/WAN » descendre tout en bas de la page puis décochez les 2 cases dans la partie « Reserved Networks »

Reserved Networks		
Block private networks and loopback addresses	<input type="checkbox"/>	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input type="checkbox"/>	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.
Save		

Ensuite, allez dans l'onglet « Firewall / Rules » Commencez par la partie WAN, modifier la règle en changeant le protocole par « Any » puis sauvegardez

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Appliquez les mêmes paramètres pour la partie LAN et IPsec puis rajoutez une règle en autorisant le protocole ICMP dans IPsec.

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

IPsec

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes

Any

Alternate Host
Datagram conversion error
Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

2.5 Test de connexion

IPsec Status								
ID	Description	Local		Remote	Role	Timers	Algo	Status
con1 #2	vpn	ID: 192.168.89.113 	Host: 192.168.89.113:500	ID: 192.168.89.14 Host: 192.168.89.14:500	IKEv2 Responder	Rekey: 25439s (07:03:59) Reauth: Disabled	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established 28 seconds (00:00:28) ago
con1: #4	site 1 vers site 2	Local: 192.168.30.0/24 	Remote: c3d2d147	192.168.20.0/24 Remote: c31db392	Rekey: 2938s (00:48:58) Life: 3572s (00:59:32) Install: 28s (00:00:28)	AES_GCM_16 (128) IPComp: None	Bytes-In: 0 (0 B) Packets-In: 0 Bytes-Out: 0 (0 B) Packets-Out: 0	Installed

```

Microsoft Windows [version 10.0.19044.1889]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\user>ping 192.168.125.113

Envoi d'une requête 'Ping' à 192.168.125.113 avec 32 octets de données :
Réponse de 192.168.125.113 : octets=32 temps=10 ms TTL=63
Réponse de 192.168.125.113 : octets=32 temps=29 ms TTL=63
Réponse de 192.168.125.113 : octets=32 temps=10 ms TTL=63
Réponse de 192.168.125.113 : octets=32 temps=9 ms TTL=63

Statistiques Ping pour 192.168.125.113:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 9ms, Maximum = 110ms, Moyenne = 39ms

C:\Users\user>

```

Remote: ca9e05d5 Life: 3495s (00:58:15)
Install: 105s (00:01:45) IPComp: None
Packets-In: 0 Bytes-Out: 0 (0 B) Packets-Out: 0

La connexion est établie et le ping passe.

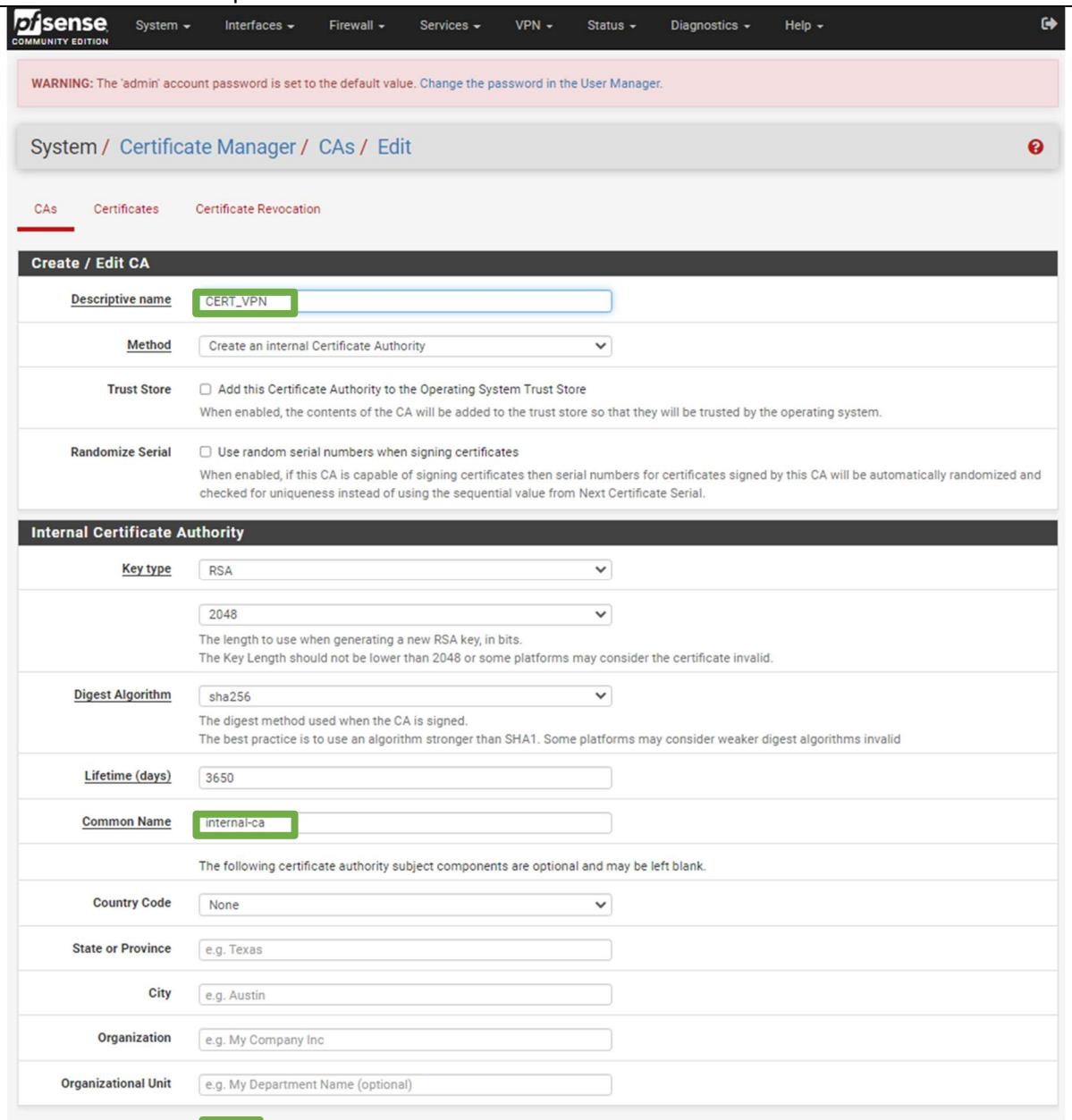
3. Installer et configurer un VPN distant (OpenVPN)

3.1 Création de l'Autorité de Certification – CA

Accédez à System > Certificate Manager > CAs, et cliquez sur le bouton Add en bas à droite.

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions

Remplir le « Descriptive name » (sans espaces, ni caractères spéciaux)
 Faire la même chose pour le Common Name



The screenshot shows the pfSense web interface under the System / Certificate Manager / CAs / Edit section. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The "Create / Edit CA" form is displayed, with the "Descriptive name" field set to "CERT_VPN". Other settings include "Method: Create an internal Certificate Authority", "Trust Store" checked, "Randomize Serial" unchecked, and "Key type: RSA" with a length of "2048". The "Common Name" field is set to "internal-ca". The "Save" button is highlighted in green.

Le certificat est créé

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CERT_VPN	✓	self-signed	0	CN=internal-ca 		   

3.2 Crédation Certificat Serveur

Dans la même rubrique Certificate Manager, accédez à l'onglet Certificat et cliquez sur le bouton Add en bas à droite.

The screenshot shows the 'Certificates' section of the pfSense Certificate Manager. It lists a single certificate entry:

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (633aa3130ba73) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-633aa3130ba73 ⓘ Valid From: Mon, 03 Oct 2022 08:53:39 +0000 Valid Until: Sun, 05 Nov 2023 08:53:39 +0000	webConfigurator	edit, delete, export, import, renew

A large green arrow points from the bottom right of the table area towards the 'Add/Sig' button.

Définir « Method » sur « Create an Internal Certificate» , donner un Nom « CERT_SERV » et sélectionner l'autorité de certification « Certificate authority » créé précédemment « CERT_VPN »

The screenshot shows the 'Add/Sign a New Certificate' form. The 'Method' dropdown is set to 'Create an internal Certificate'. The 'Common Name' field is highlighted with a green box and contains the value 'CERT_SERV'. Other fields include:

- Internal Certificate**:
 - Certificate authority: CERT_VPN
 - Key type: RSA
 - Key Length: 2048
 - Digest Algorithm: sha256
 - Lifetime (days): 3650
- Subject Fields**:
 - Country Code: None
 - State or Province: e.g. Texas
 - City: e.g. Austin
 - Organization: e.g. My Company Inc
 - Organizational Unit: e.g. My Department Name (optional)
- Certificate Attributes**: (This section is currently empty.)

Sélectionnez « Server Certificate » et sauvegardez

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type **Server Certificate** Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names FQDN or Hostname **Type** Value Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add **+ Add**

Save

Le certificat est créé

Search

Search term Both **Search** **Clear**

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

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (633aa3130ba73)	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-633aa3130ba73 i	webConfigurator	
Server Certificate CA: No Server: Yes		Valid From: Mon, 03 Oct 2022 08:53:39 +0000 Valid Until: Sun, 05 Nov 2023 08:53:39 +0000		
CERT_SERVER Server Certificate CA: No Server: Yes	CERT_VPN	CN=CERT_SERVER i Valid From: Tue, 04 Oct 2022 12:23:15 +0000 Valid Until: Fri, 01 Oct 2032 12:23:15 +0000		

+ Add/Sign

3.3 Crédit utilisation VPN

Sélectionnez : System > User Manager

WARNING: The

System / **Users** **User Manager**

User Manager

Cliquez sur « Add »

Users

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	

+ Add **Delete**

Rentrez le nom « User_vpn » et un mot de passe puis cochez la case « Click to create a user certificate » entrez le nom « CA_User » et sélectionnez le « Certificate authority » « CERT_VPN » puis « save »

The screenshot shows the 'User Properties' section of the User Manager. A new user 'User_VPN' is being created with a password. Under 'Custom Settings', the 'Click to create a user certificate' checkbox is checked. Below it, the 'Create Certificate for User' section is open, where 'CA_User' is selected as the descriptive name and 'CERT_VPN' is chosen as the certificate authority.

User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	User_VPN
Password	*****
Full name	
Expiration date	
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	admins
Not member of	
Member of	
Move to "Member of" list Move to "Not member of" list	
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	
Certificate	<input checked="" type="checkbox"/> Click to create a user certificate
Create Certificate for User	
Descriptive name	CA_User
Certificate authority	CERT_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 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

3.4 Installation du package « OpenVPN-Client-Export »

The screenshot shows the 'Available Packages' section of the Package Manager. The search bar contains 'openvpn'. The results list includes 'openvpn' and 'openvpn-client-export'. The 'openvpn-client-export' package is highlighted.

Available Packages	
openvpn	OpenVPN Client
openvpn-client-export	OpenVPN Client Export

Sélectionnez « Available Packages» , rechercher « openvpn » et installer « openvpn-client-export »

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: openvpn

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

Name	Version	Description
openvpn-client-export	1.6_4	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.

Package Dependencies:

- openvpn-client-export-2.5.2
- openvpn-2.5.4_1
- zip-3.0_1
- p7zip-16.02_3

Puis cliquez sur « Confirm »

Confirmation Required to install package pfSense-pkg-openvpn-client-export.

Confirm

Patientez le temps de l'installation

System / Package Manager / Package Installer

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

Installed Packages Available Packages Package Installer

Package Installation

```
>>> Installing pfSense-pkg-openvpn-client-export...
Updating pfSense-core repository catalogue...
```

System / Package Manager / Package Installer

pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

```
-- 
===> NOTICE:

The p7zip port currently does not have a maintainer. As a result, it is
more likely to have unresolved issues, not be up-to-date, or even be removed in
the future. To volunteer to maintain this port, please create an issue at:

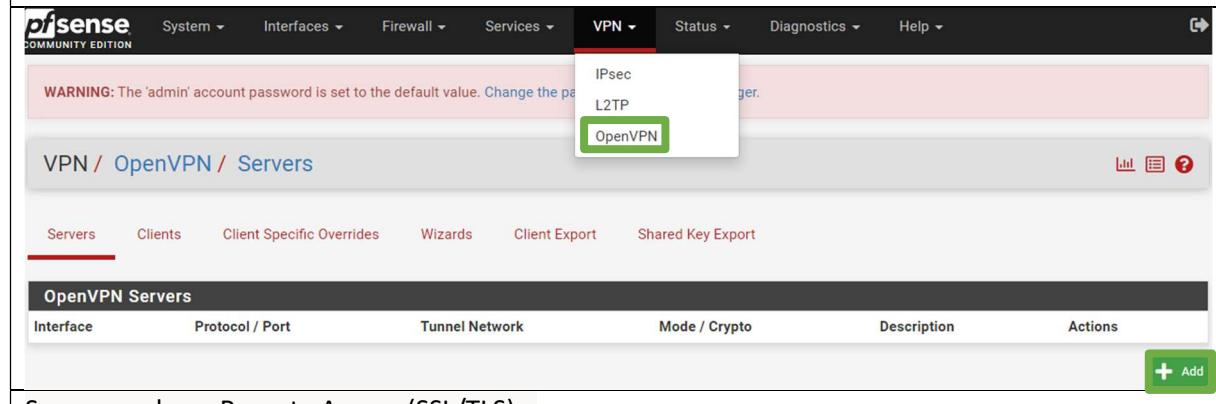
https://bugs.freebsd.org/bugzilla

More information about port maintainership is available at:

https://docs.freebsd.org/en/articles/contributing/#ports-contributing
>>> Cleaning up cache... done.
Success
```

3.5 Configurer OpenVPN

Sélectionnez « VPN » > « OpenVPN » et cliquer sur « + Add »



Server mode : « Remote Access (SSL/TLS) »
Local port : 1194 (Port par Défaut)
Description : « OpenVPN » (Nom du Tunnel VPN)

VPN / OpenVPN / Servers / Edit

General Information

Description: 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)
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: WAN
The interface or Virtual IP address where OpenVPN will receive client connections.
Local port: 1194
The port used by OpenVPN to receive client connections.

Sélectionnez votre autorité de certification « CERT_VPN » dans « Peer Certificate Authority » et le certificat Server « CERT_SERV » dans « Server certificate ».

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.
- Automatically generate a TLS Key.

Peer Certificate Authority: CERT_VPN

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: CERT_SERV (Server: Yes, CA: CERT_VPN)

IPv4 Tunnel Network : 192.168.89.0/24 (Adresse du tunnel VPN CIDR. Nous pouvons utiliser n'importe quel adresse IP privée sauf celles définies par la RFC 1918)
 Cocher « Redirect IPv4 Gateway » pour passer en mode full tunnel
 Concurrent connections : Nombre de connexions VPN simultanées (ici 20)

Tunnel Settings

IPv4 Tunnel Network 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.

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.

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.

Cocher « Dynamic IP » et laisser « Topology » sur « Subnet – One IP address per client... »

Client Settings

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

Topology Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Indiquez « auth-nocache » dans « Custom options». (Pas de mise en cache des identifiants)

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"

Puis cliquez sur « save », Le serveur vpn est créé.

3.6 Exporter la configuration VPN pour un Client

Menu « Client Export », Sélectionnez « Other » pour « Host Name Resolution » et renseigner votre IP WAN Publique dans « Host Name »

OpenVPN / Client Export Utility

- [Server](#)
- [Client](#)
- [Client Specific Overrides](#)
- [Wizards](#)
- [Client Export](#) **Client Export**
- [Shared Key Export](#)

OpenVPN Server

Remote Access Server

Client Connection Behavior

Host Name Resolution Other

Host Name Enter the hostname or IP address the client will use to connect to this server.

Indiquez « auth-nocache » dans « Additional configuration options » puis save

Advanced

Additional configuration options	auth-nocache
----------------------------------	---------------------

Toujours dans le Menu « Client Export », en bas de page, « OpenVPN Clients », 2 Solutions pour l'installation des postes Clients :

- 1ère solution : Cliquez sur « Most Clients » pour télécharger uniquement la configuration du Client à importer sur son ordinateur
- 2ème solution : Sélectionnez « 64-bit » pour télécharger le Package OpenVPN (Logiciel + fichiers de configuration)

Nous allons choisir la solution 2.

OpenVPN Clients		
User	Certificate Name	Export
Certificate (SSL/TLS, no Auth)	CA_User	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none"> Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none"> Archive Config File Only - Current Windows Installer (2.5.2-lx01): <ul style="list-style-type: none"> 64-bit 32-bit - Legacy Windows Installers (2.4.11-lx01): <ul style="list-style-type: none"> 10/2016/2019 7/8.1/2012r2 - Viscosity (Mac OS X and Windows): <ul style="list-style-type: none"> Viscosity Bundle Viscosity Inline Config - Yealink SIP Handsets: <ul style="list-style-type: none"> T28 T38G (1) T38G (2) / V83 - Snom SIP Handsets: <ul style="list-style-type: none"> SNOM

3.7 Configurer les règles du Pare-Feu pfSense

Firewall > Rules > WAN : cliquez sur "+ Add" et renseignez :

Action: Pass

Interface: WAN

Protocol: UDP

Source: any

Destination: WAN address

Destination Port Range: OpenVPN (1194)

Puis cliquez sur "Sauvegarder"

Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: UDP

Choose which IP protocol this rule should match.

Source

Source: Invert match any Source Address /

Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination: Invert match WAN address Destination Address /

Destination Port Range: OpenVPN (1194) From Custom To OpenVPN (1194) To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description:
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

Save

Firewall > Rules > OpenVPN: cliquez sur "+ Add"

Action: Pass

Interface: OpenVPN

Protocol: Any

Source: any

Destination: any

Firewall / Rules / Edit

Edit Firewall Rule

Action	Pass	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
Interface	OpenVPN	Choose the interface from which packets must come to match this rule.
Address Family	IPv4	Select the Internet Protocol version this rule applies to.
Protocol	Anycast	Choose which IP protocol this rule should match.
Source		
Source	<input type="checkbox"/> Invert match	any
Destination		
Destination	<input type="checkbox"/> Invert match	any
Extra Options		
Log	<input type="checkbox"/> Log packets that are handled by this rule	Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	Display Advanced	
Save		

3.8 Test openvpn

Tout d'abord téléchargez le paquet « x64 » dans l'onglet « vpn/openvpn/client export »

Téléchargements

openvpn-pfSense-UDP4-1194-User_VPN-install-2.5.2-l6...

Ouvrir un fichier

Installez-le sur le poste client

Setup OpenVPN 2.5.2-l601

Installing OpenVPN...

Processing Wintun driver

Une fois installé aller faire un clic droit sur l'icone vpn puis « connecter »

Connecter

Déconnecter

Reconnect

Afficher le statut

Voir le log

Editer la configuration

Effacer les mots de passe enregistrés

Changer le Mot de passe

Importer fichier...

Configuration...

Quitter

La connexion est établie



OpenVPN GUI for Windows



**pfSense-UDP4-1194-User_VPN-config
est désormais connecté.**

Adresse IP assignée: 192.168.89.2

3.9 Test OpenVPN sur mobile

Tout d'abord, télécharger le paquet "Inline Configuration Android" ou "Android/IOS".

Search

Search term

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

OpenVPN Clients

User	Certificate Name	Export
user	user	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installers (2.5.2-1x01): 64-bit 32-bit - Legacy Windows Installers (2.4.11-1x01): 10/2016/2019 7/8/8.1/2012/2 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

Ensuite, Archiver ce fichier avec Winrar ou 7-zip et envoyer le sur votre mobile via un mail.
Une fois le .zip réceptionné, téléchargez l'application RAR pour le désarchiver sur votre mobile.

Pour finir, installez l'application Openvpn sur le PlayStore de votre mobile et ouvrez-la, une page d'import de profil va s'afficher. Importez le fichier importé.

09:33 72%

← Import Profile

URL FILE

You can import only one profile at a time.

BROWSE

Une fois l'import effectuer, connecter vous avec les identifiants de l'utilisateur que vous avez créer préalablement sur PfSense.

09:28 73%

☰ Profiles

CONNECTED

OpenVPN Profile
192.168.89.14 [PfSense-UDP4-11
94-user-android-config]

CONNECTION STATS

39kB/s

0B/s

BYTES IN 4 B/S

BYTES OUT 11 B/S

DURATION 0:00:37

PACKET RECEIVED 9 sec ago

YOU user

YOUR PRIVATE IP 172.168.10.2

+

4. Problèmes / Résolutions

4.1 Connexion

Les VPN ne s'interconnecteront pas tant qu'ils n'ont pas des IP WAN sous le même réseau. L'idéal pour résoudre ce problème, est de connecter les VM sur la même connexion internet. Ensuite, accédez au terminal de votre serveur PfSense.

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.125.128/24
LAN (lan)      -> em1      -> v4: 192.168.10.5/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

Tapez 2 "Set interface(s) IP address"

Configurez l'adresse et sélectionnez DHCP

Tapez 5 « Reboot system »

Une fois que vos VM ont redémarré, ils prendront une adresse IP WAN sous le même réseaux (192.168.125...)

4.2 Connexion des serveurs en site-à-site

Les deux VPN peuvent ne pas se connecter, pour cela il faut désactiver les pare-feux du PC hôte et des VMs.

Pour cela, tapez « pare-feu » sur la barre de recherche Windows.



Vérifier l'état du **pare-feu**

Panneau de configuration

Une fenêtre concernant l'état des pare-feux va apparaître, de là il est possible de les désactiver.

4.3 Problème rencontrés

Absence de ping	Paramétrier correctement les règles pare-feu sur PFSense
Absence de connexion Phase 2	Lors de la configuration, mettre l'adresse réseau de l'adresse LAN et non l'adresse LAN directement Exemple : Adresse IP LAN : 192.168.125.93 Adresse réseau : 192.168.125.0