

BTS 2 option SISR

## Pfsense Intiation

I.	Pfsense.....	2
A.	Pré-installation Pfsense.....	2
1.	Téléchargement.....	2
2.	Créations des LAN.....	2
3.	Configuration du Pfsense.....	3
B.	Installation Pfsense.....	4
C.	Configuration de l'interface LAN.....	5
D.	Interface web.....	6
1.	<b>Connexion</b> à l'interface web.....	6
2.	Changer le mot de passe administrateur.....	7
3.	Mettre clavier en AZERTY.....	7
4.	Configuration de l' <b>accès</b> à l'interface.....	7
5.	Configuration de l'interface WAN.....	8
6.	<b>Désactiver le pare-feu de pfsense</b> .....	10
7.	<b>Vérification des règles de pare-feu</b> .....	10
E.	VPN avec OpenVPN.....	11
1.	Création du Certificate Authority dans le LAN_Naturacorp.....	11
2.	Création des utilisateurs.....	12
3.	Création du serveur OpenVPN.....	13
4.	Installation du plugin du client OpenVPN.....	15
5.	<b>Téléchargement du client OpenVPN</b> .....	16
6.	Installation et configuration du client OpenVPN.....	16
F.	IPsec.....	17
1.	Contexte.....	17
1.	Configuration du VPN du site 1.....	18
2.	Configuration du VPN du site 2.....	20
3.	Configuration du pare-feu et redirections de ports.....	21
4.	Configuration la redirection de port des routeurs.....	22
5.	Test du VPN.....	22
6.	Valider le fonctionnement du VPN.....	22

# I. Pfsense

## A. Pré-installation Pfsense

### 1. Téléchargement

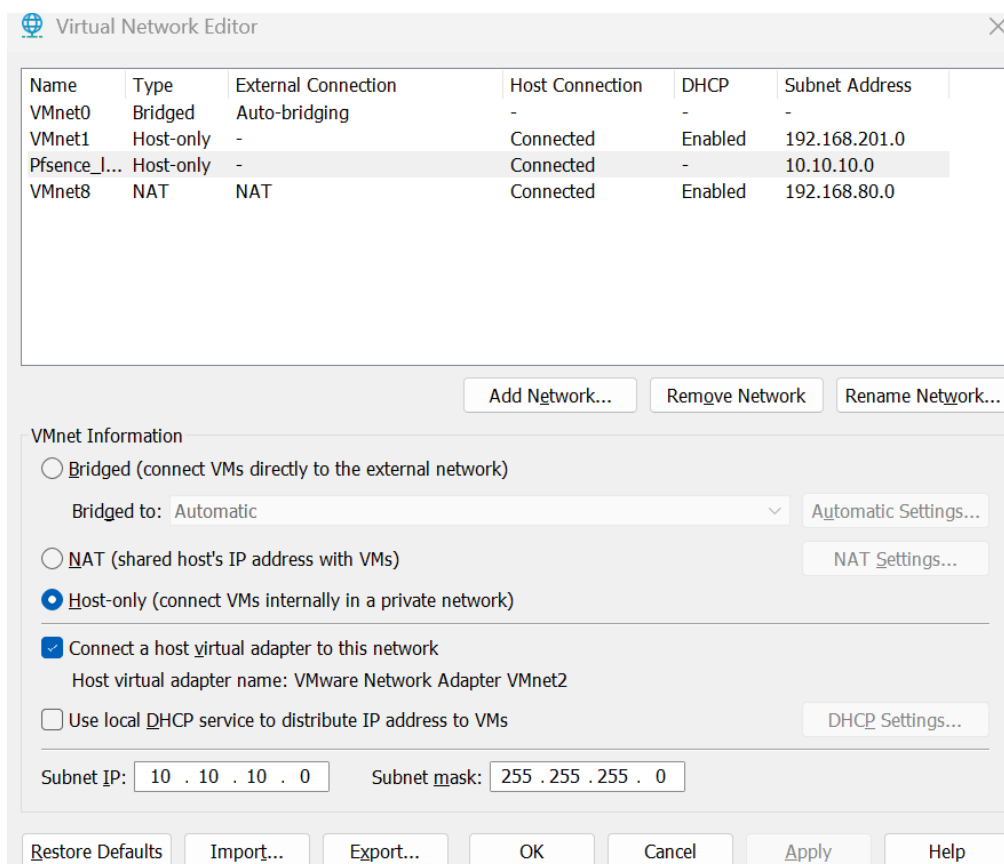
Dans le lien <https://sgpfiles.netgate.com/mirror/downloads/> , télécharger la dernière version comportant .gz :

## Index of /mirror/downloads/

../			
<a href="#">pfSense-CE-2.6.0-RELEASE-amd64.iso.gz</a>	31-Jan-2022 20:31	437073513	
<a href="#">pfSense-CE-2.6.0-RELEASE-amd64.iso.gz.sha256</a>	31-Jan-2022 20:32	114	
<a href="#">pfSense-CE-2.7.0-RELEASE-amd64.iso.gz</a>	29-Jun-2023 20:11	495733706	
<a href="#">pfSense-CE-2.7.0-RELEASE-amd64.iso.gz.sha256</a>	29-Jun-2023 20:11	114	
<a href="#">pfSense-CE-2.7.1-RELEASE-amd64.iso.gz</a>	17-Nov-2023 00:47	574639430	
<a href="#">pfSense-CE-2.7.1-RELEASE-amd64.iso.gz.sha256</a>	17-Nov-2023 00:47	114	
<a href="#">pfSense-CE-2.7.2-RELEASE-amd64.iso.gz</a>	08-Dec-2023 18:27	574277009	

### 2. Créations des LAN

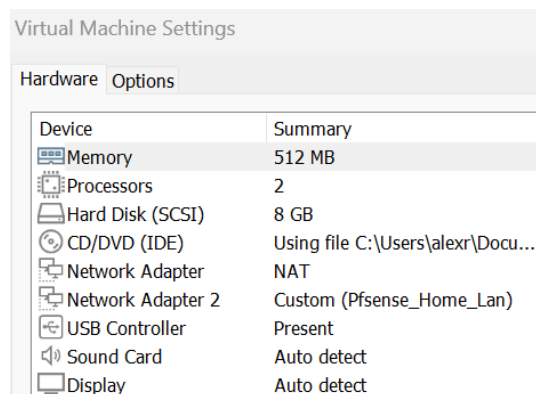
Dans VMware > Edit > Virtual Network Editor > Add Network, ajoutez la LAN Pfsence\_Iniatiation en Host-only sans de DHCP:



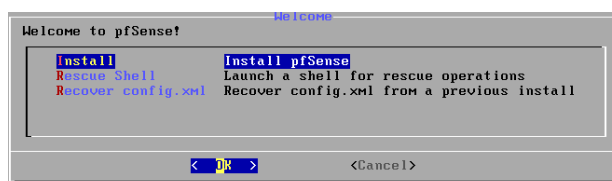
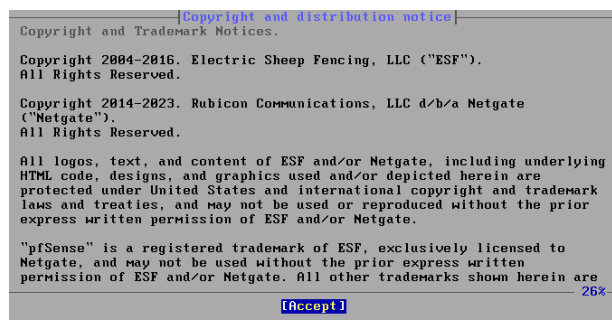
### 3. Configuration du Pfsense

Créez une VM possédant la configuration suivante :

- Type de VM dans VMware : linux
- Hard Disk : 8 gb
- Memory : 512 mb
- Network adapter 1 : NAT
- Network adapter 2 : LAN créer précédemment



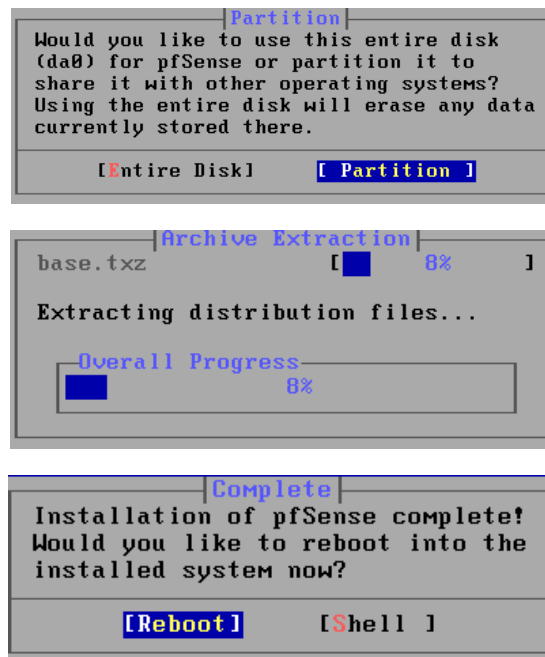
### B. Installation Pfsense



- Sélectionnez le partitionnement automatique "ZFS" ou "UFS" :



- Partitionnement automatique "UFS" :



## C. Configuration de l'interface LAN

Après l'installation de Pfsense la première chose à faire est de configurer l'interface du LAN qui n'est pas par défaut dans le réseau local. Il faut adapter l'IP en fonction du LAN créé précédemment dans notre cas (10.10.10.254 = Pfsense\_Initiation; 10.10.2.254 = LAN\_ ESN) :

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: d27b6043dd8895e4dbb6

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.1.22.23/23
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: █
```

- Pour configurer l'interface du LAN tapez 2 et suivez les commandes indiquées ci-dessous :

```

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - dhcp)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.10.254

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

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

```

```

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

```

```

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.10.10.100
Enter the end address of the IPv4 client address range: 10.10.10.200
Disabling IPv6 DHCPD...

]

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 LAN address has been set to 10.10.10.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
        http://10.10.10.254/

Press <ENTER> to continue.

```

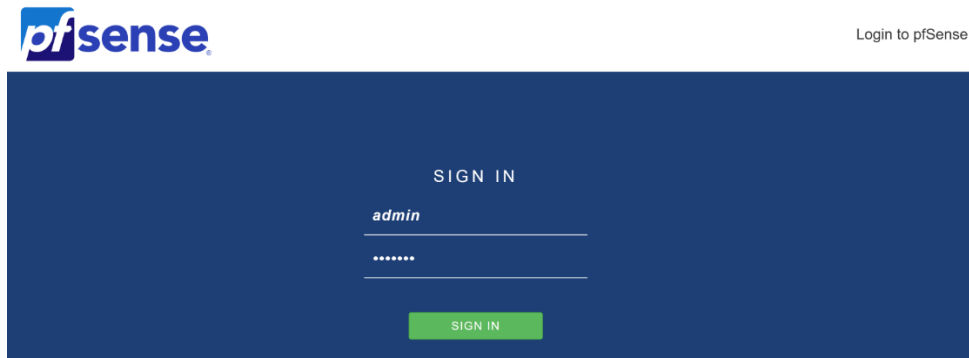
## D. Interface web

### 1. Connexion à l'interface web

Connectez-vous à l'interface web depuis l'IP de l'interface LAN en utilisant l'identifiant suivant :

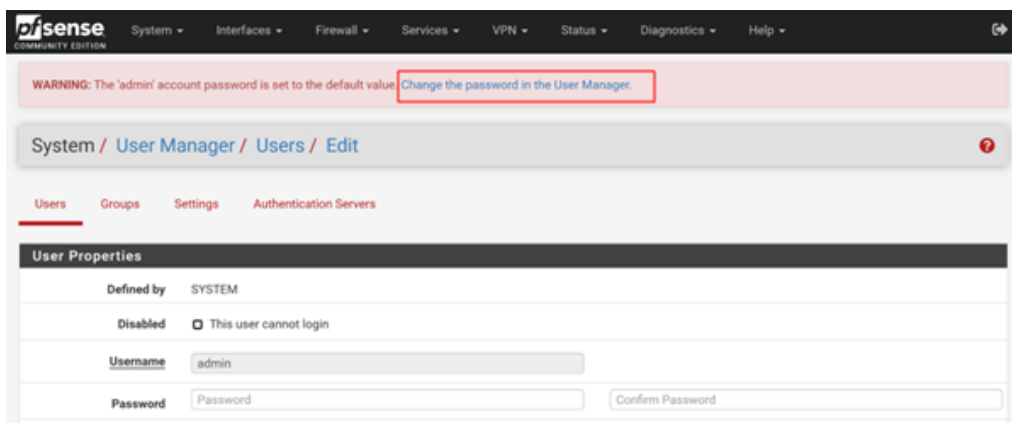
- <https://10.10.10.254> (Pfsense\_Initiation),

- Username : admin
- Password : pfsense



## 2. Changer le mot de passe administrateur

Après la première connexion, un encadré rouge est affiché sur la page d'accueil. Cliquez sur le lien en bleu pour le modifier :



## 3. Mettre clavier en AZERTY

Installer le service shellcmd avec System > Package Manager > Available Packages :

Services: Shellcmd Settings / Edit

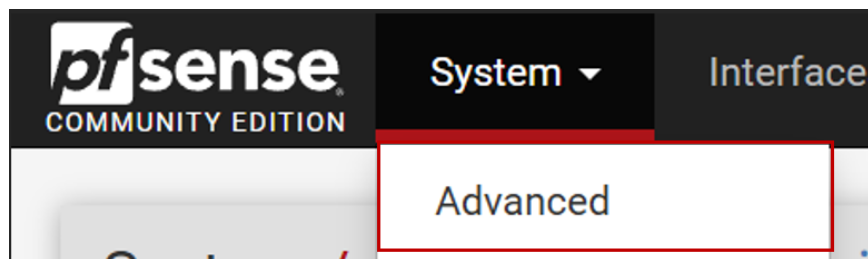
### Shellcmd Configuration

<b>Command</b>	<input type="text" value="kbdcontrol -I /usr/share/syscons/keymaps/fr.iso.kbd"/>
Enter the command to run.	
<b>Shellcmd Type</b>	<input type="text" value="shellcmd"/>
Choose the shellcmd type. Click Info for details. <a href="#">i</a>	
<b>Description</b>	<input type="text" value="clavier azerty"/>
Enter a description for this command. (This is for your reference only.)	

[Save](#)

#### 4. Configuration de l'accès à l'interface

- Dans System > Advanced :



- Mettre le protocole en « HTTPS » pour plus de sécurité et augmenter le nombre de connexions simultanées à l'interface web :

webConfigurator

<b>Protocol</b>	<input type="radio"/> HTTP	<input checked="" type="radio"/> HTTPS (SSL/TLS)
<b>SSL/TLS Certificate</b>	<input type="text" value="GUI default (67600011c04a2)"/>	
Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.		
<b>TCP port</b>	<input type="text" value="443"/>	
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.		
<b>Max Processes</b>	<input type="text" value="10"/>	
Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.		

- Désactiver l'option « Browser http\_REFERER enforcement » pour avoir accès à l'interface web du Pfsense depuis l'adresse publique :

<b>Browser HTTP_REFERER enforcement</b>	<input checked="" type="checkbox"/> Disable HTTP_REFERER enforcement check
When this is unchecked, access to the webConfigurator is protected against HTTP_REFERER redirection attempts. Check this box to disable this protection if it interferes with webConfigurator access in certain corner cases such as using external scripts to interact with this system. More information on HTTP_REFERER is available from <a href="#">Wikipedia</a> .	

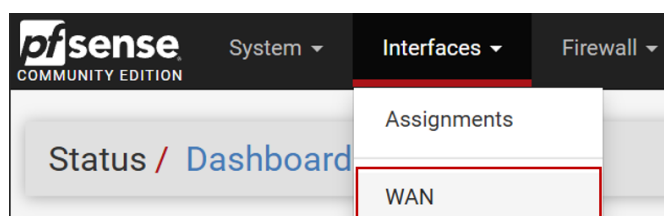




An HTTP\_REFERER was detected other than what is defined in System -> Advanced (https://mon\_ip\_public:22000/). If not needed, this check can be disabled in System -> Advanced -> Admin.

## 5. Configuration de l'interface WAN

- Dans Interfaces > WAN :



- Pfsense bloque par défaut l'accès à l'interface Web avec l'IP WAN. Mettre une IP fixe avec bonne gateway donner par VMware dans « Virtual Network Editor » et décocher les 2 dernières cases de la rubrique « Reserved Networks > NAT Settings » :

**Static IPv4 Configuration**

IPv4 Address: 192.168.1.24 / 24

IPv4 Upstream gateway: WANGW1 - 192.168.1.1 [+ Add a new gateway](#)

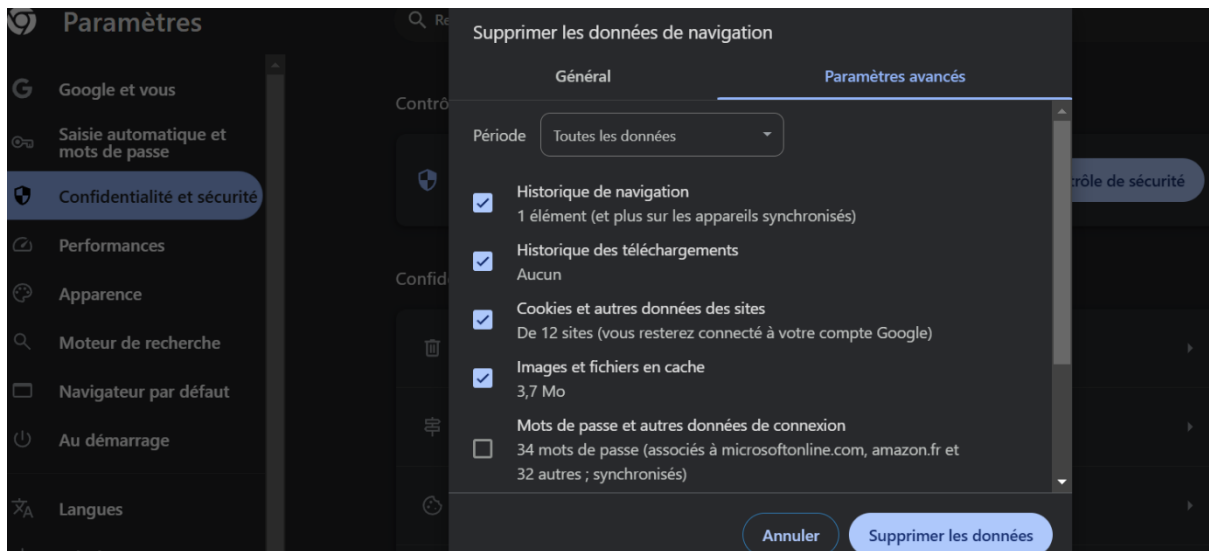
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none".  
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.  
Gateways can be managed by [clicking here](#).

**Reserved Networks**

**Block private networks and loopback addresses** ☐  
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** ☐  
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.

- DEBUG connexion interface (2). Il est possible d'avoir une erreur concernant les cookies ou le jeton CSRF, videz le cache de votre navigateur et essayez de vous reconnecter. Chrome > Supprimez les données de navigations :



## 6. Désactiver le pare-feu de pfsense

- Désactiver les règles de pare-feu en cas d'erreur ou le temps de configurer correctement pfsense. Tapez « 8 » pour ouvrir le shell et tapez pour arrêter le pare-feu « pfctl -d » :

```
[2.7.2-RELEASE][root@pfSense.home.arpal/root: pfctl -d
pf disabled
```

- Tapez pour relancer le pare-feu « pfctl -e » :

```
[2.7.2-RELEASE][root@pfSense.home.arpal/root: pfctl -e
pf enabled
```

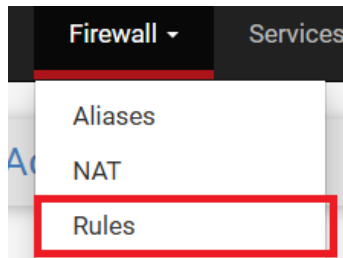
- Le pare-feu se relance à chaque modification de configuration. Pour garder le pare-feu éteint, tapez « sh -c 'while true; do pfctl -d; sleep 5; done' » :

```
[2.7.2-RELEASE][root@pfSense.home.arpal/root: sh -c 'while true; do pfctl -d; sl
eep 5; done'
pf disabled
pfctl: pf not enabled
```

- Pour sortir du shell tapez « exit »

## 7. Vérification des règles de pare-feu

- Dans Firewall > Rules



- Pour le WAN :

Firewall / Rules / WAN

Floating WAN LAN OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	*	*	WAN subnets	443 (HTTPS)	*	none			

Add Add Delete Toggle Copy Save Separator

- Pour le LAN :

Firewall / Rules / LAN

Floating WAN LAN IPsec OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
2/1.06 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Logout Rule	
0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

## E. VPN avec OpenVPN

Un VPN Site-to-Site, ou LAN-to-LAN, connecte deux réseaux locaux distants pour qu'ils communiquent comme s'ils étaient sur un même réseau. Dans notre cas on utilisera l'outil OpenVPN pour connecter le poste Windows Client Home situé dans le LAN\_Home au LAN\_Naturacorp.

### 1. Création du Certificate Authority dans le LAN\_Naturacorp

- Dans System > Certificate > Add :

System / Certificate / Authorities

Authorities Certificates Revocation

**Search**

Search term  Both

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

**Certificate Authorities**

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
+ Add						

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

**Create / Edit CA**

**Descriptive name**   
 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: ?, >, <, &, /, \, ' , "

**Method**

**Trust Store** ☐ Add this Certificate Authority to the Operating System Trust Store  
 When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

**Randomize Serial** ☐ Use random serial numbers when signing certificates  
 When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

**Internal Certificate Authority**

**Key type**   
  
 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**   
 The digest method used when the CA is signed.  
 The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

**Lifetime (days)**

**Common Name**

The following certificate authority subject components are optional and may be left blank.

**Country Code**

- Mettre la bonne localisation du Pfsense indiquer dans le certificat sinon des problèmes d'identification peuvent survenir. Dans System > General Setup > Localisation :

**Localization**

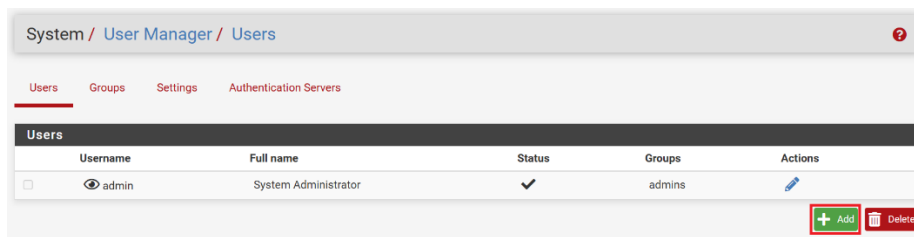
**Timezone**   
 Select a geographic region name (Continent/Location) to determine the timezone for the firewall.  
 Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.

**Timeservers**   
 Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!

**Language**   
 Choose a language for the webConfigurator

## 2. Création des utilisateurs

- Dans System > User Manager > Users > Add :



- Renseigner les informations et joindre le certificat comme ci-dessous :

### 3. Création du serveur OpenVPN

- Dans Menu VPN > OpenVPN > Wizards puis sélectionner « Local User Access » :

- Sélectionner le certificat créer « VPN Server CA » :

- Créer un nouveau certificat :

Step 7 of 11

### Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

### Choose a Server Certificate

Certificate: GUI default (67600011c04a2) ▼

» Add new Certificate
» Next

Step 8 of 11

### User Properties

### Add a Server Certificate

OpenVPN Remote Access Server Setup Wizard

### Create a New Server Certificate

Descriptive name: CertifOpenVPNprincipal  
A name for administrative reference, to identify this certificate.

Key length: 2048 bit ▼  
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see [keylength.com](http://keylength.com)

Lifetime: 398  
Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name:   
The internal name of the server certificate, used as a part of the certificate subject. Typically set to the hostname of this system. This value is also used as a Subject Alternative Name (SAN). If left blank, the Descriptive Name value will be used for the Common Name and SAN instead.

Country Code: FR  
Two-letter ISO country code (e.g. US, AU, CA)

State or Province: France  
Full State of Province name, not abbreviated (e.g. Texas, Indiana, Ontario).

City:   
City or other Locality name (e.g. Austin, Indianapolis, Toronto).

Organization:   
Organization name, often the company or group name.

Organizational Unit:   
Organizational Unit name, often a department or team name.

» Create new Certificate

- Configurer le tunnel :
  - Dans « IPv4 Tunnel Network » mettre le réseau du VPN dont le PC distant (le poste Windows Client Home) fera partie : 10.10.11.0/24
  - Dans « IPv4 Local Network » mettre le réseau du VPN dont le PC distant fera partie : 10.10.10.0/24

### Tunnel Settings

IPv4 Tunnel Network: 10.10.11.0/24  
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

Redirect IPv4 Gateway: ☐ Force all client generated traffic through the tunnel.

IPv4 Local Network: 10.10.10.0/24  
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. 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.

- Dans « DNS Server 1 » mettre l'IP de l'interface LAN : 10.10.10.254

**Advanced Client Settings**

DNS Default Domain

Provide a default domain name to clients.

---

DNS Server 1

DNS server IP to provide to connecting clients.

- Cocher les 2 règles :

**Traffic from clients to server**

**Firewall Rule**

☒ Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.

---

**Traffic from clients through VPN**

**OpenVPN rule**

☒ Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

[Next](#)

- Résultat :

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

**OpenVPN Servers**

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.10.11.0/24	<b>Mode:</b> Remote Access ( SSL/TLS + User Auth ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256 <b>D-H Params:</b> 2048 bits		<a href="#">Edit</a> <a href="#">Delete</a>

[+ Add](#)

- Dans Firewall > Rules > WAN, une règle c'est créer pour OpenVPN :

Firewall / Rules / WAN

Floating WAN LAN IPsec OpenVPN

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none		<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Toggle</a> <a href="#">Copy</a> <a href="#">Save</a> <a href="#">Separator</a>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/76 KIB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none	OpenVPN wizard	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Toggle</a> <a href="#">Copy</a> <a href="#">Save</a> <a href="#">Separator</a>

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

#### 4. Installation du plugin du client OpenVPN

- Dans System > Package Manager > Available Packages :

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term open Name Search Clear

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

Packages

Name	Version	Description	
Open-VM-Tools	10.1.0_5.1	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.	+ Install
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.	+ Install

Package Dependencies:

open-vm-tools-12.3.5.2

Package Dependencies:

openvpn-client-export-2.6.7 openvpn-2.6.8\_1 zip-3.0\_1 7-zip-23.01

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

Installed Packages Available Packages Package Installer

Package Installation

```
[4/5] Installing 7-zip-23.01...
[4/5] Extracting 7-zip-23.01: ..... done
[5/5] Installing pfSense-pkg-openvpn-client-export-1.9.2...
[5/5] Extracting pfSense-pkg-openvpn-client-export-1.9.2: ..... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Writing configuration... done.
>>> Cleaning up cache... done.
Success
```

## 5. Téléchargement du client OpenVPN

- Dans OpenVPN > Client Export > OpenVPN Clients :

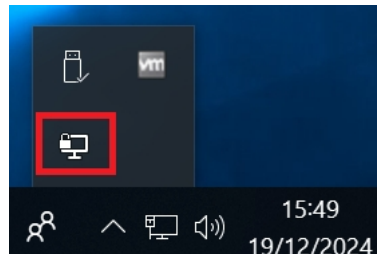
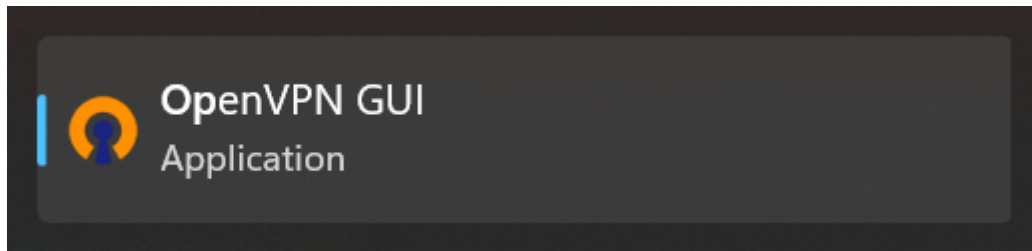
OpenVPN Clients

User	Certificate Name	Export
Alex	VPNCert	<p>- Inline Configurations:</p> <p>Most Clients Android OpenVPN Connect (iOS/Android)</p> <p>- Bundled Configurations:</p> <p>Archive Config File Only</p> <p>- Current Windows Installers (2.6.7-ix001):</p> <p>64-bit 32-bit</p> <p>- Previous Windows Installers (2.5.9-ix601):</p> <p>64-bit 32-bit</p> <p>- Legacy Windows Installers (2.4.12-ix601):</p> <p>10/2016/2019 7/8/8.1/2012/2</p> <p>- Viscosity (Mac OS X and Windows):</p> <p>Viscosity Bundle Viscosity Inline Config</p>

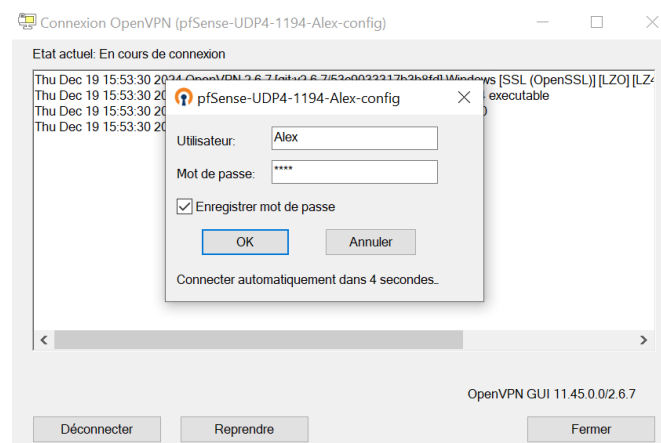
## 6. Installation et configuration du client OpenVPN

- Installer le client OpenVPN sur le poste Windows Client Home et lancer l'application avec l'icône dans la barre de notification ou le menu déroulant, puis « Connecter » :

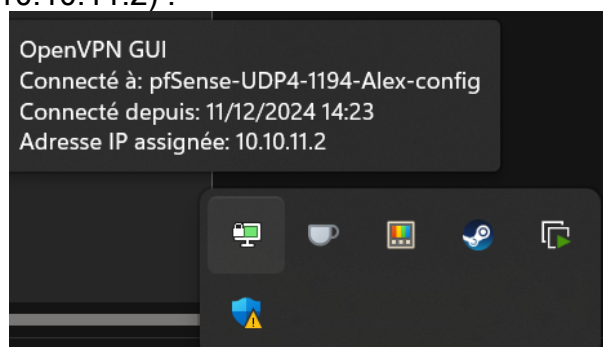




- Mettre l'identifiant et le mot de passe de l'utilisateur :



- L'icône devient verte quand le tunnel VPN est bien monter. En plaçant le curseur de la souris sur l'icône, une fenêtre d'information donnera l'IP assignée (10.10.11.2) :



## F. IPsec

### 1. Contexte

IPSEC (Internet Protocol Security) est un ensemble de protocoles standard open source de la couche 3 qui sécurise le transport des données sur un réseau à l'aide d'algorithmes et de protocoles.

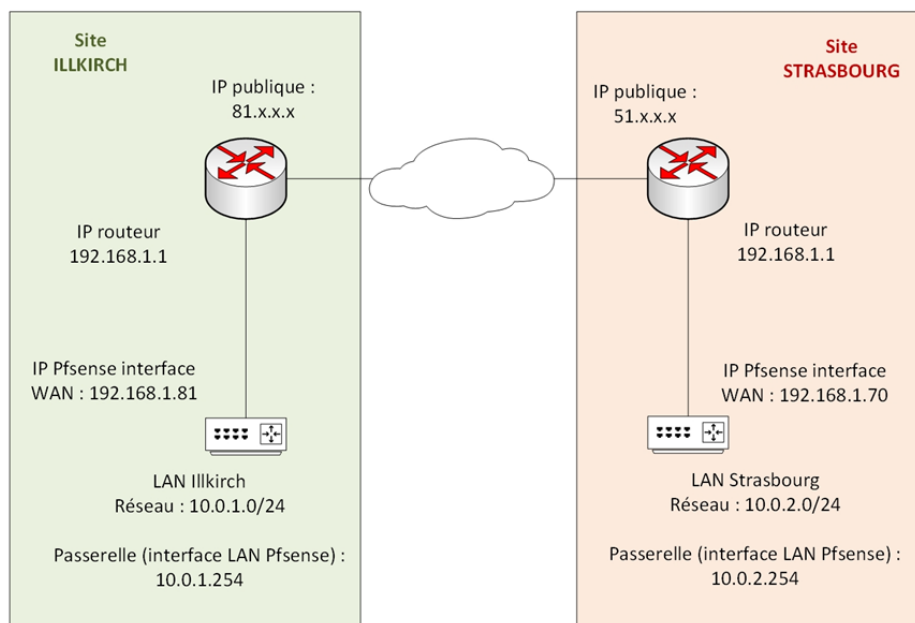
Présentation de l'architecture :

#### Réseau 1 : Illkirch

- Nom machine : PFSense\_ILLKIRCH
- Réseau LAN : 10.0.1.0/24
- IP interface LAN : 10.0.1.254
- IP publique : 81.x.x.x

#### Réseau 2 : Strasbourg

- Nom machine : PFSense\_STRASBOURG
- Réseau LAN : 10.0.2.0/24
- IP interface LAN : 10.0.2.254
- IP publique : 51.x.x.x



### 1. Configuration du VPN du site 1

Configuration du VPN d'ILLKIRCH

- Menu Pfsense : VPN > IPsec > Tunnels
  - Cliquez sur le bouton vert "Add P1" pour ajouter une première phase.
  - Information générale :
    - Key Exchange version : IKEv2
    - Protocole : IPv4
    - Interface : WAN
    - Remote gateway : l'IP publique du PFSENSE 2 DONC 10.168.1.25
    - Description : VPN vers Strasbourg

VPN / IPsec / Tunnels / Edit Phase 1

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

### General Information

**Description** VPN vers Strasbourg  
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 ID** 1

### IKE Endpoint Configuration

**Key Exchange version** IKEv2  
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** IPv4  
Select the Internet Protocol family.

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

**Remote Gateway** 192.168.1.25  
Enter the public IP address or host name of the remote gateway.

- Phase 1 proposal :
  - Authentication method : Mutual PSK
  - Negotiation mode : Agressive
  - My identifier : IP address = l'adresse IP publique de ce site (ILLKIRCH 192.168.1.24)
  - Peer identifier : IP address = l'adresse IP publique du site distant (STRASBOURG 192.168.1.25)
  - Pre-shared Key : **générez une clé et copiez la dans un fichier texte. Vous en aurez besoin pour la configuration du PFSENSE 2, de Strasbourg f78b328ae4a9d60ad29c0f94083b0478554f2b711fc90d517f5835a1**
  - Encryption : laissez tout par défaut

### Phase 1 Proposal (Authentication)

**Authentication Method** Mutual PSK  
Must match the setting chosen on the remote side.

**My identifier** IP address 192.168.1.24

**Peer identifier** IP address 192.168.1.25

**Pre-Shared Key** f78b328ae4a9d60ad29c0f94083b0478554f2b711fc90d517f5835a1  
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.  
[Generate new Pre-Shared Key](#)

- Enregistrez (bouton "Save" en bas de page)

IPsec Tunnels									
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	V2	WAN 192.168.1.25	Mutual PSK -	AES (128 bits)	SHA256	14 (2048 bit)	VPN vers Strasbourg	
<a href="#">+ Show Phase 2 Entries (0)</a>									

- Cliquez sur Show phase 2 > Add P2 :

IPsec Tunnels									
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	V2	WAN 192.168.1.25	Mutual PSK -	AES (128 bits)	SHA256	14 (2048 bit)	VPN vers Strasbourg	
	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<a href="#">+ Add P2</a>									

- Laissez tout par défaut et renseignez uniquement la partie :
  - Remote network : IP du réseau LAN distant, celui de votre PFSense 2 (dans mon cas, le LAN de Strasbourg 10.1.22.25/24)

Status / IPsec / Overview									
Overview Leases SADs SPDs									
IPsec Status									
ID	Description	Local	Remote	Role	Timers	Algo	Status		
con1	VPN vers Strasbourg	ID: 10.1.22.24 Host: 10.1.22.24	ID: 10.1.22.25 Host: 10.1.22.25				Disconnected		
							<a href="#">Connect P1 and P2s</a>		
							<a href="#">Connect P1</a>		

## 2. Configuration du VPN du site 2

### Configuration du VPN de STRASBOURG

- Menu Pfsense : VPN > IPsec > Tunnels
  - Cliquez sur le bouton vert "Add P1" pour ajouter une première phase.
  - Information générale :
    - Key Exchange version : IKEv2
    - Protocole : IPv4
    - Interface : WAN
    - Remote gateway : l'IP publique du PFSense 2 DONC 10.168.1.24
    - Description : VPN vers Illkirch
  - Phase 1 proposal :
    - Authentication method : Mutual PSK

- Negotiation mode : Aggressive
- My identifier : IP address = l'adresse IP publique de ce site (STRASBOURG 192.168.1.25)
- Peer identifier : IP address = l'adresse IP publique du site distant (ILLKIRCH 192.168.1.24)
- Pre-shared Key : **générez une clé et copiez la dans un fichier texte. Vous en aurez besoin pour la configuration du PFSENSE 2, de Strasbourg f78b328ae4a9d60ad29c0f94083b0478554f2b711fc90d517f5835a1**
- Encryption : laissez tout par défaut

General Information	
Description	VPN vers Illkirch <small>A description may be entered here for administrative reference (not parsed).</small>
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
IKE ID	1
IKE Endpoint Configuration	
Key Exchange version	IKEv2 <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</small>
Internet Protocol	IPv4 <small>Select the Internet Protocol family.</small>
Interface	WAN <small>Select the interface for the local endpoint of this phase1 entry.</small>
Remote Gateway	192.168.1.24 <small>Enter the public IP address or host name of the remote gateway.</small>
Phase 1 Proposal (Authentication)	
Authentication Method	Mutual PSK <small>Must match the setting chosen on the remote side.</small>
My identifier	IP address 192.168.1.25
Peer identifier	IP address 192.168.1.24
Pre-Shared Key	f78b328ae4a9d60ad29c0f94083b0478554f2b711fc90d517f5835a1

- Phase 2 :
  - Remote network : IP du réseau LAN distant, celui de votre PFSENSE 1 (dans mon cas, le LAN d'ILLKIRCH 10.1.22.24)

### 3. Configuration du pare-feu et redirections de ports

- Par défaut, Pfsense a ajouté la règle suivante :
  - Interface : IPsec
  - Protocole : IPv4 TCP
  - Source / destination : any

Firewall / Rules / IPsec

The changes have been applied successfully. The firewall rules are now reloading in the background.  
[Monitor the filter reload progress.](#)

Floating WAN LAN IPsec OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	*	*	*	*	*	none			

Add 
 Add 
 Delete 
 Toggle 
 Copy 
 Save 
 Separator

- Modifiez cette règle pour autoriser tous les protocoles :

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	*	*	*	*	*	none			

- Les règles de pare-feu pour le LAN devraient être les suivantes :

Firewall / Rules / LAN

Floating WAN LAN IPsec OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/16.77 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
0/2 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

#### 4. Configuration la redirection de port des routeurs

Pour finir, vous devez ouvrir et rediriger les ports nécessaires à IPsec sur vos routeurs.

Les ports sont les suivants :

- Protocol: UDP, port 500 (IKE, pour gérer les clés de chiffrement)
- Protocol: UDP, port 4500 (IPSEC NAT-Traversal mode)
- Protocol: ESP, value 50 (IPSEC)

#### 5. Test du VPN

- Status > IPsec > Overview > Connect VPN :

Status / IPsec / Overview

Overview Leases SADs SPDs

### IPsec Status

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #1	VPN vers Strasbourg	ID: 192.168.1.24 Host: 192.168.1.24:500 SPI: b1b83457dc357363	ID: 192.168.1.25 Host: 192.168.1.25:500 SPI: c0494a94a74f71c0	IKEv2 Initiator	Rekey: 24121s (06:42:01) Reauth: Disabled	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established 8 seconds (00:00:08) ago <a href="#">Disconnect P1</a>

Show child SA entries (1 Connected)

- Si le tunnel VPN s'est monté, le status devient "ESTABLISHED".

## 6. Valider le fonctionnement du VPN

Pour tester que votre VPN fonctionne, vous pouvez utiliser l'outil de PING intégré à Pfsense :

- Diagnostics > Ping
  - Renseignez l'IP de l'interface LAN du site distant
  - Testez depuis le Pfsense 2 (interface LAN 10.10.10.254) pour essayer d'accéder à l'interface LAN du Pfsense 1 (10.0.1.254)

Diagnostics / Ping

### Ping

Hostname: 10.10.10.254

IP Protocol: IPv4

Source address: LAN  
Select source address for the ping.

Maximum number of pings: 3  
Select the maximum number of pings.

Seconds between pings: 1  
Select the number of seconds to wait between pings.

[Ping](#)

### Results

```
PING 10.10.10.254 (10.10.10.254) from 10.0.1.254: 56 data bytes
64 bytes from 10.10.10.254: icmp_seq=0 ttl=64 time=2.155 ms
64 bytes from 10.10.10.254: icmp_seq=1 ttl=64 time=1.697 ms
64 bytes from 10.10.10.254: icmp_seq=2 ttl=64 time=2.036 ms

--- 10.10.10.254 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.697/1.963/2.155/0.194 ms
```

- Testez depuis le Pfsense 1 (10.0.1.254) vers Pfsense 2 (interface LAN 10.10.10.254) :

Ping

Hostname

10.0.1.254

IP Protocol

IPv4

Source address

LAN

Select source address for the ping.

Maximum number of pings


3

Select the maximum number of pings.

Seconds between pings

1

Select the number of seconds to wait between pings.

 Ping

Results

PING 10.0.1.254 (10.0.1.254) from 10.10.10.254: 56 data bytes  
64 bytes from 10.0.1.254: icmp\_seq=0 ttl=64 time=2.420 ms  
64 bytes from 10.0.1.254: icmp\_seq=1 ttl=64 time=3.721 ms  
64 bytes from 10.0.1.254: icmp\_seq=2 ttl=64 time=1.857 ms  
  
--- 10.0.1.254 ping statistics ---  
3 packets transmitted, 3 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 1.857/2.666/3.721/0.781 ms