

Chéridanh TSIELA

Pfsense

VPN Site to Site IPsec

I – Introduction

PfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.

IPSec est un ensemble de règles ou de protocoles de communication permettant d'établir des connexions sécurisées sur un réseau. Le protocole Internet (IP) est la norme commune qui détermine comment les données circulent sur Internet. IPSec ajoute le chiffrement et l'authentification pour rendre le protocole plus sûr. Par exemple, il chiffre les données à la source et les déchiffre à la destination. Il authentifie également la source des données.

II – Prérequis

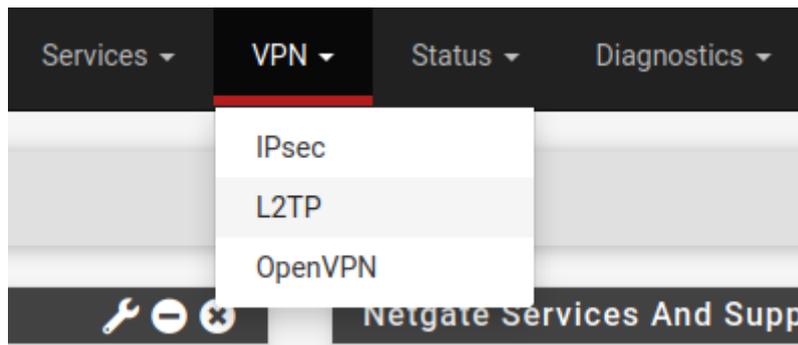
- Deux routeurs Pfsense
- Mot de passe admin des firewalls

II – Prérequis

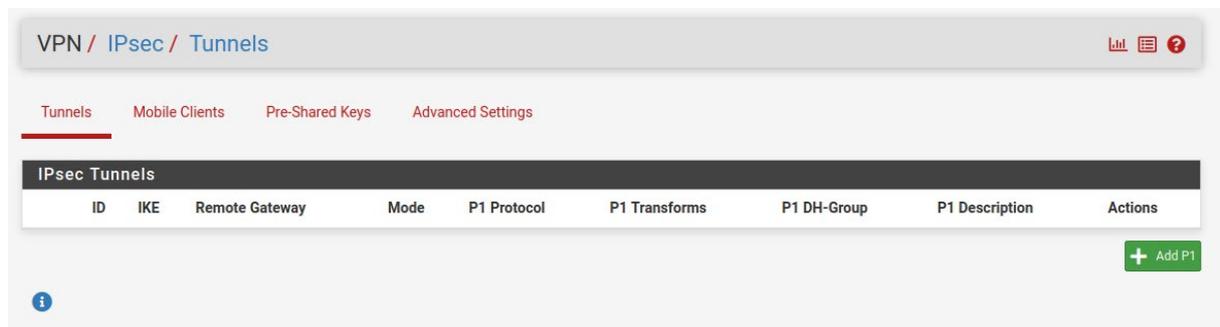
Dans ce TP nous disposons de deux routeurs

Sites	WAN	LAN
Pfsense 1	192.168.91.132/24	192.168.100.0/24
Pfsense 2	192.168.91.133/24	192.168.200.0/24

Pour configurer notre connexion VPN avec IPsec il faudra se rendre le menu « **VPN => IPsec** »

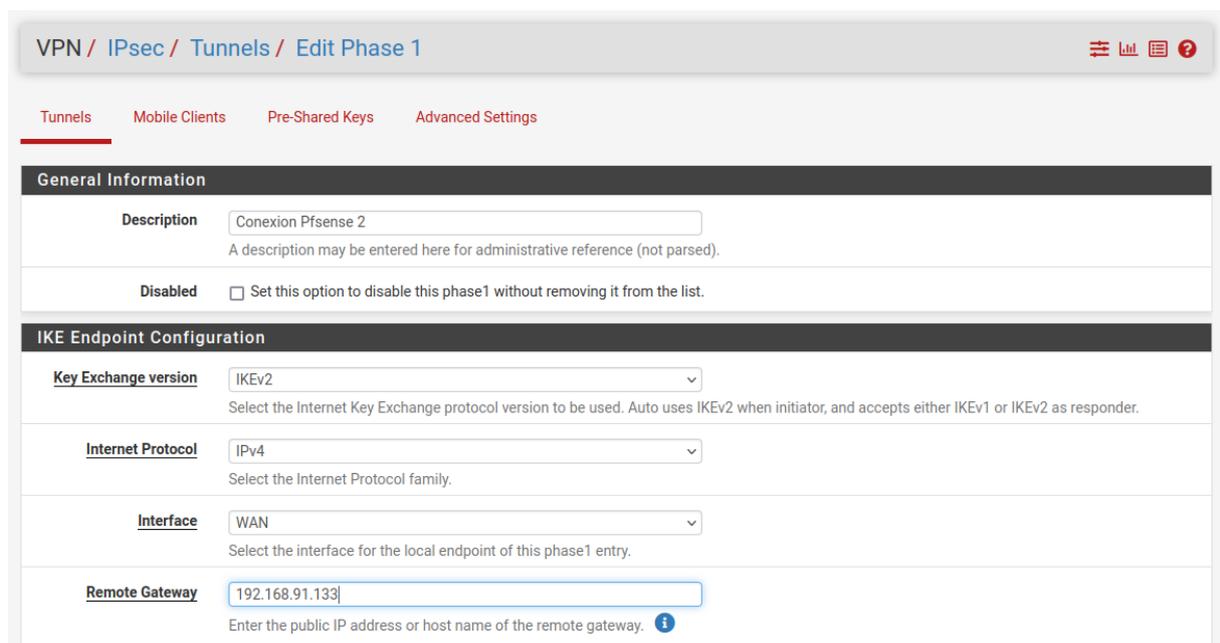


Une fois dans l'interface de VPN cliquez sur « Add P1 »



Dans le routeur Pfsense 1 (Site A)

- **Description** : Connexion vers Site B
- **Remote Gateway** : 192.168.91.133 (Wan Pfsense 2)
- **Pre-shared Key** : cheridanh.cg
- **Encryption Algorithm** : AES256-GCM



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
 Algorithm Key length Hash DH Group

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

Add Algorithm

Laissez tout le reste par défaut, cliquez sur « **Save** » puis sur « **Apply changes** »

VPN / IPsec / Tunnels ▶ ⌵ ⌶ ?

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The IPsec tunnel configuration has been changed. The changes must be applied for them to take effect.

IPsec Tunnels

	ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> <input type="button" value="🔗"/>	1	V2	WAN 192.168.91.133		AES256-GCM (128 bits)	SHA256	14 (2048 bit)	Conexion PfSense 2	<input type="button" value="🔗"/> <input type="button" value="🗑️"/>

De nouveau sur cette page, cliquez sur « **Show Phase 2 Entries** » puis cliquez sur « **Add P2** »

VPN / IPsec / Tunnels ↻ ⌵ ⌶ ?

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The changes have been applied successfully. ✕

IPsec Tunnels

	ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> <input type="button" value="🔗"/>	1	V2	WAN 192.168.91.133		AES256-GCM (128 bits)	SHA256	14 (2048 bit)	Conexion PfSense 2	<input type="button" value="🔗"/> <input type="button" value="🗑️"/>

	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="button" value="+ Add P2"/>									

Renseignez les champs suivants :

- **Description** : LAN Pfsense 2
- **Remote** : Network
- **Adress** : 192.168.200.0
- **Encryption Algorithm** : AES256-GCM
- **Automatically ping host** : 192.168.200.254

Tunnels Mobile Clients Pre-Shared Keys **Advanced Settings**

General Information

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

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

Mode

Phase 1

Networks

Local Network /
Type Address
Local network component of this IPsec security association.

NAT/BINAT translation /
Type Address
If NAT/BINAT is required on this network specify the address to be translated

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

Phase 2 Proposal (SA/Key Exchange)

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

Encryption Algorithms

<input type="checkbox"/> AES	<input type="text" value="128 bits"/>
<input type="checkbox"/> AES128-GCM	<input type="text" value="128 bits"/>
<input type="checkbox"/> AES192-GCM	<input type="text" value="Auto"/>
<input checked="" type="checkbox"/> AES256-GCM	<input type="text" value="128 bits"/>
<input type="checkbox"/> CHACHA20-POLY1305	

Hash Algorithms SHA1 SHA256 SHA384 SHA512 AES-XCBC
Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

PFS key group
Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Keep Alive

Automatically ping host
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 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.

Il faudra faire de même sur dans le routeur Pfense 2 en renseignant cette fois les informations concernant le réseau de la Pfsense 1.

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

The changes have been applied successfully.

IPsec Tunnels									
ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions	
<input type="checkbox"/> Anchor Disable	1	V2	WAN	192.168.91.132	AES256-GCM (128 bits)	SHA256	14 (2048 bit)	Connexion Pfsense 1	Edit Copy Delete

ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="checkbox"/> Anchor Disable	1	tunnel	LAN	192.168.100.0/24	ESP	AES256-GCM (128 bits)	LAN Pfsense 1	Edit Copy Delete

[+ Add P2](#)

[+ Add P1](#) [Delete P1s](#)

Rendez-vous dans l'onglet « Firewall » puis « Rules »

Interfaces Firewall Services

Aliases

NAT

Rules

Schedules

Rendez-vous dans l'onglet « IPsec » cliquez sur « Add »

Adaptez la règle selon vos besoins et cliquez sur « Save »

Floating WAN LAN IPsec

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IP4 TCP	*	*	*	*	*	none		Add Add Delete Toggle Copy Save Separator

A ce stade, notre connexion devrait être déjà établie entre nos deux Pfsenses.

Pour vérifier la connexion rendez-vous dans le menu « **Status => IPsec** »

Dans notre cas, on peut voir que la connexion s'est effectuée sans problème dans nos 2 Pfsenses.

The screenshot shows the Mikrotik WinBox interface for IPsec status. The breadcrumb is 'Status / IPsec / Overview'. There are tabs for 'Overview', 'Leases', 'SADs', and 'SPDs'. The 'Overview' tab is active. Below the tabs is a table titled 'IPsec Status' with columns: ID, Description, Local, Remote, Role, Timers, Algo, and Status. One entry is shown: ID 'con1 #1', Description 'Connexion Pfsense 2', Local ID '192.168.91.132', Local Host '192.168.91.132:500', Local SPI '0f950b53913daed4', Remote ID '192.168.91.133', Remote Host '192.168.91.133:500', Remote SPI '21498423fc67994b', Role 'IKEv2 Initiator', Timers 'Rekey: 23190s (06:26:30), Reauth: Disabled', Algo 'AES_GCM_16 (256), PRF_HMAC_SHA2_256, MODP_2048', and Status 'Established 1335 seconds (00:22:15) ago'. A 'Disconnect P1' button is visible. Below the table is a button 'Show child SA entries (1 Connected)' and an information icon.

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #1	Connexion Pfsense 2	ID: 192.168.91.132 Host: 192.168.91.132:500 SPI: 0f950b53913daed4	ID: 192.168.91.133 Host: 192.168.91.133:500 SPI: 21498423fc67994b	IKEv2 Initiator	Rekey: 23190s (06:26:30) Reauth: Disabled	AES_GCM_16 (256) PRF_HMAC_SHA2_256 MODP_2048	Established 1335 seconds (00:22:15) ago

The screenshot shows the Mikrotik WinBox interface for IPsec status. The breadcrumb is 'Status / IPsec / Overview'. There are tabs for 'Overview', 'Leases', 'SADs', and 'SPDs'. The 'Overview' tab is active. Below the tabs is a table titled 'IPsec Status' with columns: ID, Description, Local, Remote, Role, Timers, Algo, and Status. One entry is shown: ID 'con1 #1', Description 'Connexion Pfsense 1', Local ID '192.168.91.133', Local Host '192.168.91.133:500', Local SPI '21498423fc67994b', Remote ID '192.168.91.132', Remote Host '192.168.91.132:500', Remote SPI '0f950b53913daed4', Role 'IKEv2 Responder', Timers 'Rekey: 21584s (05:59:44), Reauth: Disabled', Algo 'AES_GCM_16 (256), PRF_HMAC_SHA2_256, MODP_2048', and Status 'Established 1504 seconds (00:25:04) ago'. A 'Disconnect P1' button is visible. Below the table is a button 'Show child SA entries (1 Connected)' and an information icon.

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #1	Connexion Pfsense 1	ID: 192.168.91.133 Host: 192.168.91.133:500 SPI: 21498423fc67994b	ID: 192.168.91.132 Host: 192.168.91.132:500 SPI: 0f950b53913daed4	IKEv2 Responder	Rekey: 21584s (05:59:44) Reauth: Disabled	AES_GCM_16 (256) PRF_HMAC_SHA2_256 MODP_2048	Established 1504 seconds (00:25:04) ago

C'est la fin de ce TP ! Merci d'avoir suivi jusqu'au bout !

Liens utiles :

<https://docs.netgate.com/pfsense/en/latest/>

<https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-psk.html>

Chéridanh TSIELA

N'hésitez pas à me laisser un message sur mon site :

<https://cheridanh.cg/about>