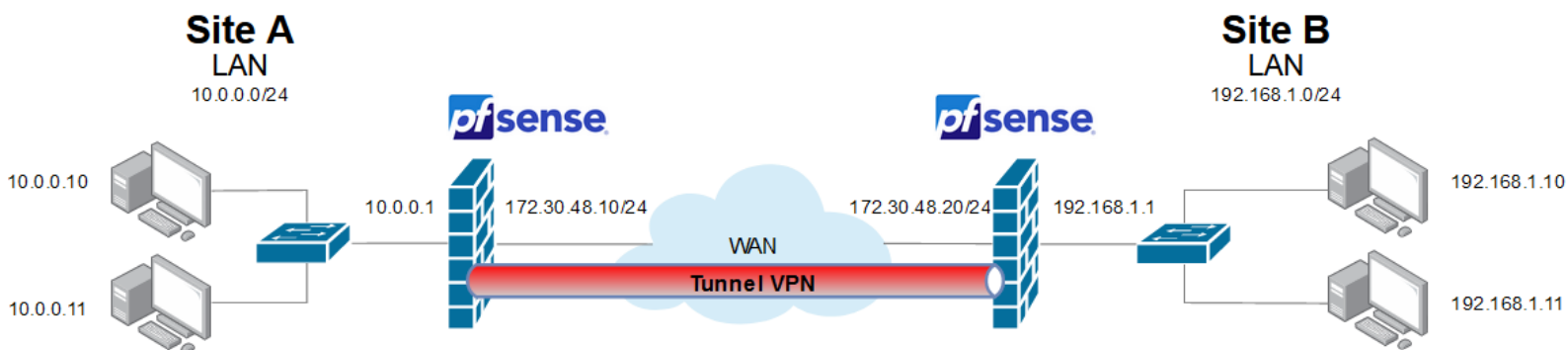


Mise en place d'un tunnel VPN IPsec avec Pfsense



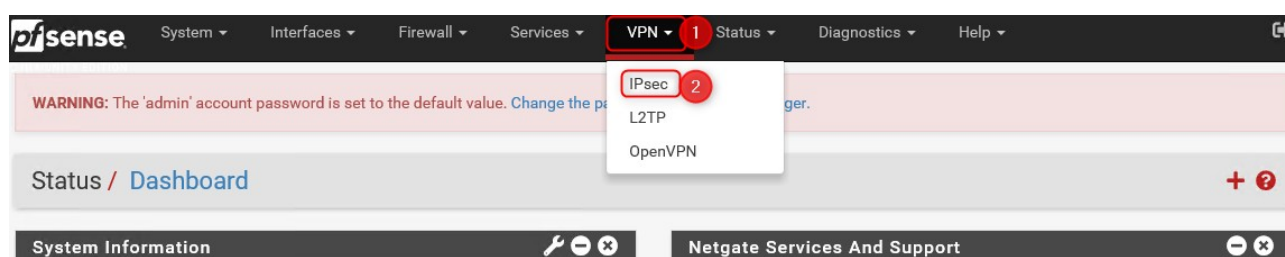
Prérequis :

Deux machines virtuelles Pfsense doivent être installées et configurées avec le plan d'adressage représenté sur le schéma. (Les adresses WAN peuvent être différentes suivant votre virtualisation mais statiques et ajoutez bien l'IPv4 Upstream gateway)

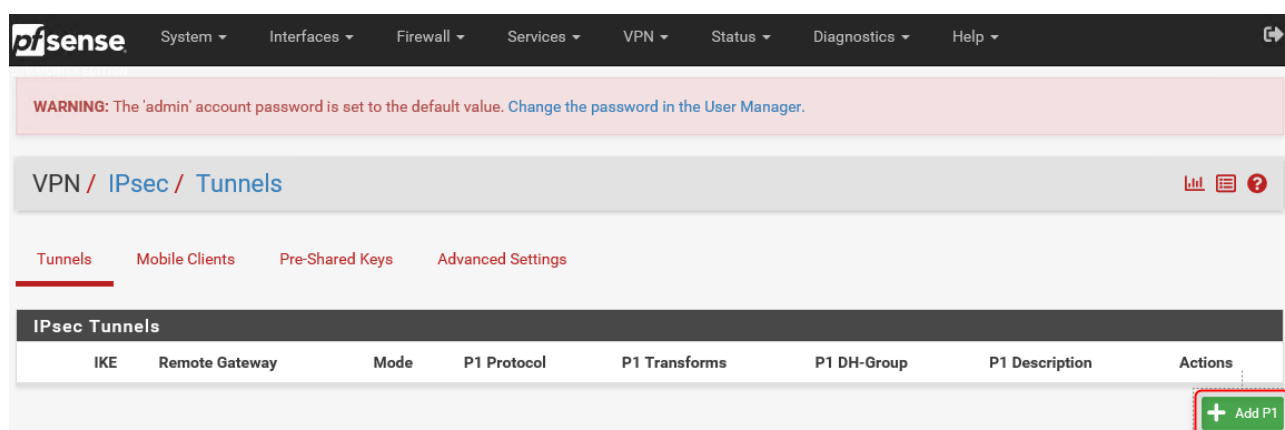
Pour les site A et B, au choix, vous pouvez installer des VM win10 ou Linux

Mise en Oeuvre :

Configurez le Pfsense du site A, allez dans VPN puis IPsec



cliquez sur **Add P1** pour créer la Phase 1



Dans le champ Remote Gateway, indiquez l'adresse IP WAN du Pfsense du site B.

Vous pouvez également entrer une description.

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

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

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 172.30.48.20
Enter the public IP address or host name of the remote gateway. ⓘ

Description Connexion VPN Site to Site - to Site B X
A description may be entered here for administrative reference (not parsed).

Dans la partie suivante, les pfsense utiliseront leur adresse IP comme identifiant.

Nous utiliserons la clé pré-partagée, générez-en une

Vous pouvez changer le type d'algorithme de chiffrement et les longueurs de clés.

Et laisser les autres valeurs par défaut. Sauvegardez et appliquez

Phase 1 Proposal (Authentication)

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

My identifier My IP address

Peer identifier Peer IP address

Pre-Shared Key 92c1b66e52f334c253c88c27809032dc4acb654143836fec3e03d41a
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](#)

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm AES
Algorithm

Key length 256 bits

Hash SHA256

DH Group 14 (2048 bit) [Delete](#)

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 [+ Add Algorithm](#)

Passez à la phase 2

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

IPsec Tunnels

	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
  Disable	V2	WAN 172.30.48.20		AES (256 bits)	SHA256	14 (2048 bit)	Connexion VPN Site to Site - to Site B	  
➕ Show Phase 2 Entries (0)								

➕ Add P1 🗑 Delete P1s

et cliquez sur **Add P2**

Définissiez le réseau LAN distant

General Information

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

Mode Tunnel IPv4

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 192.168.1.0 / 24
Type Address
Remote network component of this IPsec security association.

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

Choisissez le protocole ESP et un chiffrement AES 256 bits

Phase 2 Proposal (SA/Key Exchange)

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

Encryption Algorithms

<input checked="" type="checkbox"/> AES	256 bits
<input checked="" type="checkbox"/> AES128-GCM	128 bits
<input type="checkbox"/> AES192-GCM	Auto
<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.

Laissez les autres valeurs par défaut.

Sauvegardez et appliquez les changements

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

	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> Disable	V2	WAN 172.30.48.20		AES (256 bits)	SHA256	14 (2048 bit)	Connexion VPN Site to Site - to Site B	

[Show Phase 2 Entries \(1\)](#)

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

Faites ensuite la même configuration sur le firewall pfense du site B en adaptant les adresses IP. Activez les règles de pare-feu afin de permettre au trafic de passer dans le tunnel VPN de monter

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**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4 *	*	*	*	*	none			Anchor Edit Copy Refresh Delete

[↑ Add](#) [↓ Add](#) [Delete](#) [Save](#) [+ Separator](#)

Allez dans le menu **Status/Ipsec** afin de voir l'état du tunnel VPN.

Cliquez sur connect VPN , vous devez avoir cela

Status / IPsec / Overview

Overview Leases SADs SPDs

IPsec Status

IPsec ID	Description	Local	Remote	Role	Timers	Algo	Status
con100000: #1	connexion VPN site to site to site A	ID: 172.30.48.20 Host: 172.30.48.20:500 SPI: dc5a298f7041a34c	ID: 172.30.48.10 Host: 172.30.48.10:500 SPI: 586d2e0fa73968be	IKEv2 initiator	Rekey: 24211s (06:43:31) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	ESTABLISHED 41 seconds (00:00:41) ago Disconnect

[+ Show child SA entries \(1\)](#)

[i](#)

Vous pouvez vérifier également que les associations de sécurité sont bien opérationnelles :

Status / IPsec / SADs						
Overview	Leases	SADs	SPDs			
Source	Destination	Protocol	SPI	Enc. alg.	Auth. alg.	Data
172.30.48.20	172.30.48.10	ESP	cf8509e0	aes-gcm-16		3364 B
172.30.48.10	172.30.48.20	ESP	cbd0d947	aes-gcm-16		0 B

Vous devriez être capable de pinger la machine du site B à partir du site A

Si cela ne fonctionne pas, commencez le troubleshooting. Voir le status des services, Pinger de proche en proche, vérifiez la configuration etc..