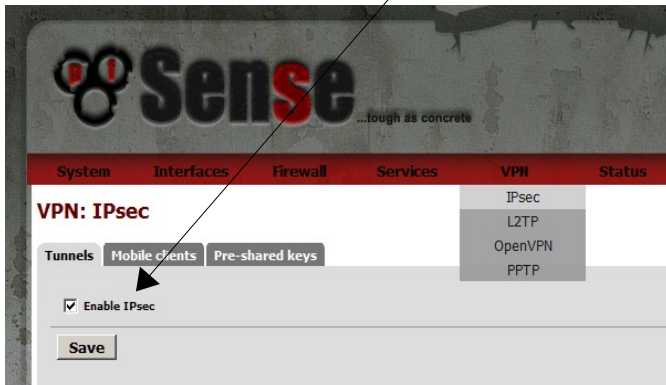



**PROCÉDURE DE CRÉATION
D'UN TUNNEL VPN IPSEC
ENTRE PFSENSE 2.0 ET IPCOP 1.4.21
AVEC IDENTIFICATION DE CLÉ PARTAGÉE**

Configuration PfSense :

- Aller dans le menu VPN → IPsec
- Cocher la case Enable IPsec puis sur Save



- Ajouter une liaison en cliquant sur 

- Renseigner les champs comme suit :

VPN: IPsec: Edit Phase 1

Tunnels Mobile clients Pre-shared keys

General information

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

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

Description
You may enter a description here for your reference (not parsed).

L'interface pour rejoindre l'hôte distant

Adresse IP ou nom de l'hôte distante

Phase 1 proposal (Authentication)

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

Negotiation mode
Aggressive is more flexible, but less secure.

My identifier

Peer identifier

Pre-Shared Key
Input your pre-shared key string.

Proposal Checking
Specifies the action of lifetime length, key length, and PFS of the action of lifetime check in phase 1.

Encryption algorithm
Must match the setting chosen on the remote side.

Hash algorithm
Must match the setting chosen on the remote side.

DH key group
1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit
Must match the setting chosen on the remote side.

Lifetime seconds

Méthode d'identification, ici par clé partagée

Méthode de négociation (agressive mode transmet la clé en clair)

Clé partagée, doit être identique sur l'IPcop (ici très simplifiée)

Algorithme de cryptage (doit être le même sur l'IPcop)

Algorithme vérifiant l'intégrité des données

Advanced Options

NAT Traversal Disable
Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) for clients that are behind restrictive firewalls.

Dead Peer Detection ☒ Enable DPD
 Delay between requesting peer acknowledgement: 10 seconds
 Number of consecutive failures allowed before disconnect: 5 retries

Save

- Cliquer sur Save et appliquer les changements

VPN: IPsec S L ?

The IPsec tunnel configuration has been changed. You must apply the changes in order for them to take effect. **Apply changes**

Tunnels **Mobile clients** Pre-shared keys

☒ Enable IPsec

Save

Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
WAN xxx.xxx.xxx.xxx	main	Blowfish (256 bits)	MD5	Tunnel Test <-> Relais 62

- Cliquer sur le +

xxx.xxx.xxx.xxx

+ - Show 1 Phase-2 entries

- Cliquer sur le +

Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods

- Renseigner les champs comme suit :

VPN: IPsec: Edit Phase 2

Tunnels **Mobile clients** Pre-shared keys

Disabled ☐ Disable this phase2 entry
Set this option to disable this phase2 entry without removing it from the list

Mode Tunnel

Local Network Type: LAN subnet Address: / 0

Remote Network Type: Network Address: 192.168.0.0 / 24

Description
You may enter a description here for your reference (not parsed).

Réseau Local

Réseau distant

Phase 2 proposal (SA/Key Exchange)

Protocol ESP ESP is encryption, AH is authentication only ← Choisir ESP

Encryption algorithms

☐ AES auto

☒ Blowfish 256 bits ← Encryption Blowfish

☐ 3DES

☐ CAST128

☐ DES

Hint: use 3DES for best compatibility or if you have a hardware crypto accelerator in software encryption.

Hash algorithms

☒ SHA1 ← SHA1 et MD5

☒ MD5

PFS key group 5 ← PFS key group 5 (1536b)

1 = 768 bit, 2 = 1024 bit, 5 = 1536 bit

Lifetime 28800 seconds

Advanced Options

Automatically ping host IP address

Save

- Cliquer sur Save et appliquer les changements

- Cliquer ensuite si besoin sur l'onglet Mobile clients puis cocher Enable IPsec Mobile Client Support

Tunnels **Mobile clients** **Pre-shared keys**

IKE Extensions ☒ Enable IPsec Mobile Client Support

Extended Authentication (Xauth)

User Authentication Source: system

Group Authentication Source: system

Client Configuration (mode-cfg)

Virtual Address Pool ☐ Provide a virtual IP address to clients

Network: / 24

Network List ☐ Provide a list of accessible networks to clients

Save Xauth Password ☐ Allow clients to save Xauth passwords (Cisco VPN client only).
NOTE: With iPhone clients, this does not work when deployed via the iPhone conf

DNS Default Domain ☐ Provide a default domain name to clients

DNS Servers ☐ Provide a DNS server list to clients

Server #1:

Server #2:

Server #3:

Server #4:

WINS Servers ☐ Provide a WINS server list to clients

Server #1:

Server #2:

Phase2 PFS Group ☒ Provide the Phase2 PFS group to clients (overrides all mobile phase2 settings) ← Cocher et choisir 5

Group: 5

Phase 2 PFS Group

Cocher et choisir 5

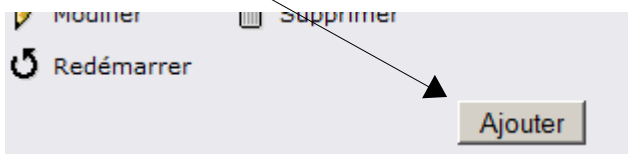
- cliquer sur Save et appliquer les changements

Configuration IPcop :

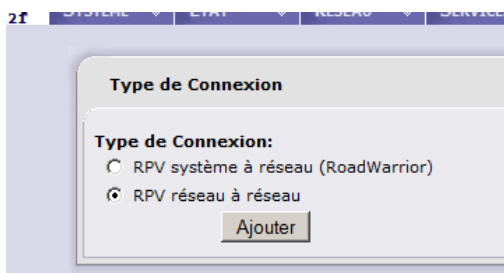
- Aller dans RPVs → RPVs



- Cliquer sur ajouter



- Choisir RPV réseau à réseau puis cliquer sur Ajouter



- Renseigner les champs comme suit :

The screenshot shows the 'Connexion:' form in the IPcop web interface. The form contains the following fields and values:

- Nom: lereleistest
- Activé: ☒
- Adresse IP de la machine: RED (xxx.xxx.xxx.xxx)
- Sous-réseau local: 192.168.0.0/255.255.255.0
- ID Locale: (câd : @xy.example.com)
- Action quand le 'pair' disparaît: restart 2
- Remarque:
- Serveur/IP distant: xxxxxxxx t.dyndns.org
- Sous-réseau distant: 192.168.30.0/255.255.255.0
- ID Distant:

L'interface pour rejoindre l'hôte distant

Adresse du réseau privé local et son masque de sous réseau

Adresse fixe ou dynamique du serveur PfSense

Adresse du réseau privé distant et son masque de sous réseau

- Cliquer sur Poursuivre avec la configuration avancée

☒ Poursuivre avec la configuration avancée.

- Choisir Utiliser une clé partagée (PSK) et renseigner le champs par la même clé insérée dans Pfsense

☐ Poursuivre avec la configuration avancée.

Authentification :

☒ Utiliser une clé partagée (PSK) :

☐ Transférer une demande de certificat :

☐ Transférer un certificat

Parc

- Cliquer sur Enregistrer
- Renseigner les champs comme suit :

Avancé:

Encryptage IKE :
 Durée de vie IKE : heures

Encryptage ESP :
 Durée de vie de la clé ESP : heures

Intégrité IKE :
 Intégrité ESP :
 MD5

Grouptype IKE :
 MODP-2048
 MODP-1536
 MODP-1024

Grouptype ESP :

☐ IKE+ESP: Utilisez seulement les paramètres proposés.
☐ Autorise la négociation IKE 'aggressive mode'. A éviter dans la mesure du possible (clé transmise en clair).
☒ Perfect Forward Secrecy (PFS)
☐ Compression du payload si possible

Enregistrer
 Annuler

Encryptage IKE :

Blowfish 256 bit

MD5

MODP-1536

Durée de vie IKE : 1

Encryptage ESP :

Blowfish 256 bit

SHA1

MD5

MODP-1536

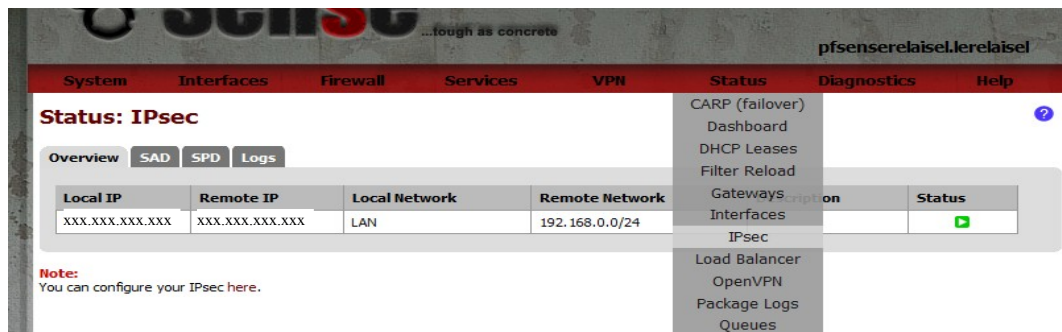
Durée de vie la clé ESP : 8

- Cliquer ensuite sur Enregistrer
- Le statut du VPN va apparaître en OUVERT dans quelques instants

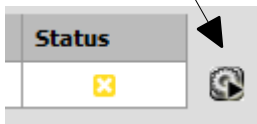
Statut VPN sur l'IPcop :

lerelaistest	Réseau (Clé partagée (PSK))	192.168.0.0/255.255.255.0 xxx.xxx.xxx.xxx [dyndns.org] 192.168.30.0/255.255.255.0	OUVERT
lerelaistest	Réseau (Certificat)	lerelaistest en le relais	FERMÉ

Statut VPN sur le PfSense :



- Dans le cas où la connexion ne se fait pas automatiquement aller dans Status → IPsec et cliquer sur l'icône connecter sur le PfSense



Synoptique :

