Mise en place IPsec L2TP entre deux Pfsense

Introduction

Pour résumer Ipsec va permettre de chiffrer les données avant de les envoyer dans le tunnel qui sera mis en place par L2TP.

Avec cette forme de vpn nous avons deux phase :

La sécurité IPSec est divisée en deux phases. La première phase est la phase de négociation de la sécurité, qui établit une connexion sécurisée entre les deux extrémités d'une communication VPN. La deuxième phase est la phase de transfert de données, qui permet le transfert de données chiffrées entre les deux extrémités [1].

La phase 1 de IPSec est utilisée pour établir une connexion sécurisée entre les deux extrémités d'une communication VPN. Elle utilise le protocole IKE (Internet Key Exchange) pour négocier les paramètres de sécurité nécessaires à la communication

L2TP est un protocole de tunneling qui permet de créer un tunnel sécurisé entre deux réseaux. Il est souvent utilisé en combinaison avec IPSec pour fournir une sécurité supplémentaire

La phase 2 de IPSec est utilisée pour transférer des données chiffrées entre les deux extrémités d'une communication VPN. Elle utilise le protocole ESP (Encapsulating Security Payload) pour chiffrer les données en transit

En résumé, la phase 1 de IPSec est utilisée pour établir une connexion sécurisée entre les deux extrémités d'une communication VPN, tandis que la phase 2 est utilisée pour transférer des données chiffrées entre les deux extrémités. L2TP est souvent utilisé en combinaison avec IPSec pour fournir une sécurité supplémentaire

Topologie

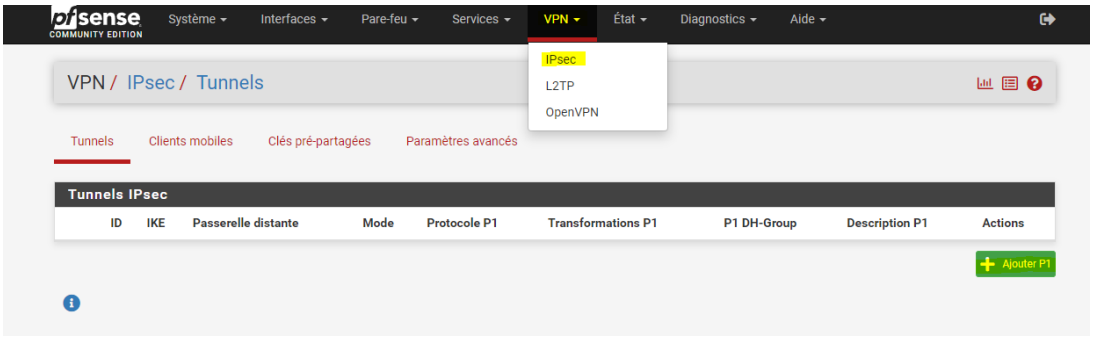
Les deux firewall sur leur pates WAN sont dans le même réseau 10.0.0.0/24

WAN PPFSENSE 1 : 10.0.0.253, LAN : 172.16.0.0 /24 WAN PFSENSE 2 : 10.0.0.254, LAN : 172.20.0.0 /24

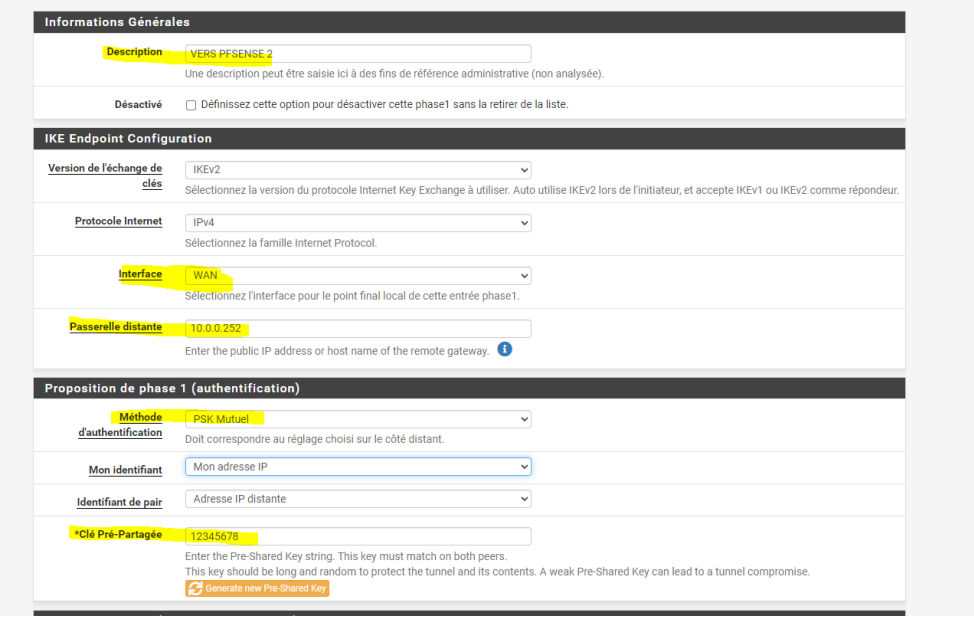
Objectif pour notre labo créer un VPN ipsec entre les deux pfsense pour faire communiquer nos deux LAN de manière transparente.

Activation IPSEC + phase 1

On se rend directement dans le menu "VPN" puis dans "IPsec" :



Ensuite on clique sur ajouter P1

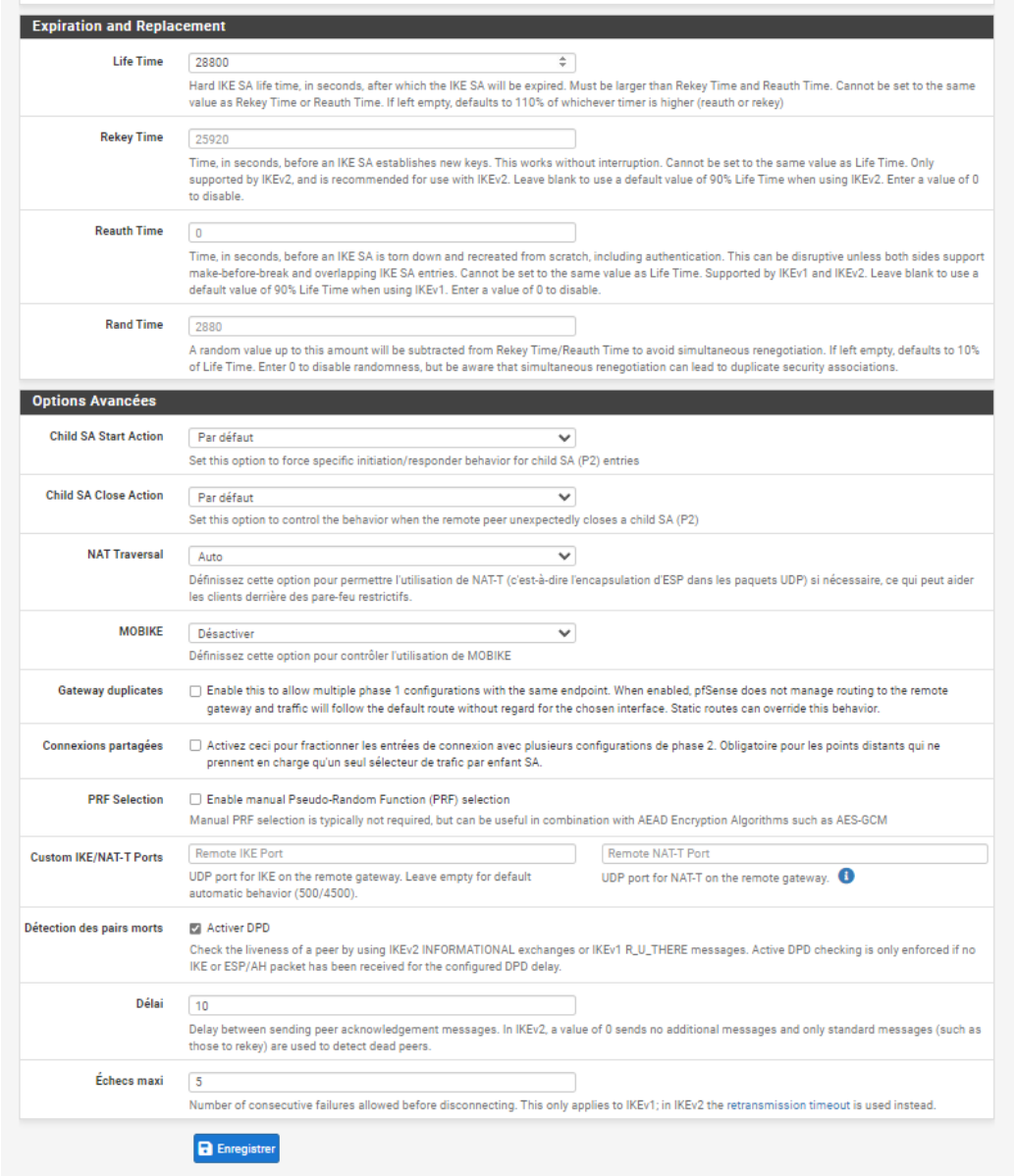


Du coup on a pas beaucoup de choses à modifier au niveau des algorithmes laissez par défaut car ipsec est très sensible.

Je définis quel interface je vais utiliser pour communiquer avec l'autre pare-feu je renseigne ensuite son IP.

Et je choisis une authentification via clé pré partagé je mets un mot de passe simple pour l'exercie !

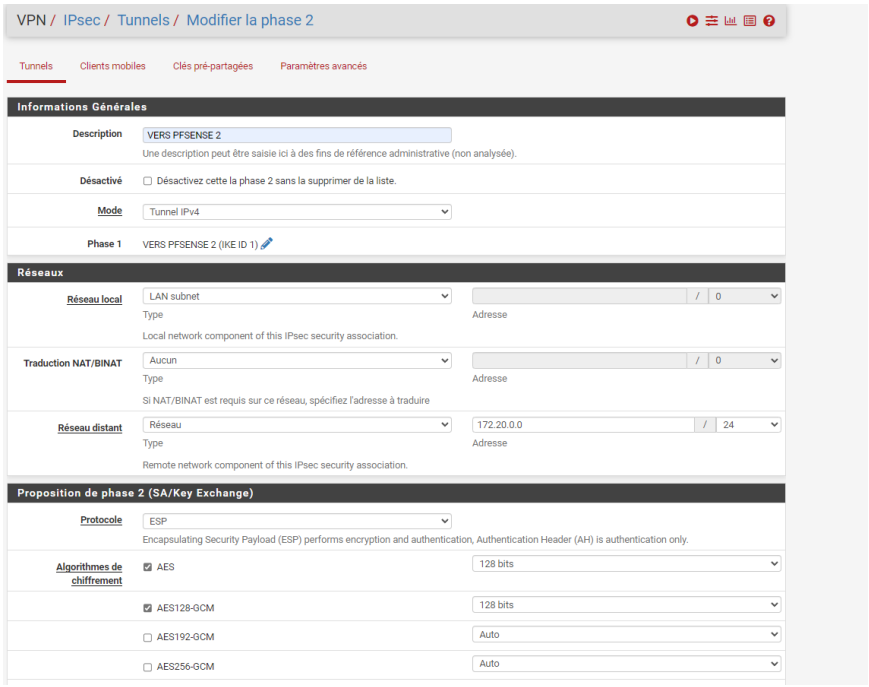
Ensuite je modifie rien d'autre

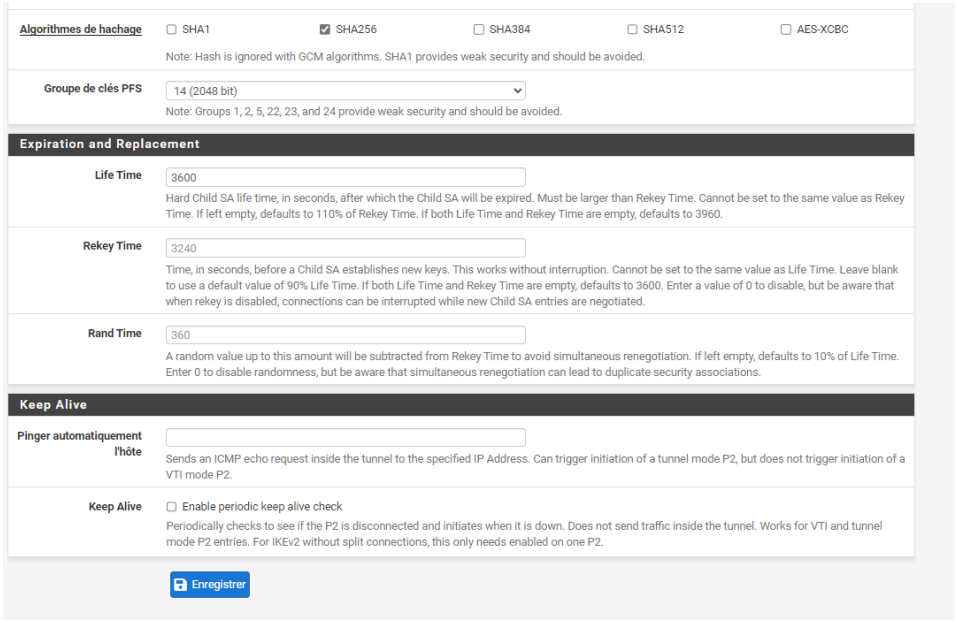


Ensuite on valide et on affiche les entrée pour la P2 que l'on va devoir modifier

Ensuite on ajoute P2

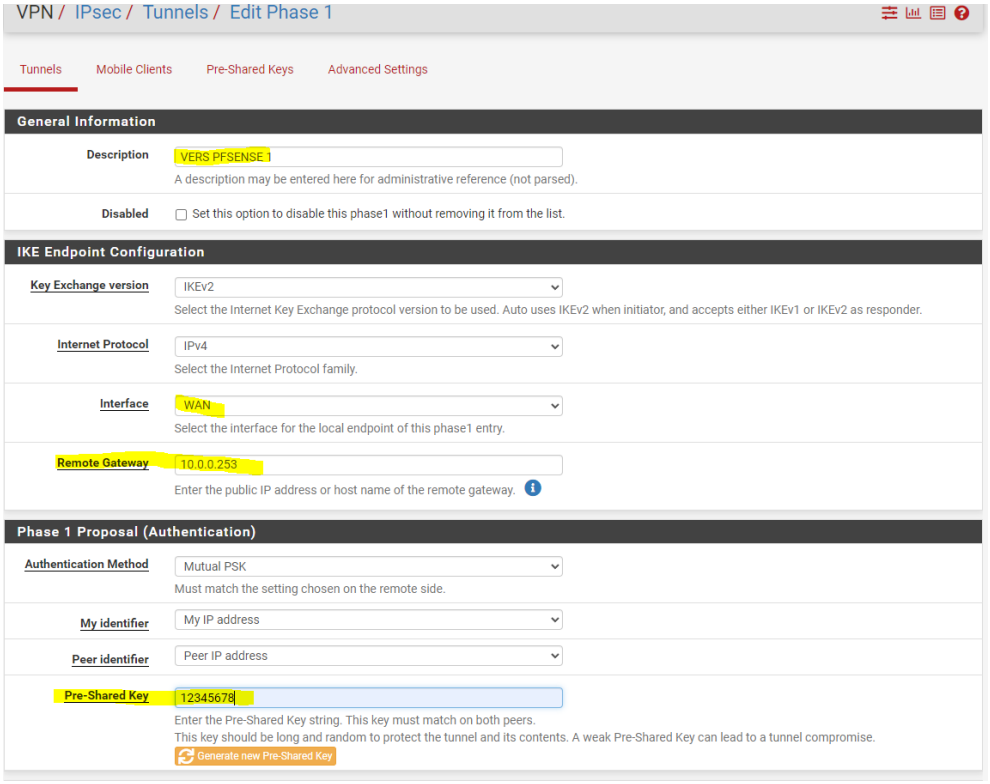
Pas grand-chose à modifier ici juste l'ip du LAN derrière le second routeur

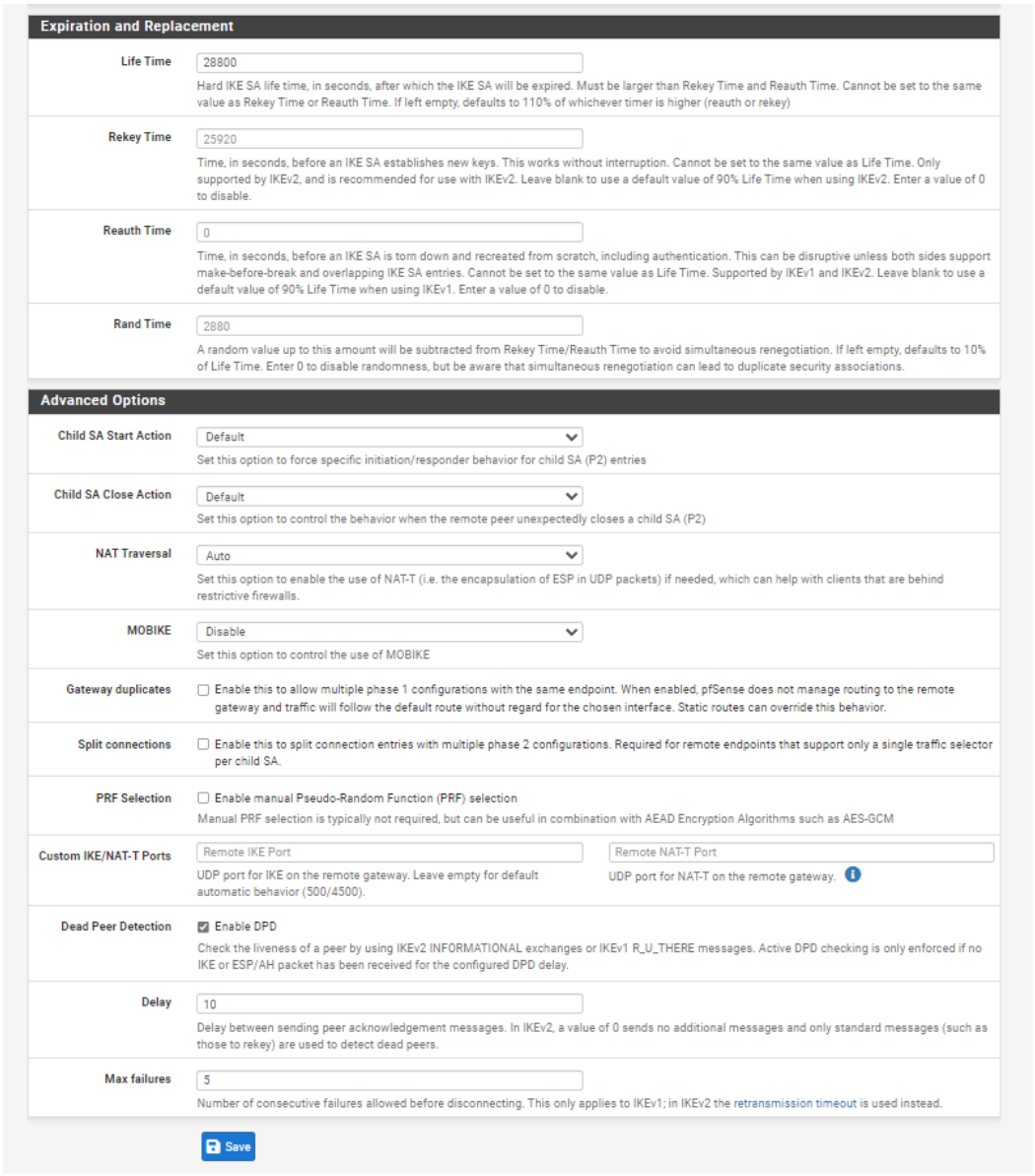




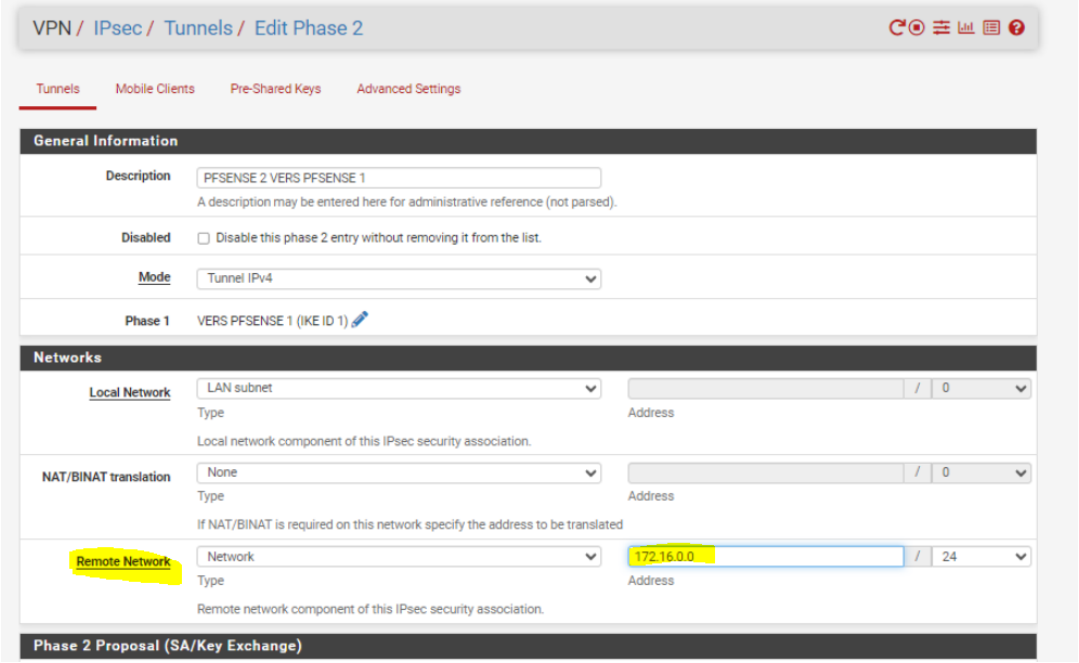
Ensuite on refait exactement la même config de l'autre coté en inversant certains parametre

Coter second routeur :

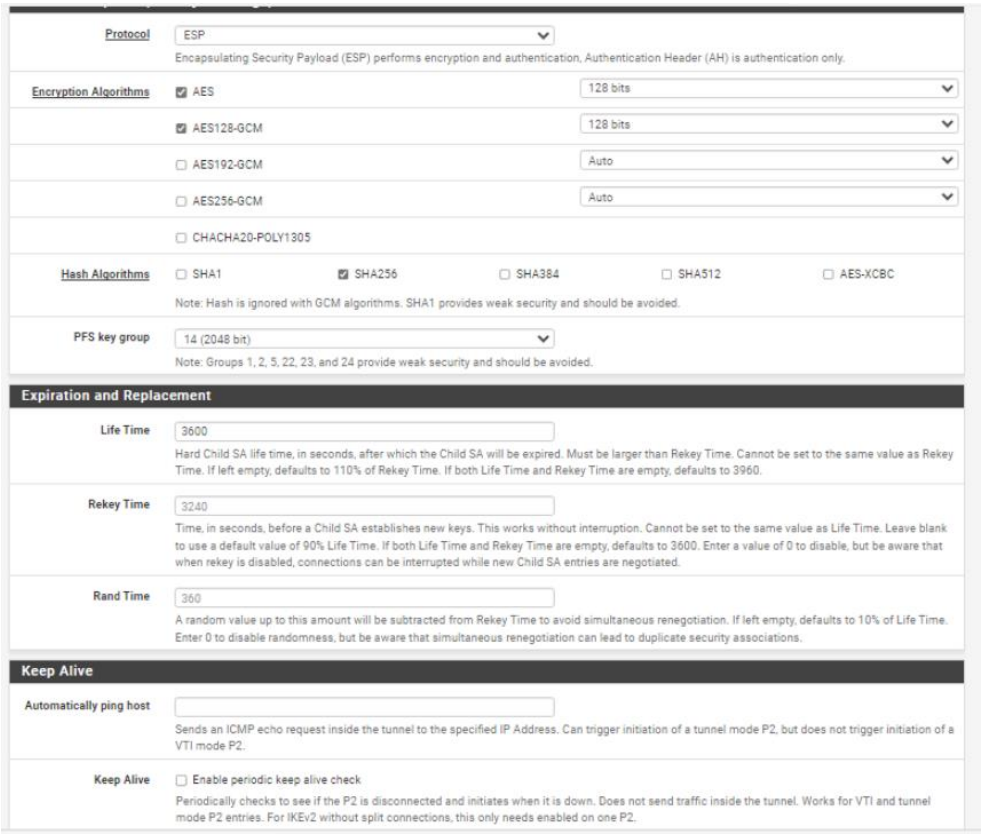

VPN / IPsec / Tunnels / Edit Phase 1
Tunnels
Mobile Clients
Pre-Shared Keys
Advanced Settings
General Information
Description
VERS PFSENSE 1
A description may be entered here for administrative reference (not parsed).
Disabled
Set this option to disable this phase1 without removing it from the list.
IKE Endpoint Configuration
Key Exchange version
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
10.0.0.253
Enter the public IP address or host name of the remote gateway.
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
12345678
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


Expiration and Replacement
Life Time
28800
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
25920
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
0
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
2880
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
Default
Set this option to force specific initiation/responder behavior for child SA (P2) entries
Child SA Close Action
Default
Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)
NAT Traversal
Auto
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
Disable
Set this option to control the use of MOBIKE
Gateway duplicates
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
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
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
Remote IKE Port
UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500).
Remote NAT-T Port
UDP port for NAT-T on the remote gateway.
Dead Peer Detection
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
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
5
Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the retransmission timeout is used instead.
Save

P2 :



Même conf que l'autre pfsense

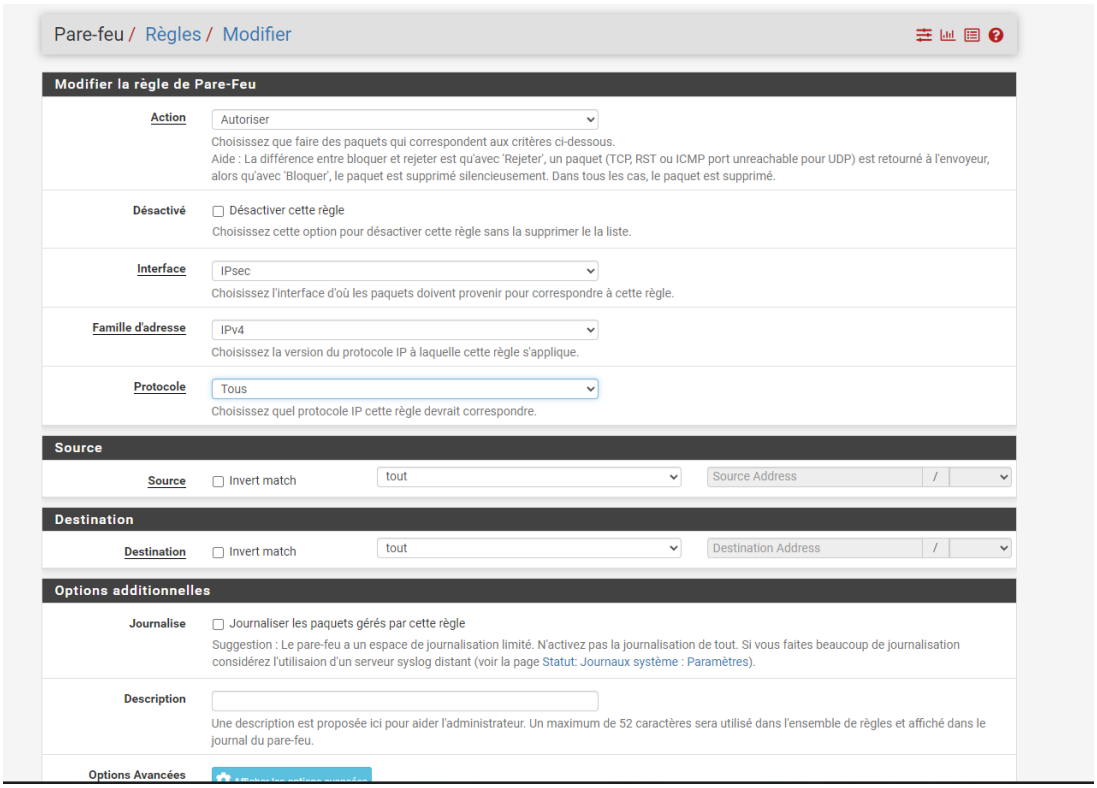


Règles pare-feu

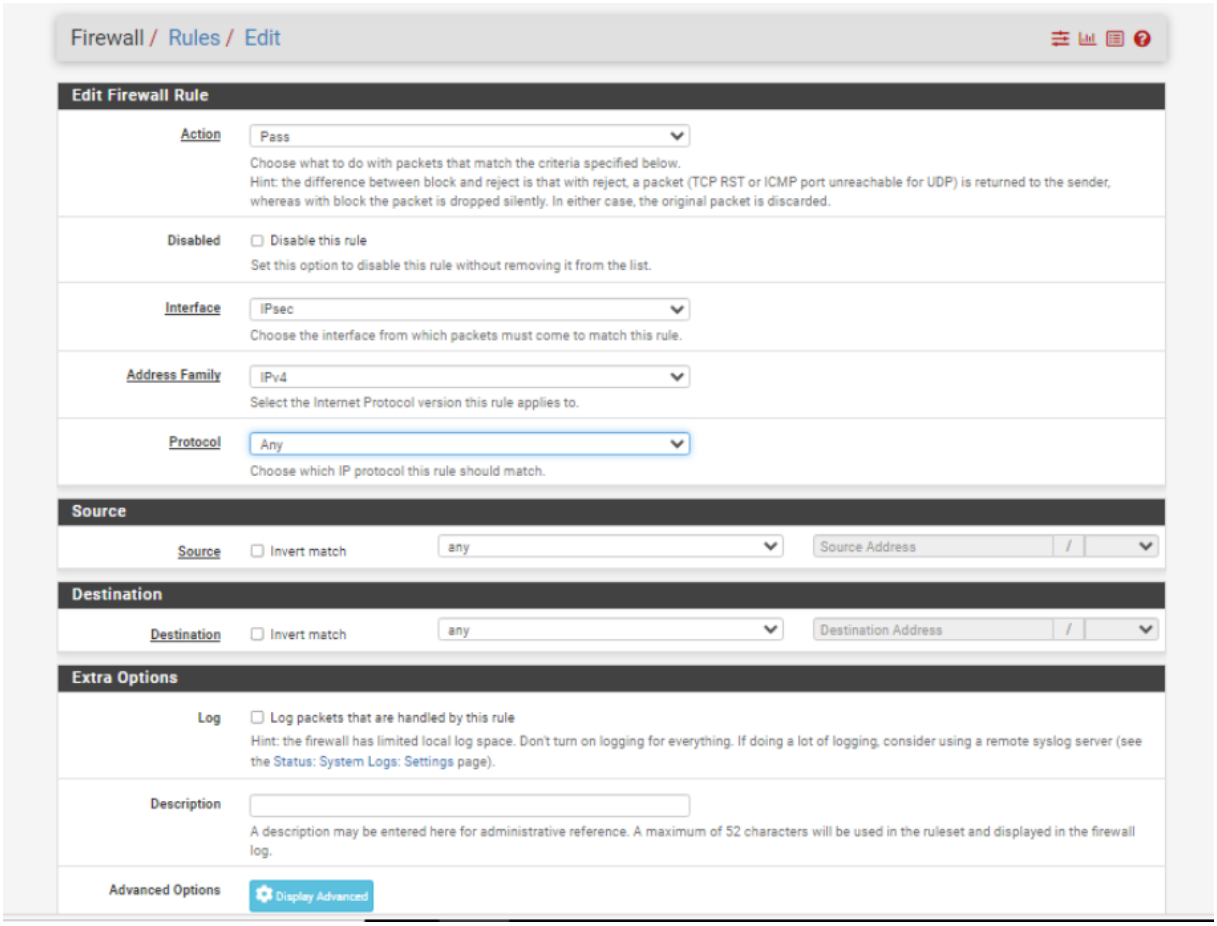
Il faut mettre en place des règles sur l'interface IPsec pour que le trafic puisse correctement passé car par défaut il est bloqué.

J'autorise tout en restreindra plus tard

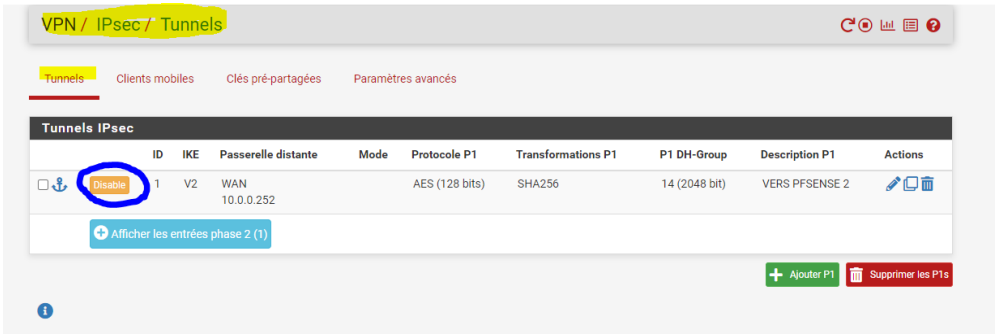
PFSENSE 1



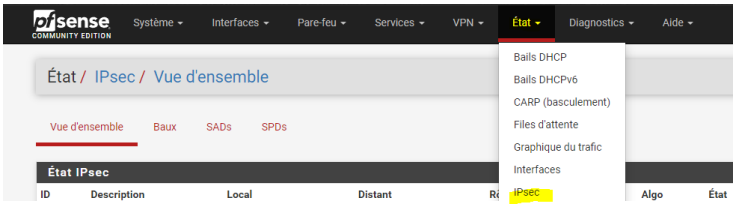
PFSENSE 2



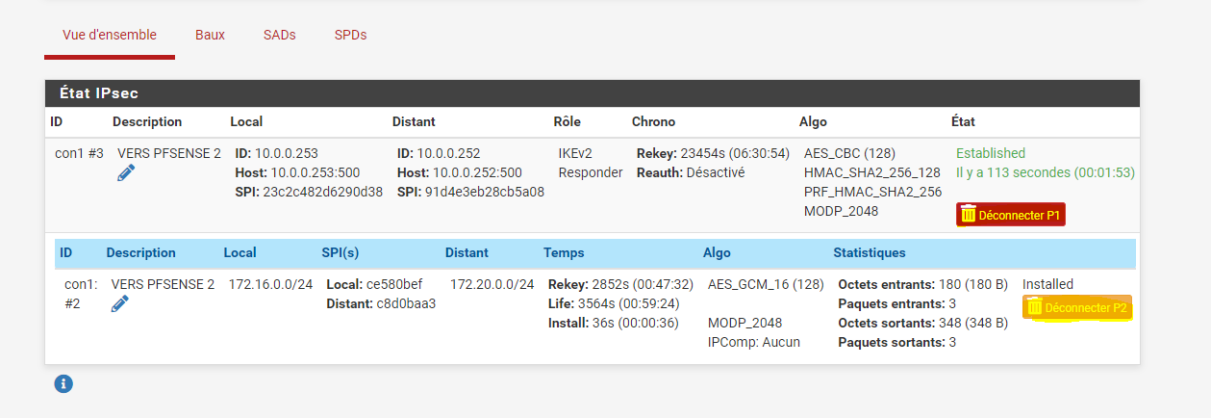
Ensuite ne pas appuyer sur Disable pour passer en Enable car sa désactive s'active rien.



Ensuite pour vérifier que le VPN fonctionne correctement.



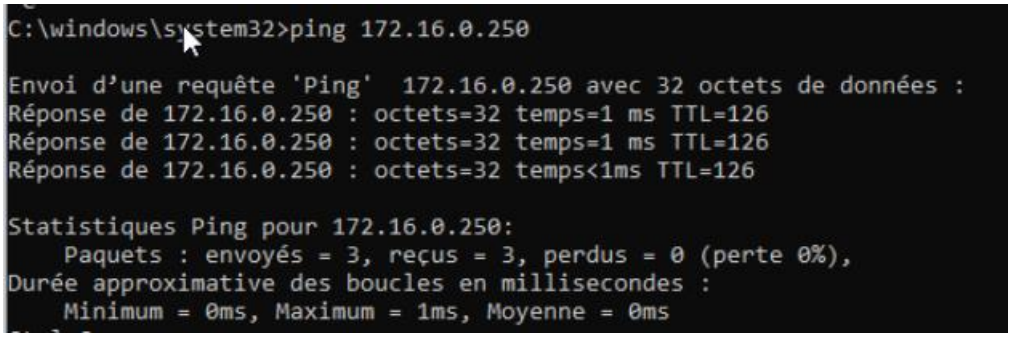
Ensuite on doit voir que les phases fonctionnent



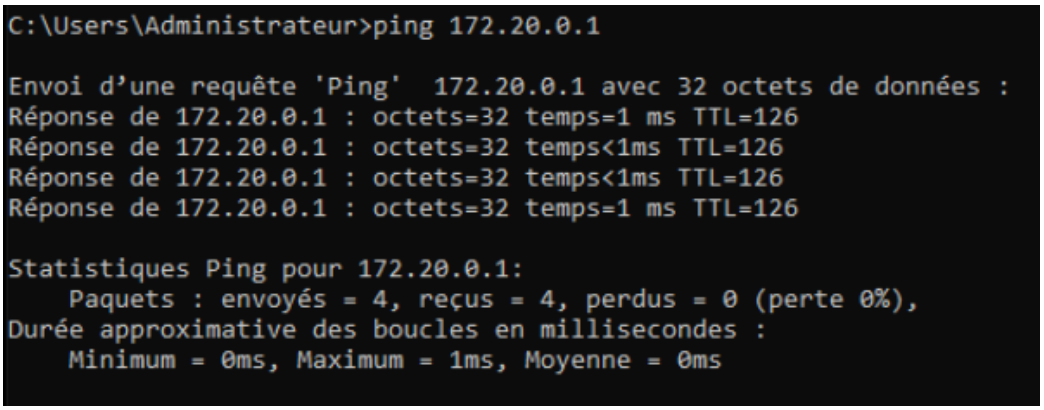
Si la une fonctionne sans la deux peut être d'un coté ou l'autre elle est désactivé ou il y'a un soucis dans la conf mais si les deux machine sur leur interfaces WAN ce ping et que la conf est correct il n'ya pas de raison que ça ne fonctionne pas.

Test

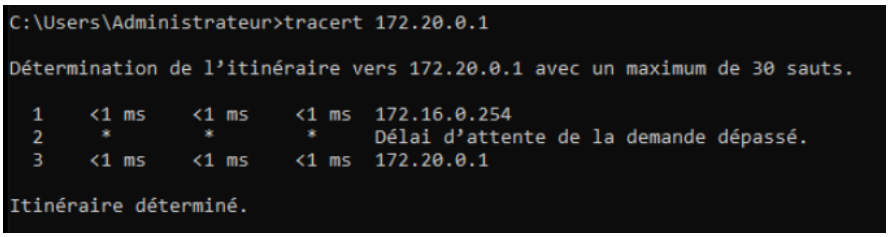
Ping depuis 172.20.0.0 vers 172.16.0.0



Depuis 172.16.0.0 vers 172.20.0.0



+ tracert



Voila maintenant nous savons comment mettre en place IPsec entre deux firewall pfsense.