# Mise en place d'un VPN site à site

# Sommaire :

## I. Présentation du VPN site à site :

Le VPN (Virtual Private Network) site à site est une technologie permettant d'interconnecter de manière sécurisée deux réseaux locaux (LAN) géographiquement séparés, en utilisant une infrastructure réseau publique comme Internet. Contrairement à un VPN d'accès distant, qui connecte un utilisateur à un réseau d'entreprise, le VPN site à site relie directement deux sites entiers.

Cette solution est couramment utilisée par les entreprises possédant plusieurs agences ou filiales. Elle permet un échange sécurisé des données comme si les machines distantes appartenaient au même réseau local, tout en évitant les frais liés à l'installation d'un réseau privé physique.

Le VPN site à site repose sur des protocoles de tunneling et de chiffrement, tels qu'IPsec, afin de garantir la confidentialité, l'intégrité et l'authenticité des données échangées entre les sites. Il est généralement mis en œuvre à l'aide de pare-feux ou de routeurs compatibles, comme **pfSense**, qui sera utilisé dans ce projet.

## II. Objectif du projet :

Le but de ce projet est de connecter deux sites distants entre eux en utilisant un VPN site à site. Pour cela, j'utiliserai pfSense sur chaque site, qui servira à établir et gérer le tunnel VPN.

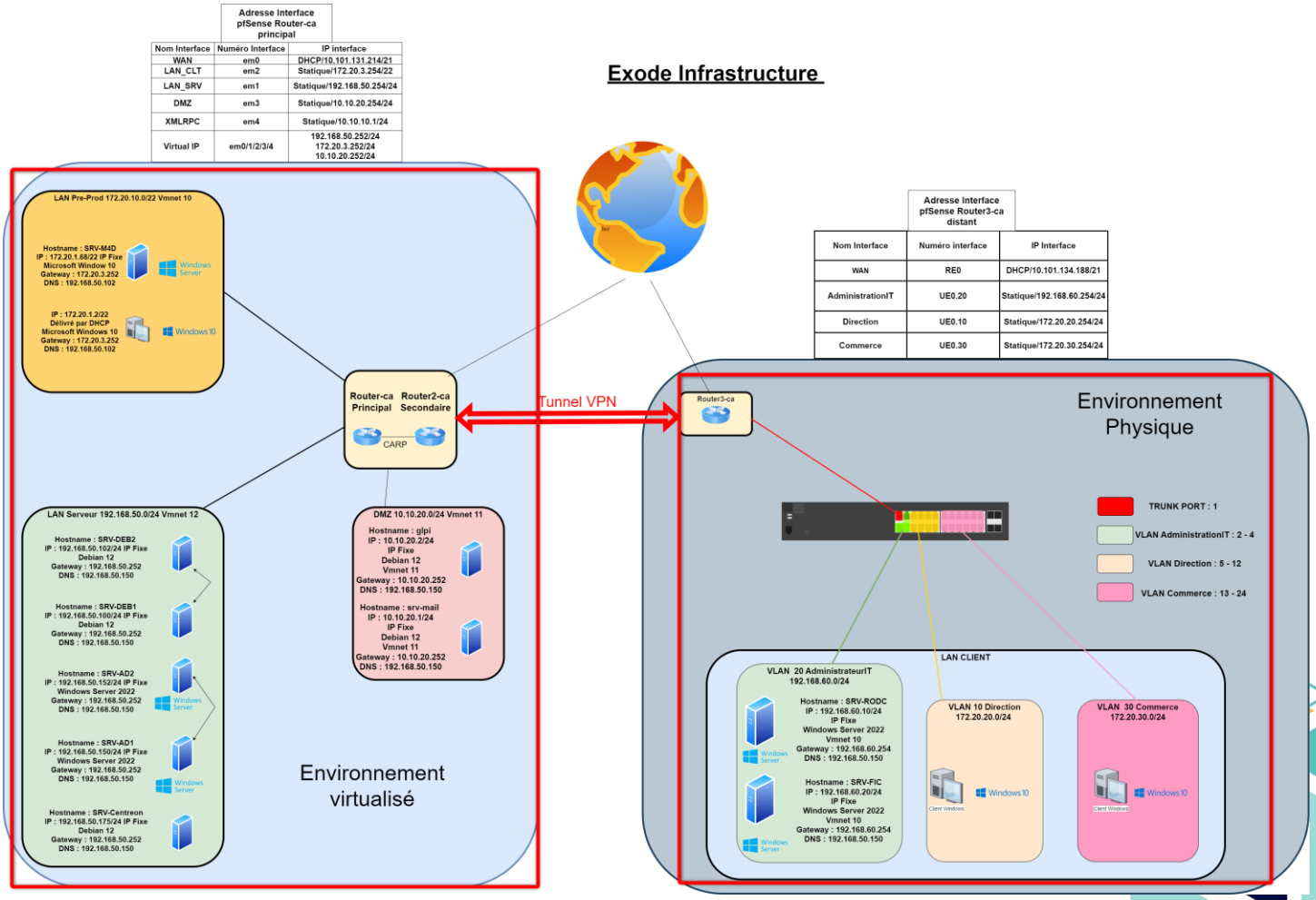
Un VPN (Virtual Private Network) est une technologie qui permet de créer une connexion sécurisée à travers un réseau non sécurisé, comme Internet. Il garantit la confidentialité et la sécurité des échanges de données entre deux points.

Dans ce projet, le protocole utilisé sera IPsec (Internet Protocol Security). IPsec est un protocole de sécurité conçu pour chiffrer et authentifier les paquets IP. Il est particulièrement adapté aux connexions VPN site à site, car il est stable, sécurisé, et largement compatible avec les équipements réseau professionnels comme pfSense. IPsec est plus adapté qu'un protocole comme OpenVPN pour ce type d'architecture, car il est directement pris en charge au niveau du système et des équipements réseau, ce qui en fait un choix privilégié dans les infrastructures professionnelles pour interconnecter plusieurs sites de façon permanente et fiable.

Grâce à cette configuration, les deux sites pourront communiquer comme s'ils faisaient partie d'un même réseau local, tout en passant par une connexion chiffrée sur Internet.

## III. Mise en place du VPN site à site avec pfSense :

Comme vu précédemment IPsec est utilisé lors d'une interconnexion entre deux sites distants. Dans mon cas et suivant ce schéma réseau, IPsec répond donc parfaitement à mon besoin de VPN site à site.

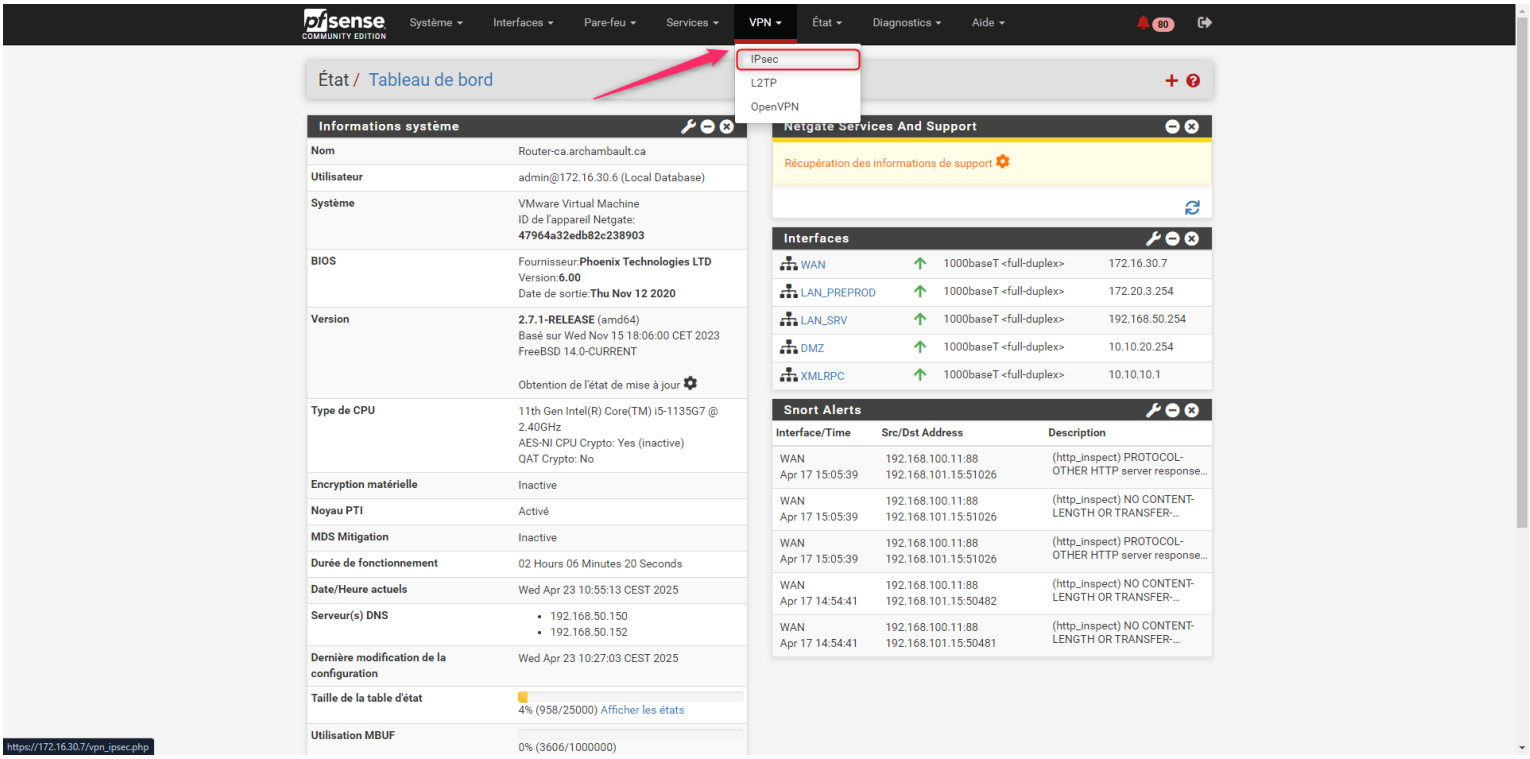



Dans cette configuration, il faut commencer par la configuration de VPN IPsec sur le site principal, en bleu clair.

## 1- Configuration du VPN IPsec sur le site principal :

Dans un premier temps, connectez vous sur l'interface pfSense du site principal.

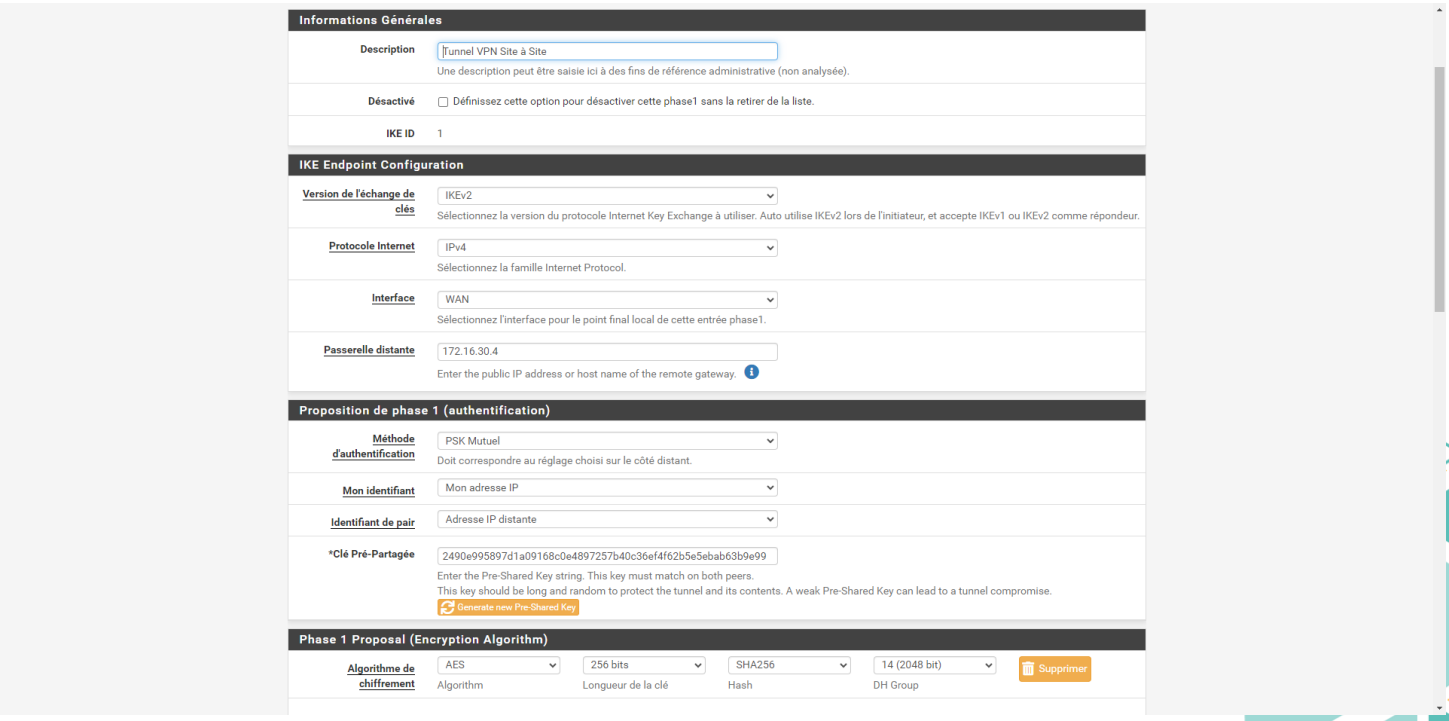
Il faut ensuite aller dans l'onglet VPN > IPsec

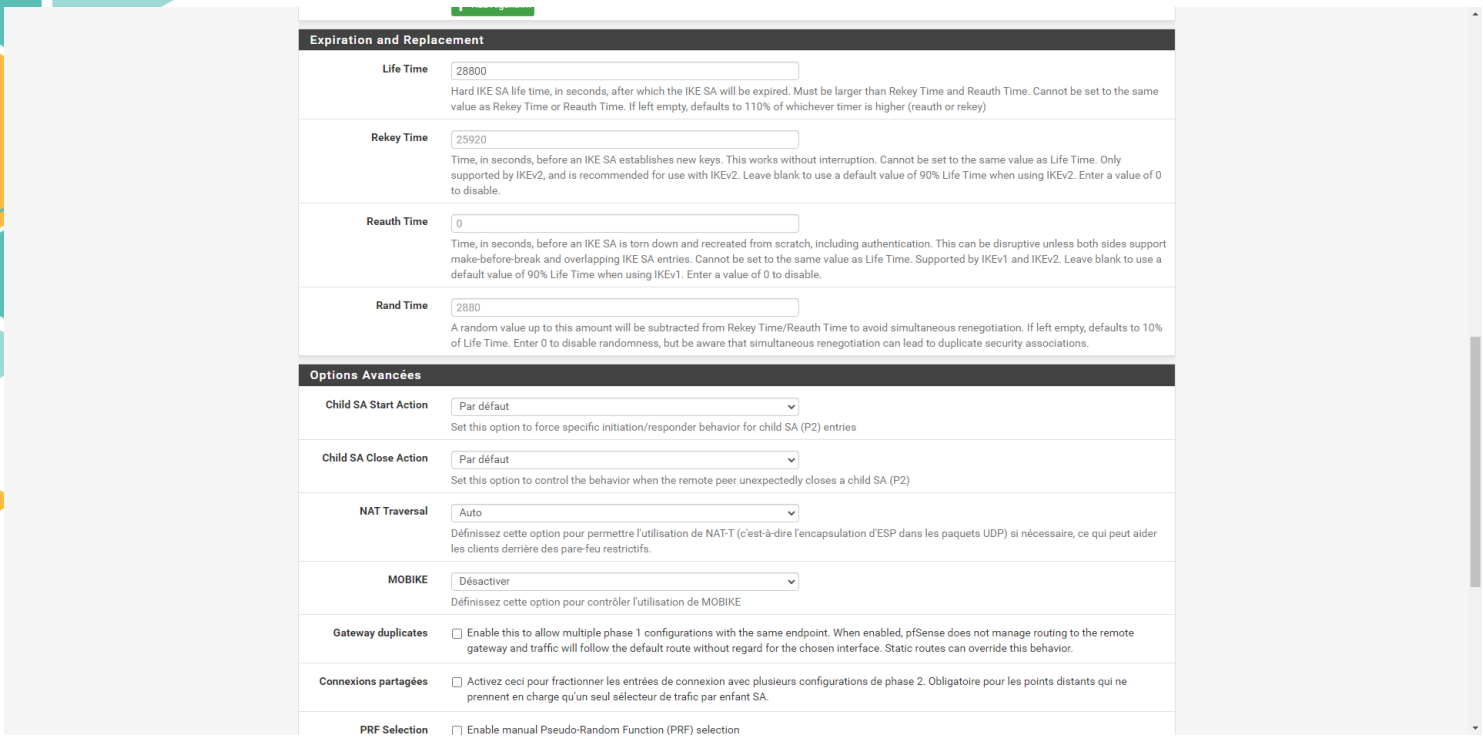



Une fois dans la section de configuration IPsec de pfSense, la première étape consiste à configurer la Phase 1. Cette phase permet d'établir une connexion sécurisée initiale entre les deux sites, en s'appuyant sur le protocole IKE (Internet Key Exchange). IKE est utilisé pour négocier et établir une association de sécurité (Security Association - SA) entre les deux pare-feux pfSense.

Voici les paramètres importants à définir dans la phase 1 :

- Key Exchange version : IKEv2 (recommandé pour sa robustesse et sa compatibilité)
- Remote Gateway : Adresse IP publique du site distant
- Authentication Method : Pre-Shared Key (clé partagée, plus simple pour un environnement de test)
- My identifier / Peer identifier : Généralement configuré avec les adresses IP ou FQDN
- Encryption Algorithm : AES (256 bits recommandé)
- Hash Algorithm : SHA256
- DH Group : 14 ou 19 (selon le niveau de sécurité souhaité)
- Lifetime : 28800 secondes (valeur par défaut généralement conservée)





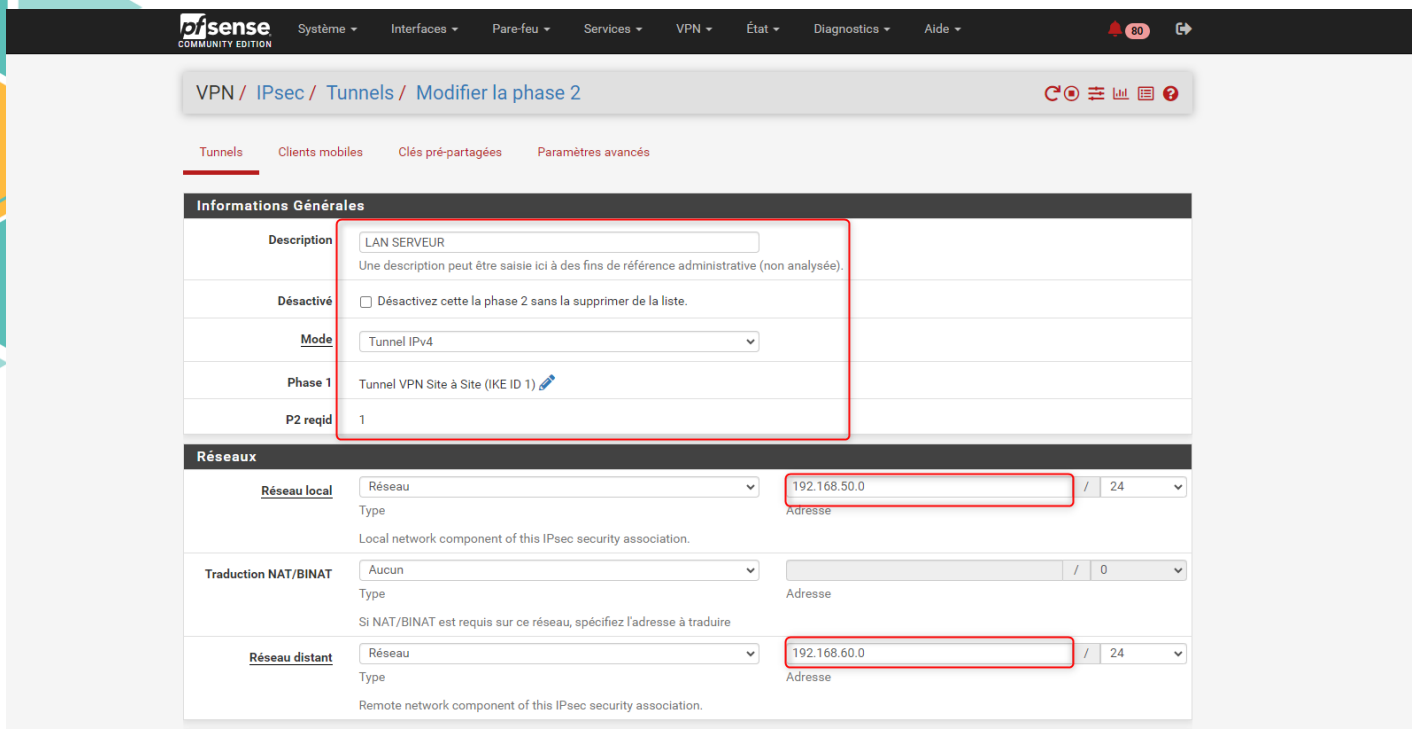

Une fois tous les champs correctement remplis, il suffit d'enregistrer la phase 1, puis de passer à la configuration de la phase 2, qui permettra de définir les réseaux autorisés à communiquer à travers le tunnel.

Toujours dans VPN > IPsec, cliquez sur Show Phase 2 Entries sous la configuration de la phase 1.

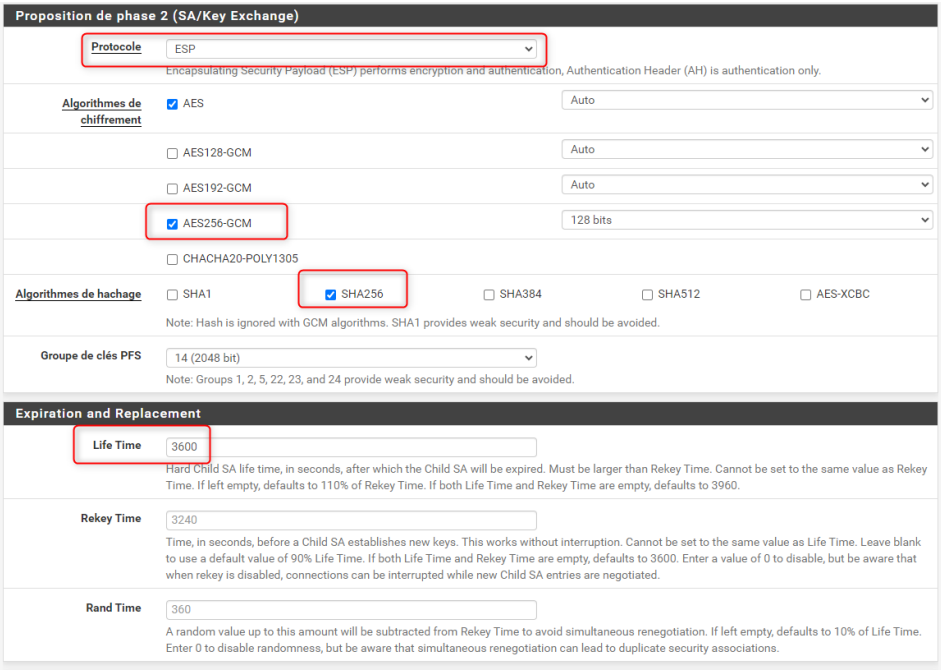
Cliquez sur Add P2.

Et remplir les informations suivantes :

- Mode : Tunnel IPv4
- Local Network : Réseau LAN du site principal
- Remote Network : Réseau LAN du site distant

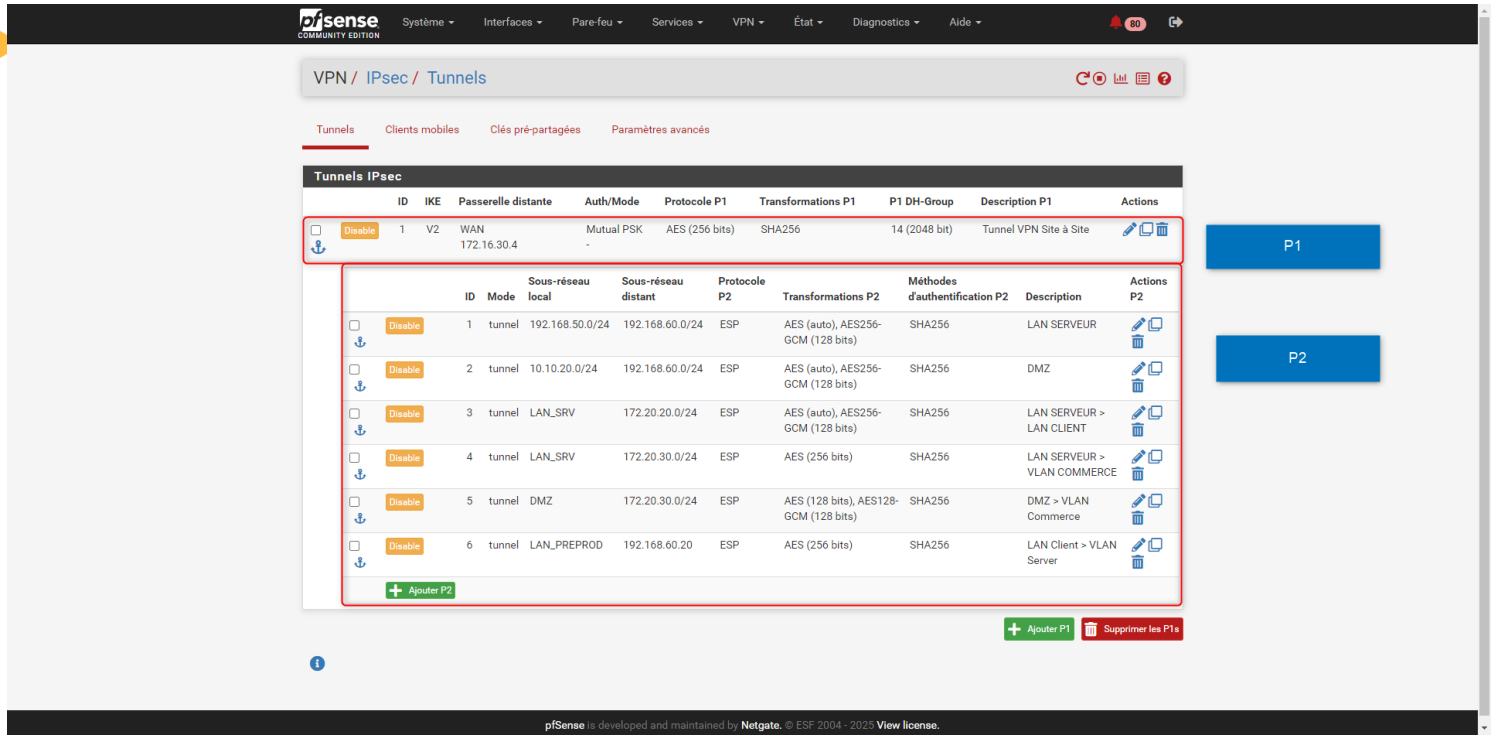



- Protocol : ESP
- Encryption Algorithms : AES 256
- Hash Algorithms : SHA256
- PFS Key Group : 14 (2048-bit)
- Lifetime : 3600 (par défaut)

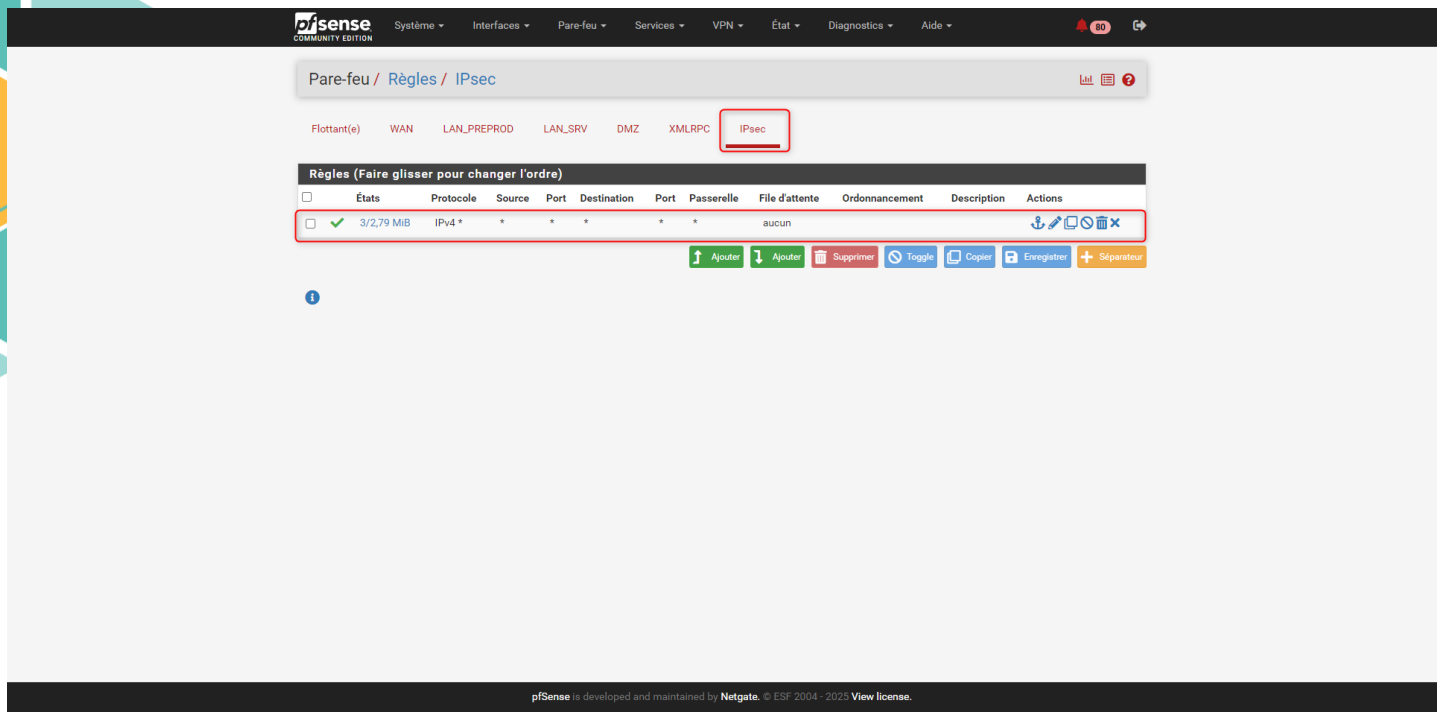


Sauvegarder et appliquer.

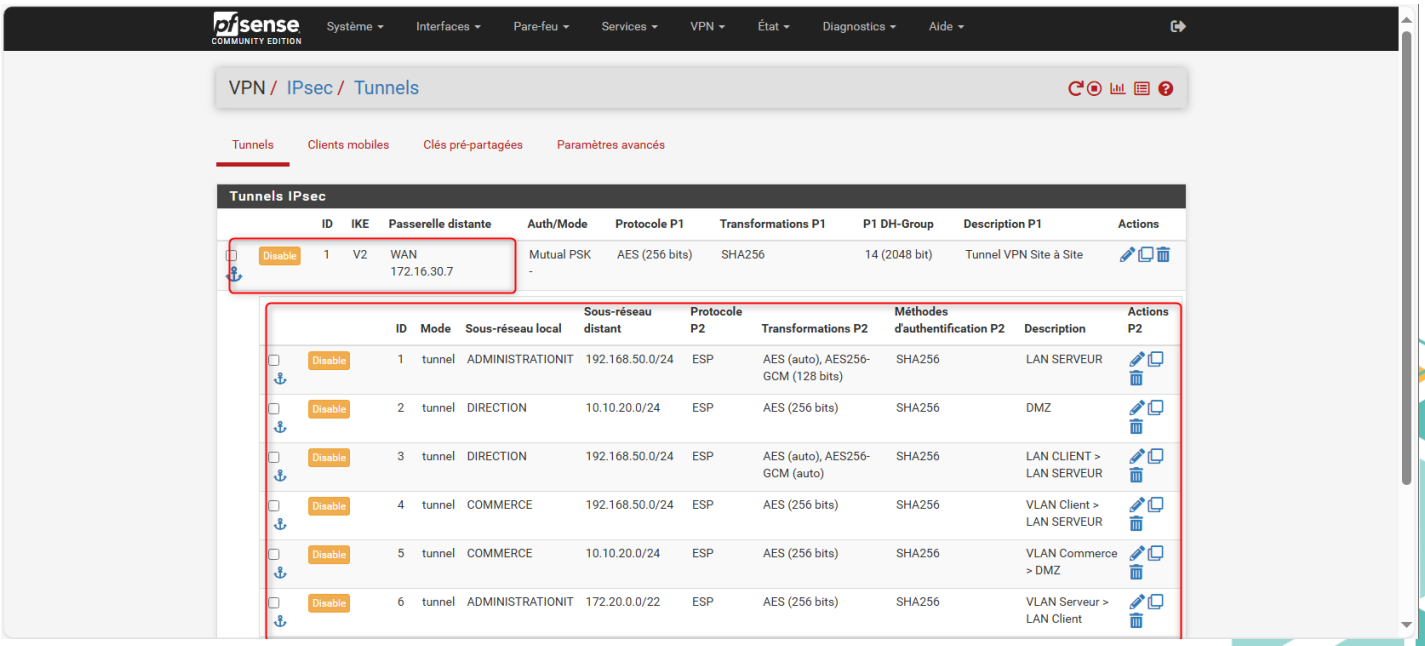
Une fois la configuration terminée, la configuration devrait ressembler à ça :




Une fois la phase 1 et la phase 2 configurées, allez dans les règles de pare-feu IPsec pour ajouter une règle permettant la communication. Ici nous allons tout ouvrir puisque les règles spécifiques s'appliqueront sur les interfaces des différents réseaux.




Une fois la configuration sur le site principal faites, allez sur l'interface web du pfSense distant et rentré l'identique configuration, mais avec les adresses inverses.



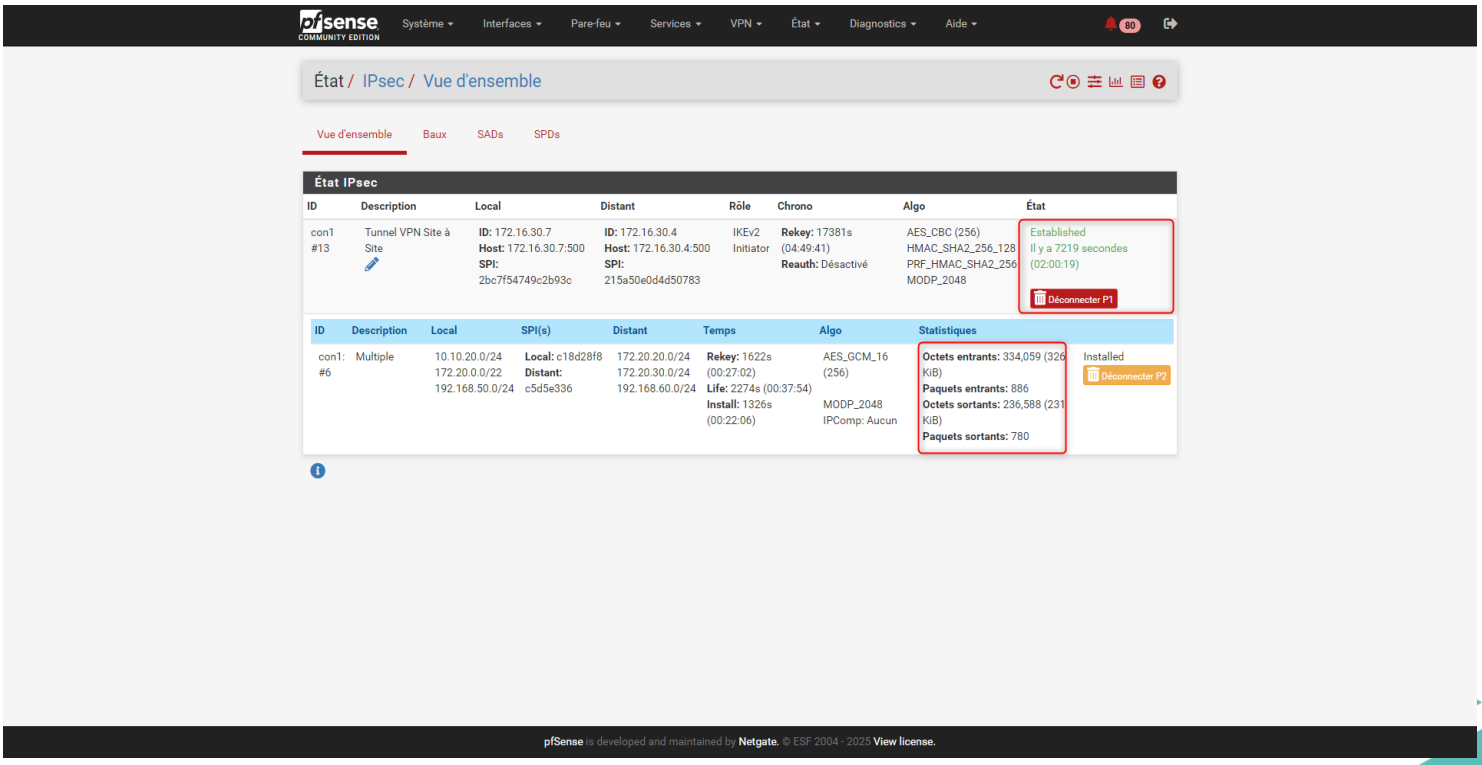

Ici sur l'interface web du pfSense distant on retrouve bien la phase 1, avec comme passerelle distante l'IP WAN du site principal.

Ainsi que toutes les phases 2 permettant aux VLANs du site distant de communiquer avec les différents services présents sur le site principal.

## IV. Tests de connectivité et vérifications :

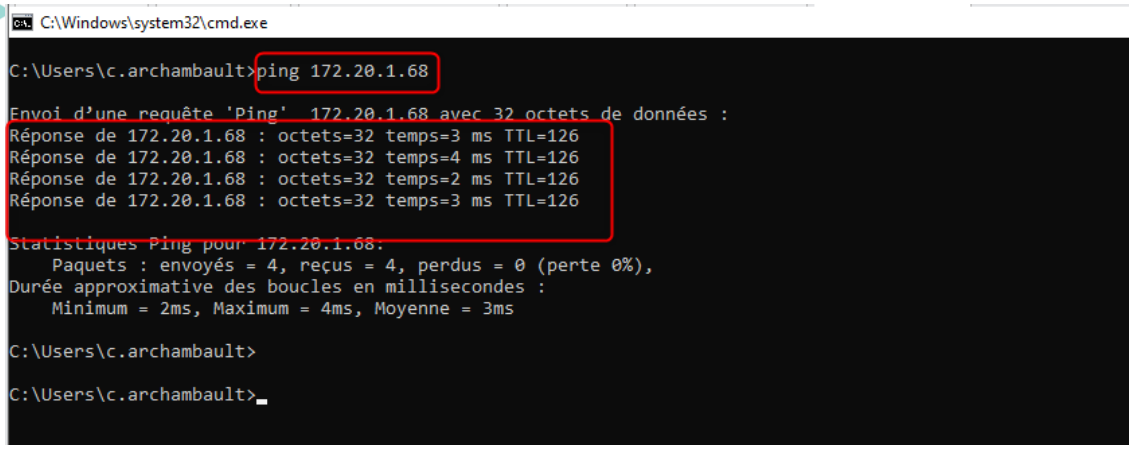
Une fois les deux configurations terminées, allez dans sur l'interface pfSense d'un des deux routeurs dans la partie Etat > IPsec.

Connecter les phases 1 et 2 et vérifier si la connexion est établie avec une indication « ESTABLISHED ».




Il est possible maintenant d'effectuer un test de ping entre différentes machines présentes sur les réseaux distant.

Ici je vais vérifier que mon SRV-FIC (serveur fichier) situé dans le VLAN serveur sur le site secondaire peut communiquer avec mon serveur de fichier SRV-M4D (serveur application métier) situé dans le LAN_PREPROD sur le site distant.




Le test de connectivité est donc bien fonctionnel.

## V. Compétences mises en œuvre :

| Compétence du référentiel | Mise en œuvre dans le projet |
|---|---|
| Gérer le patrimoine informatique | Recherche des ressources disponibles sur l'infrastructure pour la création du VPN. Configuration du matériel sur les deux sites. |
| Répondre aux incidents et aux demandes d'assistance et d'évolution | Rattachement du site étendu à l'infrastructure initiale (site principale). |
| Mettre à disposition des utilisateurs un service informatique | Mise en place d'un tunnel VPN entre les deux sites pour garantir l'accès aux services pour les utilisateurs du site distant. |

## VI. Problèmes rencontrés et solutions :

Lors de la mise en place du VPN site-à-site avec pfSense, plusieurs difficultés ont été rencontrées, dont une erreur importante liée à la configuration de la Phase 2 du tunnel IPsec.

### Problème :

Lors de l'établissement du tunnel VPN, la Phase 2 a été mal configurée. Plus précisément, les réseaux définis ne correspondaient pas correctement aux réseaux LAN à interconnecter, notamment le LAN_PREPROD qui n'arrivait pas à communiquer avec les VLANs distants du site opposé. Cette mauvaise configuration empêchait tout échange de paquets entre les deux sites malgré un tunnel apparemment actif en Phase 1.

### Solution :

Après analyse des logs et tests de connectivité, il a été constaté que la Phase 2 devait être recréée proprement, avec une définition correcte des réseaux locaux et distants. Une fois les bons sréseaux renseignés dans la configuration de la Phase 2, la communication entre les VLANs a été rétablie et le LAN Préproduction a pu accéder aux ressources distantes comme prévu.

Cette erreur a mis en évidence l'importance de bien définir les correspondances réseau dans la Phase 2 d'un VPN IPsec, car une Phase 1 établie sans Phase 2 fonctionnelle bloque complètement le trafic inter-sites.