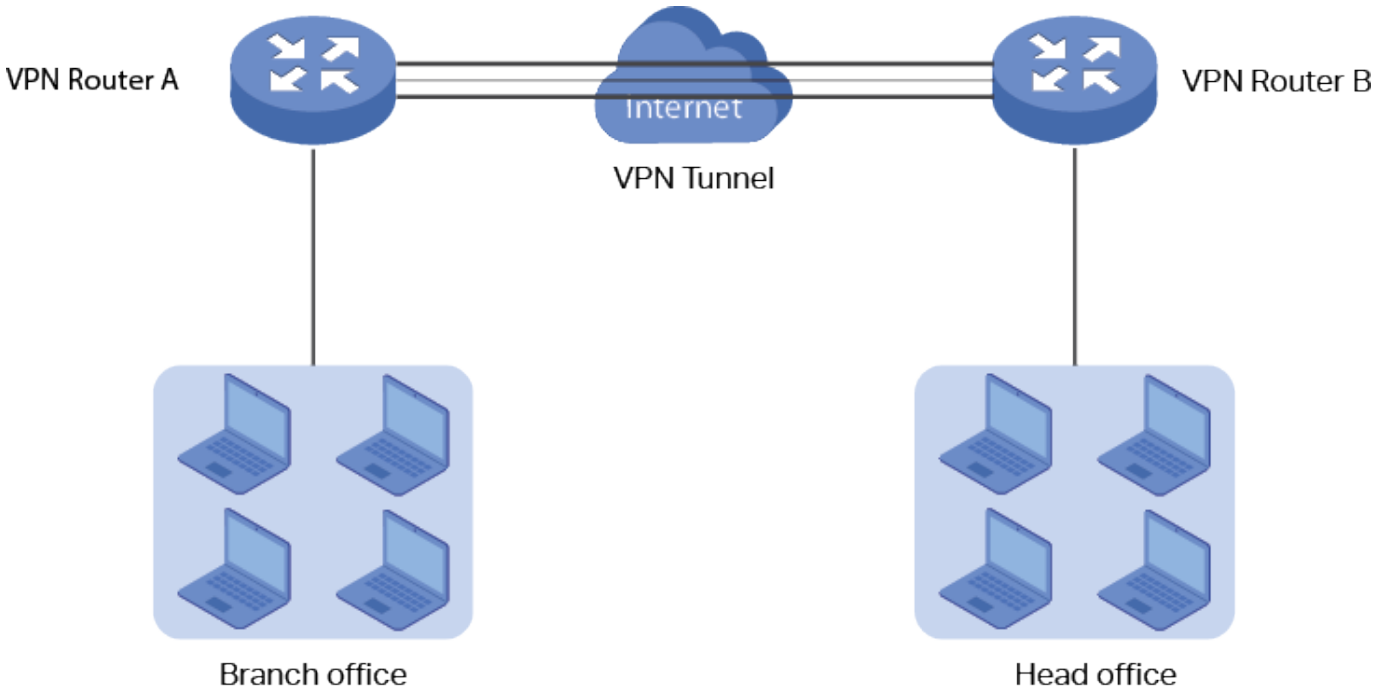
Rayyan Guenfoud
Hugo Garreau
Alexandre Thuret

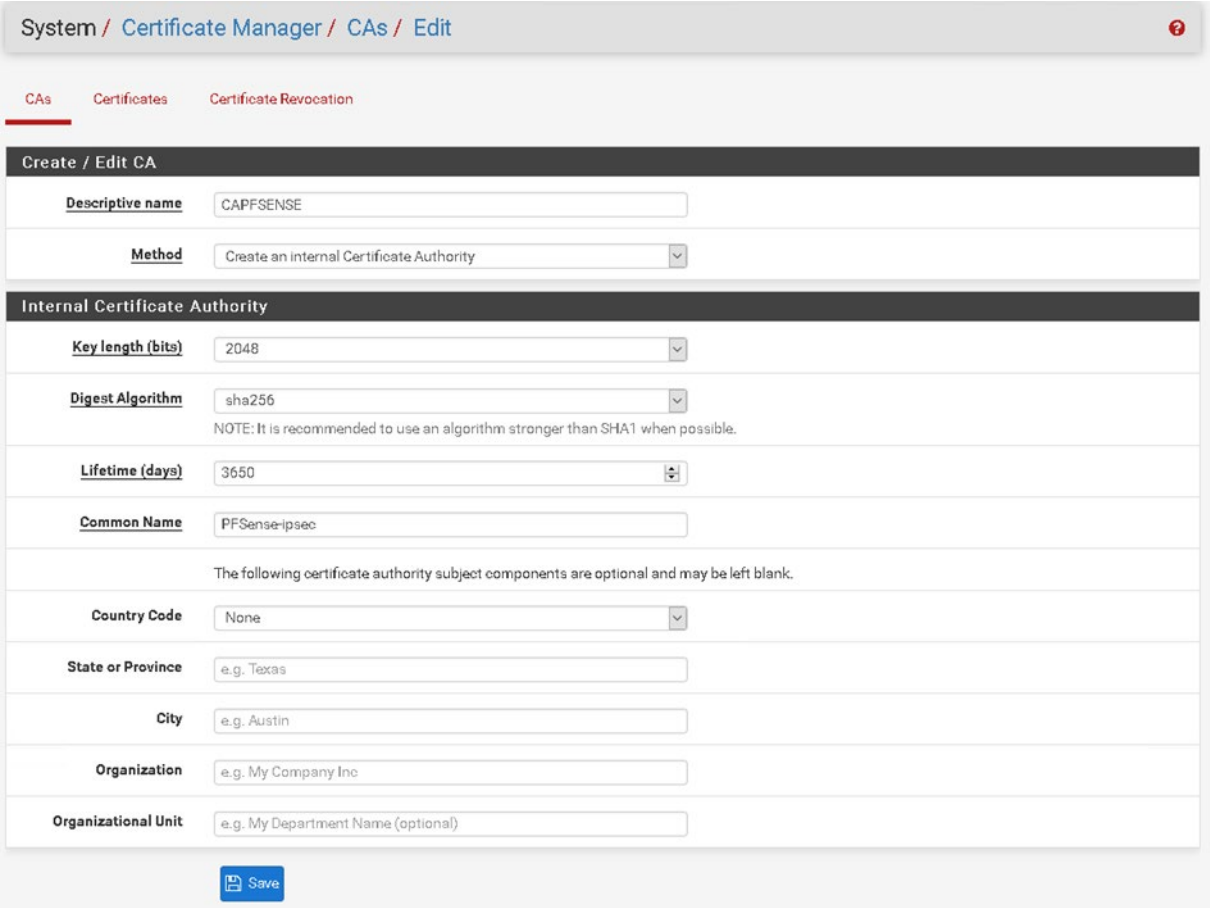
TP Tunnel Host To Lan IPsec & AD

Table des matières

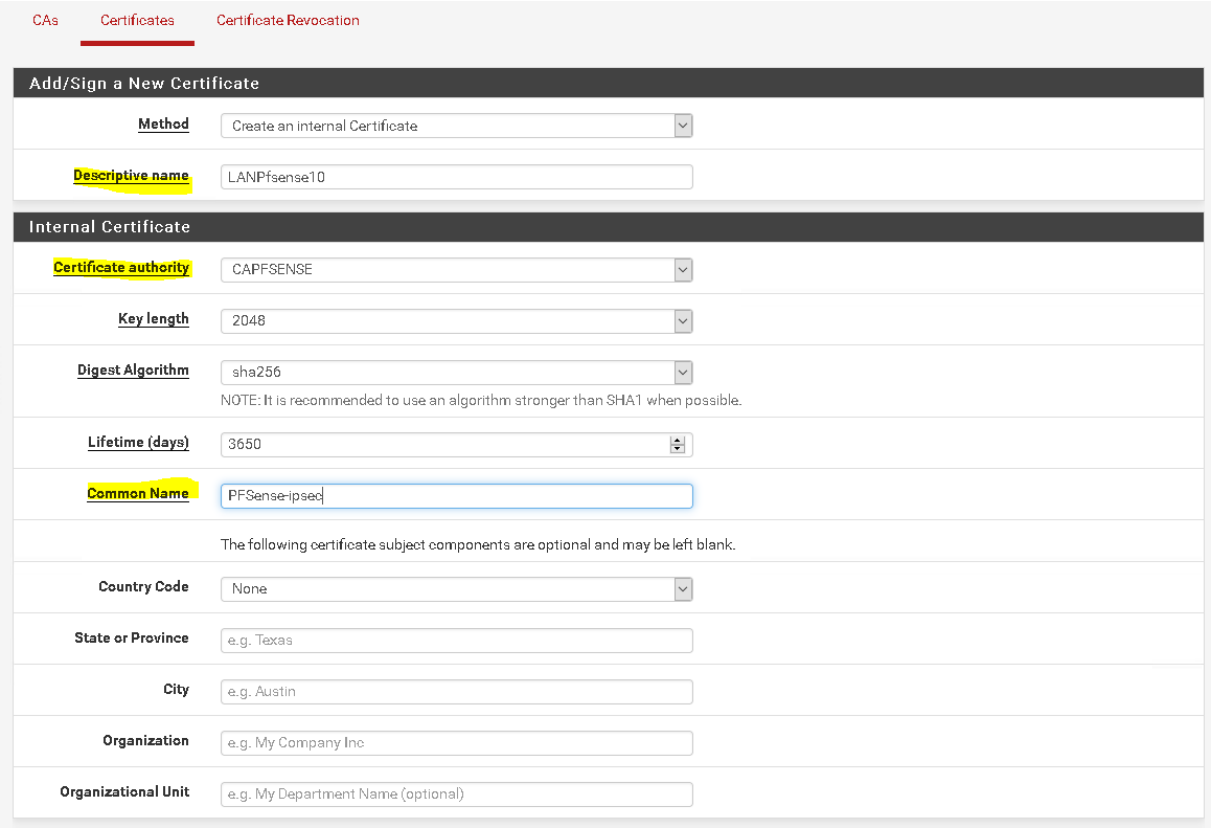


1- Création de l’autoritée de certification

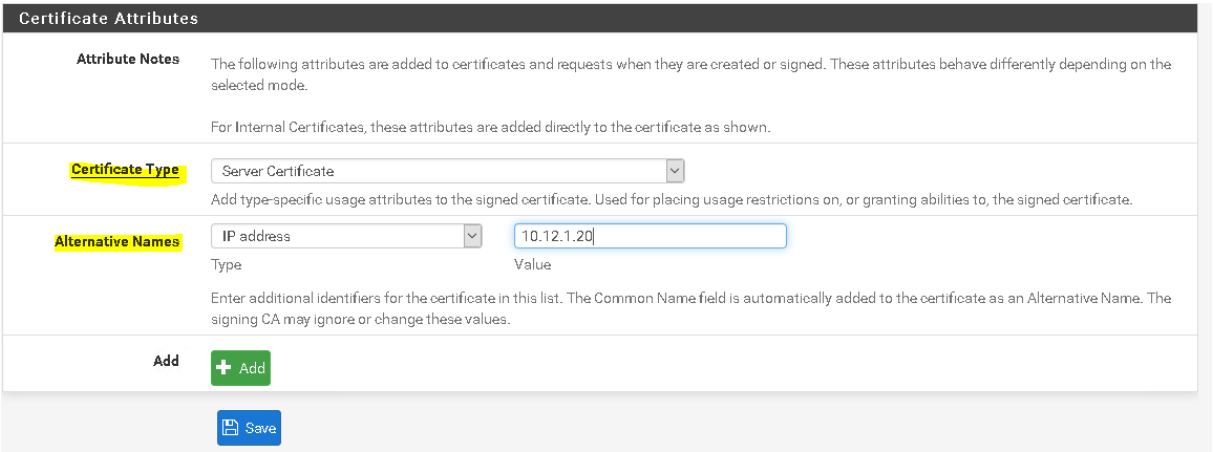
Dans l’onglet Sytem/Certificate Manager/CAs on commence par le nommer et vérifier le Digest Algorithme (sha256) Pour une meilleure sécuritée.



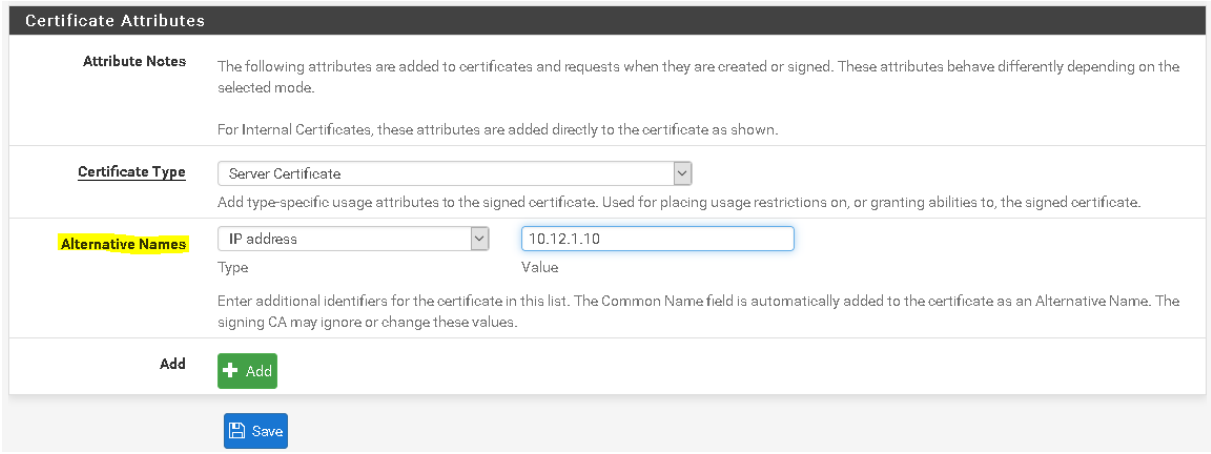
Nous allons ensuite dans l'onglet certificates ou l'ont précise authorité de certification ainsi que le nom du certificat.



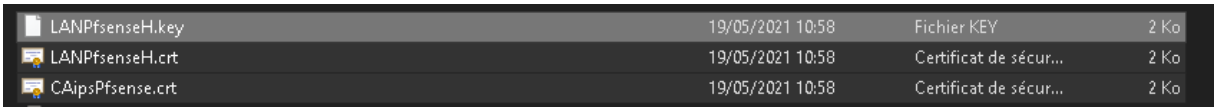
On choisi le type de certificat (ici « Server Certificate »)
Et enfin on ajoute l'adresse IP de la carte WAN du serveur.



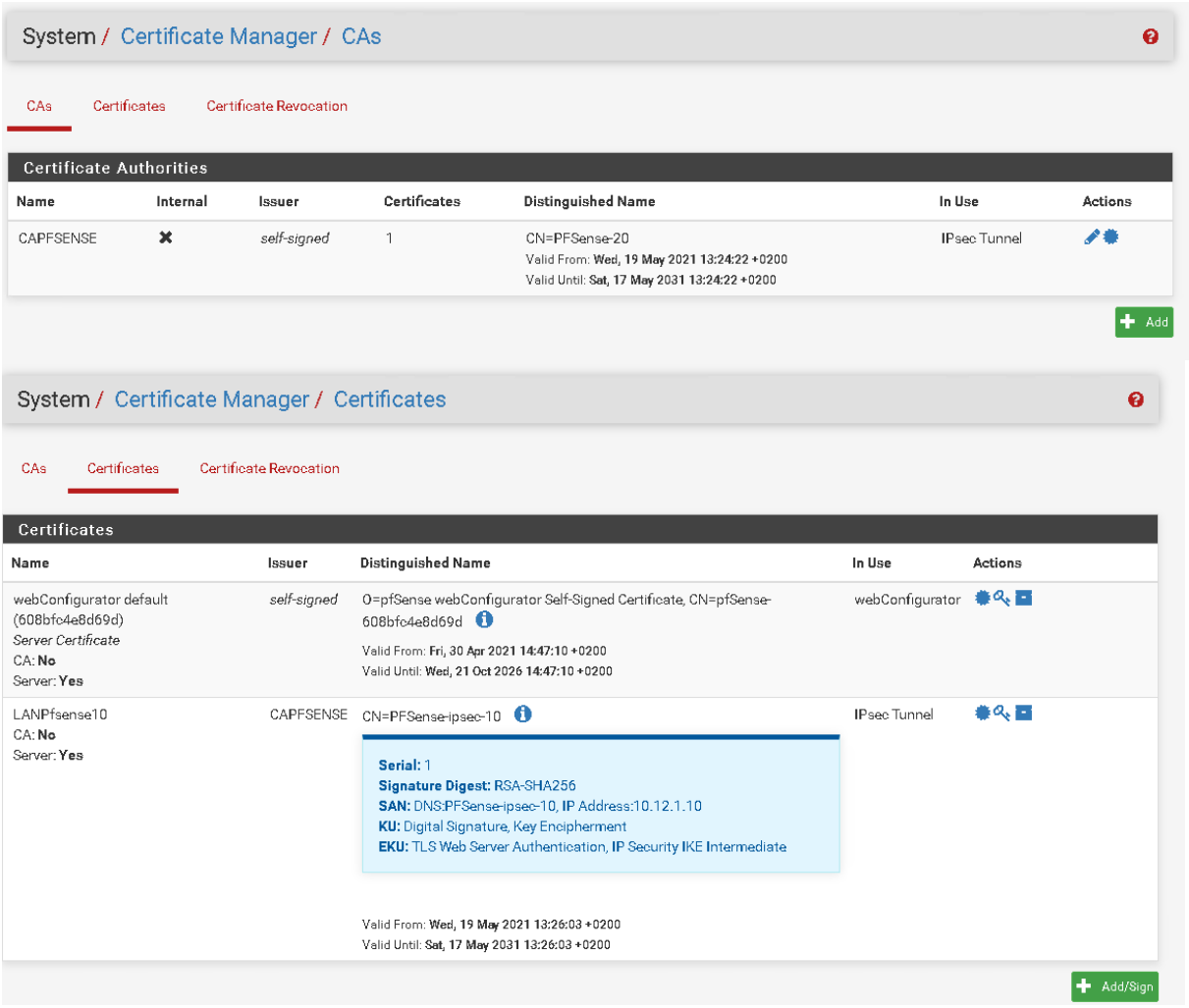
Puis on refait un autre certificat en entrant cette fois-ci l'adresse du second serveur.



On exporte ensuite le premier certificat vers le second serveur.
Certificat & Clé :



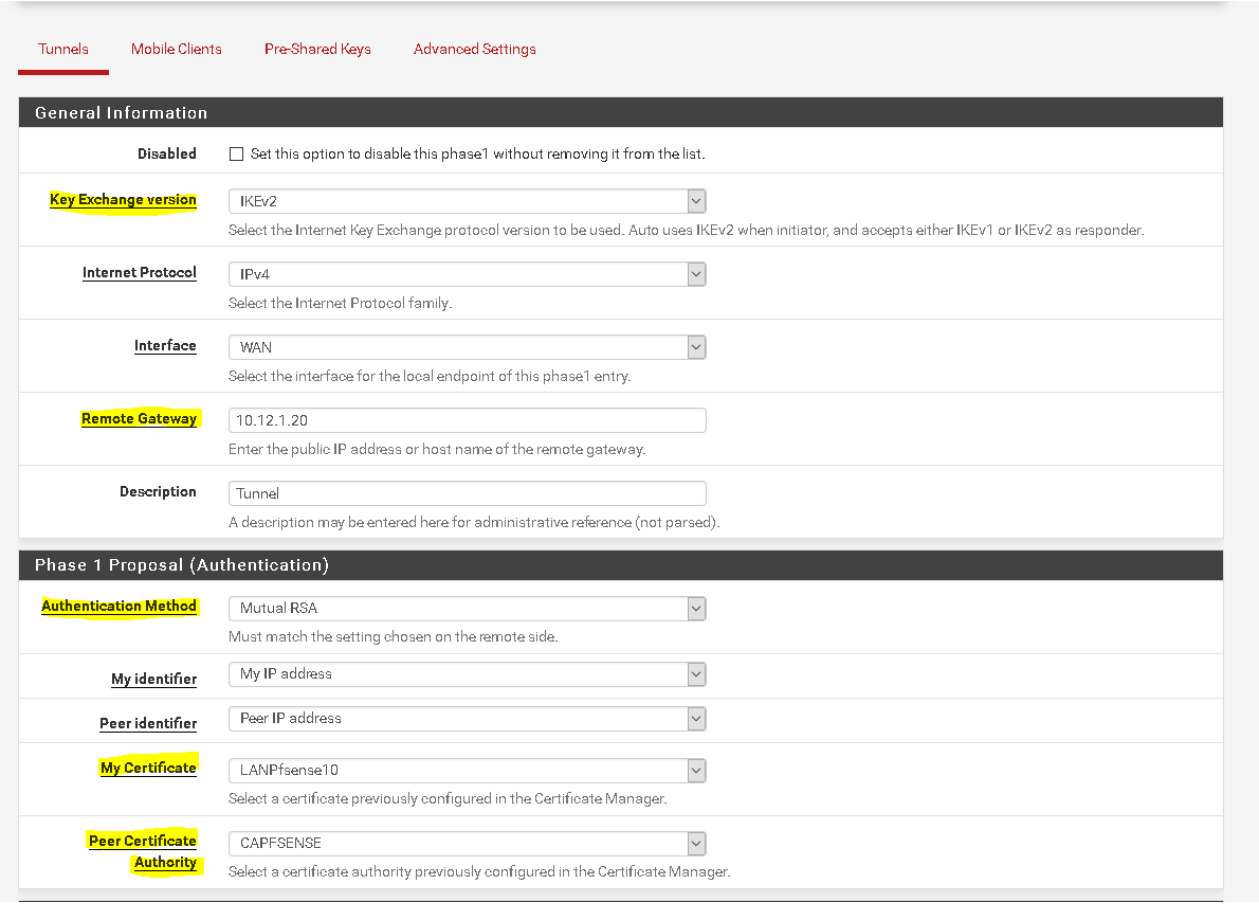
Le certificat sur le second serveur :



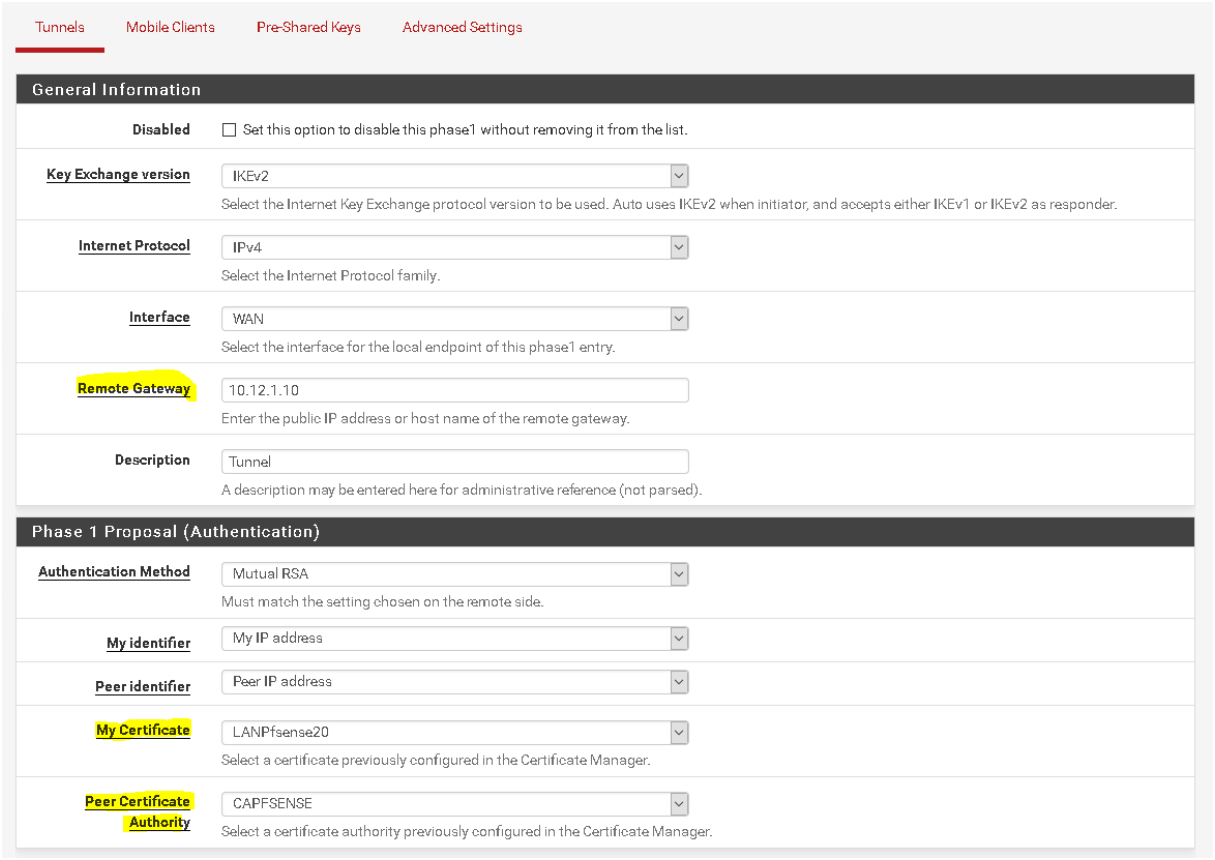
2- VPN – IPSec

On se rend dans VPN/IPSec pour ajouter sur les deux serveurs Pfsense un tunnel pointant vers le réseau WAN de chacun.

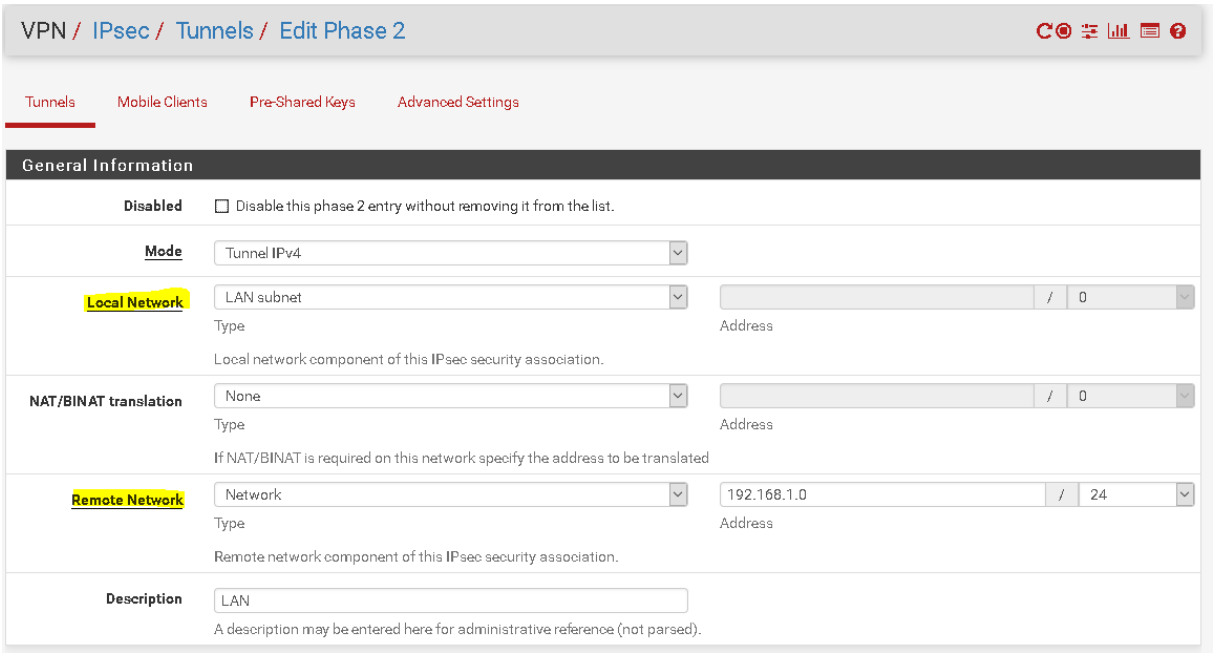
On précise la version Key Exchange, la gateway du serveur distant, la méthode d'authentification (Mutual RSA) ainsi que le certificat précédemment créé et l'authorité de certification.



On reproduit ensuite la même manipulation sur le second serveur.

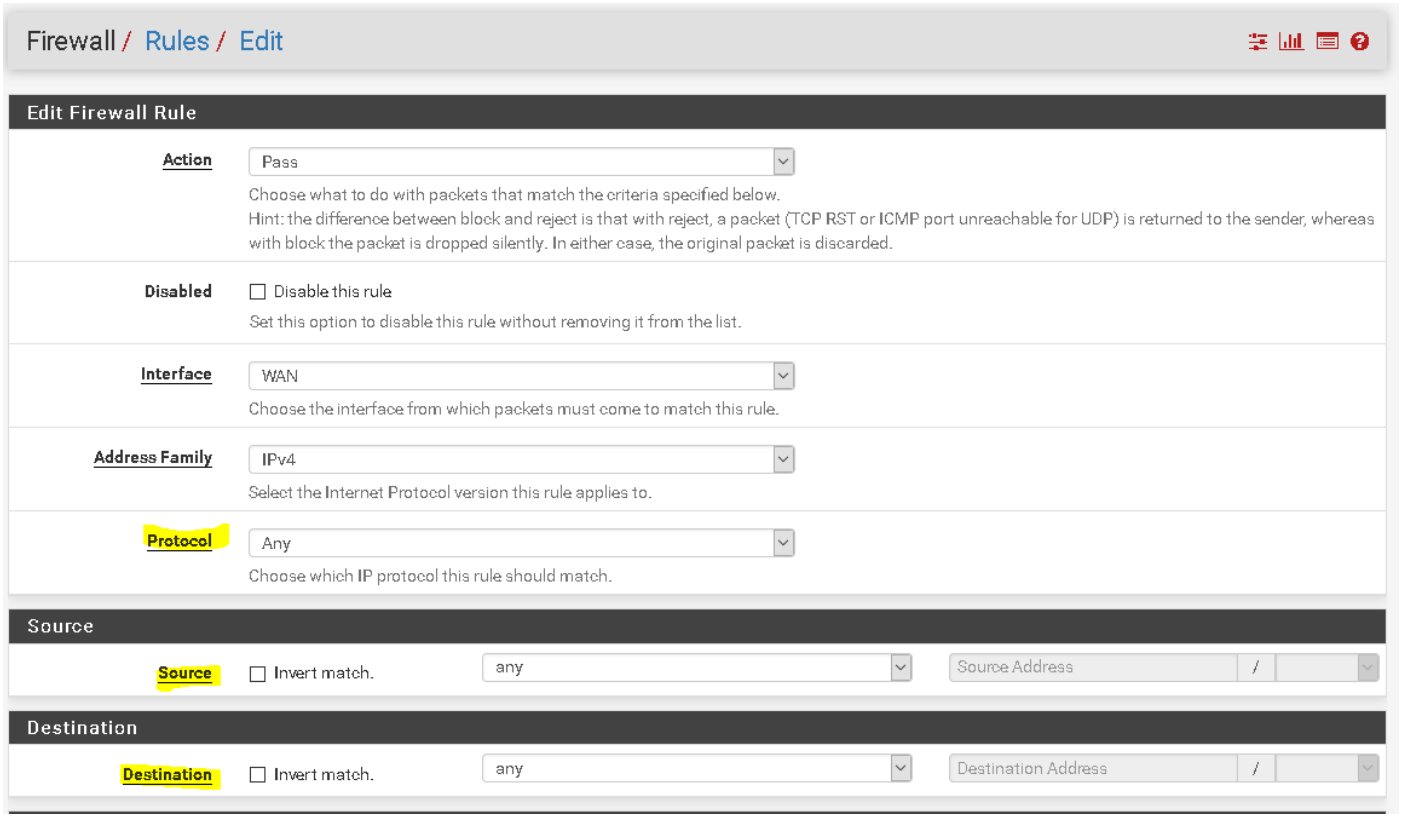


Puis on créer une « Phase » sur chacun des serveurs.

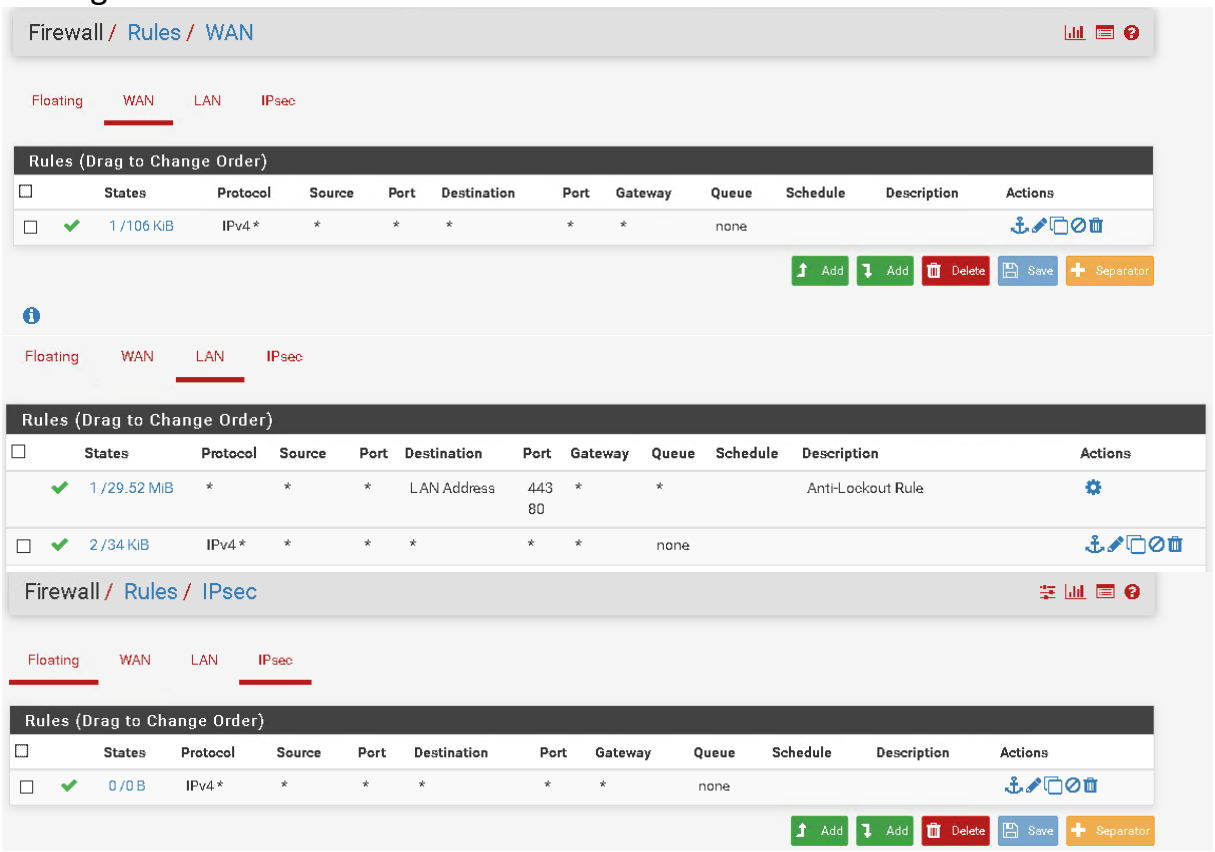


3- Règles de Firewall

Sur les deux serveurs on ouvre les ports any-any-any pour les règles WAN/LAN et IPSec.

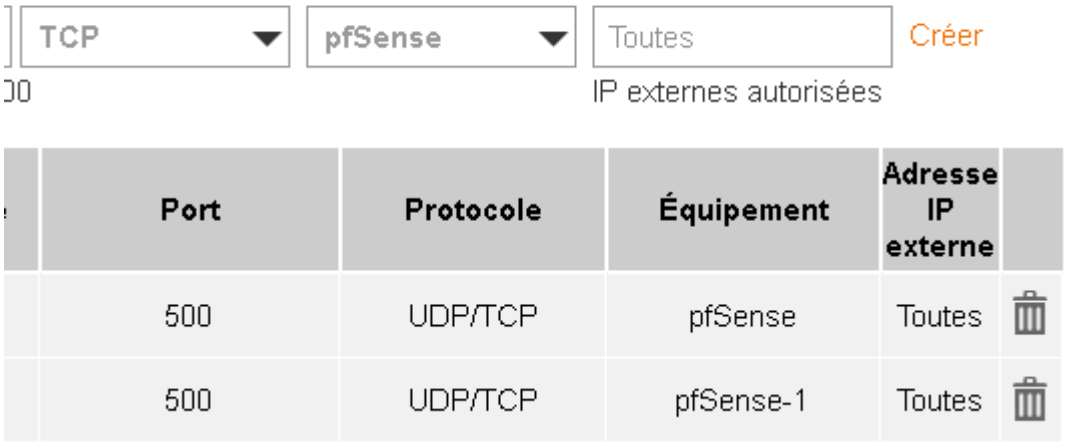


Les règles :



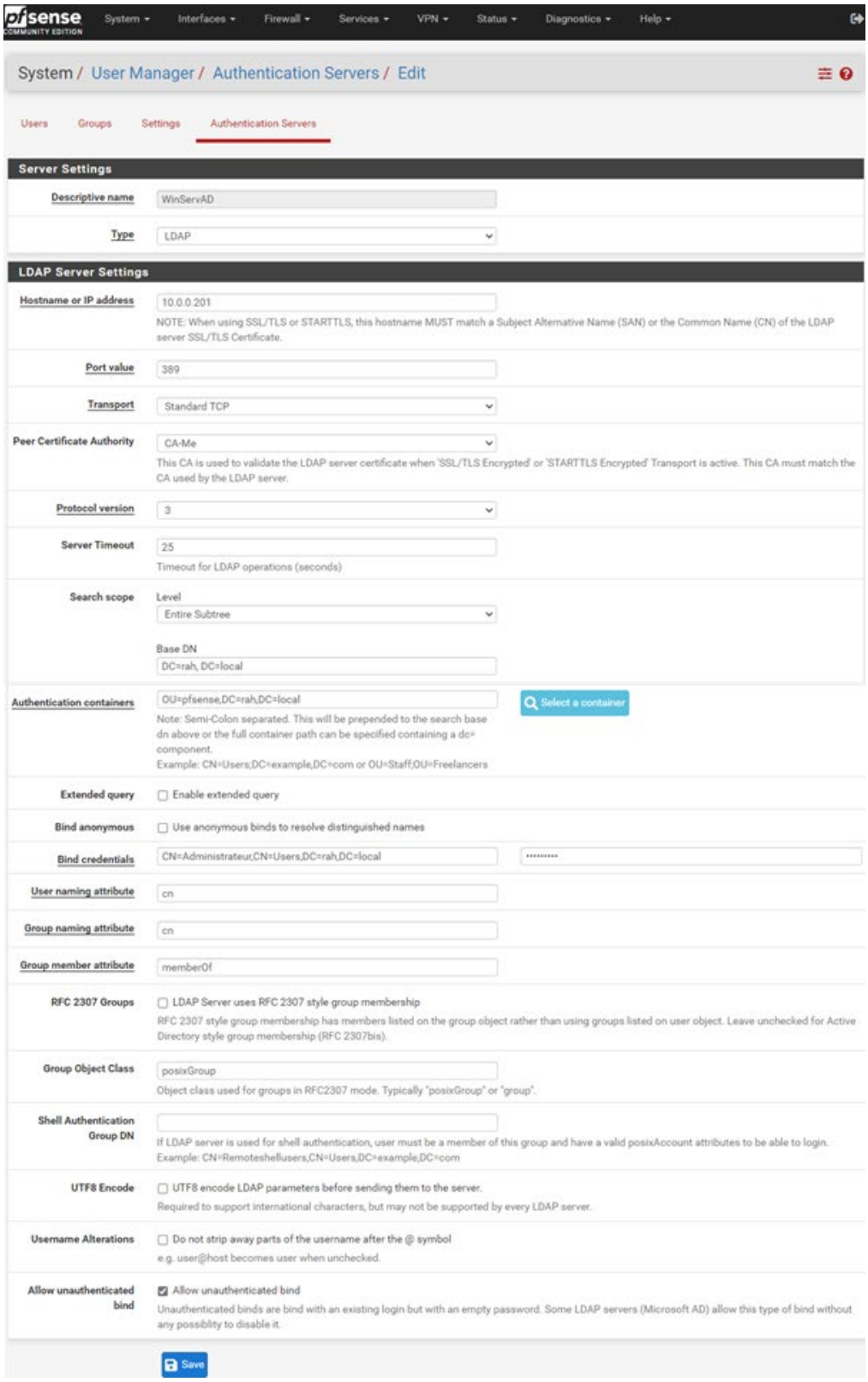
Pour que tout fonctionne nous avons dû ouvrir le port 500 sur le routeur.

le pare-feu (pour équipements IPv6).



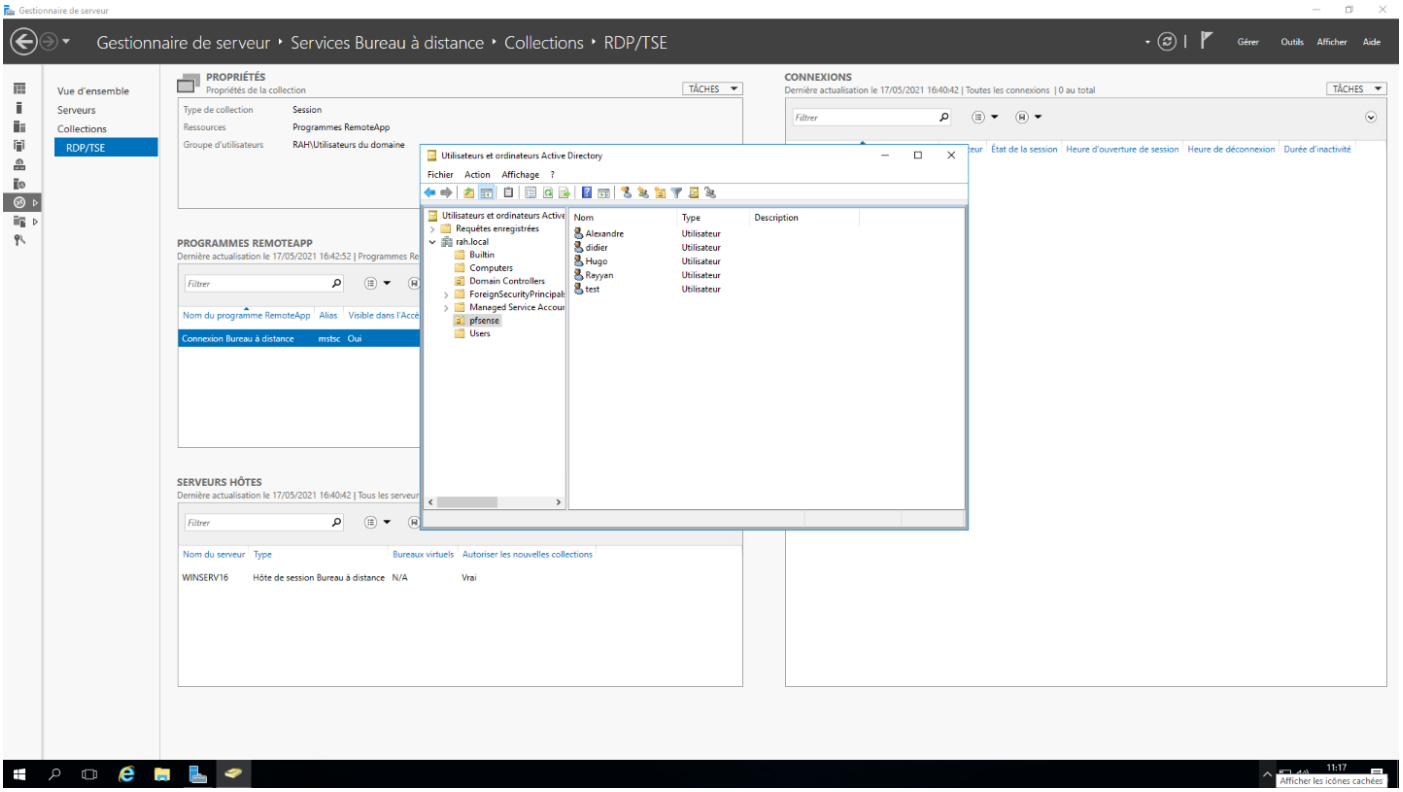
4- Authentication AD dans le Pfsense

On indique dans la configuration d'authentification du serveur l'adresse IP de ce dernier ainsi que le Bind Crédential qui permettra au Pfsense de s'authentifier dans l'AD, l'authentication containers où l'ont indique l'OU qu'il utilisera pour identifier les utilisateurs et enfin le certificat.



5- L’UO Pfsense dans l’AD

Nous pouvons voir ici les utilisateurs dans l’UO utilisé par Pfsense pour accorder l’accès au Vpn.



6- Test Final

Nous pouvons enfin tester la connectivité entre les deux Pfsense :