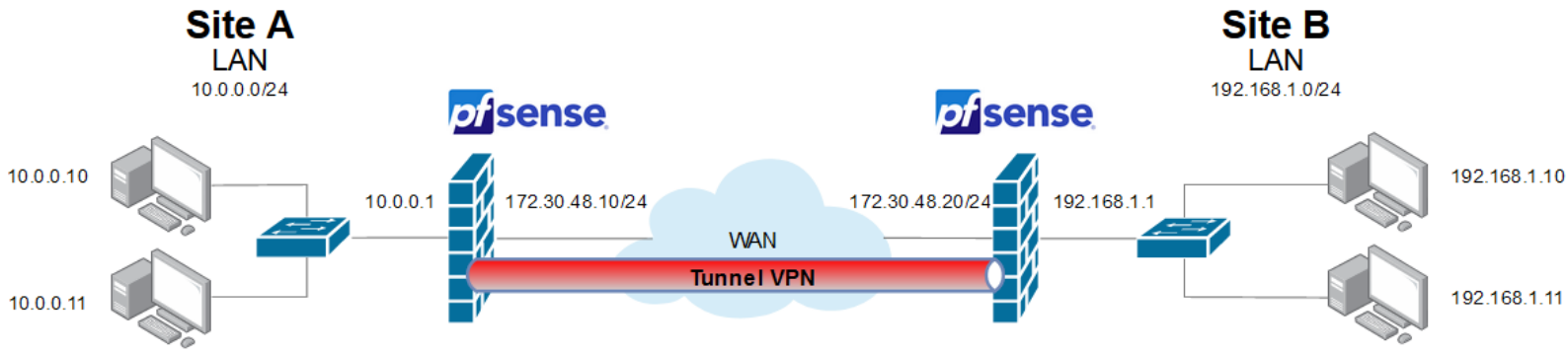
Mise en place d’un tunnel VPN IPsec avec Pfsense



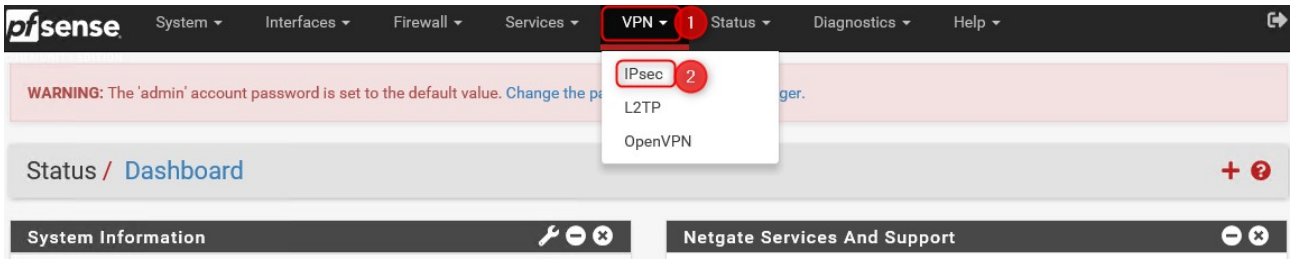
Prérequis :

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)

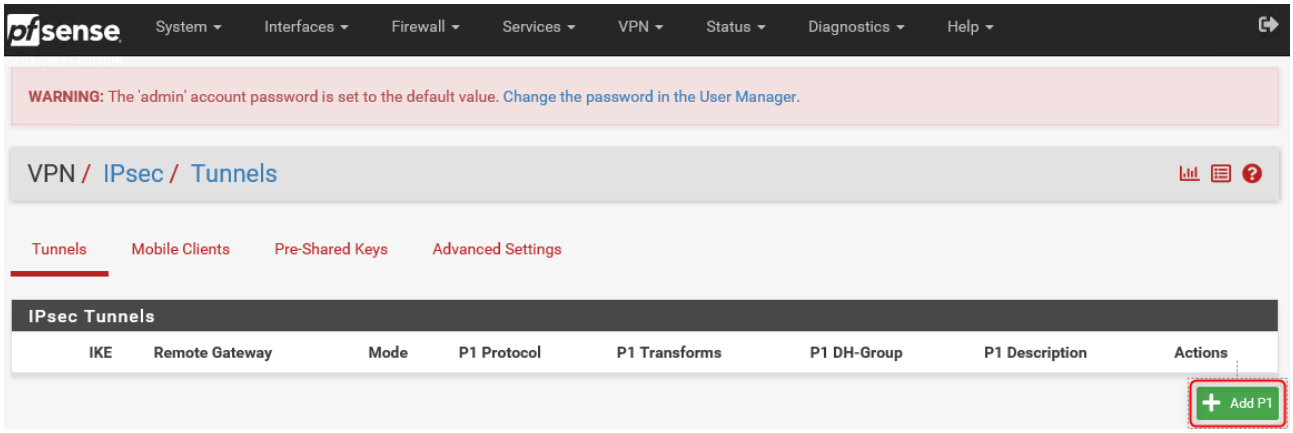
Pour les site A et B, au choix, vous pouvez installer des VM win10 ou Linux

Mise en Oeuvre :

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

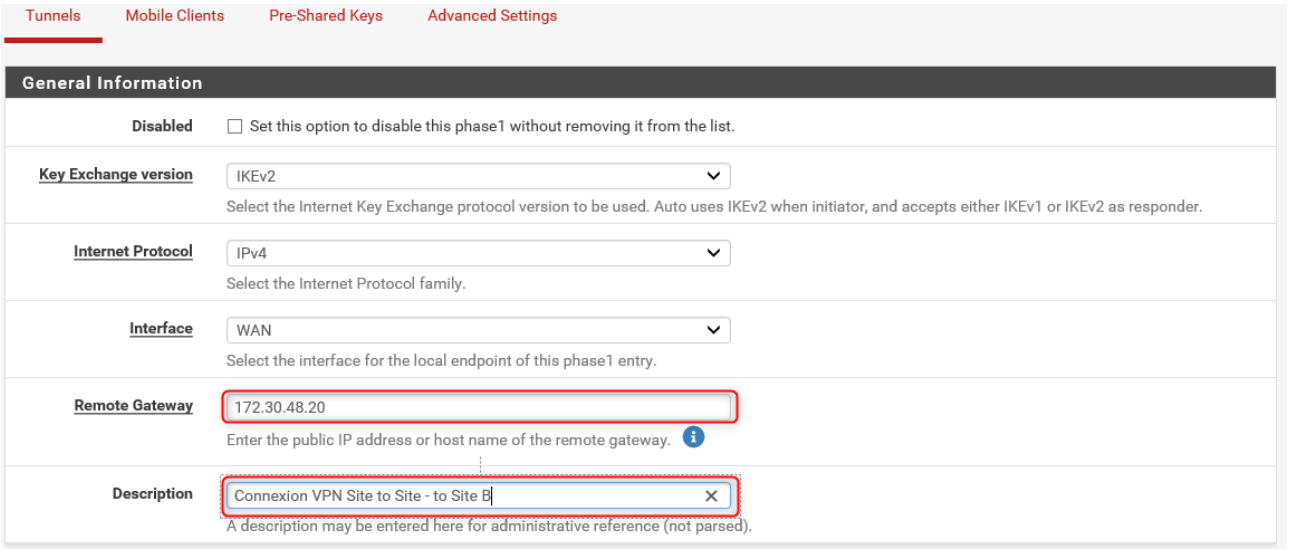


cliquez sur **Add P1** pour créer la Phase 1



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

Vous pouvez également entrer une description.

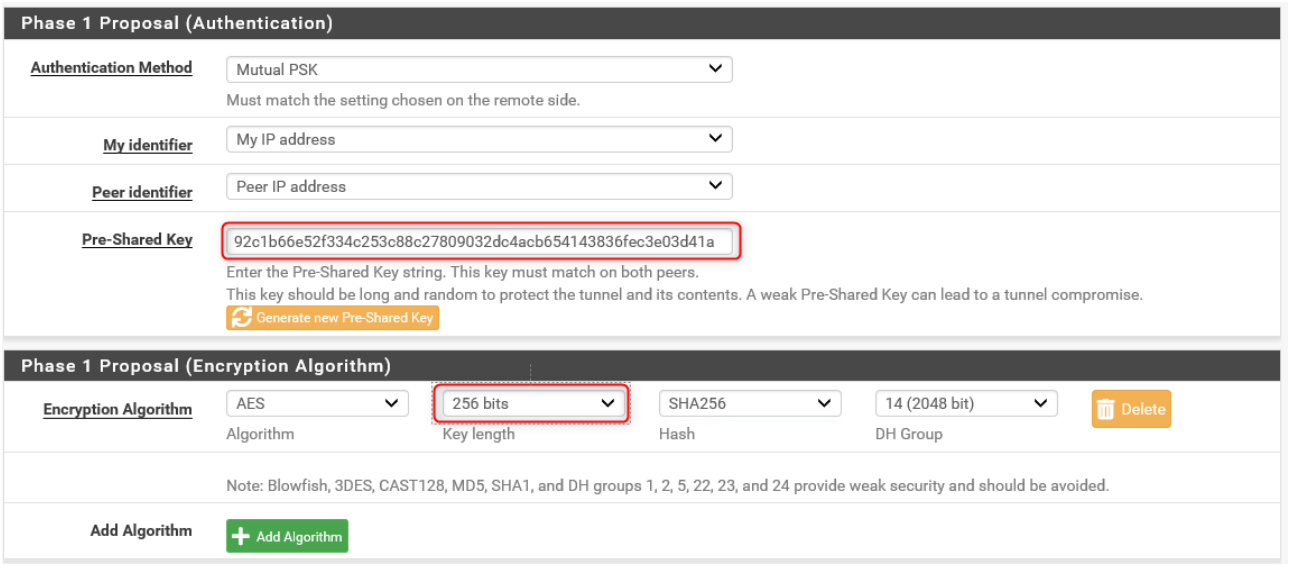


Dans la partie suivante, les pfsense utiliseront leur adresse IP comme identifiant.

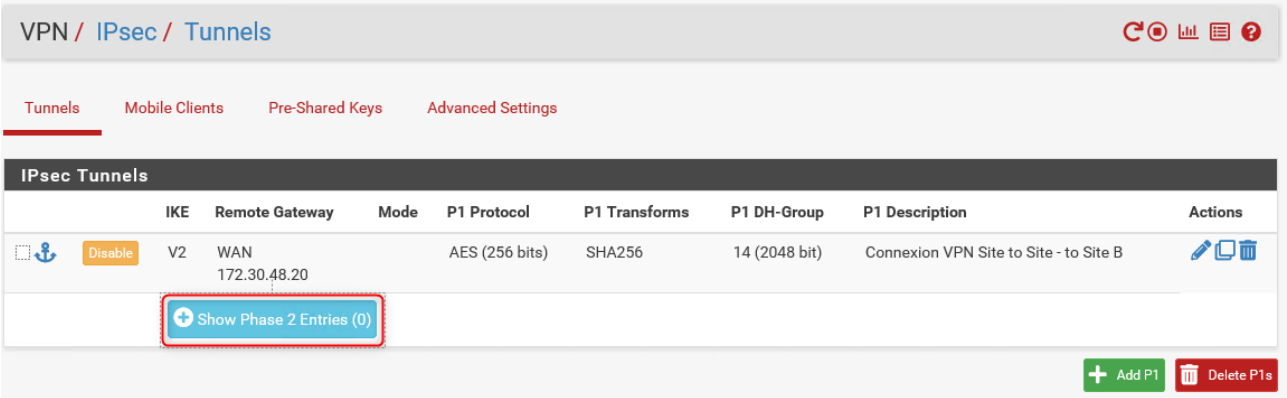
Nous utiliserons la clé pré-partagée, générez-en une

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

Et laisser les autres valeurs par défaut. Sauvegardez et appliquez

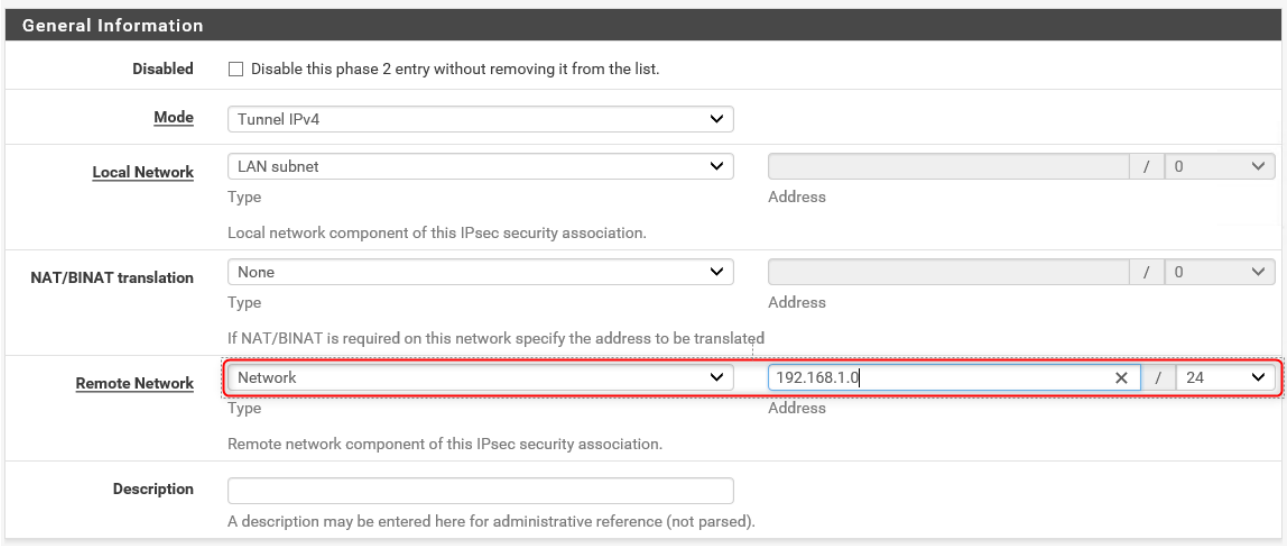


Passez à la phase 2

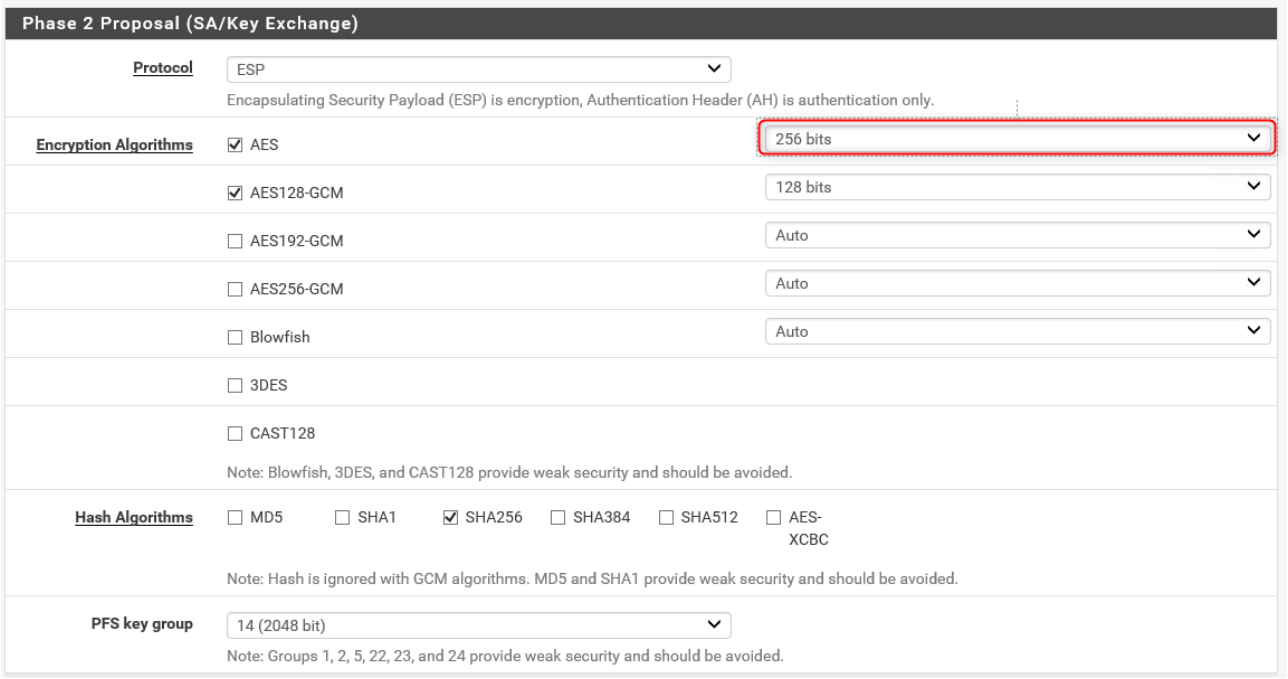


et cliquez sur **Add P2**

Définissiez le réseau LAN distant

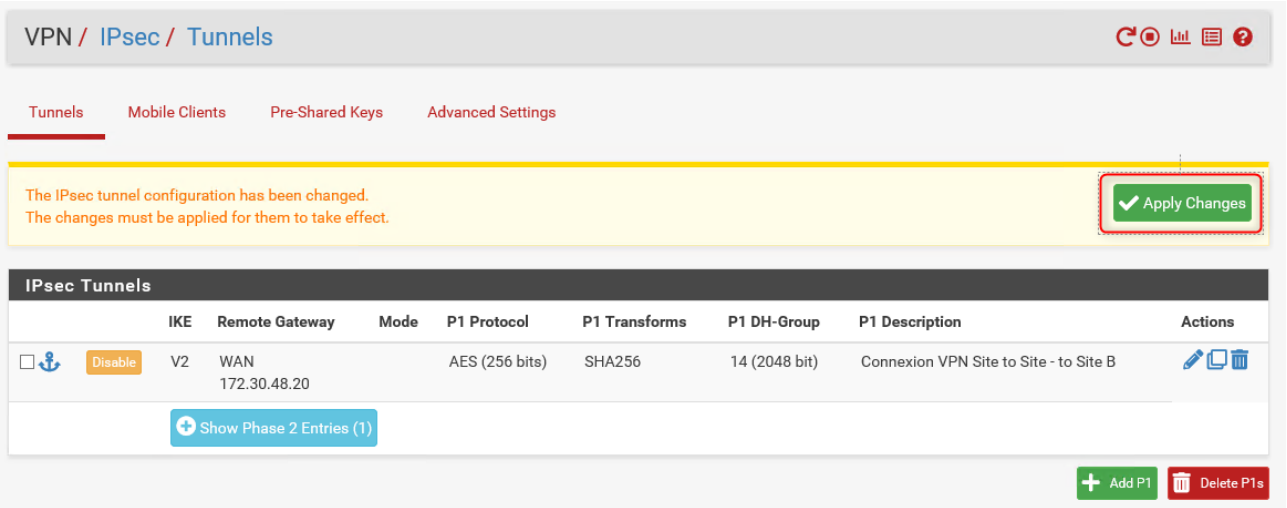


Choisissez le protocole ESP et un chiffrement AES 256 bits



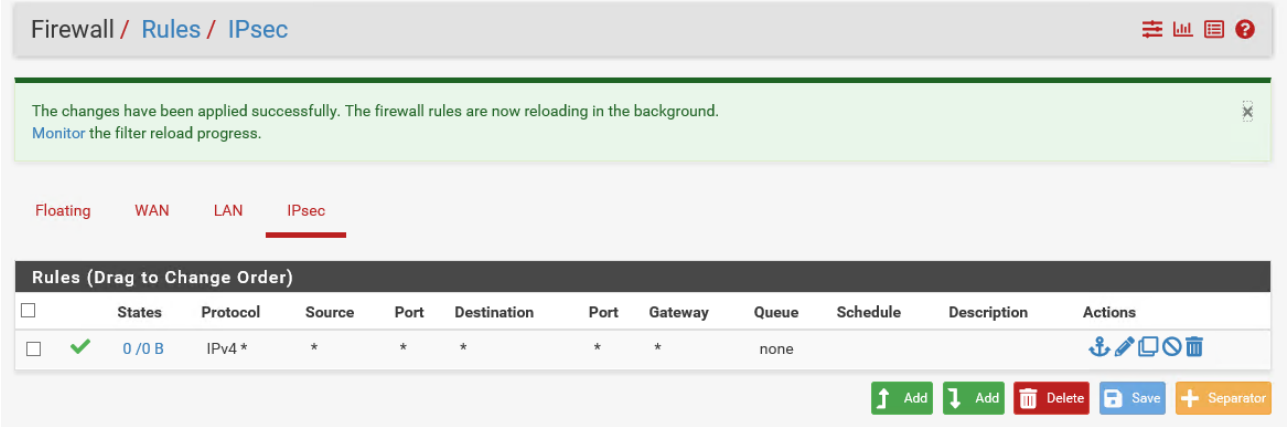
Laissez les autres valeurs par défaut.

Sauvegardez et appliquez les changements



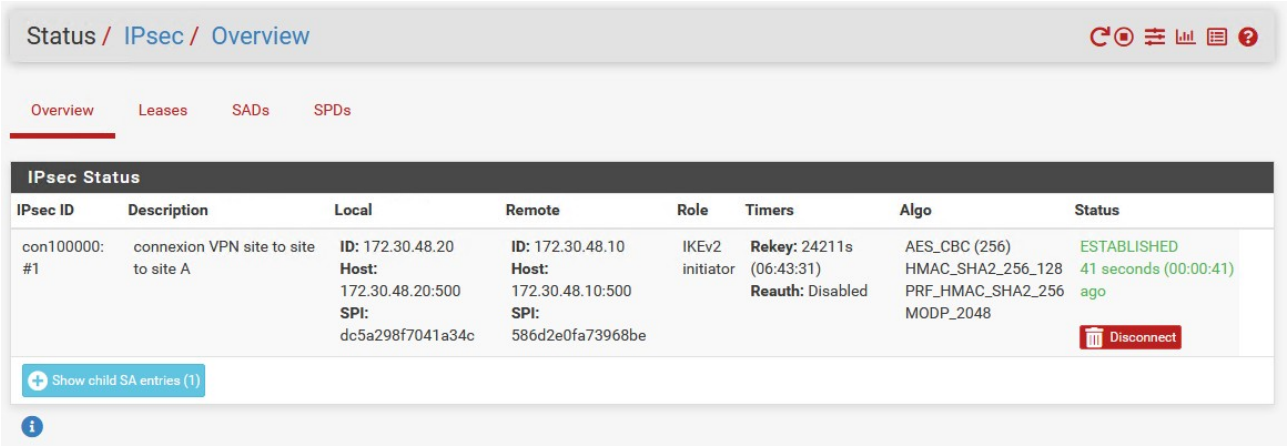
Faites ensuite la même configuration sur le firewall psfense du site B en adaptant les adresses IP.

Activez les règles de pare-feu afin de permettre au trafic de passer dans le tunnel VPN de monter



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

Cliquez sur connect VPN , vous devez avoir cela



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

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..