IPsec site-à-site avec pfsense

Installation et configuration de l'IPsec site-à-site avec pfsense pour un domaine

EHRET Louis

Table des matières

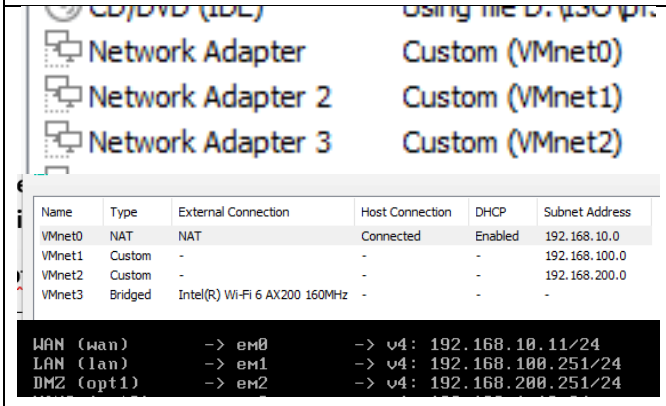
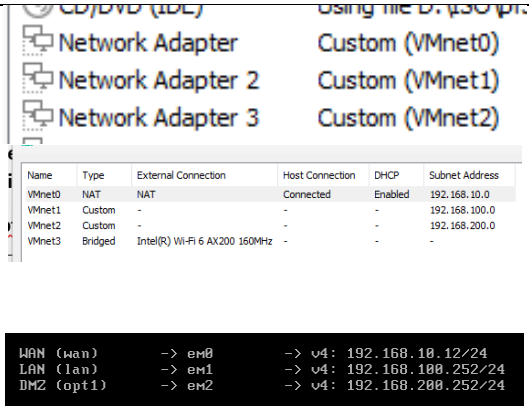
1. IPsec

IPSec signifie « Internet Protocol Security »

IPSec est un ensemble de protocoles (couche 3 modèle OSI) utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP. Réalisé dans le but de fonctionner avec le protocole IPv6, il fut adapté pour l'actuel protocole IP: IPv4. avec le protocole

Son but est d'authentifier et de chiffrer les données : le flux ne pourra être compréhensible que par le destinataire final (chiffrement).

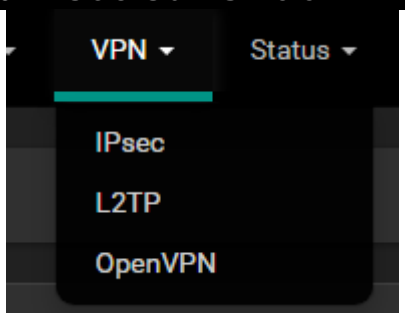
2. Configuration des postes

SECCIV-RTE-01	SECCIV-RTE-02
	

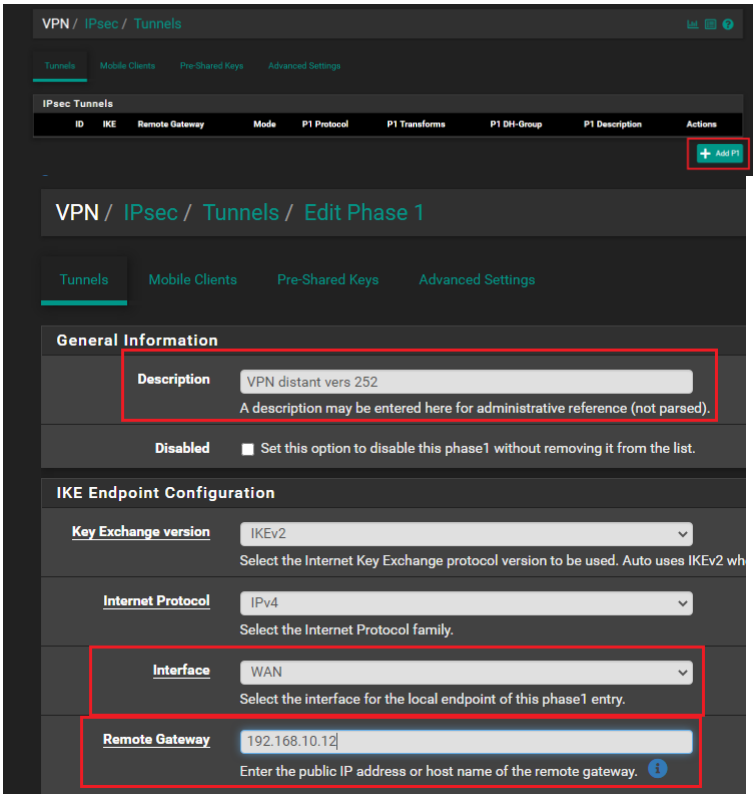
Nous allons utiliser les adresses WAN, donc directement connectés à internet, pour connecter les 2 pfsense. On va donc créer un pont chiffré entre 2 sites distants grâce au WAN. Les 2 pfsense vont communiquer via le WAN, qui est mon NAT dans ma configuration.

3. Mise en place d'IPsec sur SECCIV-RTE-01 (1er)

Pour effectuer l'ajout d'IPsec sur le premier serveur, se rendre sur le premier pfsense et accéder à VPN -> IPsec



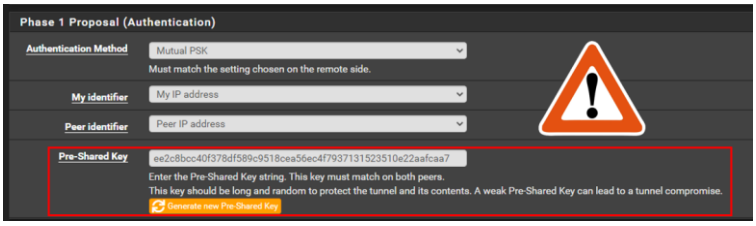
Nous allons ajouter un tunnel IPsec, cliquer sur Add

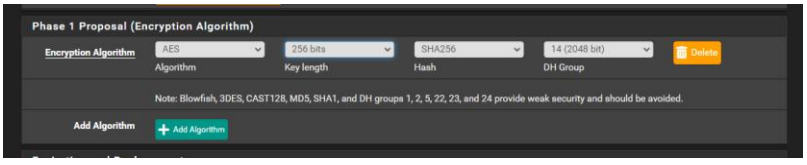


On va mettre une description, comme « VPN distant vers 252 » pour signifier que c'est un tunnel vers un autre pfsense

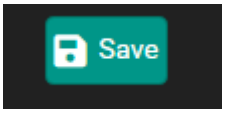
On indique l'IP WAN du pfsense distant, ici 192.168.10.12.

Pour l'authentification, nous avons choisi de générer une clé d'authentification Pour le chiffrement nous avons choisi du 256 bits en algorithme AES, hash SHA256. Il faut bien la retenir car il va falloir l'indiquer sur le pfsense distant 252.

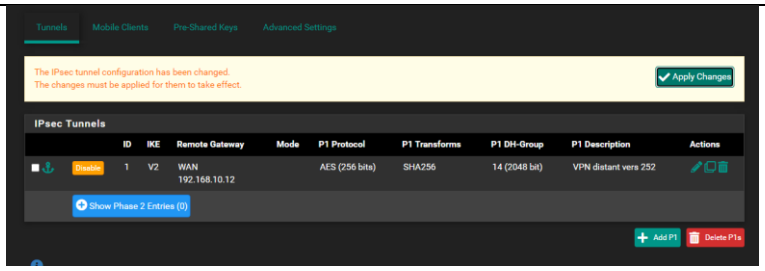




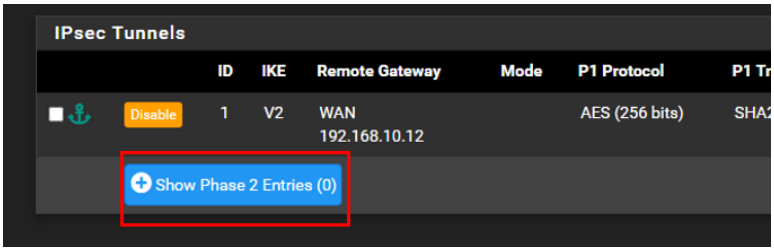
Rien d'autre à modifier, enregistrer



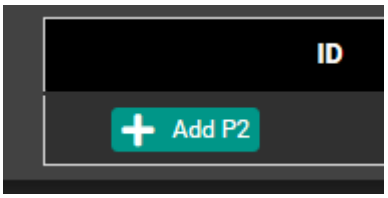
Premier tunnel, appliquer les changements.



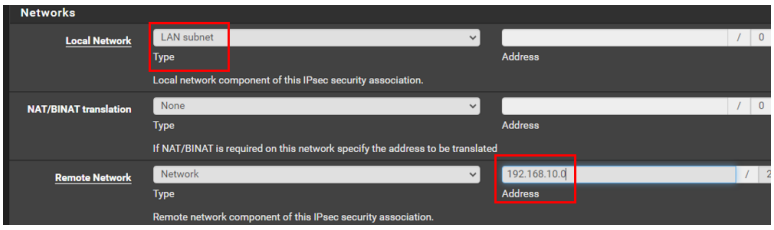
Il faut ensuite sauvegarder la configuration. Pour poursuivre, il faut cliquer sur le bouton « Show phase 2 entries »



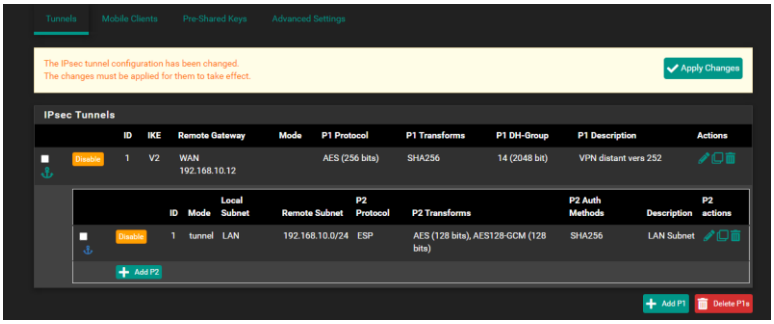
On va appuyer sur Add P2, pour ajouter un réseau.



On indique c'est via le réseau LAN Subnet qui est bien notre réseau local, et le réseau distant, 192.168.10.0 car 192.168.10.12 est dans ce sous-réseau, comme le nôtre. Nous allons donc pouvoir communiquer.



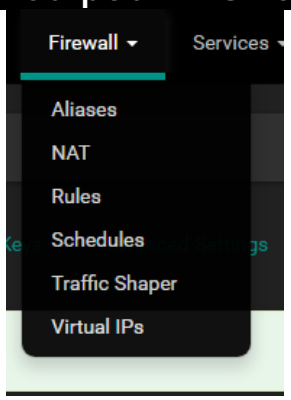
Nous avons nos 2 configurations, enregistrer les changements en appuyant sur « Apply Changes ».



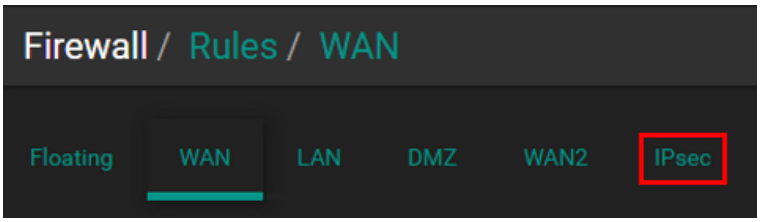
4. Règle de pare-feu pour IPSEC

On va mettre également une règle de pare-feu pour IPsec,

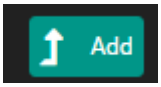
Se rendre dans Firewall -> Rules



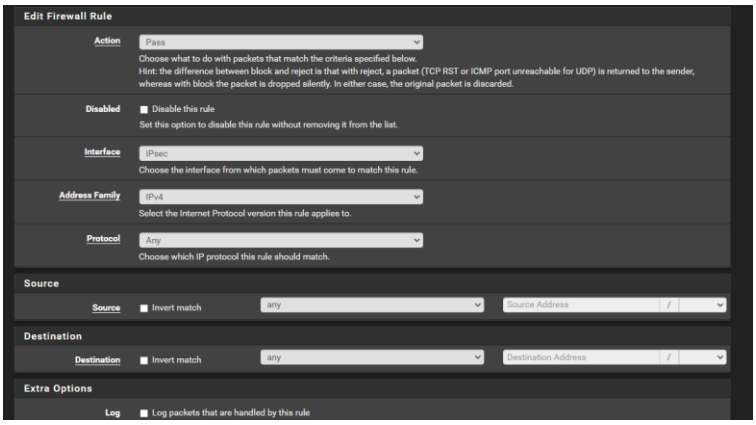
Cliquer sur IPsec, car nous voulons configurer une règle sur l'interface ipsec.



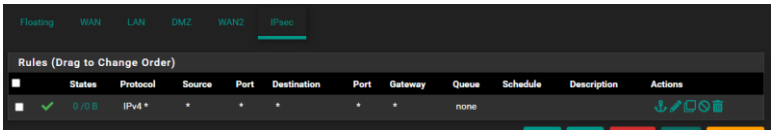
Cliquer sur add



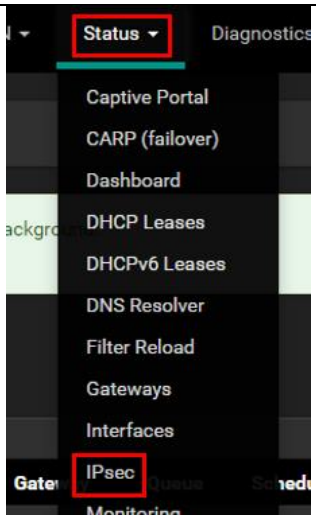
On va autoriser pour la configuration la règle Ipsec donc ouvert pour tout vers tout.



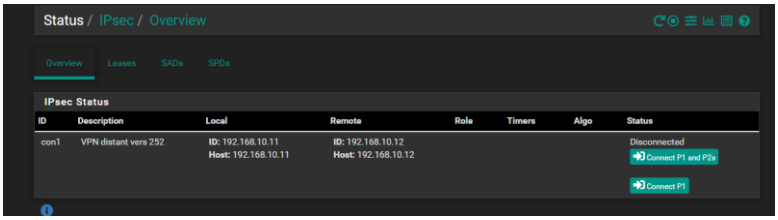
Elle a bien été ajoutée.



Ensuite, une fois la configuration faite, on peut se rendre sur Status -> IPsec pour vérifier si la configuration a été effectuée.



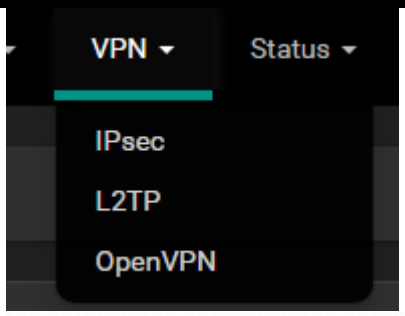
Nous avons bien une configuration pour un tunnel IPsec de prête.



5. Mise en place d'IPsec sur SECCIV-RTE-02 (2eme)

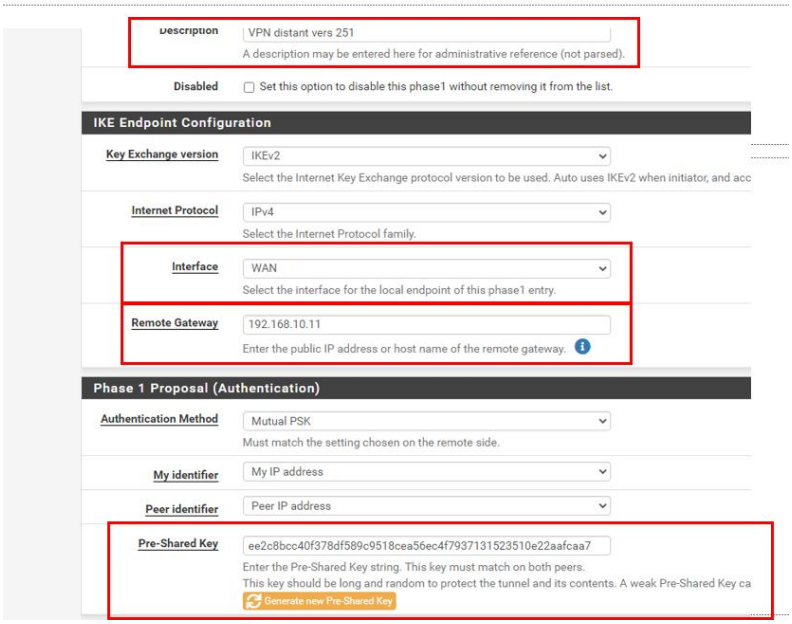
On va mettre en place l'IPsec sur le deuxième serveur

VPN -> IPsec

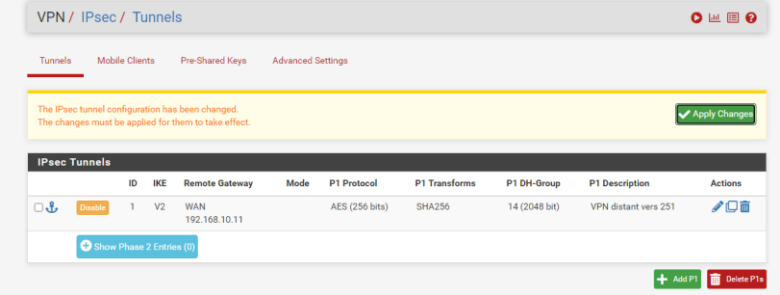


On fait la même configuration que sur le premier, en renseignant les IP du premier pfsense.

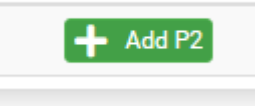
Et renseigner, copier-coller, la clé partagée du premier serveur sur le deuxième, donc celui-ci.



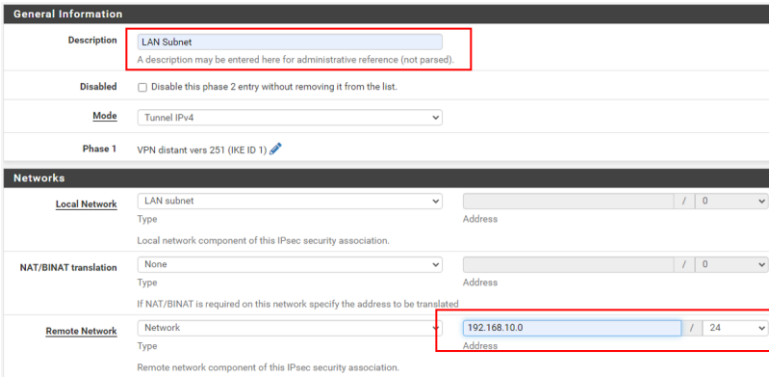
Nous avons bien configuré notre premier tunnel IPsec.



On va ajouter comme avant un réseau, avec add P2

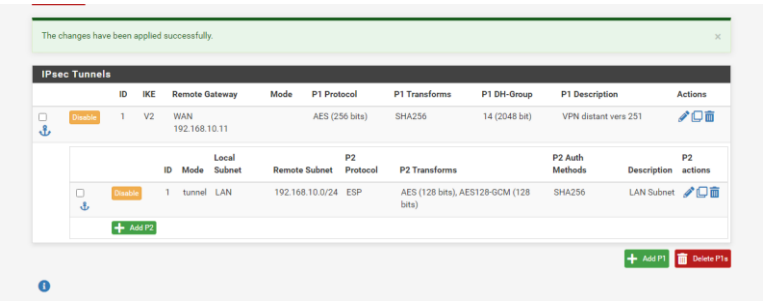


De même ici, on renseigne le réseau lan comme réseau local et le réseau local 192.168.10.0

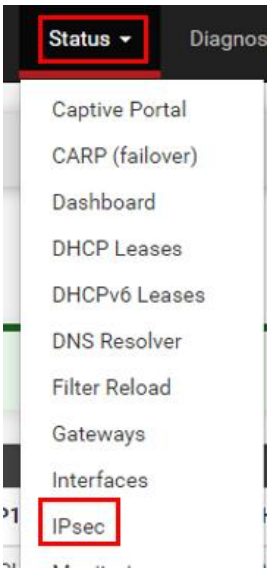


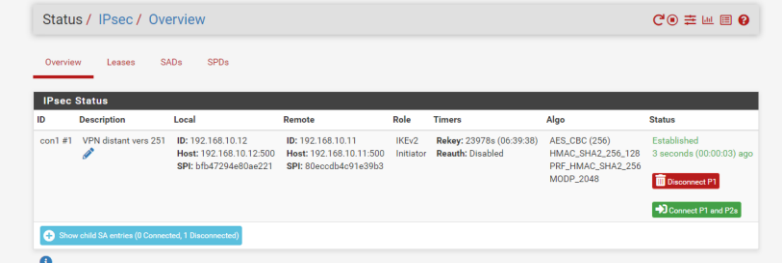
On a bien nos 2 configurations, enregistrer les modifications.

Bien revérifier que tout est correct



Et si on retourne dans Status -> IPsec sur l'un des deux pfsense,



On remarque que la connexion a été établie avec « Established » qui a été ajouté. Notre connexion IPsec entre les 2 pfsense d'un domaine a fonctionné.	

Notre connexion IPsec est fonctionnelle et opérationnelle.