



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	2
2. Configuration des postes	2
3. Mise en place d'IPsec sur SECCIV-RTE-01 (1 ^{er})	3
4. Règle de pare-feu pour IPSEC	5
5. Mise en place d'IPsec sur SECCIV-RTE-02 (2eme)	6

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

CD/DVD (IDE) Using file D:\ISO\pr...

- Network Adapter Custom (VMnet0)
- Network Adapter 2 Custom (VMnet1)
- Network Adapter 3 Custom (VMnet2)

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	NAT	NAT	Connected	Enabled	192.168.10.0
VMnet1	Custom	-	-	-	192.168.100.0
VMnet2	Custom	-	-	-	192.168.200.0
VMnet3	Bridged	Intel(R) Wi-Fi 6 AX200 160MHz	-	-	-

```

WAN (wan)    -> em0    -> v4: 192.168.10.11/24
LAN (lan)    -> em1    -> v4: 192.168.100.251/24
DMZ (opt1)   -> em2    -> v4: 192.168.200.251/24

```

SECCIV-RTE-02

CD/DVD (IDE) Using file D:\ISO\pr...

- Network Adapter Custom (VMnet0)
- Network Adapter 2 Custom (VMnet1)
- Network Adapter 3 Custom (VMnet2)

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	NAT	NAT	Connected	Enabled	192.168.10.0
VMnet1	Custom	-	-	-	192.168.100.0
VMnet2	Custom	-	-	-	192.168.200.0
VMnet3	Bridged	Intel(R) Wi-Fi 6 AX200 160MHz	-	-	-

```

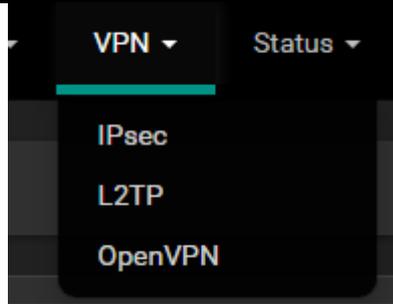
WAN (wan)    -> em0    -> v4: 192.168.10.12/24
LAN (lan)    -> em1    -> v4: 192.168.100.252/24
DMZ (opt1)   -> em2    -> v4: 192.168.200.252/24

```

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 (1^{er})

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



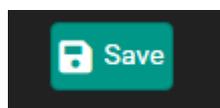
Nous allons ajouter un tunnel IPsec, cliquer sur Add

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.

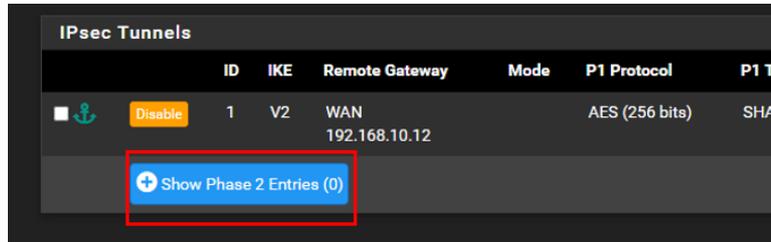
Rien d'autre à modifier, enregistrer



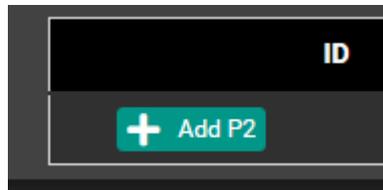
Premier tunnel, appliquer les changements.



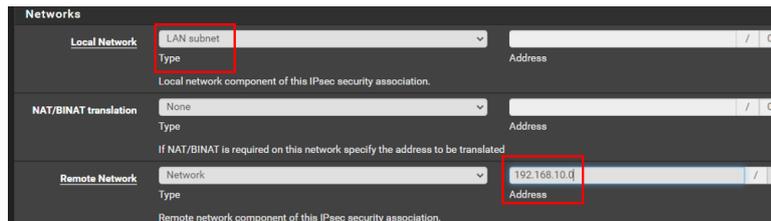
Il faut ensuite sauvegarder la configuration. Pour poursuivre, il faut cliquer sur le bouton « Show phase 2 entrees »



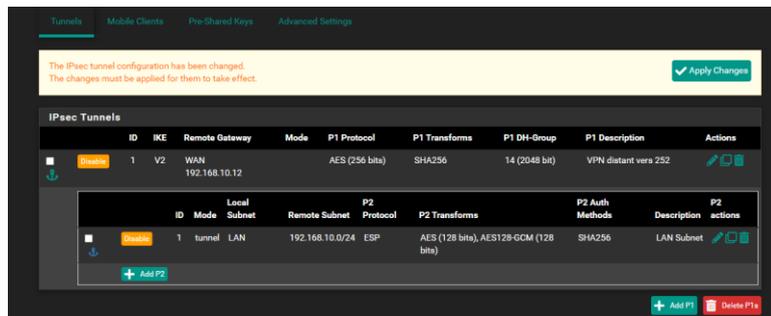
On va appuyer sur Add P2, pour ajouter un réseau.



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.



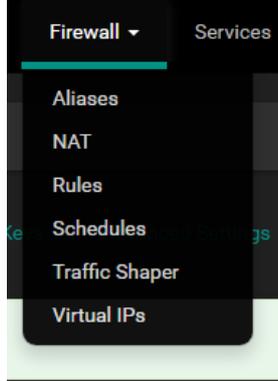
Nous avons nos 2 configurations, enregistrer les changements en appuyant sur « Apply Changes ».



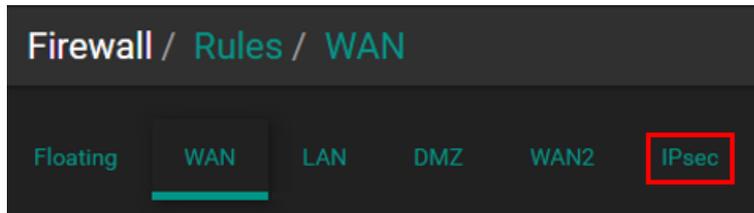
4. Règle de pare-feu pour IPSEC

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

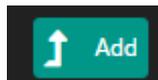
Se rendre dans Firewall -> Rules



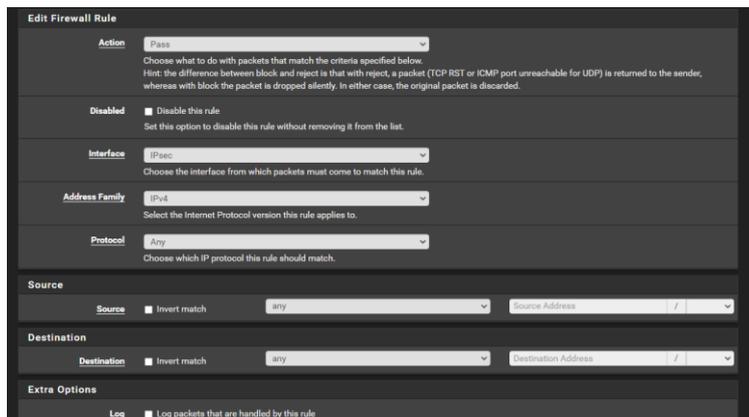
Cliquer sur IPsec, car nous voulons configurer une règle sur l'interface ipsec.



Cliquer sur add



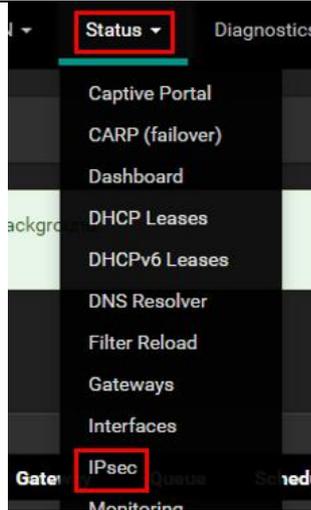
On va autoriser pour la configuration la règle Ipsec donc ouvert pour tout vers tout.



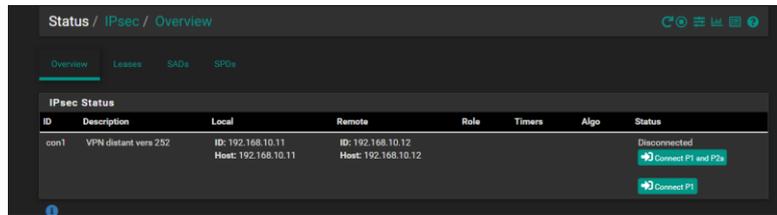
Elle a bien été ajoutée.



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



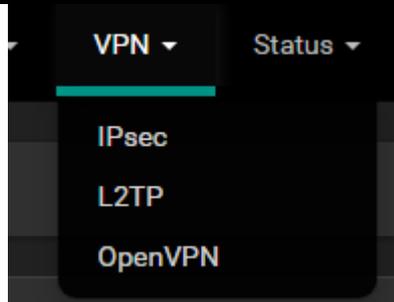
Nous avons bien une configuration pour un tunnel IPsec de prêt.



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

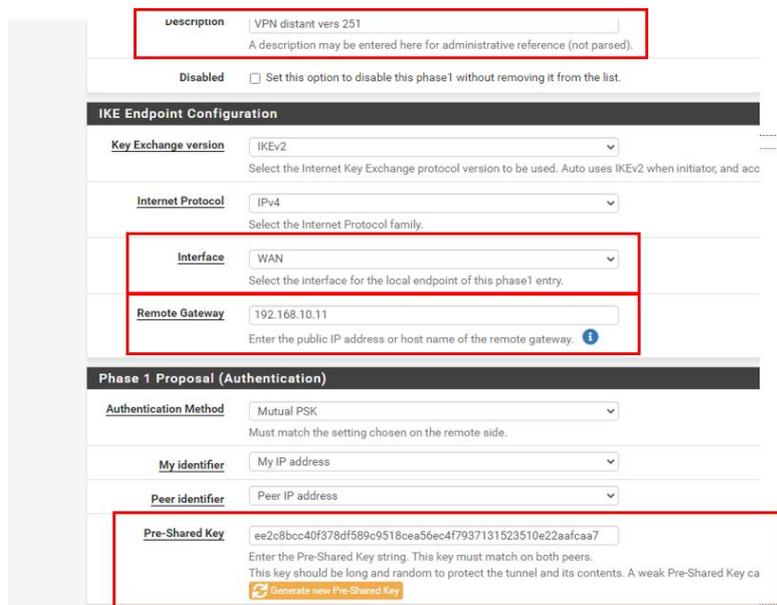
On va mettre en place l'IPsec sur le deuxième serveur

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 vérifier 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.

The screenshot shows the pfSense IPsec Status page. The main heading is 'IPsec Status'. Below it, there is a table with columns: ID, Description, Local, Remote, Role, Timers, Algo, and Status. The table contains one entry with ID 'con1 #1' and Description 'VPN distant vers 251'. The Local and Remote columns show IP addresses and SPIs. The Status column shows 'Established' with a timestamp '3 seconds (00:00:03) ago'. There are also buttons for 'Disconnect P1' and 'Connect P1 and P2s'.

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #1	VPN distant vers 251	ID: 192.168.10.12 Host: 192.168.10.12:500 SPI: bfb47294e80ae221	ID: 192.168.10.11 Host: 192.168.10.11:500 SPI: 80eccdb4c91e39b3	IKEv2 Initiator	Rekey: 23978s (06:39:38) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established 3 seconds (00:00:03) ago

Notre connexion IPsec est fonctionnelle et opérationnelle.