COMPTE-RENDU : VPN IPSec PfSense

I) Contexte :

Nous souhaitons relier 2 réseaux privés différents et distant. Pour cela, nous allons créer une liaison sécurisée entre les deux réseaux via PfSense en utilisant un VPN avec le protocole IPSec pour la tunnellisation.

II) Prérequis :

Nous avons besoin de 2 réseaux distinct composé chacun d'une machine Pare-feu (PfSense) et d'une machine station de travail sous Windows 10. Cela est nécessaire à la configuration de notre VPN mais servira aussi à tester celui-ci.

Il faudra aussi éditer sur la logiciel VMware, le « **VMnet8 »** servant au NAT car l'adresse de base 192.168.x.x peut créer un conflit et gêner à la communication entre machine.

Voilà notre configuration pour ce TP :

1. **Réseau 1 :**
   - Machine PfSense 01 :
     - Nom de la machine : pfSense01
     - Network Adapter 1 : NAT / WAN IpV4 : 80.10.200.130/24
     - Network Adapter 2 : VMnet0 / LAN IpV4 : 192.168.0.1/24
   - Machine Windows 01 :
     - Nom de l'ordinateur : PcWork01
     - Network Adapter : VMnet0 / LAN IpV4 : 192.168.0.10/24
2. **Réseau 2 :**
   - Machine PfSense 02 :
     - Nom de la machine : pfSense02
     - Network Adapter 1 : NAT / WAN IpV4 : 80.10.200.131/24
     - Network Adapter 2 : VMnet2 / LAN IpV4 : 172.68.0.1/24
   - Machine Windows 02 :
     - Nom de l'ordinateur : PcWork02
     - Network Adapter : VMnet2 / LAN IpV4 : 172.68.0.10/24

Il faut aussi désactiver préalablement les Pares-feux Windows sur nos machines.

Il faudrait aussi ajouter **« IPsec »** sur le Dashboard de PfSense en cliquant sur **« + »**.

III) Tutoriel :

Pour créer le VPN, il faut aller dans **« VPN »** puis sélectionner **« IPsec »**. Pour ajouter un Tunnel, il faudra rentrer 2 Phases, une pour le WAN et une pour le LAN.

Voici les étapes à suivre et les lignes à éditer pour les Phases puis à appliquer sur les 2 machines Pare-Feu :

P1 WAN (En cliquant sur **« Add P1 »**) :

- Key Exchange Version : **IKEv1**
- Internet Protocol : **IPv4**
- Interface : **WAN**
- Remote Gateway : On rentre ici l'adresse WAN PfSense du réseau qu'on souhaite joindre. Ce qui nous donne avec notre configuration actuelle et selon les machines :
  - De pfSense01 vers PfSense02 : 80.10.200.131
  - De pfSense02 vers PfSense01 : 80.10.200.130
- Description : On rentre ce qu'on veut, c'est pour mieux s'y retrouver dans notre Phase.
- My identifier / Peer identifier : On met en **«User distinguished name»** puis on met ensuite un identifiant unique dans le monde comme une adresse mail. On mettra ici **jeremy.joudon@gmail.com**
- Pre-Shared Key : il est préférable de mettre une clé compliquée pour s'identifier en situation normale mais ici on mettra **« toto »** vu qu'on est en Lab.
- Il nous reste plus qu'à **Save**

P2 LAN (En cliquant sur **« Show Phase 2 Entries »** et **« Add P2 »** :

- Mode : **Tunnel IPv4**
- Local network : **LAN subnet**
- NAT/BINAT translation : **None**
- Remote Network : **Network** puis à droite, on met l'IP Lan correspondante avec son masque de sous-réseau au PfSense du réseau qu'on souhaite joindre. Comme précédemment on a 2 configurations selon la machine :
  - De PfSense01 vers PfSense02 : 172.68.0.1/24
  - De PfSense02 vers PfSense01 : 192.168.0.1/24
- Description : Pareil que pour la P1.
- Il nous reste plus qu'à **Save**.
- Cette fois ci, il faut en plus cliquer sur **« Apply changes »**.

La configuration des 2 Phases étant terminé, il faut maintenant autoriser certaines règles à notre Pare-Feu pour le fonctionnement de notre VPN IPsec.

On va dans « Firewall » et ensuite « Rules ». Il nous faut ajouter 2 règles dans **« WAN »** et une dans **« IPsec »** en utilisant le bouton **« Add »**.

On commence par le WAN :

1. Autorisation Port 4500 IPsec NAT-T :
    - Action : **Pass**
    - Interface : **WAN**
    - Address Family : **IPv4**
    - Protocol : **UDP**
    - Destination Port Range : **IPsec NAT-T (4500)**

2. Autorisation Port 500 ISAKMP :
    - Action : **Pass**
    - Interface : **WAN**
    - Address Family : **IPv4**
    - Protocol : **UDP**
    - Destination Port Range : **IPsec NAT-T (500)**

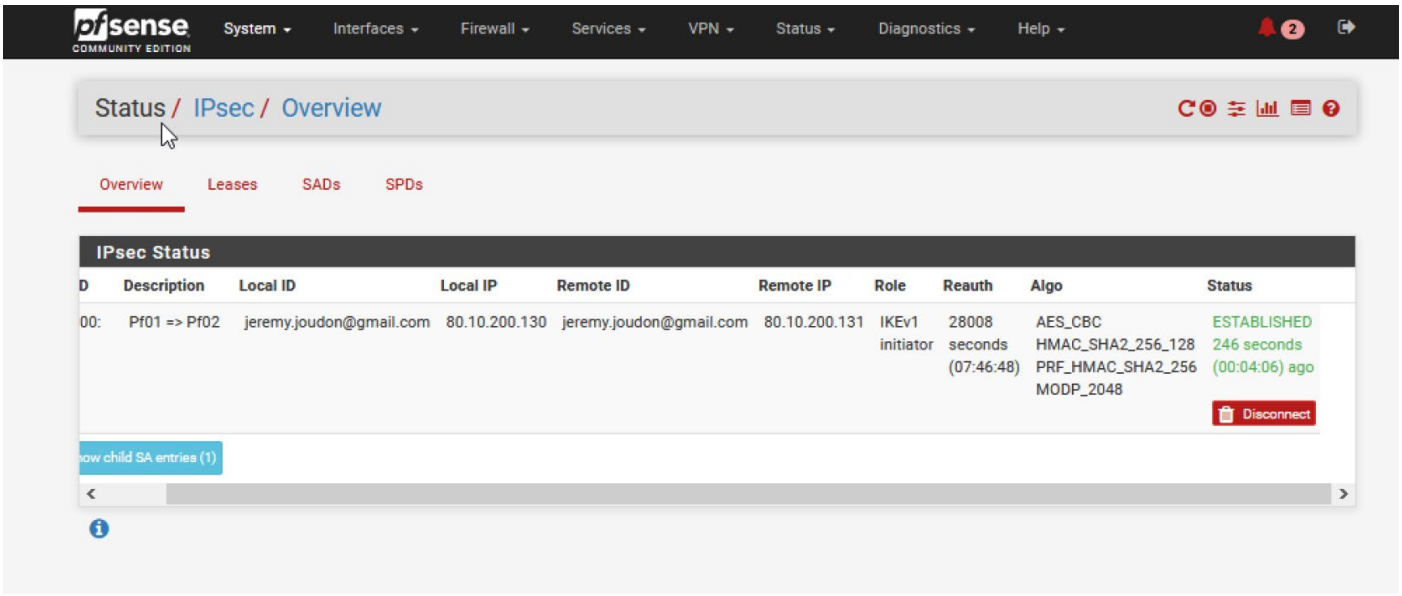
On termine donc avec une règle pour « IPsec » :

1. Autorisation de tous les protocoles :
    - Action : **Pass**
    - Interface : **IPsec**
    - Address Family : **IPv4**
    - Protocol : **Any**

Il faut encore une fois cliquer sur **« Apply changes »**.

IV) Mode opératoire :

Pour allumer le VPN après la configuration, il faut cliquer sur **« IPsec »** sur le Dashboard puis une fois dans le menu, défiler à droite et cliquer sur **« Connect »**. On se retrouve normalement avec le **« Status »** suivant :



On voit bien que notre VPN est actif et connecté vu qu'il est marqué **« ESTABLISHED »** en vert. Il faut savoir que la connexion se fera automatiquement sans le besoin de cliquer sur **« Connect »** si les deux pares-feux sont allumés et que leur configuration n'a pas changé.

On va donc maintenant vérifier avec nos deux machines si elles arrivent à communiquer entre elles avec la commande **« Ping » :**

Machine01 (192.168.0.10/24) à Machine02 (172.68.0.10/24) :

```
Envoi d'une requête 'Ping'  172.68.0.10 avec 32 octets de données :
Réponse de 172.68.0.10 : octets=32 temps<1ms TTL=126
Réponse de 172.68.0.10 : octets=32 temps<1ms TTL=126
Réponse de 172.68.0.10 : octets=32 temps<1ms TTL=126
Réponse de 172.68.0.10 : octets=32 temps<1ms TTL=126

Statistiques Ping pour 172.68.0.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Machine02(172.68.0.10/24) à Machine01(192.168.0.10/24) :

```
Envoi d'une requête 'Ping'  192.168.0.10 avec 32 octets de données :
Réponse de 192.168.0.10 : octets=32 temps<1ms TTL=126
Réponse de 192.168.0.10 : octets=32 temps<1ms TTL=126
Réponse de 192.168.0.10 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.0.10 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 192.168.0.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```