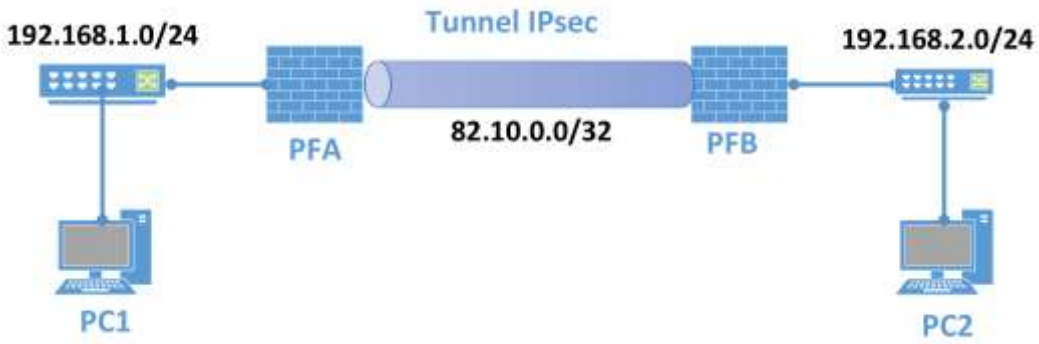
TP5 : IPSEC

L'objectif de ce TP est de mettre en œuvre deux routeurs dans le cas classique d'un VPN protégé par une clé partagée (Pre-Shared Key ou PSK). Ce TP vous permettra de comprendre le fonctionnement et le mode opératoire de IPSec qui est un protocole complexe mais très important dans la sécurisation des flux réseaux de nos jours. Bien que ce TP ne sera pas noté, les notions traitées sont nécessaires pour réussir le DE et le projet.

SCHEMA DE TOPOLOGIE :

Le schéma ci-dessous résume les réseaux intervenant dans notre exemple :



Le tunnel **IPsec** à créer sera entre le **PFA** et **PFB**. Les Parefeux peuvent être des machines Linux, des machines pfSense ou bien tout autre élément implémentant IPsec.

1. Réaliser la maquette demandée en utilisant l'adressage IP de votre choix. L'adressage sur le schéma est donné à titre d'exemple.

CHOIX DES PARAMETRES

2. Expliquer le rôle de SAD et de SPD dans IPSec.
3. Expliquer le fonctionnement du protocole IKE. Quel est l'entité qui implémente ce protocole dans votre système ? Est-ce que ceci est compatible avec le modèle OSI ?
4. Choisir les éléments de sécurité pour les deux phases d'échange de clé **IKE** : algorithmes de chiffrement, d'intégrité, durée de vie, … etc.
5. Configurer votre SPD en choisissant ESP en mode tunnel, et en indiquant les extrémités du tunnel. Le trafic provenant des PC vers Internet ne passe pas par le tunnel.
6. Configurer les règles sur les deux Parefeux pour être compatible avec la SPD.
    a. Autoriser les deux ports 500 et 4500. De quoi s'agit-il ?
    b. Accepter de forwarder un paquet uniquement s'il est protégé par IPsec.

INSTRUCTIONS DE GESTION DU VPN

7. Essayer un ping entre PC1 et PC2. Le ping doit réussir. S'il y a une erreur, essayer de résoudre le problème.
8. Afficher la liste des SA dans votre SAD.

9. Tests de validation : Plusieurs points sont à vérifier pour valider le bon fonctionnement du VPN :
    - Le trafic passe bien entre PC1 et PC2 pour différents protocoles.
    - Idem dans l'autre direction.
    - Le trafic passe bien dans le VPN et non pas en direct.
    - Le trafic est bien stoppé quand nous stoppons le VPN.

POUR ALLER PLUS LOIN

10. Mode transport : réaliser maintenant une connexion VPN IPsec en mode transport entre PC1 et PC2.
11. Client nomade : un employé de l'entreprise et en télétravail depuis son domicile. Faites les configurations nécessaires pour lui permettre d'accéder au réseau privé de son entreprise (VPN Client-à-Site).