Utilisation d'IPSec, mise en place d'un réseau privé virtuel

Votre travail doit être rendu avant le mercredi 21 décembre. Le travail est effectué en binôme. Tous les fichiers utiles doivent être envoyés par mèl (avec une description de ces fichiers) à `coulbois@cmi.univ-mrs.fr` et `ragopian@cmi.univ-mrs.fr`. Les fichiers de configuration doivent être lisibles et bien documentés.

L'objectif de ce travail est d'une part de comprendre concrètement le fonctionnement d'IPSec, d'autre part de mettre en place un réseau privé virtuel.

Vous devrez rendre à la fin de ces séances :
- une courte présentation d'IPSec (notemment des techniques cryptographiques rencontrées) et de son fonctionnement dans les implémentations utilisées ;
- un compte rendu des difficultés rencontrées ;
- une description des tests effectués ;
- les différents fichiers de configurations commentés utilisés.

L'objectif minimal de ces 4 séances (deux TP et deux TD) est de proposer :

1. une configuration IPSec pour que tout le trafic entre deux machines soit confidentiel, alors que ces machines restent en contact avec le reste de l'internet ;
2. une configurationin IPSec pour former un réseau privé virtuel à travers deux passerelles de sécurité liées par un tunnel, là aussi les les machines doivent avoir accès au reste de l'internet.

Les prolongements naturels de votre travail sont :
- d'aborder le problème de l'architecture d'échange de clés publiques (IKE) ;
- de tenir compte de l'hétérogénéité des systèmes (Windows et Linux par exemple) ;
- de combiner votre VPN avec un service NAT.