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

Votre travail doit être rendu avant le mercredi 10 janvier 2007. 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 commentés.

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 2 séances de 3h de TP est de proposer :

1. une configuration IPSec pour assurer la confidentialité du traffic entre deux machines. Chacune de ces deux machines doit pouvoir se connecter au reste de l'internet. Cette partie est à faire en binôme.
2. une configurationin IPSec pour former un réseau privé virtuel en reliant deux sous réseaux à travers deux passerelles de sécurité par un tunnel. Les machines des deux sous-réseaux doivent avoir accès au reste de l'internet. Vous détaillerez le routage des paquets pour la configuration que vous aurez choisie. Cette partie est à faire en regroupant deux binômes (environ quatre étudiants).

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.

Vous trouverez sur la page `http://www.latp.univ-mrs.fr/~coulbois/2007/crypto` des liens vers les docs et RFC dont vous pouvez avoir besoin.