1 OpenVPN

1.1 Introduction

1.1.1 Généralités

OpenVPN est un outil Open-Source permettant de créer des tunnels sécurisés (SSL/TLS) à travers un réseau non sûr comme Internet. OpenVPN est à la fois facile à installer et à configurer, en plus d'être disponible sur à peut prêt toutes les plates-formes (Linux, Windows, BSD, Mac OS, Solaris). Le principe de configuration reste le même quelque soit la plate-forme utilisée.

OpenVPN est basé sur une architecture client-server. Le VPN fonctionne soit site-à-site, soit avec des clefs partagées. Les données sont tunnelisées sur un seul port, TCP ou UDP.

1.1.2 Les deux types de VPN

Il existe deux types de VPN : les VPN bridgés et les VPN routés. Dans le cas du mode bridgé le réseau virtuel créé devient une réelle extension du réseau local. L'avantage de ce mode est la facilité d'intégration de la solution VPN au sein de l'infrastructure déjà en place. Ce mode est d'ailleurs la seule option si pour une raison ou pour une autre des paquets broadcasts doivent traverser le VPN. Le principal inconvénient de ce mode apparait lors du passage à l'échelle : comme c'est le réseau local qui doit absorber les clients du VPN, il faut suffisament de ressources disponibles (adresses IP, etc.).

Le mode routé est le mode le plus utilisé. Bien que sa mise en place soit plus complexe, ce mode permet de faire du réseau virtuel un réseau à part du réseau local. On est ainsi capable de mettre en place une politique d'accès différente pour les utilisateurs connectés depuis l'extérieur, ce qui renforce encore la sécurité de l'infrastructure. Le second grand aventage des VPN routés est que le passage a l'échelle s'effectue sans douleur étant donné que l'on n'impacte pas l'utilisation du réseau local.

La figure 1 résume les avantages et inconvénient de chacun des deux types de VPN :

VPN bridgé	VPN routé
extension du réseau local	réseau à part
mauvais passage à l'échelle	passage à l'échelle
laisse passer les broadcasts	broadcasts impossibles

FIGURE 1 – Avantages et inconvénients des deux types de VPN

Nous avons choisi de mettre en place une configuration de VPN routé, car mieux adaptée à l'utilisation que l'ISIMA pourrait en faire.

1.2 Mise en place côté serveur

La mise en place de l'infrastructure s'effectue en plusieures étapes. Tout d'abord nous installerons et configurerons OpenVPN sur le serveur, ensuite nous génèrerons les clefs et certificats de sécurité nécessaires, et enfin nous mettrons en place les outils nécessaires pour authentifier les utilisateurs via l'annuaire NIS de l'ISIMA.

1.2.1 Installation et configuration d'OpenVPN

La machine fonctionne sous `Linux CentOS 5.1`. OpenVPN n'étant pas disponible directement dans les paquets de cette distribution, nous allons construire notre propre rpm. Les paquets requis pour mener à bien cette étape sont à installer grâce à la commande suivante :

```
[root@centosvpn ~]# yum install openssl-devel pam-devel rpm-build gcc-c++
```

La version d'OpenVPN utilisée pour le projet est la 2.0.9 disponible sur `http://openvpn.net/`. Celle-ci dépend des paquets `lzo-devel-1.08-fr2.i386` et `lzo-1.08-fr2.i386`, disponibles par exemple sur `http://rpmfind.net/`.

```
[root@centosvpn ~]# wget ftp://rpmfind.net/linux/freshrpms/redhat/9/lzo/lzo-devel-1.08-
```

1.2.2 Génération des clefs et certificats de sécurité

1.2.3 Authentification via l'annuaire de l'ISIMA