Institut Supérieur
d'Informatique, de
Modélisation et de
leurs Applications

R&D Lannion 2,
Avenue Pierre Marzin
22307 LANNION

Rapport de projet de troisième année
Filière 5 : Infrastructure entreprise, réseaux et télécoms

Etude d'une architecture VPN pour l'ISIMA

Auteurs :
Léonardo Coscia
Julien Dessaux

Responsable ISIMA :
Christophe Gouinaud

2008-2009

Résumé

bla bla bla

Mots-Clés : .

Abstract

bla bla bla

Keywords : .

Remerciements

Nous tenons à remercier ... :
– 1
– 2

Table des matières

Introduction

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

Conclusion

Bibliographie

[RFC3261] IETF Network Working Group, SIP : Session Initiation Protocol, IETF, 2002

[SIPp] SIPp : a free Open Source test tool [en ligne]. Etats-Unis. Disponible sur `http://sipp.sourceforge.net`

[IMS-Bench] The IMS/NGN Performance Benchmark [en ligne]. Etats-Unis. Disponible sur : `http://sipp.sourceforge.net/ims_bench/`

[Seagull] Seagull : an Open Source Multi-protocol traffic generator [en ligne]. Etats-Unis. Disponible sur : `http://gull.sourceforge.net/`

[Clif] The CLIF Project [en ligne] Etats-Unis. Disponible sur :`http://clif.objectweb.org/`

[OPENSER] The new breed of communication engine [en ligne]. Allemagne. Disponible sur `http://www.openser.org/`

[Debian] Debian : Le Système d'Exploitation Universel [en ligne]. Etats-Unis. Disponible sur `http://www.debian.org`

[FreeBSD] The FreeBSD Project [en ligne]. Etats-Unis. Disponible sur `http://www.freebsd.org`

Lexique

CSV : Coma Separated Value, ou valeurs séparées par des virgules. Format de fichier de données.

GNUPlot : Boîte à outils permettant, entre autres, d'automatiser la génération de graphiques.

Open-Source : Se dit d'un logiciel dont la licence correspond à certains critères comme le libre accès à son code source ainsi que sa libre redistribution.

OpenSER : Proxy SIP reconnu pour ses excellentes performances.

Pipe nommé : Un pseudo fichier permettant la redirection d'une sortie sur une entrée.

Protocole de transport : Protocole dont le rôle consiste à délivrer les données aux applications.

Proxy : Serveur jouant un rôle dans la sécurité des réseaux, servant intermédiaire aux transactions.

Raptor : Outil de génération de trafic RTP interne à FT R&D.

RTP : Protocole applicatif d'échange de données audio et vidéo.

Script : Programme s'exécutant sans compilation.

Table ARP : Table de correspondance entre les adresses physiques (MAC) et logiques (IP).

TCP : Protocole de transport fiable au dessus de IP.

TLS : Protocole de session sécurisé et reposant sur TCP.

SDP : Protocole de description de session sur lequel s'appuie SIP.

SIP : Protocole applicatif permettant de gérer des sessions multimédia, et notamment de téléphonie.

UDP : Protocole de transport de type *best-effort* au dessus de IP.

Socket : Interface logicielle permettant l'utilisation des ressources réseau sur une machine.

VoIP : Qualificatif de l'ensemble des technologies vouées au transport de la voix sur un réseau IP.

XML : Langage permettant le stockage de données quelconques sous une forme standardisée.

Table des figures