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

Rapport de projet de dernière année d'école d'ingénieur
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

VPN est le nom donné à une technologie permettant de mettre en place une connexion sécurisée avec un réseau interne comme celui de l'ISIMA. En l'absence d'une telle technologie d'accès, les élèves et professeurs de l'ISIMA sont réduits à utiliser des moyens mal adaptés et contraignants pour accéder aux machines de l'école.

Ce projet a été conduit en vue d'étudier des moyens technologiques pour palier à ce manque. Il existe un grand nombre de solutions parmi lesquelles trois ont été considérées comme représentative du marché. Deux d'entre-elles sont propriétaires, l'une dépendant des technologies **CISCO**, l'autre fonctionnant dans un environnement **Windows**. La dernière est issue du monde **Open-Source** et s'exécute sous Linux.

L'étude repose sur la mise en place d'une plateforme de test mettant bien en évidence la problématique de la **sécurité** au sein des **VPN**. Le niveau d'intégration des différentes solutions au coeur du réseau existant est un critère déterminant du projet.

Mots-Clés : VPN, Open-Source, CISCO, Windows, sécurité.

Abstract

A **VPN** designates a technology that allows a user to establish a secure channel with a internal network like the ISIMA's network. Without this kind of technology, the ISIMA's students and professors are forced to use user-unfriendly means to gain access to the school's machines.

This project has been made to study technological means to solve this problem. Plenty of solutions exists, we kept three that represent the market. Two of them are proprietary, the first is **CISCO**'s technology, wihle the other works in a Windows environment. The last one is an **Open-Source** solution running on Linux.

The study is based on an implementation of a test bed showing the problematic of the **security** in the **VPN**. The integration level of those solutions in the existing network core is a decisive critera of the project.

Keywords : VPN, Open-Source, CISCO, Windows, security

Remerciements

Nous tenons à remercier tout particulièrement Christophe Gouinaud, sous directeur de l'ISIMA, pour nous avoir encadré tout à long de notre étude sur les solutions VPN et pour nous avoir aidé dans l'étape de configuration de l'autorité de certification.

Nous voudrions également remercier Patrice Laurençot, Responsable de la Filière Réseaux et Télécom, pour nous avoir aidé lors des différentes mises à jour des routeurs CISCO ainsi que lors de notre investigation des problèmes de performance des routeurs.

Pour finir, nous remercions Laurent Césari, intervenant extérieur de chez IBM, pour son cours sur la sécurité réseau.

Table des matières

Introduction

Les VPN se sont développés parallèlement à l'essor des technologies de communication. L'informatique s'est vite révélé être un formidable outil, mais le besoin d'échanger des informations de façon sécurisé a vite tempéré les esprits. De nombreuses solutions soit-disant sécurisées se sont rapidement développés, mais beaucoup ont échoué car elles considéraient la sécurité comme une fin et non comme un moyen.

Les technologies d'accès distant comme les VPN ont été la réponse à une approche réfléchie de la problématique de la sécurité, ce qui explique que leur essor se poursuit encore à l'heure actuelle. Cette problématique se pose également pour l'ISIMA, et c'est ce qui a motivé notre projet. Un tel accès permettrait d'améliorer concrètement la façon dont étudiants et professeurs travaillent, en leur fournissant un moyen adapté, flexible et sûr d'accéder au réseau de l'école depuis l'extérieur.

Dans un premier temps, nous présenterons plus en détail ce qu'est un VPN, nous évoquerons les différentes solutions sur le marché ainsi que sur les protocoles sur lesquels elles reposent. Nous présenterons également de façon schématique la plate-forme de test que nous utiliserons.

Dans un second temps, nous entrerons dans les détails de la configuration de chaque solution, tant d'un point de vue serveur que d'un point de vue client. Pour chacune d'entre-elles nous effectuerons un bilan et en dégagerons les limites.

Fnalement, les différentes solutions seront confrontées selon plusieurs critères prenant en compte les contraintes de sécurité des VPN. Elles seront d'abord évaluées en termes de complexité d'installation et d'administration, puis en termes de performances, de niveau de sécurité fourni et de facilité d'utilisation. Ces différents résultats nous permettront de déterminer le meilleur choix d'implémentation pour l'ISIMA.

1 Introduction à l'étude

1.1 Sujet de l'étude

L'objet de cette étude est d'évaluer différentes technologies permettant de mettre en place des connexions sécurisées via des Réseaux Privés Virtuels (VPN). L'objectif est de recenser plusieurs solutions fonctionnant sur divers systèmes d'exploitation et de les confronter entre-elles. Les différentes solutions seront d'abord évaluées en termes de complexité d'installation et d'administration, puis en termes de performances et de facilité d'utilisation.

VPN, ou Réseau Privé Virtuel, est le nom donné à une technologie permettant de relier des machines de façon sécurisée à travers un réseau non sûr comme Internet. Ce travail est effectué en vue de mettre en place une telle solution d'accès au sein de l'ISIMA. Les avantages d'une telle installation seraient multiples, du fait de la possibilité d'accéder au réseau interne de l'école depuis l'extérieur dans les mêmes conditions que si l'on était à l'intérieur.

Deux catégories de solutions VPN existent. On distingue les plate-formes dédiées tels les concentrateurs que les grands équipementiers proposent, et les solutions logicielles disponibles sur les systèmes d'exploitation courants : Microsoft a sa solution, le monde de l'Open-Source également.

Trois architecture ont donc été étudiées afin d'être en accord avec la diversité des solutions existantes : un routeur CISCO 2811XM configuré pour faire du VPN, un WindowsServer2K3 avec les services requis pour établir de connexions VPN, ainsi qu'un serveur Linux CentOS 5.1 avec le logiciel libre OpenVPN. La mise en place d'une plate-forme de test sera au coeur de cette étude.

1.2 Architecture étudiée

1.2.1 Schéma logique

Le travail a été intégralement réalisé dans la salle A214 de l'école. Nous avons pu mettre en place une maquette complète, permettant de simuler les accès depuis Internet vers un réseau interne. La figure 1 présente un schéma logique de la maquette.

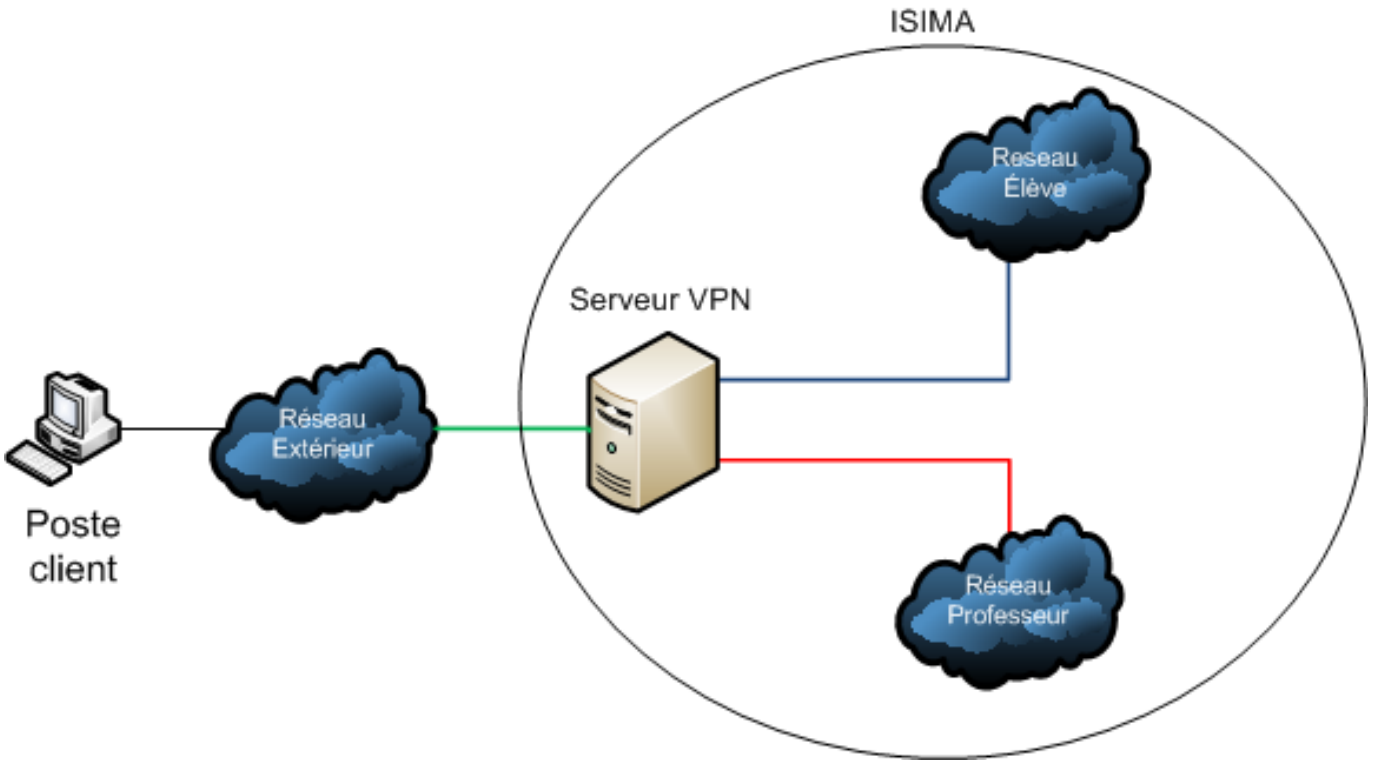

FIGURE 1 – Schéma logique de la maquette

1.2.2 Schéma physique

Pour faire cohabiter physiquement les trois architectures ensembles nous avons dû faire des conscessions. La plus importante a consisté à récupérer en DHCP les adresses IP des interfaces connectées au réseau de l'ISIMA, dans un coucis d'interropérabilité. La figure 2 illustre l'architecture mise en place :

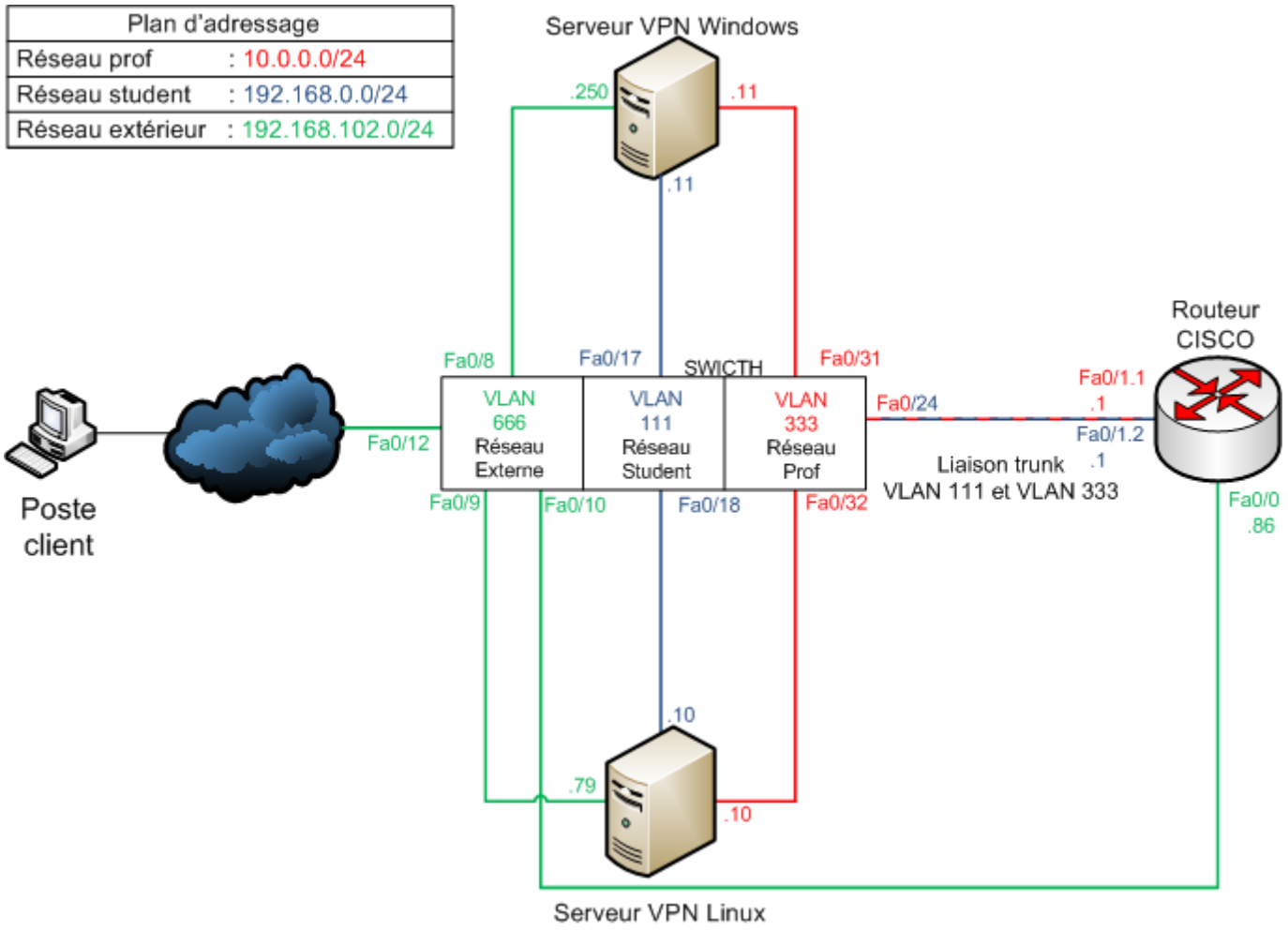

FIGURE 2 – Schéma physique de la maquette

1.3 Etat de l'art

1.3.1 Le problème de la sécurité

Comme expliqué précédemment, un VPN est une technologie permettant de créer des connexions sécurisés à travers un réseau non sûr. Il y a plusieurs menaces dont une connexion VPN doit être capable de nous protéger : l'espionnage, l'altération des données et le rejeu de paquets.

L'espionnage de données correspond à l'aspect le plus connu auquel sont confrontés les échanges, allant jusqu'à occulter (à tord) les deux autres. La parade contre l'espionnage consiste en la mise en place d'un chiffrement fort des données.

L'interception de données correspond au cas où un attaquant est présent en tant qu'intermédiaire dans le flot de communication, capable d'insérer, de modifier ou de supprimer des paquets circulant dans ce flot. Cette problématique a été à la fois la plus importante et la plus difficile à résoudre, la parade consistant à une authentification systématique en signant chaque paquet émis afin de pouvoir identifier ceux qui sont frauduleux. Le mécanisme le plus répendu d'authentification de paquet est

nommé construction HMAC (Hash Message Authentication Code).

Le problème du rejeu est complémentaire de l'interception : il s'agit de réémettre des paquets valides ayant déjà circulé sur le réseau avec bien sûr de mauvaises intentions. La parade consiste ici à inclure un identifiant unique (ou un timestamp) pour chaque paquet dans sa signature. Lorsqu'une entité reçoit un paquet elle garde trace des identifiants unique déjà reçus et refuse un paquet qui serait déjà passé. Des implémentations d'algorithmes à glissement de fenêtre sont les protections les plus utilisées contre le rejeu.

1.3.2 Le problème de l'authentification

L'authentification des tiers est l'une des solutions clefs pour mettre en place des communications sécurisées. Néanmoins ce moyen de résoudre un problème ne fait que conduire à un autre plus gros encore : celui de la gestion des clefs. En effet les algorithmes utilisés pour le chiffrement des échanges réclament des clefs de session pour fonctionner, et pour que notre connexion puisse être considérée comme sécurisée ces clefs doivent changer régulièrement. Ainsi la mise en place d'une connexion sécurisée impose d'avoir un moyen d'échanger des clefs de session de façon sécurisée alors que notre connexion ne l'est pas encore : c'est la cryptographie à clefs privées qui va résout ce problème.

1.3.3 Les différents types de VPN

Il existe deux façons d'aborder la mise en place d'une technologie VPN, chacune ayant sa finalité : les VPN bridgés et les VPN routés. Les VPN bridgés sont généralement utilisés lors de connexions site-à-site, tandis que les VPN routés sont eux préférés pour connecter des clients nomades. La mise en place d'un VPN routé s'impose donc pour cette étude, car en plus d'être facilement intégrable à l'architecture existante, elle est parfaitement adaptée à l'usage que l'ISIMA pourrait en faire.

1.3.4 Les classes de protocoles

a) IPsec

IPsec est une suite protocolaire de niveau 3, visant à apporter la sécurité manquant au protocole IP. Cette suite utilise plusieurs protocoles au cours des différentes phases de mise en place d'IPsec.

La première phase est une phase négociation au cours de laquelle les parties se mettent d'accord sur les algorithmes de chiffrement à utiliser et échangent des clefs de session via le protocole ISAKMP (Internet Security Association and Key Management Protocol). Au cours de cette phase le protocole IKE (Internet Key Exchange) intervient également pour générer ces clefs de session soit grâce à une clef partagée soit à l'aide de certificats RSA.

La seconde phase est la phase de communication au cours de laquelle les données peuvent traverser le tunnel et sont chiffrées. Deux protocoles peuvent intervenir en fonction de la finalité du tunnel : ESP qui fournit à la fois intégrité et confidentialité des données, et AH qui fournit l'intégrité et l'authentification.

b) pptp

PPTP (Point to Point Tunneling Protocol) est un protocole dont le rôle consiste à construire des paquets PPP (Point to Point Protocole) pour les encapsuler dans des datagrammes IP. PPTP tire ainsi avantage des mécanismes d'authentification, de chiffrement et de compression déjà existants

pour PPP (niveau 2) en les appliquant au niveau 3. Le principal avantage de ce protocole est son excellente intégration avec les systèmes Microsoft, au sein desquels la suite protocolaire de PPP a été réimplémentée pour accompagner PPTP.

Ainsi on utilise MS-Chap v2 (Microsoft-Challenge Handshake Authentication Protocol) pour l'authentification, et MPPe 'Microsoft Point to Point Encryption) pour le chiffrement. Au cours d'une session VPN entre un client et le serveur, une connexion TCP est utilisée pour le contrôle de la liaison. Quand à l'échange de données, celui-ci requiert un canal UDP et s'appuie sur le protocole GRE (Generic Routing Encapsulation).

c) TLS

Le protocole TLS est une évolution du protocole SSL qui, après s'être rendu extrêmement populaire dans le domaine des transaction sécurisées au niveau applicatif (notamment le web), a être utilisé dans le domaine des VPN. Le but de ces technologies VPN est de s'appuyer sur la maturité de TLS pour gérer la gestion du tunnel de données ainsi que tous les éléments cryptographiques nécessaires : authentification, confidentialité et intégrité.

Une erreur commune est de penser que comme TLS n'est pas un protocole de niveau 3 les technologies s'appuyant sur lui ne répondent pas aux critères fondamentaux des VPN : il n'en est rien. Il s'agit simplement d'une approche différente du problème, issue d'une constatattion simple : Les systèmes complexes sont les plus difficiles à sécuriser. Là où la mise en place d'IPsec dépend d'une nouvelle pile IP et implique des intéractions à la fois très fortes et très sophistiquées avec le noyau du système, les technologies basées sur TLS s'appuient sur du code s'exécutant dans l'espace utilisateur : une simple interface réseau virtuelle est utilisée pour parvenir à ce résultat.

1.4 Objectifs fixés

Les objectifs pour la suite du projet sont donc d'étudier la mise en place d'une plate-forme de test pour les différentes solutions qui ont été recensées conformément aux représentations logique et physique de l'architecture présentées en partie 1.2 page 2. Les différentes solutions seront finalement confrontées les unes aux autres dans une dernière partie.

Nous commencerons par étudier la solution Microsoft, viendra ensuite le logiciel OpenVPN sous Linux, et enfin la technologie CISCO. Pour la mise en place de chacune de ces trois solutions, nous nous attarderons sur les problématiques de l'installation et de la configuration, que ce soit côté serveur ou côté client. Chacune de ces parties fera état des problèmes rencontrés au cours de l'étude ainsi que des limites de chaque solution.

2 Mise en place des maquettes

2.1 Solution Windows

Le choix de Windows Server 2003 Entreprise Edition s'est imposé pour l'installation de la maquette. Cette version intégrant toutes les fonctionnalités nécessaires à la mise en place d'un VPN aucune application tierce ne sera à priori requise.

Nous commencerons par détailler les différents services nécessaires au fonctionnement du VPN sur le serveur, ensuite nous verrons les méthodes de configuration d'un poste client et enfin nous effectuerons une synthèse des avantages et inconvénients de la solution Microsoft.

2.1.1 Côté serveur : les services installés

Dans cette section nous détaillerons tour à tour la configuration des nombreux services requis pour le bon fonctionnement du service VPN :

- service DHCP.
- service DNS.
- Active Directory.
- routage et accès distant (VPN).
- autorité de certification (CA).
- IIS (requis pour l'authorité de certification)

a) Caractéristiques de la machine

Le serveur windows est installé sur un DELL PowerEdge 1300. Il est doté d'un processeur INTEL de type Pentium II cadencé à 348 Mhz, possède 512 Mo de mémoire vive ainsi qu'un disque dur de 9 Go. La machine est également équipée de trois cartes réseaux 100Mbps configurées comme suit :

Référence	Réseau	Adresse IP
Realtek RTL 8139 Familly	réseau PROFS	10.0.0.11/24
Realtek RTL 8139 Familly	réseau extérieur	192.168.102.250/24
Fast Ethernet CNET PRO 200P	réseau STUDENTS	192.168.0.11/24

FIGURE 3 – Configuration des cartes réseaux

b) Service DHCP

Ce service est nécessaire pour l'attribution des adresses IP qui seront allouées à chaque client voulant se connecter. La configuration du service DHCP met en évidence les deux pools d'adresses nécessaires à l'adressage de chacun de nos réseaux internes :

Caractéristique	Réseau PROFS	Réseau STUDENTS
Désignation Carte réseau	DHCP_PROFS	DHCP_STUDENTS
Adresse IP Carte réseau	10.0.0.11	192.168.0.11
Pool d'adresse	10.0.2.100 à 10.0.2.254	192.168.2.100 à 192.168.2.254
Masque réseau	255.255.255.0	255.255.255.0
Serveur DNS/routeur	10.0.0.11	192.168.0.11
Nom du domaine DNS	wvpn.isima.fr	wvpn.isima.fr

FIGURE 4 – Caractéristiques du service DHCP

L'installation du service DHCP ne requiert aucune modification des options par défaut, et ne nécessite que d'indiquer qu'elles sont les cartes réseau à adresser. La figure 5 illustre cette configuration :

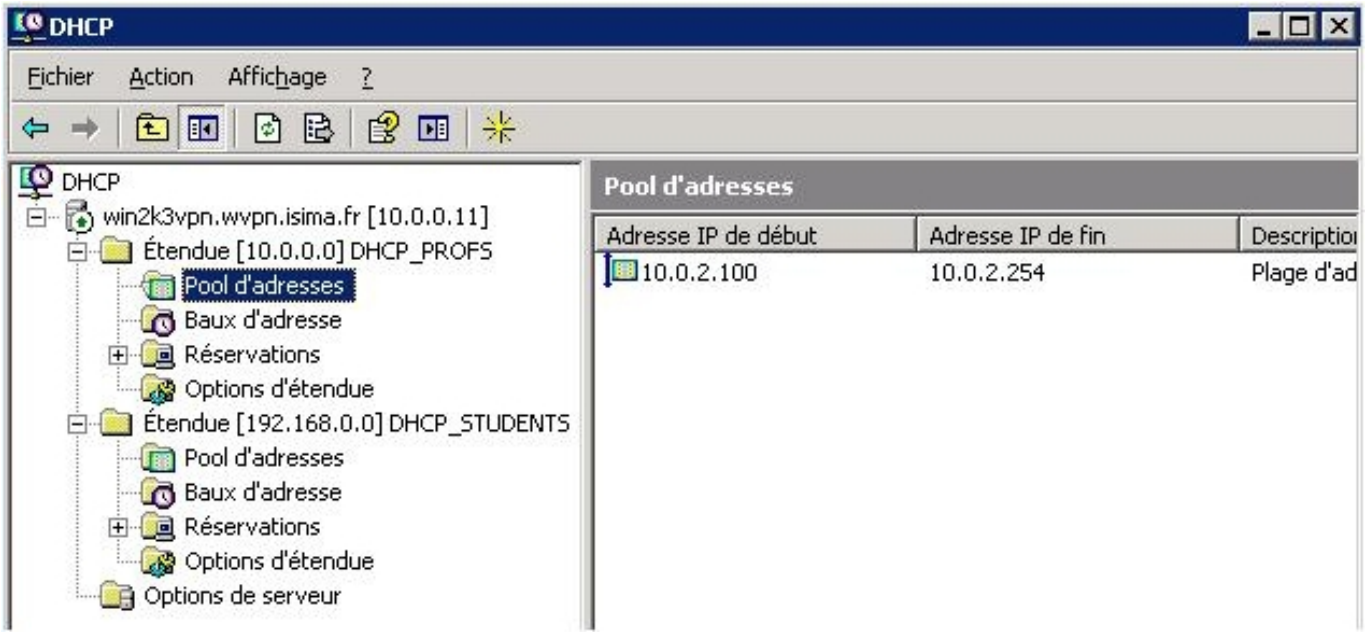

FIGURE 5 – Etendue DHCP du réseau professeurs

Il est à noter que sous Windows le service DHCP est attaché à une seule carte réseau qui répondra aux demandes des clients, ici la carte `DHCP_PROFS`

c) Service DNS

En préliminaire à l'installation de Active Directory, un service DNS est requis. Les caractéristiques de ce dernier sont les suivantes :

- Nom de la machine : win2k3vpn.
- Nom de domaine : wvpn.isima.fr.
- Type de zone : zone principale.

Tout comme pour le service DHCP, le service DNS est attaché à une seule carte réseau.

d) Active Directory

Ce service fournit le support d'un annuaire permettant l'identification des clients. Notre VPN proposant deux accès distincts, deux groupes doivent être créés : un groupe STUDENTS et un groupe PROFS. Lors de la configuration d'un nouvel utilisateur, celui-ci doit être ajouté dans l'un de ces groupes et doit être explicitement autorisé à pouvoir se connecter :

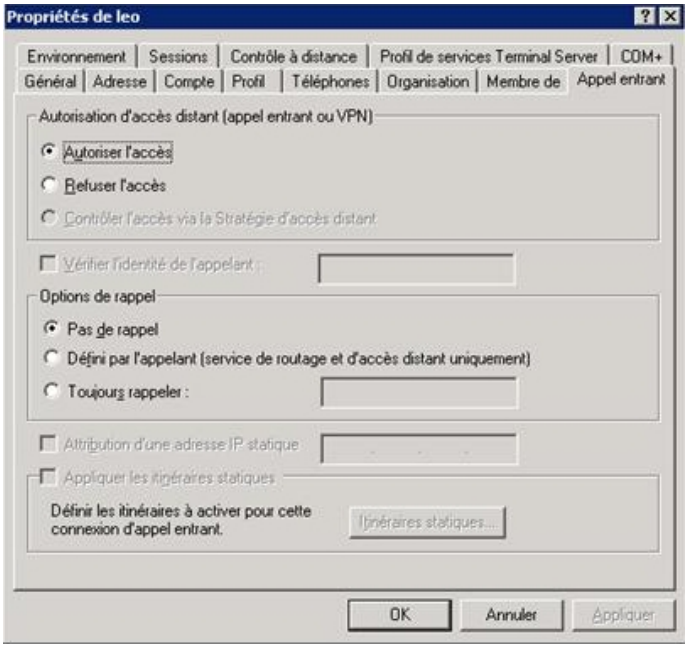

FIGURE 6 – Autorisation d'un utilisateur à se connecter au VPN

La stratégie de groupe (GPO) a été laissée à sa configuration par défaut.

e) Routage et accès distant

Le service routage et accès distant est le service qui va nous permettre de monter un tunnel sécurisé. Lors de son installation, l'administrateur doit choisir l'option "routage pour réseaux locaux uniquement" ainsi que l'option "serveur d'accès distant". Une fois le service installé, il faut configurer les options de sécurité qui sont propre au serveur (un clic droit sur le nom du serveur permet de modifier les propriétés) pour correspondre à la manière dont les utilisateurs s'identifient. Le service propose deux choix : identification par l'annuaire et identification via un serveur RADIUS.

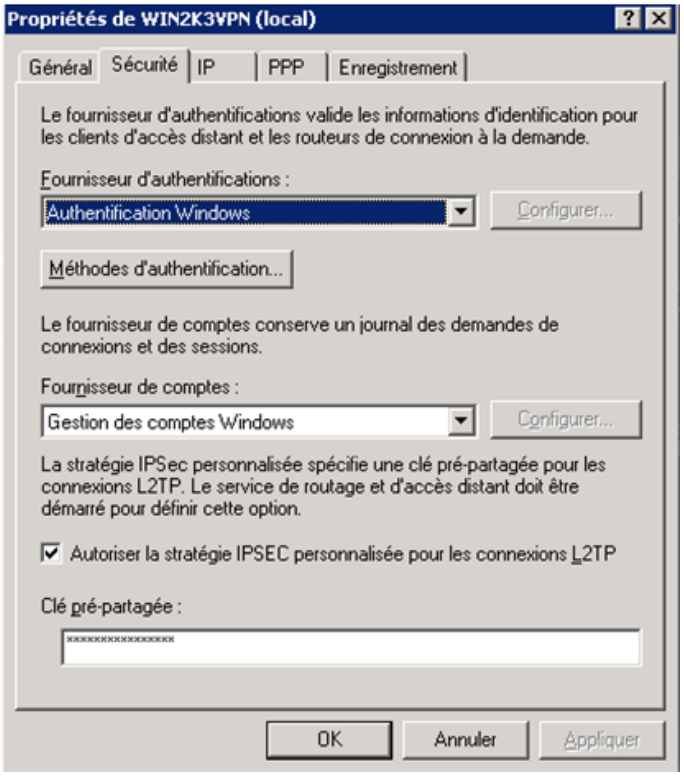

FIGURE 7 – Choix de la méthode d'identification

Nous avons testé la maquette en activant l'identification via un serveur RADIUS afin de pouvoir récupérer l'annuaire de l'ISIMA (comme présenté pour la configuration du routeur CICSO en 2.3.2.b) page 24), mais cela n'a jamais fonctionné comme escompté. Afin de travailler avec une maquette fonctionnelle nous avons dû rétablir le mode d'authentification via annuaire local.

Dans l'onglet IP, il faut configurer la manière dont le service va attribuer les adresses IP aux clients : soit via le service DHCP (méthode la plus flexible, que nous avons retenue), soit en définissant manuellement une plage statique à adresser. L'option "carte" correspond à la carte réseau qui repondra aux demandes des clients.

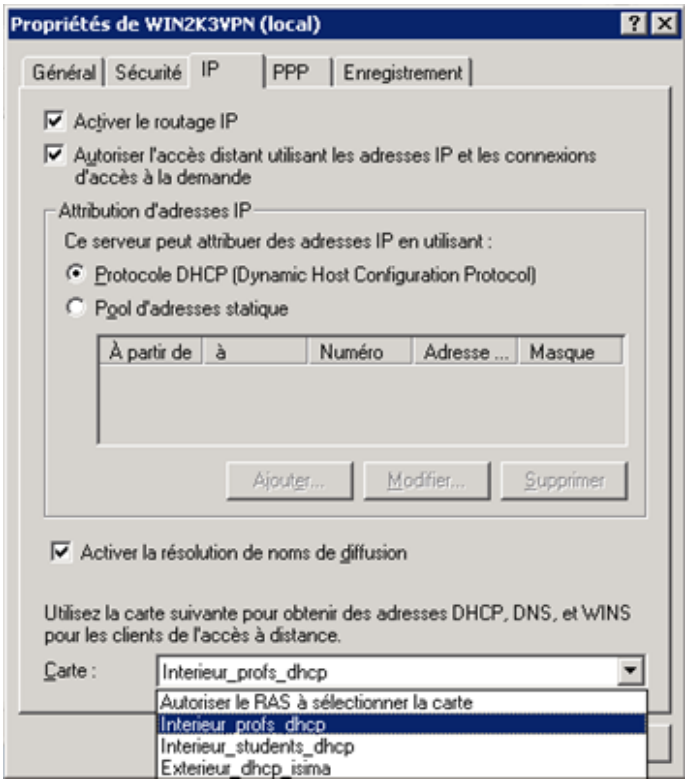

FIGURE 8 – Configuration du routage IP

La problème est le même que pour les services DHCP et DNS : le service d'accès distant s'attache à une seule carte réseau. L'aspect sécurité est géré par l'intermédiaire des stratégies d'accès distant. Il nous en falait une dont voici les spécifications :

- Appartenance à un groupe : PROFS ou STUDENTS
- Type d'authentification : MS-CHAP V2
- Spécification du type de connexion : VPN

La stratégie d'accès distant permet de contrôler finement quelles sont les conditions que doit remplir un utilisateur pour pouvoir se connecter, par exemple en définissant une plage horraire de connexion, etc. L'authentification utilise le protocole propriétaire Ms-Chap v2 qui permet une authentification mutuelle du client et du serveur. L'inconvénient de ce protocole est qu'il laisse passer le login du client en clair sur le réseau, mais les mots de passes sont bien sûr hashés.

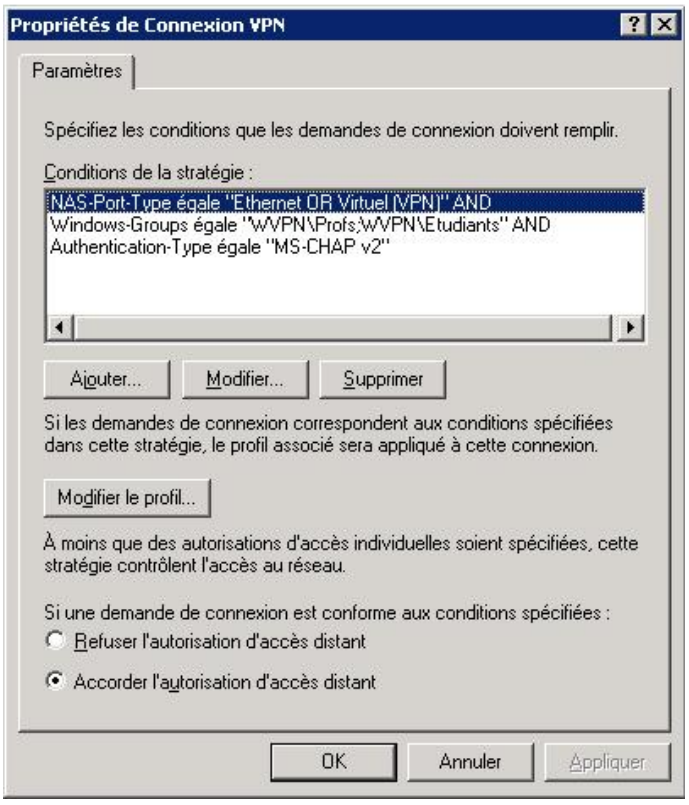

FIGURE 9 – Stratégie d'accès distant

f) Autorité de certification

La sécurité de la solution n'est pas complète sans une identification via certificats, nous allons donc configurer une autorité de certification sur le serveur. Cette autorité va notamment nous permettre de délivrer des certificats signés qui nous seront utile pour la solution Microsoft, mais aussi lors de la configuration du routeur CISCO. L'autorité racine aura comme nom commun ISIMA et les certificats seront valides un an. L'ensemble correspond à la configuration du service Windows 2003 SCEP. D'un point de vue technique, l'autorité de certification utilise l'algorithme de hashage SHA-1 pour la signature, et un chiffrement de clefs de longueur 2048 bits par l'algorithme RSA.

Pour effectuer une demande de certificat, les clients doivent se connecter sur l'URL suivante : `http://192.168.102.250/certsrv`. Deux types de certificats sont proposés : WEB ou MESSAGERIE. L'interface de l'autorité de certification permet de répondre aux demanded de certificats en choisissant d'accepter ou non de les délivrer. Si la demande est validée, l'utilisateur doit se connecter à nouveau sur le site WEB afin d'installer le certificat sur sa machine.

Malheureusement, après plusieurs essais infructueux nous constatons que le système de certificats ne nous permet plus de se connecter au VPN. Le problème se situe probablement dans l'écriture des demandes de certificats mais nous ne sommes pas parvenus le résoudre, et cela est dommageable pour le niveau de sécurité de la solution.

2.1.2 Configuration du client

L'un des avantages majeurs de la solution Windows est que le client VPN est déjà intégrer dans le système d'exploitation de Microsoft. L'un des inconvénients majeurs de la solution Windows est que malgré touts nos efforts nous ne sommes jamais parvenus à nous connecter au VPN Windows depuis un client Linux. Cette section présente les différentes étapes nécessaires à la création d'une connexion VPN sous Windows, et débute par la configuration d'une nouvelle connexion de type entreprise :

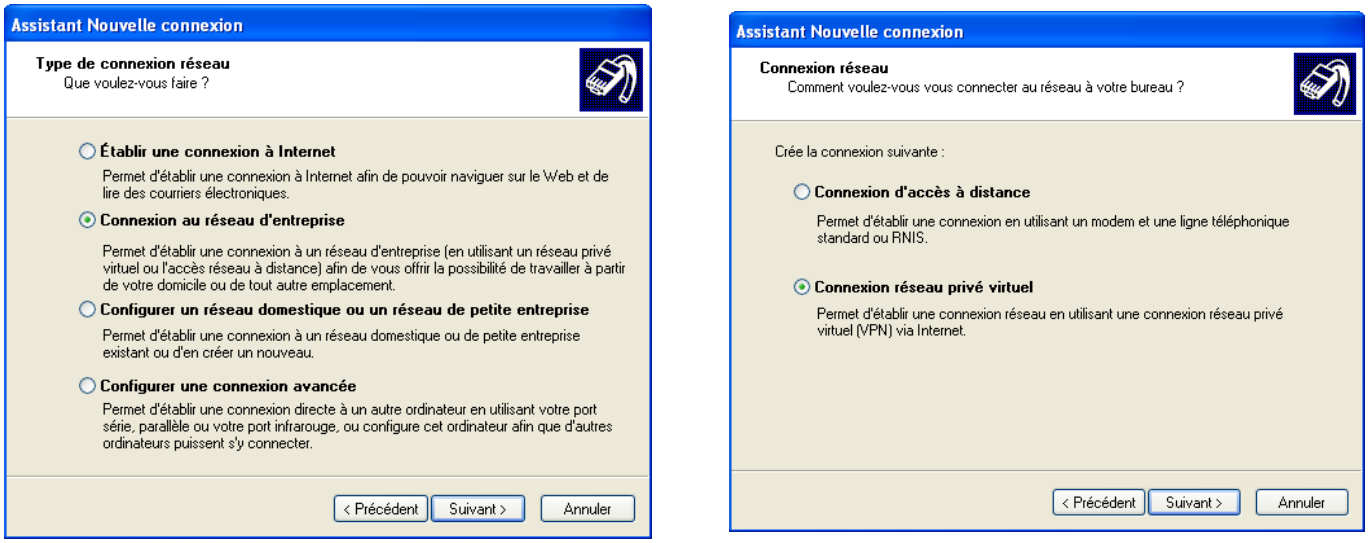

FIGURE 10 – 1ère étape de la configuration d'une nouvelle connexion

La 2ème étape consiste à nommer la connexion et à désactiver le mécanisme de connexion initiale automatique :

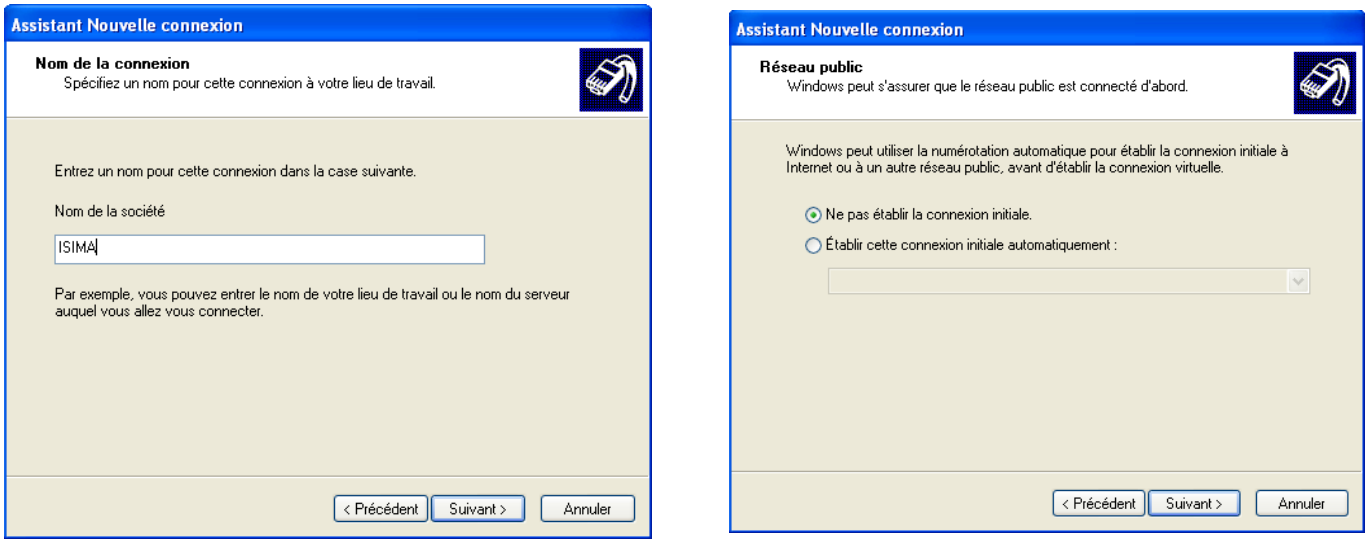

FIGURE 11 – 2ème étape de la configuration d'une nouvelle connexion

La dernière étape permet de spécifier l'adresse IP du serveur distant :

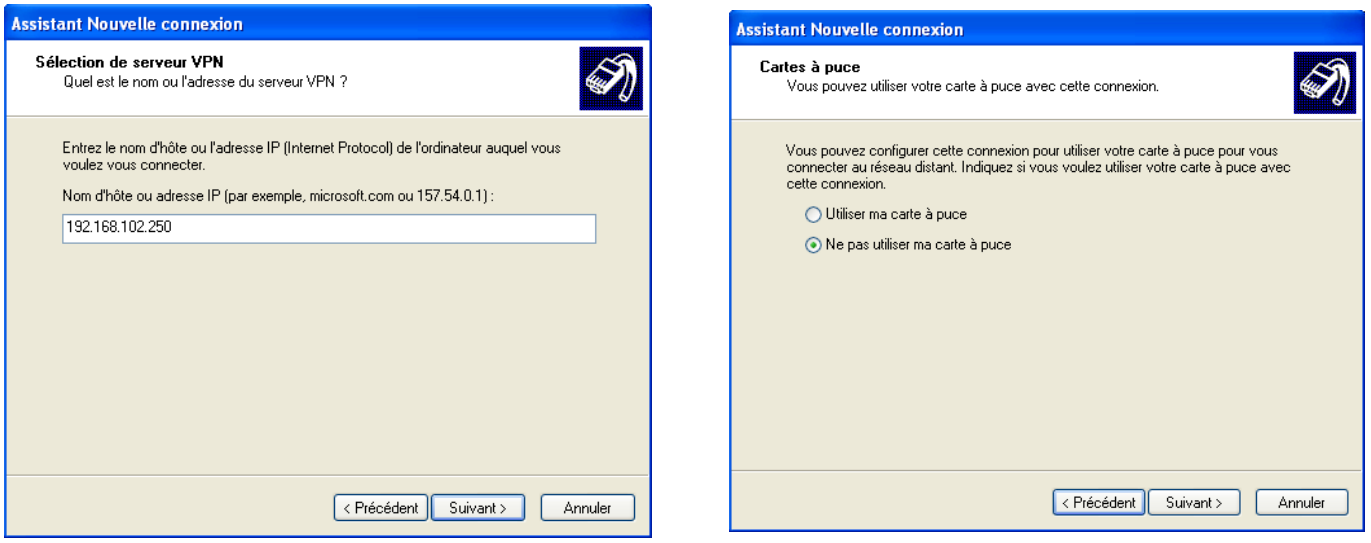

FIGURE 12 – 3ème étape de la configuration d'une nouvelle connexion

Ceci achève la configuration de la nouvelle connexion, les paramètres de sécurité du client ont été laissés aux valeurs par défaut. Lorsqu'il tentera de se connecter, l'utilisateur devra entrer ses identifiant et mot de passe comme définis dans l'Active Directory. La figure 13 présente l'état de la connexion après authentification : le VPN utilise le protocole PPTP, nous avons reçu l'adresse IP 10.0.2.106, authentification Ms-Chap v2, chiffrement MPPe 128 bits.

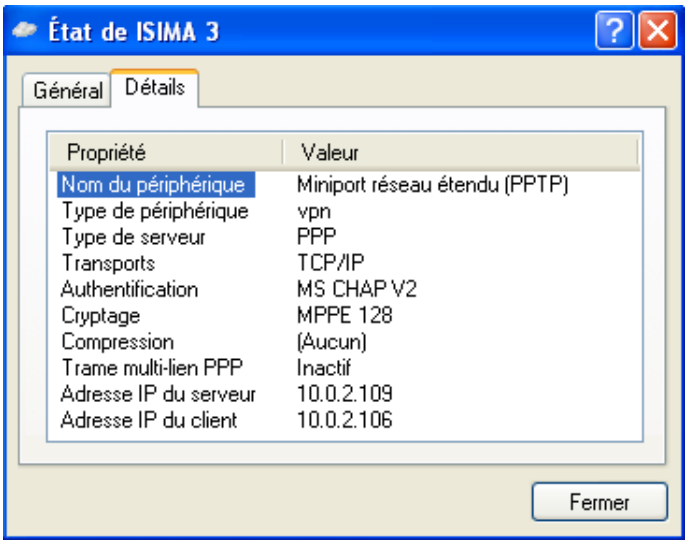

FIGURE 13 – Informations d'état de la connexion

Une remarque sur le chiffrement MPPe : Windows 2000 ne permet pas l'utilisation de clefs de longueur supérieure à 40 bits. Il est possible de permettre l'utilisation de clefs plus faibles que 128 bits sur le serveur, afin de permettre à ces clients de se connecter, mais ce n'est pas recommandé.

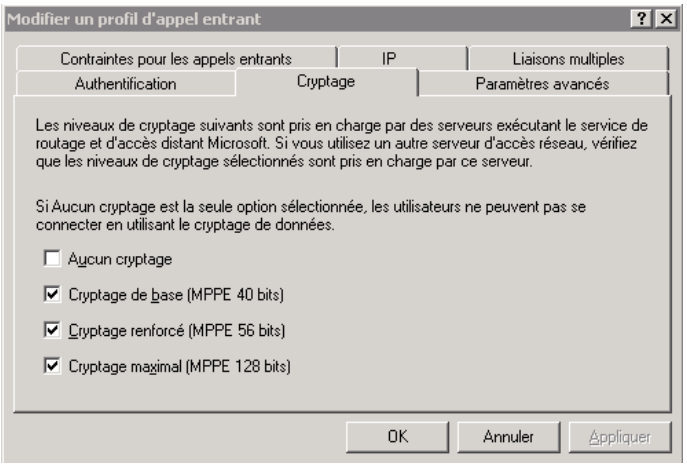

FIGURE 14 – Cryptage MPPE

2.1.3 Bilan et limites de la solution

Microsoft propose une solution VPN à la fois intéressante et facile à mettre en place (côté serveur comme côté client), mais demeure vraiment destinée à de petites structures. Dans le cas de l'ISIMA, la structure du réseau est plus complexe, avec la séparation des réseaux professeurs et étudiants.

L'inconvénient majeur de Windows Server est que chaque service doit se lier avec une seule carte réseau. Il est donc impossible de dissocier le trafic réseau sur des deux cartes, ce qui ne respecte pas le cachier des charges du projet. Une solution envisageable serait de virtualiser un serveur Windows 2003 et de lier les cartes réseau virtuelles aux cartes réseaux physiques de la machine. Rappelons également que côté client nous n'avons pas réussi à nous connecter depuis une une machine Linux à cause d'une mauvaise implémentation du protocole PPTP.

La récupération des identifiants et mots de passe depuis l'annuaire de l'ISIMA n'a pas pu être effectuée et nous avons choisi de ne pas tenter d'interfacer notre maquette avec le réseau de l'école. Comme nous l'avons expliqué, le service VPN est attaché à une seule carte réseau, et ceci nous empêche de savoir quel type d'utilisateur est connecté (professeur ou étudiant). La procédure à suivre serait d'intégrer le serveur VPN Windows sur le domaine de l'ISIMA et de lancer une réplication de la base Active Directory.

Nous avons également suivi une autre piste pour tenter de s'interfacer avec la base NIS de l'ISIMA. Microsoft propose une suite d'outil `Windows Service for UNIX` téléchargeable directement depuis leur site. Cette suite propose d'intégrer à Windows des commandes et services généralement spécifiques aux systèmes UNIX, parmis lesquels un client NIS. Une amélioration possible de la maquette serait de récupérer les informations utilisateurs de l'ISIMA via ces outils : l'interopérabilité serait alors complète.

L'absence de certificats signés pour l'authentification des pairs pose un réel probléme de sécurité. De plus bien que les mots de passes clients soient hashés, les identifiants et le nom d'hôte de la machine circulent en clair sur le réseau au cours de la phase d'authentification. La figure 15 illustre ce problème :

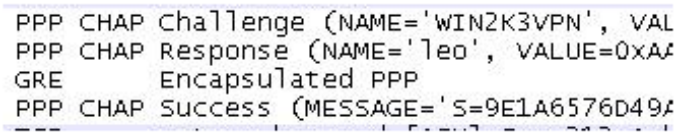

FIGURE 15 – Trace d'une connexion

En conclusion, la solution Microsoft bien que simple à mettre en place demeure incomplète, ne répond pas à notre cahier des charges en termes de sécurité et n'est pas multiplates-formes.

2.2 OpenVPN

2.2.1 Généralités

OpenVPN est un outil Open-Source permettant de créer des tunnels sécurisés utilisant un chiffrement SSL/TLS. OpenVPN propose un client 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.

2.2.2 Mise en place du 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 générerons 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.

Les interfaces de la machine sont configurées comme indiqué figure 2 page 2, et résumé dans le tableau figure 16 :

Interface	Adresse IP	Commentaire
eth0	192.168.0.10	Réseau interne étudiants
eth1	192.168.102.121	Réseau externe
eth2	10.0.0.10	Réseau interne profs

FIGURE 16 – Configuration des interfaces de la machine Linux

a) Installation et configuration d'OpenVPN

Résolution des dépendances

La machine fonctionne sous `Linux CentOS 5.1`. OpenVPN n'étant pas disponible directement dans les paquets de cette distribution (vieille de deux ans à l'écriture de ces lignes), 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-fr2.i386.rpm
[root@centosvpn ~]# wget ftp://rpmfind.net/linux/freshrpms/redhat/9/lzo/lzo-1.08-fr2.i386.rpm
[root@centosvpn ~]# rpm -ivh lzo-1.08-fr2.i386 lzo-devel-1.08-fr2.i386.rpm
```

Compiler OpenVPN

Lors de la configuration de notre maquette la version courante d'OpenVPN était la 2.0.9 ; adaptez les numéros de version avec celui de la dernière release stable d'OpenVPN. Les commandes suivantes permettent à la fois de la récupérer, de la compiler, et de l'installer :

```
[root@centosvpn ~]# wget http://openvpn.net/release/openvpn-2.0.9.tar.gz
[root@centosvpn ~]# rpmbuild -tb openvpn-2.0.9.tar.gz
[root@centosvpn ~]# rpm -ivh /usr/src/redhat/RPMS/i386/openvpn-2.0.9-1.i386.rpm
```

Configuration de base

Une instance d'OpenVPN ne peut gérer qu'un seul pool d'adresses à la fois, et donc un seul type de clients pour le VPN. La solution pour gérer à la fois les professeurs et les étudiants grâce à une même machine est donc de lancer deux instances du serveur en écoute sur un port différent. Nous allons donc utiliser deux fichiers de configuration distincts dont la figure 17 présente les paramètres qui leurs sont communs : Interface d'écoute, protocole de transport, etc.

Pour toute la suite nous considérerons que ces fichiers se trouvent dans le dossier `/etc/openvpn/` et portent les noms `server-prof.conf` et `server-student.conf` :

```
local 192.168.102.121
proto udp
dev tap
client-to-client
duplicate-cn
keepalive 10 120
comp-lzo
user nobody
group nobody
persist-key
persist-tun
status openvpn-status.log
verb 3
```

FIGURE 17 – Configuration de base d'OpenVPN

Pour configurer correctement deux instances qui puissent cohabiter, celles-ci doivent se mettre en écoute sur un port différent. Nous avons choisi le port 1194 (port par défaut d'OpenVPN) pour le serveur profs, ainsi que le port 1195 pour le serveur étudiant. Les figures 18 et 19 détaillent également la configuration des pools d'adresses à affecter aux clients, ainsi que les informations de routage à leur transmettre :

```
port 1194
server 10.0.1.0 255.255.255.0
ifconfig-pool-persist ipp-profs.txt
push ''route 10.0.0.0 255.255.255.0''
```

FIGURE 18 – Configuration spécifique aux profs

```
port 1195
server 192.168.1.0 255.255.255.0
ifconfig-pool-persist ipp-profs.txt
push ''route 192.168.0.0 255.255.255.0''
```

FIGURE 19 – Configuration spécifique aux étudiants

b) Génération des clefs et certificats de sécurité

Dans cette section nous allons voir comment générer les clefs et certificats qui serviront à sécuriser les authentifications auprès du serveur OpenVPN. Pour cela nous allons utiliser une suite de scripts shell nommée `easy-rsa`, une sorte de frontend pour OpenSSL. Cette suite `easy-rsa` fournie avec OpenVPN permet de grandement simplifier le travail de génération et de gestion des clefs et certificats.

Commençons par récupérer les outils. Si OpenVPN a été compilé suivant les étapes ci-dessus, ceux-ci se trouve dans le répertoire `/usr/share/openvpn/easy-rsa`. Il faut copier ce répertoire dans un lieu sûr puis ouvrir un shell à cet endroit. L'étape suivante consiste à éditer le fichier `vars` pour configurer les paramètres globaux des scripts, comme indiqué figure 20 :

```
export KEY_COUNTRY=FR
export KEY_PROVINCE=FR
export KEY_CITY=''Clermont-Ferrand''
export KEY_ORG=''ISIMA''
export KEY_EMAIL=''nobody@nowhere.com''
```

FIGURE 20 – Paramètres globaux des certificats

L'environnement du shell doit ensuite être initialisé en important le contenu du fichier vars :
`[root@centosvpn easy-rsa]# . ./vars`
Comme c'est notre premier lancement on s'assure que tout est propre :

```
[root@centosvpn easy-rsa]# ./clean-all
```

Nous créons ensuite nos clef et certificat de CA (Certificate Authority) afin de pouvoir signer les certificats de nos clients. Seule l'entrée "COMMON NAME" n'est pas tirée du fichier `vars`, la valeur `ISIMA CA` fera très bien l'affaire :

```
[root@centosvpn easy-rsa]# ./build-ca
```

Nous allons maintenant générer les clefs et certificats pour le serveur et les deux types de clients. L'entrée "COMMON NAME" devra être précisée de façon à prendre respectivement les valeurs "ISIMA SERVER", "ISIMA PROF" et "ISIMA STUDENT". De plus il faut signer chaque certificat avec notre CA et commiter le résultat dans la base OpenSSL du serveur :

```
[root@centosvpn easy-rsa]# ./build-key-server server
[root@centosvpn easy-rsa]# ./build-key prof
[root@centosvpn easy-rsa]# ./build-key student
```

Ensuite nous initialisons un générateur de grand nombres premiers pour le procédé d'échange de clefs via la méthode Diffie Hellman :

```
[root@centosvpn easy-rsa]# ./build-dh
```

Pour finir, il nous reste à générer une dernière clef qui sera utilisée pour signer chaque paquet échangé entre les clients et le serveur et augmenter encore le niveau de sécurité du serveur VPN :

```
[root@centosvpn easy-rsa]# (cd keys ; openvpn --genkey --secret ta.key)
```

Dans cette section nous avons généré de nombreuses clefs et certificats dans le dossier `keys` de notre répertoire de travail. Le tableau de la figure 21 indique les rôles et finalité de chacun des fichiers, ainsi que leur niveau de confidentialité. Les fichiers qui ne figurent pas dans le tableau peuvent être simplement supprimés.

Fichier	Requis par	Rôle	Secret
ta.key	Tous	clef de signature	OUI
ca.crt	Tous	certificat Root CA	non
ca.key	serveur	clef privée Root CA	OUI
dhn.pem	serveur	paramètres Diffie Hellman	non
server.crt	serveur	certificat serveur	non
server.key	serveur	server Key	OUI
prof.crt	professeurs	certificat public professeurs	non
prof.key	professeurs	clef privée professeurs	OUI
student.crt	étudiants	certificat public étudiants	non
student.key	étudiants	clef privée étudiants	OUI

FIGURE 21 – Rôle des clefs et certificats

Il reste donc à copier les clefs et certificats du serveur dans le dossier `/etc/openvpn` et à indiquer à nos deux fichiers de configuration d'utiliser ces clefs et certificats en leur ajoutant les lignes suivantes :

```
ca         /etc/openvpn/ca.crt
cert       /etc/openvpn/server.crt
key        /etc/openvpn/server.key
dh         /etc/openvpn/dh1024.pem
tls-auth   /etc/openvpn/ta.key          0
```

FIGURE 22 – Configuration des clefs et certificats

c) Authentification via l'annuaire de l'ISIMA

OpenVPN étant capable de réaliser une authentification PAM (méthode standart sur les systèmes de type UNIX), c'est la solution que nous avons retenue. Nous allons donc configurer un client NIS sur la machine de test, et indiquer à OpenVPN comment l'utiliser.

La première étape consiste à installer le client NIS si ce n'est pas déjà fait (paquet `ypserv`) et à faire entrer la machine dans le domaine NIS de l'ISIMA en ajoutant la ligne suivante au fichier `/etc/yp.conf`. Il va de soie que glouglou doit être référencé dans le fichier `/etc/hosts` de la machine.

```
domain glouglou.isima.fr server glouglou
```

La deuxième étape consiste à indiquer au système qu'il doit intérroger la base NIS lorsqu'un utilisateur tente de s'authentifier. Pour cela il faut modifier trois lignes dans le fichier `/etc/nsswitch.conf` de façon à avoir :

```
passwd:     files nis
shadow:     files nis
group:      files nis
```

FIGURE 23 – Authentification via l'annuaire NIS

Le dernier point consiste à indiquer aux instances d'OpenVPN qu'elles doivent charger le module d'authentification PAM, en ajoutant une ligne à la configuration de chaque serveur :

```
plugin /usr/share/openvpn/plugin/lib/openvpn-auth-pam.so login
```

d) Finalisation du serveur

La configuration du serveur touche à sa fin, il faut encore protéger nos fichiers de configurations, clefs et certificats des regards indiscrets. Il est également judicieux de supprimer les clefs privées du répertoire `easy-rsa`.

```
[root@centosvpn ~]# chmod -R 600 /etc/openvpn
```

Il nous reste à planifier le lancement des services au démarrage :

```
[root@centosvpn ~]# chkconfig --add ypbind
[root@centosvpn ~]# chkconfig --add openvpn
```

2.2.3 Mise en place du client

Comme expliqué précédemment, il existe un client pour OpenVPN quelque soit la plate-forme utilisée. Le client pour Windows peut être récupéré depuis le site officiel d'OpenVPN et à l'installer comme n'importe quel autre logiciel. Pour ce qui est des systèmes Linux récents, ils possèdent tous un client OpenVPN intégré à la distribution. Concernant les autres systèmes, c'est à dire les Linux moins récents, MacOS, Solaris et BSD il est nécessaire de récupérer les sources du client (au format tar.gz) depuis le site officiel d'OpenVPN et de les compiler. De nombreux tutoriaux existent et couvrent tous les cas de figure pour ces différents systèmes.

Une fois le client installé la configuration est extrêmement simple : il suffit de copier le fichier de paramètres ainsi que le certificat et la clef du client dans le bon répertoire : `/etc/openvpn/` pour les systèmes UNIX, et généralement `c:\Program Files\openvpn\config` sous Windows. Les différents fichiers pourrait typiquement être récupérés depuis l'intranet.

La figure 24 présente le contenu des fichiers de configuration pour les clients étudiant et professeur :

```
client
dev tap
proto udp
remote 192.168.102.121 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert prof.crt
key prof.key
ns-cert-type server
tls-auth ta.key 1
comp-lzo
verb 3
auth-user-pass
```

```
client
dev tap
proto udp
remote 192.168.102.121 1195
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert student.crt
key student.key
ns-cert-type server
tls-auth ta.key 1
comp-lzo
verb 3
auth-user-pass
```

FIGURE 24 – Configuration des clients OpenVPN étudiant et professeur

Une fois installé et lancé, le client est très discret, comme le montre la figure 25

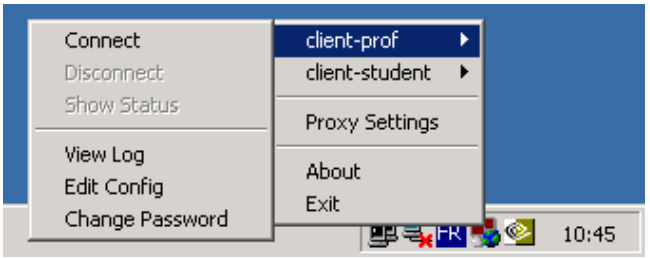

FIGURE 25 – Client OpenVPN sous windows

2.2.4 Bilan et limites de la solution

Une fois passée la phase un peu fastidieuse de mise en place et de configuration du serveur, OpenVPN se révèle facile à installer et à utiliser. Côté serveur, une fois les phases de compilation, installation, configuration, génération des certificats et lien avec la base NIS accomplies, le travail d'administration est quasi nul et n'impose plus que de regénérer les certificats de temps en temps.

Côté client la tâche est aisée, tout du moins sous Linux et Windows. Pour les autres systèmes la tâche peut se révéler complexe, mais le client a au moins le mérite d'exister et de fonctionner parfaitement.

La solution en elle même fournit un très bon niveau de sécurité. Les différents certificats permettent non seulement d'identifier les clients auprès du serveur, mais assurent également les clients qu'ils s'adressent bien au bon serveur. Pour finir l'authentification des clients est réalisée en faisant directement appel à l'annuaire de l'ISIMA.

En conclusion, OpenVPN est une solution mature et flexible qui rempli parfaitement le cahier des charges, tant du point de vue de la sécurité et de la méthode d'authentification que par son caractère multiplate-formes.

2.3 Solution Cisco

2.3.1 Généralités

Les grands équipementiers comme CISCO proposent tous des solutions matérielles pour mettre en oeuvre des connexions VPN. Pour cette étude nous avons utilisé un routeur 2811XM adjoint des fonctionnalités de sécurité avancées fournies par la version `c2800mn-advsecurityk9-mz.124-24.T.bin` de l'IOS.

Le choix d'IPsec s'est imposé comme solution naturelle, car très bien intégrée aux technologies CISCO. Ils proposent de plus un client IPsec multiplate-formes, permettent de gérer le processus d'authentification via certificats, et de s'interfacer à un annuaire d'identification en RADIUS.

2.3.2 Mise en place côté serveur

a) Configuration de base

Commençons par configurer les interfaces du routeur. L'interface connectée au réseau de l'ISIMA récupère son adresse IP via DHCP ce qui ne serait pas le cas dans un environnement de production. En parallèle à cette configuration nous mettons en place deux ACL permettant de s'assurer sur seuls les clients du VPN pourront accéder au réseau interne.

```
(config)# hostname CISCOVPN
(config)# enable secret cisco
(config)# no ip domain-lookup
(config)# access-list 1 permit 10.0.1.0 0.0.0.255
(config)# access-list 2 permit 192.168.1.0 0.0.0.255
(config)# interface FastEthernet0/0
(config-if)# description interface to the external network
(config-if)# ip address dhcp
(config-if)# no shutdown
```

```
(config-if)# exit
(config)# interface FastEthernet0/1.1
(config-if)# description interface to the prof network
(config-if)# encapsulation dot1Q 333
(config-if)# ip address 10.0.0.1 255.255.255.0
(config-if)# ip access-group 1 out
(config-if)# exit
(config)# interface FastEthernet0/1.2
(config-if)# description interface to the student network
(config-if)# encapsulation dot1Q 111
(config-if)# ip address 192.168.0.1 255.255.255.0
(config-if)# ip access-group 2 out
(config-if)# exit
(config)# interface FastEthernet0/1
(config-if)# no shutdown
(config-if)# exit
```

FIGURE 26 – Configuration des interfaces

Configurons maintenant les accès à distance au routeur :

```
(config)# banner login #Unauthorized access prohibited - F5 only!#
(config)# banner motd #
This router is part of a wonderfull ZZ3F5 project for 2008-2009.
If you have any question, comment, insults, whatsoever...
please contact coscia@poste.isima.fr and dessaux@poste.isima.fr.
Thank you if you read this till the end.#
(config)# enable secret cisco
(config)# line con 0
(config-line)# logging synchronous
(config-line)# password cisco
(config-line)# login
(config-line)# exit
(config)# line vty 0 4
(config-line)# transport input telnet
(config-line)# password cisco
(config-line)# login
(config-line)# exit
(config)# service password-encryption
```

FIGURE 27 – Configuration de l'accès à distance

b) Configuration de l'authentification Radius

Dans cette section nous allons interfacer le routeur avec un serveur RADIUS. Pour installer ce serveur nous allons tirer parti du serveur `Linux CentOS 5.1` qui est déjà capable de récupérer les identifiants via l'annuaire NIS de l'ISIMA.

Le serveur à installer est FreeRadius, qui est disponible dans les paquets de la distribution :
`[root@centosvpn ~]# yum install freeradius`

La configuration de base de FreeRadius étant déjà fonctionnelle nous n'auront que très peu de modifications à lui apporter. Tout d'abord nous allons configurer une authentification PAP entre le routeur et le serveur Radius, en ajoutant `ciscovpn User-Password := "isima"` au début du fichier `/etc/raddb/users`, où ciscovpn est le hostname du routeur et isima le mot de passe qui lui sera associé.

Nous allons ensuite autoriser le routeur à se connecter en ajoutant les lignes suivantes dans le fichier `/etc/raddb/clients.conf`, en supposant que `192.168.102.86` est l'adresse IP du routeur sur le réseau de l'ISIMA :

```
client 192.168.102.86 {
        secret = isima
        shortname = isima
}
```

Il reste à indiquer au Radius qu'il doit interroger la base NIS pour obtenir les identifiants et mots de passes utilisateurs. Cela se fait en commentant la ligne indiquant à FreeRadius le chemin vers le fichier `shadow` dans le fichier `/etc/raddb/radiusd.conf`. En effet, en l'absence de fichier `shadow`, FreeRadius se rabat sur les mécanismes d'authentification PAM standarts dont nous avons besoin.

Du point de vue du routeur, le protocole RADIUS étant parfaitement géré par les équipements CISCO la configuration qui en découle est relativement simple :

```
(config)# aaa new-model
(config)# radius-server host 192.168.102.121 auth-port 1812
acct-port 1813 key isima
(config)# ip radius source-interface FastEthernet 0/0
(config)# aaa  group server radius RadiusServer
(config-sg-radius)# radius-server host 192.168.102.121 auth-port
1812 acct-port 1813
(config-sg-radius)# exit
(config)# aaa authentication login default group RadiusServer
```

FIGURE 28 – Configuration de l'authentification Radius

c) Configuration d'IPsec

Les lignes qui suivent permettent de configurer la cryptographie isakmp comme suit :

- algorithme de chiffrement triple DES.
- algorithme de hashage sha-1.
- authentification via clefs partagées.
- Diffie-Hellman 1024 bits.
- durée de vie du contexte cryptographique égale à une journée.
- utilisation du hostname plutôt que de l'adresse IP pour protéger les échanges.

```
(config)# crypto isakmp policy 1
(config-isakmp)# encryption 3des
(config-isakmp)# hash sha
(config-isakmp)# authentication pre-share
(config-isakmp)# group 2
(config-isakmp)# lifetime 86400
(config-isakmp)# exit
(config)# crypto isakmp identity hostname
```

FIGURE 29 – Configuration IKE

Ajoutons les pools DHCP qui fourniront leurs adresses IP aux étudiants et aux professeurs :

```
(config)# ip local pool profs 10.0.1.20 10.0.1.254
(config)# crypto  isakmp client configuration group profs
(config-isakmp-group)# key isimaprofs
(config-isakmp-group)# dns 10.0.0.11
(config-isakmp-group)# domain isima.fr
(config-isakmp-group)# pool profs
(config-isakmp-group)# exit

(config)# ip local pool students 192.168.1.20 192.168.1.254
(config)# crypto  isakmp client configuration group students
(config-isakmp-group)# key isimastudents
(config-isakmp-group)# dns 192.168.1.11
(config-isakmp-group)# domain isima.fr
(config-isakmp-group)# pool students
(config-isakmp-group)# exit
```

FIGURE 30 – Configuration des pools utilisateurs

Configurons maintenant la police IPsec :
- Mise en place de l'ACL pour indiquer que l'on veut filtrer l'ensemble du trafic IP.
- Encapsulation ESP, chiffrement 3des, intégrité sha-1.
- Configuration de l'authentification des profs et des étudiants via le serveur radius.

```
(config)# access-list 101 permit ip any any
(config)# crypto ipsec transform-set policy esp-3des esp-sha-hmac
(cfg-crypto-trans)# exit
(config)# crypto dynamic-map prof-map 1
(config-crypto-map)# set transform-set policy
(config-crypto-map)# exit

(config)# crypto map prof-map
(config)# crypto map prof-map 1 ipsec-isakmp dynamic prof-map
(config)# crypto map prof-map client authentication list RadiusServer
(config)# crypto map prof-map client configuration address respond
(config)# crypto map prof-map isakmp authorization list 101

(config)# aaa authorization network 101 local
```

FIGURE 31 – Configuration de la police IPsec

La présence d'une authentification en fonction de groupes protégés via une clef partagée est une lacune sécuritaire de notre solution. En effet un étudiant pourrait "facilement" se faire passer pour un professeur. Pour remédier à ce problème un mécanisme d'authentification via certificats est nécessaire.

Nous allons utiliser le service Windows 2003 SCEP installé dans la partie 2.1.1.f) page 12. La figure 32 détaille la configuration d'une authentification par certificats sur le routeur. Lors de la requête de certificat, un mot de passe permettant de vérifier la validité de la demande est demandé : il se trouve à l'adresse `http://192.168.102.250/certsrv/mscep/mscep.dll`

```
(config)# crypto ca identity isima.fr
(ca-trustpoint)# enrollment url
http://192.168.102.250/certsrv/mscep/mscep.dll
(ca-trustpoint)# exit
(config)# crypto ca authenticate isima.fr
(config)# crypto ca trustpoint isima.fr
(ca-trustpoint)# crl optional
(ca-trustpoint)# exit
(config)# crypto isakmp policy 1
(config-isakmp)# authentication rsa-sig
(config-isakmp)# exit
```

FIGURE 32 – Configuration de l'authentification via certificats

Il ne reste plus qu'à attendre la validation (manuelle !) de la demande de certificat par l'administrateur du serveur jouant le rôle de l'autorité de certification.

2.3.3 Mise en place côté client

Cette partie présente l'installation du client CISCO sur une machine Windows. Bien que ce client aie la particularité d'être compatible avec Linux nous ne sommes pas parvenus, ni à la compiler (il réclame la compilation d'un module noyau), ni à nous en servir.

L'installation du client est comme pour n'importe quel logiciel sous Windows. Une fois lancé il faut établir une nouvelle connexion (bouton "new"). La figure 33 présente les informations nécessaires à la connexion : legroupe d'appartenance du client, l'adresse IP du serveur et la clé partagé.

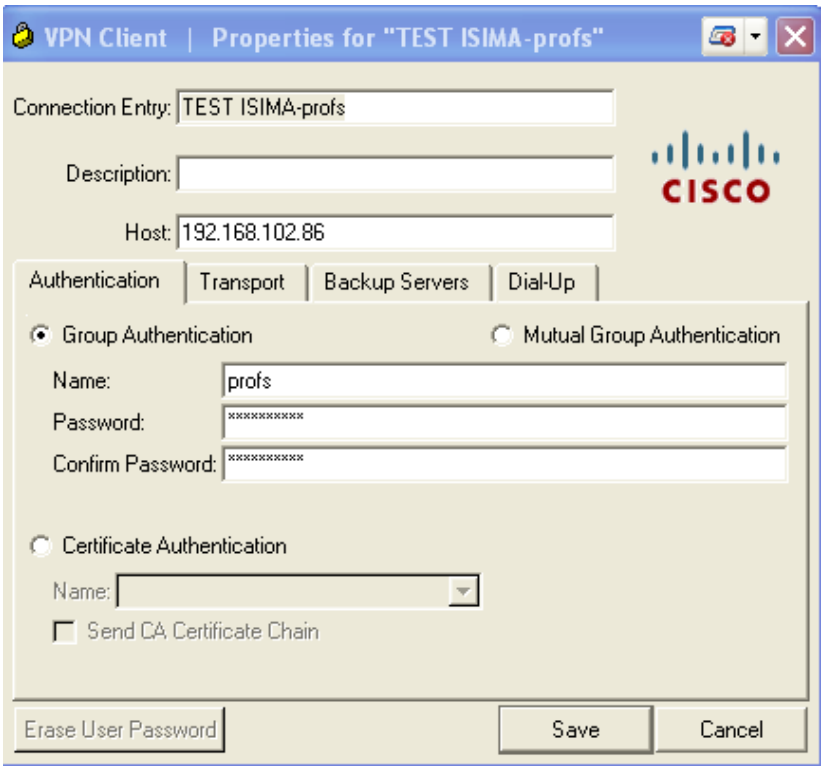

FIGURE 33 – Client CISCO

Si la configuration est correcte, lorsque l'utilisateur tentera de se connecter au VPN il se verra demander ses identifiant et mot de passe, correspondant à ceux inscrits dans l'annuaire de l'ISIMA :

FIGURE 34 – Identification du client

2.3.4 Bilan et limites de la solution

La phase de configuration du routeur a tiré sa difficulté de la complexité inhérente à IPsec. Cette complexité impose de suivre l'ensemble des étapes qui nous avons détaillées "à la lettre" afin de valider par étapes les paramètres de chaque élément constitutif d'IPsec.

L'aspect sécurité est très présent, étant la raison d'être d'IPsec. En effet, dès le début de la phase d'authentification, l'ensemble des échanges est chiffré. Le principal problème que nous avons rencontré concerne le mécanisme d'authentification. En effet, le système en place sur la solution n'est qu'un système à clef partagée car nous ne sommes pas parvenus à aller au bout de la mise en place des certificats. En effet nous avons été capables de fournir des certificats signés par notre autorité au routeur comme au client, néanmoins la connexion n'a jamais pu être établie.

Ceci clos cette partie de mise en place de la plate-forme de test ainsi que la configuration des différentes solutions. Nous allons maintenant effectuer une synthèse de tout cela, en confrontant les avantages et inconvénients de ces différentes solutions.

3 Confrontation des résultats

Dans cette partie, nous allons confronter l'ensemble des résultats obtenus afin de choisir la solution correspondant le plus au cahier des charges fixé en première partie de ce rapport. Nous commencerons par mettre en évidence les critères selon lesquels les différentes solutions seront évaluées, avant d'effectuer la confrontation elle-même, pour finalement établir un bilan.

3.1 Critères d'évaluation

Nous avons établit la liste des critères d'évaluation à partir du cahier des charges que nous nous sommes fixé en première partie de ce rapport. Ce cahier des charges comprenait les 5 axes suivants :

- Facilité de déploiement du serveur.
- Client VPN multiplate-forme.
- Facilité d'installation, de configuration de d'utilisation du client.
- Intégration au sein du réseau de l'ISIMA.
- Niveau de sécurité fourni par la solution.

De ce cahier des charges on dégage rapidement trois catégories de critères à étudier : l'aspect client, le côté serveur, ainsi que le niveau de sécurité.

3.1.1 Côte Client

a) Déploiement du client

Lors de la mise en place de chacune des solutions, nous avons présenté le processus d'installation et de mise en place du client pour l'utilisateur. Nous nous limiterons à un comparatif des clients sous Windows car c'est le seul système pour lequel les clients de chaque solution sont fonctionnels.

Pour la solution VPN de Microsoft, le client étant intégré au système d'exploitation, l'utilisateur a juste à créer une nouvelle connexion et la paramètrer en mode VPN qui prend plus ou moins 30 secondes en suivant les directives présentées en 2.1.2 page 13.

Concernant OpenVPN, l'utilisateur doit dans un premier temps télécharger le client VPN depuis le site officiel (qui aurait éventuellement sa place sur l'Intranet de l'ISIMA). Le client est très léger (978 Ko), mais la durée nécessaire à l'installationdépend des capacité de la machine, le client devat installer une carte réseau virtuelle pour son bon fonctionnement. Néanmoins, une fois installé il suffit de copier le fichier de configuration ainsi que le certificat et la clef utilisateur dans le dossier d'installation. L'ensemble prend 5 à 10 minutes.

La solution CISCO impose, de même que pour OpenVPN, de télécharger leur client. Celui-ci est plus conséquent (9 Mo) et aurait également sa place sur l'intranet de l'ISIMA. L'installation est par contre rapide (moins de 2 minutes). Pour la configuration du client, l'utilisateur a le choix. Soit il configure manuellement la connexion VPN, cela sous-entendant qu'il en connaisse les paramètres, soit il importe directement un fichier de configuration (environ 1Ko). La procédure prend en tout de 5 à 10 minutes.

D'un point de vue déploiement du client VPN, la solution de Microsoft reste donc la plus avantageuse sous Windows.

b) Délai de connexion

Nous nous sommes intéressés à évaluer la durée nécessaire à l'établissement de la connexion VPN. Avec le client CISCO, le délai de connexion est assez long. En effet, la connexion s'effectue en deux phases, avec tout d'abord l'authentification IKE, et ensuite l'identification en interrogeant le serveur RADIUS qui lui même interroge la base NIS.

Avec le client Windows, nous avons remarqué que le temps de connexion était plus rapide qu'avec le client CISCO. Cependant, la phase de challenge MD5 peut être longue en fonction de la charge réseau à laquelle le serveur est soumis.

Avec le client OpenVPN, l'utilisateur s'authentifie et s'identifie très rapidement en comparaison des deux autres solutions. Nous pensons que la présence d'un certificat signé sur le poste utilisateur accélère cette phase de connexion.

Concernant le délai de connexion, le client de OpenVPN s'avère être le plus performant. Il est à noter que nous n'avons pas souhaité mésurer avec précision le délai de connexion, car ne s'agissant que d'une maquette sur un réseau local une telle mesure n'aurait pas été représentative.

3.1.2 Côté Serveur

a) Déploiement du serveur

L'installation du serveur OpenVPN a été particulièrement longue. En effet, il a fallu dans un premier temps installer sur le serveur CentOS l'ensemble des dépendances nécessairesà la compilation d'OpenVPN, à le compiler, puis enfin à installer le logiciel. Une fois l'installation terminée, il nous a fallu générer les différents certificats pour les groupes PROFS et STUDENTS. En dernier temps il a fallu interfacer le serveur avec la base NIS de l'ISIMA pour récupérer les identifiants et mots de passes des utilisateurs.

Pour Windows Server, nous avons dû installer quatre services différents : DNS, DHCP, Active Directory, Service d'accès distant. Une fois cette phase achevée, la configuration de chacun de ses services a été effectuée rapidement en comparaison d'OpenVPN.

Enfin pour la solution CISCO, le serveur VPN est inclus dans le matériel. Toutefois nous avons dû installer un serveur RADIUS sur le serveur Linux afin que celui-ci consulte la base NIS pour authentifier l'utilisateur. L'avantage de la solution CISCO est que le fichier de configuration du routeur peut-être sauvegardé et réutilisé. Si un jour le routeur tombe en panne, il faudrait moins de dix minutes pour que le nouveau routeur démarre et récupère la configurationvia TFTP.

On se rend compte rapidement que la solution CISCO est la plus adapté du point de vue temps d'installation mais aussi du point de vue de l'administration requise.

Rappelons qu'aucune des trois solutions n'est indépendante et autonome. En effet, chacune d'entre-elles a besoin d'un autre serveur pour fonctionner : Windows a besoin de se synchroniser avec le serveur ISIMA pour répliquer son Active Directory, OpenVPN fonctionne conjointement avec la base NIS, quant au routeur il dépend du serveur RADIUS qui dépend du NIS.

b) Coût de chaque solution

Il nous était impossible de proposer la meilleure solution VPN sans évoquer l'aspect financier. En effet chacune des ces solutions a un coût, à commencer par la solution CISCO qui est la plus onéreuse

des trois, à cause de l'investissement matériel nécessaire. Pour Microsoft, la coût de la solution est à imputer à la licence, tandis que OpenVPN étant Open-Source le coût est nul.

D'un point de vue coût on se rend compte que la solution OpenVPN est la plus avantageuse par rapport au deux autres.

3.1.3 Sécurité

a) Authentification et identification

Ce critère concerne la manière dont un client est authentifié et identifié. Pour la solution Microsoft, Le système d'authentification en place est un système faible à base de clefs partagées. L'identification passe par un annuaire Active Directory local référençant les identifiants et mots de passes. Rappelons que l'une des faiblesses de l'identification avec MS-Chap v2 était que l'identifiant utilisateur ciscule en clair sur le réseau.

La solution CISCO utilise également une authentification via clefs partagées. Par contre l'identification faitintervenir un serveur RADIUS qui lui même consulte la base NIS de l'école afin de récupérer les identifiants de l'ISIMA.

Quant à OpenVPN l'authentification se fait par l'intermédiaire de certificats signés. Il s'agit du moyen le plus sûr mis en place sur la plate-forme. L'identification passe par une consultation de la base NIS.

D'un point de vue authentification et identification, la solution OpenVPN est la plus fiable. Rappelons malgré tout que la solution CISCO peut également fonctionner avec des certificats mais nous ne sommes jamais parvenus à mettre ce système en place, d'où notre choix pour OpenVPN.

b) Efficacité des algorithmes de chiffrement

Lors de l'implémentation des trois solutions, nous avons remarqué une différence sur le type de chiffrement exploités par les solutions. Microsoft utilise un chiffrement symétrique de type MPPE avec une clef de 128 bits. Un inconvénient est que les systèmes d'exploitation antérieur à Windows XP sont incapables de le gérer, et réclameraient un chiffrement plus faible.

La solution CISCO utilise elle aussi un chiffrement symétrique mais sur 168 bits. OpenVPN quant à lui utilise une première phase de négociation en chiffrement asymétrique basé sur des certificats et clefs RSA de longueur 1024bits, puis se rabat sur un chiffrement symétrique 256 bits.

La comparaison au niveau sécurité élimine clairement la solution de Microsoft (dans l'état où nous l'avons configurée) de la liste des solutions envisageable. Nous ne pouvons départager OpenVPN et CISCO car les deux types de chiffrements se vaudraient si seulement l'authentification via certificats avait fonctionné sur le routeur.

3.2 Analyse des performances

Dans cette section nous allons mener une analyse des performances de chaque solution, en termes de quantité de trafic que les machines sont capables de traiter. En raison de l'utilisation massive des algorithmes de chiffrement et déchiffrement, ce sont les capacités processeur des machines seront déterminantes.

Nous avons utilisé un outil Open-Source afin de mener à bien cette évaluation des performances. Ce logiciel très simple nommé IPperf envoie simplement le plus de paquets d'un point à un autre.

3.2.1 Configuration d'IPperf

Le but de ce benchmark est de générer du trafic et de forcer son passage à travers le tunnel VPN. Pour pouvoir effectuer des mesures, IPperf doit être lancé sur une machine cliente d'un côté du tunnel, ainsi que sur une machine serveur de l'autre côté :

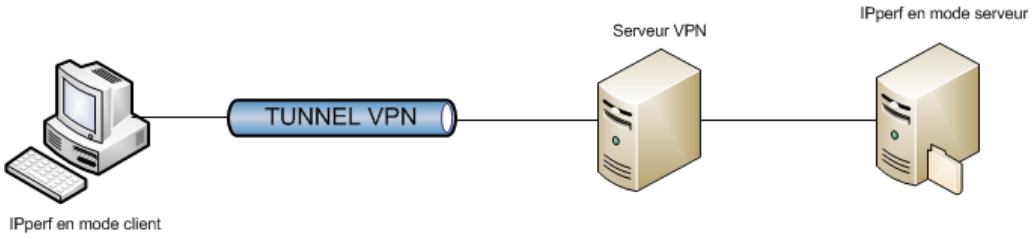

FIGURE 35 – Protocole de test

Voici la configuration d'IPperf : En mode serveur : `iperf.exe -s -i1`. L'option `-s` correspond au mode serveur et le `-i1` correpond à la fréquence de prise de mesure (ici une seconde).

En mode client : `iperf.exe -c 10.0.1.25 -i1 -t40` . L'option `-c` correspond au mode client et l'option `-t40` indique la durée pendant laquelle on va générer du trafic.

3.2.2 Confrontration des résultats

Voici les caractéristiques de la plateforme ayant fait office de serveur :

Caractéristiques	Machine
CPU	Intel Core 2 Duo T8100 2,10GHz
RAM	3 Go
Carte réseau	Intel 82566MM Gigabit

FIGURE 36 – Caractéristiques de la plateforme serveur

Les machines clientes utilisées sont celles présentes en salle A214. La figure 37 présente les résultats que nous avons obtenus. Le débit indiqué correspond à une moyenne sur quarante secondes :

Solutions	WINDOWS	LINUX	CISCO
Bande Passante(moyenne)	18Mbps	50Mbps	31Mbps
Utilisation CPU	100%	80%	100%

FIGURE 37 – Résultats des benchmarks

Le taux d'utilisation processeur n'est pas fournit par IPperf. Cette valeur a été obtenue directement en visualisant la charge de la machine. Dès lors que du trafic traverse le tunnel, les serveurs VPN se trouvent fortement sollicités, et il devient rapidement très difficile d'exécuter une tâche en parallèle. Comme prévu, le taux d'occupation processeur est le facteur limitant pour chaque solution, ce dernier étant responsable du traitement des packets transitant sur le carte réseau.

En terme de bande passante, la solution OpenVPN se révèle être la plus performante. Cependant, nous avons remarqué des fluctuations durant les mesures, ce qui n'est pas le cas de routeur CISCO dont le débit est extrêment stable.

3.3 Bilan

Notre bilan commence par une comparaison de la comptabilité des solutions VPN avec les systèmes d'éxploitation les plus répandus :

OS	Solution Windows	Solution Linux	Solution CISCO
Windows	Oui	Oui	Oui
Linux	Oui en théorie, Non en pratique	Oui	Oui
MAC (en théorie)	Oui	Oui	Oui

FIGURE 38 – Compatibilité des clients VPN avec les différents OS

Les solutions CISCO et OpenVPN répondent au cahier des charges en terme de compatibilité multiplate-formes. Il est à noter que nous n'avons pas pu tester nos différentes solutions sur MAC.

Afin de choisir la meilleure solution VPN, nous avons décidé de mettre des notes échelonnées de zéro (mauvais) à cinq (excellent) sur chacuns des critères que nous avons expliquer et de les regrouper dans des graphes comparatifs.

Sur chaque graphe nous trouverons les critères suivants :
- Déploiement du serveur.
- Bande passante effective.
- Utilisation CPU.
- Coût.
- Stabilité de connexion.
- Déploiement du client.
- Niveau de sécurité.

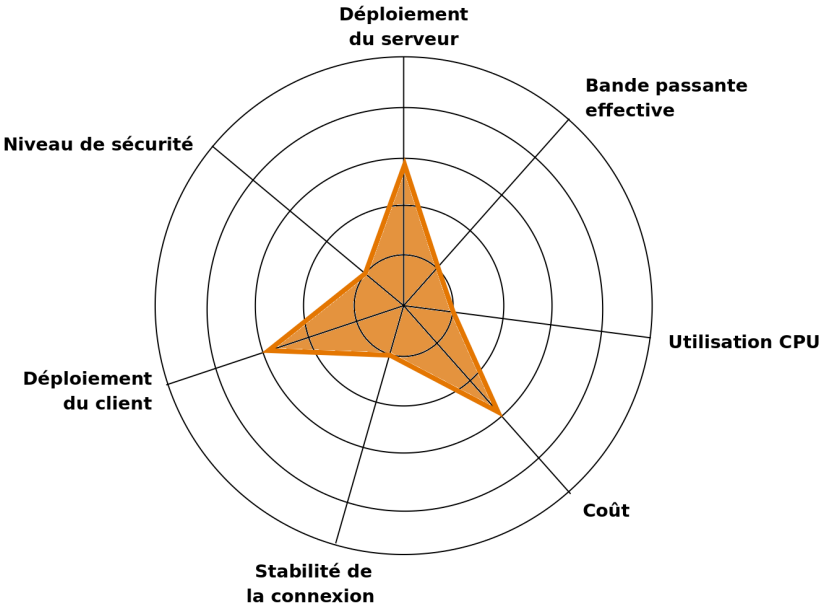

FIGURE 39 – Bilan final de la solution Windows

En sommant les différents critères la solution Microsoft obtient une note égale à `13`

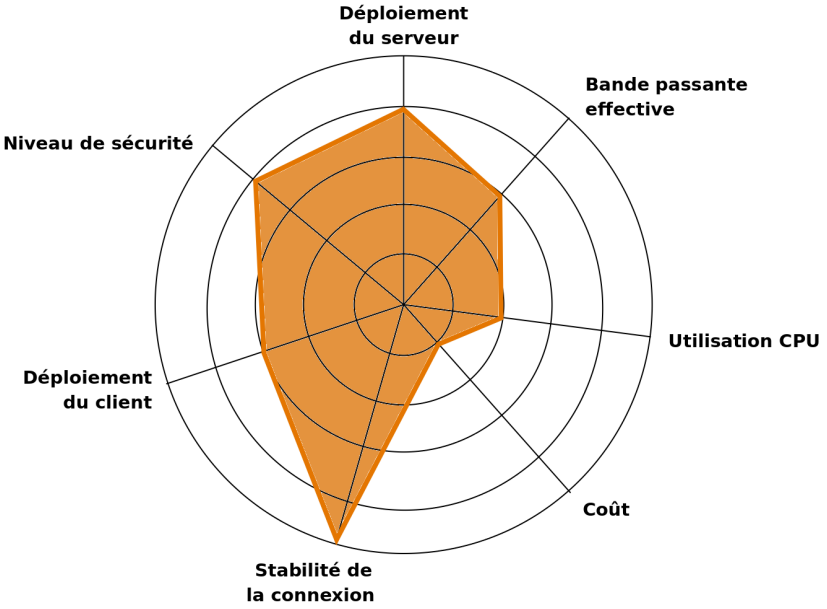

FIGURE 40 – Bilan final de la solution cisco

En sommant les différents critères la solution Cisco obtient une note égale à `21`

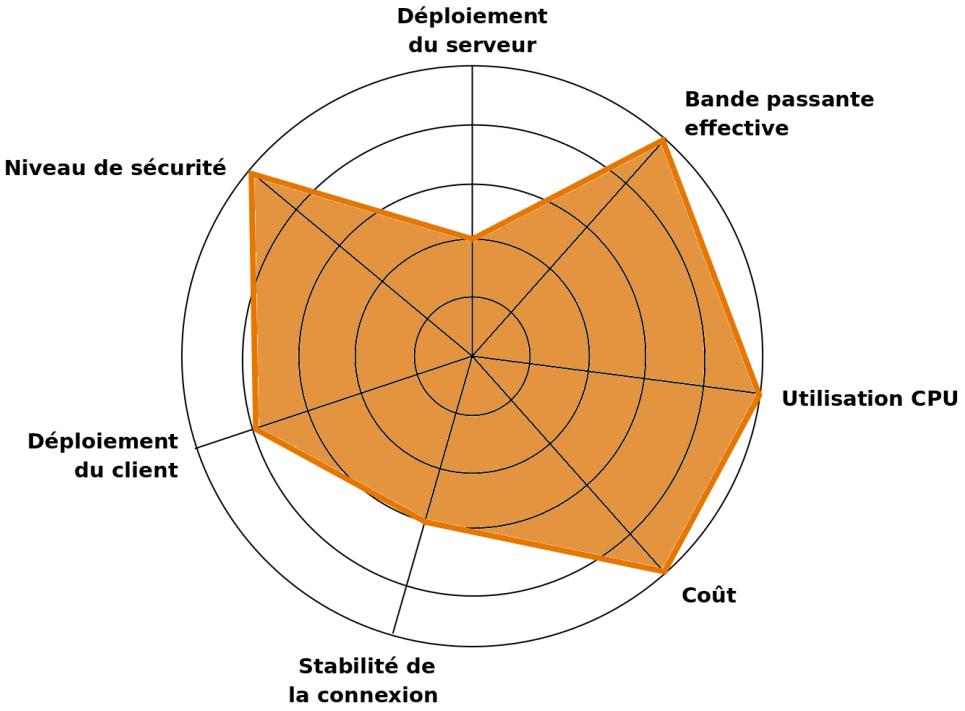

FIGURE 41 – Bilan final de la solution Linux

En sommant les différents critères la solution Linux a une note égale à 29

Au vue de ces différents bilans prenant en compte l'ensemble des critères que nous avons pu aborder au cours de cette partie, nous pouvons conclure que la solution OpenVPN serait la plus adaptée à la mise en place d'un accès VPN au sein de l'ISIMA.

Conclusion

L'objectif de ce projet était d'étudier la mise en place de trois solutions VPN. Nous avons commencé par étudier la solution de Microsoft, puis le logiciel OpenVPN sous Linux, et enfin la solution de CISCO. L'étude de ces solutions a été guidée par plusieurs critères constituant notre cahier des charges, comme la facilité de déploiement des clients et du serveur, le niveau de sécurité de l'accès et enfin la complexité de l'administration du serveur VPN.

Au cours de ce projet, nous avons rencontré trois grandes difficultés. La première concerne la problématique de la sécurité, car même si nous avons une formation théorique sur les différents protocoles et mécanismes qui y sont liés, cela reste insuffisant pour comprendre les enjeux de la sécurité. Ce projet a été pour nous l'opportunité d'appliquer nos bagages théoriques à un problème concret.

Une seconde difficulté concerne le peu de documentation sur ce sujet. En effet, dès que l'on commence à chercher des informations spécifiques, comme par exemple la configuration d'un service en particulier, ou sur la génération de clefs on ne trouve rien de concluant. Même sur les sites des différents constructeurs, l'informations n'est pas explicitement présentée. Une dernière difficulté, concerne les limitations du système d'exploitation de Microsoft. En effet, il nous a fallu du temps pour comprendre que les services réseau se lient à une seule carte, même si leur fonctionnement doit en impacter plusieurs. Nous avons essayer de trouver divers moyens pour contourner ce problème mais sans aucun succès.

Dans un futur proche, nous pensons que nos différentes maquettes peuvent être améliorées. En effet, pour la solution CISCO il faudrait achever de mettre en place une authentification par certificats pour améliorer le niveau de sécurité. Concernant OpenVPN, on pourrait envisager d'implementer un renouvellement automatique des certificats chaque année, qui les publierait directement sur l'intranet de l'ISIMA.

Si l'ISIMA souhaite concrétiser son projet de solution VPN, nous recommandons l'implémentation d'OpenVPN car il est a parfaitement répondu au cahier des charges, se révélant à la fois performant, sécurisé et compatible avec n'importe quel type de système d'exploitation.

Bibliographie

[1] Mise en place d'un client RADIUS sous Windows [en ligne]. Etats-Unis. Disponible sur http://technet.microsoft.com/fr-fr/library/cc757473.aspx

[2] Installation du service VPN sous Windows [en ligne]. Etats-Unis. Disponible sur http://technet.microsoft.com/fr-fr/library/cc781701.aspx

[3] Documentation générale sur WindowsServer2k3 [en ligne]. Etats-Unis. Disponible sur http://technet.microsoft.com/fr-fr/library/cc706993.aspx

[4] Documentation de Windows Services for Unix [en ligne]. Etats-Unis. Disponible sur http://technet.microsoft.com/fr-fr/library/bb463193.aspx

[5] Service SCEP sous Windows [en ligne]. Etats-Unis. Disponible sur http://www.microsoft.com/downloads/details.aspx?FamilyID=9f306763-d036-41d8-8860-1636411b2d01\&DisplayLang=en

[6] Site officiel d'OpenVPN [en ligne]. Etats-Unis. Disponible sur http://openvpn.net/

[7] Document The User-Space VPN and OpenVPN [en ligne]. Etats-Unis. Disponible sur http://openvpn.net/papers/BLUG-talk/index.html

[8] CISCO IOS Cookbook, O'REILLY, Kevin Dooley & Ian J. Brown, 2007.

[9] Site officiel de CISCO [en ligne]. Etats-Unis. Disponible sur http://www.cisco.com

[10] Site officiel du générateur de traffic IPPERF [en ligne]. Etats-Unis. Disponible sur http://www.noc.ucf.edu/Tools/Iperf/

Lexique

Annuaire : Base de données contenant les informations des utilisateurs.

Chiffrement : Procédé cryptographique permettant de rendre illisible un document.

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.

NIS : Network Identification System. Protocole standart pour l'échange d'identifiants sous Unix.

PAM : Pluggable Authentification Modules, Système d'authentification standart sous Unix.

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 d'intermédiaire aux transactions.

TCP : Protocole de transport fiable au dessus de IP.

TLS : Protocole de session sécurisé et reposant sur TCP.

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

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

Table des figures