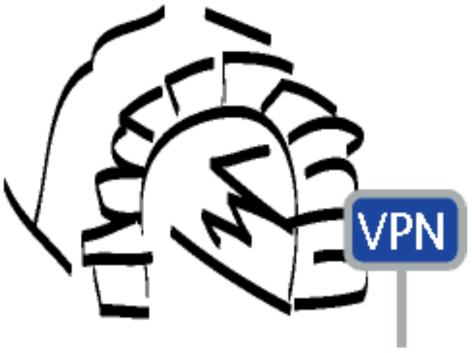
Jérémie
Dupraz-Dange
TSMSI 10/04

Mise en place d'une interconnexion VPN



Formation de Technicien Supérieur en Maintenance
et Support Informatique

Tuteur: Yannick Recour

Ce document a été réalisé à l'aide de nombreux logiciels libres (The GIMP, Winefish, iTexMac, TexLive DVD 2004)
et Visio 2003 de Microsoft pour les schémas.

Remerciements

Tout d'abord, je tiens à remercier :

Mon tuteur, Yannick Recour, et le directeur de l'entreprise NBM-Europe, Olivier Bail, pour m'avoir accueilli dans leur entreprise (ce qui m'a permis de suivre la formation TSMSI) ainsi que de m'avoir soutenu, appuyé et conseillé durant les deux années du cycle. En outre, ils m'ont donné la possibilité de travailler rapidement de façon autonome.

Les employés de la société (Alex Favre-Félix, Yves Michel-Grosjean et Pierre-Sébastien Hervé) pour leur disponibilité et leur aide lorsque j'étais en difficulté mais également pour le partage de leurs connaissances et de leurs expériences.

Ma famille et mes proches qui m'ont soutenu durant ces deux années.

Synthèse

Le projet que je vous présente dans ce mémoire est la mise en place d'une interconnexion de type VPN*[1]. Cette interconnexion permet d'accéder à des ressources et à des services appartenant à un réseau privé (comme celui d'une entreprise) d'une façon tout à fait sécurisée et transparente depuis un accès Internet quelconque.

Cette technologie peut être utilisée dans de nombreux cas de figures. Un commercial peut, par exemple, lors d'un déplacement récuperer rapidement des données tarifaires à jour qu'il aurait oubliées, cela, à la seule condition qu'il ait une connexion Internet. Un télé-travailleur peut retrouver des documents pour les éditer comme s'il était dans les bâtiments de l'entreprise. Enfin, on peut également relier deux sites géographiques d'une société pour ne faire qu'un réseau unique et logique. Les utilisateurs ne sauraient alors pas s'ils travaillent sur des données situées à distance ou non.

L'utilisation de cette technologie croît rapidement car les entreprises doivent être toujours plus souples et plus réactives. Par ailleurs, le fait de centraliser des données permet un gain pécunier pour les investissements dans les équipements matériels mais également pour les maintenances.

La simplicité d'accès à toutes ces informations ne doit toutefois pas se faire au détriment d'une baisse de la sécurité globale. C'est pour cela que je vous présente en détail dans le projet les solutions actuelles les plus abouties qui intègrent dans leurs fonctionnements des algorithmes d'authentification et de chiffrement.

Ces solutions ont été ensuite comparées car elles ne sont équivalentes, ni au niveau de leurs sûretés et de leurs facilités d'utilisation, ni au niveau de leur coût de mise en place et de maintenance. Les protocoles* de tunnellisation, PPTP et IPSec (mécanisme ESP), ont répondu au mieux aux différents critères définis suivant les besoins des entreprises et des utilisateurs et ont donc été retenus pour l'élaboration du projet.

[1] lorsqu'un mot est suivi d'un asterisque, sa définition se trouve dans le glossaire

Table des matières

Introduction

L'informatique a toujours été une passion pour moi et jusqu'à cette formation, je n'ai jamais suivi de cours d'informatique proprement dit. J'ai donc étudié ce domaine de façon autodidacte ou en effectuant des stages.

À la fin de ma Terminale Générale Scientifique, j'ai alors décidé de commencer à rentrer concrètement dans le monde actif. La formation de Technicien Supérieur en Maintenance et Support Informatique du CESI s'est présentée à moi et correspondait tout à fait à mes attentes en proposant le système de l'alternance et une formation très technique. Le fait de suivre une formation par alternance m'a alors permis d'améliorer très rapidement mes compétences techniques à l'administration des réseaux.

Durant ce cycle de formation, en entreprise, j'ai pu prendre conscience de certains besoins des entreprises. Une de leur demande a fait l'objet de ma problématique pour mon mémoire : la mise en place d'interconnexion VPN*, c'est-à-dire le moyen d'accéder à des services privés de façon sécurisé depuis le monde entier.

Dans mon mémoire, je commencerais par vous présenter l'entreprise NBM-Europe, qui m'a accueilli en décrivant son organisation, ses services et la place qu'y tient l'informatique. La deuxième partie de ce document explique et synthétise les deux années de l'alternance. Enfin la dernière partie est ma problématique, mon projet.

Note : Tout terme suivi d'un astérisque sera explicité dans le glossaire.

Chapitre 1

Présentation de l'entreprise

1.1 Pour commencer

Afin de suivre ma formation TSMSI par alternance au CESI d'Ecully, j'ai été embauché par la société NBM-Europe. Il s'agit d'une jeune PME fondée au mois de septembre de l'an 2000 et au capital de 20'800 €. Elle est implantée à Prevessin-Moëns dans le Pays de Gex, tout près de la frontière Suisse et de Genève.

Lors de mon arrivée en septembre 2004, l'entreprise comptait trois employés au total. Aujourd'hui, nous sommes six à y travailler (dont quatre à plein-temps et deux en alternance).

NBM-Europe est une Société de Services en Ingéniérie Informatique, aussi appelée une SSII. Elle vend donc ses services et compétences en informatique et réseaux à des entreprises mais aussi à des particuliers exigeants. Afin de diversifier son marché et de suivre les attentes de ses clients, elle assure, en plus, un service pour la téléphonie et est en mesure de s'occuper de la mise en place des câblages (réseaux et téléphoniques). Des formations sont également proposées aux particuliers et aux entreprises. Il lui est possible de fournir ce panel de services car chacun des employés de NBM-Europe dispose de ses compétences propres. Les prestations de l'entreprise sont décrites en détails dans la partie suivante[1].

La réputation de la Suisse voisine oblige la société à être très vigilante sur la qualité de ses services. Elle se veut dynamique et dispose donc de trois véhicules pour répondre rapidement et en toutes circonstances aux interventions urgentes.

La clientèle est très variée, NBM-Europe travaille principalement avec des entreprises Suisses ou Françaises mais aussi avec un certain nombre de collectivités locales qui lui font confiance. Une antenne suisse de la société s'est d'ailleurs ouverte au cours de l'année 2005 pour satisfaire la clientèle helvète. Il arrive que des déplacements à l'étranger pour des organismes internationaux ou des travaux avec des entreprises informatiques étrangères soient nécessaires. Les particuliers ne représentent eux qu'une faible partie des interventions.

L'entreprise dispose d'un local de 200 m^2 (comprenant la boutique, l'atelier, les bureaux, la salle de formation et la réserve), pour accueillir la clientèle et lui présenter les produits et solutions. Ci-dessous trois photos de la boutique (vitrine et intérieur).

[1] Chapitre 1 : Section 2

1.2 Les domaines d'activité

1.2.1 L'informatique

Lors de la fondation de la société, l'informatique était la seule compétence proposée à la clientèle. Aujourd'hui, il s'agit toujours de son activité principale. Pour répondre à toutes les demandes et besoins de ce domaine très vaste, deux équipes techniques aux missions complémentaires ainsi qu'une équipe commerciale ont été définies.
Il arrive cependant que ces équipes soient temporairement et ponctuellement modifiées (lors de l'absence d'un des techniciens ou lors de missions spécifiques).

Nous avons tout d'abord une équipe qui est orientée sur les interventions dites "locales". Cette dernière est composée de deux personnes et fournit un panel de services pour tout ce qui compose un ordinateur personnel (moniteur, unité centrale, périphériques[2], logiciels, pièces, connexions internet...). Comme tout cela est lié à une machine unique, l'équipe s'occupe rarement de problèmes réseaux et reste généralement au sein de l'entreprise dans l'atelier. Elle a donc également en charge la réception des appels téléphoniques, et éventuellement leur orientation vers la personne concernée, mais aussi l'accueil de la clientèle lors de son passage au magasin.

FIG. 1.1 – Réparation d'un ordinateur

Les services proposés peuvent être résumés comme ci-dessous :

- La vente du matériel d'usage personnel
- La maintenance (réparations matériels et logiciels)
- L'expertise (conseils à la clientèle sur les produits les plus adaptés)
- La livraison (possibilité de livrer le matériel et de l'installer sur place)
- La location et/ou le prêt (lors d'une panne prolongée, par exemple)
- La mise en place de petits réseaux domestiques

La deuxième équipe technique qui est également composée de deux personnes, est davantage tournée vers les interventions de types réseaux. C'est-à-dire de ce qui touche aux produits du genre : serveur, onduleur, connexion internet professionnelle, logiciels (réseaux, de sauvegarde...), hébergement... Les services proposés par cette équipe sont relativement similaires à ceux de la première :

- La vente de produits orientés réseaux
- La maintenance (installation et réparation)
- Le support (contact avec les sociétés de garantie, avec le registrar* de leur domaine...)
- L'expertise (conseils et étude de mise à jour...)
- La livraison (installation du matériel sur place)

FIG. 1.2 – Intervention sur une baie de brassage

Cette équipe est bien entendu le plus souvent en déplacement chez des professionnels. De plus, si une entreprise cliente est liée avec NBM-Europe par un contrat de maintenance, cette équipe procède à une maintenance préventive de son système d'informations et dispose d'un accès distant lui permettant de faire de la télémaintenance*.

Enfin, pour finir, le chef d'entreprise travaille avant tout comme commercial. Il rencontre ainsi la clientèle, pour lui présenter de nouveaux produits qui pourraient lui être utiles et répondre à ses besoins. De plus, il planifie les rendez-vous avec les techniciens ou intervient sur des problèmes techniques lors de congés.

[2]imprimante, scanner, webcam...

Ci-jointes, deux photos de l'atelier des réparations :

1.2.2 La téléphonie et le câblage

Les services offerts par l'entreprise, en téléphonie, sont arrivés plus tard durant l'année 2001. Le chef d'entreprise s'était alors associé avec un spécialiste, permettant à NBM-Europe d'offrir cette nouvelle compétence. Aujourd'hui, la téléphonie reste son deuxième secteur d'activité mais elle n'en est pas moins importante. En effet, cela est un point très positif pour la clientèle, car elle n'a alors qu'une seule entreprise interlocutrice à contacter en cas de problèmes.

L'associé planifie et organise des interventions pour les personnes de l'équipe informatique "locale" mais a également d'autres tâches sous sa responsabilité :

Bien sûr, il offre son savoir faire en téléphonie à la société et donc assure toutes les interventions liées à ce domaine (pour les entreprises comme pour les particuliers) :
- La vente du matériel téléphonique.
- L'installation de nouveaux produits (téléphone, fax, centraux téléphoniques, VoIP* (Figure 1.3)...).
- La maintenance d'une infrastructure existante.
- Le conseil aux clients sur les différents produits existants.

Fig. 1.3 – Un exemple de téléphone IP

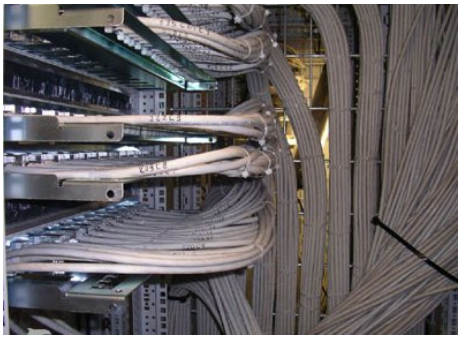


Fig. 1.4 – Câblage Informatique

Il assure, ensuite, l'installation des différents câblages (réseaux informatiques et téléphoniques (Figure 1.4)) même si bien sûr lors de gros chantiers, un ou plusieurs autre(s) technicien(s) l'accompagne(nt) pour l'aider. Il peut donc aussi mettre en place des goulottes, des prises réseaux, une armoire de brassage*...

Il est aussi responsable de la gestion des commandes de matériel. Les équipes informatiques lui ayant communiqué au préalable les besoins de leurs activités respectives. En relation avec cela, il s'occupe, en plus, des procédures de retours de marchandises informatiques et téléphoniques défectueuses couvertes par les garanties.

Ces services l'obligent à être souvent en déplacement chez des professionnels pour, tout d'abord, faire l'état des lieux avant de commencer des chantiers et pour, ensuite, mettre en place les équipements.

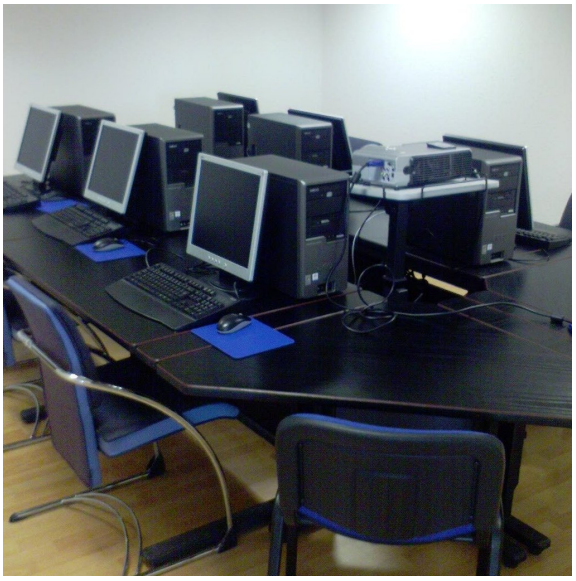
1.2.3 La formation

Depuis le début de l'année 2005, NBM-Europe met à la disposition des entreprises une salle de formation comportant sept postes informatiques, dont un pour le formateur équipé d'un vidéo-projecteur. Les entreprises ayant un grand besoin d'initier ou de perfectionner leurs personnels à l'outil informatique pour augmenter leur productivité, peuvent ainsi louer la salle pour la journée en général. Dans le cas de formations professionnelles, le formateur est un intervenant extérieur. Ce dernier point permet à la société de proposer de nombreuses formations aussi bien pointues que variées et d'assurer en même temps la qualité de la pédagogie.

Des particuliers peuvent également faire une demande de formation. À l'origine celles-ci devaient être dispensées par un des employés de NBM-Europe si le nombre de personnes ayant fait une demande similaire était suffisant. Mais l'entreprise s'est rapidement tournée vers une personne ayant une solide expérience de pédagogue. Cette personne assure donc, aujourd'hui, les formations pour particulier avec des sujets variés tel que : les systèmes d'exploitation Windows[3] et MacOS[4], Office[5], Photoshop[6], FileMaker[7]... Il est possible également de suivre ces formations à domicile. Une fiche d'information détaillée sur les formations proposées à NBM-Europe est jointe en Annexe 1.

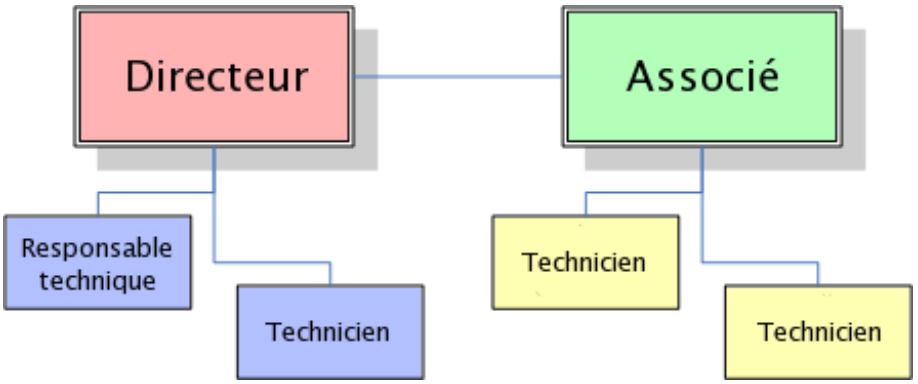
À l'heure actuelle, la formation est une activité jeune et marginale de NBM-Europe. Son développement est freiné par la méconnaissance de cette prestation de la part de notre clientèle.

Ci-dessous, une photo de la salle de formation :



[3]Windows est une marque déposée par Microsoft Corporation http ://www.microsoft.com
[4]Mac OS est une marque déposée par Apple Computer http ://www.apple.com/
[5]Office est une marque déposée par Microsoft Corporation http ://www.microsoft.com
[6]Photoshop est une marque déposée par Adobe http ://www.adobe.com
[7]FileMaker est une marque déposée par FileMaker, Inc http ://www.filemaker.com

1.3 Organigramme de la société



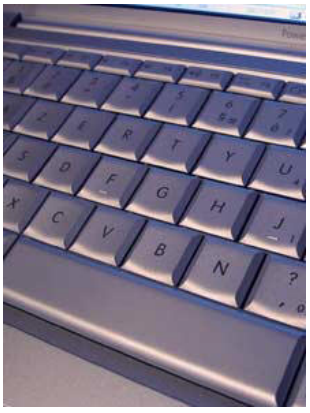
Les couleurs représente les fonctions de chacun.
En rouge, nous avons le commercial qui dirige l'équipe "réseau" en bleue.
Et nous avons l'associé en vert qui dirige lui l'équipe "locale" en jaune.

1.4 Une entreprise au coeur de l'informatique

À NBM-Europe, l'informatique est un outil omniprésent et la place qu'il occupe dans l'entreprise est capitale. En effet, l'informatique est le domaine de compétence de la société. Mais, cette dernière est également dépendante de cet outil pour ses propres besoins. Nous pouvons donc distinguer deux types de relation entre NBM-Europe et l'informatique : "une externe" et "une interne".

1.4.1 Une informatique d'extérieur

La première relation, qualifiée "d'externe", existe bien sûr depuis la création de la société puisqu'il s'agissait du service de base proposé par NBM-Europe à la clientèle étrangère et il le reste encore à l'heure actuelle. Les différentes voies prises par la société, ces dernières années, se caractérisent toujours par cette relation (la téléphonie, la formation...). Nous pourrions penser que le domaine de la téléphonie n'est pas lié à cette relation mais cette dernière existe car un phénomène récent est apparu : la convergence des supports de l'information. En effet, le second domaine d'activité : la téléphonie, se rapproche de plus en plus de l'informatique. Par exemple, sur certains points, les deux domaines ont déjà fusionné, comme dans le cadre de la VoIP*.



Concrètement, cette relation "externe" concerne directement cinq emplois sur six de la société et indirectement le sixième (le spécialiste en téléphonie). Elle représente donc la totalité de la main d'oeuvre aussi bien en temps qu'en moyens. Tout cela même si les missions et objectifs des employés de la société diffèrent bien souvent.

L'informatique est tout simplement le moteur de l'entreprise et lui permet d'exister.

1.4.2 Une informatique d'intérieur

La seconde relation, qualifiée "d'interne", est pour sa part une conséquence de la dépendance que NBM-Europe possède vis-à-vis de cet outil. Cette dépendance découle de deux besoins vitaux de la société.

Un service à la productivité

L'informatique est pour commencer un outil au service de la productivité, c'est-à-dire qu'il aide à gagner du temps sur des tâches quotidiennes mais néanmoins indispensables. Nous pouvons

citer, par exemple, la facturation, la comptabilité, la gestion des stocks ou de tous types de documents administratifs. Toutes ces informations, bien qu'indépendantes du domaine d'activité d'une entreprise, sont complètement traitées et stockées par informatique.

Un service à l'activité

L'informatique est également un outil au service de l'activité. Le domaine d'activité est donc bien la cause de cette autre dépendance de l'informatique. Plus concrètement, il s'agit des outils d'intervention, de dépannage et de travail. Les possibilités d'interventions à distance chez les clients, la messagerie interne, les facultés de s'informer (chez les constructeurs ou dans des bases de connaissances en ligne*), les sauvegardes des clients situées sur les serveurs ou encore le système de suivi des interventions sont autant d'outils nécessaires à l'accomplissement de celles-ci.

Le travail quotidien est donc entièrement assisté par l'outil informatique.

1.5 Mon rôle au sein de NBM-Europe

À l'origine, ma candidature pour NBM-Europe était spontanée. La société recherchait tout de même un technicien à plein-temps. Cependant, la répartition du travail entre l'entreprise et l'école de trois semaines pour une semaine a séduit le chef d'entreprise. Mes connaissances en informatique, acquises de façon autodidacte, ont jouées un rôle déterminant dans le choix de ma candidature.

1.5.1 La première année

La première année, j'ai pour la première fois mis les pieds dans le monde de l'entreprise. Bien heureusement, j'ai su m'adapter facilement aux nouvelles situations que je rencontrais. Cela m'a permis de me sentir rapidement à l'aise avec les employés.

J'ai travaillé pour commencer avec l'équipe "locale". Comme cette dernière reste dans les locaux de l'entreprise, l'équipe de NBM-Europe a pu vérifier et étalonner mes compétences et connaissances préexistantes en informatique. Les employés ont alors rapidement eu confiance en moi. J'ai eu de nombreuses tâches variées à exécuter touchant ou non à l'informatique (comme des livraisons ou des tâches administratives...). En informatique, mes interventions restaient tout de même relativement simples et rapides à réaliser. Il était déjà prévu que j'intègre l'équipe en charge des interventions de type réseau, je suis donc tout de même intervenu chez des professionnels et cela de plus en plus fréquemment avec le temps ; afin que je puisse connaître la clientèle de la société et puisse me sentir à l'aise lors de déplacements.

Durant cette année, j'ai plutôt joué le rôle de soutien et de "tampon", en allégeant le travail des employés lors de périodes chargées, mais je me suis également préparé à mon changement d'équipe.

1.5.2 La deuxième année

Au début de la deuxième année du cycle TSMSI, un nouvel apprenti a intégré la société et a repris ma place en atelier. Ceci m'a donc permis de changer d'équipe et de pouvoir ainsi m'occuper des réseaux informatiques, comme cela était prévu.

Cette seconde "étape" était beaucoup plus axée sur mon autonomie au quotidien et surtout lors de déplacements professionnels. J'étais bien moins suivi par les employés de la société mais ils restaient tout de même à ma disposition en cas de problème. Cette fois-ci, les tâches que je devais exécuter étaient pratiquement toutes liées à l'informatique mais surtout elles étaient souvent plus complexes et plus longues à résoudre. Mon travail et mon emploi du temps étaient donc, à partir de ce moment là, similaires à ceux de mes collègues. J'ai alors pu travailler de façon autonome sur de nombreuses interventions avec la confiance et la sûreté que j'avais acquise l'année précédente.

Mon rôle était alors pleinement celui d'un des employés de la société et mon autonomie fut bien souvent complète. Malheureusement du fait de mon alternance, je n'ai pas pu toujours suivre les interventions du début à la fin.

Chapitre 2

Synthèse du cycle TSMSI 2004-2006

2.1 L'alternance en entreprise

Je débuterai, bien sûr, la synthèse de ces deux dernières années par ce que j'ai vécu en alternance dans mon entreprise tutrice. Cette synthèse de mon alternance en entreprise s'articule autour de trois axes de mon évolution : mon intégration, mon apprentissage et pour finir mon autonomie.

2.1.1 Mon intégration

À mon arrivée à NBM-Europe, je mettais pour la première fois les pieds dans le monde de l'entreprise car je sortais tout juste de ma Terminale Générale Scientifique. Les changements furent nombreux et déroutants. Par exemple, le premier jour à l'heure du déjeuner, je ne savais pas si je pouvais partir ou si je devais demander l'autorisation de mon tuteur. Mais ensuite, passé ces petits embarras d'organisation et de mise en situation, je n'eus pas trop de mal à m'intégrer à l'équipe de la société.

Bien sûr à mon arrivée, je n'ai pas eu de tâches ou de missions très techniques. Si cela devait arriver, un des employés vérifiait mon travail et me conseillait.

Le fonctionnement de l'entreprise

J'ai donc commencé par réceptionner les colis, vérifier leur état et leur contenu avant d'étiqueter les produits qui étaient à l'intérieur.

Bien que ces tâches fussent répétitives et sans intérêt technique, elles furent instructives. En effet, le fait de préparer des commandes ou d'étiqueter des produits m'a permis d'apprendre à utiliser l'outil de gestion commercial de la société et parallèlement le fonctionnement de l'entreprise. Cela m'a permis de trouver mes repères pour travailler efficacement et de me sentir à l'aise dans l'accomplissement de mes tâches.

Le contact avec la clientèle

Il a fallu que je réponde aux appels téléphoniques pour procéder à un service technique de premier niveau. Si le problème était trop complexe pour moi ou bien que l'appelant désirait un employé en particulier, je pouvais le diriger vers la personne appropriée.

Ce support m'a beaucoup aidé car à ce moment là, j'avais du mal à m'exprimer et répondre au téléphone était quelque chose de problématique.

Réparation de poste informatique

D'autre part, j'ai travaillé sur des problèmes de base en informatique. Par exemple, les tâches les plus fréquentes étaient :

- La configuration d'une connexion internet sur un poste sous Microsoft Windows XP.
- La réinstallation et reconfiguration complète de poste informatique sous Microsoft Windows en utilisant le formatage* puis en procédant à une réinstallation (du système d'exploitation, des mises à jours, des pilotes*).
- Le changement de diverses pièces défectueuses internes à une unité centrale comme la carte-mère ou le disque dur.

Ces dépannages furent relativement simples à réaliser pour moi et je pus les exécuter sans difficultés avec mes connaissances personnelles.

Apple iMac G5 démonté

Réparation d'imprimante

J'ai, en plus, travaillé sur des pannes d'imprimante jet d'encre ou laser. Les dysfonctionnements sur ce type d'appareil étaient systématiquement matériels et non logiciels. Il était fréquent de voir des imprimantes lasers qui ne prenaient plus le papier et dont il fallait changer le kit de maintenance[1]. Par contre, les imprimantes jet d'encre avaient plus de problème avec leurs têtes d'impression qui étaient bouchées et empêchaient d'obtenir une impression de bonne qualité.

FIG. 2.1 – Une imprimante laser HP

Tout comme pour les dépannages de postes, ces interventions furent assez faciles à effectuer car logiques et mécaniques. Je n'eus pas de difficultés particulières à les exécuter.

2.1.2 Mon apprentissage

Lorsque mes repères furent complets, j'ai pu travaillé sur des problèmes plus poussés techniquement et commencer pleinement mon apprentissage.

Les pannes matérielles

J'ai souvent eu des réparations matérielles à effectuer pour des ordinateurs, des imprimantes ou des connexions diverses.

Les ordinateurs : Il fallait soit les monter car ils étaient vendus, soit changer des pièces défaillantes ou à améliorer.

[1] pack comprenant toutes les pièces de prise papier en caoutchouc

Les imprimantes : À part lors d'une installation neuve, elles avaient plutôt des problèmes de prises de papier et il était nécessaire de changer certaines pièces. Sinon, il arrivait qu'elles soient mal configurées (surtout pour les imprimantes réseaux).

Les connexions : Les connexions Internet ont posé pas mal de problèmes, surtout de synchronisation*. Dans les autres cas, il fallait les reconfigurer ou élargir le réseau local en ajoutant un accès sans-fil (technologie WiFi[2] ou en câblant davantage (de la téléphonie comme de l'informatique).

Exemple : **Mise en place d'une connexion Internet partagée avec du sans-fil (technologie WiFi)**

> J'ai eu de nombreuses connexions Internet partagées pour particuliers à mettre en place. Pour faire cela, nous avons besoin d'un appareil que l'on appelle un routeur (illustré ci-dessous)
>
> 
>
>
> C'est ce petit appareil qui partage la connexion et que je devais configurer. Pour cela, il faut brancher un ordinateur sur l'appareil et accéder depuis un navigateur Internet à la page de configuration de ce dernier. En Annexe 2, vous trouverez joint l'interface de configuration de l'accès Internet d'un routeur de marque Linksys. Il faut alors compléter les champs marqués en rouge. Ils permettent respectivement : de se faire identifier par le fournisseur d'accès (1), de configurer le réseau local (2) et enfin de permettre l'accès aux services DNS* (3). Ensuite, on doit configurer la connexion sans-fil. Comme illustré à l'Annexe 3, il faut donc créer une connexion en la nommant (a) puis la protéger grâce au chiffrement (b) et enfin indiquer les autorisations d'accès (c).

Ces interventions qui sont globalement d'ordre physiques et non virtuelles ne m'ont pas posé de réels problèmes. En effet, je disposais déjà des compétences nécessaires à leurs résolutions. Cela dit j'ai tout de même du suivre l'évolution des technologies au cours de ces deux années.

Les pannes logicielles

Dans la grande majorité des cas, il s'agissait d'interventions sur des éléments virtuels : les logiciels. Ces derniers sont malheureusement au vu de leur nombre, bien plus complexes à dépanner que du matériel.

- Ce qui revenait le plus souvent était les pannes d'ordinateurs sous Microsoft Windows. Ces pannes étaient très différentes les unes des autres mais globalement les problèmes venaient soit d'une mauvaise configuration, d'un déréglage du système (Cache* à vider, Registre* abimé, Système de fichiers* corrompu, etc...) soit de la présence de virus ou de spywares*. Dans les deux cas, il fallait d'abord vérifier s'il était possible de réparer et si oui dans quel délai. Finalement, si la réparation n'est pas viable, on formate* l'ordinateur et on réinstalle tout en remettant les données.
- J'ai eu également l'occasion de travailler sur des ordinateurs sous MacOS. Ces derniers demandaient le plus souvent une installation, une mise en réseau (adressage, partage d'imprimante et/ou de données...) ou un autre genre de configuration.
- Ensuite viennent les applications plus spécifiques. Celles-ci sont souvent les plus délicates à prendre en main car elles dépendent des habitudes de chacun. Et il arrive que l'on ne la

[2]Le terme "WiFi" est volontairement non utilisé car la commission générale de terminologie et de néologie française ne l'approuve pas.

connaisse pas ce qui peut rapidement être problèmatique.

Exemple : **Formatage* d'un ordinateur pour le réinstaller correctement**[3]

> La tâche la plus courante à effectuer sur un ordinateur logiciellement en panne est de le formater* pour le réinstaller proprement ensuite. Pour cela, nous devons d'abord commencer par sauvegarder les données contenues dans l'ordinateur grâce à des utilitaires de sauvegarde spécifiques. Suite à cela, nous pouvons le vider complètement en formatant* son contenu et commencer une nouvelle installation du système d'exploitation. Une fois le système installé, il faut procéder aux mises à jours au moyen de l'outil Windows Update de Microsoft (voir Annexe 4), puis à l'installation des pilotes* pour le matériel (pour savoir lesquels installer, il faut connaître les composants qui sont dans l'ordinateur). Quand tout cela est fait, il ne reste plus qu'à remettre les données du client contenues dans la sauvegarde effectuée au début de l'opération.

Ces interventions furent des plus instructives techniquement pour plusieurs raisons. Tout d'abord, elles étaient toutes différentes ce qui m'obligeait sans cesse à chercher de nouvelles informations sur le fonctionnement interne d'un outil, pour finalement le connaître sous de nombreux angles différents. Mais ce n'est pas tout, cela fut aussi très intéressant car cela m'a permis de comparer des produits différents, notamment concernant leurs choix technologiques et les conséquences qui en découlent.

Le conseil à la clientèle

Enfin mon travail s'est également porté sur le conseil à la clientèle.
Les besoins des clients étaient très différents les uns des autres.
En général, les particuliers désiraient des informations sur l'acquisition d'un nouveau poste informatique (portable surtout) ou sur des pièces spécifiques (une nouvelle carte d'extension, un périphérique...)
Par contre les professionnels n'avaient pas les mêmes attentes. Ils avaient bien souvent un besoin à satisfaire sur des points plus précis (par exemple créer des fichiers au format PDF facilement ou pouvoir inter-réagir sur les calendriers de leurs collègues...).
Ces contacts s'établissaient soit physiquement (chez le client, au sein de NBM-Europe) ou bien par téléphone.

Ces nombreuses rencontres furent enrichissantes. Tout d'abord, cela m'a permis de m'exprimer plus facilement en prenant confiance en moi. Ensuite, j'ai pu connaître davantage la clientèle et ses désirs. Il arrivait également que le client ne parle pas français, m'obligeant ainsi à m'exprimer en anglais et donc à pratiquer cette langue.

[3] Les procédures détaillées pour réinstaller un système d'exploitation de type Microsoft Windows XP sont décrites sur le site internet : http ://support.microsoft.com/default.aspx ?scid=kb ;FR ;315341

Les déplacement

Parallèlement à cela, je suis également intervenu en clientèle assez régulièrement, même si à la base mes tâches devaient davantage s'effectuer en atelier. Ces déplacements s'effectuaient chez des particuliers comme chez des professionnels.

Les déplacements m'ont apporté bien sûr les contacts avec la clientèle comme je l'ai abordé précédemment, mais aussi plus de transparence avec elle et une meilleure qualité de travail. En effet, il est plutôt conseillé de ne pas faire d'erreur chez le client et il est souvent nécessaire de lui faire vérifier son travail à la fin de son intervention afin de valider celle-ci avec lui.

2.1.3 Mon autonomie

Après que j'ai été suffisamment à l'aise en intervention, il ne me restait plus qu'à renforcer mon autonomie et à améliorer mes compétences.

Les interventions réseaux

La formation que je suivais au CESI de technicien supérieur en maintenance informatique et réseaux étant relativement axée sur l'administration réseaux, il était normal que je renforce cette compétence. J'ai donc travaillé sur de nombreuses missions en rapport avec les réseaux et les serveurs.

Les domaines Microsoft : Sur les domaines Windows, j'avais régulièrement à gérer des utilisateurs (en créer de nouveau, modifier leur mot de passe...), monter des contrôleurs de domaine, surveiller l'état des contrôleurs de domaine déjà en cours de fonctionnement. Il était rare d'avoir des pannes importantes sur ces produits mais il y avait souvent un petit point à modifier et/ou à corriger.

Les groupes de travail : Les groupes de travail ont été relativement présents mais plutôt chez les particuliers ou dans les toutes petites entreprises. En général, j'ai dû résoudre un problème de détection de poste ou bien de partages de ressources défectueux. Les applications métiers (décrites ci-dessous) travaillent souvent sur de simple groupe de travail.

Les applications métiers : Les applications métiers sont des applications spécifiques à un corps de métier. Elles sont donc différentes pour bon nombre de nos clients. Le temps de dépannage est, de ce fait, extrèmement variable (suivant la conception du logiciel, la qualité de la hotline). Mes tâches sur ce genre d'applications furent très diverses.

Les applications serveurs : J'ai dû également monter des serveurs de mails (Exchange[4] par exemple) ou les entretenir et les réparer. Il faut vérifier si l'on n'a pas trop de mail en attente d'envoi ce qui signiferait un problème, par exemple. Autrement, il y avait également des serveurs Web* ou FTP* à créer ou à entretenir. Sinon, il arrivait aussi qu'il y ait des problèmes avec des serveurs DNS*.

Les logiciels Antivirus : Les antivirus sont aujourd'hui obligatoires lorsqu'une connexion Internet est présente et il fallait que j'installe un antivirus comme Symantec AntiVirus sur des parcs informatiques. Cet antivirus me permettait de travailler depuis un seul poste serveur et de répercuter mes modifications sur les autres automatiquement. D'ailleurs, il arrivait qu'il faille dépanner justement cette répercution qui posait quelquefois souci. Dans un autre registre, j'ai géré les filtres AntiSpam sur les serveurs de messagerie de nos clients en vérifiant qu'il n'y ai pas de faux-positifs (du spam reconnu comme des mails légitimes) ou de faux-négatifs (des mails légitimes reconnus comme du spam).

Les logiciels de sauvegarde : La gestion des sauvegarde était en général de mon ressort. Je prenais donc le temps de vérifier que les sauvegarde s'effectuaient correctement chaque jour chez nos clients. Les outils de sauvegarde les plus utilisés étant TapeWare de Yosemite et

[4]Exchange est un produit de Microsoft qui sert de serveur de messagerie

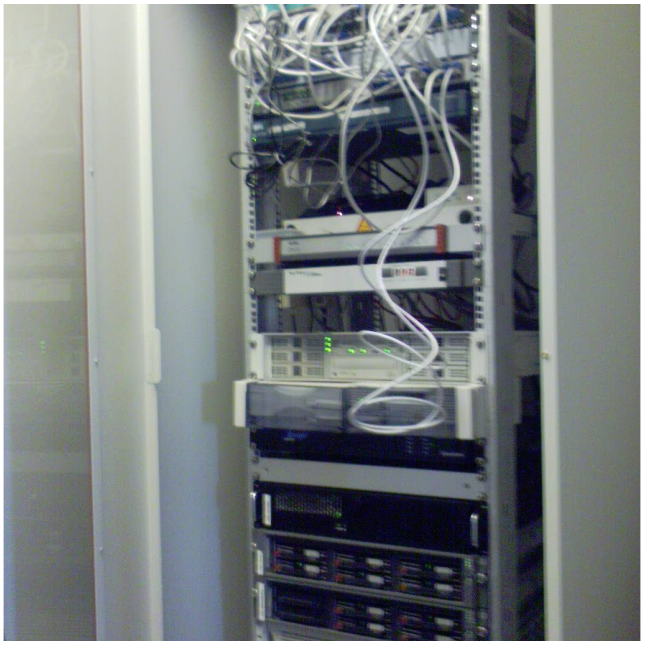
Véritas de Symantec.

J'ai ainsi beaucoup travaillé sur des serveurs de marque HP car ce sont ces produits qui sont vendus à NBM-Europe.

Exemple : **Création d'une boîte aux lettres pour un utilisateur dans un domaine**

> Une tâche d'administration réseau assez fréquente était la mise en service d'un compte mail pour un utilisateur. Pour cela, il est nécessaire de prendre le contrôle d'un des contrôleurs de domaine de l'entreprise concernée (bien souvent il n'y a qu'un serveur de ce type dans les entreprises de type PME). Ensuite, il faut lancer la console d'administration des utilisateurs de l'Active Directory*. Après cela, on sélectionne l'utilisateur qui désire obtenir une boîte de messagerie électronique à l'aide d'un clic droit pour ensuite atteindre "tâches exchange". Un assistant s'ouvre alors pour nous guider à la création de la boîte e-mail. L'opération complète est illustrée en Annexe 5.

Ces interventions furent à mon sens les plus intéressantes car elles correspondent tout à fait à mes objectifs professionnels. Mes compétences personnelles ont été grandement améliorées avec celles-ci.



Une armoire serveur/de brassage* où il fallait que j'intervienne régulièrement chez un des clients.

2.2 Mon travail personnel

Il est très important d'écrire quelques lignes à ce sujet, car l'informatique, nécessite qu'on lui consacre beaucoup de temps en dehors du travail. Ceci pour plusieurs raisons, tout d'abord car l'informatique est un ensemble de technologies en continuelle évolution et l'on doit rester informé des nouveautés, ensuite parce que les cours dispensés par la formation TSMSI ne sont pas assez approfondis pour justifier la maîtrise d'un des outils ou d'une des techniques étudiées. Enfin, il faut également rester ouvert et s'informer sur d'autres outils que ceux étudiés en cours ou vus en entreprise car ils peuvent devenir les standards de demain.

2.2.1 En relation au travail en entreprise

Mes recherches personnelles ont commencé bien sûr avec le travail que je devais effectuer au sein de NBM-Europe. Il fallait, en effet, que j'acquière les compétences suffisantes pour travailler de façon correcte et avec un minimum d'autonomie.

Je connaissais déjà assez bien ce qui était lié aux réparations et aux montages d'ordinateurs mais en ce qui concerne les logiciels, j'avais des lacunes sur les produits utilisés par la société. J'ai donc porté mon attention sur les produits Microsoft avec lesquels l'entreprise travaille. Je connaissais déjà bien sûr une partie de ses produits, notamment les versions postes de travail de Windows (c'est-à-dire Microsoft Windows 95/98, Me, 2000 et XP) mais beaucoup moins les produits serveurs. Je me suis donc réservé une machine personnelle pour installer des systèmes d'exploitation comme Microsoft Windows 2003 Serveur accompagnés du logiciels de sauvegarde Veritas Backup.

Cela m'a permis de prendre en main les produits, de surveiller le comportement de l'ensemble en réglant certains paramètres.

J'ai ensuite mis en place un serveur Exchange 2003 sur un domaine. À partir de là, je me suis fixé des objectifs :
- ajouter le chiffrement SSL*[5] au Webmail (OWA) de Exchange 2003 pour élever la sécurité.
- mettre en place la sauvegarde de l'annuaire Active Directory* et des bases de données de Exchange 2003.
- tester la restauration de ces sauvegardes.
- tester la mise en place d'un domaine avec plusieurs contrôleurs de domaine.

2.2.2 En relation aux cours du CESI

Il m'est arrivé de nombreuses fois de continuer et d'approfondir des sujets étudiés durant les cours du CESI. Généralement, j'approfondissais ceux que je trouvais intéressants ou ceux qui étaient importants pour la suite.

Par exemple, j'ai vraiment beaucoup travaillé sur la création de site Internet en PHP*. Mais je suis allé plus loin dans la complexité du langage PHP* et dans la rigueur de développement (certification de code XHTML/CSS*). Avec cela, j'ai fait des applications Internet interactives (comme un annuaire ou un site sur lequel je suis toujours en train de travailler). Je me suis vraiment attaché à la clareté du code et à respecter les standards établis. C'est pour cette raison que je n'ai pas continué sur d'autres chemins comme ce que l'on appelle le Web 2.0. Ce dernier qui offre bien des possibilités intéressantes reste complètement hors des standards actuels. J'ai également travaillé sur des traductions de sites ou applications en PHP* à l'aide de gettext*.

Les cours sur les produits Microsoft Windows ont également été approfondi comme je l'ai expliqué précédement mais avant tout pour répondre aux besoins de mon employeur.

2.2.3 Mes recherches personnelles

Sinon personnellement, j'ai étudié de nombreux outils mais surtout des outils libres.

Administration réseaux

J'ai monté de nombreux serveurs sous GNU/Linux* qui répondent à des nombreuses tâches (serveur de fichiers, serveur de mail, serveur DNS*, serveur d'impression, serveur VPN, pare-feu...)

J'ai aussi étudié plusieurs protocoles* afin de mettre en place des règles de pare-feu* très strictes et précises (SMB, PPTP, ...).

[5]SSL est un protocole* de sécurisation des échanges, développé par Netscape. Il a été conçu pour assurer la sécurité des transactions sur Internet (notamment entre un client et un serveur), et il est intégré depuis 1994 dans les navigateurs. Il existe plusieurs versions : la version 2.0 développée par Netscape ; la version 3.0 qui est actuellement la plus répandue, et la version 3.1 baptisée TLS (Transport Layer Security) et standardisée par l'IETF.

J'ai travaillé sur une interopérabilité entre un serveur de fichiers GNU/linux* et un domaine Windows 2003, en joignant le serveur GNU/linux* directement dans le domaine.

Ou encore, j'ai testé la mise en place d'un cluster* sous GNU/linux* composé de deux machines. Et je l'ai soumis à différents tests comme des simulations de pannes, afin d'étudier le comportement de l'ensemble.

Je me suis penché aussi sur la VoIP* qui est une solution qu'il faut de plus en plus maîtriser. J'ai donc installé un serveur de VoIP*. Puis j'ai testé avec des téléphones IP, la qualité du son obtenu, la qualité du lien, l'utilisation du réseau...

J'ai également travaillé sur une plateforme équivalente à Exchange mais avec des solutions libres. Il me fallait donc que les mails, le calendrier et les contacts soient disponibles depuis un webmail ou avec un client mail standard, en utilisant différentes technologies Internet (du SSL*, WebDav*, SASLv2* sur TLS*,...). Cela dit mes travaux sur ce projet ne sont pas encore terminés.

Développement

En plus d'avoir travaillé PHP/MySQL/XHTML/CSS*, j'ai étudié brièvement le langage C* que j'ai associé à GTK+* afin de pouvoir mettre au point des applications graphiques portables et multiplateformes. Aucun projet n'a vraiment abouti pour le moment, juste des tests comme un éditeur de texte de base.

Divers

J'ai testé l'installation sur plusieurs ordinateurs d'un système GNU/Linux* en tant que poste de travail.

J'ai collaboré avec des projets libres comme SystemRescueCD[6] ou Samba 3[7] en aidant à la traduction de leurs manuels.

J'ai utilisé le système MacOS et effectué de nombreux travaux dessus mais dans le cadre d'une utilisation poste de travail et non serveur.

J'ai pour finir, profité de ce mémoire, pour apprendre le langage LaTeX. Il s'agit d'un langage de programmation utilisé dans le monde de l'édition pour écrire du texte d'une façon propre et claire simplement.

2.3 Bilan et évolution

Durant ces deux années du cycle TSMSI, je suis rentré dans le monde actif. J'ai donc pris connaissance de l'univers de l'entreprise où j'ai pu grandement m'améliorer.

Tout d'abord, j'ai pu gagner en maturité et en confiance personnelle grâce aux relations que j'ai du établir avec la clientèle.

De plus, mon niveau de compétence technique a été largement élevé grâce aux travaux en entreprise, aux cours mais aussi à mes travaux personnels. Ces compétences touchent de nombreux domaine comme l'administration réseaux, l'administration système, le développement,...

Enfin, j'ai pu acquérir une autonomie de travail. Je peux aujourd'hui travaillé seul sans difficultés alors que ce n'était pas le cas au début du cycle.

[6] SystemRescueCD est un projet libre. Ce projet a pour but de fournir un CD-ROM d'aide au dépannage des ordinateurs. Plus d'informations sur : http ://www.sysresccd.org

[7] Le projet libre Samba vise à permettre l'échange de données entre des ordinateurs sous Windows et les autres. Plus d'informations sur : http ://www.samba.org

Chapitre 3

Projet : Mise en place d'une interconnexion/VPN

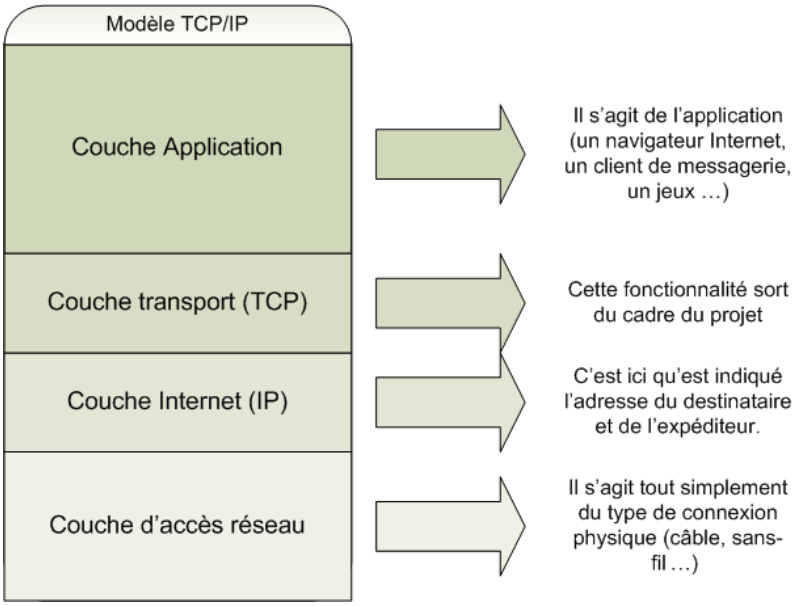
3.1 Introduction et pré-requis

Mon projet de mémoire de fin de cycle TSMSI va traiter de la mise en place d'une interconnexion de type VPN*. J'ai choisi ce sujet car il s'agit à l'heure actuelle d'une technique très utilisée dans les entreprises, qui présente de nombreux avantages et qui a encore beaucoup d'avenir. Le projet sera décrit d'une façon générique et transposable pour n'importe quelle société et non pas adapté à une situation spécifique. Pour présenter ce sujet, j'expliquerai tout d'abord le principe de cette technologie et son fonctionnement, puis je déterminerai les besoins actuels et futurs qui la rendent si utile. Ensuite, je détaillerai les solutions existantes en les comparant les unes aux autres. Et je terminerai par la mise en place de la solution.

Les pré-requis : TCP/IP

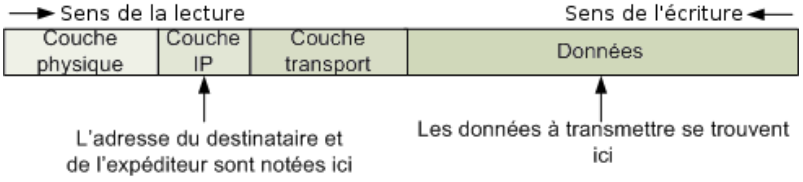
Pour pouvoir suivre les indications techniques décrites dans ce chapitre, il est nécessaire de faire un bref rappel des bases du protocole* TCP/IP[1] . Le sigle TCP/IP signifie "Transmission Control Protocol/Internet Protocol". Il provient des noms des deux protocoles* majeurs TCP et IP. Il s'agit du protocole* de communication actuellement et massivement utilisé sur Internet (bien qu'il en existe de nombreux autres). Ce protocole* permet d'envoyer une information sous forme de "paquet" (qu'il en faille un seul ou plusieurs). Pour cela, l'ordinateur travaille à l'aide du modèle TCP/IP, illustré sur la page suivante.

[1]Ce rappel est très approximatif par rapport à la complexité du protocole* TCP/IP mais il permet de bien comprendre la suite du projet.



Le modèle TCP/IP

Lorsqu'un ordinateur doit envoyer une information, il fragmente tout d'abord les données pour qu'elles aient une certaine taille[2] et puis il rajoute pour chaque segment de données les informations nécessaires à leur acheminement comme l'adresse de destination, l'adresse de l'expéditeur ou le type de donnée (page internet, mail, messagerie instantanée...). Cet ensemble est alors appelé : "paquet" et il suffit maintenant à l'ordinateur de l'envoyer. Ci-dessous l'organisation de base d'un paquet de type TCP/IP :



Un paquet de type TCP/IP

Ensuite lorsqu'un ordinateur reçoit un paquet TCP/IP, il procède à la décomposition de ce dernier pour ne garder que les données. Si les données sont fragmentées, alors il attend l'arrivée de tous les paquets pour reconstituer l'information complète.

3.1.1 Définitions

Une interconnexion VPN*, de l'anglais Virtual Private Network, désigne une solution qui permet de créer un chemin virtuel sécurisé entre une source et une destination. Il s'agit donc de créer un "tunnel" entre deux entités via un réseau public, en général Internet. Les deux extrémités du tunnel sont identifiées et les données qu'elles échangent sont chiffrées[3]. Un réseau privé virtuel repose sur un protocole*, appelé protocole* de tunnellisation, c'est-à-dire un protocole* permettant aux données passant d'une extrémité à l'autre du tunnel d'être sécurisées par des algorithmes de chiffrement. Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie de la connexion les données sont chiffrées et donc incompréhensibles pour toute personne extérieure à celle-ci, comme si les données passaient dans un tunnel.

[2]Cette taille dépend de plusieurs facteurs, notamment du support physique employé : câble, sans-fils...

[3]Il est plus juste de parler de chiffrement que de cryptage en langue française d'après la commission gérérale de terminologie et de néologie

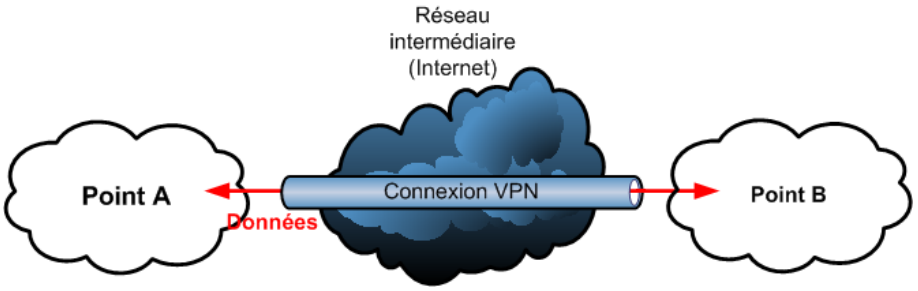
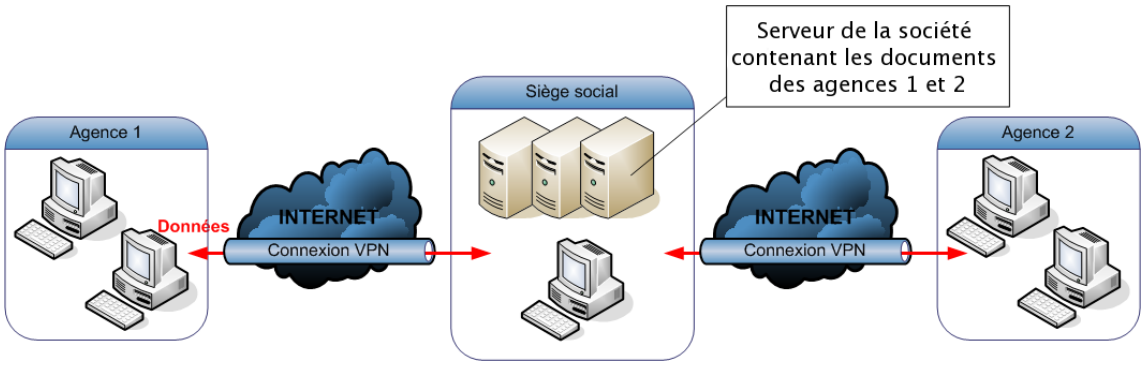


Schéma de fonctionnement d'une connexion VPN*

3.1.2 Les besoins

L'accessibilité des services

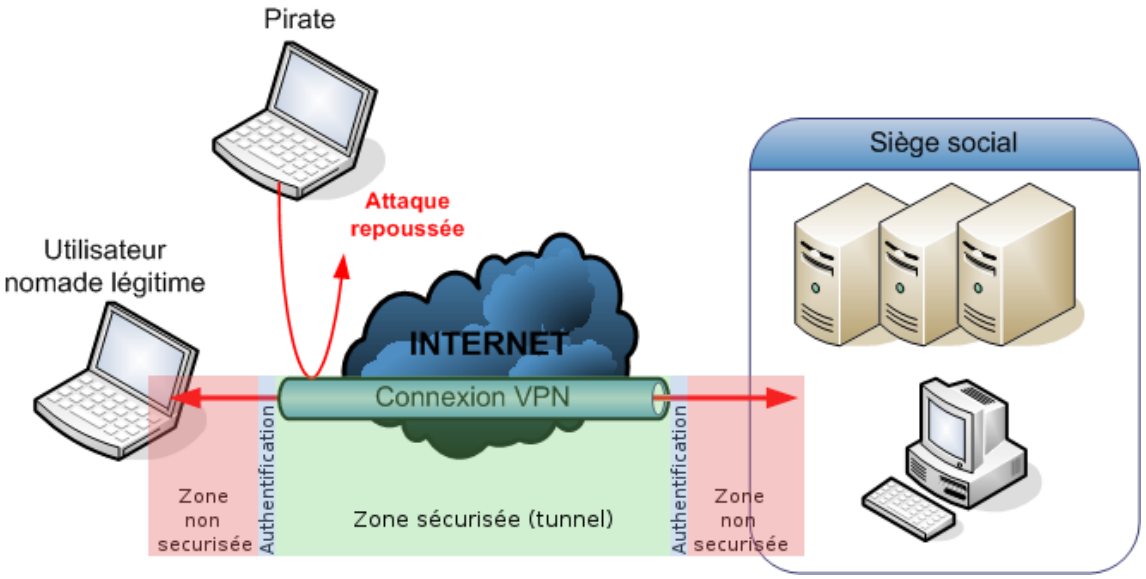
Les entreprises actuelles font appel à la technologie VPN* pour de nombreuses raisons. Tout d'abord avec l'arrivée des réseaux locaux et pour des questions de coût de l'administration et de la maintenabilité*, elles ont regroupé l'ensemble de leurs données sur des entités logiques. C'est-à-dire qu'elles ont centralisé, par exemple, leurs documents sur un seul serveur de fichier afin de faciliter l'entretien de ce dernier ou encore de faciliter sa sauvegarde. La nécessité d'accéder à ces données depuis des endroits géographiques différents et éloignés (suite à la création de nouvelles agences, de nouveaux sites...) est alors apparue. A l'heure actuelle, les services qui doivent rester accessibles sont très divers. On peut citer tout d'abord, l'accès aux documents d'un utilisateur et donc connaître les droit d'accès de cet utilisateur ou encore l'accès à une imprimante ou à un poste informatique. La téléphonie sur IP est également de plus en plus répandue et il ne serait pas étonnant de voir ce service utilisé à travers des connexions VPN*.



Exemple d'une société qui centralise ses informations

La sécurité

Un point très important est également la sécurité. En effet, l'accès facile à tous ces services internes à l'entreprise doit être sécurisé. Cela tout d'abord afin de protéger les données confidentielles de la société et puis d'éviter l'utilisation de service à mauvais escient. Par exemple, la connexion Internet de l'entreprise pourrait être utilisée par un pirate pour lancer des attaques (afin de se rendre anonyme) ou bien un serveur pourrait servir de stockage pour diverses données illicites.



Exemple d'une attaque sur une connexion VPN* en cours d'utilisation

Les protocoles* de tunnellisation doivent répondre à cette demande et utiliser deux types de protections (comme illustré sur le schéma ci-dessus). La première est que chaque entité de bout de tunnel doit être authentifiée pour éviter les usurpations d'identités. Et la deuxième est que tout ce qui transite dans le tunnel doit être chiffré afin d'éviter que des personnes étrangères puissent lire les données.

La facilité d'accès

Un autre besoin qui touche avant tout les utilisateurs nomades avec un portable comme des commerciaux et les télé-travailleurs qui désirent se connecter au réseau de l'entreprise pour travailler, est la facilité d'accès. En effet, il est important que l'utilisation de cette connexion reste simple et transparente pour les utilisateurs. Par contre pour créer un lien permanent entre deux sites d'une entreprise ce besoin n'existe pas.

Le coût

Il faut noter qu'il existe des connexions physiques que l'on peut louer auprès de l'opérateur historique. Ces connexions permettent alors de relier des sites géographiquement éloignés de façon sûre et fiable. Malheureusement, cette solution reste malgré tout onéreuse. Et l'augmentation rapide des débits de l'ADSL* pour un coût relativement faible la rend d'autant moins intéressante.

3.2 Les solutions existantes

Il existe à l'heure actuelle de nombreux protocoles* de tunnellisation sur le marché. Je ne vous présenterai que les protocoles* les plus utilisés et les plus aboutis car il n'est pas possible de les citer tous. J'ai donc sélectionné les protocoles* de tunnellisation suivants :

PPTP (Point-to-Point Tunneling Protocol) est un protocole* développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics. Il est actuellement beaucoup utilisé car très simple à mettre en oeuvre.

L2F (Layer Two Forwarding) est un protocole* développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète (je ne l'aborderai donc pas plus loin).

L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF [4] pour faire converger les fonctionnalités de PPTP et L2F.

IPSec est un protocole* issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux TCP/IP.

OpenVPN est un protocole* de tunnellisation basé sur SSL* (Secure Socket Layer).

Il est à noter que pour une question de simplicité, je n'expliquerai pas tous ces protocoles* dans les détails de leur fonctionnement. Le mode d'établissement de leur connexion et les connexions de contrôles seront ignorées et certains points resteront approximatifs.
L'importance des éléments indiqués dans les pages qui suivent, est de montrer les avantages et les inconvénients de tel ou tel protocole* de tunnellisation. Pour toutes informations pointues et précises, les RFC* de l'IETF sont disponibles sur leur site internet [5].

3.2.1 PPTP/L2TP

Informations sur le protocole*

Le protocole* de tunnellisation PPTP, pour Point-to-Point Tunneling Protocol, est un protocole* qui utilise un réseau TCP/IP pour créer un réseau privé virtuel (VPN*). Microsoft lui a implémenté ses propres algorithmes de chiffrement et de compression et l'a intégré dans ses versions de Windows. Ainsi, le protocole* PPTP est une solution très employée dans les produits commerciaux à cause de son intégration au sein des systèmes d'exploitation Microsoft.

En ce qui concerne la sécurité, il est capable de chiffrer les données ainsi que de les compresser à la volée* afin de gagner en débit. L'authentification se fait grâce au protocole* MS-CHAP v2[7] ou PAP[7] de Microsoft. Le chiffrement des données s'effectue grâce au protocole* MPPE[7] (Microsoft Point-to-Point Encryption). Et enfin, la partie compression peut être réalisée par MPPC[7] (Microsoft Point-to-Point Compression).

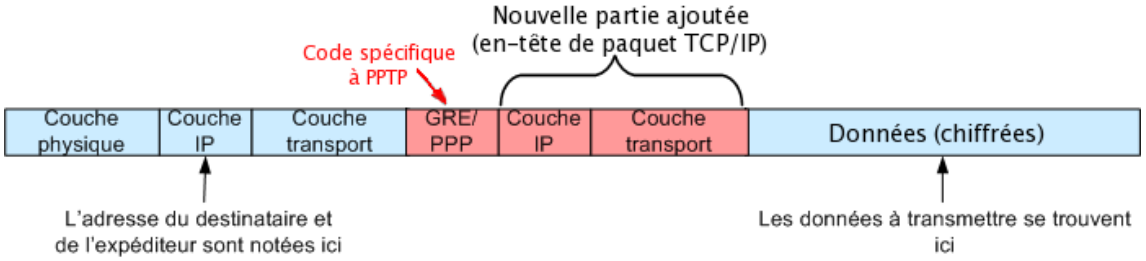
Le principe du protocole* PPTP est de créer des paquets TCP/IP et de les encapsuler dans d'autres paquets TCP/IP. Ce protocole* utilise pour cela une méthode d'encapsulation proposée par le protocole* GRE[6]. Un tunnel PPTP se caractérise toujours par trois points :
- Le tunnel est créé à la demande d'une initialisation de la part d'un client.
- Il existe une connexion de contrôle entre le client et le serveur (hors du tunnel).
- La clôture du tunnel s'effectue par le serveur.

Quand un tunnel PPTP est en service, tout le trafic à destination d'Internet emprunte la connexion physique normale alors que le trafic conçu pour le réseau privé distant, passe par la connexion virtuelle de PPTP.

[4] IETF : Internet Engineering Task Force. Il s'agit d'un groupe informel, international, ouvert à tout individu, qui participe à l'élaboration de standards pour Internet. L'IETF produit la plupart des nouveaux standards d'Internet.
[5] Rendez-vous sur l'adresse Internet : http ://www.ietf.org/rfc.html
[6] Generic Routing Encapsulation : protocole* permettant d'encapsuler un paquet de type TCP/IP dans un autre.
[7] Le nom des protocoles* employés par PPTP sont donnés à titre indicatif. Leur étude n'est nullement nécessaire à la compréhension du protocole* PPTP.

Concrètement

Lorsqu'une connexion PPTP est établie entre un poste informatique et un autre, ils conversent à l'aide de paquets TCP/IP formés par le protocole* PPTP qui ressemble à celui figurant juste ci-dessous :



Un paquet TCP/IP généré par le protocole* PPTP

Le paquet TCP/IP après son passage à un des bouts du tunnel

On peut constater qu'à l'intérieur d'un paquet TCP/IP normal, le protocole* PPTP a rajouté les informations d'un deuxième paquet TCP/IP (c'est à dire un nouvel en-tête d'information comprenant l'adresse de destination, l'adresse de l'expéditeur...) et a également chiffré et éventuellement compressé les données contenues. Une fois réceptionné par son destinataire, le protocole* PPTP fera le travail inverse en enlevant la première partie du paquet (comme sur l'image précédente) et déchiffrera la partie contenant les données afin de retrouver le paquet originel. Maintenant, ou l'ordinateur est le destinataire du paquet et donc le lit, ou il le diffuse sur le réseau local auquel il appartient afin d'envoyer ce paquet vers son destinataire. Lorsque ce dernier répondra, le poste qui a diffusé le paquet se fera passer pour l'expéditeur du paquet précédent pour le renvoyer à son véritable expéditeur. Cela est expliqué de manière visuelle sur le schéma qui suit :

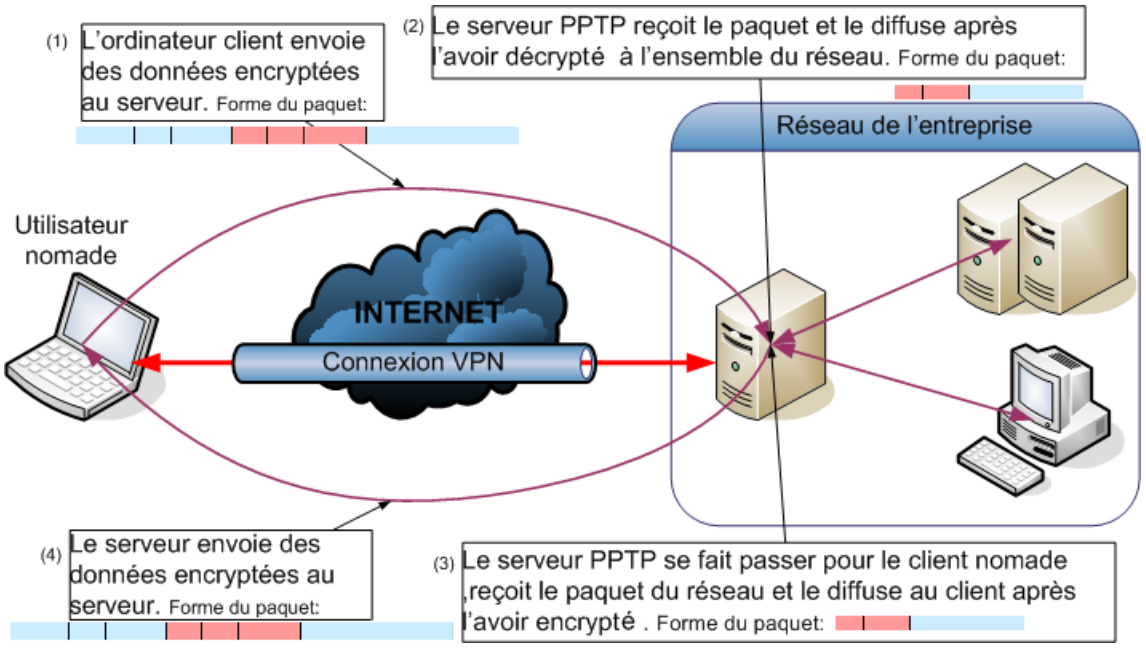


Schéma résumant le fonctionnement du protocole* PPTP

3.2.2 L2TP

Informations sur le protocole*

Le protocole* de tunnellisation L2TP, pour Layer Two Tunneling Protocol, est un protocole* qui comme PPTP peut utiliser un réseau TCP/IP pour créer un réseau privé virtuel (VPN*).

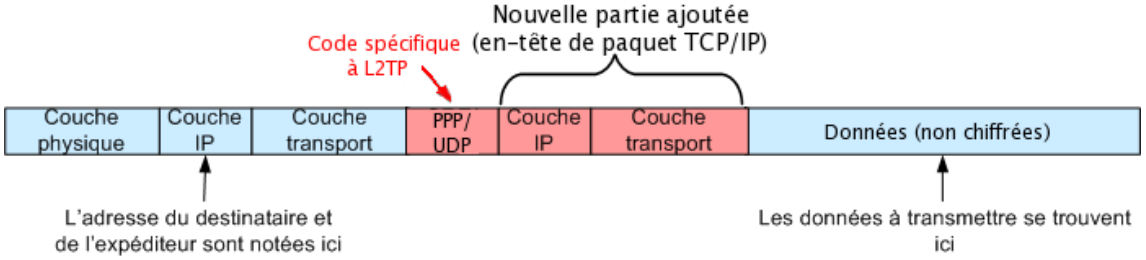
Il peut aussi fonctionner sur d'autres type de réseaux contrairement à PPTP. Actuellement, le protocole* L2TP s'implante sur le marché mais n'est pas encore natif* à l'ensemble des parcs informatiques. Le protocole* L2TP est né de la fusion des deux autres protocoles* PPTP et L2F. Il est actuellement développé et évalué conjointement par Cisco Systems, Microsoft, Ascend, 3Com ainsi que d'autres acteurs-clés du marché des réseaux.

En ce qui concerne la sécurité, L2TP n'intègre pas directement de protocole* pour le chiffrement des données. C'est pourquoi l'IETF préconise l'utilisation conjointe d'un autre protocole* avec L2TP. On peut toutefois se servir entre autres du protocole* ESP d'IPSec[7] pour chiffrer les échanges. De même, L2TP n'intègre pas de protocole* pour une éventuelle compression des données. Néammois, il gère tout de même l'authentification des deux bouts du tunnel.

Le principe du protocole* L2TP est le même que celui du PPTP dont il est issu, à savoir d'encapsuler un premier paquet TCP/IP dans un autre paquet TCP/IP (ou un autre type de paquet suivant le réseau support). Ce protocole* crée ainsi un tunnel en se servant du protocole* PPP (Pont-to-Point Protocol) et non plus du protocole* GRE comme le fait PPTP.

Concrètement

Le fonctionnement du protocole* L2TP est très proche du protocole* PPTP. Lorsqu'une connexion L2TP de base est établie entre un poste informatique et un autre, ils conversent à l'aide de paquets TCP/IP formés par le protocole* L2TP qui ressemble à celui figurant juste ci-dessous :



Un paquet TCP/IP généré par le protocole* L2TP

Le paquet TCP/IP après son passage à un des bouts du tunnel

On constate comme avec le protocole* PPTP qu'un paquet TCP/IP a été inséré dans un autre. Ensuite le fonctionnement reste exactement le même qu'avec le protocole* PPTP sauf qu'avec L2TP tout seul, nous ne profitons ni du chiffrement, ni de la compression. Cela peut être ajouté avec des modules séparés, ce qui nous permet de choisir ce que nous voulons utiliser.

3.2.3 IPSec

Informations sur le protocole*

IPSec est un protocole* qui vise à sécuriser l'échange de données au niveau de la couche d'accès réseau donc au début de tous les paquets TCP/IP (comme nous l'avons vu en introduction). IPSec, pour Ip Security Protocols, est basé sur deux mécanismes de sécurisation :

AH (pour Authentification Header) vise à assurer l'intégrité et l'authenticité des paquets IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par ce mécanisme ne sont pas chiffrées.

ESP (pour Encapsulating Security Payload) peut aussi permettre l'authentification des données mais est principalement utilisé pour le chiffrement des informations.

Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement. Enfin, le protocole* IKE permet de gérer les échanges ou les associations entre les protocoles* de sécurité

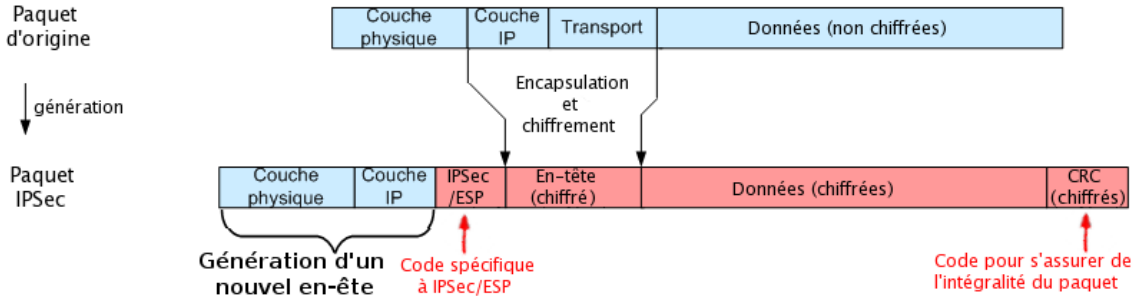
[7] Voir point suivant concernant IPSec (Chapitre 3, Section 2, Sous-section 3)

(afin qu'ils se mettent d'accord sur les algorithmes de chiffrement, d'authentification...). IPSec est le protocole* de tunnellisation le plus complexe et le plus sûr actuellement disponible sur le marché. Mais comme bien d'autres protocoles* (L2TP, OpenVPN (SSL*)...), il souffre d'un manque de diffusion sur le marché.

IPSec travaille nettement plus en profondeur dans le modèle TCP/IP que les autres protocoles* que nous avons rencontrés. Ce qui fait que toutes les données qui rentrent ou sortent de l'ordinateur sont analysées par le protocole* IPSec et sont redirigées vers la bonne connexion même si elles n'ont aucun lien avec le tunnel établi.
Pour le projet, nous nous tournerons plutôt sur le mécanisme ESP de IPSec pour pouvoir à la fois authentifier les connexions VPN* et les chiffrer obtenant ainsi un maximum de sécurité.

Concrètement

Comme il a été dit précédemment, en fonctionnement, le protocole* IPSec détecte lui-même quels sont les paquets qui doivent ou non passer par le tunnel VPN*. S'il rencontre un de ces paquets, il lui fait alors subir quelques modifications (expliquées par le schéma ci-dessous).



Génération d'un paquet IP par IPSec/ESP en mode tunnel

En fait, avec IPSec, tout l'en-tête du paquet originel (les informations de la couche IP et de la couche transport) est chiffré ainsi que les données transportées. Un CRC* est également ajouté pour s'assurer de l'intégrité de l'information. Ensuite un nouvel en-tête est construit pour le paquet et il s'agit de la seule partie de ce dernier qui n'est pas chiffrée. Ensuite le principe reste le même qu'avec PPTP ou L2TP quand le paquet TCP/IP arrive à sa destination, il est décomposé et éventuellement diffusé.

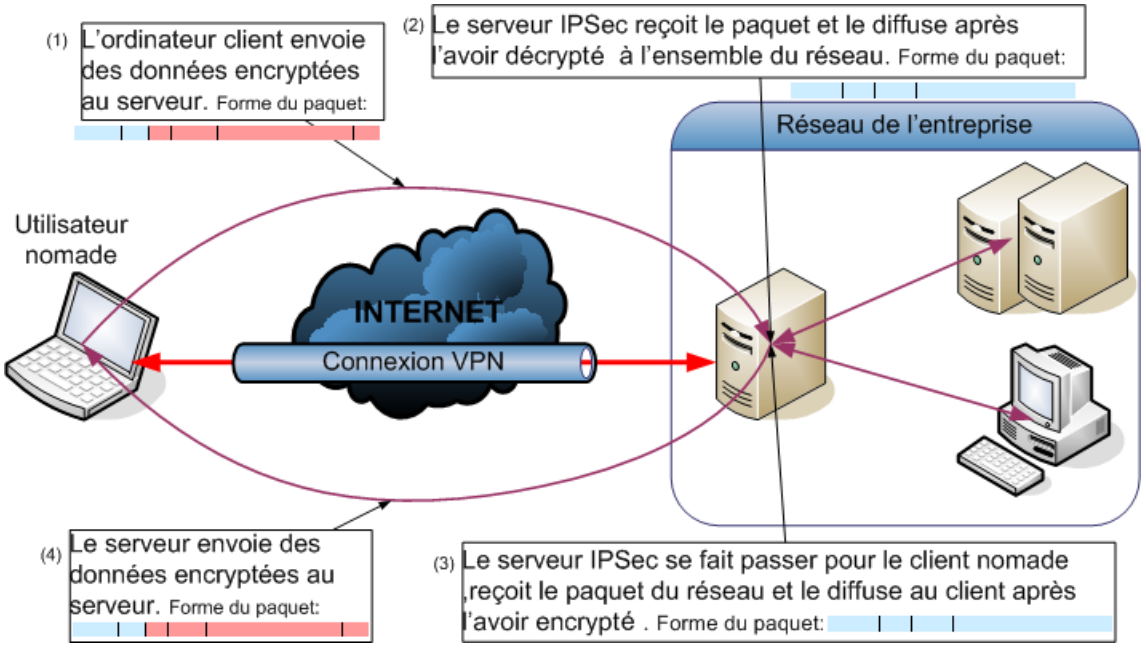


Schéma résumant le fonctionnement d'une connexion IPSec/ESP en mode tunnel

3.2.4 OpenVPN

Informations sur le protocole*

OpenVPN est une autre solution pour mettre en place une connexion VPN* sur un réseau TCP/IP. Ce dernier n'est pas aussi lié au modèle TCP/IP que les autres protocoles* étudiés précédemment. En effet, OpenVPN se base sur le protocole* SSL*/TLS*, il travaille donc sur la couche application du modèle TCP/IP vu au début du chapitre. L'une des particularités de ce protocole* est qu'il est libre, ce qui veut dire qu'au besoin on peut le modifier ou ajouter des fonctionnalités supplémentaires.

Pour sécuriser les échanges de données, OpenVPN utilise donc le protocole* SSL*/TLS* (Secure Socket Layer/Transport Layer Security) largement utilisé par les sites Internet (comme les sites marchands). OpenVPN gère également la compression des données à la volée* avec l'algorithme IZO (utilisé d'ailleurs par la NASA avec la sonde Pathfinder sur Mars). L'authentification des deux bouts du tunnel peut, elle, s'effectuer selon deux modes :

Un secret partagé (type PSK) : Cette méthode est la plus simple mais pour la mettre en pratique, il faut que toutes les machines qui devront utiliser le VPN* aient connaissance d'un mot de passe commun. La confiance que l'on peut accordé à cette authentification baisse alors rapidement avec le nombre de machines.

Des certificats (type X509) : La deuxième méthode est plus complexe mais elle est largement plus fiable. Il faut pour l'utiliser que chaque machine ait une clé publique et une clé privée. Le principe simple est illustré avec le schéma suivant :

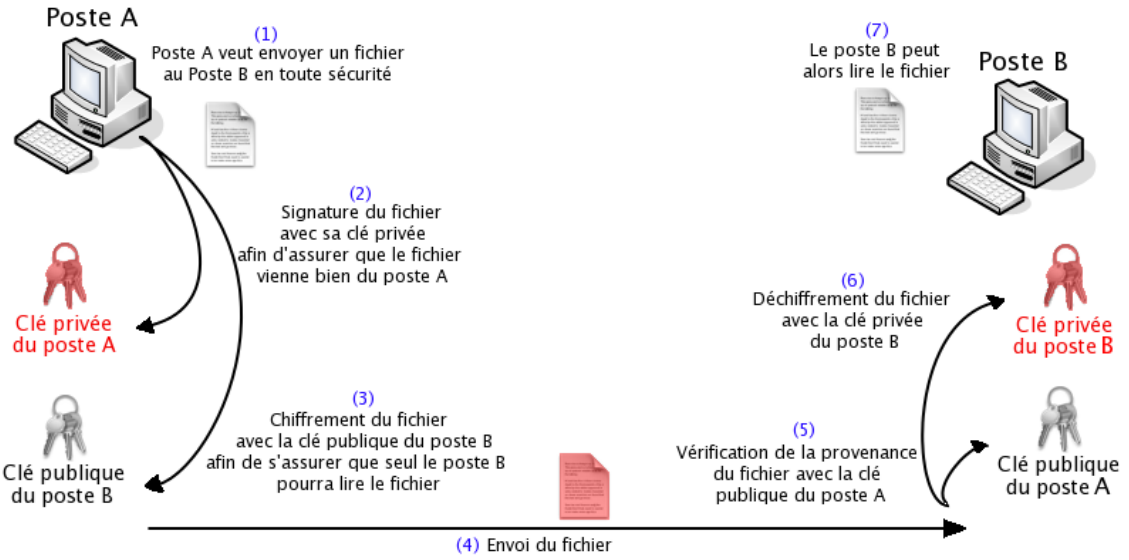
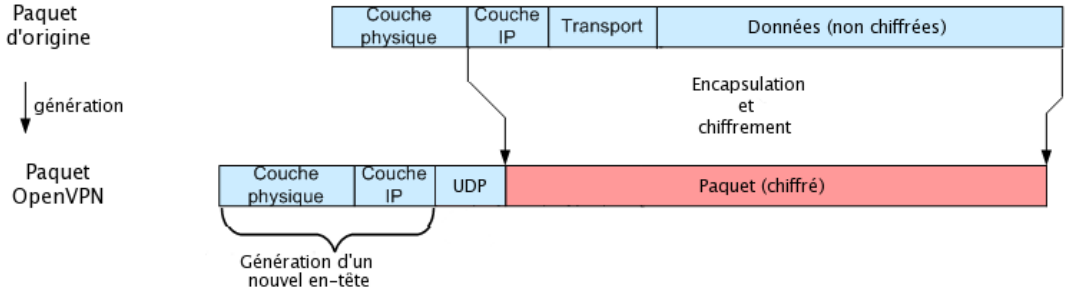


Schéma explicatif d'un système d'authentification à clé privée/clé publique de type X509

Concrètement

Le mode de fonctionnement de OpenVPN reste bien sûr similaire à celui des autres protocoles* au niveau du modèle TCP/IP. Cependant, il peut travailler sur un mode connecté (TCP) ou non connecté (UDP)[8]. Même s'il est souvent conseillé d'utiliser du TCP, il vaut mieux travailler en UDP. En effet, lorsqu'un tunnel de type "TCP over TCP" est utilisé, il existe alors une double gestion dynamique du délai : une à l'extérieur du tunnel et l'autre à l'intérieur. C'est-à-dire que si la connexion physique perd en qualité et que l'on ne reçoit pas d'accusé de réception, le paquet sera réémis et cela sur un délai de plus en plus long et la connexion dans le tunnel, qui est aussi en mode connecté, doit faire face aux mêmes difficultés ce qui entraînera très facilement la rupture du tunnel.

[8]En mode connecté (TCP) à chaque paquet envoyé, il y a un accusé de réception d'émis contrairement au mode non connecté (UDP).



Un paquet IP généré par OpenVPN

Comme l'explique le schéma précédent, OpenVPN prend simplement le paquet TCP/IP original complet, le chiffre et éventuellement le compresse directement dans un nouveau paquet. A cela s'ajoute la sécurité d'authentification qui n'est pas représentée sur le schéma mais qui est contenue dans la partie chiffrée.

3.2.5 Autres

Il existe de nombreuses autres solutions pour exploiter la technologie VPN*. Nous retrouverons des solutions propriétaires qui sont aujourd'hui obsolètes car trop lentes ou trop peu sécurisées. Ces solutions propriétaires peuvent aussi être très au point, mais ne respectant aucun standard, elles contraignent l'acheteur à ne pas utiliser d'autres alternatives ultérieurement, ce qui n'est pas intéressant sur le long terme pour la pérennité de l'investissement. Il existe aussi un bon nombre de solutions libres qui respectent en général correctement les standards mais qui sont obsolètes aujourd'hui. Elles peuvent également être au goût du jour mais pas assez utilisées en production pour garantir une certaine stabilité de fonctionnement.

3.3 Les solutions les plus adaptées

Nous venons d'étudier un certain nombre de solutions possibles pour la mise en place d'une interconnexion VPN*. Il faut maintenant sélectionner la solution la plus adaptée aux besoins définis au début du chapitre. Il y a donc deux besoins distincts : un pour les utilisateurs et un pour les réseaux.

Tout d'abord pour les utilisateurs (appelés souvent utilisateurs Road Warrior), il leur faut une solution simple et utilisable rapidement partout avec n'importe quelle connexion Internet. Le protocole* PPTP répond parfaitement à ces attentes. En effet, il est intégré d'origine au système d'exploitation MS Windows, Apple MacOS X et à la plupart des distributions GNU/Linux*. Une connexion PPTP est alors très simple à mettre en place. Par contre avec IPSec, L2TP et OpenVPN, il faut obligatoirement installer une couche application supplémentaire et la configuration des connexions peut être déroutante et laborieuse. IPSec peut poser des soucis d'établissement du tunnel sur des connexions Internet partagées (le passage dans la translation d'adresse, NAT*, peut ne pas s'effectuer correctement car IPSec rajoute des informations sur l'intégrité des paquets qui empêchent ces derniers d'être modifiés). L2TP n'a pas ce problème mais la modularité de sa mise en place et le fait qu'il ne soit pas intégré aux systèmes d'exploitation actuels le rend difficile à installer et à déployer sur de grands parcs informatiques. Enfin pour OpenVPN le problème reste le même que pour IPSec et L2TP, il est difficile de l'installer et de le déployer rapidement. Le seul problème de PPTP est son faible niveau de sécurité car même s'il intègre un système d'authentification et de chiffrement, ces derniers connaissent de nombreuses failles de sécurité[9].

Pour interconnecter deux réseaux entre eux de façon permanente, les besoins ne sont pas les mêmes. La solution PPTP n'est alors pas du tout intéressante du fait de ces nombreuses failles de sécurité. Pour interconnecter deux réseaux ensembles, la solution la plus adaptée est le protocole* IPSec qui offre l'une des meilleures protections. Sa mise en place peut être grandement facilitée car bon nombre de routeurs Internet professionnels gère ce protocole*. Pour le protocole* L2TP, il doit également exister des modèles de routeurs qui l'intègrent mais L2TP reste moins fiable et moins sécurisé que IPSec. Enfin, OpenVPN nécessiterait l'installation d'une machine serveur sur chaque site.

Protocole*	Natif*	Sécurité	Compression	Utilisation	Autres
PPTP	Oui	Authentification et Chiffrement	Oui	Simple	Failles de sécurité
L2TP	Non	Authentification	Non	Difficile	Modulaire
IPSec	Non	Authentification et Chiffrement	Non	Difficile	Problème avec le NAT*
OpenVPN	Non	Authentification et Chiffrement	Oui	Moyenne	Libre Modulaire

Tableau récapitulatif des solutions

3.4 Coût d'installation et de maintenance

Après avoir sélectionné les solutions les plus adaptées pour les deux besoins qui ressortaient de l'étude, il est important de vérifier et de chiffrer le coût de ces deux solutions. Il est, en effet, inutile de mettre en place une interconnexion VPN* entre deux réseaux géographiquement éloignés si le coût est plus élevé que la location d'une ligne spécialisée ou tout simplement si la maintenance de ce lien est trop onéreuse.

Les utilisateurs : PPTP

Le protocole* PPTP est le protocole* le plus implanté dans les différents systèmes d'exploitation. Il n'y a donc pas de coût à prévoir pour l'acquisition d'éventuelles licences. De plus la création et la configuration d'un tunnel sur un poste client est très facile à réaliser ce qui peut donc être effectué en cinq minutes par des utilisateurs de base (la configuration d'un client PPTP sur

[9]Des concepteurs de produits utilisant PPTP expliquent les soucis de sécurité de ce protocole* sur le site Internet : http ://pptop.sourceforge.net/dox/protocol-security.phtml

un poste Microsoft Windows XP va être décrit dans les pages suivantes[10]). Il est tout de même nécessaire de disposer d'un serveur pour accueillir les connexions. Si l'on possède déjà un serveur sous Microsoft Windows Serveur, il suffit de le configurer pour ajouter cette fonctionnalité. Sinon inutile d'acquérir une licence Microsoft Windows Serveur supplémentaire, il est possible de mettre en place un serveur PPTP sous un système GNU/Linux* libre et gratuit. Cependant, vu les failles de sécurité, il faut néanmoins prendre le temps de vérifier régulièrement les accès qui ont été établis.

Conclusion : Le coût de déploiement est quasiment nul et la mise en place d'un serveur ne nécessite, dans les pires des cas, que l'acquisition d'un nouveau poste serveur pour environ un millier d'euros (le double si l'on veut en plus mettre un système de redondance*).

Les interconnexions réseaux : IPSec

Le protocole* IPSec est le protocole* le plus sécurisé avec OpenVPN présenté dans ce chapitre. Pour des interconnexions réseaux, sa mise en place est assez simple et nécessite l'acquisition de routeurs capables de gérer ce protocole*. Le nombre de liens IPSec à envisager fait que l'on se tournera vers un modèle plus ou moins puissant. Mais une fois le tunnel en place et fonctionnel, il n'y pas de maintenance particulière à envisager sauf en cas de panne ce qui reste relativement rare sur ce genre de matériel. Il est à noter qu'il vaut mieux se tourner vers des équipements du même constructeur pour éviter des problèmes de compatibilité.

Conclusion : La mise en place d'interconnexions réseaux VPN* avec IPSec nécessite l'acquisition d'équipements spécifiques dont le coût se situe dans la fourchette de trois cents à mille euros par site à interconnecter (suivant le nombre de connexions nécessaires). Ensuite le coût de maintenance est quasiment nul.

Les deux autres : OpenVPN et L2TP

Ces deux solutions bien que matures et efficaces ont malheureusement un coût de déploiement trop élevé. En effet, pour L2TP, il faudra sur certaines plateformes acheter les licences nécessaires. De plus, il faudra ensuite procéder à l'installation et à la configuration de tous les postes concernés. Une formation interne des utilisateurs ne serait pas non plus superflue pour éviter des temps importants en maintenance.

Conclusion : La solution de OpenVPN peut être intéressante pour les utilisateurs si la sécurité est un point crucial et que le coût de maintenance et de mise en place passe au second plan.

Protocole*	Coût de mise en place	Coût de maintenance
PPTP	nul	faible
L2TP	élevé	moyen
IPSec	moyen	faible/nul
OpenVPN	élevé	moyen

Tableau récapitulatif du coût des différentes solutions

3.5 Installation

3.5.1 Mise en place du PPTP (serveur)

Pour la mise en place du serveur PPTP, j'ai choisi de présenter les deux alternatives possibles que j'avais mentionnées c'est-à-dire l'installation du service PPTP sous Microsoft Windows Serveur et sous GNU/Linux*. Je commencerai par détailler la mise en place du serveur sous Microsoft Windows puis sous GNU/Linux* (distribution Debian). Dans les deux cas, il est nécessaire de laisser rentrer le flux PPTP[11] et de le rediriger vers la machine serveur au niveau de la passerelle.

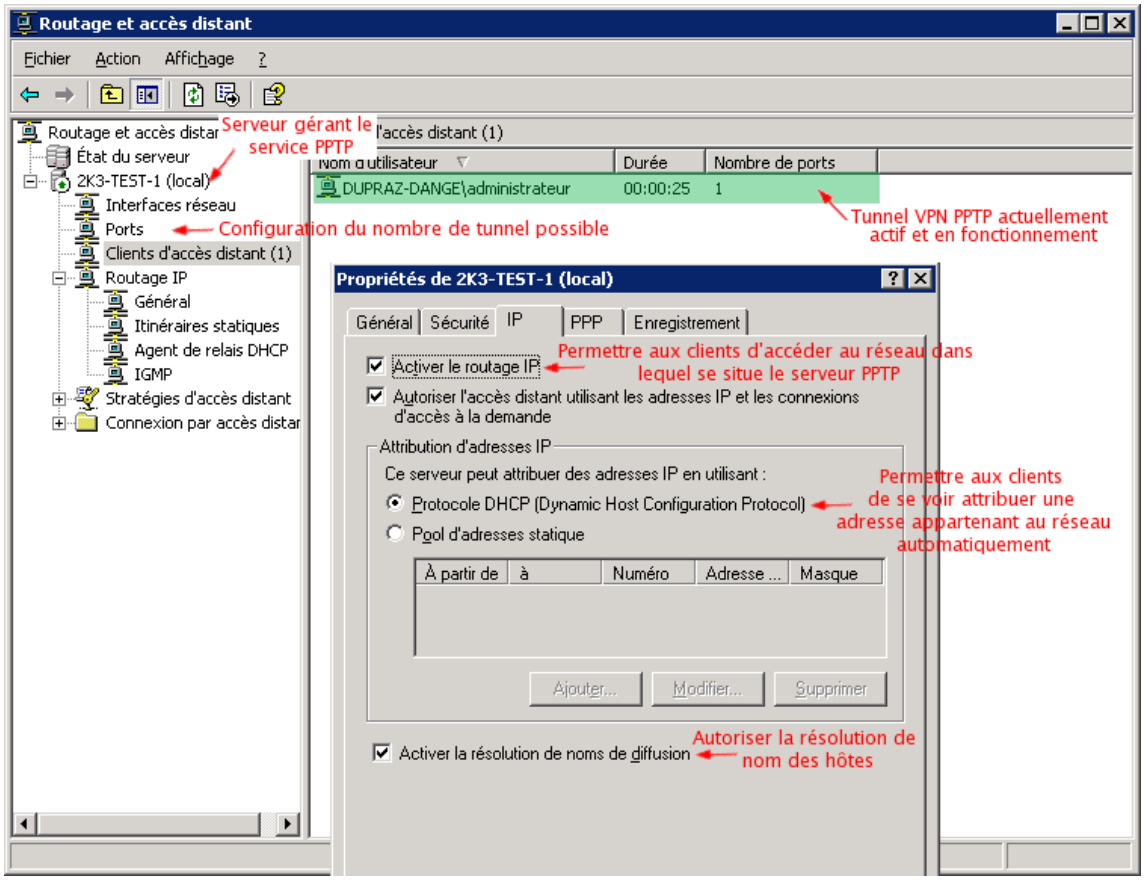
[10] Chapitre 3, section 5, sous-section 2

[11] PPTP nécessite deux éléments : le port 1723 en TCP et puis le protocole* GRE

Mise en place d'un serveur PPTP sous environnement Microsoft Windows Serveur 2003

Note : Les étapes détaillées et illustrées pour l'installation et la configuration du serveur PPTP sur un serveur Microsoft Windows Serveur 2003 préexistant sont décrites en Annexe 6 à la fin de ce document.

Lorsque le service PPTP est installé correctement, nous pouvons l'administrer avec la console d'administration "Routage et accès distant" préconfigurée de Microsoft.



Console d'administration : Routage IP

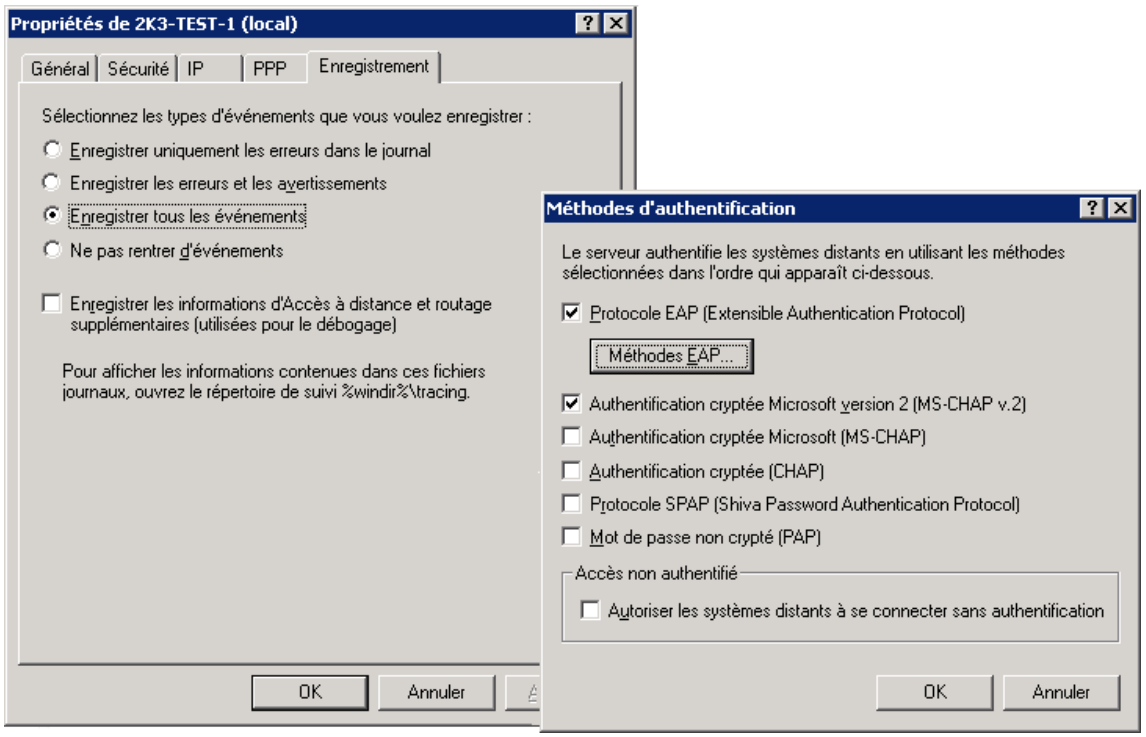
Sur cette première illustration, on peut voir qu'un tunnel PPTP est actuellement en cours de fonctionnement avec l'utilisateur Administrateur (surligné en vert). J'ai également ouvert la fenêtre de configuration IP du service PPTP où nous retrouvons tous les paramètres nécessaires à la "conversation" des postes entre eux. Les points importants sont :

Routage IP : Il permet d'autoriser les clients qui se connectent par VPN* à accéder au(x) réseau(x) auquel(s) appartient le serveur (si l'option est activée).

Attribution d'adresse IP : Il permet d'attribuer une adresse virtuelle dans la zone d'adressage d'un des réseaux du serveur, aux clients qui se connectent.

La résolution de noms de diffusion : Il permet d'autoriser le passage des paquets IP broadcast notamment utilisés pour la diffusion des noms d'hôtes NetBIOS*. D'une façon simple, il s'agit de paquets qui ont pour destinataire tout le réseau. Ces paquets sont utilisés avec le protocole* NetBIOS* pour que les postes puissent se déclarer aux autres : "Bonjour à tous, je suis MachineY et j'ai l'adresse x.x.x.x !".

Nous allons maintenant voir la fenêtre de configuration des différentes sécurités et des enregistrements.



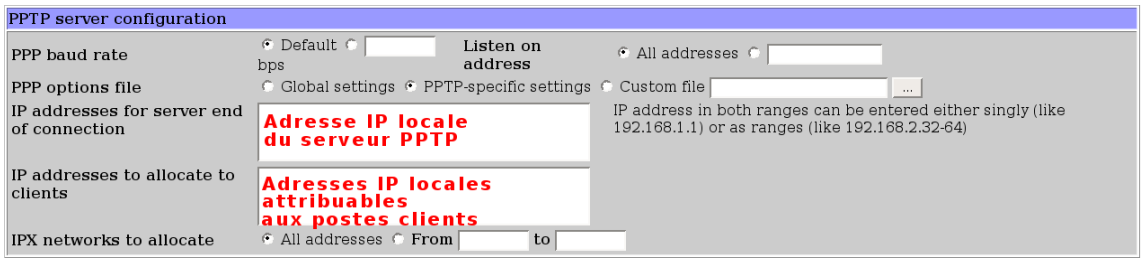
Console d'administration : Sécurité et enregistrements

La console d'administration permet, d'autre part, de spécifier les paramètres d'enregistrements et de sécurités. Les enregistrements correspondent à un historique des connexions et déconnexions qui s'établissent sur le serveur PPTP. On peut régler des niveaux d'enregistrements (tout enregistrer, uniquement des erreurs...) néanmoins, il est fortement conseillé de procéder à un enregistrement maximal au vu des failles de sécurité importantes que comporte ce protocole*. Un enregistrement important permettra de garder de nombreuses traces sur les connexions, leurs durées, leurs dates ou encore leurs provenances. En ce qui concerne les paramètres de sécurité, on peut forcer l'utilisation des versions les plus sécurisées des algorithmes comme MS-CHAP v2.

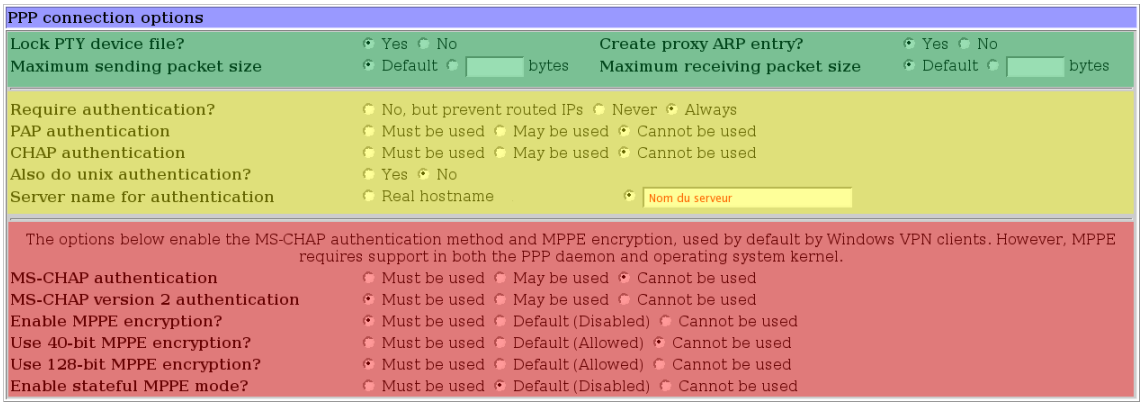
Mise en place d'un serveur PPTP sous environnement GNU/Linux* avec Webmin (distribution Debian)

Note : Comme pour Microsoft Windows Serveur 2003, les étapes détaillées et illustrées pour l'installation et la configuration du serveur PPTP sur un serveur GNU/Linux* préexistant sont décrites en Annexe 7 à la fin de ce document.

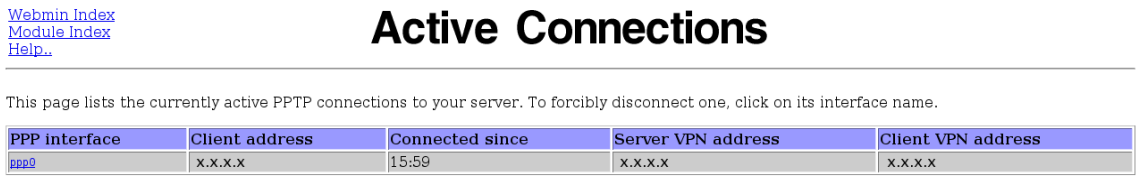
Pour la configuration du serveur PPTP sous GNU/Linux*, il est plus commode d'utiliser un outil graphique appelé Webmin qui peut être lancé à l'aide d'un navigateur Internet.



Webmin : Configuration du routage IP



Webmin : Configuration de la sécurité



Webmin : Connexions en cours

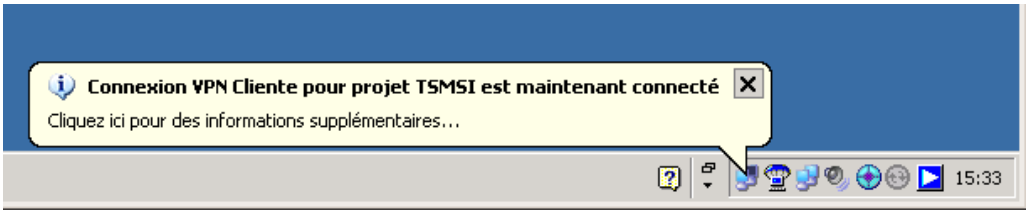
La page de configuration du routage IP est assez dépouillée. Les deux informations importantes à rentrer sont l'adresse locale du serveur PPTP et enfin la plage d'adresses locales attribuées pour les postes clients qui désirent se connecter.
La page de configuration de la sécurité est plus complète et plus complexe. Tout d'abord dans la zone surlignée en vert, il est possible de configurer la taille des paquets IP échangés. Ensuite dans la zone surlignée en jaune, se trouvent les paramètres généraux de la sécurité (si une authentification est obligatoire, s'il faut utiliser les protocoles* PAP ou CHAP pour l'authentification...). Enfin de la zone en rouge, il s'agit de la configuration avancée de la sécurité où l'on peut régler finement les paramètres de chiffrement et d'authentification.
Pour finir sur la dernière illustration, on peut voir une connexion VPN* établie et en cours de fonctionnement.

3.5.2 Mise en place du PPTP (client)

Note : Les étapes détaillées et illustrées pour l'installation et la configuration du client PPTP sur un poste Microsoft Windows XP préexistant sont décrites en Annexe 8 à la fin de ce document.

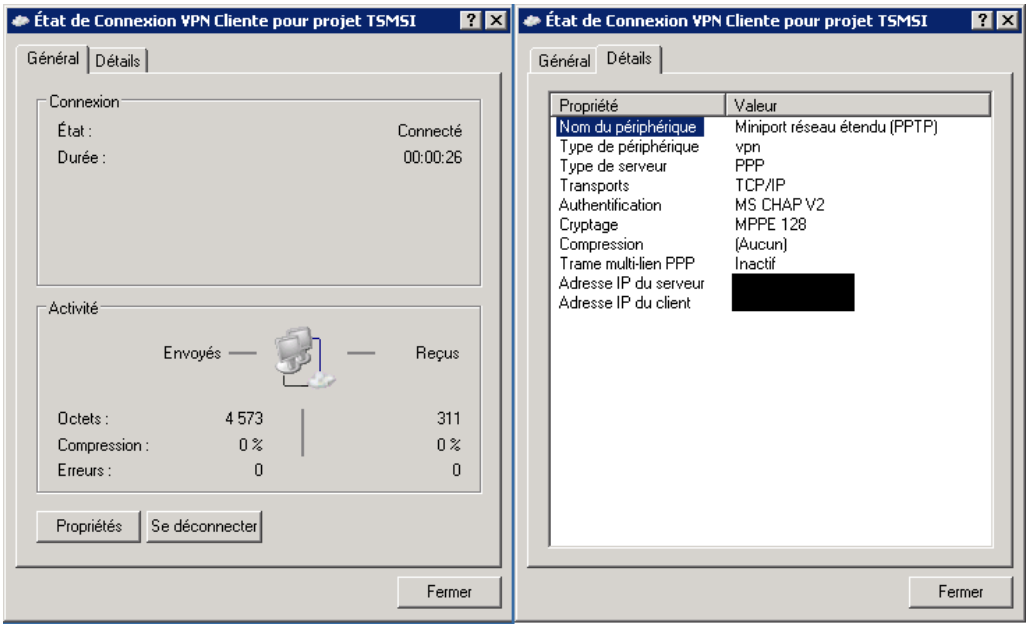
Lorsque la connexion est créée, il suffit de la lancer en double cliquant dessus. Une fenêtre s'ouvre alors pour demander le nom d'utilisateur et le mot de passe nécessaire à l'établissement de la connexion comme le montre l'image suivante :

Ouverture d'une connexion VPN*



La connexion s'est établie avec succès

Lorsque les champs ont été remplis et la connexion lancée en ayant cliqué sur le bouton "se connecter", la connexion s'établit et elle apparaît en bas à droite de l'écran à côté de l'horloge. Si l'on regarde dans les propriétés de la connexion virtuelle qui s'est créée, on peut noter plusieurs informations que le serveur nous a fourni : notre adresse IP virtuelle du réseau distant, le chiffrement utilisé, l'authentification utilisée, la durée de connexion ou encore le gain obtenu grâce à la compression.



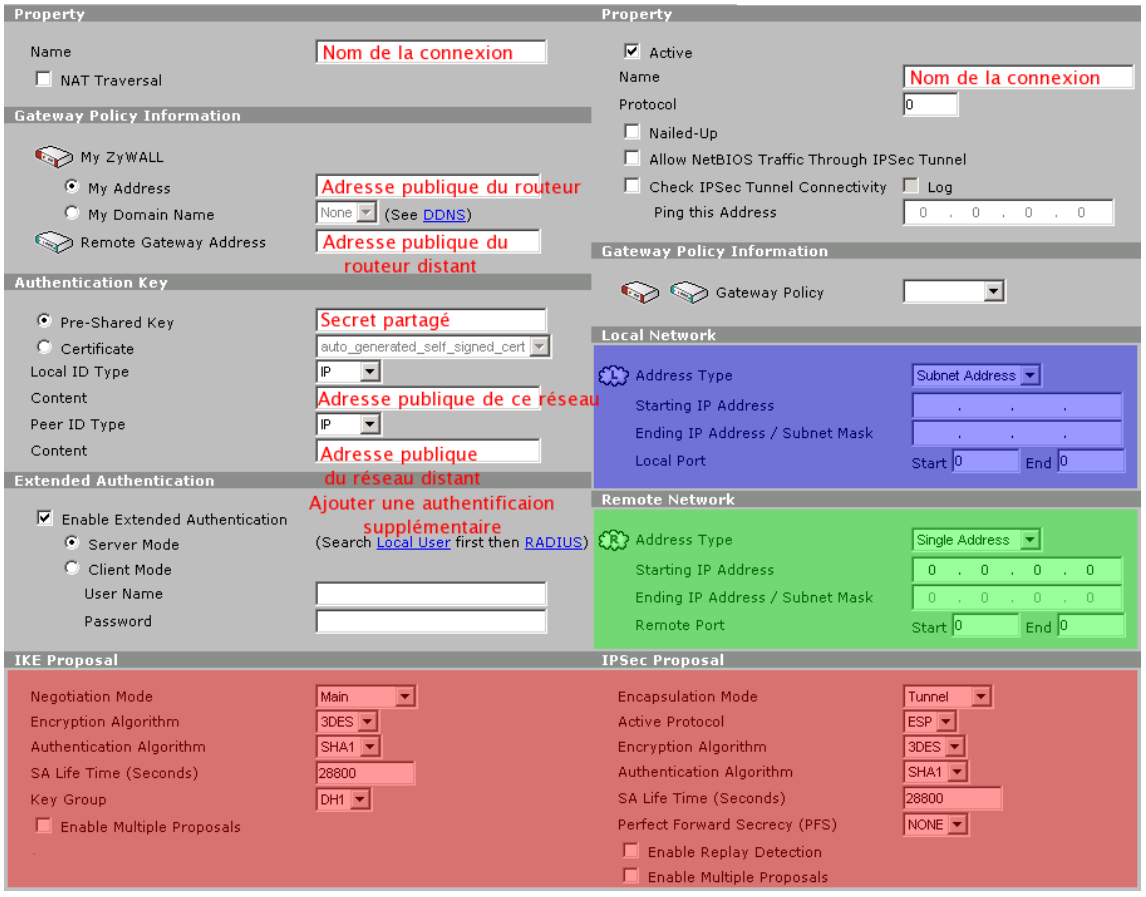
Informations sur la connexion PPTP créée

Résultat : Il est possible dorénavant d'employer les outils habituels que nous utiliserions au bureau pour travailler : le client de messagerie, une application métier... De plus, il est également possible d'accéder aux données partagées comme si l'ordinateur était physiquement dans le réseau auquel il vient d'être connecté. Tout cela de n'importe où, il suffit juste d'avoir un accès à Internet.

3.5.3 Mise en place de l'interconnexion IPSec

Pour la mise en place d'une connexion de type IPSec, j'ai opté pour l'utilisation de routeurs ZyWall 5 de la marque Zyxel car mon entreprise tutrice, NBM-Europe, en vend un certain nombre et de plus il s'agit de produits très implantés sur Suisse.

Avant de mettre en place la connexion IPSec entre deux sites, il faut bien sûr vérifier le fonctionnement des liens Internet. Ensuite, il est possible de configurer les paramètres de IPSec à travers une interface Internet intégrée au routeur.



Interface Internet d'administration de la connexion IPSec

Pour mettre en place l'interconnexion VPN*, il faut régler quelques données :
- Mettre un nom de connexion
- Indiquer l'adresse publique du routeur local (s'il a une adresse fixe sinon il suffit d'indiquer le nom FQDN*)
- Indiquer également l'adresse publique du routeur distant ou son nom FQDN*
- Mettre en place un système d'authentification par secret partagé ou par certificat
- Ajouter ou non une authentification supplémentaire

Ensuite, la zone rouge permet de spécifier les algorithmes de chiffrement, d'authentification, de vérification d'intégrité ou bien encore le mécanisme utilisé (ESP ou AH) et le mode de fonctionnement (tunnel ou transport). Les zones bleues et vertes permettent de configurer les deux réseaux en présence (le local et le distant respectivement).

Lorsque l'on a configuré un des deux routeurs, il faut procéder à la mise en place du second en prenant bien en compte les informations que l'on a rempli dans le premier.

1. Les informations sur le type de tunnel, les chiffrement contenues dans la zone rouge doivent être identiques.
2. Si l'authentification étendue a été mise en place, l'un des deux routeurs doit faire office de serveur et l'autre de client.
3. Le secret partagé ou les certificats doivent être échangés.
4. Les informations sur les réseaux dans les zones bleues et vertes doivent être inversées
5. Les adressages publiques doivent également être inversés.

Résultat : A la fin de la mise en place, un lien IPSec a été créé entre les deux routeurs et des données peuvent être échangées en permanence et de façon totalement transparente entre les deux réseaux distincts qui peuvent être séparés de plusieurs milliers de kilomètres. Si la connexion Internet de l'un des sites tombe momentanément en panne, le tunnel sera automatiquement remis en place dès que la connexion sera de nouveau disponible.

3.5.4 Problèmes rencontrés

Durant la réalisation de mon projet, j'ai rencontré quelques difficultés.

Des problèmes de documentation

Tout d'abord, j'ai eu du mal à obtenir des informations claires et complètes sur les différents protocoles* de tunnellisation qui ont été présentés.

- Pour le protocole* PPTP, les documentations furent nombreuses. J'ai donc pu travaillé dessus facilement.
- Pour le protocole* L2TP, les informations techniques et complètes se sont raréfiées.
- Pour le protocole* IPSec, j'ai trouvé beaucoup de données tout comme le protocole* PPTP.
- Pour le protocole* OpenVPN, j'ai eu beaucoup de mal à obtenir de la documentation technique sur le fonctionnement du protocole*. Par contre, il y avait un grand nombre d'informations sur les moyens de mise en place de cette solution.

Des problèmes de mise en place

Ensuite les difficultés se sont portées sur la mise en place des solutions :

- Serveur PPTP sous Microsoft Windows Serveur : Je n'ai pas rencontré de difficulté quant à l'installation du service PPTP dans un environnement Microsoft Windows Serveur. La mise en place est assistée et intuitive.
- Serveur PPTP sous GNU/Linux* : La configuration du service PPTP en elle-même s'est déroulée correctement. Mais j'ai tout de même eu une difficulté au niveau de l'algorithme de chiffrement MPPE. En effet, ce dernier est propriétaire[12] et la distribution GNU/Linux* (Debian) que j'ai employée, n'incorpore pas de logiciels ou code propriétaire par philosophie. Il a donc fallu que je recompile un noyau complet avec un patch spécifique au support de l'algorithme MPPE et ensuite tout a bien fonctionné.
- Client PPTP sous Microsoft Windows : Tout comme pour l'installation du serveur PPTP, la configuration du client PPTP sous Microsoft Windows est simple et intuitive (comme en témoignent les étapes décrites en Annexe).
- Serveur IPSec : La configuration de routeurs Zyxel ZyWall ne m'a pas posé de problèmes. En effet, il s'agit de produits que j'utilise fréquemment lors de mes périodes en entreprise.

[12] Il appartient à Microsoft

3.6 Vérification du fonctionnement

Une fois la connexion établie depuis un poste client Microsoft Windows XP, il est possible de tester le fonctionnement du tunnel et de s'assurer que des données circulent bien à l'intérieur. Cela s'effectue tout simplement en vérifiant que l'on peut appeler un appareil situé sur le réseau distant. Cette manipulation s'effectue grâce à la commande "ping" qui est une commande de base en réseau. Elle permet d'interroger une machine qui renvoie une réponse si elle est autorisée (aucun pare-feu* ne bloque la réponse ou la requête). Nous allons donc tester une requête ping sur un nom d'hôte (ce qui oblige en plus l'ordinateur à procèder à une résolution d'adresse sur le serveur DNS* distant).

Comme on peut le voir sur la capture d'écran précédente (les adresses et les noms d'hôtes ont été modifiés), une réponse est bien reçue de l'hôte que l'on a demandé. Cela signifie donc que les données transitent bien dans le tunnel PPTP et que nous avons accès aux différents services disponibles sur le réseau distant auquel on s'est connecté. Avec la commande "ipconfig", on constate également qu'une deuxième connexion s'est créée. Elle est virtuelle et représente justement ce tunnel VPN*.

3.7 Conclusion

L'utilisation de ces techniques

J'ai commencé ce chapitre en définissant ce qu'était une interconnexion VPN* et en expliquant les besoins des entreprises qui font que l'on rencontre ce type de solutions de plus en plus fréquemment. J'ai ensuite détaillé un certain nombre de solutions mûres et éprouvées. Je les ai donc comparées en prenant compte de leurs réponses aux besoins des entreprises et de leurs coûts de mise en place et de maintenance après installation. Enfin, j'ai présenté la mise en place de ces solutions et leur fonctionnement général.

Cependant, je n'ai pas montré directement l'utilisation concrète qu'il pouvait être faite de cette technologie avec des exemples.

- Bien sûr, nous pouvons utiliser cette technologie pour permettre l'accès aux données des utilisateurs partout dans le monde comme je l'ai déjà indiqué. Ces données peuvent être sous de nombreuses formes : des courriers, des fichiers ou bien un Intranet...
- Il peut aussi permettre l'accès à des ressources également à travers le monde comme des ordinateurs, des imprimantes...
- On peut se servir de ce moyen technique pour ne plus utiliser d'ordinateurs standards dans toute l'entreprise mais utiliser ce que l'on appelle des clients légers. Il s'agit de petits ordinateurs qui ne peuvent rien stocker et ne peuvent pas démarrer sans l'aide d'un serveur spécifique. Avec ce client léger, on travaille directement sur le serveur comme si l'on était physiquement dessus. Tout cela a des avantages de coût (client léger peu cher et administration à n'effectuer que sur le serveur qui néanmoins doit être puissant).
- La téléphonie sur IP ou VoIP* peut également bénéficier de cette technologie. On peut imaginer une entreprise où toute la téléphonie utilise de la VoIP* qui passe par les connexions VPN*, et donc réduit à zéro les frais de communication interne.
- Il existe bien d'autres applications possibles et imaginables...

Pour terminer

La mise en place de ce type de solution à donc des répercussions sur le travail du personnel, sa productivité et son organisation. Il lui est, en effet, maintenant possible de reprendre un travail non achevé à n'importe quel moment, depuis n'importe où et donc de gagner du temps. De plus ce système est mis à contribution pour gagner en frais de maintenance (informatique, téléphonique...) et en frais de "communication". Il est possible, d'une part, de coupler cette solution avec un filtrage tel qu'un pare-feu* afin de consolider encore la sécurité de l'entrée VPN* en contrôlant davantage ce qui est autorisé à emprunter le tunnel concerné. Mais d'autre part, il est envisageable de mettre en service un système redondant pour le serveur VPN*.

Chapitre 4

Conclusion

Durant le cycle TMSI, le travail que j'ai pu réaliser au sein de la société NBM-Europe fut très varié. J'ai donc pu acquérir une large expérience qui m'a appris ce qu'est le travail de technicien informatique en administration réseau. Mais dans l'ensemble, il fallait répondre aux besoins de petites ou moyennes entreprises qui restent tout de même assez proches même si les outils de travail diffèrent.

J'ai donc durant ces deux années acquis un certain nombre de compétences :

- Une compétence technique : J'ai dû travailler sur de nombreux outils aux fonctionnalités totalement différentes allant de la gestion de partage sur un système d'exploitation classique Microsoft Windows 2003 Serveur à la mise en place de logiciels métier fonctionnant sur des partages spécifiques et uniques)
- Une veille technologique : J'ai pu voir avec des collègues des tests de nouveaux produits avant leurs mises en fonctionnement de production. Par exemple l'utilisation de la technologie VoIP* sur des connexions de type VPN* comme sur mon projet.
- Une expérience sociale : J'ai, de plus, beaucoup appris sur les relations fournisseurs/clients et sur le contact ou la communication plus simplement. Il est à noter également que j'ai pu me faire de nombreuses relations avec des personnes du métier.

Ce mémoire m'a permis de faire le point sur mon évolution au cours de ces deux années et d'apprendre l'utilisation de nouveaux outils comme : LaTeX

Maintenant, je ne pense pas continuer mes études mais intégrer la société qui m'a suivi jusqu'à aujourd'hui afin de renforcer mon expérience professionnelle. Et ensuite, augmenter mon niveau scolaire à l'aide des validations des acquis de compétences.

Glossaire

Active Directory : Annuaire de Microsoft qui contient de nombreuses informations comme les utilisateurs, les ordinateurs, les imprimantes...

ADSL : (Asymmetric Digital Subscriber Line) Technique d'utilisation d'une ligne téléphonique pour accèder à Internet.

A la volée : Qui est fait en temps réel.

Armoire de brassage : Armoire informatique où se regroupent toutes les prises informatiques murales d'un bâtiment ou d'un local.

Base de connaissance : Dans notre cas, il s'agit d'une page Internet (généralement d'un fabricant) qui propose des solutions à de nombreux problème pour un produit.

Cache : Espace mémoire qui contient des données temporaires.

Cluster : Un cluster est un ensemble de machines qui contiennent les mêmes données afin que ces dernières restent disponibles en cas de panne de l'une des machines.

CRC : (Cyclical Redundancy Check) Méthode qui permet de vérifier si des données sont valides.

DNS : (Domain Name Service) Il s'agit d'un service qui permet de trouver une machine grâce à un nom (exemple : machine.domaine.com) au lieu d'une adresse IP composée de chiffres.

Formater : Initialiser un système de fichier* sur le disque dur d'un ordinateur (ce qui videra son contenu).

FQDN : (Fully Qualified Domain Name) Il s'agit du nom complet d'une machine (par exemple machine.domaine.com. est une adresse FQDN).

Gettext : Il s'agit d'une technique en programmation qui permet de traduire facilement des programmes dans différentes langues.

GNU/Linux : Système d"exploitation libre utilisant les applications GNU et le noyau Linux pour fonctionner.

GTK+ : Il s'agit d'une bibliothèque qui permet de créer des interfaces graphiques pour des programmes informatiques.

Langage C : Langage informatique utilisé pour l'élaboration de nombreux programmes.

Maintenabilité : La maintenabilité est la capacité de pouvoir maintenir de manière cohérente et à moindre coût certains composants ou applications.

NAT : (Network Address Translation) Méthode qui permet l'utilisation d'une seule connexion Internet par plusieurs postes informatiques.

Natif : Se dit native une fonctionnalité qui fonctionne directement sans nécessiter l'installation d'un autre composant.

NetBIOS : Protocole* de résolution de noms permettant donc de retrouver une machine par son nom et non pas par son adresse IP.

Pare-Feu : Un pare-feu est un logiciel ou un équipement qui permet de filtrer les données qui passent à travers lui.

PHP : Langage de programmation utilisé pour obtenir des pages Internet dites dynamiques (qui prennent en compte des paramètres sur l'internaute...).

PHP/MySQL/XHTML/CSS : Le fait de combiner le langage PHP* avec les langages XHTML/CSS* et en utilisant en plus une base de données (MySQL).

Pilote : Composant logiciel qui permet de faire fonctionner un périphérique spécifique (imprimante, scanner...) avec un ordinateur.

Protocole : Spécification d'un dialogue qui permet à plusieurs ordinateurs de communiquer.

Registrar : Société gérant des noms de domaines (par exemple : nom-de-domaine.com).

Registre : Sur Microsoft Windows, il s'agit d'un ensemble de fichiers qui contiennent la quasi totalité de la configuration du système.

RFC : Documentation sur les spécifications exactes d'un standard ou d'un protocole*.

SASL : Méthode d'authentification.

Serveur FTP : Serveur qui offre un service adapté au transfert de fichier.

Serveur Web : Serveur capable de fournir des pages Internet.

Spyware : Un logiciel espion.

SSL : (Secure Socket Layer) Algorithme de chiffrement largement utilisé sur Internet.

Synchronisation : Action de détecter le signal ADSL sur une ligne téléphonique.

Système de fichier : Il s'agit de l'organisation de la méthode d'organisation des données contenue sur un disque dur.

Système de redondance : Ce système permet le fonctionnement d'un équipement même si une de ces pièces est défecteuse.

Télémaintenance : Maintenance s'effectuant à distance.

TLS : Algorithme de chiffrement (successeur de SSL*).

VoIP : Technologie permettant de faire transiter des communications téléphoniques sur un réseau informatique.

VPN : (Virtual Private Network) Technique qui permet de créer un réseau virtuel sur un autre réseau.

WebDav : Technologie permettant d'utiliser le service Web* qui sert à afficher des pages Internet comme un serveur FTP*.

XHTML/CSS : Langage de programmation utilisé pour mettre en page des pages Internet (XHTML contenant les données et CSS indiquant comment les afficher).

Annexes

Annexe 1

Présentation des formations proposées à NBM-Europe

N B M • **FORMATION**
373, Route du Nant - Z.A. de Magny
01280 Prévessin Moëns
Tél. 04 50 28 07 29 - Fax 04 50 28 08 04
e-mail : [redacted]@nbm-europe.com - http://www.nbm-europe.

***NBM** propose des formations pour les entreprises et les particuliers (Macintosh-MacOS ou PC-Windows). Notre formatrice, [redacted], met à votre disposition ses 15 années d'expérience et vous propose toute une gamme variée de cours.*

LISTE DES COURS

Systèmes d'exploitation : **Mac OS 9 & X - Microsoft Windows 2000-XP**
Traitement de texte : **Microsoft Word**
Tableur : **Microsoft Excel**
Intégré : **AppleWorks**
Base de données : **FileMaker Pro**
Mise en pages : **QuarkXpress - Indesign**
Graphisme : **Adobe Illustrator**
Traitement de l'image : **Adobe Photoshop**
Échange de document : **Adobe Acrobat**
Navigation Internet : **Microsoft Internet Explorer - Safari**
Mail : **Microsoft Entourage - Microsoft Outlook - Mail**
Publication Internet : **Microsoft FrontPage**
Présentation de diaporamas : **Microsoft Powerpoint**
iApplications : **iCal, iSync, iChat, iPhoto, iTunes, iMovie, iDVD**

INFORMATIONS PRATIQUES

Chaque participant dispose d'un support de cours. La salle de formation est équipée de 6 ordinateurs PC récents et d'une projection sur grand écran.

Votre contact : [redacted]
• Par téléphone : 04 50 28 07 29
• Par courrier : 373, Route du Nant - Z.A. de Magny - 01280 Prévessin Moëns
• Par e-mail : [redacted]@nbm-europe.com

TARIFS

Tarif-Entreprise : **une journée** de 6 heures de formation (Prix Hors Taxes)
- sur la base de **1** personne ..... [redacted] € HT
- sur la base de **2** personnes ..... [redacted] € HT
- sur la base de **3** personnes ..... [redacted] € HT
- sur la base de **4** personnes ..... [redacted] € HT
- sur la base de **5** personnes ..... [redacted] € HT
- sur la base de **6** personnes ..... [redacted] € HT

Tarif-Particulier : 1 heure ..... [redacted] € TTC (minimum 2 heures consécutives)
Tarif-Particulier : Forfait 10 heures (par 2 heures)..... [redacted] € TTC
(Frais de déplacement hors Prévessin-Ferney [redacted] €)

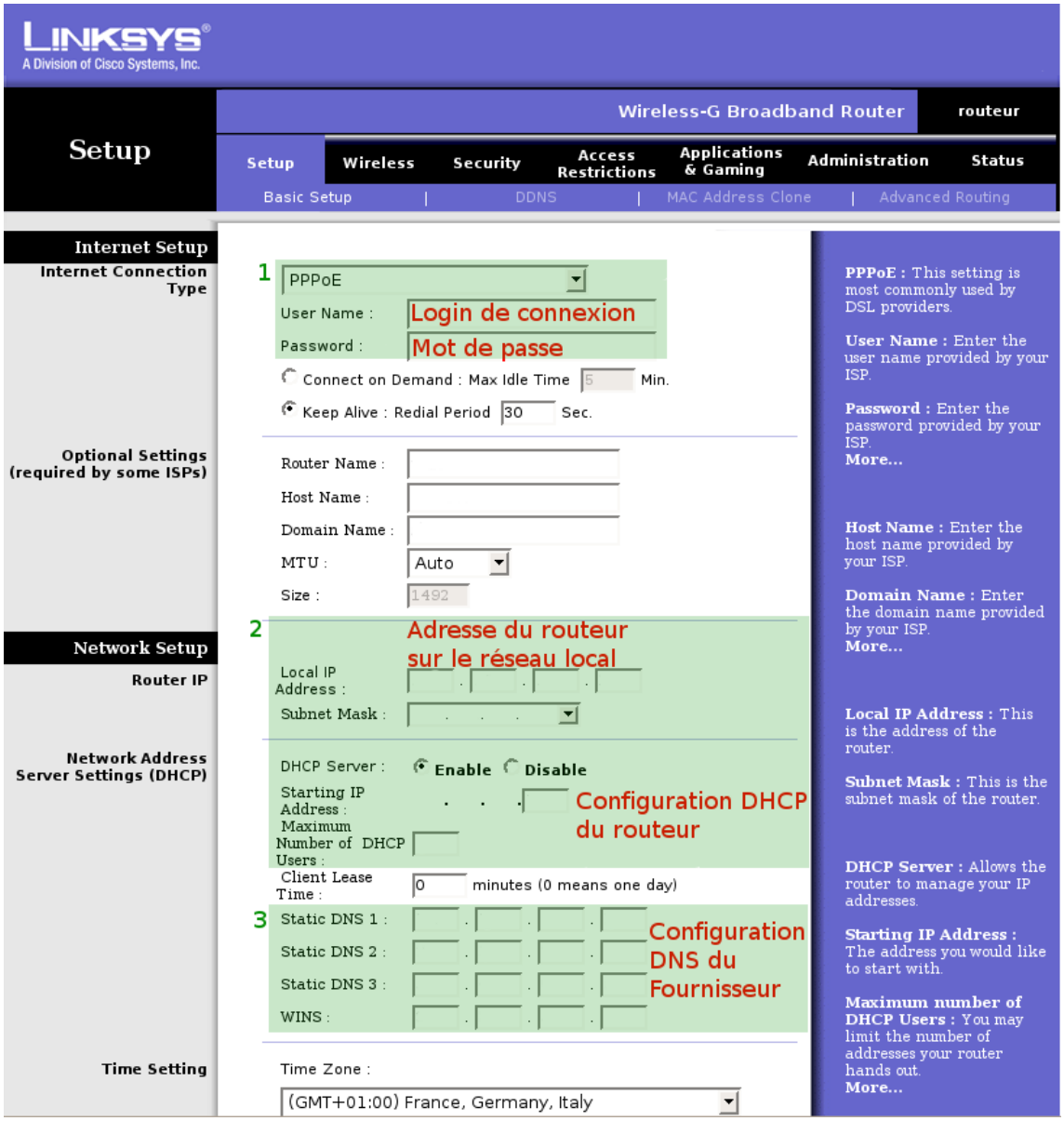
CONDITIONS GÉNÉRALES

Paiement : L'inscription ne sera retenue qu'après le versement de 30% d'acompte. Le solde après la formation.
Annulation : le participant devra annoncer son désistement au minimum 5 jours avant la date du cours. Passé ce délai, l'acompte sera retenu. NBM se réserve le droit d'annuler une formation. Nous vous proposerons alors de nouvelles dates.

NBM Europe.com - 373, Route du Nant - Z.A. de Magny - 01280 Prévessin Moëns

Annexe 2

Configuration d'une connexion Internet partagée (1)

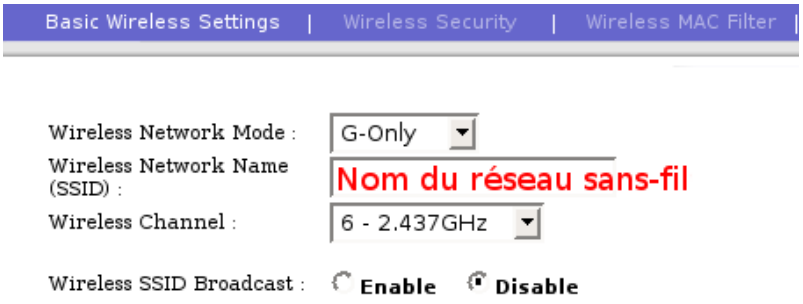


Aperçu de l'interface de configuration d'un routeur pour Internet[1]

[1]Linksys est une marque déposée ou marque de Cisco Systems, Inc. http ://www.linksys.fr

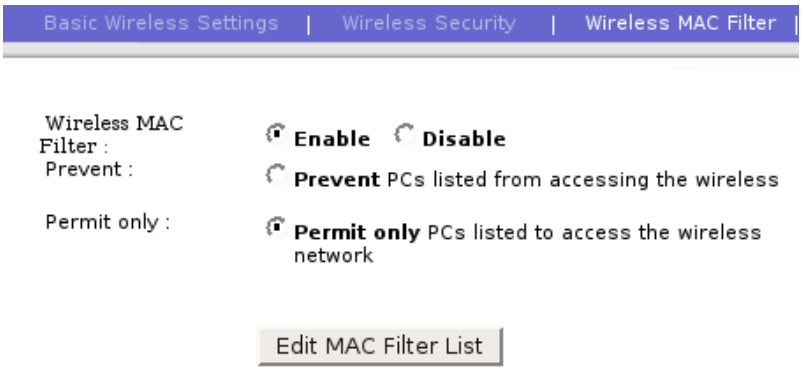
Annexe 3

Configuration d'une connexion Internet partagée (2)



(a) Zone de configuration du sans-fil

(b) Zone de configuration de la sécurité du sans-fil



(c) Zone de configuration de l'accès au sans-fil

Annexe 4

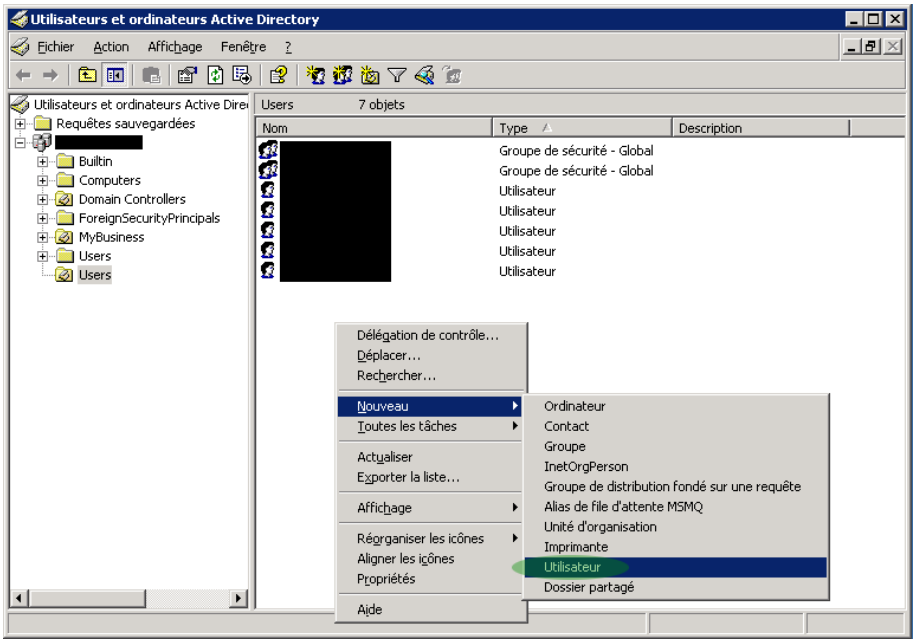
Réinstallation d'un poste informatique : Procédure de mise à jour

Menu pour accèder à l'outil Windows Update

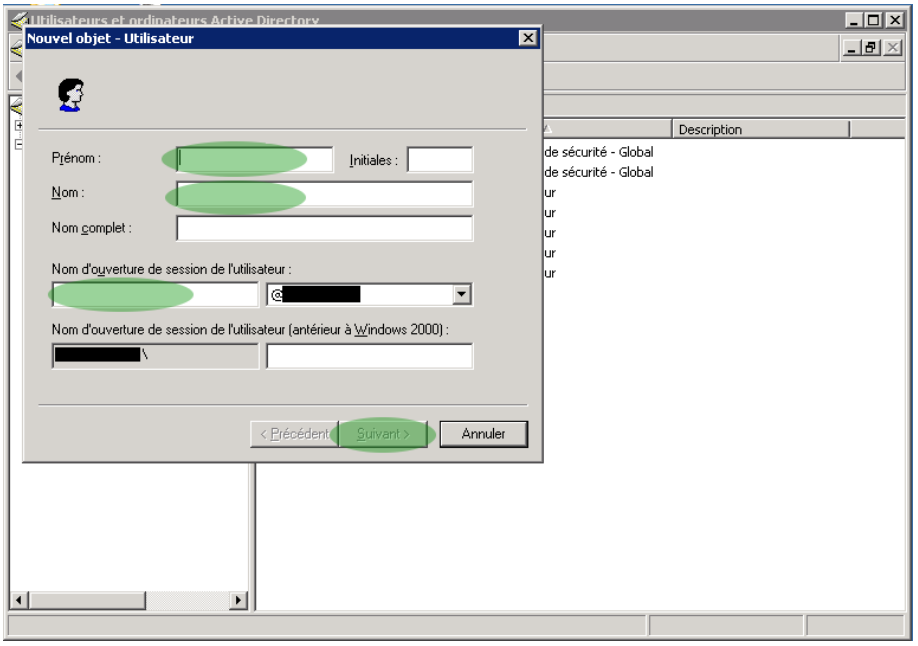
Interface de Windows Update qui nous guide pour installer les mises à jours à effectuer

Annexe 5

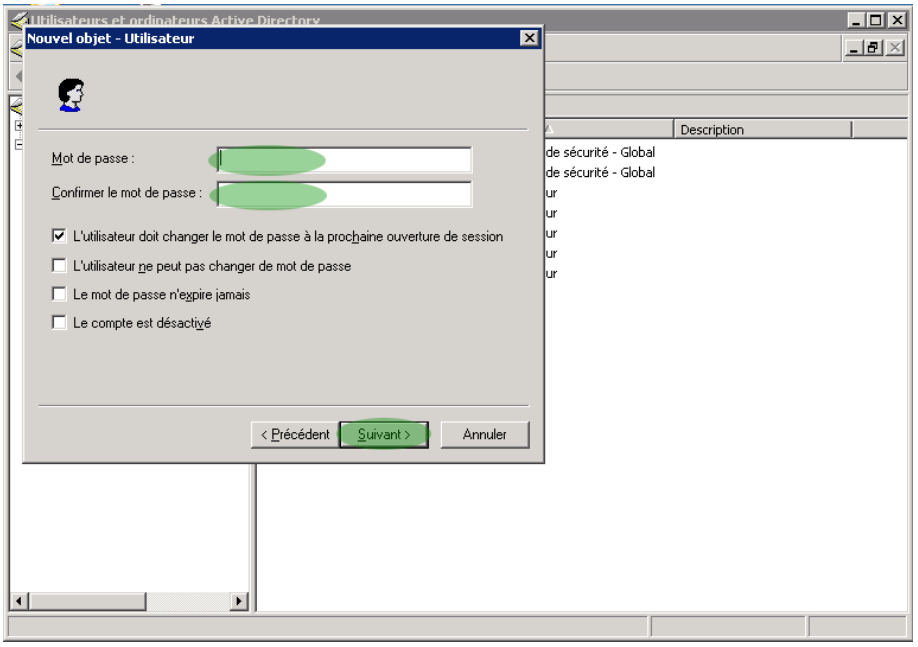
Ajout d'un utilisateur avec sa boite de e-mail sous Microsoft Windows Serveur 2003 avec Exchange 2003



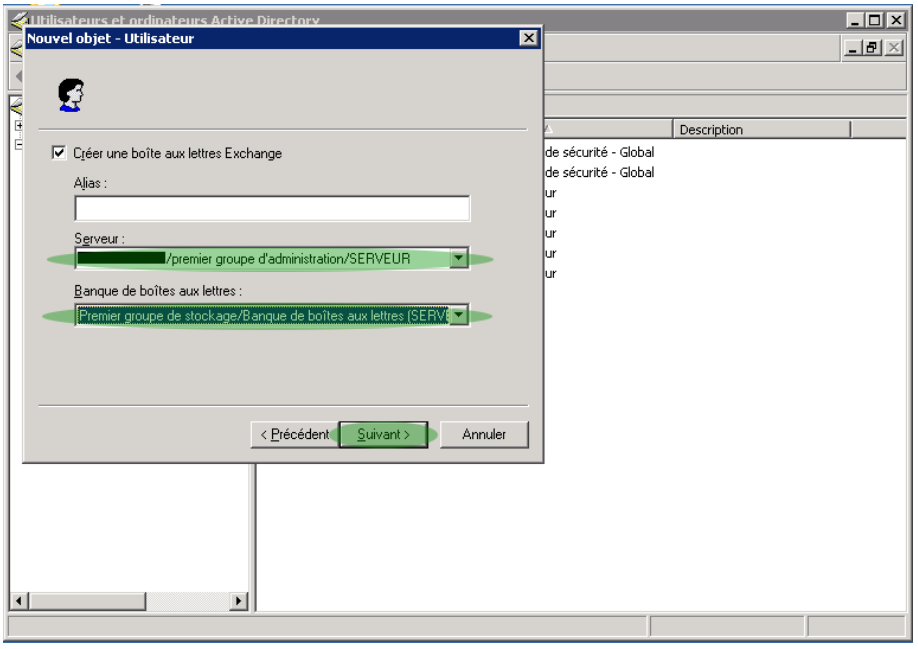
Première étape : Lorsque la console d'administration des utilisateurs de l'Active Directory est ouverte, il suffit de faire un clic droit dans la liste, de pointer sur "nouveau" et sur "utilisateur" puis de cliquer.



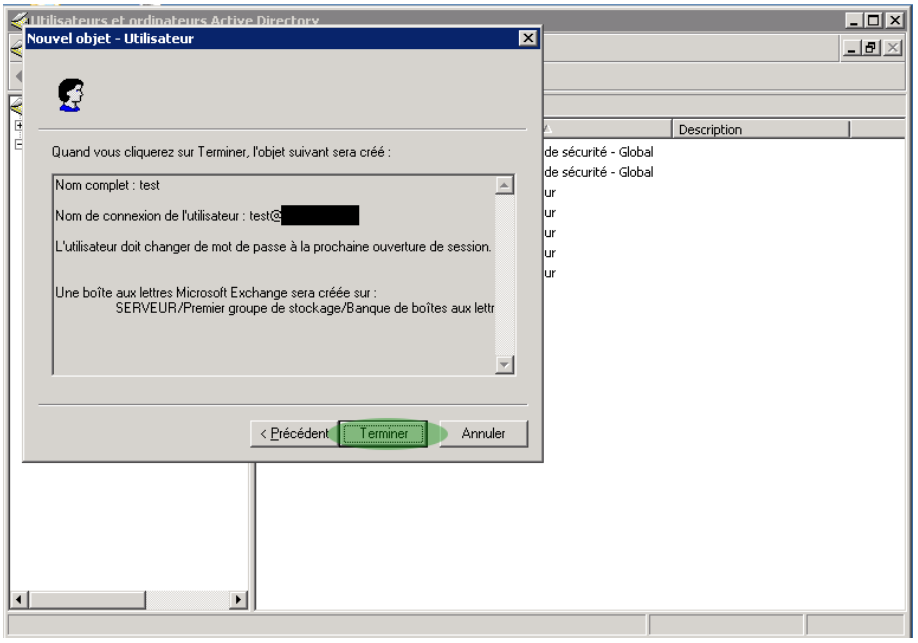
Deuxième étape : L'assistant s'ouvre, nous permettant alors de rentrer les informations sur le nouvel utilisateur (son nom, son login,...). Quand toutes les données ont été complétées, nous pouvons cliquer sur "suivant".



Troisième étape : L'assistant nous demande ensuite le mot de passe de l'utilisateur.



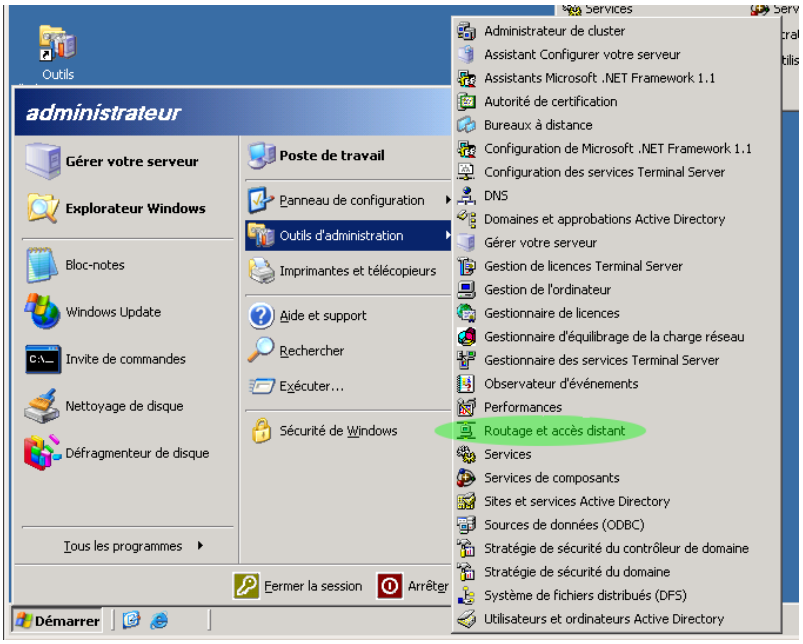
Quatrième étape : Il est nécessaire maintenant d'indiquer quel serveur et quelle base de donnée contiendra les données et les paramètres du nouvel utilisateur.



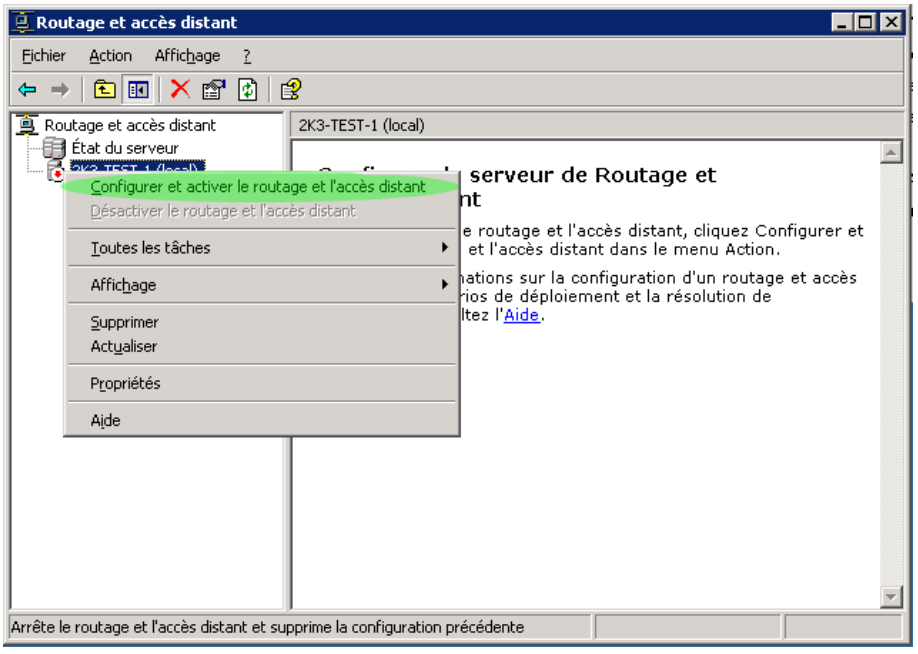
Cinquième étape : Pour finir, l'assistant récapitule les informations saisies et il suffit de cliquer sur "Terminer" pour créer l'utilisateur avec sa boite mail.

Annexe 6

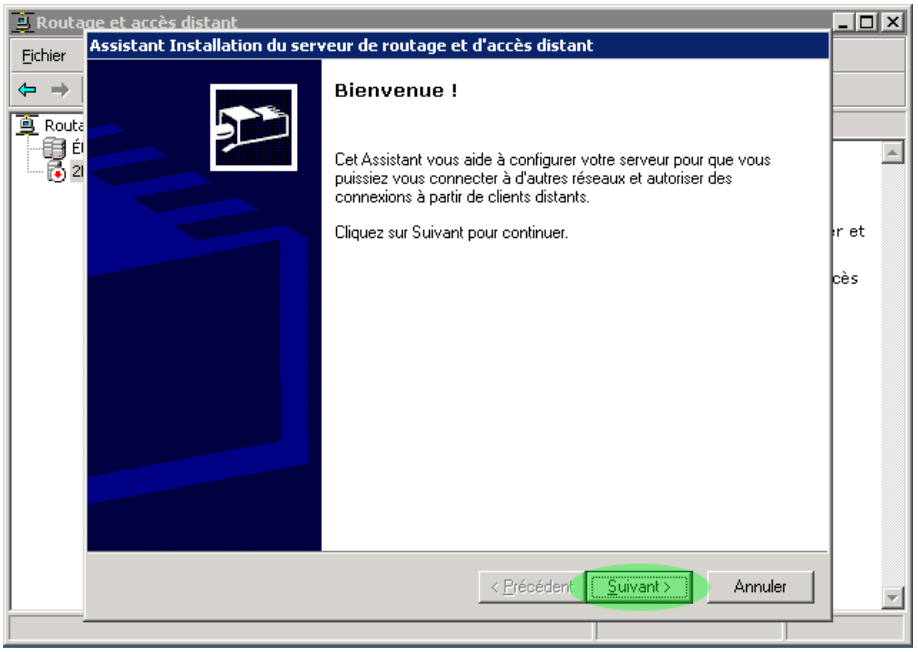
Projet : Installation d'un serveur PPTP sous Microsoft Windows Serveur (Partie 1)



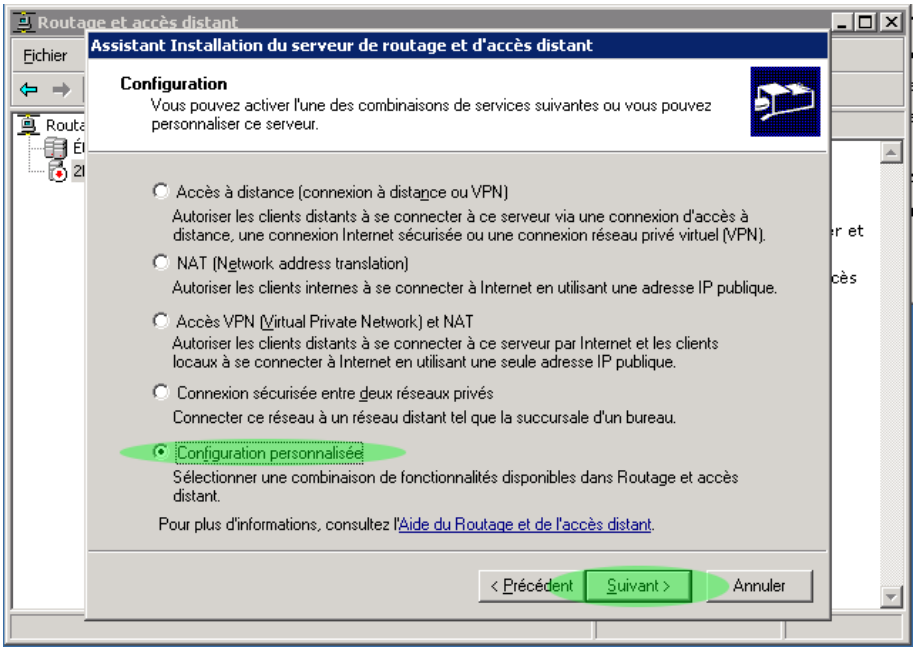
Première étape : Lancement de l'outil "routage et accès distant" dans le menu Démarrer.



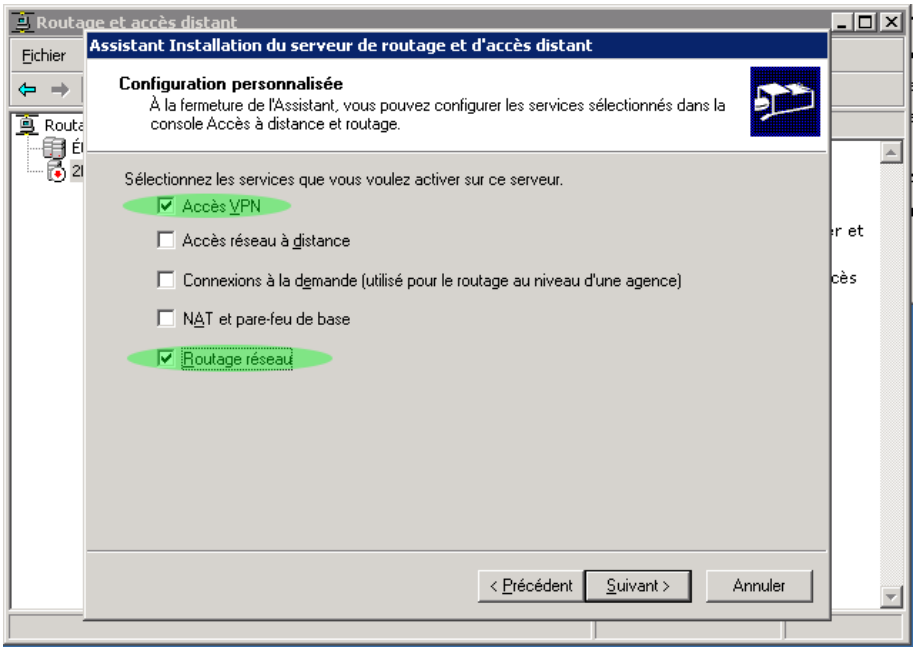
Deuxième étape : La console d'administration "routage et accès distant" s'est ouverte, il faut à l'aide d'un clic droit sur le serveur choisir : "Configurer et activer le routage et l'accès distant".



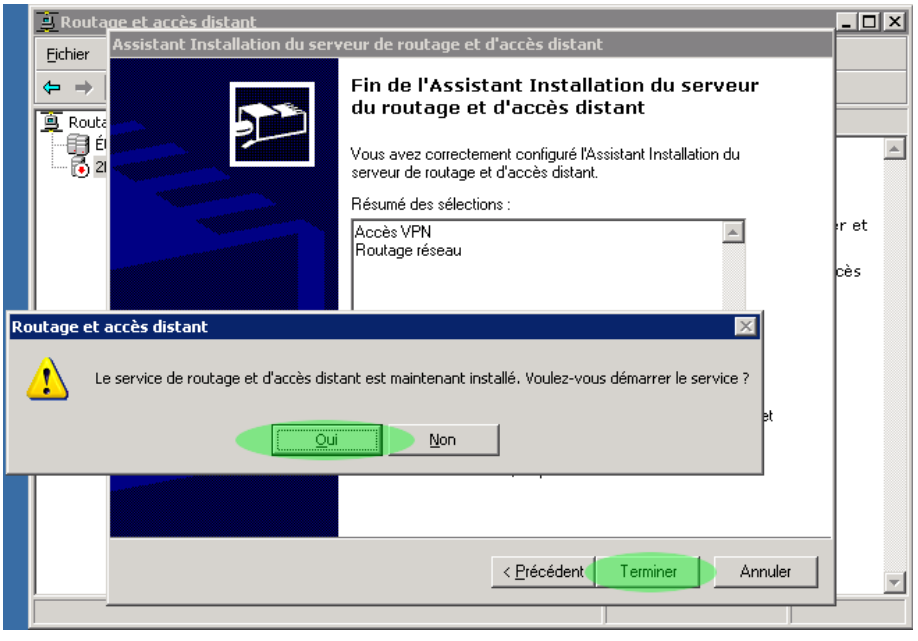
Troisième étape : Un assistant qu'il reste à suivre fait son apparition.



Quatrième étape : Dans l'assistant, il faut alors sélectionner "Configuration personnalisée" et non pas "Accès VPN" car cet dernier choix exige que l'on dispose de deux interfaces réseaux ce qui n'est pas forcément notre cas.



Cinquième étape : Ensuite, il est nécessaire de cocher les cases "Accès VPN" pour autoriser les connexions PPTP vers le serveur et "Routage réseau" pour permettre aux clients qui se connecteront d'accéder au réseau du serveur.



Sixième étape : Enfin pour finir, il faut cliquer sur "Terminer". Une fenêtre s'ouvre alors nous demandant si nous voulons déjà lancer le serveur. Nous répondrons donc "Oui".

Annexe 7

Projet : Installation d'un serveur PPTP sous GNU/Linux

```
Ordinateur:/#cd /proc/sys/net/ipv4
Ordinateur:/proc/sys/net/ipv4#cat ip_forward
1
Ordinateur:/proc/sys/net/ipv4#
```

Première étape : Il faut commencer par vérifier que le poste informatique a bien le routage IP d'activé. C'est-à-dire s'il laisse bien passer les données d'une connexion PPTP vers son réseau local. Si le contenu du fichier "ip_forward" est "un" alors le routage IP est activé, s'il est "zéro"", il ne l'est pas.

```
apt-get install pptpd webmin-pptp-server webmin-pptp-client
```

Deuxième étape : On installe alors le serveur PPTP en lui-même avec l'interface d'administration Webmin pour plus de convivialité lors des différentes maintenances.

```
Ordinateur:/#cd /etc/
Ordinateur:/etc#vi pptp.conf

logwtmp
localip (adresse IP locale du serveur)
remoteip (plage d'adresse locale utilisable par les clients PPTP)
max_connections (nombre de connexions autorisées simultanément maximum)
```

Troisième étape : Il est nécessaire d'éditer le fichier /etc/pptp.conf et de le remplir correctement.

```
Ordinateur:/#cd /etc/ppp/
Ordinateur:/etc#vi chap-secret

utilisateur serveur password (adresse publique autorisée)
utilisateur2 serveur password (adresse publique autorisée)
...
```

Quatrième étape : Il faut, ensuite, éditer le fichier/etc/ppp/chap-secret qui contient les données sur les comptes utilisateurs.

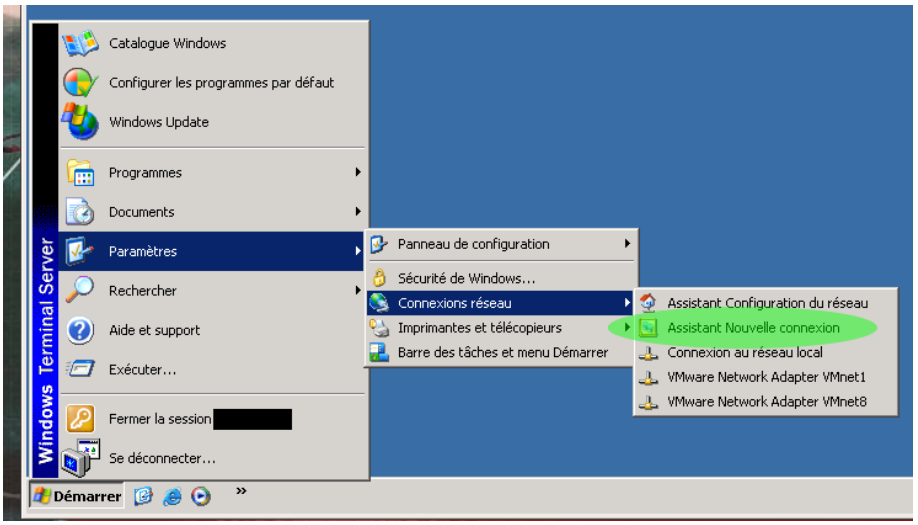
```
Ordinateur:/#cd /etc/ppp/
Ordinateur:/etc#vi pptp.options

name  (nom du serveur)
domain  (domaine du réseau)
chapms-strip-domain
refuse-pap  (refuser un protocole* pas assez sûr)
refuse-chap (refuser un protocole* pas assez sûr)
refuse-mschap (refuser un protocole* pas assez sûr)
require-mschap-v2 (demander l'utilisation de MS-CHAPv2)
require-mppe-128 (demander l'utilisation du chiffrement MPPE sur 128bits)
ms-dns  (adresse du serveur DNS*)
proxyarp
nodefaultroute
lock
nobsdcomp
auth
require-mppe
nomppe-40 (refuser un protocole* pas assez sûr)
```

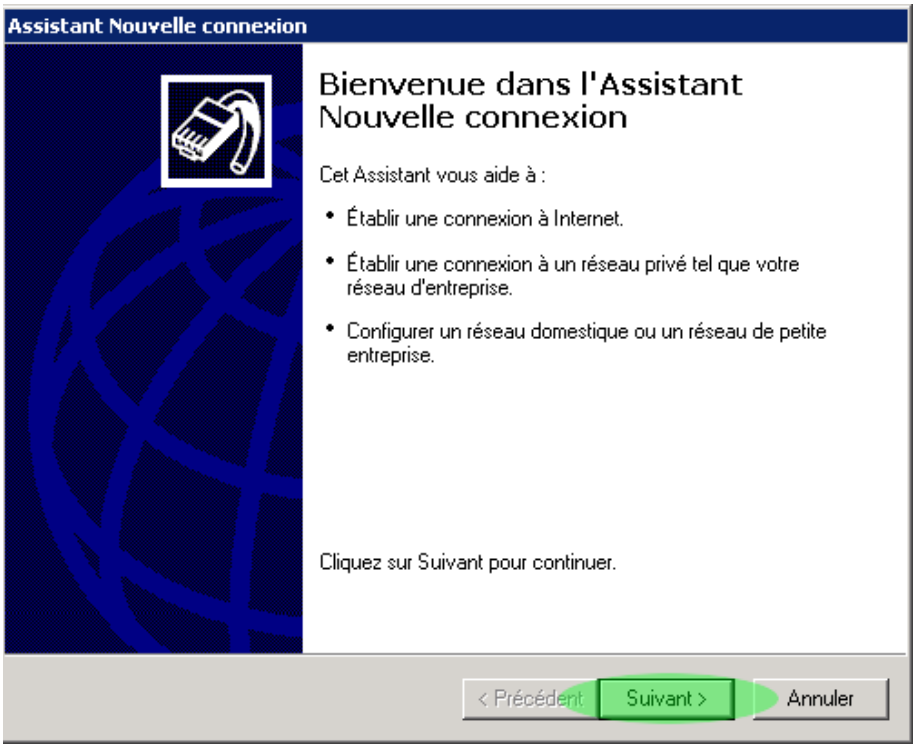
Cinquième étape : Pour finir, il suffit d'éditer le fichier/etc/ppp/pptp.options qui contient la configuration de la sécurité du serveur PPTP. Bien entendu, il vaut mieux empêcher les connexions basées sur des protocoles* trop peu fiables.

Annexe 8

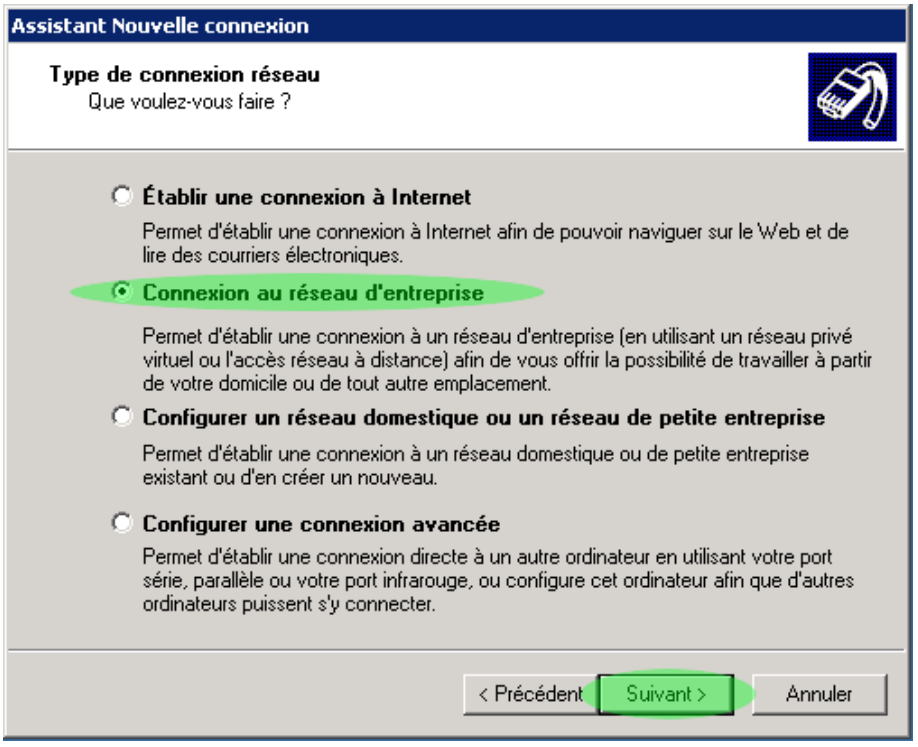
Projet : Installation d'un client PPTP sous Microsoft Windows XP (Partie 1)



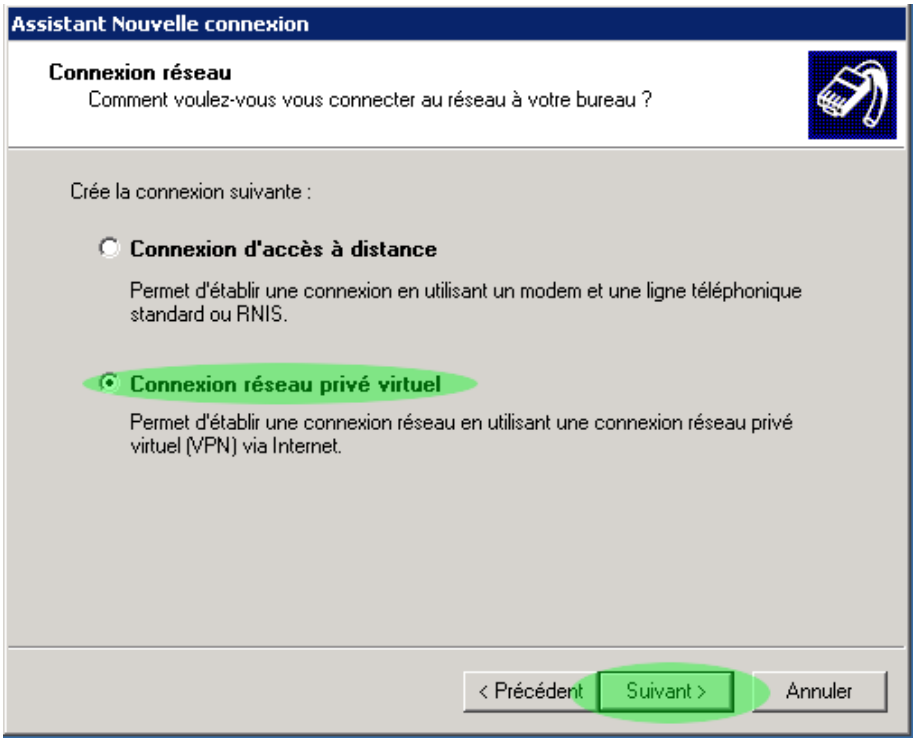
Première étape : Lancement de l'assistant "Assistant Nouvelle connexion" dans le menu Démarrer.



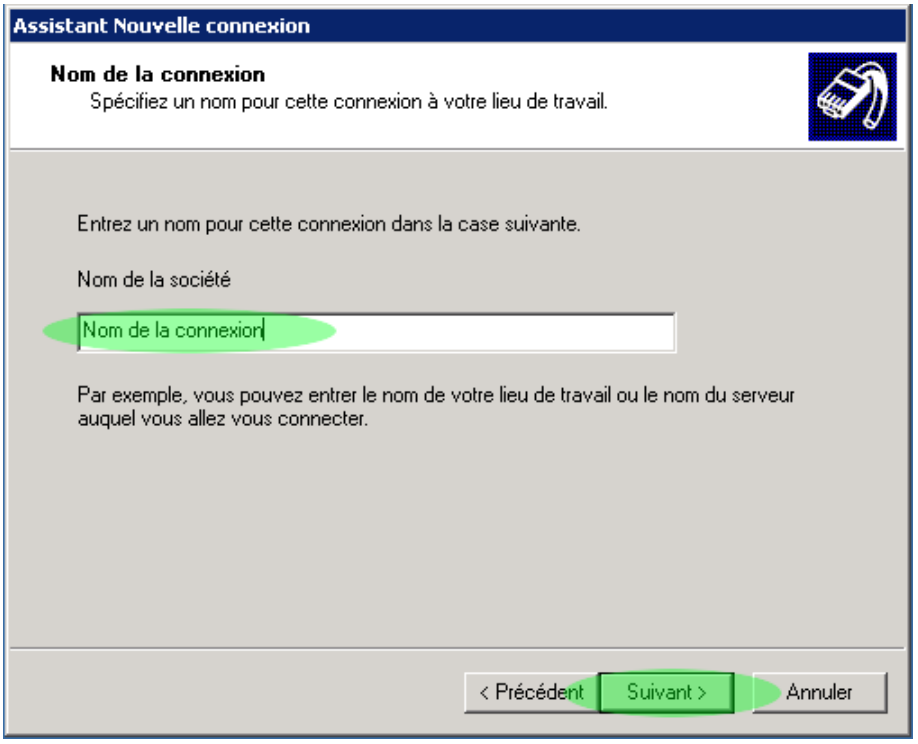
Deuxième étape : L'assistant que l'on doit suivre s'ouvre.



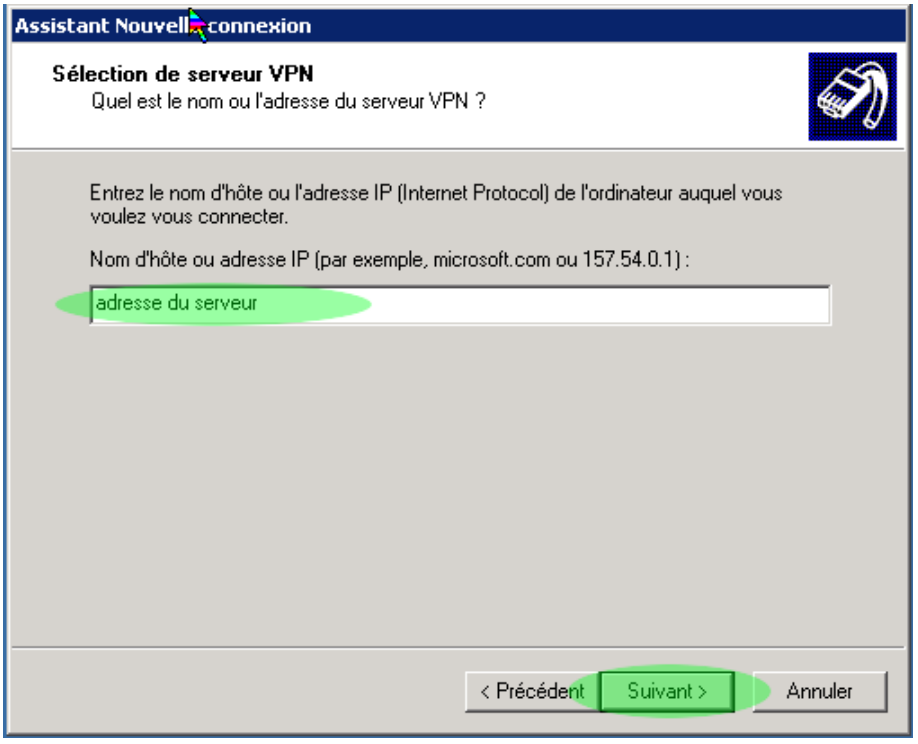
Troisième étape : Dans l'assistant, il faut choisir : "Connexion au réseau d'entreprise".



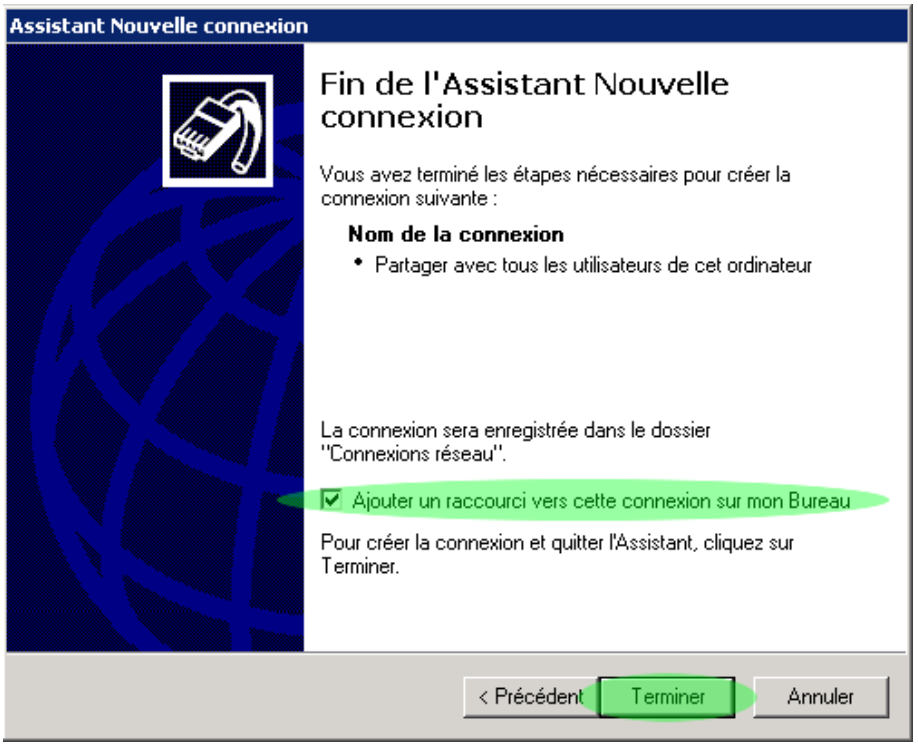
Quatrième étape : Une fois la sélection faite, un nouveau choix apparaît, il faut cocher : "Connexion réseau privé virtuel".



Cinquième étape : Ensuite, il est nécessaire de nommer cette future connexion VPN*.



Sixième étape : Puis, l'assistant nous demande l'adresse IP publique ou le nom d'hôte FQDN* qu'il faut bien sûr remplir pour que le client puisse trouver le serveur sur Internet.



Septième étape : Enfin, l'assistant peut créer la connexion PPTP. Nous pouvons cocher la case : "Ajouter un raccourci vers cette connexion sur mon bureau" et cliquer sur "Terminer".