MASTER EN SCIENCES INFORMATIQUES

Accès à distance
fonctionnement, sécurité et implémentation

Poncelet, Nicolas

Award date:
2006

Facultés Universitaires Notre-Dame de la Paix, Namur

Institut d'Informatique

Année académique 2005-2006

Accès à Distance

Fonctionnement, Sécurité et Implémentation

Nicolas Poncelet

Mémoire présenté en vue de l'obtention du grade de maître en informatique

Résumé

Si les solutions d'accès à distance offrent toute une nouvelle gamme de services pour leurs utilisateurs, il se peut qu'elles ouvrent certaines failles au niveau de la sécurité des systèmes d'information de ces derniers. Les utilisateurs de technologies d'accès à distance étant principalement des entreprises, allant de la simple A.S.B.L. à la société bancaire internationale, il est clair que l'aspect de sécurité des accès distants n'est pas à négliger.

L'objectif du présent travail est donc d'explorer le monde de l'accès à distance ainsi que les implications sécuritaires que présente ce mécanisme. Afin de mieux comprendre les risques, en termes de sécurité informatique, que peuvent présenter les solutions d'accès à distance, nous couvrons les différentes technologies sur lesquelles se basent ces solutions. Nous analysons aussi certaines normes qui régulent l'accès à distance et nous terminons par la proposition d'améliorations qui pourraient être apportées aux solutions d'accès à distance.

Ce mémoire fut notamment basé sur l'expérience et la connaissance acquise durant le stage qui s'est déroulé au Sénégal dans un contexte d'Institutions de Micro Finance, au sein d'une ONG belge du nom d'AQUADEV. C'est pour le compte de cette dernière qu'une solution d'accès à distance a été mise en place.

Du présent travail nous avons pu constater l'énorme intérêt que présente la sécurité en ce qui concerne les solutions d'accès à distance. Nous avons notamment remarqué que les solutions d'accès à distance offertes sont suffisamment sécurisées et que la présence de failles dépend de l'utilisation qui est faite de ces dernières par les utilisateurs.

Mots-clés : Dial-up, VPN, modem, Réseau Téléphonique Commuté, Internet, Institution de Micro Finance, norme, confidentialité, authentification, intégrité, fichier log.

Abstract

Whilst remote access solutions offer a whole new range of services to their users, it's possible that they could also be at the origin of certain security weaknesses in the information systems of the latter. The end users of remote access technology being composed mostly of businesses, ranging from the plain non-profit organisation to the international banking company, it is quite clear that the security perspective of distant access is not negligible.

Hence, the goal of this document is to explore the world of distant access as well as the security implications that this type of mecanism presents. In order to better understand the risks, in terms of IT security, which remote access solutions could present, we cover the different technologies upon which these solutions could be based. Certain regulations concerning remote access are analyzed as well, and we will finish with some recommendations for improvement.

This thesis was especially based on the experience and knowledge acquired during the end of studies internship which took place in Senegal in a Micro Finance Institutions context, within a belgian NGO called AQUADEV. It was for the latter that a remote access solution was set up during the internship.

From this work we have been able to observe the great interest in security presented by remote access solutions. We have especially noticed that remote access solutions are sufficiently secure and that the presence of weaknesses depends on the use that is made by the end users.

Keywords : Dial-up, VPN, modem, Public Switched Telephone Network, Internet, Micro Finance Institution, regulation, confidentiality, authentication, integrity, log file.

Avant-propos

Nous tenons à remercier tout particulièrement le professeur Laurent Schumacher, en sa qualité de promoteur, pour tout le suivi et l'aide qu'il nous a apportés, que ce soit lors du stage ou bien lors de la rédaction du mémoire.

Merci aussi à Michel Vanderheyden, pour nous avoir mis en contact avec AQUADEV et sans qui ce stage n'aurait pas eu lieu.

Nous remercions aussi tous les membres d'AQUADEV en Belgique et au Sénégal. Nous remercions en particulier Laurent Schyns, pour nous avoir encadré à distance et avec qui nous avons pu arranger la faisabilité du stage, Hassan Diallo, pour nous avoir encadré sur place et pour nous avoir intégré dans l'équipe de développement, dans laquelle se trouvaient Antoine Delvaux, Mouhamadou Diouf, et Papa Ndiaye et que nous souhaitons aussi remercier pour leurs formations et leur accueil.

Un grand merci aussi à Franck Goma pour son soutient et sa bonne humeur lors de notre séjour au Sénégal.

Finalement, nous souhaitons surtout remercier nos parents, nos frère et sœur, et notre compagne pour nous avoir soutenu tout au long de la durée du stage et de la rédaction du mémoire.

Table des Matières

Table des Figures

Table des Acronymes

3DES - Triple Data Encryption Standard
AAA - Authentication, Authorization, and Accounting
ADSL - Asymmetric Digital Subscriber Line
AES - Advanced Encryption Standard
AH - Authentication Header
ATM - Asynchronous Transfer Mode
CA - Certification Authorities
CEN - Comité Européen de Normalisation
CERT - Computer Emergency Response Team
CERT/CC - CERT Coordination Center
CPU - Central Processing Unit
CRC - Cyclic Redundancy Check
DNS - Domain Name System
EESSI - European Electronic Signature Standardization Initiative
ESP - Enterprise Service Provider
- Encapsulation Security Payload
GPL - General Public License
GRE - Generic Routing Encapsulation
HMAC - keyed-Hash Message Authentication Code
ICMP - Internet Control Message Protocol
IETF - Internet Engineering Task Force
IKE - Internet Key Exchange
IMF - Institution de Micro Finance
IP - Internet Protocol
IPCP - IP Control Protocol
IPsec - IP security
ISAKMP - Internet Security Association and Key Management Protocol
ISDN - Integrated Services Digital Network
ISO - International Standards Organization
ISP - Internet Service Provider
KDE - K Desktop Environment
L2F - Layer 2 Forwarding
L2TP - Layer 2 Tunnelling Protocol
L2TPv3 - Layer 2 Tunnelling Protocol version 3
LAN - Local Area Network
LCP - Link Control Protocol
MAN - Metropolitan Area Network
MD5 - Message-Digest algorithm 5
MITM - Man-In-The-Middle attack
MPLS - Multi-Protocol Label Switching
NAS - Network Access Server
NAT - Network Address Translation
NCP - Network Control Protocol
NSA - National Security Agency
ONG - Organisation Non Gouvernementale

OSI - Open Systems Interconnection
PAC - PPTP Access Concentrator
PAD - Packet Assembler and Disassembler
PDUs - Protocol Data Unit
PKI - Public Key Infrastructure
PNS - PPTP Network Server
PPP - Point-to-Point Protocol
PPTP - Point-to-Point Tunneling Protocol
PSTN - Public Switched Telephone Network
PVC - Permanent Virtual Circuit
QoS - Quality of Service
RAM - Random Access Memory
RAS - Remote Access Service
RC4 - nom de l'algorithme de chiffrement RC4
RDP - Remote Desktop Protocol
RFB - Remote Frame Buffer
RFC - Request For Comments
RPM - Red Hat Package Manager
RSA - Rivest Shamir Adleman
RTC - Réseau Téléphonique Commuté
SA - Security Association
SHA - Secure Hash Algorithm
SLA - Service Level Agreement
SLIP - Serial Line Internet Protocol
SMB - Server Message Block
S-MIME - Secure Multipurpose Internet Mail Extensions
SNMP - Simple Network Management Protocol
SPI - Security Parameter Index
SSH - Secure SHell
SSL - Secure Sockets Layer
SVC - Switched Virtual Circuit
SVPN - Secure Virtual Private Network
TCP - Transmission Control Protocol
TLS - Transport Layer Security
UDP - User Datagramme Protocol
VPN - Virtual Private Network
VPNC - Virtual Private Network Consortium
VPDN - Virtual Private *Dial-up* Network
WAN - Wide Area Network
WEP - Wired Equivalent Privacy
X11 - X Window System

Introduction

De nos jours, l'informatique se trouve partout. Les enfants sont baignés dans ce monde abstrait dès le plus jeune age tandis que beaucoup de personnes plus âgées se disent qu'elles feraient bien de s'y mettre. Que ce soit dans de grandes multinationales, dans des écoles ou chez les particuliers, les ordinateurs font désormais partie de notre vie quotidienne.

Au début, l'informatique était admirée pour la puissance de calcul qu'elle offrait et la masse de données qu'elle pouvait traiter. Par la suite, les avancées technologiques ont permis la miniaturisation des ordinateurs ce qui a ouvert la voie au développement de nouveaux outils tel que les logiciels de traitement de texte.

L'arrivée de l'informatique a poussé les gens à adopter un style de vie différent. Les règles à calcul étaient rangées dans le placard à profit de la calculatrice, les machines à écrire à profit des logiciels de traitement de texte. On pouvait maintenant faire des calculs à une vitesse incroyable et nous n'étions plus obligés d'utiliser du papier carbone pour dupliquer des documents. Evidemment, la venue d'Internet n'a fait qu'accroître l'attrait de l'informatique.

Mais l'informatique ne s'est pas limitée à cela. Lorsque l'accès à distance a vu le jour, il a annoncé l'arrivée d'une nouvelle forme d'organisation du travail : le télétravail. Grâce à l'accès à distance, nous pouvons travailler chez nous sans avoir à perdre du temps pour nous rendre à notre bureau. Par ailleurs, nous pouvons nous rendre chez davantage de clients en une journée et instantanément mettre à jour leurs profils chez la société mère. Nous pouvons accéder à des documents qui ne sont pas physiquement accessibles et nous pouvons même bénéficier de la puissance de calcul d'une machine distante plus performante que la nôtre. Il est même parfois possible de carrément prendre le contrôle de l'ordinateur distant ; un jeune internaute peut ainsi montrer à ses parents comment installer la dernière version d'un antivirus sans être à leurs côtés, des techniciens peuvent dépanner des systèmes informatiques sans se rendre sur place, etc.

Néanmoins, l'accès à distance a évolué conjointement avec les avancées technologiques, permettant de profiter de taux de transfert de plus en plus rapides et il peut également être établi sous diverses formes. De nos jours nous pouvons d'ailleurs trouver toute une série de solutions d'accès à distance, toutes différentes les unes des autres, avec différents degrés de sécurité et pratiquant différents prix. Cette disparité de solutions nous a donc poussé à les comparer sur base de différents critères. Une telle comparaison permet de constater les différentes fonctionnalités qui sont offertes selon le type de solution d'accès à distance qui est choisie.

C'est ce genre de comparaison que nous avons fait pendant les quatre mois de stage de fin d'études que nous avons effectué dans une ONG située à Dakar, Sénégal. Cette ONG, du nom d'AQUADEV souhaitait disposer d'une solution d'accès à distance pour être en mesure de maintenir à distance un logiciel de micro finance qu'elle avait développé. Nous avons donc dû nous renseigner sur les différentes solutions d'accès à distance qui existaient pour en choisir la meilleure.

Cependant, avant de pouvoir évaluer ces différentes solutions d'accès à distance, il faut d'abord comprendre comment celles-ci fonctionnent. Le premier chapitre présentera donc une étude des différents moyens par lesquels peut être établi un accès à distance.

Une fois les principes et mécanismes de base couverts, nous pourrons ensuite examiner comment ils sont utilisés dans quelques solutions d'accès à distance actuellement disponibles sur le marché. Nous énumérerons les différentes caractéristiques de ces solutions.

Ensuite nous ferons une analyse des normes et législations qui s'appliquent à l'accès à distance, directement ou indirectement. Ceci se fera dans un souci de mieux comprendre les enjeux qui sont présents lorsque nous nous trouvons sur un réseau tel qu'Internet.

Le chapitre qui suit l'analyse des normes est lié au stage effectué au premier semestre de cette année. Lors de ce chapitre, nous décrirons la solution d'accès à distance que nous avons mis au point lors du stage.

Finalement, nous enchaînerons avec un recensement des lacunes que nous avons perçues ainsi quelques solutions que nous y avons proposées. Ensuite nous terminerons avec une vue sur les perspectives futures de l'accès à distance.

Chapitre 1 : Etablissement d'un accès à distance

Depuis l'arrivée de l'accès à distance, toute une série de moyens technologiques ont pu être développés au fil du temps pour permettre aux utilisateurs de systèmes informatiques de pouvoir profiter de ce genre de fonctionnalité. L'objectif de ce chapitre est d'acquérir une compréhension plus complète du fonctionnement des solutions d'accès à distance. Pour ainsi faire, nous proposons donc d'analyser les moyens d'accès à distance les plus répandus ainsi que de passer en revue les principaux protocoles qui y sont utilisés. De ceci on pourra retenir les différentes fonctionnalités et la sécurité qui sont offertes par une solution selon le moyen d'accès à distance qui y est utilisé.

1.1 Dial-up

L'accès à distance via *Dial-up* est certainement le moyen d'accès à distance le plus ancien. A l'origine, le *Dial-up* consistait en l'établissement d'un accès à distance par l'intermédiaire du RTC (Réseau Téléphonique Commuté), ou PSTN (Public Switched Telephone Network) en anglais.

Dans le cas de deux ordinateurs par exemple, il suffisait que chaque ordinateur soit branché à un câble téléphonique pour que l'un puisse "appeler" l'autre, et ainsi créer une connexion logique entre les deux, en composant le numéro attribué à la ligne téléphonique du second ordinateur.

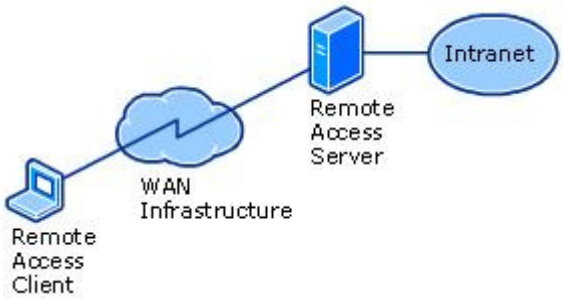


Fig. 1.1 – Les composants d'un accès à distance par *Dial-up* [MIC Dial-up]

De façon simplifiée, dans le cas d'entreprises qui veulent fournir un accès à distance à leurs employés il existe quatre composants (cfr. figure 1.1) : l'employé, un serveur d'accès distant, le RTC, sans oublier le réseau interne de l'entreprise [MIC Dial-up]. De la même façon que dans le scénario d'un *Dial-up* entre deux ordinateurs, l'employé travaillant à distance utilise son ordinateur portable, par exemple pour se connecter au serveur d'accès distant de son entreprise, en numérotant un numéro de téléphone propre au serveur d'accès à distance de l'entreprise. Par la suite, c'est le serveur d'accès à distance qui fera suivre les informations entre l'employé distant et le réseau interne de l'entreprise [MIC Dial-up].

Les performances que l'on pourrait observer sur un tel type d'accès à distance dépendent notamment de l'infrastructure de télécommunications se trouvant entre l'ordinateur

de l'employé et le serveur d'accès distant. Cette infrastructure peut être soit le PSTN, l'ISDN (Integrated Services Digital Network), X.25, ou bien l'ATM (Asynchronous Transfer Mode) par-dessus de l'ADSL (Asymmetric Digital Suscriber Line) [MIC Dial-up].

1.1.1 Dial-up par PSTN

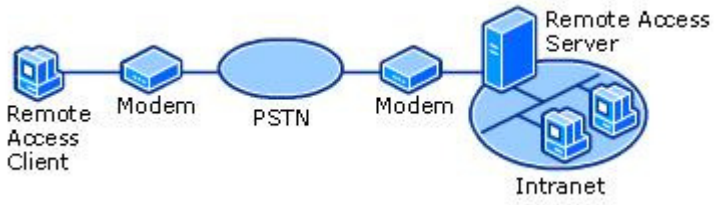


Fig. 1.2 – Une connexion d'accès à distance à travers le PSTN [MIC Dial-up]

L'infrastructure PSTN est celle qui fournit les services de téléphonie analogique et est l'infrastructure dont l'usage est le plus répandu en ce qui concerne l'établissement d'accès à distance [MIC Dial-up].

Comme nous pouvons le constater à la figure 1.2, pour cette infrastructure il est nécessaire de mettre en place un modem analogique du côté de l'employé et au moins un[1] du côté de l'entreprise [MIC Dial-up]. Plus précisément, du côté de l'employé, l'ordinateur est branché au modem analogique qui lui est connecté au PSTN. Du côté de l'entreprise, le ou les modems sont connectés au PSTN d'un côté et sont reliés au serveur d'accès distant de l'autre. Evidemment, plus l'entreprise a de modems analogiques, plus elle pourra avoir d'employés connectés à distance simultanément.

Vu que le PSTN a été conçu afin de transporter les fréquences minimales requises pour différencier les voix humaines, le taux de transfert de données atteint un seuil maximal de 33,6 Kbps. Néanmoins, lorsque la technologie V.90 est arrivée, elle permit à l'employé de pouvoir atteindre un taux de réception de données maximal de 56 Kbps tout en gardant son taux d'envoi de données maximal à 33,6 Kbps. [MIC Dial-up]

1.1.2 Dial-up par ISDN

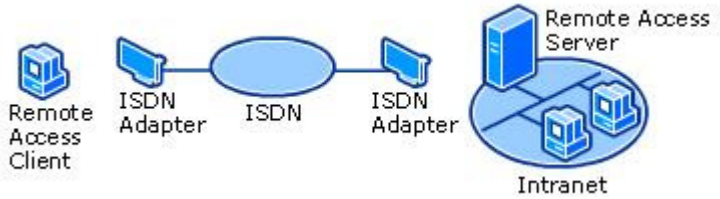


Fig. 1.3 – Une connexion d'accès à distance à travers l'ISDN [MIC Dial-up]

Par la suite est arrivé l'ISDN[2], un ensemble de spécifications internationales, qui consistait en un seul réseau digital permettant de gérer la voix, les données, le fax, ainsi que d'autres services, entre plusieurs entités [MIC Dial-up].

[1] Des grandes entreprises pourraient avoir des centaines de modems [MIC Dial-up].
[2] L'ISDN coexiste actuellement avec le PSTN.

En se référant à la figure 1.3, nous voyons qu'une connexion d'accès à distance est déployée à peu près de la même façon, que nous nous trouvions sur une infrastructure PSTN ou ISDN. D'ailleurs, cette dernière fonctionne de la même façon que les lignes téléphoniques analogiques mais de manière numérique, ce qui permet d'avoir des taux de transferts plus élevés ainsi qu'un temps de connexion beaucoup plus court [MIC Dial-up].

D'un point de vue matériel, c'est un modem ISDN[3] ou adaptateur ISDN qui sert d'intermédiaire entre l'ordinateur de l'employé et l'infrastructure ISDN, mais le scénario de connexion reste à peu près le même que dans le cas d'une infrastructure PSTN.

1.1.3 Dial-up par X.25

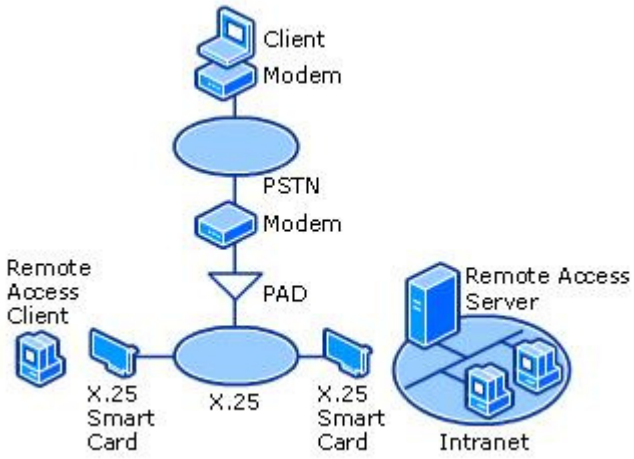


Fig. 1.4 – Une connexion d'accès à distance à travers X.25 et PSTN [MIC Dial-up]

X.25[4] est un standard international pour l'envoi de données à travers des réseaux publics de commutation de paquets [MIC Dial-up].

La figure 1.4 présente un exemple de connexion d'accès à distance via X.25 et PSTN. Pour prendre comme exemple le cas de Windows Server 2003, des *smart cards* X.25 sont utilisées du côté de l'employé. Elles permettent de se connecter directement au réseau de données X.25 et d'utiliser le protocole X.25 afin d'établir les connexions, ainsi que d'envoyer et de recevoir les données [MIC Dial-up].

Un employé se trouvant sur une infrastructure PSTN peut se connecter à l'infrastructure X.25 par l'intermédiaire d'un PAD (Packet Assembler and Disassembler) tandis qu'un serveur d'accès distant ne peut se connecter directement qu'à l'infrastructure X.25 en utilisant une *smart card* X.25 [MIC Dial-up].

[3] A ne pas confondre avec le modem analogique puisque le modem ISDN fonctionne de manière numérique.
[4] Egalement appelé *packet switched network* [wiki X.25].

1.1.4 Dial-up par ATM sur ADSL

Fig. 1.5 – Une connexion d'accès à distance par ATM sur ADSL [MIC Dial-up]

ATM est une technologie de commutation de paquets basé sur des cellules de taille fixe [MIC Dial-up]. Les données sont échangées à travers un réseau ATM sur lequel il est possible d'établir des connexions PPP au dessus de connexions ATM SVC (Switched Virtual Circuit) ou ATM PVC (Permanent Virtual Circuit) [MIC Dial-up].

On remarque à la figure 1.5 qu'afin de pouvoir établir ces connexions PPP, des adaptateurs ATM sont nécessaires pour établir une connexion physique au réseau ATM, mais une fois installés, ces adaptateurs apparaissent comme étant des dispositifs *Dial-up* [MIC Dial-up]. En ce qui concerne les boucles locales[5], l'ADSL est une technologie fort répandue [MIC Dial-up].

Lorsque les adaptateurs ADSL apparaissent comme des dispositifs *Dial-up*, l'ADSL fournit une connexion physique entre l'employé et le serveur d'accès distant et les paquets sont échangés entre eux par l'utilisation du protocole ATM [MIC Dial-up]. Pour ainsi faire, il faut installer des adaptateurs ATM avec un port ADSL du côté de l'employé distant et de l'entreprise [MIC Dial-up].

1.2 Différents moyens d'accès à distance par Dial-up

Nous venons de voir que le *Dial-up* pouvait être effectué à travers plusieurs infrastructures intermédiaires. Maintenant nous allons voir, à un niveau plus général, les différents moyens d'établir un accès à distance par *Dial-up*, parmi lesquels nous trouvons la connectivité *LAN-to-LAN*, l'accès par ISP, et finalement l'accès d'utilisateurs distants [CW DU]. Ensuite, à un niveau plus spécifique, nous verrons les différents protocoles qui peuvent être utilisés pour établir un *Dial-up*.

1.2.1 LAN-to-LAN

Par accès à distance *LAN-to-LAN*, nous entendons une connexion *Dial-up* entre deux réseaux ; c'est le cas, par exemple, de bureaux distants qui se connectent au réseau interne du bureau central [CW DU].

Lorsqu'une connexion est établie entre deux réseaux, un routage convenable est nécessaire afin de pouvoir accéder à des ressources se trouvant sur un réseau tout en se trouvant dans un autre. Ainsi, lorsqu'un utilisateur veut avoir accès à une ressource se trouvant sur un réseau distant, le serveur d'accès distant identifie ce besoin et va automatiquement se

[5] La boucle locale ou *local loop* en anglais, fait référence au lien ou circuit physique entre le client et le réseau du fournisseur de services de télécommunications [wiki LL].

connecter au réseau distant approprié. Une fois la connexion établie, le serveur d'accès distant surveillera la connexion selon des paramètres de contrôle qui auront été fixés par l'administrateur réseau de l'entreprise. [CW DU]

Parmi ces paramètres de contrôle, les plus courants sont un mécanisme de déconnexion automatique après une période de *time-out* et un mécanisme qui empêche certaines connexions pendant certaines heures de la journée. Cette possibilité de connexion automatique facilite la tâche de l'administrateur réseau et permet que l'accès aux ressources distantes soit transparent pour les utilisateurs. [CW DU]

1.2.2 ISP

Le même genre de solution peut être adoptée entre un bureau et un fournisseur d'accès Internet, ou ISP (Internet Service Provider). Ainsi les serveurs d'accès distant agissent de la même façon que dans le cas d'accès distant *LAN-to-LAN*, mais en se connectant à l'ISP cette fois-ci, tout en offrant les mêmes paramètres de contrôle selon un temps d'inactivité ou selon l'heure de la journée. Certains serveurs d'accès distant peuvent même faire office de pare-feu entre le réseau interne de l'entreprise et l'ISP. [CW DU]

De plus en plus d'entreprises utilisent également l'Internet afin d'étendre leur réseau interne pour en faire un intranet qui sera accessible par l'intermédiaire de simples navigateurs Internet[6]. De cette manière, l'entreprise peut se passer de l'investissement en des serveurs d'accès distant, ainsi que la maintenance qui en découle, et il suffit aux utilisateurs de se connecter à l'ISP le plus proche, permettant ainsi de contrôler les coûts. [CW DU]

1.2.3 Utilisateurs Distants

En fonction de la nature des activités d'une entreprise, il se peut qu'elle ait des employés qui soient fréquemment en déplacement et qui aient également besoin d'avoir accès au réseau interne de l'entreprise.

Cet accès distant au réseau interne de l'entreprise peut se faire grâce à un modem et un logiciel d'accès à distance installé sur l'ordinateur des employés "mobiles", leur donnant accès au réseau interne par l'intermédiaire d'un serveur *Dial-up*. Evidemment, ce genre de scénario fonctionne le mieux lorsque l'utilisateur distant fait des requêtes brèves ou travaille sur des données qu'il aurait téléchargées ; par exemple, un utilisateur qui consulte son courrier électronique ou qui travaille sur un fichier texte ou Excel qu'il aurait téléchargé. [CW DU]

Une autre option est le contrôle à distance. A ce moment là, l'utilisateur distant prend le contrôle d'un ordinateur, sur le réseau interne de l'entreprise, et il pourra agir comme si il se trouvait derrière l'ordinateur interne. Ceci a l'avantage que les calculs et les traitements d'informations s'effectuent directement sur l'ordinateur du réseau interne [CW DU]. De ce fait, les utilisateurs distants évitent de devoir à chaque fois rapatrier de gros fichiers sur leur ordinateur et les renvoyer de retour à l'ordinateur du réseau interne vu que désormais il n'y a plus que les mouvements de souris ou les entrées de clavier qui sont transmis de l'ordinateur distant à l'ordinateur du réseau interne.

[6] Nous pouvons penser, par exemple, à Microsoft Internet Explorer, Netscape Navigator, Mozilla Firefox, etc.

1.2.4 Protocoles d'accès à distance par Dial-up

Depuis que le principe de *Dial-up* a été établi, plusieurs protocoles différents ont été développés pour permettre le fonctionnement de ce mécanisme. Néanmoins, lorsque de nouveaux protocoles, avec de meilleures performances, apparaissaient, en général leur usage se répandait assez rapidement en laissant à l'abandon les protocoles qui étaient utilisés précédemment. Par conséquent, nous n'allons pas nous encombrer d'une révision de tous les protocoles possibles et imaginables pour le *Dial-up*, mais nous nous limiterons aux plus répandus, à savoir PPP et SLIP.

1.3 Dial-up basé sur PPP

Comme son nom l'indique, PPP, ou Point-to-Point Protocol, est un protocole de la couche liaison fonctionnant sur une liaison *point-to-point* ; c'est-à-dire une liaison connectant directement deux hôtes, un hôte se trouvant de chaque côté de la liaison [Kurose et Ross]. C'est à travers cette liaison que le protocole PPP permet le transport de datagrammes multi protocolaires [RFC 1661]. PPP est maintenant le protocole le plus utilisé lors de l'établissement de liaisons *Dial-up*.

1.3.1 Fonctionnement du protocole PPP

PPP a été conçu pour fournir une solution commune pour des connexions faciles entre une grande variété d'hôtes. Le transport de paquets se fait entre deux hôtes à travers des liaisons simples, *full-duplex*[7], qui sont supposées livrer les paquets dans l'ordre [RFC 1661]. A l'origine l'IETF avait défini certaines exigences pour la conception du protocole PPP ; nous allons les passer en revue. [Kurose et Ross]

Vu que nous nous trouvons à la couche liaison, nous avons affaire à des trames, ou *frames* en anglais, lorsqu'on parle de l'envoi et la réception d'informations. Ainsi, lorsqu'un paquet de la couche réseau doit être envoyé, il doit être encapsulé dans une trame de la couche liaison avant d'être transmise à la couche physique. En anglais, ce procédé est nommé *packet framing* ou *framing*. Evidemment, lorsque l'hôte émetteur encapsule un paquet de la couche réseau, il doit le faire de telle manière que l'hôte destinataire puisse aussi bien identifier le début et la fin de la trame que le début et la fin du paquet se trouvant dans la trame. [Kurose et Ross]

Le protocole PPP doit également être transparent, c'est-à-dire qu'il ne peut pas imposer des contraintes sur le format des paquets de la couche réseau. En d'autres termes, PPP ne peut pas par exemple interdire l'usage de certaines suites de bits dans le *header* ou le champ de données du paquet de la couche réseau. Le protocole PPP doit également être capable de supporter l'envoi de plusieurs protocoles différents à travers la même liaison physique en même temps. A ceci s'ajoute le fait que PPP doit être en mesure de fonctionner par-dessus une grande variété de liaisons tel que des liaisons en série ou parallèles, synchrones ou asynchrones, de haute vitesse ou de basse vitesse, électriques ou optiques. [Kurose et Ross]

[7] C'est-à-dire que les entités, entre lesquelles est établie le lien, peuvent envoyer et recevoir des données simultanément [Kurose et Ross].

Pour ce qui est de la découverte des problèmes, le récepteur PPP doit être capable de détecter des erreurs de bits dans la trame reçue ainsi que de détecter et de signaler un mauvais fonctionnement au niveau de la couche liaison. Finalement, le protocole PPP doit également être en mesure de fournir un mécanisme de négociation d'adresses IP entre les couches réseau des deux hôtes en communication. [Kurose et Ross]

En faisant la liste des exigences que devait rencontrer le protocole PPP, l'IETF a également précisé des fonctionnalités supplémentaires mais qui ne sont pas requises ; à savoir la correction d'erreurs, le contrôle de flux, le séquençage, ainsi que la possibilité d'établir des liaisons multipoint [Kurose et Ross]. De par ces exigences, nous pouvons découper le protocole PPP en trois composants, à savoir l'encapsulation, le LCP (Link Control Protocol), et des NCP (Network Control Protocol) [RFC 1661].

1.3.2 Format des trames PPP

Afin de mieux comprendre l'encapsulation, jetons un coup d'œil sur le format des trames de données PPP.

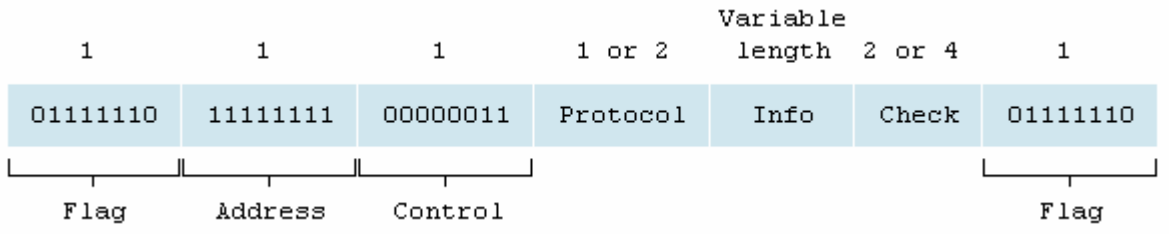


Fig. 1.6 – Trame PPP [Kurose et Ross]

Comme nous pouvons le constater à la figure 1.6, chaque trame PPP commence et se termine avec un champ *flag* d'un octet ayant pour valeur 01111110. Après le champ *flag* de début se trouve un champ adresse, dont la seule valeur possible est 11111111, ainsi qu'un champ de contrôle dont la seule valeur possible est 00000011[8]. Vu l'inutilité de deux champs ayant une valeur fixe, PPP permet que l'hôte émetteur n'envoie pas les octets de ces champs, évitant ainsi de "gaspiller" deux octets par trame envoyée. Le quatrième champ est un champ de protocole, ce qui permet au récepteur PPP de savoir à quel protocole appartiennent les données encapsulées dans la trame. Ensuite se trouve le champ de données proprement dit, contenant le paquet encapsulé, avec une taille maximale par défaut de 1.500 octets[9]. Après ce champ se trouve le champ checksum qui sert à détecter les erreurs de bit dans la trame envoyée en utilisant un CRC (Cyclic Redundancy Check) de deux ou quatre octets. [Kurose et Ross]

C'est avec une telle encapsulation que PPP permet le multiplexage[10] simultané de différents protocoles de la couche réseau comme exigé par l'IETF [RFC 1661].

[8] Ces deux champs n'ont qu'une valeur possible parce que le RFC 1662 proposait ces valeurs arbitraires en disant que d'autres valeurs pouvaient être définies plus tard. Depuis lors, aucune autre valeur n'a été définie donc les valeurs proposées initialement sont devenues les seules valeurs possibles. [Kurose et Ross]

[9] Néanmoins cette taille maximale peut être négociée lors de la première configuration de la liaison [Kurose et Ross].

[10] C'est-à-dire le fait de regrouper différentes données en un segment pour remplacer plusieurs envois d'informations entre deux hôtes par un seul envoi [Kurose et Ross].

1.3.3 Link Control Protocol

A l'encapsulation s'ajoute le LCP, ou Link Control Protocol, qui est fourni par PPP afin que ce dernier puisse être portable à plusieurs environnements [RFC 1661].

Les buts de LCP sont l'initialisation, la maintenance, la signalisation d'erreur et la terminaison des liaisons PPP [Kurose et Ross]. LCP est également utilisé pour choisir de façon automatique les options de format d'encapsulation, les tailles maximales des trames, et la détection d'erreurs de configuration. Avant qu'une communication par PPP puisse être établie entre les deux hôtes, la liaison de données doit d'abord être configurée et testée par l'envoi de paquets LCP [RFC 1661]. Tout comme pour les protocoles de la couche réseau, les paquets LCP sont encapsulés dans des trames PPP avant d'être envoyés à l'hôte destinataire [Kurose et Ross].

D'autres fonctionnalités optionnelles fournies par LCP sont l'authentification de l'identité des entités liées ainsi qu'un diagnostic du bon fonctionnement de la liaison PPP [RFC 1661].

1.3.4 Network Control Protocol

Finalement, nous avons une famille de NCPs, ou Network Control Protocols, c'est-à-dire des protocoles de contrôle de réseau.

Si l'allocation et la gestion des adresses IP sont déjà problématiques dans des LAN, elles le sont plus encore lorsqu'il s'agit de liaisons *point-to-point* par commutation de circuits. Les problèmes dans ce genre sont contrôlés par le protocole NCP correspondant, ce qui permet de gérer les besoins des différents protocoles de la couche réseau. [RFC 1661]

Dans le cas de la transmission de paquets IP par-dessus la liaison PPP, le IPCP (IP Control Protocol) est utilisé afin de configurer les modules IP de chaque côté de la liaison. Ainsi, les deux modules IP pourront par exemple échanger ou configurer leurs adresses IP et négocier si oui ou non les paquets IP seront envoyés sous forme compressée. [Kurose et Ross]

1.4 Dial-up basé sur SLIP

A son époque, SLIP, ou Serial Line Internet Protocol, était le standard de facto pour les connexions série *point-to-point* définissant ainsi la manière d'encapsuler des paquets IP pour la transmission sur des lignes série. Néanmoins, il faut remarquer qu'il n'y avait pas de spécifications standard pour l'implémentation de SLIP. [RFC 1055]

SLIP est un standard d'accès à distance plus ancien que PPP[11] et qui est typiquement utilisé par des serveurs d'accès distant UNIX [MIC Dial-up]. Par ce fait, SLIP présente plusieurs lacunes par rapport à PPP. Par exemple, SLIP n'offre pas de détection d'erreur, fonctionnalité qui est offerte par PPP, et SLIP offre des niveaux de sécurité et de compression de données moindres que ce qui est offert par PPP. Vu la plus grande efficacité qui est offerte

[11] A titre de comparaison, nous pouvons remarquer que le premier RFC concernant SLIP est apparu en 1988 alors que le premier RFC concernant PPP est apparu en 1990! [RFC editor]

par l'utilisation de PPP au lieu de SLIP, ce premier a été préféré à SLIP au fil du temps. [MH PPP]

1.4.1 Fonctionnement du protocole SLIP

Lors de la transmission d'un paquet, l'hôte émetteur commence simplement à envoyer les données du paquet, et lorsqu'il arrive à la fin du paquet, il émet un caractère spécial END ; dans le cas où un octet de données a la même valeur que le caractère END, un autre caractère spécial ESC et une valeur octale de 334 sont envoyés en lieu et place. [RFC 1055]

Vu le manque de spécifications pour le protocole SLIP, aucune taille maximale de paquet n'était définie. Néanmoins, dans le RFC 1055, l'IETF propose d'adopter la taille maximale de paquet utilisée par les pilotes SLIP de la version UNIX de Berkeley, à savoir 1006 octets, n'incluant pas les caractères d'encapsulation. [RFC 1055]

1.4.2 Lacunes du protocole SLIP

Si le protocole SLIP a l'avantage d'être plus facile à implémenter et utiliser que PPP, il a le désavantage de ne pas offrir une série de fonctionnalités. Tout d'abord, SLIP n'offre aucun mécanisme d'adressage, c'est-à-dire que les hôtes sur une liaison SLIP n'ont pas de moyen pour communiquer leurs informations d'adressage. De plus, SLIP n'offre aucune identification de type de paquets, c'est-à-dire qu'aucun champ de protocole n'est utilisé. Par ce fait, un seul protocole peut être utilisé par-dessus une même ligne série utilisant SLIP[12]. [RFC 1055]

Il manque également à SLIP un mécanisme de détection et de correction d'erreurs. Vu que n'importe quelle application devrait être en mesure de détecter des paquets corrompus, la détection au niveau SLIP n'est pas absolument nécessaire. Par contre, à l'époque nous nous trouvions généralement sur une ligne ayant une bande passante assez faible, ce qui veut dire que la retransmission d'un paquet, qui aurait été endommagé, était assez coûteuse. C'est afin d'éviter ces coûteuses retransmissions qu'il aurait été utile d'incorporer un mécanisme simple de correction d'erreurs dans le protocole SLIP, ce qui l'aurait rendu plus efficace. [RFC 1055]

Vu la faible bande passante qui était régulièrement rencontrée, il aurait également été utile d'incorporer un mécanisme de compression des données, ce qui aurait pu concerner au premier chef les *headers* des paquets de la couche réseau. En effet, en général lors d'une suite de paquets IP par exemple, le contenu des *headers* change très peu ; nous aurions donc pu n'envoyer que les changements du contenu des *headers* suite à l'envoi du premier paquet IP "complet"[13] [RFC 1055]. Ceci aurait été plus facile à implémenter par le fait que de toute façon nous étions limités à un protocole de la couche réseau par liaison SLIP.

1.5 VPN

Un VPN, ou Virtual Private Network, est, comme son nom l'indique, un réseau privé virtuel. Un VPN est privé car il appartient à une entreprise et n'est, en principe, utilisable et utilisé que par l'entreprise ainsi que ses employés[14]. Un VPN est virtuel car c'est un ensemble

[12] Le multiplexage qu'offre PPP ne peut donc pas être offert par ce protocole.
[13] Plus d'informations sur la compression des *headers* TCP/IP peuvent être obtenus dans le RFC 1144.
[14] Néanmoins, un VPN est déployé sur une infrastructure publique [VPN Consortium].

de sous réseaux d'une entreprise qui ne sont pas connectés directement, se trouvant parfois dans plusieurs pays différents, que l'on fait paraître comme n'étant qu'un seul réseau.

Une définition plus légitime et complète d'un VPN est donnée par le VPN Consortium qui dicte que "A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures" [VPN Consortium].

1.5.1 Fonctionnement général

Auparavant les entreprises qui voulaient établir un réseau étendu, ou *Wide Area Network*[15] (WAN), le faisaient par l'intermédiaire de lignes dédiées[16] (*leased lines* en anglais). Un WAN construit sur des lignes dédiées garantissait certes une plus grande fiabilité, performance, et sécurité que le réseau public, mais ça coûtait également très cher et les coûts augmentaient proportionnellement à la distance entre les différents sous réseaux interconnectés [HSW VPN]. Depuis, bon nombre d'entreprises se sont tournées vers l'Internet et les VPNs pour réduire les coûts de construction et de maintien des WAN sur lignes dédiées [VPN Consortium].

Le flux de données d'un VPN est transmis soit à travers les infrastructures réseau publiques, par exemple Internet, en utilisant des protocoles standards, soit à travers le réseau d'un fournisseur d'accès qui fournit un service VPN protégé par un *Service Level Agreement* (SLA) entre le client VPN et le fournisseur du service VPN [wiki VPN en]. On distingue généralement le réseau interne, qui fourni un certain niveau de sécurité physique et administratif en ce qui concerne la protection des transmissions de données, et le réseau externe, qui est considéré comme étant peu sûr ; l'Internet est le plus grand de ces réseaux externes non fiables [wiki VPN en]. Avec l'Internet, un tel réseau peut dès lors s'étendre à tous les coins du monde puisqu'il permettrait aux employés d'une entreprise de pouvoir se connecter au VPN de leur entreprise à partir de n'importe où. En effet, un tel employé se trouvant "à l'extérieur" du VPN de son entreprise pourrait utiliser l'Internet afin d'établir une connexion sécurisée au VPN comme si il faisait partie intégrante du réseau interne.

1.5.2 Composants requis par les VPNs

Différents composants sont requis pour établir un VPN de façon efficace dépendant de la catégorie du VPN qui doit être établi. Par exemple, lorsqu'on sous-traite le VPN à un ESP (Enterprise Service Provider), nous pouvons trouver comme composants, des logiciels d'accès à distance pour les utilisateurs distants, du matériel dédié tel un concentrateur VPN ou un pare-feu PIX, des serveurs VPN dédiés pour des services Dial-up, et des NAS (Network Access Server) [HSW VPN].

---

[15] Les différents types de réseaux sont classés en trois catégories selon les distances entre différentes entités du réseau. Lorsque la distance concernée est de quelques mètres (et ne dépassant pas cent mètres), nous avons affaire à un réseau local ou LAN (Local Area Network) et on utilise en général des connexions Ethernet sur câbles de paires torsadées. Lorsque la distance dépasse cent mètres et atteint quelques kilomètres, nous parlons de réseaux métropolitains ou MAN (Metropolitan Area Network) et on utilise en général des connexions de type fibre optique. Une fois que la distance est plus grande que quelques kilomètres, nous parlons de réseaux étendus ou WAN (Wide Area Network) et on utilise en général les services offerts par un transporteur (*carrier* en anglais) tel Belgacom, France Télécom, etc. [wiki WAN fr]

[16] Les lignes dédiées variaient en général entre des lignes de type ISDN (Integrated Services Digital Network) avec un débit de 128 Kbps et des lignes de fibre optique de type OC3 (Optical Carrier-3) avec un taux de transfert de 155 Mbps [HSW VPN].

1.5.3 Sécurité

La sécurité des VPNs se base sur plusieurs moyens pour protéger les connexions ainsi que les données qui y transitent. Ceci concerne notamment les pare-feu, l'encryption, et le protocole sur lequel sont établis les VPNs [HSW VPN].

De nos jours, avec toutes les menaces et dangers informatiques qui se propagent nous trouvons des pare-feu presque partout, dans des entreprises aussi bien que dans les domiciles d'individus. Les pare-feu sont le plus souvent connus sous la forme de logiciel, mais il existe également des pare-feu matériels. Tous deux exécutent la même fonction, contrôler le trafic entre deux zones de confiance ; par exemple entre l'Internet (une zone de non confiance) et le LAN d'un domicile (une zone de haute confiance) [wiki Firewall]. Un pare-feu peut ainsi protéger le réseau interne que forme un VPN (zone de haute confiance) des insécurités liées aux communications avec l'extérieur de ce réseau interne (zone de non confiance). Dans le cas où des employés distants veulent se connecter au VPN de leur entreprise, il faut tout de même être en mesure de protéger le réseau interne d'une intrusion non autorisée. En effet, vu qu'un VPN ne profite pas du haut niveau de sécurité offert par des lignes dédiées, il faut faire particulièrement attention à certains aspects de sécurité, notamment aux failles de sécurité qui se trouvent le plus souvent du côté client (c'est-à-dire du côté de l'employé distant).

Afin d'assurer cette protection, les employés se connectant au réseau distant doivent transmettre des données d'authentification au pare-feu qui retransmet ces informations à un service d'authentification se trouvant sur le réseau interne. Beaucoup de clients VPN peuvent être configurés pour requérir que tout trafic IP passe par le tunnel tant que la connexion au VPN est encore active, ce qui permet de protéger tout accès provenant de l'extérieur du VPN[17] par le même pare-feu que si l'employé se trouvait physiquement à l'intérieur du réseau interne. Ainsi une personne malveillante, ou bien un concurrent de l'entreprise de l'employé, ne pourrait pas s'introduire à l'intérieur du VPN en attaquant l'ordinateur de l'employé distant et se faire passer pour se dernier [wiki VPN en]. Il est d'ailleurs assez fréquent que des entreprises imposent l'installation d'un pare-feu "hardware" aux employés qui souhaitent accéder au VPN à partir de leur domicile [wiki VPN en].

Au niveau des données échangées, qui transitent à travers la zone de non confiance qu'est l'Internet, il faut également s'assurer que leur contenu ne puisse être récupéré par une tierce partie. Afin d'assurer cette protection des données, il est possible de recourir à un système d'encryption. Plusieurs méthodes d'encryption existent, mais les plus répandues sont celles de l'encryption à clés symétriques et asymétriques (ou à clés publiques) [HSW VPN]. Dans le cas d'employés distants qui veulent se connecter au VPN de leur entreprise, une connexion sécurisée peut être réalisée en utilisant un protocole de "tunnelisation" (*tunneling* en anglais), tel le *port forwarding*, qui établira un véritable "tunnel" virtuel entre un employé distant et le VPN qui permettra de protéger les données échangées en encapsulant les données de façon chiffrée [wiki VPN fr]. Ainsi, même si une personne arrivait à récupérer des informations qui transitent entre les deux entités, ces données ne lui seraient d'aucune utilité puisqu'elles seraient incompréhensibles par le fait qu'elles sont chiffrées.

En ce qui concerne les protocoles utilisés pour établir un VPN, il existe IPsec et SSL/TLS. IPsec est un ensemble de protocoles qui fournit une certaine sécurité au niveau de la couche réseau du modèle OSI [Kurose et Ross]. IPsec fonctionne soit en mode tunnel (le

[17] On pense par exemple à un employé qui accède au VPN de son entreprise à partir de son domicile.

header et le *payload* de chaque paquet est encrypté) soit en mode transport (seul le *payload* est encrypté) [HSW VPN]. Le protocole SSL/TLS est un protocole offrant une protection au niveau de la couche transport du modèle OSI. SSL/TLS peut également être utilisé pour protéger les données transmises entre deux entités.

1.6 Différents types de VPN : niveau fonctionnel

Une entreprise pourrait ressentir le besoin d'avoir un VPN pour plusieurs raisons mais en général il existe un certain nombre de différents types de VPN. Ces différents VPNs peuvent être classés selon leur aspect fonctionnel ou technique.

En utilisant une classification fonctionnelle, nous trouvons généralement deux catégories de VPN. Il s'agit notamment de VPNs *site-to-site* ou bien des VPNs d'accès à distance. Ces types de VPN sont repris à la figure 1.7 ci-dessous.

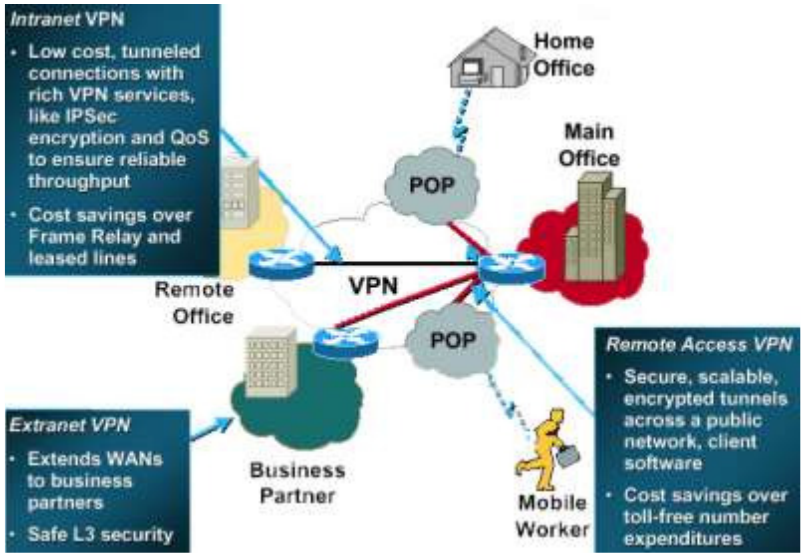


Fig. 1.7 – Les différents types de VPN [HSW VPN]

1.6.1 VPN site-to-site

Comme nous pouvons le constater à la figure 1.7 ci-dessus, parmi les VPNs *site-to-site*, certains sont basés sur un Intranet alors que d'autres sont basés sur un Extranet.

Les VPNs *site-to-site* basés sur un Intranet permettent à une entreprise de mettre en contact ses différents bureaux en interconnectant leurs LANs ensemble pour créer l'illusion de n'avoir qu'un seul WAN [HSW VPN]. Lorsqu'une entreprise a une relation de partenariat, fournisseur, ou client avec une autre entreprise, elle peut recourir à la catégorie de VPN *site-to-site* basé sur un Extranet qui permet, tout comme le VPN basé sur un intranet, d'interconnecter leurs LANs afin de pouvoir collaborer ensemble dans un environnement partagé [HSW VPN].

1.6.2 VPN d'accès à distance

En observant la figure 1.7, nous remarquons qu'il existe aussi des VPNs d'accès à distance, que l'on appelle également VPDN (Virtual Private *Dial-up* Network).

Cette catégorie de VPN permet aux employés d'une entreprise de se connecter au réseau local ou LAN (Local Area Network) de l'entreprise à partir de n'importe quel endroit en composant un numéro de téléphone gratuit [HSW VPN]. En général, lorsqu'une entreprise souhaite avoir un VPDN de grande envergure, elle le sous-traitera à un ESP [HSW VPN].

1.7 Différents types de VPN : niveau technique

Comme nous l'avons précisé à la section précédente, il existe différents types de VPN et ceux-ci peuvent être classés selon leur aspect fonctionnel ou technique.

En utilisant une classification plutôt technique, nous avons généralement la possibilité de choisir entre trois types de VPN. Ces VPNs peuvent être soit un VPN de confiance (*trusted VPN*), soit un VPN sécurisé (*secure VPN*), soit un VPN hybride (*hybrid VPN*) [VPN Consortium]. En général, les VPNs *site-to-site* peuvent être de confiance, sécurisés, ou hybrides, tandis que les VPNs d'accès à distance sont toujours de type sécurisé.

1.7.1 VPN de confiance

Avant l'arrivée d'Internet, il n'y avait que des VPNs de confiance ou *trusted VPN*[18]. Ceux-ci consistent en un ou plusieurs circuits, appartenant à des fournisseurs de communications, mais qui sont dédiés à des entreprises clientes. Si ce moyen d'établir un VPN s'avère assez cher, en revanche, le fournisseur de communications garantit que personne d'autre n'aura accès aux circuits dédiés d'une entreprise et celle-ci peut avoir son propre adressage IP ainsi que ses propres politiques de sécurité. [VPN Consortium]

Néanmoins, ces circuits dédiés traversent un ou plusieurs commutateurs de communication par lesquels la confidentialité des données peut être compromise par quelqu'un qui voudrait observer le flux des données. L'entreprise cliente n'a donc pas le choix, elle doit faire confiance au fournisseur pour qu'il maintienne l'intégrité des circuits et qu'il mette en place les moyens les plus efficaces pour empêcher l'espionnage du trafic réseau ; c'est pour cette raison qu'on appelle cela des VPNs de *confiance*. [VPN Consortium]

N'offrant aucune réelle garantie en ce qui concerne la protection des données, les VPNs de confiance intéressent surtout les entreprises qui veulent que leurs données transitent à travers certains chemins qui ont des propriétés spécifiques, qui veulent utiliser leur propre adressage IP, et parfois même qui veulent gérer leur propre routage [VPN Consortium]. Un autre avantage des VPNs de confiance est qu'il n'y a aucun investissement à faire en termes d'équipement, puisque tout est géré par le fournisseur ; ils sont donc moins chers que des VPNs sécurisés à court terme, mais ce n'est pas le cas à long terme [SF VPN].

[18] A ne pas confondre avec Trusted VPN™ qui est en réalité un VPN sécurisé. Trusted VPN™ est une solution d'accès à distance offerte par Thales. [THALES]

Du côté du fournisseur, il peut assurer la séparation des différents circuits dédiés en utilisant un des deux protocoles qui ont été développés à cette fin, à savoir MPLS (Multi-Protocol Label Switching) et L2F (Layer 2 Forwarding) [wiki VPN en].

1.7.2 VPN sécurisé

Mais l'Internet devenant de plus en plus répandu, et se rendant compte que les fournisseurs de communications n'offraient aucune sécurité réelle par rapport aux données de leurs clients, certains *vendors* ont commencé à proposer des protocoles d'encryption. La motivation de ces protocoles d'encryption était de trouver un moyen qui permettrait de protéger les données au niveau de l'ordinateur émetteur ; ces données encryptées seraient ensuite transmises à travers l'Internet comme n'importe quelle autre donnée, et seraient finalement décryptées au niveau de l'ordinateur récepteur. [VPN Consortium]

Tous ces efforts ont donné lieu aux protocoles de "tunnelisation" cryptographique tel que nous les connaissons aujourd'hui. Ils fournissent des niveaux de confidentialité, d'authentification, et d'intégrité qui assurent que les informations transitant au travers d'un VPN restent privées. Ainsi, lorsque ces protocoles sont bien utilisés et implémentés, ils nous permettent de mettre en place une communication sécurisée sur un réseau non sécurisé ; la confidentialité nous permet de rendre inutile toute tentative d'écoute, l'authentification nous permet d'empêcher l'usurpation d'identité, et l'intégrité nous assure que les informations reçues n'ont pas été modifiées en cours de route. [wiki VPN en]

Nous entendons donc par VPN sécurisé, ou *Secure VPN* (SVPN), tout VPN qui a été construit en utilisant de l'encryption. Les VPNs sécurisés sont toujours utilisés lorsqu'un VPN d'accès à distance est requis, où le but est que les employés d'une entreprise puissent se connecter au VPN de leur entreprise à partir de n'importe où [VPN Consortium]. Ceci ne serait évidemment pas réalisable dans le cas d'un VPN de confiance ou hybride vu que l'employé devrait se trouver sur un des circuits dédiés de l'entreprise pour pouvoir se connecter au VPN de confiance.

A ce jour, il existe plusieurs protocoles avec lesquels nous pouvons construire un VPN sécurisé, à savoir IPsec (IP security), SSL/TLS (Secure Sockets Layer/Transport Layer Security), PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunnelling Protocol), et L2TPv3 (Layer 2 Tunnelling Protocol version 3) [wiki VPN en].

1.7.3 VPN hybride

Finalement, il y a le troisième type de VPN, le VPN hybride. A la base de ce type de VPN, nous trouvons un VPN de confiance de la nouvelle génération[19] dont une partie peut être utilisée pour établir un VPN sécurisé, qui peut être contrôlé par le client ou bien par le même fournisseur qui fourni le VPN de confiance. Parfois l'entièreté d'un VPN hybride est sécurisé par le VPN sécurisé, mais la plupart du temps seule une partie du VPN hybride est sécurisée. [VPN Consortium]

[19] La nouvelle génération de VPNs de confiance offerts par les fournisseurs de services utilise l'Internet au lieu du réseau téléphonique commuté (RTC), ou PSTN (Public Switched Telephone Network), comme moyen de communication. Cette nouvelle génération de VPN de confiance n'offre pas plus de sécurité qu'avant, mais elle permet une division du WAN d'une entreprise en plusieurs segments qui, en général, comprennent une garantie de qualité de service, ou QoS (Quality of Service), par le fournisseur. [VPN Consortium]

L'intérêt des VPNs hybrides est qu'ils permettent de tirer profit des avantages offerts par les VPNs sécurisés et de confiance, en combinant la sécurité offerte par les VPNs sécurisés et la garantie de certaines propriétés du routage, tel QoS, offerte par les VPNs de confiance. Un scénario typique pour le déploiement d'un VPN hybride se présente quand une entreprise utilise déjà un VPN de confiance mais que certains départements requièrent qu'au moins une partie du VPN mis en place ait un certain niveau de sécurité. [VPN Consortium]

1.7.4 VPNs et l'accès à distance

Etant donné que l'accès à distance est notre intérêt principal, nous nous focaliserons davantage sur les VPNs sécurisés en laissant de côté les VPNs de confiance avec lesquels il n'est pas possible d'établir un accès distant. Ainsi nous proposons de passer en revue les différentes technologies qui peuvent être utilisées pour établir des VPNs sécurisés, à savoir IPsec, SSL/TLS, PPTP, L2TP.

1.8 VPN securisé basé sur IPsec

IPsec constitue un ensemble de protocoles fournissant une sécurité au niveau de la couche réseau [Kurose et Ross]. Le but d'IPsec est de fournir plusieurs services de sécurité pour le trafic IP, donc pour la couche réseau, aussi bien pour IPv4 que pour IPv6. Parmi ces services se trouvent la confidentialité, l'authentification, l'intégrité, ainsi qu'une protection contre les attaques de rejoue. En outre, IPsec peut protéger un ou plusieurs "chemins" qui relieraient deux hôtes, deux passerelles de sécurité[20], ou bien un hôte et une passerelle de sécurité. [RFC 2401]

1.8.1 Composition du protocole IPsec

Les principaux protocoles qui sont compris dans la suite de protocoles IPsec sont les protocoles AH (Authentication Header) et ESP (Encapsulation Security Payload).

Ainsi un émetteur qui envoie un datagramme sécurisé à un destinataire utilise soit le protocole AH, afin de garantir l'authentification de la source et l'intégrité des données, soit le protocole ESP, afin de garantir l'authentification, l'intégrité, et la confidentialité des données. Même si les deux protocoles ne fonctionnent pas de la même manière et offrent des fonctionnalités différentes, tous deux commencent par un *handshake* entre l'émetteur et le destinataire afin d'établir une connexion logique simplex[21], ou SA (Security Association), au niveau de la couche réseau. Notons que la protection des données transitant par la SA dépend du protocole qui est utilisé [RFC 2401]. Chaque connexion SA est identifiée par l'identifiant du protocole utilisé, l'adresse IP de la source de la connexion simplex, et un identifiant de la connexion de 32 bits appelé le SPI (Security Parameter Index). [Kurose et Ross]

Les deux protocoles utilisent également une même méthode d'authentification appelée HMAC qui utilise une encryption symétrique pour authentifier les messages envoyés [Kurose

[20] Le terme passerelle de sécurité est utilisé dans les RFCs pour parler des différents systèmes intermédiaires qui font usage des protocoles IPsec. Un routeur ou pare-feu, utilisant un ou plusieurs protocoles IPsec, sont des exemples de passerelle de sécurité. [RFC 2401]

[21] C'est-à-dire une connexion unidirectionnelle. Ainsi, si deux hôtes veulent échanger des datagrammes sécurisés entre eux, il devront établir deux SA. [Kurose et Ross]

et Ross]. Il est également utile de savoir que chacun de ces protocoles peut être utilisé soit en mode transport, soit en mode tunnel en fonction du mode utilisé par la SA [RFC 2401].

1.8.2 Security Association

En mode transport, la SA (Security Association) est une connexion logique entre deux hôtes[22]. Pour le protocole ESP, une SA en mode transport n'offre aucun service de sécurité pour le *header* IP et les *headers* d'extensions qui précédent le *header* ESP. Par contre, dans le cas du protocole AH, les services de sécurité sont d'application pour certaines parties du *header* IP, certaines parties des *headers* d'extension, et certaines options[23]. [RFC 2401]

Une SA en mode tunnel est en fait une SA appliquée à un tunnel IP et, afin d'éviter des problèmes potentiels dus à la fragmentation de paquets IPsec, ce type de SA doit toujours être utilisé lorsqu'une passerelle de sécurité est présente à l'un ou l'autre bout de la connexion SA. Ainsi une SA entre deux passerelles de sécurité ou entre un hôte et une passerelle de sécurité sera toujours une SA en mode tunnel[24]. En revanche, deux hôtes peuvent établir une SA en mode tunnel s'ils le désirent. Lorsqu'on établit une SA en mode tunnel, nous avons un *header* IP "extérieur", indiquant une destination utilisée par IPsec, et un *header* IP "intérieur", indiquant la destination réelle du paquet, et entre lesquels se trouve le *header* AH ou ESP. Lorsque le protocole AH est utilisé, des éléments du *header* IP "extérieur" ainsi que l'entièreté du paquet IP "intérieur"[25] sont protégés par le service de sécurité offert par le protocole. Lorsque nous utilisons le protocole ESP, les services de sécurité du protocole ne protégent que le paquet IP "intérieur" et pas le *header* IP "extérieur". [RFC 2401]

1.8.3 Protocole AH

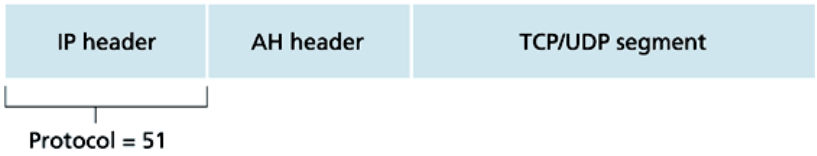


Fig. 1.8 – Datagramme IP utilisant le protocole AH [Kurose et Ross]

Une fois la SA établie, l'hôte source peut envoyer des datagrammes sécurisés à l'hôte destinataire. Comme nous pouvons le constater à la figure 1.8, ces datagrammes sécurisés contiennent un *header* AH qui est inséré entre le datagramme IP original et le *header* IP, ce qui veut dire que le champ de données augmente en taille et est encapsulé comme un datagramme IP standard. Dans le *header* IP se trouve un champ de protocole qui contiendra désormais la valeur 51, ce qui permettra à l'hôte destinataire de savoir que le datagramme a été encapsulé en utilisant le protocole AH. [Kurose et Ross]

[22] Seul l'emplacement du header AH ou ESP dans le datagramme IP change lorsqu'on se trouve en IPv4 ou en IPv6 [RFC 2401].
[23] Ces options se trouvent dans différents *headers* selon que l'on est en IPv4 ou en IPv6 [RFC 2401].
[24] Quelques exceptions sont faites, notamment lorsque le trafic est destiné à la passerelle de sécurité qui, par ce fait, est considérée comme un hôte et l'utilisation du mode transport est permis [RFC 2401].
[25] C'est-à-dire le paquet IP qui est transmis par le tunnel.

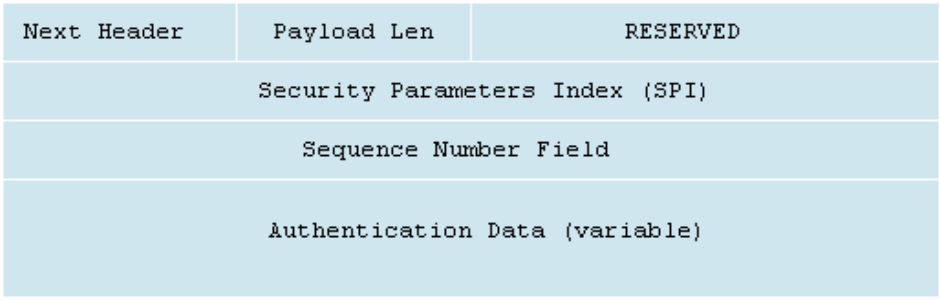


Fig. 1.9 – *Header* AH, inspiré de [RFC 2402]

Quant au *header* AH, nous pouvons remarquer à la figure 1.9 qu'il contient quatre champs : *Next header* (indique le protocole de la couche transport que le datagramme IP utilise pour les données se trouvant après le *header* AH[26]), *SPI* (une valeur arbitraire de 32 bits qui, en combinaison avec l'adresse IP de destination et le protocole utilisé, permet d'identifier la SA du datagramme), *Sequence Number* (un champ de 32 bits contenant un numéro de séquence afin d'empêcher des attaques de rejoue ou de MITM[27]), et *Authentication Data* (un champ de taille variable contenant une signature digitale propre à chaque datagramme[28] qui authentifie l'hôte source du datagramme et en garantit l'intégrité) [Kurose et Ross].

Néanmoins, il faut remarquer que la protection contre les attaques de rejoue ou de MITM est optionnelle et doit être activée par l'hôte destinataire lors de l'établissement de la SA ; le *Sequence Number* est incrémenté par défaut par l'hôte émetteur, mais ce champ n'est d'aucune utilité contre ces attaques si il n'est pas vérifié par l'hôte destinataire. [RFC 2402]

1.8.4 Protocole ESP

L'hôte source peut également sécuriser les datagrammes en utilisant le protocole ESP une fois que la SA est établie. Le protocole ESP offrant la confidentialité en plus de l'authentification et l'intégrité offertes par le protocole AH, il est également plus compliqué à mettre en œuvre [Kurose et Ross].

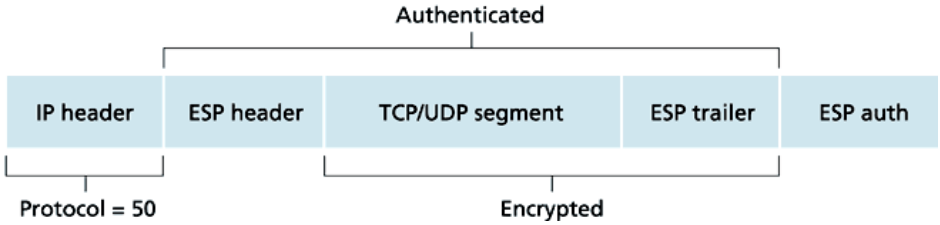


Fig. 1.10 – Datagramme IP utilisant le protocole ESP [Kurose et Ross]

En effet, la figure 1.10 nous montre que nous commençons par entourer les données du datagramme IP avec des champs *header* et *trailer* et on insérera cette information

[26] Ce champ permet de savoir si nous avons affaire à un segment du protocole TCP, UDP, ICMP, etc. Cette information devrait normalement se trouver dans le champ protocole du header IP mais chez champ a été utilisé pour indiquer l'utilisation du protocole AH, donc cette information est "sauvegardée" dans le champ *Next Header* du *header* AH.
[27] Man-In-The-Middle.
[28] Cette signature digitale est obtenue par l'utilisation d'une fonction de hachage, tel MD5 ou SHA, sur l'entièreté du datagramme IP [Kurose et Ross].

encapsulée dans le champ de données du datagramme IP. Cette fois-ci c'est la valeur 50 qui sera insérée dans le champ de protocole du *header* IP afin d'informer l'hôte destinataire de l'utilisation du protocole ESP, et donc de la présence du *header* et *trailer* ESP supplémentaires. Ensuite, les données initiales du datagramme et le *trailer* ESP sont encryptés avec l'algorithme de chiffrement DES-CBC afin de fournir la confidentialité des données. [Kurose et Ross]

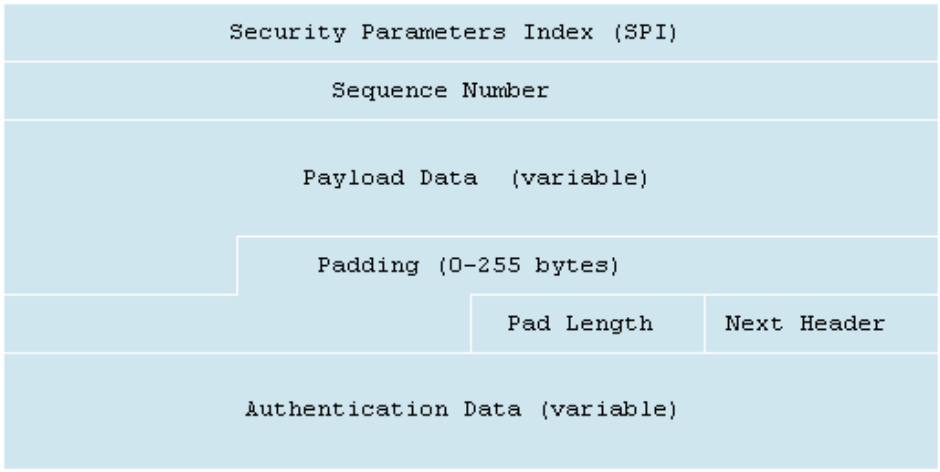


Fig. 1.11 – *Header* ESP, inspiré de [RFC 2406]

A la figure 1.11, nous pouvons voir que, comme dans le *header* AH, nous trouvons dans le *header* ESP un champ *SPI* et un champ *Sequence Number*, alors que le champ *Next header* se trouve lui dans le *trailer* ESP[29]. Finalement vient le champ *Authentication Data*, un champ à part qui se trouve après le *trailer* ESP [Kurose et Ross]. Il faut tout de même savoir que les différents services de sécurité offerts par le protocole ESP (confidentialité, authentification, intégrité) sont optionnels mais au moins un des services doit être utilisé, soit la confidentialité, soit l'authentification en combinaison avec l'intégrité [RFC 2406].

1.8.5 Gestion des clés et des SA

Afin de pouvoir utiliser IPsec de manière efficace, il faut avoir un moyen automatisé pour gérer les clés d'encryption et les SA, fonctionnalité qui est offerte par les protocoles ISAKMP (Internet Security Association and Key Management Protocol) et IKE (Internet Key Exchange) [Kurose et Ross]. Néanmoins, d'autres protocoles pourraient être utilisés tel que Kerberos ou SKIP [RFC 2401].

ISAKMP est un protocole qui combine l'authentification, la gestion de clés, et des SA afin de fournir la sécurité requise pour toutes sortes de communications passant par Internet. Plus précisément, ISAKMP définit les procédures et les formats de paquets pour établir, négocier, modifier, et supprimer des SA [RFC 2408].

Il faut noter que ISAKMP se distingue des protocoles d'échange de clés afin d'avoir une séparation nette entre les détails de gestion de SA et de clés, et les détails de l'échange de clés. En effet, il peut y avoir plusieurs protocoles d'échange de clés, ayant chacun des propriétés de sécurité différentes, mais un cadre commun est nécessaire, aussi bien pour

[29] Vu que le *trailer* ESP sera encrypté, cela nous offre encore plus de sécurité par le fait qu'un intrus ne pourra même pas savoir quel protocole de la couche transport est utilisé pour la communication [Kurose et Ross].

pouvoir décider du format des attributs des SA, que pour la négociation, la modification, et la suppression des SA. Ainsi, en ce qui concerne la négociation des SA, ISAKMP s'en occupe pour toutes les couches de la pile protocolaire, ce qui a l'avantage de réduire les duplications de fonctionnalités dans différents protocoles de sécurité, et permet aussi de réduire le temps d'établissement d'une connexion par le fait qu'on peut négocier toute une série de services en une fois. [RFC 2408]

Un autre avantage de la négociation d'ISAKMP est qu'elle permet d'arriver à un accord sur le niveau de sécurité à adopter entre plusieurs groupes d'utilisateurs lorsque ceux-ci ont des exigences de sécurité qui diffèrent ; par exigences de sécurité nous entendons les différents algorithmes d'encryption, d'authentification, d'échange de clés, et l'IPsec. Nous pourrions, par exemple, penser à un VPN qui aurait différents niveaux de sécurité pour chaque département d'une entreprise, selon que le département traite des données plus ou moins sensibles, ainsi qu'un niveau de sécurité très élevé pour les employés se connectant à partir de l'extérieur du VPN. [RFC 2408]

ISAKMP est également assez flexible de par le fait que son mécanisme de négociation du niveau de sécurité permet que de nouveaux algorithmes d'encryption ou d'authentification puissent être utilisés par la suite, lorsqu'une faille a été trouvée dans un ancien algorithme ou qu'un meilleur algorithme a été développé, sans avoir à redéfinir un tout nouveau protocole [RFC 2408].

Quant à IKE, c'est un protocole hybride utilisant des parties des protocoles Oakley[30] et SKEME[31], tout en restant indépendant de ces protocoles, en combinaison avec ISAKMP. Le but du protocole est de permettre de négocier des SA ainsi que de leur fournir les mécanismes d'échange de clés appropriés, particulièrement en ayant en tête les VPNs ainsi que les utilisateurs voulant accéder aux VPNs à distance. En particulier, il utilise des algorithmes d'encryption, d'authentification, et des fonctions de hachage. [RFC 2409]

1.9 VPN sécurisé basé sur SSL/TLS

SSL est un protocole qui a été développé par Netscape afin de fournir une encryption des données ainsi qu'une authentification entre deux entités. Ce protocole est assez répandu de nos jours et est implémenté dans presque tous les navigateurs Internet et serveurs Web [Kurose et Ross]. Par la suite, l'IETF a créé le protocole TLS afin de rassembler les différentes implémentations de SSL en un standard commun ; TLS est donc l'équivalent de la version 3 du protocole SSL, avec quelques modifications mineures [SANS OpenVPN]. Pour ne pas saturer le texte, nous utiliserons simplement le terme SSL lorsqu'on parlera de SSL/TLS par la suite.

1.9.1 Fonctionnement du protocole SSL

En gros, la façon dont fonctionne SSL est assez simple ; du côté de l'hôte émetteur, les données provenant de la couche applicative sont encryptées par SSL et envoyées à un *socket*

[30] Un protocole regroupant une série de différents mécanismes d'échange de clés, notamment le Diffie-Hellman Key Exchange [RFC 2409].
[31] Une technique souple d'échange de clés offrant l'anonymat, la répudiation, ainsi qu'un renouvellement rapide des clés [RFC 2409].

TCP, et du côté de l'hôte destinataire, les données encryptées provenant du *socket* TCP sont décryptées par SSL et envoyées à la couche applicative pour être traitées. Mais avant que l'envoi de données puisse être protégé, le protocole SSL débute par une phase de *handshake*, qui comprend toute une série d'étapes, afin de négocier l'algorithme d'encryption et les clés qui seront utilisés. Donc une fois la phase de *handshake* complétée, les données qui transiteront entre les deux entités seront encryptées avec les clés de session qui avaient été négociées lors de cette phase initiale.

A un plus haut niveau, nous proposons de nous placer dans un contexte de commerce électronique et de parcourir les différentes étapes concernées lors d'une transaction électronique, ceci afin de mieux comprendre le fonctionnement d'SSL.

Tout d'abord, nous avons un client qui se rend, par l'intermédiaire de son navigateur (compatible avec SSL), sur la page web sécurisée d'un marchand, qui est gérée par le serveur web (compatible avec SSL) du marchand[32]. A ce moment là, le navigateur et le serveur font un *handshake* afin d'authentifier le serveur[33] et générer une clé symétrique, en utilisant la technologie des clés publiques RSA. Une fois la clé généré et partagée entre les deux entités, toutes les données que celles-ci s'échangeront par la suite seront encryptées par cette clé symétrique. La communication entre les deux entités sera donc bel et bien protégée [Kurose et Ross]

1.9.2 Authentification

Afin de garantir l'authentification entre serveur et client, SSL fait usage des certificats électroniques et d'autorités de certification, ou CA (Certification Authorities) [Kurose et Ross].

Dans le cadre du commerce électronique, les navigateurs Internet qui sont compatibles avec SSL maintiennent une liste de CA en qui ils ont confiance, ainsi que leurs clés publiques. De cette manière, lorsqu'un client veut interagir avec le serveur web d'un marchand, qui est compatible avec SSL, le client demande le certificat électronique du serveur qui contient la clé publique du serveur. Ce certificat électronique, étant signé par un CA se trouvant parmi la liste des CA de confiance, permet au client d'être sûr que le serveur web qu'il contacte est bien celui qu'il dit être dans son certificat. Ainsi, le client sait que ce n'est pas un intrus qui se fait passer pour le serveur web lorsqu'il envoie une information sensible[34]. [Kurose et Ross]

A l'inverse, nous pouvons également authentifier le client auprès du serveur en utilisant les certificats et CA de confiance de la même manière. Cette authentification est très utile dans des situations où c'est le serveur qui serait susceptible de transmettre des informations sensibles[35], mais vu que ce genre de situation n'est pas la plus répandue, l'authentification du client auprès du serveur est optionnelle. [Kurose et Ross]

Une fois que la phase d'authentification est terminée, la confidentialité des informations échangées entre les deux entités est assurée par l'encryption et la désencryption des données par le navigateur et le serveur web. Ceci, en combinaison avec un mécanisme

[32] Il est intéressant de remarquer que la page web du marchand est sécurisée par le fait qu'elle utilise https au lieu du protocole habituel, http. Notons que https n'est pas en soit un protocole, mais plutôt une combinaison du protocole http avec SSL ou TLS [wiki https].

[33] La phase de *handshake* permet également d'authentifier le client auprès du serveur, mais cette deuxième authentification est optionnelle [Kurose et Ross].

[34] Notamment un numéro de carte de crédit en cas d'achat électronique par Internet.

[35] Le cas d'une banque qui transmet les informations financières de son client est un bon exemple [Kurose et Ross].

fourni par SSL qui assure l'intégrité des données, permet au client et au marchand d'être sûrs que les informations qu'ils s'échangent ne seront pas lisibles ni modifiables par un éventuel intrus. [Kurose et Ross]

1.9.3 Handshake

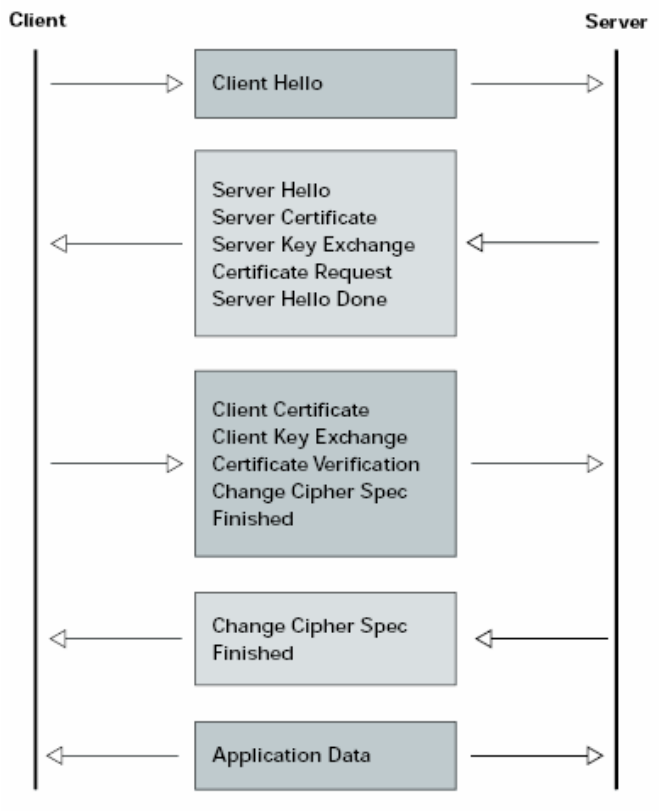


Fig. 1.12 – *Handshake* SSL, inspiré de [CISCO SSL]

Comme nous pouvons le voir à la figure 1.12, la première étape du *handshake*, l'étape *Client Hello*, est exécutée. Cette étape consiste en l'envoi d'informations du client vers le serveur, contenant notamment la version SSL du navigateur ainsi que les préférences au niveau des différents algorithmes cryptographiques qu'il est possible d'utiliser pour assurer l'encryption des données ultérieurement. Ensuite, c'est l'étape *Server Hello* où c'est au tour du serveur d'envoyer la version SSL qu'il utilise et ses préférences cryptographiques. En même temps, le serveur envoie aussi son certificat électronique, *Server Certificate*, duquel le client pourra extraire la clé publique RSA du serveur. Puis il averti le client qu'il a fini d'envoyer toutes les informations nécessaires, *Server Hello Done* [Kurose et Ross]

Vu que ce certificat est signé par un CA de confiance, donc avec la clé privée du CA, si ce CA se trouve dans la liste des CA de confiance du client, il pourra récupérer la clé publique du CA pour vérifier la validité du certificat. Si le CA ne se trouve pas dans la liste des CA de confiance, le client sera averti de la non fiabilité du certificat [Kurose et Ross]. En effet, le client pourra vérifier l'identité du serveur en analysant le certificat, mais cette identification ne peut être fiable tant que le certificat n'a pas été signé par un CA de confiance.

Une fois la clé publique du serveur récupérée, le client créera une clé symétrique aléatoire qu'il encryptera avec cette clé publique et enverra le résultat au serveur, *Client Key*

Exchange. Vu que le serveur a en sa possession la clé privée correspondant à la clé publique, il pourra décrypter le message envoyé par le client pour obtenir la clé symétrique qui sera désormais partagée entre les deux entités. Ensuite, le client dira au serveur que les prochaines informations que recevra le serveur seront encryptées avec la clé symétrique, *Change Cipher Spec*, puis il enverra un message encrypté au serveur pour indiquer qu'il a fini sa partie du *handshake*, *Finished*. Le serveur suivra les mêmes étapes et enverra le même genre de messages au client pour terminer sa partie du *handshake* ; à ce moment-ci, toutes les données qui seront échangées par la suite seront encryptées et décryptées avec la clé symétrique qui a été partagée précédemment. [Kurose et Ross]

Notons que les messages *Server Key Exchange*, *Certificate Request*, *Client Certificate* sont optionnels. En effet, ces messages ne sont utilisés que lorsqu'une authentification du client auprès du serveur est exigée. [RFC 4346]

Le client pourra donc maintenant effectuer le paiement en ligne sans soucis. Mais ce genre de scénario s'applique également à d'autres transactions telles que le *PC-banking* ou bien la vente et l'achat de valeurs boursières [Kurose et Ross]. Rappelons nous que le fonctionnement du *handshake*, tel que nous l'avons expliqué ici, se situe dans le cadre du commerce électronique, mais ce sont néanmoins les mêmes mécanismes qui sont utilisés de manière identique pour établir un VPN SSL.

1.9.4 VPN sécurisé basé sur SSL : en théorie et en pratique

En théorie, il est tout à fait possible de concevoir un VPN basé sur le protocole SSL et offrant les mêmes fonctionnalités qu'un VPN basé sur IPsec. Ainsi, le *handshake* RSA, dont le fonctionnement a été expliqué auparavant, fournit le même mécanisme d'échange de clés que celui qui est offert par le protocole IKE dans IPsec. En ce qui concerne la protection des données, SSL fait usage de sa librairie cryptographique pour fournir des méthodes d'encryption similaires à celles utilisées pour protéger les données qui transiteront par les tunnels IPsec. [SANS OpenVPN]

En réalité, la pratique dévie de la théorie dans le monde des VPNs SSL. En effet, alors que certaines solutions de VPNs SSL incorporent réellement les différentes fonctionnalités que devrait avoir un vrai VPN SSL, d'autres solutions délaissent ces fonctionnalités et se font quand même passer pour un VPN SSL [SANS OpenVPN].

Le grand problème est que les fournisseurs de solutions incomplètes utilisent comme argument principal de vente le fait que leurs solutions sont *clientless*[36], c'est-à-dire qu'il n'y a pas besoin d'installer un logiciel spécifique du côté de l'ordinateur client pour que la solution fonctionne. Mais en réalité, ce type de solution utilise quand même un client universel, le navigateur Internet ; la nuance se trouve donc dans le fait qu'aucun logiciel *supplémentaire* ne doit être installé du côté de l'ordinateur client. [SANS OpenVPN]

Ces solutions procèdent par l'établissement d'une passerelle SSL qui fournit un accès aux applications de l'entreprise, opération qui peut s'effectuer de quatre façons différentes : par un mécanisme de proxy, par traduction d'application, par *port forwarding*, et par extension

[36] Avec ces solutions soi-disant *clientless*, les vendeurs utilisent comme argument la facilité d'utilisation et le fait de pouvoir se connecter à partir de n'importe où, même à partir de cyber-cafés ; c'est dire à quelle point leurs solutions sont peu sûres! [SANS OpenVPN]

de réseau. Il n'y a que par l'extension de réseau que l'on peut établir un véritable VPN tel qu'un VPN IPsec, mais dans tous les cas il requiert l'utilisation d'un logiciel client et seuls quelques vendeurs de VPNs SSL permettent l'extension de réseau. [SANS OpenVPN]

1.9.5 Limites du protocole SSL

Finalement, il est tout de même important de remarquer que SSL a ses limites. En effet, si l'utilisation de SSL est fort répandue dans des situations de commerce électronique, ce n'est pas à cet usage qu'a été développé SSL mais plutôt pour fournir un moyen générique de communication sécurisé entre un client et un serveur. De ce fait, lorsqu'un client utilise SSL pour authentifier le serveur d'un marchand, cette authentification ne peut rien garantir en ce qui concerne la fiabilité du marchand ni son droit d'accepter des paiements électroniques. Inversement, si le mécanisme optionnel d'authentification SSL garantit au marchand que le client est bien celui qu'il dit être, rien ne prouve que la carte de crédit utilisée appartienne bien au client. [Kurose et Ross]

1.10 VPN sécurisé basé sur PPTP

PPTP, signifiant Point-to-Point Tunneling Protocol, est un protocole permettant la "tunnelisation" du protocole PPP à travers un réseau IP. Il ne change en rien le protocole PPP ; il ne fait que définir une nouvelle façon de transporter ce protocole. PPTP spécifie également des protocoles de contrôle et de gestion d'appels, de type *Dial-up* sur circuit commuté, provenant du PSTN ou de l'ISDN. Ces deux protocoles permettent aussi d'initier des connexions de type circuit commuté vers l'extérieur. Afin de pouvoir fournir un service de datagrammes encapsulés avec un contrôle de flux et de congestion, PPTP utilise un mécanisme GRE (Generic Routing Encapsulation). [RFC 2637]

1.10.1 Composition du protocole PPTP

Par l'utilisation d'une architecture client-serveur, PPTP permet la séparation des fonctions NAS (Network Access Server) ; nous avons donc d'un côté le PNS (PPTP Network Server) et de l'autre le PAC (PPTP Access Concentrator), c'est-à-dire le client [RFC 2637].

En temps normal, quelques fonctionnalités offertes par un NAS sont le contrôle des modems externes ou adaptateurs terminaux, la terminaison logique des sessions LCP d'une liaison PPP, une participation dans les protocoles d'authentification de PPP, la terminaison logique de plusieurs NCP, et le routage multi protocolaire entre interfaces NAS. Ces fonctions sont donc maintenant partagées entre le PAC et le PNS ; le PAC s'occupe des deux premières fonctionnalités et peut s'occuper de la troisième, le PNS s'occupe des deux dernières fonctionnalités et peut également s'occuper de la troisième. [RFC 2637]

PPTP s'occupe donc du transport des PDUs (Protocol Data Unit) du protocole PPP entre le PAC et le PNS ainsi que du contrôle et de la gestion des appels. Le protocole PPTP n'est implémenté que par le PAC et le PNS de façon à ce que les autres systèmes ne soient pas au courant de son existence. Ainsi des logiciels client PPP continuent à fonctionner de la même manière que d'habitude, mais à travers un tunnel par lequel passe la liaison PPP. [RFC 2637]

Le protocole PPTP prévoit également qu'il y ait une relation plusieurs-à-plusieurs entre PACs et PNSs. Ainsi, un fournisseur Internet pourrait décider d'accepter le PPTP pour un certain nombre de clients d'un réseau interne et créer des VPNs pour eux, et chaque réseau interne pourrait opérer un ou plusieurs PNSs, auxquels seraient associés plusieurs PACs pour ainsi regrouper le trafic provenant de plusieurs endroits géographiques différents. Avec l'utilisation d'une version étendue de GRE, PPTP peut fournir un contrôle de flux et de congestion pour les tunnels utilisés pour transporter les trames PPP entre PACs et PNSs, ce qui permet une gestion plus efficace de la bande passante disponible pour les tunnels et évite des retransmissions inutiles. [RFC 2637]

1.10.2 Fonctionnement du protocole PPTP

PPTP utilise deux composants ; une connexion de contrôle entre chaque paire PAC-PNS et un tunnel IP entre ces mêmes paires, servant au transport des trames PPP encapsulés par GRE [RFC 2637].

Avant l'établissement du tunnel entre un PAC et un PNS, il faut effectuer la connexion de contrôle, qui est en fait une session TCP standard établie sur le port 1723. Cette connexion de contrôle est utilisée pour transmettre les informations de gestion et de contrôle d'appels du protocole PPTP, mais elle est également responsable de la création, de la gestion et de la suppression des sessions qui ont lieu à travers le tunnel. Ainsi, pour chaque paire PAC-PNS il existe un tunnel ainsi que la connexion de contrôle qui y est associée. Afin de s'assurer que la connexion de contrôle est toujours en état de marche, un mécanisme de messages *keep-alive* est utilisé. D'autre part, pour permettre le multiplexage et démultiplexage des trames PPP, une clé de session est présente dans le *header* GRE pour indiquer à quelle session appartient une trame PPP ; cette clé de session est déterminée lors de la procédure d'établissement d'appel, ce qui est fait sur la connexion de contrôle. [RFC 2637]

1.10.3 Format des messages PPTP

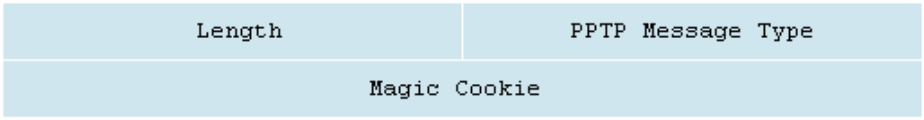


Fig. 1.13 – Format d'un message PPTP, inspiré de [RFC 2637]

Comme nous pouvons le voir à la figure 1.13, chaque message transmis sur la connexion de contrôle commence avec un *header* de 8 octets, contenant la taille totale du message, un indicateur du type de message PPTP, et un *Magic Cookie*. L'indicateur du type de message PPTP indique si l'on a affaire à un message de contrôle d'appel ou un message de gestion d'appel, tandis que le *Magic Cookie* est la constante 0x1A2B3C4D et qui permet au récepteur de s'assurer qu'il est bien synchronisé avec le flux de données TCP. En ce qui concerne le tunnel IP, les trames PPP sont encapsulées par GRE, et le résultat est ensuite envoyé par le protocole IP. [RFC 2637]

1.11 VPN sécurisé basé sur L2TP

L2TP, ou Layer 2 Tunnelling Protocol, est aussi un protocole permettant la "tunnelisation" des trames PPP à travers un réseau, et ceci de façon transparente pour les utilisateurs ainsi que pour les applications [RFC 2661].

1.11.1 Composition du protocole L2TP

Le protocole PPP (que nous avons déjà vu auparavant) définit un mécanisme d'encapsulation pour le transport de paquets multi protocolaires à travers des connexions *point-to-point* de la couche liaison (c'est-à-dire la deuxième couche dans la pile protocolaire OSI). En général, un utilisateur établit une liaison de la couche 2 avec un NAS par l'intermédiaire d'une technique spécifique (tel un *Dial-up* PSTN, ISDN, ADSL, etc) et puis utilise le protocole PPP par-dessus cette liaison. [RFC 2661]

Dans un tel scénario, le point de terminaison de la liaison de la couche 2 ainsi que le *endpoint* de la session PPP se trouve sur le même support physique, à savoir le NAS. L2TP, lui, permet d'étendre le modèle PPP en permettant que le point de terminaison de la couche 2 et le *endpoint* de la session PPP puissent se trouver sur deux supports différents, connectés par un réseau de commutation de paquets. Ainsi, avec L2TP, un utilisateur établit une liaison de la couche 2 avec un concentrateur d'accès (par exemple, un *modem bank*, ADSL DSLAM, etc) et puis le concentrateur "tunnelise" chaque trame PPP vers le NAS. [RFC 2661]

Ceci permet la séparation entre le traitement des trames PPP et le point de terminaison de la liaison de la couche 2. Un grand avantage d'une telle séparation est qu'au lieu d'obliger la liaison de la couche 2 à se connecter directement au NAS, cette liaison peut être faite avec un concentrateur de circuit local qui étendra ensuite la session logique PPP à travers une infrastructure partagée telle un *frame relay circuit* ou bien l'Internet. Evidemment ceci est tout à fait transparent du point de vue de l'utilisateur. [RFC 2661]

1.11.2 Fonctionnement du protocole L2TP

Tout comme PPTP, L2TP transmet deux types de messages ; des messages de contrôle ainsi que des messages de données. De la même façon, les messages de contrôle sont également utilisés pour l'établissement, la maintenance, et la terminaison des tunnels et des appels, et les messages de données sont utilisés pour encapsuler les trames PPP qui sont transportées à travers les tunnels. [RFC 2661]

En ce qui concerne l'envoi des messages, les messages de données sont transmis par un canal non fiable (donc si il y a une perte de paquet, il n'est pas retransmis), ce qui n'est pas le cas des messages de contrôle qui eux sont transmis par un canal fiable. Des numéros de séquence sont donc utilisés dans les messages de contrôle afin d'assurer cette fiabilité. Si ces deux types de messages ont des finalités différentes, ils partagent néanmoins le même format de header. [RFC 2661]

1.11.3 Format de header des messages L2TP

Vu que le format du *header* est partagé par les messages de données et les messages de contrôle, certains champs du *header* sont optionnels. Dans le cas où un champ n'est pas

utilisé, on signale son absence dans le *header* et l'espace qu'il aurait normalement occupé n'existe plus [RFC 2661].

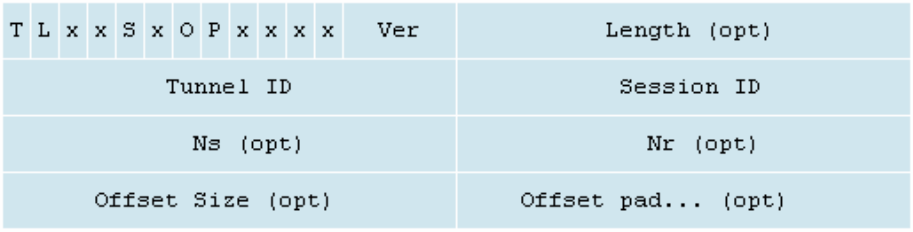


Fig. 1.14 – Format du *header* d'un message L2TP, inspiré de [RFC 2661]

A la figure 1.14 nous pouvons constater les différents champs qui composent le *header* d'un message L2TP. Le premier champ que l'on rencontre (*T*) est un bit de type de message, permettant au récepteur de distinguer s'il s'agit d'un message de contrôle ou de données ; une valeur de 0 nous dit que nous avons affaire à un message de données tandis qu'une valeur de 1 nous dit que nous avons affaire à un message de contrôle. Ensuite nous avons un bit de présence du champ longueur (*L*) ; ce bit doit être initialisé à 1 si le champ longueur est présent. Puis nous trouvons certains bits qui ont été réservés pour des extensions futures du protocole (*x*) ; pour L2TP, ces bits doivent être mis à 0 pour tous les messages sortants, et ils doivent être ignorés lors de la réception. [RFC 2661]

Nous trouvons également un bit de présence de *Sequence* (*S*) et de *Offset* (*O*) ; si ces bits ont une valeur de 1, le premier indique la présence des champs *Ns* et *Nr* tandis que le deuxième indique la présence du champ *Offset Size*. Après vient un bit de *Priority* (*P*) qui signale que le paquet doit être traité en priorité du côté émetteur lorsqu'il a une valeur de 1. Tel serait le cas par exemple pour les messages LCP utilisés comme *keep-alive* pour la liaison, qui ne peuvent pas se permettre d'avoir du retard dû à une congestion locale. Ensuite nous trouvons un champ *Ver* servant à indiquer la version du *header* du message de données L2TP ; une valeur de 2 doit être utilisée[37]. Après nous pouvons connaître la taille totale du message, mesuré en octets, en regardant le contenu du champ *Length*. [RFC 2661]

Ensuite nous passons au champ *Tunnel ID*. Ce champ est un identifiant pour la connexion de contrôle, mais chaque côté de la connexion a un identifiant de la connexion qui lui est propre. C'est-à-dire que le même tunnel aura un identifiant différent pour chaque bout du tunnel, donc la valeur contenue dans le champ *Tunnel ID* du message qui sera envoyé correspondra à l'identifiant associé au récepteur du message. Evidemment ces identifiants sont choisis pendant la création du tunnel. Le champ *Session ID*, qui est également propre à l'extrémité du tunnel duquel on se situe, remplit la même fonction et fonctionne de la même manière que le champ *Tunnel ID*. La seule différence est que le *Session ID* identifie une session établie au travers du tunnel et ces identifiants sont choisis pendant la création de la session. [RFC 2661]

Après le champ *Session ID* se trouve *Ns* qui est un numéro de séquence pour les messages de contrôle ou de données, et ce champ est incrémenté à chaque message envoyé. Le champ *Nr*, quant à lui, est un champ qui indique le numéro de séquence attendu pour le prochain message de contrôle qui sera reçu. La valeur du champ *Nr* est donc égale à la valeur

[37] La valeur de 1 pour le champ *Ver* est réservée pour la détection de paquets L2F qui arriveraient parmi des paquets L2TP. Des paquets ayant une valeur inconnue pour le champ *Ver* doivent être rejetés. [RFC 2661]

du champ *Ns*, plus un. Finalement, nous avons le champ *Offset Size*. Ce champ est utilisé pour indiquer à partir de combien d'octets, après le *header* L2TP, nous pouvons nous attendre à rencontrer le début des données. De façon plus simplifiée, ce champ indique à quel endroit commencent les données dans le message. [RFC 2661]

Nous avons vu que certains champs, tel *Length*, *Ns*, et *Nr*, sont optionnels et ne sont donc pas toujours utilisés. Cependant, le caractère optionnel est restreint aux messages de données. Ces champs doivent donc être obligatoirement utilisés pour tous les messages de contrôle [RFC 2661].

Chapitre 2 : L'état de l'art de l'accès à distance

Les besoins d'accès à distance se font sentir de plus en plus de nos jours, que ce soit pour des particuliers, des PME, ou bien des multinationales. Bien évidemment, ces utilisateurs potentiels de l'accès à distance pourraient mettre en œuvre les concepts et mécanismes vus au chapitre précédent pour développer leur propre solution d'accès à distance. La création d'une solution personnalisée peut être motivée par une envie de l'entreprise d'avoir une solution d'accès à distance qui soit adaptée à ses besoins et qui respecte un niveau de sécurité qu'elle considère comme étant adéquat. Néanmoins, ceci peut s'avérer être un choix assez coûteux en termes de moyens et de temps, sans avoir une garantie de retour sur investissement. Il va de soi que ce constat est d'autant plus vrai lorsque c'est un individu ou une PME qui envisage cette option.

Heureusement pour eux, l'idée d'accéder à distance à des ressources informatiques ne date pas d'hier et il existe déjà un certain nombre de solutions d'accès à distance toutes faites. L'objectif de ce chapitre est de constater les différents mécanismes de sécurité qui sont offerts par ces différentes solutions. Nous proposons donc de passer en revue quelques solutions d'accès à distance qui sont les plus répandues à ce jour en portant une attention particulière aux aspects de sécurité.

2.1 GoToMyPC (Citrix)

GoToMyPC est un logiciel d'accès à distance développé par Citrix. Ce logiciel est basé sur la technologie web et fonctionne de façon à ce qu'on ne doive pas paramétrer notre pare-feu, ouvrir ou fermer des ports, configurer des adresses IP, ou acheter et installer du matériel spécifique.

Pour l'instant, GoToMyPC propose trois solutions d'accès à distance différentes, à savoir GoToMyPC, GoToMyPC Pro, et GoToMyPC Corporate. Ces trois solutions diffèrent seulement au niveau du nombre d'ordinateurs qui peuvent être accédés à distance, la première solution permettant d'accéder jusqu'à 3 ordinateurs, la deuxième solution permettant d'accéder entre 4 et 20 ordinateurs, et la dernière solution permettant l'accès à plus de 20 ordinateurs.

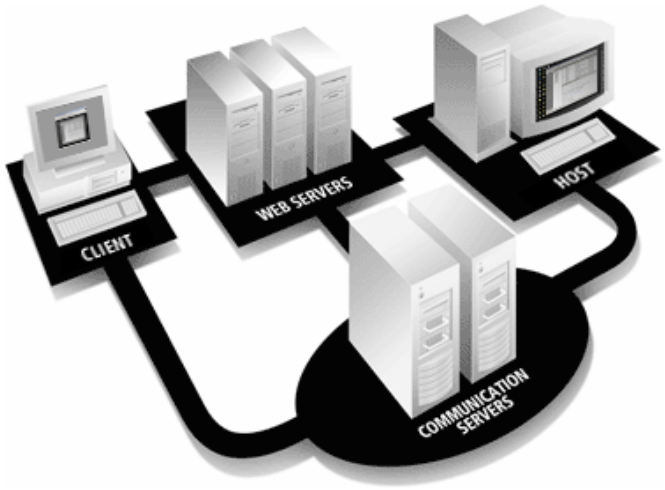


Fig. 2.1 – Les différents composants de GoToMyPC [GTMP]

Comme nous pouvons le constater à la figure 2.1, différents composants sont nécessaires afin que GoToMyPC puisse établir un accès à distance entre deux ordinateurs :

- Le site web de GoToMyPC. Ce site permet aux utilisateurs de créer un compte et enregistrer les ordinateurs qu'ils voudront accéder à distance. Par la suite, ils se connecteront sur le site pour établir la connexion avec l'ordinateur distant de leur choix.

- Le logiciel GoToMyPC. L'utilisateur télécharge un fichier d'installation faisant 1,4 MB avec lequel il installera GoToMyPC sur les ordinateurs hôtes (c'est-à-dire les ordinateurs qui seront accédés à distance). Lorsque le logiciel est installé, il s'exécute comme un service en attente d'une requête de connexion. Une fois cette requête reçue, un code d'accès est demandé à l'utilisateur distant avant de lui permettre l'accès à l'ordinateur hôte.

- Le *viewer*. Ce composant est en fait une espèce de fenêtre de visualisation dans laquelle s'affichera l'écran de l'ordinateur distant et qui est redimensionnable pour en faciliter l'usage. Deux types de ces fenêtres de visualisation existent, à savoir le *Native Viewer* et le *Universal Viewer*. Le premier est utilisé lorsque l'accès à distance se fait à partir d'un ordinateur client (c'est-à-dire l'ordinateur utilisé pour accéder à l'ordinateur hôte) tournant sur une version du système d'exploitation Windows, tandis que le deuxième est utilisé lorsque l'ordinateur client tourne sur un système d'exploitation Mac ou Unix. Mais afin de faciliter encore plus l'utilisation de GoToMyPC, l'utilisateur ne doit même pas choisir la fenêtre de visualisation à utiliser ; c'est le logiciel même qui fait ce choix en détectant automatiquement le système d'exploitation qu'utilise l'ordinateur client.

- Des serveurs web et de communication. A part la génération des pages web du site, les serveurs web servent surtout pour signaler une demande de connexion à un ordinateur hôte et passent la main au *broker* (voir ci-dessous) pour établir la connexion entre les deux ordinateurs. Une fois la connexion établie, le flux de données encryptées transite par les serveurs de communication pour être renvoyé à l'ordinateur client correspondant.

- Le *broker* GoToMyPC. Ce composant assure l'établissement correct de la connexion entre un ordinateur client ayant fait une requête de connexion et l'ordinateur distant auquel il veut accéder. Lorsque l'ordinateur hôte est allumé, il initialise une connexion sortante avec le broker GoToMyPC pour s'enregistrer comme étant actif. Par la suite il émet des *ping* périodiquement pour voir si il n'y a pas une requête d'accès à distance qui le concerne. Une fois la connexion établie, la "session" est assignée à un serveur de communication de façon optimale en utilisant le principe du *load-balancing*.

- Des outils de gestion et d'administration. Lorsque GoToMyPC est utilisé pour des entreprises, des outils sont mis à disposition afin de pouvoir surveiller l'usage qui est fait de GoToMyPC par les différents utilisateurs. Ces outils permettent également de consulter et modifier les paramètres qui déterminent quels employés pourront accéder à quels ordinateurs et à quel moment. Ainsi, l'administrateur

pourrait faire en sorte que seul un groupe spécifique d'employés puisse accéder à un certain ordinateur, uniquement les lundis et jeudis, entre 17h et 19h.

La façon dont a été conçu GoToMyPC procure plusieurs avantages aux utilisateurs. Pour commencer, l'accès se fait par l'intermédiaire du site web de GoToMyPC, ce qui fait qu'il n'y a rien à installer du côté client. Ce site web est d'ailleurs sécurisé par une authentification et encryption SSL, empêchant ainsi que des personnes tierces puissent avoir accès au mot de passe lorsqu'on établit la connexion avec un ordinateur distant. A ceci s'ajoute une encryption AES de 128 bits du flux de données entre l'ordinateur client et hôte, ainsi que des entrées clavier et souris de l'ordinateur hôte.

Il y a également la possibilité d'utiliser des *one-time passwords*, un code d'accès pour chaque ordinateur hôte, et une déconnexion automatique après un certain laps de temps d'inactivité de la part de l'ordinateur client. A ceci s'ajoute aussi une désactivation de la permission d'accès à un ordinateur hôte lors d'un certain nombre de tentatives erronées de connexion. Avec les outils de gestion et d'administration, il y a moyen d'extraire des fichiers log toutes les connexions effectuées par un utilisateur, avec la fréquence, la durée, et la date et heure de début et de fin de chacune. Afin d'assurer la sécurité et l'intégrité des fichiers log, ces derniers sont stockés sur des serveurs appartenant à Citrix.

Au niveau hardware, Citrix assure une redondance de switches, routeurs, et serveurs afin de garantir un haut niveau de fiabilité et d'opérabilité. Ceci nous permettrait aussi de nous passer des coûts de maintenance et de déploiement puisque tout est géré par Citrix à ce niveau là. GoToMyPC offre également l'avantage de ne pas avoir à reconfigurer un pare-feu existant et permet ainsi de garantir le niveau de sécurité actuel de celui-ci. Ceci est assuré par le fait qu'il n'y a que l'ordinateur client et l'ordinateur hôte qui initialisent des connexions sortantes en utilisant des ports TCP qui sont fréquemment laissés ouverts ; par exemple le port 80, 443, et/ou 8200.

GoToMyPC offre aussi une bonne performance, même sur des connexions par modem 56kbps, en utilisant une forte compression des données et en transmettant seulement une image de l'écran de l'ordinateur hôte ; une nouvelle image n'est renvoyée que lorsqu'il y a eu des changements sur l'écran hôte. L'ordinateur hôte est même accessible par des PDAs et certains téléphones mobiles sur lesquels tourne une version simplifiée de Windows.

Au niveau des fonctionnalités offertes, certaines pourraient s'avérer assez pratiques. Nous pouvons penser notamment au fait que GoToMyPC offre la possibilité d'imprimer à partir de n'importe où, de faire des copier-coller et même de "glisser" des documents directement entre les ordinateurs client et hôte. Il y a en outre moyen pour l'ordinateur client de verrouiller le clavier et la souris de l'ordinateur hôte ainsi que d'empêcher l'affichage à l'écran.

Citrix semble offrir une bonne solution d'accès à distance en proposant GoToMyPC. Les inconvénients auxquels nous pourrions songer seraient le coût (minimum 20$ par mois pour avoir accès à un seul ordinateur) et le fait que seuls des ordinateurs ayant un système d'exploitation de Windows peuvent être accédés à distance. Mais nous pourrions également ajouter un inconvénient indirect qui est celui de la dépendance que nous aurons vis-à-vis de GoToMyPC. En effet, si Citrix décide de ne plus continuer à offrir ce service, nous n'aurions plus de solution d'accès à distance du tout. Evidemment ce risque est peu probable, mais néanmoins non négligeable.

Sources : [GTMP], [GTMP PO], [GTMP PSWP]

2.2 PcAnywhere (Symantec)

PcAnywhere est un outil d'accès à distance développé par Symantec. Cet outil offre la possibilité d'établir des accès à distance à travers des réseaux LAN, WAN, et Internet. Il permet également d'établir des connexions modem à modem voir même des connexions directes entre deux ordinateurs par l'intermédiaire d'un port série ou parallèle, ainsi que le câble correspondant.

PcAnywhere présente l'avantage de permettre l'accès à des ordinateurs hôtes qui tournent soit sur Windows, Linux, ou Mac OS X, à partir de n'importe quel ordinateur tournant sur Windows, Linux, Mac OS X, ou même à partir de PDAs. Avec ce logiciel, nous avons également la possibilité de résoudre des problèmes sur un ordinateur ou serveur distant, voir même installer ou désinstaller des programmes. Il permet également de télécharger ou "uploader" entre l'ordinateur client et hôte, peu importe le système d'exploitation sur lesquels ils tournent. Ces transferts de fichiers peuvent même être programmés pour s'exécuter à la fin de la journée pour que des transferts de fichiers de grande taille ne perturbent pas l'utilisation de la bande passante. Récemment une fonctionnalité a été rajoutée pour empêcher l'accès à un ordinateur hôte pendant certaines heures pour certains jours. PcAnywhere est aussi capable de détecter automatiquement le type de bande passante utilisée afin de maximiser la performance pour chaque type de connexion.

Au niveau de l'authentification, PcAnywhere est compatible avec une série de méthodes d'authentification selon l'infrastructure informatique dans laquelle on se trouve. Ainsi, pour une utilisation personnelle, PcAnywhere offre un moyen d'authentification de base en vérifiant une liste d'utilisateurs et de mots de passe qui est stockée sur l'ordinateur hôte. Ce moyen d'authentification est évidemment le moins fiable et n'est donc pas admissible pour une utilisation en entreprise.

C'est pourquoi Symantec a fait en sorte que PcAnywhere puisse également utiliser une authentification basée sur des *directory server* tel le Microsoft Active Directory Service (ADS), le Novell Directory Service (NDS), Novell Bindery, ou bien une implémentation du Lightweight Directory Access Protocol (LDAP) de Microsoft, Novell, ou Netscape. Ce type d'authentification vérifie les droits d'accès d'un utilisateur ou d'un groupe d'utilisateurs par rapport à une liste qui est stockée sur un *directory server* appartenant à l'entreprise.

A ceci s'ajoute également la possibilité de pouvoir utiliser le RSA SecurID comme moyen d'authentification. Cette technologie consiste en l'utilisation d'un code d'accès provenant d'un *token* – une pièce de hardware qui génère des codes d'accès toutes les 60 secondes – ainsi qu'un code PIN uniquement connu de l'utilisateur détenteur de ce *token* pour lui accorder l'accès à une ressource informatique de l'entreprise. PcAnywhere peut donc être configuré afin d'utiliser le RSA SecurID, actuellement en place dans l'entreprise, pour authentifier l'utilisateur distant qui voudrait avoir accès à un ordinateur hôte se trouvant sur le réseau de l'entreprise.

Quant à l'encryption, PcAnywhere offre trois méthodes différentes, à savoir un encodage de base de PcAnywhere, une encryption symétrique et une encryption à clé publique. Si la méthode d'encryption utilisée diffère entre l'ordinateur hôte et l'ordinateur client, PcAnywhere oblige l'ordinateur utilisant le niveau d'encryption le plus faible à utiliser une méthode plus sécurisée. Par exemple, si l'ordinateur client a été configuré pour utiliser le simple encodage de PcAnywhere et que l'ordinateur hôte a été configuré pour utiliser l'encryption à clés symétriques, PcAnywhere obligera l'ordinateur client à utiliser une encryption à clés symétriques. De temps en temps il se peut qu'on ait installé une version

précédente à PcAnywhere 11 sur un des ordinateurs et que cet ordinateur ne puisse donc utiliser les méthodes de cryptage plus avancées qui sont offertes par les versions ultérieures. Pour ces cas là, le choix est laissé à l'utilisateur de l'ordinateur hôte qui peut décider soit d'empêcher que la connexion soit établie, soit de permettre que la connexion soit établie mais en obligeant l'ordinateur ayant la version la plus récente à utiliser la même méthode cryptographique que l'ordinateur ayant la version la plus ancienne.

Selon Symantec, l'encodage PcAnywhere consiste en une simple transformation des données échangées afin que le flux de données ne puisse pas être facilement compréhensible par un intrus.

En ce qui concerne l'encryption symétrique, PcAnywhere permet de choisir l'algorithme de cryptographie symétrique à utiliser ainsi que la longueur de la clé d'encryption. Par exemple, PcAnywhere offre une encryption AES avec une taille de clé maximale de 256 bits. Evidemment, plus la clé d'encryption est longue, plus les données sont sécurisées, mais ça a aussi comme effet de générer davantage de trafic et donc ralentit le transfert de données essentielles au fonctionnement de PcAnywhere. Lorsque l'algorithme de chiffrement RC4 – qui est déjà utilisé dans certains protocoles assez répandus tels que SSL ou WEP – a été choisi pour protéger les données, PcAnywhere requiert une API cryptographique de Microsoft qui se trouve dans les versions de Microsoft Internet Explorer 6 et ultérieures.

Pour ce qui est de la cryptographie à clé publique, PcAnywhere utilise des certificats électroniques pour vérifier l'identité de la personne voulant se connecter à distance, et sécurise ensuite la connexion en utilisant un algorithme de cryptographie symétrique.

PcAnywhere propose aussi différentes solutions pour garder des fichiers log pour des raisons de sécurité ou de dépannage. On peut penser notamment au fait d'enregistrer de l'information tel le nombre de tentatives erronées de connexion, combien de sessions d'accès à distance sont en cours ainsi que ceux qui sont connectés, ou bien si des fichiers d'une certaine importance ont été accédés. Le maintien de fichiers log peut se faire soit en local – c'est à dire soit sur l'ordinateur hôte, soit sur l'ordinateur client –, soit sur un autre ordinateur, soit sur un serveur central.

Le maintien de fichiers log en local est l'option par défaut offerte par le logiciel qui, pour ce faire, nous laisse le choix entre utiliser des fichiers log du type PcAnywhere ou du type *Windows Event Viewer*. Une particularité que l'on trouve dans le système de maintien de fichiers log du type PcAnywhere est que certains évènements sont stockés sur l'ordinateur hôte alors que d'autres le sont sur l'ordinateur client, selon que ce sont des évènements initiés par l'hôte ou par le client. Le concept d'évènement initié par l'hôte peut paraître un peu perturbant vu qu'il n'y a personne derrière l'ordinateur hôte pour être à l'origine de ces évènements. Au fait, un évènement initié par l'hôte serait par exemple l'impression, sur une imprimante du côté client, d'un document se trouvant sur l'ordinateur hôte [Imran].

En utilisant un système de maintien de fichiers log de type *Windows Event Viewer*, nous avons même la possibilité d'enregistrer les fichiers log sur un autre ordinateur. Evidemment l'utilisation de ce système de maintien de fichiers log requiert un système d'exploitation Microsoft Windows aussi bien sur l'ordinateur générateur des fichiers que sur l'ordinateur récepteur.

Mais, comme nous l'avons mentionné auparavant, nous pouvons également enregistrer les fichiers log sur un serveur central sécurisé. Ceci permet de protéger les fichiers log de plusieurs ordinateurs en même temps et évite aussi d'encombrer les ordinateurs avec ces informations. Pour enregistrer ces données sur un serveur central, nous avons le choix entre utiliser une méthode propre à PcAnywhere ou bien utiliser le protocole SNMP. Bien évidemment, le fait d'utiliser le protocole SNMP dépend surtout des ressources existantes dans l'infrastructure informatique de l'entreprise.

Si PcAnywhere présente certains avantages, il existe néanmoins certains désavantages. Notamment, ce logiciel coûte environ 200$ avec des mises à jour payantes en sus, auquel il faut rajouter tous les coûts indirects de déploiement et maintenance. Mais outre le coût, le logiciel présente des problèmes lorsqu'il est confronté à un routeur et la technologie NAT qui y est éventuellement utilisée.

Vu que la connexion est initialisée de l'extérieur, PcAnywhere ne peut savoir quelle est l'adresse IP de l'ordinateur hôte se trouvant derrière le routeur. Afin de remédier à ce problème, l'utilisateur est obligé de configurer le routeur pour "mapper" l'adresse IP privée de l'ordinateur hôte à deux ports utilisés par PcAnywhere ; le port TCP 5631 pour les données et le port UDP 5632 pour le statut. Ainsi le routeur pourra correctement rediriger les données vers l'ordinateur hôte.

Si l'on veut pouvoir accéder à plus d'un ordinateur derrière le routeur, il faut à ce moment là installer le Symantec PcAnywhere Gateway qui permettra d'établir jusqu'à cinq connexions TCP/IP simultanées. Evidemment, ce genre de manipulation requiert l'intervention de l'administrateur réseau lorsqu'on dépasse le cadre d'un réseau personnel et que l'on se trouve dans une entreprise.

Le même genre de problème apparaît lorsque PcAnywhere est confronté à un pare-feu. Un des buts premiers d'un pare-feu étant d'empêcher des connexions non autorisées à partir de l'extérieur vers le réseau interne se trouvant derrière le pare-feu, l'utilisateur distant doit disposer d'un moyen pour se connecter à ce réseau pour pouvoir accéder à l'ordinateur hôte. Ceci peut se faire soit par le biais d'un Remote Access Service (RAS) soit par le biais d'un Virtual Private Network (VPN). Dans le cadre d'une entreprise, l'intervention de l'administrateur réseau est à nouveau requise.

Sources : [PcAny], [PcAny UM], [Imran]

2.3 LogMeIn (3am Labs)

3am Labs propose quatre solutions d'accès à distance, à savoir LogMeIn Pro, LogMeIn Backup, LogMeIn Rescue, et LogMeIn IT Reach. 3am Labs offre même une version gratuite de son logiciel mais qui, bien évidemment, ne donne droit qu'à une période d'essai de LogMeIn Pro.

La différence entre les quatre solutions d'accès à distance se situe surtout au niveau du but recherché par l'utilisateur. Ainsi, LogMeIn Pro permet de contrôler un ordinateur personnel à distance tandis que LogMeIn Backup sert plutôt d'utilitaire de synchronisation de fichiers entre plusieurs ordinateurs afin de pouvoir récupérer des fichiers en cas de suppression ou non fonctionnement de ceux-ci. Pour les deux dernières solutions, la première, LogMeIn Rescue, est une solution du type *helpdesk* qui permet de dépanner des clients de façon réactive, c'est-à-dire lors de la survenance de certains problèmes, tandis que la deuxième, LogMeIn IT Reach, est plutôt orienté vers une résolution proactive, c'est-à-dire avant même l'apparition des problèmes pour empêcher qu'ils n'aient lieu.

En utilisant LogMeIn Pro, les utilisateurs auront accès à plusieurs fonctionnalités dont la possibilité de contrôler l'ordinateur hôte, transférer des fichiers de n'importe quelle taille entre l'ordinateur hôte et client, synchroniser les fichiers et répertoires des deux ordinateurs, et même imprimer localement des fichiers distants. Mais avant d'en dire plus, il serait souhaitable de parler des composants de LogMeIn.

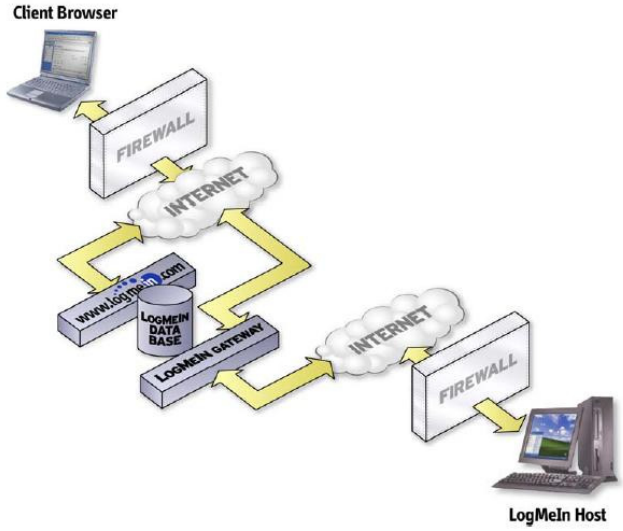


Fig. 2.2 – Les différents composants de LogMeIn [LMI security]

Comme nous pouvons le remarquer dans la figure 2.2, à part l'ordinateur client et l'ordinateur hôte, nous apercevons l'existence de 3 autres composants :

- Le site web de LogMeIn. Lorsqu'un utilisateur veut accéder à un ordinateur distant, il s'authentifie auprès du site web de LogMeIn en se loguant avec son nom d'utilisateur et mot de passe. Une fois l'utilisateur connecté, sa demande d'accès à un ordinateur hôte est transmise à un des serveurs LogMeIn Gateway qui mettra les deux ordinateurs en communication.

- Une base de données. C'est ici que sont stockées toutes les informations concernant les utilisateurs clients enregistrés auprès de LogMeIn ainsi que les ordinateurs hôte auxquels ces utilisateurs voudront accéder par la suite. C'est également dans cette base de données que sont répertoriés les droits d'accès aux différentes fonctionnalités pour chaque utilisateur.

- Les serveurs LogMeIn Gateway. Les serveurs LogMeIn Gateway servent à faire le lien entre un ordinateur client et l'ordinateur hôte qu'il essaye d'atteindre. Une fois l'ordinateur hôte allumé, il initie une connexion SSL avec un serveur LogMeIn Gateway pour signaler son état actif et il maintient cette connexion par la suite. Lorsqu'un ordinateur client demandera à accéder à cet ordinateur hôte, c'est le serveur LogMeIn Gateway qui s'occupera de transmettre les informations entre ces deux ordinateurs. Notons que l'ordinateur client devra quand même s'authentifier à nouveau auprès de l'ordinateur hôte et que le serveur LogMeIn Gateway ne fait que les mettre en communication l'un avec l'autre.

Un avantage assez important que procure LogMeIn est le fait qu'il ne faille pas manipuler ou modifier la configuration courante du routeur ou du pare-feu, et ceci que ce soit du côté client ou hôte. Ceci est possible grâce au fait que c'est aussi bien l'ordinateur client que l'ordinateur hôte qui initialisent les connexions sortantes ouvertes lors de chaque accès à distance.

Au niveau de l'authentification, elle se fait à plusieurs reprises et à plusieurs niveaux. Lorsqu'un utilisateur arrive sur le site web de LogMeIn et se logue, il sera ensuite en communication avec un des serveurs LogMeIn Gateway. Afin d'authentifier ses serveurs

auprès des utilisateurs, LogMeIn procède à une authentification sur base de certificats électroniques. Une fois l'authentification opérée, une clé de chiffrement est générée et partagée entre l'ordinateur client et un des serveurs pour sécuriser l'échange de données entre eux. Par la suite, il est conseillé aux utilisateurs d'activer une méthode d'authentification plus avancée pour se connecter au LogMeIn Gateway ou à l'hôte.

Parmi ces méthodes se trouve le *one-time password*. La façon dont LogMeIn a décidé de mettre en œuvre cette méthode consiste à obliger l'utilisateur à imprimer une liste de mots de passe aléatoires, générés automatiquement par le LogMeIn Gateway. Ainsi, à chaque fois que l'utilisateur se connecte, il devra fournir un des mots de passe qu'il n'aura pas encore utilisés ; une nouvelle liste de mots de passe est renvoyée à l'utilisateur avant qu'il ne tombe à court de mots de passe. Cette façon de procéder nous semble assez absurde vu qu'un mot de passe perd tout son intérêt lorsqu'il se trouve imprimé sur une feuille de papier ! L'autre méthode d'authentification, plus sûre, consiste en l'envoi d'un mot de passe, à usage unique et ayant une durée de vie déterminée, sur le téléphone portable de l'utilisateur distant. Ainsi, dès que celui-ci se sera logué, il recevra un mot de passe envoyé par le LogMeIn Gateway qui ne sera plus valable après un certain délai ou une fois que l'utilisateur l'aura utilisé.

Du côté de l'ordinateur hôte, on authentifie d'abord les serveurs LogMeIn Gateway auprès de l'ordinateur hôte qui voudra établir une connexion avec celui-ci, afin de pouvoir signaler son état actif. Cette authentification se fait de la même manière qu'elle se faisait pour l'ordinateur client, c'est-à-dire par l'utilisation de certificats électroniques. A l'inverse, lorsque l'ordinateur hôte accepte une demande d'accès à distance, le serveur LogMeIn Gateway vérifie l'identité de l'ordinateur hôte selon un identifiant, sous forme d'un long string. C'est le serveur qui attribue cet identifiant à l'ordinateur hôte lorsque ce dernier établit la première connexion avec le serveur. L'identifiant n'est communiqué que via un canal sécurisé par SSL et seulement après que l'ordinateur hôte ait authentifié le serveur. Tel le système de *one-time password* utilisé pour l'utilisateur client, ce moyen d'authentification n'est pas des plus efficaces non plus. En effet, a priori, rien n'empêcherait une personne malveillante de se faire passer pour un ordinateur hôte auprès du serveur LogMeIn Gateway.

Et pour finir, afin d'authentifier l'utilisateur distant auprès de l'ordinateur hôte, on a recours au *Windows Authentication*. Ce moyen d'authentification consiste simplement à entrer le nom d'utilisateur ainsi que le mot de passe qui sont habituellement utilisés lorsque l'utilisateur se logue sur l'ordinateur hôte en étant physiquement sur place. Afin de rajouter une couche supplémentaire de sécurité, LogMeIn a fait en sorte qu'il soit compatible avec l'utilisation de la technologie SecurID de RSA Security.

Au niveau de l'encryption des données, le choix entre plusieurs algorithmes de chiffrement différents est offert par LogMeIn. Les algorithmes disponibles sont le RC4 à 128 bits, le 3DES à 168 bits, l'AES à 128 ou l'AES à 256 bits. Lorsque l'ordinateur client se connecte à un des serveurs LogMeIn Gateway, ils se mettent d'accord sur l'algorithme le plus sûr. Ainsi, l'ordinateur client enverra la liste des algorithmes qu'il accepte d'utiliser et le serveur choisira celui qu'il préfère, a priori le plus sécurisé.

Pour ce qui est du système de fichiers log, les informations propres au logiciel sont enregistrées dans le répertoire d'installation sur l'ordinateur hôte. Quant aux informations les plus importantes, telles les connexions ou déconnexions, elles sont également enregistrées en tant qu'évènements dans le *Windows Event Viewer*. Il est également possible d'envoyer les informations à un serveur central de type Syslog[38].

[38] C'est-à-dire qu'il est possible d'avoir un serveur qui garderait les messages log qui lui sont envoyés par tout ordinateur qui implémente le protocole Syslog. Pour plus d'information, le fonctionnement du protocole Syslog est développé dans le RFC 3164, *The BSD Syslog Protocol*.

Un gros désavantage de LogMeIn c'est qu'il ne fonctionne que pour des ordinateurs hôte ayant un système d'exploitation de Microsoft Windows. On peut néanmoins accéder l'ordinateur hôte à partir d'un ordinateur ayant n'importe quel système d'exploitation pour autant qu'il ait une connexion Internet ainsi qu'un navigateur. A part ça, il faut compter un abonnement d'à peu près 13$ par mois.

Sources : [LMI], [LMI security]

2.4 NX (NoMachine)

NX, un logiciel développé par NoMachine, est une solution d'accès à distance qui offre le même genre de fonctionnalités que les solutions précédentes. Néanmoins, ce logiciel se distingue assez fortement des autres solutions.

Premièrement, l'aspect qui différencie NX le plus par rapport à d'autres solutions d'accès distant est le fait que NX n'offre ce type de solutions que pour des ordinateurs ayant un système d'exploitation de type Linux ou Solaris ; et donc pas pour Microsoft Windows! Plus précisément, NX consiste en un composant client, avec lequel on accède à l'ordinateur distant, et un composant serveur, avec lequel on rend accessible l'ordinateur hôte ; c'est ce second composant qui n'est pas disponible pour Windows. En effet, si NoMachine a développé une série de composants clients aussi bien pour Windows que pour Linux, Mac OS X, et Solaris, elle n'a développé des composants serveurs qui ne peuvent être installés que sur Linux[39] ou Solaris[40].

Néanmoins, NoMachine offre quand même la possibilité d'accéder à un Windows Terminal Server par l'intermédiaire du composant serveur. Donc un utilisateur voulant accéder à un application Windows distante pourrait le faire en utilisant le composant client NX pour se connecter à un composant serveur NX (donc installé sur Linux ou Solaris) qui servira de passerelle pour atteindre le Windows Terminal Server.

NX offre la possibilité de pouvoir exécuter des applications à interface graphique à travers n'importe quelle connexion réseau, comme si nous nous trouvions physiquement en face de l'ordinateur distant. Cela veut dire qu'il est même possible d'établir un accès à distance à travers une connexion par modem analogique ; un des objectifs prioritaires lorsque cette solution fut développée. Cette performance est possible grâce à l'utilisation d'un niveau de compression remarquable ainsi que l'utilisation du système *X-Window*, auxquels nous pouvons ajouter une intégration avec les capacités performantes d'audio, d'impression, et de partage des ressources provenant du monde Unix. A ceci s'ajoute le fait que NX est tout à fait compatible avec le protocole SMB, ce qui rend possible l'échange de fichiers entre deux ordinateurs ayant des systèmes d'exploitation différents et qui ne sont normalement pas compatibles. Ainsi, nous pourrions penser à l'échange de fichiers entre un ordinateur hôte Linux et un ordinateur client Windows ou Mac OS X.

NX arrive également à rediriger de façon transparente les sorties multimédia de Linux, ce qui offre une fonctionnalité supplémentaire, mais plutôt amusante qu'utile. En effet, ceci

[39] Plus précisément des versions de SuSE, RedHat, Mandriva, Debian, et quelques autres distributions, qui ont étés développées autour des noyaux Linux 2.2, 2.4, ou 2.6 (valable pour des architectures de microprocesseurs de type i386 ou AMD 64)

[40] Plus précisément les versions 8, 9, et 10 de Solaris

permettrait l'utilisateur de pouvoir exécuter la lecture de fichiers mp3 sur le serveur et en entendre la musique en étant derrière l'ordinateur client.

Ce qui est également assez surprenant chez NoMachine, c'est que les composants client et serveur sont disponibles gratuitement! Mais pour les versions de NX destinées à une utilisation en entreprise, les fonctionnalités les plus importantes qui sont normalement présentes dans le composant serveur, ne seront disponibles que pendant une période d'essai de 30 jours[41]. Néanmoins, la version de NX destinée à une utilisation personnelle n'est pas affectée par cette politique, donc un utilisateur pourrait installer et utiliser NX sans aucun frais. En revanche, c'est au moment où apparaissent les problèmes que ça devient payant.

En effet, NoMachine propose un système d'abonnement annuel payant qui en retour permettra à l'entreprise de pouvoir être dépanné par les experts chez NoMachine. Cet abonnement lui permettra aussi de pouvoir à nouveau utiliser certaines fonctionnalités qui auraient été désactivées à la fin de la période d'essai. L'entreprise pourra également télécharger les dernières mise à jour ou *patches* de sécurité et être avertie lorsque ces fichiers seront disponibles. Différents types d'abonnements sont disponibles et leurs prix peuvent varier entre à peu près 425$/an et à peu près 5 500$/an selon le nombre d'utilisateurs ou d'ordinateurs qui seront couverts par l'abonnement. C'est donc un système forfaitaire pour lequel un utilisateur sera dépanné autant de fois que nécessaire pendant un an à partir du moment où il aura payé.

Néanmoins, si l'utilisateur ne veut pas prendre un abonnement et qu'il rencontre quand même un problème qu'il n'arrive pas à résoudre, NoMachine offre aussi la possibilité de payer par intervention. Ceci coûterait à peu près 125$ par intervention.

Du côté du composant serveur, NoMachine a implémenté un serveur X standard qui se charge d'encoder le protocole X11 de manière efficace et d'envoyer le résultat au composant client. Donc, a priori, n'importe quelle application utilisant le protocole *X-Window* pour l'affichage à l'écran devrait être compatible avec NX sans avoir à recourir à des modifications quelconques. Mais vu le grand nombre d'implémentations différentes qui ont été faites du système *X-Window* ainsi que la difficulté de déployer de manière efficace une application *X-Window* à travers l'Internet, il se peut que des problèmes apparaissent avec certaines applications[42]. Néanmoins, NoMachine est continuellement en train d'améliorer la compatibilité de NX avec le plus d'applications possible.

En ce qui concerne l'accès à distance à un Windows Terminal Server, les informations passant du serveur Windows au serveur NX sont transmises en utilisant le protocole RDP (Remote Desktop Protocol). Le protocole RDP étant un protocole propre à Windows, le composant serveur NX s'occupe de traduire les informations qui utilisent ce protocole vers leur équivalent sous le protocole X-11 pour ensuite les envoyer au composant client NX.

NX paraît être une solution d'accès à distance idéale. Ce n'est pas le cas évidemment pour ceux qui préfèrent Microsoft Windows, mais ça l'est clairement pour les partisans de l'*open source* ou pour les particuliers qui sont limités au niveau du budget. NX a également l'avantage d'offrir de bonnes performances même via des liaisons de faible bande passante.

[41] Il est tout de même possible de télécharger à nouveau le composant serveur au bout de la période de 30 jours d'essai.

[42] Pour l'instant, NX garantit être compatible avec les applications Mozilla Firefox et Thunderbird, Sun OpenOffice et StarOffice, Novell Evolution, KDE Konqueror, GNOME Nautilus, et les environnements de bureau KDE, GNOME, et CDE ainsi que la plupart de leurs applications.

Quant au système de paiement pratiqué par NoMachine, il est certes inhabituel mais pourrait être fort avantageux avec le système de paiement par intervention.

Sources : [NX]

2.5 VNC (RealVNC)

VNC, qui signifie Virtual Network Computing, est une solution d'accès à distance qui a été développée par les fondateurs de l'entreprise RealVNC. Cette solution est disponible sous trois versions, à savoir la Free Edition, la Personal Edition, et l'Enterprise Edition.

Cette solution permet de prendre le contrôle d'un ordinateur éloigné peu importe le système d'exploitation de l'ordinateur hôte ou client. Un utilisateur pourrait donc très bien accéder à son poste de travail au bureau qui tourne sur Linux, à partir de son ordinateur domestique qui tourne sur Windows. L'ordinateur distant pourrait même être accessible à partir d'un PDA, avec la seule condition que le PDA ait assez de mémoire RAM. Pour plus de facilité, un *viewer* Java est même fourni pour permettre de contrôler un ordinateur à distance à partir de n'importe quel navigateur Internet compatible avec Java, donc sans l'obligation d'installer un logiciel supplémentaire.

VNC peut donc être utilisé à plusieurs fins, que ce soit pour l'administration ou la maintenance de systèmes informatiques, ou bien pour se connecter au réseau de l'entreprise à partir de la maison ou en étant sur la route. En plus, ce logiciel offre la possibilité de connecter plusieurs utilisateurs sur le même ordinateur hôte. Dans un contexte éducatif, cette fonctionnalité pourrait, par exemple, être utilisée afin de reproduire l'écran de l'enseignant sur l'écran des différents étudiants, ou bien l'enseignant pourrait contrôler l'ordinateur d'un étudiant pour l'aider lorsqu'il rencontre un problème. Un avantage supplémentaire est que la taille de ce logiciel est assez basse, variant entre 721 K et 2.7M dépendant de la plateforme sur laquelle il sera installé. Néanmoins, VNC présente le désavantage de nécessiter une configuration du pare-feu pour qu'il puisse fonctionner correctement.

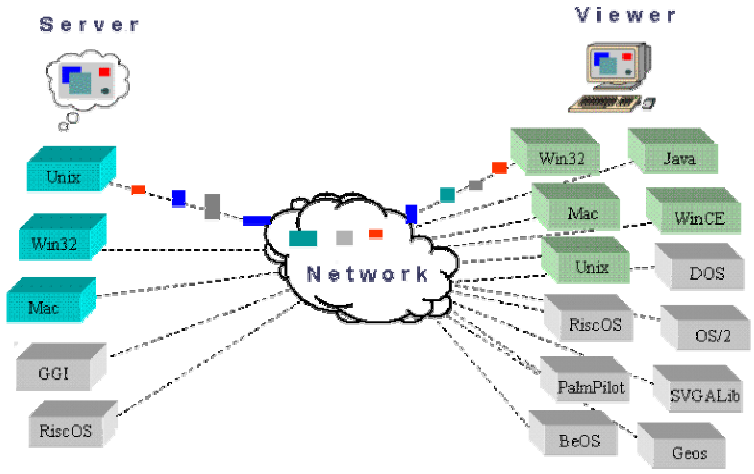


Fig. 2.3 – Les composants serveur et client de VNC selon le système d'exploitation [VNC]

VNC consiste en un composant serveur qui est installé sur l'ordinateur hôte, ainsi que le client ou *viewer* qui est installé sur l'ordinateur distant. Comme nous pouvons le voir à la

figure 2.3 ci-dessus, ces composants sont disponibles pour toute une série de systèmes opérationnels différents grâce à un protocole simple et indépendant des systèmes d'exploitation. Nous parlons là du protocole RFB (Remote Frame Buffer) qui permet l'interopérabilité entre différents systèmes d'exploitation et logiciels qui font usage d'un système de fenêtrage. En bref, ce protocole fonctionne par l'envoi des données correspondant à ce qui est affiché sur l'ordinateur hôte, vers l'ordinateur distant, afin de reconstituer cet affichage pour l'utilisateur distant. Une fois que le client aura reçu l'affichage complet de l'écran distant, par la suite il suffira de lui envoyer les informations correspondant qu'aux changements qui auront eux lieu par rapport à l'écran de l'ordinateur hôte.

C'est également ce protocole qui permet que le composant *viewer* puisse être *stateless*, c'est-à-dire que si la connexion entre l'ordinateur hôte et l'ordinateur distant est rompue, il n'y a pas de perte de données et il suffira à l'utilisateur distant de se reconnecter pour reprendre ses activités.

VNC est disponible gratuitement (Free Edition) avec une série de fonctionnalités limitée[43], ainsi qu'en versions payantes, les Personal et Enterprise Editions, qui offrent davantage de fonctionnalités et surtout plus de sécurité. Par exemple, ces deux versions payantes offrent la possibilité de transférer des fichiers entre l'ordinateur hôte et l'ordinateur distant, ce qui n'est pas possible avec la version gratuite.

D'un point de vue sécurité, ces versions payantes offrent une encryption AES de 128 bits pour sécuriser la communication et une authentification de l'ordinateur hôte par utilisation de clés RSA de 2 048 bits. Quant à l'authentification de l'utilisateur distant par contre, elles n'offrent qu'une authentification sur base de noms d'utilisateur et de mots de passe qui ont une taille maximale de 256 caractères chacun.

Afin de se connecter au composant serveur, il faut tout d'abord que l'utilisateur distant entre l'adresse IP ou le nom de l'ordinateur hôte. A ce moment-là, le serveur requerra l'authentification du client en lui demandant son nom d'utilisateur ainsi que son mot de passe. Ensuite, les composants serveur et client s'échangeront des messages afin de paramétrer la résolution des écrans, le format des pixels qu'ils s'échangeront[44], et l'encodage des informations qui sera utilisé. Après cela, le client fait une demande d'envoi de l'affichage complet de l'écran de l'ordinateur hôte et la session peut commencer.

A première vue, VNC parait également être une bonne solution d'accès à distance. Seulement, si les utilisateurs potentiels de cette solution n'ont pas les moyens d'acquérir une des deux versions payantes, l'utilité de VNC s'en voit nettement réduite. En effet, vu le peu de sécurité offert par la VNC Free Edition contre des attaques potentielles lors d'un accès à distance par Internet, le seul intérêt que pourrait présenter cette version gratuite serait un déploiement sur un réseau interne privé. Quant aux versions payantes, il faut investir 30$ (Personal Edition) ou 50$ (Enterprise Edition) pour chaque composant serveur qui sera installé.

Sources : [VNC], [VNC RFB]

[43] Néanmoins, une version *open source* existe depuis 1998 et est comprise dans toute une série de distributions de Linux.

[44] En effet, les pixels peuvent être envoyés sous différents formats, par exemple en *true colour* de 24, 16, ou 8 bits [VNC RFB].

2.6 Comparaison des solutions

Après avoir parcouru les différentes informations concernant les solutions d'accès à distance traitées lors de ce chapitre, nous proposons un tableau (cfr. figure 2.4) qui synthétise toutes ces informations afin de pouvoir mieux comparer les solutions entre elles.

A partir de ce tableau, nous pouvons constater qu'il est tout à fait possible de se procurer une solution d'accès à distance gratuite qui offre néanmoins des mécanismes de sécurité suffisants que pour protéger la connexion et les données qui y transitent. Nous constatons également qu'il n'existe pas de rapport entre le coût minimum d'une solution et la variété de mécanismes de sécurité qu'elle offre. Quant aux fichiers log, on remarque qu'il n'existe pas vraiment de pratique commune quant à l'emplacement de ces derniers.

2.6.1 Critères de comparaison

Le tableau ci-dessus fut basé sur neuf critères de comparaison. Ces différents critères sont repris ci-dessous afin d'en expliquer leur signification.

Version gratuite : indique si une version gratuite de la solution d'accès à distance est disponible

Coût : coût minimum pour les versions payantes[45]

Plateforme : - Serveur : les systèmes d'exploitation pour lesquels un composant serveur existe
- Client : les systèmes d'exploitation pour lesquels un composant client existe

Configuration nécessaire : indique si une configuration est nécessaire vis-à-vis du pare-feu, routeur, etc

Installation client : indique si l'installation d'un composant client est nécessaire

Autonomie : indique si la performance de la solution d'accès à distance dépend de l'existence et de la pérennité du fabricant

Encryption : indique les différents algorithmes d'encryption qui sont mis à disposition par la solution d'accès à distance

Authentification : indique les différents mécanismes, permettant une authentification, qui sont proposés par la solution d'accès à distance

Fichiers log : indique l'emplacement de stockage des fichiers log

[45] Ce champ est donc également applicable aux solutions d'accès à distance qui offrent une version entièrement gratuite.

2.6.2 Tableau comparatif

		GoToMyPC	PcAnywhere	LogMeIn	NX	VNC
Version gratuite		Evaluation 30 jours	Non	Oui	Oui	Oui[46]
Coût		Minimum 19,95$/mois	Paiement unique de 199,95$	Minimum 12,95$/mois	Minimum 35,38$/mois ou 125$/intervention	Paiement unique de minimum 30$
Plateforme	**Serveur**	Windows uniquement	Windows, Linux, Mac OS X	Windows uniquement	Linux, Solaris	Windows, Linux, Mac OS X, etc
	Client	Navigateur*	Windows, Linux, Mac OS X	Navigateur*	Windows, Linux, Mac OS X, Solaris	Navigateur*
Configuration nécessaire		Non	Oui	Non	Non	Oui
Installation client		Non	Oui	Non	Oui	Au choix[47]
Autonomie		Non	Oui	Non	Oui	Oui
Encryption		AES 128 bits	PcAnywhere, AES 256 bits, RC4, publique	3DES 168 bits, AES 128 bits, AES 256 bits, RC4 128 bits	SSL	AES 128 bits
Authentification		*One-time password*	PcAnywhere, *directory server*, certificats électroniques, RSA SecurID	*Windows Authentication*, *One-time password*, certificats électroniques, RSA SecurID	SSH	RSA 2 048 bits
Fichiers log		Citrix[48]	Client, serveur, autre ordinateur, serveur central	Serveur	Serveur	Serveur

Fig. 2.4 – Tableau comparatif des différentes solutions d'accès à distance

* Ces solutions d'accès à distance font usage d'un navigateur Internet comme composant client, ceci implique que tout système d'exploitation supportant des navigateurs est supporté par ces solutions

[46] Notons néanmoins que cette version gratuite ne comporte aucune protection des données et n'est donc pas d'une très grande utilité.
[47] L'utilisateur distant peut choisir d'installer un composant client ou utiliser un navigateur Internet.
[48] Les fichiers log sont stockés sur des serveurs se trouvant chez Citrix, le fabricant de GoToMyPC.

Chapitre 3 : Normes et recommandations

Chaque jour, de plus en plus de questions liées à la sécurité des réseaux et des systèmes d'information apparaissent. On découvre à peine la solution à un problème qu'un autre apparaît. Dès qu'on arrive à mettre en place des moyens pour se protéger des différentes menaces qui existent, d'autres moyens sont élaborés pour contourner cette protection. Lorsque les dernières mises à jour sont distribuées pour réparer les failles d'un système d'exploitation, une nouvelle version de ce système d'exploitation, avec de nouvelles failles, surgira. Evidemment, ce genre de problèmes empêche le bon fonctionnement des systèmes d'information ou une bonne utilisation des réseaux informatiques.

3.1 Contexte

Les mondes des réseaux informatiques et des systèmes d'information étant en mouvement perpétuel, il n'est pas possible de trouver une solution une bonne fois pour toutes. Par conséquent, lorsqu'on veut établir des normes ou des règles, il faut que ce soit fait de manière générique, de façon à pouvoir couvrir le plus de cas possibles en une fois. C'est pour cette raison que nous ne trouvons que rarement des lois ou des normes spécifiques à un genre d'attaque ou de faille.

3.1.1 L'importance des normes

Lorsqu'il s'agit d'un utilisateur isolé qui se fait voler des informations stockées sur son disque dur, les dégâts paraissent assez limités. Mais lorsqu'il s'agit d'une attaque sur le site web d'un commerçant électronique et que des milliers de numéros de cartes de crédit sont récupérés, on peut facilement deviner toutes les utilisations frauduleuses, possibles et imaginables, qui seront le résultat d'une telle attaque.

Nous voyons donc immédiatement l'importance de la mise en place d'une protection des réseaux et des systèmes d'information contre de telles attaques. D'ailleurs, l'importance de la sécurité des réseaux et des systèmes d'information se fait sentir de plus en plus de par le nombre croissant d'utilisateurs ainsi que les transactions qu'ils exécutent [SSI netsec]. Cette importance est aussi accentuée par le fait que l'Internet "constitue l'un des moteurs essentiels de la productivité des économies de l'UE" [SSI netsec].

3.1.2 Les acteurs

Vu que les services de communication sont généralement offerts par des entreprises privées et vu le caractère global de l'Internet, on pourrait se dire que le rôle des gouvernements est assez limité en ce qui concerne la sécurité des réseaux [SSI netsec]. Mais ceci n'est pas justifié. En effet, il existe déjà, au niveau européen, des obligations pour les opérateurs et fournisseurs de services à offrir une certaine sécurité, qui soit en adéquation avec les services qu'ils offrent [SSI netsec]. D'un côté, la Commission Européenne estime que le fait que les opérateurs privés soient en concurrence devrait faire en sorte que les opérateurs augmentent d'office le niveau de sécurité qu'ils offrent afin de pouvoir se distinguer de leurs concurrents [SSI netsec]. Mais en même temps, la Commission Européenne avoue que, les

investissements en matière de sécurité s'avérant très coûteux, il se pourrait qu'à l'inverse, les opérateurs réduisent leurs mécanismes de sécurité afin d'être plus attirants au niveau du prix de leurs services [SSI netsec]. Il est donc clair qu'un minimum de régulation est nécessaire de la part des autorités des différents pays.

3.1.3 Choix des normes

La suite de ce chapitre analysera les normes et régulations qui régissent la sécurité des réseaux informatiques et systèmes d'information. Néanmoins, vu la quantité de normes qui existent en la matière et pour différents pays, et vu que ceci n'est pas le thème principal de ce mémoire, nous avons préféré nous limiter à l'analyse d'un nombre restreint de normes. Nous analyserons notamment des normes provenant de la Commission Européenne et du Conseil de l'Union Européenne, du CEN (Comité Européen de Normalisation), du VPNC (Virtual Private Network Consortium), et de l'ISO (International Standards Organization). Du point de vue de la Commission Européenne, le Conseil de l'Union Européenne et le CEN, les normes proposées sont plutôt génériques et traitent le sujet de l'accès à distance indirectement. Les normes provenant de la part du VPNC sont plus spécifiques aux VPNs, tandis que les normes ISO traitent spécifiquement le sujet de l'accès à distance.

3.2 Normes issues de la Commission et du Conseil de l'Union Européenne

En ce qui concerne la sécurité des réseaux informatiques, elle est définie par la Commission Européenne comme étant "la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, aux événements accidentels ou aux actions malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité des données stockées ou transmises et des services connexes que ces réseaux et systèmes offrent ou qu'ils rendent accessibles" [SSI netsec].

3.2.1 Exigences de sécurité

A partir de la définition de la sécurité des réseaux informatiques que nous venons de citer, nous pouvons remarquer les quatre exigences qui sont requises pour pouvoir déclarer qu'un réseau ou un système d'information soit sûr. Ces quatre exigences sont la disponibilité, l'authentification, l'intégrité et la confidentialité [SSI netsec]. La Commission Européenne définit ces quatre exigences comme suit :

> " **Disponibilité** – Signifie que les données sont accessibles et les services opérationnels, même en cas d'événements perturbants tels que des pannes de courant, des catastrophes naturelles, des accidents ou des attaques. Cette caractéristique est particulièrement importante lorsqu'une défaillance du réseau de communication peut provoquer des pannes dans d'autres réseaux critiques tels que les transports aériens ou la fourniture d'électricité.
>
> **Authentification** – Confirmation de l'identité supposée d'entités ou d'utilisateurs. Des méthodes d'authentification appropriées sont nécessaires pour de nombreux services et applications, comme la conclusion d'un contrat en ligne, le contrôle de l'accès à certains services et données (pour les télétravailleurs, par exemple) et l'authentification des sites Web (pour les banques Internet, par exemple). L'authentification doit également inclure la possibilité de rester anonyme, dans la mesure où de nombreux services ne nécessitent pas l'identité de l'utilisateur, mais seulement la confirmation de certains critères (pièces justificatives anonymes), telle la capacité de paiement .

Intégrité – Confirmation que les données qui ont été envoyées, reçues ou stockées sont complètes et n'ont pas été modifiées. Ceci est particulièrement important pour l'authentification en vue de la conclusion de contrats ou quand l'exactitude des données est nécessaires (données médicales, design industriel, etc).

Confidentialité – Protection des communications ou des données stockées contre l'interception et la lecture par des personnes non autorisées. La confidentialité est particulièrement nécessaire pour la transmission des données sensibles et constitue une des exigences pour aborder les problèmes de protection de la vie privée des utilisateurs des réseaux de communication. " [SSI netsec].

Ces exigences visent à protéger les réseaux de communication des intentions malveillantes que pourraient avoir certains utilisateurs, mais elles prennent également en compte tout incident non malveillant et non intentionnel. Parmi les intentions malveillantes, nous pouvons distinguer différentes catégories d'attaques tel l'interception des communications, l'accès non autorisé à un ordinateur ou à des informations, la perturbation des réseaux, l'exécution de logiciels malveillants et les déclarations mensongères [SSI netsec]. Parmi les incidents non malveillants et non intentionnels se trouvent les désastres naturels, des pannes de courant, des erreurs humaines, etc [SSI netsec]. La Commission Européenne propose également des "solutions envisageables" pour chacune de ces attaques.

3.2.2 Interception de communications

Pour ce qui est des interceptions de communications, elle propose que les opérateurs protégent leurs réseaux conformément à la directive 97/66/CE et que les utilisateurs utilisent des mécanismes d'encryption pour les données qu'ils enverront à travers le réseau [SSI netsec]. De cette façon, avec la sécurité renforcée qui serait mise en place par l'opérateur, il sera plus difficile d'arriver à intercepter des communications. De plus, avec l'encryption qu'utiliseraient les utilisateurs, même si une communication est interceptée malgré la sécurité accrue, les données seraient incompréhensibles pour l'intercepteur. C'est notamment avec cette encryption que nous pouvons garantir la confidentialité au travers des réseaux informatiques.

Evidemment il existe différents moyens pour garantir l'encryption des données mais aucun de ces moyens n'est imposé en tant que norme ou standard [SSI netsec]. Tel est le cas par exemple pour S-MIME et OpenPGP, qui peuvent tous les deux être utilisés pour sécuriser le courrier électronique, mais le choix d'utiliser l'un ou l'autre repose entièrement entre les mains des correspondants[49] [SSI netsec].

Néanmoins, si en général les autorités n'imposent pas l'utilisation de mécanismes d'encryption spécifiques, il y a de plus en plus de gouvernements de l'Union Européenne qui se tournent vers une utilisation de logiciels libres d'encryption dans toutes leurs institutions gouvernementales. C'est surtout la révélation de l'existence du système étasunien ECHELON[50] qui motive l'utilisation croissante d'outils d'encryption issus du monde des logiciels libres, par les gouvernements européens qui craignent un espionnage de la part du gouvernement étasunien [SSI netsec]. En effet, l'avantage du logiciel libre est le fait que le code source peut être consulté à tout moment, ce qui permet de vérifier que l'outil

[49] C'est-à-dire que l'émetteur et le destinataire se mettront d'accord sur l'outil d'encryption/désencryption qu'ils utiliseront par la suite pour protéger les messages qu'ils s'échangeront.

[50] Ce système permettrait au gouvernement étasunien d'intercepter les courriers électroniques, communications téléphoniques, etc [SSI netsec].

d'encryption ne présente pas de failles dans l'algorithme de chiffrement, ni qu'il y ait des *backdoors*[51] incorporées.

L'interception de communications est devenu une infraction pénale punissable par l'article 3 de la "décision-cadre du Conseil [de l'Union Européenne] relative aux attaques visant les systèmes d'information" [SSI com2002173]. Néanmoins, les interceptions peuvent être considérées comme étant légales dans un nombre limité de cas où cette mesure est considérée comme étant nécessaire, justifiée, et proportionnée [SSI CrimeCom].

3.2.3 Accès non autorisé

Afin d'empêcher des accès non autorisés à des ordinateurs ou à des informations, les utilisateurs se contentent généralement d'installer des pare-feux ou d'utiliser de simples mots de passe [SSI netsec]. N'offrant qu'un niveau de sécurité limité, ces moyens seuls sont considérés insuffisants par la Commission Européenne qui propose donc de compléter ces moyens par l'utilisation d'autres contrôles de sécurité tels la reconnaissance d'attaques, la détection d'intrusions et des contrôles au niveau des applications [SSI netsec]. C'est par l'intermédiaire de ces moyens qu'on pourra assurer l'authentification qu'exige la Commission Européenne. Evidemment, le degré de sécurité nécessaire dépendra des activités des utilisateurs [SSI netsec]. Ainsi, lorsqu'il s'agira d'une page web personnelle, le propriétaire de cette page web pourra se contenter de protéger son site par un simple mot de passe. Ce n'est pas le cas lorsqu'il s'agira de la page web d'un commerçant électronique, qui est tout de suite une cible beaucoup plus attirante, pour des personnes malveillantes, qu'une page web personnelle. Dans le cas du commerçant électronique il est clair que l'investissement en un mécanisme plus sécurisé pour sa page web ne sera pas une perte d'argent!

Quoiqu'il en soit, vu les avancées technologiques ainsi que les nouvelles menaces qui apparaissent, il faut régulièrement revoir le système de sécurité qui a été mis en place afin de minimiser les possibilités d'accès non autorisés aux ordinateurs ou aux informations qui y sont contenues [SSI netsec].

L'accès intentionnel et non autorisé à des ordinateurs ou aux informations qui y sont contenues est devenu une infraction pénale punissable par l'article 3 de la "décision-cadre du Conseil [de l'Union Européenne] relative aux attaques visant les systèmes d'information" [SSI com2002173].

3.2.4 Perturbation des réseaux

Par la perturbation des réseaux, nous entendons toute attaque visant à rendre indisponible un réseau informatique. Ceci peut se faire à travers l'exploitation des faiblesses et vulnérabilités que peuvent présenter certains composants d'un réseau tel des routeurs, systèmes d'exploitation, etc. Ainsi on peut penser à des attaques contre des serveurs DNS, des attaques contre le système de routage, ou bien des attaques de saturation et refus de service [SSI netsec]. C'est bien évidemment pour combattre ce genre d'attaques que la Commission

[51] Une *backdoor*, ou *trapdoor*, est une "porte de derrière" dans un système d'information qui permettrait à une personne tierce de pénétrer dans ce système sans avoir l'autorisation nécessaire. Ce fut le cas par exemple, lorsque Microsoft avait incorporé une *backdoor* dans Windows NT pour le compte de la NSA (National Security Agency) aux Etats-Unis, ce qui a effrayé pas mal de gouvernements étrangers [HEISE]. Au niveau des outils d'encryption, une *backdoor* permettrait de déchiffrer un message sans avoir la clé de chiffrement requise.

Européenne inclut la disponibilité parmi les exigences de sécurité pour les réseaux informatiques.

En ce qui concerne les attaques contre les serveurs DNS, la Commission Européenne ne fait que constater que "le processus administratif nécessaire pour accroître la confiance entre les domaines DNS doit devenir plus efficace" [SSI netsec]. Par contre, en ce qui concerne les attaques contre les systèmes de routage, la Commission Européenne avoue qu'il "n'existe aucun moyen efficace de sécuriser les protocoles de routage" et aucune solution n'est proposée pour les attaques de saturation et de refus de service [SSI netsec].

Les perturbations des réseaux sont devenues des infractions pénales punissables par l'article 4 de la "décision-cadre du Conseil [de l'Union Européenne] relative aux attaques visant les systèmes d'information" [SSI com2002173].

3.2.5 Exécution de logiciels malveillants

Lorsque nous parlons de l'exécution de logiciels malveillants, il s'agit de logiciels qui donnent lieu à une modification ou une destruction des données lorsque ce logiciel est exécuté [SSI netsec]. Ce type de logiciel malveillant est plus couramment connu sous le nom générique de "virus". Ce sont donc des logiciels antivirus qui sont utilisés afin d'empêcher que des virus ne modifient ou ne détruisent les données des utilisateurs. Parmi les logiciels antivirus nous trouvons deux types différents ; il y a ceux qui identifient et suppriment les virus par le biais d'une liste de virus connus à l'avance, et puis il y a ceux qui contrôlent l'intégrité du système en détectant des modifications faites par n'importe quel virus, qu'il soit connu ou pas [SSI netsec]. Nous trouvons ici l'exigence de sécurité de l'intégrité des réseaux informatiques, tel que suggérée par la Commission Européenne.

Malgré l'existence d'outils de défense contre les virus, il ne cesse d'y avoir des problèmes de virus dus, d'une part, à la facilité avec laquelle les pirates peuvent s'échanger les informations à travers l'Internet, et d'autre part, à l'arrivée de nouveaux utilisateurs d'Internet qui ne sont pas forcément au courant des dangers présents sur Internet. La seule façon de combattre les virus est d'utiliser ces logiciels antivirus de façon appropriée et de se tenir à jour, ce qui requiert également que les utilisateurs d'Internet soient mis au courant des menaces qu'ils pourraient rencontrer [SSI netsec]. D'ailleurs, le Conseil de l'Union Européenne propose de renforcer ou promouvoir davantage les notions de sécurité dans l'enseignement de l'informatique [SSI res15152].

L'exécution de logiciels malveillants est devenu une infraction pénale punissable par l'article 4 de la "décision-cadre du Conseil [de l'Union Européenne] relative aux attaques visant les systèmes d'information" [SSI com2002173].

3.2.6 Déclaration mensongère

Une autre intention malveillante est celle des déclarations mensongères. Nous entendons par la tout ce qui consiste en l'usurpation d'identité[52], *spoofing*[53], *phishing*[54], etc.

[52] Le fait de se faire passer pour une personne en particulier.
[53] Le fait de cacher son identité en se faisant passer pour n'importe quelle autre personne.
[54] Le fait de créer, par exemple, un site web pareil à un autre, afin de le faire passer comme étant le véritable site web pour soutirer des informations sensibles, tel des numéros de carte de crédit, des utilisateurs habituels du premier site web.

C'est à cause de ces déclarations mensongères qu'un meilleur niveau d'authentification est exigé dans les réseaux informatiques, en plus d'exiger la confidentialité et l'intégrité des données lorsque les informations transmises sont de caractère sensible.

La Commission Européenne recommande l'utilisation de VPNs basés sur SSL ou IPsec mais elle mentionne également le fait que ces solutions, reposant sur des certificats électroniques, n'offrent aucune garantie quant à l'identité du détenteur du certificat électronique à moins de faire usage des autorités de certifications [SSI netsec]. La Commission Européenne nous dirige vers la directive sur les signatures électroniques afin de rendre plus claires les exigences spécifiques à l'authentification électronique ; ces exigences visent, bien sûr, l'élaboration de signatures électroniques qui soient plus sûres, notamment d'un point de vue de leur reconnaissance juridique [SSI netsec].

3.2.7 Incidents non malveillants et non intentionnels

Au niveau de tous ces désastres naturels qu'il est possible de rencontrer (désastres naturels, pannes de courant, etc.), la Commission Européenne exige des Etats membres, par la Directive Interconnexion 97/33/CE et la Directive Téléphonie Vocale 98/10/CE, qu'ils veillent à ce que leurs réseaux publics soient disponibles à tout moment, même après qu'un de ces désastres naturels a causé la coupure du réseau [SSI netsec]. Quant aux erreurs humaines, la Commission Européenne propose comme solution des actions de formation et de sensibilisation auprès des utilisateurs ainsi que l'établissement de politiques de sécurité au niveau des entreprises [SSI netsec].

3.2.8 Recommandations

Les actions que la Commission Européenne estime les plus importantes du point de vue de chaque Etat membre, sont surtout la sensibilisation des utilisateurs[55] par rapport aux risques liés à l'Internet ainsi qu'une accentuation sur les cours de sécurité dans les systèmes éducatifs [SSI netsec]. En ce qui concerne la sensibilisation aux dangers d'Internet, quatre groupes sont visés 1) les enseignants, 2) le grand public (notamment les parents et les enfants), 3) les pouvoirs publics et le milieu des medias, et 4) les entreprises (en particulier les "créateurs, assembleurs, et diffuseurs de contenus en ligne") [SSI com2002152].

Une autre action également proposée, est que chaque Etat membre encourage l'adoption de meilleures pratiques de sécurité, notamment auprès des petites et moyennes entreprises, en se basant sur des normes reconnues [SSI res15152]. Parmi les normes les plus importantes en matière de sécurité informatique se trouvent les normes ISO-18028 et ISO-17799. Ces normes seront analysées à la section 3.5 du présent chapitre.

La Commission Européenne encourage aussi l'élaboration de systèmes d'alerte et d'information par rapport aux menaces de l'Internet [SSI netsec]. De tels systèmes existent déjà au niveau des Etats membres individuels et sont généralement connus sous le nom de CERT (Computer Emergency Response Team) et la coordination entre ces CERT au niveau mondial est assurée par la CERT/CC (CERT Coordination Center). La Commission Européenne propose donc que les Etats membres renforcent les compétences et les équipements de leurs systèmes CERT, et lorsqu'un réseau CERT sera convenablement établi à

[55] D'ailleurs, l'article 4 de la directive 97/66/CE requiert que tous les fournisseurs de services de télécommunications informent leurs clients des risques présents sur leur réseau ainsi que la façon dont ils peuvent se protéger de ces risques [SSI netsec].

travers l'Union Européenne, elle propose d'étendre ce réseau à d'autres systèmes à travers le monde [SSI netsec]. Le CEN, dont nous reparlerons plus tard, recommande également l'utilisation à grande échelle des systèmes CERT [CEN nisissue]. Néanmoins, la Commission ne néglige pas non plus la nécessité de continuellement faire des recherches dans le monde de la sécurité informatique, notamment la cryptographie.

Mais à part la recherche, il est surtout très important d'établir une normalisation et une certification des mécanismes de sécurité afin de garantir l'interopérabilité lorsque deux utilisateurs veulent communiquer l'un avec l'autre. Nous pouvons penser par exemple à l'initiative Européenne en ce qui concerne la normalisation des signatures électroniques, EESSI (European Electronic Signature Standardization Initiative), ou bien des initiatives qui visent à promouvoir des cartes à puces ou la mise en œuvre d'infrastructures de clé publique, PKI (Public Key Infrastructure). La Commission Européenne propose également qu'une législation soit adoptée afin de rapprocher les droits pénaux nationaux en ce qui concerne toute attaque informatique tel que le piratage, attaques de refus de service, etc. [SSI netsec]

3.2.9 Normes existantes

En termes de régulation il en existe déjà une série qui se manifestent au travers de certaines lois et textes législatifs. Tel est le cas en ce qui concerne la vie privée par exemple. En effet, la protection de la vie privée a été reconnue comme un droit fondamental dans l'article 8 de la Convention Européenne des Droits de l'Homme ainsi que dans les articles 7 et 8 de la Charte des Droits Fondamentaux de l'Union Européenne. Ces deux derniers articles précisent même que ce droit inclut "la vie privée et familiale, du domicile, des *communications* et des données à caractère personnel". [SSI netsec]

Pour plus de précision, nous pouvons également nous tourner vers l'article 5 de la directive sur la protection des données dans le secteur des télécommunications. En effet, cet article exige que les Etats membres assurent la confidentialité au travers des réseaux publics de télécommunications et que les fournisseurs de services et de réseaux publiques mettent en œuvre les moyens techniques et organisationnels nécessaires pour assurer la sécurité de leurs services et réseaux. [SSI netsec]

Selon l'article 17 de la directive générale sur la protection des données 95/46/CE, les responsables des réseaux et systèmes d'information sont obligés de mettre en œuvre les moyens techniques et organisationnels pour faire face à l'accès non autorisé, la destruction, la modification, et la diffusion des données, que ces actions soient accidentelles ou illicites [SSI netsec].

3.3 Normes issues du CEN

Du côté du CEN (Comité Européen de Normalisation), nous pouvons retrouver les mêmes principes que cités précédemment. En effet, le CEN a établi une série d'exigences générales de sécurité en ce qui concerne les utilisateurs individuels, les PME, ainsi que les grandes entreprises et l'industrie.

3.3.1 Les acteurs

Pour ce qui est des utilisateurs individuels, on considère qu'ils sont généralement peu familiers avec les notions de sécurité informatique. Le CEN propose donc d'établir des *checklists* de sécurité afin de promouvoir la conscience des utilisateurs par rapport aux dangers qu'ils risquent de rencontrer. [CEN nisissue]

Ces derniers n'étant pas toujours capables d'assurer la confidentialité et l'intégrité de leurs données personnelles, le CEN encourage également tous les fournisseurs d'accès Internet à fournir à leurs clients des services de sécurité de base, tels que des pare-feux ou un filtrage des virus se trouvant dans le courrier électronique. Cette recommandation ne vise pas à déresponsabiliser l'utilisateur individuel, mais veut protéger ce dernier lors des transactions qu'il effectuera en ligne. [CEN nisissue]

Les fournisseurs d'applications, de systèmes d'exploitation, etc. sont également conviés à faire en sorte que leurs produits résistent aux attaques tels des virus ou des tentatives d'intrusion de *hackers*. En ce qui concerne l'employé travaillant à domicile, son employeur devrait lui fournir des solutions avec un bon niveau de sécurité tels des VPNs ou des moyens d'encryption de point à point. [CEN nisissue]

Pour ce qui est des PME, elles ont généralement tendance à moins se préoccuper des aspects de sécurité informatique que les grandes multinationales, arguant qu'il s'agit là d'un investissement trop lourd. Le CEN propose donc également d'"éduquer" les PMEs aux risques de l'Internet ainsi qu'aux solutions qui existent pour les contrer.

En ce qui concerne les grandes entreprises par contre, elles sont généralement plus au courant de la nécessité d'avoir un bon niveau de sécurité, mais n'ont pas toujours les ressources nécessaires pour le mettre en œuvre. Néanmoins, elles sont généralement plus aptes à investir en des mécanismes de sécurité et pourront chercher conseil en matière de standards, d'évaluation des risques, etc. [CEN nisissue]

3.3.2 L'accès à distance

En ce qui concerne l'accès à distance, afin de pouvoir se protéger contre d'éventuelles attaques, le CEN encourage la mise en place de services d'authentification et de confidentialité.

Avec l'authentification nous cherchons à pouvoir nous assurer que l'utilisateur distant est bien la personne qu'il prétend être, et ainsi il n'aura accès qu'aux informations et ressources pour lesquelles il est accrédité. Sans une authentification adéquate, toute la sécurité offerte par les mécanismes mis en place pourrait tomber à l'eau. Néanmoins, il ne s'agit pas de simplement mettre en place un mécanisme d'authentification, il faut également s'assurer de l'interopérabilité de ce mécanisme afin que ce même mécanisme puisse être utilisé pour n'importe quelle transaction. [CEN nisissue]

L'aspect de la confidentialité assure le transfert des informations de manière sûre et secrète. De cette manière, l'interception des informations lors d'un accès à distance ne présentera aucun danger pour le réseau ou le système d'information. A cette fin, le CEN met en avant l'utilisation de mécanismes d'encryption symétrique et asymétrique. Pour ce qui est du courrier électronique, il met en avant le S-MIME (qui peut utiliser une encryption DES, 3DES, RC2, et RSA) ainsi que le PGP. En ce qui concerne les communications au travers des réseaux en général, il propose l'utilisation de TLS/SSL ainsi que d'IPsec. [CEN nisissue]

3.4 Normes issues de VPNC

En ce qui concerne spécifiquement les VPNs, il existe un organisme, appelé le VPNC (Virtual Private Network Consortium), qui a pour but d'accroître l'interopérabilité entre les différentes solutions proposées et de promouvoir les échanges entre les différents membres. Nous voyons donc qu'il y a également des organismes non publics qui contribuent à l'élaboration de normes, à la seule différence que les normes publiques s'appliquent généralement à un zone géographique déterminée alors que les normes privées visent généralement une application globale. VPNC a notamment posé certaines exigences quant aux contenus des différentes solutions de VPNs disponibles.

3.4.1 VPNs de confiance

En ce qui concerne les VPNs de confiance, il faut que personne d'autre ne puisse influencer la modification ou la création d'un circuit dans le VPN de confiance à part le ou les fournisseurs de VPN de confiance. Il en est de même en ce qui concerne le flux de données au travers du VPN ; il faut que personne d'autre ne puisse insérer, modifier ou supprimer des données passant par un circuit dans le VPN. Finalement, il faut aussi que le client ainsi que le fournisseur du VPN de confiance se mettent d'accord sur le routage et l'adressage qui sera utilisé dans le VPN de confiance avant que celui-ci ne soit établi. Par ailleurs, le VPNC n'accepte que les circuits ATM, les circuits *Frame Relay* ou bien le MPLS comme technologie utilisé afin de fournir un VPN de confiance. [VPN Consortium]

3.4.2 VPNs sécurisés

Afin qu'un VPN puisse être considéré comme un VPN sécurisé, il faut que tout le trafic qui le traverse soit encrypté et authentifié. Malheureusement, il existe plusieurs VPNs qui se disent être des VPNs sécurisés alors qu'ils n'offrent aucune encryption ; ces VPNs n'offrent donc aucune confidentialité et par conséquent ne peuvent être considérés comme des VPNs sécurisés. Lors de l'établissement d'un VPN, il faut également que les aspects de sécurité fassent l'objet d'un accord entre les deux entités communicantes et il devrait donc être impossible pour une personne tierce de pouvoir effectuer des changements à ces aspects de sécurité. Du point de vue de la technologie se trouvant derrière les VPNs sécurisés, le VPNC n'accepte qu'IPsec avec encryption, IPsec au dessus de L2TP ou TLS/SSL avec encryption. [VPN Consortium]

3.4.3 VPNs hybrides

Lorsqu'il s'agit d'un VPN hybride il y a une exigence supplémentaire qui est celle d'avoir une séparation nette entre la partie du VPN de confiance qui est sécurisée et la partie qui ne l'est pas. De cette manière l'administrateur du VPN sera en mesure de dire si la communication entre n'importe quelle paire d'adresses IP est sécurisée ou pas. Du point de vue technologique il est évident que, pour établir un VPN hybride, le VPNC accepte l'utilisation de toute technologie acceptée pour les VPNs sécurisés, au dessus de toute technologie acceptée pour les VPNs de confiance. [VPN Consortium]

3.5 Normes issues de l'ISO

L'ISO (International Standards Organization) est une autre organisation non gouvernementale qui à pour but d'établir des standards mondiaux. Seulement, à la différence de VPNC, l'ISO ne s'occupe pas que d'un domaine spécifique en informatique mais tente de mettre en place des normes internationales qui touchent à toute une série de secteurs différents.

3.5.1 ISO-18028

La première suggestion faite par la norme ISO-18028 est que tout accès à distance devrait être traité par un serveur d'accès à distance au lieu de faire un accès direct aux différents ordinateurs. Ceci s'explique par le risque accru que présenterait le deuxième scénario. [ISO 18028]

Lors d'un accès à distance, plusieurs risques peuvent se présenter, à savoir : il se peut que des personnes non autorisées arrivent à avoir accès à l'ordinateur hôte et/ou à l'ordinateur client, ou bien il se peut que ces personnes puissent avoir intercepté et/ou modifié les informations échangées entre deux entités. La norme ISO-18028 pose certaines exigences afin d'empêcher que ce genre d'évènements ait lieu. [ISO 18028]

3.5.2 ISO-18028 et l'authentification

La première de ces exigences est celle d'une authentification permettant d'identifier, de manière unique, l'utilisateur distant, et cette authentification devrait se faire à chaque établissement de connexion. Cette authentification peut être menée à bien au biais de divers mécanismes tel des *one-time passwords*. Evidemment, il existe des mécanismes plus simples, comme le simple login avec le mot de passe associé, ainsi que des mécanismes plus sophistiqués, comme l'authentification biométrique. Une fois la connexion établie, la politique de droits d'accès et restrictions, qui est normalement en place, devrait aussi s'appliquer aux utilisateurs distants afin qu'ils n'aient pas un accès illimité au système local. [ISO 18028]

Lorsque l'accès à distance est d'une certaine importance pour l'entreprise, dans le cadre du télétravail par exemple, il faut également assurer la disponibilité du service d'accès distant. Cette disponibilité peut être offerte par la mise en place d'un système alternatif ou redondant du service d'accès distant en cas de panne générale ou partielle de ce dernier. [ISO 18028]

3.5.3 ISO-18028 et la protection des données

La norme ISO-18028 encourage aussi fortement la mise en place d'une protection des données qui seront échangées vu qu'elles peuvent être de caractère sensible. Cette protection devrait inclure la confidentialité, l'intégrité, et l'authentification des données. Afin de rencontrer ces trois critères, la norme en question propose l'utilisation de trois technologies : TLS/SSL, IPsec et SSH[56]. [ISO 18028]

[56] SSH, ou Secure SHell, est un protocole qui permet un accès distant sécurisé au travers d'un réseau non sécurisé. Lorsque la phase d'authentification a été réussie, une connexion sécurisée est établie avec l'ordinateur distant. [ISO 18028]

Lorsqu'il s'agit d'un accès distant pour des raisons de maintenance, il est fortement suggéré de maintenir des fichiers log dans lesquels sont enregistrées toutes les activités menées à distance. On insiste d'autant plus sur cette suggestion lorsque les activités de maintenance sont sous-traitées à une partie tierce. Il est également conseillé de faire un audit sur ces fichiers log immédiatement après qu'a eu lieu l'intervention à distance de maintenance. [ISO 18028]

3.5.4 ISO-18028 et la sécurité

Lorsqu'un employé travaille à distance avec un ordinateur portable et qu'il accède au réseau de son entreprise, l'ordinateur portable qu'il utilise est le composant qui présente le plus de risques pour la sécurité de l'entreprise. Il convient donc de protéger cet élément le mieux possible, selon l'importance et la sensibilité des données qui sont échangées.

Afin d'effectuer cette protection, plusieurs mécanismes existent. La norme ISO-18028 conseille tout d'abord de mettre en place un mot de passe au niveau *boot* ainsi qu'au niveau du système d'exploitation, et que le compte de l'utilisateur distant ne soit pas un compte administrateur mais un compte d'utilisateur normal [ISO 18028]. Evidemment, en ce qui concerne les mots de passe, il est impératif qu'ils soient choisis de manière intelligente afin qu'ils ne puissent pas être facilement devinés par une tierce personne, mais d'autres moyens d'authentification peuvent également être utilisés (comme mentionné précédemment).

Ensuite, il est également conseillé de protéger les données se trouvant sur le disque dur en les cryptant ainsi qu'en installant et en gardant à jour des programmes anti-virus. Et lorsque l'accès à distance se fait par l'intermédiaire d'un modem, il est fortement conseillé de configurer le modem pour ne pas accepter les appels entrants. [ISO 18028]

En ce qui concerne la sécurité au niveau des serveurs d'accès distant, ça se limite en général à une protection physique et contre des pannes de courant. Ainsi, la norme ISO-18028 conseille de garder les serveurs d'accès distant dans des pièces isolées, et équipées de générateurs d'électricité en cas de pannes de courant, auxquelles l'accès est restreint à un nombre réduit d'utilisateurs de confiance. [ISO 18028]

3.5.5 ISO-17799

La norme ISO-17799 dicte qu'aucun accès à distance ne devrait être permis avant qu'un contrôle adéquat ne soit mis en place, par exemple, un contrat d'utilisation acceptable de l'accès à distance, statuant les conditions pour l'accès. Il faut donc que la partie accédant à distance soit au courant de ses obligations et qu'elle accepte ses responsabilités telles quelles sont décrites dans le contrat mentionné précédemment. [ISO 17799]

3.5.6 ISO-17799 et les contrats d'obligations

Dans les contrats d'obligations, il est conseillé d'inclure une clause permettant à la partie accédée de révoquer les droits d'accès à certaines informations pour certaines personnes. La partie accédée devrait aussi être capable d'interrompre la connexion entre les deux systèmes. La norme ISO-17799 conseille également d'ajouter une clause garantissant la confidentialité, l'intégrité, et la disponibilité des informations du côté de la partie accédée. [ISO 17799]

Cette norme propose aussi d'inclure une mention par rapport au droit qu'a la partie accédée de surveiller et interrompre n'importe quelle activité de la partie distante qui soit liée

aux informations détenues par la partie accédée. Plus spécifiquement, cette surveillance devrait garder une trace des évènements liés à la sécurité, les problèmes opérationnels, les pannes de fonctionnement du système, etc, afin d'assurer l'intégrité des données et du système de la partie accédée. La partie accédée a également le droit de demander un audit des activités menées à bien par la partie distante, et cet audit devrait être effectué par une tierce partie. Le but de cette surveillance est de pouvoir détecter des activités de traitement d'informations qui n'auraient pas été autorisées préalablement par la partie accédée. [ISO 17799]

Afin de garder une trace des activités menées à distance, il est conseillé d'utiliser un système de fichiers log, dans lesquels seront enregistrées toutes les informations liées à ces activités. L'objectif principal des fichiers log est certes de s'assurer que les politiques d'utilisation, ainsi que les obligations qui s'y trouvent, soient bien respectées, mais il ne faut tout de même pas négliger l'utilité que ces fichiers présenteront lorsqu'il s'agira d'identifier le plus rapidement possible les problèmes du système qui pourraient être présents. [ISO 17799]

3.5.7 ISO-17799 et les fichiers log

Idéalement, les fichiers log devraient inclure, lorsque c'est applicable, une identification de l'utilisateur sur la machine locale ainsi que son identification distante ou son emplacement si possible. A ceci devrait s'ajouter la date, l'heure, et les détails de chaque tentative de connexion/déconnexion à la machine distante ; parmi ces détails devraient se trouver des informations indiquant la réussite ou la non-réussite de ces tentatives. Il serait également important de savoir quels programmes et utilitaires ont été utilisés, les fichiers qui ont été accédés ainsi que le type d'accès et les privilèges qui ont été utilisés sans oublier les éventuels changements qui auraient été effectués par rapport à la configuration du système. D'autres informations importantes seraient les adresses et protocoles réseau utilisés, les éventuelles alarmes qui auraient été levées par le système de contrôle d'accès, et l'activation ou désactivation des systèmes de protection tel des programmes anti-virus et de détection d'intrusion. [ISO 17799]

Vu l'importance des informations contenues dans les fichiers log, il est impératif que ces informations soient protégées contre des accès ou modifications non autorisées. Plus spécifiquement, il ne devrait pas être possible de modifier ou supprimer les fichiers log ni les messages contenus dans ces fichiers. Lorsque c'est possible, il est également conseillé d'empêcher que les administrateurs système puissent être en mesure d'effacer ou de désactiver les fichiers log qui contiendraient leurs propres activités. Il faudrait aussi veiller à ne pas tomber à court d'emplacement mémoire, ce qui pourrait entraîner des erreurs d'enregistrement, voire même une écriture qui écraserait les anciens fichiers log. Il va de soi que les informations contenues dans les fichiers log peuvent parfois être superflues par rapport à une surveillance purement sécuritaire. Il peut donc être utile de mettre en place un système de filtrage des messages log afin de recopier dans un deuxième fichier log les messages les plus importants d'un point de vue sécurité.

Il est également conseillé de maintenir un fichier log séparé qui enregistrera les accès aux fichiers log principaux. En ce qui concerne l'accès aux fichiers log, ils ne devraient être accessibles qu'en lecture seule, mais une exception pourrait être faite pour des copies isolées des fichiers log. [ISO 17799]

Evidemment, toute activité de surveillance est soumise aux exigences des lois les concernant. Vu que les fichiers log seraient justement susceptibles de contenir des informations personnelles ou confidentielles, des mesures appropriées devraient être prises

afin d'être sûr de ne pas empiéter sur le droit à la vie privée des utilisateurs distants. [ISO 17799]

3.5.8 ISO-17799 et le télétravail

En ce qui concerne le télétravail, tout comme la norme ISO-18028, la norme ISO-17799 suggère la mise en place d'une protection physique de l'ordinateur portable, l'utilisation de mécanismes cryptographiques et de contrôle d'accès, ainsi qu'une protection anti-virus. Mais la norme ISO-17799 suggère également de mettre en place un système de back-ups réguliers dans la politique de télétravail. Cette politique devrait aussi inclure des règles et conseils, destinés aux télétravailleurs, quant à la façon de se connecter ainsi que les précautions à prendre lorsqu'ils se connectent dans des lieux publics. La norme ISO-17799 statue également que le télétravail ne devrait être possible qu'après une identification et authentification réussie de l'employé distant, sans oublier un mécanisme de contrôle d'accès adéquat. La norme insiste fortement sur l'importance de la formation des télétravailleurs afin de les sensibiliser aux dangers qu'ils pourraient rencontrer lors de leur travail à distance. [ISO 17799]

Chapitre 4 : L'accès à distance en pratique

Jusqu'à présent nous avons parcouru toute une série d'informations à un niveau théorique. Nous avons passé en revue les différents moyens d'établir un accès à distance, nous avons exposé certaines solutions qui existent déjà, et nous avons analysé différentes normes qui traitent ce sujet. Heureusement pour nous, toute cette théorie sur l'accès à distance a pu être mise en pratique lors du stage de fin d'études. En effet, nous avons eu l'occasion de tester une solution d'accès à distance mentionnée au chapitre 2 ainsi que de mettre en œuvre une autre solution d'accès à distance (vu la non adéquation de la première solution). L'objectif de ce chapitre est donc de montrer la façon dont une solution d'accès à distance est généralement déployée en pratique. A ceci s'ajoute le déploiement d'une solution d'accès à distance en présence de contraintes du terrain, telles qu'elles sont fréquemment rencontrés dans les pays en voie de développement.

4.1 Contexte

Le stage de quatre mois que nous avons effectué en début d'année s'est déroulé au Sénégal, plus précisément à Dakar, dans les bureaux d'une ONG belge du nom d'AQUADEV. Cette dernière est basée à Bruxelles et est impliquée dans le secteur du développement à plusieurs niveaux, notamment la micro finance, la sécurité nutritionnelle, ainsi que l'environnement en milieu urbain.

En ce qui concerne le domaine de la micro finance, AQUADEV a chargé son équipe de développement, basée à Dakar, de développer ADbanking, un "logiciel de gestion transactionnelle à destination des institutions de micro finance" [AQUADEV] des pays en voie de développement. C'est au sein de cette équipe de développement, et avec leur soutien, que s'est effectué le stage. Nous avons donc eu l'occasion de constater les difficultés que l'on rencontre généralement lorsque l'on met en place une solution informatique dans ce type de pays du tiers monde. Par la suite, nous utiliserons le terme AQUADEV pour parler de AQUADEV-Dakar, sauf mention explicite.

4.2 Objectifs du stage

La mise en place d'un d'accès à distance pouvait se faire de plusieurs manières vu les différentes solutions qui s'offrent à nous. Il fallait donc que la solution d'accès à distance remplisse certains objectifs tels que ceux repris ci-dessous, qui furent établis par M Laurent Schyns. La solution d'accès à distance devait fournir la possibilité de :

- Enregistrer toutes les manipulations effectuées à distance sur le système
- Authentifier le client par le serveur
- Crypter les données échangées
- Consulter, via une interface ou application simple d'utilisation (pour un non informaticien), la liste des interventions antérieures ainsi que les enregistrements des manipulations (mentionnés précédemment)

- Via la même interface, attribuer ou révoquer la permission d'intervenir à distance sur un serveur ADbanking, et ceci uniquement lorsque l'IMF propriétaire du serveur l'aura autorisé
- Ne pas attribuer plus de droits à l'intervenant à distance que le minimum nécessaire pour effectuer les manipulations demandées
- Couper la connexion manuellement du côté de l'IMF
- Couper la connexion manuellement du côté d'AQUADEV
- Couper la connexion automatiquement après un certain laps de temps

4.3 Installation et test de solutions d'accès à distance : NX

En fin de compte, nous avons choisi NX (cfr. chapitre 2) comme étant la solution d'accès à distance qui correspondait le mieux aux critères préalablement établis (voir annexe I). Nous avons donc installé et testé les performances de cette solution pour voir si elle était vraiment à la hauteur des objectifs visés.

4.3.1 Installation et fonctionnement

A l'époque où nous allions tester NX, le composant serveur pour Linux n'était pas encore facile à installer. Comme c'est souvent le cas pour les installations de logiciels *open source*, il fallait télécharger les différents composants d'NX, ainsi que les différentes librairies nécessaires, et "construire" le tout avant de pouvoir commencer l'installation. Heureusement pour nous, un certain Rick Stout avait créé des fichiers RPM[57], ce qui a grandement simplifié l'installation de cette solution d'accès à distance. Maintenant des fichiers RPM pour le composant client et serveur sont disponibles directement sur la page web de NoMachine.

Une fois l'installation faite, les tests de performance ont pu débuter. Afin de s'assurer qu'on arrivait à faire fonctionner NX, nous l'avons d'abord testé en communiquant avec des serveurs de test distants, se trouvant en Italie et en Allemagne, qui étaient mis à disposition par NoMachine. Au niveau de l'utilisation d'NX, la première chose à faire était de copier la clé publique du serveur sur l'ordinateur client. Ensuite, une fois que l'ordinateur client et l'ordinateur serveur étaient connectés au réseau, il suffisait d'ouvrir l'interface du composant client et démarrer la connexion en entrant les bons paramètres. Parmi ces paramètres se trouvaient, entre autres, l'adresse IP ou le nom de domaine de l'ordinateur serveur, le type de connexion (modem, ISDN, ADSL, WAN, LAN), la taille ou la résolution de la fenêtre qui afficherait l'écran du serveur, etc.

4.3.2 Test et évaluation

Une fois que nous avions compris comment fonctionnait NX, nous l'avons directement testé avec les contraintes du terrain, c'est-à-dire via modem analogique. Ce test a requis deux ordinateurs et un modem analogique (un des ordinateurs avait un modem directement incorporé). Sur le premier ordinateur nous avons branché le modem analogique qui a été relié au réseau téléphonique interne d'AQUADEV en empruntant la ligne téléphonique d'un des téléphones se trouvant dans le bureau. Le deuxième ordinateur fut directement relié au réseau téléphonique interne d'AQUADEV avec son modem incorporé. Une fois les deux ordinateurs

[57] Des fichiers d'installation automatique propres à la distribution Fedora.

reliés au réseau téléphonique interne, un des deux, l'ordinateur client, a été utilisé pour "appeler" l'autre, l'ordinateur serveur, par un *Dial-up*. Lorsque l'ordinateur serveur avait "répondu" à l'appel de l'ordinateur client, une liaison IP entre les deux ordinateurs a été automatiquement établie par le *Dial-up*. A ce moment là nous avons pu tester NX à travers cette liaison nouvellement créée, et cela a marché !

Afin de pouvoir évaluer la performance de NX via modem, nous l'avons comparé à la performance observée lorsqu'on utilisait NX pour communiquer avec les serveurs de test distants qui avaient été fournis par NoMachine. Dans les deux cas, une fois que la connexion était établie, et ayant choisi une résolution plein écran de l'écran de l'ordinateur distant, on se croyait vraiment derrière l'ordinateur serveur. Même si un des tests passait par Internet alors que l'autre passait par le réseau téléphonique interne d'AQUADEV, la différence ne se sentait presque pas ; la résolution était la même des deux côtés et pourtant la fréquence de rafraîchissement au niveau graphique était à peine plus lente pour l'"infrastructure modem" lorsqu'un programme était exécuté à distance. La seule réelle différence se sent au début, lorsque l'affichage complet de l'écran de l'ordinateur serveur est transmis à l'ordinateur client ; ceci prend plus de temps pour l'"infrastructure modem".

4.4 Résolution des problèmes

Deux problèmes ont été rencontrés lors du stage, néanmoins ces obstacles ont pu être contournés en implémentant une solution d'accès à distance alternative. Le premier problème concernait le fait que NX fonctionnait sur base d'interfaces graphiques, tandis que le deuxième problème concernait une incompatibilité de modems avec Linux (cfr. annexe I). Pour plus de facilité, nous traiterons d'abord le deuxième problème.

4.4.1 Incompatibilité modems et Linux

Au début de l'ère du modem analogique, le modem était un simple boîtier électronique dont l'utilité était de "traduire" des signaux analogiques (provenant de la ligne téléphonique) en signaux numériques (à destination de l'ordinateur), et vice versa. Mais la fin des années '90 a vu l'arrivée des *soft modems*[58]. Evidemment ce genre de technologie a donné lieu à la nécessité de pilotes pour faire fonctionner cette nouvelle génération de modems. Mais pendant longtemps, ces pilotes n'étaient disponibles que pour Windows[59], donc la plupart de ces nouveaux modems ne marchaient pas sous Linux. C'est précisément la nécessité d'avoir ces pilotes, qui est à l'origine des problèmes actuels au niveau de la compatibilité des modems sous Linux. En gros, si ce n'est pas un *linmodem*[60] ni un *hard modem*[61], ça ne fonctionnera pas sous Linux.

---

[58] Appelés aussi *controllerless modems*, les *soft modems* ont la particularité de déléguer une partie, voir même l'entièreté, de leur travail au CPU de l'ordinateur auquel ils sont raccordés (d'où la survenance d'autres noms tels *host-controlled modem* ou *host-based modem*). Ce genre de modem a l'avantage de coûter moins cher, vu qu'on peut se passer des composants électroniques, devenus de plus en plus complexes, qui faisaient auparavant le travail dorénavant exécuté par le CPU.

59 D'où l'apparition du nom *Winmodem* pour les modems qui ne sont compatible qu'avec Windows.

60 Le terme *linmodem* se réfère aux *soft modems* pour lesquels des pilotes ont pu être écrits pour assurer leur compatibilité sous Linux.

61 Le *hard modem*, étant l'opposé du *soft modem*, est le genre de modem qui n'a besoin d'aucun pilote pour fonctionner. La "traduction" analogique/numérique et vice-versa est assurée uniquement par les composants

Evidemment, de nos jours il est assez difficile de trouver des *linmodems*. D'ailleurs, après bon nombre de tentatives, de discussions, et de recherches pour faire reconnaître des modems sur des ordinateurs d'AQUADEV, nous nous sommes dit qu'il valait mieux essayer de trouver des hard modems. En même temps, l'achat de hard modems aurait permis d'éviter de perdre du temps à configurer les soft modems pour tourner sous Linux dans le cas où ils auraient été compatibles. Malheureusement, les hard modems étaient encore plus difficiles à trouver que les *linmodems*, même dans un pays en voie de développement.

Afin de contourner l'obstacle que présentait ce problème de modems, nous avons décidé de modifier le déploiement initialement prévu pour la solution d'accès à distance. Au début, il était prévu que l'ordinateur client communique directement avec l'ordinateur hôte, mais la seule façon de pouvoir faire cela requérait une version de Windows qui tourne sur ces deux ordinateurs. En ce qui concerne l'ordinateur client, c'est-à-dire l'ordinateur d'un des développeurs d'AQUADEV, cette condition ne posait pas de problème[62], mais ce n'est pas le cas pour l'ordinateur hôte, c'est-à-dire le serveur d'une IMF. En effet, le serveur d'une IMF ne peut tourner que sur Linux, par contre, les autres ordinateurs de l'IMF, qui font partie du même réseau local que le serveur, tournent sur Windows.

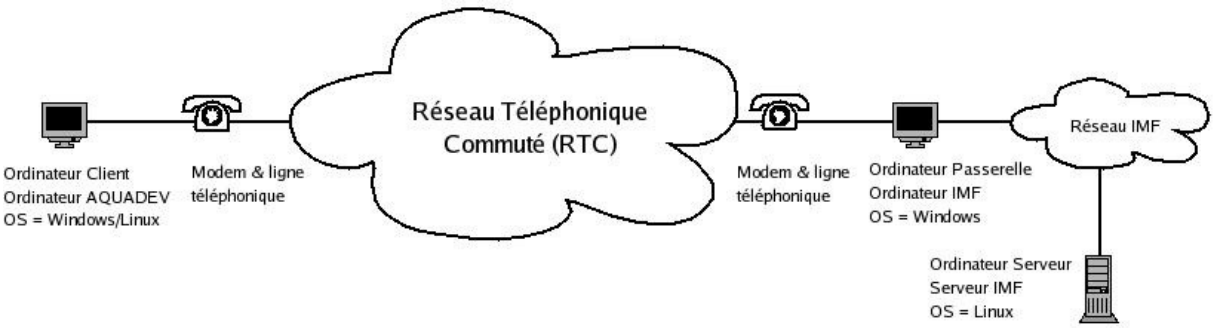


Fig. 4.1 – Déploiement alternatif de la solution d'accès à distance

C'est de cette constatation que nous est venue l'idée de bifurquer la liaison par un des ordinateurs du réseau local de l'IMF, un ordinateur "passerelle", pour pouvoir accéder au serveur (cfr. figure 4.1). Ainsi, lors de la survenance d'un problème, nous connecterions l'ordinateur client et l'ordinateur "passerelle" à des modems, qui eux sont reliés au RTC. A ce moment là, il suffirait à l'ordinateur client d'"appeler" l'ordinateur "passerelle", et une fois que ce dernier aura "répondu" et que la liaison sera établie, il suffirait d'établir la communication avec le serveur. Le seul problème qui reste à résoudre est de trouver l'outil qui permettrait d'établir cette communication.

4.4.2 Inadéquation de NX

A part le problème de modems, il y avait aussi le problème concernant le fait que les serveurs des IMFs n'avaient pas d'interface graphique installée. Par conséquent, ceci rendait NX inutilisable et non adéquat aux besoins exprimés initialement par AQUADEV. Il a donc fallu chercher une autre solution d'accès à distance, ce qui ne fut pas très difficile. En effet, lorsqu'une interface graphique n'est pas nécessaire, quel meilleur moyen d'établir un accès à distance qu'une connexion SSH ?

---

internes tels des circuits électroniques intégrés.

[62] Vu que les ordinateurs des développeurs sont tous *dual-boot* Windows/Linux (cfr. annexe I).

Le protocole SSH a l'avantage de nous permettre de nous connecter à un ordinateur distant avec le même nom d'utilisateur et mot de passe que celui que nous utiliserions pour nous loguer physiquement sur cet ordinateur distant. SSH présente aussi l'avantage de pouvoir encrypter la communication et permet une authentification sur base de clés publiques. Seulement, si un client SSH et un serveur SSH sont inclus dans toutes les versions de Linux, ce n'est pas le cas pour Windows. Néanmoins, il existe un client SSH qui est gratuit et presque aussi connu que le protocole SSH. Nous parlons ici de Putty. Quant au serveur SSH, il existe un émulateur Linux pour Windows pour lequel un package contenant un serveur SSH peut être téléchargé. Nous parlons ici de Cygwin. Ce sont ce client SSH et ce serveur SSH que nous avons incorporé dans la mise en place de notre solution d'accès à distance. Voilà donc la solution qui fut trouvée pour remplacer NX.

4.5 Implémentation finale d'une solution d'accès à distance

Ayant résolu les problèmes que nous avions rencontrés, nous avons pu mettre en place un mécanisme d'accès à distance qui fut établi en utilisant différents outils. En effet, une fois que nous pouvions établir la liaison entre l'ordinateur client et l'ordinateur "passerelle", il nous suffisait d'utiliser les utilitaires Putty et Cygwin pour créer une connexion SSH sécurisée entre ces mêmes ordinateurs. De cette manière nous pouvions être logués à distance sur l'ordinateur "passerelle" et il nous suffisait de refaire une connexion SSH sur le serveur de l'IMF vu qu'il se trouve sur le même réseau local que l'ordinateur "passerelle". Ainsi, la personne utilisant l'ordinateur client sera logué à distance sur le serveur et pourra y effectuer toutes les opérations nécessaires à la résolution du bug d'ADbanking ou du problème de base de données.

Evidemment, il ne faut pas oublier de créer des comptes d'utilisateurs, sur l'ordinateur "passerelle" et le serveur, pour l'équipe de développement d'AQUADEV afin qu'elle puisse se loguer sur ces machines pour finalement accéder au serveur de l'IMF. Néanmoins, en créant ces comptes d'utilisateurs, il faut faire bien attention à n'attribuer que le strict minimum de droits d'accès à ce compte d'utilisateur distant. Idéalement, ce compte ne devrait pas avoir plus de droits d'accès que ceux nécessaires pour dépanner le système distant.

Lors du stage, nous avions également pris soin de rédiger des documents qui serviraient de manuels d'utilisation pour la solution d'accès à distance finale que nous avions mis en place. Ces divers documents se trouvent dans les annexes. Le premier document, l'annexe II, est un document expliquant le déploiement et l'utilisation générale de la solution d'accès à distance. Les deux documents qui suivent expliquent comment procéder du côté de la partie contrôlante, annexe III, et du côté de la partie contrôlée, annexe IV[63]. Le dernier document, annexe V, explique comment configurer la partie contrôlée.

[63] Par partie contrôlante nous entendons la partie qui va accéder l'autre partie à distance. La partie contrôlée est celle qui va être accédée par la partie contrôlante.

Chapitre 5 : Lacunes et perspectives

Cela fait maintenant des années que l'accès à distance existe, et ceci sous diverses formes. Par conséquent, il existe un certain nombre de normes qui s'appliquent à tous les types d'accès à distance imaginables en proposant certaines bonnes pratiques à suivre. Ces normes et bonnes pratiques sont issues d'un désir d'empêcher, le plus possible, l'apparition de failles dans les systèmes d'accès à distance. Mais est-ce que l'application de ces normes et règles de bonne pratique suffit pour vraiment obtenir un niveau de sécurité permettant de se protéger de toute attaque? Evidemment la réponse est négative. L'objectif de ces normes est surtout de servir de recommandations pour qu'un niveau de sécurité convenable puisse être obtenu lors du déploiement du système d'accès à distance.

Le but ultime de tous les organismes qui émettent des normes est qu'un niveau minimal de sécurité soit adopté par le plus grand nombre possible d'utilisateurs afin d'augmenter la sécurité globale de l'immense réseau qu'est l'Internet. Certaines normes sont plutôt générales et s'appliquent indirectement à l'accès à distance tandis que d'autres ont été établies en vue de réguler de façon précise l'accès à distance. Quoi qu'il en soit, ces normes et recommandations ont été faites de manière à englober l'utilisation de toutes sortes de technologie afin de ne pas se limiter qu'à l'utilisation d'un certain nombre ou à un certain type de technologie. Néanmoins, nous trouvons qu'il y a tout de même des lacunes au niveau des normes et recommandations.

5.1 Lacune : maintien de fichiers log

Si la confidentialité, l'authentification, et l'intégrité sont mentionnées à plusieurs reprises, ce n'est que rarement le cas pour le maintien de ce qu'on appelle une "traçabilité". Par "traçabilité" nous entendons le fait de garder une "trace" des actions qui ont été effectuées par l'utilisateur accédant à distance à un ordinateur. Ces "traces" sont généralement enregistrées dans un fichier log, sous format texte, et permettent ainsi de pouvoir surveiller les actions menées par l'utilisateur distant. Bien évidemment, ces fichiers log peuvent être d'une très haute importance, dépendant du contexte.

Dans certains scénarios, il pourrait s'agir d'un jeune qui accède à l'ordinateur de ses parents pour leur montrer comment installer un logiciel antivirus. Il est évident que dans cette situation un certain niveau de confiance existe entre les deux parties et que les dégâts éventuels seraient minimes. L'importance des fichiers log s'en trouve réduit d'autant.

Par contre, lorsqu'il s'agit d'une grande société bancaire qui est accédée par une entreprise informatique pour entretenir son système informatique, pour faire une mise à jour, etc. il en va de soi que l'importance des fichiers log est beaucoup plus grande que dans le cas précédent. En effet, la société bancaire se trouve dans une situation à risque de part le fait qu'un tiers a accès à son système informatique. Mais les fichiers log garantiraient à la société bancaire que l'entreprise informatique puisse être tenue pour responsable en cas de toute tentative frauduleuse de sa part. Cependant, des recommandations détaillées concernant le maintien de fichiers log se trouvent rarement dans les normes liées à l'accès à distance, à l'exception des normes ISO-17799 et ISO-18028 évidemment.

5.2 Lacune : contenu des fichiers log

Si la traçabilité de l'accès à distance est parfois mentionnée dans certaines normes, ce n'est fait que de façon brève et simplifiée. En effet, aucune recommandation concrète n'est émise quant aux informations qui devraient être contenues dans les fichiers log, à part les heures de connexion et de déconnexion de l'utilisateur distant ainsi que la réussite ou l'échec de sa tentative de connexion. Mais il est clair que ce genre d'information n'est d'aucune utilité pour trouver l'auteur de faits délictueux lorsque le problème survient pendant que plusieurs utilisateurs sont connectés en même temps.

La façon dont sont rédigées les recommandations concernant les fichiers log dans ces normes, pourrait laisser croire aux administrateurs les moins expérimentés, notamment ceux qui sont responsables de la sécurité informatique, qu'il leur suffirait de garder la trace des heures de connexions et de déconnexions afin d'assurer un niveau de sécurité convenable. Mais la sécurité qu'offrirait cette politique de maintien de fichiers log est presque inexistante, c'est pourquoi certaines institutions préfèreront qu'une gamme d'informations plus vaste soit enregistrée, telles toutes les actions effectuées par l'utilisateur distant. Ceci peut inclure les fichiers que l'utilisateur a ouverts, les pages web qu'il aurait consultées, les programmes qu'il aurait exécutés, etc. Avec de tels fichiers log, il serait difficile d'arriver à commettre des actes répréhensibles sans se faire repérer. Néanmoins, vu que toutes les actions de l'utilisateur peuvent être enregistrées, il va de soi qu'une attention particulière doit être apportée au respect de la vie privée des utilisateurs qui seront ainsi surveillés.

Mis à part cet aspect, nous pouvons constater que le degré de traçabilité (déterminé par l'étendue des informations qui seront enregistrées) peut facilement être générateur de fichiers log d'une taille assez importante. Par conséquent, il serait judicieux de tenir compte de cet aspect lors l'établissement du *capacity planning*[64] de l'entreprise.

5.3 Lacune : emplacement des fichiers log

Une lacune supplémentaire peut être remarquée concernant la traçabilité de l'accès à distance, même lorsqu'elle est mentionnée dans les normes ISO-17799 et ISO-18028. En effet, aucune mention n'est faite quant à l'emplacement des fichiers log.

Habituellement les fichiers log sont stockés du côté de la partie accédée, que ce soit sur l'ordinateur hôte ou sur un serveur central qui regroupe les fichiers log pour un ensemble d'ordinateurs. Ainsi, lorsqu'une anomalie apparaît ou bien lors d'un audit préétabli, la partie accédée peut facilement consulter ses fichiers log afin de trouver l'origine du problème, voir même le coupable si c'est lié à une faute humaine. Il serait donc contre toute logique de stocker les fichiers log du côté de la partie distante vu qu'elle pourrait modifier ces fichiers pour cacher les erreurs qu'elle aurait commises. Mais tout risque n'est pas écarté lorsque les fichiers log sont stockés chez la partie accédée. En effet, on pourrait se dire qu'à partir du moment où la partie distante mène à bien des actes frauduleux sur l'ordinateur hôte auquel elle a accès, elle pourrait très bien essayer de modifier le contenu des fichiers log pour effacer toute trace de ses actes frauduleux.

[64] C'est-à-dire l'estimation des futurs besoins, en termes de ressources matérielles informatiques, d'une entreprise.

Il est logique que la partie accédée doit faire en sorte que son système de fichiers log soit inaccessible à l'utilisateur distant. Vu que ce dernier est obligé d'avoir un accès à l'ordinateur distant, en général il suffit de lui créer un compte utilisateur à part et ne donner le droit d'accès aux fichiers log qu'à certains utilisateurs tel des administrateurs.

Néanmoins, il persiste un risque vu que l'utilisateur distant a tout de même un accès, quoique partiel, à l'ordinateur hôte ; dans le cas où le mot de passe du compte administrateur/*root* est trop simple, l'utilisateur pourrait facilement avoir accès aux fichiers log. Afin de contourner ce problème, il suffirait de choisir un bon mot de passe mais, comme nous l'avons vu, on peut également accroître la sécurité des fichiers log en les stockant sur un serveur central où seront gardés les fichiers log de tous les ordinateurs qui sont accessibles à distance. Ainsi l'utilisateur distant n'aura même pas un accès partiel au serveur central. Evidemment, il se pourrait que l'utilisateur distant soit capable de localiser le serveur et tenter d'y accéder. Nous retrouvons donc à nouveau l'importance du choix d'un bon mot de passe, puisque généralement cette solution offrirait un niveau de sécurité plus que suffisant pour les fichiers log.

Quoi qu'il en soit, dans le monde de la sécurité informatique il est fortement conseillé de partir d'un point de vue paranoïaque afin d'être sûr de couvrir tous les scénarios *worst case*. En procédant dans cette optique, nous pouvons penser à une faille que présenterait le système de fichiers log tel que décrit précédemment. Pour reprendre l'exemple cité précédemment, on peut penser à un scénario où la société bancaire compte un informaticien administrateur parmi ses employés, qui s'occupe justement de la gestion du système informatique, mais qu'un appel est fait à une société informatique extérieure pour effectuer les mises à jour de ce système. Dans ce contexte il serait tout à fait possible que cet informaticien s'empare d'une certaine somme d'argent en manipulant le système informatique de la banque et il pourrait facilement effacer toute trace de ses actes. Ou bien pire, il pourrait modifier les fichiers log pour rejeter le soupçon sur l'entreprise informatique.

Ces deux possibilités seraient tout à fait plausibles vu que les fichiers log sont en la possession de l'informaticien administrateur et qu'il a donc également les droits d'accès nécessaires pour manipuler les fichiers log à sa guise. Les conséquences de tels actes pourraient bien évidemment être catastrophiques pour l'entreprise informatique et pourtant cette problématique n'est pas adressée par les normes informatiques, même celles qui mettent en avant le maintien d'un système de fichiers log. Nous pourrions donc nous demander comment adresser ce problème.

5.3.1 Première proposition de solution

La première solution qui nous vient à l'esprit est celle de stocker les fichiers log du côté de l'entreprise informatique, mais de façon à ce qu'ils ne soient accessibles que par la société bancaire.

Par cela nous entendons que le système de fichiers log fonctionne de la même manière qu'avant sauf exception en ce qui concerne l'enregistrement de ces fichiers. Au lieu d'être simplement enregistrés comme ils l'étaient d'habitude, cette fois-ci les fichiers log seraient protégés par un mécanisme qui requerrait l'introduction d'un mot de passe afin de pouvoir consulter les fichiers. Bien évidemment, cette authentification pourrait être faite sur base d'autres moyens qu'un mot de passe, tel des certificats électroniques. Ainsi, l'informaticien administrateur de la société bancaire ne pourrait être en mesure de modifier les fichiers log pour effacer les traces de ses actes. De même, l'entreprise informatique ne pourrait pas non

plus être en mesure d'effacer la trace d'un acte délictueux quelle aurait commis sur le système bancaire.

Néanmoins, le problème que pose cette solution est le fait qu'il faille rapatrier les fichiers log de la société bancaire vers l'entreprise informatique. D'un côté, le danger d'un tel rapatriement se trouve dans la possibilité d'une panne de courant pendant l'intervention distante, ce qui pourrait fausser le contenu des fichiers log par rapport à ce qui aurait réellement été fait sur l'ordinateur hôte. D'un autre côté, il se pourrait que l'informaticien administrateur de la société bancaire insère des informations supplémentaires dans le flux de rapatriement. Ces informations seraient donc comprises dans les fichiers log rapatriés et pourraient tenir l'entreprise informatique coupable pour des actes qu'elle n'aurait pas commis. Cette solution ne nous conviendrait donc pas.

5.3.2 Deuxième proposition de solution

Une autre possibilité de solution au problème initial serait la mise en place d'un système qui requerra une double authentification pour l'accès aux fichiers log qui seraient stockés chez la société bancaire. Cette solution est semblable à la précédente à l'exception du nombre de mots de passe qui seraient nécessaires pour l'accès aux fichiers log.

Cette fois-ci le système requerra deux mots de passe, dont un qui serait détenu par la société bancaire, et donc inconnu pour l'entreprise informatique. Inversement, le deuxième mot de passe serait détenu par l'entreprise informatique, et donc inconnu pour la société bancaire. Notons que nous pourrions également utiliser d'autres moyens, tel des certificats électroniques, pour authentifier la société bancaire. Avec un tel mécanisme mis en place, l'informaticien administrateur de la société bancaire ne pourrait modifier les fichiers log sans avoir le consentement de l'entreprise informatique.

Cette solution pourrait paraître satisfaisante pour le problème qui se présente à nous, et pourtant il existe quand même une faille. En effet, même si la suppression des fichiers log pouvait être protégée par le mécanisme de double authentification, il ne faut pas oublier que ces informations sont stockées sur du matériel informatique appartenant à la société bancaire. Cela implique que ce matériel serait physiquement accessible par l'informaticien administrateur. Par conséquent, ce dernier pourrait physiquement détruire les fichiers log une fois qu'il aura pris connaissance de leur emplacement physique.

Cependant, il serait logique de se dire que c'est la responsabilité de la société bancaire d'assurer l'intégrité des fichiers log à partir du moment où ceux-ci sont enregistrés sur du matériel informatique appartenant à la société bancaire. De cette façon, il n'y aurait que la société bancaire qui pourrait être tenue responsable pour quelconque acte frauduleux en cas de perte des fichiers log. Néanmoins, l'informaticien administrateur pourrait être capable de mettre en place un mécanisme permettant de filtrer les messages log avant qu'ils ne soient enregistrés dans le fichier log qui sera protégé par les deux mots de passe ou certificats électroniques. De cette façon, il pourrait empêcher qu'une trace de ses actes ne soit gardée. Mais ce mécanisme pourrait également permettre à l'informaticien administrateur d'insérer des messages log supplémentaires avant l'enregistrement et la protection des fichiers log. De cette manière, il pourrait faire passer pour coupable l'entreprise informatique pour les actes frauduleux qu'il aurait commis. Cette faille rendrait donc inacceptable la solution que nous proposons.

5.3.3 Troisième proposition de solution

En analysant les problèmes qui survenaient lors des solutions précédentes, nous pouvons proposer une troisième solution. Par rapport aux tentatives précédentes pour trouver une solution, on remarque que nous rencontrions des problèmes peu importe que les fichiers log soient enregistrés du côté de la société bancaire ou du côté de l'entreprise informatique. En partant de cette constatation, nous proposons une solution où les fichiers log ne seraient enregistrés chez aucune des deux parties mentionnées précédemment, mais plutôt chez un tiers de confiance. Pour ce faire, il suffirait de mettre en place un système par lequel toute la communication entre la partie accédante à distance et la partie accédée à distance.

Ainsi, nous pourrions penser à un tiers de confiance par qui passeraient toutes les commandes envoyées par l'entreprise informatique. Ensuite le tiers de confiance relaierait ces commandes vers la société bancaire après les avoir copiées dans un fichier temporaire qu'il gardera chez lui. Une fois que la société bancaire reçoit les commandes de la part du tiers de confiance et les exécute, elle enverrait un message confirmant la bonne exécution des commandes reçues. A ce moment là, le tiers de confiance pourra faire un *commit* des commandes précédemment enregistrées dans un fichier log final.

De cette façon, les fichiers log seront stockés chez le tiers de confiance de façon à ce qu'ils ne puissent être modifiés par aucune des deux parties. En effet, l'entreprise informatique ne pourrait modifier les traces des informations qu'elle a envoyées sans avoir la permission du tiers de confiance. Et la société bancaire ne pourrait pas non plus modifier le contenu des fichiers log puisque, à part exécuter les instructions qu'elle reçoit, elle ne peut faire que confirmer ou non le bon déroulement de ces instructions. Ceci nous garantirait que les informations enregistrées dans les fichier log du tiers de confiance sont bel et bien les instructions qui ont réellement été envoyées par l'entreprise informatique et exécutées par la société bancaire. Ceci permettrait que, lors d'un litige, chacune des deux parties pourrait faire appel au tiers de confiance afin qu'il fournisse une copie des fichiers log qu'il détient.

Un avantage supplémentaire de cette solution est qu'à partir du moment où les fichiers log sont enregistrés chez le tiers de confiance, ça permet aussi bien à l'entreprise informatique qu'à la société bancaire de ne pas devoir se préoccuper d'avoir suffisamment d'espace disque que pour stocker ces fichiers.

5.4 Perspective : avancées futures

Dans le futur nous pouvons nous attendre à voir de nouvelles avancées dans le domaine de l'accès à distance. Certaines avancées seront dues à des changements technologiques, tandis que d'autres avancées seront liées à différents domaines d'application auxquels s'étendrait l'accès à distance.

En effet, de plus en plus de systèmes nous sont proposés, ou nous sont promis pour le futur, qui permettraient de gérer différents aspects de notre vie quotidienne à distance. Nous pouvons penser par exemple aux systèmes qui permettraient de gérer le système d'alarmes et de surveillance de sa maison à distance lorsqu'on est en vacances. Nous pouvons également penser aux systèmes qui nous permettraient d'allumer le chauffage ou d'allumer le four une fois qu'on quitte le bureau pour qu'on puisse arriver dans une maison réchauffée avec un souper chaud qui nous attend dans la cuisine. Même lorsqu'on aurait oublié de faire la liste

des courses avant d'aller au supermarché on pourrait interagir avec le frigo de la maison pour en vérifier les produits qui y sont contenus ainsi que leurs dates de péremption. Alors que certaines personnes se voient ravies d'entendre de telles nouvelles, il faut tout de même garder un aspect critique vis-à-vis de ces systèmes.

En effet, il ne faut pas oublier que si ces systèmes présentent certaines facilités pour les utilisateurs de par leur aspect d'accessibilité à distance, c'est ce même aspect qui pourrait donner lieu à des attaques distantes qui n'auraient pas été possibles autrefois. Ces attaques pourraient aller de la simple farce, où l'"attaquant" allumerait toutes les lumières de la maison pendant la nuit lorsque les occupants dorment, jusqu'au cambriolage, où l'"attaquant" désactiverait à distance le système d'alarme avant de pénétrer à son aise dans la maison. Nous pouvons donc voir que l'aspect de sécurité ne devrait pas être négligé lorsque ces nouvelles implémentations d'accès à distance seront développées.

5.5 Perspective : propositions d'améliorations futures

Dans une autre optique, toutes ces avancées s'appliquent à un contexte où nous nous trouvons dans un pays développé. En effet, comme nous avons pu le constater dans les chapitres précédents, les pays en voie de développement ne sont pas toujours en mesure d'offrir les mêmes possibilités d'accès à distance que nous.

Dans le cadre de l'Afrique, il est vrai que les réseaux de télécommunications se répandent de plus en plus, mais l'accès à ces réseaux laisse encore à désirer. Si nous prenons le cas du Sénégal par exemple, qui se trouve parmi les pays africains les plus développés, l'accès à Internet par ADSL est déjà une réalité. Pour les particuliers nous pouvons y trouver des abonnements de lignes ADSL de 256 kbits/s pour 13 500 CFA (20,25€) ou de 512 kbits/s pour 23 000 CFA (34,50€) [SONATEL]. Et lorsque nous nous trouvons dans un cybercafé à Dakar, le coût d'une heure de "navigation" sur une ligne de 1024 kbits/s peut varier entre 500 CFA (0,75€) et 1 000 CFA (1,50€). Néanmoins, si les tarifs pratiqués nous paraissent accessibles, il faut remarquer que le revenu moyen d'un adulte sénégalais est d'à peu près 17 000 CFA (25,50€) par mois [UNECA]. Nous pouvons donc constater que ce moyen de télécommunications reste encore inaccessible pour une très grande partie de la population.

Quant aux entreprises, seules les plus riches peuvent se permettre d'allouer un budget pour un accès Internet. Comme nous l'avons vu précédemment, les entreprises qui ne sont pas assez avantagées que pour avoir un accès Internet, telles les Institutions de Micro Finance, sont obligées de trouver d'autres moyens que l'Internet pour mettre en place un mécanisme d'accès à distance. Ces entreprises sont donc confrontées à une performance nettement moins élevée de leurs solutions d'accès à distance. Par conséquent, il aurait été souhaitable que cet aspect soit pris en compte lors des avancées futures de l'accès à distance.

Peut être qu'il y aurait moyen d'améliorer les performances de l'accès à distance via modem et le Réseau Téléphonique Commuté par exemple? Mais en même temps, ceux qui participent au développement des solutions d'accès à distance, en général, ne voient que peu d'intérêt à se lancer dans cette direction. En effet, ce moyen de communication revêt de moins en moins d'intérêt. Pour constater ceci il suffit de penser à la difficulté croissante que nous rencontrons lorsqu'on essaye de trouver un modem analogique de nos jours, même dans des pays en voie de développement tel que le Sénégal. Cette logique nous pousse à penser que la

seule solution pour améliorer les performances d'accès à distance dans ces pays en voie de développement serait de faciliter l'accès à Internet par quelque moyen que ce soit.

Néanmoins, même si l'Internet était plus accessible dans ces pays, un problème fondamental persisterait encore toujours. Ce problème concerne les pannes de courant qui sont assez fréquentes dans ce genre de pays et qui donneraient donc lieu à une interruption de la communication mise en place lors d'un accès distant. Vu que ce ne sera pas d'ici demain que seront résolus les problèmes de pannes de courant dans les pays du tiers monde, il faudrait à ce moment là passer en revue les solutions d'accès à distance qui seraient susceptibles d'être déployées dans ces pays afin de s'assurer qu'ils prennent bien en compte l'éventualité d'une coupure de courant.

Conclusion

De nos jours, plus personne ne conteste l'utilité de l'accès à distance. Pour certaines entreprises, plus que d'autres, cet outil est devenu indispensable. Du télétravail et l'accès de fichiers distants, à la maintenance et dépannage de système distants, les avantages offerts par l'accès à distance sont incommensurables.

Au travers de ce mémoire nous avons eu l'occasion de mettre en évidence divers aspects de l'accès à distance. A un niveau plutôt technique, nous avons passé en revue les différents mécanismes qui peuvent être implémentés pour l'établissement d'un accès à distance, en théorie ainsi qu'en pratique. Nous avons également parcouru certaines normes qui s'appliquent à l'accès à distance en Europe. A ce niveau-ci nous avons approfondi le sujet du mémoire en présentant des recommandations concernant ces normes, et plus spécifiquement le fait d'attribuer une plus grande importance aux fichiers log. Finalement, nous avons également proposé des améliorations futures souhaitables concernant l'accès à distance.

Par ces différentes facettes de l'accès à distance, nous avons pu remarquer l'utilité que présente une bonne solution d'accès à distance ainsi que l'importance de son niveau de sécurité. Mais nous avons également vu que les solutions d'accès à distance qui sont proposées sur le marché sont suffisamment sécurisées que pour empêcher la mise en danger du système qui l'implémenterait. Il est d'ailleurs même possible de trouver de telles solutions en versions gratuites, toutes offrant un niveau de sécurité comparable aux payantes. Néanmoins, c'est la façon dont sont utilisés ces solutions d'accès à distance, par les utilisateurs, qui mérite une plus grande attention à un niveau sécuritaire.

Comme nous pouvons le voir, les aspects les plus importants de l'accès à distance ont pu être couverts lors de la rédaction de ce mémoire. Evidemment, si nous n'étions pas limités d'un point de vue des ressources pécuniaires, matérielles et temporelles, il aurait été intéressant de pouvoir approfondir encore plus le sujet développé dans ce mémoire.

Si nous prenons le cas de l'étude comparative des différentes solutions d'accès à distance par exemple, il serait bénéfique d'étendre cette étude à davantage de solutions afin qu'elle soit plus complète.

L'étude pratique de deux solutions d'accès à distance lors du stage nous a permis de constater l'influence qu'on les contraintes du terrain sur les critères de choix. Par conséquent, il serait intéressant de pouvoir mener une étude comparative à un niveau pratique, c'est-à-dire en testant chaque solution une par une. Avec une telle étude, nous bénéficierions d'une comparaison qui reflète plus la réalité des performances individuelles de chaque solution.

En ce qui concerne le *Dial-up*, une plus grande documentation permettrait une étude technique plus approfondie de ce sujet. Néanmoins, vu que le *Dial-up* n'est plus tellement d'actualité, il est peu probable qu'une documentation supplémentaire n'apparaisse un de ces jours.

Pour ce qui est des normes, il serait également intéressant d'élargir l'analyse à un nombre plus élevé de normes qui régulent l'accès à distance. Evidemment, la plupart de ces

documents étant payants et généralement peu abordable pour des particuliers, c'est l'inaccessibilité plutôt que le manque de documentation qui se pose comme obstacle pour cette direction.nous empêcha d'avancer dans cette direction.

Finalement, une autre optique qui susciterait aussi pas mal d'intérêt est celle de l'implémentation des solutions proposées au chapitre 5 pour les fichiers log. La mise en œuvre de tels mécanismes de maintien de fichiers log pourrait mieux mettre en avant les avantages de ces solutions.

Néanmoins, il ne faut pas oublier que, outre l'intérêt que présenteraient ces propositions, elles nécessiteraient beaucoup plus de ressources pécuniaires, matérielles, et temporelles que celles qui étaient à notre disposition.

Bibliographie

Pages web consultées :

[AQUADEV] http://www.aquadev.org (avril 2006)
[GTMP] http://www.gotomypc.com (avril 2006)
[LMI] http://www.secure.logmein.com (avril 2006)
[NX] http://www.nomachine.com (avril 2006)
[PcAny] http://www.symantec.com (avril 2006)
[RFC editor] http://www.rfc-editor.org (août 2006)
[SONATEL] http://www.sonatel.sn (août 2006)
[THALES] http://www.thales-esecurity.com/ProductsServices/TVPN.shtml (juillet 2006)
[VNC] http://www.realvnc.com (août 2006)
[VPN Consortium] http://www.vpnc.org (juillet 2006)

Articles et documents issus de pages web :

[CEN nisissue] CEN, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach*, http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/nisissuewithtoc11.pdf (13 octobre 2003).
[CISCO SSL] CISCO, *Introduction to Secure Sockets Layer*, http://www.cisco.com/warp/public/cc/so/neso/cxne/cxdimng/wpsot_wp.pdf.
[CW DU] Ajith Ram, *Remote Access through a dial-up network*, http://www.computerweekly.com/Articles/1999/08/19/178922/Remote+Access+through+a+dial-up+network.htm (19 août 1999).
[GTMP PO] Lisa Phifer, *GoToMyPC : Making Life Simpler for Remote and Mobile Workers*, https://www.gotomypc.com/downloads/pdf/m/GoToMyPC_Personal_Overview.pdf.
[GTMP PSWP] Lisa Phifer, *GoToMyPC Security*, https://www.gotomypc.com/downloads/pdf/m/GoToMyPC_Personal_Security_White_Paper.pdf.
[HEISE] Duncan Campbell, *How NSA access was built into Windows*, http://www.heise.de/tp/r4/artikel/5/5263/1.html (4 septembre 1999).
[HSW VPN] Jeff Tyson, *How Virtual Private Networks Work*, http://computer.howstuffworks.com/vpn.htm.
[LMI security] Márton Anka, *LogMeIn Security – an In-Depth Look*, https://secure.logmein.com/wp_lmi_security.pdf.
[MH PPP] ModemHelp.net, *What is PPP? What is SLIP?*, http://www.modemhelp.net/faqs/ppp.shtml (14 janvier 2004).
[MIC Dial-up] Microsoft, *Dial-up Remote Access Technical Reference*, http://technet2.microsoft.com/WindowsServer/en/Library/71b2fe2a-5be3-4566-a2f6-c03a758a8dfb1033.mspx?mfr=true (28 mars 2003).
[PcAny UM] Symantec, *Symantec pcAnywhere User's Guide*, ftp://ftp.symantec.com/public/english_us_canada/products/pcanywhere/12.0/manuals/pcauser.pdf.

[RFC 1055] J. Romkey, *A NONSTANDARD FOR TRANSMISSION OF IP DATAGRAMS OVER SERIAL LINES: SLIP*, ftp://ftp.rfc-editor.org/in-notes/rfc1055.txt (juin 1988).
[RFC 1661] W. Simpson, *The Point-to-Point Protocol (PPP)*, ftp://ftp.rfc-editor.org/in-notes/rfc1661.txt (juillet 1994).
[RFC 2401] S. Kent et R. Atkinson, *Security Architecture for the Internet Protocol*, ftp://ftp.rfc-editor.org/in-notes/rfc2401.txt (novembre 1998).
[RFC 2402] S. Kent et R. Atkinson, *IP Authentication Header*, ftp://ftp.rfc-editor.org/in-notes/rfc2402.txt (novembre 1998).
[RFC 2406] S. Kent et R. Atkinson, *IP Encapsulating Security Payload (ESP)*, ftp://ftp.rfc-editor.org/in-notes/rfc2406.txt (novembre 1998).
[RFC 2408] D. Maughan, M. Schertler, M. Schneider, et J. Turner, *Internet Security Association and Key Management Protocol (ISAKMP)*, ftp://ftp.rfc-editor.org/in-notes/rfc2408.txt (novembre 1998).
[RFC 2409] D. Harkins et D. Carrel, *The Internet Key Exchange (IKE)*, ftp://ftp.rfc-editor.org/in-notes/rfc2409.txt (novembre 1998).
[RFC 2637] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, et G. Zorn, *Point-to-Point Tunneling Protocol (PPTP)*, ftp://ftp.rfc-editor.org/in-notes/rfc2637.txt (juillet 1999).
[RFC 2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, et B. Palter, *Layer Two Tunneling Protocol "L2TP"*, ftp://ftp.rfc-editor.org/in-notes/rfc2661.txt (août 1999).
[RFC 2764] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, et A. Malis, *A Framework for IP Based Virtual Private Networks*, ftp://ftp.rfc-editor.org/in-notes/rfc2764.txt (février 2000).
[RFC 4346] T. Dierks et E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.1*, ftp://ftp.rfc-editor.org/in-notes/rfc4346.txt (avril 2006).
[SANS OpenVPN] Charlie Hosner, *OpenVPN and the SSL VPN Revolution*, http://www.sans.org/reading_room/whitepapers/vpns/1459.php (8 août 2004).
[SF VPN] David Aylesworth, *What to look for when buying a VPN*, http://poptop.sourceforge.net/dox/whatvpn.html (16 janvier 2003).
[SSI CrimeCom] Commission Européenne, *Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité*, http://www.ssi.gouv.fr/fr/reglementation/CrfimeComFR.pdf.
[SSI com2002152] Commission Européenne, *Poursuite du plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux*, http://www.ssi.gouv.fr/fr/reglementation/com2002152.pdf (22 mars 2002).
[SSI com2002173] Conseil de l'Union Européenne, *Proposition de décision-cadre du Conseil relative aux attaques visant les systèmes d'information*, http://www.ssi.gouv.fr/fr/reglementation/com2002173fin.pdf (27 août 2002).
[SSI netsec] Commission Européenne, *Sécurité des réseaux et de l'information: Proposition pour une approche politique européenne*, http://www.ssi.gouv.fr/fr/reglementation/netsec_fr.pdf.
[SSI res15152] Conseil de l'Union Européenne, *RÉSOLUTION DU CONSEIL du [6] décembre 2001 relative à une approche commune et à des actions spécifiques dans le domaine de la sécurité des réseaux et de l'information*, http://www.ssi.gouv.fr/fr/reglementation/resolution15152.pdf (11décembre 2001).
[UNECA] Commission économique pour l'Afrique, *Le Processus du DSRP au Sénégal*, http://www.uneca.org/prsp/docs/prsp_final/Senegal.PDF#search=%22%22revenu%20moyen%22%20s%C3%A9n%C3%A9gal%22 (18 novembre 2002).
[VNC RFB] Tristan Richardson, *The RFB Protocol*, http://www.realvnc.com/docs/rfbproto.pdf (8 juillet 2005).

[wiki Firewall] *Firewall (Networking)*, http://en.wikipedia.org/wiki/Firewall_%28networking%29.
[wiki https] *Https*, http://en.wikipedia.org/wiki/Https.
[wiki LL] *Local Loop*, http://en.wikipedia.org/wiki/Local_loop.
[wiki VPN en] *Virtual Private Network*, http://en.wikipedia.org/wiki/Virtual_private_network.
[wiki VPN fr] *Réseau Privé Virtuel*, http://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel.
[wiki WAN fr] *Réseau Etendu*, http://fr.wikipedia.org/wiki/R%C3%A9seau_%C3%A9tendu.
[wiki X.25] *X.25*, http://en.wikipedia.org/wiki/X.25.

Personnes :

[Diallo] Hassan Diallo – Chef de projet pour ADbanking, AQUADEV-Sénégal
[Imran] Imran – Symantec Authorized Technical Support
[Schyns] Laurent Schyns – Responsable Outils et Stratégie, AQUADEV-Europe

Ouvrages :

[ISO 17799] JTC 1/SC 27, *Information technology -- Security techniques -- Code of practice for information security management*, Institut Belge de Normalisation, juin 2005
[ISO 18028] JTC 1/SC 27, *Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access*, avril 2005
[Kurose et Ross] James F. Kurose et Keith W. Ross, *Computer Networking : A Top-Down Approach Featuring The Internet*, Addison-Wesley, Etats-Unis, 2005.

Annexe I : Déroulement et critique de stage

A : Déroulement du stage

A.1 Description du stage

Après discussion avec le Responsable Outils et Stratégie d'AQUADEV-Europe, M. Laurent Schyns, deux sujets ont été définis préalablement au stage. Néanmoins, le deuxième sujet, qui concernait la synchronisation d'envoi de fichiers, devait être fait en collaboration avec une équipe de développement se trouvant au Maroc qui a malheureusement pris du retard et par conséquent, il n'y a que le premier sujet qui fut approfondi. Dorénavant, nous ne parlerons donc plus que de ce premier sujet.

Le sujet traité lors du stage concernait la survenance d'un bug au sein d'ADbanking. Comme nous le savons tous, presque tout développement d'un logiciel mènera à la découverte de bugs par la suite. Dans le cas d'AQUADEV, ce sont les Institutions de Micro Finance (IMF) qui découvrent de temps en temps un bug dans la version d'ADbanking installée sur leur serveur ou une anomalie dans la base de données nécessaire au bon fonctionnement d'ADbanking. Dans ce cas, AQUADEV doit envoyer un membre de l'équipe de développement sur place pour tenter de résoudre le problème. Nous pouvons facilement imaginer les inconvénients que ce genre de situation représente pour AQUADEV. Non seulement elle subit une perte d'argent dû au déplacement mais, vu l'absence d'un membre de l'équipe de développement pendant la durée du débogage sur place, le développement des versions ultérieures d'ADbanking accumule les retards.

L'objectif du stage était donc de répondre à ce problème par la "mise en place d'une infrastructure permettant de prendre à distance le contrôle d'un serveur ADbanking en vue de faire un diagnostic d'un problème qui serait survenu, d'intervenir pour résoudre ce problème et, éventuellement, d'effectuer des maintenances (ex : installer une nouvelle version du logiciel, ou installer un *patch* correctif)" [Schyns]. En bref, il fallait mettre en place une solution d'accès à distance mais plus précisément, un contrôle à distance sur les serveurs des IMFs. Le scénario typique envisagé au départ était que l'IMF, ayant un problème qu'elle ne savait pas résoudre, aurait contacté AQUADEV qui à son tour, avec l'accord de l'IMF concernée, aurait accédé au serveur à distance afin de résoudre le problème.

ADbanking ayant été développé pour des IMFs se situant dans des pays en voie de développement, deux situations peuvent se présenter. Soit on se trouve dans le cas où l'IMF, bien établie, est en mesure de s'équiper d'une connexion à l'Internet, soit elle n'en a pas les moyens. Vu que la deuxième situation est la plus répandue, c'est surtout dans ce contexte que l'implémentation de la solution d'accès à distance a le plus d'importance. Evidemment, comme ces IMFs n'ont pas de "connexion au monde", l'idée est d'effectuer l'accès à distance via modem et le Réseau Téléphonique Commuté (RTC).

A.2 Méthodologie envisagée

Comme nous avons pu le constater lors des chapitres précédents, le concept de d'accès à distance ne date pas d'hier et par conséquent, il était évident qu'il ne fallait pas négliger la possibilité qu'il puisse y avoir une solution toute faite (cfr. chapitre 2) qui aurait satisfait les objectifs préalablement fixés. Mais la question qui se posait était surtout de savoir laquelle de ces solutions aurait le mieux répondu aux besoins exprimés par AQUADEV.

Afin de pouvoir comparer les différentes solutions d'accès à distance, il fallait choisir des critères de comparaison. Bien évidemment il fallait que la solution satisfasse les objectifs convenus pour le stage, mais ce n'était pas le seul critère. Un critère fondamental était le fait qu'il fallait tenir compte des contraintes propres au terrain, à savoir un débit limité dû au fait que la combinaison du modem et du RTC était le seul moyen d'établir une connexion avec les IMFs. En effet, vu que la plupart des IMFs n'ont pas les moyens de se procurer une connexion Internet, nous ne pouvons pas exiger qu'elles s'en procurent une pour les seuls besoins d'un contrôle à distance en cas d'une éventuelle panne de ADbanking ou du serveur. Finalement, étant donné que le stage s'effectuait pour le compte d'une ONG, il ne fallait surtout pas oublier de prendre en compte le critère de coût.

Dans le cas où une de ces applications aurait répondu de manière satisfaisante aux critères cités précédemment, l'étape suivante était de tester l'application en question sur le terrain. Cette étape aurait permis de savoir si l'outil convenait réellement aux attentes d'AQUADEV. Si ce n'était pas le cas, le "plan de secours" était soit de procéder à une amélioration de l'application si possible (par exemple, si l'application était *open source*), soit d'écrire une nouvelle application, soit encore d'établir une procédure qui aurait permis d'effectuer un contrôle à distance tout en satisfaisant les critères de choix cités précédemment.

Fig. 4.1 – Déploiement envisagé de la solution d'accès à distance

A un niveau plus technique, le déploiement prévu de la solution d'accès à distance était assez simple, comme nous pouvons le constater à la figure 4.1. Du côté des IMFs, les employés travaillaient sur des ordinateurs tournant sur Windows mais le serveur sur lequel était installé ADbanking tournait sur Linux, tandis que du côté d'AQUADEV, les développeurs travaillaient sur des ordinateurs *dual-boot*[65] équipés d'une version de Linux et de Windows. Donc une fois qu'une solution adéquate d'accès à distance avait été choisie, le déploiement de cette solution consistait simplement en l'installation du composant serveur sur l'ordinateur hôte de l'IMF (c'est-à-dire son serveur) et l'installation du composant client sur un ordinateur client d'AQUADEV (c'est-à-dire l'ordinateur d'un des développeurs). Ainsi, lors de la survenance d'un problème, les deux parties feraient en sorte que l'ordinateur client (AQUADEV) et l'ordinateur hôte (IMF) soient branchés au RTC par l'intermédiaire d'un modem analogique. A ce moment, afin d'établir l'accès à distance, nous avons décidé d'utiliser le *Dial-up* [Diallo].

[65] C'est-à-dire que plus d'un système d'exploitation a été installé sur l'ordinateur.

A.3 Déroulement du stage

Suite à l'élaboration de la méthodologie envisagée, nous avons pu commencer la mise en place du système d'accès à distance. En fin de compte, le stage s'est déroulé, non sans imprévus, en suivant à la lettre la méthodologie qui avait été envisagée à la section A.2.

A.3.1 Choix et test d'une solution d'accès à distance

Après un temps de recherche en matière de technologies permettant d'établir un accès à distance, nous avons procédé à une analyse comparative des différentes solutions "toutes faites" qui existaient (cfr. chapitre 2). Le résultat de cette analyse a fait ressortir NX comme étant l'application d'accès à distance qui remplissait le mieux les critères de comparaison. Ce qui distinguait surtout NX des autres applications de contrôle à distance était le fait que cette application avait été développée en tenant particulièrement compte des bandes passantes à plus faible débit des modems analogiques ou numériques (ISDN). Les critères étant remplis, nous avons confronté l'application aux conditions du terrain, c'est-à-dire que nous avons testé sa performance via modem. Tous ces tests se sont bien passés et la performance offerte par NX était incontestable (comme nous le verrons par la suite), et pourtant il a fallu faire appel au "plan de secours".

A.3.2 Changement de plans

Pendant que s'effectuaient les tests d'NX, une discussion avec des membres de l'équipe de développement d'AQUADEV nous a permis de nous rendre compte que les serveurs des IMFs avaient été installés avec une version serveur de la distribution Fedora Core. Ceci impliquait qu'il n'y avait pas de système *X-Window* (ou X11) qui tournait sur le serveur, donc pas d'interface graphique. Et vu que le fonctionnement de NX se basait essentiellement sur le protocole X et la compression de ce dernier, il allait de soi que cette application était devenue inutile dans le cas qui nous concernait. NX étant disponible en *open source*, en suivant la méthodologie qui avait été envisagée il aurait été possible de modifier NX pour l'adapter aux besoins d'AQUADEV. Néanmoins, l'étendue et la lourdeur des changements qui auraient été requis rendaient cette option inutile. Nous avons donc choisi d'"implémenter" une autre solution d'accès à distance, comme nous le verrons par la suite.

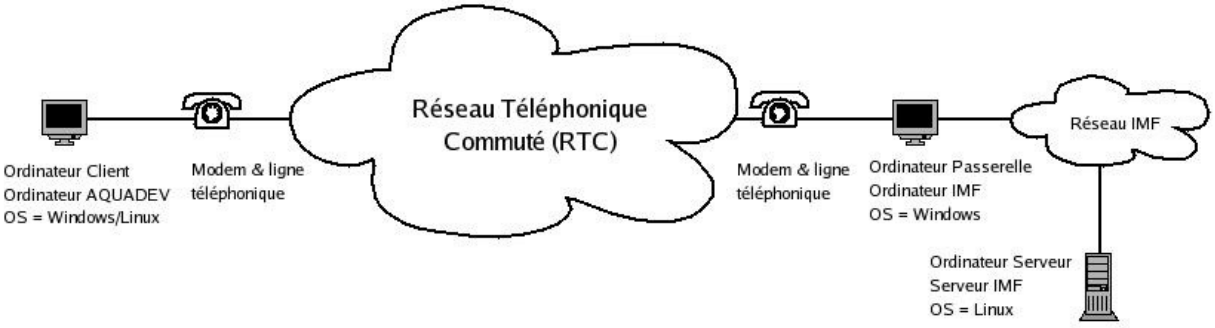


Fig. 4.2 – Déploiement alternatif de la solution d'accès à distance

Au niveau technique, l'établissement de la liaison entre les ordinateurs client et hôte, tel que nous l'avions prévu auparavant, s'est révélé irréalisable en raison d'un problème de compatibilité des modems analogiques sous Linux (ce problème sera traité de façon plus

détaillée par la suite). En effet, l'idée de départ avait été de relier un ordinateur d'AQUADEV (l'ordinateur client) directement au serveur de l'IMF (l'ordinateur hôte), mais le problème de compatibilité empêchait qu'un modem analogique puisse être utilisé sur le serveur Linux de l'IMF. Afin de résoudre cet empêchement, un changement avait été apporté quant au déploiement initialement prévu pour la solution d'accès à distance (cfr. figure 4.2). Au lieu d'avoir une liaison directe entre l'ordinateur client et l'ordinateur hôte, nous allions faire bifurquer la communication par un troisième ordinateur (se trouvant sur le réseau local de l'IMF) que nous nommerons l'ordinateur "passerelle". Ce changement fait également partie de "l'implémentation" de solution d'accès à distance que nous avons mentionnée auparavant et qu'on expliquera plus en détail par la suite.

A.4 Eléments supplémentaires de la solution finale

A.4.1 Droits d'accès et suivi des manipulations distantes

Pour que l'accès distant soit d'une quelconque utilité, il faut bien que celui qui accède à distance ait suffisamment de droits que pour effectuer les opérations nécessaires ou utiliser les services dont il aura besoin.

En ce qui concerne le cas d'accès à distance chez AQUADEV, les services auxquels il fallait pouvoir accéder étaient ceux de *status*, *start*, *stop*, et *restart* pour les processus *network*, *httpd*, et *postgresql*. Ceux-ci n'étaient normalement pas accessibles pour une session autre que *root*, donc nous avons configuré la commande "sudo" pour inclure les services précédemment mentionnés.

A part l'accès à ces services, il fallait également qu'AQUADEV puisse avoir accès en lecture aux fichiers de l'utilisateur "adbanking" ainsi qu'un accès en lecture-écriture à certains fichiers de configuration, notamment *httpd.conf*, *php.ini*, et *postgresql.conf*. Ceci pouvait se faire facilement en modifiant les droits d'accès à ces fichiers en utilisant la commande "chown" ou "chmod", mais il fallait faire attention parce que certains processus refusaient de démarrer lorsque les droits d'accès à certains de leurs fichiers avaient été modifiés.

Sinon, en ce qui concernait l'enregistrement de "toutes les manipulations effectuées à distance sur le système", la première idée était d'utiliser la commande "history" qui reprend l'historique des commandes passées au shell Linux. Seulement cette méthode n'aurait pas été assez fiable vu que la liste des commandes passées était facilement modifiable.

Une solution beaucoup plus fiable et utile avait été proposée par un assistant de l'Institut d'informatique. Cette solution aurait permis de bien tracer toutes les commandes qu'aurait tapé l'intervenant distant, mais elle aurait été fort demandeuse en temps au niveau de l'implémentation, et d'autant plus lorsqu'on n'a pas les compétences nécessaires en C. Nous nous sommes donc mis d'accord pour ne tracer que les informations nécessaires, notamment celles liées aux connexions SSH (pour la connexion et déconnexion distante) et celles liées aux accès à la base de données Postgresql (puisque c'est surtout là dessus que portait le dépannage en général). Nous nous sommes donc résolus à garder des traces de ceux-ci dans des fichiers log en profitant du protocole "syslog" déjà présent dans toute installation de base de Linux.

A.4.2 Interface

Pour finir, il fallait également garantir la possibilité de "consulter, via une interface […] simple d'utilisation (pour un non informaticien), la liste des interventions antérieures ainsi que les enregistrements des manipulations" ainsi "qu'attribuer ou révoquer la permission d'intervention à distance". Il a donc fallu suivre une brève et rapide formation sur postgresql, le php, ainsi que la façon dont fonctionnait ADbanking, pour savoir comment intégrer ces fonctionnalités dans l'interface existante.

En ce qui concerne la consultation des interventions antérieures et les manipulations enregistrées, il suffisait de faire une lecture sur les fichiers logs qui avaient été créés pour SSH et Postgresql. Par contre, en ce qui concernait la permission d'accès à distance, nous avions décidé de jouer sur "l'activation/désactivation" de la session avec laquelle se serait connecté l'intervenant à distance. Ceci pouvait se faire de façon relativement simple avec la commande "passwd", mais afin de faciliter la tâche pour l'acteur, non informaticien, du côté de l'IMF, il fallait intégrer ceci dans l'interface actuelle d'ADbanking et, de préférence, de façon automatique.

L'idée de M Schyns était de définir une plage horaire pour l'intervention, et la permission d'accès au système pour la session distante serait attribuée et révoquée aux heures précisées pour le début et la fin de ladite plage horaire. Afin de pouvoir mettre en œuvre ce système de plage horaire, les recherches parmi les pages "man" ont montré la possibilité d'utiliser soit la commande "cron" ou "at". La première étant une commande qui servait à exécuter une même série d'instructions de façon périodique (par exemple pour faire un back-up du système à trois heures du matin, chaque cinquième jour des mois pairs), nous avons préféré utiliser la deuxième commande, "at", qui elle servait à exécuter cette série d'instructions qu'une seule fois. Ainsi, lorsque nous créions une plage horaire d'intervention distante, une commande "at" était enregistrée pour activer la session destinée à l'utilisateur à la date et l'heure de début de plage horaire, et une deuxième commande "at" était enregistrée pour désactiver cette même session à la date et à l'heure de fin de cette même plage horaire.

B : Critique du stage

Après les quatre mois de stage passés au sein d'AQUADEV, pendant lesquels des recherches ont été menées à bien, l'implémentation a été réalisée, des tests ont été exécutés, et la documentation a été rédigée, un mécanisme d'accès à distance a pu être mis en place. Mais après tout ce temps passé sur l'élaboration de cette solution, il est temps de faire un compte rendu de tout ceci.

B.1 Critique par objectif

Cette première partie du présent chapitre sera une critique du stage par rapport aux objectifs qui avaient été fixés avant le début du stage. Pour chaque objectif qui avait été énoncé, on décrira d'abord les moyens qui avaient été mis en œuvre afin de pouvoir respecter au mieux l'objectif en question. On déterminera ensuite si l'objectif avait bien été satisfait et, le cas échéant, on finira par proposer des modifications qu'on pourrait apporter à la solution finale afin de mieux respecter l'objectif en question.

B.1.1 Enregistrement des manipulations distantes

Comme mentionnée précédemment, l'enregistrement des manipulations effectuées à distance a été assuré par l'utilisation du protocole syslog. Afin de faire ceci, il a fallu se renseigner sur Internet et dans les "pages man" pour savoir comment configurer SSH et Postgresql afin d'activer l'envoi de leurs messages au démon syslogd. Suite à la configuration correcte de ces derniers, les informations sur les manipulations distantes sont maintenant stockées dans des fichiers log se trouvant dans un répertoire caché, dont les droits d'accès ont été réglés pour que ces fichiers ne soient accessibles que par l'utilisateur "adbanking". Ceci nous assure que l'intervenant à distance ne puisse pas modifier les fichiers log afin de se décharger de toute responsabilité lorsqu'il aurait commis un acte frauduleux.

Le système de suivi d'intervention qui a été mis en place pourrait, à première vue, être perçu comme une solution qui remplit bien l'objectif fixé au départ. Néanmoins, ce système présente une série de lacunes qui remettent en question cet a priori.

Pour commencer, nous ne gardons trace que des messages émis par SSH et Postgresql. La menace qui se présente dans ce genre de cas est que l'intervenant a beau être "suivi" lorsqu'il se connecte au serveur ou lorsqu'il effectue des opérations sur le serveur de l'IMF, mais en dehors de ces situations il est libre de faire ce qu'il veut sans qu'une trace en soit conservée. L'intervenant pourrait donc, par exemple, rapatrier ou supprimer des fichiers confidentiels qui se trouveraient sur le serveur auquel il est connecté.

D'un autre côté, le suivi de Postgresql se fait un peu "trop bien" dans le sens qu'il enregistre non seulement ce que fait l'intervenant mais aussi ce que fait l'application ADbanking. C'est-à-dire que, vu que ce dernier fait également des accès à la base de données lorsqu'il est utilisé, si l'IMF utilise ADbanking pendant l'intervention, le fichier log de Postgresql se remplirait avec les requêtes faites par l'intervenant ainsi que celles faites par ADbanking. Evidemment, ceci n'est pas tellement une menace mais plutôt un encombrement vu que les informations générées par l'utilisation d'ADbanking ne nous seraient d'aucune utilité.

Finalement, il y a aussi le problème des fichiers log qui sont peu protégés. Certes ils sont inaccessibles par l'intervenant dans la situation actuelle, mais ce n'est plus le cas si l'intervenant venait à connaître le mot de passe *root* du serveur de l'IMF. A ce moment là il pourrait faire toutes les manipulations frauduleuses qu'il voudrait sur le serveur, et ensuite il pourrait modifier les fichiers log pour qu'aucune trace ne soit laissée de ses actions malicieuses.

Afin de résoudre le problème d'un "suivi incomplet", nous aurions pu mettre en place un système beaucoup plus fiable comme proposé par M Toussaint (assistant à l'Institut d'informatique). Ce système consiste en l'utilisation de la commande "strace" afin de tracer tous les appels systèmes qu'auraient été faits sur le serveur et ensuite filtrer le résultat obtenu en supprimant les informations superflues. En implémentant ce genre de solution, on aurait pu tracer de manière efficace toutes les commandes qu'aurait tapé l'intervenant à distance. Ceci aurait, de plus, l'avantage de nous débarrasser du problème de l'enregistrement des informations superflues liées à l'utilisation simultanée d'ADbanking.

En ce qui concerne le problème de la protection des fichiers log, plusieurs alternatives pourraient être envisagées mais ces solutions sont plutôt des propositions d'amélioration concernant les systèmes de maintien de fichiers log en général. Elles seront donc développées plus en détail lors du prochain chapitre.

B.1.2 Authentification du client par le serveur

Dans une première phase, l'authentification se faisait par demande de mot de passe pour la session avec laquelle on se connectait. Mais afin de réduire les risques liés à cette authentification faible, nous avons décidé d'utiliser une authentification par clé publique. La clé privée sera gardée soigneusement chez AQUADEV et la clé publique sera copiée sur le serveur de l'IMF. De cette manière, il n'y aura qu'AQUADEV qui sera autorisé à se loguer sur le serveur de l'IMF. Par contre, la situation étant qu'AQUADEV dessert plusieurs IMFs simultanément, il y avait deux scénarios possibles pour déployer l'authentification par clé publique. Le choix du type de déploiement à mettre en place sera laissé à AQUADEV.

Le premier scénario consiste en la création d'une seule paire de clés publique et privée, et que la clé publique soit distribuée à toutes les IMFs qui seront contrôlées à distance par AQUADEV. L'avantage de ce scénario est la facilité avec laquelle on peut effectuer un contrôle à distance, peu importe l'IMF qu'on veut contacter, du fait qu'il n'y a qu'une seule clé privée qui permet de contacter toutes les IMFs. Le désavantage est, évidemment, qu'en cas de suppression, vol, perte, ou corruption de la clé privée, il faudra générer une nouvelle paire de clés publique et privée et repasser chez toutes les IMFs afin de leur fournir la nouvelle clé publique.

Le deuxième scénario consiste en la création d'une nouvelle paire de clés publique et privée pour chaque IMF qui serait contrôlée à distance par AQUADEV. L'avantage de ce scénario est qu'en cas de suppression, vol, perte, ou corruption d'une des clés privées, il faudra bien évidemment re-générer une nouvelle paire de clés publique et privée pour l'IMF concernée, mais cette fois il ne faudra passer que chez une des IMFs pour fournir la nouvelle clé publique. Bien sûr, le désavantage serait la complication amenée lorsqu'il faut contacter une IMF et qu'il faut d'abord retrouver la clé privée correspondante à l'IMF.

En fin de compte, le l'ordinateur client, c'est-à-dire l'ordinateur d'un développeur chez AQUADEV, sera bien authentifié auprès de l'ordinateur hôte, c'est-à-dire le serveur de l'IMF. Ceci est vrai peu importe le scénario de déploiement qu'aura choisi AQUADEV. Nous

pouvons donc dire que l'objectif de l'authentification a bien été satisfait. Bien sûr, ceci sera le cas tant que la ou les clés privées seront bien gardées à l'abri des intrus chez AQUADEV.

B.1.3 Encryption des données échangées

Une fois l'authentification faite, il faut également que les données échangées soient protégées par la suite. Lorsqu'il s'agit de protéger des données qui transitent d'un ordinateur à l'autre, nous ne pouvons penser à un autre protocole plus connu que le protocole SSH, qui a l'avantage supplémentaire d'avoir eu le temps de faire ses preuves.

Comme nous l'avons mentionné précédemment, ce protocole n'est pas disponible sous Windows. Nous avons donc utilisé le client PuTTY du côté d'AQUADEV pour l'établissement de la connexion SSH. Du côté de l'IMF, vu que la première connexion se fait sur l'ordinateur "passerelle", qui tourne sous Windows, il a fallu y installer Cygwin sans oublier de télécharger le package OpenSSH. Ainsi, l'ordinateur passerelle se trouvant dans le réseau local de l'IMF pourrait servir de serveur SSH pour la première connexion et servir de client SSH pour établir la deuxième connexion sur le serveur de l'IMF. De par l'utilisation de ces éléments, les données échangées entre ces trois entités seront encryptées avec des clés cryptographiques[66], qui sont générées et partagées grâce au protocole Diffie-Hellman.

Le seul désavantage que pourrait présenter la solution apportée est une faille connue du protocole Diffie-Hellman, qui est celle de l'attaque de "l'homme au milieu". Mais cette attaque n'est possible que lorsqu'il n'y a pas de vérification d'identité entre les deux parties, ce qui n'est pas le cas avec la solution que nous avons proposée. En effet, l'utilisation d'une authentification par clé publique nous permet d'être sûr de l'identité de notre correspondant. Ceci nous permet de pouvoir protéger de manière efficace les données échangées entre AQUADEV et l'IMF par encryption. On peut ainsi garantir la confidentialité des données échangées et satisfaire l'objectif concerné.

B.1.4 Consultation : interventions antérieures et enregistrements des manipulations

La solution finale apportée comprend la possibilité de consulter la liste des interventions antérieures ainsi que les enregistrements des manipulations effectuées par l'intervenant distant lors de ces interventions.

Ceci a été accompli par un ajout à l'interface existante d'ADbanking qui permet de consulter les interventions sous forme de liste. Ainsi, si au moins deux interventions ont eu lieu pendant deux années différentes, alors la liste est d'abord triée par année[67]. Une fois l'année sélectionnée, une deuxième liste des interventions à distance est présentée à l'utilisateur, mais triée par mois cette fois-ci[68]. On finit par sélectionner la plage horaire sur laquelle on voulait se renseigner et on se retrouve face aux informations désirées, notamment la date de l'intervention, ses heures de début et de fin, ainsi que la raison pour laquelle une demande d'intervention à distance avait été introduite. Il y a également des liens qui permettent de consulter les fichiers log de SSH et Postgresql, mentionnés auparavant. Ce sont ces fichiers que l'on considère comme les "enregistrements des manipulations", qui sont désormais consultables via la nouvelle interface d'ADbanking.

---

[66] Celles qui seront utilisées pour encrypter les données ultérieurement.
[67] Si les interventions ont toutes eu lieu pendant la même année, la liste sera d'abord triée par mois.
[68] Si les interventions ont toutes eu lieu pendant le même mois, la liste présentera directement les différentes interventions à distance qui ont eu lieu.

Les modifications apportées à l'interface d'ADbanking ont donné lieu à une nouvelle interface qui satisfait dorénavant l'objectif concernant la consultation des interventions et les manipulations enregistrées. En plus, ces modifications ont été faites de manière à ce que l'utilisation de l'interface concernant le contrôle à distance soit intuitive pour un non informaticien, tout en s'intégrant bien à l'interface d'ADbanking.

B.1.5 Attribution et révocation de la permission d'intervention à distance

Afin de pouvoir assurer l'attribution et la révocation de la permission d'intervenir à distance sur le serveur de l'IMF, un système de plages horaires, tel que mentionné ci-dessus, a été mis en place dans l'interface d'ADbanking.

Le principe des plages horaires est que, lorsqu'une IMF remarque un problème pour lequel elle aurait besoin d'une intervention à distance de la part d'AQUADEV, l'IMF lui signale le problème. Une fois les deux entités en contact, elles se mettent d'accord sur la date à laquelle aura lieu l'intervention, ainsi que l'heure de début et de fin de celle-ci. L'IMF procèdera ensuite à la création d'une plage horaire d'intervention dont le début et la fin correspondraient aux heures de début et de fin qui avaient été décidées auparavant. Vu que ces heures représentent la tranche de temps pendant laquelle AQUADEV sera autorisée à accéder à l'IMF, la session d'accès à distance qu'utilisera AQUADEV sera activée et désactivée aux heures de début et de fin de la plage horaire en question. En plus de la création de plages horaires, l'IMF pourra également supprimer ou modifier des plages horaires qui ont été crées précédemment, et tout ceci via la nouvelle interface modifiée d'ADbanking.

C'est par l'intermédiaire de ces plages horaires que se feront l'attribution et la révocation de la permission d'intervention à distance. Par la même occasion, AQUADEV n'aura accès à distance à l'IMF que lorsque celle-ci l'aura décidé. Nous satisfaisons ainsi l'objectif qui avait été fixé par rapport à la permission d'intervention.

B.1.6 Attribution des droits nécessaires pour la maintenance

Il était évidemment hors de question qu'AQUADEV puisse avoir un accès complet au serveur de l'IMF. Il était donc nécessaire de correctement attribuer certains droits d'accès qui sont nécessaires pour pouvoir effectuer la maintenance à distance.

Afin de garantir ceci, une nouvelle session allait être créée sur le serveur de l'IMF, et c'est avec cette session que se connecterait AQUADEV au serveur. Mais nous ne pouvions pas nous arrêter là puisqu'une session normale aurait été trop restrictive et empêcherait l'intervenant de mener à bien la maintenance requise. Nous avons donc discuté avec certains membres de l'équipe de développement à Dakar afin d'établir une liste des droits et des services auxquels ils faisaient appel lorsqu'ils effectuaient les maintenances sur place chez les IMFs.

Par la suite, nous avons transcrit ces droits et services comme étant ceux auxquels il fallait que l'équipe de développement puisse encore accéder malgré les restrictions de la session qu'ils utiliseraient. Le changement des droits d'accès et des permissions d'utilisation de ces services ont été effectués sans trop de problèmes, sauf un. Il s'agissait d'un fichier de configuration de la base de données, *postgresql.conf*, auquel AQUADEV aurait bien voulu pouvoir accéder en lecture-écriture. Le problème était que le service Postgresql refusait de démarrer si les droits d'accès au fichier *postgresql.conf* étaient étendus à d'autres utilisateurs.

Nous avons essayé toutes sortes de combinaisons de droits d'accès mais il n'y avait rien à faire, même un simple accès en lecture n'était plus possible.

A part l'impossibilité d'accéder au fichier *postgresql.conf*, nous pouvons dire que l'objectif a bien été rencontré, d'autant plus que l'accès à ce fichier n'était pas tout à fait indispensable. Evidemment l'accès à ce fichier aurait représenté une facilité pour l'intervenant, mais jusqu'à présent aucune solution n'a été trouvée pour résoudre ce problème d'accès sans compromettre le bon fonctionnement de Postgresql.

B.1.7 Coupure manuelle de la connexion du côté de l'IMF

Par défaut, la connexion d'accès à distance peut être interrompue par l'IMF à tout moment. En effet, vu que la connexion est établie via modem, il suffirait que l'IMF débranche le câble téléphonique du modem de l'ordinateur servant de passerelle au réseau local de l'IMF pour couper la connexion. Une autre manière, moins radicale, serait d'arrêter le processus du démon SSH, "sshd", sur l'ordinateur passerelle pour interrompre la première connexion SSH. Ou encore, l'IMF pourrait couper la connexion *Dial-up* qui avait été établie entre l'ordinateur passerelle et l'ordinateur de l'intervenant distant se trouvant chez AQUADEV.

Malgré ces différents moyens de déconnexion, une autre approche a été implémentée afin de pouvoir déconnecter l'intervenant de façon plus "propre". Cette fonctionnalité supplémentaire a été intégrée dans l'interface d'ADbanking par un système d'affichage des plages horaires. Ce système affiche non seulement les plages horaires qui ont été créées, mais il met aussi en évidence une plage horaire si celle-ci est en cours au moment de l'affichage. Si c'est le cas, on trouvera, en dessous de la plage horaire en cours, un bouton qui permettra d'arrêter la plage horaire en question. Le fait d'interrompre une plage horaire en cours a comme effet de désactiver la session utilisée pour l'accès à distance[69], ce qui empêcherait donc à AQUADEV de pouvoir se reconnecter avant le début de la prochaine plage horaire.

A première vue, on pourrait croire que l'objectif a été atteint, mais il persiste un problème plutôt gênant. Si le mécanisme mis en place empêche bien qu'AQUADEV ne puisse pas se reconnecter ultérieurement, elle ne permet pas pour autant de le déconnecter. C'est-à-dire que la commande Linux qui permet la désactivation d'une session, a été implémentée d'une telle façon à ce que la désactivation n'ait lieu qu'une fois que l'utilisateur aura fermé la session. Donc tant que l'intervenant n'aura pas fermé la session d'accès à distance, il pourra continuer à faire ce qu'il voudra sur le serveur.

Pour contourner ce problème, l'idéal aurait été de pouvoir automatiquement déconnecter la session SSH d'AQUADEV à la fin de la plage horaire. Ceci permettrait que la session d'accès à distance puisse être désactivée avant qu'AQUADEV n'ait le temps de rétablir une connexion SSH. Le problème c'est que, jusqu'à présent, nous ne voyons pas d'autre manière pour réaliser cela que le démarrage du service SSH. Le désavantage de ce genre de solution est que ça couperait toute autre connexion SSH qui serait en cours au même moment, ce qui pourrait être indésirable si un employé de l'IMF était en train de travailler en étant connecté au serveur.

B.1.8 Coupure manuelle de la connexion du côté d'AQUADEV

Comme pour l'IMF, un mécanisme de déconnexion "propre" a également été mis en

[69] Comme nous le verrons par la suite, cette désactivation n'a pas comme effet de déconnecter l'utilisateur. Elle n'aura donc pas d'effets sur la cohérence du serveur.

œuvre afin qu'AQUADEV puisse mettre un terme à la connexion en cours autrement qu'en débranchant le câble téléphonique ou qu'en arrêtant la connexion *Dial-up* ou SSH.

Ce mécanisme consiste en la création d'un fichier exécutable lors du début de la plage horaire qui était prévue. Vu que ce fichier est sauvegardé dans le répertoire racine de la session qu'utilise AQUADEV pour se connecter, ce dernier peut facilement y accéder et l'exécuter. Ceci fera que la session d'accès distant soit désactivée et empêchera donc toute tentative d'établir une nouvelle connexion avant la prochaine plage horaire.

Malheureusement, le mécanisme concerné présente la même faille que pour la déconnexion par l'IMF. C'est-à-dire qu'il peut efficacement empêcher toute nouvelle tentative de connexion, mais il n'est pas capable de déconnecter l'intervenant. Encore une fois, on pourrait utiliser le même système que celui proposé à la section précédente pour résoudre ce problème, mais les inconvénients resteraient les mêmes.

B.1.9 Coupure automatique de la connexion

En plus de la coupure manuelle de la connexion par AQUADEV ou l'IMF existe également la possibilité de couper la connexion d'accès à distance après un certain laps de temps. Cette fonctionnalité a été intégrée dans l'interface modifiée d'ADbanking à travers l'implémentation du système de plages horaires. En effet, lorsque la plage horaire touche à sa fin, la session d'accès à distance est désactivée automatiquement et, encore une fois, empêche ainsi qu'on puisse se reconnecter avec cette session.

A nouveau, ce mécanisme utilise la même logique que les deux premiers. Nul besoin de répéter que ce système présente la même faille que les deux mentionnés précédemment.

B.2 Critique générale

Comme nous avons pu le constater, les objectifs qui avaient été fixés avant le début du stage ont, pour la plus grande partie, été satisfaits. Il y a certes eu quelques manquements pour certains des objectifs, ce qui était principalement dû à un manque de temps. A la source de ce manque de temps se trouvaient bien sûr certains évènements imprévisibles mais également une planification qui aurait pu être mieux faite. D'ailleurs, si le stage était à refaire, on aurait porté plus d'attention à certains détails.

Cette deuxième partie du présent chapitre sera donc le recueil de critiques plus générales, qui ont également leur importance mais qui ne sont pas directement liés aux objectifs à proprement parler.

B.2.1 Analyse des besoins

Le stage a débuté par l'établissement d'une analyse des besoins afin de pouvoir se familiariser avec le contexte dans lequel allait se faire le travail et également pour préciser davantage les objectifs du stage. En général, l'analyse des besoins a été bien menée à tous les niveaux, mais elle aurait pu être mieux faite. Par exemple, nous aurions dû approfondir la question des serveurs se trouvant chez les IMFs. Si cela avait été fait, nous aurions su dès le départ que les ordinateurs, servant de serveurs chez les IMFs, tournaient sur une version de Linux faite pour serveurs. Ceci implique qu'il n'y avait donc pas d'interface graphique sur les

serveurs et nous aurions su tout de suite qu'une solution du style NX était peu utile dans notre cas. Si c'était le cas, nous aurions pu gagner tout le temps passé sur les tests de déploiement de l'application en question.

B.2.2 Modems

En plus du temps perdu suite à ce manque de rigueur dans l'analyse sont venus s'ajouter d'autres problèmes. Il y avait notamment le problème de la reconnaissance des modems sous Linux. Nous avions été prévenus de la possibilité de survenance de ces problèmes, et par conséquent nous avions prévu le temps nécessaire à leur résolution dans la planification. Néanmoins, plus de temps a été alloué à ces problèmes que ce qui était prévu, principalement à cause d'une obstination à vouloir résoudre ce problème à tout prix.

A un moment donné nous nous sommes dit qu'il était temps de chercher une autre solution et c'est à ce moment-là que nous avons opté pour l'établissement du contrôle distant par l'intermédiaire d'un ordinateur servant de passerelle dans le réseau local de l'IMF. Seulement, lorsque cette solution fut trouvée et que nous allions procéder à des tests, un autre problème est survenu. Il s'agissait notamment de l'établissement de la connexion *Dial-up*.

Afin de pouvoir tester l'établissement de connexions *Dial-up*, il fallait avoir accès à une ligne téléphonique sortante. Evidemment la seule ligne sortante se trouvait au secrétariat donc il ne fallait pas qu'on empêche les appels téléphoniques d'atteindre AQUADEV en monopolisant la ligne téléphonique toute la journée. Puisqu'il fallait attendre l'heure de fermeture avant de pouvoir effectuer des tests, le temps qui avait été alloué à cette phase a également été tiré en longueur.

Mais à ceci s'est ajouté un problème avec la ligne sortante elle-même. Le problème était que, lorsqu'on essayait d'établir une connexion, un message d'erreur s'affichait en disant qu'il fallait une ligne de téléphone analogique et non numérique pour effectuer cette connexion. Pendant longtemps nous étions persuadés que la ligne téléphonique était bien une ligne analogique, mais en fin de compte nous avons essayé sur une deuxième ligne qui était réservée au fax et cette fois là ça avait marché. Nous avions donc également passé un temps considérable, et plus que prévu, sur ce problème dû à notre conviction sur la nature de la ligne téléphonique.

B.2.3 Tests

Malheureusement, tout ceci nous a fait perdre pas mal de temps qui aurait pu être mis à profit pour améliorer la solution finale. Par exemple, davantage de temps aurait pu être investi dans les tests d'acceptation de la solution finale. Nous aurions peut être même eu l'occasion de pouvoir effectuer ces tests sur un vrai cas pratique pour une IMF qui avait des problèmes vers la fin du stage.

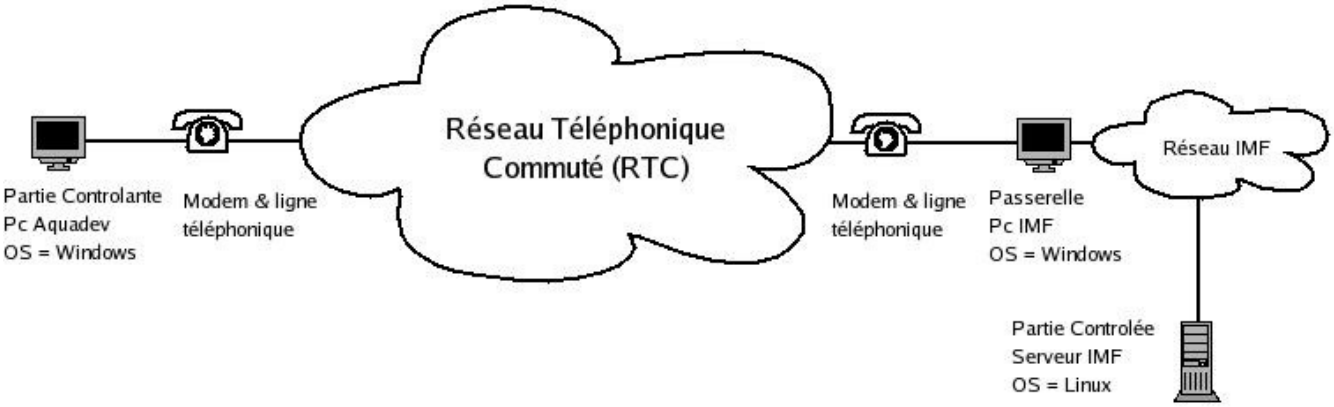
En effectuant ces tests nous aurions pu nous rendre compte immédiatement de l'existence des failles de sécurité mentionnées précédemment et y apporter les solutions adaptées. Nous aurions également pu découvrir plus tôt une faille qui se trouve au niveau de Cygwin. En effet, après le stage nous nous sommes rendus compte que, une fois la première connexion établie sur l'ordinateur passerelle, et par conséquent sur Cygwin, il y a moyen de "sortir" de l'environnement Linux pour se retrouver dans l'environnement Windows. A ce moment-là, l'intervenant distant aurait été libre de faire ce qu'il voulait avec l'ordinateur passerelle, que ses intentions soient bonnes ou mauvaises.

B.2.4 Temps

En voyant ce qui a été dit précédemment, il est clair qu'une solution plus sécurisée aurait pu être mise en place. Cependant la perte de temps liée à la survenance des évènements mentionnés auparavant justifie le fait qu'une telle solution n'a pas pu être implémentée sur la durée prévue du stage. En fin de compte, nous estimons que notre stage a été fructueux.

Annexe II : Document de stage – Procédure à suivre

Scénario:



Description:

Nous nous trouvons dans une situation où une IMF a besoin d'être "dépannée" (suite à une incohérence dans la base de données, un bug dans ADbanking, etc) mais ne possède pas de connexion internet. L'IMF a un réseau local dans lequel se trouvent le serveur de l'IMF et un ordinateur qui fait office de passerelle. A part le téléphone, l'IMF est donc "coupée du monde", donc on va l'atteindre via le Réseau Téléphonique Commuté (RTC). C'est à dire que nous utiliserons des modems et des lignes téléphoniques pour établir la connexion avec l'IMF distante. Mais l'utilisation du modem pose certains problèmes, notamment la difficulté de reconnaissance du modem sous Linux (lorsqu'il s'agit d'un winmodem ou softmodem) et la difficulté de trouver un "vrai" modem externe (même au Sénégal). D'où l'idée d'utiliser un ordinateur tournant sous Windows comme "passerelle" chez l'IMF pour qu'on puisse établir la connexion entre Aquadev et l'IMF. Via la connexion à la "passerelle" sous une session CAD (Contrôle A Distance), on pourra accéder au serveur pour pouvoir y effectuer les changements nécessaires.

Pré-requis:

- Installation correcte d'ADbanking chez l'IMF
- Installation correcte du système de contrôle à distance

Procédure:

Lorsque l'IMF rencontre un problème qu'elle n'arrive pas à résoudre par elle même, elle fait appel à Aquadev (via téléphone, mail, Skype, etc...). Lors de ce contact, l'IMF communiquera un nouveau mot de passe pour la session "CAD" (mot de passe qui sera utilisé pour établir la connexion avec l'IMF), transmettra le numéro de téléphone à composer pour

l'atteindre, et fixera l'heure à laquelle aura lieu le "dépannage". Un peu avant l'heure convenue, l'IMF veillera à effectivement changer le mot de passe sur le serveur (via l'interface d'ADbanking) ET l'ordinateur passerelle, pour qu'il corresponde bien à celui qu'elle aura communiqué à Aquadev. Elle veillera également à brancher la ligne téléphonique appropriée au modem de l'ordinateur passerelle. Aquadev établira alors une connexion SSH sur l'ordinateur "passerelle" et ensuite établira une deuxième connexion SSH sur le serveur de l'IMF. À partir d'ici, Aquadev pourra effectuer les opérations nécessaires pour tenter de venir à bout du problème.

Lorsque la session de "dépannage" aura pris fin, il ne faut pas que l'IMF oublie de débrancher le câble téléphonique du modem. L'IMF veillera également à rechanger le mot de passe de la session "CAD" sur le serveur ET l'ordinateur "passerelle".

Annexe III : Document de stage – Utilisation Partie Contrôlante

Configuration avant le Contrôle à Distance

Cette étape est à faire avant l'installation du système de Contrôle à Distance chez l'IMF que vous voulez contacter.

A.Créer une paire de clés publique et privée

(Traduction partielle et amélioration de la procédure trouvée sur http://the.earth.li/~sgtatham/putty/0.58/puttydoc.txt)

N.B. Avant de commencer, il faut savoir que deux solutions sont possibles. Soit vous créez une paire de clés pour l'ensemble des IMFs (c'est-à-dire que vous garderez votre unique clé privée et toutes les IMFs auront la même clé publique), soit vous créez une nouvelle paire de clés pour chaque IMF (c'est-à-dire que vous aurez autant de clés privées que d'IMFs que vous comptez contacter et chaque IMF aura sa propre clé publique). Chaque solution a ses avantages et ses désavantages:

Solution à une seule paire de clés

Avantages:
- facilité à effectuer le contrôle à distance du fait qu'il n'y a qu'une seule clé privée pour contacter toutes les IMFs que vous voulez
- pas besoin de se demander quelle est la clé privée correspondant à telle ou telle IMF

Désavantages:
- si l'unique clé privée est supprimée ou corrompue, il faut contacter toutes les IMFs pour leur fournir une nouvelle clé publique valable
- si l'unique clé privée est perdue ou volée, il faut contacter toutes les IMFs pour qu'elles n'acceptent plus des demandes d'accès venant de cette clé privée et leur fournir une nouvelle clé publique

Solution à plusieurs paires de clés

Avantages:
- si une des clés privées est supprimée ou corrompue, il suffit de contacter qu'une seule IMF pour lui fournir une nouvelle clé publique valable
- si une des clés privées est perdue ou volée, il suffit de contacter qu'une seule IMF pour qu'elle n'accepte plus des demandes d'accès venant de cette clé privée, et lui fournir une nouvelle clé publique

Désavantages:
- chaque IMF a une clé privée correspondante, quelle est la clé privée correspondant à l'IMF qu'on essaye de contacter?
- si une des clés privées est perdue ou volée, il y a de fortes chances qu'elle ne soit pas

la seule à l'avoir été, donc a ce moment la il faudrait quand même contacter plusieurs IMFs

Pré requis:
\

Procédure:

- obtenir PuTTYgen.exe à partir du package d'installation ou bien de http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
- double cliquer sur l'icône de PuTTYgen.exe
- dans la section "Parameters", s'assurer que l'option "SSH-2 RSA" a été choisie
- dans le champ "Number of bits in a generated key", garder la valeur 1024
- Ensuite cliquer sur "Generate"
- Une fois que vous avez cliqué sur "Generate", vous remarquerez que la barre d'état d'avancement n'avance plus. En fait le programme attend que vous secouiez la souris au dessus de l'espace vide se trouvant en dessous de la barre d'état d'avancement. Au fur et à mesure que vous faites ceci, la barre d'état d'avancement progressera. Ceci n'est pas une blague! C'est un moyen de créer l'aspect aléatoire dans la création des clés.
- Une fois que vous aurez "secoué votre souris", la génération de la parie de clés commencera
- Dans le prochain écran se trouve un champ "Key Comment", vous pouvez entrer un nom pour la clé. Ceci est particulièrement utile si vous optez pour la création d'une paire de clés par IMF (voir plus haut). Si vous hésitez, il y a toujours moyen de modifier le nom par la suite
- Dans le champ "Key passphrase", il faut entrer une sorte de mot de passe qui est préférablement une "phrase" de passe. Ceci protégera la clé sur votre ordinateur, donc même si quelqu'un s'empare de votre clé, il ne pourra l'utiliser qu'en connaissant la "phrase" de passe. Evidemment, plus la phrase est longue, plus sur ce sera! Le champ d'en dessous demande la confirmation de cette phrase. Il ne faut surtout pas oublier cette phrase, il n'y a pas moyen de récupérer la clé d'une autre façon.
- Ensuite sauvegarder vos clés publique et privée en faisant "Save private key" et "Save public key", un chemin d'accès vous sera demandé
- Voilà, maintenant vous êtes prêt à copier la clé publique du coté du serveur (voir ConfigurationPartieControlée)!

Comment établir un Contrôle à Distance

Les manipulations suivantes sont les étapes à suivre, sous Windows XP Pro (possiblement de fortes ressemblances sous d'autres versions de Windows), pour préparer votre ordinateur à appeler une machine distante.

Ces manipulations ne seront d'une utilité que si l'IMF que vous voulez contacter a été convenablement configuré auparavant.

B. Créer une connexion à l'ordinateur distant:

Pré requis:
\

Procédure:

- Aller dans "Démarrer>Panneau de Configuration>Connexions réseau et Internet>Créer une connexion au réseau sur votre lieu de travail"
- Garder l'option "Connexion d'accès à distance"
- Entrer n'importe quel nom pour nommer la connexion (de préférence quelque chose de significatif comme le nom et emplacement de l'IMF)
- Entrer le numéro de téléphone à composer (vous pouvez toujours le changer par la suite)
- A vous de décider si vous voulez "Ajouter un raccourci vers cette connexion sur mon Bureau" et ensuite cliquer sur "Terminer"

Il se peut que pendant ces étapes on vous demande un nom d'utilisateur et un mot de passe, ceux-ci correspondent au nom d'utilisateur et au mot de passe de votre session sur l'ordinateur distant!
A ce moment une connexion devrait être créée. Pour vérifier que ce soit bien le cas vous pouvez aller dans "Démarrer>Connexions>Afficher toutes les connexions" ou bien dans "Démarrer>Favoris Réseau>Afficher les connexions réseau" et regarder qu'il existe bien une icône sous "Accès à distance" qui porte le nom que vous venez de donner à la connexion. Vous pouvez également vérifier sur le bureau si vous avez coché cette option lors de la création de la connexion.

Résolution de problèmes:

Normalement il ne devrait pas y avoir de problèmes ici à moins que le modem ne soit pas bien installé. Si c'est le cas, réinstaller ou mettre à jour les pilotes.

C. Etablir la connexion avec l'ordinateur distant:

Pour éviter de ralentir la connexion, il est fortement conseillé d'arrêter tout téléchargement ou toute utilisation d'Internet qui serait en cours. De même pour l'IMF.

Pré requis:

- Création d'une connexion à l'ordinateur distant (voir section A)
- La passerelle Windows du coté de l'IMF doit être allumé et convenablement configuré
- Bien vérifier que l'IMF et vous-même soyez bien sur un réseau téléphonique analogique!!!

Procédure:

- Aller dans "Démarrer>Connexions>Afficher toutes les connexions" ou bien dans "Démarrer>Favoris Réseau>Afficher les connexions réseau"
- Sélectionner l"Accès à distance" que vous voulez établir (si vous avez plusieurs

"Accès à distance" et que vous n'êtes pas sur de celle qui correspond à l'IMF que vous voulez joindre, faites un clique droit sur l'icône et allez dans propriétés, ceci révèlera le numéro de téléphone qui sera composé)
- Après avoir sélectionné la connexion appropriée, une fenêtre apparaîtra avec un champ "Nom d'utilisateur" et un champ "Mot de Passe", ceux-ci correspondent à votre session sur l'ordinateur distant!
- Remplir ces champs avec les informations correctes si ce n'est pas déjà le cas
- Vérifier que le numéro de téléphone soit correct et ensuite cliquer sur "Numéroter"
- Normalement, à partir d'ici tout devrait se passer sans problèmes et une icône représentant la connexion devrait apparaître dans le "System Tray" en bas à droite de votre écran
- Vous pouvez faire un double-clique sur cette icône pour afficher des informations sur la connexion. En allant dans l'onglet "Détails" vous pouvez obtenir l'adresse IP de la passerelle de l'IMF ("adresse IP du serveur")

Résolution de problèmes:

N.B. si vous êtes sur un réseau téléphonique interne, il se peut que vous ayez à composer un "0," ou un "9,", le chiffre étant celui que vous utilisez pour téléphoner à l'extérieur, suivi d'une virgule pour marquer un temps d'attente avant la numérotation du numéro de téléphone

"Connected phone line is not compatible with this modem. Only analog phone lines are supported.":
- Vérifier que vous êtes bien sur une ligne normale. Ceci peut se faire en vérifiant qu'il y ait bien une tonalité avec un téléphone normal (veiller à ce que ce soit bien un téléphone normal et pas un standard, ça change tout!). Si il n'y a pas de tonalité avec un téléphone normal, il y a beaucoup de chances que la ligne physique desserve plusieurs lignes à un standard et donc ne marchera pas pour le contrôle à distance. Essayer avec une autre ligne téléphonique.

"Erreur 649: Le compte n'a pas l'autorisation de recevoir les appels entrants":
- Il faut que le coté contrôlé vous donne l'autorisation d'y accéder, il faudra les contacter pour qu'ils le fassent
- Si ils ne savent pas comment faire, il faudra leur dire d'aller dans "Démarrer>Connexions>Afficher toutes les connexions " ou bien "Démarrer>Favoris Réseau>Afficher les connexions réseau", faire un clique droit sur l'icône des "Connexions entrantes" et rentrer dans "Propriétés". Aller dans l'onglet "Utilisateurs" et cocher la session appropriée et cliquer sur "Ok".

"Erreur 678: L'ordinateur distant n'a pas répondu. Pour obtenir de l'assistance, cliquez sur Plus d'informations ou recherchez le numéro de cette erreur dans le centre d'aide et de support":
- Vérifier que la ligne téléphonique soit bien branchée dans le modem et que le modem soit bien branché au poste de travail si il s'agit d'un modem externe.

"Erreur 680: Il n'y a pas de tonalité":
- Aller dans "Démarrer", clique droit sur "Poste de Travail", "Propriétés>Matériel>Gestionnaire de Périphériques>Modems". Double-cliquer sur le modem approprié et aller dans l'onglet "Modem". Dans la partie "Contrôle de

numérotation", décocher l'option "Attendre la tonalité avant la numérotation".

- Si ça persiste, vérifier qu'il y ait bien une tonalité avec un téléphone normal (veiller à ce que ce soit bien un téléphone normal et pas un standard, ça change tout!). Si il n'y a pas de tonalité avec un téléphone normal, essayer avec une autre ligne téléphonique.
- Si il y a une tonalité avec le téléphone normal mais que vous n'arrivez pas à composer, vérifier que vous n'êtes pas sur une ligne interne. Si c'est le cas, quel numéro devez vous entrer (pour avoir la ligne externe) avant de composer un numéro de téléphone à l'extérieur? Normalement il suffit d'entrer ce préfixe, suivi d'une virgule, avant le numéro de téléphone que vous voulez atteindre (la virgule marque une pause, le temps que vous ayez la ligne externe).

D.Etablir une connexion SSH via l'outil Putty:

Pré requis:

- Connexion en cours, via modem, avec l'IMF (voir section B)
- Connaissance de l'adresse IP de l'IMF (voir 2 dernières étapes de la procédure de la section B)
- La passerelle Windows du coté de l'IMF doit être allumé et convenablement configuré

Procédure:

- Commencer par se procurer l'installeur de Putty via ADFinance ou sur http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
- Double cliquer sur l'icône de Putty
- Vous verrez un écran qui est partagé en deux parties. A gauche il y a la partie " Category" qui contient une liste. La partie de droite change lorsqu'on clique sur les différents éléments de la liste à gauche dans " Category"
- Aller dans "Category>Session", et dans la partie de droite entrer l'adresse IP à laquelle vous voulez vous connecter dans "Host Name (or IP address)"
- S'assurer, dans la partie "Protocol", que l'option "SSH" à été choisie
- Aller dans "Category>Terminal", et pour "Local echo" dans la partie "Line discipline options", cocher la case "Force off".
- Aller dans "Category>Connection>SSH", dans "Protocol Options" cocher la case "Enable Compression"
- Aller dans "Category>Connection>SSH>Auth". A droite, dans le "Authentication Parameters", cliquer sur le bouton "Browse" qui se trouve à droite du champ de texte intitulé "Private key file for authentication". Ensuite sélectionner la clé privée que vous avez généré auparavant et qui correspond à l'IMF que vous allez tenter de contacter.
- De retour dans "Category>Session", si vous voulez, vous pouvez attribuer un nom à la connexion dans le champ "Saved Sessions" et cliquer sur "Save" dans la partie de droite pour sauvegarder la configuration
- Une fois que tout ceci a été fait, cliquer sur "Open" ou double-cliquer sur la session que vous venez de nommer
- Ceci ouvrira une fenêtre genre commandes MS-DOS et Putty vous affichera un message (auquel vous répondrez "oui") dans le genre:

```
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
```

```
The server's rsa2 key fingerprint is:
ssh-rsa 1024 7b:e5:6f:a7:f4:f9:81:62:5c:e3:1f:bf:8b:57:6c:5a
If you trust this host, hit Yes to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the
connection.
```

- Vous êtes maintenant connecté via SSH au poste Windows servant de passerelle chez l'IMF. Connectez vous au serveur en tapant la commande "ssh CAD@*serveur*" où *serveur* est l'adresse IP ou le nom du serveur de l'IMF. Putty vous répondra probablement avec la question suivante (à laquelle vous répondrez "yes")

```
The authenticity of host 'serveur' can't be established.
RSA key fingerprint is
ad:1a:1e:51:f6:b3:ed:73:31:b5:a0:d7:b8:6a:e3:1c.
Are you sure you want to continue connecting (yes/no)?
```

-
- Vous pouvez maintenant effectuer les opérations nécessaires pour le dépannage
- Pour arrêter la connexion SSH, taper "exit" dans la fenêtre de Putty ou simplement fermer la fenêtre

Résolution de problèmes:

"Server refused our key":

- S'assurer d'avoir bien recopié la clé publique sur le serveur

Annexe IV : Document de stage – Utilisation Partie Contrôlée

Comment permettre un Contrôle à Distance

Les manipulations suivantes sont les étapes à suivre, sous Windows XP Pro, pour permettre à votre ordinateur de recevoir des appels d'une machine distante.

Ces manipulations ne seront d'une utilité que si l'IMF a été convenablement configuré auparavant.

A. Comment accepter les appels entrants:

Ces étapes sont à faire sur le poste client Windows servant de passerelle!

Pré requis:

- L'existence d'une session CAD sur le système
- Modem installé, fonctionnant correctement
- Ligne téléphonique branchée au modem du poste client Windows servant de passerelle

Procédure:

- Aller dans "Démarrer>Connexions>Afficher toutes les connexions>Créer une nouvelle connexion" ou bien "Démarrer>Favoris Réseau>Afficher les connexions réseau>Créer une nouvelle connexion" et cliquer sur "Suivant"
- Choisir l'option "Configurer une connexion avancée"
- Garder l'option "Accepter les connexions entrantes"
- Choisir le modem approprié
- Garder l'option "Ne pas autoriser les connexions privées virtuelles"
- Sélectionner seulement la session "CAD" pour qu'elle soit la seule session via laquelle on puisse accéder à votre ordinateur
- Vérifier que le protocole TCP/IP soit sélectionné (si il n'existe pas dans la liste, le rajouter)
- Cliquer sur "Terminer"

B. Comment NE PLUS accepter les appels entrants:

Ces étapes sont à faire sur le poste client Windows servant de passerelle!

Pré requis:

\

Procédure:

- Aller dans "Démarrer>Connexions>Afficher toutes les connexions" ou bien

"Démarrer>Favoris Réseau>Afficher les connexions réseau"

- Faire un clique droit sur l'icône "Connexions entrantes" et choisir supprimer
- De préférence, il vaut mieux également changer le mot de passe de la session CAD sous Windows (voir section suivante) et même débrancher la ligne téléphonique du modem

C. Comment changer le mot de passe de la session CAD

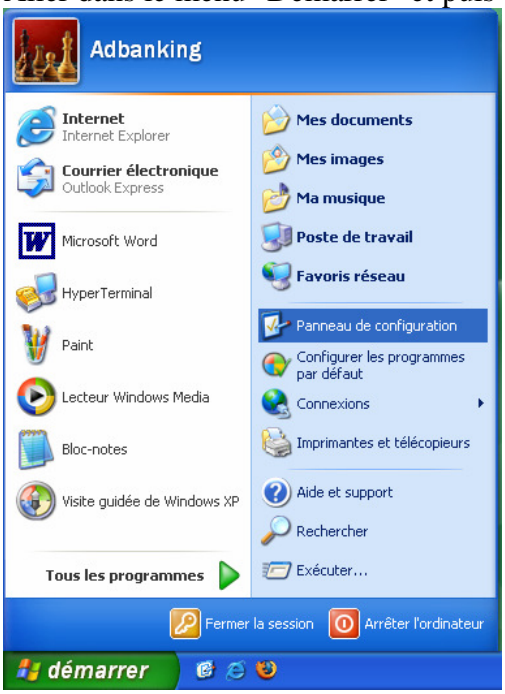
Ces étapes sont à faire sur le poste client Windows servant de passerelle!

Pré requis:

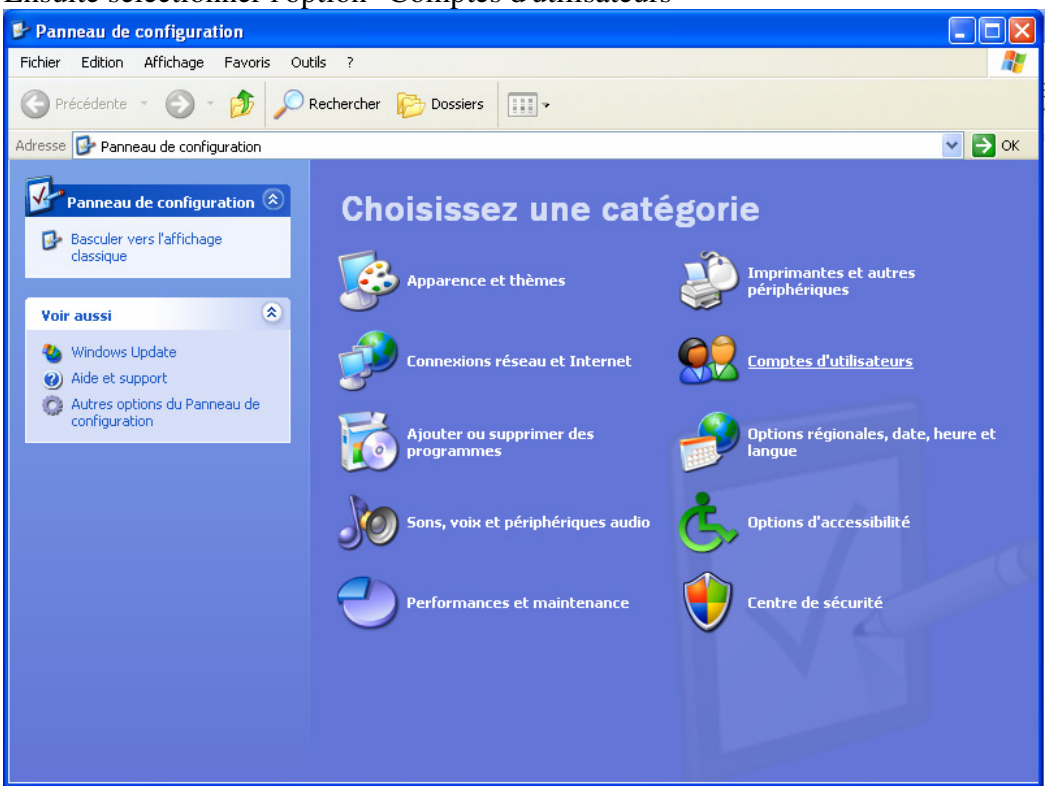
\

Procédure:

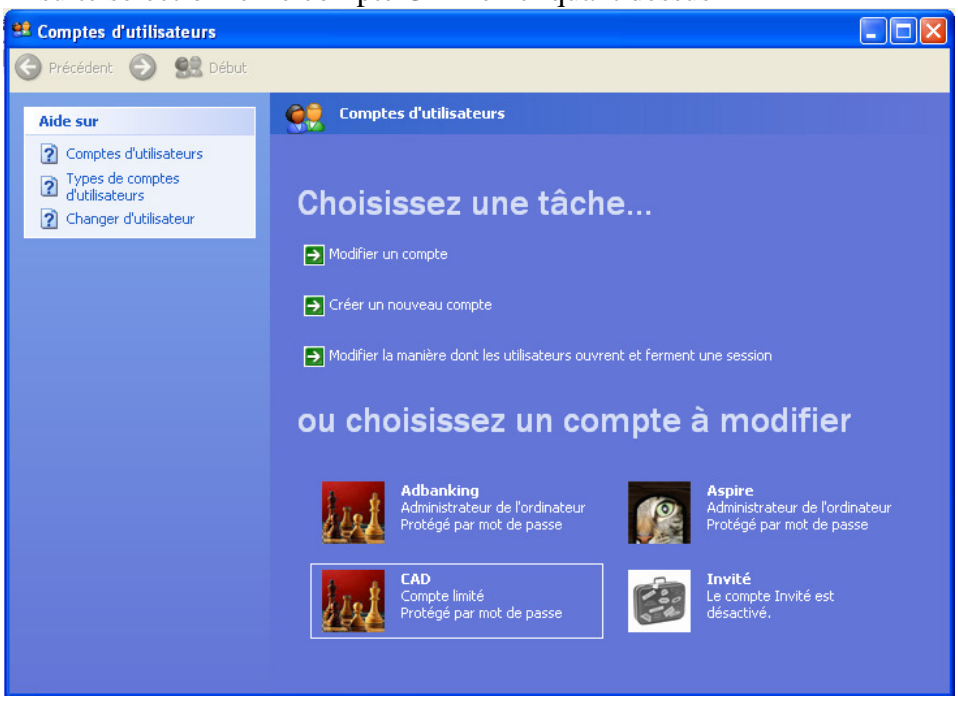
Aller dans le menu "Démarrer" et puis dans "Panneau de Configuration"



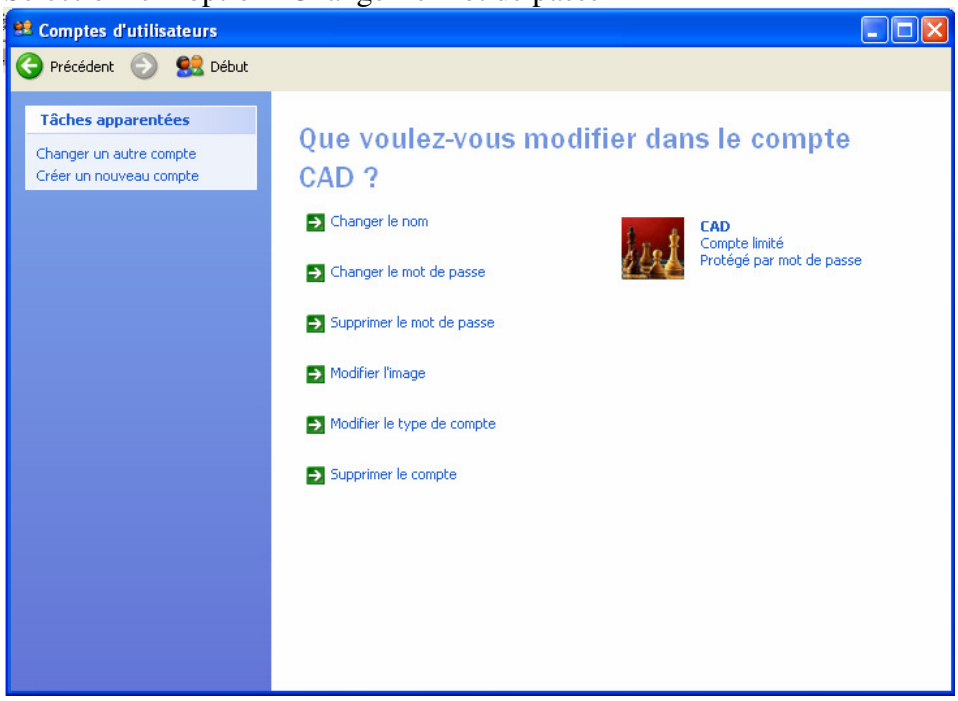
Ensuite sélectionner l'option "Comptes d'utilisateurs"



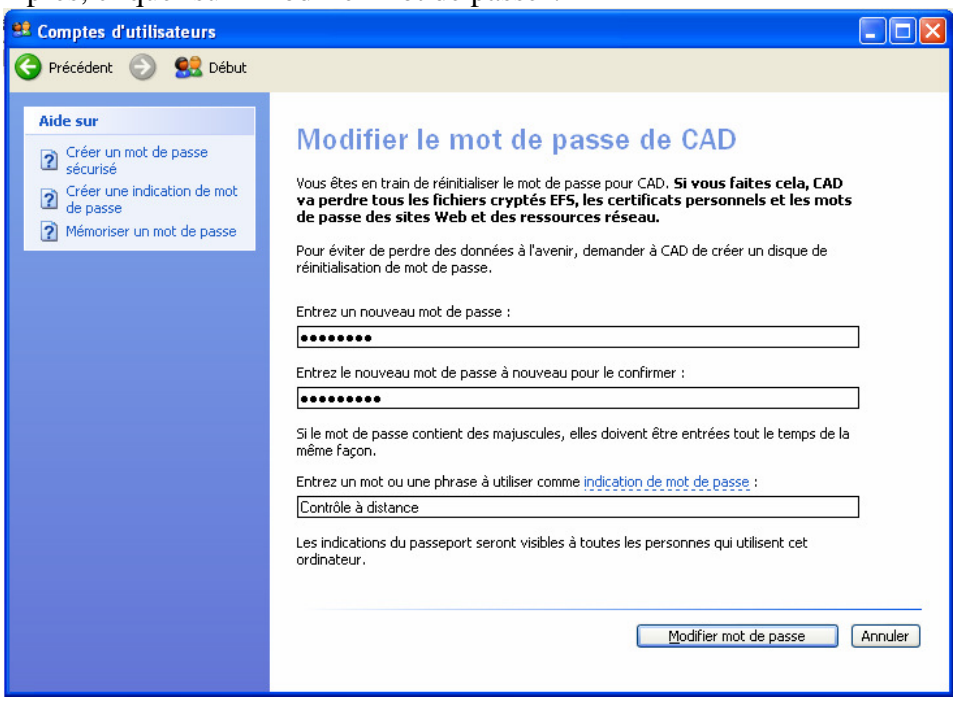
Ensuite sélectionner le compte CAD en cliquant dessus



Sélectionner l'option "Changer le mot de passe"



Finalement, entrer le nouveau mot de passe dans les deux premiers champs et, si vous le souhaitez, modifier le mot ou la phrase qui sert à vous rappeler le mot de passe en cas d'oubli. Après, cliquer sur "Modifier mot de passe".



Annexe V : Document de stage – Configuration Partie Contrôlée

Configuration de la Partie Contrôlée

Étapes à suivre:

A. créer une session "CAD" (Contrôle A Distance) sur le serveur
B. configuration pour permettre la "traçabilité" des informations utiles
C. créer une session "CAD" sur la passerelle Windows
D. installer cygwin sur la passerelle Windows
E. copier la clé publique sur la passerelle Windows

A. Créer une session "CAD" (Contrôle A Distance) sur le serveur

Ces étapes sont à faire sur le poste client Windows servant de passerelle!

Pré requis:

\

Procédure:

On commence par créer une session "cad" sous Linux et Postgresql

- ouvrir un terminal
- se logger en tant que root en tapant "su -" et en fournissant le mot de passe root
- exécuter le script "creationSessionCAD"
- lorsqu'il demande "Shall the new user be allowed to create databases? (y/n)", répondre "n"
- lorsqu'il demande "Shall the new user be allowed to create more new users? (y/n)", répondre "n"
- si il répond "CREATE USER", c'est bon, l'utilisateur "cad" a été créé dans postgresql et sous linux!

Ensuite on va modifier les droits d'accès à la bd "adbanking" pour que la session "cad" puisse y avoir accès:

- ouvrir un terminal
- se logger en tant qu'adbanking
- exécuter le script "modifDroitsBD"
- si il répond avec une liste de "GRANT", c'est que les modifications de droit d'accès ont étés fait correctement!

Il faut maintenant procéder à une configuration pour la session "cad":

Appartenance au groupe adbanking

- se logger en tant que root
- ouvrir fichier /etc/group
- chercher la ligne qui ressemble à "adbanking:x:501:" (vers la fin du fichier normalement)
- ajouter "cad" à la fin pour que le résultat final ressemble à "adbanking:x:501:cad"
- #chercher la ligne qui ressemble à "postgres:x:26:" (vers la fin du fichier normalement)
- #ajouter "cad" à la fin pour que le résultat final ressemble à "postgres:x:26:cad"
- sauvegarder le fichier

Accès au démarrage des services apache, postgresql, et network:

- taper "visudo"
- à la fin du fichier qui apparaitra, rajouter la ligne "cad ALL=/sbin/service network start, /sbin/service network stop, /sbin/service network restart, /sbin/service network status, /sbin/service postgresql start, /sbin/service postgresql stop, /sbin/service postgresql restart, /sbin/service postgresql status, /sbin/service httpd start, /sbin/service httpd stop, /sbin/service httpd restart, /sbin/service httpd status"
- lorseque vous "contrôlerez à distance", ces services pourront être utilisés en tapant par

exemple "sudo /sbin/service network status"

- rajouter également la ligne "apache ALL=NOPASSWD: /usr/bin/passwd -l cad, /usr/bin/passwd -u cad" et sauvegarder le fichier

B. Configuration pour permettre la "traçabilité" des informations utiles

Ces étapes sont à faire sur le serveur!

Pré requis:

- la création de la session "cad" sur le serveur

Procédure:

Avant toute chose, on se log en tant que root en tapant "su -" et en fournissant le mot de passe root.

On commence par configurer syslog pour recevoir les logs de sshd et postgresql:

- ouvrir le fichier /etc/syslog.conf
- rajouter les lignes "auth.* /home/adbanking/.contadis/logs/sshd.log" et "local0.* /home/adbanking/.contadis/logs /postgresql.log"

Ensuite on configure sshd pour qu'il envoie ses logs au démon syslog:

- ouvrir le fichier /etc/ssh/sshd_config
- dans la section "# Logging", s'assurer que la ligne "SyslogFacility" apparaisse sans # et qu'elle soit suivie de "AUTH"
- s'assurer également que la ligne "LogLevel" apparaisse sans # et qu'elle soit suivie de "DEBUG"
- si ce n'est pas le cas, faire les modifications et supprimer toute autre ligne contenant "SyslogFacility" ou "LogLevel" qui n'est pas précédée de "#".

Ensuite on configure postgresql pour qu'il envoie ses logs au démon syslog:

- ouvir le fichier /var/lib/pgsql/data/postgresql.conf
- dans la section "Error Reporting and Logging", ajouter les lignes suivantes (préférablement juste après leurs valeurs par défaut):
  - syslog = 2
  - log_connections = true
  - log_pid = true
  - log_statement = true
  - log_timestamp = true
- vérifier que la valeur par défaut de syslog_facility = 'LOCAL0'
- ouvrir le fichier /etc/init.d/postgresql
- chercher la ligne "PGLOG=/dev/null" et la changer à "PGLOG=/var/log/postgresql.log"

Petite configuration pour que le module de contrôle à distance d'adbanking puisse fonctionner:

- ouvrir le fichier /etc/passwd
- chercher la ligne commençant avec "apache"
- si cette ligne se termine avec "/sbin/nologin" modifier la ligne en remplaçant "/sbin/nologin" par "/bin/bash"
- par exemple, si vous trouvez la ligne "apache:x:48:48:Apache:/var/www:/sbin/nologin", vous la remplacerait par "apache:x:48:48:Apache:/var/www:/bin/bash"

Vous pouvez maintenant soit redémarrer les services postgresql et syslog en tapant "service syslog restart" et "service postgresql restart" soit redémarrer l'ordinateur pour prendre en compte les changements.

C. Créer une session "CAD" (Contrôle A Distance) sur la passerelle Windows

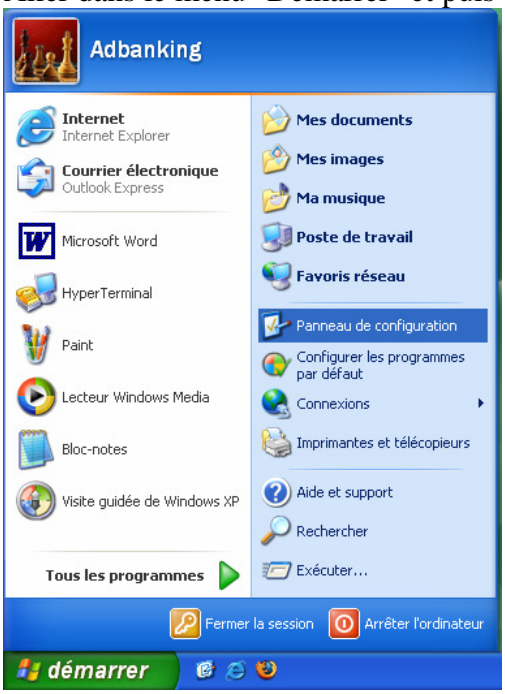
Ces étapes sont à faire sur le poste client Windows servant de passerelle!

Pré requis:

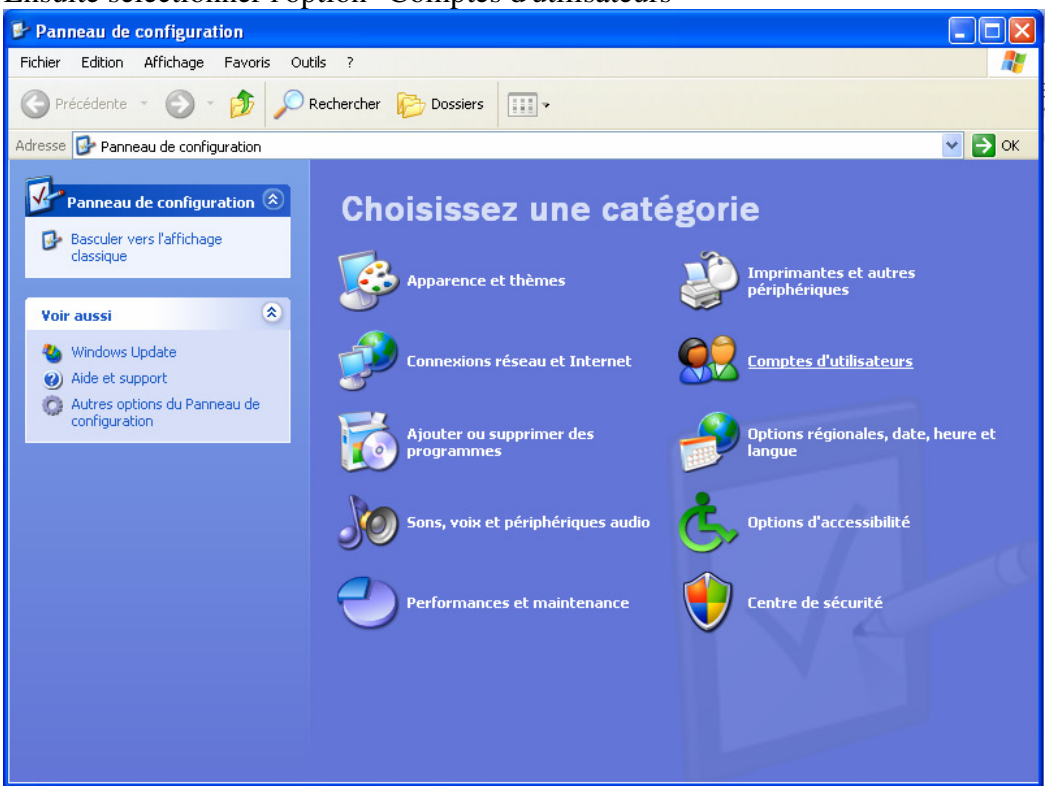
\

Procédure:

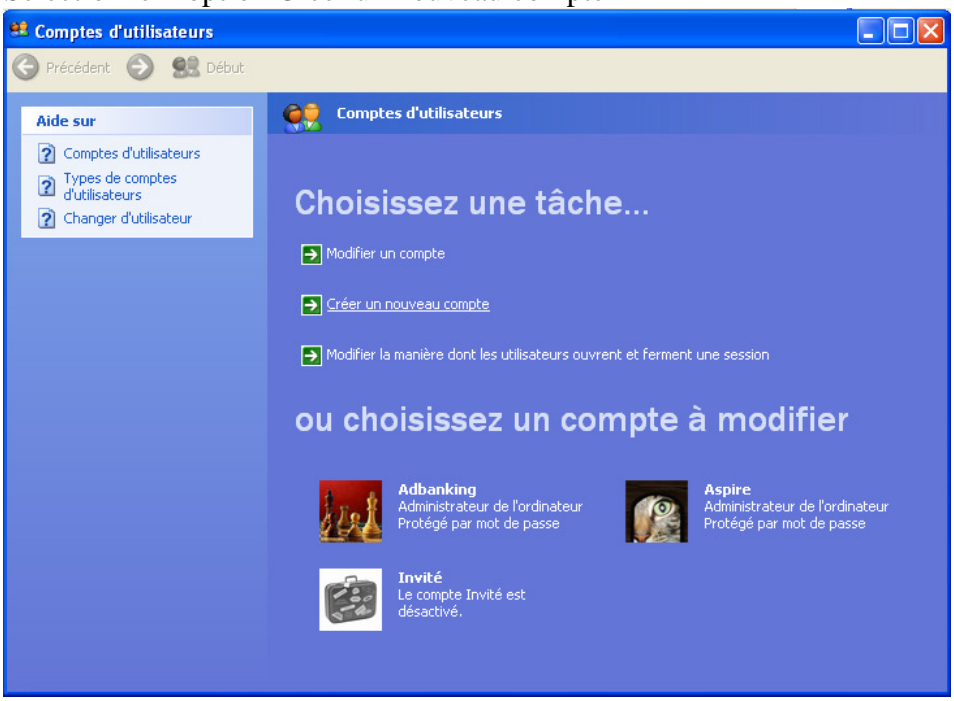
Aller dans le menu "Démarrer" et puis dans "Panneau de Configuration"



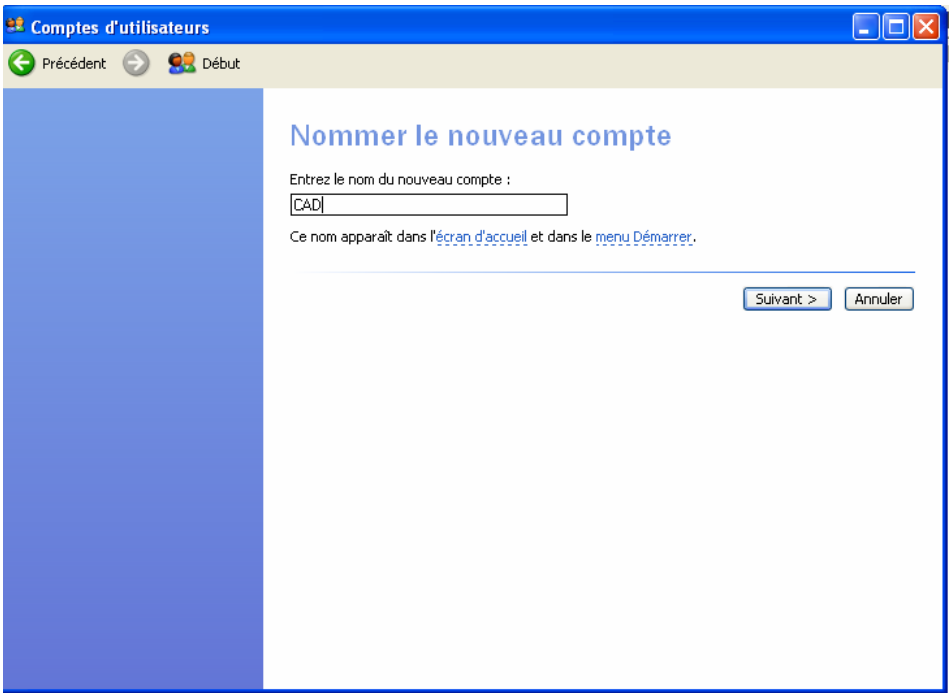
Ensuite sélectionner l'option "Comptes d'utilisateurs"



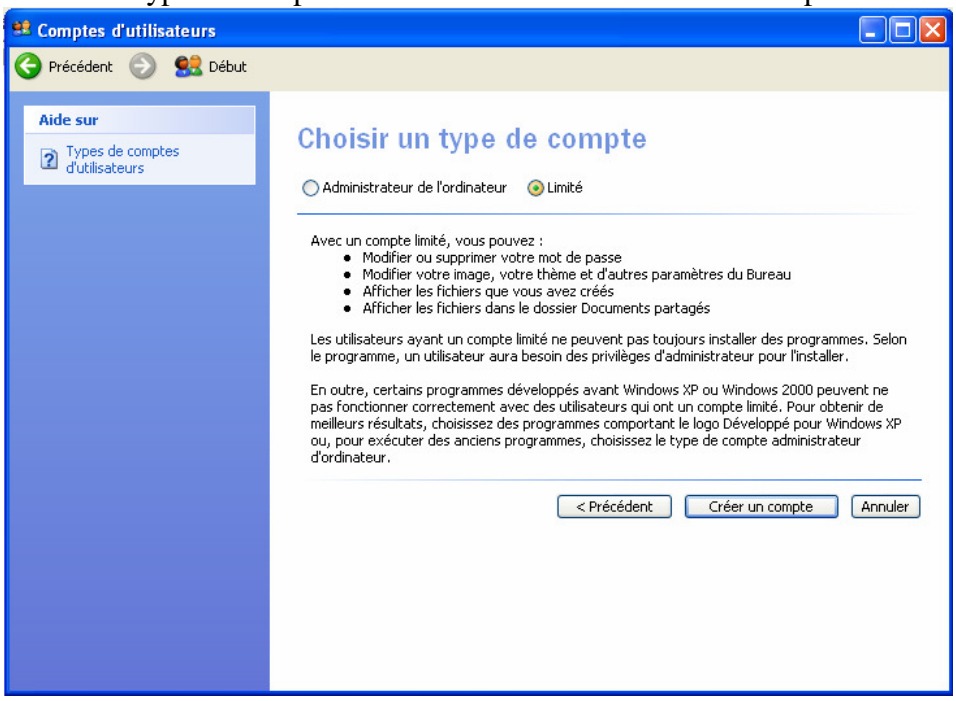
Sélectionner l'option Créer un nouveau compte



Entrer le nom d'utilisateur CAD

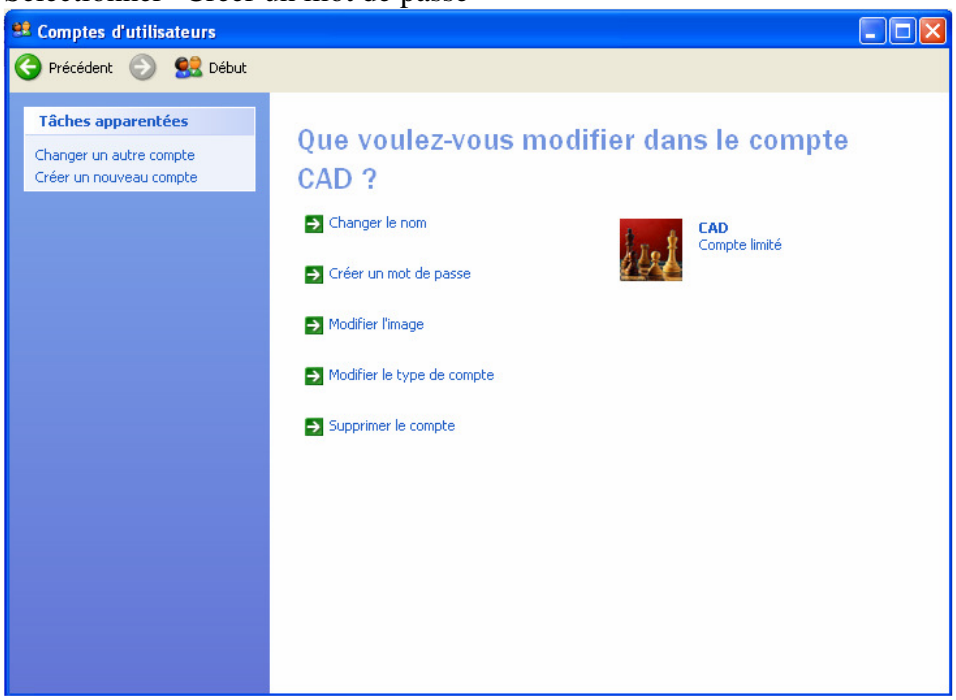


Choisir le type de compte limité et sélectionner "Créer un compte"

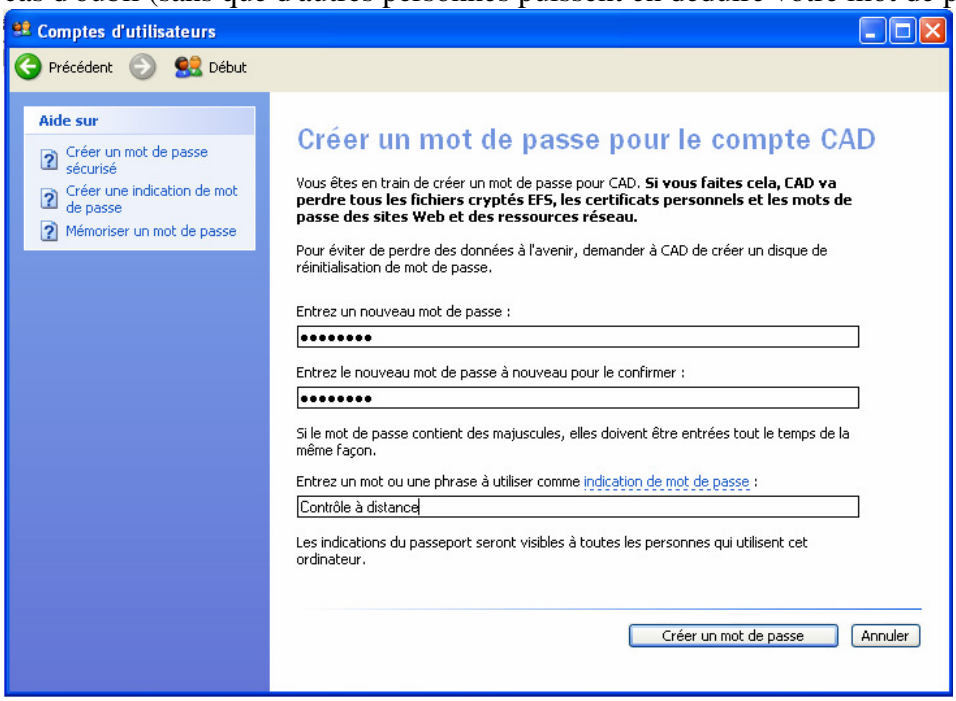


Maintenant vous devriez voir le nouveau compte qui vient d'être créé, mais il faut encore lui assigner un mot de passe. Pour ceci, cliquer sur l'icône de l'utilisateur nouvellement créé.

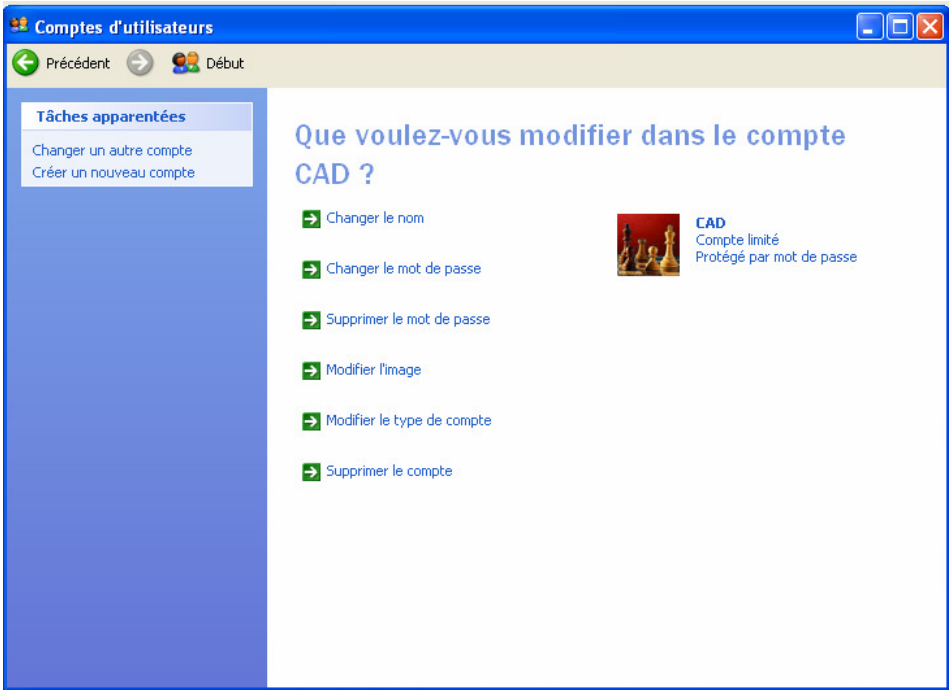
Sélectionner "Créer un mot de passe"



Remplir les champs correspondants avec le mot de passe que vous avez choisi. Entrer un mot ou une phrase dans la dernière case qui vous permettra de vous souvenir du mot de passe en cas d'oubli (sans que d'autres personnes puissent en déduire votre mot de passe évidemment).



Voila, le compte devrait être créé et protégé par un mot de passe



D. Installer cygwin sur la passerelle Windows

(Traduction partielle et amélioration de la procédure trouvée sur http://pigtail.net/LRP/printsrv/cygwin-sshd.html)

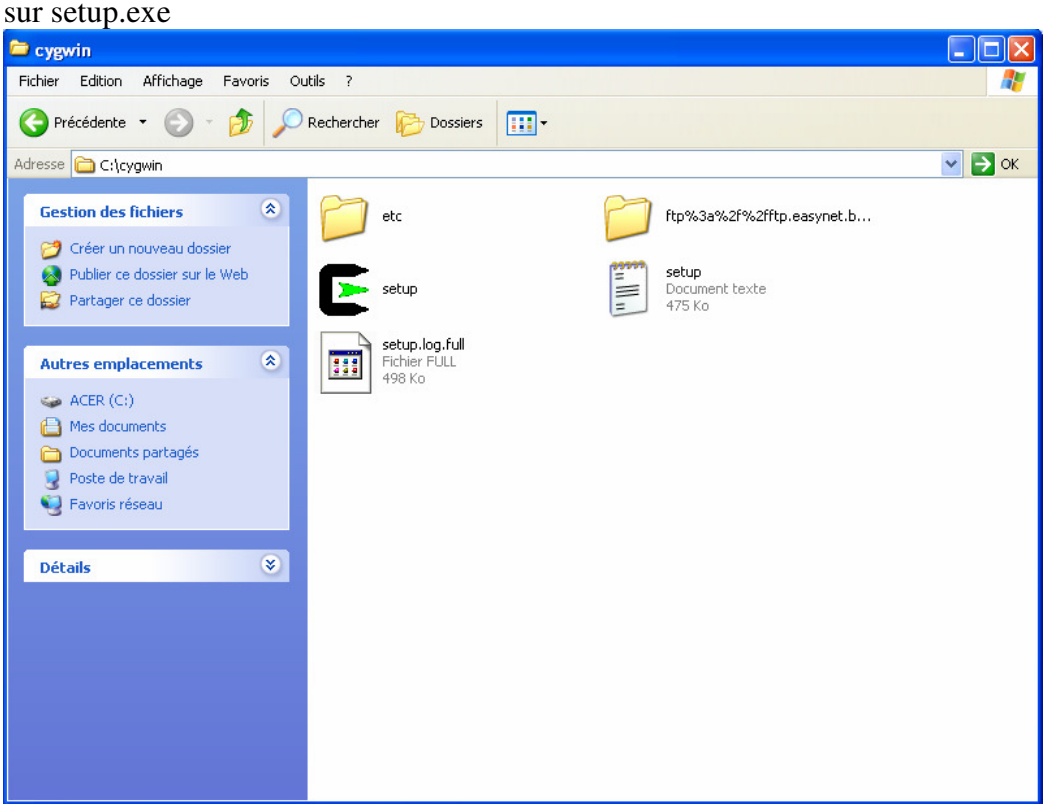
Ces étapes sont à faire sur le poste client Windows servant de passerelle!

Pré requis:

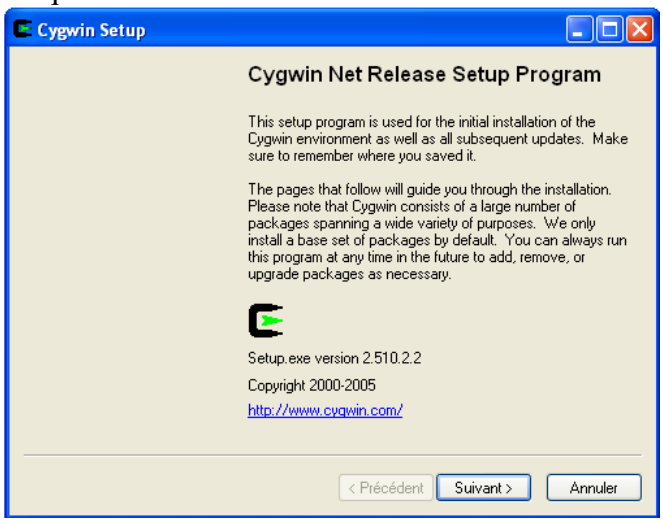
- L'existence d'une session CAD sur le système

Procédure:

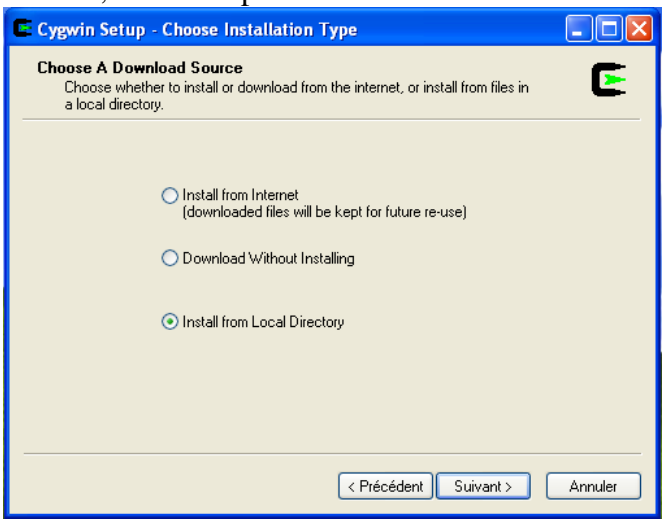
Commencer par vous logger en tant qu'administrateur sur la passerelle Windows. Ensuite créer un répertoire C:\cygwin et vous procurer les fichiers nécessaires à l'installation de cygwin via le package d'installation, soit installer à partir de http://www.cygwin.com/. Dans les deux cas il faut placer les fichiers dans le répertoire C:\cygwin\. Ensuite, double-cliquer sur setup.exe



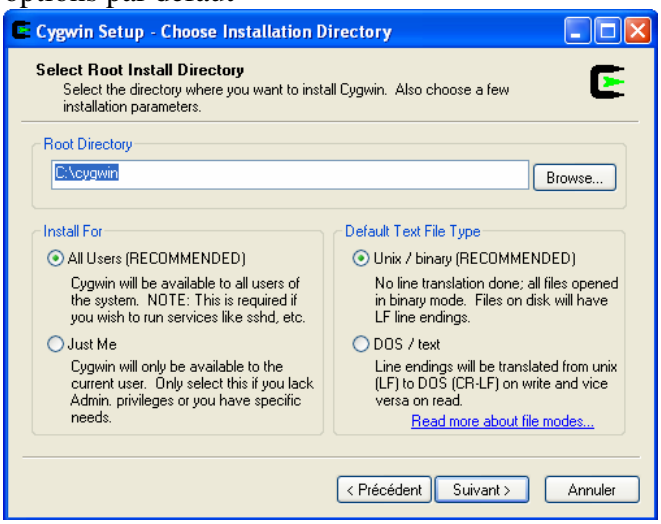
Cliquer sur suivant



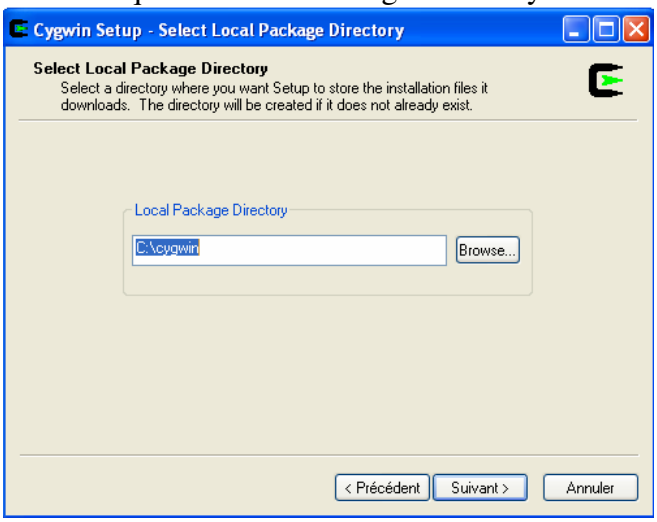
Ensuite, choisir l'option "Install from Local Directory"



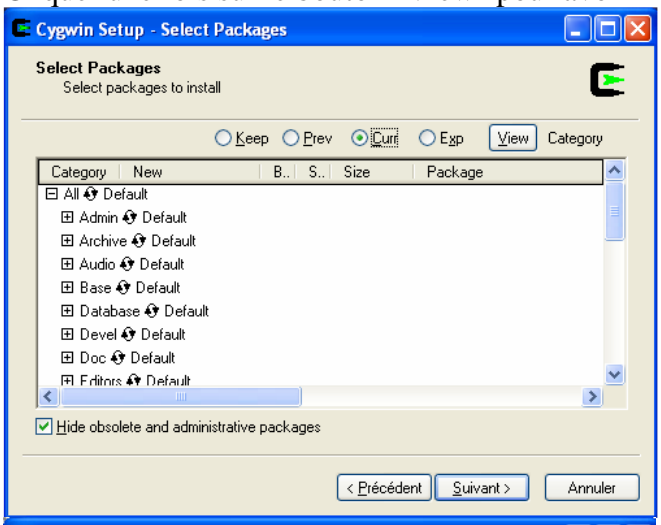
S'assurer que le chemin d'accès dans "Root Directory" soit bien C:\cygwin, laisser les autres options par défaut

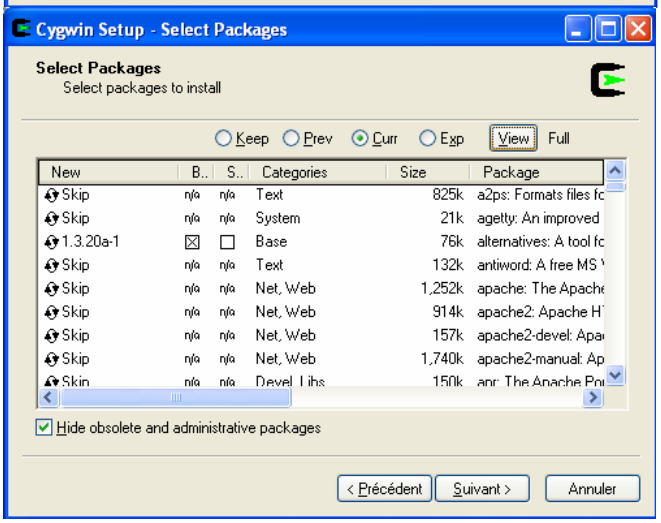


S'assurer que le "Local Package Directory" contienne bien C:\cygwin comme chemin d'accès

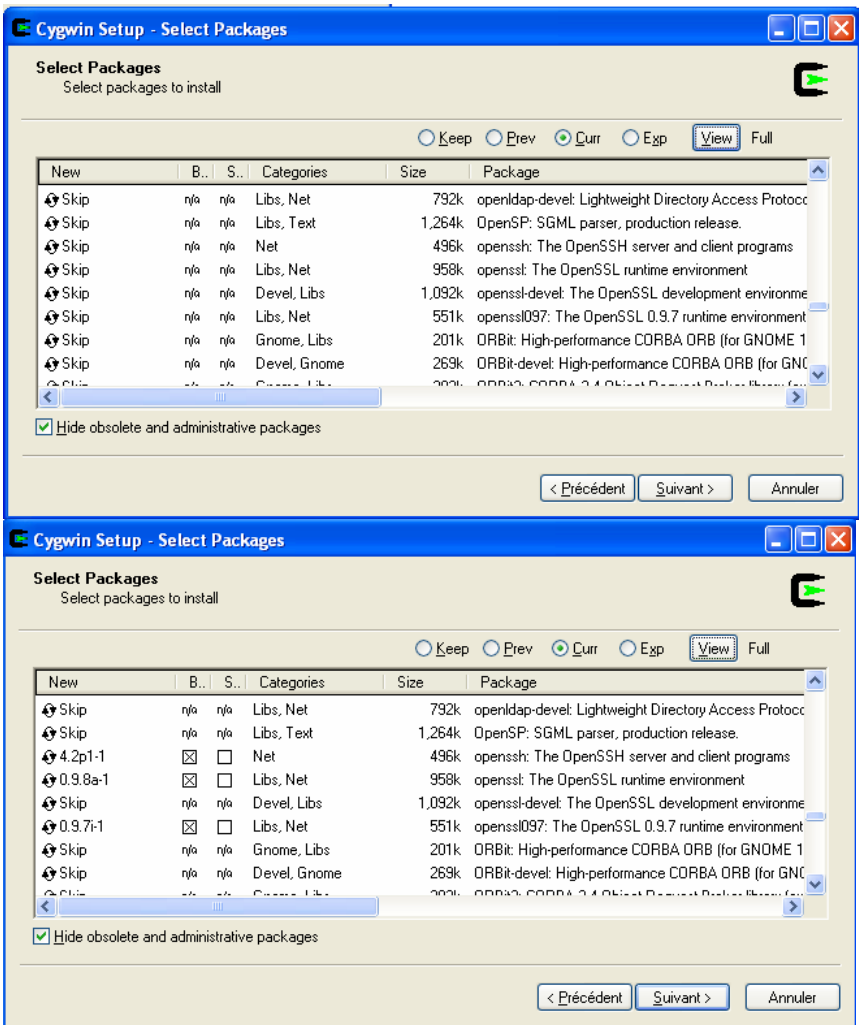


Cliquer une fois sur le bouton "View" pour avoir "Full" écrit à coté.

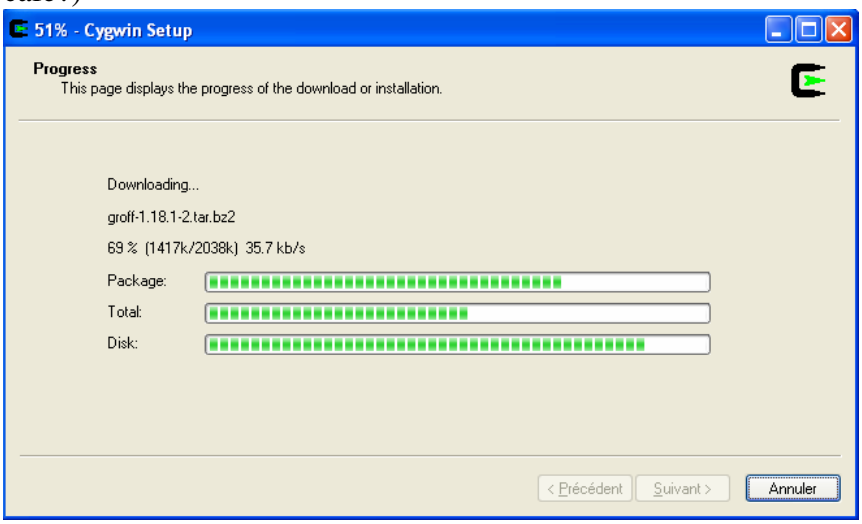




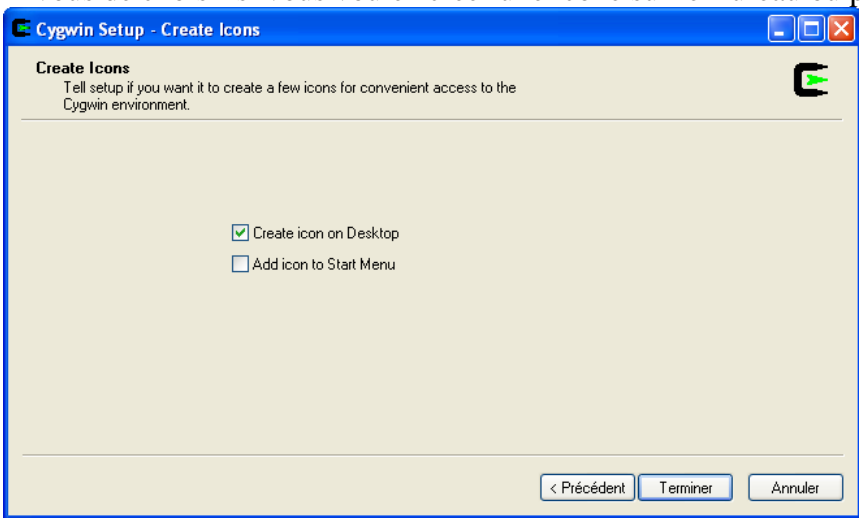
Trouver la ligne "OpenSSH" dans la colonne Package, cliquer une fois seulement sur le mot "skip" pour qu'un ☒ apparaisse dans la colonne B. D'autres ☒ apparaîtront ailleurs, c'est normal.



L'installation devrait démarrer sans poser de problèmes mais prend un certain temps (pause café?)

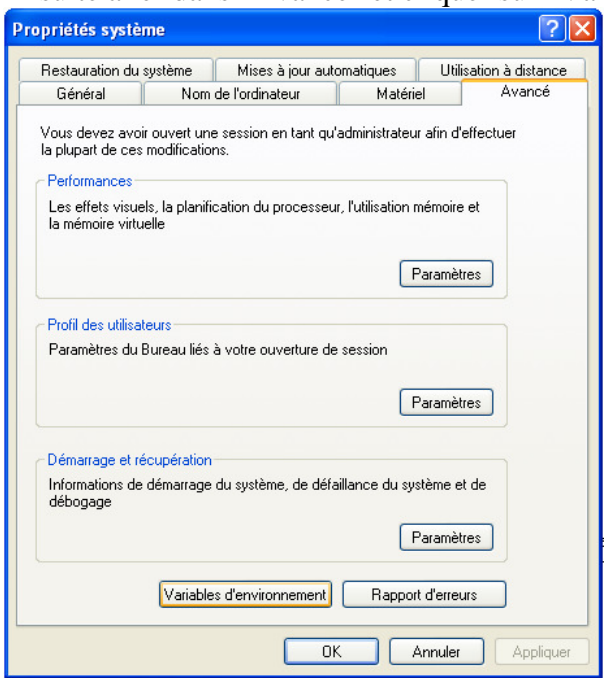


A vous de choisir si vous voulez créer une icône sur le Bureau ou pas

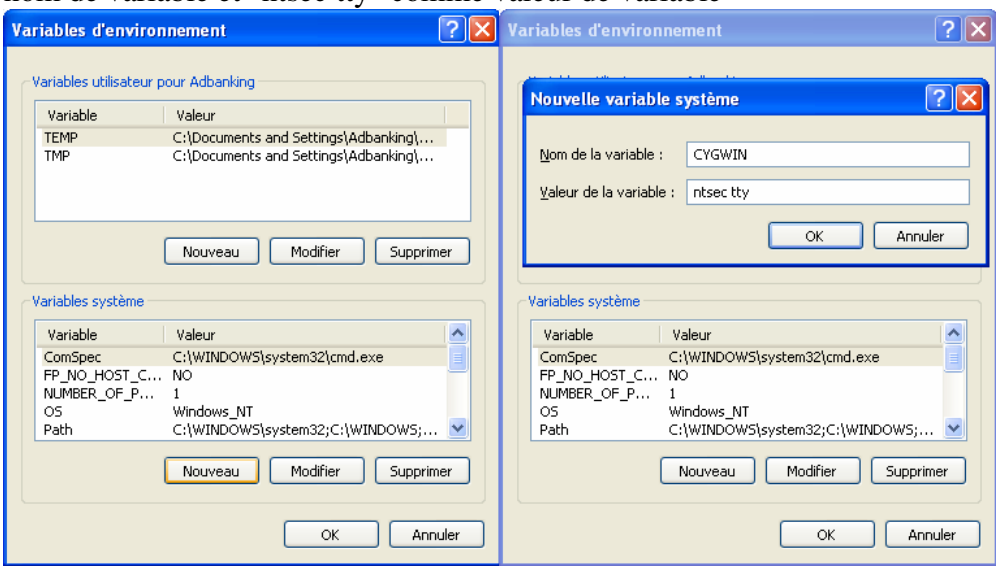


Cygwin est installé, il faut maintenant le configurer. Faire un clique-droit sur "Poste de Travail" et aller dans "Propriétés"

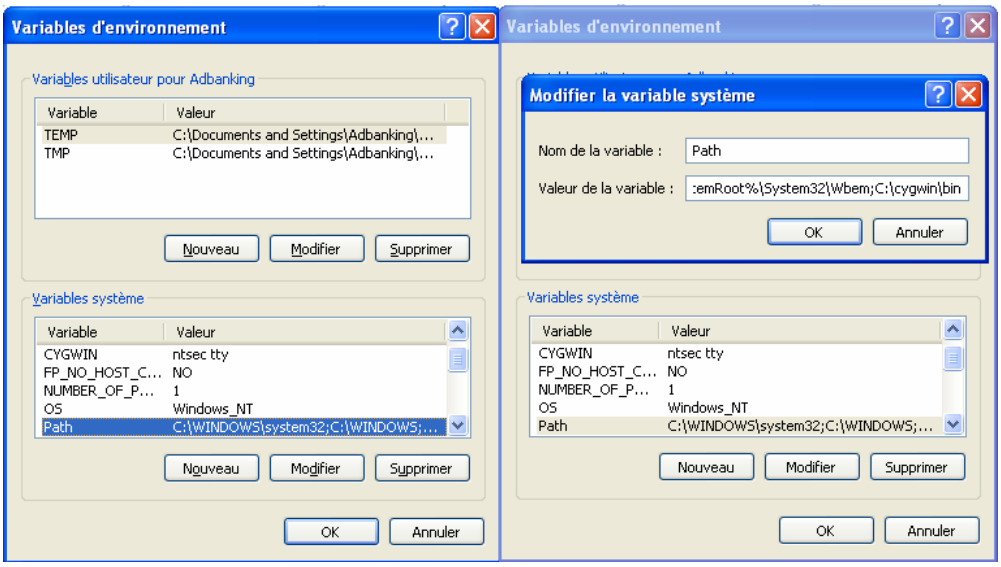
Ensuite aller dans "Avancé" et cliquer sur "Variables d'Environnement"



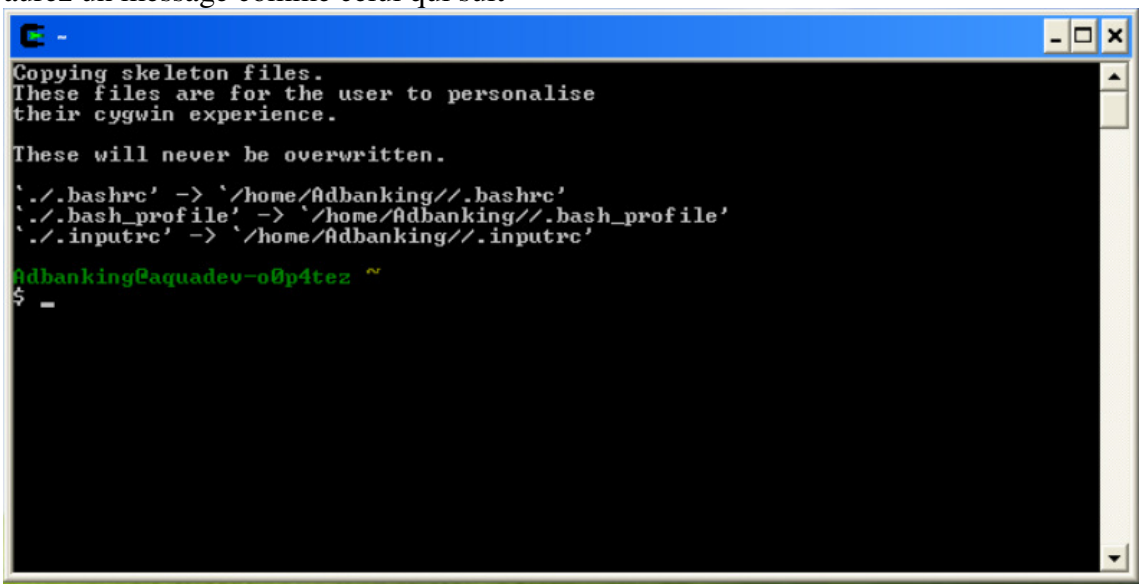
Cliquer sur le bouton "Nouveau" dans "Variables Système" et mettre "CYGWIN" comme nom de variable et "ntsec tty" comme valeur de variable



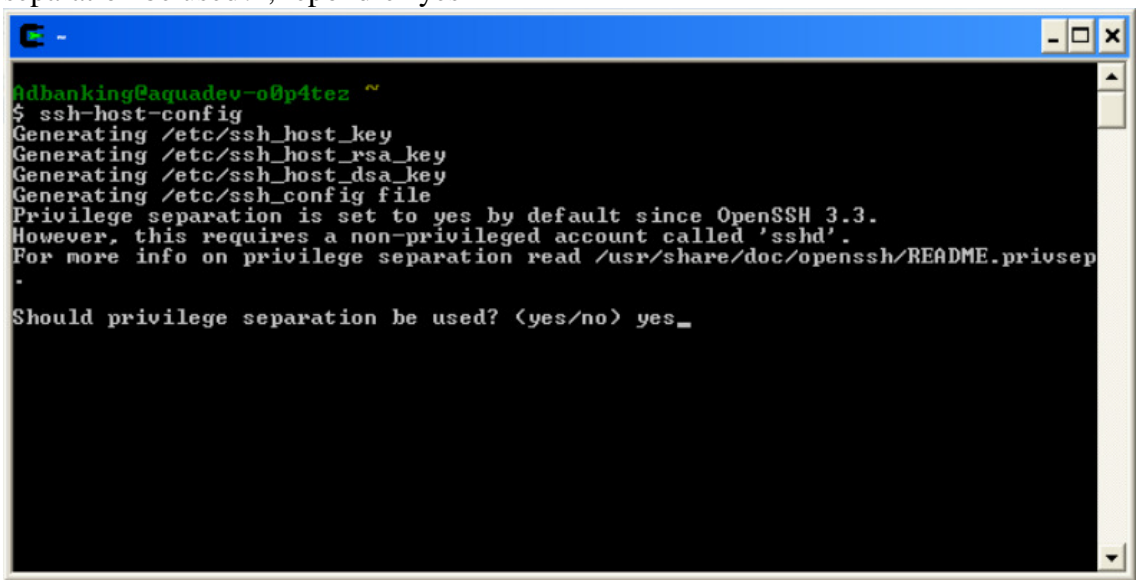
Toujours dans les "Variables d'Environnement", sélectionner la variable système "Path", cliquer sur le bouton "Modifier", et rajouter ";C:\cygwin\bin"à la fin de valeur existante de la variable



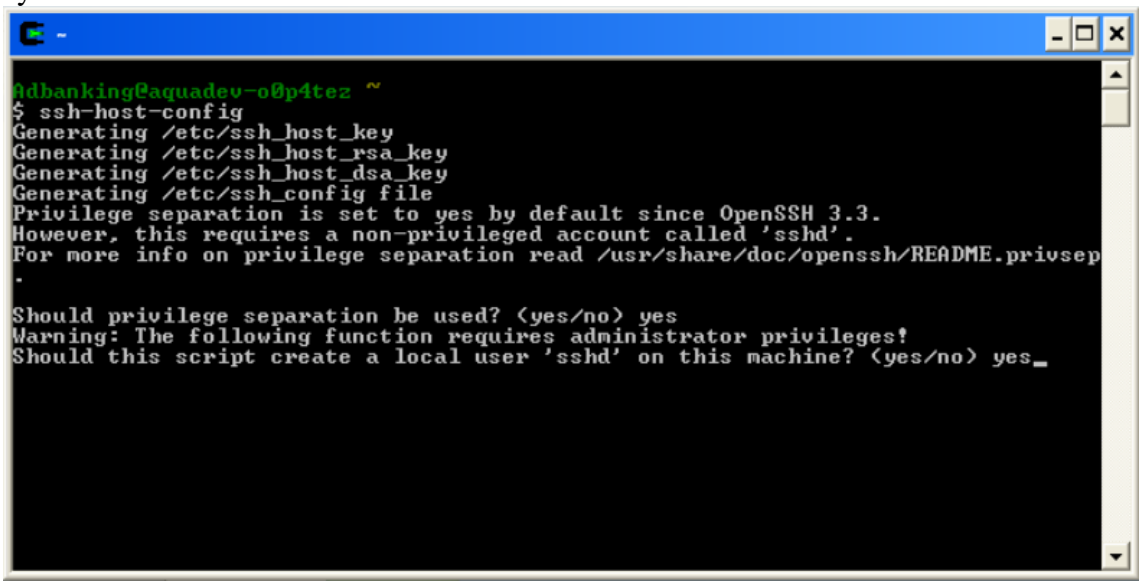
Ensuite ***se logger en tant que "CAD"*** et ouvrir une fenêtre cygwin en double-cliquant sur , l'icône de cygwin. La première fois que vous ouvrirez une fenêtre cygwin, vous aurez un message comme celui qui suit



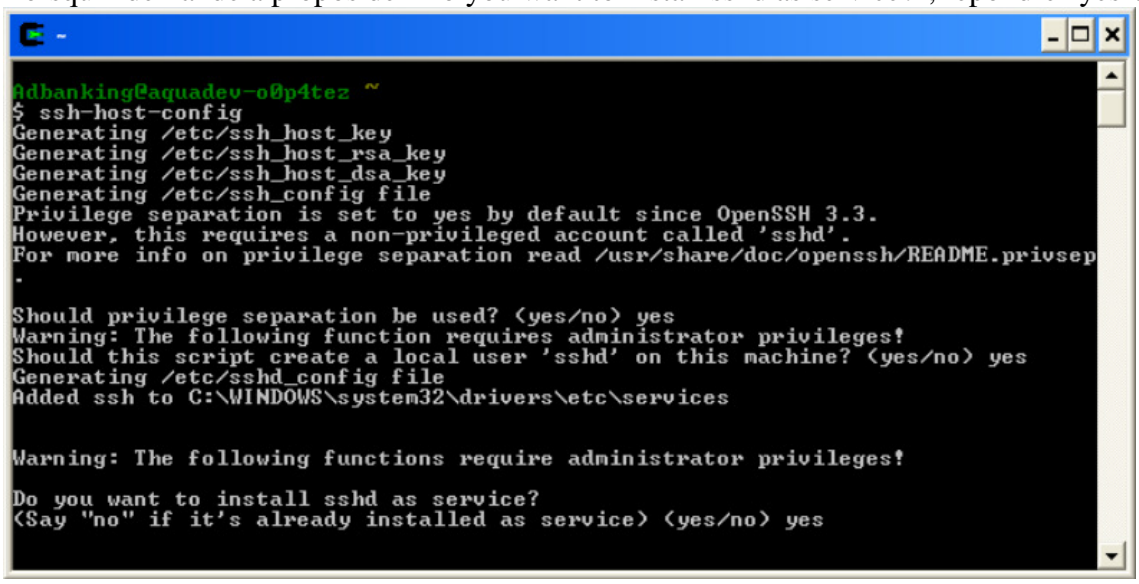
Dans la fenêtre qui apparaît, taper "ssh-host-config". Lorsqu'il demande "Should privilege separation be used?", répondre "yes"



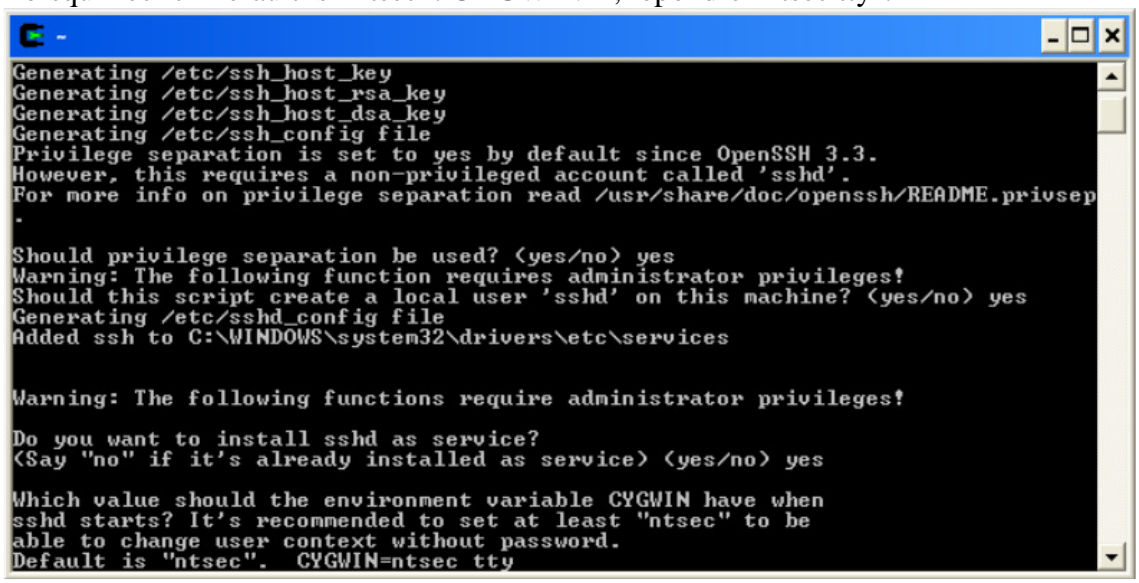
Lorsqu'il demande "Should this script create a local user 'sshd' on this machine?", répondre "yes"



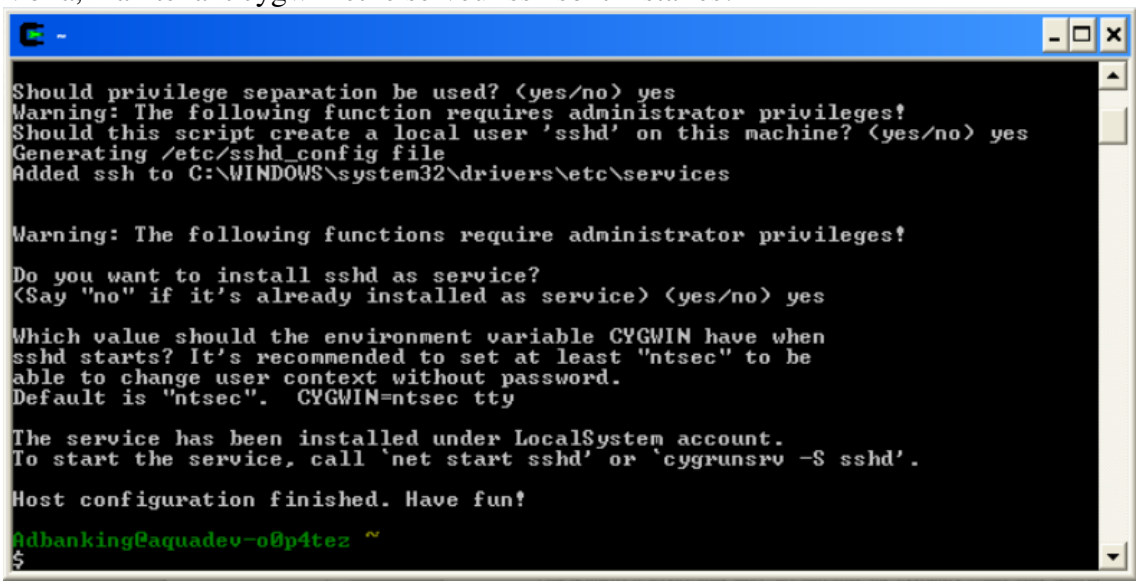
Lorsqu'il demande à propos de "Do you want to install sshd as service?", répondre "yes".



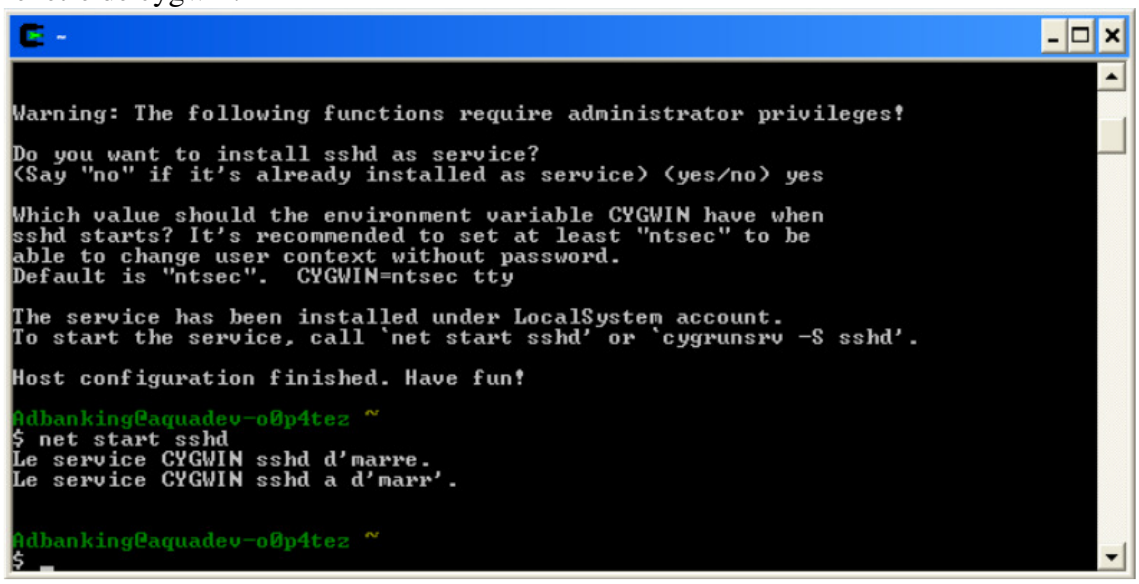
Lorsqu'il écrit "Default is «ntsec». CYGWIN=", répondre "ntsec tty".



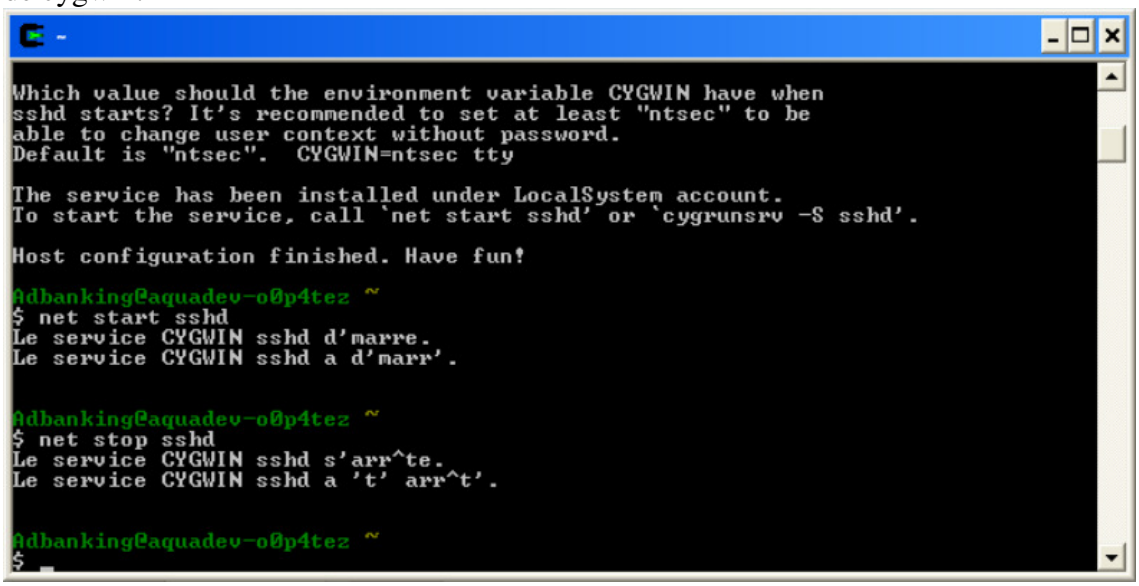
Voilà, maintenant cygwin et le serveur ssh sont installés!



Pour démarrer le service sshd, taper "net start sshd" ou "cygrunsrv --start sshd" dans la fenêtre de cygwin.

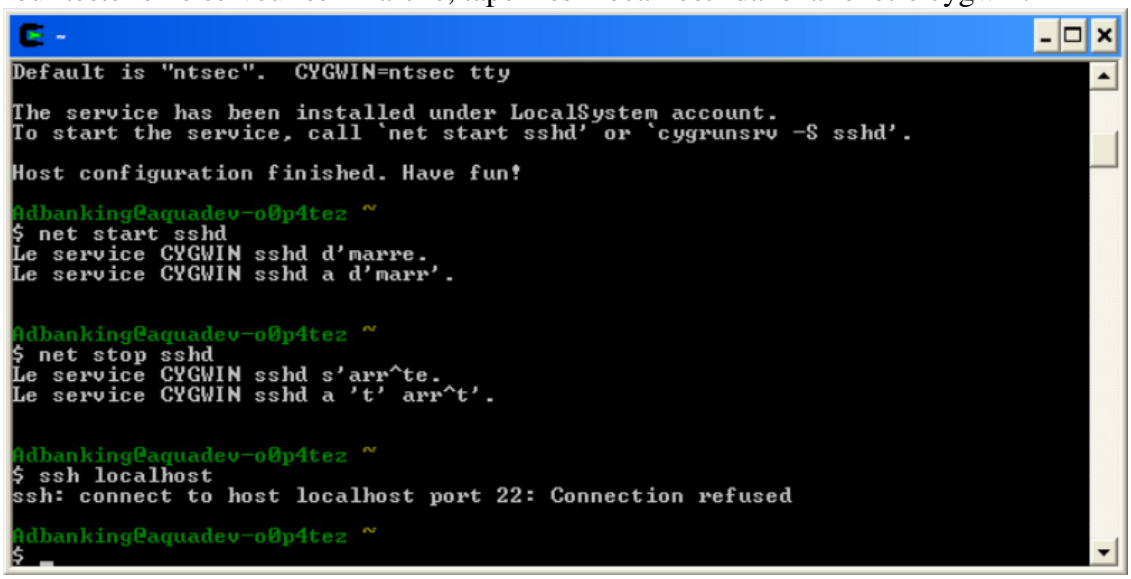


Pour arrêter le service sshd, taper "net stop sshd" ou "cygrunsrv --stop sshd" dans la fenêtre de cygwin.

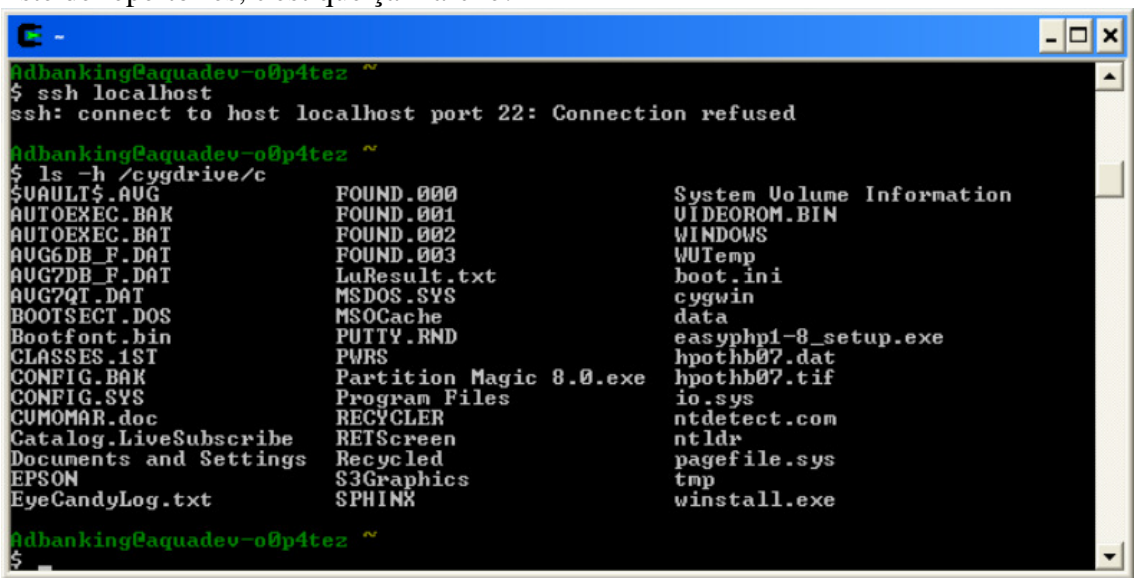


Normalement le service démarrera tout seul la prochaine fois que l'ordinateur sera allumé.

Pour tester si le serveur ssh marche, taper "ssh localhost" dans la fenêtre cygwin.



Si vous obtenez une erreur "Connection refused", taper "ls –h /cygdrive/c". Si vous voyez une liste de répertoires, c'est que ça marche!



E. Copier la clé publique sur la passerelle Windows

Ces étapes sont à faire sur le poste client Windows servant de passerelle!

Pré requis:

- Toutes les étapes précédentes ont étés effectuées convenablement
- Une clé publique à été générée du coté contrôlant et elle est en votre possession

Procédure:

- ouvrir une fenêtre cygwin
- taper "ssh-user-config"
- lorsqu'il demande "Shall I create an SSH1 RSA identity file for you? (yes/no)" répondre "no"
- lorsqu'il demande "Shall I create an SSH2 RSA identity file for you? (yes/no)" répondre "yes"
- lorsqu'il demande "Enter passphrase (empty for no passphrase):" entrer un mot de passe ou laisser vide
- lorsqu'il demande "Enter same passphrase again:" répéter le mot de passe si vous en avez fourni un
- lorsqu'il demande "Do you want to use this identity to login to this machine? (yes/no)" répondre "yes"
- lorsqu'il demande "Shall I create an SSH2 DSA identity file for you? (yes/no)" répondre "no"
- ouvrir le fichier "Authorized_Keys" se trouvant dans "C:\cygwin\home\CAD\.ssh\" avec Wordpad
- ouvrir également le fichier contenant la clé publique que vous allez copier
- à la fin du fichier "Authorized_Keys", rajouter un saut à la ligne, "ssh-rsa ", et ensuite la clé.
- Par exemple, si la clé publique s'affiche comme ceci

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20051102"
AAAAB3NzaC1yc2EAAAABJQAAAIBq4j5pE0cdPuVgloYlowZTlADbDWbhSlVqxbA
t
+WuOBciTkCIkh8JwAYlp0YnfxE54+UxJn27LMy4BqJefaINlpVKvly77p4JbVy0
X
gBV/z1owovAdHXzM2Z//3ECK/p8Ptsno6W51SEUhTtidFZd4slW7cg3r4+AF8Qh
A
Y4FWIw==
---- END SSH2 PUBLIC KEY ----
```

- alors on rajouterait ceci (en supprimant les sauts de ligne pour que le tout tienne sur une ligne)

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIBq4j5pE0cdPuVgloYlowZTlADbDWbhSlVqxbA
t+WuOBciTkCIkh8JwAYlp0YnfxE54+UxJn27LMy4BqJefaINlpVKvly77p4JbVy
0XgBV/z1owovAdHXzM2Z//3ECK/p8Ptsno6W51SEUhTtidFZd4slW7cg3r4+AF8
QhAY4FWIw==
```

- sauvegarder et fermer les fichiers
- ouvrir une fenêtre cygwin et taper "cd /etc", ensuite "chmod a+w sshd_config"
- taper maintenant "ls -l" et normalement l'avant dernière ligne devrait ressembler à:

-rw-rw-rw- 1 SYSTEM Aucun 2932 Nov 8 11:57 sshd_config

- ouvrir le fichier "C:\cygwin\etc\sshd_config" avec wordpad et rechercher les phrases "#PasswordAuthentication" et "#ChallengeResponseAuthentication", ceux-ci devraient être suivis de "no". Si ce n'est pas le cas, modifier le fichier pour que les phrases ressemblent à "PasswordAuthentication no" et "ChallengeResponseAuthentication no" (surtout ne pas oublier de supprimer les "#" précédant la phrase).
- sauvegarder le fichier et redémarrer le service sshd ou même redémarrer complètement la machine pour être sur